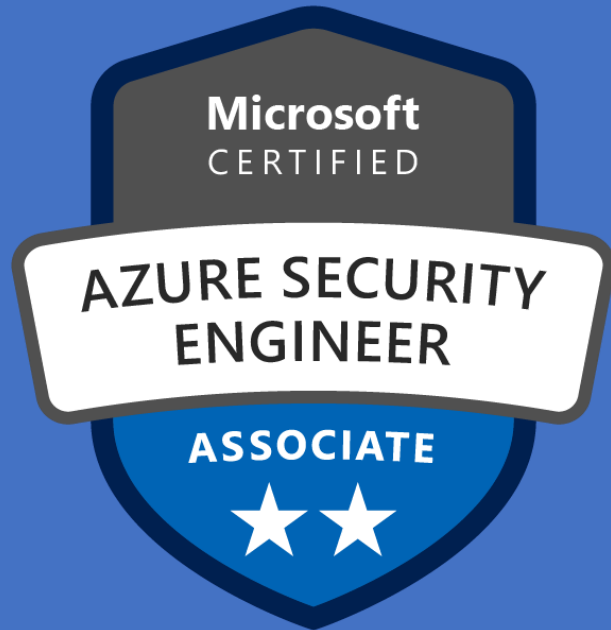




AZ-500

Episode 01

AZ-500 Course Introduction

Hello! Instructor Introduction



Susanth Sutheesh

Blog: AGuideToCloud.com

 [@AGuideToCloud](https://twitter.com/AGuideToCloud)



Skills measured



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

Additional Resources (Optional)



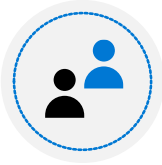
Microsoft Learn



Azure Documentation



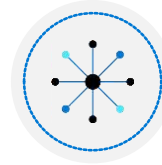
Azure Forum



Azure Tuesdays with Corey



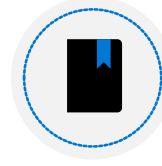
Azure Fridays with Scott Hanselman



Channel 9



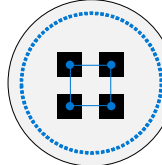
Microsoft Azure Blog



Microsoft Learning Community Blog



Bookmarks are in your training materials – Welcome section



A Guide To Cloud with Susanth Sutheesh

About this Course



Audience

Prerequisites

Azure Security Engineers

Course Syllabus



Module 01: Manage Identity and Access

Module 02: Implement Platform Protection

Module 03: Secure Data and Applications

Module 04: Manage Security Operations

Exam Basics



40-60 questions

- Some questions worth more than 1 point
- Answer all the questions
 - *No penalty for guessing*
 - *Some questions cannot be skipped!*
- Mark items for review if you're not sure of your answer



Plan for 180 minutes

- 150 minutes to answer questions
- 30 minutes for instructions, comments, score reporting, etc.



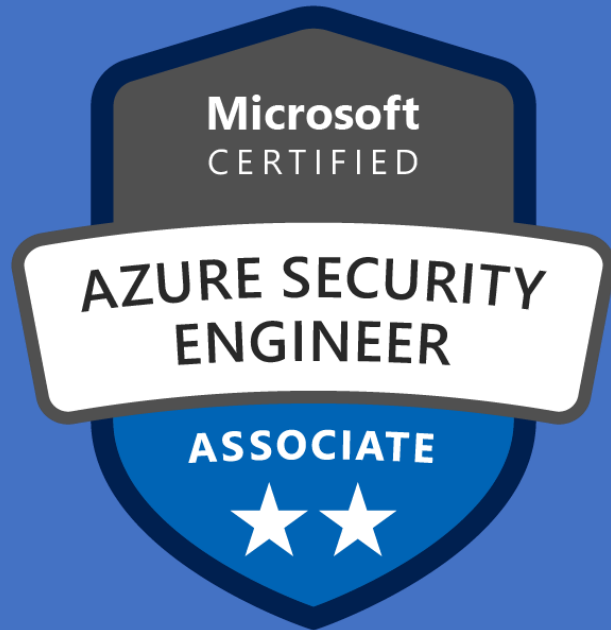
More than just multiple-choice questions!

- Build list, hot area, active screen, drag and drop, etc.



Case Studies

- Detailed information on business and technical requirements; existing environment and other background you need to solve problems
- Requires you to understand and integrate information across multiple sources, determine what's important, and make the best decision



AZ-500

Episode 02

Azure Active Directory





Azure AD Lesson Objectives



Azure AD Features



Azure AD vs AD DS



Roles for Azure AD



Azure AD Domain Services



Azure AD Users



Azure AD Groups



Azure MFA Concepts

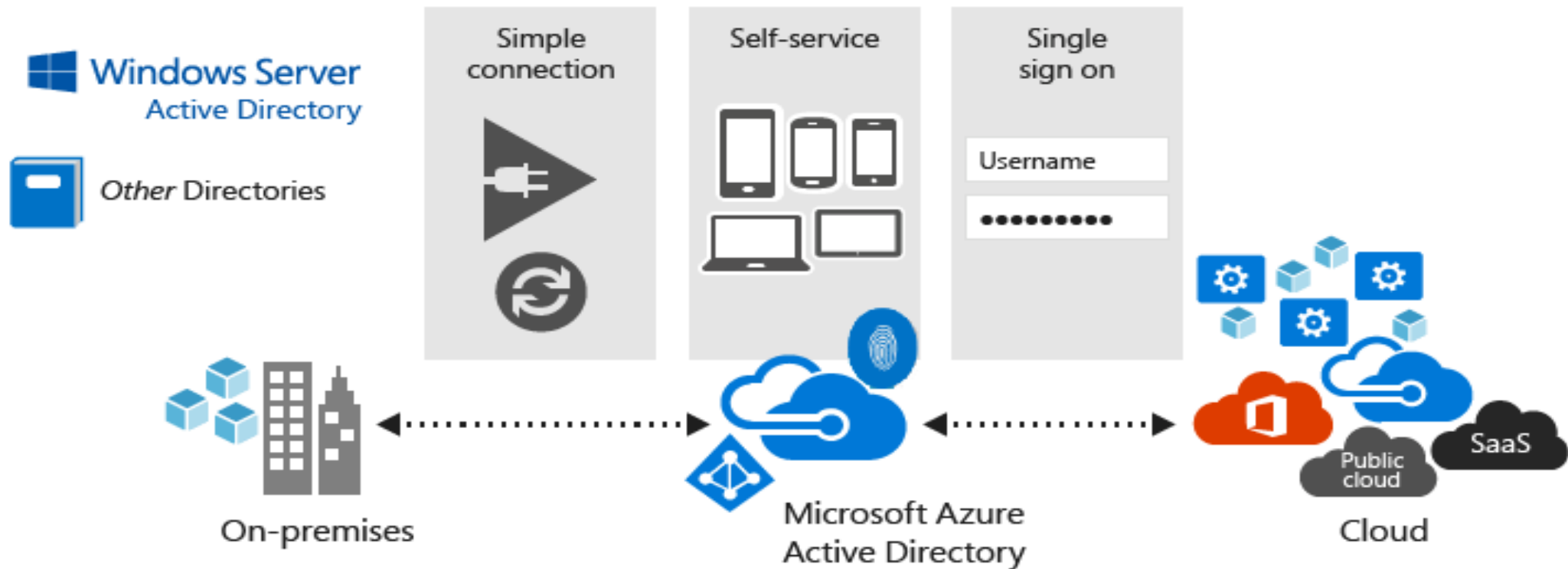


Enabling MFA

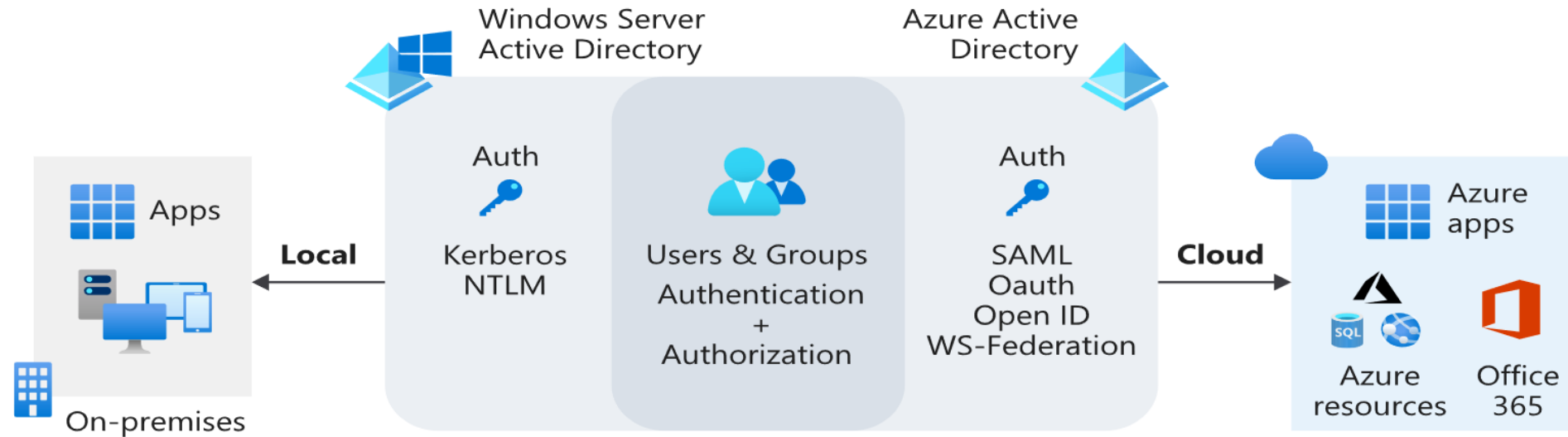


MFA Settings

Azure Active Directory Features



Azure AD vs Active Directory



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

Azure AD Characteristics



Identity Solution

REST API Querying

Communication Protocols

Authentication Services

Authorization Service

Federation Services

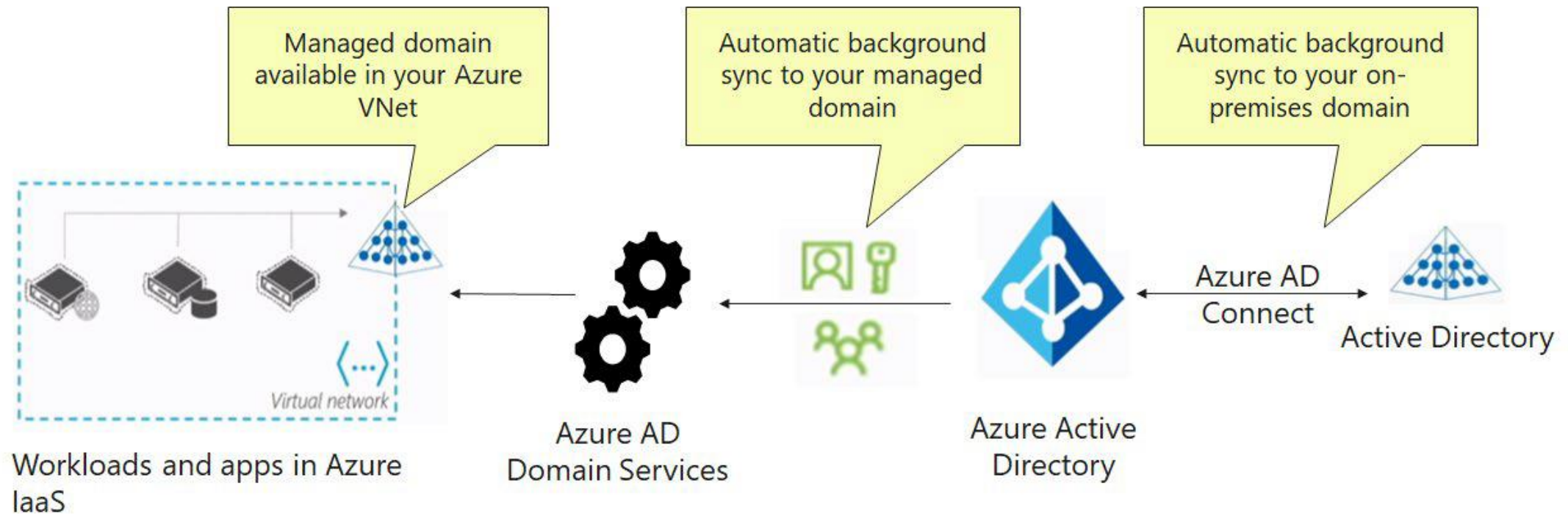
Flat Structure

Azure AD Administrator Roles



Built-in Role	Description
Global Administrator	Users with this role have access to all administrative features in Azure Active Directory
Security Administrator	Users with this role have permissions to manage security-related features in the Microsoft 365 Security Center, Security Center, Azure Active Directory Identity Protection, Azure Information Protection, and Office 365 Security & Compliance Center
Directory Reader	Makes purchases, manages subscriptions, manages support tickets, and monitors service health
Global Reader	Users in this role can read settings and administrative information across Microsoft 365 services but can't take management actions.

Azure AD Domain Services



Azure AD DS Features & Benefits



Simplified deployment experience

Integrated with Azure AD

Use your corporate credentials/passwords

NTLM and Kerberos authentication

High availability

Azure AD Users



Users - All users
microsoft - Azure Active Directory

Search (Ctrl+/) << + New user + New guest user Reset password Delete user Multi-Factor Authentication Refresh Columns

NAME	USER NAME	USER TYPE	SOURCE
 Retail Crisis Notifications	 @microsoft.com	Member	Windows Server AD
 "Planning & Launch Services OEM Inquiries	 @microsoft.com		Windows Server AD
 Bert	 @hotmail.com	Guest	Azure Active Directory
  @fi.pwc.com	 @fi.pwc.com	Guest	Azure Active Directory

Cloud Identities

Directory-synchronized identities

Guest users

Azure AD Group Accounts



Users and groups - All groups

Search (Ctrl+ /)

Overview

MANAGE

All users

All groups

Search groups

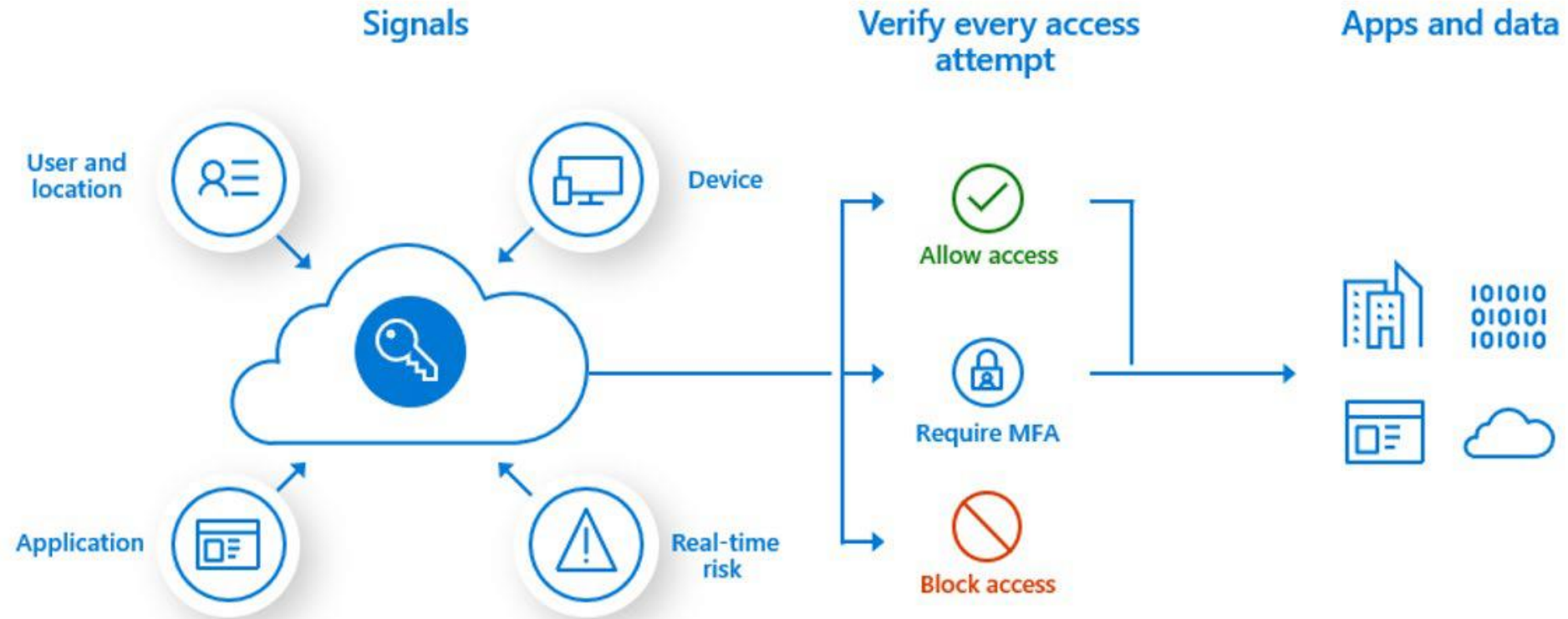
NAME	GROUP TYPE	MEMBERSHIP TYPE
GR Group1	Security	Assigned
GR Group2	Security	Assigned
GR Group23	Security	Assigned

Assigned

Dynamic User

Dynamic Device (Security Groups Only)

Azure Multi-Factor Authentication



Azure MFA Features



Get more security with less complexity

Mitigate threats with real-time monitoring and alerts

Deploy on-premises or on Azure

Use with Office 365, Salesforce, and more

Add protection for Azure administrator accounts

MFA Authentication Options



multi-factor authentication
users **service settings**

verification options [\(learn more\)](#)

Methods available to users:

- ☒ Call to phone
- ☒ Text message to phone
- ☒ Notification through mobile app
- ☒ Verification code from mobile app or hardware token

save

Call to Phone

Text message to phone

Notification through Mobile App

Verification code from Mobile App

MFA Settings



Account Lockout

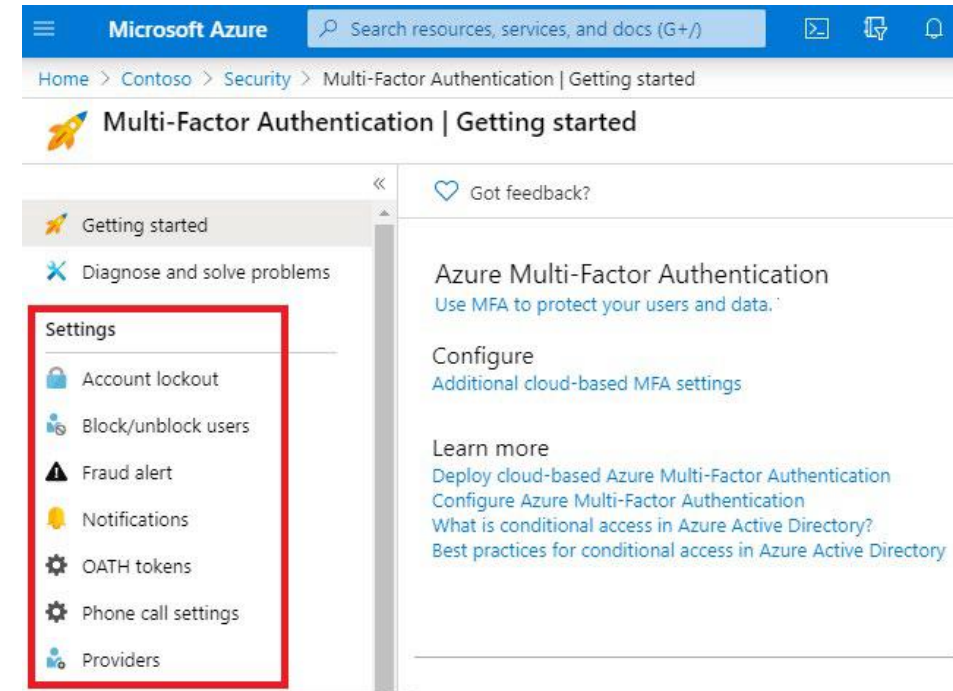
Block and unblock users

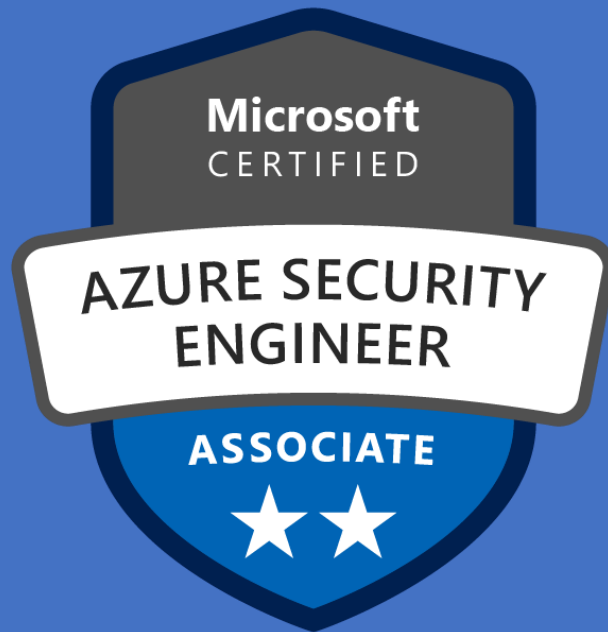
Fraud Alerts

Notifications

OAUTH tokens

Trusted IPs





AZ-500

Episode 03

Azure AD Identity Protection

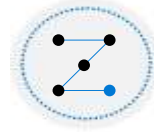




Azure AD Identity Protection Lesson Objectives



Azure AD Identity Protection



Risk Events



User Risk Policy



Sign-in Risk Policy



Azure AD Conditional Access



Conditions



Access Reviews

Identity Protection Policies



Policy name Multi-factor authentication registration policy Assignments Users ⓘ All users Controls Access ⓘ Require Azure MFA registration ⓘ MFA Registration Policy only affects cloud-based Azure MFA. If you have MFA Server it will not be affected. Enforce Policy ☒ On ☐ Off	Policy name User risk remediation policy Assignments Users ⓘ All users Conditions ⓘ User risk Controls Access ⓘ Require password change Review Estimated impact ⓘ Number of users impacted Enforce Policy ☒ On ☐ Off	Policy name Sign-in risk remediation policy Assignments Users ⓘ All users Conditions ⓘ Sign-in risk Controls Access ⓘ Require multi-factor authentication Review Estimated impact ⓘ Number of sign-ins impacted Enforce Policy ☒ On ☐ Off
--	--	---

Azure MFA Registration Policy

Sign-in risk policy

Custom Conditional Access policy

Risk Events



Leaked credentials

Sign in from anonymous IP addresses

Impossible travel to atypical locations

Sign-in from unfamiliar locations

Sign-ins from infected devices

Sign-ins from IP addresses with suspicious activity

Vulnerabilities ⓘ

5

RISK LEVEL	COUNT	VULNERABILITY
Low	14	Unmanaged apps discovered in last 7 days
Medium	382	Users without multi-factor authentication registration
Low	8	Redundant administrators increase your attack surface
Medium	17	Weak authentication is configured for role activation
Low	15	Too many global administrators increase your attack surface

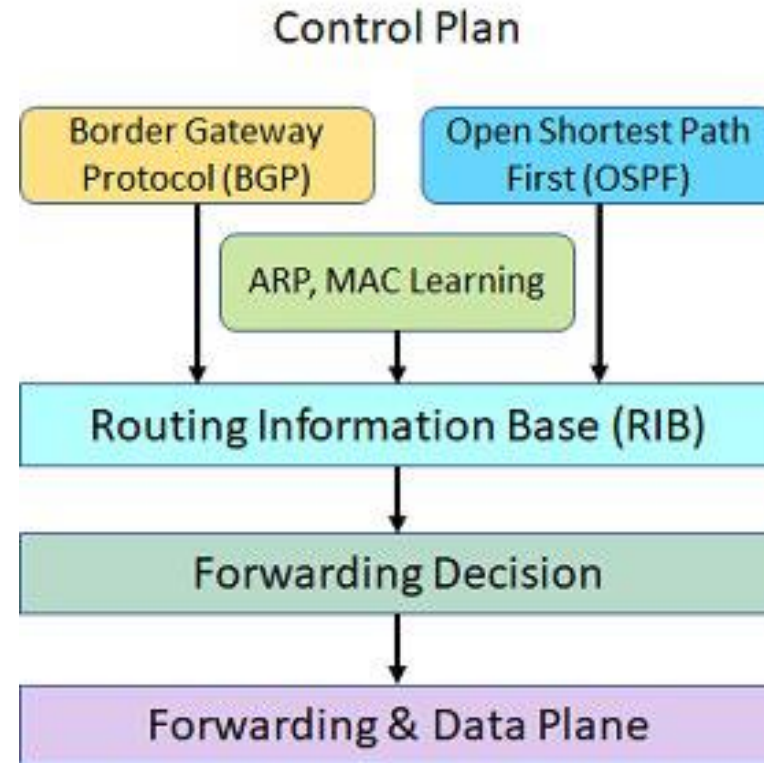
User Risk Policy



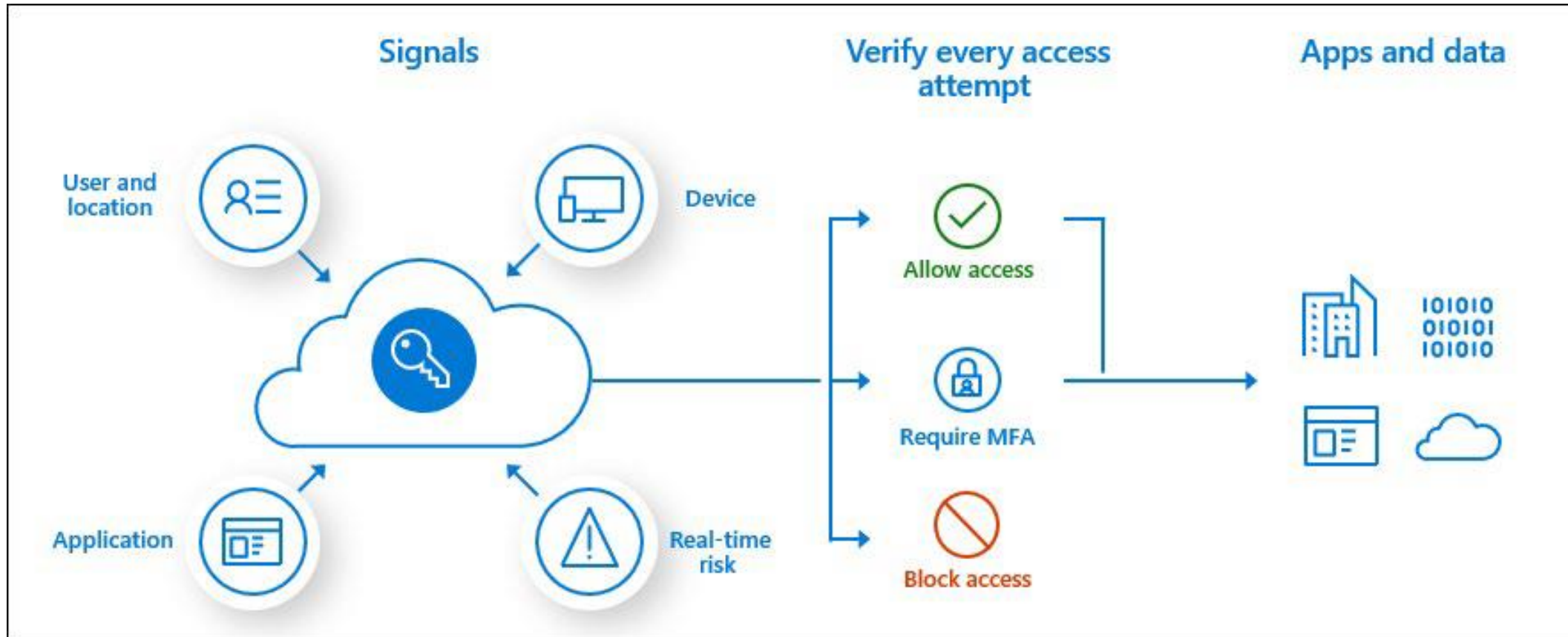
Sign-in Risk Policy



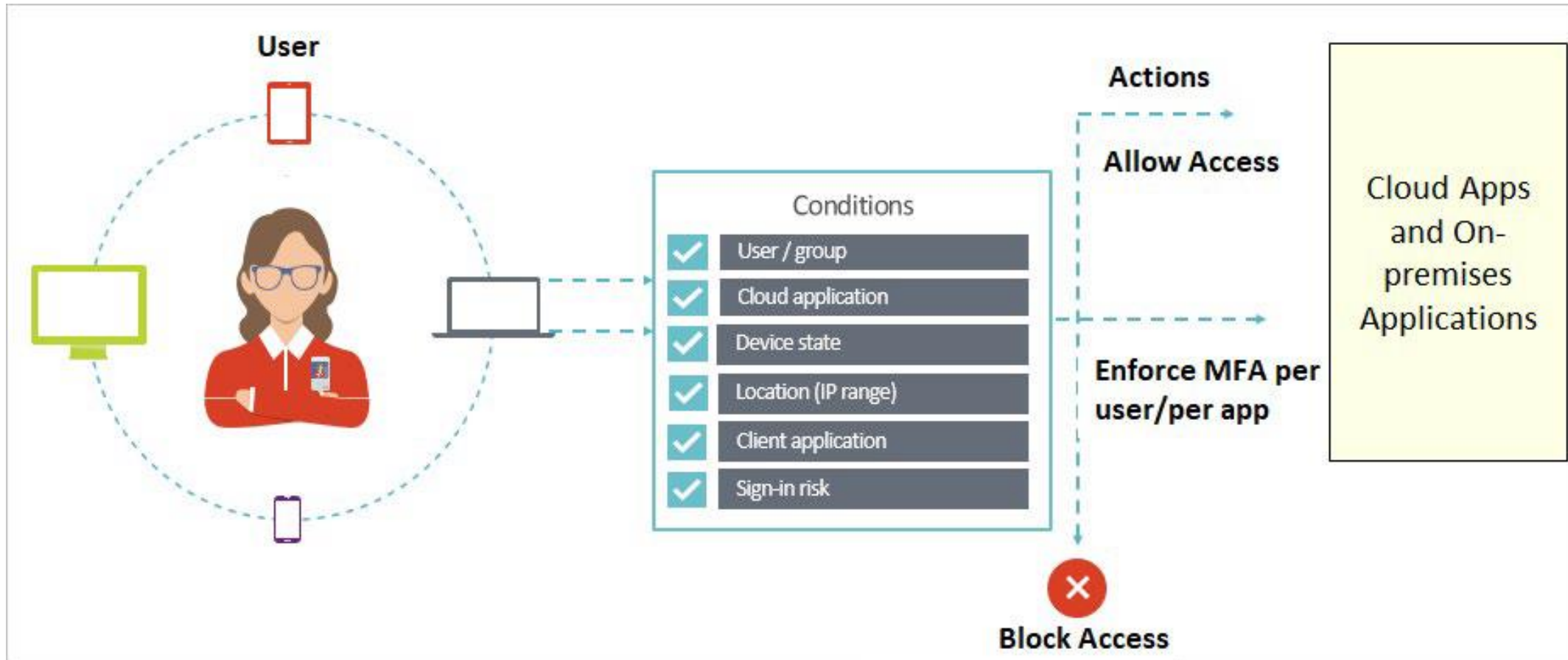
Identity as a Service



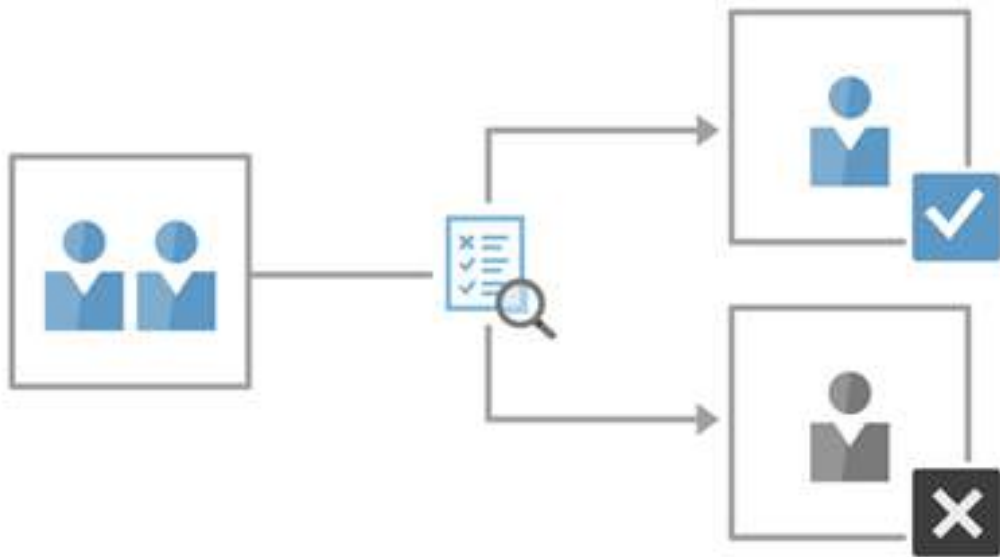
Azure AD Conditional Access



Conditions



Access Reviews



Too many users in privileged roles

When automation is infeasible

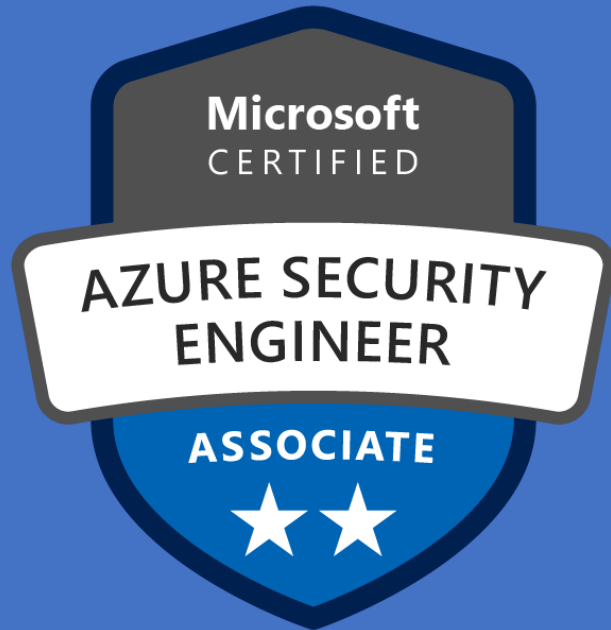
When group is used for new purpose

Business critical data access

To maintain a policy's exception list

Ask group owners to confirm

Have reviews recur periodically



AZ-500

Episode 04

Enterprise Governance





Enterprise Governance Lesson Objectives



Shared Responsibility Model



Azure Cloud Security Advantages



Azure Hierarchy



Azure Policy



Azure Role Based Access Control (RBAC)



Azure RBAC vs Azure Policies



Built-in Roles



Resource Locks



Azure Blueprints



Azure Subscription Management

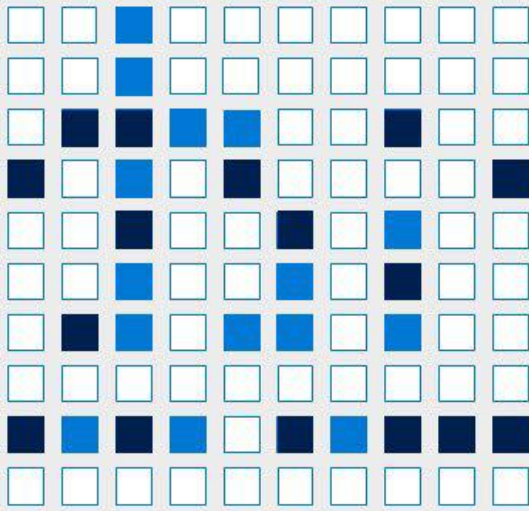
Shared Responsibility Model



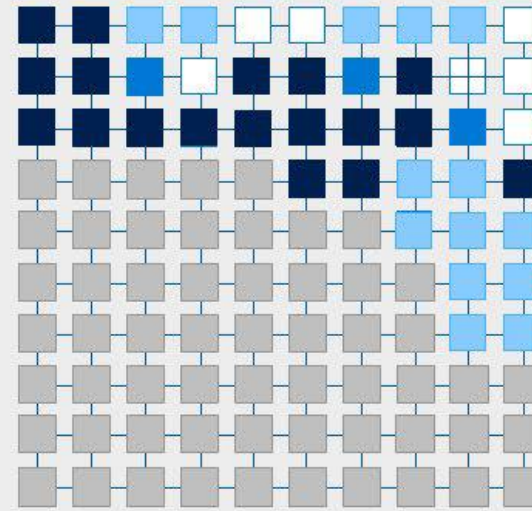
Azure Cloud Security Advantages



TRADITIONAL APPROACH



CLOUD-ENABLED SECURITY



Security is a challenging and under-resourced function

- Satisfied responsibility
- Partially met responsibility
- Unmet responsibility
- Cloud provider responsibility

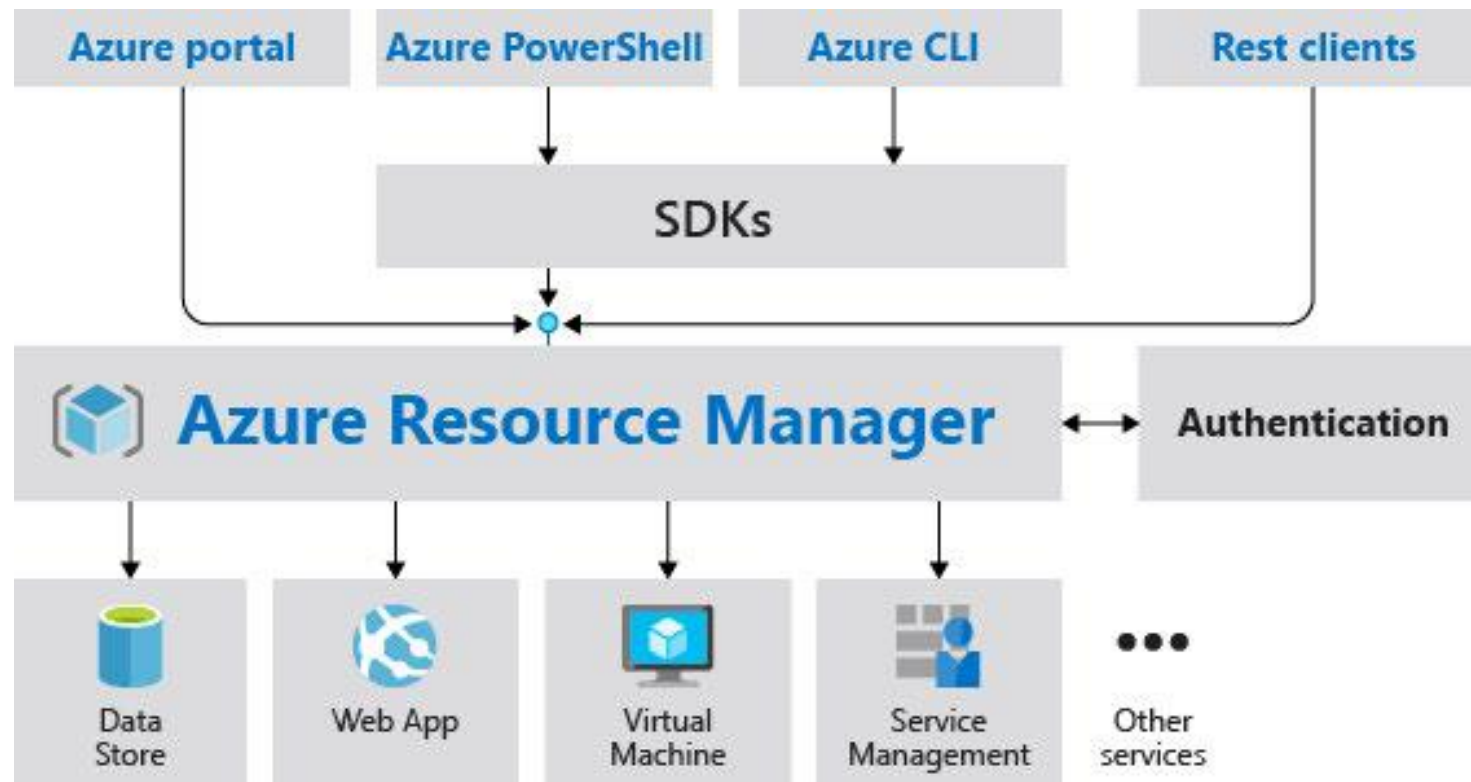
Cloud Technology enables security to:

- Shift commodity responsibilities to provider and re-allocate your resources
- Leverage cloud-based security capabilities for more effectiveness
- Use cloud intelligence to improve detection/response time

Azure Hierarchy



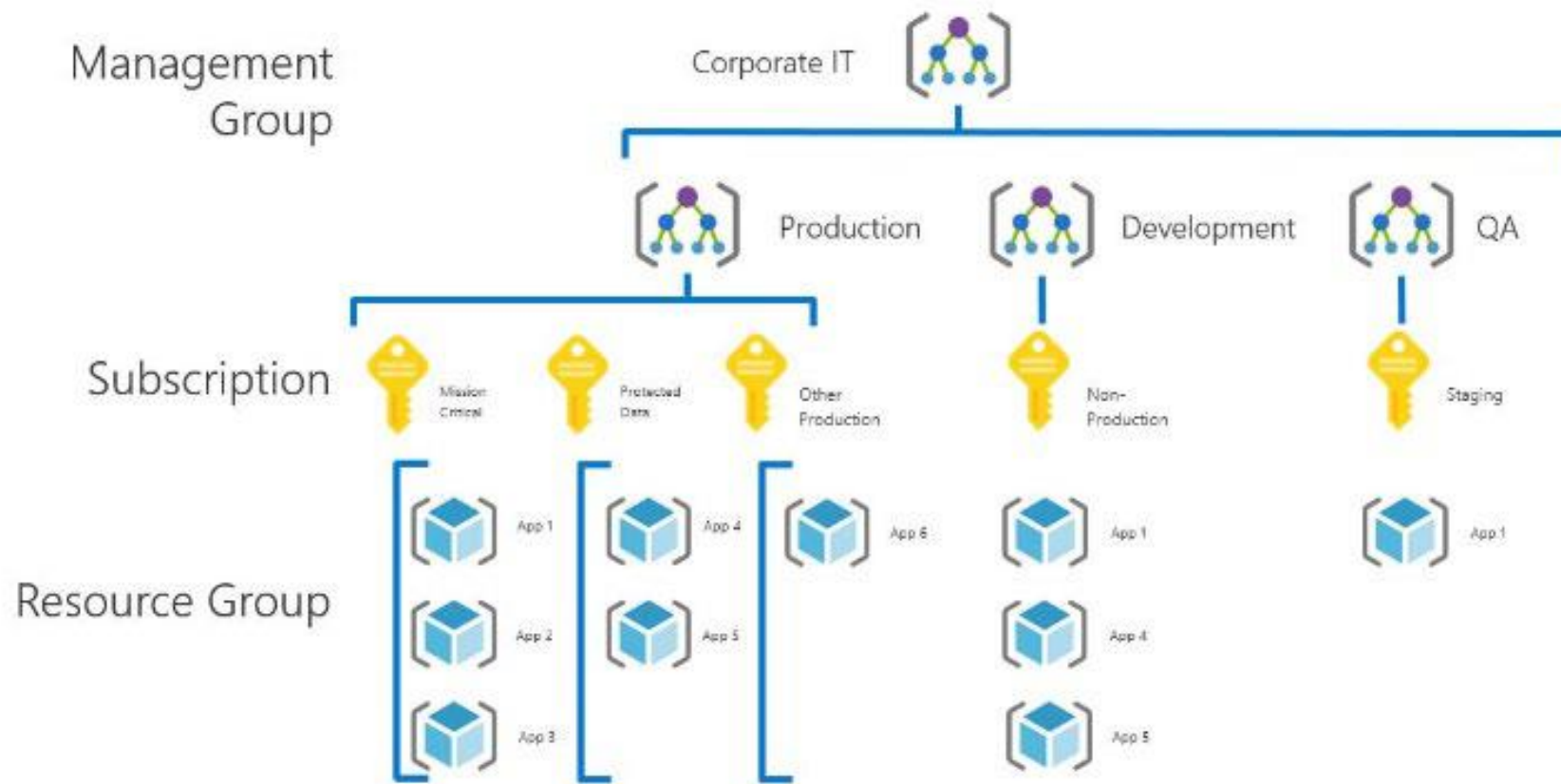
Azure Resource Manager



Azure Hierarchy - continued



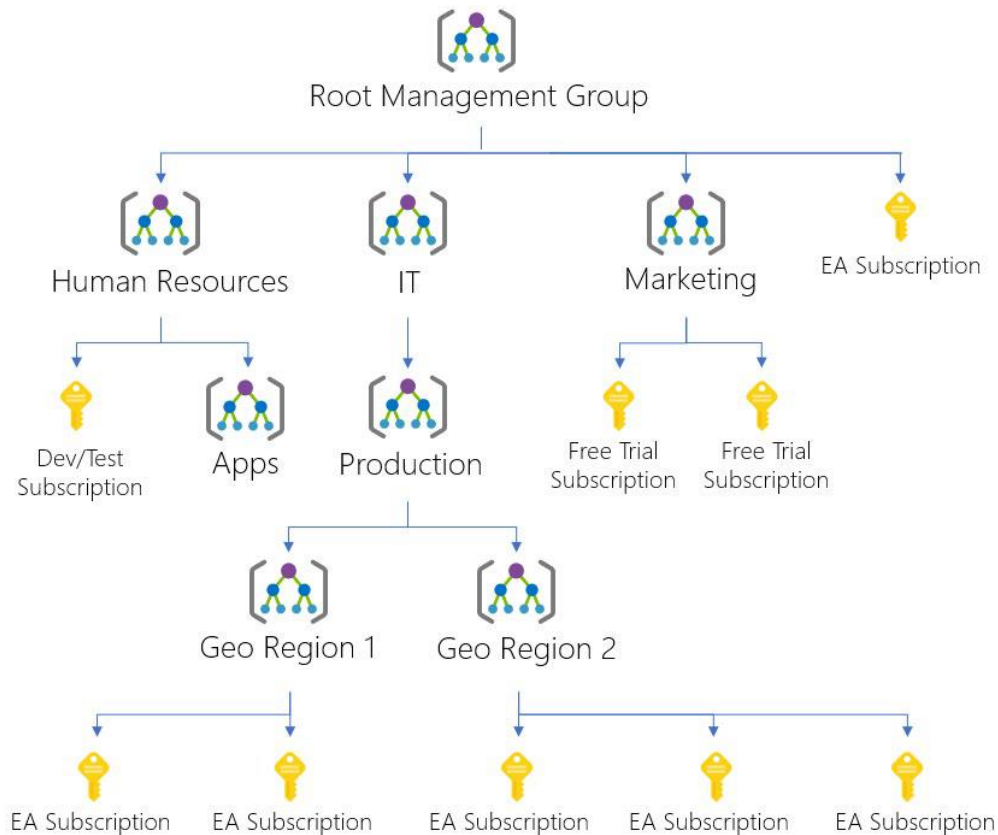
Understand Scope



Azure Hierarchy - continued



Management Groups

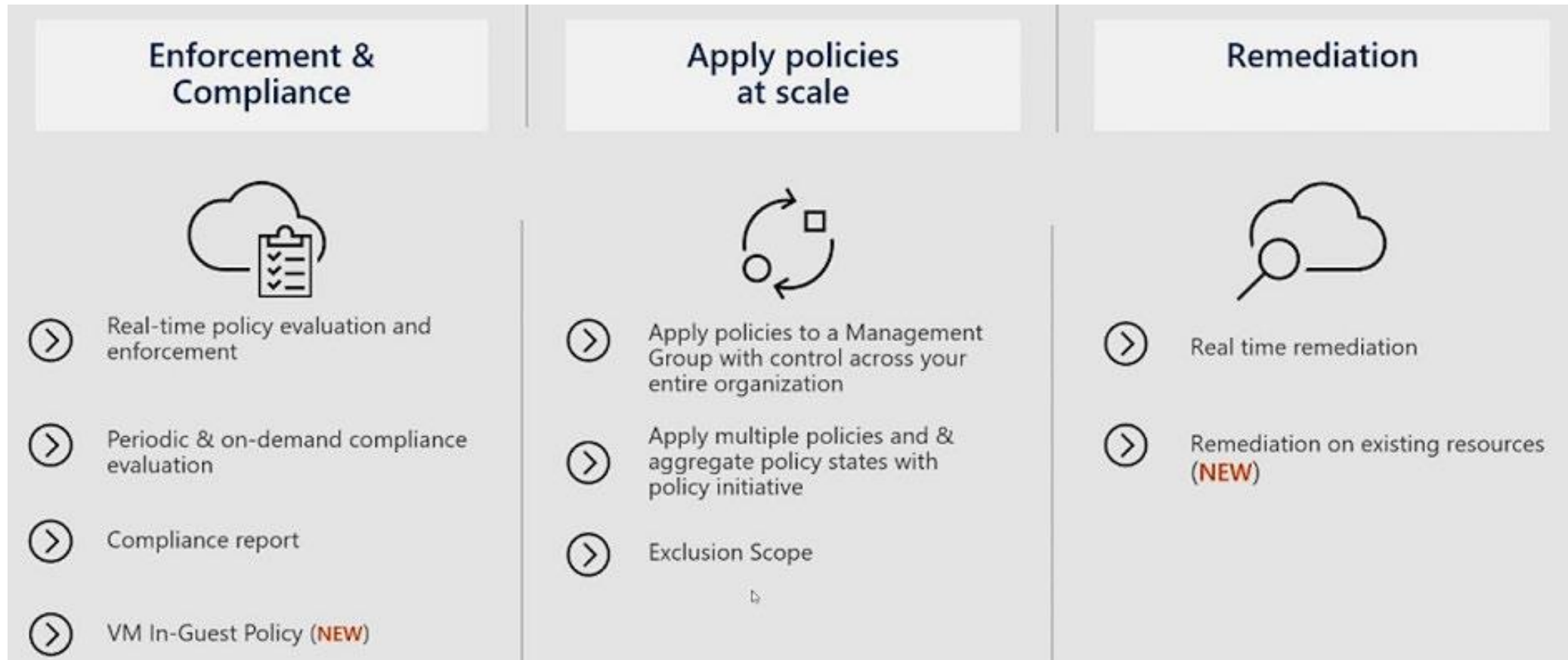


Group your subscriptions

Mirror your organization's structure

Apply policies or access controls

Azure Policies



Composing an Azure Policy



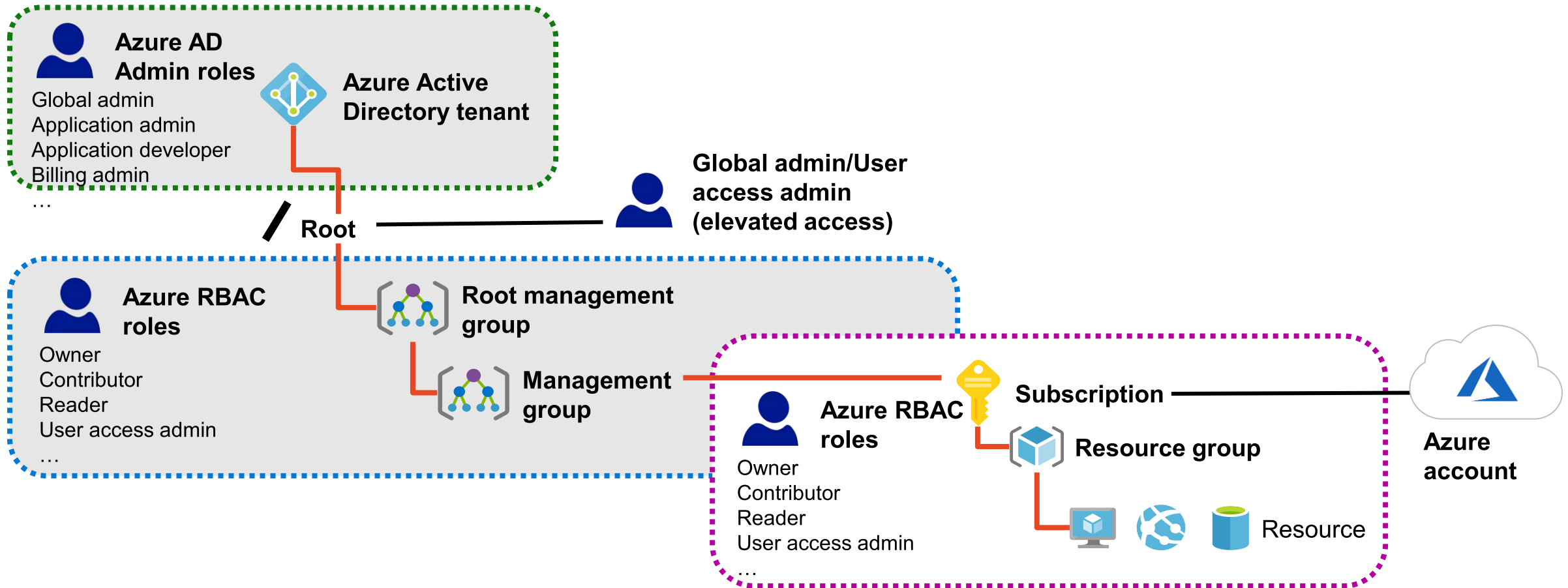
Policy Definition

Policy Assignment

Policy Parameters

Usage Cases
Allowed resource types
Allowed virtual machine SKUs
Allowed locations
Require tag and its value
Azure Backup should be enabled for Virtual Machines

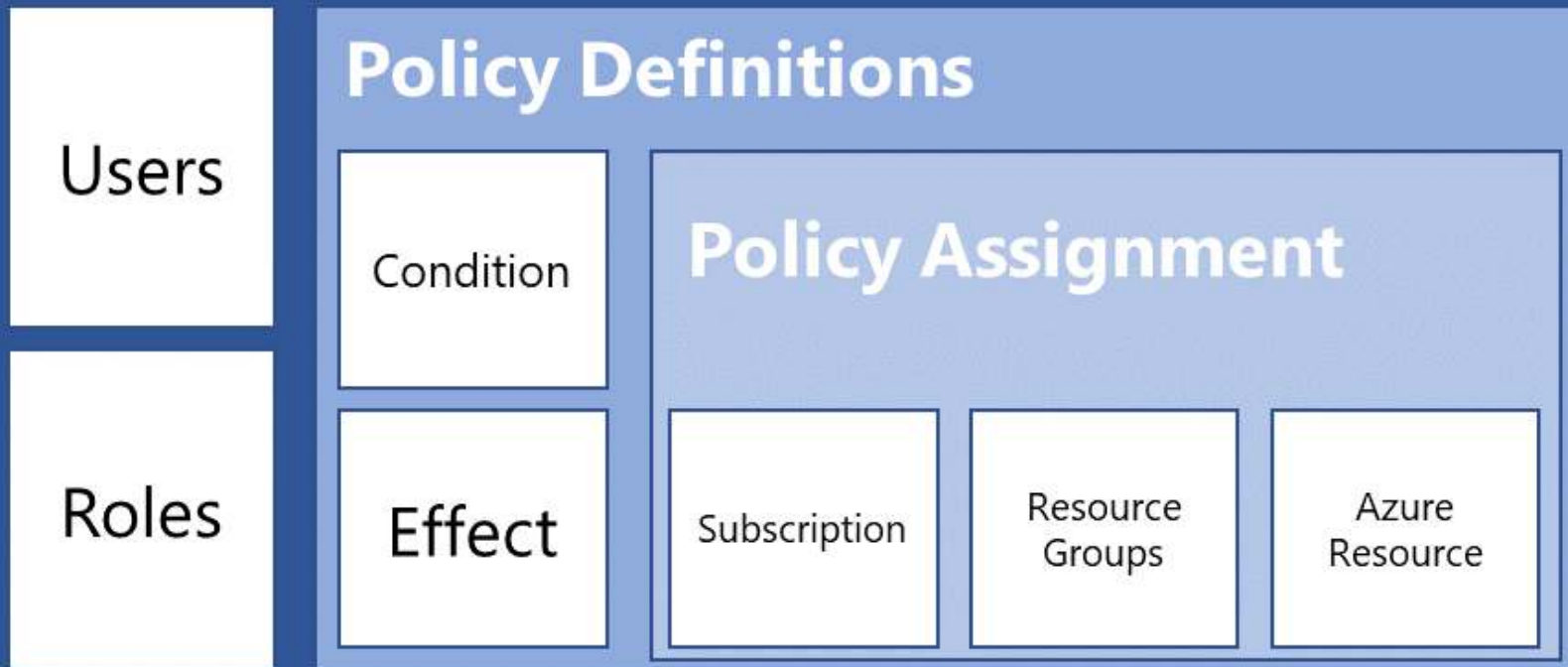
Azure Role-Based Access Control



Azure RBAC vs Azure Policies



Role Based Access Control (RBAC)



Azure Built-in Roles



Built-in Role	Description
Built-in Role	Allows you to manage everything including access to resources
Owner	Allows you to manage everything except managing access to resources
Contributor	Allows you to view everything but not make any changes
Reader	Allows you to manage user access to Azure resources

Resource Locks



CanNotDelete

ReadOnly

Management locks

contososerverexample

+ Add 🔒 Resource group 🔒 Subscription 🔄 Refresh

Add lock

Lock name

DatabaseServerLock ✓

Lock type

Delete ▼

Notes

Prevent deleting the database server

OK

Cancel

Azure Blueprints



Designed to help with environment setup

How is it different from Resource Manager Template?

How its different from Azure Policy?

Azure Subscription Management



[Home](#) > Subscriptions

Subscriptions

Microsoft

[+ Add](#)

Showing subscriptions in Microsoft. Don't see a subscription? [Switch directories](#)

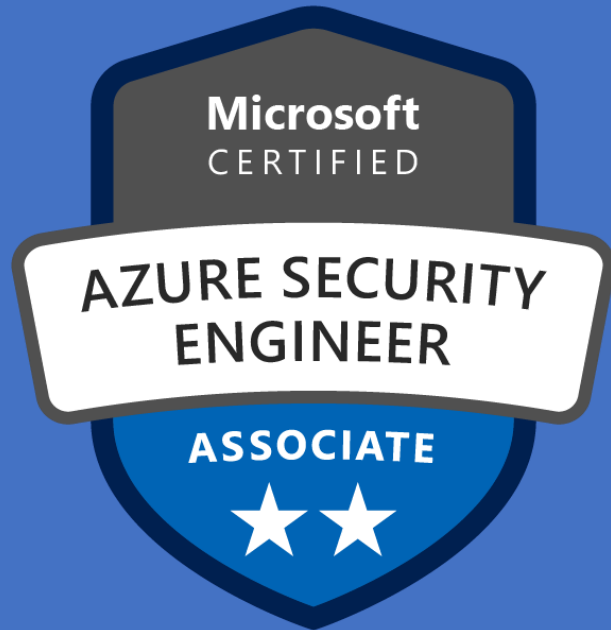
My role ⓘ 0 selected ▼ Status ⓘ 0 selected

[Apply](#)

☒ Show only subscriptions selected in the [global subscriptions filter](#) ⓘ

Manage API access to Azure Subscriptions and Resources

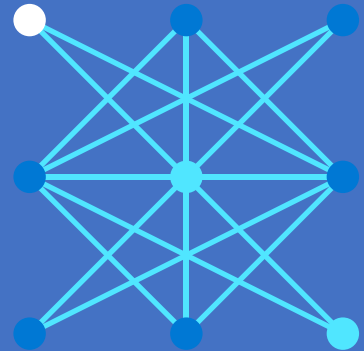
Who can transfer a subscription?



AZ-500

Episode 05

Azure AD Privileged Identity Management





Privileged Identity Management (PIM) Lesson Objectives



Microsoft's Zero Trust Model



MIM Evolution



PIM Features



PIM Scope



PIM Onboarding

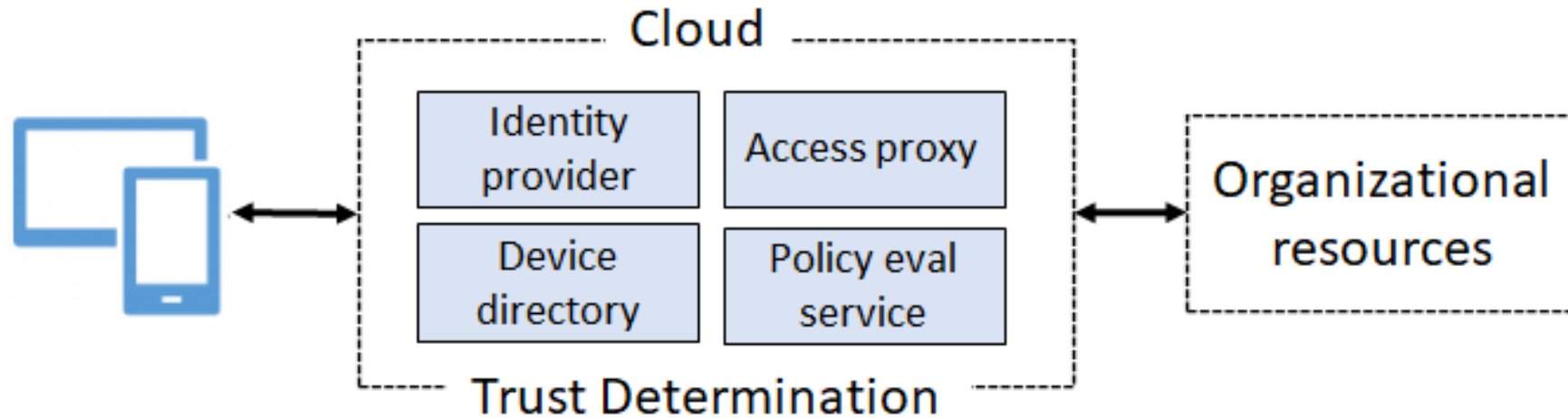


PIM Configuration Settings



PIM Workflow

What does Zero Trust Mean



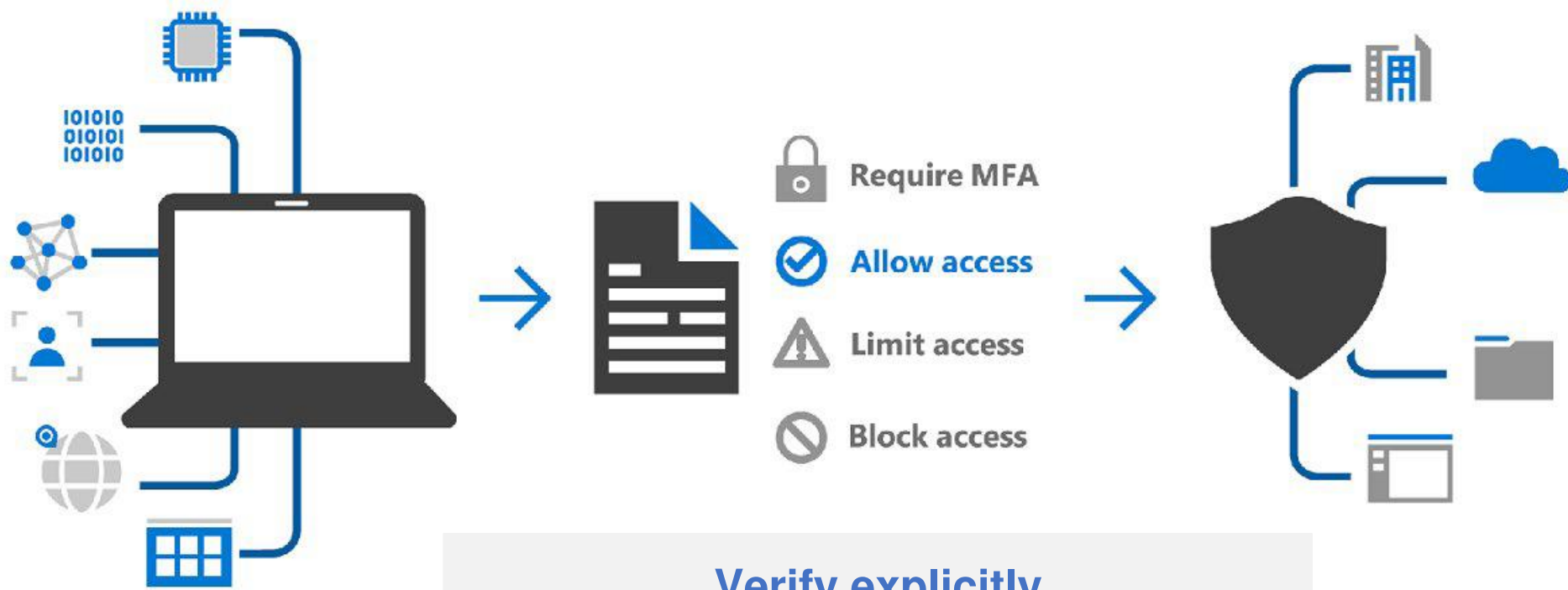
Identity Provider

Device Directory

Policy Evaluation Service

Access proxy

Implementing a Zero Trust Security

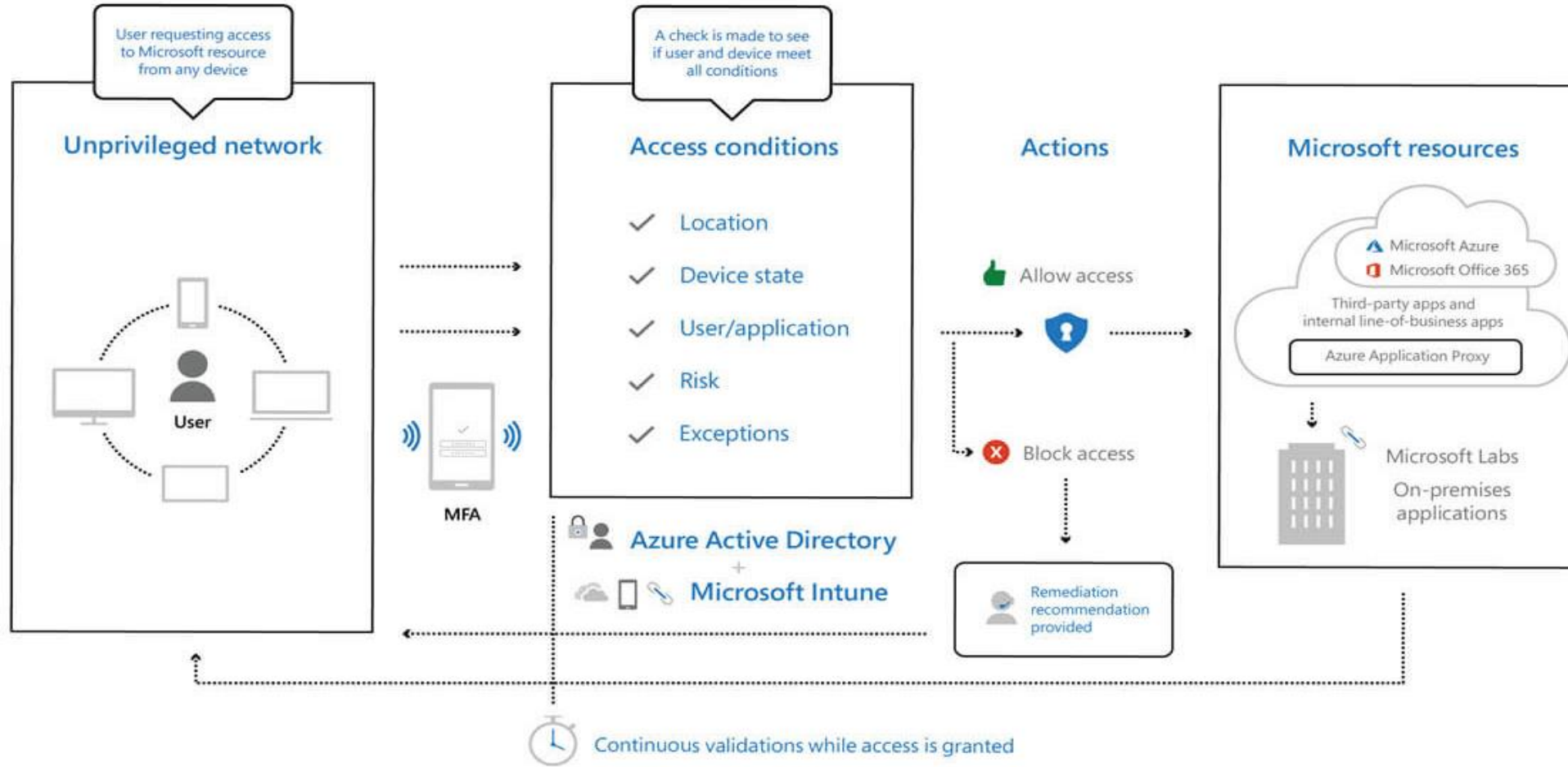


Verify explicitly

Use least Privileged access

Assume breach

Microsoft's Zero Trust Model



Microsoft Identity Management



Credentials + Privileges
=
Digital Identity



Evolution of Identities



Traditional Identity Approaches

Advanced Identity Approaches

Optimal Identity Approaches

Steps for a passwordless world



Enforce MFA

Reduce legacy Authentication Workflows

Remove passwords

Privileged Identity Management



**Just-in-time privileged
access to Azure**

**Time-bound access to
resources**

**Approval to activate
privileged roles**

**Multi-factor authentication to
activate any role**



**Justification to understand
why users activate**

**Notifications when privileged
roles are activated**

**Access reviews to ensure
users still need roles**

**Audit history for internal or
external audit**

PIM Scope



Azure AD roles

Azure resource roles

Privileged Identity Management

Privileged Identity Management

Manage

-  Azure AD roles
-  Azure resources

PIM Onboarding



Azure AD Premium P2, Enterprise Mobility + Security (EMS) E5, or Microsoft 365 M5 license

The Global administrator (first user) who enables PIM gets write access

The first user can assign others to the Privileged Role Administrator

Global administrators (not first user), Security administrators, and Security readers have read-only access

Ensure there are always at least two Privileged Role Administrators

The screenshot shows the 'Add managed members' dialog box. The left pane has two sections: 'Select a role' with 'Privileged Role Administrator' selected, and 'Select members' with 'No members were selected'. The right pane has an 'Invite' button, a list of members (Admin and Admin 2), and a 'Select' button.

Add managed members		Select members	
* Select a role Privileged Role Administrator		+ Invite	
* Select members No members were selected		☒	RA Admin admin@
			RA Admin 2 admin2@
		Selected Admin	
		Select	

PIM Configuration Settings



Activation

Activation maximum duration (hours)

On activation, require ☒ Azure MFA ☐ None

☒ Require justification on activation

☐ Require ticket information on activation

☐ Require approval to activate

Select approver(s) >

No approver selected

Assignment

☒ Allow permanent eligible assignment

Expire eligible assignments after

1 Year

☒ Allow permanent active assignment

Expire active assignments after

6 Months

☐ Require Azure Multi-Factor Authentication

☒ Require justification on active assignment

Notifications

Send notifications when members are assigned as eligible to this role:

Role assignment alert	☒ Admin
Notification to the assigned user (assignee)	☒ Assignee
Request to approve a role assignment renewal/...	☒ Approver

Send notifications when members are assigned as active to this role:

Role assignment alert	☒ Admin
Notification to the assigned user (assignee)	☒ Assignee
Request to approve a role assignment renewal/...	☒ Approver

Send notifications when eligible members activate this role:

Role activation alert	☒ Admin
Notification to activated user (requestor)	☒ Requestor
Request to approve an activation	☒ Approver

PIM workflow

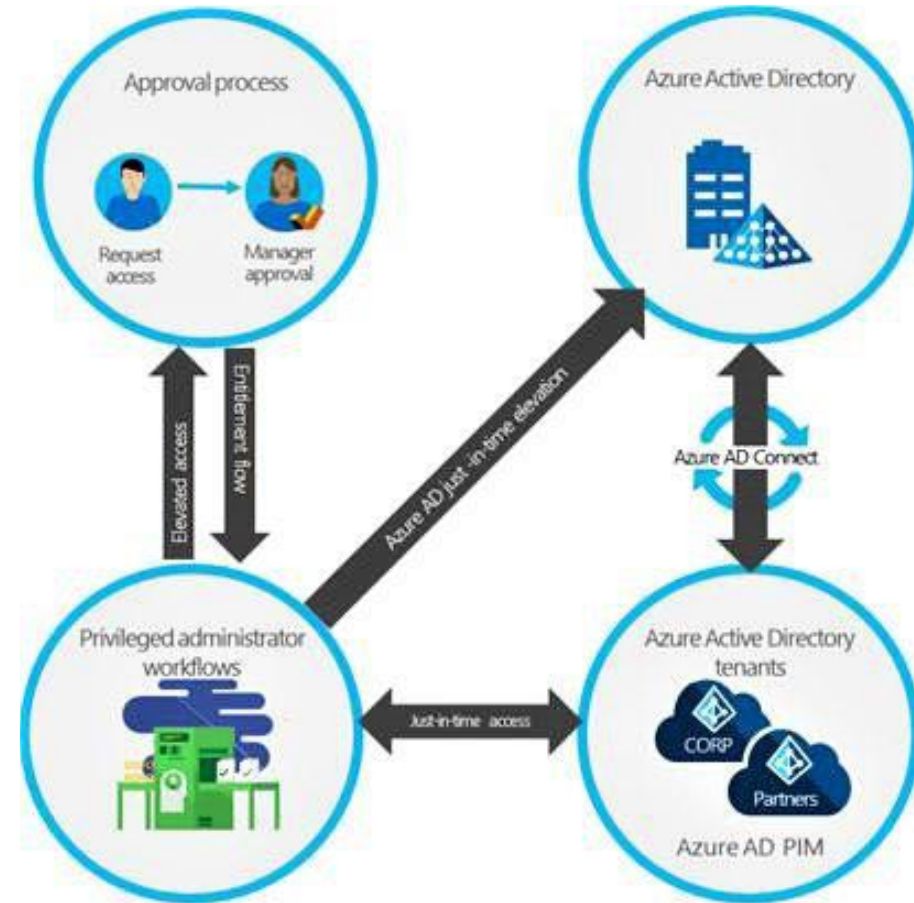


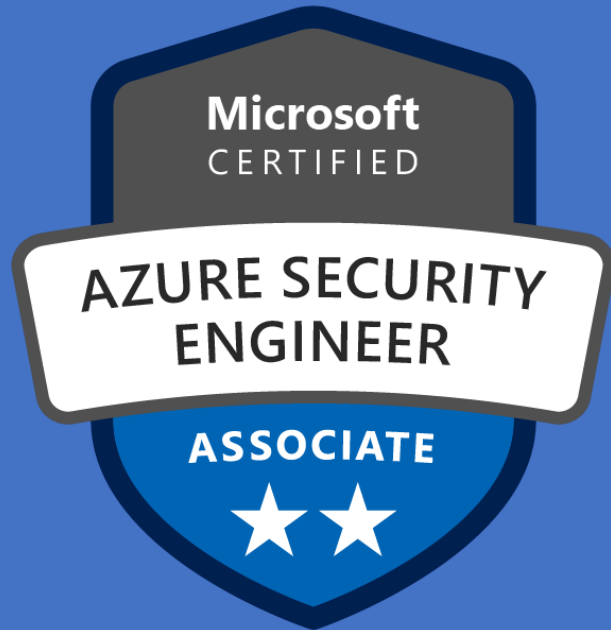
Elevated workflow

JIT administrator access

Role Activation in Azure AD

Tracking the use of PIM

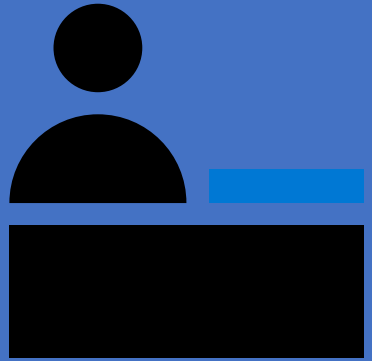




AZ-500

Episode 06

Hybrid Identity





Hybrid Identity Lesson Objectives



Azure AD Connect



Authentication Options



Password Hash Synchronization



Pass-through Authentication (PTA)



Federation with Azure AD

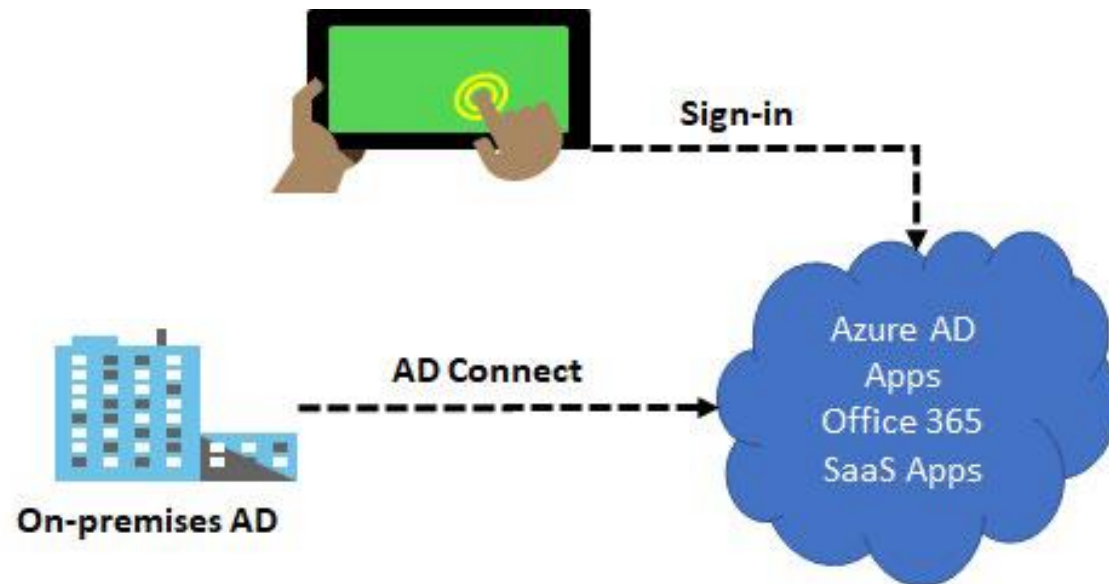


Password Writeback



Authentication Decision Tree

Azure AD Connect



Password hash synchronization

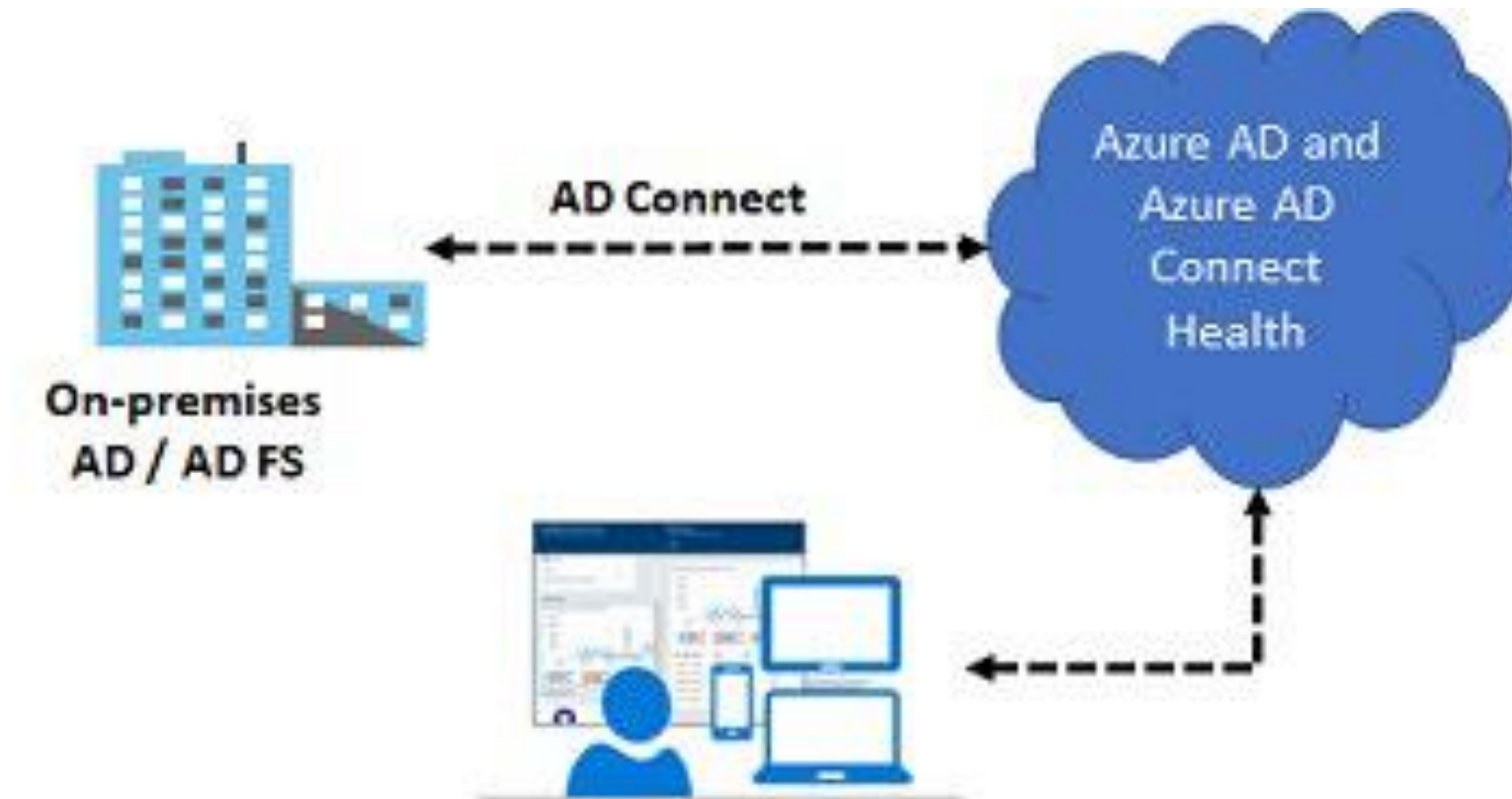
Pass-through authentication

Federation integration

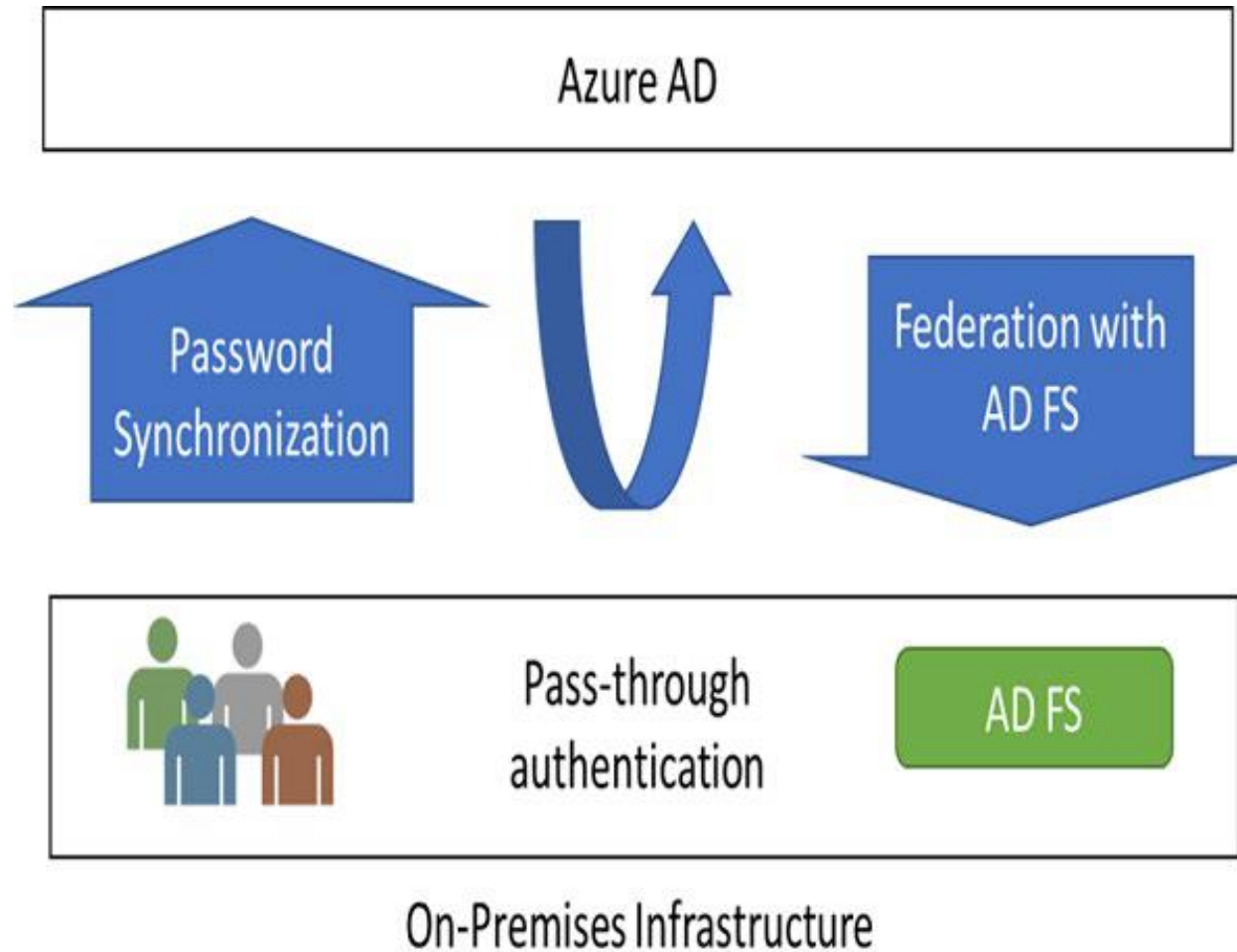
Synchronization

Health Monitoring

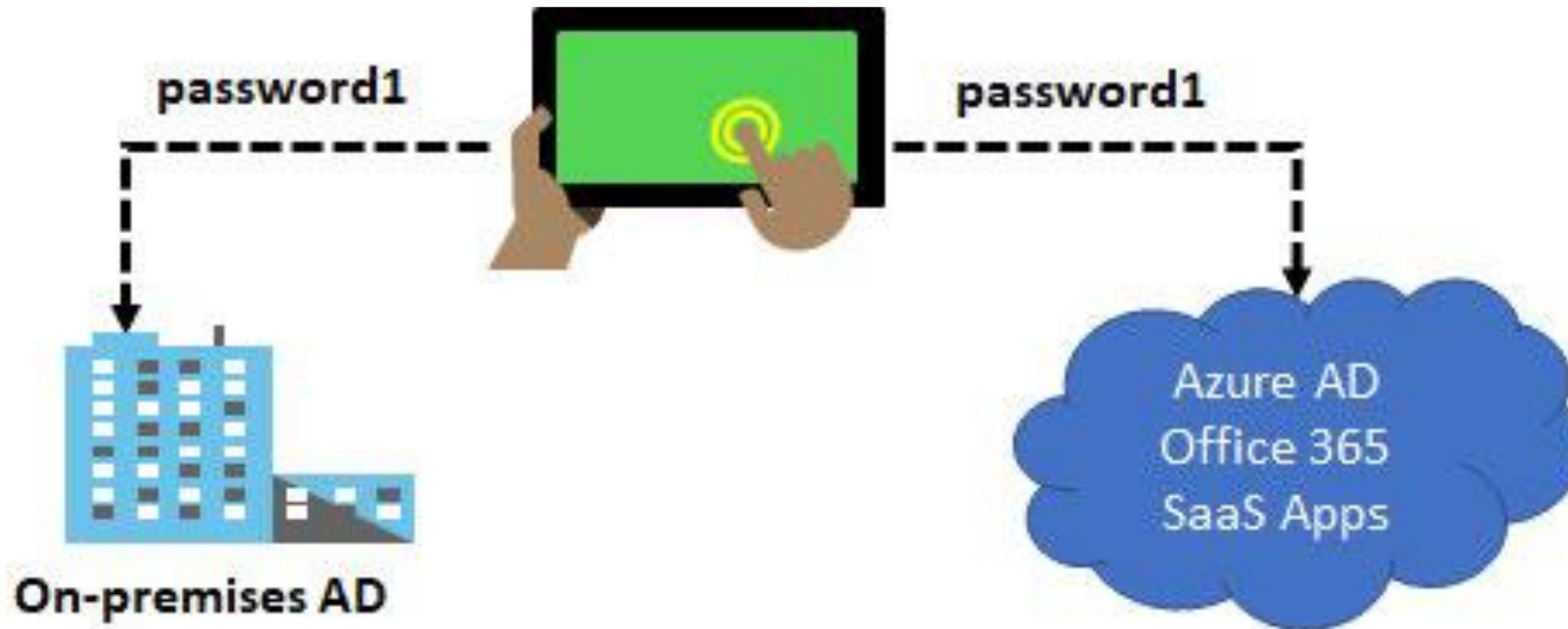
Azure AD Connect Health



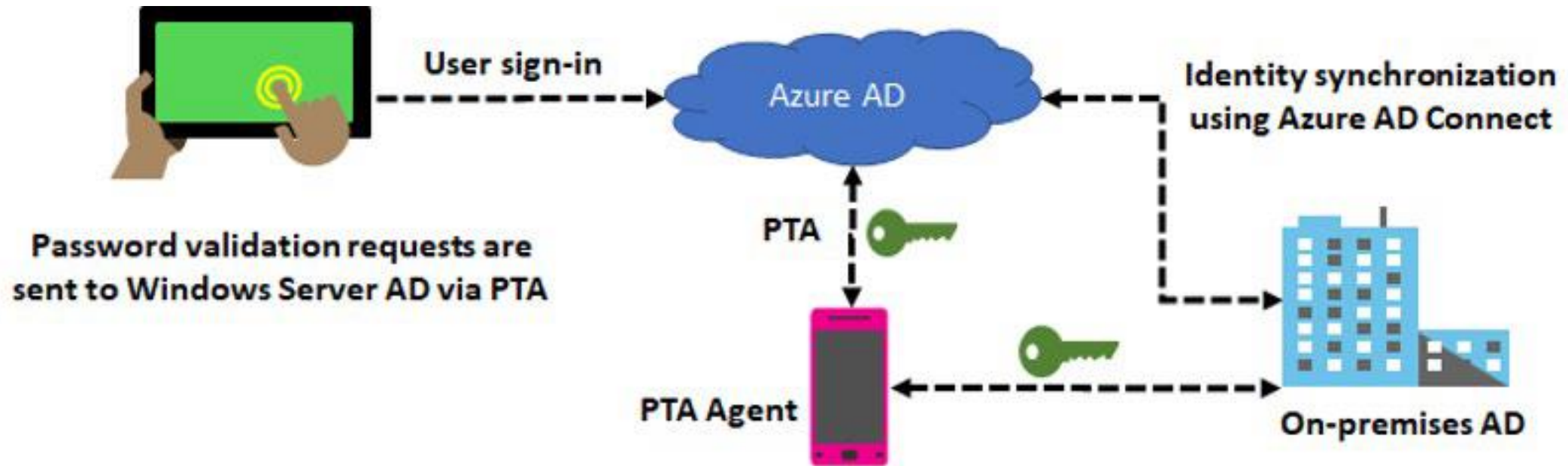
Authentication Options



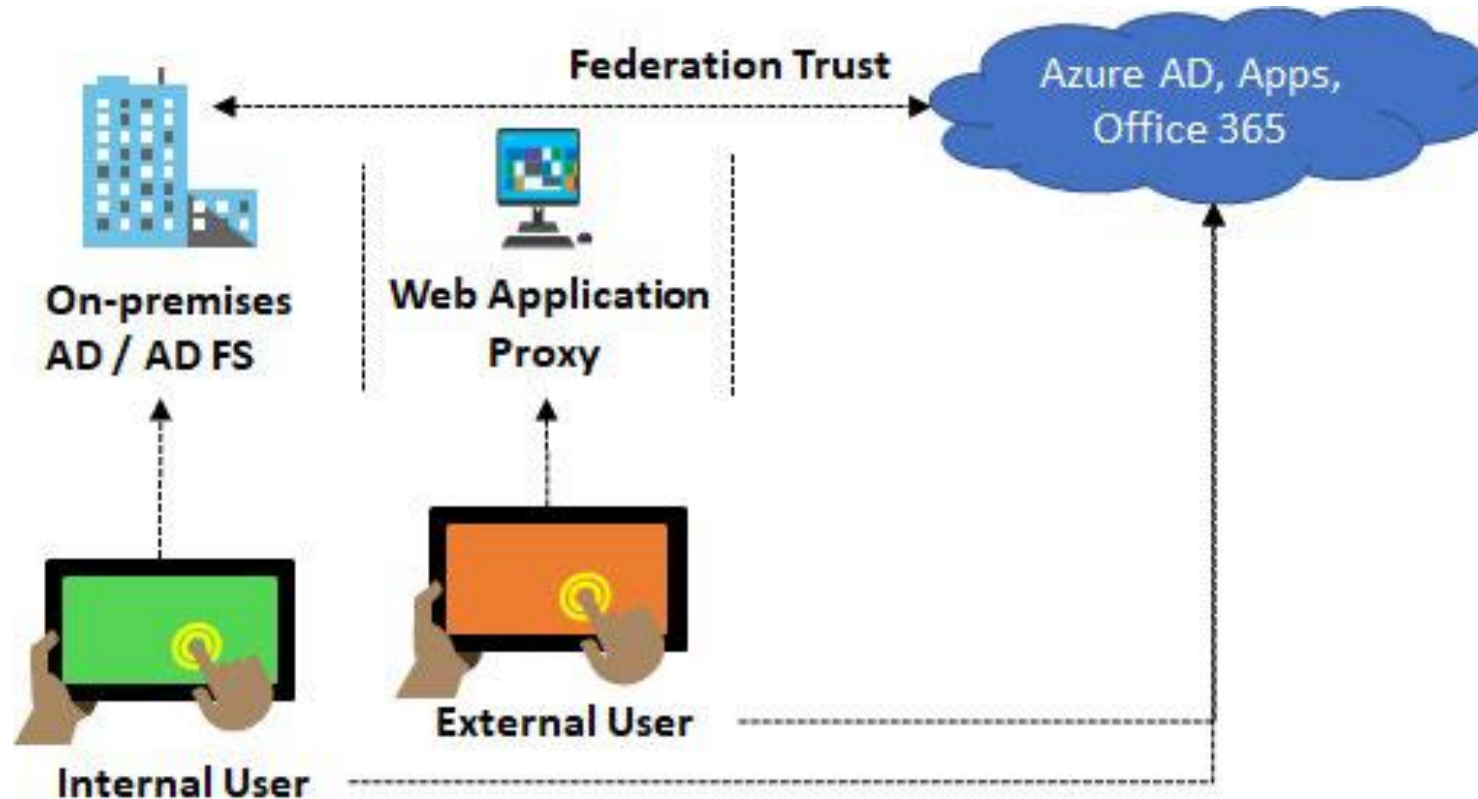
Password Hash Synchronization (PHS)



Pass-through Authentication (PTA)



Federation with Azure AD



Password Writeback



Microsoft Azure Active Directory Connect

Optional features

Select enhanced functionality if required by your organization.

- ☐ Exchange hybrid deployment ?
- ☐ Azure AD app and attribute filtering ?
- ☒ Password synchronization ?
- ☒ Password writeback ?
- ☐ Group writeback (Preview) ?
- ☐ Device writeback ?
- ☐ Directory extension attribute sync ?

Enforcement of on-premises Active Directory Password policies

Zero-delay feedback

Supports password changes from the access panel and Office 365

Supports password writeback when an admin resets them from the Azure portal

Doesn't require any inbound firewall rules

Azure AD External Identities

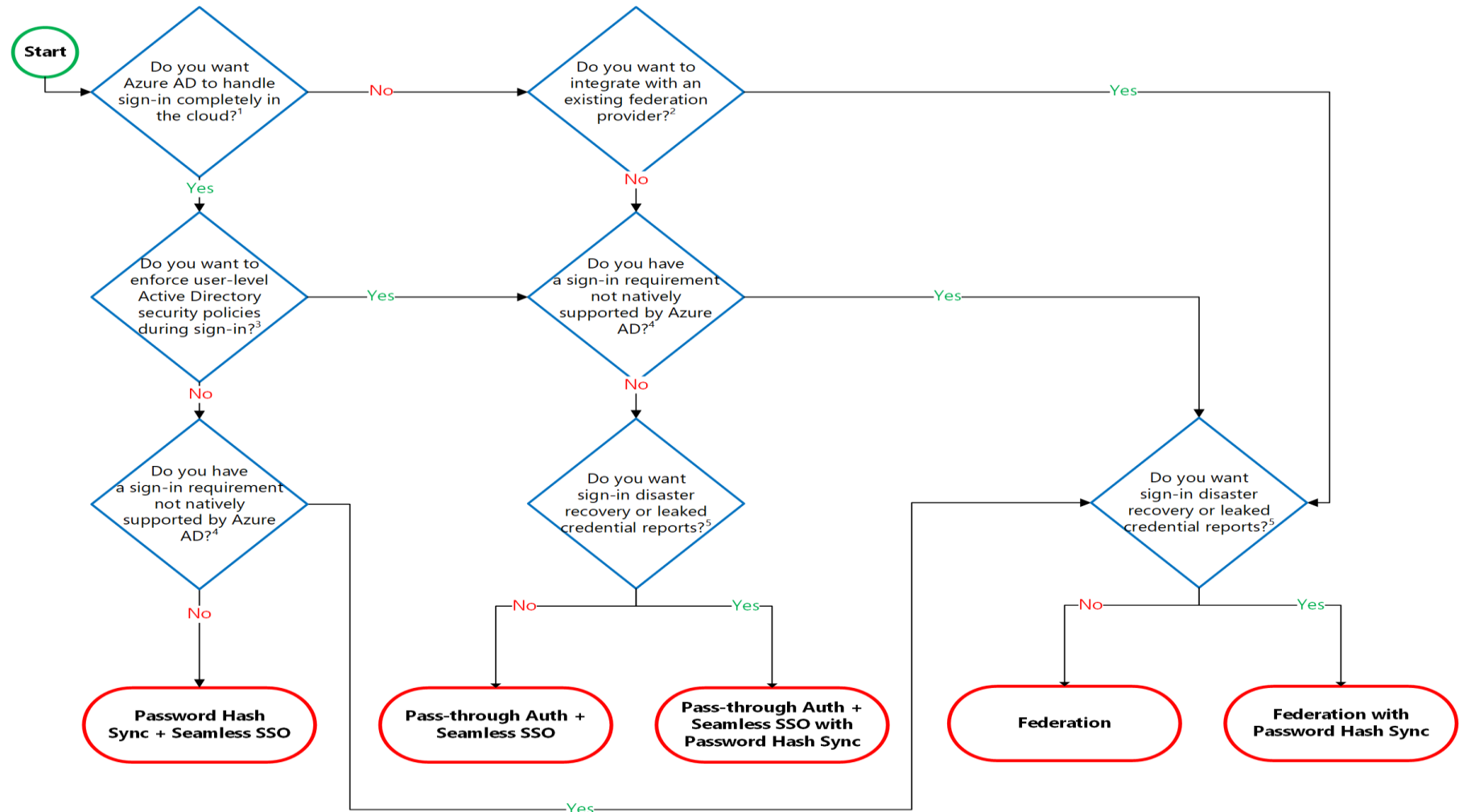


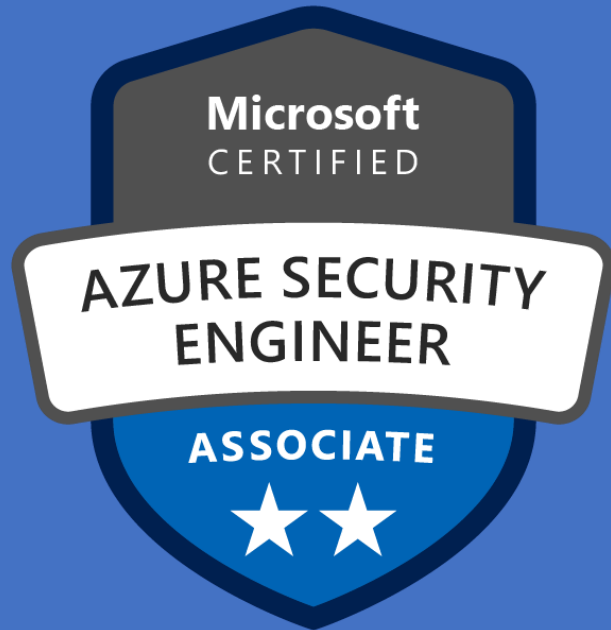
Azure AD

Azure AD B2B

Azure AD B2C

Decision Tree





AZ-500

Episode 07

Module 01 Knowledge Check



Review Question 1



Your organization is considering Azure Multi-Factor Authentication. Your manager asks about secondary verification methods. Which of the following options is not valid? Select one.

- ☐ Automated phone call
- ☒ Emailed link to verification website
- ☐ Microsoft Authenticator app with OATH verification code
- ☐ Push notification to the phone
- ☐ Text message with authentication code

Review Question 2



Your organization has implemented Azure Multi-Factor Authentication. You need to provide a status report by user account. Which of the following is not a valid MFA status? Select one.

☐ Disabled

☐ Enabled

☐ Enforced

☒ Required

Review Question 3



You are configuring Azure Multi-Factor Authentication. You can configure all the following options, except? Select one.

- ☐ Block a user if fraud is suspected.
- ☒ Configure IP addresses outside the company intranet that should be blocked.
- ☐ One time bypass for a user that is locked out.
- ☐ User self-reporting for fraud attempts on their account.

Review Question 4



You are assigning Azure AD roles. Which role will allow the user to manage all the groups in a tenant, and would be able to assign other admin roles? Select one.

- ☒ Global administrator
- ☐ Password administrator
- ☐ Security administrator
- ☐ User administrator

Review Question 5



You are creating an Azure AD security group. All the following are ways you can assign group membership, except? Select one.

- ☐ Assigned
- ☐ Dynamic device
- ☐ Dynamic user
- ☒ Office 365 user

Review Question 6



Your Compliance auditors wants to ensure as employees change jobs or leave the company that their privileges are also changed or revoked. They are especially concerned about the Administrator group. To address their concerns. you implement which of the following? Select one.

- ☒ Access reviews
- ☐ Azure time-based policies
- ☐ IT virtual machine access
- ☐ Management groups

Review Question 7



Identity Protection has reported that a user's credentials have been leaked. According to policy, the user's password must be reset. Which Azure AD role can reset the password? Select one.

- ☒ Global Administrator
- ☐ Security Administrator
- ☐ Security Operator
- ☐ Security Reader

Review Question 8



Identity Protection identifies risks in the following classifications, except? Select one.

- ☐ Anonymous IP address
- ☐ Atypical travel
- ☐ Unfamiliar sign-in properties
- ☒ Unregistered device

Review Question 9



You have implemented Identity Protection and are reviewing the Risky users report. For each reported event you can choose any of the following actions, except? Select one.

- ☐ Block user from signing in
- ☐ Confirm user compromise
- ☒ Delete the risk event
- ☐ Dismiss user risk

Review Question 10



Conditional access policies can help with all the following, except? Select one.

- ☐ Block or grant access from specific locations
- ☒ Designate privileged user accounts.
- ☐ Require multi-factor authentication.
- ☐ Require trusted locations.

Review Question 11



Which licensing plan supports Identity Protection?

- ☐ Azure Active Directory Free
- ☐ Azure Active Directory Premium P1
- ☒ Azure Active Directory Premium P2

Review Question 12



You hire a new administrator and you create a new Azure AD user account for them. The new hire must be able to:

- **Read/write resource deployments they are responsible for.**
- **Read Azure AD access permissions**

They should not be able to view Azure subscription information. What should you do? Select one.

- ☒ **Assign the user the Contributor role at the resource group level.**
- ☐ Assign the user the Owner role at the resource level.
- ☐ Assign the user the Global Administrator role.
- ☐ Assign the user the Virtual Machine contributor role at the subscription level.

Review Question 13



Which of the following would be good example of when to use a resource lock? Select one.

- ☒ An ExpressRoute circuit with connectivity back to your on-premises network.
- ☐ A virtual machine used to test occasional application builds.
- ☐ A storage account used to store images processed in a development environment.
- ☐ A resource group for a new branch office that is just starting up.

Review Question 14



You have three virtual machines (VM1, VM2, and VM3) in a resource group. The Helpdesk hires a new employee. The new employee must be able to modify the settings on VM3, but not on VM1 and VM2. Your solution must minimize administrative overhead. What should you do? Select one.

- ☐ Assign the user to the Contributor role on the resource group.
- ☒ Assign the user to the Contributor role on VM3.
- ☐ Move VM3 to a new resource group and assign the user to the Contributor role on VM3.
- ☐ Assign the user to the Contributor role on the resource group, then assign the user to the Owner role on VM3.

Review Question 15



You need to target policies and review spend budgets across several subscriptions you manage. What should you create for the subscriptions? Select one.

- ☐ A billing group
- ☒ A management group
- ☐ A nested resource group
- ☐ A policy initiative

Review Question 16



Your manager asks you to explain how Azure uses resource groups. You can provide all of the following information, except? Select one.

- ☐ **Resources can be in only one resource group.**
- ☐ **Resources can be moved from one resource group to another resource group.**
- ☒ **Resource groups can be nested.**
- ☐ **Role-based access control can be applied to the resource group.**

Review Question 17



You wish to enable Azure AD PIM for your directory. What Azure AD Role do you need to enable PIM?
Select one.

- ☐ PIM Administrator
- ☐ Office 365 Admin
- ☐ Co-Administrator
- ☒ Global Admin

Review Question 18



You company has implemented Azure AD PIM. You need to ensure a new hires request elevation before they make any changes in Azure. What should you do? Select one.

- ☐ Activate the new hire.
- ☒ Assign the new hire the Eligible role membership type.
- ☐ Include the new hire in a an access review.
- ☐ Require the new hire to use MFA.

Review Question 19



Azure AD PIM is used to manage which two of the following?
Select two.

- ☐ Azure privileged users
- ☐ Azure resource groups
- ☒ Azure AD roles
- ☒ Azure resource roles

Review Question 20



Your organization has enabled Azure AD PIM. The senior IT manager does not want to perform any action to use a role. What should you do? Select one.

- ☐ Give the manager JIT access to the role.
- ☒ Make the manager Permanent Active in the role.
- ☐ Make the manager Assigned to a role.
- ☐ Make the manager Permanent Eligible in the role.

Review Question 21



Your IT helpdesk wants to reduce password reset support tickets. You suggest having users sign-in to both on-premises and cloud-based applications using the same password. Your organization does not plan on using Azure AD Identity Protection, so which feature would be easiest to implement given the requirements?

- ☐ Federation
- ☒ Pass-through authentication
- ☐ Password hash synchronization
- ☐ Password writeback

Review Question 22



Which tool can you use to synchronize Active AD passwords with on-premises Active Directory?

- ☒ Azure AD Connect
- ☐ Azure AD Health
- ☐ Active Directory Federation Services
- ☐ Password writeback

Review Question 23



Azure AD does not use which of the following security protocols? Select one.

☒ Kerberos

☐ OAuth

☐ OpenID

☐ SAML

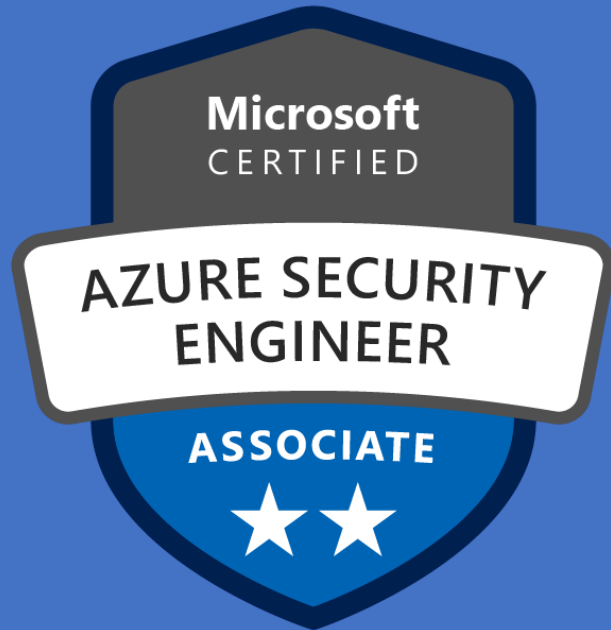
☐ WS-Federation

Review Question 24



Which of the following is not a passwordless authentication option that integrates with Azure Active Directory? Select one.

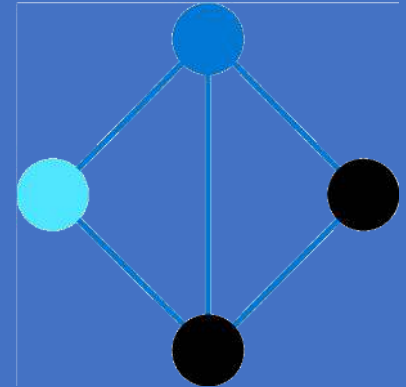
- ☐ FIDO2 security keys
- ☐ Microsoft Authenticator app
- ☒ Multi-Factor Authentication
- ☐ Windows Hello for Business



AZ-500

Episode 08

Perimeter Security





Hybrid Identity Lesson Objectives



Defense in Depth



Virtual Network Security



Distributed Denial of Service (DDoS)



DDoS Implementation



Azure Firewall Features



Azure Firewall Implementation

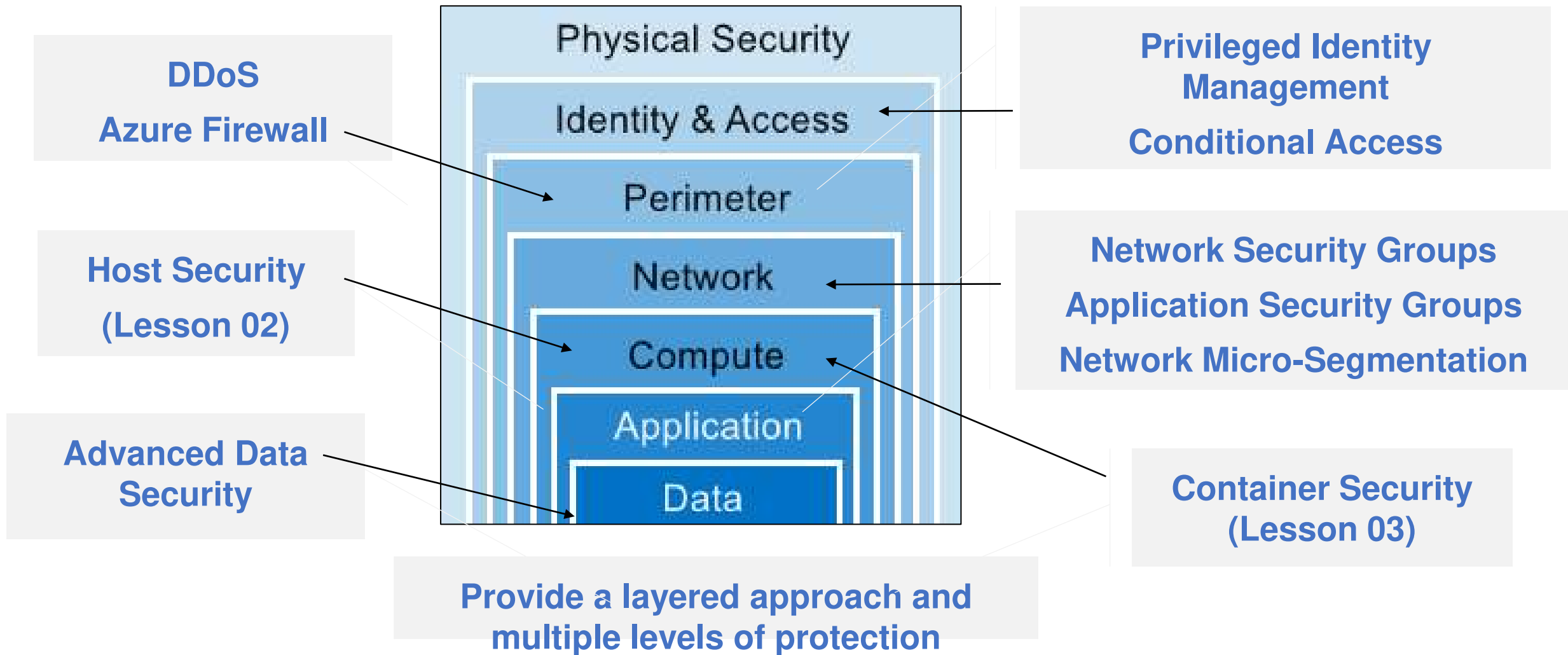


VPN Forced Tunneling



UDRs and NVAs

Defense in Depth



Network Micro-Segmentation



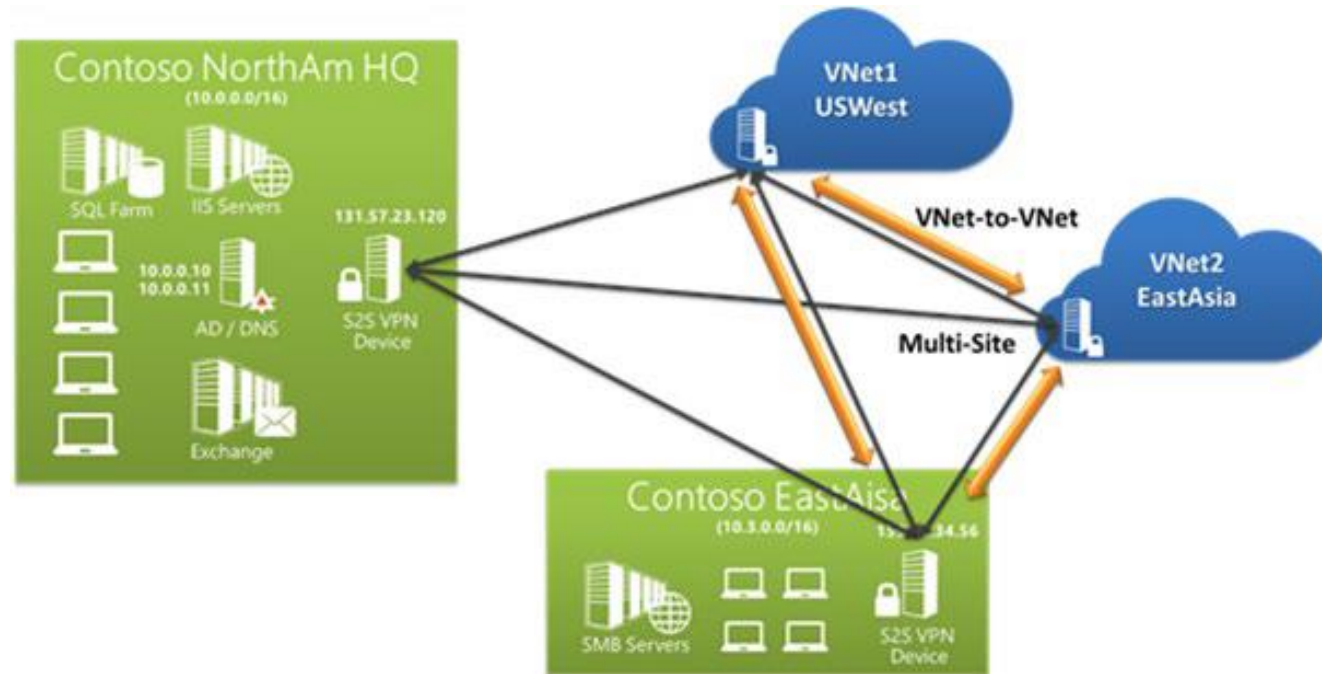
Azure Network Security Groups

Application Security Groups

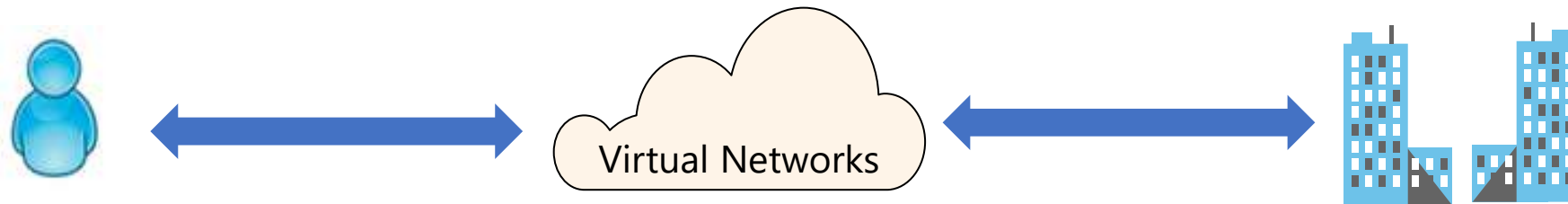
Azure Web Application Firewall & Azure Firewall

Local Admin Password Solution (LAPS)

Virtual Network Security



Virtual Networks



IT addresses



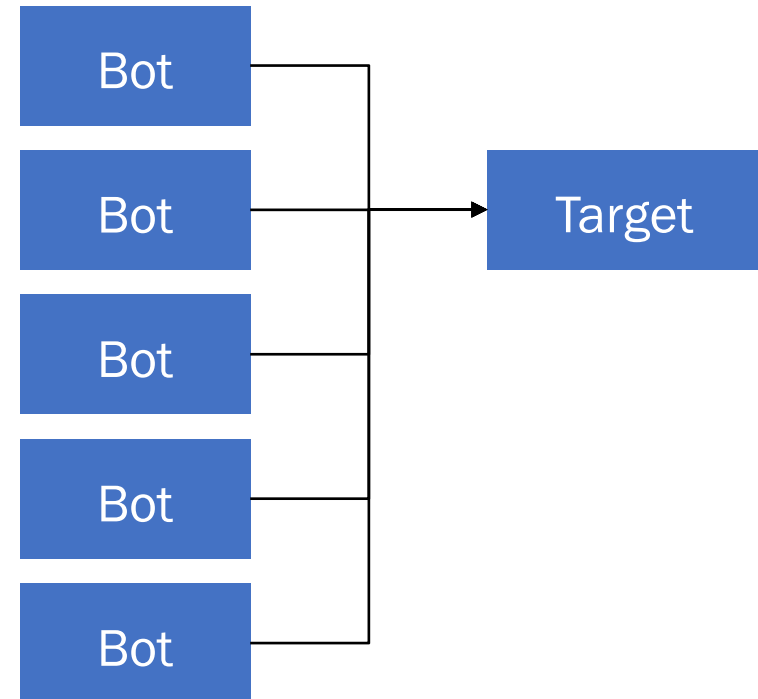
Private

Public

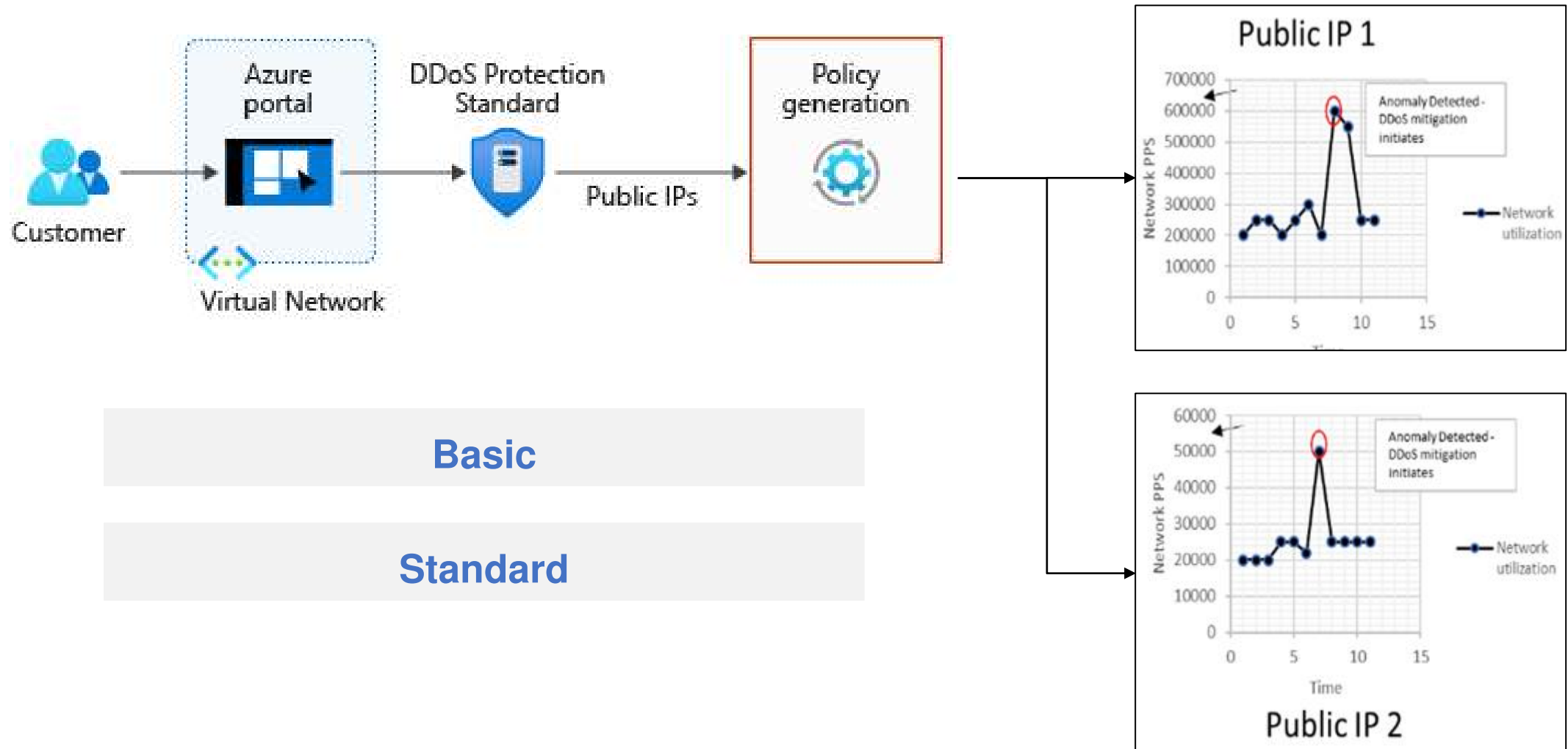
Distributed Denial of Service (DDoS)



DDoS is a collection of attack types aimed at disrupting the availability of a target



DDoS Implementation



Types of DDoS attacks

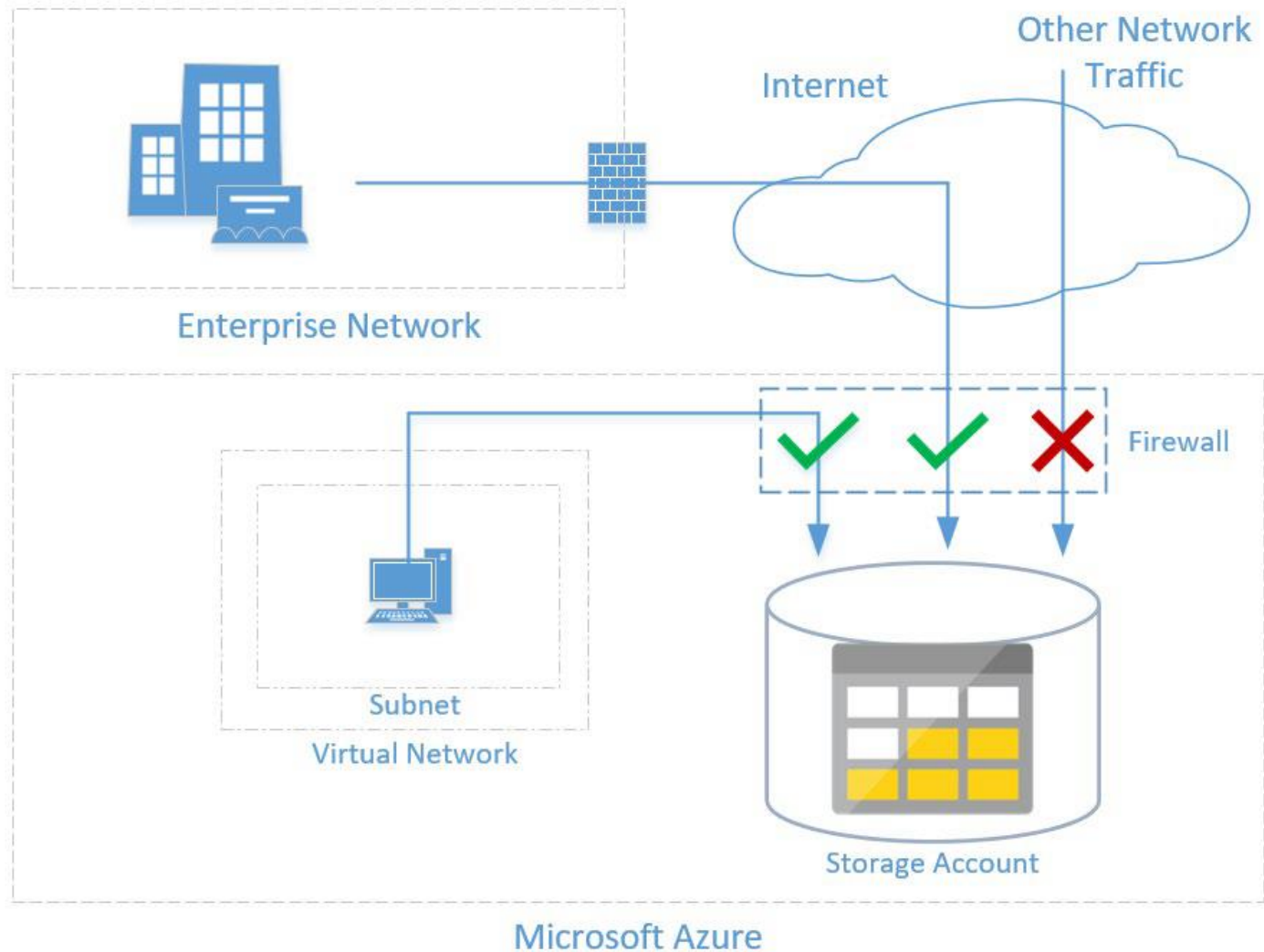


Volumetric Attacks

Protocol attacks

Resource (application) layer attacks

Azure Firewall



Built-in high availability

Unrestricted cloud scalability

Application FQDN filtering rules

Network traffic filtering rules

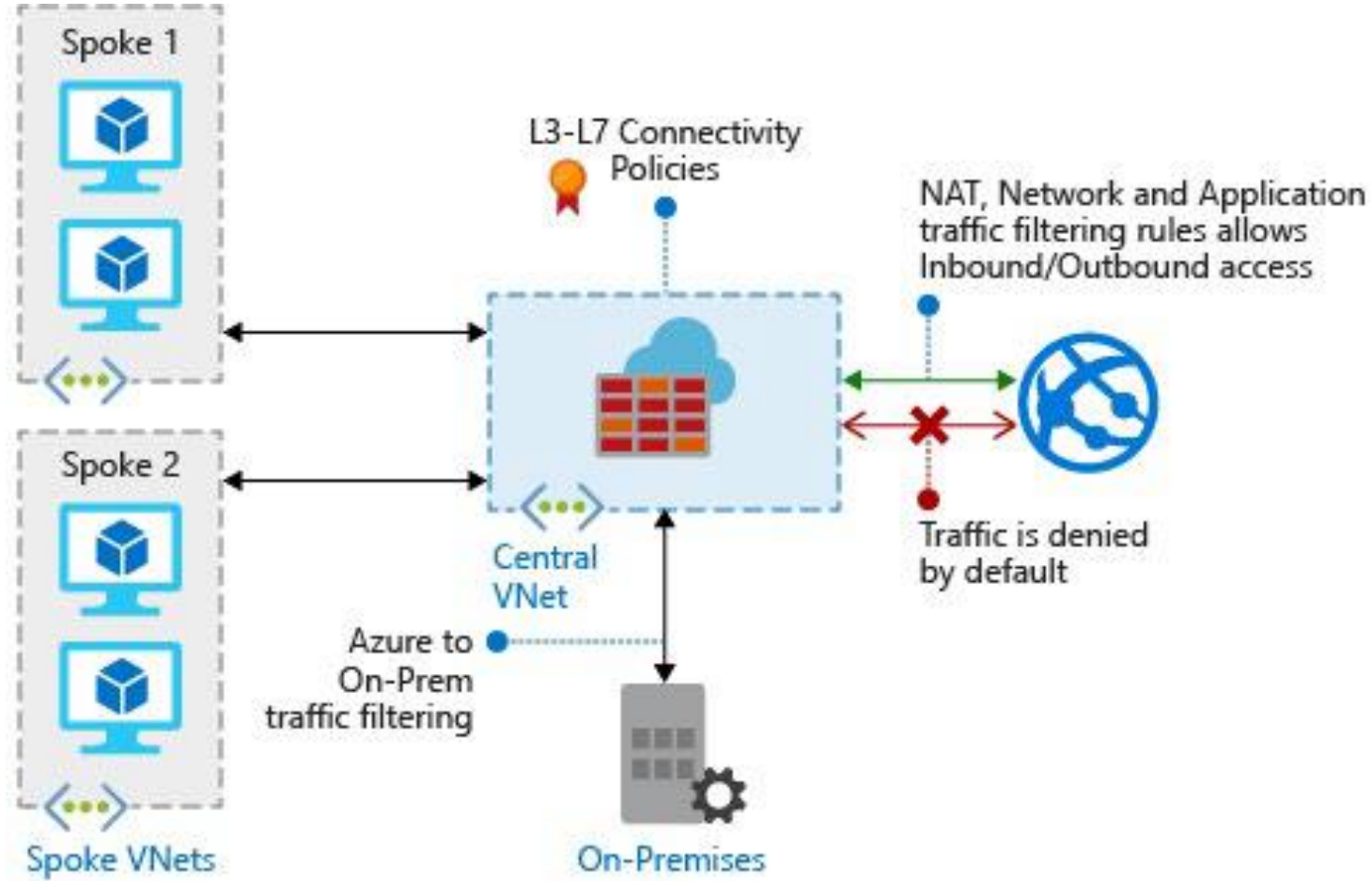
FQDN tags

OSNAT

DNAT

Azure Monitor logging

Azure Firewall Implementation



Azure Firewall Concepts



FQDN tags

Infrastructure FQDNs

Logs and Metrics

Threat intelligence-based filtering

Rule processing logic

Service Tags

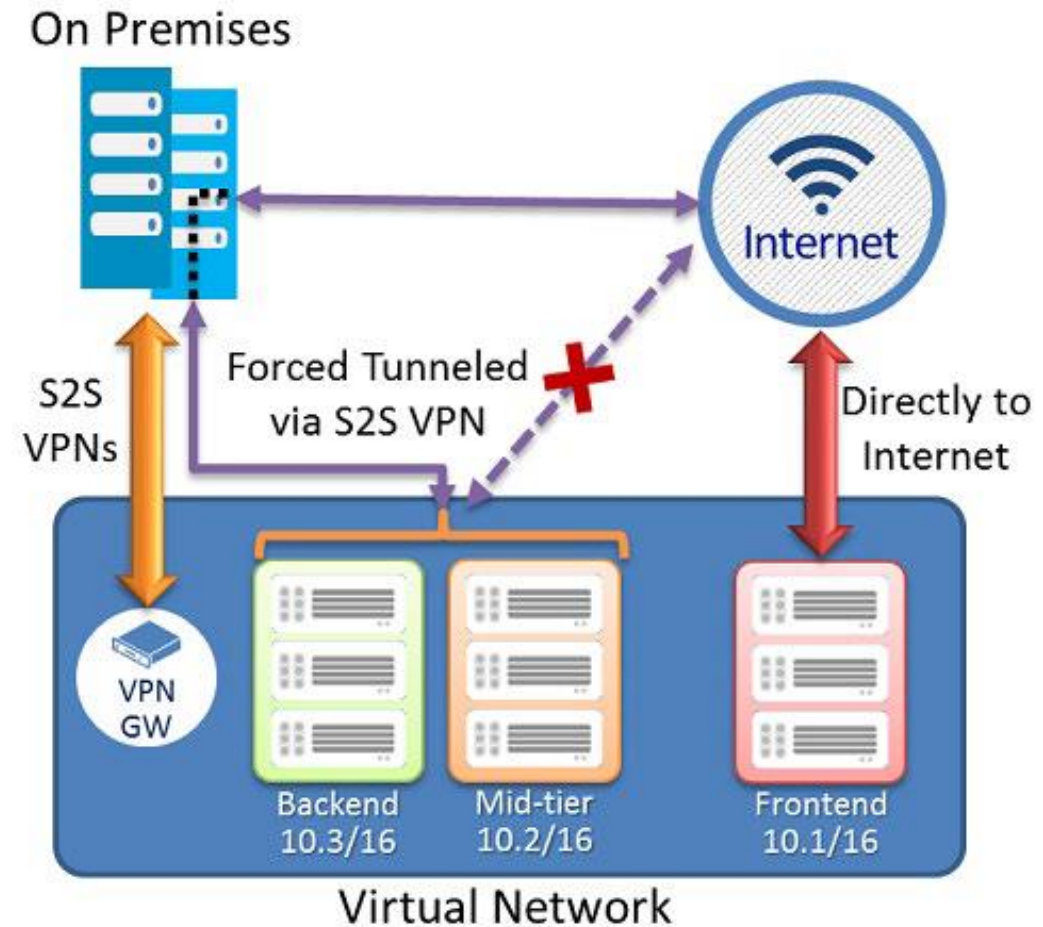
Remote work support

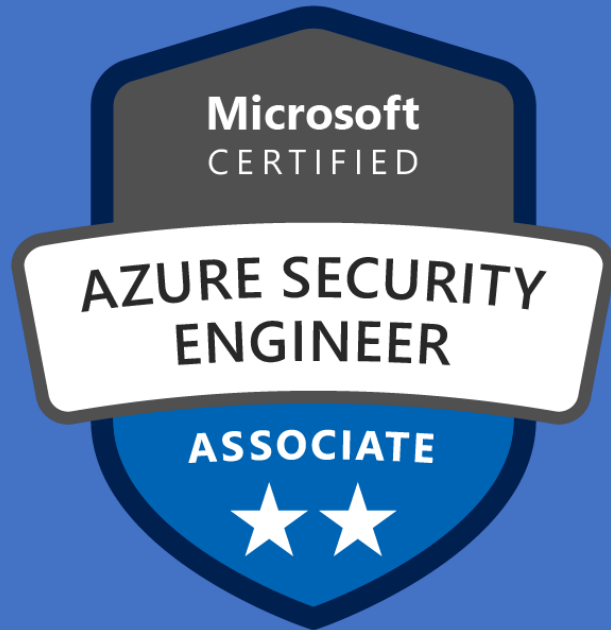
VPN Forced Tunneling



Redirect internet-bound traffic back to the company's on-premises infrastructure for inspection and auditing

Internet-bound traffic from VMs always traverses from Azure network infrastructure directly out to the internet, without inspection or audit

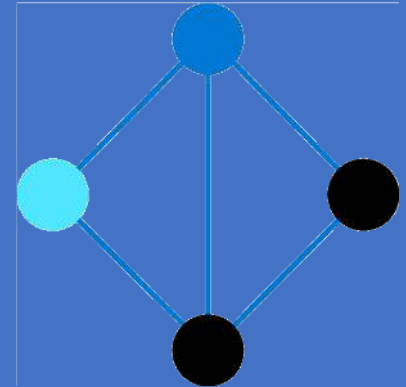




AZ-500

Episode 09

Network Security





Network Security Lesson Objectives



Network Security Groups (NSG)



NSG Implementation



Application Security Groups



Service Endpoints



Private Links



Azure Application Gateway



Web Application Firewall



Azure Front Door

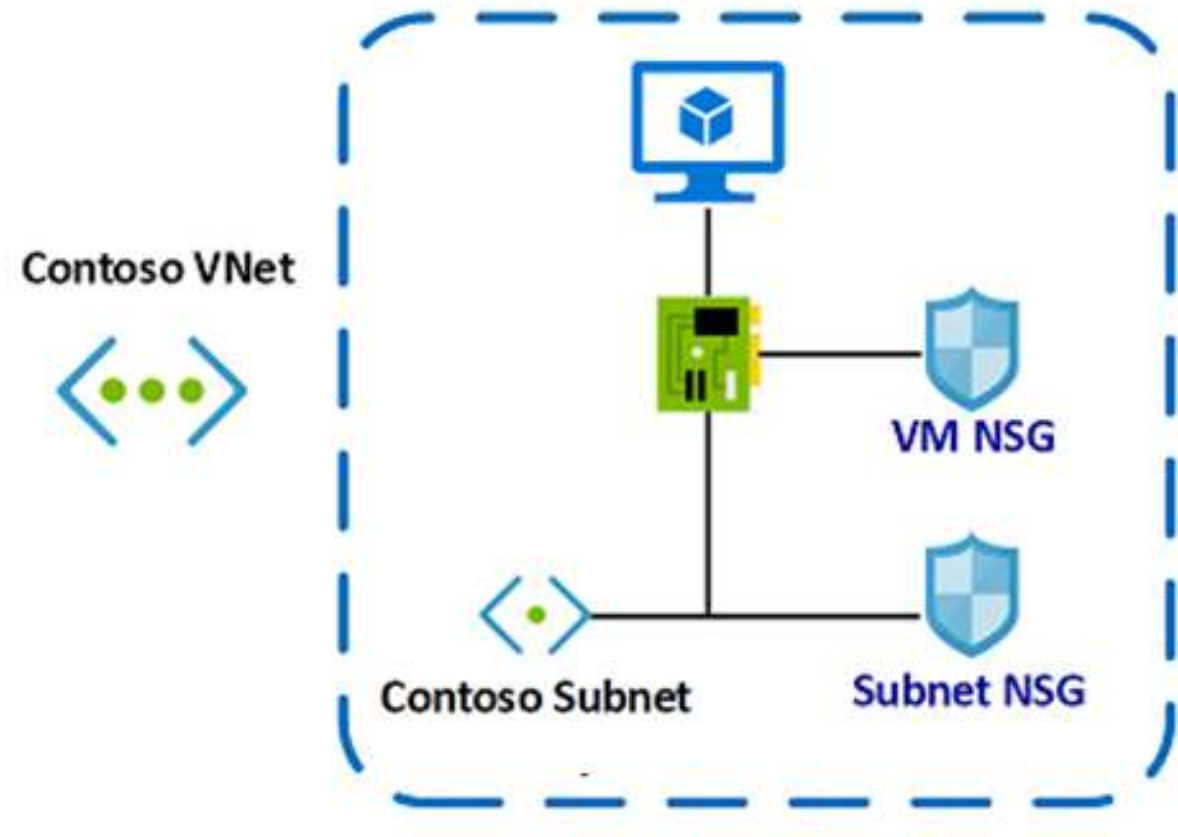


ExpressRoute

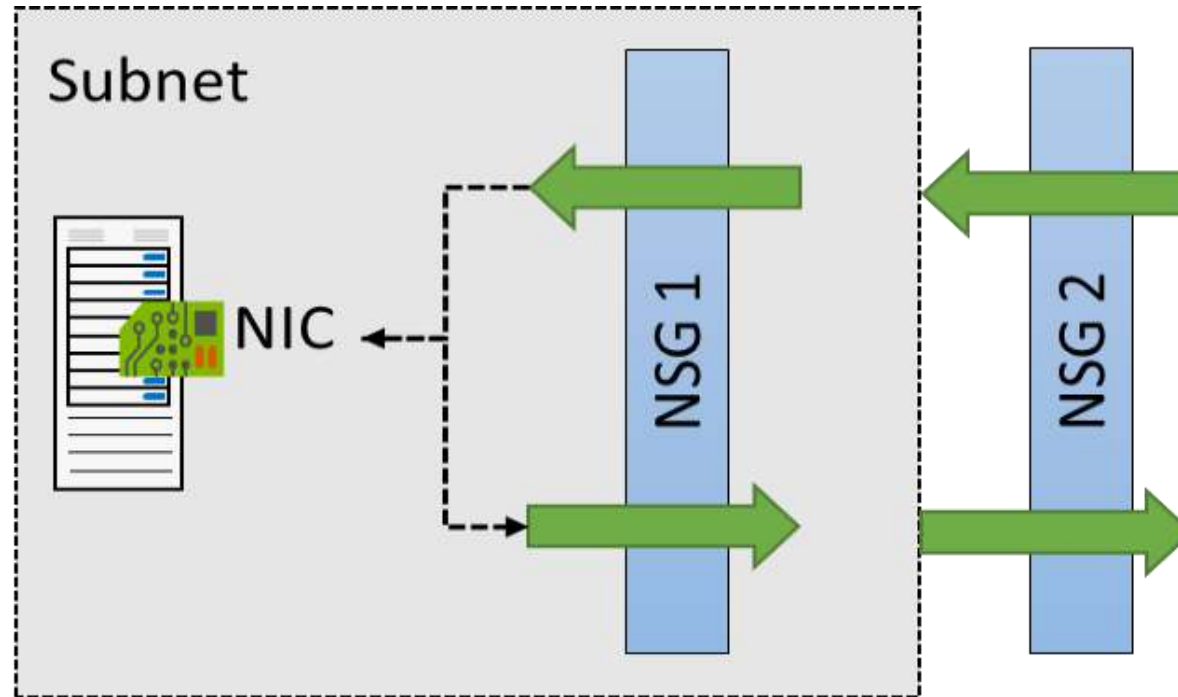
Network Security Groups (NSGs)



Name
Direction
Priority
Access
Source IP address prefix
Source port range
Destination IP address prefix
Destination port range
Protocol



NSG Implementation



Application Security Groups

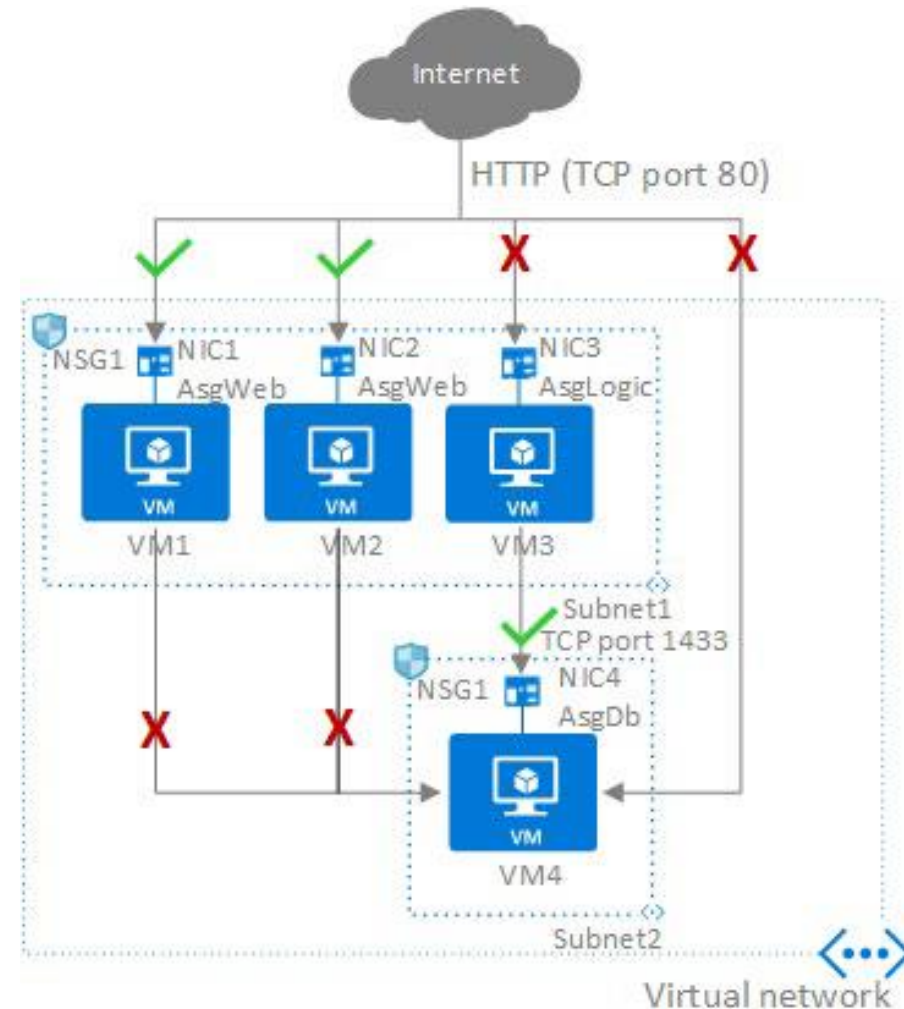


Extends your application's structure

ASGs logically group virtual machines – web servers, application servers

Define rules to control the traffic flow

Wrap the ASG with an NSG for added security



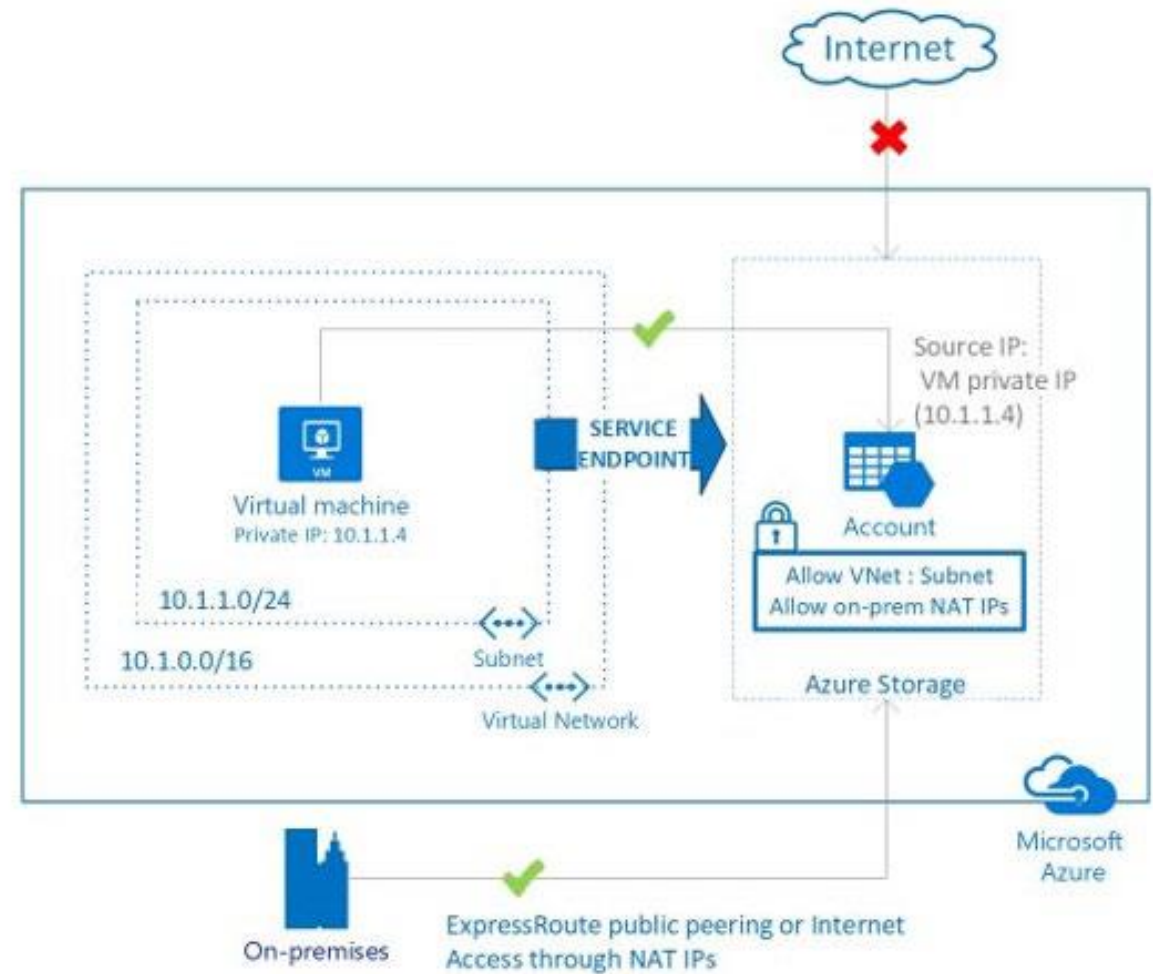
Service Endpoints



Endpoints use the Microsoft Azure backbone network

Improved security for your Azure service resources

Simple to set up with less management overhead



Why use a service endpoint?



Improved security for your Azure service resources

Optimal routing for Azure traffic from your virtual network

Endpoints always take service traffic directly from your virtual network to the service on the Microsoft backbone network

Simple to set up with less management overhead

Service Endpoint Services



Add service endpoints

Service *

Microsoft.Storage

Filter services

Microsoft.AzureActiveDirectory

Microsoft.AzureCosmosDB

Microsoft.CognitiveServices

Microsoft.ContainerRegistry

Microsoft.EventHub

Microsoft.KeyVault

Microsoft.ServiceBus

Microsoft.Sql

Microsoft.Storage

Microsoft.Web

Add

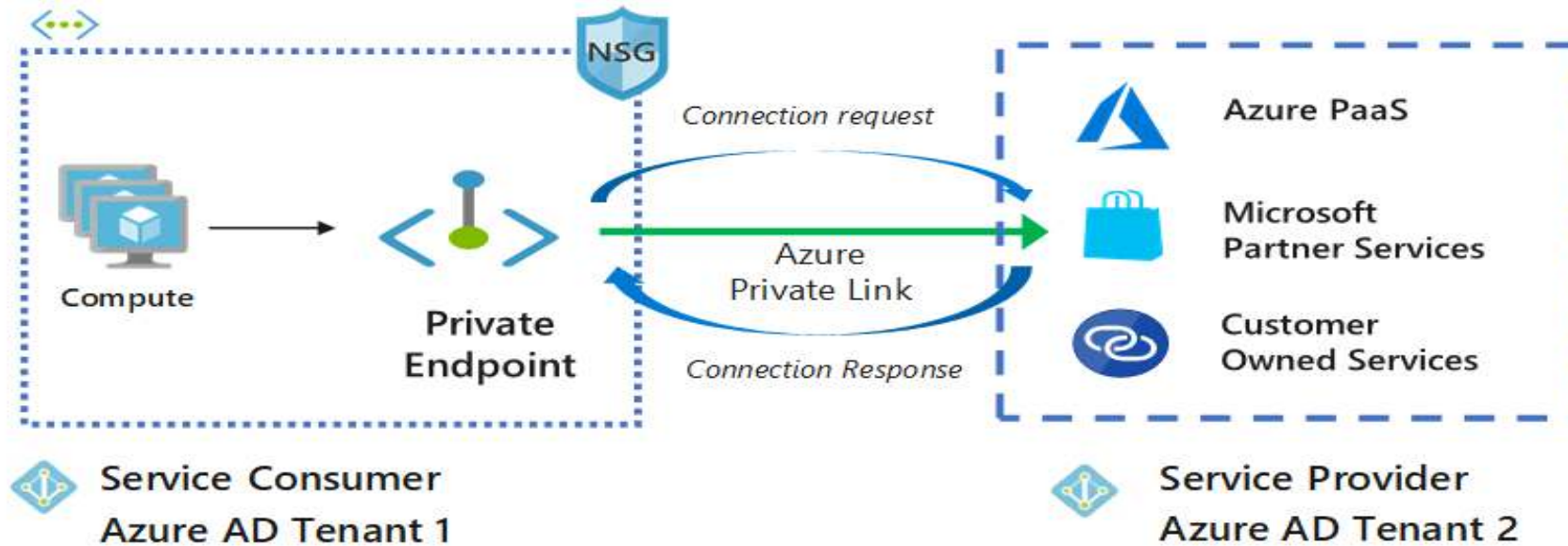
Peered, connected, or multiple virtual networks

Filtering outbound traffic from a virtual network to Azure services

Securing Azure resources to services deployed directly into virtual networks

Disk traffic from an Azure virtual machine

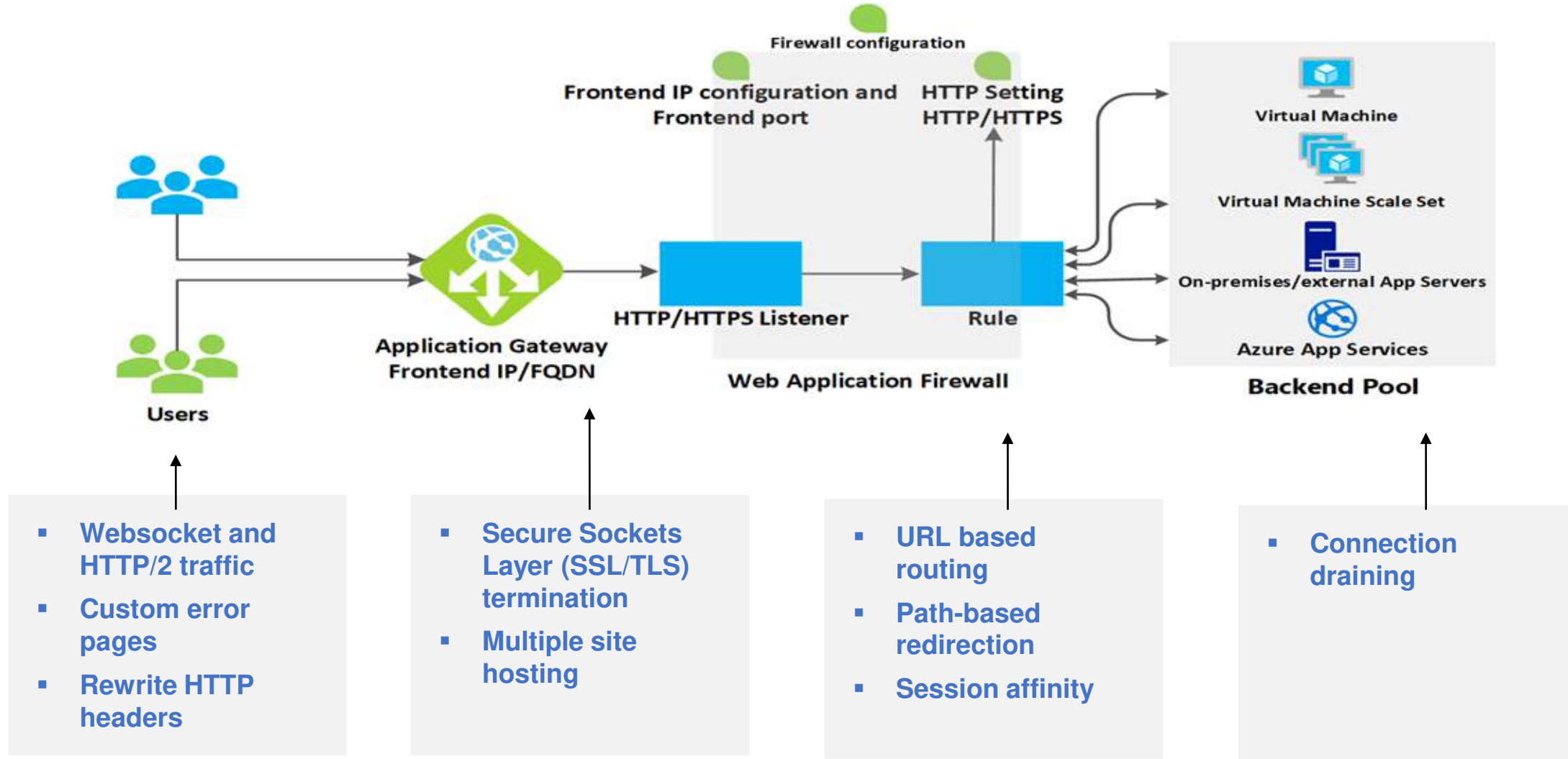
Private Links



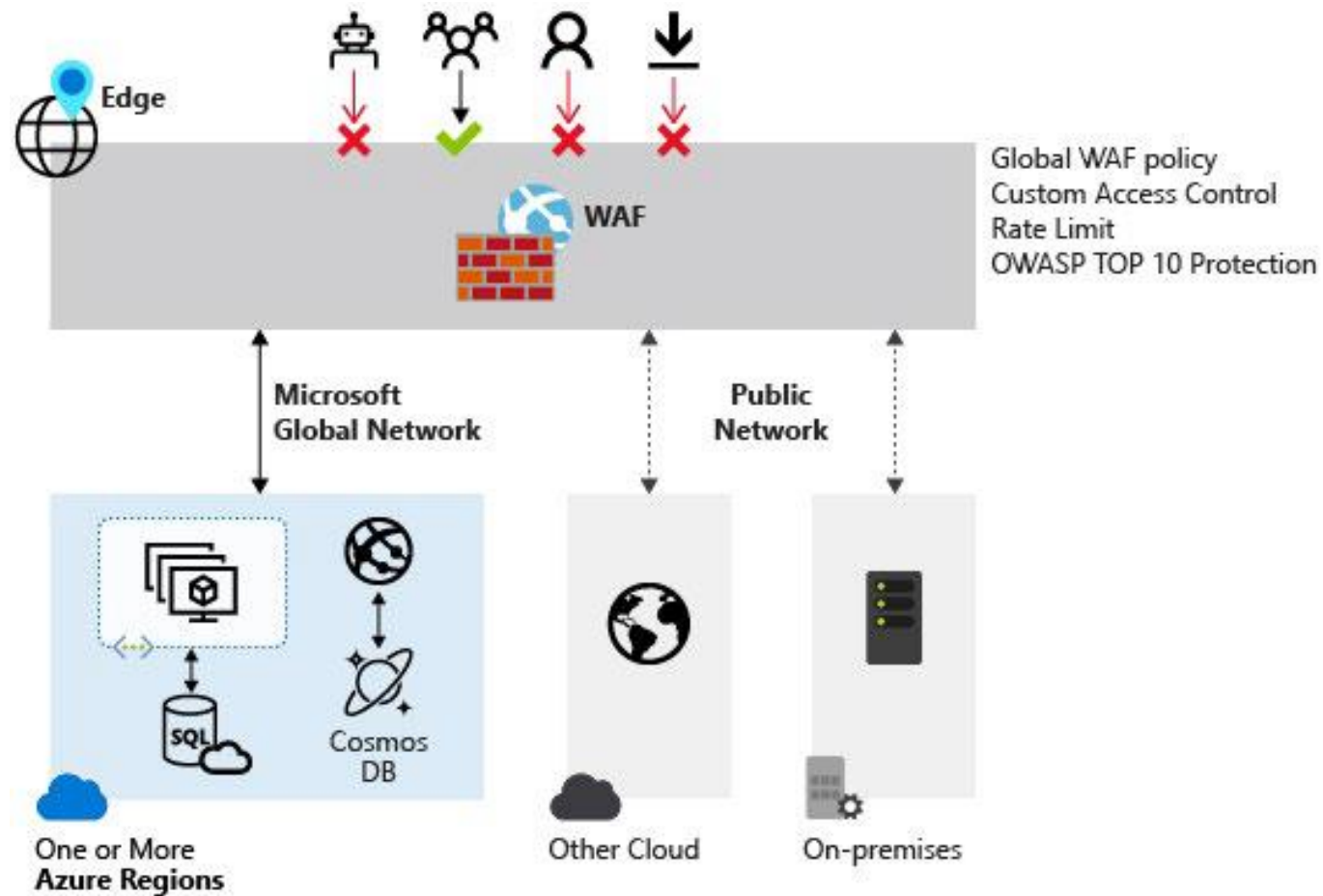
Automatic

Manual

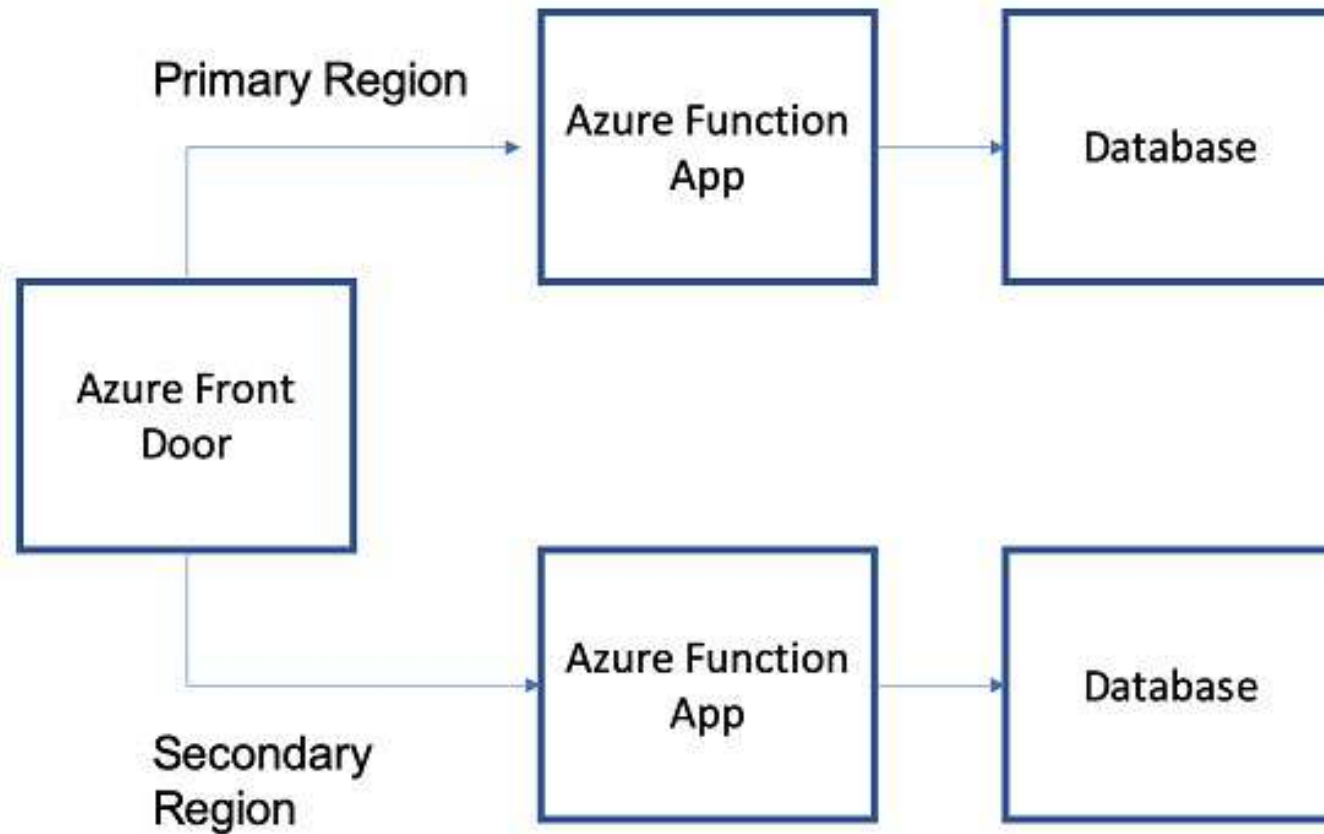
Azure Application Gateway



Web Application Firewall



Azure Front Door



Azure Front Door Features



Accelerate application performance

URL-based routing

Session affinity

Custom domains & certificate mgt

URL redirection

Increase application availability

Multiple-site hosting

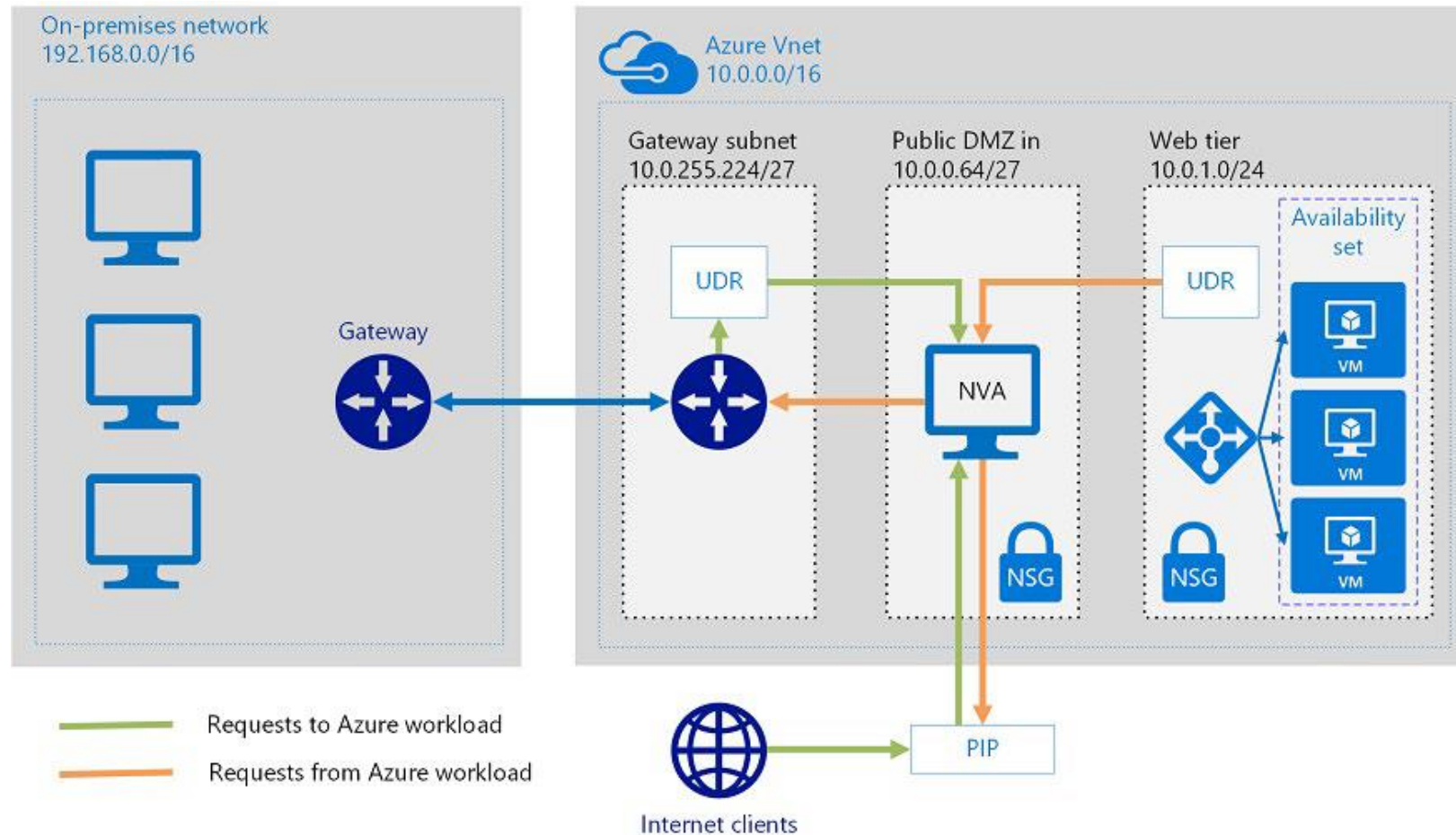
TLS termination

Application layer security

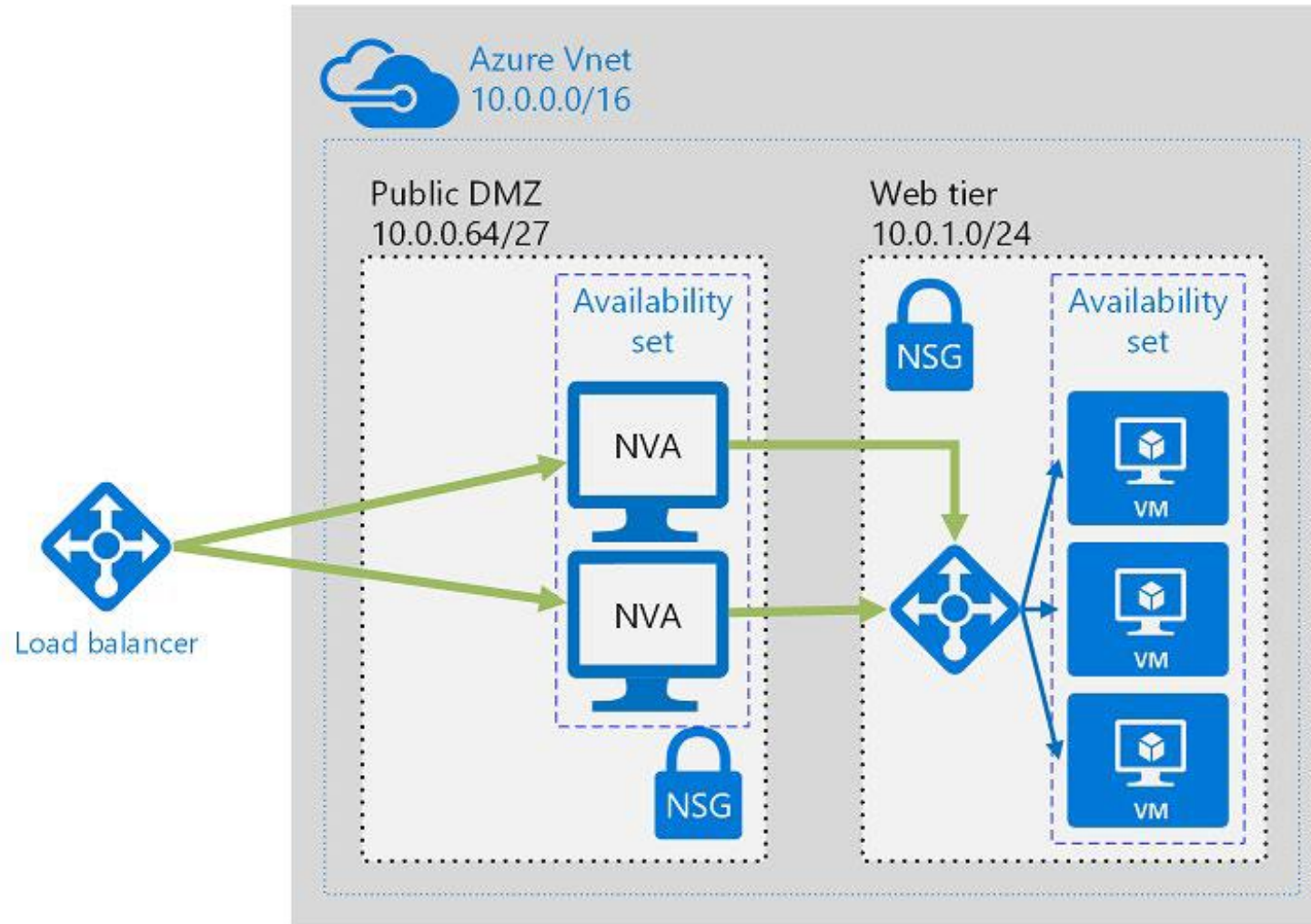
URL rewrite

Protocol support – IPv6 and HTTP/2 traffic

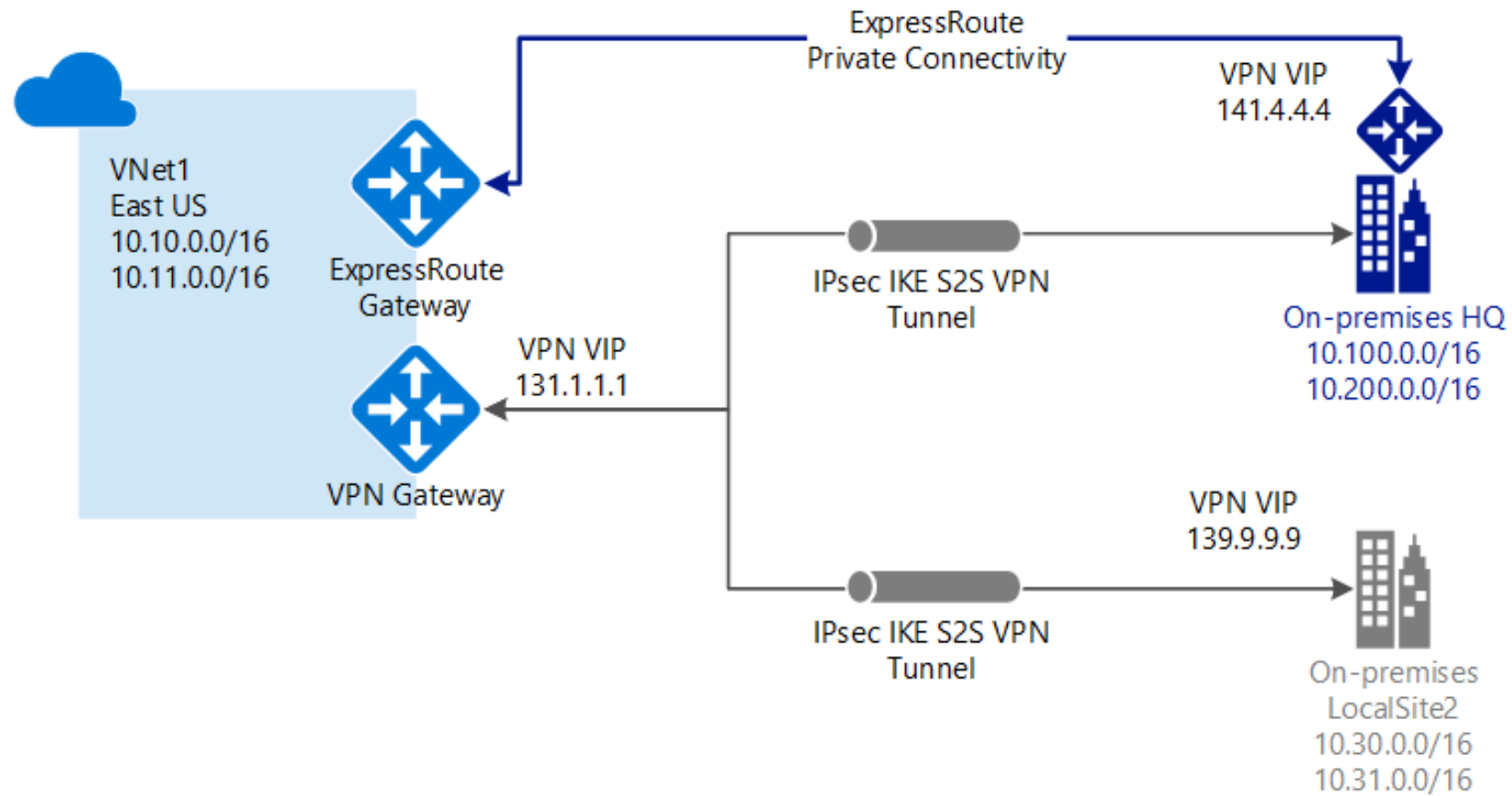
User Defined Routes



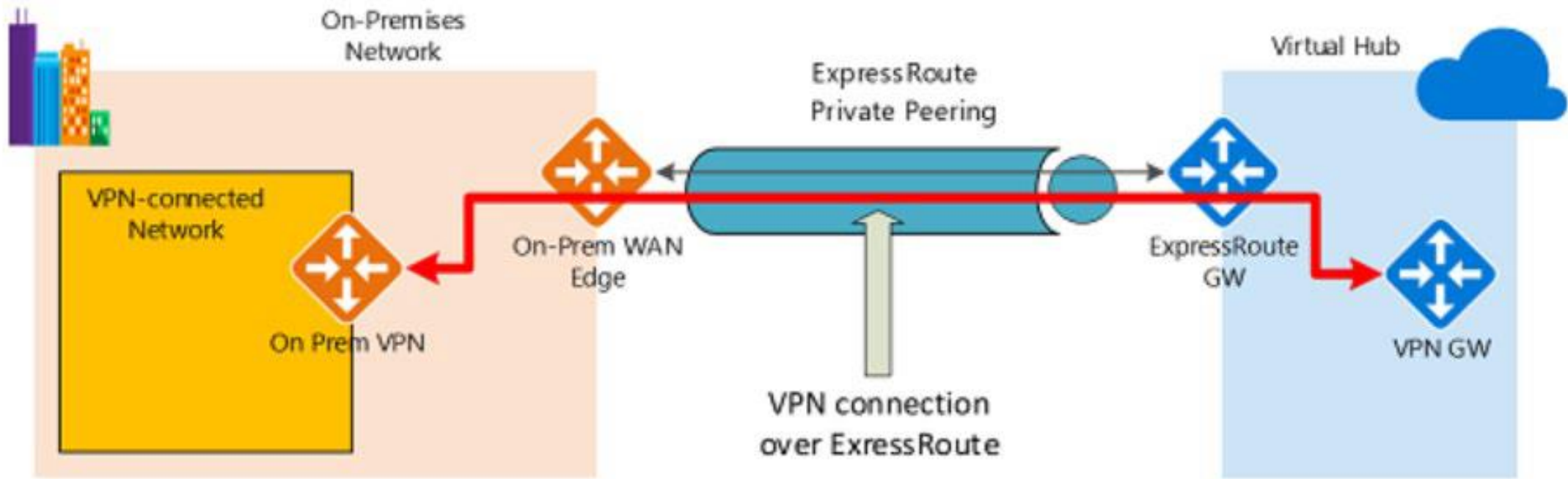
Network Virtual Appliances



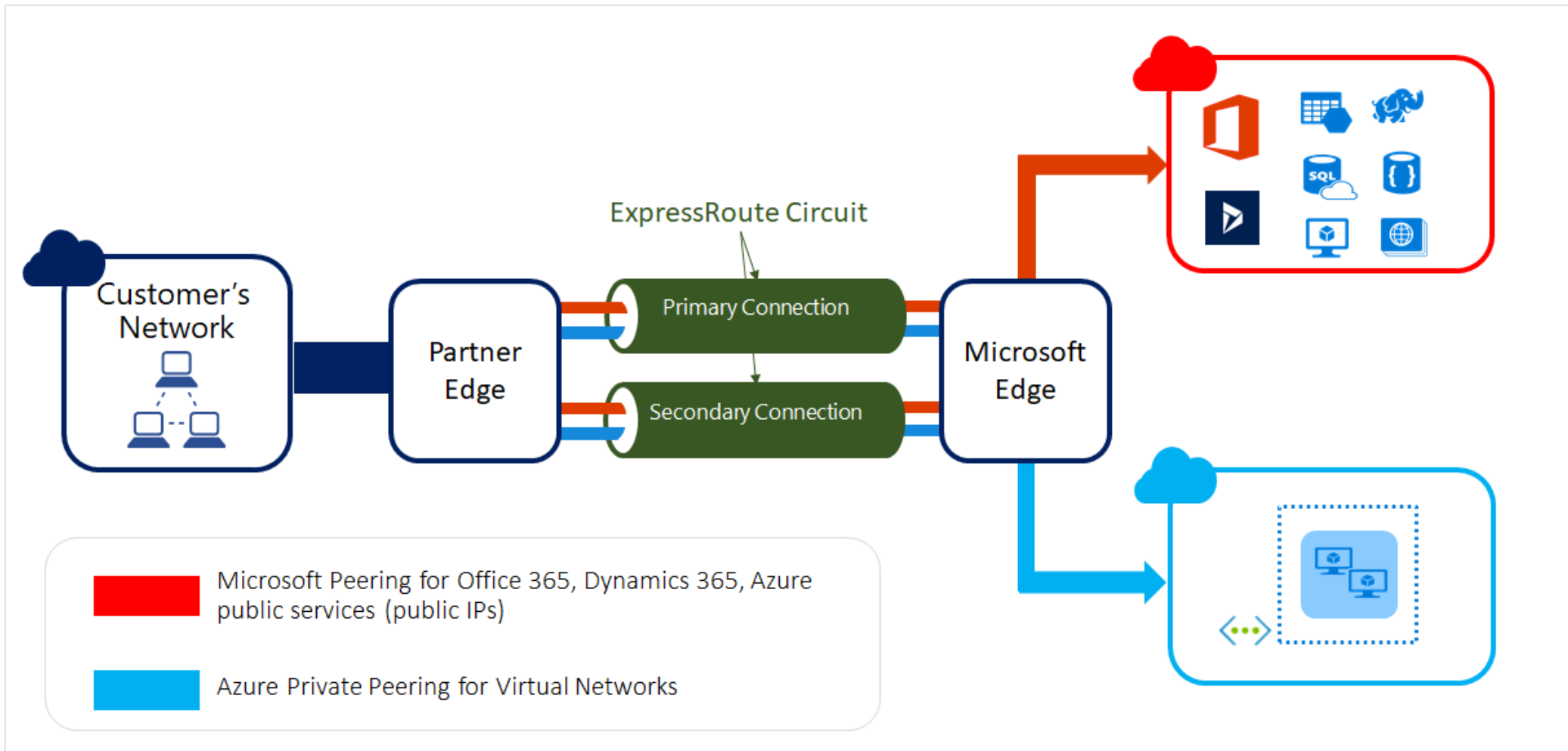
ExpressRoute

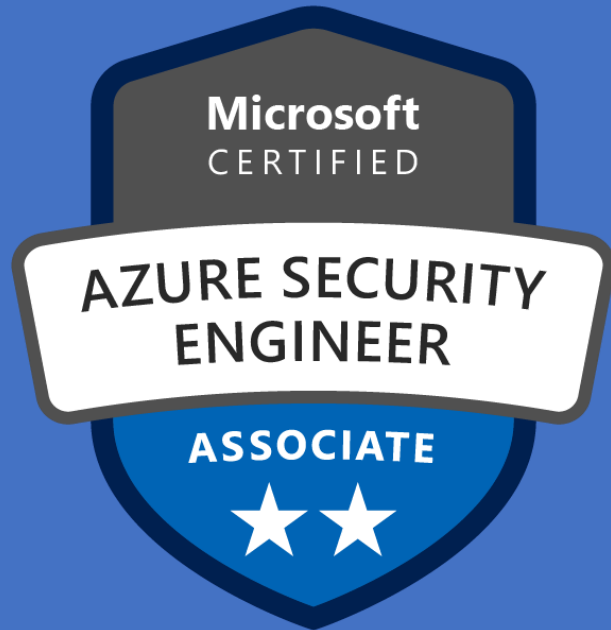


ExpressRoute Encryption



ExpressRoute Direct





AZ-500

Episode 10

Host Security





Host Security Lesson Objectives



Endpoint Protection



Privileged Access Workstations



Virtual Machine Templates



Remote Access Management



Update Management



Disk Encryption



Windows Defender

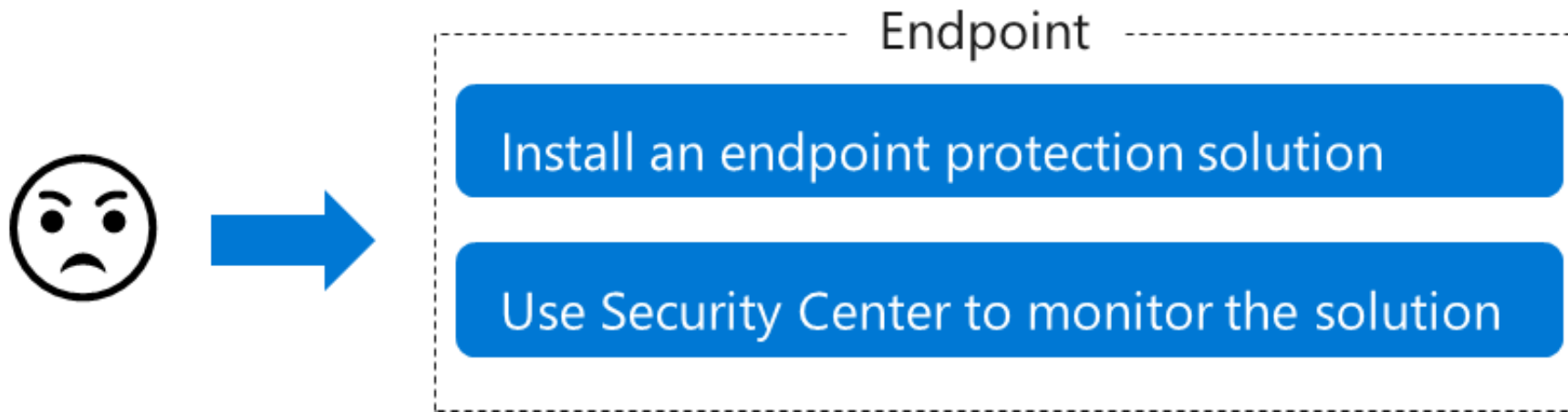


Security Center Host Recommendations



Securing Azure Workloads

Endpoint Protection



Endpoint systems interact directly with users

Endpoint systems are typically vulnerable to security attacks

Azure Security Center provides the tools you need to harden your network, secure your services, and solidify your security posture

Privileged Access Workstations



Internet attacks

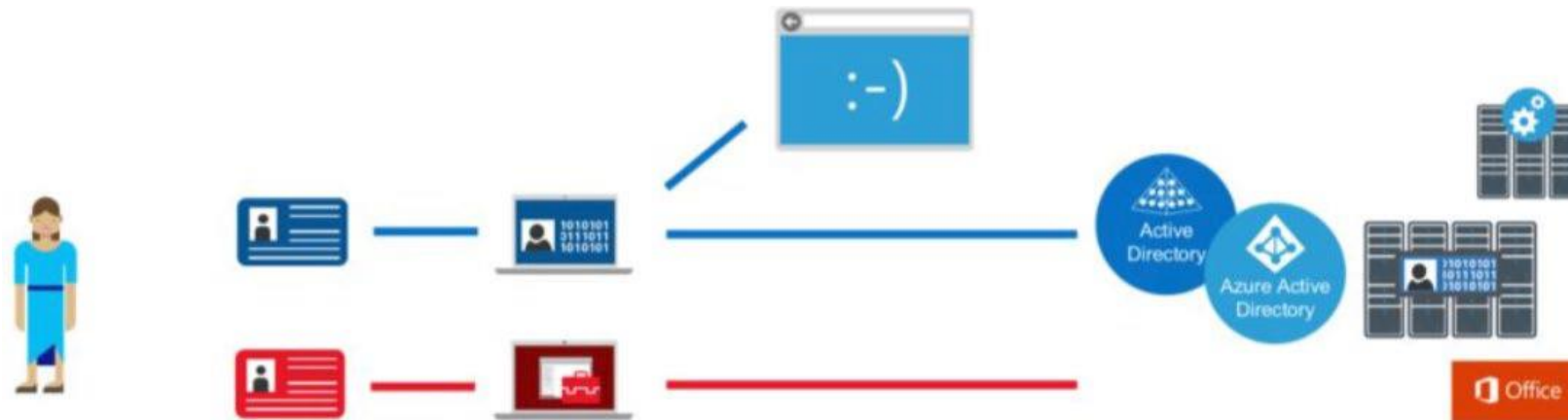
Usability risk

Environment risks

Supply chain tampering

Physical attacks

PAW Architecture Overview



Administrative Privileges

High Sensitive Information workers

PAW Jump Box



Virtual Machine Templates



Improves consistency

Express complex deployments

Reduce manual, error prone tasks

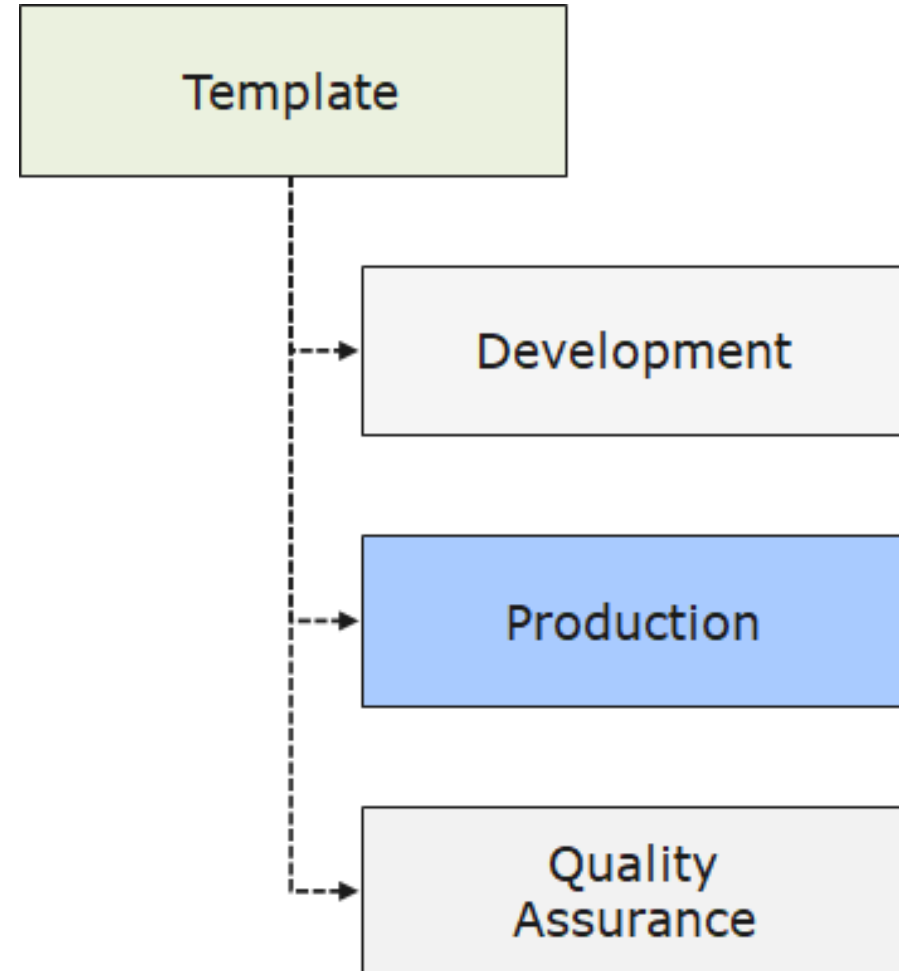
Express requirements through code

Promotes reuse

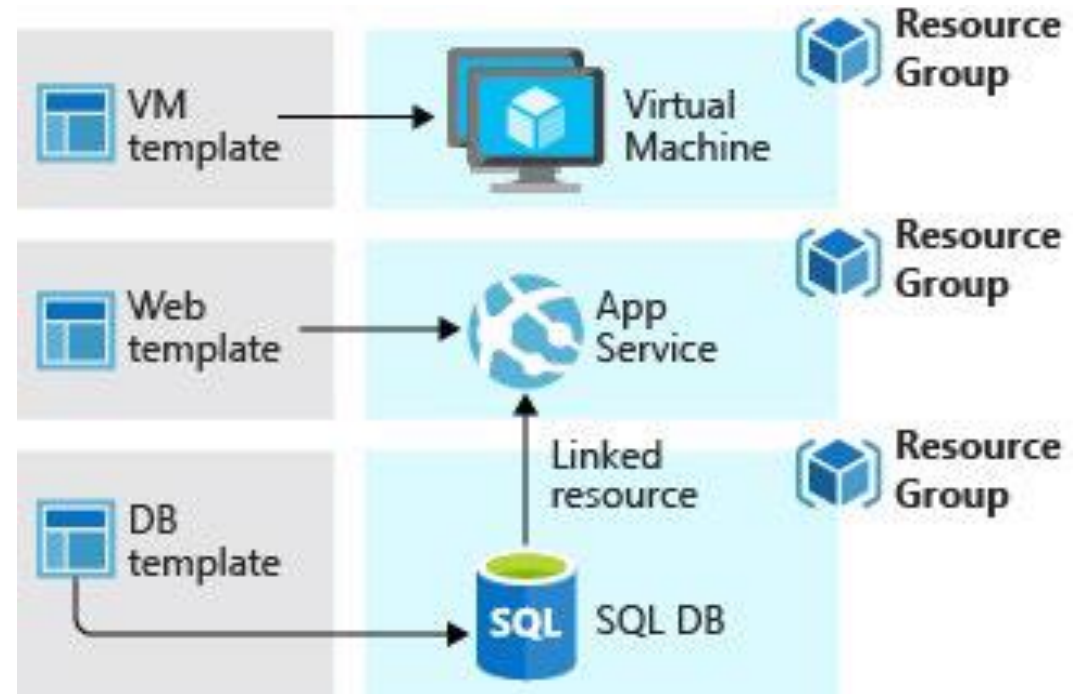
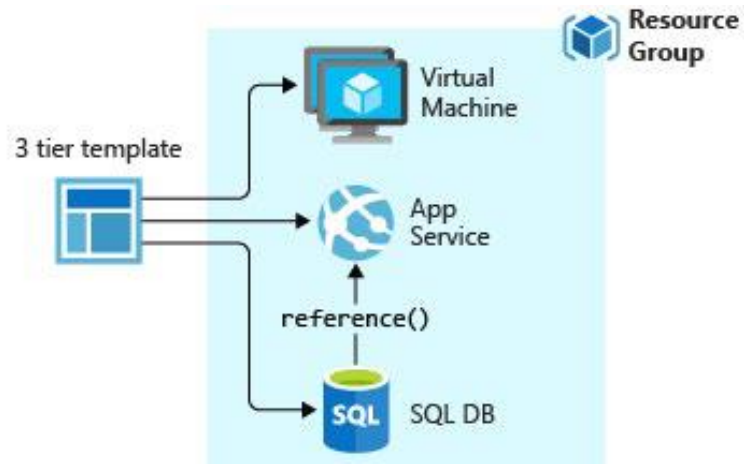
Modular and can be linked

Simplifies orchestration

Enforces security concerns



Template Design



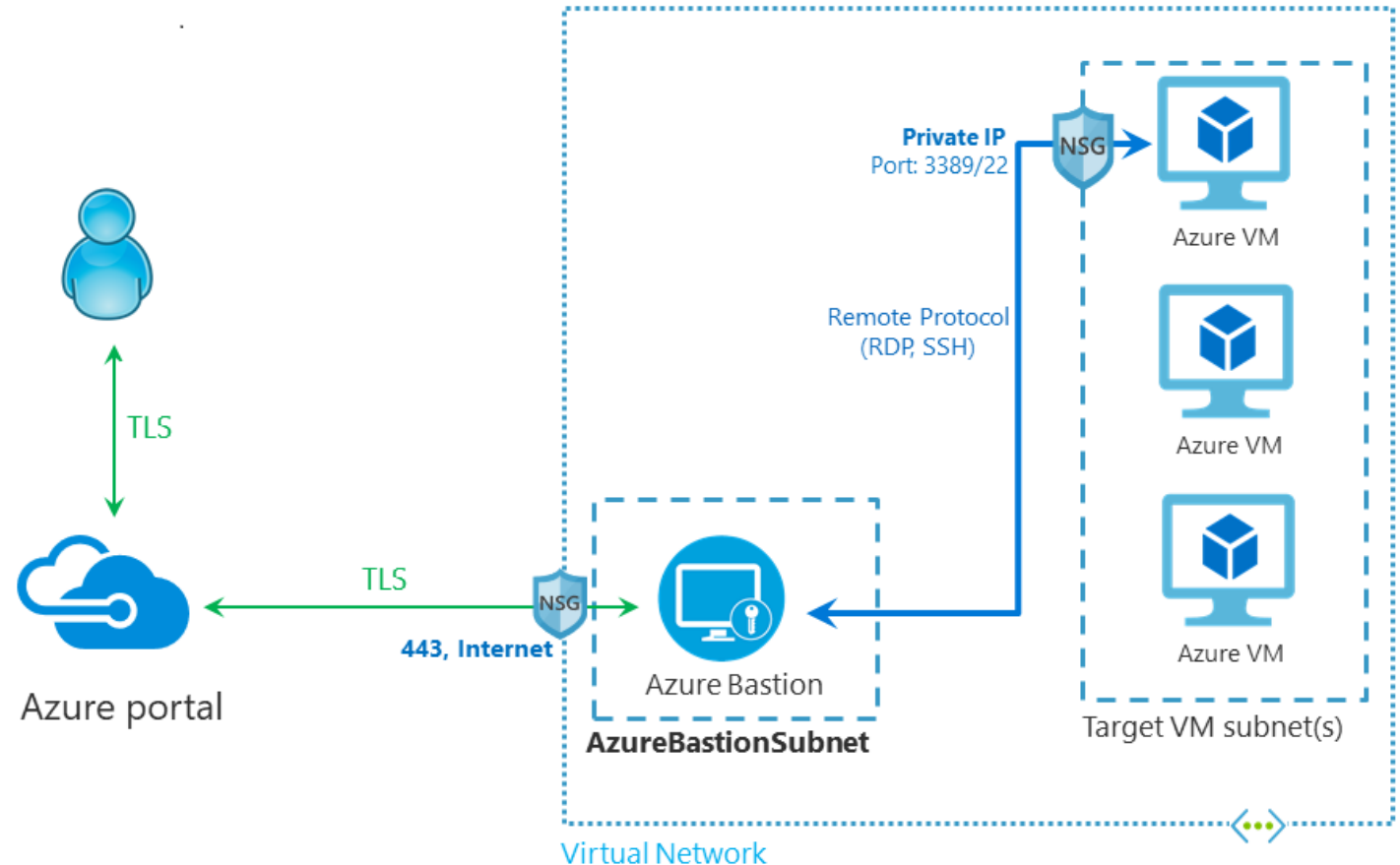
Remote Access Management



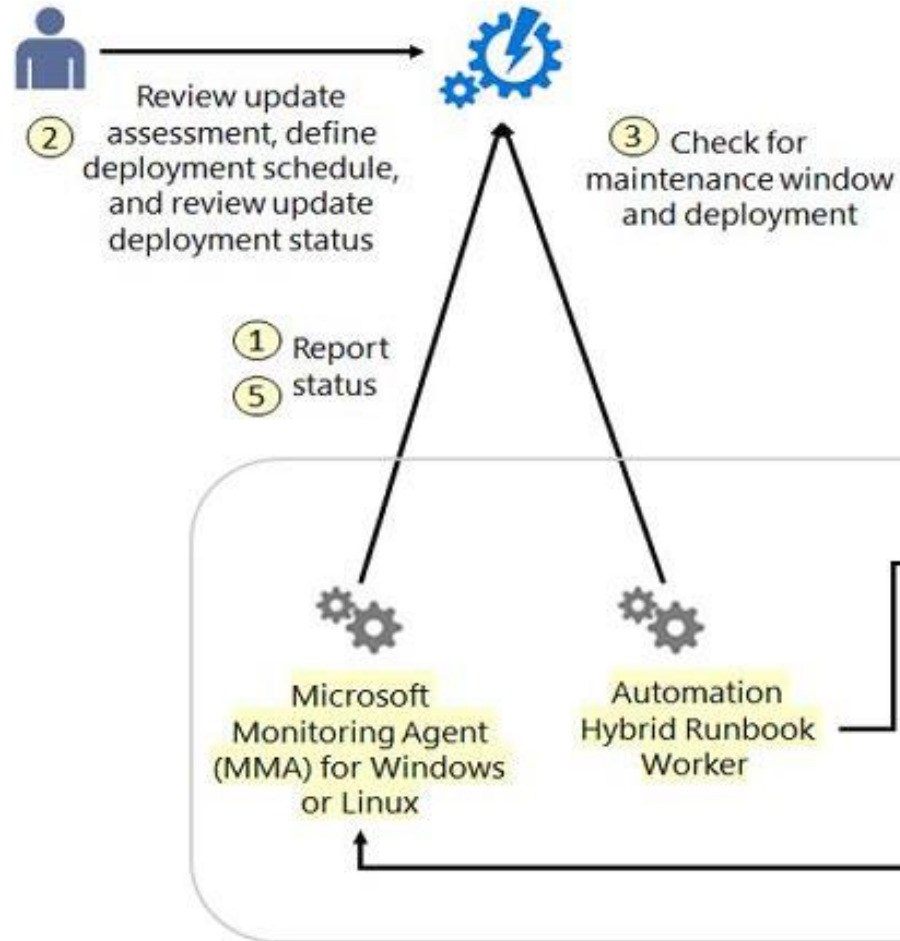
Remote Desktop Protocol (RDP) for
Windows-based virtual machines

Secure Shell Protocol (SSH) for Linux
based virtual machines

Bastion Subnet for RDP/SSH through
the Portal over SSL



Update Management



Updates for Windows and Linux machines in Azure, in on-premises environments, and in other cloud environments.

Manage updates for Multiple VMs



Non-compliant machines ⓘ

3 ⓘ

out of 4

Machines need attention (4) ⓘ

Critical and security 3

Other 1

Not assessed 0

Missing updates (32)

Critical 1 ⓘ

Security 0

Others 31

Failed update deployments ⓘ

2 ⓘ

out of 8 in the past six months

Learn more

Update Management

Provide feedback

Machines (4)

Missing updates (32)

Update deployments

Scheduled update deployments

Filter by name

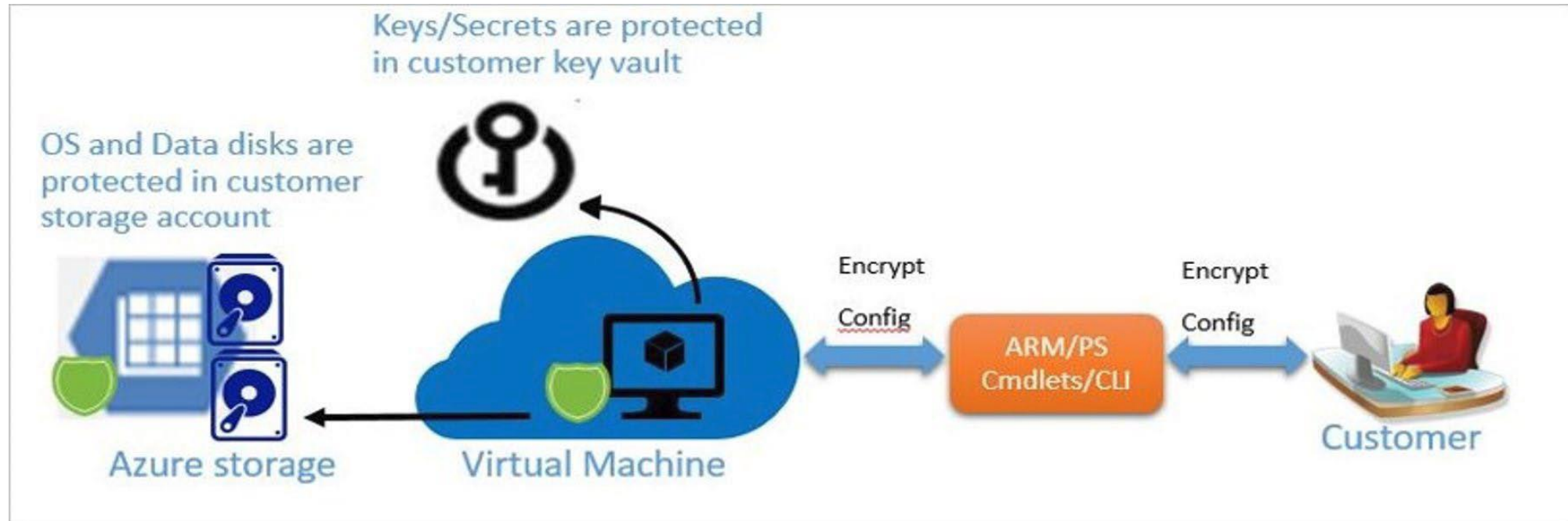
Compliance: All

Platform: All

Operating system: All

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

Disk Encryption



Supported VMs and operating systems

Networking requirements

Group policy requirements

Encryption Key Storage requirements

Windows Defender



Platforms

Windows 10, Windows Server 2016, and Windows Server 2019

Windows Defender Credential Guard

Virtualization-based security to isolate secrets so that only privileged system software can access them

Windows Defender Application Control

Mitigate attacks from spyware, adware, rootkits, viruses, and keyloggers, by restricting the applications that users can run and the code that runs in the system core or kernel

Security Center Recommendations



Security policy

Visual Studio Ultimate with MSDN

Save Discard

Prevention policy

Visual Studio Ultimate with MSDN

Data collection

Collect data from virtual machines ⓘ

☒ On ☐ Off

Choose a storage account per region

All configured >

Policy components

Prevention policy >

Email notifications >

Pricing tier >

Show recommendations for

System updates ⓘ	☒ On ☐ Off
OS vulnerabilities ⓘ	☒ On ☐ Off
Endpoint protection ⓘ	☒ On ☐ Off
Disk encryption	☒ On ☐ Off
Network security groups	☒ On ☐ Off
Web application firewall	☒ On ☐ Off
Next generation firewall	☒ On ☐ Off
Vulnerability Assessment	☒ On ☐ Off
SQL auditing & Threat detection	☒ On ☐ Off
SQL transparent data encryption	☒ On ☐ Off

Virtual machines

SECURITY HEALTH

MONITORING RECOMMENDATIONS

	TOTAL
Data collection installation status	1 of 8 VMs

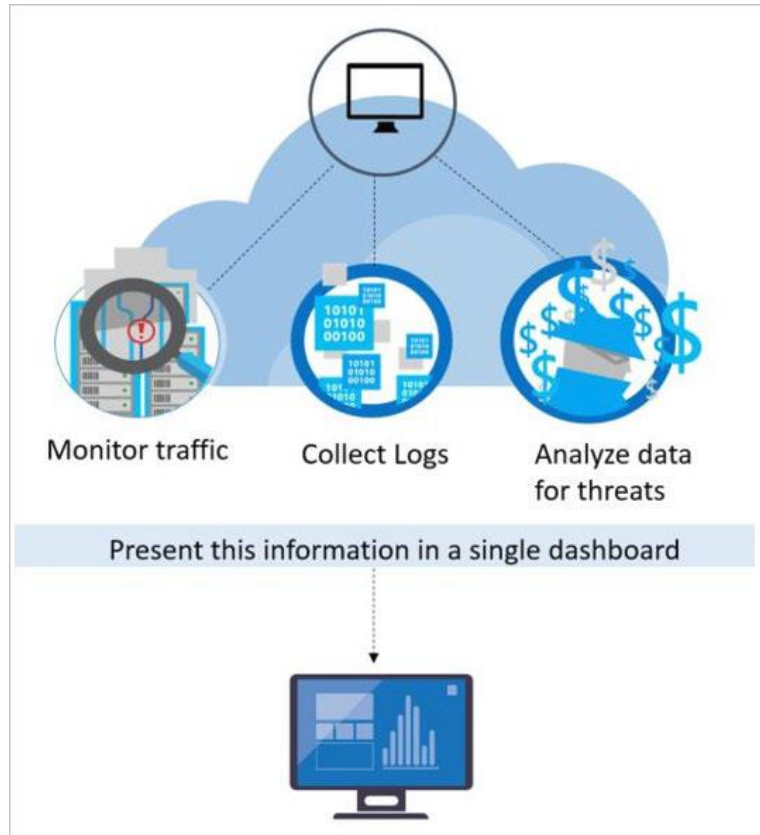
VIRTUAL MACHINES RECOMMENDATIONS

	TOTAL
Endpoint Protection not installed	3 of 8 VMs
Missing scan data	2 of 8 VMs
Remediate OS vulnerabilities (by Microsoft)	1 of 8 VMs
Restart pending	1 of 8 VMs
Missing disk encryption	2 of 8 VMs
Healthy	1 of 8 VMs

Virtual machines

NAME	MONITORED	SYSTEM UPDATES	ENDPOINT PROTE...	VULNERABILITIES	DISK ENCRYPTION
RomeDC					
FileServer					
VM01					
RomeWin10Client					
IgniteOMS					
Win10Client					
AppServer					
VMDemo01					

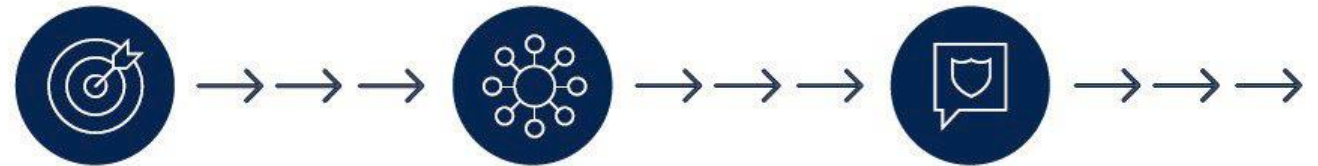
Security Center Threat Detection



Integrated threat intelligence

Behavioral analytics

Anomaly detection



TARGET AND ATTACK

Inbound brute force RDP, SSH, SQL attacks and more

Application and DDoS attacks (WAF partners)

Intrusion detection (NG Firewall partners)

INSTALL AND EXPLOIT

In-memory malware and exploit attempts

Suspicious process execution

Lateral movement

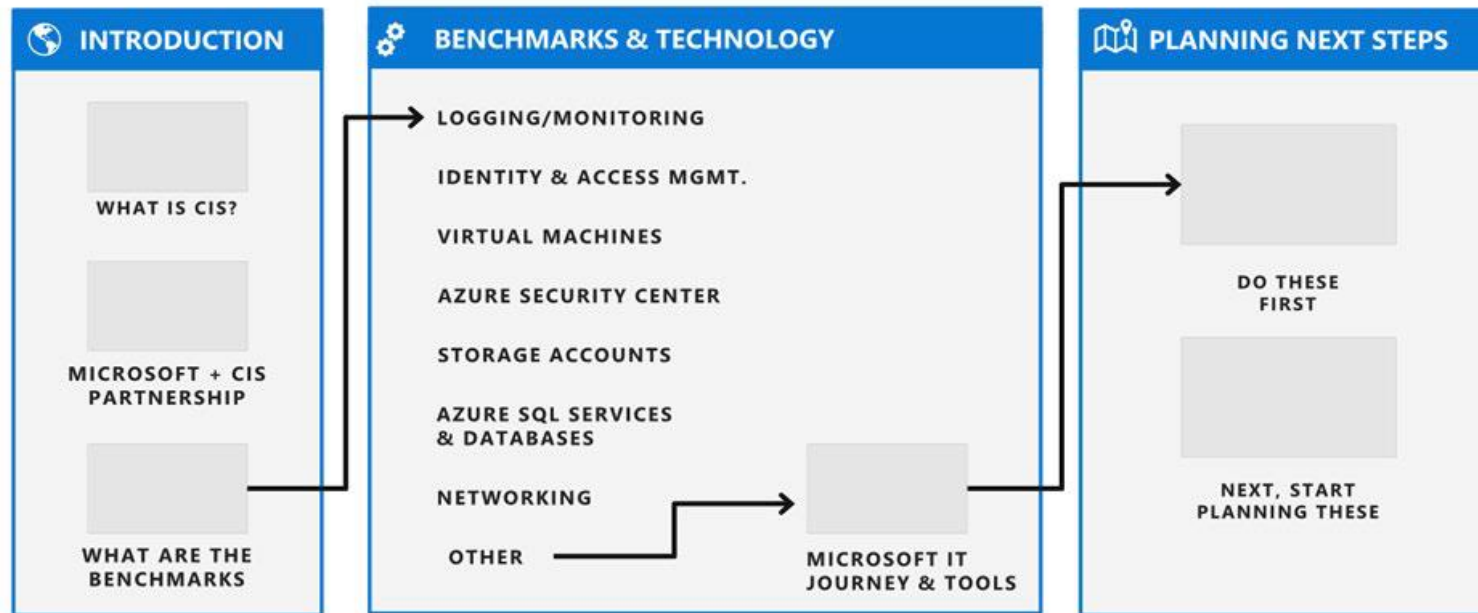
Internal reconnaissance

POST BREACH

Communication to a known malicious IP (data exfiltration or command and control)

Using compromised resources to mount additional attacks (outbound port scanning, brute force RDP/SSH attacks, DDoS, and spam)

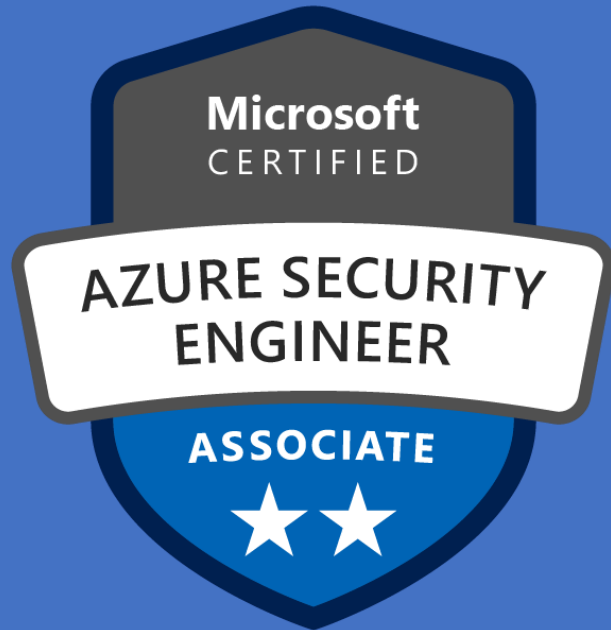
Securing Azure Workloads



CIS best practices to establish security baselines

Recommendations are divided into categories

Two levels (minimum and highly secure)



AZ-500

Episode 11

Container Security





Container Security Lesson Objectives



Containers



ACI Security



Azure Container Instances (ACI)



Azure Container Registry (ACR)



ACR Authentication



Azure Kubernetes Service (AKS)



AKS Terminology



AKS Architecture



AKS Networking

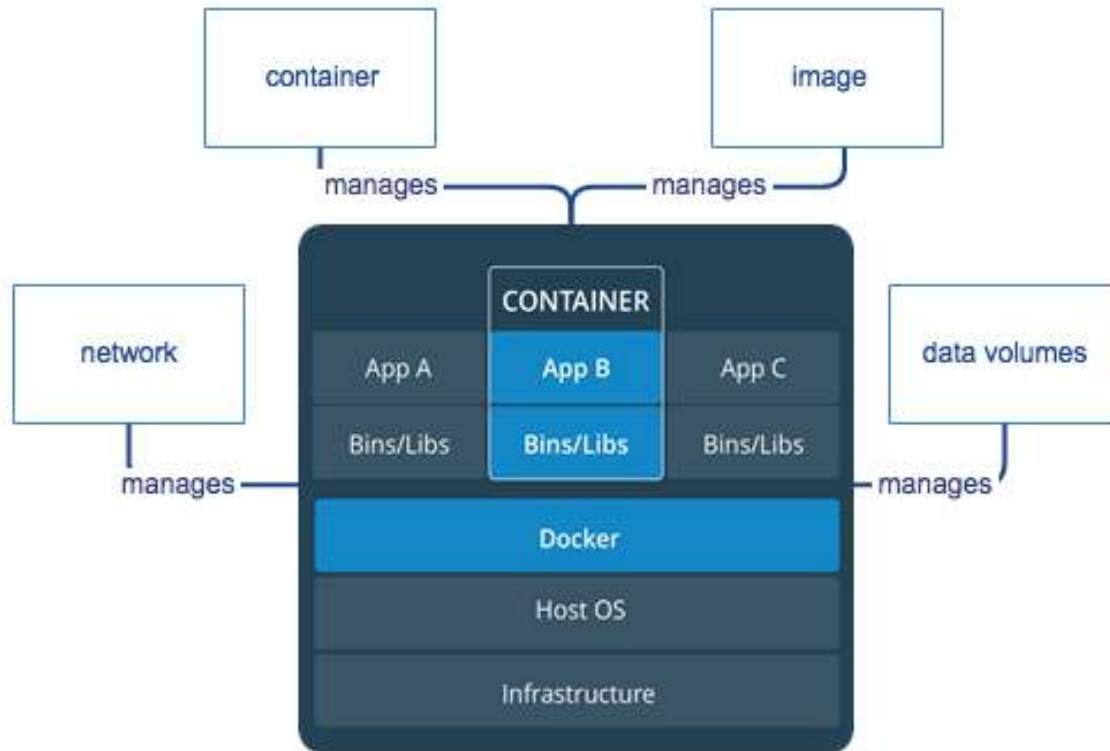


AKS Storage



AKS and Active Directory

Containers



Isolation

Operating System

Deployment

Persistent Storage

Fault tolerance

ACI Security



Continuously scan registry images

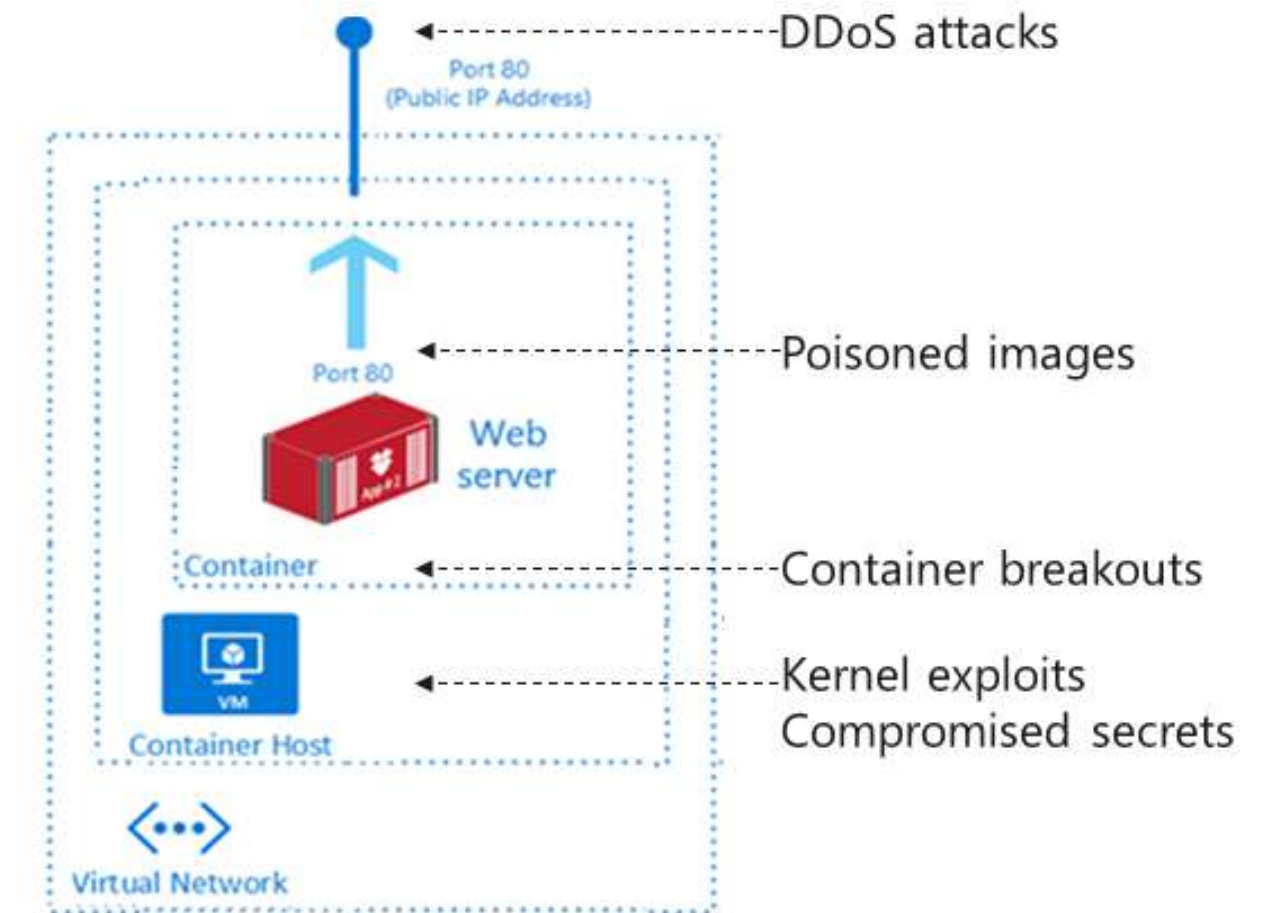
Use approved images – chain of custody, signing

Run with least privileges

Whitelist files the container can access

Maintain network segmentation

Monitor and log activities



Azure Container Instances (ACI)



Fast startup times

Container access

Container deployment

Hypervisor-level security

Custom sizes

Persistent storage

Flexible billing

Linux and Windows containers

Co-scheduled groups

Virtual network deployment

Home > Container instances > Create container instance

Create container instance

Basics Networking Advanced Tags Review + create

Container details

Container name * ⓘ

Region * ⓘ (US) West US 2 ▼

Image source * ⓘ ☒ Quickstart images
☐ Azure Container Registry
☐ Docker Hub or other registry

Image * ⓘ microsoft/aci-helloworld (Linux) ▼

Size * ⓘ 1 vcpu, 1.5 GiB memory, 0 gpus
[Change size](#)

Azure Container Registry (ACR)



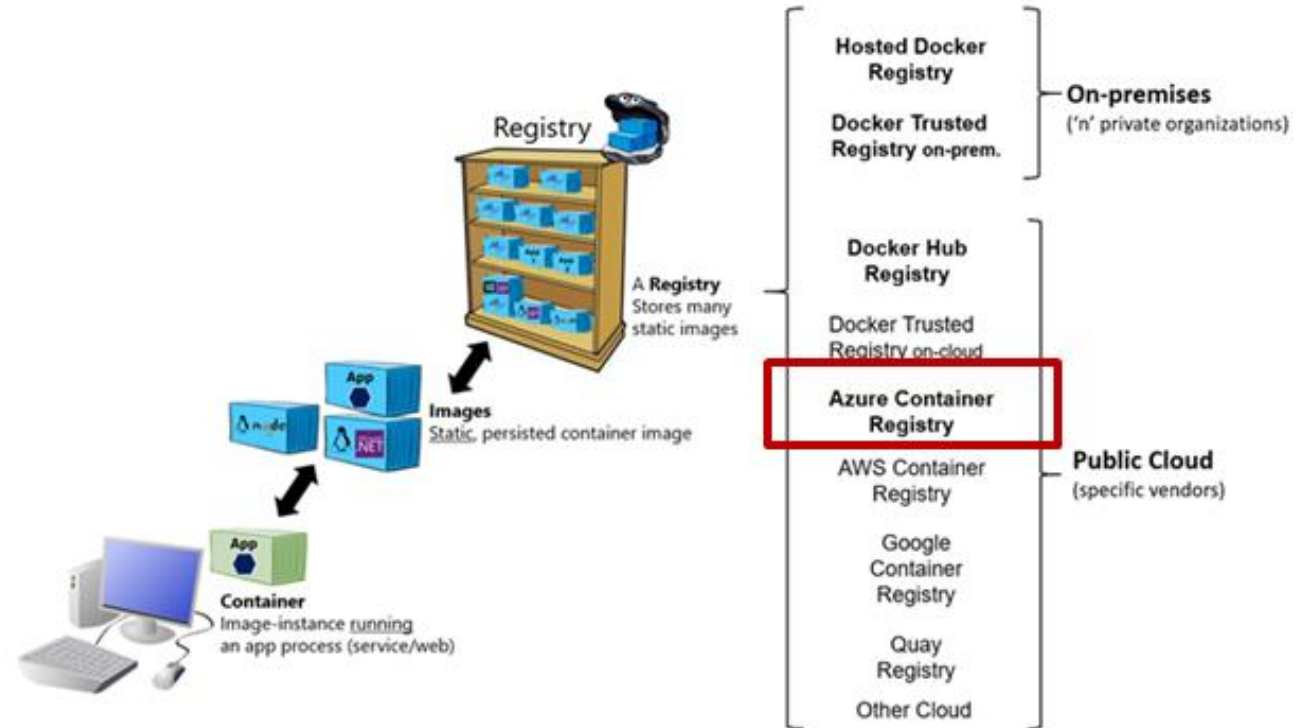
Registry

Security and access

Repository

Image

Monitor container activity and user access



ACR Authentication



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.

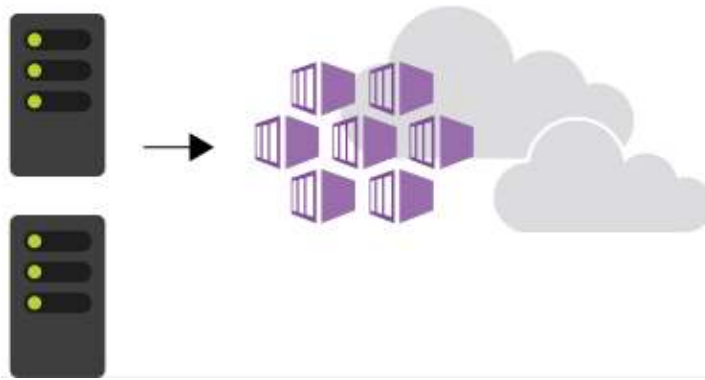
Azure Kubernetes Service (AKS)



Fully managed

Public IP and FQDN (Private IP option)

Accessed with RBAC or Azure AD

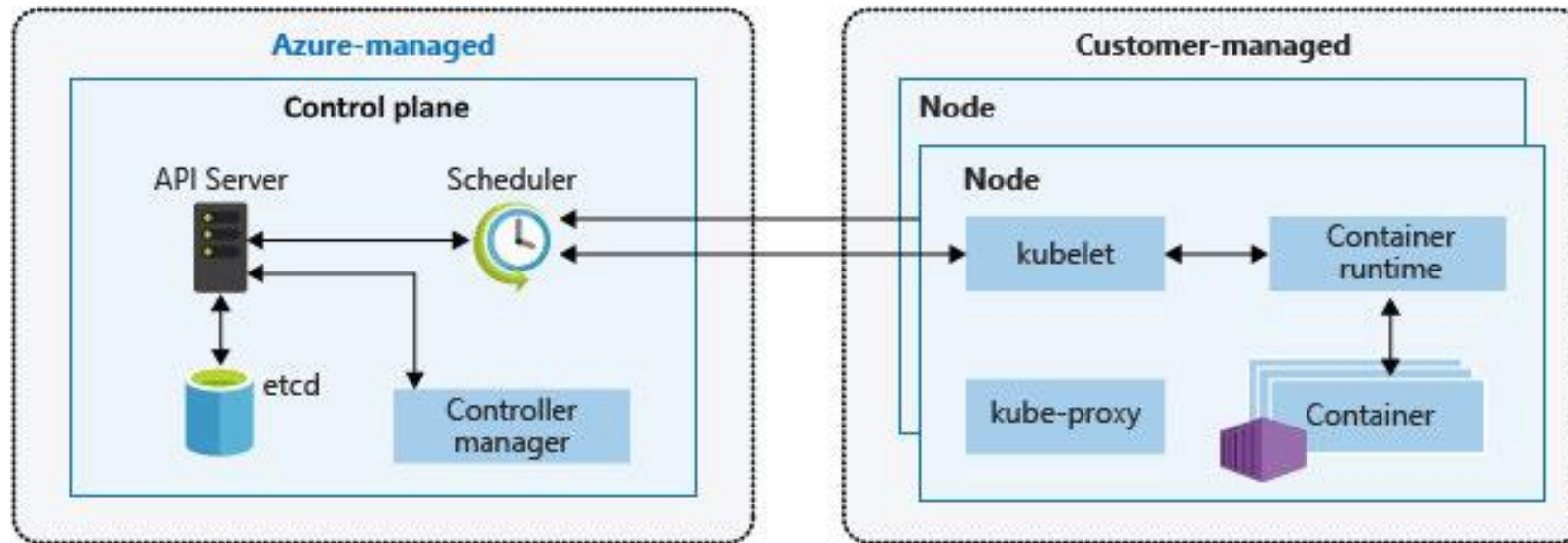


Dynamic scale containers

Automation of rolling updates and rollbacks of containers

Management of storage, network traffic, and sensitive information

Kubernetes Cluster Architecture



Kube-apiserver

etcd

Kube-scheduler

Kube-controller-manager

AKS Terminology



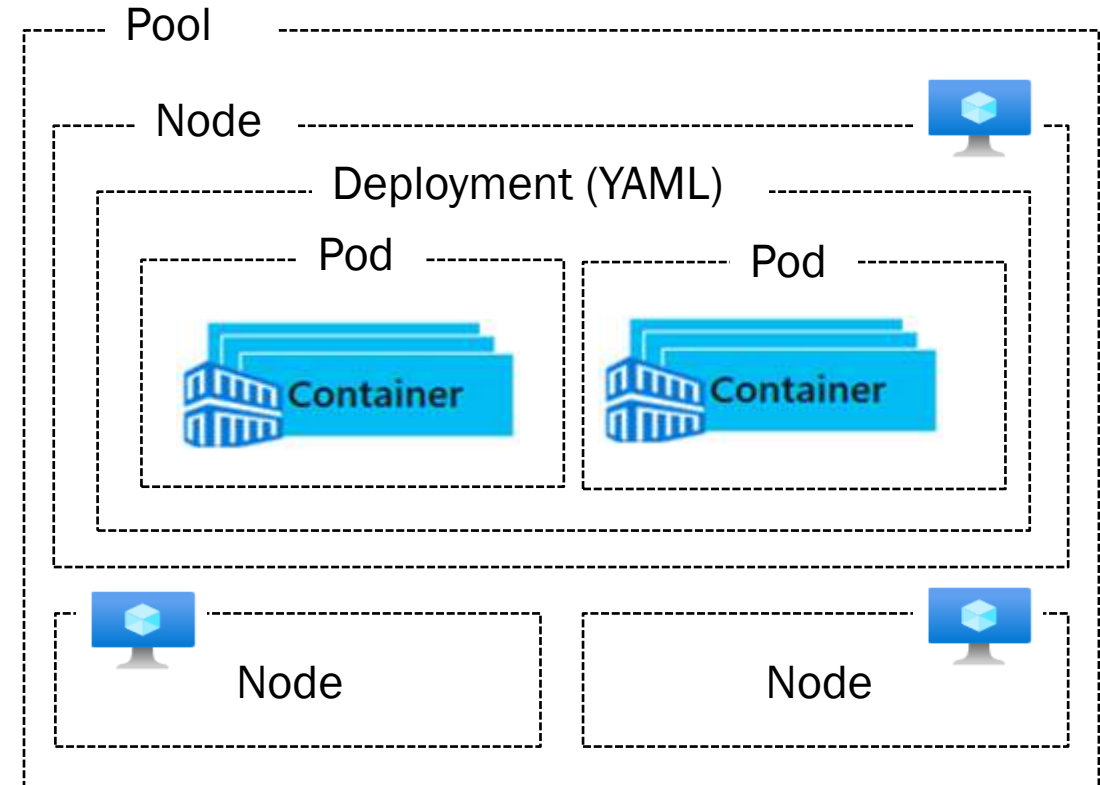
Pools

Node

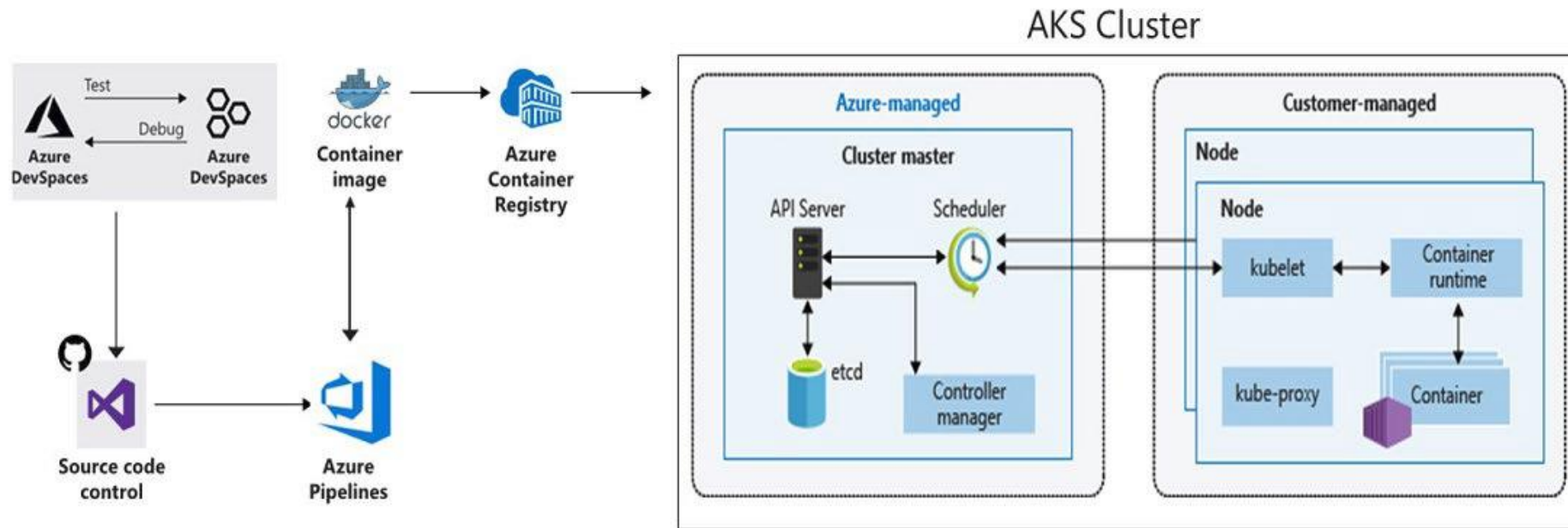
Pods

Deployment

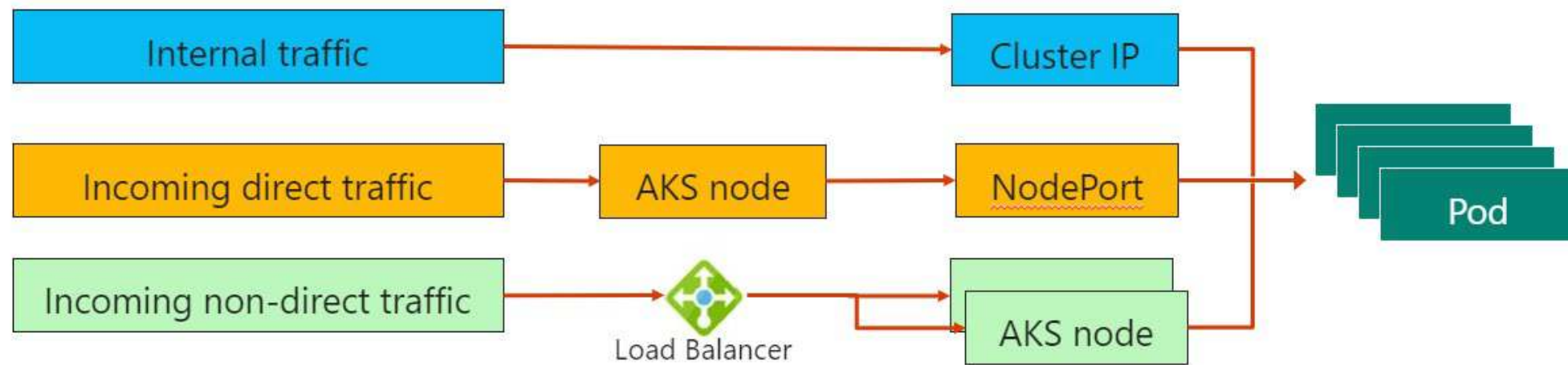
Manifest



AKS Architecture



AKS Networking



Cluster IP

NodePort

LoadBalancer

ExternalName

AKS Storage

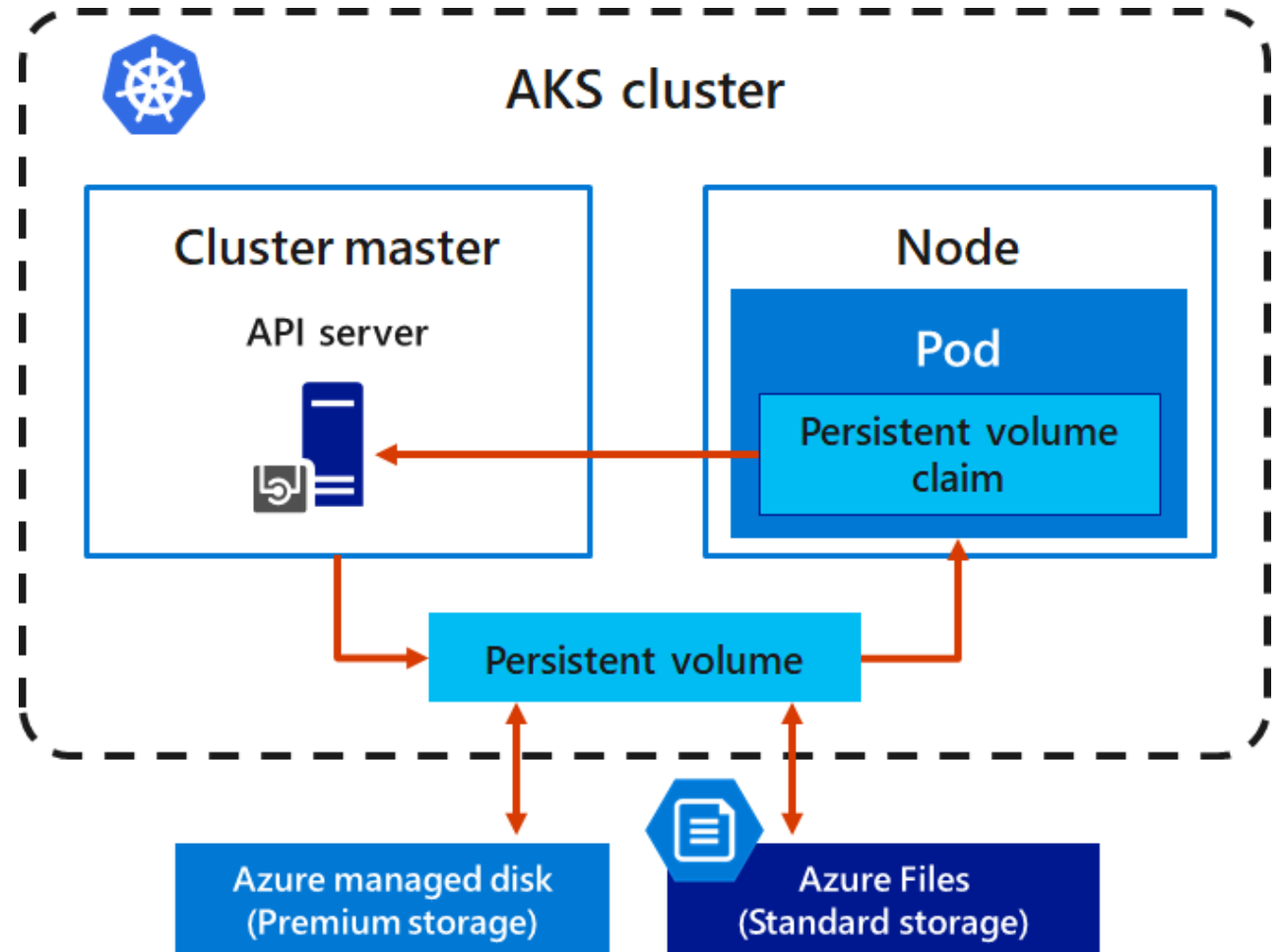


Local storage on the node is fast and simple to use

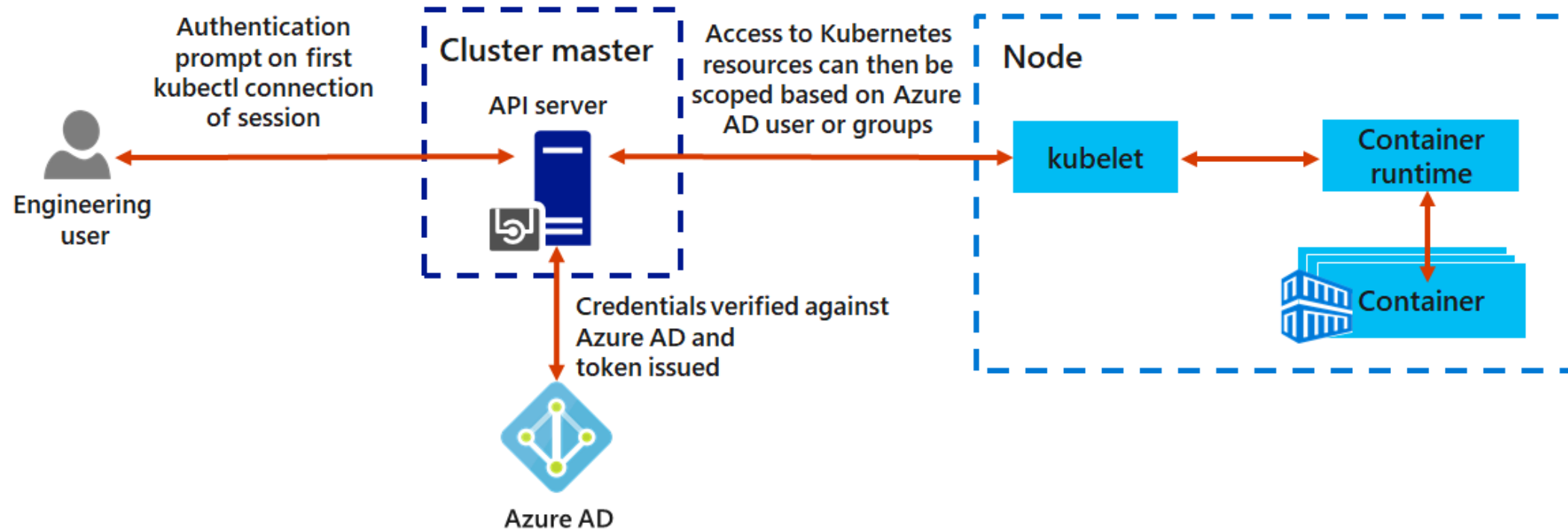
Local storage might not be available after the pod is deleted

Multiple pods may share data volumes

Storage could potentially be reattached to another pod

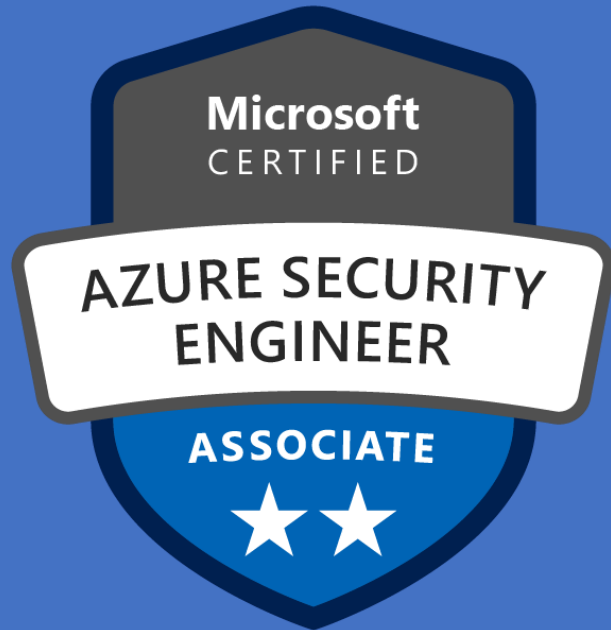


AKS and Azure Active Directory



Use Azure AD as an integrated identity solution

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



AZ-500

Episode 12

Module 02 Knowledge Check



Review Question 1



Which of the following two features of Azure networking provide the ability to redirect all Internet traffic back to your company's on-premises servers for packet inspection? Select two.

- ☒ User Defined Routes
- ☐ Cross-premises network connectivity
- ☐ Traffic Manager
- ☒ Forced Tunneling
- ☐ System Routes

Review Question 2



You are configuring Azure Firewall. You need to allow Windows Update network traffic through the firewall. Which of the following should you use?

- ☒ Application rules
- ☐ Destination inbound rules
- ☐ NAT rules
- ☐ Network rules

Review Question 3



You would like to limit outbound Internet traffic from a subnet. Which product should you install and configure?

- ☒ Azure Firewall
- ☐ Azure Web Application Firewall
- ☐ Load Balancer
- ☐ Sentinel

Review Question 4



Your organization has a web application and is concerned about attacks that flood the network layer with a substantial amount of seemingly legitimate traffic. What should you do?

- ☐ Add a Web Application Firewall
- ☐ Add an Azure Firewall
- ☒ Create a DDoS policy
- ☐ Create Network Security Group

Review Question 5



You are deploying the Azure Application Gateway and want to ensure incoming requests are checked for common security threats like cross-site scripting and crawlers. To address your concerns what should you do?

- ☐ Install an external load balancer
- ☐ Install an internal load balancer
- ☐ Install Azure Firewall
- ☒ Install the Web Application Firewall

Review Question 6



Which services below are features of Azure Application Gateway? Select three.

- ☐ Authentication
- ☒ Layer 7 load balancing
- ☒ Offloading of CPU intensive SSL terminations
- ☒ Round robin distribution of incoming traffic
- ☐ Vulnerability assessments

Review Question 7



You are configuring a Network Security Group. All the following are default rules, except?

- ☐ ~~Allow~~ all virtual networks inbound and outbound
- ☐ ~~Allow~~ Azure load balancer inbound
- ☒ Allow Internet inbound
- ☐ ~~Allow~~ Internet outbound

Review Question 8



Your organization has web servers in different regions and you want to optimize the availability of the servers. Which of the following is best suited for this purposed? Select one.

- ☐ Azure Application Gateway
- ☒ Azure Front Door
- ☐ Custom routing
- ☐ Web Application Firewall

Review Question 9



Your organization has a security policy that prohibits exposing SSH ports to the outside world. You need to connect to an Azure Linux virtual machine to install software. What should you do? Select one.

- ☒ **Configure the Bastion service**
- ☐ **Configure a Guest configuration on the virtual machine**
- ☐ **Create a custom script extension**
- ☐ **Work offline and then reimage the virtual machine.**

Review Question 10



What type of disk encryption is used for Linux disks?

☐ Bitlocker

☒ DM-Crypt

☐ FileVault

☐ FastPass

☐ Veracrypt

Review Question 11



You need to ensure your virtual machines are kept up to date with security patches. Update Management includes all of the following except? Select one.

- ☐ Azure Automation uses runbooks to install updates.
- ☐ The Microsoft Monitoring Agent must be installed for both Windows and Linux virtual machines.
- ☐ Update Management is available at no additional cost (except log data storage).
- ☒ Update Management only pertains to cloud deployed virtual machines.

Review Question 12



Which of the following is not a High severity Security Center recommendation for virtual machines and servers? Select one.

- ☐ Disk encryption should be applied on virtual machines
- ☒ Install endpoint protection solution on virtual machines
- ☐ System updates should be installed on your machines.
- ☐ OS version should be updated for your cloud service roles.

Review Question 13



Privileged access workstations provide all the following, except? Select one.

- ☒ **Protects against attackers who have gained administrative access.**
- ☐ **Protects against phishing attacks, various impersonation attacks, and credential theft attacks such as keystroke logging.**
- ☐ **Protects high impact IT administrative roles and tasks.**
- ☐ **Protects highly sensitive information worker tasks.**

Review Question 14



To interact with Azure APIs, an Azure Kubernetes Service (AKS) cluster requires which of following? Select two.

- ☐ AKS contributor
- ☒ Azure AD service principal
- ☐ Global Administrator permissions
- ☒ Managed identity

Review Question 15



You are using Azure Kubernetes Service (AKS) and need to control the flow of traffic between pods and block traffic directly to the backend application. What should you do? Select one.

- ☒ Create a AKS network policy
- ☐ Create an application gateway
- ☐ Create a Azure firewall
- ☐ Create a network security group

Review Question 16



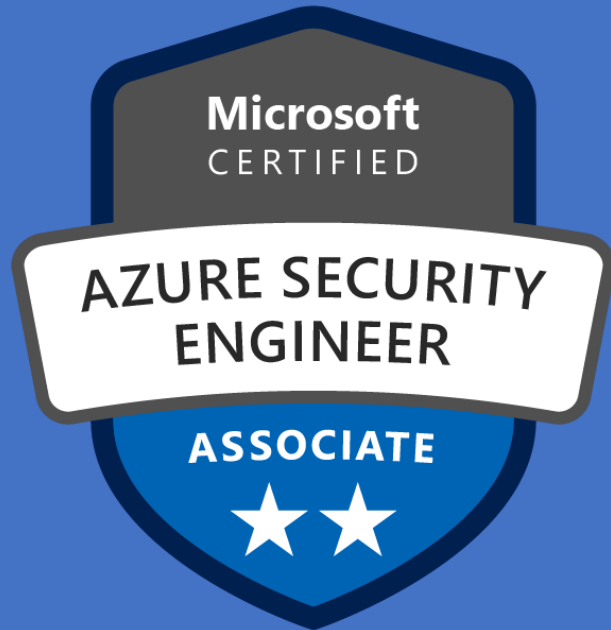
You are defining RBAC rules for the Azure Kubernetes security team. You need to grant permissions across the entire cluster. Which two items would you define? Select two.

☒ ClusterRoles

☒ ClusterRoleBindings

☐ Roles

☐ RoleBindings



AZ-500

Episode 13

Azure Key Vault





Azure Key Vault Lesson Objectives



Azure Key Vault Features



Key Vault Access



Key Vault Example



Key Vault Certificates



Key Vault Keys



Customer Managed Keys



Key Vault Secrets



Key Rotation

Azure Key Vault



Secrets Management

Key Management

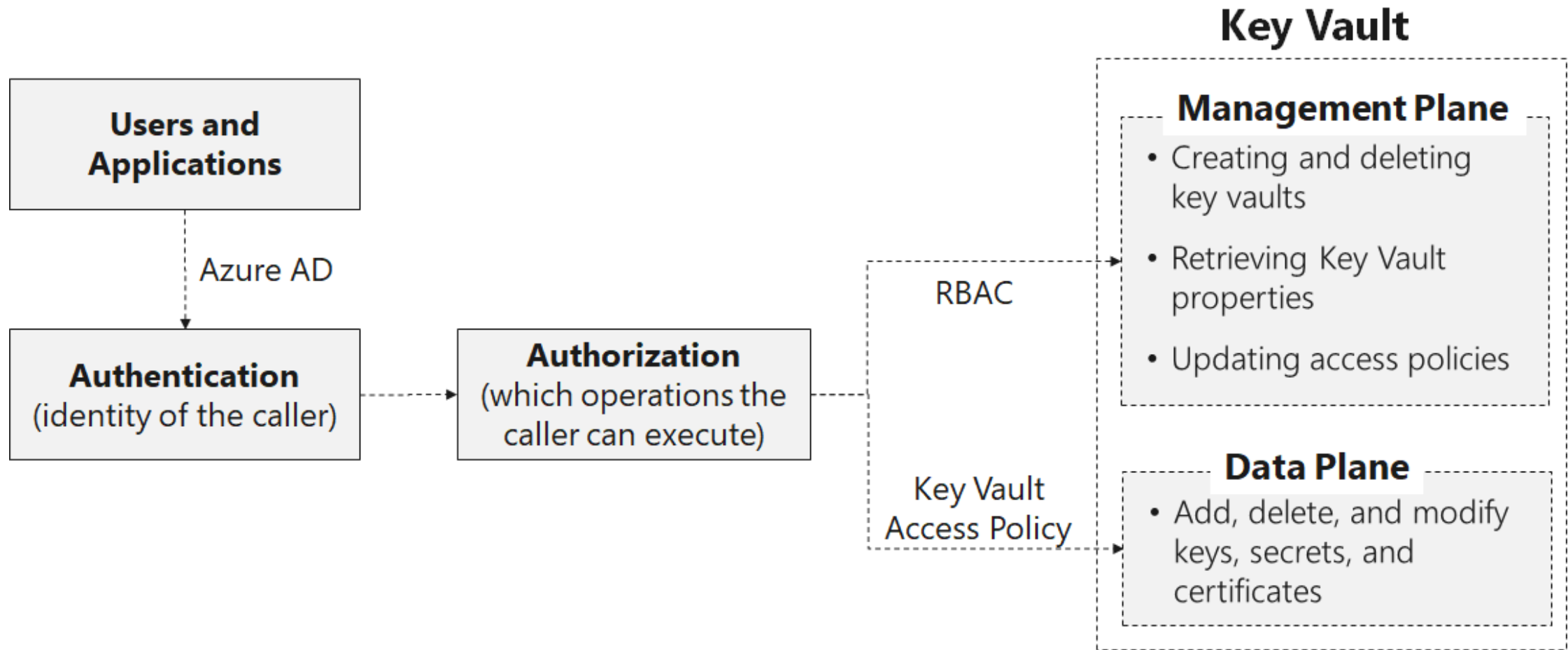
Certificate Management

Store secrets backed by HSMs



Safeguard cryptographic keys and secrets that cloud applications and services use

Key Vault Access



Key Vault Example



SSL certificate for SSL

**Storage key for access
the Storage account**

**RSA 2,048-bit key for
sign in operations**

**Bootstrap certificate for
authentication to Azure
AD**



Role	Management Plane	Data plane
Security team	Key Vault Contributor	Keys: backup, create, delete, get, import, list, restore Secrets: all operations
Developers and operators	Key Vault deploy permission	None
Auditors	None	Keys: list Secrets: list
Application	None	Keys: sign Secrets: get

Key Vault Certificates



Manages X509 v3 certificates (PFX, PEM)

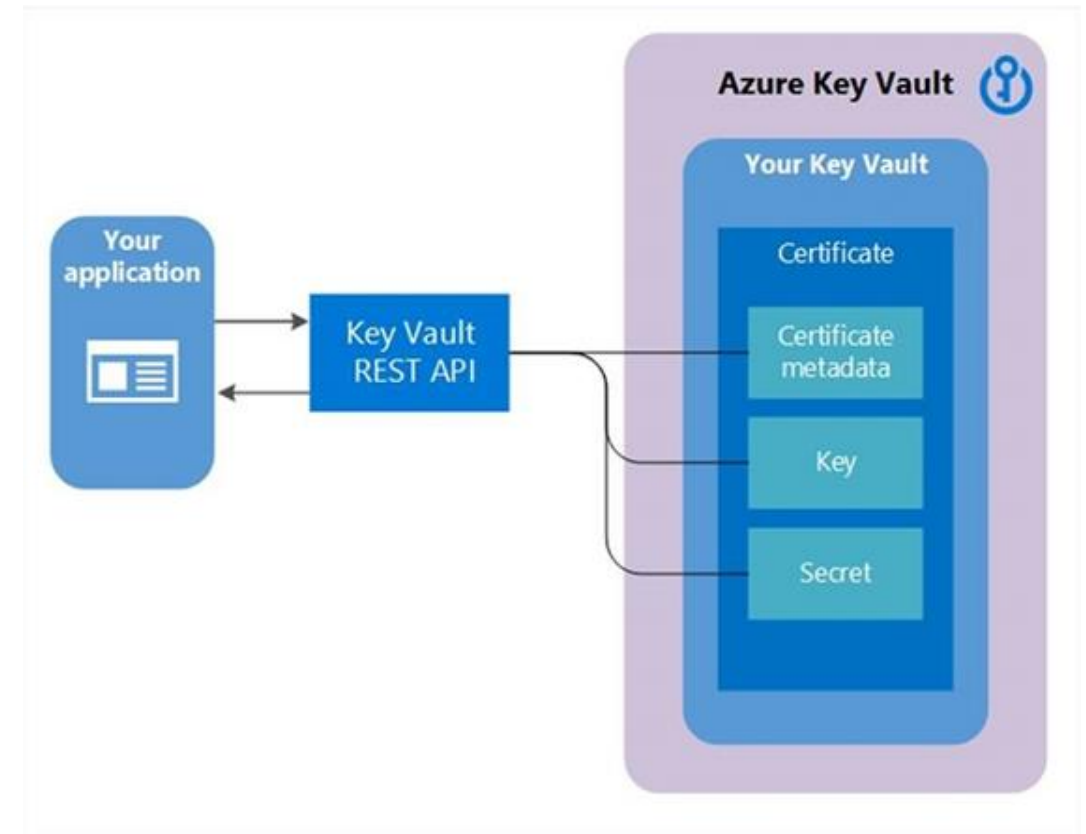
Created by the Key Vault or by import

Self-signed and Certificate Authority certificates

Lifecycle management including automatic renewal and contact notification

Minimum 2048-bit encryption

RSA or RSA HSM with certificates



Key Vault Keys



Soft Keys

Hard Keys

Supports operations
like create, delete,
update, and list

Key permissions

2 selected ^

☒ Select all

Key Management Operations

☒ Get

☒ List

☐ Update

☐ Create

☐ Import

☐ Delete

☐ Recover

☐ Backup

☐ Restore

Cryptographic Operations

☐ Decrypt

☐ Encrypt

☐ Unwrap Key

☐ Wrap Key

☐ Verify

☐ Sign

Privileged Key Operations

☐ Purge

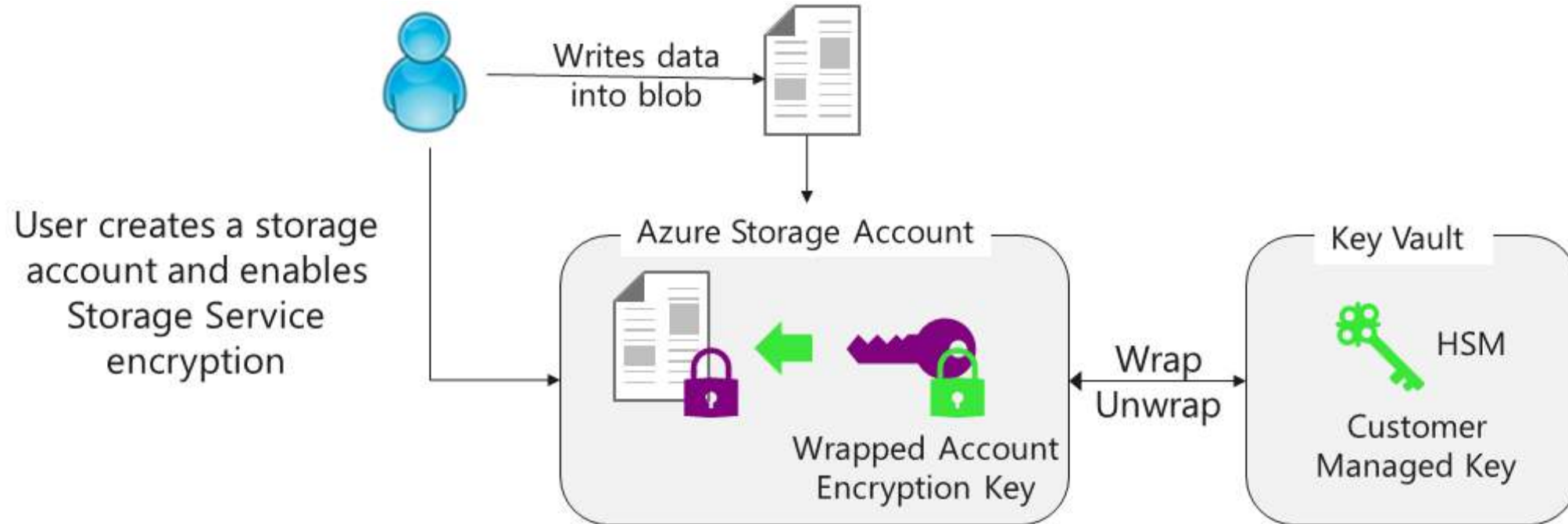
Supports
cryptographic
operations

Sign and Verify

Key encryption/wrapping

Encrypt and Decrypt

Customer Managed Keys



Update keys and secrets without affecting applications

Updates can be manual, programmatic, or automated

Key Vault Secrets



Name-value pair

Name must be unique in the vault

Value can be any UTF-8 string – max 25 KB in size

Manual or certificate creation

Home > Key vaults > AZ500DemoKeyVault | Secrets > Create a secret

Create a secret

Upload options

Manual ▼

Upload options

Manual ^

Manual

Certificate

Name * ⓘ

Value * ⓘ

Enter the secret.

Content type (optional)

Set activation date? ⓘ ☐

Set expiration date? ⓘ ☐

Enabled? Yes No

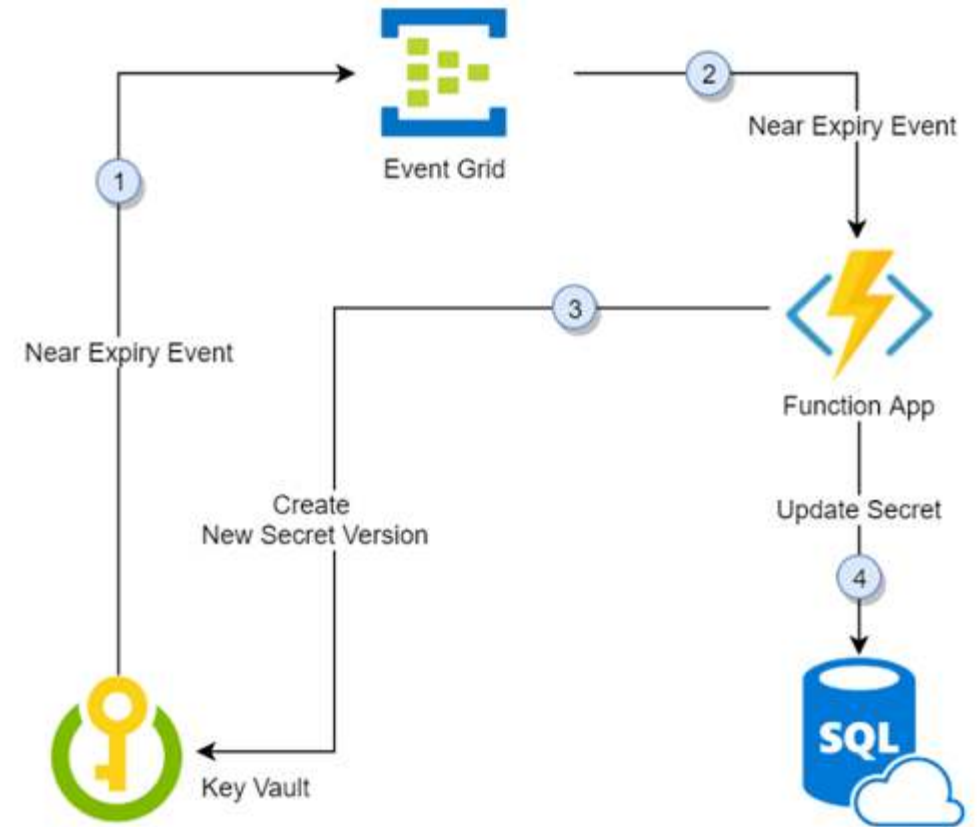
Key and Secret Rotation

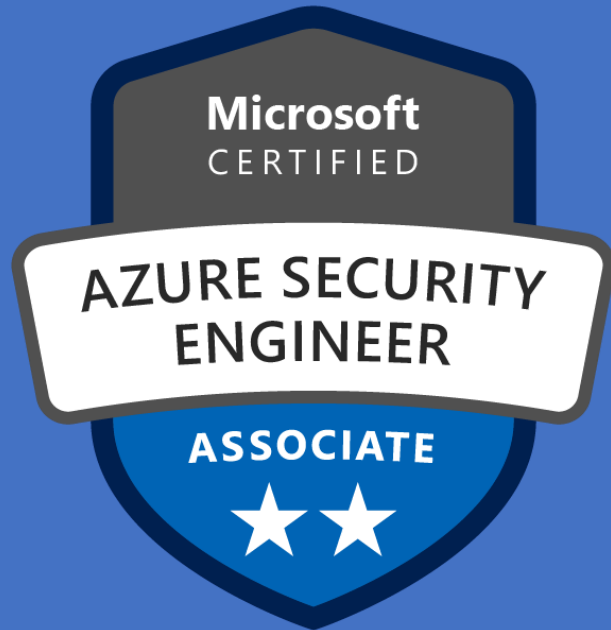


Update keys and secrets without affecting your application

Rotate keys and secrets in several ways:

- As part of a manual process
- Programmatically with the REST API
- With an Azure Automation script





AZ-500

Episode 14

Application Security





Application Security Lesson Objectives



Microsoft Identity Platform



Azure AD Application Scenarios



App Registration



Microsoft Graph Permissions



Managed Identities



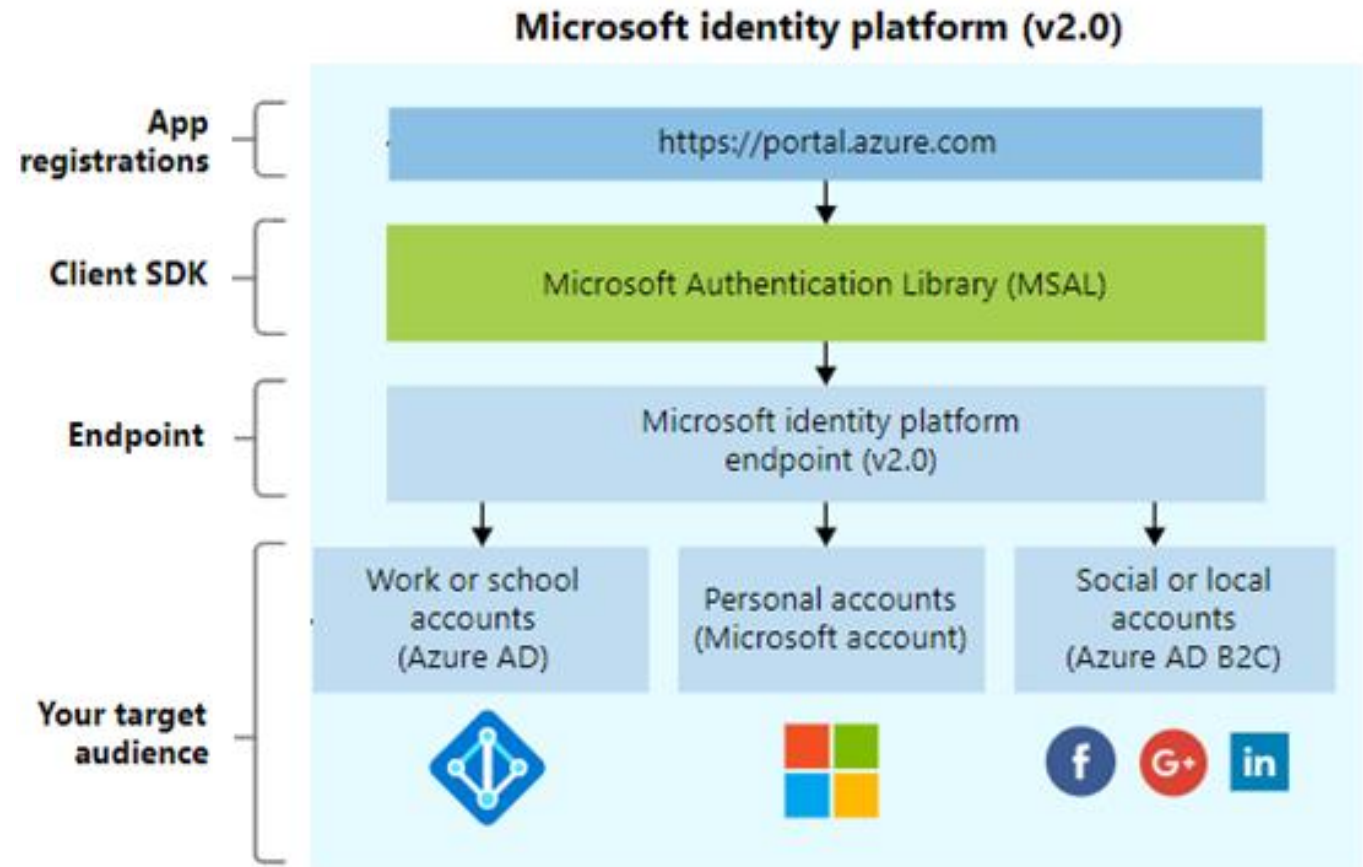
Web App Certificates

Microsoft Identity Platform



**Write code once and
authenticate any Microsoft
identity into your
application**

**Use the Microsoft Graph
API for programmatic
application configuration**



Azure AD Application Scenarios



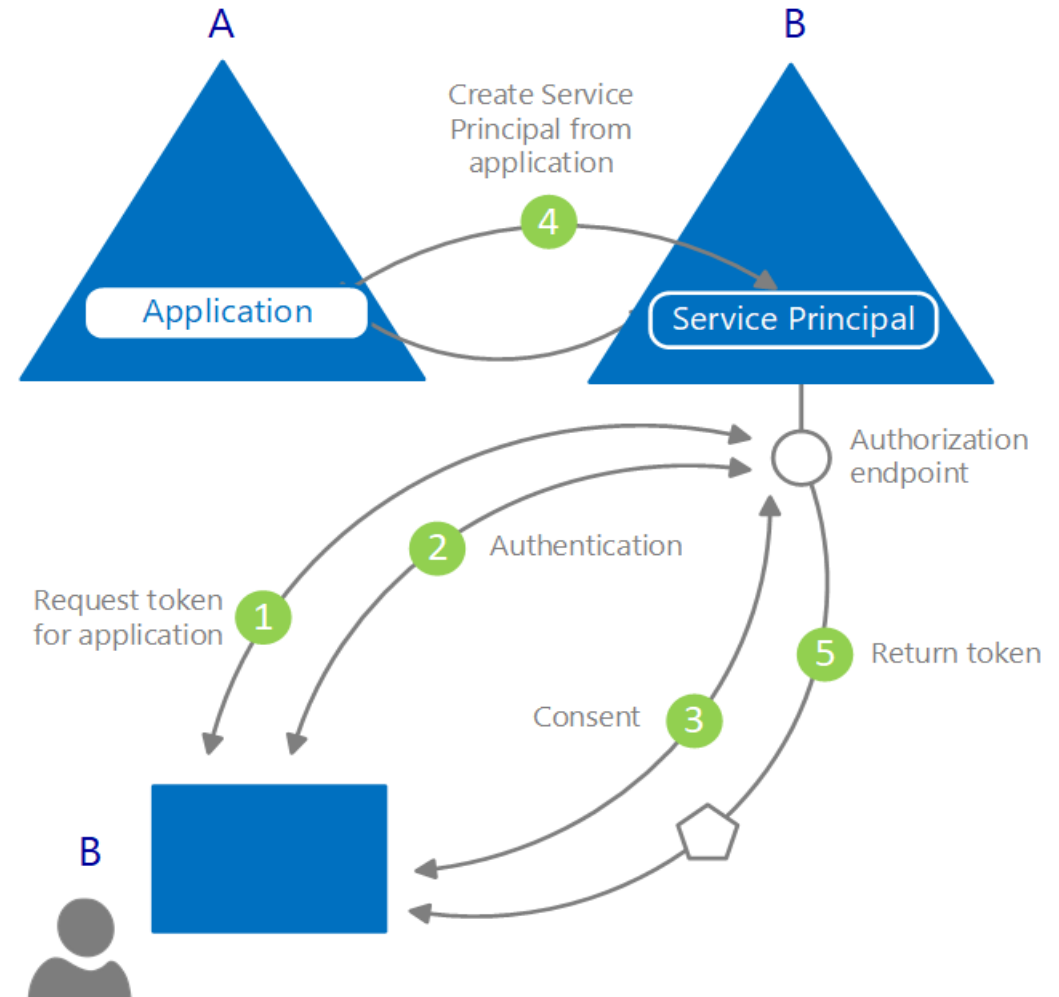
Single page frontends that run in a browser

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

Home > App registrations > Register an application

Register an application

PREVIEW

*** Name**

The user-facing display name for this application (this can be changed later).

ContosoApp_1 ✓

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Contoso Enterprises)

☐ Accounts in any organizational directory

☐ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URL after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ▼ https://contosoapp1/auth ✓

Register

Microsoft Graph Permissions



Delegated Permissions

Application Permissions

Request API permissions

Select an API

Microsoft APIs

APIs my organization uses

My APIs

Commonly used Microsoft APIs



Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud



Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets



Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions



Azure Data Explorer (with Multifactor Authentication)

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions



Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults



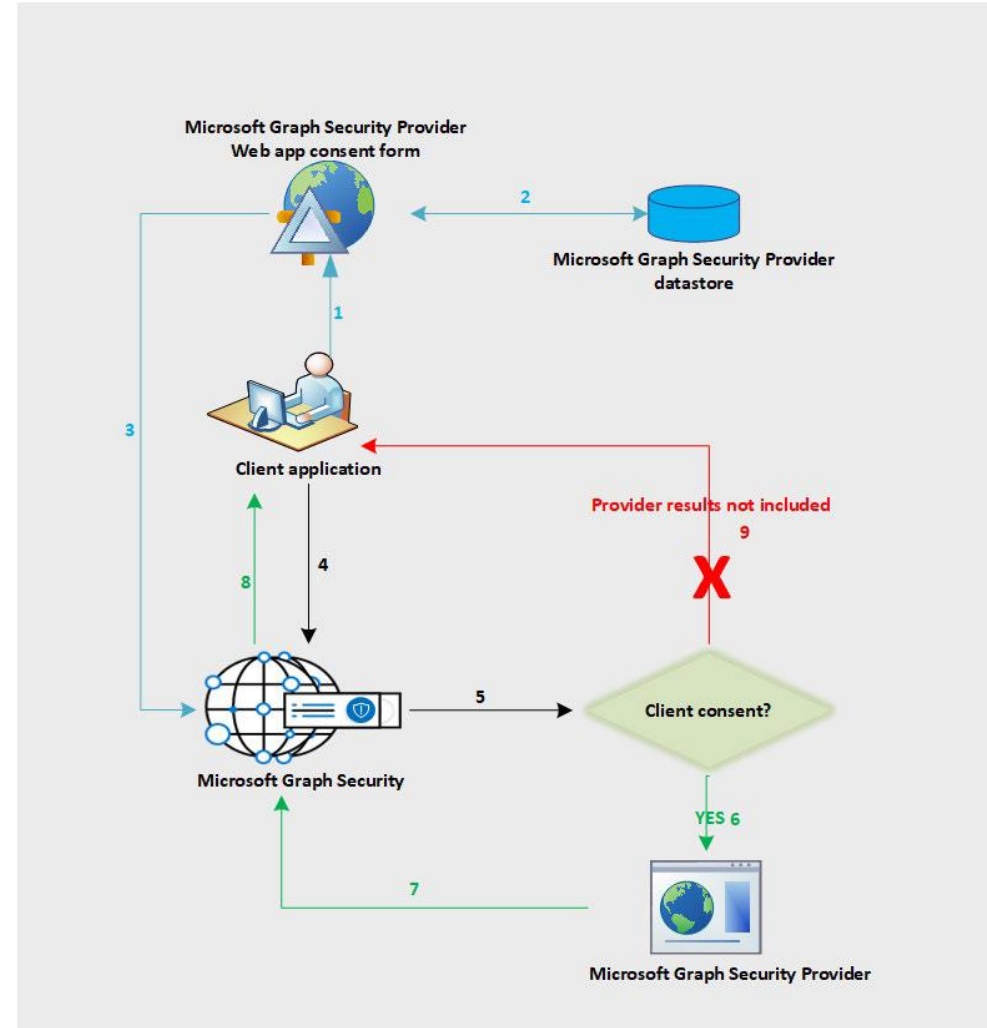
Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

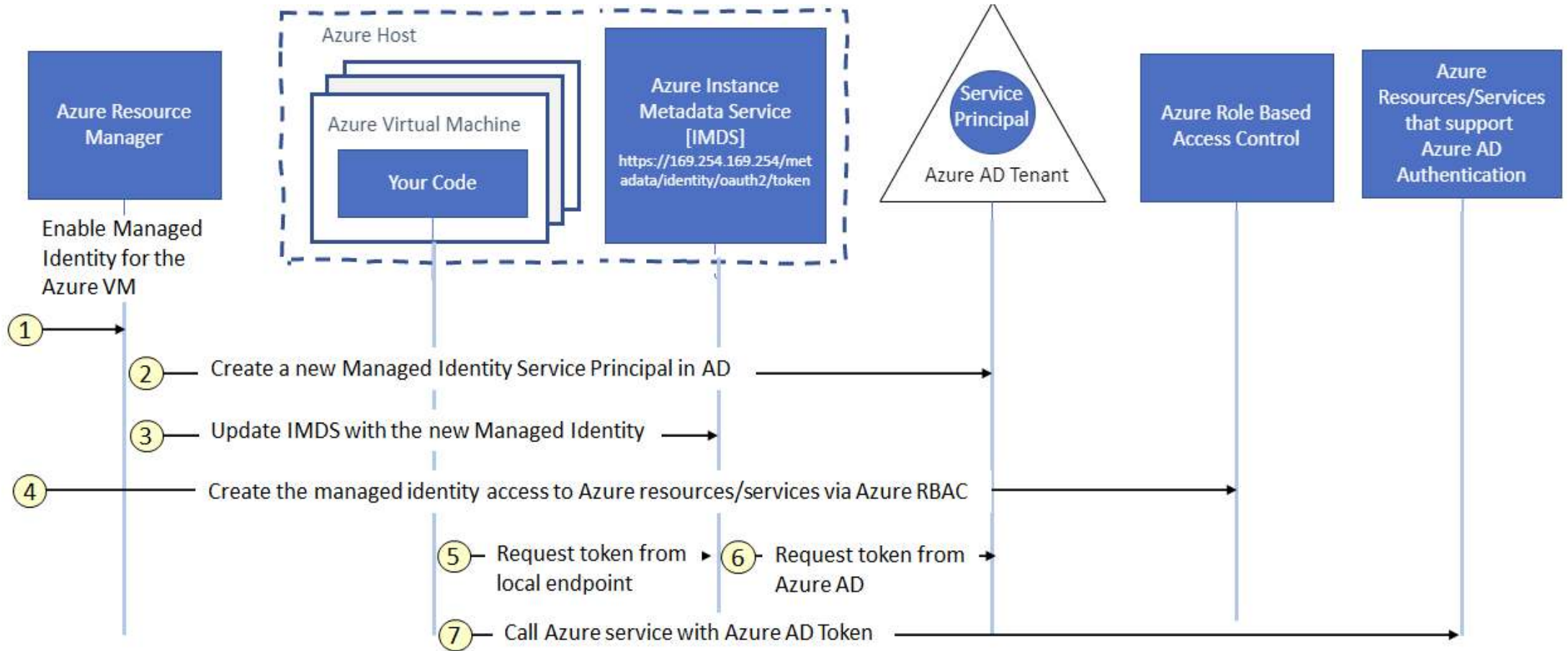
Microsoft Graph API



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



Managed Identities



Web App Certificates



Enable require incoming certificate

Basic app plan tier or above

Requires HTTPS

Private or public certificates

Allow anonymous access with an exclusion path

 **HumanResources | TLS/SSL settings**
App Service

Bindings Private Key Certificates (.pfx) Public Key Certificates (.cer)

 **Protocol Settings**

Protocol settings are global and apply to all bindings defined by your app.

HTTPS Only: ⓘ Off On

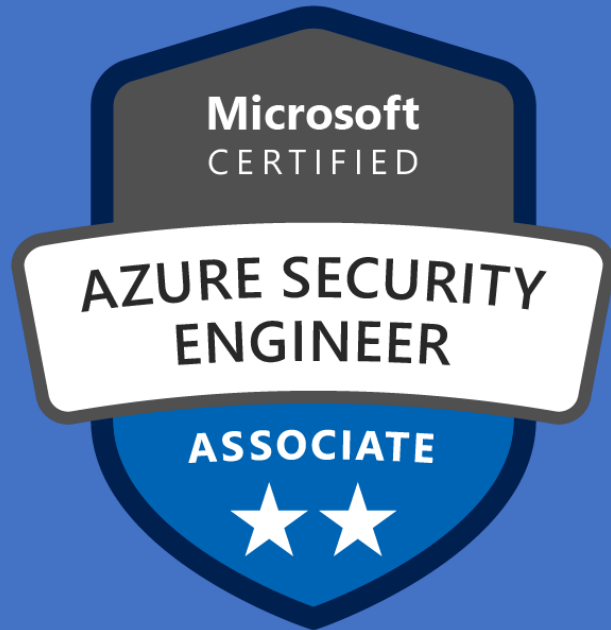
Minimum TLS Version ⓘ 1.0 1.1 1.2

 **TLS/SSL bindings**

Bindings let you specify which certificate to use when responding to requests to a specific hostname over HTTPS. TLS/SSL Binding requires valid private certificate (.pfx) issued for the specific hostname.

+ Add TLS/SSL Binding

☐ Host name	Private Certificate Thumbprint	TLS/SSL Type
No TLS/SSL bindings configured		



AZ-500

Episode 15

Storage Security





Storage Security Lesson Objectives



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



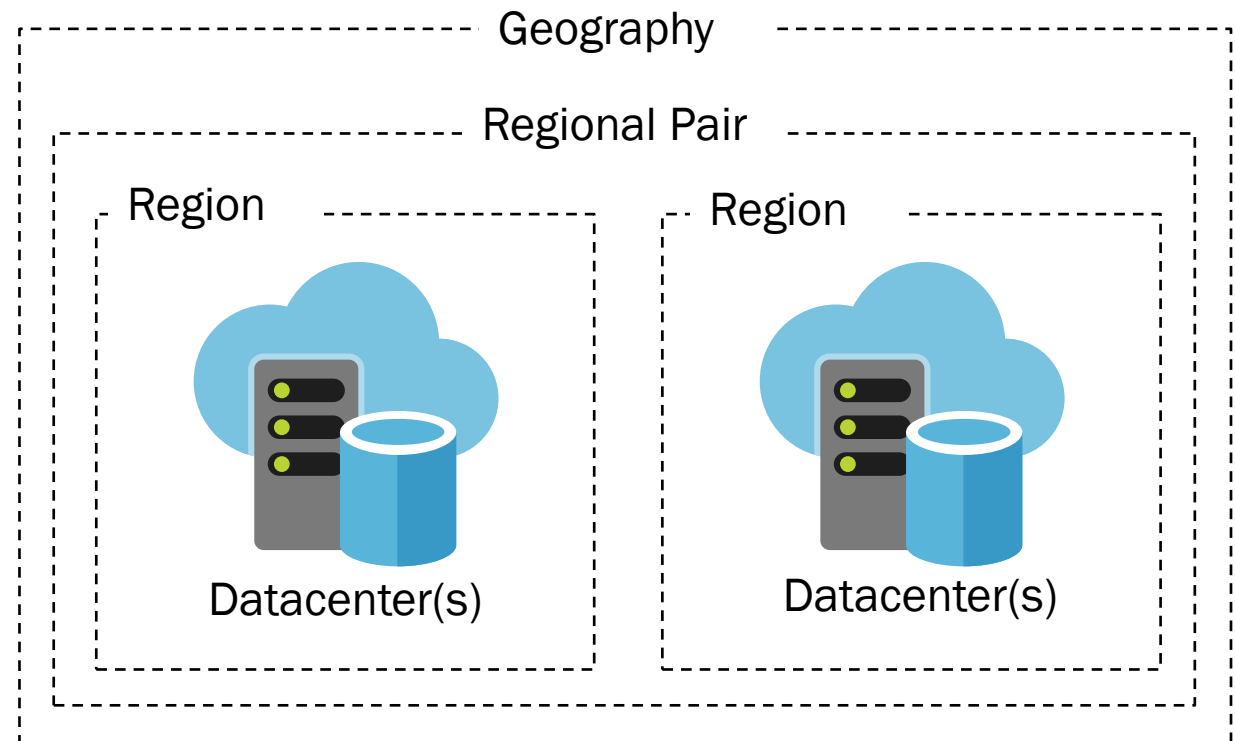
Physical isolation

Platform-provided replication

Region recovery order

Sequential updates

Data residency



Azure Storage Access



Storage	Storage Account Shared Key	Shared access signature	Azure Active Directory	Active Directory (preview)	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

Configure permissions, start/expiry times, IP addresses, and allowed protocols

www.AGuideToCloud.com

Azure AD Storage Authentication

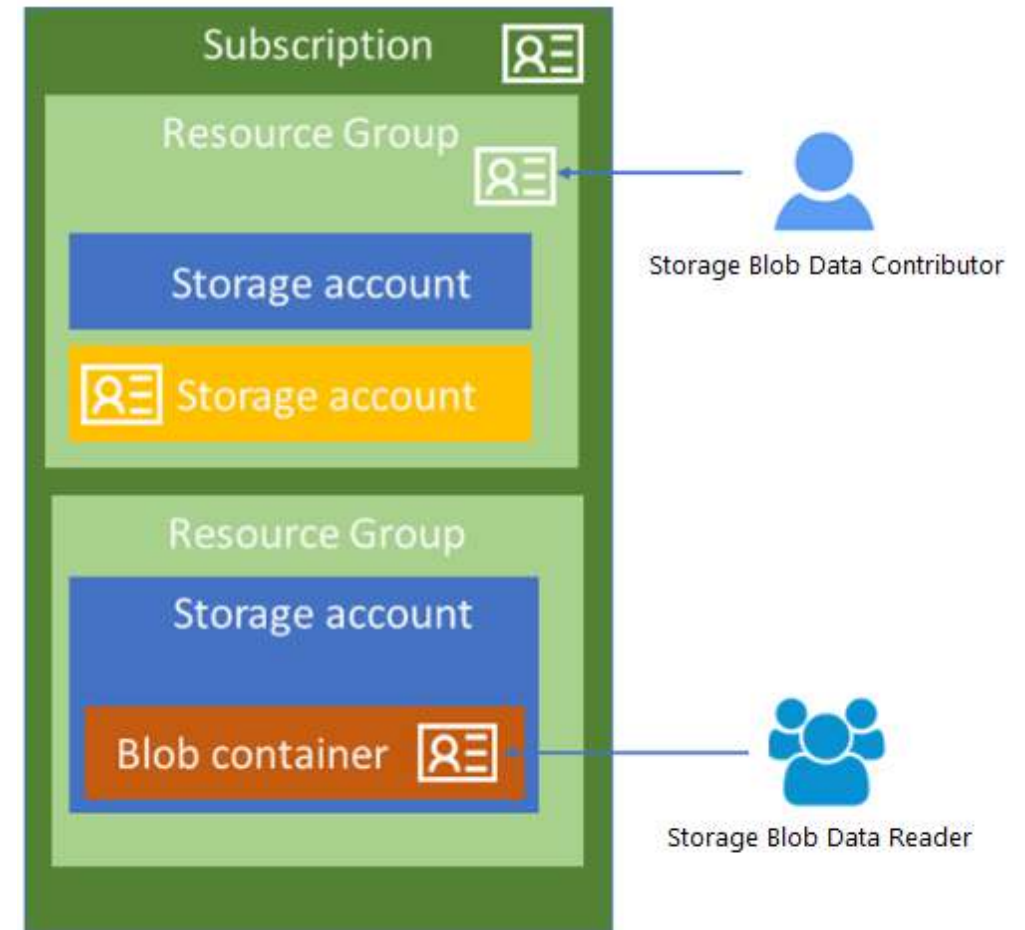


Available for Blob and Queue storage

Several built-in roles including Data Owner, Data Contributor, and Data Reader

Two-step process: authentication (token returned) and then authorization

Scope from Management Group down to individual blob or queue



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

Encryption

 Save  Discard

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

By default, data in the storage account is encrypted using Microsoft Managed Keys. You may choose to bring your own key.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process.

[Learn More about Azure Storage Encryption](#) 

Encryption type

- ☒ Microsoft Managed Keys
☐ Customer Managed Keys

Blob Data Retention Policies



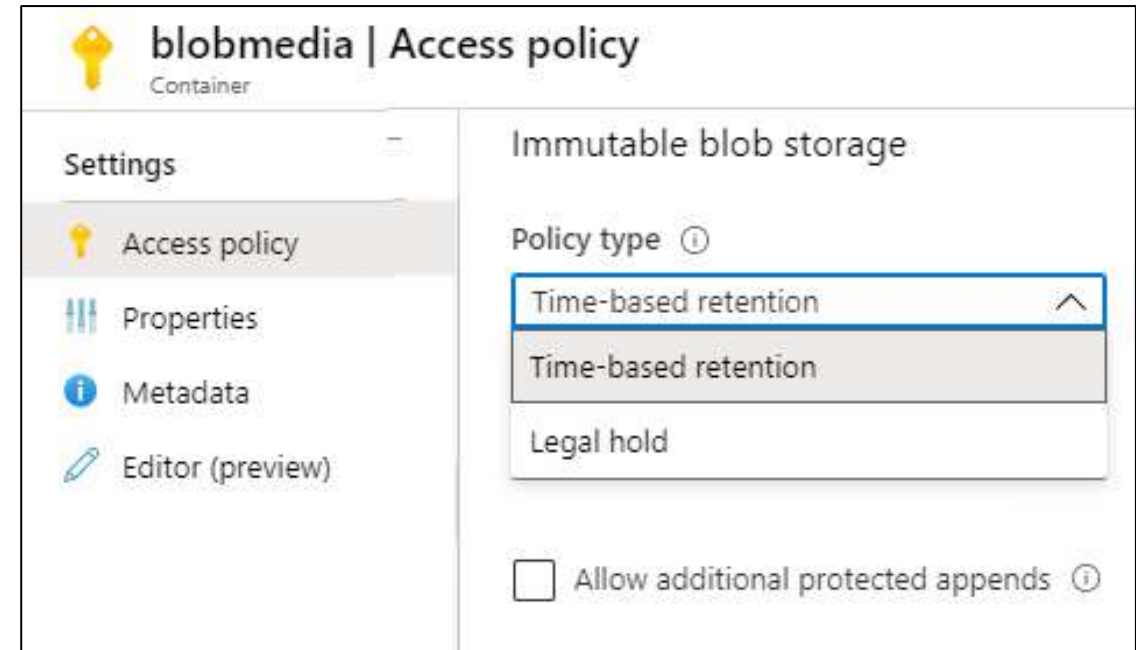
Data recovery and disposal rules

Time-based retention for a specified interval (days)

Legal-hold retention based on tags – no editing or deleting of the content

Container policies apply to all existing and new content

Supports audit logging



Azure Files Authentication

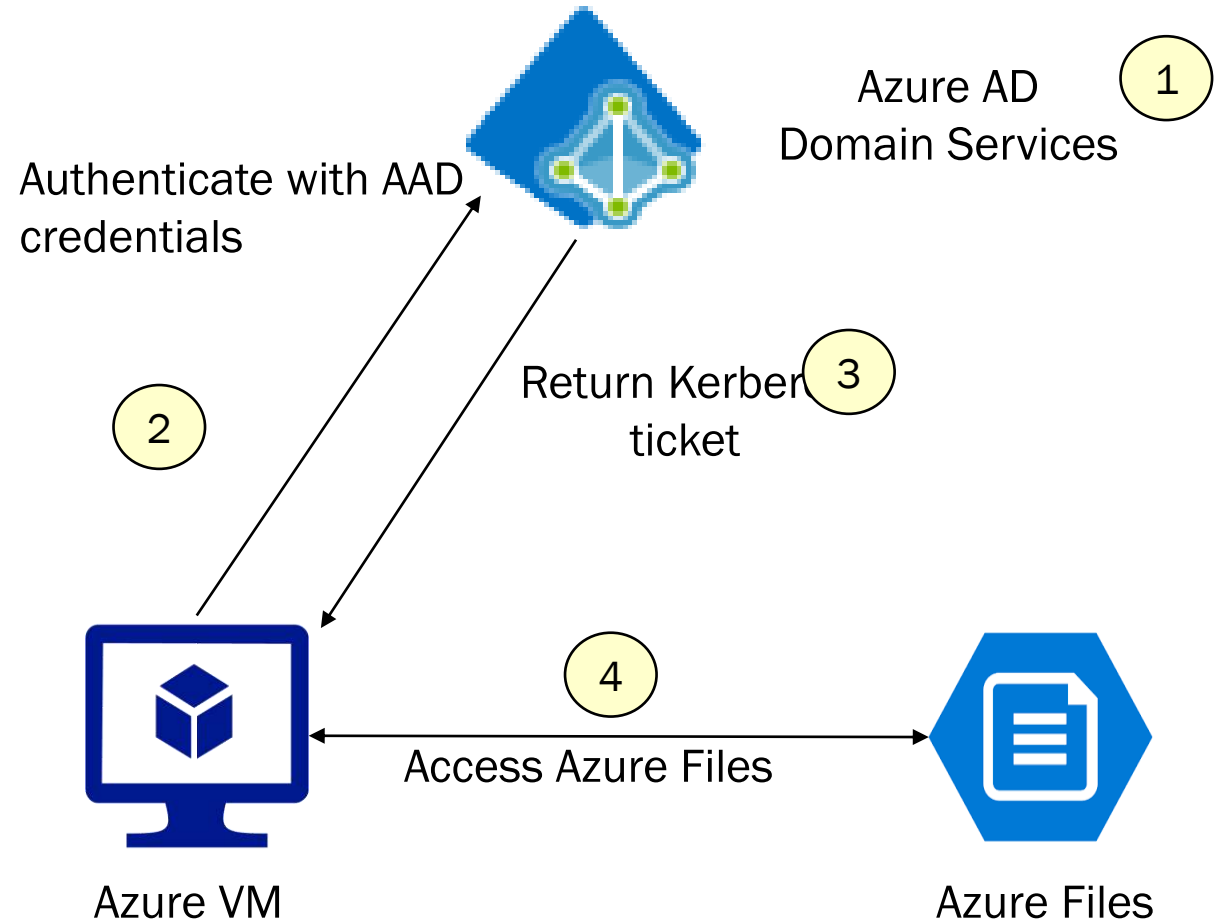


Enable identity-based authentication

Use Azure AD DS or on-premises AD DS (preview)

Use RBAC roles to assign access rights to the file shares

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



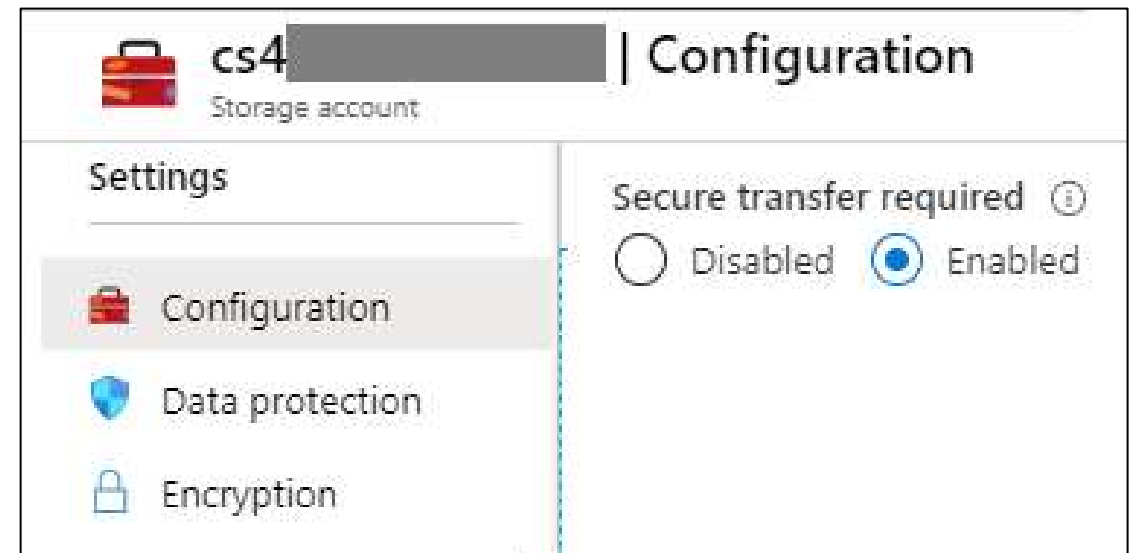
Secure Transfer Required

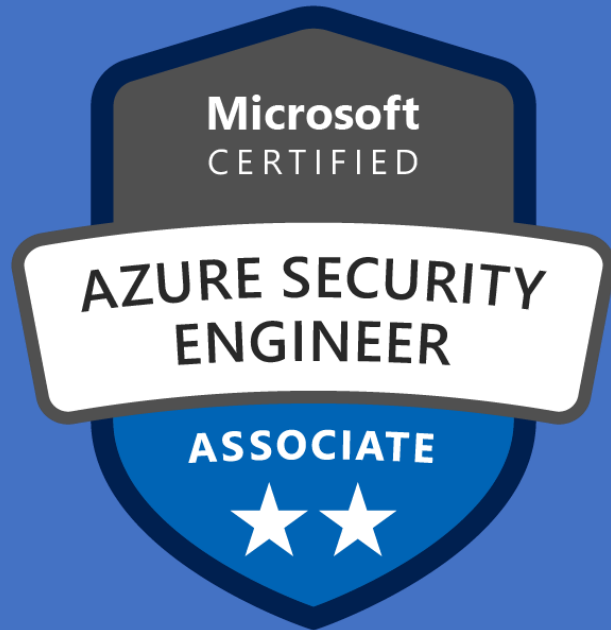


Storage account connections must be secure (HTTPS)

HTTPS for custom domain names not supported

Azure Files connections require encryption (SMB)





AZ-500

Episode 16

Database Security





Database Security Lesson Objectives



Data Sovereignty



SQL Database Authentication



SQL Database Firewalls



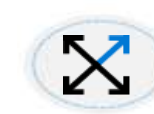
Database Auditing



Data Discovery and Classification



Vulnerability Assessment



Advanced Threat Protection



Dynamic Data Masking



Transparent Data Encryption



Always Encrypted

SQL Database Authentication

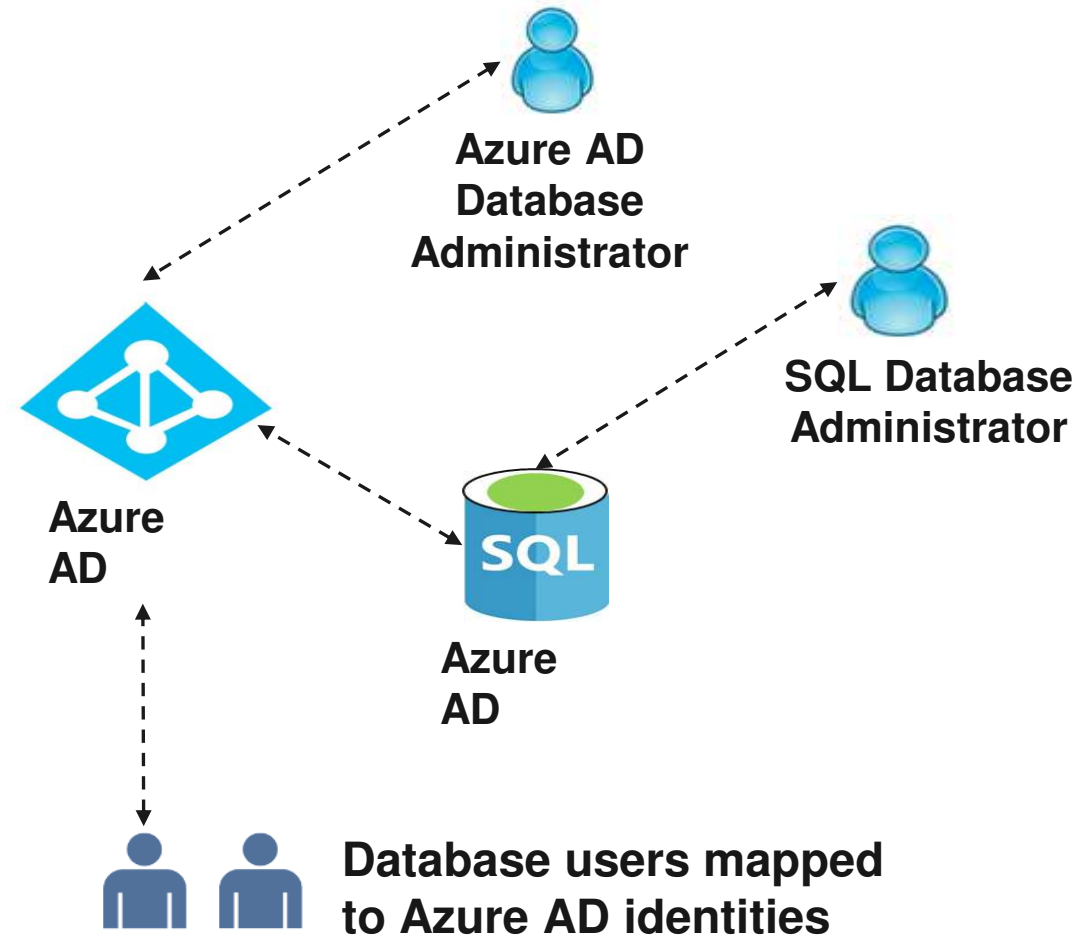


An alternative to SQL Server authentication

Helps stop the proliferation of user identities across database servers

Allows password rotation in a single place

Customers can manage database permissions using external (Azure AD) groups



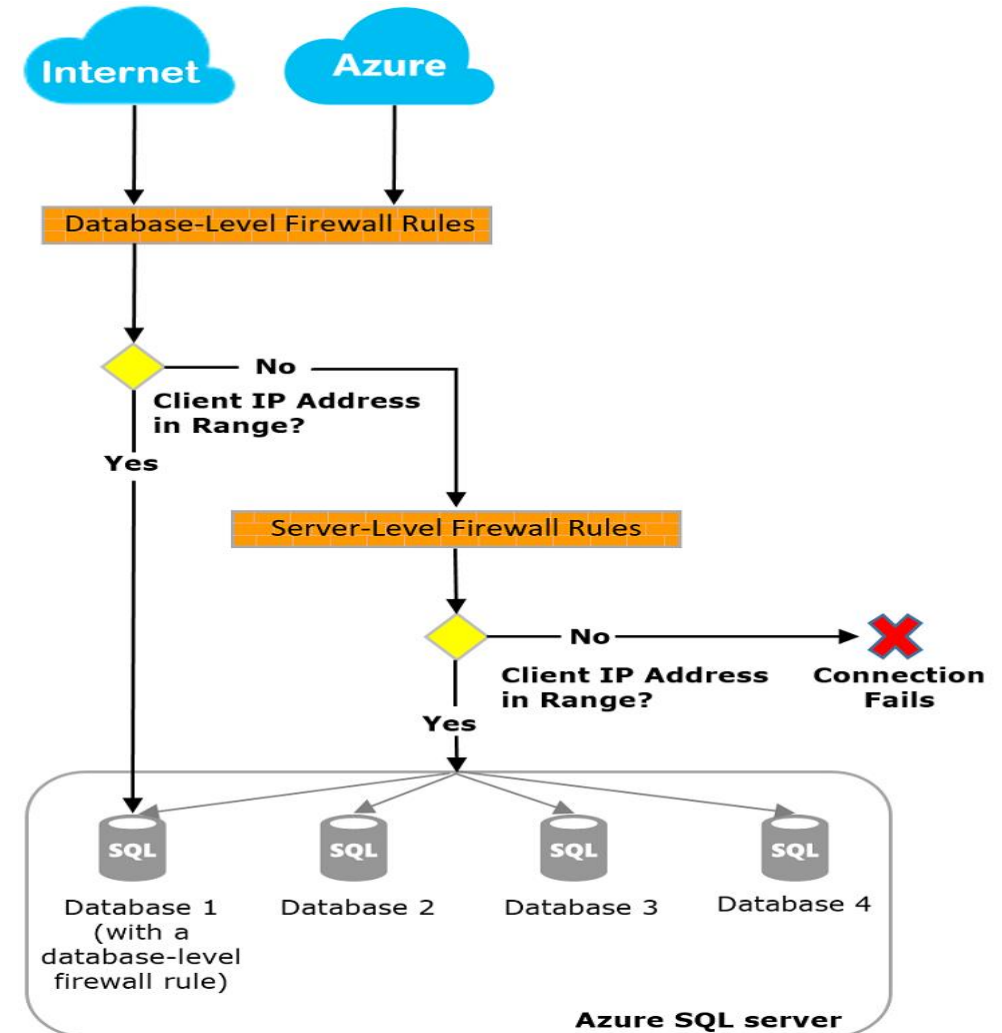
SQL Database Firewalls



1. By default, firewall denies all access

2. Database-level firewall rules add allowed client IP addresses and/or all Azure services and resources

3. Server-level firewall rules are added programmatically – subnet of the database level clients



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

ads- [redacted] | Auditing
SQL database

[View server settings](#)

Server-level Auditing: **Disabled**

Auditing ⁱ

ON OFF

Audit log destination (choose at least one):

☒ Storage

Storage details ⁱ >

Configure

☐ Log Analytics (Preview)

☐ Event Hub (Preview)

*Storage account >

adsstorageaccount

Retention (Days) ⁱ

60

Storage access key ⁱ

Primary Secondary

Data Discovery and Classification

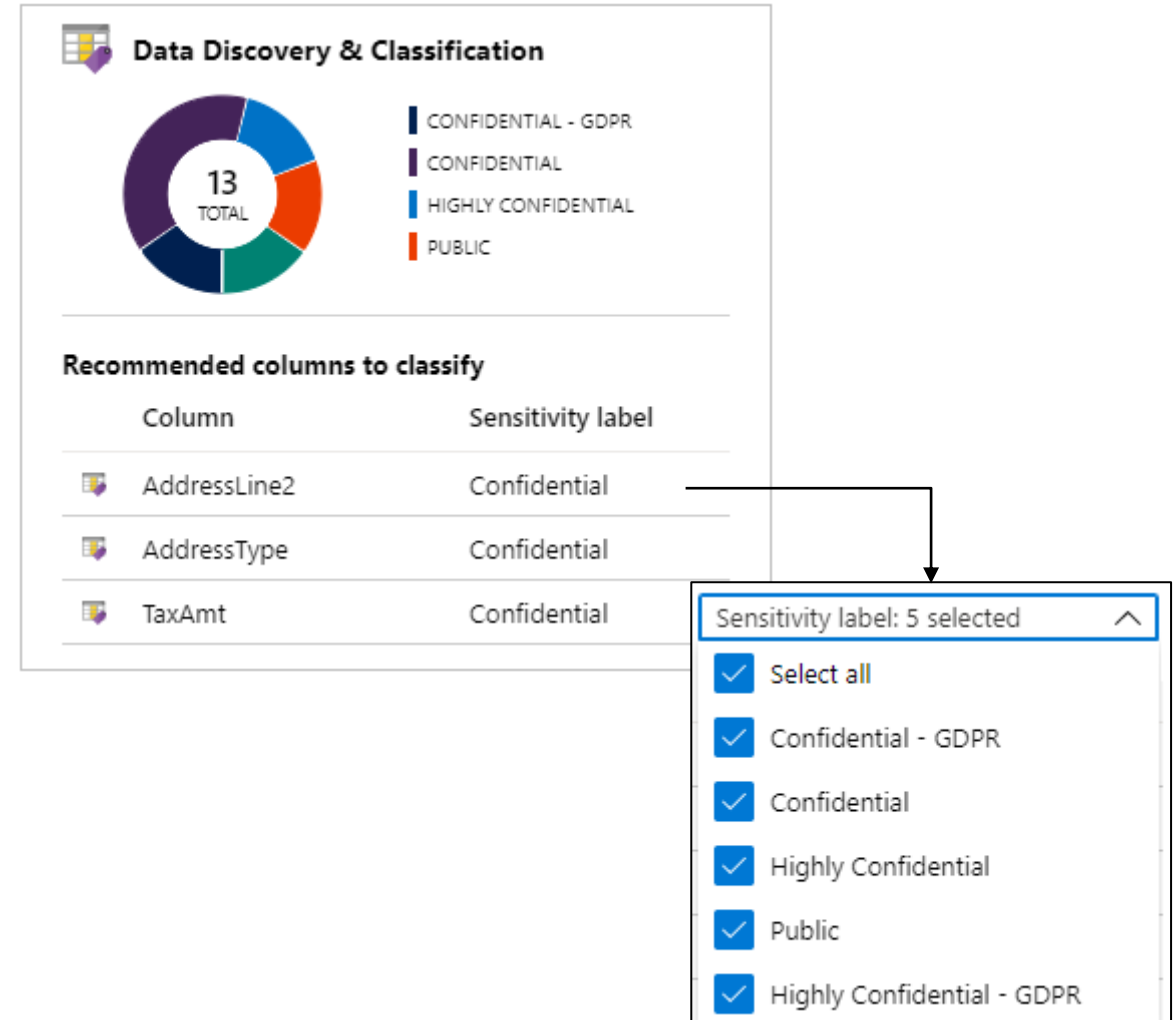


Built-in to Azure SQL Database

Scans your database and identifies columns that contain potentially sensitive data

Provides classification recommendations and reports

Let's you apply sensitivity-classification labels



Vulnerability Assessment



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

 Scan	 Export Scan Results	 Scan History	 Settings	 Feedback
Total failing checks 6  Total passing checks 42  Risk summary High Risk 2  Medium Risk 3  Low Risk 1 				
Failed (6)		Passed (42)		
ID 	SECURITY CHECK			
VA2108	Minimal set of principals should be members of fixed high impact database roles			
VA20...	Server-level firewall rules should be tracked and maintained at a strict minimum			
VA10...	Excessive permissions should not be granted to PUBLIC role			
VA1281	All memberships for user-defined roles should be intended			
VA1288	Sensitive data columns should be classified			
VA1282	Orphan roles should be removed			

Advanced Threat Protection



Vulnerability to SQL injection

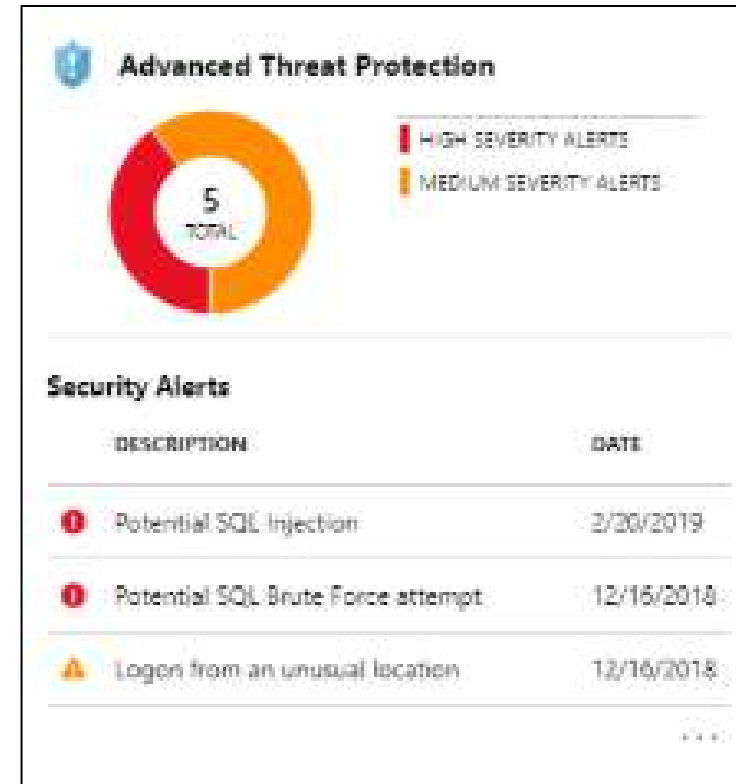
Potential SQL injection

Access from unusual location

Access from unusual location

Access from harmful application

Brute force SQL credentials



Integrated with Azure Security Center to detect and respond to potential threats as they occur

Dynamic Data Masking



Dynamic Data Masking
SQL database

Recommended fields to mask

Schema	Table	Column	
SalesLT	Customer	FirstName	<button>Add mask</button>
SalesLT	Customer	LastName	<button>Add mask</button>
SalesLT	Customer	EmailAddress	<button>Add mask</button>
SalesLT	Customer	Phone	<button>Add mask</button>

Masking field format

- Default value (0, xxxx, 01-01-1900)
- Default value (0, xxxx, 01-01-1900)
- Credit card value (xxxx-xxxx-xxxx-1234)
- Email (aXXX@XXXX.com)
- Number (random number range)
- Custom string (prefix [padding] suffix)

Masking Field Format

Custom text

Exposed Prefix	Padding String	Exposed Suffix
3	X*X*X	2

Masks sensitive data for non-privileged users

Administrators are excluded; you can add others

Rules apply the masking logic; several formats are available

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

 **ads-server | Transparent data encryption**
SQL server

Transparent data encryption

Transparent data encryption encrypts your databases, backups, and logs at rest without any changes to your application. To enable encryption, go to each database.

Transparent data encryption ⓘ ☒ **Service-managed key** ☐ Customer-managed key

OR

Transparent data encryption ⓘ ☐ Service-managed key ☒ **Customer-managed key**

Key selection method ☒ **Select a key** ☐ Enter a key identifier

Key vault *

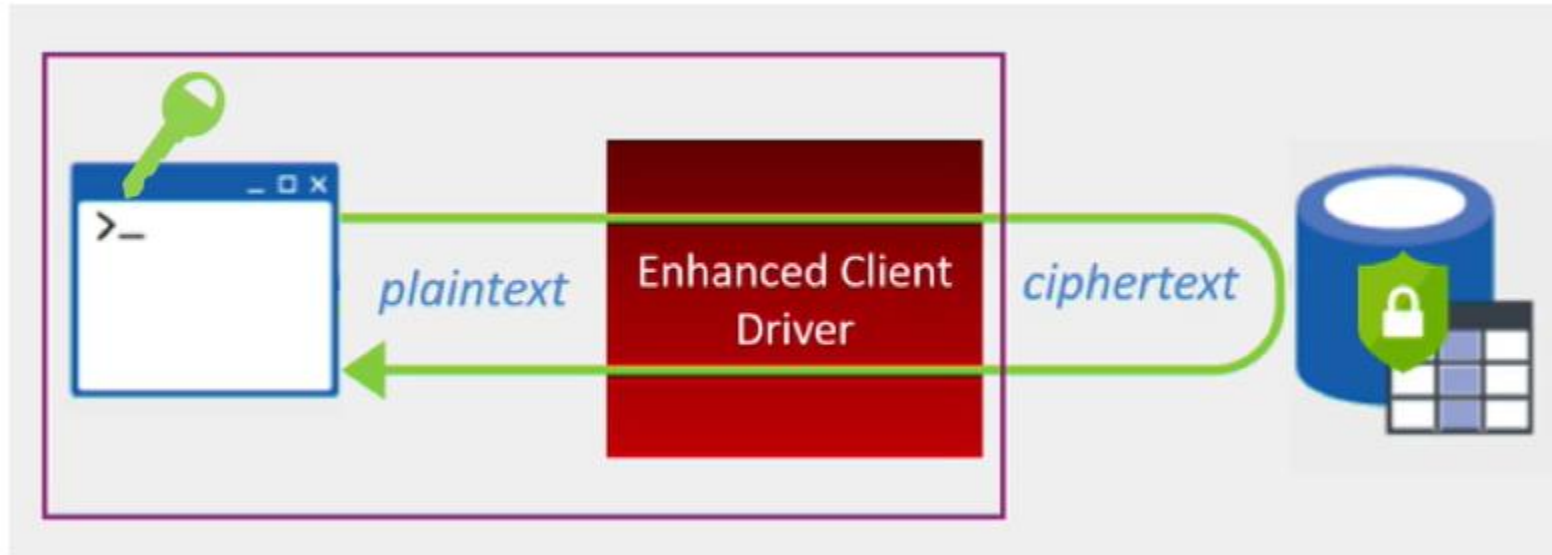
Select a key vault
[Change key vault](#)

Key *

Select a key
[Change key](#)

☒ Make the selected key the default TDE protector.

Always Encrypted



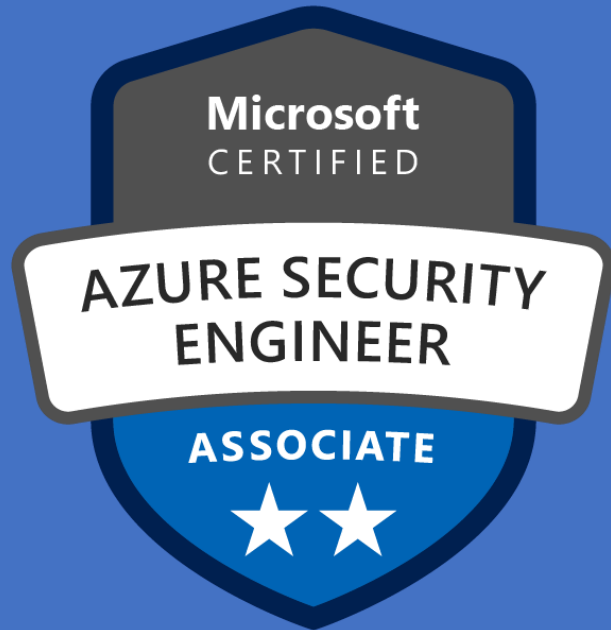
Protects sensitive data at rest, in transit, and in use

Database data always remains encrypted

Data access is only from client applications and servers

Uses client-side encryption – enhanced client driver

Separates data owners from data managers



AZ-500

Episode 17

Module 03 Knowledge Check



Review Question 1



Which one of the following should not be stored in Azure Key Vault? What are the differences between these items? Select one.

- ☐ Key management
- ☐ Secret management
- ☐ Certificate management
- ☒ Identity management

Review Question 2



A select group of users must be able to create and delete keys in the key vault. How should you grant these permissions?

- ☐ Service identities
- ☐ Azure AD authentication
- ☐ Key vault access policies
- ☒ Role-based Access Control

Review Question 3



Which of these statements best describes Azure Key Vault's authentication and authorization process? Select one.

- ☐ Applications authenticate to a vault with the username and password of the lead developer and have full access to all secrets in the vault.
- ☒ Applications and users authenticate to a vault with their Azure Active Directory identities and are authorized to perform actions on all secrets in the vault.
- ☐ Applications and users authenticate to a vault with a Microsoft account and are authorized to access specific secrets.
- ☐ Applications authenticate to a vault with the username and password of a user that signs in to the web app, and is granted access to secrets owned by that user.

Review Question 4



How does Azure Key Vault help protect your secrets after they have been loaded by your app? Select one.

- ☐ Azure Key Vault automatically generates a new secret after every use.
- ☐ The Azure Key Vault client library protects regions of memory used by your application to prevent accidental secret exposure.
- ☐ Azure Key Vault double-encrypts secrets, requiring your app to decrypt them locally every time they're used.
- ☒ It doesn't protect your secrets. Secrets are unprotected once they're loaded by your application.

Review Question 5



Your manager wants to know more about software-protected keys and hardware-protected keys. You discuss which three of the following statements? Select three.

- ☐ Only hardware-protected keys are encrypted at rest.
- ☐ Software-protected keys are not isolated from the application.
- ☒ Software-protected cryptographic operations are performed in software
- ☒ Hardware-protected cryptographic operations are performed within the HSM
- ☒ Only hardware-protected keys offer FIPS 140-2 Level 2 assurance.

Review Question 6



What method does Microsoft Azure App Service use to obtain credentials for users attempting to access an app? Select one.

- ☐ Credentials that are stored in the browser
- ☐ Pass-through authentication
- ☒ Redirection to a provider endpoint
- ☐ Synchronization of accounts across providers

Review Question 7



What type of Managed Service Identities can you create?
Select two.

- ☐ Application-assigned
- ☐ Database-assigned
- ☒ System-assigned
- ☒ User-assigned
- ☐ VM-assigned

Review Question 8



Your App Service application stores page graphics in an Azure storage account. The app needs to authenticate programmatically to the storage account. What should you do? Select one.

- ☐ ~~✗~~ Create an Azure AD system user
- ☒ Create a managed identity
- ☐ ~~✗~~ Create a RBAC role assignment
- ☐ ~~✗~~ Create a service principal

Review Question 9



How does using managed identities for Azure resources change the way an app authenticates to Azure Key Vault?
Select one.

- ☐ Each user of the app must enter a password.
- ☒ The app gets tokens from a token service instead of Azure Active Directory.
- ☐ The app uses a certificate to authenticate instead of a secret.
- ☐ Managed identities are automatically recognized by Azure Key Vault and authenticated automatically.

Review Question 10



You need to provide a contingent staff employee temporary read-only access to the contents of an Azure storage account container named “Media”. It is important that you grant access while adhering to the security principle of least-privilege. What should you do? Select one.

- ☐ Set the public access level to container.
- ☒ Generate a shared access signature (SAS) token for the container.
- ☐ Share the container entity tag (Etag) with the contingent staff member.
- ☐ Configure a Cross-Origin Resource Sharing (CORS) rule for the storage account.

Review Question 11



Your company has both a development and production environment. The development environment needs time-limited access to storage. The production environment needs unrestricted access to storage resources. You need to configure storage access to meet the requirements. What should you do? Each answer presents part of the solution. Select two.

- ☒ Use shared access signatures for the development apps.
- ☐ Use shared access signatures for the production apps.
- ☐ Use access keys for the development apps.
- ☒ Use access keys for the production apps.
- ☐ Use Stored Access Policies for the production apps.
- ☐ Use Cross Origin Resource Sharing for the development apps.

Review Question 12



Your company is being audited. It is not known how long the audit will take, but during that time files must not be changed or removed. It is okay to read or create new files. What should you do? Select two. Each correct answer is required for the solution.

- ☐ Add a time-based retention policy to the blob container.
- ☒ Add legal hold retention policy to the blob container.
- ☐ Configure a retention time period of 2 weeks with an option to renew.
- ☒ Identify a tag for the items that are being protected.

Review Question 13



You are configuring an Azure File share for the business group. Which of the following is not true? Select one?

- ☐ Azure Files can authenticate to Azure Active Directory Domain Services.
- ☐ Azure Files can authenticate to on-premises Active Directory Domain Services.
- ☒ Azure Files can use RBAC for share-level or directory/file permissions.
- ☐ Azure Files uses SMB.

Review Question 14



You are configuring Secure transfer required. Your Compliance office wants to know more about this feature. You provide all the following information, except? Select one.

- ☐ Requests to storage can be HTTPS or HTTP.
- ☐ Requests to storage must be SMB with encryption.
- ☐ By default, new storage accounts have secure transfer required enabled.
- ☐ Azure storage doesn't support HTTPS for custom domain names

Review Question 15



Your SQL database administrator has recently read about SQL injection attacks. They ask you what can be done to minimize the risk of this type of attack. You suggest implementing which of the following features?

- ☒ Advanced Threat Protection
- ☐ Data Discovery and Classification
- ☐ Dynamic Data Masking
- ☐ Transparent Data Encryption

Review Question 16



Your organization provides a Help Desk for its customers. Service representatives need to identify callers using the last four numbers of their credit card. You need to ensure the complete credit card number is not fully exposed to the service representatives. Which of the following features do you implement?

- ☐ Always Encrypted
- ☐ Data Classification
- ☒ Dynamic Data Masking
- ☐ Transparent Data Encryption

Review Question 17



Your organization auditors need to be assured that sensitive database data always remains encrypted at rest, in transit, and in use. You assure the auditors this is being done because you have configured which feature?

- ☒ Always Encrypted
- ☐ Disk Encryption
- ☐ Dynamic Data Masking
- ☐ Transparent Data Encryption

Review Question 18



You have an App Service web application uses a SQL database. Users need to authenticate to the database with their Azure AD credentials. You perform all the following tasks, except? Select one.

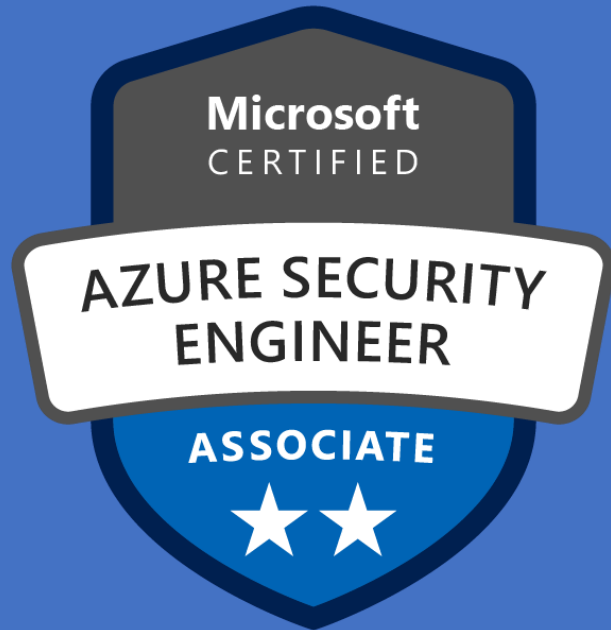
- ☐ Create a SQL Database Administrator
- ☐ Create an Azure AD Database Administrator
- ☒ Create users in the Master db
- ☐ Map database users to Azure AD identities

Review Question 19



What type of firewall rules can you configure for an Azure SQL database? Select two.

- ☐ Datacenter-level firewall rules
- ☒ Server-level firewall rules
- ☐ Azure-level firewall rules
- ☐ Table-level firewall rules
- ☒ Database-level firewall rules



AZ-500

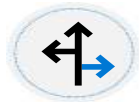
Episode 18

Azure Monitor





Azure Monitor Lesson Objectives



Azure Monitor



Metrics and Logs



Log Analytics



Connected Sources

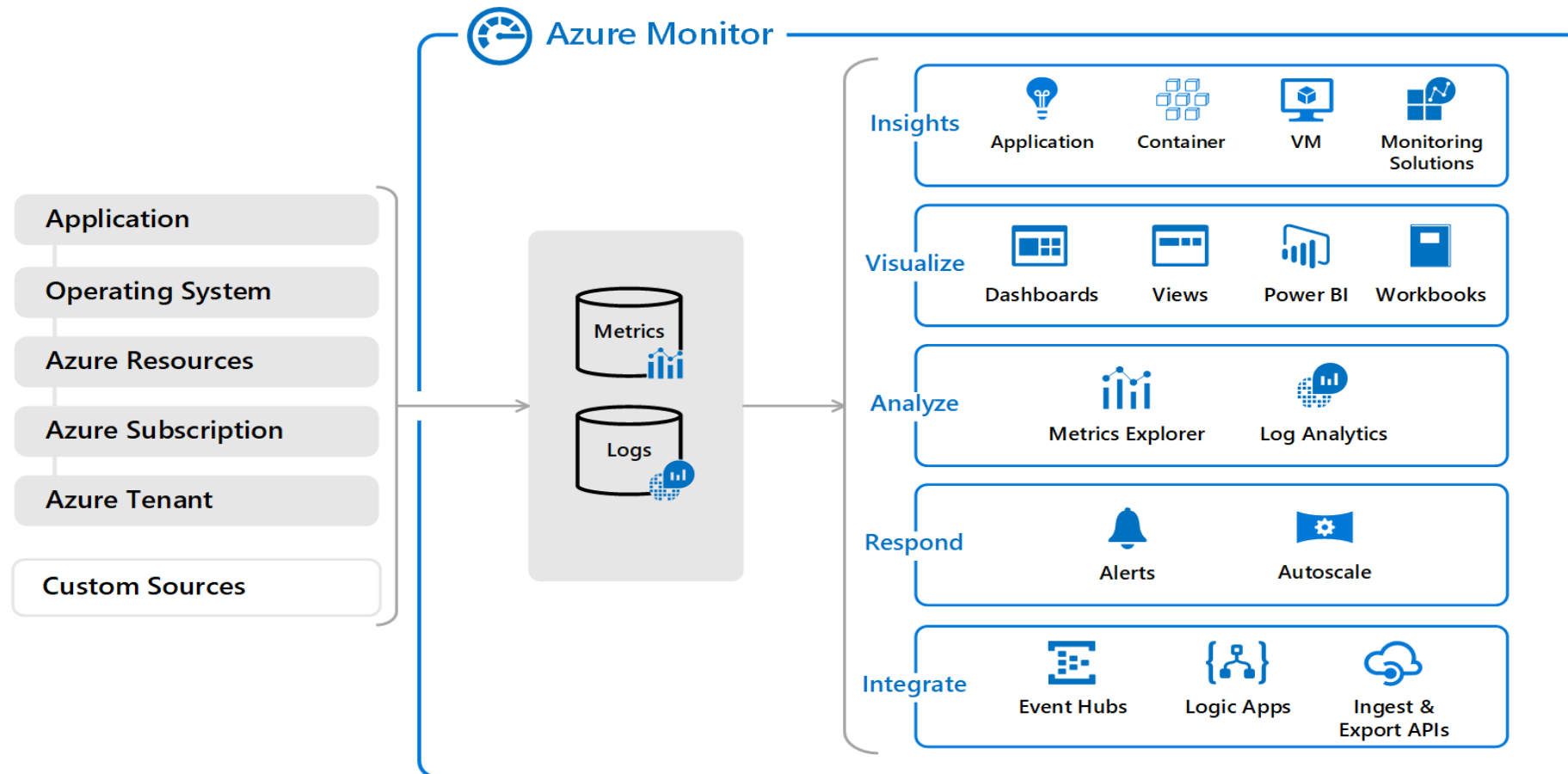


Azure Monitor Alerts

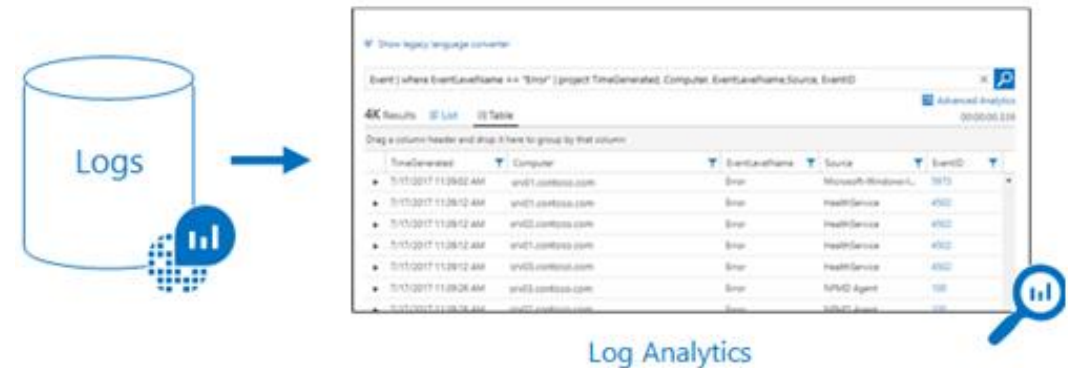


Diagnostic Logging

Azure Monitor Architecture



Metrics and Logs



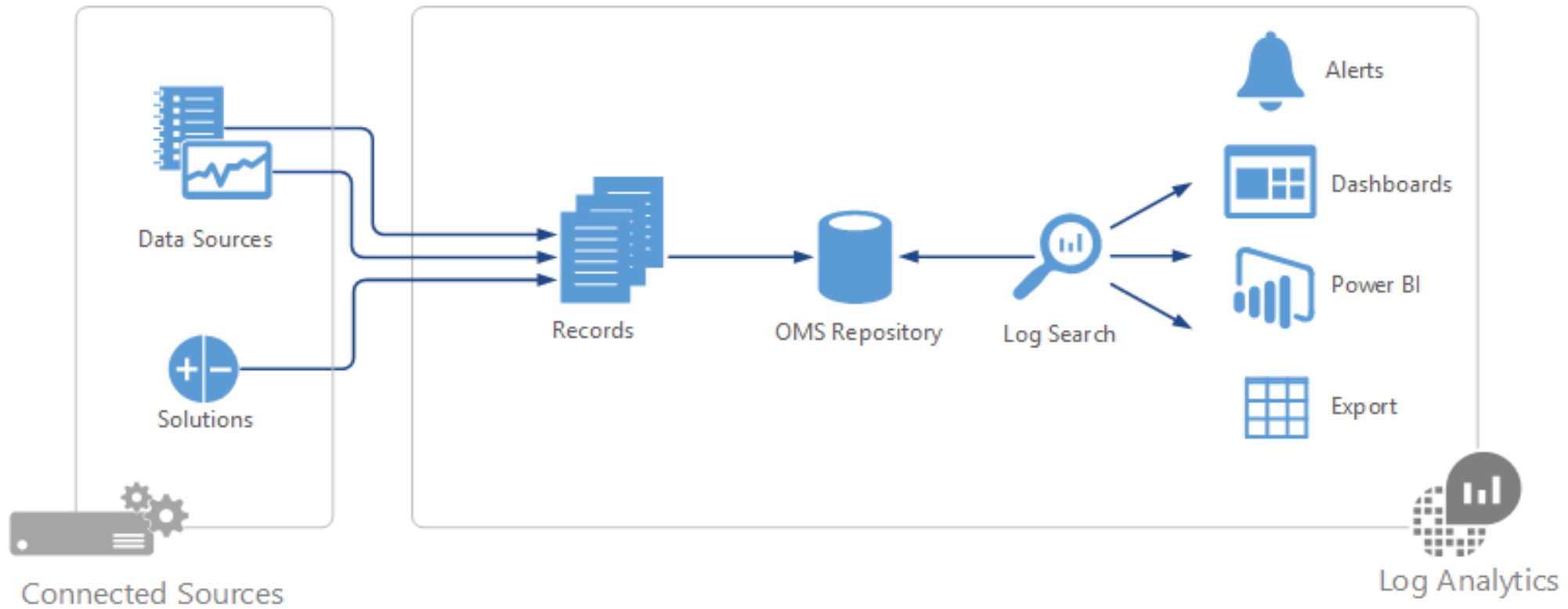
Metrics are numerical values that describe some aspect of a system at a point in time

They are lightweight and capable of supporting near real-time scenarios

Logs contain different kinds of data organized into records with different sets of properties for each type

Telemetry (events, traces) and performance data can be combined for analysis

Log Analytics



Log Analytics



Alert Rules

Dashboards

Views

Export

PowerShell

Azure Monitor Logs
API

The screenshot displays the Azure Monitor Logs interface. On the left is a navigation pane with categories like Overview, Activity log, Alerts, Metrics, Logs, Service Health, Insights, Applications, Virtual Machines, Containers, Network, and Settings. The 'Logs' section is selected. The main area shows a 'New Query 1*' tab with a Kusto query editor. The query calculates the availability rate of connected computers over the last 24 hours. Below the editor, a table shows the results of the query.

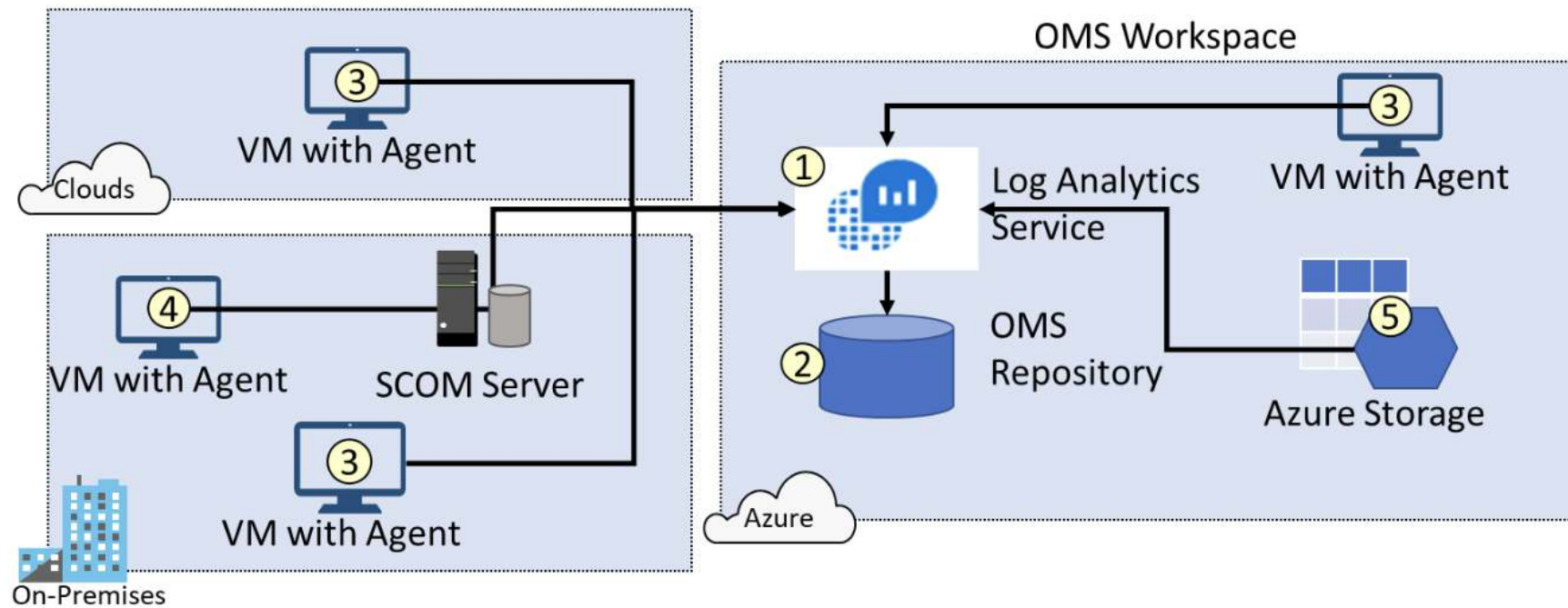
```
// Availability rate
// Calculate the availability rate of each connected computer
Heartbeat
// bin_at is used to set the time grain to 1 hour, starting exactly 24 hours ago
summarize heartbeatPerHour = count() by bin_at(TimeGenerated, 1h, ago(24h)), Computer
extend availablePerHour = iff(heartbeatPerHour > 0, true, false)
summarize totalAvailableHours = countif(availablePerHour == true) by Computer
extend availabilityRate = totalAvailableHours*100.0/24
```

Completed. Showing results from the last 24 hours. 00:00:00.424 62 records

Computer	totalAvailableHours	availabilityRate
> App04	24	100
> retailEUS8	24	100
> aks-agentpool-40719753-2	24	100
> App06	24	100
> deletethism	24	100
> Data06	24	100
> ContosoWeb	24	100
> ContosoSQLSrv2.ContosoRetail.com	24	100
> OnPremise-125	24	100

Page 1 of 2 50 items per page 1 - 50 of 62 items

Connected Sources



Azure Monitor Alerts



Select the target resource to monitor

Add a condition to select a signal and define the logic

Notify the team or automate follow-on actions

Display by severity (0 to 4)

Administer with New, Acknowledged, and Closed status

Create rule

Rules management



*** RESOURCE**

Select the target(s) that you wish to monitor

Select



*** CONDITION**

No condition defined, click on 'Add condition' to select a signal and define its logic

Add condition



ACTION GROUPS

Notify your team via email and text messages or automate actions using webhooks, runbooks, functions, logic apps or integrating with external ITSM solutions. Learn more [here](#)

ACTION GROUP NAME	ACTION GROUP TYPE
No action group selected	

Select existing

Create New

www.AGuideToCloud.com

Diagnostic Logging



Resource level logging (NSG rule counters and Key Vault audits)

Different from Activity Logs (operational)

Different from Guest OS Logs (VM agents)

Retention times are available for archiving to a storage account

Home > Monitor | Diagnostics settings > Diagnostics settings

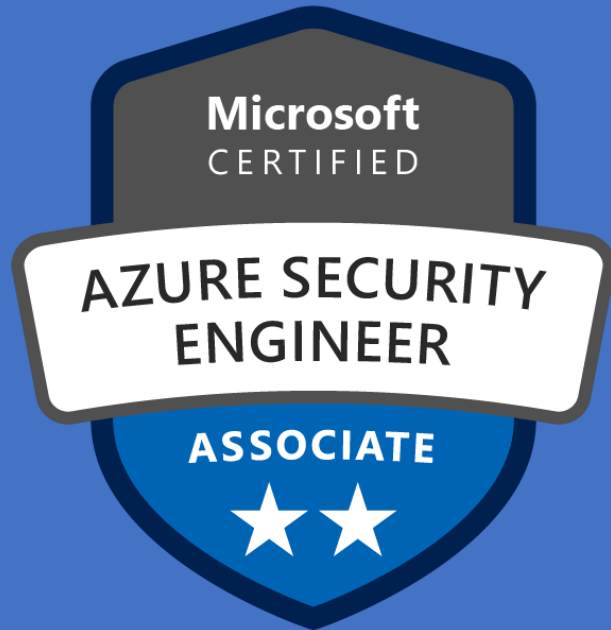
Diagnostics settings

Save Discard Delete Provide feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostics settings name *

Category details	Destination details
log ☐ WorkflowRuntime	☐ Send to Log Analytics
metric ☐ AllMetrics	☐ Archive to a storage account ☐ Stream to an event hub



AZ-500

Episode 19

Azure Security Center

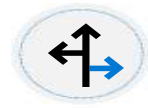




Azure Security Center Lesson Objectives



Cyber Kill Chain



Azure Security Center Features



Security Center Policies



Security Center Recommendations



Secure Score

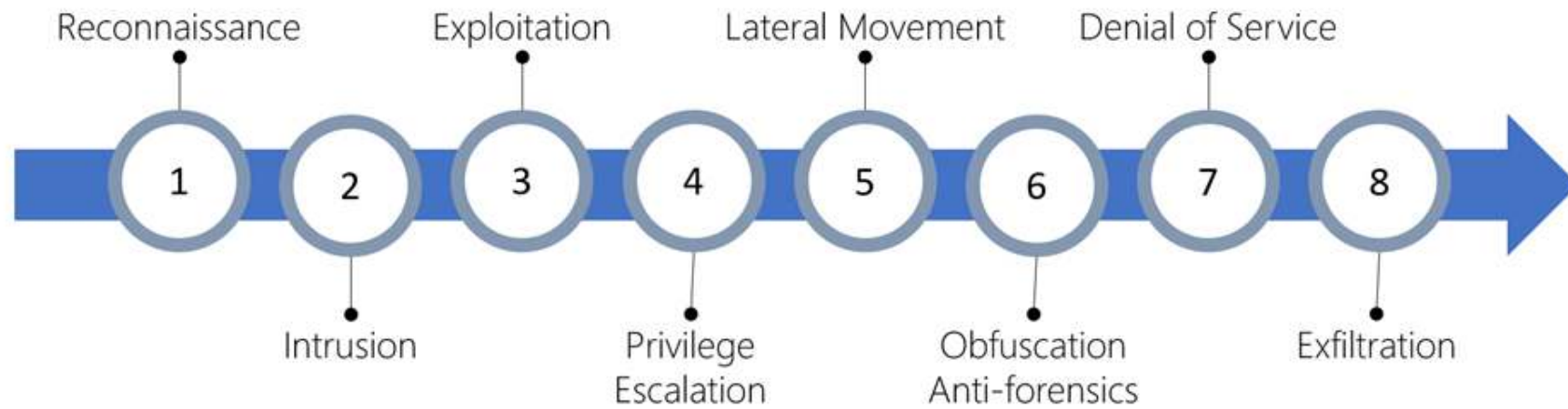


Brute Force Attacks



Just in Time Virtual Machine Access

Cyber Kill Chain



Series of steps that trace the stages of a cyberattack

Different types of attacks are associated with each stage, and they target various subsystems

Security Center is designed around the kill chain

Azure Security Center



Rapidly changing workloads

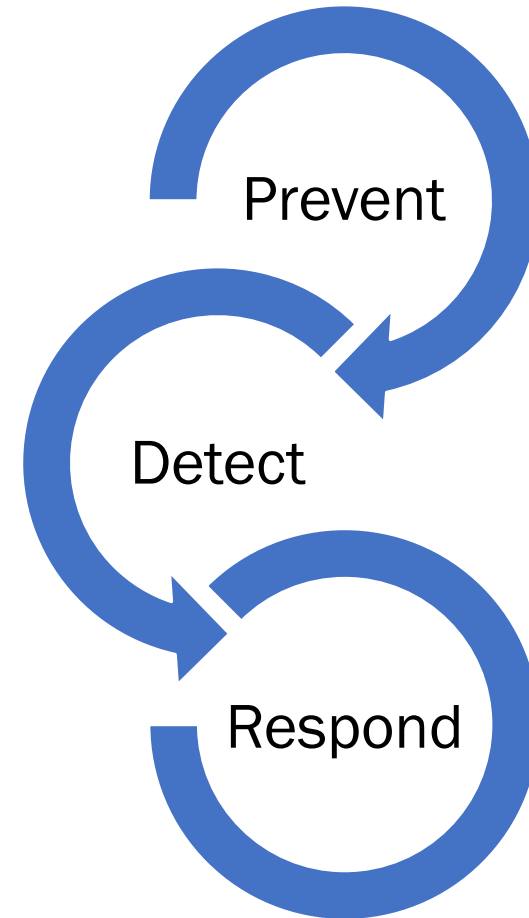
Increasingly sophisticated attacks

Security skills are in short supply

Strengthen security posture

Protect against threats

Get secure faster



Azure Security Center Policies



Defines the desired configuration for workloads

View and edit the built-in default policy

Add your own custom policies

Add regulatory compliance policies

Ensures compliance and regulatory requirements

[All services](#) > [Security Center](#) | [Security policy](#) > [Security policy](#) > [Security policy](#)

Security policy

ASC DEMO

^ Compute And Apps (33 out of 34 policies enabled)

Monitor missing Endpoint Protection in Azure Security Center ⓘ

System updates should be installed on your machines ⓘ

Vulnerabilities in security configuration on your machines should be remediated ⓘ

Vulnerabilities in container security configurations should be remediated ⓘ

^ Network (8 out of 9 policies enabled)

Subnets should be associated with a Network Security Group ⓘ

Internet-facing virtual machines should be protected with Network Security Groups ⓘ

The NSGs rules for web applications on IaaS should be hardened ⓘ

Monitor unprotected network endpoints in Azure Security Center ⓘ

^ Data (18 out of 18 policies enabled)

Secure transfer to storage accounts should be enabled ⓘ

Monitor unaudited SQL servers in Azure Security Center ⓘ

Transparent Data Encryption on SQL databases should be enabled ⓘ

Audit unrestricted network access to storage accounts ⓘ

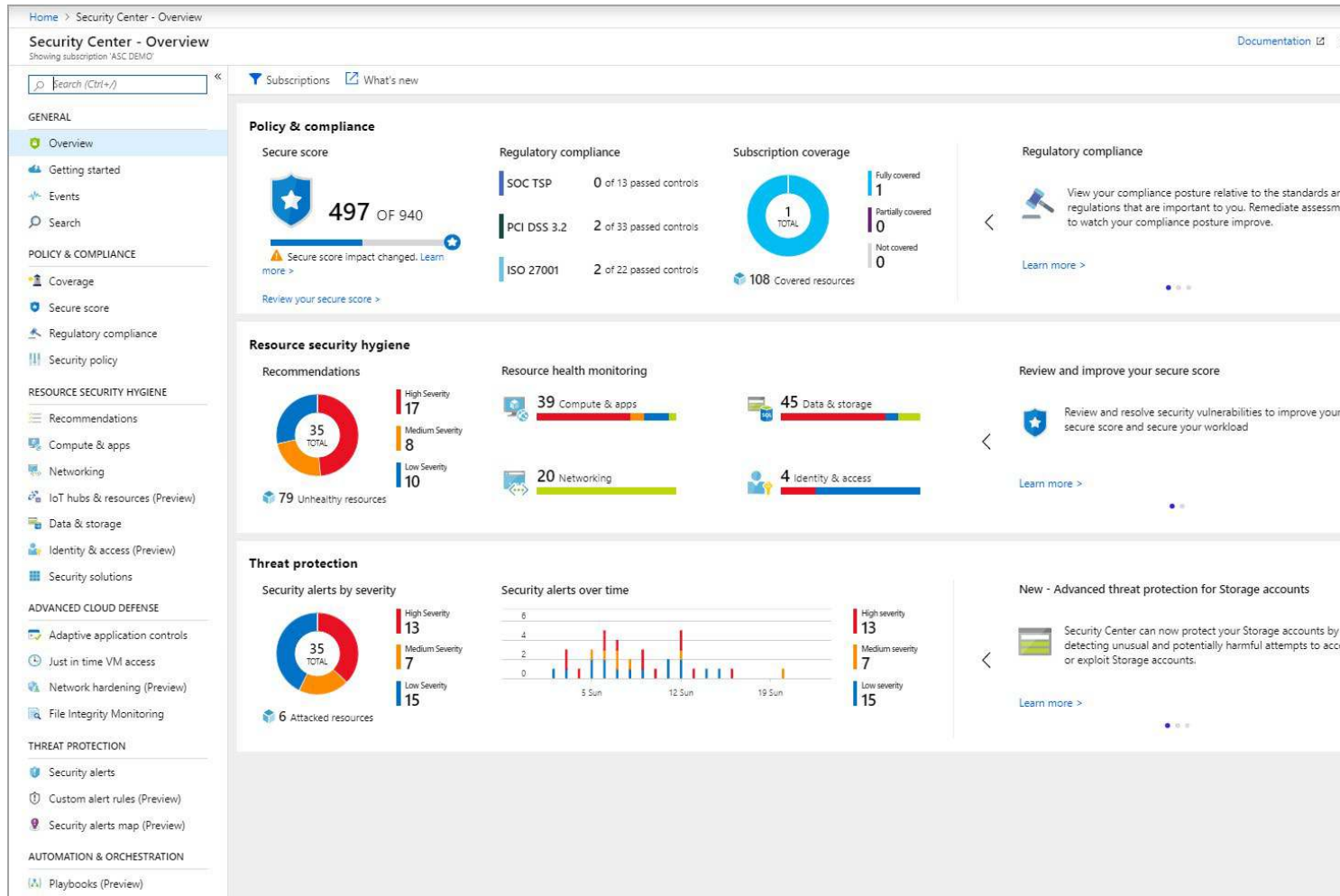
^ Identity (11 out of 11 policies enabled)

A maximum of 3 owners should be designated for your subscription ⓘ

There should be more than one owner assigned to your subscription ⓘ

MFA should be enabled on accounts with owner permissions on your subscription ⓘ

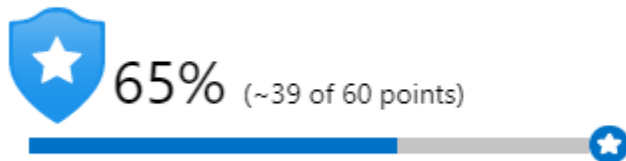
Security Center Recommendations



Secure Score



Overall Secure Score



Subscriptions with the lowest scores



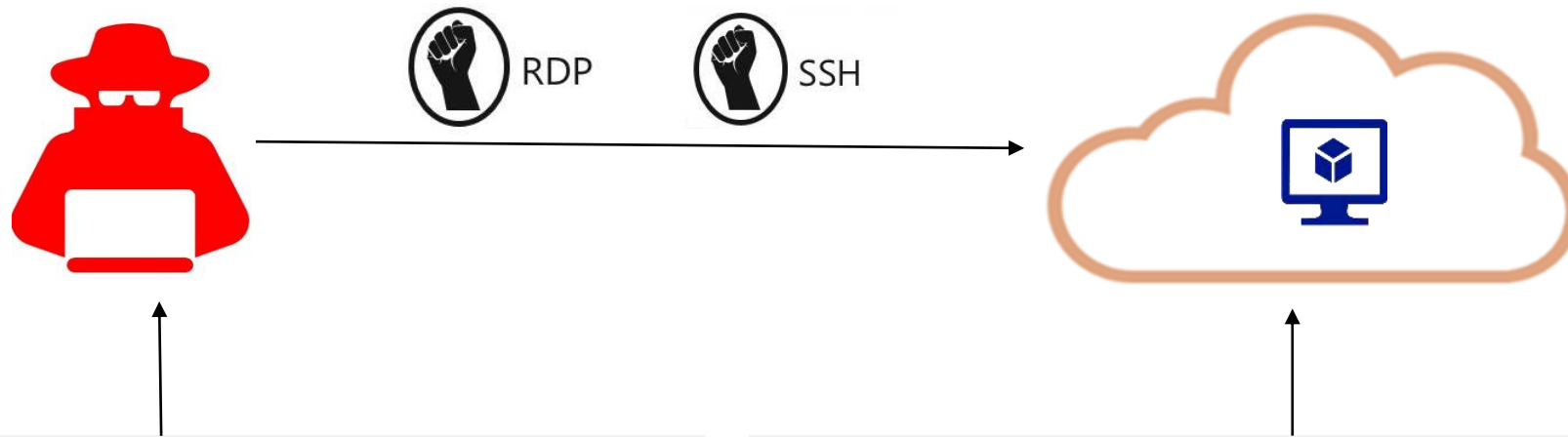
A snapshot of your current security situation

Helps prioritize and manage your security efforts

The higher the score, the lower the identified risk level

Your score only improves if you remediate all the recommendations for a single resource within a control

Brute Force Attacks



Targets management ports to gain access to a virtual machine

- **Disable the public IP address - Bastion**
- **Use Point-to-Site VPN, Site-to-Site VPN, or Azure ExpressRoute**
- **Require two-factor authentication**
- **Use complex passwords**
- **Limit the time that the ports are open (next slide)**

Just In Time VM Access

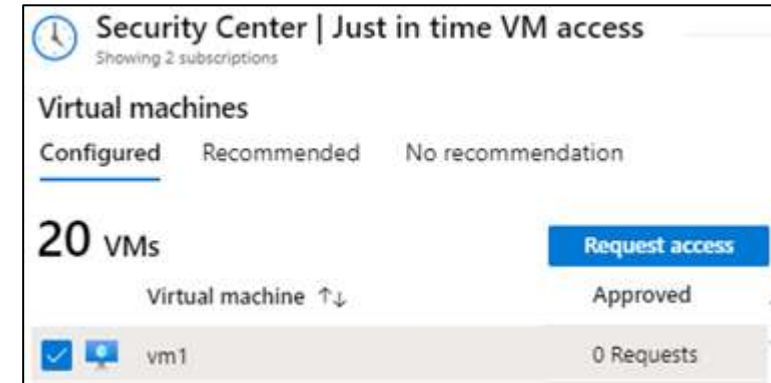


Recommends virtual machines in NSGs with public IP addresses

Select virtual machines and configure ports, source IP addresses, and time range

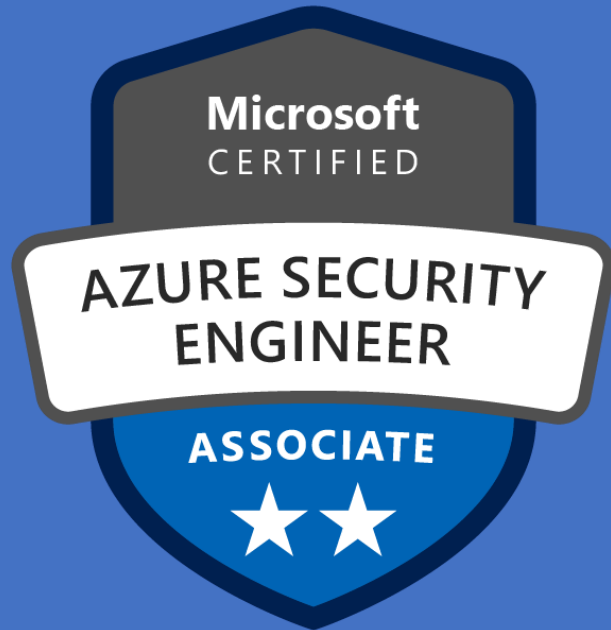
Security Center locks down inbound traffic by creating an NSG rule

Events are captured in the Activity Log



Please select the ports that you would like to open per virtual machine.

PORT	TOGGLE	ALLOWED SOURCE IP	IP RANGE	TIMERANGE
▼ vm1				
22	☒ On ☐ Off	My IP IP Range	No range	<input type="range" value="3"/>
3389	☒ On ☐ Off	My IP IP Range	No range	<input type="range" value="3"/>
5985	☐ On ☒ Off	My IP IP Range	No range	<input type="range" value="3"/>
5986	☐ On ☒ Off	My IP IP Range	No range	<input type="range" value="3"/>



AZ-500

Episode 20

Azure Sentinel





Azure Sentinel Lesson Objectives



Azure Sentinel



Data Connections



Workbooks



Incidents



Playbooks



Hunting

Azure Sentinel

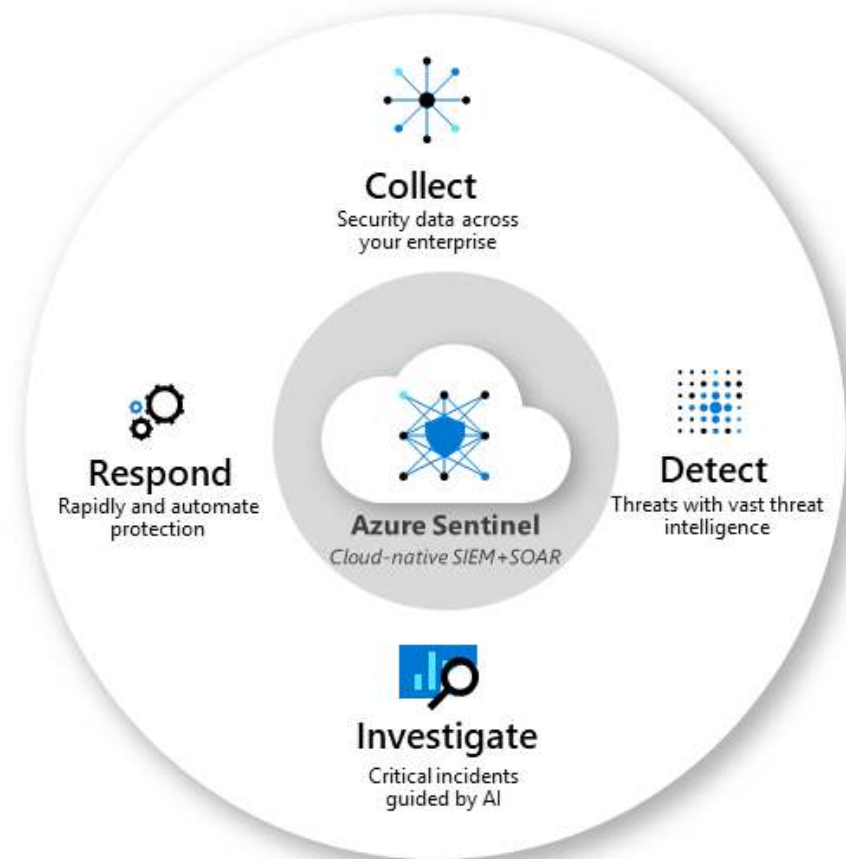


Collect data at cloud scale

Detect threats, and minimize false positives

Investigate threats with artificial intelligence

Respond to incidents rapidly



Data Connections



Service to service integration (AWS, Azure AD, Office 365 ..)

External solutions via API (Barracuda, F5 BIG-IP, ForcePoint DLP ...)

External solutions that can perform real-time log streaming using the Syslog protocol, via an agent (Cisco ASA, Fortinet ...)

Azure Sentinel - Data Connectors	
Selected workspace: 'CyberSecurityDemo'	
 23 Connectors	 17 Connected
	 0 Coming soon
STATUS	CONNECTOR NAME
	Amazon Web Services Amazon
	Azure Active Directory Microsoft
	Azure Active Directory Identity Protection Microsoft
	Azure Activity Microsoft
	Barracuda Web Application Firewall Barracuda
	Check Point CheckPoint
	Cisco ASA Cisco

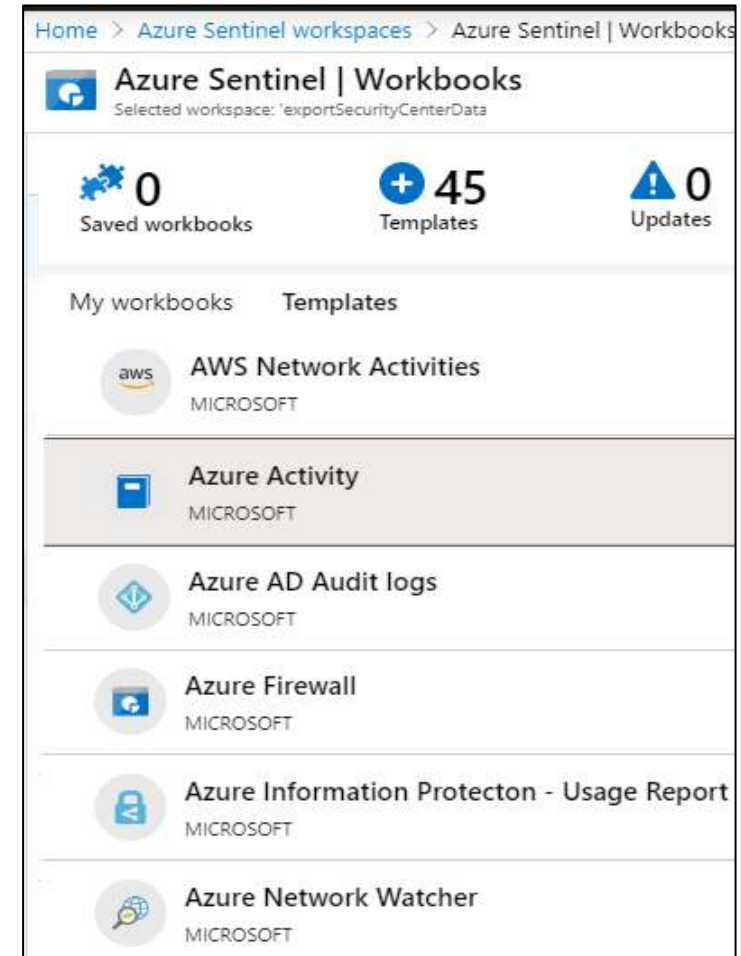
Workbooks



Analyze and correlate all user operations and events

Learn about all user operations, trends, and anomalous changes over time

Drill down into caller activities and summarize detected failure and warning events



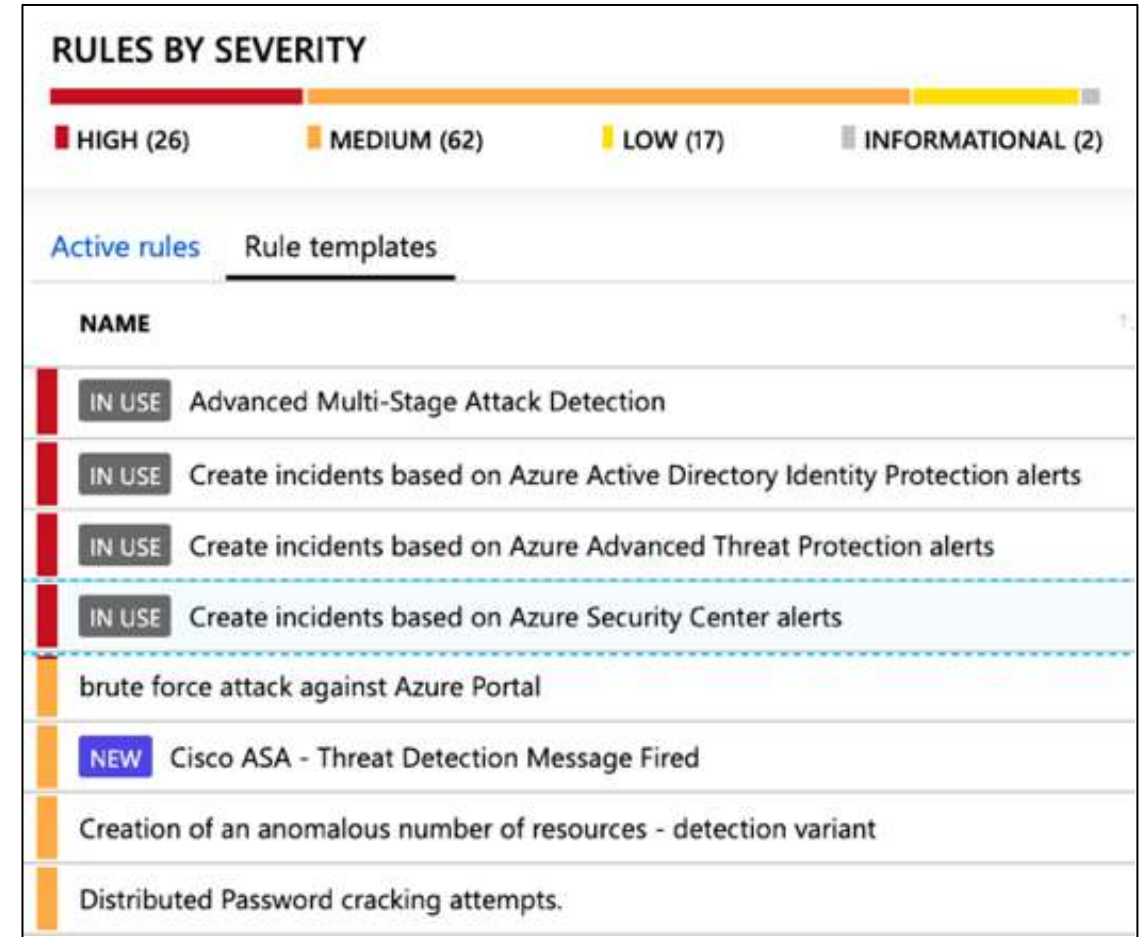
Incidents



Create incidents when an alert is triggered from a connected source

Select from built-in rule templates or create your own

Use Azure AD Information Protection to automatically enable incident generation when connected



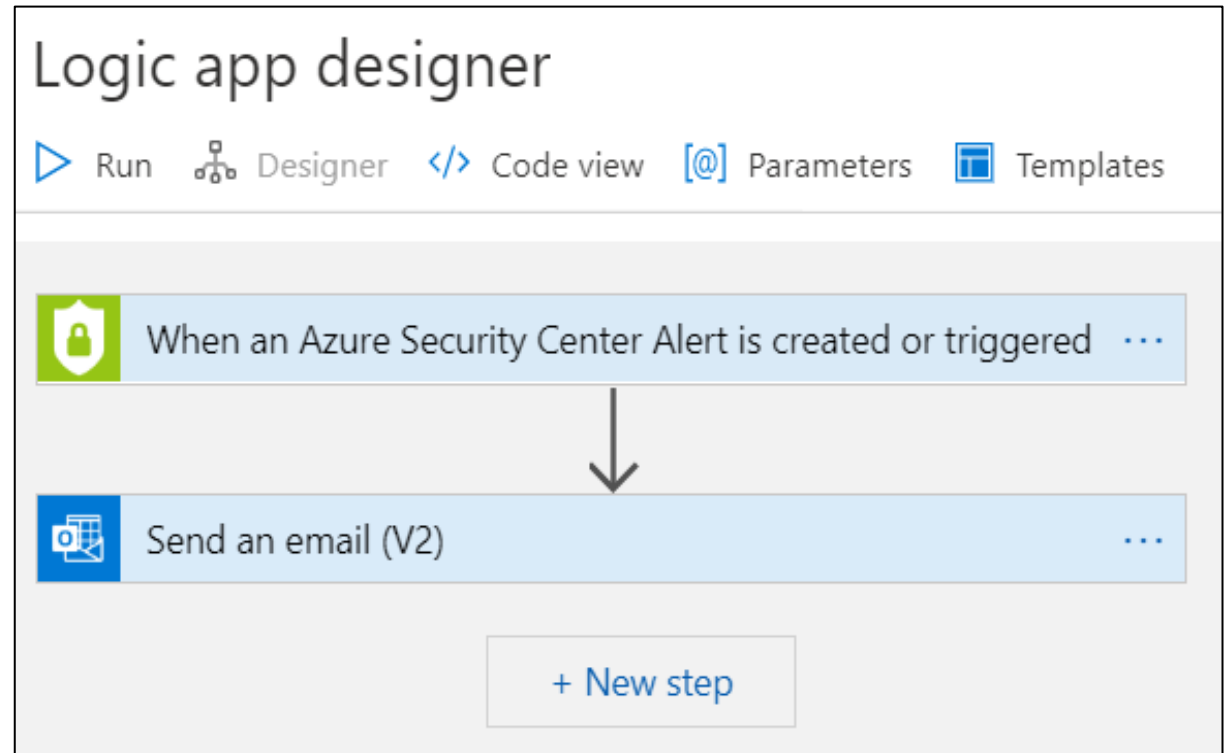
Playbooks



Collection of procedures that can be run from Azure Sentinel in response to an alert

Based on Azure Logic Apps – 200+ connectors

Can be run manually or set to run automatically



Hunting

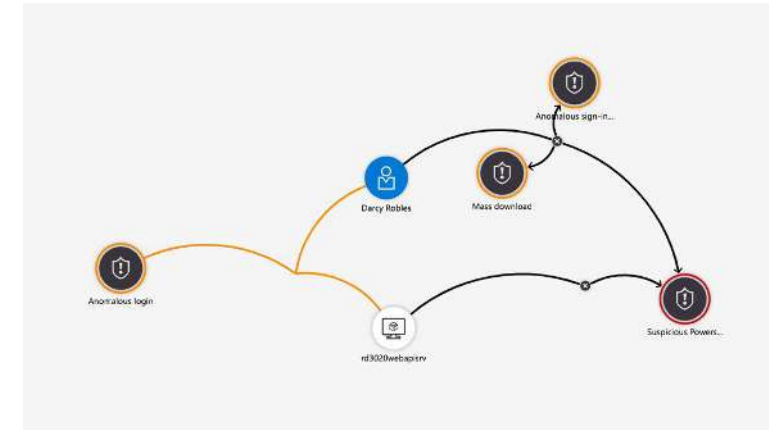


Built-in hunting queries

Custom queries with IntelliSense

Create bookmarks for later review

Jupyter notebooks and Python integration



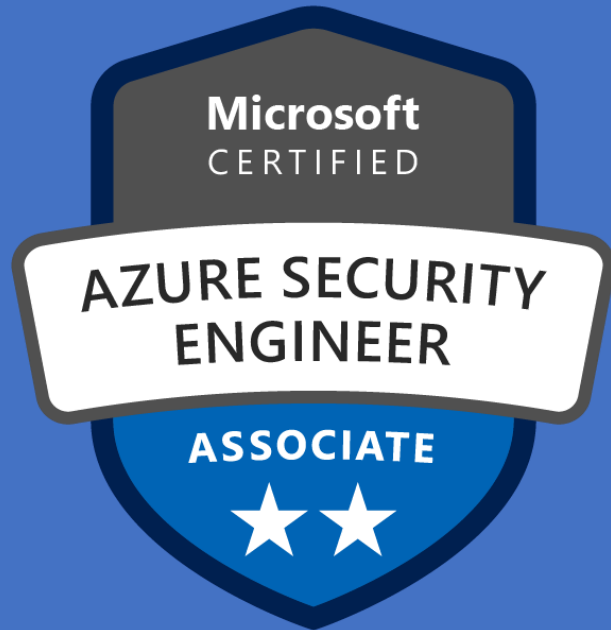
Home > Azure Sentinel workspaces > Azure Sentinel - Hunting

Azure Sentinel - Hunting
Selected workspace: 'ASIHuntOMS'

20 Total Queries	94 Total Results	4 Total Bookmarks	0 My Bookmarks
---------------------	---------------------	----------------------	-------------------

Queries Bookmarks

QUERY	DESCRIPTION
★ Uncommon processes/files - bottom 5%	Shows the rarest processes seen running for the first...
★ Script usage summary (cscript.exe)	Daily summary of vbs scripts run across the environ...
★ Summary of users created using uncommon ...	Summarizes users of uncommon & undocumented ...
★ Office365 authentications	Shows authentication volume by user agent and IP ...
★ New processes observed in last 24 hours	Shows new processes observed in the last 24 hours ...
★ Summary of failed user logons by reason of f...	A summary of failed logons can be used to infer lat...
★ Anomalous Azure AD apps based on authent...	This query over Azure AD sign-in activity highlights...



AZ-500

Episode 21

Module 04 Knowledge Check



Review Question 1



Data collected by Azure Monitor collects fits into which two fundamental types? What are differences in those types of data? Select two.

☐ Events

☒ Logs

☒ Metrics

☐ Records

Review Question 2



You can query Log Analytics workspace with which of the following? Select one.

- ☐ Contextual Query Language
- ☐ Embedded SQL
- ☐ Graph API
- ☒ Kusto Query Language

Review Question 3



You want to be notified when any virtual machine in the production resource group is deleted. What should you configure? Select one.

☒ Activity log alert

☐ Application alert

☐ Log alert

☐ Metric alert

Review Question 4



The IT managers would like to use a visualization tool for the Azure Monitor results. You suggest all the following, except?

☐ Dashboard

☒ Logic Apps

☐ Power BI

☐ Workbook

Review Question 5



Which of following is not included in the Security Center free tier? Select one.

- ☐ ~~M~~onitor identity and access on the key vault
- ☐ ~~M~~onitor IoT hubs and resources
- ☐ ~~M~~onitor network access and endpoint security
- ☐ Monitor non-Azure resources

Review Question 6



Your organization compliance group requires client authentication use Azure AD, and Key Vault diagnostic logs to be enabled. What is the easiest way to accomplish this? Select one.

- ☐ Create Desired Configuration State scripts
- ☐ Create resource groups and locks
- ☐ Configure management groups
- ☒ Implement Security Center policies

Review Question 7



Your Azure Security Center dashboard presents a Secure Score. How would you describe that score? Select one.

- ☒ **The Secure Score is a calculation based on the ratio of healthy resources vs. total resources.**
- ☐ **The Secure Score is a count of recommendations made against your monitored resources.**
- ☐ **The Secure Score is a machine-learning based prediction of how likely your resources are to be infiltrated by a hacker.**
- ☐ **The Secure Score changes only when premium features are purchased.**

Review Question 8



Your organization is working with an outside agency that needs to access a virtual machine. There is a real concern about brute-force login attacks targeted at virtual machine management ports. Which of the following can be used to open the management ports for a defined time range? Select one.

- ☐ Azure Firewall
- ☐ Bastion service
- ☒ Just-in-Time virtual machine access
- ☐ Azure Sentinel

Review Question 9



You are using Azure Security Center (ASC) to provide visibility into your virtual machine security settings. With ASC monitoring you can be notified of all the following, except? Select one.

- ☒ A newer operating system version is available.
- ☐ System security updates and critical updates that are missing.
- ☐ Disk encryption should be applied on virtual machines.
- ☐ Endpoint protections services need to be installed.

Review Question 10



Where can you create and manage custom security alerts?

- ☐ Azure Security Center
- ☒ Azure Sentinel
- ☐ Azure Storage
- ☐ Application Security Groups

Review Question 11



You are explaining what an Azure Sentinel playbook is and how it can be used? You cover all the following, except? Select one.

- ☐ A Sentinel playbook is a collection of procedures that can be run in response to an alert.
- ☐ A Sentinel playbook can help automate and orchestrate an incident response.
- ☐ A Sentinel playbook be run manually or set to run automatically when specific alerts are triggered.
- ☐ A Sentinel playbook be created to handle several subscriptions at once.

Review Question 12



You are using Sentinel to investigate an incident. When you view the incident detailed information you see all of the following, except? Select one.

- ☐ Incident ID
- ☒ Incident owner
- ☐ Number of entities involved
- ☐ Raw events that triggered the incident
- ☐ Severity

Review Question 13



You are an investigator who wants to be proactive about looking for security threats. You have read about Sentinel's hunting capabilities and notebooks. What is an Azure Sentinel notebook? Select one.

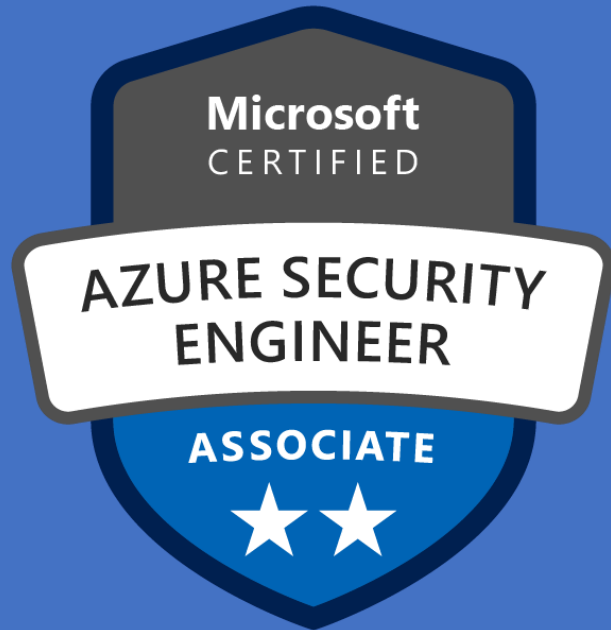
- ☐ A built-in query to provide you with an entry point to look for new detections and figure out where to start hunting for the beginnings of new attacks.
- ☐ A saved item you can come back to create an incident for investigation.
- ☒ A step-by-step playbook where you can walk through to the steps of an investigation and hunt.
- ☐ A table you can query to locate actions like DNS events.

Review Question 14



You are creating roles within your security operations team to grant appropriate access to Azure Sentinel. All the following are built-in Azure Sentinel roles, except? Select one.

- ☐ Azure Sentinel contributor
- ☐ Azure Sentinel reader
- ☐ Azure Sentinel responder
- ☒ Azure Sentinel owner



AZ-500

THANK YOU!

