O'REILLY®

Microsoft Azure Security Technologies (AZ-500) Bootcamp

Earn Your Azure Security Engineer Associate Badge

Reza Salehi

Cloud Consultant and Trainer

@zaalion

Pulse Check: Are you familiar with Azure Fundamentals?

Microsoft Azure Fundamentals (AZ-900) Certification Course, 2nd Edition

Continue

4h 55m remaining

With your instructor

Reza Salehi

+ Add to playlist

Associated roles

Cloud native engineer | Cloud solutions architect | Cybersecurity engineer | Database administrator

+1 more

Skills covered

AZ-900: Microsoft Azure Fundamentals

AZ-303: Microsoft Azure Architect...

AZ-500: Microsoft Azure Security...

AI-900: Microsoft Azure AI Fundamentals

Includes quizzes

Test your knowledge during the course and with a final quiz.

October 2024

O'Reilly Media, Inc.

Learning Outcomes

- Gain knowledge of Azure cloud concepts and services
- Explore Azure services in greater depth
- Get ready for Exam AZ-900: Microsoft Azure Fundamentals
- Comfortably work with the Azure portal

The Microsoft Azure Fundamentals (AZ-900) exam is one of the most popular certifications for those who are just beginning to work with cloud-based solutions and services or who are new to Azure. The exam certifies knowledge of cloud concepts, Azure services, workloads, security and privacy, and pricing and support.

In this self-paced course, Reza Salehi will help you get familiar with Microsoft Azure's cloud services and begin your Azure certification journey. This course is aligned to the AZ-900 exam objective domains and has recently been updated to reflect the most current version of the exam (2024). It covers all the services and concepts in the Azure ecosystem you need to know in order to prepare for the test.

What you'll learn and how to apply it

By the end of this certification course, you will understand the following:

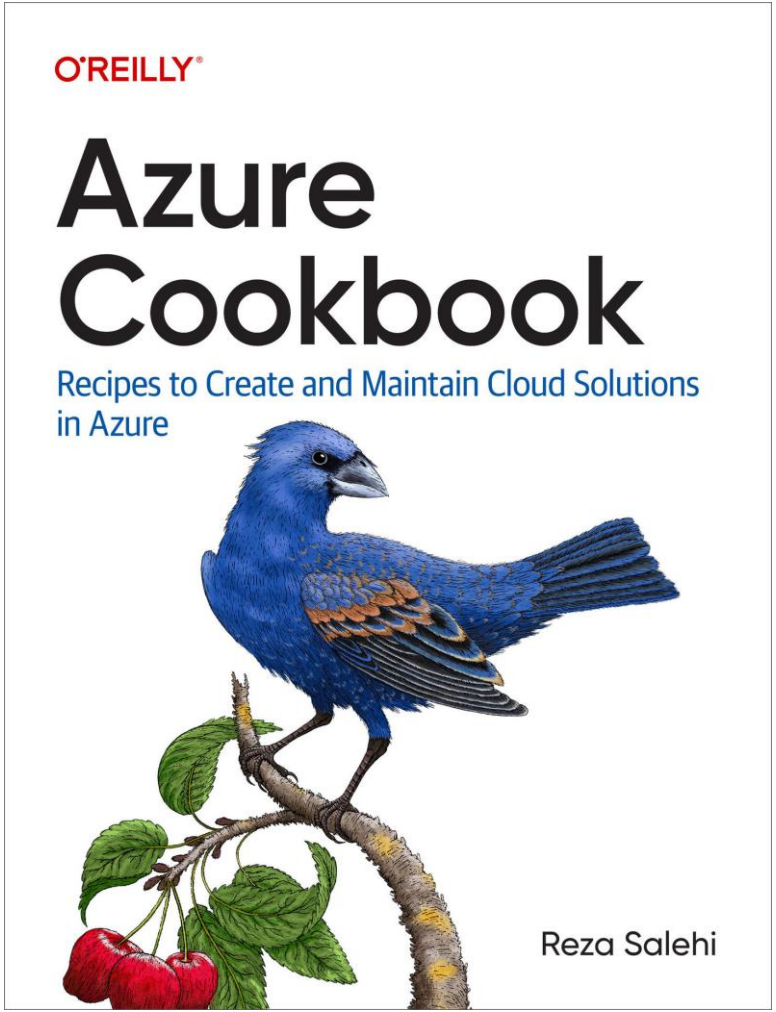
- General cloud concepts
- Core Azure services
- Core solutions and management tools on Azure
- General security and network security features
- Identity, governance, privacy, and compliance features
- Azure cost management and service-level agreements

Azure Cookbook

https://learning.oreilly.com/library/view/azure-cookbook/9781098135782/

https://www.amazon.ca/Azure-Cookbook-Recipes-Maintain-Solutions/dp/1098135792/

https://www.amazon.com/Azure-Cookbook-Recipes-Maintain-Solutions/dp/1098135792



Pulse Check: Do you need to secure Azure reosurces as a part of your job role?

Course Overview

AZ-500 Bootcamp

- Day 1
  - Manage identity and access
  - Secure networking

AZ-500 Bootcamp

- Day 2
  - Secure compute, storage, and databases
  - Manage security operations

Course Repository

https://github.com/zaalion/oreilly-az-500

Congratulations, you passed!

You've renewed your Microsoft Certified: Azure Security Engineer Associate and have extended it by **one year**.

See your results

zaalion / **oreilly-az-500** Private

Code | Issues | Pull requests | Actions | Projects | Wiki | Security | Insights | Settings

main | 1 branch | 0 tags | Go to file | Add file | Code

rezasalehinewsig Slide deck for December 22

OReilly-AZ-500-Slide-Deck.pptx	Slide deck for December 22
README.md	Initial commit

README.md

oreilly-az-500

Local | Codespaces New

Clone

HTTPS | SSH | GitHub CLI

https://github.com/zaalion/oreilly-az-500.git

Use Git or checkout with SVN using the web URL.

Open with GitHub Desktop

Open with Visual Studio

Download ZIP

CERTIFICATION

Microsoft Certified: Azure Security Engineer Associate

Demonstrate the skills needed to implement security controls, maintain an organization's security posture, and identify and remediate security vulnerabilities.

At a glance

Level
Intermediate

Product
Azure

Prepare for the exam

COURSE

Microsoft Azure Security Technologies

Continue course >

Training in this course

AZ-500: Manage identity and access

7 hr 11 min • Learning Path • 4 units

AZ-500: Secure networking

3 hr 15 min • Learning Path • 3 units

AZ-500: Secure compute, storage, and databases

3 hr 59 min • Learning Path • 3 units

AZ-500: Manage security operations

5 hr 42 min • Learning Path • 4 units

Filter by title

Study guide for Exam AZ-400
Study guide for Exam AZ-500
Study guide for Exam AZ-700
Study guide for Exam AZ-800
Study guide for Exam AZ-801
Study guide for Exam AZ-900
Study guide for Exam DP-100
Study guide for Exam DP-203
Study guide for Exam DP-300
Study guide for Exam DP-420
Study guide for Exam DP-600
Study guide for Exam DP-700
Study guide for Exam DP-900
Study guide for Exam MB-210
Study guide for Exam MB-220
Study guide for Exam MB-230
Study guide for Exam MB-240

Study guide for Exam AZ-500: Microsoft Azure Security Technologies

Article • 01/06/2025 • 2 contributors

Feedback

In this article

Purpose of this document

This study guide should help you understand what to expect on the exam and includes a summary of the topics the exam might cover and links to additional resources. The information and materials in this document should help you focus your studies as you prepare for the exam.

Microsoft Cybersecurity Reference Architectures

https://learn.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra

Day 1

Microsoft Azure Security Technologies Bootcamp

- Secure identity and access (15-20%)
- Secure networking (20-25%)

Secure Identity and Access

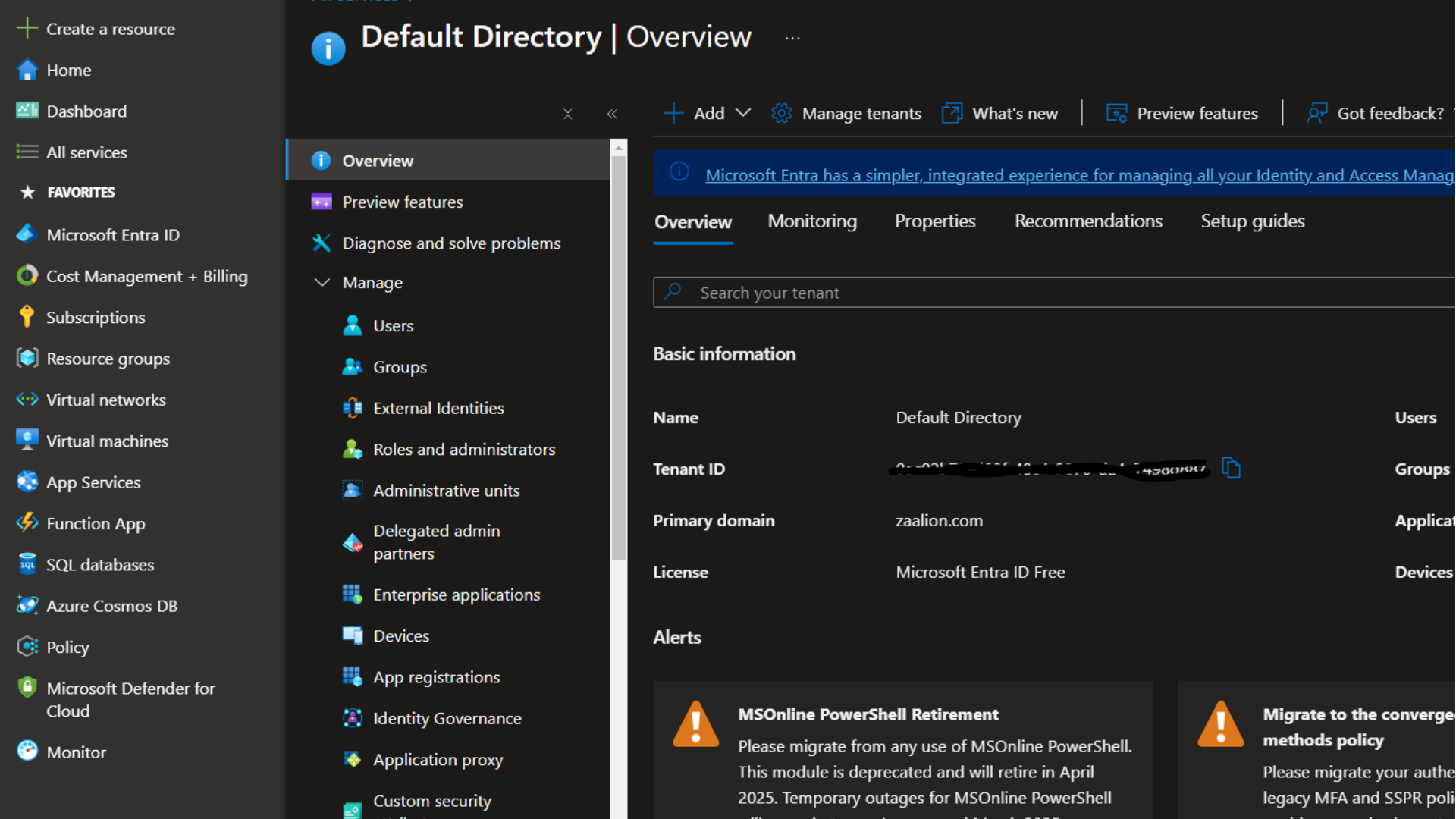
- Manage security controls for identity and access
- Manage Microsoft Entra application access

Poll: Reza is assigned the subscription Owner role. Can he add new users to Microsoft Entra ID?

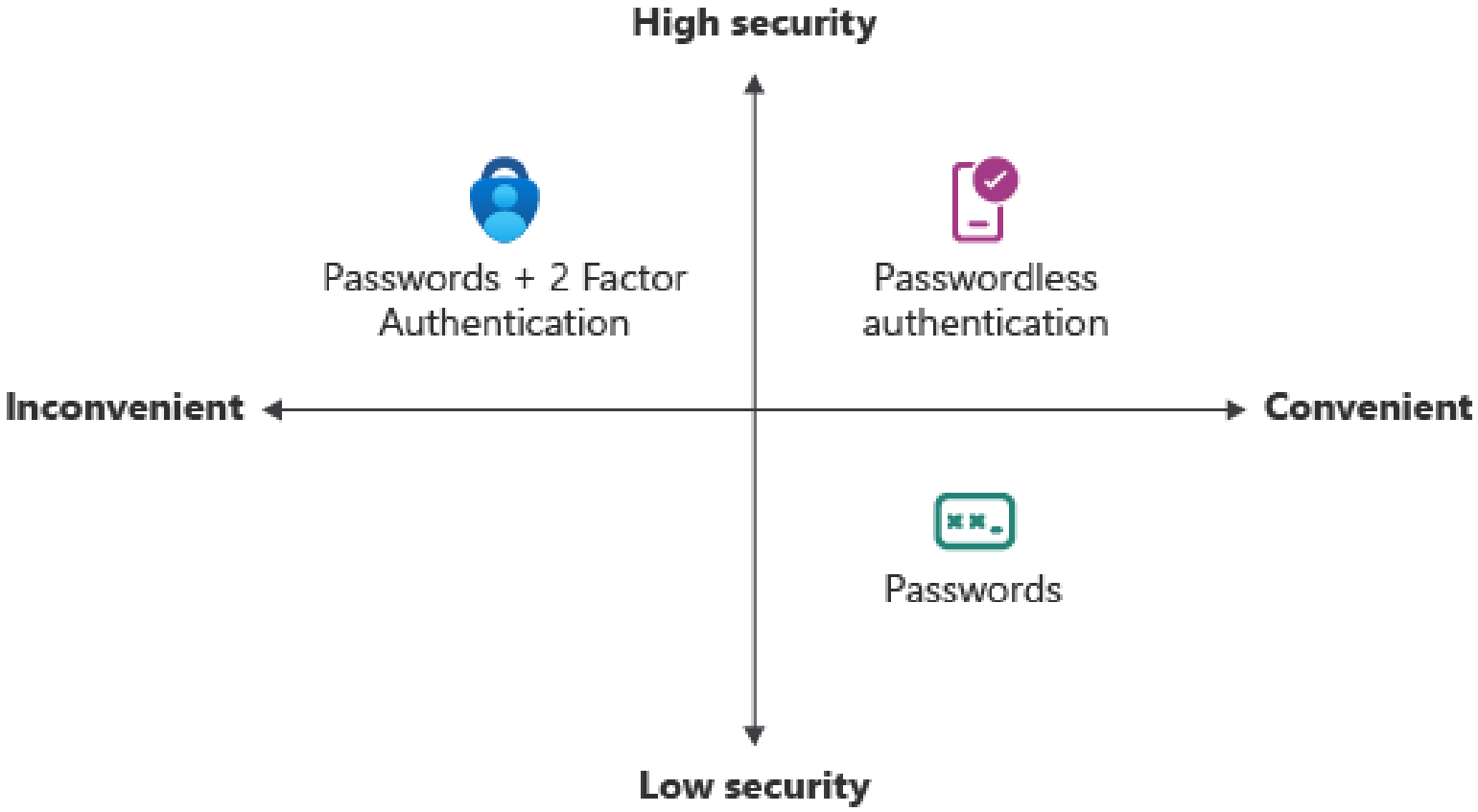
- Yes
- No

Manage security controls for identity and access

- Manage Azure built-in role assignments [see 1 2]
- Manage custom roles, including Azure roles and Microsoft Entra roles
- Implement and manage Microsoft Entra Permissions Management [see 1 2]
- Plan and manage Azure resources in Microsoft Entra Privileged Identity Management, including settings and assignments [see 1 2]
- Implement multi-factor authentication (MFA) for access to Azure resources [see 1 2]
- Implement Conditional Access policies for cloud resources in Azure [see 1]


Create a resource
Home
Dashboard
All services
FAVORITES
Microsoft Entra ID
Cost Management + Billing
Subscriptions
Resource groups
Virtual networks
Virtual machines
App Services
Function App
SQL databases
Azure Cosmos DB
Policy
Microsoft Defender for Cloud
Monitor
Default Directory | Overview
Add
Manage tenants
What's new
Preview features
Got feedback?
Overview
Preview features
Diagnose and solve problems
Manage
Users
Groups
External Identities
Roles and administrators
Administrative units
Delegated admin partners
Enterprise applications
Devices
App registrations
Identity Governance
Application proxy
Custom security
Microsoft Entra has a simpler, integrated experience for managing all your Identity and Access Manag
Overview
Monitoring
Properties
Recommendations
Setup guides
Search your tenant
Basic information
Name
Default Directory
Tenant ID
Primary domain
zaalion.com
License
Microsoft Entra ID Free
Users
Groups
Applicat
Devices
Alerts
MSOnline PowerShell Retirement
Please migrate from any use of MSOnline PowerShell. This module is deprecated and will retire in April 2025. Temporary outages for MSOnline PowerShell
Migrate to the converge
methods policy
Please migrate your authe
legacy MFA and SSPR poli

Microsoft Entra multifactor authentication

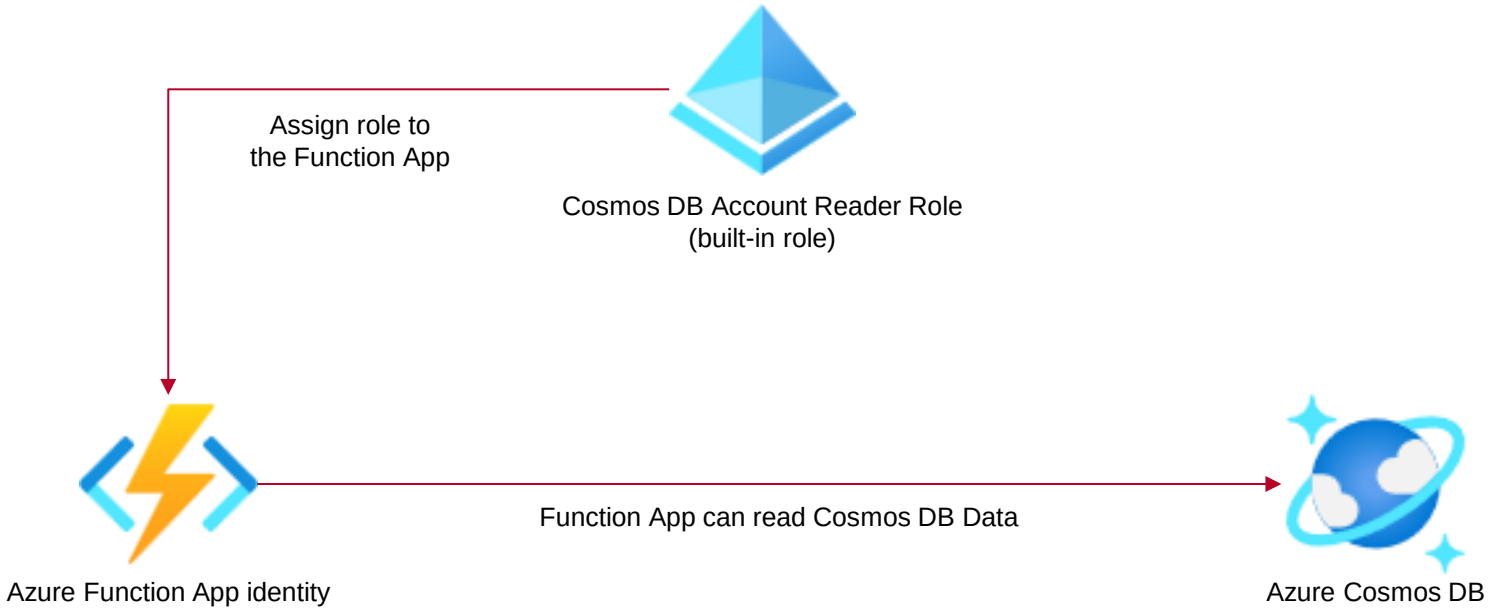

High security
Passwords + 2 Factor Authentication
Passwordless authentication
Inconvenient
Convenient
Passwords
Low security

Azure Role-based Access Control (RBAC)

Provides fine-grained access management to Azure resources.

https://learn.microsoft.com/en-us/azure/role-based-access-control/overview

Azure RBAC



https://learn.microsoft.com/en-us/azure/role-based-access-control/overview

Azure RBAC Role

- A role is a group of permissions (actions)
- There are several built-in roles which you can use
- You can define a custom role if needed

https://learn.microsoft.com/en-us/azure/role-based-access-control/overview

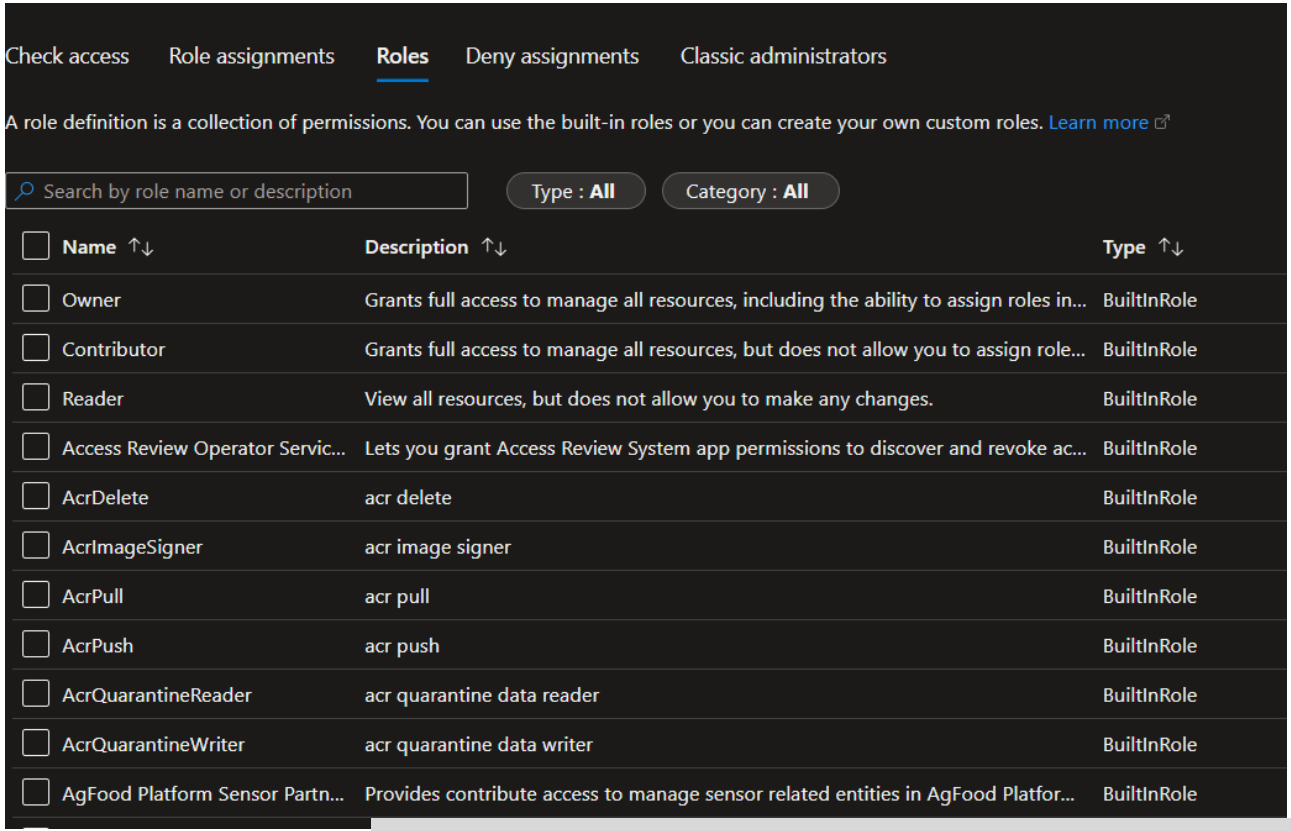
Example: Cosmos DB Account Reader Role

JSON Copy


```
{
  "assignableScopes": [
    "/"
  ],
  "description": "Can read Azure Cosmos DB Accounts data",
  "id": "/subscriptions/{subscriptionId}/providers/Microsoft.Authorization/roleDefinitions/fbdf93bf-df7d-
  "name": "fbdf93bf-df7d-467e-a4d2-9458aa1360c8",
  "permissions": [
    {
      "actions": [
        "Microsoft.Authorization/*/read",
        "Microsoft.DocumentDB/*/read",
        "Microsoft.DocumentDB/databaseAccounts/readonlykeys/action",
        "Microsoft.Insights/MetricDefinitions/read",
        "Microsoft.Insights/Metrics/read",
        "Microsoft.Resources/subscriptions/resourceGroups/read",
        "Microsoft.Support/*"
      ],
      "notActions": [],
      "dataActions": [],
      "notDataActions": []
    }
  ],
  "roleName": "Cosmos DB Account Reader Role",
  "roleType": "BuiltInRole",
  "type": "Microsoft.Authorization/roleDefinitions"
}
```

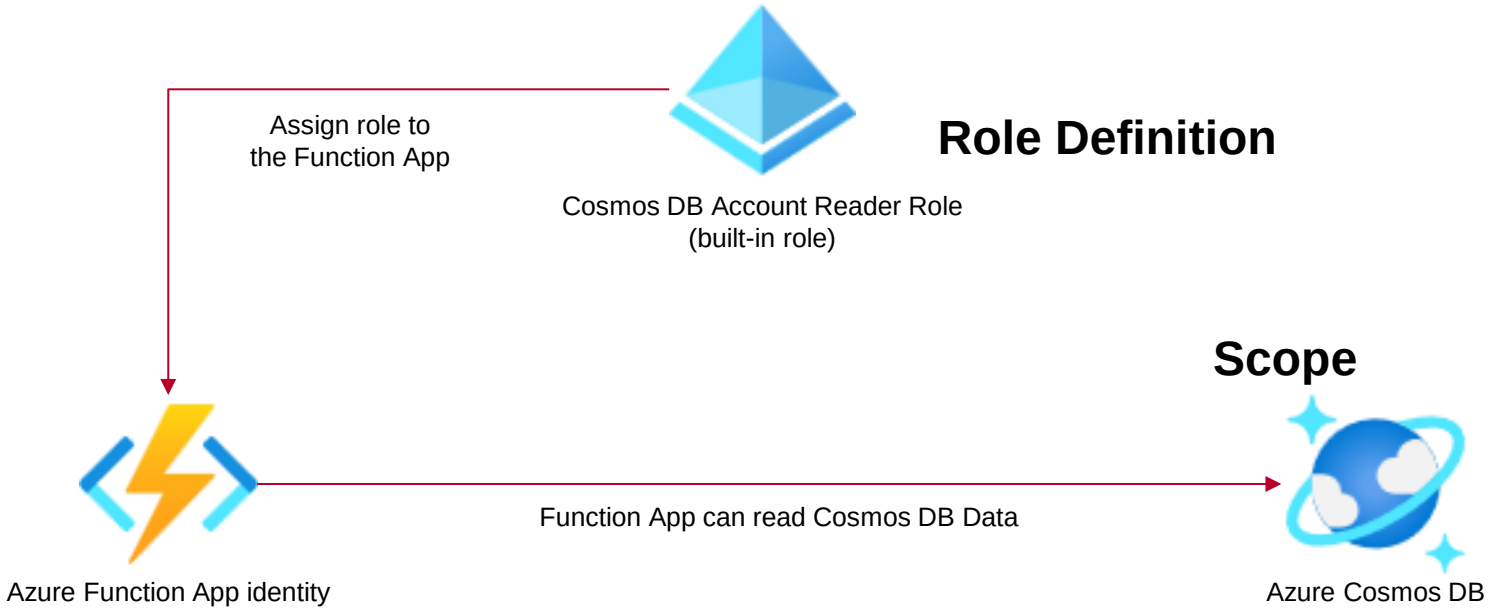

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#cosmos-db-account-reader-role

Some Built-in Roles



https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

How Azure RBAC works



https://learn.microsoft.com/en-us/azure/role-based-access-control/overview

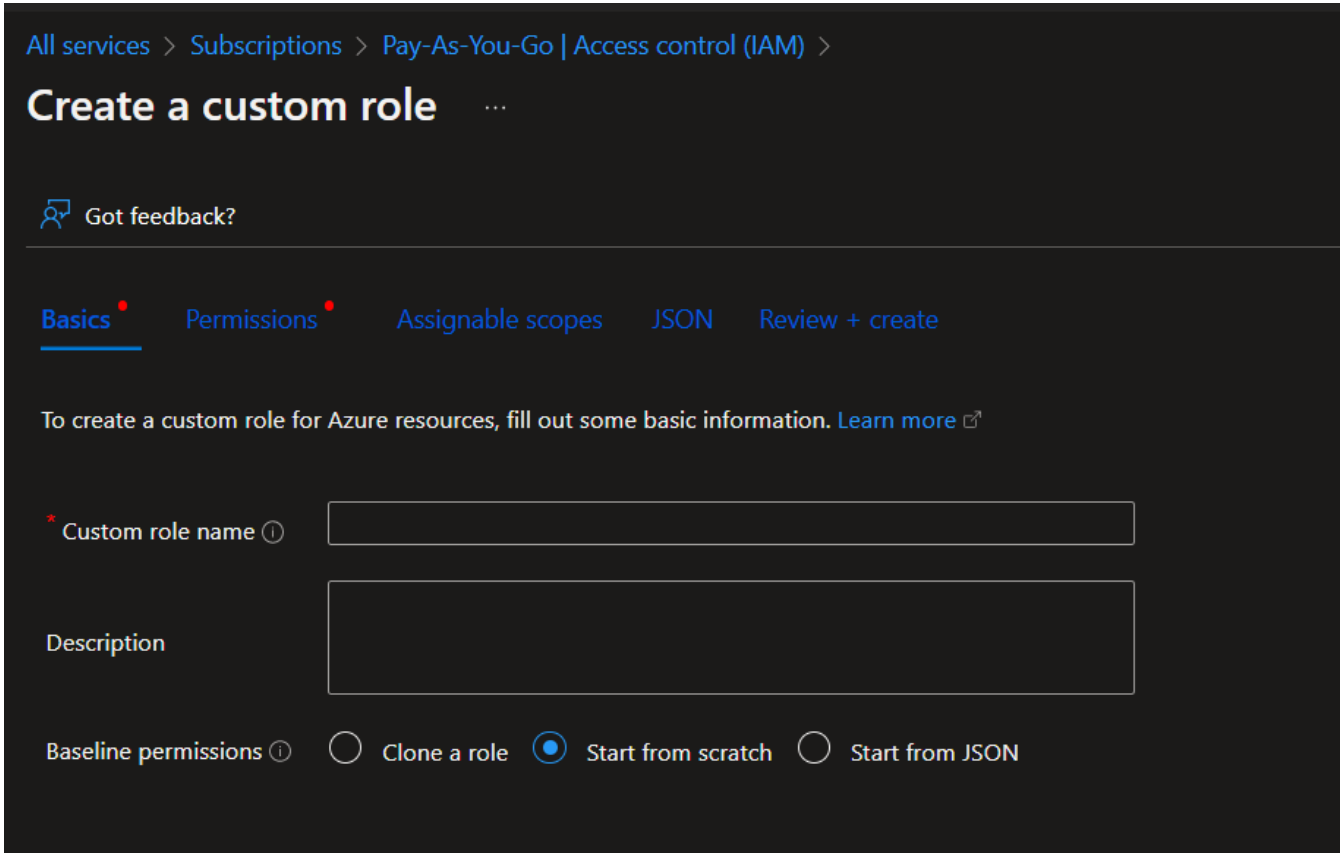
Azure RBAC Roles

Resource roles

- Fundamental (Owner, Contributor, Reader, etc.)
- Resource-specific (Azure Blob Data Reader)

Microsoft Entra ID roles (Global Administrator)

https://learn.microsoft.com/en-us/azure/role-based-access-control/overview


All services > Subscriptions > Pay-As-You-Go | Access control (IAM) >
Create a custom role
...
Got feedback?
Basics
Permissions
Assignable scopes
JSON
Review + create
To create a custom role for Azure resources, fill out some basic information. Learn more
* Custom role name
Description
Baseline permissions
Clone a role
Start from scratch
Start from JSON

Privileged Identity Management | Quick start

Privileged Identity Management

Quick start

Tasks

My roles

My requests

Approve requests

Review access

Manage

Azure AD roles

Privileged access groups (Preview)

Azure resources

Activity

My audit history

Troubleshooting + Support

Troubleshoot

New support request

You are using the updated Privileged Identity Management experience for Azure AD roles. →

What's new | Get started

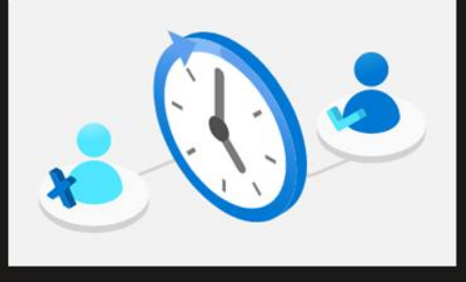
Manage your privileged access

Use Privileged Identity Management to manage the lifecycle of role assignments, enforce just-in-time access policy, and discover who has what roles. Learn more

Manage access

Users with excessive access are vulnerable in the event of account compromise. Ensure your organization manages to least privilege by periodically reviewing, renewing, or extending access to resources.

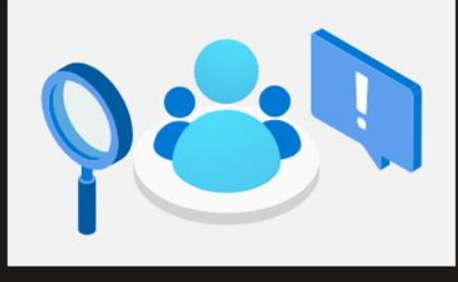
Manage



Activate just in time

Reduce the potential for lateral movement in the event of account compromise by eliminating persistent access to privileged roles and resources. Enforce just in time access to critical roles with PIM.

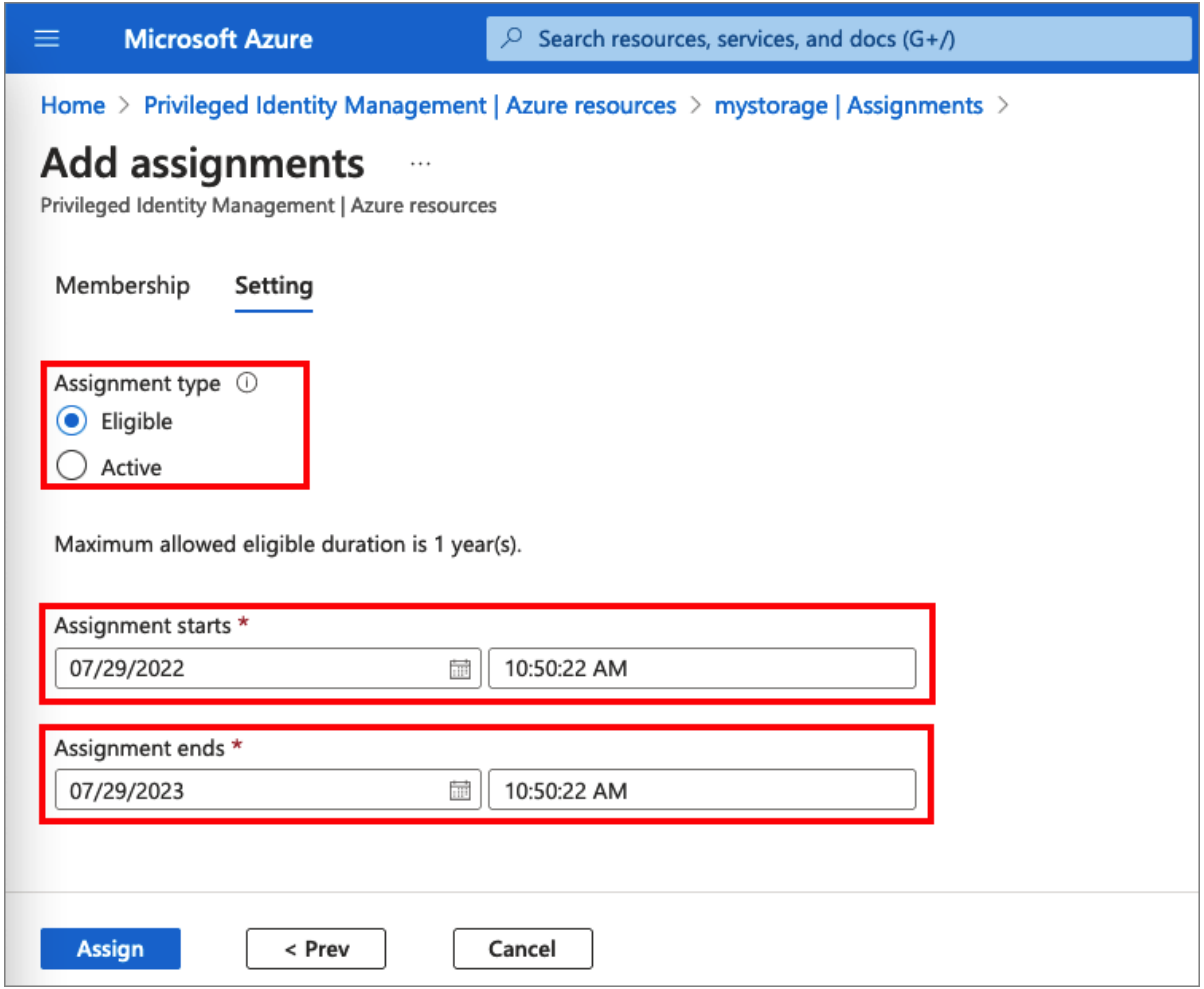
Activate



Discover and monitor

It is common for access to critical resources to go undetected. Ensure you know who has access to what, and receive notifications when new assignments are granted to accounts in your organization.

Discover


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Privileged Identity Management | Azure resources > mystorage | Assignments >
Add assignments
...
Privileged Identity Management | Azure resources
Membership
Setting
Assignment type
Eligible
Active
Maximum allowed eligible duration is 1 year(s).
Assignment starts *
07/29/2022
10:50:22 AM
Assignment ends *
07/29/2023
10:50:22 AM
Assign
< Prev
Cancel

Entra ID Conditional Access

With Conditional Access, organizations can use identity-driven signals as part of their access control decisions.

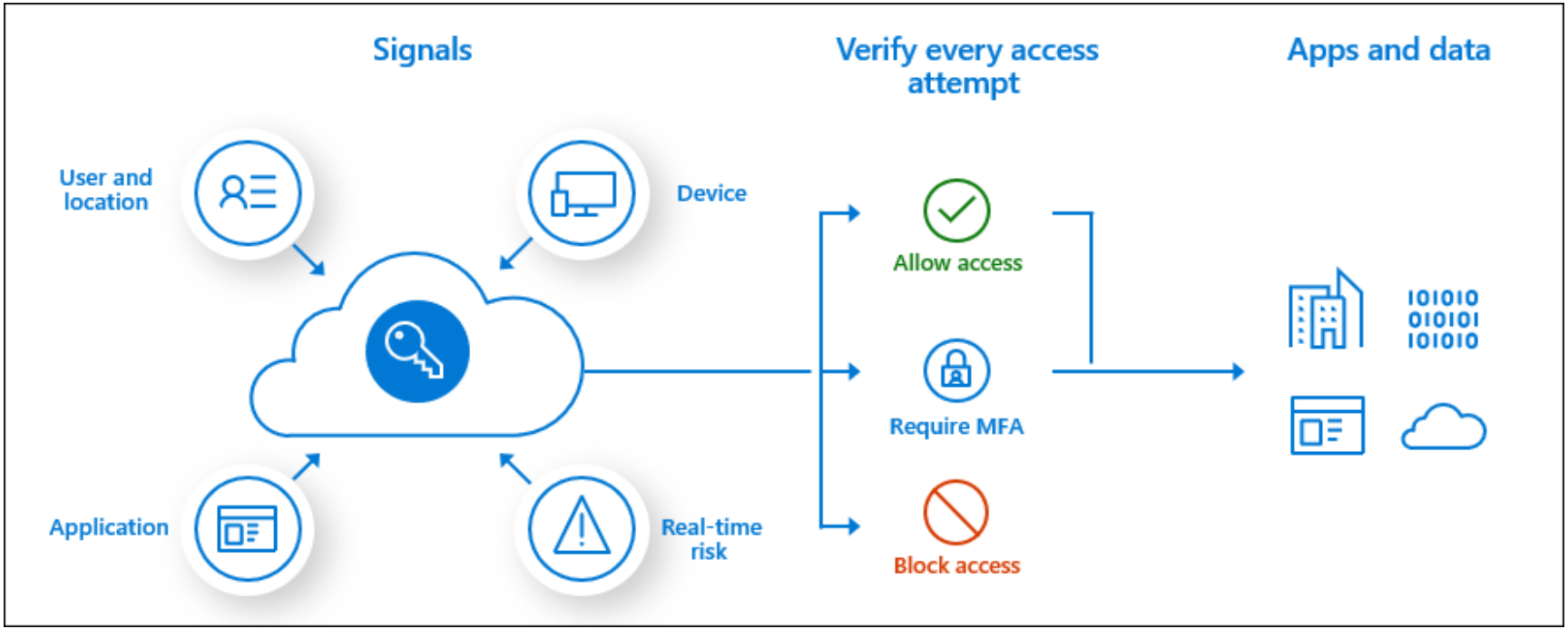
https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview

Entra ID Conditional Access

- Requiring multi-factor authentication for users with administrative roles
- Requiring multi-factor authentication for Azure management tasks
- Blocking sign-ins for users attempting to use legacy auth. protocols
- Requiring trusted locations for Entra ID Multi-Factor Authentication registration
- Blocking or granting access from specific location

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Entra ID Conditional Access



Conditional Access Signals

- User’s group membership
- User IP Location information
- Device the user is using
- Application the user tries to access
- Real-time and calculated risk detection
- Microsoft Defender for Cloud Apps

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview#common-signals

Conditional Access Decisions

- Block access
- Allow access
- Allow access after multifactor authentication, etc.

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview#common-decisions

License Requirements

Using Conditional Access requires an Entra ID Premium P1 or P2 license.

https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview#license-requirements

Poll: We need to enable a Function App to read from an Azure Cosmos DB database. Which principal(s) can we use?

- Entra ID User
- Entra ID Group
- Managed Identity
- Entra ID App Registration

Manage Microsoft Entra application access

- Manage access to enterprise applications in Microsoft Entra ID, including OAuth permission grants [see 1 2 3]
- Manage Microsoft Entra app registrations [see 1]
- Configure app registration permission scopes [see 1]
- Manage app registration permission consent [see 1]
- Manage and use service principals [see 1]
- Manage managed identities [see 1]

Create User Assigned Managed Identity ...

Basics Tags Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ Pay-As-You-Go

Resource group * ⓘ

Create new

Instance details

Region * ⓘ West US

Name * ⓘ

Azure services that can use managed identities to access other services

Article • 08/17/2022 • 3 minutes to read • 15 contributors

Managed identities for Azure resources provide Azure services with an automatically managed identity in Azure Active Directory. Using a managed identity, you can authenticate to any service that supports Azure AD authentication without managing credentials. We are integrating managed identities for Azure resources and Azure AD authentication across Azure. This page provides links to services' content that can use managed identities to access other Azure resources. Each entry in the table includes a link to service documentation discussing managed identities.

Important

New technical content is added daily. This list does not include every article that talks about managed identities. Please refer to each service's content set for details on their managed identities support. Resource provider namespace information is available in the article titled Resource providers for Azure services.

The following Azure services support managed identities for Azure resources:

Service Name	Documentation
API Management	Use managed identities in Azure API Management
Application Gateway	TLS termination with Key Vault certificates

Default Directory | App registrations

Microsoft Entra ID

- Overview
- Preview features
- Diagnose and solve problems

Manage

- Users
- Groups
- External Identities
- Roles and administrators
- Administrative units
- Delegated admin partners
- Enterprise applications
- Devices
- App registrations
- Identity Governance

New registration | Endpoints | Troubleshooting | Refresh | Download | Preview features | Got fe

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Activ
provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to
(MSAL) and Microsoft Graph. Learn more

All applications | **Owned applications** | Deleted applications | Applications from personal account

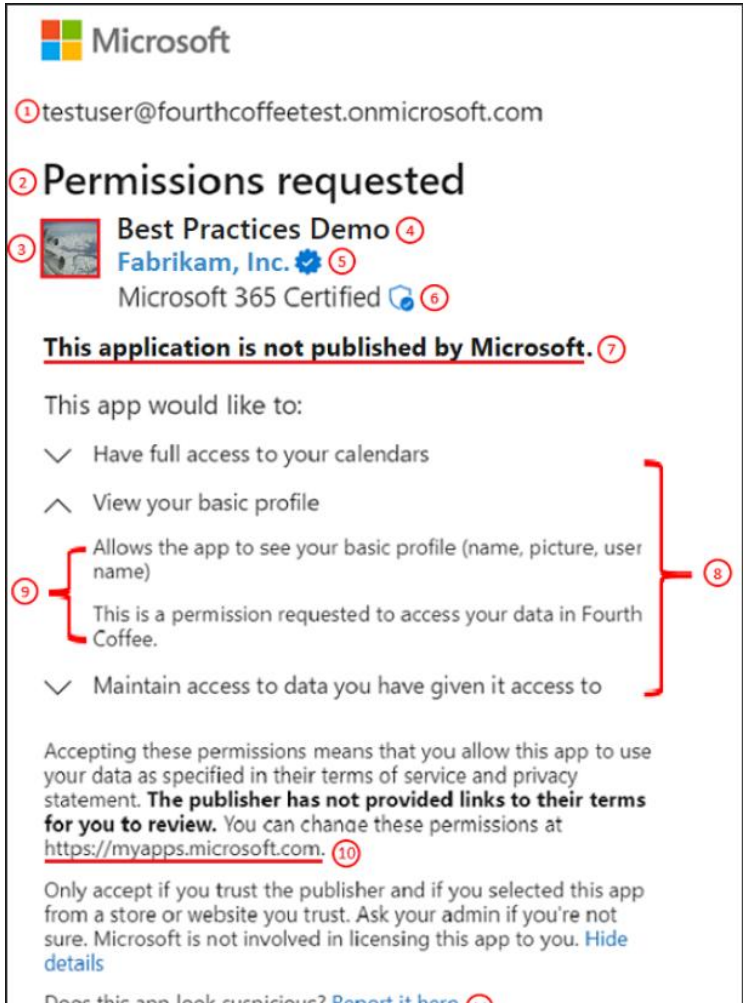
Start typing a display name or application (client) ID to filter these r...

Add filters

This account isn't listed as an owner of any applications in this directory.

View all applications in the directory

View all applications from personal account


Microsoft
1 testuser@fourthcoffeetest.onmicrosoft.com
2 Permissions requested
3
Best Practices Demo 4
Fabrikam, Inc. 5
Microsoft 365 Certified 6
This application is not published by Microsoft. 7
This app would like to:
Have full access to your calendars
View your basic profile
9
Allows the app to see your basic profile (name, picture, user name)
This is a permission requested to access your data in Fourth Coffee.
8
Maintain access to data you have given it access to
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. The publisher has not provided links to their terms for you to review. You can change these permissions at https://myapps.microsoft.com. 10
Only accept if you trust the publisher and if you selected this app from a store or website you trust. Ask your admin if you're not sure. Microsoft is not involved in licensing this app to you. Hide details

app-databricks | API permissions

Search (Ctrl+/)

Overview
Quickstart
Integration assistant

Manage

Branding & properties
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API
App roles
Owners
Roles and administrators
Manifest

Refresh | Got feedback?

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app
reflect the value in your organization, or in organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured per
all the permissions the application needs. Learn more about permissions and consent

Add a permission | Grant admin consent for Default Directory

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	

To view and manage permissions and user consent, try Enterprise applications.

Secure Networking

- Plan and implement security for virtual networks
- Plan and implement security for private access to Azure resources
- Plan and implement security for public access to Azure resources

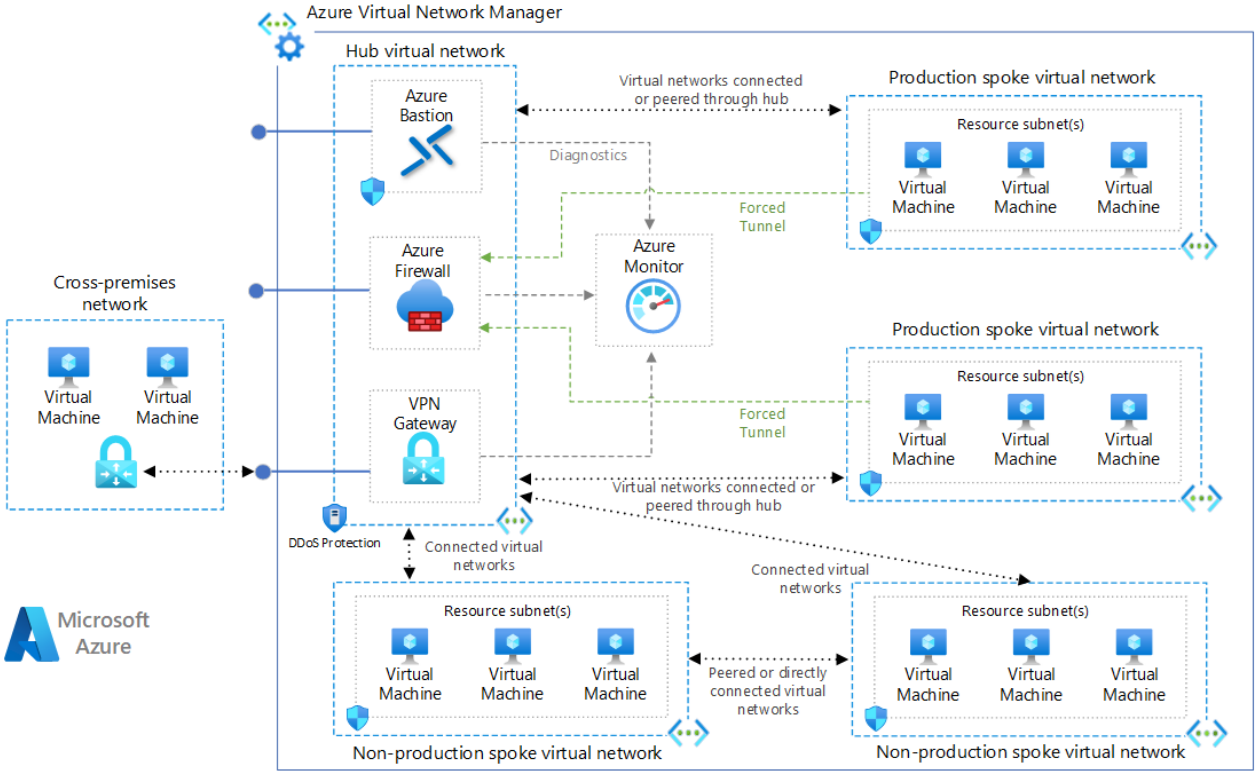
Poll: Which resource ensures that outbound VNET traffic is routed through Azure Firewall first?

- Network Security Groups (NSGs)
- Route Tables (UDR)
- Web Application Firewall (WAF)
- Azure VNET Peering

Plan and implement security for virtual networks

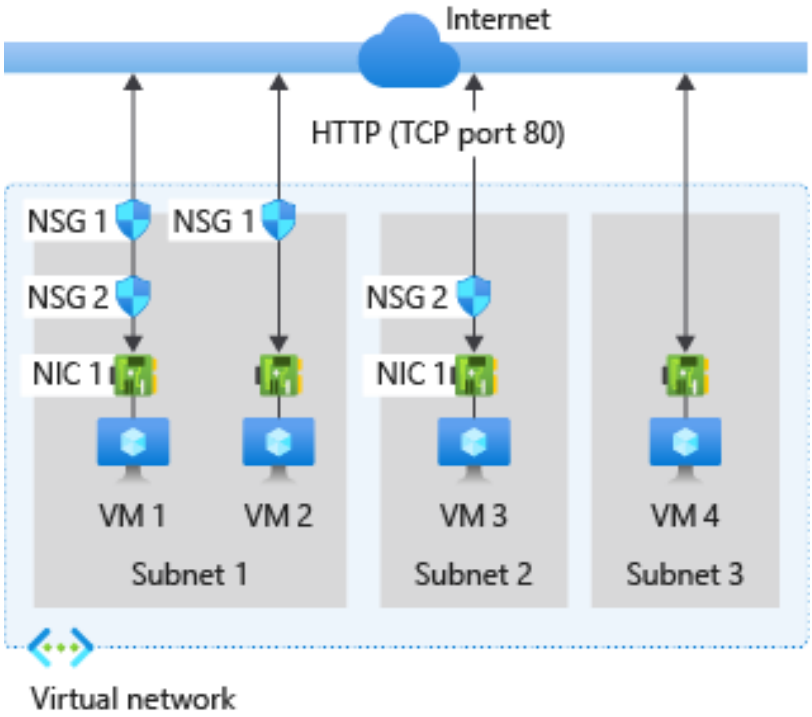
- Plan and implement Network Security Groups (NSGs) and Application Security Groups (ASGs)
- Manage virtual networks by using Azure Virtual Network Manager [see 1]
- Plan and implement user-defined routes (UDRs)
- Plan and implement VNET peering or VPN gateway
- Plan and implement Virtual WAN, including secured virtual hub
- Secure VPN connectivity, including point-to-site and site-to-site
- Implement encryption over ExpressRoute
- Configure firewall settings on PaaS resources [see 1, 2, 3]
- Monitor network security by using Network Watcher, including NSG flow logging

Azure Network Security Groups (NSGs)



https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli

Azure Network Security Groups (NSGs)



https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works

UDR (User-defined Routes)

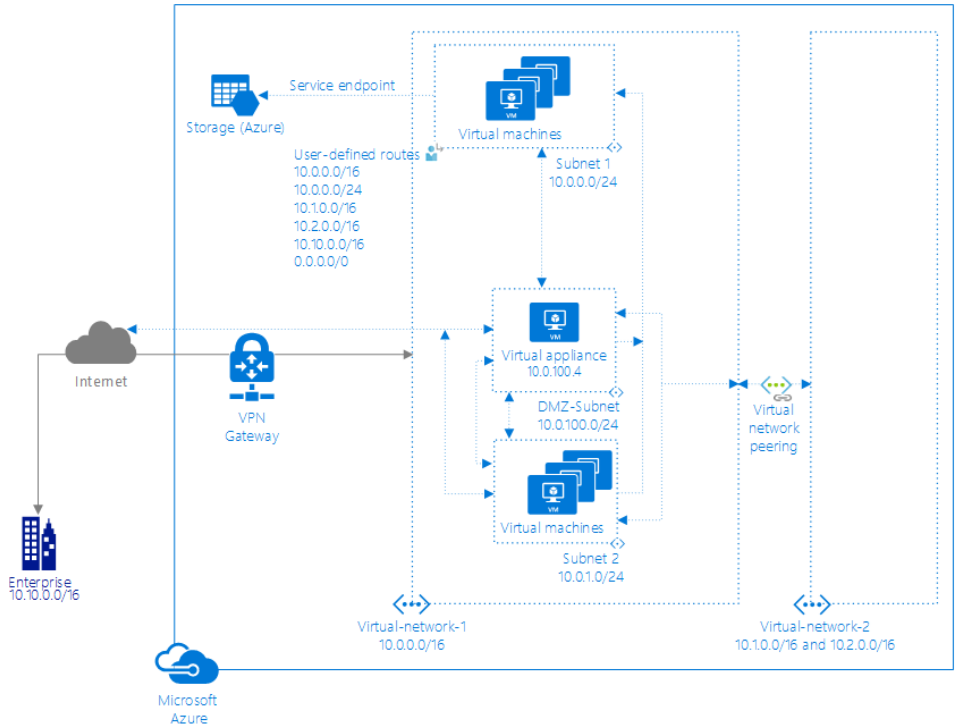
System routes

Azure automatically creates system routes and assigns the routes to each subnet in a virtual network. You can't create system routes, nor can you remove system routes, but you can override some system routes with custom routes. Azure creates default system routes for each subnet, and adds more optional default routes to specific subnets, or every subnet, when you use specific Azure capabilities.

Default

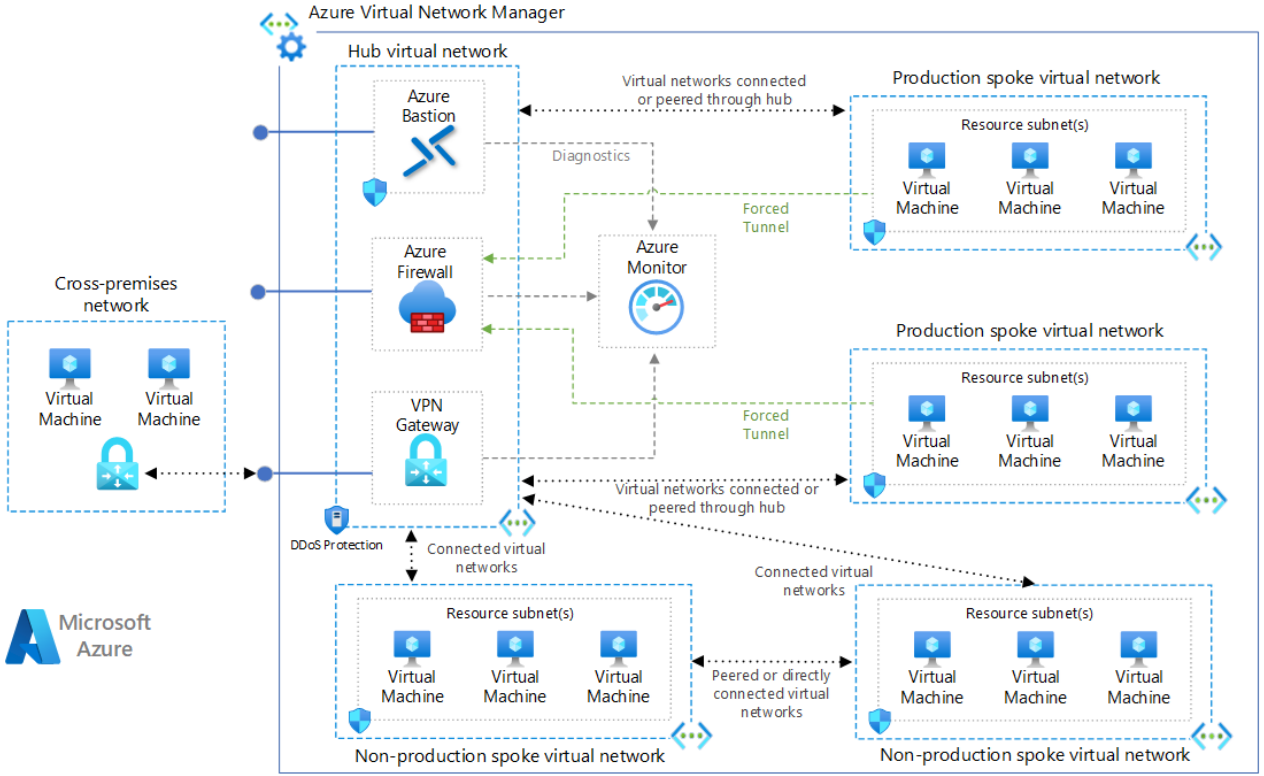
Each route contains an address prefix and next hop type. When traffic leaving a subnet is sent to an IP address within the address prefix of a route, the route that contains the prefix is the route Azure uses. Learn more about how Azure selects a route when multiple routes contain the same prefixes, or overlapping prefixes. Whenever a virtual network is created, Azure automatically creates the following default system routes for each subnet within the virtual network:

Source	Address prefixes	Next hop type
Default	Unique to the virtual network	Virtual network
Default	0.0.0.0/0	Internet
Default	10.0.0.0/8	None
Default	172.16.0.0/12	None
Default	192.168.0.0/16	None
Default	100.64.0.0/10	None



https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

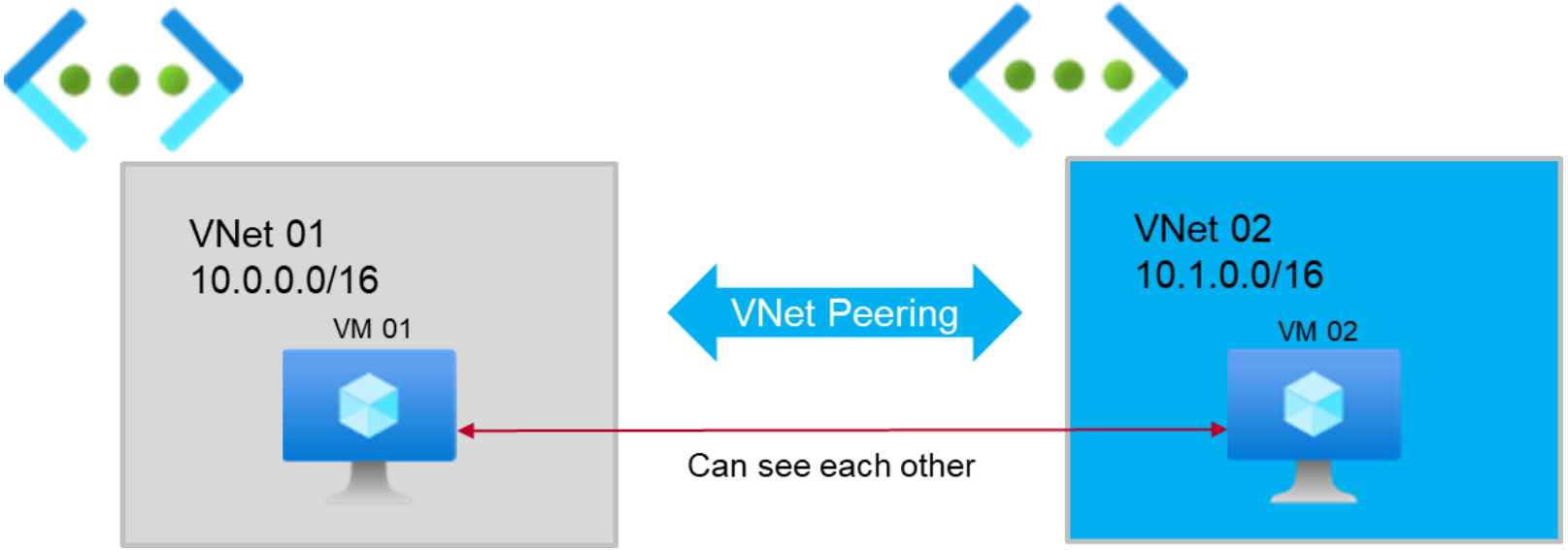
Azure Firewall Forced Tunneling



https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli

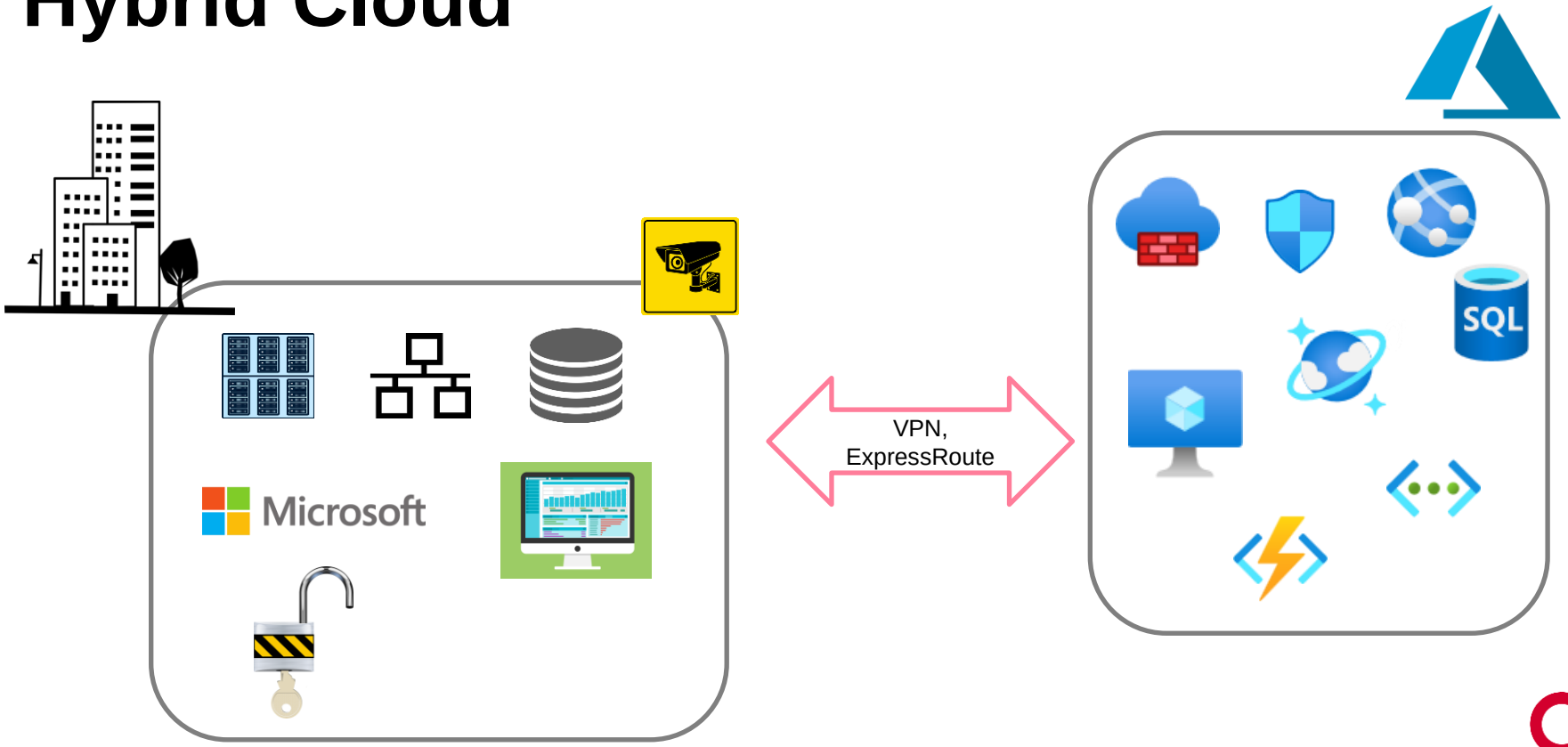
https://learn.microsoft.com/en-us/azure/firewall/forced-tunneling

VNet Peering



https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

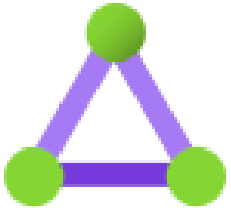
Hybrid Cloud



Connecting Other Networks to Azure

Microsoft allows you to connect your on-premises networks to Azure using a few options.

VPN gateway

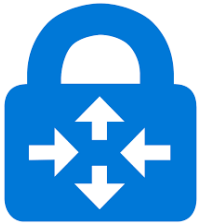


ExpressRoute

https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/

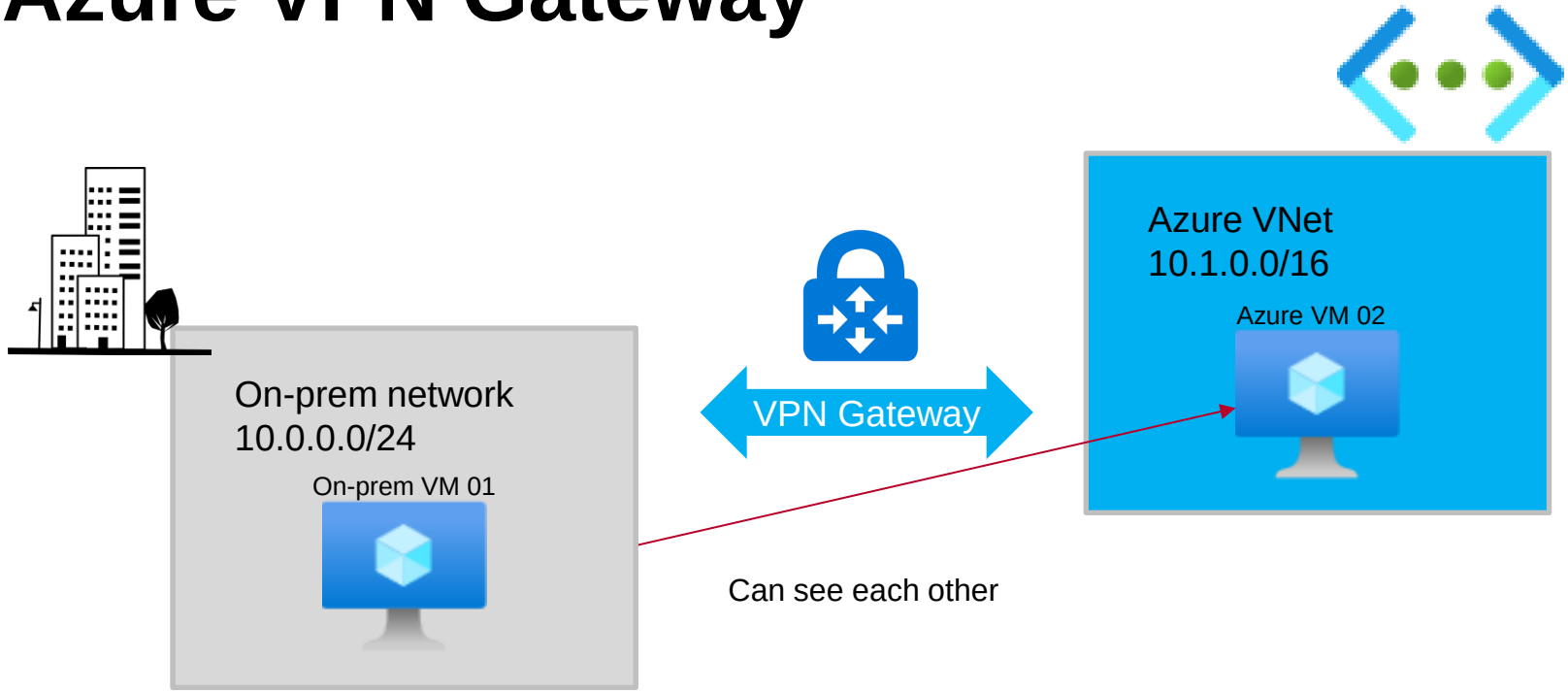
Azure VPN Gateway

- A virtual network gateway that sends encrypted traffic between an Azure virtual network (VNet) and an on-premises network
- The encrypted traffic goes over the public Internet.



https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

Azure VPN Gateway



https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

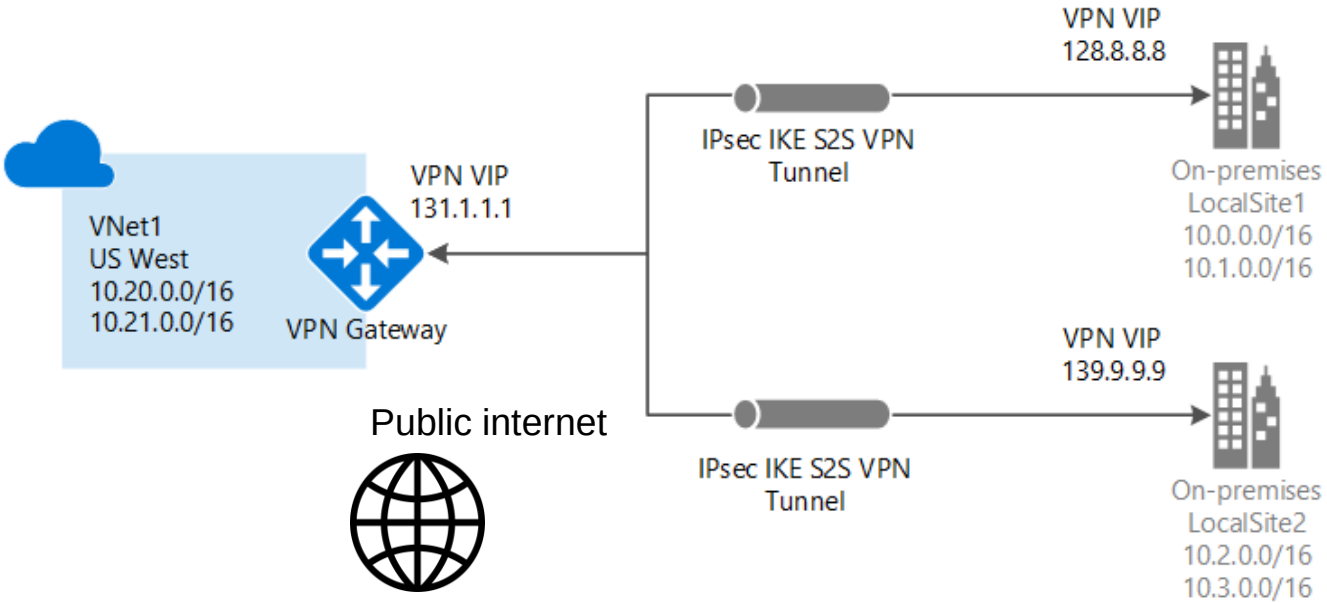
VPN Connection Types

Point-to-Site VPN

Site-to-Site VPN

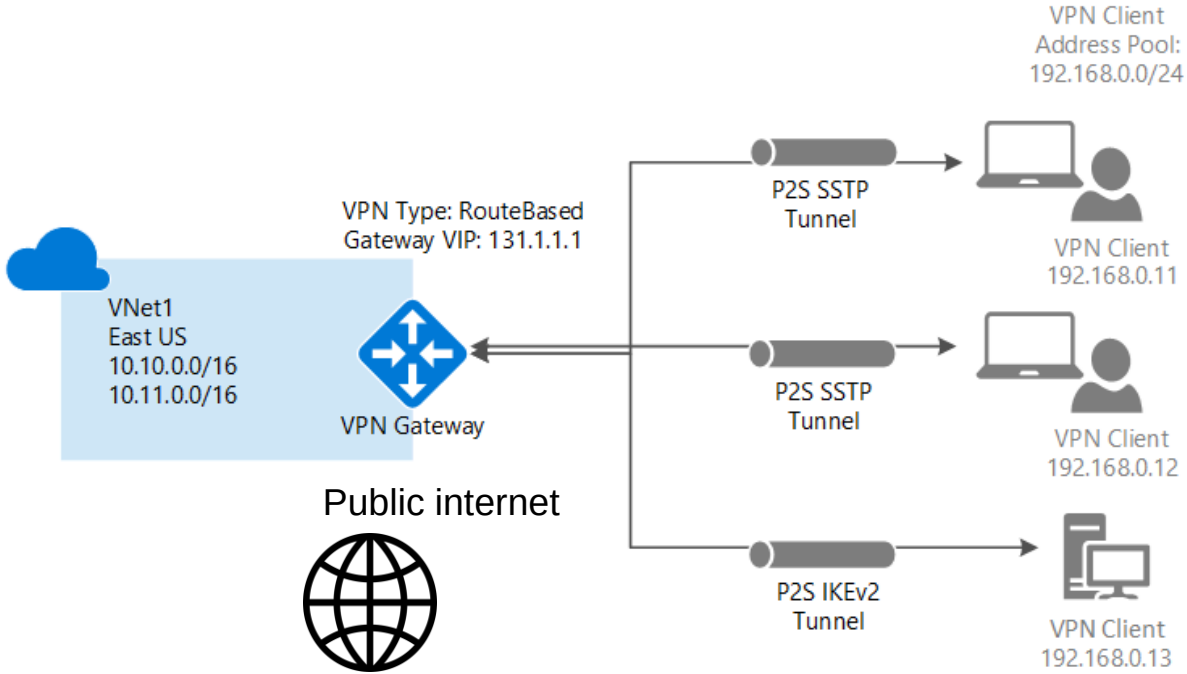
https://learn.microsoft.com/en-us/azure/vpn-gateway/design

Site-to-Site VPN



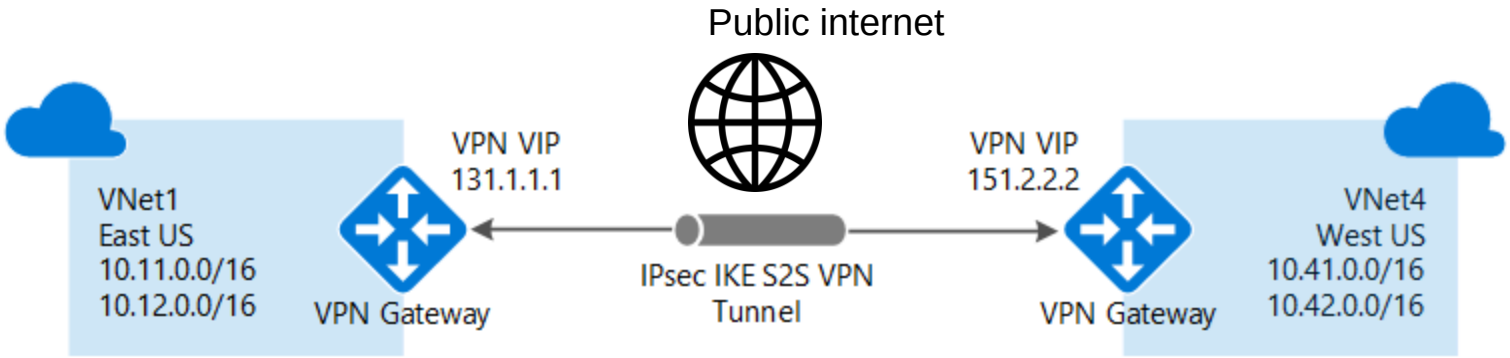
https://learn.microsoft.com/en-us/azure/vpn-gateway/design#s2smulti

Point-to-Site VPN



https://learn.microsoft.com/en-us/azure/vpn-gateway/design#P2S

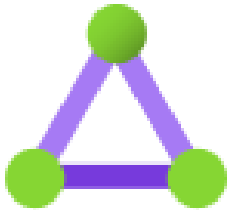
VNet-to-VNet Connections



https://learn.microsoft.com/en-us/azure/vpn-gateway/design#V2V

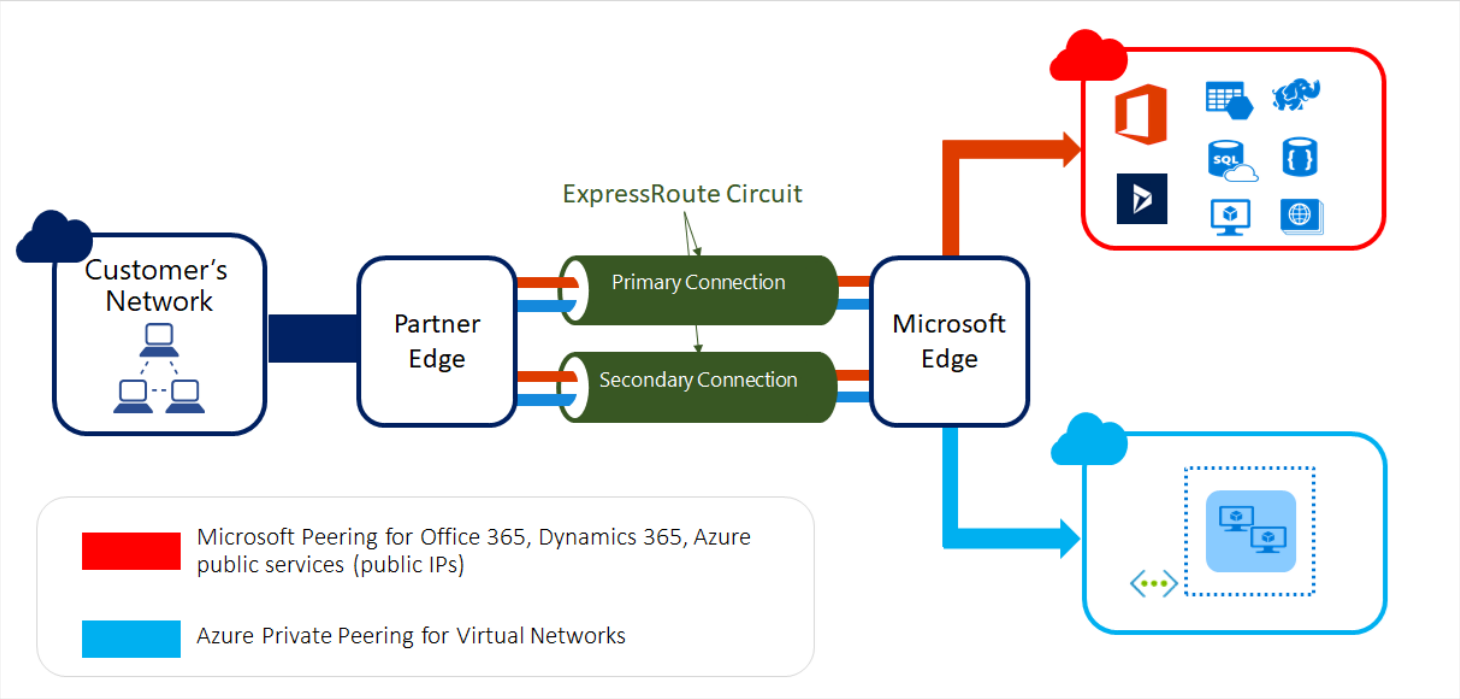
Azure ExpressRoute

- Enables you to extend your on-premises networks into Azure.
- The connection is private (not going over public internet)
- The help of a connectivity provider is required



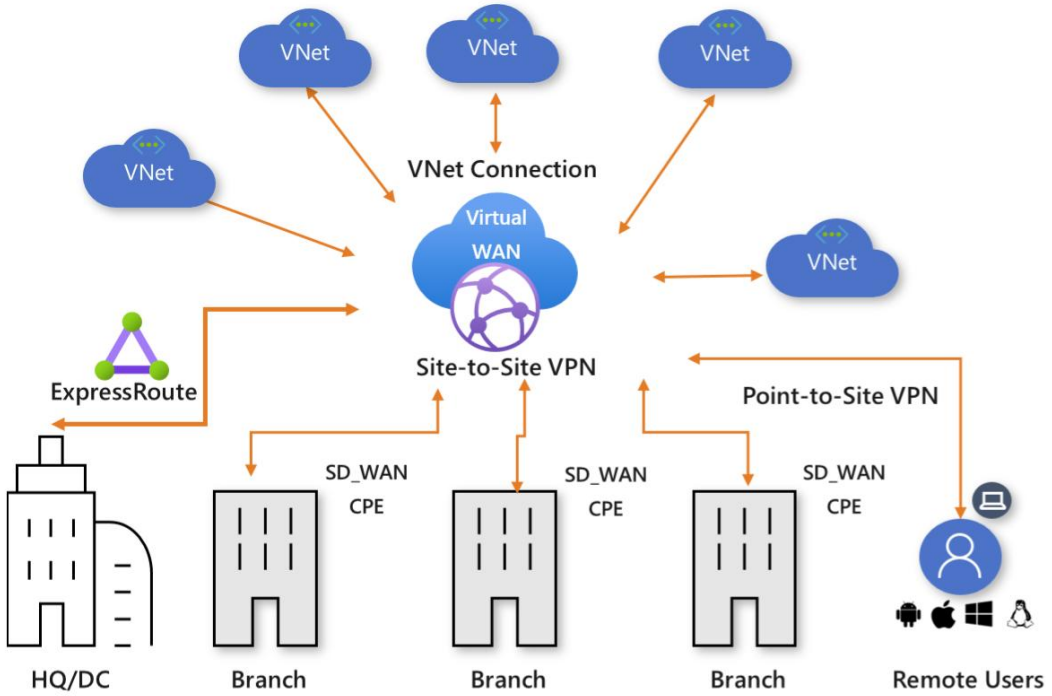
https://learn.microsoft.com/en-us/azure/expressroute/expressroute-introduction

Azure ExpressRoute



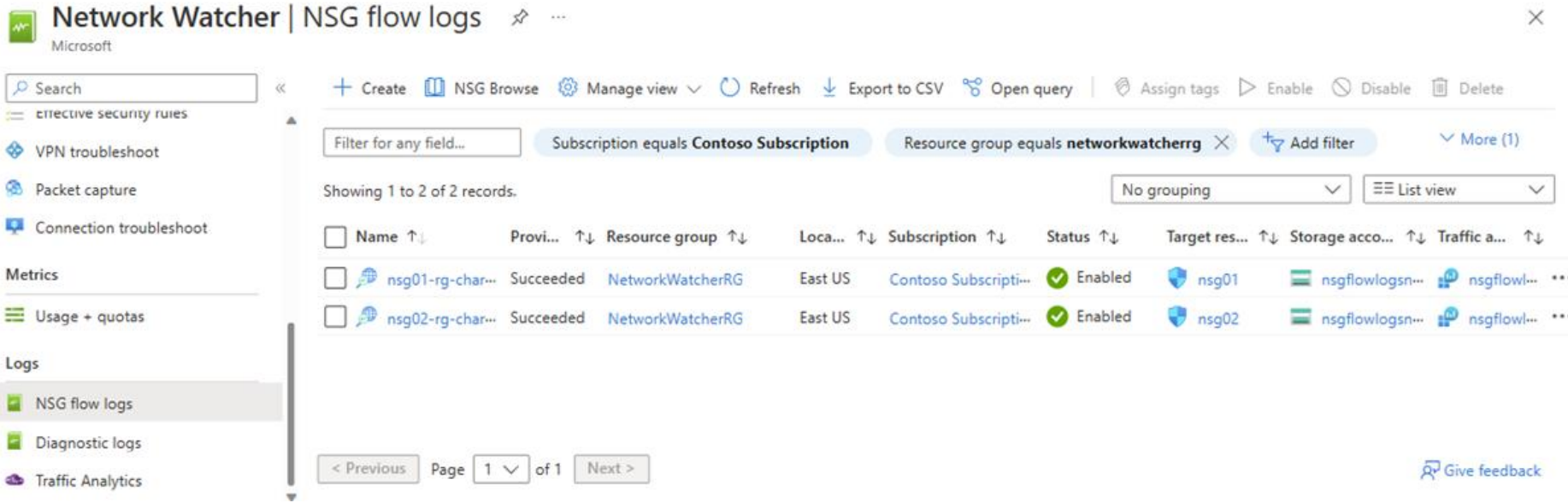
https://learn.microsoft.com/en-us/azure/expressroute/expressroute-introduction
https://learn.microsoft.com/en-us/azure/expressroute/expressroute-locations

Azure Virtual WAN



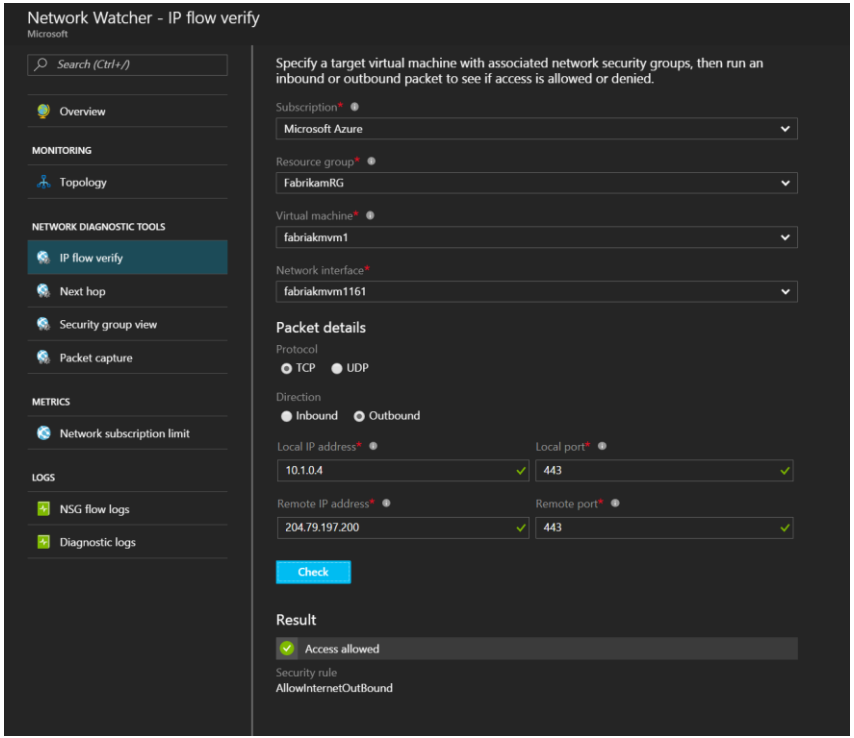
https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about

Azure Network Security Groups Flow Logs



https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview

Azure Network Security Groups Flow Logs



https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

Poll: Which Azure resource enables secure access to services over the Microsoft backbone network without exposing them to the public internet?

- Azure VPN Gateway
- Azure Private Endpoint
- Azure Public IP
- Azure Load Balancer

Plan and implement security for private access to Azure resources

- Plan and implement virtual network Service Endpoints
- Plan and implement Private Endpoints
- Plan and implement Private Link services
- Plan and implement network integration for Azure App Service and Azure Functions
- Plan and implement network security configurations for an App Service Environment (ASE)
- Plan and implement network security configurations for an Azure SQL Managed Instance

Note

Microsoft recommends use of Azure Private Link and private endpoints for secure and private access to services hosted on the Azure platform. Azure Private Link provisions a network interface into a virtual network of your choosing for Azure services such as Azure Storage or Azure SQL. For more information, see Azure Private Link and What is a private endpoint?.

Service Endpoints

Allows clients and users to reach out to an Azure service

Public Endpoint

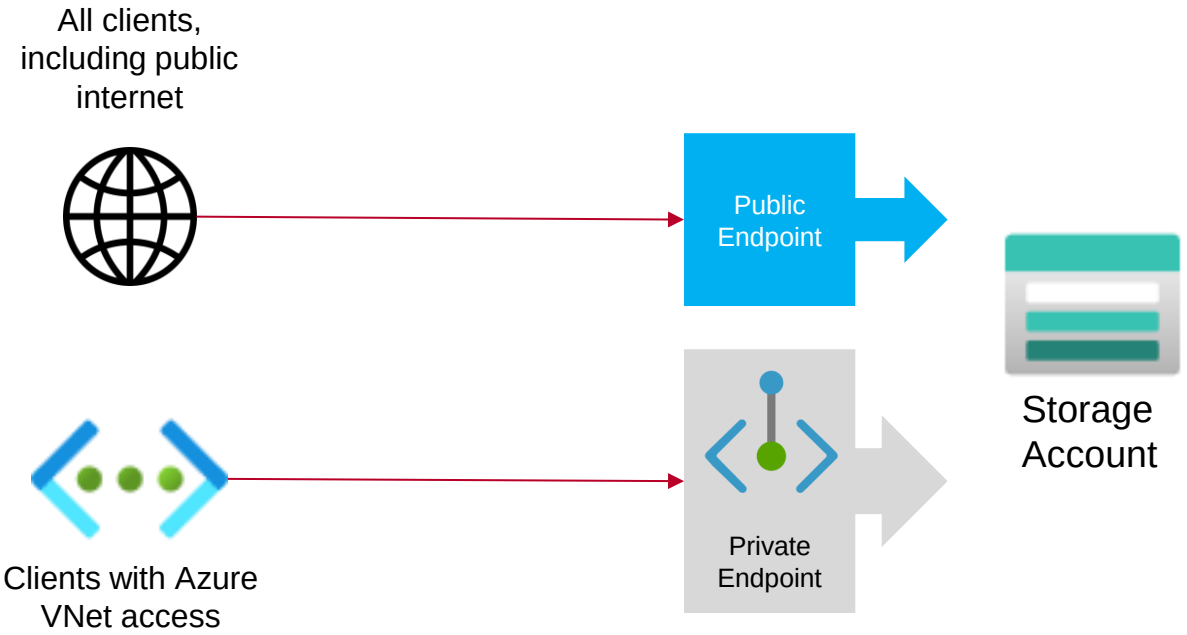
Private Endpoint

Azure Private Endpoint

- A network interface that uses a private IP address from your VNet
- Brings your service to an Azure virtual network (VNet)
- Public clients will not see your resource anymore
- The traffic goes over Microsoft private backbone network

https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-overview

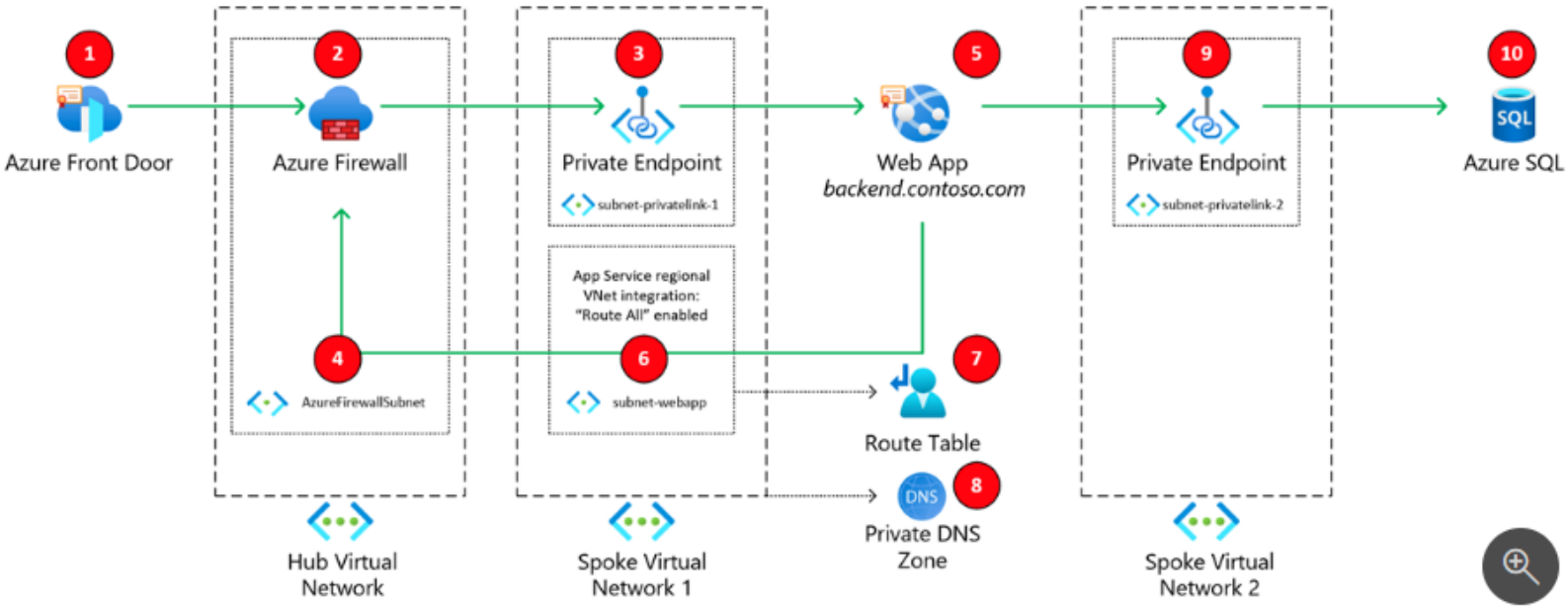
Service Endpoints



Azure Private Endpoint Support

- Azure App Configuration
- Azure Automation
- Azure Cosmos DB
- Azure Batch
- Azure Cache for Redis
- Azure Cache for Redis Enterprise
- Azure Cognitive Services
- Azure Managed Disks
- Azure Container Registry
- Azure Kubernetes Service - Kubernetes API
- Azure Data Factory
- Azure Data Explorer
- Azure Database for MariaDB
- Azure Database for MySQL
- Azure Database for PostgreSQL - Single server
- Azure Device Provisioning Service
- Azure IoT Hub
- Azure IoT Central
- Azure Digital Twins
- Azure Event Grid
- Azure Event Grid
- Azure Event Hub
- Azure HDInsight
- Azure API for FHIR (Fast Healthcare Interoperability Resources)
- Azure Key Vault HSM (hardware security module)
- Azure Key Vault
- Azure Machine Learning
- Azure Migrate
- Application Gateway
- Private Link service (your own service)
- Power BI
- Microsoft Purview
- Microsoft Purview
- Azure Backup
- Azure Relay
- Azure Cognitive Search
- Azure Service Bus
- Azure SignalR Service
- Azure SignalR Service
- Azure SQL Database
- Azure Storage
- Azure File Sync
- Azure Synapse
- Azure Synapse Analytics
- Azure App Service
- Azure App Service
- Azure Static Web Apps
- Azure Media Services

https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-overview#private-link-resource


1
Azure Front Door
2
Azure Firewall
4
AzureFirewallSubnet
Hub Virtual Network
3
Private Endpoint
subnet-privatelink-1
App Service regional VNet integration: "Route All" enabled
6
subnet-webapp
Spoke Virtual Network 1
5
Web App
backend.contoso.com
7
Route Table
8
DNS
Private DNS Zone
9
Private Endpoint
subnet-privatelink-2
Spoke Virtual Network 2
10
SQL
Azure SQL

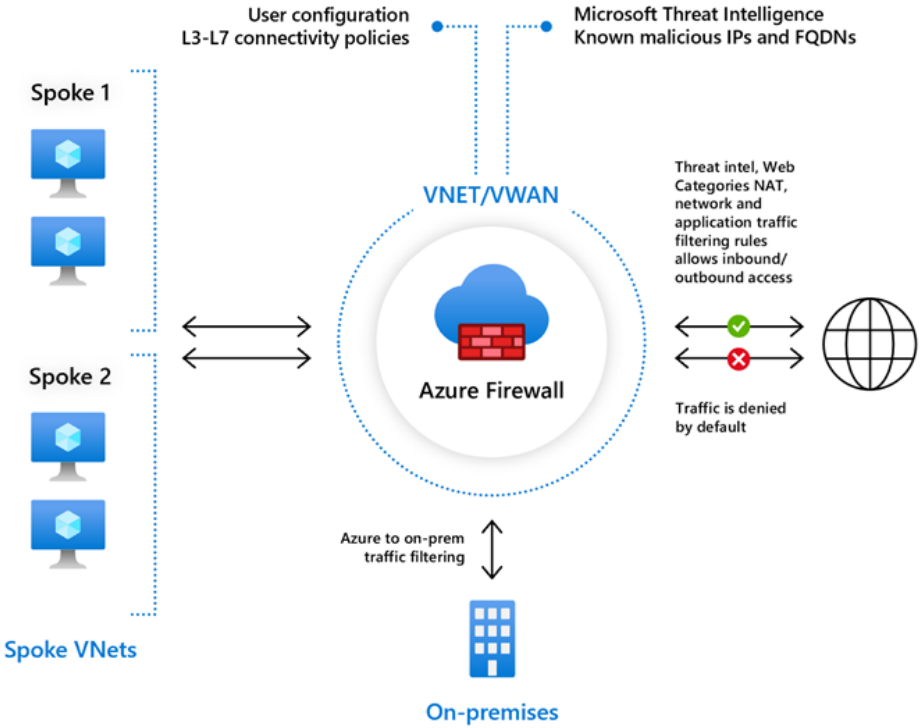
Poll: Which Azure service provides protection against common web vulnerabilities such as SQL injection and cross-site scripting (XSS)?

- Azure DDoS Protection
- Azure Firewall
- Web Application Firewall (WAF)
- Azure Traffic Manager

Plan and implement security for public access to Azure resources

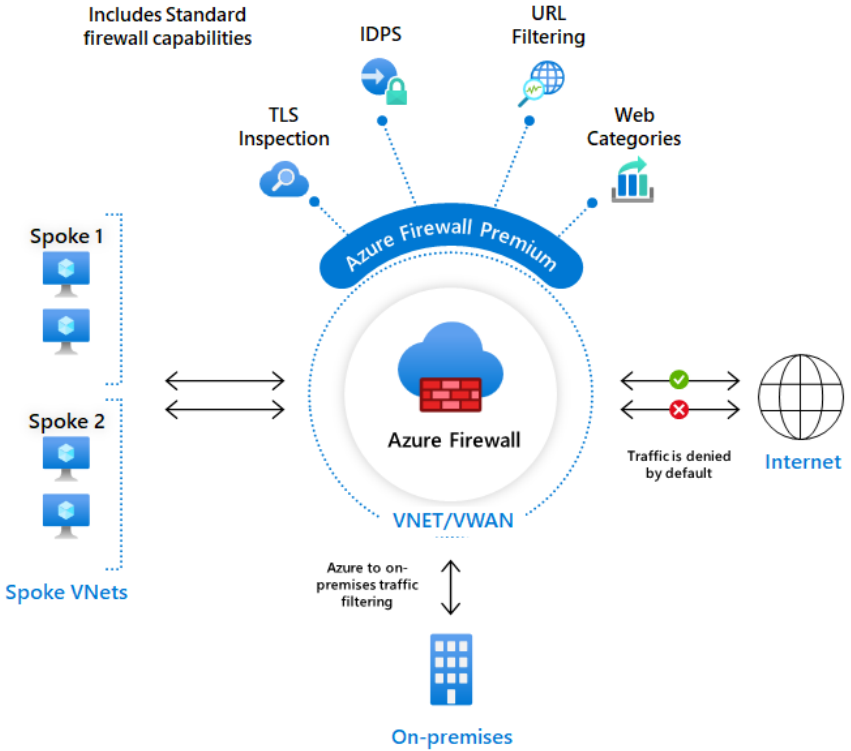
- Plan and implement TLS to applications, including Azure App Service and API Management
- Plan, implement, and manage an Azure Firewall, including Azure Firewall Manager and firewall policies
- Plan and implement an Azure Application Gateway
- Plan and implement an Azure Front Door, including Content Delivery Network (CDN)
- Plan and implement a Web Application Firewall (WAF)
- Recommend when to use Azure DDoS Protection Standard

Azure Firewall



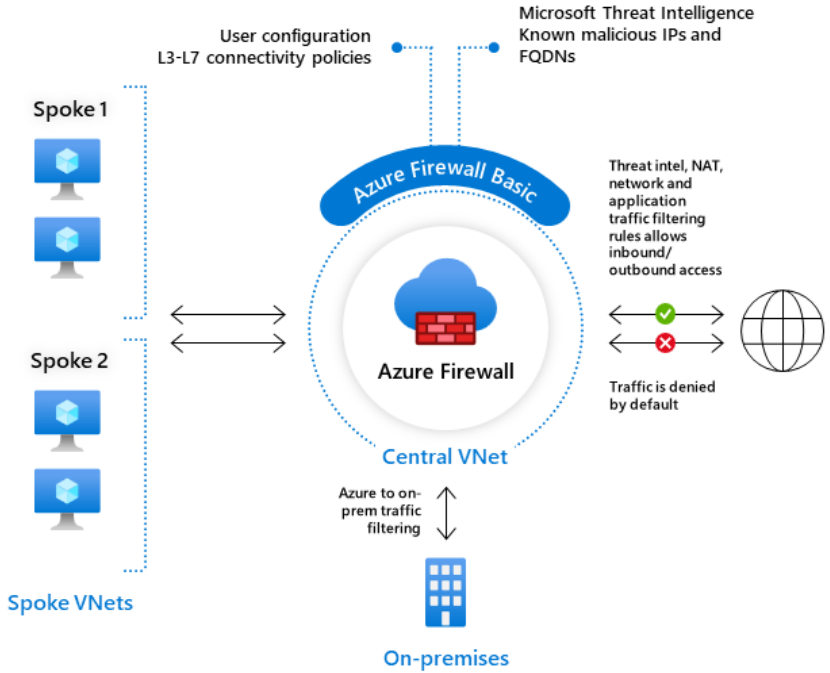
https://learn.microsoft.com/en-us/azure/firewall/overview

Azure Firewall Premium



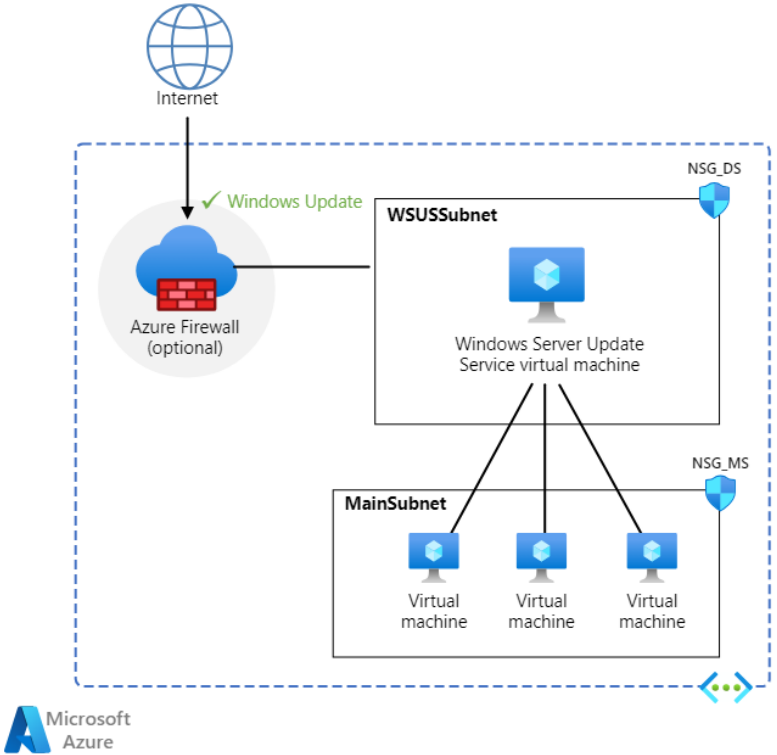
https://learn.microsoft.com/en-us/azure/firewall/overview

Azure Firewall Basic



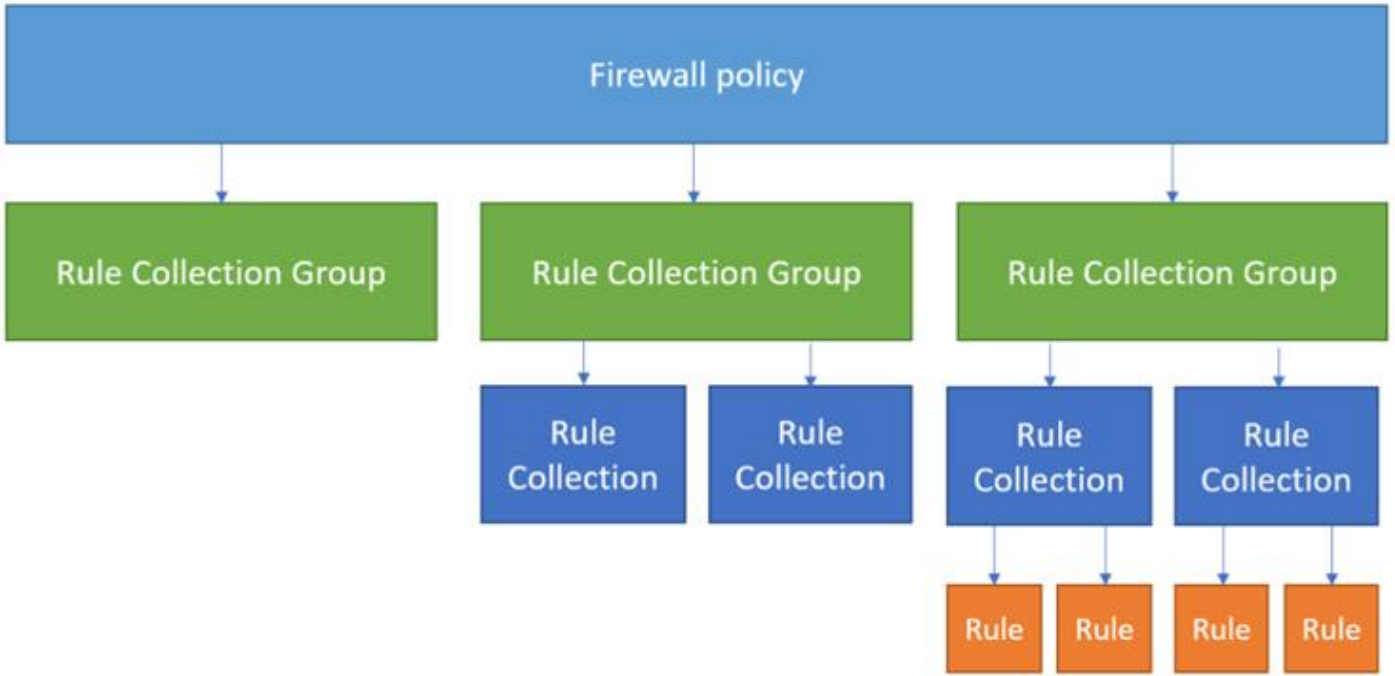
https://learn.microsoft.com/en-us/azure/firewall/overview

Azure Firewall



https://learn.microsoft.com/en-us/azure/architecture/example-scenario/wsus/

Azure Firewall Rules



- Set of Rule Collections

- Set of Rules
- Define Priority
- Determine Allow/Deny

- Define 5-Tuple traffic
- DNAT, Application, Network

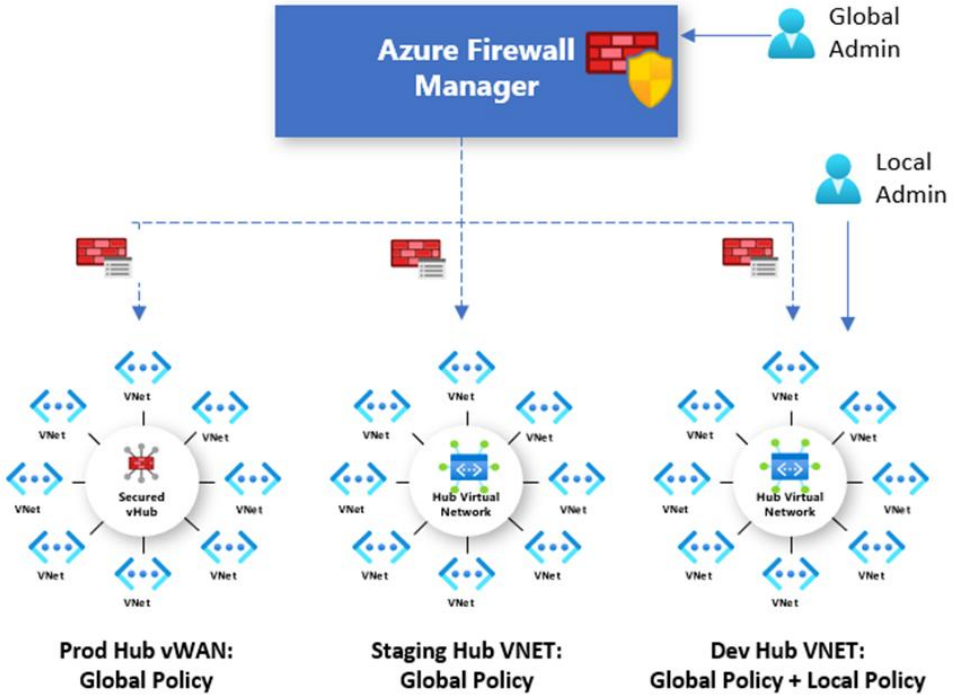
https://learn.microsoft.com/en-us/azure/firewall/policy-rule-sets

Azure Firewall Rules

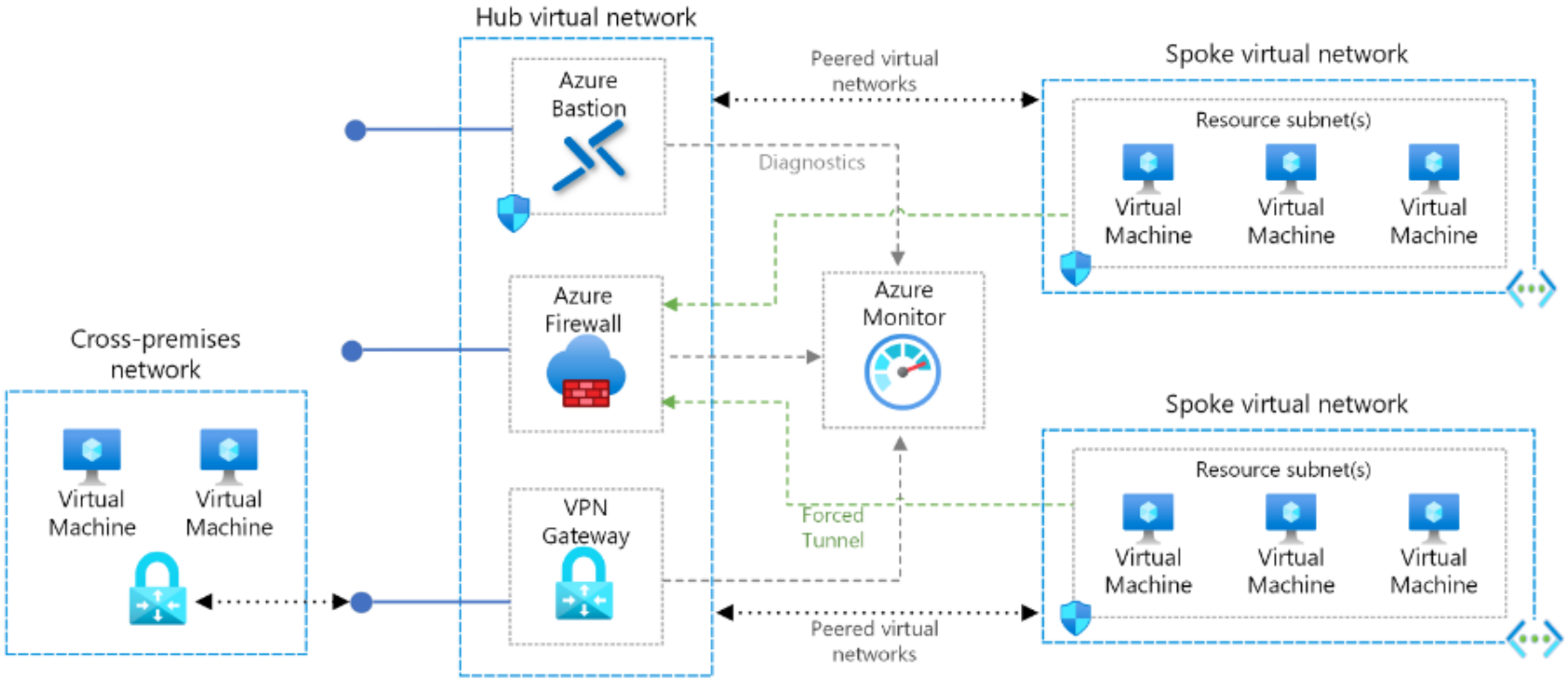
- DNAT
- Network
- Application

https://learn.microsoft.com/en-us/azure/firewall/policy-rule-sets

Azure Firewall (Manager) Policy



https://learn.microsoft.com/en-us/azure/firewall-manager/policy-overview



Microsoft Azure

Azure WAF (Web Application Firewall)

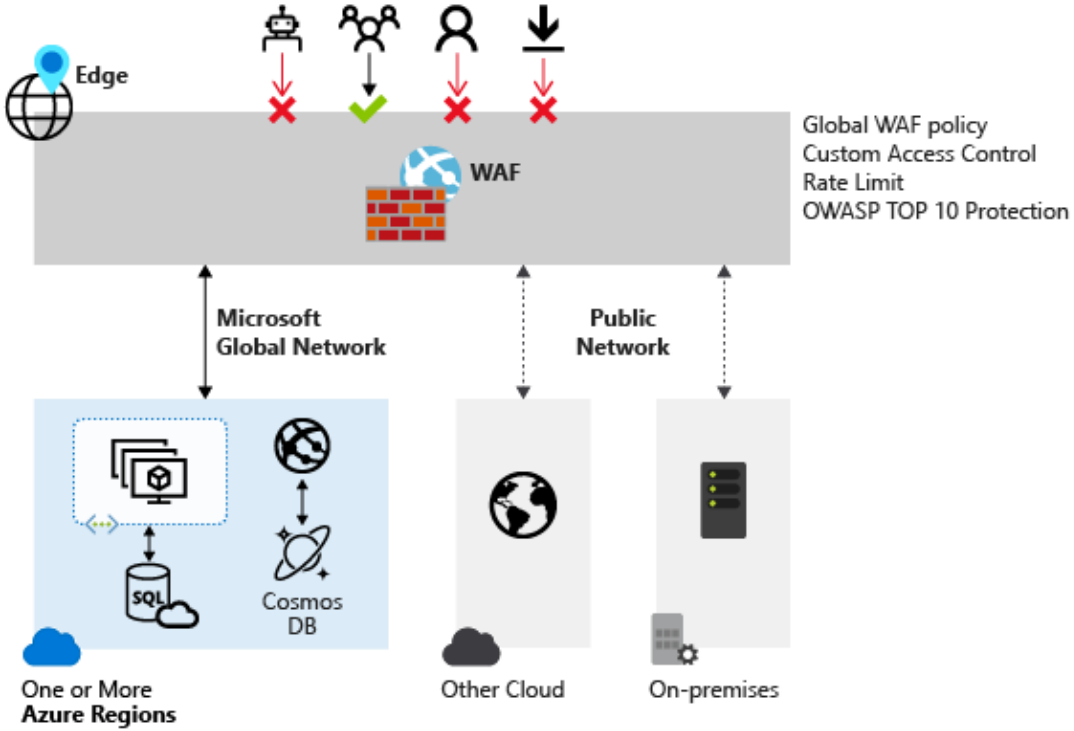
Front Door

Application Gateway

CDN

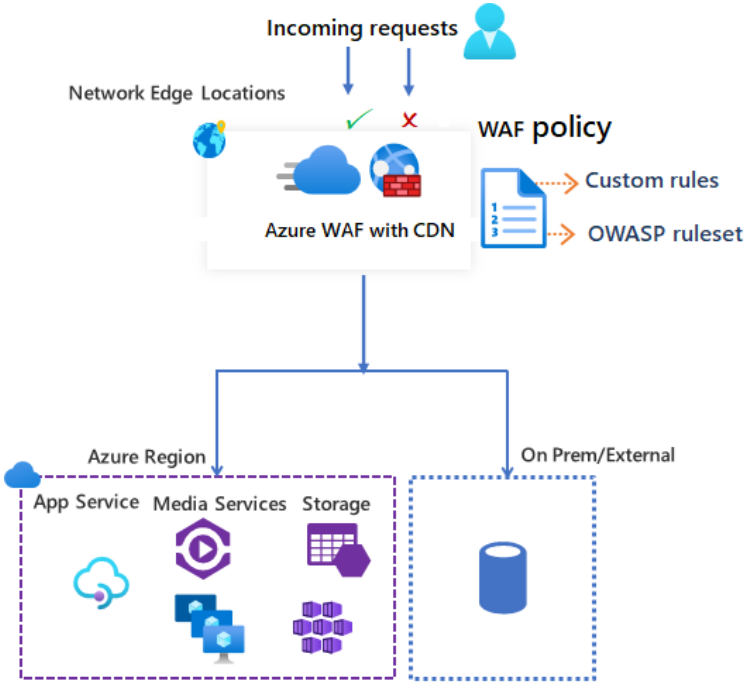
https://learn.microsoft.com/en-us/azure/web-application-firewall/overview

Azure WAF (Azure Front Door)



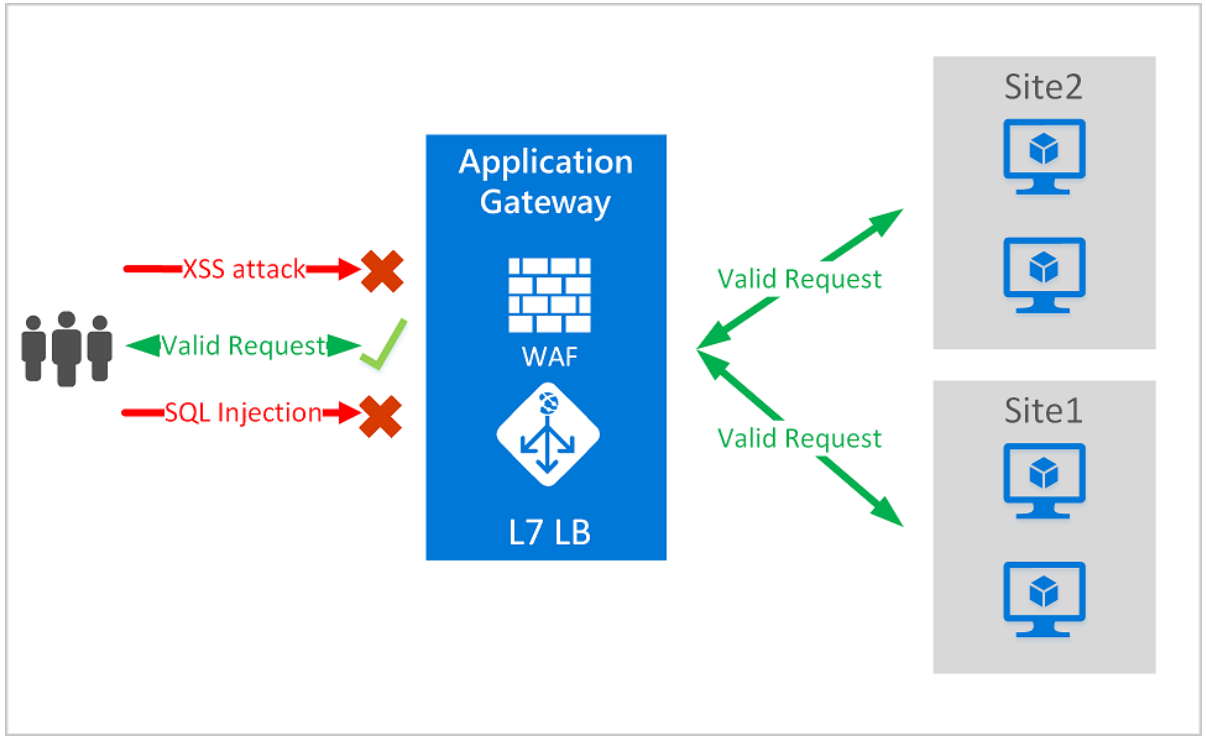
https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview

Azure WAF (Azure CDN)



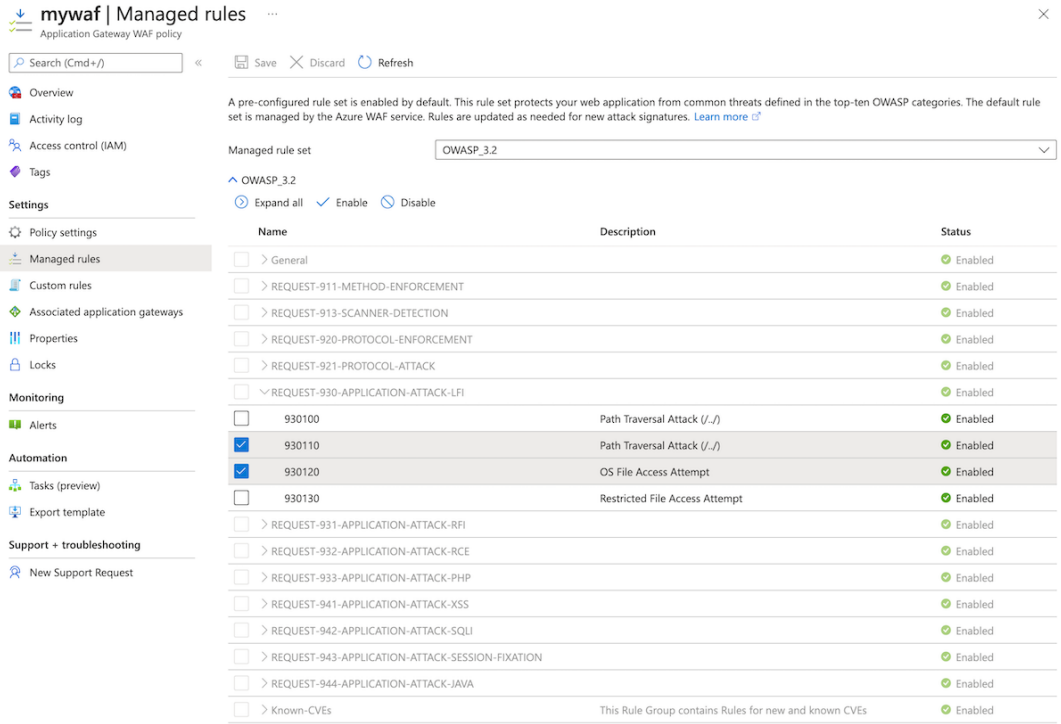
https://learn.microsoft.com/en-us/azure/web-application-firewall/cdn/cdn-overview

Azure WAF (Azure Application Gateway)



https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview

Azure WAF Managed Rules



https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/application-gateway-crs-rulegroups-rules?tabs=owasp32

Azure WAF Custom Rules

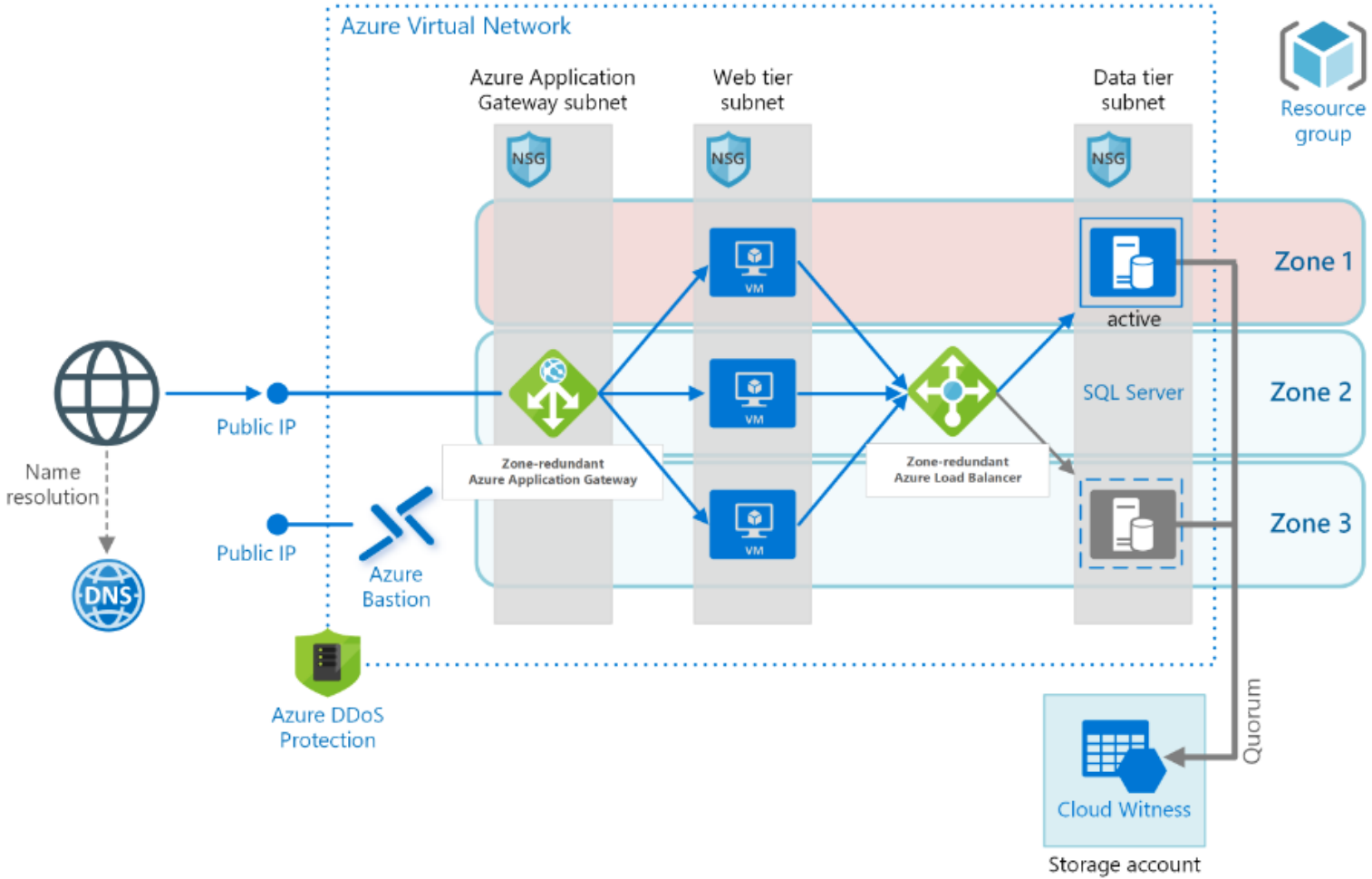
Azure PowerShell

Copy

```
$AllowRule = New-AzApplicationGatewayFirewallCustomRule `
    -Name example1 `
    -Priority 2 `
    -RuleType MatchRule `
    -MatchCondition $condition `
    -Action Allow `
    -State Enabled

$BlockRule = New-AzApplicationGatewayFirewallCustomRule `
    -Name example2 `
    -Priority 2 `
    -RuleType MatchRule `
    -MatchCondition $condition `
    -Action Block `
    -State Enabled
```

https://learn.microsoft.com/en-us/azure/web-application-firewall/ag/custom-waf-rules-overview


Azure Virtual Network
Azure Application Gateway subnet
Web tier subnet
Data tier subnet
Resource group
NSG
NSG
NSG
VM
VM
VM
active
SQL Server
Zone 1
Zone 2
Zone 3
Public IP
Name resolution
DNS
Public IP
Azure Bastion
Zone-redundant Azure Application Gateway
Zone-redundant Azure Load Balancer
Azure DDoS Protection
Quorum
Cloud Witness
Storage account

Day 2

Microsoft Azure Security Technologies Bootcamp

- Secure compute, storage, and databases (20-25%)
- Secure Azure using Microsoft Defender for Cloud and Microsoft Sentinel (30–35%)

Secure Compute, Storage, and Databases

- Plan and implement advanced security for compute
- Plan and implement security for storage
- Plan and implement security for Azure SQL Database and Azure SQL Managed Instance

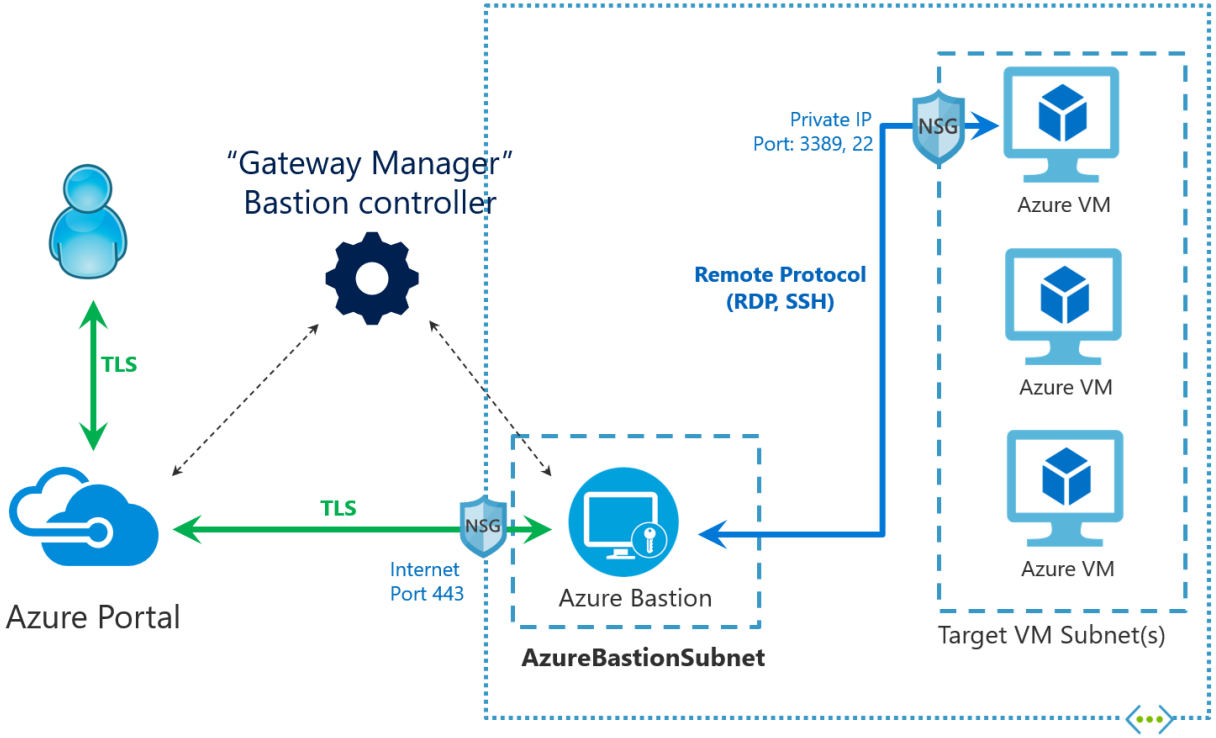
Poll: Which Azure service allows agentless RDP and SSH access to private VMs directly from a browser?

- Azure VPN Gateway
- Azure Bastion
- A jumpbox VM
- Azure Firewall

Plan and implement advanced security for compute

- Plan and implement remote access to public endpoints, including Azure Bastion and just-in-time JIT virtual machine (VM) access
- Configure network isolation for Azure Kubernetes Service (AKS)
- Secure and monitor AKS
- Configure authentication for AKS
- Configure security monitoring for Azure Container Instances (ACIs)
- Configure security monitoring for Azure Container Apps (ACAs)
- Manage access to Azure Container Registry (ACR) [Also see 1]
- Configure disk encryption, including Azure Disk Encryption (ADE), encryption as host, and confidential disk encryption
- Recommend security configurations for Azure API Management

NSG Access and Azure Bastion



https://learn.microsoft.com/en-us/azure/bastion/bastion-nsg

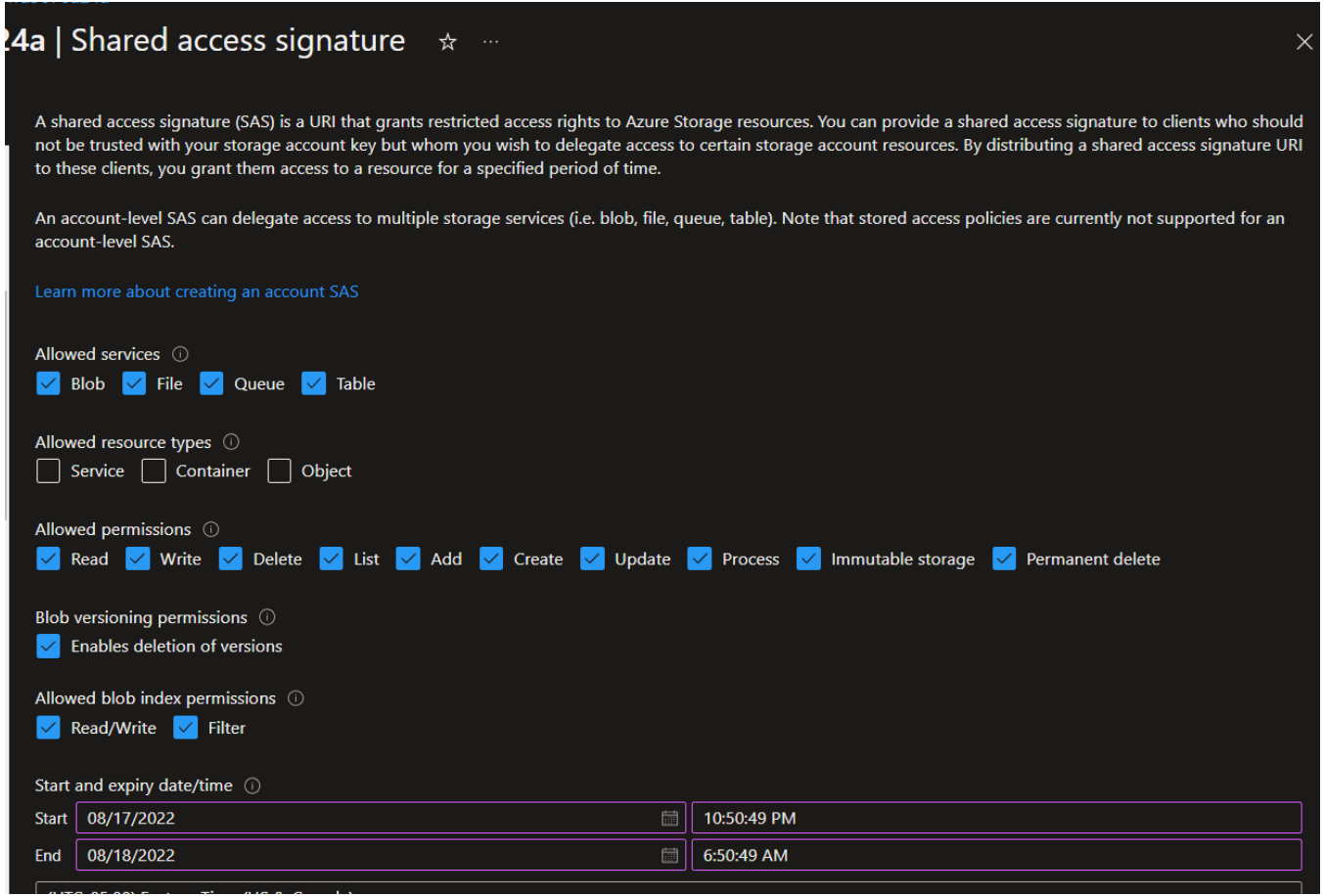
Poll: Which Azure feature ensures that blob storage data cannot be modified or deleted for a specified retention period?

- Azure Immutable Storage
- Azure Blob Soft Delete
- Azure Backup
- Azure Storage replication

Plan and implement security for storage

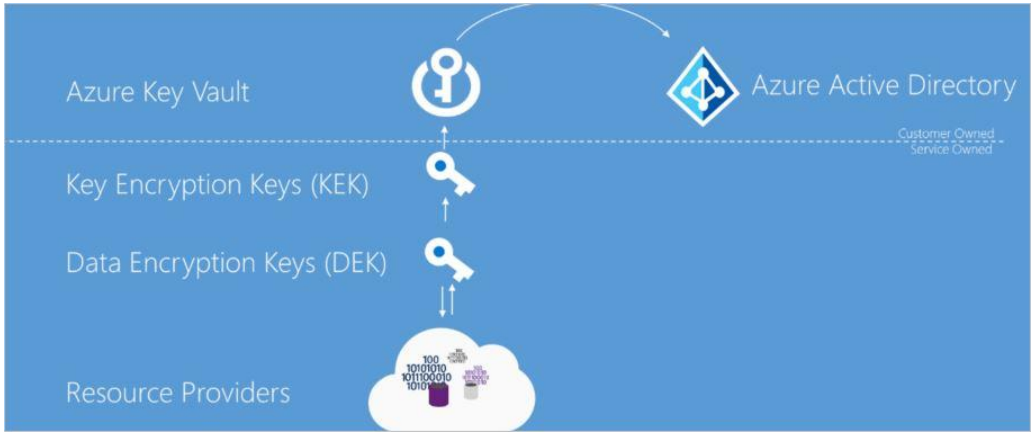
- Configure access control for storage accounts
- Manage storage account access keys
- Select and configure an appropriate method for access to Azure Files
- Select and configure an appropriate method for access to Azure Blob Storage
- Select and configure appropriate methods for protecting against data security threats, including soft delete, backups, versioning, and immutable storage [Also see 1]
- Configure Bring your own key (BYOK)
- Enable double encryption at the Azure Storage infrastructure level

Azure artifact	Shared Key (storage account key)	Shared access signature (SAS)	Azure Active Directory (Azure AD)	On-premises Active Directory Domain Services	Anonymous public read access	Storage Local Users
Azure Blobs	Supported	Supported	Supported	Not supported	Supported	Supported, only for SFTP
Azure Files (SMB)	Supported	Not supported	Supported, only with AAD Domain Services	Supported, credentials must be synced to Azure AD	Not supported	Supported
Azure Files (REST)	Supported	Supported	Not supported	Not supported	Not supported	Not supported
Azure Queues	Supported	Supported	Supported	Not Supported	Not supported	Not supported
Azure Tables	Supported	Supported	Supported	Not supported	Not supported	Not supported


24a | Shared access signature
A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources. You can provide a shared access signature to clients who should not be trusted with your storage account key but whom you wish to delegate access to certain storage account resources. By distributing a shared access signature URI to these clients, you grant them access to a resource for a specified period of time.
An account-level SAS can delegate access to multiple storage services (i.e. blob, file, queue, table). Note that stored access policies are currently not supported for an account-level SAS.
Learn more about creating an account SAS
Allowed services
Blob
File
Queue
Table
Allowed resource types
Service
Container
Object
Allowed permissions
Read
Write
Delete
List
Add
Create
Update
Process
Immutable storage
Permanent delete
Blob versioning permissions
Enables deletion of versions
Allowed blob index permissions
Read/Write
Filter
Start and expiry date/time
Start
08/17/2022
10:50:49 PM
End
08/18/2022
6:50:49 AM

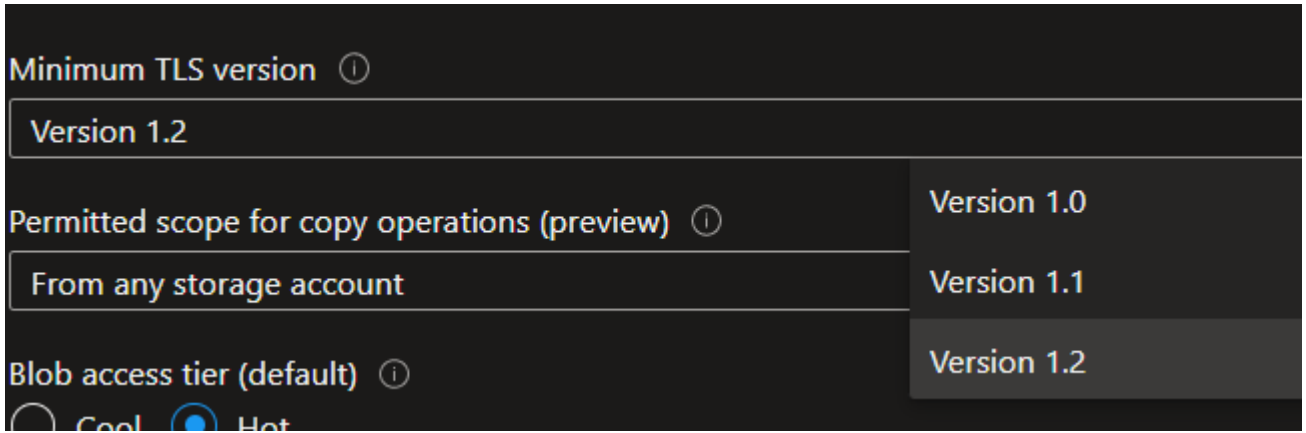
Configure Encryption at Rest

- Azure Data Encryption at rest
- Azure Storage encryption for data at rest
- Data encryption in Azure Cosmos DB



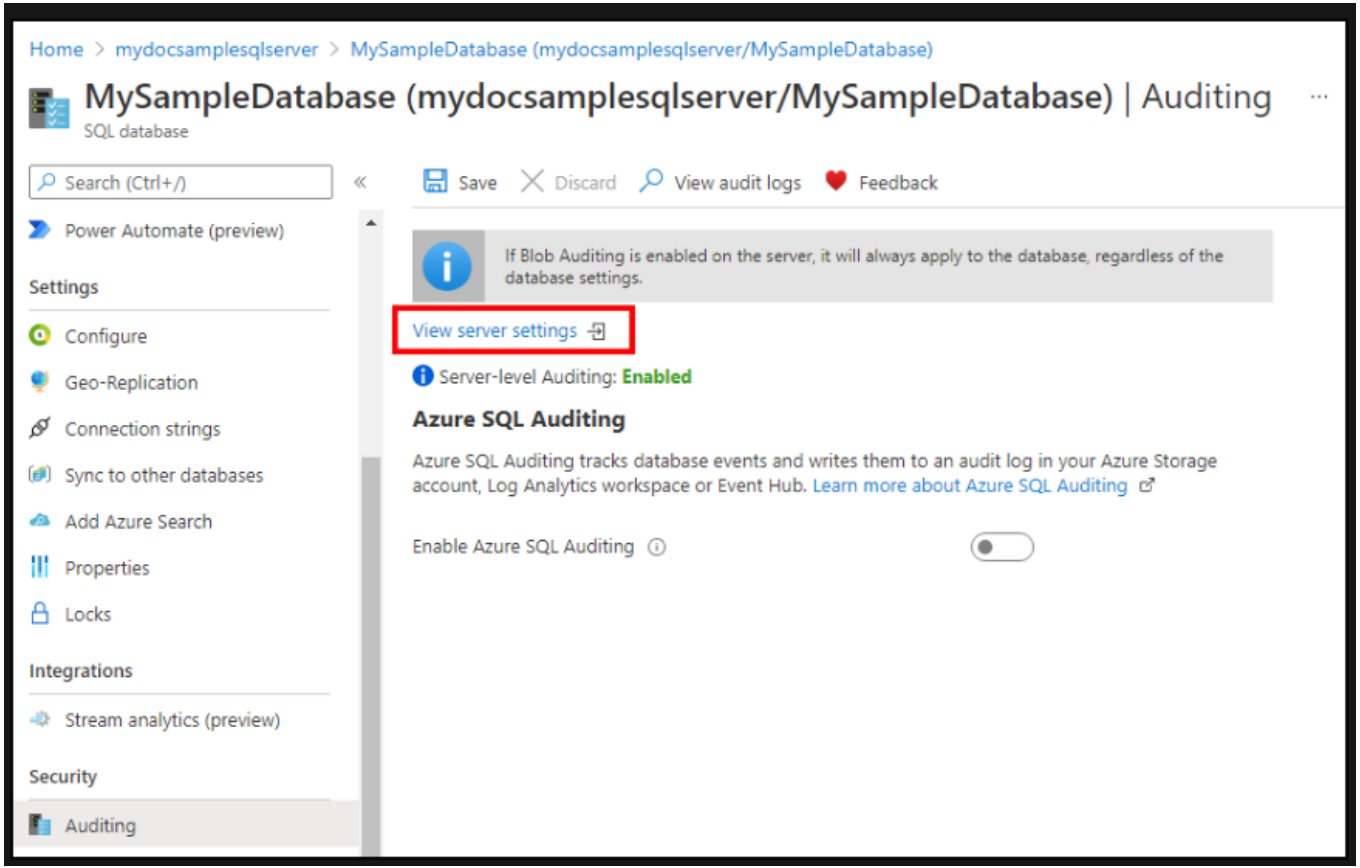
Configure Encryption in Transit

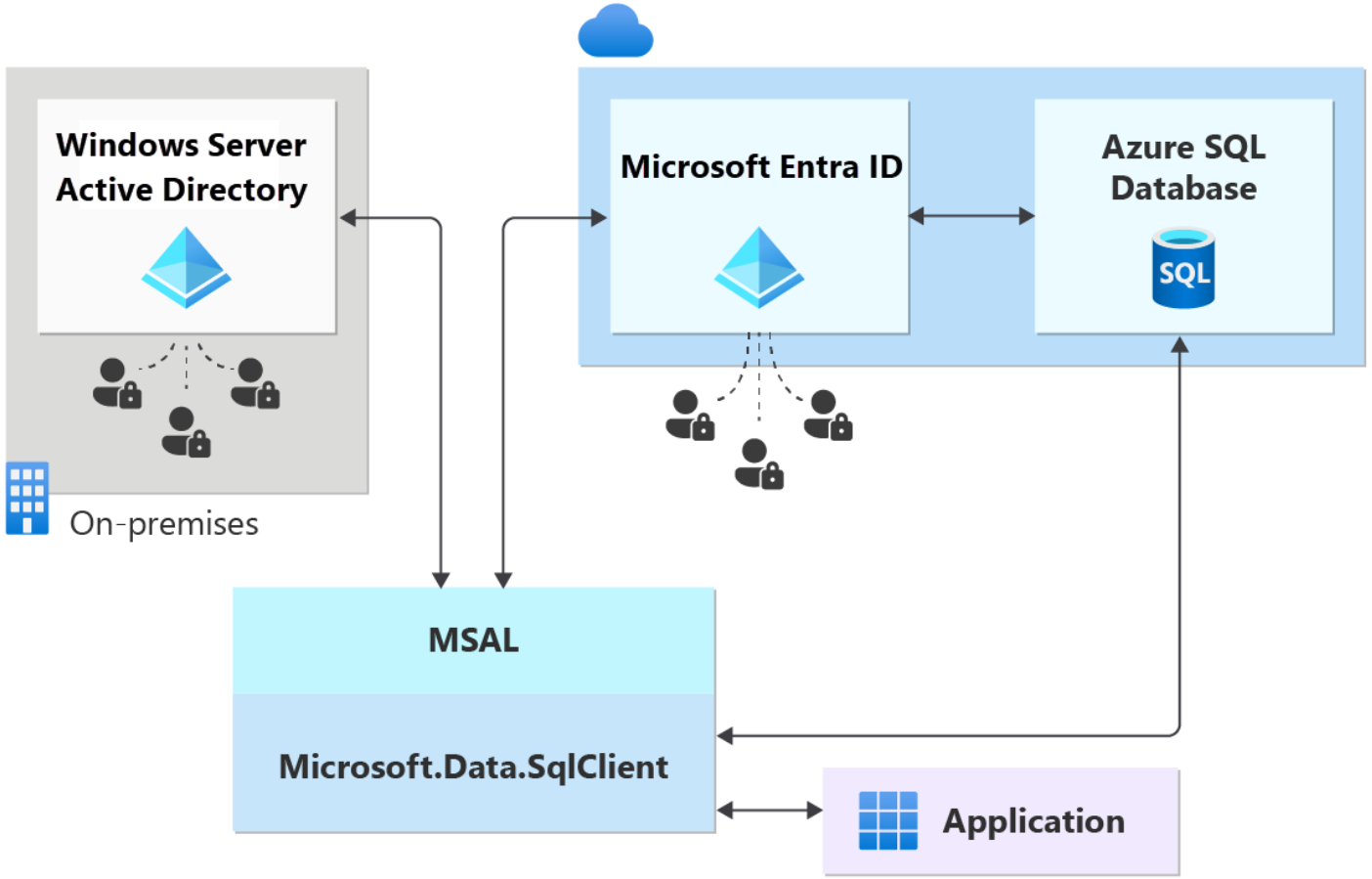
- Encryption of data in transit



Plan and implement security for Azure SQL Database and Azure SQL Managed Instance

- Enable Microsoft Entra database authentication [see 1]
- Enable database auditing
- Plan and implement dynamic masking
- Implement Transparent Database Encryption (TDE)
- Recommend when to use Azure SQL Database Always Encrypted


Home > mydocsamplesqlserver > MySampleDatabase (mydocsamplesqlserver/MySampleDatabase)
MySampleDatabase (mydocsamplesqlserver/MySampleDatabase) | Auditing
SQL database
Search (Ctrl+/)
Save
Discard
View audit logs
Feedback
Power Automate (preview)
Settings
Configure
Geo-Replication
Connection strings
Sync to other databases
Add Azure Search
Properties
Locks
Integrations
Stream analytics (preview)
Security
Auditing
If Blob Auditing is enabled on the server, it will always apply to the database, regardless of the database settings.
View server settings
Server-level Auditing: Enabled
Azure SQL Auditing
Azure SQL Auditing tracks database events and writes them to an audit log in your Azure Storage account, Log Analytics workspace or Event Hub. Learn more about Azure SQL Auditing
Enable Azure SQL Auditing


Windows Server
Active Directory
On-premises
Microsoft Entra ID
Azure SQL
Database
SQL
MSAL
Microsoft.Data.SqlClient
Application

Manage security operations

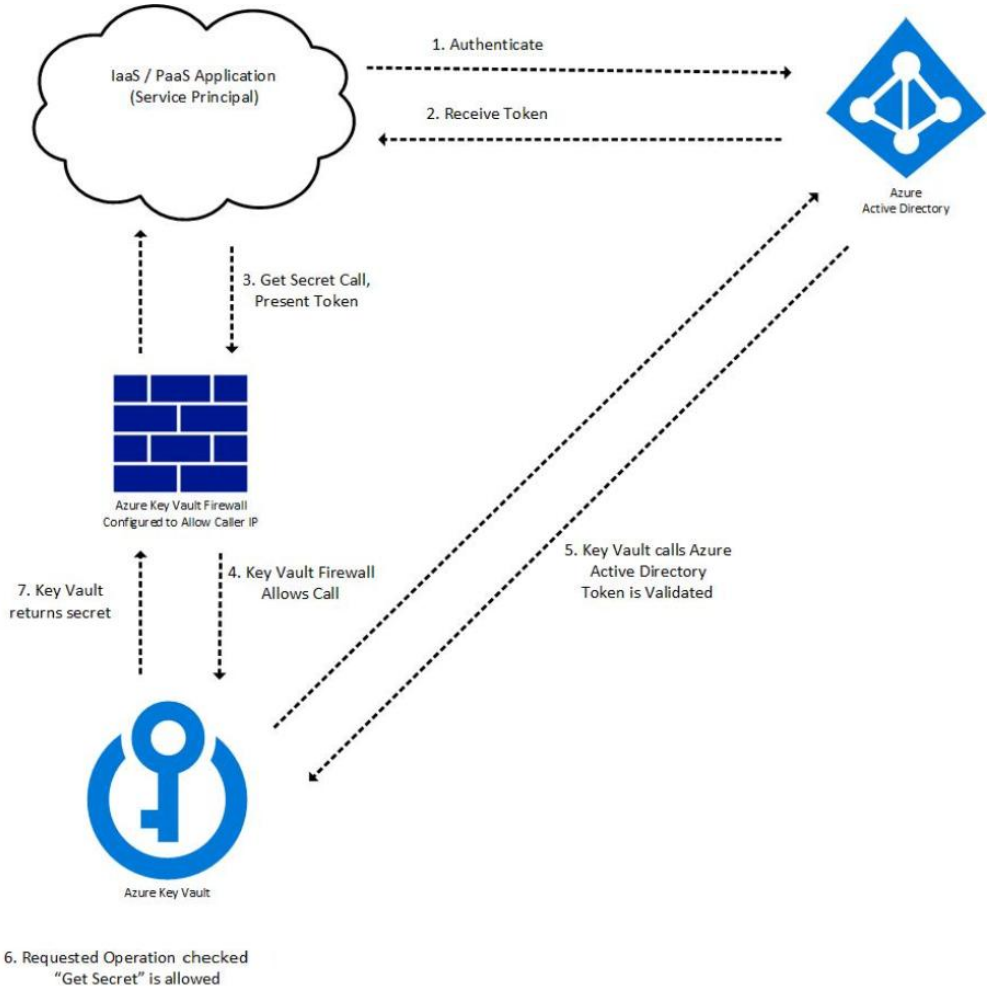
- Implement and manage enforcement of cloud governance policies
- Manage security posture by using Microsoft Defender for Cloud
- Configure and manage threat protection by using Microsoft Defender for Cloud
- Configure and manage security monitoring and automation solutions

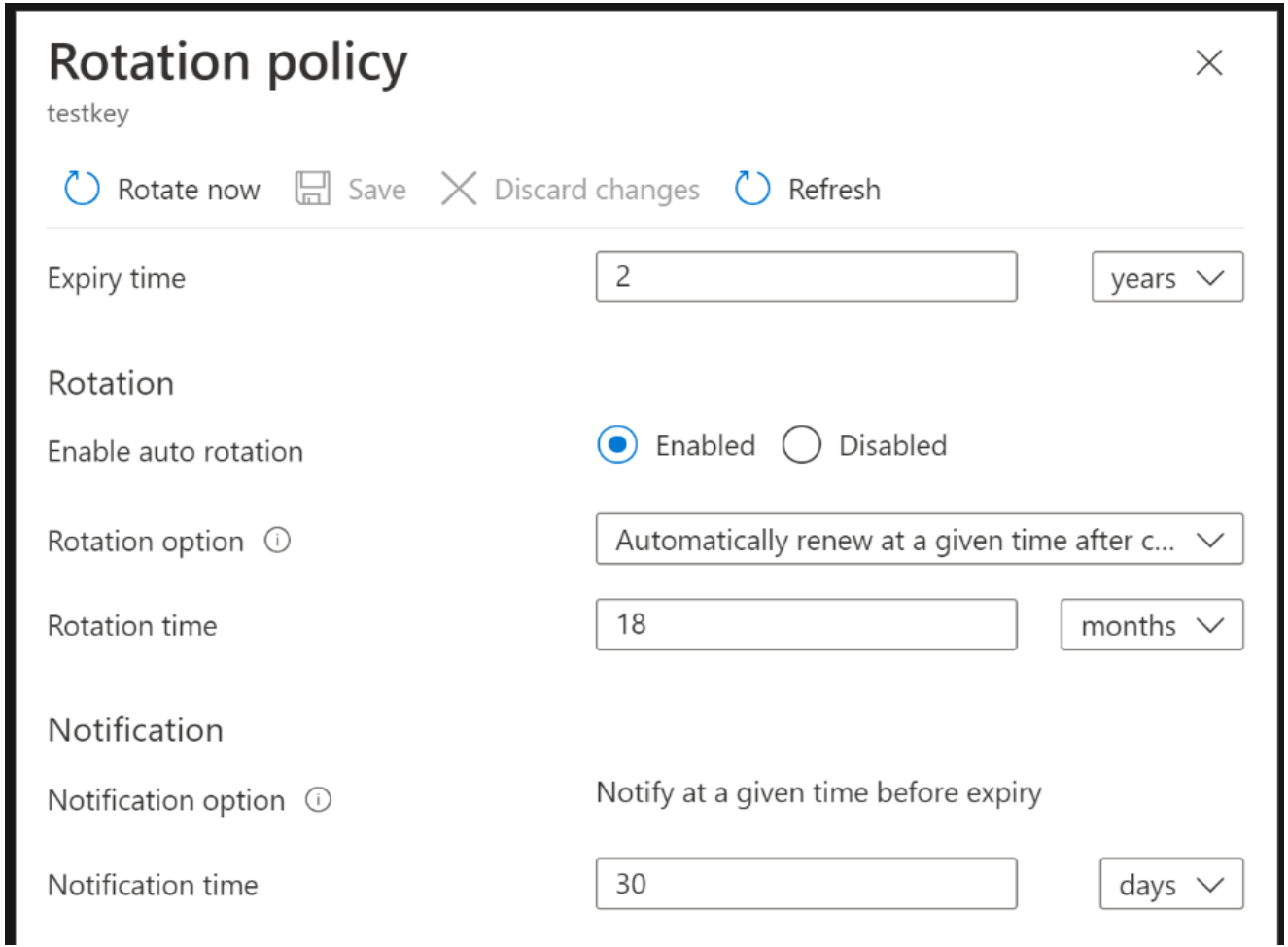
Poll: Is it possible to prevent Azure Key Vault creation if private access is not enabled for the vault?

- Yes, using Azure Policy
- Yes, using Azure Firewall
- Yes, using WAF
- No

Implement and manage enforcement of cloud governance policies

- Create, assign, and interpret policies and initiatives in Azure Policy
- Configure Azure Key Vault network settings [see 1]
- Configure access to Key Vault, including vault access policies and Azure Role Based Access Control
- Manage certificates, secrets, and keys
- Configure key rotation
- Perform backup and recovery of certificates, secrets, and keys
- Implement security controls to protect backups [see 1 2]
- Implement security controls for asset management [see 1]


IaaS / PaaS Application
(Service Principal)
1. Authenticate
2. Receive Token
Azure
Active Directory
3. Get Secret Call,
Present Token
Azure Key Vault Firewall
Configured to Allow Caller IP
5. Key Vault calls Azure
Active Directory
Token is Validated
7. Key Vault
returns secret
4. Key Vault Firewall
Allows Call
Azure Key Vault
6. Requested Operation checked
"Get Secret" is allowed


Rotation policy
testkey
Rotate now
Save
Discard changes
Refresh
Expiry time
2
years
Rotation
Enable auto rotation
Enabled
Disabled
Rotation option
Automatically renew at a given time after c...
Rotation time
18
months
Notification
Notification option
Notify at a given time before expiry
Notification time
30
days

Poll: Which Azure service functions as a security advisor, identifying vulnerabilities in your subscription?

- Azure Firewall
- Azure Sentinel
- Microsoft Defender for Cloud
- Azure Advisor

Manage security posture by using Microsoft Defender for Cloud

- Identify and remediate security risks by using the Microsoft Defender for Cloud Secure Score and Inventory
- Assess compliance against security frameworks and Microsoft Defender for Cloud
- Add industry and regulatory standards to Microsoft Defender for Cloud
- Add custom initiatives to Microsoft Defender for Cloud
- Connect hybrid cloud and multi-cloud environments to Microsoft Defender for Cloud
- Identify and monitor external assets by using Microsoft Defender External Attack Surface Management (EASM)

Poll: Is Microsoft Defender for Cloud free?

- No
- Yes
- Yes, basic features are free for some services, but the standard version is paid.

Configure and manage threat protection by using Microsoft Defender for Cloud

- Enable workload protection services in Microsoft Defender for Cloud [see 1]
- Configure Microsoft Defender for Servers, Microsoft Defender for Databases, and Microsoft Defender for Storage
- Implement and manage agentless scanning for virtual machines in Microsoft Defender for Servers [see 1]
- Implement and manage Microsoft Defender Vulnerability Management for Azure virtual machines [see 1]
- Connect to and configure settings in Microsoft Defender for Cloud Devops Security, including GitHub, Azure DevOps, and GitLab [see 1]

Poll: Which Azure service helps analyze security data and detect threats across your cloud and on-premises environments?

- Azure Monitor
- Microsoft Defender for Cloud
- Azure Sentinel
- Azure Log Analytics

Configure and manage security monitoring and automation solutions

- Manage and respond to security alerts in Microsoft Defender for Cloud [see 1]
- Configure workflow automation by using Microsoft Defender for Cloud [see 1]
- Monitor network security events and performance data by configuring data collection rules (DCRs) in Azure Monitor [see 1]
- Configure data connectors in Microsoft Sentinel [see 1]
- Enable analytics rules in Microsoft Sentinel [see 1]
- Configure automation in Microsoft Sentinel [see 1 2]

Settings | Security policy

Pay-As-You-Go

Search (Ctrl+/)

Settings

- Defender plans
- Auto provisioning
- Email notifications
- Integrations
- Workflow automation
- Continuous export

Policy settings

- Security policy
- Governance rules (preview)

Security policy on: Pay-As-You-Go

initiatives enabled on this subscription

Default initiative

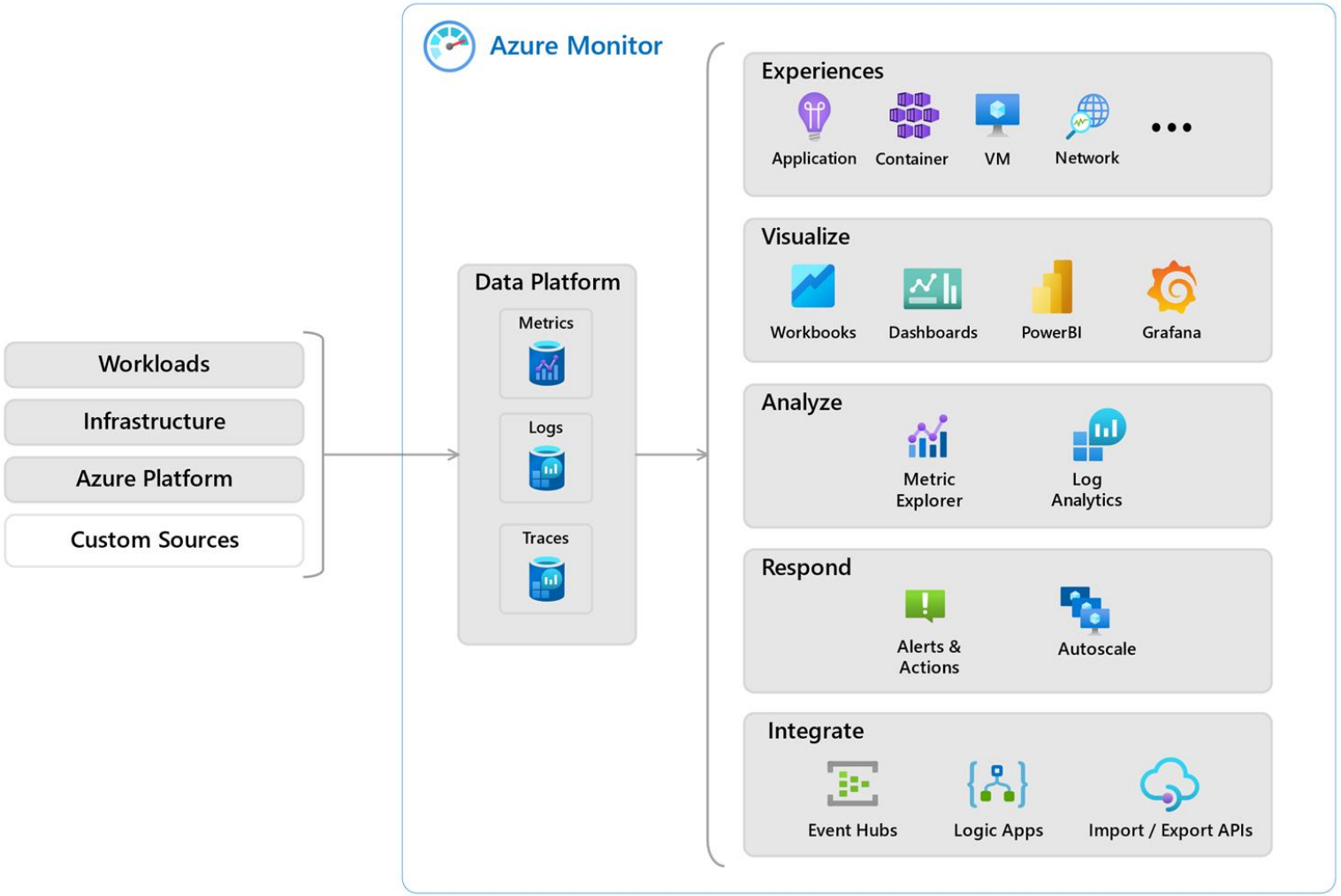
The default initiative enabled on your subscription generates the security recommendations in the **Recommendations** pag

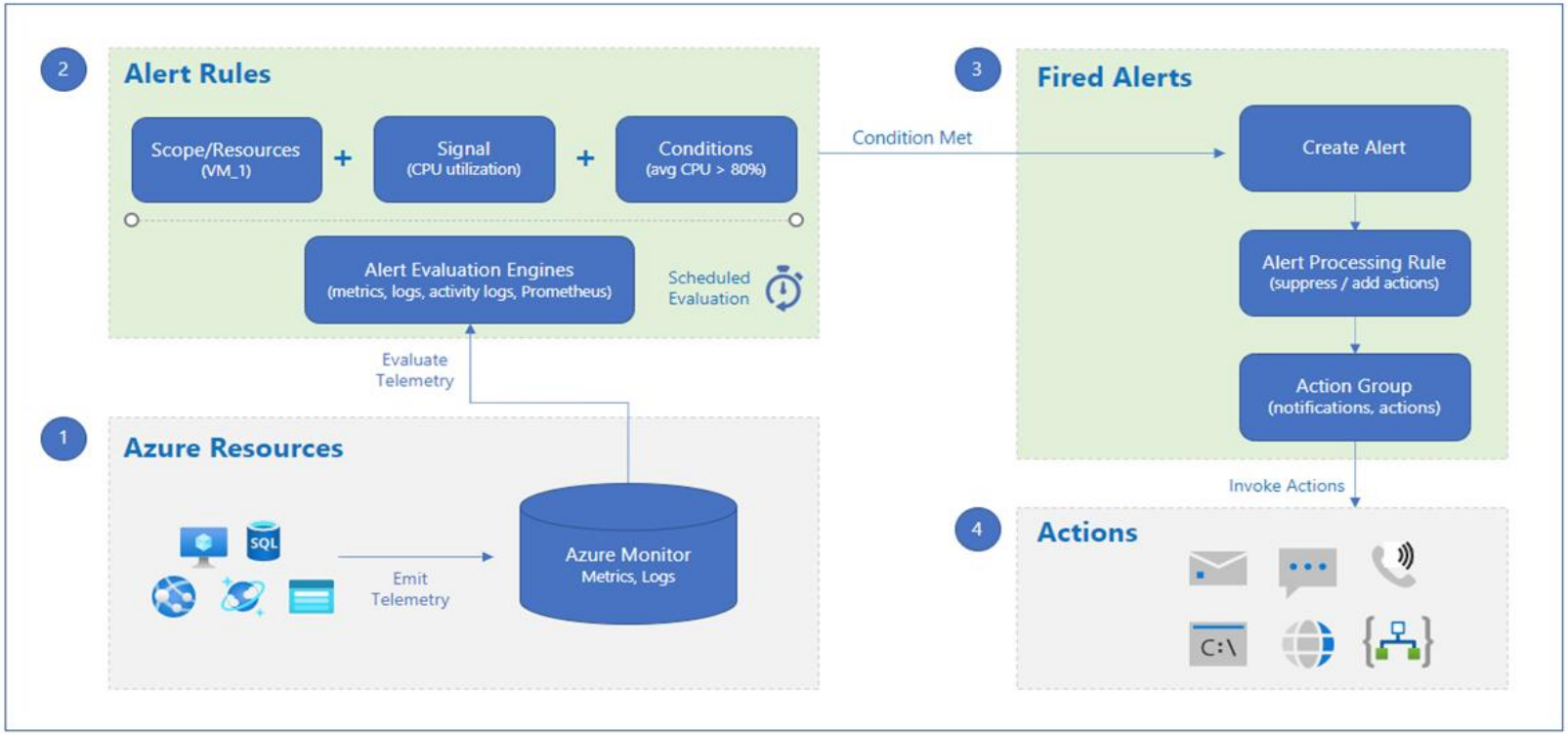
Assignment	Assigned On	Audit policies	Deny policies
ASC Default (subscription: 19969c81-e...	Subscription	188	0

Industry & regulatory standards

Compliance initiatives shown in the **Regulatory compliance dashboard.**

Azure Security	Track Azure Security	Out of the


Azure Monitor
Workloads
Infrastructure
Azure Platform
Custom Sources
Data Platform
Metrics
Logs
Traces
Experiences
Application
Container
VM
Network
Visualize
Workbooks
Dashboards
PowerBI
Grafana
Analyze
Metric Explorer
Log Analytics
Respond
Alerts & Actions
Autoscale
Integrate
Event Hubs
Logic Apps
Import / Export APIs



Alerts boundary

External boundary

The Exam

Questions in AZ-500

- Number of Questions ~45 Questions
- Questions (see the exam sandbox)
  - Multiple choice
  - Drag and drop
  - Scenario based
- The exam currently does not include labs but watch for updates!
- Pass Score 700 (on a scale of 1-1000)

AZ-500

- Exam AZ-500
- Skills measured
- AZ-500 Exam Prep videos
- Demo the exam experience by visiting the Exam Sandbox

AZ-500

- Exam AZ-500:
  https://learn.microsoft.com/en-us/certifications/exams/az-500
- Skills measured :
  https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3VC70

Practice for the exam

PRACTICE ASSESSMENT

Assess your knowledge

Practice assessments provide you with an overview of the style, wording, and difficulty of the questions you're likely to experience on the exam. Through these assessments, you're able to assess your readiness, determine where additional preparation is needed, and fill knowledge gaps bringing you one step closer to the likelihood of passing your exam.

Take the practice assessment

EXAM SANDBOX

Experience demo

Experience the look and feel of the exam before taking it. You'll be able to interact with different question types in the same user interface you'll use during the exam.

Launch the sandbox

VIDEO

Exam AZ-500 prep videos

Join our experts as they provide tips, tricks, and strategies for preparing for this Microsoft Certification exam.

Watch video

Take the exam

You will have **100 minutes** to complete this assessment.

Exam policy

This exam will be proctored, and is not open book. You may have interactive components to complete as part of this exam. To learn more about exam duration and experience, visit: Exam duration and exam experience.

If you fail a certification exam, don't worry. You can retake it 24 hours after the first attempt. For subsequent retakes, the amount of time varies. For full details, visit: Exam retake policy.

Need accommodations?

We offer a variety of accommodations to support you.

Learn More

This exam is offered in the following languages:

English, Japanese, Chinese (Simplified), Korean, German, French, Spanish, Portuguese (Brazil), Arabic (Saudi Arabia), Russian, Chinese (Traditional), Italian, Indonesian (Indonesia)

Schedule through Pearson Vue

Schedule exam >

ⓘ We strongly recommend that you register for an exam with a personal MSA account. If you register with an organizational (work/school) AAD account, your exam

United States

$165 USD*

Price based on the country or region in which the exam is proctored.

Where do you want to take your exam?

At a test center | OnVUE Online at my home or office | I have a Private Access Code

Prepare for your online exam at your home or office

Your computer

Use a personal computer that has a reliable webcam and internet connection.

Run system test.

Your testing space

The room should be a distraction-free, private place.

See acceptable spaces and view permitted comfort aid list.

Your photo ID

We'll verify your government-issued identification (ID) when you arrive for your exam.

Review admission & ID policies

What to expect

Check in for your OnVUE exam 30 minutes before your appointment time.

Watch our short video to get familiar with the process.

Questions?

Check out the OnVUE FAQs and minimum technical requirements.

It’s time to test your system

Order #: 0064-8802-7606

Your appointment is confirmed! An order confirmation containing important exam day information has been sent to: zaalion@gmail.com

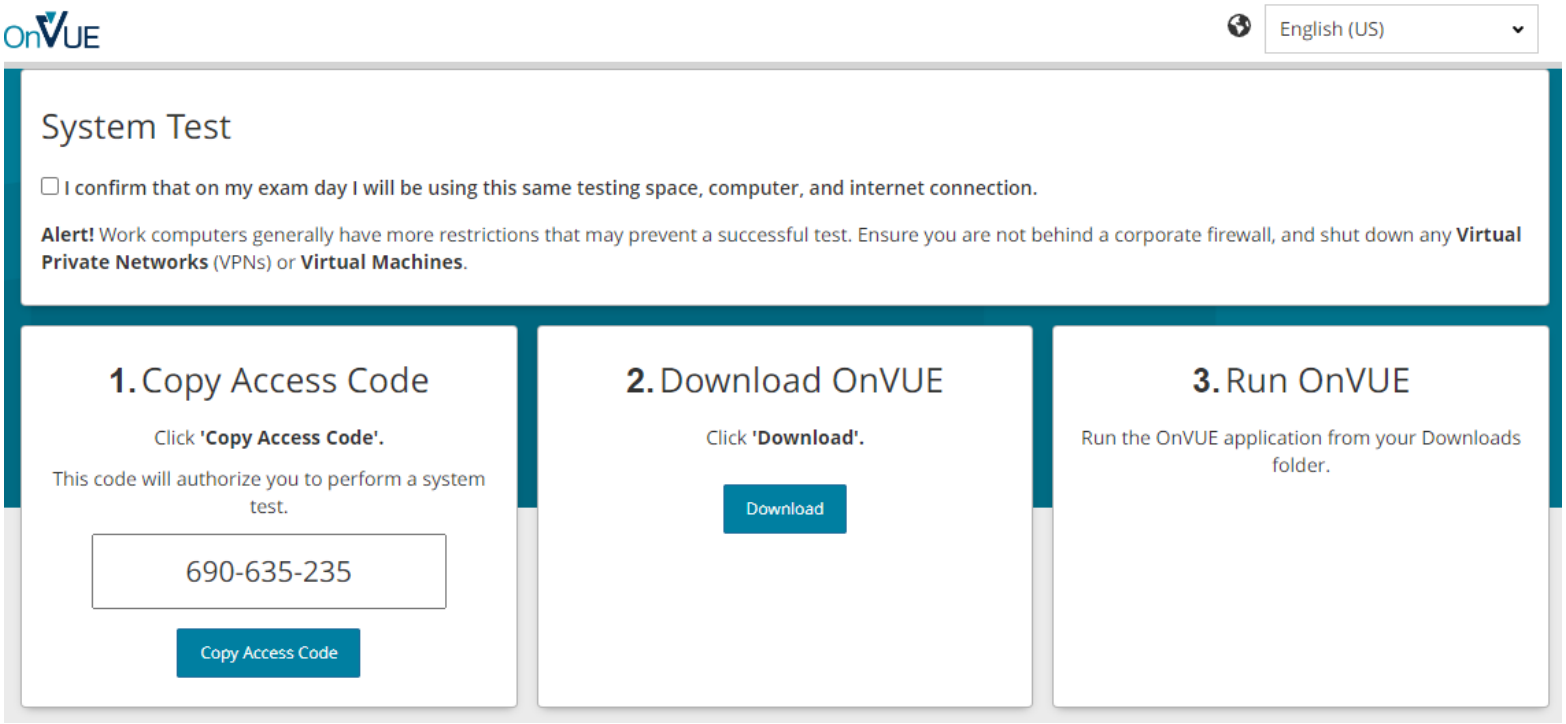
What's next?

Run a system test

We need to verify that the computer and internet connection you plan to use on exam day meet the minimum requirements for online testing. It’ll just take 5 minutes to run:

- Equipment and internet connection checks
- Exam simulation

Description	Details	Order Information	Price
			165.00


OnVUE
English (US)
System Test
I confirm that on my exam day I will be using this same testing space, computer, and internet connection.
Alert! Work computers generally have more restrictions that may prevent a successful test. Ensure you are not behind a corporate firewall, and shut down any Virtual Private Networks (VPNs) or Virtual Machines.
1. Copy Access Code
Click 'Copy Access Code'.
This code will authorize you to perform a system test.
690-635-235
Copy Access Code
2. Download OnVUE
Click 'Download'.
Download
3. Run OnVUE
Run the OnVUE application from your Downloads folder.

Course Repository

https://github.com/zaalion/oreilly-az-500

Microsoft Azure Fundamentals (AZ-900) Certification Course, 2nd Edition

Continue

4h 55m remaining

With your instructor

Reza Salehi

+ Add to playlist

Associated roles

Cloud native engineer | Cloud solutions architect | Cybersecurity engineer | Database administrator

+1 more

Skills covered

AZ-900: Microsoft Azure Fundamentals

AZ-303: Microsoft Azure Architect...

AZ-500: Microsoft Azure Security...

AI-900: Microsoft Azure AI Fundamentals

Includes quizzes

Test your knowledge during the course and with a final quiz.

October 2024

O'Reilly Media, Inc.

Learning Outcomes

- Gain knowledge of Azure cloud concepts and services
- Explore Azure services in greater depth
- Get ready for Exam AZ-900: Microsoft Azure Fundamentals
- Comfortably work with the Azure portal

The Microsoft Azure Fundamentals (AZ-900) exam is one of the most popular certifications for those who are just beginning to work with cloud-based solutions and services or who are new to Azure. The exam certifies knowledge of cloud concepts, Azure services, workloads, security and privacy, and pricing and support.

In this self-paced course, Reza Salehi will help you get familiar with Microsoft Azure's cloud services and begin your Azure certification journey. This course is aligned to the AZ-900 exam objective domains and has recently been updated to reflect the most current version of the exam (2024). It covers all the services and concepts in the Azure ecosystem you need to know in order to prepare for the test.

What you'll learn and how to apply it

By the end of this certification course, you will understand the following:

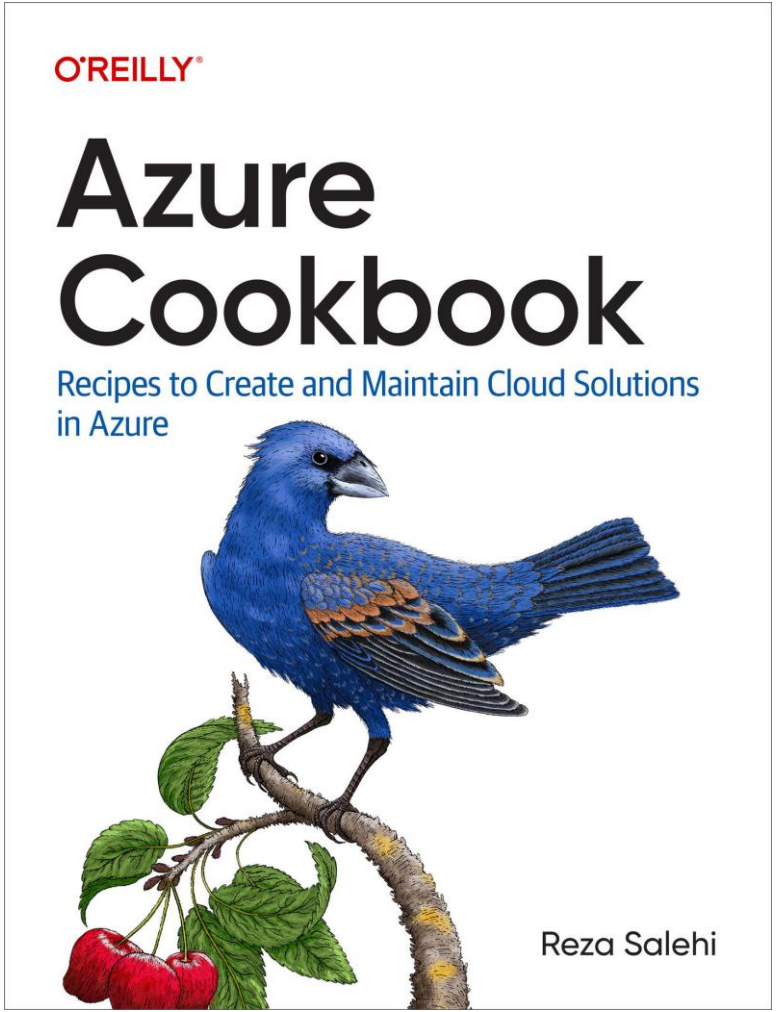
- General cloud concepts
- Core Azure services
- Core solutions and management tools on Azure
- General security and network security features
- Identity, governance, privacy, and compliance features
- Azure cost management and service-level agreements

Azure Cookbook

https://learning.oreilly.com/library/view/azure-cookbook/9781098135782/

https://www.amazon.ca/Azure-Cookbook-Recipes-Maintain-Solutions/dp/1098135792/

https://www.amazon.com/Azure-Cookbook-Recipes-Maintain-Solutions/dp/1098135792



O'REILLY®

Thank you!

Reza Salehi

@zaalion