O'REILLY®

Microsoft Azure Security Technologies (AZ-500) Bootcamp

Earn Your Azure Security Engineer Associate Badge

Reza Salehi

Cloud Consultant and Trainer

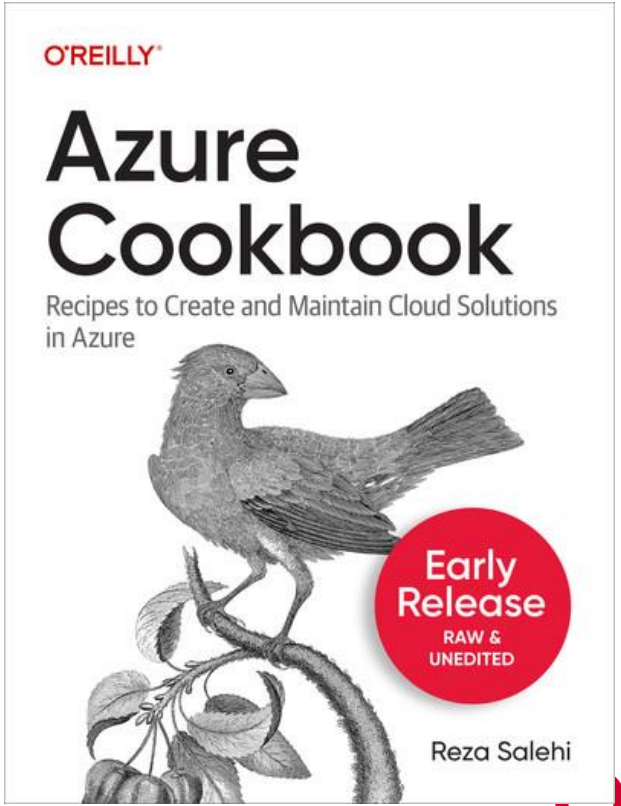
@zaalion

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



Course Overview

AZ-500 Bootcamp

- Day 1
  - Manage identity and access
  - Secure networking

AZ-500 Bootcamp

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

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

EXAMS

Exam AZ-500: Microsoft Azure Security Technologies

Candidates for this exam should have subject matter expertise implementing Azure security controls that protect identity, access, data, applications, and networks in cloud and hybrid environments as part of an end-to-end infrastructure.

Responsibilities for an Azure security engineer include managing the security posture, identifying and remediating vulnerabilities, performing threat modeling, implementing threat protection, and responding to security incident escalations.

Azure security engineers often serve as part of a larger team to plan and implement cloud-based management and security.

Candidates for this exam should have practical experience in administration of Azure and hybrid environments. Candidates should have experience with infrastructure as code, security operations processes, cloud capabilities, and Azure services.

You may be eligible for ACE college credit if you pass this certification exam. See ACE college credit for certification exams for details.

Important

Azure security engineers often serve as part of a larger team to plan and implement cloud-based management and security.

Candidates for this exam should have practical experience in administration of Azure and hybrid environments. Candidates should have experience with infrastructure as code, security operations processes, cloud capabilities, and Azure services.

You may be eligible for ACE college credit if you pass this certification exam. See ACE college credit for certification exams for details.

Important

The English language version of this exam was updated on August 2, 2022. Please download the study guide listed in the "Tip" box to see the current skills measured. If a localized version of this exam is available, it will be updated approximately eight weeks after this date.

Passing score: 700. **Learn more about exam scores.**

Tip

- Watch **AZ-500 Exam Prep videos** on Learn
- Download the **AZ-500 study guide** to help you prepare for the exam
- Demo the exam experience by visiting our **Exam Sandbox**

Part of the requirements for: Microsoft Certified: Azure Security Engineer Associate
Related exams: none
Important: See details
Go to Certification Dashboard

Schedule exam

Exam AZ-500: Microsoft Azure Security Technologies

United States

Languages: English, Japanese, Chinese (Simplified), Korean, German, French, Spanish, Portuguese (Brazil), Arabic (Saudi Arabia), Russian, Chinese (Traditional), Italian, Indonesian (Indonesia)
Retirement date: none

$165 USD*

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

Two ways to prepare

Online - Free | Instructor-led - Paid

Items in this collection

LEARNING PATH

AZ-500: Manage Identity and Access

5 Modules

Intermediate | Security Engineer | Azure

Start >

⊕ Save

LEARNING PATH

AZ-500: Implement platform protection

4 Modules

Intermediate | Administrator | Azure

⊕ Save

LEARNING PATH

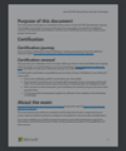
AZ-500: Secure your data and applications

4 Modules

Intermediate | Administrator | Azure

⊕ Save


1


2


3


4

Study Guide

Exam AZ-500: Microsoft Azure Security Technologies

Quick navigation

Microsoft Cybersecurity Reference Architectures

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

Day 1

Microsoft Azure Security Technologies Bootcamp

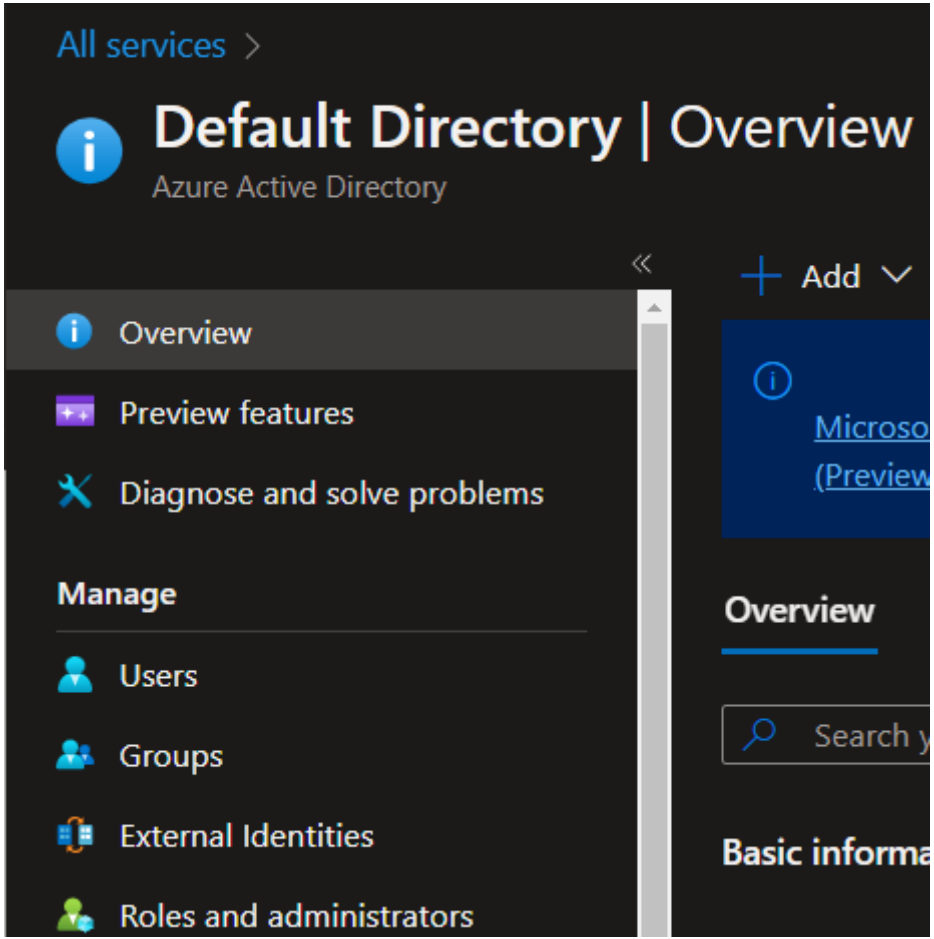
- Manage identity and access (25-30%)
- Secure networking (20-25%)

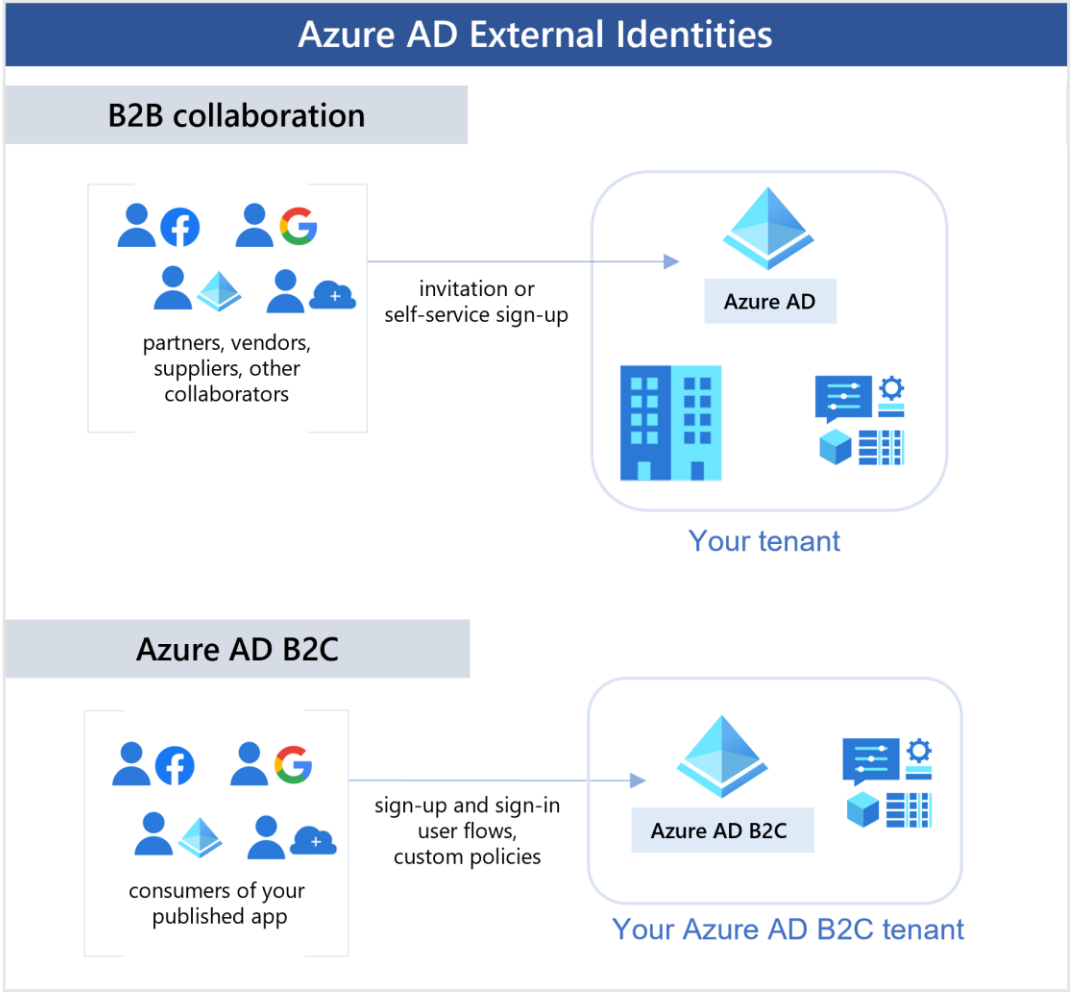
Manage Identity and Access

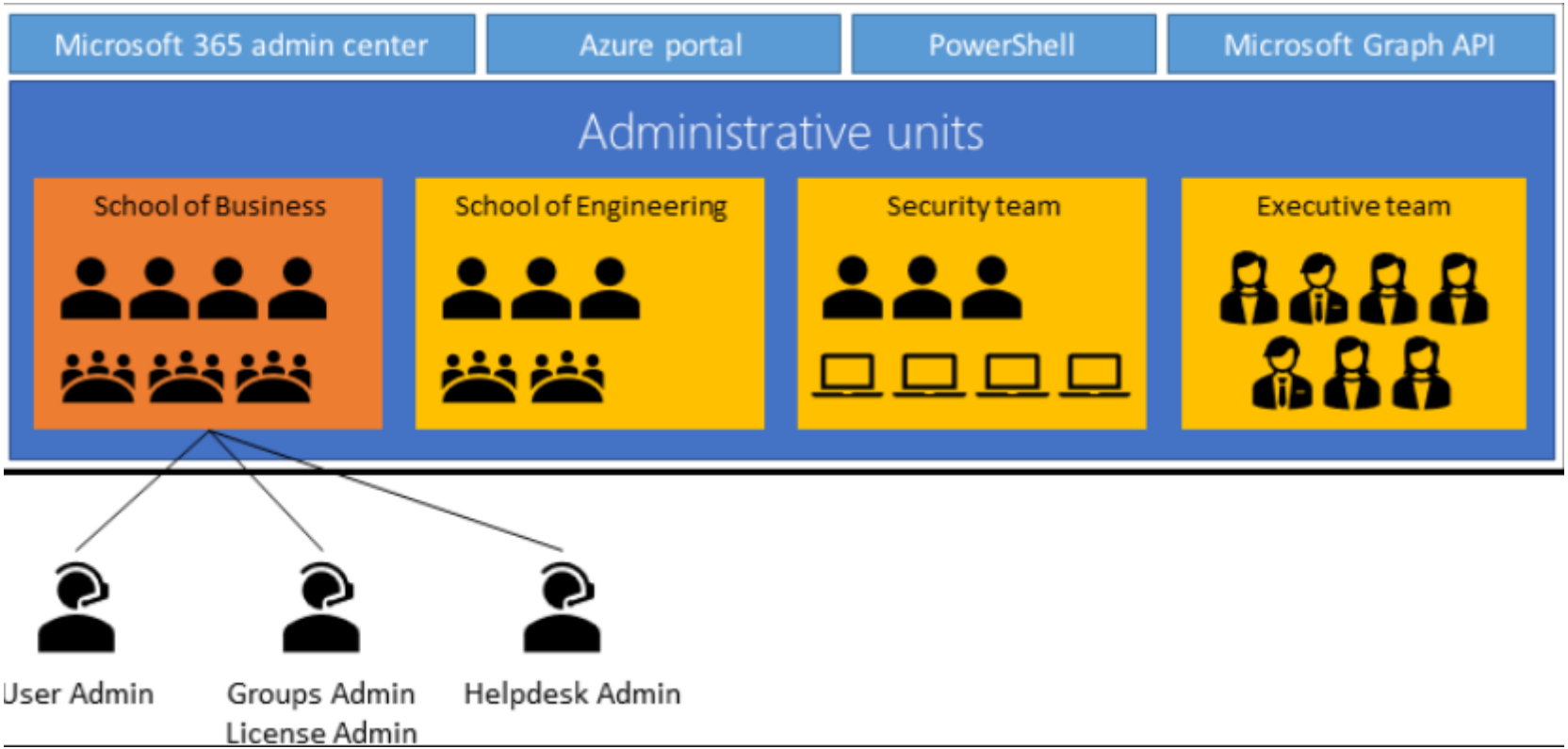
- Manage identities in Azure AD
- Manage authentication by using Azure AD
- Manage authorization by using Azure AD
- Manage application access in Azure AD

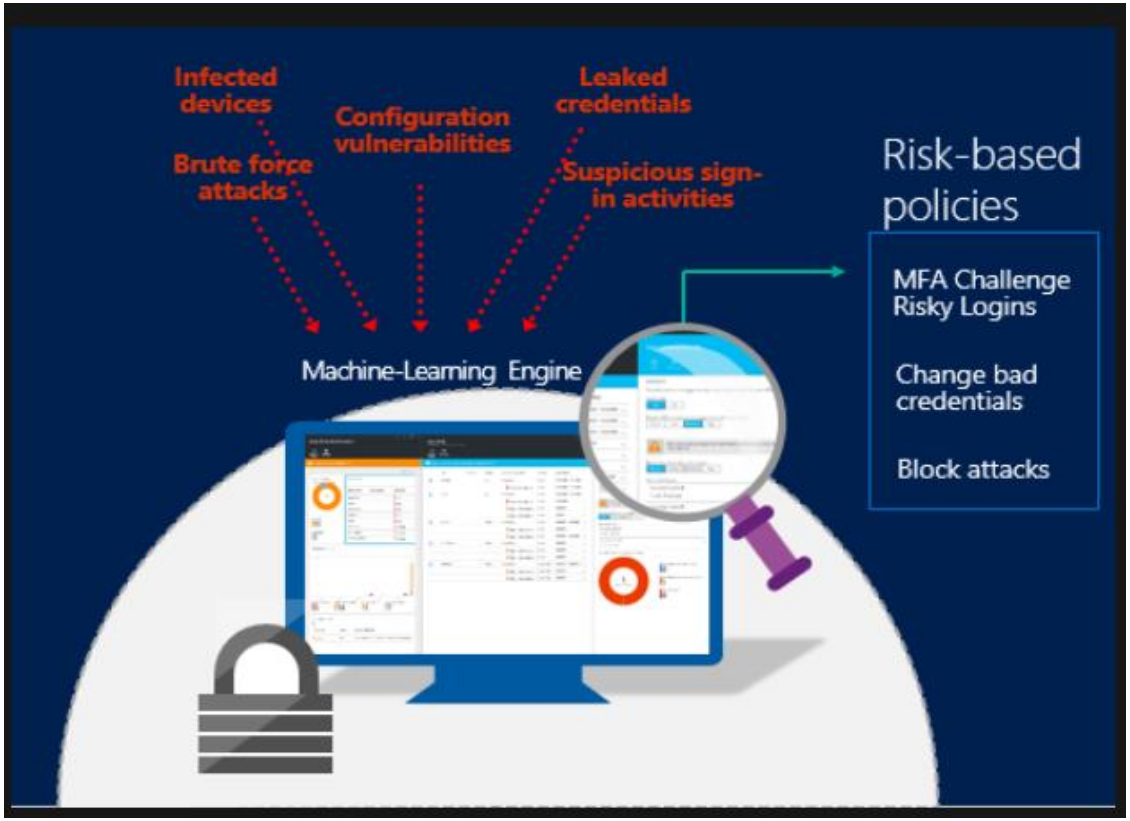
Manage identities in Azure AD

- Secure users in Azure AD
- Secure directory groups in Azure AD
- Recommend when to use external identities
- Secure external identities
- Implement Azure AD Identity Protection


All services
Default Directory | Overview
Azure Active Directory
Add
Overview
Preview features
Diagnose and solve problems
Manage
Users
Groups
External Identities
Roles and administrators
Overview
Basic informa


Azure AD External Identities
B2B collaboration
partners, vendors, suppliers, other collaborators
invitation or self-service sign-up
Azure AD
Your tenant
Azure AD B2C
consumers of your published app
sign-up and sign-in user flows, custom policies
Azure AD B2C
Your Azure AD B2C tenant


Microsoft 365 admin center
Azure portal
PowerShell
Microsoft Graph API
Administrative units
School of Business
School of Engineering
Security team
Executive team
User Admin
Groups Admin
License Admin
Helpdesk Admin

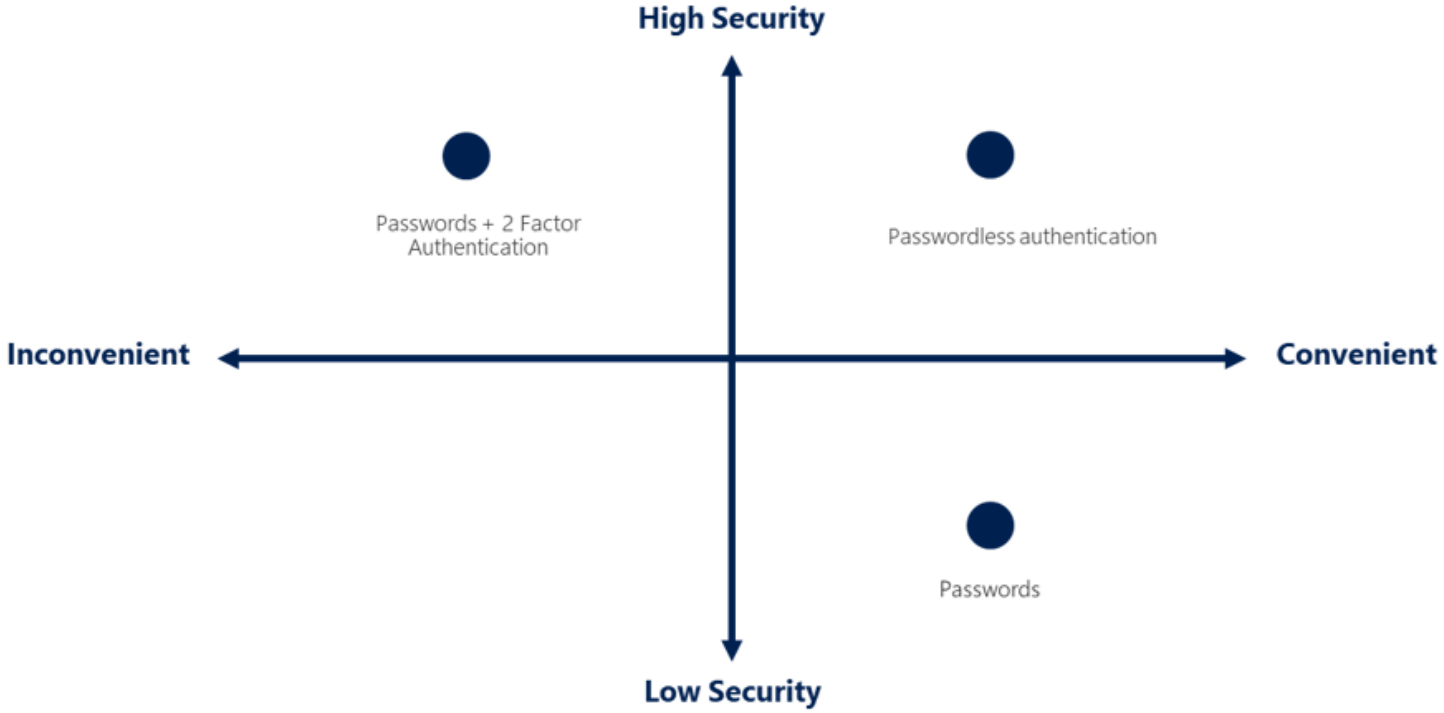

Infected devices
Brute force attacks
Configuration vulnerabilities
Leaked credentials
Suspicious sign-in activities
Machine-Learning Engine
Risk-based policies
MFA Challenge Risky Logins
Change bad credentials
Block attacks

Manage authentication by using Azure AD

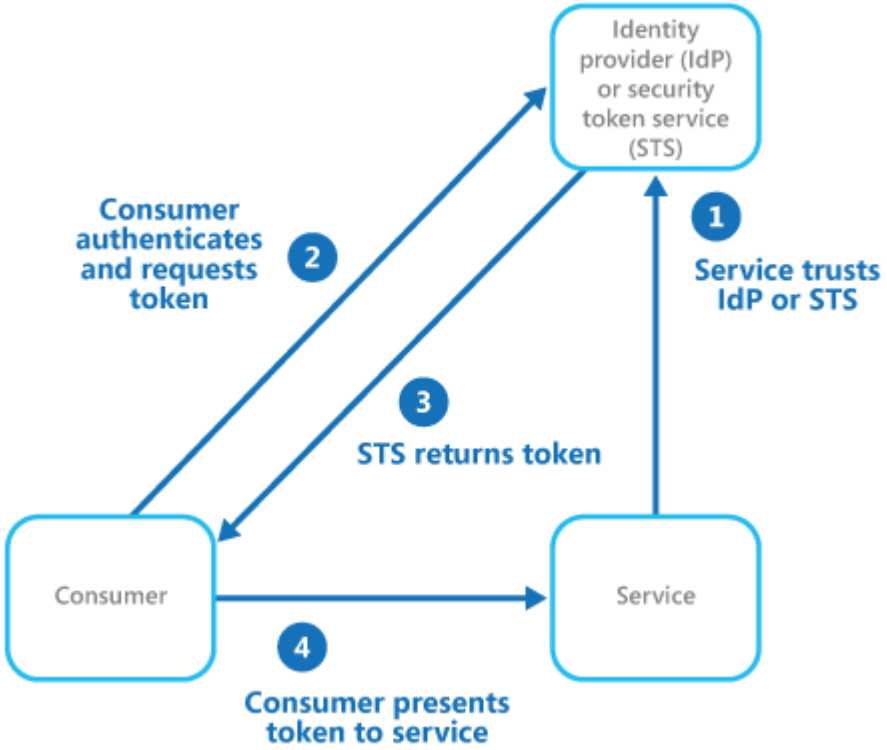
- Configure Microsoft Entra Verified ID
- Implement multi-factor authentication (MFA)
- Implement passwordless authentication
- Implement password protection
- Implement single sign-on (SSO)
- Integrate single sign on (SSO) and identity providers
- Recommend and enforce modern authentication protocols

Azure AD Multi-Factor Authentication

Passwordless authentication options for AAD



Federated Identity Pattern and SSO



Manage authorization by using Azure AD

- Configure Azure role permissions for management groups, subscriptions, resource groups, and resources
- Assign built-in roles in Azure AD
- Assign built-in roles in Azure
- Create and assign custom roles, including Azure roles and Azure AD roles
- Implement and manage Microsoft Entra Permissions Management
- Configure Azure AD Privileged Identity Management (PIM)
- Configure role management access reviews using Microsoft Entra
- Implement Conditional Access policies

Pay-As-Y
Subscription

Search (Ctrl+/)

- Overview
- Activity log
- Access control (IAM
- Tags
- Diagnose and solve
- Security
- Events

Cost Management

- Cost analysis
- Cost alerts
- Budgets
- Advisor recommen

Billing

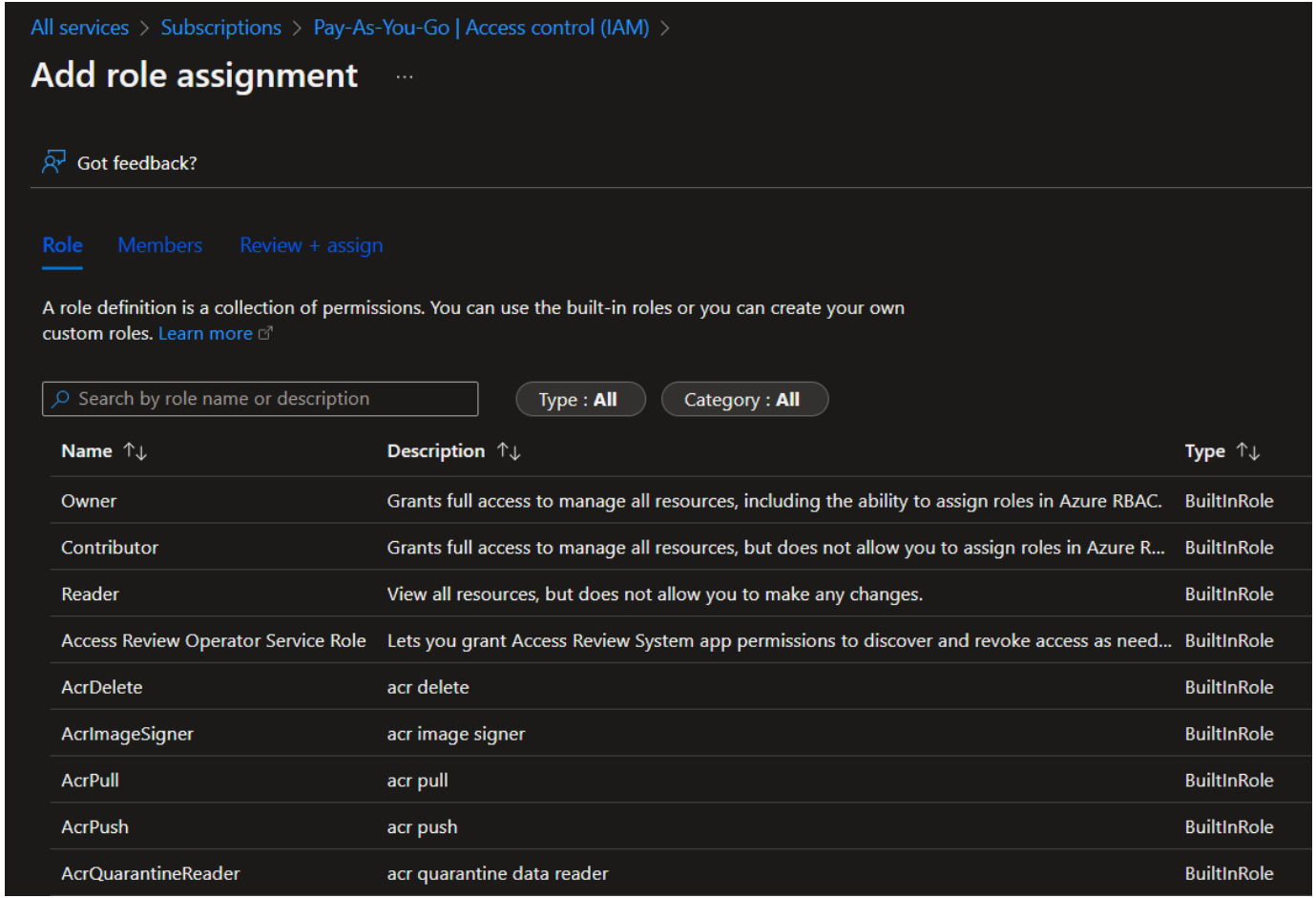
- Invoices
- External services

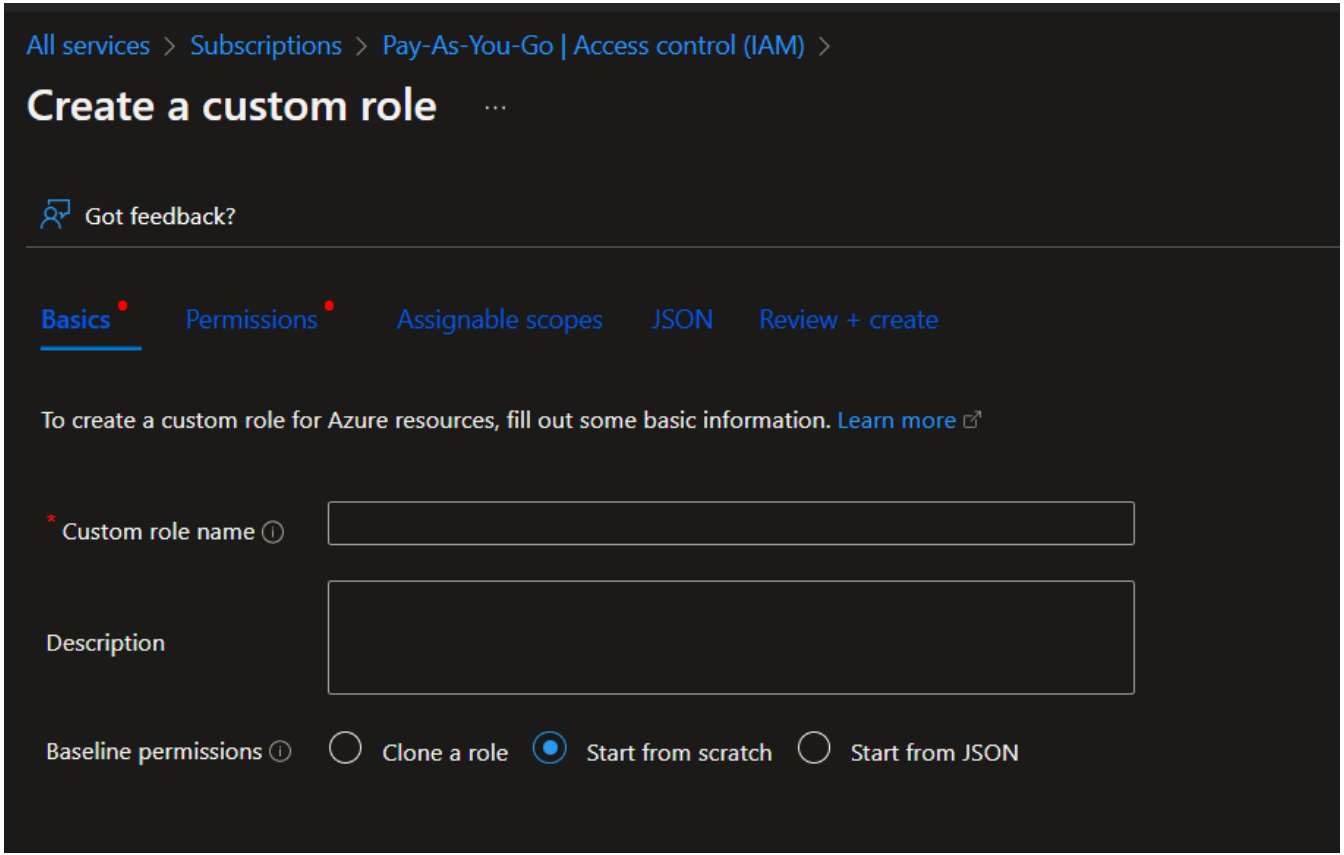
Reader

BuiltInRole

Permissions | JSON | Assignments


```
{
    "id": "/providers/Microsoft.Authorization/roleDefinitions/acdd72a7-3385-48ef-bd42-f606fba81ae7",
    "properties": {
        "roleName": "Reader",
        "description": "View all resources, but does not allow you to make any changes.",
        "assignableScopes": [
            "/"
        ],
        "permissions": [
            {
                "actions": [
                    "*/read"
                ],
                "notActions": [],
                "dataActions": [],
                "notDataActions": []
            }
        ]
    }
}
```


All services > Subscriptions > Pay-As-You-Go | Access control (IAM) >
Add role assignment ...
Got feedback?
Role
Members
Review + assign
A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more
Search by role name or description
Type : All
Category : All
Name
Description
Type
Owner
Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.
BuiltInRole
Contributor
Grants full access to manage all resources, but does not allow you to assign roles in Azure R...
BuiltInRole
Reader
View all resources, but does not allow you to make any changes.
BuiltInRole
Access Review Operator Service Role
Lets you grant Access Review System app permissions to discover and revoke access as need...
BuiltInRole
AcrDelete
acr delete
BuiltInRole
AcrImageSigner
acr image signer
BuiltInRole
AcrPull
acr pull
BuiltInRole
AcrPush
acr push
BuiltInRole
AcrQuarantineReader
acr quarantine data reader
BuiltInRole


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. →

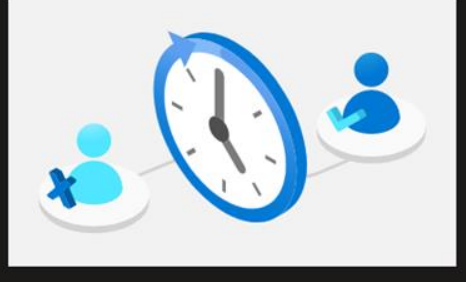
What's new | Get started

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

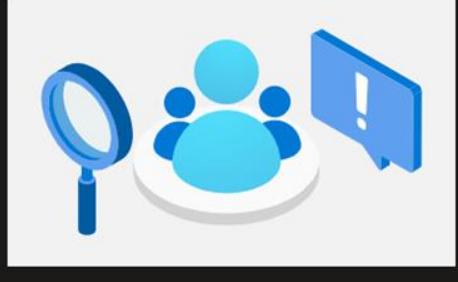
Manage access

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.



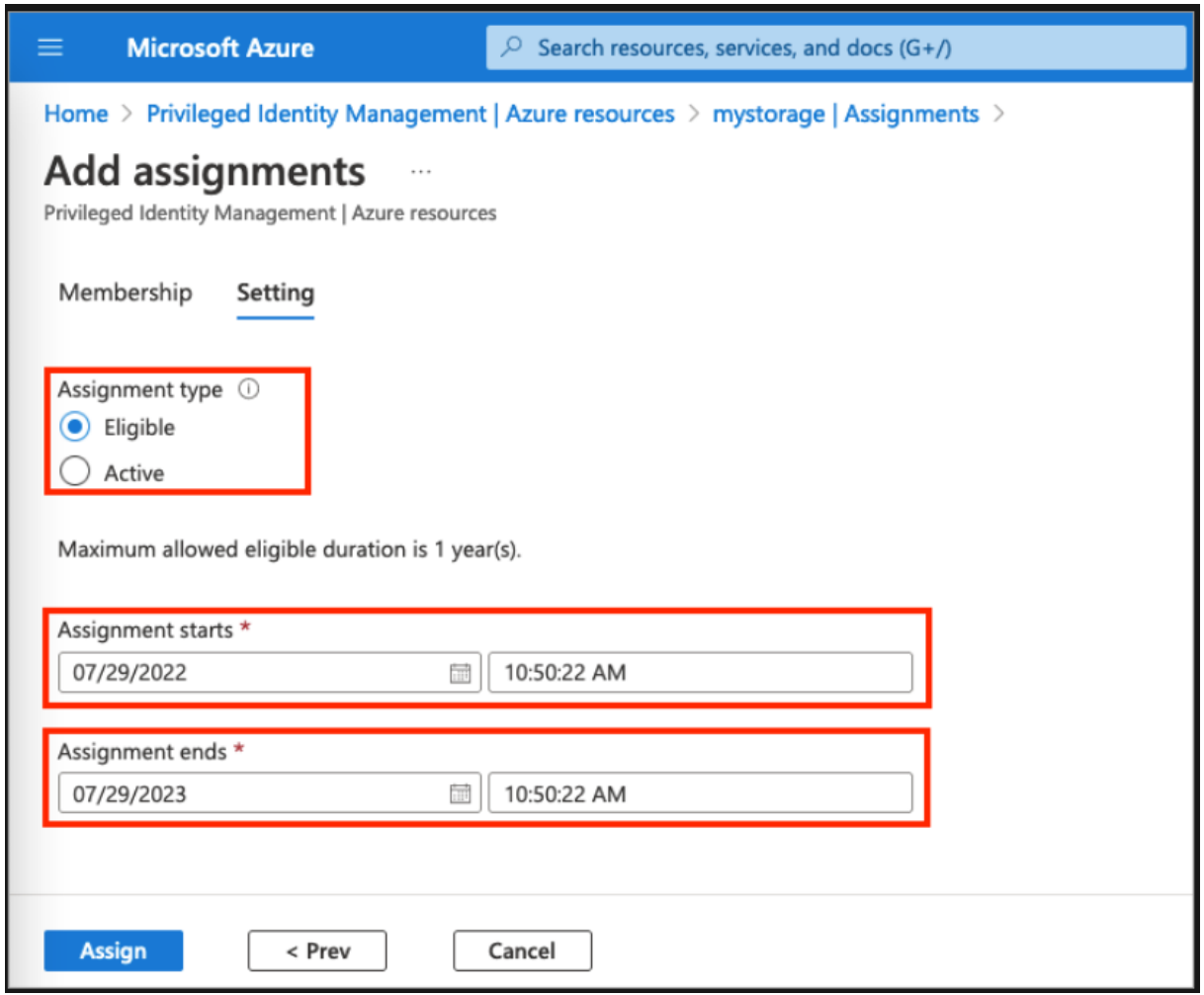
Activate just in time

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.

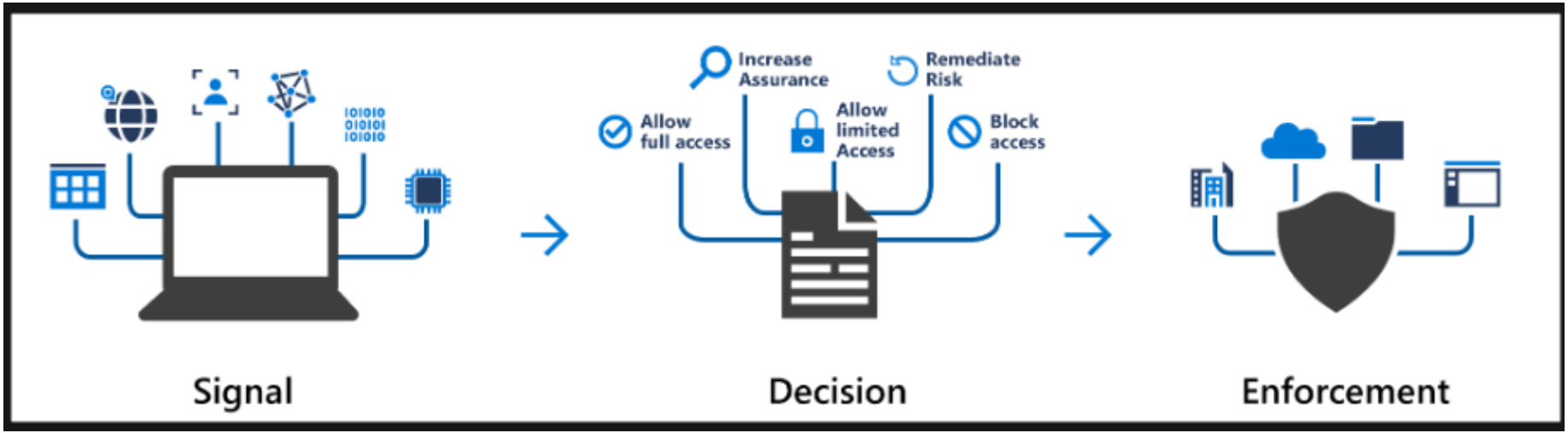


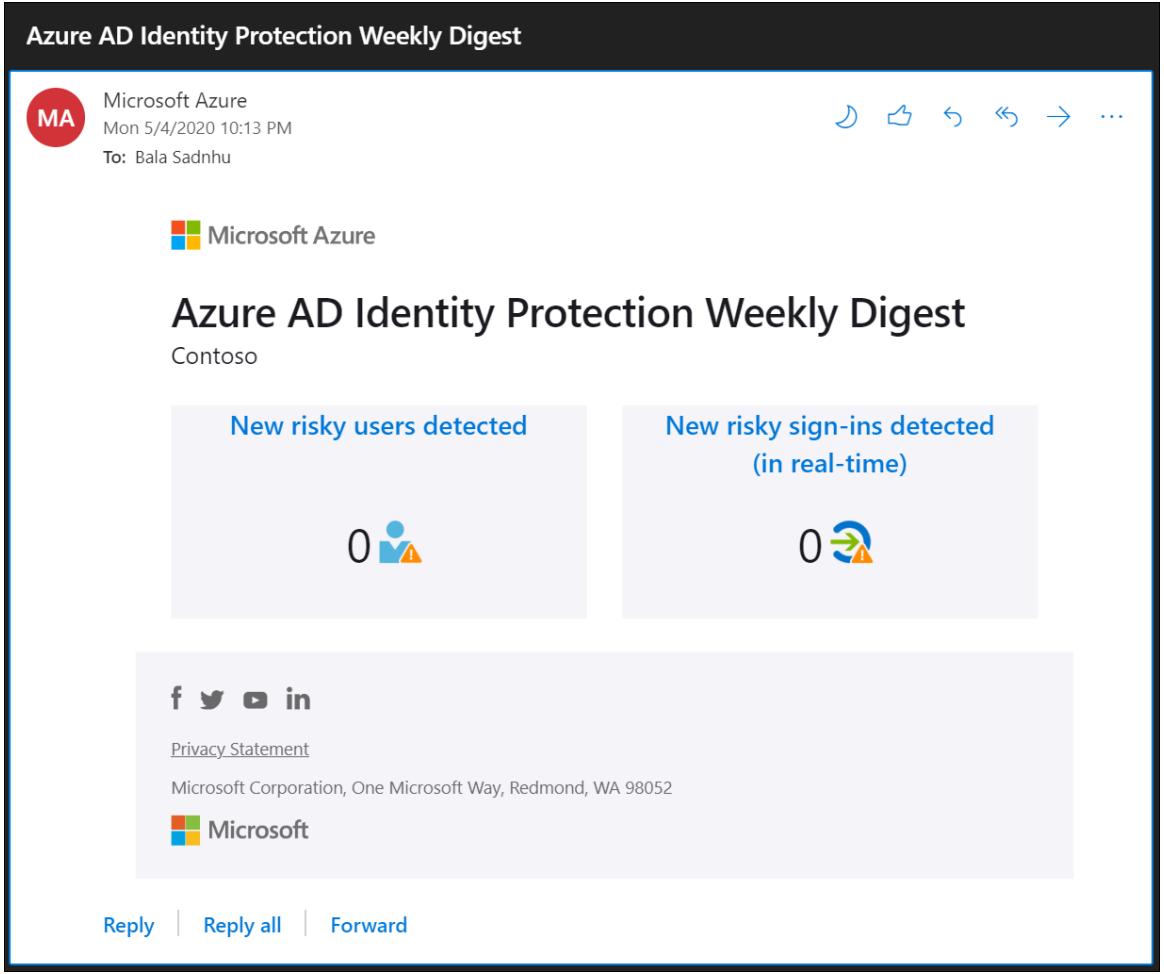
Discover and monitor

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.

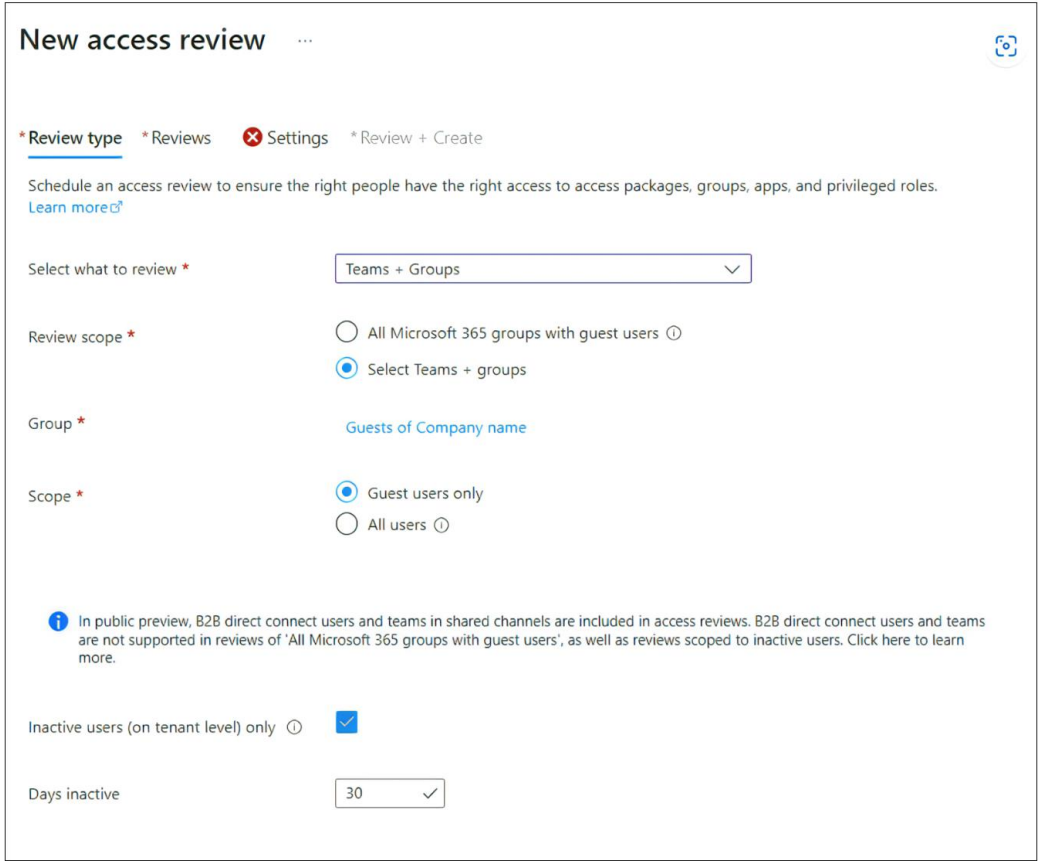

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Privileged Identity Management | Azure resources > mystorage | Assignments >
Add assignments
Privileged Identity Management | Azure resources
Membership
Setting
Assignment type
Eligible
Active
Maximum allowed eligible duration is 1 year(s).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

Azure AD Conditional Access




Azure AD Identity Protection Weekly Digest
MA
Microsoft Azure
Mon 5/4/2020 10:13 PM
To: Bala Sadnhu
Microsoft Azure
Azure AD Identity Protection Weekly Digest
Contoso
New risky users detected
0
New risky sign-ins detected (in real-time)
0
Privacy Statement
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052
Microsoft
Reply
Reply all
Forward

Configure Access Reviews



Manage authorization by using Azure AD

- Manage access to enterprise applications in Azure AD, including OAuth permission grants
- Manage app registrations in Azure AD
- Configure app registration permission scopes
- Manage app registration permission consent
- Manage and use service principals
- Manage managed identities for Azure resources
- Recommend when to use and configure authentication for an Azure AD Application Proxy

Create a virtual machine

Basics | Disks | Networking | Management | Guest config | Tags | Review + create

Configure monitoring and management options for your VM.

MONITORING

Boot diagnostics ⓘ — On / Off

OS guest diagnostics ⓘ — On / Off

* Diagnostics storage account ⓘ — azurefunctions12941ee6

Create new

IDENTITY

Managed service identity ⓘ — On / Off

AUTO-SHUTDOWN

Enable auto-shutdown ⓘ — On / Off

BACKUP

Enable backup ⓘ — On / Off

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

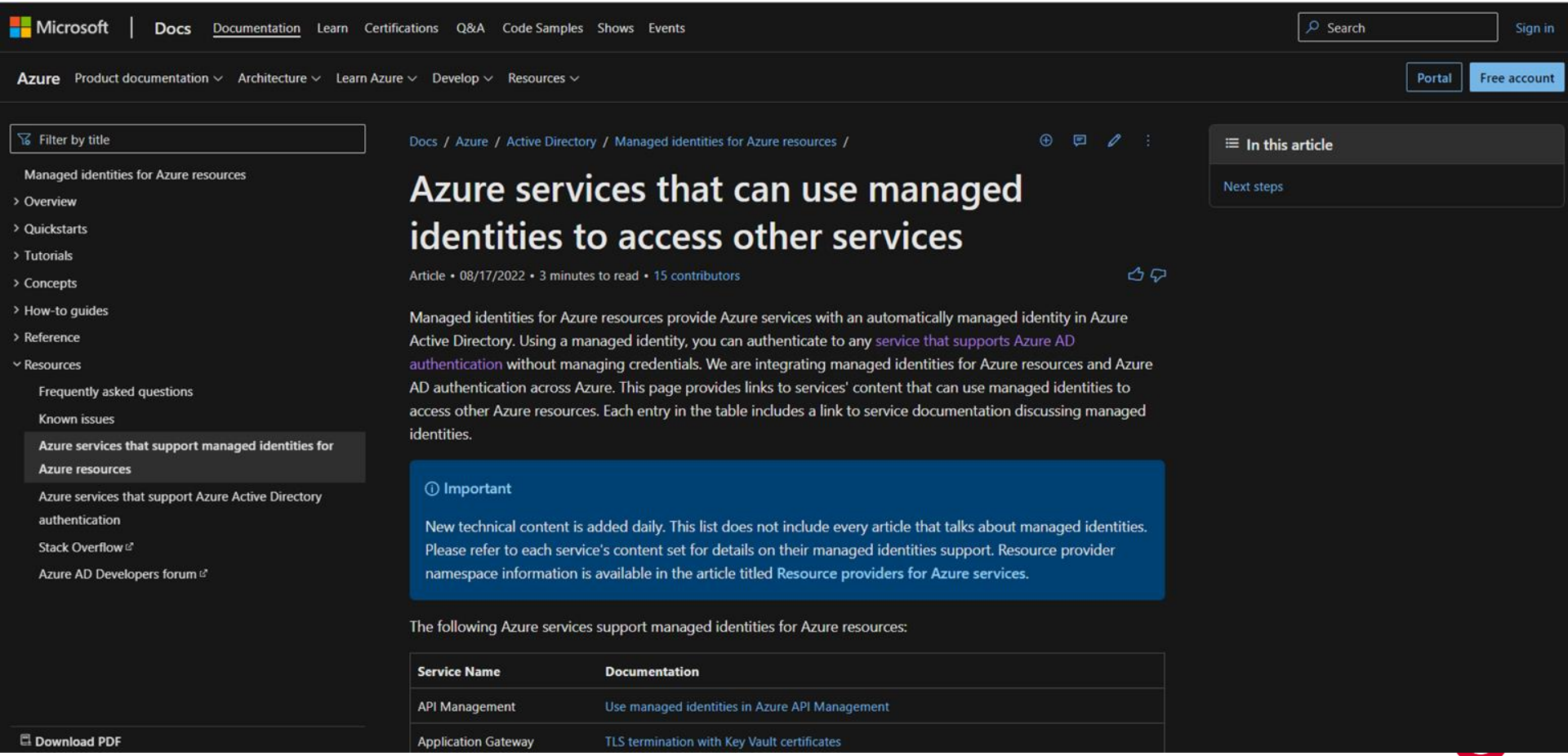
Resource group * ⓘ:

Create new

Instance details

Region * ⓘ: West US

Name * ⓘ:


Microsoft | Docs Documentation Learn Certifications Q&A Code Samples Shows Events
Search
Sign in
Azure Product documentation Architecture Learn Azure Develop Resources
Portal
Free account
Filter by title
Managed identities for Azure resources
Overview
Quickstarts
Tutorials
Concepts
How-to guides
Reference
Resources
Frequently asked questions
Known issues
Azure services that support managed identities for Azure resources
Azure services that support Azure Active Directory authentication
Stack Overflow
Azure AD Developers forum
Download PDF
Docs / Azure / Active Directory / Managed identities for Azure resources /
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
In this article
Next steps

Default Directory | App registrations

Azure Active Directory

- Overview
- Preview features
- Diagnose and solve problems

Manage

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

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

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

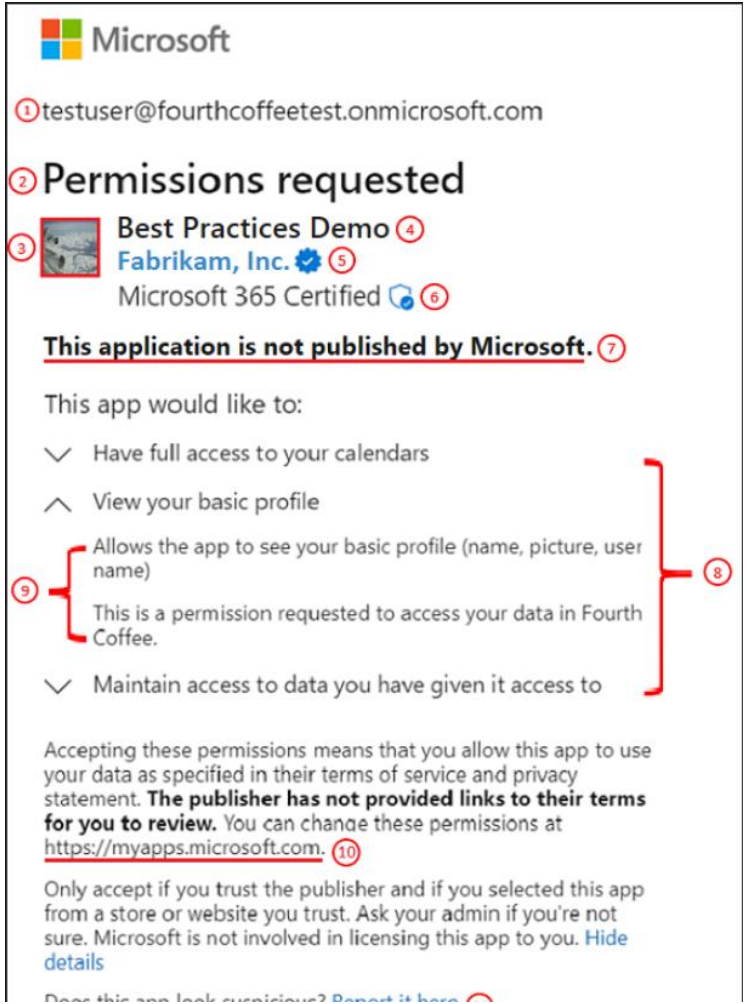
All applications | **Owned applications** | Deleted applications | Applications from personal account

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

Add filters

3 applications found

Display name	Application (client) ID
AP [redacted]	[redacted]9456-fa43724
ID [redacted]	a8e7964b-[redacted]-a707-9f9e3b8
KV kvder[redacted]	d9c2d[redacted]1-b4c9-771541


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.

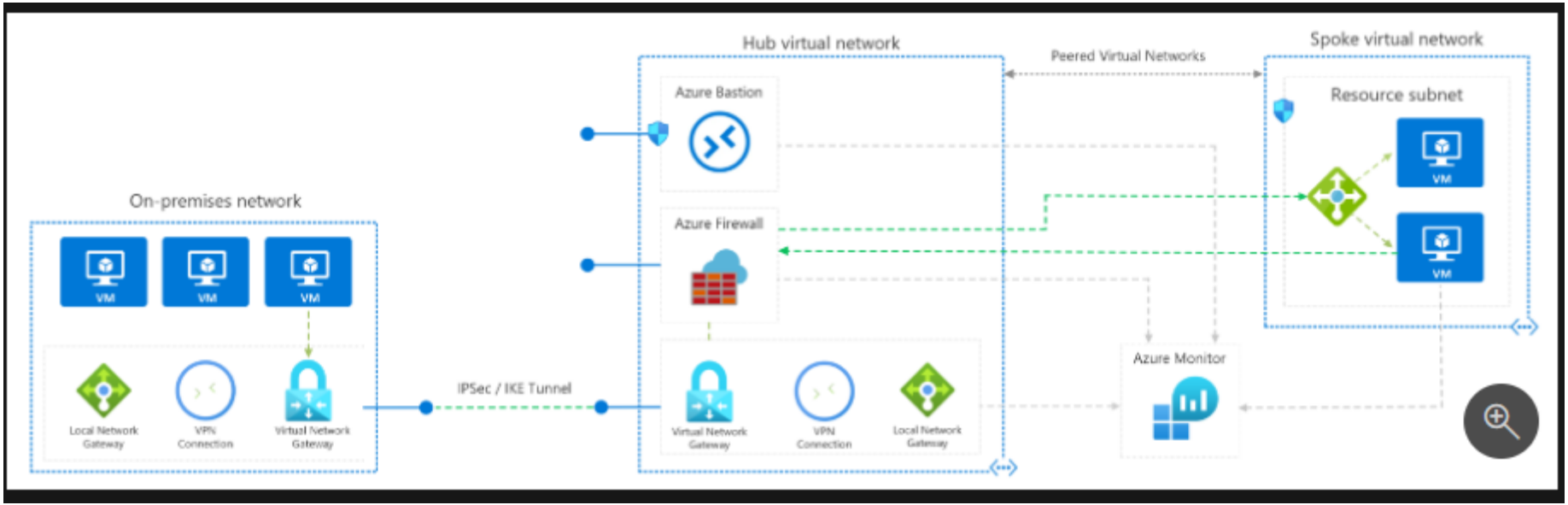
Secure networking

- 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

Plan and implement security for virtual networks

- Plan and implement Network Security Groups (NSGs) and Application Security Groups (ASGs)
- 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

Hybrid Network

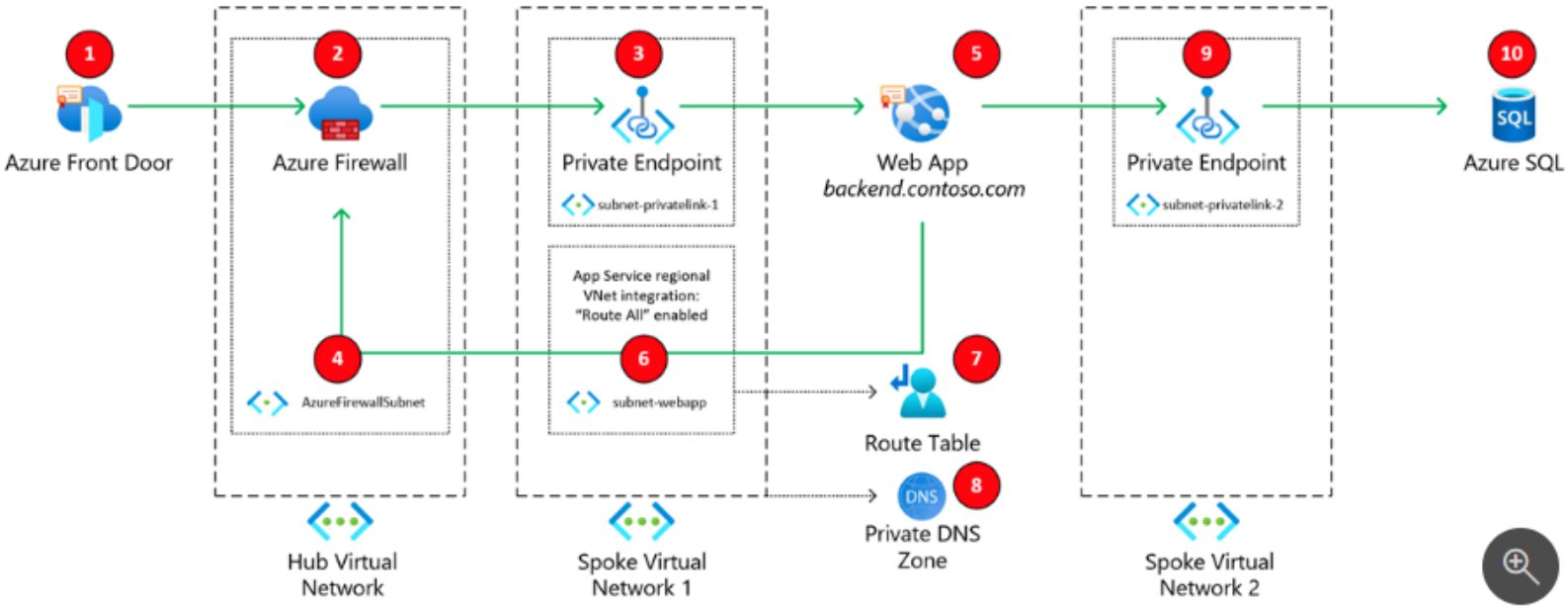


Plan and implement security for private access to Azure resources

- 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

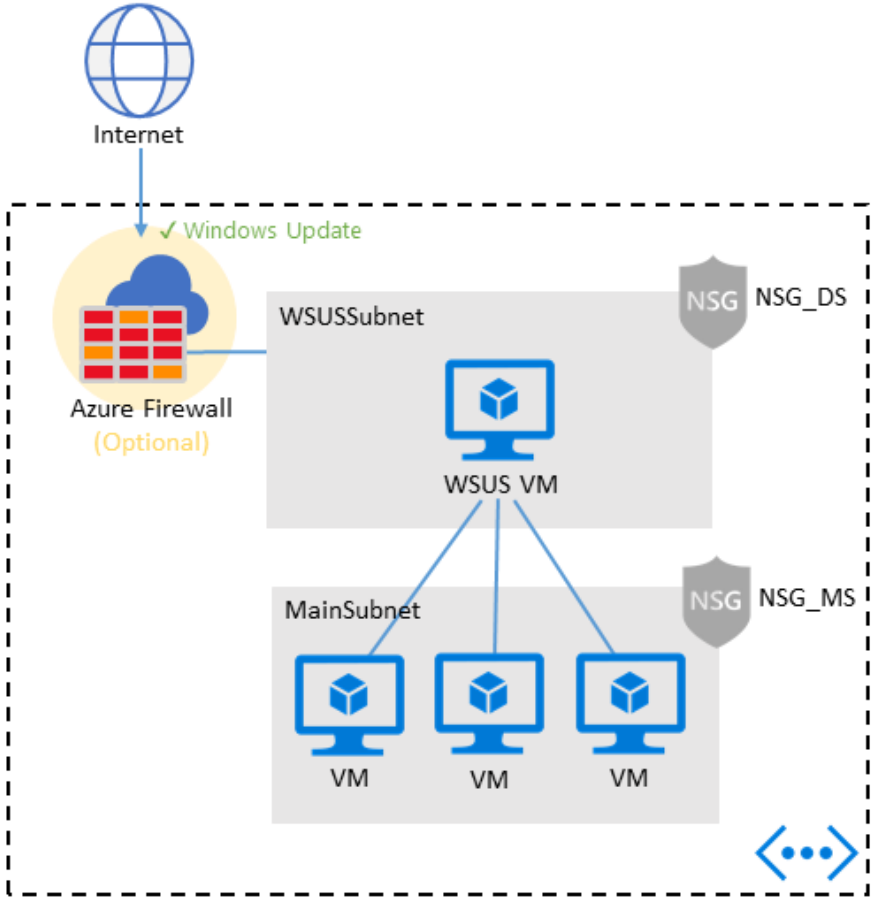
Note

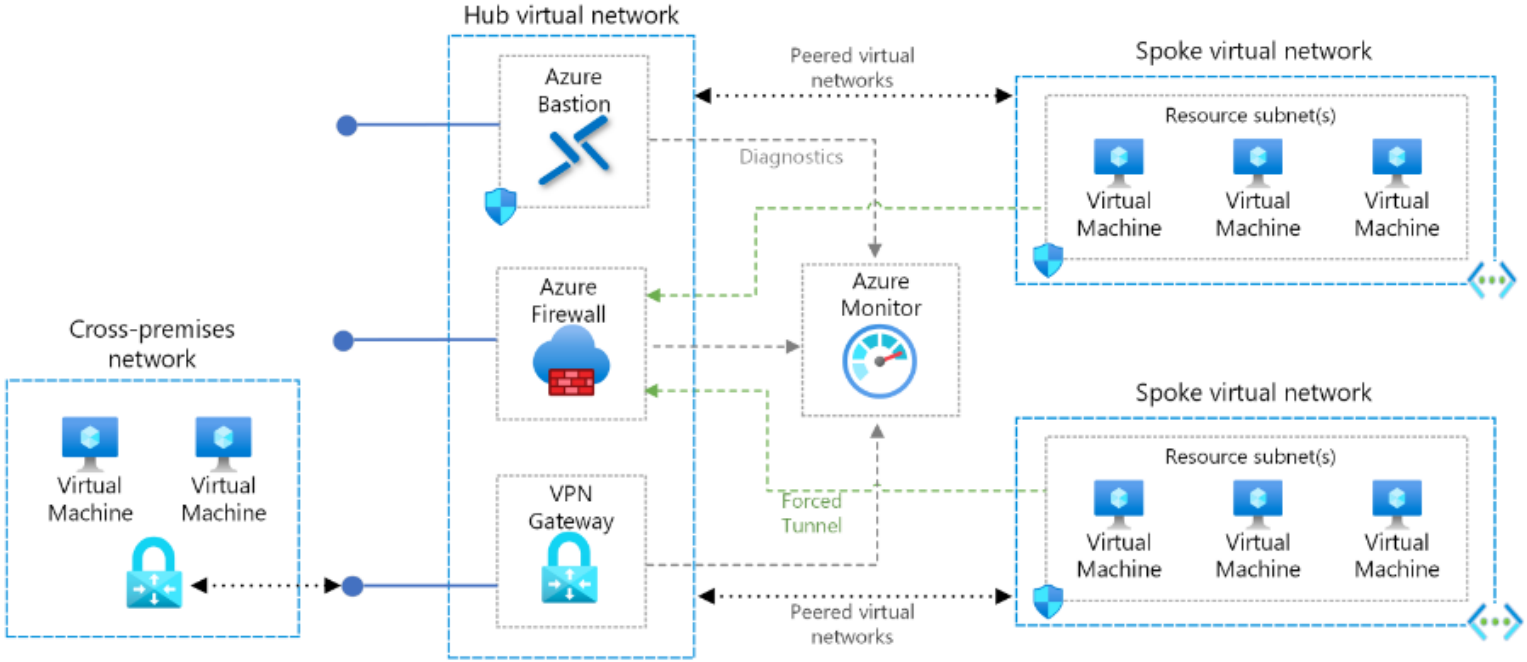
Microsoft recommends use of Azure Private Link for secure and private access to services hosted on Azure platform. For more information, see **Azure Private Link**.


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

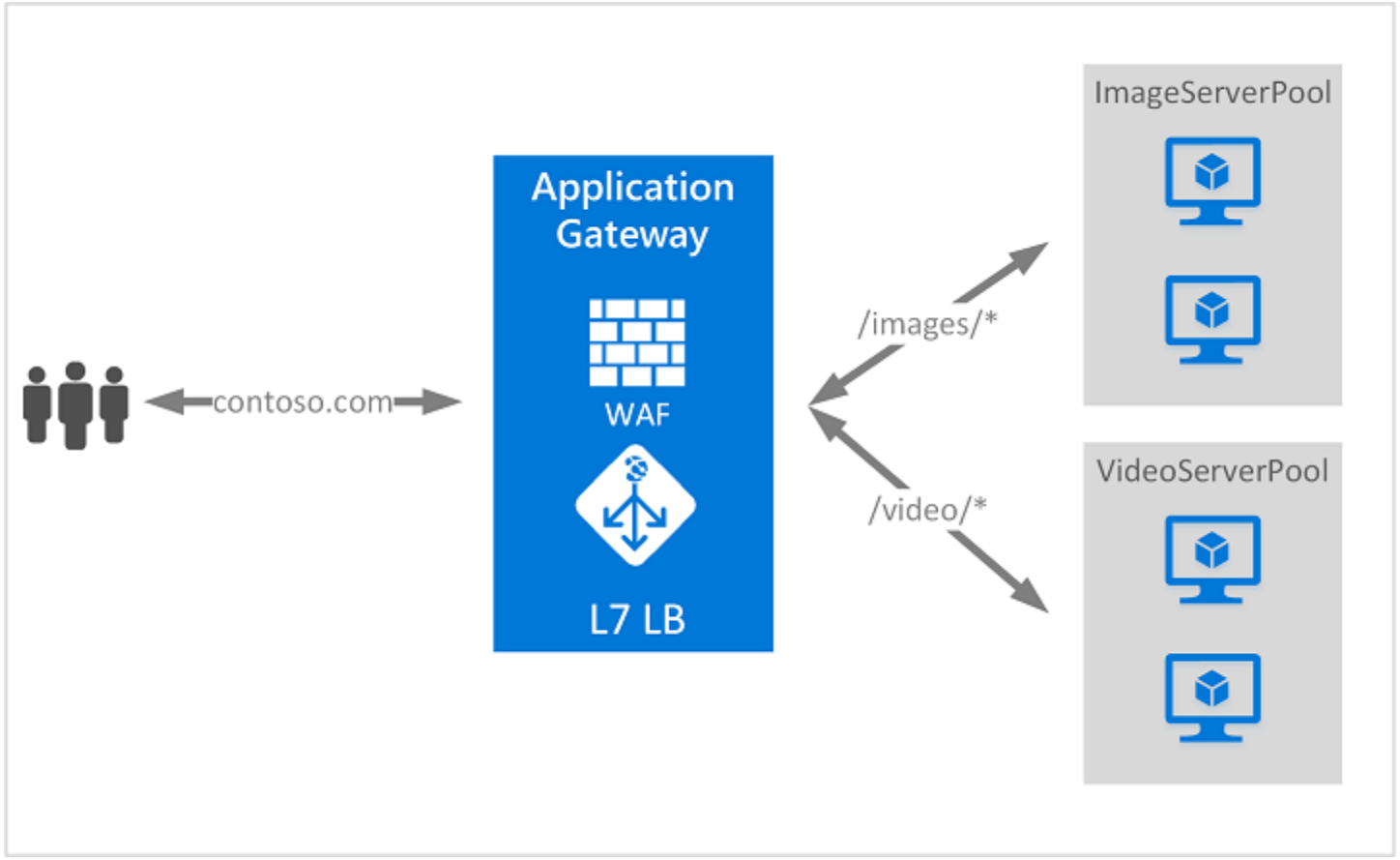
Plan and implement security for public access to Azure resources

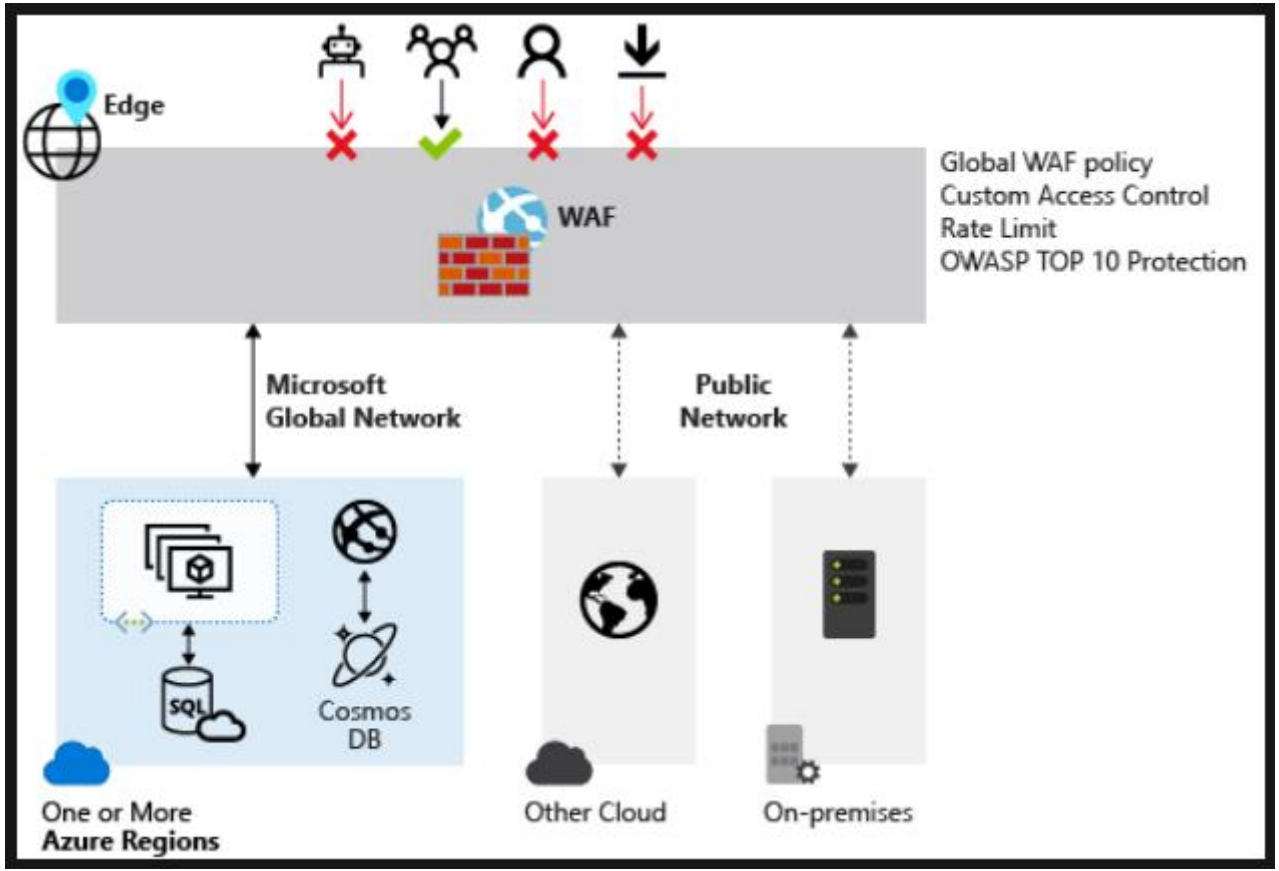
- Plan and implement TLS to applications, including Azure App Service and API Management
- Plan, implement, and manage an Azure Firewall, including Azure Firewall Manager and firewall policies
- Plan and implement an Azure Application Gateway
- Plan and implement an Azure Front Door, including Content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

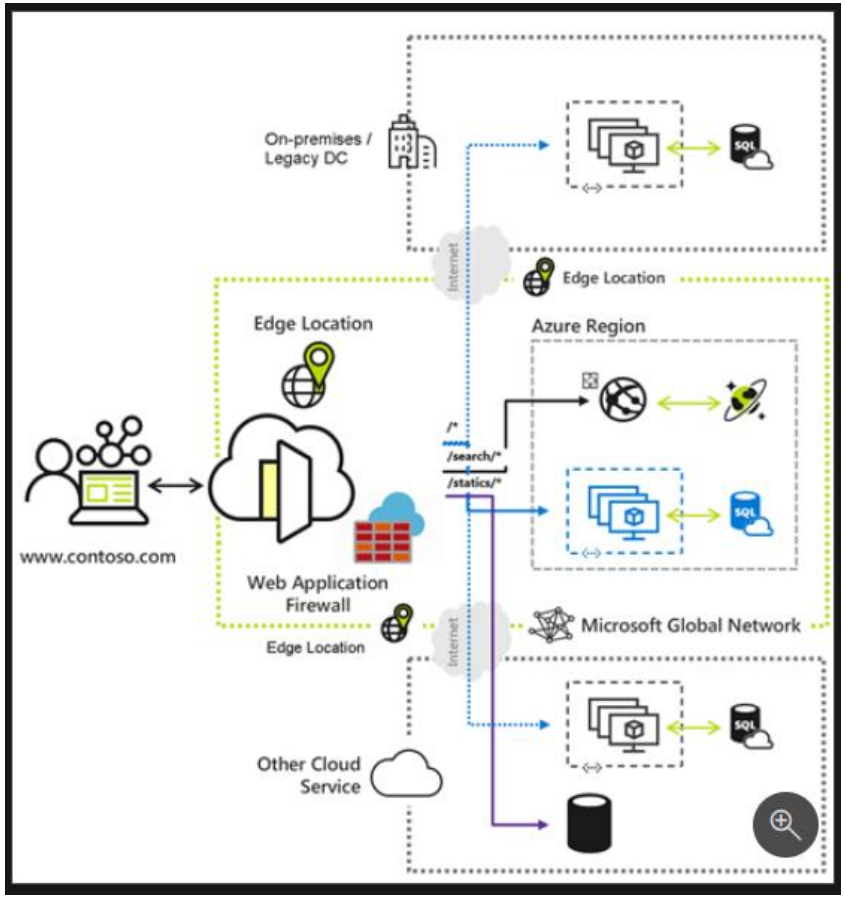

Internet
✓ Windows Update
Azure Firewall
(Optional)
WSUSSubnet
NSG
NSG_DS
WSUS VM
MainSubnet
NSG
NSG_MS
VM
VM
VM

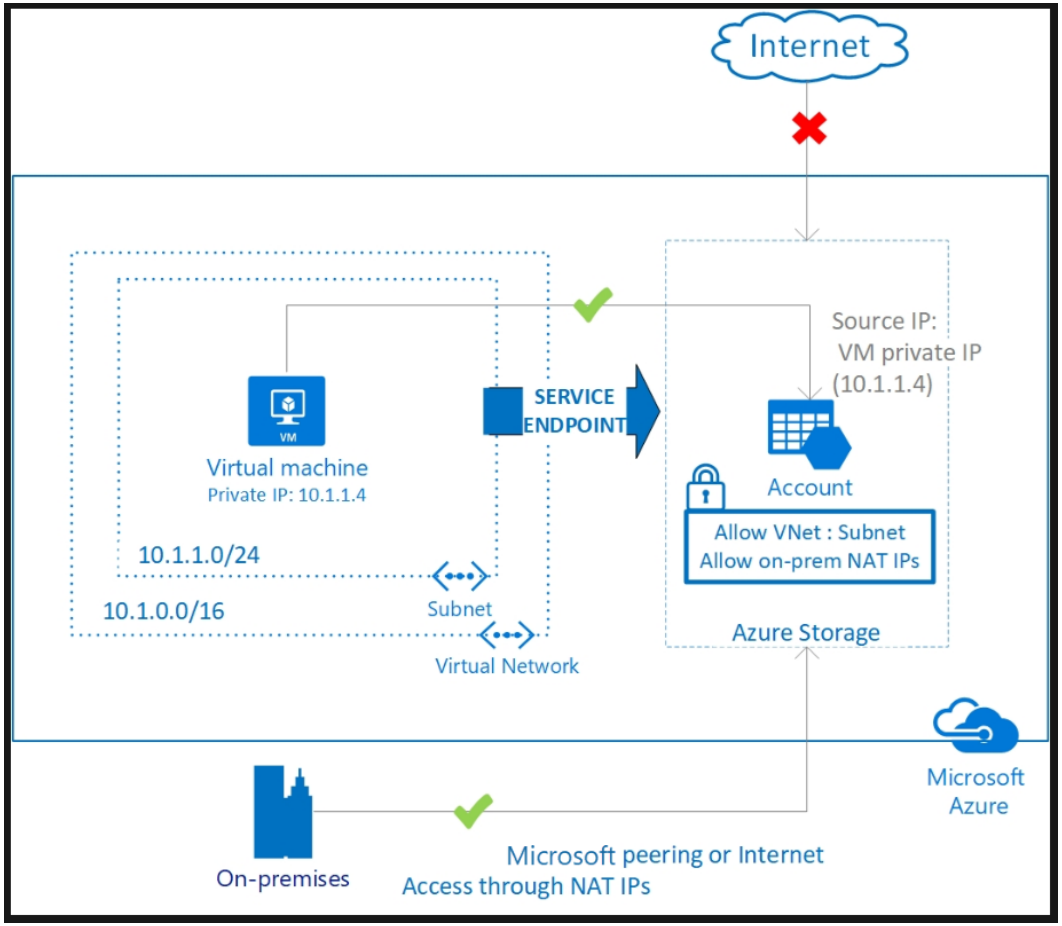


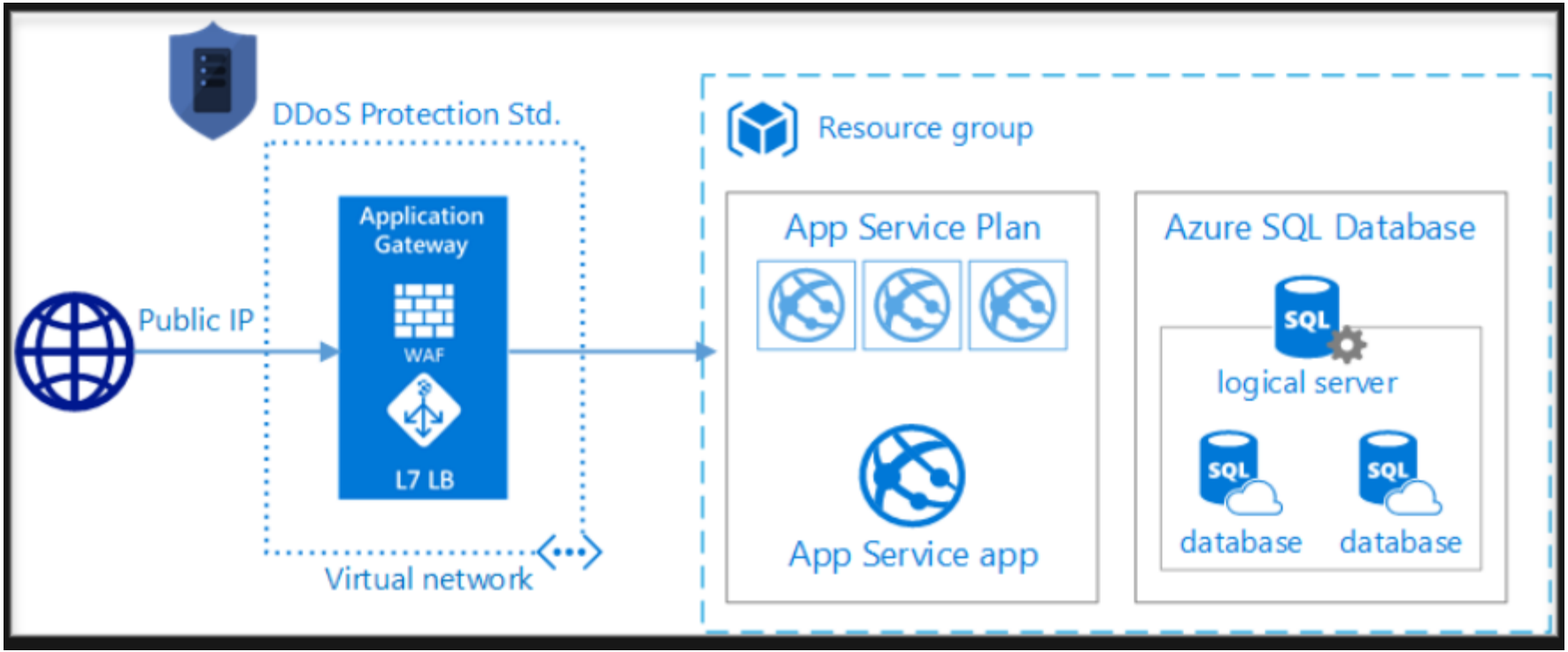
Microsoft Azure

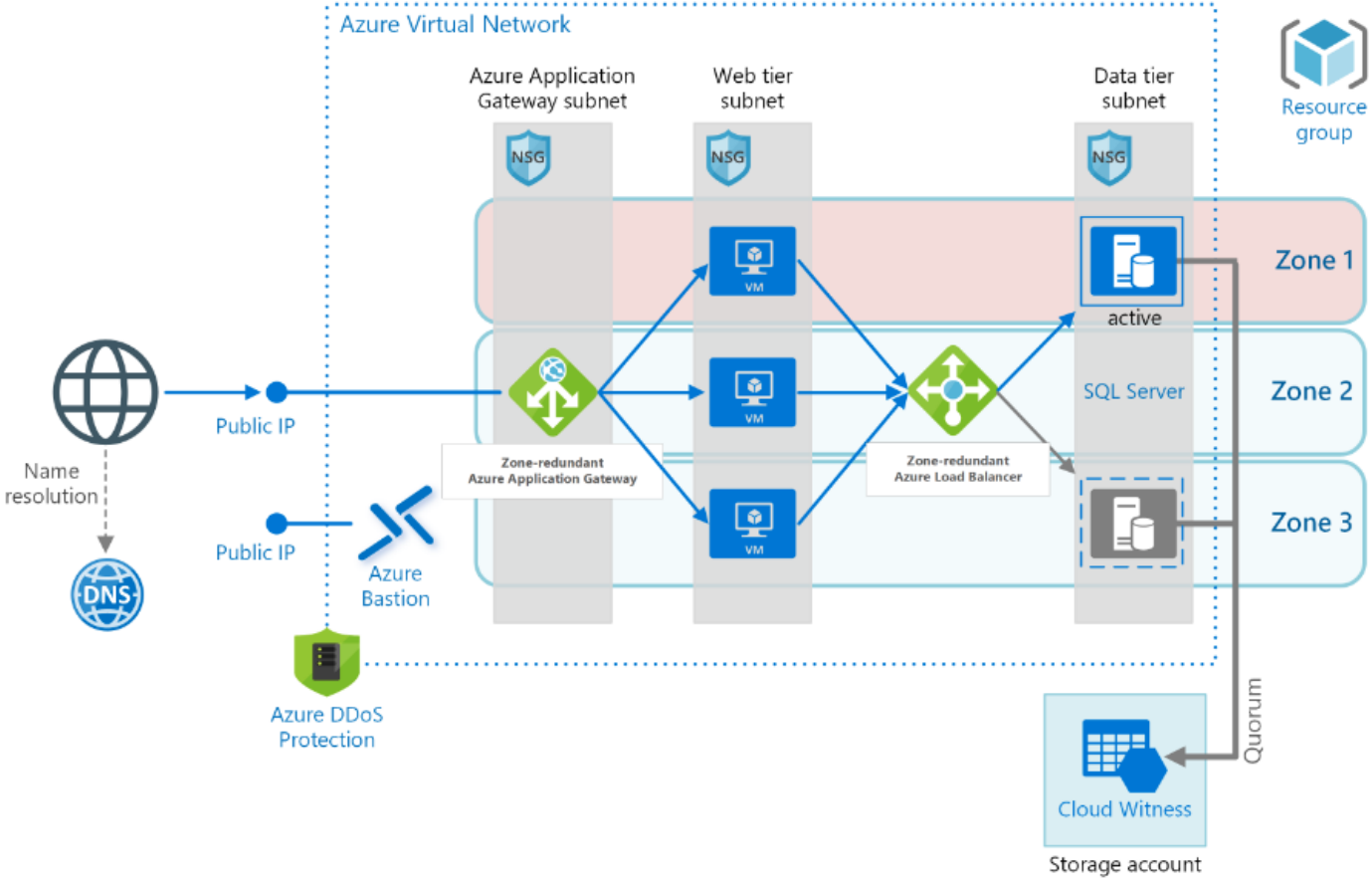

Application Gateway
WAF
L7 LB
contoso.com
/images/*
/video/*
ImageServerPool
VideoServerPool


Edge
WAF
Global WAF policy
Custom Access Control
Rate Limit
OWASP TOP 10 Protection
Microsoft
Global Network
Public
Network
SQL
Cosmos
DB
One or More
Azure Regions
Other Cloud
On-premises


On-premises /
Legacy DC
SQL
Internet
Edge Location
Edge Location
Azure Region
/*
/search/*
/statics/*
SQL
www.contoso.com
Web Application
Firewall
Edge Location
Internet
Microsoft Global Network
SQL
Other Cloud
Service


Internet
Source IP:
VM private IP
(10.1.1.4)
SERVICE
ENDPOINT
VM
Virtual machine
Private IP: 10.1.1.4
Account
Allow VNet : Subnet
Allow on-prem NAT IPs
10.1.1.0/24
10.1.0.0/16
Subnet
Virtual Network
Azure Storage
Microsoft
Azure
On-premises
Microsoft peering or Internet
Access through NAT IPs


DDoS Protection Std.
Resource group
Application Gateway
WAF
L7 LB
Public IP
App Service Plan
App Service app
Azure SQL Database
SQL
logical server
SQL
database
SQL
database
Virtual network


Azure Virtual Network
Azure Application Gateway subnet
Web tier subnet
Data tier subnet
Resource group
NSG
NSG
NSG
VM
VM
VM
Zone 1
Zone 2
Zone 3
active
SQL Server
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%)
- Manage security operations (25–30%)

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

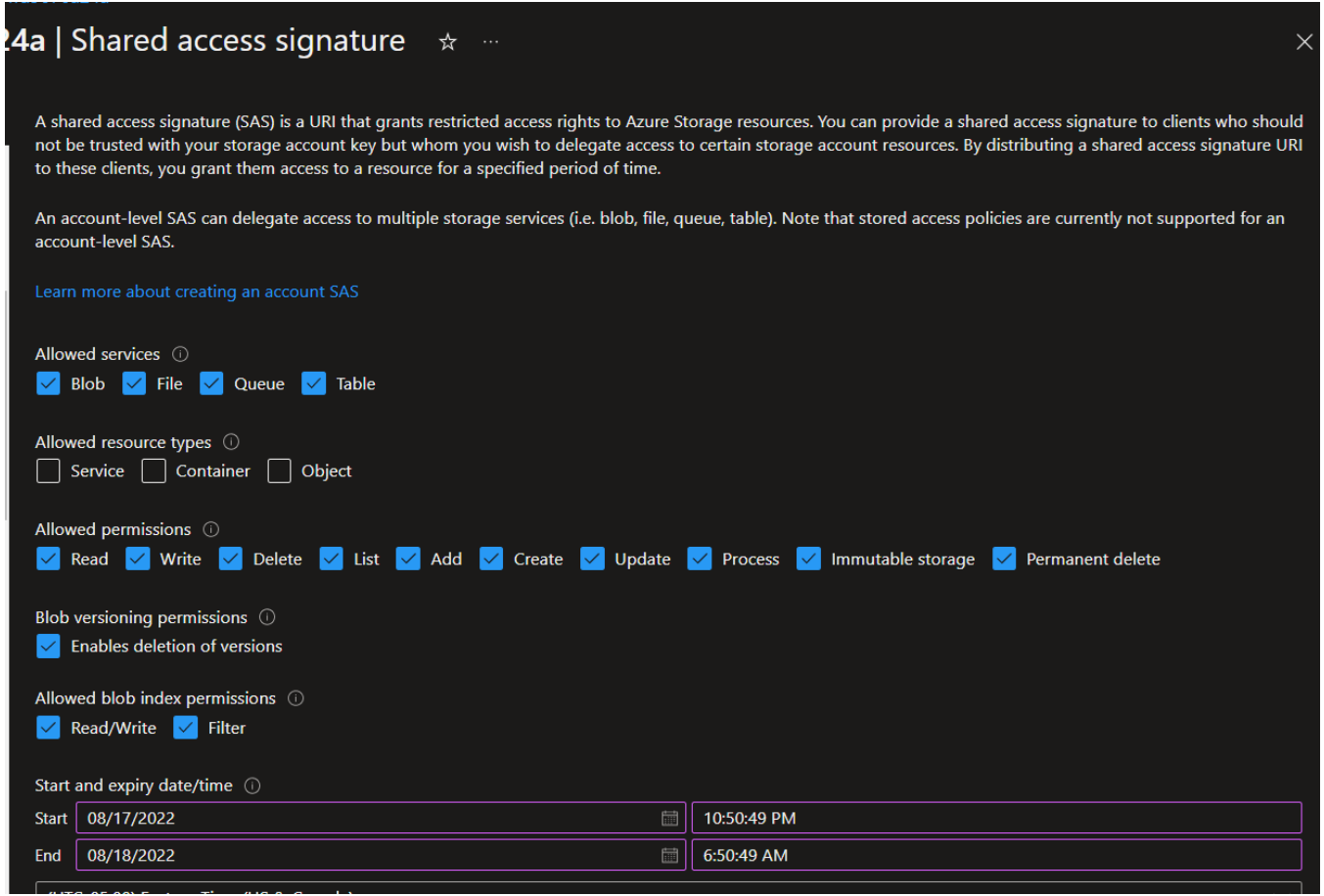
Plan and implement advanced security for compute

- Plan and implement remote access to public endpoints, including Azure Bastion and JIT
- 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

Plan and implement security for storage

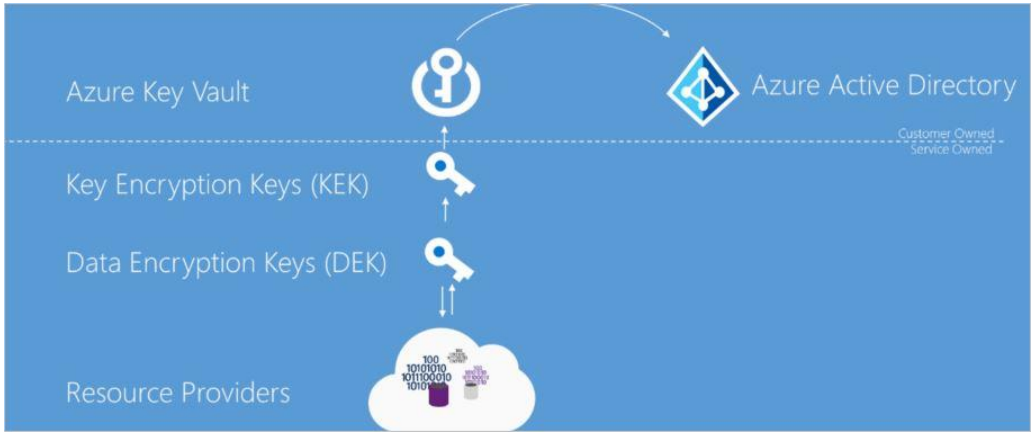
- Configure access control for storage accounts
- Manage life cycle for storage account access keys
- Select and configure an appropriate method for access to Azure Files
- Select and configure an appropriate method for access to Azure Blob Storage
- Select and configure an appropriate method for access to Azure Tables
- Select and configure an appropriate method for access to Azure Queues
- 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

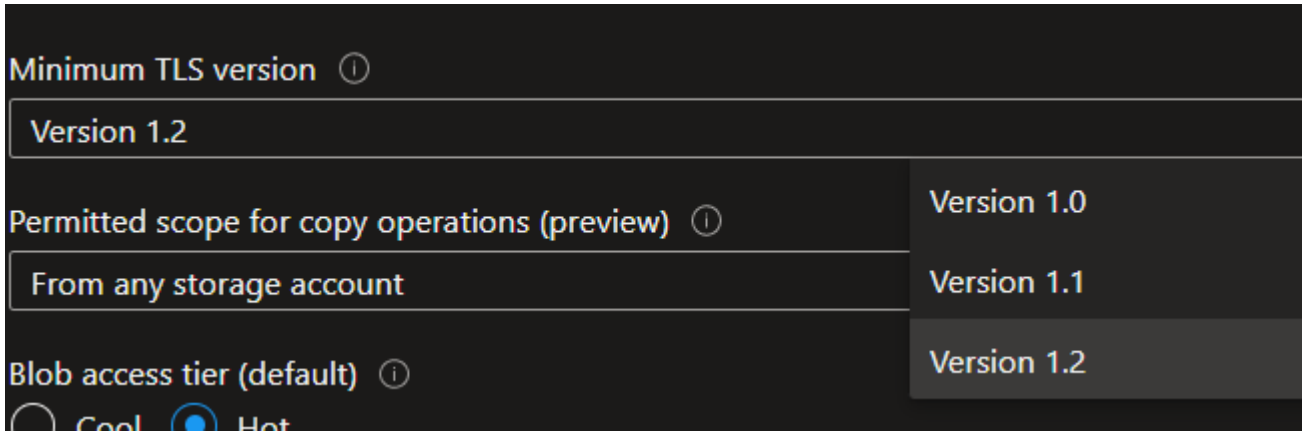
Configure Encryption at Rest

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



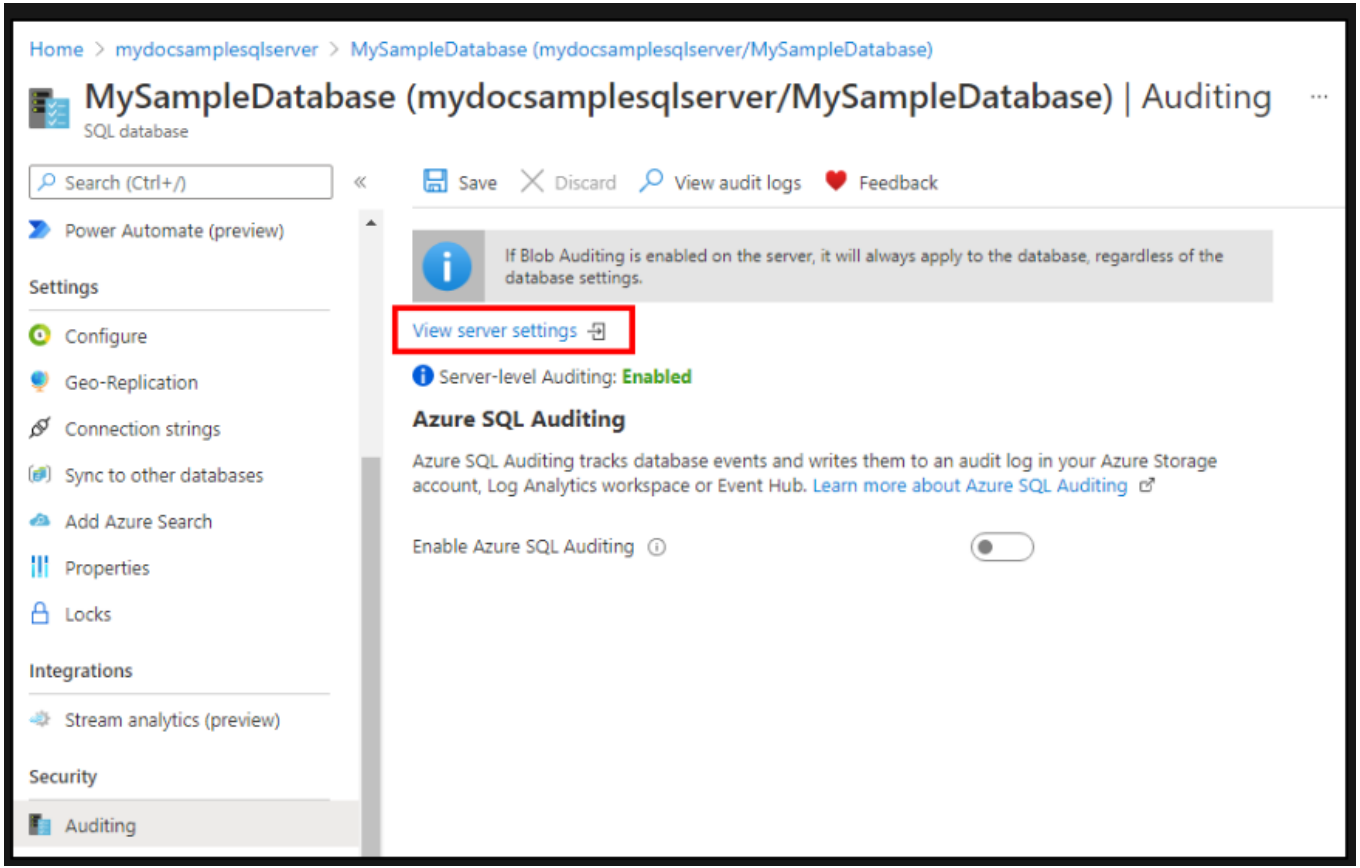
Configure Encryption in Transit

- Encryption of data in transit

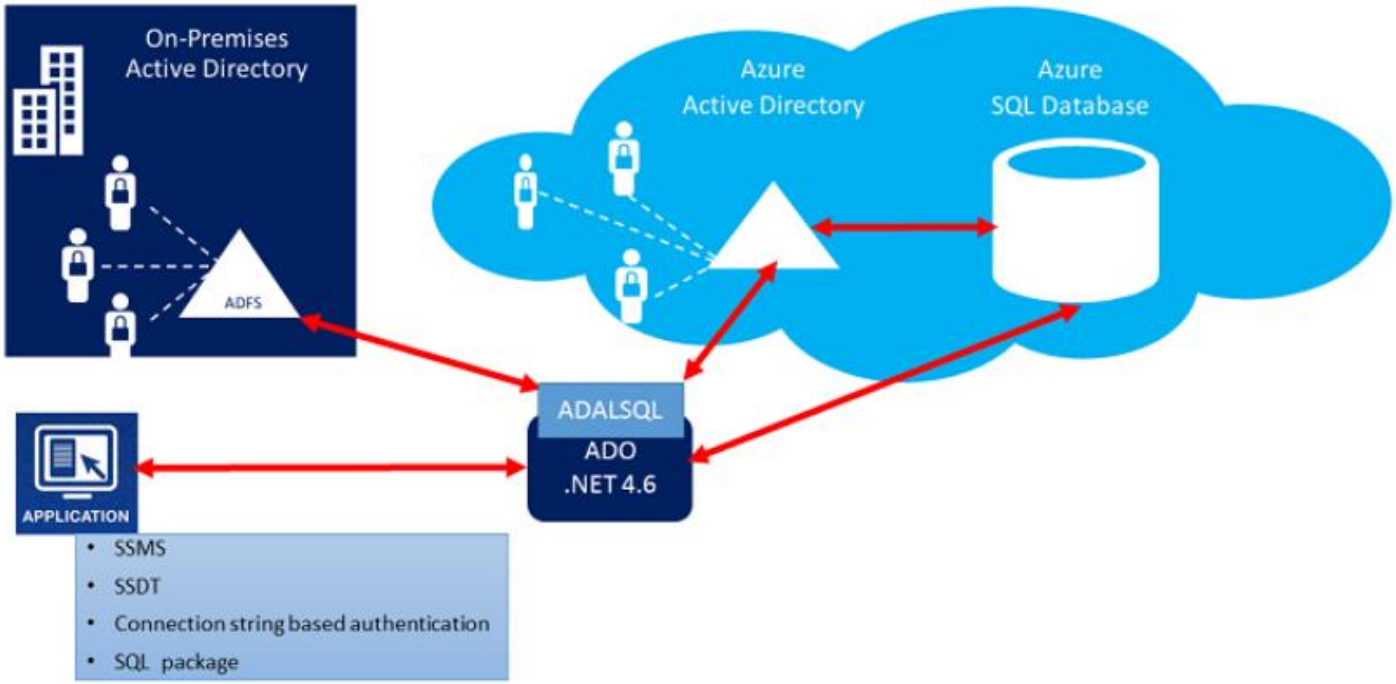


Plan and implement security for Azure SQL Database and Azure SQL Managed Instance

- Enable database authentication by using Microsoft Azure Active Directory (Azure AD), part of Microsoft Entra
- Enable database auditing
- Identify use cases for the Microsoft Purview governance portal
- Implement data classification of sensitive information by using the Microsoft Purview governance portal
- 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

Azure AD Authentication with SQL V12 DB

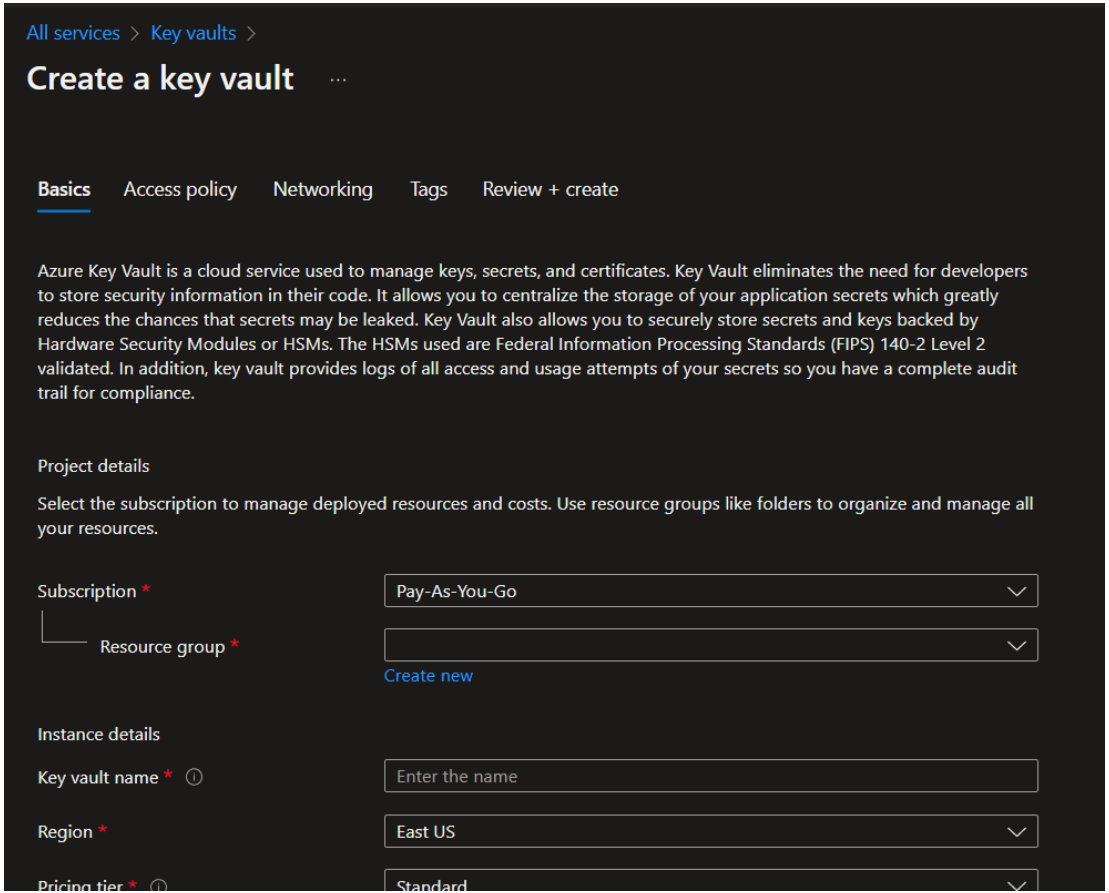


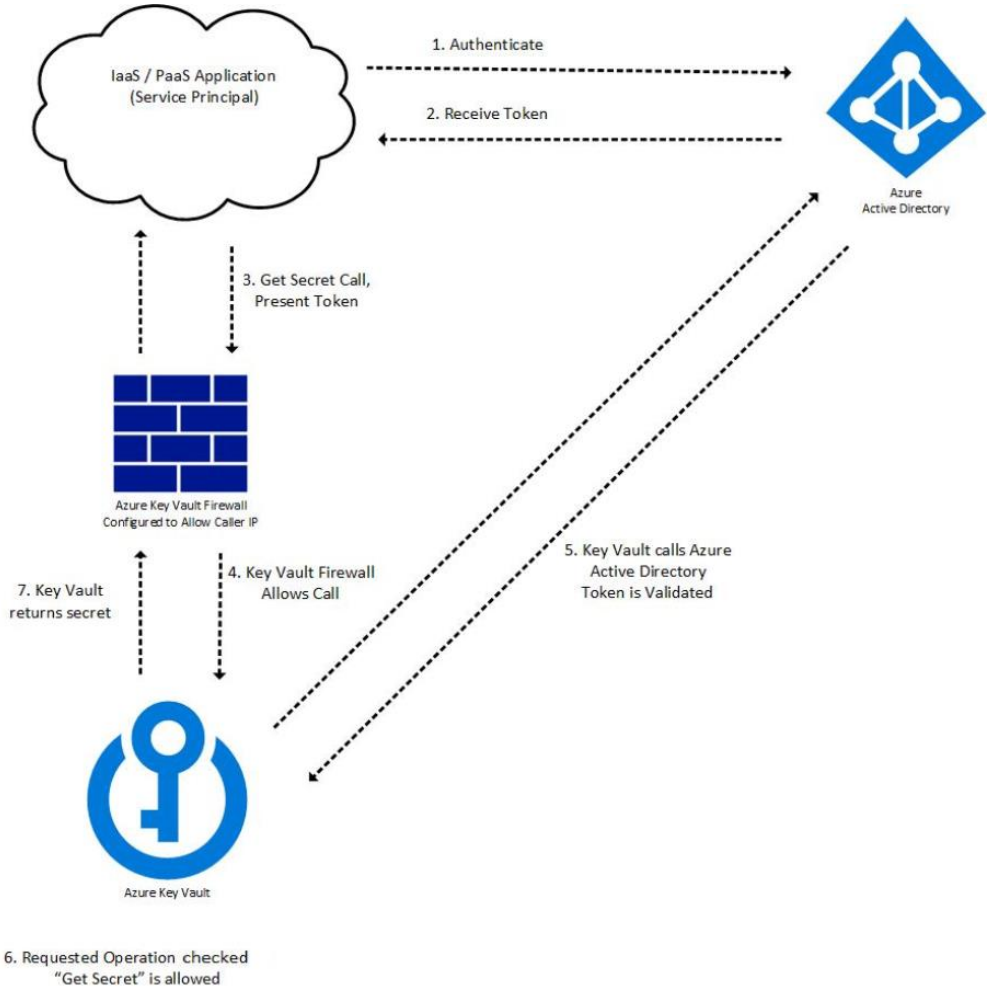
Manage security operations

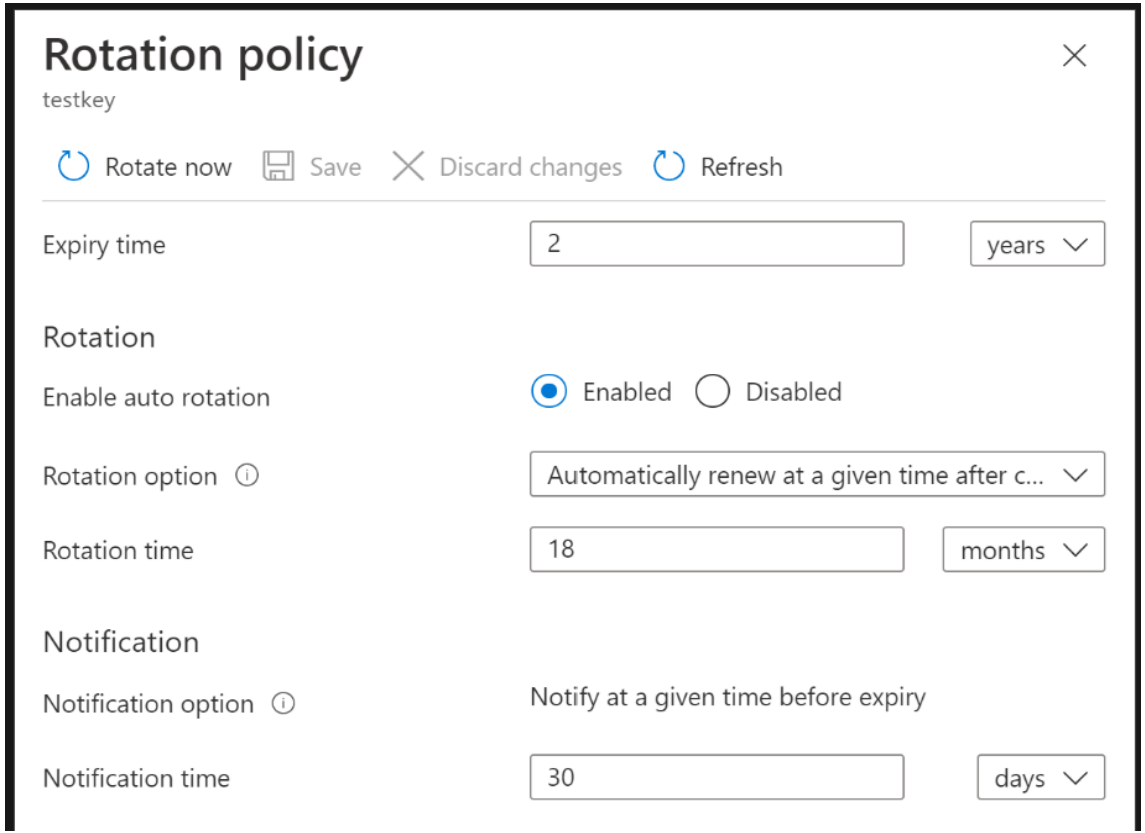
- Plan, implement, and manage governance for security
- Manage security posture by using Microsoft Defender for Cloud
- Configure and manage threat protection by using Microsoft Defender for Cloud
- Configure and manage security monitoring and automation solutions

Plan, implement, and manage governance for security

- Create, assign, and interpret security policies and initiatives in Azure Policy
- Configure security settings by using Azure Blueprint
- Deploy secure infrastructures by using a landing zone
- Create and configure an Azure Key Vault
- Recommend when to use a Dedicated HSM
- Configure access to Key Vault, including vault access policies and Azure Role Based Access Control
- Manage certificates, secrets, and keys
- Configure key rotation
- Configure backup and recovery of certificates, secrets, and keys


All services > Key vaults >
Create a key vault
...
Basics
Access policy
Networking
Tags
Review + create
Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. Key Vault eliminates the need for developers to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, key vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance.
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
Key vault name *
Enter the name
Region *
East US
Pricing tier *
Standard


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

Home > Key vaults > new-primary-vault | Keys >

test

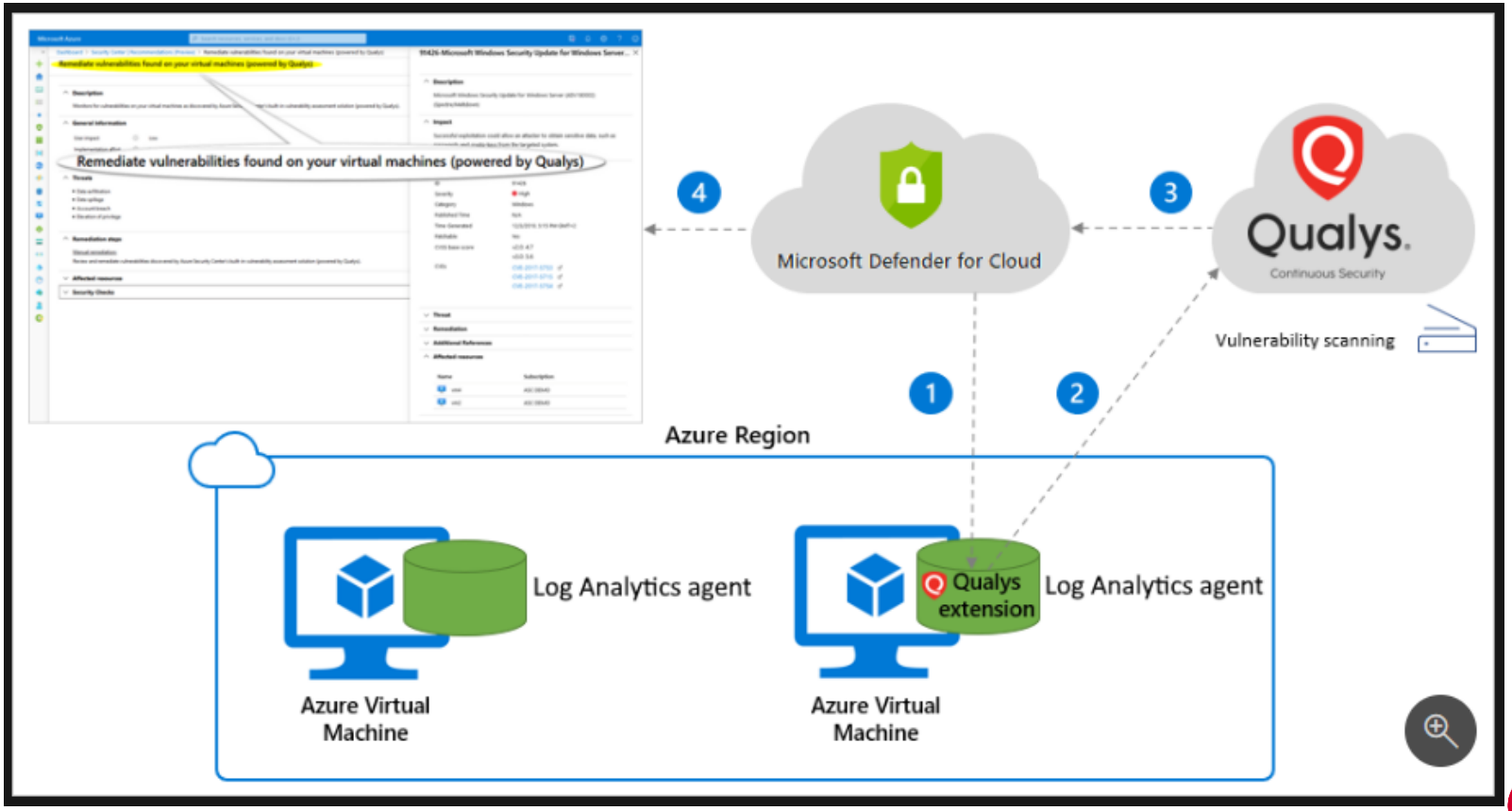
Versions

+ New Version | Refresh | Delete | Download Backup

Version	Status	Activation Date	Expiration Date
CURRENT VERSION			
f3c	✓ Enabled		
OLDER VERSIONS			
0ee1	✓ Enabled	5/5/2020	5/5/2022

Manage security posture by using Microsoft Defender for Cloud

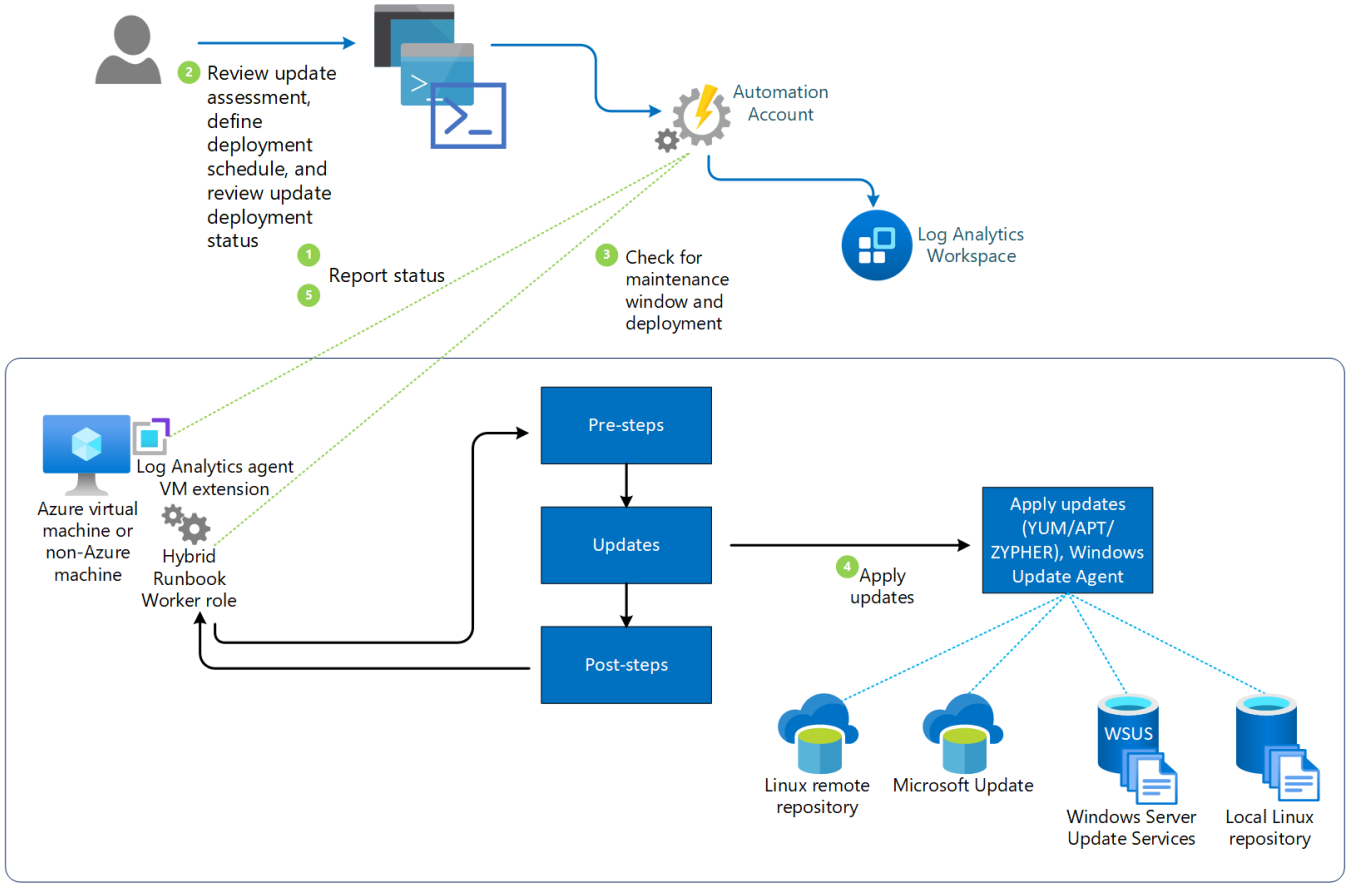
- Identify and remediate security risks by using the Microsoft Defender for Cloud Secure Score and Inventory
- Assess compliance against security frameworks and Microsoft Defender for Cloud
- Add industry and regulatory standards to Microsoft Defender for Cloud
- Add custom initiatives to Microsoft Defender 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


Remediate vulnerabilities found on your virtual machines (powered by Qualys)
4
Microsoft Defender for Cloud
3
Qualys.
Continuous Security
Vulnerability scanning
1
2
Azure Region
Log Analytics agent
Azure Virtual Machine
Qualys extension
Log Analytics agent
Azure Virtual Machine

Configure and manage threat protection by using Microsoft Defender for Cloud

- Enable workload protection services in Microsoft Defender for Cloud, including Microsoft Defender for Storage, Databases, Containers, App Service, Key Vault, Resource Manager, and DNS
- Configure Microsoft Defender for Servers
- Configure Microsoft Defender for Azure SQL Database
- Manage and respond to security alerts in Microsoft Defender for Cloud
- Configure workflow automation by using Microsoft Defender for Cloud
- Evaluate vulnerability scans from Microsoft Defender for Server
- Use the Microsoft Threat Modeling Tool

Implement and Manage Security Updates for VMs



Configure and manage security monitoring and automation solutions

- Monitor security events by using Azure Monitor
- Configure data connectors in Microsoft Sentinel
- Create and customize analytics rules in Microsoft Sentinel
- Evaluate alerts and incidents in Microsoft Sentinel
- Configure automation in Microsoft Sentinel

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

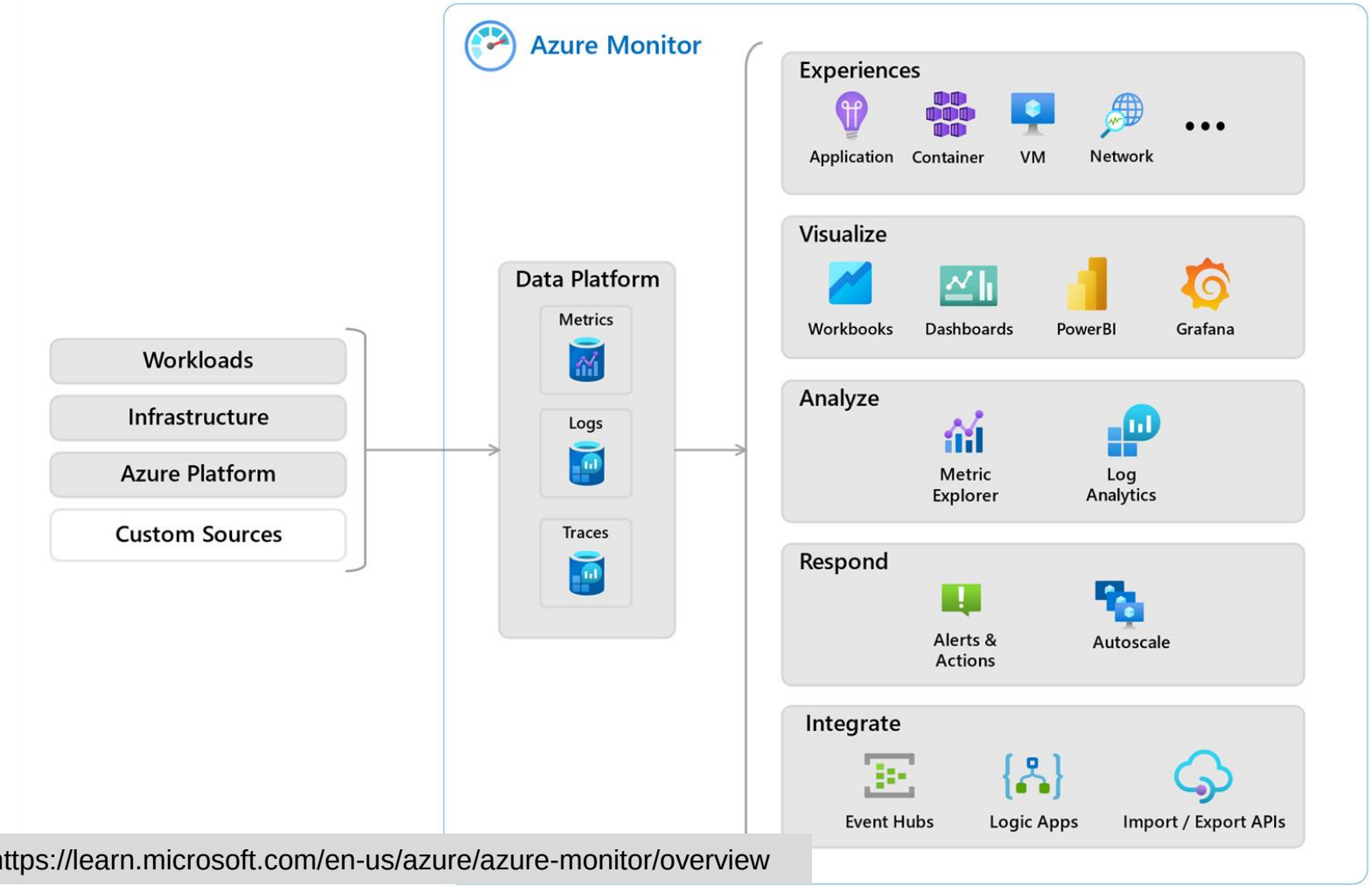
The default initiative enabled on your subscription generates the security recommendations in the **Recommendations** pag

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

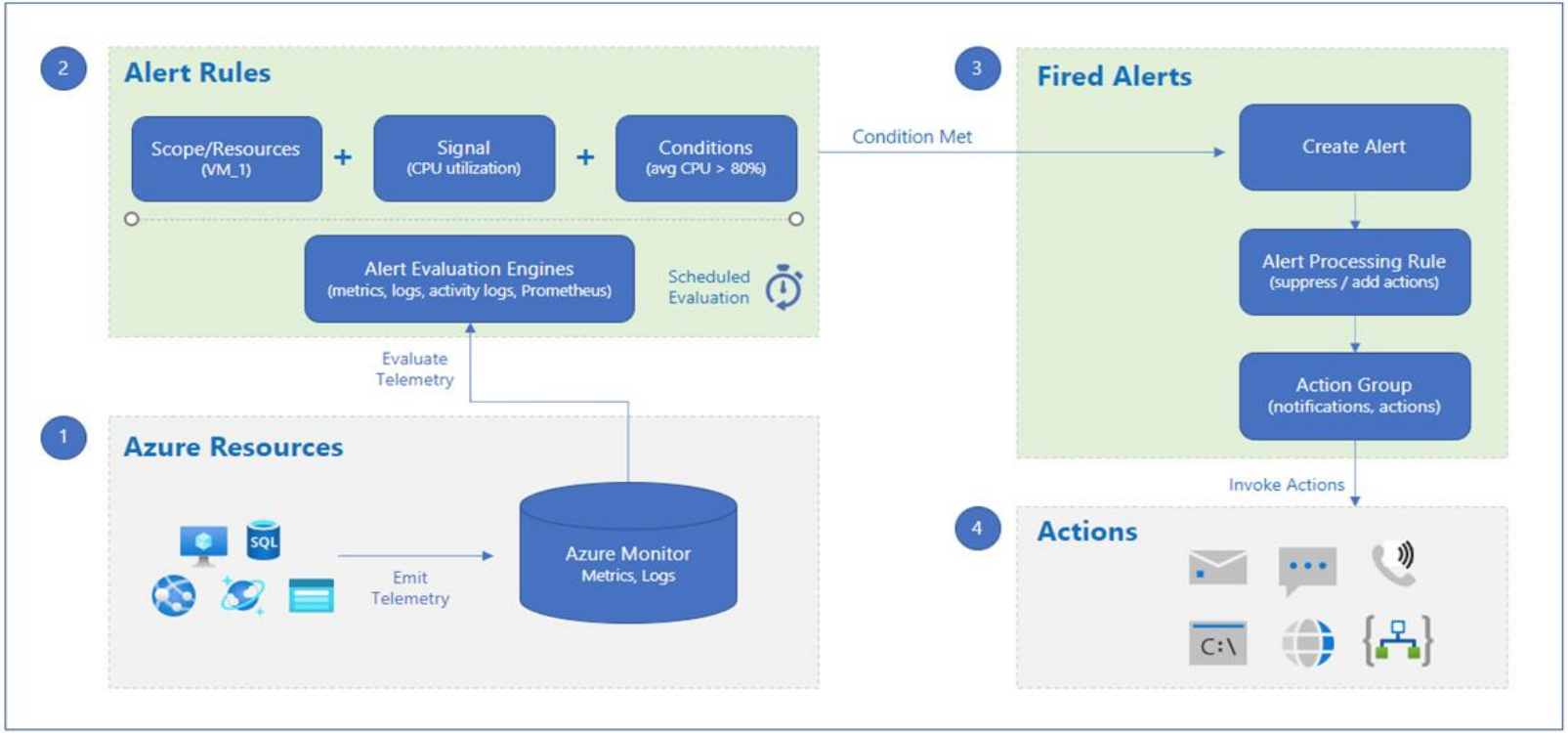
Industry & regulatory standards

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

Azure Security	Track Azure Security	Out of the

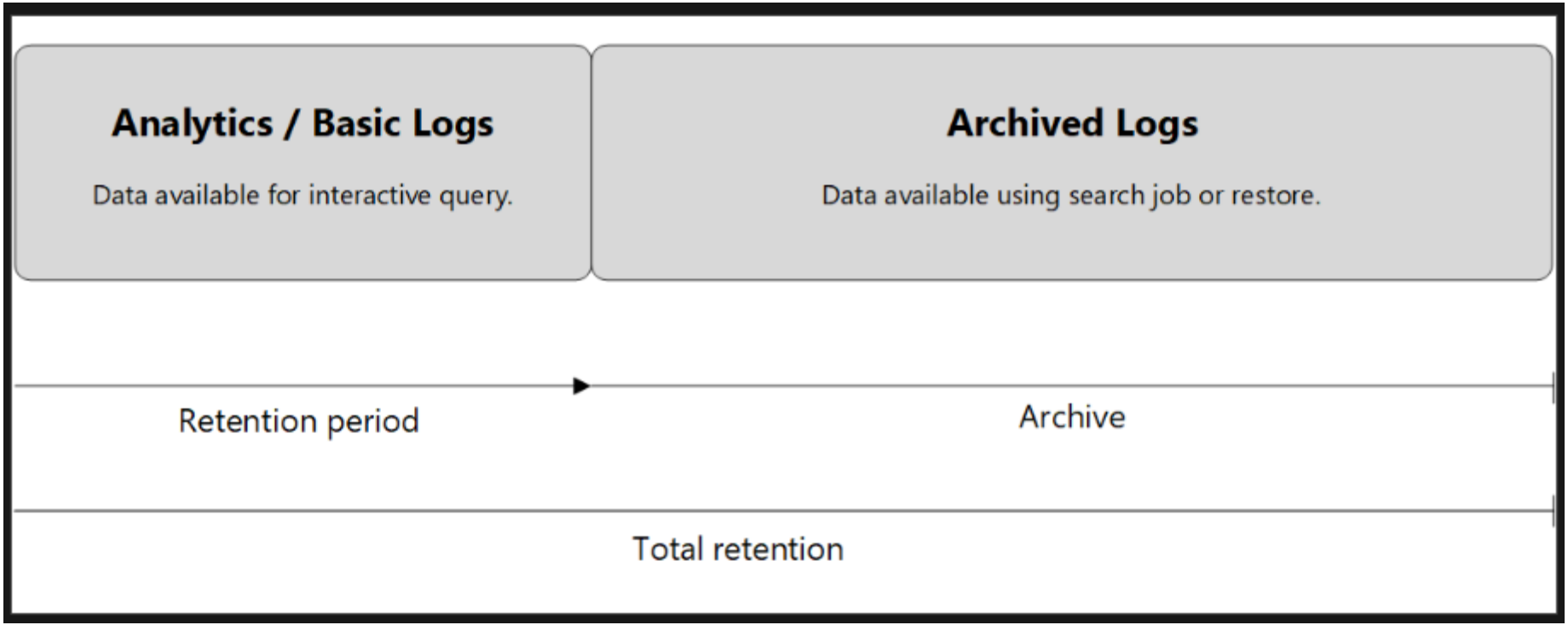


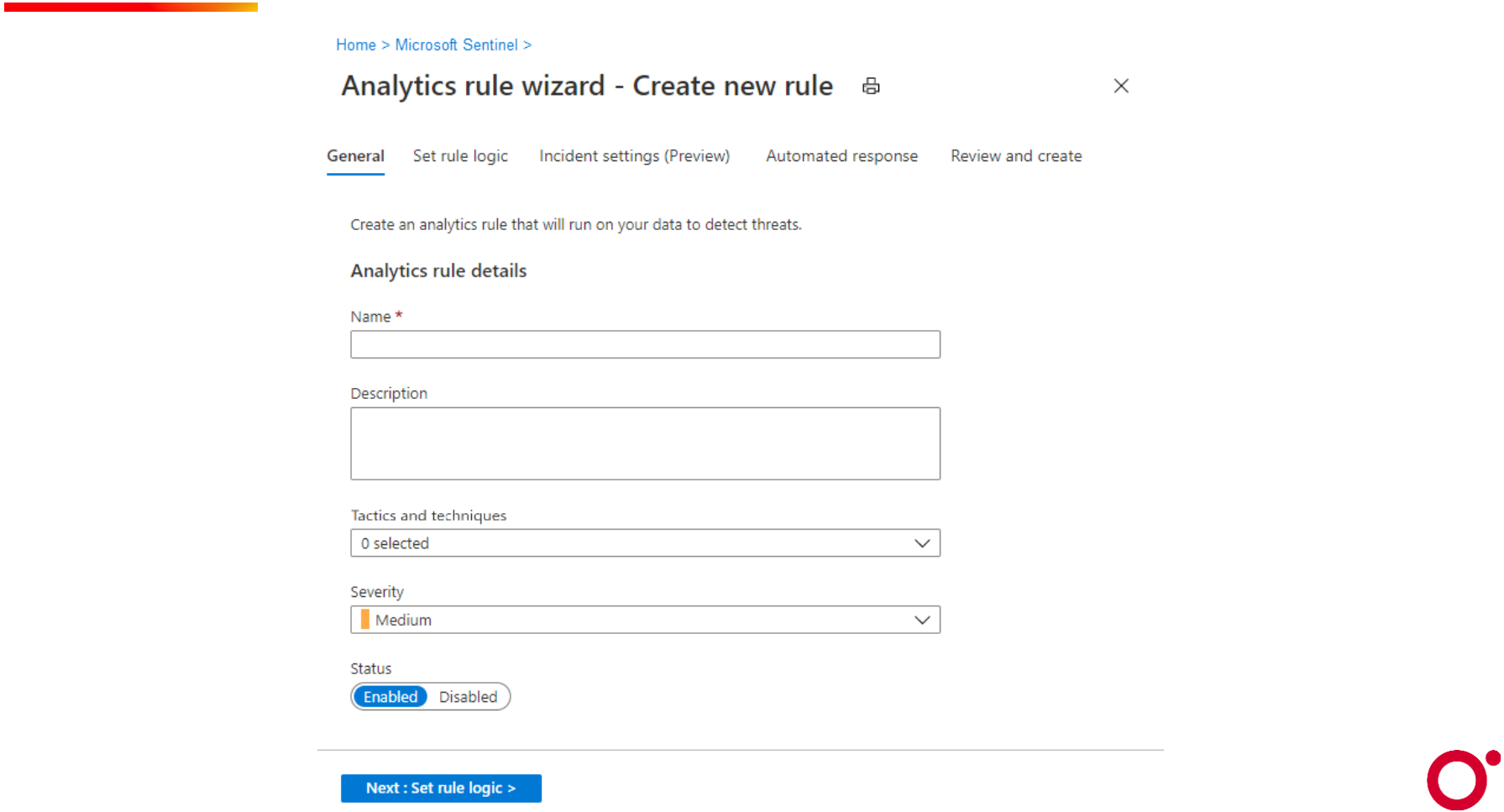
https://learn.microsoft.com/en-us/azure/azure-monitor/overview



Alerts boundary

External boundary


Analytics / Basic Logs
Data available for interactive query.
Archived Logs
Data available using search job or restore.
Retention period
Archive
Total retention


Home > Microsoft Sentinel >
Analytics rule wizard - Create new rule
General
Set rule logic
Incident settings (Preview)
Automated response
Review and create
Create an analytics rule that will run on your data to detect threats.
Analytics rule details
Name *
Description
Tactics and techniques
0 selected
Severity
Medium
Status
Enabled
Disabled
Next : Set rule logic >

The Exam

Questions in AZ-500

- Number of Questions ~45 Questions
- Questions
  - Multiple choice
  - Drag and drop
  - Scenario based
- There will NOT be hands-on 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 our Exam Sandbox

AZ-500

- Exam AZ-204:

  https://learn.microsoft.com/en-us/certifications/exams/az-500
- Skills measured :

  https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3VC70

Questions in AZ-500

Tip

- Watch **AZ-500 Exam Prep videos** on Learn
- Download the **AZ-500 study guide** to help you prepare for the exam
- Demo the exam experience by visiting our **Exam Sandbox**

Schedule exam

Exam AZ-500: Microsoft Azure Security Technologies

United States

Languages: English, Japanese, Chinese (Simplified), Korean, German, French, Spanish, Portuguese (Brazil), Arabic (Saudi Arabia), Russian, Chinese (Traditional), Italian, Indonesian (Indonesia)
Retirement date: none

This exam measures your ability to accomplish the following technical tasks: manage identity and access; implement platform protection; manage security operations; and secure data and applications.

$165 USD*

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

Schedule exam >

Official practice test for Microsoft Azure Security Technologies
All objectives of the exam are covered in depth so you'll be ready for any question on the exam.

⊕ Save

Select exam options

AZ-104: Microsoft Azure Administrator

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

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.

Cart

Review and confirm contact information to avoid issues on test day.

Description	Details	Price	Actions
		165.00	Remove

Available Products

In addition to scheduling your exam, you might be interested in the following products.

Microsoft Official Practice Test powered by MeasureUp - 30 day online access
Get a discount on available Microsoft Official Practice Test for Microsoft certification exams (Fundamentals, Role-based, or Specialty) 30-day online access.

Special offer: Regularly priced at USD 99.00! Click here for details

More Details

USD 80.00

Add to Order

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

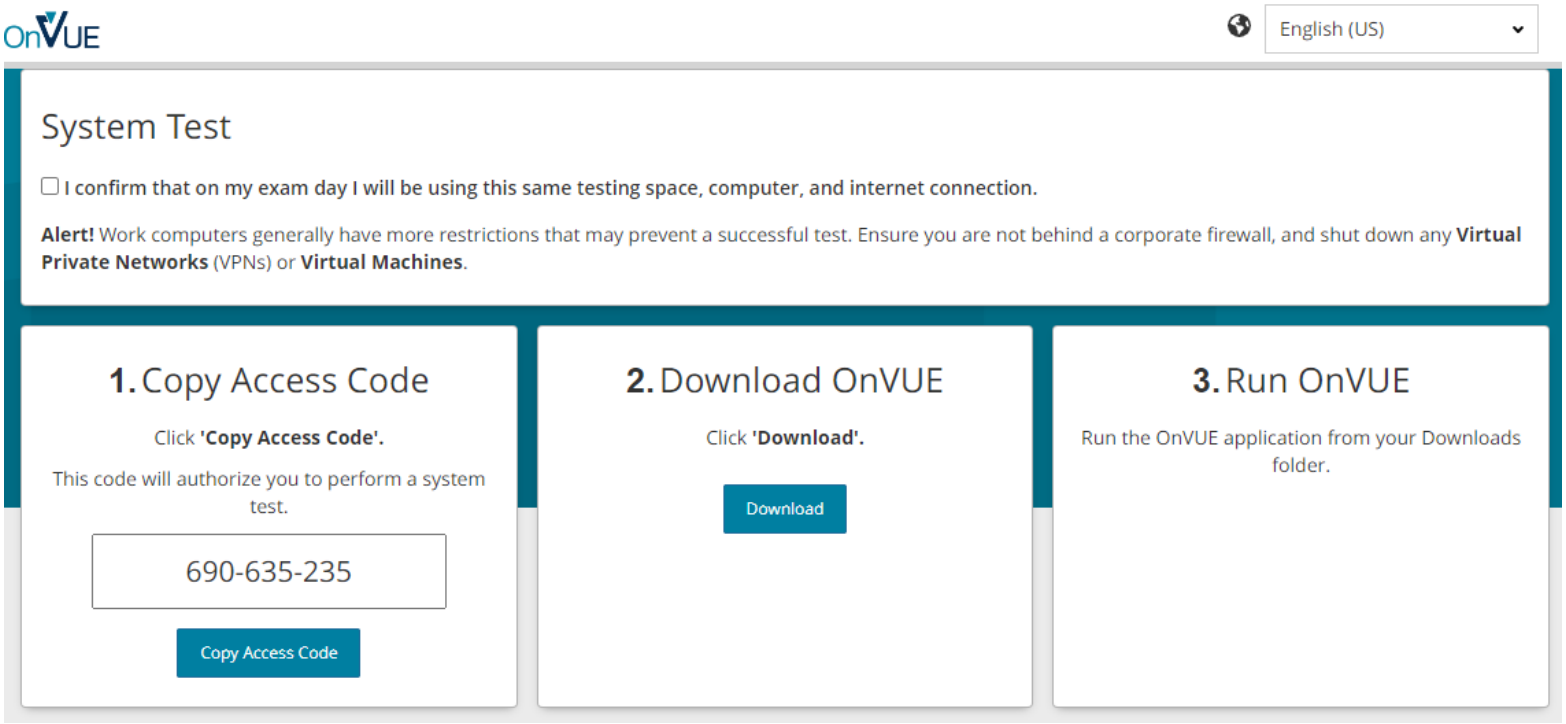
What's next?

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

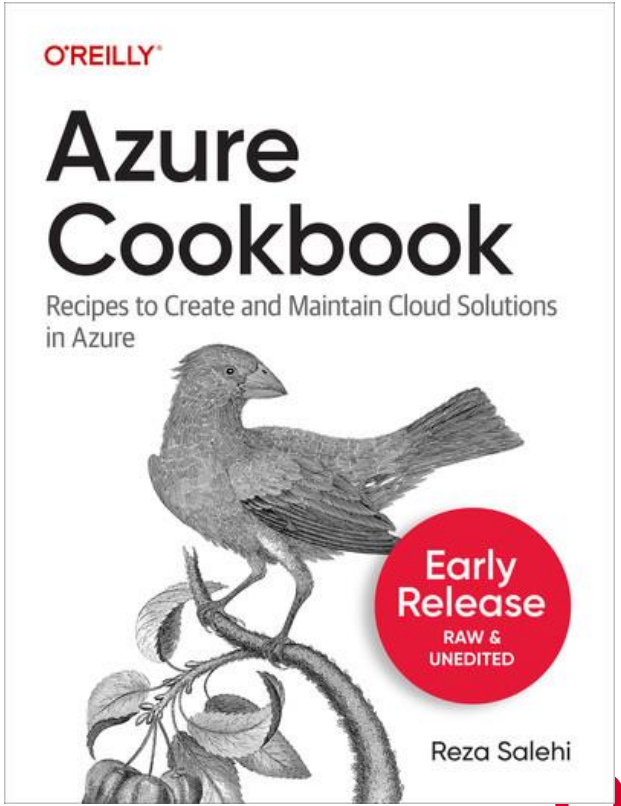
https://github.com/zaalion/oreilly-az-500

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