



## Microsoft Azure Security Technologies (AZ-500) Bootcamp

Earn Your Azure Security Engineer Associate Badge





# Reza Salehi

Cloud Consultant and Trainer



@zaalion



# Course Overview

---

# AZ-500 Bootcamp

- Day 1
  - Manage identity and access
  - Implement platform protection



---

# AZ-500 Bootcamp

- Day 2
  - Manage security operations
  - Secure data and applications



---

# Course Repository

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



---

# Microsoft Cybersecurity Reference Architectures

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



 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 

 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

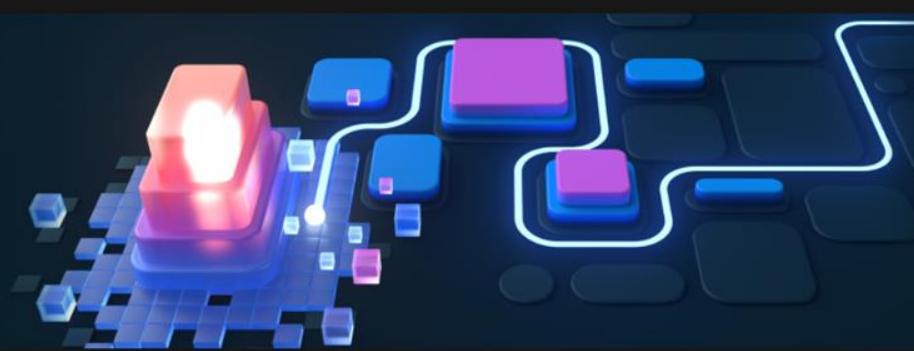
 Open with Visual Studio

 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

Exam AZ-500: Microsoft Azure Security Technologies

# Study Guide

## Exam AZ-500: Microsoft Azure Security Technologies

### Quick navigation

[Purpose of this document](#)

[Certification](#)

[Certification journey](#)

[Certification renewal](#)

[About the exam](#)

[Passing score](#)

[What to expect on the exam](#)

[Prepare to take the exam](#)

[Request accommodations](#)

[Take practice tests](#)

[Objective domain: skills the exam measures](#)

[Skills measured](#)

[Functional groups](#)

[Corresponding learning paths and modules](#)

[Additional study resources](#)

# Day 1

---

# Microsoft Azure Security Technologies Bootcamp

- Manage identity and access (30-35%)
- Implement platform protection (15-20%)



---

# Manage Identity and Access (30–35%)

- Manage Azure Active Directory (Azure AD) identities
- Manage secure access by using Azure AD
- Manage application access
- Manage access control



# Manage Azure Active Directory (Azure AD) Identities

- Create and manage a managed identity for Azure resources
- Manage Azure AD groups
- Manage Azure AD users
- Manage external identities by using Azure AD
- Manage administrative units



## 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     
[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 \* ⓘ

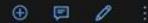
West US



Name \* ⓘ



Filter by title

[Docs](#) / [Azure](#) / [Active Directory](#) / [Managed identities for Azure resources](#) /

In this article

Next steps

## 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

# 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	<a href="#">Use managed identities in Azure API Management</a>
Application Gateway	<a href="#">TLS termination with Key Vault certificates</a>

All services >



# Default Directory | Overview

Azure Active Directory



+ Add



Microsoft  
(Preview)

i Overview

Preview features

Diagnose and solve problems

## Manage

Users

Groups

External Identities

Roles and administrators

## Overview

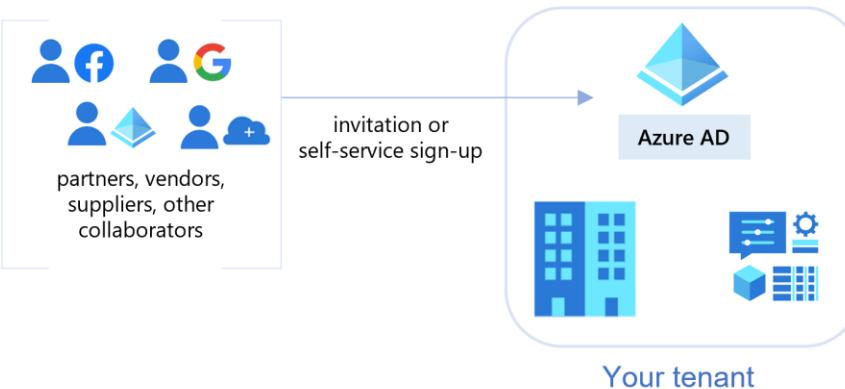
Search your directory

## Basic information

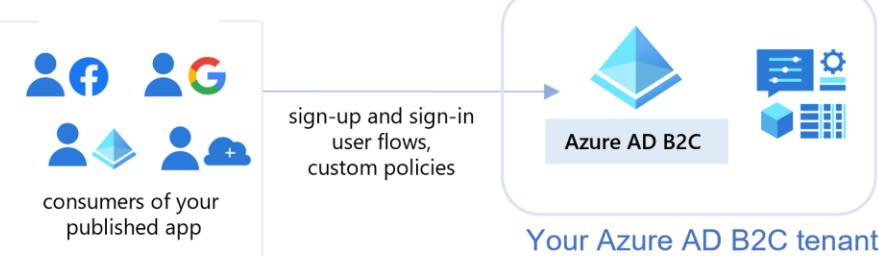


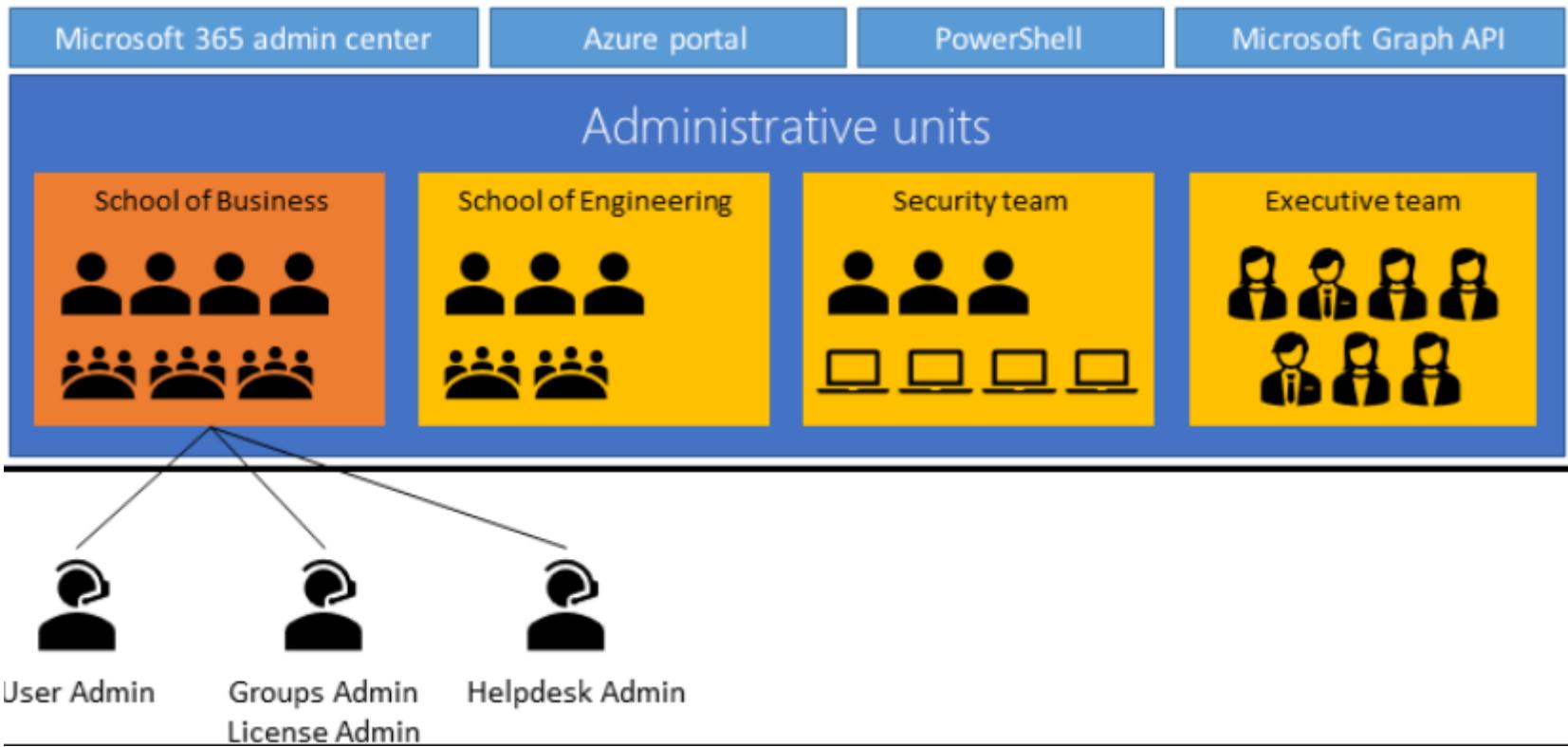
## Azure AD External Identities

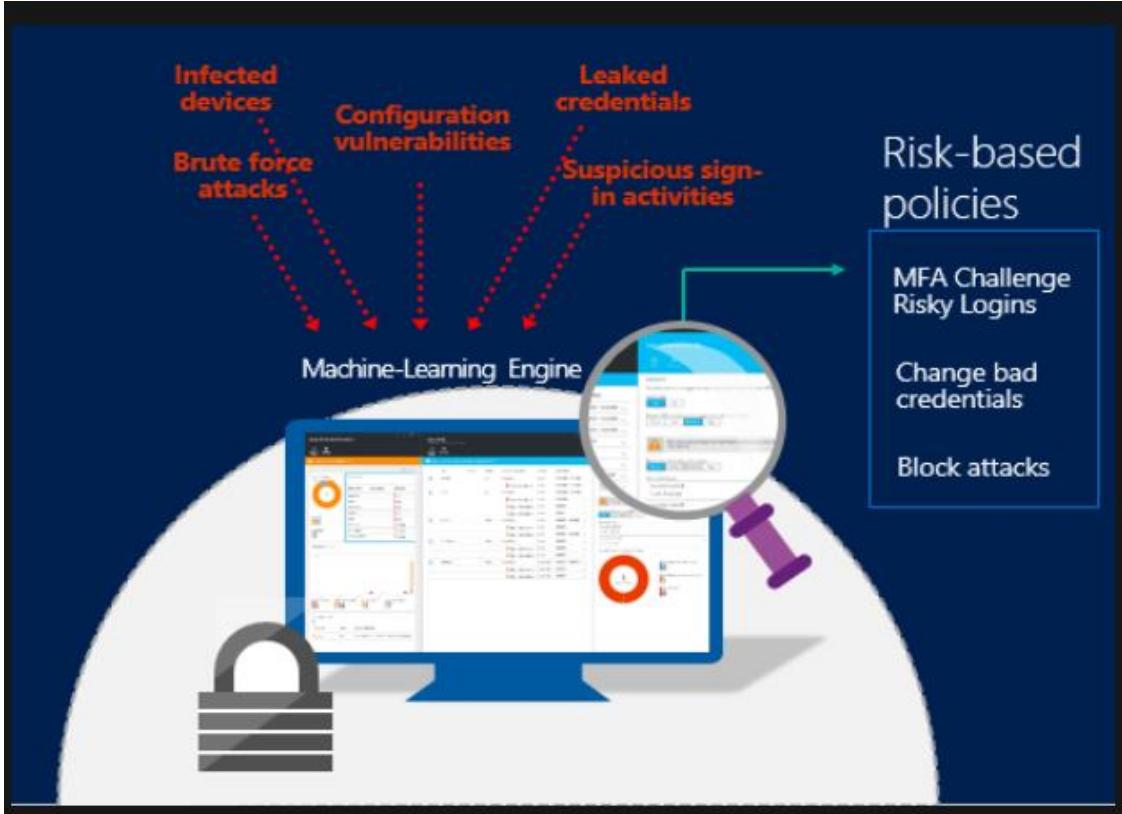
### B2B collaboration



### Azure AD B2C







# Manage Secure Access by Using Azure AD

- Configure Azure AD Privileged Identity Management (PIM)
- Implement Conditional Access policies, including MFA
- Implement Azure AD Identity Protection
- Implement passwordless authentication
- Configure access reviews (and see these ones too)



# Privileged Identity Management | Quick start



Privileged Identity Management



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

Quick start

What's new

Get started

## 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

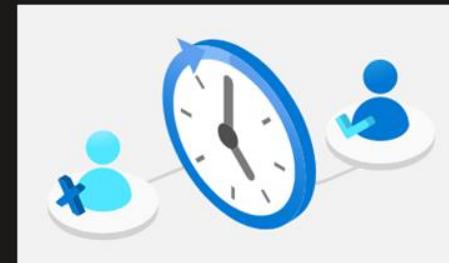
Manage

Activate

Discover

## 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.



## Add assignments

...

[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

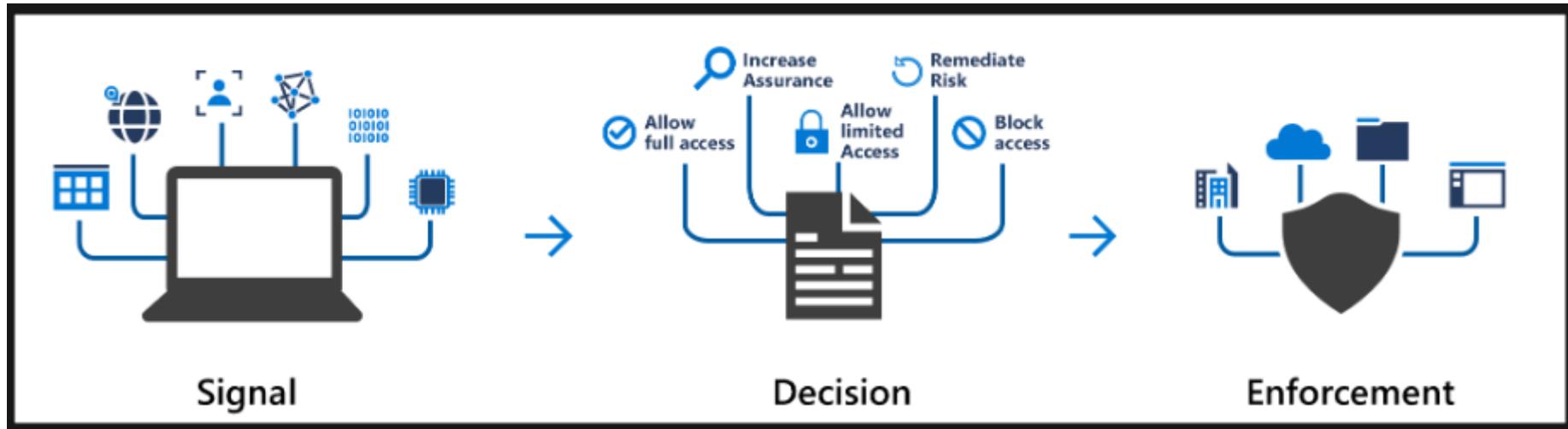
[Assign](#)

&lt; Prev

Cancel



# Azure AD Conditional Access



## Azure AD Identity Protection Weekly Digest

MA

Microsoft Azure  
Mon 5/4/2020 10:13 PM  
To: Bala Sadhu



## Azure AD Identity Protection Weekly Digest

Contoso

New risky users detected

0

New risky sign-ins detected  
(in real-time)

0



[Privacy Statement](#)

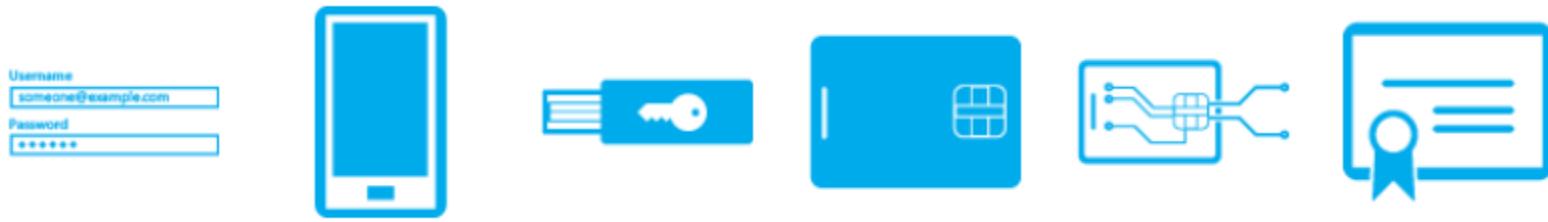
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052



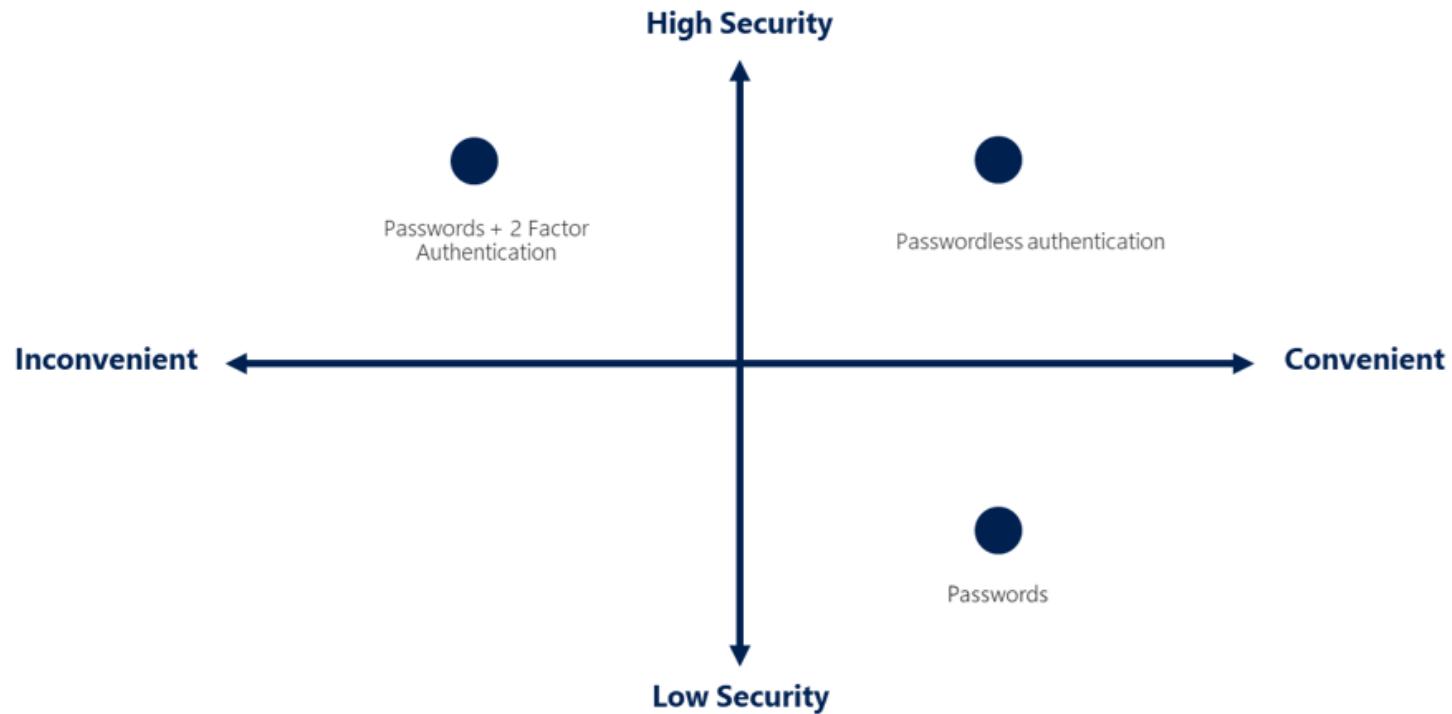
[Reply](#) | [Reply all](#) | [Forward](#)



# Azure AD Multi-Factor Authentication



# Passwordless authentication options for AAD



# Configure Access Reviews

New access review ...

\* Review type   \* Reviews   Settings   \* Review + Create

Schedule an access review to ensure the right people have the right access to access packages, groups, apps, and privileged roles.  
[Learn more](#)

Select what to review \*

Teams + Groups

Review scope \*

All Microsoft 365 groups with guest users   
 Select Teams + groups

Group \*

Guests of Company name

Scope \*

Guest users only  
 All users

In public preview, B2B direct connect users and teams in shared channels are included in access reviews. B2B direct connect users and teams are not supported in reviews of 'All Microsoft 365 groups with guest users', as well as reviews scoped to inactive users. Click here to learn more.

Inactive users (on tenant level) only

Days inactive

30



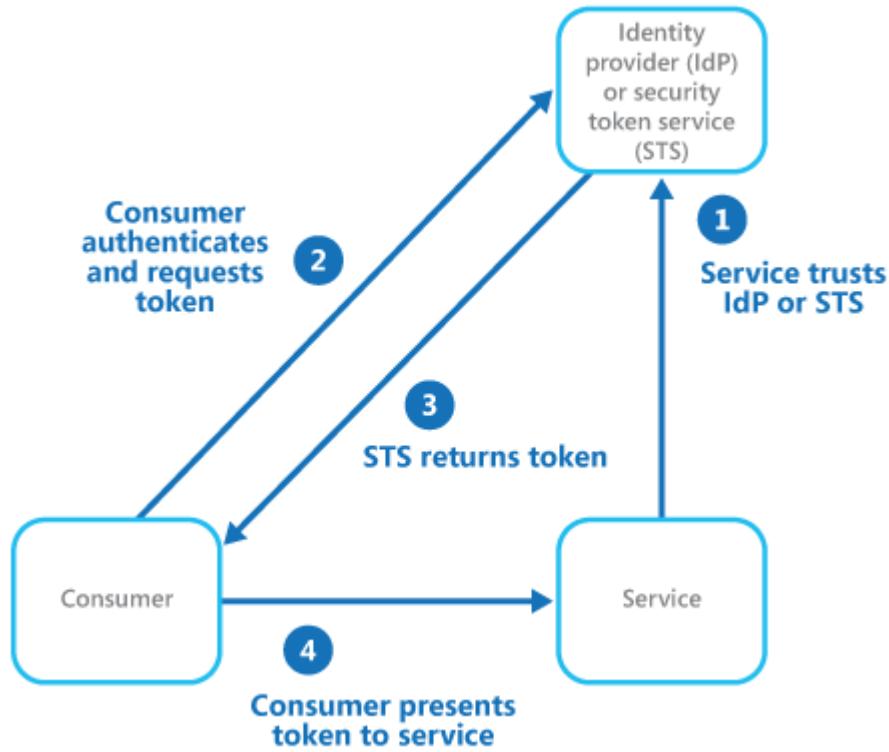
---

# Manage Application Access

- Integrate single sign-on (SSO) and identity providers for authentication
- Create an app registration
- Configure app registration permission scopes
- Manage app registration permission consent
- Manage API permissions to Azure subscriptions and resources
- Configure an authentication method for a service principal



# Federated Identity Pattern and SSO



# Default Directory | App registrations

Azure Active Directory

[New registration](#)[Endpoints](#)[Troubleshooting](#)[Refresh](#)[Download](#)[Preview features](#)[Overview](#)[Preview features](#)[Diagnose and solve problems](#)

## Manage

[Users](#)[Groups](#)[External Identities](#)[Roles and administrators](#)[Administrative units](#)[Enterprise applications](#)[Devices](#)[App registrations](#)[Identity Governance](#)

**i** Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to 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 results...[Add filters](#)

3 applications found

[Display name ↑](#)[Application \(client\) ID](#)

AP	Display name	Application (client) ID
AP	app-databricks	b3d01750-407e-4555-9456-fa43724
ID	IdentityApp	a8e7964b-c...-a707-9f9e3b8
KV	kvdev-testapp	d9c2db92-c1...-b4c9-771541



① testuser@fourthcoffeetest.onmicrosoft.com

## ② Permissions requested



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

Allows the app to see your basic profile (name, picture, user name)  
⑨

This is a permission requested to access your data in Fourth Coffee.  
⑩

✓ 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>. ⑪

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](#)

Does this app look suspicious? Report it here



# app-databricks | API permissions



...

 Search (Ctrl+ /)

Refresh

Got feedback?

Overview

Quickstart

Integration assistant

## Manage

Branding &amp; properties

Authentication

Certificates &amp; secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators

Manifest



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 permissions shows 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 req...	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](#).

---

# Manage Access Control

- Configure Azure role permissions for management groups, subscriptions, resource groups, and resources
- Interpret role and resource permissions
- Assign built-in Azure AD roles
- Create and assign custom roles, including Azure roles and Azure AD roles



# Reader



BuiltInRole

Search (Ctrl+ /)

Permissions

JSON

Assignments

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve

Security

Events

## Cost Management

Cost analysis

Cost alerts

Budgets

Advisor recommendations

## Billing

Invoices

External services

```
1  {
2      "id": "/providers/Microsoft.Authorization/roleDefinitions/acdd72a7-3385-48ef-bd42-f606fba81ae7",
3      "properties": {
4          "roleName": "Reader",
5          "description": "View all resources, but does not allow you to make any changes.",
6          "assignableScopes": [
7              "/"
8          ],
9          "permissions": [
10             {
11                 "actions": [
12                     "*/*read"
13                 ],
14                 "notActions": [],
15                 "dataActions": [],
16                 "notDataActions": []
17             }
18         ]
19     }
20 }
```

## 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



## 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



---

# Implement Platform Protection (15–20%)

- Implement advanced network security
- Configure advanced security for compute

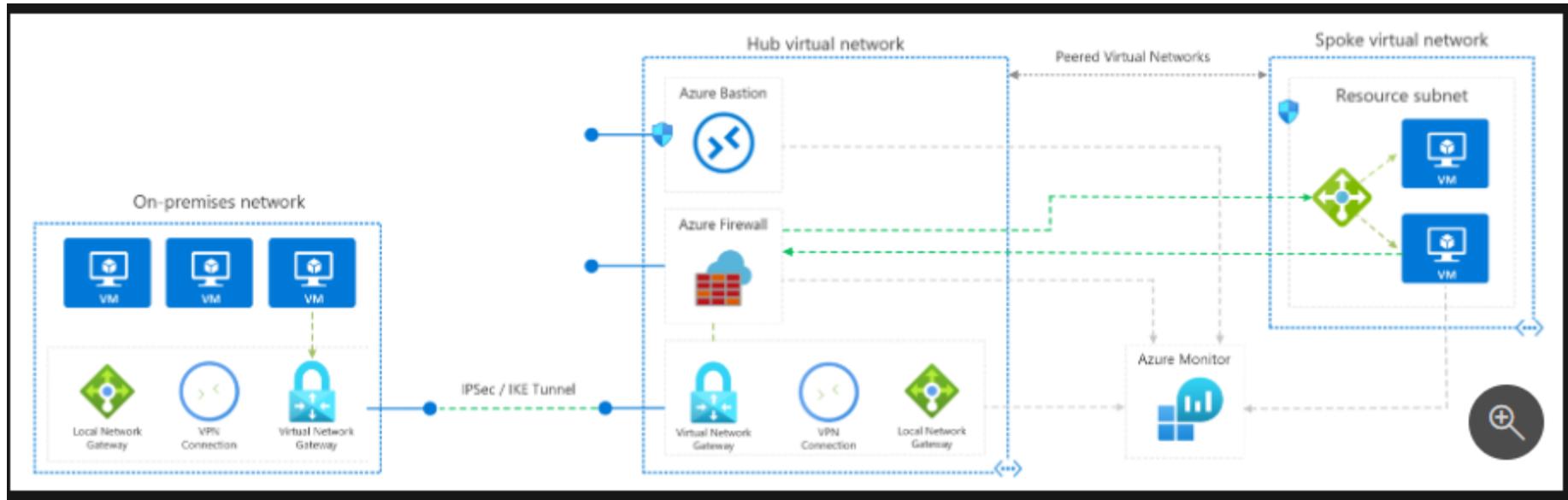


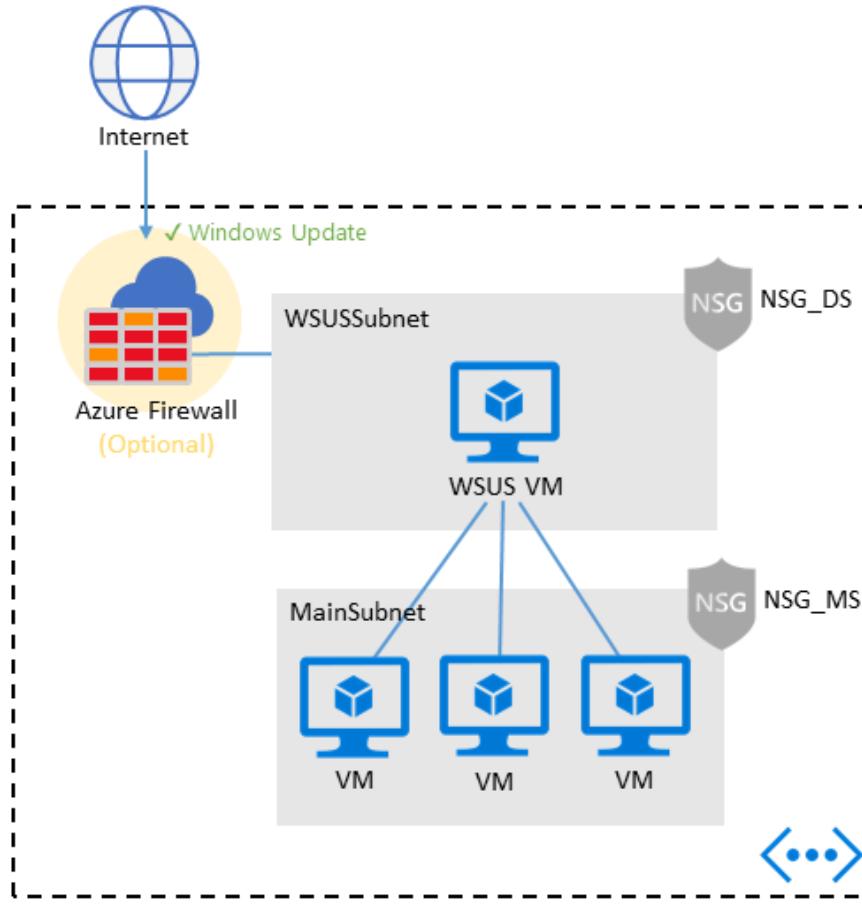
# Implement Advanced Network Security

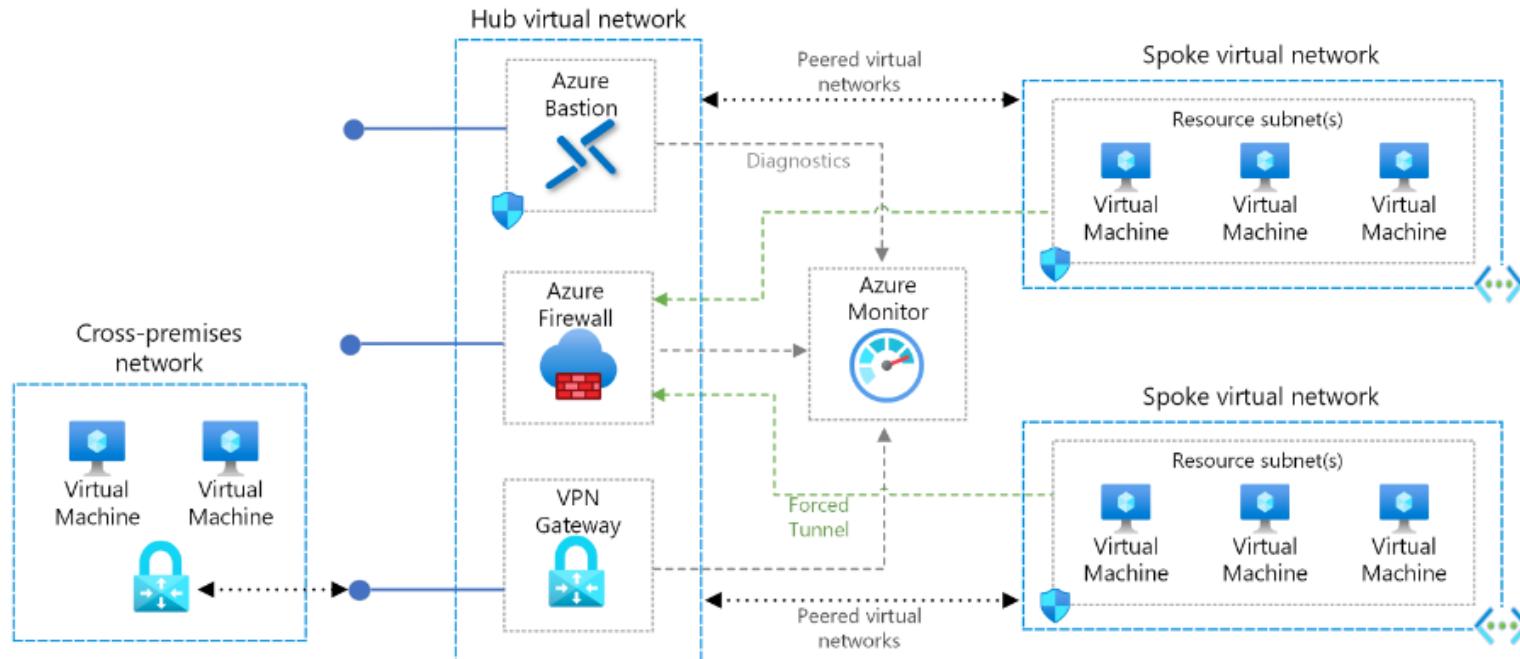
- Secure the connectivity of hybrid networks
- Secure the connectivity of virtual networks
- Create and configure Azure Firewall
- Create and configure Azure Firewall Manager
- Create and configure Azure Application Gateway
- Create and configure Azure Front Door
- Create and configure Web Application Firewall (WAF)
- Configure a resource firewall, including storage account, Azure SQL, Azure Key Vault, or Azure App Service
- Configure network isolation for Web Apps and Azure Functions
- Implement Azure Service Endpoints
- Implement Azure Private Endpoints, including integrating with other services
- Implement Azure Private Links
- Implement Azure DDoS Protection

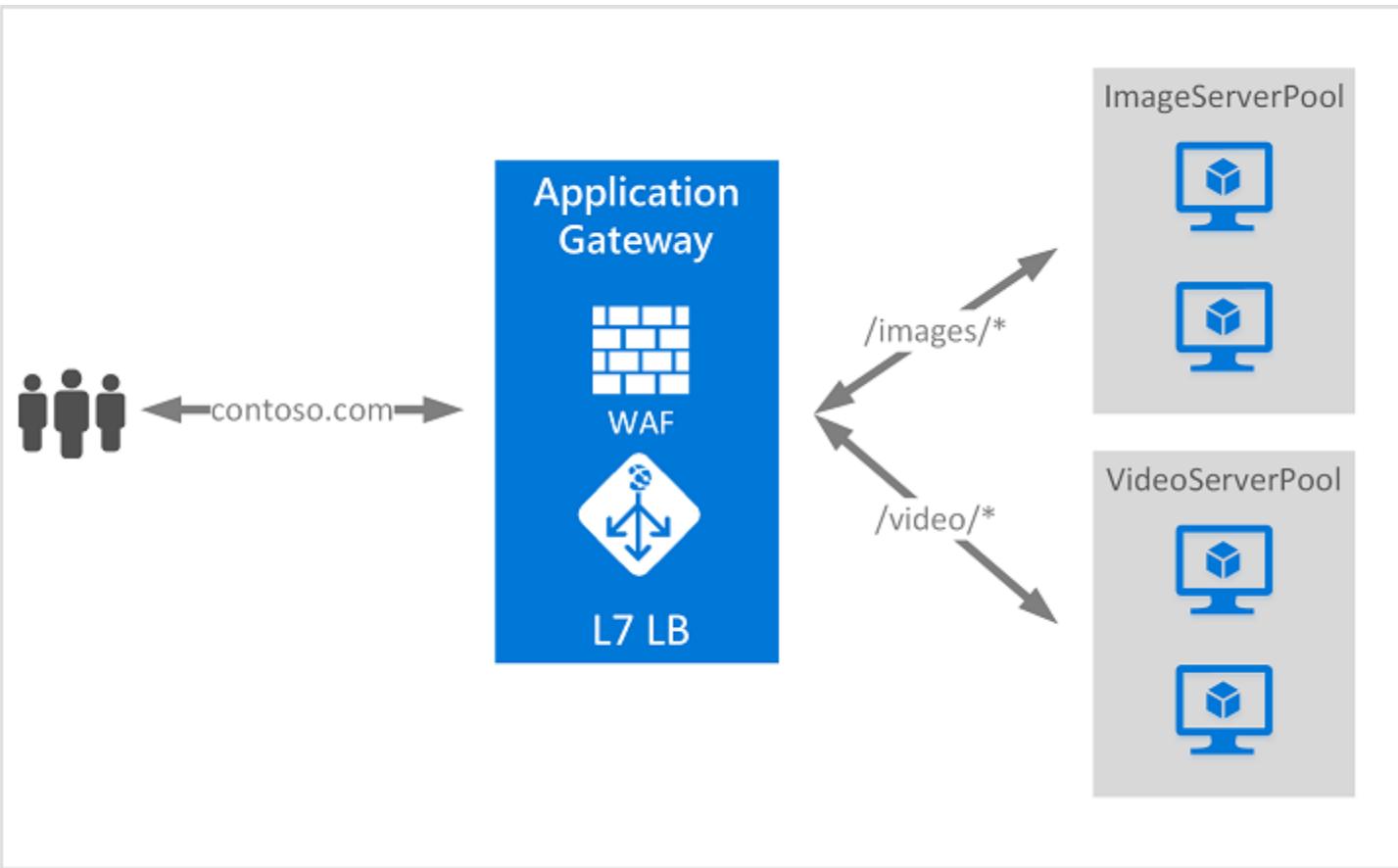


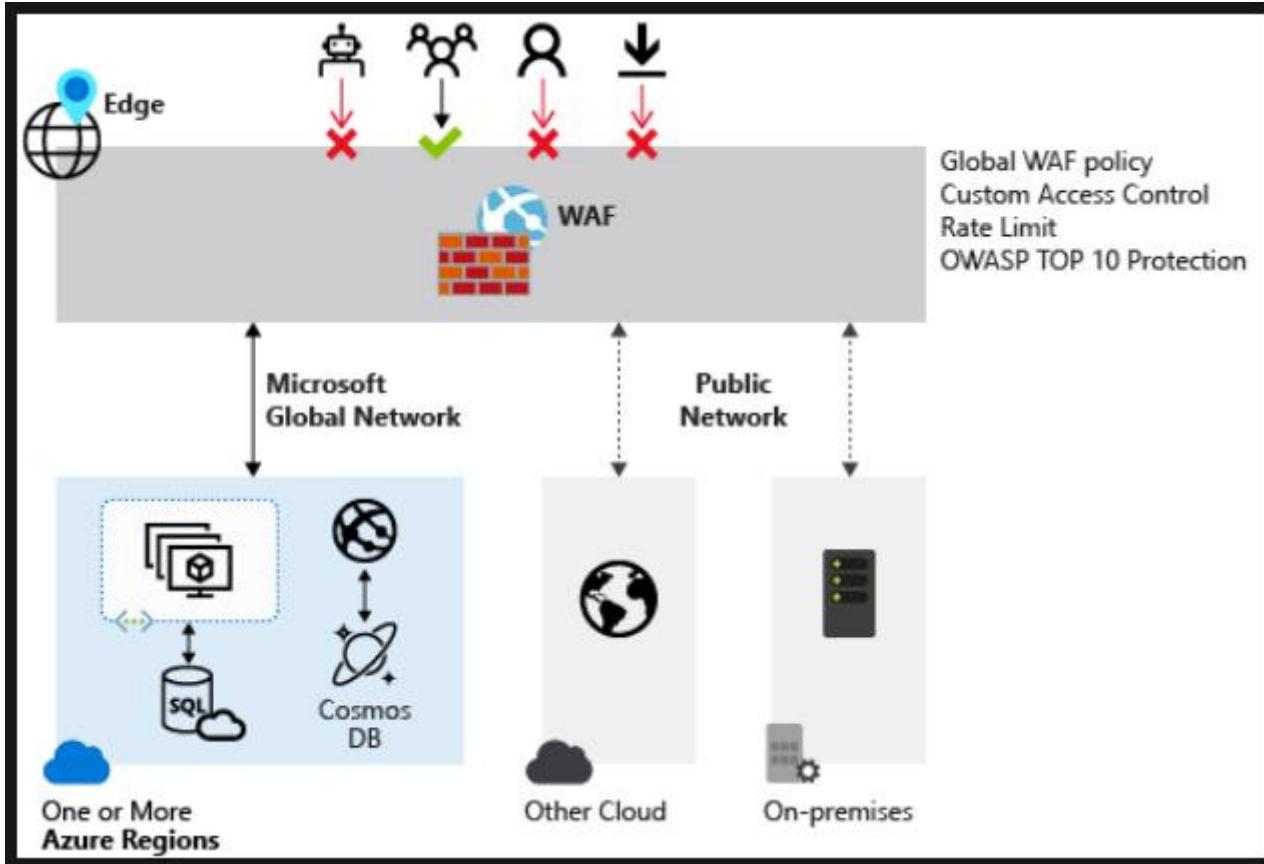
# Hybrid Network

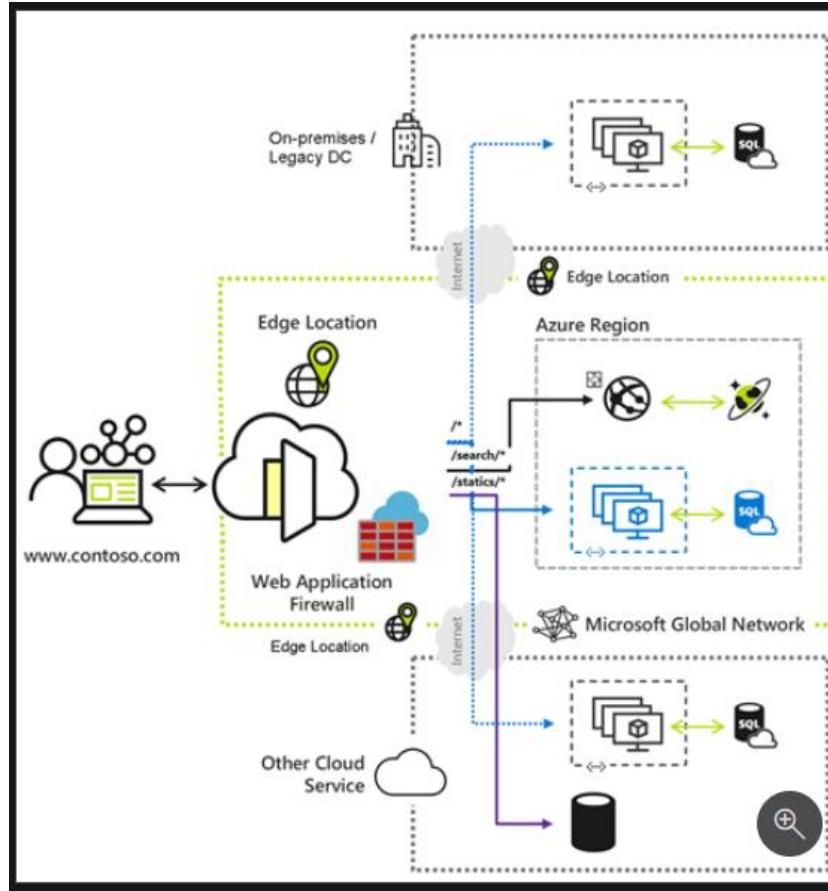


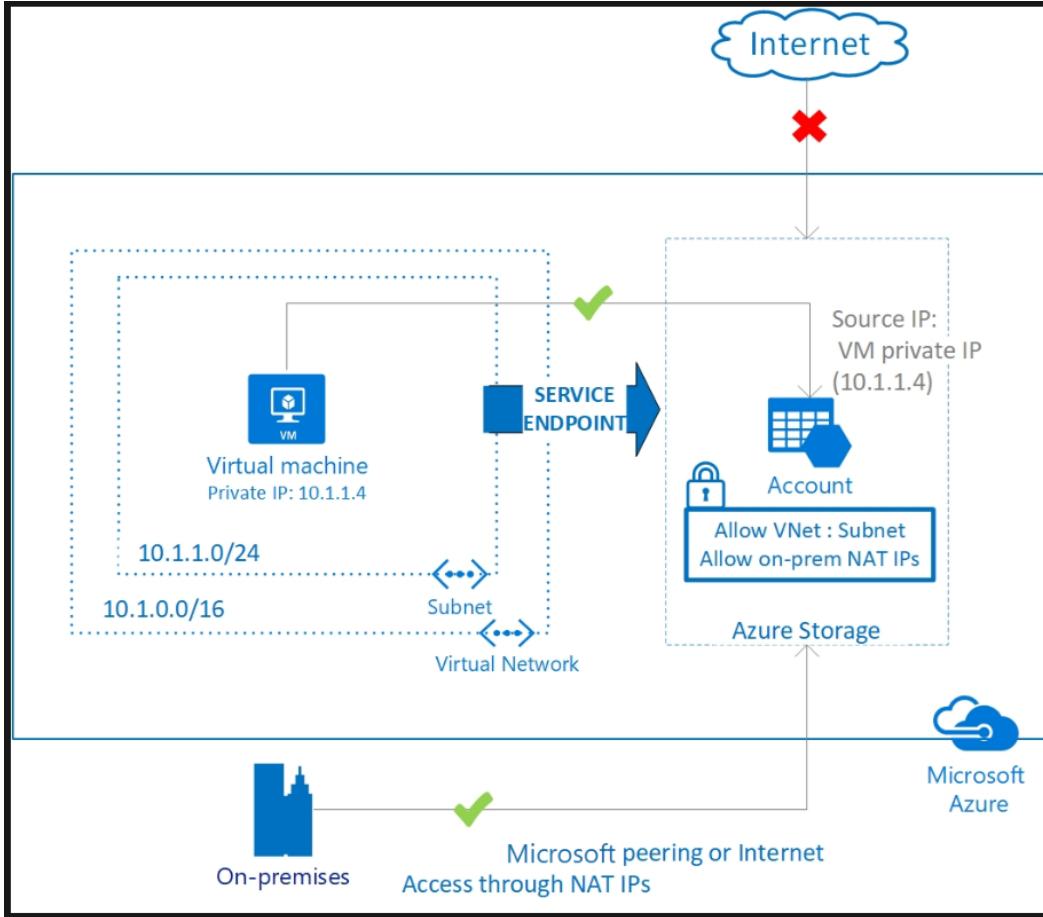










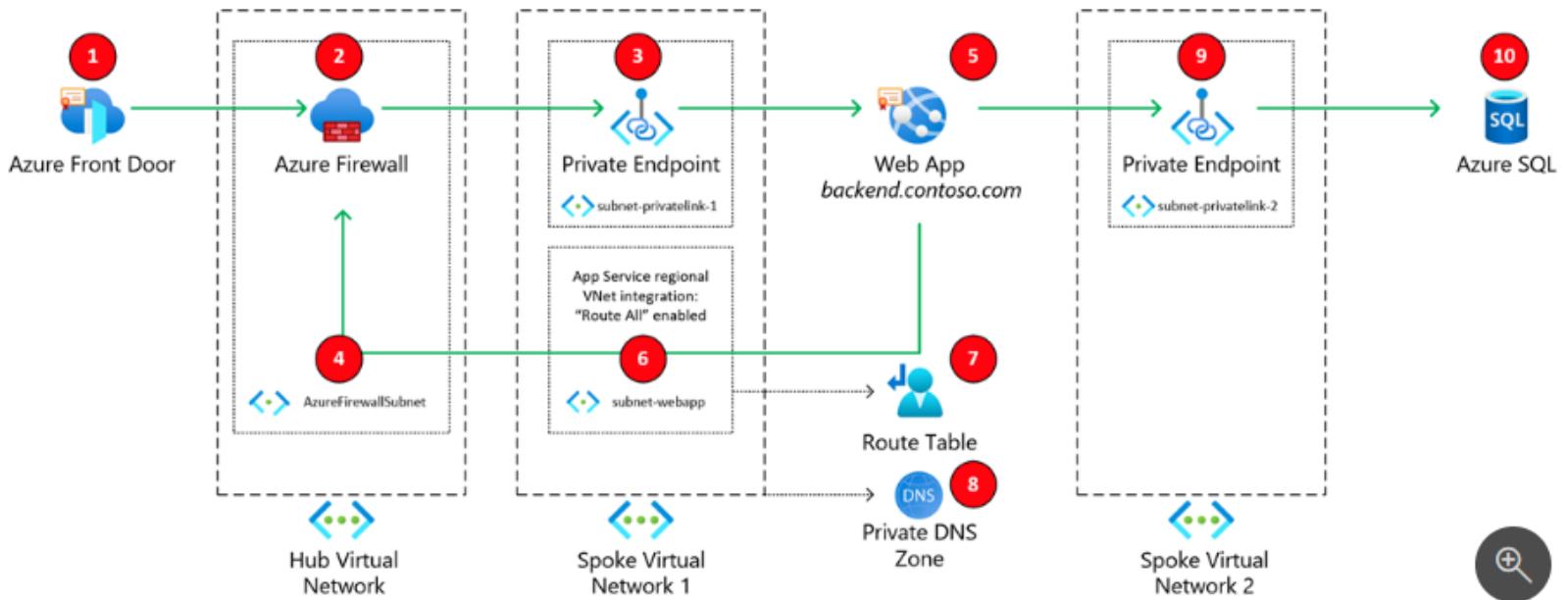


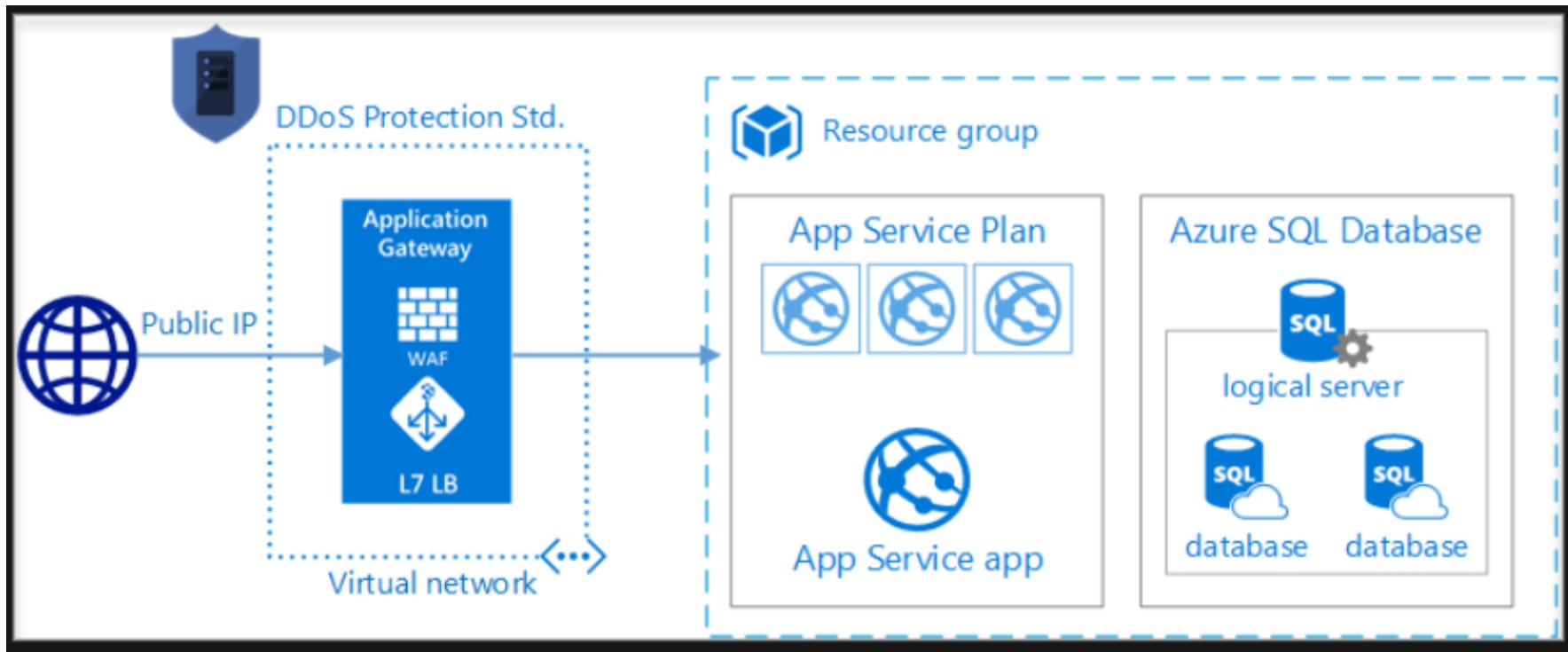
---

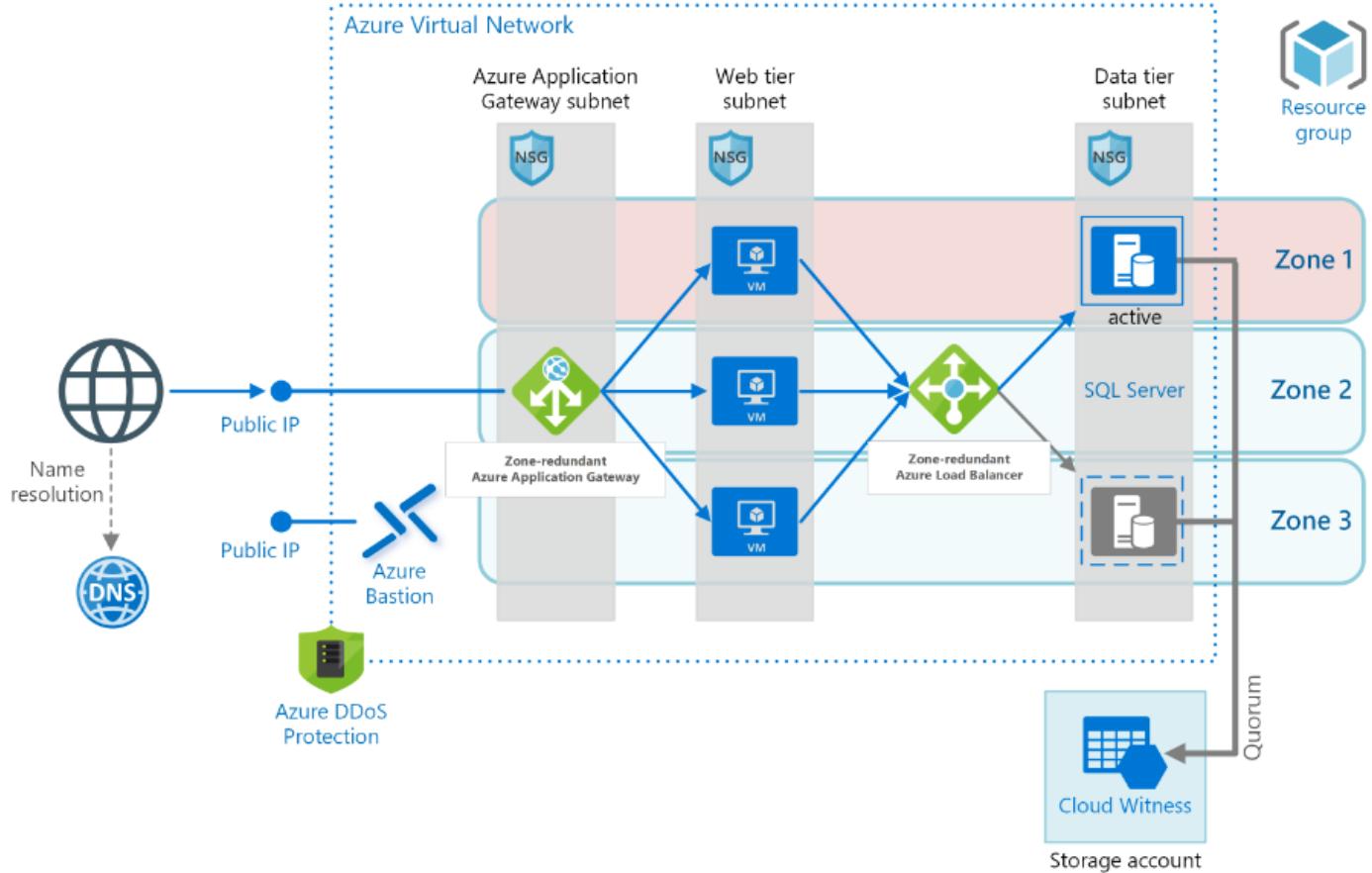
 **Note**

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](#).









# Configure Advanced Security for Compute

- Configure Endpoint Protection for virtual machines (VMs)
- Implement and manage security updates for VMs
- Configure security for container services
- Manage access to Azure Container Registry
- Configure security for serverless compute
- Configure security for an Azure App Service
- Configure encryption at rest
- Configure encryption in transit



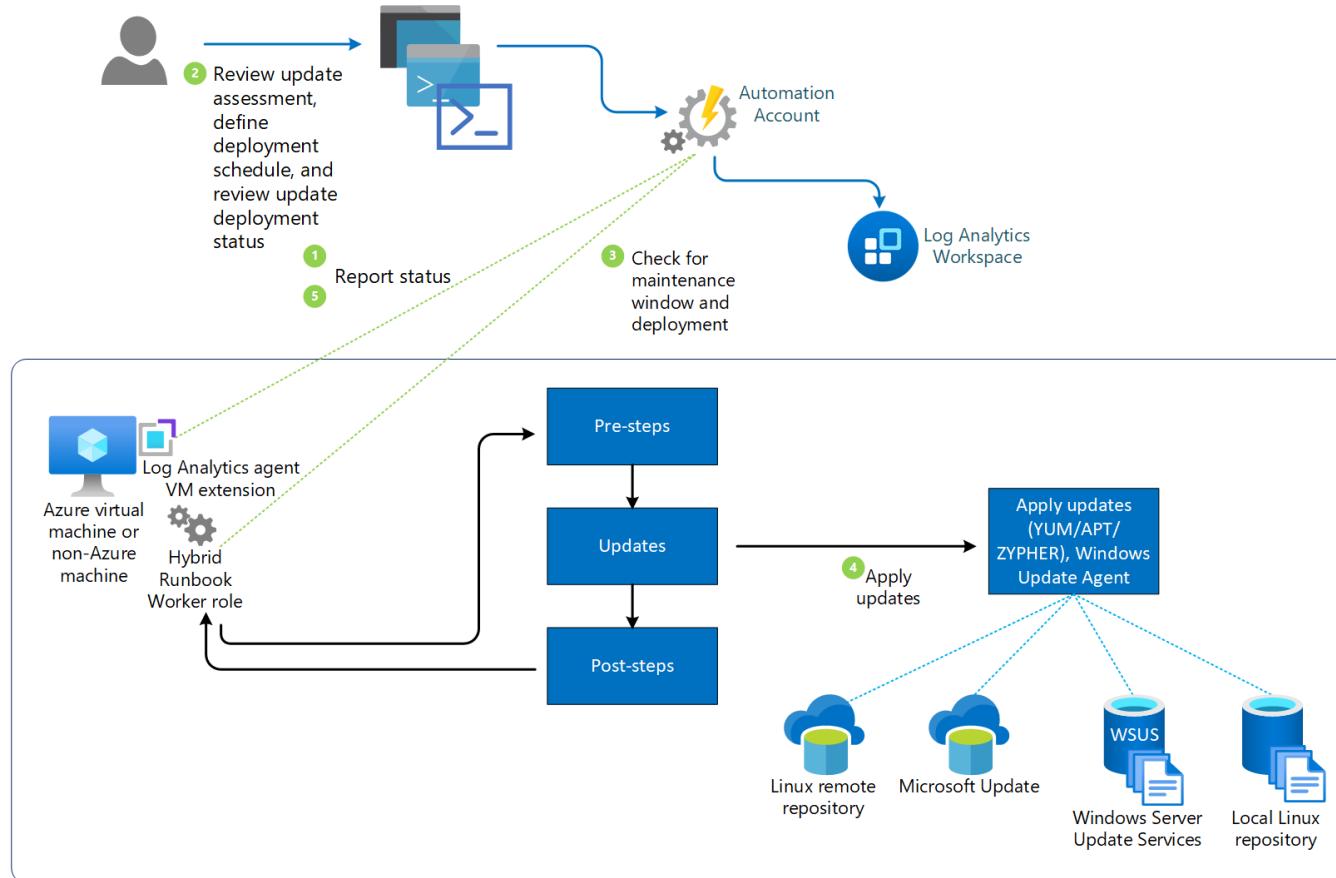
# Configure Endpoint Protection for Azure VMs

- Windows Defender
- Microsoft System Center endpoint protection
- Trend Micro
- Symantec endpoint protection
- McAfee endpoint protection for Windows
- McAfee Endpoint Security for Linux Threat Prevention
- Sophos Antivirus for Linux

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/endpoint-protection-recommendations-technical>



# Implement and Manage Security Updates for VMs



# Configure Security for Container Services

- Security considerations for Azure Container Instances
- Overview of Microsoft Defender for Containers
- Azure security baseline for Container Instances
- Security concepts for applications and clusters in Azure Kubernetes Service (AKS)
- Authentication and authorization in Azure Container Apps



---

# Manage Access to Azure Container Registry

- Authenticate with an Azure container registry
- Azure Container Registry roles and permissions



---

# Configure Security for Serverless Compute

- Secure access and data in Azure Logic Apps
- Secure Azure Functions



# Configure Security for an Azure App Service

- Security in Azure App Service
- Security recommendations for App Service
- Azure security baseline for App Service



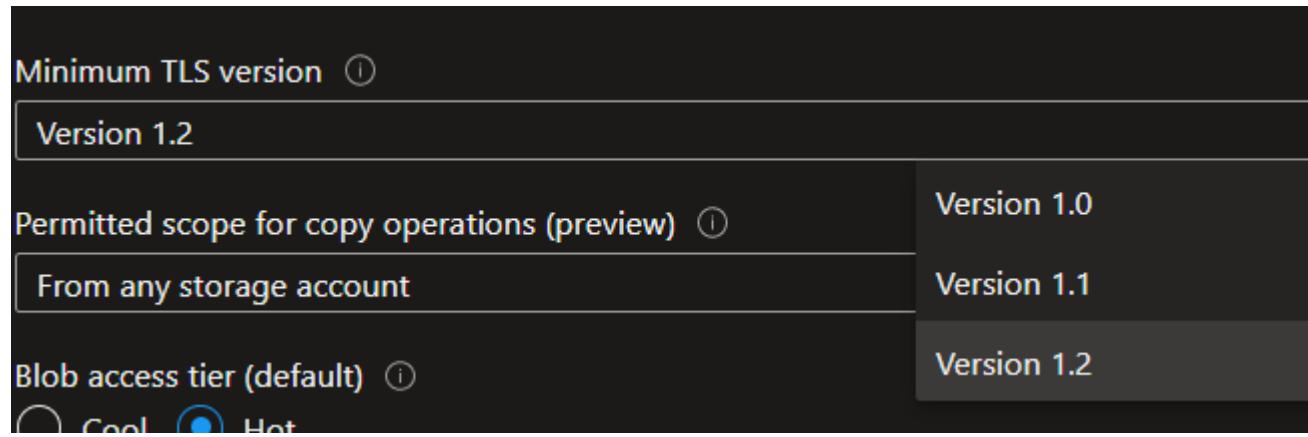
# Configure Encryption at Rest

- 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



# Day 2

---

# Microsoft Azure Security Technologies Bootcamp

- Manage security operations (25–30%)
- Secure data and applications (25–30%)



---

# Manage Security Operations (25–30%)

- Configure centralized policy management
- Configure and manage threat protection
- Configure and manage security monitoring solutions



---

# Configure Centralized Policy Management

- Configure a custom security policy
- Create a policy initiative
- Configure security settings and auditing by using Azure Policy



---

# Azure Built-in Policy Definitions

- Azure Policy built-in policy definitions



# Settings | Security policy

Pay-As-You-Go

Search (Ctrl+ /)



## Security policy on: Pay-As-You-Go

### Settings

Defender plans

Auto provisioning

Email notifications

Integrations

Workflow automation

Continuous export

### Policy settings

Security policy

Governance rules (preview)

initiatives enabled on this subscription



### Default initiative

The default initiative enabled on your subscription generates the security recommendations in the [Recommendations](#) page.

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



### Industry & regulatory standards

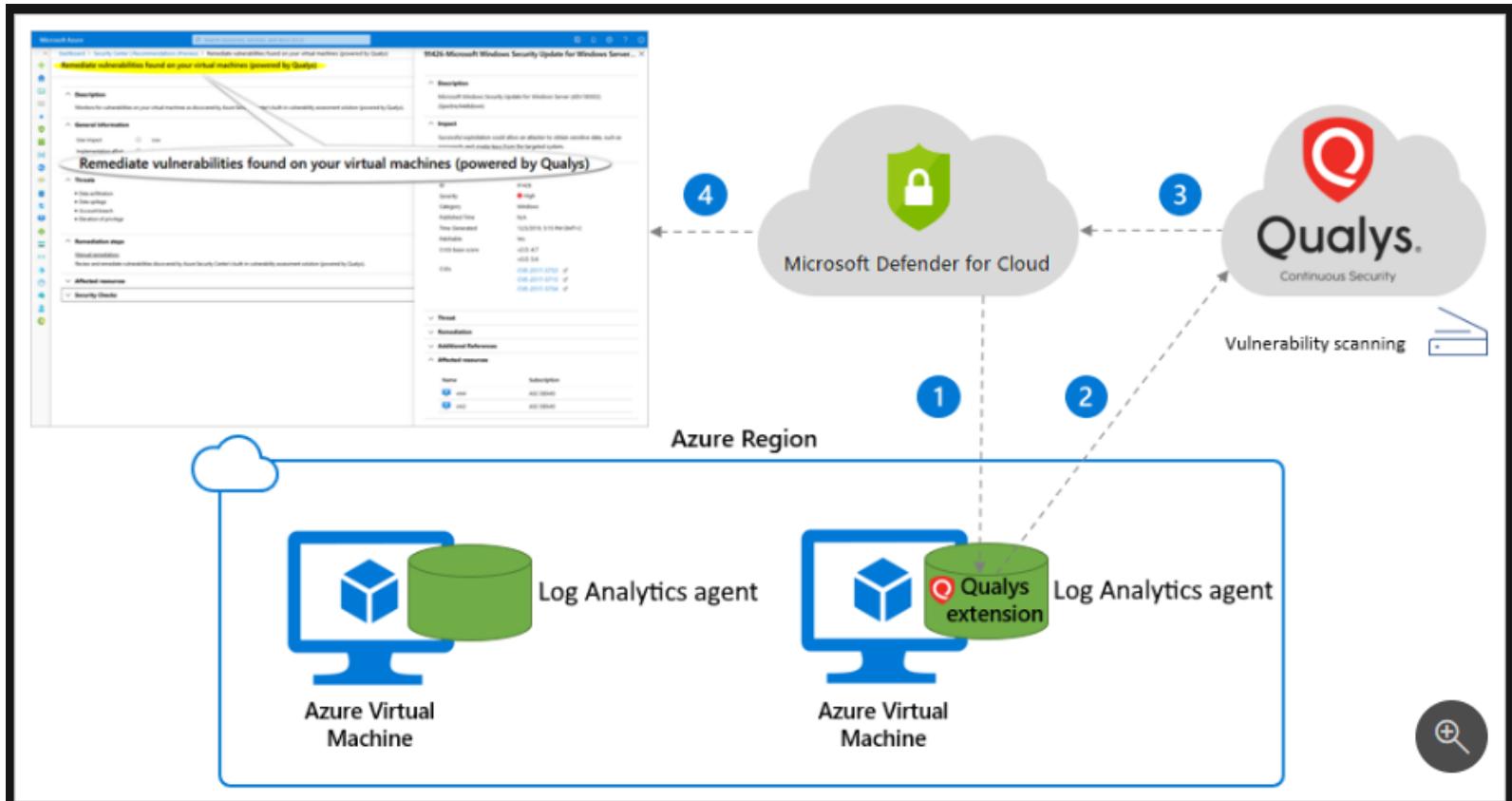
Compliance initiatives shown in the [Regulatory compliance dashboard](#).

---

# Configure and Manage Threat Protection

- Configure Microsoft Defender for Servers (not including Microsoft Defender for Endpoint)
- Evaluate vulnerability scans from Microsoft Defender for Cloud
- Configure Microsoft Defender for SQL
- Use the Microsoft Threat Modeling Tool

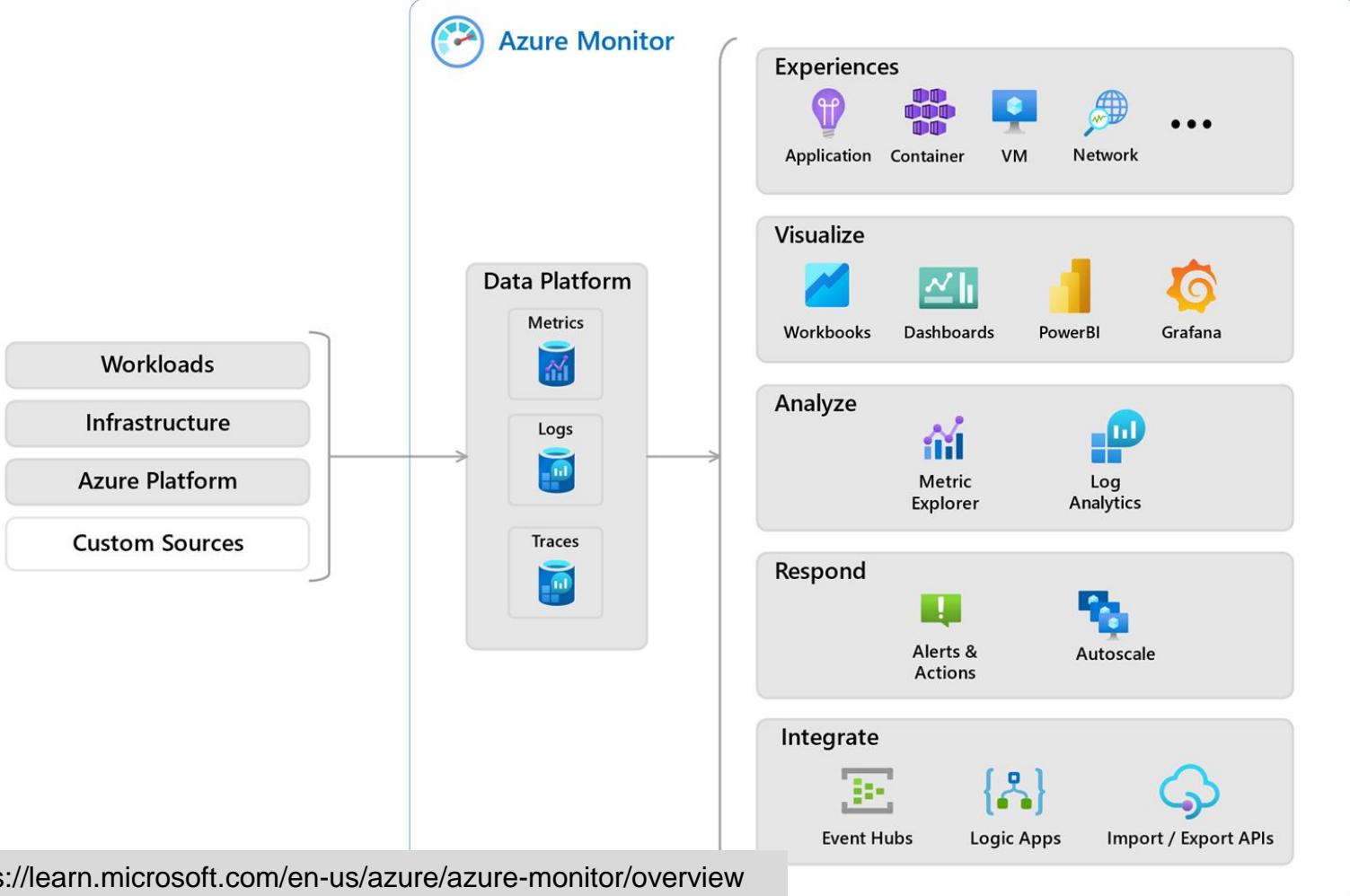




# Configure and Manage Security Monitoring Solutions

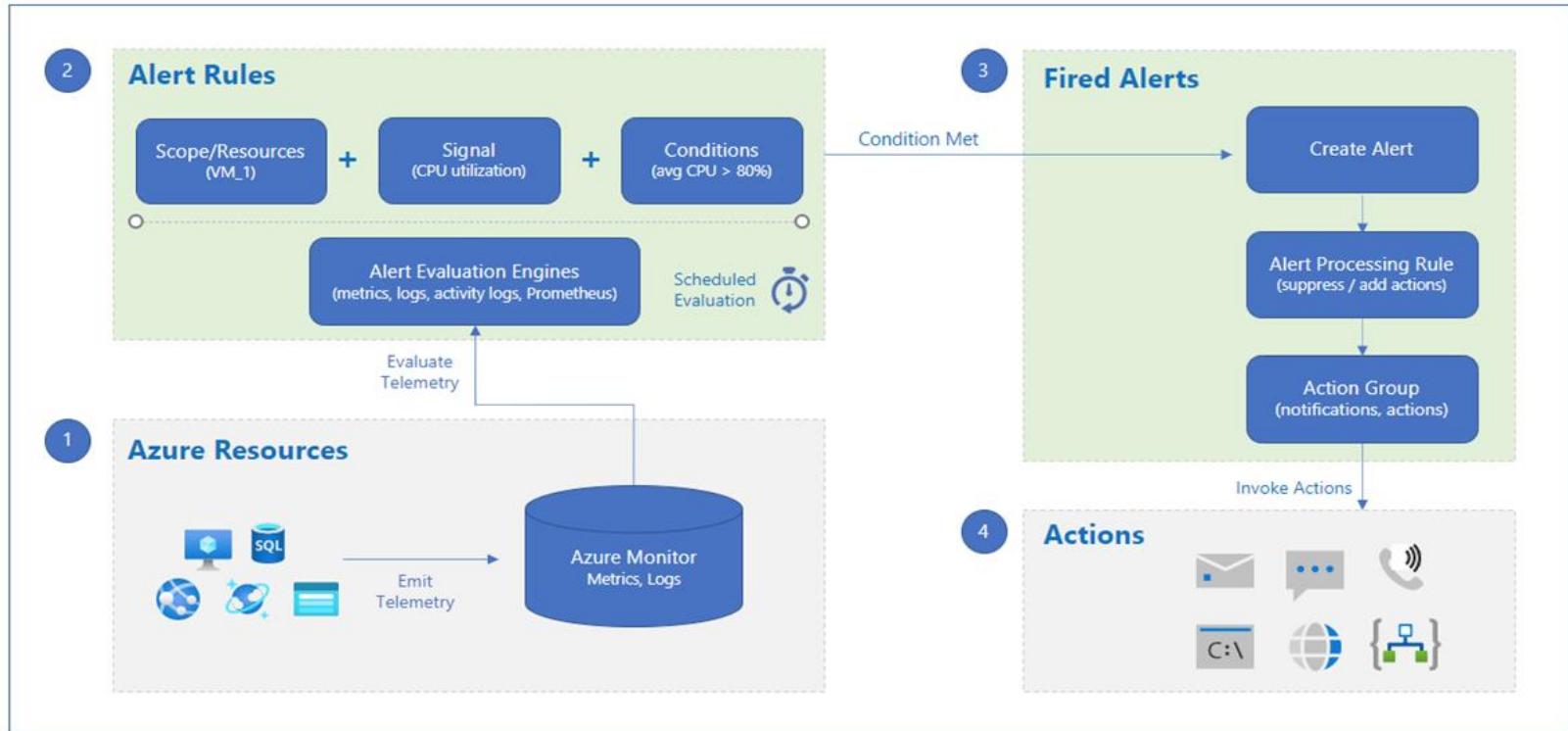
- Create and customize alert rules by using Azure Monitor
- Configure diagnostic logging and log retention by using Azure Monitor
- Monitor security logs by using Azure Monitor
- Create and customize alert rules in Microsoft Sentinel
- Configure connectors in Microsoft Sentinel
- Evaluate alerts and incidents in Microsoft Sentinel





<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



## 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 >



---

# Secure Data and Applications (25–30%)

- Configure security for storage
- Configure security for data
- Configure and manage Azure Key Vault



---

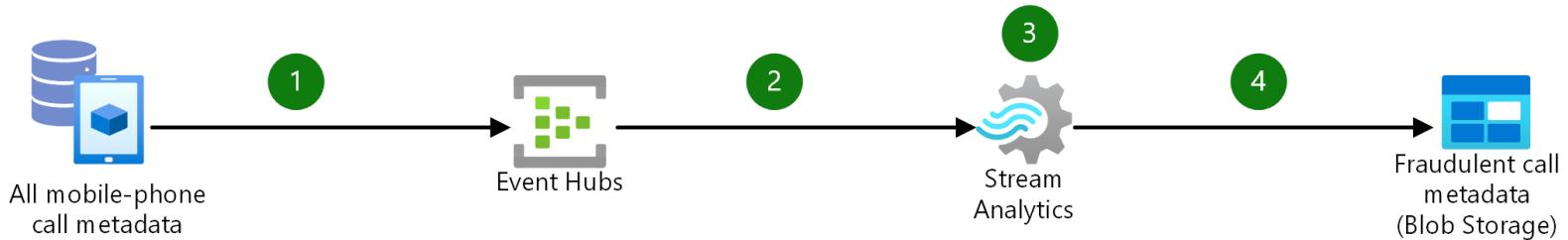
# Configure Security for Storage

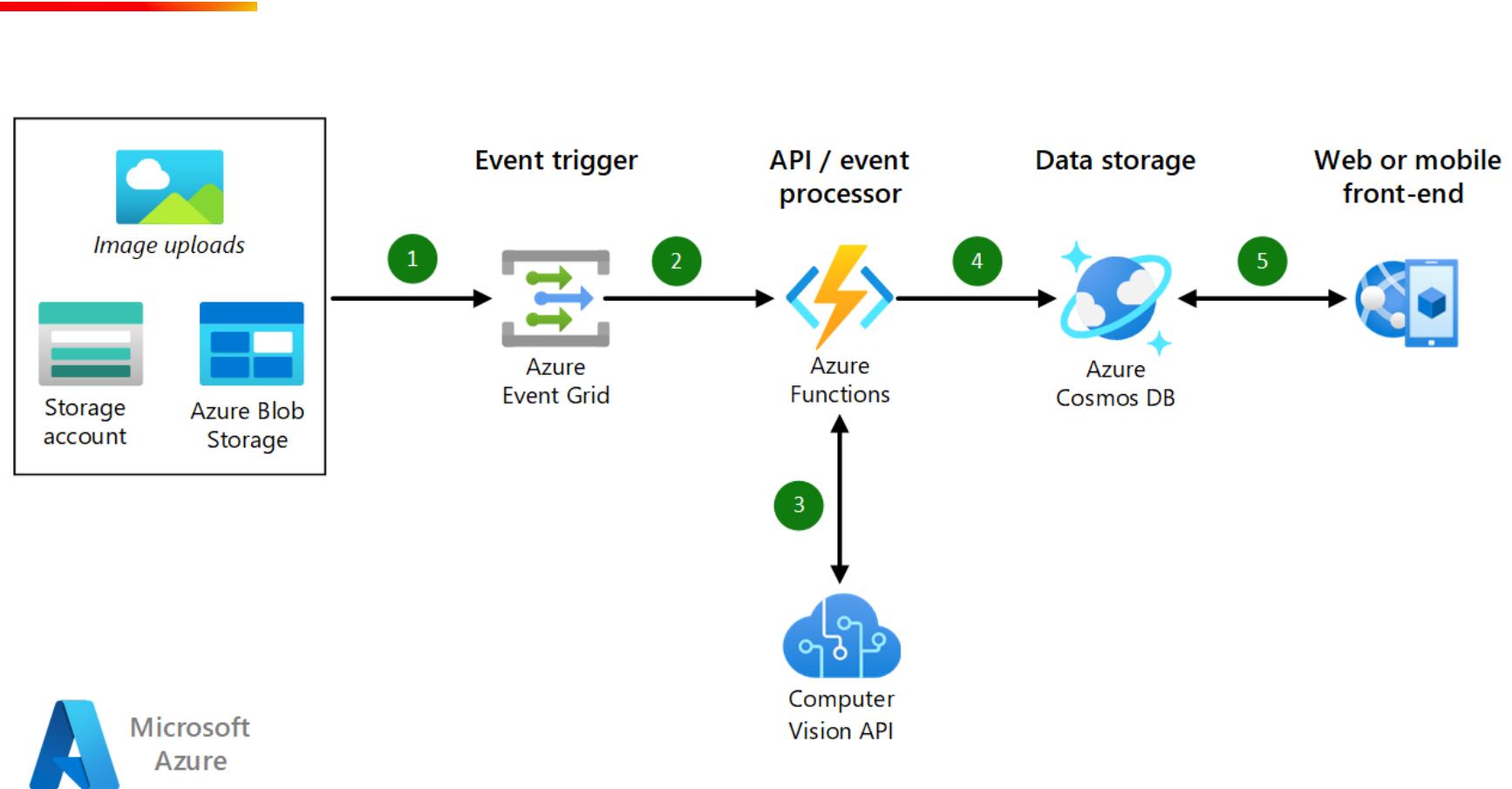
- Configure access control for storage accounts
- Configure storage account access keys
- Configure Azure AD authentication for Azure Blobs and Azure Files
- Configure delegated access



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

10:50:49 PM

End

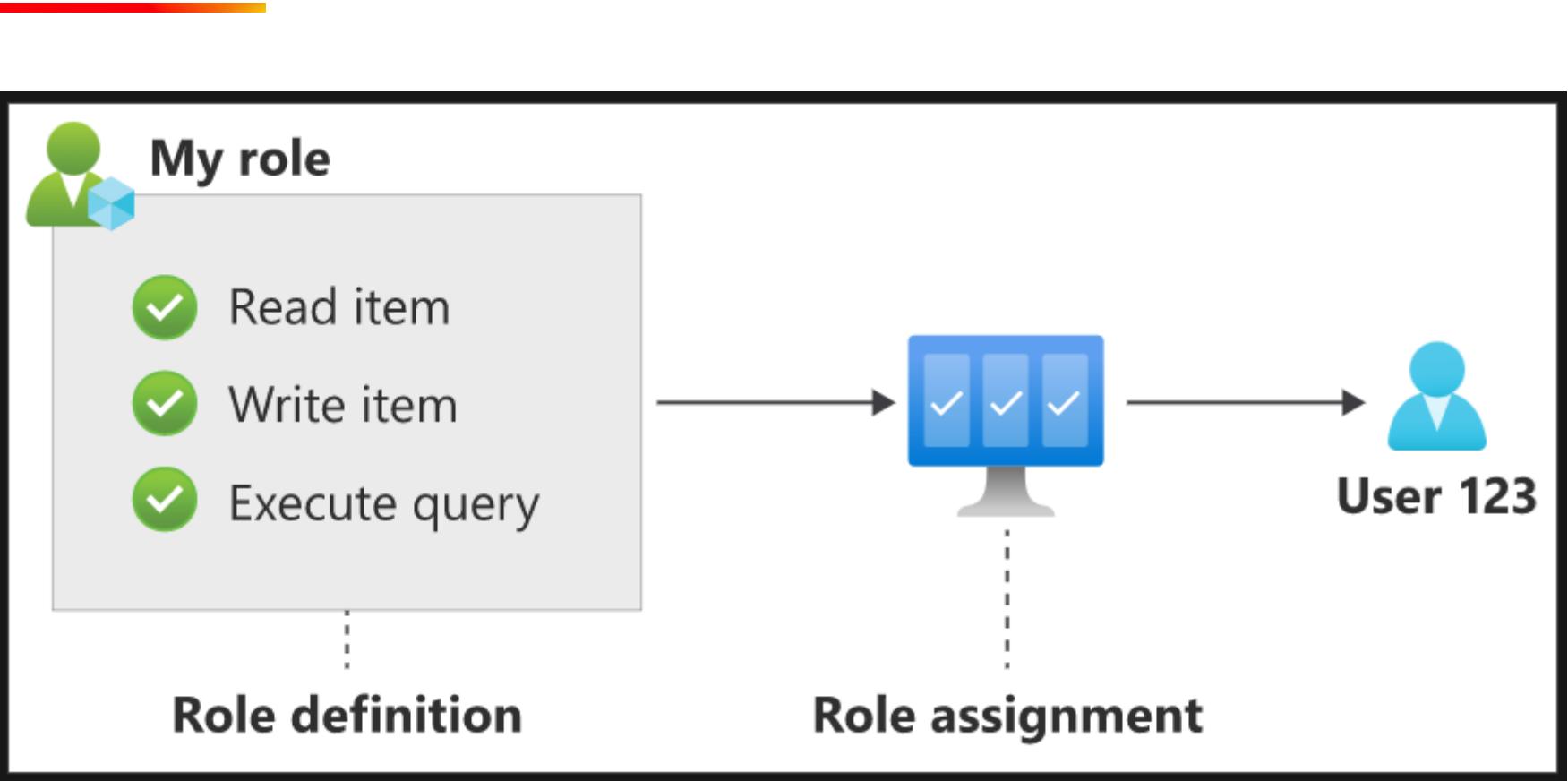
6:50:49 AM



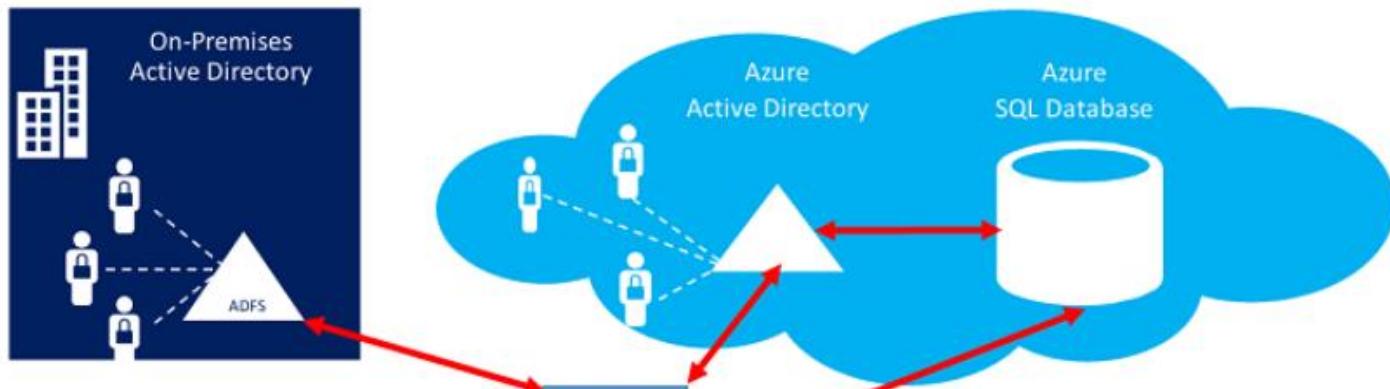
# Configure Security for Data

- Enable database authentication by using Azure AD
- Enable database auditing
- Configure dynamic masking on SQL workloads
- Implement database encryption for Azure SQL Database
- Implement network isolation for data solutions, including Azure Synapse Analytics and Azure Cosmos DB





# Azure AD Authentication with SQL V12 DB



APPLICATION

- SSMS
- SSDT
- Connection string based authentication
- SQL package





## 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

[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



# Configure and Manage Azure Key Vault

- Create and configure Key Vault
- Configure access to Key Vault
- Manage certificates, secrets, and keys
- Configure key rotation
- Configure backup and recovery of certificates, secrets, and keys



## 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

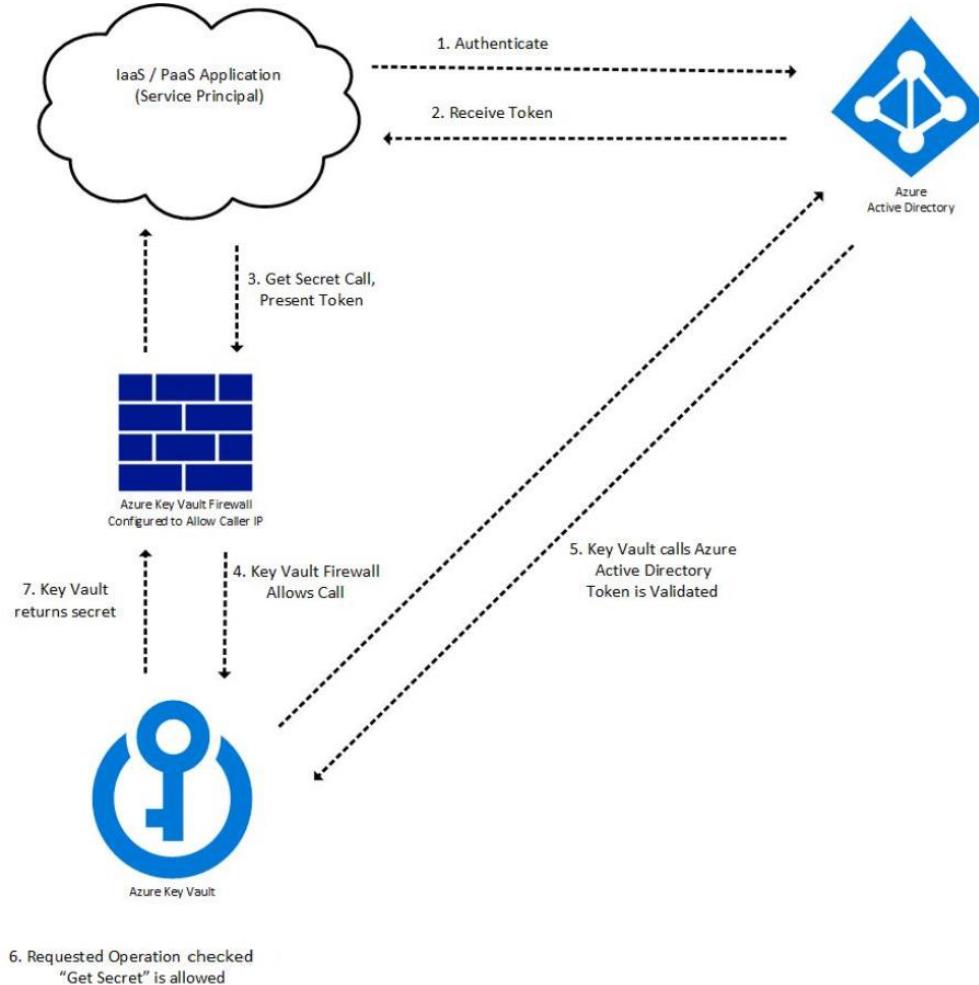
Region \*

East US

Pricing tier \* ⓘ

Standard





# Rotation policy

testkey

X

 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
<strong>CURRENT VERSION</strong>			
f3c!	✓ Enabled		
<strong>OLDER VERSIONS</strong>			
0ee1'	✓ Enabled	5/5/2020	5/5/2022



# 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

**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.

[Schedule exam >](#)

United States



**\$165 USD\***

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

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



Online at my home or office

I have a Private Access Code



Where do you want to take your exam?



At a test center



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	<a href="#">Remove</a>

## 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.

USD 80.00

[Add to Order](#)

**Special offer:** Regularly priced at USD 99.00! [Click here for details](#)

[More Details](#)



# 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





## 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>





Thank you!

Reza Salehi

@zaalion

