O'REILLY®

Azure Application Security

Protect Your Applications in the Cloud

December/2022

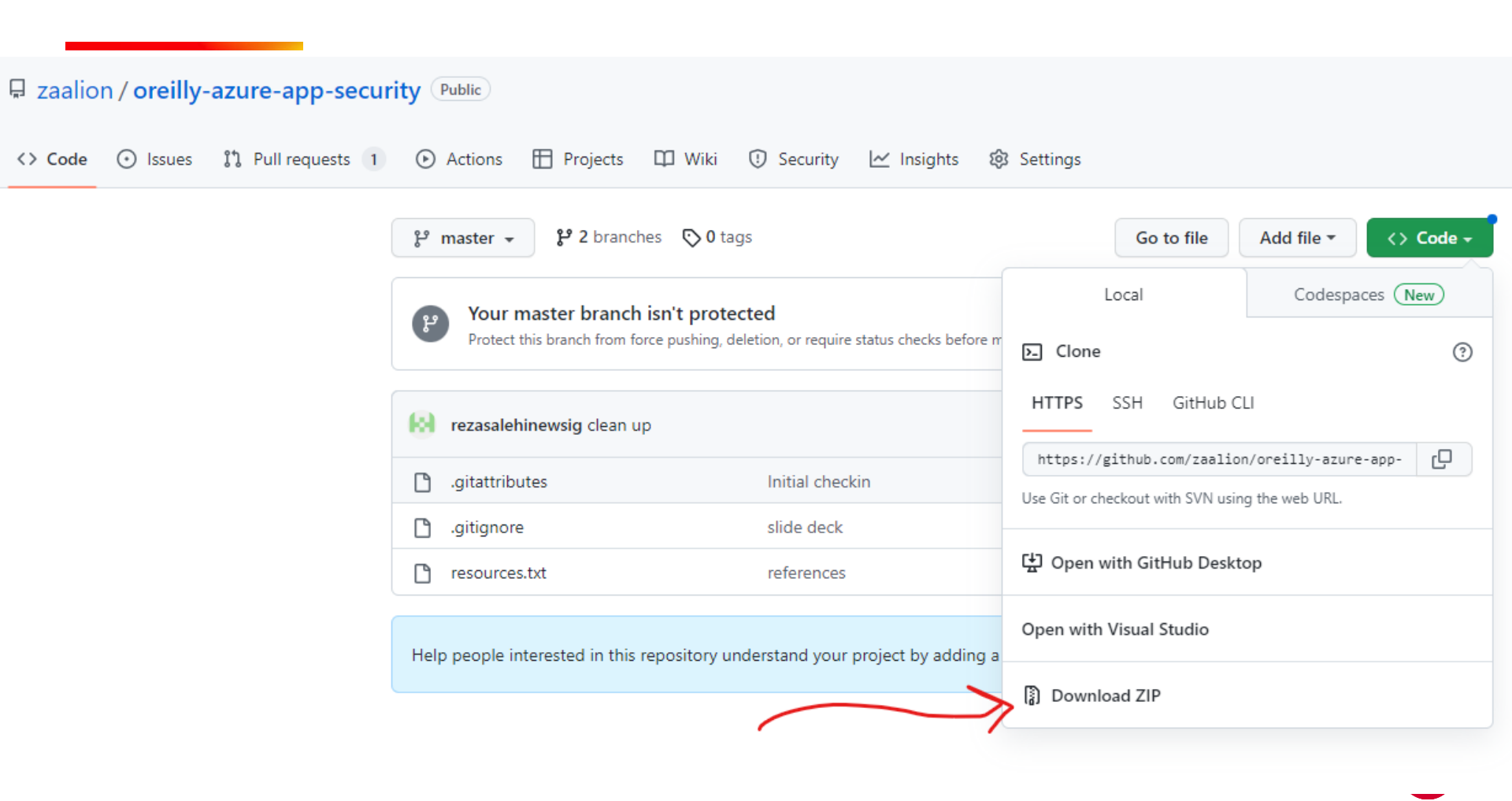
Reza Salehi

Cloud Consultant and Trainer

@zaalion

Course Repository

https://github.com/zaalion/oreilly-azure-app-security


zaalion / oreilly-azure-app-security
Public
Code
Issues
Pull requests 1
Actions
Projects
Wiki
Security
Insights
Settings
master
2 branches
0 tags
Go to file
Add file
Code
Your master branch isn't protected
Protect this branch from force pushing, deletion, or require status checks before m
rezasalehinewsig clean up
.gitattributes
Initial checkin
.gitignore
slide deck
resources.txt
references
Help people interested in this repository understand your project by adding a
Local
Codespaces New
Clone
HTTPS
SSH
GitHub CLI
https://github.com/zaalion/oreilly-azure-app-
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

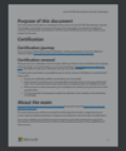
AZ-500: Secure your data and applications

4 Modules

Intermediate | Administrator | Azure

⊕ Save


1


2


3


4

Study Guide

Exam AZ-500: Microsoft Azure Security Technologies

Quick navigation

Learn /

Microsoft Azure Well-Architected Framework

Article • 11/30/2022 • 4 minutes to read • 7 contributors

Feedback

The Azure Well-Architected Framework is a set of guiding tenets that can be used to improve the quality of a workload. The framework consists of five pillars of architectural excellence:

- Reliability
- Security
- Cost Optimization
- Operational Excellence
- Performance Efficiency

Incorporating these pillars helps produce a high quality, stable, and efficient cloud architecture:

Pillar	Description
Reliability	The ability of a system to recover from failures and continue to function.
Security	Protecting applications and data from threats.
Cost Optimization	Managing costs to maximize the value delivered.
Operational Excellence	Operations processes that keep a system running in production.
Performance Efficiency	The ability of a system to adapt to changes in load.

Learn / Security / Benchmark /

Overview of Azure security controls (v2)

Article • 11/14/2022 • 4 minutes to read • 2 contributors

Feedback

The Azure Security Benchmark (ASB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure.

This benchmark is part of a set of holistic security guidance that also includes:

- **Cloud Adoption Framework** – Guidance on security, including strategy, roles and responsibilities, Azure Top 10 Security Best Practices, and reference implementation.
- **Azure Well-Architected Framework** – Guidance on securing your workloads on Azure.
- **Microsoft Security Best Practices** – recommendations with examples on Azure.

The Azure Security Benchmark focuses on cloud-centric control areas. These controls are consistent with well-known security benchmarks, such as those described by the Center for Internet Security (CIS) Controls Version 7.1 and National Institute of Standards and Technology (NIST) SP 800-53. The following controls are included in the Azure Security Benchmark:

Manage Azure Active Directory (Azure AD) Identities

- Create and manage a managed identity for Azure resources

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

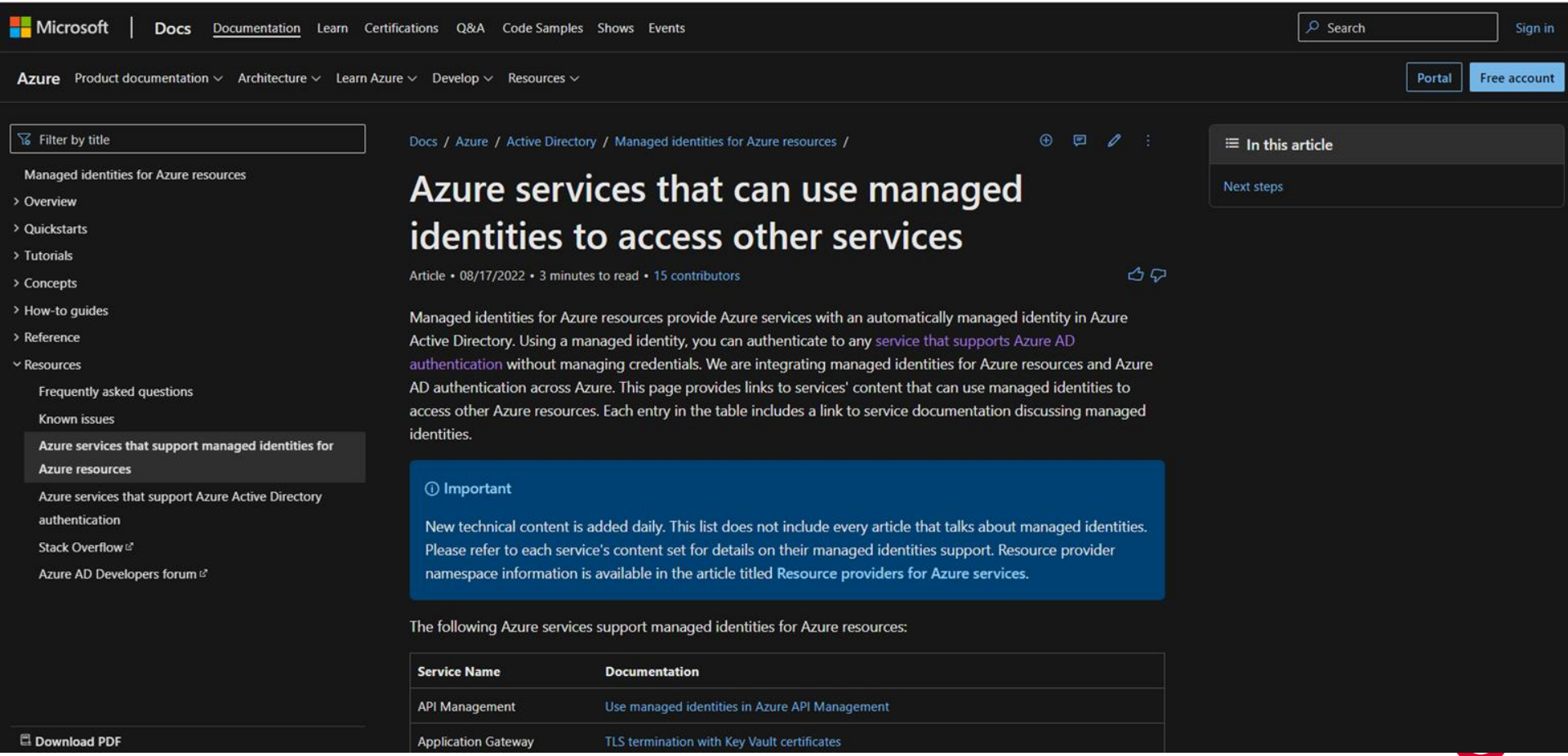
Resource group * ⓘ:

Create new

Instance details

Region * ⓘ: West US

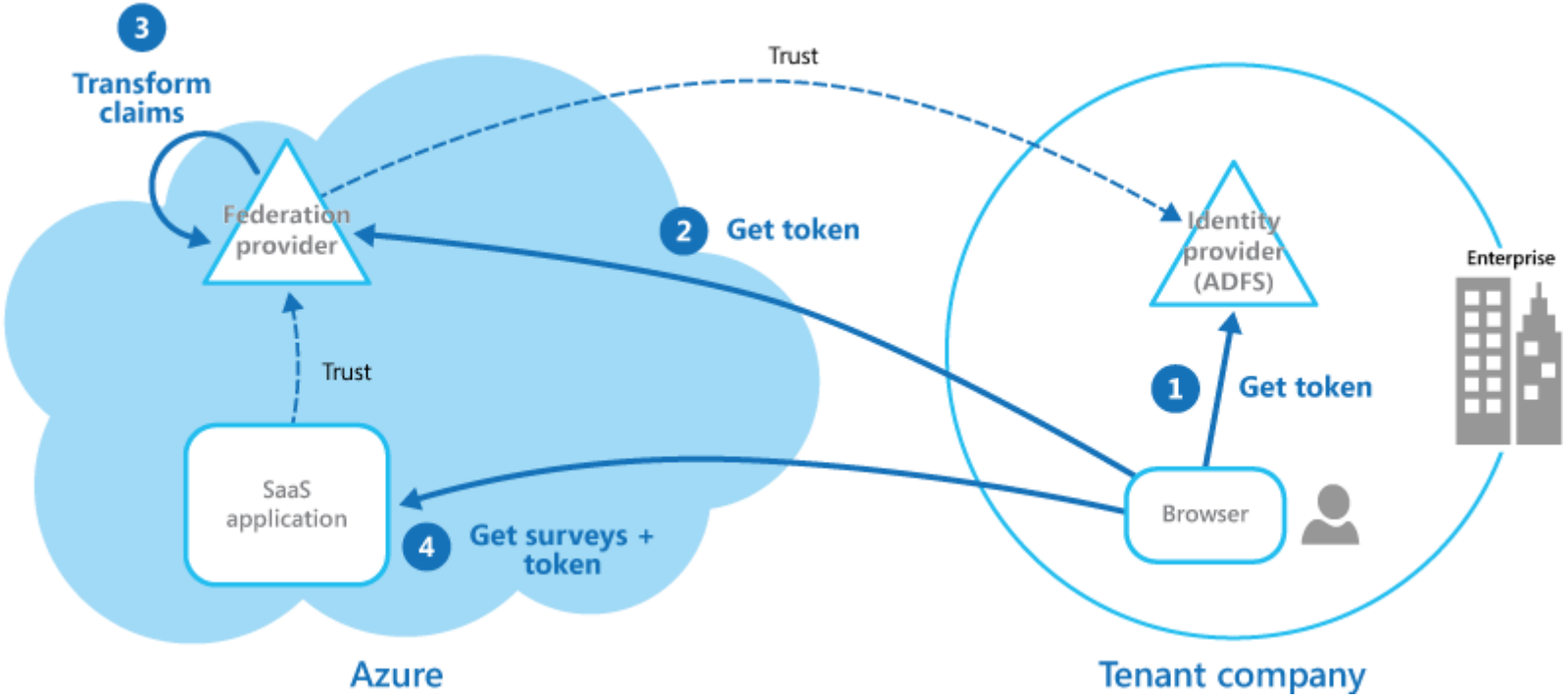
Name * ⓘ:


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

Manage Application Access

- 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

- 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

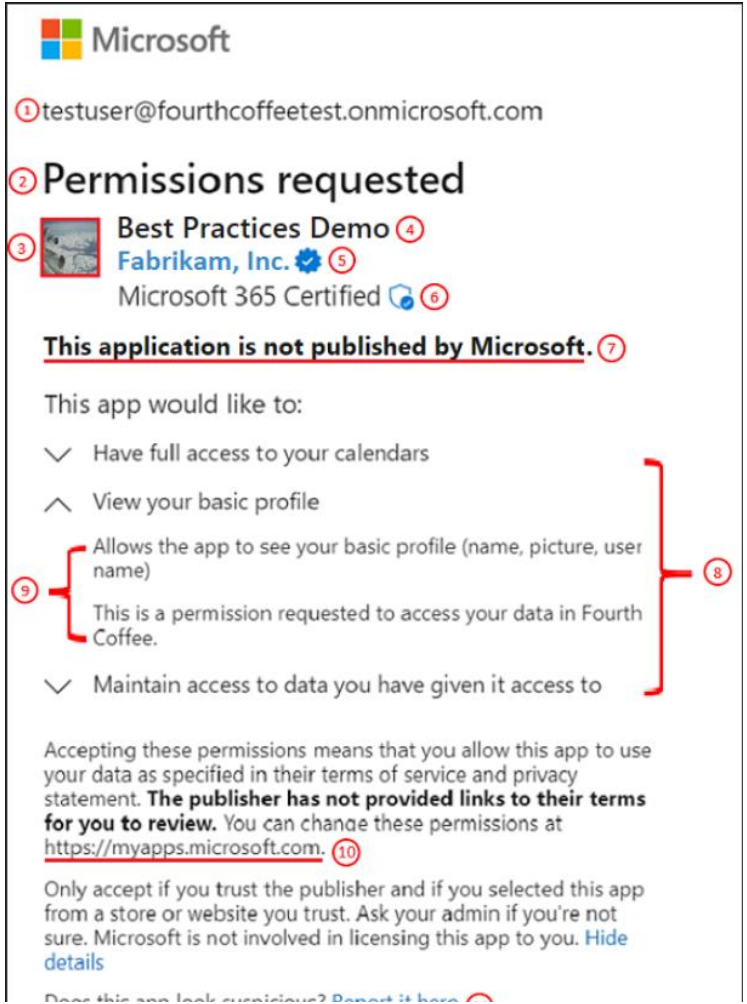
All applications | **Owned applications** | Deleted applications | Applications from personal account

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

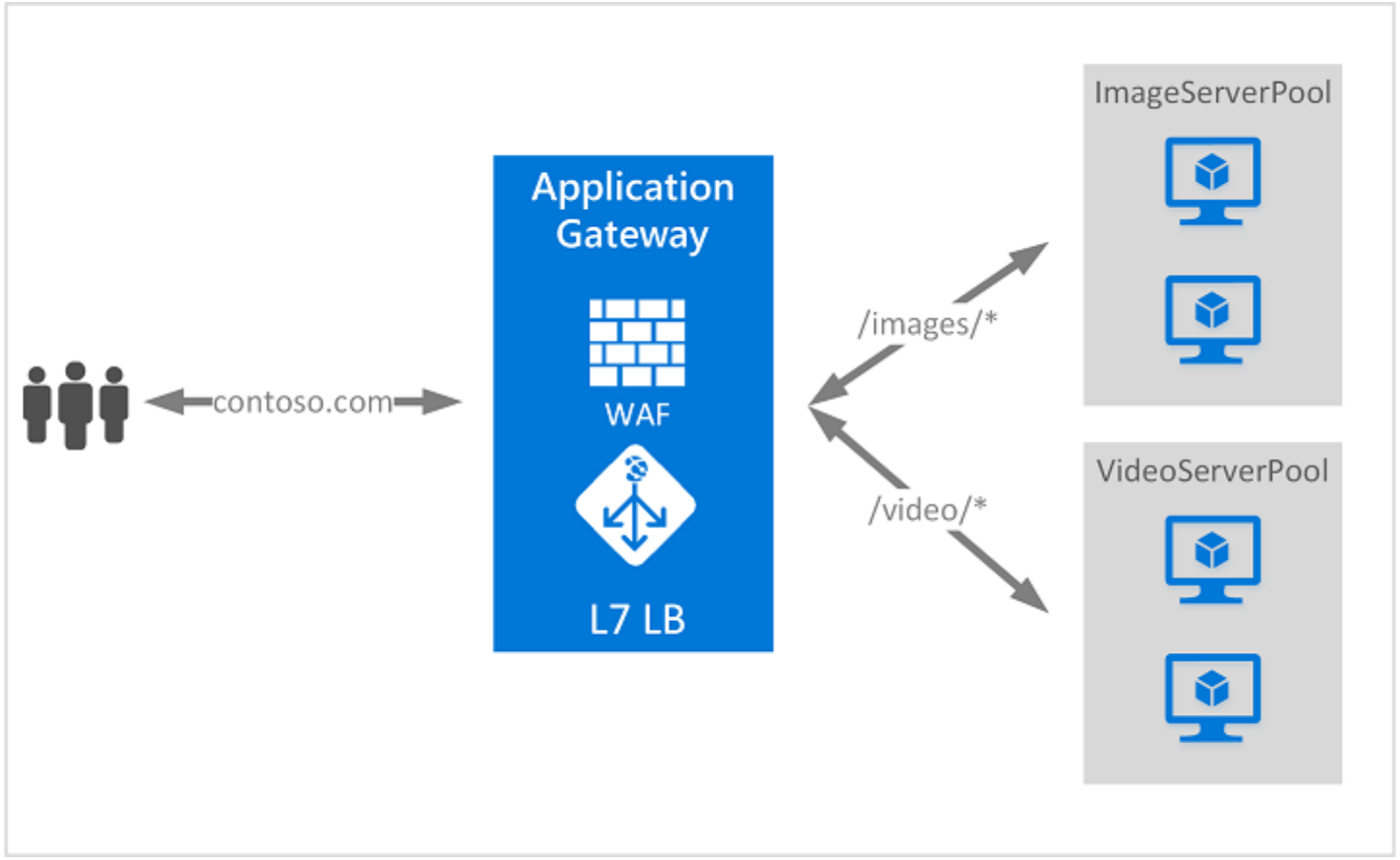
Add a permission | Grant admin consent for Default Directory

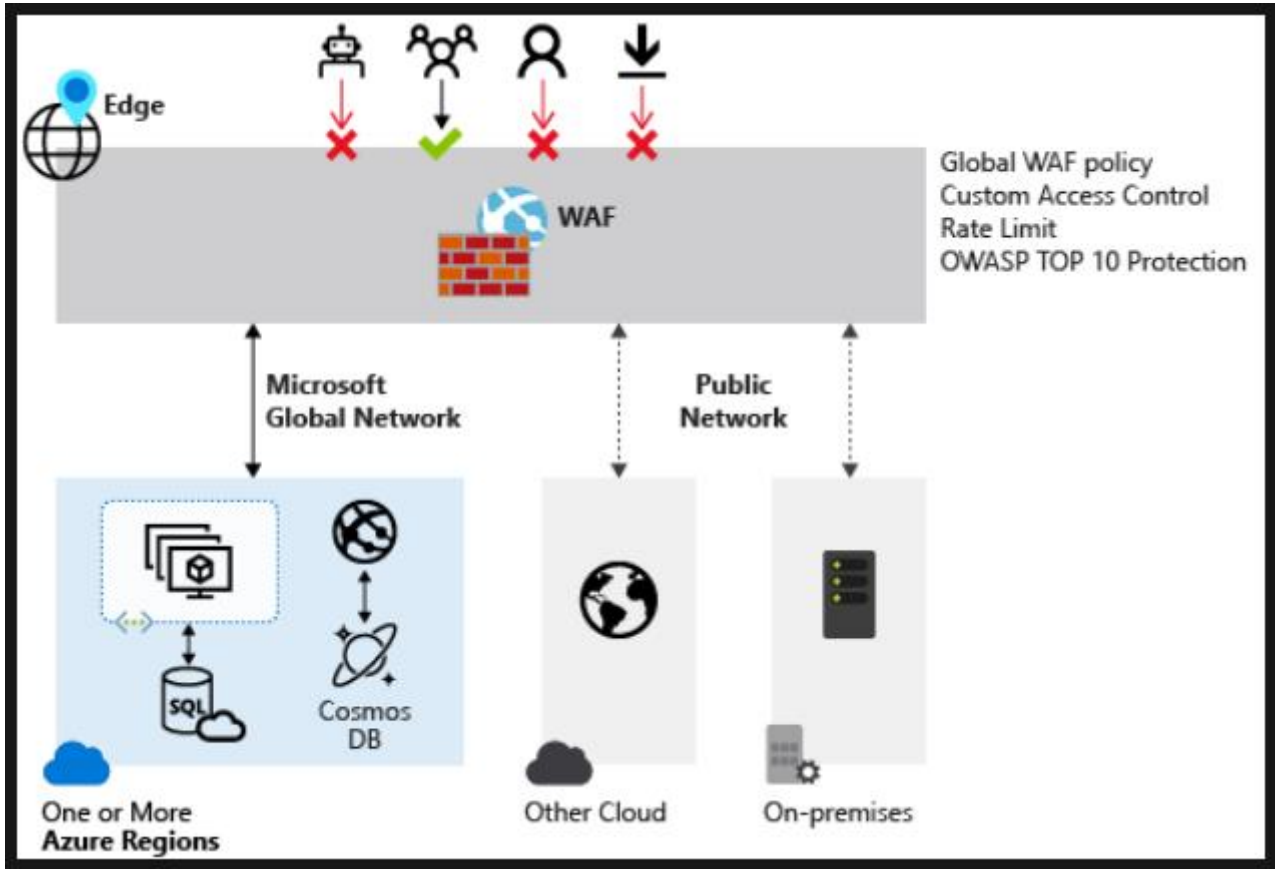
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	No	

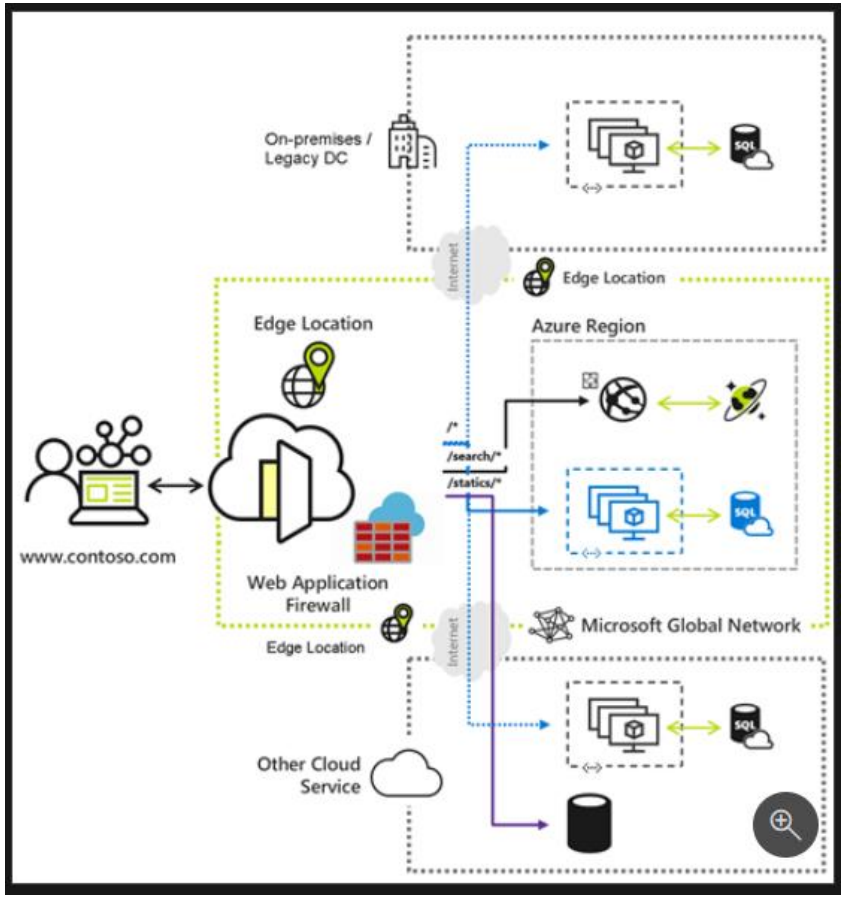
To view and manage permissions and user consent, try Enterprise applications.

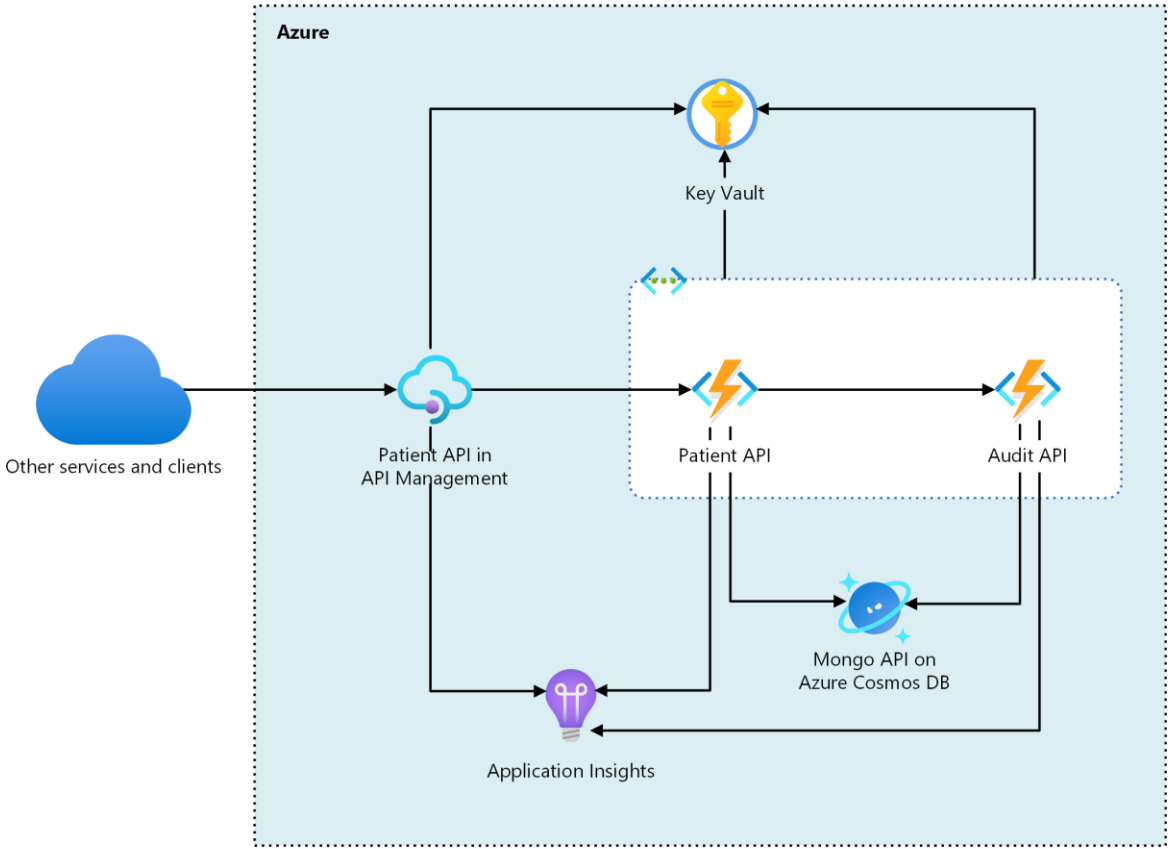
Implement Advanced Network Security

- Secure the connectivity of virtual networks
- 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

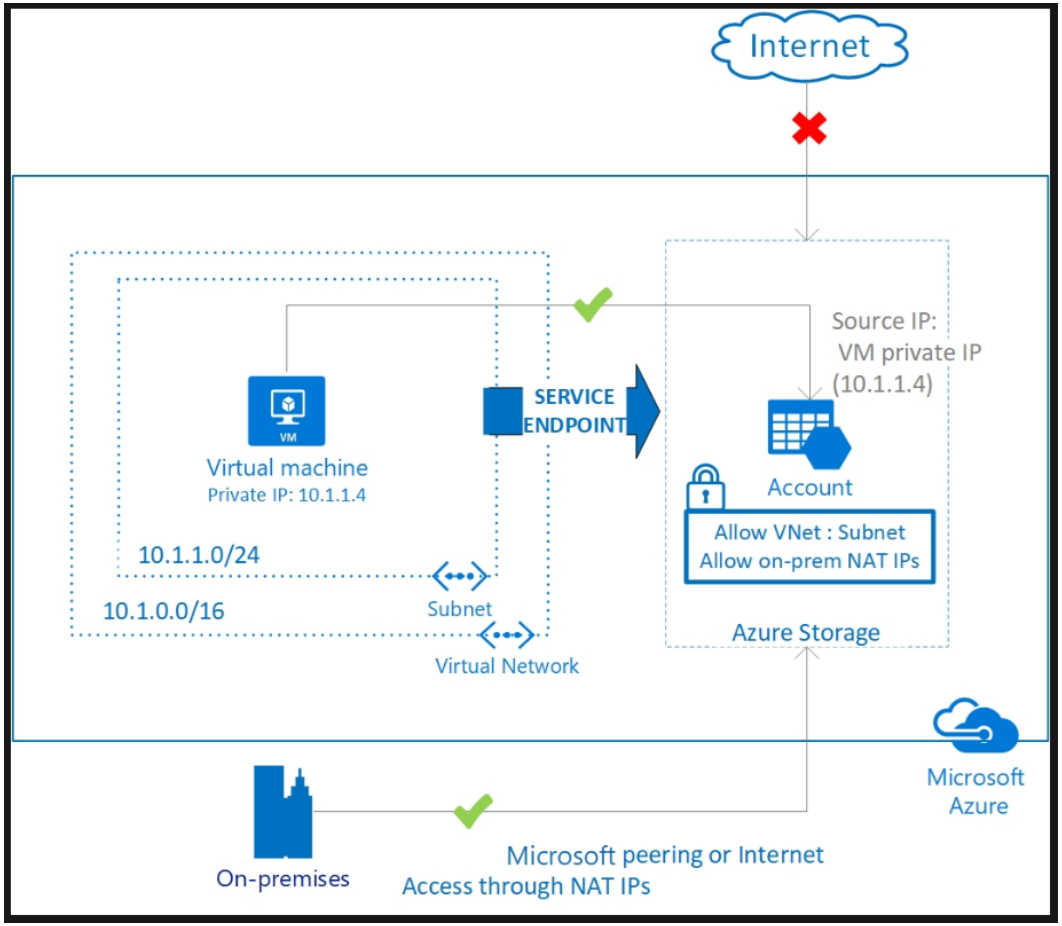

Application Gateway
WAF
L7 LB
contoso.com
/images/*
/video/*
ImageServerPool
VideoServerPool


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

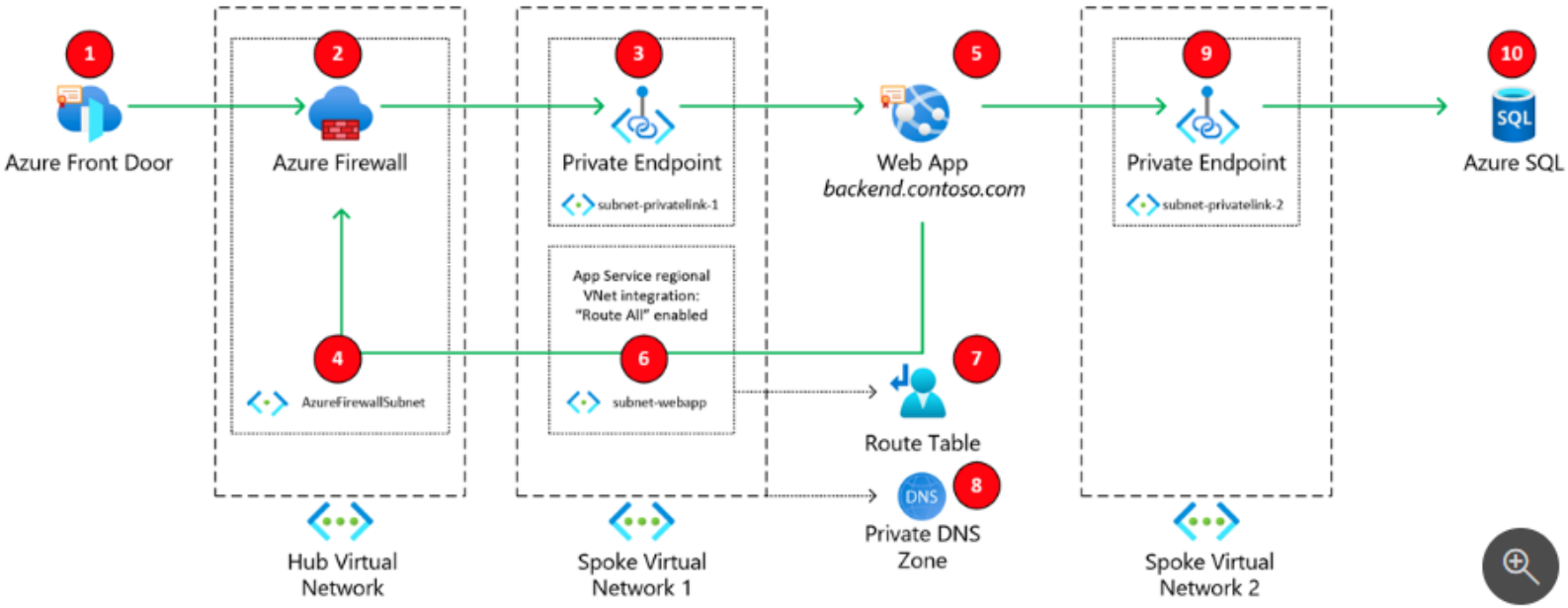


Microsoft
Azure


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

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

Configure Advanced Security for Compute

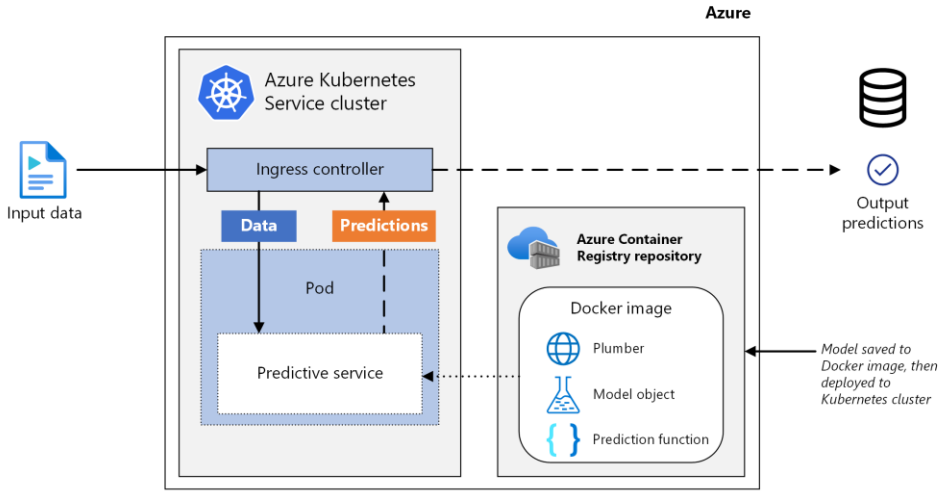
- Configure security for container services
- Manage access to Azure Container Registry
- Configure security for serverless compute
- Configure security for an Azure App Service
- Configure encryption at rest
- Configure encryption in transit

Configure Security for Container Services

- Security considerations for Azure Container Instances
- Azure security baseline for Container Instances
- Security concepts for 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



Microsoft Azure

Configure Security for Serverless Compute

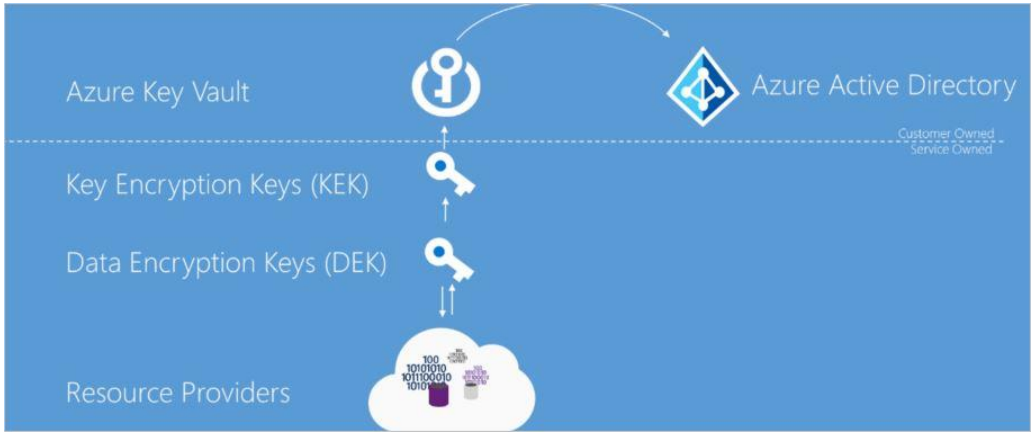
- Secure access and data in Azure Logic Apps
- Secure Azure Functions

Configure Security for an Azure App Service

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

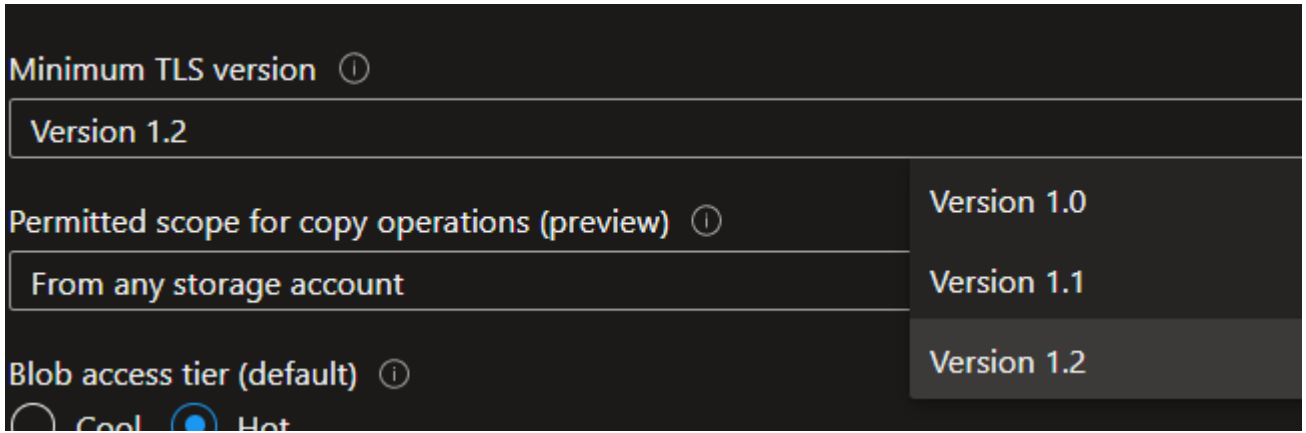
Configure Encryption at Rest

- 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

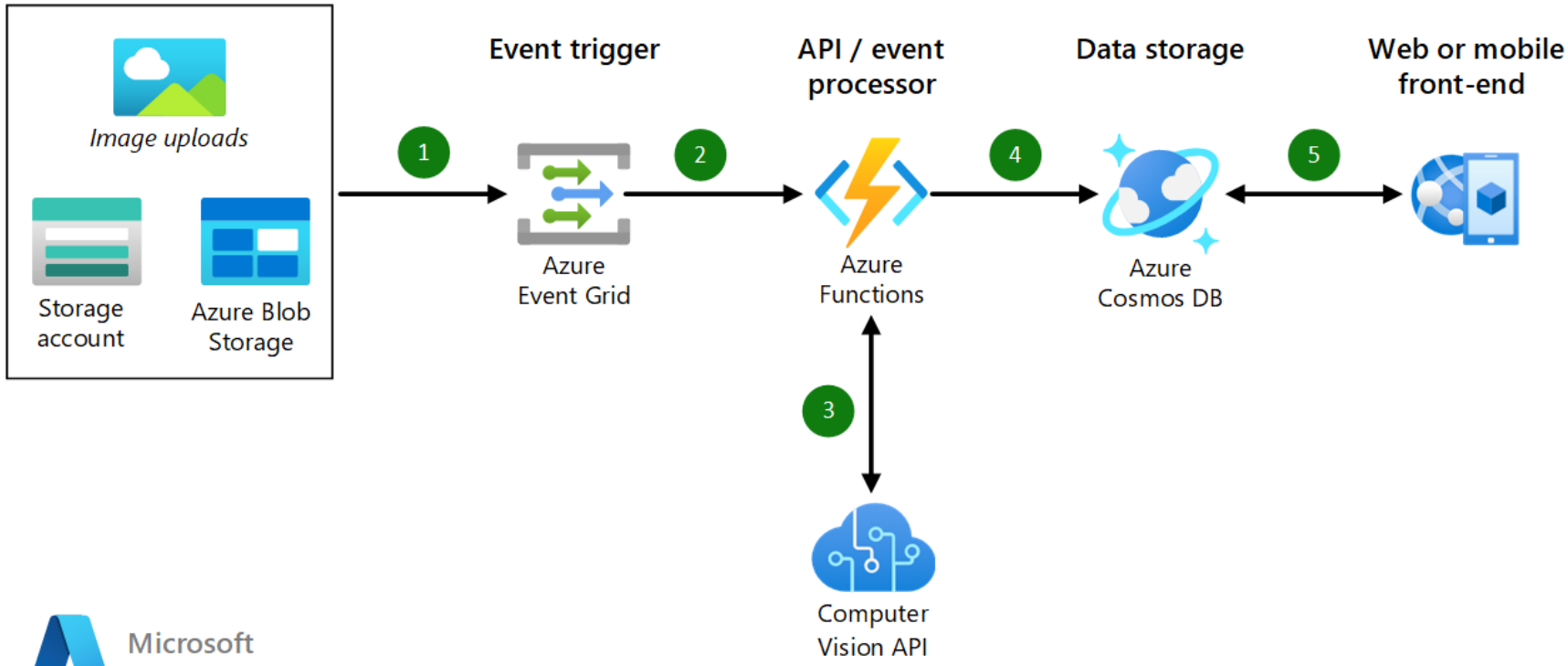


Configure Security for Storage

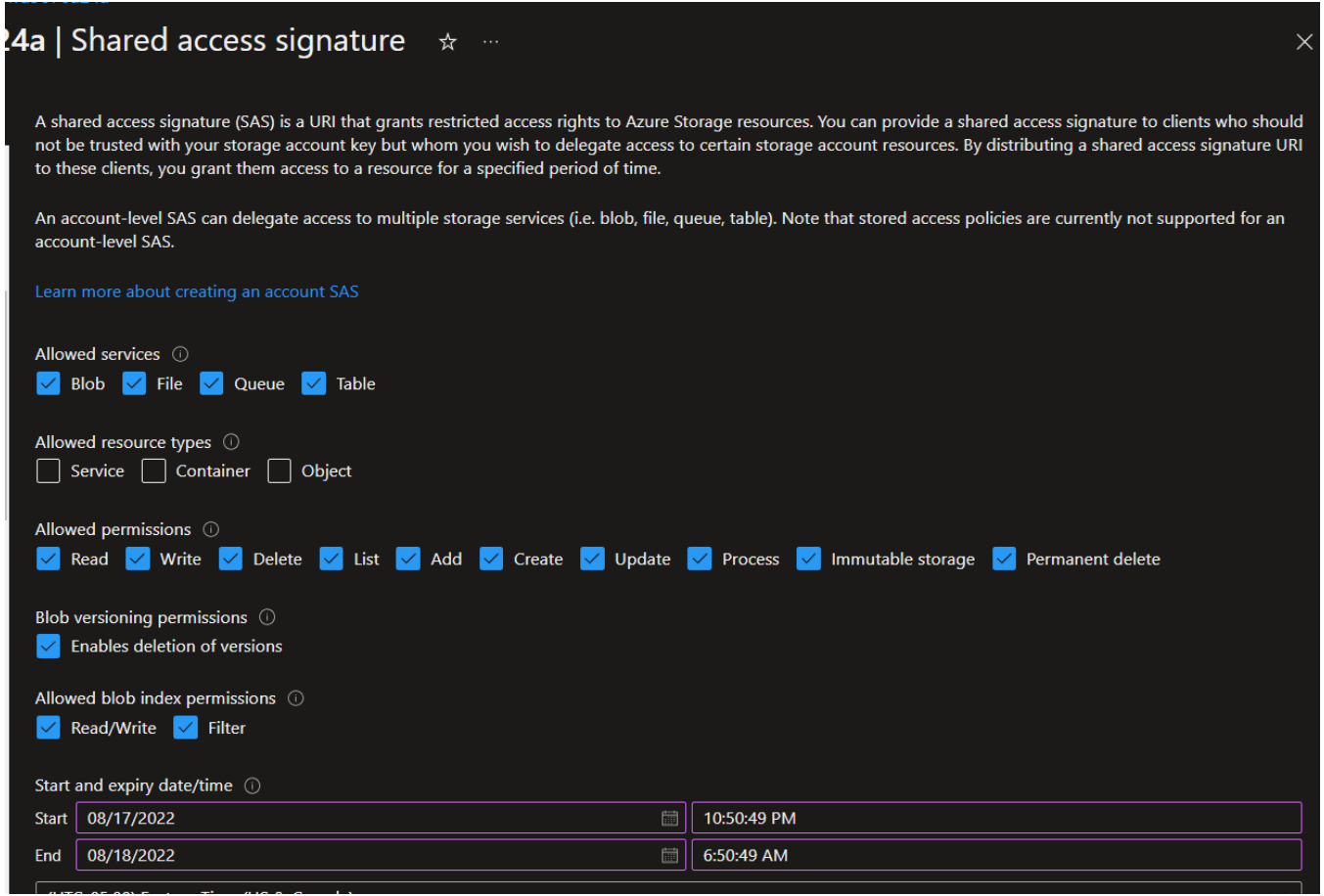
- Configure access control for storage accounts
- Configure storage account access keys
- Configure Azure AD authentication for Azure Blobs and Azure Files
- Configure delegated access

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

Microsoft Azure

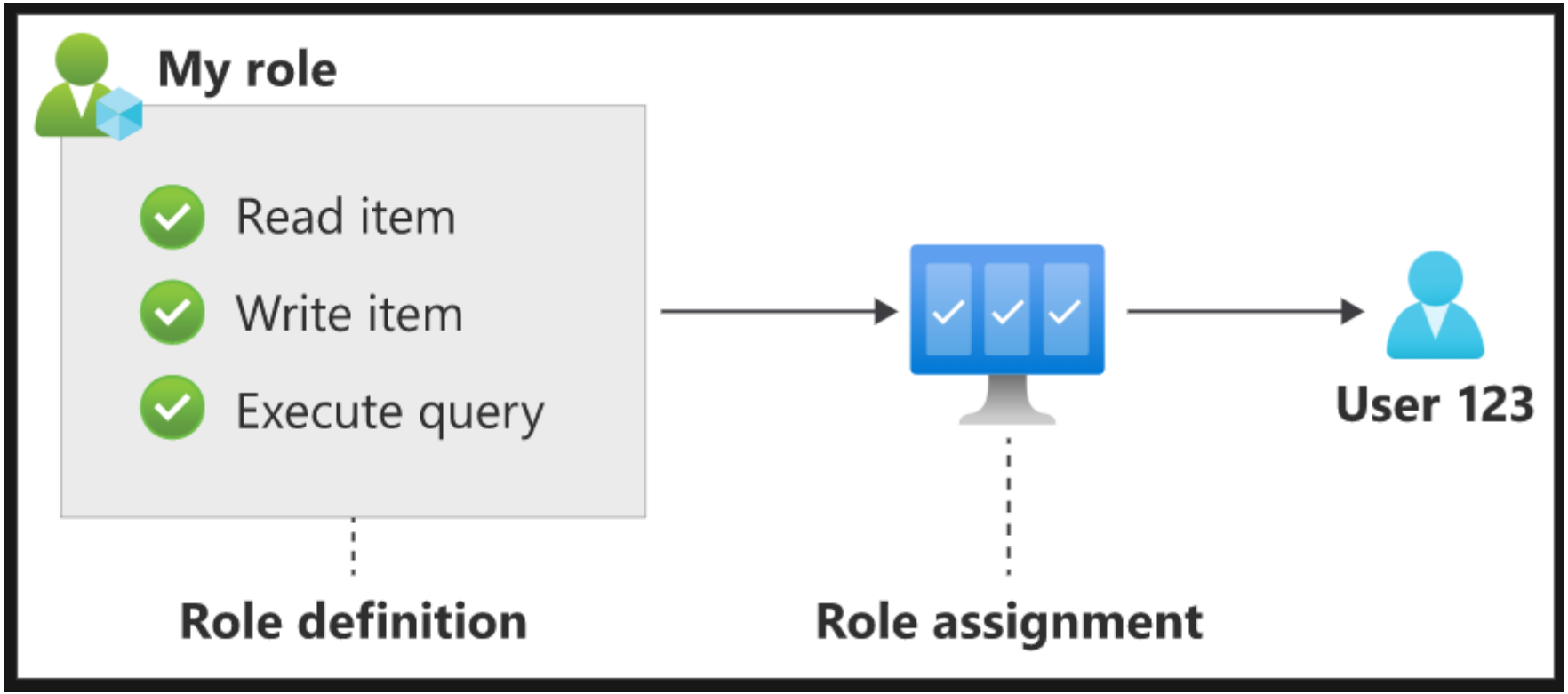


Microsoft Azure

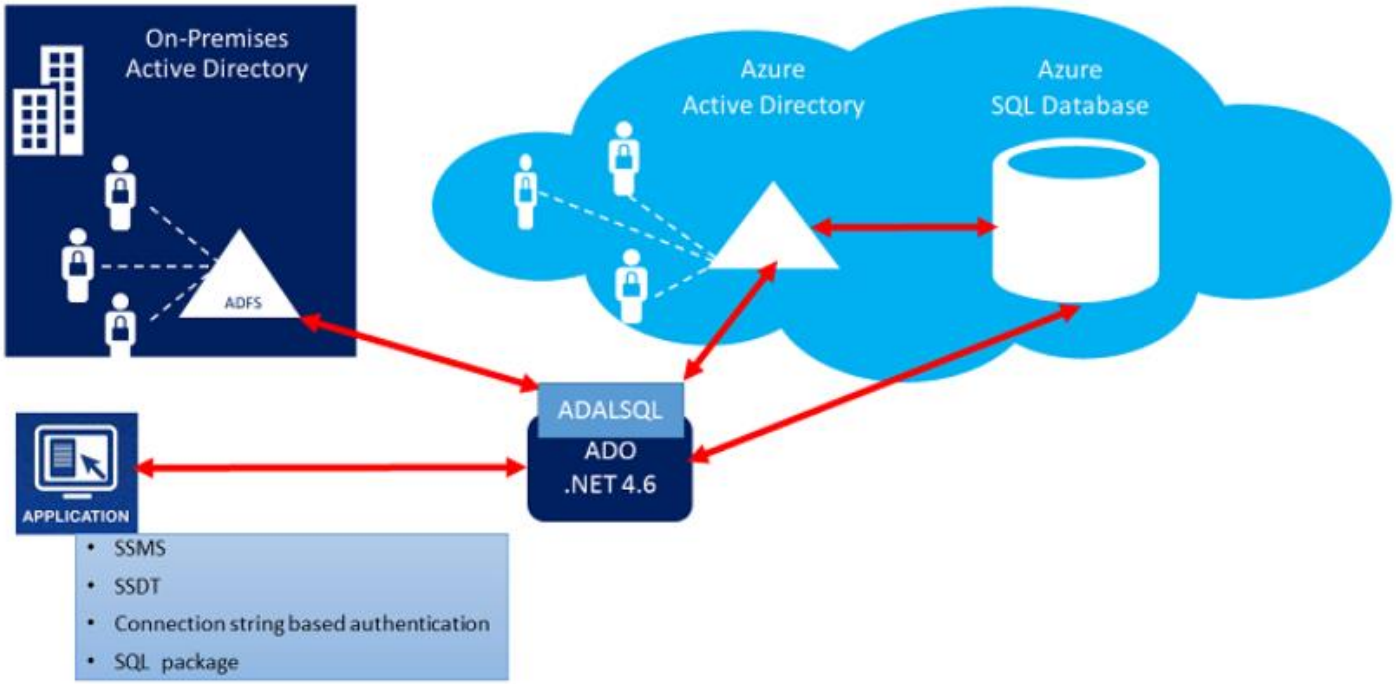

24a | Shared access signature
A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources. You can provide a shared access signature to clients who should not be trusted with your storage account key but whom you wish to delegate access to certain storage 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

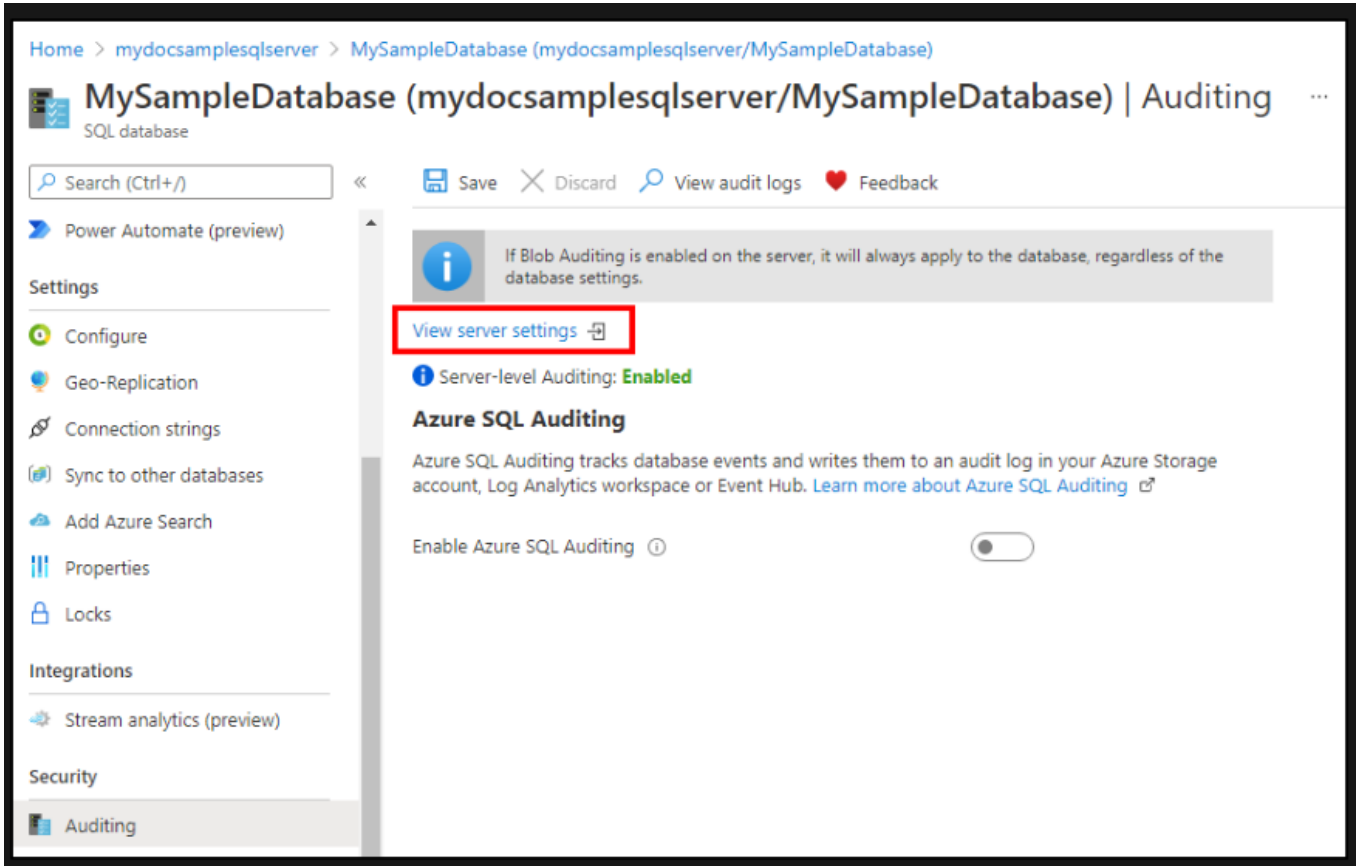
Configure Security for Data

- 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


My role
Read item
Write item
Execute query
User 123
Role definition
Role assignment

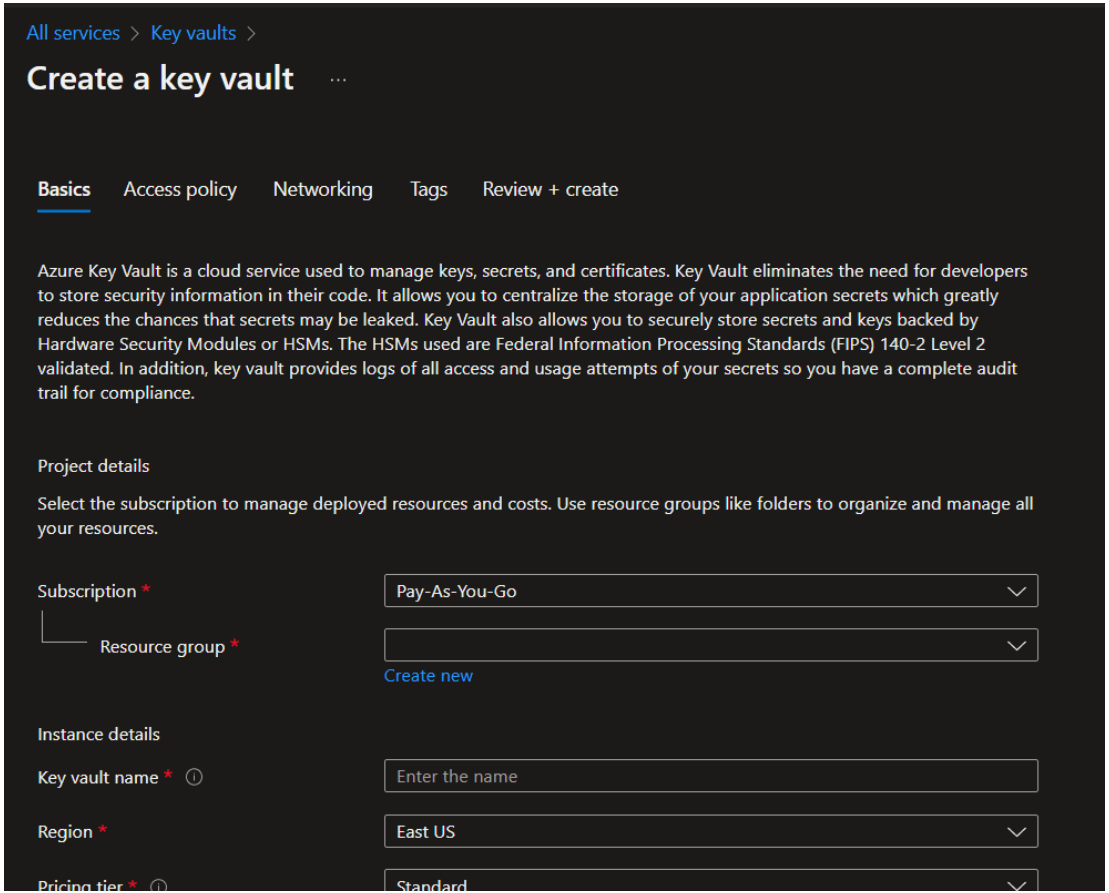
Azure AD Authentication with SQL V12 DB

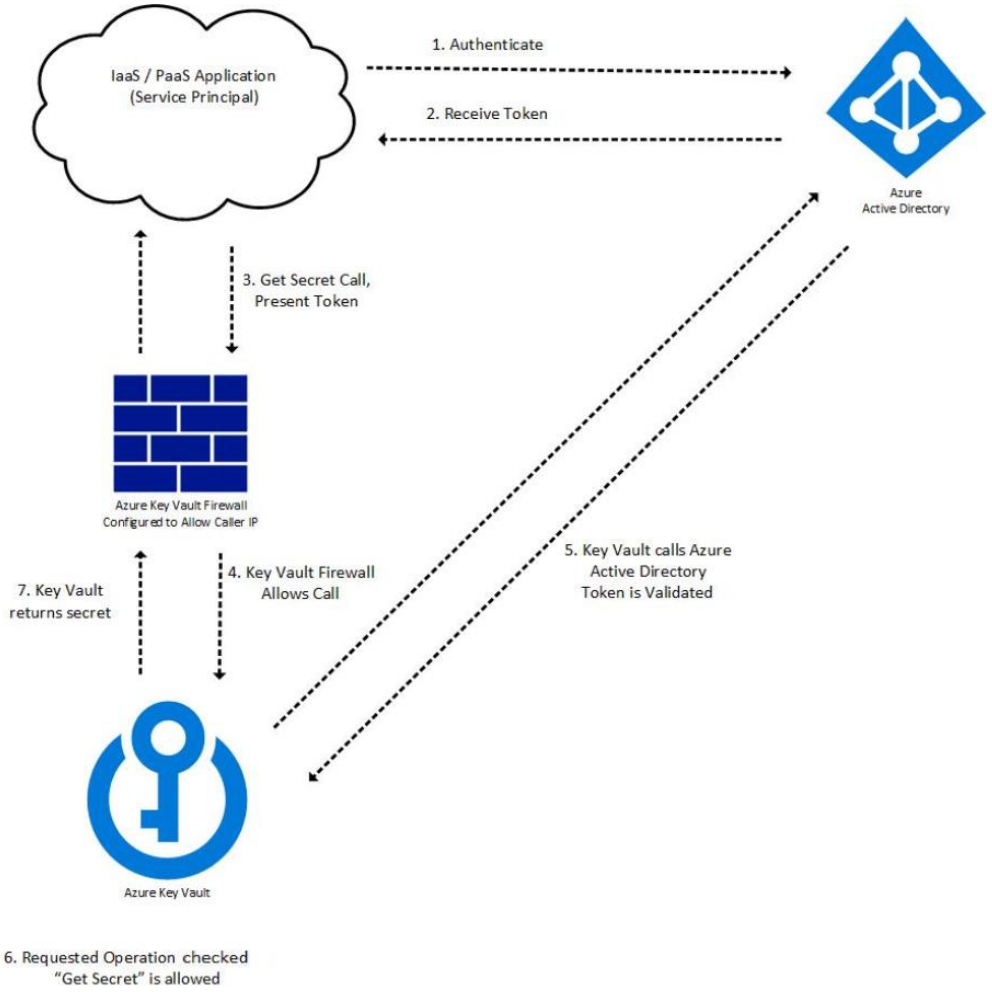


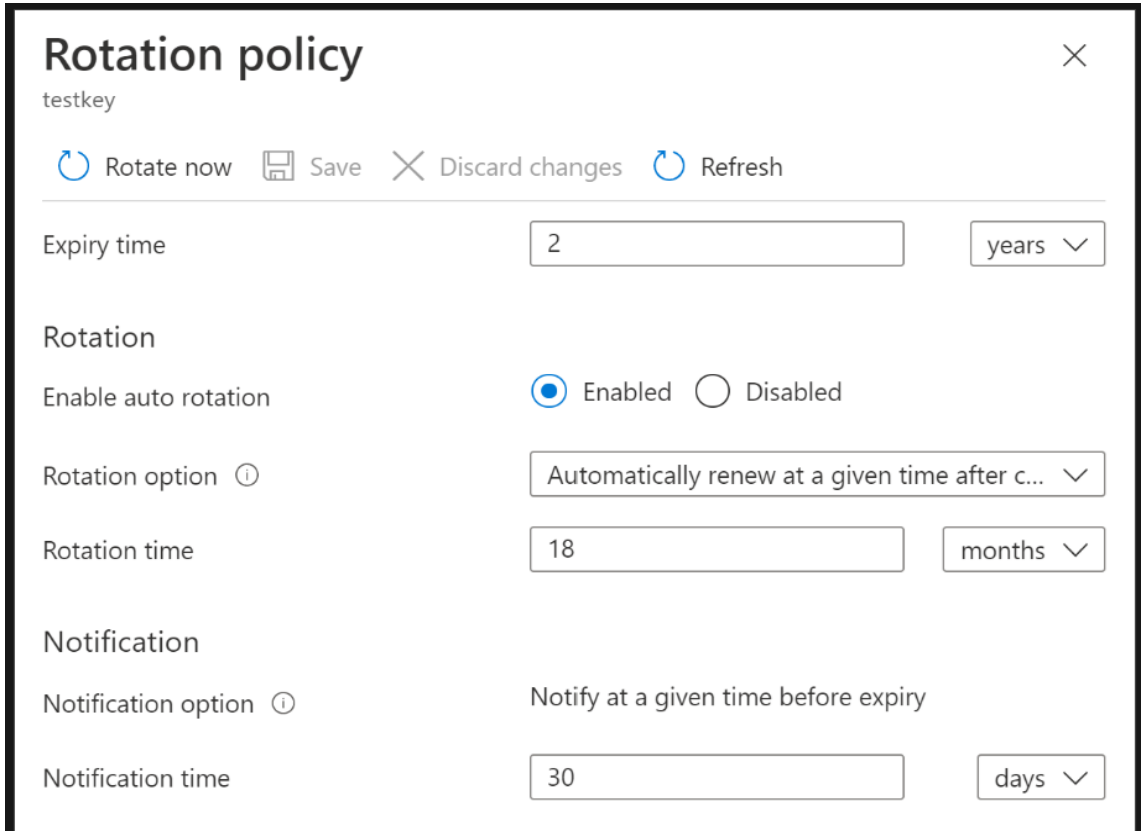

Home > mydocsamplesqlserver > MySampleDatabase (mydocsamplesqlserver/MySampleDatabase)
MySampleDatabase (mydocsamplesqlserver/MySampleDatabase) | Auditing
SQL database
Search (Ctrl+/)
Save
Discard
View audit logs
Feedback
Power Automate (preview)
Settings
Configure
Geo-Replication
Connection strings
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

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


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

O'REILLY®

Thank you!

Reza Salehi

@zaalion