KVASIR

Think evil, do good

MS Azure Security Technologies

AZ-500 Certification

The Collective Conspiracy Coven of Conspicuous Insight and Contagious Brilliance

Version 1.0

December 2, 2019

Contents

1 The Certification

1.1 The Candidates

Candidates for this exam are Microsoft Azure security engineers who implement security controls, maintain the security posture, manages identity and access, and protects data, applications, and networks. Candidates identify and remediate vulnerabilities by using a variety of security tools, implements threat protection, and responds to security incident escalations. As a Microsoft Azure security engineer, candidates often serve as part of a larger team dedicated to cloud-based management and security and may also secure hybrid environments as part of an end-to-end infrastructure.

Candidates for this exam should have strong skills in scripting and automation, a deep understanding of networking, virtualization, and cloud N-tier architecture, and a strong familiarity with cloud capabilities, Microsoft Azure products and services, and other Microsoft products and services.

1.2 Content Overview

- Manage identity and access (20-25%)
  - Configure Microsoft Azure Active Directory for workloads
  - Configure Microsoft Azure AD Privileged Identity Management
  - Configure Microsoft Azure tenant security
- Implement platform protection (35-40%)
  - Implement network security
  - Implement host security
  - Configure container security
  - Implement Microsoft Azure Resource management security
- Manage security operations (15-20%)
  - Configure security services
  - Configure security policies
  - Manage security alerts
- Secure data and applications (30-35%)
  - Configure security policies to manage data
  - Configure security for data infrastructure
  - Configure encryption for data at rest
  - Implement security for application delivery
  - Configure application security
  - Configure and manage Key Vault

1.3 Prerequisites

The AZ-500 Azure Security Engineer Exam, like the MS-500 exam, covers a wide range of topics and technologies. Before considering taking this exam, you should first have good knowledge in the Azure technologies themselves which makes sense. You should learn what are the different Azure platform technologies in order to learn how to secure them.

So a good way to do that is to take the Azure AZ-900 (Azure Fundamentals) or the AZ-103 (Azure Administrator) exam first to learn more about Azure technologies. Now this is not a requirement for taking the AZ-500 exam, but it is a good start. If you are familiar with Azure technologies, then you can go and take the AZ-500 Azure Security Engineer Exam right away.

1.4 The exam

The AZ-500 Azure Security Engineer Exam expects you to know how to implement security controls, maintain the security posture, manages identity and access, and protects data, applications, and networks.

As per the AZ-500 Azure Security Engineer Exam official documentation:

> Candidates identify and remediate vulnerabilities by using a variety of security tools, implements threat protection, and responds to security incident escalations. As a Microsoft Azure security engineer, candidates often serve as part of a larger team dedicated to cloud-based management and security and may also secure hybrid environments as part of an end-to-end infrastructure

2 Certification Content

2.1 Manage identity and access (20-25%)

2.1.1 Configure Microsoft Azure Active Directory for workloads

- Create App registration
- Configure App registration permission scopes
- Manage App registration permission consent
- Configure multi-factor authentication settings
- Manage Microsoft Azure AD directory groups
- Manage Microsoft Azure AD users
- Install and configure Microsoft Azure AD Connect
- Configure authentication methods
- Implement conditional access policies
- Configure Microsoft Azure AD identity protection

Revision notes

- Create App registration
  Tree Supported account types:
  - Azure AD only single-tenant -> LOB app.
  - Azure AD only multi-tenant -> All business and educational users.
  - Azure AD multi-tenant and personal Microsoft accounts -> Widest set of users.
- Configure App registration permission scopes
  Uses OAuth 2.0 for third parti app access.
  MS strongly recommends that you use Microsoft Graph.
  Two Permission types:
  - Delegated permissions -> App permission ∩ User permission
  - Application permissions -> App permission

  Interesting scopes:
  - openid -> Required for OpenID Connect.
  - email -> access to the user's primary email address.
  - profile -> access to a substantial amount of information about the user. See id tokens
  - offline_access -> Maintain access to data you have given it access to.
- Manage App registration permission consent
  Consent can be given by individuals or by Admins for an entire tenant.
  Admin consent can only be granted with the "admin consent endpoint"

Literature	
Quickstart: Register an application with the Microsoft identity platform	3 (5)
Permissions and consent in the Azure Active Directory v1.0 endpoint	6 (10)
Permissions and consent in the Microsoft identity platform endpoint	18
Configure Azure Multi-Factor Authentication settings	21
Use groups for management	3
Custom installation of Azure AD Connect	26 (90)
Authentication method for Azure Active Directory hybrid identity solution	15+13
Best practices for Conditional Access in Azure Active Directory	6
What is Azure Active Directory Identity Protection?	3
	114

2.1.2 Configure Microsoft Azure AD Privileged Identity Management

- monitor privileged access
- configure access reviews It is possible to setup periodic reviews for
- activate Privileged Identity Management
  The first user of PIM get two rols:
  - Security-administrator -> manage security-related features in the Microsoft 365 security center, Azure Active Directory Identity Protection, Azure Information Protection, and Office 365 Security & Compliance Center.
  - Privileged Role Administrator -> manage assignments for all Azure AD roles including the Global Administrator role

Literature	
Start using Privileged Identity Management	3
Deploy Azure AD Privileged Identity Management (PIM)	26
What are Azure AD access reviews?	6+12
	47

2.1.3 Configure Microsoft Azure tenant security

- transfer Microsoft Azure subscriptions between Microsoft Azure AD tenants
- manage API access to Microsoft Azure subscriptions and resources

Literature	
Transfer billing ownership of an Azure subscription to another account	10
Authorize developer accounts by using Azure Active Directory in Azure API Management	4
Authentication flows and application scenarios	10
Azure Active Directory Graph API	4
	28

2.2 Implement platform protection (35-40%)

2.2.1 Implement network security

- configure virtual network connectivity
- configure Network Security Groups (NSGs)
- create and configure Microsoft Azure firewall
- create and configure application security groups
- configure remote access management
- configure baseline
- configure resource firewall

Literature	
What is Azure Virtual Network?	5
Create, change, or delete a network security group	13
Tutorial: Deploy and configure Azure Firewall using the Azure portal	7
Application Security Groups now generally available in all Azure regions	6
Security management in Azure	20
Protect your network resources in Azure Security Center	9
Configure Azure Storage firewalls and virtual networks	17
Azure SQL Database and Azure SQL Data Warehouse IP firewall rules	11
	88

2.2.2 Implement host security

- configure endpoint security within the VM
- configure VM security
- harden VMs in Microsoft Azure
- configure system updates for VMs in Microsoft Azure
- configure baseline

Literature	
Microsoft Antimalware for Azure Cloud Services and Virtual Machines	10
Security best practices for IaaS workloads in Azure	12
Harden Your Azure Infrastructure Using Azure Security Center Just-In-Time VM Access	10
Manage updates and patches for your Azure VMs	10
Retirement of Security Center features (July 2019)	7
	49

2.2.3 Configure container security

- configure network
- configure authentication
- configure container isolation
- configure AKS security
- configure container registry

- configure container instance security
- implement vulnerability management

Literature	
Azure Virtual Network capabilities	3
Service principals with Azure Kubernetes Service (AKS)	6
Container Security in Microsoft Azure	45
Security concepts for applications and clusters in Azure Kubernetes Service (AKS)	6
Security considerations for Azure Container Instances	9
	69

2.2.4 Implement Microsoft Azure Resource management security

- create Microsoft Azure resource locks
- manage resource group security
- configure Microsoft Azure policies
- configure custom RBAC roles
- configure subscription and resource permissions

Literature	
Lock resources to prevent unexpected changes	6
What is role-based access control (RBAC) for Azure resources?	7
Tutorial: Create and manage policies to enforce compliance	14
Custom roles for Azure resources	4
Manage access to Azure resources using RBAC and the Azure portal	6
	37

2.3 Manage security operations (15-20%)

2.3.1 Configure security services

- configure Microsoft Azure monitor
- configure Microsoft Azure log analytics
- configure diagnostic logging and log retention
- configure vulnerability scanning

Literature	
Azure Management - Monitoring	3
Manage access to log data and workspaces in Azure Monitor	10
Azure Resource logs overview	2
Vulnerability assessment in Azure Security Center	4
	19

2.3.2 Configure security policies

- configure centralized policy management by using Microsoft Azure Security Center
- configure Just in Time VM access by using Microsoft Azure Security Center

Literature	
Working with security policies	9
Manage virtual machine access using just-in-time	11
	20

2.3.3 Manage security alerts

- create and customize alerts
- review and respond to alerts and recommendations
- configure a playbook for a security event by using Microsoft Azure Security Center
- investigate escalated security incidents

Literature	
Manage and respond to security alerts in Azure Security Center	2
Security recommendations in Azure Security Center	2
Security Playbook in Azure Security Center (Preview)	3
Security alerts investigation	5
	12

2.4 Secure data and applications (30-35%)

2.4.1 Configure security policies to manage data

- configure data classification
- configure data retention
- configure data sovereignty

Literature	
Tutorial: Configure Azure Information Protection policy settings that work together	8
Setting a Storage Analytics data retention policy	2
Retention policy	2
Sample - Allowed region locations	5
	17

2.4.2 Configure security for data infrastructure

- enable database authentication
- enable database auditing
- configure Microsoft Azure SQL Database threat detection
- configure access control for storage accounts
- configure key management for storage accounts
- create and manage Shared Access Signatures (SAS)
- configure security
  - HDInsights
  - Cosmos DB
  - Microsoft Azure Data Lake

Literature	
Use Azure Active Directory Authentication for authentication with SQL	9
Get started with SQL database auditing	12
Azure SQL Database Advanced Threat Protection for single or pooled databases	2
Azure Storage security guide	44
Configure customer-managed keys for Azure Storage encryption from the Azure portal	2
Grant limited access to Azure Storage resources using shared access signatures (SAS)	11
Enterprise Security Package configurations with Azure Active Directory Domain Services in HDInsight	7
Security in Azure Cosmos DB - overview	7
Virtual network integration for Azure Data Lake Storage Gen1	6
	100

2.4.3 Configure encryption for data at rest

- implement Microsoft Azure SQL Database Always Encrypted
- implement encryption
  - database

  - Storage Service
  - disk
  - backup

Literature	
Always Encrypted: Protect sensitive data and store encryption keys in the Windows certificate store	12
Transparent Data Encryption (TDE)	11
Azure Storage encryption for data at rest	8
Azure Disk Encryption for virtual machines and virtual machine scale sets	2
Azure Backup - Frequently asked questions	8
	41

2.4.4 Implement security for application delivery

- implement security validations for application development
- configure synthetic security transactions

Literature	
Securing PaaS deployments	12
Unified cross-component transaction diagnostics	4
	16

2.4.5 Configure application security

- configure SSL/TLS certs
- configure Microsoft Azure services to protect web apps
- create an application security baseline

Literature	
Tutorial: Upload and bind SSL certificates to Azure App Service	9
Configure App Service with Application Gateway	5
Securing PaaS deployments	12
	26

2.4.6 Configure and manage Key Vault

- manage access to Key Vault
- manage permissions to secrets, certificates, and keys
- manage certificates
- manage secrets
- configure key rotation

Literature	
Secure access to a key vault	13
About keys, secrets, and certificates	26
Set up Azure Key Vault with key rotation and auditing	14
	53

3 Extended notes

3.1 Manage identity and access

3.1.1 Application management : authorisation

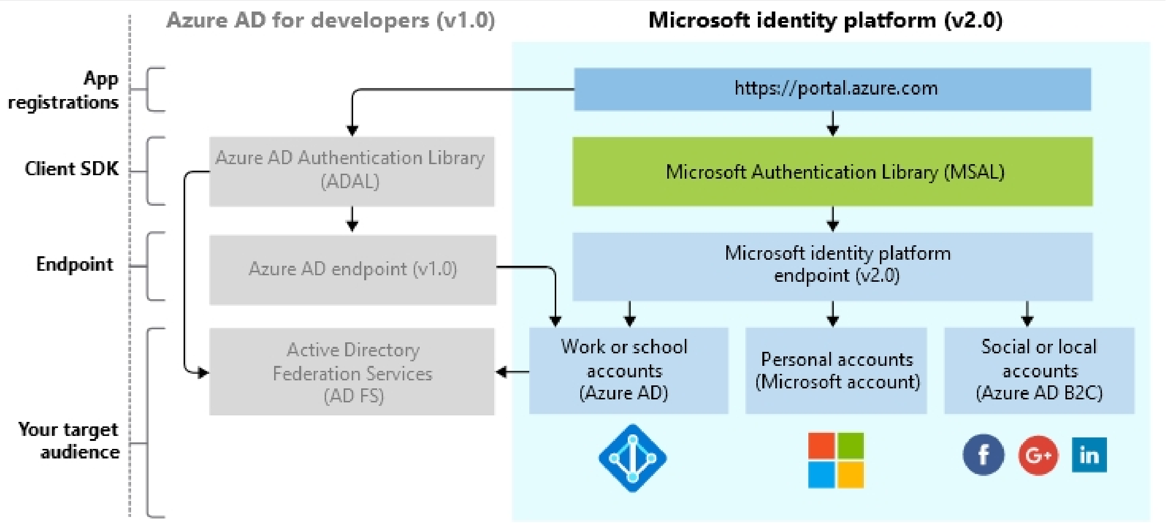

Azure AD for developers (v1.0)
Microsoft identity platform (v2.0)
App registrations
Client SDK
Endpoint
Your target audience
https://portal.azure.com
Azure AD Authentication Library (ADAL)
Microsoft Authentication Library (MSAL)
Azure AD endpoint (v1.0)
Microsoft identity platform endpoint (v2.0)
Active Directory Federation Services (AD FS)
Work or school accounts (Azure AD)
Personal accounts (Microsoft account)
Social or local accounts (Azure AD B2C)

Figure 1: Microsoft identity platform

Permission / scope
Azure AD defines two kinds of permissions:

- Delegated. Applications with signed in users. Can be either user or admin consent. The application is granted permission to act as the singed-in user when making requests.
  Effective permissions are the *least* privileged intersection of the delegated permissions for the application itself (through consent) and the privileges of the signed-in user. Within organizations, the privileges of the signed-in user may be determined by policy or by group membership.
- Application. Applications without signed in users. Can only be granted by administrator or the user which is stated as owner of the resource application.
  Effective permissions is the full set of privileges granted by the permission.

Effective permissions are the permissions that your app will have when making requests to an API.

Consent
Applications in Azure AD rely on consent in order to gain access to necessary resources or APIs.

- Static user. All required permissions are pre-specified in the app's configuration in Azure portal.
- Dynamic user. Additional permissions can be obtained when using the application. Users are prompted for additional permissions as required.
- Admin user. Required for specific high-privilege permissions. Must be granted ahead of time, cannot be dynamic.

Trivia and quirks

1. Microsoft identity platform is an evolution of the Azure Active Directory developer platform
2. Preview versions of MSAL libraries have the same level of support as production versions of MSAL and ADAL.

3. Microsoft identity platform (v2.0) endpoint is now OIDC certified

3.1.2 Application management : authentication

The Microsoft identity platform (v2.0) endpoint supports authentication for different kinds of modern application architectures based on either the OAuth 2.0 or OpenID Connect protocols.
Supported platforms and languages

1. JavaScript
2. .NET Framework
3. .NET Core
4. Windows 10/UWP
5. Xamarin.iOS
6. Xamarin.Android
7. Native iOS
8. macOS
9. Native Android
10. Java
11. Python

Note that some application types aren't available on every platform.

Scenario	Windows	Linux	Mac	iOS	Android
Single-page app	MSAL.js	MSAL.js	MSAL.js	MSAL.js	MSAL.js
Web App, users	ASP.NET Core	ASP.NET Core	ASP.NET Core		
Web App, web APIs	ASP.NET Core + MSAL.NET MSAL Java Flask + MSAL Python	ASP.NET Core + MSAL.NET MSAL Java Flask + MSAL Python	ASP.NET Core + MSAL.NET MSAL Java Flask + MSAL Python		
Desktop app	MSAL Java MSAL Python	MSAL.NET MSAL Java MSAL Python	MSAL.NET MSAL Java MSAL Python MSAL.objc	MSAL.NET	
Mobile app	MSAL.NET			MSAL.objc	MSAL.Android
Daemon app	MSAL.NET MSAL Java MSAL Python	MSAL.NET MSAL Java MSAL Python	MSAL.NET MSAL Java MSAL Python		

3.1.3 User management

When using groups for managing the following methods should be considered:

Self-service group management. When Azure AD groups are managed by group owners instead of IT administrators.

Dynamic group membership. When a series of rules govern membership in Azure AD groups, by automatically add or remove user accounts.

1. If a new user account matches all the rules for the group, it becomes a member.
2. If a user account isn't a member of the group, but its attributes change so that it matches all the rules for the group, it becomes a member of that group.
3. If a user account is a member of the group, but its attributes change so that it no longer matches all the rules for the group, it is removed as a member of the group.

Group-based licensing. Automating the assigning, and removal, of licenses based on group membership.

Trivia and quirks

1. Self-service group management is available only for Azure AD security and Office 365 groups. *It is not available for mail-enabled groups, distribution lists, or any group that has been synchronized from your on-premises Active Directory Domain Services (AD DS).*

3.1.4 Conditional Access

Application and enforcement

1. All policies that apply must be satisfied.
2. Phase 1 : All policies are evaluated and all access controls that aren't satisfied are collected.
3. Phase 2 : Prompted to satisfy the requirements you haven't met *in order*.
   (a) Multi-factor authentication
   (b) Compliant device
   (c) Hybrid Azure AD joined device
   (d) Approved client app

The Conditional Access framework provides you with a great configuration flexibility. However, great flexibility also means that you should carefully review each configuration policy before releasing it to avoid undesirable results.

When new policies are ready for your environment, deploy them in phases:

1. Apply a policy to a small set of users and verify it behaves as expected.
2. When you expand a policy to include more users. Continue to exclude all administrators from the policy to ensure that they still have access and can update a policy if a change is required.
3. Apply a policy to all users only if necessary.

- As a first step, you should evaluate your policy using the what if tool.
- Create a user account that is:
  - Dedicated to policy administration
  - Excluded from all your policies

3.1.5 Identity protection

Identity Protection seeks to accomplish three key tasks:

1. Automate the detection and remediation of identity-based risks.
2. Investigate risks using data in the portal.
3. Export risk detection data to third-party utilities for further analysis.

Risk detection
Risk detections in Azure AD Identity Protection include any identified suspicious actions related to user accounts in the directory.

- User
  - Leaked Credentials. *This risk detection indicates that the user’s valid credentials have been leaked.*
  - Azure AD threat intelligence. *Microsoft’s internal and external threat intelligence sources have identified a known attack pattern.*
- Sign-in
  - Atypical travel. *Sign in from an atypical location based on the user’s recent sign-ins.*
  - Anonymous IP address. *Sign in from an anonymous IP address (for example: Tor browser, anonymizer VPNs).*
  - Unfamiliar sign-in properties. *Sign in with properties we‘ve not seen recently for the given user.*
  - Malware linked IP address. *Sign in from a malware linked IP address.*
  - Admin confirmed user compromised. *This detection indicates an admin has selected ’Confirm user compromised’ in the Risky users UI or using riskyUsers API.*
  - Malicious IP address. *This detection indicates sign-in from a malicious IP address. An IP address is considered malicious based on high failure rates because of invalid credentials received from the IP address or other IP reputation sources.*

Investigating risk

- Risky users

  Information
  - Users at risk
  - Details about detections
  - History of risky sign-ins
  - Risk history

  Actions
  - Reset the user password
  - Confirm user compromise
  - Dismiss user risk
  - Block user from signing in
  - Investigate further using Azure ATP

- Risky sign-ins. *The risky sign-ins report contains data for up to the past 30 days.*

Information

- Sign-ins indicating risk
- Real-time and aggregate risk levels associated with sign-in attempts
- Detection types triggered
- Conditional Access policies applied
- MFA details
- Device information
- Application information
- Location information

Actions

- Confirm sign-in compromise
- Confirm sign-in safe

- Risk detections

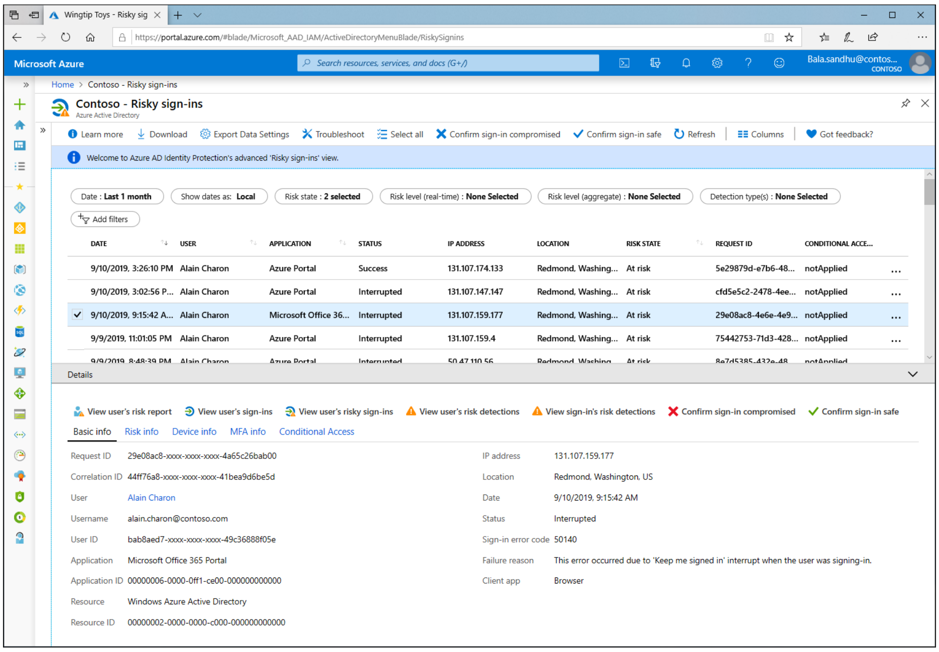
Information

- Information about each risk detection including type
- Other risks triggered at the same time
- Sign-in attempt location
- Link out to more detail from Microsoft Cloud App Security (MCAS)

Actions

- Return to either user risk or sign-in report and take action there

The three reports are found in the Azure portal > Azure Active Directory > Security.



Welcome to Azure AD Identity Protection's advanced 'Risky sign-ins' view.

Date : **Last 1 month** | Show dates as: **Local** | Risk state : **2 selected** | Risk level (real-time) : **None Selected** | Risk level (aggregate) : **None Selected** | Detection type(s) : **None Selected**

	DATE	USER	APPLICATION	STATUS	IP ADDRESS	LOCATION	RISK STATE	REQUEST ID	CONDITIONAL ACCE...	
	9/10/2019, 3:26:10 PM	Alain Charon	Azure Portal	Success	131.107.174.133	Redmond, Washing...	At risk	5e29879d-e7b6-48...	notApplied	...
	9/10/2019, 3:02:56 P...	Alain Charon	Azure Portal	Interrupted	131.107.147.147	Redmond, Washing...	At risk	cfd5e5c2-2478-4ee...	notApplied	...
✓	9/10/2019, 9:15:42 A...	Alain Charon	Microsoft Office 36...	Interrupted	131.107.159.177	Redmond, Washing...	At risk	29e08ac8-4e6e-4e9...	notApplied	...
	9/9/2019, 11:01:05 PM	Alain Charon	Azure Portal	Interrupted	131.107.159.4	Redmond, Washing...	At risk	75442753-71d3-428...	notApplied	...
	9/9/2019, 8:48:39 PM	Alain Charon	Azure Portal	Interrupted	50.47.110.56	Redmond, Washing...	At risk	8e7d5385-432e-48	notApplied	

Request ID	29e08ac8-xxxx-xxxx-xxxx-4a65c26bab00	IP address	131.107.159.177
Correlation ID	44ff76a8-xxxx-xxxx-xxxx-41bea9d6be5d	Location	Redmond, Washington, US
User	Alain Charon	Date	9/10/2019, 9:15:42 AM
Username	alain.charon@contoso.com	Status	Interrupted
User ID	bab8aed7-xxxx-xxxx-xxxx-49c36888f05e	Sign-in error code	50140
Application	Microsoft Office 365 Portal	Failure reason	This error occurred due to 'Keep me signed in' interrupt when the user was signing-in.
Application ID	00000006-0000-0ff1-ce00-000000000000	Client app	Browser
Resource	Windows Azure Active Directory		
Resource ID	00000002-0000-0000-c000-000000000000		

Figure 2: Identify protection risky sign-ins report

Remediation

1. Technical tools

   (a) Azure Multi-Factor Authentication

   (b) Reset their password using self-service password reset

   (c) Blocking until an administrator takes action

2. Policies
    (a) MFA registration policy. *Can help organizations roll out MFA using a Conditional Access policy requiring registration at sign-in.*
    (b) Sign-in risk policy. *Analyzes signals from each sign-in, both real-time and offline, and calculates a risk score based on the probability that the sign-in wasn't performed by the user. If risk is detected, users can perform multi-factor authentication to self-remediate and close the risky sign-in event to prevent unnecessary noise.*
    (c) User risk policy. *Calculate what it believes is normal for a user's behaviour and use that to base decisions for their risk. If risk is detected, users can perform self-service password reset to self-remediate and close the user risk event to prevent unnecessary noise.*

License requirements

		Premium P2	Premium P1	Basic/Free
Risk policies	User risk policy	✓	✗	✗
Risk policies	Sign-in risk policy	✓	✗	✗
Security reports	Overview	✓	✗	✗
Security reports	Risky users	✓	Limited	Limited
Security reports	Risky sign-ins	✓	Limited	Limited
Security reports	Risk detections	✓	Limited	✗
Notifications	Users at risk detected alerts	✓	✗	✗
Notifications	Weekly digest	✓	✗	✗
	MFA registration policy	✓	✗	✗

Users role with Identity Protection access

1. Security Reader
2. Security Operator
3. Security Administrator
4. Global Reader
5. Global Administrator

3.1.6 Azure AD Connect

Wizards

- Express. Requires high level of privileges and does not require creating users or configuring permissions. Requires two accounts a) AD DS Enterprise Administrator and b) Azure AD Global Administrator.
- Custom. It is used in all cases where the express installation option does not satisfy your deployment or topology.

Accounts

- Synchronisation
    - AD DS Connector account:
      Used to read/write information to Windows Server Active Directory.
    - ADSync service account:
      Used to run the synchronization service and access the SQL database.

  - Azure AD Connector account:
    Used to write information to Azure AD.

- Installation
  - Local Administrator account:
    The administrator who is installing Azure AD Connect and who has local Administrator permissions on the machine.
  - AD DS Enterprise Administrator account:
    Optionally used to create the "AD DS Connector account" above.
  - Azure AD Global Administrator account:
    Used to create the Azure AD Connector account and configure Azure AD.
    After installation this account should be changed from Global Administrator role to the *Directory Synchronization Accounts* role.
  - SQL SA account (optional):
    Used to create the ADSync database when using the full version of SQL Server. This account could be the same account as the Enterprise Administrator.

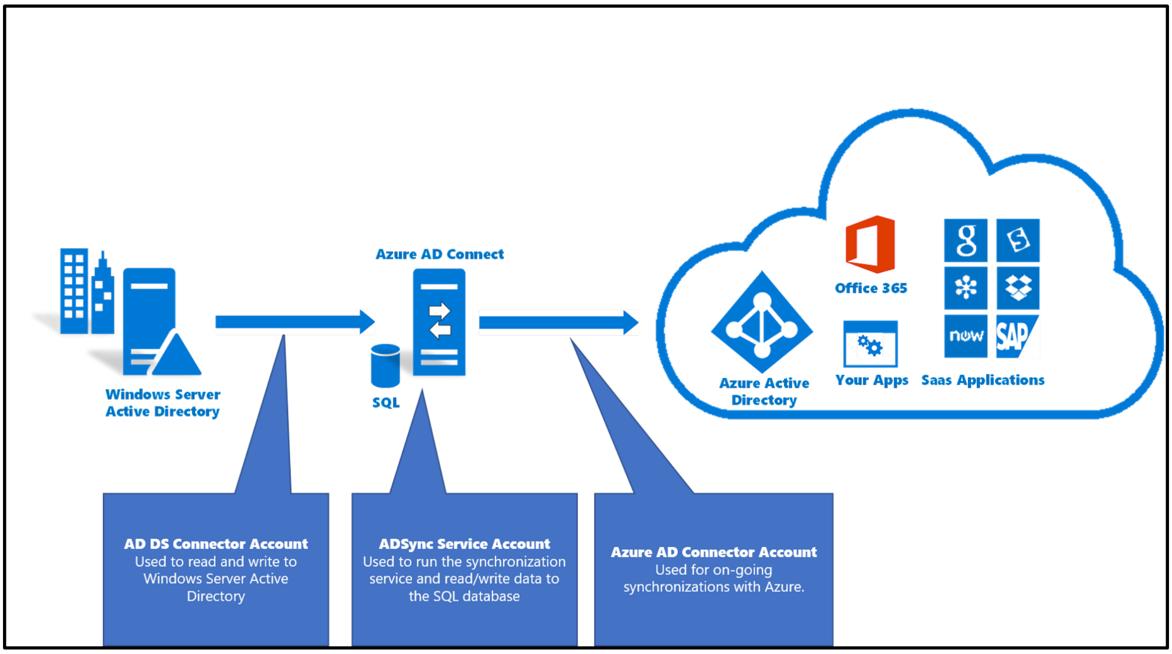

Azure AD Connect
Windows Server Active Directory
SQL
Office 365
Azure Active Directory
Your Apps
Saas Applications
AD DS Connector Account
Used to read and write to Windows Server Active Directory
ADSync Service Account
Used to run the synchronization service and read/write data to the SQL database
Azure AD Connector Account
Used for on-going synchronizations with Azure.

Figure 3: Accounts used for Azure AD Connect

Components

- SQL Server 2012 Express, LocalDB instance
- User sign-in scheme
  - Password Hash Sync. *The users passwords are synchronized to Azure AD as a password hash and authentication occurs in the cloud.*
  - Pass-through Authentication. *The users password is passed through to the on-premises Active Directory domain controller to be validated.*
  - Federation with AD FS. *The users are redirected to their on-premises AD FS instance to sign in and authentication occurs on-premises.*

  - Federation with PingFederate. *The users are redirected to their on-premises PingFederate instance to sign in and authentication occurs on-premises.*
  - Do not configure. *No user sign-in feature is installed and configured. Choose this option if you already have a 3rd party federation server or another existing solution in place.*

Option Enable Single Sign on. *Provides a single sign on experience for desktop users on the corporate network. For Hash or Pass-through.*

3.1.7 Privileged identity management

Privileged identity management seeks to accomplish:

- Integrated access reviews
- Manage risk : least privilege access
  - Just-in-time access
  - Request approval workflows
- Address compliance and governance
- Prevention of malicious activities in real time

Setup

1. Sign in. *As global administrator.*
2. Navigate to PIM service. *Click All services and find the Azure AD Privileged Identity Management service.*
3. Setup MFA for account. *If not already done.*
4. Consent to PIM. *Automatically assigned the Security Administrator and Privileged Role Administrator roles.*
5. Verify identify. *With MFA.*

Deployment

1. Identify stakeholders
2. Enable Privileged Identity Management
3. Enforce principle of least privilege
   (a) Understand the granularity of the roles
   (b) List who has privileged roles in your organization
   (c) Reduce the amount of Global Administrators. *Consider automating with acess review.*
   (d) Reduce other administrators. *Consider automating with acess review.*
4. Decide which role assignments should be protected by Privileged Identity Management
   (a) Should be atleast Global Administrators and Security Administrators
   (b) All guest users
   (c) Owner roles and User Access Administrator roles of all subscriptions/resources
5. Decide which role assignments should be permanent or eligible

    (a) Two break-glass emergency access accounts

6. Draft your Privileged Identity Management settings

1. Use Privileged Identity Management alerts to safeguard your privileged access
2. Set up recurring access reviews to regularly audit your organization's privileged identities
    (a) Quarterly access reviews for all your Azure AD and Azure resource roles

    (b) Secondary email address for all accounts with privileged role assignments that are not linked to a regularly checked email address
3. Get the most out of your audit log to improve security and compliance
    (a) Read all audit events on a weekly basis and export your audit events on a monthly basis

    (b) Use Azure log monitoring to archive audit events in an Azure storage account for the need of security and compliance

Features

Tasks	
My roles	List of eligible[1] and active roles assigned to you.
My requests	Pending requests to activate eligible role assignments.
Approve requests	Requests to activate eligible roles, that you are designated to approve.
Review access	Active access reviews you are assigned to complete, whether you're reviewing access for yourself or someone else.
Manage	
Azure AD roles	Dashboard and settings to manage Azure AD role assignments. *Only for privileged role administrators.*
Azure resources	Dashboard and settings to manage Azure resource role assignments. *Only for privileged role administrators.*

Restrictions

Privileged Identity Management does not allow the management for all roles. Specifically some classic subscription administrator roles and some Exchange and Sharepoint roles.

- Account Administrator
- Service Administrator
- Co-Administrator
- Exchange Online roles
- SharePoint Online roles

Exchange Administrator and SharePoint Administrator are available, but can experience delays.

Depending on the Privileged Identity Management settings configured for the role, the user must complete certain steps (such as performing multi-factor authentication, getting approval, or specifying a reason.)

License requirements

- Azure AD Premium P2
- Enterprise Mobility + Security (EMS) E5
- Microsoft 365 M5

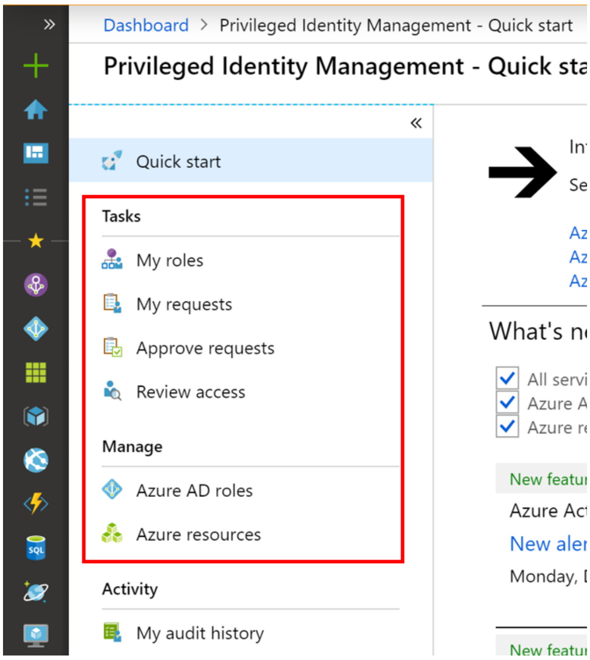


Figure 4: Privileged Identity Management - Quick start

User roles with Privileged Identity Management access Each administrator or user who interacts with or receives a benefit from Privileged Identity Management must have a license. Examples include:

- Administrators
  - with Azure AD roles managed using PIM
  - Azure resource roles managed using PIM
  - assigned to the Privileged Role Administrator role
- Users
  - assigned as eligible to Azure AD roles managed using PIM
  - able to approve/reject requests in PIM
  - assigned to an Azure resource role with just-in-time or direct (time-based) assignments
  - assigned to an access review
  - who perform access reviews

Trivia and quirks

1. First person to use Privileged Identity Management in your directory, is automatically assigned the Security Administrator and Privileged Role Administrator roles
2. Only *organizational* accounts, with Global Administrator role, can enable Privileged Identity Management for a directory

3.1.8 Azure Active Directory Graph API

In the process of deprecation in favor of Microsoft Graph API.
Applications can use Azure AD Graph API to perform create, read, update, and delete (CRUD) op-

erations on directory data and objects.

1. Create a new user in a directory
2. Get a user's detailed properties, such as their groups
3. Update a user's properties, such as their location and phone number, or change their password
4. Check a user's group membership for role-based access
5. Disable a user's account or delete it entirely

Additionally, you can perform similar operations on other objects such as groups and applications.

Features

1. REST API Endpoints.
2. Authentication with Azure AD.
3. Role-Based Authorization (RBAC). *Security groups are used to perform RBAC in Azure AD Graph API. For example, if you want to determine whether a user has access to a specific resource.*
4. Differential Query. *Differential query allows you to track changes in a directory between two time periods without having to make frequent queries to Azure AD Graph API.*
5. Directory Extensions. *You can add custom properties to directory objects without requiring an external data store.*
6. Secured by permission scopes. *Delegated and application.*

3.1.9 Access review

3.1.10 Azure Tenants

Transferring subscriptions
It is possible to transfer a subscription to another tenant, this will remove all role-based access control (RBAC) assignments to manage resources in the original subscription. It is also possible to transfer just the billing ownership of an account, without moving the subscription to the new accounts tenant - this is done by unchecking the box for Subscription Azure AD.

External developer account
It is possible to enable access to the developer portal for users from Azure Active Directory (Azure AD). This is intended to provide access for external developers and this feature is available in the Premium, Standard and Developer tiers of API Management.

3.2 Implement platform protection

3.2.1 Implement network security

Azure Virtual Network
Design best practices:

1. Minimise conflicts. *Ensure non-overlapping address spaces. The VNet address space (CIDR block) should not overlap with your organization's other network ranges.*
2. Keep a reserve space. *Reserve some of the address space of the VNet.*
3. Minimise management overhead. *Create a few large VNets, rather than multiple small VNets.*
4. Secure it. *Secure your VNet using Network Security Groups (NSGs).*

Communication:
All resources in a VNet can communicate outbound to the internet, by default. You can communicate inbound to a resource by assigning a public IP address or a public Load Balancer. When using only an internal Standard Load Balancer, outbound connectivity is not available until you define how you want outbound connections to work with an instance-level public IP or a public Load Balancer.

The communication options of Azure resources are:

- Virtual network: *Deploy VMs, and other Azure resources to a virtual network, such as Azure App Service Environments, the Azure Kubernetes Service (AKS), or Azure Virtual Machine Scale Sets.*
- Through a virtual network service endpoint: *Extend your virtual network private address space and the identity of your virtual network to Azure service resources, such as Azure Storage accounts and Azure SQL databases, over a direct connection. Service endpoints allow you to secure your critical Azure service resources to only a virtual network.*
- VNet Peering: *Connect virtual networks to each other, enabling resources in either virtual network to communicate with each other, using virtual network peering. The virtual networks you connect can be in the same, or different, Azure regions.*

The communication options for on-premise resources are:

- Point-to-site virtual private network (VPN): *Established between a virtual network and a single computer in your network. Each computer must configure an individual connection. Intended for developers, as it requires few adjustments to existing network. The communication is encrypted.*
- Site-to-site VPN: *Established between on-premises VPN device and an Azure VPN Gateway in a virtual network. This connection type enables any on-premises resource that you authorize to access a virtual network. The communication is encrypted.*
- Azure ExpressRoute: *Established between your network and Azure, through an ExpressRoute partner. This connection is private. Traffic does not go over the internet.* This is not encrypted by default.

You can filter network traffic between subnets using either or both of the following options:

- Security groups: *Network security groups and application security groups can contain multiple inbound and outbound security rules that enable you to filter traffic to and from resources by source and destination IP address, port, and protocol.*

- Network virtual appliances:*A network virtual appliance is a VM that performs a network function, such as a firewall, WAN optimization, or other network function.*

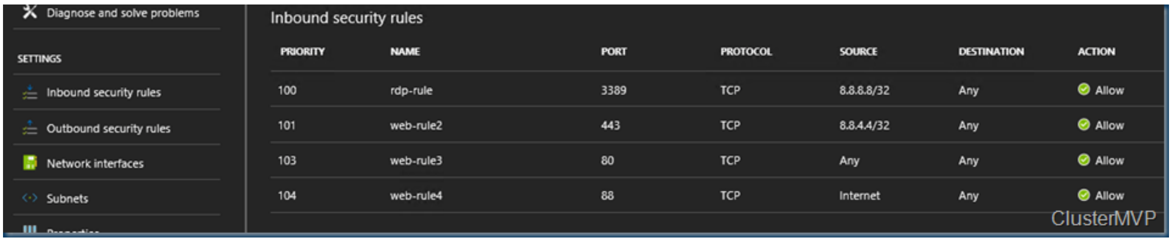
Azure routes traffic between subnets, connected virtual networks, on-premises networks, and the Internet, by default. You can implement either or both of the following options to override the default routes Azure creates:

- Route tables: *Custom route tables with routes that control where traffic is routed to for each subnet.*

- Border gateway protocol (BGP) routes: *Connect the virtual network to the on-premises network using an Azure VPN Gateway or ExpressRoute connection, you can propagate your on-premises BGP routes to your virtual networks.*

Network Security Groups
Security rules in network security groups enable you to filter the type of network traffic that can flow in and out of virtual network subnets and network interfaces.

A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager). When an NSG is associated to a subnet, the rules apply to all resources connected to the subnet. Traffic can further be restricted by also associating an NSG to a VM or NIC.



Inbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	rdp-rule	3389	TCP	8.8.8.8/32	Any	✓ Allow
101	web-rule2	443	TCP	8.8.4.4/32	Any	✓ Allow
103	web-rule3	80	TCP	Any	Any	✓ Allow
104	web-rule4	88	TCP	Internet	Any	✓ Allow

Figure 5: List of inbound security rules

Application Security Groups
Feature for security micro-segmentation for your virtual networks in Azure.

Network segmentation. Centralized on applications, instead of explicit IP addresses. Implementing granular security traffic controls improves isolation of workloads and protects them individually.

Filtering traffic based on applications patterns

- Define your application groups

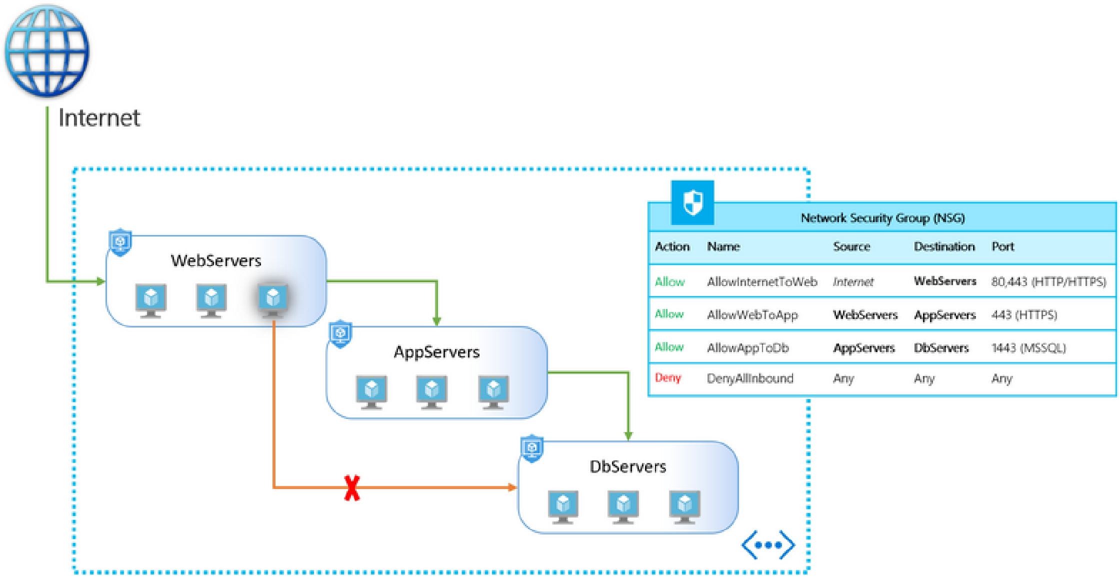
- Define a single collection of rules using ASGs and Network Security Groups (NSG)

- Scale at your own pace. When you deploy VMs, make them members of the appropriate ASGs. *Implement a zero-trust model, limiting access to the application flows that are explicitly permitted.*

Firewall
Outbound network access controls:

- Application rules that define fully qualified domain names (FQDNs) that can be accessed from a subnet.

- Network rules that define source address, protocol, destination port, and destination address.



Network Security Group (NSG)

Action	Name	Source	Destination	Port
Allow	AllowInternetToWeb	*Internet*	**WebServers**	80,443 (HTTP/HTTPS)
Allow	AllowWebToApp	**WebServers**	**AppServers**	443 (HTTPS)
Allow	AllowAppToDb	**AppServers**	**DbServers**	1443 (MSSQL)
Deny	DenyAllInbound	Any	Any	Any

Figure 6: Application Security Groups (ASG) in all Azure regions

3.2.2 Security management

For more secure management and operations, you can minimize a client's attack surface by reducing the number of possible entry points. This can be done through security principles: "separation of duties" and "segregation of environments."

- Isolate sensitive functions *from one another to decrease the likelihood that a mistake at one level leads to a breach in another. I.e. do not perform tasks such as browsing or email on secured workstations.*
- Reduce the system's attack surface by removing unnecessary software *i.e. email client and productivity applications.*
- Secure management workstations. *Client systems that have administrator access to infrastructure components should be subjected to the strictest possible policy to reduce security risks.*
  - Security policies > Group Policy > Deny open Internet access
  - Use Internet Protocol security (IPsec) VPNs if direct access is needed
  - Separate management and development Active Directory domains
  - Isolate and filter management workstation network traffic
  - Antimalware software
  - Multi-factor authentication

Security mechanisms
Azure provides security mechanisms to aid administrators who manage Azure cloud services and virtual machines. These mechanisms include:

- Authentication and role-based access control.
- Monitoring, logging, and auditing.
- Certificates and encrypted communications.

- A web management portal.
- Network packet filtering.

Hardened workstation

- Active scanning and patching.
- Limited functionality.
- Network hardening. *Use Windows Firewall rules to allow only valid IP addresses, ports, and URLs related to Azure management. Ensure that inbound remote connections to the workstation are also blocked.*
- Execution restriction. *Allow only a set of predefined executable files that are needed for management to run (referred to as "default-deny").*
- Least privilege. *Management workstation users should not have any administrative privileges on the local machine itself.*

You can enforce all this by using Group Policy Objects (GPOs) in Active Directory Domain Services (AD DS) and applying them through your (local) management domain to all management accounts.

- IE hardening. *Review your client policies and enforce running in protected mode, disabling add-ons, disabling file downloads, and using Microsoft SmartScreen filtering. Ensure that security warnings are displayed. Take advantage of Internet zones and create a list of trusted sites for which you have configured reasonable hardening. Block all other sites and in-browser code, such as ActiveX and Java.*
- Standard user. *Running as a standard user brings a number of benefits, the biggest of which is that stealing administrator credentials via malware becomes more difficult. In addition, a standard user account does not have elevated privileges on the root operating system, and many configuration options and APIs are locked out by default.*
- AppLocker. *Use AppLocker to restrict the programs and scripts that users can run. You can run AppLocker in audit or enforcement mode. By default, AppLocker has an allow rule that enables users who have an admin token to run all code on the client.*
- Code signing. *Code signing all tools and scripts used by administrators provides a manageable mechanism for deploying application lockdown policies. Hashes do not scale with rapid changes to the code, and file paths do not provide a high level of security. You should combine AppLocker rules with a PowerShell execution policy that only allows specific signed code and scripts to be executed.*
- Group Policy. *Create a global administrative policy that is applied to any domain workstation that is used for management (and block access from all others), and to user accounts authenticated on those workstations.*
- Security-enhanced provisioning. *Safeguard your baseline hardened workstation image to help protect against tampering. Use security measures like encryption and isolation to store images, virtual machines, and scripts, and restrict access (consider using an auditable check-in/check-out process).*
- Patching.
- Encryption. *Make sure that management workstations have a Trusted Platform Module*

- Governance. Use *AD DS GPOs to control all the administrators' Windows interfaces, such as file sharing. Include management workstations in auditing, monitoring, and logging processes. Track all administrator and developer access and usage.*

Best practices

Do	**Don't**
Maintain confidentiality by delivering account names and passwords directly, perform a remote installation of client/server certificates (via an encrypted session), download from a protected network share, or distribute by hand via removable media.	Don't email credentials for administrator access or other secrets (for example, SSL or management certificates)
Proactively manage certificate life cycles.	
Establish security management principles and system hardening policies. Apply them to your development environments.	Don't store account passwords unencrypted or un-hashed.
Use Enhanced Mitigation Experience Toolkit 5.5 certificate pinning rules to ensure proper access to Azure SSL/TLS sites.	
Create a dedicated Microsoft account to manage your Azure subscription	Don't share accounts and passwords between administrators, or reuse passwords across multiple user accounts or services, particularly those for social media or other non-administrative activities.
Configuration files and profiles should be installed from a trusted source.	Don't email configuration files.
Enforce strong password policies, expiration cycles (changeon-first-use), console timeouts, and automatic account lockouts. Use a client password management system with multi-factor authentication for password vault access.	Don't use weak or simple logon passwords.
Lock down Azure ports and IP addresses to restrict management access.	Don't expose management ports to the Internet.
Use firewalls, VPNs, and NAP for all management connections.	

Azure Storage firewalls

Azure Storage provides a layered security model. This model enables you to secure and control the level of access to your storage accounts that your applications and enterprise environments demand, based on the type and subset of networks used. When network rules are configured, only applications requesting data over the specified set of networks can access a storage account. You can limit access to your storage account to requests originating from specified IP addresses, IP ranges or from a list of subnets in an Azure Virtual Network (VNet).

An application that accesses a storage account when network rules are in effect still requires proper authorization for the request. Authorization is supported with Azure Active Directory (Azure AD) credentials for blobs and queues, with a valid account access key, or with an SAS token.

Turning on firewall rules for your storage account blocks incoming requests for data by default, unless the requests originate from a service operating within an Azure Virtual Network (VNet) or from allowed public IP addresses. Requests that are blocked include those from other Azure services, from the Azure portal, from logging and metrics services, and so on.

You can grant access to Azure services that operate from within a VNet by allowing traffic from the subnet hosting the service instance. You can also enable a limited number of scenarios through the Exceptions mechanism.

Appendix A Glossary

A.1 Acronyms

MCAS Microsoft Cloud App Security

NSG Network Security Group

LOB Line-of-business (application)

OIDC OpenID Connect

PIM Privileged identity management

RBAC Role-Based Access Control

SIEM Security information and event management

Appendix B Quiz

B.1 Manage identity and access

As an enterprise or software-as-a-service (SaaS) developer you which to build an application which allows users to sign in using their Personal Microsoft accounts. Which Microsoft Identity platform library provides authentication tools for Personal Microsoft accounts?

□ Microsoft Authentication Library (MSAL)

□ Azure AD Authentication Library (ADAL)

□ .NET DotNetOpenAuth (OAuth)

□ Microsoft Active Directory Library (MADL)

An application which allows users to update their contact information, is created utilising the delegated permission scheme. Can the current user signed in, Bob from HR, update the contact information of his colleague Alice, using the application? *The application has the User.ReadWrite.All delegated permission in Microsoft Graph.*

□ Yes. The effective permissions granted by the application allows signed-in user the ability to update all users.

□ No. The effective permissions granted by the application does not allow signed-in user the ability to update all users.

As part of a merger is is necessary to transfer the billing ownership of several user accounts. Which of the these account types can have their billing ownership transferred.

□ Azure in Open (AIO)

□ Visual Studio Enterprise (MPN) subscribers

□ Visual Studio Professional

□ Microsoft Partner Network

□ Free Trial

□ Pay-As-You-Go

Create additional questions from https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-permissions-and-consent#using-the-admin-consent-endpoint

Appendix C Quiz (with answers)

C.1 Manage identity and access

As an enterprise or software-as-a-service (SaaS) developer you which to build an application which allows users to sign in using their Personal Microsoft accounts. Which Microsoft Identity platform library provides authentication tools for Personal Microsoft accounts?

☑ Microsoft Authentication Library (MSAL)

☒ Azure AD Authentication Library (ADAL)

☒ .NET DotNetOpenAuth (OAuth)

☒ Microsoft Active Directory Library (MADL)

An application which allows users to update their contact information, is created utilising the delegated permission scheme. Can the current user signed in, Bob from HR, update the contact information of his colleague Alice, using the application? *The application has the User.ReadWrite.All delegated permission in Microsoft Graph.*

☒ Yes The effective permissions granted by the application allows signed-in user the ability to update all users.

☑ No. The effective permissions for the application does not allow signed-in user the ability to update all users.

As part of a merger is is necessary to transfer the billing ownership of several user accounts. Which of the these account types can have their billing ownership transferred.

☒ Azure in Open (AIO)

☑ Visual Studio Enterprise (MPN) subscribers

☑ Visual Studio Professional

☑ Microsoft Partner Network

☒ Free Trial

☑ Pay-As-You-Go
