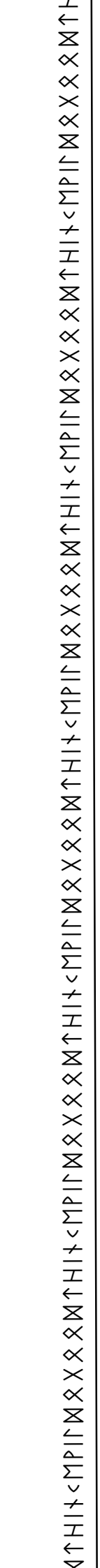

MS Azure Security Technologies

AZ-500 Certification

The Collective Conspiracy Coven of Conspicuous Insight and Contagious Brilliance

Version 1.0

November 7, 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
  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"
- 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

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
- 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

Appendix A Glossary

A.1 Acronyms

LOB Line-of-business (application)

OIDC OpenID Connect

SIEM Security information and event management

MCAS Microsoft Cloud App Security

Appendix B Extended notes

B.1 Manage identity and access

B.1.1 Application management

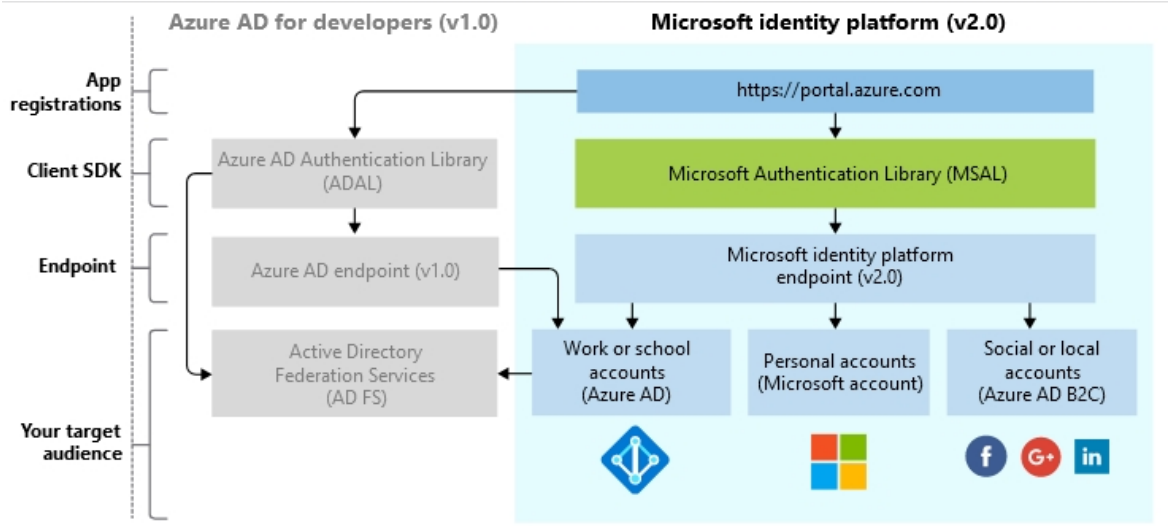

Figure 1: Microsoft identity platform

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

B.1.2 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).*

B.1.3 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.

Remediation tools

1. Azure Multi-Factor Authentication
2. Reset their password using self-service password reset

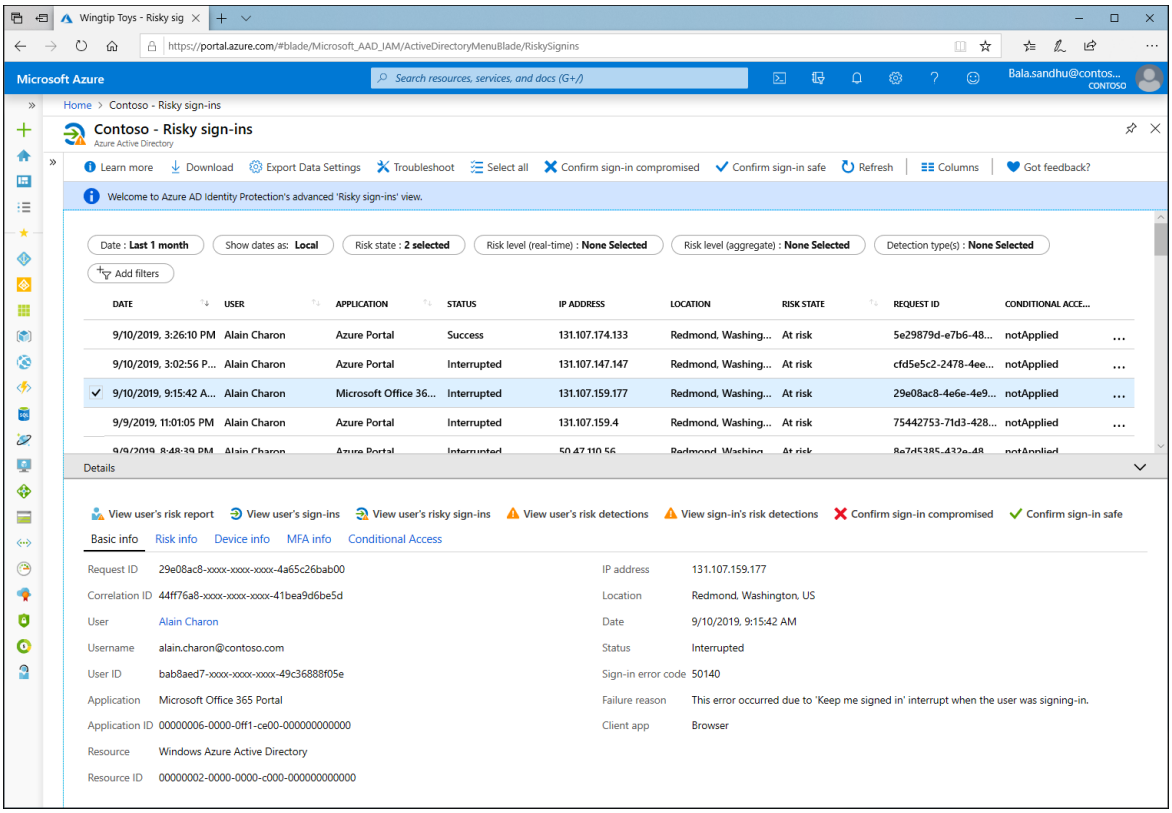

Figure 2: Identify protection risky sign-ins report

3. Blocking until an administrator takes action

Users role with Identity Protection Access

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

License requirements

		Premium P2	Premium P1	Basic/Free
Risk policies	User risk policy *Identity Protection*	✓	✗	✗
Risk policies	Sign-in risk policy *Identity Protection/Conditional Access*	✓	✗	✗
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	✓	✗	✗

B.1.4 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.

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.*

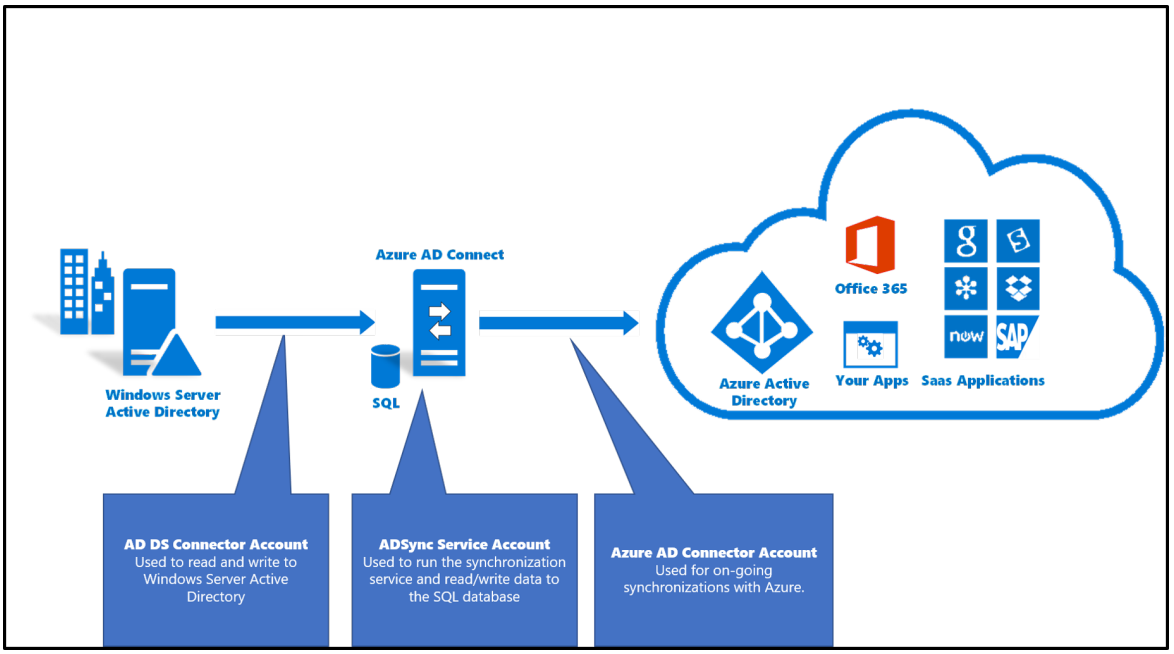

Figure 3: Accounts used for Azure AD Connect

– 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.*

Appendix C Quiz

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 granted by the application does not allow signed-in user the ability to update all users.

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

Appendix D Quiz (with answers)

D.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.