AZ-500: Microsoft Azure Security Technologies

Course Navigation

Manage Identity and Access
Section 1

Platform Protection
Section 2

Security Operations
Section 3

Secure Data and Applications
Section 4

Exam Preparation

Linux Academy

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Course Navigation

Topics in this section include:

AD Users

AAD Connect

AD Groups

Application Security:
Registration, permissions, scopes, and consent!

Authentication:
Password sync, pass-through authentication

Azure MFA

Conditional Access

Azure Active Directory Identity Protection:
Registration, permission scopes and permission consent

Users

Back to Main

Linux Academy

Active Directory Users

A **Users:**
Who are they? Why do we care?

B **Managing Users:**
What tools are available to manage users?

C **B2B:**
Opening our doors to the outside.

AAD

Groups

Active Directory Users

A user account is required to access Azure resources. This includes software as a service (SaaS) applications such as Office 365, as well as custom applications that are written by your in-house development team.

This account is also sometimes called a work or school account.

A user account can be any one of the following types:

A cloud-based user account (Azure Active Directory)
A synchronized on-premises directory account (AD -> AAD)
A guest user, also knows as a B2B collaboration guest.

Close

AAD

Groups

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Active Directory Users Management

Azure
Portal

Azure
PowerShell

Azure
CLI

Close

AAD

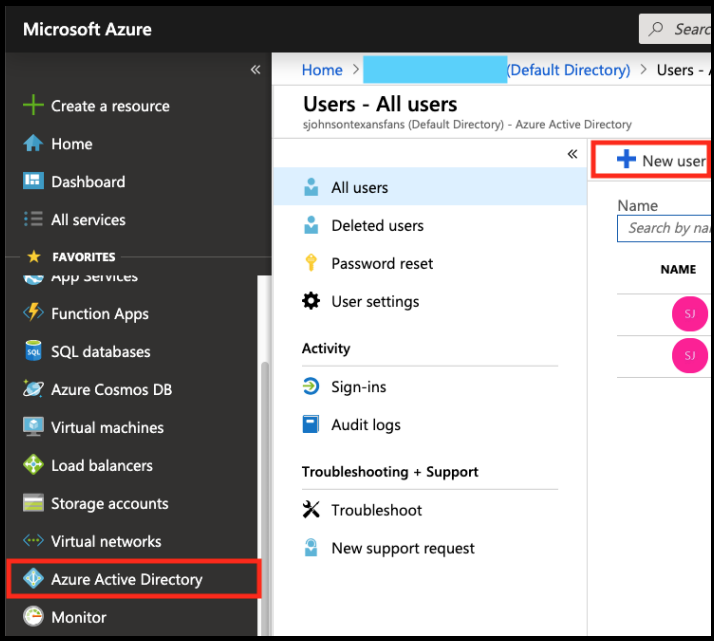
Groups

Back to Main

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Active Directory Users Management: Azure Portal



Close

AAD

Groups

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Active Directory Users Management: Azure PowerShell

```
New-AzADUser
   -DisplayName <String>
   -UserPrincipalName <String>
   -Password <SecureString>
   [-ImmutableId <String>]
   -MailNickname <String>
   [-ForceChangePasswordNextLogin]
   [-DefaultProfile
<IAzureContextContainer>]
   [-WhatIf]
   [-Confirm]
   [<CommonParameters>]
```

```
$SecureStringPassword = ConvertTo-SecureString -String
"password" -AsPlainText -Force
New-AzADUser -DisplayName "MyDisplayName"
-UserPrincipalName "myemail@domain.com" -Password
$SecureStringPassword -MailNickname "MyMailNickName"
```

Azure PS Documentation

Close

AAD

Groups

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Active Directory Users Management: Azure CLI

```
az ad user create --display-name
                  --password
                  --user-principal-name
[--force-change-password-next-login
{false, true}]
                  [--immutable-id]
                  [--mail-nickname]
                  [--subscription]
```

```
az ad user create --display-name MyDisplayName
--password 123456 --user-principal-name
myemail@domain.com --force-change-password-next-login
true
```

Azure CLI Documentation

Close

AAD

Groups

Active Directory Users

Azure B2B allows you to **invite and authorize users from outside of your organization** to access resources you specify.

These users manage their own identities through their own identity provider (such as Azure AD) or social media accounts. This means they are responsible for keeping track of their information including username and password changes. Therefore, there is **no additional administrative overhead.**

You can choose to increase security for B2B user accounts by requiring **multi-factor authentication**.

You can also create a custom API for **self-service sign-up.**

Close

AAD

Groups

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Active Directory Groups

A — **Groups:** Examining group and membership types.

B — **Managing Groups:** Reviewing tools available to manage groups.

C — **Tips and Tricks:** Providing the inside scoop.

AAD

Applications

Back to Main

Active Directory Groups

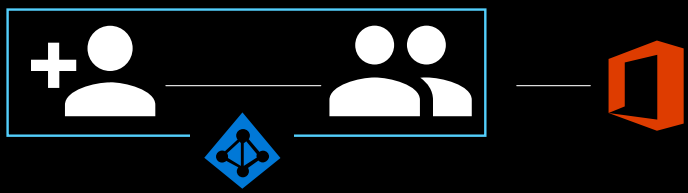
Groups are populated with user accounts and those groups can then be granted access to data or applications.

Types of groups:

- Security
- Office 365

Membership types for security groups:

- Assigned
- Dynamic User
- Dynamic Device (security groups only)



Close

AAD

Applications

Active Directory Groups

Security Groups

Used to manage member and device access to shared resources. This way you can give a set of permissions to all the members at once instead of having to individually add permissions to each member.

Close

Active Directory Groups

Office 365 Groups

Provide collaboration by giving members access to a shared mailbox, calendar, SharePoint site, files, and more.

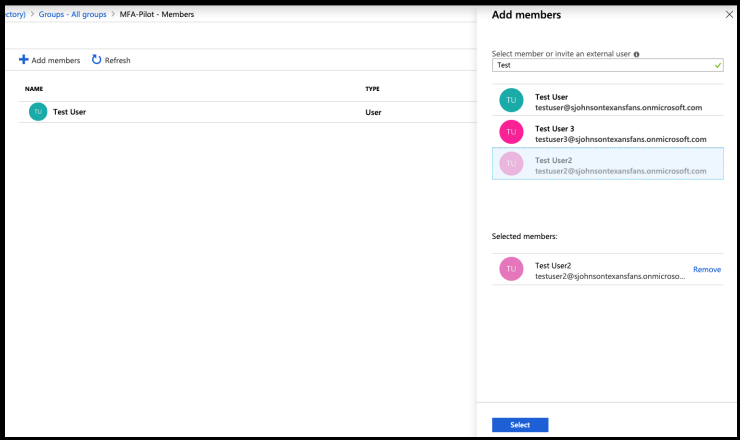
Office 365 Groups

Close

Active Directory Groups

Assigned Membership

Static in nature. The **administrator** determines group membership.



Close

AAD

Applications

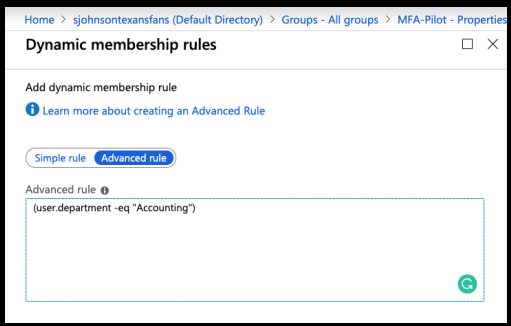
Active Directory Groups

Dynamic Membership

User and device membership based on **attribute values**.

Queries determine which attributes are used to determine group membership.

If a particular user or device account matches the query, it is **added** to the group. If the attribute changes, the account is **removed**.



Close

Active Directory Group Management

Azure
Portal

Azure
PowerShell

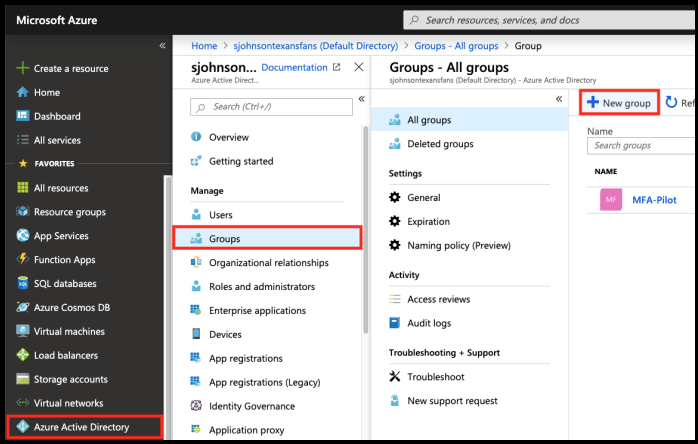
Azure
CLI

Close

AAD

Applications

Active Directory Group Management: Azure Portal



Close

AAD

Applications

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Active Directory Group Management: Azure PowerShell

```
New-AzADGroup
   -DisplayName <String>
   -MailNickname <String>
   [-DefaultProfile
<IAzureContextContainer>]
   [-WhatIf]
   [-Confirm]
   [<CommonParameters>]
```

```
New-AzADGroup -DisplayName "MyGroupDisplayName"
-MailNickname "MyGroupNick"
```

Azure PS Documentation

Close

AAD

Applications

Back to Main

Active Directory Group Management: Azure CLI

```
az ad group create --display-name
                   --mail-nickname
                   [--force {false, true}]
                   [--subscription]
```

```
az ad group create --display-name "Test Group 3"
-mail-nickname "TestGroup3"
```

Azure CLI Documentation

Close

AAD

Applications

Active Directory Groups: Tips and Tricks

When using dynamic user or dynamic device membership types, you can only use one or the other, **not both**.

When creating a dynamic device membership type, **attributes for the specific device** are examined to determine group membership, not the attributes for the device's owner.

You also have the ability to add a security group to another security group. This is known as a **nested group**. There are a few rules limiting the nesting of groups, but as long as these are followed, nested groups can be a way to easily manage group membership as well as licenses and permissions for users.

Close

Active Directory Groups

The following are not supported in regards to nested groups:

- Adding groups to a group synced with on-premises Active Directory.
- Adding security groups to Office 365 groups.
- Adding Office 365 groups to security groups or other Office 365 groups.
- Assigning apps to nested groups.
- Applying licenses to nested groups.

Close

AAD

Applications

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Securing Applications With Azure Active Directory

A **Apps and Azure AD:**
Getting started protecting your app.

B **Scopes:**
What can your app do for you?

C **Permissions:**
Making sense of the chaos.

D **Consent:**
Allowing apps to work for you.

Scopes and Permissions Cheat Sheet

AAD

Hybrid

Back to Main

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Securing Applications With Azure Active Directory

Developers can build line-of-business applications that can be integrated with the Microsoft identity platform to provide secure sign-in and authorization for their services.

- Users can use their existing Azure AD credentials to access these applications. No more secondary logins for LOB applications!
- Microsoft IdP is based on the **OAuth 2.0** authorization protocol. This allows third-party applications to access web-hosted resources on behalf of a logged-in user.
- These resources can also define a set of permissions that can be used to divide the functionality of that resource into smaller chunks. These are known as **scopes**.
- User and application **permissions** are used with scopes to maintain fine-grained control over resource data as well as safeguard API exposure.

See It in Action!

Close

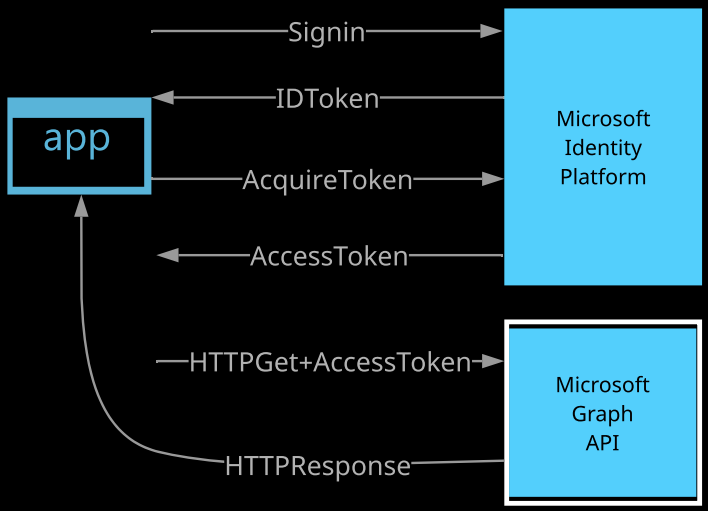
AAD

Hybrid

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Securing Applications With Azure Active Directory



Close

AAD

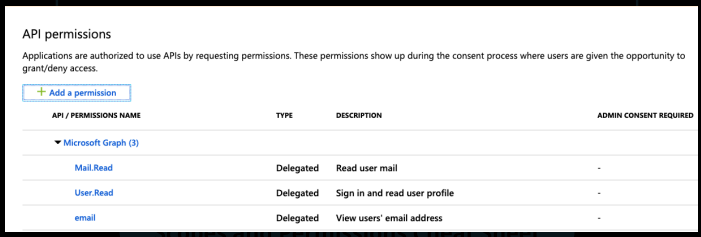
Hybrid

Securing Applications With Azure Active Directory

Scopes are permissions used to define what actions an application can perform on behalf of the user against a resource.

Scopes allow for fine-grained control over their data and how API functionality is exposed. A third-party app can request these permissions from users and administrators, who must approve the request before the app can access data or act on a user's behalf.

Scopes are configured in App Registrations (for application permissions) OR requested via the sign-in process (for delegated permissions).



API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny access.

+ Add a permission

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
Microsoft Graph (3)			
Mail.Read	Delegated	Read user mail	-
User.Read	Delegated	Sign in and read user profile	-
email	Delegated	View users' email address	-

Azure

API Scope Definition

Close

AAD

Hybrid

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Securing Applications With Azure Active Directory

```
GET
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?
client_id=6731de76-14a6-49ae-97bc-6eba6914391e
&response_type=code
&redirect_uri=http%3A%2F%2Flocalhost%2Fmyapp%2F
&response_mode=query
&scope=
https%3A%2F%2Fgraph.microsoft.com%2Fcalendars.read%20
https%3A%2F%2Fgraph.microsoft.com%2Fmail.send
&state=12345
```

C

Permissions:
Making sense of the chaos.

Scope
Query at user sign in

Close

D

Consent:
Allowing apps to work for you.

Scopes and Permissions Cheat Sheet

AAD

Hybrid

Securing Applications With Azure Active Directory

Permissions for users! Permissions for apps! So many permissions!

While scopes are technically permissions, we use the term in other ways. Specifically, permissions define what a user or an app can directly access in Azure.

User and app permissions are defined via roles. These roles use role based access control, or RBAC to determine privileges to resources.

A user may have privileges to write to the global directory, but the defined scope of permissions for an application may only require read permissions. So what happens? The user is only allowed read permissions when using the application. This is due to the concept of **effective permissions**.

- For **delegated permissions**, the effective permissions of your app will be the **least privileged** between the delegated permissions granted to the app (via consent) and the privileges of the currently signed-in user.
- For **application permissions**, the effective permissions of your app will be the **full level of privileges** granted to the app. These are used by apps that run without a signed-in user.

Close

AAD

Hybrid

Securing Applications With Azure Active Directory

In order for an application to perform a task on your behalf, you have to agree to let it do so.

This is referred to as **consent**. Consent occurs at user sign-in, when a scope query has been presented to the Microsoft identity platform. There are two types of consent:

- Individual **user consent** occurs when a user logs in to the Microsoft identity platform and they are asked to consent to these permissions.
- An administrator can grant consent for the application to act on behalf of any user in the tenant. If the administrator grants consent for the entire tenant, the organization's users won't see a consent page for the application. This is known as **administrator consent**. This can also occur for administrator-restricted permissions, such as the ability to read all user profiles in the directory.

Scopes and Permissions Cheat Sheet

Close

AAD

Hybrid

Securing Applications With Azure Active Directory

Scopes and Permissions Cheat Sheet

Scopes: privileges an app can make directly to APIs or on your behalf.

- Application ccopes are set in Azure Portal (API Permissions)
- Delegated scopes are queries sent with authentication call to Microsoft identity platform (login) .

Permissions: privileges the user or app can make to Azure AD and/or Azure resources.

- Azure AD: based on Directory Role.
- Azure: based on the RBAC role and scope assigned to the user or app service principal.

Scopes and permissions work together to grant access (this is known as **effective permissions**).

- **Delegated permissions:** used when a signed-in user is present.
  - Least privilege between consented app permissions and user permissions.
  - The app can never have more permission than the sign-ed in user.
- **Application permissions:** used by apps that run without a signed-in user present. For example, apps that run as background services or daemons.

Close

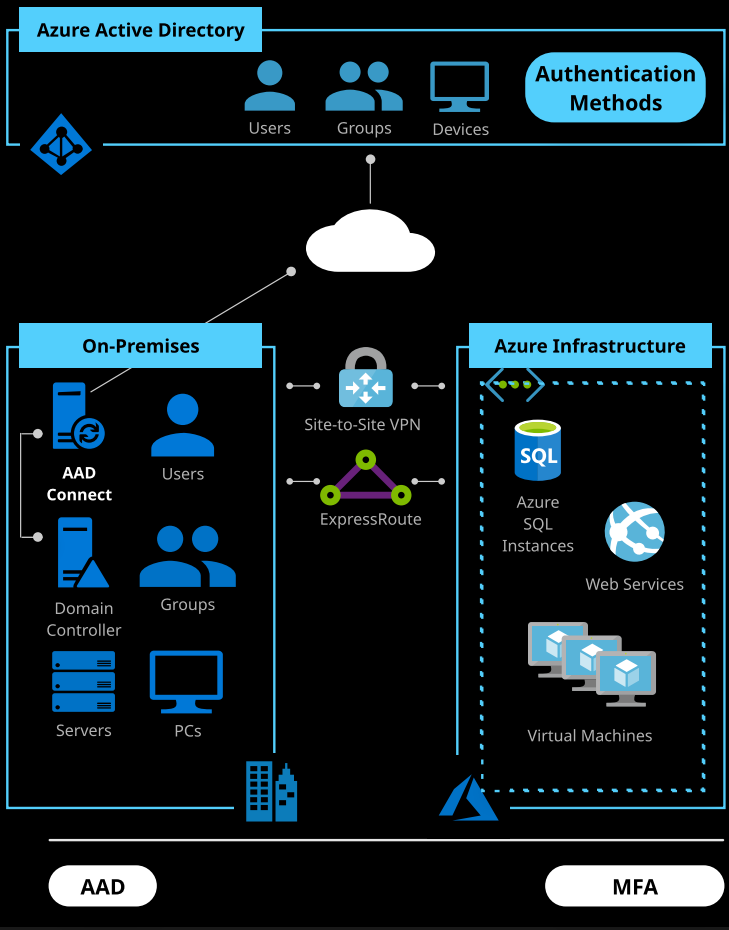
AAD

Hybrid

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Azure Active Directory Connect (AAD Connect)



Back to Main

Azure Active Directory Connect (AAD Connect)

What is Azure Active Directory Connect?

Azure Active Directory (AD) Connect is the underlying Microsoft tool used to deploy, configure, manage, and monitor hybrid identity between on-premises AD and Azure AD.

Azure AD Connect is supported on **Windows Server 2012 R2** and up.

MORE INFORMATION

Key Features | Prerequisites | Sync Scheduler | Rules Editor

Azure Active Directory Connect

Close

AAD

MFA

Azure Active Directory Connect (AAD Connect)

AAD Connect: Key Features

- Synchronization of users, groups, and other objects between on-premises AD and Azure AD
- Provides the ability to configure and deploy the following hybrid identity solutions:
  - Password hash synchronization (PHS)
  - Pass-through authentication (PTA)
  - Federation integration including AD Federation Services
- Health monitoring by providing monitoring data visible within the Azure Portal

MORE INFORMATION

Key Features | Prerequisites | Sync Scheduler | Rules Editor

Azure Active Directory Connect

Back

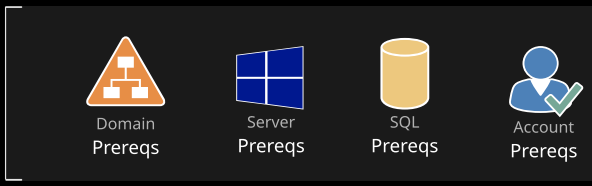
AAD

MFA

Back to Main

Azure Active Directory Connect (AAD Connect)

AAD Connect: Prerequisites



Microsoft Prerequisite Documentation

MORE INFORMATION

Key Features | Prerequisites | Sync Scheduler | Rules Editor

Azure Active Directory Connect

Back

AAD

MFA

Azure Active Directory Connect (AAD Connect)

AAD Connect: Domain Prerequisites

- You have to be using **Active Directory** as your on-premises identity platform.
- Schema version and forest functional level must be at **Windows Server 2003** or later.
- The on-premises domain controller used by AADC must be writable; **no read-only domain controllers**.
- "Dotted" NetBIOS domain names are unsupported.
- It is **strongly recommended** to enable the AD Recycle Bin.
- Domain name must be **Internet routable**!

Back

Azure Active Directory Connect (AAD Connect)

AAD Connect: Server Prerequisites

- **Windows Server 2008 R2** or later.
- This server **must be domain-joined** and may be a domain controller or a member server.
- If you install Azure AD Connect on Windows Server 2008 R2, the **server must be fully patched**.
- **.NET Framework 4.5.1** or later must be installed
- **Microsoft PowerShell 3.0** or later must be installed.
- **Password synchronization** requires the server to be on **Windows Server 2008 R2 SP1** or later.
- **Group managed service accounts** require the server to be on **Windows Server 2012** or later.

Hardware prerequisites:

# AD Objects	CPU	Memory	HD Size
< 50,000	1.6 Ghz	4 GB	70 GB
50K - 100K	1.6 Ghz	16 GB	100 GB
100K - 300 K	1.6 Ghz	32 GB	300 GB
300K - 600 K	1.6 Ghz	32 GB	450 GB
> 600K	1.6 Ghz	32 GB	500 GB

Back

AAD

MFA

Back to Main

Azure Active Directory Connect (AAD Connect)

AAD Connect: SQL Prerequisites

- Azure AD Connect requires a SQL Server database to store identity data.
  - **SQL Server 2012 Express LocalDB** is installed by default.
  - SQL Server Express has a **10GB size limit** which enables you to manage approximately **100,000 objects**.
  - If you need to manage a greater volume of directory objects, you need to point the installation wizard to a different installation of SQL Server.
- All versions of Microsoft SQL Server from **SQL Server 2008 R2** (with latest Service Pack) to **SQL Server 2019** are supported.
- Microsoft **Azure SQL Database** is not supported as a database.
- You must use a case-insensitive SQL collation. These collations are identified with a _CI_ in their name.
- **You can only have one sync engine per SQL instance.** It is not supported to share a SQL instance with FIM/MIM Sync, DirSync, or Azure AD Sync.

Back

Azure Active Directory Connect (AAD Connect)

AAD Connect: Account Prerequisites

- An **Azure AD Global Administrator** account for the Azure AD tenant you wish to integrate with. This account must be a school or organization account and cannot be a Microsoft Account.
- If you use **express settings** or upgrade from DirSync, then you must have an **Enterprise Administrator** account for your on-premises Active Directory.
- If you use the **custom settings** installation path, either use an Enterprise Administrator account for your on-premises Active Directory or refer to the **Microsoft documentation**.

Back

AAD

MFA

Back to Main

Azure Active Directory Connect (AAD Connect)

AAD Connect: Synchronization Scheduler

The following is a summary of some key management operations.

- By default, sync operations will operate **every 30 minutes**.
- The **Synchronization Service Manager** GUI tool supports configuration and monitoring of synchronization operations.
- To check the status of the synchronization service with PowerShell use **Get-ADSyncScheduler**.
- Sync operations can be triggered with PowerShell by using **Start-ADSyncSyncCycle**.

MORE INFORMATION

Key Features | Prerequisites | Sync Scheduler | Rules Editor

Azure Active Directory Connect

Close

AAD | MFA

Azure Active Directory Connect (AAD Connect)

AAD Connect: Rules Editor

- Allows for **customized synchronization rules** in Azure AD Connect.
- Provides **in-depth LDAP attribute filtering** above and beyond default AADC filtering options.
- Can be used to **fix modified default rules**.
- **BE CAREFUL!** You can overwrite the default synchronization options, which can break synchronization!
- **Clone, Clone, Clone!**

MORE INFORMATION

Key Features | Prerequisites | Sync Scheduler | Rules Editor

Azure Active Directory Connect

Close

AAD | MFA

Azure Active Directory Connect (AAD Connect)

Azure AD Authentication Methods

To achieve **hybrid identity** with Azure AD, one of three authentication methods can be used depending on your scenarios. The three methods are listed below.

AUTHENTICATION METHODS

- Password Hash Synchronization (PHS)
- Pass-through Authentication (PTA)
- Federation

Azure Active Directory Connect

Close

AAD

MFA

Azure Active Directory Connect (AAD Connect)

Password Hash Synchronization (PHS)

PHS synchronizes **a hash** of a user's on-premises password to Azure Active Directory (AD). Using Azure AD Connect, we can configure PHS so **all cloud user authentication occurs in Azure AD**. PHS can optionally be configured as a backup for ADFS.

Azure AD Connect express install defaults to deploying Password Hash Sync.

The main benefits:

- Synchronizes users, contacts, and group accounts between on-premises and Azure AD.
- Supports Office 365 hybrid identity.
- Enables users to **sign in and access cloud services/apps using on-premises credentials**.

Important considerations:

- PHS provides the fewest features.
- Multifactor authentication (MFA) with PHS is **only possible using Azure AD MFA**.
- Some organizations have security restrictions which prevent passwords being stored in the cloud.

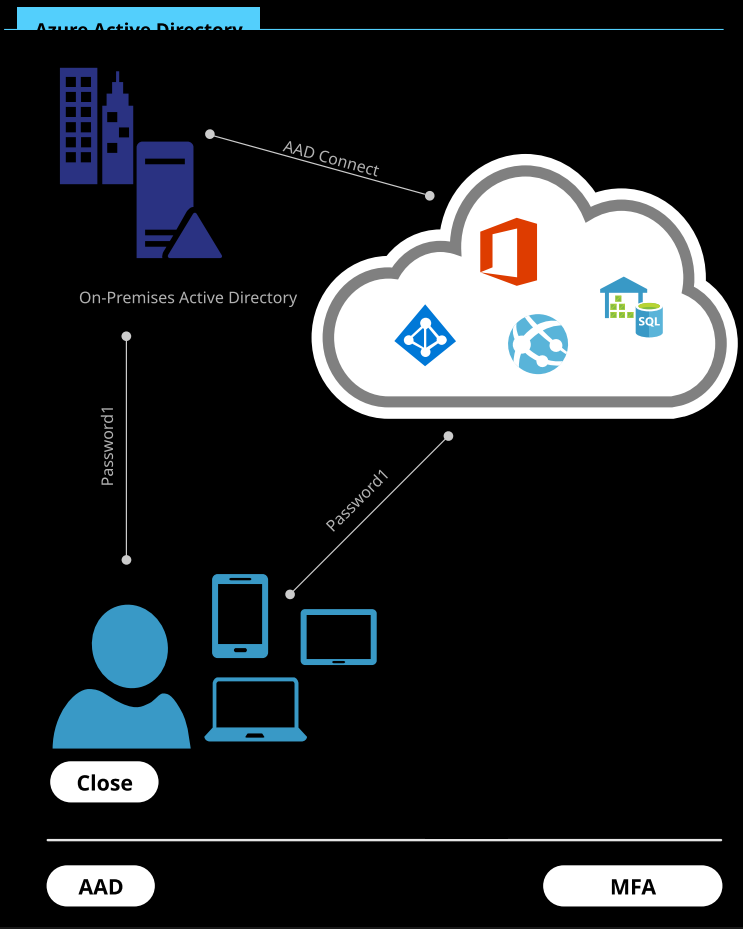
Close | Diagram

AAD | MFA

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Azure Active Directory Connect (AAD Connect)



Azure Active Directory Connect (AAD Connect)

Pass-Through Authentication (PTA)

PTA provides the same seamless single sign-on experience as PHS, but offers additional security benefits.

The main benefits:

- Synchronization of users, contacts, and group accounts between on-premises and Azure AD.
- Supports Office 365 hybrid identity.
- Enables users to sign in and access cloud services and apps using on-premises credentials.
- Does not require password hashes to be stored in the cloud.
- Only requires outbound connectivity from the on-premises Authentication Agents.
- All on-premises account policies are enforced when the user signs in (e.g. expiry, login hours, etc.)

Important considerations:

- On-premises multi-factor authentication (MFA) solutions are not supported with PTA.
- PTA is not integrated with Azure AD Connect Health.
- Detection of users with leaked credentials is not available.
- Seamless Single Sign On!

Close

Diagram

AAD

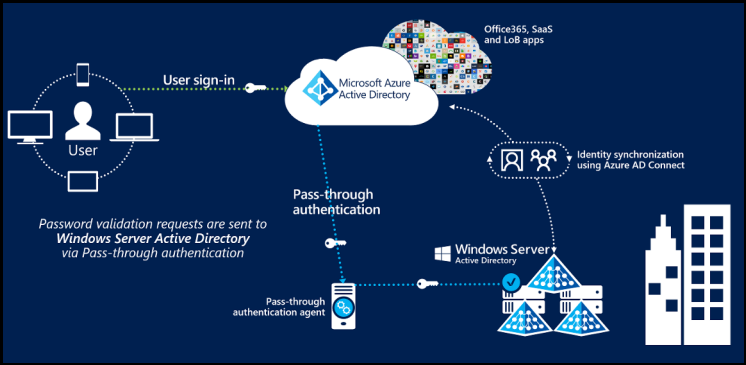
MFA

Back to Main

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Azure Active Directory Connect (AAD Connect)



Close

AAD

MFA

Azure Active Directory Connect (AAD Connect)

Federation

Federation is a collection of domains that have established trusts. When an on-premises directory is federated with Azure Active Directory, the trust is established. This provides authentication (confirming you are who you say you are) and authorization (determining what you are allowed access).

With federated identity, **all user authentication occurs on-premises**.

The main benefits:

- Supports an array of third-party and on-premises multifactor authentication solutions.
- Supports smart card authentication.
- Allows the display of password expiry notifications in the Office Portal and Windows 10 desktop.
- Supports all on-premises account policies (e.g. expiry, hours logged in, etc.) as on-premises sign in occurs.

Important considerations,

- Requires more infrastructure.
- Is more complex to configure and maintain.
- **Does not support seamless single sign-on**.

Close

Diagram

AAD

MFA

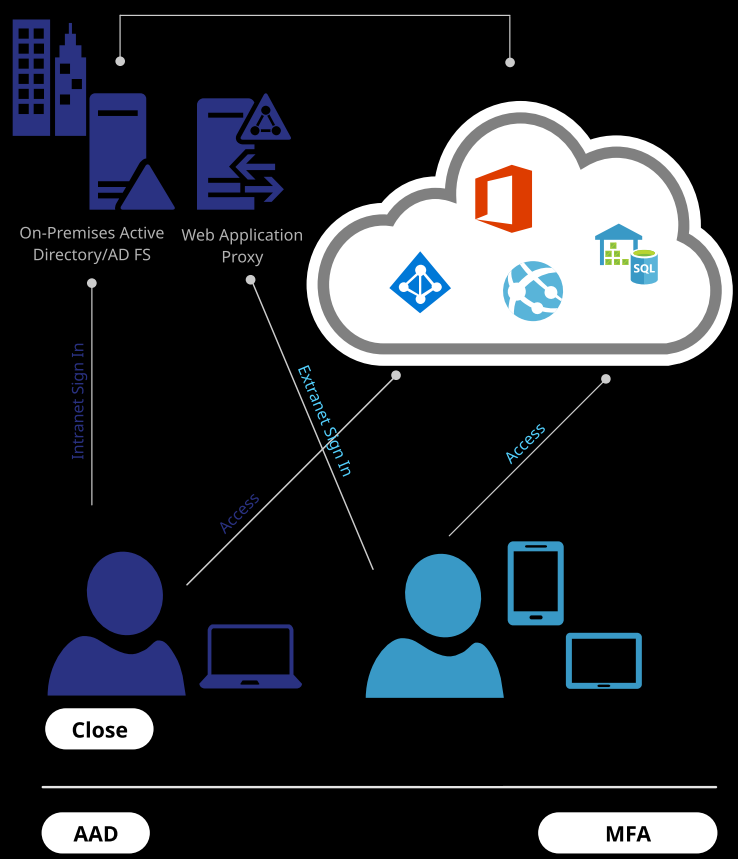
Back to Main

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Course Navigation

Azure Active Directory Connect (AAD Connect)



Back to Main

Linux Academy

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Multi-Factor Authentication (MFA)

A — **What is MFA?**
We cover the basics.

B — **Types of MFA:**
We discuss the various types of MFA, which to use, and how to get them.

C — **Best Practices:**
MFA can cause tremendous headaches. We provide some tips to avoid them.

D — **Configuration:**
We talk about rolling MFA out to your organization.

AAD

Conditional Access

Multi-Factor Authentication (MFA): What Is It?

Simply put, multi-factor authentication (MFA) is logging into Azure AD using more than one form of authentication.

- Provides additional security for user accounts by requiring a second form of authentication.
- Typically, authentication methods are:
  - **Something you know** : typically a password.
  - **Something you have**: a trusted device that is not easily duplicated, like a phone.
  - **Something you are**: biometrics.
- Delivers strong authentication via a range of easy to use authentication methods.
  - Text message
  - Phone call
  - Authentication request via app
  - Auth code via app
  - Hard tokens
- MFA can be bypassed based on the configuration of the product.

Close

AAD

Conditional Access

Multi-Factor Authentication (MFA): Types of MFA

There are different types of MFA available to meet organizational security requirements.

- **Azure Cloud MFA**
- **MFA Server**: used to secure **on-premises resources** with Azure MFA.
  - Remote Desktop, IIS Web Apps, etc.
  - **Dual registration**
  - Use only when necessary
- **RADIUS Integration**: used for integration with RDS and VPN.
- **Global Administrators**

How Do We Get It?

- **Licenses!**
  - Azure AD Premium
  - Azure AD Free or Basic
  - Office 365
  - Azure AD Global Administrators
  - **Microsoft MFA Licensing Information**

Close

AAD

Conditional Access

Multi-Factor Authentication (MFA): Best Practices

MFA can be very frustrating for your users and support staff if it isn't implemented properly. Here are a few tips to avoid potential problems.

- Communication
  - Microsoft **communication templates** and **end-user documentation** make this easier.
- Conditional access
  - **Exclusions** for support staff
  - **Named locations**
- Azure Identity Protection

Close

AAD

Conditional Access

Multi-Factor Authentication (MFA): Configuration

Making it work!

- **Licensing** users
- **Configuring** MFA service
  - Other configuration options
  - App passwords
- Authenticator app
- **Per-user vs. conditional access vs. IDP**
  - We will discuss conditional access in an upcoming lesson.
  - We will discuss IDP in an upcoming lesson.

Close

AAD

Conditional Access

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Conditional Access in Azure

A **Conditional Access Overview:**
Security on your terms!

B **Access Policies:**
The four Ws: Who, What, Where and How...

C **Best Practices:**
Dos and Don'ts.

D **Deployment:**
Start securing your environment.

AAD

AD IDP

Back to Main

Conditional Access in Azure: An Overview

Conditional access is automated access control that strengthens user sign-in and access to cloud applications.

- **Not** used as a first-factor authentication; passwords are still required.
- Can be used to **require multi-factor authentication**.

- Common scenarios
  - **Sign-in risk**
    - Bad actor detection (e.g. leaked credentials)
    - Need more information
    - Require MFA
    - Block specific applications if unable to obtain proof
  - **Location**
    - On-premises (named locations) vs. internet
    - Countries and regions
    - MFA-trusted IPs
  - **Device management**
    - What device are you using?
    - Corporate-owned devices
    - BYOD
  - **Client application**

Close

AAD

AD IDP

Conditional Access in Azure: Access Policies

Access policies are the focus of conditional access

When This Happens	Do This

Policies are based on **conditions** and **access controls**.

- When this happens (**condition**)
  - **Who** are you?
    - User/group membership
  - **What** are you accessing?
  - Required: User and Application
  - Others: location, sign-in risk
- Do this (**access control**)
  - Grant controls
  - Used to **gate** access (let you in)
    - In order to gain access, you must:
      - Use MFA.
      - Use a compliant device
      - Use a hybrid-joined device (workstation).
      - Use an approved client app.
  - Session controls
    - Limited experience within a **cloud app**.

Close

AAD

AD IDP

Conditional Access in Azure: Best Practices

Like MFA, failure to carefully execute conditional access policies could have catastrophic consequences.

Donts:

- For all users/all cloud apps:
  - Block access.
  - Require compliant device.
  - Require domain join.
  - Require app protection policy.
- For all users, all cloud apps, and all device platforms:
  - Block access . This configuration blocks your entire organization, which is definitely not a good idea.

Dos:

- Have exclusions for admin personnel.
  - Being locked out of Admin Portal is bad. Trust me.
- Use the What-If tool to test policies.
- Pilot access using groups. Don't start with everyone!

Close

AAD

AD IDP

Conditional Access in Azure: Deployment!

Now that we've discussed conditional access in depth, let's roll it out!

- Licensing users.
- Configuring access policies.
- Testing with client user accounts.
- Locking ourselves out (don't try this at home)!

Close

AAD

AD IDP

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Azure AD Identity Protection

A **What is AD Identity Protection:**
Going over the basics.

B **Identity Protection Components:**
Getting under the hood with AADIP.

C **Risks:**
Covering the risks and how AADIP helps.

D **Best Practices:**
Providing security without the headaches.

E **Configuration:**
Securing our environment using AADIP.

AAD

AD PIM

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Azure AD Identity Management: Automated Protection for User Identities; More Security and Less Administration

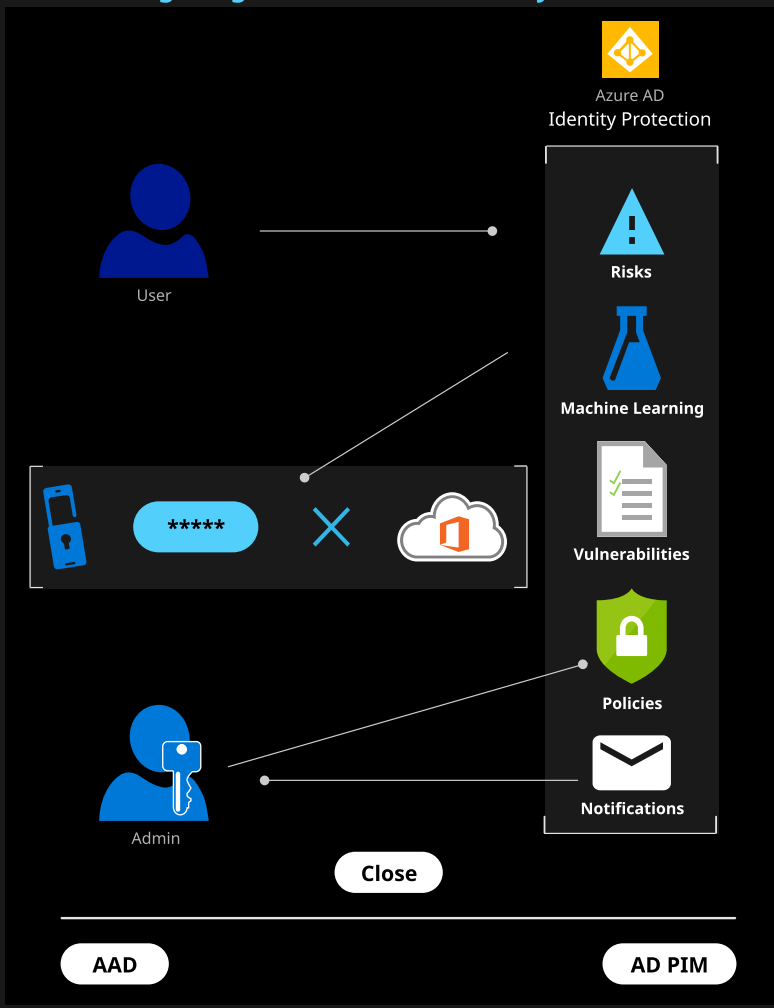
- Stolen user identities are the number one cause of security breaches. Attackers leverage **phishing attacks and malware** to gain access to systems.
- Even low-level user accounts can be used to gain access to a majority of network resources.
- Administrators must protect all identities, **no matter the privilege level** and ensure that compromised identities do not gain access.
- This typically involves **full-time awareness and monitoring** of all user identities. The administrative effort is huge, and most of the time, completely reactive in nature.
- Azure AD Identity Protection removes much of this effort by providing a comprehensive solution that:
  - Proactively prevents compromised identities from accessing resources.
  - Provides recommendations to improve security by analyzing vulnerabilities, such as user and sign-in risk levels and risk events, as well as environmental factors.
  - Notifies administrators of risk events.
  - Allows administrators to create policies to automatically mitigate risk events.

Close

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Course Navigation



Back to Main

Linux Academy

Manage Identity and Access

Configuring Azure Active Directory for Workloads

Risks: What Azure AD Identity Protection Is Designed to Mitigate

There are two types of risks:

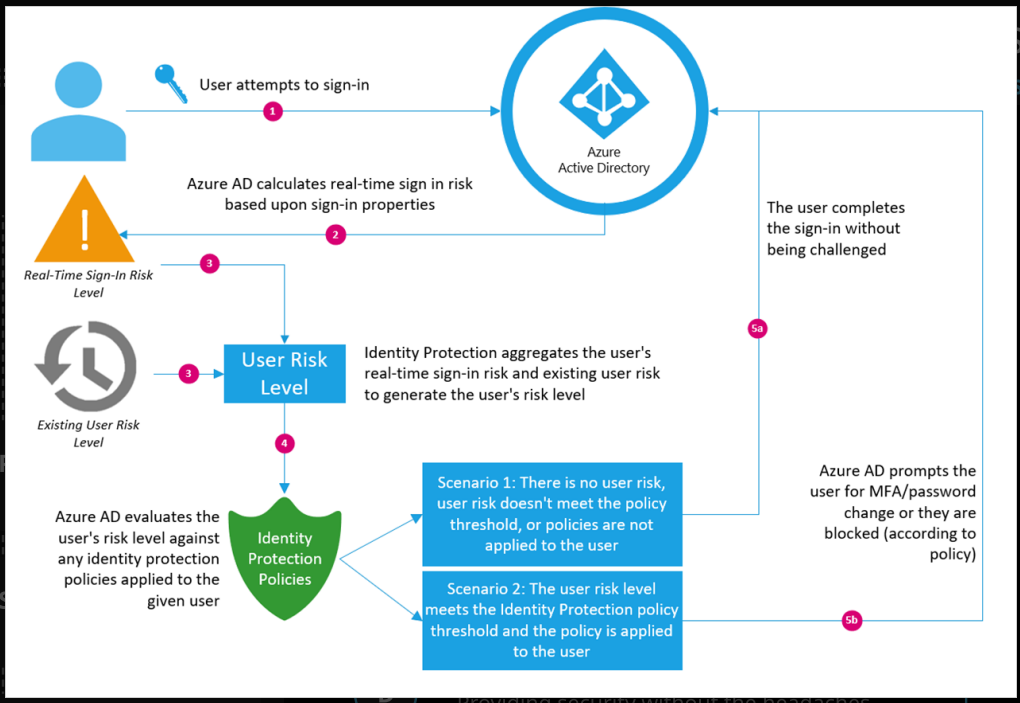
- **Sign-in risk**
  - Represents the likelihood a given authentication request isn't authorized by the identity owner.
  - Two evaluations of sign-in risk:
    - Sign-in risk (Real-time)
    - Sign-in risk (Aggregate)
- **User risk**
  - Represents the likelihood a given identity is compromised.
  - Calculated by:
    - All risky sign-ins
    - All risky events not linked to a sign-in
    - The current user risk
    - Any risk remediation or dismissal actions

Types of risk events:

- Atypical travel
- Anonymous IP addresses
- Unfamiliar sign-in properties
- IP addresses linked to malware
- Leaked credentials

Diagram

Close



Secure Data and Applications

Section 4

Providing security without the headaches.

Close

E

Configuration:

Securing our environment using AADIP.

AAD

AD PIM

Back to Main

Linux Academy

Azure AD Identity Protection

A **What is AD Identity Protection:**
Going over the basics.

B **Identity Protection Components:**

C **Configuration:**
Securing our environment using AADIP.

D **Best Practices:**
Providing security without the headaches.

E

Machine Learning

Azure Active Directory uses **adaptive machine learning algorithms and heuristics** to detect anomalies and suspicious incidents. These could indicate potentially compromised identities.

Using this data, Identity Protection generates reports and alerts enabling you to evaluate the detected issues and take appropriate mitigation or remediation actions.

This data is also used when evaluating conditional access policies to determine automatic remediation of user or sign-in risks.

Close

AAD

AD PIM

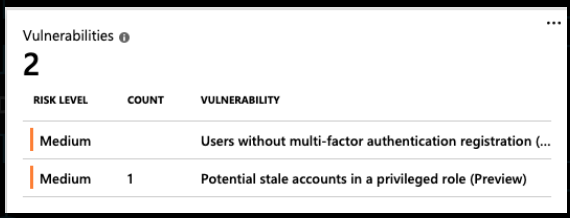
Azure AD Identity Protection

Vulnerabilities

Vulnerabilities are weaknesses in an environment that can be exploited by an attacker.

Azure AD Identity Protection identifies these vulnerabilities and presents them in the **Overview Dashboard**. Clicking on each one provides more information and recommendations on how to remediate them, strengthening the security score of the organization.

If configured, alerts from **Privileged Identity Management** appear here.



Close

AAD

AD PIM

Azure AD Identity Protection

Policies

In order to take advantage of risks and vulnerabilities detected by Azure AD Identity Protection, there are three policies we can configure to automate responses to these potential threats.

- **Multi-factor authentication registration policy**
  - This policy is used to **require registration** to the Azure MFA service.
  - The Azure MFA service should be configured beforehand.
  - User communication should occur **before** implementing this policy.
- **User risk policy**
  - Automatically responds to a user risk (**identity compromise**).
  - Policy can be configured to block access to your resources or require a password change.
- **Sign-in risk policy**
  - Used to react to suspicious actions that come along with the user sign-in.
  - Can be configured to block the account or require MFA.

Close

Azure AD Identity Protection

Notifications

Azure AD Identity Protection sends two types of **automated notification emails** to help administrators manage user risk and risk events.

- **Users at risk detected email**
  - Emails are sent per used incident.
  - Risk levels and recipients are adjustable for these notifications.
  - Email contains a **Users flagged for risk** report.
  - Administrators will only receive one emails when the user reaches this risk level.
  - Upon receipt, the user **should immediately be investigated**.
- **Weekly digest email**
  - Emails are sent once a week to all **Global Administrators, Security Administrators, and Security Readers.**
  - Contains a summary of new risk events. This includes:
    - Users at risk
    - Suspicious activities
    - Detected vulnerabilities
    - Links to the related reports in Identity Protection

Close

AAD

AD PIM

Azure AD Identity Protection: Best Practices

- A **high** threshold reduces the number of times a policy is triggered.
  - Minimizes the impact to users.
  - Excludes low and medium sign-ins flagged for risk.
  - May not block an attacker.
- When setting the policy:
  - Exclude users who **do not or cannot have multi-factor authentication.**
  - Exclude users in locales where enabling the policy is not practical (e.g. **no access to helpdesk**).
  - Exclude users who are **likely to generate many false-positives**, such as developers and security analysts.
- Use a high threshold during initial policy roll-out.
- Use a low threshold if your organization requires greater security.
- Selecting a low threshold introduces additional user sign-in challenges, but grants increased security.
- **The recommended default for most organizations is to configure a rule for a medium threshold.**

Close

Azure AD Identity Protection Configuration Steps

- **License** users (Azure AD Premium P2).
- Onboard Azure AD Identity Protection.
- Configure **MFA registration policy** (optional but recommended).
- Configure **user risk policy.**
- Configure **sign-in risk policy.**
- Test the configurations.

Close

Manage Identity and Access

Azure AD Privileged Identity Management

Course Navigation

Manage Identity and Access
Section 1

- Configuring Azure Active Directory for Workloads
- Azure AD Privileged Identity Management
- Azure Tenant Security

Platform Protection
Section 2

Security Operations
Section 3

Secure Data and Applications
Section 4

A **Overview and Activation**
Let's talk PIM and get started!

B **Configuration, Access Requests, and Approval**
Security wizard, role settings and more.

C **Reviewing Access**
Auditing and access reviews.

AAD

Tenant Security

Back to Main

Linux Academy

Manage Identity and Access

Azure AD Privileged Identity Management

Course Navigation

Manage Identity and Access
Section 1

- **Configuring Azure Active Directory for Workloads**
- **Azure AD Privileged Identity Management**
- Azure Tenant Security

Platform Protection
Section 2

Security Operations
Section 3

Secure Data and Applications
Section 4

Part I: Overview and Activation

What Is
PIM?

Azure
AD

Azure
Resources

PIM
Terminology

Licensing
Requirements

PIM
Activation

MS PIM
Documentation

Close

Back to Main

Linux Academy

Azure AD Privileged Identity Management

- Concerned about privileged access?
- Too many administrators?
- Duplicate access rights?

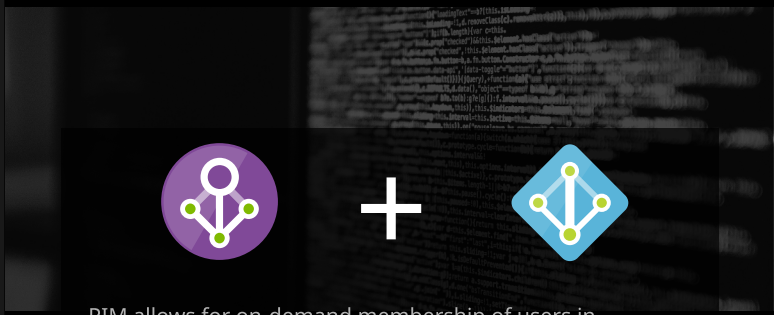
Azure Active Directory Privileged Identity Management (PIM) can help by providing:

- **Just-in-time** (as needed) privileged access to Azure AD and Azure resources.
- **Time-bound** (expiring) access to resources.
- **Approval requirements** to activate privileged roles.
- **Multi-factor authentication** enforcement to activate any role.
- **Justification** to understand why users activate.
- **Notifications** when privileged roles are activated.
- **Access reviews** to ensure users still need roles.
- Downloadable **history** for internal or external audit.

Close

Manage Identity and Access

Azure AD Privileged Identity Management



PIM allows for on-demand membership of users in elevated directory roles, such as:

- **Global administrator**
- **Security administrator**
- **User administrator**
- **Exchange administrator**
- **SharePoint administrator**
- **Intune administrator**
- **Security reader**
- **Service administrator**
- **Billing administrator**
- **Skype for Business administrator**
- **And most others!**

Close

AAD

Tenant Security

Back to Main

Linux Academy

Manage Identity and Access

Azure AD Privileged Identity Management

In addition to management of AD directory roles, PIM allows for on-demand management of members for Azure resource roles. These include:

- **Owner**
- **Contributor**
- **User Access Administrator**
- **Security Admin**

Subscription-level roles and Azure Management Groups can be managed with PIM.

Close

AAD

Tenant Security

PIM Terminology

These are relevant terms used in PIM architecture. You should review these to better understand PIM management of AD roles and Azure resources.

- Eligible
- Active
- Activate
- Activated
- Assigned
- Permanent eligible
- Permanent active
- Expire eligible
- Expire active
- Just-in-time (JIT) access
- Principle of least privilege access

Close

AAD

Tenant Security

Licensing PIM

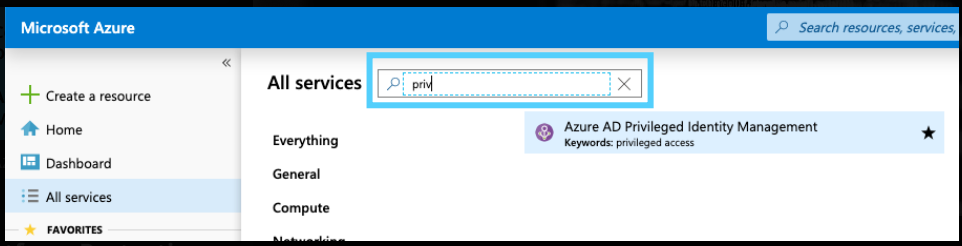
Azure AD must have one of the following paid or trial licenses in order to use PIM:

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

Which users must have licenses? Each administrator or user interacting with or receiving a benefit from PIM.

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

Activating PIM

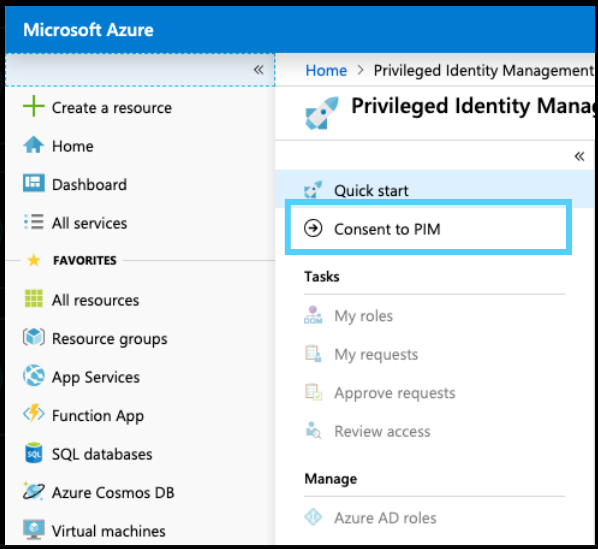


To Activate PIM:

- You must be a **Global Administrator**.
- You must use an **organizational account** (not a personal account).

Upon Activation:

- You are automatically assigned the **Security Administrator** and **Privileged Role Administrator** roles in Azure AD.

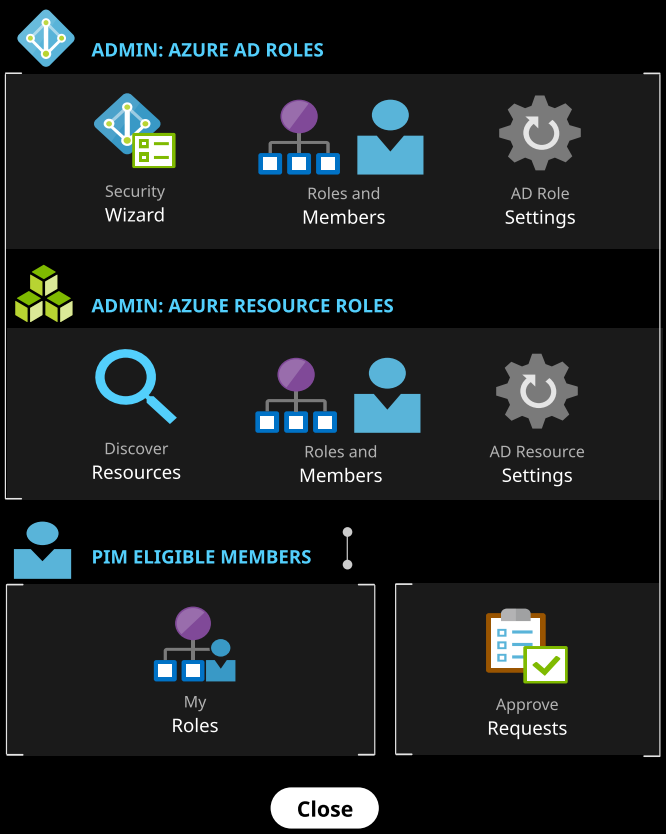


Close

Manage Identity and Access

Azure AD Privileged Identity Management

Part II: Configuration, Access Requests, and Approval



PIM Security Wizard

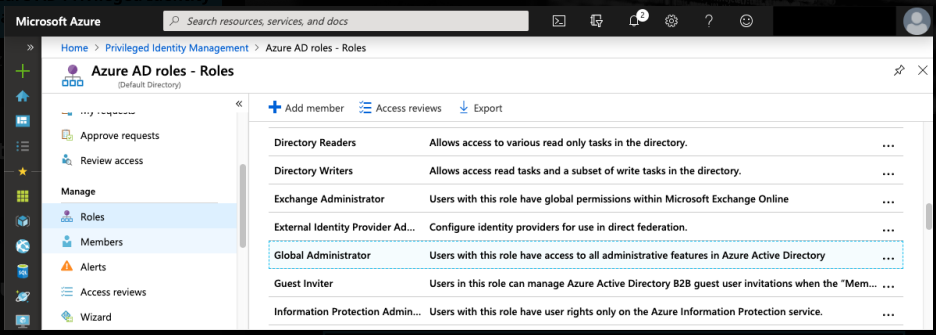
- Use the **Security Wizard** to determine the current membership of all high-privileged AD Security Roles. You can then use the Wizard to **reduce the number of permanently assigned role holders** by converting those to eligible role assignments.
- You can choose not to act on any security assignments at the time and instead **perform the changes later**.
- If you choose to modify the security assignments, make sure the **changes are announced to all administrators and business units ahead of time**!
- **At least one organizational account** (not a personal account) must hold permanent Global Administrator and Privileged Role Administrator rights.
- If there is only one Privileged Role Administrator in the organization, **the organization will not be able to manage PIM if that account is deleted**.

Close

AAD

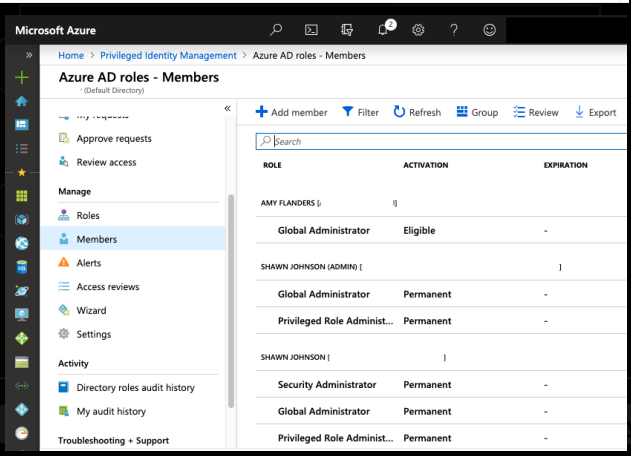
Tenant Security

Azure AD Roles and Members



Roles:
Use **Azure AD roles** to add an eligible member to a privileged group. You can also convert the eligible assignment to permanent or vice-versa.

Members:
Use **Members** to view assignments or add an assignment.

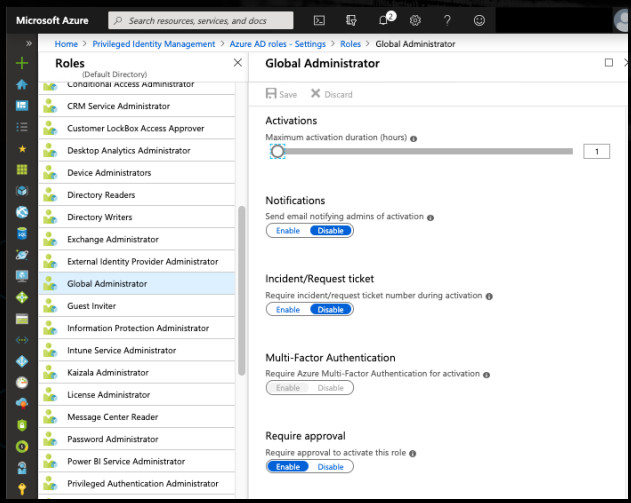


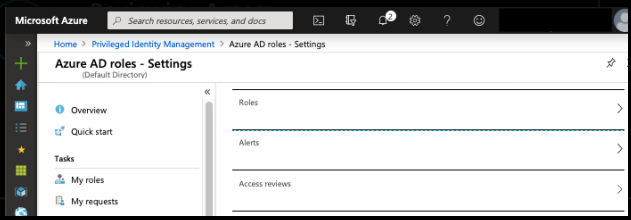
Close

Azure AD Role Settings

Use **Azure AD Role Settings** to configure activation duration, notifications, MFA, approval, and other settings per AD role.

Settings can also be configured for **alerts and access reviews** for AD role elevation.





Close

Discover Azure Resources

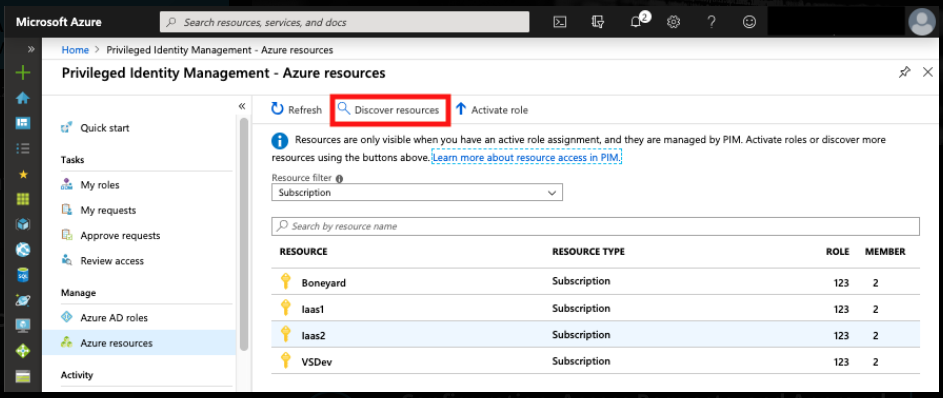
- When first setting up PIM for Azure resources, discover and select the resources PIM. protects
- There's no limit to the number of resources you can manage with PIM.
- Resources are discovered based on Azure subscription and management group.
- Once a management group or subscription is set to managed, it can't be unmanaged. This prevents another resource administrator from removing PIM settings.

Close

AAD

Tenant Security

Azure Resource Roles and Members



Roles:
Use **Azure resource roles** to add an eligible member to a privileged role. You can also convert the eligible assignment to permanent or vice-versa.

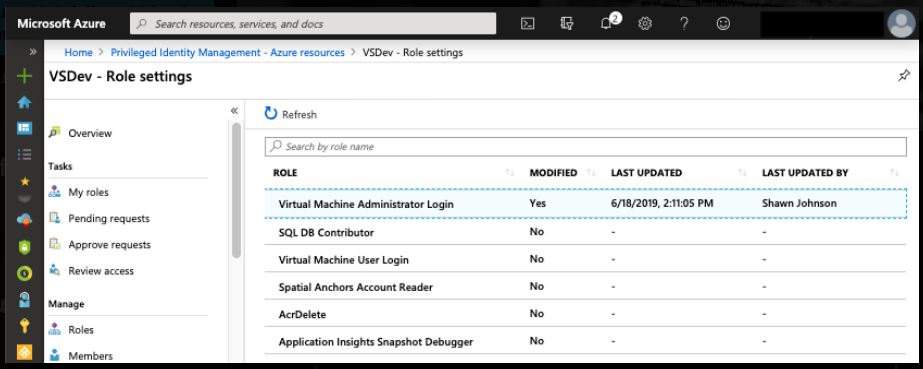
Members:
Use **Members** to view assignments or add an assignment.

Close

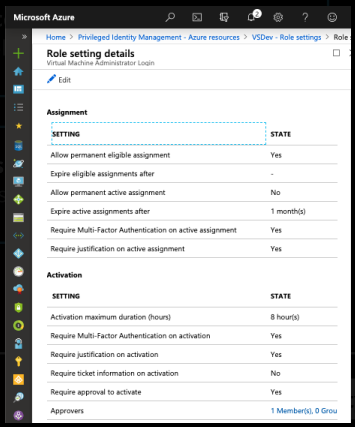
AAD

Tenant Security

Azure Resource Settings

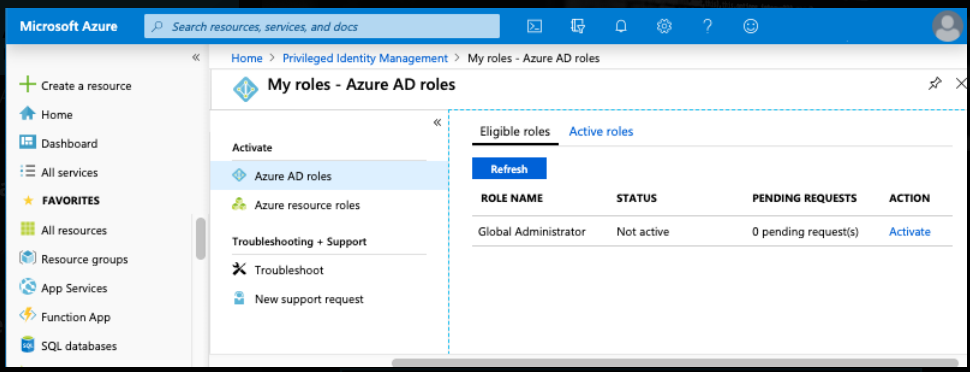


Use **Azure Resource Role Settings** to configure activation duration, notifications, MFA, approval, and other settings per AD role.



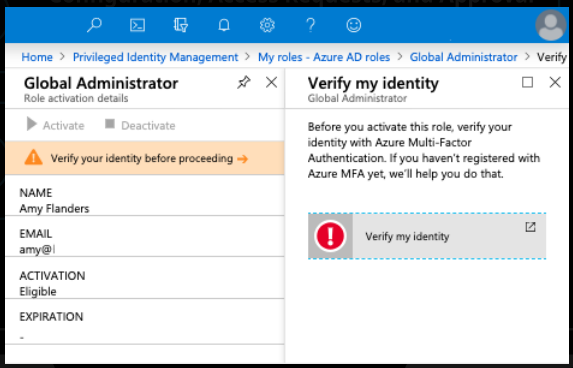
Close

My Roles



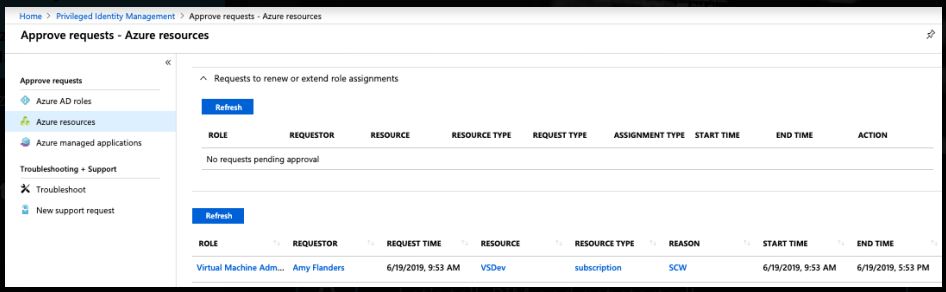
My Roles:
Use **My roles** to view and activate any Azure AD or Azure resource privilege elevation.

MFA:
If the elevation requires multi-factor authentication, you will be required to verify your identity prior to activation.



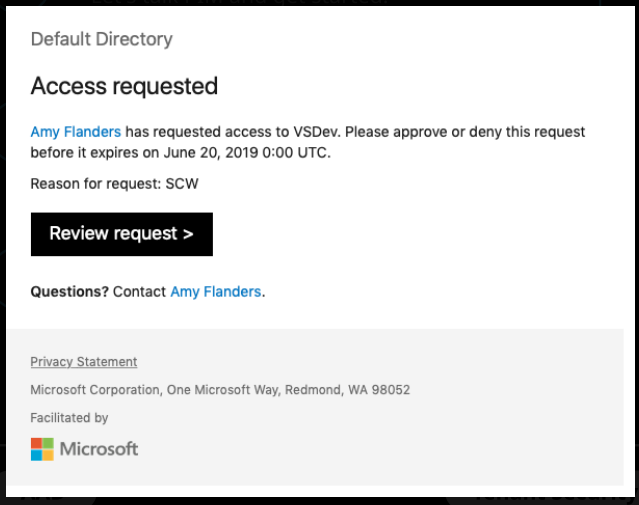
Close

Approve Requests



Approve Requests:
Use **Approve requests** to view and approve any requests for Azure AD or Azure resource privilege elevation.

Email:
If notifications are enabled for requests, then the approver will receive a message asking them to review the request.



Close

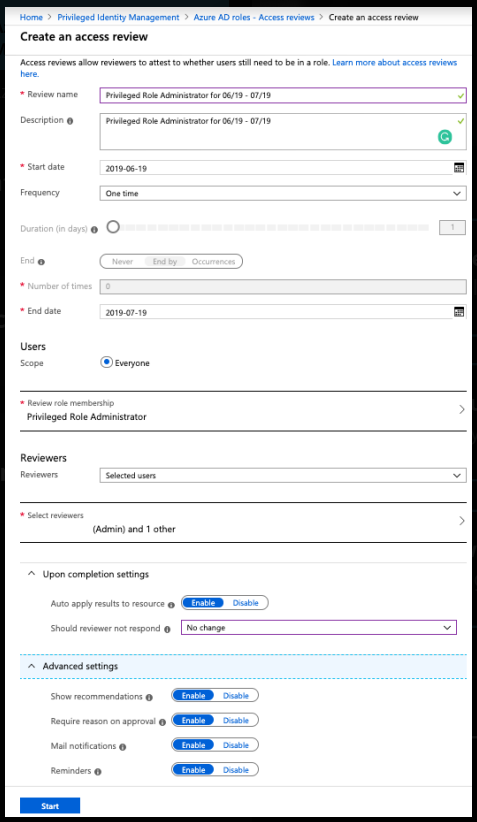
Manage Identity and Access

Azure AD Privileged Identity Management

Part III: Reviewing Access

Close

Access Reviews



Since access to privileged Azure AD roles for employees change over time, you should **regularly review access** to determine if elevated privileges are still necessary.

You can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to create **access reviews** for privileged Azure AD roles as well as Azure resources.

You can also configure **recurring access reviews** that automatically occur.

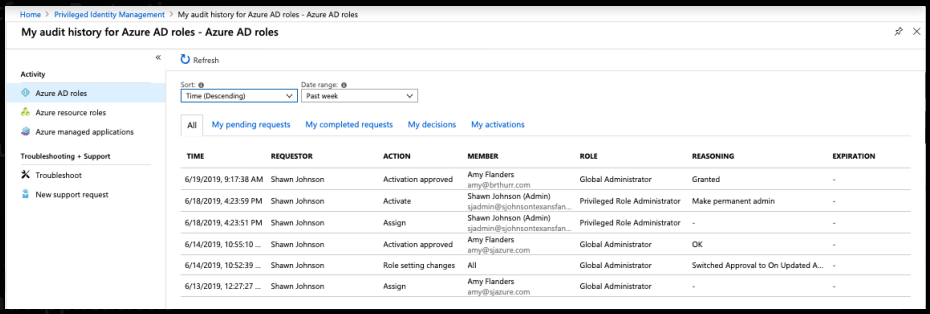
Eligible members of privileged roles are **notified in the Azure Portal** when they are required to justify access. **Email communication** can also be configured to notify your users of an access review.

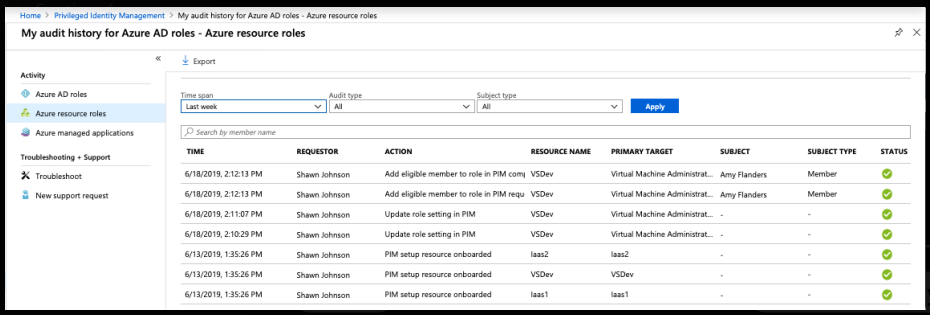
Azure PIM can determine the appropriate course of action based on factors such as time since elevation and more. **These recommendations can be implemented for non-responders.**

Close

My Audit History

Use **My audit history** to view all PIM activites for the signed-in user. This includes role assignments and activations within the past 30 days for all privileged roles. You can use **My audit history** to view assignments and activations for Azure AD and Azure resource privileged roles.





Close

Directory Roles Audit History

Use **Directory roles audit history** to to view all events for all Azure AD roles. This includes events performed by all Privileged Role Administrators as well as PIM.

TIME	REQUESTOR	ACTION	MEMBER	ROLE	REASONING	EXPIRATION
6/19/2019, 10:17:40 AM	Azure AD PIM	Deactivate	Amy Flanders	Global Administrator	Expired	-
6/19/2019, 9:17:38 AM	Amy Flanders	Activate	Amy Flanders	Global Administrator	Please activate.	6/19/2019, 10:17:38 AM
6/19/2019, 9:17:38 AM	Shawn Johnson	Activation approved	Amy Flanders	Global Administrator	Granted	-
6/19/2019, 9:15:55 AM	Amy Flanders	Activation requested	Amy Flanders	Global Administrator	Please activate.	-
6/18/2019, 4:23:59 PM	Shawn Johnson	Activate	Shawn Johnson (Admin)	Privileged Role Administrator	Make permanent admin	-
6/18/2019, 4:23:51 PM	Shawn Johnson	Assign	Shawn Johnson (Admin)	Privileged Role Administrator	-	-
6/14/2019, 11:55:12 AM	Azure AD PIM	Deactivate	Amy Flanders	Global Administrator	Expired	-
6/14/2019, 10:55:11 AM	Amy Flanders	Activate	Amy Flanders	Global Administrator	I need it!	6/14/2019, 11:55:10 AM
6/14/2019, 10:55:10 AM	Shawn Johnson	Activation approved	Amy Flanders	Global Administrator	OK	-
6/14/2019, 10:54:02 AM	Amy Flanders	Activation requested	Amy Flanders	Global Administrator	I need it!	-

Close

Azure Tenant Security

Topics in this section include:

A Transferring Azure Subscriptions

This section contains some important topics that **will be included on the exam** but don't really fit in the other lessons.

AD PIM

Platform Protection

Back to Main

Azure Tenant Security

Transferring an Azure Subscription

- Transferring billing ownership of an Azure subscription takes place in the **Cost Management + Billing** pane or in the **Account Center**.
- When transferring to another tenant, **all users, groups, and RBAC access to resources in the source tenant are lost** on the resources in the subscription. The user accepting the transfer request is the only account with access to the resources.
- **Management certificates, access keys, and remote access credentials will remain intact.** These should be updated if the source account no longer requires access to these resources.
- Visual Studio, MPN, and Pay-As-You-Go Dev/Test subscriptions with recurring Azure credits will not transfer between accounts. **The subscription will use the credit in the destination Visual Studio account, should one exist.**
- Only **these subscription types** are eligible for transfer.
- Transfers between countries cannot be performed in the portal. **You need to contact support to initiate a cross-country transfer.**
- In order to complete the transfer, **the recipient must accept billing ownership and provide payment details.**
- If the recipient does not have an Azure account, **they must create one** to accept the transfer.

AD PIM

Close

Platform Protection

Back to Main

Azure Tenant Security

Topics in this section include:

Azure Subscriptions Eligible for Transfer

Subscription transfer in the Azure portal is available for the subscription types listed below. Currently transfer is **not supported for Free Trial or Azure in Open (AIO) subscriptions**.

- Microsoft Partner Network
- Visual Studio Enterprise (MPN) subscribers
- MSDN Platforms
- Pay-As-You-Go
- Pay-As-You-Go Dev/Test
- Visual Studio Enterprise
- Visual Studio Enterprise: BizSpark
- Visual Studio Professional
- Visual Studio Test Professional
- Enterprise Agreement (EA) - Through the EA Portal.
- Microsoft Azure Plan - Only supported for accounts created during signup on the Azure website.

Close

This s… important topics that **will be** inclu… it in the other lessons.

Topics Included in This Section

- Virtual Network [Review] 
- Network Security Groups [Review] 
- Application Security Groups 
- Azure Firewall 
- Resource Firewalls 

VNets

Network Security: Virtual Networks

Virtual Networks (VNets) are used to create a virtual private network within Azure where resources can be networked to one another similar to a private on-premises environment.

- The VNet has an **internal address space** (e.g. 10.1.0.0/16).
- Resources connect to **subnets within a VNet** to gain network access.
- Subnets within the VNet **must exist within the same address space**.
- **All subnets** within a virtual network **can communicate with each other**.
- Default routing can be modified with **user-defined route tables**.

VNets can be **peered** with one another to allow for communication between each other.

VNets can also be connected with on-premises networks (as well as other VNets) with Site-to-Site VPN or ExpressRoute connections. These require **Virtual Network Gateways** to be present inside the VNet.

AZ-300 Blueshift Guide: Networking

Network Security **NSGs**

Network Security: Network Security Groups

Network Security Groups (NSGs) are used to provide network layer security for resources within a Virtual Network (VNet). When attached to a resource, they can **allow or deny traffic** based on rules you configure.

Overview:

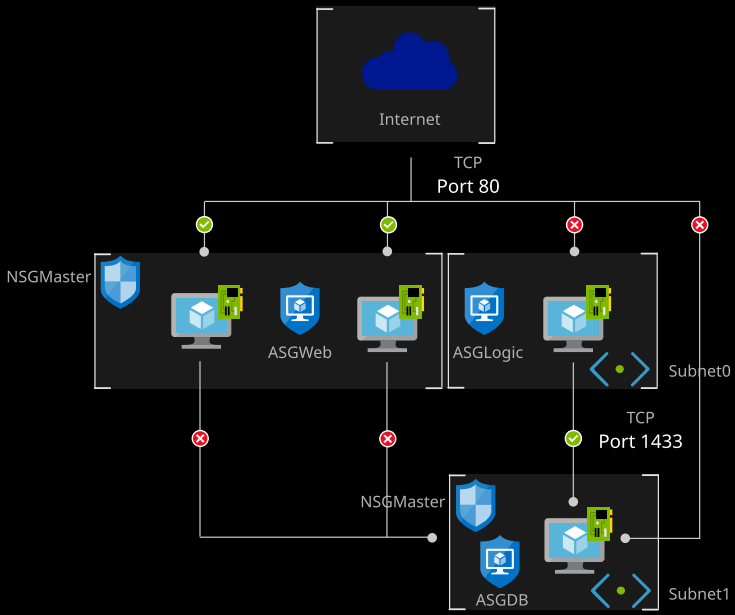
- The best practice is to **block ALL traffic** except required communication. This is sometimes called "default deny."
- NSGs can be applied to either a **Network Interface Card (NIC), a subnet, or both**.
  - When NSGs are assigned to both, **rules from both are evaluated.**
- NSG rules are stateful, so **reply traffic is automatically allowed** regardless of other rules.
- NSGs contain "Default Rules" which **cannot be deleted**; you need higher priority rules to override them.
- Once a rule is matched, **no further rules are processed**.

AZ-300 Blueshift Guide: Networking

Network Security: Application Security Groups

An **Application Security Group (ASG)** is a **logical collection** of virtual machines, specifically their network interface cards (**NICs**). You join virtual machines to the ASG and then use the application security group as a source or destination in **NSG rules**.

Think of ASGs as a way to create **custom service tags** for a network security group.



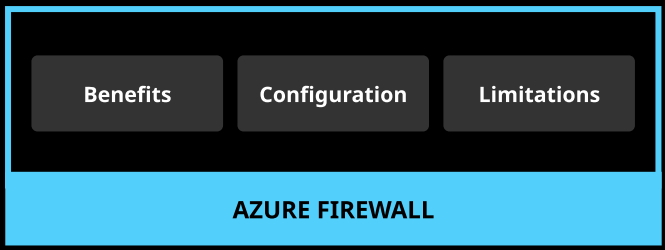
Network Security

Remote Desktop

Network Security: Azure Firewall

In addition to NSGs, there are a few other network-layer Azure offerings we can implement to harden network security. Typically, these were third-party products called Network Virtual Appliances (NVAs) used to inspect all inbound and outbound network traffic to an entire virtual network.

Microsoft recently released **Azure Firewall**-as-a-Service, intending it to be an alternative to third-party NVAs. Microsoft designed Azure Firewall for The Cloud, **specifically Azure**.



Topics Included in This Section

Azure Firewall offers:

- **A stateful** firewall as a service.
- Built-in **high-availability** with unrestricted cloud scalability.
- FQDN **filtering and tags**.
- Rules for filtering network traffic.
- Outbound **SNAT** support.
- Inbound **DNAT** support (port forwarding).
- A central place to create, enforce, and log application and network **connectivity policies** across Azure subscriptions and VNETs.
- **Full integration with Azure Monitor** for logging and analytics.

Close

Resource Firewalls

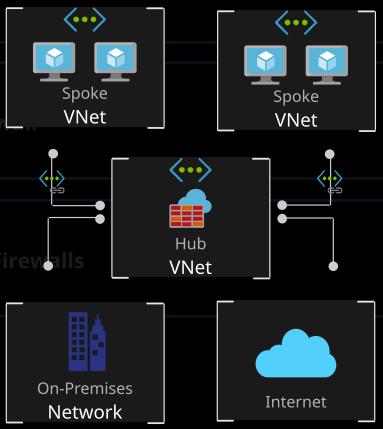
VNets

Azure Firewall Configuration

The typical deployment for Azure Firewall is in a central virtual network. Other virtual networks are then peered to it in a hub-and-spoke fashion. Default routes from the peered virtual networks are pointed to the central firewall virtual network. The firewall, subnet, VNet, and the public IP address must all be in the same resource group.

Global VNet peering is supported, but it isn't recommended because of potential performance and latency issues across regions. For best performance, deploy one firewall per region.

The advantage of this model is the ability to centrally exert control on multiple spoke VNETs across different subscriptions.



Close

Topics Included in This Section

Azure Firewall Limitations

- Network filtering rules for non-TCP/UDP protocols (such as ICMP) don't work for Internet-bound traffic.
- **You cannot move Azure Firewall** to a different resource group or subscription.
- Limited port range.
- No **custom DNS** support.
- **No SNAT/DNAT** for private IP destinations.
- Complete list of limitations available here.

Close

Application Security Groups

Azure Firewall

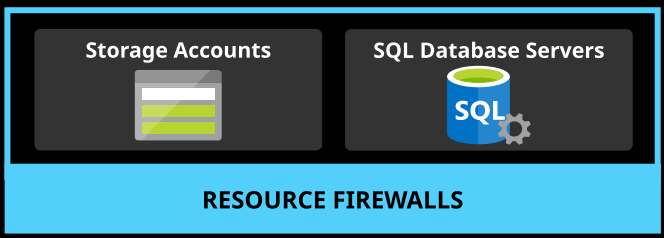
Resource Firewalls

VNets

Network Security: Resource Firewalls

Individual Azure resources also maintain their own set of firewall rules. These rules can allow or deny access to Azure virtual networks, **Azure services** such as backup and SQL, and Internet hosts.

These access rules are configured within the Azure resources themselves. The most common resources with this additional protection are Azure Storage Accounts and Azure SQL server databases.



Back to Main

Topics Included in This Section

Virtual Network [Review]

Azure Services that can be allowed via resource firewalls:

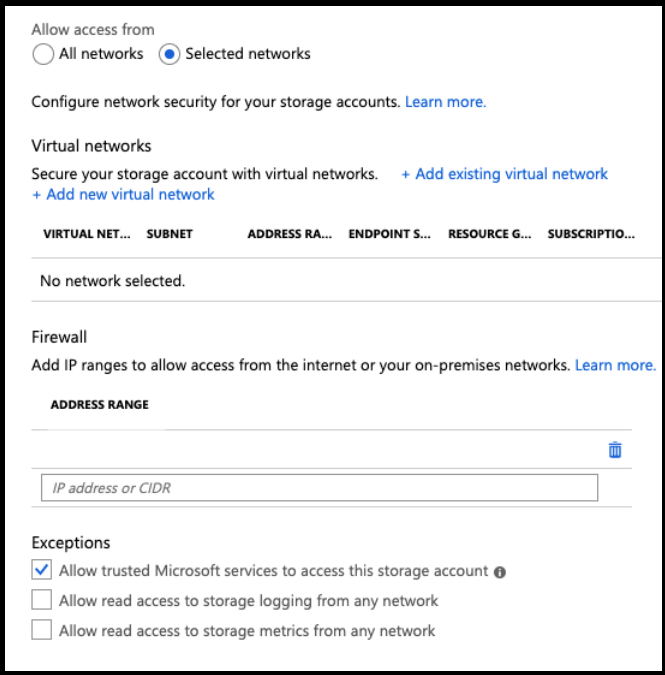
- Azure Backup
- Azure Data Box
- Azure DevTest Labs
- Azure Event Grid
- Azure Event Hubs
- Azure HDInsight
- Azure Monitor
- Azure Networking
- Azure Site Recovery
- Azure SQL Data Warehouse

Close

Resource Firewalls

VNets

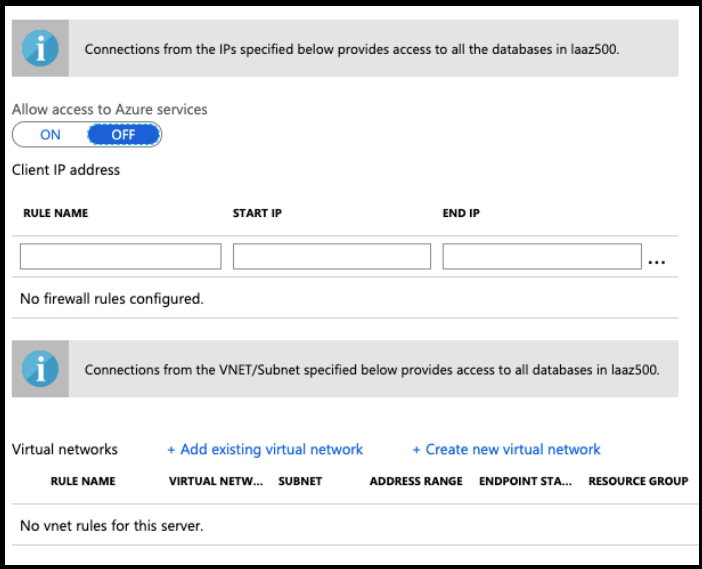
Azure Resource Firewalls: Storage Accounts



Close

VNets

Azure Resource Firewalls: SQL Servers



Close

Topics in this section include:

A **Endpoint Protection:**
Securing your hosts against viruses and malware.

B **Update Management:**
Keeping your Azure VMs up-to-date.

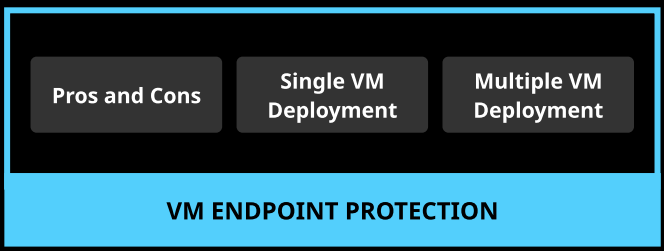
Endpoint Protection

Host Security: VM Endpoint Security

Microsoft Antimalware for Azure is a free real-time protection service that helps identify and remove viruses, spyware, and other malicious software. It generates alerts when known malicious or unwanted software tries to install itself or run on your Azure systems.

Features include:

- Real-time protection
- Malware remediation
- Signature updates
- Antimalware engine updates
- Antimalware platform updates
- Active protection
- Samples reporting
- Exclusions
- Antimalware event collection



Host Security

VM Updates

Topics in this section include:

A **Endpoint Protection:** Securing your hosts against viruses and malware.

B **Update Management:** Keeping your Azure VMs up-to-date.

VM Endpoint Protection: Pros and Cons

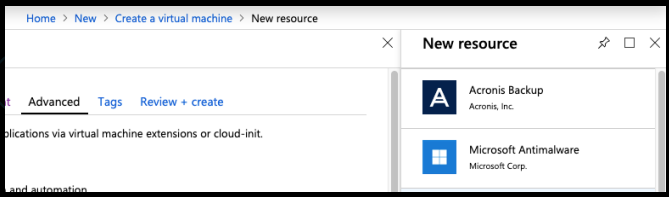
Advantages (Pros)	Disadvantages (Cons)
Free!!	Difficult to modify
Easy to deploy	Limited client availability
Fully featured	No centralized management

Close

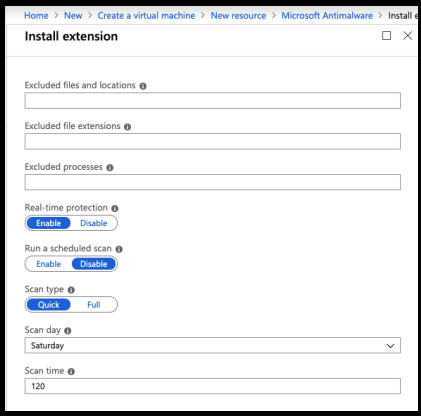
Endpoint Protection

Antimalware: Single VM Deployment

Configure and deploy Microsoft Antimalware using Azure extensions. This can be performed on new VM deployments as well as existing VMs.



Exclusions and protection parameters are specified at deployment.



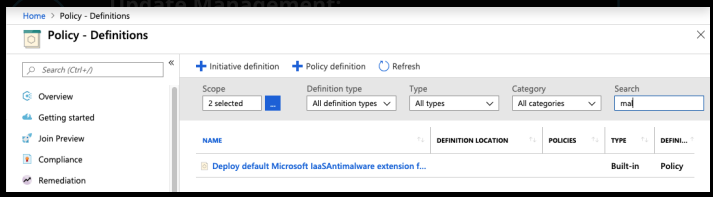
Close

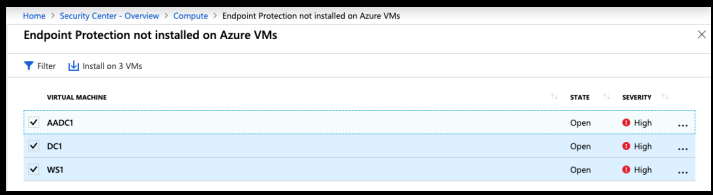
Endpoint Protection

Topics in this section include:

Antimalware: Multiple VM Deployment

Configure and deploy Microsoft Antimalware using Azure Policy or Azure Security Center.



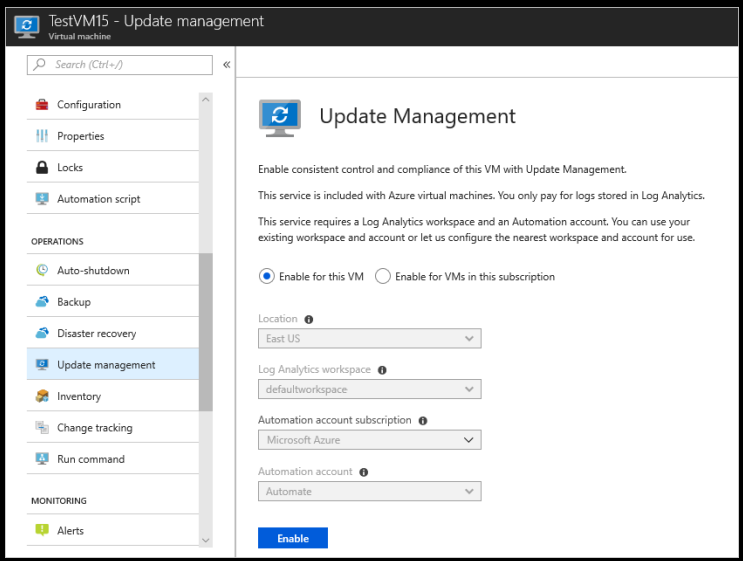


Close

Endpoint Protection

Host Security: Update Management

Azure provides the Update Management solution to allow you to manage updates and patches for your Windows Virtual Machines. The solution requires Azure Log Analytics and an Azure Automation Account. If these are not available at deployment, they can be provisioned for you.



Platform Protection

Securing Azure Resources

Topics in this section include:

A. **Role-based Access Control (RBAC) [Review]:** Managing permissions on Azure resources.

B. **Managed Identities [Review]:** Access to resources without credentials!

C. **Azure Resource Locks:** Preventing deletion of Azure resources.

D. **Management Groups:** Managing multiple subscriptions with ease!

E. **Azure Policies:** Automatically enforce compliance in Azure.

RBAC

Securing Azure Resources: RBAC [Review]

While Conditional Access and Identity Protection are used to control access to Azure AD managed resources, **role-based access control (RBAC)** is used to provide **granular access** to Azure resources.

These roles can be assigned at the **subscription, resource group,** or **resource** level.

- Azure includes a range of over 70 **built-in roles** for controlling access to Azure resources. Some examples are:
  - **Owner**: Includes full access to the assigned resource(s) including rights to grant access to others.
  - **Contributor**: Provides full access to the assigned resource(s) except for rights to change permissions.
  - **Reader**: Provides full view access to the assigned resource(s), but no ability to make changes.

For more information, refer to the **article on built-in roles for Azure resources**.

If the built-in roles are not sufficient, **custom roles** can be created.

- For roles to take affect, they must be assigned.
  - Roles are assigned to an **Azure AD user, group,** or **service principal**.
  - They must be assigned to something: a **subscription, resource group,** or **resource**.

AZ-300: RBAC

Securing Resources

Managed Identities

Back to Main

Securing Azure Resources: Managed Identities [Review]

Managed Identities provides a secure method for authenticating Azure resources against other Azure services **without needing to include credentials**. Managed Identities is a feature of Azure AD which specifically provides an Azure resource with a managed identity within Azure AD.

This feature provides the ability to authenticate an Azure resource "behind-the-scenes." This does not provide any implicit permissions (authorization) though. Those must be configured separately.

- **Avoids the need for application credentials to be stored** in code (e.g. Client ID and secrets).
- Is **fully managed by Microsoft**, so credentials no longer need to be rotated by developers.
- **Automates the creation and registration of an application** within Azure AD, Service Principal, and Client ID.
- Includes built-in functionality for Azure resources to **securely obtain an authentication token**.
- **Does not imply any authorization**, since the identity must still be granted whatever permissions are desired.

AZ-300: Managed IDs

Securing Resources

Resource Locks

Back to Main

Securing Azure Resources: Azure Resource Locks

We can use **Azure resource locks** to prevent other users in our organization from **accidentally deleting or modifying** critical resources such as a subscriptions, resource groups, or resources.

There are two types of resource locks:

- **CanNotDelete** means authorized users can still read and modify a resource, but they can't delete that resource.
- **ReadOnly** means authorized users can read a resource, but they can't delete or update it. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

When a resource lock is used at a parent scope, such as a subscription or resource group, **all resources within that scope inherit the same lock**. Resources added later inherit the lock from the parent. When a resource inherits multiple locks, the **most restrictive lock in the inheritance takes precedence**.

Unlike role-based access control, resource locks apply a restriction **across all users and roles**.

We must have access to **`Microsoft.Authorization/*`** or **`Microsoft.Authorization/locks/*`** actions to create or delete management locks. **Owner** and **User Access Administrator** are the only built-in roles granted those actions.

Securing Resources

Azure Policies

Back to Main

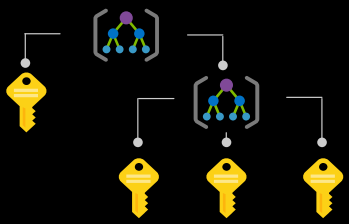
Securing Azure Resources: Management Groups

Azure **management groups** allow us to group subscriptions to manage **access, policies,** and **compliance**. Think of them as **one level above subscriptions**, but only for management. Billing responsibility is still handled on the subscription level.

Subscriptions within a management group **inherit the access, policies,** and **other compliance** factors applied to it. A management group **may contain individual subscriptions or other management groups** in a nested hierarchy.

You can create management groups and apply a policy requiring all Azure resources to be created in a particular Azure region for compliance purposes. Another management group can be used to determine access to multiple subscriptions (via RBAC), as opposed to granting access on the subscription level.

When using management groups, the first group is called the **Tenant Root Group** and is used to manage all subscriptions. If you are a Global Administrator, you can **elevate your access** to allow you to manage access to the root group.



Securing Resources

Azure Policies

Securing Azure Resources: Azure Policies

Azure Policy is a service in Azure you use to create, assign, and manage policies. These policies **enforce different rules and effects** over your resources so those resources stay compliant with your **corporate, technical,** or **government standards**.

For example, you can define the policy to **allow only a certain SKU size** of virtual machines in your environment. If an Azure administrator attempts to deploy a virtual machine outside one of your defined SKU sizes, **the deployment will fail validation and will not be deployed**.

Also, existing resources found to be non-compliant can be **remediated**.

Policy **definitions** outline the **specific criteria** to be evaluated. **Assignments** determine where these policies are applied. They can be applied to Azure subscriptions and optionally to child resource groups. Child resources **inherit the policy settings** applied to their parents.

Policy **initiatives** are **collections of policy definitions** designed to accomplish a singular goal, such as the overall compliance of corporate standards. They are assigned in the same manner as individual definitions.

Securing Resources

Security Operations

Back to Main

Platform Protection

Container Security

Course Navigation

- **Manage Identity and Access** — Section 1
- **Platform Protection** — Section 2
  - Network Security
  - Host Security
  - Securing Azure Resources
  - Container Security
- **Security Operations** — Section 3
- **Secure Data and Applications** — Section 4

Topics in this section include:

Configure and Secure Azure Container Registry
Protecting your image repositories the Azure way!

Container Instance Security
ACR Tasks and security considerations.

Container Groups
Container collections working together.

Container Vulnerability Management
Scan images for vulnerabilities.

Azure Kubernetes Service (AKS) Security
Best Practices for AKS.

Back to Main

Linux Academy

Azure Container Registry

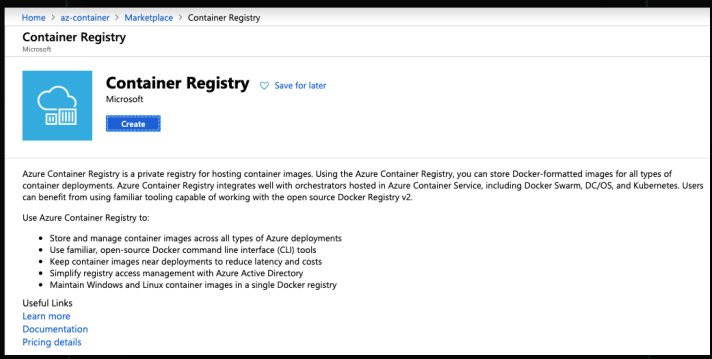
1. **Creating a Container Registry**
   - Azure Portal
   - Azure CLI
   - Azure PowerShell
2. **CR Authentication**
   - Accessing the registry
   - Azure AD
   - Service principals
   - Admin account
3. **Pushing an Image to the Registry**
   - Supported image formats
   - Pushing using Azure CLI
4. **Locks/VNet/ Firewall**
   - Locking a container image
   - Preventing deletion and update
   - VNet and Firewall rules

Close

Topics in this section include:

Azure Container Registry: Creating a Container Registry

Azure Portal



Azure CLI

```
az group create --name myResourceGroup --location eastus
az acr create --resource-group myResourceGroup --name
myContainerRegistry007 --sku Basic
```

Azure PowerShell

```
New-AzResourceGroup -Name myResourceGroup -Location EastUS
New-AzContainerRegistry -ResourceGroupName "myResourceGroup"
-Name "myContainerRegistry007" -EnableAdminUser -Sku Basic
```

Close

Topics in this section include:

Azure Container Registry: Security

1. **Azure AD**
   - Used when working with your registry directly.
   - Role-based access (AcrPull, AcrPush, Owner).

Container Instance Security
ACR Tasks and security considerations

2. **Service Principal**
   - Applications or services can use it for headless authentication.
   - Role-based access (AcrPull, AcrPush, Owner).

Container collections working together.

3. **Admin Account**
   - Designed for a single user to access the registry.
   - Full access to the registry.

Azure Kubernetes Service (AKS) Security
Best Practices for AKS.

Close

Topics in this section include:

Azure Container Registry: Pushing a Container Image

Azure CLI

Createaresourcegroup:

```
az group create --name myResourceGroup --location
eastus
```

Createacontainerregistry:

```
az acr create --resource-group myResourceGroup
--name myContainerRegistry008 --sku Basic
```

Logintotheregistry:

```
az acr login --name myContainerRegistry008
```

Pushimagetotheregistry:

```
1. docker pull hello-world
2. docker tag hello-world
myContainerRegistry008.azurecr.io/hello-world:v1
3. docker push
myContainerRegistry008.azurecr.io/hello-world:v1
```

Runimagefromtheregistry:

```
1. docker run
myContainerRegistry008.azurecr.io/hello-world:v1
```

Close

Topics in this section include:

Azure Container Registry: Lock/VNet/Firewall

Configure and Secure Azure Container Registry

1 **Locks**

- Similar to other Azure resource locks.
- Locks prevent deletion and updates.

ACR Tasks and security considerations.

2 **VNet/Firewall**

- Only resources in the virtual network access the registry.
- Firewall rules allow registry access only from specific IPs.

Container Vulnerability Management
Scan images for vulnerabilities.

Azure Kubernetes Service (AKS) Security
Best Practices for AKS.

Close

Azure Container Instances: Security

1. **ACR Tasks**
   - Automate container image builds and maintenance.
   - Tight control of images used in Container Instance deployment.
2. **Security Considerations**
   - Private registries.
   - Monitor and scan container images.
   - Protect credentials.
3. **Creating a Container Instance**
   - Authenticate with Azure Container Registry from Azure Container Instances.
4. **Content Trust**
   - Pushing and pulling of signed images.

Close

Topics in this section include:

Configure and Secure Azure Container Registry
Protecting your image repositories the Azure way!

Container Instance Security
ACR Tasks and security considerations.

Container Groups
Container instances working together.

Container Vulnerability Management
Scan images for [illegible].

Azure Kubernetes Service (AKS) Security
Best Practices for AKS.

Azure Container Instances: ACR Tasks

ACR Tasks is a suite of features within Azure Container Registry. It provides cloud-based container image building for Linux, Windows, and ARM. It can also **automate OS and framework patching** for our Docker containers.

- On-demand container image builds.
- Automated builds on source code commit or when a container's base image is updated.

Close

Topics in this section include:

Azure Container Instances: Security Considerations

Use private registries.

- **A publicly available container image does not guarantee security!**
- Docker trusted registry (on-premises).
- Azure Container registry (cloud-based).

Monitor and scan container images.

- Security monitoring and scanning solutions are available through the Azure Marketplace.
- Use them to scan container images in a private registry and identify potential vulnerabilities.
- **Scan before pushing!**

Protect credentials.

- Inventory all credential secrets.
- Require developers to use emerging secrets-management tools that are designed for container platforms.
- **Azure Key Vault.**

Close

Topics in this section include:

Azure Container Instances: Creating a Container Instance

Configure and Secure Azure Container Registry
Protecting your image repositories the Azure way!

Azure CLI

Createaserviceprincipal:

```
#!/bin/bash
ACR_NAME=mycontainerregistry
SERVICE_PRINCIPAL_NAME=acr-service-principal
ACR_REGISTRY_ID=$(az acr show --name $ACR_NAME --query
id --output tsv)
SP_PASSWD=$(az ad sp create-for-rbac --name
http://$SERVICE_PRINCIPAL_NAME --scopes $  ACR_REGISTRY_ID
--role acrpull --query password -  -output tsv)
SP_APP_ID=$(az ad sp show --id
http://$SERVICE_PRINCIPAL_NAME --query appId --output
tsv)

echo "Service principal ID: $SP_APP_ID"
echo "Service principal password: $SP_PASSWD"
```

Createacontainerinstance:

```
az container create \
--resource-group myResourceGroup \
--name mycontainer \
--image mycontainerregistry.azurecr.io/myimage:v1 \
--registry-login-server mycontainerregistry.azurecr.io \
--registry-username <service-principal-ID> \
--registry-password <service-principal-password>
```

Close

Topics in this section include:

Azure Container Instances: Content Trust

Azure Container Registry implements **Docker's content trust model**, enabling pushing and pulling of signed images.

Content trust is a feature of the **Premium SKU** of Azure Container Registry.

Content trust allows us to **sign the images** we push to our registry. Consumers of our images (people or systems pulling images from our registry) can configure their clients to **pull only signed images**. When an image consumer pulls a signed image, their Docker client **verifies the integrity** of the image.

Close

Azure Container Instances: Container Groups

A **container group** is a collection of containers that get scheduled on the same host machine. The containers in a container group **share a lifecycle, resources, local network, and storage volumes**. It's similar in concept to a **pod in Kubernetes**.

A container group is useful when building an application sidecar for **logging, monitoring, or any other configuration** where a service needs a second attached process.

Container groups

- Are deployed on a single VM.
- Only support Linux VMs.
- Can sit behind a public IP with optional exposed ports.
- Can be deployed via ARM or YAML.

Close

Azure Container Instances: Vulnerability Management

As mentioned in the Security Considerations lesson, vulnerability management is an important part of container security. Scanning containerized images for vulnerabilities of bad configurations is crucial to maintaining secure container instances.

Security monitoring and scanning solutions such as **Twistlock** and **Aqua Security** are available through the Azure Marketplace. These can be used to scan container images in a private registry and identify potential vulnerabilities.

Aqua Security

Twistlock

Close

Azure Kubernetes Service: Security

1. **Security Concepts**
   - Master security.
   - Node security.
   - Kubernetes secrets.

2. **Best Practices**
   - Secure access to the API server and cluster nodes.
   - Upgrade cluster.
   - Update nodes.

3. **Authenticating to ACR from AKS**
   - Security principals.
   - Kubernetes Secrets.

Close

Topics in this section include:

Azure Kubernetes Service: Security Concepts

Master security

- In AKS, the Kubernetes master components are part of the managed service provided by Microsoft. Each AKS cluster has its own single-tenanted, dedicated Kubernetes master to provide the API Server, Scheduler, etc.
- This master is managed and maintained by Microsoft.
- By default, the Kubernetes API server uses a public IP address with fully qualified domain name (FQDN). We can control access to the API server using Kubernetes role-based access controls and Azure Active Directory.

Node security

- AKS nodes are Azure virtual machines we manage and maintain.
- Linux nodes run an optimized Ubuntu distribution using the Moby container runtime.
- Windows Server nodes (currently in preview in AKS) run an optimized Windows Server 2019 release and also use the Moby container runtime.
- When an AKS cluster is created or scaled up, the nodes are automatically deployed with the latest OS security updates and configurations.

Kubernetes Secrets

- A Kubernetes Secret is used to inject sensitive data into pods, such as access credentials or keys.

Close

Topics in this section include:

Configure and Secure Azure Container Registry
Protecting your image repositories the Azure way!

Container Instance Security
ACR Tasks and security considerations.

Container Vulnerability Management
Scan images for [illegible].

Azure Kubernetes Service (AKS) Security
Best Practices for AKS.

Azure Kubernetes Service: Best Practices

- Secure access.
- Secure container access to resources.
- Regularly update to the latest version of Kubernetes.
- Process Linux node updates and reboots using kured.

Close

Azure Kubernetes Service: Authentication to ACR

Topics in this section include:

Azure CLI

GrantAKSaccesstoACR:

```
#!/bin/bash
AKS_RESOURCE_GROUP=myAKSResourceGroup
AKS_CLUSTER_NAME=myAKSCluster
ACR_RESOURCE_GROUP=myACRResourceGroup
ACR_NAME=myACRRegistry
# Get the id of the service principal configured for AKS
CLIENT_ID=$(az aks show --resource-group $AKS_RESOURCE_GROUP
--name $AKS_CLUSTER_NAME --query
"servicePrincipalProfile.clientId" --output tsv)
# Get the ACR registry resource id
ACR_ID=$(az acr show --name $ACR_NAME --resource-group
$ACR_RESOURCE_GROUP --query "id" --output tsv)
# Create role assignment
az role assignment create --assignee $CLIENT_ID --role
acrpull --scope $ACR_ID
```

AccesswithKubernetesSecrets:

```
#!/bin/bash
ACR_NAME=myacrinstance
SERVICE_PRINCIPAL_NAME=acr-service-principal
# Populate the ACR login server and resource id.
ACR_LOGIN_SERVER=$(az acr show --name $ACR_NAME --query
loginServer --output tsv)
ACR_REGISTRY_ID=$(az acr show --name $ACR_NAME --query id
--output tsv)
# Create acrpull role assignment with a scope of the ACR
resource.
SP_PASSWD=$(az ad sp create-for-rbac --name
http://$SERVICE_PRINCIPAL_NAME --role acrpull --scopes
$ACR_REGISTRY_ID --query password --output tsv)
# Get the service principal client id.
CLIENT_ID=$(az ad sp show --id
http://$SERVICE_PRINCIPAL_NAME --query appId --output tsv)
# Output used when creating Kubernetes secret.
echo "Service principal ID: $CLIENT_ID"
echo "Service principal password: $SP_PASSWD"
```

Close

Security Operations

Configuring Security Services

Topics in this section include:

Microsoft Azure Monitor [Review]
Keeping an eye on your Azure environment.

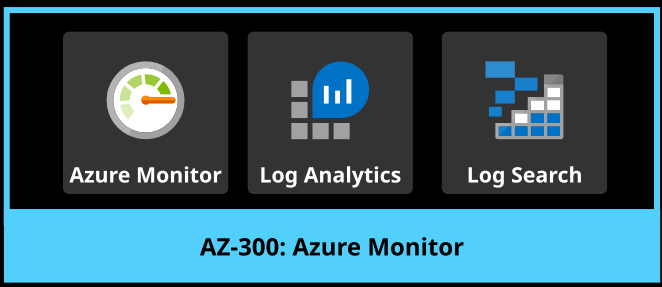
Diagnostic Logging and Log Retention
Working with your log data.

Topics in this section include:

Configuring Security Services: Azure Monitor [Review]

Monitoring is the act of collecting and analyzing data to determine the performance, health, and availability of our business application and the resources it depends on.

Monitoring in Azure is primarily provided by **Azure Monitor** which provides common stores for storing monitoring data, multiple data sources for collecting data from the different tiers supporting our application, and features for analyzing and responding to collected data **such as query and alert functionality.**



Close

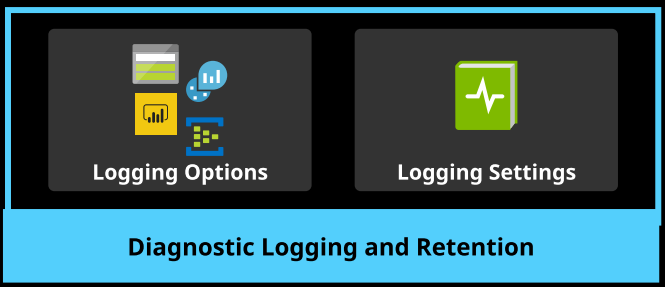
Topics in this section include:

Configuring Security Services: Diagnostic Logging and Retention

Diagnostic logs provide data about the operation of Azure resources. There are two different types of diagnostic logs.

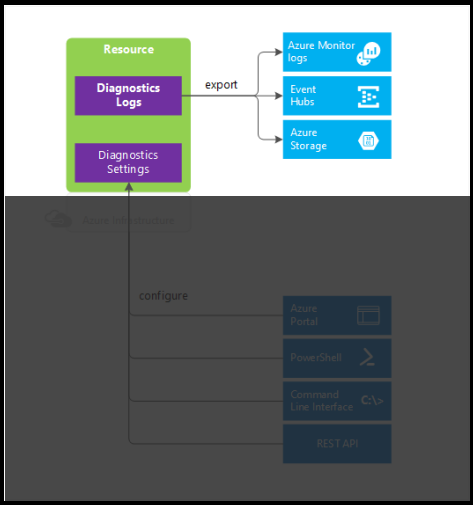
- **Tenant logs**: Logs originating from tenant-level services such as Azure Active Directory.
- **Resource logs**: Logs originate from resources within an Azure subscription, such as network security groups or Storage accounts.

These **do not include** the Azure Activity Log or any OS-level logging.



Close

Configuring Security Services: Logging Options

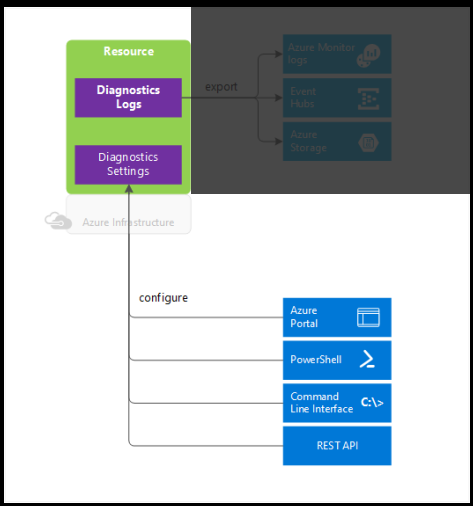


We have a few options available for working with diagnostic logs:

- Save them to a **Storage account** for auditing or manual inspection.
- Stream them to **event hubs** for ingestion by a custom analytics solution such as **Power BI**.
- Analyze them with **Azure Monitor**.

Close

Configuring Security Services: Logging Settings



Resource diagnostic logs are configured using **resource diagnostic settings**. Tenant diagnostic logs are configured using a **tenant diagnostic setting**. These settings determine:

- Diagnostic logs and metrics destinations.
- Log categories and metric data options.
- Retention time (**Storage account only**).

Close

Topics in this section include:

Just in Time VM Access Using Microsoft Azure Security Center
VM access only when required.

Configuring Security Policies: Just in Time VM Access Using Azure Security Center

Just-in-time (JIT) virtual machine (VM) access allows us to lock down access to our Azure virtual machines, allowing access only when required by our support personnel or other users.

Azure Security Center standard is required to configure this feature.

Security Center just-in-time VM access currently **supports only VMs deployed through Azure Resource Manager**.

To create or edit a JIT policy:

- `Microsoft.Security/locations/jitNetworkAccessPolicies/write` (subscription or resource group)
- `Microsoft.Compute/virtualMachines/write` (subscription, resource group, or VM)

To request JIT access:

- `Microsoft.Security/locations/{the_location_of_the_VM}/jitNetworkAccessPolicies/initiate/action` (subscription or resource group)
- `Microsoft.Compute/virtualMachines/read` (subscription, resource group, or VM)

Close

Topics in this section include:

Reviewing and Responding to Alerts and Recommendations

Microsoft Azure Security Center Playbooks

Topics in this section include:

Security Alerts: Reviewing and Responding to Alerts and Recommendations

Security Alerts:
Based on data collected by Azure Security Center, threats are detected. For each threat, an alert is generated.

A list of alerts is shown in **Security Center** along with the information we need to quickly investigate the problem and recommendations for how to remediate an attack.

Recommendations:
Recommendations are actions to take to secure our resources. The recommendations are based on best practices and trusted security advisories.

Each recommendation provides the following:

- A description.
- Remediation steps.
- Affected resources.
- Secure score impact.

Close

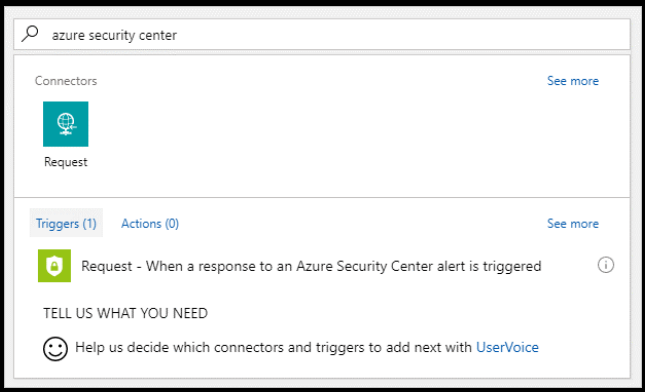
Topics in this section include:

Security Alerts: Microsoft Azure Security Center Playbooks

A security playbook is simply a collection of procedures. These procedures are executed when a playbook is triggered. Security alerts are the trigger that starts playbook running.

Playbooks can help us craft and execute automated responses to security alerts, helping us manage our Azure environment with little administrative effort.

Security playbooks in **Security Center** are based on Azure Logic Apps.



Close

Secure Data and Applications

Data Security

Course Navigation

Topics in this section include:

Data Classification Using Azure Information Protection

Storage Analytics Data Retention Policies

Data Sovereignty with Azure Policy

Back to Main

Topics in this section include:

Data Classification Using Azure Information Protection

- What Is Azure Information Protection (AIP)?
- AIP Permissions
- Labelling Data in AIP

Close

Secure Data and Applications

Data Security

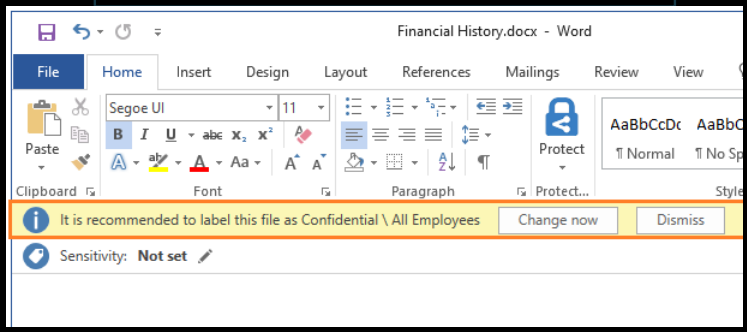
Topics in this section include:

Data Classification using Azure Information Protection: What is AIP?

Azure Information Protection (AIP) is a cloud-based rights management solution that helps our organization **classify and protect** documents and emails.

Classification is achieved by applying **labels**. Labels determine the confidentiality of the data based on conditions that can be set by administrators or optionally by end users. AIP can also recommend certain labels be applied to documents and emails based on the type of data created.

Azure Active Directory Premium P1 or P2 licenses are required to use AIP. A comparison of AIP features can be found **here**.



AIP in Microsoft Word

Close

Topics in this section include:

Data Classification Using Azure Information Protection

Data Classification Using Azure Information Protection: Permissions

AIP includes several built-in permission sets for access to labeled data. These roles can be applied to members of our Azure Active Directory as well as external recipients (specified by internet domain name).

- **Co-Owner**
- **Co-Author**
- **Reviewer**
- **Viewer**
- **Custom**

Close

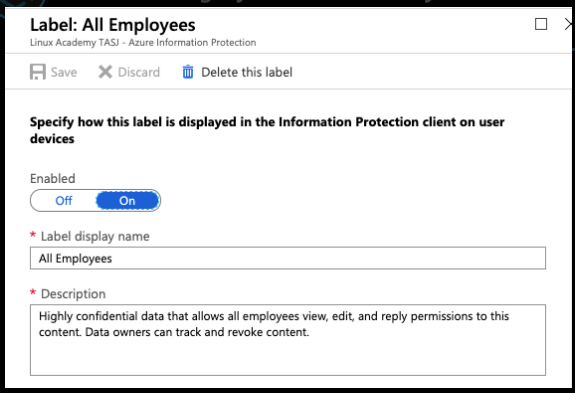
Topics in this section include:

Data Classification using Azure Information Protection: Labelling

In AIP, labels determine the classification of a piece of data. Data labelled "General" is not protected and can be distriuted inside and outside of an organization, whereas data labelled "Confidential" cannot. Labels can be applied manually to a piece of data or can be applied automatically based on conditions, such as the data format.

AIP contains 100 preconfigured conditions, or we can create our own based upon a regular expression.

Applying conditions to a label requires Azure Active Directory P2 licensing.



Close

Topics in this section include:

Storage Analytics Data Retention Policies

In our Diagnostic Logging and Retention lesson, we discussed the ability to configure the retention settings on Azure Storage Accounts. If we wish to retain our storage analytics logging data, then there are a few things we should take note of.

- By default, Storage Analytics **will not delete** any logging or metrics data.
- Blobs and table entities **will continue to be written** until the shared 20TB limit is reached.
- Once the 20TB limit is reached, **Storage Analytics will stop writing new data** and will not resume until free space is available.

To better manage this data, we can **create a retention policy.** Retention policies can be created via the REST API or in the Azure Portal.

Close

Secure Data and Applications

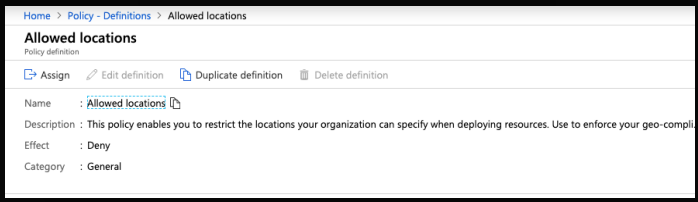
Data Security

Topics in this section include:

Data Sovereignty with Azure Policy

Sometimes, due to governmental or other regulations, it is necessary to ensure our organizational data resides in a particular country of origin. In Azure, we are able to create Azure resources in regions located all over the world. To enforce data sovereignty, we can use Azure Policy to enforce where Azure resources and the data contained therein are located.

Azure Policy contains many preconfigured policies to assist us with our compliance goals. One of these determines allowed locations where Azure resources can be deployed.



Azure Allowed Locations Policy

Close

Secure Data and Applications

Azure Key Vault

Course Navigation

Topics in this section include:

What Is Azure Key Vault?

Managing Access to Key Vault, Secrets, Certificates, and Keys

Managing Certificates and Secrets

Back to Main

Secure Data and Applications

Azure Key Vault

Topics in this section include:

What is Azure Key Vault?

Azure Key Vault helps safeguard and manage keys for cryptography and secrets used by Azure applications and services.

With Azure Key Vault, we can perform the following tasks:

- Securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets.
- Create and control the encryption keys used to encrypt data.
- Provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with internal connected resources.
- Azure Resource Manager templates can access secrets and keys stored in key vault during deployment of other Azure resources.

Close

Secure Data and Applications

Azure Key Vault

Topics in this section include:

Managing Access to Key Vault, Secrets, Certificates, and Keys

Because Azure Key Vault data is sensitive and business critical, we need to secure access to our key vaults by allowing only authorized applications and users.

Access to Azure Key Vault is controlled by an access policy. Access policies determine what privileges are granted for keys, secrets, and certificates stored in Key Vault.

RBAC is also used to determine access to the Key Vault resource.

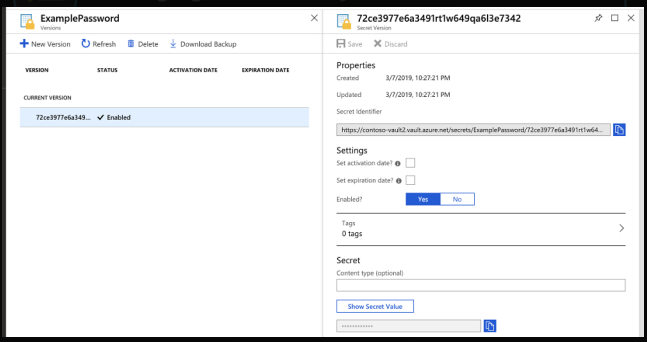
Close

Back to Main

Topics in this section include:

Managing Certificates and Secrets

We can use the Azure Portal, PowerShell, and the CLI to set and retrieve both secrets and certificates from Azure Key Vault.



Key Vault in the Azure Portal

Close

Secure Data and Applications

Security for Data Infrastructure

Course Navigation

Topics in this section include:

Database Authentication and Auditing

Azure SQL Database Threat Protection

Managing Access Control and Keys for Storage Accounts [Review]

Security for HDInsights

Security for Cosmos DB

Security for Microsoft Azure Data Lake

Back to Main

Secure Data and Applications

Security for Data Infrastructure

Course Navigation

- **Manage Identity and Access** Section 1
- **Platform Protection** Section 2
- **Security Operations** Section 3
- **Secure Data and Applications** Section 4
  - **Data Security**
  - **Azure Key Vault**
  - **Security for Data Infrastructure**
  - Encryption for Data at Rest
  - Security for Application Delivery

Topics in this section include:

- Database Authentication and Auditing
- Azure SQL Database Threat Protection
- SQL Database Authentication with Azure AD
- Managing Access Control and Keys for Storage Accounts [Review]
- SQL Database Auditing
- Security for HDInsights
- Security for Cosmos DB
- Security for Microsoft Azure Data Lake

Database Authentication and Auditing

Close

Back to Main

Linux Academy

Secure Data and Applications

Security for Data Infrastructure

Topics in this section include:

Database Authentication and Auditing:

SQL Database Authentication with Azure AD

By default, Azure SQL databases, managed instances, and data warehouses use local user accounts for authentication. When one of the above mentioned resources is initially deployed, a SQL server account is created for administration (**think SA account in MS SQL Server**).

Azure Active Directory can be configured to simplify authentication to any of these resources,. Benefits to Azure AD authentication are:

- **Single user account for DB authentication.**
- **Password strength based on Azure AD policies.**
- **Support for ADFS authentication.**
- **Support for MFA.**
- **Use of SQL management tools with Azure AD authentication.**

In order to integrate with Azure AD, **an Azure AD administrator must be assigned** to the SQL database, managed instance, or data warehouse. This can be either a user or group object. This user or group can assign other Azure AD users and groups to SQL resources.

Close

Secure Data and Applications

Security for Data Infrastructure

Topics in this section include:

Database Authentication and Auditing:

SQL Database Auditing

Auditing SQL databases and data warehouses helps us **maintain compliance and gain insight** into the activity in these critical Azure resources.

We can use SQL auditing to **retain auditing data** of events pertaining to our SQL databases, **create reports** on database activity, and **analyze these reports** with Azure Monitor to discover unusual events and activities.

SQL audit logs can be configured for the SQL server as a whole or at the individual database level. If you define server-level auditing, **database-level auditing will be enabled as well**. If you audit both server-level and database-level components, then **some audit data will be captured twice**. Be careful when doing this, as you could deplete the space allocated for auditing data in your Azure storage account. See **Diagnostic Logging and Retention** for more information.

Auditing logs can be sent to **Azure storage accounts**, **Log Analytics** (to be used by Azure Monitor), or **Event Hub** (to be ingested by a third-party solution or Power BI).

Logging can be configured using the Azure Portal, PowerShell, the REST API, or ARM templates.

Close

Back to Main

Secure Data and Applications

Security for Data Infrastructure

Topics in this section include:

Database Authentication and Auditing

Azure SQL Database Threat Protection

Advanced Threat Protection, part of Advanced Data Security in SQL databases, can help protect your Azure SQL infrastructure by detecting and alerting on activities indicating unusual and potentially harmful attempts to access or exploit databases.

Advanced Threat Protection can identify potential SQL injections, access from an unusual location or data center, access from an unfamiliar principal or potentially harmful application, and brute force SQL credentials.

Notifications on alerts can be viewed in the Azure Portal or e-mailed.

Advanced data security is a premium service that entails additional cost. Refer to Azure pricing for more information.

Close

Security for Cosmos DB

Security for Microsoft Azure Data Lake

Topics in this section include:

Managing Access Control and Keys for Storage Accounts [Review]

Azure storage accounts are the repositories for data accessed by users, applications, and other Azure services. Locking down these storage accounts is a critical component of Azure security.

We can use several different methods for securing storage accounts. We can utilize access keys, which grant the user full control to the entire storage account.

We can also use shared access signatures (SAS), which grant fine-grained access to storage account services. For example, we can apply an SAS to grant read-only access to a blob container within a storage account.

AZ-300 Blueshift Guide

Close

Secure Data and Applications

Security for Data Infrastructure

Topics in this section include:

Security for HDInsight

Enterprise Security Package (ESP) clusters provide multi-user access on Azure HDInsight clusters. HDInsight clusters with ESP are connected to a domain so domain users can use their domain credentials to authenticate with the clusters and run big data jobs.

In order to create an HDInsight cluster with ESP, Azure Active Directory Domain Services (Azure AD DS) must be deployed in our Azure tenant.

Once enabled, a managed identity for the HDInsight cluster must be created and assigned the HDInsight Domain Services Contributor role in the AD DS instance.

Once these prerequisites are complete, the HDInsight cluster with ESP can be deployed in Azure.

Microsoft: HDInsight with ESP

Close

Secure Data and Applications

Security for Data Infrastructure

Topics in this section include:

Security for Cosmos DB

Azure Cosmos DB uses two types of keys to authenticate users and provide access to its data and resources:

- Master keys: used for administrative resources such as database accounts, databases, users, and permissions.
- Resource tokens: used for application resources such as containers, documents, attachments, stored procedures, triggers, and UDFs.

Each account consists of two master keys: a primary key and a secondary key. The purpose of dual keys is so we can regenerate or roll keys, providing continuous access to our account and data.

We can use a resource token (by creating Cosmos DB users and permissions) when we want to provide access to resources in our Cosmos DB account to a client that cannot be trusted with the master key.

Microsoft: Azure Cosmos DB

Close

Secure Data and Applications

Security for Data Infrastructure

Topics in this section include:

- Database Authentication and Auditing
- Azure Storage Access Control and Keys for Storage Accounts [Review]
- Security for Cost Insights
- Security for Microsoft Azure Data Lake

Security for Microsoft Azure Data Lake

Securing data in Azure Data Lake Storage uses a combination of Azure AD role-based permissions and access control lists within the Data Lake file system.

- AAD security principals control access to the Data Lake Storage Gen1 account from the portal and management operations from the portal or through APIs.
- These principals also regulate access control on the data stored in Data Lake Storage Gen1.
- We can also lock down access to the Data Lake at the network level by using a resource firewall.

Close

Secure Data and Applications

Encryption for Data at Rest

Topics in this section include:

Microsoft Azure SQL Database Always Encrypted

Database Encryption [Review]

Storage Service Encryption

Disk Encryption

Backup Encryption

Back to Main

Secure Data and Applications

Encryption for Data at Rest

Topics in this section include:

Microsoft Azure SQL Database Always Encrypted

Always Encrypted is a data encryption technology in Azure SQL Database and SQL Server that helps protect sensitive data at rest on the server, during movement between client and server, and while the data is in use. This ensures sensitive data never appears as plaintext inside the database system.

After we encrypt data, only client applications or app servers that have access to the keys can access plaintext data.

Always Encrypted is configured in SQL Server Management Studio using the Always Encrypted Wizard.

We can use Always Encrypted to encrypt entire databases or individual columns and rows within the database.

Close

Secure Data and Applications

Encryption for Data at Rest

Topics in this section include:

Database Encryption [Review]

Database encryption is available for Azure SQL Server, SQL Database, SQL Data Warehouse, Cosmos DB, and Data Lake using various technologies.

In Linux Academy's **Microsoft Azure Exam DP-200 - Implementing an Azure Data Solution** course, Brian Roehm explains how encryption is achieved for each type of Azure database solution.

DP-200: Diagram

Close

Secure Data and Applications

Encryption for Data at Rest

Topics in this section include:

Storage Service Encryption

Azure Storage automatically encrypts your data with 256-bit AES encryption. Data in Azure Storage is encrypted and decrypted transparently.

Azure Storage encryption is enabled for all new and existing storage accounts and cannot be disabled.

All Azure Storage account tiers and deployment models are encrypted.

Azure customers have a choice of choosing Microsoft to manage the encryption key for storage accounts, or we can provide our own key and manage the key using Azure Key Vault.

Customer-managed keys can be configured using the Azure Portal, PowerShell, and the Azure CLI.

Close

Secure Data and Applications

Encryption for Data at Rest

Topics in this section include:

Disk Encryption

Azure customers can choose to encrypt their Virtual Machine managed disks to protect data.

Azure uses **BitLocker disk encryption for Windows** managed disks and **DM-Crypt disk encryption for Linux managed disks**.

Standard and premium disks can benefit from disk encryption.

We can use **Azure Security Center** to be alerted of any virtual machines not utilizing disk encryption and view instructions on how to encrypt these disks.

Azure Key Vault can be used to manage keys used to encrypt disks. **Azure Disk Encryption requires that your key vault and VMs reside in the same Azure region and subscription.**

Supported Operating Systems

Close

Secure Data and Applications

Encryption for Data at Rest

Topics in this section include:

Microsoft Azure SQL Database Always Encrypted

Database Encryption [Review]

Storage Service Encryption

Disk Encryption

Backup Encryption

Disk Encryption

Supported Operating Systems

Windows:

- Workstation: Windows 8 and later
- Server: Windows Server 2008 R2 and later

Linux:

- Ubuntu: 14.04.5, 16.04, 18.04
- RHEL: 6.7, 6.8, 7.2 - 7.6
- CentOS: 6.8, 7.2n, 7.3 - 7.6
- openSUSE: 42.3
- SLES: 12-SP3,SP4

Close

Topics in this section include:

Backup Encryption

Backups in Azure are encrypted with AES-256 encryption and are transmitted to the Azure Backup vault using secure HTTPS communication.

Azure backups are encrypted at rest by default. No configuration is necessary to enable this feature.

- On-premise backups use the passphrase configured when installing the Azure Backup client.
- Azure VMs are encrypted at rest using Storage Service Encryption.

If the passphrase created at client installation is lost, then the backup data is unrecoverable.

Azure Key Vault can be used to store Azure backup passphrases as secrets.

Close

Secure Data and Applications

Security for Application Delivery

Course Navigation

Topics in this section include:

Implementing Security Validations for Application Development

Synthetic Security Transactions to Monitor Site Availability

SSL/TLS Certificates

Protecting Web Apps

Back to Main

Secure Data and Applications

Security for Application Delivery

Topics in this section include:

Implementing Security Validations for Application Development

Application development using PaaS resources allows easier deployment of web and mobile applications, as we, the end user, are **no longer responsible for items such as physical infrastructure and networking**.

This is not to say that security is no longer of importance when developing and deploying PaaS-based applications. Caution must be taken when securing these applications, **which by design are more vulnerable** than on-premises applications.

Some best practices for securing PaaS applications:

- Adopt a policy of **identity** as the primary security perimeter.
- **Secure your keys and credentials** to secure your PaaS deployment.
- **Manage your PaaS resources directly** whenever possible.
- Use strong authentication and authorization.
- Use a web application firewall.
- Monitor app performance.
- Perform penetration testing.

Close

Secure Data and Applications

Security for Application Delivery

Topics in this section include:

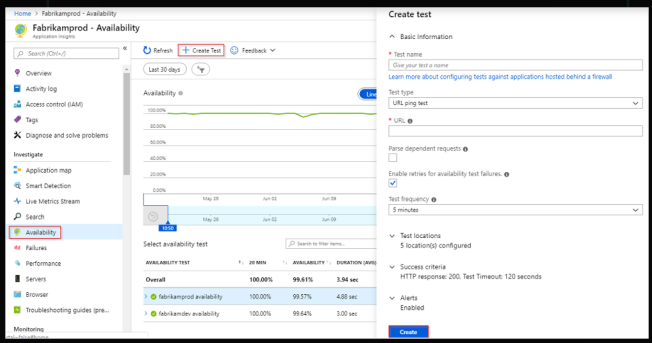
Synthetic Security Transactions to Monitor Site Availability

Azure Application Insights can be used to monitor App Service by running recurring tests to monitor availability and responsiveness.

Performance and availability issues could be a result of underlying security problems, so it is recommended to run these tests often.

There are three types of availability tests:

- **URL ping test**
- **Multi-step web test**
- **Custom track availability tests**



Close

Secure Data and Applications

Security for Application Delivery

Topics in this section include:

Implementing Security Validations for Application Development

Synthetic Security Transactions to Monitor Site Availability

SSL/TLS Certificates

Securing Web Apps

SSL/TLS Certificates

Private and public SSL certificates can be used to secure communication on Azure Web Apps. Combined with custom domains, we can give our applications a "vanity" namespace for user access.

App Service Plans in the Basic, Standard, Premium, or Isolated tiers are required to use custom SSL certificates.

Certificates can be managed with the Azure Portal, CLI, or PowerShell.

Close

Secure Data and Applications

Security for Application Delivery

Topics in this section include:

Protecting Web Apps

Azure Web Apps can be protected by deploying other Azure resources such as Application Gateway and Web App Firewall in front of your web apps.

Application Gateways provide network load balancing and traffic management for Azure virtual machines, virtual machine scale-sets, and app services. With an application gateway, we can configure **URL-based routing and multi-site hosting** along with other features to increase the availability of web applications.

Web application firewall (WAF) is a feature of Application Gateway that provides **centralized protection of our web applications** from common exploits and vulnerabilities. WAF is based on rules from the **OWASP (Open Web Application Security Project) core rule sets 3.0 or 2.2.9**.

Close

Course Navigation

Manage Identity and Access
Section 1

Platform Protection
Section 2

Security Operations
Section 3

Secure Data and Applications
Section 4

The AZ-500 Exam

About the Exam:

Length: 180 Minutes

- Number of Questions: ~40
- Format:
  - Case study
  - Drag and drop
  - Exhibit
  - True or false

Cost: $165.00 USD

Register for the Exam:

https://www.microsoft.com/en-us/learning/exam-az-500.aspx

The exam can be taken at a local test center, at your home office, or at a Pearson VUE test center. If you choose at home or office, you must have the following system requirements:
https://www.microsoft.com/en-us/learning/online-exams.aspx

Preparing for the Exam:

- Watch and follow along with all the video lessons.
- Complete every hands-on lab at least twice.
- Take and pass the practice exam at least twice.
- Memorize the flashcard deck and create your own to increase memorization.
- Review the interactive diagram and understand the concepts.
- Participate in the Linux Academy community.
- Participate in a Linux Academy study group or start your own!

Back to Main