PROJECT
Privileged Identity Management

Plan and implement privileged access:

1. Overview and setup prerequisites for roles and licenses.
2. Explore Just-In-Time.
3. Configure Azure roles in Privileged Identity Management (PIM), including settings and assignments.
4. Configure Azure resources in PIM, including settings and assignments.
4. Configure Privileged Access groups.
5. Set up PIM requests and approval process.
6. Analyze PIM audit history and reports.
7. Create and manage break-glass accounts.
8. Explore Eligible and Active Roles.
10. Set the time limit of the Roles.

R&D Document: Planning and Implementing Privileged Access with Just-In-Time Access

Introduction

Privileged Access Management (PAM) is essential for securing critical systems and sensitive information within an organization. This document provides an overview and setup prerequisites for roles and licenses, explores Just-In-Time (JIT) access, and details steps for configuring Azure resources in PIM, setting up privileged access groups, PIM requests and approval processes, analyzing PIM audit history, managing break-glass accounts, and exploring eligible and active roles with time limits.

1. Overview and Setup Prerequisites for Roles and Licenses

Overview

Privileged access involves granting administrative or elevated permissions to users who need to perform critical tasks. Proper management of privileged access reduces the risk of security breaches by ensuring that only authorized personnel can access sensitive systems and data.

Setup Prerequisites

1.1. Roles and Responsibilities

Before implementing PAM, it's crucial to define roles and responsibilities within your organization:

- **Privileged Role Administrator**: Manages privileged roles and access policies.
- **Global Administrator**: Has full access to all administrative features.
- **Security Administrator**: Manages security-related settings and features.
- **Compliance Administrator**: Oversees compliance policies and audit logs.

1.2. Licenses

Ensure you have the appropriate licenses for implementing PAM and JIT access. Microsoft Azure Active Directory (Azure AD) provides Privileged Identity Management (PIM) capabilities, which require specific licenses:

- **Azure AD Premium P2**: Required for using Azure AD PIM.
- **Microsoft 365 E5**: Includes Azure AD Premium P2 features.

1.3. Azure AD PIM Setup

To set up Azure AD PIM, follow these steps:

Assign Licenses:

- In the Azure portal, go to Azure Active Directory > Licenses.
- Assign the Azure AD Premium P2 licenses to the users who will manage and use PIM.

Enable PIM:

- In the Azure portal, go to Azure Active Directory > Privileged Identity Management.
- Select Get started to enable PIM.

Configure PIM Settings:

- Navigate to Privileged Identity Management > Azure AD roles.
- Select Settings to configure role settings, including activation duration, notifications, and multi-factor authentication (MFA) requirements.

2. Explore Just-In-Time (JIT) Access

Overview

Just-In-Time (JIT) access minimizes the risk associated with standing privileged access by granting permissions only when needed and for a limited time. This approach reduces the attack surface and helps prevent unauthorized access.

Implementing JIT Access

2.1. Role Activation

Configure Role Settings:

- In PIM, select the role you want to configure for JIT access (e.g., Global Administrator).
- Set the Activation maximum duration to define how long a user can have elevated access (e.g., 1 hour).

Require Approval for Activation:

- For highly sensitive roles, enable Require approval to activate.
- Specify the approvers who can approve activation requests.

Multi-Factor Authentication (MFA):

- Enforce MFA for role activation to add an extra layer of security.
- In PIM settings, enable Require MFA to activate.

2.2. Role Assignment

Eligible Assignments:

- Assign users as Eligible for roles rather than Active. This means they can activate the role when needed but do not have continuous access.
- Navigate to Azure AD roles in PIM, select the role, and assign users as Eligible.

Activate Roles:

- Users can activate their eligible roles by going to the My roles section in PIM.
- They need to provide a justification for the activation and complete the MFA prompt if required.

Access Reviews:

- Regularly review and audit role activations to ensure compliance.
- Set up access reviews in PIM to periodically check if users still need their eligible roles.

Monitoring and Auditing

Audit Logs:

- Monitor audit logs to track role activations and access changes.
- In the Azure portal, go to Azure Active Directory > Audit logs.

Alerts and Notifications:

- Configure alerts to notify administrators of unusual activities or critical changes.
- In PIM settings, set up notifications for role activations and access reviews.

Best Practices

Least Privilege Principle:

- Assign the minimum necessary permissions to users.
- Regularly review and adjust roles to ensure they align with current job functions.

Regular Access Reviews:

- Conduct periodic access reviews to validate the necessity of privileged roles.
- Revoke access for users who no longer need elevated permissions.

Separation of Duties:

- Implement separation of duties to prevent conflicts of interest and reduce the risk of insider threats.
- Ensure that critical tasks require multiple approvals or are divided among different users.

3. Configuring Azure Roles in Privileged Identity Management (PIM)

Steps to Configure Azure Roles in PIM

1. Enable PIM

Sign in to the Azure Portal:

1. Go to the Azure Portal

Navigate to Azure AD:

1. Select Azure Active Directory from the left-hand menu.

Access PIM:

1. In the Azure AD overview, select Privileged Identity Management from the menu.

Get Started with PIM:

1. If this is your first time using PIM, select Get started and follow the prompts to enable PIM for your directory.

2. Configure Azure AD Roles

2.1. Configure Role Settings

Navigate to Azure AD Roles:

1. In the PIM dashboard, select Azure AD roles.

Select a Role to Configure:

1. Browse the list of roles and select the role you want to configure (e.g., Global Administrator, User Administrator).

Role Settings:

1. In the role's settings, configure the following:

    1. **Activation maximum duration**: Specify the maximum time a user can be in an active role session (e.g., 1 hour, 4 hours).
    2. **Require MFA**: Enforce multi-factor authentication for role activation.
    3. **Require approval to activate**: Enable this setting if role activation requires approval from specified approvers.
    4. **Notifications**: Set up notifications for role activations and expirations.

Save Settings:

1. Click Save to apply the changes.

2.2. Assign Users to Roles

Add Eligible Assignments:

1. In the PIM dashboard, select Azure AD roles and then Roles.
2. Choose the role you want to assign and click + Add assignments.

Select Users or Groups:

1. In the Add assignments pane, select the users or groups to assign the role.
2. Set the Assignment type to Eligible.

Configure Assignment Duration:

1. Specify the start and end dates for the assignment, if applicable.
2. Click Assign to complete the assignment.

3. Configure Azure Resource Roles

3.1. Enable PIM for Azure Resources

Navigate to Azure Resources:

1. In the PIM dashboard, select Azure resources.

Select a Subscription:

1. Browse and select the subscription or resource group you want to manage with PIM.

Enable PIM:

1. Follow the prompts to enable PIM for the selected subscription or resource group.

3.2. Configure Resource Role Settings

Select a Role:

1. In the Azure resources section, choose the role you want to configure (e.g., Owner, Contributor).

Role Settings:

1. Configure the settings for the selected role, similar to the Azure AD roles:
    1. **Activation maximum duration**
    2. **Require MFA**
    3. **Require approval to activate**
    4. **Notifications**

Save Settings:

1. Click Save to apply the changes.

3.3. Assign Users to Resource Roles

Add Eligible Assignments:

1. Select the resource role you want to assign and click + Add assignments.

Select Users or Groups:

1. Choose the users or groups to assign the role.
2. Set the Assignment type to Eligible.

Configure Assignment Duration:

1. Specify the start and end dates for the assignment, if applicable.
2. Click Assign to complete the assignment.

4. Monitor and Review

Access Reviews:

1. In the PIM dashboard, navigate to Access reviews.
2. Set up periodic reviews to ensure that users still need the roles they have been assigned.

Audit Logs:

1. Monitor audit logs for role activations, assignments, and other activities.
2. In the Azure portal, go to Azure Active Directory > Audit logs.

Alerts and Notifications:

1. Configure alerts and notifications for unusual activities or critical changes.
2. Set up notifications in the PIM settings for role activations and access reviews.

4. Configure Azure Resources in PIM

4.1. Configure Settings

Navigate to Azure AD PIM:

- In the Azure portal, go to Azure Active Directory > Privileged Identity Management.

Configure Resource Settings:

- Select Azure resources and choose the subscription or resource group you want to manage.
- Configure settings such as MFA, approval requirements, and activation duration for each resource.

4.2. Assign Users to Roles

1. **Assign Eligible Roles**:

   - In PIM, navigate to Azure AD roles or Azure resources.
   - Select the role and click Add assignments.
   - Choose the users or groups and set them as Eligible for the role.

5. Configure Privileged Access Groups

5.1. Create and Configure Groups

Create a New Group:

- In the Azure portal, go to Azure Active Directory > Groups.
- Click New group, select Security, and provide a name and description.

Enable PIM for the Group:

- Navigate to Azure AD PIM, select Azure AD roles, and then Groups.
- Enable PIM for the group and configure settings such as activation duration, MFA, and approval requirements.

5.2. Assign Members to the Group

1. **Add Eligible Members**:

   - In PIM, select the group and click Add assignments.
   - Choose the users or groups to be added as Eligible members.

6. Set Up PIM Requests and Approval Process

6.1. Configure Approval Workflow

1. **Set Up Approvers**:

   - In PIM, navigate to Azure AD roles or Azure resources.
   - Select the role, go to Settings, and enable Require approval to activate.
   - Specify the users or groups who will act as approvers.

6.2. Submit and Approve Requests

Submit Activation Requests:

- Eligible users can request activation by going to My roles in PIM and selecting the role to activate.
- Provide justification and complete MFA if required.

Approve or Deny Requests:

- Approvers receive notifications of requests and can approve or deny them in the PIM portal.

7. Analyze PIM Audit History and Reports

7.1. Access Audit Logs

1. **View Audit Logs**:

   - In the Azure portal, go to Azure Active Directory > Audit logs.
   - Filter logs to view activities related to PIM, such as role activations and assignments.

7.2. Generate Reports

1. **Generate PIM Reports**:

   - In PIM, navigate to Reports.
   - Generate and export reports on role assignments, activations, and access reviews for analysis.

8. Create and Manage Break-Glass Accounts

8.1. Create Break-Glass Accounts

1. **Create Emergency Accounts**:

   - In the Azure portal, go to Azure Active Directory > Users.
   - Create accounts with a descriptive name (e.g., BreakGlassAdmin).

8.2. Secure and Monitor Break-Glass Accounts

Secure Break-Glass Accounts:

- Assign minimal roles and permissions necessary for emergency use.
- Store credentials securely and restrict access.

Monitor Usage:

- Regularly monitor audit logs for any use of break-glass accounts.
- Investigate and document any use of these accounts.

9. Explore Eligible and Active Roles

9.1. Assign Eligible Roles

1. **Assign Eligible Users**:

   - In PIM, assign users to roles as Eligible, meaning they can activate the role when needed.

9.2. Activate Roles

1. **Activate Roles**:

   - Eligible users can activate roles from the My roles section in PIM.

10. Set the Time Limit of the Roles

10.1. Configure Activation Duration

1. **Set Time Limits**:

   - In PIM, configure the maximum duration for role activations.
   - Navigate to Azure AD roles or Azure resources, select the role, and set the Activation maximum duration.