**Handout: Administer Identity in Azure (AZ-104 Module)**

**Overview**

This handout summarizes key concepts, benefits, and configurations related to managing identities in Azure Active Directory (Azure AD), based on the Administer Identity module of the AZ-104 certification.

**1. Identity and Accounts in Azure AD**

* **Identity**: An object, such as a user or device, that can be authenticated and authorized. It allows access to resources such as applications and files.
* **Account**: An identity that has been given credentials (username, password) to access specific resources. It also contains user profile information like name, email, phone, etc.
* **Azure AD Tenant**: A dedicated, trusted instance of Azure AD for an organization. It acts as a container for users, devices, and groups. Tenants are automatically created when an organization subscribes to a Microsoft cloud service like Azure or Office 365.

**Key Differences Between Identity and Account**

* An **identity** can exist without any login credentials (such as service principals used by apps), while an **account** includes credentials for authentication.

**2. Comparison: Azure AD vs. AD DS**

| **Feature** | **Azure Active Directory (Azure AD)** | **Active Directory Domain Services (AD DS)** |
| --- | --- | --- |
| **Purpose** | Cloud-based identity and access management | On-premises identity management |
| **Communication Protocols** | HTTP, HTTPS, REST API, OAuth 2.0, SAML, OpenID Connect | LDAP, Kerberos, NTLM |
| **Structure** | Flat hierarchy (no OUs or GPOs) | Hierarchical structure (with OUs and Group Policy Objects - GPOs) |
| **Authentication** | Supports cloud-first services (OAuth, SAML, OpenID Connect) | Primarily on-premises services (Kerberos, LDAP) |
| **Management** | Cloud-based, managed by Microsoft | Self-managed, including patches, updates, and server management |
| **Hybrid Support** | Supports Hybrid Identity (Azure AD Connect, Azure AD Domain Services) | On-premises support only unless integrated with Azure AD |

**Use Case:**

* **Azure AD**: Designed for cloud-first organizations, provides SSO (Single Sign-On) and identity management for cloud apps like Office 365, Microsoft Teams, and other SaaS solutions.
* **AD DS**: Suited for traditional IT environments that rely on on-premises infrastructure, often used in organizations with existing Windows servers and applications that need internal management.

**3. Azure AD Features and Editions**

Azure AD offers different editions depending on the needs of the organization. Each edition provides varying levels of functionality.

**Azure AD Editions:**

* **Free**:
  + Basic identity and access management.
  + Limited directory size (500,000 objects).
  + Single Sign-On (SSO) for Azure and Office 365 services.
* **Microsoft 365 Apps**:
  + Includes all Free-tier features plus access to Office 365 services.
* **Premium P1**:
  + Adds advanced identity management features like **Conditional Access**, **Group-based Access Management**, and **Hybrid Identity**.
  + Ideal for organizations with both on-premises and cloud infrastructure.
* **Premium P2**:
  + Provides the most advanced security features like **Identity Protection** (risk-based conditional access) and **Identity Governance** for monitoring user and admin activities.
  + Suitable for larger organizations with a need for comprehensive identity governance and security.

**Common Features in All Editions:**

* Directory objects (users, groups, devices).
* Single Sign-On (SSO) for Microsoft services.
* Core identity and access management.
* Collaboration with external B2B users.

**4. Managing Users and Groups in Azure AD**

Managing users and groups is a core task in Azure AD administration. These operations allow administrators to assign permissions, enforce security policies, and manage resources effectively.

**User Accounts:**

* Every user must have an account in Azure AD to authenticate and access resources. Each account includes properties such as email, phone, and other profile information.
* User accounts can be managed via the Azure Portal, PowerShell, or Azure AD Graph API.

**Group Accounts:**

* Groups simplify user management by aggregating user permissions into manageable units.
  + **Security Groups**: These groups manage access to resources such as apps or file shares.
  + **Microsoft 365 Groups**: These groups are used for collaboration across services like Teams, SharePoint, and Outlook.
* **Assignment Types**:
  + **Assigned**: Admins manually add or remove users from the group.
  + **Dynamic**: Automatically adds or removes users based on attributes like department or location. These dynamic groups are ideal for keeping group memberships up to date with minimal admin intervention.

**Best Practices:**

* Use **Dynamic Groups** to streamline user management based on rules.
* Implement **Role-Based Access Control (RBAC)** by using security groups to limit access based on roles.

**5. Configuring Device Identities in Azure AD**

Device identities allow organizations to manage how devices access resources. Azure AD supports three main types of device identity:

**Device Identity Options:**

1. **Azure AD Registered Devices**:
   * Used in BYOD (Bring Your Own Device) scenarios where personal devices are registered with Azure AD but not fully managed.
   * Devices remain part of the user’s personal environment but can access corporate resources like email or SharePoint.
   * Managed using Mobile Device Management (MDM) solutions like Microsoft Intune.
2. **Azure AD Joined Devices**:
   * These are corporate-owned devices that are fully joined to Azure AD.
   * Provides access to cloud-based services and can be fully managed with Intune, including policy enforcement and software deployment.
   * Suitable for organizations that rely heavily on Azure-based services.
3. **Hybrid Azure AD Joined Devices**:
   * These devices are joined to both Azure AD and on-premises AD DS.
   * Allows organizations with existing infrastructure to gradually transition to cloud services while maintaining on-premises management through Group Policy and SCCM.
   * Ideal for organizations that need access to both cloud and on-premises resources.

**6. Self-Service Password Reset (SSPR)**

Self-Service Password Reset (SSPR) allows users to reset their passwords without needing administrator intervention, improving security and reducing help desk calls.

**SSPR Configuration:**

* **Authentication Methods**:
  + Email verification.
  + Phone (call or SMS).
  + Security questions.
  + Mobile app notification or code.
* Admins can configure how many authentication methods users must provide for password reset. For example, requiring two methods can add a layer of security.

**Best Practices for SSPR:**

* Ensure all users are registered for SSPR.
* Combine SSPR with Multi-Factor Authentication (MFA) to enhance security.

**7. Administering Bulk Updates and Administrative Units**

**Bulk User and Group Updates:**

* Azure AD allows for bulk user and group updates using CSV files. This is particularly useful for large organizations with frequent user updates.
* Administrators can download templates from the Azure Portal to perform bulk operations like creating users, adding users to groups, or updating profile properties.

**Administrative Units:**

* Administrative Units allow for scoped management, letting you delegate permissions to specific departments or teams.
* Example: In a large university, each school (Business, Engineering) could have its own administrative unit managed independently by the respective IT admins.

**Best Practice:**

* Use **Administrative Units** in complex organizations where different teams need autonomous control over users and resources.

**8. Key Terminologies**

| **Term** | **Description** |
| --- | --- |
| **Tenant/Directory** | A dedicated Azure AD instance for an organization |
| **Subscription** | The method by which Azure services are paid for and managed |
| **Conditional Access** | Policies that enforce access control based on specific conditions |
| **Dynamic Group Membership** | Automatically adds/removes users based on their attributes |
| **Device Identity** | Used to control how corporate and personal devices access resources |

**9. Lab 01: Managing Azure AD Identities**

**Scenario**: You are tasked with provisioning Azure AD users and groups for Contoso. Group membership will be updated automatically based on job titles, and a test Azure AD tenant will be created.

**Objectives**:

1. **Create and configure Azure AD users**: Use the Azure Portal or PowerShell to create users and assign them to groups.
2. **Create Azure AD groups with dynamic and assigned membership**: Implement dynamic groups based on attributes like department, role, or location.
3. **Create a test Azure AD tenant**: Set up a test environment for managing users and assigning access.
4. **Manage guest users**: Learn how to add guest users to your tenant and configure access to resources.

**Summary**

Azure AD offers a range of features for managing users, devices, and resources in a secure and scalable way. Whether working in an entirely cloud-based environment or a hybrid setup, tools like Dynamic Groups, Conditional Access, and Self-Service Password Reset (SSPR) make managing identities more efficient.

By completing the labs, you will gain hands-on experience with provisioning users, creating groups, and managing devices in Azure AD.

Relevant links

<https://docs.microsoft.com/learn/browse/>

<https://docs.microsoft.com/learn/paths/az-104-manage-identities-governance>

<https://docs.microsoft.com/azure/active-directory/fundamentals/active-directory-whatis>

<https://docs.microsoft.com/azure/active-directory/fundamentals/active-directory-whatis#terminology>

<https://docs.microsoft.com/azure/active-directory/fundamentals/active-directory-compare-azure-ad-to-ad>

<https://azure.microsoft.com/pricing/details/active-directory/>

<https://docs.microsoft.com/azure/active-directory/authentication/howto-sspr-deployment>

Azure AD registered devices - https://docs.microsoft.com/azure/active-directory/devices/concept-azure-ad-register

Azure AD joined devices - https://docs.microsoft.com/azure/active-directory/devices/concept-azure-ad-join

Hybrid Azure AD joined devices - https://docs.microsoft.com/azure/active-directory/devices/concept-azure-ad-join-hybrid

**Configure User and Group Accounts**

<https://docs.microsoft.com/azure/active-directory/fundamentals/add-users-azure-active-directory>

Bulk create users in Azure Active Directory - https://docs.microsoft.com/azure/active-directory/users-groups-roles/users-bulk-add

Bulk add group members in Azure Active Directory - https://docs.microsoft.com/azure/active-directory/enterprise-users/groups-bulk-import-members

<https://docs.microsoft.com/azure/active-directory/fundamentals/active-directory-manage-groups>

Assign or remove licenses in the Azure Active Directory portal - https://docs.microsoft.com/azure/active-directory/fundamentals/license-users-groups

Choose the best license for your business - https://www.microsoft.com/security/business/identity-access-management/azure-ad-pricing?rtc=1#office-SKUChooser-q6q98uk

<https://docs.microsoft.com/azure/active-directory/roles/administrative-units>