**VIRTUALIZATION & CLOUD COMPUTING**

**ASSIGNMENT**

**Explain User Management in Azure**

Azure Active Directory user management services such as groups and administrator role assignments help you accomplish your top tasks quickly. Assign licenses, assign application access to groups or users, or delegate permissions to distribute identity management tasks

**AUTHENTICATION METHODS FOR USER:**

As an administrator, choosing authentication methods for Azure Multi-Factor Authentication and self-service password reset (SSPR) it is recommended that you require users to register multiple authentication methods. When an authentication method is not available for a user, they can choose to authenticate with another method. Administrators can define in policy which authentication methods are available to users of SSPR and MFA.

**ASSIGN USERS TO GROUPS:**

You can use groups in Azure ACTIVE DIRECTORY to assign licenses to large numbers of users, or to assign user access to deployed enterprise apps. You can use groups to assign all administrator roles except for Global Administrator in Azure Active Directory, or you can grant access to resources that are external, such as SaaS applications or SharePoint sites.

For additional flexibility and to reduce the work of managing group membership, you can use [dynamic groups](https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-create-rule) in Azure Active Directory to expand and contract group membership automatically. You'll need an Azure Active Directory Premium P1 license for each unique user that is a member of one or more dynamic groups.

**ASSIGN LICENSES TO GROUPS USER:**

Assigning or removing licenses from users individually can demand time and attention. If you [assign licenses to groups](https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/license-users-groups?context=azure/active-directory/users-groups-roles/context/ugr-context) instead, you can make your large-scale license management easier.

In Azure Active Directory, when users join a licensed group, they're automatically assigned the appropriate licenses. When users leave the group, Azure Active Directory removes their license assignments. Without Azure Active Directory groups, you'd have to write a PowerShell script or use Graph API to bulk add or remove user licenses for users joining or leaving the organization.

**ADD USER IN AZURE ACTIVE DIRECTORY:**

1. You can create a new user using the Azure Active Directory portal .To add a new user, follow these steps:
   1. Sign in to the [Azure portal](https://portal.azure.com/) as a User administrator for the organization.
   2. Search for and select Azure Active Directory from any page.
   3. Select **Users**, and then select **New user**.
2. Add a new guest user. You can also invite new guest user to collaborate with your organization by selecting Invite user from the New user page. If your organization's external collaboration settings are configured such that you're allowed to invite guests, the user will be emailed an invitation they must accept in order to begin collaborating.
3. Add a consumer user. There might be scenarios in which you want to manually create consumer accounts in your Azure Active Directory B2C (Azure B2C) directory.
4. Add a new user within a hybrid environment .If you have an environment with both Azure Active Directory (cloud) and Windows Server Active Directory (on-premises), you can add new users by syncing the existing user account data.
5. You can delete an existing user using Azure Active Directory portal .To delete a user, follow these steps:
6. Sign in to the [Azure portal](https://portal.azure.com/) using a User administrator account for the organization.
7. Search for and select Azure Active Directory from any page.
8. Search for and select the user you want to delete from your Azure Active Directory tenant. For example, Mary Parker.

**DELEGATE ADMINISTRATOR ROLES:**

Many large organizations want options for their users to obtain sufficient permissions for their work tasks without assigning the powerful Global Administrator role to, for example, users who must register applications. Here's an example of new Azure Active Directory administrator roles to help you distribute the work of application management with more granularity:

Application Administrator:

Can add and manage enterprise applications and application registrations, and configure proxy application settings. Application Administrators can view Conditional Access policies and devices, but not manage them.

Cloud Application Administrator:

Can add and manage enterprise applications and enterprise app registrations. This role has all of the permissions of the Application Administrator, except it can't manage application proxy settings.

Application Developer:

Can add and update application registrations, but can't manage enterprise applications or configure an application proxy.

**ASSIGN APP ACCESS:**

Azure Active Directory also gives you granular control of the data that flows between the app and the groups to whom you assign access. In [Enterprise Applications](https://portal.azure.com/#blade/Microsoft_AAD_IAM/StartboardApplicationsMenuBlade/AllApps), open an app and select Provisioning to:

1. Set up automatic provisioning for apps that support it
2. Provide credentials to connect to the app's user management API
3. Set up the mappings that control which user attributes flow between Azure Active Directory and the app when user accounts are provisioned or updated
4. Start and stop the Azure Active Directory provisioning service for an app, clear the provisioning cache, or restart the service
5. View the Provisioning activity report that provides a log of all users and groups created, updated, and removed between Azure Active Directory and the app, and the Provisioning error report that provides more detailed error messages

**MANAGE USER DOMAIN NAMES IN YOUR AZURE ACTIVE DIRECTORY:**

A domain name is an important part of the identifier for many directory resources: it's part of a user name or email address for a user, part of the address for a group, and is sometimes part of the app ID URI for an application.

1. Set the primary domain name for your Azure Active Directory When your directory is created, the initial domain name, such as ‘contoso.onmicrosoft.com,’ is also the primary domain name. The primary domain is the default domain name for a new user when you create a new user.
2. Add custom domain names to your Azure Active Directory Organization. You can add up to 900 managed domain names. If you're configuring all your domains for federation with on-premises Active Directory, you can add up to 450 domain names in each directory.
3. Add sub domains of a custom domain. If you want to add a third-level domain name such as ‘europe.contoso.com’ to your directory, you should first add and verify the second-level domain, such as contoso.com.
4. Delete a custom domain name. You can delete a custom domain name from your Azure Active Directory if your organization no longer uses that domain name, or if you need to use that domain name with another Azure Active Directory.