MANAGING AZURE AD OBJECTS

Contents

Introduction

This companion guide for the “Managing Azure AD Objects” section of AZ-104 Exam Prep: Microsoft Azure Administrator is intended to provide some background context and use cases for topics covered in this section. Combining this information with the demos and hands-on labs should ensure you have a full grasp of the topics in this section of the course.

Custom Domains in Azure AD

When you create a new Azure AD tenant, it comes with an initial domain name. This domain name comes in the form of <domainname>.onmicrosoft.com. While you can’t change or delete the initial domain name, you can add your own custom domain name. You can even add multiple custom domain names. Organizations typically add custom domain names to Azure AD so that they can create usernames that are familiar to your users. Instead of making users login with names like jsmith@bluewidgetcorp.onmicrosoft.com, users can login with more familiar names, like jsmit@bluewidgetcorp.com.

Azure AD Users and Groups

Users and groups are really the bedrock of authentication and authorization in Azure AD. Adding users and groups to multiple subscriptions allows users to create, control, and access resources in the subscriptions they have accounts in.

Users

Before a user can access Azure resources, that user needs an Azure user account. User accounts in Azure contains information that’s needed to authenticate those users during the sign-on process. Once a user has been authenticated, Azure Active Directory creates an access token. The access token that Azure AD creates is then used to authorize the user and determine what resources the user can access. The token also determines what the user can do with those resources.

While you can use the command line to manage users, you will typically use the Azure AD dashboard, within the Azure portal, to manage users. It’s important to understand that you can only work with a single directory at a time. To manage multiple directories, you can use the **Directory + Subscription** panel to switch between the directories you need to manage. There’s also a **Switch directory** button in the toolbar, in the dashboard, that you can use to even more easily switch to another directory if you need to do so.

Groups

Azure AD groups are used to organize users and to simplify permissions management. By adding users to groups, resource owners can assign access permissions to everyone in the group at one time, instead of having to assign the permissions, on-by-on, to every user who needs access.

Groups provide security boundaries because they allow you to add and remove specific users to them, allowing you to grant or deny access to resources with minimal effort. To make things even easier, Azure AD supports dynamic groups. The membership of a dynamic group is based on rules – and is managed automatically. For example, you can create a dynamic group called “Marketing”, and configure it so users with a department attribute of “Marketing” are automatically added to the group.

You can define two different types of group in Azure AD:

- **Security Groups:** Security groups are the most common type of group. You use these to manage user and computer access to shared resources.
- **Microsoft 365 Groups:** This type of group provides collaboration opportunities to your users. You typically use this group type to give users access to a shared mailboxes, calendars, files, SharePoint sites, and more. You can even give people outside of your organization access to the group.

Bulk User Operations

If you need to add a large number of users to Azure AD, delete a large number of users from Azure AD, or even add a large number of users to a group, you can use the Azure AD portal and a CSV file to do so.

You can download a template CSV file from Azure AD. The rows in a downloaded CSV template are as follows:

- **Version number:** The first row containing the version number must be included in the upload CSV.
- **Column headings:** The format of the column headings is <Item name> [PropertyName] <Required or blank>. For example, Member object ID or user principal name [memberObjectIdOrUpn] Required. Some older versions of the template might have slight variations. For group membership changes, you have the option of which identifier to use: member object ID or user principal name.
- **Examples row:** The template includes a row of examples of acceptable values for each column. You must remove the examples row and replace it with your own entries.

Guest Accounts

Azure AD B2B (Business to Business) is a feature within External Identities that allows you invite guest users to collaborate with your organization. Azure B2B collaboration allows organizations to securely share applications and services with guest users from other organizations, while allowing them to retain control over their corporate data.

Azure AD B2B uses an easy invitation and redemption process that allows partners use their own credentials to access your company's resources.

Configuring Device Settings

As an administrator, you'll often need to manage devices in Azure AD. You can do so from two different locations:

- Azure portal > Azure Active Directory > Devices
- Azure portal > Azure Active Directory > Users > Select a user > Devices

These options allow administrators to not only search for devices in their directory, but to also see details for those devices. Such device details include:

- Device name

- Device ID
- OS and Version
- Join type
- Owner
- Mobile device management and compliance
- BitLocker recovery key

These options also allow administrators to perform device identity management tasks like, enable, disable, delete, or manage.

It's important to note that the management options in Azure AD for printers and for Windows Autopilot devices are really limited. These devices should be managed from their respective admin interfaces, instead of Azure AD.

Azure AD Join

Azure AD join is a feature that's intended for organizations that want to limit their on-prem footprint. Its for organizations that wish to be cloud-first or cloud-only. You can use Azure AD join to join devices directly to Azure AD, without the need for a traditional on-prem Active Directory.

Azure AD join also works in a hybrid environment. This enables access to both cloud and on-premises apps and resources.

Self-Service Password Reset

The Self-Service Password Reset offering allows users to change or reset their passwords, without the need to involve an administrator or help desk. If a user locks their account out, or forgets their password, they can follow a few prompts to unlock the account, and get back to work. Organizations typically use SSPR to reduce help desk calls when a user can't sign in to their device or even to an application.

Self-Service Password Reset can be used in the following cases:

- **Password Change** - when a user knows their password but wants to change it to something new.
- **Password Reset** - when a user can't sign in, such as when they forgot password, and want to reset their password.
- **Account Unlock** - when a user can't sign in because their account is locked out and want to unlock their account.

You can even use Password Writeback in Azure AD to writeback passwords to an on-prem AD, which means when a user updates or resets their password, using self-service password reset, the password can then be written back to the on-prem Active Directory environment. This writeback process ensures a user can immediately use their updated credentials with on-prem devices and applications.