Microsoft

Microsoft 365 Identity and Services

SECOND EDITION

Exam Ref MS-100

Orin Thomas

Microsoft

Exam Ref MS-100 Microsoft 365 Identity and Services

Orin Thomas

3. The first user account created for a subscription will be assigned global administrator privileges. This will be the user account of the IT staff member who recently left and who set up Microsoft 365.
4. The license conflict can be resolved by either manually removing licenses from the 10 users who have left the organization or by deleting their user accounts.

Chapter summary

- When you create a Microsoft 365 subscription, the subscription tenancy is automatically assigned a custom onmicrosoft.com domain.
- No two organizations can share the same tenant name.
- The tenant name chosen at setup remains with the subscription over the course of the subscription's existence.
- You can assign a domain name that you own to the tenant so that you don't have to use the onmicrosoft.com tenant name.
- To use a domain with Microsoft 365, the DNS servers used as name servers for the domain must support CNAME, SPF/TXT, SRV, and MX records.
- You can confirm ownership of a domain by configuring special TXT or MX records.
- Setting the default domain configures which domain suffix will automatically be used with Microsoft 365 user accounts.
- Changing the primary email address also changes the user name.
- You can perform a bulk email address update using PowerShell.
- Additional email addresses allow mailboxes to receive messages from more than a single address and can use any domain name associated with the organization's Microsoft 365 tenancy.
- A Microsoft 365 endpoint is a URL or IP address that hosts a specific Microsoft 365 or Office 365 service.
- Microsoft places each Microsoft 365 and Office 365 endpoint into one of three categories: optimize, allow, and default. Optimize requires minimum disruptions caused by latency and availability. Allow endpoints are less problematic, and default endpoints do not require optimization.
- Privileged access management allows you to configure policies that apply just-in-time administrative principles to sensitive administrative roles.
- Cloud authentication occurs against Azure AD. Use it with a password hash with a single sign-on and pass-through authentication with single sign-on.
- Federated authentication can occur using AD FS or a third-party authentication provider.
- Mail reports allow you to view how Office 365 mailboxes are used.

- Usage reports allow you to view information about browsers, operating systems, and license consumption.
- Skype for Business reports allow you to see how Skype for Business is being used in the organization.
- SharePoint reports allow you to see how SharePoint is being used with the Office 365 subscription.
- Data loss prevention (DLP) reports allow you to view how DLP rules and policies are being applied to message traffic.
- The Service Health dashboard is available from the Microsoft 365 Admin Center, allowing you to determine the status of the various elements of Microsoft 365, including fault history and planned maintenance.
- Users assigned the global administrator role have access to all administrative features.
- Users assigned the billing administrator role can make purchases, manage subscriptions, manage support tickets, and monitor service health.
- Users assigned the helpdesk (password) administrator role can reset the passwords of most Office 365 user accounts (except those assigned the global administrator, service administrator, or billing roles).
- Users assigned the service administrator role can manage service requests and monitor service health.
- You can assign and remove licenses by editing an Office 365 user's properties.
- Deleting a user removes all licenses assigned to that user.
- Pilot users should be a representative sample of your organization.
- You can use the SharePoint Migration Tool to migrate on-premises SharePoint document libraries, lists, and regular file shares to SharePoint Online.
- The OneDrive client allows you to drag and drop files on a client computer and have those files sync either with OneDrive for Business or SharePoint Online.
- You can use the bulk import method to import a CSV file of user identities into Azure AD.

CHAPTER 2

Manage user identity and roles

A key aspect of deploying Microsoft 365 is ensuring that user identity is configured properly. When this is done, users can seamlessly access resources in the on-premises environment as well as in the Microsoft 365 environment. If it is not done correctly, users must juggle different accounts, depending on whether the accessible resources are hosted locally or in the cloud.

In this chapter, you will learn about designing an identity strategy, how to plan identity synchronization with Azure AD Connect, how to manage that synchronization, how to manage Azure AD identities, and how to manage Azure AD user roles.

Skills in this chapter:

- Skill 2.1: Design identity strategy
- Skill 2.2: Plan identity synchronization by using Azure AD Connect
- Skill 2.3: Manage identity synchronization by using Azure Active Directory
- Skill 2.4: Manage Azure AD identities
- Skill 2.5: Manage user roles

Skill 2.1: Design identity strategy

This skill deals with designing a strategy related to on-premises and cloud-based identity. To master this skill, you'll need to understand how to determine your organization's requirements when it comes to synchronization, what an appropriate identity-management solution is, and what type of authentication solution is appropriate for your environment.

This section covers the following topics:

- Evaluate requirements and solution for synchronization
- Evaluate requirements and solution for identity management
- Evaluate requirements and solution for authentication

Evaluate requirements and solution for synchronization

Synchronization is the process of replicating on-premises identities, such as users and groups, to the cloud. Synchronization is necessary only when an on-premises identity provider is present. In some synchronization models, every on-premises identity is replicated to the cloud. In other models, only a subset of the on-premises identities is replicated.

Another consideration in evaluating synchronization requirements is determining what information about a user's identity needs to be synchronized to the cloud. Depending on the model chosen, some or all of the properties of those on-premises identities can be replicated. For example, some organizations store sensitive private data about employees within Active Directory. Only replicating what is necessary is especially important given the increasing regulation of data involving personal information.

Should an organization choose, it is possible to perform a complete replication of every aspect of an Active Directory object to the cloud. For example, an organization can deploy a domain controller, SharePoint Farm, System Center, and Exchange Server in Azure infrastructure-as-a-service (IaaS) virtual machines (VMs). You can have those VMs connected via VPN or an ExpressRoute connection to an on-premises Active Directory instance. In this scenario, the Azure IaaS VMs would essentially function as an expensive branch office site running in the Azure cloud.

When evaluating requirements and a solution for synchronization, consider the following questions:

- Which identities need to be replicated to the cloud?
- How often do those identities need to be replicated to the cloud?
- What properties of those identities need to be replicated to the cloud?

Which identities to replicate?

Deployment of Microsoft 365 gives organizations an ability to assess their existing identity needs. If an organization has been using Active Directory for a long time, it's likely that objects don't need to be replicated to the cloud and probably don't need to be in the on-premises Active Directory instance. It's a good idea, before implementing any Microsoft 365 replication scheme, to do a thorough audit of all the objects present within the on-premises directory and to clean out those that are no longer required.

Another issue to address is whether every on-premises identity needs to be present in Azure Active Directory. Many organizations take a phased approach to the introduction of Microsoft 365, migrating small groups of users to the service at a time rather than every user in the organization all at once. Users who are only present in the on-premises directory service won't need to have Microsoft 365 licenses assigned to them.

There are also special account types that are commonly present in an on-premises Active Directory instance that do not need to be, or simply cannot be, replicated to Azure Active Directory. For example, there is no need to replicate service accounts or accounts that are used for specific administrative purposes for on-premises resources, such as the management of an on-premises SQL Server database server or other workload.

Another challenge to consider is that many on-premises environments are more complicated than a single Active Directory domain. Some organizations have multidomain Active Directory forests. In addition, since it is a recommended Microsoft secure administrative practice, an increasing number of large organizations have multiforest deployments—for example, an Enhanced Security Administrative Environment (ESAE) forest to store privileged accounts for the production forest.

User accounts are not the only identity that an organization may want to replicate to the cloud. It may be necessary to replicate some groups to the cloud because these groups may be useful in mediating access to Microsoft 365 workloads. For example, if your organization already has a local security group that is used to collect together members of the accounting team, you may want that group also present as a method of mediating access to resources and workloads within Microsoft 365.

How often to replicate?

When evaluating requirements and a solution for synchronization, you need to answer several important questions. For example, how often do the properties of an on-premises identity change and how soon must those changes be present within Azure Active Directory?

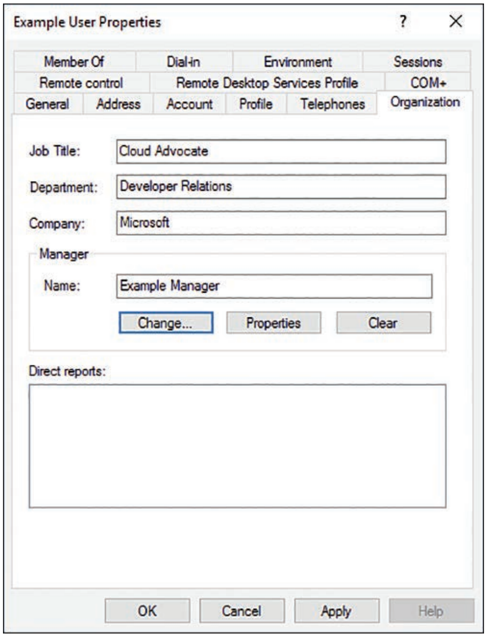
You don't want a user who changes his or her password to have to wait 24 hours before that new password can be used against cloud identities. Similarly, if you deprovision a user account because a person's employment with the organization has terminated, you'll want that action to be reflected in limiting access to Microsoft 365 workloads, rather than the user account having continued access for some time after the user's on-premises identity has been disabled.

Although there can be bandwidth considerations around identity synchronization, the majority of such traffic is going to be the replication of changes, also known as *delta*, rather than constant replications of the entire identity database. The amount of bandwidth consumed by delta identity synchronization traffic is often insignificant compared to the bandwidth consumed by other Microsoft 365 workloads and services.

Which properties to replicate?

Active Directory has been present at some organizations for almost two decades. One of the original selling points of Active Directory was that it could store far more information than just user names and passwords. Because of this, many organizations use Active Directory to store a substantive amount of information about personnel, including telephone numbers, the user's position within the organization, and the branch office where the user works.

When considering a synchronization solution, determine which on-premises Active Directory attribute information needs to be replicated to Azure Active Directory. For example, you may have an application running in Azure that needs access to the Job Title, Department, Company, and Manager attributes, as shown in Figure 2-1.



Job Title: Cloud Advocate

Department: Developer Relations

Company: Microsoft

Manager

Name: Example Manager

Direct reports:

FIGURE 2-1 Which attributes to replicate

Evaluate requirements and solutions for identity management

Evaluating the requirements and solutions for identity management first involves determining what your organization's source of authority is. The source of authority is the directory service that functions as the primary location for the creation and management of user and group accounts. You can choose between having an on-premises Active Directory instance function as a source of authority, or you can have Azure Active Directory function as the source of authority.

Even though Azure Active Directory is present in a hybrid deployment, the source of authority will be the on-premises Azure AD instance. Hybrid deployment accounts are used for authentication and authorization purposes with existing on-premises resources as well as Microsoft 365 workloads.

Source of authority is a very important concept when it comes to creating users and groups in an environment where Azure AD Connect is configured to synchronize an on-premises Active Directory with the Azure Active Directory instance that supports the Microsoft 365 tenancy. When you create a user or group in the on-premises Active Directory instance, the on-premises Active Directory instance retains authority over that object. Objects created