Answer Key

To set up a custom domain, you can go to the Microsoft 365 admin center, then navigate to Setup and select Domains.

To add user accounts in the Microsoft 365 admin center, click on Users and then Active users.

To ensure the security of your organization's data and meet any regulatory requirements, you'll need to configure security and compliance settings in the Microsoft 365 admin center.

To confirm domain ownership, you need to enter your domain name, add TXT or MX records to the DNS zone based on the info provided by the Microsoft 365 setup wizard, and then verify the domain ownership within the wizard.

A subscription is a paid plan that gives you access to various Microsoft cloud services, like Exchange Online, SharePoint Online, OneDrive for Business, and Microsoft Teams.

A tenant is a dedicated instance of the Microsoft cloud environment that your organization uses to manage its subscription and resources.

When you sign up for a subscription, you'll provide some basic information, and Microsoft will use this to create a new tenant with a unique URL, like https://surfcityboats.onmicrosoft.com.

With a Microsoft 365 subscription, you can add up to nine-hundred domains to a single tenant.

Every Microsoft 365 tenant includes a dedicated Azure Active Directory (Azure AD) tenant.

To edit your organization's profile information, go to the Microsoft 365 admin center, select Settings, then Org settings, and then choose the Organization profile tab.

When checking service health, you may come across various status definitions. When Microsoft is aware of a potential issue and is gathering more information to determine the scope of impact and what's causing the problem, a status of Investigating will show.

The Microsoft Adoption Score provides insights about how your organization uses Microsoft 365 and its technology experiences.

To enable Adoption Score, sign in to the Microsoft 365 admin center as a Global Administrator and then browse to Reports > Adoption Score.

Your Adoption Score is based on combined scores from people and technology experiences categories, with a total of eight-hundred possible points.

When adding a new user, the Optional settings page is where you can select any roles you want to assign to the user.

When adding a new user, you can use the Licenses page to set the sign-in status, location, and licenses for your new users.

The New-MgUser PowerShell command is used to create a new user in Microsoft 365, via Microsoft Graph.

A user’s OneDrive tab in the Microsoft 365 admin center allows you to access the user's files, view the storage quota, and force a sign-out from all Microsoft 365 sessions.

Mail contacts have email addresses outside your organization's domain.

To create mail contacts, you need permissions, which can come from the Recipient Management role group, the Organization Management role group, or the Mail Recipients role.

To create a group in the Microsoft 365 Admin Center, you can click on Teams and Groups in the left navigation pane, then Active Teams and Groups, and then finally, Add a Group.

When you delete a Microsoft 365 group, it'll be retained for thirty days, giving you the chance to restore it if needed.

Using PowerShell, you can use the Get-MgSubscribedSku command to view the available licensing plans and the number of available licenses in your organization.

Azure Active Directory was recently (as of this course publication) renamed to Microsoft Entra.

The CSV templates for bulk user creations, bulk deletions of users, and bulk restores of deleted users are different.

To bulk restore deleted users, you need the ObjectID for each user in the CSV file.

SECTION: Manage roles in Microsoft 365

A user with the Global Reader role can view admin features and settings in admin centers that the global admin can view but cannot edit any settings.

An administrative unit in Azure Active Directory (AD) is a resource that can act as a container for other Azure AD resources, like users, groups, or devices.

To use administrative units, you'll need an Azure AD Premium P1 license for each administrative unit administrator and an Azure AD Free license for each member.

One of the main benefits of PIM is its ability to provide JIT administrative access.

Privileged Identity Management introduces the concept of an eligible administrator, which is a user who needs privileged access periodically but not continuously.