📘 Managing Microsoft Entra ID Tenants

1. ✅ What is a Microsoft Entra ID Tenant?

- A **tenant** is a **dedicated and isolated instance** of Microsoft Entra ID (formerly Azure AD).
- Created automatically when an organization signs up for any Microsoft cloud service (Microsoft 365, Azure, etc.).
- Represents your organization's **identity environment**.
- It **stores and manages**:
  - Users
  - Groups
  - Devices
  - Applications
  - Security and access configurations

2. 🌐 Tenant vs Directory vs Subscription

Concept	Description
Tenant	Logical identity boundary; unique instance of Entra ID tied to your org.
Directory	The identity store within a tenant (same thing in most cases).

Subscription	The Azure billing unit; used to manage Azure resources. A tenant can have multiple subscriptions.

> 💡 A subscription is **linked to one tenant** only, but a tenant can contain **multiple subscriptions**.

---

3. 🛠️ Key Tenant-Level Management Tasks (Exam-Relevant)

Task	Description
View tenant information	Name, tenant ID (GUID), primary domain, default domain (`.onmicrosoft.com`).
Add/verify custom domain	E.g., `contoso.com`. Needed for user-friendly logins.
Directory roles	Assign roles like Global Administrator, User Administrator, etc.
Configure external collaboration	Enable/disable guest access, invitation settings.
Enable Security Defaults	Enforces MFA and basic protection policies.
Branding	Customize the sign-in experience with logos, messages.
Directory Settings	Includes user creation, device registration limits, self-service password reset (SSPR), etc.

---

4. 🔒 Security Configuration at Tenant Level

- **Security Defaults** (one-click enablement of MFA, user protections)
- **Conditional Access** (enforce location, device, app access rules)
- **MFA Enforcement** (per user or via policy)
- **Identity Protection** (automated risk-based responses to suspicious behavior)
- **Self-Service Password Reset (SSPR)** — end-user recovery options

5. 🔄 Tenant Types

Tenant Type	Description
Workforce tenant	Default tenant used by businesses (users/employees access Azure, M365, etc.)
B2B collaboration	Allows external (guest) users to access resources using their own credentials
B2C tenant	Specialized tenant for customer-facing apps with identity flows like sign-up/sign-in

> 🔔 **AZ-104 focuses mostly on workforce tenants**, but you should know that B2B collaboration exists.

6. 🚪 Access and Roles

- **Directory Roles** (Entra ID roles):
  - Global Administrator
  - User Administrator
  - Password Administrator
  - Security Administrator
  - Billing Administrator
- **Azure RBAC Roles** (used for Azure resources, not Entra ID itself)
  - Contributor
  - Reader
  - Owner

- Important: AZ-104 expects you to **differentiate** between **directory roles** and **Azure roles**

---

7. 🧰 Tools Used to Manage the Tenant

Tool	Use Case
Microsoft Entra Admin Center (`entra.microsoft.com`)	Primary interface to manage tenant settings, roles, users, and policies
Azure Portal (`portal.azure.com`)	For managing subscriptions, RBAC, resources
PowerShell (`MSOnline`, `AzureAD`, `Entra` modules)	Scripting and automation
Microsoft Graph API	Programmatic access and integration
Azure CLI (`az ad`)	Command-line Azure identity management

---

8. 🧠 Key Exam Concepts You MUST Know

- Identify the **tenant ID**, **directory name**, and **default domain**.
- Know how to **add and verify a custom domain**.
- Understand how to **assign directory roles** to users.
- Know how to **enable/disable external collaboration** and invite guests.
- Configure **security defaults** and understand their limitations.
- Differentiate **Azure AD roles** vs **Azure resource roles**.

Sure! Here's a **step-by-step lab document** based on the detailed Microsoft Entra ID tenant management content you provided, aligned with AZ-104 concepts.

Lab: Creating and Managing Microsoft Entra ID Tenants

Objective

- Understand Microsoft Entra ID tenant types
- Create a new workforce tenant
- Create a new customer tenant
- Switch between tenants
- Explore administrative units and tenant isolation

Prerequisites

- Access to an Azure account with permissions to create tenants and manage subscriptions
- Access to Microsoft Entra Admin Center: https://entra.microsoft.com
- Basic understanding of Azure Portal and Entra ID concepts

Lab Environment

- Microsoft Entra Admin Center (Primary tool)
- Azure Portal (for subscription and resource group management)

Step 1: Overview of Tenant Types

Before creating tenants, understand:

Tenant Type	Description
Workforce	Contains your employees, internal applications, and resources. Supports external users as guests (B2B).
Customer	Customer-facing apps and resources. Supports self-service sign-up and multiple authentication methods.

Step 2: Access Microsoft Entra Admin Center and Manage Tenants

1. Open https://entra.microsoft.com and sign in with your admin account.
2. In the overview pane, locate and click **Manage tenants**.
3. Explore the **Managed tenants** overview to see tenants you currently manage.
4. Click **Create a new tenant**.

Step 3: Create a Workforce Tenant

1. In the tenant creation pane, select **Workforce** tenant type.

2. Enter a **tenant name** (e.g., `Contoso Workforce Tenant`).
3. (Optional) Enter a domain name (this is *not* the custom domain, but a unique identifier).
4. Select the **region** where tenant data will be stored. Choose carefully for compliance with data residency.
5. Complete CAPTCHA validation and click **Submit**.
6. Wait a few minutes for the tenant creation to complete.

Step 4: Create a Customer Tenant

1. Return to the **Manage tenants** page.
2. Click **Create a new tenant** and select **Customer** tenant type.
3. Enter a **tenant name** (e.g., `Contoso Customer Tenant`).
4. Enter a domain name or web URL relevant to your customer-facing app.
5. Select an **Azure subscription** to link this tenant (can use an existing subscription or create a new one).
6. Optionally, create a **new resource group** to organize resources related to this tenant.
7. Select the **resource location** (e.g., East US).
8. Click **Review + Create**, then **Create**.
9. Wait for the deployment to complete.

Step 5: Switch Between Tenants

1. In the Entra Admin Center or Azure Portal, click on the **gear icon** in the top-right corner.

2. Select **Switch directory** or **Switch tenant**.

3. Search and select the new tenant directory you created.

4. Confirm the switch.

5. Observe that the environment now shows the new tenant, with only the initial user active.

Step 6: Understand Administrative Units (Conceptual)

- Large organizations can segment tenant administration using **Administrative Units**.

- Example: HR department manages users and policies only within the HR administrative unit, without affecting the entire tenant.

- This segmentation improves security and allows delegated management.

Lab Wrap-Up

- You created **workforce** and **customer** tenants.

- Learned how to link customer tenants to Azure subscriptions and resource groups.

- Switched between different tenants to manage isolated environments.

- Discussed how administrative units provide granular delegated management inside tenants.

Review Questions

1. What is the primary difference between a workforce tenant and a customer tenant?

2. Why is region selection important when creating a tenant?

3. How do you switch between different tenants in the Azure Portal?

4. What role do administrative units play in tenant management?

5. Can a customer tenant exist without an Azure subscription?

Additional Resources

- Microsoft Entra ID Documentation: https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

- Create and manage tenants: https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-create-new-tenant

- Azure Subscription and Tenant Relationships: https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/overview