Course Outline

Course 10993: Integrating On-Premises Identity Infrastructure with Microsoft Azure

Duration: 2 days

About this course

This course teaches IT professionals how to integrate their on-premises AD DS environment with Azure AD and how to use Azure AD as a directory service. It also teaches candidates how to use Azure RMS to protect sensitive documents. Additionally, it focusses on how to enhance authentication with multi-factor authentication and how to monitor directory synchronization health.

Audience profile

The primary audience for this course is existing IT professionals who have some knowledge and experience with Azure, and advanced experience with the Windows Server operating system. In addition, IT professionals who take this course typically want to develop knowledge of identity services integration between on-premises services and cloud services. This would typically include:

- AD DS administrators who are looking to train in cloud identity and access technologies.
- System or infrastructure administrators with general AD DS experience and knowledge, who are looking for more advanced identity training for Azure services.

At course completion

After completing this course, students will be able to:

- Compare Azure AD to AD DS, perform Azure AD tenant provisioning, and manage objects and user roles in Azure AD.
- Implement and configure directory synchronization and manage synchronized directories.
- Use Azure AD as a directory service for an on-premises environment, configure single sign-on (SSO) in Azure AD, and protect privileged identities.
- Implement multi-factor authentication.
- Implement Azure RMS and integrate Azure RMS with on-premises services.
- Configure alerts and monitor directory services infrastructure.

➢ Module 1: Introducing Azure AD This module describes the differences between Azure AD and AD DS, and the Azure AD versions. It also explains how to perform Azure AD tenant provisioning and how to manage objects and user roles in Azure AD. Lessons

- Azure AD overview

- Implementing and configuring Azure AD
- Managing Azure AD
    - ❖ Lab: Creating and managing an Azure AD tenant
        - Activating Azure and Office 365 trial subscriptions
        - Configuring an Azure AD tenant and objects in Azure AD
        - Configuring user roles in Azure AD

After completing this module, students will be able to:

- Describe Azure AD.
- Implement and configure Azure AD.
- Manage Azure AD.

➢ Module 2: Integrating on-premises Active Directory with Azure This module explains how to extend an on-premises Active Directory domain to Azure, and how directory synchronization works. It also describes how to implement and configure directory synchronization. Additionally, this module describes how to manage synchronized directories. Lessons

- Extending an on-premises Active Directory domain to Azure
- Directory synchronization overview
- Implementing and configuring directory synchronization
- Managing synchronized directories
    - ❖ Lab: Implementing directory synchronization
        - Implementing Azure AD Connect
        - Managing directory synchronization

After completing this module, students will be able to:

- Describe how to extend on-premises Active Directory to Azure.
- Describe directory synchronization.
- Implement and configure directory synchronization.
- Manage synchronized directories.

➢ Module 3: Using Azure AD as a directory service in hybrid environments This module explains how to use Azure AD as a directory service for on-premises resources, and how to configure SSO in Azure AD. It also describes how to implement Azure AD Privileged Identity Management (PIM). Lessons

- Azure AD as a directory service for on-premises environments
- Configuring SSO with Azure AD
- Implementing Azure AD PIM
    - ❖ Lab: Using Azure AD in hybrid environments
        - Joining a Windows 10 computer to Azure AD
        - Implementing SSO with Azure AD
        - Configuring and using Azure AD PIM

After completing this module, students will be able to:

- Describe how to use Azure AD as a directory service for an on-premises resources.
- Configure SSO in Azure AD.

- Implement PIM with Azure AD.

➢ Module 4: Configuring and protecting authentication in hybrid environments This module explains how authentication works in hybrid environments. In addition, it describes how to implement Azure Multi-Factor Authentication. Lessons

- Authenticating users in hybrid environments
- Implementing multi-factor authentication
  - ❖ Lab: Configuring authentication in hybrid environments
    - Implementing user password reset policy
    - Implementing Multi-Factor Authentication
    - Implementing Multi-Factor Authentication Server on premises

After completing this module, students will be able to:

- Describe how authentication works in hybrid environments.
- Implement multi-factor authentication.

➢ Module 5: Deploying Azure RMS with on-premises services This module provides an overview of rights management, and describes the differences between Active Directory Rights Management Services (AD RMS) and Azure RMS. It also explains how to implement Azure RMS and integrate it with on-premises services. Lessons

- RMS overview
- Implementing Azure RMS
- Integrating Azure RMS with on-premises services
  - ❖ Lab: Implementing Azure RMS
    - Enabling and configuring Azure RMS
    - Integrating Azure RMS with FCI
    - Using the RMS sharing application on a client

After completing this module, students will be able to:

- Describe Microsoft Rights Management services (RMS).
- Implement Azure RMS.
- Integrate Azure RMS with on-premises services.

➢ Module 6: Monitoring Azure AD This module describes how to use Azure AD reporting, and how to configure Azure AD notifications. It also describes how to monitor AD DS and Azure AD by using Azure AD Connect Health and Microsoft Operations Management Suite (OMS). Lessons

- Azure AD reporting
- Monitoring Azure AD
  - ❖ Lab: Configuring reporting and monitoring
    - Configuring Azure AD reports and notifications
    - Configuring Azure AD monitoring

After completing this module, students will be able to:

- Describe and use Azure AD reporting.
- Monitor Azure AD.

Prerequisites

In addition to their professional experience, students who attend this training should already have the following technical knowledge:

- Experience with AD DS concepts and technologies in Windows Server 2012 or Windows Server 2016.
- Experience working with and configuring Windows Server 2012 or Windows Server 2016.
- Basic experience with Windows PowerShell.
- Basic experience with cloud services such as Microsoft Office 365.
- Basic experience with the Azure platform.
- Basic experience with identities on premises or in cloud.