

Introduction:

The **Identity with Windows Server 2016** training course is tailored for IT professionals with prior knowledge of Active Directory Domain Services (AD DS) and aims to deepen understanding of identity management and access technologies in Windows Server 2016. This course offers in-depth training on the synchronization of AD DS with Microsoft Azure Active Directory, equipping participants with the skills to manage and secure data access, streamline identity management, and maintain a highly secure and available server environment.

Designed to enhance your Microsoft Windows Server administration skills, this training prepares participants for advanced server administration tasks related to Windows Identity Foundation Server 2016 and identity management.

Targeted Groups:

- IT professionals seeking to develop expertise in identity and access technologies in Windows Server 2016.
- Directory administrators looking to expand their skills in managing identity and access technologies.
- System or infrastructure administrators with AD DS experience who want to cross-train in core and advanced identity and access technologies.
- IT professionals aiming to consolidate their knowledge of AD DS and related identity management technologies within a Windows Server environment.

Course Objectives:

By the end of this course, participants will be able to:

- Install and configure domain controllers.
- Manage objects in AD DS using graphical tools and PowerShell.
- Implement AD DS in complex environments.
- Configure and manage replication within AD DS sites.
- Implement and manage Group Policy Objects (GPOs) for efficient user settings.

- Secure AD DS and user accounts.
- Implement and manage a Certificate Authority (CA) hierarchy using AD Certificate Services (AD CS).
- Deploy and manage certificates effectively.
- Administer Active Directory Federation Services (AD FS).
- Implement and administer Active Directory Rights Management Services (AD RMS).
- Synchronize AD DS with Azure AD for cloud-based identity management.
- Monitor, troubleshoot, and ensure business continuity for AD DS services.

Targeted Competencies:

At the conclusion of this course, participants will have developed competencies in:

- Managing AD DS objects.
- Administering and troubleshooting AD DS services.
- Troubleshooting and managing Group Policy Infrastructure.
- Managing user settings via Group Policy Objects (GPOs).
- Recovering AD DS objects.
- Configuring directory synchronization with Azure AD.

Course Content:

Unit 1: Installing and Configuring Domain Controllers (DCs)

- Overview of AD DS and domain controllers.
- Step-by-step deployment of domain controllers in Windows Server 2016.

Unit 2: Managing Objects in AD DS

- Managing user accounts and group objects.

- Managing computer accounts and organizational units (OUs).
- Using Windows PowerShell for AD DS administration.

Unit 3: Advanced AD DS Infrastructure Management

- Configuring advanced AD DS deployments.
- Deploying distributed AD DS environments.
- Configuring and managing AD DS trusts.

Unit 4: Implementing and Administering AD DS Sites and Replication

- Overview of AD DS replication and its importance.
- Configuring AD DS sites and replication.
- Monitoring and troubleshooting AD DS replication.

Unit 5: Implementing Group Policy

- Introduction to Group Policy and its application.
- Implementing and administering GPOs.
- Understanding Group Policy scope and processing.
- Troubleshooting GPO application.

Unit 6: Managing User Settings with Group Policy

- Implementing administrative templates in GPOs.
- Configuring Folder Redirection and scripts.
- Configuring Group Policy preferences to enhance user management.

Unit 7: Securing Active Directory Domain Services

- Securing domain controllers and user accounts.

- Implementing auditing and account security measures.
- Configuring Managed Service Accounts (MSAs) for enhanced security.

Unit 8: Deploying and Managing AD CS (Active Directory Certificate Services)

- Deploying Certificate Authorities (CAs).
- Administering and maintaining CAs.
- Troubleshooting CA issues and ensuring smooth operations.

Unit 9: Deploying and Managing Certificates

- Deploying and managing certificate templates.
- Managing certificate deployment, revocation, and recovery.
- Using certificates in a business environment, including the management of smart cards.

Unit 10: Implementing and Administering AD FS (Active Directory Federation Services)

- Overview of AD FS and its benefits for Single Sign-On (SSO).
- Requirements, planning, and deployment of AD FS.
- Configuring the Web Application Proxy for external access.

Unit 11: Implementing and Administering AD RMS (Active Directory Rights Management Services)

- Understanding AD RMS and its use in protecting content.
- Deploying and managing an AD RMS infrastructure.
- Configuring AD RMS to protect sensitive business data.

Unit 12: Implementing AD DS Synchronization with Azure AD

- Planning and preparing for directory synchronization with Azure AD.
- Implementing Azure AD Connect to synchronize identities between on-premises AD DS and Azure

AD.

- Managing identities and ensuring seamless synchronization with Azure AD.

Unit 13: Monitoring, Managing, and Recovering AD DS

- Monitoring the health and performance of AD DS.
- Managing and troubleshooting the Active Directory database.
- Implementing backup and recovery solutions for AD DS to ensure business continuity.

By the end of this course, participants will be equipped with the necessary skills to manage and secure identities in Windows Server 2016, ensuring that your organization can handle complex identity management tasks efficiently and securely. This training is a crucial step toward mastering the identity and access management features of Windows Server 2016.