The DevOps Company

Microsoft Partner

CL_55351
Identity with Windows Server

About this course.

This course is intended for IT professionals who want to learn about administering, configuring, troubleshooting, and operating identity services in the Active Directory Domain Services (AD DS) and Azure AD. Course covers core AD DS identity services such as GPOs, AD CS, AD FS and also hybrid solutions with Azure AD.

Length.

5 Days.

Audience profile.

This course is intended for IT professionals who work on administering, configuring, troubleshooting, and operating identity services in the Active Directory Domain Services and Azure AD. It is also useful for system or infrastructure administrators with general AD DS experience and knowledge who want to cross-train in core and advanced identity and access technologies in Windows Server and Azure AD.

Prerequisites.

Before attending this course, students must have:

- Some exposure to and experience with AD DS concepts and technologies in Windows Server 2012 or newer.
- Experience working with and configuring Windows Server 2012 or newer.
- Experience working with and an understanding of Microsoft Hyper-V and basic server virtualization concepts.
- An awareness of basic security best practices.
- Hands-on working experience with Windows client operating systems such as Windows 7, Windows 8, Windows 8.1, or Windows 10.
- Basic experience with the Windows PowerShell command-line interface.

At Course Completion.

- Install and configure domain controllers in AD DS.
- Manage objects in AD DS by using graphical tools and Windows PowerShell modules.
- Implement AD DS in complex environments.
- Implement and configure AD DS sites, and configure and manage replication.
- Implement and manage Group Policy Objects (GPOs) in AD DS.
- Manage user settings by using GPOs.
- Secure AD DS.
- Implement and manage a certificate authority (CA) hierarchy with AD CS.
- Deploy and manage certificates.
- Implement and administer Active Directory Federation Services (AD FS).
- Implement synchronization between AD DS and Azure AD.
- Monitor, troubleshoot, and establish business continuity for AD DS services.

Exam.

None.

Course outline.

Module 1: Deploy Active Directory services.

Active Directory Domain Services (AD DS) is the cornerstone of on-premises networks for many organizations worldwide. AD DS delivers authentication and authorization by using domain controllers (DCs) for on-premises apps and services. In this module, you'll learn how to configure DCs to suit your specific organizational needs and integrate AD DS with Microsoft Azure Active Directory (Azure AD) to provide single sign-on (SSO) for users that access both on-premises and cloud-based apps.

- Components of AD DS.
- AD DS DCs.
- Deploy AD DS DCs.
- Azure AD overview.

Labs: Deploy and administer AD DS.

- Deploy AD DS.
- Deploy DCs by performing DC cloning.
- Administer AD DS.

After completing this module, students will be able to:

- Deploy AD DS and DCs.
- Administer AD DS.

Module 2: Manage directory objects.

Active Directory, at its heart, is a hierarchical database. Unlike a traditional database, however, you can create many different types of records within Active Directory. These records are referred to as objects, which you can create to represent almost anything in your network, from users and groups to printers, shared folders, and computers.

Each object can have many different properties, referred to as attributes. For example, the user object type has attributes in which you can store the user's sign-in name, and street and email addresses.

Not only does Active Directory allow you to store information about objects, but it also enables you to manage those objects. After you create objects, you can use AD DS to manage and control these objects, which you can group together in containers to easily apply policies to them.

Active Directory is a powerful tool to centrally manage your network. Large organizations might want to distribute management to different teams of administrators. Active Directory enables this by allowing a domain administrator to provide lower-level administrators access to specific objects and containers.

- Manage user accounts.
- Manage groups in AD DS.
- Manage computer objects in AD DS.
- Administer AD DS by using PowerShell.
- Implement and manage OUs.

Labs: Manage AD DS Objects.

- Create and manage groups in AD DS.
- Create and configure user accounts in AD DS.
- Manage computer objects in AD DS.

Labs: Administer AD.

- Delegate administration for OUs.
- Create and modify AD DS objects with Windows PowerShell.

After completing this module, students will be able to:

- Manage objects in AD DS.
- Delegate administration in AD DS.
- Use PowerShell to manage AD DS objects.

Module 3: Advanced AD DS infrastructure management.

This module describes key technologies that serve as the building blocks of more advanced AD DS environments and provides guidance about implementing and managing such environments.

- Overview of advanced AD DS deployments.
- Deploy a distributed AD DS environment.
- Configure AD DS trusts.

Labs: Domain and trust management in AD DS.

- Implement forest trusts.
- Implement child domains in AD DS.

After completing this module, students will be able to:

- Understand the role of AD DS domains and forests in establishing security and administration boundaries.
- Identify scenarios in which having multiple AD DS domains is beneficial or required.
- Identify scenarios in which having multiple AD DS forests is beneficial or required.
- Understand considerations applicable to deploying AD DS DCs in Microsoft Azure VMs.
- Describe considerations applicable to managing users, groups, and computer objects in advanced AD DS deployments.
- Understand AD DS domain-functional levels.
- Understand AD DS forest-functional levels.
- Explain how to create a new AD DS domain.
- Install a DC in a new domain in an existing forest.
- Explain how to upgrade an AD DS environment.
- Explain how to migrate between AD DS environments.
- List factors to consider when implementing complex AD DS environments.
- Understand the trust types that you can configure in a multi-domain and multi-forest environment.
- Explain how trusts work in an AD DS forest.
- Explain how trusts work between AD DS forests.
- Describe how to configure advanced trust settings.
- Configure a forest trust.

Module 4: Implement and administer AD DS sites and replication.

In this module, you'll learn about the technical details of AD DS replication and how you can leverage that knowledge to optimize the design and implementation of AD DS environments that consist of multiple geographically distributed DCs.

- Overview of AD DS replication
- Configure AD DS sites
- Describe AD DS sites.
- Explain reasons to implement additional sites.
- Configure additional AD DS sites.
- Describe how AD DS replication works between sites.
- Describe the intersite topology generator.
- Describe SRV resource records.
- Describe how domain-joined computers locate DCs.
- Explain how to move DCs between sites.

Labs: Implement AD DS sites and replication.

- Describe AD DS site links.
- Explain the concept of site-link bridging.
- Describe how to manage intersite replication.
- Configure AD DS intersite replication.
- Describe the tools for monitoring and managing replication.

After completing this module, students will be able to:

- Describe AD DS partitions.
- Describe characteristics of AD DS replication.
- Explain how AD DS replication works within a site.
- Explain how replication conflicts are resolved.
- Explain how replication topology is generated.
- Explain how SYSVOL replication works.
- Describe AD DS sites.
- Explain reasons to implement additional sites.
- Configure additional AD DS sites.
- Describe how AD DS replication works between sites.
- Describe the intersite topology generator.
- Describe SRV resource records.
- Describe how domain-joined computers locate DCs.
- Explain how to move DCs between sites.
- Describe AD DS site links.
- Explain the concept of site-link bridging.
- Describe how to manage intersite replication.
- Configure AD DS intersite replication.
- Describe the tools for monitoring and managing replication.

Module 5: Implement Group Policy.

For organizations operating in an on-premises AD DS environment, Group Policy offers centralized management of both user and computer settings. This enables administrators to configure, enforce, and maintain their organization's on-premises configuration. GPOs are linked to container objects such as sites, domains, and OUs. Users and computers placed in those containers inherit the applicable container's settings. However, GPOs can be blocked, unlinked, or enforced to override the default application behavior. GPOs can also be filtered based on security-group membership and Windows Management Instrumentation (WMI) filters. When settings don't apply as you expect, it's important that you know how to investigate and resolve the issues.

- What is Group Policy?
- Implement and administer Group Policy.

- Group Policy scope and processing.
- Troubleshoot the application of GPOs.

Labs: Implement a Group Policy Infrastructure.

- Creating and configuring GPOs.
- Managing GPO scope.

Labs: Troubleshoot Group Policy infrastructure.

- Verify GPO application.
- Troubleshoot GPOs.

After completing this module, students will be able to:

- Describe configuration management with Group Policy.
- Describe Group Policy tools.
- Describe the benefits of Group Policy.
- Describe the Group Policy Client service and client-side extensions (CSEs).
- Describe Group Policy in Azure AD DS
- Describe domain-based GPOs.
- Describe GPO storage and replication.
- Describe Starter GPOs.
- Describe common GPO management tasks.
- Explain how to delegate administration of Group Policies.
- Delegate administration of Group Policy.
- Describe GPO links.
- Describe Group Policy processing, inheritance, and precedence.
- Use security filtering and WMI filtering to modify Group Policy scope.
- Filter Group Policy application.
- Enable or disable GPOs and GPO nodes.
- Describe loopback-policy processing.
- Describe considerations for slow links and disconnected systems.
- Identify when settings become effective.
- Describe RSoP.
- Generate RSoP reports.
- Examine Group Policy event logs.
- Detect issues with the health of GPOs.

Module 6: Manage user settings with Group Policy.

You can use GPOs to create a standard desktop for the entire organization or on a departmental basis. You construct this standard desktop by using features such as administrative templates, Folder Redirection, and Group Policy preferences.

- Implement administrative templates.
- Configure Folder Redirection, software installation, and scripts.
- Configure Group Policy preferences.

Labs: Manage user settings with Group Policy.

- Use administrative templates to manage user settings.
- Implement settings by using Group Policy preferences.
- Configure Folder Redirection.

After completing this module, students will be able to:

- Describe administrative templates.
- Describe the central store.
- Configure settings with administrative templates.
- Import security templates.
- Describe Folder Redirection.
- Explain the Folder Redirection configuration settings.
- Explain security requirements for redirected folders.
- Configure Folder Redirection.
- Manage application software using Group Policy.
- Manage scripts using Group Policy.
- Describe Group Policy preferences.
- Compare Group Policy preferences with settings.
- Explain features of Group Policy preferences.
- Implement item-level targeting.
- Configure Group Policy preferences.

Module 7: Secure AD DS.

AD DS contains sensitive information about many parts of your IT infrastructure, such as users and their passwords. An issue with your AD DS security can result in data loss, data leakage, parts of your IT infrastructure being disabled, or even your entire IT infrastructure being compromised. As an AD DS administrator, you need to understand the potential threats to AD DS and how to mitigate them.

- Secure DCs.
- Implement account security.
- Implement authentication auditing.
- Configure managed service accounts.

Labs: Secure AD DS.

- Implement security-related polices in AD DS.
- Implement Read Only Domain Controllers to secure AD DS.
- Create and manage service accounts.

After completing this module, students will be able to:

- Describe the security risks that can affect DCs.
- Modify DC security settings.
- Explain how to implement secure authentication.
- Secure physical access to DCs.
- Describe RODCs.
- Deploy an RODC.
- Plan password replication for RODCs.
- Configure password replication for RODCs.
- Explain how to separate RODC local administration.
- Explain password policies, account-lockout policies, and Kerberos authentication policies.
- Configure domain-account policies.
- Explain how to protect groups in AD DS.
- Describe fine-grained password and lockout policies.
- Create and manage PSOs.
- Configure a fine-grained password policy.
- Describe how to enhance password authentication with Windows Hello and the Microsoft Azure AD Multifactor Authentication (MFA) service.
- Explain options for securing accounts in Azure.
- Describe logon events and account logon events.
- Configure audit policies for authentication.
- Explain how to scope audit policies.
- Review logon events.
- Explain why service accounts are required.
- List the challenges of using service accounts.
- Describe how MSAs differ from standard user accounts.
- Explain the purpose and benefits of group MSAs.
- Configure group MSAs.
- Explain SPNs and Kerberos delegation.

Module 8: Deploy and manage AD CS.

Public key infrastructure (PKI) is the tools and processes that allow you to issue digital certificates, which are commonly used for authentication and to help secure network communication. You can configurate Windows Server as a CA that issues digital certificates by installing the AD CS role.

- Deploy CAs
- Administer CAs
- Troubleshoot and maintain CAs

Labs: Deploy and configure a two-tier CA hierarchy.

- Deploy an offline root CA.
- Deploy an enterprise subordinate CA.

After completing this module, students will be able to:

- Describe the AD CS server role.
- Explain the options for implementing CA hierarchies.
- Describe the differences between standalone and enterprise CAs.
- List the factors to consider when deploying a root CA.
- Deploy an enterprise root CA.
- Explain the factors that are relevant to deploying a subordinate CA.
- Deploy a CA by using a CAPolicy.inf file.
- Describe the tools available for managing CAs.
- Explain how to configure CA security.
- Describe the security roles available for CA administration.
- Configure policy and exit modules.
- Customize CDP and AIA locations for a CA.
- Configure the properties of a CA.
- Explain how to troubleshoot a CA.
- Describe the process for renewing a CA certificate.
- Explain how to move a root CA to a new server.
- Monitor CA operations.

Module 9: Deploy and manage certificates.

Planning a CA hierarchy is just the first part of implementing PKI for your organization. You also need to understand how to manage certificate templates to ensure that users and computers get certificates with the correct configuration. Additionally, you need to know how to manage certificates, including certificate revocation, and how you can use certificates for purposes such as securing network communication.

- Deploy and manage certificate templates.
- Manage certificate deployment, revocation, and recovery.
- Use certificates in a business environment.

Labs: Deploy and use certificates.

- Configure certificate templates for end users.
- Enroll for certificate and use certificates.
- Configure key recovery for critical certificates.

After completing this module, students will be able to:

- Describe certificate templates.
- List the certificate template versions in Windows Server.
- Configure certificate-template settings and permissions.
- Explain the process for updating a certificate template.
- Modify and enable a certificate template.
- List certificate enrollment methods.
- Explain how to implement certificate autoenrollment.
- Describe the purpose of an enrollment agent.
- Explain how certificate revocation works.
- Describe key archival and recovery.
- Explain how to configure automatic key archival.
- Configure a CA for key archival.
- Describe how certificates are used with TLS to help secure network communication.
- Explain how certificates are used to create digital signatures.
- Create a digitally signed document.
- Explain how certificates are used for content encryption.
- Encrypt a file with Encrypting File System (EFS).
- Describe how certificates are used for authentication.

Module 10: Implement and administer AD FS.

Windows Server provides AD FS, an SSO solution. AD FS enables organizations to provide users with the ability to sign in and authenticate to services and apps locally, in partner companies, and online. AD FS service provides SSO functionality for many services in various organizations. In this module, you'll learn how AD FS works and how to implement it in different scenarios.

- Overview of AD FS.
- AD FS requirements and planning.
- Deploy and configure AD FS.
- Web Application Proxy Overview.

Labs: Implement AD FS.

- Deploy AD FS infrastructure.
- Configure an application to use AD FS.
- Configure AD FS for a business-partner scenario.

After completing this module, students will be able to:

- Describe identity federation.
- Describe claims-based identity and claims-based authentication.
- Describe AD FS.
- Explain how AD FS enables SSO in a single organization.
- Explain how AD FS enables SSO in a business-to-business federation.
- Describe AD FS claims and claims rules.
- Describe a claims provider trust.
- Describe a relying party trust.
- Configure claims provider and relying party trusts.
- Install and configure AD FS.
- Describe how to configure an account partner and a resource partner.
- Describe how to configure claims rules.
- Explain how home realm discovery works.
- Configure claims rules.
- Manage an AD FS deployment.
- Describe WAP.
- Describe WAP authentication methods.
- Describe scenarios for using WAP.
- Explain how to install and configure WAP.
- Describe Azure AD Application Proxy.

Module 11: Implement AD DS synchronization with Microsoft Azure AD.

In this module, you'll learn how to plan, prepare, and implement directory synchronization between local AD DS and Azure AD.

- Plan and prepare for directory synchronization.
- Implement directory synchronization by using Azure AD Connect.
- Manage identities with directory synchronization.

Labs: Configure Directory Synchronization.

- Deploy directory synchronization between the AD DS and Azure AD.
- Manage users and groups in a directory synchronization scenario.

After completing this module, students will be able to:

- Explain the current AD DS scope of functionality and its limitations.
- Describe Azure AD as an authentication system.
- Describe directory synchronization.
- Plan directory synchronization.
- Describe prerequisites and preparation steps for directory synchronization.

- Configure a tenant for directory synchronization.
- Explain how AD FS and Azure AD work together.
- Describe Azure AD Connect.
- Describe Azure AD Connect requirements.
- Explain Azure AD Connect express synchronization.
- Explain Azure AD Connect customized synchronization.
- Install and configure Azure AD Connect.
- Monitor Azure AD Connect with Azure AD Connect Health.
- Describe options for identity synchronization and authentication.
- Describe writeback options with directory synchronization.
- Modify directory synchronization.
- Describe Azure AD Privileged Identity Management.
- Monitor directory synchronization.
- Troubleshoot directory synchronization.

Module 12: Monitor, manage, and recover AD DS.

At the heart of AD DS is the Active Directory database. A major responsibility for administrators is to monitor AD DS and its associated services, which ensures you're managing issues proactively. In a worst-case scenario, administrators might have to restore the Active Directory database from a backup, which requires a methodical approach to creating, testing, and performing regular backups. Microsoft provides several tools for monitoring AD DS in real time, and for storing data to recognize trends over time. There are also specific tools to help you backup and restore an Active Directory database.

- Monitor AD DS.
- Manage the Active Directory database.
- Active Directory backup and recovery solutions.

Labs: Recover Objects in AD DS.

- Backup and restore AD DS.
- Recover objects in AD DS.
- Monitor Azure AD.

After completing this module, students will be able to:

- Explain performance bottlenecks.
- Use the monitoring tools available in Windows Server.
- Understand Performance Monitor, performance objects, and counters.
- Explain how data collector sets can help you to spot performance trends.
- Describe the counters available specifically for tracking domain controller performance.
- Identify the files that comprise an Active Directory database.
- Manage the Active Directory database with Ntdsutil.exe.
- Understand restartable AD DS.
- Create and manage Active Directory snapshots.
- Understand what happens to deleted objects in Active Directory.
- Configure and use the AD Recycle Bin tool.
- Describe backup options and recovery tools in Windows Server.
- Perform Active Directory backups and restores.