Identity with Windows Server

Formerly 20742, available on Courseware Marketplace as 55351AC

About this course

This course is for IT professionals who have some knowledge about, and experience with, Windows Server identity services, and who aim to develop additional knowledge about Windows Server identity and access technologies.

By completing this course, you'll achieve the knowledge and skills to:

- Deploy Active Directory services.
- Manage directory objects.
- Execute advanced Active Directory Domain Services (AD DS) infrastructure management.
- Implement and administer AD DS sites and replication.
- Implement Group Policy.
- Manage user settings with Group Policy.
- Secure AD DS.
- Deploy and manage Active Directory Certificate Services (AD CS).
- Deploy and manage certificates.
- Implement and administer Active Directory Federation Services (AD FS).
- Implement AD DS synchronization with Microsoft Entra ID.
- Monitor, manage, and recover AD DS.

Target audience

This course is intended for IT professionals who have some experience working with Windows Server, and who are looking for a single five-day course that covers storage and compute technologies in Windows Server. This course will help them update their knowledge and skills related to storage and compute for Windows Server. This typically includes:

- AD DS administrators who want to train in identity and access technologies with Windows Server.
- 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.
- A secondary audience comprised of IT professionals who want to consolidate their knowledge about AD DS and related technologies and those who want to prepare for certification exams.

Recommended prerequisites

Before attending this course, students should 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 with, and an understanding of, core networking technologies such as IP addressing, name resolution, and Dynamic Host Configuration Protocol (DHCP).
- An awareness of basic security best practices.
- Practical working experience with Windows client operating systems such as Windows 7, Windows 10, or Windows 11.
- Basic experience with the Windows PowerShell command-line interface.
- Basic experience with Microsoft cloud services, such as Office 365.

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.

Lesson 1 Components of AD DS

- What is an AD DS forest?
- What is an AD DS domain?
- What are organizational units (OUs)?
- What is the AD DS schema?
- Overview of AD DS administration tools
- Demonstration: Manage AD DS

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe AD DS forests.
- Describe AD DS domains.
- Describe OUs.
- Describe the AD DS schema.
- Select appropriate AD DS administration tools.
- Manage AD DS.

Lesson 2 AD DS DCs

- What is a DC?
- What are the global catalog servers?
- Overview of service (SRV) records
- Demonstration: Review SRV records in Domain Name System (DNS)
- How does the AD DS sign-in process work?
- Overview of operations masters
- Transfer and seize roles

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe the DC role.

- Describe global catalog servers.
- Describe SRV records.
- Review SRV records in DNS.
- Explain how the AD DS sign-in process works.
- Describe operations masters.
- Transfer and seize roles.

Lesson 3 Deploy AD DS DCs

- Install a DC from Server Manager
- Install a DC on a Server Core
- Upgrade a DC
- Install a DC from media
- Clone DCs
- Best practices for DC virtualization

By completing this lesson, you'll achieve the knowledge and skills to:

- Install a DC.
- Install a DC on a Server Core.
- Upgrade a DC.
- Install a DC from media.
- Clone DCs.
- Describe best practices for DC virtualization.

Lesson 4 Azure AD overview

- What is Azure AD?
- How does Azure AD compare with AD DS?
- Azure AD editions
- Azure AD administration tools
- Azure AD Domain Services (Azure AD DS)

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe Azure AD.
- Compare Azure AD with AD DS.
- Describe available Azure AD editions.
- Explain the available Azure AD administration tools.
- Describe Azure AD DS.

Lab 1 Deploy and administer AD DS

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

By completing this lab, you'll achieve the knowledge and skills to:

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

By completing this module, you'll achieve the knowledge and skills to:

- Describe the AD DS components.
- Describe the role of DCs.
- Deploy DCs.
- Describe Azure AD.

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.

Lesson 1 Manage user accounts

- Create user accounts
- Demonstration: Manage user accounts
- Disable and delete user accounts
- Perform bulk operations on Active Directory objects
- Demonstration: Perform bulk operations in Active Directory Users and Computers
- User-account templates
- Demonstration: Use templates to create accounts
- Manage user objects in Azure AD

By completing this lesson, you'll achieve the knowledge and skills to:

- Create and manage user accounts.
- Configure user attributes.
- Manage inactive and disabled user accounts.
- Create and manage user profiles.
- Use graphical tools to perform bulk operations.
- Manage user objects in Azure AD.

Lesson 2 Manage groups in AD DS

- Security and distribution groups
- Group scopes
- Implement group management (IGDLA)
- Delegate management of groups in Active Directory
- Restricted groups
- Default groups
- Special identities
- Demonstration: Manage groups in Windows Server
- Manage groups in Azure AD

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe group types and scopes.
- Understand the membership rules of each group scope.
- Delegate group management.
- Understand different methods to administer groups, including Group Policy.
- Understand default, special, and restricted groups.

Lesson 3 Manage computer objects in AD DS

- The default Computers container
- Create an OU structure for managing computer objects
- Control who can create computer objects
- Join a computer to a domain
- Computer accounts and secure channels
- Offline domain joins

By completing this lesson, you'll achieve the knowledge and skills to:

- Understand the purpose of the Computers container.
- Configure the location of computer accounts.
- Control who has permission to create computer accounts.

- Join a computer to a domain.
- Join a computer to Azure AD to create a hybrid join.
- Describe computer accounts and secure channels.
- Reset the secure channel.
- Perform an offline domain join.

Lab 2 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.

By completing this lab, you'll achieve the knowledge and skills to manage objects in AD DS.

Lesson 4 Administer AD DS by using PowerShell

- Use Windows PowerShell to manage user accounts
- Use PowerShell for bulk operations
- Demonstration: Use graphical tools to perform bulk operations
- Query objects with Windows PowerShell
- Use text files for bulk operations
- Demonstration: Perform bulk operations with Windows PowerShell

By completing this lesson, you'll achieve the knowledge and skills to:

- Use PowerShell to manage user accounts.
- Use PowerShell to manage groups.
- Use PowerShell to manage computer accounts.
- Use PowerShell to manage OUs.
- Describe bulk operations.
- Use graphical tools to perform bulk operations.
- Use PowerShell to query objects.
- Use PowerShell to modify objects.
- Work with comma-separated value files (CSV files).
- Use PowerShell to perform bulk operations.

Lesson 5 Implement and manage OUs

- Plan OUs
- OU planning strategies
- Delegate administrative control

- Create OUs
- Manage permissions in Active Directory
- Demonstration: Delegate administrative permissions on an OU

By completing this lesson, you'll achieve the knowledge and skills to:

- Plan OUs.
- Describe OU hierarchy considerations.
- Describe considerations for using OUs.
- Explain AD DS permissions.
- Use OUs to delegate administration.

Lab 3 Administer Active Directory

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

By completing this lab, you'll achieve the knowledge and skills to:

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

By completing this module, you'll achieve the knowledge and skills to:

- Manage user accounts.
- Manage group objects and understand the different types of groups.
- Manage computer objects.
- Manage containers, referred to as organizational units (OUs).
- Administer Active Directory by using GUI tools and Windows PowerShell.

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.

Lesson 1 Overview of advanced AD DS deployments

- Overview of domain and forest boundaries
- Implementation of multiple domains and forests
- Deploy a DC in an Azure virtual machine (VM)
- Manage objects in complex AD DS deployments

By completing this lesson, you'll achieve the knowledge and skills 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.

Lesson 2 Deploy a distributed AD DS environment

- AD DS domain and forest-functional levels
- Deploy new AD DS domains
- Demonstration: Install a DC in a new domain in an existing forest
- Upgrade and migrate AD DS domains
- Factors to consider when implementing complex AD DS environments

By completing this lesson, you'll achieve the knowledge and skills to:

- 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.

Lesson 3 Configure AD DS trusts

- Overview of AD DS trust types
- How do trusts work in a forest?
- How do trusts work between forests?
- Configure advanced AD DS trust settings
- Demonstration: Configure a forest trust

By completing this lesson, you'll achieve the knowledge and skills to:

- 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.

Lab 4 Domain and trust management in AD DS

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

By completing this lab, you'll achieve the knowledge and skills to:

- Implement trust relationships in AD DS.
- Implement child domains in AD DS.

By completing this module, you'll achieve the knowledge and skills to:

- Describe the technologies that are essential to implementing advanced AD DS environments.
- Deploy a distributed AD DS environment.
- Implement trusts in multi-domain and multi-forest AD DS environments.

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.

Lesson 1 Overview of AD DS replication

- What are AD DS partitions?
- Characteristics of AD DS replication
- How AD DS replication works within a site
- Resolve replication conflicts
- How replication topology is generated
- How SYSVOL replication works

By completing this lesson, you'll achieve the knowledge and skills 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.

Lesson 2 Configure AD DS sites

- What are AD DS sites?
- Why implement additional sites?
- Demonstration: Configure AD DS sites
- How replication works between sites
- What is the intersite topology generator (ISTG)?
- Overview of SRV records
- How domain-joined computers locate DCs

By completing this lesson, you'll achieve the knowledge and skills to:

- 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.

Lesson 3 Configure and monitor AD DS replication

- What are AD DS site links?
- What is site-link bridging?
- Manage site-link replication.
- Demonstration: Configure AD DS intersite replication.
- Tools for monitoring and managing replication.

By completing this lesson, you'll achieve the knowledge and skills to:

- 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.

Lab 5 Implement AD DS sites and replication

- Modify the default site.
- Create additional sites and subnets.

- Configure AD DS replication.
- Monitor and troubleshoot AD DS replication.

By completing this lab, you'll achieve the knowledge and skills to:

- Manage sites and subnets in AD DS.
- Configure replication options for AD DS.
- Monitor and troubleshoot replication.

By completing this module, you'll achieve the knowledge and skills to:

- Understand how AD DS replication works.
- Configure AD DS sites to optimize authentication and replication traffic.
- Configure and monitor AD DS 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.

Lesson 1 What is Group Policy?

- What is configuration management?
- Select a Group Policy management tool
- What are the benefits of Group Policy?
- What are GPOs?
- Manage GPO scope and inheritance
- What are the Group Policy Client service and client-side extensions?
- Implement GPOs in Azure AD DS

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe configuration management with Group Policy.
- Describe Group Policy tools.
- Describe the benefits of Group Policy.
- Describe GPOs.
- Explain GPO scope and inheritance.
- Describe the Group Policy Client service and client-side extensions (CSEs).

- Describe Group Policy in Azure AD DS..

Lesson 2 Implement and administer Group Policy

- Implement domain-based GPOs
- Understand GPO storage and replication
- What are Starter GPOs?
- Common GPO management tasks
- What is Group Policy delegation?
- Demonstration: Delegate Group Policy administration

By completing this lesson, you'll achieve the knowledge and skills to:

- 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.

Lesson 3 Group Policy scope and processing

- Link GPOs to containers
- Understand Group Policy processing, inheritance, and precedence
- Implement security filtering and WMI filtering
- Demonstration: Filter Group Policy application
- Enable and disable GPOs and GPO nodes
- Implement loopback processing
- Manage slow links and disconnected systems
- Identify when settings become effective

By completing this lesson, you'll achieve the knowledge and skills to:

- 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.

Lab 6 Implement a Group Policy infrastructure

- Creating and configuring GPOs.
- Managing GPO scope.

By completing this lab, you'll achieve the knowledge and skills to:

- Create and configure GPOs.
- Manage scope for GPOs.

Lesson 4 Troubleshoot the application of GPOs

- What is Resultant Set of Policy (RSoP)?
- Demonstration: Generate RSoP reports
- Examine Group Policy event logs
- Detect issues with the health of GPOs

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe RSoP.
- Generate RSoP reports.
- Examine Group Policy event logs.
- Detect issues with the health of GPOs.

Lab 7 Troubleshoot Group Policy infrastructure

- Verify GPO application.
- Troubleshoot GPOs.

By completing this lab, you'll achieve the knowledge and skills to:

- Verify when a GPO is applied.
- Troubleshoot a GPO.

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.

Lesson 1 Implement administrative templates

- What are administrative templates?

- Overview of the central store
- Demonstration: Configure settings with administrative templates
- Import security templates

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe administrative templates.
- Describe the central store.
- Configure settings with administrative templates.
- Import security templates.

Lesson 2 Configure Folder Redirection, software installation, and scripts

- What is Folder Redirection?
- Settings for configuring Folder Redirection
- Security settings for redirected folders
- Demonstration: Configure Folder Redirection
- Manage software with Group Policy.
- Group Policy settings for applying scripts.

By completing this lesson, you'll achieve the knowledge and skills to:

- 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.

Lesson 3 Configure Group Policy preferences

- What are Group Policy preferences?
- Compare Group Policy preferences with settings
- Features of Group Policy preferences
- Item-level targeting options
- Demonstration: Configure Group Policy preferences

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe Group Policy preferences.
- Compare Group Policy preferences with settings.

- Explain features of Group Policy preferences.
- Implement item-level targeting.
- Configure Group Policy preferences.

Lab 8 Manage user settings with Group Policy

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

By completing this lab, you'll achieve the knowledge and skills to:

- Use administrative templates for management of user settings.
- Use Group Policy preferences.
- Configure Folder Redirection by using Group Policy.

By completing this module, you'll achieve the knowledge and skills to:

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

Lesson 1 Secure DCs

- What security risks can affect DCs?
- Modify security settings of DCs
- Implement secure authentication
- Secure physical access to DCs
- What are RODCs?
- Deploy an RODC
- Plan and configure an RODC password-replication policy
- Demonstration: Configure a password-replication policy
- Separate RODC local administration

By completing this lesson, you'll achieve the knowledge and skills 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.

Lesson 2 Implement account security

- Account security in Windows Server
- Understand password policies, account lockout policies, and Kerberos authentication policies
- Demonstration: Configure domain account policies
- Protect groups in AD DS.
- Fine-grained password and lockout policies.
- Create and manage Password Settings objects (PSOs).
- Demonstration: Configure a fine-grained password policy
- Enhance password authentication with Windows Hello
- Options for securing accounts in Azure AD

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe account security in Windows Server.
- 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.

Lesson 3 Implement authentication auditing

- Account logon and logon events
- Demonstration: Configure authentication-related audit policies
- Scope audit policies
- Demonstration: Review logon events

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe logon events and account logon events.
- Configure audit policies for authentication.
- Explain how to scope audit policies.
- Review logon events.

Lesson 4 Configure managed service accounts

- Overview of service accounts
- Challenges of using service accounts
- Service principal names (SPNs) and Kerberos delegation
- Overview of managed service accounts
- What are group managed service accounts (MSAs)?
- Demonstration: Configure group MSAs

By completing this lesson, you'll achieve the knowledge and skills to:

- 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.

Lab 9 Secure AD DS

- Implement security policies for accounts, passwords, and administrative groups.
- Deploy and configure an RODC.
- Create and associate a group MSA.

By completing this lab, you'll achieve the knowledge and skills to:

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

By completing this module, you'll achieve the knowledge and skills to:

- Explain how to secure DCs.
- Implement account security.
- Plan and configure audit authentication.
- Configure managed service accounts (MSAs).

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.

Lesson 1 Deploy CAs

- What is AD CS?
- Options for implementing CA hierarchies
- Standalone vs. enterprise CAs
- Factors to consider when deploying a root CA
- Demonstration: Deploy an enterprise root CA
- Considerations for deploying a subordinate CA
- How to install a CA by using the CAPolicy.inf file

By completing this lesson, you'll achieve the knowledge and skills 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.

Lesson 2 Administer CAs

- Manage CAs
- Configure CA security
- Security roles for CA administration
- Configure CA policy and exit modules
- Configure certification revocation list distribution point (CDP) and authority information access (AIA) locations
- Demonstration: Configure CA properties

By completing this lesson, you'll achieve the knowledge and skills to:

- 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.

Lesson 3 Troubleshoot and maintain CAs

- Monitor CA operations
- Troubleshoot CAs
- Renew a CA certificate
- Move a root CA to another computer

By completing this lesson, you'll achieve the knowledge and skills to:

- 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.

Lab 10 Deploy and configure a two-tier CA hierarchy

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

By completing this lab, you'll achieve the knowledge and skills to:

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

By completing this module, you'll achieve the knowledge and skills to:

- Deploy CAs.
- Administer CAs.
- Troubleshoot and maintain CAs.

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.

Lesson 1 Deploy and manage certificate templates

- What are certificates and certificate templates?
- Schema versions for certificate templates
- Configure certificate-template settings and permissions

- Options for updating a certificate template
- Demonstration: Modify and enable a certificate template

By completing this lesson, you'll achieve the knowledge and skills 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.

Lesson 2 Manage certificate deployment, revocation, and recovery

- Certificate enrollment methods
- Overview of certificate autoenrollment
- What is an enrollment agent?
- How does certificate revocation work?
- Overview of key archival and recovery
- Configure automatic key archival
- Demonstration: Configure a CA for key archival

By completing this lesson, you'll achieve the knowledge and skills to:

- 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.

Lesson 3 Use certificates in a business environment

- Use certificates for Transport Layer Security (TLS)
- Use certificates for digital signatures
- Demonstration: Sign a document digitally
- Use certificates for content encryption
- Demonstration: Encrypt a file with EFS
- Use certificates for authentication

By completing this lesson, you'll achieve the knowledge and skills to:

- 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.

Lab 11 Deploy and use certificates

- Configure certificate templates.
- Enroll and use certificates.
- Configure and implement key recovery.

By completing this lab, you'll achieve the knowledge and skills to:

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

By completing this module, you'll achieve the knowledge and skills to:

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

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.

Lesson 1 Overview of AD FS

- What is identity federation?
- What are claims-based identity and claims-based authentication?
- What is AD FS?
- How does AD FS enable SSO in a single organization?
- How does AD FS enable SSO in a business-to-business federation?

By completing this lesson, you'll achieve the knowledge and skills 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.

Lesson 2 AD FS requirements and planning

- AD FS components and requirements
- PKI and certificate requirements
- Plan an AD FS deployment for online services
- Plan a highly available AD FS deployment
- Capacity planning
- Deploy AD FS in Azure
- Demonstration: Install the AD FS server role

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe AD FS components and requirements.
- Describe PKI and certificate requirements.
- Plan AD FS deployment for online services.
- Plan a highly available AD FS deployment.
- Explain how to perform AD FS capacity planning.
- Deploy AD FS in Azure.
- Install the AD FS server role.

Lesson 3 Deploy and configure AD FS

- What are AD FS claims and claims rules?
- What is a claims provider trust?
- What is a relying party trust?
- Demonstration: Configure claims provider and relying-party trusts
- Install and configure AD FS
- Configure an account partner and resource partner
- Configure claims rules
- How does home-realm discovery work?
- Demonstration: Configure claims rules
- Manage an AD FS deployment

By completing this lesson, you'll achieve the knowledge and skills to:

- 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.

Lesson 4 Web Application Proxy overview

- What is the Web Application Proxy?
- Web Application Proxy authentication methods
- Scenarios for using Web Application Proxy
- Install and configure Web Application Proxy
- Azure AD Application Proxy overview
- Demonstration: Install and configure WAP

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe WAP.
- Describe WAP authentication methods.
- Describe scenarios for using WAP.
- Explain how to install and configure WAP.
- Describe Azure AD Application Proxy.

Lab 12 Implement AD FS

- Configure AD FS prerequisites.
- Install and configure AD FS.
- Configure an internal application for AD FS.
- Configure AD FS for federated business partners.

By completing this lab, you'll achieve the knowledge and skills to:

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

By completing this module, you'll achieve the knowledge and skills to:

- Describe Active Directory Federation Services (AD FS).
- Describe AD FS requirements and planning.
- Deploy and configure AD FS.
- Describe Application Proxy.

Module 11 Implement AD DS synchronization with Microsoft Entra ID

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

Lesson 1 Plan and prepare for directory synchronization

- AD DS scope and limitations
- Microsoft Entra ID as a cloud identity service
- Authentication with Entra ID
- Overview of directory synchronization
- Plan directory synchronization
- Prerequisites and preparation for directory synchronization
- Prepare Azure AD tenant for directory synchronization
- AD FS and Entra ID

By completing this lesson, you'll achieve the knowledge and skills to:

- Explain the current AD DS scope of functionality and its limitations.
- Describe Microsoft Entra ID as an authentication system.
- Explain the supported authentication methods for Entra ID.
- 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 Entra ID work together.
- Describe Microsoft Entra Cloud sync.

Lesson 2 Implement directory synchronization by using Entra Connect

- Overview of Entra Connect

- Entra Connect requirements
- Entra Connect express synchronization
- Entra Connect customized synchronization
- Demonstration: Install and configure Entra Connect
- Monitor directory synchronization with Entra Connect Health

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe Entra Connect.
- Describe Entra Connect requirements.
- Explain Entra Connect express synchronization.
- Explain Entra Connect customized synchronization.
- Install and configure Entra Connect.
- Monitor Entra Connect with Entra Connect Health.

Lesson 3 Manage identities with directory synchronization

- Options for identity synchronization and authentication
- Writeback options with directory synchronization
- Modify directory synchronization
- Manage privileged identities in Entra ID
- Monitor directory synchronization
- Troubleshoot directory synchronization

By completing this lesson, you'll achieve the knowledge and skills to:

- Describe options for identity synchronization and authentication.
- Describe writeback options with directory synchronization.
- Modify directory synchronization.
- Describe Entra Privileged Identity Management.
- Monitor directory synchronization.
- Troubleshoot directory synchronization.

Lab 13 Configure directory synchronization

- Prepare for directory synchronization
- Configure directory synchronization
- Manage Active Directory users and groups, and validate directory synchronization

By completing this lab, you'll achieve the knowledge and skills to:

- Deploy and configure directory synchronization.

- Manage users and groups in a directory synchronization scenario.

By completing this module, you'll achieve the knowledge and skills to:

- Plan and prepare for directory synchronization.
- Implement directory synchronization by using Microsoft Entra Connect.
- Manage identities with 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.

Lesson 1 Monitor AD DS

- Performance bottlenecks
- Potential hardware bottlenecks
- Monitoring tools in Windows Server
- Use Performance Monitor
- Demonstration: Monitor AD DS

By completing this lesson, you'll achieve the knowledge and skills 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.

Lesson 2 Manage the Active Directory database

- Active Directory database overview
- Use **NtdsUtil.exe** to manage the Active Directory database
- Demonstration: Perform database management
- Active Directory snapshots

By completing this lesson, you'll achieve the knowledge and skills to:

- 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.

Lesson 3 Active Directory backup and recovery solutions

- Understand object deletion and recovery
- Undelete objects without the recycle bin
- Enable the AD Recycle Bin tool
- Configure the AD Recycle Bin tool
- General backup and recovery tools

By completing this lesson, you'll achieve the knowledge and skills to:

- 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.

Lab 14 Recover objects in AD DS

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

By completing this lab, you'll achieve the knowledge and skills to:

- Perform backup and restore for AD DS.
- Perform object recovery in AD DS.
- Perform monitoring for Azure AD.