Identity in Windows Server

Duration: 5 Days   **Course Code: M20742**   **Version: A**

Overview:

This five-day instructor-led course teaches IT Pros how to deploy and configure Active Directory Domain Services (AD DS) in a distributed environment, how to implement Group Policy, how to perform backup and restore, and how to monitor and troubleshoot Active Directory–related issues with Windows Server 2016.

Additionally, this course teaches how to deploy other Active Directory server roles such as Active Directory Federation Services (AD FS) and Active Directory Certificate Services (AD CS).

Target Audience:

This course is primarily intended for existing IT professionals who have some AD DS knowledge and experience and who aim to develop knowledge about identity and access technologies in Windows Server 2016. This would typically include: AD DS administrators who are looking to train in identity and access technologies with Windows Server 2012 or Windows Server 2016. System or infrastructure administrators with general AD DS experience and knowledge who are looking to cross-train in core and advanced identity and access technologies in Windows Server 2012 or Windows Server 2016.

Objectives:

- Install and configure domain controllers.

- Manage objects in AD DS by using graphical tools and Windows PowerShell.

- Implement AD DS in complex environments.

- Implement AD DS sites, and configure and manage replication.

- Implement and manage Group Policy Objects (GPOs).

- Manage user settings by using GPOs.

- Secure AD DS and user accounts.

- Implement and manage a certificate authority (CA) hierarchy with AD CS.

- Deploy and manage certificates.

- Implement and administer AD FS.

- Implement and administer Active Directory Rights Management Services (AD RMS).

- Implement synchronization between AD DS and Azure AD.

- Monitor, troubleshoot, and establish business continuity for AD DS services.

Prerequisites:

- Some exposure to and 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
- Experience and an understanding of core networking technologies such as IP addressing, name resolution, and Dynamic Host Configuration Protocol (DHCP).
- 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.

Testing and Certification

-

Content:

Module 1: Installing and configuring DCs

This module describes features of AD DS and how to install domain controllers (DCs). It also covers the considerations for deploying DCs.

- Overview of AD DS
- Overview of AD DS DCs
- Deploying DCsLab : Deploying and administering AD DS
- Deploying AD DS
- Deploying a DC by performing DC cloning
- Administering AD DS by using Active Directory Administrative Center

After completing this module, students will be able to:

- Describe AD DS and its main components.
- Describe the purpose of DCs and the roles that a DC can hold.
- Describe the considerations for deploying DCs.
- Describe and perform various techniques to manage user accounts.
- Manage groups in AD DS.
- Manage computers in AD DS.
- Use Windows PowerShell to manage AD DS more efficiently.
- Delegate permission to perform AD DS administration.
- Describe the components of an advanced AD DS deployment.
- Implement a distributed AD DS environment.
- Configure AD DS trusts.
- Describe how replication works in a Windows Server 2012 AD DS environment.
- Configure AD DS sites to optimize AD DS network traffic.
- Configure and monitor AD DS replication.
- Describe the components and technologies that compose the Group Policy framework.
- Configure and understand a variety of policy setting types.
- Scope GPOs by using links, security groups, Windows Management Instrumentation (WMI) filters, loopback processing, and preference targeting.
- Troubleshoot the application of GPOs.
- Describe administrative templates.
- Configure Folder Redirection and scripts.
- Configure GPO preferences.
- Secure domain controllers.
- Implement password and lockout policies.
- Configure authentication auditing and examine the resulting audit log.
- Configure gMSAs.
- Plan and implement an AD CS CA infrastructure.
- Administer CAs.
- Troubleshoot and maintain CAs.
- Plan and implement a certificate template deployment by using an AD CS CA.

This module describes how to implement a GPO infrastructure. The module provides an overview of the components and technologies that compose the Group Policy framework.

- Introducing Group Policy
- Implementing and administering GPOs
- Group Policy scope and Group Policy processing
- Troubleshooting the application of GPOsLab : Implementing a Group Policy infrastructure
- Creating and configuring GPOs
- Managing GPO scopeLab : Troubleshooting a Group Policy infrastructure
- Verify GPO application
- Troubleshooting GPOs

After completing this module, students will be able to:

- Describe AD DS and its main components.
- Describe the purpose of DCs and the roles that a DC can hold.
- Describe the considerations for deploying DCs.
- Describe and perform various techniques to manage user accounts.
- Manage groups in AD DS.
- Manage computers in AD DS.
- Use Windows PowerShell to manage AD DS more efficiently.
- Delegate permission to perform AD DS administration.
- Describe the components of an advanced AD DS deployment.
- Implement a distributed AD DS environment.
- Configure AD DS trusts.
- Describe how replication works in a Windows Server 2012 AD DS environment.
- Configure AD DS sites to optimize AD DS network traffic.
- Configure and monitor AD DS replication.
- Describe the components and technologies that compose the Group Policy framework.
- Configure and understand a variety of policy setting types.
- Scope GPOs by using links, security groups, Windows Management Instrumentation (WMI) filters, loopback processing, and preference targeting.
- Troubleshoot the application of GPOs.
- Describe administrative templates.
- Configure Folder Redirection and scripts.
- Configure GPO preferences.
- Secure domain controllers.
- Implement password and lockout policies.
- Configure authentication auditing and

After completing this module, students will be able to:

- Describe AD DS and its main components.
- Describe the purpose of DCs and the roles that a DC can hold.
- Describe the considerations for deploying DCs.
- Describe and perform various techniques to manage user accounts.
- Manage groups in AD DS.
- Manage computers in AD DS.
- Use Windows PowerShell to manage AD DS more efficiently.
- Delegate permission to perform AD DS administration.
- Describe the components of an advanced AD DS deployment.
- Implement a distributed AD DS environment.
- Configure AD DS trusts.
- Describe how replication works in a Windows Server 2012 AD DS environment.
- Configure AD DS sites to optimize AD DS network traffic.
- Configure and monitor AD DS replication.
- Describe the components and technologies that compose the Group Policy framework.
- Configure and understand a variety of policy setting types.
- Scope GPOs by using links, security groups, Windows Management Instrumentation (WMI) filters, loopback processing, and preference targeting.
- Troubleshoot the application of GPOs.
- Describe administrative templates.
- Configure Folder Redirection and scripts.
- Configure GPO preferences.
- Secure domain controllers.
- Implement password and lockout policies.
- Configure authentication auditing and examine the resulting audit log.
- Configure gMSAs.
- Plan and implement an AD CS CA infrastructure.
- Administer CAs.
- Troubleshoot and maintain CAs.
- Plan and implement a certificate template deployment by using an AD CS CA.
- Describe and perform certificate enrollment, revocation, and recovery.
- Describe and use certificates in business environments.
- Describe how to use certificates with smart cards.
- Describe identity federation business scenarios and how AD FS can address them.
- Configure AD FS prerequisites and plan AD FS services.
- Implement AD FS to enable single sign-on (SSO) in various scenarios.

- Describe and perform certificate enrollment, revocation, and recovery.
- Describe and use certificates in business environments.
- Describe how to use certificates with smart cards.
- Describe identity federation business scenarios and how AD FS can address them.
- Configure AD FS prerequisites and plan AD FS services.
- Implement AD FS to enable single sign-on (SSO) in various scenarios.
- Describe Web Application Proxy.
- Describe AD RMS and how it can help protect content.
- Deploy and manage an AD RMS infrastructure.
- Configure content protection by using AD RMS.
- Plan and prepare for the deployment of directory synchronization.
- Configure directory synchronization by using Azure AD Connect.
- Manage identities after deploying directory synchronization.
- Monitor AD DS.
- Manage the AD DS database.
- Perform AD DS backup and restore operations, and to recover deleted objects from AD DS.

Module 2: Managing objects in AD DS

This module describes how to use various techniques to manage objects in AD DS. This includes creating and configuring user, group, and computer objects.

- Managing user accounts
- Managing groups in AD DS
- Managing computer accounts
- Using Windows PowerShell for AD DS administration
- Implementing and managing organizational unitsLab : Deploying and administering AD DS
- Creating and configuring user accounts in AD DS
- Creating and configuring groups in AD DS
- Managing computer objects in AD DSLab : Administering AD DS
- Delegating administration for a branch office
- Creating user accounts and groups by using Windows PowerShell

After completing this module, students will be able to:

- Describe AD DS and its main components.
- Describe the purpose of DCs and the roles that a DC can hold.
- Describe the considerations for deploying DCs.
- Describe and perform various techniques to

examine the resulting audit log.
- Configure gMSAs.
- Plan and implement an AD CS CA infrastructure.
- Administer CAs.
- Troubleshoot and maintain CAs.
- Plan and implement a certificate template deployment by using an AD CS CA.
- Describe and perform certificate enrollment, revocation, and recovery.
- Describe and use certificates in business environments.
- Describe how to use certificates with smart cards.
- Describe identity federation business scenarios and how AD FS can address them.
- Configure AD FS prerequisites and plan AD FS services.
- Implement AD FS to enable single sign-on (SSO) in various scenarios.
- Describe Web Application Proxy.
- Describe AD RMS and how it can help protect content.
- Deploy and manage an AD RMS infrastructure.
- Configure content protection by using AD RMS.
- Plan and prepare for the deployment of directory synchronization.
- Configure directory synchronization by using Azure AD Connect.
- Manage identities after deploying directory synchronization.
- Monitor AD DS.
- Manage the AD DS database.
- Perform AD DS backup and restore operations, and to recover deleted objects from AD DS.

Module 6: Managing user settings with GPOs

This module describes how to configure Group Policy settings and Group Policy preferences. This includes implementing administrative templates, configuring folder redirection and scripts, and configuring Group Policy preferences.

- Implementing administrative templates
- Configuring Folder Redirection and scripts
- Configuring Group Policy preferencesLab : Managing user settings with GPOs
- Using administrative templates to manage user settings
- Implement settings by using Group Policy preferences
- Configuring Folder Redirection
- Planning Group Policy (optional)

After completing this module, students will be able to:

- Describe AD DS and its main

- Describe Web Application Proxy.
- Describe AD RMS and how it can help protect content.
- Deploy and manage an AD RMS infrastructure.
- Configure content protection by using AD RMS.
- Plan and prepare for the deployment of directory synchronization.
- Configure directory synchronization by using Azure AD Connect.
- Manage identities after deploying directory synchronization.
- Monitor AD DS.
- Manage the AD DS database.
- Perform AD DS backup and restore operations, and to recover deleted objects from AD DS.

Module 10: Implementing and administering AD FS

This module describes AD FS and how to configure AD FS in a single-organization scenario and in a partner-organization scenario.

- Overview of AD FS
- AD FS requirements and planning
- Deploying and configuring AD FS
- Overview of Web Application ProxyLab : Implementing AD FS
- Configuring AD FS prerequisites
- Installing and configuring AD FS
- Configuring AD FS for a single organization
- Configuring AD FS for federated business partners

After completing this module, students will be able to:

- Describe AD DS and its main components.
- Describe the purpose of DCs and the roles that a DC can hold.
- Describe the considerations for deploying DCs.
- Describe and perform various techniques to manage user accounts.
- Manage groups in AD DS.
- Manage computers in AD DS.
- Use Windows PowerShell to manage AD DS more efficiently.
- Delegate permission to perform AD DS administration.
- Describe the components of an advanced AD DS deployment.
- Implement a distributed AD DS environment.
- Configure AD DS trusts.
- Describe how replication works in a Windows Server 2012 AD DS environment.
- Configure AD DS sites to optimize AD DS network traffic.

- manage user accounts.
- Manage groups in AD DS.
- Manage computers in AD DS.
- Use Windows PowerShell to manage AD DS more efficiently.
- Delegate permission to perform AD DS administration.
- Describe the components of an advanced AD DS deployment.
- Implement a distributed AD DS environment.
- Configure AD DS trusts.
- Describe how replication works in a Windows Server 2012 AD DS environment.
- Configure AD DS sites to optimize AD DS network traffic.
- Configure and monitor AD DS replication.
- Describe the components and technologies that compose the Group Policy framework.
- Configure and understand a variety of policy setting types.
- Scope GPOs by using links, security groups, Windows Management Instrumentation (WMI) filters, loopback processing, and preference targeting.
- Troubleshoot the application of GPOs.
- Describe administrative templates.
- Configure Folder Redirection and scripts.
- Configure GPO preferences.
- Secure domain controllers.
- Implement password and lockout policies.
- Configure authentication auditing and examine the resulting audit log.
- Configure gMSAs.
- Plan and implement an AD CS CA infrastructure.
- Administer CAs.
- Troubleshoot and maintain CAs.
- Plan and implement a certificate template deployment by using an AD CS CA.
- Describe and perform certificate enrollment, revocation, and recovery.
- Describe and use certificates in business environments.
- Describe how to use certificates with smart cards.
- Describe identity federation business scenarios and how AD FS can address them.
- Configure AD FS prerequisites and plan AD FS services.
- Implement AD FS to enable single sign-on (SSO) in various scenarios.
- Describe Web Application Proxy.
- Describe AD RMS and how it can help protect content.
- Deploy and manage an AD RMS infrastructure.
- Configure content protection by using AD RMS.
- Plan and prepare for the deployment of directory synchronization.
- Configure directory synchronization by using Azure AD Connect.
- Manage identities after deploying directory synchronization.
- Monitor AD DS.

- components.
- Describe the purpose of DCs and the roles that a DC can hold.
- Describe the considerations for deploying DCs.
- Describe and perform various techniques to manage user accounts.
- Manage groups in AD DS.
- Manage computers in AD DS.
- Use Windows PowerShell to manage AD DS more efficiently.
- Delegate permission to perform AD DS administration.
- Describe the components of an advanced AD DS deployment.
- Implement a distributed AD DS environment.
- Configure AD DS trusts.
- Describe how replication works in a Windows Server 2012 AD DS environment.
- Configure AD DS sites to optimize AD DS network traffic.
- Configure and monitor AD DS replication.
- Describe the components and technologies that compose the Group Policy framework.
- Configure and understand a variety of policy setting types.
- Scope GPOs by using links, security groups, Windows Management Instrumentation (WMI) filters, loopback processing, and preference targeting.
- Troubleshoot the application of GPOs.
- Describe administrative templates.
- Configure Folder Redirection and scripts.
- Configure GPO preferences.
- Secure domain controllers.
- Implement password and lockout policies.
- Configure authentication auditing and examine the resulting audit log.
- Configure gMSAs.
- Plan and implement an AD CS CA infrastructure.
- Administer CAs.
- Troubleshoot and maintain CAs.
- Plan and implement a certificate template deployment by using an AD CS CA.
- Describe and perform certificate enrollment, revocation, and recovery.
- Describe and use certificates in business environments.
- Describe how to use certificates with smart cards.
- Describe identity federation business scenarios and how AD FS can address them.
- Configure AD FS prerequisites and plan AD FS services.
- Implement AD FS to enable single sign-on (SSO) in various scenarios.
- Describe Web Application Proxy.
- Describe AD RMS and how it can help protect content.
- Deploy and manage an AD RMS

- Configure and monitor AD DS replication.
- Describe the components and technologies that compose the Group Policy framework.
- Configure and understand a variety of policy setting types.
- Scope GPOs by using links, security groups, Windows Management Instrumentation (WMI) filters, loopback processing, and preference targeting.
- Troubleshoot the application of GPOs.
- Describe administrative templates.
- Configure Folder Redirection and scripts.
- Configure GPO preferences.
- Secure domain controllers.
- Implement password and lockout policies.
- Configure authentication auditing and examine the resulting audit log.
- Configure gMSAs.
- Plan and implement an AD CS CA infrastructure.
- Administer CAs.
- Troubleshoot and maintain CAs.
- Plan and implement a certificate template deployment by using an AD CS CA.
- Describe and perform certificate enrollment, revocation, and recovery.
- Describe and use certificates in business environments.
- Describe how to use certificates with smart cards.
- Describe identity federation business scenarios and how AD FS can address them.
- Configure AD FS prerequisites and plan AD FS services.
- Implement AD FS to enable single sign-on (SSO) in various scenarios.
- Describe Web Application Proxy.
- Describe AD RMS and how it can help protect content.
- Deploy and manage an AD RMS infrastructure.
- Configure content protection by using AD RMS.
- Plan and prepare for the deployment of directory synchronization.
- Configure directory synchronization by using Azure AD Connect.
- Manage identities after deploying directory synchronization.
- Monitor AD DS.
- Manage the AD DS database.
- Perform AD DS backup and restore operations, and to recover deleted objects from AD DS.

Module 11: Implementing and administering AD RMS

This module describes how to implement an AD RMS deployment. The module provides an overview of AD RMS, explains how to deploy and manage an AD RMS infrastructure, and explains how to configure

- Manage the AD DS database.
- Perform AD DS backup and restore operations, and to recover deleted objects from AD DS.

Module 3: Advanced AD DS infrastructure management

This module describes how to plan and implement an AD DS deployment that includes multiple domains and forests. The module provides an overview of the components in an advanced AD DS deployment, the process of implementing a distributed AD DS environment, and the procedure for configuring AD DS trusts.

- Overview of advanced AD DS deployments
- Deploying a distributed AD DS environment
- Configuring AD DS trustsLab : Domain and trust management in AD DS
- Implementing child domains in AD DS
- Implementing forest trusts

After completing this module, students will be able to:

- Describe AD DS and its main components.
- Describe the purpose of DCs and the roles that a DC can hold.
- Describe the considerations for deploying DCs.
- Describe and perform various techniques to manage user accounts.
- Manage groups in AD DS.
- Manage computers in AD DS.
- Use Windows PowerShell to manage AD DS more efficiently.
- Delegate permission to perform AD DS administration.
- Describe the components of an advanced AD DS deployment.
- Implement a distributed AD DS environment.
- Configure AD DS trusts.
- Describe how replication works in a Windows Server 2012 AD DS environment.
- Configure AD DS sites to optimize AD DS network traffic.
- Configure and monitor AD DS replication.
- Describe the components and technologies that compose the Group Policy framework.
- Configure and understand a variety of policy setting types.
- Scope GPOs by using links, security groups, Windows Management Instrumentation (WMI) filters, loopback processing, and preference targeting.
- Troubleshoot the application of GPOs.
- Describe administrative templates.
- Configure Folder Redirection and scripts.
- Configure GPO preferences.
- Secure domain controllers.
- Implement password and lockout policies.
- Configure authentication auditing and examine the resulting audit log.
- Configure gMSAs.

infrastructure.
- Configure content protection by using AD RMS.
- Plan and prepare for the deployment of directory synchronization.
- Configure directory synchronization by using Azure AD Connect.
- Manage identities after deploying directory synchronization.
- Monitor AD DS.
- Manage the AD DS database.
- Perform AD DS backup and restore operations, and to recover deleted objects from AD DS.

Module 7: Securing AD DS

This module describes how to configure domain controller security, account security, password security, and Group Managed Service Accounts (gMSA).

- Securing domain controllers
- Implementing account security
- Audit authentication
- Configuring managed service accounts (MSAs)Lab : Securing AD DS
- Implementing security policies for accounts and passwords
- Implementing administrative security policies
- Deploying and configuring a read-only domain controller (RODC)
- Creating and associating a gMSA

After completing this module, students will be able to:

- Describe AD DS and its main components.
- Describe the purpose of DCs and the roles that a DC can hold.
- Describe the considerations for deploying DCs.
- Describe and perform various techniques to manage user accounts.
- Manage groups in AD DS.
- Manage computers in AD DS.
- Use Windows PowerShell to manage AD DS more efficiently.
- Delegate permission to perform AD DS administration.
- Describe the components of an advanced AD DS deployment.
- Implement a distributed AD DS environment.
- Configure AD DS trusts.
- Describe how replication works in a Windows Server 2012 AD DS environment.
- Configure AD DS sites to optimize AD DS network traffic.
- Configure and monitor AD DS replication.
- Describe the components and technologies that compose the Group

AD RMS content protection.

- Overview of AD RMS
- Deploying and managing an AD RMS infrastructure
- Configuring AD RMS content protectionLab : Implementing an AD RMS infrastructure
- Installing and configuring AD RMS
- Configuring AD RMS templates
- Using AD RMS on clients

After completing this module, students will be able to:

- Describe AD DS and its main components.
- Describe the purpose of DCs and the roles that a DC can hold.
- Describe the considerations for deploying DCs.
- Describe and perform various techniques to manage user accounts.
- Manage groups in AD DS.
- Manage computers in AD DS.
- Use Windows PowerShell to manage AD DS more efficiently.
- Delegate permission to perform AD DS administration.
- Describe the components of an advanced AD DS deployment.
- Implement a distributed AD DS environment.
- Configure AD DS trusts.
- Describe how replication works in a Windows Server 2012 AD DS environment.
- Configure AD DS sites to optimize AD DS network traffic.
- Configure and monitor AD DS replication.
- Describe the components and technologies that compose the Group Policy framework.
- Configure and understand a variety of policy setting types.
- Scope GPOs by using links, security groups, Windows Management Instrumentation (WMI) filters, loopback processing, and preference targeting.
- Troubleshoot the application of GPOs.
- Describe administrative templates.
- Configure Folder Redirection and scripts.
- Configure GPO preferences.
- Secure domain controllers.
- Implement password and lockout policies.
- Configure authentication auditing and examine the resulting audit log.
- Configure gMSAs.
- Plan and implement an AD CS CA infrastructure.
- Administer CAs.
- Troubleshoot and maintain CAs.
- Plan and implement a certificate template deployment by using an AD CS CA.
- Describe and perform certificate enrollment, revocation, and recovery.
- Describe and use certificates in business

- Plan and implement an AD CS CA infrastructure.
- Administer CAs.
- Troubleshoot and maintain CAs.
- Plan and implement a certificate template deployment by using an AD CS CA.
- Describe and perform certificate enrollment, revocation, and recovery.
- Describe and use certificates in business environments.
- Describe how to use certificates with smart cards.
- Describe identity federation business scenarios and how AD FS can address them.
- Configure AD FS prerequisites and plan AD FS services.
- Implement AD FS to enable single sign-on (SSO) in various scenarios.
- Describe Web Application Proxy.
- Describe AD RMS and how it can help protect content.
- Deploy and manage an AD RMS infrastructure.
- Configure content protection by using AD RMS.
- Plan and prepare for the deployment of directory synchronization.
- Configure directory synchronization by using Azure AD Connect.
- Manage identities after deploying directory synchronization.
- Monitor AD DS.
- Manage the AD DS database.
- Perform AD DS backup and restore operations, and to recover deleted objects from AD DS.

Module 4: Implementing and administering AD DS sites and replication

This module describes how to plan and implement an AD DS deployment that includes multiple locations. The module explains how replication works in a Windows Server 2016 AD DS environment.

- Overview of AD DS replication
- Configuring AD DS sites
- Configuring and monitoring AD DS replicationLab : Managing and implementing AD DS sites and replication
- Modifying the default site
- Creating additional sites and subnets
- Configuring AD DS replication
- Monitoring and troubleshooting AD DS replication

After completing this module, students will be able to:

- Describe AD DS and its main components.
- Describe the purpose of DCs and the roles that a DC can hold.
- Describe the considerations for deploying

Policy framework.
- Configure and understand a variety of policy setting types.
- Scope GPOs by using links, security groups, Windows Management Instrumentation (WMI) filters, loopback processing, and preference targeting.
- Troubleshoot the application of GPOs.
- Describe administrative templates.
- Configure Folder Redirection and scripts.
- Configure GPO preferences.
- Secure domain controllers.
- Implement password and lockout policies.
- Configure authentication auditing and examine the resulting audit log.
- Configure gMSAs.
- Plan and implement an AD CS CA infrastructure.
- Administer CAs.
- Troubleshoot and maintain CAs.
- Plan and implement a certificate template deployment by using an AD CS CA.
- Describe and perform certificate enrollment, revocation, and recovery.
- Describe and use certificates in business environments.
- Describe how to use certificates with smart cards.
- Describe identity federation business scenarios and how AD FS can address them.
- Configure AD FS prerequisites and plan AD FS services.
- Implement AD FS to enable single sign-on (SSO) in various scenarios.
- Describe Web Application Proxy.
- Describe AD RMS and how it can help protect content.
- Deploy and manage an AD RMS infrastructure.
- Configure content protection by using AD RMS.
- Plan and prepare for the deployment of directory synchronization.
- Configure directory synchronization by using Azure AD Connect.
- Manage identities after deploying directory synchronization.
- Monitor AD DS.
- Manage the AD DS database.
- Perform AD DS backup and restore operations, and to recover deleted objects from AD DS.

Module 8: Deploying and managing AD CS

This module describes how to implement an AD CS deployment. This includes deploying, administering, and troubleshooting CAs.

- Deploying CAs
- Administering CAs
- Troubleshooting and maintaining CAsLab : Deploying and configuring a two-tier CA

environments.
- Describe how to use certificates with smart cards.
- Describe identity federation business scenarios and how AD FS can address them.
- Configure AD FS prerequisites and plan AD FS services.
- Implement AD FS to enable single sign-on (SSO) in various scenarios.
- Describe Web Application Proxy.
- Describe AD RMS and how it can help protect content.
- Deploy and manage an AD RMS infrastructure.
- Configure content protection by using AD RMS.
- Plan and prepare for the deployment of directory synchronization.
- Configure directory synchronization by using Azure AD Connect.
- Manage identities after deploying directory synchronization.
- Monitor AD DS.
- Manage the AD DS database.
- Perform AD DS backup and restore operations, and to recover deleted objects from AD DS.

Module 12: Implementing AD DS synchronization with Azure AD

This module describes how to plan and configure directory syncing between Microsoft Azure Active Directory (Azure AD) and on-premises AD DS. The modules describes various sync scenarios, such as Azure AD sync, AD FS and Azure AD, and Azure AD Connect.

- Planning and preparing for directory synchronization
- Implementing directory synchronization by using Azure AD Connect
- Managing identities with directory synchronizationLab : Configuring directory synchronization
- Preparing for directory synchronization
- Configuring directory synchronization
- Managing Active Directory users and groups

After completing this module, students will be able to:

- Describe AD DS and its main components.
- Describe the purpose of DCs and the roles that a DC can hold.
- Describe the considerations for deploying DCs.
- Describe and perform various techniques to manage user accounts.
- Manage groups in AD DS.
- Manage computers in AD DS.
- Use Windows PowerShell to manage AD

DCs.

- Describe and perform various techniques to manage user accounts.
- Manage groups in AD DS.
- Manage computers in AD DS.
- Use Windows PowerShell to manage AD DS more efficiently.
- Delegate permission to perform AD DS administration.
- Describe the components of an advanced AD DS deployment.
- Implement a distributed AD DS environment.
- Configure AD DS trusts.
- Describe how replication works in a Windows Server 2012 AD DS environment.
- Configure AD DS sites to optimize AD DS network traffic.
- Configure and monitor AD DS replication.
- Describe the components and technologies that compose the Group Policy framework.
- Configure and understand a variety of policy setting types.
- Scope GPOs by using links, security groups, Windows Management Instrumentation (WMI) filters, loopback processing, and preference targeting.
- Troubleshoot the application of GPOs.
- Describe administrative templates.
- Configure Folder Redirection and scripts.
- Configure GPO preferences.
- Secure domain controllers.
- Implement password and lockout policies.
- Configure authentication auditing and examine the resulting audit log.
- Configure gMSAs.
- Plan and implement an AD CS CA infrastructure.
- Administer CAs.
- Troubleshoot and maintain CAs.
- Plan and implement a certificate template deployment by using an AD CS CA.
- Describe and perform certificate enrollment, revocation, and recovery.
- Describe and use certificates in business environments.
- Describe how to use certificates with smart cards.
- Describe identity federation business scenarios and how AD FS can address them.
- Configure AD FS prerequisites and plan AD FS services.
- Implement AD FS to enable single sign-on (SSO) in various scenarios.
- Describe Web Application Proxy.
- Describe AD RMS and how it can help protect content.
- Deploy and manage an AD RMS infrastructure.
- Configure content protection by using AD RMS.
- Plan and prepare for the deployment of directory synchronization.
- Configure directory synchronization by using Azure AD Connect.
- Manage identities after deploying directory

hierarchy

- Deploying an offline root CA
- Deploying an enterprise subordinate CA

After completing this module, students will be able to:

- Describe AD DS and its main components.
- Describe the purpose of DCs and the roles that a DC can hold.
- Describe the considerations for deploying DCs.
- Describe and perform various techniques to manage user accounts.
- Manage groups in AD DS.
- Manage computers in AD DS.
- Use Windows PowerShell to manage AD DS more efficiently.
- Delegate permission to perform AD DS administration.
- Describe the components of an advanced AD DS deployment.
- Implement a distributed AD DS environment.
- Configure AD DS trusts.
- Describe how replication works in a Windows Server 2012 AD DS environment.
- Configure AD DS sites to optimize AD DS network traffic.
- Configure and monitor AD DS replication.
- Describe the components and technologies that compose the Group Policy framework.
- Configure and understand a variety of policy setting types.
- Scope GPOs by using links, security groups, Windows Management Instrumentation (WMI) filters, loopback processing, and preference targeting.
- Troubleshoot the application of GPOs.
- Describe administrative templates.
- Configure Folder Redirection and scripts.
- Configure GPO preferences.
- Secure domain controllers.
- Implement password and lockout policies.
- Configure authentication auditing and examine the resulting audit log.
- Configure gMSAs.
- Plan and implement an AD CS CA infrastructure.
- Administer CAs.
- Troubleshoot and maintain CAs.
- Plan and implement a certificate template deployment by using an AD CS CA.
- Describe and perform certificate enrollment, revocation, and recovery.
- Describe and use certificates in business environments.
- Describe how to use certificates with smart cards.
- Describe identity federation business scenarios and how AD FS can address them.

DS more efficiently.

- Delegate permission to perform AD DS administration.
- Describe the components of an advanced AD DS deployment.
- Implement a distributed AD DS environment.
- Configure AD DS trusts.
- Describe how replication works in a Windows Server 2012 AD DS environment.
- Configure AD DS sites to optimize AD DS network traffic.
- Configure and monitor AD DS replication.
- Describe the components and technologies that compose the Group Policy framework.
- Configure and understand a variety of policy setting types.
- Scope GPOs by using links, security groups, Windows Management Instrumentation (WMI) filters, loopback processing, and preference targeting.
- Troubleshoot the application of GPOs.
- Describe administrative templates.
- Configure Folder Redirection and scripts.
- Configure GPO preferences.
- Secure domain controllers.
- Implement password and lockout policies.
- Configure authentication auditing and examine the resulting audit log.
- Configure gMSAs.
- Plan and implement an AD CS CA infrastructure.
- Administer CAs.
- Troubleshoot and maintain CAs.
- Plan and implement a certificate template deployment by using an AD CS CA.
- Describe and perform certificate enrollment, revocation, and recovery.
- Describe and use certificates in business environments.
- Describe how to use certificates with smart cards.
- Describe identity federation business scenarios and how AD FS can address them.
- Configure AD FS prerequisites and plan AD FS services.
- Implement AD FS to enable single sign-on (SSO) in various scenarios.
- Describe Web Application Proxy.
- Describe AD RMS and how it can help protect content.
- Deploy and manage an AD RMS infrastructure.
- Configure content protection by using AD RMS.
- Plan and prepare for the deployment of directory synchronization.
- Configure directory synchronization by using Azure AD Connect.
- Manage identities after deploying directory synchronization.
- Monitor AD DS.
- Manage the AD DS database.

synchronization.
- Monitor AD DS.
- Manage the AD DS database.
- Perform AD DS backup and restore operations, and to recover deleted objects from AD DS.

Module 5: Implementing Group Policy

- Configure AD FS prerequisites and plan AD FS services.
- Implement AD FS to enable single sign-on (SSO) in various scenarios.
- Describe Web Application Proxy.
- Describe AD RMS and how it can help protect content.
- Deploy and manage an AD RMS infrastructure.
- Configure content protection by using AD RMS.
- Plan and prepare for the deployment of directory synchronization.
- Configure directory synchronization by using Azure AD Connect.
- Manage identities after deploying directory synchronization.
- Monitor AD DS.
- Manage the AD DS database.
- Perform AD DS backup and restore operations, and to recover deleted objects from AD DS.

Module 9: Deploying and managing certificates

This module describes how to deploy and manage certificates in an AD DS environment. This involves deploying and managing certificate templates, managing certificate revocation and recovery, using certificates in a business environment, and implementing smart cards.

- Deploying and managing certificate templates
- Managing certificate deployment, revocation, and recovery
- Using certificates in a business environment
- Implementing and managing smart cardsLab : Deploying certificates
- Configuring certificate templates
- Enrolling and using certificates
- Configuring and implementing key recovery

- Perform AD DS backup and restore operations, and to recover deleted objects from AD DS.

Module 13: Monitoring, managing, and recovering AD DS

This module describes how to monitor, manage, and maintain AD DS to help achieve high availability of AD DS.

- Monitoring AD DS
- Managing the AD DS database
- Recovering AD DS objectsLab : Recovering objects in AD DS
- Backing up and restoring AD DS
- Recovering objects in AD DS

After completing this module, students will be able to:

- Describe AD DS and its main components.
- Describe the purpose of DCs and the roles that a DC can hold.
- Describe the considerations for deploying DCs.
- Describe and perform various techniques to manage user accounts.
- Manage groups in AD DS.
- Manage computers in AD DS.
- Use Windows PowerShell to manage AD DS more efficiently.
- Delegate permission to perform AD DS administration.
- Describe the components of an advanced AD DS deployment.
- Implement a distributed AD DS environment.
- Configure AD DS trusts.
- Describe how replication works in a Windows Server 2012 AD DS environment.
- Configure AD DS sites to optimize AD DS network traffic.
- Configure and monitor AD DS replication.
- Describe the components and technologies that compose the Group Policy framework.
- Configure and understand a variety of policy setting types.
- Scope GPOs by using links, security groups, Windows Management Instrumentation (WMI) filters, loopback processing, and preference targeting.
- Troubleshoot the application of GPOs.
- Describe administrative templates.
- Configure Folder Redirection and scripts.
- Configure GPO preferences.
- Secure domain controllers.
- Implement password and lockout policies.
- Configure authentication auditing and examine the resulting audit log.
- Configure gMSAs.
- Plan and implement an AD CS CA infrastructure.

- Administer CAs.
- Troubleshoot and maintain CAs.
- Plan and implement a certificate template deployment by using an AD CS CA.
- Describe and perform certificate enrollment, revocation, and recovery.
- Describe and use certificates in business environments.
- Describe how to use certificates with smart cards.
- Describe identity federation business scenarios and how AD FS can address them.
- Configure AD FS prerequisites and plan AD FS services.
- Implement AD FS to enable single sign-on (SSO) in various scenarios.
- Describe Web Application Proxy.
- Describe AD RMS and how it can help protect content.
- Deploy and manage an AD RMS infrastructure.
- Configure content protection by using AD RMS.
- Plan and prepare for the deployment of directory synchronization.
- Configure directory synchronization by using Azure AD Connect.
- Manage identities after deploying directory synchronization.
- Monitor AD DS.
- Manage the AD DS database.
- Perform AD DS backup and restore operations, and to recover deleted objects from AD DS.

Further Information:

For More information, or to book your course, please Email us on:

KENYA - training.kenya@clclearningafrica.com

TANZANIA - training.tanzania@clclearningafrica.com

UGANDA - training.uganda@clclearningafrica.com

RWANDA - training.rwanda@clclearningafrica.com

UAE - training.emea@clclearningafrica.com