

## Active Directory services with Windows Server

**Duration: 5 Days**    **Course Code: M10969**    **Version: B**    **Delivery Method: Virtual Learning**

### Overview:

EOL - 30/12/21

Get Hands on instruction and practice administering Active Directory technologies in Windows Server 2012 and Windows Server 2012 R2 in this 5-day Microsoft Official Course. You will learn the skills you need to better manage and protect data access and information, simplify deployment and management of your identity infrastructure, and provide more secure access to data. You will learn how to configure some of the key features in Active Directory such as Active Directory Domain Services (AD DS), Group Policy, Dynamic Access Control (DAC), Work Folders, Work Place Join, Certificate Services, Rights Management Services (RMS), Federation Services, as well as integrating your on premise environment with cloud based technologies such as Windows Azure Active Directory. As part of the learning experience, you will perform hands-on exercises in a virtual lab environment.

### Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

### Target Audience:

This course is intended for Information Technology (IT) Professionals who have Active Directory Domain Services (AD DS) experience and are looking to for a single course that will further develop knowledge and skills using Access and Information Protection technologies in Windows Server 2012 and Windows Server 2012 R2. This would typically include: AD DS Administrators who are looking to further develop skills in the latest Access and Information Protection technologies with Windows Server 2012 and Windows Server 2012 R2. System or Infrastructure administrators with general AD DS experience and knowledge who are looking to build upon that core knowledge and cross-train into advanced Active Directory technologies in Windows Server 2012 and Windows Server 2012 R2. IT Professionals who have taken the 10967A: Fundamentals of a Windows Server Infrastructure course and are looking to build upon that Active directory knowledge.

### Objectives:

- After completing this course, students will be able to:
- Understand available solutions for identity management and be able to address scenarios with appropriate solutions. Deploy and administer AD DS in Windows Server 2012.
- Secure AD DS deployment.
- Implement AD DS sites, configure and manage replication
- Implement and manage Group Policy
- Manage user settings with Group Policy
- Implement certification authority (CA) hierarchy with AD CS and how to manage CAs.
- Implement, deploy and manage certificates.
- Implement and manage AD RMS.
- Implement and administer AD FS.
- Secure and provision data access using technologies such as Dynamic Access Control, Work Folders and Workplace Join
- Monitor, troubleshoot and establish business continuity for AD DS services.
- Implement Windows Azure Active Directory.
- Implement and administer Active Directory Lightweight Directory Services (AD LDS).

### Prerequisites:

- Before attending this course, students must have:
- Experience working with Active Directory Domain Services (AD DS)
- Experience working in a Windows Server Infrastructure enterprise environment

- Experience working with and troubleshooting core networking infrastructure technologies such as name resolution, IP Addressing, Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP)
  - Experience working with Hyper-V and Server Virtualization concepts
  - An awareness and understanding of general security best practices
  - Experience working hands on with Windows client operating systems such as Windows Vista, Windows 7 or Windows 8
-

## Content:

**Module 1: Overview of Access and Information Protection**This module provides an overview of multiple Access and Information Protection (AIP) technologies and services what are available with Windows Server 2012 and Windows Server 2012 R2 from a business perspective and maps business problems to technical solutions. It also includes coverage of Forefront Identify Manager (FIM).Lessons

- Introduction to Access and Information Protection Solutions in Business
- Overview of AIP Solutions in Windows Server 2012
- Overview of FIM 2010 R2

Lab : Choosing an Appropriate Access and Information Protection Management Solution

After completing this module students will be able to:

- Describe Access and Information Protection solutions in business.
- Describe Access and Information Protection solutions in Windows Server 2012 and Windows Server 2012 R2.
- Describe Microsoft Forefront Identity Manager (FIM) 2010 R2.

**Module 2: Advanced Deployment and Administration of AD DS**This module explains how to deploy AD DS remotely and describes the virtualization safeguards, cloning abilities and extending AD DS to the cloud.Lessons

- Deploying AD DS
- Deploying and Cloning Virtual Domain Controllers
- Deploying Domain Controllers in Windows Azure
- Administering AD DS

Lab : Deploying and Administering AD DS

After completing this module, students will be able to:

- Describe and perform various deployment techniques for AD DS.
- Describe virtual domain controller deployment considerations.
- Explain how new technologies in Windows Server 2012 and Windows Server 2012 R2 support virtual domain controllers.
- Describe Domain Controller cloning.
- Implement AD DS using the tools provided in Windows Server 2012 and Windows Server 2012 R2.
- Understand the importance of securing domain controllers.

**Module 6: Managing User Settings with Group Policy**This module describes how to use GPO Administrative Templates, Folder Redirection, and Group Policy features to configure users' computer settings.Lessons

- Implementing Administrative Templates
- Configuring Folder Redirection and Scripts
- Configuring Group Policy Preferences

Lab : Managing User Desktops with Group Policy

After completing this module, students will be able to:

- Describe and perform various deployment techniques for AD DS.
- Describe virtual domain controller deployment considerations.
- Explain how new technologies in Windows Server 2012 and Windows Server 2012 R2 support virtual domain controllers.
- Describe Domain Controller cloning.
- Implement AD DS using the tools provided in Windows Server 2012 and Windows Server 2012 R2.
- Understand the importance of securing domain controllers.
- Describe the benefit of read-only domain controllers (RODCs).
- Explain and implement password and account lockout policies.
- Implement audit authentication.
- Describe AD DS replication.
- Configure AD DS sites.
- Configure and monitor AD DS replication.
- Describe Group Policy.
- Implement and administer GPOs.
- Describe Group Policy scope and Group Policy processing.
- Troubleshoot the application of GPOs.
- Implement Administrative Templates.
- Configure Folder Redirection and scripts.
- Configure Group Policy preferences.
- Deploy Certificate Authorities.
- Administer Certificate Authorities.
- Troubleshoot, maintain, and monitor Certificate Authorities.
- Use certificates in business environments.
- Deploy and manage certificate templates.
- Manage certificates deployment, revocation and recovery.
- Implement and manage smart cards.
- Describe AD RMS.
- Explain how to deploy and manage an AD RMS infrastructure.
- Explain how to configure AD RMS content protection.

**Module 11: Implementing Secure Shared File Access**This module explains how to use Dynamic Access Control (DAC), Work Folders, Work place Join and how to plan and implement these technologies.Lessons

- Overview of Dynamic Access Control
- Implementing DAC Components
- Implementing DAC for Access Control
- Implementing Access Denied Assistance
- Implementing and Managing Work Folders
- Implementing Workplace Join

Lab : Implementing Secure File Access

After completing this module, students will be able to:

- Describe and perform various deployment techniques for AD DS.
- Describe virtual domain controller deployment considerations.
- Explain how new technologies in Windows Server 2012 and Windows Server 2012 R2 support virtual domain controllers.
- Describe Domain Controller cloning.
- Implement AD DS using the tools provided in Windows Server 2012 and Windows Server 2012 R2.
- Understand the importance of securing domain controllers.
- Describe the benefit of read-only domain controllers (RODCs).
- Explain and implement password and account lockout policies.
- Implement audit authentication.
- Describe AD DS replication.
- Configure AD DS sites.
- Configure and monitor AD DS replication.
- Describe Group Policy.
- Implement and administer GPOs.
- Describe Group Policy scope and Group Policy processing.
- Troubleshoot the application of GPOs.
- Implement Administrative Templates.
- Configure Folder Redirection and scripts.
- Configure Group Policy preferences.
- Deploy Certificate Authorities.
- Administer Certificate Authorities.
- Troubleshoot, maintain, and monitor Certificate Authorities.
- Use certificates in business environments.
- Deploy and manage certificate templates.
- Manage certificates deployment, revocation and recovery.
- Implement and manage smart cards.
- Describe AD RMS.
- Explain how to deploy and manage an AD RMS infrastructure.
- Explain how to configure AD RMS content protection.
- Explain how to configure external access

- Describe the benefit of read-only domain controllers (RODCs).
- Explain and implement password and account lockout policies.
- Implement audit authentication.
- Describe AD DS replication.
- Configure AD DS sites.
- Configure and monitor AD DS replication.
- Describe Group Policy.
- Implement and administer GPOs.
- Describe Group Policy scope and Group Policy processing.
- Troubleshoot the application of GPOs.
- Implement Administrative Templates.
- Configure Folder Redirection and scripts.
- Configure Group Policy preferences.
- Deploy Certificate Authorities.
- Administer Certificate Authorities.
- Troubleshoot, maintain, and monitor Certificate Authorities.
- Use certificates in business environments.
- Deploy and manage certificate templates.
- Manage certificates deployment, revocation and recovery.
- Implement and manage smart cards.
- Describe AD RMS.
- Explain how to deploy and manage an AD RMS infrastructure.
- Explain how to configure AD RMS content protection.
- Explain how to configure external access to AD RMS.
- Describe AD FS.
- Explain how to configure the AD FS prerequisites, and deploy AD FS services.
- Describe how to implement AD FS for a single organization.
- Deploy AD FS in a business-to-business federation scenario.
- Deploy the Web Application Proxy.
- Describe DAC.
- Implement DAC components.
- Implement DAC for access control.
- Implement access-denied assistance.
- Implement and manage Work Folders.
- Implement Workplace Join.
- Monitor AD DS.
- Manage the AD DS database.
- Recover objects from the AD DS database.
- Describe Windows Azure AD.
- Administer Azure AD.
- Describe AD LDS.
- Explain how to deploy AD LDS.
- Explain how to configure AD LDS instances and partitions.

Module 3: Securing AD DS This module describes the threats to domain controllers and what methods can be used to secure the AD DS and its domain controllers. Lessons

- Securing Domain Controllers
- Implementing Account Security
- Implementing Audit Authentication

- Explain how to configure external access to AD RMS.
- Describe AD FS.
- Explain how to configure the AD FS prerequisites, and deploy AD FS services.
- Describe how to implement AD FS for a single organization.
- Deploy AD FS in a business-to-business federation scenario.
- Deploy the Web Application Proxy.
- Describe DAC.
- Implement DAC components.
- Implement DAC for access control.
- Implement access-denied assistance.
- Implement and manage Work Folders.
- Implement Workplace Join.
- Monitor AD DS.
- Manage the AD DS database.
- Recover objects from the AD DS database.
- Describe Windows Azure AD.
- Administer Azure AD.
- Describe AD LDS.
- Explain how to deploy AD LDS.
- Explain how to configure AD LDS instances and partitions.

Module 7: Deploying and Managing AD CS This module explain how to deploy and manage Certificate Authorities (CAs) with Active Directory Certificate Services (AD CS) Lessons

- Deploying CAs
- Administering CAs
- Troubleshooting, Maintaining, and Monitoring CAs

Lab : Deploying and Configuring a Two-Tier CA Hierarchy

After completing this module, students will be able to:

- Describe and perform various deployment techniques for AD DS.
- Describe virtual domain controller deployment considerations.
- Explain how new technologies in Windows Server 2012 and Windows Server 2012 R2 support virtual domain controllers.
- Describe Domain Controller cloning.
- Implement AD DS using the tools provided in Windows Server 2012 and Windows Server 2012 R2.
- Understand the importance of securing domain controllers.
- Describe the benefit of read-only domain controllers (RODCs).
- Explain and implement password and account lockout policies.
- Implement audit authentication.

- to AD RMS.
- Describe AD FS.
- Explain how to configure the AD FS prerequisites, and deploy AD FS services.
- Describe how to implement AD FS for a single organization.
- Deploy AD FS in a business-to-business federation scenario.
- Deploy the Web Application Proxy.
- Describe DAC.
- Implement DAC components.
- Implement DAC for access control.
- Implement access-denied assistance.
- Implement and manage Work Folders.
- Implement Workplace Join.
- Monitor AD DS.
- Manage the AD DS database.
- Recover objects from the AD DS database.
- Describe Windows Azure AD.
- Administer Azure AD.
- Describe AD LDS.
- Explain how to deploy AD LDS.
- Explain how to configure AD LDS instances and partitions.

Module 12: Monitoring, Managing, and Recovering AD DS This module explains how to use tools that help monitor performance in real time, and how to record performance over time to spot potential problems by observing performance trends. This module also explains how to optimize and protect your directory service and related identity and access solutions so that if a service does fail, you can restart it as quickly as possible. Lessons

- Monitoring AD DS
- Managing the AD DS Database
- AD DS Backup and Recovery Options for AD DS and Other Identity and Access Solutions

Lab : Monitoring AD DS Lab : Recovering Objects in AD DS

After completing this module, students will be able to:

- Describe and perform various deployment techniques for AD DS.
- Describe virtual domain controller deployment considerations.
- Explain how new technologies in Windows Server 2012 and Windows Server 2012 R2 support virtual domain controllers.
- Describe Domain Controller cloning.
- Implement AD DS using the tools provided in Windows Server 2012 and Windows Server 2012 R2.
- Understand the importance of securing domain controllers.
- Describe the benefit of read-only domain

## Lab : Securing AD DS

After completing this module, students will be able to:

- Describe and perform various deployment techniques for AD DS.
- Describe virtual domain controller deployment considerations.
- Explain how new technologies in Windows Server 2012 and Windows Server 2012 R2 support virtual domain controllers.
- Describe Domain Controller cloning.
- Implement AD DS using the tools provided in Windows Server 2012 and Windows Server 2012 R2.
- Understand the importance of securing domain controllers.
- Describe the benefit of read-only domain controllers (RODCs).
- Explain and implement password and account lockout policies.
- Implement audit authentication.
- Describe AD DS replication.
- Configure AD DS sites.
- Configure and monitor AD DS replication.
- Describe Group Policy.
- Implement and administer GPOs.
- Describe Group Policy scope and Group Policy processing.
- Troubleshoot the application of GPOs.
- Implement Administrative Templates.
- Configure Folder Redirection and scripts.
- Configure Group Policy preferences.
- Deploy Certificate Authorities.
- Administer Certificate Authorities.
- Troubleshoot, maintain, and monitor Certificate Authorities.
- Use certificates in business environments.
- Deploy and manage certificate templates.
- Manage certificates deployment, revocation and recovery.
- Implement and manage smart cards.
- Describe AD RMS.
- Explain how to deploy and manage an AD RMS infrastructure.
- Explain how to configure AD RMS content protection.
- Explain how to configure external access to AD RMS.
- Describe AD FS.
- Explain how to configure the AD FS prerequisites, and deploy AD FS services.
- Describe how to implement AD FS for a single organization.
- Deploy AD FS in a business-to-business federation scenario.
- Deploy the Web Application Proxy.
- Describe DAC.
- Implement DAC components.
- Implement DAC for access control.
- Implement access-denied assistance.
- Implement and manage Work Folders.
- Implement Workplace Join.
- Monitor AD DS.
- Manage the AD DS database.
- Recover objects from the AD DS database.
- Describe Windows Azure AD.
- Administer Azure AD.
- Describe AD LDS.
- Explain how to deploy AD LDS.
- Explain how to configure AD LDS instances and partitions.

- Describe AD DS replication.
- Configure AD DS sites.
- Configure and monitor AD DS replication.
- Describe Group Policy.
- Implement and administer GPOs.
- Describe Group Policy scope and Group Policy processing.
- Troubleshoot the application of GPOs.
- Implement Administrative Templates.
- Configure Folder Redirection and scripts.
- Configure Group Policy preferences.
- Deploy Certificate Authorities.
- Administer Certificate Authorities.
- Troubleshoot, maintain, and monitor Certificate Authorities.
- Use certificates in business environments.
- Deploy and manage certificate templates.
- Manage certificates deployment, revocation and recovery.
- Implement and manage smart cards.
- Describe AD RMS.
- Explain how to deploy and manage an AD RMS infrastructure.
- Explain how to configure AD RMS content protection.
- Explain how to configure external access to AD RMS.
- Describe AD FS.
- Explain how to configure the AD FS prerequisites, and deploy AD FS services.
- Describe how to implement AD FS for a single organization.
- Deploy AD FS in a business-to-business federation scenario.
- Deploy the Web Application Proxy.
- Describe DAC.
- Implement DAC components.
- Implement DAC for access control.
- Implement access-denied assistance.
- Implement and manage Work Folders.
- Implement Workplace Join.
- Monitor AD DS.
- Manage the AD DS database.
- Recover objects from the AD DS database.
- Describe Windows Azure AD.
- Administer Azure AD.
- Describe AD LDS.
- Explain how to deploy AD LDS.
- Explain how to configure AD LDS instances and partitions.

**Module 8: Deploying and Managing Certificates**This module describes certificate usage in business environments and explains how to deploy and manage certificates, configure certificate templates and manage enrolment process. This module also covers the deployment and management of smart cards.

- Using Certificates in a Business Environment

- controllers (RODCs).
- Explain and implement password and account lockout policies.
- Implement audit authentication.
- Describe AD DS replication.
- Configure AD DS sites.
- Configure and monitor AD DS replication.
- Describe Group Policy.
- Implement and administer GPOs.
- Describe Group Policy scope and Group Policy processing.
- Troubleshoot the application of GPOs.
- Implement Administrative Templates.
- Configure Folder Redirection and scripts.
- Configure Group Policy preferences.
- Deploy Certificate Authorities.
- Administer Certificate Authorities.
- Troubleshoot, maintain, and monitor Certificate Authorities.
- Use certificates in business environments.
- Deploy and manage certificate templates.
- Manage certificates deployment, revocation and recovery.
- Implement and manage smart cards.
- Describe AD RMS.
- Explain how to deploy and manage an AD RMS infrastructure.
- Explain how to configure AD RMS content protection.
- Explain how to configure external access to AD RMS.
- Describe AD FS.
- Explain how to configure the AD FS prerequisites, and deploy AD FS services.
- Describe how to implement AD FS for a single organization.
- Deploy AD FS in a business-to-business federation scenario.
- Deploy the Web Application Proxy.
- Describe DAC.
- Implement DAC components.
- Implement DAC for access control.
- Implement access-denied assistance.
- Implement and manage Work Folders.
- Implement Workplace Join.
- Monitor AD DS.
- Manage the AD DS database.
- Recover objects from the AD DS database.
- Describe Windows Azure AD.
- Administer Azure AD.
- Describe AD LDS.
- Explain how to deploy AD LDS.
- Explain how to configure AD LDS instances and partitions.

**Module 13: Implementing Windows Azure Active Directory**This module explains the concepts and technologies in Windows Azure Active Directory and how to implement and integrate it within your organization

- Overview of Windows Azure AD
- Managing Windows Azure AD Accounts

- Monitor AD DS.
- Manage the AD DS database.
- Recover objects from the AD DS database.
- Describe Windows Azure AD.
- Administer Azure AD.
- Describe AD LDS.
- Explain how to deploy AD LDS.
- Explain how to configure AD LDS instances and partitions.

Module 4: Implementing and Administering AD DS Sites and Replication This module explains how AD DS replicates information between domain controllers within a single site and throughout multiple sites. This module also explains how to create multiple sites and how to monitor replication to help optimize AD DS replication and authentication traffic. Lessons

- Overview of AD DS Replication
- Configuring AD DS Sites
- Configuring and Monitoring AD DS Replication

Lab : Implementing AD DS Sites and Replication

After completing this module, students will be able to:

- Describe and perform various deployment techniques for AD DS.
- Describe virtual domain controller deployment considerations.
- Explain how new technologies in Windows Server 2012 and Windows Server 2012 R2 support virtual domain controllers.
- Describe Domain Controller cloning.
- Implement AD DS using the tools provided in Windows Server 2012 and Windows Server 2012 R2.
- Understand the importance of securing domain controllers.
- Describe the benefit of read-only domain controllers (RODCs).
- Explain and implement password and account lockout policies.
- Implement audit authentication.
- Describe AD DS replication.
- Configure AD DS sites.
- Configure and monitor AD DS replication.
- Describe Group Policy.
- Implement and administer GPOs.
- Describe Group Policy scope and Group Policy processing.
- Troubleshoot the application of GPOs.
- Implement Administrative Templates.
- Configure Folder Redirection and scripts.
- Configure Group Policy preferences.
- Deploy Certificate Authorities.
- Administer Certificate Authorities.
- Troubleshoot, maintain, and monitor Certificate Authorities.
- Use certificates in business environments.

- Deploying and Managing Certificate Templates
- Managing Certificates Deployment, Revocation, and Recovery
- Implementing and Managing Smart Cards

Lab : Deploying and Using Certificates

After completing this module, students will be able to:

- Describe and perform various deployment techniques for AD DS.
- Describe virtual domain controller deployment considerations.
- Explain how new technologies in Windows Server 2012 and Windows Server 2012 R2 support virtual domain controllers.
- Describe Domain Controller cloning.
- Implement AD DS using the tools provided in Windows Server 2012 and Windows Server 2012 R2.
- Understand the importance of securing domain controllers.
- Describe the benefit of read-only domain controllers (RODCs).
- Explain and implement password and account lockout policies.
- Implement audit authentication.
- Describe AD DS replication.
- Configure AD DS sites.
- Configure and monitor AD DS replication.
- Describe Group Policy.
- Implement and administer GPOs.
- Describe Group Policy scope and Group Policy processing.
- Troubleshoot the application of GPOs.
- Implement Administrative Templates.
- Configure Folder Redirection and scripts.
- Configure Group Policy preferences.
- Deploy Certificate Authorities.
- Administer Certificate Authorities.
- Troubleshoot, maintain, and monitor Certificate Authorities.
- Use certificates in business environments.
- Deploy and manage certificate templates.
- Manage certificates deployment, revocation and recovery.
- Implement and manage smart cards.
- Describe AD RMS.
- Explain how to deploy and manage an AD RMS infrastructure.
- Explain how to configure AD RMS content protection.
- Explain how to configure external access to AD RMS.
- Describe AD FS.
- Explain how to configure the AD FS prerequisites, and deploy AD FS services.
- Describe how to implement AD FS for a

Lab : Implementing Windows Azure AD

After completing this module, students will be able to:

- Describe and perform various deployment techniques for AD DS.
- Describe virtual domain controller deployment considerations.
- Explain how new technologies in Windows Server 2012 and Windows Server 2012 R2 support virtual domain controllers.
- Describe Domain Controller cloning.
- Implement AD DS using the tools provided in Windows Server 2012 and Windows Server 2012 R2.
- Understand the importance of securing domain controllers.
- Describe the benefit of read-only domain controllers (RODCs).
- Explain and implement password and account lockout policies.
- Implement audit authentication.
- Describe AD DS replication.
- Configure AD DS sites.
- Configure and monitor AD DS replication.
- Describe Group Policy.
- Implement and administer GPOs.
- Describe Group Policy scope and Group Policy processing.
- Troubleshoot the application of GPOs.
- Implement Administrative Templates.
- Configure Folder Redirection and scripts.
- Configure Group Policy preferences.
- Deploy Certificate Authorities.
- Administer Certificate Authorities.
- Troubleshoot, maintain, and monitor Certificate Authorities.
- Use certificates in business environments.
- Deploy and manage certificate templates.
- Manage certificates deployment, revocation and recovery.
- Implement and manage smart cards.
- Describe AD RMS.
- Explain how to deploy and manage an AD RMS infrastructure.
- Explain how to configure AD RMS content protection.
- Explain how to configure external access to AD RMS.
- Describe AD FS.
- Explain how to configure the AD FS prerequisites, and deploy AD FS services.
- Describe how to implement AD FS for a single organization.
- Deploy AD FS in a business-to-business federation scenario.
- Deploy the Web Application Proxy.
- Describe DAC.
- Implement DAC components.
- Implement DAC for access control.
- Implement access-denied assistance.
- Implement and manage Work Folders.
- Implement Workplace Join.

- Deploy and manage certificate templates.
- Manage certificates deployment, revocation and recovery.
- Implement and manage smart cards.
- Describe AD RMS.
- Explain how to deploy and manage an AD RMS infrastructure.
- Explain how to configure AD RMS content protection.
- Explain how to configure external access to AD RMS.
- Describe AD FS.
- Explain how to configure the AD FS prerequisites, and deploy AD FS services.
- Describe how to implement AD FS for a single organization.
- Deploy AD FS in a business-to-business federation scenario.
- Deploy the Web Application Proxy.
- Describe DAC.
- Implement DAC components.
- Implement DAC for access control.
- Implement access-denied assistance.
- Implement and manage Work Folders.
- Implement Workplace Join.
- Monitor AD DS.
- Manage the AD DS database.
- Recover objects from the AD DS database.
- Describe Windows Azure AD.
- Administer Azure AD.
- Describe AD LDS.
- Explain how to deploy AD LDS.
- Explain how to configure AD LDS instances and partitions.

Module 5: Implementing Group Policy This module describes Group Policy, how it works, and how best to implement it within your organization. Lessons

- Introducing Group Policy
- Implementing and Administering GPOs
- Group Policy Scope and Group Policy Processing
- Troubleshooting the Application of GPOs

Lab : Implementing and Troubleshooting a Group Policy Infrastructure

After completing this module, students will be able to:

- Describe and perform various deployment techniques for AD DS.
- Describe virtual domain controller deployment considerations.
- Explain how new technologies in Windows Server 2012 and Windows Server 2012 R2 support virtual domain controllers.
- Describe Domain Controller cloning.
- Implement AD DS using the tools provided in Windows Server 2012 and Windows Server 2012 R2.
- Understand the importance of securing

- single organization.
- Deploy AD FS in a business-to-business federation scenario.
- Deploy the Web Application Proxy.
- Describe DAC.
- Implement DAC components.
- Implement DAC for access control.
- Implement access-denied assistance.
- Implement and manage Work Folders.
- Implement Workplace Join.
- Monitor AD DS.
- Manage the AD DS database.
- Recover objects from the AD DS database.
- Describe Windows Azure AD.
- Administer Azure AD.
- Describe AD LDS.
- Explain how to deploy AD LDS.
- Explain how to configure AD LDS instances and partitions.

Module 9: Implementing and Administering AD RMS This module introduces Active Directory Rights Management Services (AD RMS). It also describes how to deploy AD RMS, how to configure content protection, and how to make AD RMS-protected documents available to external users. Lessons

- Overview of AD RMS
- Deploying and Managing an AD RMS Infrastructure
- Configuring AD RMS Content Protection
- Configuring External Access to AD RMS

Lab : Implementing an AD RMS Infrastructure

After completing this module, students will be able to:

- Describe and perform various deployment techniques for AD DS.
- Describe virtual domain controller deployment considerations.
- Explain how new technologies in Windows Server 2012 and Windows Server 2012 R2 support virtual domain controllers.
- Describe Domain Controller cloning.
- Implement AD DS using the tools provided in Windows Server 2012 and Windows Server 2012 R2.
- Understand the importance of securing domain controllers.
- Describe the benefit of read-only domain controllers (RODCs).
- Explain and implement password and account lockout policies.
- Implement audit authentication.
- Describe AD DS replication.
- Configure AD DS sites.
- Configure and monitor AD DS replication.
- Describe Group Policy.

- Monitor AD DS.
- Manage the AD DS database.
- Recover objects from the AD DS database.
- Describe Windows Azure AD.
- Administer Azure AD.
- Describe AD LDS.
- Explain how to deploy AD LDS.
- Explain how to configure AD LDS instances and partitions.

Module 14: Implementing and Administering AD LDS This module explains how to deploy and configure Active Directory Lightweight Directory Services (AD LDS) Lessons

- Overview of AD LDS
- Deploying AD LDS
- Configuring AD LDS Instances and Partitions
- Configuring AD LDS Replication
- Integrating AD LDS with AD DS

Lab : Implementing and Administering AD LDS

After completing this module, students will be able to:

- Describe and perform various deployment techniques for AD DS.
- Describe virtual domain controller deployment considerations.
- Explain how new technologies in Windows Server 2012 and Windows Server 2012 R2 support virtual domain controllers.
- Describe Domain Controller cloning.
- Implement AD DS using the tools provided in Windows Server 2012 and Windows Server 2012 R2.
- Understand the importance of securing domain controllers.
- Describe the benefit of read-only domain controllers (RODCs).
- Explain and implement password and account lockout policies.
- Implement audit authentication.
- Describe AD DS replication.
- Configure AD DS sites.
- Configure and monitor AD DS replication.
- Describe Group Policy.
- Implement and administer GPOs.
- Describe Group Policy scope and Group Policy processing.
- Troubleshoot the application of GPOs.
- Implement Administrative Templates.
- Configure Folder Redirection and scripts.
- Configure Group Policy preferences.
- Deploy Certificate Authorities.
- Administer Certificate Authorities.
- Troubleshoot, maintain, and monitor Certificate Authorities.
- Use certificates in business environments.
- Deploy and manage certificate templates.

- domain controllers.
- Describe the benefit of read-only domain controllers (RODCs).
- Explain and implement password and account lockout policies.
- Implement audit authentication.
- Describe AD DS replication.
- Configure AD DS sites.
- Configure and monitor AD DS replication.
- Describe Group Policy.
- Implement and administer GPOs.
- Describe Group Policy scope and Group Policy processing.
- Troubleshoot the application of GPOs.
- Implement Administrative Templates.
- Configure Folder Redirection and scripts.
- Configure Group Policy preferences.
- Deploy Certificate Authorities.
- Administer Certificate Authorities.
- Troubleshoot, maintain, and monitor Certificate Authorities.
- Use certificates in business environments.
- Deploy and manage certificate templates.
- Manage certificates deployment, revocation and recovery.
- Implement and manage smart cards.
- Describe AD RMS.
- Explain how to deploy and manage an AD RMS infrastructure.
- Explain how to configure AD RMS content protection.
- Explain how to configure external access to AD RMS.
- Describe AD FS.
- Explain how to configure the AD FS prerequisites, and deploy AD FS services.
- Describe how to implement AD FS for a single organization.
- Deploy AD FS in a business-to-business federation scenario.
- Deploy the Web Application Proxy.
- Describe DAC.
- Implement DAC components.
- Implement DAC for access control.
- Implement access-denied assistance.
- Implement and manage Work Folders.
- Implement Workplace Join.
- Monitor AD DS.
- Manage the AD DS database.
- Recover objects from the AD DS database.
- Describe Windows Azure AD.
- Administer Azure AD.
- Describe AD LDS.
- Explain how to deploy AD LDS.
- Explain how to configure AD LDS instances and partitions.

- Implement and administer GPOs.
- Describe Group Policy scope and Group Policy processing.
- Troubleshoot the application of GPOs.
- Implement Administrative Templates.
- Configure Folder Redirection and scripts.
- Configure Group Policy preferences.
- Deploy Certificate Authorities.
- Administer Certificate Authorities.
- Troubleshoot, maintain, and monitor Certificate Authorities.
- Use certificates in business environments.
- Deploy and manage certificate templates.
- Manage certificates deployment, revocation and recovery.
- Implement and manage smart cards.
- Describe AD RMS.
- Explain how to deploy and manage an AD RMS infrastructure.
- Explain how to configure AD RMS content protection.
- Explain how to configure external access to AD RMS.
- Describe AD FS.
- Explain how to configure the AD FS prerequisites, and deploy AD FS services.
- Describe how to implement AD FS for a single organization.
- Deploy AD FS in a business-to-business federation scenario.
- Deploy the Web Application Proxy.
- Describe DAC.
- Implement DAC components.
- Implement DAC for access control.
- Implement access-denied assistance.
- Implement and manage Work Folders.
- Implement Workplace Join.
- Monitor AD DS.
- Manage the AD DS database.
- Recover objects from the AD DS database.
- Describe Windows Azure AD.
- Administer Azure AD.
- Describe AD LDS.
- Explain how to deploy AD LDS.
- Explain how to configure AD LDS instances and partitions.

Module 10: Implementing and Administering AD FS This module explains AD FS, and then provides details on how to configure AD FS in both a single organization scenario and in a partner organization scenario. This module also describes the Web Application Proxy feature in Windows Server 2012 R2 that functions as an AD FS proxy and reverse proxy for web-based applications. Lessons

- Overview of AD FS
- Deploying AD FS
- Implementing AD FS for a Single Organization
- Deploying AD FS in a

- Manage certificates deployment, revocation and recovery.
- Implement and manage smart cards.
- Describe AD RMS.
- Explain how to deploy and manage an AD RMS infrastructure.
- Explain how to configure AD RMS content protection.
- Explain how to configure external access to AD RMS.
- Describe AD FS.
- Explain how to configure the AD FS prerequisites, and deploy AD FS services.
- Describe how to implement AD FS for a single organization.
- Deploy AD FS in a business-to-business federation scenario.
- Deploy the Web Application Proxy.
- Describe DAC.
- Implement DAC components.
- Implement DAC for access control.
- Implement access-denied assistance.
- Implement and manage Work Folders.
- Implement Workplace Join.
- Monitor AD DS.
- Manage the AD DS database.
- Recover objects from the AD DS database.
- Describe Windows Azure AD.
- Administer Azure AD.
- Describe AD LDS.
- Explain how to deploy AD LDS.
- Explain how to configure AD LDS instances and partitions.

Explain how to configure AD LDS replication.



Business-to-Business Federation  
Scenario

■ Extending AD FS to External Clients

Lab : Implementing AD FS

After completing this module, students will be able to:

- Describe and perform various deployment techniques for AD DS.
- Describe virtual domain controller deployment considerations.
- Explain how new technologies in Windows Server 2012 and Windows Server 2012 R2 support virtual domain controllers.
- Describe Domain Controller cloning.
- Implement AD DS using the tools provided in Windows Server 2012 and Windows Server 2012 R2.
- Understand the importance of securing domain controllers.
- Describe the benefit of read-only domain controllers (RODCs).
- Explain and implement password and account lockout policies.
- Implement audit authentication.
- Describe AD DS replication.
- Configure AD DS sites.
- Configure and monitor AD DS replication.
- Describe Group Policy.
- Implement and administer GPOs.
- Describe Group Policy scope and Group Policy processing.
- Troubleshoot the application of GPOs.
- Implement Administrative Templates.
- Configure Folder Redirection and scripts.
- Configure Group Policy preferences.
- Deploy Certificate Authorities.
- Administer Certificate Authorities.
- Troubleshoot, maintain, and monitor Certificate Authorities.
- Use certificates in business environments.
- Deploy and manage certificate templates.
- Manage certificates deployment, revocation and recovery.
- Implement and manage smart cards.
- Describe AD RMS.
- Explain how to deploy and manage an AD RMS infrastructure.
- Explain how to configure AD RMS content protection.
- Explain how to configure external access to AD RMS.
- Describe AD FS.
- Explain how to configure the AD FS prerequisites, and deploy AD FS services.
- Describe how to implement AD FS for a single organization.
- Deploy AD FS in a business-to-business federation scenario.

- Deploy the Web Application Proxy.
- Describe DAC.
- Implement DAC components.
- Implement DAC for access control.
- Implement access-denied assistance.
- Implement and manage Work Folders.
- Implement Workplace Join.
- Monitor AD DS.
- Manage the AD DS database.
- Recover objects from the AD DS database.
- Describe Windows Azure AD.
- Administer Azure AD.
- Describe AD LDS.
- Explain how to deploy AD LDS.
- Explain how to configure AD LDS instances and partitions.

---

### Additional Information:

To help you prepare for this exam, Microsoft recommends that you have hands-on experience with the product and that you use the specified training resources.

These training resources do not necessarily cover all topics listed in the "Skills measured" section.

Looking for training resources, events and advice from peers? Join the [Microsoft Training and Certification Community](#) .

Preparing for an exam now? Find your [Microsoft Certification Study Group](#) .

Talk to us on these social networks: [Facebook](#) [Twitter](#) [LinkedIn](#)

---

### Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

[info@globalknowledge.co.uk](mailto:info@globalknowledge.co.uk)

[www.globalknowledge.com/en-gb/](http://www.globalknowledge.com/en-gb/)

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK