



Administering Windows Server 2012 36 Contact Hours

Course Overview

This version of this course 20411A utilizes pre-release software in the virtual machines for the labs. The course is part two of a series of three courses, which provide the skills and knowledge necessary to implement a core Windows Server 2012 infrastructure in an existing enterprise environment. The three courses in total will collectively cover implementing, managing, maintaining and provisioning services and infrastructure in a Windows Server 2012 environment. While there is some cross-over in skillset and tasks across the courses, this course will primarily cover the administration tasks necessary to maintain a Windows Server 2012 infrastructure, such as user and group management, network access and data security.

Audience

This course is intended for Information Technology (IT) Professionals with hands on experience working in a Windows Server 2008 or Windows Server 2012 environment, who wish to acquire the skills and knowledge necessary to be able to manage and maintain the core infrastructure required for a Windows Server 2012 environment. The key focus for students in this course is to broaden the initial deployment of Windows Server 2012 services and infrastructure and provide the skills necessary to manage and maintain a domain based Windows Server 2012 environment, such as user and group management, network access and data security.

Candidates would typically be System Administrators or aspiring to be System Administrators. They must have at least one year hands on experience working in a Windows Server 2008 or Windows Server 2012 environment. Candidates must also have knowledge equivalent to that already covered in “20410A: Installing and Configuring Windows Server 2012” course as this course will build upon that knowledge.

At Course Completion

After completing this course, students will be able to:

- Implement a Group Policy infrastructure.
- Manage user desktops with Group Policy.
- Manage user and service accounts .
- Maintain Active Directory Domain Services (AD DS) .
- Configure and troubleshoot Domain Name System (DNS) .
- Configure and troubleshoot Remote Access .
- Install, configure, and troubleshoot the Network Policy Server (NPS) role .
- Implement Network Access Protection (NAP) .
- Optimize file services .
- Configure encryption and advanced auditing .
- Deploy and maintain server images.



Implement Update Management.
Monitor Windows Server 2012.

Prerequisites

A good understanding of networking fundamentals.
An understanding and experience configuring security and administration tasks in an enterprise environment.
Experience supporting or configuring Microsoft Windows clients.

Course Outline

Module 1: Implementing a Group Policy Infrastructure

This module covers how to implement a Group Policy infrastructure and then how to configure and manage that infrastructure. It also covers how to scope Group Policy objects (GPOs) using links, security groups, WMI filters, loopback processing, and preference targeting as well as covering troubleshooting policy application.

Lessons

- Understanding Group Policy
- Implementing GPOs
- Managing Group Policy Scope
- Group Policy Processing
- Troubleshooting Policy Application
- Lab : Implementing a Group Policy Infrastructure
- Creating and Configuring Group Policy Objects
- Managing Group Policy Scope
- Verifying Group Policy Application
- Managing Group Policy Objects

After completing this module, students will be able to:

- Implement a Group Policy infrastructure .
- Implement GPOs .
- Manage Group Policy scope .
- Outline and describe Group Policy processing .
- Troubleshoot policy application.

Module 2: Managing User Desktops with Group Policy

This module covers implementing administrative templates, how to configure GPO preferences and folder redirection as well as managing software with Group Policy.

Lessons

- Implementing Administrative Templates
- Configuring Group Policy Preferences
- Managing Software with GPSI
- Lab : Managing User Desktops with Group Policy



Deploying Software Using Group Policy
Implementing Settings Using Group Policy Preferences
Configuring Folder Redirection
After completing this module, students will be able to:
Implement administrative templates.
Configure Group Policy preferences.
Manage software with Group Policy.

Module 3: Managing User and Service Accounts

This module covers how to create and administer user accounts as well as configure user object attributes. It also covers automating user account creation and configuring Managed Service Accounts.

Lessons

Creating and Administering User Accounts
Configuring User Object Attributes
Automating User Account Creation
Configuring Managed Service Accounts
Lab : Managing User and Service Accounts
Configuring Password Policy and Account Lockout Settings
Creating and Associating a Managed Service Account
After completing this module, students will be able to:
Create and administer user accounts.
Configure user object attributes.
Automate user account creation.
Configure managed service accounts.

Module 4: Maintaining Active Directory Domain Services

This module covers how to implement Virtualized and Read Only Domain Controllers as well as how to perform common AD DS administrative tasks. The module will also cover how to manage the AD DS database.

Lessons

Implementing Virtualized Domain Controllers
Implementing Read Only Domain Controllers
Administering AD DS
Managing the AD DS Database
Lab : Maintaining Active Directory Domain Services
Deploying a Virtualized Domain Controller Clone
Installing and Configuring a Read Only Domain Controller
Configuring and Viewing Active Directory Snapshots
Configuring the Active Directory Recycle Bin
After completing this module, students will be able to:
Implement Virtualized domain controllers.
Implement Read Only domain controllers.



Administer AD DS.
Manage the AD DS database.

Module 5: Configuring and Troubleshooting DNS

This module covers installing and configuring the DNS server role as well as creating and configuring DNS zones and zone transfers. It will also cover managing and troubleshooting DNS.

Lessons

- Installing the DNS Server Role
- Configuring the DNS Server Role
- Configuring DNS Zones
- Configuring DNS Zone Transfers
- Managing and Troubleshooting DNS
- Lab : Configuring and Troubleshooting DNS
- Configuring DNS Resource Records
- Configuring DNS Conditional Forwarding
- Installing and Configuring DNS Zones
- Troubleshooting DNS

After completing this module, students will be able to:

- Install the DNS server role.
- Configure the DNS server role.
- Configure DNS zones.
- Configure DNS zone transfers.
- Manage and troubleshoot DNS.

Module 6: Configuring and Troubleshooting Remote Access

This module covers configuring network access, creating and configuring virtual private networks (VPNs) and Network Policies as well as troubleshooting routing and remote access. It will also cover configuration of DirectAccess.

Lessons

- Configuring Network Access
- Configuring VPN Access
- Overview of Network Policies
- Troubleshooting Routing and Remote Access
- Configuring DirectAccess
- Lab : Configuring and Troubleshooting Remote Access
- Configuring a VPN Server
- Configuring a Network Policy for VPN Clients
- Configuring Direct Access

After completing this module, students will be able to:

- Configure network access.
- Configure VPN access.
- Explain the purpose of network policies.



Troubleshoot routing and remote access.
Configure DirectAccess.

Module 7: Installing, Configuring, and Troubleshooting the Network Policy Server Role

This module covers installing and configuring NPS as well as remote authentication dial in user service (RADIUS) clients and servers. It will also deal with NPS authentication methods and monitoring and troubleshooting a NPS.

Lessons

- Installing and Configuring a Network Policy Server
- Configuring RADIUS Clients and Servers
- NPS Authentication Methods
- Monitoring and Troubleshooting a Network Policy Server
- Lab : Installing and Configuring a Network Policy Server
- Installing and Configuring NPS to Support RADIUS
- Configuring a RADIUS Client

After completing this module, students will be able to:

- Install and configure a NPS.
- Configure RADIUS clients and servers.
- Describe NPS authentication methods.
- Monitor and troubleshoot a NPS.

Module 8: Implementing Network Access Protection

This module will provide an overview of NAP, detailing the functionality and infrastructure requirements. It will also cover configuration, monitoring and troubleshooting NAP.

Lessons

- Overview of Network Access Protection
- How NAP Works
- Configuring NAP
- Monitoring and Troubleshooting NAP
- Lab : Implementing Network Access Protection
- Configuring NAP Components
- Configuring the Client Settings to Support NAP

After completing this module, students will be able to:

- Understand the functionality and requirements of NAP.
- Configure and Implement NAP.
- Monitor and troubleshoot NAP.

Module 9: Optimizing File Services

This module covers File Server Resource Manager (FSRM) and how to use it to implement Quotas, file screens and Storage Reports. It will also outline how to implement Classification Management and File Management Tasks as well as covering how to implement DFS, DFS Namespaces and configuring and troubleshooting DFS Replication.



Lessons

Overview of FSRM

Using FSRM to Manage Quotas, File Screens, and Storage Reports
Implementing Classification Management and File Management Tasks

DFS Overview

Configuring DFS Namespaces

Configuring and Troubleshooting DFS Replication

Lab : Lab A: Configuring Quotas and File Screening Using FSRM

Configuring FSRM Quotas

Configuring File Screening

Lab : Lab B: Configuring DFS Namespaces and Replication

Installing and Configuring the DFS Namespaces Server Role

Configuring DFS Folder Targets

Configuring DFS Replication

After completing this module, students will be able to:

Manage quotas, file screens, and storage reports by using FSRM.

Implement classification management and file management tasks.

Configure DFS namespaces.

Configure and troubleshoot DFS Replication.

Module 10: Configuring Encryption and Advanced Auditing

This module covers how to increase file system security by configuring file encryption with Encrypting File System (EFS) as well as how to enable and implement advanced auditing features.

Lessons

Encrypting Network Files with EFS

Configuring Advanced Auditing

Lab : Lab A: Encrypting and Recovering Files

Encrypting and Recovering Files

Lab : Lab B: Implementing Advanced Audit Policy Configuration

Configuring Advanced Audit Policy Configuration

After completing this module, students will be able to:

Encrypt network files with EFS.

Enable and implement advanced audit policies.

Module 11: Deploying and Maintaining Server Images

This module covers the features and functionality of Windows Deployment Services (WDS) as well as providing considerations for its use. It will also cover how to Perform deployments with WDS.

Lessons

Overview of WDS

Implementing Deployment with WDS

Administering WDS

Lab : Deploying and Maintaining Server Images Using Windows Deployment Services



Installing and Configuring Windows Deployment Services

Deploying a Server Image

After completing this module, students will be able to:

Understand the features and functionality of Windows Deployment Services (WDS).

Determine the appropriateness of its use in particular situations.

Perform deployments with WDS.

Module 12: Implementing Update Management

This module covers the features and functionality of Windows Server Update Services (WSUS) as well as detailing how to provision updates with WSUS.

Lessons

Overview of WSUS

Deploying Updates with WSUS

Lab : Implementing Update Management

Implementing the WSUS Server Role

Configuring Update Settings

Approving and Deploying an Update using WSUS

After completing this module, students will be able to:

Understand the features and functionality of WSUS .

Deploy Updates with WSUS.

Module 13: Monitoring Windows Server 2012

This module covers the various monitoring tools available in Windows Server 2012. It will cover the use of Performance Monitor as well as how to monitor and successfully utilize Event logs.

Lessons

Monitoring Tools

Using Performance Monitor

Monitoring Event Logs

Lab : Monitoring Windows Server 2012

Establishing a Performance Baseline

Identifying the Source of a Performance Problem

Viewing and Configuring Centralized Event Logs

After completing this module, students will be able to:

Describe and understand the various monitoring tools available in Windows Server 2012.

Use Performance Monitor.

Monitor and successfully utilize Event logs.