directions

Fundamentals of a Windows Server Infrastructure

OD10967A; On-Demand, Video-based

Course Description

This course covers the basic skills and knowledge that are required in order to build a Windows Server Infrastructure. It covers networking architecture and topologies, security considerations and best practices as well as basic Windows Server administration skills and technologies such as Windows Server 2012 Installation, configuration, maintenance and performance. Within that it will also cover specific areas such as Active Directory Domain Services (AD DS), Domain Name Services (DNS), Storage and many others.

This course is designed to provide foundational level knowledge needed to prepare students to start a career or cross train in Microsoft Windows Server technologies.

Audience Profile

Candidates for this course are people who are starting out their career or looking to change careers into Windows Server Technologies and need the fundamental knowledge to help them achieve that. It would be of interest to home computer users, small business owners, academic students, information workers, developers, technical managers, help desk technicians or students who are looking to cross train from an alternative technology.

This course is needed as a first step in preparing for a job in IT or as prerequisite training before beginning the Microsoft Certified System Administrator (MCSA) training and certification path.

At Course Completion

After completing this course, students will be able to:

- Perform a local media-based installation of Windows Server 2012
- Select appropriate storage technologies and configure storage on Windows Server
- Describe fundamental network components and terminology thus enabling you to select an appropriate network component in a particular scenario
- Implement a network by selecting network hardware components and technologies and determine the appropriate network hardware and wiring components for a given situation

- Describe the protocols and services within the Transmission Control Protocol/Internet Protocol (TCP/IP) suite of protocols and implement IPv4 within a Windows Server environment
- Describe server roles
- Implement and configure an Active Directory Domain Service (AD DS) forest
- Describe the concept of defense-in-depth and determine how to implement this approach with Windows Server
- Identify the security features in Windows Server that help to provide defense-in-depth
- Identify the network-related security features in Windows Server to mitigate security threats to you network
- Identify and implement additional software components to enhance your organization's security
- Monitor a server to determine the performance level
- Identify the Windows Server tools available to maintain and troubleshoot Windows Server

Prerequisites

In addition to their professional experience, before attending this course, students must have:

- A good fundamental knowledge of general computing concepts
- Knowledge equivalent to the MTA exam *98-349: Windows Operating System Fundamentals*

Course Outline

Module 1: Installing and Configuring Windows Server 2012

This module explains how the Windows Server 2012 editions, installation options, optimal service and device configuration and general post-installation configuration all contribute to the functionality and effectiveness of your Windows Server implementation.

Lessons

- Installing Windows Server
- Configuring Services
- Configuring Peripherals and Devices

Lab: Installing Windows Server

- Performing a Local Media-Based Installation
- Configuring Windows Server
- Converting Server Core
- Configuring Services
- Configuring Devices

After completing this module, student will be able to:

- Install Windows Server 2012

- Manage services
- Manage devices and device drivers

Module 2: Implementing Storage in Windows Server

This module will introduce you to different storage technologies, discuss how to implement the storage solutions in Windows Server and will finish a discussion on a resilient strategy for your storage that will be tolerant in various ways, helping to avoid unplanned downtime and loss of data.

Lessons

- Identifying Storage Technologies
- Managing Disks and Volumes
- Fault Tolerance

Lab: Implementing Storage in Windows Server

- Creating and Mounting a VHD File
- Creating a New Volume
- Creating a Storage Pool Using VHDs
- Implementing the Windows iSCSI Initiator

After completing this module, students will be able to:

- Identify a suitable storage technology
- Manage storage within Windows Server
- Implement disk fault tolerance

Module 3: Understanding Network Infrastructure

In this module, students will learn how to describe fundamental network component and terminology thus enabling the student to select an appropriate network component in a particular scenario.

Lessons

- Network Architecture Standards
- Local Area Networking
- Wide Area Networking
- Wireless Networking
- Connecting to the Internet
- Remote Access

Lab: Selecting Network Infrastructure Components

- Determining Appropriate Network Components

After completing this module, students will be able to:

- Describe physical network topologies and standards
- Define LANs
- Define WANs
- Describe wireless networking technologies
- Explain how to connect a network to the Internet
- Describe how technologies connect remote access

Module 4: Connecting Network Components

This module explores the functionality of low-level networking components, including switches and routers. In addition, the module provides guidance on how best to connect these and other components together to provide additional network functionality.

Lessons

- Understanding the OSI Model
- Understanding Media Types
- Understanding Adapters, Hubs, and Switches
- Understanding Routing

Lab: Connecting Network Components

- Determining the Appropriate Network Hardware
- Selecting a Suitable Wiring Infrastructure

After completing this module, students will be able to:

- Describe the industry standard protocol model
- Describe adapters, hubs, and switches
- Describe routing technologies and protocols
- Describe wiring methodologies and standards

Module 5: Implementing TCP/IP

This module describes the requirements of a protocol stack and then focuses on the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol stack.

Lessons

- Overview of TCP/IP
- Understanding IPv4 Addressing
- Configuring IPv4
- Understanding IPv6
- Name Resolution

Lab: Implementing TCP/IP

- Determining an Appropriate IPv4 Addressing Scheme
- Configuring IPv4 with Windows Server
- Verifying the Configuration
- Configuring and testing name resolution
- Viewing the IPv6 Configuration

After completing this module, students will be able to:

- Describe the Functionality of the TCP/IP Suite
- Describe IPv4 Addressing
- Configure an IPv4 Network
- Describe IPv6 Addressing and Transition
- Describe the Various Name Resolution Methods Used by TCP/IP Hosts

Module 6: Implementing Windows Server Roles

This module explains the functional requirements of a server computer and how to select and deploy appropriate server roles to support these functional requirements.

Lessons

- Role Based Deployment
- Deploying Role-Specific Services
- Virtualizing Windows Server Roles
- Best Practices for management of Windows Server Roles

Lab: Implementing Server Roles

- Determining the Appropriate Roles to Deploy

Lab: Implementing Virtualization

- Creating Virtual Hard Disks
- Creating New Virtual Machines
- Modifying Virtual Machine Settings
- Deploying the Determined Server Roles Remotely on multiple Servers

After completing this module, students will be able to:

- Select and install server roles and features to support different types of servers
- Describe different types of servers

Module 7: Implementing Active Directory Domain Services

This module explains that, as a directory service, how AD DS stores information about objects on a network and makes this information available to users and network administrators.

Lessons

- Introducing AD DS
- Implementing AD DS
- Managing Users, Groups, and Computers
- Implementing Organizational Units
- Implementing Group Policy

Lab: Implementing AD DS

- Promoting a New Domain Controller
- Creating an Organizational Unit
- Configuring Accounts
- Creating a GPO

After completing this module, students will be able to:

- Describe the fundamental features of AD DS
- Implement AD DS
- Manage objects in a domain
- Implement organizational units (OUs) for managing groups and objects
- Configure client computers centrally with group policy objects (GPOs)

Module 8: Implementing IT Security Layers

This module explains how, in addition to file and share permissions, you can also use data encryption to restrict data access.

Lessons

- Overview of Defense-in-Depth
- Physical Security
- Internet Security

Lab: Implementing IT Security Layers

- Implementing Physical Security
- Configuring Security Settings in Internet Explorer

After completing this module, students will be able to:

- Identify security threats at all levels and mitigate those threats
- Describe physical security risks and identify mitigations
- Identify Internet-based security threats and protect against them

Module 9: Implementing Windows Server Security

This module reviews the tools and concepts available for implementing security within a Microsoft Windows infrastructure.

Lessons

- Overview of Windows Security
- Securing Files and Folders
- Implementing Encryption

Lab: Implementing Windows Security

- Configuring an Accounts Policy
- Securing NTFS Files and Folders
- Encrypting Files

After completing this module, students will be able to:

- Describe the features in Windows Server 2012 that help improve your network's security
- Explain how to secure files and folders
- Explain how to use the encryption features provided by Windows Server 2012 to secure access to resources

Module 10: Implementing Network Security

This module explains possible threats when you connect your computers to a network, how to identify them, and how implement appropriate Windows network security features to help to eliminate them.

Lessons

- Overview of Network Security
- Implementing Firewalls

Lab: Implementing Network Security

- Configuring Windows Firewall with Advanced Security

After completing this module, students will be able to:

- Identify network-based security threats
- Implement Windows Firewall to secure Windows hosts
- Explain how to enforce corporate compliance

Module 11: Implementing Security Software

This module explains how an information technology (IT) administrator can account for and mitigate the risks of malicious code, unauthorized use, and data theft.

Lessons

- Client Protection Features
- E-Mail Protection
- Server Protection

Lab: Implementing Security Software

- Restricting Applications with AppLocker
- Using the Security Configuration Wizard
- Configure, Run and View Results from Best Practice Analyzer (BPA)

After completing this module, students will be able to:

- Implement Windows Server technologies and features to improve client security
- Describe security threats posed by e-mail and how to mitigate these threats
- Explain how to improve server security using Windows Server security analysis and hardening tools

Module 12: Monitoring Server Performance

This module discusses the importance of monitoring the performance of servers, and how you monitor servers to ensure that they run efficiently and use available server capacity. It also explains performance monitoring tools to identify components that require additional tuning and troubleshooting, so that you can improve the efficiency of your servers.

Lessons

- Windows Logs
- Performance Monitoring

Lab: Monitoring Server Performance

- Creating a Performance Baseline

- Simulating a Server Load
- Gathering Additional Performance Data
- Determining Probable Performance Bottlenecks

After completing this module, students will be able to:

- Identify server components that are impacted through excessive workloads
- Measure system resource usage and identify component bottlenecks

Module 13: Maintaining Windows Server

This module explains the importance of system updates, how to troubleshoot the Windows Server boot process, and how to implement high availability and recovery technologies to improve system availability.

Lessons

- Troubleshooting Windows Server Startup
- Server Availability and Data Recovery
- Applying Updates to Windows Server
- Troubleshooting Windows Server

Lab: Maintaining Windows Server

- Troubleshooting the Startup Process
- Configuring WSUS
- Gathering Information to Start the Troubleshooting Process

After completing this module, students will be able to:

- Troubleshoot the Windows Server boot process
- Implement high availability and recovery technologies to improve system availability
- Explain the importance of system updates
- Implement an appropriate troubleshooting methodology to resolve problems with Windows Server