Course 10967A:

Fundamentals of a Windows Server Infrastructure

Course Details

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

- Windows Server Architecture.
- Installing Windows Server.
- Configuring Services.
- Configuring Devices and Device Drivers.

Lab : Installing and Configuring Windows Server 2012

- 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:

- Describe Windows Server components and architecture.
- Install Windows Server 2012.
- Configure services.
- Configure devices and device drivers.

Module 2: Implementing Storage in Windows Server

This module will introduce you to different storage technologies and discuss how to implement the storage solutions in Windows Server. There is also a discussion on how to create a resilient strategy for your storage, 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

- Create and Mount a VHD File.
- Creating and Making Available New Volumes.
- Vary the Sizes of NTFS and ReFS Volumes.
- Create a Fault Tolerant Disk Configuration.

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 local area networks (LANs).
- Define wide area networks (WANs).

- Describe wireless networking technologies.
- Explain how to connect a network to the Internet.
- Describe how technologies are used for 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 wiring methodologies and standards.
- Describe adapters, hubs, and switches.
- Describe routing technologies and protocols.

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.
- IPv4 Addressing.
- IPv6 Addressing.
- 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.
- Considerations for Provisioning Roles.

Lab : Implementing Server Roles

- Determining the Appropriate Roles to Deploy.

Lab : Implementing Server Roles

- Determining the Appropriate Roles to Deploy.
- Deploying and Configuring the Determined Server Roles.

After completing this module, students will be able to:

- Describe role-based deployment.
- Deploy role-specific servers.
- Describe deployment options for server roles.

Module 7: Implementing Active Directory

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 Active Directory Domain Services (AD DS).
- Implementing AD DS.
- Managing Users, Groups, and Computers.
- 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.
- 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:

- Describe the risks posed by connecting to the Internet.
- Describe possible mitigations to these risks.
- Describe the Windows Server components and features that can help provide his Internet security.

Module 9: Implementing Security in Windows Server

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 a Fine-Grained Password Policy
- Securing NTFS Files and Folders.
- Encrypting Files and Folders.

After completing this module, students will be able to:

- Describe the Windows Server features that help improve your network's security.
- Explain how to secure files and folders in the Windows Server environment.
- Explain how to use the Windows Server encryption features to help 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.
- Internet Protocol Security (IPsec)

Lab : Implementing Network Security

- Configuring Windows Firewall with Advanced Security.
- Create a Server to Server Connection Security Rule.

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 Software Protection Features.
- E-Mail Protection.
- Server Protection.

Lab : Implementing Security Software

- Create and Enforce an AppLocker Rule.
- Use the Security Configuration Wizard.
- Run the 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 reduce 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

- Event Logging.
- Performance Monitoring.

Lab : Monitoring Server Performance

- Creating a Performance Baseline.
- Simulating a Server Load.
- Determining Probable Performance Bottlenecks.
- Create, Test, and Verify an Alert.

After completing this module, students will be able to:

- Use the Event Viewer to identify and interpret Windows Logs, and Application and Services Logs.

- 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

- Installing and Configuring Windows Server Update Services.
- 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.
