#10967: FUNDAMENTALS OF A WINDOWS SERVER INFRASTRUCTURE

Available Dates: **Call for Dates**
Class Length: **5 day**
Cost:
Email Computer Visions about this class

Class Outline:

Description:
Learn the fundamental knowledge and skills that you need to build a Windows Server infrastructure with Windows Server 2012.

This five-day course provides the networking, security, and system administration information that you need to implement a Windows Server infrastructure. It covers the basics of installation and configuration, storage, network infrastructure, network components, network protocols, server roles, Active Directory Domain Services (AD DS), Group Policy, IT security, server security, network security, security software, monitoring server performance, and maintaining a Windows Server.

This course includes the foundational level knowledge to prepare students to start a career or cross train in Microsoft Windows Server technologies.

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.

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.

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.

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.

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.

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.

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

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.

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.

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)

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.

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.

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.