

Course 6421B:

Configuring and Troubleshooting a Windows Server 2008 Network Infrastructure

Length:	5 Days
Published:	June 24, 2011
Language(s):	English
Audience(s):	IT Professionals
Level:	200
Technology:	Windows Server 2008
Type:	Course
Delivery Method:	Instructor-led (classroom)

[Show all items](#)

### Overview

#### **About this Course**

This five-day instructor-led course provides students with the knowledge and skills to configure and troubleshoot Windows Server 2008 and Windows Server 2008 R2 Sp1 Network Infrastructures. It will cover networking technologies most commonly used with Windows Server 2008 and Windows Server 2008 R2 Sp1 such as DNS, DHCP, IPv4 and IPv6 network addressing, Network Policy server and Network Access Protection and configuring secure network access. It also covers fault tolerant storage technologies, Network Storage and routing and remote access, monitoring and compliance updates as well as other relevant technologies

#### **Audience Profile**

This course will be of interest and benefit to attendees with different back grounds and career aspirations. It will be of interest to Network Administrators who currently are, or will be, working with Windows Server 2008 servers. It will also be of interest and benefit to Active Directory technology specialists who aspire to be Enterprise Administrators (Tier 4 day-to-day network operations) or experienced Server Administrators who aspire to be Enterprise Administrators.

Storage Area Network Administrators who need to understand this information to deploy or extend their current storage infrastructure and Operations Managers who need this information to support troubleshooting efforts and business decisions would also benefit from this course

This course also maps directly to the **70-642:TS: Windows Server 2008 Network Infrastructure, Configuring** exam objective domain and is part of the MCTS prerequisites for the **MCITP: Server Administrator** credential. As such people looking to take the 70-642 exam or obtain the **MCITP: Server Administrator** credential would also benefit from attending this course.

#### **At Course Completion**

After completing this course, students will be able to:

- Plan and configure an IPv4 network infrastructure.
- Implement DHCP within their organization.

- Configure and troubleshoot DNS.
- Configure, transition to, and troubleshoot IPv6.
- Configure and troubleshoot Routing and Remote Access.
- Install, configure, and troubleshoot the Network Policy Server Role service.
- Implement Network Access Protection.
- Implement security features within Windows Server 2008 and Windows Server 2008 R2.
- Implement security features within Windows Server 2008 and Windows Server 2008 R2 that help to secure network communications.
- Configure and troubleshoot file and print services.
- Enable and configure services to optimize branch office data access.
- Control and monitor network storage.
- Recover data on Windows Server 2008 and Windows Server 2008 R2 servers.
- Monitor Windows Server 2008 and Windows Server R2 network infrastructure services.

---

## Course Details

**Course Outline**  
**Module 1: Planning and Configuring IPv4** This module explains how to deploy and configure networking services in your organization. This module explains how to implement an IPv4 addressing scheme, determine which name services to deploy, and troubleshoot network-related problems.

**Lessons**

- Implementing an IPv4 Network Infrastructure
- Overview of Name Resolution Services in an IPv4 Network Infrastructure
- Configuring and Troubleshooting IPv4

**Lab : Planning and Configuring IPv4**

- Selecting an IPv4 Addressing scheme for branch offices
- Implementing and Verifying IPv4 in the branch office

After completing this module, students will be able to:

- Plan an IPv4 addressing scheme.
- Determine which name services you must deploy.
- Configure and troubleshoot an IPv4 network.

**Module 2: Configuring and Troubleshooting DHCP** This module introduces you to Dynamic Host Configuration Protocol (DHCP), which plays an important role in the Windows Server 2008 R2 infrastructure. It is the primary means of distributing important network configuration information to network clients, and it provides configuration information to other network-enabled services, including Windows Deployment Services (WDS) and Network Access Protection (NAP). To support and troubleshoot a Windows Server-based network infrastructure, it is important that you understand how to deploy, configure, and troubleshoot the DHCP Server Role.

**Lessons**

- Overview of the DHCP Server Role
- Configuring DHCP Scopes
- Configuring DHCP Options

- Managing a DHCP Database
- Monitoring and Troubleshooting DHCP
- Configuring DHCP Security

**Lab : Configuring and Troubleshooting the DHCP Server Role**

- Selecting a Suitable DHCP Configuration
- Implementing DHCP
- Reconfiguring DHCP in the Head Office
- Testing the Configuration
- Troubleshooting DHCP Issues

After completing this module, students will be able to:

- Describe the function of the DHCP Server Role.
- Configure DHCP scopes.
- Configure DHCP options.
- Manage a DHCP database.
- Monitor and troubleshoot the DHCP Server Role.
- Configure security the DHCP Server Role.

**Module 3: Configuring and Troubleshooting DNS** This module introduces you to Domain Name System (DNS), which is the foundation name service in Windows Server 2008 R2. It is vital that you understand how to deploy, configure, manage, and troubleshoot this critical service. **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**

- Selecting a DNS Configuration
- Deploying and Configuring DNS
- Troubleshooting DNS

After completing this module, students will be able to:

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

**Module 4: Configuring and Troubleshooting IPv6 TCP/IP** This module introduces you to IPv6, a technology that will help ensure that the Internet can support a growing user base and the increasingly large number of IP-enabled devices. The current Internet Protocol Version 4 (IPv4) has served as the underlying Internet protocol for almost thirty years. Its robustness, scalability, and limited feature set is now challenged by the growing need for new IP addresses, due in large part to the rapid growth of new network-aware devices. **Lessons**

- Overview of IPv6
- IPv6 Addressing
- Coexistence with IPv6

- IPv6 Transition Technologies
- Transitioning from IPv4 to IPv6

**Lab : Configuring an ISATAP Router**

- Configuring a New IPv6 Network and Client
- Configuring an ISATAP Router to Enable Communication Between an IPv4 Network and an IPv6 Network

**Lab : Converting the Network to Native IPv6**

- Transitioning to a Native IPv6 Network

After completing this module, students will be able to:

- Describe the features and benefits of IPv6.
- Implement IPv6 addressing.
- Implement an IPv6 coexistence strategy.
- Describe and select a suitable IPv6 transition solution.
- Transition from IPv4 to IPv6.
- Troubleshoot an IPv6-based network.

**Module 5: Configuring and Troubleshooting Routing and Remote Access** To support your organization's distributed workforce, you must become familiar with technologies that enable remote users to connect to your organization's network infrastructure. These technologies include virtual private networks (VPNs) and DirectAccess. It is important that you understand how to configure and secure your remote access clients by using network policies. This module explores these remote access technologies.

- Lessons**
- Configuring Network Access
  - Configuring VPN Access
  - Overview of Network Policies
  - Overview of the Connection Manager Administration Kit
  - Troubleshooting Routing and Remote Access
  - Configuring DirectAccess

**Lab : Configuring and Managing Network Access**

- Configuring Routing and Remote Access as a VPN Remote Access Solution
- Configuring a Custom Network Policy
- Create and distribute a CMAK Profile

**Lab : Configuring and Managing DirectAccess**

- Configure the AD DS Domain Controller and DNS
- Configure the PKI Environment
- Configure the DirectAccess Clients and Test Intranet Access
- Configure the DirectAccess Server
- Verify DirectAccess Functionality

After completing this module, students will be able to:

- Configure network access.
- Create and configure a VPN solution.
- Describe the role of network policies.
- Use the Connection Manager Administration Kit to create and configure client connection profiles.

- Troubleshoot routing and remote access.
- Implement DirectAccess.

### **Module 6: Installing, Configuring, and Troubleshooting the Network Policy Server Role**

**Service**NPS provides support for the Remote Authentication Dial-In User Service (RADIUS) protocol, and can be configured as a RADIUS server or proxy. Additionally, NPS provides functionality that is essential for the implementation of Network Access Protection (NAP). This module explains how to install, configure, and troubleshoot 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 : Configuring and Managing Network Policy Server**

- Installing and Configuring the Network Policy Server Role Service
- Configuring a RADIUS Client
- Configuring Certificate Auto-Enrollment
- Configuring and Testing the VPN

After completing this module, students will be able to:

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

**Module 7: Implementing Network Access Protection**In this module, you will learn about Network Access Protection (NAP). NAP enables you to create customized health-requirement policies to validate computer health before allowing access or communication. NAP also automatically updates compliant computers to ensure on-going compliance and can limit the access of noncompliant computers to a restricted network until they become compliant.**Lessons**

- Overview of Network Access Protection
- How NAP Works
- Configuring NAP
- Monitoring and Troubleshooting NAP

#### **Lab : Implementing NAP into a VPN Remote Access Solution**

- Configuring NAP Components
- Configuring Client Settings to Support NAP

After completing this module, students will be able to:

- Describe how NAP can help protect your network.
- Describe the various NAP enforcement processes.
- Configure NAP.
- Monitor and troubleshoot NAP.

**Module 8: Increasing Security for Windows Servers**Security is an essential consideration for networking with Windows Server 2008. In this module, you will learn how to implement various methods to increase security. Windows Firewall with Advanced Security is one of the features in Windows Server 2008 that is used to increase security. You can also use Windows Server Update Services to ensure that approved security updates are applied to servers in a timely way.**Lessons**

- Windows Security Overview

- Configuring Windows Firewall with Advanced Security
- Deploying Updates with Windows Server Update Services

**Lab : Increasing Security for Windows Servers**

- Deploying a Windows Firewall Rule
- Implementing WSUS

After completing this module, students will be able to:

- Describe a process for increasing the security of Windows Server 2008.
- Configure Windows Firewall with Advanced Security.
- Describe Windows Server Update Services and how to use it.

**Module 9: Increasing Security for Network Communication** Internet Protocol security (IPsec) is a framework of open standards for protecting communications over IP networks through cryptographic security services. IPsec supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection. The Microsoft IPsec implementation is based on standards that the Internet Engineering Task Force (IETF) IPsec working group developed. In this module, you will learn how to implement, configure, and troubleshoot IPsec.

- Lessons**
- Overview of IPsec
  - Configuring Connection Security Rules
  - Configuring NAP with IPsec Enforcement
  - Monitoring and Troubleshooting IPsec

**Lab : Increasing Security for Network Communication**

- Selecting a Network Security Configuration
- Configuring IPsec to Authenticate Computers
- Testing IPsec Authentication

After completing this module, students will be able to:

- Describe when and how to use IPsec.
- Configure Connection Security rules.
- Configure IPsec with NAP Enforcement.
- Describe how to monitor and troubleshoot IPsec.

**Module 10: Configuring and Troubleshooting Network File and Print Services** File and print services are some of the most commonly implemented network services for end users. Unlike infrastructure services like DNS, file and print services are highly visible to the end users. In this module, you will learn how to configure and troubleshoot file and print services to provide high quality service to end users. In addition, you will see how both EFS and BitLocker can be used to increase the security of files that are located in file shares.

- Lessons**
- Configuring and Troubleshooting File Shares
  - Encrypting Network Files with EFS
  - Encrypting Partitions with BitLocker
  - Configuring and Troubleshooting Network Printing

**Lab : Configuring and Troubleshooting Network File and Print Services**

- Creating and Configuring a File Share
- Encrypting and Recovering Files
- Creating and Configuring a Printer Pool

After completing this module, students will be able to:

- Describe how to manage file share security.

- Explain how to encrypt network files with EFS.
- Describe how to encrypt partitions with BitLocker.
- Discuss how to configure and troubleshoot network printing.

### **Module 11: Optimizing Data Access for Branch Offices**

Many organizations maintain a large number of file resources that need to be organized and made highly available to users. These file resources are often stored on servers and provided to users who are distributed geographically in widespread locations. In this module, you will learn how to provide efficient access to network resources with minimal traffic over a WAN link.

#### **Lessons**

- Branch Office Data Access
- DFS Overview
- Overview of DFS Namespaces
- Configuring DFS Replication
- Configuring BranchCache

#### **Lab : Implementing DFS**

- Installing the DFS Role Service
- Configuring the Required Namespace
- Configuring DFS Replication

#### **Lab : Implementing BranchCache**

- Performing Initial Configuration Tasks for BranchCache
- Configuring BranchCache Clients
- Configuring BranchCache on the Branch Server
- Monitoring BranchCache

After completing this module, students will be able to:

- Describe the challenges experienced when providing data access to branch offices.
- Identify the basic components of DFS.
- Describe DFS namespaces.
- Explain how to configure DFS replication.
- Discuss how to configure BranchCache.

**Module 12: Controlling and Monitoring Network Storage** Network storage for users is a finite resource that must be managed appropriately to ensure that it remains available for all users. If network storage is not monitored and managed, it can become filled with irrelevant data, such as personal music or movies. Irrelevant data increases network storage costs and in some cases can prevent useful data from placement on the network storage. In this module, you will learn how to monitor and manage network storage.

- #### **Lessons**
- Monitoring Network Storage
  - Controlling Network Storage Utilization
  - Managing File Types on Network Storage

#### **Lab : Controlling and Monitoring Network Storage**

- Configuring FSRM Quotas
- Configuring File Screening
- Configuring File Classification and File Management

After completing this module, students will be able to:

- Describe how to monitor network storage by using FSRM.
- Explain how to manage quotas by using FSRM.
- Describe how to implement file screening, classification management, and file management tasks by using FSRM.

**Module 13: Recovering Network Data and Servers** This module explains how to recover network data and servers. There are a variety of scenarios where a network data or a server that provides networks services can be lost. Volume shadow copies can be used to restore previous versions of files when a file is accidentally deleted or modified on a computer that is running Windows Server 2008. Windows Server Backup can be used to back up and restore data files or an entire server.

- Lessons**
- Recovering Network Data with Volume Shadow Copies
  - Recovering Network Data and Servers with Windows Server Backup

**Lab : Recovering Network Data and Servers**

- Configuring Shadow Copies
- Configuring a Scheduled Backup

After completing this module, students will be able to:

- Describe how to configure and use volume shadow copies.
- Describe how to configure and use Windows Server Backup.

**Module 14: Monitoring Windows Server 2008 Network Infrastructure Servers**

When a system failure or an event that affects system performance occurs, you need to be able to repair the problem or resolve the issue quickly and efficiently. With so many variables and possibilities in the modern network environment, the ability to determine the root cause quickly often depends on having an effective performance monitoring methodology and toolset. In this module, you will learn to use performance-monitoring tools to identify components that require additional tuning and troubleshooting. By identifying components that require additional tuning, you can improve the efficiency of your servers.

**Lessons**

- Monitoring Tools
- Using Performance Monitor
- Monitoring Event Logs

**Lab : Monitoring Windows Server 2008 Network Infrastructure Servers**

- Establishing a Performance Baseline
- Identifying the Source of a Performance Problem
- Centralizing Events Logs

After completing this module, students will be able to:

- Describe monitoring tools for Windows Server 2008 R2.
- Describe how to use performance monitor.
- Describe how to monitor event logs.

---

Prerequisites

Before attending this course, students must have:

- You must have an intermediate understanding of Windows Server operating systems such as Windows Server 2003, Windows Server 2008 or Windows Server 2008 R2 Sp1 and



Windows client operating systems such as Windows Vista or Windows 7. Client operating system knowledge equivalent to the below certifications would be of benefit.

Exam 70-680: TS: Windows 7, Configuration

or

Exam 70-620: TS: Windows Vista, Configuring

- You should understand how TCP/IP functions and have a basic understanding of addressing, name resolution (Domain Name System [DNS]/Windows Internet Name Service [WINS]), connection methods (wired, wireless, virtual private network [VPN]).
- You should have an awareness of security best practices such as understanding file system permissions, authentication methods, workstation, and server hardening methods, and so forth.

The minimum level of knowledge required in the above three bullet points, excluding the client experience, can be covered by having knowledge equivalent to the MOC course **6420B: Fundamentals of Windows Server 2008**

- Basic knowledge of Active Directory would also be of benefit.

---

### Community

**Have Questions?**For advice about training and certification, connect with peers:

- [Visit the training and certification forum](#)

For questions about a specific certification, chat with a Microsoft Certified Professional (MCP):

- [Visit our MCP newsgroups](#)

To find out about recommended blogs, Web sites, and upcoming Live Meetings on popular topics, visit our community site:

- [Visit the Microsoft Learning community](#)

## VERSÃO PORTUGUÊS

Configuração e Solução de problemas de infra-estrutura de rede do Windows Server 2008

Comprimento: 5 Dias

Publicado em: 24 de junho de 2011

Idioma (s): Inglês

Audiência (s): Profissionais de TI

Nível: 200

Tecnologia: Windows Server 2008

Tipo: Curso

Método de entrega: Conduzido por instrutor (sala de aula)

Mostrar todos os itens

Visão global

### **Sobre este Curso**

Este curso de cinco dias instrutor, fornece aos alunos o conhecimento e as habilidades para configurar e solucionar problemas do Windows Server 2008 e Windows Server 2008 R2 Infra-estruturas de rede SP1. Ele cobrirá tecnologias de rede mais utilizados com o Windows Server 2008 e Windows Server 2008 R2 SP1, como DNS, DHCP, IPv4 e IPv6 rede, servidor de rede e Política de Proteção de Acesso à rede e configuração de acesso de rede seguro. Ele também abrange tecnologias de tolerância a falhas de armazenamento, rede e roteamento e acesso remoto, monitoramento e atualizações de conformidade, bem como outras tecnologias relevantes

### **Perfil público**

Este curso será de interesse e benefício para os participantes com fundamentos diferentes costas e aspirações de carreira. Vai ser de interesse para administradores de rede, que atualmente são, ou serão, trabalhando com servidores Windows Server 2008. Também será de interesse e benefício para especialistas do Active Directory tecnologia que aspiram a ser administradores de empresas (operações Tier 4 dia-a-dia da rede) ou administradores de servidor experientes que aspiram a ser administradores de empresas.

Administradores de área de armazenamento de rede que precisam ter conhecimento dessas informações para implantar ou ampliar sua infra-estrutura de armazenamento atual e gerentes de operações que necessitam de informações para apoiar os esforços de solução de problemas e decisões de negócios também seriam beneficiados com este curso

Este curso também mapeia diretamente para o 7 **0-642: TS: Windows Server 2008 Network Infrastructure, Configuring** domínio objetivo do exame e faz parte dos pré-requisitos para o MCTS **MCITP: Server Administrator** credencial. Como essas pessoas olhando para o exame 70-642 ou obter o **MCITP: Server Administrator** credencial também seriam beneficiados com este curso.

### **Na conclusão do curso**

Após a conclusão deste curso, os alunos serão capazes de:

- Planejar e configurar uma infraestrutura de rede IPv4.
- Implementar DHCP dentro de sua organização.
- Configurar e solucionar problemas de DNS.
- Configure, a transição para e solucionar problemas de IPv6.
- Configurar e solucionar problemas de roteamento e acesso remoto.
- Instalar, configurar e solucionar problemas do Policy Network serviço de função do servidor.
- Implementar Network Access Protection.
- Implementar recursos de segurança no Windows Server 2008 e Windows Server 2008 R2.
- Implementar recursos de segurança no Windows Server 2008 e Windows Server 2008 R2 que ajudam a proteger as comunicações de rede.
- Configurar e solucionar arquivo e serviços de impressão.
- Habilitar e configurar serviços para otimizar filial acesso a dados.
- Controle e monitor de armazenamento de rede.
- Recuperar dados em Windows Server 2008 e Windows Server 2008 R2 servidores.
- Monitor de Windows Server 2008 e Windows Server R2 serviços de infraestrutura de rede.

---

## Detalhes do curso

**Esboço do Curso**  
**Módulo 1: Planejamento e configuração de IPv4** Este módulo explica como implementar e configurar serviços de rede em sua organização. Este módulo explica como implementar um esquema de endereçamento IPv4, determinar quais serviços de nome de implantar e solucionar problemas relacionados à rede.**Lições**

- Implementação de uma infra-estrutura de rede IPv4
- Visão geral dos Serviços de resolução de nomes em uma infra-estrutura de rede IPv4
- Configuração e Solução de problemas IPv4

**Laboratório: Planejamento e configuração de IPv4**

- A seleção de um esquema de endereçamento IPv4 para filiais
- Implementação e Verificação IPv4 na filial

Depois de concluir este módulo, os alunos serão capazes de:

- Planejar um esquema de endereçamento IPv4.
- Determinar quais os serviços de nome que você deve implantar.
- Configurar e solucionar problemas de uma rede IPv4.

**Módulo 2: Configuração e Solução de Problemas DHCP** Este módulo apresenta Dynamic Host Configuration Protocol (DHCP), que desempenha um papel importante na infra-estrutura Windows Server 2008 R2. É o principal meio de distribuição de informações importantes de configuração de rede para clientes de rede, e fornece informações de configuração de rede para outros serviços habilitados, incluindo o Windows Deployment Services (WDS) e Network Access Protection (NAP). Para apoiar e solucionar problemas de um servidor baseado no Windows infra-estrutura de rede, é importante que você entenda como implementar, configurar e solucionar problemas da função de servidor DHCP.**Lições**

- Visão geral da função de servidor DHCP
- Configurando o DHCP Scopes
- Configurar opções de DHCP
- Gerenciando um banco de dados DHCP
- Monitoramento e Resolução de Problemas DHCP
- Configurando o DHCP Segurança

**Laboratório: Configuração e Solução de problemas da função de servidor DHCP**

- Selecionando uma configuração de DHCP Adequado
- Implementar DHCP
- Reconfiguração DHCP na sede
- Testando a configuração
- Solução de problemas Problemas de DHCP

Depois de concluir este módulo, os alunos serão capazes de:

- Descrever a função da função de servidor DHCP.
- Configurar DHCP escopos.
- Configurar as opções DHCP.
- Gerenciar um banco de dados DHCP.
- Monitorar e solucionar a função de servidor DHCP.
- Configurar a segurança a função de servidor DHCP.

**Módulo 3: Configuração e Solução de Problemas de DNS** Este módulo apresenta Domain Name System (DNS), que é o serviço de nome de fundação no Windows Server 2008 R2. É vital que você entenda como implementar, configurar, gerenciar e solucionar esse serviço essencial.**Lições**

- Instalar a função de servidor DNS
- Configurando a função de servidor DNS
- Configurando zonas DNS
- Configurando transferências de zona DNS
- Gerenciar e solucionar problemas de DNS

### **Laboratório: Configuração e Solução de Problemas de DNS**

- Selecionando uma configuração de DNS
- Implantação e configuração de DNS
- Solução de problemas de DNS

Depois de concluir este módulo, os alunos serão capazes de:

- Instalar a função de servidor DNS.
- Configurar a função de servidor DNS.
- Criar e configurar as zonas DNS.
- Configurar transferências de zona.
- Gerenciar e solucionar problemas de DNS.

**Módulo 4: Configuração e Solução de Problemas IPv6 TCP / IP** Este módulo apresenta para o IPv6, uma tecnologia que vai ajudar a garantir que a Internet pode apoiar uma base de usuários crescente e ao número cada vez maior de dispositivos habilitados para IP. A versão actual protocolo Internet 4 (IPv4) tem servido como o protocolo de Internet básica para quase trinta anos. A sua robustez, escalabilidade e conjunto limitado de funcionalidades é agora contestado pela crescente necessidade de novos endereços IP, em grande parte devido ao rápido crescimento de novas redes de reconhecimento de dispositivos. **Lições**

- Visão geral do IPv6
- Endereçamento IPv6
- Convivência com o IPv6
- Tecnologias de transição IPv6
- A transição do IPv4 para o IPv6

### **Laboratório: Configuração de um roteador ISATAP**

- Configurando uma nova rede IPv6 e cliente
- Configurando um roteador ISATAP para permitir a comunicação entre uma rede IPv4 e uma rede IPv6

### **Laboratório: Converter a rede para IPv6 nativo**

- Transição para uma rede IPv6 nativa

Depois de concluir este módulo, os alunos serão capazes de:

- Descrever as características e benefícios do IPv6.
- Implementar o endereçamento IPv6.
- Implementar uma estratégia de convivência IPv6.
- Descrever e selecionar uma solução de transição adequado IPv6.
- Transição do IPv4 para o IPv6.
- Solucionar problemas de uma rede baseada em IPv6.

**Módulo 5: Configuração e Solução de Problemas de Roteamento e Acesso Remoto** Para suportar força de trabalho distribuída da sua organização, você deve se familiarizar com as tecnologias que permitem que usuários remotos se conectem à infra-estrutura de rede da organização. Essas tecnologias incluem redes privadas virtuais (VPNs) e DirectAccess. É importante que você entenda como configurar e proteger seus clientes de acesso remoto através de políticas de rede. Este módulo explora as tecnologias de acesso remoto. **Lições**

- Configurando acesso à rede
- Configurando o acesso VPN
- Visão geral de políticas de rede
- Visão geral do Kit de Administração do Gerenciador de Conexões
- Resolução de Problemas de Roteamento e Acesso Remoto
- Configurando o DirectAccess

### **Laboratório: Configuração e Gerenciamento de Acesso à Rede**

- Configurando o roteamento e acesso remoto como uma solução de acesso remoto VPN
- Configurar uma diretiva de rede personalizada
- Criar e distribuir um perfil CMAK

### **Laboratório: Configurando e Gerenciando DirectAccess**

- Configurar o AD DS Domain Controller e DNS
- Configurar o ambiente de PKI
- Configure os clientes DirectAccess e Teste de acesso Intranet
- Configurar o servidor DirectAccess
- Verifique a funcionalidade do DirectAccess

Depois de concluir este módulo, os alunos serão capazes de:

- Configure o acesso à rede.
- Criar e configurar uma solução de VPN.
- Descrever o papel das políticas de rede.
- Use o Kit de administração Manager para criar e configurar perfis de conexão do cliente.
- Solucionar problemas de roteamento e acesso remoto.
- Implementar o DirectAccess.

**Módulo 6: Instalação, Configuração e Solução de Problemas da Rede Política de função do servidor serviçoNPS** fornece suporte para o Remote Authentication Dial-In User Service (RADIUS) protocolo, e pode ser configurado como um servidor RADIUS ou proxy. Além disso, o NPS fornece funcionalidade que é essencial para a implementação da Rede de Proteção de Acesso (NAP). Este módulo explica como instalar, configurar e solucionar problemas de NPS.**Lições**

- Instalando e Configurando um Servidor de Diretivas de Rede
- Configurando clientes e servidores RADIUS
- Métodos de autenticação do NPS
- Monitoramento e solução de problemas de uma Network Policy Server

### **Laboratório: Configurando e Gerenciando Network Policy Server**

- Instalando e Configurando o Policy Network serviço de função Servidor
- Configurando um cliente RADIUS
- Configurando um certificado de inscrição automática
- Configurando e testando a VPN

Depois de concluir este módulo, os alunos serão capazes de:

- Instalar e configurar o NPS.
- Configurar clientes e servidores RADIUS.
- Descrever os métodos de autenticação do NPS.
- Monitorar e solucionar problemas de NPS.

**Módulo 7: Implementando Network Access Protection** Neste módulo, você vai aprender sobre Network Access Protection (NAP). NAP permite que você crie personalizados saúde exigência de políticas para validar o computador, antes de permitir o acesso ou a comunicação. PAN também automaticamente atualizações de computadores compatíveis para garantir a conformidade em curso e pode limitar o acesso de computadores não compatíveis a uma rede restrita até que eles se tornem compatíveis.**Lições**

- Visão geral de Proteção de Acesso à Rede
- Como NAP funciona
- Configurando NAP
- Monitoramento e Resolução de Problemas NAP

### **Laboratório: Implementando NAP em uma solução de acesso remoto VPN**

- Configurando componentes NAP
- Configurar as definições do cliente para suportar NAP

Depois de concluir este módulo, os alunos serão capazes de:

- Descreva como o NAP pode ajudar a proteger sua rede.
- Descrever os processos de execução vários NAP.
- Configurar NAP.
- Monitorar e solucionar problemas de NAP.

**Módulo 8: Aumentar a segurança para Windows Servers** A segurança é uma consideração

essencial para redes com o Windows Server 2008. Neste módulo, você vai aprender como implementar vários métodos para aumentar a segurança. Windows Firewall com segurança avançada é um dos recursos do Windows Server 2008 que é usado para aumentar a segurança. Você também pode usar Windows Server Update Services para garantir que as atualizações de segurança aprovadas são aplicadas a servidores de uma maneira oportuna. **Lições**

- Visão geral de segurança do Windows
- Configurando o Windows Firewall com segurança avançada
- Implantando atualizações com o Windows Server Update Services

**Laboratório: Aumentar a segurança para Windows Servers**

- Implantação de uma regra de firewall do Windows
- Implementação do WSUS

Depois de concluir este módulo, os alunos serão capazes de:

- Descrever um processo para aumentar a segurança do Windows Server 2008.
- Configure o Windows Firewall com segurança avançada.
- Descreva Windows Server Update Services e como usá-lo.

**Módulo 9: Aumentar a segurança para Rede de Comunicação** Internet Protocol Security (IPSec) é uma estrutura de padrões abertos para proteger as comunicações em redes IP através de serviços de segurança criptográfica. IPsec suporta em nível de rede de pares de autenticação, os dados origem autenticação, integridade de dados, confidencialidade de dados (criptografia) e proteção contra reprodução. A implementação do Microsoft IPsec é baseado em padrões que a Internet Engineering Task Force (IETF) IPsec grupo de trabalho desenvolvidos. Neste módulo, você vai aprender a implementar, configurar e solucionar problemas de IPsec. **Lições**

- Visão de IPsec
- Configurando regras de segurança de conexão
- Configurando NAP com IPsec Enforcement
- Monitoramento e solução de problemas IPsec

**Laboratório: Aumentar a segurança para comunicação de rede**

- Seleção de uma configuração de segurança da rede
- A configuração do IPsec para autenticar computadores
- Teste IPsec Autenticação

Depois de concluir este módulo, os alunos serão capazes de:

- Descrever quando e como usar o IPsec.
- Configurar regras de segurança de conexão.
- Configurar o IPsec com imposição de NAP.
- Descreva como monitorar e solucionar problemas de IPsec.

**Módulo 10: Configuração e Solução de problemas de arquivos de rede e Serviços de impressão** de arquivos e serviços de impressão são alguns dos serviços de rede mais comumente implementadas para usuários finais. Ao contrário dos serviços de infraestrutura, como DNS, serviços de arquivo e impressão são altamente visíveis para os usuários finais. Neste módulo, você vai aprender a configurar e solucionar problemas de arquivo e serviços de impressão para fornecer serviços de alta qualidade para os usuários finais. Além disso, você vai ver como os dois EFS e BitLocker pode ser usado para aumentar a segurança dos arquivos que estão localizados em compartimentos de arquivos. **Lições**

- Configuração e Solução de Problemas compartimentos de arquivos
- Criptografar arquivos de rede com o EFS
- Criptografando partições com o BitLocker
- Configuração e Solução de Problemas de Impressão em Rede

**Laboratório: Configuração e Solução de problemas de arquivos de rede e serviços de impressão**

- Criando e Configurando um compartimento de arquivos
- Criptografando e Recuperação de Arquivos
- Criando e Configurando um pool de impressão

Depois de concluir este módulo, os alunos serão capazes de:

- Descreva como gerenciar a segurança de compartilhamento de arquivos.
- Explique como criptografar arquivos de rede com EFS.
- Descreva como criptografar partições com o BitLocker.
- Discutir como configurar e solucionar problemas de impressão em rede.

### **Módulo 11: Otimizando o acesso a dados para filiais**

Muitas organizações manter um grande número de recursos de arquivos que precisam ser organizados e altamente disponível para os usuários. Estes recursos de arquivos são muitas vezes armazenados em servidores e fornece aos usuários que estão distribuídos geograficamente em locais amplos. Neste módulo, você vai aprender como fornecer acesso eficiente a recursos de rede com tráfego mínimo através de um link WAN.

#### **Lições**

- Filial de acesso a dados
- DFS Visão
- Visão de Namespaces DFS
- Configurando Replicação DFS
- Configurando BranchCache

#### **Laboratório: Implementando DFS**

- Instalar o serviço de função DFS
- Configurando o namespace necessário
- Configurando Replicação DFS

#### **Laboratório: Implementando BranchCache**

- Executando tarefas de configuração iniciais para BranchCache
- Configurando clientes BranchCache
- Configurando BranchCache no Servidor de Filial
- Monitoramento BranchCache

Depois de concluir este módulo, os alunos serão capazes de:

- Descrever os desafios vivenciados ao fornecer acesso a dados para filiais.
- Identificar os componentes básicos de DFS.
- Descreva namespaces DFS.
- Explicar como configurar a replicação DFS.
- Discutir como configurar BranchCache.

**Módulo 12: Controle e Monitoramento de armazenamento de rede** armazenamento de rede para os usuários é um recurso finito que deve ser gerenciado de forma adequada para garantir que ele fica disponível para todos os usuários. Se o armazenamento de rede não é monitorado e gerenciado, ele pode tornar-se preenchido com dados irrelevantes, como pessoal de música ou filmes. Dados irrelevantes aumenta os custos de armazenamento em rede e em alguns casos pode evitar que dados úteis de colocação no armazenamento de rede. Neste módulo, você vai aprender como monitorar e gerenciar o armazenamento de rede.

- #### **Lições**
- Monitoramento de armazenamento de rede
  - Controlar a utilização de armazenamento de rede
  - Gerenciando tipos de arquivo no armazenamento de rede

#### **Laboratório: Controle e Monitoramento de armazenamento de rede**

- Configurando cotas FSRM
- Configurando Triagem de Arquivo
- Configurando Classificação Arquivo e Gestão de Ficheiros

Depois de concluir este módulo, os alunos serão capazes de:

- Descrever como monitorar o armazenamento de rede usando FSRM.
- Explique como gerenciar cotas usando FSRM.
- Descrevem como implementar a triagem de arquivos, gerenciamento de classificação, e as tarefas de gerenciamento de arquivos usando FSRM.

**Módulo 13: Recuperação de dados de rede e servidores** Este módulo explica como recuperar dados de rede e servidores. Há uma variedade de cenários onde uma rede de dados ou um servidor que fornece serviços de redes podem ser perdidos. Cópias de sombra de volume pode ser usado para restaurar versões anteriores de arquivos quando um arquivo é apagado acidentalmente ou modificado em um computador que está executando o Windows Server 2008. Backup do Windows Server pode ser usado para fazer backup e restaurar arquivos de dados ou um servidor inteiro.

- Lições**
- Recuperação de dados de rede com cópias de sombra de volume
  - Recuperação de dados de rede e servidores com Windows Server Backup

**Laboratório: Rede de Dados Recuperação e Servidores**

- Configurando Cópias de Sombra
- Configurando um backup agendado

Depois de concluir este módulo, os alunos serão capazes de:

- Descrever como configurar e usar cópias de sombra de volume.
- Descrever como configurar e usar o Backup do Windows Server.

**Módulo 14: Monitoramento servidores Windows Server 2008 Network Infrastructure**

Quando uma falha de sistema ou de um evento que afeta o desempenho do sistema ocorre, você precisa ser capaz de reparar o problema ou resolver o problema de forma rápida e eficiente. Com tantas variáveis e possibilidades no ambiente de rede moderna, a capacidade de determinar a causa raiz rapidamente, muitas vezes depende de uma metodologia de acompanhamento eficaz desempenho e ferramentas. Neste módulo, você vai aprender a usar ferramentas de monitoramento de desempenho para identificar os componentes que requerem um ajuste adicional e solução de problemas. Ao identificar componentes que requerem um ajuste adicional, você pode melhorar a eficiência de seus servidores.

**Lições**

- Ferramentas de monitoramento
- Usando o Monitor de Desempenho
- Logs de eventos de monitoramento

**Laboratório: Monitoramento servidores Windows Server 2008 Network Infrastructure**

- Estabelecer um parâmetro de desempenho
- Identificar a origem de um problema de desempenho
- A centralização registra eventos

Depois de concluir este módulo, os alunos serão capazes de:

- Descrever as ferramentas de monitoramento para o Windows Server 2008 R2.
- Descrever como usar o monitor de desempenho.
- Descreva como monitorar logs de eventos.

---

Pré-requisitos

Antes de participar deste curso, os alunos devem ter:

- Você deve ter um entendimento intermediário de sistemas operacionais Windows Server como o Windows Server 2003, Windows Server 2008 ou Windows Server 2008 R2 SP1 e sistemas operacionais Windows clientes, como Windows Vista ou Windows 7. Cliente conhecimento do sistema operacional equivalente às certificações abaixo seria de benefício.

Exame 70-680: TS: Windows 7, Configuration

ou

Exame 70-620: TS: Windows Vista, Configuring

- Você deve entender como funciona o TCP / IP e ter um entendimento básico de



endereçamento, resolução de nomes (Domain Name System [DNS] / Windows Internet Name Service [WINS]), métodos de ligação (com fio, sem fio, rede privada virtual [VPN]).

- Você deve ter uma consciência de melhores práticas de segurança, tais como permissões de compreensão do sistema de arquivos, métodos de autenticação de estações de trabalho e métodos de proteção de servidores, e assim por diante.

O nível mínimo de conhecimento exigido nos acima de três pontos de bala, excluindo a experiência do cliente, podem ser cobertas por ter conhecimento equivalente ao curso **MOC 6420B: Fundamentos do Windows Server 2008**

- Conhecimentos básicos de Active Directory também seria de benefício.

---

## Comunidade

**Dúvidas?** Para aconselhamento sobre treinamento e certificação, se conectar com colegas:

- [Visite o fórum de formação e certificação](#)

Para perguntas sobre uma certificação específica, conversar com um Microsoft Certified Professional (MCP):

- [Visite newsgroups nossos MCP](#)

Para saber mais sobre blogs, sites recomendados e futuras reuniões ao vivo sobre temas populares, visite o nosso site da comunidade:

- [Visite o Microsoft comunidade de aprendizagem](#)