

70-299 Implementing and Administering Security in a Microsoft Windows Server 2003 Network

- **Course Number:** 70-299
- **Length:** 1 Day(s)

Course Overview

This course is part of the MCSA training..

Prerequisites

Before attending this course, students must have 6 to 12 months of experience administering client and network operating systems in environments that have the following characteristics:

- Have experience reading user requirements and business-need documents.
- Three or more physical locations
- Three or more domain controllers
- 250 to 5,000 or more users
- Connecting branch offices and individual users in remote locations to the corporate network and connecting corporate networks to the Internet
- Network services and resources such as messaging, database, file and print, proxy server, firewall, public key infrastructure (PKI), Internet, intranet, remote access, and client computer management

Audience

As this course is part of the MCSA training, candidates are usually IT professionals who work in the typically complex computing environment of medium to large companies.

Course Outline

- Level 1
- Authorization & Authentication
- 1.1 Group Strategy
- 1.2 Group Scopes
- 1.3 Built-in Groups
- 1.4 System or Special Groups
- 1.5 Administrating Security Groups
- 1.6 Restricting Groups
- 1.7 Demo – Create a Restricted Group Policy
- 1.8 Trusts
- 1.9 Authentication
- 1.10 SID
- 1.11 Demo – Trust Relationships

- 1.12 Resource Access
- 1.13 Authentication – Continued
- 1.14 Kerberos
- 1.15 Password Security
- 1.16 Tools for Troubleshooting Authentication
- 1.17 Evaluating Your Environment
- 1.18 Password Policy
- 1.19 NTLM
- 1.20 Chapter 1 – Lab
- 1.21 Chapter 1 – Review
- Lab - Add Users to Global Group
- Lab - Restricted Group Option
- Lab - Restrict Membership
- Lab - Raise Domain and Forest Levels
- Lab - Restrict NTLM Authentication
- Level 2
- Certification Authorities
- 1.1 PKI and Certification Authorities
- 1.2 Components of a PKI
- 1.3 Accounts that use PKI – Enabled Applications
- 1.4 PKI Tools
- 1.5 Certification Authority
- 1.6 CA Hierarchy
- 1.7 Installing a Certification Authority
- 1.8 Demo – Installing a Certification Authority
- 1.9 Managing a Certification Authority
- 1.10 Revoking Certificates
- 1.11 Publishes CRLs
- 1.12 Backing Up and Restoring a (CA)
- 1.13 Chapter 2 – Lab
- 1.14 Chapter 2 – Review
- Lab - Install an Enterprise CA
- Lab - Backup a Certification Authority
- Lab - Restore a Certification Authority
- Lab - Configure the CA
- Level 3
- Certificate Management
- 1.1 Configuring Certificate Templates
- 1.2 Digital Certificates
- 1.3 Digital Certificates Life Cycle
- 1.4 Certificate Templates
- 1.5 Certificate Template Permissions
- 1.6 Updating a Certificate Template
- 1.7 Deploying and Revoking Certificates
- 1.8 Managing Certificates
- 1.9 Chapter 3 – Review

- Smart Card Certificates
- 2.1 Introduction to Multifactor Authentication
- 2.2 Multifactor Authentication Devices
- 2.3 Applications That Use Smart Cards
- 2.4 Smart Card Network Support
- 2.5 Smart Card Infrastructure
- 2.6 Certification Authority Requirements
- 2.7 Smart Card Certificate Templates
- 2.8 Certificate Enrollment Methods
- 2.9 Managing and Troubleshooting
- 2.10 Demo – Smart Cards
- 2.11 Chapter 4 – Review
- Level 4
- Encrypting File System
- 1.1 What is EFS?
- 1.2 How EFS Works
- 1.3 Best Practices for Implementing EFS
- 1.4 Self-Signed Certificates
- 1.5 Managing Plaintext Data
- 1.6 EFS in a Domain Environment with a PKI
- 1.7 EFS File Sharing
- 1.8 Moving or Copying Encrypting Files
- 1.9 Managing Remotely Encrypted Files
- 1.10 Chapter 5 – Labs
- 1.11 Chapter 5 – Review
- Member Server Baseline
- 2.1 Trusted Computing Base
- 2.2 Secure Baseline Elements
- 2.3 Server Configuration
- 2.4 Planning a Secure Member Server
- 2.5 Predefined Security Templates
- 2.6 Security Environments in Server 2003
- 2.7 Storing Security Templates
- 2.8 Administrative Group Design
- 2.9 Additional Security Settings
- 2.10 Demo - Security Templates
- 2.11 Time Synchronization
- 2.12 Security Templates – Part 2
- 2.13 Chapter 6 – Review
- Level 5
- Secure Baselines
- 1.1 Planning and Configuring Domain Controls
- 1.2 Security Threats to Domain Controllers
- 1.3 Domain Controller Baseline Policy
- 1.4 Active Directory Database and Log File
- 1.5 Ntdsuil.exe

- 1.6 SYSKEY
- 1.7 Security for DNS Servers
- 1.8 Infrastructure Servers
- 1.9 Securing WINS Server
- 1.10 Demo – DHCP
- 1.11 File and Print Servers
- 1.12 IIS Servers
- 1.13 Configuring IIS Logging
- 1.14 Demo – IIS
- 1.5 Chapter 7 – Review
- Lab - Configure Event Log Size
- Lab - Configure Startup Password
- Level 6
- Secure Client Baseline
- 1.1 Security Templates
- 1.2 Templates for Securing Clients
- 1.3 Administrative and Security Templates
- 1.4 Demo – Loopback Policy Processing
- 1.5 Client Computer Baseline
- 1.6 Planning a Software Restriction Policy
- 1.7 Software Restriction Policies
- 1.8 Planning – Continued
- 1.9 Security for Mobile Clients
- 1.10 Demo – Software Restrictions
- 1.11 Chapter 8 – Review
- Lab - Add Administrative Templates to GPO
- Lab - Enable Group Policy Loopback
- Software Update Services
- 2.1 Benefits of Software Updates Services
- 2.2 Update Management Tools for Application
- 2.3 SUS Components
- 2.4 Planning an Update Management Strategy
- 2.5 Update Management Life Cycle
- 2.6 Network Environment for Status Updates
- 2.7 Demo – MBSA
- 2.8 Installing SUS
- 2.9 Updates Client Configuration
- 2.10 Managing an SUS Server
- 2.11 Demo – SUS Admin
- 2.12 Chapter 9 – Review
- Lab - Install the Software Update Service SUS
- Lab - Install Microsoft Baseline Security Analyst
- Level 7
- Data Transmission Security
- 1.1 Why Protect Network Data
- 1.2 Threats to Secure Data Transmission

- 1.3 SSL and TLS
- 1.4 Demo – Enabling SSL
- 1.5 Securing Data with PPTP
- 1.6 Server Message Block
- 1.7 Lightweight Directory Access Protocol
- 1.8 IPsec
- 1.9 IPsec Policies
- 1.10 IPsec Implementation
- 1.11 IPsec Functionality
- 1.12 Demo – IPsec Implementation
- 1.13 IPsec Troubleshooting
- 1.14 Tools for Verification
- 1.15 Demo- IPsec Traffic
- 1.16 Chapter 10 – Review
- Lab - Install Secure Sockets Layer SSL
- Lab - Default Web Site SSL
- Level 8
- Wireless Networks
- 1.1 Securing Wireless Networks
- 1.2 How to make your network more secure
- 1.3 Wireless Network Architecture
- 1.4 802.1x Authentication
- 1.5 Hardware Requirements
- 1.6 Best Practices
- 1.7 Secure WLAN Strategy
- 1.8 IAS Configuration
- 1.9 Demo – IAS Installation
- 1.10 Registering Wireless ap as RADIUS Client
- 1.11 Back Up and Export IAS Configuration
- 1.12 IAS Remote Access Policies
- 1.13 Wireless Access Policy
- 1.14 Demo – Wireless Access Policy
- 1.15 Troubleshooting
- 1.16 Chapter 11 – Review
- Lab - Internet Authentication Service
- Lab - Configure a Wireless Access Point
- Level 9
- Perimeter Security
- 1.1 What is ISA Server?
- 1.2 ISA Server Versions & Benefits
- 1.3 ISA Server Modes
- 1.4 ISA Server Clients
- 1.5 Traffic Control with ISA Server
- 1.6 Installing ISA Server 2000
- 1.7 Pre-Installation Tasks for ISA Server 2000
- 1.8 Demo – ISA Installation

- 1.9 Perimeter Networks
- 1.10 ISA Server Services
- 1.11 Common ISA Server Deployments
- 1.12 Packet Filtering and Routing
- 1.13 Publishing Servers
- 1.14 Securing ISA Server Computers
- 1.15 Best Practices
- 1.16 Chapter 12 – Review
- Level 10
- Securing Remote Access
- 1.1 Remote Access Methods
- 1.2 Threats to Remote Access
- 1.3 Tunneling Protocols
- 1.4 Access Protocols
- 1.5 Connection Manager
- 1.6 Quarantine Service
- 1.7 Demo – Remote Access
- 1.8 Planning a Remote Access Strategy
- 1.9 Components Provided by an ISP
- 1.10 Deploying Remote Access Servers
- 1.11 data Encryption
- 1.12 Remote Access Connection Conditions
- 1.13 Deploying a VPN Server
- 1.14 Demo – Configure a VPN Server
- 1.15 Quarantine Service Components
- 1.16 Demo – RA Policy with Quarantine Properties
- 1.17 Connection Manager Administration Kit
- 1.8 Chapter 13 – Review
- Final Course Review