

Securing Windows Server® 2008: Hands-On - 4 Days

Course 964 Overview

- You Will Learn How To**
- Apply Windows Server 2008 features to secure your infrastructure
 - Deploy a Windows-based Public Key Infrastructure (PKI) as a foundation for security services
 - Enhance access controls with policy-based multifactor authentication
 - Build a scalable encryption solution that assures recovery of protected data
 - Install and configure Network Access Protection (NAP) to exclude unhealthy computers
 - Implement Domain Isolation to decrease network risk for sensitive servers

Course Benefits Securing the network infrastructure has become a top priority and a major technical challenge for most organisations. Windows Server 2008 provides powerful and complex technologies for decreasing network risk and improving policy compliance. This course provides you with the knowledge and skills necessary to correctly implement these solutions.

Who Should Attend IT professionals responsible for securing a Windows-based network infrastructure. Knowledge at the level of Course 960, "Windows Server 2008 Comprehensive Introduction", or practical experience configuring and managing Windows Server 2003, is assumed.

Hands-On Training Extensive hands-on exercises provide practical experience designing and implementing a secure network infrastructure. Exercises include:

- Deploying Certificate Servers to provide key escrow and Key Recovery Agents
- Implementing policy-based, multifactor authentication
- Restoring encrypted data with Data Recovery Agents and supporting policies
- Configuring NAP to quarantine unhealthy computers
- Remediating quarantined clients to allow full network access
- Building a Domain Isolation solution to restrict access to sensitive servers

Securing Windows Server® 2008: Hands-On - 4 Days

Course 964 Outline

Enterprise Security Infrastructure

Introduction to layered security

- Identifying key features of a secure infrastructure
- Distinguishing between enterprise and host-based security

Assessing security technologies

- Applying Windows Server 2008 enhancements
- Leveraging Windows Server 2008 server roles

Building a Public Key Infrastructure (PKI)

PKI fundamentals

- Identifying security services provided by a PKI
- Mining key business benefits of certificate services
- Implementing public key encryption

Managing certificates

- Creating and responding to certificate requests
- Controlling certificate issuance with permissions
- Securing Web-based enrolment with HTTPS
- Revoking compromised keys
- Publishing a Certificate Revocation List (CRL)

Storing, archiving and recovering keys

- Exporting certificates and private keys
- Deploying Key Recovery Agent accounts
- Maintaining secure key escrow
- Providing secure storage for private keys

Leveraging Multifactor Authentication

Extending authentication solutions

- Installing domain support for multifactor authentication
- Testing Kerberos with smart cards and biometrics

Authenticating with smart cards and tokens

- Configuring smart card enrolment stations
- Issuing smart card user certificates
- Implementing a Certificate Hold on misplaced tokens
- Rolling out domain-wide smart card user and computer policies

Credentialing with biometrics

- Surveying available biometric technologies

- Applying biometric authentication in the enterprise
- Accommodating false negatives and minimising false positives
- Controlling access to exemplar databases
- Auditing biometric user enrolment

Deploying a Scalable Data Protection Model

Identifying confidentiality solutions

- Specifying information security requirements
- Analysing data protection technologies
- Matching native solutions to enterprise requirements

Implementing EFS in the enterprise

- Invoking Group Policy to control encryption
- Assuring data access with Recovery Agents
- Recovering lost or damaged keys from escrow
- Selecting approved encryption algorithms in regulatory environments

Assuring BitLocker Data Recovery

- Analysing the business case
- Planning enterprise BitLocker deployments
- Compensating for EFS vulnerabilities
- Maximising data recovery in the event of BitLocker key loss

Implementing Network Access Protection

Maintaining network integrity with NAP

- Integrating health-based decisions with enterprise security
- Tailoring access policies for managed and unmanaged clients
- Controlling access from inside and outside machines

Verifying client health compliance

- Defining comprehensive client compliance policies
- Authenticating health claims with the System Health Validator (SHV)
- Remediating and ensuring ongoing compliance

Enforcing network access restrictions

- Configuring NAP server components
- Limiting network access to conformant machines using DHCP and VPN Quarantine Enforcement Clients (QEC)

Applying Domain and Server Isolation

Isolating high-value servers

- Protecting intellectual property and personal privacy
- Segregating servers with highly sensitive data

Securing Domain Access with IPsec

- Calculating segmentation requirements
- Building domain isolation on AD and Group Policy
- Configuring exception servers for unmanaged computers
- Maximising security while minimising user impact