

Course Code

ET 401

Course Title**Microsoft Windows 2003 Security****Course Duration**

5 Days

Course Outline**Implementing, Managing, and Troubleshooting Security Policies**

Plan security templates based on computer role. Computer roles include SQL Server computer, Microsoft Exchange Server computer, domain controller, Internet Authentication Service (IAS) server, and Internet Information Services (IIS) server.

Configure security templates.

- Configure registry and file system permissions.
- Configure account policies.
- Configure .pol files.
- Configure audit policies.
- Configure user rights assignment.
- Configure security options.
- Configure system services.
- Configure restricted groups.
- Configure event logs.

Deploy security templates.

- Plan the deployment of security templates.
- Deploy security templates by using Active Directory-based Group Policy objects (GPOs).
- Deploy security templates by using command-line tools and scripting.

Troubleshoot security template problems.

- Troubleshoot security templates in a mixed operating system environment.
- Troubleshoot security policy inheritance.
- Troubleshoot removal of security template settings.

Configure additional security based on computer roles. Server computer roles include SQL Server computer, Exchange Server computer, domain controller, Internet Authentication Service (IAS) server, and Internet Information Services (IIS) server. Client computer roles include desktop, portable, and kiosk.

- Plan and configure security settings.
- Plan network zones for computer roles.
- Plan and configure software restriction policies.
- Plan security for infrastructure services. Services include DHCP and DNS.
- Plan and configure auditing and logging for a computer role. Considerations include Windows Events, Internet Information Services (IIS), firewall log files, Netlog, and RAS log files.
- Analyze security configuration. Tools include Microsoft Baseline Security Analyzer (MBSA), the MBSA command-line tool, and Security Configuration and Analysis.

Implementing, Managing, and Troubleshooting Patch Management Infrastructure

Plan the deployment of service packs and hotfixes.

- Evaluate the applicability of service packs and hotfixes.
- Test the compatibility of service packs and hotfixes for existing applications.

- Plan patch deployment environments for both the pilot and production phases.
- Plan the batch deployment of multiple hotfixes.
- Plan rollback strategy.

Assess the current status of service packs and hotfixes. Tools include MBSA and the MBSA command-line tool.

- Assess current patch levels by using the MBSA GUI tool.
- Assess current patch levels by using the MBSA command-line tool with scripted solutions.
- Deploy service packs and hotfixes.
- Deploy service packs and hotfixes on new servers and client computers. Considerations include slipstreaming, custom scripts, and isolated installation or test networks.
- Deploy service packs and hotfixes on existing servers and client computers.

Implementing, Managing, and Troubleshooting Security for Network Communications

Plan IPsec deployment.

- Decide which IPsec mode to use.
- Plan authentication methods for IPsec.
- Test the functionality of existing applications and services.

Configure IPsec policies to secure communication between networks and hosts. Hosts include domain controllers, Internet Web servers, databases, e-mail servers, and client computers.

- Configure IPsec authentication.
- Configure appropriate encryption levels. Considerations include the selection of perfect forward secrecy (PFS) and key lifetimes.
- Configure the appropriate IPsec protocol. Protocols include Authentication Header (AH) and Encapsulating Security Payload (ESP).
- Configure IPsec inbound and outbound filters and filter actions.

Deploy and manage IPsec policies.

- Deploy IPsec policies by using Local policy objects or Group Policy objects (GPOs).
- Deploy IPsec policies by using commands and scripts. Tools include IPsecPol and NetSh.
- Deploy IPsec certificates. Considerations include deployment of certificates and renewing certificates on managed and unmanaged client computers.

Troubleshoot IPsec.

- Monitor IPsec policies by using IP Security Monitor.
- Configure IPsec logging. Considerations include Oakley logs and IPsec driver logging.
- Troubleshoot IPsec across networks. Considerations include network address translation, port filters, protocol filters, firewalls, and routers.
- Troubleshoot IPsec certificates. Considerations include enterprise trust policies and certificate revocation list (CRL) checking.

Plan and implement security for wireless networks.

- Plan the authentication methods for a wireless network.
- Plan the encryption methods for a wireless network.
- Plan wireless access policies.
- Configure wireless encryption.

- Install and configure wireless support for client computers.

Deploy, manage, and configure SSL certificates, including uses for HTTPS, LDAPS, and wireless networks. Considerations include renewing certificates and obtaining self-issued certificates instead of publicly issued certificates.

- Obtain self-issued certificates and publicly issued certificates.
- Install certificates for SSL.
- Renew certificates.
- Configure SSL to secure communication channels. Communication channels include client computer to Web server, Web server to SQL Server computer, client computer to Active Directory domain controller, and e-mail server to client computer.

Configure security for remote access users.

- Configure authentication for secure remote access. Authentication types include PAP, CHAP, MS-CHAP, MS-CHAP v2, EAP-MD5, EAP-TLS, and multifactor authentication that combines smart cards and EAP.
- Configure and troubleshoot virtual private network (VPN) protocols. Considerations include Internet service provider (ISP), client operating system, network address translation devices, Routing and Remote Access servers, and firewall servers.
- Manage client configuration for remote access security. Tools include remote access policy and the Connection Manager Administration Kit.

Planning, Configuring, and Troubleshooting Authentication, Authorization, and PKI

Plan and configure authentication.

- Plan, configure, and troubleshoot trust relationships.
- Plan and configure authentication protocols.
- Plan and configure multifactor authentication.
- Plan and configure authentication for Web users.
- Plan and configure delegated authentication.
- Plan group structure.
- Decide which types of groups to use.
- Plan security group scope.
- Plan nested group structure.

Plan and configure authorization.

- Configure access control lists (ACLs).
- Plan and troubleshoot the assignment of user rights.
- Plan requirements for digital signatures.
- Install, manage, and configure Certificate Services.
- Install and configure root, intermediate, and issuing certification authorities (CAs).

Considerations include renewals and hierarchy.

- Configure certificate templates.
- Configure, manage, and troubleshoot the publication of certificate revocation lists (CRLs).
- Configure archival and recovery of keys.
- Deploy and revoke certificates to users, computers, and CAs.
- Backup and restore the CA.

Introduction to Designing Security

The following topics are covered in this module:

- Introduction to Designing Security for Microsoft Networks
- Contoso Pharmaceuticals: A Case Study

Creating a Plan for Network Security

The following topics are covered in this module:

- Introduction to Security Policies
- Defining a Process for Designing Network Security
- Creating a Security Design Team

Identifying Threats to Network Security

The following topics are covered in this module:

- Introduction to Security Threats
- Predicting Threats to Security

Analyzing Security

The following topics are covered in this module:

- RisksIntroduction to Risk Management
- Creating a Risk Management Plan

Creating a Security Design for Physical Resources

The following topics are covered in this module:

- Determining Threats and Analyzing Risks to Physical Resources
- Designing Security for Physical Resources

Creating a Security Design for Computers

The following topics are covered in this module:

- Determine threats and analyze risks to computers.
- Design security for computers.

Creating a Security Design for Accounts

The following topics are covered in this module:

- Determine threats and analyze risks to accounts.
- Design security for accounts.

Creating a Security Design for Authentication

The following topics are covered in this module:

- Determining Threats and Analyzing Risks to Authentication
- Designing Security for Authentication

Price

15,500 Baht