COURSE TECHNOLOGY
CENGAGE Learning™

Hands-On Microsoft Windows Server 2008

Chapter 10

Securing Windows Server 2008

Objectives

- Understand the security enhancements included in Windows Server 2008
- Understand how Windows Server 2008 uses group policies
- Understand and configure security policies
- Implement Active Directory Rights Management Services
- Manage security using the Security Templates and Security Configuration and Analysis snap-ins

Objectives (continued)

- Configure security policies for client computers
- Use the *cipher* command for encryption
- Use BitLocker Drive Encryption
- Configure Network Address Translation
- Configure Windows Firewall
- Implement Network Access Protection

Security Enhancements in Windows Server 2008

- Windows Server 2008 was created to emphasize security
  - Reduced attack surface of the kernel through Server Core
  - Expanded group policy
  - Windows Firewall
  - Network Access Protection
  - Security Configuration Wizard
  - User Account Control
  - BitLocker Drive Encryption

Security Enhancements in Windows Server 2008 (continued)

- Server Core is a good solution for a Web or other server in the demilitarized zone of a network
- **Demilitarized zone (DMZ)**
  - A portion of a network that is between two networks, such as between a private network and the Internet
- New group policy categories include:
  - Power management
  - Assigning printers by location
  - Delegation of printer driver installation
  - Security settings
  - Internet Explorer settings

Security Enhancements in Windows Server 2008 (continued)

- Group policy is a way to bring consistent security and other management to Windows Server 2008
  - And to clients connecting to a server
- User Account Control (UAC)
  - Designed to keep the user running in the standard user mode as a way to:
    - More fully insulate the kernel
    - Keep operating system and desktop files stabilized
- BitLocker Drive Encryption
  - Prevents an intruder from bypassing ACL file and folder protections

Introduction to Group Policy

- **Group policy** in Windows Server 2008
  - Enables you to standardize the working environment of clients and servers by setting policies in Active Director
- Defining characteristics of group policy:
  - Group policy can be set for a site, domain, OU, or local computer
  - Group policy cannot be set for non-OU folder containers
  - Group policy settings are stored in group policy objects

Introduction to Group Policy (continued)

- Defining characteristics of group policy: (continued)
  - GPOs can be local and nonlocal
  - Group policy can be set up to affect user accounts and computers
  - When group policy is updated, old policies are removed or updated for all clients

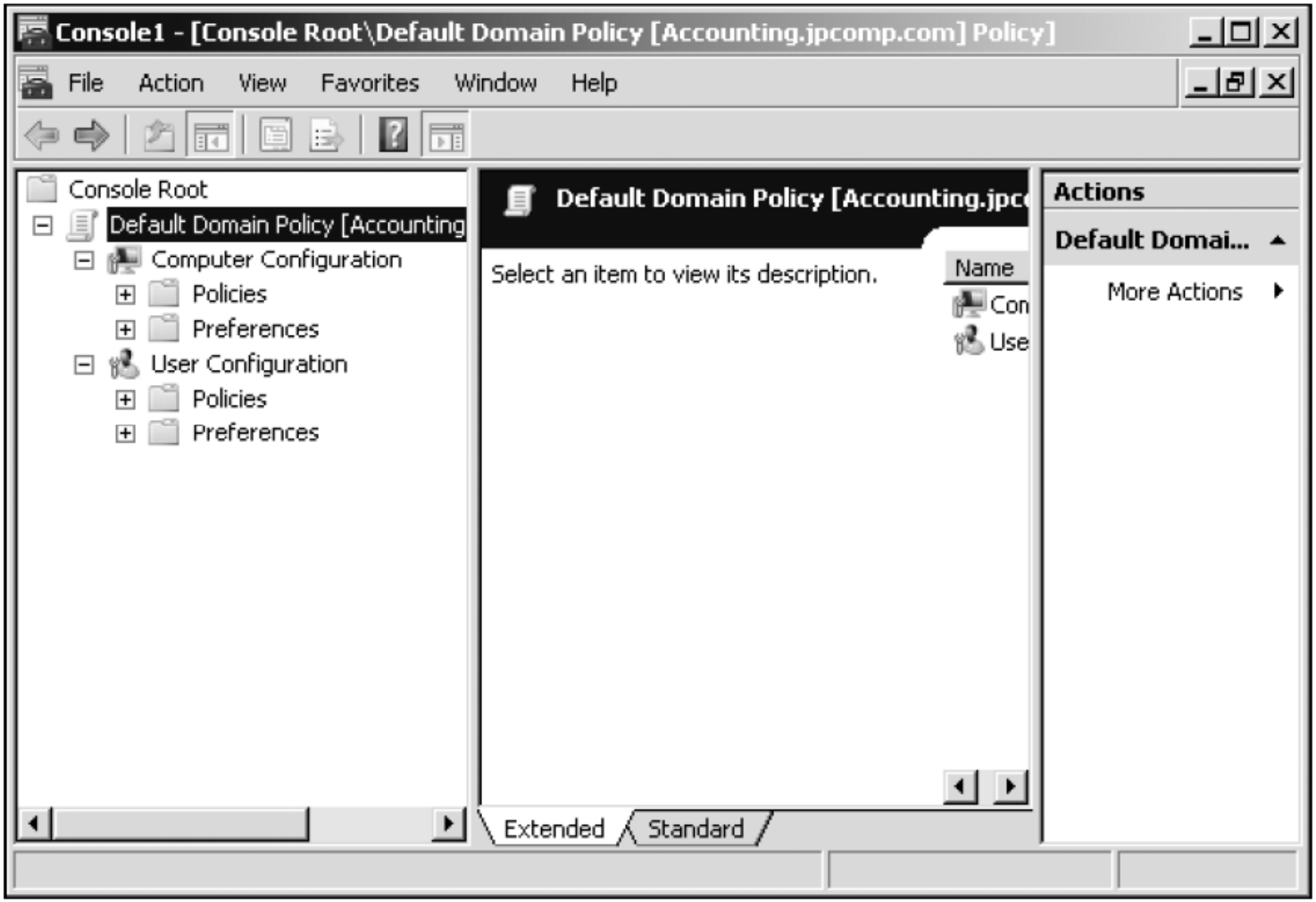

Figure 10-1 Default domain policy

Securing Windows Server 2008 Using Security Policies

- Security policies are a subset of individual policies
  - Within a larger group policy for a site, domain, OU, or local computer
- Security policies include:
  - Account Policies
  - Audit Policy
  - User Rights
  - Security Options
  - IP Security Policies

Securing Windows Server 2008 Using Security Policies (continued)

- Activity 10-1: Using the Group Policy Management Snap-In
  - Time Required: Approximately 10 minutes
  - Objective: Learn how to use the Group Policy Management MMC snap-in

Establishing Account Policies

- Account policies
  - Security measures set up in a group policy that applies to all accounts or to all accounts in a container when Active Directory is installed
- Password security
  - One option is to set a password expiration period, requiring users to change passwords at regular intervals
  - Some organizations require that all passwords have a minimum length

Establishing Account Policies (continued)

- Specific password security options:
  - Enforce password history
  - Maximum password age
  - Minimum password age
  - Minimum password length
  - Passwords must meet complexity requirements
  - Store password using reversible encryption

Establishing Account Policies (continued)

- Activity 10-2: Configuring Password Security
  - Time Required: Approximately 10 minutes
  - Objective: Configure the password security in the default domain security policy

Account Lockout

- The operating system can employ account lockout
  - To bar access to an account (including the true account owner) after a number of unsuccessful tries
- The lockout can be set to release after a specified period of time
  - Or by intervention from the server administrator
- A common policy is to have lockout go into effect after five to 10 unsuccessful logon attempts

Account Lockout (continued)

- Account lockout parameters
  - Account lockout duration
  - Account lockout threshold
  - Reset account lockout count after

Account Lockout (continued)

- Activity 10-3: Configuring Account Lockout Policy
  - Time Required: Approximately 10 minutes
  - Objective: Configure account lockout policy in the default domain security policy

Account Lockout (continued)

- **Kerberos** security
  - Involves the use of tickets that are exchanged between the client who requests logon and network services access
    - And the server or Active Directory that grants access
- Enhancements on Windows Server 2008 and Windows Vista
  - The use of Advanced Encryption Standard (AES) encryption
  - When Active Directory is installed, the account policies enable Kerberos

Account Lockout (continued)

- Options available for configuring Kerberos:
  - Enforce user logon restrictions
  - Maximum lifetime for service ticket
  - Maximum lifetime for user ticket
  - Maximum lifetime for user ticket renewal
  - Maximum tolerance for computer clock synchronization

Account Lockout (continued)

- Activity 10-4: Configuring Kerberos Security
  - Time Required: Approximately 10 minutes
  - Objective: Configure Kerberos in the default domain security policy

Establishing Audit Policies

- Examples of events that an organization can audit are as follows:
  - Account logon (and logoff) events
  - Account management
  - Directory service access
  - Logon (and logoff) events at the local computer
  - Object access
  - Policy change
  - Privilege use
  - Process tracking
  - System events

Establishing Audit Policies (continued)

- Activity 10-5: Configuring Auditing
  - Time Required: Approximately 10 minutes
  - Objective: Configure an audit policy

Configuring User Rights

- User rights enable an account or group to perform predefined tasks
  - The most basic right is the ability to access a server
  - More advanced rights give privileges to create accounts and manage server functions

Configuring User Rights (continued)

- Some examples of privileges include the following:
  - Add workstations to domain
  - Back up files and directories
  - Change the system time
  - Create permanent shared objects
  - Generate security audits
  - Load and unload device drivers
  - Perform volume maintenance tasks
  - Shut down the system

Configuring User Rights (continued)

- Examples of logon rights are as follows:
  - Access this computer from the network
  - Allow logon locally
  - Allow logon through Terminal Services
  - Deny access to this computer from the network
  - Deny logon as a service
  - Deny logon locally
  - Deny logon through Terminal Services

Configuring User Rights (continued)

- Activity 10-6: Configuring User Rights
  - Time Required: Approximately 15 minutes
  - Objective: Learn how to configure user rights

Configuring Security Options

- Over 78 specialized security options, with many new ones added for Windows Server 2008
  - Can be configured in the security policies
- Each category has specialized options

Configuring Security Options (continued)

- Activity 10-7: Configuring Security Options
  - Time Required: Approximately 10 minutes
  - Objective: Examine the Security Options and configure an option

Using IP Security Policies

- Windows Server 2008 supports the implementation of IP security (IPsec)
- When an IPsec communication begins between two computers
  - The computers first exchange certificates to authenticate the receiver and sender
- Next, data is encrypted at the NIC of the sending computer as it is formatted into an IP packet
- IPsec can provide security for all TCP/IP-based application and communications protocols

Using IP Security Policies (continued)

- A computer that is configured to use IPsec communication can function in any of three roles:
  - Client (Respond Only)
  - Secure Server (Require Security)
  - Server (Request Security)
- IPsec security policies can be established through the Default Domain Policy
- IPsec security policies can also be configured through the IP Security Policies Management MMC snap-in

Using IP Security Policies (continued)

- Activity 10-8: Configuring IPsec in the Default Domain Policy
  - Time Required: Approximately 10 minutes
  - Objective: Configure IPsec group policy elements

Active Directory Rights Management Services

- **Active Directory Rights Management Services (AD RMS)**
  - A server role to complement the client applications that can take advantage of Rights Management Services safeguards
- **Rights Management Services (RMS)**
  - Security rights developed by Microsoft to provide security for documents, spreadsheets, e-mail, and other types of files created by applications
  - Uses security capabilities such as encryption, user authentication, and security certificates to help safeguard information

Active Directory Rights Management Services (continued)

- General steps used in RMS security
  - A user creates a Word document, for example
  - In the process of protecting the document with RMS, Word encrypts the document using an AES key and an additional RSA key
  - The AD RMS server issues an identity license to the client who can access the document
  - Client shows the AD RMS server its license to access the document
  - The AD RMS server authenticates the client and determines the level of access

Managing Security Using the Security Templates and Security and Configuration Analysis Snap-Ins

- This snap-in enables you to set up security to govern the following:
  - Account policies
  - Local policies
  - Event log tracking policies
  - Group restrictions
  - Service access security
  - Registry security
  - File system security

Managing Security Using the Security Templates and Security and Configuration Analysis Snap-Ins (continued)

- Activity 10-9: Using the Security Templates Snap-In
  - Time Required: Approximately 15 minutes
  - Objective: Learn to use the Security Templates Snap-In

Managing Security Using the Security Templates and Security and Configuration Analysis Snap-Ins (continued)

- Activity 10-10: Using the Security Configuration and Analysis Snap-In
  - Time Required: Approximately 20 minutes
  - Objective: Explore the features of the Security Configuration and Analysis snap-in

Configuring Client Security Using Policies in Windows Server 2008

- Customizing settings used by clients offers several advantages
  - Enhanced security and providing a consistent working environment in an organization
- The settings are customized by configuring policies on the Windows Server 2008 servers that the clients access
  - When the client logs on to the server or the network, the policies are applied to the client

Manually Configuring Policies for Clients

- You can manually configure one or more policies that apply to clients
  - By using the Group Policy Object Editor snap-in
  - Or by using a customized snap-in, such as the Default Domain Policy console

Manually Configuring Policies for Clients (continued)

- Activity 10-11: Configuring Policies to Apply to Clients
  - Time Required: Approximately 10 minutes
  - Objective: Learn how to configure a group policy to apply to Windows Server 2008 clients

Publishing and Assigning Software

- **Publishing applications** (or software)
  - Involves setting up software through a group policy so that the application is available for users to install from a central application distribution server
    - Such as through the Add/Remove Programs capability via the user's desktop
- **Assigning applications**
  - An application is automatically represented on the user's desktop
  - Is initially really a link to the central application distribution server

Publishing and Assigning Software (continued)

- Activity 10-12: Configuring Software Installation
  - Time Required: Approximately 5 minutes
  - Objective: Learn where to set up software installation in a group policy

Resultant Set of Policy

- **Resultant Set of Policy (RSoP)**
  - Used to make the implementation and troubleshooting of group policies much simpler for an administrator
  - Can query the existing policies that are in place and then provide reports and the results of policy changes
- RSoP supports two modes: planning and logging

Resultant Set of Policy (continued)

- Activity 10-13: Using the Resultant Set of Policy Tool
  - Time Required: Approximately 10 minutes
  - Objective: Learn how to use the Resultant Set of Policy tool

Using the *cipher* Command

- When you deploy NTFS you can use the Encrypt attribute to protect folders and files
  - Enabling only the user who encrypts the folder or file to read it
- You can set the Encrypt attribute on a folder or file through working with that folder's or file's properties
  - Another option that you learn in this section is to use the *cipher* command from the Command Prompt window

Using the *cipher* Command (continued)

Table 10-2 Common *cipher* command-line parameters

Parameter	Description
/?	Lists the *cipher* commands
/e	Encrypts the specified folder so any files added to the folder are encrypted
/d	Decrypts the contents of the specified folder and sets the folder so that any files added to the folder are not encrypted
/s	Applies other *cipher* options used with the /s option to the contents of the current folder and the contents of subfolders under it
/h	Enables you to view which folders and files use the hidden or system attributes
/k	Provides the account employing *cipher* with a new encryption key, meaning that previous keys associated with other accounts are no longer valid—use with extreme caution
/n	With the */u* option, ensures that encryption keys are not modified, but that you can view the currently encrypted folders and files
/u	Updates the *cipher* user's encryption key
/r	Invokes a recovery agent key so that the server administrator can set up a recovery policy
/w	Purges data from disk space that is flagged as unused (but which still contains data that could be recovered)
/x	Copies encryption key and certificate data to a file that is encrypted for use by the *cipher* user

Using the *cipher* Command (continued)

- Activity 10-14: Using the *cipher* Command
  - Time Required: Approximately 10 minutes
  - Objective: Use the cipher command in the Command Prompt window

Using BitLocker Drive Encryption

- **BitLocker Drive Encryption**
  - A relatively new security measure for protecting hard drives
  - Uses Trusted Platform Module for one approach to security
- **Trusted Platform Module (TPM)**
  - A security specification for a hardware device that can be used to secure information on a different hardware device, such as a hard drive

Using BitLocker Drive Encryption (continued)

- When used to protect a hard drive
  - TPM verifies that the computer to which the hard drive is connected has authority to access that hard drive
- If a computer is not equipped with a TPM chip
  - BitLocker Drive Encryption can be used with a USB flash drive that contains a personal identification number (PIN)
- BitLocker Drive Encryption encrypts the entire drive, including the operating system, programs, and data files

Using BitLocker Drive Encryption (continued)

- Activity 10-15: Installing BitLocker Drive Encryption
  - Time Required: Approximately 10 minutes
  - Objective: Set up BitLocker Drive Encryption

Configuring NAT

- Network Address Translation (NAT) serves two important functions:
  - Enables an organization to automatically assign its own IP addresses on an internal network
    - Without having to set up many globally unique addresses for use over external networks
  - Protects computers on an internal network so that computers on external networks cannot identify their true IP addresses on the internal network

Configuring NAT (continued)

- NAT uses a pool of private addresses for its internal network
- Because the internal addresses are not viewed by the outside world
  - There is no need to have a large pool of IP addresses that can also be used over an external network
- Only one or a very small pool of globally unique IP addresses are needed for outside communications
- NAT is also a good security technique because internal IP addresses are concealed from the outside world

Configuring NAT (continued)

- Activity 10-16: Configuring NAT
  - Time Required: Approximately 10 minutes
  - Objective: Configure NAT for the VPN you set up in Chapter 9

Windows Firewall

- The Windows Firewall used in Windows Server 2008
  - The same firewall technology first implemented in Windows XP with Service Pack 2 and Windows Server 2003 with Service Pack 1
- Improvements
  - Protects incoming and outgoing communications
  - Merges firewall filters with IPsec settings
  - Includes the Windows Firewall with Advanced Security MMC snap-in
  - Has firewall exceptions or rules for several kinds of managed objects

Windows Firewall (continued)

- Exceptions are programs that you choose to allow through the firewall in both directions
- When considered as a group, the exceptions are a set of rules
- Exceptions can be configured for the following:
  - TCP and UDP ports
  - All or only specified ports
  - IPv4 and IPv6
  - All or only specified network interfaces
  - Services by providing the path to the service

Windows Firewall (continued)

- Activity 10-17: Configuring Windows Firewall via Control Panel
  - Time Required: Approximately 10 minutes
  - Objective: Configure Windows Firewall from Control Panel

Windows Firewall (continued)

- Activity 10-18: Configuring Windows Firewall Using the Snap-In
  - Time Required: Approximately 10 minutes
  - Objective: Use the Windows Firewall with Advanced Security MMC snap-in

Network Access Protection

- NAP can be used to keep a network healthy in the following ways:
  - Identifies clients and other computers on a network that do not comply with the security policies set through Windows Server 2008
  - Limits access by noncompliant computers
  - Automatically updates or configures a noncompliant computer to match the security policies required for access
  - Continuously checks throughout the entire network and server connection session to ensure that computers remain in compliance

Network Access Protection (continued)

- NAP can be used to ensure compliance with network security policies in the following areas:
  - IPsec
  - VPN
  - DHCP
  - Terminal Services Gateway
  - 802.1X

IPsec

- Through IPsec, NAP allows computers that are considered noncompliant to access the local network
- In conjunction with NAP, IPsec ensures that noncompliant computers are ignored by computers that are compliant
- To determine compliance, NAP uses a server that is a **Health Registration Authority (HRA)**
- The HRA server is configured through a Network Policy Server

VPN

- NAP works through a VPN by enforcing the remote access policy configured for the VPN
- The client attempts to connect, the client is checked against the remote access policy configured in the NPS server
  - And if the client properly verifies, the client is granted access

DHCP

- DHCP has always been a vulnerable protocol
  - Because it is basically simple and comes without much security
- When configured with NAP, DHCP relies on the HRA server to determine the health status of a client
- If the client is fully compliant, DHCP issues the following:
  - IP address
  - Subnet mask
  - DNS IP address information
  - Gateway IP address information

DHCP (continued)

- If the client is noncompliant, DHCP issues only the following:
  - IP address
  - Subnet mask
- If a remediation server is present on the network
  - DHCP issues to the noncompliant computer the IP address of the remediation server
- **Remediation server**
  - One that can provide updates and security policy changes to the client to bring that client into compliance

TS Gateway

- TS Gateway combined with NAP uses the HRA server to ensure that a client is compliant with the health and security policies on a network
- TS Gateway does not enable communications with a remediation server
  - So that a noncompliant client can be updated
- If a computer is noncompliant, it cannot gain full network access through TS Gateway

802.1X

- **802.1X**
  - A wired and wireless authentication approach offered by the IEEE
- When 802.1X is enabled, the network port through which communications occur allows unauthenticated communications
  - Only until a client has been verified as NAP compliant
- When implemented through NAP, 802.1X authentication uses the HRA server to determine compliance

802.1X (continued)

- Activity 10-19: Using Network Policy Server to Configure NAP
  - Time Required: Approximately 10 minutes
  - Objective: Learn about using Network Policy Server for NAP configuration

Summary

- Windows Server 2008 has many new or enhanced security features
- Group policy offers a way to standardize security across a domain, OU, site, or local server
- Configure account policies to include security features such as password security, account lockout, and Kerberos authentication
- Use audit policies to track how resources are accessed, such as folders, files, or user accounts
- User rights policies enable you to create specific security controls

Summary (continued)

- Security options are specialized policies
- Configure IPsec security policy for strong client authentication
- Implement Active Directory Rights Management Services for application-level security
- Use Resultant Set of Policy to plan and troubleshoot group policy settings
- The *cipher* command is a valuable tool for implementing the Encrypting File System from the Command Prompt window

Summary (continued)

- BitLocker Drive Encryption is a security measure for protecting entire hard drives
- Network Address Translation is used to disguise IP addresses on an internal network from the outside world
- Windows Firewall can be configured to allow traffic exceptions and to manage incoming and outgoing traffic
- Network Access Protection is designed to keep a network healthy