Chaffey College
Chino Information Technology Center

CISNTWK-11

Microsoft Network Server

Chapter 3

Configuring the Windows Server 2008 Environment

Chaffey College
Chino Information Technology Center

Objectives

- Use Server Manager and ServerManagerCmd.exe to manage a server
- Install and remove server roles
- Configure server hardware
- Configure the operating system

Objectives (continued)

- Understand and configure the Registry
- Use the Security Configuration Wizard to harden a server
- Install and use Windows PowerShell

Using Server Manager

- Server Manager
  - Consolidates administrative functions to make a server easier to manage
- Roles Summary feature
  - Displays log information to alert you to warnings or problems

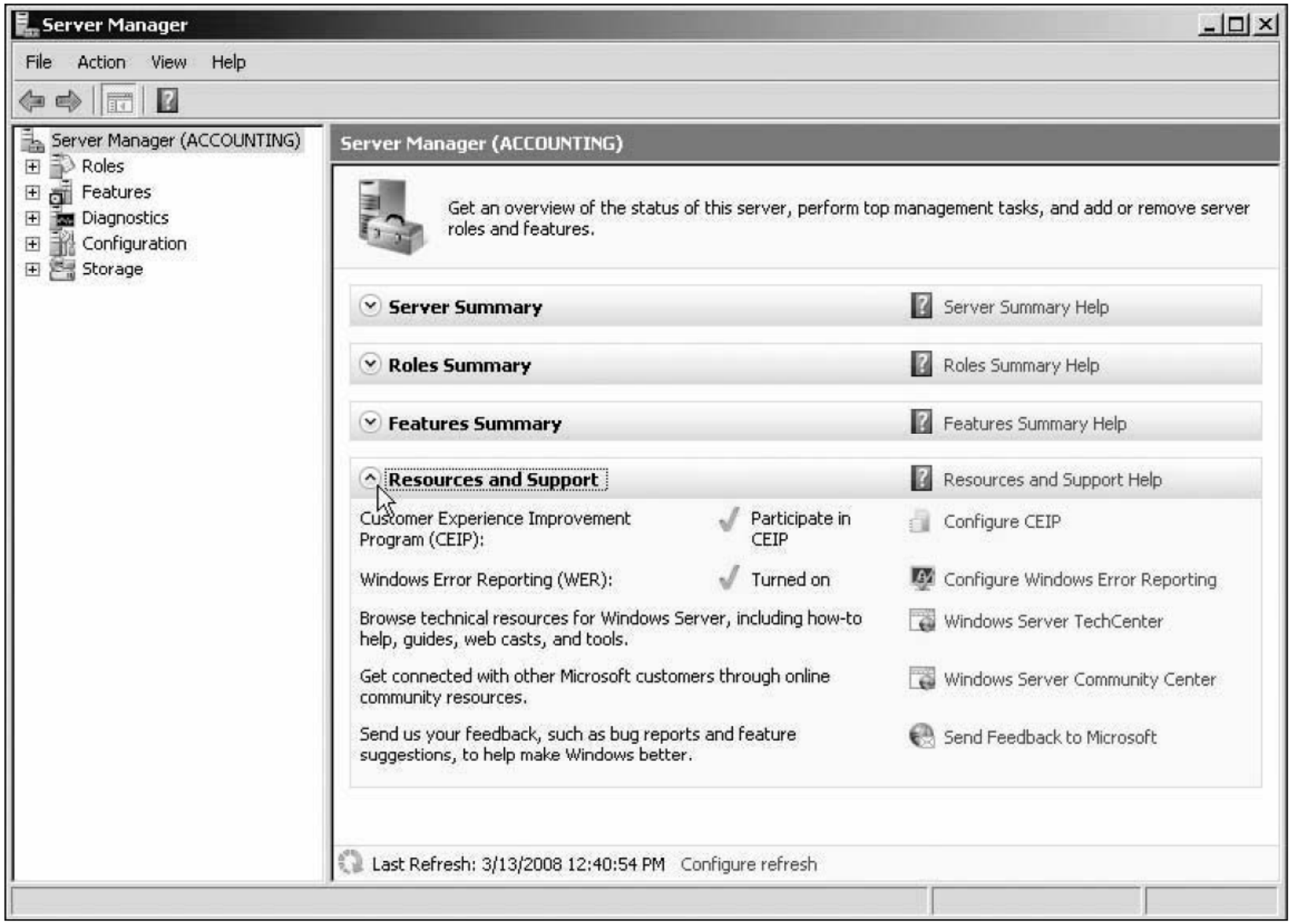

Figure 3-1 Server Manager window

Using Server Manager (continued)

- Activity 3-1: Getting to Know Server Manager
  - Time Required: Approximately 15 minutes
  - Objective: Learn how to start and use Server Manager

Installing and Removing Server Roles

- Two common roles for a Windows Server 2008 server
  - File Services role
    - Focuses on sharing files from the server or using the server to coordinate and simplify file sharing through Distributed File System (DFS)
  - Print Services role
    - Used to manage network printing services and it can offer one or more network printers connected to the network through the server itself

Installing and Removing Server Roles (continued)

- Activity 3-2: Installing and Removing Two Server Roles
  - Time Required: Approximately 20 minutes
  - Objective: Install and then remove the File Services and Print Services roles in Windows Server 2008

Using ServerManagerCmd.exe

- ServerManagerCmd.exe
  - Command-line tool for managing server roles
  - Can be used to manage features that are to be added or removed
- Management activities
  - Install a role or feature
  - Remove a role or feature
  - Query to determine what roles and features are installed

Using ServerManagerCmd.exe (continued)

- Management activities (continued)
  - Use the *whatif* option to determine which features and services will be installed by a specific role, before actually installing that role
  - Restart the computer after installing or removing a role or feature
  - Specify particular features or services to install with a role
  - Use an XML-based answer file to have ServerManagerCmd.exe install or remove server roles

Table 3-1 ServerManagerCmd.exe options

Option	Description
-install <ID>	Installs a server role or feature that is specified by the ID of the role
-remove <ID>	Removes a server role that is specified via the role ID
-query <file.xml>	Displays a list of the roles and features that can be installed and indicates those that are installed already, plus the results can optionally be saved in an XML file
-inputPath <answer.xml>	Uses the contents of an XML file to determine which roles and features to install or remove
-restart	Restarts the computer after a role has been installed or removed (used with the *-install* or *-remove* option; also, use only if it is necessary to restart the computer following action on a specific role or feature)
-allSubFeatures	Installs all of the services and features associated with a specific role (used with the *-install* option)
-setting	Configures a particular installation setting (used with the *-install* option)
-help or *-?*	Displays help documentation for ServerManagerCmd.exe

Using ServerManagerCmd.exe (continued)

Table 3-2 Major IDs for server roles

ID	Server role
Application-Server	Application Server
DHCP	DHCP Server
NPAS	Network Policy and Access Services
Print-Server	Print Services
Terminal-Services	Terminal Services
Web-Server	Web Server (IIS)

Using ServerManagerCmd.exe (continued)

- Activity 3-3: Running ServerManagerCmd.exe
  - Time Required: Approximately 10 minutes
  - Objective: Use the ServerManagerCmd.exe command to install and query server roles

Configuring Server Hardware Devices

- Hardware devices can include the following:
  - Disk drives
  - Disk controllers
  - Network adapters
  - CD/DVD drives
  - Keyboard
  - Pointing devices
  - Monitor

Plug and Play

- **Plug and Play (PnP)**
  - The ability to automatically detect and configure newly installed hardware devices
- For this capability to work, PnP must be:
  - Built into the device
  - Enabled in the target computer's BIOS
  - Built into the computer operating system kernel
- PnP eliminates hours of time that server administrators and computer users once spent installing and configuring hardware

Using Control Panel and the Add Hardware Wizard

- The Add Hardware Wizard is used for the following tasks:
  - Invoke the operating system to use PnP to detect new hardware
  - Install new non-PnP hardware and hardware drivers
  - Troubleshoot problems you might be having with existing hardware
- The Add Hardware Wizard is started from Control Panel
- Windows Server 2008 provides two Control Panel view options: Control Panel Home and Classic View

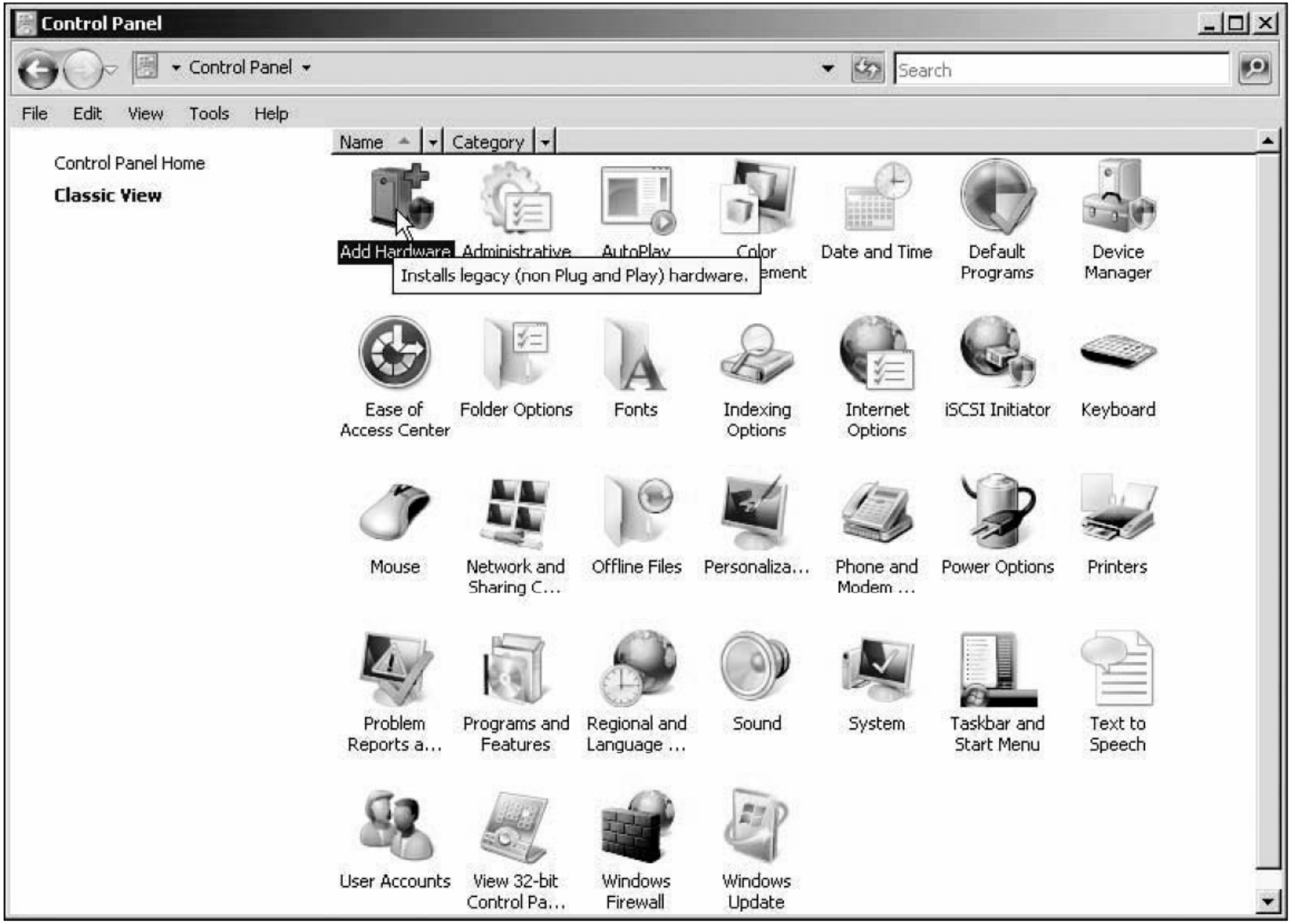

Figure 3-4 Selecting the Add Hardware applet to start the Add Hardware Wizard

Using Control Panel and the Add Hardware Wizard (continued)

- Device Manager
  - Used to check for a resource conflict and to examine other properties associated with a device
  - Provides a graphical view of all hardware currently installed on your computer
  - Can also be used to:
    - Verify if hardware installed is working properly
    - Update device drivers
    - Disable a device
    - Uninstall a device
    - Configure the settings for a device

Using Control Panel and the Add Hardware Wizard (continued)

- Activity 3-4: Resolving a Resource Conflict
  - Time Required: Approximately 10 minutes
  - Objective: Use Device Manager to resolve a resource conflict

Using Control Panel and the Add Hardware Wizard (continued)

- Driver signing
  - When a driver is verified, a unique digital signature is incorporated into it
  - When Windows Server 2008 determines that a device driver is not signed, it gives you a warning
  - Device drivers that are unsigned cannot be loaded in x64 versions of Windows Server 2008
- Use the System File Checker
  - To scan system files for integrity

Using Control Panel and the Add Hardware Wizard (continued)

- You can run this utility to:
  - Scan all system files to verify integrity
  - Scan and replace files as needed
  - Scan only certain files
- The System File Checker can be manually run from the Command Prompt window

Using Control Panel and the Add Hardware Wizard (continued)

- Activity 3-5: Manually Running the System File Checker
  - Time Required: Approximately 5 minutes to learn about the command options and 10–30 minutes to run the test
  - Objective: Use the System File Checker to verify system files

Using Control Panel and the Add Hardware Wizard (continued)

- Using Sigverif to verify system and critical files
  - **Sigverif** verifies system and critical files to determine if they have a signature
    - Only scans files and does not overwrite inappropriate files, enabling you to use the tool while users are logged on
  - After the scan is complete, the results are written to a log file, called sigverif.txt

Using Control Panel and the Add Hardware Wizard (continued)

- Activity 3-6: Verifying Critical Files for a Signature
  - Time Required: Approximately 15 minutes
  - Objective: Use Sigverif to find unsigned files

Configuring the Operating System

- After the operating system has been installed
  - It can be configured to optimize performance and meet very specific requirements

Configuring Performance Options

- Configuring processor scheduling and Data Execution Prevention
  - Processor scheduling
    - Allows you to configure how processor resources are allocated to programs
  - **Data Execution Prevention (DEP)**
    - Monitors how programs use memory to ensure they are not causing memory problems

Configuring Performance Options (continued)

- Activity 3-7: Configuring Processor Scheduling and DEP
  - Time Required: Approximately 10 minutes
  - Objective: Learn where to set up processor scheduling and system memory protection

Configuring Performance Options (continued)

- Configuring virtual memory
  - **Virtual memory**
    - Disk storage used to expand the capacity of the physical RAM installed in the computer
  - Virtual memory works through a technique called **paging**
    - Whereby blocks of information, called pages, are moved from RAM into virtual memory on disk
  - The area of disk that is allocated for this purpose is called the **paging file**

Configuring Performance Options (continued)

- Tips for placement of the paging file:
  - Server performance is better if the paging file is not placed on the boot partition
  - If there are multiple disks, performance can be improved by placing a paging file on each disk
  - In a mirrored set or volume, place the paging file on the main disk
  - Do not place the paging file on a stripe set, striped volume, stripe set with parity, or RAID-5 volume

Configuring Performance Options (continued)

- Activity 3-8: Configuring the Paging File
  - Time Required: Approximately 5 minutes
  - Objective: Learn where to configure the initial and maximum size of the paging file

Configuring Performance Options (continued)

- Configuring direct memory access for hard disks
  - Hard drives transfer modes:
    - Program Input/Output (PIO)
      - Uses CPU memory registers and RAM during the process of transferring data for disk reads and writes
    - Direct Memory Access (DMA)
      - Bypasses the use of CPU memory and writes to and reads directly from RAM
      - Which makes it much faster than PIO
  - Windows Server 2008 configures IDE/ATA/SATA drives to use the DMA transfer mode by default

Configuring Performance Options (continued)

- Activity 3-9: Configuring the DMA Transfer Mode
  - Time Required: Approximately 5 minutes
  - Objective: Determine the transfer mode used by a hard drive and set it to DMA, if necessary

Configuring Environment Variables

- Environment variables
  - Used to tell the operating system where to find certain programs and how to allocate memory to programs, and to control different programs
- **System environment variables**
  - Defined by the operating system and apply to any user logged onto the computer
- **User environment variables**
  - Can be defined on a per-user basis, such as specifying the path where application files are stored

Configuring Environment Variables (continued)

- Activity 3-10: Configuring System and Environment Variables
  - Time Required: Approximately 5 minutes
  - Objective: Learn where to configure system and user environment variables

Configuring Startup and Recovery

- You can configure the following system startup options:
  - Which operating system to boot by default, if more than one operating system is installed
  - How long to display a list of operating systems from which to boot
  - How long to display a list of recovery options, if the computer needs to go into recovery mode after a system failure

Configuring Startup and Recovery (continued)

- In the event of a system failure, you can configure these options:
  - Writing information to the system log (hard configured so you cannot change this)
  - Whether to start automatically after a system failure
  - How and where to write debugging information

Configuring Startup and Recovery (continued)

- Activity 3-11: Configuring Startup and Recovery
  - Time Required: Approximately 5 minutes
  - Objective: Configure startup and recovery options

Configuring Power Options

- The Power Options that you can set are as follows:
  - Select a power plan
  - Require a password on wakeup
  - Choose what the power button does
  - Create a power plan
  - Choose when to turn off the display
- Three power plans are already created: balanced, power saver, and high performance
- The option to create a power plan enables you to customize a power plan

Configuring Power Options (continued)

- Activity 3-12: Configuring Power Options
  - Time Required: Approximately 5 minutes
  - Objective: Configure the balanced power plan

Installing a Protocol

- You might need to add other protocols to customize the server for your network
- **Microsoft Virtual Network Switch Protocol**
  - Used when the Hyper-V role is installed in Windows Server 2008
  - Enables the use of a software virtual switch between the main operating system and the operating systems on virtual partitions
  - Reduces the overhead in network communications when Hyper-V is installed

Installing a Protocol (continued)

- **Reliable Multicast Protocol**
  - Used for multimedia transmissions
  - Runs on top of IP and simplifies multicast communications
    - Because multicasting can be done even without routers to direct network traffic

Installing a Protocol (continued)

- Activity 3-13: Installing a Protocol
  - Time Required: Approximately 10 minutes
  - Objective: Learn to install a protocol

Understanding the Windows Server 2008 Registry

- Windows Server 2008 Registry
  - A very complex database containing all information the operating system needs about the entire server
  - The Registry is the coordinating center for a specific server
- Data contained in the Registry include:
  - Information about all hardware components
  - Information about Windows Server 2008 services that are installed
  - Data about user profiles and Windows Server 2008 group policies

Understanding the Windows Server 2008 Registry (continued)

- Data contained in the Registry include: (continued)
  - Data on the last current and last known setup used to boot the computer
  - Configuration information about all software in use
  - Software licensing information
  - Server Manager and Control Panel parameter configurations
- The Registry Editor is launched from the Start button Run option as either regedt32 or regedit

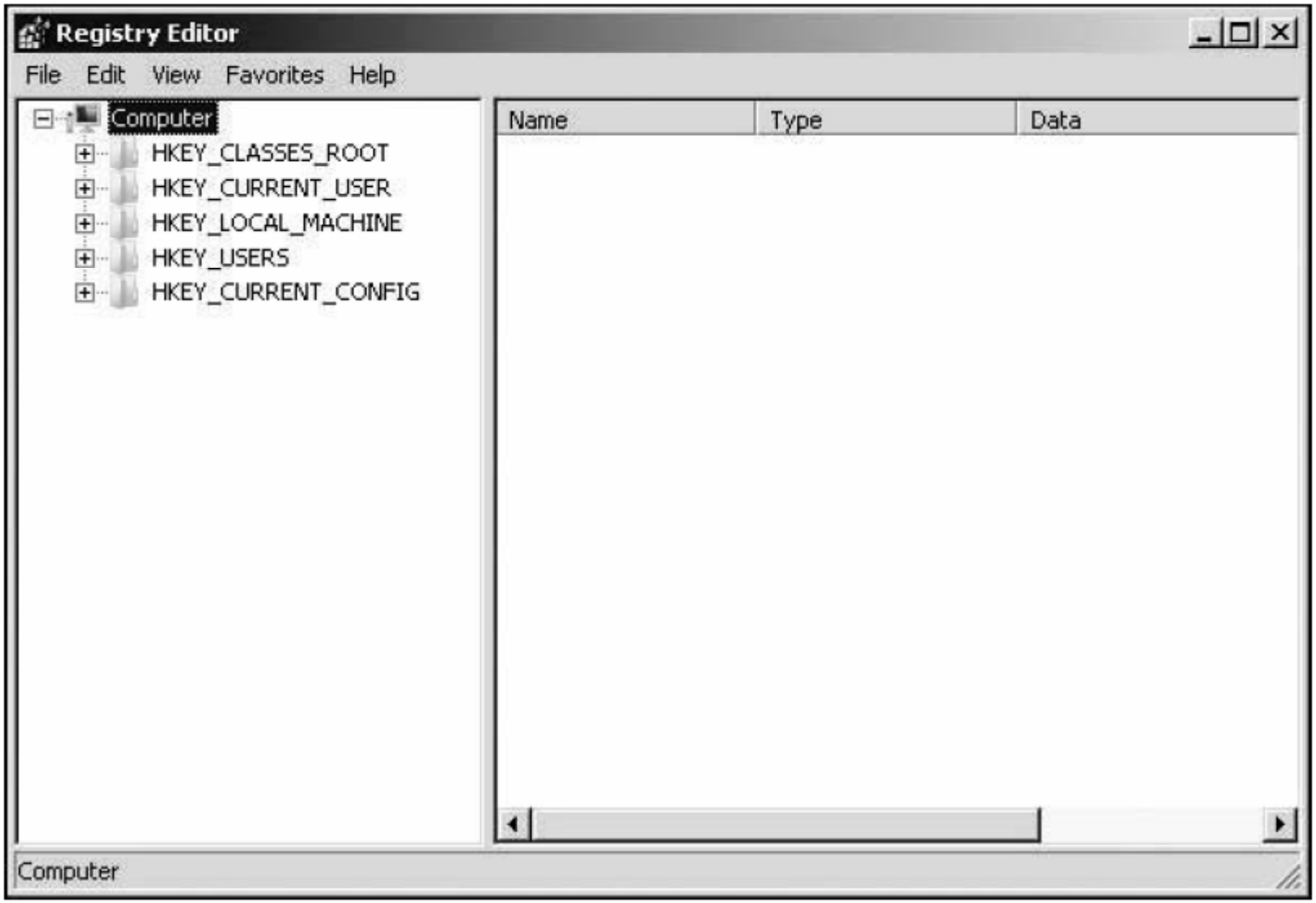

Figure 3-15 Registry Editor

Understanding the Windows Server 2008 Registry (continued)

- Precautions when working with the Registry:
  - Establish a specific group of administrators who have privileges to open and modify the Registry
  - Only make changes to the Registry as a last resort
  - Regularly back up the Registry as part of backing up the Windows Server 2008 Windows folder
  - Never copy the Registry from one Windows-based system over the Registry of a different system

Registry Contents

- The Registry is hierarchical in structure
  - Made up of keys, subkeys, and entries
- **Registry key**
  - A category or division of information within the Registry
- **Registry subkeys**
  - A single key may contain one or more lower-level keys
- **Registry entry**
  - A data parameter associated with a software or hardware characteristic under a key (or subkey)

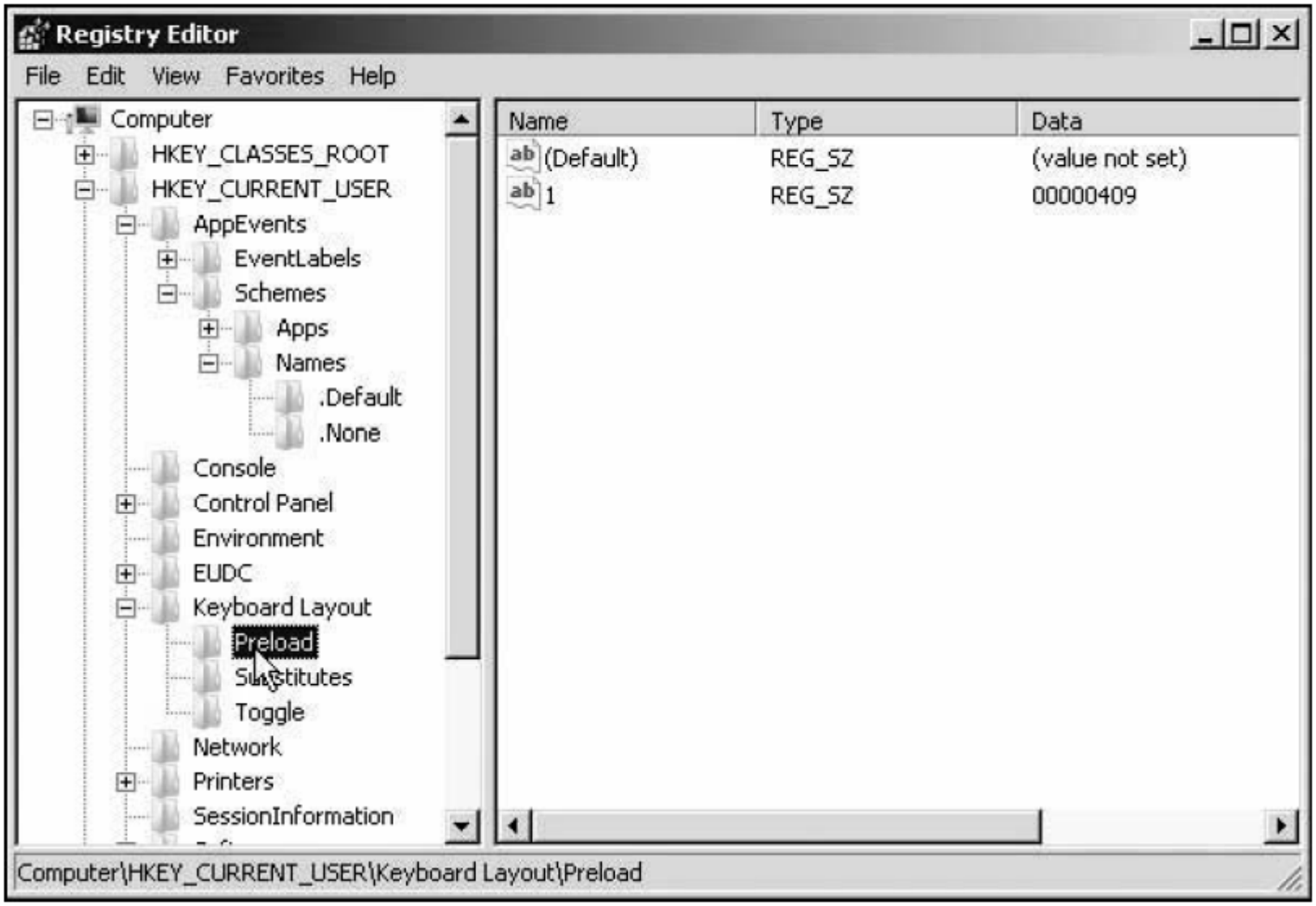

Figure 3-16 Registry's hierarchical structure

HKEY_LOCAL_MACHINE

- HKEY_LOCAL_ MACHINE root key
  - Contains information on every hardware component in the server
  - Including information about what drivers are loaded and their version levels, what IRQ lines are used, setup configurations, the BIOS version, and more
- A few subkeys are stored as a set, called **hives**, because they hold related information

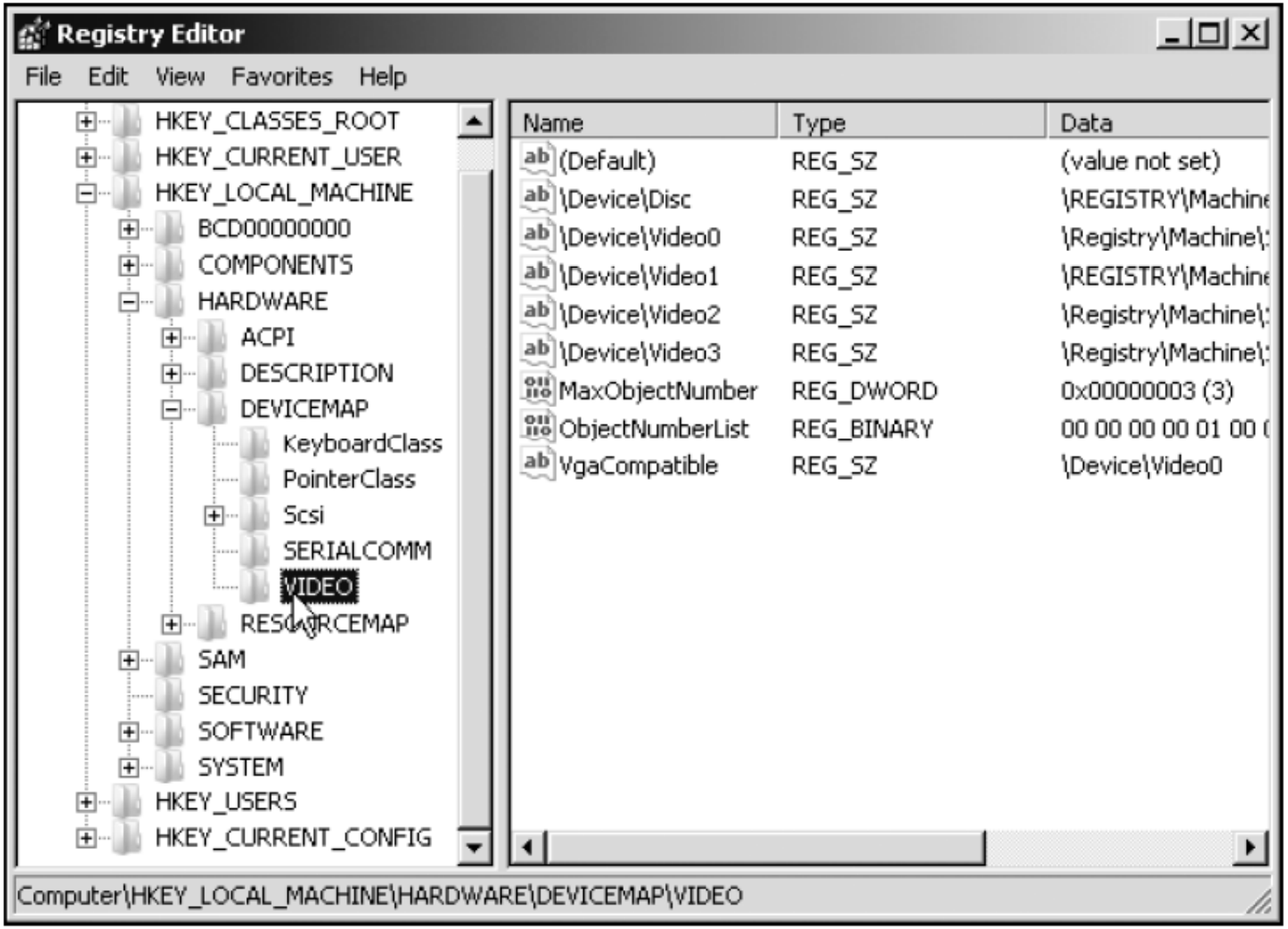

Figure 3-17 The HKEY_LOCAL_MACHINE root key

HKEY_CURRENT_USER

- HKEY_CURRENT_USER key
  - Contains information about the desktop setup for the account presently logged on to the server console
- HKEY_USERS key
  - Contains profile settings for all users who have logged onto the server

HKEY_USERS

- HKEY_USERS root key
  - Contains profile information for each user who has logged onto the computer
  - Each profile is listed under this root key

HKEY_CLASSES_ROOT

- HKEY_CLASSES_ROOT key
  - Holds data to associate file extensions with programs
- Associations exist for executable files, text files, graphics files, Clipboard files, audio files, and many more
  - These associations are used as defaults for all users who log on to Windows Server 2008

HKEY_CURRENT_CONFIG

- HKEY_CURRENT_CONFIG root key
  - Has information about the current hardware profile
  - Holds information about the monitor type, keyboard, mouse, and other hardware characteristics for the current profile

HKEY_CURRENT_CONFIG (continued)

- Activity 3-14: Using the Registry Editor
  - Time Required: Approximately 10 minutes
  - Objective: Practice using the Registry Editor to view the Registry contents

Using the Security Configuration Wizard

- **Security Configuration Wizard (SCW)**
  - Steps you through analyzing and configuring security settings on a server
- SCW examines the roles a server plays
  - And then tries to adjust security to match these roles

Using the Security Configuration Wizard (continued)

- Through the SCW, you can:
  - Disable unnecessary services and software
  - Close network communication ports and other communication resources that aren't in use
  - Examine shared files and folders to help manage network access through access protocols
  - Configure firewall rules

Using the Security Configuration Wizard (continued)

- SCW has three components:
  - GUI interactive wizard
  - Database
  - Command-line tool called *scwcmd*
- The Security Configuration Database (SCD) is a group of XML files that establish a security policy

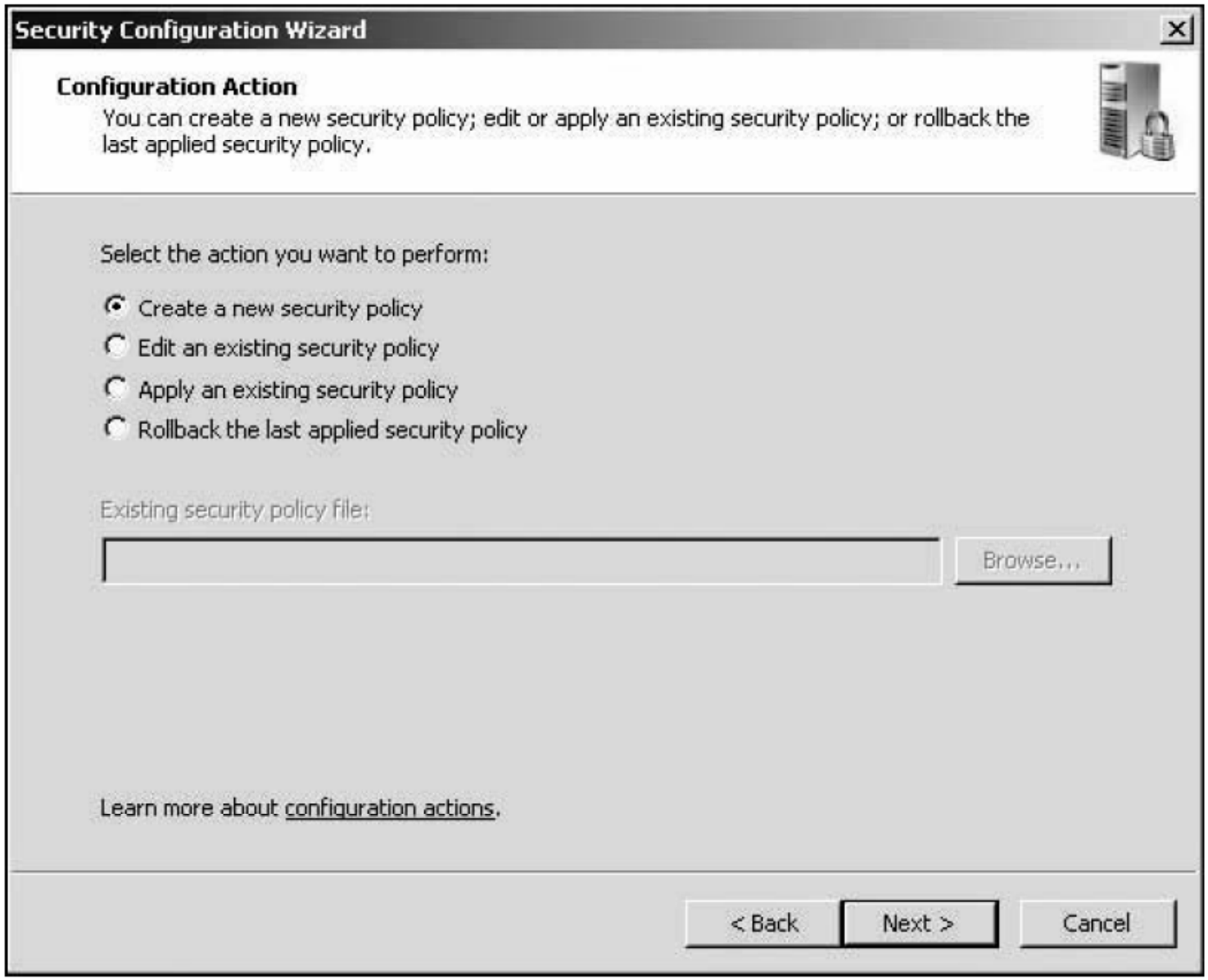

Figure 3-18 Creating a new security policy

Using the Security Configuration Wizard (continued)

Table 3-3 *scwcmd* command-line options

Option	Description
analyze	Analyzes current security settings in the SCD
configure	Configures security settings and writes them to the SCD
register	Registers new SCD extensions
rollback	Rolls back security settings to the previously configured settings
transform	Converts the XML security settings in the SCD into a Group Policy Object (GPO) usable in Active Directory
view	Enables you to view the current security settings in the SCD

Using the Security Configuration Wizard (continued)

- Activity 3-15: Using SCW to Configure a Security Policy
  - Time Required: Approximately 20–30 minutes
  - Objective: Create a new security policy
- Activity 3-16: Using *scwcmd*
  - Time Required: Approximately 30 minutes
  - Objective: View security policy settings using the *scwcmd* command-line command

Windows PowerShell

- Windows PowerShell is a command-line interface or shell
- A shell is a customized environment for executing commands and scripts
- A script is a file of commands that is run when you run the script
  - cmdlets are specialized commands for completing common tasks in PowerShell

Windows PowerShell (continued)

- Some of the tasks you can complete using Windows PowerShell include the following:
  - Manage files and folders
  - Manage network tasks
  - Manage fixed and removable storage
  - Configure printing services
  - Manage software applications and updates
  - Manage Terminal Services
  - Manage server services and features
  - Manage Web server services
  - Work with the Registry

Windows PowerShell (continued)

- Activity 3-17: Using Windows PowerShell
  - Time Required: Approximately 15 minutes
  - Objective: Use traditional Command Prompt commands and cmdlets in Windows PowerShell

Summary

- Server Manager is a new tool offered in Windows Server 2008
- ServerManagerCmd.exe is a command-line version of Server Manager and has the ability to manage multiple servers
- The Add Hardware Wizard enables the installation of hardware devices not properly detected by PnP
- Device Manager is a tool you can access from Server Manager or Control Panel to manage hardware

Summary (continued)

- The System File Checker and Sigverif are tools for verifying system files
- After Windows Server 2008 is installed, you can tune performance by configuring processor scheduling and memory use, virtual memory, and memory for network performance
- To help protect your system from power problems, configure startup and recovery options as well as power options
- Use Control Panel to install or uninstall protocols

Summary (continued)

- The Registry is a database that is at the foundation of Windows Server 2008
- The Security Configuration Wizard helps you protect Windows Server 2008 from problems caused by attackers and malicious software
- Windows PowerShell is a command-line tool that enables a system administrator to manage a server using commands, cmdlets, and scripts