Exam : **70-298**

Title : Designing Security for a MS Windows Server 2003 Network

Version : Demo

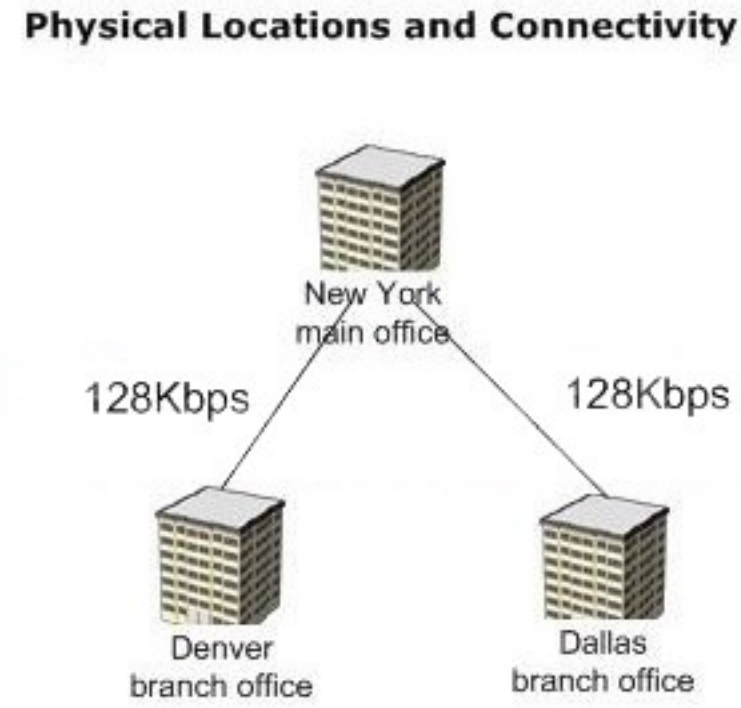
Case 1, Lucerne Publishing

Overview

Lucerne Publishing is an industry leader in publishing technology textbooks, e-books, and magazines.

Physical Locations

The company has three offices, as shown in the Physical Locations and Connectivity exhibit.



The company's main office is in New York, and it has branch offices in Denver and Dallas. The company's employees and departments are distributed as shown in the following table

Office location	Number of employees	Departments
New York	400	Editorial and information technology (IT)
Denver	95	Development
Dallas	80	Production

Business Processes

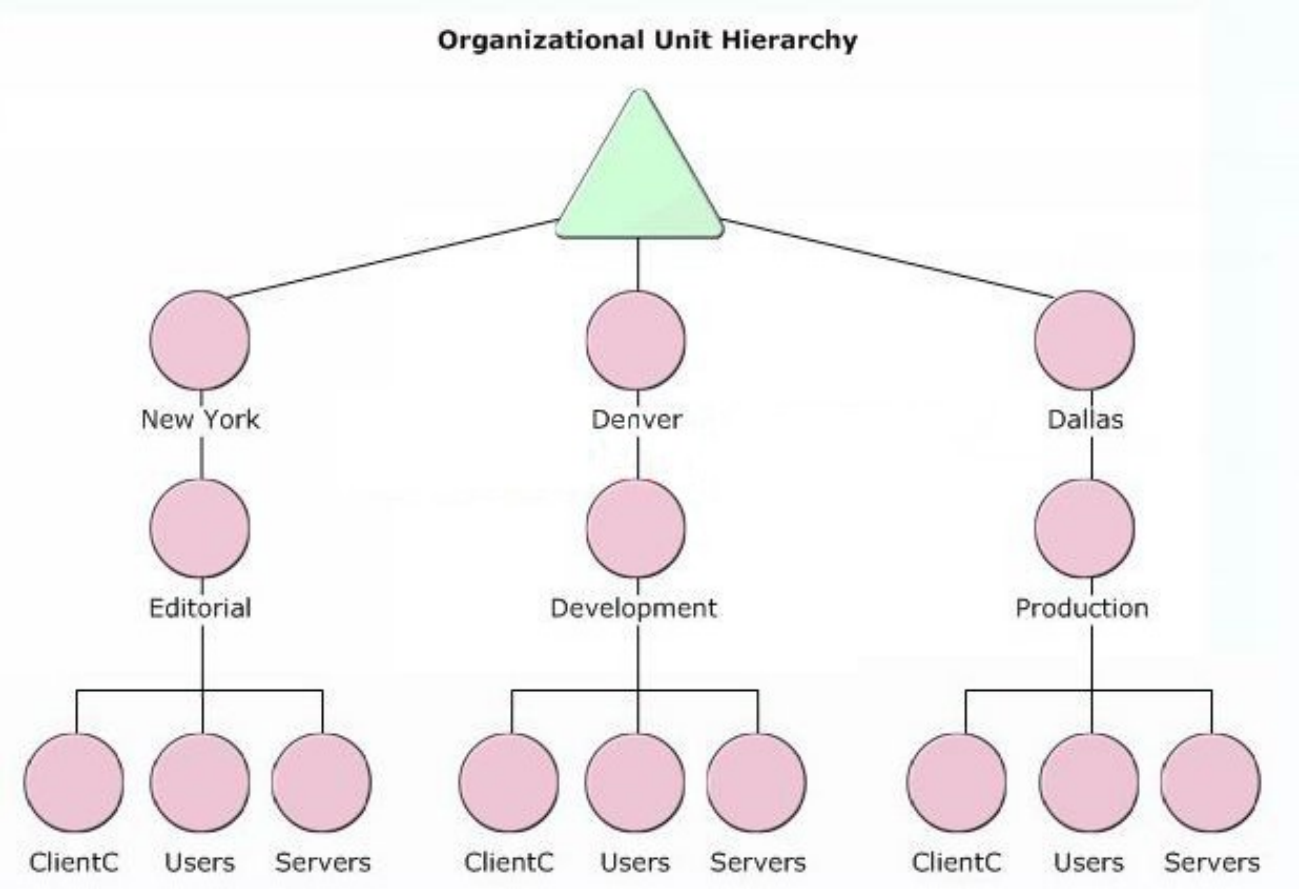
The IT staff in the New York office uses client computers to remotely administer all Lucerne Publishing servers and domain controllers. Employees use their company client computers to access archived published books and archived accounting

information through an internal Web site that runs IIS 6.0.

Directory Services

The company's network consists of a single Active Directory domain named lucernepublishing.com. All servers run Windows Server 2003, Enterprise Edition. Administration of Active Directory is centralized in New York. Denver and Dallas user and computer accounts are located in their respective child OUs, as

shown in the Organizational Unit Hierarchy exhibit.



The NYAdmins, ProductionAdmins, EditorialAdmins, and DevelopmentAdmins global user groups have full control of their respective organizational units (OUs). These global groups are located in their respective OUs.

Network Infrastructure

All client computers run Windows XP Professional.

The domain contains a public key infrastructure (PKI). The company uses an internal subordinate enterprise certification authority (CA) to issue certificates to users and computers. Each branch office has a wireless network that supports desktop and portable client computers. The wireless network infrastructure in each branch office contains an Internet Authentication Service (IAS) server and wireless access points that support IEEE 802.1x, RADIUS, and Wired Equivalent Privacy (WEP).

Problem Statements

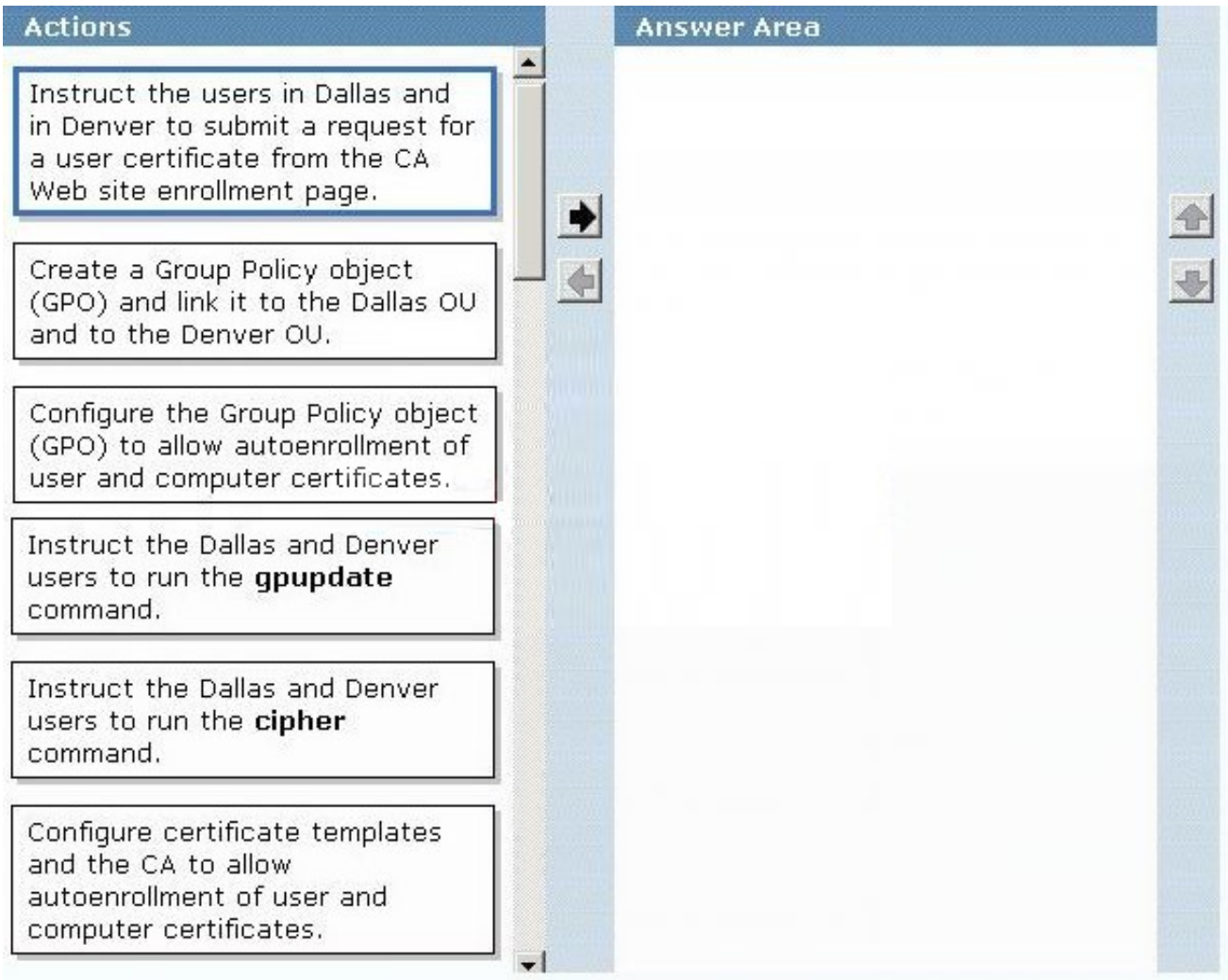
The following business problems must be considered: Members of the EditorialAdmins group and unauthorized users as members to this group. Members of this group must be restricted to only authorized users.

Editors connect to a shared folder named Edits on a member server named Server5. When they attempt to encrypt data located in Edits, they receive an error message stating that they cannot encrypt data. Editors need to encrypt data remotely on Server5.

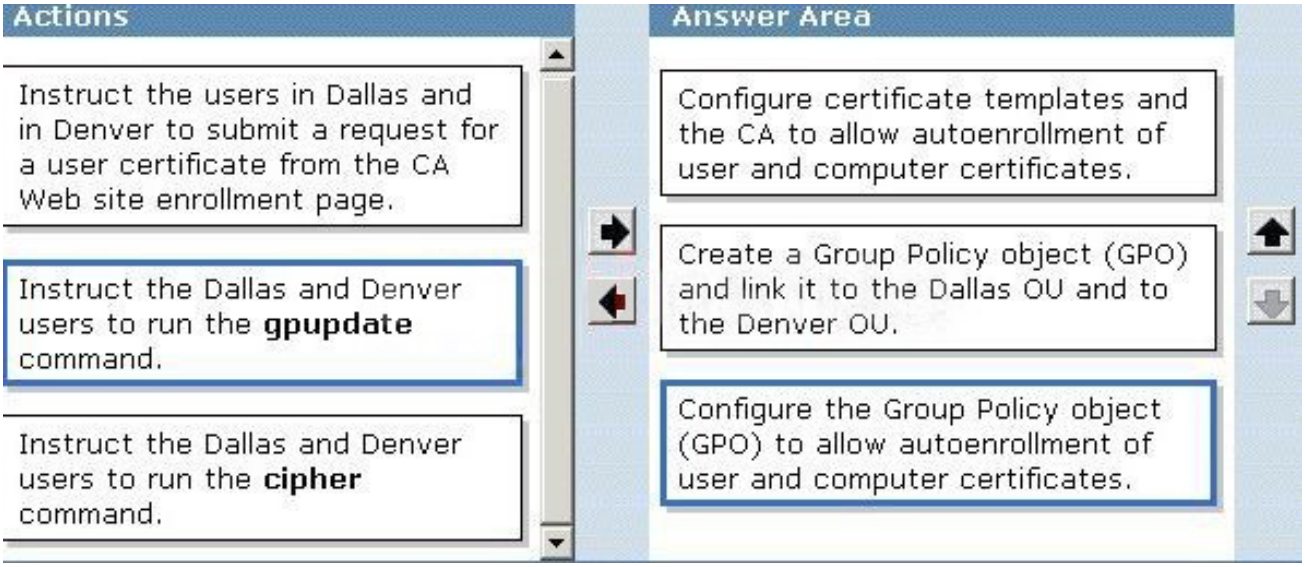
Some users in the Dallas office changed the location of their My Documents folders to shared folders on servers that do not back up their My Documents data. As a result, data was lost. The Dallas My

Documents folders need to be moved to a server that backs up user data. Users in the Dallas office must be prevented from changing the location of their My Documents folder in the future.
Chief Information Officer
Security is Lucerne Publishing's primary concern. We must improve security on client computers, servers, and domain controllers by implementing a secure password policy. For legal reasons, we need a logon message that tells users that access to servers in the development department is restricted to only authorized users.
System Administrator
Each department needs different security patches. We need to test security patches prior to deploying them. After they are tested, the patches need to be deployed automatically to servers in each department. As we deploy the patches, we need to limit the network bandwidth used to obtain security patches.
Chief Security Officer
We need to automatically track when administrators modify user rights on a server or on a domain controller and when they modify local security account manager objects on servers.
We must implement the most secure method for authenticating Denver and Dallas users that access the wireless networks.
We need to protect data as it is sent between the wireless client computers and the wireless access points. Client computers need to automatically obtain wireless network access security settings.
Written Security Policy
The Lucerne Publishing written security policy includes the following requirements.
Passwords must contain at least seven characters and must not contain all or part of the user's account name. Passwords must contain uppercase and lowercase letters and numbers. The minimum password age must be 10 days, and the maximum password age must be 45 days.
Access to data on servers in the production department must be logged.
A standard set of security settings must be deployed to all servers in the development, editorial, and production departments. These settings must be configured and managed from a central location.
Servers in the domain must be routinely examined for missing security patches and service packs and to ascertain if any unnecessary services are running.
Services on domain controllers must be controlled from a central location. Which services start automatically and which administrators have permission to stop and start services must be centrally managed.
The IIS server must be routinely examined for missing IIS Security patches.
Users of the Web site and the files they download must be tracked. This data must be stored in a Microsoft SQL Server database.
Vendors and consultants who use Windows 95 or Windows 98 client computers must have the Active Directory Client Extensions software installed to be able to authenticate to domain controllers on the company's network.

Questions
1. You need to design a certificate distribution method that meets the requirements of the chief security officer.
Your solution must require the minimum amount of user effort. What should you do?
To answer, move the appropriate actions from the list of actions to the answer area, and arrange them in the appropriate order.



Answer:



2. You need to design a method to configure the servers in the development department to meet the requirements of the chief information officer. What should you do?

A. Use error reporting on all servers in the development department to report errors for a custom

application.
B. Configure all servers in the development department so that they do not require the CTRL+ALT+DELETE keys be pressed in order to log on interactively to the server.
C. Create a Group Policy object (GPO) and link it to the development department's Servers OU. Configure the GPO with an interactive logon policy to display a message for users who attempt to log on.
D. Configure the screen saver on all servers in the development department to require a password.
Answer: C

3. You need to design a method to log changes that are made to servers and domain controllers. You also need to track when administrators modify local security account manager objects on servers. What should you do?
A. Enable failure audit for privilege use and object access on all servers and domain controllers.
B. Enable success audit for policy change and account management on all servers and domain controllers.
C. Enable success audit for process tracking and logon events on all servers and domain controllers.
D. Enable failure audit for system events and directory service access on all servers and domain controllers.
Answer: B

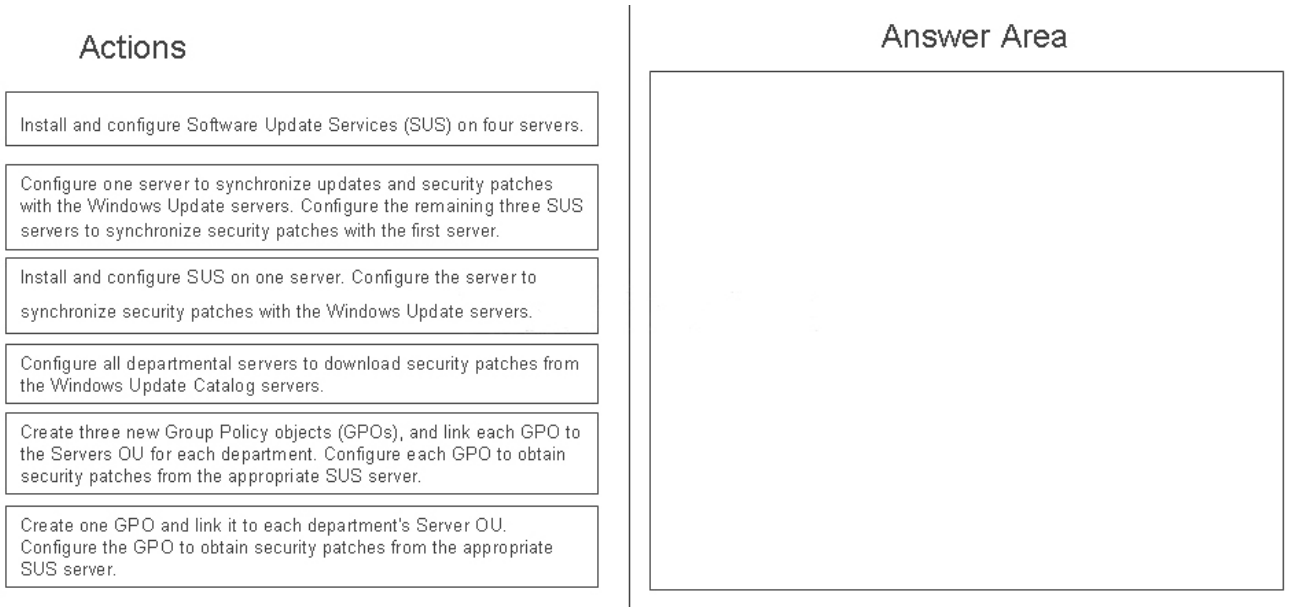
4. You need to design a strategy to ensure that all servers are in compliance with the business requirements for maintaining security patches. What should you do?
A. Log on to a domain controller and run the Resultant Set of Policy wizard in planning mode on the domain.
B. Log on to each server and run Security Configuration and Analysis to analyze the security settings by using a custom security template.
C. Create a logon script to run the secedit command to analyze all servers in the domain.
D. Run the Microsoft Baseline Security Analyzer (MBSA) on a server to scan for Windows vulnerabilities on all servers in the domain.
Answer: D

5. You need to design a method to monitor the security configuration of the IIS server to meet the requirements in the written security policy. What should you do?
A. Log on to a domain controller and run the Resultant Set of Policy wizard in planning mode on the IIS server computer account.
B. Run the Microsoft Baseline Security Analyzer (MBSA) on the IIS server and scan for vulnerabilities in Windows and IIS checks.
C. Run Security Configuration and Analysis to analyze the IIS server's security settings by using a custom security template.
D. On the IIS server, run the gpresult command from a command prompt and analyze the output.
Answer: B

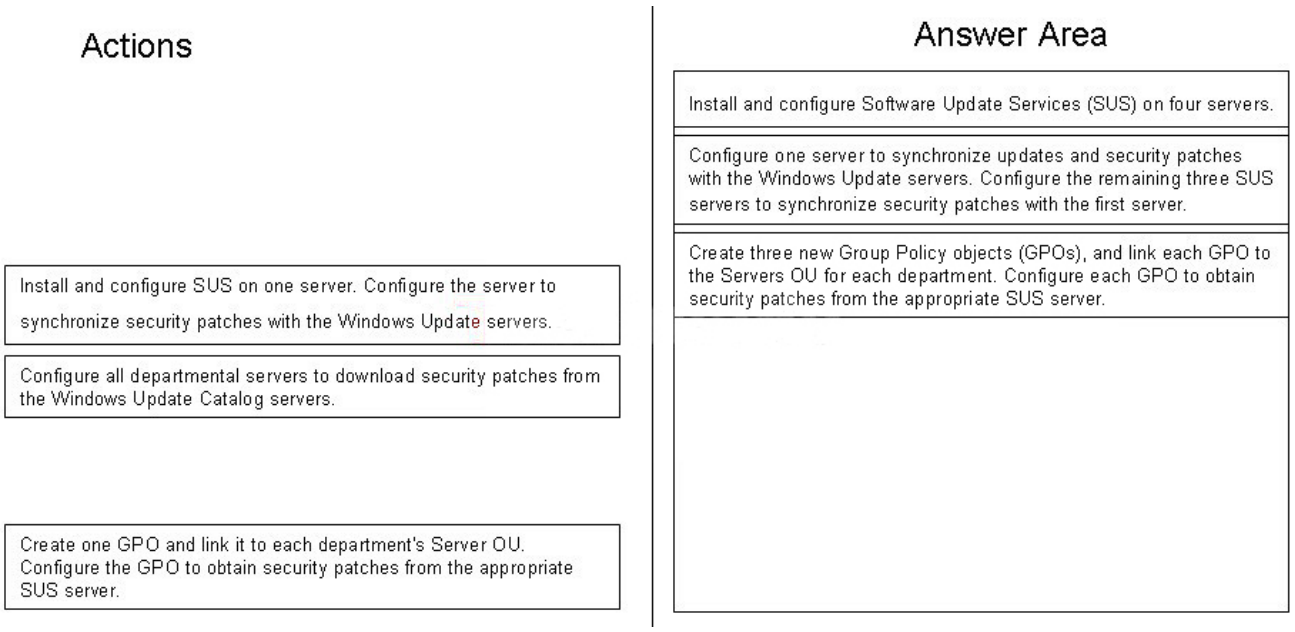
6. You need to design a monitoring strategy to meet business requirements for data on servers in the production department. What should you do?
A. Use Microsoft Baseline Security and Analyzer (MBSA) to scan for Windows vulnerabilities on all

servers in the production department.
B. Run Security and Configuration Analysis to analyze the security settings of all servers in the production department.
C. Enable auditing for data on each server in the production department. Run System Monitor on all servers in the production department to create a counter log that tracks activity for the Objects performance object.
D. Create a Group Policy object (GPO) that enables auditing for object access and link it to the product department's Servers OU. Enable auditing for data on each server in the production department.
Answer: D

7. You need to design a method to deploy security patches that meets the requirements of the systems administrator. What should you do?
To answer, move the appropriate actions from the list of actions to the answer area, and arrange them in the appropriate order. (Use only actions that apply. You might need to reuse actions.)



Answer:



8. You need to design a method to protect traffic on the wireless networks. Your solution must meet the requirements of the chief security officer. What should you do?
A. Configure the wireless access points in Denver and in Dallas to filter unauthorized Media Access Control (MAC) addresses.
B. Configure the wireless network connection properties for all computers in Denver and in Dallas to use the same
network name that the wireless access points use.
C. Create a Group Policy object (GPO) and link it to the Denver OU and to the Dallas OU. Create a wireless network policy and configure it to use Windows to configure wireless network settings for the Denver and the Dallas networks.
D. Create a Group Policy object (GPO) and link it to the Denver OU and to the Dallas OU. Create a wireless network policy and enable data encryption and dynamic key assignment for the Denver and the Dallas networks.
Answer: D

9. You need to design a strategy to log access to the company Web site. What should you do?
A. Enable logging on the company Web site and select the NCSA Common Log File Format. Store the log files on a SQL Server computer.
B. Use System Monitor to create a counter log that captures network traffic to the Web server by using the Web Service object. Store the log files on a SQL Server computer.
C. Run Network Monitor on the Web server. Create a capture filter for the SNA protocol and save the results to a capture file. Store the capture file on a SQL Server computer.
D. Enable logging on the company Web site and select ODBC Logging. Configure the ODBC logging options by using a nonadministrative SQL account.
Answer: D

10. You need to design a method to deploy security configuration settings to servers. What should you do?

A. Run the Resultant Set of Policy wizard with a Windows Management Instrumentation (WMI) filter on each department's Server OU.
B. Log on to each server and use local policy to configure and manage the security settings.
C. Create a custom security template. Log on to a domain controller and run the secedit command to import the security template.
D. Create a custom security template. Create a Group Policy object (GPO) and import the security template. Link the GPO to each department's Server OU.
Answer: D