Exam : 070-299

Title : Implementing and Administering Security in a Microsoft Windows Server 2003 Network

Ver : 11.20.07

QUESTION 1:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
At Certkiller .com there are two Routing and Remote Access servers named Certkiller -SR12 and Certkiller -SR21. There is also an Internet Authentication Services server named Certkiller -SR15. The IAS server is set to provide accounting and centralized authentication of users connecting via Certkiller -SR12 and Certkiller -SR21. There are certain Certkiller .com network users who need to work from home. They will all require 24 hour access 7 days a week.
It is your responsibility to create the appropriate remote access policies for Certkiller .com. To accommodate all the Remote access users you create a remote access policy that is configured to allow the Remote Users group the appropriate access to the VPN. For a while the network operated normally but certain remote users started complaining about not being able to access the VPN. You investigate and discover all the successfully connected users connected using a local user account located on Certkiller -SR15. You need to ensure that remote access is available whilst using the least amount of administrative effort.
What should you do?

A. Check whether Certkiller -SR12 and Certkiller -SR21 are set to support RADIUS accounting and authentication
B. Add Certkiller -SR12 and Certkiller -SR21 to the RAS and IAS Servers group in Active Directory
C. Promote the IAS server Certkiller -SR15 to a domain controller
D. Add Certkiller -SR15 to the RAS and IAS Server group in Active Directory

Answer: D

Explanation: The IAS server requires being able to read all user objects attributes which can be achieved by adding Certkiller -SR15 to the RAS and IAS Servers group in Active Directory.
Incorrect Answers:
A: The scenario states that some users connect successfully. Thus it means that the Routing and Remote Access servers are configured properly.
B: These servers do not require being added to the RAS and IAS Servers group as they do not actually authenticate the user accounts.
C: This option will also achieve the scenario objective but requires too much administrative effort.

QUESTION 2:

You work as the network administrator at Certkiller .com. The Certkiller .com

network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003. Half the client computers are portable computers, and the rest are desktop computers. The client computers are running a mix of Windows 2000 Professional Windows XP Professional.
There are many Certkiller .com Sales department users that work out of the office due to the nature of their job description. These Sales department users require access to resources on Certkiller .com when out of the office. It is your responsibility to provide the Sales department users with access to the network. To this end you have five servers that are running with Routing and Remote Access services configured for VPN connectivity. All these servers are configured with the same remote access policy.
A new written security policy has recently been issued by the Certkiller .com management and consequently you had to reconfigure the policies on each of these servers. Because of the policy changes you received instruction to centralize the remote access policies to ensure that any future changes to the policies can be made once and applied to all remote access servers.
What should you do?

A. A Domain Group Policy to apply any changes should be configured.
B. The Routing and Remote Access servers must be configured to use Internet Authentication Services (IAS).
C. An application directory partition must be implemented.
D. Extensible Authentication Protocol (EAP) should be configured on all the Routing and Remote Access servers.

Answer: B

Explanation: IAS makes use of Remote Authentication Dial-In User Service (RADIUS) to centralize policies, logging, and authentication services from a single location. This would be ideal under the circumstances of ever-changing policy application.
Incorrect answers:
A: Remote policies are not stored in group policies. Thus configuring a Domain Group policy will not centralize the policies.
C: Implementing an application directory partition will not centralize remote access policies. These partitions are used to create a section of the Active Directory database for application specific data to control replication and not for centralization of remote policies.
D: EAP is an authentication protocol and is not used to centralize remote access policies.

QUESTION 3:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and some run Windows 2000 Server and all client computers are laptop computers that run

Windows XP Professional.
At Certkiller .com there are two Routing and Remote Access servers named Certkiller -SR02 and Certkiller -SR05 respectively. The Routing and Remote Access servers are configured to accept connection requests through VPN and dial-up connections. The laptop client computers of the Certkiller .com domain currently make use of the MS-CHAP v2 protocol for authenticating to the network.
A new Certkiller .com written security policy requires centralized remote connection authentications. The policy further states that all remote connections to the Certkiller .com corporate network authenticate using smart cards ensuring the data is encrypted with L2TP with IPSec. To this end you have received instruction from the CIO to comply with the security policy. You thus need to plan a new design for both VPN and dial-up connections.
What should you do?

A. An IAS server and VPN server must be added to the domain.
Certkiller -SR02 and Certkiller -SR05 and the new VPN server must be configured to use the IAS server for authentication and make use of the EAP-TLS protocol for authentication on the IAS server
B. An additional VPN server must be added to the domain.
Certkiller -SR02 and Certkiller -SR05 must be configured to use the new VPN server for authentication and make use of the EAP-TLS protocol for authentication on the VPN server.
C. An additional IAS server and VPN server must be added to the domain.
Certkiller -SR02 and Certkiller -SR05 and the new VPN server must be configured to use the IAS server for authentication and make use of the MS-CHAP v2 protocol for authentication on the IAS server.
D. An additional VPN server must be added to the domain.
Certkiller -SR02 and Certkiller -SR05 must be configured to use the new VPN server for authentication and make use of the MS-CHAP v2 protocol for authentication on the VPN server.

Answer: A

Explanation: In the scenario you are required to use smartcards authentication and this will be achieved by adding the additional IAS server to the domain and configuring your Routing and Remote Access Service servers to use the added IAS server which should be configured to use EAP-TLS for authentication as this protocol supports the use of smartcards.
Incorrect Answers:
B: The problem with this implementation is that the authentication will not be centralized as the scenario state it is imperative authentication is centralized.
C: There is only one problem in this option and that's the use of MS-CHAP v2 as this protocol does not support smartcard authentication.
D: The problem with this implementation is that the authentication will not be centralized as the scenario state it is imperative authentication is centralized.

QUESTION 4:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. Certkiller .com has its headquarters in Chicago and a branch office in Dallas.
You are responsible for the management of the Routing and Remote Access services at Certkiller .com. You enable Routing and Remote Access on a server named Certkiller -SR05. You received a list of telephone numbers of those that are allowed to connect to the Certkiller .com network via remote access together with instruction from the CIO to configure Certkiller -SR05 to accept only connections from those numbers.
You need to configure Certkiller -SR05 to support Automatic Number Identification/Calling Line Identification (ANI/CLI). You then create a user account for each of the phone numbers on the list from which calls will be accepted. You then create a remote access policy to support these ANI/CLI connections. Now you just need to apply the policy.
What should you do?

A. Enable the Unencrypted authentication option on the Authentication tab of the remote access profile for the policy.
B. Enable the Unauthenticated access option on the Authentication tab of the remote access profile for the policy.
C. Enable the Encrypted authentication option on the Authentication tab of the remote access profile for the policy.
D. Enable the MD5-challenge authentication option on the Authentication tab of the remote access profile for the policy.

Answer: B
Explanation
: Because a user name and password are not going to be sent when an ANI/CLI connection is made, you need to allow unauthenticated access. Thus you should enable support for unauthenticated access on the Authentication tab of the remote access policy profile for the policy. Alternative you could also configure the User Identity setting for remote access policies in the registry to direct Certkiller -SR05 or IAS server to use the number from which the user is calling as the user identity.
Incorrect answers:
A: If you enable unencrypted authentication support then you will be allowing support for clients that use the Password Authentication Protocol (PAP) and this is not what is required in this scenario.
C: You enable encrypted authentication support to allow support for clients that use CHAP and MS-CHAP. This is not what is required in this scenario.
D: You do not need to enable support for MD5-challenge authentication.

QUESTION 5:

You work as the network domain administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory forest named Certkiller .com. The Certkiller .com network contains ten Windows Server 2003 Standard Edition computers and 1,200 client computers running Windows XP Professional.
You are responsible for the management of security related settings and computer accounts in the domain. You need to define a custom security template to manage configuration settings for the computers. This custom security template will have to be imported into a Group Policy Object (GPO) that is linked to the domain.
Which of the following Group Policy Object categories' related configuration settings can be managed using a security template? (Choose all that apply.)

A. Account policies
B. Disk Quotas
C. Event Log
D. File System
E. Windows File Protection
F. Local Policies
G. Registry
H. Group Policy
I. Restricted Groups
J. System Services

Answer: A, C, D, F, G, I, J

Explanation: You can make use of a security template to manage the configuration settings for the following categories: Account policies, Event Log, File System, Local Policies, Registry, Restricted Groups, and System Services
Incorrect answers:
B: Disk Quotas management: i.e. defining and setting is done using the System\Disk Quotas portion of Administrative Template.
E: Windows File Protection enabling and management of its cache is done using the System\Windows File Protection portion of Administrative Template.
H: Group Policy is managed using the System\Group Policy portion of Administrative Template

---

QUESTION 6:

You work as the network domain administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory forest named Certkiller .com. The Certkiller .com network contains several Windows Server 2003 Standard Edition computers and 1,500 client computers running Windows XP Professional.
You are responsible for the management of security related settings and computer

accounts in the domain. You need to configure settings that are related to passwords, account lockout, and Kerberos. This custom security template will be imported into a Group Policy Object (GPO) that is linked to the domain. You must thus make use a of a security template node to accomplish the task.
What should you do?

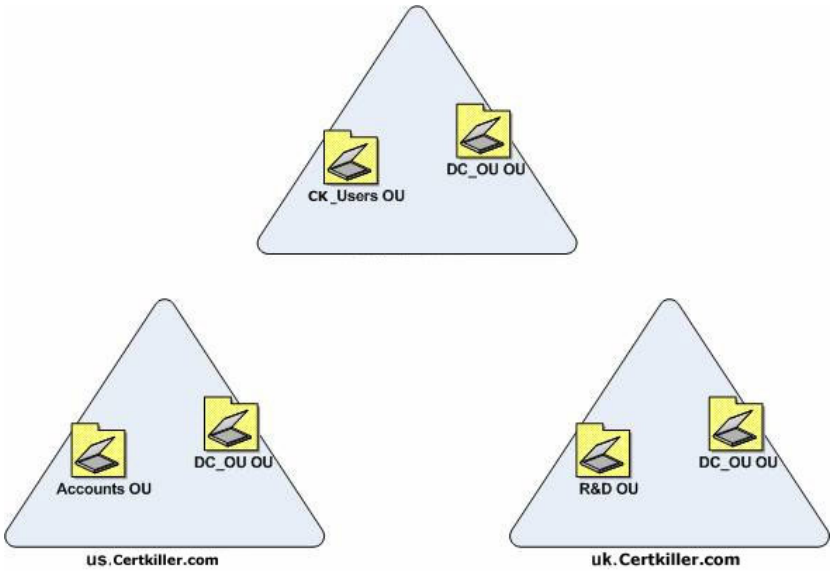
A. Use the Event Log security template node.
B. Use the Local Policies security template node.
C. Use the Account Policies security template node.
D. Use the Restricted Groups security template node.

Answer: C

Explanation: The Account Policies
node of the Security template is used to configure password- account lockout-, and Kerberos settings.
Incorrect answers:
A: The Event Log node is used to configure settings for the application, security and system event logs and not to configure passwords, account lockouts or Kerberos.
B: The Local Policies node is used to configure auditing, user rights and other security-related options and not passwords, accounts lockouts or Kerberos settings.
D: The Restricted Groups node is used to configure and manage the membership for specific security groups.

QUESTION 7:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory forest that contains three domains named Certkiller .com, us. Certkiller .com and, uk. Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com domain and organizational unit (OU) structure is illustrated by the following Exhibit.
Exhibit:



Accounts department employees have user accounts in the us. Certkiller .com domain, Research and Development employees have user accounts in the uk. Certkiller .com domain, and all other users have user accounts in the Certkiller .com domain. Each domain has an OU named DC_OU that only contains the computer accounts of the domain controllers in that particular domain.
A new Certkiller .com security policy requires the following:
1. All Accounting department users must use complex passwords with a minimum length of ten characters.
2. These password restrictions should only affect the Accounting department users.
You thus need to ensure that these requirements are successfully achieved.
What should you do?

A. Create a GPO named PWRestrict.
Link it to the DC_OU OU in the uk. Certkiller .com domain.
B. Create a GPO named PWRestrict.
Link it to the CK_Users OU in the Certkiller .com domain.
C. Create a GPO named PWRestrict.
Link it to the DC_OU OU in the Certkiller .com domain.
D. Modify the appropriate password policy settings in the Default Domain Policy GPO.
E. Create a GPO named PWRestrict.
Link it to the R&D OU in the uk. Certkiller .com domain.
F. Create a GPO named PWRestrict.
Link it to the DC_OU OU in the us. Certkiller .com domain.
G. Create a GPO named PWRestrict.
Link it to the Accounts OU in the us. Certkiller .com domain.

Answer: D

Explanation: Three domain-wide account policy settings (Password Policy, Account Lockout Policy and Kerberos Policy) should be unique to the domain and should always be defined at the domain level. These settings are enforced by the domain

controller computers in the domain, regardless of the container holding the domain controllers or the OU structure in the domain. Therefore, all domain controllers always retrieve the values of these user account policy settings from the Default Domain Policy GPO.
Incorrect Answers:
A, C, F: If you use these options, the settings you have configured will be overridden by those in the Default Domain Policy GPO.
B: Using this option would only apply the settings to users in this OU. Also, the settings you have configured will be overridden by those in the Default Domain Policy GPO.
E: There are no members of the Accounting department added to the RandD OU. This GPO will not affect these users.
G: The password policy settings are enforced on the domain controllers. While settings in a GPO linked at the OU level will apply to users or computers in the container, password policies should always be applied at the domain level so that the policy will be applied to all domain computers.

QUESTION 8:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com with sites All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. All users and computers belong to the Certkiller .com domain.
All file servers reside in an organizational unit (OU) named FileServers. Each file server hosts several shared folders, some of which contain confidential financial data. All domain users have permissions to access the information in the shared folders. You suspect that a domain user account has been used by a hacker to access confidential financial information stored on a file server named Certkiller -SR16.
You need to determine which user account has been compromised.
You plan to use auditing to track which users are logging on to the domain. However, your desire is not to examine large volumes of information to view logon attempts to domain resources. You want to use the least amount of disk space when you audit access to domain resources.
What should you do?

A. Configure a Group Policy Object (GPO) that enables the Logon Events audit policy for failure auditing and success auditing.
Link the GPO to the Active Directory container that contains your domain controllers.
B. Configure a Group Policy Object (GPO) that enables the Logon Events audit policy for success auditing.
Link the GPO to the Active Directory container that contains your domain controllers.
C. Configure a Group Policy Object (GPO) that enables the Account Logon Events audit policy for success auditing.
Link the GPO to the Active Directory container that contains your domain controllers
D. Configure a Group Policy Object (GPO) that enables the Account Logon Events audit policy for failure auditing.

Link the GPO to the Active Directory container that contains your domain controllers.

Answer: C

Explanation: The Account Logon Events policy setting is used to track which users are logging on to your domain. The Account Logon Events policy is enabled on domain controllers. Enabling success auditing will result in an entry being placed in the security log whenever a user makes a successful attempt to log on to the Certkiller .com domain by using a domain user account.
Incorrect Answers
A: The Logon Events audit policy is used to audit logon attempts using local computer accounts. This policy will only log an event when a user logs on to a domain controller.
B: The Logon Events audit policy is used to audit logon attempts using local computer accounts. This policy will only log an event when a user logs on to a domain controller.
D: Enabling failure auditing will result in an entry being placed in the security log whenever a user makes an unsuccessful attempt to log on to the Certkiller .com domain by using a domain user account. You suspect that a domain user account is already being used to access domain resources.

QUESTION 9:

You work as the senior network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
You have noticed that some unauthorized changes have been made to the registry of several computers. You suspect that one of your junior network administrators is changing the registry. You decide to:
1. Enable auditing to log all changes being made to the registry.
2. All attempts made to change the registry keys to be logged.
3. No other type of event to be included in your auditing effort.
4. Use Event Viewer to view all logged event entries.
You open the domain audit security policy and navigate to the audit policy settings under the Security Settings node. You then enable the Audit object access audit policy setting for failed events. When viewing the logged events, you discover though that there are no events logged for any successful changes made to the Registry. You want all events to be logged, and not only failed attempts to change the Registry.
How should you configure the audit policy settings of the domain audit security policy?

A. Configure the Audit privilege use audit policy setting so that successful and failed events are logged.
B. Configure the Audit directory service access audit policy setting so that successful and failed events are logged.
C. Configure the Audit Policy change audit policy setting so that successful and failed events are logged.

D. Configure the Audit object access audit policy setting so that successful and failed events are logged

Answer: D

Explanation: While you have enabled the correct audit policy setting in the Security Settings node, you have specified that only failed attempts to change the Registry be logged. You SHOULD configure the Audit object access setting if you want to track and log when a user accesses operating system components such as files, folders or registry keys. Because you need both successful and failed events logged, you should reconfigure the Audit object access audit policy setting so that both successful and failed events are logged.
Incorrect Answers:
A: You would configure the Audit privilege use audit policy setting to log when a user affects a user right.
B: The Audit directory service access policy audit policy setting logs events that pertain to when users access Active Directory objects which have system access control lists (SACLs). The Registry is not an Active Directory object. You should regard it as being computer specific.
C: The Audit Policy change audit policy setting is used to log changes that are made to the security configuration settings of the computer.

QUESTION 10:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
Clive Wilson is a manager in the Human Resources department. Clive Wilson frequently accesses files that contain confidential information on Certkiller .com's employees. The files reside in several shared folders on his Windows XP Professional computer. Both Dean and employees working in the Human Resources department modify these files.
Clive Wilson complains that this morning, when he attempted to access a file in one of the shared folders, the shared folders and files were deleted. You decide to use last nights backup to restore the files. You successfully restore the latest available backup of these files. You must immediately determine who the culprit is that deleted the files.
You suspect that someone deleted Clive's files from across the network. You log on to Clive Wilson's computer. You want to configure local security policy, so that you can determine who connected to Clive's computer and deleted the files. You want to use Event Viewer to produce a listing of all logged entries.
What should you do? (Choose the two actions which you should perform. Each correct answer presents only part of the complete solution. Choose two answers that apply.)

A. Enable the Privilege Use - Success audit policy on Clive Wilson's computer.
Use Event Viewer to configure a filter that will list all entries produced by the audit policy.
B. Enable the Logon Events - Success audit policy on Clive Wilson's computer.
Use Event Viewer to configure a filter that will list all entries produced by the audit policy.
C. Enable the Account Logon Events - Success audit policy on Clive Wilson's computer.
Use Event Viewer to configure a filter that will list all entries produced by the audit policy.
D. Enable the Object Access - Success audit policy on Clive Wilson's computer.
Use Event Viewer to configure a filter that will list all entries produced by the audit policy.

Answer: A, D

Explanation: The Privilege Use - Success audit policy will allow you to see who deleted the files from Clive Wilson's computer, and also when these files were deleted. The Object Access - Success audit policy will let you know when an individual successfully accessed Clive Wilson's files. You can then use Event Viewer to configure a filter that will list all entries produced by the audit policy.
Incorrect Answers:
C: The Logon Events - Success and Account Logon Events - Success audit policies would not work because the question states that Clive Wilson's files were deleted from over the network. These policies would inform you on who logged on to the local computer, and whether a user account was compromised.
B: The Logon Events - Success and Account Logon Events - Success audit policies would not work because the question states that Clive Wilson's files were deleted from over the network. These policies would inform you on who logged on to the local computer, and whether a user account was compromised.

QUESTION 11:

You work as the network security administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. The Certkiller .com network contains ten Windows Server 2003 computers and 1,200 client computers running Windows XP Professional. Certkiller .com can fall prey to industrial espionage. To this end Internet Protocol Security (IPSec) is implemented on the Certkiller .com network. However, it has come to the CIO's attention that one of the Certkiller .com users has been changing the IPSec policies and that it could be a user that is perhaps employed by a rival company as an industrial spy. You then receive instruction from the CIO to identify the users or users responsible for making these changes to the IPSec policies as well as attempts to make changes. You need to enable an audit policy to accomplish this task.
What should you do?

A. Enable success auditing for the Audit logon events.
B. Enable success auditing for the Audit policy change.
C. Enable success auditing for the Audit privilege use.
D. Enable success and failure auditing for the Audit logon events.
E. Enable success and failure auditing for the Audit policy change.
F. Enable success and failure auditing for the Audit privilege use.

Answer: E

Explanation: In an effort to identify the culprits making changes to the IPSec policies on the Certkiller .com network, you should enable success auditing for the Audit Policy change audit policy. And to identify the user/s attempting to make changes to the IPSec policies on the Certkiller .com network, you should also enable failure auditing for the Audit Policy change audit policy.
Incorrect answers:
A, D: The success and failure auditing of the Audit logon policy will audit each time a user attempts to log on or off as well as the successful logon and logoffs. This is not going to audit the user/s attempting to make changes to the IPSec policies.
B: This would only provide part of the information required by the CIO.
C, F: The audit privilege use audit policy audits each successful instance of a user exercising a user right and each failed attempt to exercise a user right. This is not going to identify users making or attempting to make changes to the IPSec policies of Certkiller .com.

QUESTION 12:

You work as the senior network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
You have noticed that some unauthorized changes have been made to the registry of several computers. You suspect that one of your junior network administrators is changing the registry. You decide to enable auditing to log all changes being made to the registry. You want all attempts made to change the registry keys to be logged. You want no other type of event to be included in your auditing effort.
You open the domain audit security policy and navigate to the audit policy settings under the Security Settings node. You then enable the Audit object access audit policy setting for failed events. When viewing the logged events, you discover though that there are no events logged for any successful changes made to the Registry. You want all events to be logged, and not only failed attempts to change the Registry. To this end you need to configure audit policy settings.
What should you do?

A. Set the Audit privilege use audit policy setting to log successful and failed events.
B. Set the Audit directory service access audit policy setting to log successful and failed events.

C. Set the Audit Policy change audit policy setting to log successful and failed events.
D. Set the Audit object access audit policy setting to log successful and failed events.

Answer: D

Explanation: While you have enabled the correct audit policy setting in the Security Settings node, you have specified that only failed attempts to change the Registry be logged. You should configure the Audit object access setting if you want to track and log when a user accesses operating system components such as files, folders or registry keys. Because you need both successful and failed events logged, you should reconfigure the Audit object access audit policy setting so that both successful and failed events are logged.
Incorrect Answers
A: You would configure the Audit privilege use audit policy setting to log when a use effects a user right.
B: The Audit directory service access policy audit policy setting logs events that pertain to when users access Active Directory objects which have system access control lists (SACLs). The Registry is not an Active Directory object. You should regard it as being computer specific.
C: The Audit Policy change audit policy setting is used to log changes that are made to the security configuration settings of the computer.

QUESTION 13:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
Users that work in the Research department access confidential files that reside in a shared folder named UserPerformance. None of the other Certkiller .com business units' users should be able to access these files. To this end you configure the necessary shared and NTFS permissions to ensure that only Research department users have access to the files within the UserPerformance folder.
You have been instructed by the CIO to perform monitoring on the UserPerformance folder so as to check whenever users other than the Research department access the data. To perform this exercise, you need to use a user account that does not have the shared and NTFS permissions assigned which are granted to the Research security group for the folder.
What should you do?

A. Enable auditing for failed events in Privilege Use
Use Event Viewer to examine the logged event entries
B. Enable auditing for failed events in Directory Service.
Use Event Viewer to examine the logged event entries.
C. Enable auditing for failed events in Object Access.
Use Event Viewer to examine the logged event entries.

D. Assign the Generate security audits user right to the user account.
Use Event Viewer to examine the logged event entries.

Answer: C

Explanation: Configuring the Object Access audit policy in this manner will let you know when this user account attempted to access the UserPerformance folder and failed to access the Research department's files. To view all logged event entries.
Incorrect Answers
A: The Privilege Use audit policy tracks when a user effects a user right. You do not want to track events for all rights.
B: The Directory Service audit policy tracks when users access Active Directory objects which have system access control lists (SACLs).
D: You do not want to enable the user account to make entries in the security log for object access auditing. You want to verify that the user account cannot access the UserPerformance shared folder.

QUESTION 14:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
All file servers on the network store confidential information and all file servers have auditing configured. All file servers are stored in an organizational unit (OU) named FileServers. As the senior network administrator you are responsible for ensuring that the log size and retention settings for the event logs of all file servers remain as is. No administrators are allowed to make changes to any of these settings locally, on any file servers.
While verifying the configuration for generating event logs on a file server named Certkiller -SR11, you notice that the log size and retention settings have changed. You also discover that two other file servers have had these settings changed as well. This is undesirable and you thus received instruction to address the issue.
There are thus a few tasks at hand:
1. Applying the same log size and retention settings for event logs for all Certkiller .com file servers.
2. Performing the configuration which will ensure that no administrators can change an event log's log size and retention settings at some future date.
What should you do?

A. Log on to your client computer using your Enterprise Admins group membership. Connect to each file server and configure the proper log size and retention settings in Event Viewer.
B. Configure a new Group Policy object (GPO) with the proper log size and retention settings.
Link the GPO to the FileServers OU.

C. Establish a Remote Desktop connection to connect to each file server.
Connect to each file server and configure the proper log size and retention settings in Event Viewer.
D. Configure a new security template that contains the proper log size and retention settings using the Security Configuration and Analysis tool on a file server.
Import the new security template to the local security policy of all other file servers.

Answer: B

Explanation:
Group Policy is an Active Directory feature that provides the means for you to efficiently manage large numbers of computers. You can manage user and computer configuration settings centrally through applying Group Policy settings to the appropriate Active Directory container. Group Policy settings are stored in a Group Policy Object (GPO).You can define and link GPOs to a specific OU in Active Directory. The GPOs are then applied to all Active Directory objects stored within the specific OU. Group Policy application starts at the top of the domain tree, and then moves down to the OU containing the user object or computer object. OU GPOs have the highest precedence. In your case, to prevent other administrators from logging on to a file server locally and changing the log size and retention settings, you have to configure a new Group Policy object (GPO) with the proper log size and retention settings. You have to then link the GPO to the FileServers OU, which is the OU containing all file servers. This will also update all file servers to have the same log size and retention settings.
Incorrect Answers:
A, C: You have to use Group Policy settings to ensure that the log size and retention settings are not overridden by any administrators logging on to file servers and updating the Properties sheet of the event log. A GPO will override all locally configured settings on the file servers.
D: This option will not work because a security template is not used to define the log size and retention settings of an event log.

QUESTION 15:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
A server named Certkiller -FS02 has been configured as a file server.
Certkiller -FS02 hosts a shared folder named UserDocs. A global group named Full-time Employees has been granted the Full Control Permission over UserDocs.
A Certkiller .com user complained that another employee deleted his files that he stored in the UserDocs folder. Due to this deletion of files, the CIO instructed you to record any attempts made to delete files from the UserDocs folder, as well as to record an event each time that a user modifies the permissions for the UserDocs folder. To this end you need to configure an appropriate audit policy.

What should you do?

A. Configure Audit object access policy for failure.
B. Configure Audit directory service access policy for success and failure.
C. Configure Audit object access policy for success and failure.
D. Configure Audit privilege use policy for failure.
E. Configure Audit directory service access policy for failure.

Answer: C

Explanation: You record each time a user tries to delete a file; you should configure Audit object access policy to track both successful and failed access events. The Audit object access policy setting must be enables as well as auditing must be enabled in the UserDocs DACL. Here you can get a granular method of auditing different types of access including the modification of access permissions.
Incorrect answers:
A: You should be configuring auditing to track success and failed attempts.
B: The Audit directory service access policy record each attempt to access Active Directory service objects for which SACLs have been defined. This auditing will not yield the desired results.
D: The Audit privilege use policy tracks events that are created when a user exercises a user right. This is not what needs to be tracked.
E: The Audit directory service access policy record each attempt to access Active Directory service objects for which SACLs have been defined. Configuring thus method of auditing will not yield the desired result.

QUESTION 16:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. All servers reside in an organizational unit (OU) named Servers.
One of the servers named Certkiller -DC01 has been configured as a domain controller and another server named Certkiller -FS02 has been configured as a file server. Certkiller -FS02 hosts several shared folders; one of these shared folders is named ConfidentialDocs. As the name indicates, it holds sensitive data that is meant for the Certkiller .com managers only. All the Certkiller .com managers enjoy membership of a global security group named Managers. This group has been granted Full Control permission over the ConfidentailDocs folder.
One of the Certkiller .com managers named Clive Wilson complained that he is no longer able to access the ConfidentialDocs folder and requested that the issue be resolved. You investigate the mater and discover that Clive Wilson's user account has been removed from the Managers global group. You then add Clive Wilson's user account to the Managers global group again. Now you want to find the culprit that removed Clive Wilson's user account from the Managers global group. Thus

you need to monitor all attempts to modify any group's membership.
What should you do?

A. Configure Audit account management policy for failure.
B. Configure Audit directory service access policy for success and failure.
C. Configure Audit account management policy for success and failure.
D. Configure Audit object access policy for success and failure.
E. Configure Audit privilege use policy for success and failure.
F. Configure Audit directory service access policy for failure.

Answer: C

Explanation: This policy will allow you to track events such as password changes and the creation, deletion as well as modification of user account groups. The requirements in this questions states that you need to monitor all attempts at modifying the group membership of the Managers global group, thus you should audit both success and failed events.
Incorrect answers:
A: This is only partly correct since you need to monitor both success and failed attempts.
B: The Audit directory service access policy monitors the events that are created when a user who accesses an Active Directory object has its own SACL. Thus configuring this policy to track failed and successful events will result in a record of all events in which a user gains access to a directory service object, e.g. the Managers global group. Thus it would not yield the required records in this scenario.
D: The Audit privilege use policy will track events created when a user exercises a user right. This policy auditing will not yield the required information tracking.
E: The Audit object access setting is configured to record every time that a user accesses an object whether it was successful or not. This is not what needs to be monitored.
F: The Audit directory service access policy monitors the events that are created when a user who accesses an Active Directory object has its own SACL. Thus configuring this policy to track failed events will result in a record of all events in which a user gains access to a directory service object, e.g. the Managers global group. Thus it would not yield the required records in this scenario.

QUESTION 17:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. All member servers reside in an organizational unit (OU) named Servers, and all domain controllers reside in an OU named Domain_Controllers.
The Servers OU contains four servers named Certkiller -SR21, Certkiller -SR21, Certkiller -SR23, and Certkiller -SR24 respectively. There is a new Certkiller .com written security policy that dictates that all Security log files, before deletion or overwriting must be viewed by an administrator. It further also states that these

files should be reviewed each day.
You need to comply with the new Certkiller .com security policy. To this end you run some tests because you have some concerns regarding the amount of disk space that will be required to comply with this new security policy. After running the tests, you discover that you need to double the default log size on each member server.
What should you do?

A. Create a new Group Policy object (GPO) and link it to the Servers OU.
Define a value of 32768 KB in the Maximum Security log size policy.
Enable the Overwrite events as needed option in the Retention method for security log policy.
B. Create a new Group Policy object (GPO) and link it to the Servers OU.
Define a value of 16384 KB in the Maximum Security log size policy.
Enable the Overwrite events by days option in the Retention method for security log policy.
C. Create a new Group Policy object (GPO) and link it to the Servers OU.
Define a value of 32768 KB in the Maximum Security log size policy.
Enable the Do not overwrite events (Clear log manually) option in the Retention method for security log policy.
D. Create a new Group Policy object (GPO) and link it to the Servers OU.
Define a value of 4 GB in the Maximum Security log size policy.
Enable the Do not overwrite events (Clear log manually) option in the Retention method for security log policy.

Answer: C

Explanation: The Do not Overwrite events (Clear log manually) option is the only option that will allow you to configure a manual retention method for event logging. When enabled, the events in the security log will be retained until the log is cleared manually and when the log's maximum capacity is reached new events will not be logged until more space becomes available.
You also need to increase the size of Security log to 32768 KB. The default size of this log would not be sufficient.
Incorrect Answers:
A: This option is only partly correct; however, the Overwrite events as needed option would cause the existing events in the log to be overwritten by new events when the log becomes too full.
B: The value of the Maximum security log size needs to be enlarged to comply with the new security policy since 16384 is but the default value at which the log was set and was found to be inadequate. The Overwite events by days option would enable you to specify the number of days that a log file would be retained, and after the specified amount of days, the existing log will be overwritten. This would not comply with the written security policy.
D: This option is only partly correct, however, you do not need to define a value of 4 GB, and it would be excessive albeit the maximum security log size.

QUESTION 18:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network contains five application servers running Terminal Services named Certkiller -SR01, Certkiller -SR02, Certkiller -SR03, Certkiller -SR04, and Certkiller -SR05. You have placed these servers in an organizational unit (OU) named TerminalServers.
The responsibility of dealing with support issues for these servers has been handed to seven of the IT department employees. You have created an OU named ITAdmin and added the user accounts of these IT department employees to it. These users are also members of a global group named TSAdmin.
You need to ensure that the TSAdmin group is assigned the Log on Locally user right for the application.
What should you do? (Each correct answer presents part of the solution. Choose TWO.)

A. Link AppSup to the TerminalServers OU.
B. Create a GPO named AppSup.
C. Access the Properties page of the ITAdmin OU, select the Security tab. Assign the Allow - Full Control permission for the ITAdmin OU to the TSAdmin group.
D. Access the Properties page of the ITAdmin OU, select the Group Policy tab, and assign the Create a GPO named AppSup the Allow - Full Control permission for the AppSup GPO group policy object link.
E. Create a GPO named AppSup, configure it to grant the TSAdmin group the Log on Locally user right.
F. Link AppSup to the ITAdmin OU.

Answer: A, E

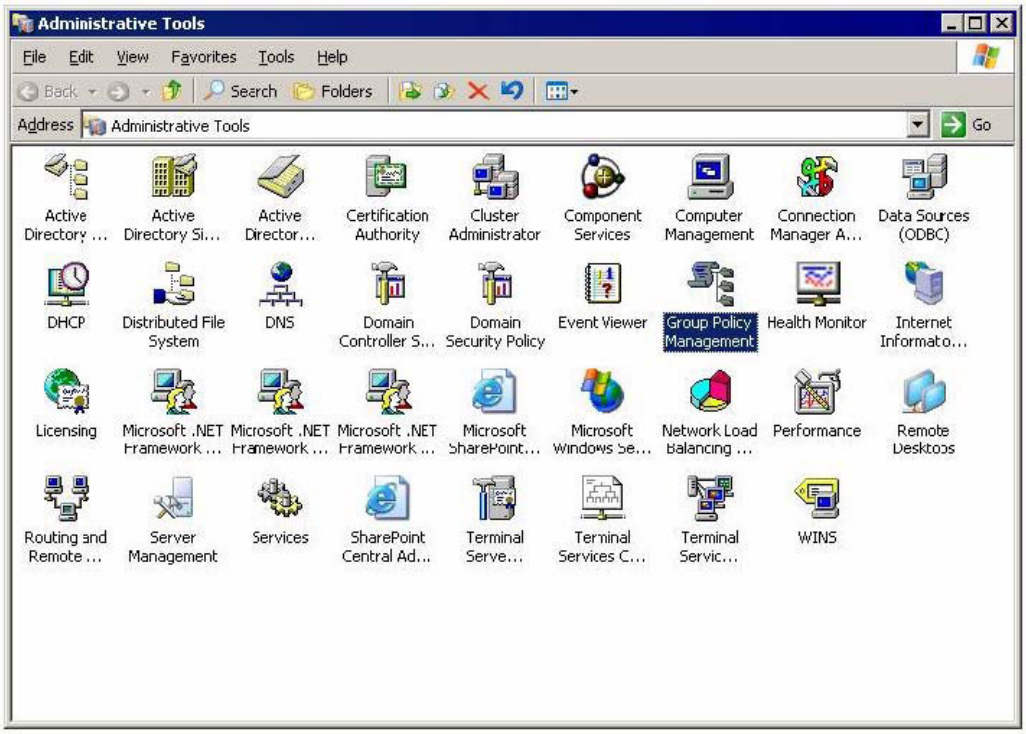
Explanation:
to allow a group of users to log on locally to servers in an OU, you can create a GPO and define the Allow log on locally setting. This setting is located in the Computer Configuration - Windows Settings - Security Settings - Local Policies - User Rights Assignment policy node. Defining this policy allows you to add users or groups that will be allowed to log on to the computer or computers where the GPO is linked. In this scenario, you want to assign this user right for the computers located in the TerminalServers OU to members of the TSAdmin global group. Therefore, the Allow log on locally setting in the AppSup GPO will be configured to include the TSAdmin group. To apply the settings, you should link the AppSup GPO to the TerminalServers OU.
Incorrect Answers:
B: This option is only partial. It suggests the creation of a GPO, but not what the GPO is

to specify. Combined with any other option it will not be specific in its purpose.
C: There is no Security tab in the OU Properties page
D: This action defines the DACLs for the group policy link object. Assigning the Allow - Full Control permission to the group policy link allows the users receiving the permission to modify, delete, and change permissions on the group policy link. It does not allow the users receiving the permission to log on locally to the application servers.
F: The ITAdmin OU contains the user accounts for the IT employees. The GPO containing the desired settings should be linked to the container that holds the application server accounts.

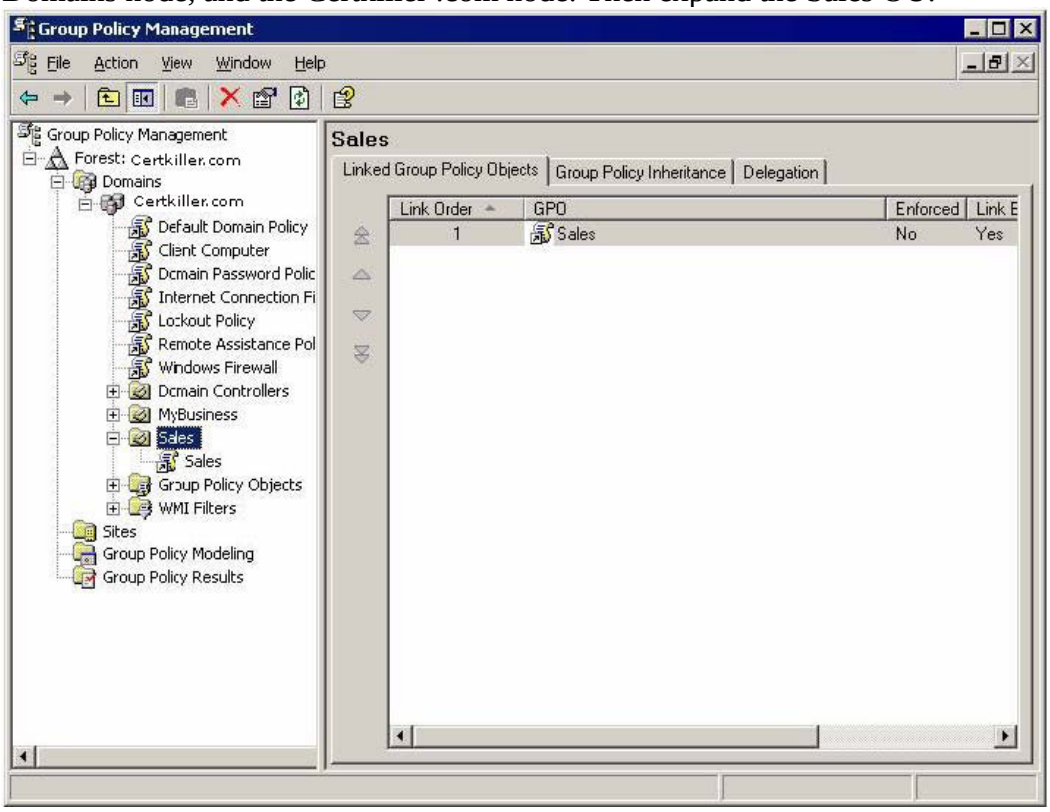
QUESTION 19:

SIMULATION
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
You are required to perform the following tasks:
1. The desktops of the employees in the Sales department have to be locked down by removing the Run command and hiding the Internet Explorer icon. You need to make sure that these settings disappear when users in the Sales department log off.
2. You have to rename the local administrator account of all Certkiller .com computers, except the computers in the Sales department, to CK_Admin.
3. You have to give the MK_Admin global group, which is located in the Marketing OU, the ability to create user accounts and reset passwords for the Marketing department.
You need to ensure that you use only the GPOs that are available and that you do not change the links of any existing GPOs. You also need to ensure that the number of GPOs that has to be edited is kept to a minimum.
What should you do? To answer, configure the appropriate options to achieve your objective.

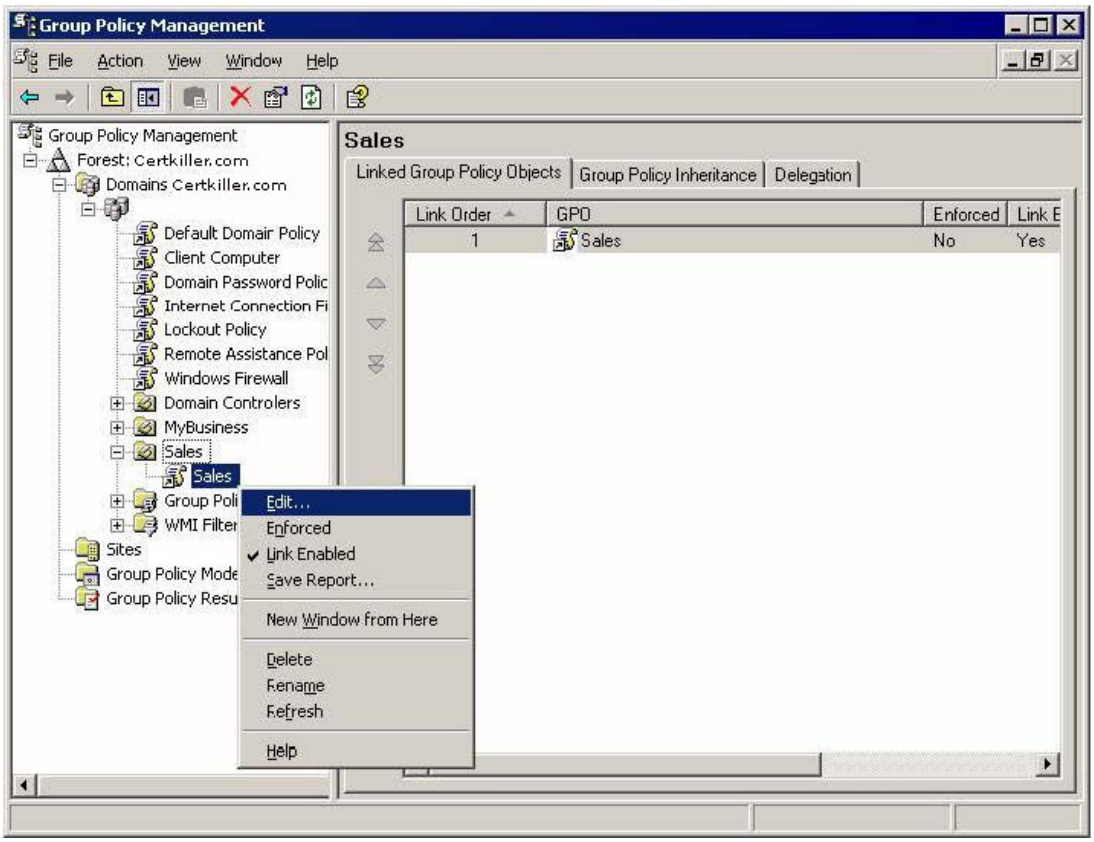
Answer:
Open Administrative Tools by clicking Start, Programs, and then Administrative Tools; or Start, Control Panel, and then Administrative Tools. Then click Group Policy Management to open the Group Policy Management console.



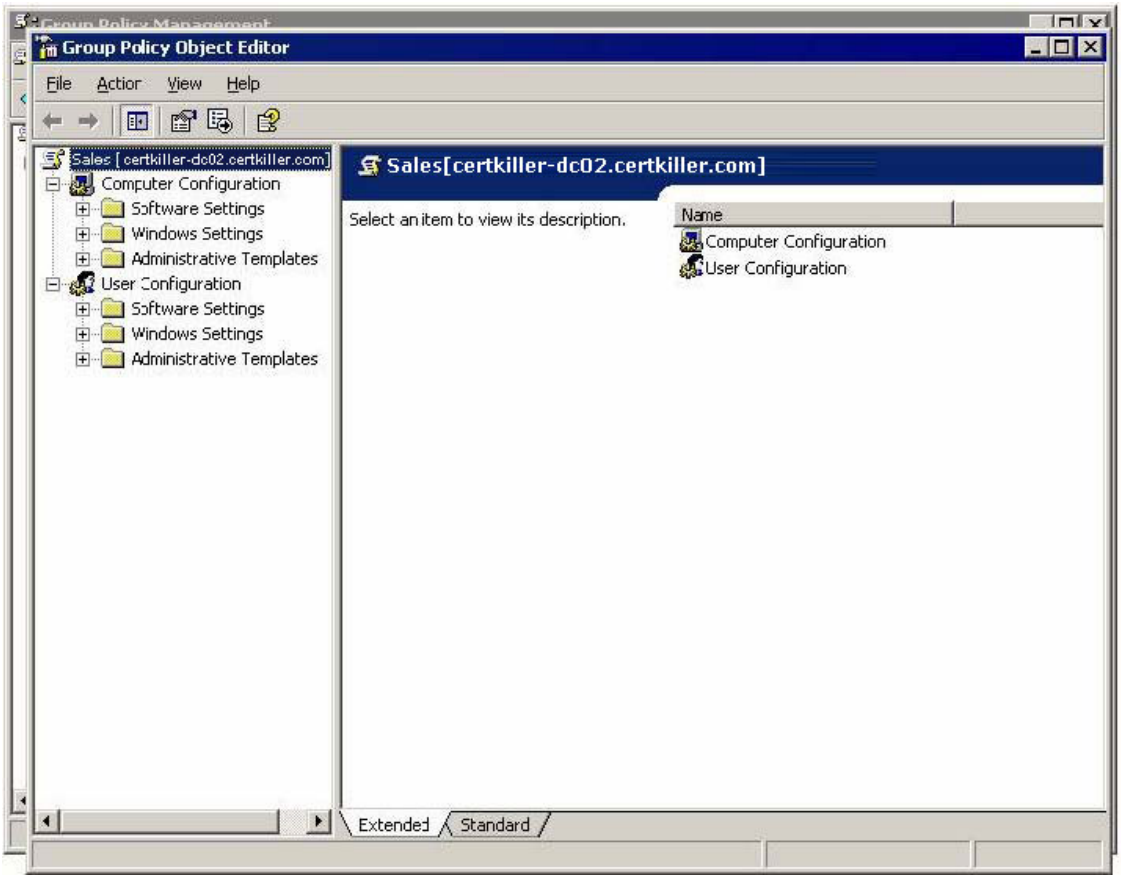
In the Group Policy Management console expand the Forest: Certkiller .com node, the Domains node, and the Certkiller .com node. Then expand the Sales OU.



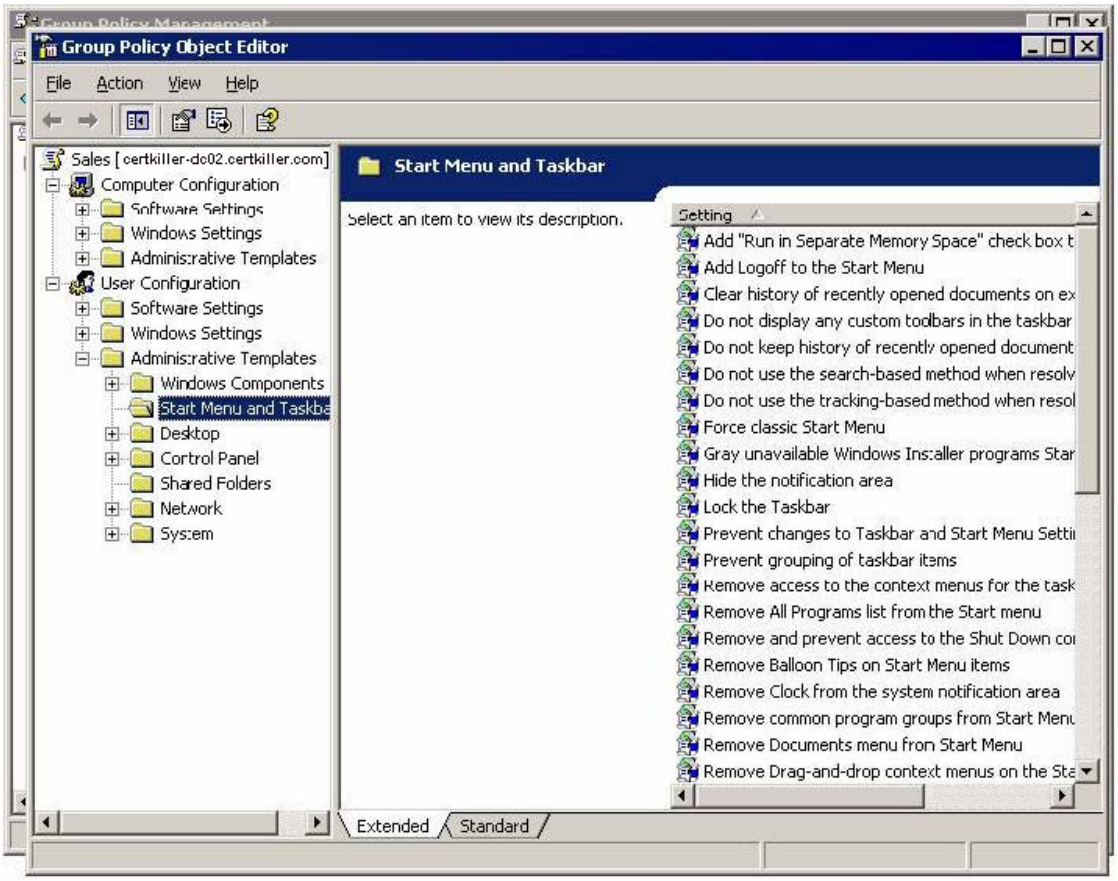
Right-click the Sales GPO under the Sales OU and select Edit from the pop-up menu.



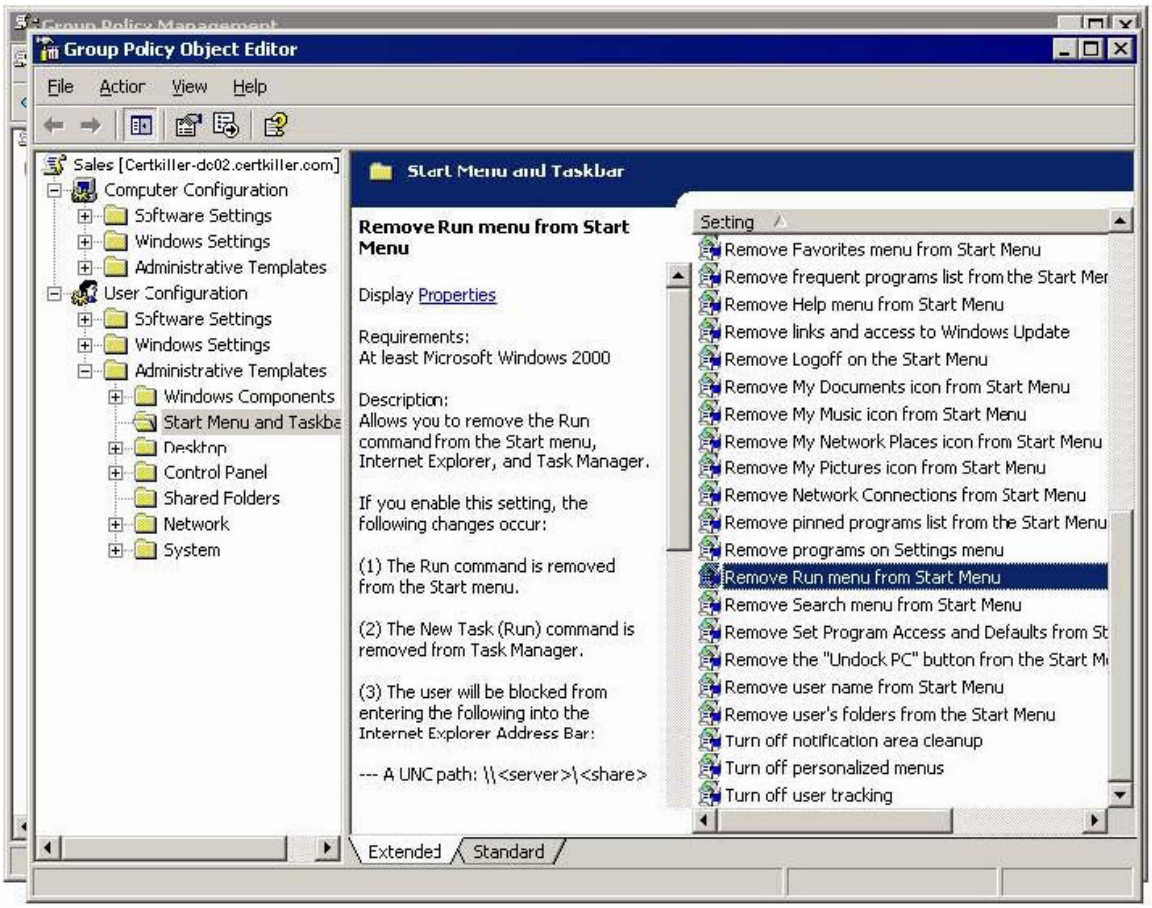
This will open the Group Policy Object Editor for the Sales GPO.



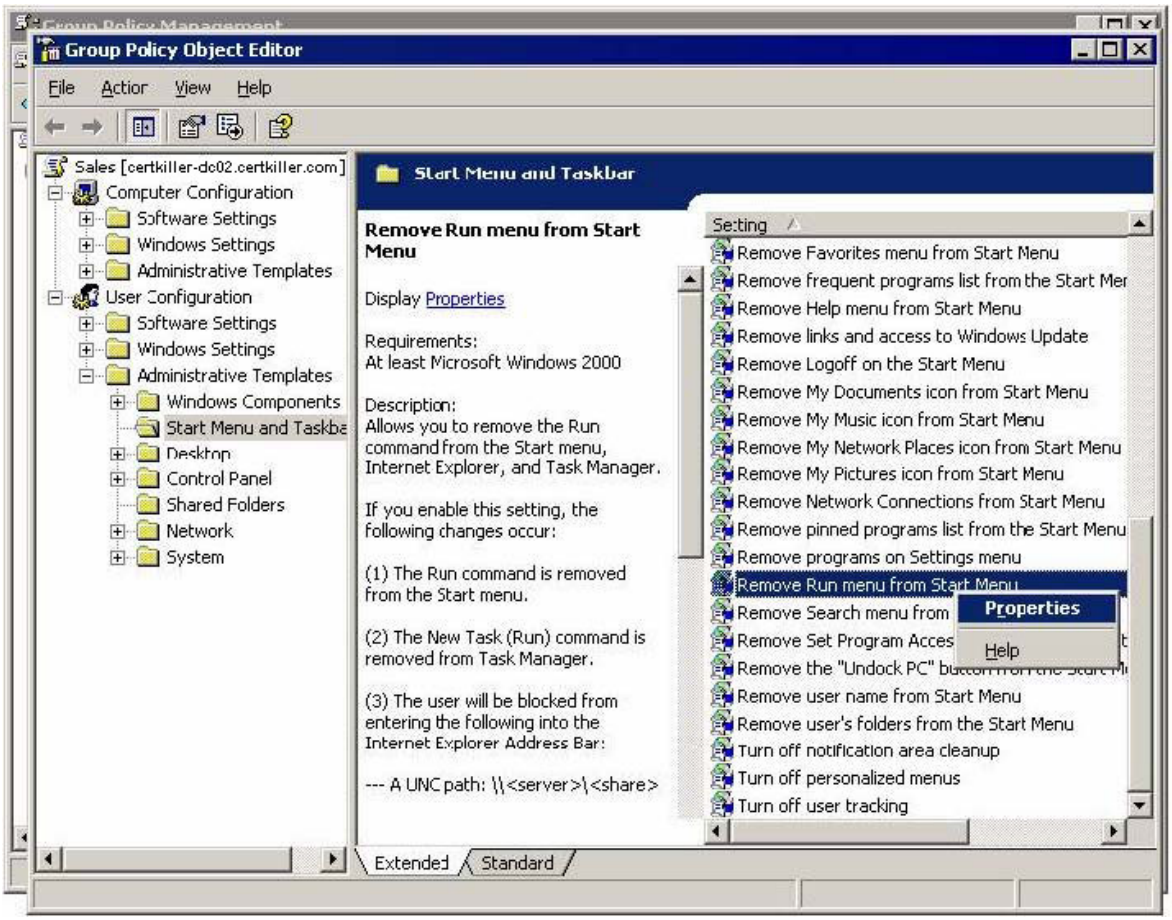
In the Group Policy Object Editor, expand the User Configuration node, and the Administrative Templates node. Then click on Start Menu and Taskbar.



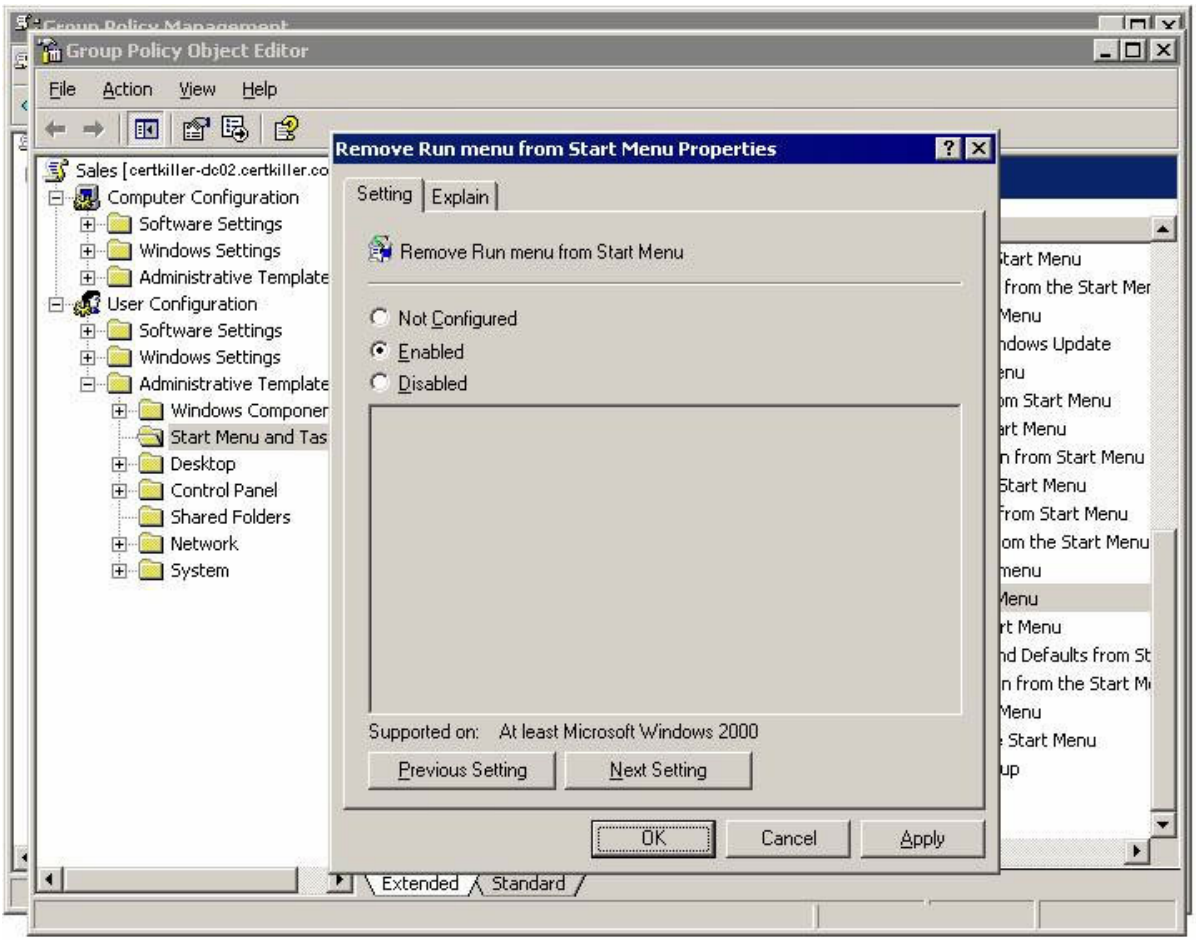
Then, in the left-hand pane, scroll down to and select the Remove Run menu from Start Menu setting.



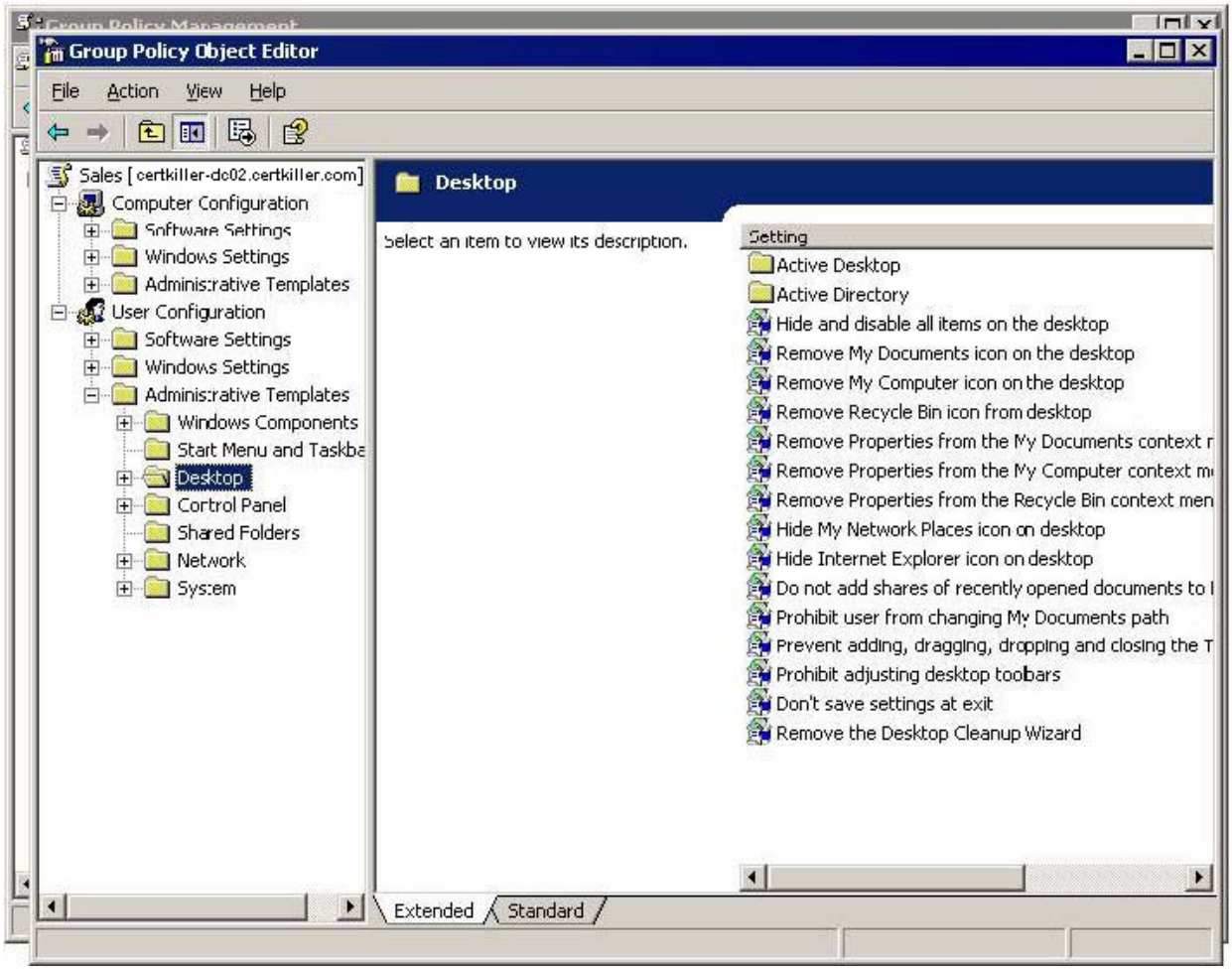
Right-click the Remove Run menu from Start Menu setting and select Properties from the pop-up menu.



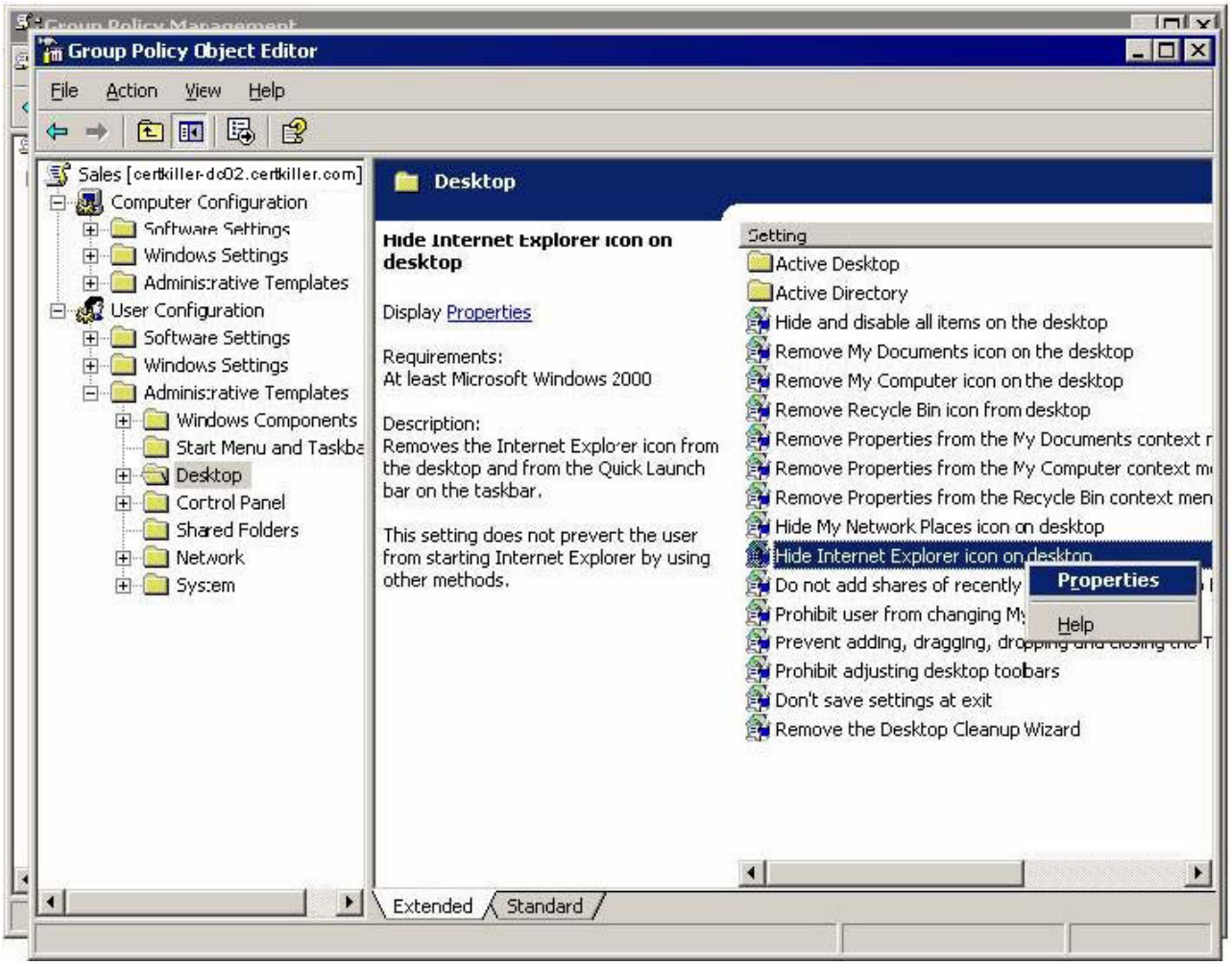
In the Remove Run menu from Start Menu Properties dialog box, select the Enabled radio button and click OK.



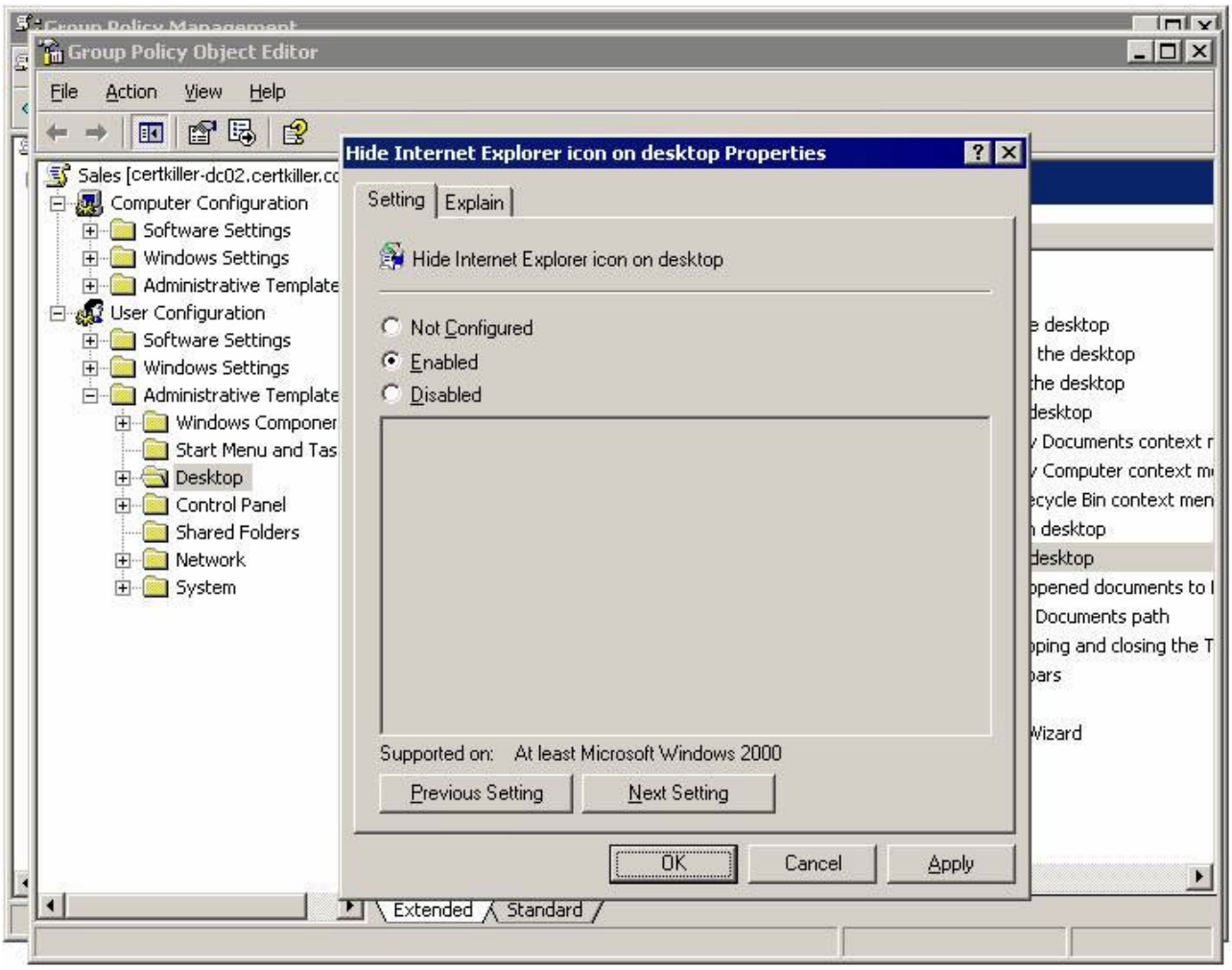
Next, click on Desktop under the Administrative Templates node in the right-hard pane of the Group Policy Object Editor.



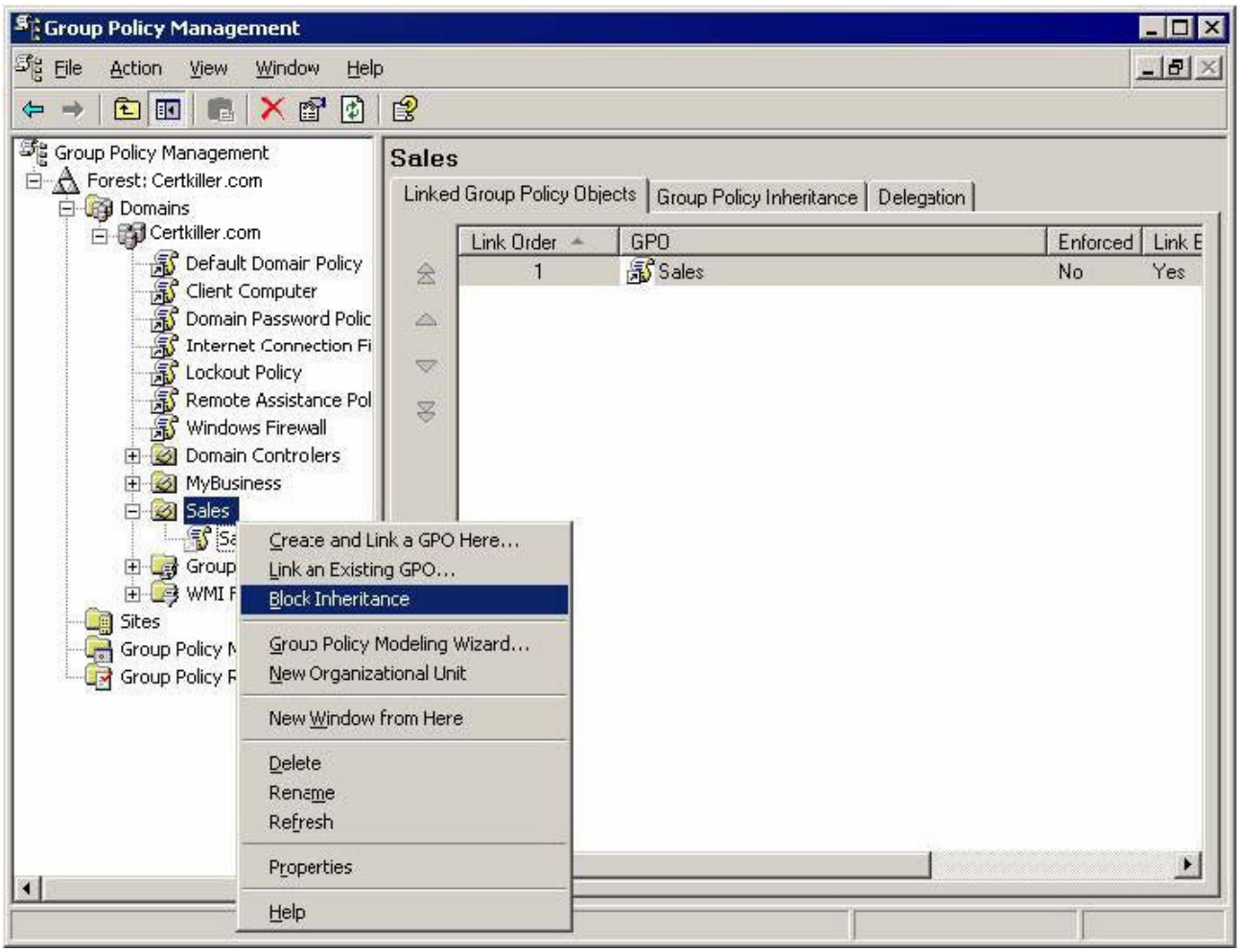
Then, right-click the Hide Internet Explorer icon on Desktop setting in the left-hand pane of the Group Policy Object Editor and select Properties from the pop-up menu.



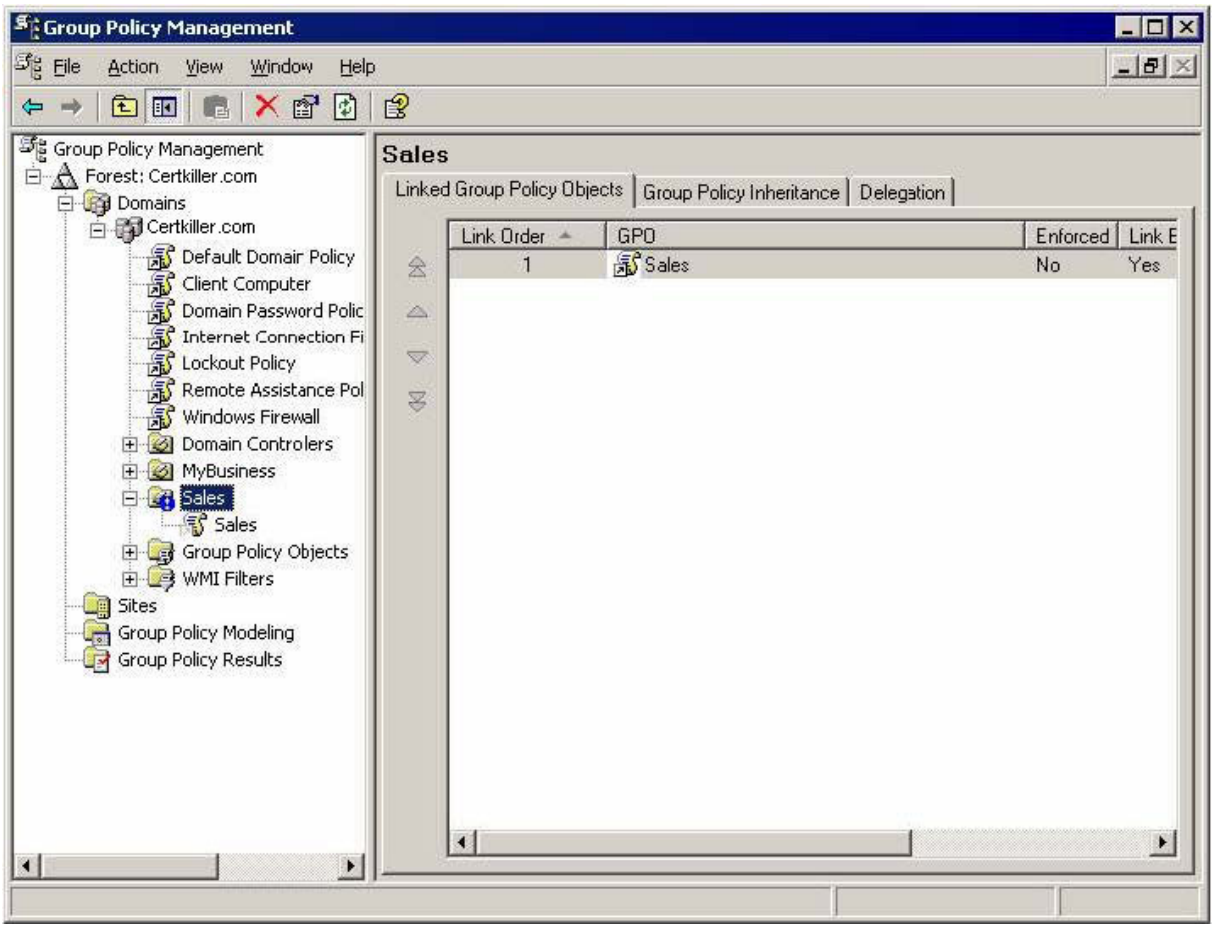
In the Hide Internet Explorer icon on Desktop Properties dialog box, select the Enabled radio button and click OK.



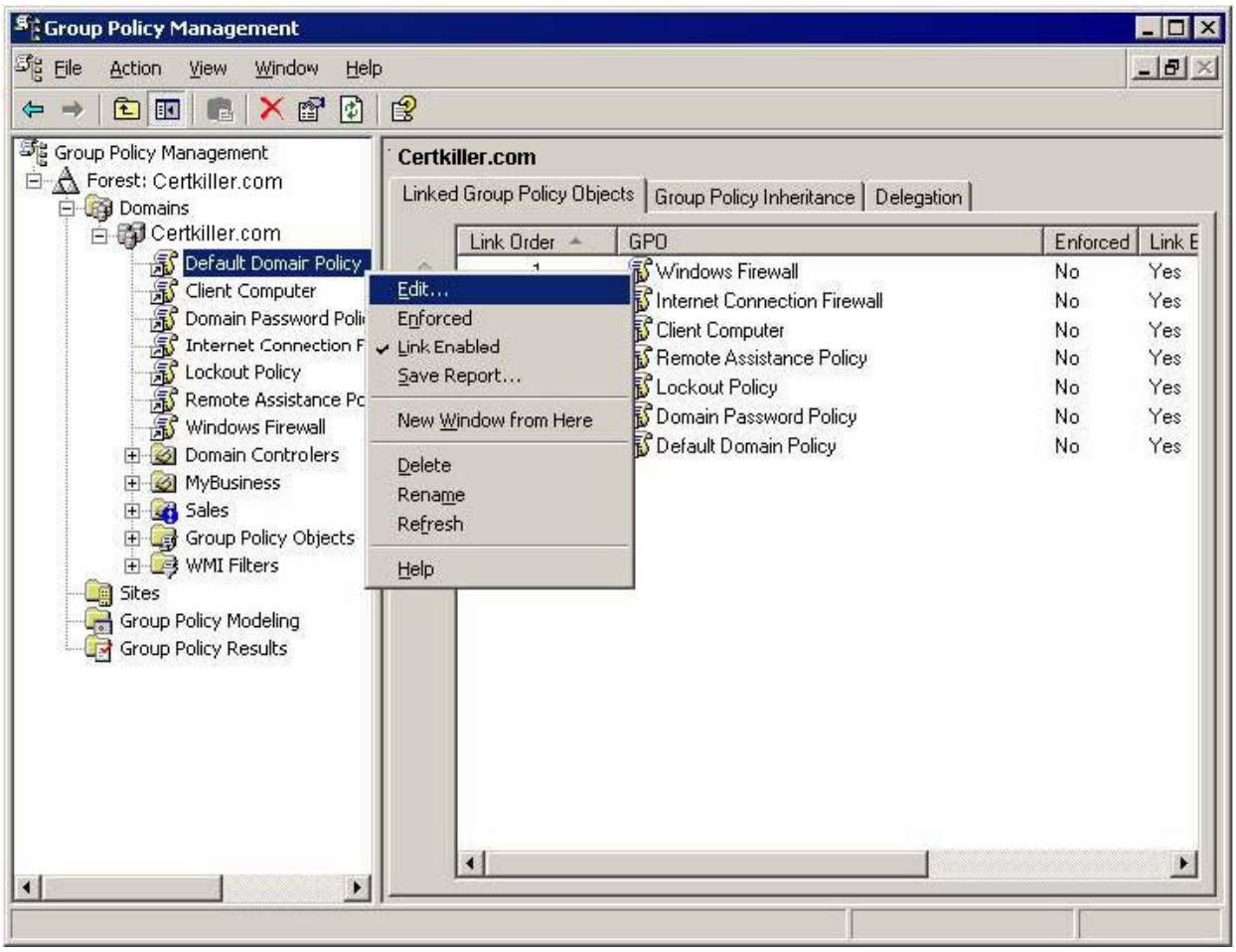
Right-click the Sales OU in the Group Policy Management console and select Block Inheritance from the pop-up menu. This will prevent the local administrator account of the computers in the Sales department from being renamed.



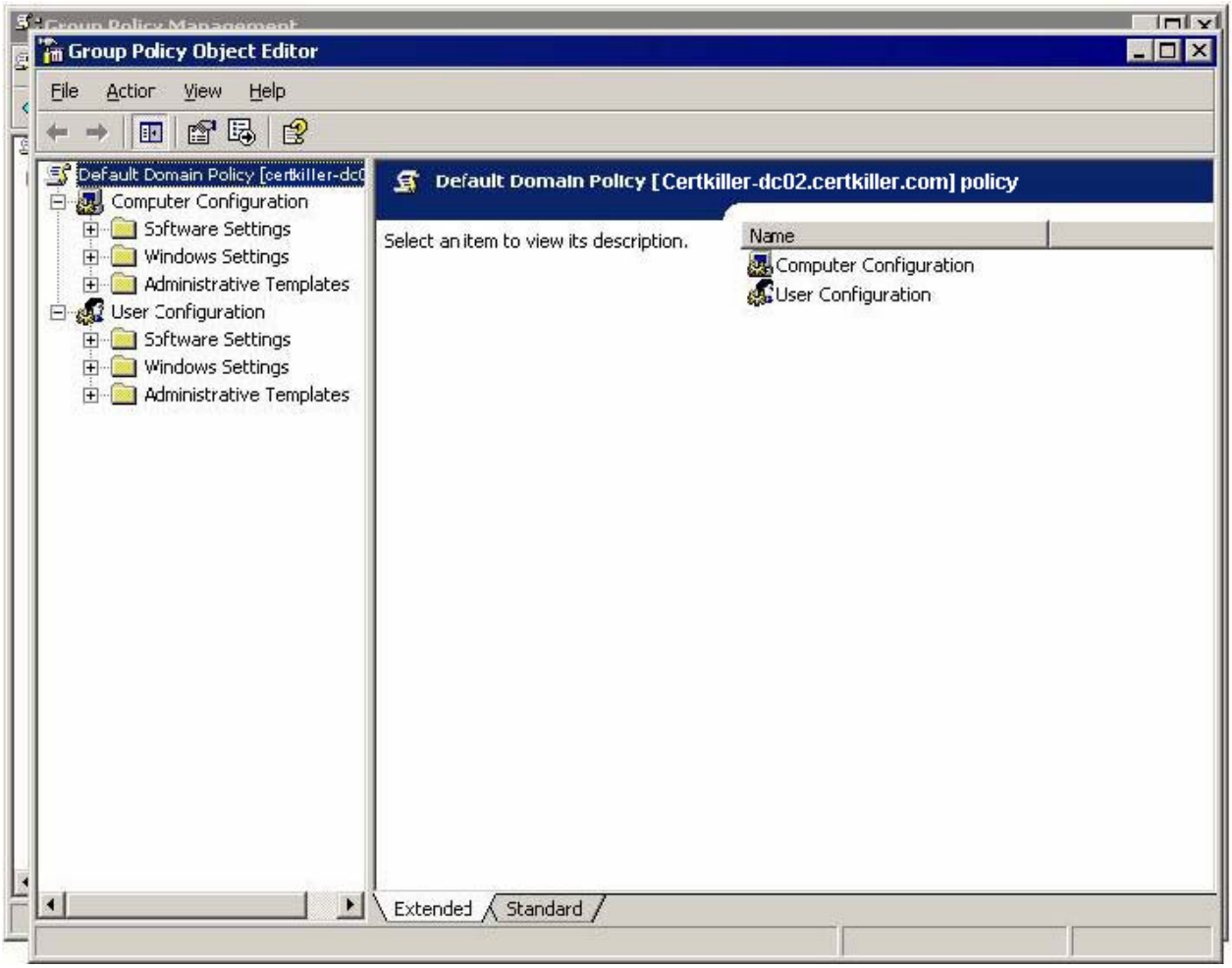
Inheritance to the Sales OU is now blocked as is indicated by the blue exclamation mark over the Sales OU icon.



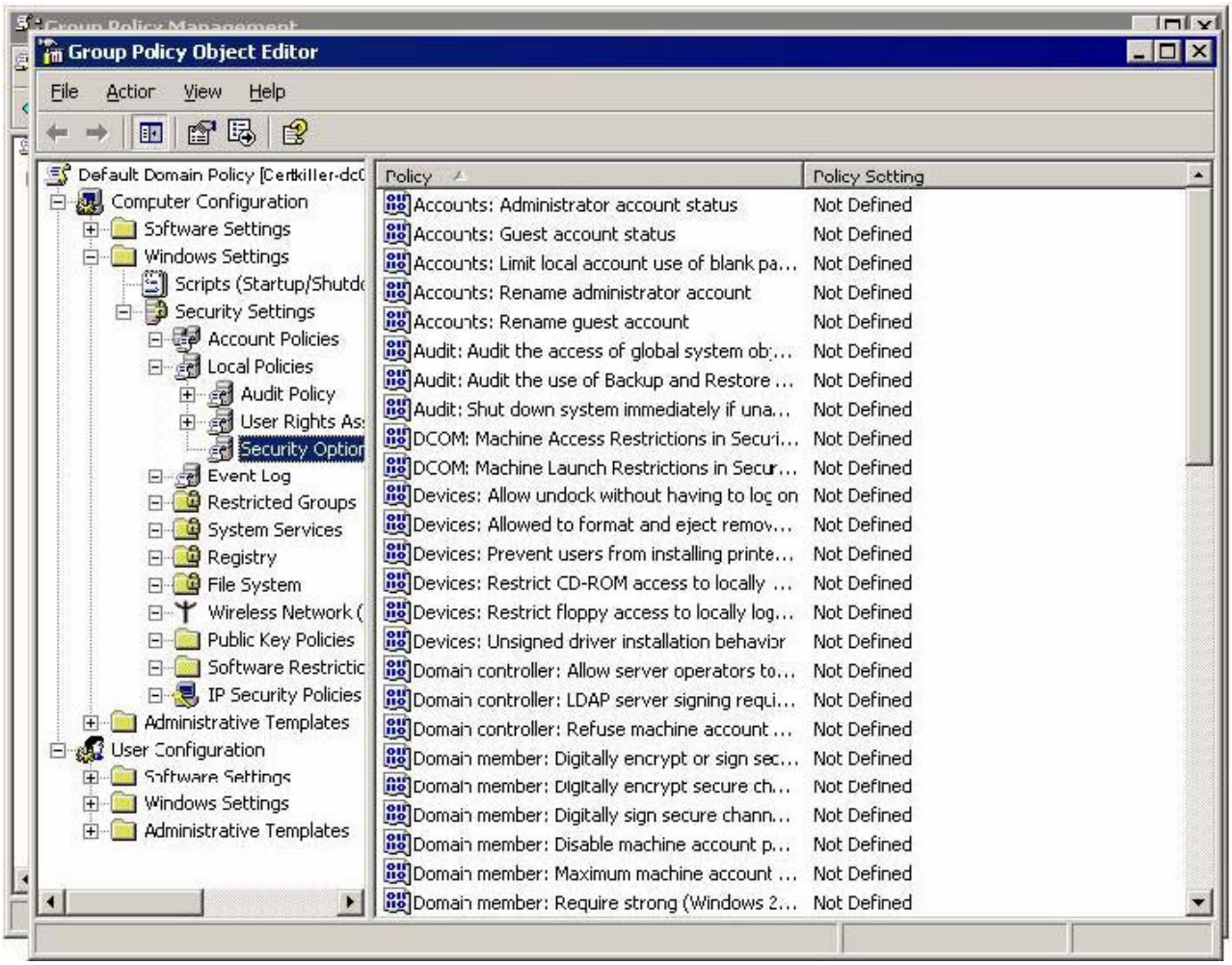
Now right click on the Default Domain Policy GPO under the Certkiller .com node and select Edit from the pop-up menu.



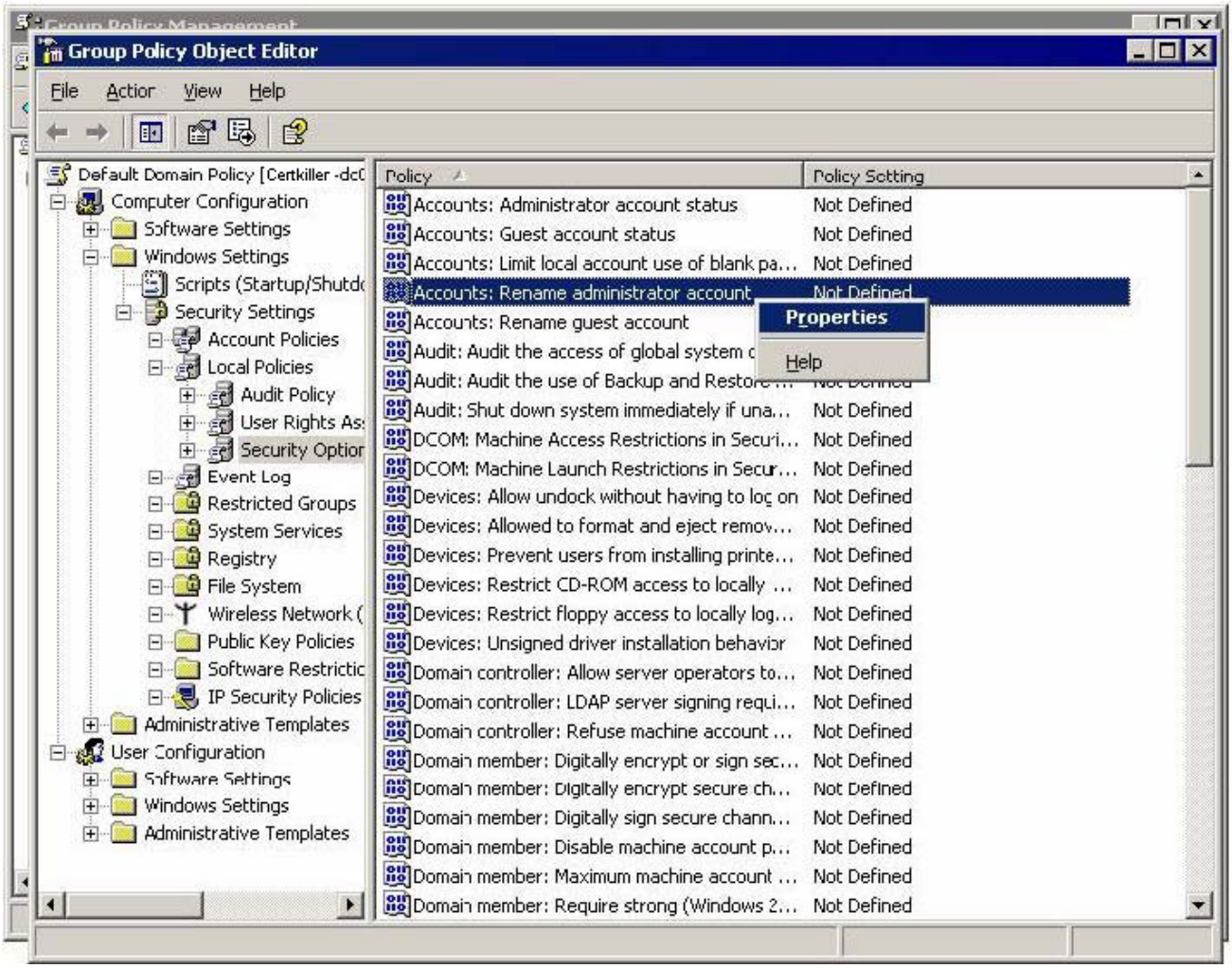
This will open the Group Policy Object Editor for the Default Domain Policy GPO.



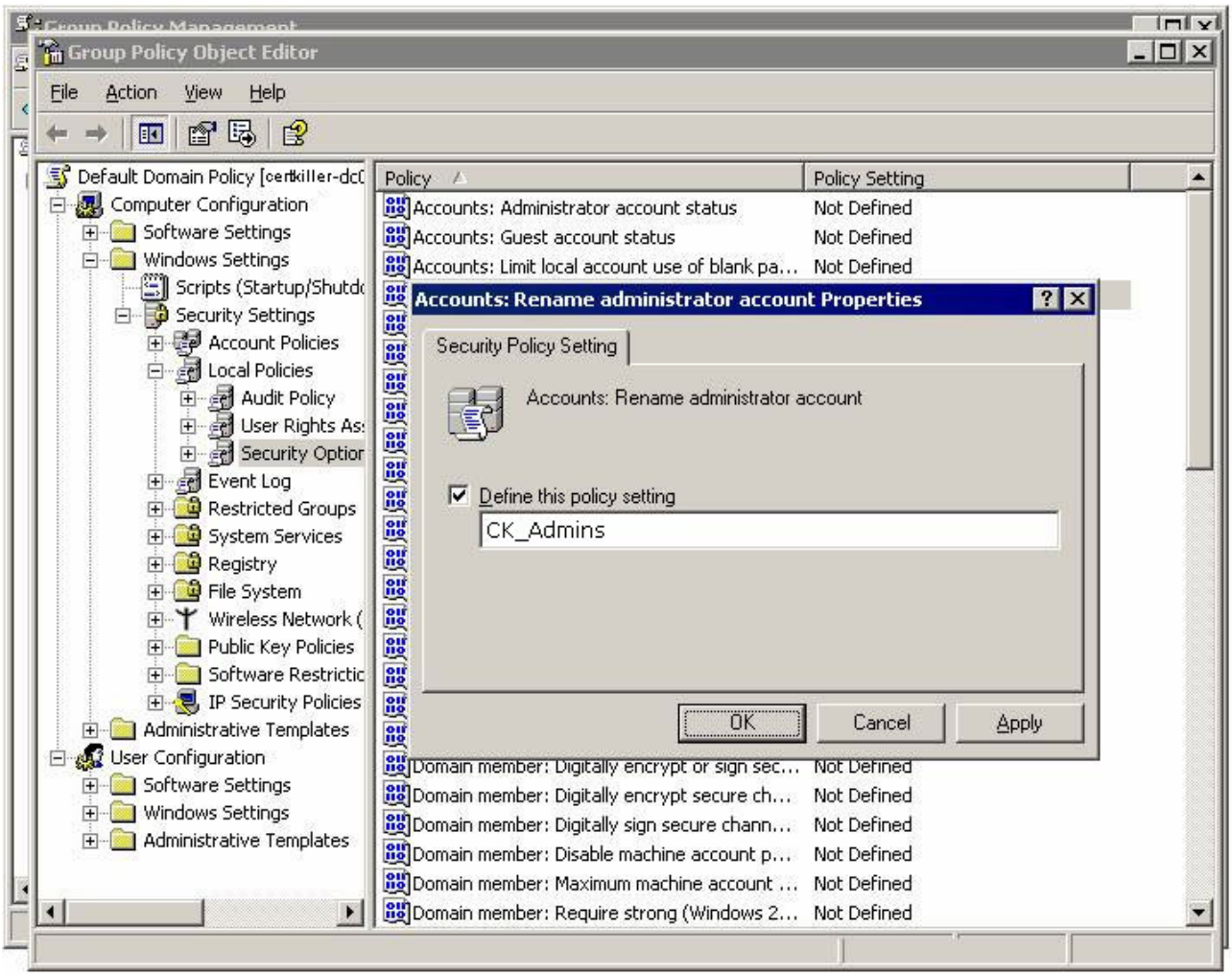
In the Group Policy Object Editor, expand the Computer Configuration node, the Windows Settings node, and the Security Settings node. Then click on Security Options.



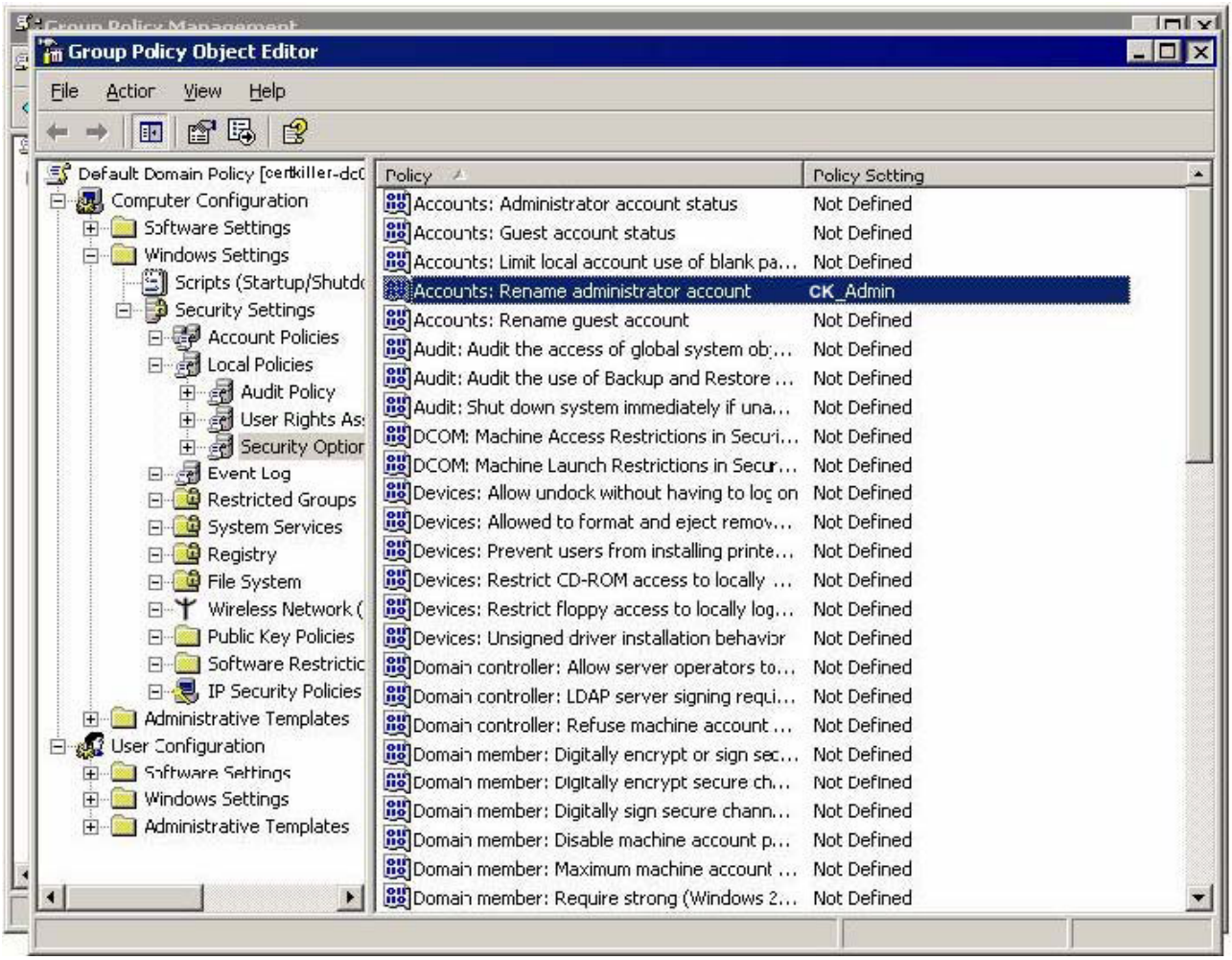
Then, in the left-hand pane, right-click on the Accounts: Rename administrator account policy and select Properties from the pop-up menu.



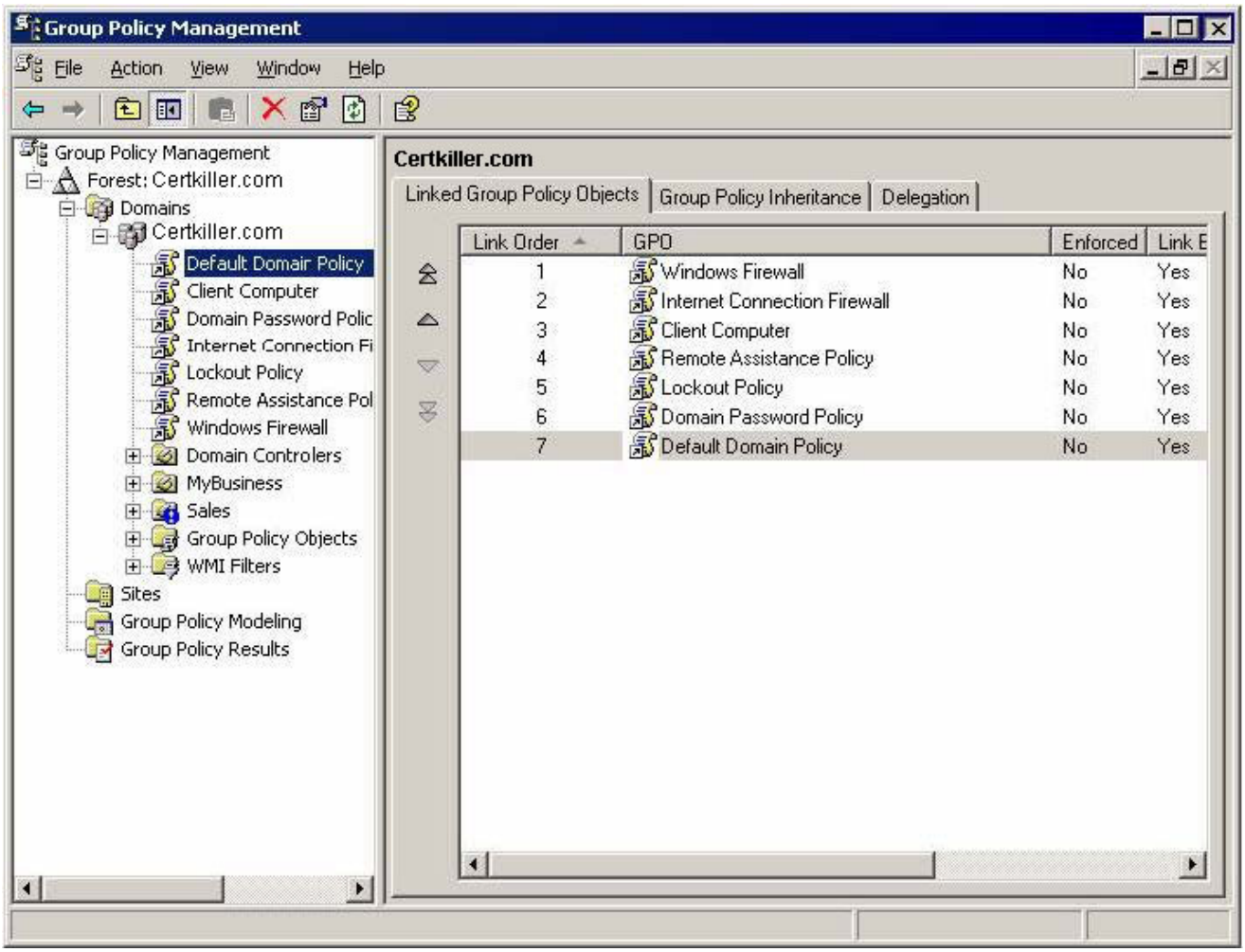
In the Accounts: Rename administrator account Properties dialog box, select the Define this policy setting check box and enter CK_Admin in the text box. Then click OK.



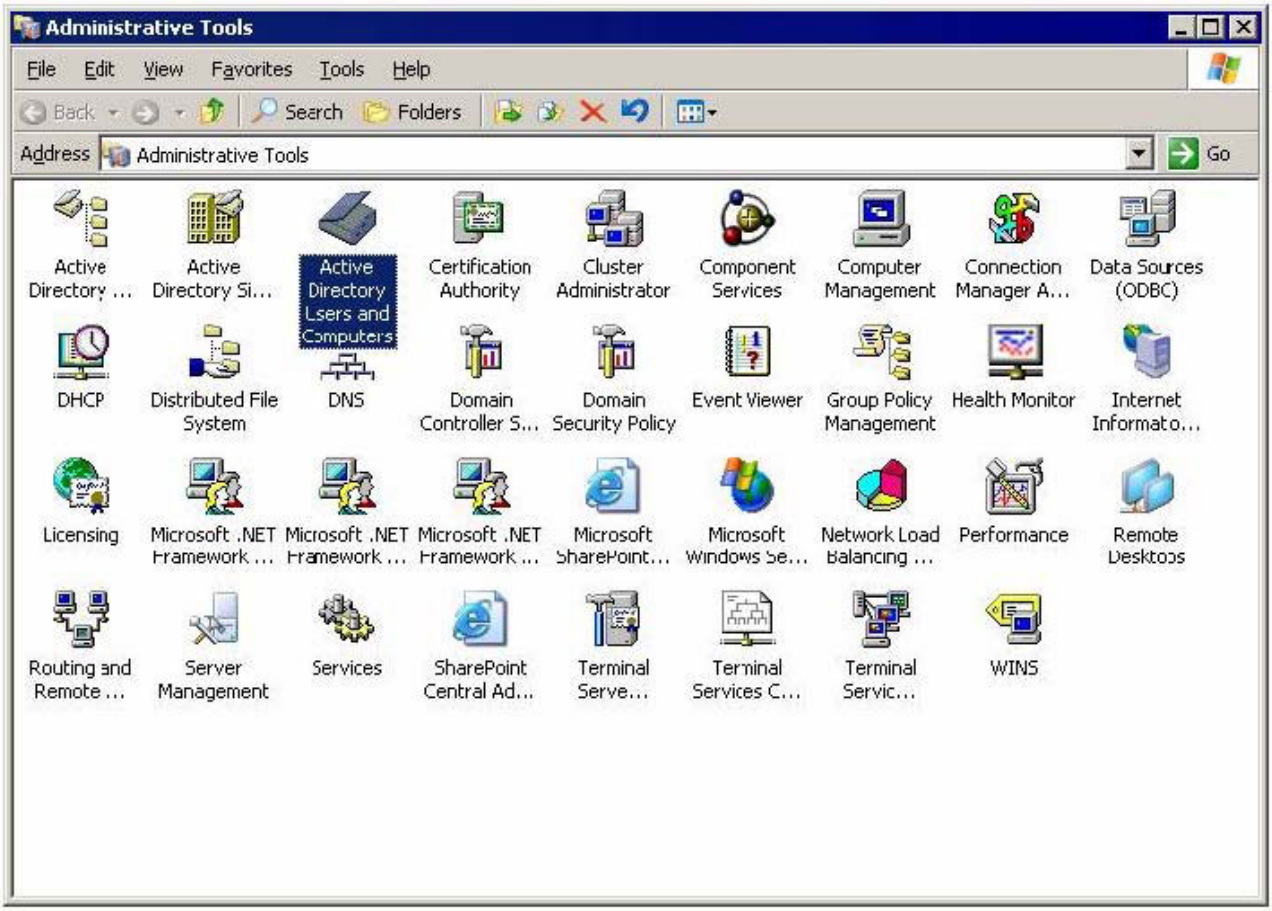
This will rename the local administrator account of all Certkiller .com computers except those in the Sales OU to CK_Admin. We've already blocked inheritance to the Sales OU so the local administrator account of the computers in the Sales OU will not be renamed. Now close the Group Policy Object Editor.



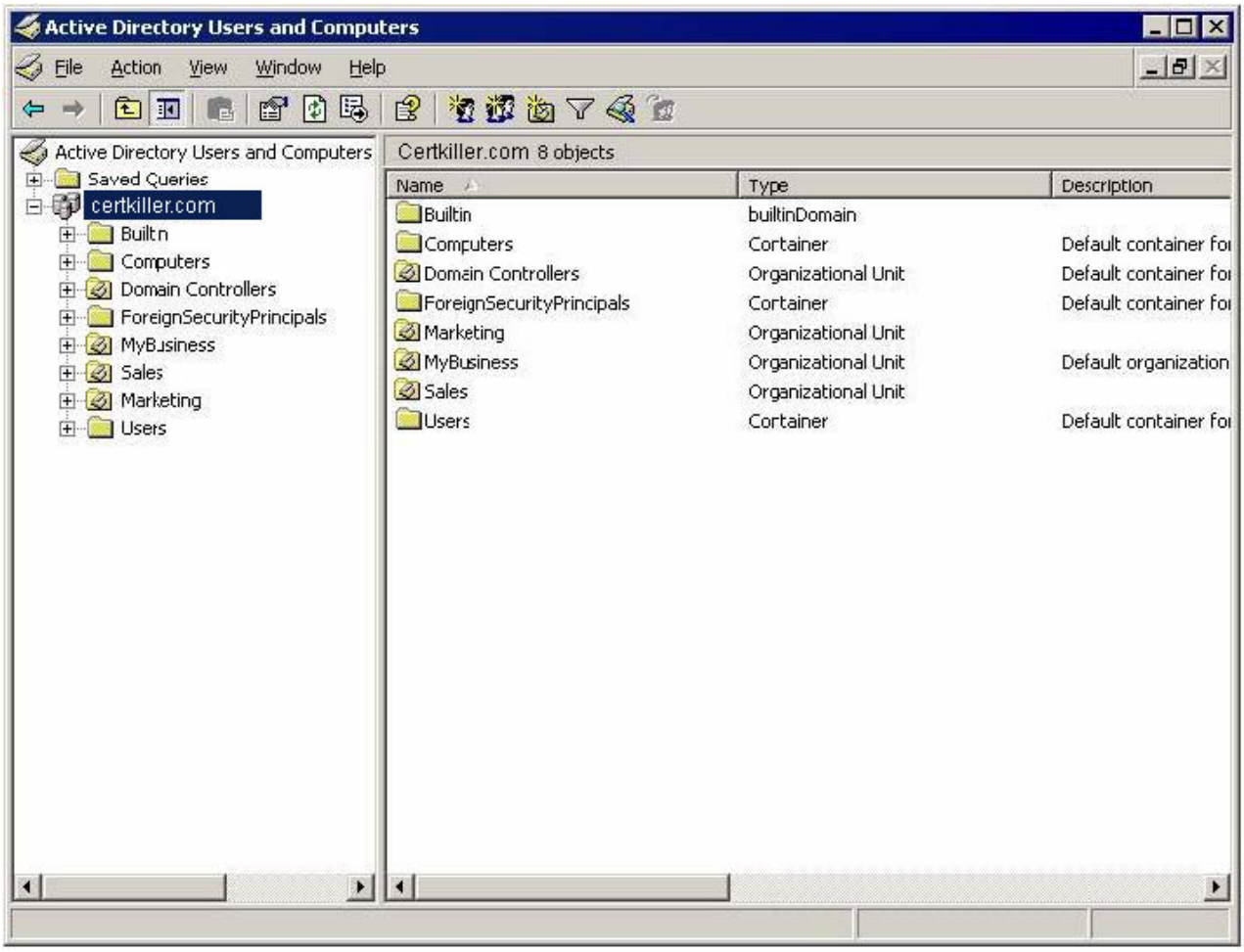
Then close the Group Policy Management console.



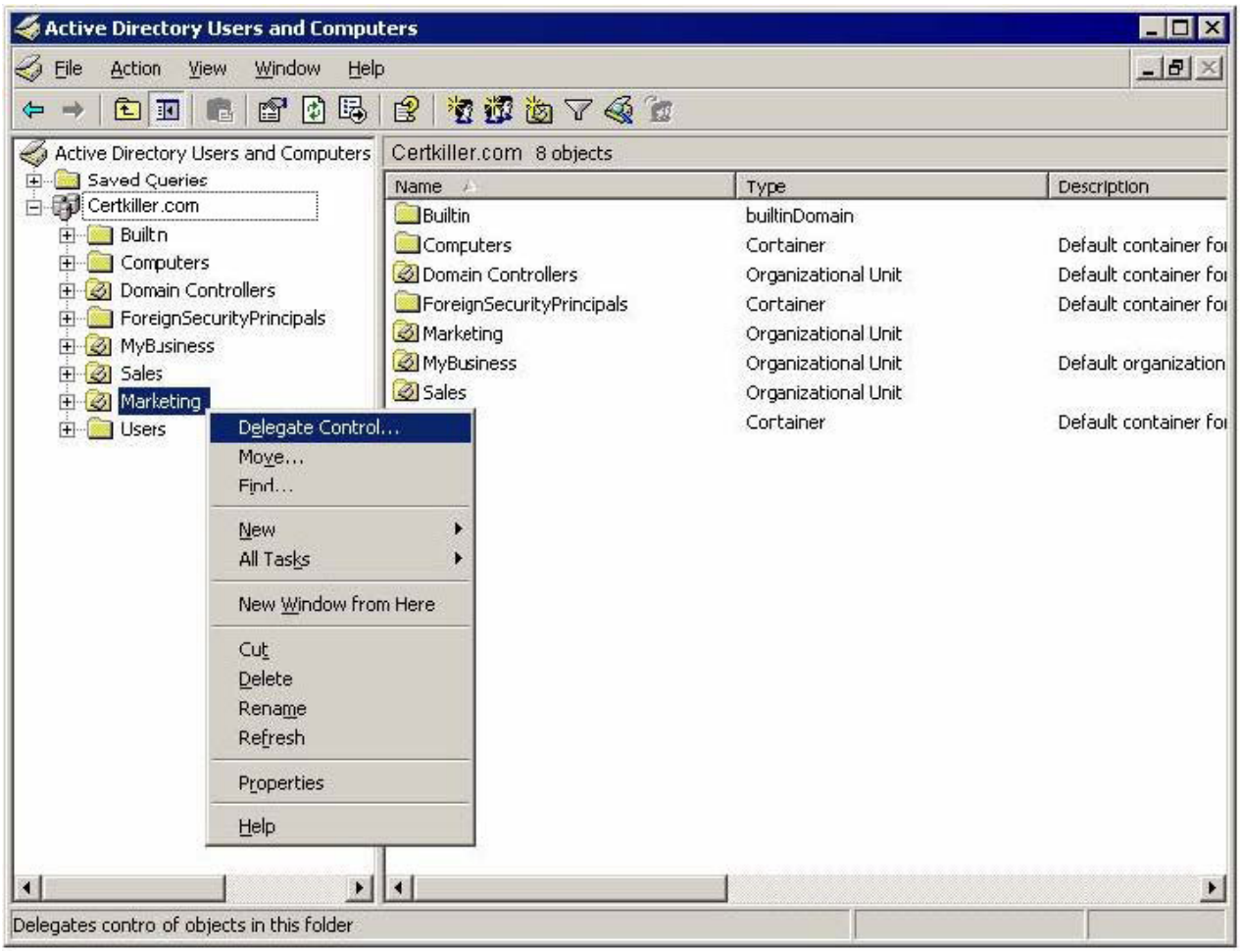
Next, in Administrative Tools, click Active Directory Users and Computers to open the Active Directory Users and Computers console.



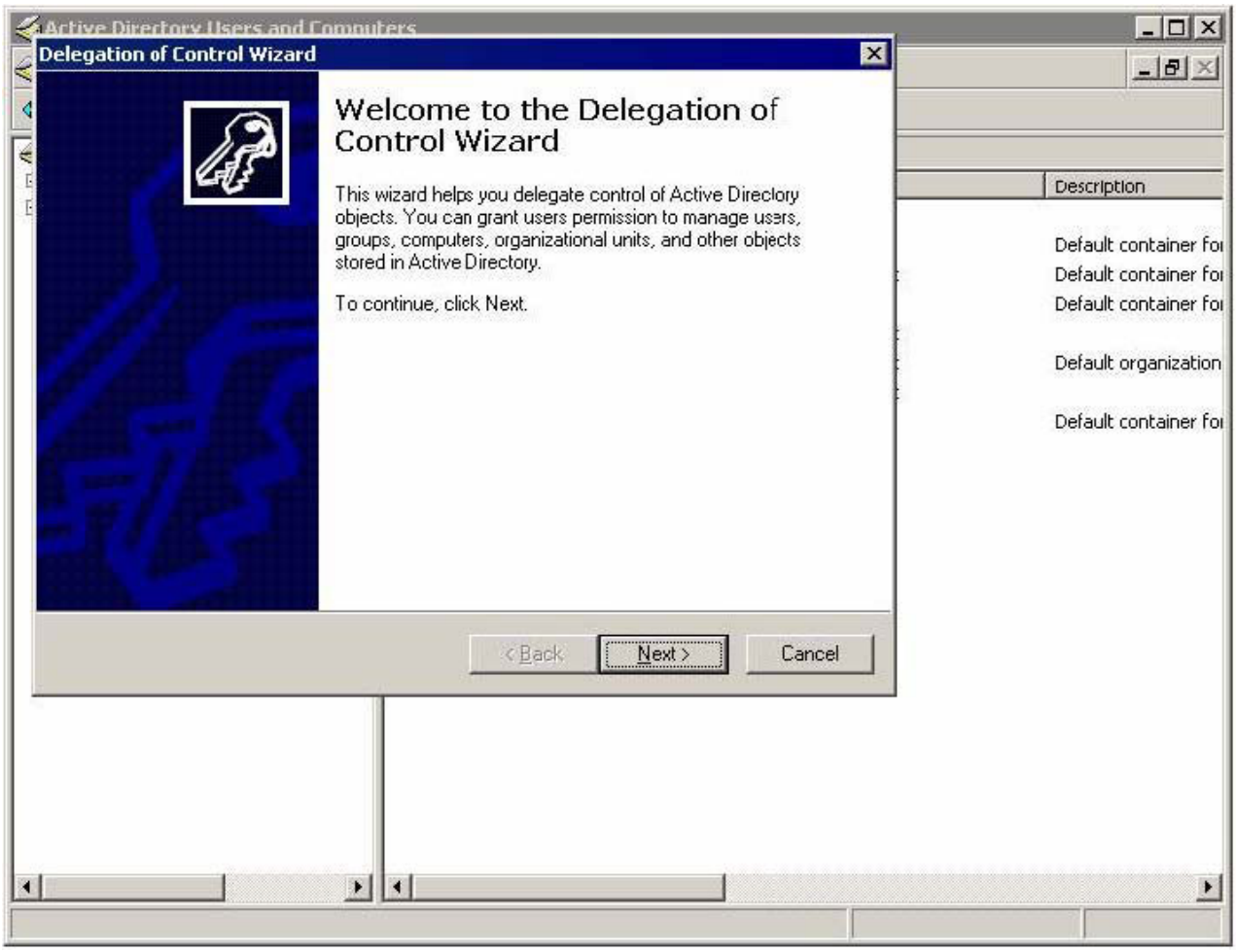
In the Active Directory Users and Computers console, expand the Certkiller .com node.



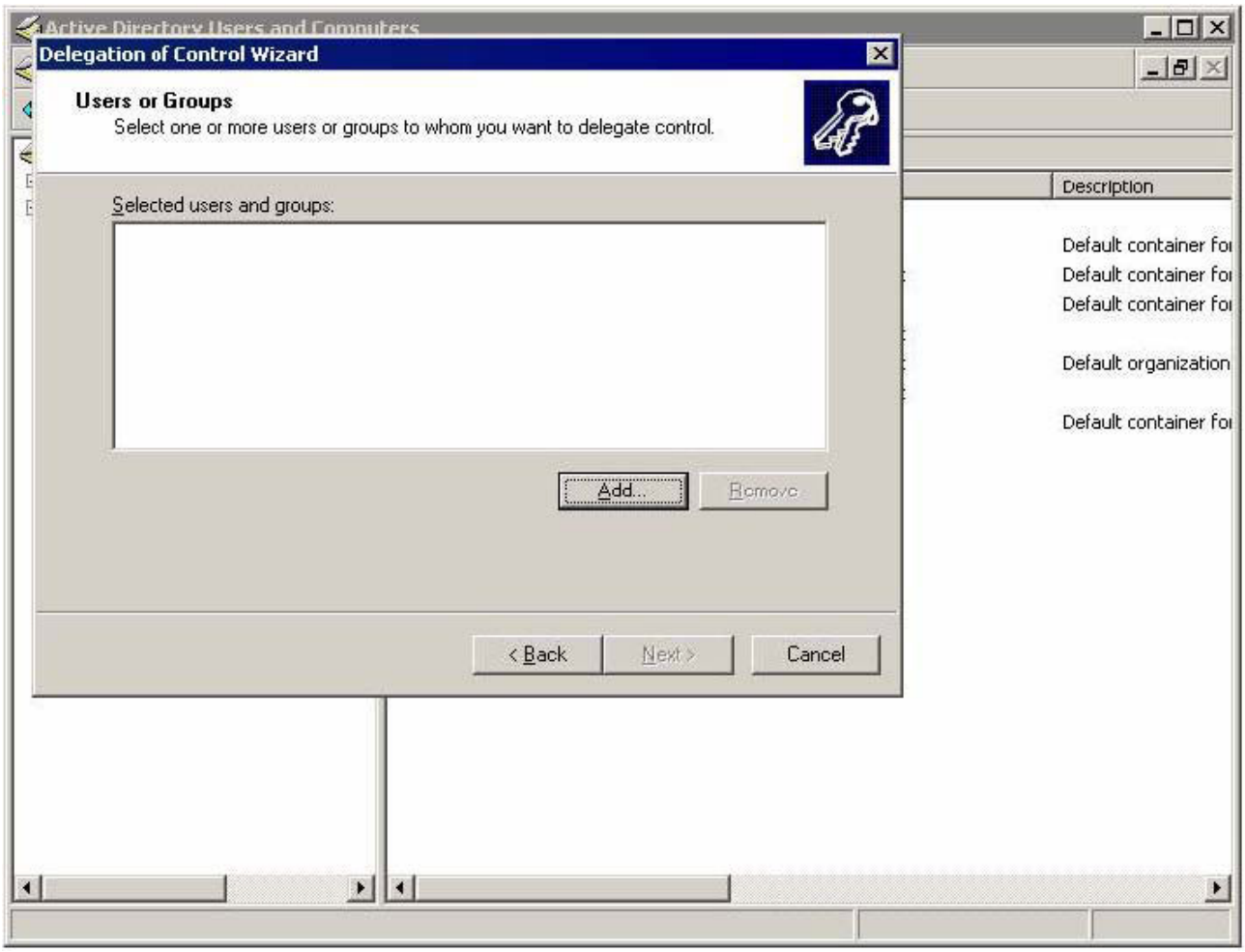
The right-click the Marketing OU and select Delegate Control from the pop-up menu top open the Delegation of Control Wizard.



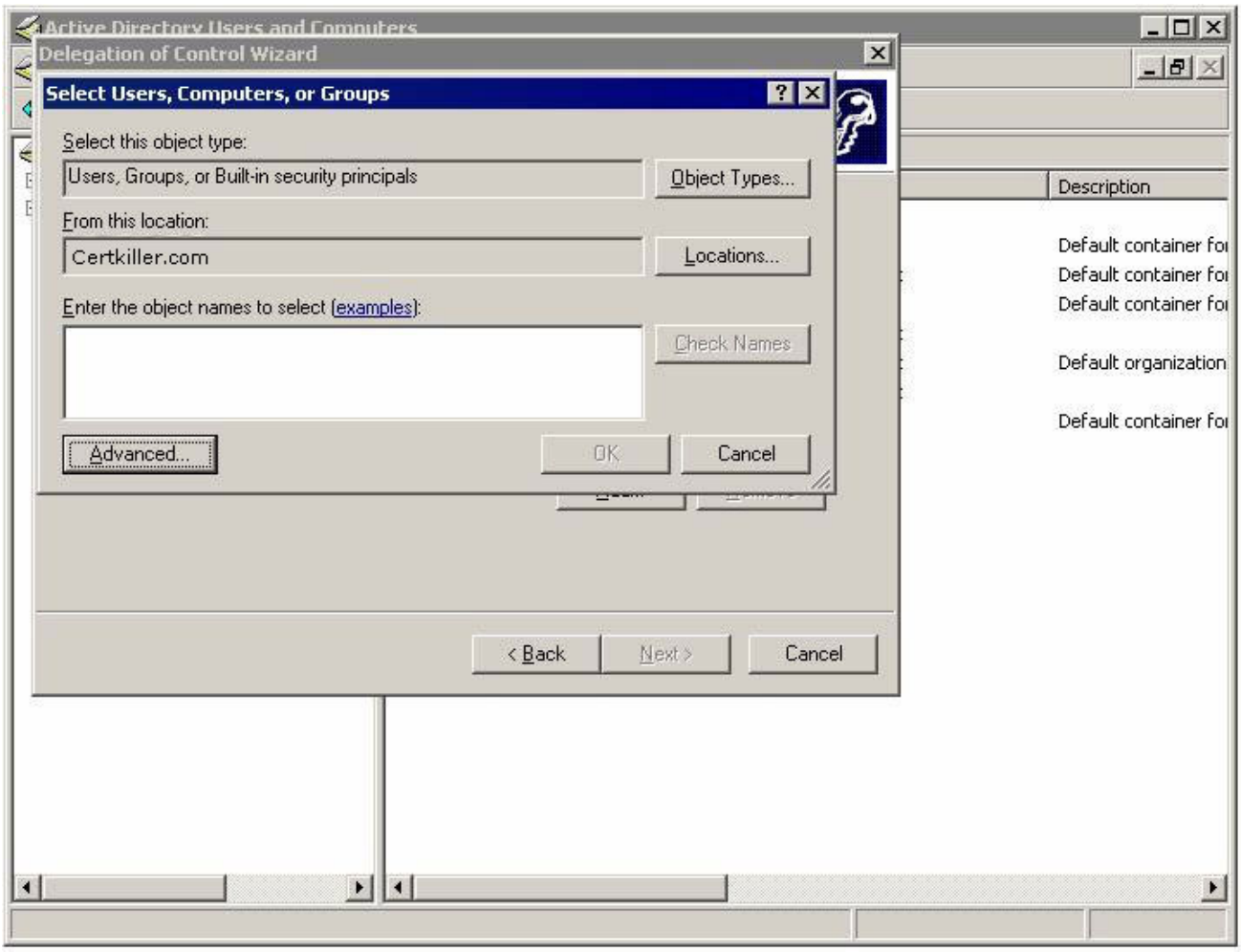
On the Welcome to the Delegation of Control Wizard page, click Next.



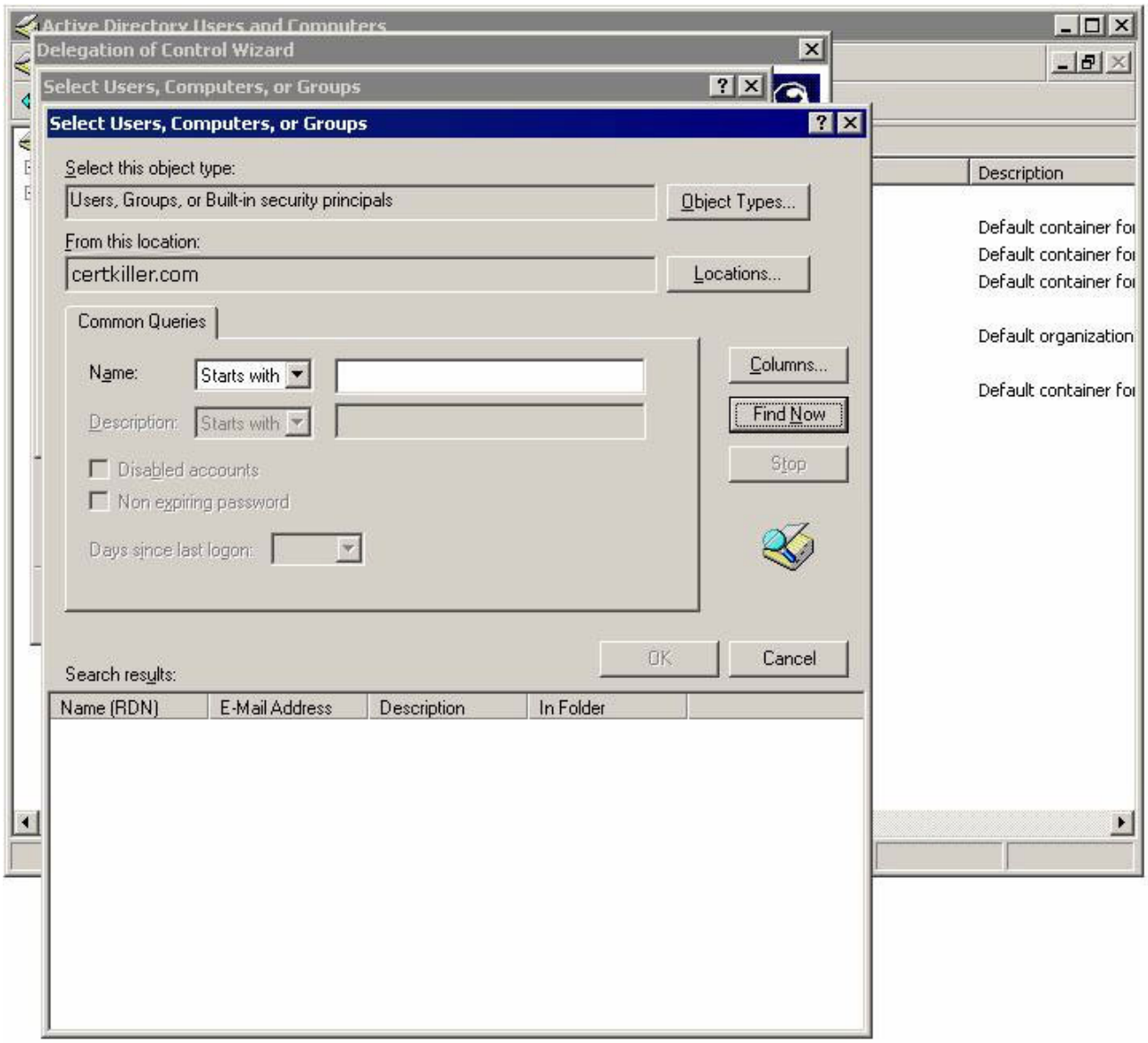
On the Users or Groups page, click Add.



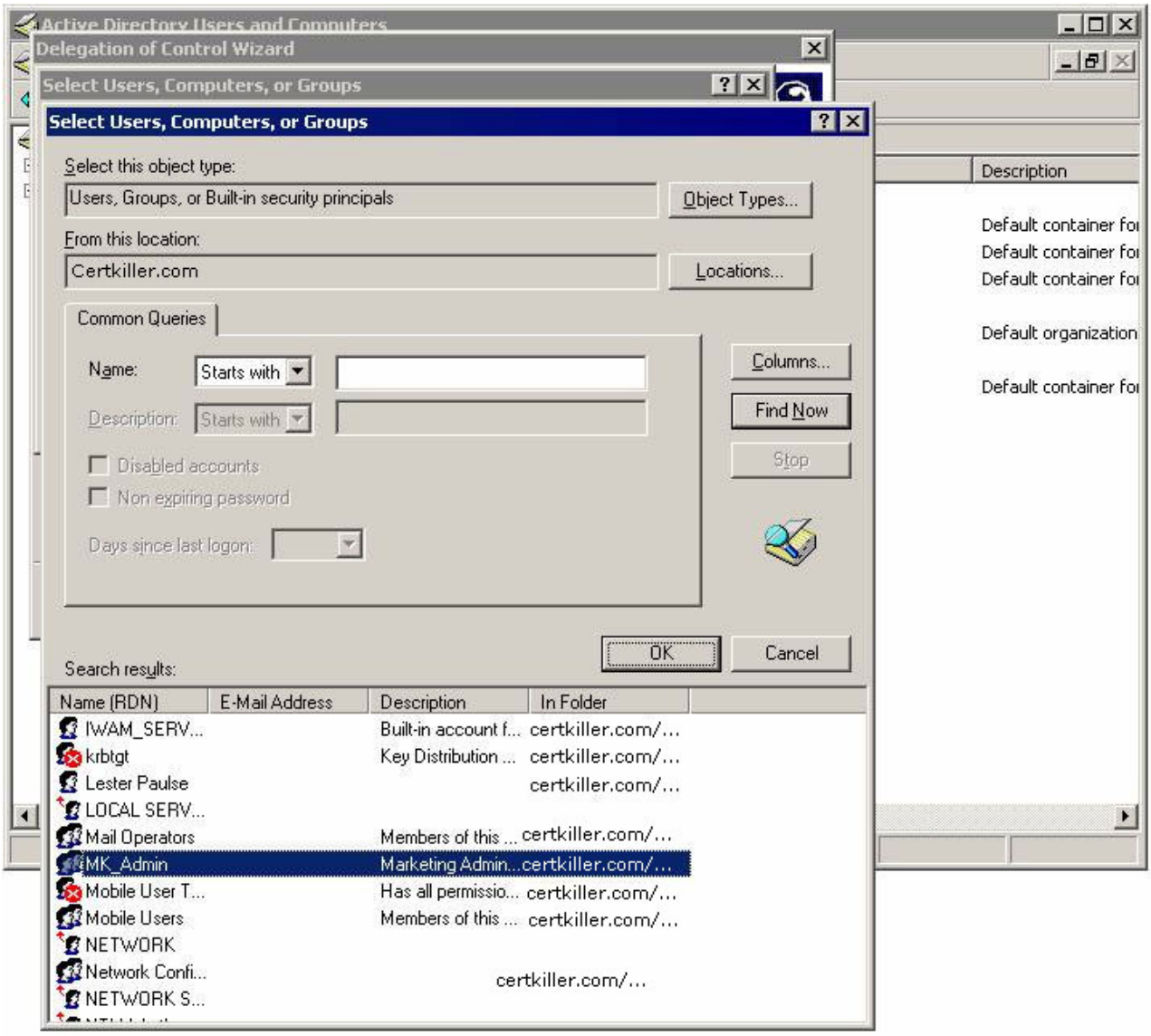
On the Select Users, Computers, or Groups dialog box, click Advanced.



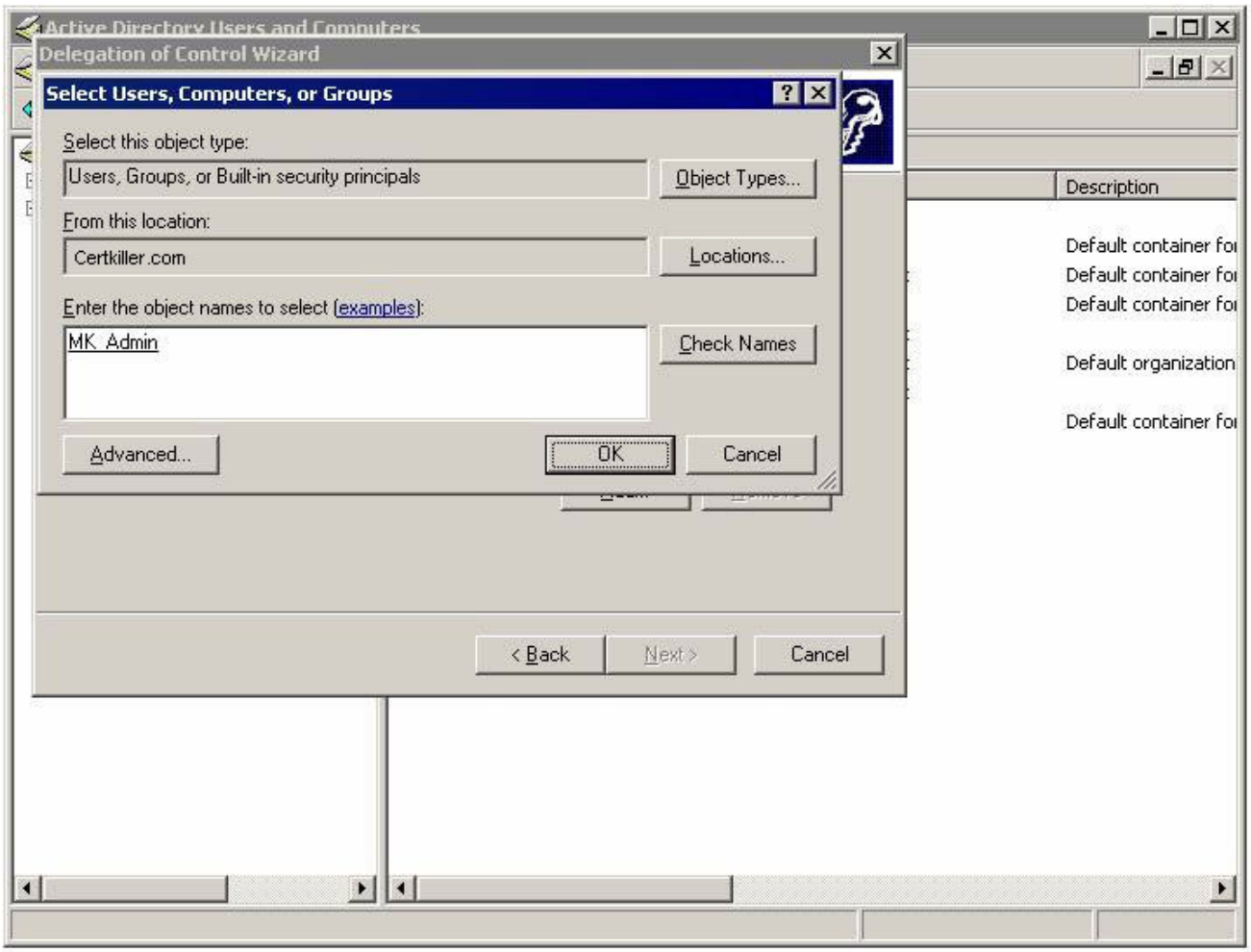
Then click Find Now.



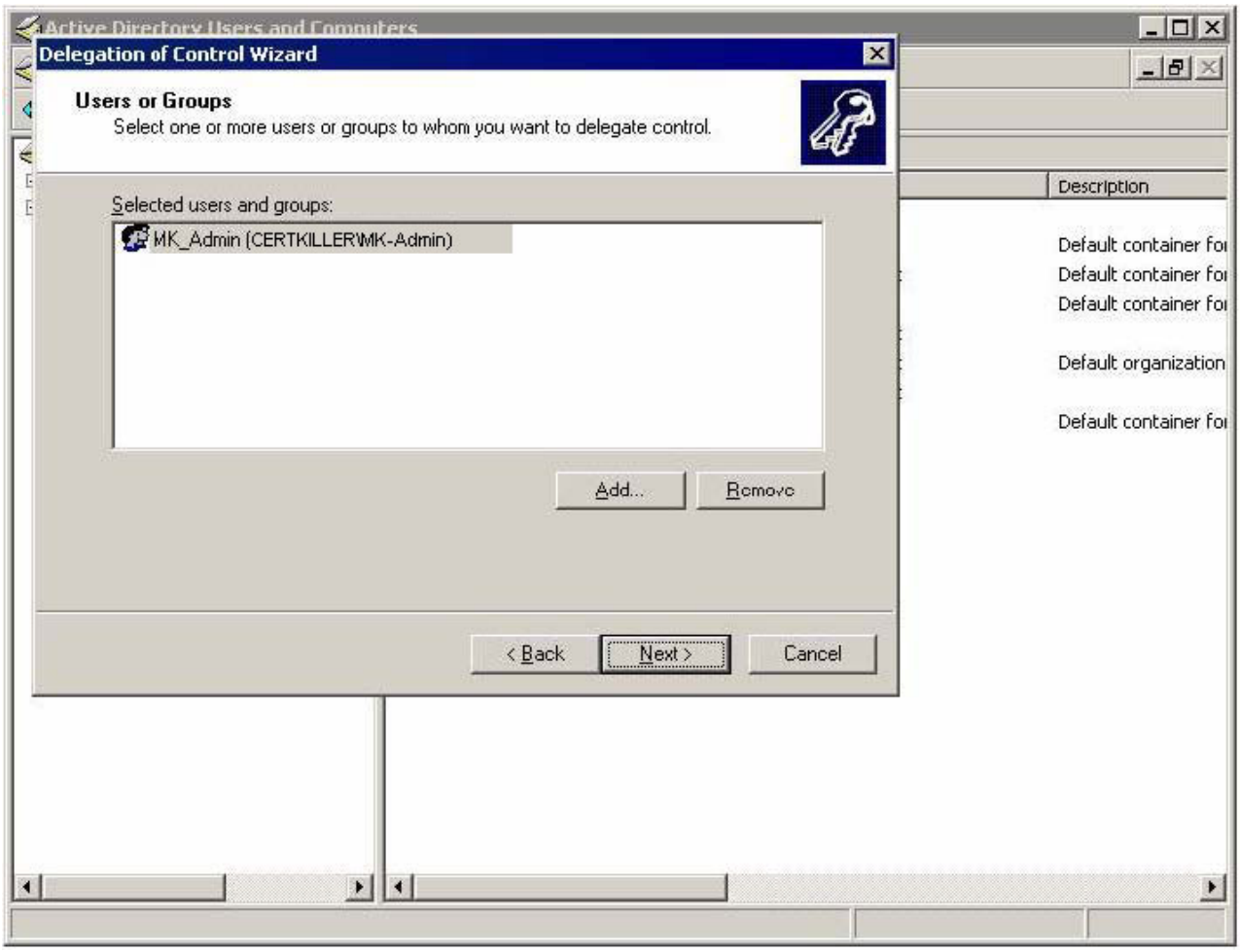
Next, scroll down to and select the MK_Admin group and click OK.



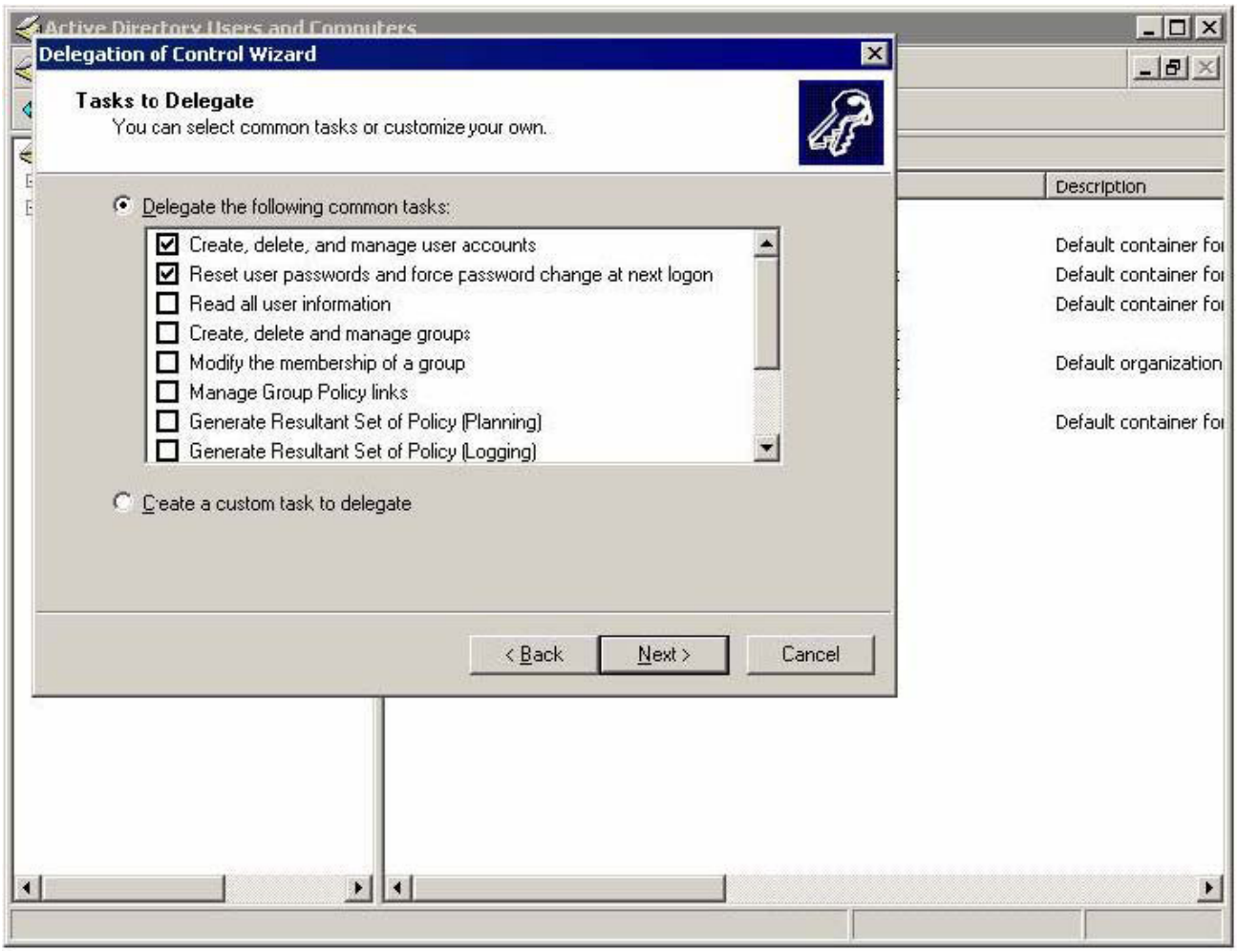
Click OK to close the Select Users, Computers, or Groups dialog box.



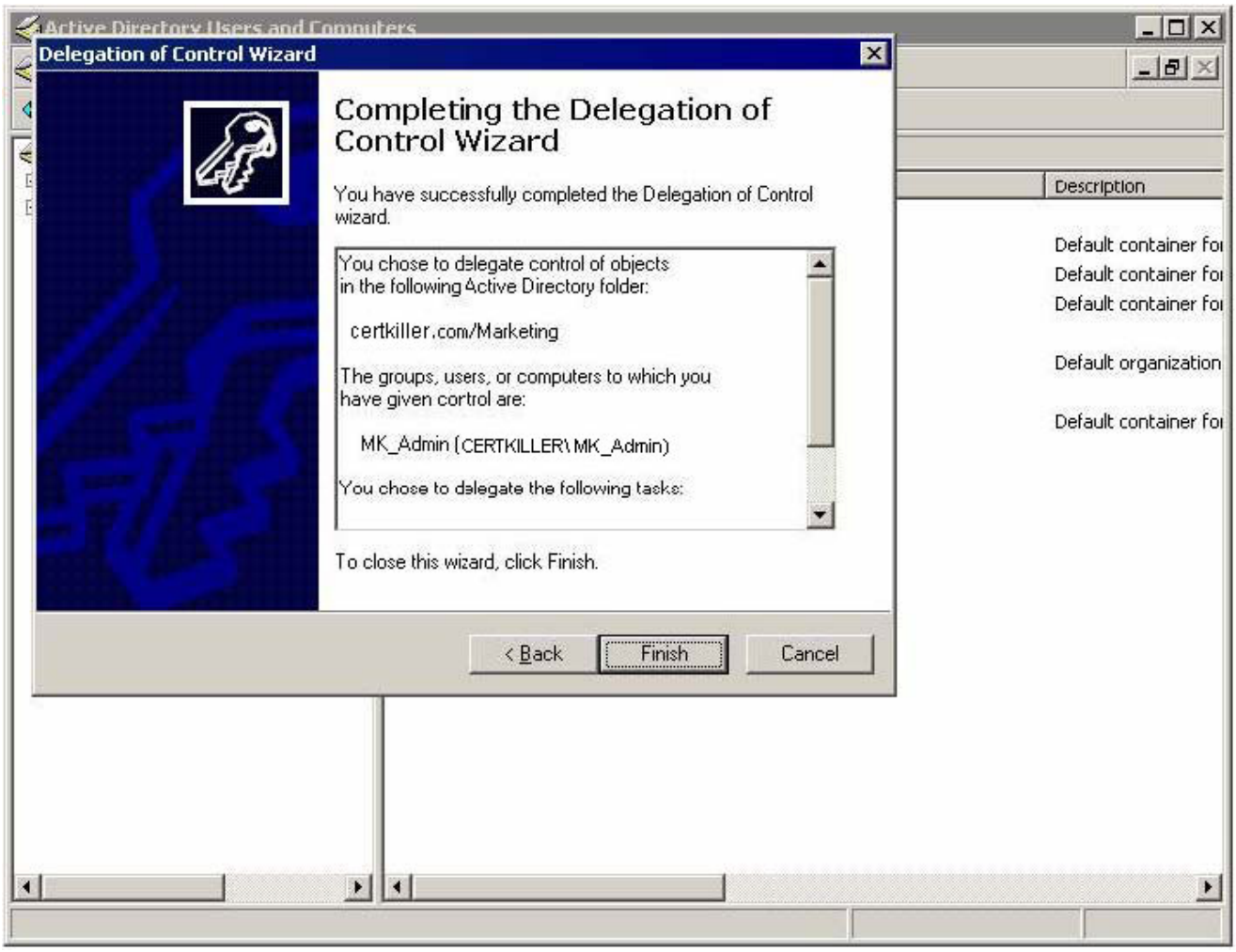
Back on the Users or Groups page of the Delegation of Control Wizard, click Next.



On the Tasks to Delegate page, select the Create, delete, and manage user accounts and the Reset user password and force password change at next logon check boxes. Then click Next.



Finally, click Finish on the Completing the Delegation of Control Wizard page.



Explanation: GPOs are stored in Active Directory, which is hosted on domain controllers. Computer-specific policies in GPOs are applied when they start up, and user-specific policies are applied to users when they log on. In this scenario, the settings should go away when the user logs off. These settings should, therefore, apply only to the users and not the computers.
This scenario requires you to minimize the number of GPOs that has to be edited. You should, therefore, configure the new name for the local administrator account for all computers in a GPO at the domain level. This GPO is the default domain policy. To prevent this setting from applying to the computers in the Sales department, you should enable Block Policy Inheritance for the Sales OU. If you enable the Block Policy Inheritance option for the Sales OU, the GPOs that are linked to the site or domain would not apply to the Sales OU.

QUESTION 20:

You work as the network engineer at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com.
Each Certkiller .com department had an organizational unit (OU) created for it.

These OUs are named to reflect the department which objects they hold, i.e. FinanceOU, ITOU, Research and DevelopmentOU, SalesOU, and MarketingOU respectively. You have been given instructions to configure settings for audit policies and user rights assignments for computers in the SalesOU. The SalesOU has a Group Policy object (GPO) linked to it.
What should you do?

A. Access the Security Templates snap-in.
B. Access the Security Configuration and Analysis snap-in.
C. Access the Resultant Set of Policy snap-in.
D. Open Group Policy Object Editor, and use Computer Configuration.

Answer: D

Explanation: To configure local account policies, such as password policy, account lockout policy, and Kerberos policy, you should navigate to and use the Computer Configuration, Windows Settings, Security Settings
, from the Group Policy Object Editor. Security Settings are also used for local policies (such as audit policies and user rights assignments), event log, restricted groups, system services, registry, and file system.
Incorrect Answers:
A: The Security Templates snap-in defines a security policy in a template.
B: The Security Configuration and Analysis snap-in is used to analyze and configure security settings using a security template.
C: The Resultant Set of Policy (RSoP) snap-in allows you to simulate a policy deployment for users and computers before applying the policies. It also allows you to view the actual policies applied to a user or computer.

QUESTION 21:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. Certkiller .com consists of four departments, named Sales, Finance, Research and Marketing. The client computers in the Finance department belong to the Finance organizational OU.
The manager of the Finance department is a user named Andy Booth. One day Andy Booth informs you that he suspects that someone is trying to gain unauthorized access to files on the client computers in the Finance department. Andy Booth asks you to identify the user account that is used to access the files. You need to accomplish this task without impacting on the other client computers. You also want to accomplish this task using the least amount of administrative effort.
What should you do?

A. Configure auditing in the Default Domain Controller Policy.
B. Configure auditing of the Everyone group for the files and folders you suspect are

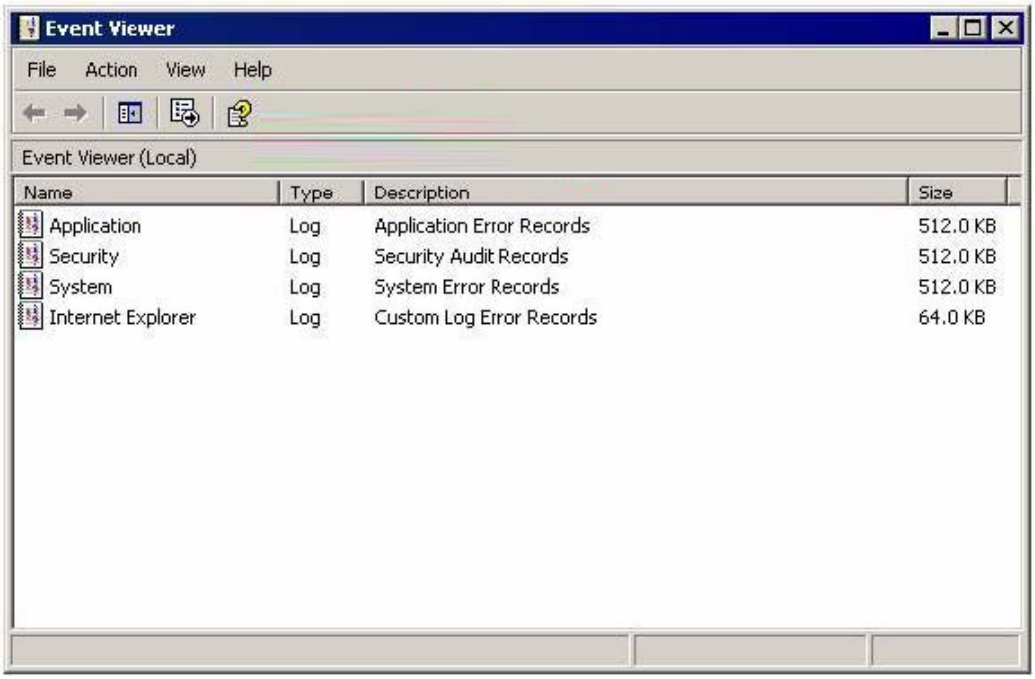
being accessed and enable an audit policy for the Finance department OU.
C. Configure auditing for each client computer in the Finance department OU.
D.
Configure auditing of the Finance group for the files and folders you suspect are being accessed.

Answer: B

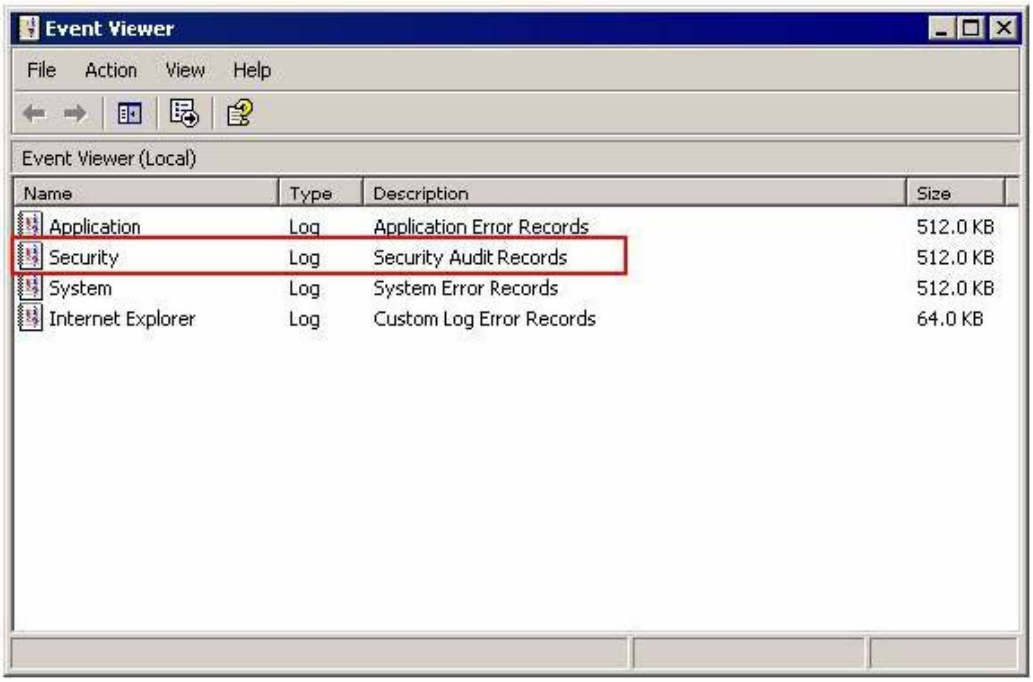
Explanation: In this scenario you are required to track file resources. Thus you should configure a GPO and link it to the Finance department OU.
Incorrect answers:
A: The Default Domain Controller Policy applies only to the Domain Controllers OU.
C: If you enabled audit only in that GPO, you would only audit the access to files, printers, registry and other recourses that are hosted on the domain controllers.
D: This option will only focus on the Finance department; the person responsible can be in any of the other departments.

QUESTION 22:

HOTSPOT
You work as the senior network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. There are currently four domain controllers on the Certkiller .com.
The Certkiller .com help desk receives complaints from users in the Finance department. The complaint is that they encounter an error message when they try to log on to the domain. Consequently you investigate the issue and then discovered that the two user accounts have been deleted. All administrators have administrative privileges assigned to manage the domain controllers and member servers in the Certkiller .com. Only administrators have the necessary permission to add and remove user accounts from the domain.
The immediate suspicion is that someone has managed to use an account that has administrative privileges assigned to delete the user accounts. Auditing is already configured to monitor and track all attempts made to access management events on the four domain controllers.
You then decide to look for entries in an event log on a domain controller that would contain information on who deleted these accounts using Event Viewer.
What should you do? (Answer by selecting the event log file you should use.)



Answer:



Explanation:
The security log event file would display information on security specific events. It would contain information on changes made to your security system, such as who deleted user accounts. The application log event file would display information on events which were logged by applications. The system event file would display information on events which were logged by system components. The Directory Access Service event log

would contain information on events that pertain to accessing directory service objects in Active Directory. The DNS log file would show you information specific to the DNS server. The File Replication Service log file would show you information specific to Active Directory replication.

QUESTION 23:

You work as the senior network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
Certkiller .com hosts a public Web site on a Web server named Certkiller -SR15. The Web site is used by customers to place orders for products offered for sale by the company. The management of Certkiller -SR15 is your responsibility. You have to ensure that the public Web site is available 24/7. For the past few weeks you notice that three services running on Certkiller -SR15 have stopped intermittently. Consequently the Certkiller .com help desk has been inundated with complaints. You must determine the reason for the failure of these services on the Web server. Only then will you get an indication of what is required to ensure that customers can access the Web site whenever they want to purchase products. You plan to use Event Viewer to obtain the required information. You want to examine information on all three services. You want to use the minimum amount of administrative effort to accomplish your task
How should you go about using Event Viewer?

A. In Event Viewer, open the Application log entries.
Create an Application log view for each service.
B. In Event Viewer, open the Security log entries.
Create a Security log view for each service.
C. Open three instances of Event Viewer on Certkiller -SR15 to view the information.
D. Open Event Viewer from three computers.
Use a different computer to collect information on each service.

Answer: A

Explanation: Log views allow you to view a subset of information of any specific event log in Event Viewer. To view information on why services have stopped running on Certkiller -SR15 using the minimum amount of administrative effort, you need to first access the Application log in Event Viewer. After this, you can create a new Application log view for each service that you want to obtain information on.
Incorrect Answers:
B: Security log entries do not provide information on why a service stopped running on a server. The security log provides information on security specific events.
C: This is unnecessary and quite administrative intensive. You only need to open one instance of Event Viewer and then create the necessary log views.

D: Using three different computers is also quite administrative intensive. You only need to open one instance of Event Viewer using one computer, and then create the necessary application views.

QUESTION 24:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com which has multiple sites. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
Certkiller .com has headquarters in London and branch offices in Paris, Berlin and Milan. Each Certkiller .com location/office is configured as a separate Active Directory site, with each site having its own Internet connection through an ISP.
WAN links connect the Paris, Berlin and Milan branch offices to the London headquarters office. WAN bandwidth at each office is limited. Each site has Software Update Services (SUS) installed on one of its local servers. Each SUS server is configured to synchronize by using the default settings.
In your solution you need to keep in mind to minimize bandwidth usage due to the limited Wide Area Network (WAN) bandwidth at each office as well as the amount of time required to download end deploy updates.
What should you do?

A. Configure each SUS server at the three branch offices to download updates from the SUS server at the London headquarters office. .
B. Configure each SUS server to download only the locales that are needed.
C. Limit the file transfer size by configuring Background Intelligent Transfer Service (BITS).
D. Delete incomplete transfer jobs after a specified amount of time by configuring Background Intelligent Transfer Service (BITS).

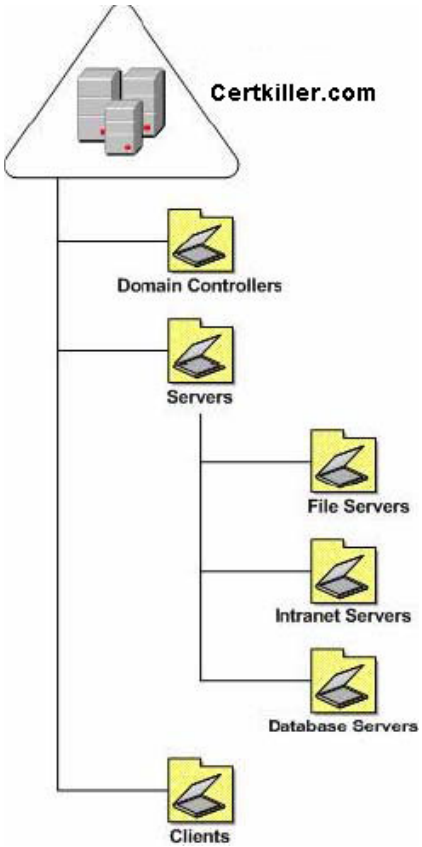
Answer: B

Explanation: You can minimize bandwidth usage and theamount of time needed to download and deploy updates by configuring your SUS servers to download only the locales that are needed. This will prevent the downloading and synchronizing of multiple copies of the same updates, but in different languages; which will conserve bandwidth. In fact, when you only select one or two locales required on your network, you reduce the amount of initial synchronization of your SUS servers drastically. You should then configure clients to download updates from their local SUS servers. This will prevent updates from being sent over the WAN links that connect the Certkiller .com branch offices.
Incorrect Answers:
A: Whether the three branch office SUS servers download updates from the London SUS server is irrelevant because the same quantity of data will be sent through the WAN links to the SUS servers.
C: You should not limit the file transfer size because the updates may be more than your

predefined file transfer size limit.
D: Deleting incomplete jobs will not minimize the amount of time needed to download and deploy updates.

QUESTION 25:

You work as a network domain administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. The Certkiller .com network contains twenty-five Windows Server 2003 servers and 5,200 client computers running Windows 2000 Professional:
1. Two of the servers function as domain controllers.
2. The rest are used as file servers, intranet servers, or database servers.
The Certkiller .com organization unit (OU) structure is based on the defined server roles.
The relevant portion of the Active Directory structure is illustrated in the Exhibit below:



You are responsible for the management of security baseline settings. Other than the domain controllers, all servers should be furnished with security baseline settings. To this end you create:
1. A security template named SRsecurity.inf. SRsecurity.inf includes the required NTFS- and registry permissions for all the servers, intranet server, as well as the database servers.
2. A security template named FSRsecurity.inf
3. A security template named IntSRsecurity.inf

4. A security template named DBserversecurity.inf
You received instruction to deploy these security templates with the least amount of administrative effort.
What should you do to accomplish this task? (Each correct answer presents part of the solution. Choose two.)

A. Create a GPO
Link it to the domain.
Import the SRsecurity.inf template into the new GPO.
B. Create a new GPO for the File Servers-, the Intranet Server- and the Database Servers OUs respectively.
Link each GPO to the File Servers-, the Intranet Server- and the Database Servers OUs respectively.
Import the FSRsecurity.inf, the IntSRsecurity.inf and the DBserversecurity.inf security templates into their respectiveGPOs.
C. Create a GPO
Link it to the File Servers-, the Intranet Server- and the Database Servers OUs.
Import the SRsecurity.inf template into the new GPO.
D. Create a GPO
Link it to the Servers OU.
Import the SRsecurity.inf template into the new GPO.
E. Create a new GPO for the File Servers-, the Intranet Server- and the Database Servers OUs respectively.
Link each GPO to the Servers OUs.
Import the FSRsecurity.inf, the IntSRsecurity.inf and the DBserversecurity.inf security templates into their respectiveGPOs.

Answer: B, D

Explanation: The SRsecurity.inf security template should be applied to all servers located in the Servers OU. To this end you need to create a GPO, link it to the Servers OU and import the appropriate security template into the GPO. This way the SRsecurity.inf settings will apply to all the servers in the Servers OU. In the same fashion you should link the respective security templates to the respective newly created GPOs to have them applied to the correct groups of servers. These methods represent the least amount of administrative effort.
Incorrect answers:
A: This GPO should be linked to the Servers OU and not the domain. This is not a recommended practice.
C: GPOs that contain role-specific security settings should be applied at the OU level to ensure that those security settings will apply to only the members of that specific OU.
E: Linking each of the different GPOs to the Servers OU will not ensure that the servers of a specific type of server receive the appropriate server-specific security settings.

QUESTION 26:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. The Certkiller .com network contains ten Windows Server 2003 computers and 1,200 client computers running Windows XP Professional. The servers, the domain controllers, and the client computers form their own OUs respectively. The client computers comprises of desktop computers as well as laptop computers.
The Certkiller .com written security policy states that Encrypting File System (EFS) should only be implemented on the client computers. You then create a domain account to serve as the data recovery agent for the entire domain.
All the security settings that are required on all the computers in the domain are contained in a Group Policy Object (GPO) named DomainSecGPO.
DomainSecGPO is currently set up to allow users to encrypt files with EFS. You need to configure the appropriate settings to ensure that the Certkiller .com written security policy is adhered to. You need to accomplish this task with the least amount of administrative effort.
What should you do? (Each correct answer presents part of the solution. Choose all that apply.)

A. Create a new GPO that allows users to use EFS.
B. Configure DomainSec GPO to prevent users from using EFS.
C. Create a new GPO that prevents users to use EFS.
D. Configure DomainSec GPO to allow users to use EFS.
E. Link the new GPO to the Clients OU.
F. Link the new GPO to the Desktop computers and Portable computers OUs.

Answer: A, B, E

Explanation: EFS can be used to encrypt data on NTFS volumes. DomainSecGPO is configured at domain level. This means that all computers including the servers support EFS. This violates the Certkiller .com written security policy. You should thus disable EFS support on domain level by configuring DomainSecGPO to prevent users from using EFS. Then to enable client computers to encrypt data, you should create a new GPO that supports EFS and link it to the Clients OU.
Incorrect answers:
C: This would be incorrect since the users who make use of the Clients OU will require making use of EFS so as to comply with the written security policy.
D: This is a superfluous option. This is in violation of the Certkiller .com written security policy since all computers, servers and client computers are already supporting EFS. This should in fact be changed.
F: This is incorrect the GPO should be linked to the Clients OU

QUESTION 27:

You work as the network security administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. The Certkiller .com network contains twenty Windows Server 2003

computers and 1,500 client computers of which 950 is running Windows XP Professional, 300 is running Windows 2000 Professional and 250 is running Windows NT Workstation 4.0.
You are responsible for the implementation of security templates at Certkiller .com. All client computer accounts on the Certkiller .com network are contained in an Organizational Unit (OU) named Clients OU. All Certkiller .com employees enjoy Users group membership. You created a Group Policy Object (GPO) named Clients_GPO and link it to the Clients OU. You then import the Securews.inf security template into the Clients_GPO. You then perform a clean installation of Windows XP Professional on all the Windows NT Workstation 4.0 client computers as well as the Windows 2000 Professional computers after which you verify that Clients_GPO is applied to each of these computers.
The next morning you received reports from several Certkiller .com users complaining that they are unable to run an application on their Windows XP Professional client computers, instead they encounter an error message that informs them that they do not have the appropriate permissions to run that particular application. This application stored user data in the Program Files folder structure. Previously these users had no trouble running this specific application on their Windows NT Workstation 4.0 computers.
You need to perform several tasks:
1. Ensure that the application will run on Windows XP Professional computers without compromising the security settings in the Securews.inf security template.
2. You should not affect the security settings that apply to the other computers in the domain.
3. You should not grant the members with the problems to access the application more permissions than is necessary.
What should you do?

A. Make these members part of the Administrators group on their computers.
B. Make these members part of the local Power Users group on their computers.
C. The Compatws.inf security template should be imported into the Clients_GPO.
D. The Setup security.inf security template should be imported into the Clients_GPO.

Answer: B

Explanation: The default security settings for the Windows XP Professional operating system are preventing the Users group from being granted too much authority. However, to run legacy/customized applications under Windows XP Professional, members of the Users group must be granted the same kind of user right and permissions as members of the Power Users group.
Incorrect answers:
A: Making these members part of the Administrators group would be granting them more permissions than is necessary.
C: Applying the Compatws.inf security template would overwrite the settings that have been applied by the securews.inf security template. The question states pertinently that you should not alter the existing security settings.

D: Applying the Setup security.inf security template will also overwrite the settings that have been applied by the securews.inf security template. Furthermore, it is not recommended to apply this template through using a GPO.

QUESTION 28:

You work as the network security administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. The Certkiller .com network contains ten Windows Server 2003 computers and 1,200 client computers of which 750 is running Windows XP Professional, 250 is running Windows 2000 Professional and 200 is running Windows NT Workstation 4.0.
You job description includes the implementation of security templates. All client computer accounts on the Certkiller .com network are contained in an Organizational Unit (OU) named Clients OU. All Certkiller .com employees enjoy Users group membership. You created a Group Policy Object (GPO) named Clients_GPO and link it to the Clients OU. You then import the Securews.inf security template into the Clients_GPO. You then perform a clean installation of Windows XP Professional on all the Windows NT Workstation 4.0 client computers as well as the Windows 2000 Professional computers after which you verify that Clients_GPO is applied to each of these computers.
The morning after you performed the latter, you received reports from several Certkiller .com users complaining that they are unable to run an application on their Windows XP Professional computers. They encounter an error message instead that states that they do not have the appropriate permissions to run that particular application. This application stored user data in the Program Files folder structure. Previously these users had no trouble running this specific application on their Windows NT Workstation 4.0 computers.
You received instruction to ensure that the application will run on Windows XP Professional computers without compromising the security settings in the Securews.inf security template. Further more, you should not affect the security settings that apply to the other computers in the domain or grant the members with the problems to access the application with more permissions than is necessary.
What should you do to accomplish this task?

A. Give these members Administrators group membership on their computers.
B. Give these members local Power Users group membership on their computers.
C. Create a new security template that merges the Securews.inf and the Compatws.inf security templates and then import the new template into the Clients_GPO.
D. Create a new security template that merges the Securews.inf and the Setup security.inf security templates and then import the new template into the Clients_GPO.

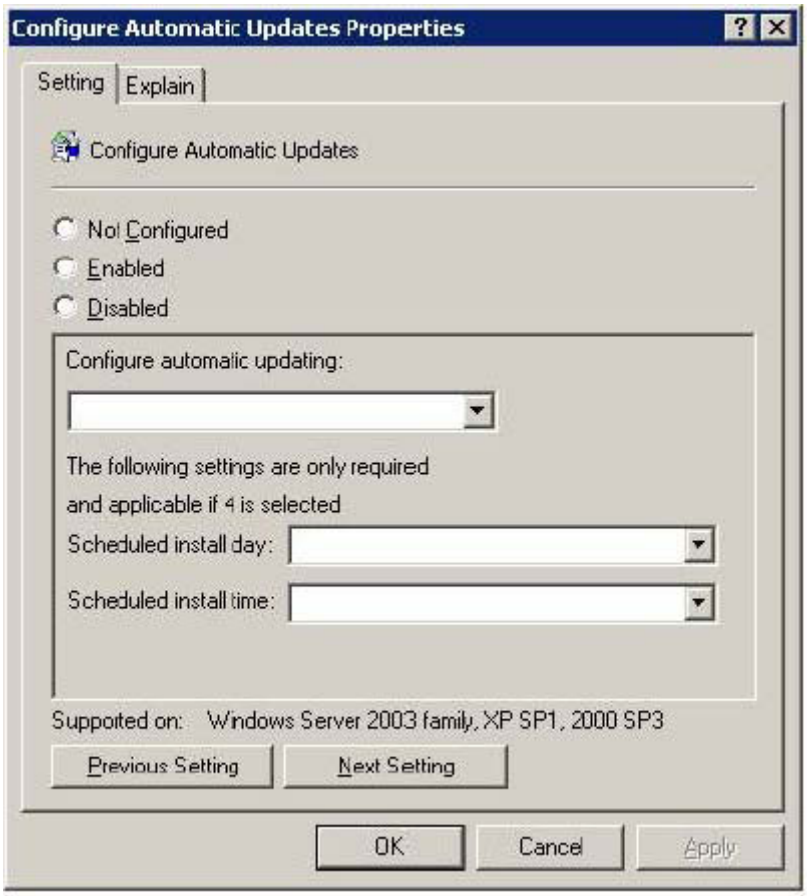
Answer: B

Explanation: The default security settings for the Windows XP Professional operating system are preventing the Users group from being granted too much authority. However,

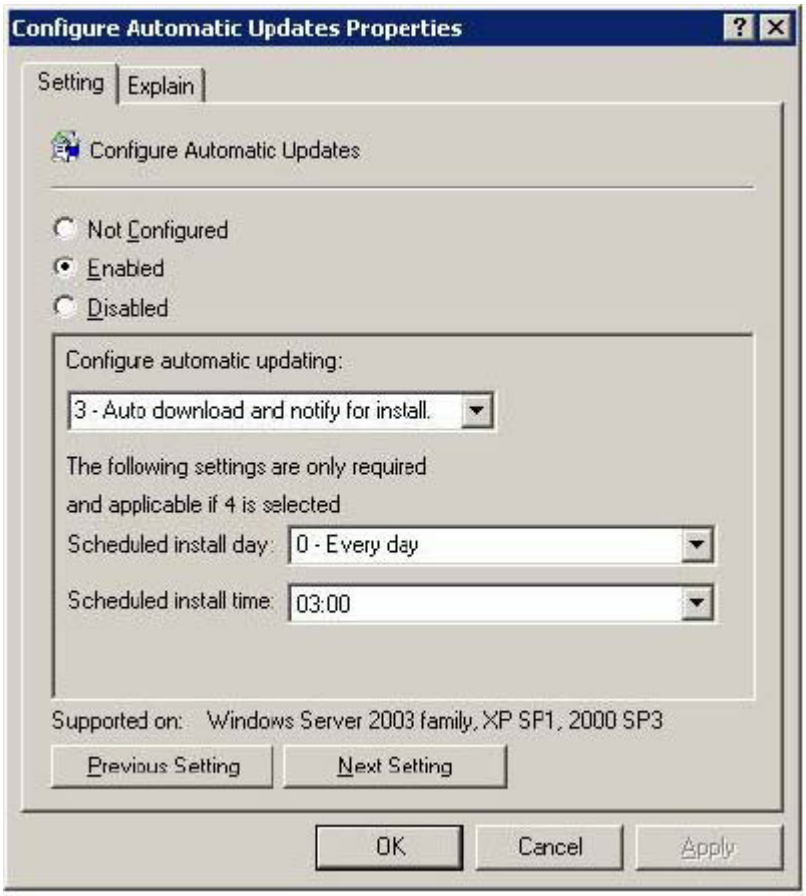
to run legacy/customized applications under Windows XP Professional, members of the Users group must be granted the same kind of user right and permissions as members of the Power Users group.
Incorrect answers:
A: Making these members part of the Administrators group would be granting them more permissions than is necessary.
C, D: Creating any new security template to import into the Clients_GPO will not ensure that the existing security settings will be maintained.

QUESTION 29:

SIMULATION
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
You are planning to implement a new security and software update infrastructure for Certkiller .com. A SUS server named Certkiller -SR22 will be deployed in the network. Certkiller -SR22 will be configured to download security updates from the Windows Update Web site and only client computers will be configured to download security updates from Certkiller -SR22.
The Certkiller .com written security policy only allows software to be installed on member servers if it has been tested and approved by a network administrator. You want all member servers to download service packs and security updates directly from the Windows Update Web site.
You create a new Group Policy Object (GPO) and link it to the Servers OU. You start configuring the GPO by accessing the Configure Automatic Updates policy to configure the settings that will allow servers to obtain service updates from Windows Update Web site, while still ensuring that the Certkiller .com written security policy is enforced.
What should you do? To answer, select the appropriate configuration options in the accompanying dialog box.


Configure Automatic Updates Properties
Setting
Explain
Configure Automatic Updates
Not Configured
Enabled
Disabled
Configure automatic updating:
The following settings are only required
and applicable if 4 is selected
Scheduled install day:
Scheduled install time:
Supported on: Windows Server 2003 family, XP SP1, 2000 SP3
Previous Setting
Next Setting
OK
Cancel
Apply

Answer:



Explanation: You want all member servers to obtain service pack updates directly from the Windows Update Web site. You should therefore enable the Configure Automatic Updates policy by selecting theEnable button. This will ensure that server computers automatically receive the latest security updates and service packs from the Windows Update Web site.
The three options available in the Configure automatic updating drop-down list box are:
1. Notify for download and notify for install
2. Auto download and notify for install
3. Auto download and schedule the install
Since the Certkiller .com written security policy only allows software to be installed on network servers if it has been tested and approved by a network administrator, you need to specify the Auto download and notify for install option. While the available updates will be automatically downloaded from the Windows Update Web site, an administrator's intervention will be needed to implement it on the server, which is in accordance with the Certkiller .com security policy.

QUESTION 30:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client

computers run Windows XP Professional.
The Certkiller .com written security policy states that no unauthorized VBScript files are to be deployed and executed on Certkiller .com client computers. All VBScript files that contain scripts which are authorized to be executed on client computers are located on several Certkiller .com servers.
You must configure a software restriction policy that will comply with the Certkiller .com written security policy. To this end you plan to configure the default security level as Unrestricted in your new software restriction policy. You do not want to modify the software restriction policy each time that a new VBScript script is authorized to be run on your client computers.
What should you do? (Each correct answer presents part of the solution. Choose three.)

A. Create a new Path rule.
Set the path to be *.vbs.
Set the security level to Disallowed.
B. Create a new Internet zone rule for authorized VBScript files.
Set the security level to Unrestricted.
C. Create a new Hash rule for authorized VBScript files.
Set the security level to Unrestricted.
D. Authorize each .vbs file by digitally signing it.
E. Create a new Certificate rule.
Set the security level to Unrestricted.

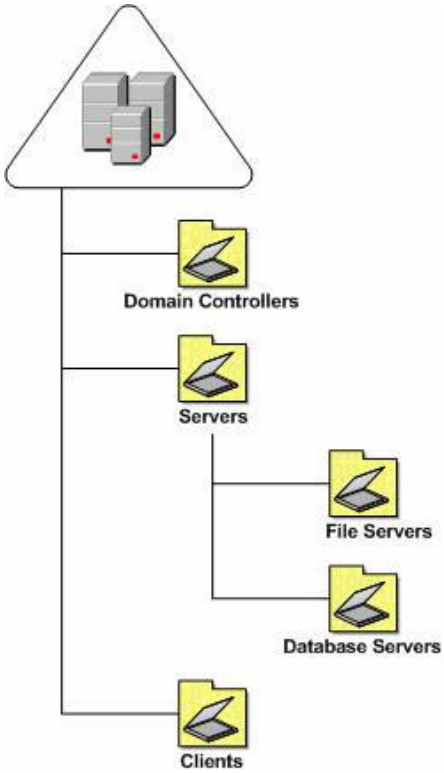
Answer: A, D, E

Explanation: There are four different types of software restriction policy rules. Because more than one rule can be applied to one file, the priority of these rules is as follows (highest to lowest):
1. Hash rules (highest priority)
2. Certificate rules take priority over Path rules.
3. Path rules take priority over Internet zone rules.
4. Internet zone rules (lowest priority)
To ensure that no unauthorized .vbs scripts are run on client computers, you need to create a new path rule, set the path to be *.vbs, and set the security level to Disallowed. After this, you need to ensure that each .vbs file that is authorized to run on client computers is digitally signed. You then need to create a new Certificate rule and set the security level to Unrestricted. Because Certificate rules take priority over Path rules, the .vbs files that are authorized WILL be allowed to run on client computers, while unauthorized files will NOT be allowed to be run.
Incorrect Answers:
B: Because Hash rules have the highest propriety, you would need to specify each authorized .vbs file in the rule. Then, whenever a new authorized .vbs file becomes available, you would need to modify the rule. The question states that you do not want to modify the software restriction policy each time that a new VBScript file is authorized to

be run on your client computers
C: Internet zone rules apply to Windows Installer .msi files.

QUESTION 31:

You work as the network security administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. Certkiller .com has its headquarters in Chicago and a branch office in Dallas. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
Between the Internet and the internal network a demilitarized zone (DMZ) segment has been configured. This DMZ contains three servers which are configured in a Web farm and are not member servers.
The Intranet consists of all the computers that are part of the domain. It contains domain controllers and 10 member servers. Two of these member servers are configured to run SQL Server 2000. There are no Web servers on the intranet. The Exhibit below illustrates the Active Directory Structure currently applied:



All the policies in operation in the intranet are applied via Group Policy objects (GPOs). You have received instruction to implement a new security template that will affect all the Web Servers.
What should you do to accomplish this task? (Each correct answer presents part of the solution. Choose two.)

A. Create a Web Servers OU in the Servers OU and place the computer accounts of the three Web Servers in it. Then create a GPO and import the new security template into it.
B. Use the Secedit.exe utility to create a batch file that contains the new security

template.
C. Run the batch file on the three Web servers in the DMZ.
D. Create a GPO and import the new security template into it.
E. Link the GPO containing the security template to the Domain Controllers OU.
F. Link the GPO containing the security template to the Servers OU.

Answer: B, C

Explanation: You should make use of the Secedit.exe utility to create a batch file that contains the new security template. After which you should run the batch file on the three Web servers in the DMZ. Since these servers do not form part of the Active Directory domain you can use Secedit.exe to create and apply templates.
Incorrect answers:
A: It is not necessary to create an OU especially for the Web servers. These servers are in a DMZ and as such does not form part of the Active Directory domain. Placing them in an OU in the Servers OU will pose an unnecessary security risk that would make the DMZ null and void.
D: This option would only work together with either option E or F which is both wrong.
E: The Web servers are not part of the Domain Controllers OU. The result would be that the GPO would apply to the Domain Controllers and not the Web servers.
F: The Web servers are not part of the Servers OU. The result would be that the GPO would apply to the Domain Controllers and not the Web servers.

QUESTION 32:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All domain controllers and member servers on the Certkiller .com network run Windows Server 2003. Half of the client computers run either Windows XP Professional or Windows 2000 Professional. The other half runs either Windows NT 4.0 Workstation or Windows 98.
The Certkiller .com written security policy only allows Kerberos and NT LAN Manager Version 2 (NTLMv2) authentication protocols to be used for access authentication to resources. To this end you perform the configurations to comply with the Certkiller .com written security policy.
While monitoring network traffic, you notice that network connection made from only Windows XP Professional and Windows 2000 Professional client computers are authenticated through Kerberos or the NTLMv2 authentication protocol. No connections initiated from client computers running Windows NT 4.0 Workstation and Windows 98 are authenticated through either of the approved authentication protocols.
You need to ensure that all client computer operating systems comply with the Certkiller .com written security policy with the least amount of administrative effort Take care not to incur any additional unnecessary expenses.
What should you do? (Each correct answer presents only part of the complete solution. Choose two.)

A. Install Active Directory client software on all Windows 98 client computers.
B. Install Active Directory client software on all Windows NT 4.0 Workstation client computers.
C. Install the latest service pack on all Windows NT 4.0 Workstation client computers.
D. Install the latest service pack on all Windows 98 client computers.
E. Upgrade all Windows NT 4.0 Workstation and Windows 98 client computers to Windows XP Professional.

Answer: A, C

Explanation: Active Directory client software
must be installed on all Windows 98 client computers if you want these computers to authenticate using NTLMv2. Kerberos authentication can be used by clients and servers running the following operating systems (OSs): Windows 2000, Windows XP Professional, Windows Server 2003. Windows 2000, Windows XP Professional, and Windows Server 2003 computers who are members of a Windows 2000 or Windows Server 2003 domain use the Kerberos protocol for network authentication for domain resources. This is the default configuration for these domains. When a down level client attempts to access a Kerberos secured resource, NTLM authentication is used; and not Kerberos authentication. Kerberos authentication though offers improved security over the standard NTLM authentication protocol.
NTLM authentication protocol employs the challenge-response authentication strategy (the user is challenged to supply unique confidential information) to authenticate the users/computers running Windows Me OS, earlier OSs, and computers running Windows 2000 or later who are not domain members. NTLMv2 uses 128-bit encryption for security, and is usually used to connect to servers running Windows 2000, Windows XP and Windows NT with Service Pack 4 or later.
Incorrect answers:
B: You do not have to install Active Directory client software on all Windows NT 4.0 Workstation client computers to enable them to authenticate using NTLMv2. Only Service Pack 4 or later has to be installed on the client computers.
D: Windows 98 client computers need to have Active Directory client software installed before they will be able to participate in NTLMv2 authentication.
E: There is no need to upgrade your older client computer operating systems before they can use NTLMv2. This is unnecessary and would require more administrative effort than just installing the necessary components for Windows NT 4.0 Workstation and Windows 98 client computers

---

QUESTION 33:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network contains file and print servers, Web servers, and

terminal servers. A new Certkiller .com security policy requires that:
1.
Each server, regardless of its type, must be configured with security settings that are specific to that type of server.
2. Certain baseline settings are applicable to all servers and server-specific settings should take precedence if it conflicts with the settings for all servers.
You create the security templates listed below:
1. AllSrv.inf
2. WebSrv.inf
3. FPS.inf
4. TS.inf
You need to ensure that these security templates are applied in accordance with Certkiller .com's new security policy, without affecting client computers.
What should you do?

A. Import the templates into a GPO in the following order: AllSrv.inf, WebSrv.inf, FPS.inf, TS.inf.
Then link the GPO to the domain.
B. Import each template into a separate GPO.
Then link the GPOs to the domain in the following order: WebSrv.inf, FPS.inf, TS.inf, AllSrv.inf.
C. Create an OU for each server type, and move the computer accounts for that server to its OU.
Then import the AllSrv.inf template into a GPO.
Then import the template for that server type to its corresponding GPO and link the GPO to OU.
D. Import the AllSrv.inf template into a GPO and link the GPO to the domain.
Create an OU for each server type, move the computer accounts for that server to its OU.
Then import the template for that server type to its corresponding GPO and link the GPO to OU.

Answer: C

Explanation: A security template is a text file that contains settings for certain policies, located under the Computer Configuration/Windows Settings/Security Settings
node in the Group Policy object (GPO) namespace that can be imported into any Active Directory-based GPO and, thereby, applied to the computers that are targeted by that GPO. In this scenario, you should place each type of member server in a separate OU because each server type must be configured differently. Since a server role-specific template has to overwrite conflicting settings from the AllSrv.inf template, you should apply the AllSrv.inf template first. To meet this requirement, you can create a GPO for each type of server, link it to the corresponding OU, and import the AllSrv.inf template followed by the server role-specific template.
Incorrect Answers:

A: If you import all the templates into the same GPO, the settings from the last template would overwrite the settings that were imported from the other templates. If you link this GPO to the domain, that hybrid configuration would be applied to all computers in the domain, including client computers.
B: If you used this option, the settings from the GPO with higher precedence would overwrite the conflicting settings from lower-priority GPOs, and the resulting uniform configuration would be applied to all computers, including client computers.
D: If you applied the AllSrv.inf template to the domain and applied each server role-specific template to the OU that contains the corresponding server, all member servers would be configured correctly because OU-level GPOs would have higher precedence than domain-level GPOs. This option would, however, affect client computers as well.

QUESTION 34:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003. Half the client computers run Windows XP Professional, and the rest run Windows NT 4.0 Workstation or Windows 98. The latest available service packs are installed on all client computers.
During the past few weeks several unauthorized attempts have been made to access confidential data communications between Certkiller .com client computers and servers. You receive instruction to implement a solution which will verify and ensure that data has not been changed while in transit through the network.
You must ensure that there is no tampering of packets traversing the network between
Certkiller .com servers and client computers. You do not want to upgrade any legacy client computers to Windows XP Professional to achieve your goal.
What should you do? (Each correct answer presents part of the solution. Choose two.)

A. Enable Server Message Block (SMB) signing on all client computers.
B. Enable Server Message Block (SMB) signing on all servers.
C. Enable IP Security (IPSec).
D. Implement Kerberos version 5 authentication protocol.

Answer: A, B

Explanation: Server Message Block (SMB) signing ensures the integrity of data in transit between a client and a server, and the authenticity of a user and the server on which the data resides. To prevent the modification of packets while in transit, SMB supports the digital signing of SMB packets. To protect against the impersonation of clients and servers in high security networking environments that include Windows 2000 based clients and down-level Windows clients, you should implement SMB signing. If you want all communication with a server to require

SMB signing; the server must be configured to enable and require the utilization of SMB signing and client computers must be configured to enable or require SMB signing.
Incorrect answers:
C: IPSec is NOT supported in Windows NT 4.0 Workstation or Windows 98.
D: Kerberos version 5 authentication is used to authenticate access to domain resources.

QUESTION 35:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003. The Certkiller .com network contains servers that are configured to function as domain controllers named Certkiller -DC01 and Certkiller -DC02. You are responsible for setting up security by means of applying security templates.
You are currently in the process of setting up two secure application servers named Certkiller -AS06 and Certkiller -AS07, which needs to have special security policy settings configured. You have installed Windows Server 2003 as well as a custom application on these servers. In addition to the policies set by the Hisecws.inf security template, you create a custom security template that locks down the server further.
You need to ensure that the appropriate security policy is applied to the computer in the correct order.
What should you do?

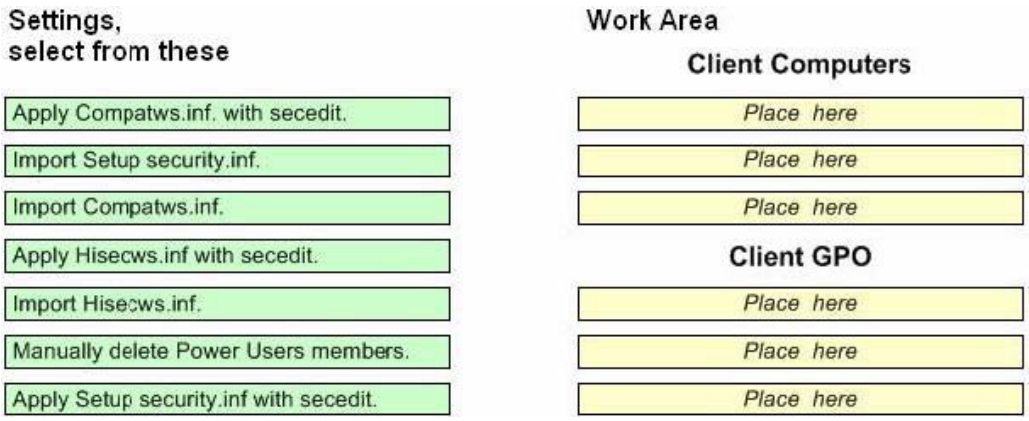
A. You should first apply the Hisecws.inf security template, followed by the custom security template, and then the Setup security.inf security template.
B. You should first apply the Hisecws.inf security template, and then the custom security template.
C. You should first apply the Securews.inf security template, followed by the Hisecws.inf security template, and then the custom security template.
D. You should first apply the Setup security.inf security template, followed by the Hisecws.inf security template, and then the custom security template.

Answer: B

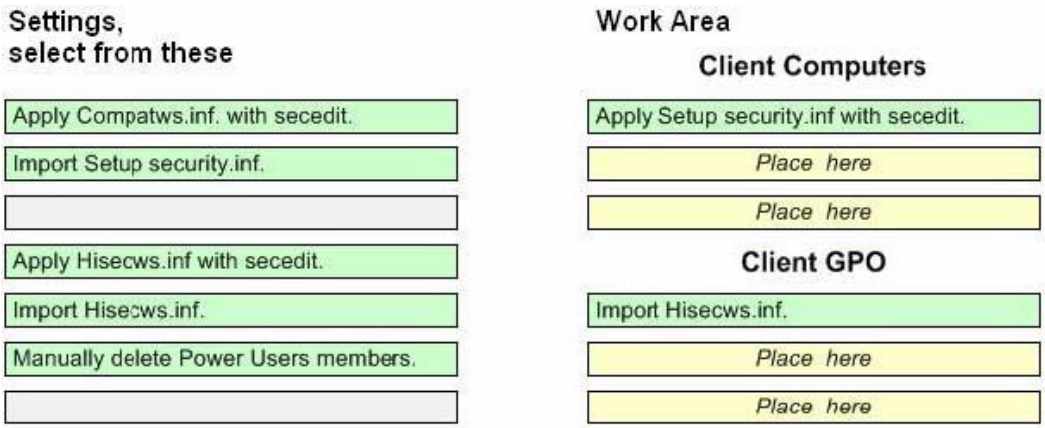
Explanation: The Hisecws.inf security template should be applied first, because the custom security template is designed to extend the changes made by the Hisecws.inf template.
Incorrect Answers:
A: Using this option would in effect unlock the server.
C: It is unnecessary to apply the Securews.inf template, because it is less secure than the Hisecws.inf security template.
D: The Setup security.inf template is the default security template and is configured automatically when Windows Server 2003 is installed.

QUESTION 36:

DRAG DROP
You have recently been employed as a network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003. Half the client computers run Windows 2000 Professional, and the rest run Windows XP Professional. All client computers are included in an OU named Client Computers, which has a GPO linked to it.
The former network administrator made the Domain Users group a member of the local Power Users group on each client computer to allow users to run a custom legacy application that does not comply with the Designed for Windows Logo Program for Software. Consequently this configuration led to various problems such as users making unauthorized modifications to their computers. You notice that the former network administrator also directly edited security policy settings on numerous client computers.
Your first task is to address these undesirable and difficult-to-maintain security configurations that were implemented by the former network administrator. However, you need to ensure that your solution does not impact negatively on network or domain performance.
What should you do?
To answer, select the appropriate options from the Available Actions box and place it under the correct node.



Answer:



Explanation:
You need to apply the Setup security.inf security template to revert each client to the default security. Microsoft specifies that Setup security.inf should never be applied through Group Policy, because a large amount of data contained in the security template can degrade performance.
You should import the Compatws.inf security template into the GPO linked to the Client Computers OU, to have it applied to all client computers. Compatws.inf is designed to remedy the compatibility issues with legacy applications that require Power Users membership by assigning necessary rights to standard users. The security template will also remove all members from the Power Users group automatically.

QUESTION 37:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. The Certkiller .com network contains 17 servers and 1,200 client computers. All servers on the Certkiller .com network run Windows Server 2003. Half the client computers run Windows 2000 Professional, and the rest run Windows XP Professional.
You are responsible for the configuration of security settings at Certkiller .com. To this end you make use of a Group Policy object (GPO) to configure security settings for the Certkiller .com users. You are planning to deploy a script to all users, which will run a program to check each client computer that they log on to for the existence of a Trojan that you believe has gained access to the Certkiller .com network. Users can only run this program if a particular hotfix is installed on their computers. In the event of the user not having that specific hotfix installed, the script should not be run.
You need to ensure that the logon script will only be applied to the users if the computer that they are logging onto has the hotfix installed.
What should you do?

A. Check each client computer for the presence of the hotfix.
Run the script locally if the hotfix is installed.
B. Create a GPO that will run the logon script and link it to the domain.
C. Create a GPO the installs the hotfix and link it to the domain.

D. Instruct the users to not run the GPO until they verify that the hotfix is installed.
E. Create a WMI Filter on the on the GPO that checks for the presence of the hotfix by using a query.

Answer: B, E

Explanation: WMI Filters contain WQL based queries, which are evaluated dynamically at the computer startup or at user logon, and depending on their outcome, allow or disallow the GPO settings to be applied. By creating a WMI Filter that checks for the presence of the hotfix on the GPO that will run the logon script, you will prevent the logon script from running on computers that do not have the hotfix installed. If the WMI Filter verifies that the hotfix is installed, the GPO will be processed and the logon script will run.
Incorrect Answers:
A: You could check each client computer individually for the presence of the hotfix, but you would have to visit 1,200 computers. Also, the script is a logon script that needs to be run each time a user logs on.
C: Using this option will install the hotfix on the client computers.
D: Users do not have the option of selecting and running GPOs.

QUESTION 38:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003. Half the client computers run Windows 2000 Professional, and the rest run Windows XP Professional.
Certkiller .com consists of three departments named Research, Development and Finance respectively. The Certkiller .com organizational unit (OU) structure reflects these departments. You are responsible for the IT security at Certkiller .com and have received instruction from the CIO to improve the security of the Certkiller .com network. To this end you test the security that you have created and put it in a Group Policy object (GPO) in a parallel environment. There after you create a GPO and linked it to the domain and import the settings.
Furthermore, you also configured a test user account in each department's OU. A day after the completion of the domain-based GPO, a user named Rory Allen contacted the CertK ign.com help desk to complain that he is unable to log on to the domain with his user account. During the investigation you notice that some of the security settings applied and some did not.
What should you do? (Select all that applies.)

A. Get the policy settings and use the Help and Support Advanced System Information and get a list of all the policies that is applied to Rory Allen and his client computer by using the Resultant Set of Policy (RSoP) in Logging mode.
B. Get the policy settings by using the Resultant Set of Policy (RSoP) in Planning mode.
C. Obtain a list of all the policies that is applied to Rory Allen and his computer by using

the GPupdate tool.
D. Obtain a list of all the policies that is applied to Rory Allen and his computer by using the GPresult tool.

Answer: A, D

Explanation: The logging mode contains a list of effective policy settings. It also has the GPOs that are applied to the policies. This will allow you to see were the conflict is. The Help and Support Advanced System Information will view the Group Policy setting that is applied.
Incorrect answers:
B: The RSoP in planning mode will allow you to test the policy before it is applied.
C: The GPupdate is used to refresh the policy settings on a computer.

QUESTION 39:

You recently work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003. Half the client computers run Windows 2000 Professional, and the rest run Windows XP Professional.
Certkiller .com consists of a Research and Development department. You are responsible for the security in the Certkiller .com domain. Certkiller .com contains a server named Certkiller -SR12. You need to test a domain and organizational unit hierarchy structure. The Certkiller .com user environment is controlled by means of the application of quite a few group policy objects. During routine monitoring you discover that quite a few users have access to the security log of Certkiller -SR12. You need to check which security settings are applied to these users.
What should you do?

A. Use GPupdate to refresh the group policy of the users.
B. Make sure that the users with there client computer has the Apply Group Policy and Read access permissions for the correct GPO.
Run the RSoP in Logging mode and make sure that the group policy setting is not blocked.
C. Run RSoP with WMI filters.
D. Run RSoP in Planning mode.

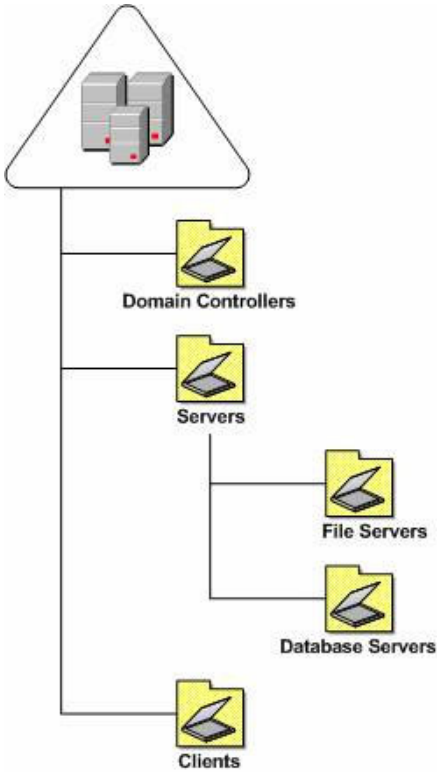
Answer: B

Explanation:
If there is no result in policies not affecting the users, you should verify the GPO settings and see if it is not blocked. You also need to make sure that the users with there client computer has the Apply Group Policy and Read access permissions for the correct GPO.
Incorrect answers:

A: The GPupdate is used to refresh the policy settings on a computer. This will not help.
C: WMI filters allow the filtering of GPO settings based on specific information which will includes computer hardware or software installed. This is not going to reveal which policies are applied to whom.
D: The RSoP in planning mode will allow you to test the policy before it is applied.

QUESTION 40:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. Certkiller .com has its headquarters in Chicago and a branch office in Dallas. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network contains:
1. A demilitarized zone (DMZ) that includes five Web servers clustered together in a Web farm.
2. This DMZ does not form part of the domain.
3. The internal network that includes: two domain controllers and ten member servers.
4. Of the ten member servers two are running SQL Server 2000.
5. All of the servers on the internal network are members of the Certkiller .com domain.
6. There are no Web servers on the internal network.
The following Exhibit illustrates the Certkiller .com's Active Directory schema.
Exhibit:



You need to implement the Certkiller .com internal policies and to this end you make

use of Group Policy objects (GPO). You have configured a new security template that has to be applied to the Web servers.
You need to ensure that this security template is implemented with as little administrative effort as possible.
What should you do?

A. Create a GPO that contains the new security template
Link the GPO to the Servers OU.
B. Create a batch file that contains the new security template using the Secedit.exe tool.
Run the batch file on the five DMZ Web servers.
C. Create a GPO that contains the new security template.
Link the GPO to the Domain Controllers OU.
D. Create an OU named Web Servers in the Servers OU.
Place the computer accounts of the Web servers in the Web Servers OU.

Answer: B

Explanation: To apply a security template, you should use the Secedit.exe tool to create a batch file that contains the new security template. You should then run the batch file on the Web servers on the demilitarized zone (DMZ). Secedit.exe is used to analyze or configure multiple computers. By calling the Secedit.exe tool at a command prompt, from a batch file, or using the automatic task scheduler, you can use it to automatically create and apply templates and analyze system security.
Incorrect Answers:
A: The Servers OU and the Domain Controllers OU contains all servers in the domain. Neither of these is required to have the new security template.
C: The Servers OU and the Domain Controllers OU contains all servers in the domain. Neither of these is required to have the new security template.
D: In a DMZ, the Web servers are purposely not members of the Active Directory domain. This is for protection of the internal network.

QUESTION 41:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The
Certkiller .com written security policy states that no unauthorized VBScript files are to be deployed and executed on Certkiller .com client computers. The only authorized VBScript file is named Market.vbs which consists of several script components; with each component representing a different task. Market.vbs is stored in a shared folder named MarketTools on a file server named Certkiller -SR05.
Before using Market.vbs, it has to be modified to ensure that only the required component is run. You need to create a software restriction policy to enforce the requirements of the Certkiller .com written security policy. You want to use the least

amount of administrative effort to accomplish your task.
What should you do? Choose two correct answers. Each correct answer presents only part of the complete solution. Choose two.

A. Create a new Path rule and set the path to Market.vbs.
Set the security level to Unrestricted.
B. Create a new Internet zone rule for Market.vbs.
Set the security level to Restricted.
C. Create a new Hash rule for all .vbs files.
Set the security level to Disallowed.
D. Digitally sign each .vbs file to authorize it.
Create a new Certificate rule and set the security level to Restricted.
E. Create a new Path rule and set the path to be *.vbs.
Set the security level to Disallowed.

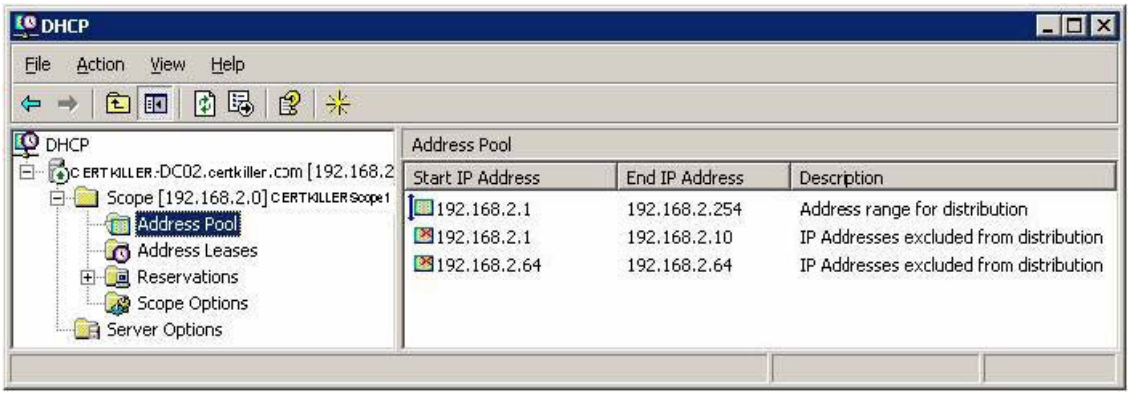
Answer: A, E

Explanation: There are four different types of software restriction policy rules. Because more than one rule can be applied to one file, the priority of these rules is as follows: Hash rules have the highest priority; Certificate rules take priority over Path rules; Path rules take priority over Internet zone rules; and Internet zone rules have the lowest priority. When the same type rule is applied to the same file, then the more specific rule overrides the less specific rule.
To ensure that no unauthorized .vbs scripts are run on client computers, you need to create a new path rule, set the path to be *.vbs, and then set the security level to Disallowed. To ensure that Market.vbs can run on client computers, you need to define a more specific Path rule to override your less specific Path rule already defined. In the more specific Path rule, you set the path to Market.vbs file, and then set the security level to Unrestricted.
Incorrect Answers:
B: Internet zone rules apply to Windows Installer .msi files.
C: It would be an enormous task to create a Hash rule for all .vbs files and then modify the rule whenever a new .vbs file is available so that it would need to be included in the rule.
D: If you choose to create a new Certificate rule, you would need to sign the file whenever it changes. This would be impractical. In this case, then the security level in this option is also incorrect. It would need to be Unrestricted.

QUESTION 42:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network contains two domain controllers named Certkiller -DC01 and Certkiller -DC02.

The Certkiller .com IP network address is 192.168.2.0/24. You need to make use of a DHCP for assigning IP configurations to all the Certkiller .com client computers and network printers automatically. You then install the DHCP Server service on a server named Certkiller -DC01. The DHCP configuration is illustrated in the following Exhibit:
Exhibit:



Shortly after installing DHCP on Certkiller -DC01, you discover that Certkiller -DC02, which is assigned the static IP address 192.168.2.15, encounters an IP address conflict with a network printer that is configured as a DHCP client. You received instruction to ensure that this conflict is resolved.
What should you do?

A. Assign the network printer the static IP address 192.168.2.200.
B. Configure the scope to exclude the IP address 192.168.2.15.
C. Delete the IP address exclusions on Certkiller -DC02.
D. Use the IP address 192.168.2.254 to define a client reservation for Certkiller -DC02.

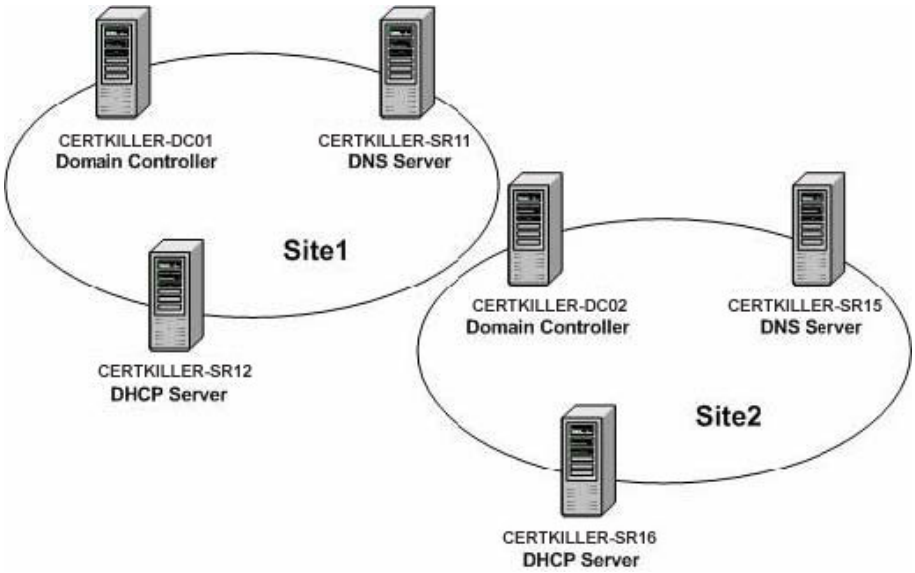
Answer: B

Explanation: IP addresses that are excluded from a DHCP scope will not be dynamically assigned to clients by the DHCP server. The current DHCP configuration does not exclude this IP address in the scope.
Incorrect Answers:
A: This might cause another IP address conflict because the IP address 192.168.2.200 is contained within the defined scope on Certkiller -DC01.
C: This will not resolve the IP address conflict between Certkiller -DC02 and the network printer.
D: A client reservation is an IP address that is reserved for a particular DHCP device. Since Certkiller -DC02 is configured with a static IP address, it is not a DHCP client and would not benefit from a client reservation in DHCP.

QUESTION 43:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory single domain named Certkiller .com with two sites. All servers on the Certkiller .com network run Windows Server 2003

and all client computers run Windows XP Professional.
The relevant portion of the network topology is illustrated in the following Exhibit:
Exhibit:



One DNS server hosts the primary DNS zone.
The other DNS server hosts the secondary DNS zone.
You received instruction to harden the Certkiller .com DNS servers. To this end you need to ensure that no interception of DNS information occurs during zone transfers. You must still ensure that all DNS server and client data is current. You also want to prevent false records from being created.
What should you do? (Each correct answer presents part of the solution. Choose TWO.)

A. Disable dynamic updates.
B. Configure the primary zone to be an Active Directory-integrated zone.
C. Enable the secure dynamic updates feature.
D. Ensure that the root zone is deleted from both DNS servers.

Answer: B, C

Explanation: An Active Directory-integrated zone is an authoritative primary zone that stores its data in Active Directory. Active Directory replication is faster, which means that the time needed to transfer zone data between zones is far less. Active Directory-integrated zones also enjoy the security features of Active Directory. When DNS and Active Directory are integrated; the Active Directory-integrated zones are replicated, and stored on any new domain controllers automatically. Synchronization takes place automatically when new domain controllers are deployed. Active Directory- integrated zones are set up to only allow secure dynamic updates. The properties dialog box of an Active Directory-integrated zone has an additional tab, called the Security tab. This is the tab where you set access permissions for the specific zone, configure who can modify the properties of a specific zone, and configure who can add dynamic updates to records for a specific

zone.
Incorrect answers:
A: Because you want DHCP clients to have current information in DNS, you need to have dynamic updates enabled.
D: Deleting the root zones would not improve or assist in hardening your DNS servers.

QUESTION 44:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
A server named Certkiller -SR12 has Software Update Services (SUS) installed and the Certkiller .com client computers are configured to download security updates from Certkiller -SR12. While examining several client computers, you discover that no updates have been installed for more than two weeks. You suspect that the client computers have stopped downloading updates from Certkiller -SR12. You received instruction to ensure that all Certkiller .com client computers download their security updates from Certkiller -SR12.
TO this end you examine the synchronization log on Certkiller -SR12 and find that several update packages have been downloaded from the Microsoft Website directly. However, they have not been installed on any of the client computers. When you try to open the Certkiller -SR12 SUS Administration Web page, you find that you are unable to do so.
What should you do?

A. Configure Certkiller -SR12 to redirect clients to the Windows Update Web site so that they can download updates directly from this Web site.
B. Examine the content in the Certkiller -SR12 approval log.
C. On Certkiller -SR12, restart the World Wide Web Publishing service.
D. On Certkiller -SR12, configure folder sharing for the folder that contains the SUS Web site.

Answer: C

Explanation: The SUS server is reliant on IIS, and SUS administration takes the form of a Web application. Because you cannot access the SUS Administration Web page on Certkiller -SR12, the issue is probably that IIS is not running on Certkiller -SR12. One of the requirements for installing SUS on a server is that the server must be running IIS 5.0 (minimally), and must be connected to the network. The SUS Web site on Certkiller -SR12 deals with requests from Automatic Updates clients. To resolve your issue, restart the World Wide Web Publishing service on Certkiller -SR12.
Incorrect Answers:
A: Because no client computers are able to access the SUS Web site on Certkiller -SR12, it is impossible to redirect the client computers to the Windows

Update Web site.
B: The content in the approval log on Certkiller -SR12 will only reveal which updates have been approved and which have not been approved.
D: There is no need to configure folder sharing for the folder that contains the SUS Web site because Automatic Updates clients use the SUS Web site and HTTP to download updates from Certkiller -SR12.

QUESTION 45:

You work as a network domain administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
A server named Certkiller -SR210 has been configured to function as a Software Update Services (SUS) server. The Certkiller .com security policy states that all computers on the network should be updated with the latest security patches on a periodical basis and that all unnecessary services should be disabled. You received instruction to verify whether all computers are in compliance with the company security policy. You need to accomplish this task with the least amount of administrative effort.
What should you do?

A. Use a GPO to deploy MBSA on all the Certkiller .com computers.
Then instruct all users to run MBSA in their respective computers.
B. Review the history and the approval logs on Certkiller -SR210.
C. On your workstation run MBSA.
Then specify that all Certkiller .com computers be scanned.
D. On your workstation run MBSA.
Then scan all Certkiller .com computers individually.

Answer: C

Explanation: MBSA will allow you to perform various checks on specified computers. To scan all the Certkiller .com computers, you should install MBSA on your computer and then specify that all computers in the domain be scanned. By default MBSA connects to the Windows Update Web site, determines which updates should be installed on each computer then compares the list of those updates to the ones that are installed on each computer in the domain. In this case you must select the Use SUS Server option and type in http:// Certkiller -SR210 in the appropriate dialog box in MBSA.
Incorrect answers:
A: This option will result in all the client computers being scanned. The servers and the domain controllers will then not be scanned. Furthermore in this case you will also have to instruct all the Certkiller .com users on MBSA usage and then also check whether they have used MBSA in the appropriate way.
B: You will be able to determine which updates have been downloaded to Certkiller -SR210 and which updates have been approved when you review the history

and approval logs on Certkiller -SR210. It will however not enable you to determine which updates are appropriate for the individual computers on the Certkiller .com domain and whether those updates have been installed.
D: Scanning each Certkiller .com computer individually will amount to unnecessary administrative effort even though it will also get the job done the question pertinently states that the task must be accomplished with the least amount of administrative effort.

QUESTION 46:

You work as a network domain administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
A server named Certkiller -SR23 has been configured to function as a Software Update Services (SUS) server. All the servers are placed in a location that is separate from the Certkiller .com work area. Consequently all servers are managed from client computers that are located in the Certkiller .com work area. Your manager requested a list of the critical updates that are available and have been approved from you.
What should you do?

A. Use the Mbsacli tool.
B. Use the Secedit tool.
C. Use the Wmic qfe tool.
D. Use the Gpupdate tool

Answer: A

Explanation: Mbsacli is the command line version of Microsoft Baseline Security Analyzer (MBSA). This option will be the best tool to use in this scenario because MBSA works by connecting to the Windows Update Web site or a specified SUS server in this case Certkiller -SR23, to obtain the list of critical updates that are available on the Windows Web site or that have been approved on Certkiller -SR23.
Incorrect answers:
B: Secedit is used to analyze and configure security settings on a computer. It is not used for the purposes required in this question.
C: The wmic qfe command with the appropriate parameters is used to check whether a specific Quick Fix Engineering (qfe) solution/patch was installed on targeted computer/s. This is thus not the appropriate tool under the circumstances.
D: Gpupdate cannot be used to determine whether a specific patch is installed on a computer and this option will thus not suffice.

QUESTION 47:

You work as a network domain administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All

servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
You are responsible for the management of a server named Certkiller -SR20. Certkiller -SR20 has been configured to function as a Software Update Services (SUS) server. All the client computers in the Certkiller .com domain are configured to receive Windows updates from Certkiller -SR20.
A new computer named Certkiller -WS299 has just been joined to the domain. There are however a few tasks that has to be done to Certkiller -WS299, such as:
1. Verify that all unnecessary services have been removed from Certkiller -WS299.
2. Verify that Certkiller -WS299 is NTFS formatted.
3. Ensure that all the operating system updates have been installed on Certkiller -WS299.
To this end you created a service.txt file and placed it on Certkiller -WS299. You then proceed to open Microsoft Baseline Security Analyzer (MBSA) on Certkiller -WS299 and select the "scan a computer" option. You received instruction to select appropriate scans that should be performed while minimizing the impact on performance.
What should you do? (Each correct answer presents part of the solution. Choose THREE.)

A. Select Certkiller -SR20 from the Use SUS server drop-down list.
B. Select the Check for IIS vulnerabilities check box.
C. Select the Check for security updates check box.
D. Select the Check for weak passwords check box.
E. Select the Check for Windows vulnerabilities check box.
F. Select the Check for SQL vulnerabilities check box.

Answer: A, C, E

Explanation: The Check for Windows Vulnerabilities check box ensures that all unnecessary services are removed from the computer and that the NTFS file system is the only file system in use. The Check for Security Updates check box will verify which updates have been installed on Certkiller -WS299. And selecting Certkiller -SR20 from the Use SUS Server drop-down list will ensure that Certkiller -WS299 will download its updates from Certkiller -SR20.
Incorrect Answers:
B: The Check for IIS vulnerabilities check box will only perform the various IIS security checks.
D: The Check for weak passwords check box will only verify the password complexity for the Certkiller -WS299 local account/s.
F: The Check for SQL vulnerabilities check box will only check the various SQL security checks.
B, D, F: No mention is made of SQL or IIS in the question. Thus running these test will impact on the performance of Certkiller -WS299. Furthermore it is not specified that MBSA should check for weak passwords.

QUESTION 48:

You work as a network domain administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network is due for an infrastructure update and this presents you with an opportunity to identify all possible security weaknesses that may exist for the network. To this end you want to make use of Microsoft Baseline Security Analyzer (MBSA) in an effort to identify all possible security weaknesses for the network. A server named Certkiller -SR10 has been configured to function as a Software Update Services (SUS) server. You need to use MBSA to scan only for updates that have been approved by Certkiller -SR10.
What should you do? (Each correct answer presents part of the solution. Choose two.)

A. Install MBSA on a client computer.
Run the mbsacli.exe /sus command at a command prompt.
B. Install MBSA on a server.
Run the mbsacli.exe /sus command at a command prompt.
C. Install MBSA on a server.
Run the mbsacli.exe /hf command at a command prompt.
D. Edit the mssecure.xml file with the approved security updates.
Scan the client computers using MBSA.

Answer: B

Explanation: MBSA connect to the Microsoft Download Centre Web site on downloads the most recent version of the mssecure.cab compressed file. From that file that contains the list of available operating system updates, MBSA extracts the mssecure.xml file. MBSA will analyze the target computer to determine which of the updates listed in the mssecure.xml file are installed on the computer and includes the results in its report. The mbsacli.exe command with the /sus switch should be typed at a command prompt from the folder where MBSA was installed. The /sus switch is added to the command with Certkiller -SR10 to check only for the updates that are approved at the specified SUS server, in this case Certkiller -SR10.
Incorrect answers:
A: You need to run install MBSA on a server in this scenario since Certkiller -SR10 is configured as the SUS server.
C: The mbsacli.exe /hf command is used to perform an HFNetChk-style scan for missing security updates and is thus not the option to choose.
D: Editing the mssecure.xml file is used be MBSA to check for all updates that are listed on the Microsoft Update Web site. You cannot edit it.

QUESTION 49:

You work as a network domain administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com network is connected to the Internet.
You have been instructed to implement a new computer named Certkiller -SR20.
You want to ensure that Certkiller -SR20 complies with the Certkiller .com security requirements. To this end you need to:
1. Verify that all the necessary security updates have been installed.
2. Verify that NFTS has been used on all the hard disks.
3. Review the list of shared folders on Certkiller -SR20, and perform similar checks.
What should you do?

A. Select the Windows Update option from the Start menu.
Follow the instructions on Certkiller -SR20.
B. Install and run Microsoft Baseline Security Analyzer (MBSA) on Certkiller -SR20.
C. Use the Security Configuration and Analysis utility to import the securews.inf security template on Certkiller -SR20.
Then analyze Certkiller -SR20 server configuration against that of the template.
D. Use IPSecMon to verify the security configuration on Certkiller -SR20.

Answer: B

Explanation: MBSA uses the HFNetChk utility to check if all the necessary security updates have been installed. MBSA can also be used to identify the file system in use on the computer's hard disks. MBSA can also be used to check the status of the Guest account, the list of available shared folders and the list of the Administrators group membership.
Incorrect answers:
A
: This option will not provide any tools to perform all the checks that are required. You will only be able to check whether all the necessary security updates are installed on Certkiller -SR20 and download and install any missing updates.
C: Security Configuration and Analysis is used to compare the security settings on a computer to a specified collection of security settings. It cannot be used to verify whether all the required security updates are installed on a computer.
D: IPSec monitor is used to collect and view statistics related to IPSec communications and to verify whether IPSec is working properly on a computer. You cannot use IPSec Monitor to perform all the required checks in this scenario.

QUESTION 50:

You work as the network administrator at Certkiller .com. The Certkiller .com

network consists of a single Active Directory domain named Certkiller .com. The Certkiller .com network contains ten Windows Server 2003 computers and 1,200 client computers running either Windows XP Professional or Windows 2000 Professional.
A Certkiller .com security policy states that all computers should be kept up to date with the Service Packs that Microsoft makes available on the Microsoft Updates Web site. Upon routine maintenance on the network you notice that none of the client computers have been updated with the latest Service Packs that are available on the Microsoft Updates Web site. You thus need to address the issue.
To simplify the process of deploying all the operating system updates to the client computers, you plan to use a server named Certkiller -SR06 as a Software Update Services (SUS) server. There are however certain prerequisites to installing SUS on a server. You need to fulfill these prerequisites.
What should you do?

A. Create and configure History.sync.xml and History.approve.xml on Certkiller -SR06.
B. Install DNS server on Certkiller -SR06.
C. Install IIS on Certkiller -SR06.
D. Install Service Pack 1 on the Windows XP Professional client computers and Service Pack 2 on the Windows 2000 Professional client computers.

Answer: C

Explanation: Because SUS is a Web application that connects via the Internet to the Microsoft Windows Update Web site, it relies on Internet Information Services (IIS). Thus you need to install IIS on Certkiller -SR06 prior to installing SUS on Certkiller -SR06.
Incorrect answers:
A: These are SUS log files that are created automatically during SUS installation.
B: DNS server installed on the same server as SUS is not a prerequisite. In fact it is not an advisable practice to have DNS and SUS installed on one server.
D: Though the Automatic Updates of the SUS Client application is supported in Windows Server 2003, Windows 2000 Professional with Service Pack 2 or higher, and Windows XP Professional with Service Pack 1 or higher, it is NOT a prerequisite for installing SUS on Certkiller -SR06. It is a prerequisite for the client computers.

QUESTION 51:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. The Certkiller .com network contains several servers that either function as domain controllers or member servers. These servers all run Windows Server 2003 and all client computers run Windows XP Professional.
You are busy creating an integrated installation of Windows Server 2003 and all the available updates and deploying it on a server named Certkiller -SR05. However,

after the installation you observed that the operating system generated memory dump errors. You investigate and then discovered that the memory dump error occurs due to a security update that is incompatible with the Explorer service. You need to address this issue as soon as possible.
What should you do?

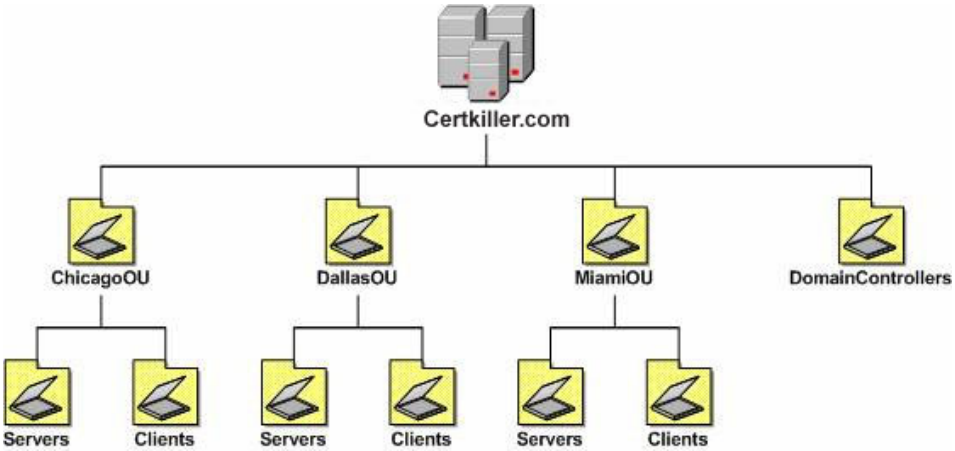
A. Use Add/Remove Programs Wizard in Control Panel to uninstall the updates.
B. You need to create a new integrated installation that excludes the security update. Then re-install the operating system.
C. Use Update.exe to uninstall the security update. Then specify the update in a Svcpack.inf file.
D. Use Qchain.exe to uninstall the update.

Answer: B

Explanation: An integrated installation affords you the opportunity to install Windows operating system and specified updates, like service packs simultaneously. However, keep in mind that these updates installed by this specific method cannot be uninstalled. Thus you need to create a new integrated installation that excludes the incompatible update and you need to reinstall the operating system.
Incorrect answers:
A: The Add/Remove Programs Wizard in Control Panel cannot be used to remove integrated installation installed updates.
C: One uses Update.exe and specifies updates in a Svcpack.inf file to create an integrated operating system installation. However, there are some updates, like the Internet Explorer updates that makes use of .inf files based installations that, by themselves, cannot be used for integrated installation.
D: Qchain.exe is used to install updates without the need to restart the computer after each installation. However, this tool is not used to uninstall updates.

QUESTION 52:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
Certkiller .com consists of a Marketing department. Certkiller .com has its headquarters in Chicago and a branch office in Dallas and Miami. In each of the offices there is an OU where the computer accounts are kept:
1. The Chicago office computer accounts are located in an OU named ChicagoOU.
2. The Dallas office computer accounts are located in an OU named DallasOU.
3. The Miami office computer accounts are located in an OU named MiamiOU.
Certkiller .com also contains a domain controller named Certkiller -DC02 that is located in a default container. In each office there is an OU for the servers named Server OU as illustrated in the Exhibit:
Exhibit:



You need to ensure that the client computers of the three offices have the latest patches and hotfixes.
What should you do?

A. Create a domain-base policy that specifies the client computers to use the Automatic Update features and the servers to use the Software Update Services.
B. Create a Group Policy object on one of the OUs that contain the client computers. Then configure the computers to use the Automatic Update features to download and install Windows updates.
Link this GPO to the other two OUs that contains the other client computers.
C. Create a domain-base Group Policy object that configures the computers to use the Automatic Update features to download and install Windows updates.
Deny apply Group Policy to the domain controllers and Servers OUs.
D. Configure each of the client computers to use the Automatic Update features to download and install Windows updates.

Answer: B

Explanation: If the Automatic Update is enabled, the computer will automatically connect to the Windows Update site and download any security updates. You should create a GPO and configure the computers to download and to use the Automatic Update feature.
Incorrect answers:
A: You only have permission at the OU level as stated in the scenario. That way you cannot create a domain-based GPO.
C: You only have permission at the OU level as stated in the scenario. That way you cannot create a domain-based GPO.
D: You can do it this way, but it will be time consuming.

QUESTION 53:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client

computers run Windows XP Professional.
Certkiller .com consists of a Research department. Certkiller .com contains a few servers that are used for downloading updates and patches. You have received instruction from the CIO to ensure that the servers are kept up to date with the latest service packs and hotfixes. You need to specify the servers to automatically receive updates and the client computers in the Research department to receive the updates on a regular basis.
What tool should you use?

A. Use the Auto update.
B. Use the Dynamic Update.
C. Use the Software Update Services.
D. Use the Intellimirror.

Answer: C
Explanation The Software Update Services synchronize updates with the Windows Update Web site. The updates are also tested in the Quality Assurance before it is installed to the servers.
Incorrect answers:
A: You can use the Auto update, but it will not be tested.
B: Dynamic Update is used for emergency fixes to address setup problems. It is also used to provide update drivers.
D: The Intellimirror manages information, settings and software. If is not used to manage the updates through service packs and hotfixes.

QUESTION 54:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The domain operates at a Windows Server 2003 functional level. The Certkiller .com head quarters are located in Chicago and the branch offices are located in Dallas, Miami, and Los Angeles. Each office is configured as a site and is connected to the Chicago office via a T1 connection. The sites are interconnected by means of 256-Kbps leased lines.
Your duties include the deployment of patches and hotfixes for the Certkiller .com network. You are currently planning the patch deployment to the clients in the branch offices. The plan is to make use of the main Software Update Service (SUS) server in the Chicago office to deploy the updates to the secondary SUS servers that are located in the branch offices. All standard updates are to be deployed across all sites while minimizing the bandwidth usage to do so.
To this end you download and approve a number of updates in the main SUS server in the Chicago office. Then you synchronize the main SUS server to the secondary SUS servers that are located in the branch offices. However, later when you attempt to connect to the Miami site and approve only selected updates, you find that you are unable to do so. On the Approve Updates page, you notice that the Approve

button is disabled. Thus you are unable to approve updates on any of the secondary SUS servers.
What should you do?

A. Modify the secondary SUS servers' configuration to download and approve updates from the official Microsoft Windows Update Web site in their respective sites.
B. Do not modify the secondary SUS server configuration.
Deploy all main SUS server approved updates to the secondary SUS servers.
C. Manually copy the selected updates to the secondary SUS servers from the Main SUS server in the Chicago office.
D. Configure the secondary SUS servers with a new aproveditems.txt file.

Answer: B

Explanation: All updates should be deployed from the main SUS server. All approved items on the secondary SUS servers will be identical to those on the main SUS server. You cannot make changes to the approved items; it can only be accepted by the secondary SUS servers. Both the main and secondary SUS servers will keep the same set of approved items. When the secondary SUS servers accept the approved items, the Approve button will become disabled on the Approved Updates page on the secondary SUS server. Thus you do not need to modify the secondary SUS server configuration.
Incorrect answers:
A: According to the scenario in the question, you must deploy the standard set of updates across all branch offices. If the SUS servers across the offices are configured to download directly from the official Microsoft Updates Web site, then there would not be any consistency in update deployment across all sites.
C: You cannot manually copy the selected updates from the main SUS server to the secondary US servers.
D: The approveditems.txt file represents the list of administrator-approved update files, the secondary SUS servers should not be configured with a new approveditems.txt file because this file should be the same for all the SUS servers.

QUESTION 55:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The domain operates at a Windows Server 2003 functional level. All servers are located in an organizational unit (OU) named Servers and all client computers are located in an OU named Client_Computers.
A server named Certkiller -SR05 has been configured with Software Update Services (SUS). Certkiller -SR05 is further configured to download updates directly from the official Microsoft Windows Update Service Web site. All the computers in the Certkiller .com domain are configured to receive their updates from Certkiller -SR05. The Default Domain Policy has been configured for automatic

updates.
Recently all the new Windows XP Professional client computers on the Certkiller .com network suffered a virus infection. The CIO then instructed you to ensure that this problem is negated in future. You thus need to ensure that all computers are installed with the latest service packs and security updates.
What should you do? (Each correct answer presents part of the solution. Choose two.)

A. Use a batch file that references all security updates.
Run this batch file after the operating system installation.
B. Use a batch file to install security updates during operating system installation.
C. Install the operating system.
Deploy the latest service pack and security updates using SUS.
D. An installation media of the operating system that includes the latest service pack should be created.
E. Install the operating system.
Scan the client operating systems using MBSA.
Obtain the missing security updates from the Certkiller -SR05.

Answer: B, D

Explanation: You need to ensure that all client computers are installed with the latest service packs and security updates. When you slipstream a service pack into the operating system installation files, the service pack is included in the installation. This should ensure that the client computers have the latest service packs installed.
And you could use a batch file to install security updates on the operating system. A batch file is also known as an answer file. You can list the security updates under the (GuiRunOnce) section and you can define the order in which you want the security updates to be applied.
Incorrect answers:
A: Installing security updates and service packs after the operating system installation will not prevent the operating system from being infected with viruses. You need to ensure that the security updates as well as the service packs are installed along with the operating system.
C: Installing security updates and service packs after the operating system installation will not prevent the operating system from being infected with viruses. You need to ensure that the security updates as well as the service packs are installed along with the operating system.
E: Installing security updates and service packs after the operating system installation will not prevent the operating system from being infected with viruses. You need to ensure that the security updates as well as the service packs are installed along with the operating system. Furthermore, the MBSA tool allows an administrator to scan for security updates, it is not used to install updates and service packs.

QUESTION 56:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The domain operates at a Windows Server 2003 functional level. The Certkiller .com head quarters are located in Chicago and the branch offices are located in Dallas and Miami. Each office is configured as a site and is connected to the Chicago office. The sites are named Certkiller A, Certkiller B, and Certkiller C respectively.
At each site a Software Update Services (SUS) server has been deployed. The main SUS server named Certkiller -SR01 is hosted in the Certkiller A site and the secondary SUS servers are located in the Certkiller B and Certkiller C sites.
You have just received notification that new security updates are available and thus you want to deploy these updates to all the client computers and servers in the shortest possible time using the least amount of administrative effort as well as the least amount of network bandwidth.
What should you do?

A. Each client computer and member server should be configured to obtain security patches and updates directly from the official Microsoft Windows Update Web site.
B. Certkiller -SR01 should be configured to download security patches and updates from the official Microsoft Windows Update Web site using the Synchronize now option. Configure Certkiller B and Certkiller C SUS servers to download security patches and updates from Certkiller -SR01.
C. Each site's SUS server should be configured to synchronized security patches and updates from the official Microsoft Windows Update Web site.
Deploy these updates and patches to client computers and servers in their respective sites.
D. Certkiller -SR01 should be configured to download security patches and updates from the official Microsoft Windows Update Web site.
Store the updates in a network share and then instruct all Certkiller .com users to install the appropriate updates.

Answer: B

Explanation: You need to synchronize the primary SUS server Certkiller -SR01 with Windows Update using the Synchronize Now option. The secondary SUS servers will download security patches and updates from Certkiller -SR01. The client computers can be configured to download patches and updates from the SUS server in the location where they are. The client computers will be prompted to download updates every 22 hours from the time the updates were approved.
Incorrect answers:
A: Configuring every client computer and member server to download security patches and updates from the official Microsoft Windows Update Web site will require more bandwidth.
C: The secondary SUS servers should not be configured to download patches and updates from the official Microsoft Windows Updates Web site; this is not required and will only

result in unnecessary bandwidth usage.
D: Storing the updates in a network share and instructing users to apply the appropriate updates will result in too much administrative effort.

QUESTION 57:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com written security policy requires all servers must to the latest available security updates installed. A server named Certkiller -SR07 has Software Update Services (SUS) installed. You plan to deploy several new file servers on the network. You need to enforce the written security policy for all new file servers. Each new file server has two local user accounts. The administrator account for each new file server is renamed.
You must make certain that none of the new file servers have any unnecessary services enabled. You must also ensure that each file server has the latest available security updates installed. You want to use the least amount of administrative effort to determine whether any servers have missing security updates. You also want to reduce the amount of bandwidth by scanning for only the required information on each server.
What should you do? (Each correct answer presents part of the solution. Choose two.)

A. Use Security Configuration and Analysis on your client computer.
B. Use Microsoft Baseline Security Analyzer (MBSA) on your client computer.
C. Use Security Configuration and Analysis on each new file server.
D. Use Certkiller -SR07 to download all missing security updates on file servers.
E. Scan each new file server for missing updates.
F. Scan each new file server's security settings.

Answer: B, E

Explanation: You should use the Microsoft Baseline Security Analyzer (MBSA) to check for and scan computers for security weaknesses, Windows vulnerabilities, and missing security updates. MBSA can be downloaded from the Microsoft website, and then used to scan for common security errors on a single computer or multiple computers. When MBSA is run from the GUI, it places reports in the SecurityScans folder of the user profile that creates the reports. You can also use MBSA from the command-line to determine whether all the necessary security updates and service packs have been installed on the computer.
Incorrect Answers
A: The Security Configuration and Analysis tool is used to scan a specific computer's security configuration against a reference computer's security configuration.
C: The Security Configuration and Analysis tool is used to scan a specific computer's

security configuration against a reference computer's security configuration. You need to ensure that the new file servers have the latest available security updates installed, and need to scan for missing updates.
D: Certkiller -SR07 can be used to deploy security updates for clients. You however need to determine whether the file servers have missing security updates.
F: You should be scanning for missing updates and not security settings.

QUESTION 58:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The implementation of security and software updates is your responsibility. You are currently planning to implement a new security and software update infrastructure for Certkiller .com. A SUS server named Certkiller -SR18 will be deployed in the network. Client computers will be configured to download security updates from Certkiller -SR18.
One of your requirements is to identify security vulnerabilities on all Certkiller .com client computers. You want to use a solution that will only scan client computers for security patches that have been authorized and deployed from Certkiller -SR18.
You do not want to scan the client computers for unnecessary information.
Furthermore the CIO requested that you furnish her with a separate security report of the scan for each client computer. To this end you install Microsoft Baseline Analyzer (MBSA) on a Windows Server 2003 computer.
What should you do next?

A. On the computer that has MBSA installed, run the mbsacli.exe/ sus command from a command prompt to scan all client computers.
B. On the computer that has MBSA installed, run the mbsacli.exe/ hf command from a command prompt to scan all client computers.
C. Modify the mssecure.xml file so that it includes all approved updates.
Run MBSA to scan the client computers.
D. Modify the approvedsecurity.text file so that it includes all approved updates.
Run MBSA to scan the client computers.

Answer: A

Explanation: You can use the MBSA from the command-line to check for missing security updates and service packs. For computers running Internet Information Services (IIS) or Microsoft SQL Server; MBSA can scan for a number of security vulnerabilities. You however want MBSA to check client computers for security updates that have been approved and implemented by your SUS server (Certkiller -SR18), therefore, you should use the / sus switch with the SUS server name to perform only this type of scan. After you install Microsoft Baseline Analyzer (MBSA) on a Windows Server 2003 computer, you should run the

mbsacli.exe/ sus command from a command prompt to scan all client computers. A separate security report will be generated for each client computer that is scanned.
Incorrect Answers
B: If you want to run a HFNetChk scan to check for missing security updates, then you would the run the mbsacli.exe/ hf command. This type of scan displays the results in the command-line window.
C: The mssecure.xml file should be used if you want to check for all updates available on the Windows Update site. This file cannot be modified.
D: The approvedsecurity.text file is non-existent in the MBSA folder.

QUESTION 59:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The domain operates at a Windows Server 2003 functional level.
A server named Certkiller -SR07 has Software Update Services (SUS) installed.
You then deployed Certkiller -SR07 in a test lab that has 25 client computers. You then discover that the official Microsoft Windows Update Web site has new security updates available. Consequently you download them to Certkiller -SR07 and deploy them on the 25 client computers in the test lab. Directly after the installation, many of the client computers in the test lab became unstable.
You need to uninstall the new security updates from all the client computers in the test lab quickly and efficiently.
What should you do?

A. Uninstall the installed updates using Certkiller -SR07.
B. Uninstall the installed updates using the Add/Remove Programs option in the Control Panel.
C. Uninstall the installed updates using the Uninstall <Update Name> option.
D. Uninstall the installed updates with a custom script.

Answer: D
Explanation
: The most efficient way to remove security updates from multiple computers is using a custom script. It will allow you to uninstall security updates from the test lab client computers with the least amount of administrative effort.
Incorrect answer:
A: You cannot use Certkiller -SR07 to uninstall security updates. A SUS server does not offer the necessary features to uninstall the security updates from client computers.
B: This is possible to uninstall the security updates by using the Add/Remove Program in the Control Panel; however, it will require greater administrative effort than is necessary.
C: The Uninstall Update <Name> option is not available with the installed updates.

QUESTION 60:

You work as a network domain administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
You have been assigned an assistant named Clive Wilson. One morning a security breach occurred in that an individual has successfully managed to gain unauthorized access to important business information by exploiting a vulnerability in the operating system. You thus investigate with the purpose to determine exactly which vulnerability the intruder exploited. You then discover that there is a security patch available that is capable of eliminating the vulnerability. You then instruct Clive Wilson to identify the particular computers on which the security patch should be installed.
What should you do?

A. Instruct Clive Wilson to use Mbsacli
B. Instruct Clive Wilson to use Secedit
C. Instruct Clive Wilson to use Wmic qfe
D. Instruct Clive Wilson to use Gpupdate

Answer: C
Explanation
: Windows Management Instrumentation (WMI) is used to monitor and manage computers on a network. Wmic can be used to perform any management task on your network. The wmic qfe command with the appropriate parameters is used to check whether a specific Quick Fix Engineering (qfe) solution/patch was installed on targeted computer/s. Thus this option will assist Amy Wilson in carrying out her task.
Incorrect answers:
A: It is sometimes possible to use mbsacli to check whether a specific update has been installed on a computer, but MBSA is not the appropriate tool for this purpose. MBSA works by connecting to the Windows Update Web site or a specified SUS server to get hold of the list of critical updates that are available on the web site or approved on the server. This still leaves you with missing information for the purpose of this question.
B: Secedit is used to analyze and configure security settings on a computer. It is not used for the purposes required in this question.
D: Gpupdate cannot be used to determine whether a specific patch is installed on a computer and this option will thus not suffice.

QUESTION 61:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
A server named Certkiller -SR16 has been configured to function as a Software

Update Services (SUS) server. Certkiller -SR16 is an intranet Web server. Certkiller .com users are allowed to directly download updates from the Windows Update Web site to their client computers. The Certkiller .com security policy does not allow users to install security updates that have NOT yet been tested and approved.
While verifying the configuration of several client computers, you discover though that a large number of these computers have different security updates applied. You also find that several client computers have differing numbers of updates applied. You decide to prevent users from automatically downloading and installing updates on their client computers. You want to configure Group Policy settings to control your security and software update management infrastructure.
What should you do? (Each correct answer presents part of the solution. Choose two.)

A. Enable the Configure Automatic Updates group policy setting.
B. Enable the Specify intranet Microsoft updates service location policy setting.
C. Configure Software Installation to publish the security updates to all client computers.
D. Enable the Remove access to use all Windows Update features policy setting.
E. Configure Software Installation to assign the security updates to all client computers.

Answer: A, B

Explanation: You can configure Windows Update policy to ensure that all client computers obtain security updates from Certkiller -SR16, the intranet Web server. Certkiller -SR16 should be configured to useWindows Update Manager to download all updates from Microsoft's Update servers. To perform this configuration, you need to enable the Configure Automatic Updates group policy setting, and then enable the Specify intranet Microsoft updates service location policy setting. To use the least amount of administrative effort, you should create a GPO and link it to the OU containing all client computers. You would then only need to perform the appropriate configuration for the Specify intranet Microsoft updates service location policy setting.
Incorrect Answers:
C: You do want users to have the choice of which published packages to install on their respective client computers. When packages are published, the package becomes available in Control Panel's Add/Remove Programs applet.
D: This will result in no client computers being able to access Certkiller -SR16.
E: This option will require you to re-package each update that becomes available, so that it can be distributed to client computers.

QUESTION 62:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003. Half the client computers run Windows XP Professional, and the rest run Windows 2000

Professional.
A member server named Certkiller -SR13 is configured as the Software Update Services (SUS) server. Certkiller -SR13 is configured to synchronize directly with the Microsoft Windows Update servers each day, using the default synchronization schedule. All client computers are configured to make use of Automatic Updates client software to download security updates from Certkiller -SR13. A Group Policy Object (GPO) named ClientUpdates contains the automatic update settings. ClientUpdates is linked to the ClientComputers OU.
A few days after the SUS deployment on the network you decide to verify that all client computers have downloaded and installed security updates from Certkiller -SR13. You discover though that only Windows XP Professional client computers have been installing security updates from Certkiller -SR13. No Windows 2000 Professional client computers have downloaded and installed any security updates from Certkiller -SR13. You need to ensure that ALL client computers obtain and install security updates from Certkiller -SR13.
What should you do?

A. Ensure that all Windows 2000 Professional client computers are upgraded to Windows XP Professional.
B. Change the functional level of the Certkiller .com domain to Windows Server 2003.
C. Install Windows Service Pack 3 on all Windows 2000 Professional client computers.
D. Add the user accounts of all Windows 2000 Professional users to the local Administrators group.

Answer: C

Explanation: SUS supports the following client platforms:
1. Windows XP Professional with Service Pack 1 or over
2. Windows XP Home Edition server with Service Pack 1 or over
3. Windows 2000 Advanced Server with Service Pack 2 or over.
4. Windows 2000 Server with Service Pack 2 or over.
5. Windows 2000 Professional with Service Pack 2 or above.
Windows Automatic Updates is the client component of SUS. The Automatic Updates client is available with Windows 2000 Service Pack 3, Windows XP Service Pack 1, and Windows Server 2003. Because the Windows XP Professional client computers are receiving updates from the SUS server, you have an issue with the Automatic Updates client software installed on the Windows 2000 Professional client computers. The updated
Automatic Updates client software is available with Windows 2000 Service Pack 3. Installing Windows Service Pack 3 on the Windows 2000 Professional client computers should resolve your issue.
Incorrect Answers:
A: Even Windows 98 computers can use Windows Update Manager to connect to Windows Update. There is no need to upgrade Windows 2000 Professional client computers to Windows XP Professional. The issue you have has to do with Windows 2000 Service Pack 3 not being installed to enable Automatic Updates client software to

work.
B: The functional level of the domain is irrelevant because it does not affect Windows Update or Automatic Updates features at all.
D: This is unnecessary because Automatic Updates client software already runs in the security context of the local system account. This account has the needed administrator rights.

QUESTION 63:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com network is spread over five different buildings. All these building are connected in a local area network (LAN) that runs at 100 Mbps.
A new Certkiller .com directive states that Internet Protocol Security (IPSec) should be used to encrypt all communication between the computers that are used by the Research Department and the Development department. These two departments are located in different buildings.
Both departments have a server that has Routing and Remote Access enabled and is configured as routers, respectively. The other computers on each of these servers' subnets make use of their local servers as their default gateway. To comply with the new Certkiller .com directive you need to implement IPSec in tunnel mode on these two servers by means of creating a custom IPSec policy on each server.
What should you do?

A. On the policy, enable and configure tunnel mode.
B. On each filter in the policy, enable and configure tunnel mode.
C. On the server, enable and configure tunnel mode.
D. On each rule in the policy, enable and configure tunnel mode.

Answer: D

Explanation: For each rule (two rules), you should select the option "The tunnel endpoint is specified by this OP address" on the Tunnel Setting tab in the Properties dialog box of the rule. One rule should include the IP address of the remote server as the tunnel endpoint as well as the filters that identify the types of outbound traffic that should be encrypted. The other rule should include the IP address of the local server as the tunnel endpoint and filters that identify the types of inbound traffic to be accepted via the tunnel. When you enable and configure tunnel mode for each rule in the policy, you will ensure that communications between these two departments will be encrypted.
Incorrect answers:
A: You do not enable and configure tunnel mode for the policy itself. You need to configure each rule in the policy to use the tunnel mode.
B: This is incorrect. You need to enable and configure the filters to define the type of traffic that should be managed by the policy.

C: You do not enable and configure tunnel mode for the server. Only one policy at a time can be assigned to a server, and you enable tunnel mode for each rule in the assigned policy.

QUESTION 64:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. Half the servers on the Certkiller .com network run Windows Server 2003 and the rest run Windows 2000 Server or Windows NT 4.0. Half the client computers run Windows XP Professional, and the rest Windows 2000 Professional or Windows NT 4.0 Workstation.
Certkiller .com has its headquarters in Chicago and branch offices in Dallas, Houston, and Miami. All servers located at the Chicago headquarters premises run Windows Server 2003 and all client computers run Windows XP Professional. T3 lines currently connect each branch office to the Chicago headquarters office. Users at the three branch offices send data over the T3 line to the Chicago headquarters office.
An attacker has managed to intercept and tamper with data as it traversed over the WAN link connecting the Dallas office and Chicago headquarters office. You are instructed to:
1. Secure all data communications traversing over WAN links between the Chicago headquarters office and all three branch offices.
2. Ensure that the security breach incident do not occur in the future.
3. Minimize any expenses incurred as a result of implementing your solution.
You upgrade all WAN routers that connect the T3 lines to routers at the Chicago headquarters office to Windows Server 2003. You must still perform the configuration that will secure data communications between the Chicago headquarters office and the three branch offices. You want to use the least amount of administrative effort to accomplish your task.
How should you configure the WAN routers?

A. Configure the routers to use IPSec in Transport Mode.
B. Configure the routers to use IPSec in Tunnel Mode.
C. Configure the routers to use IPSec Authentication Header (AH) in Transport Mode
D. Configure the routers to use IPSec Encapsulating Security Payload (ESP) in Transport Mode.

Answer: B

Explanation: The question states that you have upgraded the WAN routers that connect the T3 lines to
routers at the Chicago headquarters office to Windows Server 2003. This basically allows you to configure the WAN routers to use IPSec in Tunnel Mode. IPSec tunnel mode can be used to provide security for WAN and VPN connections that use the Internet as the connection medium. In tunnel mode, IPSec encrypts the IP header

and the IP payload. With tunneling, the data contained in a packet is encapsulated inside an additional packet. The new packet is then sent over the network. Tunnel mode is typically used for the following configurations: server to server, server to gateway, and gateway to gateway. Tunnel mode only requires the WAN routers at each end of the connection to support IPSec. No computers need to support IPSec. This is especially relevant in your case because there are both Windows NT 4.0 servers and client computers at the branch offices. Windows NT 4.0 servers and client computers do not support IPSec.
Incorrect answers:
A: Transport mode is used to provide end-to-end communication security between two computers on the network, which means that your computers must support IPSec.
C: Transport mode is used to provide end-to-end communication security between two computers on the network, which means that your computers must support IPSec.
D: Transport mode is used to provide end-to-end communication security between two computers on the network, which means that your computers must support IPSec.

QUESTION 65:

You work as the security administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
An enterprise root certification authority (CA) exists on the Certkiller .com network.
A new Certkiller .com security policy dictates that:
1. All computers must be able to make use of IPSec for communication purposes within the Certkiller .com internal network.
2. All computers have to make use of certificates for mutual authentication.
You need to ensure that these requirements are adhered to.
What should you do?

A. Acquire a computer certificate from a commercial Certification Authority (CA). Place it into a shared folder on a files server.
Then instruct users to copy the certificate to the \Windows\System32 folder on their client computers.
B. Acquire a computer certificate from an enterprise Certification Authority (CA). Use the Software Settings policy in the Default Domain Policy GPO to distribute the certificate to all client computers.
C. Configure an auto-enrollment policy for users in a new GPO.
Then link the GPO to the domain.
D. Configure an Automatic Certificate Request Settings policy for computers in the Default Domain Policy GPO.

Answer: D

Explanation: For two computers to use IPSec to communicate with each other, each of the computers should have a computer certificate and should trust the certificate

of the other computer. To automatically deploy computer certificates on your network, you can configure the appropriate Automatic Certificate Request Settings for computers in the Default Domain Policy GPO. This policy will force each computer on your network to automatically submit a certificate request to your enterprise CA.
Incorrect Answers:
A: Certificates should be installed in appropriate certificate stores, either local or in Active Directory. Simply copying a certificate file to the \Windows\System32 folder would not install the certificate on the computer. Also, each computer should be issued a unique certificate.
B: Software Settings policies are used for deploying applications with the Windows Installer .msi packages.
C: By default, the Enroll certificates automatically option is enabled for both users and computers in the Default Domain Policy GPO.

QUESTION 66:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
Certkiller .com is currently working together with another company in a joint venture. The partner company makes use of its own private root certification authority (CA). There is currently an enterprise root certification authority (CA) that exists on the Certkiller .com network.
A new Certkiller .com security policy dictates that:
1. All computers have the ability to use IPSec for communication purposes within the Certkiller .com internal network.
2. All computers must make use of certificates for mutual authentication.
3. All computers should use IPSec to communicate with computers on the network of a partner company.
You need to ensure that these requirements are adhered to.
What should you do?

A. You should acquire a computer certificate from a commercial CA.
Then import it into the Personal computer certificate store on all Certkiller .com computers.
B. You should acquire a user certificate from a commercial CA.
Then import it into the Personal user certificate store on all Certkiller .com computers.
C. You have to automatically issue computer certificates from your enterprise CA to all Certkiller .com computers using a GPO.
Then import the root CA certificate of the Certkiller .com partner company into the Trusted Root Certification Authorities user certificate store.
D. You have to automatically issue user certificates from your enterprise CA to all Certkiller .com users using a GPO
Then import the root CA certificate of the Certkiller .com partner company into the

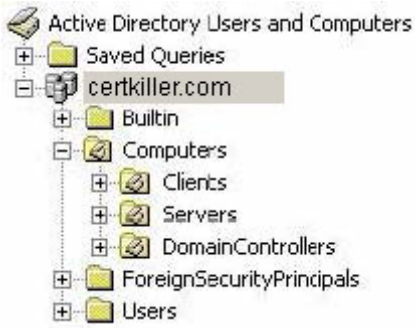
Trusted Root Certification Authorities user certificate store.

Answer: C

Explanation: For two computers to use IPSec to communicate with each other, each of the computers should have a computer certificate and should trust the certificate of the other computer. To automatically deploy computer certificates on your network, you can configure the appropriate Automatic Certificate Request Settings for computers in the Default Domain Policy GPO. This policy will force each computer on your network to automatically submit a certificate request to your enterprise CA.
All computers on your network automatically trust all certificates issued by your enterprise CA, and, therefore, they all trust each other's certificates. To ensure that computers on Certkiller .com's network also trust the certificates issued by the partner's enterprise CA, you can add the partner's root CA certificate to the Trusted Root Certification Authorities policy in the Default Domain Policy GPO. This policy will force all computers on your network to import this certificate into their corresponding certificate store.
Incorrect Answers:
A: If you acquired a computer certificate from a commercial CA and deployed it to the Personal computer certificate store on each computer on your network, then all your computers would appear to have the same identity. However, the actual computer names would not match the subject name in the certificate. This would prevent your computers from using IPSec to communicate with each other unless you also deploy a unique computer certificate from your enterprise CA to each computer or configure IPSec to allow Kerberos V5 or pr-shared key authentication instead of certificate authentication. This option does not enable your computers to trust the partner's computers' certificates issued by the partner's private CA.
B: For IPSec communications, computers must have computer certificates, but users on those computers are not necessarily required to have user certificates.
D: There is no user policy to automatically submit certificate requests on behalf of users or to import a certificate into the Trusted Root Certification Authorities user certificate store.

QUESTION 67:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network contains five domain controllers, ten member servers, and 1,000 client computers. The OU structure is as follows:
1. All client computers reside in the Clients OU.
2. All member servers reside in the Servers OU.
3. All domain controllers reside in the DomainControllers OU.
The OU structure is illustrated in the following Exhibit.



The Certkiller .com written security policy dictates that all logon attempts that use a local user account on any computer must be logged. To this end you are planning to employ group policy to implement this requirement, as well as other security related settings to all computers in the Certkiller .com domain.
You need to ensure that in the event of further changes being made to the security policy, you are able to redeploy and refresh these settings, as well as to ensure that you can verify the security settings during periodic audits.
What should you do? (Each correct answer presents part of the solution. Choose two.)

A. Create a new GPO and link it to the Computers OU.
B. Create an administrative template with the desired settings and import it into the GPO.
C. Create a new GPO and link it to the CLComputers OU.
D. Create an IPSec policy with the desired settings and import it into the GPO.
E. Create a new GPO and link it to the Servers OU.
F. Create a security template with the desired settings and import it into the GPO.
G. Create a new GPO and link it to the DomainControllers OU.

Answer: A, F

Explanation: Security templates are collections of policy settings that can be applied to a local computer, imported to a GPO, or used to analyze security. You can define the desired policy settings using the Security Templates
MMC. After the template is configured, you can apply the template to local policy on a computer or when applying the settings to a collection of users or computers, import the template into a GPO. Once applied, the security settings can be analyzed and verified using the Security Configuration and Analysis tool, which is used to is used to configure a computer with a security template or to compare the current computer settings with the settings in a security template.
Incorrect Answers:
B: The security settings in this scenario are not configured in an administrative template.
C: The security settings in this scenario should apply to all computers in the domain, not just the client computers.
D: The security settings in this scenario include settings other than those found in the IPSec policy.
E: The security settings in this scenario should apply to all computers in the domain, not just the member servers.

G: The security settings in this scenario should apply to all computers in the domain, not just the domain controllers.

QUESTION 68:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All domain controllers and servers on the Certkiller .com network run Windows Server 2003. Half the client computers run Windows XP Professional and the rest run Windows NT 4.0 Workstation.
A Certkiller .com database server named Certkiller -DB02 stores confidential data that is used by all users. Users access a custom financial application named Ck_phtester1 on Certkiller -DB02 to add, modify, and remove data from a database named ProcessingDb on the server. To this end it is absolutely essential that all users must be able to access ProcessingDb on Certkiller -DB02.
The new Certkiller .com written security policy requires all traffic between servers and client computers to be encrypted if possible. You must configure the IPSec policy that will enforce the requirements of the new Certkiller .com written security policy. Your solution must not prevent any client computers from connecting to Certkiller -DB02 and using ProcessingDb. You do not want to upgrade the Windows NT 4.0 Workstations to Windows XP Professional.
What should you do? (Each correct answer presents part of the solution. Choose TWO.)

A. Assign the Server (Request Security) IPSec policy on Certkiller -DB02.
B. Assign the Secure Server (Require Security) IPSec policy on Certkiller -DB02.
C. Assign the Server (Require Security) IPSec policy on all client computers.
D. Assign the Client (Respond Only) IPSec policy on all client computers.
E. Assign the Server (Request Security) IPSec policy on all client computers.

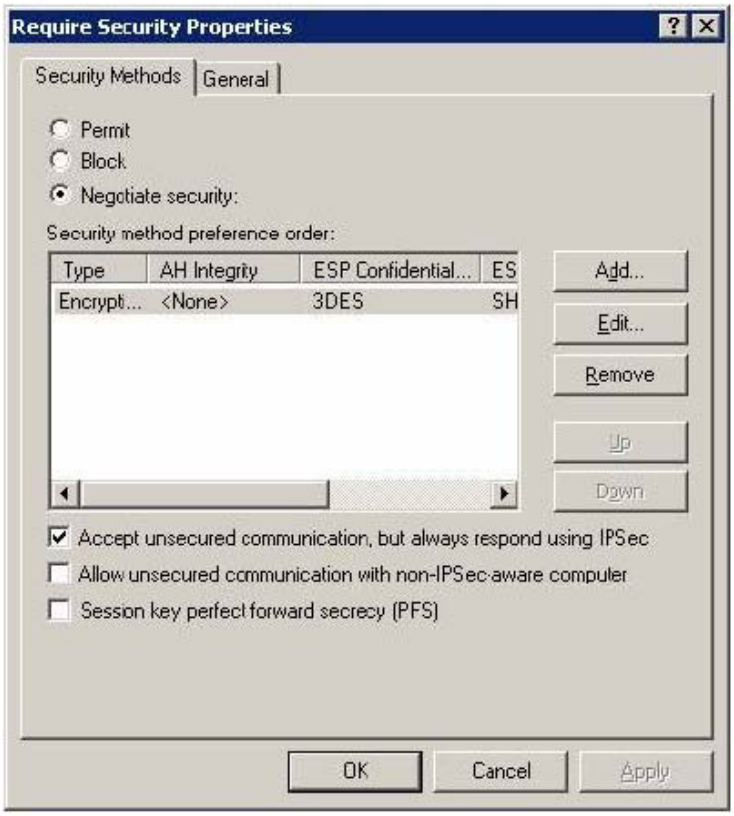
Answer: A, D

Explanation: Because you currently have Windows NT 4.0 Workstation operating system client computers on the network, you need to configure the Server (Request Security) IPSec policy for Certkiller -DB02. Windows NT 4.0 Workstation client computers do not support IPSec. Assigning the Server (Request Security)IPSec policy for Certkiller -DB02 will result in Certkiller -DB02 requesting IPSec to be used for data communications. If the other computer supports IPSec, secure data communication will take place. If the other computer does not support IPSec, Certkiller -DB02 will still allow unsecured communication with that computer. Your Windows NT 4.0 Workstation client computers will therefore still be allowed to establish unsecured data communications to Certkiller -DB02.
The Client (Respond Only) IPSec policy must be assigned to client computers. This will result in client computers responding to IPSec requests from other computers who request it. No client computers will initiate secure data communication.
Incorrect Answers:

B: Because you currently have Windows NT 4.0 Workstation client computers on the network, you cannot assign the Secure Server (Require Security) IPSec policy for Certkiller -DB02. If you do, an unsecure connection will NOT be allowed to be established from a Windows NT 4.0 Workstation client computer to Certkiller -DB02 because Certkiller -SR02 will only allow secure data communications.
C: You configure the Server (Require Security) IPSec policy and Server (Request Security) IPSec policy on computers that you want to initiate secure data communication with other computers.
E: You configure the Server (Require Security) IPSec policy and Server (Request Security) IPSec policy on computers that you want to initiate secure data communication with other computers.

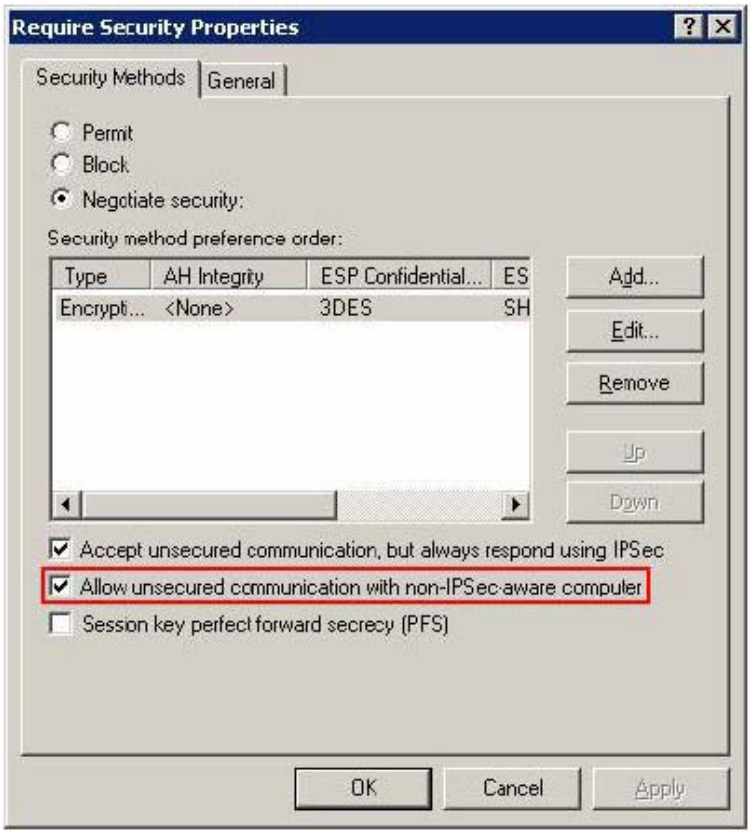
QUESTION 69:

HOTSPOT
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All domain controllers and servers on the Certkiller .com network run Windows Server 2003. Half the client computers run Windows XP Professional and the rest run Windows Me. Active Directory client software is installed on all Windows Me client computers.
All servers are located in an organization unit (OU) named Servers and all client computers are located in an organization unit (OU) named ClientComputers. The new Certkiller .com directive states that all data communications between servers and client computers are to be secured. To this end you create a new Group Policy Object (GPO) named Secure. The Secure GPO assigns a custom IPSec policy named Policy1.
The currently configured Filter Action Properties for Policy1 are illustrated in the Exhibit below:
Exhibit:



The Certkiller .com help desk received several calls from users complaining about connectivity to the servers. You investigate the issue and discover that only Windows Me users are unable to connect to servers. None of the Windows XP Professional users reported problems. You thus need to ensure that all users can access network servers, irrespective of the operating system running on their respective client computers.
What should you do? To answer, modify the settings on the following dialog box accordingly.

Answer:



Explanation:
Because your legacy Windows Me client computers do not support IPSec, you should configure your servers to allow unsecured communication with these client computers. If you update the Filter action to Permit, all traffic will be permitted. If you update the Filter action to Deny, all traffic will be blocked. Selecting the Session key perfect forward secrecy (PFS) option will result in even more security being enforced, but will still prevent Windows Me client computers from connecting to your servers.

QUESTION 70:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers runs Windows XP Professional. Two of the servers are configured to function as two domain controllers.
Certkiller .com recently opened a new staff business college. The staff business college is located at the Certkiller .com corporate headquarters. To accommodate the new staff Business College you:
1. Deploy a new application server named Certkiller -SR05 on the Certkiller .com network.
2. Install a new custom application named Ck_PhTester1 on Certkiller -SR05.
All course material is accessible through Ck_PhTester1.
3. Deploy 30 new Windows XP Professional client computers at the staff business

college.
4. Connect each new client computer to the local area network (LAN).
None of the 30 new client computers in the staff business college are domain members.
The Certkiller .com domain has no public key infrastructure (PKI) deployed. You must ensure that only authorized domain users can access Ck_PhTester1 without incurring any unnecessary overhead.
What should you do?

A. Create a new IPSec policy and configure it so that Encapsulating Security Payload (ESP) using Kerberos authentication is applied for all traffic to Certkiller -SR05.
B. Create a new IPSec policy and configure it so that Authentication Header (AH) using Kerberos authentication is applied for all traffic to Certkiller -SR05.
C. Create a new IPSec policy and configure it so that Authentication Header (AH) using certificate-based authentication is applied for all traffic to Certkiller -SR05.
D. On Certkiller -SR05, change the local security policy so that the Digitally sign server communication (always) security policy is enabled to authenticate all traffic to Certkiller -SR05.

Answer: B

Explanation: In Windows Server 2003, IPSec uses the Authentication Header (AH) protocol and Encapsulating Security Payload (ESP) protocol to provide data security. In your case, you only need to use AH. AH provides data authentication and integrity, and can therefore be used on its own when data integrity and authentication are relevant factors and confidentiality is not. This is because AH does not provide for encryption like ESP, and therefore cannot provide data confidentiality. With AH, a digital signature is used to verify the identity of the sender of the information. IPSec can use Kerberos, a preshared key, or digital certificates for authentication. Because you do not have a PKI, you should configure the IPSec policy so that Kerberos authentication is used.
Incorrect Answers:
A: Authentication Header (AH) and Encapsulating Security Payload (ESP) can be used separately, or together. ESP ensures data confidentiality through encryption, data integrity, data authentication, and other features that support optional anti-replay services. To ensure data confidentiality, a number of symmetric encryption algorithms are used. You do not need to encrypt data being sent to and from Certkiller -SR05. Encryption results in additional overhead on each packet.
C: You cannot use certificate based authentication because this method of authentication is dependent on a PKI implementation. You would have to first deploy a PKI, which would result in additional expenses.
D: The Digitally sign server communication (always) security policy would cause Certkiller -SR05 to digitally sign data before it sends the data over the network. No mutual authentication between client and server would occur.

QUESTION 71:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers runs Windows XP Professional.
Your duties include the administration of the Active Directory domain. There are two client computers named Certkiller -WS297 and Certkiller -WS299 that has accounts in the Certkiller .com domain. The Certkiller -WS297 computer account resides in the Sales organizational unit (OU) and the Certkiller -WS299 computer account resides in the Research OU. The CIO requested that you ensure that all data packets transmitted between Certkiller -WS297 and Certkiller -WS299 must be digitally signed, but NOT encrypted. Now you need to ensure that the digital signing method that you choose can support the signing of multiple network communications protocols.
What should you do?

A. Make use of SSL to digitally sign data packets transmitted between Certkiller -WS297 and Certkiller -WS299.
B. Make use of IPSec ESP to digitally sign data packets transmitted between Certkiller -WS297 and Certkiller -WS299.
C. Make use of IPSec AH to digitally sign data packets transmitted between Certkiller -WS297 and Certkiller -WS29901.
D. Make use of SMB Message Signing to digitally sign data packets transmitted between Certkiller -WS297 and Certkiller -WS299.
E. Make use of DES to digitally sign data packets transmitted between Certkiller -WS297 and Certkiller -WS299.

Answer: C

Explanation: IPSec AH must be used to digitally sign data packets transmitted between Certkiller -WS297 and Certkiller -WS299. AH processes a data packet by means of hashing algorithm which creates the digital signature that is transmitted with a data packet. When an IPSec AH supportive computer receives a digitally signed packet, it will process the packet with the same hashing algorithm and compare the digital signature it created against the digital signature that was sent with the packet. IPSec AH can be used to digital sign multiple protocols, e.g. Server Message Block (SMB) packets and IP packets.
Incorrect answers:
A: SSL is used to encrypt Web communication. Encryption is not required.
B: IPSec ESP is used to encrypt IP packets. Encryption is not a requirement.
D: SMB message signing should be used to digitally sign communication to and from Windows NT 4.0 computers since they do not support IPSec AH. In this scenario there are no Windows NT 4.0 computers.
E: DES is used in an encryption algorithm that can be used to encrypt network files or network traffic. Data encryption is not required.

QUESTION 72:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All domain controllers and servers on the Certkiller .com network run Windows Server 2003, and all client computers runs Windows XP Professional. IPSec is used to secure data communications between servers and client computers.
A server named Certkiller -SR03 is configured as a file server and currently hosts the shared folders that are accessed by all users. Certkiller -SR03 also runs Microsoft Exchange.
The current IPSec policy configured and applied to Certkiller -SR03 has the following rules:
1. Rule 1:
* Filters traffic from all IP addresses.
* Filter Action: Negotiate Security - ESP using SHA1 and 3DES.
* Kerberos authentication.
1. Rule 2:
* Filters SMTP traffic from Certkiller -SR22.
* Filter Action: Permit
1. Rule 3:
* Filters SMTP traffic from all IP addresses.
* Filter Action: Negotiate Security - AH using SHA1.
* Kerberos authentication.
Amendments to the Certkiller .com written security policy includes a number of new security requirements for Certkiller -SR03 which you must enforce:
1. Firstly, all SMTP traffic between Certkiller -SR03 and clients must be encrypted. Other than for this, no traffic need be encrypted.
2. Secondly, all computers that belong to the Certkiller .com domain must be able to access shared folders on the server.
3. Thirdly, another computer named Certkiller -SR22 must be able to access Certkiller -SR03 by using SMTP. Certkiller -SR22 is not a member of the Certkiller .com domain.
To this end you apply the Client (Respond only) IPSec policy to all client computers on the network. You still need to update the current IPSec policy to incorporate each requirement of the written security policy amendments. You do not want to add Certkiller -SR22 to the Certkiller .com domain.
What should you do? (Each correct answer presents part of the solution. Choose two.)

A. Reorder the existing rules to be: Rule 2, Rule 3, and Rule 1.
B. On Rule 1, modify the Filter Action to be Negotiate security - AH Kerberos authentication.
C. On Rule 2, modify the Filter Action to be Negotiate security - AH Certificates authentication.
D. On Rule 3, modify the Filter Action to be Negotiate security - ESP Kerberos

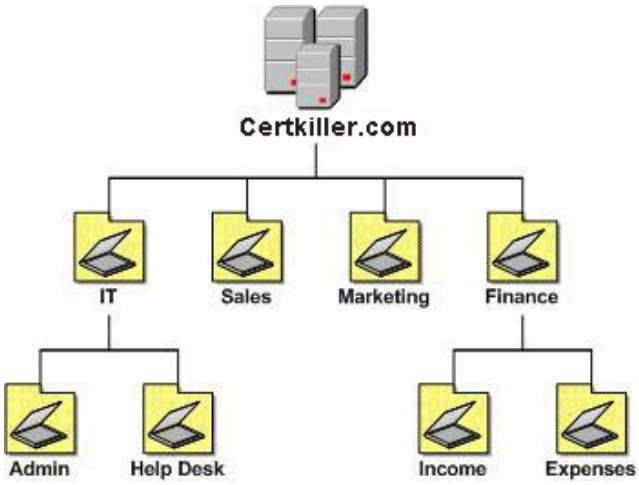
authentication.

Answer: B, D

Explanation: Because all SMTP traffic between Certkiller -SR03 and clients must be encrypted, you need to change Rule 3 by modifying the Filter Action to be Negotiate security - ESP Kerberos authentication. ESP ensures data confidentiality through encryption, data integrity, data authentication, and other features that support optional anti-replay services. To ensure data confidentiality, a number of symmetric encryption algorithms are used. Secondly, because no other traffic needs be authenticated, you need to change the Rule 1 by modifying the Filter Action to be Negotiate security - AH Kerberos authentication.
Incorrect answers:
A: The current order of application of the three rules does not need to be modified because more specific rules have precedence over less specific rules.
C: If you change Rule 2 by modifying the Filter Action so that it is Negotiate security - AH Certificates authentication, you will be preventing Certkiller -SR22 from accessing Certkiller -SR03.

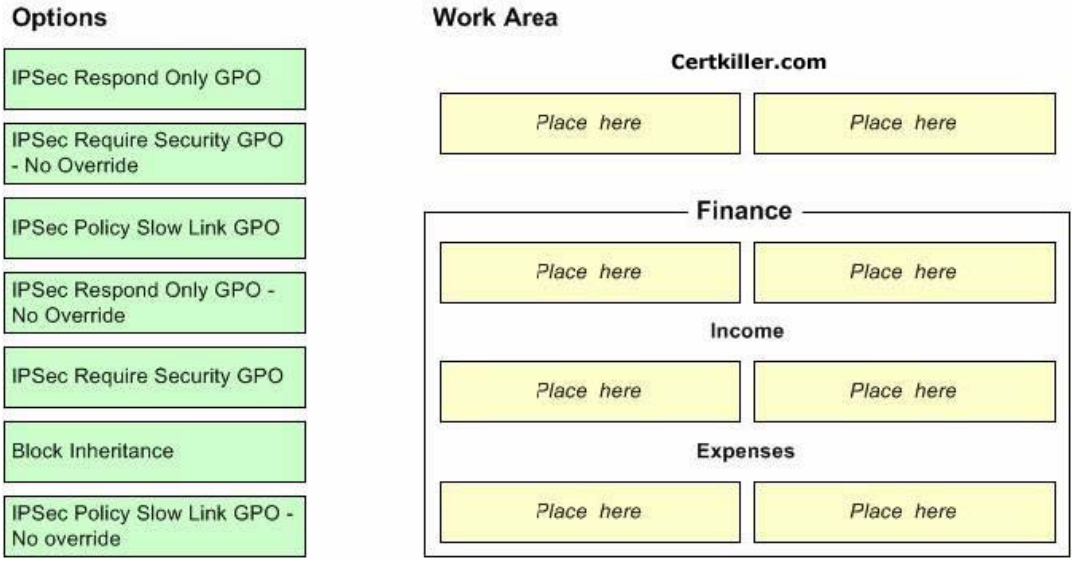
QUESTION 73:

DRAG DROP
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
You have created an OU for each of the Certkiller .com departments, named Sales, Marketing, Finance, and IT. The following Exhibit displays The Certkiller .com Active Directory structure is illustrated in the following Exhibit:
Exhibit:

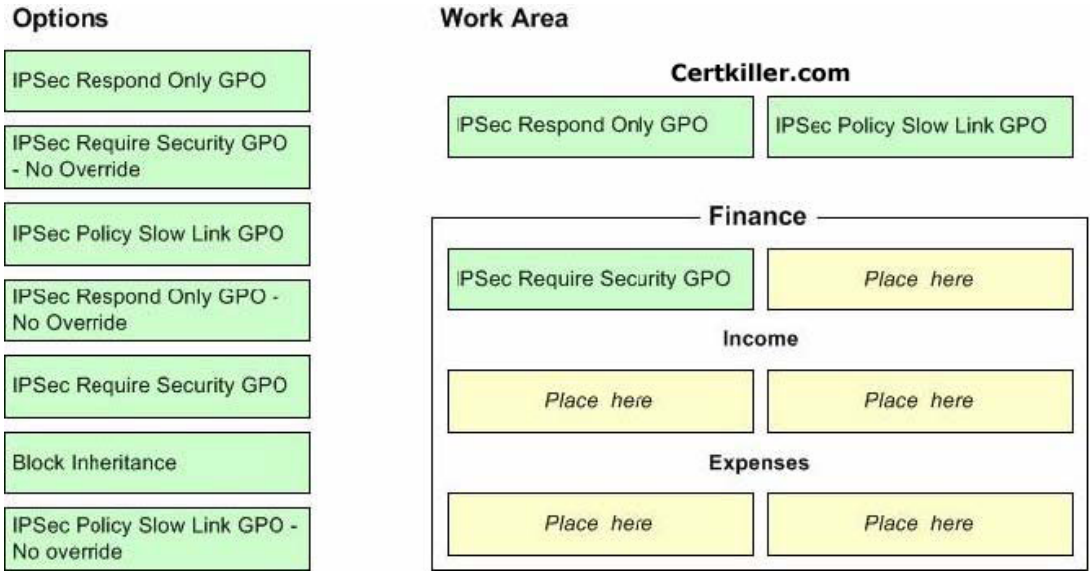


Certkiller .com, who handles classified financial data, requires you to secure all critical financial data on the local computers in the Finance department and whenever finance data is transmitted over the network. You plan to employ IP Security (IPSec) to ensure the confidentiality of the finance data.

You need to ensure that data is encrypted whenever it is transmitted by computers in the Finance department to computers within the network, and that all other computers within the network only use IPSec to communicate with computers in the Finance department. You should also ensure that all IPSec policies assigned to computers will be applied regardless of the network speed.
After a great deal of consideration, you find that Group Policy is the best method of achieving your objectives. You need to ensure that Group Policy is applied correctly.
What should you do? To answer, select the appropriate option or options and place then in the appropriate location in the work area.



Answer:



Explanation:
By linking a Group Policy object (GPO) to the Finance OU that configures an IPSec policy to require security, you will force all of the Finance computers to only

communicate using IPSec encryption. To allow the other computers in the network to communicate with the computers in the Finance department, they must also use IPSec. Since the computers outside the Finance department do not need to use IPSec to communicate with each other, you can configure a GPO at the domain level that will enable the IPSec Respond Only Policy.
To ensure that all IPSec policies configured with a GPO are applied no matter what the network speed is, you must configure a GPO that forces IPSec policies to process regardless of a slow link. By linking the GPO to the domain, it will apply to all OUs that have GPOs with IPSec policies.

QUESTION 74:

You work as the security administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. All computers on the Certkiller .com network are joined to the domain and all client computers reside in an organizational unit (OU) named Client_Computers.
A server named Certkiller -SR01 has been configured to function as an application server. Certkiller -SR01 supports multiple applications. One of the applications hosted on Certkiller -SR01 is a conferencing application named MeetingHost. When client computers are participating in a conference session, MeetingHost makes use of multicast transmissions to broadcast the conference data.
You have been instructed to secure communications to and from Certkiller -SR01. To this end you configured an IPSec policy on Certkiller -SR01.
Immediately after the configuration of the IPSec policy on Certkiller -SR01, you received complaints from some of the Certkiller .com users who need to participate in a conference session that they are unable to make use of MeetingHost. Now you need to modify the registry on Certkiller -SR01 to enable these users to participate in conferences using MeetingHost. All multicast transmissions to and from Certkiller -SR01 should thus be exempted from the IPSec policy application.
What should you do?

A. Create a new entry named NoDefaultExempt with a DWORD value of 0 under the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\IPSEC registry key.
B. Create a new entry named NoDefaultExempt with a DWORD value of 1 under the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\IPSEC registry key.
C. Create a new entry named NoDefaultExempt with a DWORD value of 2 under the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\IPSEC registry key.
D. Create a new entry named NoDefaultExempt with a DWORD value of 3 under the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\IPSEC registry key.

Answer: Btoo

Explanation: In Windows Server 2003, the default filtering exemptions will allow ISAKMP traffic, inbound multicast traffic and broadcast traffic, whereas Windows 2000

Server-based default filtering exemptions allows broadcast, multicast, Kerberos, RSVP, and ISAKMP traffic. You can manually configure filtering exemptions in Windows Server 2003 for the traffic types that were previously available by configuring the DefaultNoExempt entry with a 0, 1, 2, or 3 value. In this case you should use a value of 1 to exempt, or allow outbound multicast traffic. A value of 1 exempts all multicast traffic from IPSec filtering.
Incorrect answers:
A: A 0 value will result in applying the Windows 2000 default setting to computers that are running Windows Server 2003. This means that multicast, broadcast, SVP, Kerberos, and ISAKMP traffic will be exempted from IPSec filtering.
C: A 2 value would exempt RSVP, Kerberos, and ISAKMP traffic.
D: A 3 value will exempt only ISAKMP traffic from IPSec filtering which is the default setting in Windows Server 2003.

QUESTION 75:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers runs Windows XP Professional.
The Certkiller .com written security policy dictates that there should not be any unsecure data communication between client computers and serves. Thus IPSec is used to secure all data transmissions between client computers and servers.
While monitoring network traffic, you notice that no secure data communications are occurring between client computers and a few file server computers. You suspect that the recently configured and applied IPSec policies have configuration errors, which resulted in the Certkiller .com written security policy not being enforced.
You must immediately ensure that the requirements stipulated in the Certkiller .com written security policy are enforced. To this end you need to reconfigure any misconfigured IPSec policy and re-apply the re-configured IPSec policies with immediate effect.
What should you do?

A. Configure the IPSec policy as Dynamic using the netsh command.
B. Configure the IPSec policy as Static using the netsh command.
C. Assign the IPSec policy in the Default Domain Policy GPO.
D. Change the startup type of the IPSec service to Manual.

Answer: A

Explanation: In Windows Server 2003, the netsh command-line utility replaces the previously used Ipsecpol.exe command-line utility. You can use the netsh command-line utility to view information on IPSec policies, configure startup security for computers, configure default traffic exemptions, enable IPSec driver event logging, and troubleshoot IPSec configuration. The current (active) IPSec

policy configuration is affected by the netsh ipsec dynamic mode commands, which means that the IPSec dynamic mode commands directly change security policy settings in the security policy database.
Incorrect answers:
B: The netsh ipsec static mode commands are used to perform the same management tasks as is available in the IP Security Policy Management snap-in. You can create IPSec policies, edit existing IPSec policies, and assign IPSec policies. However, the active IPSec policy configuration remains unchanged, which means that your changes are not immediately updated in the security policy database.
C: If you apply the IPSec policy in the Default Domain GPO, then the security policy settings will be applied to all computers that belong to the Certkiller .com domain. The question states that you want to apply any reconfigured IPSec policies immediately to the misconfigured server computers.
D: If you change the startup type of the IPSec service to Manual, you would have to manually start the IPSec service whenever you restart a member server that has IPSec policies applied.

QUESTION 76:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. All users and computers belong to the Certkiller .com domain.
An enterprise root Certification Authority (CA) is deployed on a server named Certkiller -SR12.
You receive instruction to enforce the following requirements of new Certkiller .com written security policy:
1. IPSec must be used to secure data communications between all computers on the network.
2. Certificates must be used for mutual authentication.
You want to ensure that all certificates are automatically deployed to all computers on the Certkiller .com network. You also want autoenrollment enabled for all domain users and computers.
What should you do next? (Each correct answer presents part of the solution. Choose two.)

A. Configure an Automatic Certificate Request Settings policy for computers in the Default Domain Policy Group Policy Object (GPO).
B. Configure a new Group Policy Object (GPO) to apply an autoenrollment policy for all users.
Link the GPO to the Certkiller .com domain.
C. Request a computer certificate from the enterprise CA.
Add the computer certificate to a shared folder on the network..
Instruct all users to copy the computer certificate to their client computers.
D. Enable the Enroll certificates automatically option for users and computers in the

Default Domain Policy Group Policy Object (GPO).

Answer: A, D

Explanation: Before computers can participate in secure IPSec data communications, each computer must have a unique computer certificate. In addition to this, each computer must trust the certificate of the other computer. To automatically deploy computer certificates to all computers on the Certkiller .com network, and to force each computer to request a certificate, you need to configure an Automatic Certificate Request Settings policy for computers in the Default Domain Policy GPO. To enable autoenrollement for your domain users and computers, you need to enable the Enroll certificates automatically option in the Default Domain Policy GPO.
Incorrect answers:
B:
The computers on the network need to be issued with computer certificates. Configuring a new GPO to apply an autoenrollment policy for all users is not necessary. You can enable autoenrollement for your domain users and computers, by enabling the Enroll certificates automatically option in the Default Domain Policy GPO.
C: Getting your users to copy a computer certificate to their client computers does not install the certificate on their respective computers. Each computer requires a unique computer certificate. The same certificate cannot be used for all computers on the network.

QUESTION 77:

You work as a network security administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The following list details the currently applied Certkiller .com domain security:
1. Kerberos V5 is used for authentication purposes.
2. IPSec is used to secure all communications between client computers and a server named Certkiller -SR30 that contains sensitive information.
3. DNS is used for name resolution purposes.
4. DHCP is used for dynamic address allocation purposes.
You have received instruction from the CIO to ensure that Kerberos is functioning properly.
What should you do?

A. Use the Netsh utility.
B. Use the IPSec Monitor.
C. Use the Netdiag utility.
D. Use the Replication Monitor.

Answer: C

Explanation: To test Kerberos functionality you should issue the Netdiag /test:Kerberos command. Apart from authentication testing, this command will also provide domain information and a cached ticket list.
Incorrect answers:
A: Netsh is used to manipulate the network configuration of a computer and not to test whether Kerberos is functioning properly.
B: IPSec Monitor is used to monitor IPSec statistics and determining whether a connection is secure, it cannot be used to test Kerberos functionality.
D: Replication Monitor is used to monitor replication activities of Active Directory and Active Directory-Integrated DNS zones. It is not used to determine Kerberos functionality.

QUESTION 78:

You work as a network security administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The following list details the currently applied Certkiller .com domain security:
1. Kerberos V5 is used for authentication purposes.
2. IPSec is used to secure all communications between client computers and a server named Certkiller -SR30 that contains sensitive information.
3. DNS is used for name resolution purposes.
4. DHCP is used for dynamic address allocation purposes.
You have received instruction from the CIO to ensure that Kerberos is functioning properly.
What should you do? (Each answer presents a complete solution. Choose two.)

A. Use the Netsh utility.
B. Use the Network Monitor.
C. Use the IPSec Monitor.
D. Use the Netdiag utility.
E. Use the Replication Monitor.

Answer: B, D

Explanation: To test Kerberos functionality you should issue the Netdiag/test:Kerberos command. Apart from authentication testing, this command will also provide domain information and a cached ticket list.
You can also make use of Network Monitor using the Kerbtray.exe and the Klist.exe commands to diagnose Kerberos related issues.
Incorrect answers:
A: Netsh is used to manipulate the network configuration of a computer and not to test whether Kerberos is functioning properly.
C: IPSec Monitor is used to monitor IPSec statistics and determining whether a

connection is secure, it cannot be used to test Kerberos functionality.
E: Replication Monitor is used to monitor replication activities of Active Directory and Active Directory-Integrated DNS zones. It is not used to determine Kerberos functionality.

QUESTION 79:

You work as the network administrator at Certkiller .com. Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers located at the company premises run Windows XP Professional.
The Certkiller .com network consists of an internal network and a perimeter network. One firewall secures the perimeter network from the Internet and another firewall secures the internal network from the perimeter network. The Sales department users have been issued laptop computers since their job detail includes extensive traveling. These laptop computers run either Windows XP Professional or Windows 98 and a dial-up connection provides connectivity to the corporate network.
You are instructed to implement a VPN server on the corporate network. The VPN server will be used in future to provide connectivity to the corporate network for remote users. You plan to place the VPN server on the perimeter network. You need to configure the network protocols on your VPN server that will achieve these objectives without opening any unnecessary ports on the firewall. You need to choose the appropriate network protocols. The network protocols you choose must ensure user authentication through certificates, data encryption, and data integrity. What should you do? (Each correct answer presents part of the solution. Choose two.)

A. You should enable Point-to-Point Tunneling Protocol (PPTP).
B. You should enable IP Security (IPSec)
C. You should enable Microsoft Point-to-Point Encryption (MPPE).
D. You should enable Layer 2 Tunneling Protocol (L2TP).

Answer: B, D

Explanation: A better method than using PPTP tunneling is L2TP/IPSec tunneling. With L2TP/IPSec tunneling, a secure encrypted session is established between the client and server. The client establishes a L2TP tunnel to the server. The server then sends the client an authentication challenge. The client responds to the server's challenge, and uses encryption when it sends its challenge response. The server verifies that the challenge response received by the client is valid. If the response is valid, the connection is accepted. While L2TP can provide encryption and compression for encapsulated PPP frames, you have to use Microsoft's implementation of L2TP with the IPSec security protocol. When L2TP is used with IPSec, the highest level of security is assured. This includes data confidentiality and integrity, data authentication, as well as replay protection. You therefore need to

enable both L2TP and IPSec on the VPN server. To configure your Windows 98 client computers to support L2TP/IPSec, you need to install the L2TP/IPSec client software on these computers.
Incorrect answers:
A: L2TP/IPSec tunneling is better than using PPTP tunneling. This is due to PPTP incapacity to ensure data integrity.
C: PPTP encryption can only be utilized when the authentication protocol is EAP-TLS or MS-CHAP. This is due to PPTP using MPPE to encrypt VPN data in a PPTP VPN, and MPPE needing EAP-TLS or MS-CHAP generated encryption keys.

QUESTION 80:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network contains a member server named Certkiller -SR05. Certkiller -SR05 is configured as the stand-alone root CA. A member server named Certkiller -SR04 is configured as the stand-alone certification authority (CA) used to issue certificates.
Users in the Marketing department frequently travel across the country to promote Certkiller .com's products and services. These users utilize their laptop computers to access the internal network over the Internet when they travel to different client locations. A VPN server named Certkiller -SR33 resides on the internal network to provide remote access L2TP/IPsec connections for your mobile users. All mobile marketing users have laptop computers that are domain members.
Several mobile marketing users complain that they cannot obtain certificates for their laptop computers from the stand-alone CA used to issue certificates. You suspect that the stand-alone CA is not trusted by the laptop computers used by your mobile users. You need to ensure that all mobile users can obtain certificates from your stand-alone CA used to issue certificates.
What should you do?

A. Add the root CA's certificate to the Trusted Root Certification Authorities computer certificate store in the Default Domain Policy GPO.
B. Publish the root CA's certificate in Active Directory.
C. Add the stand-alone CA used to issue certificates to the Trusted Root Certification Authorities computer certificate store in the Default Domain Policy GPO.
D. Add the stand-alone CA used to issue certificates to the Certificate Trust List (CTL).

Answer: A

Explanation: A
stand-alone CA is not automatically always trusted by domain members. To enable all Certkiller .com computers to trust the issuing CA, you need to import the root CA's certificate into the Trusted Root Certification Authorities computer certificate

store in the Default Domain Policy GPO. All computers on the Certkiller .com network will then be forced to import this CA certificate to their respective computer certificate store.
Incorrect answers:
B: Publishing the root CA's certificate in Active Directory does not make the certificate trusted by domain members, which in your case are the laptop computers used by your mobile users.
C: The root CA's certificate, and not the stand-alone CA used to issue certificates, should be added to the Trusted Root Certification Authorities computer certificate store in the Default Domain Policy GPO.
D: You would only add self-signing CAs to the CTL, not a stand-alone CA used to issue certificates.

QUESTION 81:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a two Active Directory domain named Certkiller .com and us. Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers runs Windows XP Professional. All Certkiller .com user accounts and resources are located in the Certkiller .com domain. All user accounts and resources used by the Sales department reside in the us. Certkiller .com domain.
You deploy a new wireless IP network for Certkiller .com. Almost all departments have access points (APs), which provide users with wireless connectivity to the wired LAN. All users in the Sales department have laptops that contain 802.11b compliant network adapters. A few other users from the Finance and Marketing departments have also been issued with laptops that contain 802.11b compliant network adapters. Only these computers have wireless connectivity.
The Sales department users require the ability to access the wireless LAN from all areas of the company headquarters and locations. You thus need to:
1. Ensure that only the Sales department users can access the sales wireless LAN.
2. Ensure that all Sales data is secure as its traverses over the wireless LAN.
3. No users without domain user accounts in the us. Certkiller .com domain must be able to select the LAN from their Available Networks list.
To this end you configure MAC filtering on the sales wireless LAN.
What else should you do? (Each correct answer presents part of the solution. Choose two.)

A. Configure a unique Service Set Identifier (SSID) for the sales department's wireless LAN
B. Disable Service Set Identifier (SSID) broadcasting on all sales APs.
C. Configure a unique Service Set Identifier (SSID) for all departments' wireless LAN.
D. Enable Service Set Identifier (SSID) broadcasting on all sales APs.

Answer: A, B

Explanation: You should disable Service Set Identifier (SSID) broadcasting to prevent the computers that are not authorized from viewing the sales wireless LAN in the list of available networks. If SSID broadcasting is enabled, then all users in the company will see the sales wireless LAN in the Available Networks list. After disabling SSID broadcasting, you need to prevent users from accessing the original SSID. You do this by configuring a unique SSID for the sales wireless LAN.
Incorrect answers:
C: You only need to define a unique SSID name for those wireless LANs that needs to be secured.
D: SSID broadcasting is enabled by default. You need to disable SSID broadcasting to secure the sales wireless LAN.

QUESTION 82:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. Certkiller .com has its headquarters in Chicago and branch office in Dallas.
There are many Certkiller .com Sales department users that work out of the office due to their job detail involving extensive traveling. These Sales department users require access to resources on Certkiller .com when out of the office. It is your responsibility to provide the Sales department users with access to the network.
A new Certkiller .com security policy dictates that all remote connections make use of mutual authentication with data encryption. You are in the process of configuring the Remote Access Server to accept dial-in connections for the remote clients. You need to select the appropriate authentication protocol to use on the server so as to comply with the security policy.
What should you do?

A. Use the CHAP authentication protocol.
B. Use the PAP authentication protocol.
C. Use the MS-CHAP authentication protocol.
D. Use the EAP-TLS authentication protocol.
E. Use the SPAP authentication protocol.

Answer: D

Explanation: The Extensible Authentication Protocol (EAP-TLS) is the best option available in the scenario as the protocol supports mutual authentication and data encryption, for even tighter security (EAP-TLS) does not use passwords but digital certificates which can be installed on client computers or smartcards.
Incorrect Answers:
A: The Challenge Handshake Authentication Protocol (CHAP) cannot be used as it does not support the secure exchanging of encryption keys and it does not comply with the written security policy.

B: The Password Authentication Protocol (PAP) cannot be used as it does not support the secure exchanging of encryption keys and it does not comply with the written security policy.
C: The Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) cannot be used as it does not support the secure exchanging of encryption keys and it does not comply with the written security policy.
E: The Shiva Password Authentication Protocol (SPAP) cannot be used. You need to make use of EAP-TLS to comply with the written security policy.

QUESTION 83:

You work as a network designer for Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. You are in the process of designing a wireless network that will use 802.11b standards with PEAP for authentication for a single Active Directory domain named Certkiller .com.
The users of Certkiller .com travel trough out network departments in the office and require consistent connectivity when moving to the different departments. The network already has two IAS servers in place named Certkiller -SR01 and Certkiller -SR03 respectively. You now need to place numerous wireless access points (WAPs) at required locations for providing the users consistent connectivity when moving between locations. It is imperative that the users have consistent connectivity without having to CK authenticate when changing locations.
What should you do?

A. Enable fast reconnect on all the wireless access points (WAPs).
Enable fast reconnect on Certkiller -SR03.
B. Enable fast reconnect on all the wireless access points (WAPs).
Configure half the WAP's as clients of Certkiller -SR01 and the other half as clients of Certkiller -SR03.
C. Configure the Wireless Access Points (WAPs) as clients of Certkiller -SR01.
Enable PEAP fast reconnect on Certkiller -SR01.
On all clients enable PEAP fast reconnect.
D. Enable fast reconnect on Certkiller -SR03.

Answer: C

Explanation: This configuration has the correct settings that meet the wireless client's needs and by configuring the fast reconnects properly you ensure network clients are consistently connected when moving between locations.
Incorrect Answers:
A: This option does not meet all of the required conditions and should not be used in this scenario.
B: This option should not be used because you need all WAPs controlled by Certkiller -SR01.
D: There is no need for this configuration take place at all.

QUESTION 84:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers are portable computers running Windows XP Professional.
The Certkiller .com network contains two Internet Authentication Service (IAS) servers named Certkiller -SR12 and Certkiller -SR22 respectively. You are responsible for the design and the configuration of the Certkiller .com wireless network. Several technicians have been deployed to troubleshoot software and network connectivity problems.
The technicians require consistent connectivity maintained as they move from different locations without the need to re-authenticate when moving about. You are in the process of placing several wireless access points (WAPs) configured to use 802.11b with PEAP at different locations. To this end you received instruction from the CIO to ensure the technicians have consistent connectivity at all times.
What should you do? (Choose all that apply)

A. Enable PEAP fast reconnect on all the wireless access points.
B. Enable PEAP fast reconnect on Certkiller -SR12.
C. Configure the wireless access points to be clients of Certkiller -SR12.
D. Enable PEAP fast reconnect on Certkiller -SR22.
E. Enable PEAP fast reconnect on all the wireless clients.
F. From the available wireless access points configure half as clients of Certkiller -SR12 and half as clients of TESTING-SR22.

Answer: B, C, E

Explanation:
The best way in this scenario would be to configure the wireless access points as clients of Certkiller -SR12 and enable PEAP fast reconnect this will allow for the technicians to roam around without re-authenticating when changing location.
Incorrect Answers:
A: There is no need to make this configuration change as this device will not authenticate the user.
D: There is no need for this to be done unless the wireless access points were configured as clients of Certkiller -SR22.
F: This will not meet the scenario objective as the user would have to re-authenticate every time changing location.

QUESTION 85:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client

computers run Windows XP Professional. There are two domain controllers named Certkiller -DC01 and Certkiller -DC02 respectively. All computers are joined to the domain.
You implement two new Web sites named http://www. Certkiller .com and http://www2. Certkiller .com on a Web server named Certkiller -SR25. http://www. Certkiller .com is destined to provide static content to all the Certkiller .com users and customers. http://www2. Certkiller .com is destined to be a private corporate Web site, accessible only by the Certkiller .com users. All users and customers will be using the Internet to access http://www. Certkiller .com and http://www2. Certkiller .com. Both Web sites are configured to support a wide variety of Web browsers.
You receive instructions to implement the configuration which will result in accomplishing the following requirements:
1. http://www. Certkiller .com must be accessed by users and customers without either of these entities required to provide authentication credentials.
2. Only authenticated domain users may access http://www2. Certkiller .com.
3. All http://www2. Certkiller .com content must be encrypted.
You need to ensure that all users and customers can access http://www. Certkiller .com, while ensuring that only authenticated domain users can access http://www2. Certkiller .com. You also want to secure data transmissions from http://www2. Certkiller .com so that no unauthorized users can interpret the data, even if they manage to intercept it. To meet your requirements for enabling all users and the public to access http://www. Certkiller .com, you implement Anonymous authentication on http://www. Certkiller .com. Now you need to configure http://www2. Certkiller .com.
What should you do? (Each correct answer presents part of the solution. Choose TWO.)

A. Install a server certificate on Certkiller -SR25.
B. Implement Integrated Windows authentication on http://www2. Certkiller .com.
C. Implement Anonymous authentication on http://www2. Certkiller .com.
D. Implement Basic authentication over SSL on http://www2. Certkiller .com.

Answer: A, D

Explanation: You need to ensure that all connections to http://www2. Certkiller .com on Certkiller -SR25 are secure, and all information sent from http://www2. Certkiller .com is encrypted. To do this, you have to install a server certificate on Certkiller -SR25 so that users can authenticate http://www2. Certkiller .com before transmitting confidential data to the site. Because all communications with http://www2. Certkiller .com will be using the HTTPS protocol, all data transmissions will be secured.
Incorrect answers:
B: Implementing Integrated Windows authentication on http://www2. Certkiller .com will not work because you need to enable your domain users to access http://www2. Certkiller .com from over the Internet. Integrated Windows

authentication works well in situations where client computers can access domain controllers to validate credentials.
C: Implementing Anonymous authentication on http://www2. Certkiller .com will result in anyone being able to access the site. This should be prevented for http://www2. Certkiller .com, and only allowed for http://www2. Certkiller .com.

QUESTION 86:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
A Web server named Certkiller -WS09 hosts the Certkiller .com Internet e-commerce Web site. The Certkiller .com partner companies access this Web site to order merchandise offered for sale by Certkiller .com. All partner companies are authenticated by using a certificate when they log on to Web site.
Certkiller -WS09 is issued with a SSL certificate by a Certkiller .com internal stand-alone subordinate certification authority (CA). A different stand-alone subordinate CA is used to issue certificates to partner companies.
The Certkiller .com help desk then received complaints from a new partner company, stating that one of its users cannot connect to the Certkiller .com e-commerce Web site to order merchandise. You need to ensure that the new partner company can connect to the Web site to place orders for merchandise. You instruct the new partner company's user to use Certificate Services Web pages to request a certificate. However, the new partner company's user still complains that he is still unable to connect to the e-commerce Web site to order merchandise.
What should you do?

A. Instruct the new partner company's user to add the internal stand-alone subordinate CA that issued the SSL certificate for Certkiller -WS09 to the Certificate Trust List (CTL) of its computer.
B. Configure an Active Directory trust relationship between the Certkiller .com domain and the other company's domain.
C. Instruct the new partner company's user to use the Certificate Services Wizard to request a certificate.
D. Instruct the new partner company's user to add the internal stand-alone subordinate CA that issued the SSL certificate for Certkiller -WS09 to the Trusted Root Certification Authorities policy of its computer.

Answer: A

Explanation: Because you have used an internal stand-alone subordinate CA, and not an external certification CA that is widely trusted on the Internet, to issue a Web server certificate for Certkiller -WS09, your partner company needs to add your internal stand-alone subordinate CA to the Certificate Trust List (CTL) of its computer The current issue arose because the new partner company's computer

does not trust the CA that issued the SSL certificate to Certkiller -WS09.
Incorrect answers:
B: Active Directory has no impact on certificate-based authentication.
C: You can use the Certificate Services Wizard to request only certificates from enterprise CAs. You have correctly instructed the partner company to use Certificate Services Web pages to request a certificate. The Certificate Services Web pages are used to request certificates from stand-alone CAs.
D: The CA that issued the SSL certificate should NOT be added to the Trusted Root Certification Authorities policy because it is not a root CA. In addition to this, you want the partner company to trust only the CA that issued the SSL certificate used by Certkiller -WS09. You do not want the partner company to trust all certificates issued by your internal CA and its subordinate CAs.

QUESTION 87:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network contains several new Windows Server 2003 server computer running Certificate Services. These servers are configured as enterprise certification authorities (CAs). You plan to configure the servers to issue users with certificates they need for remote access, authentication, and data encryption. You need to ensure that only authorized administrators can approve requests for certificates, issue and revoke certificates, and deny and renew certificates. To this end you create a new global security group named CertAdministrators and add all authorized administrators to this group.
You need to assign the task of issuing and revoking certificates to members of the CertAdministrators group. Only members of the CertAdministrators global security group must be assigned permissions to manage certificates.
What should you do?

A. Add the CertAdministrators group to the Certificate Manager role on each enterprise CA.
B. Assign the Allow - Enroll permission for all certificate templates to the CertAdministrators group.
C. Add the CertAdministrators group to the Cert Publisher group.
D. Ensure that each member of the CertAdministrators group is issued with an Enrollment Agent certificate.

Answer: A

Explanation: In Windows Server 2003, Certificate Services uses role-based administration. Only users that belong to the Certificate Manager role can approve requests for certificates, issue and revoke certificates, and deny and renew certificates. To enable members of the CertAdministrators group to perform these

tasks, you need to add the CertAdministratorsgroup to the Certificate Manager role on each enterprise CA on the network.
Incorrect answers:
B: This will only enable members of the CertAdministrators group to request certificates that uses a certificate template.
C: The Cert Publisher group should only contain CAs, and not administrators, as members.
D: This will only enable members of the CertAdministratorsgroup to request certificates on behalf of other users.

QUESTION 88:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. All users and computers are joined to the Certkiller .com domain.
The Certkiller .com network contains two Windows Server 2003 computers running Certificate Services. Certkiller -SR15 is configured as an enterprise root certification authority (CA), and Certkiller -SR16 is configured as an enterprise subordinate CA. The enterprise subordinate CA is the issuing CA on the Certkiller .com network.
The new Certkiller .com written security policy requires that IPSec be used to secure all data communications between all the Certkiller .com computers. To this end you assign the Autoenroll and Enroll permissions for the Computer Certificate template to all computers joined to the Certkiller .com domain.
You still need to configure the certificate enrollment method which will ensure that all computers joined to the Certkiller .com domain have computer certificates which they can cause for authentication. You want your domain users to use the least amount of administrative effort to install computer certificates on their client computers.
What should you do?

A. Use the Certificate Request Wizard to request certificates for all domain computers from the issuing enterprise CA.
B. In a GPO linked to the domain, navigate to the Computer Configuration/Windows Settings/Security Settings/ Public Key Policies node to configure a Public Key Group Policy.
C. Configure a Certificate Trust List (CTL) that enables computer certificates to be used in the Certkiller .com domain.
D. In a GPO linked to the domain, navigate to the User Configuration/Windows Settings/Security Settings/ Public Key Policies node to configure a Public Key Group Policy.

Answer: B

Explanation: If you are requesting certificates from an enterprise CA, either of the following tools or utilities can be used: Certificates snap-in, Certreq.exe command-line utility, Web enrollment process, or Active Directory Group Policy. If your computers run Windows Server 2003 and Windows XP Professional, you can use Group Policy to automatically enroll users and computers with certificates, without user intervention. The requirement to do this is that Version 2 certificate templates are used for. Because all servers are running Windows Server 2003, Version 2 certificate templates are automatically being used. Autoenrollment Settings uses a grouping of Version 2 certificate templates and Group Policy settings to enable computers to enroll computer certificates automatically at user log on. The Group Policy setting for computer certificates is located under the Computer Configuration/Windows Settings/Security Settings/Public Key Policies node. The default configuration is that computer autoenrollment is enabled. You can choose to renew and revoke certificates automatically, and you can also select to update certificate template types automatically.
Incorrect answers:
A: Using the Certificate Request Wizard to request certificates for all domain computers would be an impossible, time-consuming task. This is manual certificate enrollment method, mainly used when your client computers are running operating systems prior to Windows 2000.
C: A Certificate Trust List (CTL) is a list of trusted root CAs. For each trusted root CA, the CTL specifies the purpose for which the root CA's certificate is used.
D: You need to ensure that all domain computers, and not users, receive computer certificates.

QUESTION 89:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The Certkiller .com intranet Web site is hosted on a Web server named Certkiller -SR11.
Users in the Human Resources department make confidential Certkiller .com employee information available on the Certkiller .com intranet Web site. An application named PersonalApp is used to enable users to access their personal information. All personal information resides in a virtual directory folder named Employee.
The Certkiller .com written security policy only allows employees to access their specific employee file through the intranet Web site. All information in these files is confidential. The security policy also requires all employee information to be encrypted as it is traverses the network.
You need to comply with the Certkiller .com written security policy. You do not want to encrypt all information available on the intranet Web site, other than the employee information.
What should you do? (Each correct answer presents part of the solution. Choose TWO.)

A. Configure EFS to encrypt the Employee virtual directory.
B. Configure the Employee virtual directory to require SSL
C. Install a digital certificate on Certkiller -SR11.
D. Configure Certkiller -SR11 to encrypt secure channel data.

Answer: B, C

Explanation: To ensure that all employee information is encrypted as it is transmitted over the network between Certkiller -SR11 and client computers, you need to firstly install a digital certificate on Certkiller -SR11 and then configure the Employee virtual directory to require SSL. Secure Socket Layer (SSL) is a Windows Server 2003 security protocol which utilizes a public-key technology to provide a secure channel for applications communicating over a non-secure network such as the Internet. SSL is typically used by Web browsers and Web servers for secure communication channels. The SSL protocol functions at the OSI model's network layer to provide encryption for the following protocols: HTTP, LDAP, and IMAP.
Incorrect Answers:
A: EFS is applied to file systems and not to Web servers. Also, when EFS encrypted data is transmitted over the network, it sent in the decrypted format.
D: Secure channel is used between domain controllers and domain member computers, and not between client computers and intranet Web sites.

QUESTION 90:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
All Web servers on the Certkiller .com network are placed in an OU named WebServ. The Certkiller .com network includes a Public Key Infrastructure using an Enterprise Certificate Authority. Recently a fellow network administrator named Clive Wilson created a certificate named WebCert for the Certkiller .com Web servers, and configured it to autoenroll. To this end you created a Group Policy that forces the computers to autoenroll for certificates. You then link this GPO to WebServ.
The next day you try to set up SSL on the Web servers, but find that a certificate is not available, when you check the event log on one of the Web Servers, you encounter an
error message stating that: "Automatic certificate enrollment for local system failed to enroll for one Certkiller .com WebCert certificate (0x800706ba). The RPC is unavailable."
What is the cause of this problem? (Choose all that apply.)

A. A domain controller is not available.

B. The Certificate Authority (CA) is not available on the network.
C. The certificate service on the Certificate Authority (CA) has stopped.
D. The Certificate Authority (CA) is unable to process the request due to high work load.

Answer: B, C

Explanation: The event log error means that the Certificate Authority is either not available on the network or that the certificate service has stopped running on it.
The client computers, in this case the Web servers, cannot establish a Remote Procedure Call (RPC).
Incorrect Answers:
A: If a domain controller were not available, the following error would be present in the event logs: "Automatic certificate enrollment for local system failed to contact a directory server (0x80072751). A socket operation was attempted to an unreachable host. Enrollment will not be performed."
D: If the Certificate Authority is under heavy load and cannot process the request, the following error would be present in the event logs: "Automatic certificate enrollment for local system failed to enroll for one Certkiller .COM WebCert certificate (0x8009400f). An attempt was made to open a certification authority database session, but there are already too many active sessions. The server may need to be configured to allow additional sessions."

QUESTION 91:

You work as the security administrator at Certkiller .com. The Certkiller .com network is a single Active Directory forest named Certkiller .com that spans multiple sites. All servers on the Certkiller .com network run Windows Server 2003 and the client computers run Windows XP Professional. Certkiller .com has its headquarters in Chicago and branch offices in Dallas, Miami and Los Angeles.
Part of your duties includes the management of the network connections between the offices. To this end you thus install five Routing and Remote Access Service (RRAS) servers in the head quarters and a RRAS server in each of the branch offices. The Certkiller .com written security policy dictates that all the head quarters' RRAS servers should be configured to use the same set of remote access policies and authentication methods.
You have received instruction to implement the configuration of all the RRAS servers to comply with the company written security policy with the least amount of administrative effort.
What should you do?

A. Implement an IAS server in each branch office
Configure each IAS server as a RADIUS client.
B. Implement an IAS server in each branch office.
Configure each RRAS server in the branch offices as a RADIUS client.
C. Implement IAS servers in the head quarters.
Configure each head quarters RRAS server as a RADIUS client.

D. Configure each RRAS server to run IAS.
Configure each RRAS server in Certkiller .com as a RADIUS client.

Answer: C

Explanation: IAS is the Microsoft Remote Authentication Dial-In User Service (RADIUS). Implementing an IAS server in the head quarters, configuring the appropriate set of remote access policies on the IAS server would present one part of the solution and then each head quarters RRAS server should be configured as RADIUS clients. You can, with only requiring making use of one IAS server, ensure that the same set of remote access policies and authentication methods are applied to the head quarters' RRAS servers with the least amount of administrative effort.
Incorrect answers:
A: This is an incorrect option to follow since IAS can act only as a RADIUS server or proxy.
B: Implementing an IAS server in each of the branch offices would be futile because the question pertinently states that the head quarters' RRAS servers should be configured with the same set of policies and authentication methods. No mention of configuring the branch offices' RRAS servers is made.
D: This would be impossible since IAS cannot act as server and as client.

QUESTION 92:

You work as the network administrator at Certkiller .com. The Certkiller .com network is a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and the client computers run Windows XP Professional.
There are several Certkiller .com users that require after hours access to the Certkiller .com network when they work from home. To accommodate these users a server named Certkiller -SR02 has been set up to function as a Routing and Remote Access server (RRAS). Certkiller -SR02 has been configured to accept dial-in connections.
The Certkiller .com written security policy states that smart cards should be used for remote access authentication. You now need to change the configuration on Certkiller -SR02 to be in compliance with the company written security policy.
What should you do?

A. Change the Certkiller -SR02 existing configuration to accept only PPTP connections.
B. Change the Certkiller -SR02 existing remote access policies to allow only EAP-TLS authentication.
C. Change the Certkiller -SR02 existing configuration to accept only L2TP/IPSec connections.
D. In the Default Domain Policy GPO, enable the Interactive logon: Require smart card policy.

Answer: B
Explanation
: EAP-TLS (Transport Level Security) is a high-security protocol based on the SSL (Secure Sockets Layer) system used for Web server security. EAP-TLS uses encrypted certificates for authentication. If you are using smart cards or certificates for client authentication, this is the only protocol that supports those types of authentication. To comply with the company written security policy you thus need to change the remote access policies to accept only EAP-TLS authentication.
Incorrect answers:
A: Changing the configuration to accept only PPTP connection will not work since the question pertinently states that dial-up connections will be used to access the Certkiller .com network and PPTP is a point-to-point protocol.
C: If you change the configuration to allow only L2TP/IPSec connection you will not be complying with the company written security policy. Smart cards are typically used with the EAP-TLS authentication method.
D: The Interactive logon: Require smart card policy involves the logging on to a domain and using smart cards is not related to domain logons.

QUESTION 93:

You work as the network administrator at Certkiller .com. The Certkiller .com network is a single Active Directory domain named Certkiller .com. Certkiller .com has its headquarters in Chicago and several branch offices country-wide. You are located in the head quarters.
All servers on the Certkiller .com network run Windows Server 2003. These servers are located on the internal network at the Certkiller .com head quarters and include File Transfer Protocol (FTP) servers, e-mail server, file servers and the domain controllers. The perimeter network has been set up with two computers that run the Microsoft Internet Security and Acceleration (ISA) Server: one is placed between the Internet and the perimeter network and the other is placed between the internal and the perimeter network. The head quarters provides remote access to several users in the branch offices by means of dial-up connections.
It is your duty to manage these dial-up connections. You do this through a server named Certkiller -SR06 which is configured as a Routing and Remote Access Server (RRAS). Due to the vast number of users employed at Certkiller .com, there are many operating systems in use at the various branch offices. These operating systems include Windows 95, Windows 98, Windows 2000 Professional as well as Windows XP Professional. All users are authenticated by domain user account name and password; and that is the only common factor.
You received instruction to accommodate all these users' dial-up connections and to make sure that authentication credential is passed with the strongest encryption possible. You thus need to select the appropriate authentication protocol for each client's operating system. To this end you select to use MS-CHAP for the Windows 95 client computers. Now you need to select an authentication protocol to accommodate the Windows 98, Windows 2000 Professional as well as the Windows XP Professional client computers.

What should you do?

A. Use MS-CHAP.
B. Use MS-CHAP v2.
C. Use SPAP.
D. Use CHAP.
E. Use EAP-TLS.

Answer: B

Explanation: The most secure authentication protocol choice that will accommodate Windows 98, Windows 2000 Professional and Windows XP Professional is MS-CHAPv2 because it supports mutual authentication using encrypted passwords.
Windows 95 is incapable of supporting MS-CHAPv2 and thus you should select MS-CHAP. MS-CHAP supports encrypted authentication albeit not as secure as MS-CHAPv2.
Incorrect answers:
A: MS-CHAP is not as secure as MS-CHAPv2.
C: SPAP is used with Shiva remote access products and is inherently insecure and thus not appropriate in this scenario.
D: CHAP is less secure than both MS-CHAP and MS-CHAPv2. Windows Server 20003 does not store passwords in a format that is supported by CHAP which means you need to enable the Store Passwords Using Reversible Encryption password policy and this will pose an unnecessary security risk.
E: EAP-TLS is used when smart card authentication and other certificated-based authentication mechanisms are in use. EAP-TLS is thus not appropriate in this scenario.

QUESTION 94:

You work as the network administrator at Certkiller .com. The Certkiller .com network is a single Active Directory named Certkiller .com. The servers on the Certkiller .com network and include two domain controllers that run Windows Server 2003 and two Remote Access servers: one running Windows 2000 Server and the other running Windows Server 2003.
Access to the company network is by means of dial-up networking. Consequently all users are issued with laptop client computers that run either Windows XP Professional or Windows 2000 Professional. Currently authentication to the network upon dial-up is through MS-CHAP.
A new Certkiller .com management directive includes:
1. A preference to see all users connect through a Virtual Private Network (VPN) connection as it will improve performance.
2. Making use of Layer 2 Tunneling Protocol (L2TP) with IP Security (IPSec) as the approved VPN protocol.
3. Acquiring another company that offers similar services.
When the last directive materializes there will be double the current amount of users that has to be accommodated. To this end you received instruction to devise a

plan that will allow for the authentication of all the Certkiller .com users, current and new users, whether they connect to the company network via dial-up connection or VPN connection. You need to ensure that the solution is easily scalable since this would only be the first of a whole series of planned acquisitions. There are thus two factors that have to be kept in mind: VPN requirements and scalability requirements.
What changes will enable you to support both requirements? (Each correct answer presents part of the solution. Choose THREE.)

A. Install an Internet Authentication Service (IAS) server and a VPN server in the domain.
Configure the VPN server to use EAP-TLS for authentication purposes.
B. Install an Internet Authentication Service (IAS) server and a VPN server in the domain.
Configure the Remote Access servers and the VPN server to use IAS server for authentication.
Configure the IAS server to use EAP-TLS for authentication purposes.
C. Install an Internet Authentication Service (IAS) server and a VPN server in the domain.
Configure the Remote Access servers to use MS-CHAPv2 for authentication purposes.
Configure the IAS server to use EAP-TLS for authentication purposes.
D. Reconfigure one of the Remote Access servers to be a VPN server in the domain.
Then configure the VPN server to use EAP-TLS for authentication purposes.
E. Install an Internet Authentication Service (IAS) server in the domain.
Configure the VPN server to use IAS server for authentication.
Configure the IAS server to use EAP-TLS for authentication purposes.

Answer: B

Explanation: L2TP/IPSec has to be used in conjunction with computer certificates. For this purpose thus it is best to use EAP-TLS as the authentication method. IAS enables one to authenticate remote access and policy management for multiple access points from a single server in a location. In this case you are required to implement and support a minimum of three access points (with the definite possibility of more to be added in future), thus you would be wise to make use of IAS to centralize the authentication process.
IAS is the Microsoft Remote Authentication Dial-In User Service (RADIUS).
Implementing an IAS server, configuring the appropriate set of remote access policies on the IAS server would present one part of the solution and then each RRAS server and the VPN server should be configured as RADIUS clients.
Incorrect answers:
A: Although configuring a VPN server to support EAP-TLS is possible, it is not a scalable option because each access point is providing its own authentication. This would mean that you may need to maintain any access policies at three locations (and possibly more after more acquisitions.)
C: Configuring the Remote Access servers to use MS-CHAPv2 as authentication method

is not scalable and EAP-TLS as authentication method would be better suited to the conditions.
D: Reconfiguring one of the Remote Access servers to be a VPN server will reduce the resources for dial-up client computers. Furthermore configuring the VPN server to support EAP-TLS would not be scalable since it provides its own authentication. These servers should rather be using the IAS server for authentication purposes.
E: This would only be partly correct since you also need to accommodate the desire of Certkiller .com to cater for the VPN connecting client computers as well. This option will only cater for the dial-in connecting client computers.

QUESTION 95:

You work as the network administrator at Certkiller .com. The Certkiller .com network is a single Active Directory named Certkiller .com. Certkiller .com has its headquarters in Chicago and branch offices in Dallas and Miami. All servers on the Certkiller .com network run Windows Server 2003. Each office is configured as a site. Each site is equipped with at least one domain controller. The sites are connected by means of T1 lines. Authentication is implemented by the Certkiller .com Certificate Authority hierarchy that issues certificates for Secure Sockets Layer (SSL) client authentication on the Web site. The Certkiller .com Virtual Private Network (VPN) access point is located in Chicago and the dial-up access points are located in all three offices.
The Certkiller .com Sales department has been issued with laptop computers to dial in to the company network since they need to travel extensively in the execution of their duties and as such require access to the latest stock on hand data when dealing with customers. They connect to the company network using either the VPN access point or the nearest remote access server. These laptop computers vary and run a mix of Windows XP Professional and Windows Me as well as Windows 2000 Professional.
Due to a recent spoofing of the company's VPN server by a rival company Certkiller .com management has taken a decision to strengthen security by issuing a new company security policy that has to be adhered to: This policy requires all remote access connections to use mutual authentication. And all data sent via VPN connection must be encrypted using the most secure method possible. You need to configure the remote access policies to comply with the new policies.
What should you do?

A. Configure the remote access server to allow only EAP-TLS authentication. Configure the VPN server to allow PPTP with EAP-TLS authentication.
B. Configure the remote access server to allow MS-CHAPv2 authentication. Configure the VPN server to allow L2TP/IPSec with EAP-TLS authentication.
C. Configure the remote access server to allow only MS-CHAPv2 authentication. Configure the VPN server to allow L2TP/IPSec with MS-CHAPv2 authentication.
D. Configure the remote access server to allow only MS-CHAPv2 authentication. Configure the VPN server to allow PPTP with MS-CHAPv2 authentication.

Answer: B
Explanation
: Even though both MS-CHAPv2 and EAP-TLS provide mutual authentication, the Windows Me client computers can only use EAP-TLS for VPN connections using the L2TP/IPSec client software. The only authentication protocol for dial-up connections from Windows Me client computers that offers mutual authentication is MS-CHAPv2.
Incorrect answers:
A: Remote access via dial-in connections using EAP-TLS authentication are not supported on the Windows Me client computers.
C: L2TP/IPSec requires EAP-TLS authentication and cannot be used with MS-CHAPv2 authentication.
D: L2TP/IPSec is more secure than PPTP and should thus be used rather than PPTP when possible.

QUESTION 96:

You work as the security administrator at Certkiller .com. The Certkiller .com network is a single Active Directory domain named Certkiller .com. All servers and domain controllers on the Certkiller .com network run Windows Server 2003 and the client computers run Windows XP Professional.
The Certkiller .com Sales department users travel extensively in the execution of their duties and as such require access to the latest stock on hand data when they are on the road. To accommodate them, Certkiller .com issued the Sales department users with lap top computers to dial in to the network. To lighten the administration workload, you are configuring you a server named Certkiller -SR05, a Remote Access server, to make use of DHCP to provide IP configurations for the dial-up laptop client computers. A server named Certkiller -SR02 functions as the DHCP server.
You create a dial-up connection to the network to test the configuration. However you are unable to access other network resources by using computer names or searching Active Directory, though you can connect successfully establish a connection to Certkiller -SR05. To address the problem you run ipconfig/all from a command prompt and discover that your remote access, dial-up connection, client laptop computer is configured except for the DHCP options. You need to address the problem.
What should you do?

A. Disable TCP/IP filtering in the internal interface of Certkiller -SR05.
B. Create static mapping for the Certkiller -SR05 internal interface to Certkiller -SR02.
C. Configure Certkiller -SR02 as a DHCP relay agent.
D. Configure Certkiller -SR05 as a DHCP relay agent.

Answer: D

Explanation: Windows Server 2003 allows one to configure RRAS as a DHCP relay

agent. Being a DHCP relay agent will facilitate the transmission of DHCP-inform messages. In the event of RRAS being configured to use DHCP for IP configuration, a remote access client will receive an IP address from the RRAS server. Then the RRAS client can use a DHCP-inform message to receive additional DHCP-configured options from the DHCP server.
Incorrect answers:
A: If you disable TCP/IP filtering on the Certkiller -SR05 internal interface, then DHCP-inform messages will not be forwarded to the DHCP server, Certkiller -SR02.
B: Creating static mapping will not allow IP configurations to be assigned to the dial-up client computers. And furthermore, DHCP-inform messages will not be able to pass through Certkiller -SR05 to Certkiller -SR02, the DHCP server.
C: Due to the fact that DHCP relay agents permit DHCP bound broadcast packets to be directed through routers that are not BOOTP-enabled, installing a DHCP relay agent on a DHCP server, in this case Certkiller -SR02, would be futile.

QUESTION 97:

You work as the security administrator at Certkiller .com. The Certkiller .com network is a single Active Directory forest named Certkiller .com. All servers on the Certkiller .com network run either Windows Server 2003; Windows 2000 Server or Windows NT Server 4.0. The client computers run either Windows XP Professional; Windows 2000 Professional, Windows NT Workstation 4.0 or Windows 98. Certkiller .com has its headquarters in Chicago and a branch office in Dallas. The network in each office is connected to the Internet. Each office is equipped with a server that is configured with Routing and Remote Access Services (RRAS). You received instruction from the CIO to establish a connection between the two offices over the Internet in the most secure manner possible.
What should you do?

A. Install L2TP/IPSec client software on all legacy computers in each office.
B. Configure a Router-to-Router L2TP/IPSec connection between the two offices.
C. Configure all the computers to use EAP-TLS authentication exclusively.
D. Configure the RRAS servers to accept PPTP connections.

Answer: B

Explanation: the most secure method to connect two offices in this case would be to configure a router-to-router L2TP/IPSec connection between the two offices via their RRAS servers. L2TP is a tunneling protocol, very similar to PPTP. But L2TP also uses IPSec to secure the connection. IPSec in turn requires computer level authentication by either certificates or pre-shared key. Thus if you implement L2TP/IPSec between the two communicating parties' routers, you will ensure that a secure encrypted tunnel between the two offices is established. All subsequent communication between the two offices will then by through an already encrypted connection.
Incorrect answers:
A: Legacy systems like the Windows NT and Windows 98 computers in the offices will

need to make use of Microsoft L2TP/IPSec VPN Client software in order to be able to use L2TP/IPSec. This can be done and will also work; however, it is not as efficient as a router-to-router L2TP connection between the two offices.
C: PPTP does not support computer level authentication, thus this option will not result in the most secure manner as possible.
D: Only using VPN Client software or using EAP-TLS would not be sufficient for establishing a connection between the two offices.

QUESTION 98:

You work as the security administrator at Certkiller .com. The Certkiller .com network is a single Active Directory domain named Certkiller .com that spans multiple sites. All servers on the Certkiller .com network run Windows Server 2003 and the client computers run Windows XP Professional. Certkiller .com has its headquarters in Chicago and several branch offices in different cities. Each branch office is connected to the headquarters by means of a Virtual Private Network (VPN) connection.
The Certkiller .com Sales department users require access to the latest stock on hand data when they are on the road as they need to travel extensively in the execution of their duties. To this end it has been decided that the Sales department users should connect to the network by dialing in to the Routing and Remote Access Service servers located in the branch office nearest to them. However, each Sales department user may only dial in to the branch office where he or she is assigned. There are different sets of rules that apply to each of the branch office regarding their dial-in connections.
As the security administrator you should be able to control these remote access rules of all the branch offices from the headquarters. You need to accomplish this task with the least amount of administrative effort.
What should you do?

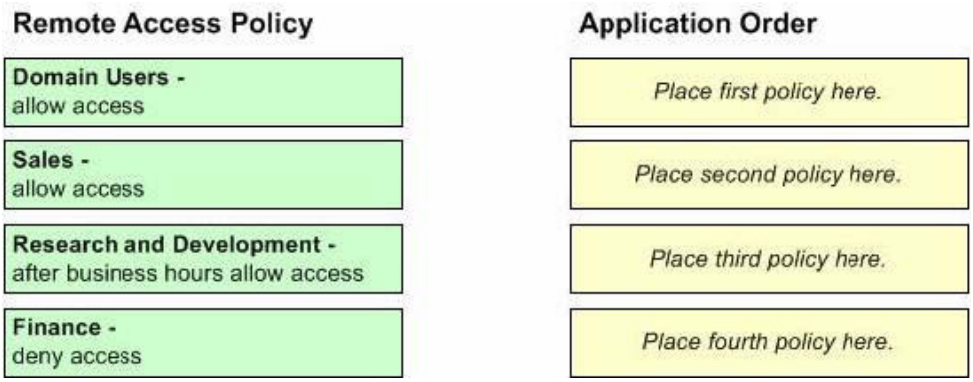
A. Configure a separate set of remote access rules for each branch office in a Group Policy Object (GPO).
Link this GPO to the site in which the branch office is located.
Use a domain controller to manage these GPOs from the Chicago office.
B. Configure a separate set of remote access rules for each branch office in a GPO.
Link this GPO to the domain.
The scope of each GPO should be filtered by assigning the appropriate permissions for the GPO to the RRAS server in the branch office where those specific permissions apply.
C. Configure a separate remote access policy for each branch office in an IAS server in the Chicago office.
You should also configure each RRAS server in the corresponding branch office to use the IAS server for user authentication.
D. Configure the appropriate remote access policies on each RRAS server in the corresponding branch office.
Manage the remote access policies from the Chicago office using Remote Desktop Connections.

Answer: C

Explanation: Remote access policies are used to control Dial-in and VPN access to a network via RRAS servers. These policies can either be configured locally per RRAS server per branch or on a single IAS server from the Chicago office. You can install IAS on a member server at the Chicago office, list all the RRAS servers of the branch offices as its clients and then configure the RRAS servers to forward all incoming connection requests to the IAS server. Furthermore on this IAS server you can also configure the appropriate set of remote access policies to the requests originating from a specific RRAS server.
Incorrect answers:
A: This option would take a lot of administrative effort and would involve you having to go to all the branch offices physically. You also cannot use a domain controller to manage the remote access policy sets of all the RRAS servers. You also cannot control remote access policies through GPOs.
B: This option would take a lot of administrative effort and would involve you having to go to all the branch offices physically. You also cannot control remote access policies through GPOs.
D: Even though it is possible to remotely control RRAS servers via Remote Desktop connections, it would require a whole lot more effort and would be less convenient than managing all the remote access policies on a single IAS server from the Chicago office.

QUESTION 99:

DRAG DROP
You work as a network domain administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
You are responsible for the configuration of remote access policies on the Certkiller .com network. You are currently busy configuring a server named Certkiller -SR07 which has Routing and Remote Access enabled. All the Certkiller .com Active Directory user accounts' dial-in properties are configured to control access by means of remote access policy. Following are the requirements as per the different departments:
1. The regular user's dial-in should be restricted to normal business hours only.
2. The Sales user group's dial-in should be allowed to happen at any time.
3. The Research and Development user group's dial-in should NOT be restricted to normal business hours.
4. The Finance user group's dial-in should be prohibited.
5. Users belonging to both Finance and Sales user groups should also be prohibited.
What should you do? To answer, drag the available remote access policy to the correct location in the work area.



Answer:

Explanation:
the Users' ability to establish remote access connections are controlled by the dial-in settings in the user account properties and remote access policies. The available policies are analyzed in sequence; the first policy whose conditions match the parameters of the incoming call dictates whether the connection should be denied of processed further. Further processing involves the analyzing of the user's dial-in properties, the profile settings and the permission that are specified in the matching remote access policy. Thus, once a matching policy is found, subsequent policies are not analyzed. It is this important to have the remote access policies ordered in such a manner from most specific to most general.
In this specific scenario:
1. The most specific policy is for the Finance users who are prohibited.
2. Followed by the Sales users - this policy should be placed second so that it will apply to the sales users who do not also belong to the Finance group.
3. Follow this with the Research and Development users who are allowed to dial-in at any hour. This policy will thus apply to the Research and Development users who do not belong to either the Sales or Finance users.
4. The most general policy should then follow - this is for the all the Certkiller .com users. This policy will then apply to all users that do not enjoy membership of either Sales, Finance of Research and Development.

QUESTION 100:

You work as the network administrator at Certkiller .com. The Certkiller .com network is a single Active Directory named Certkiller .com. Certkiller .com has its headquarters in Chicago and a branch office in Dallas and Miami. All servers on the Certkiller .com network run Windows Server 2003. Each office is configured as a site. Each site is equipped with at least one domain controller. The sites are connected by means of T1 lines.
The Chicago-based Research department makes use of wireless networking in the labs and the conference rooms. The Research department users belong to the Research group. Work is conducted in the labs from 6 A.M. through 7 P.M. on a daily basis from Monday through Friday. The research department uses the conference rooms for meetings and reporting to the IT manager. These meetings usually occur during normal business hours, between 8 A.M. and 5 P.M., Mondays through Fridays. During normal operating hours all users are allowed to connect to the network from the conference rooms during normal business hours, and the Research group members are allowed to connect to the network. No wireless access is to be granted outside of the normal hours of operation.
The Certkiller .com Sales and Marketing department users travel extensively in the execution of their duties and Certkiller .com issued the Sales and Marketing department users with laptop computers to dial in to the network. Either the VPN access point or the nearest remote access server is used to connect to the company network. These users belong to the Sales Group and the Marketing group respectively.
The policies regarding Access and Authentication for the wireless network is managed by a computer that has been configured as an Internet Authentication Service (IAS) server. The policies that are currently configured are:

Research department Policy	Day and Time Restrictions: 6 A.M. through 7 P.M.; Monday - Friday Windows Groups: Research Grant remote access permission
Conference Room Policy	Day and Time Restrictions: 6 A.M. through 5 P.M.; Monday - Friday Grant remote access permission

The access and authentication management for the remote access servers and the VPN servers are currently handled by granting each Sales and each Marketing user dial-in permissions. This arrangement does not sit well with the Certkiller .com management and they want all authentication policies to be consolidated. The IAS server must be used to determine if a user is granted or denied access to the network, irrespective of the user account settings. To this end you thus require to add a policy to the IAS server to enable it to authenticate all connection attempts. What should you do?

A. Windows groups: Sales or Marketing
Day and Time Restrictions: 24/7
Ignore-User-Dialin-Properties: False
Allow access only through these media: async, virtual

Grant remote access permission.
B. Windows groups: Sales or Marketing
Day and Time Restrictions: 24/7
Ignore-User-Dialin-Properties: True
Tunnel type: PPTP
Grant remote access permission.
C. Windows groups: Sales or Marketing
Ignore-User-Dialin-Properties: True
Allow access only through these media: async, virtual
Grant remote access permission.
D. Windows groups: Sales or Marketing
Day and Time Restrictions: 24/7
Ignore-User-Dialin-Properties: False
Grant remote access permission.

Answer: C

Explanation: Remote Policies are checked until a match is found that either allows or denies access. The first conditions of the policy are checked first. As at matches are found, the checking progresses until access is granted or denied. In this case the condition membership of either Sales or Marketing group. After a match is found, the Ignore-User-Dialin-Properties attribute is checked, if set to true, the dial-in property on the user account is ignored and the remote access permission on the policy is checked. If set to grant remote access permission, the profile settings and the settings on the user account are checked. The profile setting is where you limit connections to the media type being used to access the network. The async media type is used to allow connection via modem and the virtual media type is used to allow connection via VPN.
Incorrect answers:
A: The Ignore-user-dialin-properties should be set to true and not false. If it is set to false as is suggested in this option then the user account will be used to determine if the user should be allowed access.
B: The media condition is specified in the allow access to these media attribute. The tunnel type condition will only apply to VPN connections and not dial-in connections.
D: You are required to allow the IAS server to make the decision regarding allowing or denying access. The Ignor-User-Dialin_property should be set to True to allow this requirement.

QUESTION 101:

You work as the network administrator at Certkiller .com. The Certkiller .com network is a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and the client computers run Windows XP Professional. The network is not connected to the Internet.
Many Certkiller .com users prefer to work from home and thus connect to the company network via a Routing and Remote Access Server (RRAS) named Certkiller -SR03 which is configured to support a bank of dial-up modems. These

work-from-home users are all members of the Telecommute group.
The Telecommute group members are authorized for remote access. All the other users are denies remote access to the network. The only users allowed to connect to the network via multilink connections are the users who belong to the Research group. And the Domain Admins group members are the only users that are allowed to connect to the company network via multilink connections. Following is a list of the remote access policies that has been created:
1. StandardUser - Domain Users group. Access denied.
2. RemoteUser - Telecommute group. Access allowed 6:00 A.M. through 8:00 P.M. Multilink not allowed.
3. Research - the Research group. Access allowed 6:00 A.M. through 10:00 P.M. Multilink allowed.
4. DomainAdmins - Domain Admins group. Access allowed 24/7. Multilink not allowed.
In what order should the remote policies be listed?
To answer, choose the appropriate policy in the right column and place the selections in the list in order on the left column.

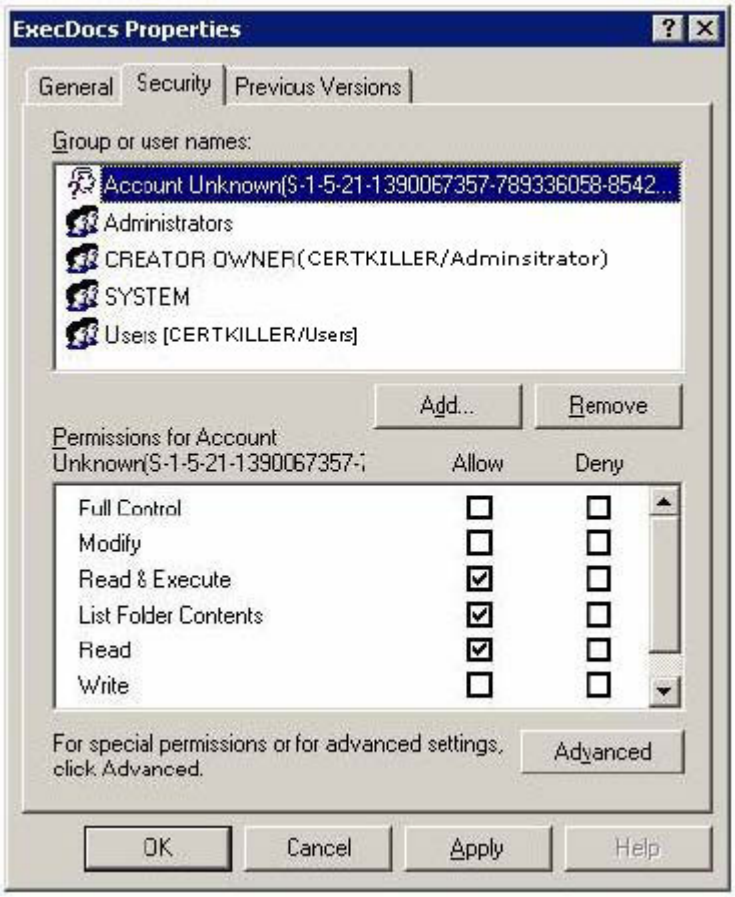
A. Remote Users, Standard Users, Domain Admins, Research Users.
B. Domain Admins, Research Users, Remote Users, Standard Users.
C. Standard Users, Research Users, Remote Users, Domain Admins.
D. Research Users, Standard Users, Remote Users, Domain Admins.

Answer: B

Explanation: The correct order for the remote policies should be:
1. Domain Admins
2. Research
3. Remote User
4. Standard User
When connecting through remote access to a network, the connection is checked against the first listed policy. If the policy applies (if a match is found) then it is used to determine the user's access. After that no further policies will be checked after that point. If the next policy does not apply, the following policy is checked to see if it applies, until each policy is checked.
Incorrect answers:
C: Any list that has the Standard User policy first will not work in these circumstances because all users qualify as Domain Users. Therefore any user connecting would be denied access.
A: Listing Remote User policy before the Research policy would not work because the Research group members are also part of the Telecommute group. Therefore, the Remote User policy would apply and the Research policy would never be checked. The Remote User policy does not allow multilink connections.
D: This will not work since the Standard Users policy is listed before remote Users and Domain Admins. This will result in any other user other than the Remote Users to be denied access.

QUESTION 102:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory forest that contains several domains. Each domain contains child domains. The functional level of the forest is set at Windows Server 2003.
You responsibility at Certkiller .com includes the management of access to resources on the Certkiller .com network. To this end you are busy with a routine check on access permissions on all shared folders. A file server named Certkiller -SR33 hosts a shared folder named ExecDocs that is being used by certain users and groups in the domain. You are currently busy reviewing access permissions for this shared folder on Certkiller -SR33. Then you notice that one entry in the list of security principals is displayed as a Security ID (SID) instead of a user name or even group name that it is supposed to represent. The following Exhibit illustrates the access permissions:
Exhibit:



What could be the cause of this type of display output? (Each correct answer presents a complete solution. Choose three.)

A. The deletion of an incoming trust with an external domain.
B. The deletion of an outgoing trust with an external domain.

C. A renamed user account.
D. A disabled user account.
E. A deleted user account.
F. The absence of domain controllers for the trusted domain due to a network failure.
G. The absence of domain controllers for the trusting domain due to a network failure.

Answer: B, E, F

Explanation: The direction of a trust is from a trusting domain toward a trusted domain, thus a trusting domain has an outgoing trust with a trusted domain. Any user accounts, global and universal groups in the trusted domain are visible and can be assigned permissions for resources in the trusting domain. But if an outgoing trust becomes unavailable due to network failure for instance, then the security principals from the trusted domain that are specified in Access Control Lists (ACLs) are represented by their SIDs and not the common names.
SIDs also appears in the ACL whenever a valid user account with the proper permissions for the resource has been deleted.
Incorrect answers:
A: A trust, per definition, is named from the trusting domain to the trusted domain rendering this option invalid, since it should rather read trusted domain.
C: A renamed user account's representation is automatically changed to the new user name.
D: A disabled user account's representation in the ACL does not change.
G: As per the definition, a trust is named from the trusting domain to the trusted domain, thus this is incorrect to talk about the trusting domain. Instead the option should read the trusted domain.

QUESTION 103:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory forest that contains several domains. Each domain contains child domains. The functional level of the forest is set at Windows Server 2003.
Your responsibility at Certkiller .com includes the creation of shared folders. To this end you are busy creating a shared folder on a file server named Certkiller -FS03. This shared folder is intended for use in one of the child domains in the forest. Certkiller .com has a partner company and in this company there is a group of employees who will also require access to this shared folder. This group of users all belong to an Active Directory child domain in another forest. You received instruction from the CIO to grant that group of employees in the partner company access to the shared folder. You now need to comply with the instruction, but you do not want these users to be able to access any other resources on the Certkiller .com forest.
What should you do?

A. Create an external trust with domain-wide authentication.

B. Create a forest trust with domain-wide authentication.
C. Create an external trust with selective authentication.
D. Create a forest trust with selective authentication.

Answer: C

Explanation: An external trust is a one-way or two-way non-transitive trust between a local domain and a domain in another forest, or between a local domain and a Windows NT domain. An external trust from the domain where Certkiller -FS03 resides to the partner company domain where users require access to a resource in your forest will allow those users to authenticate directly to your resource domain.
Selective authentication allows users from a trusted domain only to those resources to which they are explicitly allowed to authenticate
Incorrect answers:
A: Domain-wide authentication means that users from a trusted domain will have the same level of access to local resources that it provides users from the local forest. Though an external trust creation would be correct, the domain-wide authentication will cause problems.
B: A forest trust is a one-way or two-way transitive trust between two forests that operates on the same functional level. You cannot create a forest trust with domain-wide authentication in this case: it would expose the Certkiller .com resources to the partner company and it is also not mentioned that the functional level of the partner forest is set at Windows Server 2003. Domain-wide authentication means that users from a trusted domain will have the same level of access to local resources that it provides users from the local forest.
D
: A forest trust is a one-way or two-way transitive trust between two forests that operates on the same functional level. You cannot create a forest trust with selective authentication in this case: it is not mentioned that the functional level of the partner forest is set at Windows Server 2003.

QUESTION 104:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network also contains a perimeter network. The Certkiller .com intranet Web site is hosted on a Web server named Certkiller -SR17.
Certkiller -SR17 resides on the perimeter network. Other servers hosted on the perimeter network, also available to the public, are the company e-mail and FTP servers.
The Certkiller .com written security policy dictates that the Certkiller .com network is secured from attacks that originate from the Internet. You thus need to comply with the written security policy and to this end you need to secure the most vulnerable element of all servers hosted on the perimeter network. You must implement a

solution which will decrease the identified vulnerability. You do not want to move any public servers to the internal network.
What should you do?

A. Configure Kerberos authentication.
B. Install a firewall and configure packet filtering to filter traffic from the Internet.
C. Install a PKI and digital certificates on your public servers.
D. Configure NTFS permissions.

Answer: B

Explanation:
The biggest vulnerability you have is that there is no firewall between the Internet and your perimeter network. This basically means that an attack can be launched from the Internet to take control your server computers on the perimeter network. The attacker can then use one of your public servers to access the corporate network. You can mitigate this risk by implementing a firewall between your perimeter network and the Internet. You should configure packet filtering to filter all traffic passing from the Internet to the perimeter network.
Incorrect answers:
A: Kerberos authentication can only be applied in Active Directory environments.
C: You need to secure the network, and not specifically ensure that data can be encrypted through SSL.
D: NTFS permissions are configured to control access to file system resources. You should be more concerned with securing your network from attacks from Internet users.

QUESTION 105:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
An Enterprise Certification Authority is implemented on the Certkiller.com corporate network. This enterprise Certification Authority (CA is required to establish secure communications between the Certkiller .com corporate network and the networks of numerous business partners and important clients. Your plan is to employ secure virtual private network (VPN) connections over the internet. To this end you need to ensure that the VPNs use L2TP/IPSec and certificate-based authentication.
What should you do? (Choose all that apply)

A. Install a computer certificate from the enterprise CA on a VPN server.
B. Create a computer certificate template and publish it on the intranet Web site.
C. Configure a domain-level auto-enrollment policy.
D. Instruct users to use the computer certificate template to apply to a commercial CA for their computer certificates.

E. Create L2TP/IPSec connections to the other parties.
F. Implement a domain-level policy that requires encryption of traffic that is directed to external IP addresses.
G. Implement a domain-level policy that requires all secure channel data to be digitally encrypted or signed.
H. Configure a local policy that requires all secure channel data to be digitally encrypted or signed.
I. Configure a local policy that requires VPN traffic to be encrypted.

Answer: A, E, I

Explanation: This scenario requires you to enable secure connectivity with partners' and major clients' networks over the Internet. You should, therefore, configure router-to-router VPN connections on a Windows Server 2003 computer with Routing and Remote Access. A computer certificate is usually required on each L2TP/IPSec tunnel endpoint router to enable mutual authentication. Typically, you would use a certificate from a commercial CA rather than an enterprise or stand-alone CA because the certificates issued by many commercial CAs are globally trusted. This means that the Certkiller .com partners and clients may want to use their certificates for establishing communications with other parties as well.
Incorrect Answers:
B: Certificate templates are stored in Active Directory and are supported only by enterprise CAs.
C: Typically, Windows 2000 and later clients automatically enroll for computer certificates with enterprise CAs.
D: Client computers on Certkiller .com's network do not require computer certificates to communicate over router-to-router VPN connections because only VPN tunnel endpoint routers must authenticate each other.
F: The authentication of Certkiller .com's client computers and users on external networks may or may not require certificates.
G: The Domain member: Digital encrypt or sign secure channel data (always) pertains to communications between domain controllers and other member computers. This is not related to IPSec.
H: The Domain member: Digital encrypt or sign secure channel data (always) pertains to communications between domain controllers and other member computers. This is not related to IPSec.

QUESTION 106:

You work as the network engineer at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows 2000 Professional.
The Certkiller .com network contains two domain controllers named Certkiller -DC01 and Certkiller -DC02, and 4000 client computers. You are required to allow all users in the Certkiller .com domain to use smart card

authentication to log on to the network.
The Certkiller .com help desk was then inundated with reports from various users reporting that they are unable to logon to the network as a result of expired EAP certificates. You thus need to address this issue and ensure that all users are able to renew expired certificates for smart card authentication automatically, without any interference from the user.
What should you do?

A. Open the certificate template.
Click the Issuance Requirements tab.
Make the "This number of authorized signatures" value 1.
B. Make use of a smartcard logon certificate.
Select the "Enroll subject without requiring any user input" option.
C. Access the Personal folder of the Certificates snap-in.
Configure the appropriate option.
D. Access the Certification Authority snap-in.
Configure the appropriate option.

Answer: B

Explanation: To ensure that a smartcard logon certificate is renewed automatically without user intervention, you should first open the certificate template. You should use the Certificate Templates console to access the Properties dialog box of the template. Click the Request Handling tab, and then select the "Enroll subject without requiring any user input" check box. This will allow certificates to enroll to users without their awareness or interaction.
Incorrect Answers:
A: You cannot configure certificates to be enrolled and updated automatically without user intervention by using the Issuance Requirements tab. This tab is used to configure options for the issuance of certificates, such as the number of authorized signatures required to issue a certificate.
C: This option will not allow you to configure the option to automatically renew expired certificates without user interaction.
D: This option does not make provision to allow you to configure the option to automatically renew expired certificates without user interaction.

QUESTION 107:

You work as the network engineer at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and the client computers run either Windows 2000 Professional, Windows XP Professional, or Windows NT Workstation 4.0 Service Pack 6.
Certkiller .com has issued a new written security policy that states that:
1. All network transmissions that run over secure RPC must use 128-bit key encryption.

2. All network transmissions must occur through a secure channel.
3. NTLM pass through authentication must be performed through the secure channel.
4. All logon information must be encrypted during transmission.
You thus need to comply with the security policy and you also received instruction to upgrade all Windows NT Workstation 4.0 with Service Pack 6 and Windows 2000 Professional computers to Windows XP Professional. You thus need to enable some security settings on the network computers.
What should you do?

A. Enable the Domain member: Digitally encrypt secure channel data (when possible) security setting.
B. Enable the Domain member: Digitally sign secure channel data (when possible) security setting.
C. Enable the Domain member: Digitally encrypt or sign secure channel data (always) security setting.
D. Enable the Domain member: Require strong (Windows 200 or later) session key security setting.

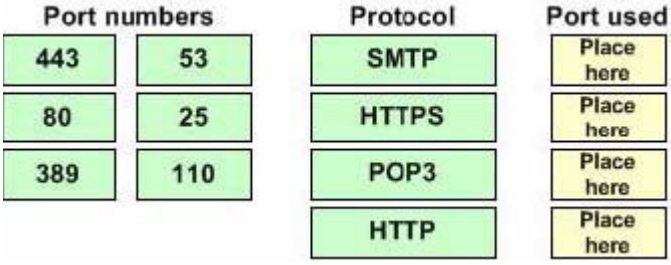
Answer: C

Explanation: When the Domain member: Digitally encrypt or sign secure channel data (always) security setting is enabled, then a secure channel is used to transmit information in encrypted or signed format.
Incorrect answers:
A: The Domain member: Digitally encrypt secure channel data (when possible) security setting permits domain controllers to support encryption on secure channels if encryption is supported by the client. And then only logon information will be encrypted if the secure channel is not supported. Thus, this is not the solution for the security policy asks for all transmissions to be encrypted using 128-bit encryption at all times.
B: The Domain member: Digitally sign secure channel data (when possible) security setting will cause clients to attempt to require the signing of all transmissions through the secure channel. If this channel is not supported, then only logon information will be encrypted when transmitted over the secure channel. This is not acceptable in terms if the new security policy.
D: The Domain member: Require strong (Windows 200 or later) session key security setting would require the use of 128-bit encryption keys to be used for all transmissions through the secure channel. However, then the logon information is not encrypted during transmission. This is unacceptable.

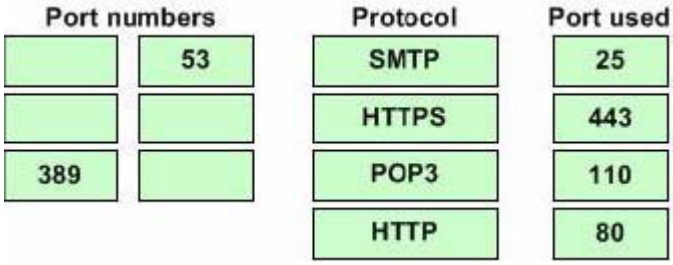
QUESTION 108:

DRAG DROP
You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client

computers run Windows XP Professional.
On the Certkiller .com network there is also a Web server named Certkiller -WS01 and e-mail server named Certkiller -ES01. Both Certkiller -WS01 and Certkiller -ES01 are protected by a firewall from the Internet.
A new Certkiller .com directive states that the website is to be made available to internet users. To this end you have received instruction to:
1. The firewall must be configured to allow internet users access to the web site using HTTP, HTTPS
2. Provision must be made for Internet users to send feedback e-mail to Certkiller .com using SMTP and POP3.
You thus need to implement some changes and have to decide which firewall port configurations you will use to comply with the instructions.
What should you do? To answer, drag the appropriate port number to the appropriate location.



Answer:



Explanation:
The port numbers are used to identify which protocol will be used to send and receive communication over the network by using port 25 and port 110 you ensure that the Internet users can send their feedback e-mail to Certkiller .com. By configuring port 80 and port 443 you ensure that the Internet users can access the web site generally or securely.
Incorrect Answers:
There is no need to configure these ports as the scenario states that only HTTP, HTTPS, SMTP and POP3 traffic be allowed through the firewall. The port 53 is used by DNS and port 389 is used by LDAP.

QUESTION 109:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client

computers run Windows XP Professional.
Your duties include the administration of a Web server named Certkiller -SR01. Certkiller -SR01 is located on the Certkiller .com internal network and serves to provide the company users with corporate information. All access to the company web site is configured in such a way that a certificate from a trusted certification authority (CA) is required by users who need to connect to the web site.
Due to the nature of the Certkiller .com business they are involved in many joint ventures with other companies. In one of these joint ventures, the other company named, AudioExams, also requires access to a web page that is hosted on Certkiller -SR01. To this end you received instruction to provide AudioExams with the required access.
1. AudioExams operates with an autonomous Windows 2000 network.
2. A Public Key Infrastructure (PKI) has been deployed on the AudioExams network.
3. The AudioExams root certificate is hosted in a Windows 2000 Server CA.
4. All AudioExams employees with user accounts in the AudioExams domain have been issued certificates by the AudioExams CA.
You then continue to configure the appropriate CA trust between Certkiller .com and AudioExams. You need to allow AudioExams users access to the web page on Certkiller -SR01. All users require the same level of access to this web page. You are also reminded by the CIO to keep in mind that the same level of access might need to be extended to other companies in future joint ventures.
What should you do?

A. Create a separate local user account for each AudioExams user.
Map each AudioExams user's certificate to the user's corresponding Certkiller -SR01 user account.
Create a group named AudioExams_Access on Certkiller -SR01.
Add each of the AudioExams_User local user accounts to AudioExams_Access.
Define access permissions for AudioExams_Access group to allow access to the required web page.
B. Create a single local user account on Certkiller -SR01 named AudioExams_User.
Define a rule that maps all AudioExams-issued certificates to the AudioExams_User account.
Create a group named AudioExams_Access on Certkiller -SR01.
Add the AudioExams_User account to AudioExams_Access
Define access permissions for AudioExams_Access group to allow access to the required web page.
C. Create a separate local user account for each AudioExams user.
Create a group named AudioExams_Access on Certkiller -SR01.
Add each of the AudioExams_User local user accounts to AudioExams_Access.
Define access permissions for AudioExams_Access group to allow access to the required web page.
D. Create a single local user account on Certkiller -SR01 named AudioExams_User.
Manually map the certificate to the user to the AudioExams_User user account.
Create a group named AudioExams_Access on Certkiller -SR01.

Add each of the AudioExams_User local user accounts to AudioExams_Access.
Define access permissions for AudioExams_Access group to allow access to the required web page.

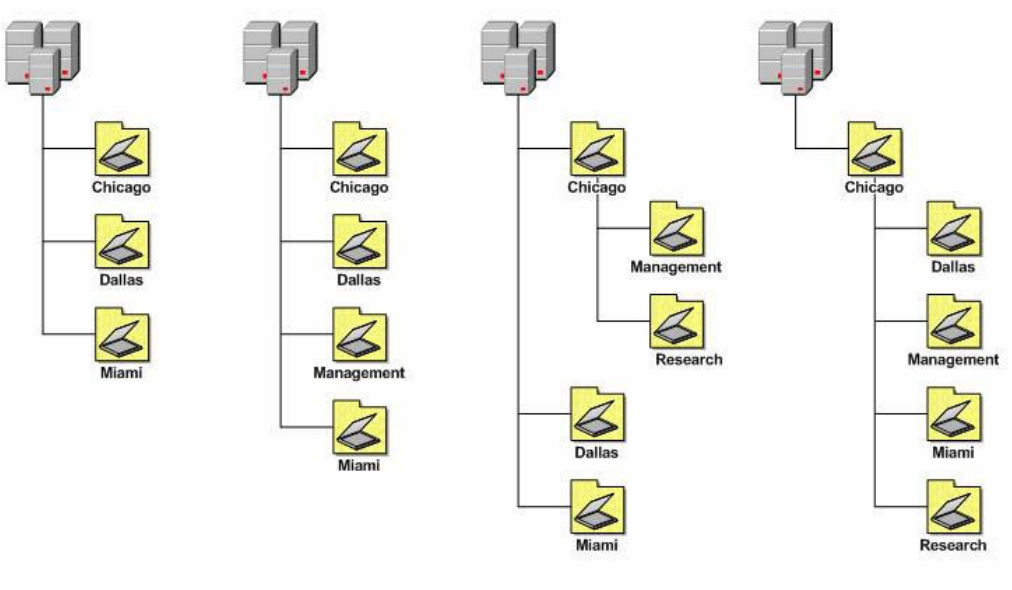
Answer: B

Explanation: Several of the AudioExams user accounts require access to the Certkiller -SR01 web page. Each user has been issued a certificate from a mutually trusted CA. Though the number of users has not been defined, it is the usual practice to use many-to-one mapping to provide an external group of users, with certificates, the same level of access to Web-based resources. In this scenario all client certificates that list AudioExams as the issuing CA would be mapped to the AudioExams_User user account. Using security groups to define access permissions for many-to-one mapped users does meet with Microsoft recommended practice. Furthermore, this step will allow for the provision of a consistent method for granting future access to other joint venture requirements.
Incorrect Answers:
A: The creation of separate user accounts and manually associating a certificate to each account will result in unnecessary administrative effort. However, further in the procedure to be followed as suggested in this option is correct.
C: All access to the Certkiller -SR01 website requires that the connecting user make use of a certificate from a trusted CA, thus you solution must include certificate mapping. This option is thus defective and will not work.
D: You cannot map a single certificate to multiple user accounts. In essence this options suggests that although a single local user account is created, access permissions has to be granted to each of the local user accounts that reside in the AudioExams_Access group.

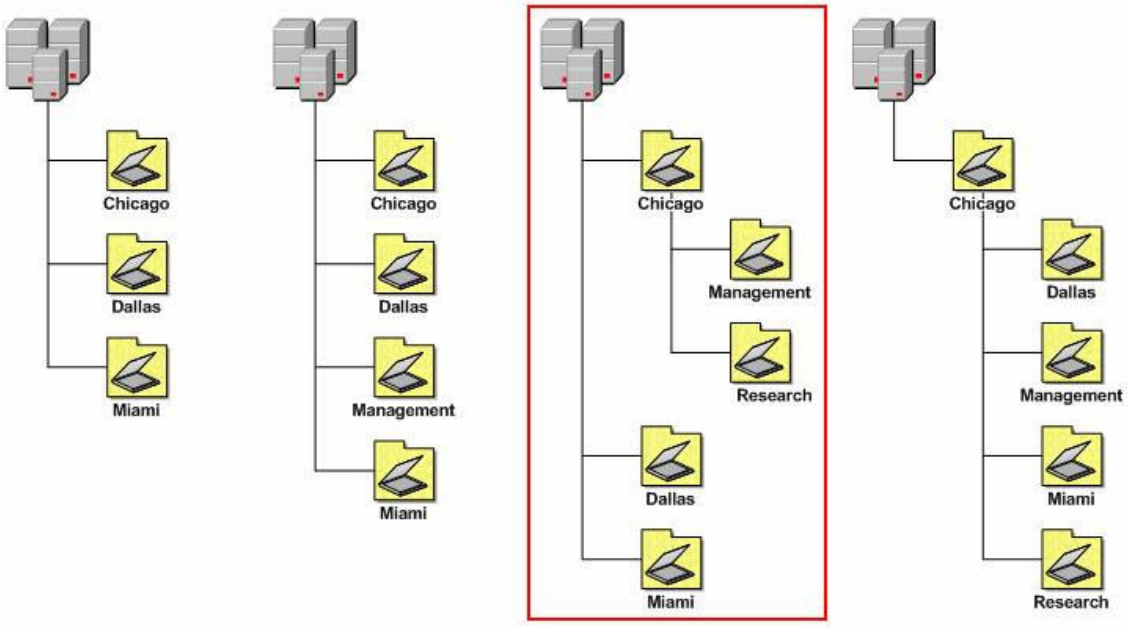
QUESTION 110:

HOTSPOT
You work as the network architect at Certkiller .com. Your job description involves designing the Certkiller .com logical network design. All servers on the Certkiller .com network will run Windows Server 2003 after they have been upgraded from Windows NT 4.0. Certkiller .com has its headquarters in Chicago and branch offices in Dallas and Miami.
Each of the Certkiller .com offices has a Finance department, Sales department and a Marketing department. Only the head quarters in Chicago has two additional departments named the Research and Development department and the Management department respectively. The Certkiller .com IT department will take care of domain administration, and onsite administrators will be deployed. The onsite administrators will be responsible for the administration of user accounts in each of the Certkiller .com branch offices where they will be deployed respectively. An administrator at the Chicago office will be assigned to manage the Research and Development department users, and another administrator to manage the Management department users.
You need to create the organization unit (OU) design to support the company's

administrative structure while being mindful that:
1. The design must allow for permissions maintenance with the least amount of administrative effort.
2. Administrators should only be delegated control to objects for which they are responsible.
3. To this end you need to decide on which OU structure would best suit the Certkiller .com administrative goals.
What should you do? (To answer choose the appropriate OU structure.)



Answer:



Explanation:
The scenario needs the OU design to accommodate the IT administrative model of the

company. There is a strong centralized tendency in the IT department being responsible for domains. But there is also the geographic aspect that has to be kept in mind. Thus it is a hybrid administrative model which calls for an OU structure that is geographically based at the higher level OU and then making use of unit-based lower level OUs. With this type of approach you can have granular delegation of administration.
Thus you should have three top level OUs based of geographic location, then create two child OUs that is subordinate to the Chicago OU. This way all the different requirements and responsibilities of the IT department are accommodated. Furthermore the containers will be tailored to both geographic and departmental requirements which making administrative permissions that have to be applied and modified possible with the least amount of administrative effort.
Incorrect answers:
A: You should not choose a geographic based OU structure. This would not make provision for the ability to maintain the permissions and administrative assignments for the Research and Development department and the Management department in an efficient way.
B: This design where the OU structure includes top-level OUs for Chicago, Dallas, Miami and Management would not provide the ability to maintain the permissions and administrative assignments for the Research and Development department and the Management department.
D: Chicago OU should not be the only top-level OU with Dallas, Miami, Research and Development, and Management the child OUs. This structure will allow for the delegation of administrative duties, but is not compatible with the Microsoft recommendations for hybrid administrative models.

QUESTION 111:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003. The functional level of the domain is set at Windows Server 2003.
The Certkiller .com organizational unit (OU) structure corresponds with the departments and consists of three top-level OUs named Personnel, Finance and Sales respectively. Each of these OUs stores the user and computer objects that are associated with their department.
The Personnel department maintains their employee records by making use of a Custom application. Consequently all employee records are stored in a non-LDAP directory service. To this end you created an InetOrgPerson object for each user to allow them to use the application. These objects are stored in the Finance OU. Synchronization between the InetOrgPerson attributes and Active Directory and the third-party directory service is dandled by Microsoft Identity Integration Server (MIIS).
An assistant administrator named Amy Wilson is responsible for the administration of InetOrgPerson class objects for the Finance department. You received instruction to ensure that Amy Wilson will be able to carry out her tasks. You now need to configure Active Directory to allow Amy Wilson to administer the

InetOrgPerson class objects without allowing her to ability to administer the Windows-based user or computer accounts.
What should you do? (Each correct answer presents a complete solution. Choose two.)

A. You should delegate control of user objects for the domain to Amy Wilson. Block inheritance of these permissions to the Personnel and Sales OUs.
B. You should delegate control of the InetOrgPerson objects for the domain to Amy Wilson. Block inheritance of these permissions to the Personnel and Sales OUs.
C. You should delegate control of InetOrgPerson objects for the domain to Amy Wilson. Block inheritance of these permissions on the Finance OU.
D. You should delegate control of InetOrgPerson objects for the domain to Amy Wilson.
E. You should delegate control of InetOrgPerson objects for the Finance department to Amy Wilson.

Answer: B, E

Explanation: The Windows Server 2003 domain functional level makes it possible to have the InetOrgPerson object. This object class is available for providing access to third party applications that do not have a LDAP-based directory service.
Custom tasks can be defined. These tasks can be managing contact objects or site link objects. In this scenario Amy Wilson requires the ability to manage InetOrgPerson objects. This can be done by defining the task to delegate and determine the level where the delegation should be configured. It is advisable to define these delegations at the lowest possible container, in this case the OU. Administrative authority for an OU and the objects that it contains can be delegated to an individual administrator or security group. You would thus delegate authority for the task at the Finance OU. Alternatively you could define this authority at the domain level and block the permission from being inherited on any container where the objects do not exist. In this case the Personnel and Sales OUs.
Incorrect answers:
A: Delegating control of user objects for the domain to Amy Wilson and blocking inheritance of these permissions to the Personnel and Sales OUs will result in her having abilities like manage user objects in the Finance OU which is beyond her scope of duty.
C: Delegating control of InetOrgPerson objects for the domain to Amy Wilson and blocking inheritance of these permissions on the Finance OU will prevent Amy Wilson from administering the InetOrgPerson objects in the Finance OU.
D: Delegating control of InetOrgPerson objects for the domain to Amy Wilson will result in her having the ability to manage all InetOrgPerson objects in the domain and not only those used to access the Finance Custom application.

QUESTION 112:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory forest that contains two domains

named us. Certkiller .com and uk. Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003. Half the client computers run Windows 2000 Professional, and the rest run Windows XP Professional.
Certkiller .com has its headquarters in Chicago and a branch office in Dallas and Miami. In the Dallas branch office resides the us. Certkiller .com, and in the Miami branch office resides the uk. Certkiller .com. The branch offices are connected through slow and unreliable links. The WAN are connected through leased lines. Each of the branch office contains file servers and two domain controllers, named Certkiller -DC01 in Dallas and Certkiller -DC02 in Miami. This means that each branch office is a domain on there own. The file servers act as member servers. Each of these branch offices also contains a global catalog server.
Certkiller .com consists of a Research department which resides in the Miami branch office. The Research department's employees need to access the files servers in thee other branch office and the main office. Most of the employees of the Research department are temporary employees. You have to have control over these users, so you need place them in a security group. You need to create a security group scope to grant these users in the Research department access to resources on the files servers. To this end you need to make a choice regarding the group scope that you will make use of.
What should you do?

A. Use global groups.
B. Use local groups.
C. Use domain local groups.
D. Use universal groups.

Answer: A

Explanation: If you want access to recourses in any domain in the Active Directory forest, you should create global groups. The resources that are needed are in the two branch offices, so you can grant the Research department the permissions to the resources in both of these branch offices.
Incorrect Answers:
B: A local group only will grant resources on a local computer. It is best to create a global group. If you want to create a local group, then you have to create local groups on each files server and each of the Research employees would need a universal or a global group.
C: You do not need domain local groups because the domain local group grants access to resources only in the same domain. The scenario states that there are two domains.
D: Universal groups are not needed here. Membership of the universal groups is replicated to every global catalog server in the forest. This will cause regular changes across the WAN.

QUESTION 113:

You work as the network administrator at Certkiller .com. The Certkiller .com

network consists of a single Active Directory forest that contains two domains named us. Certkiller .com and uk. Certkiller .com. The functional level of the forest is set at Microsoft Windows Server 2003. All servers on the Certkiller .com network run Windows Server 2003. Half the client computers run Windows 2000 Professional, and the rest run Windows XP Professional. The Certkiller .com network contains a few domain controllers.
Certkiller .com has its headquarters in Paris and a branch office in Berlin and Milan. In the Berlin branch office resides the us. Certkiller .com, and in the Milan branch office resides the uk. Certkiller .com. The links connecting the branch offices are slow and unreliable. The WAN are connected through leased lines. Both branches contain a global catalog server. The branch office also consists of its own administrator. Each branch office consists of a Marketing department. Both of these branches also contain a dedicated file server, which consists of resources required by the two branch offices.
Most of the employees are either temporary or contract staff. Each branch office consists of almost 150 employees. You need to configure security group strategies that will coincide with the Certkiller .com Marketing department needs and can be maintained with the least amount of effort.
What should you do? (Select all that apply)

A. Add the marketing employees to the Berlin Marketing and the Milam Marketing group.
Then add these groups as members of the Certkiller .com Marketing group.
B. Create two global groups named Berlin Marketing and Milan Marketing.
Then create a universal group named Certkiller .com Marketing.
C. Create two domain local groups named Berlin Marketing and Milan Marketing.
D. Add the marketing employees to the Certkiller .com Marketing group.
Then create a global group named Certkiller .com Marketing group.

Answer: A, B

Explanation: You must create a global group for the Berlin and Milan offices. The members in the global group are not replicated to every global catalog server. Most of the employees are temporary or contract workers, so it is best to have a global group. You then should create a universal group and add the global groups to the universal group. Universal groups is used anywhere in the forest.
Incorrect Answers:
C: The domain local group is used to grant permission to resources on domain controllers and member servers.
D: Global groups should be named appropriately, not Certkiller .com Marketing. You could have named it Berlin Marketing or Milam Marketing. You cannot add the marketing members to a global group named Certkiller .com Marketing. Global groups only contain members of the same domain.

QUESTION 114:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003. Half the client computers run Windows 2000 Professional, and the rest run Windows XP Professional.
Certkiller .com consists of three departments named Research, Development and Finance. The Research and the Development departments are responsible for the research and development of new in-house custom applications for Certkiller .com. The development department hosts a troubleshooting application. This application is used to troubleshoot any problems that the Certkiller .com client computers may experience. The troubleshooting application works by starting the installation of the troubleshooting application by a hyperlink that is posted in a public folder named Troubleshoot.
You have received an update for the troubleshooting application. The update is then only installed on the client computer where the application is already installed. You need to install the update by using a Group Policy object (GPO). You want to deploy the update on all the client computers where the troubleshooting application is installed.
What should you do?

A. Specify the update to users and place the user accounts of the development users into an OU.
Link the GPO to the OU.
B. Specify the update to users and link the GPO to the domain.
Add the user accounts of the development users to a security group.
Then filter the scope of the GPO by assigning permissions for the group only.
C. Specify the update to the client computers and link the GPO to the domain.
Then filter the scope of the GPO by using a WMI filter.
D. Use GPUpdate on the client computers.

Answer: C

Explanation: You need to filter the scope by using the WMI filter. You can define a filter that will cause the GPO to specify only the target computers.
Incorrect answers:
A: This action will allow the updates to be deployed only the client computers where the developments user are logged on to.
B:
You should link the GPO to the domain, but you should then use the WMI filter, not a security group.
D: This utility has nothing to do with assigning updates to users. This utility is used to refresh the computer and user settings that are applies to the Group Policies and Local policies that are applied to the user and the client computer.

QUESTION 115:

You work as the network administrator at Certkiller .com. Certkiller .com has its headquarters in London. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com that operates on Windows 2000 Native mode. All domain controllers on the Certkiller .com network run Microsoft Windows 2000 Server and all client computers run Windows XP Professional.
Certkiller .com consists of three departments, named Sales, Accounts and Marketing. Certkiller .com expands into continental Europe and opens branch offices in Paris, Milan, and Athens. Each branch office in the Certkiller .com domain has a domain controller and is a child domain of the Certkiller .com domain. The child domains are configured with default settings. The Marketing department at each office requires access to share resources throughout the forest.
It is your responsibility to provide the Marketing departments of each office access to shared resources in the forest. To this end you create a global group named CKMarketing in each office and add the Marketing department user accounts to the CKMarketing group. You want to assign permissions to the Marketing users to allow them access to all resources by using the minimum numbers of groups.
What should you do?

A. Upgrade the Windows 2000 Servers to Windows Server 2003, and create a universal group.
Add all of the CKMarketing groups to the new universal group.
Then assign permissions for all appropriate resources throughout the forest to the new universal group.
B. Create a universal group.
Add all of the CKMarketing groups to the new universal group.
Assign permissions for all appropriate resources throughout the forest to the new universal group.
C. To each CKMarketing group, assign permissions for all appropriate resources throughout the forest.
D. Upgrade one domain controller to Windows Server 2003.
Then raise the domain level to Windows Server 2003.
Create a universal group.
Then assign permissions for all appropriate resources throughout the forest to the new universal group.

Answer: C

Explanation: A global group only includes the members of the same domain where the group belongs. Therefore you need to assign permissions to each CKMarketing group.
Incorrect answers:
A: The forest root domain is Windows 200 native. When you prepared the forest for the deployment of Windows Server 2003, the functionality of the forest was set at Windows 2000. The domains at that function level do not support universal security groups.
B: The forest root domain is Windows 200 native. When you prepared the forest for the deployment of Windows Server 2003, the functionality of the forest was set at Windows

2000. The domains at that function level do not support universal security groups.
D: The forest root domain is Windows 200 native. When you prepared the forest for the deployment of Windows Server 2003, the functionality of the forest was set at Windows 2000. The domains at that function level do not support universal security groups.

QUESTION 116:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
You have recently deployed new Windows Server 2003 computers. A new network administrator named Clive Wilson is appointed to administer resources in the Certkiller .com domain. Clive Wilson uses a workstation named Certkiller -WS351.
A member server named Certkiller -SR04 is a file server and is configured to allow Remote Desktop connections. Certkiller -SR04 will be managed by Clive Wilson. You assign the Allow log on locally user right to Clive Wilson.
Clive Wilson needs to manage Certkiller -SR04 by using Remote Desktop connections. Clive Wilson complains that he is unable to log on to Certkiller -SR05 using a Remote Desktop connection. You received instruction to ensure that Clive Wilson can connect to Certkiller -SR04 by using a Remote Desktop connection. To this end you assign the Allow log on through Terminal Services user right to Clive Wilson.
What else should you do? (Each correct answer presents a complete solution. Choose two.)

A. Include Clive Wilson's user account in the Server Operators group on Certkiller -SR04.
B. Include Clive Wilson's user account in the Accounts Operators group.
C. Include Clive Wilson's user account in the Remote Desktop Users local group on Certkiller -SR04.
D. Include Clive Wilson's user account in the Remote Desktop Users domain local group on Certkiller -SR04
E. Include Clive Wilson's user account in the local Administrators group on Certkiller -SR04.

Answer: C, E

Explanation: Clive Wilson should have the Allow log on through Terminal Services user right and not the Allow log on locally user right to use a Remote Desktop connection to access Certkiller -SR04. This part of the solution is correct.
However, you have to include Clive Wilson's user account in one of two local groups on Certkiller -SR04, i.e. the Remote Desktop Users local group or the local Administrators group. The Remote Desktop Users group has the permissions needed to connect to servers remotely by using Terminal Services. Clive Wilson should therefore be included in the Remote Desktop Users group if he wants to log

on to Certkiller -SR04 remotely. Alternatively, you can add Clive Wilson to the local Administrators group on Certkiller -SR04.
Incorrect Answers
A: The Server Operators group is not defined on member servers, such as Certkiller -SR04. It is defined on domain controllers.
B: Members of the Account Operators group have the Allow logon locally and Shut down the system user rights. Assigning this permission to Clive Wilson will NOT result in him having the ability to create Remote Desktop connections to Certkiller -SR04.
D: Certkiller -SR04 is a member server. The Remote Desktop Users group on the server is a local group and not a domain group. Including Clive Wilson in the Desktop Users local group on Certkiller -SR04 would allow him to establish a Remote Desktop connection to the local file server (Certkiller -SR04).

QUESTION 117:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
Certkiller .com opens a new staff business college. The staff business college is located in the Certkiller .com corporate headquarters building. You deploy a new application server named Certkiller -SR23 on the Certkiller .com network. You install a new custom application named Ck_PhTester1 on Certkiller -SR23. All course material is accessible through Ck_PhTester1. You deploy 50 new Windows XP Professional client computers at the staff business college. You connect each new client computer to the local area network (LAN). None of the 50 new client computers in the staff business college are domain members.
Currently, no public key infrastructure (PKI) is deployed in the Certkiller .com domain. You must ensure that only authorized domain users can access Ck_PhTester1. You do not want to incur any unnecessary overhead.
What should you do? (Each correct answer presents a complete solution. Choose TWO.)

A. Create a new IPSec policy.
Configure the IPSec policy so that Encapsulating Security Payload (ESP) using Kerberos authentication is applied for all traffic to Certkiller -SR23.
B. Create a new IPSec policy.
Configure the IPSec policy so that Authentication Header (AH) using Kerberos authentication is applied for all traffic to Certkiller -SR23.
C. Create a new IPSec policy.
Configure the IPSec policy so that Authentication Header (AH) using certificate-based authentication is applied for all traffic to Certkiller -SR23.
D. Configure a new GPO to enable the Digitally sign client communication (always) security policy setting.
Link the new GPO to the Certkiller .com domain.

Answer: B, D

Explanation: In Windows Server 2003, IPSec uses the Authentication Header (AH) protocol and Encapsulating Security Payload (ESP) protocol to provide data security. In your case, you only need to use AH. AH provides data authentication and integrity, and can therefore be used on its own when data integrity and authentication are relevant factors and confidentiality is not. With AH, a digital signature is used to verify the identity of the sender of the information. IPSec can use Kerberos, a preshared key, or digital certificates for authentication. Because you do not have a PKI and you do not want to incur unnecessary expenses, you should configure the IPSec policy so that Kerberos authentication is used. Alternatively, you can enable the Digitally sign client communication (always) security policy setting in a GPO that is linked to the domain. This will force all clients to sign all client communications to Certkiller -SR23. The GPO has to be linked to the Certkiller .com domain so that this is enforced for all clients.
Incorrect Answers:
A: Authentication Header (AH) and Encapsulating Security Payload (ESP) can be used separately, or together. ESP ensures data confidentiality through encryption, data integrity, data authentication, and other features that support optional anti-replay services. To ensure data confidentiality, a number of symmetric encryption algorithms are used. You do not need to encrypt data being sent to and from Certkiller -SR23. Encryption results in additional overhead on each packet.
C: You cannot use certificate based authentication because this method of authentication is dependent on a PKI implementation. You would have to first deploy a PKI, which would result in additional expenses.

QUESTION 118:

You work as the network administrator at Certkiller .com. The Certkiller .com network is a single Active Directory named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and the client computers run Windows XP Professional.
Certkiller .com recently entered into a joint venture with TestLab.com. Consequently you need to establish a business-to business (B2B) connection between the two companies. The major requirements for this connection are:
1. All data transmitted between the two companies must be encrypted.
2. Access to data must be audited to provide nonrepudiation.
3. Two application servers must be used to communicate between the two companies.
4. These application servers must make use of A Virtual Private Network (VPN) connection.
5. IP Security (IPSec) must be used to encrypt the data.
The two application servers are currently configured to require security with the following settings:
1. They should use IPSec with DES encryption.
2. They should use certificates for authentication purposes.

3. They should use Diffie-Hellman group 2048 for key exchange.
You received instruction to increase security. What should you do? (Choose all that apply.)

A. Use Kerberos authentication.
B. Use Diffie-Hellman group 1 for key exchange.
C. Do NOT send Certificate Authority name in the payload.
D. Use 3DES for encryption purposes.
E. Use a pre-shared key for authentication purposes.

Answer: C, D

Explanation: Triple DES (3DES) makes use of 128-bit key encryption and hashes that data thrice. This makes it more secure that DES encryption. DES only hashes data once. Furthermore you can prevent the Certificate Authority (CA) name from being sent as part of the payload. This should keep the data about the company private from interlopers because when a CA name is sent, it is sent prior to negotiating security, thus it is sent in clear text.
Incorrect answers:
A: Kerberos authentication will not be appropriate because the outside company is not part of the domain. Furthermore, Kerberos authentication across the Internet will result in the computer name and domain name being sent over the Internet during the negotiation.
B: The Diffie-Hellman group 1 is less secure than Diffie-Hellman group 2048.
E: Pre-shared keys are not secure since they are stored in clear text on the computer.

QUESTION 119:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. All computers are joined to the domain. The new Certkiller .com written security policy requires you to deploy a public key infrastructure (PKI). You need to ensure that users who log on to the domain receive a certificate which they can use for authentication and secure e-mail. You deploy an enterprise certification authority (CA) on a new Windows Server 2003 server computer named Certkiller -06. You then join Certkiller -06 to the Certkiller .com domain. You configure a new certificate template named UserCerts. You instruct all users to request certificates based on this template from your enterprise CA.
However, you discover that the UserCerts certificate template contains a critical error. Consequently correct the error and now need all users that have been issued with a certificate based on the UserCerts certificate template template to enroll for a new certificate immediately.
What should you do?

A. Assign the Domain Users group the Allow - Autoenroll permission for the

UserCerts certificate template.
B. Select the Duplicate template command in the UserCerts certificate template
C. Assign the Domain Users group the Allow - Issue and Manage Certificates permission for the enterprise CA.
D. Publish the certificate in Active Directory.
E. Select the Reenroll All Certificate Holders command in the UserCerts certificate template.

Answer: E

Explanation: You need all users that have been issued with a certificate based on the UserCerts certificate template to enroll for a new certificate immediately. To do this, right-click the UserCerts certificate template, and select Reenroll All Certificate Holders from the shortcut menu. When critical changes have been made to a certificate template, and you want it to apply to all users immediately, you need to use the Reenroll All Certificate Holders option of the template.
Incorrect answers:
A: Your domain users have already requested the certificate from your enterprise CA, which means they already have the permission to use the certificate template associated with the certificate
B: You would use the Duplicate template command in the UserCerts certificate template to duplicate the certificate template, and then change and rename it. The question states that you have already corrected the error in the UserCerts certificate template.
C: This permission should never be assigned to ordinary domain users. Domain users should not be assigned with certificate management permissions.
D: Publishing the certificate in Active Directory will publish the certificate based on the certificate template in Active Directory. It will also map the certificate to the user accounts of your domain users.

QUESTION 120:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. Certkiller .com has its headquarters in Chicago and branch offices in Dallas and Miami.
The Certkiller .com network contains 4 domain controllers, 2 member servers, 75 client computers of which 5 are laptop computers as well as an enterprise certification authority (CA) server. The laptop computers all contain wireless network Interface Cards. The Certkiller .com Marketing department has been assigned the laptop computers to use when they need to go out of the office to prospective clients.
A new Certkiller .com security policy requires that all wireless laptop computers be configured to make use of the 802.1x certificate based authentication and Protected Extensible Authentication Protocol (PEAP). To this end the CIO gave you

instruction to configure all the laptop computers in compliance with the new security policy as soon as possible with the least amount of administrative effort. What should you do? (Each correct answer presents part of the solution. Choose three.)

A. Create a global group named wireless with the laptop user's user accounts added and then configure the usage of certificate autoenrollment
B. Configure the members of laptop_comp to use certificate autoenrollment.
C. Create a certificate template for IEEE 802.1x authentication usage.
D. Configure the appropriate wireless security for the Default Domain Policy GPO
E. Create a global group named laptop_comp with the wireless user's computer accounts added.

Answer: B, C, E

Explanation: The best option would be for you to create the global group laptop_comp with the wireless user's computer accounts added, remember when using PEAP; certificates are required for both servers and connecting clients. By making use of the autoenrollment feature you ensure the certificates are retrieved, issued and assigned automatically and therefore involves less administrative effort.
Incorrect Answers:
A: This option is not required as only computer accounts must be configured as the scenario states.
D: The only time configurations are made here are when you will be making configuration changes which apply to the entire domain.

QUESTION 121:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network contains a Windows Server 2003 computer named Certkiller -SR14. Certkiller -SR14 is configured as a certification authority (CA) and is used to issue certificates to Certkiller .com computers and users. Several users complain that they experience a delay when they need to execute actions such as authentication and data encryption. These actions requires the usage of a certificate. All issued certificates are valid for a three year period.
You investigate the complaints and find that most delays are experienced at the time when certificates are checked to the certificate revocation lists (CRLs). You need to ensure that users do not experience a substantial delay when the validity periods of the certificates are being checked.
What should you do?

A. Decrease the current validity period for all certificates.
B. Enable the certification authority to publish delta CRLs.

C. Increase the current validity period for all certificates.
D. Configure a subordinate CA and inform all new users to enroll for certificates using this CA.

Answer: B

Explanation: When you specify a long validity period for a CA, the CRL can grow quite large. You can use delta CRLs if your servers are running Windows Server 2003 Enterprise Edition, or Windows Server 2003 Datacenter Edition to minimize the update time needed to publish revoked certificates. When delta CRLs are used, clients are first sent the base CRL. After this, clients are only sent periodic updates, called deltas, which should be added to their base CRLs.
Incorrect answers:
A: If you decrease the current validity period, then new CRLs would need to be downloaded more frequently
C:
If you specify a long validity period for a CA, the CRL can grow quite large. This will therefore not resolve your issue.
D: Subordinate CAs acquire their authority by requesting a certificate from the root CA or from a higher-level subordinate CA. Issued certificates will still need be checked to the CRLs as they currently are.

QUESTION 122:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. All users and computers belong to the Certkiller .com domain.
Certkiller .com has headquarters in London and Sales offices in Paris and Berlin. The London office contains an offline root Certification Authority (CA) deployed on a server named Certkiller -SR45. All Certkiller .com offices have a subordinate CA that is used to issue user and computer certificates.
Certkiller .com sells the Berlin Sales office to a competitor company. On the root CA at the London office, you revoke the certificate of the subordinate CA residing at the Berlin Sales office. You must ensure that all Certkiller .com users and computers no longer accept certificates issued from the subordinate CA located in the Berlin Sales office. You want to use the minimum amount of administrative effort to accomplish this task.
What should you do?

A. Revoke all certificates issued by the subordinate CA in the Berlin Sales office.
B. Disconnect the subordinate CA in the Berlin Sales office from the Certkiller .com network.
C. Publish a new Certificate Revocation List (CRL).
Add the CRL to the Certificate Distribution Point on the Certkiller .com network.

D. Remove all CA files from the subordinate CA in the Berlin Sales office.

Answer: C

Explanation: To make certificates issued from any issuing subordinate CA invalid, you need to inform all users and computers that already trust the certificates from the issuing CA, that these certificates are not valid any longer. This is done by publishing a new
Certificate Revocation List (CRL) and making the CRL file available to all users and computers. The CRL is a list of certificates that are expired or invalid. To inform all CA clients about a change in a PKI, you need to add the change to your Certificate Distribution Point. You would be prevented from having to manually revoke each certificate issued by the CA.
Incorrect answers:
A: Revoking all certificates individually, which were issued by the subordinate CA in the Berlin Sales office would be a labor intensive process.
B: There is no need to perform either of the steps in these options because it has no bearing on users and computers that currently trust certificates from the issuing CA.
D: There is no need to perform either of the steps in these options because it has no bearing on users and computers that currently trust certificates from the issuing CA.

QUESTION 123:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network contains two Windows Server 2003 computers running Certificate Services. Certkiller -SR22 is configured as an offline root certification authority (CA), and Certkiller -SR23 is configured as an enterprise subordinate CA. Certkiller -SR23 is used to issue certificates to computers and users.
You receive instructions to implement a disaster recovery solution that will enable you to recover the Certificate Services database used by a CA on the network. To this end you need to ensure that you will be able to fully recover the Certificate Services database of any CA that fails.
What should you do?

A. Configure all certificates to allow key archival.
B. Use the Backup utility on each CA to back up the Sysvol folder.
C. Use the Backup utility on each CA to back up System State data.
D. Use the Backup utility on each CA to back up System State data and the Sysvol folder.

Answer: C

Explanation: The Certificate Services database maintained by each CA contains the

following important information:
1. All issues certificates.
2. All revoked certificates.
3. All requests for certificates.
4. All archived private keys.
When Certificate Services is installed on a Windows Server 2003 computer, the System State data of that computer includes the Certificate Services database together with all other important system services and components. For this reason, it is recommended that you back up the System State data of your CAs, and not back up the Certificate Services database in isolation.
Incorrect answers:
A: If key archival is enabled, the associated CA will store the private key of the certificate in its database. All archived key data is stored in the Certificate Services database, which means that archived key data will be included when you backup System State data on each CA. Configuring certificates to allow for key archival has nothing to do with backing up the Certificate Services database.
B: The Sysvol folder exists on domain controllers. This folder does not include any Certificate Services data.
D: The Sysvol folder exists on domain controllers. This folder does not include any Certificate Services data.

QUESTION 124:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional.
The Certkiller .com network contains several new Windows Server 2003 server computer running Certificate Services. These servers are configured as enterprise certification authorities (CAs). You plan to configure the servers to issue users with certificates they need for remote access, authentication, and data encryption. You need to ensure that only authorized administrators can approve requests for certificates, issue and revoke certificates, and deny and renew certificates. To this end you create a new global security group named CertAdministrators and add all authorized administrators to this group.
The ability to issue and revoke certificates should be assigned to members of the CertAdministrators group. Thus only members of the CertAdministrators global security group must be assigned permissions to manage certificates.
What should you do?

A. One each enterprise CA add the CertAdministrators group to the Certificate Manager role.
B. Assign the Allow - Enroll permission for all certificate templates to the CertAdministrators group.
C. Add the CertAdministrators group to the Cert Publisher group.
D. Ensure that each CertAdministrators group member is issued with an Enrollment

Agent certificate.

Answer: A

Explanation: In Windows Server 2003, Certificate Services uses role-based administration. Only users that belong to the Certificate Manager role can approve requests for certificates, issue and revoke certificates, and deny and renew certificates. To enable members of the CertAdministrators group to perform these tasks, you need to add the CertAdministratorsgroup to the Certificate Manager role on each enterprise CA on the network.
Incorrect answers:
B: This will only enable members of the CertAdministrators group to request certificates that use a certificate template.
C: The Cert Publisher group should only contain CAs, and not administrators, as members.
D: This will only enable members of the CertAdministratorsgroup to request certificates on behalf of other users.

QUESTION 125:

You work as the network administrator at Certkiller .com. The Certkiller .com network consists of a single Active Directory domain named Certkiller .com. All servers on the Certkiller .com network run Windows Server 2003 and all client computers run Windows XP Professional. The domain controllers named Certkiller -DC01 and Certkiller -DC02 run Windows Server 2003. All computers are domain members.
The basic Encryption File System (EFS) certificates were issued to all servers before the server computers were upgraded from the Windows 2000 Server to Windows Server 2003 operating system. The current validity period set for a basic EFS certificate is one year. The EFS certificate is autoenrolled to all users.
You receive instructions to modify the validity period of the basic EFS certificate to three years. You open the Certificates Templates management console to change the validity period for the basic EFS certificate template but you are unable to do so.
What should you do?

A. Duplicate and rename the basic EFS Recovery Agent Certificate template.
On the Security tab, modify the permission for the Administrators group to Full Control.
Change the validity period on the General tab.
B. Duplicate and rename the basic EFS Recovery Agent Certificate template.
Change the validity period on the General tab.
C. Duplicate and rename the basic EFS Recovery Agent Certificate template.
Change the renewal period on the General tab.
D. Open the basic EFS Recovery Agent Certificate template.
Modify the permission for the Administrators group to Full Control.
Change the validity period on the General tab

Answer: B

Explanation: The question states that the current EFS certificates were issued to all servers when they were running the Windows 2000 Server operating system. To change the validity period of the basic EFS certificate to three years, you first have to duplicate and rename the basic
EFS Recovery Agent Certificate template. This is because you cannot edit certificate templates in Windows 2000 Server. In Windows 2000 Server, certificate templates are read-only. After duplicating and renaming the basic EFS Recovery Agent Certificate template, you will be making the certificate template a Windows Server 2003 Version 2 certificate template, and will then be allowed to edit the validity period of the basic EFS certificate from one year to three years.
Incorrect answers:
A: There is no need to assign the Administrators group the Full Control permission. This permission is not needed to change the validity period of basic EFS certificates to three years. In addition to this, the Security tab is used to define role-based administration.
C: The renewal period on the General tab is used for renewing certificates. This setting has nothing to do with the validity period of certificates.
D: To change the validity period of a basic EFS certificate, you first have to make the Version 1 certificate template a Windows Server 2003 Version 2 certificate template. Only Windows Server 2003 Version 2 certificate templates can be edited. To do this, you have to duplicate and rename the basic EFS Recovery Agent Certificate template.

QUESTION 126:

Administrators in Certkiller .com use scripts to perform administrative tasks when they troubleshoot problems on client computes. They connect to the Telnet service on client computers when they run these scripts. For security reasons, all Telnet traffic is encrypted by using an IPSec policy. In addition, the Telnet service is configured for manual startup on all client computers. Administrators manually start and stop the Telnet service when they perform administrative tasks.
Administrators report that they sometimes cannot start the Telnet service on client computers. You examine several client computers and discover that the Telnet service is disabled.
You need to ensure that administrators can troubleshoot problems on client computers at all times.
What should you do?

A. Use a Restricted Groups policy in a new Group Policy object (GPO) to add the Domain Admins group to the Power Users group on each client computer.
B. Use a Restricted Groups policy in a new Group Policy object (GPO) to ensure that the Power Users group on each client computer contains no members.
C. Use a System Services policy in a new Group Policy object (GPO) to ensure that only Domain Admins can manage the Telnet service.

D. Use an Administrative Template setting to prevent local users from starting the Services snap-in.

Answer: C

Explanation: The first item is not needed as they are Administrators and they have full control.
This would work as long as the user was not part of the local Administrators group and the question does not say what the user permissions are, by default local Administrators can manage this service.

QUESTION 127:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003 computers. All computers are members of the domain.
The Certkiller .com written security policy states that all servers must have the security settings that are specified in a security template named Verify.inf. The Verify.inf security template is copied to the Systemroot\Security\Templates folder on each server.
You need to verify that the servers on the network meet the requirements in the written security policy.
What should you do?

A. On each server, run the gpresult command and save the result.
B. On each server, run the secedit.exe /analyze command for the Verify.inf security template and save the results.
C. On each server, run Microsoft Baseline Security Analyzer (MBSA) and save the results.
D. On a domain controller, import the Verify.inf security template into Security Configuration and Analysis and then start the Resultant Set of Policy Provider service.
E. On a domain controller, import the Verify.info security template into the Default Domain Policy GPO, and then run the gpupdate command.

Answer: B

Explanation: Security Configuration and Analysis performs security analysis by comparing the current state of system security against an analysis database.

QUESTION 128:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The network contains Windows XP Professional client computers and Windows Server 2003 computers only. All computers have access to the Internet.
You are planning the security patch management infrastructure. The written

security policy of Certkiller .com states that all computers must install only Certkiller .com-approved security patches.
You install Software Update Services (SUS) on a server named Certkiller -SR03.
You configure Automatic Updates on all computers to use Certkiller -SR03. You place computer accounts of several computers in a new group named CKPatchTest.
You want to test each newly approved security patch on the computers in the CKPatchTest group before you allow all computers to install the security patch.
You need to ensure that each time a new security patch is approved; only computers in the CKPatchTest group download and install the security patch.
What should you do?

A. On Certkiller -SR03, assign NTFS permissions to the CKPatchTest group for the new security patch files.
B. On Certkiller -SR03, assign NTFS permissions to the CKPatchTest group for the Approveditems.txt text files.
C. Configure Automatic Updates on the computers in the CKPatchTest group to use the Microsoft Windows Update servers. Copy an Approveditems.txt file to the Windows folder on these computers.
D. Configure Automatic Updates on the computers in the CKPatchTest group to use a second SUS server named Certkiller -SR04. Use a separate approval list on Certkiller -SR04.

Answer: D

QUESTION 129:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The network contains Windows XP Professional client computers and Windows Server 2003 computers only.
There are 15 Windows Server 2003 computers that serve as domain controllers. For security reasons, you do not allow the domain controllers to access Web sites over the Internet.
You need to scan all of the domain controllers to identify which security patches are not installed. You want to achieve this goal by using the minimum amount of administrative effort and by successfully completing the scan of all domain controllers.
What should you do?

A. Run Microsoft Baseline Security Analyzer (MBSA) on one of the domain controllers and target the domain controllers.
B. Run Microsoft Baseline Security Analyzer (MBSA) on a client computer that has Internet access and target all the domain controllers.
C. Run Microsoft Baseline Security Analyzer (MBSA) on each domain controller with a copy of the MBScan.wsf file that you downloaded from the Microsoft Web site.
D. Run Microsoft Baseline Security Analyzer (MBSA) on each domain controller with a copy of the Mssecure.cab file that you downloaded from the Microsoft Web site.

Answer: B

QUESTION 130:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
You are planning a security patch management infrastructure. You install Software Update Services (SUS) on server named Certkiller -SR22. You configure client computer to use Certkiller -SR22.
All client computers run custom applications developed by Certkiller .com.
You need to deploy custom security patches for applications that Certkiller .com developed.
What should you do?

A. Configure a GPO to install the customer security patches when the client computers start up.
B. Digitally sign the custom security patches, and then copy the files to the Content folder on Certkiller -SR22.
C. Update the Mssecure.xml file with information about the custom security patches, and then run Microsoft Baseline Security Analyzer (MBSA) with the updated MSsecure.xml file.
D. Copy the custom security patches to the Content folder on Certkiller -SR22. Run Mbsacli.exe, and configure Mbsacli.exe to use Certkiller -SR22.
E. Copy the Content folder from Certkiller -SR22 to a new Web server. Add the custom security patches to the folder. Configure Automatic Updates on the client computers to use the new Web server.

Answer: A

QUESTION 131:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The network contains Windows XP Professional client computers and Windows Server 2003 computers only.
One hundred of your users are mobile users in the sales department. These users work from home offices and use portable computers that are not members of the corporate domain. They do not connect to the corporate network on a regular basis. Mobile users communicate with users on the corporate network by using SMTP and POP3 e-mail. All mobile users have user accounts in the corporate domain.
You decide to deploy Software Update Services (SUS) as part of your patch management strategy. You install SUS on a server named Certkiller -SR25. You configure Certkiller -SR25 to be accessible to users on the Internet. You review and approve the necessary security patches.
You need to configure mobile users' computers to install only approved security

patches. You want to achieve this goal by using the minimum amount of administrative effort.
What should you do?

A. Create a new GPO that applies to only mobile users. Configure the GPO to download updates from Certkiller -SR25. Instruct users to run a script that includes the gpupdate command.
B. Create a new GPO that applies to only mobile users. Configure the GPO to download updates from Certkiller -SR25. Instruct users to run a script that includes the gpresult command.
C. Write a script that modifies the local registry of each portable computer to use Windows Update. Instruct mobile users to run the registry modification script.
D. Write a script that modifies the local registry of each portable computer to use Certkiller -SR25. Instruct mobile users to run the registry modification script.

Answer: D

QUESTION 132:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The network contains Windows XP Professional client computers and Windows Server 2003 computers only.
You install Software Update Services (SUS) on a server named Certkiller -SR23.
The Certkiller .com written security policy states that all updates must be tested and approved before they are installed on network computers.
You need to ensure that SUS uses the minimum amount of disk space on Certkiller -SR23.
What should you do?

A. Configure Certkiller -SR23 to redirect client computers to the Microsoft Windows Update servers.
B. Compress the folder in which the downloaded updates are stored.
C. Configure Certkiller -SR23 to store only the locales that are needed.
D. Download the updates, and then delete updates that are not approved for client computers.

Answer: A

QUESTION 133:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows 2000 Professional. Certkiller .com has a main office and 150 branch offices located throughout the United States and Canada. The company does not use disk-imaging software.
In the past, newly installed client computers were exploited by malicious Internet

worms before you applied all security patches.
You need to build and deploy client computers that will always have the least service packs, updates, and security patches. You want to achieve this goal by using the minimum amount of administrative effort.
What should you do?

A. Install the operating system on the computers by using the original installation media. Use Windows Update immediately after the installation to apply updates and security patches.
B. Install the operating system on the computers by using the original installation media. Configure Automatic Updates to immediately install updates and security patches.
C. Create slipstream installation media that has the latest service pack.
Install the operating system from the slipstream installation media.
Implement a Software Update Services (SUS) server to install approved updates and security patches on client computers.
D. Create slipstream installation media that has the latest service pack and includes Microsoft Baseline Security Analyzer (MBSA).
Install the operating system form the slipstream installation media.
Run MBSA immediately after installing the operating system.

Answer: C

Explanation:
Incorrect answers:
A: This would allow for exploitation as the system is new and therefore unpatched and would have to download all patches.
B: This is the same as the aforementioned.
D: This does nothing to install patches. This is still a new install and a check just to see what patches is needed.

QUESTION 134:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All 80 servers run Windows Server 2003. All 2,000 client computers run Windows XP Professional. All computers are members of the domain.
A windows Server 2003 computer named Certkiller -SR27 functions as an internal Web server. Employees in the marketing department regularly upload files to Certkiller -SR27 using the FTP service.
You decide to product this data while it is in transit via FTP to Certkiller -SR27.
You implement IPSec and assign the default IPSec Secure Server policy on Certkiller -SR27. You implement IPSec and assign the default IPSec client policy on the marketing client computer. You verify that the FTP data is encrypted by monitoring the traffic between the marketing department client computer and Certkiller -SR27.
Users report that the HTTP service on Certkiller -SR27 is no longer accessible

from client computers that are not in the marketing department. DNS queries made from Certkiller -SR24 also fail to resolve.
You need to restore access to the normal HTTP server and DNS client functionality on Certkiller -SR24 while preserving the encryption of FTP data between Certkiller -SR27 and the marketing department client computers.
What should you do?

A. Unassign the IPSec Secure Server policy and assign the default Server policy of Certkiller -SR24.
B. Unassign the Client Policy and assign a customer IPSec policy on marketing department client computers that uses authentication headers on Certkiller -SR27.
C. Unassign the IPSec Secure Server policy and assign a custom IPSec policy that requires IPSec only for FTP data on Certkiller -SR27.
D. Unassign the IPSec Secure Server policy and assign a custom IPSec policy that does not require IPSec for DNS data on Certkiller -SR27.

Answer: C

Explanation: The new policy applied has caused the error. Only FTP traffic needs to be secured. FTP is commonly misunderstood as a secure means for transferring data, because the FTP server can be configured to require a valid user name and password combination prior to granting access. Be aware that neither the credentials specified at logon nor the data itself is encrypted or encoded in any way. All credentials are sent across the network in plaintext.

QUESTION 135:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All client computers run Windows XP Professional. All servers run Windows Server 2003. All computers on the network are members of the domain.
Traffic on the network is encrypted by IPSec. The domain contains a custom IPSec policy named Lan Security that applies to all computers in the domain. The Lan Security policy does not allow unsecured communication with non-IPSec-aware computers.
The Certkiller .com written security policy states that the configuration of the domain and the configuration of the Lan Security policy must not be changed.
The domain contains a multihomed server named Certkiller -SR12.
Certkiller -SR12 is connected to the company network, and Certkiller -SR12 is also connected to a test network. Currently, the Lan Security IPSec policy applies to the network traffic on both network adapters on Certkiller -SR12.
You need to configure Certkiller -SR12 so that it communicates on the test network without IPSec security. Certkiller -SR12 must still use the Lan Security policy when it communicates on the company network.
How should you configure Certkiller -SR12?

A. Configure a packet filter for the network adapter on the test network to block the Internet Key Exchange (IKE) port.
B. Configure the network adapter on the test network to disable IEEE 802.1x authentication.
C. Configure the network adapter on the test network to enable TCP/IP filtering, and them permit all traffic.
D. Use the netsh command to assign a persistent IPSec policy that permits all traffic on the network adapter on the test network.
E. Assign an IPSec policy in the local computer policy that permits all traffic on the network adapter on the test network.

Answer: D

Explanation: Persistent IPSec policies enhance security by providing a secure transition from computer startup to IPsec policy enforcement. Persistent policy also provides backup security in the event of an IPSec policy corruption, or if errors occur during the application of local or domain-based IPSec policy. To configure persistent policies, you must use the netsh ipsec static set store location=persistent command.

QUESTION 136:

You are a security administrator for Certkiller .com. The network consists of two Active Directory domains. All servers run Windows Server 2003. Client computers run either Windows XP Professional or Windows 2000 Professional. All domain controllers in both Active Directory domains are Windows Server 2003 computers. All computers are Active Directory domain members.
During a security assessment, you discover that you can extract LAN Manager and NTLM password hashes from domain controller computers. You are able to guess many user account passwords within a short time by using a password cracking program. This poses an unacceptable security risk for Certkiller .
You need to increase the time required to guess user account passwords. You increase the minimum user account password length to nine characters, enable the Password must meet complexity requirements setting, and require all domain users to change their password at the next logon.
What else should you do?

A. Apply a security template to all domain controller computers that enables the Domain member: Require strong (Windows 2000 or later) session key setting.
B. Apply a security template to all domain controller computers that establishes the Network security: LAN Manager authentication level setting at Send NTLMv2 response only.
C. Apply a security template to all domain controller computers that enables the Network security: Do not store LAN Manager hash value on next password change setting.
D. Apply a security template to all domain controller computers that enables the System

Cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing setting.

Answer: C

QUESTION 137:

You are a security administrator for Certkiller .com. Certkiller .com consists of two divisions. One division is named Certkiller .com America and is located in San Francisco. The other division is named Certkiller .com Europe and is located in Paris. Each division is connected to the Internet by a 1.544 Mbps WAN connection.
Certkiller .com America consists of a single Active Directory forest named Certkiller -am.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. Certkiller .com America has a Microsoft SQL Server 2000 database that contains customer information. The SQL Server 2000 database is hosted on a Windows Server 2003 computer named Certkiller -SR21.
Certkiller .com Europe consists of a single Active Directory forest named Certkiller -eu.com. All servers run Windows 2000 Server. All client computers run Windows 2000 Professional or Windows NT Workstation. All computers run the latest service packs.
To enable data replication, you configure a new Windows Server 2003 computer named Certkiller -SR22 in the Certkiller -eu.com forest. You install SQL Server 2000 on Certkiller -SR22. Your database administrator configures the database on Certkiller -SR21 to replicate to Certkiller -SR22 every night.
Management reports that a competitor acquired confidential customer data. You determine that the competitor intercepted customer data as it replicated from Certkiller -SR21 to Certkiller -SR22. You decide to use IPSec to protect customer data as it replicated.
You need to configure an IPSec policy to protect customer data as it replicates.
What should you do?

A. Configure the IPSec policy to use Authentication Header (AH) in transport mode with Kerberos authentication.
B. Configure the IPSec policy to use Encapsulating Security Payload (ESP) with certificate-based authentication in tunnel mode.
C. Configure the IPSec policy to use Authentication Header (AH) with certificate-based authentication in transport mode.
D. Configure the IPSec policy to use Encapsulating Security Payload (ESP) with Kerberos authentication in tunnel mode.

Answer: B

Explanation: IPSec can operate in two different modes: transport mode and tunnel mode. Typically, you should use transport mode to protect host-to-host communications. In transport mode, IPSec tunnels traffic starting at the transport layer, also known as layer 4. Therefore, IPSec in transport mode can encrypt the User Datagram.

When you protect traffic sent directly between two hosts, you will almost always use IPSec transport mode. When you protect traffic between a host and a network, or between two networks, you must use IPSec tunnel mode. Although transport mode stores the UDP/TCP header and the application data between an IPSec header and trailer, tunnel mode stores the entire original packet.
Use transport mode when you communicate with one computer, and use tunnel mode when you communicate with an entire network, so when the decision calls for encapsulating or tunneling the IP header, use tunnel mode.

QUESTION 138:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003.
Certkiller hosts a secure Web site for customers. The secure Web site is hosted on a computer Certkiller -SR25. Customers who want access to the Web site are issued certificates from an enterprise certification authority (CA). The enterprise CA is configured to store User certificates in Active Directory.
The Certkiller .com written security policy includes the following requirements for Certkiller -SR25:
1. Only users with valid certificates that were issued by Certkiller .com are permitted to access the secure Web site.
2. User access to the secure Web site must be maintained by using minimum amount of administrative effort.
3. Security administrators must be able to audit access on per user basis.
You need to configure Certkiller -SR25 to provide the customers with access to the secure Web site.
What should you do?

A. Configure Certkiller -SR25 to require SSL for all communications.
B. Configure Certkiller -SR25 to use one-to-one certificate mapping.
C. Configure Certkiller -SR25 to use many-to-one certificate mapping.
D. Configure Certkiller -SR25 to use Windows directory service mapper.

Answer: D

QUESTION 139:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The network contains Windows XP Professional client computers and Windows Server 2003 computers only. The network contains three member servers named Certkiller -SR01, Certkiller -SR02, and Certkiller -SR03. The three member servers connected to the Internet.
You plan to implement remote access to the Certkiller .com network for users that work from home.

You configure and enable Routing and Remote Access on Certkiller -SR01 and Certkiller -SR02. Mia Hamm, who is an administrator on all member servers, configures and enables Routing and Remote Access on Certkiller -SR02. However, users cannot establish a VPN connection to Certkiller -SR03. You discover that Certkiller -SR03 can only authenticate Internet VPN connections from local users accounts.
You need to ensure that users from the domain can successfully establish a VPN connection to Certkiller -SR03.
What should you do?

A. Enable the Certkiller -SR03 computer account in Active Directory as trusted for delegation.
B. Assign the Authenticated Users group the Allow - Allowed to Authenticate permission for the Certkiller -SR03 computer account in Active Directory.
C. Assign the Certkiller -SR03 computer account the Allow - Read permission on the RAS and IAS Servers Access Check container in Active Directory.
D. Add the Certkiller -SR03 computer account to the RAS and IAS Servers security group.
E. Add the Certkiller -SR03 computer account to the Windows Authorization Access group security group.

Answer: D

QUESTION 140:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows 2000 Professional.
Certkiller .com has one main office and three branch offices. Domain controllers are located in the main office and in each office of the three branch offices. Each office is configured as a separate Active Directory site. Domain controllers in the main office are stored in a physically secure location.
The Certkiller .com written security policy states that administrators must use a smart card when logging on to a domain controller that is not stored in a physically secure location. You install smart card readers on all domain controllers and on the client computers of all administrators. You issue smart cards to all administrators.
You need to ensure that smart cards are required when logging on locally only to domain controllers that are not physically secure location.
What should you do?

A. Create a new GPO and link it to each branch office site. Filter the GPO to apply to only domain controllers. Enable the Interactive login: Require smart card setting.
B. Edit the properties of each administrator account that will be used to perform administration at the branch offices. Select the Smart card is required for interactive logon check box.
C. Enable Remote Desktop on each branch office domain controller. Instruct

administrators to use Remote Desktop Connection to connect to branch office domain controllers. Select the Smart Card check box on the properties of the Remote Desktop Connection.
D. Move all domain controller objects to a new OU named Branch Offices. Create a new GPO and link it to the Branch Offices OU. Enable the Interactive login: Require smart card setting.

Answer: A

QUESTION 141:

You are a security administrator for Certkiller .com. The network consists of two Active Directory forests. Each forest contains four domains. The root domains are named Certkiller .com and foo.com. All servers on the Certkiller .com network run Windows Server 2003.
You want to allow the users in both forests to access resources in the other forest. You create a two-way forest trust relationship between the Certkiller .com forest and the foo.com forest. However, users report that they cannot access resources on servers in the other forest.
You verify that network connectivity and DNS name resolution between the two forests are functioning correctly. The users are attempting to connect to resources for which the Authenticated Users group is assigned the Allow - Read permission. You discover that all users are members of the Other Organization group when they attempt to connect to resources in the other forest.
You need to ensure that users in one forest can access resources on servers in the other forests.
What should you do?

A. Add the Domain Computers security group from each root domain to the Windows Authentication Access Group security group in the other root domain.
B. Configure the scope of the authentication of the forest trust relationship to disable selective authentication.
C. Configure the trusted domain object (TDO) in each forest to disable name suffix routing.
D. In each root domain, configure a domain controller to be global catalog server.

Answer: C

QUESTION 142:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional. You use Group Policy objects (GPOs) to manage client computers.
Certkiller .com has a wireless LAN (WLAN) that 50 employees who have portable computers use. Management reports that an additional 500 employees will receive

portable computers in the next six months. These employees will have access to the WLAN. To address security concerns, management requires that portable computer users use smart cards to log on.
You need to plan a WAN implementation to meet management requirements. You want to achieve this goal without affecting the application of Group Policy.
Which three actions should you perform? (Each correct answer presents part of the solution. Choose THREE.)

A. Deploy WLAN hardware that supports IEEE 802.1x.
B. Deploy WLAN hardware that supports 128-bit Wired Equivalent Privacy (WEP) keys.
C. Implement an Internet Authentication Service (IAS) infrastructure.
D. Implement a public key infrastructure (PKI).
E. Implement a Routing and Remote Access infrastructure.
F. Implement IPSec on all portable computers.

Answer: A, C, D

QUESTION 143:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
Certkiller .com hosts Web applications for customers. Each customer is a company that has multiple employees who require access to the Web application. Each customer has one Web application. Each Web application is configured as a virtual directory. You configure a user account for each customer. You assign this account permission to read the virtual directory that contains the customer's Web application.
You need to ensure that employees can access only their company's Web application. You must accomplish this task without requiring customers to disclose passwords.
What should you do?

A. Configure anonymous access for each virtual directory.
Configure each virtual directory to use the customer's assigned user account.
Leave the password assigned to the user account blank.
B. Configure Microsoft .NET Passport authentication for each virtual directory.
Instruct each employee of each customer that requires access to the Web site to enroll for a new .NET Passport.
C. Configure a certification authority (CA).
Issue certificates to each employee of each customer that requires access to the Web site.
Configure many-to-one certificate mapping.
D. Acquire a Server Authentication digital certificate from a public certification authority (CA).
Configure the Web server to use this certificate and to require SSL.
E. Distribute a copy of the Server Authentication certificate to each employee of each

customer that requires access to the Web site.

Answer: C

Explanation
Anonymous would allow access to any of the websites. Microsoft .NET Passport would have the user use passwords. IIS cannot process client certificates unless you have previously installed a server certificate and enabled HTTPS.
You can use client certificate mapping to restrict access to users with specific certificates. Many-to-one certificate mapping uses wildcard matching rules that verify whether a client certificate contains specific information, such as the issuer or subject. This mapping does not identify individual client certificates; it accepts all client certificates fulfilling the specific criteria. If a client gets another certificate containing all the same user information, the existing mapping will still work. Certificates do not need to be exported for use in many-to-one mappings.

QUESTION 144:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All domain controllers run Windows Server 2003. All client computers run Windows XP Professional.
Users store files on a server named Certkiller -SR12. These files are confidential and must be encrypted at all times while on Certkiller -SR12.
You configure a new certification authority (CA) and issue certificate that support Encrypting File System (EFS) to all users. Users report that they cannot encrypt files that are stored on Certkiller -SR12. They report that they can encrypt files that are stored locally on their client computers.
You need to ensure that users can encrypt files that are stored on Certkiller -SR12.
What should you do?

A. Enroll Certkiller -SR12 for a Computer certificate that supports file encryption.
B. Configure a new EFS recovery agent.
Deploy the EFS recovery agent by using Active Directory.
C. Configure the Certkiller -SR12 computer account to be trusted for delegation.
D. Enroll each client computer for a Computer certificate that supports file encryption.

Answer: C

Explanation: When you are unable to Encrypt Files there are various reasons such as:
The file is not an NTFS volume.
You do not have Write access to the file.
If you are having trouble encrypting a remote file, check to see that your user profile is available for EFS to use on that computer (this typically means having a roaming user profile), make sure the remote computer is trusted for delegation, and make sure your account is configured to enable delegation. Sensitive accounts are not enabled for

delegation by default, so users like Enterprise Administrator might not be able to encrypt or decrypt files remotely.
When you are unable to Decrypt Remote Files - the "Access is denied" message then it could be that the computer on which the encrypted file is stored is not trusted for delegation. Or the user account that EFS needs to impersonate cannot be delegated.

QUESTION 145:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional. Users are in the marketing, sales, or production department.
A high-performance color print device named CKPrinter3 is attached to a server named Certkiller -SR09. CKPrinter3 is shared by users in the marketing department. Only users in the marketing department are permitted to print documents on CKPrinter3. Mia Hamm is a user in the marketing department. Mia Hamm is responsible for ensuring that print jobs on CKPrinter3 print properly. She is also responsible for replacing paper and for general print device maintenance. Mia Hamm is not permitted to modify the printer itself
You need to configure permissions for CKPrinter3. You create a global group named Marketing. You add all marketing users to the Marketing global group. What else should you do?

A. Assign the global group the Allow - Manage Documents permissions for CKPrinter3. Assign Mia Hamm the Allow - Manage Printers permission for CKPrinter3.
B. Assign the global group the Allow - Print permission for CKPrinter3. Create a local group on Certkiller -SR09. Add Mia Hamm to the local group. Assign the local group the Allow - Manage Printers permissions for CKPrinter3.
C. Add the global group to a local group on Certkiller -SR09. Assign the local group the Allow - Manage documents permission for CKPrinter3. Assign Mia Hamm the Allow - Manage Printers permission for CKPrinter3.
D. Add the global group to a local group on Certkiller -SR09. Assign the local group the Allow - Print permission for CKPrinter3. Create another local group on Certkiller -SR09. Add Mia Hamm to the second local group. Assign the second local group the Allow - Manage documents permission for CKPrinter3.

Answer: D

QUESTION 146:

You are a security administrator for Certkiller .com. The network consists of three Active Directory domains. All Active Directory domains are running at a Windows Server 2003 mode functionality level.
Employees in the editorial department of Certkiller .com need access to resources on file servers that are in each of the Active Directory domains.
Each Active Directory domain in the company contains at least one editorial

department employee user accounts and that has access to the resources on file server computers.
What should you do?

A. Create a global distribution group in the forest root domain and name it Company Editors.
B. Create a global security group in the forest root domain and name it Company Editors.
C. Create a universal distribution group in the forest root domain and name it Company Editors.
D. Create a universal security group in the forest root domain and name it Company Editors.

Answer: D

QUESTION 147:

You are a security administrator for Certkiller .com. The network consists of two Active Directory forests that contain two domains. The domains are named Certkiller .com and foo.com. All Active Directory domains are running at a Windows Server 2000 mixed mode functionality level.
Employees in the help desk department need to modify certain attributes of employee user accounts that reside in the Certkiller .com domain. The help desk department user accounts reside in the foo.com domain.
You need to crate a single group named Help Desk that contains all help desk department user accounts and that can be granted access to modify employee user accounts in the Certkiller .com domain.
What should you do?

A. Use a universal security group in the Certkiller .com domain named Help Desk.
B. Use a universal security group in the foo.com domain named Help Desk.
C. Use a global security group in the foo.com domain named Help Desk.
D. Use a global security group in the Certkiller .com domain named Help Desk.

Answer: C

QUESTION 148:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory forest that contains three domains in a single domain tree. All servers run Windows Server 2003. All computers are members of the domains. The functional level of the forest is Windows 2000. The functional level of each domain is Windows Server 2003.
Certkiller .com has a main office and five branch offices. Each branch office is configured as a separate Active Directory site. There is one domain controller for each of the three domains in each site. Only the main office contains global catalog servers.

Users report that logging on in the branch office takes much longer than logging on in the main office.
You need to ensure that the logon process in the branch offices completes more quickly. You do not want to install additional global catalog servers in the branch office, and you do not want to increase the bandwidth between the branch offices and the main office.
What should you do?

A. Raise the functional level of the forest to Windows Server 2003.
B. Create a two-way shortcut trust between the two child domains.
C. Enable universal group membership caching.
D. Convert all universal groups in the three domains to domain local groups or global groups.
E. Increase the maximum lifetime for Kerberos user tickets.

Answer: C
Argument for C: D - is only partially right because: When using Universal to global is only allowed if the group you want to change does not have another universal group as a member.
The question gives no indication that it does or doesn't have this level of nesting. If we work under the assumption the UG are in use then converting them would break access to the resources to which they were create for. Furthermore if the UGs were used in other DLGs for permissions/access, this too would stop working.

QUESTION 149:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory forest that contains three domains in a single domain tree. All servers run Windows Server 2003. All computers are members of the domains. The functional level of the forest is Windows 2000. The functional level of each domain is Windows Server 2003.
All users in the forest are in the root domain. The two child domains contain client computers accounts and server accounts. Only the root domain contains global catalog servers.
Certkiller .com uses an application that stores data in a custom application directory partition. The application runs on domain controllers in all three domains.
You add the users that manage the data in the custom application directory partition to a global group named App Managers. You add the App Managers group to a domain local group named App Data. You assign the App Data group the Allow - Modify permission for all objects in the custom application directory partition.
Some users in the App Managers group report that they receive an Access Denied message when they attempt to access the application data. Other users in the App Managers group can successfully access the application data in the application directory partition.
You need to ensure that all users in the App Managers group can access the

application data successfully.
What should you do?

A. Raise the functional level of the forest to Windows Server 2003.
B. Change the scope of the App Data group to universal.
C. Install a global catalog server in the two child domains.
D. Create a two-way shortcut trust relationship between the two child domains.
E. Assign the App Managers group the Allow - Allowed to Authenticate permission on all domain controllers that run the application.

Answer: B

Explanation:

QUESTION 150:

You are a security administrator for Certkiller .com. The network contains a Windows Server 2003 computer that runs IIS. You use this server to host an Internet Web site for customer product purchasing. You plan to use SSL on this computer. You do not want customer to receive a certificate-related security alert when they use SSL to connect to your Web site.
You need to select an appropriate certification authority (CA) to server as the issuer for your Web server SSL certificate.
What should you do?

A. Use an online enterprise root CA.
B. Use an online stand-alone root CA.
C. Use a commercial CA.
D. Use an offline stand-alone root CA.

Answer: C

Explanation: To use SSL, the server must have a suitable public key certificate. Additionally, some SSL scenarios allow or require the client to use a public key certificate. SSL is one of the most common uses for public key certificates, and, as a result, you can obtain SSL certificates from a wide variety of places. Any organization with a computer running Windows Server 2003 can deploy Certificate Services to issue SSL certificates without any additional cost. These certificates are suitable for intranet scenarios, in which both the servers and the clients are controlled by a single organization.

QUESTION 151:

You are a security administrator for Certkiller .com. You plan to allow certain users to receive an EFS Recovery Agent Certificate. Currently, users do not have the option to enroll for an EFS Recovery Agent certificate. You need to restrict

enrollment to members of the Certkiller .com Recovery Agents domain global group.
You add the EFS Recovery Agent certificate type to the list of approved certificate templates on the enterprise subordinate CA. You have not modified any other default Certificate Services or certificate template settings.
You need to allow only members of the Company Recovery Agents group to obtain EFS Recovery Agent Certificates.
What should you do?

A. Assign the Domain Users group the Allow - Enroll permission for the EFS Recovery certificate template.
B. Assign the Domain Users group the Allow - Read permission for the EFS Recovery certificate template.
C. Assign the Certkiller Recovery Agents group the Allow - Enroll permission for the EFS Recovery certificate template.
D. Assign the Certkiller Recovery Agents group the Allow - Read permission for the EFS Recovery certificate template.

Answer: C

Explanation: To create a recovery agent account, create a user account, then explicitly grant the account Enroll permission on Certificate Services' EFSRecovery certificate template. (The default ACL on the EFSRecovery template lets only members of the Domain Admins and Enterprise Admins groups request a recovery agent certificate.)
Open the Microsoft Management Console (MMC) Active Directory Sites and Services snap-in, then navigate to the Certificate Templates folder, To start to grant Enroll permission to a user.

QUESTION 152:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The network contains Windows XP Professional client computers and Windows Server 2003 computers.
You install Certificate Services to issue certificates to employees for secure e-mail encryption and Web site authentication. You revoke the certificates used by an employee when that employee leaves the company. Several thousand certificates are currently revoked, and multiple revocations occur daily.
Certkiller .com e-mail and Web applications already use strong revocation checking of certificates.
You need to reduce the time it takes for client computers to find out about certificate revocations and to process certificate revocation information. You also need to limit the negative impact that this change will have on network performance.
What should you do?

A. In the Certification Authority console, open the Revoked Certificates properties.

Set the Delta Certificate Revocation List (CRL) publication interval to one hour.
B. In the Certification Authority console, open the Revoked Certificates properties.
Set the full Certificate Revocation List (CRL) publication interval to one hour.
C. In the Certification Authority console, highlight Revoked Certificates, and then select the option to publish a full CRL after you revoke a certificate.
D. In the Certification Authority console, highlight Revoked Certificates, and then select the Refresh option.

Answer: A

Explanation:
Certificate revocation
A certificate has a specified lifetime, but CAs can reduce this lifetime by the process known as certificate revocation. The CA publishes a certificate revocation list (CRL) that lists serial numbers of certificates that it regards as no longer valid. The specified lifetime of CRLs is typically much shorter than that of a certificate. The CA might also include in the CRL the reason the certificate has been revoked. A revocation might occur because a private key has been compromised, because a certificate has been superseded, or because an employee has left the company. The CRL also includes the date the certificate was revoked. During signature verification, applications can check the CRL to determine whether a given certificate and key pair are still trustworthy. Applications can also determine whether the reason or date of the revocation affects the use of the certificate in question. If the certificate is being used to verify a signature, and the date on the signature precedes the date of the revocation of the certificate by the CA, the signature can still be considered valid. Off the Record: Most applications do not analyze the reason code. If a certificate is revoked, it's revoked. The reason code just isn't that important. To reduce the number of requests sent to the CA, the CRL is generally cached by the client, which can use it until it expires. If a CA publishes a new CRL, applications that have a valid CRL do not usually use the new CRL until the one they have expires.

QUESTION 153:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The Certkiller .com domain contains Windows Server 2003 computers and Windows XP Professional client computers.
All computers are members of the domain.
A Windows Server 2003 computer named Certkiller -SR23 runs Certificate Services. Certkiller -SR23 is an enterprise subordinate certification authority (CA). A Windows Server 2003 computer named Certkiller -SR22 runs IIS. Certkiller -SR22 hosts an internal human resources web site for employees. You want to ensure that the personal data of the employees is not exposed while in transit over the network. You decide to use SSL on Certkiller -SR22.
You need to ensure that employees do not receive a certificate-related security alert when they use SSL to connect to this Web site. You want to achieve this goal without spending money to purchase this certificate unless it is necessary to do so.
What should you do?

A. Use IIS to submit a certificate request to a commercial CA.
B. Use IIS to submit a certificate request to Certkiller -SR23.
C. Use the Certificates console to submit a Client certificate request to a commercial CA.
D. Use the Certificates console to submit a Client certificate request to
Certkiller -SR23.

Answer: B

QUESTION 154:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The Certkiller .com domain contains Windows Server 2003 computers and Windows XP Professional client computers. All computers are members of the domain.
The employee user accounts in Certkiller .com are members of the Administrators local group on client computers. You occasionally experience problems managing client computers because an employee removes the Domain Admins global group from the Administration local group on the computer.
You need to prevent employees from removing the Domains Admins global group from the Administrators local group on client computers.
What should you do?

A. Apply a security template to the client computers that establishes the Domain Admins global group as a member of the Administrators local group by using the Restricted Groups policy.
B. Apply a security template to the domain controller computers that establishes the Domain Admins global group as a member of the Administrators domain local group by using the Restricted Groups policy.
C. Modify the Domain Admins global group by assigning the Allow - Full Control permission to the Domain Admins global group.
D. Modify the Domain Admins global group by assigning the Deny - Full Control permission to the Domain Admins global group.

Answer: A

Explanation: When a Restricted Group policy is enforced, any current member of a restricted group that is not on the "Members" list is removed with the exception of administrator in the Administrators group. Any user on the "Members" list which is not currently a member of the restricted group is added.
Using the "Member Of" Restricted Group Portion of Policy
Only inclusion is enforced in this portion of a Restricted Group policy. The Restricted Group is not removed from other groups. It makes sure that the restricted group is a member of groups that are listed in the Member Of dialog box.

QUESTION 155:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All servers are in an OU named Servers, or in OUs contained within the Servers OU.
Based in information in recent security bulletins, you want to apply settings from a security template named Messenger.info to all servers on which the Messenger service is started. You do not want to apply these settings to servers on which the Messenger service is not started. You also do not want to move servers to outer OUs.
You need to apply the Messenger.inf security template to the appropriate servers.
What should you do?

A. Import the Messenger.info security template into a GPO, and link the GPO to the Servers OU. Configure Administrative Templates filtering in the GPO.
B. Import the Messenger.info security template into a GPO, and link the GPO to the Servers OU. Configure a Windows Management Instrumentation (WMI) filter for the GPO.
C. Configure a logon script in a GPO, and link the GPO to the Servers OU. Configure the script to run the gpupdate command if the Messenger service is running.
D. Edit the Messenger.info security template to set the Messenger service startup mode to Automatic, and then run the secedit /refreshpolicy command.

Answer: B

QUESTION 156:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
Eight Windows 2003 computers are members of the domain. These computers are used to store confidential files. They reside in a data center that only IT administration personnel have physical access to.
You need to restrict members of a group named Contractors from connecting to the filer server computers. All other employees require to these computers.
What should you do?

A. Apply a security template to the filer server computers that assigns the Access this computer from the network right to the Domain Users group.
B. Apply a security template to the filer server computers that assigns the Deny access to this computer from the network right to the Contractors group.
C. Apply a security template to the filer server computers that assigns the Allow log on locally right to the Domain Users group.
D. Apply a security template to the filer server computers that assigns the Deny log on locally right to the Contractors group.

Answer: B

Explanation:
Deny access to this computer from the network Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment Description
Determines which users are prevented from accessing a computer over the network.

QUESTION 157:

You are a security administrator for Certkiller .com. The network consists of two Active Directory forest named Certkiller .com and public. Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
The network consists of an IEEE 802.11b wireless LAN (WLAN). Employees and external users use the WLAN. User accounts for employees are located in the Certkiller .com forest. User accounts for external users are located in the public. Certkiller .com forest. External users' computers do not have computer accounts in the public. Certkiller .com forest.
To increase security, you upgrade the network hardware to support IEEE 802.1x. You configure a public key infrastructure (PKI). You issue Client Authentication certificates to employees, to client computers used by employees, and to external users.
You need to configure the WLAN to authenticate employees and external users.
What should you do?

A. Configure each wireless access point to forward RADIUS requests to a server running Internet Authentication Service (IAS).
Configure the IAS server to use a connection request policy to forward the requests to the appropriate forest.
B. Configure each wireless access point to forward requests to an Internet Authentication Service (IAS) server in the Certkiller .com forest.
Configure the IAS server in the Certkiller .com forest to use the Tunnel-Server-Endpt attribute.
C. Use the Connection Manager Administration Kit (CMAK).
Configure one connection profile for external users.
Configure a second connection profile for employees.
D. Establish a forest trust relationship between the Certkiller .com forest and the public. Certkiller .com forest.

Answer: A

Explanation: Connection request policies are sets of conditions and profile settings that give network administrators flexibility in configuring how incoming authentication and accounting request messages are handled by the IAS server. With connection request policies, you can create a series of policies so that some RADIUS request messages sent from RADIUS clients are processed locally (IAS is being used as a RADIUS server) and other types of messages are forwarded to another RADIUS server (IAS is being used as a

RADIUS proxy). This capability allows IAS to be deployed in many new RADIUS scenarios.

QUESTION 158:

You are a security administrator for Certkiller .com. The network consists of seven Active Directory domains. These domains are in the same Active Directory forest. All seven Active Directory domains operate at a Windows Server 2003 domain functional level.
Each domain contains an internal Web site that is used to publish information to the Certkiller .com managers. Access to the information on this Web site must not be restricted to managers. An existing global group in each domain contains the management user accounts that exist in that domain.
You need to restrict access to the internal Web sites to Certkiller .com managers. You want to achieve this goal by using the minimum amount of administrative effort.
What should you do?

A. Create a universal group in one of the Active Directory domains.
Add the existing management global groups as members of the universal group.
Assign only this universal group permissions to access the Web sites.
B. Create a global group in one of the Active Directory domains.
Add the existing management global groups as members of the global group.
Assign only this global group permissions to access the Web sites.
C. Create a domain local group in one of the Active Directory domains.
Add the existing management global groups as members of the domain local group.
Assign only this domain local group permissions to access the Web sites.
D. Assign only the existing management global permissions to access the Web sites.

Answer: A

Explanation: Global: accounts from the same domain, and global groups from the same domain
Domain local: accounts from any domain, global groups from any domain, universal groups from any domain, and domain local groups from the same domain
Windows 2000 global groups are effectively the same as Windows NT global groups. In terms of membership, they have domain-wide scope, but can be granted permissions in any domain, even in other forests and earlier version domains as long as a trust relationship exists.
Universal groups can contain members from any Windows 2000 domain in the forest, but cannot contain members from outside the forest. You can grant universal groups permissions in any domain, even in other forests, as long as a trust relationship exists.
Although universal groups can have members from mixed mode domains in the same forest, the universal group will not be added to the access token of these members because universal groups are not available in mixed mode.
You can add users to a universal group, but it is recommended that you restrict universal

group membership to global groups. Universal groups are available only in native mode domains.
You can use universal groups to build groups that perform a common function within an enterprise.
Universal groups could be used as a container in these circumstances to hold global groups from each subsidiary or department, with a single access control entry (ACE) for the universal group to protect the team resources.

QUESTION 159:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
All computers are configured to use Automatic Updates to install updates without user intervention. Updates are scheduled to occur during off-peak hours.
During a security audit, you notice some client computers are not receiving updates on a regular basis. You verify that Automatic Updates is running on all client computers, and you verify that users cannot modify the Automatic Updates settings.
You need to ensure that computers on your network receive all updates.
What should you do?

A. Enable the No auto-restart for scheduled Automatic Updates Installations settings.
B. Disable the Specify intranet Microsoft update service location setting.
C. Enable the Remove access to use all Windows Update features setting.
D. Enable the Reschedule Automatic Updates scheduled installations setting.

Answer: D

QUESTION 160:

You are a security administrator for Certkiller .com. The network consists of two Active Directory domains. These domains each belong to separate Active Directory forests. The domain Certkiller .com is used primarily to support company employees. The domain named bar.biz is used to support company customers. The functional level of all domains is Windows Server 2003 interim mode. A one-way external trust relationship exists in which the Certkiller .com domain trusts the bar.biz domain.
A Windows Server 2003 computer named Certkiller -SR25 is a member of the bar.biz domain. Certkiller -SR25 provides customers access to a Microsoft SQL Server 2000 database. The user accounts used by customers reside in the local account database on Certkiller -SR25. All the customer user accounts belong to a local computer group named Customers. SQL Server is configured to use Windows Integrated authentication.
Certkiller .com has additional SQL Server 2000 database that reside on three Windows Server 2003 computers. These computers are members of the Certkiller .com domain. The Certkiller .com written security policy states that customer user accounts must reside on computers in the bar.biz domain.

You need to plan a strategy for providing customers with access to the additional databases. You want to achieve this goal by using the minimal amount of administrative effort.
What should you do?

A. Create a new user account in the bar.biz Active Directory domain for each customer. Create a universal group in the bar.biz domain. Add the new customer domain user accounts as members of the new universal group. Assign this group permissions to access the databases.
B. Create a new user account in the bar.biz Active Directory domain for each customer. Create a global group in the bar.biz domain. Add the new customer domain user accounts as members of the new global group. Assign this group permissions to access the databases.
C. Create a new user account in the Certkiller .com Active Directory domain for each customer. Create a global group in the Certkiller .com domain. Add the new customer domain user accounts as members of the new global group. Assign this group permissions to access the databases.
D. Create a new user account in the Certkiller .com Active Directory domain for each customer. Create a global group in the Certkiller .com domain. Add the new customer domain user accounts as members of the new global group. Assign this group permissions to access the databases.

Answer: B

QUESTION 161:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The Certkiller .com domain contains Windows Server 2003 computers and Windows XP Professional client computers. All computers are members of the domain.
Certkiller .com uses a custom application to track help desk calls.
You receive a security bulletin that describes vulnerability in the customer application. To fix this vulnerability, you need to change a value in the user subtree of the registry for each user. Each user has only read permissions on the registry key that must be changed.
You need to ensure that the registry value is changed for each user the next time the user logs on to the network.
What should you do?

A. Create a script that changes the registry value. Assign the script as login script in the domain user account of all users.
B. Create a script that changes the registry value. Assign the script as user logon script in a Group Policy Object (GPO) that applies to all users.
C. Create a script that change the registry value. Assign the computer startup script in a GPO that applies to all client computers.
D. Add the registry value to the Administrative Template section of a GPO that applies to

all users.
E. Export the registry value to a registry file named appfix.reg. In the Startup group for each user, create a shortcut to the regedit.exe /s appfix.reg command.

Answer: D

QUESTION 162:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. Servers run either Windows Server 2003 or Windows 2000 Server. All client computers run Windows XP Professional.
The Certkiller .com written security policy states that user accounts must be locked if an unauthorized user attempts to guess the users' passwords.
The current account policy locks out a user after two invalid password attempts in five minutes. The user remains locked out until the account is reset by the administrator. Users frequently call the help desk to have their account unlocked.
Calls related to account lockout constitute 25 percent of help desk calls.
You need to reduce the number of help desk calls related to account lockout.
What should you do?

A. Modify the Default Domain Controllers Policy Group Policy object (GPO).
Increase the maximum lifetime for service tickets.
B. Modify the Default Domain Policy Group Policy object (GPO).
Configure an account lockout threshold of 10.
C. Modify the Default Domain Controllers Policy Group Policy object (GPO).
Disable the enforcement of user logon restrictions.
D. Modify the Default Domain Policy Group Policy object (GPO).
Increase the maximum password age.

Answer: B
Explanation
: Account Lockout Policy determines the circumstances and length of time that an account will be locked out of the system. Security Alert Enabling account lockout doesn't necessarily increase security. In fact, it actually creates a new vulnerability. An attacker who knows valid user names can guess incorrect passwords for users and lock legitimate users out, creating a denial-of-service attack.

QUESTION 163:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run either Windows XP Professional or Windows NT Workstation 4.0.
Certkiller .com's written security policy states that all users must acknowledge a legal message before they use any client computers.
You need to configure the network to ensure that all client computers comply with

the written security policy.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose TWO.)

A. Create a new GPO and link it to an OU. Configure the GPO to display the legal message. Place all Windows XP Professional computers in the OU.
B. Create a new GPO and link it to an OU. Configure the GPO to display the legal message. Place all Windows NT Workstation 4.0 computers in the OU.
C. Modify the Default Controllers Policy GPO by configuring it to display the legal message.
D. Create a Config.pol file that displays the legal message. Place the file in the SYSVOL shared folder.
E. Create a Config.pol file that displays the legal message. Place the file in the NETLOGIN shared folder.

Answer: A, E

QUESTION 164:

You are a security administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows 2000 Professional.
Certkiller 's written security policy states the following requirements:
1. All access to files must be audited.
2. File servers must be able to record all security events.
You create a new Group Policy object (GPO) and filter it to apply to only file servers. You configure an audit policy to audit files and folders on file servers. You configure a system access control list (SACL) to audit the appropriate files.
You need to ensure that the GPO enforces the written security policy.
Which two additional actions should you perform to configure the GPO? (Each correct answer presents part of the solution. Choose TWO.)

A. Set a manual retention method for the security log.
B. Set the security log to retain entries for 7 days.
C. Set the maximum security log size to the maximum allowed size.
D. Configure the GPO to shut down the computer of it is unable to log security audits.
E. Ensure that users who are responsible for reviewing audit log data are granted the right to manage the security log.

Answer: A, D

QUESTION 165:

You are a security administrator for Certkiller .com. All domain controllers run Windows Server 2003. All client computers run Windows XP Professional.
Certkiller .com has offices in Berlin, Bonn, Stuttgart, and Frankfurt.

The network consists of a single Active Directory forest that contains four domains. The domains are named berlin. Certkiller .com, bonn. Certkiller .com, stuttgart. Certkiller .com and frankfurt. Certkiller .com. Each city is configured as an Active Directory site. Each site contains file servers and client computers from every domain.
To comply with local laws, the Certkiller .com written security policy states that security events on file servers must be maintained as shown in the following table:

City	Presentation
Berlin	14 days
Bonn	28 days
Stuttgart	10 days
Frankfurt	31 days

You need to configure the network to comply with the written security policy. You want to achieve this goal by using the minimum amount of administrative effort. What should you do?

A. In each domain, create an OU for each of the other domains. Create a new GPO and link it to each OU. Configure each GPO to meet the requirements of the written security policy.
B. Create a GPO for each city and link each GPO to the corresponding site. Configure each GPO to meet the requirements of the written security policy.
C. Modify the Default Domain Policy GPO in each domain. Configure the GPO to meet the requirements of the written security policy.
D. Modify the Default Domain Controllers Policy GPO in each domain. Configure the GPO to meet the requirements of the written security policy.

Answer: B

Explanation: There are special Considerations for Site-linked GPOs - GPOs linked to sites might be appropriate to use for setting policy for proxy settings and network-related settings. Any GPO that is linked to a site container is applied to all computers in that site, regardless of which domain in the forest the computer belongs to. This has the following implications:
Ensure that the computers do not access a site Group Policy object across a WAN link, which would lead to significant performance issues.
By default, to manage site GPOs, you need to be either an Enterprise Admin, or the domain admin of the forest root domain.

QUESTION 166:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
Terminal Services is running on four Windows Server 2003 computers. Members of

a group named Remote Application need to access applications by using Terminal Services. You assigned the Remote Application group the appropriate NTFS permissions for the application folder and the appropriate RDP-Tcp connection permissions on the terminal servers. Currently no users have the right to connect to the terminal servers.
You need to assign users in the Remote Application group the minimum rights necessary to access the applications.
What should you do to configure the terminal servers?

A. Apply a security template that assigns the Access this computer from the network right to the Remote Application group.
B. Apply a security template that assigns the Allow log on locally right to the Remote Application group.
C. Apply a security template that assigns the Log on as a service right to the Remote Application group.
D. Apply a security template that assigns the Allow log on through Terminal Services right to the Remote Application group.

Answer: D

QUESTION 167:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003.
Certkiller .com provides remote access to the company network for domain users that work from home. Users create VPN connections to a remote access server named Certkiller -SR14. Certkiller -SR14 is a member server in the domain.
The authentication provider on the remote access server is Windows Authentication.
To minimize the risk of a dictionary attack on user password, you implemented a domain account lockout policy in Active Directory. You also configured remote access account lockout on Certkiller -SR14. The account lockout threshold in the domain and the maximum number of failed attempts on Certkiller -SR14 are both set to four invalid logon attempts. The account lockout counters in the domain are reset after one hour. The account lockout counters on Certkiller -SR14 are reset after two hours.
You receive reports that several users in the domain were prevented from logging on to the Certkiller .com network because invalid remote access login attempts locked the domain user accounts.
You need to ensure that invalid remote access logon attempts do not cause the domain user account to lock out. You do not want to disable the domain account lockout policy.
What should you do?

A. Configure the remote access service on Certkiller -SR14 to not accept the

MS-CHAP authentication method.
B. Configure the maximum number of failed attempts on Certkiller -SR14 to three invalid logon attempts.
C. Configure an account lockout policy in a GPO that is linked to the OU than contains Certkiller -SR14. Use an account lockout threshold of three.
D. Add Certkiller -SR14 computer account to the Windows Authorization Access Group security group.

Answer: B

Explanation:
Since domain lockout needs to be minimized, the best option is to allow the lockout to occur on the remote access server.

QUESTION 168:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
Several client computers are configured as kiosk computers that visitors and employees use. The kiosk computers are managed by using GPOs. The GPOs enforce a secure configuration. Multiple users log on to these computers every day.
You review the results of a security audit. You discover that when some users log on the secure configuration is removed.
You need to ensure that the secure configuration is enforced at all times.
What should you do?

A. Apply the Securews.inf security template to the kiosk computers.
B. Configure the default user profile on kiosk computers as a mandatory user profile.
C. Edit the GPO that manages kiosk computers. Disable the Secondary Logon service.
D. Edit the GPO that manages kiosk computers. Enable loopback processing.

Answer: D

QUESTION 169:

You are a security administrator for Certkiller .com. Certkiller .com has offices in New York, San Francisco, and Toronto. The network consists of a single Active Directory domain named Certkiller .com. Each office is configured as an Active Directory site. All servers run Windows Server 2003. All client computers run Windows XP Professional.
Users in the Toronto office work in the research department. User objects for users who work in the research department is stored in an organizational unit (OU) named Toronto. Users in other offices frequently travel to the Toronto office for meeting and training.
The Certkiller .com written security policy requires that the following settings be

enforced on computers at the Toronto office:
1. A warning message that reminds users to protect Certkiller .com information must be displayed before users log on.
2. Domain controller authentication is required when users unlock client computers.
3. The highest possible level of authentication must be used on the network at all times.
You create a new Group Policy object (GPO) named TorontoSecurity to meet the requirements of the written security policy.
Users who travel to the Toronto office report that they are not presented with the warning message and that their screen savers do not require a password to deactivate.
You need to ensure that the written security policy is enforced for other users only when they travel to the Toronto office. You want to achieve this goal by using the minimum amount of administrative effort.
What should you do?

A. Link the TorontoSecurity GPO to the Toronto OU.
B. Link the TorontoSecurity GPO to the domain.
C. Configure a logon script to apply a custom security template when users travel to the Toronto office.
D. Link the TorontoSecurity GPO to the Toronto site.

Answer: D

Explanation: GPOs linked to sites might be appropriate to use for setting policy for proxy settings and network-related settings. Any GPO that is linked to a site container is applied to all computers in that site, regardless of which domain in the forest the computer belongs to. This has the following implications: Ensure that the computers do not access a site Group Policy object across a WAN link, which would lead to significant performance issues. By default, to manage site GPOs, you need to be either an Enterprise Admin, or the domain admin of the forest root domain.

QUESTION 170:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The network contains Windows XP Professional client computers and Windows Server 2003 computers.
The domain contains three domain controllers. All domain controllers are in the Domain Controllers OU. A new password policy is defined in a security template named Certkiller .inf.
You need to implement the new password policy for domain accounts.
What should you do?

A. Import the Certkiller .inf security template into the Default Domain Policy GPO.
B. Import the Certkiller .inf security template into the Default Domain Controllers Policy GPO.

C. On each domain controller, import the Certkiller .inf security template into the local computer policy.
D. On each domain controller, import the Certkiller .inf security template into Security Configuration and Analysis, and then use the Configure Computer Now command.
E. On each domain controller, run the secedit /import Certkiller .inf command and then runt secedit /configure command.

Answer: B
Why import on the "Default Domain Policy's"? The question states that the new password policy has to be implemented for "domain accounts"!
The Domain accounts are all managed on the three domain controllers. So we need to import the inf-template only into the "Default Domain Controller Policy"!
When we would import the inf-template, with the password policy, into the "Default Domain Policy" also Client Computers would be affected and also local Computer-Accounts would get this new password policy, what's not stating in the question, only domain accounts.

QUESTION 171:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All domain controllers run Windows Server 2003. All domain controllers are in the same Active Directory site.
You want to implement a new auditing policy on the domain controllers. You also want to delegate the management of the auditing and security log on the domain controllers to members of a group named Auditors.
You create a new security template named Certkiller .inf. The Certkiller .Inf security template contains the new auditing policy settings and the user right settings to delegate the management of the auditing and security log. On a domain controller named Certkiller -DC03, you import the Certkiller .inf security template into Security Configuration and Analysis, and then use the Configure Computer Now command. Finally, you use the Analyze Computer now command to verify that the new settings are applied to Certkiller -DC03.
The next day, a member of the Auditors group reports that the new auditing policy settings and user right settings are not in effect on two of the domain controllers.
You need to ensure that the new auditing policy and user right settings are configured on all domain controllers.
What should you do?

A. On each domain controller, use the Configure Computer Now command to apply the Certkiller .inf security template.
B. On Certkiller -DC03, after you use the Analyze the Computer Now command, run the repadmin.exe /replicate /force command.
C. On Certkiller -DC03, after you use the Analyze the Computer Now command, run the gpudate.exe /force command.
D. On each domain controller, import the Certkiller .inf security template into the local computer policy.

E.
On Certkiller -DC03, import the Certkiller .inf security template into the Default Domain Controllers GPO.

Answer: E

QUESTION 172:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The network contains Windows XP Professional client computers and Windows Server 2003 computers only. All computers are members of the domain.
You need to test IPSec interoperability on your network. To do this, you create a new GPO named Certkiller IPSec. In the Certkiller IPSec GPO, you create an IPSec policy named Certkiller Test. The Certkiller Test policy contains a rule that specifies the use of Encapsulating Security Payload (ESP) with null encryption. The Certkiller Test policy is applied to all servers in the domain.
After all the tests are concluded, you need to ensure that the Certkiller Test policy is no longer used by the servers on the network.
What should you do?

A. In the domain, delete the Certkiller IPSec GPO.
B. In the Certkiller IPSec GPO, unassign the Certkiller Test policy.
C. On the servers, restart the IPSec services service.
D. On the servers, in the IP Security Policies, use the Restore Default Policies command.
E. On the servers, run the Netsh ipsec delete policy name = * Certkiller Test" command

Answer: B

QUESTION 173:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The network contains Windows XP Professional, Windows 2000 Professional, and Windows Server 2003 computers.
You discover that users in one domain can obtain a list of account names for users in the other domain. This capability allows unauthorized users to guess password and to access confidential data.
You need to ensure that account names can be obtained only by users of the domain in which the accounts reside.
Which two actions should you perform on the domain controllers? (Each correct answer presents part of the solution. Choose TWO.)

A. Apply a security template that disables the Network access: Allow anonymous SID/Name translation setting.
B. Apply a security template that disables the Network access: Do not allow anonymous enumeration of SAM accounts setting.

C. Apply a security template that disables the Network security: Do not store LAN Manager hash value on next password change setting.
D. Apply a security template that sets the Domain controller:LDAP server signing requirements setting to Require signing.

Answer: A, B

QUESTION 174:

You are a security administrator for Certkiller .com. Certkiller .com has one main office in Toronto and five branch offices in Boston, New York, Mexico City, Cape Town, and London respectively.
Network administrators work in the main office and each branch office. Network administrators in the main office frequently create scripts that automate common administrative tasks. You review each script to ensure it does not introduce security vulnerabilities. Scripts that do not introduce security vulnerabilities are considered approved.
Occasionally, branch office administrators modify these scripts and distribute the modified scripts to other branch office administrators. Branch office administrators often report that they accidentally run a modified version of a script.
You need to ensure that branch office administrators can verify which scripts are approved scripts.
What should you do?

A. Maintain a list of the dates the approved scripts were last modified. Instruct branch office administrators to verify the file modification date.
B. Digitally sign all approved scripts. Instruct branch office administrators to verify the signature before using a script.
C. Distribute all approved scripts to branch office administrators in an e-mail message.
D. Place all approved scripts on a file server in the main office. Assign all branch office administrators only the Allow - Read permission for the folder that contains the approved scripts. Instruct administrators to copy scripts from this file server.

Answer: B

QUESTION 175:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All servers are members of the domain.
Certkiller .com plans to deploy a new application named Ck_phtester1. The application runs on several servers. To test the compatibility between Ck_phtester1 and other applications that run on the servers, you need to change several file and registry permissions in the Windows folder on the servers. A security template named TestPerms contains the file and registry permissions that need to be set for the application testing.

You create a new Group Policy object (GPO) named TestApp. You import the TestPerms security template into the TestApp GPO. You link the TestApp GPO to an organizational unit (OU) that contains only the servers that are used for the test. You need to ensure that the file and registry permissions are set up to the permission in the TestPerms security template only during application testing. What should you do when the application testing ends?

A. Disable the computer configuration settings in the TestApp GPO.
B. Disable the TestApp GPO link to the OU.
C. Unlink the TestApp GPO from the OU.
D. Delete the TestApp GPO, and then run the gpupdate.exe /sync command.
E. Delete the TestApp GPO, and then apply a security template that contains the original permissions.

Answer: E

QUESTION 176:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
One hundred Certkiller .com users are currently using an application named Certkiller App. Certkiller App is stored in a folder on the hard disk of each user's client computer. To secure Certkiller App, you create a new GPO named Certkiller App Policy. The Certkiller App Policy GPO contains a file system security policy that applies a customer DACL to Certkiller App. You configure the DACL to assign all users only the Allow - Read permission. You filter the Certkiller App Policy GPO to apply only to computers that have Certkiller App installed.
After you apply the Certkiller App GPO, users immediately report that they receive an error message when they attempt to use Certkiller App. You delete the entry for Certkiller App in the file system security policy. Users continue to report that they receive the same error message when they attempt to use Certkiller App.
You need to configure the network so that users can use Certkiller App. You want to achieve this goal by using the minimum amount of administrative effort.
What should you do?

A. Delete the Certkiller App Policy GPO. Restart all client computers.
B. Create a new file system security policy in the Certkiller App Policy GPO that assigns default permissions to Certkiller App.
C. Import the Setup security.inf security template into the Certkiller App Policy GPO.
D. Disable the Certkiller App Policy GPO.

Answer: B

QUESTION 177:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain contains Windows Server 2003 domain controllers, Windows Server 2003 member servers, and Windows XP Professional client computers.
Currently, all employees use the local administrator account to log on to the member servers and client computers. The Certkiller .com written security policy states that only authorized network administration are allowed to log on by using the local administration account. The written security policy also states that passwords must be at last 12 characters long and that this requirement must be enforced at all times.
You create a GPO named Corporate Policy and link it to the domain. You configure the GPO to disable local administrator accounts and to require a password that consists of at least 12 characters.
The next day, you discover that the computer account for the client computer named Certkiller -WS299 was deleted. Users report they cannot log on to Certkiller -WS299. You create a new computer account to rejoin Certkiller -WS299 to the domain. You discover you cannot log on to Certkiller -WS299 as either the local administrator or the domain administrator.
You need to rejoin Certkiller -WS299 to the domain.
What should you do?

A. Disable the Corporate Policy GPO
B. Restart Certkiller -WS299 in Safe mode.
C. Reset the password for the local administrator account on Certkiller -WS299 to be at least 12 characters long.
D. Rename the local administrator account on Certkiller -WS299.
E. On Certkiller -WS299, on the Administrator Properties tab of the local administrator account, clear the Password never expires check box.

Answer: B

Explanation: Only the computer account has been deleted, only local policies apply and only local accounts or cached domain credentials can be used to logon. Since the question does not state that cached credentials are in use they cannot be used.
The CorporateGPO has disabled the local administrator account so the best solution to get this computer up and running is to use the Recovery Console using an ERD or perform a parallel install to delete the original SAM databases and restart the computer. Once restarted that SAM will be rebuilt to the default status and the local administrator account password would be blank. You could then change the machine from domain to workgroup and workgroup back to the domain and rejoin the computer to the domain.
If there were not ERD and the use of the Recovery Console is not possible, then a parallel install would have to be performed, then you could delete the original SAM database, restart the system and it will rebuild. This would set the local administrator's account to be active again and the password would be blank.
Three are also third party tools that would assist with this.
Restarting the computer in safe mode (B) would still require a local user account / local

administrator's account to logon. You must still be able to authenticate to the local SAM. Until you can logon to the computer, modifications are not possible.
The only modification possible is to disable the new GPO so that the original machine policies would apply.

QUESTION 178:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All domain controllers and servers run Windows Server 2003. All computers are members of the domain.
The domain contains 12 database servers. The database servers are in an organizational unit (OU) named DBServers. The domain controllers and the database servers are in the same Active Directory site.
You receive a security report that requires you to apply a security template named Lockdown.inf ti all database servers as quickly as possible. You import Lockdown.inf into a Group Policy object (GPO) that is linked to the DBServers OU.
You need to ensure that the settings in the Lockdown.info security template are applied to all database servers as quickly as possible.
What should you do?

A. On each database server, run the repadmin /replicate command.
B. On each database server, run the gpupdate command.
C. On each database server, run the secedit /refreshpolicy command.
D. On each database server, open Local Computer Policy, select Security Settings, and then use the Reload command.
E. On each database server, open Resultant Set of Policy, and then use the Refresh Query command.

Answer: B

Explanation: Using secedit /refreshpolicy option is no longer available with Windows 2003.
GpupdateRefreshes local and Active Directory-based Group Policy settings, including security settings. This command supersedes the now obsolete /refreshpolicy option for the secedit command.
Syntax: gpupdate [/target:{computer|user}] [/force] [/wait:value] [/logoff] [/boot]

QUESTION 179:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
You manage the network by using a combination of Group Policy objects (GPOs) and scripts. File names for scripts have the .vbs file name extension. Scripts are stored in a shared folder named Scripts on a server named Certkiller 1.
Users report that they accidentally run scripts that are received through e-mail and

the Internet. They further reports that these scripts cause problems with their client computers and often delete or change files. You discover that these scripts have .wsh, .wsf, .vbs, or .vbe file name extensions. You decide to use software restriction policies to prevent the use of unauthorized scripts.
You need to configure a software restriction policy for your network. You want to achieve this goal without affecting management of your network.
Which three rules should you include in your software restriction policy? (Each correct answer presents part of the solution. Choose THREE.)

A. A path rule that disallows *.vb? files.
B. A path rule that disallows *.ws? files.
C. A trusted sites rule that allows the local intranet zone.
D. A trusted sites rule that disallows the Internet zone.
E. A path rule that allows \\ Certkiller 1\scripts*.vb? files.

Answer: A, B, E

Explanation: By using the software restriction policy, you allow unknown code, which might contain viruses or code that conflicts with currently installed programs, to run only in a constrained environment (often called a sandbox) where it is disallowed from accessing any security-sensitive user privileges. For example, an e-mail attachment that contains a worm would be prohibited from automatically accessing your address book and therefore could not propagate itself. If the e-mail attachment contained a virus, the software restriction policy would restrict its ability to damage your system because it would be allowed to run only in a constrained environment.
If you create a path rule for a program with a security level of Disallowed, a user can still run the software by copying it to another location.
The wildcard characters that are supported by the path rule are the asterisk (*) and the question mark (?).
You can use environment variables, such as %programfiles% or %systemroot%, in your path rule.
To create a path rule for software when you do not know where it is stored on a computer but you have its registry key, you can create a registry path rule.
To prevent users from running e-mail attachments, you can create a path rule for your mail program's attachment folder that prevents users from running e-mail attachments.
The only file types that are affected by path rules are those that are listed in Designated file types. There is one list of designated file types that is shared by all rules.
For software restriction policies to take effect, users must update policy settings by logging off from and then logging on to their computers.
When more than one rule is applied to policy settings, there is a precedence of rules for handling conflicts.

QUESTION 180:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server

2003. All client computers run Windows XP Professional.
Certkiller .com occasionally experiences downtime because of malicious Internet worms that arrive as Microsoft Visual Basic scripting Edition (VBS) files.
You examine several client computers and discover that VBS files are downloaded by using Microsoft Outlook, instant messaging, or peer-to-peer file sharing programs.
You need to prevent users from running VBS files regardless of how they arrive on client computers.
What should you do?

A. Use a software restriction policy to disable all unauthorized scripts.
B. Use an Administrative Template to ensure that Outlook and Internet Explorer are in the Restricted Sites security zone.
C. Use a centralized login script to rename the Wscript.exe file on each computer to contain a nonexecutab le extension.
D. Use a file system security policy to assign the Deny - Execute permission for the Wscript.exe file.

Answer: A

QUESTION 181:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. One server named Certkiller -SR25 is not a member of the domain. The other servers are members of the domain.
The Certkiller .com written security policy states that all servers must have certain security settings, including specific event log settings and registry permissions settings. The required security settings are specified in a security template named Certkiller .inf.
You need to apply the settings from Certkiller .Info security template to Certkiller -SR25. You do not want to add Certkiller -SR25 to the domain.
What should you do?

A. On Certkiller -SR25, from the Administrative Tools menu, open Local Security Policy, and then use the Import Policy command to import Certkiller .inf.
B. On Certkiller -SR25, open Local Security Policy, and then select Security Settings. Use the Import Policy command to import Certkiller .inf.
C. On Certkiller -SR25, open Security Configuration and Analysis. Use the Import Template command to import Certkiller .inf, and then use the Configure Computer Now command.
D. On Certkiller -SR25, copy Certkiller .inf to the Systemroot\Security\Templates folder.
E. On Certkiller -SR25, copy Certkiller .inf to the Systemroot\System32\GroupPolicy\Machine folder.

Answer: C

QUESTION 182:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain contains Windows Server 2003 server computers. Twelve of these servers are configured as Web servers.
You need to produce a report that identifies which Microsoft security patches are not installed on the Web servers.
What should you do?

A. Run Gpresult.exe on the Web servers.
B. Run Mbsacli.exe on the Web servers.
C. Run Secedit.exe on the Web servers.
D. Run Qfecheck.exe on the Web servers.
E. Run Qchain.exe on the Web servers.

Answer: B

QUESTION 183:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory forest named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
Several client computers at Certkiller .com are kiosk computers and are in public locations. Certkiller .com's written security policy states the following requirements for the use of kiosk computers:
1. Users must use Remote Desktop Connection to connect to application servers and client computers
2. User can run only applications that are stored in the Windows and the Program Files folders.
3. Local administration can run any application.
You place all kiosk client computers in an OU named CKKiosk. You create a new GPO named CKPolicy, and you link the CKPolicy GPO to the CKKiosk OU. You create a software restrictions policy in the CKPolicy GPO.
You need to configure the software policy in the CKPolicy GPO.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose TWO.)

A. Change the default security level to disallowed.
B. Change the default enforcement policy to allow local administrators to run any application.
C. Create a certificate rule to allow all software signed by Microsoft.
D. Create a path rule to allow Remote Desktop Connection.

Answer: A, B

QUESTION 184:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
Some users in your company work from home offices. These users have client computers that are configured to use VPN connections to log on to the corporate domain. These computers are also members of the corporate domain. You configure these computers to use split tunneling when connecting to the corporate network.
You use Software Update Services (SUS) as part of your patch management strategy. You install SUS on a server named Certkiller -SR24. Certkiller -SR24 is part of the Certkiller .com network. You plan to review and approve security patches that meet Certkiller .com requirements on Certkiller -SR24. You configure a new GPO and filter the GPO to apply to computers used in home offices.
You need to ensure that home office computers have the latest approved security patches. You want to achieve this goal while minimizing the amount of traffic on the corporate network and by using the least amount of administrative effort.
What should you do?

A. Configure the GPO to automatically install security patches from the Windows Update Web site.
B. Configure the GPO to disable Automatic updated. E-mail approved security patches to home office users.
C. Configure the GPO to download security patches to Certkiller -SR24. Configure Certkiller -SR24 to redirect clients to the Windows Update Web site.
D. Configure the GPO to download security patches to Certkiller -SR24. Configure Certkiller -SR24 to download and store security patches locally.

Answer: C

QUESTION 185:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional. All computers are members of the domain.
The network contains 10 Active Directory sites. Each site represents one of the company's offices. The offices are located around the world. Each office has a connection to the Internet. Certkiller .com maintains dedicated leases lines between the offices.
You are planning a security patch management infrastructure for Microsoft security patches. You install Software Update Services (SUS) on a server named Certkiller -SR29.

You need to ensure that Automatic Updates on the client computers and servers installs only security patches that are company approved. You want to limit the use of the leased line between the offices by allowing each computer to download security patches from the Internet.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose TWO.)

A. Configure Automatic Updates on all computers to use the Microsoft Windows Update servers.
B. Configure Automatic Updates on all computers to use SUS on Certkiller -SR29.
C. Copy the Approveditems.txt file from Certkiller -SR29 to the Windows folder on each computer.
D. Configure Certkiller -SR29 to maintain updates on the Microsoft Windows Update Servers.
E. Use Group Policy to configure the SUS server location as the URL of the Microsoft Windows Update Web site on all computers.
F. On all computers, configure the value of the Run key in the registry as the URL of the Microsoft Windows Update Web site.

Answer: B, D

QUESTION 186:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional. All computers are members of the domain.
Certkiller .com has a main office and six branch offices. Each branch office is connected to the main office by a dedicated leased line. All offices are connected to the Internet. Each office contains multiple servers and hundreds of client computers.
You are planning a security patch management infrastructure. You install a Software Update Services (SUS) server in the main office and in each branch office. You configure the main office SUS server to store updates locally.
You need to ensure that all client computers automatically install the latest security patches. You want to minimize the network traffic on the leased lines between the offices and on the connections to the Internet.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose TWO.)

A. Configure the branch office SUS servers to maintain updates on the Microsoft Windows Update servers.
B. Configure Automatic Updates on the branch office SUS servers to use the main office SUS server.
C. Configure the branch office SUS servers to obtain updates from the main office SUS server.

D. Configure Automatic Updates on the client computers to use the SUS server in the local office.
E. Configure Automatic Updates on the client computers to use the main office SUS server.

Answer: C, D

Explanation: SUS is designed to be used in large organizations. Almost every aspect of the behavior can be customized. For example, the SUS server can download updates from Microsoft automatically, manually, or on a schedule specified by an administrator. SUS servers can be tiered with multiple SUS servers synchronizing updates between each other. This optimizes the use of your Internet connection by only requiring each update to be downloaded once for the entire organization. It also optimizes traffic on your wide area networks by allowing clients to download updates from a local SUS server.

QUESTION 187:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run either Windows XP Professional or Windows 2000 Professional.
You decide to use Software Update Services (SUS) as part of your patch management strategy.
You need to test all software updates on test computers before you distribute the updates to your entire production network. You want to achieve this goal by using the minimum amount of administrative effort while ensuring that all computers receive updates on a regular basis.
What should you do?

A. Deploy one SUS server. On test computers, configure Automatic Updates to install updates without user involvement. On production computers, configure Automatic Updates to ask for user approval before installing updates. Send out global e-mail that users when it is safe to apply new updates to production computers.
B. Deploy one SUS server. On test and production computers, configure Automatic Updates to install updates without user involvement. Use Group Policy to enable or disable Automatic Updates on production computers according to results from the test computers.
C. Deploy two SUS servers. Configure one server to the test computers and one server for the production computers. Configure the test computers to use the test SUS server for updates. Configure the production computers to use the production SUS server for updates.
D. Deploy two SUS servers. Configure one server to the test computers and one server for the production computers. Configure the test computers to use the test SUS server for updates. Configure the production computers to use the production SUS server for updates. Use Group Policy to enable to disable Automatic Updates on the production computers according to results from the test computers.

Answer: C

Explanation: You need to set up two SUS servers-let's call them SUSTest and SUSProd. Configure your production computers to pull their updates from SUSProd by editing an appropriate Group Policy Object (GPO) that you apply to all your production computers; maneuvering to Computer Configuration, Administrative Templates, Windows Components, Windows Update; and entering SUSProd as the Set intranet update service for detecting updates option. Next, create another GPO, link it to your test computers, and enter SUSTest as the Set intranet update service for detecting updates option. To test an update, simply approve it on SUSTest and all your test computers will install it. After you're satisfied that the update is safe for wider deployment, log on to SUSProd and approve the update.
To reduce the likelihood of errors (e.g., accidentally approving the update in SUSProd before you approve it in SUSTest), you can create separate user accounts such as SUSTestAdmin and SUSProdAdmin and place each user in the local Administrators group on the corresponding SUS server. Let's hope that Microsoft will enhance SUS so that you can manage both your test and production environments from one SUS server and that you can someday use SUS to require that an update be approved in the test environment before you can approve it in production. But, for now, the dual SUS server method isn't a bad solution. If you need to approve different updates for different types of computers (e.g., servers, workstations, domain controllers-DCs) in your production environment, you need to set up different SUS servers for each of type of system and configure those systems to pull updates from their corresponding SUS servers.

QUESTION 188:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003.
The Certkiller .com written security policy states that security patches must be manually installed on servers by administrators.
You need to configure the network to comply with the written security policy. You need to maintain security patches by using the minimum amount of administrative effort.
What should you do?

A. Create a new organizational unit (OU) to contain all server computers.
Create a new Group Policy object (GPO) and link it to the OU.
Configure the GPO to disable Automatic Updates.
Allow only administrators to start Automatic Updates.
B. Create a new organizational unit (OU) to contain all server computers.
Create a new Group Policy object (GPO) and link it to the OU.
Configure the GPO to automatically download updates and notify when they are ready to be installed.

C. Create a new organizational unit (OU) named Admins to contain all administrators.
Create a second OU named Servers to contain all server computers.
Create a new Group Policy object (GPO) and link it to the Admins OU.
Configure the GPO to disable Automatic Updates.
D. Modify the Default Domain Policy Group Policy object (GPO) to disable Windows Update and to disable Automatic Updates.
Create a new organizational unit (OU) named Admins.
Place all administrator accounts in the Admins OU.
Block GPO inheritance on the Admins OU.

Answer: B

Explanation: The correct syntax is mbsacli /hf -i hosts.txt syntax. The -i flag is used to scan one or more Internet Protocol (IP) addresses.
The mbsacli /hf -fh hosts.txt. The -fh flag causes the tool to scan the NetBIOS computer names specified in the named text file. You must specify one computer name on each line in the .txt file, up to a maximum of 256 names.
The mbsacli /hf -r hosts.txt syntax. The -r flag is used to specify a range of IP addresses to be scanned.
Incorrect Answers:
A: Cannot be done using Network Neighborhood.
C: Scanning the finance subnet would report on all computers on the subnet, including non-finance computers.
D: This option again would scan all systems in the domain, not just the finance once. The scan should be done from an administrative machine, not a users' machine.

QUESTION 189:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows 2000 Professional.
You regularly install security patches on Windows Server 2003 computers.
You need to create a plan to restore computers to their original state if a security patch causes unwanted results.
Which action should you perform first?

A. Create a Recovery Console on the computer before you install the security patch.
B. Create a mirrored volume on the computer before you install the security patch.
C. Create a RAID 5 disk on the computer before you install the security patch.
D. Create a script that runs the patch file with uninstall option.

Answer: D

Explanation:
Standard Installer Command Line Options [Windows Installer]

The executable program that interprets packages and installs products is Msiexec.exe. Note Msiexec also sets an error level on return that corresponds to system error codes.

QUESTION 190:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The Certkiller .com Active Directory domain contains 150 Windows Server 2003 computers and 7,500 Windows XP Professional client computers. The network is made up of 64 class C IP subnets t hat range from 172.16.0.0 through 172.16.63.0.
The finance department uses 135 computers on the 172.16.9.0 /24 IP subnet. This subnet also contains computers that belong to other departments in the company.
All finance department computers are members of the Certkiller .com Active Directory domain.
You need to produce a report that identifies which Microsoft security patches are not installed on the computers in the finance department. The report must contain information about only the finance department computers. You want to achieve this goal by using the minimum amount of administrative effort.
What should you do?

A. Run Mbsacli.exe on a finance department computer with the option to scan computers in the Network Neighborhood.
B. Run Mbsacli.exe on a finance department computer with the option to scan computers by using a list of individual IP addresses on the finance department computers.
C. Run Mbsacli.exe on a finance department computer with the option to scan computers on the finance department IP subnet.
D. Run Mbsacli.exe on a finance department computer with the option to scan computers in the Certkiller .com Active Directory domain.

Answer: B

Explanation: Since there are non-accounting computers on the subnet, the scan needs to be performed by individual IP.
The correct syntax is mbsacli /hf -fh hosts.txt. The -fh flag causes the tool to scan the NetBIOS computer names specified in the named text file. You must specify one computer name on each line in the .txt file, up to a maximum of 256 names.
You should not use the mbsacli /hf -i hosts.txt syntax. The -i flag is used to scan one or more Internet Protocol (IP) addresses.
You should not use the mbsacli /hf -r hosts.txt syntax. The -r flag is used to specify a range of IP addresses to be scanned.
Reference:
Microsoft Baseline Security Analyzer (MBSA) version 1.2 is available, Microsoft Knowledge Base Article - 320454

QUESTION 191:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The servers on the network runs Windows Server 2003 and all servers are members of the domain.
You plan to deploy a new service pack for Windows Server 2003 on existing servers.
You install Software Update Services (SUS) on a server named Certkiller -SR23.
You need to deploy the new service pack to the servers in a group named TestServers before you deploy the service to all servers.
What should you do?

A. Slipstream the service pack files into the Windows folder on the servers in the TestServers group.
B. Copy the service pack executable file to Certkiller -SR23. Configure read permission on the file for only the TestServers group.
C. Copy the service pack executable file to a new SUS server. Configure Automatic Updates on the servers in the Test Servers group to use the new SUS server.
D. Create a new GPO to deploy the service pack. Filter the GPO so that it applies to only the TestServers group.

Answer: D

QUESTION 192:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The Certkiller .com domain contains Windows Server 2003 computers and Windows XP Professional client computers.
All computers are members of the domain, except a server named Certkiller -SR15.
The network contains an enterprise certification authority (CA). All computers on the network trust the CA.
The Certkiller .com written security policy states that all network traffic from the computers in the domain to Certkiller -SR15 must be encrypted.
Certkiller -SR15 must not be added to the domain.
You configure a GPO that assigns the predefined IPSec policy named Client (Respond Only). You link the GPO to the domain. You configure Certkiller -SR15 to use the predefined IPSec policy named Secure Server (Require Security).
When you test this configuration, you cannot connect to Certkiller -SR15 from the computers in the domain.
When need to implement the written security policy.
What should you do?

A. Disable the default exemptions to IPSec filtering on all computers in the domain.
B. Disable the default response rule in the Client (Respond Only) IPSec policy in the domain.
C. Configure Certkiller -SR15 so that it uses the predefined IPSec policy named Server (Request Security).
D. Configure the security options of the local computer policy on Certkiller -SR15 to

always digitally sign communications.
E. Configure the assigned IPSec policies on Certkiller -SR15 and in the domain to use certificate-based authentication.

Answer: E

Explanation: When you use IPSec certificate-based authentication, you limit authentication to certificates from a specific CA. Therefore, you need to use a dedicated Enterprise CA for each IPSec policy you plan to configure. You can use an existing Enterprise CA, so long as you don't need to issue IPSec certificates from that CA for other reasons. If you don't have an existing CA that you can use for this purpose, install Certificate Services on any Windows 2000 Server that's a member of your Active Directory domain.
Reference:
www.winnetmag.com/WindowsSecurity/ Article/ArticleID/26112/26112.html

---

QUESTION 193:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
The network contains an enterprise certificate authority (CA). The CA is trusted by all computers.
One segment of the Certkiller .com network is behind a device that performs Network Address Translation (NAT) and is used as a test network. The rest of the network is the production network. The computers on the test network are not members of the domain. The computers on the production network are members of the domain. The NAT device supports both TCP and UDP address translation.
Users on the test network are allowed to connect to servers on the production network.
You need to ensure that FTP traffic and e-mail traffic from computers on the test network to FTP servers and mail servers on the production network is encrypted.
For monitoring reasons, all other network traffic to those servers must not be encrypted.
What should you do?

A. Implement an IPSec policy that uses Encapsulating Security Payload (ESP) rules in Transport mode.
B. Implement an IPSec policy that uses Encapsulating Security Payload (ESP) rules in Tunnel mode.
C. Implement an IPSec policy that uses only IPSec Authentication Header (AH).
D. Implement an IPSec policy that uses Kerberos authentication.

Answer: A

Explanation: Transport mode is the default mode for IPSec, and it is used for

end-to-end communications (for example, for communications between a client and a server). When transport mode is used, IPSec encrypts only the IP payload. Encapsulating Security Payload (ESP) provides confidentiality (in addition to authentication, integrity, and anti-replay protection) for the IP payload. ESP in transport mode does not sign the entire packet. Only the IP payload (not the IP header) is protected. ESP can be used alone or in combination with AH.

QUESTION 194:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
Certkiller .com uses an accounting and payroll application. Twenty payroll clerks use the application to input data from their client computers to a database running on a Microsoft SQL Server 2000 computer named Certkiller 6.
You need to prevent unauthorized interception of the data as it travels over the company network.
What are two possible ways to achieve this goal? (Each correct answer is a complete solution. Choose TWO.)

A. Configure SQL Server 2000 on Certkiller 6 to use SSL.
B. Configure an IPSec policy to require Authentication Headers (Ahs) between the payroll client computers and Certkiller 6.
C. Configure an IPSec policy Encapsulating Security Payload (ESP) between the payroll client computers on Certkiller 6.
D. Configure Certkiller 6 to require Server Message Block (SMB) signing.

Answer: A, C

QUESTION 195:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. Server runs either Windows Server 2003 or Windows 2000 Server. All client computers run Windows 2000 Professional. The latest operating system service packs is installed on each computer.
Thirty Windows Server 2003 computers are members of the domain and functions as file servers. Client computers access files on these file servers over the network by using the Server Message Block (SMB) protocol. You are concerned about the possible occurrence of man-in-the-middle attacks during SMB communications.
You need to ensure that SMB communications between the Windows Server 2003 file servers and the client computers are cryptographically signed. The file servers must not communicate with client computers if the client computers cannot sign SMB communications. Client computers must be able to use unsigned SMB communications with all other computers in the domain.
What should you do to configure the file servers?

A. Apply a security template that enables the Microsoft network server:Digitally sign communications (always) setting.
B. Apply a security template that enables the Microsoft network server:Digitally sign communications (if client aggrees) setting.
C. Apply a security template that enables the Domain member:Digitally sign secure channel data (when possible) setting.
D. Apply a security template that enables the Domain member:Digitally encrypt or sign secure channel data (always) setting.

Answer: A

QUESTION 196:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The network contains Windows Server 2003 computers and Windows XP Professional client computers.
You install Certificate Services on two Windows Server 2003 computers named Certkiller -SR11 and Certkiller -SR12. Certkiller -SR11 is the root certification authority (CA) and Certkiller -SR12 is the subordinate CA. You configure the root CA certificate with a validity period of eight years. You configure the subordinate CA certificate with a validity period of two years.
You create a custom User certificate type that has a validity period of three years.
You allow employees to enroll for this user certificate by using Certkiller -SR12.
You discover that all issued certificates do not remain valid for three years as expected.
You need to ensure that the custom User certificates are issued with validity period of three years.
What should you do?

A. Generate a new CA certificate for Certkiller -SR11 with a validity period of three years.
B. Generate a new CA certificate for Certkiller -SR12 with a validity period of four years.
C. Create a new custom User certificate type with a validity period of four years.
D. Create a new custom Administration certificate type with a validity period of three years.

Answer: B

Explanation: Certificates are enabled for a specific length of time, which is the validity period. This time is expressed in a length of time beginning from when a certificate is issued. When that length of time is reached, the certificate is no longer valid and cannot be trusted. Because an expired certificate can cause problems, certificates can be renewed to extend their validity period.

QUESTION 197:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
Certkiller .com hosts Web applications for customers. Each customer is a company that has multiple employees who require access to the Web applications. Each customer has one Web application. Each Web application is configured as a virtual directory. The virtual directory is configured to require 128-bit encryption, the client certificates configured to Require Client Certificates, and the Client Certificate Mapping is enabled.
Many-to-one certificate mapping is configured to authenticate users that attempt to access the virtual directory. Customers request certificates from private and public certification authorities (CAs).
You discover that unauthorized users accessed Web application by using certificates that were issued by CAs that are not authorized to issue certificates to customers.
You need to ensure that only authorized employees can access their company's Web application.
What should do?

A. Configure each Web application to use a certificate trust list (CTL). Include only CAs that you trust to issue certificates to customers in the CTL.
B. Create a new enterprise subordinate CA that uses qualified subordination. Issue Client Authentication certificates for each employee of each customer that requires access to the Web application.
C. Create a new enterprise subordinate CA. Cross certify the new enterprise subordinate CA with each CA that you trust to issue certificates to customers.
D. Configure the Web server to enable the Windows directory services mapper.

Answer: D

QUESTION 198:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003.
Certkiller .com uses the Internet to sell products. Customers place and view the status by using a Web application named Certkiller App3. Certkiller App3 is hosted on a Windows Server 2003 computer that runs IIS. Users access Certkiller App3 by using various Web browsers. You configure SSL for connections to Certkiller App3.
The Certkiller .com written security policy state the following requirements:
1. All users must enter a user name and password when they access Certkiller App3.
2. All users must use the same authentication method.
3. All users must use credentials in the Certkiller .com domain.
You need to configure IIS to support the required authentication.
What should you do?

A. Enable Digest authentication for Windows domain servers.
B. Enable .NET passport authentication.
C. Enable Basic authentication (password is sent in clear text).
D. Enable Integrated Windows authentication.

Answer: C

Explanation: Basic authentication. This authentication method prompts the user for a user name and a password, also called credentials, which are sent unencrypted over the network.
Incorrect Answers:
A: The Digest authentication method operates much like Basic authentication, except that passwords are sent across the network as a hash value for additional security. Digest authentication is available only on domains with domain controllers running Windows server operating systems.
B: The .NET Passport-enabled sites rely on the .NET Passport central server to authenticate users; .NET Passport-enabled sites do not host and maintain their own proprietary authentication systems.
D: The Integrated Windows authentication method uses hashing technology to scramble user names and passwords before sending them over the network.
Reference:
http://support.microsoft.com/default.aspx?scid=kb;en-us;313251
http://support.microsoft.com/default.aspx?scid=kb;en-us;299875

QUESTION 199:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The network includes a public key infrastructure (PKI) that support smart card logon. All client computers have smart card readers. Managers are issued smart cards. Managers are required to use smart cards when logging on to the client computers.
You need to ensure that managers are required to use a smart card when logging on to any client computer and that all other users are required to use a smart card when logging on to a client computer assigned to a manager.
Which two actions should you perform? (Each correct answer is a part of the solution. Choose TWO.)

A. On the properties of each user account used by a manager, select the Smart card required for Interactive logon check box.
B. On the computer account for each manager's client computer, edit the DACL so that only managers are assigned the Allow - Allowed to authenticate permission.
C. Place all client computers used by managers in an OU. Link a new GPO to the OU. Configure the GPO to enforce the Interactive logon:Require smart card setting.
D. Place all client computers used by managers in an OU. Link a new GPO to the OU. Configure the GPO to set the startup type of the Smard Card service to Automatic.

Answer: A, C

Explanation: Several Group Policy settings are specific to smart card management. You can use these Group Policy settings to manage smart cards in your organization.
Other security policy settings, such as lockout policy or restricted logon times, can also impact smart card users if they use their cards for account logon.
Smart card required for interactive logon - When you set this policy on a user account, the user cannot log on to the account by using a password. They can only log on by using a smart card. The advantage of using this policy setting is that it enforces strict security. However, if users are unable to log on by using conventional passwords, you must provide an alternate solution in the event that smart cards become unusable.

QUESTION 200:

You are the security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. Servers on the network run Windows Server 2003. All computers are in the domain.
You enable Remote Desktop for Administration on a member server named Certkiller -SR21.
You want to allow members of a domain global group named Server Managers to create a Remote Desktop connection to Certkiller -SR21. The members of the Server Managers group are not in the Administrators group on Certkiller -SR21.
What should you do?

A. Grant the Server Managers group Read permission on the Terminal Services service.
B. Grant the Server Managers group Connect permission on the RDP-Tcp connection.
C. Assign the Allow log on locally right to the Server Managers group.
D. Add the Server Managers group to the Remote Desktop Users group.

Answer: D

Explanation: By default, the Remote Desktop Users group is not populated. You must decide which users and groups should have permission to log on remotely, and then manually add them to the group.
To open Computer Management, click Start, and then click Control Panel. Click Performance and Maintenance, click Administrative Tools, and then double-click Computer Management.

QUESTION 201:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The network contains Windows XP Professional client computers and Windows Server 2003 computers. The network also consists of a public key infrastructure (PKI) that supports smart card

authentication.
The Certkiller .com written security policy states the following network administration requirements:
1. All domain controllers must be stored in a restricted location. Only Server Administration Staff are permitted to access this location.
2. All Directory Services Administration staff must use a smart card when performing administrative tasks interactively on domain controllers.
3. All administration of domain controllers that is performed remotely must be protected by encryption.
To comply with the written security policy, you move all domain controllers to a secure server room and provide only Server Administration staff with access to the server room. You create an additional account for each member of the Directory Services Administration staff. You configure the new accounts to require a smart card during authentication.
You need to ensure that Directory Services Administration staff is able to administer domain controllers. You must achieve this goal without violating the written security policy.
What should you do?

A. Configure a smart card reader on the client computer of each Directory Services Administration staff member. Instruct Directory Services Administration staff to connect to domain controllers using a Remote Desktop connection.
B. Configure a smart card reader on each domain controller. Instruct Directory Services Administration staff to use the runas command to open a Telnet session when administering domain controllers.
C. Create a customer Microsoft Management Console (MMC). Include all snap-ins required by Directory Services Administration staff. Instruct Directory Services Administration staff to use the runas command to open the customer MMC.
D. Install IIS on one domain controller. Include the remote administration components. Configure IIS to require HTTPS connections. Instruct administrators to connect to the remote administration Web site on the IIS server.

Answer: A

QUESTION 202:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003.
You plan to deploy remote access to the network for users that work from home, including users who are member of a group named Certkiller Staff. All members of the Certkiller Staff group are in the Domain Users group.
The Certkiller .com written security policy states the following remote access requirements:
1. Users, except member of the Certkiller Staff group, are allowed to use remote access at any tome for an unlimited duration.

2. Members of the Certkiller Staff group are allowed to use remote access during the day only for a maximum of 30 minutes.
You configure and enable Routing and Remote Access on a member server named Certkiller -SR25. You delete the predefined remote access policy. The remote access permission for all user accounts in the domain is set to use remote access policies. Now you need to apply the appropriate Remote Access policies in the correct order so as to comply with the Certkiller .com written security policy.
Following are the Remote Access Policies:
1. Domain Users - Deny - 30 minutes
2. Domain Users - Grant - 30 minutes
3. Domain Users/During day - Grant - Unlimited
4. Certkiller Staff - Deny - Unlimited
5. Certkiller Staff/During day - Grant - 30 minutes.
You need to make a decision on how to apply these remote access policies.
What should you do?

A. You should apply the remote access policies as follows:
first - Certkiller Staff/During day - Grant - 30 minutes
second - TestingStaff - Deny - Unlimited
third - Domain Users - Grant - 30 minutes
B. You should apply the remote access policies as follows:
first - Certkiller Staff/During day - Grant - 30 minutes
second - TestingStaff - Deny - Unlimited
third - Domain Users - Deny - 30 minutes
C. You should apply the remote access policies as follows:
first - Certkiller Staff/During day - Grant - 30 minutes
second - Certkiller Staff - Deny - Unlimited
third - Domain Users/During day - Grant - Unlimited
D. You should apply the remote access policies as follows:
first - Domain Users - Grant - 30 minutes
second - CertK tingStaff - Deny - Unlimited
third - Domain Users/During day - Grant - Unlimited

Answer: C

Explanation: The remote access polices are tried in order. The more specific remote access policies are placed in order ahead of the more general remote access policies. If the first policy in the ordered list of remote access policies does not match the connection attempt, the next policy is tried.

QUESTION 203:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003.
You plan to deploy remote access to the network for users that work from home.

The Certkiller .com written security policy states the following remote access requirements:
1. Users are allowed to use remote access during the day only.
2. Enterprise Admins are never allowed to use remote access.
3. Domain Admins are always allowed to use remote access.
4. A user who is a member of both the Enterprise Admins group and the Domains Admins group is not allowed to use remote access.
You configure and enable Routing and Remote Access on a member server named Certkiller 1. You delete the predefined remote access polices. The remote access permission for all user accounts in the domains is set to use remote access polices.
You must apply the appropriate Remote Access polices in the correct order so as to comply with the Certkiller .com written security policy.
Following are the Remote Access Polices:
1. Domain Users/during day - Allow access
2. Domain Users/during night - Deny access
3. Domain Admins/all times - Allow Access
4. Enterprise Admins/all times - Deny access
5. Enterprise Admins/during day - Deny access
You need to ensure that the remote access polices on Certkiller 1 comply with the written security policy and thus need to make a decision on how to apply these remote access polices.
What should you do?

A. You should apply the remote access policies as follows:
first - Enterprise Admins/during day - Deny access
second - Domain Admins/all times - Allow Access
third - Domain Users/during day - Allow access
B. You should apply the remote access policies as follows:
first - Enterprise Admins/ during day - Deny access
second - Domain Admins/all times - Allow Access
third - Domain Users/during day - Allow access
C. You should apply the remote access policies as follows:
first - Enterprise Admins/all times - Deny access
second - Domain Admins/all times - Allow Access
third - Domain Users/ during night - Deny access
D. You should apply the remote access policies as follows:
first - Enterprise Admins/all times - Deny access
second - Domain Admins/all times - Allow Access
third - Domain Users/during day - Allow access

Answer: D

Explanation: The remote access polices are tried in order. The more specific remote access policies are placed in order ahead of the more general remote access policies. If the first policy in the ordered list of remote access policies does not match the connection attempt, the next policy is tried.

The most specific policy is Enterprise Admins/all times Deny access, so it should be placed first.
The next most specific policy is Domain Admins/all times Allow access. This policy should be placed second.
The most general remote access policy is Domain Users/during day - Allow Access. This policy should be placed last.
The reason for this is that everyone by default is part of the Domain Users group. If this was first or second, Enterprise Admins would be allowed to connect and Domain Admins would only be able to connect during the day.

QUESTION 204:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
Certkiller .com hosts an extranet Web site that allows employees from a partner company to access confidential information over the Internet. You want to require the partner company employees to use certificate-based authentication to access the extranet Web site.
You have a public key infrastructure (PKI), which consists of a stand-alone root certification authority (CA) and an enterprise subordinate C
A. The partner
company does not have a PKI.
You decide to issue certificates from your CA hierarchy to the partner company employees. The partner company certificates will require a different certificate policy than the policy currently used for issuing certificates to internal employees. Certificate revocation checking will be used during certificate-based authentication.
You need to implement the necessary PKI changes to comply with these requirements. You want to achieve this goal by using the minimum amount of administrative effort.
Which three actions should you perform? (Each correct answer presents part of the solution. Choose THREE.)

A. Use a new subordinate CA in your CA hierarchy to issue certificates to partner company employees and to the extranet Web server.
B. Use the eixisting subordinate CA in your CA hierarchy to issue certificates to partner company employees and to the extranet Web server.
C. Add the certificate of the root CA to the Trusted Root Certification Authorities store on the partner company's computers.
D. Add the certificate of the subordinate CA to the Trusted Root Certification Authorities store on the partner company's computers.
E. Create new HTTP Authority Information Access (AIA) paths and certificate revocation list (CRL) distribution points that specify locations on the extranet Web site.
F. Create new LDAP Authority Information Access (AIA) paths and certificate revocation list (CRL) distribution points that specify locations on the extranet Web site.

Answer: A, C, E

QUESTION 205:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The domain contains Windows Server 2003 computers. You manage a Windows Server 2003 computer named Certkiller -SR26 that is a domain member server. You use IIS on Certkiller -SR26 to host an Internet Web site. This web site published information to employees of a partner company.
The partner company network consists of a single Active Directory domain. Approximately 500 partner company employees connect over the Internet to access company confidential data on Certkiller -SR26. All partner company employees need access to the same data.
The partner company IT department maintains a certificate authority (CA). They use this CA to issue Authentication Session certificates to all employees in their company. Copies of these certificates are stored with employee user accounts in the partner company's Active Directory domain.
You need to authenticate users to Certkiller -SR26 based on possession of their company-issued certificate. You want to achieve this goal by using the minimum amount of administrative effort. You enable SSL and the certificate-based authentication option on Certkiller -SR26. You add the partner root CA certificate to the Trusted Root Certification Authorities store on Certkiller -SR26.
Which three additional actions you perform? (Each correct answer presents part of the solution. Choose THREE.)

A. Create a security group named PartnerEmployees and a user account named PartnerUser in your Active Directory domain. Add this account to the PartnerEmployees group.
B. Create a security group named PartnerEmployees and a user account for every partner company employee in your Active Directory domain. Add these accounts to the PartnerEmployees group.
C. Assign the PartnerEmployees group access to the appropriate data on Certkiller -SR26.
D. Add a many-to-one certificate mapping in ISS on Certkiller -SR26. Create a mapping rule to accept certificates issued by the partner company's internal CA.
E. Add one-to-one certificate mappings for every partner employee in IIS on Certkiller -SR26.

Answer: A, C, D
Note: Many-to-one certificate mapping uses wildcard matching rules that verify whether a client certificate contains specific information, such as the issuer or subject.

QUESTION 206:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The network contains Windows XP Professional client computers and Windows Server 2003 computers only.
You manage a Windows Server 2003 computer named Certkiller -SR12 that is a domain member server. You use IIS on Certkiller -SR12 to host an Internet Web site. Approximately 4,000 Certkiller .com employees connect over the Internet to access company confidential data on Certkiller -SR12. You control access to data on Certkiller -SR12 by using NTFS file permissions assigned to groups. Different groups are assigned access to different files. Employees must have access only to files that they are assigned access to, based on their membership in a group.
You enable SSL on Certkiller -SR12 to protect confidential data while it is in transit. You issue each employee an Authenticated Session certificate and store a copy of that certificate with their user account in the Active Directory domain.
You need ensure that Certkiller -SR12 authenticates users based on possession of their certificate.
What should you do?

A. Request a Web server certificate from a commercial certification authority (CA).
B. Configure access restrictions based on employee IP address.
C. Enable Digest authentication for Windows domain servers.
D. Configure client certificate mapping.

Answer: D

QUESTION 207:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.
Certkiller .com uses a Web application named Certkiller App. Certkiller App is hosted on a web server named Certkiller -SR29. Only managers who have accounts on the internal network use Certkiller App. Managers are members of a global group named Certkiller Managers. Only Certkiller Managers has access to Certkiller App.
You need to ensure that only managers can access Certkiller App and that managers are required to enter their user name and password as seldom as possible.
You need to configure IIS to support the required authentication.
What should you do?

A. Enable .NET passport authentication.
B. Enable Basic authentication (password is sent in clear text).
C. Enable Digest authentication for Windows domain servers.
D. Enable Integrated Windows authentication.

Answer: D

Explanation:

Integrated Windows authentication, and only Integrated Windows authentication, meets the requirements of this scenario. Since only managers are allowed to access and are members of the domain, they are already authenticated to the domain. Integrated authentication will simply accept the user credential used from the client workstation.
Incorrect Answers:
A: The .NET Passport-enabled sites rely on the .NET Passport central server to authenticate users; .NET Passport-enabled sites do not host and maintain their own proprietary authentication systems.
B: The Basic authentication method prompts the user for a user name and a password, also called credentials, which are sent unencrypted over the network.
C: The Digest authentication method operates much like Basic authentication, except that passwords are sent across the network as a hash value for additional security. Digest authentication is available only on domains with domain controllers running Windows server operating systems.
http://support.microsoft.com/default.aspx?scid=kb;en-us;313251
http://support.microsoft.com/default.aspx?scid=kb;en-us;299875

QUESTION 208:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The functional level of the domain is Windows Server 2003 interim mode.
Employees in the human resources department of Certkiller .com need to modify certain attributes of employee user accounts. You plan to use a global group named HR Users to contain all user accounts for the human resources department. You plan to create a new group that includes the HR Users global group as a member.
You need to choose the appropriate type of group to implement your plan.
What type of group should you choose?

A. A domain local security group
B. A domain local distribution group
C. A universal security group
D. A universal distribution group

Answer: A

QUESTION 209:

You are a security administrator for Certkiller .com. The network consists of two Active Directory domains named Certkiller .com and de. Certkiller .com. These domains are in the same Active Directory forest. Both domains operate at a Windows 2000 mixed mode functional level.
A Windows Server 2003 computer named Certkiller -SR12 issues certificates for users and computer in the Certkiller .com network. Certkiller -SR12 is a member in the Certkiller .com Active Directory domain. You plan to use Certkiller -SR12 to

deploy certificates to authorized computer in the de. Certkiller .com Active Directory domain.
You need to create an access control solution that restricts certificate enrollment to authorized computers. You want to achieve this goal by using the minimum amount of administrative effort.
What should you do?

A. Add the accounts of authorized computers to a global group in the de. Certkiller .com domain.
B. Add the accounts of authorized computers to a universal group in the de. Certkiller .com domain.
C. Add the accounts of authorized computers to a global group in the Certkiller .com domain.
D. Add the accounts of authorized computers to a universal group in the Certkiller .com domain.

Answer: A

QUESTION 210:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. The network contains Windows Server 2003 computers and Windows XP Professional client computers.
A Windows Server 2003 computer named Certkiller -SR21 is a member of a workgroup. Certkiller -SR21 hosts a knowledge management application that is accessed from the network.
Contract employees require access to the knowledge management application. However, you do not want contract employees to have the right to create other user accounts on Certkiller -SR21.
You need to assign the contract employees appropriate permissions to use the application on Certkiller -SR21.
What should you do?

A. Create the user accounts in the Active Directory domain.
Place the user accounts in the default Authenticated Users group in the Active Directory domain, and then assign this group appropriate permissions on Certkiller -SR21.
B. Create the user accounts in the Active Directory domain.
Place the user accounts in the default Domain Users group in the Active Directory domain, and then assign this group appropriate permissions on Certkiller -SR21.
C. Create the user accounts in the local accounts database on Certkiller -SR21.
Place the user accounts in the default Users group on Certkiller -SR21, and then assign this group appropriate permissions on Certkiller -SR21.
D. Create the user accounts in the local accounts database on Certkiller -SR21.
Place the user accounts in the default Power Users group on Certkiller -SR21, and then assign this group appropriate permissions on Certkiller -SR21.

Answer: C

Explanation: Since this server in not in a domain, access can only be granted by using the local SAM database. Access can be granted by using the default Users group even though Power Users would also work. However, Power User is probably more permissions than is needed to run the application. Of course this would depend on how the application was written. However, this multiple users will be accessing this server the question does not mention that the users will need the 'Access this computer from the network' right.
The Principle of Least Privilege - In the real world, the built-in groups are often misused. It's a common practice to add users to the Power Users group so that an application that won't run with regular User privileges will work as expected. While this is better than adding the user to the Administrators group, there is a risk associated with this practice-the risk that the user will be granted unnecessary rights that will later be misused. Even if the user would never intentionally misuse the elevated privileges of the Power Users group, a virus or Trojan horse might take advantage of the additional privileges without the user being aware.

QUESTION 211:

You are a security administrator for Certkiller .com. The network consists of a single Active Directory domain named Certkiller .com. All servers run Windows Server 2003. All client computers run Windows 2000 Professional.
You installed Terminal Server on a member server named Certkiller -SR17. Users in the domain connect remotely to Certkiller -SR17 to run applications.
Terminal Services on Certkiller -SR17 is configured to run in Full Security mode.
You do not want to change the configuration to Relaxed Security mode.
You want to limit the effective permissions for the Program Files folder on Certkiller -SR17 when users connect remotely. By default, a few groups have Modify permissions for the Program Files folder. You want to ensure that these users have Modify permissions only when they are logged on locally to Certkiller -SR17. When they are remotely connected to Certkiller -SR17, they are not allowed to change to the Program Files folder.
You need to assign the appropriate permissions.
What should you do?

A. Assign the Remote Interactive Logon group the Deny - Write permission for the Program Files folder.
B. Assign the Remote Desktop Logon group the Deny - Write permission for the Program Files folder.
C. Assign the Terminal Server Users Logon group the Deny - Write permission for the Program Files folder.
D. Apply the Rootsec.inf security template to Certkiller -SR17.
E. Apply the Hisecws.inf security template to Certkiller -SR17.

Answer: A