

**Exam 70-299 study material**

**Made available by CertsKing.com**



**Free 70-299 Exam Preparation Questions**

**Exam 70-299: Implementing and Administering Security in a Microsoft Windows Server 2003 Network**

**Question: 1**

You work as a network designer for Cer-tech.com. All servers on the Cer-tech.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 Cer-tech.com. The users of Cer-tech.com travel through 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 Server01 and Server03 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 Server03.
- B. Enable fast reconnect on all the wireless access points (WAPs). Configure half the WAP's as clients of Server01 and the other half as clients of Server03.
- C. Configure the Wireless Access Points (WAPs) as clients of Server01. Enable PEAP fast reconnect on Server01. On all clients enable PEAP fast reconnect.
- D. Enable fast reconnect on Server03.

**Answer: C****Question: 2**

You work as a security administrator for Cer-tech.com. The company's network consists of a single Active Directory domain named Cer-tech.com. There are several departments in your company. The company has deployed Windows Server 2003 on all servers and Windows XP Professional on all client computers. In the company some of the servers are file servers which contain shared files. Users in the Service and Account department use these shared files. The file servers are located in an organizational unit (OU) named FServers. According to the requirement of the company security policy, when a user successfully establishes a session to a file server, the date and time must be recorded. If users try to modify files on the file servers, no matter it is successful or not, the data and time must also be recorded. After a new Group Policy object (GPO) is created, you link it to the FServers OU. The work area shows the Audit Policy section of the GPO. In order to meet the requirements of the company security policy, you have to configure the audit policy while using as little audit settings as possible. Of the following options, which are the correct policy settings for Audit logon events and Audit object access?

- A. Audit logon events: Failure
- B. Audit logon events: Success
- C. Audit object access: Success
- D. Audit object access: Failure. Success
- E. Audit logon events: Failure. Success

**Answer: B, D****Question: 3**

You work as the network administrator at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory domain named Cer-tech.com. The Cer-tech.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 Cer-tech.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 Cer-tech.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**

**Question: 4**

You work as the security administrator at Cer-tech.com. The Cer-tech.com network is a single Active Directory forest named Cer-tech.com that spans multiple sites. All servers on the Certech.com network run Windows Server 2003 and the client computers run Windows XP Professional. Cer-tech.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 Cer-tech.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 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 Cer-tech.com as a RADIUS client.

**Answer: C**

**Question: 5**

You work as the network administrator at Cer-tech.com. The Cer-tech.com network is a single Active Directory domain named Cer-tech.com. Cer-tech.com has its headquarters in Chicago and several branch offices country-wide. You are located in the head quarters. All servers on the Certech.com network run Windows Server 2003. These servers are located on the internal network at the Cer-tech.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 Server01 which is configured as a Routing and Remote Access Server (RRAS). Due to the vast number of users employed at Cer-tech.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**

**Question: 6**

You work as the network administrator at Cer-tech.com. The Cer-tech.com network is a single Active Directory named Cer-tech.com. Cer-tech.com has its headquarters in Chicago and branch offices in Dallas and Miami. All servers on the Cer-tech.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 Cer-

tech.com Certificate Authority hierarchy that issues certificates for Secure Sockets Layer (SSL) client authentication on the Web site. The Cer-tech.com Virtual Private Network (VPN) access point is located in Chicago and the dial-up access points are located in all three offices. The Certech.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 Cer-tech.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**

**Question: 7**

You work as the security administrator at Cer-tech.com. The Cer-tech.com network is a single Active Directory domain named Cer-tech.com that spans multiple sites. All servers on the Certech.com network run Windows Server 2003 and the client computers run Windows XP Professional. Cer-tech.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 Cer-tech.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**

**Question: 8**

You work as the network administrator at Cer-tech.com. The Cer-tech.com network is a single Active Directory domain named Cer-tech.com. All servers on the Cer-tech.com network run Windows Server 2003 and the client computers run Windows XP Professional. The network is not connected to the Internet. Many Cer-tech.com users prefer to work from home and thus connect to the company network via a Routing and Remote Access Server (RRAS) named Server01 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 denied 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**

**Question: 9**

You work as the network administrator at Cer-tech.com. The Cer-tech.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 Cer-tech.com includes the creation of shared folders. To this end you are busy creating a shared folder on a file server named Server01. This shared folder is intended for use in one of the child domains in the forest. Cer-tech.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 belongs 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 Cer-tech.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**

**Question: 10**

You work as the network administrator at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory domain named Cer-tech.com. All servers on the Cer-tech.com network run Windows Server 2003 and all client computers run Windows XP Professional. The Cer-tech.com network also contains a perimeter network. The Cer-tech.com intranet Web site is hosted on a Web server named Server01. Server01 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 Cer-tech.com written security policy dictates that the Cer-tech.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**

**Question: 11**

You work as the network administrator at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory domain named Cer-tech.com. All servers on the Cer-tech.com network run Windows Server 2003 and all client computers are portable computers running Windows XP Professional. The Cer-tech.com network contains two Internet Authentication Service (IAS) servers named Server01 and Server02 respectively. You are responsible for the design and the configuration of the Cer-tech.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 Server01.
- C. Configure the wireless access points to be clients of Server01.
- D. Enable PEAP fast reconnect on Server02.
- E. Enable PEAP fast reconnect on all the wireless clients.
- F. From the available wireless access points configure half as clients of Server01 and half as clients of Server02.

**Answer: B, C, E**

**Question: 12**

You work as the network administrator at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory domain named Cer-tech.com. All servers on the Cer-tech.com network run Windows Server 2003. The functional level of the domain is set at Windows Server 2003. The Cer-tech.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 handled 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**

**Question: 13**

You work as the network administrator at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory forest that contains two domains named us.Cer-tech.com and uk.Cer-tech.com. The functional level of the forest is set at Microsoft Windows Server 2003. All servers on the Cer-tech.com network run Windows Server 2003. Half the client computers run Windows 2000 Professional, and the rest run Windows XP Professional. The Cer-tech.com network contains a few domain controllers. Cer-tech.com has its headquarters in Paris and a branch office in Berlin and Milan. In the Berlin branch office resides the us.Cer-tech.com, and in the Milan branch office resides the uk.Cer-tech.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 Cer-tech.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 Milan Marketing group. Then add these groups as members of the Cer-tech.com Marketing group.
- B. Create two global groups named Berlin Marketing and Milan Marketing. Then create a universal group named Cer-tech.com Marketing.
- C. Create two domain local groups named Berlin Marketing and Milan Marketing.
- D. Add the marketing employees to the Cer-tech.com Marketing group. Then create a global group named Cer-tech.com Marketing group.

**Answer: A, B**

**Question: 14**

You work as the network administrator at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory domain named Cer-tech.com which has multiple sites. All servers on the Cer-tech.com network run Windows Server 2003 and all client computers run Windows XP Professional. Cer-tech.com has headquarters in London and branch offices in Paris, Berlin and Milan. Each Cer-tech.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 and 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**

**Question: 15**

You work as the senior network administrator at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory domain named Cer-tech.com. All servers on the Certech.com network run Windows Server 2003 and all client computers run Windows XP Professional. Cer-tech.com hosts a public Web site on a Web server named Server01. The Web site is used by customers to place orders for products offered for sale by the company. The management of Server01 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 Server01 have stopped intermittently. Consequently the Cer-tech.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 Server01 to view the information.
- D. Open Event Viewer from three computers. Use a different computer to collect information on each service.

**Answer: A**

**Question: 16**

You work as the network administrator at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory domain named Cer-tech.com. All servers on the Cer-tech.com network run Windows Server 2003 and all client computers run Windows XP Professional. Cer-tech.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**

**Question: 17**

You work as the network engineer at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory domain named Cer-tech.com. Each Cer-tech.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**

**Question: 18**

You work as the network administrator at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory domain named Cer-tech.com. All servers on the Cer-tech.com network run Windows Server 2003 and all client computers run Windows XP Professional. A Web server named Server01 hosts the Cer-tech.com Internet e-commerce Web site. The Cer-tech.com partner companies access this Web site to order merchandise offered for sale by Cer-tech.com. All partner companies are authenticated by using a certificate when they log on to Web site. Server01 is issued with a SSL certificate by a Cer-tech.com internal stand-alone subordinate certification authority (CA). A different stand-alone subordinate CA is used to issue certificates to partner companies. The Cer-tech.com help desk then received complaints from a new partner company, stating that one of its users cannot connect to the Cer-tech.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 Server01 to the Certificate Trust List (CTL) of its computer.
- B. Configure an Active Directory trust relationship between the Cer-tech.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 Server01 to the Trusted Root Certification Authorities policy of its computer.

**Answer: A**

**Question: 19**

You work as the network administrator at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory domain named Cer-tech.com. All servers on the Cer-tech.com network run Windows Server 2003 and all client computers run Windows XP Professional. The Cer-tech.com network contains five application servers running Terminal Services named Server01, Server02, Server03, Server04, and Server05. 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**

**Question: 20**

You work as a security administrator for Cer-tech.com. The company's network consists of a single Active Directory domain named Cer-tech.com. Your company has deployed Windows Server 2003 on all servers. According to the company security policy, security patches must be installed on servers manually by administrators. You have to configure the network to be in conformity with the written security policy. You should use as little administrative effort as possible to maintain security patches. So what action should you perform?

- A. First a new organizational unit (OU) should be created to contain all server computers, and then you should create a new Group Policy object (GPO) and link it to the OU. Configure the GPO, making it automatically download updates and notify when they are ready to be installed.
- B. First a new organizational unit (OU) should be created to contain all server computers, and then you should create a new Group Policy object (GPO) and link it to the OU. Configure the GPO, making it disable Automatic Updates. At last permit only administrators to start Automatic Updates.
- C. First you should modify the Default Domain Policy Group Policy object (GPO), making it disable Windows Update and Automatic Updates. After a new organizational unit (OU) named Admins is created, place all administrator accounts in the Admins OU. Block GPO inheritance on the Admins OU.
- D. First a new organizational unit (OU) named Admins should be created to contain all administrators, and then you should create a second OU named Servers to contain all server computers. After you create a new Group Policy object (GPO), you should link it to the Admins OU. At last you should configure the GPO, making it disable Automatic Updates.

**Answer: A**

**Question: 21**

You work as the network administrator at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory domain named Cer-tech.com. All servers on the Cer-tech.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 Server01, Server02, Server03, and Server04 respectively. There is a new Cer-tech.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 Cer-tech.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**

**Question: 22**

You work as a security administrator for Cer-tech.com. The company's network consists of a single Active Directory domain named Cer-tech.com and ten Active Directory sites. Your company has deployed Windows Server 2003 on all servers and Windows XP Professional on all client computers. All computers are members of the single Active Directory domain. Since there are ten offices in the company, each site stands for one of the offices. These offices reside over the world and each one can connect to the Internet. Dedicated leased lines are kept between the offices by the company. For Microsoft security patches, you are planning a security patch management infrastructure. There is a server named S1 in the company network. You perform the installation of Software Update Services (SUS) on S1. Now you receive an order from your company, according to the company requirement, on the client computers and servers, Automatic Updates installs only security patches that are approved by the company. You are asked to make sure of this. Through the way of allowing each computer to download the security patches from the Internet, you intend to restrict the use of the leased lines between the offices. What should you do? (choose more than one)

- A. On all computers, you should configure Automatic Updates to use SUS on S1.
- B. You should configure S1 to maintain updates on the Microsoft Windows Update servers.
- C. On all computers, you should configure Automatic Updates to use the Microsoft Windows Update servers.
- D. You should copy the Approveditems.txt file from S1 to the Windows folder on each computer.
- E. You should configure the value of the Run key in the registry as the URL of the Microsoft Windows Update Web site on all computers.
- F. On all computers, you should configure the SUS server location as the URL of the Microsoft Windows Update Web site by using Group Policy.

**Answer: A, B**

**Question: 23**

You work as the network administrator at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory domain named Cer-tech.com. All servers on the Cer-tech.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 DC01 has been configured as a domain controller and another server named Server02 has been configured as a file server. Server02 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 Certech.com managers only. All the Cer-tech.com managers enjoy membership of a global security group named Managers. This group has been granted Full Control permission over the ConfidentialDocs folder. One of the Cer-tech.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 matter 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?

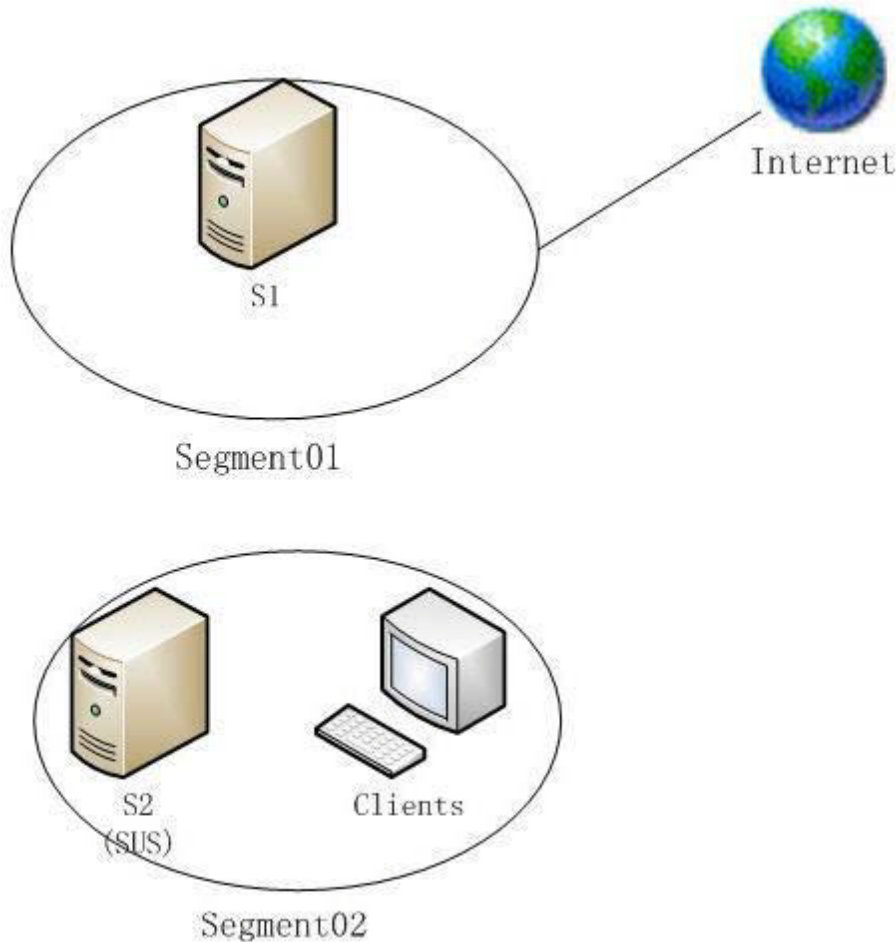
- A. Configure Audit account management policy for failure.
- B. Configure Audit directory service access policy for success and failure.
- C. Configure Audit account management policy for success and failure.

- 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**

**Question: 24**

You work as a security administrator for Cer-tech.com. The company's network consists of a single Active Directory domain named Cer-tech.com. There are two segments in the company network. The two segments are respectively named Segment01 and Segment02. Your company has deployed Windows Server 2003 on all servers and Windows XP Professional on all client computers. There is a single server named S1 in Segment01. All other computers are contained in Segment02, including a server named S2. According to the company security public, Segment01 is allowed to connect to the Internet but Segment 02 must not be connected to the Internet. Segment01 is not connected to Segment 02. You can use a CD-ROM to transport the files between the two segments. The exhibit below shows the network topology. (Click the Exhibit button.) Recently you are designing a patch management infrastructure. On S2, Software Update Services (SUS) is installed on Segment02. In segment02, you configure Automatic Updates on all computers, making it use http://S2 and install security patches. Now you must make sure that all computers in Segment02 automatically install security patches. So what action should you perform to achieve this goal?



- A. You should configure Automatic Updates to use the URL of the Microsoft Windows Update Web site on S1. Then you should copy the downloaded files and the Mssecure.xml file to the Content folder on S2 periodically.
- B. On S1, you should install SUS. Copy the files in the Content folder and in the SUS root folder from S1 to S2 Periodically.
- C. On S1, you should install SUS. Copy the files in the Content folder from S1 to S2 Periodically and copy the Approveditems.txt file from S1 to the Windows folder on S2.
- D. You should periodically connect to the Microsoft Windows Update Catalog Web site and download new security

patches on S1. Then you should copy the files to the Content folder on S2.

**Answer: B**

**Question: 25**

You work as the network administrator at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory domain named Cer-tech.com. All servers on the Cer-tech.com network run Windows Server 2003 and all client computers run Windows XP Professional. A server named Server01 has been configured as a file server. Server01 hosts a shared folder named UserDocs. A global group named Full-time Employees has been granted the Full Control Permission over UserDocs. A Cer-tech.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**

**Question: 26**

You work as the network administrator at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory domain named Cer-tech.com. All servers on the Cer-tech.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 Server01, 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 Cer-tech.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**

**Question: 27**

You work as the network administrator at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory domain named Cer-tech.com. All servers on the Cer-tech.com network run Windows Server 2003 and all client computers run Windows XP Professional. The Cer-tech.com network contains several new Windows Server 2003 server computers 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 GPadmin and add all authorized administrators to this group. You need to assign the task of issuing and revoking certificates to members of the GPadmin group. Only members of the GPadmin global security group must be assigned permissions to manage certificates. What should you do?

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

**Answer: A**

**Question: 28**

You work as the network administrator at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory domain named Cer-tech.com. All servers on the Cer-tech.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 Cer-tech.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**

**Question: 29**

You work as the senior network administrator at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory domain named Cer-tech.com. All servers on the Certech.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**

**Question: 30**

You work as a security administrator for Cer-tech.com. The company's network consists of a single Active Directory

domain named Cer-tech.com. Your company has deployed Windows Server 2003 on all servers and Windows XP Professional on all client computers. Web applications are hosted for clients in the company. Each client is a company which contains many employees. These employees all need access to the Web applications. Each client owns one Web application and each Web application is configured as a virtual directory. After a user account is configured for each client, you assign this account permission to read the virtual directory which contains the client's Web application. According to the company requirement, employees are only allowed to access only their company's Web application. You have to make sure of this while not asking clients to disclose passwords. So what action should you perform to ensure this?

- A. First you should configure a certification authority (CA). Issue certificates to each employee of each client that requires access to the Web site, then you should configure many-to-one certificate mapping.
- B. You have to configure anonymous access for each virtual directory and configure each virtual directory to use the client's assigned user account. Then leave the password assigned to the user account blank.
- C. First you should acquire a Server Authentication digital certificate from a public certification authority (CA), and then you should configure the Web server to use this certificate and to require SSL. At last you should distribute a copy of the Server Authentication certificate to each employee of each client that requires access to the Web site.
- D. First you should configure Microsoft .NET Passport authentication for each virtual directory. And then you should ask each employee of each client that requires access to the Web site to enroll for a new .NET Passport.

**Answer: A**

**Question: 31**

You work as the network security administrator at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory domain named Cer-tech.com. The Cer-tech.com network contains ten Windows Server 2003 computers and 1,200 client computers running Windows XP Professional. Cer-tech.com can fall prey to industrial espionage. To this end Internet Protocol Security (IPSec) is implemented on the Cer-tech.com network. However, it has come to the CIO's attention that one of the Cer-tech.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**

**Question: 32**

You work as the network administrator at Cer-tech.com. The Cer-tech.com network consists of a single Active Directory domain named Cer-tech.com. All servers on the Cer-tech.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 Cer-tech.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 night's 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

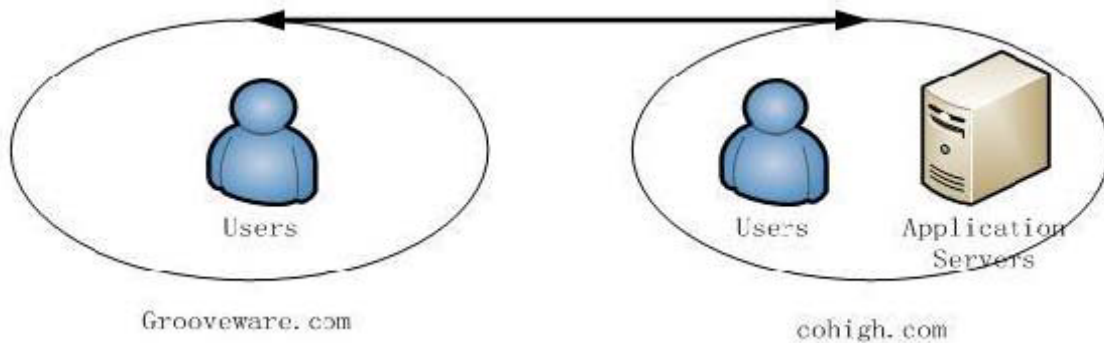
that will list all entries produced by the audit policy.

- 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**

**Question: 33**

You work as a security administrator for Cer-tech.com. The network contains two single Active Directory domains. The two domains are respectively named Grooveware.com and cohight.com. The two domains are located in the same Active Directory forest. The grooveware.com Active Directory domain runs at a Windows 2000 mixed mode functional level, while the cohight.com Active Directory domain runs at a Windows 2000 native mode functional level. There is an application which runs on four Windows Server 2003 computers which are domain member servers in the grooveware.com Active Directory domain. Authorized users in both the grooveware.com and the cohight.com domains require access to this application. The network is depicted in the exhibit. (Click the Exhibit button.) In order to control user access to the application, you must plan an authorization model. You will place grooveware.com user accounts in a group named Grooveware AppUsers. You will assign permissions that allow access to the application by using a group named AppResources. You have to identify the appropriate types of groups to implement your plan. Of the following types of groups, which should you choose?



- A. In the cohight.com domain, you should use a global group named Cohight AppUsers.
- B. In the grooveware.com domain, you should use a global group named Grooveware AppUsers.
- C. In the cohight.com domain, you should use a domain local group named Cohight AppUsers.
- D. In the grooveware.com domain, you should use a domain local group named Grooveware AppUsers.
- E. In the cohight.com domain, you should use a global group named AppResources that contains the Grooveware AppUsers and the Cohight AppUsers groups.
- F. In the grooveware.com domain, you should use a global group named AppResources that contains the Grooveware AppUsers and the Cohight AppUsers groups.
- G. In the cohight.com domain, you should use a domain local group named AppResources that contains the Grooveware AppUsers and the Cohight AppUsers groups.
- H. In the grooveware.com domain, you should use a domain local group named AppResources that contains the Grooveware AppUsers and the Cohight AppUsers groups.

**Answer: A, B, H**

For complete [Exam 70-299 Training kits and Self-Paced Study Material](http://www.certsking.com/70-299)

Visit:

<http://www.certsking.com/70-299.html>

**CERTSKING**

The Best Leader In Certifications

<http://www.certsking.com/>

