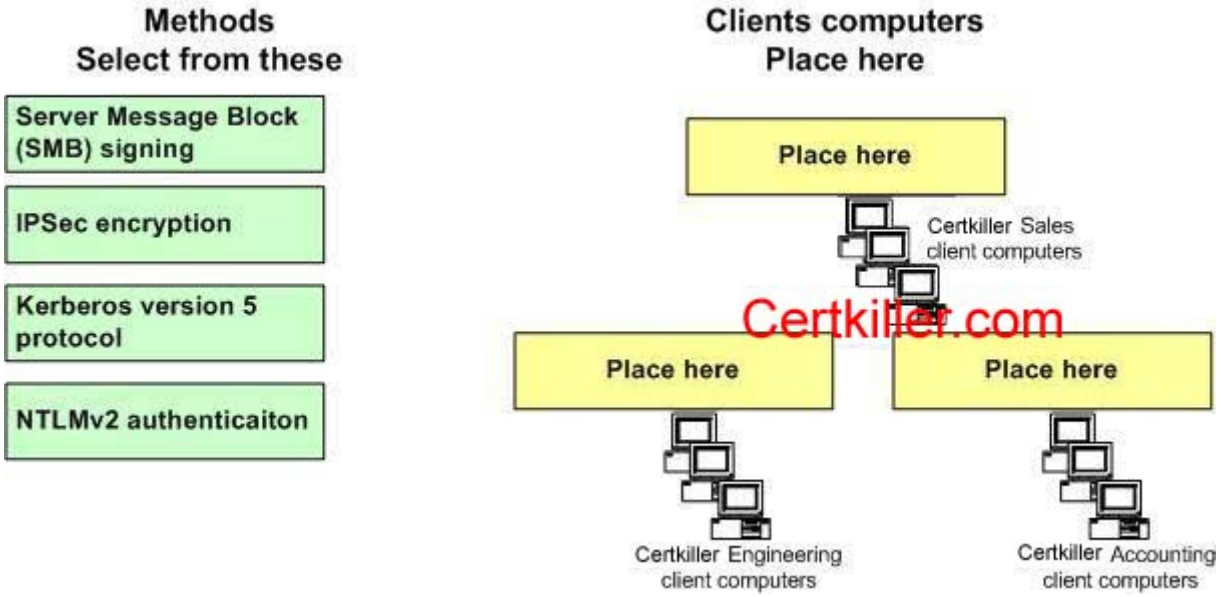
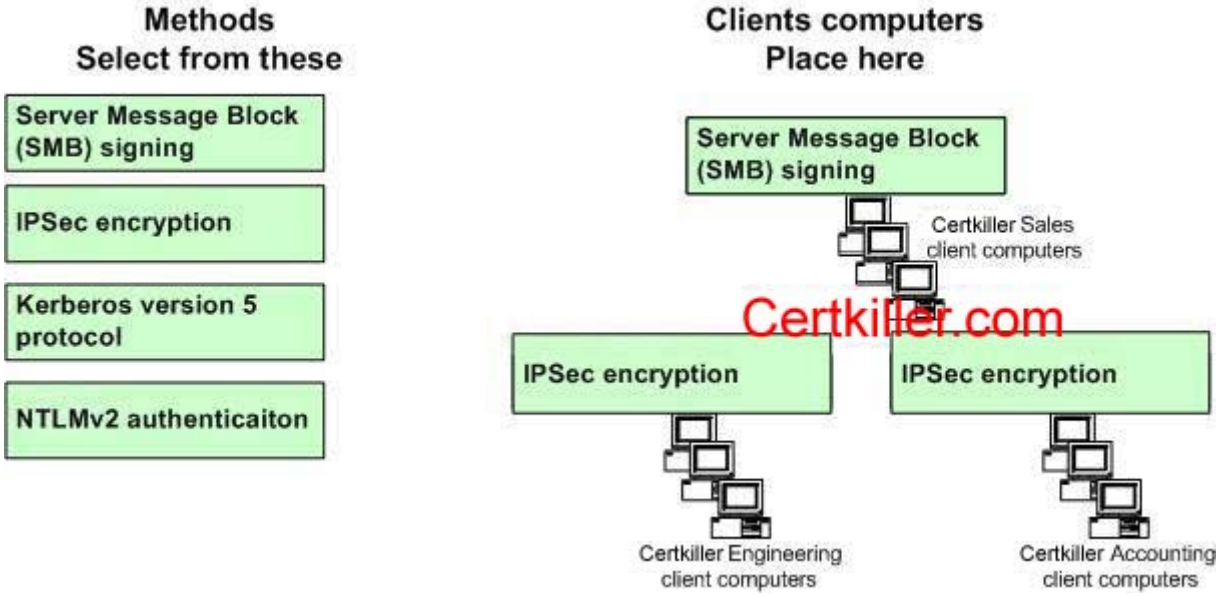
QUESTION 1
You are a network administrator for Certkiller. The network contains two Windows Server 2003 computers named CertkillerA and CertkillerB. These servers host an intranet application. Currently, 40 users connect to CertkillerA and 44 users connect to CertkillerB. The company is adding 35 employees who will need access to the intranet application. Testing shows that each server is capable of supporting approximately 50 users without adversely affecting the performance of the application. You need to provide a solution for supporting the additional 35 employees. The solution must include
providing server fault tolerance. You need to minimize the costs and administrative effort required by your solution. You add a new server named CertkillerC to the network and install the intranet application on CertkillerC. What else should you do?
A. Use Network Load Balancing Manager to configure CertkillerA, CertkillerB, and CertkillerC as a Network Load Balancing cluster.
B. Use Cluster Administrator to configure CertkillerA, CertkillerB, and CertkillerC as a three-node server cluster. Use the Majority Node Set option.
Configure the cluster so that all three nodes are active.
C. Use Cluster Administrator to configure CertkillerA, CertkillerB, and CertkillerC as a three-node server cluster. Configure the cluster so that two nodes are active and one node is a hot standby node.
D. Use DNS load balancing to utilize all three servers by using the same virtual server name.
Answer: A
Explanation:
We can use Network Load Balancing to balance the load on the three web servers.
Reference:
Deploying Network Load Balancing
Overview of the NLB Deployment Process
A Network Load Balancing cluster comprises multiple servers running any version of the Microsoft(r) Windows(r) Server 2003 family, including Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Datacenter Edition, and Windows Server 2003 Web Edition. Clustering allows you to combine application servers to provide a level of scaling, availability, or security that is not possible with an individual server. Network Load Balancing distributes incoming client requests among the servers in the cluster to more evenly balance the workload of each server and prevent overload on any one server. To client computers, the Network Load Balancing cluster appears as a single server that is highly scalable and fault tolerant. The Network Load Balancing deployment process assumes that your design team has completed the design of the Network Load Balancing solution for your organization and has performed limited testing in a lab. After the design team tests the design in the lab, your deployment team implements the Network Load Balancing solution first in a pilot environment and then in your production environment.
Upon completing the deployment process presented here, your Network Load Balancing solution (the Network Load Balancing cluster and the applications and services running on the cluster) will be in place. For more information about the procedures for deploying Network Load Balancing on individual servers, see the appropriate Network Load Balancing topics in Help and Support Center for Windows Server 2003
Incorrect Answers:
B: We already have three servers. A cluster would require different hardware and would thus be more expensive.
C: We already have three servers. A cluster would require different hardware and would thus be more expensive.
D: Round Robin DNS would load balance the servers, but if one server failed, clients would still be directed to the failed server.

QUESTION 2
You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. All domain controllers run Windows Server 2003. All application servers run Windows Server 2003. Client computers in the accounting department run Windows XP Professional. Client computers in the engineering department run Windows 2000 Professional. Client computers in the Sales department run either Windows NT Workstation 4.0 or Windows 98. All client computers access data files on the application server. You need to plan the method of securing the data transmissions for the client computers. You want to ensure that the data is not modified while it is transmitted between the application servers and the client computers. You also want to protect the confidentiality of the data, if possible. What should you do?
To answer, drag the appropriate method or methods to the correct department's client computers.



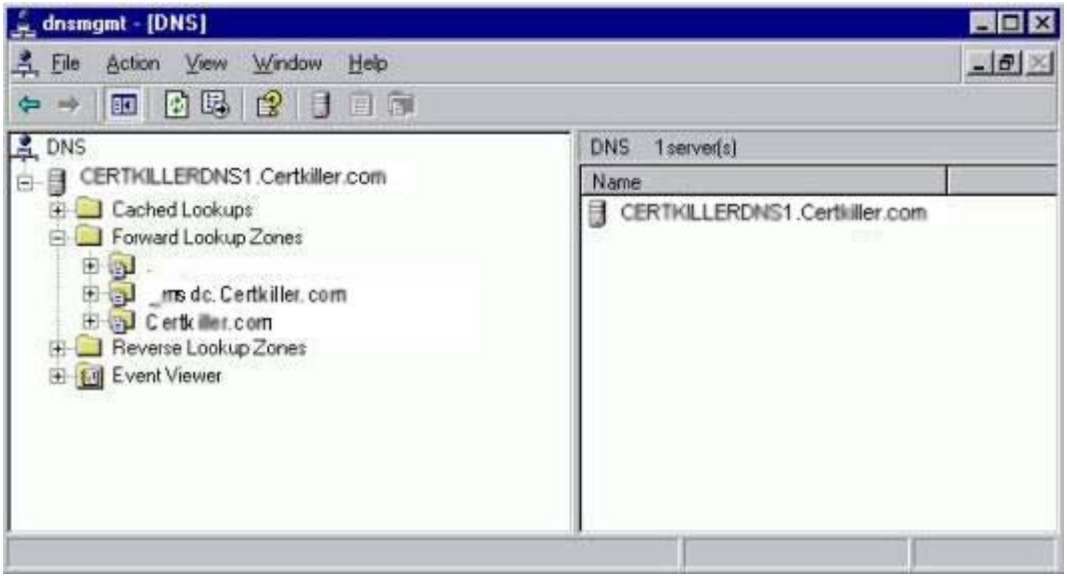
Answer:



Explanation
We can use IPSEC on Windows 2000 and Windows XP but we cannot use IPSEC for Legacy clients except for

VPNs. Sales contains Windows NT 4.0 and Windows 98; in this case we use SMB signing. With Windows 2000 and Windows XP both methods are supported in this case and for security reasons we will use IPSEC rules. SMB signed is supported by Windows 2000 an XP by local policies or domain policies to be enforced To be supported in legacy clients you must modify the registry in Windows 98 and Windows NT
SMB on Windows 98 KB article 230545
Windows 98 includes an updated version of the SMB authentication protocol. However, using SMB signing slows down performance when it is enabled. This setting should be used only when network security is a concern. The performance decrease usually averages between 10-15 percent. SMB signing requires that every packet is signed for and every packet must be verified.
SMB on Windows NT KB article 161372
Windows NT 4.0 Service Pack 3 provides an updated version of the Server Message Block (SMB) authentication protocol, also known as the Common Internet File System (CIFS) file sharing protocol
IPSEC
The Internet Protocol Security (IPsec) feature in Windows 2000, Windows XP and Windows Server 2003 was not designed as a full-featured host-based firewall. It was designed to provide basic permit and block filtering by using address, protocol and port information in network packets. IPsec was also designed as an administrative tool to enhance the security of communications in a way that is transparent to the programs. Because of this, it provides traffic filtering that is necessary to negotiate security for IPsec transport mode or IPsec tunnel mode, primarily for intranet environments where machine trust was available from the Kerberos service or for specific paths across the Internet where public key infrastructure (PKI) digital certificates can be used.
IPSEC is not supported on legacy clients just is supported for VPN
http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/l2tpclient.asp Microsoft L2TP/IPSec VPN Client is a free download that allows computers running Windows 98, Windows Millennium Edition (Me), or Windows NT(r) Workstation 4.0 to use Layer Two Tunneling Protocol (L2TP) connections with Internet Protocol security (IPSec).
Windows 98 (all versions) with Microsoft Internet Explorer 5.01 (or later) and the Dial-up Networking version 1.4 upgrade.
Windows Me with the Virtual Private Networking communications component and Microsoft Internet Explorer 5.5 (or later)
Windows NT Workstation 4.0 with Remote Access Service (RAS), the Point-to-Point Tunneling Protocol, Service Pack 6, and Microsoft Internet Explorer 5.01 (or later)

QUESTION 3
You are the systems engineer for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. All servers run Windows Server 2003. A Windows Server 2003 computer named CertkillerDNS1 functions as the internal DNS server and has zones configured as shown in the exhibit.



The network is not currently connected to the Internet. Certkiller maintains a separate network that contains publicly accessible Web and mail servers. These Web and mail servers are members of a DNS domain named Certkiller.com. The Certkiller.com zone is hosted by a UNIX-based DNS server named UNIX DNS, which is running the latest version of BIND. The company plans to allow users of the internal network to access Internet-based resources. The company's written security policy states that resources located on the internal network must never be exposed to the Internet. The written security policy states that the internal network's DNS namespace must never be exposed to the Internet. To meet these requirements, the design specifies that all name resolution requests for Internet-based resources from computers on the internal network must be sent from CertkillerDNS1. The current design also specifies that UNIX DNS must attempt to resolve any name resolution requests before sending them to name servers on the Internet.

You need to plan a name resolution strategy for Internet access. You need to configure CertkillerDNS1 so that it complies with company requirements and restrictions. hat should you do?

A. Delete the root zone form CertkillerDNS1. Configure CertkillerDNS1 to forward requests to UNIX DNS.

B. Copy the Cache.dns file from the Windows Server 2003 installation CD-ROM to the C:\Windows\System32\Dns folder on CertkillerDNS1.

C. Add a name server (NS) resource record for UNIX DNS to your zone. Configure UNIX DNS with current root hints.

D. On CertkillerDNS1, configure a secondary zone named Certkiller.com that uses UNIX DNS as the master server. Configure UNIX DNS to forward requests to your ISP's DNS servers.

Answer: A

Explanation:

We need to delete the root zone from the internal DNS server. This will enable us to configure the server to forward internet name resolution requests to the external DNS server (UNIX DNS). A DNS server configured to use a forwarder will behave differently than a DNS server that is not configured to use a forwarder. A DNS server configured to use a forwarder behaves as follows:

1. When the DNS server receives a query, it attempts to resolve this query using the primary and secondary zones that it hosts and its cache.
2. If the query cannot be resolved using this local data, then it will forward the query to the DNS server designated as a forwarder.
3. The DNS server will wait briefly for an answer from the forwarder before attempting to contact the DNS servers specified in its root hints.

Incorrect Answers:
B: The Cache.dns file contains the IP addresses of the internet root DNS servers. We don't want the internal DNS server to query the root DNS servers, so we don't need the cache.dns file.
C: Unix dns already has root hints. An NS record on the internal DNS server won't fulfil the requirements of the question.
D: We don't need a secondary zone on the internal DNS server. All external resolution requests must be forwarded to the external DNS server.

QUESTION 4
You are the system engineer for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. All servers run Windows Server 2003. The network is connected to the Internet by a dedicated T3 line. Certkiller enters into a partnership with another company for a new project. The partner company's network consists of a single Active Directory forest that contains two domains. All servers in the network run Windows 2003 Server. The partner network is also connected to the Internet by a dedicated T3 line. The partner network is accessible by a VPN connection that was established between the two networks. The VPN connection was tested and was verified to provide a functional connection between the two networks. Users from both companies need to connect to resources located on another network. A forest trust relationship exists between the two companies' forests to allow user access to resources. Users in your company report that they can access resources on the partner network, but that it can take up to several minutes for the connection to be established. This problem is most pronounced during the morning. You verify that there is sufficient available bandwidth on the connection between the two networks to provide access. You also verify that both network's routing tables are configured correctly to route requests to the appropriate destinations. When you attempt to connect to a server in the partner network by host name by using the ping command, the connection times out. However, when you attempt to connect to the server a second time by IP address by using the ping command, you receive a response within a few seconds. You need to improve the performance of the network connection between the two networks. What should you do?
A. Add the partner network's domain names and DNS server addresses to the forwarders list on your DNS servers.
B. Update the root hints list on your DNS servers to include the host names and IP addresses of the partner network's DNS servers.
C. Disable recursion on the DNS servers in both companies' networks.
D. Add the partner network's DNS server addresses to the 006 DNS Servers scope option in your DHCP scope.
Answer: A
Explanation:
It is taking a long time to locate resources on the other network. This is because name resolution requests are being passed to the internet root servers, then down through the internet DNS hierarchy before the request finally reaches the appropriate DNS server. We can speed up this process by using conditional forwarding. This would enable resolution requests for resources in the partner network to be forwarded directly to the partner's DNS server.
Conditional forwarders
A conditional forwarder is a DNS server on a network that is used to forward DNS queries according to the DNS domain name in the query. For example, a DNS server can be configured to forward all the queries it receives for names ending with widgets.example.com to the IP address of a specific DNS server or to the IP addresses of multiple DNS servers.
Incorrect Answers:
B: The root hints are used to locate internet root DNS servers.

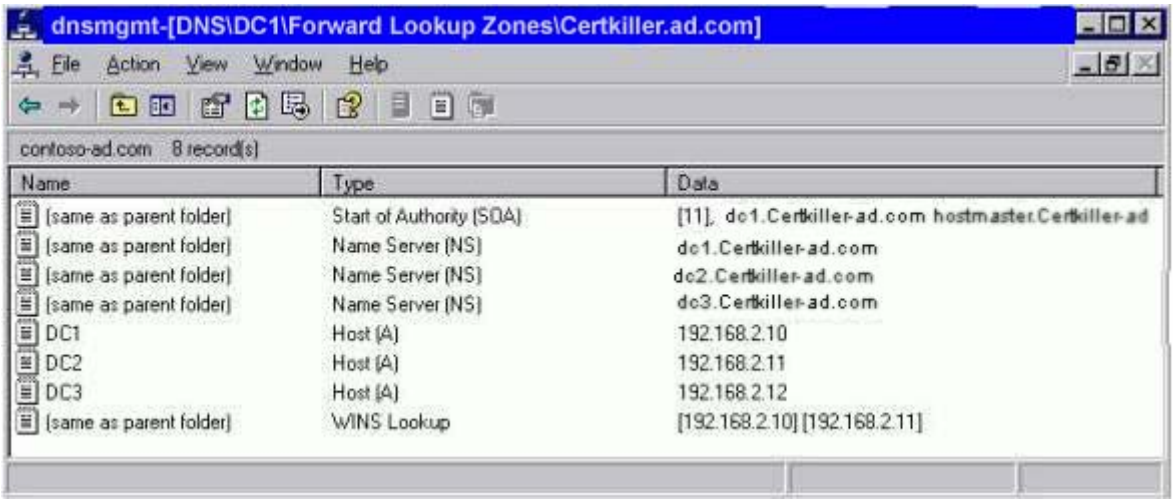
C: This won't help. It would mean that the internal DNS servers wouldn't forward external resolution requests to other DNS servers such as the root servers.
D: The partner network's DNS servers would never be used unless the local DNS server failed.

QUESTION 5
You are the network administrator for Contoso, Ltd. The network consists of a single Active Directory forest. The functional level of the forest is Windows Server 2003. The forest root domain is contoso.com. Contoso, Ltd,. recently merged with another company named Certkiller, whose network consists of a single Active Directory forest. The functional level of the Certkiller forest is Windows Server 2003. The forest root domain for Certkiller is Certkiller.com. You need to create a forest trust relationship between the two forests. Each company has dedicated connections to the Internet. You need to configure DNS to support the forest trust relationship. You want to maintain Internet name resolution capability for each company's network. What should you do?
A. Configure the contoso.com DNS servers to forward to the Certkiller.com DNS servers. Configure the Certkiller.com DNS servers to forward to the contoso.com DNS servers.
B. Configure conditional forwarding of Certkiller.com on the contoso.com DNS servers to the Certkiller.com DNS servers. Configure conditional forwarding of contoso.com on the Certkiller.com DNS servers to the contoso.com DNS servers.
C. Configure a standard primary zone for Certkiller.com on one of the contoso.com DNS servers. Configure a standard primary zone for contoso.com on one of the Certkiller.com DNS servers.
D. Configure an Active Directory-integrated zone for Certkiller.com on the contoso.com DNS servers. Configure an Active Directory-integrated zone for contoso.com on the Certkiller.com DNS servers.
Answer: B
Explanation:
This is a typical scenario for conditional forwarding
Conditional forwarders. A conditional forwarder is a DNS server on a network that is used to forward DNS queries according to the DNS domain name in the query. For example, a DNS server can be configured to forward all the queries it receives for names ending with widgets.example.com to the IP address of a specific DNS server or to the IP addresses of multiple DNS servers.
Incorrect Answers:
A: We don't want ALL resolution requests to be forwarded to the other DNS servers.
C: We can't host primary zones on multiple servers.
D: We can't host AD integrates zones on DNS servers in a different forest.

QUESTION 6
You are the network administrator for Certkiller. The network consists of a single Active Directory forest that contains three domains. Each domain contains domain controllers that run Windows 2000 Server and domain controllers that run Windows Server 2003. The DNS Server service is installed on all domain controllers. All client computers run Windows XP Professional. You need to add an additional DNS zone that is hosted on at least one DNS server on each domain. You want to configure the zone to allow secure updates only. What should you do?
A. Configure the new zone on DNS servers in the root domain. Configure stub zones that refer to DNS servers in another two domains.
B. Configure the new zone as a primary zone on one DNS server. Configure other DNS servers in the three domains as secondary servers for this zone.
Enable the DNS Security Extensions (DNSSEC) protocol.

C. Configure the new zone as an Active Directory-integrated zone on DNS servers in the three domains. Store the zone data in the DNS directory partition named DomainDNSZones.
D. Configure the new zone as an Active Directory-integrated zone on DNS servers in the three domains. Store the zone data in the DNS directory partition named ForestDNSZones.
Answer: D
Explanation:
To enable secure updates, we need an Active Directory integrated zone. To replicate to the DNS servers in the other domains, the zone must be installed on a Windows 2003 domain controller in each domain. During the configuration of the zone, you can select the option to replicate the zone information to all domain controllers in the forest; this will store the zone data in the DNS directory partition named ForestDNSZones.
Incorrect Answers:
A: We need Active Directory integrated zones, not stub zones.
B: Secondary zones are not writeable and so cannot accept updates.
C: If we store the zone data in the DNS directory partition named DomainDNSZones, it will only be replicated in a single domain, not the entire forest.

QUESTION 7
You are the systems engineer for Certkiller GmBh. The network consists of three Windows NT 4.0 domains in a master domain model configuration. The servers on the network run either Windows NT Server 4.0 or Windows 2000 Server. All domain controllers run Windows NT Server 4.0.
The network also contains 10 UNIX-based application servers. All host name resolution services are provided by a UNIX-based server running the latest version of BIND, which currently hosts the zone for the Certkiller.com domain. All NetBIOS name resolution services are provided by two Windows 2000 Server WINS servers. The company is in the process of migrating to a single Windows Server 2003 Active Directory domain based network. The new domain is named Certkiller-ad.com, and it will be hosted in an Active Directory integrated zone that is stored on the domain controllers. Servers that are not domain controllers will not be updated at this time. The migration plan requires that all computers must use DNS to resolve host names and computer redundancy for the Windows-based DNS servers. You upgrade the domain controllers in the master domain to Windows Server 2003. You also migrate all user and computer accounts to the new Active Directory domain. The DNS zone on the Windows Server 2003 computers is configured as shown in the exhibit.



You now need to configure the required redundancy between the Windows-based DNS servers and the server computers. Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

A. On a Windows Server 2003 DNS server, create a secondary zone that uses the UNIX-based DNS server as the master server.
B. On the UNIX-based DNS server, create a secondary zone that uses a Windows-based DNS server as the master server.
C. On a Windows Server 2003 DNS server, create a stub zone that uses the UNIX-based DNS server as the master server.
D. Add a delegation in the Certkiller.com zone that delegates authority of the Certkiller-ad.com zone to a Windows Server 2003 DNS server.
E. Configure the Certkiller-ad.com zone to not replicate WINS-specific resource records during zone transfers.
Answer: B, E
Explanation:
This is a trick question because it is asking for redundancy for the Windows 2003 DNS servers. We can provide this by configuring the UNIX DNS server to resolve names in the Certkiller-ad.com domain. With a secondary zone on the UNIX DNS server, the UNIX DNS server will be able to resolve host name resolutions requests in the Certkiller-ad.com domain. The Certkiller-ad.com DNS is configured to query WINS if required. When configuring a UNIX DNS server with a secondary zone, we should configure the zone to not replicate WINS-specific resource records during zone transfers.
Incorrect Answers:
A: This would provide redundancy for the UNIX server; the question isn't asking for that.
C: This won't provide any redundancy.
D: Certkiller-ad.com isn't a subdomain of Certkiller.com so no delegation is required.

QUESTION 8
You are the network administrator for Certkiller. The network consists of an internal network and a perimeter network. The internal network is protected by a firewall. The perimeter network is exposed to the Internet. You are deploying 10 Windows Server 2003 computers as Web servers. The servers will be located in the perimeter network. The servers will host only publicly available Web pages. You want to reduce the possibility that users can gain unauthorized access to the servers. You are concerned that a user will probe the Web servers and find ports or services to attack. What should you do?
A. Disable File and Printer Sharing on the servers.
B. Disable the IIS Admin service on the servers.
C. Enable Server Message Block (SMB) signing on the servers.
D. Assign the Secure Server (Require Security) IPSec policy to the servers.
Answer: A
Explanation:
We can secure the web servers by disabling File and Printer sharing.
File and Printer Sharing for Microsoft Networks
The File and Printer Sharing for Microsoft Networks component allows other computers on a network to access resources on your computer by using a Microsoft network. This component is installed and enabled by default for all VPN connections. However, this component needs to be enabled for PPPoE and dial-up connections. It is enabled per connection and is necessary to share local folders. The File and Printer Sharing for Microsoft Networks component is the equivalent of the Server service in Windows NT 4.0. File and Printer sharing is not required on web servers because the web pages are accesses over web protocols such as http or https, and not over a Microsoft LAN.
Incorrect Answers:
B: This is needed to administer the web servers. Whilst it could be disabled, disabling File and Printer sharing

will secure the servers more.
C: SMB signing is used to verify, that the data has not been changed during the transit through the network. It will not help in reducing the possibility that users can gain unauthorized access to the servers.
D: This will prevent computers on the internet accessing the web pages.

QUESTION 9
You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. Certkiller's perimeter network contains 50 Web servers that host the company's public Internet site. The Web servers are not members of the domain. The network design team completed a new design specification for the security of servers in specific roles. The network design requires that security settings must be applied to Web servers. These settings include password restrictions, audit settings, and automatic update settings. You need to comply with the design requirements for securing the Web servers. You also want to be able to verify the security settings and generate a report during routine maintenance. You want to achieve
these goals by using the minimum amount of administrative effort. What should you do?
A. Create a custom security template named Web.inf that contains the required security settings. Create a new organizational unit (OU) named Web Servers and move the Web servers into the new OU. Apply Web.inf to the Web Servers OU.
B. Create a custom security template named Web.inf that contains the required security settings, and deploy Web.inf to each Web server by using Security Configuration and Analysis.
C. Create an image of a Web server that has the required security settings, and replicate the image to each Web server.
D. Manually configure the required security settings on each Web server.
Answer: B
Explanation:
The easiest way to deploy multiple security settings to a Windows 2003 computer is to create a security template with all the required settings and import the settings using the Security Configuration and Analysis tool.
Incorrect Answers:
A: The web servers aren't members of the domain. Therefore they cannot be moved to an OU in Active Directory.
C: We cannot use imaging in this way.
D: This is a long way of doing it. A security template would simply the task.

QUESTION 10
You are the network administrator for Certkiller. The network contains a Windows Server 2003 Web server that hosts the company intranet. The human resources department uses the server to publish information relating to vacations and public holidays. This information does not need to be secure. The finance department wants to publish payroll information on the server. The payroll information will be published in a virtual directory named Payroll, which was created under the default Web site on the server. The company's written security policy states that all payroll-related information must be encrypted on the network. You need to ensure that all payroll-related information is encrypted on the network. To preserve performance, you need to ensure that other information is not encrypted unnecessarily. You obtain and install a server certificate. What else should you do?
A. Select the Require secure channel (SSL) check box for the default Web site.
B. Assign the Secure Server (Require Security) IPSec policy option for the server.
C. Select the Encrypt contents to secure data check box for the Payroll folder.

D. Select the Require secure channel (SSL) check box for the Payroll virtual directory.
Answer: D
Explanation:
Short for Secure Sockets Layer, a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with https: instead of http:.
Incorrect Answers:
A: This will encrypt all data from the web server. We only need to encrypt the payroll data.
B: This will encrypt all data from the web server. We only need to encrypt the payroll data.
C: This will encrypt the data on the hard disk using EFS. It won't encrypt the data as it is transferred over the network.

QUESTION 11
You are a network administrator for Certkiller Inc. The network consists of a single Active Directory forest as shown in the exhibit.

Your company's written security policy requires that all domain controllers in the child1.Certkiller.com domain must accept a LAN Manager authentication level of only NTLMv2. You also want to restrict the ability to start a domain controller to the Domain Admins group. You need to configure the domain controllers in the child1.Certkiller.com domain to meet the new security requirements. Which two actions should you take? (Each correct answer presents part of the solution. Choose two)
A. Import the Rootsec.inf security template into the Default Domain Controllers Policy Group Policy object (GPO) on the child1.Certkiller.com domain.
B. Import the Rootsec.inf security template into the Default Domain Policy Group Policy object (GPO) in the child1.Certkiller.com domain.
C. Import the Securedc.inf security template into the Default Domain Controllers Policy Group Policy object (GPO) in the child1.Certkiller.com domain.
D. Import the Securedc.inf security template into the Default Domain Policy Group Policy object (GPO) in the child1.Certkiller.com domain.
E. Run the system key utility (syskey) on each domain controller in the child1.Certkiller.com domain. In the Account Database Key dialog box, select the Password Startup option.

F. Run the system key utility (syskey) on each domain controller in the child1.Certkiller.com domain. In the Account Database Key dialog box, select the Store Startup Key Locally option.
Answer: C, E
Explanation:
Secure (Secure*.inf) Template
The Secure templates define enhanced security settings that are least likely to impact application compatibility. For example, the Secure templates define stronger password, lockout, and audit settings. Additionally, the Secure templates limit the use of LAN Manager and NTLM authentication protocols by configuring clients to send only NTLMv2 responses and configuring servers to refuse LAN Manager responses.
• In order to apply Securews.inf to a member computer, all of the domain controllers that contain the accounts of all users that log on to the client must run Windows NT 4.0 Service Pack 4 or higher.
The system key utility (SYSKEY)
A security measure used to restrict logon names to user accounts and access to computer systems and resources. By running the syskey utility with the Password startup option, the account information in the directory services is encrypted and a password needs to be entered during system start. The start of the Domain Controllers is therefore restricted to everybody with this password.
Reference:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/s

System key option	Relative security level	Description
System Generated Password, Store Startup Key Locally	Secure	Uses a computer-generated random key as the system key and stores an encrypted version of the key on the local computer. This option provides strong encryption of password information in the registry, and it enables the user to restart the computer without the need for an administrator to enter a password or insert a disk.
Administrator generated password, **Password Startup**	More secure	Uses a computer-generated random key as the system key and stores an encrypted version of the key on the local computer. The key is also protected by an administrator-chosen password. Users are prompted for the system key password when the computer is in the initial startup sequence. The system key password is not stored anywhere on the computer.
System Generated Password, Store Startup Key on Floppy Disk	Most secure	Uses a computer-generated random key and stores the key on a floppy disk. The floppy disk that contains the system key is required for the system to start, and it must be inserted at a prompt during the startup sequence. The system key is not stored anywhere on the computer.

Incorrect Answers:
A: The Rootsec.inf security template defines permissions for the root of the system drive. This template can be used to reapply the root directory permissions to other volumes.
B: The Rootsec.inf security template defines permissions for the root of the system drive. This template can be used to reapply the root directory permissions to other volumes.
D: We need to apply the policy to the domain controllers container, not the entire domain.
F: The System Key Utility (syskey) is used to encrypt the account password information that is stored in the SAM database or in the directory services. By selecting "Store Key locally" the computer stores an encrypted version of the key on the local computer. This doesn't help in controlling the start of the Domain Controllers.

QUESTION 12
You are a network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. The domain name is Certkiller.com. The network contains three Windows Server 2003 domain controllers. You are creating the recovery plan for the company. According to the existing backup plan, domain controllers are backed up by using normal backups each night. The normal backups of the domain

controllers include the system state of each domain controller. Your recovery plan must incorporate the following organization requirements:
• Active Directory objects that are accidentally or maliciously deleted must be recoverable.
• Active Directory must be restored to its most recent state of quickly as possible.
• Active Directory database replication must be minimized.
You need to create a plan to restore a deleted organizational unit (OU). Which two actions should you include in your plan? (Each correct answer presents part of the solution. Choose two)
A. Restart a domain controller in Directory Services Restore Mode.
B. Restart a domain controller in Safe Mode.
C. Use the Ntdsutil to perform an authorities restore operation of the Active Directory database.
D. Restore the system state by using the Always replace the file on my computer option.
E. Use the Ntdsutil utility to perform an authoritative restore operation of the appropriate subtree.
Answer: A, E
Explanation:
If an OU gets deleted from the Active Directory, we can restore it from a backup of the system state data. Directory Services Restore Mode is a sort of safe mode in which we can boot a domain controller without loading the Active Directory. This will enable us to restore all or part of the Active Directory database. To ensure that the deleted OU isn't deleted again by replication from another domain controller, we must use the Ntdsutil utility to mark the restored subtree as authoritative.
Incorrect Answers:
B: To restore part of the Active Directory, we must start a domain controller in Directory Services Restore Mode, not safe mode.
C: We don't need to restore the entire Active Directory database; we can just restore part of it.
D: This will overwrite the existing Active Directory database.

QUESTION 13
You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. The network contains 10 domain controllers and 50 servers in application server roles. All servers run Windows Server 2003. The application servers are configured with custom security settings that are specific to their roles as application servers. Application servers are required to audit account logon events, object access events,
and system events. Application servers are required to have passwords that meet complexity requirements, to enforce password history, and to enforce password aging. Application servers must also be protected against man-in-the-middle attacks during authentication. You need to deploy and refresh the custom security settings on a routine basis. You also need to be able to verify the custom security settings during audits. What should you do?
A. Create a custom security template and apply it by using Group Policy.
B. Create a custom IPSec policy and assign it by using Group Policy.
C. Create and apply a custom Administrative Template.
D. Create a custom application server image and deploy it by using RIS.
Answer: A
Explanation:
The easiest way to deploy multiple security settings to a Windows 2003 computer is to create a security template with all the required settings and import the settings into a group policy. We can also use secedit to analyze the current security settings to verify that the required security settings are in place.
Incorrect Answers:

B: An IPSec policy will not configure the required auditing policy.
C: We need a security template, not an administrative template.
D: This will create multiple identical machines. We cannot use RIS images in this scenario.

QUESTION 14
You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. All computers on the network are members of the domain. The domain contains a Windows Server 2003 computer named Certkiller5. You are planning a public key infrastructure (PKI) for the company. You want to deploy a certification authority (CA) on Certkiller5. You create a new global security group named Cert Administrators. You need to delegate the tasks to issue, approve, and revoke certificates to members of the Cert Administrators group. What should you do?
A. Add the Cert Administrators group to the Cert Publishers group in the domain.
B. Configure the Certificates Templates container in the Active Directory configuration naming context to assign the Cert Administrators group the Allow - Write permission.
C. Configure the CertSrv virtual directory on Certkiller5 to assign the Cert Administrators group the Allow
D. Assign the Certificate Managers role to the Cert Administrators group.
Answer: D
Explanation:
To be able to issue, approve and revoke certificates, the Cert Administrators group needs to be assigned the role of Certificate Manager. The following table describes different roles and their associated permissions.

Roles and groups	Security permission	Description
CA Administrator	**Manage CA** permission	Configure and maintain the CA. This is a CA role and includes the ability to assign all other CA roles and renew the CA certificate.
Certificate Manager	**Issue and Manage Certificates** permission	Approve certificate enrollment and revocation requests. This is a CA role. This role is sometimes referred to as CA Officer.
Backup Operator	**Back up file and directories** and **Restore file and directories** permissions	Perform system backup and recovery. This is an operating system role.
Auditor	**Manage auditing and security log** permission	Configure, view, and maintain audit logs. This is an operating system role.
Enrollees	Authenticated Users	Enrollees are clients who are authorized to request certificates from the CA. This is not a CA role.

QUESTION 15
You are a network administrator for Certkiller. The network contains a perimeter network. The perimeter network contains four Windows Server 2003, Web Edition computers that are configured as a Network Load Balancing cluster. The cluster hosts an e-commerce Web site that must be available 24 hours per day. The cluster is located in a physically secure data center and uses an Internet-addressable virtual IP address. All servers in the cluster are configured with Hisecws.inf templates. You need to implement protective measures against the cluster's most significant security vulnerability. What should you do?
A. Use Encrypting File System (EFS) for all files that contain confidential data stored on the cluster.
B. Use packet filtering on all inbound traffic to the cluster.
C. Use Security Configuration and Analysis regularly to compare the security settings on all servers in the cluster with the baseline settings.
D. Use intrusion detection on the perimeter network.
Answer: B
Explanation:

The most sensitive element in this case is the network card that uses an Internet-addressable virtual IP address. The question doesn't mention a firewall implementation or and intrusion detection system (Usually Hardware). Therefore, we should set up packet filtering.
REF:
Deploying Network Services (Windows Server 2003 Reskit) Using a Perimeter Network IP packet filtering
You can configure packet filtering, the earliest implementation of firewall technology, to accept or deny specific types of packets. Packet headers are examined for source and destination addresses, TCP and UDP port numbers, and other information. Packet filtering is a limited technology that works best in clear security environments where, for example, everything outside the perimeter network is not trusted and everything inside is. You cannot use IP packet filtering when IP packet payloads are encrypted because the port numbers are encrypted and therefore cannot be examined. In recent years, various vendors have improved on the packet filtering method by adding intelligent decision-making features to the packet-filtering core, thus creating a new form of packet filtering called stateful protocol inspection.

QUESTION 16
You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. All computers on the network are members of the domain. All servers run Windows Server 2003 and all client computers run Windows XP Professional. You are planning a security update infrastructure. You need to find out which computers are exposed to known vulnerabilities. You need to collect the information on existing vulnerabilities for each computer every night. You want this process to occur automatically. What should you do?
A. Schedule the secedit command to run every night.
B. Schedule the mbsacli.exe command to run every night.
C. Install Microsoft Baseline Security Analyzer (MBSA) on one of the servers. Configure Automatic Updates on all other computers to use that server.
D. Install Software Update Services (SUS) on one of the servers. Configure the SUS server to update every night.
Answer: B
Explanation:
We can schedule the mbsacli.exe command to periodically scan for security vulnerabilities. Running a Scan Against All Computers in a Domain Using a Batch File:
Create a batch file called mbsascan.cmd with the following text:
@Echo Off
CLS
Set MBSA_Install_Path="C:\Program Files\Microsoft Baseline Security Analyzer"
cls
cd %MBSA_Install_Path%
mbsacli.exe /d edc /n password
Echo Scan complete
Pause
Exit
To run the tool from the command line (from the MBSA installation folder), type mbsacli.exe, and use the following parameters. To Select Which Computer to Scan
• no option - Scan the local computer.
• r /c domainname\computername- Scan the named computer.
• /i xxx.xxx.xxx.xxx - Scan the named IP address.

• /r xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx - Scan the range of IP addresses.
• /d domainname - Scan the named domain.
To Select Which Scan Options to Not Perform Note You can concatenate these options. For example, you can use/n OS + IIS + Updates.
• /n IIS - Skip IIS checks.
• /n OS - Skip Windows operating system checks.
• /n Password - Skip password checks.
• /n SQL - Skip SQL checks.
• /n Updates - Skip security update checks.
Security Update Scan Options
• /sus server - Check only for security updates that are approved at the specified SUS server.
• /s 1 - Suppress security update check notes.
• /s 2 - Suppress security update check notes and warnings.
• /nosum - Security update checks will not test file checksums.
To Specify the Output File Name Template
• /o domain - computername (date)
To Display the Results and Details
• /e - List the errors from the latest scan.
• /l - List all the reports that are available.
• /ls - List the reports from the latest scan.
• /lr report name - Display an overview report.
• /ld report name - Display a detailed report.
Miscellaneous Options
• /? - Usage help.
• /qp - Do not display progress.
• /qe - Do not display error list.
• /qr - Do not display report list.
• /q - Do not display progress, error list, or report list.
• /f - Redirect the output to a file.
MBSA is the graphical interface of Mbsacli.exe. This can be installed and run on Microsoft(r) Windows(r) 2000 Server, Windows 2000 Professional, Windows XP Home Edition, Windows XP Professional, and Windows Server 2003. The tool can be run over the network against Microsoft Windows NT(r) 4.0 Server and Windows NT 4.0 Workstation, Windows 2000 Server, Windows 2000 Workstation, Windows XP Professional and Home Edition, and Windows Server 2003. MBSA does not run on or against Windows 95, 98 or Me systems.
• You can use MBSA by using the graphical user interface (GUI) or from the command line. The GUI executable is Mbsa.exe and the command line executable is Mbsacli.exe.
• MBSA uses ports 138 and 139 to perform its scans.
• MBSA requires administrator privileges on the computer that you scan. The options /u (username) and /p (password) can be used to specify the username to run the scan. Do not store user names and passwords in text files such as command files or scripts.
• MBSA requires the following software:
• Windows NT 4.0 SP4 and above, Windows 2000, or Windows XP (local scans only on Windows XP computers that use simple file sharing)
• IIS 4.0, 5.0 (required for IIS vulnerability checks)
• SQL 7.0, 2000 (required for SQL vulnerability checks)
• Microsoft Office 2000, XP (required for Office vulnerability checks)

• The following services must be installed/enabled: Server service, Remote Registry service, File & Print Sharing
• The section Additional Information later in this How To includes tips on working with MBSA.
Scanning for Security Updates and Patches You can run Mbsa.exe and Mbsacli.exe with options to verify the presence of security patches.

QUESTION 17
You are the security analyst 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 XP Professional. The perimeter network contains an application server, which is accessible to external users.
You view the logs on your intrusion-detection system (IDS) and on the router and discover that very large numbers of TCP SYN packets are being sent to the application server. The application server is responding with SYN-ACK packets to several different IP addresses, but is not receiving ACK responses. You note that all incoming SYN packets appear to be originating from IP addresses located within the perimeter network's subnet address range. No computers in your perimeter network are configured with these IP addresses. The router logs show that these packets are originating from locations on the Internet. You need to prevent this type of attack from occurring until a patch is made available from the application vendor. Because of budget constraints, you cannot add any new hardware or software to the network. Your solution cannot adversely affect legitimate traffic to the application server. What should you do?
A. Relocate the application server to the company intranet. Configure the firewall to allow inbound and outbound traffic on the ports and protocols used by the application.
B. Configure network ingress filters on the router to drop packets that have local addresses but that appear to originate from outside the company network.
C. Create access control lists (ACLs) and packet filters on the router to allow perimeter network access to only authorized users and to drop all other packets originating from the Internet.
D. Configure the IDS on the perimeter network with a response rule that sends a remote shutdown command to the application server in the event of a similar denial-of-service attack.
Answer: B
Explanation:
This type of attack is known as a Denial of Service Attack.
Dropping spoofed packets
In an ideal world, each router would be configured with ingress filters that would drop packets arriving from "internal" networks whose source address was not a member of the set of network addresses that this router serves. The majority of routers could be so configured. Backbone routers and edge routers for complex topologies probably could not be configured with such filters. These ingress filters should be required as part of a "good neighbor policy." Ingress filters would not totally eliminate denial of service attacks but could greatly reduce such attacks. An attacker could still spoof an address within a local subnet, but that would permit backtracking the packets to the source subnet. Cisco's unicast reverse path forwarding also can be used to block spoofed packets at edge routers. Routers that implement ingress filtering will not forward the packets sent by a mobile host in a foreign network.

QUESTION 18
You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. All computers on the network are members of the domain. The network contains a Windows Server 2003 computer named CertkillerCA. The company uses an enterprise certification authority (CA) on CertkillerCA to issue certificates. A certificate to encrypt files is auto enrolled to all users. The

certificate is based on a custom Encryption File System (EFS) certificate template. The validity period if the certificate is set to two years. Currently, the network is configured to use data recovery agents. You are planning to implement key archival for the keys that users use to decrypt files. You configure the CA and the custom EFS certificate template to enable key archival of the encryption private keys. You need to ensure that the private EFS key of each user who logs on to the domain is archived. What should you do?
A. Configure a new issuance policy for the custom EFS certificate template.
B. Configure the custom EFS certificate template to reenroll all certificate holders.
C. Select the Automatically Enroll Certificates command in the Certificates console.
D. Configure a logon script that runs the gpupdate.exe /force command for the users.
Answer: C
Explanation:
Key Archival and Management in Windows Server 2003
Reference:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/operate/kyacws03.asp
EFS always attempts to enroll for the Basic EFS template. The EFS driver generates an auto enrollment request that Auto enrollment tries to fulfill. For customers that want to ensure that a specific template is used for EFS (such as to include key archival), the new template should supercede the Basic EFS template. This will ensure that Auto enrollment will not attempt enrollment for Basic EFS any more.
Key Archival
The private key database is the same as the database used to store the certificate requests. The Windows Server 2003 Certification Authority database has been extended to support storing the encrypted private key along with the associated encrypted symmetric key and issued certificate. The recovery blob will be stored in the same row as the signed certificate request and any other information the CA persists in its database for each request transaction. The actual encrypted blob is stored as an encrypted PKCS #7 blob. The Microsoft Certification Authority uses the JET database engine upon which various JET utilities may be used for maintenance purposes.

QUESTION 19
You are the network administrator for Certkiller. The network consists of a single Active Directory forest. The forest contains Windows Server 2003 servers and Windows XP Professional computers. The forest consists of a forest root domain named Certkiller.com and two child domains named child1.Certkiller.com and child2.Certkiller.com. The child1.Certkiller.com domain contains a member server named CertkillerSrvC. You configure CertkillerSrvC to be an enterprise certification authority (CA), and you configure a user certificate template. You enable the Publish certificate in Active Directory setting in the certificate template. You instruct users in both the child1.Certkiller.com and the child2.Certkiller.com domains to enroll for user certificates. You discover that the certificates for user accounts in the child1.Certkiller.com domain are being published to Active Directory, but the certificates for user accounts in the child2.Certkiller.com domain are not. You want certificates issued by CertkillerSrvC to child2.Certkiller.com domain user accounts to be published in Active Directory. What should you do?
A. Configure user certificate auto enrollment for all domain user accounts in the Certkiller.com.
B. Configure user certificate auto enrollment for all domain user accounts in the child2.Certkiller.com domain.
C. Add CertkillerSrvC to the Cert Publisher group in the Certkiller.com domain.
D. Add CertkillerSrvC to the Cert Publisher group in the child2.Certkiller.com domain.
Answer: D
Explanation:

The problem here is that CertkillerSrvC doesn't have the necessary permission to publish certificates for users in child2.Certkiller.com. We can solve this problem by adding CertkillerSrvC to the Cert Publisher group in the child2.Certkiller.com domain.
Reference:
http://support.microsoft.com/default.aspx?scid=kb;en-us;219059

QUESTION 20
You are a network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. The functional level of the domain is Windows Server 2003. All domain controllers run Windows Server 2003. The domain controllers are e configured as shown in the following table.

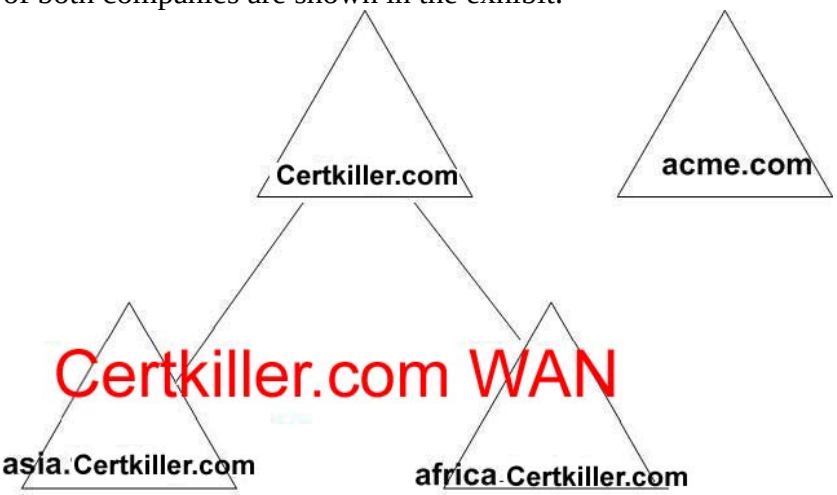
Server name	Server role
CertkillerSrvA	Global catalog server, schema master, domain naming master
CertkillerSrvB	Domain controller, infrastructure master, PDC emulator
CertkillerSrvC	Domain controller
CertkillerSrvD	Global catalog server, relative ID (RID) master

You plan to take CertkillerSrvD offline for maintenance. Another network administrator plans to add 1,250 new user accounts while CertkillerSrvD is offline. You need to ensure that the network administrator can add the user accounts while CertkillerSrvD is offline. You also need to ensure that there is no disruption of user account creation after CertkillerSrvD is brought back online. Which two actions should you take? (Each correct answer presents part of the solution. Choose two)
A. Connect to CertkillerA by using the Ntdsutil utility.
B. Connect to CertkillerSrvD by using the Ntdsutil utility.
C. Remove the global catalog server role from CertkillerSrvD.
D. Add the global catalog server role to CertkillerSrvD.
E. Transfer the RID master role.
Answer: A, E
Explanation:
The RID master is assigned to allocate unique sequences of relative IDs to each domain controller in its domain. As the domain controllers use the IDs allocated, they contact the RID master and are allocated additional sequences as needed. At any time, the RID master role can be assigned to only one domain controller in each domain. The Relative ID is part of a security ID (SID) that uniquely identifies an account or group within a domain. We will be creating 1250 new user accounts so the domain controller will need to contact the RID master to obtain more RIDs. We can transfer the RID master role using the ntdsutil utility.
Incorrect Answers:
B: We need to connect to the computer we will be transferring the role to, not from.
C: We have a Global Catalog on CertkillerSrvA. We don't need another one.
D: CertkillerSrvD is already a global catalog server.
Reference:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_adTransRIDMaster.asp

---

QUESTION 21
You are the network administrator for Certkiller. The network consists of a single Active Directory forest that contains three domains. The functional level of all three domains is Windows 2000 native. Your company is merging with a company named Acme. The Acme., network consists of a single Active Directory forest that

contains one domain named acme.com. The functional level of the domain is Windows 2000 native. The forests of both companies are shown in the exhibit.



You need to allow users in each forest to fully access resources in the domains of the other forest. In addition, users must be able to log on between domains by using Kerberos authentication. You need to ensure that users can continue to access all resources by using their existing user accounts. What should you do?

A. Demote the Windows 2000 domain controllers in the acme.com domain to become member servers. Promote these servers into the Certkiller.com domain.

B. Demote the Windows 2000 domain controllers in the acme.com domain to become member servers. Upgrade these servers to Windows Server 2003.
Promote the upgraded computers to become domain controllers for a new domain tree in the Certkiller forest.

C. Upgrade the Windows 2000 domain controllers in the acme.com domain to Windows Server 2003. Create external trust relationships between the root domains of each forest.

D. Upgrade all domain controllers in both forests to Windows Server 2003. Raise the functional level of both forests to Windows Server 2003. Create a forest trust relationship between the root domains of each forest.

Answer: D

Explanation:

To enable users in each forest to fully access resources in the domains of the other forest and log on to either domain with Kerberos authentication, we need to create a forest trust between the two forests. To create a forest trust, the forests must be in Windows 2003 domain functional level. This requires that all domain controllers in each domain are running Windows server 2003.

Incorrect Answers:

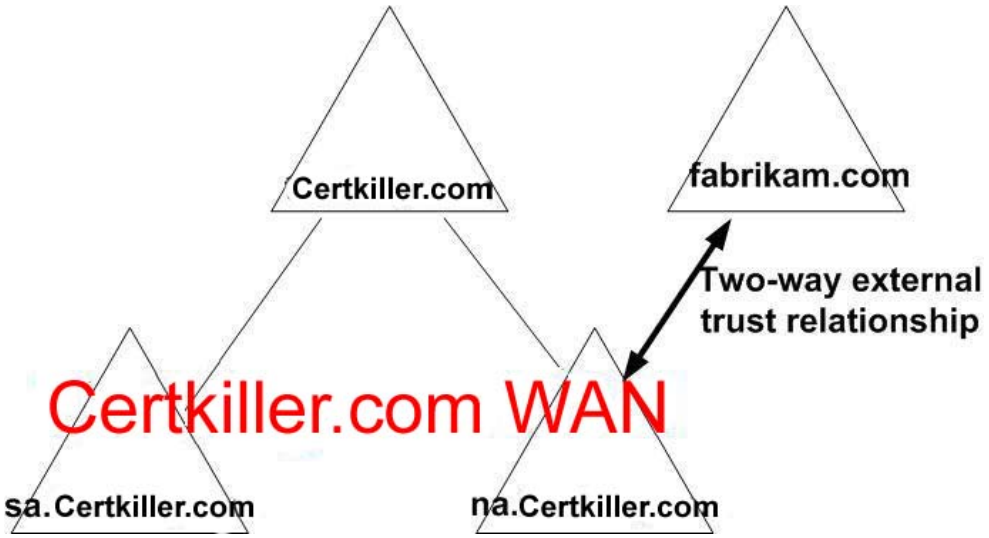
A: This will decommission the acme.com domain/forest. This isn't a requirement.

B: This will decommission the acme.com forest. This isn't a requirement.

C: We need a forest trust to enable Kerberos authentication across the trust link.

QUESTION 22

You are the network administrator for your company. The company consists of two subsidiaries named Certkiller., and Fabrikam, Inc. The network consists of two Active Directory forests. All servers run Windows Server 2003. The domain configuration is shown in the exhibit.



The North American department in the company is renamed to North wind Traders. You rename the NA.Certkiller.com domain to northwindtraders.com. You change the NetBIOS name for the domain to northwindtraders. The northwindtraders.com domain is a second tree in the Certkiller.com forest. After the domain is renamed, users in the northwindtraders.com domain report that they cannot access any shared resourced in the fabrikam.com domain. In addition, users in the fabrikam.com domain report that they cannot access shared resources in the northwindtraders.com domain. You need to re-enable the sharing of resources between the northwindtraders.com domain and the fabrikam.com domain. What should you do?

A. Change the NetBIOS name for the northwindtraders.com domain to NA.

B. Delete and re-create the two one-way trust relationships between the northwindtraders.com domain and the fabrikam.com domain.

C. Configure conditional forwarding on the DNS server in the fabrikam.com domain to forward requests for the northwindtraders.com domain to the DNS servers in the Certkiller.com domain.

D. Reset the computer account passwords on all of the domain controllers in the northwindtraders.com domain.

Answer: B

Explanation:

After renaming the domain, the external trust relationships will need to be recreated.

Creating Necessary Shortcut Trust Relationships

You can reposition any domain within the domain tree hierarchy of a forest, with the exception of the forest root domain. Remember that although the forest root domain can be renamed (its DNS and NetBIOS names can change), it cannot be repositioned in such a way that you designate a different domain to become the new forest root domain. If your domain rename operation involves restructuring the forest through repositioning of the domains in the domain tree hierarchy as opposed to simply changing the names of the domains in-place, you first need to create the necessary shortcut trust relationships between domains such that the new forest structure has two-way transitive trust paths between every pair of domains in the target forest, just as your current forest does.

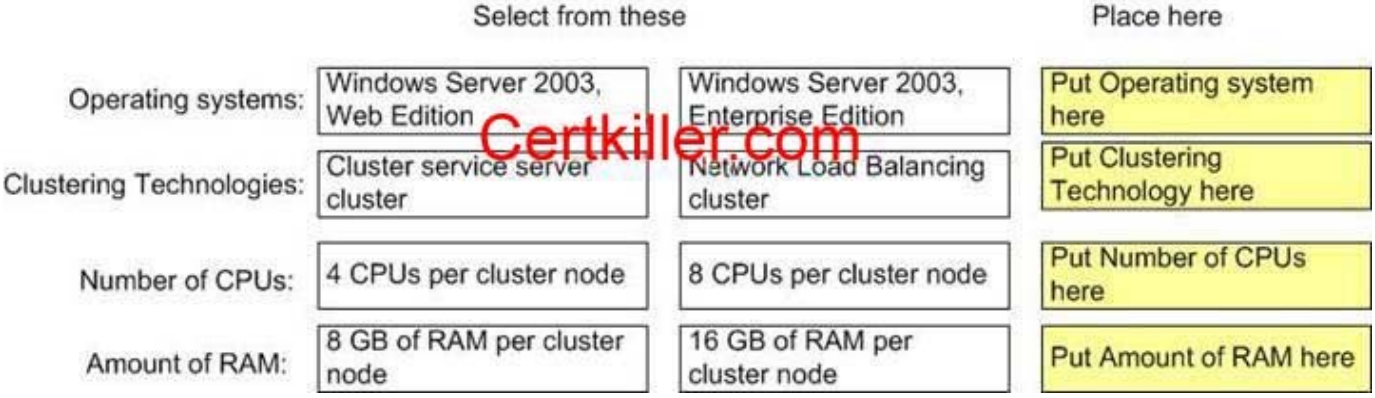
Forest restructuring

Using domain rename, you can also restructure the hierarchy of domains in your forest so that a domain residing in one domain tree In DNS, the inverted hierarchical tree structure that is used to index domain names. Domain trees are similar in purpose and concept to the directory trees used by computer filing systems for disk storage. For example, when numerous files are stored on disk, directories can be used to organize the files into logical collections. When a domain tree has one or more branches, each branch can organize domain names used in the namespace into logical collections. In Active Directory, a hierarchical structure of one or more

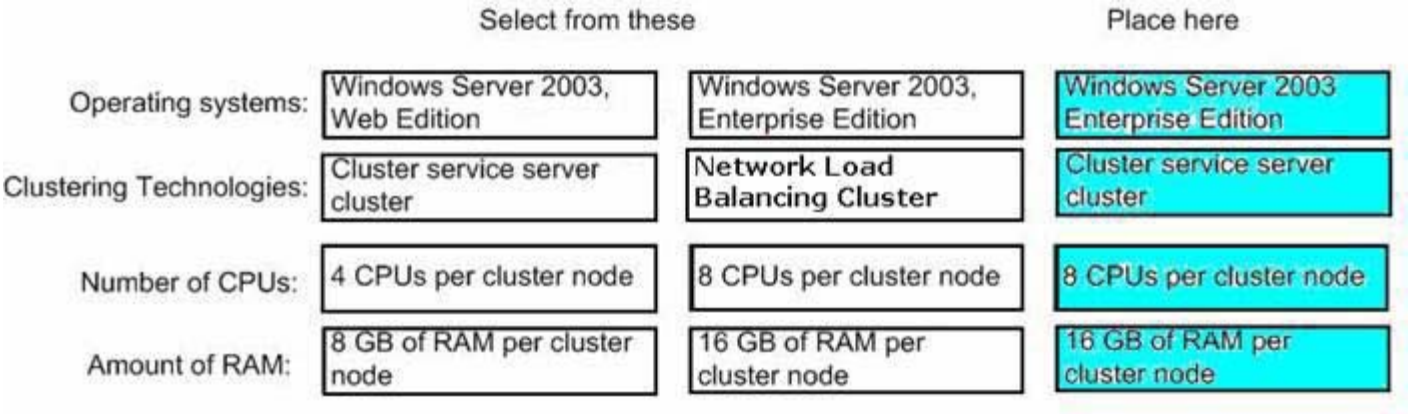
domains, connected by transitive, bidirectional trusts, that forms a contiguous namespace. Multiple domain trees can belong to the same forest. Domains can be moved to another domain tree. Restructuring a forest allows you to move a domain anywhere
within the forest in which it resides (except the forest root domain). This includes the ability to move a domain so that it becomes the root of its own domain tree. You can use the domain rename utility (Rendom.exe) to rename or restructure a domain. The Rendom.exe utility can be found in the Valueadd\Msft\Mgmt\Domren directory on the operating system installation CD. A domain rename will affect every domain controller in your forest and is a multistep process that requires a detailed understanding of the operation. Renaming a domain controller requires that you first provide a FQDN as a new computer name for the domain controller. All of the computer accounts for the domain controller must contain the updated SPN attribute and all the authoritative DNS servers for the domain name must contain the host (A) resource record for the new computer name. Both the old and new computer names are maintained until you remove the old computer name. This ensures that there will be no interruption in the ability of clients to locate or authenticate to the renamed domain controller, except when the domain controller is restarted Renaming domain controllers The SPN value of the computer account must be replicated to all domain controllers for the domain and the DNS resource records for the new computer name must be distributed to all the authoritative DNS servers for the domain name. If the updates and registrations have not occurred prior to removing the old computer name, then some clients may be unable to locate this computer using the new or old name.
References:
Server Help Window Server 2003 MS White paper Step-by-Step Guide to Implementing Domain Rename

---

QUESTION 23
You are the network administrator for Certkiller. The company needs to implement a Web application that uses two Microsoft SQL Server 2000 database instances. You expect the size of each database instance to be between 200 GB and 300 GB at any given time. Several tables in each database contain data that is updated once every few seconds, on average. You estimate that each database instance requires 7 GB of memory, and that each instance requires 70 percent usage of four CPUs, on average. Using two servers CertkillerSQL1 and CertkillerSQL2, you need to plan the minimum highly available server infrastructure for the databases that meets the requirements. You also want to minimize the costs and administrative effort required to maintain the infrastructure. What should you do?
To answer, drag the appropriate configuration settings to the Cluster Configuration.



Answer:



Explanation:
We are running two different databases so we need a Cluster Service Cluster rather than a Network Load Balancing cluster (We can only use NLB if the two servers are hosting identical content). For a Cluster Service Cluster, we need to use Windows Server 2003 Enterprise Edition. We need to ensure that the database will still run if one of the cluster nodes fails. Therefore each cluster node will need enough resources to run both databases. Each database requires four CPUs, so each cluster node must have 8 CPUs in order to run both databases in the event of a cluster node failure. Each database requires 7 GB of RAM so each cluster node must have at least 14 GB of RAM in order to run both databases in the event of a cluster node failure (our only option above 14GB or RAM is to put 16GB of RAM in each cluster node).

QUESTION 24
You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. The functional level of the domain is Windows Server 2003. The domain contains a secure site and a main office site, as shown in the exhibit.

All domain controllers are configured as shown in the following table.

Drive	Contents
C	Boot partition, system partition, Active Directory database log files
D	Active Directory database
E	Files and folders

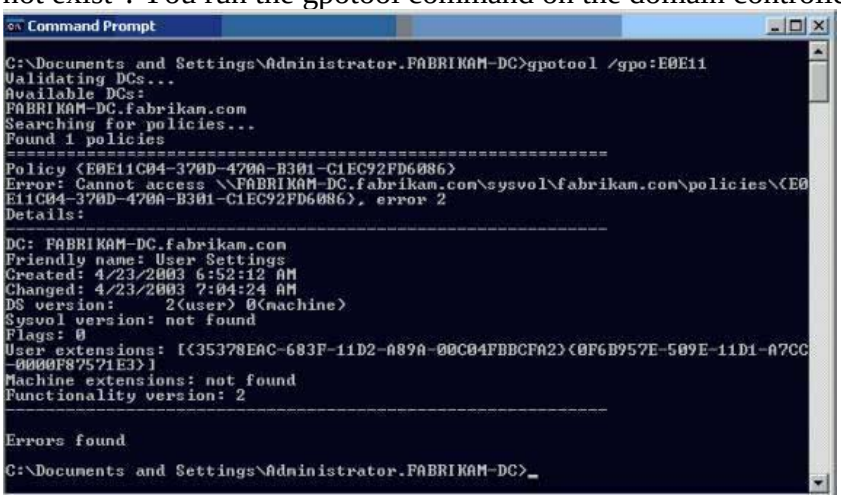
The motherboard on Certkiller2 fails and Certkiller2 is taken offline. One week later, an administrator connects to Certkiller3 and seizes the schema master role. You need to access files on drive E on Certkiller2. You replace the motherboard on Certkiller2 and bring Certkiller2 online on an isolated subnet. You need to be able to bring Certkiller2 back into the secure site as quickly as possible in order to access the files. What should you do?
A. Perform a full format of drive D on Certkiller2. Transfer the schema master role to a domain controller in the MainOffice site. Remove references to Certkiller2 from Active Directory by using the Ntdsutil utility and the

ADSIEdit utility on Certkiller1.
B. Perform a full format of drive C on Certkiller2. Reinstall the operating system on Certkiller2. Remove references to Certkiller2 from Active Directory by using the Ntdsutil utility and the ADSIEdit utility on Certkiller1.
C. Perform a full format of drive E on Certkiller2. Run the dcpromo command on Certkiller2. Transfer the schema master role to a domain controller in the MainOffice site. Join Certkiller2 to the domain.
D. Perform a full format of drive C on Certkiller2. Transfer the schema master role to a domain controller in the MainOffice site. Remove references to Certkiller2 from Active Directory by using the Ntdsutil utility and the ADSIEdut utility on Certkiller1.
Answer: B
Explanation:
We have seized the schema master role from Certkiller2 on Certkiller3. Therefore, we don't want to bring Certkiller2 back online with it's old schema master role. Having two schema masters will cause problems in the forest. To bring Certkiller2 back online, we should format the C drive and reinstall the operating system. We should also 'clean' the Active Directory database by removing references to Certkiller2 from Active Directory by using the Ntdsutil utility and the ADSIEdit utility on another domain controller.
Incorrect Answers:
A: We need to reinstall the operating system, so we should format drive C, not drive D.
C: Formatting drive E will erase the data we want to access.
D: The schema master role has already been transferred. We need to reinstall the operating system after formatting drive C.

QUESTION 25
You are a network administrator for Certkiller. Your network consists of a single Active Directory domain named Certkiller.com. All servers run Windows Server 2003. A help desk user reports that a user object was accidentally deleted and the user can no longer log on to the domain and access resources. You confirm that the user object was included in the most recent backup. You need to enable the user to log on to the domain. You must ensure that the user retains access to resources. What should you do?
A. Install a new domain controller. Install Active Directory from media by using the most recent backup. Manually initiate replication.
B. Decrease the garbage collection interval. Perform a nonauthorative restoration of Active Directory by using the most recent backup.
C. Perform a nonauthorative restoration of Active Directory by using the most recent backup. Authoritatively restore the user object that was deleted.
D. Re-create a user object that has the same user principal name (UPN) as the user object that was deleted. Authoritatively restore this user object.
Answer: C
Explanation:
If you inadvertently delete or modify objects stored in the Active Directory service, and those objects are replicated or distributed to other servers, you will need to authoritatively restore those objects so they are replicated or distributed to the other servers. If you do not authoritatively restore the objects, they will never get replicated or distributed to your other servers because they will appear to be older than the objects currently on your other servers. Using the Ntdsutil utility to mark objects for authoritative restore ensures that the data you want to restore gets replicated or distributed throughout your organization. On the other hand, if your system disk has failed or the Active Directory database is corrupted, then you can simply restore the data no authoritatively without using the Ntdsutil utility. Active Directory gives network users access to permitted

resources anywhere on the network using a single logon process. It provides network administrators with an intuitive, hierarchical view of the network and a single point of administration for all network objects. Active directory service data can be restored using one of three restore methods:
• Primary restore
• Normal (nonauthoritative) restore
• Authoritative restore
In Backup, a type of restore operation performed on an Active Directory domain controller in which the objects in the restored directory are treated as authoritative, replacing (through replication) all existing copies of those objects. We need to restore the Active Directory database non-authoritatively, then from the restored copy of the database, we need to authoritatively restore the user object.
Incorrect Answers:
A: It isn't necessary to install a new domain controller.
B: We need to authoritatively restore the user object, otherwise AD replication will delete the user object again.
D: Creating a new user account won't work because the new user account will have a different SID from the deleted account.

QUESTION 26
You are the network administrator for Fabrikam, Inc. The network consists of a single Active Directory domain that contains one domain controller. All servers run Windows Server 2003. All client computers run Windows XP Professional. The company uses Group Policy objects (GPOs) to configure user and computer settings. A new user named Dr. King reports that his Windows desktop is different from others in the company and that he does not have access to the same applications as other users. You discover that none of the user settings from any GPOs are in effect in Dr. King's computer after Dr. King logs on. You instruct Dr. King to run the gpresult command, and he reports that he receives the following error message: "INFO: The group policy object does not exist". You run the gpotool command on the domain controller and receive the output shown in the exhibit.



You need to ensure that Group Policy settings can be applied correctly. What should you do?
A. Run the gpupdate /force command on the domain controller.
B. Run the gpupdate /force command on Dr. King's computer.
C. Restore the system state on the domain controller from a valid backup.
D. Restore the backup state on Dr. King's computer from a valid backup.
Answer: C
Explanation:
We can see from the exhibit that there is a problem with the group policy. It seems to have become corrupted.

To restore the group policy, we'll need to restore the system state data on a domain controller.
The gpotool is the Group Policy Object verification tool
Usage: gpotool [options]
Options:
/gpo:GPO[,GPO...] Preffered policies. Partial GUID and friendly name match accepted. If not specified, process all policies in the domain.
/domain:name Specify the DNS name for the domain hosting the policies. If not present, assume user's domain.
/dc:DC[,DC...] Preffered list of domain controllers. If not specified, find all controllers in the domain.
/checkacl Verify sysvol ACL. For faster processing, this step is skipped
/verbose Display detailed information.
Identifying the File-Based GPO Structure on the System Volume
1. On a domain controller in the domain identified above, determine which drive hosts the system volume (Sysvol).
2. Using Windows Explorer, open the Sysvol folder.
3. The following folders exist: Domain, Staging, Staging Areas, and Sysvol. Change to the Sysvol folder.
4. A folder with the name of the domain that the local domain controller is a member of should exist. Change to the following folder: Path to Sysvol\Sysvol\DomainName\Policies. A folder for each GPO created in the domain, each identified by its GUID, should exist.
5. Open the folder identified by the GUID of the GPO that you recorded in the previous section of this article.
Note:
The Group Policy structure on the system volume contains a Gpt.ini file that contains version information (of the GPO) and other optional data. Additionally, the file-based policy is broken into Machine and User folders with the appropriate policy for each. An Adm folder may also be present when software policies (administrative templates) are being used. Without access to the properties of a given GPO, the administrator can use other methods of attaining either the GUID for a known GPO or the friendly name of a GPO of which the administrator has the associated GUID.
Reference:
Troubleshooting Group Policy Application Problems. Microsoft Knowledge Base Article - 216359
Troubleshooting Group Policy Application Problems. Microsoft Knowledge Base Article - 250842

QUESTION 27
You are a network administrator for Certkiller. The company consists of a single Active Directory domain named Certkiller.com. All client computers run Windows XP Professional. The company's main office is located in Dallas. You are a network administrator at the company's branch office in Boston. You create a Group Policy object (GPO) that redirects the Start menu for users in the Boston branch office to a shared folder on a file server. Several users in Boston report that many of the programs that they normally use are missing from their Start menus. The programs were available on the Start menu he previous day, but did not appear when the users logged on today. You log on to one of the client computers. All of the required programs appear on the Start menu. You verify that users can access the shared folder on the server. You need to find out why the Start menu changed for these users. What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)
A. In the Group Policy Management Console (GPMC), select the file server that hosts the shared folder and a user account that is in the Domain Admins global group and run Resultant Set Of Policy (RSoP) in planning mode.
B. In the Group Policy Management Console (GPMC), select one of the affected user accounts and run

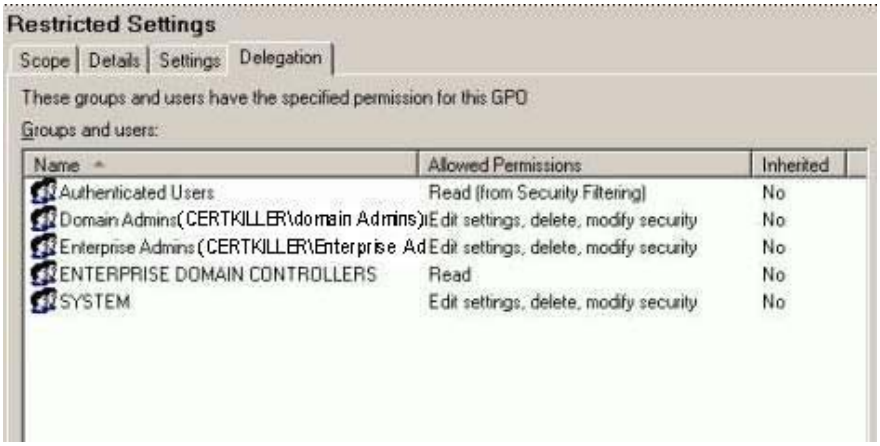
Resultant Set of Policy (RSoP) in logging mode.
C. On one of the affected client computers, run the gpresult command.
D. On one of the affected client computers, run the gpupdate command.
E. On one of the affected client computers, run the secedit command.
Answer: B, C
Explanation:
We need to view the effective group policy settings for the users or the computers that the users are using. We can use gpresult or RSoP.
Gpresult
Displays Group Policy settings and Resultant Set of Policy (RSoP) for a user or a computer.
RSoP overview Resultant Set of Policy (RSoP) is an addition to Group Policy
RSoP provides details about all policy settings that are configured by an Administrator, including Administrative Templates, Folder Redirection, Internet Explorer Maintenance, Security Settings, Scripts, and Group Policy Software Installation.
RSoP consists of two modes:
Planning mode and logging mode. With planning mode, you can simulate the effect of policy settings that you want to apply to a computer and user.
Logging mode reports the existing policy settings for a computer and user that is currently logged on.
Incorrect Answers:
A: We need to test the effective policy from a user's computer, not the file server.
D: Gpudate, is the tool used to refresh the policy settings in Windows XP and Windows Server 2003.
E: Secedit is the tool used to refresh the policy in Windows 2000 professional and server editions.

QUESTION 28
You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. You are testing Group Policy object (GPOs) on an organizational unit (OU) named Test. The Test OU contains a Windows XP Professional client computer that you use as a test computer. The domain contains a group named Security. You create a new GPO and configure the Computer Configuration section to grant the Security group the Change the system time user right. You log on to the test computer and discover that the setting you set through the GPO is not in effect. You need to apply the GPO settings immediately. What should you do?
A. Log off the test computer and log on again.
B. Log off the test computer. Create a test user account in the Test OU and then log on as the test user account.
C. On the test computer, run the gpresult command.
D. On the test computer, run the gpupdate /force command.
Answer: D
Explanation:
We need to apply the group policy immediately, rather than wait for the next group policy refresh interval. We can do this using the gpupdate /force command.
Gpupdate
Refreshes local Group Policy settings and Group Policy settings that are stored in Active Directory, including security settings. This command supersedes the now obsolete /refreshpolicy option for the secedit command.
The switch /force Ignores all processing optimizations and reapplies all settings.
Incorrect Answers:
A: We need to apply a computer policy, so we would need to restart the computer rather than just logging off.

B: There is no need to create another user account.
C: Gpresult is used to display the effective group policy settings. It does not apply group policy settings.

QUESTION 29
You are the network administrator for Certkiller GmBh. 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 Active Directory structure is shown in the Active Directory exhibit.

The company's written policy states that users in the manufacturing department are given only restricted access to settings and applications on their computers. The written policy also states that this limitation does not apply to members of a security group named Managers. You create a Group Policy object (GPO) named Restricted Settings and link the GPO to the domain. This GPO contains the policy settings required by the written company policy. You discover that the restricted settings apply to all users. You examine the Restricted Settings GPO by using the Group Policy Management Console (GPMC). The relevant information is shown in the GPMC exhibit.



You need to configure the network so that the written policy is enforced correctly. Which two actions should you take? (Each correct answer presents part of the solution. Choose two)
A. Unlink the Restricted Settings GPO from the domain. Link it to the Manufacturing organizational unit (OU).
B. Unlink the Restricted Settings GPO from the domain. Link it to the Company Users organizational unit (OU).

C. Assign the Authenticated Users group to the Deny - Apply Group Policy permission for the Restricted Settings GPO.
D. Assign the Managers group the Deny - Apply Group Policy permission for the Restricted Settings GPO.
Answer: A, D
Explanation:
The question states that the restricted settings should apply to users in the Manufacturing OU. The policy is currently linked to the domain which is why it is being applied to all users in the domain. We should unlink the policy from the domain and link it to the Manufacturing organizational unit (OU). Members of the Managers group should not receive the settings from the OU. We can fulfil this requirement by assigning the Managers group the Deny - Apply Group Policy permission for the Restricted Settings GPO.
Incorrect Answers:
B: The restricted settings should apply to users in the Manufacturing OU, not the Company Users OU.
C: This would prevent the policy applying to all users. The policy should apply to users in the Manufacturing OU.

QUESTION 30
You are the network administrator for Certkiller. The company has a main office and six branch offices. Each branch office employs fewer than 15 users. The network consists of a single Active Directory domain configured as a single site. All servers run Windows Server 2003. Domain controllers are located in the main office. All branch offices are connected to the main office by WAN connections. All users are required to change their password every 10 days. They are further restricted from reusing a password until after they have used five different passwords. You discover that users in the branch office can log on by using recently expired passwords and access local resources during a WAN connection failure that lasts for 24 hours or longer. You need to ensure that users can log on to the domain only by using a current password. What should you do?
A. Enable universal group membership caching in the site.
B. Instruct all users to log on by using their principal names (UPNs).
C. In Active Directory Users and Computers, require all users to change their passwords to the next time they log on to the domain.
D. Configure the Default Domain Policy Group Policy object (GPO) to prevent logon attempts that use cached credentials.
Answer: D
Explanation:
When the client computers are unable to contact a domain controller at the main office, the users are being logged on using 'cached credentials'. This means that the client computer remembers that the user successfully authenticated with the domain controller recently, so the client computer assumes it is ok to log the user on again after failing to contact a domain controller. We can disable this behavior using a group policy.
Incorrect Answers:
A: Enabling universal group caching won't prevent the logons.
B: This won't prevent the users' ability to log on.
C: This won't prevent the users' ability to log on.