QUESTION 1
You are the network administrator for Certkiller. The network consists of a single Active Directory forest that contains three domains named Certkiller.com, texas.Certkiller.com, and dakota.Certkiller.com. The functional level of the forest is Windows Server 2003. Both texas.Certkiller.com and dakota.Certkiller.com contain employee user accounts, client computer accounts, and resource server computer accounts. The domain named Certkiller.com contains only administrative user accounts and computer accounts for two domain controllers. Each resource server computer provides a single service of file server, print server, Web server, or database server. Certkiller plans to use Group Policy objects (GPOs) to centrally apply security settings to resource server computers. Some security settings need to apply to all resource servers and must not be overridden. Other security settings need to apply to specific server roles only. You need to create an organizational unit (OU) structure to support the GPO requirements. You want to create as few GPOs and links as possible. What should you do?
A. Create a top-level OU for each server role under the Certkiller.com domain. Create a top-level OU named Servers under the texas.Certkiller.com domain. Create a top-level OU named Servers under the dakota.Certkiller.com domain.
B. Create a top-level OU named Servers under the texas.Certkiller.com domain. Create a child OU for each server role under the Servers OU. Create a top-level OU named Servers under the Dakota.Certkiller.com domain.
Create a child OU for each server role under the Servers OU.
C. Create a top-level OU named Servers under the Certkiller.com domain. Create a child OU for each server role under the Servers OU.
D. Create a top-level OU for each server role under the texas.Certkiller.com domain. Create a top-level OU for each server role under the dakota.Certkiller.com domain.
Answer: B
Explanation:
With a top-level OU named Servers, we can apply group policies to all the resource servers. With child OUs for each server role, we can apply group policies to individual server roles. Two domains have resource servers, dakota.Certkiller.com and texas.Certkiller.com. We need to create the OU structure in each of these two domains.
Incorrect Answers:
A: We need an OU for each server role in dakota.Certkiller.com and texas.Certkiller.com, because the resource servers are in those domains.
C: We need a top level OU for all the resource servers in dakota.Certkiller.com and texas.Certkiller.com, so we can apply group policies to all the servers.
D: We need a top level OU for all the resource servers in dakota.Certkiller.com and texas.Certkiller.com, so we can apply group policies to all the servers.

QUESTION 2
You are a network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com All client computers run Windows XP Professional. Certkiller's main office is located in Cape Town. You are a network administrator at Certkiller's branch office in Nairobi. You create a Group Policy object (GPO) that redirects the Start menu for users in the Nairobi branch office to a shared folder on a file server. Server user in Nairobi report that many of the programs that they normally use are missing from their Start menus. The programs were available on the Start menu the 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 of 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 3
You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. Certkiller has one office in Hong Kong and another office in Beijing. Each office is configured as an Active Directory site. Each site contains two domain controllers. The network is configured to display a legal notice on the computer screens of all users before they log on to their client computers. At the request of the legal department, you make changes to the wording of the notice by changing the settings in a Group Policy object (GPO). The GPO is linked to the domain. The legal department reports that not all users are receiving the new notice. You discover that users in the Beijing office receive the new notice, but users in the Hong Kong office receive the old notice. The problem continues for several days. You need to ensure that the new notice appears correctly on all computers in the network. What should you do?
A. Create a new security group that contains the computer accounts for all computers in the Hong Kong site. Grant permissions to this security group to read and apply the GPO.
B. Temporarily assign one of the domain controllers in the Hong Kong site to the Beijing site. Wait 24 hours, and then reassign the domain controller to the Hong Kong site.
C. Force replication of Active Directory between the two sites.
D. Log on to one of the domain controllers in the Hong Kong site, and seize the infrastructure master role.
Answer: C

Explanation:
It looks like the GPO settings haven't been replicated to the Hong Kong office - they are still receiving the old notice. We can manually force replication between the two sites to ensure that the Hong Kong office receives the new GPO settings.
Incorrect Answers:
A: The Hong Kong users still receive the old legal notice. Therefore, this is not a permissions problem on the group policy object.
B: This is unnecessary an impractical.
D: This has nothing to do with the replication of the GPO.

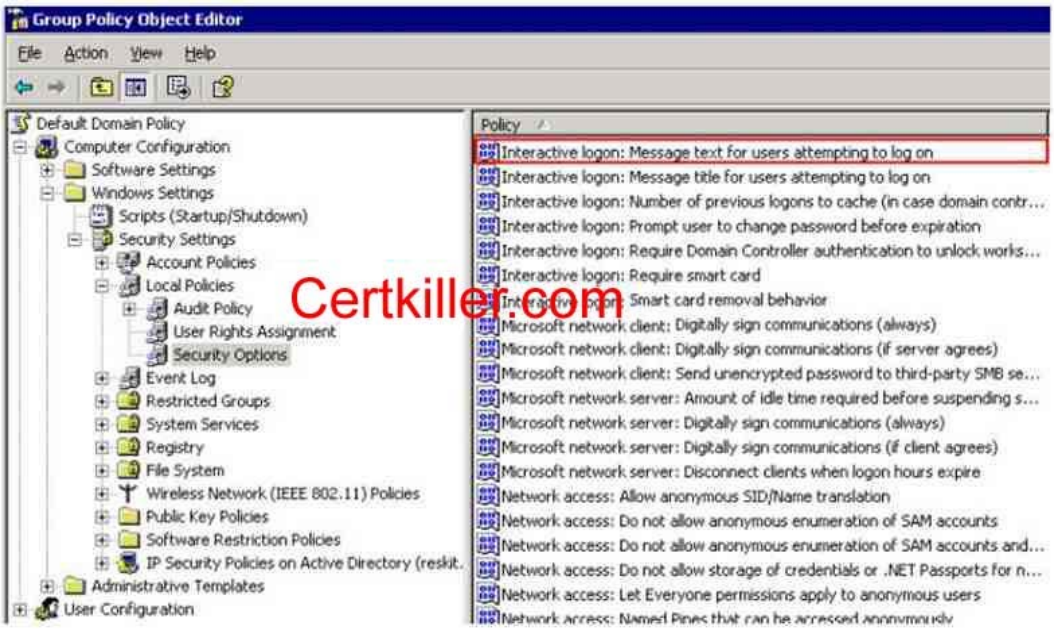
QUESTION 4
You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. The domain contains an organizational unit (OU) named Sales. You create three Group Policy objects (GPOs) that have four configuration settings, as shown in the following table.

Location	GPO name	GPO configuration	Setting
Domain	Screensaver	Hide Screen Saver tab	Disabled
Sales OU	Display and Wallpaper	Hide Screen Saver tab	Enabled
Sales OU	Display and Wallpaper	Set Active Desktop Wallpaper to c:\WINNT\web\wallpaper\bliss.jpg	Enabled
Sales OU	Wallpaper	Set Active Desktop Wallpaper to c:\WINNT\web\wallpaper\autumn.jpg	Enabled

The Screensaver GPO has the No Override setting enabled. The Sales OU has the Block Policy inheritance setting enabled. The priority for GPOs linked to the Sales OU specifies first priority for the Display and Wallpaper GPO and second priority for the Wallpaper GPO. For user accounts in the Sales OU, you want the Screen Saver tab to be hidden and the desktop wallpaper to be Autumn.jpg. You log on to a test computer by using a user account from the Sales OU,
but you do not receive the settings you wanted. You need to configure the settings to hide the Screen Saver tab and set the desktop wallpaper to Autumn.jpg for the user accounts in the Sales OU. You want to avoid affecting user accounts in other OUs. What should you do?
A. Enable the No Override setting for the Display and Wallpaper GPO.
B. Disable the No Override setting on the Screensaver GPO. Reorder the Wallpaper GPO to be first in the list.
C. Create a GPO and link it to the Default-First-Site-Name. Configure the GPO to set the Active Desktop Wallpaper to c:\WINNT\web\wallpaper\autumn.jpg.
D. Disable the Block Policy inheritance setting on the Sales OU. Change the Display and Wallpaper GPO to set the Active Desktop Wallpaper to c:\WINNT\web\wallpaper\autumn.jpg.
Answer: B
Explanation:
The No Override setting on the Screensaver GPO is causing all computers in the domain to display the Screensaver tab. We want to hide the screensaver tab for the sales OU, so we'll have to remove the No Override settings from the Screensaver GPO. This will enable the Screensaver GPO settings to be overwritten by other GPOs.
By configuring the Wallpaper GPO to be first in the list, we are giving it a higher priority than the Display and Wallpaper GPO. This means that the Wallpaper GPO settings will overwrite the Display and Wallpaper GPO settings, thus setting the wallpaper to Autumn.jpg. Group Policy Order of application
1. The unique local Group Policy object.
2. Site Group Policy objects, in administratively specified order.

3. Domain Group Policy objects, in administratively specified order.
4. Organizational unit Group Policy objects, from largest to smallest organizational unit (parent to child organizational unit) and in administratively specified order at the level of each organizational unit. Enforcing policy from above You can set policies that would otherwise be overwritten by policies in child organizational units to No Override at the Group Policy object level.
• Policies set to No Override cannot be blocked.
• The No Override and Block options should be used sparingly. Casual use of these advanced features complicates troubleshooting.
Reference:
Server Help

QUESTION 5
You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. All servers run Windows Server 2003. Each client computer runs Windows NT Workstation 4.0, Windows 2000 Professional, or Windows XP Professional. The computer accounts for all client computers are located in an organizational unit (OU) named Company Computers. All user accounts are located in an OU named Company Users.
Certkiller has a written policy that requires a logon banner to be presented to all users when they log on to any client computer on the network. The banner must display a warning about unauthorized use of the computer.
You need to ensure when a user logs on to a client computer. Which two actions should you take? (Each correct answer presents part of the solution. Choose two)
A. Create a Group Policy object (GPO) that includes the appropriate settings in the interactive logon section. Link the GPO to the domain.
B. Create a script that presents the required warning. Create a Group Policy object (GPO) that will cause the script to run during the startup process. Link the GPO to CertkillerUsers OU.
C. Create a system policy file named Ntconfig.pol that includes the appropriate settings. Place a copy of this file in the appropriate folder on the domain controller.
D. Create a batch file named Autoexec.bat that presents the required warning. Copy the file to root folder on the system partition of all computers affected by the policy.
Answer: A, C
Explanation:
We need to configure a GPO to display the logon message that will apply to the Windows 2000 and Windows XP clients. We need to configure a system policy to display the logon message that will apply to the Windows NT clients. This policy is created with System policies and the System Policy Editor, System policies are used by network
administrators to configure and control individual users and their computers. Administrators use POLEDIT.EXE to set Windows NT profiles that are either network- or user-based. Using this application, you can create policies, which are either local or network-driven, that can affect Registry settings for both hardware and users. The file created to apply the policy is named NTConfig.pol. Interactive logon: Message text for users attempting to log on Description This security setting specifies a text message that is displayed to users when they log on. This text is often used for legal reasons, for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited.
Default: No message.
Configuring this security setting
You can configure this security setting by opening the appropriate policy and expanding the console tree as such: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\



Reference
Group Policy Help

QUESTION 6
You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. Except for IT staff, users are not local administrators on client computers. Certkiller obtains a new application for order processing. This application must be installed on each client computer. The application is contained in an .msi file. You copy the .msi file to a shared folder on a file server. You assign the Authenticated Users group the Allow - Read permissions for the shared folder. To deploy the application, you instruct users to double-click the .msi file in the shared folder. When users attempt to install the application, they receive an error message, and setup fails. You need to configure the network so that the application can be installed successfully. What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)
A. Modify the Default Domain Policy Group Policy object (GPO) and assign the new application to all client computers.
B. Grant the users the permissions required to create temporary files in the shared folder that contains the .msi file.
C. Modify the Default Domain Policy Group Policy object (GPO) and disable the Prohibit User Installs setting in the Windows Installer section of the computer settings.
D. Modify the Default Domain Policy Group Policy object (GPO) and enable the Always install with elevated privileges setting in the Windows Installer section of the computer settings.
Answer: A, D
Explanation:
The software installation fails because the users don't have the necessary permissions to install the software. We can solve this problem by either assigning the application to the users in a group policy, or by using a group policy to enable the Always install with elevated privileges setting in the Windows Installer section of the computer settings.
Software installation

You can use the Software Installation extension of Group Policy to centrally manage software distribution in your organization. You can assign and publish software for groups of users and computers using this extension.

Assigning Applications

When you assign applications to users or computers, the applications are automatically installed on their computers at logon (for user-assigned applications) or startup (for computer-assigned applications.) When assigning applications to users, the default behavior is that the application will be advertised to the computer the next time the user logs on. This means that the application shortcut appears on the Start menu, and the registry is updated with information about the application, including the location of the application package and the location of the source files for the installation. With this advertisement information on the user's computer, the application is installed the first time the user tries to use the application. In addition to this default behavior, Windows XP Professional and Windows Server 2003 clients support an option to fully install the package at logon, as an alternative to installation upon first use. Note that if this option is set, it is ignored by computers running Windows 2000, which will always advertise user-assigned applications. When assigning applications to computers, the application is installed the next time the computer boots up. Applications assigned to computers are not advertised, but are installed with the default set of features configured for the package. Assigning applications through Group Policy requires that the application setup is authored as a Windows Installer (.msi) package.

Publishing Applications

You can also publish applications to users, making the application available for users to install. To install a published application, users can use Add or Remove Programs in Control Panel, which includes a list of all published applications that are available for them to install. Alternatively, if the administrator has selected the a published application. For example, double clicking an .xls file will trigger the installation of Microsoft Excel, if it is not already installed. Publishing applications only applies to user policy; you cannot publish applications to computers. To take advantage of all of the features of Group Policy Software Installation, it is best to use applications that include a Windows Installer (.msi) package. For example, published MSI packages support installation for users who do not have administrative credentials. However, you can also publish legacy setup programs using a .zap file. These applications will be displayed in Add or Remove Programs like any other published application, but typically can only be installed by users with administrative credentials. A .zap file is a simple text file that describes the path to the setup program, as well as any arguments to be passed on the command line. A simple example illustrating the syntax of a .zap file is shown below:

```
[Application]
Friendly Name = Microsoft Works 4.5a
SetupCommand = ""\\DeploymentServer\Apps\Works 4.5a\Standard\Setup.exe""
```

Note

When using quotes in zap files, the following rules apply:

• The path and name of the setup executable must always be quoted.

• If there are no command-line arguments, they must be quoted twice.

Non-Windows Installer Applications

It is possible to publish applications that do not install with the Windows Installer. They can only be published to users and they are installed using their existing Setup programs.

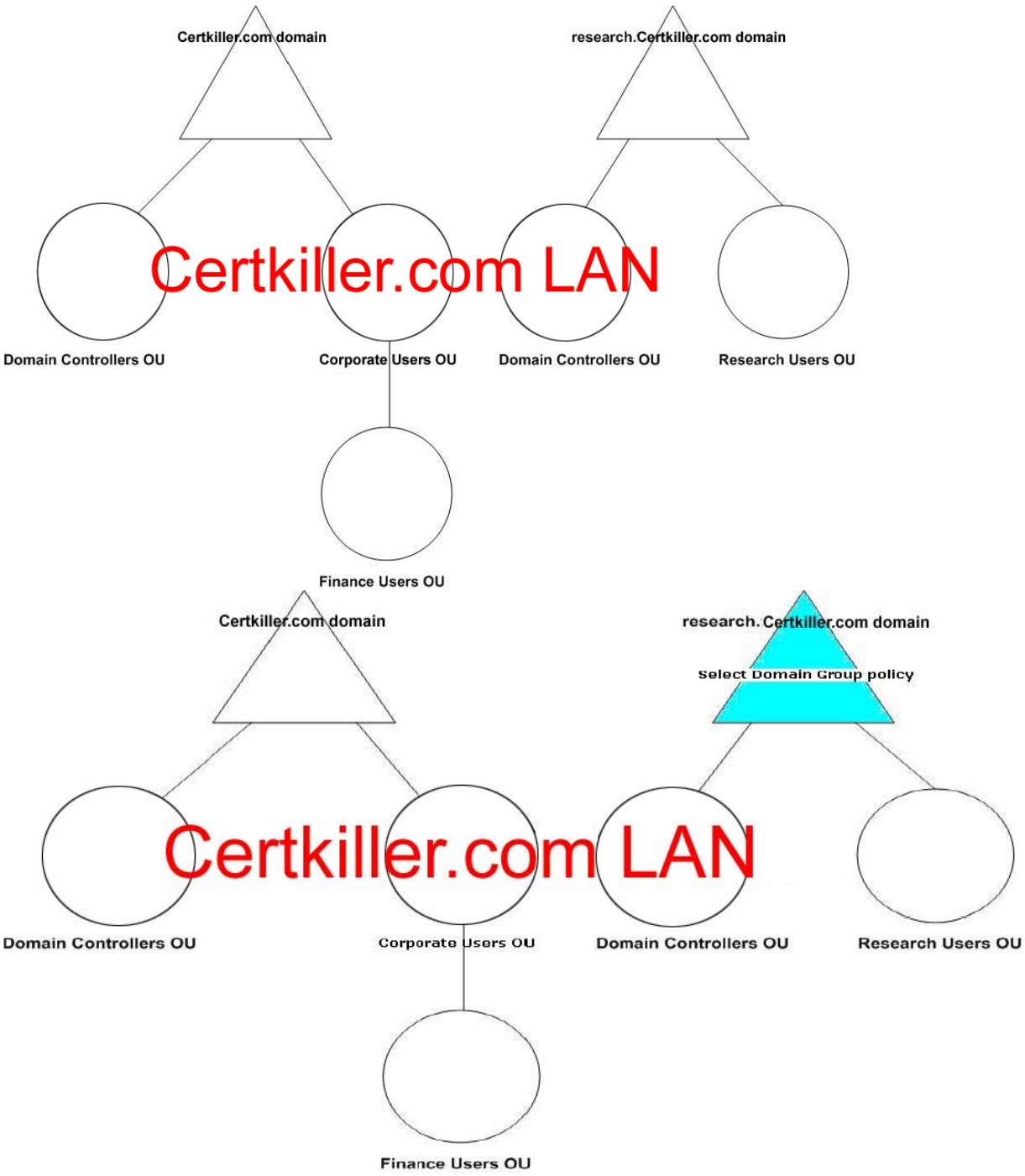
Impersonate a client after authentication Description

Assigning this privilege to a user allows programs running on behalf of that user to impersonate a client. Requiring this user right for this kind of impersonation prevents an unauthorized user from convincing a client to connect (for example, by remote procedure call (RPC) or named pipes) to a service that they have created and then impersonating that client, which can elevate the unauthorized user's permissions to administrative or system levels.

Caution
Assigning this user right can be a security risk. Only assign this user right to trusted users.
Non Windows installer applications
Because these non-Windows Installer applications use their existing Setup programs, such applications cannot:
Use elevated privileges for installation.
Install on the first use of the software.
Install a feature on the first use of the feature.
Rollback an unsuccessful operation, such a install, modify, repair, or removal, or take advantage of other features of the Windows Installer.
Detect a broken state and automatically repair it.
References:
Group policy help
Step-by-Step Guide to Software Installation and Maintenance
http://www.microsoft.com/windows2000/techinfo/planning/management/swinstall.asp

---

QUESTION 7
You are a network administrator for Certkiller. The network consists of a single Active Directory forest that contains two domains. All servers run Windows Server 2003. The domains and organizational units (OUs) are structured as shown in the work area. Users in the research department have user accounts in the research.Certkiller.com domain. All other user
accounts and resources are in the Certkiller.com domain. All domain controllers are in the Domain Controllers OU of their respective domain. No other computer or user accounts are in the Domain Controllers OUs. A written company policy requires that all users working in the research department must use complex passwords of at least nine characters in length. The written policy states that no other users are to have password restrictions. All affected users have user accounts in an OU named Research Users in the research.Certkiller.com domain. You create a Group Policy object (GPO) that contains the required settings. You need to ensure that these settings affect the users in the research department, and that the settings do not affect any other domain users or local accounts. Where should you link the GPO?
To answer, select the appropriate location or locations in the work area.



Answer: Select the research.Certkiller.com domain.
Explanation:
Password restrictions for domain user accounts must always be set at domain level. Password policies applied at OU level will only apply to local user accounts. In this scenario, research.Certkiller.com contains only research users so applying the policy at the domain level will not affect any other others.

QUESTION 8
You are the network administrator for Certkiller. The network consists of a single Active Directory domain

named Certkiller.com.. All servers run Windows Server 2003. All client computers run Windows XP Professional. All servers that are not domain controllers have computer accounts in an organizational unit (OU) named Application Servers. Client computers have computer accounts in 15 OUs organized by department. All users have user accounts in an OU named Company Users. Certkiller wants all users to have Microsoft Word available on their client computers. Certkiller does not want to install Word on domain controller or other servers. You need to configure the network to install the application as required, without affecting any existing policies or settings. What should you do?
A. Create a Group Policy object (GPO) configured with Microsoft Word listed in the software installation section of the computer settings. Link this GPO to the domain. Configure the Domain Controllers OU and the Application Servers OU to block policy inheritance.
B. Create a Group Policy object (GPO) configured with Microsoft Word listed in the software installation section of the computer settings. Link this GPO to the domain. Configure permissions on the GPO so that all servers and domain controller accounts are denied the permissions to read and apply the GPO.
C. Create a Group Policy object (GPO) configured with Microsoft Word listed in the software installation section of the user settings. Link this GPO to the domain. Configure the Domain Controllers OU and the Application Servers OU to block policy inheritance.
D. Create a Group Policy object (GPO) configured with Microsoft Word listed in the software installation section of the user settings. Link this GPO to the domain. Configure permissions on the GPO so that all server and domain controller accounts are denied the permissions to read and apply the GPO.
Answer: B
Explanation:
The software can be installed on all the client computers, but not the domain controllers or application servers. Because the client computers are in 15 OUs, it would be easier to link the GPO at the domain level. The OUs containing the client computers would then inherit the GPO settings. To prevent the GPO applying to the domain controllers and servers, we can simply deny the permissions to read and apply the GPO for the domain controller and server computer accounts.
Software installation
You can use the Software Installation extension of Group Policy to centrally manage software distribution in your organization. You can assign and publish software for groups of users and computers using this extension.
Assigning Applications
When you assign applications to users or computers, the applications are automatically installed on their computers at logon (for user-assigned applications) or startup (for computer-assigned applications.) When assigning applications to users, the default behavior is that the application will be advertised to the computer the next time the user logs on. This means that the application shortcut appears on the Start menu, and the registry is updated with information about the application, including the location of the application package and the location of the source files for the installation. With this advertisement information on the user's computer, the application is installed the first time the user tries to use the application. In addition to this default behavior, Windows XP Professional and Windows Server 2003 clients support an option to fully install the package at logon, as an alternative to installation upon first use. Note that if this option is set, it is ignored by computers running Windows 2000, which will always advertise user-assigned applications. When assigning applications to computers, the application is installed the next time the computer boots up. Applications assigned to computers are not advertised, but are installed with the default set of features configured for the package. Assigning applications through Group Policy requires that the application setup is authored as a Windows Installer (.msi) package.
Publishing Applications
You can also publish applications to users, making the application available for users to install. To install a

published application, users can use Add or Remove Programs in Control Panel, which includes a list of all published applications that are available for them to install. Alternatively, if the administrator has selected the a published application. For example, double clicking an .xls file will trigger the installation of Microsoft Excel, if it is not already installed. Publishing applications only applies to user policy; you cannot publish applications to computers.
Filter user policy settings based on membership in security groups.
You can specify users or groups for which you do not want a policy setting to apply by clearing the Apply Group Policy and Read check boxes, which are located on the Security tab of the properties dialog box for the GPO.
When the Read permission is denied, the policy setting is not downloaded by the computer.
As a result, less bandwidth is consumed by downloading unnecessary policy settings, which enables the network to function more quickly. To deny the Read permission, select Deny for the Read check box, which is located on the Security tab of the properties dialog box for the GPO.
Incorrect Answers:
A: It is likely that some domain level policies should apply to the domain controllers and the servers. Therefore, blocking policy inheritance isn't recommended.
C: It is likely that some domain level policies should apply to the domain controllers and the servers. Therefore, blocking policy inheritance isn't recommended.
D: This won't stop the software being installed on the servers, because the software installation would be defined in the user section of the group policy.

QUESTION 9
You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. All servers run Windows Server 2003. All client computers run either Windows XP Professional or Windows 2000 Professional. All client computer accounts are located in an organizational unit (OU) named Workstation.
A written company policy states that the Windows 2000 Professional computers must not use offline folders. You create a Group Policy object (GPO) to enforce this requirement. The settings in the GPO exist for both Windows 2000 Professional computers and Windows XP Professional computers. You need to configure the GPO to apply only to Windows 2000 Professional computers. What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)
A. Create a WMI filter that will apply the GPO to computers that are running Windows 2000 Professional.
B. Create a WMI filter that will apply the GPO to computers that are not running Windows XP Professional.
C. Create two OUs under the Workstation OU. Place the computer accounts for the Windows XP Professional computers in one OU, and place the computer accounts for the Windows 2000 Professional computers in the other OU. Link the GPO to the Workstation OU.
D. Create a group that includes the Windows XP Professional computers. Assign the group the Deny - General Resultant Set of Policy(Logging) permission.
E. Create a group that includes the Windows 2000 Professional computers Assign the group the Dent - Apply Group Policy permission.
Answer: A, B
Explanation:
This is a tricky question because WMI filters are ignored by Windows 2000 clients. However, that doesn't matter. The Windows XP clients can evaluate the filters and that is good enough. For answer A, the XP clients will evaluate the filter and see that the GPO should not apply to them. The Windows 2000 clients will just apply the GPO without evaluating the WMI filter. For answer B, the same thing will happen. The XP clients will

evaluate the filter and see that the GPO should not apply to them. The Windows 2000 clients will just apply the GPO without evaluating the WMI filter. WMI filtering WMI filters are only available in domains that have the Windows Server 2003 configuration. Although none of the domain controllers need to be running Windows Server 2003, you must have run ADPrep /DomainPrep in this domain. Also note that WMI filters are only evaluated by clients running Windows XP, Windows Server 2003, or later. WMI filters associated with a Group Policy object will be ignored by Windows 2000 clients and the GPO will always be applied on Windows 2000.
Incorrect Answers:
C: This looks like a good idea. However, applying the GPO to the Workstation OU will (by inheritance) apply the GPO to the two child OUs.
D: This won't prevent the application of the GPO.
E: This answer is close, but incorrect. This will prevent the GPO applying to the Windows 2000 clients. If the group contained the Windows XP clients, then it would work.

QUESTION 10
You are the network administrator for Certkiller. The network consists of a Single Active Directory domain named Certkiller.com with three sites. There is a domain controller at each site. All servers run Windows Server 2003. Each client computer runs either Windows 2000 Professional or Windows XP Professional. The IT staff is organized into four groups. The IT staff works at the three different sites. The computers for the IT staff must be configured by using scripts. The script or scripts must run differently based on which site the IT staff user is logging on to and which of the four groups the IT staff user is a member of. You need to ensure that the correct logon script is applied to the IT staff users based on group membership and site location. What should you do?
A. Create four Group Policy objects (GPOs). Create a script in each GPO that corresponds to one of the four groups.
Link the four new GPOs to all three sites. Grant each group permissions to apply only the GPO that was created for the group.
B. Create a single script that performs the appropriate configuration based on the user's group membership. Place the script in the Netlogon shared folders on the domain controllers.
C. Configure a Group Policy object (GPO) with a startup script that configures computers based on IT staff group. Link the GPO to the three sites.
D. Create a script that configures the computers based on IT staff group membership and site. Create and link a GPO to the Domain Controllers OU to run the script.
Answer: A
Explanation:
The easiest way to filter which users or computers a GPO should apply to is to set permissions on the GPOs. A user or computer needs the Allow - Read and Apply Group Policy permissions in order to apply the GPO. In this question, we have four groups, each with different requirements. By creating four different GPOs and linking them to each of the three sites, we can manage who receives the GPO by configuring the permissions on the GPOs.
Incorrect Answers:
B: The script needs to be linked to an Active Directory container.
C: It's easier to use GPO permissions to determine which users or computers should receive a GPO.
D: It's easier to use GPO permissions to determine which users or computers should receive a GPO. Furthermore, the GPO is linked to the wrong container in this answer.

QUESTION 11
You are the network administrator for Certkiller, a company that has a single office. The network consists of a

single Active Directory domain named Certkiller.com and a single site. All servers run Windows Server 2003. All file and print servers and application servers are located in an organizational unit (OU) named Servers. A server support team handles daily support issues for the file and print servers and application servers. All of the server support team's user accounts are located in the OU named SST. You are responsible for managing security for Certkiller's servers. You create a group named Server Support that includes all the user accounts of the server support team. You need to ensure that members of the server support team can log on locally to only the file and print servers and the application servers. What should you do?
A. Create a Group Policy object (GPO) to grant the Server Support group the Allow log on locally user right. Link the GPO to the SST OU.
B. Create a Group Policy object (GPO) to grant the Server Support group the Allow log on locally user right. Link the GPO to the Servers OU.
C. Assign the Server Support group the Allow - Full Control permission for the Servers OU.
D. Assign the Server Support group the Allow - Full Control permission for the Computers container.
Answer: B
Explanation:
All file and print servers and application servers are located in an organizational unit (OU) named Servers. Therefore, we can simply a Group Policy object (GPO) to grant the Server Support group the Allow log on locally user right and link the GPO to the Servers OU.
Incorrect Answers:
A: The GPO needs to be linked to the OU containing the computer accounts for the servers.
C: This would allow the Server Support group to create objects in the OU, and to modify the permission on existing objects. This is more 'permission' than necessary.
D: This would allow the Server Support group to create objects in the computers container, and to modify the permission on existing objects. This would have no effect on the servers because they are in a separate OU.

QUESTION 12
You are the network administrator for Certkiller. The network consists of a single Active Directory forest. The forest consists of 19 Active Directory domains. Fifteen of the domains contain Windows Server 2003 domain controllers. The functional level of all the domains is Windows 2000 native. The network consists of a single Microsoft Exchange 2000 Server organization. You need to create groups that can be used only to send e-mail messages to user accounts throughout
Certkiller. You want to achieve this goal by using the minimum amount of replication traffic and minimizing the size of the Active Directory database. You need to create a plan for creating e-mail groups for Certkiller. What should you do?
A. Create global distribution groups in each domain.
Make the appropriate users from each domain members of the global distribution group in the same domain.
Create universal distribution groups.
Make the global distribution groups in each domain members of the universal distribution groups.
B. Create global security groups in each domain.
Make the appropriate users from each domain members of the security group in the same domain. Create universal security groups.
Make the global security groups in each domain members of the universal security groups.
C. Create universal distribution groups.
Make the appropriate users from each domain members of a universal distribution group.
D. Create universal security groups. Make the appropriate users from each domain members of a universal security group.

Answer: A
Explanation:
We need to minimize replication traffic. We can do this by placing the users into Global groups, then place the Global groups into Universal groups. In Active Directory, a Universal group lists all its members. If the Universal group contained user accounts, and a user account was added or removed, then the Universal group information would be replicated throughout the forest. This is why placing user accounts directly into Universal groups isn't recommended. We need to use Distribution groups for email groups. Answers B and D are wrong because they suggest using security groups. Answer C is wrong because it suggests placing the user accounts directly into Universal groups.

Domain functional levels	Domain controllers supported	Group scopes supported
Windows 2000 mixed (default)	Windows NT Server 4.0, Windows 2000, Windows Server 2003	Global, domain local
Windows 2000 native	Windows 2000, Windows Server 2003	Global, domain local, universal
Windows Server 2003	Windows Server 2003	Global, domain local, universal

When to use global groups
Because global groups have a forest-wide visibility, do not create them for domain-specific resource access. Use a global group to organize users who share the same job tasks and need similar network access requirements. A different group type is more appropriate for controlling access to resources within a domain.
When to use universal groups
Use universal groups to nest global groups so that you can assign permissions to related resources in multiple domains. A Windows Server 2003 domain must be in Windows 2000 native mode or higher to use universal groups. When to use domain local groups Use a domain local group to assign permissions to resources that are located in the same domain as the domain local group. You can place all global groups that need to share the same resources into the appropriate domain local group. MS THUMB RULES Grant permissions to groups instead of users.
• A G P
• A DL P
• A G DL P
• A G U DL P
• A G L P
A (Account)
G (Global Group)
U (Universal Group)
DL (Domain Local Group)
P (Permissions)

Group scope

Groups, whether a security group or a distribution group, are characterized by a scope that identifies the extent to which the group is applied in the domain tree or forest. There are three group scopes: universal, global, and domain local.

- Members of universal groups can include other groups and accounts from any domain in the domain tree or forest and can be assigned permissions in any domain in the domain tree or forest.
- Members of global groups can include other groups and accounts only from the domain in which the group is defined and can be assigned permissions in any domain in the forest.
- Members of domain local groups can include other groups and accounts from Windows Server 2003, Windows 2000, or Windows NT domains and can be assigned permissions only within a domain.

The following table summarizes the behaviors of the different group scopes.

Universal scope	Global scope	Domain local scope
When the domain functional level is set to Windows 2000 native or Windows Server 2003, members of universal groups can include accounts, global groups, and universal groups from any domain.	When the domain functional level is set to Windows 2000 native or Windows Server 2003, members of global groups can include accounts and global groups from the same domain.	When the domain functional level is set to Windows 2000 native or Windows Server 2003, members of domain local scope can include accounts, global groups, and universal groups from any domain, as well as domain local groups from the same domain.
When the domain functional level is set to Windows 2000 mixed, security groups with universal scope cannot be created.	When the domain functional level is set to Windows 2000 mixed, members of global groups can include accounts from the same domain.	When the domain functional level is set to Windows 2000 native or Windows Server 2003, members of domain local groups can include accounts and global groups from any domain.
When the domain functional level is set to Windows 2000 native or Windows Server 2003, groups can be added to other groups and assigned permissions in any domain.	Groups can be added to other groups and assigned permissions in any domain.	Groups can be added to other domain local groups and assigned permissions only in the same domain.
Groups can be converted to domain local scope. Groups can be converted to global scope, as long as no other universal groups exists as members.	Groups can be converted to universal scope, as long as the group is not a member of any other group with global scope.	Groups can be converted to universal scope, as long as the group does not have as its member another group with domain local scope.

Reference
Server Help
Schema classes and attributes, MS workshop 2209

QUESTION 13
You are the network administrator for Acme Inc. Your network consists of a single Active Directory forest that contains one domain named acme.com. The functional level of the forest is Windows Server 2003. Acme, Inc., acquires a company named Certkiller. The Certkiller network consists of a single Active Directory forest that contains a root domain named Certkiller.com and a child domain named asia.Certkiller.com. The functional level of the forest is Windows 2000. The functional level of the asia.Certkiller.com domain is Windows 2000 native. A business decision by Certkiller requires that asia.Certkiller.com domain to be removed. You need to move all user accounts from the asia.Certkiller.com domain to the acme.com domain by using the Active Directory Migration Tool. You need to accomplish this task without changing the logon rights and permissions

for all other users. You need to ensure that users in asia.Certkiller.com can log on to acme.com by using their current user names and passwords. What should you do?
A. Create a two-way Windows Server 2003 external trust relationship between the acme.com domain and the Certkiller.com domain.
B. Create a one-way Windows Server 2003 external trust relationship in which the acme.com domain trusts the Certkiller.com domain.
C. Create a temporary two-way external trust relationship between the acme.com domain and the asia.Certkiller.com domain.
D. Create a temporary one-way external trust relationship in which the asia.Certkiller.com domain trusts the acme.com domain.
Answer: C
Explanation:
To use ADMT, we need a two way trust between the acme.com domain and the asia.Certkiller.com domain.
Incorrect Answers:
A: This would enable users in Certkiller.com to log in to acme.com and users in acme.com to log in to Certkiller.com.
B: This would enable users in Certkiller.com to log in to acme.com.
D: The trust must be a two-way trust.

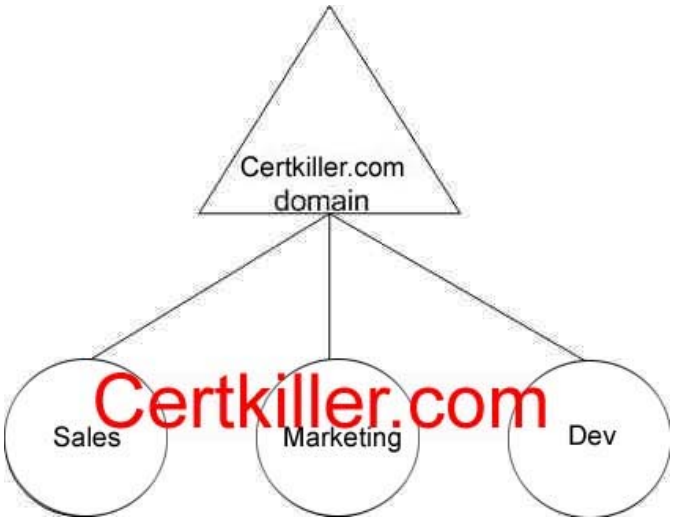
QUESTION 14
You are the network administrator for Certkiller. Your network consists of a single Active Directory forest that contains three domains. The forest root domain is named Certkiller.com. The domain contains two child domains named asia.Certkiller.com and africa.Certkiller.com. The functional level of the forest is Windows Server 2003. Each domain contains two Windows Server 2003 domain controllers named DC1 and DC2. DC1 in the Certkiller.com domain performs the following two operations master roles: schema master and domain naming master. DC1 in each child domain performs the following three operations master roles: PDC emulator master, relative ID (RID) master, and infrastructure master. DC1 in each domain is also a global catalog server. The user account for Jack King in the africa.Certkiller.com domain is a member of the Medicine Students security group. Because of a name change, the domain administrator of africa.Certkiller.com changes the Last name field of Jack's user account from King to Edwards. The domain administrator of asia.Certkiller.com discovers that the user account for Jack is still listed as Jack King. You need to ensure that the user account for Jack Edwards is correctly listed in the Medicine Students group. What should you do?
A. Transfer the PDC emulator master role from DC1 to DC2 in each domain.
B. Transfer the infrastructure master role from DC1 to DC2 in each domain.
C. Transfer the RID master role from DC1 to DC2 on each domain.
D. Transfer the schema master role from DC1 to DC2 in the Certkiller.com domain.
Answer: B
Explanation:
Problems like this can occur when the infrastructure master role is on the same domain controller as the Global Catalog. There is no reason to transfer any other master roles.
Infrastructure master
A domain controller that holds the infrastructure operations master role in Active Directory. The infrastructure master updates the group-to-user reference whenever group memberships change and replicates these changes across the domain. At any time, the infrastructure master role can be assigned to only one domain controller in each domain. in each domain. The infrastructure master is responsible for updating references from objects in its domain to objects in other domains. The infrastructure master compares its data with that of a global catalog.

Global catalogs receive regular updates for objects in all domains through replication, so the global catalog data will always be up to date. If the infrastructure master finds data that is out of date, it requests the updated data from a global catalog. The infrastructure master then replicates that updated data to the other domain controllers in the domain.
Important
Unless there is only one domain controller in the domain, the infrastructure master role should not be assigned to the domain controller that is hosting the global catalog. If the infrastructure master and global catalog are on the same domain controller, the infrastructure master will not function. The infrastructure master will never find data that is out of date, so it will never replicate any changes to the other domain controllers in the domain. In the case where all of the domain controllers in a domain are also hosting the global catalog, all of the domain controllers will have the current data and it does not matter which domain controller holds the infrastructure master role. The infrastructure master is also responsible for updating the group-to-user references whenever the members of groups are renamed or changed. When you rename or move a member of a group (and that member resides in a different domain from the group), the group may temporarily appear not to contain that member. The infrastructure master of the group's domain is responsible for updating the group so it knows the new name or location of the member. This prevents the loss of group memberships associated with a user account when the user account is renamed or moved. The infrastructure master distributes the update via multimaster replication. There is no compromise to security during the time between the member rename and the group update. Only an administrator looking at that particular group membership would notice the temporary inconsistency.

QUESTION 15
You are the network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com with two sites. Each site contains two domain controllers. One domain controller in each site is a global catalog server. You add a domain controller to each site. Each new domain controller has a faster processor than the existing domain controllers. Certkiller requires Active Directory replication to flow through the servers that have the most powerful CPUs in each site. You need to configure the intersite replication to comply with Certkiller's requirement for Active Directory replication. What should you do?
A. Configure the new domain controllers as global catalog servers.
B. Configure the new domain controller in each site as a preferred bridgehead server for the IP transport.
C. Configure the new domain controller in each site as a preferred bridgehead server for the SMTP transport.
D. Configure an additional IP site link between the two sites.
Assign a lower site link cost to this site link than the site link cost for the original site link.
Answer: B
Explanation:
Replication.
Directory information is replicated both within and among sites. Active Directory replicates information within a site more frequently than across sites. This balances the need for up-to-date directory information with the limitations imposed by available network bandwidth. You customize how Active Directory replicates information using site links to specify how your sites are connected. Active Directory uses the information about how sites are connected to generate Connection objects that provide efficient replication and fault tolerance. You provide information about the cost of a site link, times when the link is available for use and how often the link should be used. Active Directory uses this information to determine which site link will be used to replicate information. Customizing replication schedules so replication occurs during specific times, such as when network traffic is low, will make replication more efficient. Ordinarily, all domain controllers are used to exchange information between sites, but you can further control replication behavior by specifying a bridgehead

server for inter-site replicated information. Establish a bridgehead server when you have a specific server you want to dedicate for inter-site replication, rather than using any server available. You can also establish a bridgehead server when your deployment uses proxy servers, such as for sending and receiving information through a firewall.
Site link
Site links are logical paths that the KCC uses to establish a connection for Active Directory replication. Site links are stored in Active Directory as site link objects. A site link object represents a set of sites that can communicate at uniform cost through a specified intersite transport. All sites contained within the site link are considered to be connected by means of the same network type. Sites must be manually linked to other sites by using site links so that domain controllers in one site can replicate directory changes from domain controllers in another site. Because site links do not correspond to the actual path taken by network packets on the physical network during replication, you do not need to create redundant site links to improve Active Directory replication efficiency. When two sites are connected by a site link, the replication system automatically creates connections between specific domain controllers in each site called bridgehead servers. In Microsoft(r) Windows(r) 2000, intersite replication of the directory partitions (e.g. domain, configuration, and schema) between domain controllers in different sites is performed by the domain controllers (one per directory partition) in those sites designated by the KCC as the bridgehead server. In Windows Server 2003, the KCC may designate more than one domain controller per site hosting the same directory partition as a candidate bridgehead server. The replication connections created by the KCC are randomly distributed between all candidate bridgehead servers in a site to share the replication workload. By default, the randomized selection process takes place only when new connection objects are added to the site. However, you can run Adlb.exe, a new Windows Resource Kit tool called Active Directory Load Balancing (ADLB) to rebalance the load each time a change occurs in the site topology or in the number of domain controllers the site. In addition, ADLB can stagger schedules so that the outbound replication load for each domain controller is spread out evenly across time. Consider using ADLB to balance replication traffic between the Windows Server 2003-based domain controllers when they are replicating to more than 20 other sites hosting the same domain
Reference
MS Windows Server 2003 Deployment Kit
Designing and Deploying Directory and Security Services
Active Directory Replication Concepts

QUESTION 16
You are a network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com. All servers run Windows Server 2003. The functional level of the domain is Windows Server 2003. The organizational unit (OU) structure is shown in the exhibit.



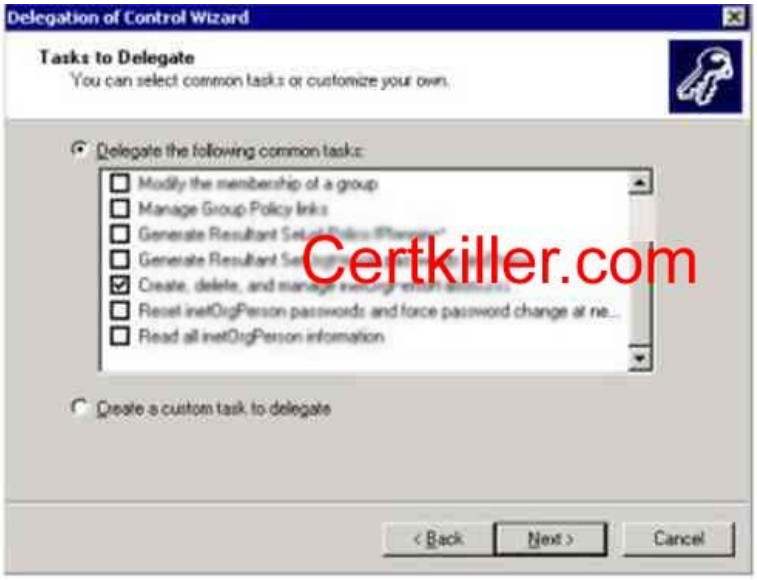
Certkiller uses an X.500 directory service enabled product to support a sales and marketing application. The application is used only by users in the sales department and the marketing department. The application uses InetOrgPerson objects as user accounts. InetOrgPerson objects have been created in Active Directory for all Sales and Marketing users. These users are instructed to log on by using their InetOrgPerson object as their user account. Microsoft Identity Integration Server is configured to copy changes to InetOrgPerson objects from Active Directory to the X.500 directory service enabled product. All InetOrgPerson objects for marketing employees are located in the Marketing OU. All InetOrgPerson objects for sales employees are located in the Sales OU. King is another administrator in Certkiller. King is responsible for managing the objects for users who require access to the X.500 directory service enabled product. You need to configure Active Directory to allow King to perform his responsibilities. Which action or actions should you take? (Choose all that apply)

A. On the domain, grant King the permission to manage user objects.
B. On the domain, grant King the permission to manage InetorgPerson objects.
C. On the Sales OU, block the inheritance of permissions.
D. On the Marketing OU, block the inheritance of permissions.
E. On the Dev OU, block the inheritance of permissions.

Answer: B, E

Explanation:

The administrator named King needs to manage the InetorgPerson objects. We could delegate this task as shown in the exhibit below, but this isn't given as an option.



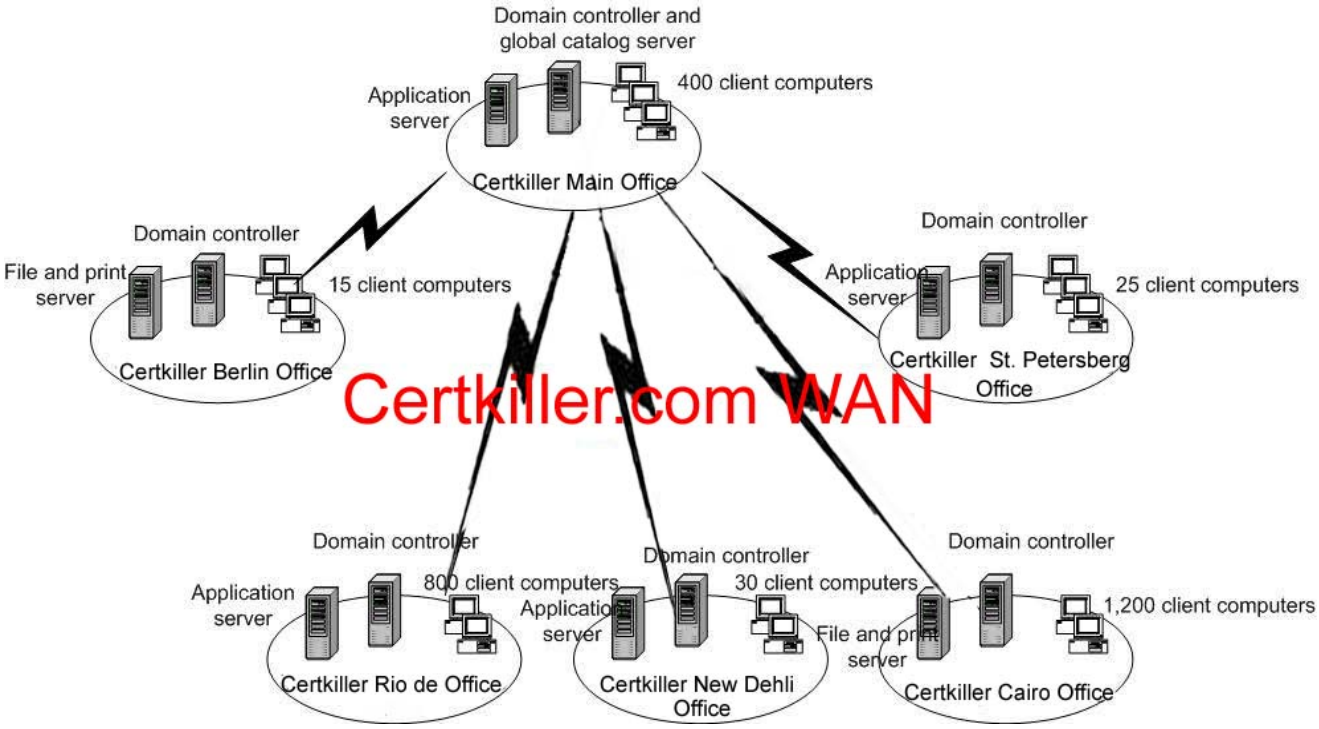
Instead we can set permissions at the domain level. The permissions shouldn't apply to the Dev OU, so we'll have to block the inheritance of the permissions for the Dev OU.

QUESTION 17

You are the network administrator for Certkiller. The network consists of a single Active Directory forest that contains five domains. The functional level of the forest is Windows 2000. You have not configured any universal groups in the forest. One domain is a child domain named usa.Certkiller.com that contains two domain controllers and 50 client computers. The functional level of the domain is Windows Server 2003. The network includes an Active Directory site named Site1 that contains two domain controllers. Site1 represents a remote clinic, and the location changes every few months. All of the computers in usa.Certkiller.com are located in the remote clinic. The single WAN connection that connects the remote clinic to the main network is often saturated or unavailable. Site1 does not include any global catalog servers. You create several new user

accounts on the domain controllers located in Site1. You need to ensure that users in the remote clinic can always quickly and successfully log on to the domain. What should you do?
A. Enable universal group membership caching in Site1.
B. Add the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\IgnoreGCFailures key to the registry on both domain controllers in Site1.
C. Add the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\IgnoreGCFailures key to the registry on all global catalog servers in the forest.
D. Raise the functional level of the forest to Windows Server 2003.
Answer: B
Explanation:
Native Mode Domain
A native mode domain, where all domain controllers are Windows 2000 domain controllers and the domain has been irrevocably switched to native mode, allows the usage of universal groups. When processing a logon request for a user in a native-mode domain, a domain controller sends a query to a global catalog server to determine the user's universal group memberships. Since you can explicitly deny a group access to a resource, complete knowledge of a user's group memberships is necessary to enforce access control correctly. If a domain controller of a native-mode domain cannot contact a global catalog server to determine universal group membership when a user wants to log on, the domain controller refuses the logon request. The following registry key can be set so that the domain controller ignores the global catalog server failure when expanding universal groups:
HKEY_LOCAL_MACHINE \System \CurrentControlSet \Control \Lsa \IgnoreGCFailures
The domain controller still tries to connect to the global catalog server, however, and the timeout for that query must expire. For more information on using this registry key, refer to article Q241789 in the Microsoft Knowledge Base.

QUESTION 18
You are a network administrator for Certkiller that has a main office and five branch offices. The network consists of six Active Directory domains. All servers run Windows Server 2003. Each office is configured as a single domain. Each office is also configured as an Active Directory site. Certkiller uses an application server that queries user information from the global catalog. You install application servers in the main office and in three branch offices. The network is configured as shown in the exhibit.



You monitor the WAN connections between the main office and each branch office and discover that the utilization increased from 70 percent to 90 percent. Users report slow response times when accessing information on the application server. You need to place global catalog servers in offices where they will improve the response times for the application servers. You need to achieve this goal with a minimum amount of increase in WAN traffic. In which office or offices should you place a new global catalog server or servers? (Choose all that apply)

A. Berlin
B. Rio de Janeiro
C. New Delhi
D. St Petersburg
E. Cairo

Answer: B, C, D

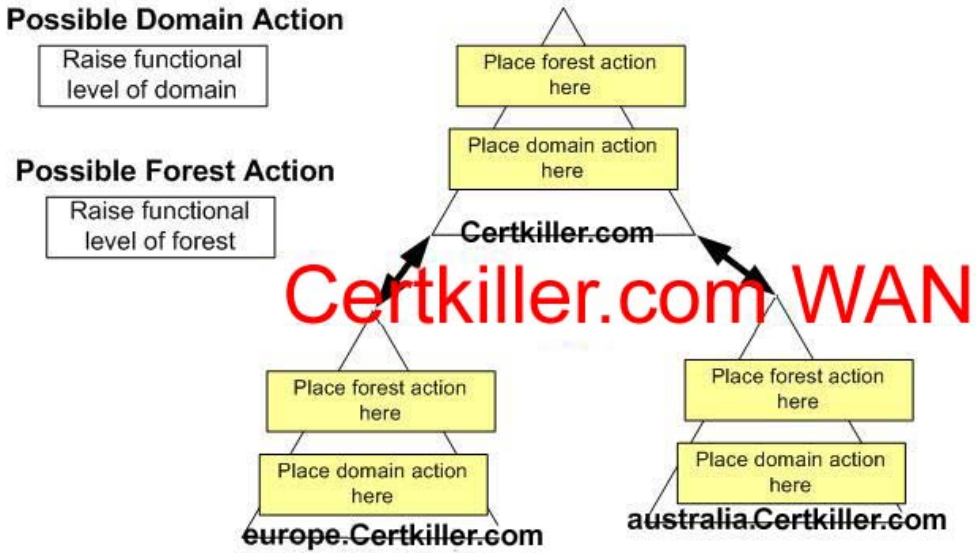
Explanation:

Because the application server queries Global catalog attributes, we need to put one Global Catalog server in each site hosting an application server; in this case Rio de Janeiro, New Delhi and St Petersburg.

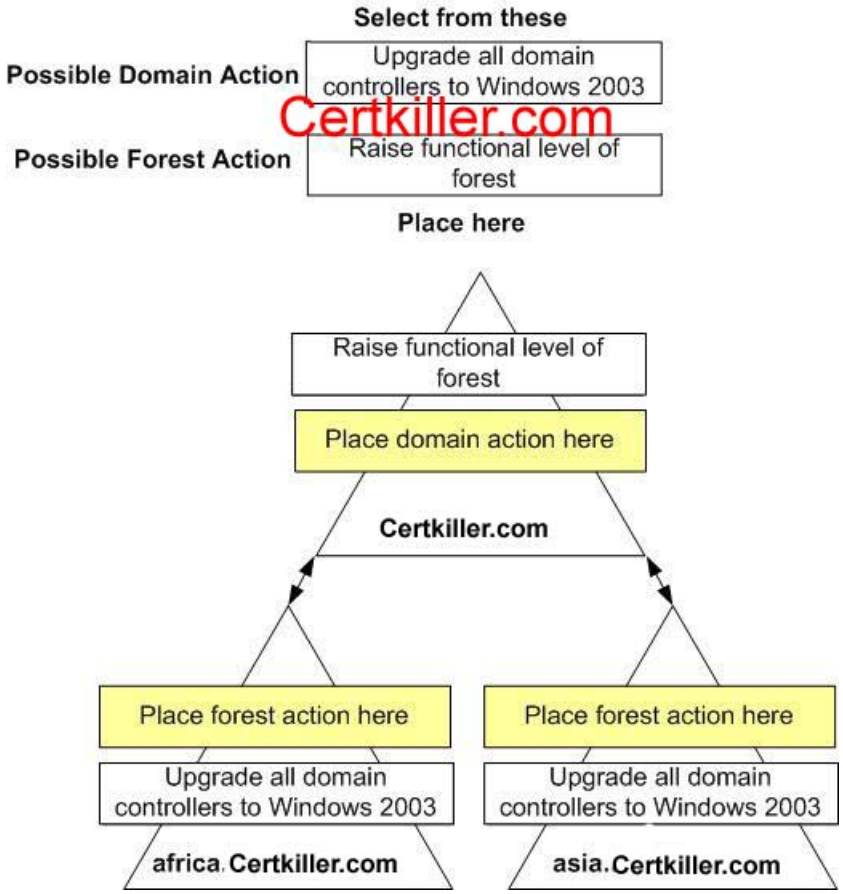
QUESTION 19

You are the network administrator for Certkiller. The network consists of a single Active Directory forest. The functional level of the forest is Windows 2000. The forest consists of a root domain named Certkiller.com and two child domains named europe.Certkiller.com and australia.Certkiller.com. The functional level of all domains is Windows 2000 native. All domain controllers in the Certkiller.com domain run Windows Server 2003. All domain controllers in the europe.Certkiller.com and australia.Certkiller.com domains run Windows 2000 Server. You need to able to rename all domain controllers in Certkiller.com. You want to minimize impact to the network. What should you do?

To answer, drag the appropriate action or actions to the correct location or locations in the work area.



Answer:



Explanation:

To rename domain controllers, the domains have to be in Windows 2003 functional level. We don't have the option to raise the domain functional levels, but upgrading the forest functional level will automatically upgrade the domain functional levels if the domains are in Windows 2000 native functional level.

To rename a Windows Server 2003 domain controller,

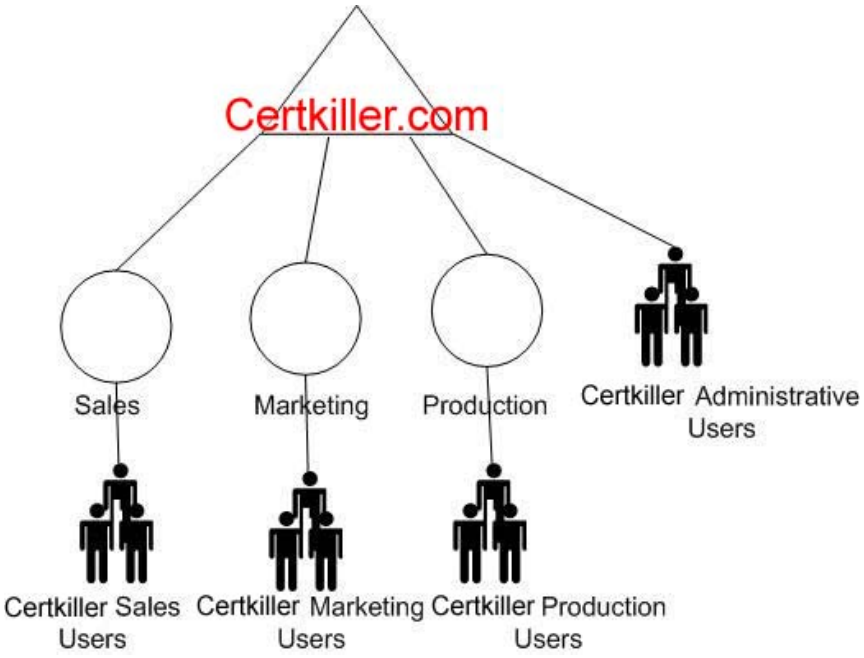
You must be a member of the Domain Admins group or the Enterprise Admins group in Active Directory.

Domain functional level is set to Windows Server 2003 NOTE: YOU do not need to raise the forest level, just domain level.
Note :
Before you rename a domain controller in a domain with multiple domain controllers, make sure that the computer that you want to rename is not the global catalog server and that it does not hold other Flexible Single Master Operations (FSMO) roles. TO Rename a Domain Controller in a Domain that Contains a Single Domain Controller To rename a domain controller in a domain that contains a single domain controller:
1. Install a second Windows Server 2003 computer in the same domain with the server that you want to rename. Raising the forest functional level to Windows Server 2003 is not possible if there is any domain controller in the forest that remains to be upgraded to Windows Server 2003 or if any domain in the forest still has Windows 2000 mixed domain functionality. Assuming these requirements are satisfied, you can raise the forest level to Windows Server 2003.
NOTE: 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
Reference:
MS white paper
Step-by-Step Guide to Implementing Domain Rename
MS Knowledge base article
Q814589 HOW TO: Rename a Windows 2003 Domain Controller

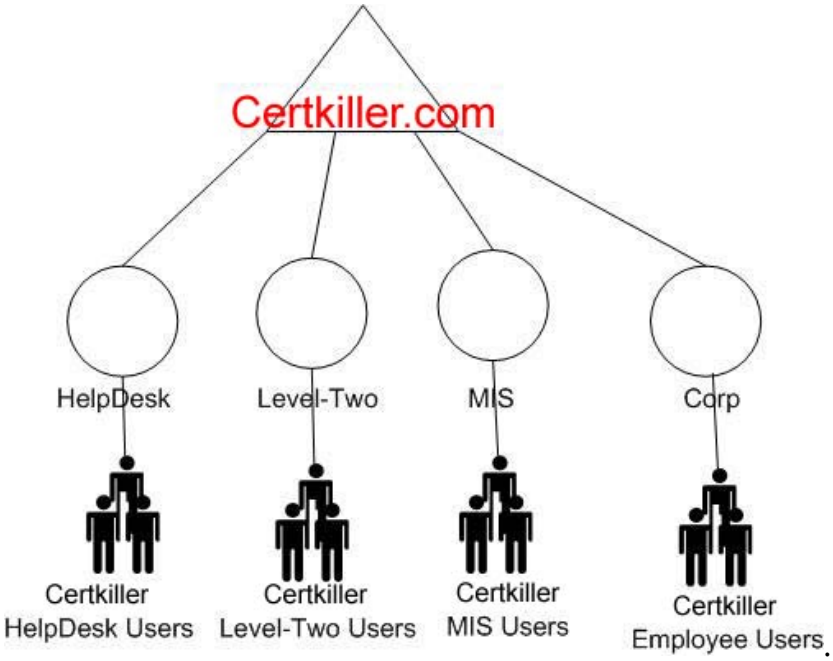
QUESTION 20
You are the network administrator for Certkiller, a company with six offices. The network consists of a single Active Directory domain named Certkiller.com. Each office has users who work in the sales, marketing, and production departments. All Active Directory administration is performed by the IT group. The IT group provides a help desk, a level-two support group, and an MIS group. Each office has one employee who works for the help desk group. Administrative responsibilities are listed in the following table.

Group	Role
Help desk	User account maintenance for all employees who are not management
Level-two support	User account maintenance for all employees, the help desk users, and all management users
MIS group	Service account maintenance, maintenance of domain administrator accounts, and built-in accounts in Active Directory

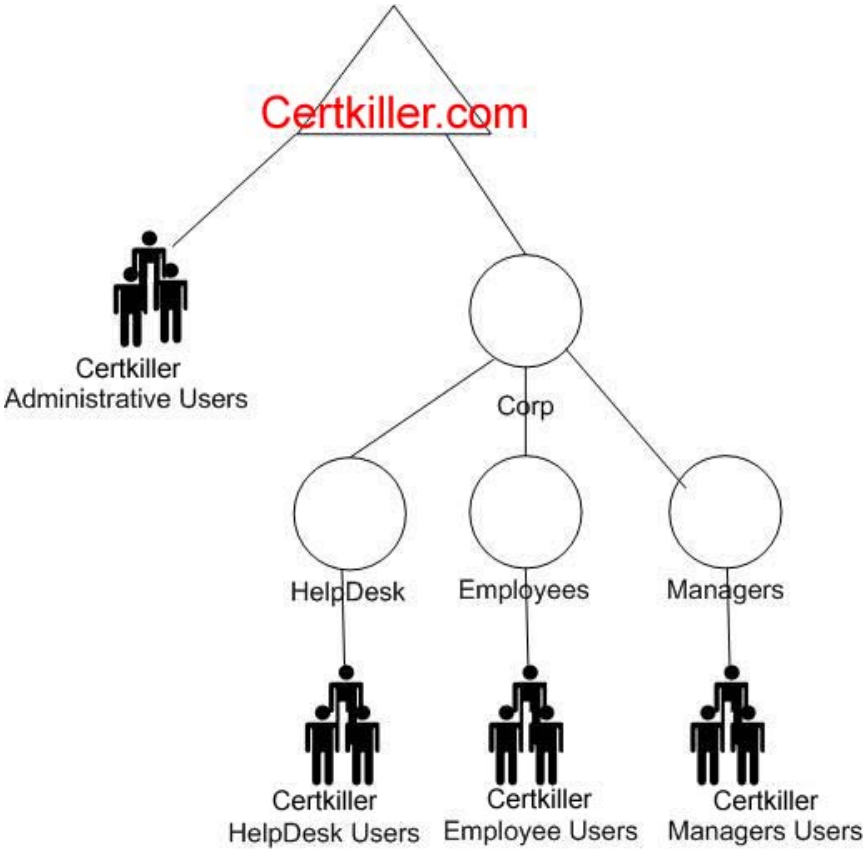
You need to plan an organizational unit (OU) structure that allows delegation of administration. Your plan must ensure that permissions can be maintained by using the minimum amount of administrative effort. Which OU structure should you use?
A.


Certkiller.com
Sales
Marketing
Production
Certkiller Administrative Users
Certkiller Sales Users
Certkiller Marketing Users
Certkiller Production Users

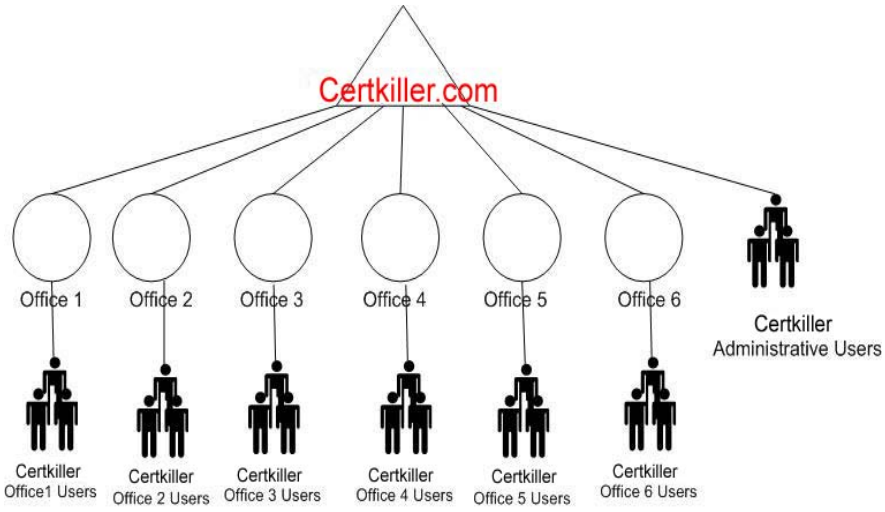
B


Certkiller.com
HelpDesk
Level-Two
MIS
Corp
Certkiller HelpDesk Users
Certkiller Level-Two Users
Certkiller MIS Users
Certkiller Employee Users

C.



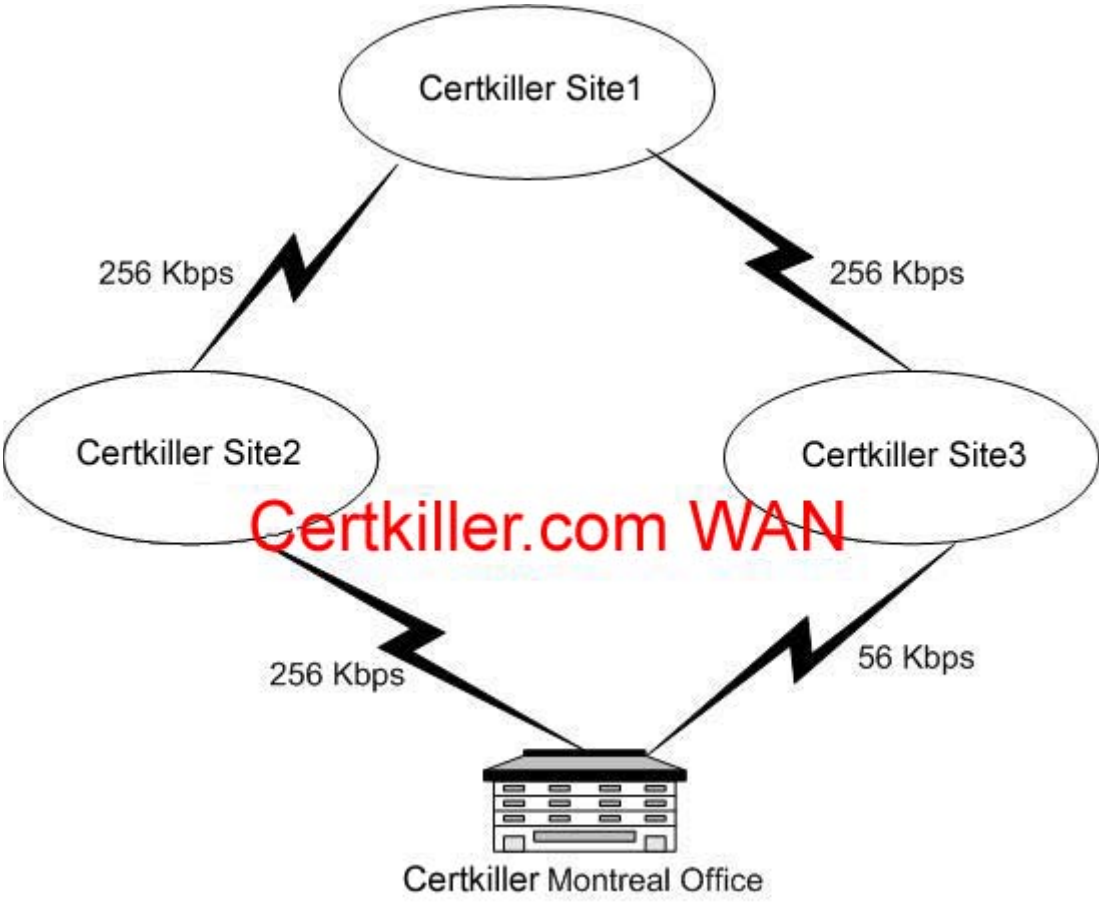
D.



Answer: C

Explanation: We need to delegate the management of different groups of users. We have the nonmanagement employees, who should be managed by the Help Desk staff. We have the employees (including management and help desk staff), who should be managed by the level 2 staff. The MIS group need to manage every other account. To solution to this question is to delegate the management of user accounts at domain level for the MIS group. Delegate the management of user accounts to the Employees OU to the help desk staff. Delegate the management of user accounts to the Corp OU to the second-level support staff.

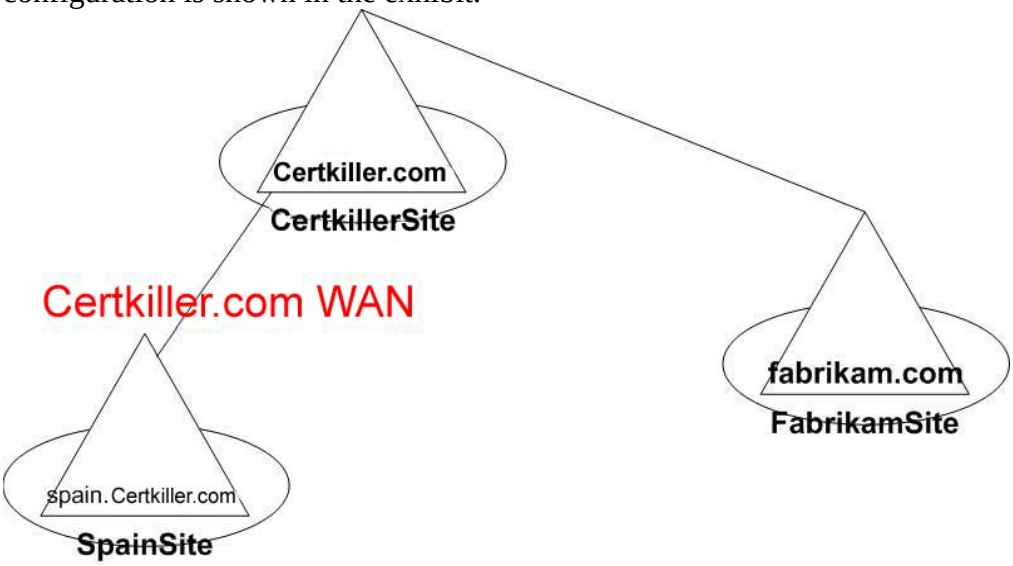
QUESTION 21
You are the network administrator for Certkiller. Certkiller has three offices. The network consists of a single Active Directory domain named Certkiller.com with three sites. Each office is configured as a separate site. Certkiller opens a new branch office in Montreal that has 10 users. This office does not contain a domain controller. The Montreal Office has WAN connections to two of the existing offices. A router is installed at each of the four offices to route network traffic across the WAN connections. The network after the addition of the Montreal Office is shown in the exhibit.



You need to ensure that when the users in the Montreal office log on the domain during normal operations, they will be authenticated by a domain controller in Certkiller Site2. What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)
A. Create a new IP subnet object that includes the subnet used in the Montreal Office. Link the new subnet object to the Certkiller Site2 site object.
B. Create a new IP subnet object that includes the subnet used in the Montreal Office. Link the new subnet object to the Certkiller Site3 site object.
C. Create an additional site for the Montreal Office. Configure a site link to Certkiller Site3 with a cost of 300. Configure a site link to Certkiller Site2 with a cost of 200.
D. Create an additional site for the Montreal Office. Configure a site link to Certkiller Site2 with a cost of 300. Configure a site link to Certkiller Site3 with a cost of 200.
E. Assign IP addresses to the client computers in the Montreal Office that are on the same IP subnet as the network at Site2.
Answer: A, C
Explanation:

If we create a new subnet for Montreal site and include in this site the DC for that site, all the computers that are in that subnet will logon in the DC of Montreal subnet. If we create a new site, and configure a site link to Certkiller Site3 with a cost of 300 and a site link to Certkiller Site2 with a cost of 200, user logons will go over the site link with the lowest cost.
Setting Site Link Properties
Intersite replication occurs according to the properties of the connection objects. When the KCC creates connection objects it derives the replication schedule from properties of the site link objects. Each site link object represents the WAN connection between two or more sites.
Setting site link object properties includes the following steps:
Determining the cost that is associated with that replication path.
• The KCC uses cost to determine the least expensive route for replication between two sites that replicate the same directory partition.
• Determining the schedule that defines the times during which intersite replication can occur.
• Determining the replication interval that defines how frequently replication should occur during the times when replication is allowed as defined in the schedule.
Reference:
MS Windows server 2003 Deployment Kit
Designing and Deploying Directory and Security Services
Setting Site Link Properties

QUESTION 22
You are the network administrator for Acme. Acme consists of two subsidiaries named Certkiller and Fabrikam, Inc. The network consists of a single Active Directory forest that contains three domains. The domain and site configuration is shown in the exhibit.



A computer named DC1.spain.Certkiller.com is a domain controller in the spain.Certkiller.com domain. DC1.spain.Certkiller.com is also a global catalog server and the preferred bridgehead server for Spain Site. The Active Directory database on DC1.spain.Certkiller.com contains 1 GB of data. The Spain departments in Certkiller are implementing an Active Directory-enabled application. You expect size of the database on DC1.spain.Certkiller.com to increase by 200 MB. Active Directory stops responding on DC1.spain.Certkiller.com. You discover that the hard disk has less then 5 MB of space remaining. You need to configure DC1.spain.Certkiller.com so that Active Directory can restart. You also need to configure the server

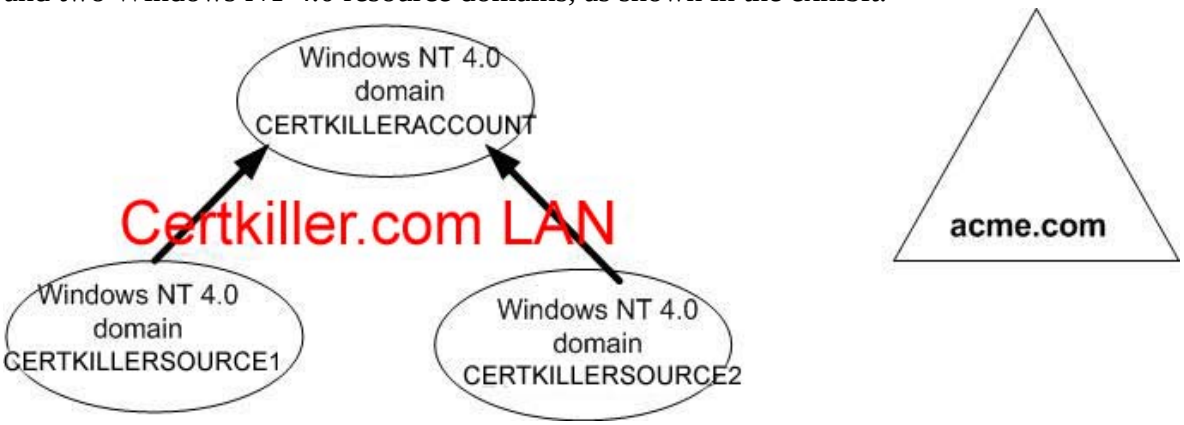
so that additional space is available on the hard disk for the additional data that will
be added to the Active Directory database. What should you do?
A. Delete all log files that are located in the NTDS folder.
B. Install another hard disk in DC1.spain.Certkiller.com. Use the Ntdsutil utility to move the database to the new hard disk.
C. Install another hard disk in DC1.spain.Certkiller.com. Use the Ntdsutil utility to move the transaction logs to the new hard disk.
D. Configure another server in the site to operate as a preferred bridgehead server. Configure DC1.spain.Certkiller.com so that it no longer operates as a preferred bridgehead server.
Answer: B
Explanation:
You will need to use the NTDSUTIL command with the 'files' switch. To perform this operation you will need to restart the DC in Directory services restore mode. This operation can not be performed in normal mode, because the database and log are in use.
Ntdsutil
Ntdsutil.exe is a command-line tool that provides management facilities for Active Directory. Use Ntdsutil.exe to perform database maintenance of Active Directory, manage and control single master operations, and remove metadata left behind by domain controllers that were removed from the network without being properly uninstalled. This tool is intended for use by experienced administrators.
Files
Provides commands for managing the directory service data and log files. The data file is called Ntds.dit. At the files: prompt, type any of the parameters listed under Syntax.
Syntax
{compact to %s|header | info | integrity|move DB to %s|move logs to %s|recover|set path backup %s|set path db %s|set path logs %s|set path working dir %s
Parameters
compact to %s (where %s identifies an empty target directory) Invokes Esentutl.exe to compact the existing data file and writes the compacted file to the specified directory. The directory can be remote, that is, mapped by means of the net use command or similar means. After compaction is complete, archive the old data file, and move the newly compacted file back to the original location of the data file. ESENT supports online compaction, but this compaction only rearranges pages within the data file and does not release space back to the file system. (The directory service invokes online compaction regularly.)
header
Writes the header of the Ntds.dit data file to the screen. This command can help support personnel analyze database problems.
info
Analyzes and reports the free space for the disks that are installed in the system, reads the registry, and then reports the sizes of the data and log files. (The directory service maintains the registry, which identifies the location of the data files, log files, and directory service working directory.)
integrity
Invokes Esentutl.exe to perform an integrity check on the data file, which can detect any kind of low-level database corruption. It reads every byte of your data file; thus it can take a long time to process large databases.Note that you should always run Recover before performing an integrity check. move DB to %s(where %s identifies a target directory)
Moves the Ntds.dit data file to the new directory specified by %s and updates the registry so that, upon system restart, the directory service uses the new location. move logs to %s(where %s identifies a target directory)

Moves the directory service log files to the new directory specified by %s and updates the registry so that, upon system restart, the directory service uses the new location.
recover
Invokes Esentutl.exe to perform a soft recovery of the database. Soft recovery scans the log files and ensures all committed transactions therein are also reflected in the data file. The Windows 2000 Backup program truncates the log files appropriately. Logs are used to ensure committed transactions are not lost if your system fails or if you have unexpected power loss. In essence, transaction data is written first to a log file and then to the data file. When you restart after failure, you can rerun the log to reproduce the transactions that were committed but hadn't made it to the data file.
set path backup %s (where %s identifies a target directory) Sets the disk-to-disk backup target to the directory specified by %s. The directory service can be configured to perform an online disk-to-disk backup at scheduled intervals.
set path db %s (where %s identifies a target directory) Updates the part of the registry that identifies the location and file name of the data file. Use this command only to rebuild a domain controller that has lost its data file and that is not being restored by means of normal restoration procedures.
set path logs %s (where %s identifies a target directory)
Updates the part of the registry that identifies the location of the log files. Use this command only if you are rebuilding a domain controller that has lost its log files and is not being restored by means of normal restoration procedures.
set path working dir %s (where %s identifies a target directory)
Sets the part of the registry that identifies the directory service's working directory to the directory specified by %s.
%s An alphanumeric variable, such as a domain or domain controller name.
quit
Takes you back to the previous menu or exits the utility.
? or help
Displays help at the command prompt.
Reference
SERVER HELP

QUESTION 23
You are the network administrator for Certkiller. Your network consists of a single Active Directory domain named Certkiller.com. The functional level of the domain is Windows Server 2003. You add eight servers for a new application. You create an organizational unit (OU) named Application to hold the servers and other resources for the application. Users and groups in the domain will need varied permissions on the application servers. The members of a global group named Server Access Team need to be able to grant access to the servers. The Server Access Team group does not need to be able to perform any other tasks on the servers. You need to allow the Server Access Team group to grant permissions for the application servers without granting the Server Access Team group unnecessary permissions.
What should you do?
A. Create a Group Policy object (GPO) for restricted groups. Configure the GPO to make the Server Access Team group a member of the Power Users group on each application server. Link the GPO to the Application OU.
B. Grant the Server Access Team group permissions to modify computer objects in the Application OU.
C. Move the Server Access Team group object into the Application OU.
D. Create domain local groups that grant access to the application servers Grant the Server Access Team group

permissions to modify the membership of the domain local groups.
Answer: D
Explanation:
The simplest way to do this is to create domain local groups with various permissions to the application servers. For example, one group has read access, another group has read and write access and so on. We can then use the Delegation of Control Wizard to grant the right to add or remove members of the groups.
Incorrect Answers:
A: The Power Users group can perform many administrative tasks on the servers. This is more permission than necessary.
B: They don't need to modify the computer objects. This is more permission than necessary.
C: This won't give them the required permissions.

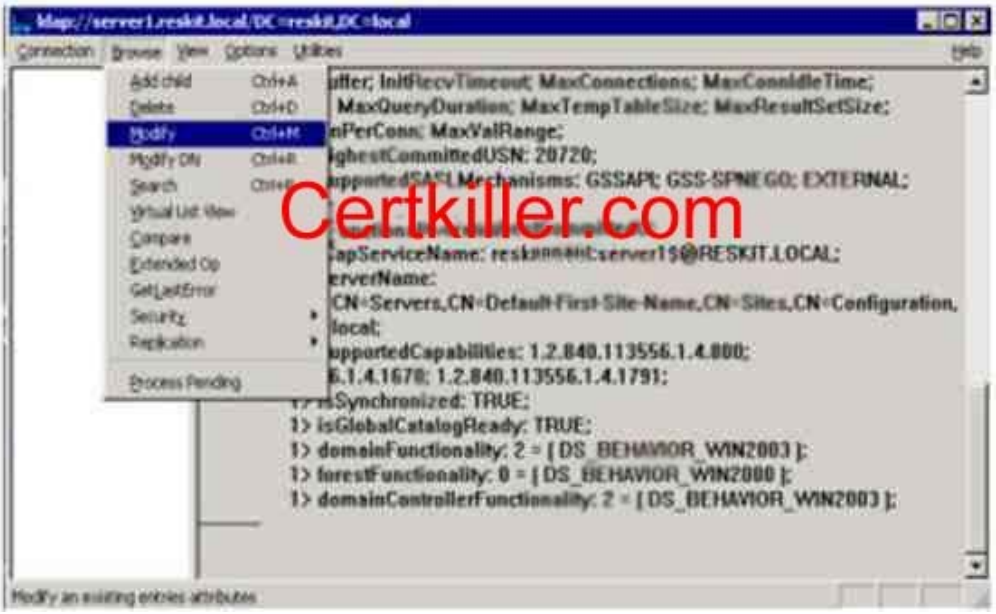
QUESTION 24
You are the network administrator at Acme Inc. The network consists of a single Active Directory forest that contains a single domain named acme.com. The functional level of the forest is Windows Server 2003. Acme purchase a company named Certkiller. The Certkiller network consists of one Windows NT 4.0 account domain and two Windows NT 4.0 resource domains, as shown in the exhibit.



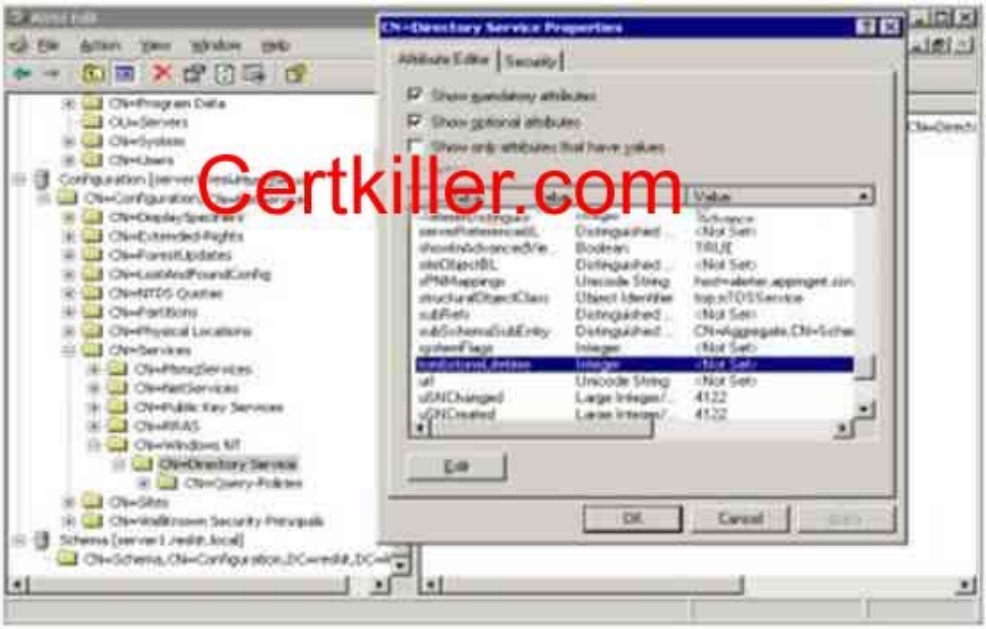
All file resources are stored on file servers in the acme.com domain and in the CertkillerSOURCE1 domain.
You need to accomplish the following goals:
• You need to minimize the number of trust relationships that must be maintained in the network environment.
• Users in each company must be able to access the file resources on the file servers in the other company's domain.
Which two actions should you take? (Each correct answer presents part of the solution. Choose two)
A. Create a one-way external trust relationship in which the CertkillerSOURCE1 domain trusts the acme.com domain.
B. Create a one-way external trust relationship in which the acme.com domain trusts the CertkillerSOURCE1 domain.
C. Create a one-way external trust relationship in which the acme.com domain trusts the CertkillerACCOUNT domain.
D. Create a one-way external trust relationship in which the CertkillerACCOUNT domain trusts the acme.com domain.
Answer: A, C
Explanation:
For users in the acme.com domain to access resources in the CertkillerSOURCE1 domain, the CertkillerSOURCE1 domain needs to trust the acme.com domain. For users in the CertkillerACCOUNT

domain to access resources in the acme.com domain, the acme.com domain needs to trust the CertkillerACCOUNT domain.

QUESTION 25
You are a network administrator for Acme. Acme consists of two subsidiaries named Litware Inc., and Certkiller GmBh. The network consists of a single Active Directory forest. The functional level of the forest is Windows Server 2003. The forest contains a forest root domain named litwareinc.com and an additional domain tree named Certkiller.com, which contains two child domains. All domain controllers run Windows Server 2003. The Directory Services object is configured with the default property settings. The forest contains 250,000 objects that are changed frequently. You need to be able to restore objects in one of the child domains in the Certkiller.com domain tree from a three-month-old backup. You need to make a change to a Directory Services property on a domain controller in one of the domains in order to achieve this goal.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)
A. Run the netdom command on a domain controller in Certkiller.com.
B. Use the Ntdsutil utility on a domain controller in litwareinc.com.
C. Use the ADSIEdit utility on a domain controller in Certkiller.com.
D. Run the Idp command on a domain controller in litwareince.com.
Answer: C, D
Explanation:
We need to edit a property of Active Directory. We can need to use a low level editor to do this. AdsiEdit. A Microsoft Management Console (MMC) snap-in that acts as a low-level editor for the Active Directory(r) service. Through the Active Directory Services Interfaces (ADSI), it provides a means to add, delete, and move objects within the Directory Services. The attributes of each object can be viewed, changed, and deleted. Ldp. A graphical tool that allows users to perform Lightweight Directory Access Protocol (LDAP) operations, such as connect, bind, search, modify, add, and delete, against any LDAP-compatible directory, such as Active Directory. LDAP is an Internet-standard wire protocol used by Active Directory.
Reference:
http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q216/9/93.ASP&NoWebContent=1
Backup of the Active Directory Has 60-Day Useful Life MS KB article 216993
Use the Active Directory editing tool of your choice so that the "tombstone Lifetime" attribute is set to be older than the backup used to restore the Active Directory. Supported tools include Adsiedit.msc, Ldp.exe, and ADSI Scripts. LDP provides an interface to perform LDAP operations against Active Directory.

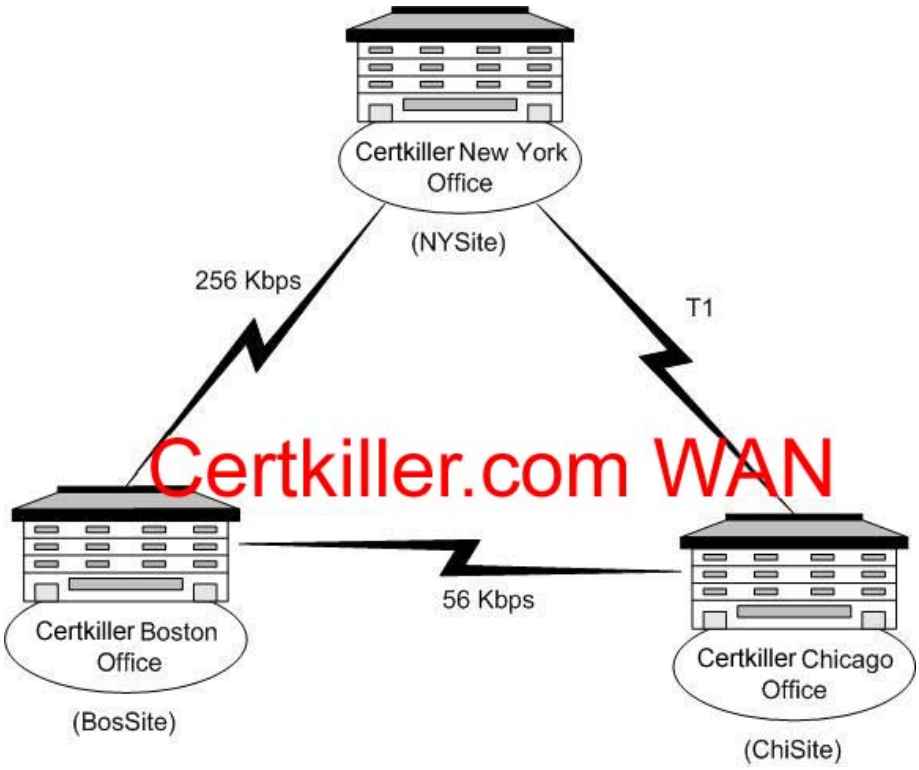


ADSI Edit you can use to edit objects in the Active Directory database.



QUESTION 26

You are the network administrator for Certkiller, a company that has three offices. The offices are in Boston, Chicago, and New York. All three offices are connected by leased lines as shown in the exhibit.



Certkiller is deploying a Windows Server 2003 forest. You create a single Active Directory domain named Certkiller.com You configure each office as a single site. You configure three domain controllers in NYSite. You create a domain controller in each of the other sites. You create site links based on the network topology. Each leased line is represented by a site link. Each site link connects only two sites. The cost and the schedule for all site links is the same. The sites and site links are named as shown in the following table.

Site link name	Linked site	Linked site
NYBoston	NYSite	BosSite
NYChi	NYSite	ChiSite
ChiBoston	ChiSite	BosSite

Users report that network requests between BosSite and ChiSite are taking much longer than they used to take. You discover that replication traffic is using an unacceptably large percentage of the bandwidth between BosSite and ChiSite

You need to reduce replication traffic over the ChiBoston site link. What should you do?

A. Create an SMTP-based connection object from a domain controller in NYSite to a domain controller in BosSite.

B. Increase the cost of the ChiBoston site link.

C. Create a site link bridge that includes the NYBoston and NYChi site links.

D. Increase the replication interval for the NYBoston site link.

Answer: B

Explanation:

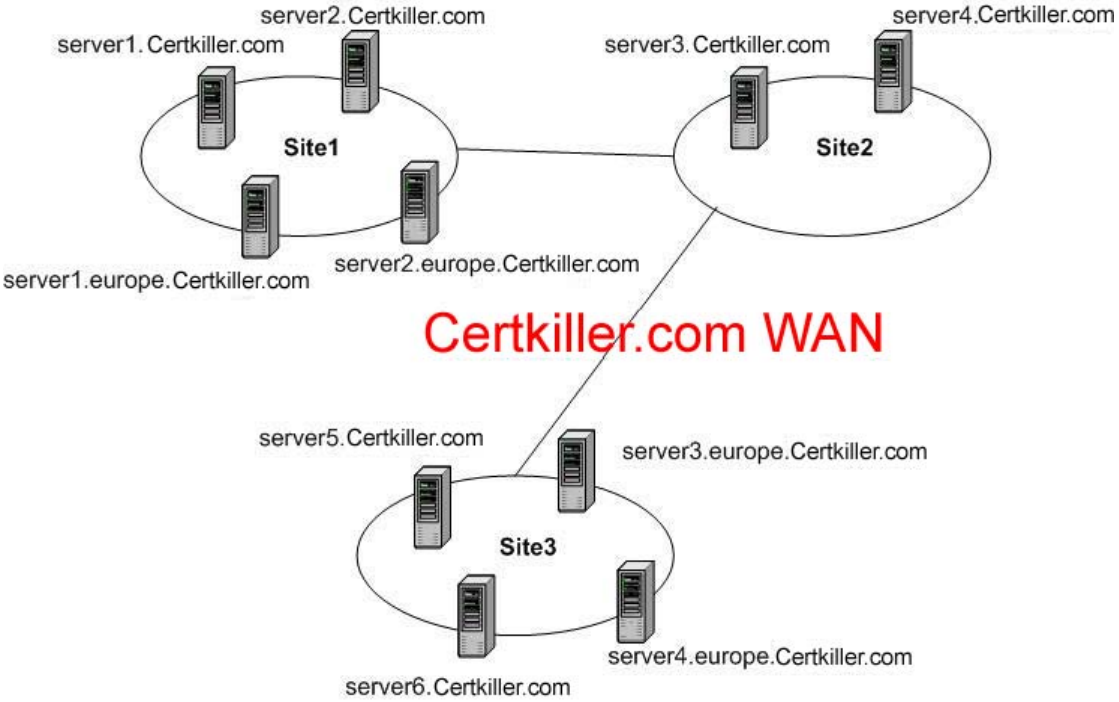
If we increase the cost of the ChiBoston site link to a value greater than the cost of the other two links added together, then no replication will go over the ChiBoston site link - it will all travel over the NYBoston and the NYChi site links.

Setting Site Link Properties

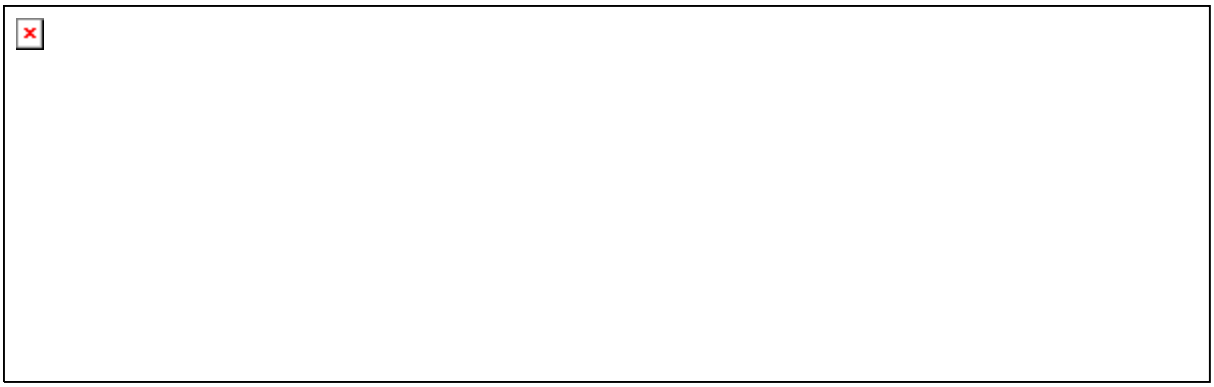
Intersite replication occurs according to the properties of the connection objects. When the KCC creates connection objects it derives the replication schedule from properties of the site link objects. Each site link

object represents the WAN connection between two or more sites.
Setting site link object properties includes the following steps:
Determining the cost that is associated with that replication path.
• The KCC uses cost to determine the least expensive route for replication between two sites that replicate the same directory partition.
• Determining the schedule that defines the times during which intersite replication can occur.
• Determining the replication interval that defines how frequently replication should occur during the times when replication is allowed as defined in the schedule.
Reference:
MS Windows server 2003 Deployment Kit
Designing and Deploying Directory and Security Services
Setting Site Link Properties

QUESTION 27
You are the network administrator for Certkiller. The network consists of a single Active Directory forest that contains one root domain and one child domain. The forest also contains three separate sites, as shown in the Network Diagram exhibit.

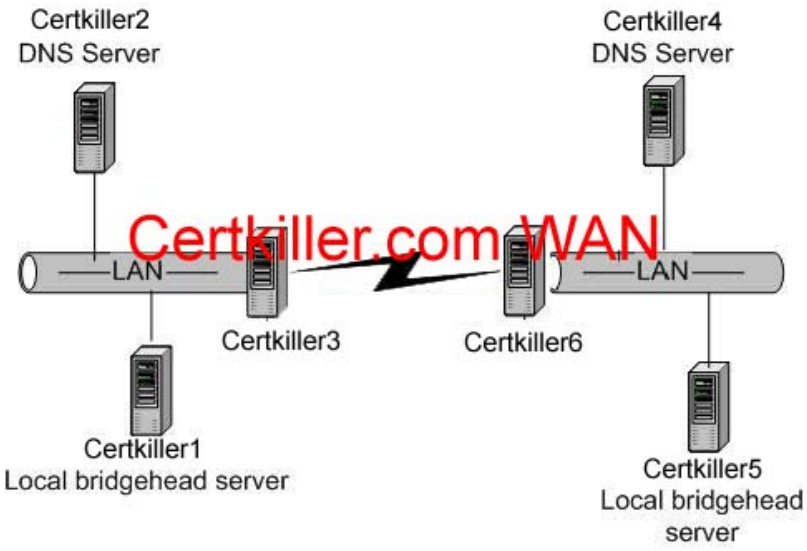


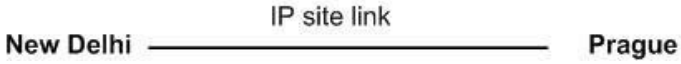
The network is not fully routed and there is no direct physical connection between Site1 and Site3. Site links are not bridged. You discover that the domain controllers for europe.Certkiller.com located in Site1 have additional accounts that are not on the domain controllers for europe.Certkiller.com located in Site3. You examine the directory service log in Event Viewer on a domain controller for europe.Certkiller.com-You discover the error message shown in the Error Message exhibit.



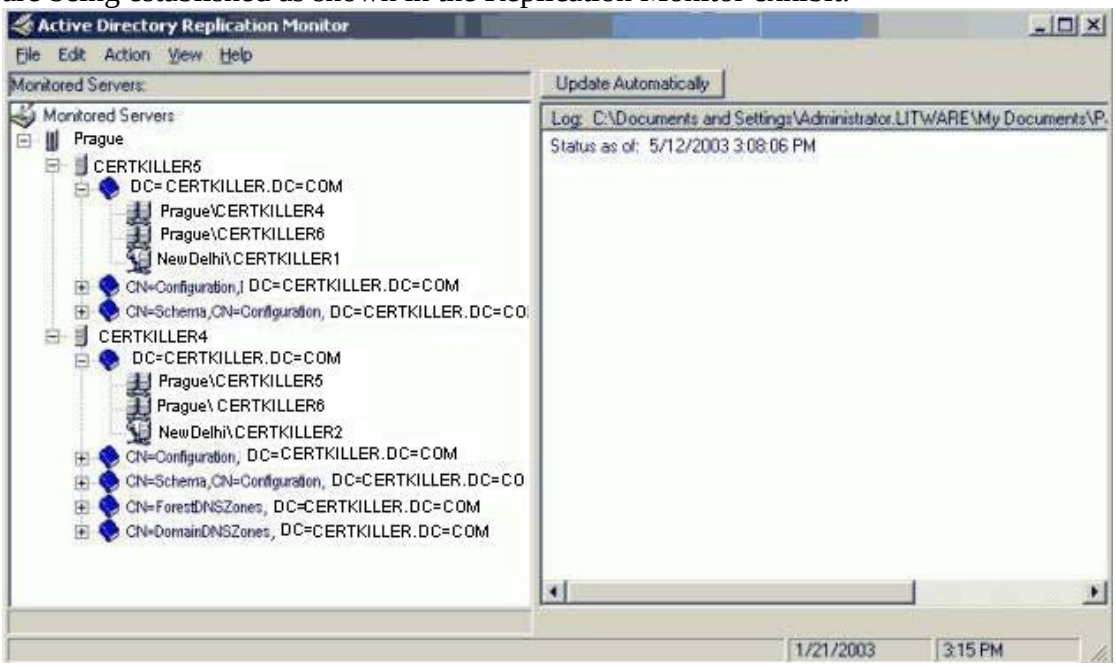
You need to resolve the condition that is causing this error. What should you do?
A. Add a domain controller for the europe.Certkiller.com domain to Site2.
B. Configure a site link bridge between the site links for Site1 and Site3.
C. Configure at least one domain controller in each site to be a global catalog server.
D. Create a site link between Site1 and Site3.
Answer: B
Explanation:
We don't have a site link between site1 and site3. We have a site link between Site1 and Site2 and between Site2 and Site3. We have no physical connectivity between site1 and site3, so we should therefore create a site link bridge between the site links for Site1 and Site3. Any replication between site1 and site3 will then travel over the two existing site links. One computer in any given site owns the role of creating inbound replication connection objects between bridgehead servers from other sites. This domain controller is known as the Inter-Site Topology Generator. While analyzing the Site Link and Site Link Bridge structure to determine the most cost-effective route to synchronize a naming context between two points, it may determine that a site does not have membership in any Site Link and therefore has no means to create a replication object to a bridgehead server in that site. The first site in the Active Directory (named "Default-First-Site-Name"), is created automatically for the administrator. This site is a member of the default Site Link ("DEFAULTIPSITELINK"), which is also created automatically for the administrator, and is used for RPC communication over TCP/IP. If the administrator were to create two additional sites ("Site1" and "Site2" for example), the administrator must define a Site Link that the site will be a member of before they can be written to the Active Directory. However, the administrator can open the properties of a Site Link and modify which sites reside in the Site Link. If the administrator were to remove a site from all Site Links, the KCC displays the error message listed above to indicate that a correction needs to be made to the configuration.
References:
Troubleshooting Event ID 1311: Knowledge Consistency Checker KB article 214745
Incorrect Answers:
A: This will cause excessive replication traffic between site2 and site3. This defeats the object of using sites to control replication traffic.
C: Global Catalog placement is not the cause of the error in this question.
D: We have no physical connectivity between site1 and site3.

QUESTION 28
You are a network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com com with two sites. All servers run Windows Server 2003. The network is configured as shown in the Network Diagram exhibit.





You use Replication Monitor to monitor Active Directory replication. You discover that replication connections are being established as shown in the Replication Monitor exhibit.



You need to ensure that replication takes place only between defined preferred bridgehead servers. You need to accomplish this task without incurring any additional replication traffic. What should you do?

A. Configure Certkiller1 and Certkiller5 as additional DNS servers.

B. Configure Certkiller3 and Certkiller6 as additional DNS servers.

C. Configure only Certkiller2 and Certkiller4 as preferred bridgehead servers.

D. Configure only Certkiller3 and Certkiller4 as preferred bridgehead servers.

Answer: C

Explanation:

We have replication between the bridgehead servers and the between the DNS servers. If we configure the DNS

servers as bridgehead servers, all the replication will be between the two machines. When two sites are connected by a site link, the replication system automatically creates connections between specific domain controllers in each site called bridgehead servers. In Microsoft(r) Windows(r) 2000, intersite replication of the directory partitions (e.g. domain, configuration, and schema) between domain controllers in different sites is performed by the domain controllers (one per directory partition) in those sites designated by the KCC as the bridgehead server. In Windows Server 2003, the KCC may designate more than one domain controller per site hosting the same directory partition as a candidate bridgehead server. The replication connections created by the KCC are randomly distributed between all candidate bridgehead servers in a site to share the replication workload. By default, the randomized selection process takes place only when new connection objects are added to the site. However, you can run Adlb.exe, a new Windows Resource Kit tool called Active Directory Load Balancing (ADLB) to rebalance the load each time a change occurs in the site topology or in the number of domain controllers the site. In addition, ADLB can stagger schedules so that the outbound replication load for each domain controller is spread out evenly across time. Consider using ADLB to balance replication traffic between the Windows Server 2003-based domain controllers when they are replicating to more than 20 other sites hosting the same domain

---

QUESTION 29

You are a network administrator for Certkiller. The network consists of a single Active Directory domain named Certkiller.com with two sites. The Active Directory database is backed up every evening. A network administrator in Site1 deletes an empty organizational unit (OU) named Projects. At about the same time, a network administrator in Site2 moves 20 existing user accounts into the Projects OU. Later, the administrator in Site2 discovers that the Projects OU was deleted from Active Directory. He cannot see the user accounts that he moved into the OU. You need to provide an OU named Projects and add the 20 user accounts to the Projects OU. The users' access to network resources must not be affected by this process. What should you do?

A. Perform an authoritative restore operation of the Projects OU and the user accounts on a domain controller in Site2.

B. Perform a nonauthoritative restore operation of the Projects OU and the user accounts on a domain controller in Site2.

C. Create a new OU named Projects. Create 20 new user accounts that have the same user principal name (UPN) prefix.
Move the user accounts into the new Projects OU.

D. Create a new OU named Projects. Move the 20 user accounts from the LastAndFound container to the new Projects OU.

Answer: D

Explanation:

You moved the users to an OU that had just been deleted. When you move objects to an object that is no longer there, the objects get moved to the LostAndFound container. This means that we haven't lost the user accounts, so we can just re-create the Projects OU and move the users from the LostAndFound container to the new OU.

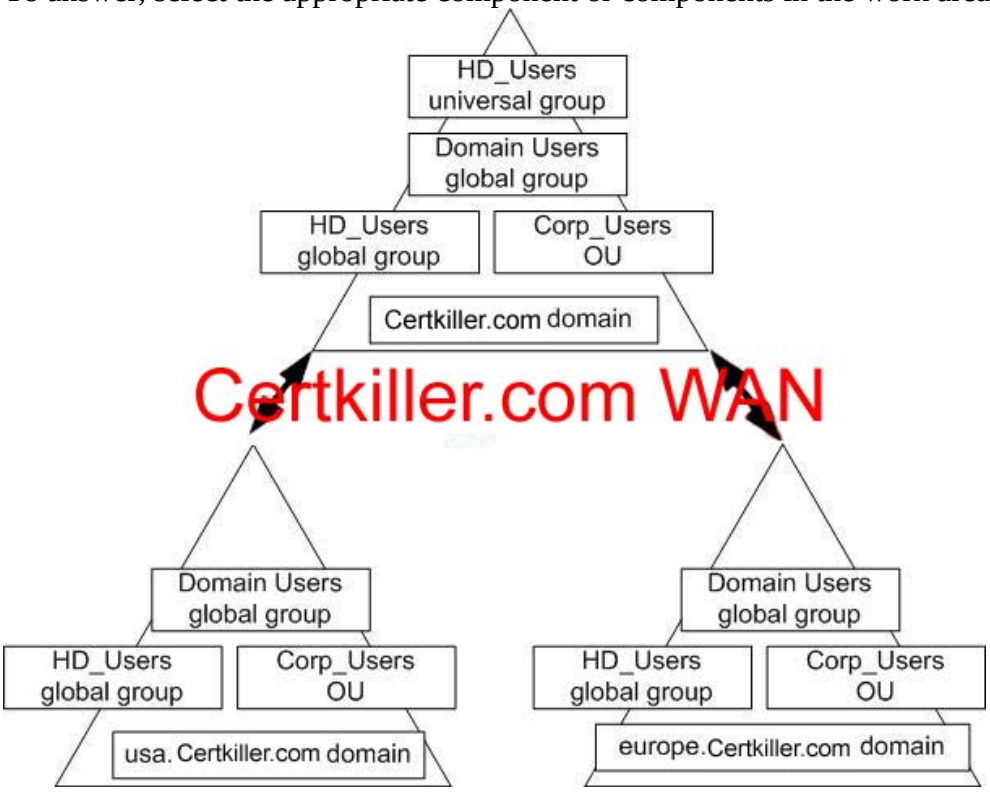
Incorrect Answers:

A: The user accounts haven't been deleted, so we don't need to restore them.

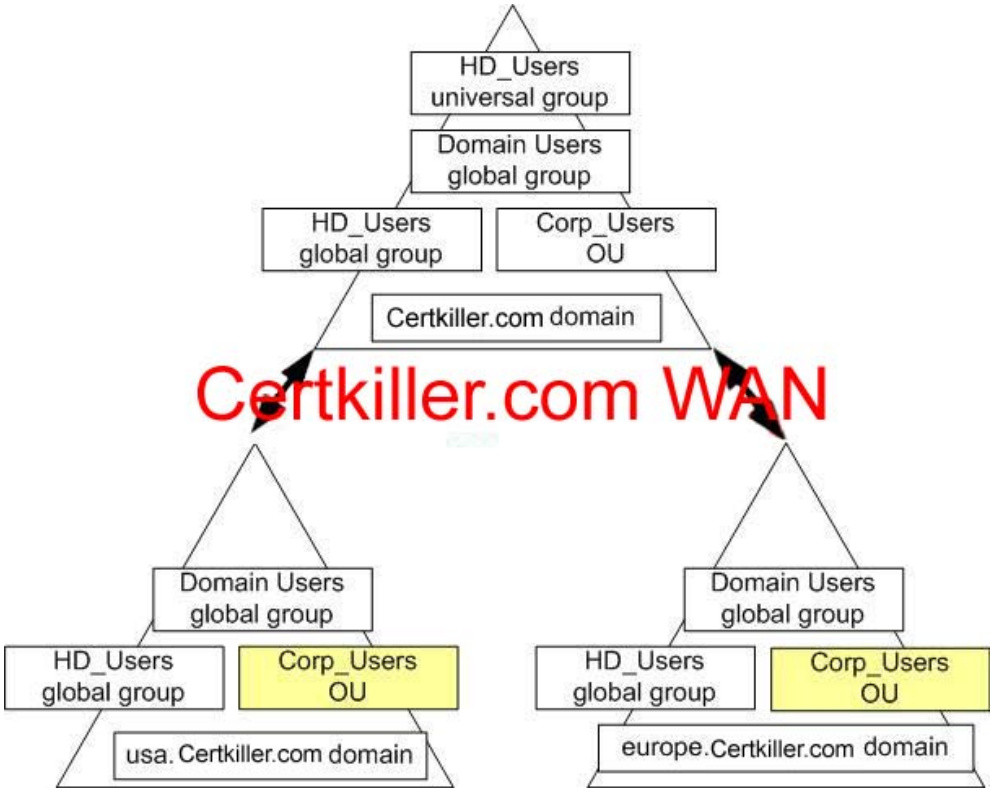
B: The user accounts haven't been deleted, so we don't need to restore them.

C: The user accounts haven't been deleted, so we don't need to recreate them. Furthermore, recreating the user accounts in this way will not work to restore the original accounts. The new accounts will be different accounts with different SIDs (Security Identifiers).

QUESTION 30
You are the network administrator for Certkiller. The network consists of a single Active Directory forest that contains three domains named Certkiller.com, usa.Certkiller.com, and europe.Certkiller.com. The functional level of the forest is Windows Server 2003. The help desk department is responsible for resetting passwords for all user accounts in the forest except for accounts that have administrative privileges. There is an organizational unit (OU) named Corp_Users in each domain that contains the user accounts in that domain. All of the user accounts that have administrative privileges are in the default Users container in each domain. There is a universal group named HD_Users in the Certkiller.com domain. All user accounts for the help desk department users are members of the HD_Users group. You need to delegate the required authority for resetting passwords to the users in the help desk department. For which Active Directory component or components should you delegate control?
To answer, select the appropriate component or components in the work area.



Answer:



Explanation: We need to delegate the required authority for resetting passwords for the Corp_Users OU to the HD_Users universal group. The Corp_Users OU in each domain contains the users that the help desk staff need to reset passwords for. The HD_Users universal group contains the help desk staff and is visible to all domains in the forest.