
QUESTION 1 You are the administrator of a Windows NT domain. You recently used Syskey.exe on a BDC named serverA. ServerA is backed up once each week, and a new emergency Repair Disk is created at the same time. You shut down ServerA and cannot restart it. You cannot locate the floppy disk that contains the Syskey encryption key.

What should you do so that you can start ServerA?

- A. Start serverA by choosing the safe mode option, and use Windows NT backup to restore ServerA's registry from the most recent backup tape that was created before Syskey.exe was used
- B. Start serverA by choosing the safe mode option, and use Windows NT backup to restore ServerA's registry from the first recent backup tape that was created after Syskey.exe was used
- C. Run the emergency repair process by using the most recent ERD that was created before Syskey.exe was used
- D. Run the emergency repair process by using the ERD that was created after Syskey.exe was used.

Answer: C

Explanation:

In order to back off the process, you need to restore the SAM as well as the key. Running the emergency repair process with the older ERD will properly regress the syskey.

Incorrect Answers:

- A, B. Windows NT does not have a "safe mode" startup. This is available in Windows 98 and Windows 2000. That aside, restoring the registry is not enough, the SAM (the accounts database) would need to be restored also. The emergency repair process should accomplish this.
- D. Assuming that a new ERD was created after the syskey operation, this would put you right back where you were, a system that can't start and no encryption key to start it.

QUESTION 2 You are the lead administrator of a Windows NT server network. Occasionally, an assistant administrator temporarily adds a user account to the Domain Admins group and then forgets to remove that user account when the need for the extra permissions has passed. You want to ensure that unwanted additional to your Domain Admins group are periodically removed, and that any existing user accounts that are accidentally removed are added back to the group. You want to accomplish these tasks by using the least amount of administrative effort.

What should you do?

- A. Create a batch file that deletes the Domain Admins group and then re-creates it and adds the appropriate user accounts as members. Configure the Task Scheduler service on the PDC to run this batch file every Monday and Thursday.
- B. Create a batch file that deletes the Domain Admins group and then re-creates it and adds the appropriate user accounts as members. Configure the Task Scheduler service on your client computer to run this batch file every Monday and Thursday.
- C. Create a security template that lists the Domain Admins group as a restricted group that has the appropriate user accounts as members. Configure the Task Scheduler service on the PDC to run the command-line version of Security Configuration Manager so that it applies the template every Monday and Thursday.
- D. Create a security template that lists the Domain Admins group as a restricted group that has the appropriate user accounts as members. Every Monday and Thursday, on your client computer, run the GUI version of Security Configuration Manager to apply the template to the PDC.

Answer: A

Explanation: As much as I don't like this, this is the best choice. I don't like it because if the procedure fails, you better have a backup way into the system, because the Domain Admins could end up empty if the procedure

fails after the delete. Anyway, this solution will work. Running the task on different days, and not every day does the periodic cleanup, is less often, and there is less of an exposure for failure. Since Monday and Thursday are the same options in ALL the choices, we don't need to address that. Finally, we want procedure to occur on the PDC, so that it will run even if the network is down.

Incorrect Answers:

B. Running the procedure on the client is a security risk, anyone who can compromise the client can also compromise the entire network. Workstations are not always kept in secure locations. Also, even if the workstation was secured, it might not always be up, as some people physically turn off the machine after-hours. Finally, if the network is down, or the workstation is unplugged, the procedure will not run, where if it runs on the PDC, it will always have access to the SAM database. Example: Supposed my user account was added to Domain Admin, and I knew this procedure ran, and when. I could go to the client, disconnect the network cable, and the update does not occur. I have now subverted the security.

C, D. Restricted groups were introduced in Windows 2000. It does not exist in Windows NT. If it did, it would have to be added with Service Pack 4 or later. Note that authenticated users were added in SP3. Since this is a NT server network, which implies NT 4.0, then we can't use this option.

QUESTION 3 Two weeks ago, you became the lead administrator of an existing Windows NT domain. Success and failure auditing of Logon and Logoff events is enabled for the domain. Success and failure auditing of file and object access events is also enabled.

Every Friday afternoon, an assistant administrator backs up each of the event logs and archives them to CD-ROM. Your event logs are each configured to have a maximum size of 32,768KB, and they are configured so that events in the log are not overwritten.

On Thursday at 5:00 P.M., during a week when almost everyone in the company has been working longer than usual, your PDC fails and displays the following stop error:

STOP: C0000244 (Audit Failed)

An Attempt to generate a security audit failed.

You restart the PDC, but after approximately five minutes, it stops again and displays the same message.

You need to restore the PDC to full functionality.

What three courses of action should you take? (Each correct answer presents part of the solution. Choose Three)

A. On BDC, start User manager for Domains. In the Audit Policy dialog box, click the Do Not Audit option button.

B. Restart the PDC, and log on to it as Administrator

C. Use Event Viewer to archive the PDC's system, log

D. Use Event Viewer to archive the PDC's security log

E. Use Event Viewer to configure Event Log Wrapping to overwrite events older than seven days for the PDC's system log

F. Use Event Viewer to configure Event Log Wrapping to overwrite events older than seven days for the PDC's security log

G. Use Event Viewer to configure the PDC's system log to have a maximum log size of 48,064 KB

H. Use Event Viewer to configure the PDC's security log to have a maximum log size of 48,064 KB

Answer: B, D, H

Explanation: If the CrashOnAuditFail registry key is set to 1 and the Security Event log is full on a computer running Windows NT, the following blue screen error message may be displayed:

STOP: C0000244 {Audit Failed}

An attempt to generate a security audit failed.

This occurs when the security log is full, since the PDC failed, you must log onto the PDC. You must work with

the security log, and not the system log, since it is the security log at issue here. So you would want to archive the FULL security log, and since it is not large enough, make it larger.

Incorrect Answers:

- A. The recovery must be done on the failing system.
- C. Must work with Security Log, not System Log.
- E. Must work with Security Log, not System Log.
- F. Wrapping the security log has a potential of losing security audit records. This is not good security practice.
- G. Must work with Security Log, not System Log.

QUESTION 4 You are the Administrator of one of your company's Windows NT domains. You are modifying a security template that was created by the administrator of one of the company's other domain. The template contains password policy settings that represent the company's minimum standards for password policy. When you finish modifying the template, it will be applied to all domain controllers in every domain in the company. You have the template open in security configuration manager on your PDC. You are modifying a portion of the Security option section of the template. You analyze your domain's current settings against the template's settings. The results of the analysis are shown in the exhibit.

Attribute	Stored Configuration	Analyzed System Sett..
Allow system to be shutdown without having to log on	Disabled	Enabled
Audit access to internal system object	Disabled	Disabled
Audit use of all users rights including Backup and Restore	Not Configured	Not configured
Autodisconnect: Allow sessions to be disconnected when are idle	Enabled	Enabled
Autodisconnect: Amount of idle time required before disconnecting sess...	15	15
Change Administrator account name to	Not Configured	Bos\$8
Change Guest account name to	Not Configured	G7&yt
Clear virtual memory pagefile when system shuts down	Enabled	Disabled
Digitally sign client side communication always	Disabled	Disabled
Digitally sign client side communication when possible	Enabled	Enabled
Digitally sign server-side communication always	Disabled	Enabled
Digitally sign server-side communication when possible	Enabled	Enabled
Disallow enumeration of account names and shares by anonymous users	Disabled	Enabled
Do not display last username in logon screen	Enabled	Enabled
Forcibly logoff when logon hours expire	Enabled	Enabled

You want to ensure that the level of security on the servers in your domain will not be weakened after you apply the modified template.

Which four changes should you make to the template? (Each correct answer presents part of the solution. Choose four)

- A. Set the Audit use of all user rights including Backup and Restore attribute to Enable
- B. Set the change administrator account name to attribute to Bos\$8
- C. Set the change Guest account name to attribute to G7&yt
- D. Set the Digitally sign server-side communication when possible attribute to Enabled
- E. Set the Digitally sign server-side communication when possible attribute to Disabled
- F. Set the Disallow enumeration of account names and shares by anonymous users attribute to Enabled
- G. Set the Forcibly logoff when logon hours expire attribute to disabled

Answer: Unknown

Explanation: This is a rough question. The problem is that the stored configuration is the template configuration, and the Analyzed configuration is the current domain settings. There are 4 situations where one side (Stored vs. Analyzed) is enabled and the other is disabled. Those need to be concentrated on. When you have a template as

Not Configured, it does not change or affect the current settings when applied, so those can be ignore, and you can ignore when both sides are Not Configured. In this question, where the Stored matches the Analyzed, there

is no need to change them - because applying the template does not change the current system settings. Your objective is to prevent the security from being weakened, but you were not given the task to make it stronger. Incorrect Answers:

A. Since this option is not configured in the current system, nor the template, this option will not change. We are not deciding on new options for security to make it better, our objective is to make sure that applying the template does not regress the current security profile.

B, C - These entries show up as defined in the current configuration, but not-configured in the template. Since it is not-configured in the template, application of the template will not change or affect these entries.

D. Since this is enabled for the current system and the template, the resulting application of the template does not change the option. We are not deciding on new options for security to make it better, our objective is to make sure that applying the template does not regress the current security profile.

E. If we set this to disable, we weaken the current security model. This would actually be a change to set new security policy since this option is enabled in both the current system and the template. We are not deciding on new options for security to make it better, our objective is to make sure that applying the template does not regress the current security profile.

F. It is already enabled.

G. Since this is enabled for the current system and the template, the resulting application of the template does not change the option. We are not deciding on new options for security to make it better, our objective is to make sure that applying the template does not regress the current security profile.

QUESTION 5 You are the administrator of a Windows NT domain. In user manager for domains, you enable auditing as shown in the following table.

Audit event	Success	Failure
Logon and Logoff		X
File and Object Access	X	
Use if User Rights	X	
Security Policy Changes	X	X
Process Tracking	X	X

On a member server named Sea009, you enable access and failure auditing for the Everyone group on a shared folder named Bus Plans. Three days later, you examine the event logs on sea009, and you notice that no audit events are listed for the Bus Plans folder.

You want to audit all successful and failed attempts to access the Bus Plans folder.

What should you do?

A. Enable failure auditing of File and Object Access event for the domain.

B. Enable failure auditing of Use of User Rights event for the domain.

C. Enable success and failure auditing of file and object access events on sea009.

D. Enable success and failure auditing of Use of User Rights events on Sea009.

Answer: C

Explanation: A member server requires auditing to be enabled directly on the server itself. Domain auditing, which is set on a Domain Controller does not apply in this case. Also, your thinking in this type of situation should be: Why weren't there any Successes logged, were all the accesses failures? It should be apparent that either no one is

accessing the folder at all, or all accesses were failures Try to reason these issues when looking at the question.

Incorrect Answers:














A. A member server requires auditing to be enabled directly on the server itself. Domain auditing, which is set on a Domain Controller does not apply in this case.

B, D. Regardless of where the settings are performed, Use of ser Rights does not apply to use of a file. It is a file being used since we are auditing a shared folder.

QUESTION 6 You are the administrator of a Windows NT server network. Auditing is configured to audit individual accesses to the confidential data files on your network. Your audit logs are backed up and then cleared every Monday morning.

Last Friday, a security breach occurred on a confidential data file on one of your network servers, which is named Server3. The security log on Server3 contained no Audit events after last Wednesday morning.

You decide to use Security configuration manager to edit a security template and to apply the template to all servers that contain confidential data. You want the template to have appropriate settings so that all events for which auditing is enabled will be successfully recorded in your audit logs. You plan to continue to back up and then clear your audit logs every Monday morning. You start security configuration Manager, and you import the Hisecdc4.inf template. You analyze server3's current settings against the template's settings. The settings for event logs portion of the template and the results of the analysis are shown in the exhibit.

Attribute	Stored Configuration	Analyzed System Sett..
 Maximum log size for Application Log	6144 Kbytes	512 KBytes
 Maximum Log Size for Security Log	6144 Kbytes	512 KBytes
 Restrict Guest access to Application Log	6144 Kbytes	512 KBytes
 Restrict Guest access to System Log	Enabled	Disabled
 Restrict Guest access to Security Log	Enabled	Disabled
 Retain Application Log for	Enabled	Disabled
 Retain Application Log for	Not Configured	7 Days
 Retain Security Log for	Not Configured	7 Days
 Retain System Log for	Not Configured	7 Days
 Retention method for Application Log	As Needed	By Days
 Retention method for Security Log	As Needed	By Days
 Retention method for System Log	As Needed	By Days
 Shutdown system when security audit log becomes full	Not Configured	Disabled

Which two changes should you make to the template? (Each correct answer presents part of the solution. Choose two)

- A. Set the maximum log size for security log attribute to 512 Kbytes
- B. Set the maximum log size for system log attribute to 512 Kbytes
- C. Set the Restrict guest access to security log attribute to Disabled
- D. Set the Retention method for security log attribute to Do Not overwrite events
- E. Set the Retention method for system log attribute to Do not overwrite events
- F. Set the Shutdown system when security audit log becomes full attribute to Enabled

Answer: D, F

Explanation: The problem here is that the security log got overwhelmed, and data got lost. To prevent this loss, the security log should be increased in size, set to not overwrite, and if really critical, stop everything before data gets lost.

With answer D, we prevent the loss of data by preventing entries from being overridden. By answer F, we stop everything before we end up losing stuff. The template did not configure either of these two options, and left us to keep the file around for 7 days, but when the file was full, the recording stopped. This is why we only had a couple of days in the log. Also note, that since we are talking security here, we don't really care about the application logs. The answers about application logs are thrown in to confuse you and see if you know which log has to be configured.

Incorrect Answers:

B, E. We don't really care about the system log, we need to preserve the security log to prevent loss of audit records.

C. We want to restrict guest access. We don't want the guest account poking around the security log and see what is and isn't being audited.

QUESTION 7 You are the administrator of a Windows NT domain that contains Windows NT server computers and Windows NT Workstation computers. You train users on the use of strong passwords, and you configure your domain's account policy to require users to use at least eight characters in their passwords. However, you discover that you can guess the passwords. However, you discover that you can guess the passwords for five of the users.

You want to prevent users from using simple passwords that can be easily guessed.

What should you do?

A. Use Syskey.exe on each domain controller, and click the store Startup key Locally option button.

B. Use Syskey.exe on each domain controller, and click the password Startup option button.

C. Configure all domain controllers to use Passfilt.dll

D. Configure all client computers to use Passfilt.dll

Answer: C

Explanation: The passfilt.dll will enforce strong passwords. Passwords cannot contain the username or part of the username, must contain characters from 3 out of 4 different groups (Uppercase, Lowercase, Numbers, and Special Characters), and must be at least 6 characters in length. The utility is enabled by modification of a registry key, which should be done on the PDC, and any BDC that may be promoted to a PDC.







Incorrect Answers:

A. Syskey is a utility used to encrypt the passwords in the SAM database. It protects passwords, it does not control the generation of the passwords, nor does it enforce policies.

B. Syskey is a utility used to encrypt the passwords in the SAM database. It protects passwords, it does not control the generation of the passwords, nor does it enforce policies.

D. This utility is configured on the Domain Controllers, not the Clients.

QUESTION 8 You are the administrator of a Windows NT domain in one of your company's branch offices. You receive a security template from company headquarters. The template contains password policy settings that represent the company's minimum standards for password policy. You open the template in security Configuration Manager on your PDC, and you analyze your domain's current settings against the template's settings. The results of the analysis are shown in the exhibit.

Attribute	Stored Configuration	Analyzed System Sett..
 Enforce password uniqueness by remembering last	6 Passwords	7 Password
 Maximum Password Age	42 Days	35 Days
 Minimum Password Age	2 Days	1 Days
 Minimum Password Length	8 Characters	7 Characters
 Passwords must meet complexity requirements of installed password filter	Disabled	Enabled
 User must logon to change password	Disabled	Enabled

You do not want to simply apply the template to your PDC, because some of your local standards might be higher than those in the template. You need to increase security on your domain in order to meet the company's minimum standards.

Which two solutions should you take? (Each correct answer presents part of the solution. Choose two)

A. Configure passwords to expire in 42 days

B. Allow passwords to contain at least eight characters

C. Use Passprop.exe from the Windows NT Server Resource Kit to configure your domain to require strong

passwords

D. Do not require users to log on in order to change their passwords

Answer: A, B

Explanation: The stored configuration settings (middle column) is the company's minimum standards, and the analyzed system settings is the current settings in place in the system. The objective is to change the settings WITHOUT applying the actual template, so the weaker security parameters have to be applied by hand. The first, is to change the password maximum age from 42 days to 35 days. The second is to increase the minimum size of the password from 7 to 8 characters. A longer password is harder to crack, so we take the company standard.

Incorrect Answers:

C. The domain is already configured for stronger passwords, this is not needed.

D. It is more secure to force users to logon to change passwords. This would weaken security if we made the change.

QUESTION 9 You are the administrator of a Windows NT domain that contains Windows NT server computers and Windows NT workstation computers. All users have administrative privileges on their Windows NT workstation computers. You install security configuration manager on your client computer, and you use it to customize a template that you want to apply to all of the Windows NT workstation computers in the domain. You want to use the least amount of administrative effort when applying the customized template.

Which three actions should you take? (Each correct answer presents part of the solution. Choose three)

A. Place the customized template in the NETLOGON share folder on the PDC

B. Place Secedit.exe, Esent.dll, and Secedll.dll in the NETLOGON shared folder on the PDC.

C. Install both the GUI version and the command-line version of security configuration manager on each client computer

D. Install only the command-line version of security configuration manager on each client computer.

E. Use security configuration manager on each client computer to apply the customized template

F. Add a statement to each user's logon script that runs Secedit.exe to apply the customized template.

Answer: A, B, F

Explanation: We re going to use a technique where we can use a logon script to perform the update. In order to do this, we put the template and utility into the NETLOGON folder, since this folder will be available during logon. We then add the secedit commands to the logon scripts to apply the template. We run the command line secedit program to this.

Incorrect Answers:

C. We could do this, but this is a lot of work and we would have to visit every workstation. Try this in a company with 5000 workstations, and maybe you will finish before you retire from the company. You want to use the least amount of administrative effort, and this isn't the way. Also, we don't want the users running the SCM (Security Control Manager) and modifying the template (remember that everyone has administrative privilege on their workstation).

D. We could do this, but this is a lot of work and we would have to visit every workstation. Try this in a company with 5000 workstations, and maybe you will finish before you retire from the company. You want to use the least amount of administrative effort, and this isn't the way.

E. We could do this, but this is a lot of work and we would have to visit every workstation. Try this in a company with 5000 workstations, and maybe you will finish before you retire from the company. You want to use the least amount of administrative effort, and this isn't the way.

Note: C, D, E represent manual labor to visit each workstation and get the job done, but it is a lot of work. A, B, F is an automated method, and less work.

QUESTION 10 You are the administrator of a Windows NT domain that contains Windows NT server computers and Windows NT workstation computers. You use Security configuration manager to create and customize a security template named Securews.inf. During the weekend, you apply the new security template to all of the client computers in the domain.

On Monday morning, users report that some of their applications no longer function correctly. You need to restore the client computers to full functionality as quickly as possible.

What should you do?

- A. Uninstall Security Configuration Manager from each client computer in the domain
- B. On each client computer in the domain, delete the securews.inf template, and rename the Compws4.inf template as Securews.inf
- C. Use Secedit.exe to apply the Hisecws4.inf template to each client computer
- D. Use Secedit.exe to apply the Basicwk4.inf template to each client computer

Answer: D

Explanation: The Basicwk4.inf template represents the default configuration of a Windows NT 4.0 workstation, out of the box. By applying this template, we regress back to the original security settings. This assumes that a different template was not applied previously, and that this is the first attempt to lockdown security.

Incorrect Answers:

- A. Security configuration manager (SCM) is a tool used to change the registry. Once the registry is changed, it stays changed until the SCM is run again and a configuration is executed. Deleting the SCM and the templates after the fact does not change the registry back.
- B. Templates are not used, until applied using the Security Control Manager. Once applied, the templates are not used. Renaming the templates, deleting them, adding new ones, all will not affect the running of the system. They must be applied using the configure this computer task.
- C. Hisecws4 is a high security template, which has settings which lock down the workstation. Applying this template might not affect the workstations, or make matters worse.

QUESTION 11 You are the administrator of a network that consists of three Windows NT domains, which are named ROMEHQ, LONDON, and PARIS. The three domains contain Windows NT server computers, Windows NT workstation computers, and Windows 2000 Professional computers. The domains are configured as a

complete trust domain model. You have a Web server farm that consists of 25 member servers in the LONDON domain. You want to allow five designated users from each domain to fully administer any of the web servers.

You do not want these users to be able to administer other servers in any domain.

Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

- A. In each domain, create a local group named WebAdmin, and add the five users to this group.
- B. In each domain, create a global group named WebAdmin, and add the five users to this group.
- C. In each domain, create a universal group named WebAdmin, and add the five users to this group.
- D. Add the WebAdmin group from each domain to the Administrator groups in the LONDON domain.
- E. Add the WebAdmin group from each domain to the Domain Admin groups in the LONDON domain.
- F. Add the WebAdmin group from each domain to the Power Users group on each web server.
- G. Add the WebAdmin group from each domain to the administrators group on each web server.

Answer: B, G

Explanation: Since the web servers might not be in the same domain as the user account (user account crosses domain boundaries) we need to define a global group. For example a user from domain ROMEHQ needs to access the web servers in LONDON. The trust relationships are there, since we have a complete trust model.

Now we need to now decide where to assign these new Global Groups. The question indicates "to fully administer any of the web servers", so we need to add the WebAdmin global group to the administrators group for each web server.

Remember, the Web server farm contains 25 member servers, not domain controllers. So we can set up administration rights and permissions by assigning to each individual member server.

Incorrect Answers:

A. We have to cross domain boundaries, we need to use Global Groups.

C. Hey, this is Windows NT - we don't have Universal Groups!

D. If we do this, then the web administrators can administer anything in the LONDON domain, which is too much power. We only want them to administrator the web servers.

E. If we do this, then the web administrators can administer anything in the LONDON domain, which is too much power. We only want them to administrator the web servers.

F. Power users have limited administrative authority on the member servers. We want full administrative rights on each of those web servers.

QUESTION 12 You are the new network administrator for a small company. The network consists of three Windows NT domains, which are named SALES, MKT, and ACCT. You have no documentation that describes how the domains are configured or what trust relationships exist

A user named Jenny is an employee in the sales department. Jenny is using an available computer in the accounting department today because her computer would not start. Jenny reports that she cannot log on to the network by using her normal user account of SALES\Jenny. Until now, she has always been able to log on to the network by using her account.

You go to the computer that Jenny is using, and you verify that she cannot log on to the network. When you log on by using the user account ACCT\administrator, you can log on successfully. You examine Jenny's account and decide that she should be able to log on to the network. You want to allow jenny to log on to the network by using this computer. You also want to ensure that users are able to log on to the network by using any client computer in the company.

What should you do?

A. Configure a complete trust domain model.

B. Configure the MKT and ACCT domains to trust the SALES domain.

C. Create an account for Jenny in the ACCT domain.

D. Create a computer account for Jenny's computer in the SALES domain.

Answer: A

Explanation: We don't know where the accounts are, and if they are spread across all three domains, then each domain needs to trust the other two domains because the user account could be in any of the three. These leads to a complete trust model.

Incorrect Answers:

B. This is not a full solution. For example, suppose the user account is in MKT, and the user tries to use a computer in ACCT, we need ACCT to trust MKT. The proposed solution does not provide that trust relationship.

C. This does solve anything. First, the duplicate account that was just created does not have the same access and permissions as the original account in the SALES domain. The SID will be different, and it will appear that Jenny account is different person. Second, this does no solve the required solution that any user can use any machine to logon.

D. The problem is not with the computer account, and we still did not solve the required solution that any user can use any machine to logon.

QUESTION 13 You are the administrator of a Windows NT server network that contains Windows 2000 Professional computers. You are creating a system policy for the network. The network currently has no system policies. Your company has a new company logo, and the executives want you to configure all of the client computers to use the new logo as the desktop wallpaper. You create a system policy file that contains a group policy for the Everyone group. The group policy is configured to use the new logo as the desktop wallpaper. You need to ensure that the Windows 2000 Professional computers will use the new group policy.

What should you do?

- A. Place the system policy file in the NETLOGON shared folder on the PDC
- B. Place the system policy file in the home directory of each Windows 2000 Professional user account
- C. Place the system policy file in a shared folder on a server. Modify the registry on each Windows 2000 Professional computer to configure the system policy's Network Path value
- D. Place the system policy file in the C:\Documents and Settings\Default User folder on each Windows 2000 Professional computer. Modify the registry on each Windows 2000 Professional computer to configure the system policy's Network Path value

Answer: A

Explanation: Even on Windows 2000, the system policy is added to the NETLOGON folder. By adding the policy to the NETLOGON folder, the Windows 2000 workstations will pick it up. Since the Windows 2000 workstations can authenticate via a BDC, these policy files should be replicated to the NETLOGON folder of all domain controllers within the domain.

Incorrect Answers:

- B. System policy is taken off the domain controller and applied to the clients. It is not taken from the workstation.
- C. This is not an approved or standard method of applying system policy, and would require too much system administration.
- D. This is not an approved or standard method of applying system policy, and would require too much system administration. There would also be a possibility of subverting the policy, and since it would be user based, would have required additional administration each time a user was added. Also, even if this was doable, a policy added AFTER the user was created would never be picked up. The Default User is only used as a template when a new user is added to the system. Policies would never be updated.

QUESTION 14 You are the user account administrator for a Windows NT domain. Ninety percent of your users work in a call center that runs three eight-hour shifts, seven days a week. The employee turnover rate is high. You are constantly creating user accounts for new employees. All users in the call center have the same group memberships and profile settings. You want to simplify the process of creating new user accounts.

Which two courses of action should you take? (Each correct answer presents part of the solution. Choose two)

- A. Create a new user account named Template, and configure it with the appropriate group memberships and profile settings. Configure the Template account as a global account.
- B. Create a new user account named Template, and configure it with the appropriate group memberships and profile settings. Configure the Template account as a local account.
- C. In user manager for Domains, select the Template account, and then create a new local group named Template.
- D. In user manager for domains, select the Template account, and then on the User menu click New User Name the new account as desired.
- E. In user manager for domains, select the Template account, and then on the User menu click copy. Name the new account as desired.

Answer: A, E

Explanation: The objective is to reduce the repetition of configuring parameters, home directories, and other items for the user. Then you copy the template, and only enter the user details, which is userid, name, and password. Since this is a Domain user, we want a Domain account, which is global. Do not confuse a Global Account with a Global Group.

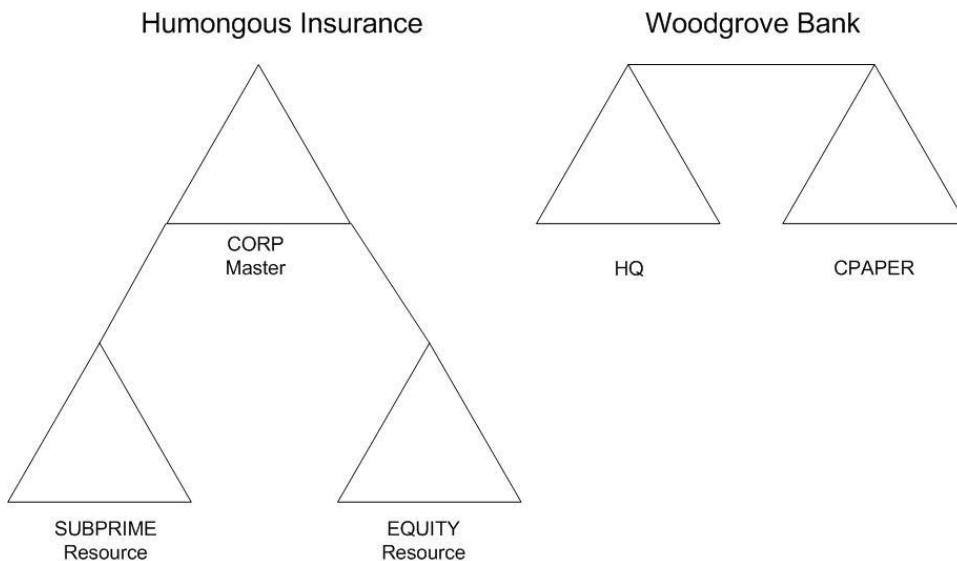
Incorrect Answers:

B. You do not want a account local to the server where the template is generated. Remember, user manager for domains can run on any machine, and does not need to be performed on a domain controller.

C. There are no default templates distributed with Windows NT. You must create a template from scratch first.

D. This operation would create a new user from scratch without the pre-configuration in the template. It would be as if the template never existed in the first place.

QUESTION 15 You are the network administrator for Humongous Insurance, which is acquiring a company name WoodGrove Bank. The Humongous Insurance network consists of three Windows NT domains. The WoodGrove Bank network consists of two Windows NT domains. The two networks are shown in the exhibit. Click the exhibit button.



The Humongous Insurance domains are configured as a single master domain model, and the WoodGrove bank domains are configured as a complete trust domain model. All shared network resources on the Humongous Insurance network are in the resource domains, and user accounts are in the master domain. You install network connections between Humongous Insurance and WoodGrove bank. All network administration will be performed from the CORP domain. You want users in both companies to be able to connect to shared resources in the resource domains. Before you assign specific permissions for resources, you need to configure the trust relationships between the two networks. You want to accomplish this task by using the smallest number of trust relationships required.

Which three actions should you take? (Each correct answer presents part of the solution. Choose three)

- A. Configure one-way trust relationships so that the SUBPRIME domain trusts the HQ and CPAPER domains.
- B. Configure one-way trust relationships so that the EQUITY domain trusts the HQ and CPAPER domains.
- C. Configure two-way trust relationships between the CORP domain and the HQ and CPAPER domains.
- D. Configure one-way trust relationships so that the CORP domain trusts the HQ and CPAPER domains.
- E. Configure one-way trust relationships so that the HQ and CPAPER domains trust the CORP domain.

- F. Configure two-way trust relationships between the SUBPRIME domain and the HQ and CPAPER domains.
- G. Configure two-way trust relationships between the RQUITY domain and the HQ and CPAPER domains.

Answer: A, B, E

Explanation: Resource domains must trust Account domains, in order for accounts in the trusted domain to be accepted in the trusting domains. Accounts are in CORP, HQ and CPAPER. SUBPRIME and EQUITY already trust CORP.

They need to trust HQ and CPAPER. (This is covered in A & B). Since the Administrators in CORP will manage HQ and CPAPER, we need HQ and CPAPER to trust CORP. (This is covered in E).

Incorrect Answers:

C, F, G. Windows NT does not have two way trusts, and if it did, it poses unnecessary additional trusts which is not needed.

D. CORP does not have resources, therefore, this trust is not required.

QUESTION 16 You are the administrator of a Windows NT domain. You recently configured the domain so that users are required to change their passwords every 42 days. Now, some of the users report that when they log on, they receive the following message "Your password will expire in 14 days. Do you want to change it now?" when these users attempt to change their passwords, they receive the following error message: "The password on this account cannot be changed at this time."

You want to enable users to change their passwords when prompted.

How should you configure the Account policy for your domain?

- A. Allow passwords to be changed after a minimum of 27 days
- B. Configure passwords to expire in 15 days
- C. Do not require users to log on in order to change their passwords
- D. Do not require that password history be kept

Answer: A

Explanation: Let's do some math. If the passwords have to expire in 42 days, and the users are told they have 14 days left, then the passwords are 27 days old. The fact that we can't change them, indicates that the minimum is greater than 27 days. We need to drop the minimum down so that the passwords can be changed.

Incorrect Answers:

B. This makes it impossible to change the passwords. The passwords would immediately expire on every machine, since it is obvious that the passwords are at least 27 days old. If the minimum password age was not reached yet, then you have a situation where the password has to be changed but it isn't old enough to allow the change. This is a serious conflict.

C. Even if the user has permission to change the password without logging on, this problem will not change.

D. The problem is not related to the password history. The password history is only used to enforce complex passwords. It does not affect the expiration time of the password itself.

QUESTION 17 You are the administrator of a network that consists of two Windows NT domains, which are named CHICAGO and BOSTON. The domains are configured as a complete trust domain model. Both domains contain Windows NT server computers and Windows NT workstation computers.

Five members of the help desk staff have user accounts in the CHICAGO domain. These five users need to be able to reset passwords for users in both domains. You want to assign these five users the minimum permissions that will allow them to reset passwords.

Which two courses of action should you take? (Each correct answer presents part of the solution. Choose two)

- A. Create a global group named ResetPW in the CHICAGO domain. Add the appropriate help desk user accounts to this group.

- B. Create a local group named ResetPW in the CHICAGO domain. Add the appropriate help desk user account to this group.
- C. Add the ResetPW group to the Administrator group in both domains.
- D. Add the ResetPW group to the Account Operators local group in both domains.
- E. Add the ResetPW group to the Administrators group on all client computers.
- F. Add the ResetPW group to the local power users group on all client computers.

Answer: A, D

Explanation: Add users to GLOBAL groups, not LOCAL groups. The minimum security level required is Account Operator.

Incorrect Answers:

- B. Do not add users to local groups. Local groups are not used to cross domains.
- C. This gives too much rights. We want minimum permissions and rights.
- E. This does not accomplish anything. In order to reset domain passwords, you would need to be a domain level account operator or administrator, not a client level.
- F. This does not accomplish anything. In order to reset domain passwords, you would need to be a domain level account operator or administrator, not a client level.

QUESTION 18 You are the administrator of a network that consists of two Windows NT domains, which are named VHHICAGO and DENVER. The domains are configured as a complete trust domain model. Each domain contains Windows NT server computers and Windows NT workstation computers. You hire a new assistant administrator named Marie. She will be responsible for creating, configuring, and managing all printers on all servers in both domains. Marie has a user account in the DENVER domain. You want to assign Marie the fewest permissions possible.

What should you do?

- A. Add Marie's user account to the server operators group in each domain, and add Marie's user account to the Administrators group on each member server
- B. Add Marie's user account to the server operators group in each domain, and add Marie's user account to the power Users group on each member server
- C. Add Marie's user account to the server operators group in each domain, and add Marie's user account to the Users group on each member server
- D. Add Marie's user account to the Print operators group in each domain, and add Marie's user account to the Users group on each member server
- E. Add Marie's user account to the Print operators group in each domain, and add Marie's user account to the Power Users group on each member server
- F. Add Marie's user account to the Print operators group in each domain, and add Marie's user account to the Administrators group on each member server

Answer: E

Explanation: In order to just manage the print servers and print operations, Marie just needs to be added to the Print Operators group, which allows her to manage printers on Domain Controllers. In order to manage the printers on the member servers, being a Power User will give sufficient rights to manage the printers there.

Incorrect Answers:

- A. This option gives Marie too much rights everywhere..
- B. This option gives Marie too much rights in the domain.
- C. This option gives Marie too much rights in the domain, and not enough rights on the member servers.
- D. This option is correct for the domain, but not enough rights on the member servers.
- F. This option is correct for the domain, but too much rights for the member servers.

QUESTION 19 You are the administrator of a network that consists of four Windows NT domains. The domains are configured as a complete trust domain model. Each domain contains at least 10 servers. Server backups are currently performed by the administrator of each server. You want to allow any user account from any domain to back up any domain controller or member server in any domain. You want to assign the minimum rights necessary for accomplishing the backups.

Which three courses of action should you take? (Each correct answer presents part of the solution. Choose three)

- A. In each domain, create a local group named Backup. Add to this group the user accounts in that domain that will perform backups
- B. In each domain, create a global group named Backup. Add to this group the user accounts in that domain that will perform backups
- C. In each domain, create a Universal group named Backup. Add to this group the user accounts in that domain that will perform backups
- D. Add the backup group from each domain to the Backup Operators group in every domain.
- E. Add the backup group from each domain to the Backup Operators group in each member server in each domain.
- F. Add the backup group from each domain to the Domain Admins group in every domain.

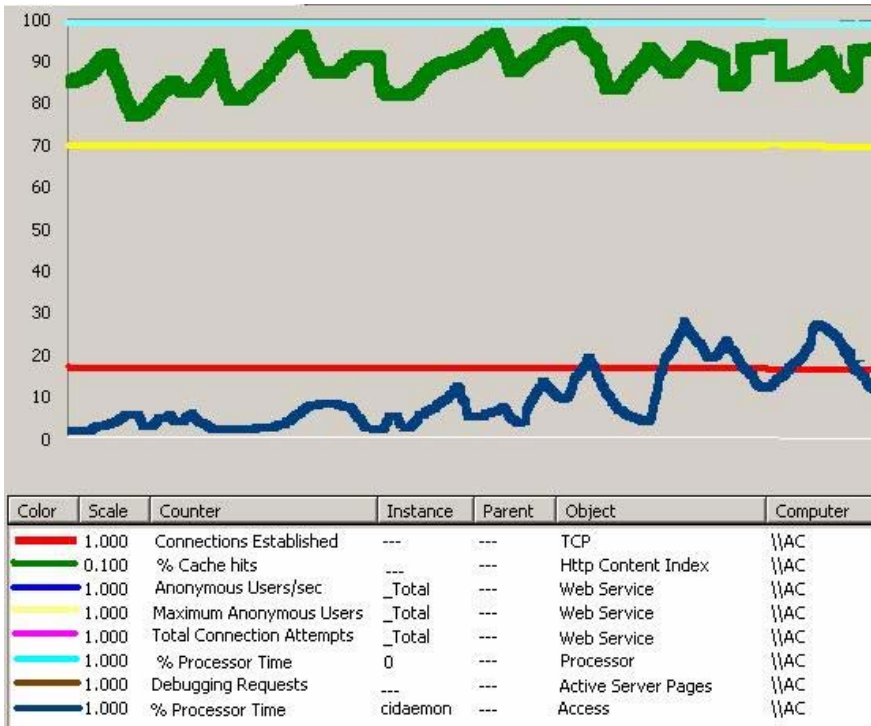
Answer: B, D, E

Explanation: Users are added to Global Groups in each domain. Global groups can cross domain boundaries, and this is the recommended sequence, user to global groups. We then add this global group to the domain Backup Operators, which gives the ability to backup and restore data on Domain Controllers. This does NOT allow access to the member servers, so we add the global group to each and every member server.

Incorrect Answers:

- A. Local groups are not used to traverse domain boundaries. Adding users to the local group is not the proper design, even when all the resources are in the SAME domain.
- C. This is Windows NT, not Windows 2000. We don't have Universal groups yet.
- F. This would provide too much permission and rights. The question says minimum rights.

QUESTION 20 You are the administrator of a Windows NT server computer that hosts your company's Internet web site. Your site receives approximately 100,000 hits per day. Site visitors report that they occasionally receive connection error messages when they attempt to connect to the web site. You notice that the web site responds very slowly every two or three hours. During one of the slowdowns, you run performance Monitor and receive the results shown in the exhibit.



You want to eliminate the slowdowns and enable users to connect to the web site without receiving connection error messages.

What should you do?

- A. Configure Microsoft index server to run index catalog builds during off-peak hours.
- B. Reconfigure the web site as a virtual directory under the default Microsoft Internet Information Server web site.
- C. Configure the web site to run with performance settings for more than 100,000 hits per day.
- D. Configure the web site to run at an Application Protection level of high.

Answer: A, C

Explanation: If we look at the bottom of the page, we see the process cidaemon running and absorbing a lot of CPU resources. This utility is used to build the index in index server, and is a very resource consumption hog. This is a utility that should be run off hours and not during the day, and the schedule should be changed. We are seeing this at the bottom entry. We also see that over the 1000,000 seconds time period (Graph Time, assuming the default of one second interval) that we need to set the performance settings for the web site at over 100,000 per day.

Incorrect Answers:

- B. The location of the website on the disk should not make a difference. We are not monitoring disk activity, so we don't even know if we have a disk problem.
- D. We don't see any indication that the application protection level is impacting performance. If it was, we can't tell from the variables being used.

QUESTION 21 You are the Webmaster of your company's internet web site. The web site is hosted by a Windows NT server computer. You create an FTP site to allow users to upload and download documents. You want to assign user names and passwords to each user who is authorized to access the site. You also want to hide the FTP site from users who might be randomly trying to access FTP sites on various servers.

Which three actions should you take? (Each correct answer presents part of the solution. Choose three)

- A. configure the FTP site to use port 21

- B. configure the FTP site to use port 26
- C. configure the FTP site to disallow anonymous access
- D. configure the FTP site to allow anonymous access
- E. configure the FTP site to assign the Read and Write permissions for the IUSR_FTP account
- F. configure the FTP site to assign the Read and write permissions for each FTP user account.

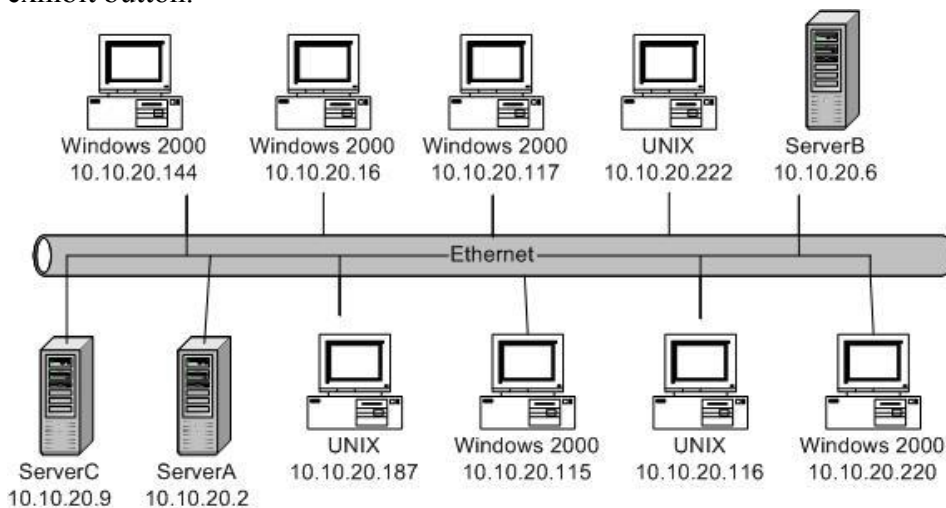
Answer: B, C, F

Explanation: Port 26 is unused, and by setting the FTP port to 26, it is assigned to a port not assigned to FTP. A hacker would have to scan all the ports or find this port by accident. To assign usernames and passwords to each account, you probably no longer want anonymous access, so this should be disabled. Finally, you configure permissions for each account. The way FTP works under IIS 4 (and IIS 5) is that if a user signs in under a username, their home directory is automatically set to a directory that is the same as the username.

Incorrect Answers:

- A. Port 21 is the standard assigned port for FTP. You want to hide it, and using Port 21 leaves the port out in the open.
- D. With the requirement to have usernames and passwords, you want to lock down the FTP site. This usually includes disabling anonymous access, otherwise anyone can bypass the account security.
- E. The IUSR_FTP is the anonymous user account, this is not the account you want to use. Actually, you want to disable anonymous access.

QUESTION 22 You are the administrator of a Windows NT server network. Three of the Windows NT server computers on the network are named ServerA, ServerB, and ServerC. The network also contains Windows 2000 Professional client computers and UNIX servers. A portion of the network is shown in the exhibit. Click the exhibit button.



ServerA is a DHCP server that is configured to use a DHCP scope of 10.10.20.10 to 10.10.20.255. All of the UNIX servers are configured to use static IP addresses, and the Windows 2000 Professional computers are configured to use DHCP.

Every day, users report that they cannot connect to the network when they first start their computers. The users usually receive the following error message:

The system has detected an IP address conflict with another system on the network. The local interface has been disabled. More details are available in the system event log. Consult your network administrator to resolve the conflict.

Each user can connect to the network after waiting about 30 minutes and restarting the computer. You want to enable users to connect to the network and log on successfully without having to wait and restart their

computers.

What should you do?

- A. Change the DHCP scope on ServerA to 10.10.20.50 to 10.10.20.255.
- B. Change the DHCP scope on ServerA to exclude the addresses of the UNIX servers.
- C. Configure the WINS server address on all of the Windows 2000 Professional computers to 10.10.20.80.
- D. Configure the DNS server address on all of the Windows 2000 Professional computers to 10.10.20.80.

Answer: B

Explanation: The UNIX servers have IP addresses that overlap the scope range. For example one UNIX machine uses 10.10.20.187 which falls in the scope. What we need to do is make reservations for the UNIX machines, or customize the scope to exclude those addresses. One other thing that is broken in this question, and not addressed (could be a typo) is that a broadcast address (10.10.20.255) should never be in a scope!

Incorrect Answers:

- A. Changing the scope in this way does not correct the overlap.
- C, D. The configuration of a WINS or DNS server address does not affect the assigned IP address. When this error occurs, two machines have the same IP address, and is caused by DHCP giving out an address that is in use. DNS and WINS don't assign addresses, and changing the clients' pointer to them does not affect the situation.

QUESTION 23 You are the administrator of a Windows NT server computer named ServerA. ServerA is routing and remote access server for your network. ServerA is connected to the Internet and is configured to provide virtual private network connections to your intranet. You want to prevent unauthorized users from gaining access to your network by using VPN connections on serverA. You want to ensure that only VPN connections are used on serverA.

What should you do?

- A. Configure the VPN connection on computers that connect to serverA to require data encryption.
- B. Configure the VPN connection on computers that connect to serverA to use the Extensible Authentication Protocol.
- C. Configure Routing and Remote access service on ServerA to disable IP forwarding.
- D. Configure TCP/IP on serverA to enable PPTP filtering for the network adapter that is connected to the Internet.

Answer: D

Explanation: By filtering the PPTP protocol (Point To Point Tunneling protocol) on the Internet connection, (PPTP is the protocol for VPN in Windows NT), if you block the protocol, then you can't set up a VPN to or from the Internet. Since there are no default filters in effect (all is open), the network adapter to the Intranet will allow VPNs, so VPNs will work on the Intranet.

Incorrect Answers:

- A. Data encryption will protect the data on a session, but it does not prevent unauthorized users from creating a VPN.
- B. This authorization will control connections on the Intranet, since it is the Intranet client computers being modified. This still does not prevent outside users from attempting to establish a VPN.
- C. This can interfere with the operation of the server, which is running as a router. Even without IP forwarding, an unauthorized user can still establish a VPN to the server and hack it.

QUESTION 24 You are the administrator of a Windows NT server network that contains Windows 2000 Professional computers. The network is divided into five TCP/IP subnets, and each subnet has its own Windows NT server computer. You add a Windows NT server computer named ServerA to one of the subnets, and you

configure the DHCP server service on ServerA. You create a DHCP scope for each of the subnets. You configure all of the client computers to use DHCP. When the client computers start, only computers on the same subnet as ServerA can obtain DHCP addresses. You want to allow all of the client computers to obtain their TCP/IP configurations from ServerA. You want to accomplish this task by using least amount of administrative effort.

What should you do?

- A. Configure the DHCP server service on each Windows NT server computer, and assign an IP scope for each subnet
- B. Configure the DHCP server service on serverA to exclude the IP addresses of the routers from the subnet scopes you have defined
- C. Configure the DHCP relay agent on each Windows NT server computer
- D. Configure a WINS service on each Windows NT server computer

Answer: C

Explanation: This is a classic question, which appears in many forms on many different exams. Unless it is stated that the router between the subnets is capable of supporting the passing of BootP traffic, DHCP packets will not traverse the router. This is because the DHCP packets are broadcasts packets, and routers do not pass broadcasts. The question says: using the least amount of administrative effort. What is needed is to configure a DHCP relay network on all subnets where the DHCP server does not exist.

Incorrect Answers:

A. This will actually work, but the question says: "using the least amount of administrative effort", and setting up a relay agent is less effort than setting up a new DHCP server.

B. This needs to be done, but this is not the problem. Without the relay agent, you can't assign any addresses. If you did accidentally assign a router IP address to a workstation, the workstation would detect a duplicate IP address, and not use it. If the router IP addresses are not excluded or reserved in the scope, then there will be trouble later on. But the problem, as described in the question, is that the DHCP records are not passing the router, and the relay agent will fix the problem.

D. WINS is not the answer. WINS does name resolution. If you do not have a DHCP assigned IP address (when the DHCP client is activated on each workstation), then it would even be unlikely that you could even reach the WINS server. This problem is not related to WINS.

QUESTION 25 You are the administrator of your company's Internet web server. The web server is a Windows NT server computer that hosts five public web sites. One of these five sites is your company's public web site. You want to allow employees to download company documents from the web server when the employees are away from the office. You want to protect the security of each employee's user name and password when employees are accessing the documents. You also want to ensure that only employees can access the documents.

What should you do?

- A. Create an FTP site, and configure it to allow only Windows NT server connections
- B. Create an FTP site, and configure it to allow only anonymous user connections.
- C. Create a new web site, configure it to use Windows NT Challenge/Response authentication, and enable directory browsing
- D. Configure your company's web site to use Windows NT Challenge/Response authentication, and enable directory browsing.

Answer: C

Explanation: This question leaves C & D as a toss-up. The FTP options that are provided won't work. That leaves using HTTP. So, use the current Web Site, or create a new site? Suppose you use the same site. Enabling

directory browsing can only be done on a directory by directory basis. If all the documents were in the same directory, then a virtual directory could be used, and security placed on that directory. Documents spread through the site would be harder to control. Creation of an entire new website can be easier to control, with less opportunities of security exposures caused by a bad configuration. Using a different web site is not required, and more work, but is safer, security wise, and this is why C is chosen.

Incorrect Answers:

- A. FTP only supports usernames and passwords, which are transmitted in the clear. There is no way to determine or control which clients actually connect.
- B. In order to use usernames and passwords to control access, you would require non-anonymous access, and to make the server secure would want to disable the anonymous connections.
- D. This may work, but may not be as secure.

QUESTION 26 You are the Webmaster for an Internet hosting company. The company uses Windows NT server computers and Microsoft Internet Information Server to host multiple web sites in each server. Microsoft index server is also used to provide indexing and searching services. Each server hosts approximately 20 individual web sites. The hosted web sites are performed in a web site to return for only that web site. What should you do?

- A. Re-create hosted web sites by using virtual directories
- B. Re-create hosted web sites by placing them under the default web site
- C. Create an index server catalog for each hosted web site, and assign a catalog to each hosted web site by using the web site's IP address
- D. Create a single index server catalog for the default web sites, and add the name of each hosted web site to the server's Noise.enu file

Answer: C

Explanation: We want to configure the Index server so that users are able to search individual web sites. In order to accomplish this we must create an index server catalog for every Web site.

Note: Microsoft Index Server is integrated with Microsoft Internet Information Server (IIS) and the Windows NT Server 4.0 operating system to allow Web searching on corporate intranets and Internet sites.

Incorrect Answers:

- A, B: We must configure the Index Server, not the IIS server.
- D: If we create just a single index server catalog we would only be able to search all the web sites, not the individual web sites.

QUESTION 27 You are the administrator of a network that consists of a single Windows NT domain. The domain contains Windows NT server computers and Windows 2000 Professional computers. A Windows NT server computer named ServerA provides DHCP, WINS, and DNS services. The DNS service is used to provide name resolution for access to the company's intranet web site.

The domain also contains UNIX client computers that use UNIX-based DNS service. The UNIX DNS server is configured to forward unresolved named resolution requests to ServerA's DNS service.

You want to enable the UNIX computers to access new Windows NT server computers when they are added to the network. You want the UNIX computers to be able to connect to the Windows NT server computers by using host names rather than IP addresses. You want to accomplish this task by using the least amount of ongoing administrative effort.

What should you do?

- A. Configure the WINS service to have static mappings for each UNIX client computer.

- B. Configure ServerA's DNS service to use WINS name resolution.
- C. Configure ServerA's WINS service to use the UNIX DNS server as a push partner.
- D. Configure a HOSTS file on ServerA that contains an entry for each Windows NT server computer.

Answer: B

Explanation: Assuming that all the Windows NT Servers are configured to be WINS clients, each server will be registered with WINS. By having the DNS server on ServerA ask the WINS server for the addresses, we get the current address of the new servers. The Unix servers will use DNS and contact ServerA's DNS server. If the new Windows NT servers are not registered in DNS, they will be in WINS, and the name to IP address will get resolved.

Incorrect Answers:

- A. First, this is a very intensive as the number of workstations increase. Second, we didn't accomplish the task. We can access the UNIX client by name, but this does not provide the ability of the Unix clients on discovering the new Windows NT servers. The Windows NT servers need to be resolved through DNS, and this is accomplished under this solution.
- C. WINS and DNS are not partners. The databases are completely different, and are not interchanged. It doesn't matter if it is a Windows NT DNS or a UNIX DNS, this is not a feature.
- D. For a host file to be usable for this solution, we would need to put the HOSTS file on every UNIX client, not ServerA. Even with proper placement of the file, this is still prohibitive, because we would need to update the HOSTS file on every UNIX client each time we add a new server. This is why DNS was invented in the first place.

QUESTION 28 You are the administrator of a Windows NT domain. The domain contains Windows NT server computers and Windows 2000 Professional computers. The domain uses DNS and WINS for name resolution. ServerA is a Windows NT server computer that provides a DNS service. The DNS service is used to provide name resolution for access to the company's intranet web sites and Internet web sites.

You want to provide fault tolerance for the DNS service on ServerA.

What should you do?

- A. Configure another server as a caching-only DNS server
- B. Configure another server as a secondary DNS server
- C. Configure ServerA's DNS service to use a WINS server as a push partner
- D. Configure ServerA's DNS service to use WINS name resolution

Answer: B

Explanation: For fault tolerance, you install a secondary DNS server, and point the clients to both the primary and secondary.

If the primary goes down, the requests will time out and the secondary will be contacted. The secondary holds a copy of the zone database, and can do searches to look up information.

Incorrect Answers:

- A. A caching-only server does not have its own copy of the zone. It builds a dynamic copy of the database by making requests and saving the results. A reboot of the caching-only server will lose the cached information. If the primary goes down, and it does not have the necessary information because it hasn't been cached yet, then the server will fail to resolve the name. This is not fault tolerant.
 - C. DNS and WINS do not share databases, and can't be partners.
 - D. If the only DNS server in the network is down, there will be no response to DNS calls. A client will not ask a WINS server for information if the DNS server is down. The WINS server is not a partner to DNS for fault tolerance.
-

QUESTION 29 You are the administrator of a network that consists of a single Windows NT domain. The domain contains Windows NT server computers, UNIX servers, and Windows 2000 Professional client computers. The client computers are configured to use DHCP and WINS. You are adding a new UNIX server named Server1 to the network. You want users to be able to connect to Server1 by using its name rather than its IP address.

What should you do?

- A. Create an internet Group WINS record that points to the IP address of server1
- B. Create a Unique WINS record that points to the IP address of Server1
- C. Configure the Network DHCP scope to include the IP address of Server1 in its range.
- D. Configure the network DHCP scope to use server1 as a DNS server

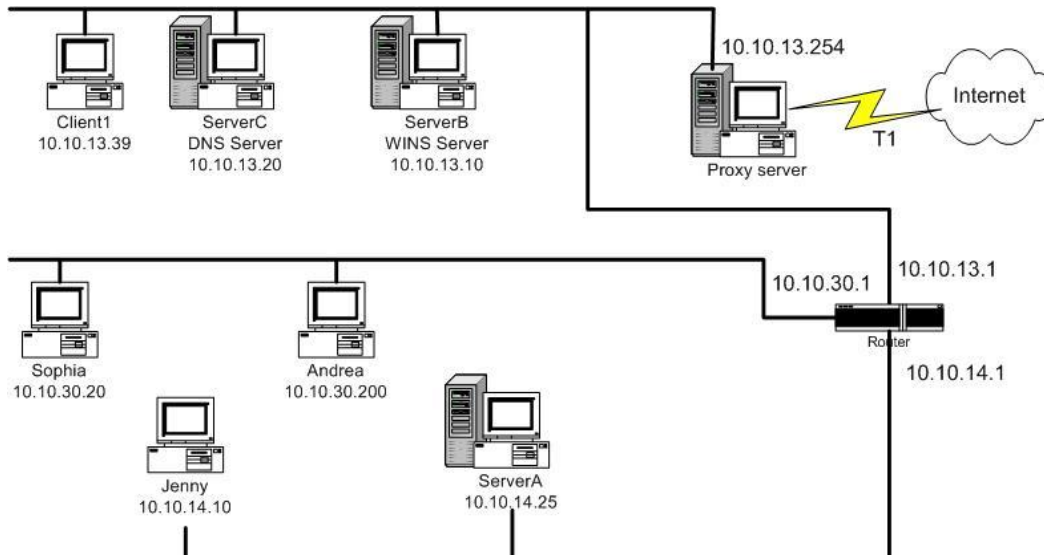
Answer: B

Explanation: The client computers are already using WINS for name resolution. Since WINS is used for NETBIOS name resolution, the Unix server is probably going to be running a SMB client, such as SAMBA. We want a unique, static, entry.

Incorrect Answers:

- A. A unique entry is required.
- C. Adding the IP address of the Unix server to the scope range of IP addresses should not be done, unless the Unix server is a DHCP client. This is not a recommended configuration (having a server as a DHCP client). Doing this, even properly, still does not provide the ability to access the Unix server by name.
- D. The question did not say that Server1 was a DNS server. We would have to make Server1 a DNS server, configuring and activating the service. If NETBIOS functions were required, then the WINS entry would still be required.

QUESTION 30 You are the administrator of a Windows NT domain. The domain contains Windows NT server computers and Windows 2000 Professional computers. You are responsible for supporting all of the computers in the domain. Another group in your company manages the network routers. A portion of your network is shown in the exhibit.



A user named Marc is using the computer named client1. Marc reports that he cannot access a resource on ServerA. You verify that you can connect to ServerA from the computer named Sophia.

You want to find out whether client1 can connect to serverA.

What should you do?

- A. On Client1, run the Ping command to test the address of 10.10.10.1
- B. On Client1, run the tracert command to test the address of 10.10.14.25
- C. On ServerA, run the ping command to test the address of 10.10.14.1
- D. On ServerA, run the tracert command to test the address of 10.10.13.1

Answer: B

Explanation: A tracert command will attempt to access the device, and report along the way each hop. There is only one hop here, since there is only one router in the path. The tracert will provide information whether the packets can reach the router, go through the router, and eventually reach the server. Tracert is a diagnostic tool used for network troubleshooting. The IP address, 10.10.14.25 is the address of ServerA, so we are trying to check connectivity FROM Client1 to ServerA. We also want to note that Sophia is also on a different subnet than ServerA. By being able to access ServerA from Sophia, we know that ServerA is operational (otherwise the server could have crashed and be down). We know that there is some activity in the router, since Sophia has to go through the router to reach ServerA. However, since Sophia is on a different subnet than Client1, there could still be a router problem, as the routing table could be bad.

Incorrect Answers:

- A. The IP address of 10.10.10.1 isn't even on the network. Pinging that address doesn't accomplish anything.
- C, D. Being able to reach from ServerA to Client1 doesn't prove anything. For example, incorrect routing tables in the router could cause a problem. These tables could be correct in one direction and bad for the other direction. We know that ServerA can communicate with the router, because Sophia can contact ServerA. This rules out ServerA having a bad default gateway specification.

QUESTION 31 You are the administrator of a network that contains Windows NT server computers and NetWare 3.x servers. A Windows NT server computer named ServerA is the Routing and Remote Access Server for your network.

ServerA has a 12-port analog 56-Kbps modem card installed. Routing and Remote Access Service is configured to use the modem card for incoming analog connections. Users connect to serverA by using portable computers that have PC card modems.

A user named Marc was recently assigned dial-in permissions to serverA. Marc reports that every time his computer dials into serverA, he receives confirmation that his user name and password were verified, and then ServerA disconnects.

You want to enable Marc to dial in successfully.

What should you do?

- A. Configure serverA to use DHCP leases for dial-in users, and configure the DHCP scope to use the local default gateway
- B. Configure serverA to use TCP/IP, NetBEUI, and NWLink IPX/SPX Compatible Transport for the dial-in ports
- C. Configure Marc's account so that it has no restrictions for logon hours.
- D. Configure Marc's account to disable callback

Answer: D

Explanation: The most likely problem is that callback is enabled, and RRAS is probably calling back the wrong number.

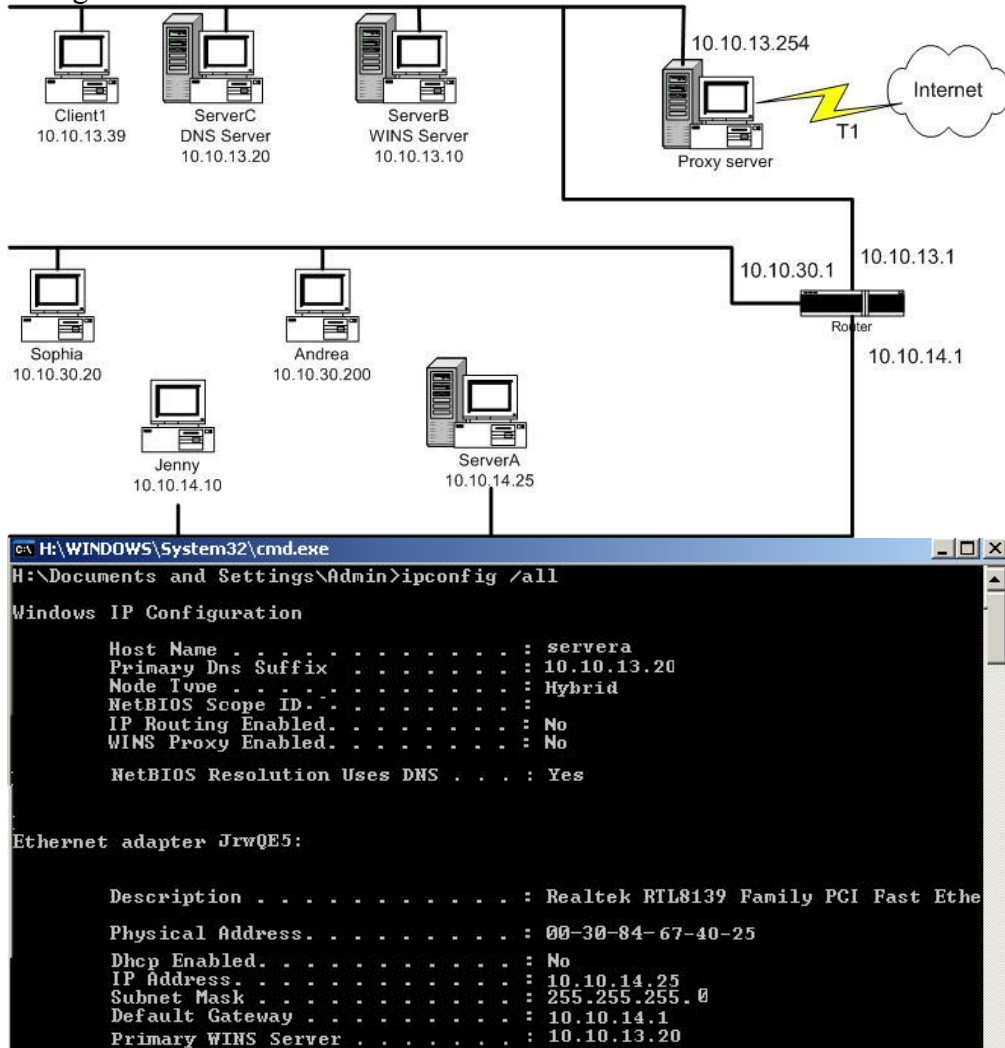
Everything connects OK, then a disconnect, would indicate that the RRAS server disconnects and is getting ready to call back.

Incorrect Answers:

- A. This does not have to be an IP issue. Since there are Netware 3.x servers, which only function using IPX, an IP address may not be needed, and the lack of one being assigned should not drop the connection.

- B. If the required protocols were missing, then there would be a message that the server did not have those protocols enabled for RRAS.
- C. If there were a restriction, Marc would have gotten a message indicating so.

QUESTION 32 You are the administrator of a Windows NT server network. You are adding a new Windows NT server computer named serverA to the network. A portion of the network is shown in the Network configuration exhibit. Click the exhibit button.



You install and begin to test ServerA. You logon to Cleint1 and connect to a shared folder on serverA. You then log on locally to serverA and attempt to connect to a shared folder on serverB by using the path \\serverB\share1. You receive the following error message: "the network path \\ServerB\Share1 could not be found."

You run the ipconfig command on serverA and receive the results shown in the IP configuration exhibit. Click the exhibit button

You need to ensure that serverA can connect to ServerB. What should you do?

- A. Force serverB to replicate ServerA's [1Ch] record to all other WINS servers
- B. Configure serverB to use serverA as a pull partner
- C. Configure serverA to use 10.10.13.10 as its primary and secondary WINS address

D. Configure serverA to use 10.10.13.254 as the default gateway

Answer: C

Explanation: As we can see from the output of the ipconfig command, the server is configured to point to the WINS server on 10.10.13.20, but if you look at the diagram, the WINS server is at 10.10.13.10, and it is the DNS server that I at 10.10.13.20.

Incorrect Answers:

A, B. The problem here is not that we need to configure or force replication. At this point, until serverA points to a valid WINS server, any customization of the replication services is premature.

B. Partnerships between WINS servers (where databases are exchanged and updated) only occurs between WINS servers, and there is not indication that serverA is a WINS server.

D. The default gateway configuration was correct. Changing to this value is definitely wrong, since the default gateway MUST be on the same subnet as the node, in this case serverA which requires a 10.10.14 network (we are class C subnet mask).

QUESTION 33 You are the administrator of a Windows NT server network. Your company plans to deploy Windows 2000 Professional to 1,000 client computers during the evening. The installations will be performed from shared folders. You have four Windows NT servers available for this purpose. The servers are named Files1, Files2, Files3, and Files4. You want to ensure that the installation files are available on several file servers, and you want the client computers to provide automatic load balancing across the available file servers. What should you do?

A. Install Remote Installation Services on all four file servers.

B. Configure the Directory Replicator Service on all four file servers to replicate the installation files to each server.

C. Install distributed file system on Files4, and then configure a Dfs root. Create three replicas on files4 that each point to one of the remaining file servers.

D. Ensure that your DNS server contains an A record for each file server, and then enable DNS round robin.

Answer: D

Explanation: By using round robin on the DNS server, requests are sent to the each of the four file servers in rotating order.

This provides the automatic load balancing.

Incorrect Answers:

A. RIS is a Windows 2000 function, requiring Windows 2000 Server, an Active Directory. We are running Windows NT, which does not support RIS.

B. This might distribute the files, but does not provide load balancing.

C. Windows NT does not have DFS replicas that are load balancing.

QUESTION 34 You are the administrator of a Windows NT server computer named FS1. FS1 contains two hard disks, which are named drive C and drive D. Drive C has a 2-GB capacity and is formatted with the FAT file system. Drive D has a 4-GB capacity and is formatted with the NTFS file system. You place several documents in C:\Docs. You plan to access these documents from the server console, but you want to ensure that the documents are available on the network to all members of the Domain Users group. You do not want these users to modify any files.

What should you do?

A. Share C:\Docs as docs1.

Ensure that the Protected Storage Service is set to start automatically.

Log on by using the Local system account.

B. Share C:\Docs as docs1. Create a Microsoft Internet Information Server virtual directory that points to \\FS1\Docs1.

Configure the virtual directory as read-only

C. Share C:\Docs as Docs1. Configure the files in C:\Docs as read-only

D. Share C:\Docs as Docs1. Remove the Everyone group from the permissions on Docs1. Assign the domain users group the Read permission for Docs1.

Answer: D

Explanation: This is the correct way to do it. By default, when the share is created, it will have the Everyone group with full control. You need to remove this, and add the Domain Users as read-only.

Incorrect Answers:

A. There is no protected storage service, and you can't logon to the system account. Sharing the DOCS will be with full control by default, and anyone can read and write (or erase) those files.

B. Using IIS in this case will allow everyone, including non-domain users (example: guests) to read the docs, which is too loose of a security model. Using IIS is also a lot of work. The reason is that you do not assign file and directory security in IIS, you do it in NTFS, and the C disk is FAT.

C. FAT does not support individual permissions on Directories and/or files. Everyone has access locally and via a Share, unless the permissions are explicitly set in the definition of the share itself.

QUESTION 35 You are the administrator of a Windows NT server computer named FS1. Company files are stored on FS1 in the E:\Files\Company Folder, which is shared as CompFiles. The shared folder was created by using the default permissions.

Permissions for the files in E:\Files\Company\Finance are assigned as shown in the following table.

Group	Permissions
Domain users	None
Accounting	Read
AcctManagers	Write Delete
Finance	Full control
Interns	No access
Marketing	No access

A user named Andrea is a member of the Domain users, Accounting, and Interns groups. The Interns group is used only to restrict access to the files in E:\Files\Company\Finance. Drive M on Andrea's computer is mapped to \\FS1\CompFiles. Andrea needs to modify the files in M:\Finance on a regular basis. She reports that she cannot access any files in the finance folder.

You need to ensure that Andrea can modify the appropriate files. You want to assign her the minimum permissions necessary, and you want to avoid assigning her additional permissions for other files on FS1.

Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

A. Remove Andrea's user account from the Accounting group.

B. Remove Andrea's user account from the Interns group.

C. Add Andrea's user account to the AcctManagers group.

D. Add Andrea's user account to the finance group.

E. Add Andrea's user account to the marketing group.

F. Assign the Accounting group the Read, Write, and Delete permissions for \\FS1\CompFiles.

G. Assign the Interns group the Read permissions for \\FS1\CompFiles.

Answer: B, C

Explanation: The first answer, B should not be a surprise, nothing changed. When you have "No Access" for a

directory and files, nothing overrides it, so we need to get Andrea out of the Interns group to get rid of the no access. By adding AcctManagers, Andrea can now write to the files, since she needs to modify them.

Incorrect Answers:

A. She still needs access to the accounting group to read the files in M:\Finance.

D. Adding her to the Finance group is overkill, she will have more permissions than needed, including the ability to change the permissions.

E. Marketing has no access to the directory, and adding he in will be sure to prevent her from accessing M:\Finance.

F, G. These actions modify permissions of other groups and users, most likely adding additional permissions.

We only know the permission structure of \\FS1\CompFiles\Finance, and not \\FS1\CompFiles. Changing these permissions would not affect Finance, unless Finance was inheriting permissions from the Company folder (its parent).

QUESTION 36 You are the administrator of a Windows NT server computer that is used as a print server. You use the default settings to share a printer on the server as a Check Printer. Check Printer is used for printing payroll checks.

A user named Carmen is your company's payroll clerk. Carmen reports that some employees print documents to Check Printer, which wastes blank checks and prevents Carmen from printing Payroll checks.

You need to allow only Carmen to send documents to Check Printer.

What should you do?

A. Change the share name of Check Printer to Check Printer\$. Configure Carmen's computer to print to Check Printer\$.

B. Assign Carmen the Full Control permissions for the printer driver files. Assign the Domain Users group the No Access permissions for the Printer driver files.

C. Assign Carmen the printer permission for Check Printer. Remove the Everyone group from the Check Printer access control list

D. Assign Carmen the Print permissions for Check Printer. Assign the Everyone group the No access permission for Check Printer

E. Assign Carmen the Manage documents permissions for Check Printer. Assign the Everyone group the No access permissions for Check Printer

Answer: C

Explanation: The default settings will be that the everyone group has full control, so you need to remove that setting. You then explicitly assign Carmen access to the printer.

Incorrect Answers:

A. This is not a secure answer. All you did is hide the share name. Anyone who knows the share name can still connect and destroy checks. Sometimes hiding something helps make it a little secure, because knowledge would be needed. But since everyone using the printer has inside knowledge, finding this printer should not be difficult. The correct course of action is to change the printer access permissions.

B. You can put access controls on the printer or printer share to control access. Access is not controlled by access control of the print drivers themselves. The print drivers are loaded by the OS (Windows NT), and security is not based on the user. Besides that not working, Carmen will most likely be a member of Domain Users, and setting no access will not only lock out everyone else from using the printer, but Carmen won't be able to use it herself.

D, E. The everyone group includes everyone, users and guests. By setting no access none, including Carmen and any administrator will NOT be able to print on the printer.

QUESTION 37 You are the administrator of a Windows NT server computer. The server runs Microsoft Internet Information Server (IIS) and hosts a web site. The web site is configured so that it has the default settings. Company employees access the web site by means of the company intranet and the Internet. The first page that employees see when they access the web site is named Default.asp. This page allows them to provide a user name and password. The page then redirects employees to a menu of available options. You want to ensure that employee user names and passwords are not transmitted over the Internet in plain text. You also want to ensure that the server's performance is minimally affected by employees who access the web site. You install a server encryption certificate on the server.

What should you do next?

- A. Configure Default.asp to disallow anonymous access
- B. Configure Default.asp to require secure communications for all connections
- C. Configure the web site to require secure communications for all connections.
- D. Configure the web site to allow Windows NT challenge/Response authentication

Answer: C

Explanation: When configuring the security on a web site, there are three options that may be selected: Anonymous, Basic, and Integrated (Windows NT Challenge/Response authentication). These are options used for internal security, and selecting Integrated is the only option that would protect passwords, as Anonymous does not use username and passwords for access control, and basic transmits password in the clear. EXCEPT, we are concerned here with that logon scenario. The Default.asp active server page is collecting the username and password as page data. This collection does not fall under the IIS security model, IIS does not know that username and password is being collected, these are not Operating System accounts. This is home grown internal security, such as internal security that has been built into a software package and does not integrate with Windows NT access lists. This is why a certificate was needed in the first step! We need to encrypt all the pages that could be carrying the information requiring protection. In this case we protect the web site itself.

Incorrect Answers:

- A, B. Security settings for either authentication or secure communications can only be configured on the Directory level, either in a Web Site or a Virtual Directory. It is not done on a page by page basis.
- D. Windows NT Challenge/Response authentication is part of integrated security, but as already explained, we are not doing Operating System authentication, we are performing application internal password processing.

QUESTION 38 You are the new administrator of your company's Windows NT server computers. A server named Web1 hosts a web site, which is configured to use integrated security and to disallow anonymous access. Company employees access the web site by means of the company intranet and the Internet. An employee named Marc reports that he cannot access the web site from his home computer. You verify that Marc can log onto the web site from the client computer in his office. You verify that Marc is using the correct browser version on his home computer. Marc's home computer connects to the Internet by using a dial-up account to an Internet Service Provider. You need to ensure that Marc can access the web site from his home computer.

What should you do?

- A. Assign the IUSR_Web1 user account and the domain users group the read permission for the web site files. Remove any permissions that are assigned to Marc's user account
- B. Configure the web site to allow anonymous access
- C. Create a new user account. Verify that the user account can access the web site from your home computer. Instruct Marc to use the new account when he accesses the web site from his home computer.
- D. Remove any IP address restrictions from the web site's directory security settings.

Answer: D

Explanation: We will see below that A, B, C will not apply here, so this leaves as a matter of elimination, choice D. It is possible, since an ISP is being used, that there could be IP restrictions that control the valid range of IP addresses. For example, suppose the IP restriction only allowed the Intranet and specific IP addresses of remote

users (assuming in this case that the home users ISP had assigned static IP addresses), Marc's IP address would have to be added in the list. So, choice D is a feasible answer in some situations, so for this case it is correct. Notice the format of this question. You are given a situation with a choice of answers. The question does not give you enough information to zero in on the correct answer, you need to know enough to eliminate the bad answers and take the choice that can work and is left. This is a manner of elimination.

Incorrect Answers:

A, C. Marc can connect using his account from work. Marc's account is already validated as having the correct access. Modifying the ACL or even creating a separate user account will not fix the situation. Marc can get into the site, and should be able to do it from anywhere. We also take notice that the question does not say anything about marc ability to sign on to the network, only that he cannot access the website. This should indicate that marc was able to establish a connection using the dial-up line. If Marc was unable to get pass establishment of the dial-up connection, then creating a new userid that was tested with the dial-up might be creditable. Also, in the Choice A, we might be assigning read permissions that allow unauthorized users to access the site - we have no idea how the site is, and should be permissioned.

D. Most of the explanation so far is basically saying that we are not dealing with a permission issue here with the ACL, but we add here that if we change the Authentication to allow anonymous users, then anyone can now access the site, and we have decreased our security protection. Also, as an anonymous user we would be using the IUSR_WEB1 user id, not Marc's, so Marc may have access control issues to access pages and files.

QUESTION 39 You are the administrator of a Windows NT server computer. The server is connected to a laser printer device, which is shared as Laser1.

The office staff uses Laser1 to print word processing documents and spreadsheets. The accounting staff uses Laser1 to print financial reports. These financial reports usually take a long to print.

The office manager informs you that the financial reports are preventing the office staff from using Laser1 effectively. She also tells you that the financial reports can be printed on Laser1 in the evening when other documents are not being printed.

You want to allow the accounting staff to send print jobs during the day without interrupting the office staff's printing activity.

What should you do?

A. Create a shared printer named acct to print to the laser print device. Set the priority on Acct to 30 and the priority on Laser 1 to 50. Instruct the accounting staff to print the financial reports to Acct.

B. Create a shared printer named acct to print to the laser print device. Set the priority on Acct to 50 and the priority on Laser 1 to 30. Instruct the accounting staff to print the financial reports to Acct.

C. Write a batch file that assigns the accounting staff the Print permissions for Laser1. Schedule the batch file to run each morning at 5:00 A.M. Write a second batch file that removes the print permission for laser1 from the accounting staff. Schedule the batch file to run each evening at 8:00 P.M

D. Create a shared printer named Finance to print to the laser device. In the Finance printer properties, configure the printer to be available from 8:00P.M to 5:00A.M. Instruct the accounting staff to print the financial reports to Finance.

E. Create a shared printer named Reports to print to the laser print device. Set the priority on reports to 10. Instruct the account staff to print the financial reports to Reports

Answer: D

Explanation: The accounting staff are printing LONG reports which tie up the printer. Since these reports do not have a high priority for turnaround, we can let them print at night when no one is around. To do this, we create another printer (Finance), using the same printer device (printer device pointed by Laser1), and restrict printing to off

hours. Notice that anyone printing to Laser1 directly can still print 24 hours a day, only print jobs directed to Finance will be restricted.

Incorrect Answers:

A, B, E. Priority here is not appropriate. All priority will do is change the order in which a print job comes off the queue. For example, suppose someone in accounting sends an 8 hour print job to the printer when the queue is empty, so it goes to the head of the queue and starts printing. If this happens at 9am, then the printer is totally unavailable for any other print job until after 5pm. Changing priority does not hold off the long print jobs until off hours, and can still lock out office users from using the printer during the day.

C. This answer is almost ridiculous, writing batch files to change permissions is not the accepted way to resolve this issue, since there are better way to get this done. Even if the batch script was used, this approach does not accomplish anything. What we are controlling is not when jobs can print, but when jobs are submitted. If everyone is working 9-5, no one should be around at 10pm so they can submit a print job. Now these people may be working late, but this script imposes the restriction that accounting can only submit the print job to the shared queue between 5am and 8pm, when everyone is basically in the office working, so the accounting print jobs will still conflict.

QUESTION 40 You are the administrator of a Windows NT server computer named Web1. Web1 runs Microsoft Internet Information Server and hosts an Intranet web site. The web site is configured so that it has the default settings. You add a virtual directory named marketing to the web site. The virtual directory points to the \\Files1\MktDocs shared folder, which contains documents that are published by your company's marketing department. You verify that users can view the documents by means of a web browser and HTTP. Several months later, users report that they can no longer access the documents by using HTTP. Some users can access the documents on their client computers by means of the \\Files1\MktDocs shared folder. You need to ensure that all users can access the documents by using the web site.

What should you do?

- A. Assign the Everyone group the Read permissions for the files in \\Files1\MktDocs
- B. Assign the Everyone group the Read permission for \\Files1\Marketing
- C. Configure the web site to allow anonymous access and to disallow Basic authentication
- D. Configure the user account that the virtual directory uses to access \\Files1\MktDocs so that the account is not locked out and so that the password never expires.

Answer: D

Explanation: We see that the Server is Web1 but the Shared Folder is on Files1, which is a different machine. When we set up the virtual directory, we were prompted with a username and password that would be used by Web1 to connect to the share. If that account gets deleted, locked out, disabled, or the password changes and we have exhausted the retries, then IIS will not be able to connect to the share.

Incorrect Answers:

A, B. We are not dealing with a permission issue, unless someone went in and changed the permissions. This was a working website. For both A & B, we could be downgrading the security settings allowing unauthorized users to see confidential data. These options are not recommended, and most likely will weaken the security set on those files.

C. The question says that the site was built with default settings, so anonymous access and disable Basic authentication IS THE DEFAULT, so we are not changing anything here.

QUESTION 41 You are the administrator of a Windows NT server computer named FS1. FS1 is used as a file server and has security configuration manager installed. FS1 contains several shared folders, which were created by using the default settings. The share HRDocs points to D:\Documents\HRDocs.

An employee named Bruno is a member of the HR group and the Operations group. Bruno reports that he cannot modify the documents in \\FS1\HRDocs from his Windows 2000 Professional computer.

You log on to the FS1 server console to examine the permissions for D:\Documents\HRDocs. The folder permissions are assigned as shown in the following table.

Group	Permissions
Domain users	Read: Allow
HR	Full Control: Allow
Operations	Write: Deny Read and Execute: Allow

You need to ensure that Bruno can read and modify the files in \\FS1\HRDocs.

What should you do?

- A. Add Bruno's user account to the list of permissions for D:\Documents\HRDocs, and then assign Bruno the Full Control: Allow permission.
- B. Create a domain user group named Operations2. Add the Operations2 group to the list of permissions for D:\Documents\HRDocs, and then assign the group the Full Control: Allow permission. Add Bruno's user account to the Operations2 group
- C. Remove Bruno's user account from the Operations group.
- D. Remove all user accounts except Bruno's from the operations group. Add Bruno's user account to the list of permissions for D:\Documents\HRDocs, and then assign Bruno the Write: Allow permission.

Answer: C

Explanation: If you belong to any group that has "no access", then your combined permissions is "no access". Bruno is a member of the operations group, which is denied write access to the directory and files. We need to remove Bruno from the Operations Group.

Incorrect Answers:

- A. Bruno has a deny, and no matter what else you do, the "no access" takes precedence.
- B. Bruno has a deny, and no matter what else you do, the "no access" takes precedence.
- D. Bruno has a deny, and no matter what else you do, the "no access" takes precedence. In this case you need to remove Bruno, not the other users.

QUESTION 42 You are the administrator of a Windows NT server computer named Public, which is a member of a Windows NT domain named CORP. Public runs Microsoft Internet Information Server and hosts an FTP site. The FTP site is configured so that it has the default settings. The site's home directory is C:\inetpub\Ftproot.

You need to use Public to allow a specific customer to upload and download files. You do not want this customer to have any other type of access. You do not want anyone else to have this type of access. You need to configure Public to support these requirements.

Which three actions should you take? (Each correct answer presents part of the solution. Choose three)

- A. Create a user account named Customer on Public
- B. Create a user account named Customer in CORP
- C. Assign the IUSR_Public user account the appropriate NTFS permissions for C:\inetpub\Ftproot
- D. Assign customer the appropriate NTFS permissions for C:\inetpub\Ftproot
- E. Configure the FTP site to allow anonymous access

F. Configure the FTP site to disallow anonymous access

Answer: A, D, F

Explanation: We are going to disable anonymous access so that only a user with a valid userid can get onto FTP. We restrict that access by creating a userid and setting NTFS permissions to the FTP directory. The user will be unable to do anything else, since we set NTFS permissions. This account is only valid on the member server PUBLIC, so the user would not be able to access anything else anywhere in the domain.

Incorrect Answers:

B. This could accidentally provide too much access, and is not required unless the IIS server was installed on a Domain Controller. Since the question just says server, we can assume that it is a member server. If the question should change or vary, realize that if the question specifically says Domain Controller, then we need a domain account, not a local account. Domain Controllers do NOT have local accounts.

C. IUSR_Public is the account for the anonymous user. We will be blocking anonymous access so no one else can access the web site / FTP site, so this is NOT the ID that we need to add permissions.

E. Allowing anonymous access (which is already done, it is the default) is NOT what we wish to do here. We want to block anonymous access because we don't want just anybody getting into the site. We need to disable anonymous access.

QUESTION 43 You are the administrator of a Windows NT server computer. The computer is used as a print server and shares 20 printers. The server contains two hard disks, which are named drive C and Drive D. Drive C has a 2-GB capacity and contains all of the operating system files. Drive D has a 10-GB capacity and contains no files.

During a maintenance inspection, you notice that drive C has only 3 MB of free disk space. You need to make space available on drive C and prevent the drive from filling up again.

What should you do?

A. Disable the creation of memory dump files when a STOP error occurs.

B. Configure the server to place spooled print jobs in a folder on drive D. stop and restart the Print Spooler service.

C. Create a new disk quota limit on volume C to deny space to users who exceed their quota limit

D. Pause the Print Spooler service. In the shared printer properties, use a smaller file type for the print mode.

Restart the print spooler service

Answer: B

Explanation: Since Drive D is the larger drive, we should move the SPOOL to that drive. And, even if the users fill up that drive instead, the Operating System (Windows NT) will not be impacted by a full drive. This is why we use partitioning to separate data from the Operating System to prevent a full drive from crashing the system.

Incorrect Answers:

A. I doubt we are running 2GB of ram where a memory dump filled up the drive. There is no indication that we even took a dump. The most likely cause of this situation was the spool filling up, and even if we were taking dumps, it would be better to move the spool anyway.

C. This is Windows NT, we don't support (Natively) disk quotas. In Windows 2000, disk quotas apply to individual files, not print spool, and even if it did, take 50,000 users sending small print job and you could still fill up 2GB without tripping the quota (with 50K users you could probably fill up the entire 20GB too).

D. There is no smaller file type.

QUESTION 44 You are the administrator of a Windows NT server computer. The computer is used as a print server and has several shared printers.

A user reports that she cancelled a print job several hours ago, but the job continues to appear in the print queue.

You examine the print queue and discover that the print job is canceling. Several other print jobs are waiting in the print queue.

You need to remove the cancelled print jobs and ensure that the other print jobs print.

Which three courses of action should you take? (Each correct answer presents part of the solution. Choose three)

- A. Stop the print spooler service
- B. Stop the server service
- C. Log on to the server as an administrator, and delete the print job file from the spool folder
- D. Log on to the server as an administrator, and cancel the print job in the print queue.
- E. Log on to the server as an administrator, and delete the printer port. Re-create the printer port, and assign it to the shared printer
- F. Start the Print Spooler service
- G. Start the server service

Answer: A, C, F

Explanation: We have a stuck print job, and usually recycling the print spooler service will clear it up. We need to delete the job, otherwise it will restart on the printer. In most cases this problem was caused by the print job itself, (corrupted file), and if we don't delete it, then it may restart and tie up the queue again.

Incorrect Answers:

B, G. Changing the server service will not fix the problem, and may cause other problems. Stopping the server service will prevent users from using the shared folders and printers on the machine. This only prevents submission and management of the print jobs. However, it does not affect the print queue, which is stuck. We have to work with the spooler service - that is where the print job is stuck.

D. The print job is already cancelled. We need to delete it to make sure it does not re-queue after recycling the print spooler.

E. Adding and deleting the port will not correct the problem. We need to work with the print spooler, which is the software where the print job is hung.

QUESTION 45 You are the administrator of a Windows NT server computer. You perform tape backups of the server as shown in the following table:

Evening	Time	Backup type
Sunday	10:00 P.M	Full backup
Monday, Wednesday and Friday	11:00 P.M	Incremental back up
Tuesday and Thursday	11:00 P.M	Differential backup

You use two sets of six tapes to perform your backups, and you alternate sets every week. You use a different tape for each backup and overwrite the tape as necessary.

On Thursday at 3:30 P.M., the server's hard disk fails. You need to restore as much data as possible from the backup tapes. You also want to complete the restoration as quickly as possible.

What should you do?

- A. Perform the restoration by using the Sunday backup, then the Monday backup, and then the Wednesday backup.
- B. Perform the restoration by using the Monday backup, then the Tuesday backup, and then the Wednesday backup
- C. Perform the restoration by using the Sunday backup and then the Tuesday backup
- D. Perform the restoration by using the Sunday backup, then the Wednesday backup, and then the Tuesday backup

Answer: A

Explanation: Three things to note here. First, We must always do a Full restore when a hard drive is replaced. Second, the tapes must be applied (restored) in the order that the backups were taken, finally, we don't mix Incremental with Differential backups. We need Wednesday's restore to bring the drive back, so we will also need Monday's incremental too.

Incorrect Answers:

B. We need to start with the Sunday, we need to do a full restore.

C. In this case we lost Wednesday's data, so we don't have as much recovery as we would like.

D. Don't mix the backups, and this is the wrong order too.

QUESTION 46 You are the administrator of a Windows NT server computer named server1 that has service pack 6a installed. Server1 runs a business application that must be available at all times. You install a new SCSI device that was provided by the computer manufacturer. You restart server1.

During the startup process, server1 stops, and you receive a STOP error message.

You need to return Server1 to full functionality as quickly as possible.

What should you do?

A. Use a parallel installation of Windows NT server to restart Server1. Reinstall service Pack 6a

B. Use a Windows NT server CD-ROM to restart server1 in recovery mode. After Setup completes, restart the computer

C. Use the Last Known Good configuration setting to restart server1.

D. Use the Recovery Console to restart server1. Use an older copy of the device driver file to overwrite the new file. Restart the server1.

Answer: C

Explanation: You must read the wording of the question very carefully, especially since Microsoft may add a variation to the question, or this question was not copied correctly. This question says a SCSI "device". This solution should work for a device, such as a SCSI Tape Controller. It will NOT work for a SCSI Controller Card, which is imbedded more into the operating system, and would not be disabled by using Last Known Good. Also take note in this question that it says that a NEW device was installed. This solution most likely will NOT work if the question said NEW device drivers for an existing SCSI device. These require external action, where we can't bring up the system on its own.

Incorrect Answers:

A. Re-installation of Service Pack 6a might be required if the device drivers from the manufacturer regressed the service. This will not get us up in the quickest possible time. Especially if you have to do the parallel installation right now, which could take an hour or two - at minimum.

B. Unless you have a Windows NT Server CDROM at Service Pack 6a (Microsoft does not distribute Windows NT 4 this way, you get the service packs separate), this process will regress the entire service pack. Once you re-boot, the service pack has to be re-installed, and you might not get the system up anyway. And, this would not be the fastest way to get up and running again.

D. Recovery Console is provided via Windows 2000, but if we did have recovery console, we could use it here since recovery console will support a Windows NT system. However, using an older copy of the device driver is not the answer. First, we added the device, we did not upgrade the drivers. Second, there is no telling if the regression to an older device driver will fix the problem.

QUESTION 47 You are the administrator of a Windows NT server network. Your company plans to deploy Windows 2000 Professional to 800 client computers on your network. From the Windows 2000 Professional CDROM, you copy the contents of the i386 folder to D:\Win2000p\i386 on a Windows NT server computer named Apps1. You share D:\Win2000p as Proinstall. You receive a CD-ROM that contains the most recent

Windows 2000 service pack. You want all new Windows 2000 Professional deployments to include the service pack. You want to deploy the service packs by using the least amount of administrative effort.

What should you do on Apps1?

- A. Run the Update.exe /s D:\Win2000p command from the service pack CD-ROM
- B. Install remote installation services. Configure RIS to deploy the service pack at the same time that Windows 2000 Professional is deployed
- C. Copy the contents of the service pack CD-ROM to D:\Win2000p\i386. Click yes if you are prompted to overwrite existing files.
- D. Copy the contents of the service pack CD-ROM to D:\Win2000\Sp. Install Windows 2000 Professional on a client computer, and then run the \\Apps1\Proinstall\sp\Update.exe command from that computer.

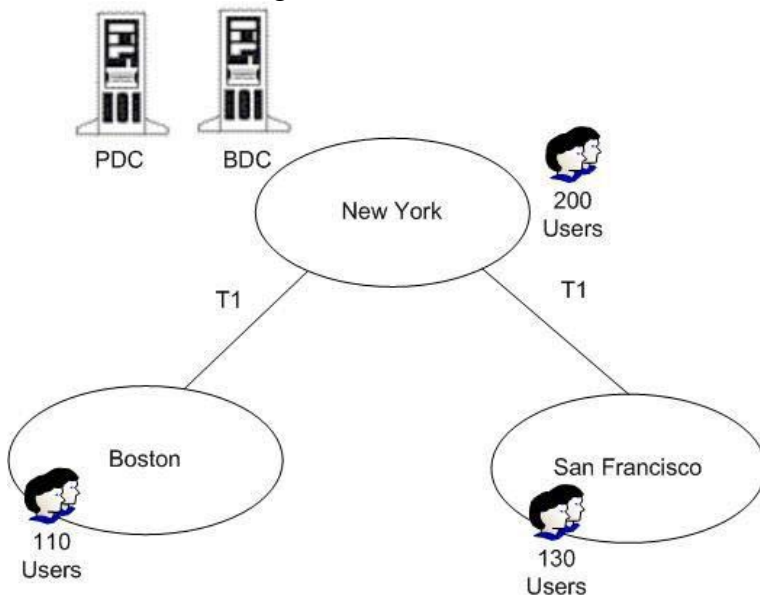
Answer: A

Explanation: Windows 2000 allows you to update an image using the update.exe command. After running the update command, the Windows 2000 Professional image will be at the new service pack. Any deployment after applying the service pack will automatically have the maintenance applied, which eliminates the need to apply the service pack separately.

Incorrect Answers:

- B. RIS is only supported on Windows 2000 Active Directory Domain.
- C. The service pack structure is a little more complicated. You might manage to replace files, but there is more going on in the service pack apply that needs to be checked and changed in the original image, so we need to run the update.exe.
- D. This process would allow us to apply the service pack off a network drive. But it would be two step, first build the system, then apply the service pack, where Choice A is one step.

QUESTION 48 You are the administrator of a company network that consists of a single Windows NT domain named CORP1. Your company's headquarters is located in New York. The company has one branch office in Boston and one branch office in San Francisco. All network administrators are located at headquarters. The network is configured as shown in the exhibit.



Users at the branch office reports the their logon scripts take a long time to run. You want to reduce the time require for the logon scripts to run. You also want to maintain the ability to manage all company user accounts from headquarters.

What should you do?

- A. Install a PDC for a domain named BOSTON in the Boston office. Install a PDC for a domain named SANFRAN in the San Francisco office. Configure the CORP1 PDC to trust the two new PDCs. Create user accounts on the CORP1 PDC
- B. Install Windows NT BDC servers in each branch office. Configure directory replication to replicate the logon scripts from the CORP1 PDC to the two new BDCs
- C. Install a stand-alone Windows NT server computer in each branch office. Configure directory replication to replicate the logon script from the CORP1 PDC to these two new servers
- D. Configure an LMHOSTS file so that it contains the IP addresses of the CORP1 PDC and BDC. Place this file on the client computers at the branch offices

Answer: B

Explanation: The assumption here is that the time to run the logon scripts is being impacted by contention at the central location and network traffic across the T1 lines. We can speed this by adding local BDCs and replicating the logon scripts to them. This way HQ can still maintain the scripts and user accounts at the central office.

Incorrect Answers:

- A. This process could speed up logon processing, but the logon scripts have to be migrated too, and there is no provision here to replicate them. Also, we just made the environment a lot more complex by going multidomain.
- C. Logon Scripts execute out of the NETLOGON folder of a BDC or PDC. NOT Member servers.
- D. The issue is transferring the logon scripts. There is no indication that there was a slowdown in locating servers. LMHOSTS would not have been the way to go if finding the server was an issue, you would use WINS. We have located the server, so it is not a IP to NAME resolution problem.

QUESTION 49 You are the administrator of a Windows NT server computer named server1. Server1 contains three 12- GB hard disks and 256MB of RAM. Server1 has a single 324-MB paging file on drive C. Server 1 supports an application that your company's software developers are creating. The application must be available at all times.

While you are running performance monitoring tools on Server1, you notice that users access drive C much more than the other two drives. Users report that server1 is slower than other servers on your network. You want to reduce the load on drive C and to improve the performance of Server1. You need to ensure that server1 continues to provide diagnostic information to the application developers in the event of a failure.

What should you do?

- A. Schedule the Chkdsk utility to complete a full scan, excluding a surface-level scan, on drive C the next time server1 is restarted. Restart server1.
- B. Configure server1 to perform a small memory dump to the paging file in the event of a STOP error C. Resize the paging file on drive C to 256 MB. Create a 50-MB paging file on the drive D and a 50-MB paging file in drive E.
- D. Create a 324-MB paging file on drive D. Remove the paging file from drive C.

Answer: C

Explanation: Paging performance will be better if spreading it across multiple physical disk drives. (Not disk partitions on the same physical drive). Since we want diagnostic information, in other words a dump during failure, we need a page file on the boot device that will hold all of RAM, so we need at least 256MB (the size of RAM on this server) as the smallest page file for C.

Incorrect Answers:

- A. Using Chkdsk is when the file system gets corrupted. There is no evidence that the system slowness is due to a corrupted file system. Usually you lose files.

B. A small memory dump does not provide as much diagnostic information as a full dump, and would not solve the slowness (probably due to contention of the page file) unless the page file was moved somewhere else and decreased in size.

D. This may make the system faster, but lack of a page file on C will prevent diagnostic dumps from being taken.

QUESTION 50 You are the administrator of a Windows NT server computer named serverA. ServerA has two 20-GB IDE hard disks that are configured as a mirrored pair. ServerA has two IDE channels. Disk 0 is the primary drive and the IDE master device for channel 0. Disk 1 is the shadow drive and the IDE master device for channel 1.

ServerA shuts down due to permanent failure of Disk 0. You have a replacement disk available for this server. You need to enable serverA to restart so that you can recover from the failure and reconfigure fault tolerance.

Which two courses of action should you take? (Each correct answer presents part of the solution. Choose two)

A. Modify the Boot.ini file on a fault-tolerance boot disk to point to multi (1) disk (0) rdisk (1).

B. Modify the Boot.ini file on a fault-tolerance boot disk to point to multi (0) disk (1) rdisk (0).

C. Modify the Boot.ini file on a fault-tolerance boot disk to point to multi (1) disk (0) rdisk (0).

D. Replace Disk 0 with the replacement disk. Configure the replacement disk as the IDE master device on Channel 0

E. Replace Disk 0 with disk 1. Configure the replacement, and configure it as the IDE master device on Channel 0

F. Replace Disk 0 with disk 0. Configure the replacement disk, and configure it as the IDE slave device on Channel 0

Answer: C, D

Explanation: We have to boot the system up with a floppy because the physical disk that would be booted is now dead. With the exception of Partition, all the other parameters in the boot.ini (ARC) definitions are zero relative. For Channel 1, it is Multi(0), and for the first device (Master), it is rdisk(0). Now all we need to do is boot the floppy, and the system will come up. We also should replace the defective drive with the replacement.

Incorrect Answers:

A. This definition is for the slave (rdisk=1)

B. This definition is invalid for an IDE configuration.

E. For recovery, you do not re-cable disks to change the ARC settings.

F. This answer doesn't even make sense, replace 0 with 0?

QUESTION 51 You're the administrator of a Windows NT domain that contains a Windows NT server computer named FPS1. FPS1 is used as a file and print server. The server hosts eight shared printers. Each shared printer is configured to use a different print device.

An employee named Lilly is responsible for changing the toner cartridges, adding paper, and completing other maintenance tasks for five of the print devices.

Users often ask Lilly to move shorter print jobs to the top of the print queue and to cancel long-running print jobs so that the printers are available for immediate use. However, Lilly cannot change the priority of a print job or cancel a print job.

You need to enable Lilly to perform these tasks for the five print devices for which she is responsible, but you need to prevent her from modifying the printer properties.

What should you do?

A. Add Lilly's user account to the Print Operators group. Assign Lilly the No Access permission for the three printers for which she is not responsible.

- B. Add a "\$" to the value of the Network path property on the five printers for which Lilly is responsible.
- C. Assign Lilly the full control permission for the five printers for which she is responsible
- D. Assign Lilly the manage documents permission for the five printers for which she is responsible.

Answer: D

Explanation: Manage documents will allow Lilly to change priority and cancel print jobs.

Incorrect Answers:

- A. Print Operator will allow Lilly to change printer properties, which is not what we want to allow. This gives her too much permissions, as well as permissions on new printers which have not been added yet.
- B. The \$ will hide the share, and has no effect on the ACL for the device. Further, the \$ will affect the share name, which affect the printer, not the print device.
- C. Full control is too much permissions, it will allow printer properties to be changed.

QUESTION 52 You are the administrator of a Windows NT server computer. The computer is connected to two identical print devices. You create one shared printer for each print device by using the default settings. One printer is shared as Executive, and the other is shared as Office. The president of your company often has to wait for his documents to print to the Executive printer because other office employees also print to it. You need to configure the printer so that the president's documents print as quickly as possible.

Because the office printer is too busy to accommodate all office print jobs, you need to ensure that office employees can also print to the Executive printer.

What should you do?

- A. Add Executive\$ as a new share name for the Executive shared printer. Reconfigure the president's computer to print to Executive\$.
- B. Add Exec Staff as a new share name for the Executive shared printer. Set the permissions for the Executive shared printer to allow only the president's user account to print. Reconfigure the office computers to print to Exec Staff.
- C. Create a shared printer named Pres for the print device that is associated with the Executive shared printer. Configure the Pres shared printer so that it has a priority of 98. Reconfigure the office computers to print to Pres.
- D. Create a shared printer named PresOnly for the print device that is associated with the Executive shared printer. Configure the PresOnly shared printer so that it has a priority of 98. Reconfigure the president's computer to print to PresOnly.
- E. Create a shared printer named Staff for the print device that is associated with the executive shared printer. Assign the president the manage documents permissions for the executive shared printer. Assign the office staff the print permission for the Staff shared printer. Configure the office computers to print to Staff.

Answer: D

Explanation: Print priority can be set between 1 and 99, where 99 is the highest and 1 is the lowest. We can make different printers and point those printers to the same print device. In this case, we create a separate printer with a priority of 98, which is almost the highest it goes, and will be higher than the default print priorities used by the office users. In this scenario, even though the president has to share the printer, the president's jobs will always go to the head of the queue and will be the next job to print on the printer. This satisfies the requirement to get the president's jobs printing as quickly as possible.

Incorrect Answers:

- A. Adding a \$ to the end of a share name makes that share a hidden share. It will not affect the print priority nor will it affect the print permissions on the resource.

B. This scenario enforces that the president can only print to the new printer. However, the president's print jobs will have the default priority, and will fall into line with the print jobs from the office workers. The president will have to wait in line like everyone else, and this does not get the president's print jobs printing as quickly as possible.

C. In this scenario, the office computers will be printing with a priority of 98. Since 98 is almost the highest priority, the president's jobs, which will have a lower priority (the default priority setting) will go to the back of the line and will not print until there are no longer any office print jobs in the print queue.

E. Again, the print device will be shared, and there is no separation of priorities. The president will wait in line like everyone else. Now the president can manipulate the queues with this option, however this is not a feasible solution.

QUESTION 53 You are the administrator of your company's network. The network includes two identical print devices and a Windows NT server computer. The printers for these print devices are shared as Printer1 and Printer2. The server is used as a print server.

Users can print to both shared printers. However, most of the client computers are configured to use only one printer or the other. Client computers in the accounting department are also configured to use Printer1.

Users in the operations department report that the users in the accounting department often print large reports. The users in the operations department must wait for their documents to be printed even though few or no documents are being printed on Printer2.

You want to configure the printers so that the printing load from both departments is evenly distributed. What should you do?

A. Create a new shared named Printer3. Configure printer3 to use both print devices in a printer pool. Configure all user accounts to print to printer3.

B. Configure printer1 to print to the same port as printer2. Set the priority on printer1 to 50 and the priority on printer2 to 75.

C. Configure printer2 to print to the same port as printer1. Set the priority on printer 1 and printer2 to 50.

D. Modify the registry so that printer1 and printer2 use the same folder to store spooled print jobs.

Answer: A

Explanation: This will end up being the best choice. Printer load balancing will allow the print jobs to print on the next available printer. This also makes the printers evenly balanced. Unfortunately in real life this is not the best solution, because the accounting department will have long jobs on BOTH printers, and still tie everything up. But, we are not offered solutions here that parallel real life.

Incorrect Answers:

B, C. We have two physical print devices, each on it's own port. We do not want to change either printer so that both printers are printing to the same port. Doing so in this problem leaves us with only one printer working and operational.

D. You do not want to merge print spool folders. This will be a problem because there are indexes in the folder of the net spool file, the files are numbered and can overlap, and it will be rare that the correct answer to a Microsoft Exam will involve changing the registry in order to fix a problem.

QUESTION 54 You are the administrator of a Windows NT server computer. The computer is used as a file and print server and shares four printers. The printers are shared as printer1, printer2, printer3, and printer4. A user reports that a document has been first in the printer2 print queue for several hours and that nothing is printing on the print device. You examine the print queue and discover that the first job is spooling. Several other print jobs are waiting in the print queue. You verify that the print device is functioning correctly. You attempt to cancel the spooling print job, and you want to minimize downtime for other users.

What should you do?

- A. Restart the computer. Reset the printer2 print device while the computers is restarting
- B. Stop the print spooler service, and then delete the files in the folder that contains spooled print jobs.
- C. Reset the printer2 print device. Stop and restart the server service
- D. Stop the print spooler service and the server service. Reset the printer2 print device, and then restart both services.
- E. Delete any zero-byte files from the print spool folder.

Answer: B

Explanation: Usually, when the print spooler hangs for any reason, you recycle the print spooler by Stopping and then starting the print spooler. However, if we just do that, the bad job may try to print again and hang the spooler again. So, we recycle the spooler, but clear the spool of bad print jobs. Because of the indexing of the jobs in the spool, we need to clear the entire folder of spooled print jobs.

Incorrect Answers:

- A. The computer is used as a file and print server. Restarting the entire computer or recycling the server service will impact the file server functions, and anyone using files on shared folders will be impacted.
- C. The computer is used as a file and print server. Restarting the entire computer or recycling the server service will impact the file server functions, and anyone using files on shared folders will be impacted. In this case, we need to stop and start the print spooler service, so not only did we impact the file users, but we did nothing for the printer.
- D. The computer is used as a file and print server. Restarting the entire computer or recycling the server service will impact the file server functions, and anyone using files on shared folders will be impacted.
- E. We need to stop the print spooler because the spooler may have those files open, and they can't be deleted while open. Also, deleting the files will not get the spooler going again, it needs to be recycled.

QUESTION 55 You are the lead administrator of a Windows NT domain that contains Windows NT server computers, Windows NT workstation computers, Windows 2000 Professional computers, and Windows 98 computers. TCP/IP is the only network protocol that is used on your network.

While an assistant administrator was using Network monitor to troubleshoot a network problem, she captured confidential corporate data as it was transmitted over the network.

You need to protect confidential data from this kind of capture.

Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

- A. Configure each server that contains confidential data to require Windows NT LAN manager version 1 authentication.
- B. Configure each server that contains confidential data to require Windows NT LAN manager version 2 authentication.
- C. Configure each server that contains confidential data to require SMB signing.
- D. Enable SMB signing on each client computer.
- E. Install Active Directory client software on each Windows NT workstation computer.
- F. Install Active Directory client software on each Windows 98 computer

Answer: B, F

Explanation: NTLM V2 is a more secure form of authentication using encrypted data. It requires SP2 on a Windows NT 4.0 system, and can be run on a Windows 98 system with the Active Directory Client installed. In both cases, the clients and the server may require (the Windows 98 & Windows NT definitely do) registry settings to be made to enable NTLMv2 or force this as the only acceptable authentication method.

Incorrect Answers:

- A. All the Windows NT 4.0 systems and Windows 98 systems already will be using NTLMv1 by default. This

level does not provide protection of the data.

C, D. SMB Signing is not supported for Windows 98. SMB signing will sign the packets to ensure that the packets are not modified in transit. However, signing the SMB blocks does not protect the confidentiality of the data within the SMB.

E. The workstation should be at SP4 or later. Support for NTLMv2 on Windows NT 4.0 is not added by using the Directory Service Client.

QUESTION 56 You are the administrator of a Windows NT server computer named Server1. Server1 hosts an application named App1. App1 must be available at all times, except during scheduled maintenance periods. During a scheduled maintenance period, you install the most recent Windows NT server service pack on server1 by using the default settings.

You also install two recent Microsoft hot fixes, which are named Hotfix1.exe and Hotfix2.exe. Hotfix1.exe corrects a security vulnerability, and Hotfix2.exe corrects a disk performance problem.

After you install hotfix2.exe, you discover that the hot fix is incompatible with a device driver on server1 and is preventing App1 from functioning properly.

You need to restore app1 to full functionality as quickly as possible. You also want to ensure that server1 retains the most recent security updates.

What should you do?

A. Reinstall Hotfix2.exe

B. Uninstall Hotfix2.exe

C. Reinstall the service pack. Install Hotfix1.exe

D. Uninstall and reinstall the service pack. Copy the files from Hotfix1.exe to a folder on Server1.

Answer: B

Explanation: The hot fixes have an uninstall feature. This question would have been more complicated if we needed to back off Hotfix1 instead, but we got lucky. Since it was the last hot fix applied, we only need to uninstall it.

Incorrect Answers:

A. Why would we do this? This is the fix that is giving us problems. We want to get rid of the fix (back it off), not apply it again.

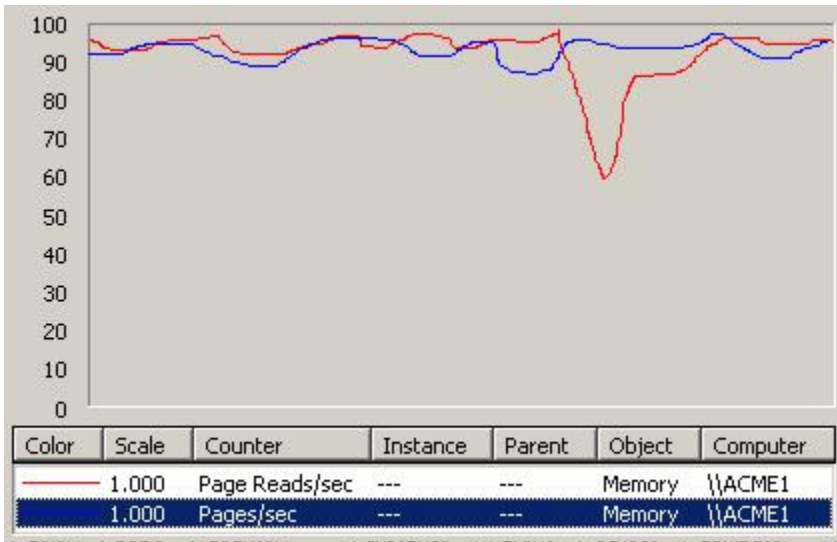
C. A hot fix is service that is released before a service pack because it is critical to be applied, and can't wait for the formal service pack to be released. It does not mean nor imply that modules changed by the hot fix are all in the previous or earlier service packs. Reinstalling the service pack is not guaranteed to regress both hot fixes. And if some of the modules modified by the hot fix is in the service pack, and some are not, then this scenario will destabilize the system.

D. This almost does the same thing a C, and could even be a little more dangerous. Service Packs and Hot fixes do more than copying files. They may make registry changes and update files (change the files, not replace them), so copying files could be a problem and should not be done. A hot fix is service that is released before a service pack because it is critical to be applied, and can't wait for the formal service pack to be released. It does not mean nor imply that modules changed by the hot fix are all in the previous or earlier service packs. Reinstalling the service pack is not guaranteed to regress both hot fixes. And if some of the modules modified by the hot fix is in the service pack, and some are not, then this scenario will destabilize the system.

QUESTION 57 You are the administrator of a Windows NT server computer. The computer contains a single 400-MHz processor, 128 MB of RAM, and a single hard disk. The computer is used as a file server and also runs client/server applications.

Users report that the server's performance is slow. You run performance monitor and receive the results shown

in the exhibit.



You examine Task Manager for several minutes and discover that the System idle task is receiving an average of 90 percent of the processor utilization. You need to improve the server's performance.

What should you install on the server?

- A. A faster hard disk
- B. An Additional 128 MB of Ram
- C. An additional processor
- D. An additional hard disk

Answer: B

Explanation: The system is showing a high paging rate, which can be reduced by adding more memory (RAM).

Incorrect Answers:

- A. A faster hard drive will page faster, but the solution is to reduce the paging itself.
- C. At 90% idle time, we do not have a processor contention problem, a processor upgrade will not fix the problem.
- D. The problem is with paging, An additional hard drive may help the system to page better, but in this case what we to do is reduce the paging, not make it work better.

QUESTION 58 You are the administrator of a Windows NT server computer. A 12-GB DAT drive is attached to the server. The DAT drive does not support data compression. The server contains two 20-GB hard disks that are configured as a RAID-1 array.

The server is configured to perform a full backup to tape every night. However, the backups are failing because the backup tape fills up before the backup is complete.

If necessary, you can purchase a maximum of two additional DAT drives to support the nightly full backups.

However, you need to purchase the minimum number of drives necessary to complete the task.

If two or three drives will not allow the full backups to complete successfully each night, you need to create a backup plan that uses only one drive and does not require nightly full backups.

What should you do?

- A. Use only the original 12-GB DAT drive. Create a backup plan that backs up a different 12-GB portion of the hard disks four days per week.
- B. Use only the original 12-GB DAT drive. Create a backup plan that performs a differential backup every night. Perform a full backup on Monday afternoons, and change DAT tapes as necessary.
- C. Purchase one additional 12-GB DAT drive. Create a backup plan that performs a full backup every night and

uses both DAT drives.

D. Purchase two additional 12-GB DAT drive. Create a backup plan that performs a full backup every night and uses all three DAT drives.

Answer: C

Explanation: Since we are running RAID-1, we need to know RAID. RAID-1 is mirroring, so the two 20 GB drives are mirror of each other. We only need (and only should) be backing up 1 of the disk drives (physically), so we have a maximum of 20GB of data - assuming that the drives are completely full. Two 12GB DAT tapes will

hold up to 24GB of data (Uncompressed). This even gives us 4GB to spare on the tape.

Incorrect Answers:

A, B. We can do this with two tape drives (one extra to be acquired), so we don't need an alternate plan.

D. We can do this with two tape drives, so we don't need to buy a third.

QUESTION 59 You are the administrator of your company's Windows NT server network. You are installing Windows NT server on a new computer. The computer has five 18-GB hard disks. You want to configure the computer to provide fault tolerance for the operating system files and data files. You plan to use two logical drives on the computer. The operating system files will be stored on drive C, and user data files will be stored on drive D. You need to configure the hard disks. You want to minimize wasted disk space and maximize performance.

Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

A. Create a mirrored pair for drive C.

B. Use a single hard disk to contain drive C.

C. Create a mirrored pair for drive D.

D. Create a stripe set for drive D.

E. Create a stripe set with parity for drive D

F. Create a volume set for drive D.

Answer: A, E.

Explanation: We have 5 drives. We will also assume here that we are using software RAID, although that is not a requirement for this question. It would be an issue since you can't boot off of a striped solution using software RAID, the only fault tolerant solution for the C drive would be mirroring. For data, we would want to use RAID 5 (Striped with Parity) since it only wastes one drive. The more drives in the RAID Array, the less wasted. The best breakdown is 2 and 3, 2 Mirror and 2 Striped with Parity.

Incorrect Answers:

B, D. These are not fault tolerant solutions.

C. This wastes too much space, mirrors waste 50%, the Striped with Parity (for 3 drives) wastes 33.3%

F. This is not fault tolerant, and is only supported on Windows 2000 and higher.

QUESTION 60 You are the administrator of a Windows NT domain named CORP1. Your network also includes a domain named APP1 which currently contains no member servers or user accounts. Your company purchases an application that runs on a Windows NT server computer. The application has the ability to assign its security permissions to user accounts and groups in a Windows NT domain.

An employee named Bruno needs membership in the Domain Admins group to properly administer the application. However, company policy does not allow him to have access to the user account information in CORP1.

You need to provide Bruno with the appropriate access to administer the new application. You want the application to assign security permissions to user accounts in CORP1.

Which three actions should you take? (Each correct answer presents part of the solution. Choose three)

- A. Install the application on the APP1 PDC
- B. Install the application on a CORP1 BDC
- C. Add Bruno's user account to the domain Admins group in APP1
- D. Add Bruno's user account to the Domain Admins group in CORP1
- E. Add Bruno's user account to the local Administrators group in the member server that hosts the application
- F. Configure a one-way trust relationship so that CORP1 trusts APP1.
- G. Configure one-way trust relationship so that APP1 trusts CORP1

Answer: A, C, G

Explanation: Bruno needs Domain Admin permissions, but can't (not allowed by policy) access CORP1's account information. This leaves us to put the application in its own domain, and make Bruno the Domain Admin there. Just because Bruno is the Domain Admin of one, doesn't implicitly make him a Domain Admin of the other,

regardless of trust relationship. Since the application will make changes to security settings in CORP1, the application will require permissions to access and modify the user accounts and security settings in CORP1. Bruno's account is most likely defined in CORP1 because APP1 does not have user accounts (or member servers) of its own. So, if Bruno's account is in CORP1, then APP1 has to trust CORP1 so that a CORP1 user account (in this case, Bruno) can manage resources in the APP1 domain.

Incorrect Answers:

- B. The overall plan requires Bruno to be segregated into a different permission domain, so we need to put the application into its own domain.
- D. If we added Bruno as a Domain Admin to CORP1, then he could access the user accounts, and this problem forbids that.
- E. The application is being installed on a Domain Controller, not a member server, so there is no local administrator.
- F. APP1 needs to trust CORP1, but since there are no user accounts in APP1, CORP1 does not need to trust APP1.

QUESTION 61 You are the administrator of a Windows NT server computer named serverA. ServerA is the routing and remote access server for your network. The server has a 12-port analog 56-Kbps modem card installed. Routing and remote access service is configured to use the modem card for incoming analog connections.

You create a new user account for a consultant named Jenny. Jenny is using a UNIX computer to work on a database project for your company.

Jenny reports that she can't connect to serverA by using her UNIX-based SLIP client software. When you dial in to serverA from your Windows 2000 Professional computer, you can connect by using jenny's account.

You need to resolve this problem.

What should you do?

- A. Configure Jenny's account to disable callback
- B. Configure Jenny's account to include the MAC address of her UNIX computer in the list of authorized workstations.
- C. Configure Jenny's computer to use UNIX-based PPP client software
- D. Configure Jenny's computer to disable data encryption in her dial-up connection properties.

Answer: C

Explanation: A RAS server does not support SLIP, only PPP connections.

Incorrect Answers:

- A. Even if callback was in effect, you need to connect into the RAS server first, and this can't be done.
- B. The MAC address is not the issue, the protocol isn't supported.
- D. This is not an encryption issue, the protocol isn't supported.

QUESTION 62 You are the administrator of a network that consists of a single Windows NT domain. The domain contains Windows NT server computers, UNIX computers, and Windows 2000 Professional computers. The domain also contains a DHCP server and a WINS server.

The UNIX computers use a DNS service on a computer named UNIX1 that is managed by an offsite contractor. The contractor usually takes three to five days to respond to requests.

Users of the Windows 2000 Professional computers are required to use IP addresses to access the UNIX computers. You want to configure the network to make it easier for these users to access the UNIX computers. You also want to eliminate the need for a contractor to manage the name resolution for the UNIX computers. Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

- A. Configure the network DHCP scope to include the IP addresses of the UNIX computers in its range.
- B. Configure the network DHCP scope to use UNIX1 as a DNS server
- C. Configure the network DHCP scope to use a Windows NT server computer as a DNS server
- D. Install the DNS server service on a Windows NT server computer, and configure the UNIX computers to use the new DNS server service.
- E. Install an additional WINS server, and create WINS records for each UNIX computer.

Answer: C, D

Explanation: What we are doing here is replacing the UNIX DNS server with a Windows NT DNS server. We can set in the scope options that the client is to receive the name or IP address of the DNS server through the scope. Answer C does this, so each Windows 2000 Professional computer will point to the new DNS server. But we don't have a DNS server, so we have to make one. Answer D (which should be done first) will create a Windows NT DNS server. Remember in the question that before we did this the users had to access the UNIX computers via IP address? This hint tells us that the UNIX computers are most likely STATIC IP addresses. If they weren't, then using an IP address would be almost impossible because it could change often (at each reboot). For this reason, the UNIX computers are most likely NOT DHCP clients, so we have to go in and manually configure the UNIX machines to use the new DNS server.

Incorrect Answers:

- A. This task has no use. It appears that the UNIX machines are static IP addressed, and adding the IP range to the scope (without the proper reservations) will cause havoc as DHCP could possibly reissue active IP addresses.
- B. It is obvious that we want to get off the UNIX server. Why would Microsoft ask you a question on the exam where you will make the UNIX machine a better option? Think about it, you probably have the contractor do the UNIX configuration because no one else has the experience. You are becoming a Windows NT specialist, so you should know how to set up DNS. Therefore, it is going to be better to run the DNS on the Windows NT server, because you as a MCSE will know how to configure it, and then get rid of the contractor.
- E. Unless you re running SAMBA, WINS will have limited use. At this point you need to access the UNIX computers using DNS. You already have a WINS server, so there is no need to create a second one - except for fault tolerance. Since we need two answers, there actually is no other choice that can work with this potential answer.

QUESTION 63 You are the Webmaster of your company's intranet. The intranet is hosted by a Windows NT server computer named ServerA. Users access the intranet by using the URL <http://intranet>. You are adding a new web site to serverA. The company plans to use the new web site to track details of customer projects. You

want users to be able to access the site by using the URL `http://Projects`.

What should you do?

- A. Add a WINS entry for Projects that includes the IP address of serverA. Configure the Projects web site to use host headers
- B. Add a DNS entry for Projects that includes the IP address of ServerA
- C. Create the Projects Web site as a virtual directory, and place it under the intranet web site.
- D. Create the projects web site as a folder in the intranet web site.

Answer: A

Explanation: In the DNS, if we point Projects to the IP address of ServerA, then those calls will be routed there. The Projects web site will need host headers to determine which traffic goes there. Although Answer A mentions the host headers, it is not a good choice, see explanation below.

Incorrect Answers:

- A. Depending on configuration, this may work on a Windows NT/2000 client. But we aren't told which clients are on the Intranet. Clients like Unix do not support WINS, and there are other details from the question that are missing. If we knew that there was a Windows NT DNS server that referred requests to the WINS server, A could be workable, but in the absence of that information B is the better choice.
- C, D. This doesn't give the desired result. To reference the Projects directory, we would have to use: `http://Intranet/Projects`, which is the wrong form.

QUESTION 64 You are the administrator of a Windows NT sever computer named ServerA. Two users, who are named Katrin and Peter, report that network performance is sometimes very slow when they access ServerA. You want to be notified when network performance is slow for Katrin's and Peter's computers. Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

- A. Install the SNMP service on Katrin's and Peter's computer.
- B. Install the SNMP service on serverA.
- C. Install the Network Monitor Agent on Katrin's and Peter's computers.
- D. Install Network monitor Agent on ServerA.
- E. Run performance Monitor in Alert View on your client computer to view the Network Segment counter for Katrin's and Peter's computers.
- F. Run performance monitor in Log View on your client computer to log the Network Interface counter for Katrin's and Peter's computers.

Answer: C, E

Explanation: The first thing that needs to be done is to install the Network Monitor Agent, because installing the client installs the driver, and the driver installs the performance variables. So, if you want to use performance monitor, then you need performance variables, and the Network Monitor Agent install caused them to be installed. You need to cover each computer that has to be monitored, so we do this for both users. Then we want to do the monitoring, but we want to be notified when the performance is slow, meaning at the moment it is slow, we want to know. This way, then we can do other things at that moment to drill down the problem and look at other

factors. Therefore, we need to be in alert status, so we can receive an alert when the exceptions occur.

Incorrect Answers:

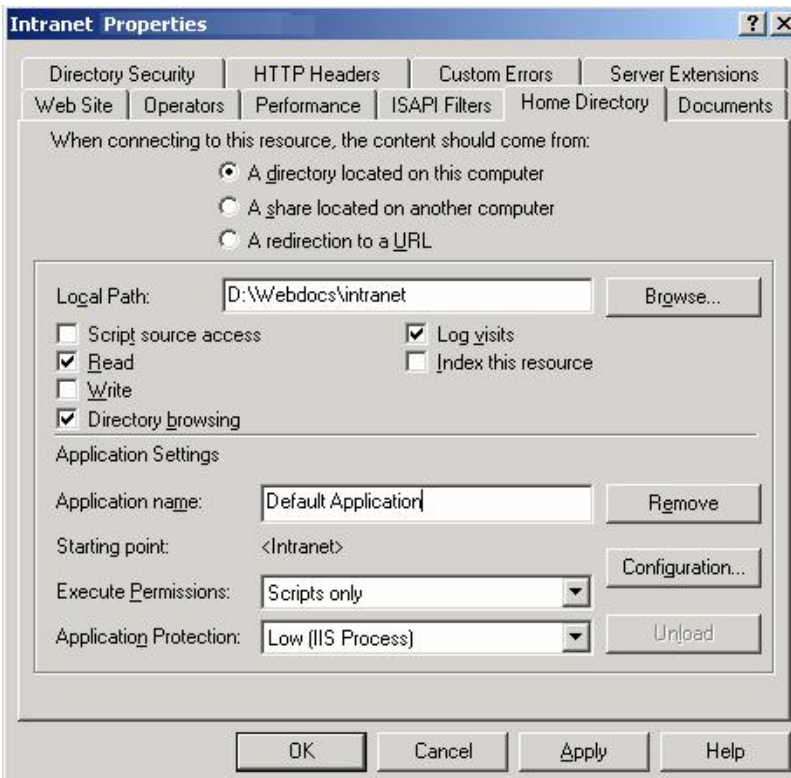
- A. SNMP will install TCP/IP counters, but these users might not even be using TCP/IP. We need to check network parameters, and those are installed via the install of the Network Monitor Agent.
- B. Actually, we won't be using SNMP here, we need to install the Network Segment Counters on the workstations that are having trouble.
- D. We don't need the counters on the server yet, we need to see what the problem is with the workstations, so

we will monitor the workstations.

F. If we use LOG View, then we will miss an opportunity when the problem occurs. We can't find out until after the fact, probably a long time after the problem occurred and disappeared. Evidence of the problem may be lost, and opportunities to troubleshoot the problem at the time of failure will also be lost.

QUESTION 65 You are the Webmaster of your company's intranet. The Intranet is hosted by a Windows NT server computer. You need to install a new server component that web developers will use to create a new service. The new component is an ISAPI-based application. You install the component in a virtual directory named Apps. You define the Read permission and enable all Execute permissions.

When the developers begin to test the new service that uses the new component, they receive an error message that states that the component could not be started. You view the properties of the intranet web site, which are shown in the exhibit.



You need to ensure that developers can use the component.

What should you do?

- A. Configure the Apps virtual directory to run at an Application Protection level of Medium
- B. Configure the Apps virtual directory to run at an application protection level of high
- C. Configure the web site application settings to enable scripts and executables
- D. Configure the web site to remove the default application

Answer: C

Explanation: The pull-down box at Execute Permissions needs to be set for executables. This includes the ISAPI and CGI applications that are usually .EXE programs. There are three options: None, Scripts Only, and Scripts and Executables. We need to set it as Scripts and Executables.

Incorrect Answers:

A. The protection is used to help control applications from stepping on each other. Changing this parameter will not affect the application ability to start, just how much the application will be isolated from other applications.

- B. The protection is used to help control applications from stepping on each other. Changing this parameter will not affect the application ability to start, just how much the application will be isolated from other applications.
- D. The default application naming does not affect the application' ability to start.

QUESTION 66 You are a Webmaster for a company that provides Internet hosting services for Internet web sites. The company is adding a new low-cost service to provide web site hosting for low-usage sites. For this service, the company plans to use a Windows NT server computer that has a dedicated T1 line. The server is expected to host approximately 50 web sites. You want to ensure that the Internet connection to the server will be sufficient to handle the anticipated number of web sites.

What should you do?

- A. Configure the default Microsoft internet information server web site to use bandwidth throttling set to 25 Kbps
- B. Configure each web site to use bandwidth throttling set to 25 Kbps
- C. Configure the default Microsoft Internet Information Server web site to use a connection limit of 50
- D. Configure each web site to use a connection limit of 50

Answer: B

Explanation: A T1 is 1.544Mbps in speed. Bandwidth Throttling comes into play when there is contention for the line. By setting a 25Kbps limit, 50x25Kbps would limit total bandwidth to 1.250Mbps, which is lightly less than a T1. In this scenario, everyone would be at least guaranteed a 25Kbps service in heavy network activity.

Incorrect Answers:

- A. This would only insure that the Default website would get service (at a minimum of 25Kbps), and that the other websites would contend for the rest of the T1 line. It would be possible that some websites would NOT get any service, since bandwidth was not reserved for them.
- C, D. It can take one user to consume ALL the bandwidth of a T1, for example, file downloads. By setting connection limits, you still haven't reserved bandwidth, and some sites could be starved. Using connection limits do help in keeping the workload limited, but no to the point where we can insure that all 50 websites will get some bandwidth.

QUESTION 67 You are the administrator of a Windows NT server network. You are configuring a shared printer on a Windows NT workstation computer named Accounting2. Accounting2 is used 24 hours a day, seven days a week. During each day, as many as four different users use Accounting2 at different times. Users of other computers will access the shared printer over the network. You want to allow users to manage and delete only their own print jobs. However, you want to enable the user who is logged on locally to accounting2 to manage and delete any print job that is sent to the printer.

What should you do?

- A. Assign the interactive group the Manage Documents permission for the printer
- B. Assign the Network group the Full control permission for the printer
- C. Assign the Authenticated users group the full control permission for the printer
- D. Assign each user who will log on to Accounting2 the Full Control permission for the printer.

Answer: A

Explanation: The group interactive is a special group. For example: Users become members of these special groups depending on the operation that they are trying to perform. For example, a user gains the Interactive group membership in their token whenever they use a computer locally. The Network group would be added to a user's token anytime that a user connects over the network to a computer. So, and interactive user is the one logged on locally, and by giving Manage Documents permissions, we get the desired result. As far as users managing only their OWN print jobs, that is the default permission, so we don't need to change anything for

that.

Incorrect Answers:

B. Giving full control to the network users violates the desired result. Everyone (except the locally logged on user) will have full rights, which is not the intention. The problem states that we want to allow users to manage and delete only their own print jobs.

C. Giving full control to the authenticated users violates the desired result. Everyone (including the locally logged on user) will have full rights, which is not the intention. The problem states that we want to allow users to manage and delete only their own print jobs.

D. First, doing it by the user is an administrative headache, since we have to keep up with each user as they are added. Then, if that user connects via the network, they are not local and we don't want them to manage other people's print jobs. Finally, this is too much rights, because above what we wanted the user to do, they can now change permissions, take ownership, and even delete the printer, extra permissions that the local logged on user should not have. These are permissions that are above what was required to do the job.

QUESTION 68 You are the administrator of a Windows NT domain. Your company recently hired a new employee named Susanne. You create a new user account in your domain that has the settings shown in the following table.

User account property	Configured As
User cannot change password	Selected
Username	Susanne
Password never expires	Selected
Account disabled	Cleared
Account locked out	Cleared
Member of	Domain users
User may log on to all workstations	Selected
Account expires	Never
Account type	Local account

You install a new Windows NT workstation computer named SusanneWS, and you join it to the domain.

When Susanne attempts to log on to this computer for the first time, she receives the following error message: The system could not log you on. Make sure your username and domain are correct, then type your password again. Letters in passwords must be typed using the correct case. Make sure that Caps Lock is not accidentally on.

You verify that Susanne typed her user name and password correctly.

What should you do so that she can log on?

A. Clear the User cannot change password checkbox.

B. Reconfigure the account Type as a Global account.

C. Clear the password Never expires check box.

D. Click the user may log on to these workstations option button, and type a computer name of SusanneWS in the first text box.

Answer: B

Explanation: This question can surely confuse you, so be aware of the accounts. Notice that the problem says you created the user account in your domain. This does not absolutely indicate that you were logged on locally to a Domain Controller. You may have been logged on locally to a member server, or even a workstation. It is common for an Administrator to install the server tools on their workstation, and run User Manager for Domains on their Windows NT 4.0 workstation. In User Manager for Domains, you get a pull down list of all the domains and the local workstation. What happened here is that the User was created on the Administrative Workstation as a local account. The account needs to be a Domain Account, created in the proper domain. But instead of saying a Domain account, they say Global. In this case Global means across all machines, which is how a Global Account works. Also, make sure you do not confuse Local/Global accounts with Local/Global

groups, which is a different concept.

Incorrect Answers:

A. Changing the password is not an issue here. If the user was in a situation where the password expired, and a paradox occurred that the user can't change password and the password needs to be changed, would prevent the user from a successful logon, but would not indicate that the password was wrong.

C. Whether the password is allowed to expire, or not, would not cause a situation where the user would get a message of a bad password, or non-existent user.

D. The default for a new user is that they can log onto any workstation. Adding this would then ONLY allow SusanneWS to be used. However, this security failure results in a different message, because it is an authorization failure, not a password failure.

QUESTION 69 You are the lead administrator of your company's Windows NT domain. The domain contains a domain controller named ServerA. ServerA also functions as your company's RAS server. You and your assistant administrator perform backups by using a user account that is a member of only the Backup Operators group in the domain.

On Friday night, an assistant administrator named Eric performs a backup on serverA. After the backup is complete, Eric chooses the Shut down the computer option when attempting to log off. Users cannot dial in to your network during the weekend.

You want to ensure that this problem does not occur again.

What should you do?

A. Remove the user account that is used for backups from the Backup Operators group, and add this user account to the Server Operators group.

B. Remove the user account that used for backups from the backup operators group. Create a new local group named Backup only in the domain. To this backup only group, add the user account that is used for backups. Assign this Backup Only group the Back up files and directories user right and the restore files and directories user right.

C. Configure the user rights policy so that the Backup operators group does not have the shut down the system user right

D. Configure the user rights policy so that the Backup operators group does not have the log on locally user right.

Answer: C

Explanation: The backup operator is an administrator account that limited permissions and rights. If the user did a shutdown, the user had the right to shutdown the system. All you need to do is take away this right, and none of the other permissions or rights will be affected.

Incorrect Answers:

A. The Server Operator would no longer be able to perform backups, and can still do a system shutdown.

You haven't prevented anything, except you prevented the backup operator from even doing its assigned tasks.

B. ServerA is a domain controller. In order to logon to the server to do the backups, the log on locally user right is required, and this scenario does not have it. Too many rights and maybe some permissions would be lost.

D. ServerA is a domain controller. In order to logon to the server to do the backups, the log on locally user right is required, otherwise the operator can't perform his assigned duties.

QUESTION 70 You are the administrator if a network that consists of a single Windows NT domain. The domain contains Windows NT server computers, Windows NT workstation computers, Windows 2000 Professional computers, and Windows 98 computers. All of the client computers are configured to authenticate user logons with the Windows NT domain. You want to create a system policy to place a new Helpdesk icon in

the Start menu of all of the client computers. You log on to your Windows NT workstation computer and create a system policy. You save this system policy in the NETLOGON shared folder on the PDC. You then log on to a Windows 98 computer and create a system policy. You save this system policy in the home directory of each Windows 98 user account. You then log on to the network from a Windows NT workstation computer and a Windows 2000 Professional computer. The new Helpdesk icon appears in the start menu on both computers. When you log on to a Windows 98 computer, the Helpdesk icon does not appear. You need to ensure that the Helpdesk icon appears in the Start menu of the Windows 98 computers.

What should you do?

- A. Log on to a Windows 2000 Professional computer, create the system policy for the Windows 98 computers, and save it in the NETLOGON shared folder on the PDC
- B. Log on to the domain, and move the Windows 98 system policy to the NETLOGON shared folder on the PDC.
- C. Log on to the domain, and replace the Windows 98 system policy file in the NETLOGON shared folder on the PDC with a copy of the Windows NT system policy.
- D. Create a profile directory for the user account of each Windows 98 user, and place a copy of the Windows 98 system policy in each profile directory.

Answer: B

Explanation: System policy for a Windows 98 system is downloaded by the client from the NETLOGON folder on the PDC.

Since the Windows 98 system does NOT authenticate with BDCs, it is not required to add the profile to the NETLOGON on the BDC controllers. However, using replication, it is a good practice to place the Windows 98 profiles on the BDC in case you need to promote that BDC to a PDC.

Incorrect Answers:

- A. System policies for Windows 98 can only be generated on a Windows 98 workstation computer.
- C. System policies for Windows 98 can only be generated on a Windows 98 workstation computer. A system policy from either Windows NT or Windows 2000 is not compatible with a Windows 98 system policy.
- D. The system policies do NOT go in the profiles, they are stored in NETLOGON folder of the PDC.

QUESTION 71 You are the administrator of a network that consists of three Windows NT domains, which are named HQ, SEATTLE, and CHICAGO. The domains are configured as a complete trust domain model. You create a shared folder named CorpInfo on a domain controller in the CHICAGO domain. You want only users who log on by using a user account from any domain to be able to access the CorpInfo shared folder.

What should you do?

- A. Assign the InterActive group permissions for the CorpInfo shared folder.
- B. Assign the Authenticated Users group permissions for the CorpInfo shared folder
- C. Assign the Everyone group permissions for the CorpInfo shared folder.
- D. Create a new local group named CorpInfo in the CHICAGO domain, and assign this group permissions for the CorpInfo shared folder. Add the Domain Guests group from each domain to the CorpInfo group.

Answer: B

Explanation: Since we have a complete trust model in effect, and we only want users who logged on using an account from any domain, we want to set the permission to authenticated users. An authenticated user is a user who signed onto the domain using a user account, and has been authenticated.

Incorrect Answers:

- A. You do not assign the interactive group for folder permissions.
- C. Everyone would include peer users from other domains, that were not authenticated in the trust model. This may allow access to users not using a user account from any of the domains.

D. Using Domain Guests could allow users to access the resource without logging onto a domain using a user account. This will usually occur in peer systems.

QUESTION 72 Five months ago, you became the administrator of an existing Windows NT domain that contains Windows NT server computers and Windows NT workstation computers. Four months ago, you configured the domain so that users are required to change their passwords every 42 days. You now discover that when users are required to change their passwords, many of the users change their password and then immediately change it back to their favourite password. You need to prevent users from doing this.

Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

- A. Use Syskey.exe on each domain controller, and click the Store Startup Key Locally option button.
- B. Use Syskey.exe on each domain controller, and click the Password Startup option button.
- C. Configure all domain controller to use Passfilt.dll
- D. Configure all client computers to use Passfilt.dll
- E. Configure password uniqueness so that the last five passwords are remembered
- F. Allow passwords to be changed after a minimum of five days

Answer: E, F

Explanation: The users change their passwords to anything, and then back to their favourite. If we set the password uniqueness to five, then the user would need to change the password 6 times to get back to their favourite. And users will do this, 1,2, 3. However, by forcing the password change to a minimum of 5 days, it would take a

minimum of 30 days to get back to the favourite password. We restrict how fast the user can change those passwords by using a minimum age requirement.

Incorrect Answers:

A, B. Syskey.exe is used to encrypt the passwords in the SAM database. It protects the data, it does not enforce any rules restricting the data.

C, D. Passfilt.dll is a utility used to enforce uniqueness of the passwords by forcing the passwords to contain combinations of Upper and Lower case letters, numeric, and special characters (a password must use 3 of those 4 categories). This only enforces the makeup of the password. If someone has a favourite password that meets those requirements, then Passfilt.dll will allow the password, and we haven't stopped anything. This restricted content, but not reuse.

QUESTION 73 You are the network administrator for a company that is located in Los Angeles. The network consists of six Windows NT domains. The domains are configured as a single master domain model. The master model is named CORP, and there are five resources domains.

The company is opening an office in London. Because of the time difference between the two offices, the London office will have its own local network administrators. These administrators will be responsible for the network and user account administration in only the London office. You will be responsible for providing backup assistance to the network administrators in London.

You want users in both offices to be able to access resources in any domain. Before you assign specific permissions for resources, you need to configure the trust relationships between the domains. You want to accomplish this task by using the smallest number of trust relationships required. You create a domain named LONDON, and now you need to configure the domain structure to accommodate the new office.

Which four actions should you take? (Each correct answer presents part of the solution. Choose four)

- A. Place all of the London servers in the LONDON domain.
- B. Place all of the London servers in the CORP domain

- C. Place the London network administrators in the Domain Admins group in the CORP domain
- D. Place the London network Administrators in the Domain Admins group in the LONDON domain
- E. Configure a one-way trust relationship so that the LONDON domain trusts the CORP domain
- F. Configure a one-way trust relationship so that the LONDON domain trusts the LONDON domain
- G. Configure two-way trust relationships between the resources domain and the LONDON domain.
- H. Configure one-way trust relationships so that each resource domain trusts the LONDON domain.

Answer: A, D, E, H

Explanation: The requirements are that there be local administrators in London, administering the LONDON domain, and no others. In order to separate administrative control in this manner, we need a separate domain (LONDON) and place those local administrators into the DOMAIN ADMINS group, since they are administrators and need the permissions. Now, we also need to have administrative backup, i.e. the CORP administrators need to also manage LONDON. Since CORP users will be managing objects in the LONDON domain (User Accounts and LONDON resources), the LONDON domain must trust the CORP domain, saying that LONDON trusts the administrative users in CORP that had logged onto CORP and were authenticated by CORP. CORP does not need to trust LONDON, since the LONDON administrators will not be administering the user accounts in CORP.

Now, we need to finally handle: "You want users in both offices to be able to access resources in any domain". Let's first see, what do we have?

CORP is already trusted by the 5 other resource domains, because this is the default Master/Resource model. In addition, by selecting answer E, by LONDON trusting CORP, the CORP users already have access to the resources in LONDON. So, CORP is covered. At this point, no one trusts LONDON, and by default only resources in LONDON can be accessed by users in LONDON. What is missing is that LONDON now needs access to the 5 original resource domains. So, we add a one-way trust such that each resource domain "trusts" the user accounts in LONDON.

Incorrect Answers:

B, C. If we add the London local administrators to CORP, and/or put the London servers into CORP, we will be unable to satisfy the separation of duties, the requirement that London local administrators can only manage LONDON.

F. You never have a domain trusting itself.

G. Well you don't do two-way trusts in Windows NT. If you want to read this as relationships that imply the two one-way trusts, then this is overkill, as having LONDON trust the resource domains is a waste, since there are no user accounts in the resource domain to trust (we know this by the single master domain model definition).

QUESTION 74 You are the network administrator for Litware, Inc. The network consists of three Windows NT domains. The domains are configured as a complete trust domain model. The domains are named HQ, RESEARCH, and MFG.

Fabrikam, Inc., is acquiring Litware, Inc. The Fabrikam, Inc., network consists of two Windows NT domains that contain Windows 2000 Server computers running in mixed mode. The two domains are named CORP and HOLDINGS. The CORP domain is the master domain and HOLDINGS is the resource domain.

You install network connections between Litware, Inc., Fabrikam, Inc. You want to perform the following tasks:

Allow the Fabrikam, Inc., users to access resources in any domain

Allow the Litware, Inc., users to access any network resources in the Litware, Inc., domain and in the HOLDINGS domain at Fabrikam, Inc.

You want to accomplish these tasks by using the smallest number of trust relationships required.

Which two actions should you take? (Each correct answer presents part of the solution. Choose two)

- A. Configure two-way trust relationships between the Litware, Inc., domains and the HOLDINGS domain
- B. Configure two-way trust relationships between the Litware, Inc., domains and the CORP domain.
- C. Configure one-way trust relationships so that the HOLDINGS domain trusts the HQ, RESEARCH, and MFG domains.
- D. Configure one-way trust relationships so that the HQ, RESEARCH, and MFG domains trust the CORP domain.
- E. Configure one-way trust relationships so that CORP domain trusts the HQ, RESEARCH, and MFG domains.
- F. Configure one-way trust relationships so that the HQ, RESEARCH, and MFG domains trust the HOLDINGS domain.

Answer: C, D

Explanation: The questioning gets confusing when they say the Windows 2000 servers are running in mixed mode. Mixed mode is used for a Windows 2000 domain, but it is clear here that we are only discussing Windows NT domains. We need to remember that in Windows NT, there are only one-way trust relationships. For example, in the case of the beginning paragraph, in order for the three domains to be in a complete trust model, two one-way trusts have to be set up between pairs of domains until a complete mesh is established. This brings about another characteristic of NT trusts, they are NOT transitive.

Now lets take a look at the Fabrikam Inc. network. It is using a Master/Resource Model. In this model, all the users are in the Master (CORP) and the resources in the resource domain (HOLDINGS), and there is at least a one-way trust where HOLDING trusts CORP, and that allows the users of CORP to use resources in HOLDINGS.

Now, let's look at the problem:

Allow the Fabrikam, Inc., users to access resources in any domain: Well, as we said, Fabrikam, Inc users are assumed to already have access to HOLDINGS, because it is a Master/Resource configuration already. So, we need to add three (3) one-way trusts, such that the resources in each of the Liteware domains trust CORP. Why? Every resource domain must trust the user accounts in CORP.

Allow the Litware, Inc., users to access any network resources in the Litware, Inc., domain and in the HOLDINGS domain at Fabrikam, Inc.: Well, in this case, because of the complete trust model, Liteware users already have access to any resource in the Liteware network. All we need to do is add a one-way trust between each Liteware domain and HOLDINGS, where HOLDINGS trusts the Liteware domains. Why? Because any of the three Liteware domains may contain user accounts, and HOLDINGS has to trust each domain that might have user accounts defined.

Incorrect Answers:

- A, B. Keep it easy, Windows NT does not have nor support two-way trusts, these are easily discarded.
- E. The CORP, HQ, RESEARCH and MFG domains all contain user accounts, this trust relationship does not answer the problem. The resources of Fabrikam are in HOLDINGS. HQ, RESEARCH and MFG must trust CORP for the CORP user accounts to be able to use those resources. When a domain A "trusts" another domain B, it says that A trusts the user accounts from the domain B, and B is the trusted domain.
- F. This is also reversed. HOLDINGS has the resources, and HQ, RESEARCH and MFG have the accounts, so HOLDINGS should be the trusting domain.

QUESTION 75 You are the administrator of a Windows NT domain named CORP. the CORP domain is configured as shown in the exhibit. Click the exhibit button.

ServerA is a new Windows NT server computer. You are installing routing and remote access service on serverA. You also install a 12-port analog 56-Kbps modem card and configure RRAS to use the modem card for incoming analog connections. You configure RRAS to use a static pool of IP addresses for client computers

when they use a dial-up connection. The static pool uses the IP address range of 10.11.10.201 to 10.11.10.220. The network subnet mask is 255.255.0.0

Remote users report that they cannot access shared resources when they dial in to the network. You want remote users to be able to access all shared resources when they dial in to the network.

What should you do?

- A. Configure RRAS on ServerA to use DHCP to obtain IP addresses for remote users
- B. Configure TCP/IP on ServerA to use DHCP for its Ethernet network adapter
- C. Create a computer account in the CORP domain for all computers that are used by remote users
- D. Configure the computers that connect to ServerA to use 10.10.20.9 as the default gateway

Answer: A

Explanation: The remote users are able to connect to the network, but they are not able to access resources on it. One probable cause of this problem is that the IP address range, 10.11.10.201 to 10.11.10.220 and subnet mask 255.255.0.0, is not the same used at the network. This would make the clients able to gain remote access but they would not be able to connect to any resources. This problem can be overcome by configuring the RRAS server to use DHCP to lease IP addresses for remote users. The remote clients would get the same IP configuration as the local clients.

Incorrect Answers:

B: Configuring the TCP/IP properties on the RAS server to use DHCP would not help the remote clients.

C: The remote clients are able to connect to the network. There is no need to create computer accounts.

D: An incorrect default gateway setting of the remote clients would not prevent them from accessing resources on the same subnet as the RAS server. It would prevent them from accessing resources on other subnets on the network though.