

GlobalTcert

GLOBALTCERT.COM
Your gateway to success



Demo
STUDY GUIDE

© Copy Right 1998-2005 GlobalTcert LLC. All Rights Reserved.

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