



[www.chinatag.com](http://www.chinatag.com)

**CHINATAG**

70-214

Implementing and Administering Security in  
a Microsoft Windows 2000 Network

Q&A

DEMO Version

Copyright (c) 2003 Chinatag LLC. All rights reserved.

## **Important Note Please Read Carefully**

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are not encrypted. Feel free to distribute copies among your friends and let them know Chinatag website. Our IT certification products start at only **\$7.99**.

## **Study Tips**

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

## **Latest Version**

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 180 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to [feedback@chinatag.com](mailto:feedback@chinatag.com).

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team  
Chinatag LLC.

**QUESTION NO: 1**

You are the network administrator for Chinatag. The network consists of a Windows 2000 Active Directory domain. The network contains two Windows 2000 Server computers configured as domain controllers and 1,500 Windows 2000 Professional client computers.

Chinatag has three departments: research, sales, and operations. Each department has a separate organizational unit (OU) in the domain that contains all user and group accounts for that department. Chinatag policy prevents configuration of Block Policy inheritance on the OUs.

You scan the domain controllers with the Microsoft Baseline Security Analyzer (MBSA) and receive the following message:

Computer is running with RestrictAnonymous = 0.  
This level prevents basic enumeration of user accounts, account policies, and system information.  
Set RestrictAnonymous = 2 to ensure maximum security.

Your manager tells you to use a security template to apply the MBSA-recommended setting to the domain controllers. You are not allowed to modify the configuration of other computers on the domain. You create a new security template based on the existing configuration of your domain controllers.

**What should you do next?**

- A. In the template, set the **Additional Restrictions for Anonymous Connections** policy to **No access without explicit anonymous permission**.  
Import this template into the Domain Controller Security Policy.
- B. In the template, configure the Workstation service for **Manual** startup and deny **Write** access to the Anonymous Logon group.  
Import this template in the Domain Controller Security Policy.
- C. In the template, set the **Additional Restrictions for Anonymous Connections** policy to **Do not allow enumeration of SAM accounts and shares**.  
Import this template into the Domain Security Policy.
- D. In the template, configure the Workstation service for **Manual** startup and deny **Read** access to the Anonymous Logon group.  
Import this template into the Domain Security Policy.

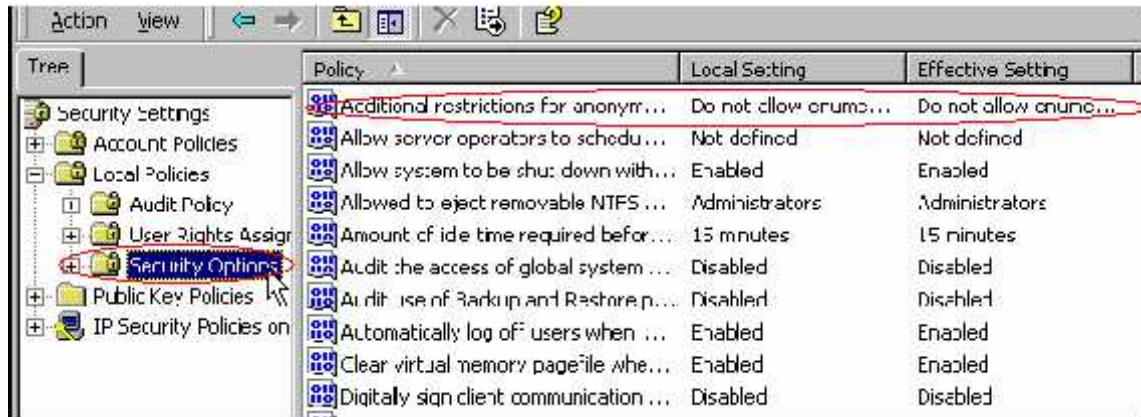
**Answer: A**

**Explanation:** MBSA shows that the computer runs with RestrictAnonymous=0. The RestrictAnonymous numbers correspond to the following settings:

0 None. Rely on default permissions

1 Do not allow enumeration of SAM accounts and names 2  
 No access without explicit anonymous permissions

The RestrictAnonymous=0 setting is a security risk and it allow hackers to probe machine from the Internet for a list of the Users (SAM Accounts) and Shares (Shared folders and Printers). We can change this setting to 2, which is the recommendation from MBSA, y Enabling "Additional restrictions for anonymous connections" (see picture)..



And then set this policy to **No access without explicit anonymous permission**.

**Note:** Microsoft Baseline Security Analyzer (MBSA) scans for missing hotfixes and vulnerabilities in Windows, IIS, SQL Server, Internet Explorer, and MS Office.

#### Reference:

How to Use the RestrictAnonymous Registry Value in Windows 2000, Microsoft Knowledge Base Article - Q246261

Microsoft Baseline Security Analyzer (MBSA) Version 1.0 Is Available. Microsoft Knowledge Base Article - Q320454

#### Incorrect Answers

**B, D:** Manual startup of the workstation service would be awkward for the users. They would not be able to browse the network without this service.

**C:** This option would improve security, but security would be even better even we choose the

**No access without explicit anonymous permission**. instead of **Do not allow enumeration of SAM accounts and shares**. This is also the recommendation of MBSA.

#### QUESTION NO: 2

You are the administrator of a Windows 2000 network. The network consists of a Windows 2000 Active Directory domain named chinatag.com. The domain contains Windows 2000 Server computers and Windows 2000 Professional client computers. The client computers are in an organizational unit (OU) named Clients. You use Group Policy objects (GPOs) to administer the configuration of the Windows 2000 Professional client computers.

To increase the security of the client computers, you want to ensure that the configuration settings in the client computers are always corrected whenever a user changes these settings manually.

**What should you do?**

- A. Configure the Task Scheduler on the client computers to periodically run the **secedit /refreshpolicy machine\_policy** and the **secedit /refreshpolicy user\_policy** commands.
- B. Configure the Default Domain Group Policy object (GPO) to enable **Group Policy refresh interval for computers** settings and a **Group Policy refresh interval for users** setting.
- C. Create a GPO and link it to the Domain Controllers OU.  
Configure the GPO to enable the **User Group Policy loopback processing mode** in merge mode.
- D. Create a GPO and link it to the Clients OU.  
Configure the GPO to enable the settings to process policies even if the GPOs have not changed.
- E. Create a GPO and link it to the Clients OU.  
Configure the GPO to disable the **Enforce Show Policies Only** setting.

**Answer: D?**

**Explanation:**

**Reference:** HOW TO: How to Modify the Default Group Policy Refresh Interval, Microsoft Knowledge Base Article - Q203607

**Incorrect Answers**

- A:** This is an awkward indirect way of applying security templates.
- B:** The **Group Policy refresh interval for computers** is used to modify the refresh and offset intervals settings. Is not used to enable a setting.
- C:** Loopback processing mode is used to establish machine-specific settings, so that the computer's client settings take precedence. It does not fit in this scenario.
- E:** The **Enforce Show Policies Only** policy prevents administrators from viewing or using Group Policy preferences. If we disable it administrators will be able to view and use Group Policy preferences. This does not address the problem at hand.

**QUESTION NO: 3**

You are the network administrator for Chinatag. The network consists of a Windows 2000 Active Directory domain. The domain includes two organizational units (OU) named Manufacturing and Sales. The network contains two Windows 2000 Server computers configured as domain controllers and 1,500 Windows 2000 Professional client computers. All user accounts are located in the Manufacturing OU and Sales OU.

Your manager wants you to ensure that the domain Account Policies are no less secure than the Account Policies in the Securedc.inf template. You run the Security Configuration and Analysis console on a network domain controller, and you use Securedc.inf to analyze the computer.

You review the Password Policy portion of the analysis, which the following table shows.

Policy	Database setting	Computer setting
Enforce Password history	24 passwords remembered	1 password remembered
Maximum password age	42 days	0
Minimum password age	2 days	4 days
Minimum password length	8 characters	8 characters
Password must meet complexity requirements	Enables	Enabled
Store password using reversible encryption	Disabled	Enabled

Your manager does not want to reduce the existing security level. You must increase the security of the Password Policy in all areas in which it is less restrictive than the Securedc.inf template.

**What should you do?**

- A. Import Securedc.inf template into the Domain Security Policy.
- B. Create a new Group Policy object (GPO) and link it to the Sales and Manufacturing OUs.  
Import the Securedc.inf template into the new GPO.
- C. Create a new security template.  
Set **Enforce password history** to **24 passwords**, **Maximum password age** to **42 days**, and **Minimum password age** to **4 days**.  
Import the new template to the Domain Security Policy.
- D. Create a new Group Policy object (GPO) and link it to the Sales and Manufacturing OUs.  
Create a new security template.  
Set **Enforce password history** to **24 passwords**, **Maximum password age** to **0**, and **Minimum password age** to **4 days**.  
Import the new template to the new GPO.

**Answer: C**

**Explanation:** We must create a new security template that is at least restrictive as the current settings. This ensures that security only improves and not decreases.

**Incorrect Answers**

**A:** When merging security templates the last one imported, Securedc.inf, takes precedence

when there is contention. Importing the Securedc.inf security templates would therefore decrease **Minimum password age** and disable **Store password using reversible encryption**. This is not acceptable.

**B, D:** Windows 2000 only allows one domain account policy: the account policy applied to the root domain of the domain tree.

**QUESTION NO: 4**

You are the network administrator for Chinatag. The network consists of a Windows 2000 Active Directory domain. The network contains two Windows 2000 Server computers configured as domain controllers, 100 Windows 2000 Professional client computers, and 100 Windows 98 client computers, All Windows 98 Second Edition client computers have the Microsoft Directory Services Client installed and are configured with the appropriate LMCompatibilityLevel registry value.

Chinatag has three departments: research, sales, and operations. Each department has a separate organizational unit (OU) in the domain that contains all user and group accounts for that department.

The written security policy for Chinatag requires that domain controllers authenticate user logons only by using the most secure Microsoft authentication method available to all clients on the network. You review the Security Options portion of the security template for the domain. The following table shows the relevant Security Options settings in the template.

<b>Policy</b>	<b>Computer settings</b>
Lan Manager Authentication Level	Send NTLM response only
Message text for users attempting to log on	Not defined
Message title for users attempting to Log on	Not defined
Number of previous logons to cache (in case domain controllers is not available)	1 logons

You must ensure that no Windows 98 client computer can authenticate with the domain controller by using anything less than the most secure authentication method available.

**What should you do?**

- A. Configure the **Lan Manager Authentication Level** on the security template to **Not defined**.  
Import the template into the Domain Controllers Security Policy.
- B. Configure the **Lan Manager Authentication Level** on the security template to **Send NTLMv2 response only/refuse LM & NTLM**.  
Import the template into the Domain Security Policy.
- C. Configure the Default Domain Policy Group Policy object (GPO) to enable the **Digitally encrypt secure channel data (when possible)** setting in the Secure Options policy.
- D. Configure the Default Domain Controllers Policy Group Policy object (GPO) to enable the **Digitally encrypt or sign secure channel data (always)** setting in the Secure Options policy.

**Answer: B**

**Explanation:** NTLM 2 is the most secure LAN Manager authentication level. NTLM2 support to Windows 95 and Windows 98 can be added by installing the Directory Services Client from the Windows 2000 CD-ROM. This step has been taken in this scenario. By enforcing use of NTLMv2 we would ensure that the most secure authentication method is available.

**Note:** The **LAN Manager authentication level** determines which challenge/response authentication protocol is used for network logons. This choice affects the level of authentication protocol used by clients, the level of session security negotiated, and the level of authentication accepted by servers. The NTLM authentication package in Windows 2000 supports three methods of challenge/response authentication: LAN Manager (LM) which is least secure, NTLM version 1, NTLM version 2 which is the most secure.

By default, all three challenge/response mechanisms are enabled. You can disable authentication using weaker variants by setting the LAN Manager authentication level security option in local security policy for the computer.

**Reference:** How to Enable NTLM 2 Authentication for Windows 95/98/2000 and NT, Microsoft Knowledge Base Article - Q239869

#### **Incorrect Answers**

**A:** A **Lan Manager Authentication Level of Not defined** would enable LAN Manager (LM) authentication which is least secure authentication method..

**C:** The **Digitally encrypt secure channel data (when possible)** setting is enabled, it ensures that all secure channel traffic is encrypted if the partner domain controller is also capable of encrypting all secure channel traffic. However, it allows unencrypted data. Furthermore it only applies to communication between domain controllers.

**D:** The **Digitally encrypt or sign secure channel data (always)** setting determines whether a secure channel can be established with a domain controller that is not capable of signing or encrypting all secure channel traffic. If this setting is enabled, a secure channel cannot be established with any domain controller that cannot sign or encrypt all secure channel data. It only applies to communication between domain controllers and is therefore useless in this scenario.

#### **QUESTION NO: 5**

You are the network administrator for Chinatag. The network consists of a Windows 2000 Active Directory domain. The domain includes two Windows 2000 Server computers running as domain controllers, five Windows 2000 Server computers running as file servers, and 500 Windows 2000 Professional client computers.

All the domain controllers are in the Domain\_Computers organizational unit (OU). The file servers are in an OU named Servers. The client computers are in an OU named Clients. The Domain\_Computers OU is the parent OU to both the Servers OU and the Clients OU.

The written security policy for Chinatag requires that you track attempts to log on to a computer that use a local user accounts.

**What should you do?**

- A. Create a security template that enables the **Audit Account Logon Events** policy for successful and failed attempts.  
Create a Group Policy object (GPO) and link it to the domain.  
Import the template into the new GPO.
- B. Create a security template that enables the **Audit Account Logon Events** policy for successful and failed attempts.  
Create a Group Policy object (GPO) and link it to the Servers OU.  
Import the template into the new GPO.
- C. Create a security template that enables the **Audit Logon Events** policy for successful and failed attempts.  
Create a Group Policy object (GPO) and link it to the Clients OU.  
Import the template into the new GPO.
- D. Create a security template that enables the **Audit Logon Events** policy for successful and failed attempts.  
Create a Group Policy object (GPO) and link it to the Domain\_Computers OU.  
Import the template to the new GPO.

**Answer: D**

**Explanation:** A **Logon event** occurs when a user logged on or logged off, or a user made or canceled a network connection to the computer. This includes attempts to log on a computer with a local user account. By linking the appropriately configured GPO to the Domain\_Computers OU, it will be applied to both child OUs; the Servers OU and the Clients OU. This ensures that all logon attempts on computers with local accounts are audited.

**Reference:** HOW TO: Monitor for Unauthorized User Access in Windows 2000, Microsoft Knowledge Base Article - Q300958

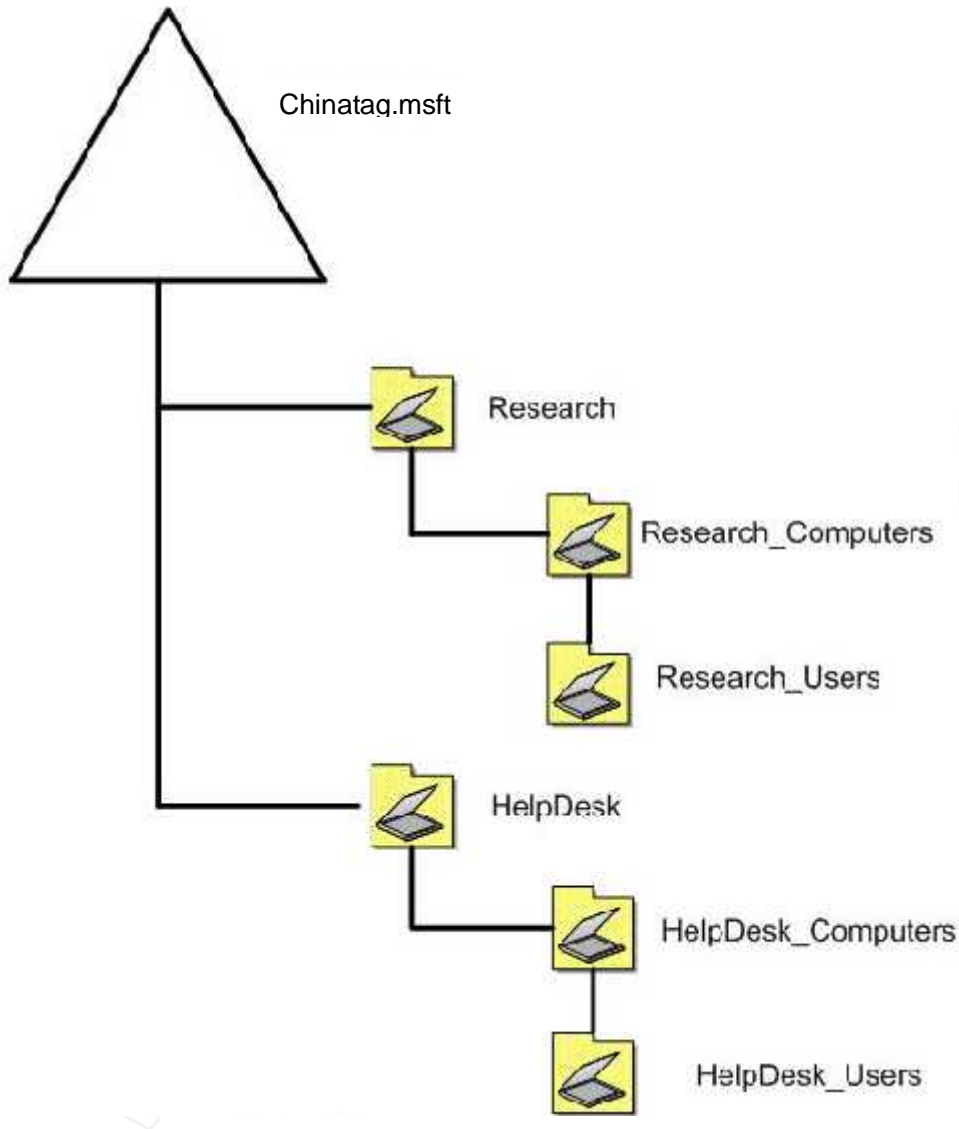
**Incorrect Answers**

- A:** An **Account Logon Event** occurs when a domain controller received a request to validate a user account. However, we want to audit local login attempts, not domain logon attempts.
- B:** Client computers also have local account. The GPO must be applied to them as well.
- C:** Member servers also have local account. The GPO must be applied to them as well.

**QUESTION NO: 6**

You are the network administrator for Chinatag. The network consists of a Windows 2000 Active Directory domain. The domain contains two Windows 2000 domain controllers and 500 Windows Professional computers.

The relevant portion of the Active Directory hierarchy is shown in the exhibit.



The user accounts for all employees in the Technical Support department are located in the HelpDesk\_Users organizational unit (OU). The client computer accounts for these employees' computers are located in the HelpDesk\_Computers OU. All other user accounts are located in the Research\_Users OU. All other client computer accounts are located in the Research\_Computers OU.

You create a Group Policy object (GPO) named GPO1 and link it to the Research\_Computers OU. You configure the GPO1 as shown in the following table.

Policy or Setting	Status
Do not display last user name on logon screen	Enabled
Disable Computer Configuration Settings	Selected
Disable User Configuration Settings	Cleared

Another administrator moves a user account named Tess to the Research\_Computers OU. You notice that Tess's computer displays another user's name in the logon dialog

box. You need to ensure that the name of the last user to log on does not appear in the logon dialog box when Tess logs on to her computer.

**What should you do?**

- A. Move Tess's user account to the Research\_Users OU.
- B. Clear the **Disable Computer Configuration Settings** check box in GPO1.
- C. Disable the **Do not display last user name in logon screen** policy in GPO1.
- D. Run the **secedit /refreshpolicy user\_policy /enforce** command on Maria's client computer.

**Answer: B**

**Explanation:** After you disable the Computer Configuration settings in a Group Policy object, by selecting **Disable Computer Configuration Settings**, the computers configuration no longer affect. This is the reason the **Do not display last user name on logon screen** policy is not used. We must therefore clear the **Disable Computer Configuration Settings** setting.

**Reference:**

HOW TO: Administer GPO Properties in Windows 2000, Microsoft Knowledge Base Article - Q322176

Using Secedit.exe to Force Group Policy to Be Applied Again, Microsoft Knowledge Base Article - Q227448

**Incorrect Answers**

**A:** Moving Maria's user account is not necessary. We only need to adjust the GPO.

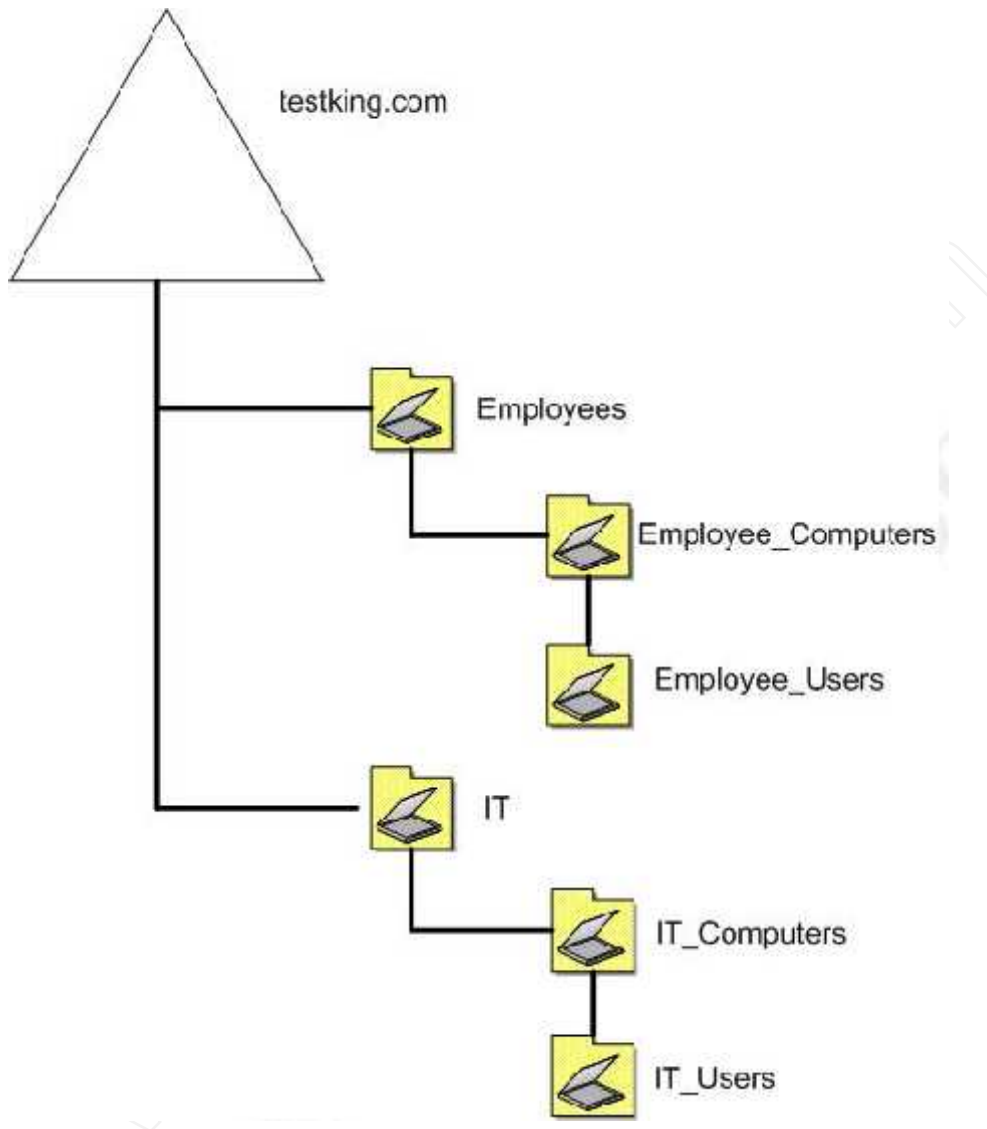
**C:** The **Do not display last user name in logon screen** is already correctly configured in GPO1. We should not disable this policy.

**D:** The GPO is already applied, it must be reconfigured however.

**QUESTION NO: 7**

You are the network administrator for Testking. The network consists of a Windows 2000 Active Directory domain chinatag.com. The domain contains Windows 2000 Server computers and Windows 2000 Professional computers. All domain controllers run Windows 2000 Server.

The relevant portion of the Active Directory hierarchy is shown in the exhibit.



The written security policy for Chinatag requires that only network administrators have administrative capabilities on the domain controllers and member servers in the domain. An administrator's user account must not have administrative capabilities on any client computer in the domain, including the administrator's own client computer.

A Group Policy object (GPO) named `Secure_lockdown` is linked to the `IT_Users` OU and the `Employee_Users` OU. The `Secure_lockdown` GPO removes many Start menu options and does not give the users access to Control Panel utilities. Administrators report that they cannot view all Start menu options when they log on to their client computers by using their domain user accounts.

You need to ensure that the administrators have access to all Start menu options and Control Panel utilities on their client computers but not on other client computers in Chinatag.

**What should you do?**

- A. Create a group named IT\_staff.  
Add each administrator's user account to the IT\_staff group.  
In the Default Domain Policy GPO, add the Administrators group under the **Restricted Groups** policy.  
Add the IT\_staff group to the member list in the Administrators group.
- B. Create a group named IT\_staff.  
Add each administrator's user account to the IT\_staff group.  
Run the Delegation of Control wizard for the IT\_Computers OU.  
Grant the IT\_staff group **Full Control** permission for the Computer objects.
- C. Create a GPO and link it to the IT\_Users OU.  
In the computer configuration section of the GPO, set the loopback processing policy to **Replace**.  
In the user configuration section of the GPO, configure **Start** menu options and Control Panel utilities to be accessible.
- D. Create a GPO and link it to the IT\_Computers OU.  
In the computer configuration section of the GPO, set the loopback processing policy to **Replace**.  
In the user configuration section, configure **Start** menu options and Control Panel utilities to be accessible.

**Answer: D**

**Explanation:** Normally Group Policies apply to the user or computer in a manner that depends on where both the user and the computer objects are located in Active Directory. However, in some cases, users may need policy applied to them based on the location of the computer object alone. You can use the Group Policy loopback feature to apply Group Policy Objects (GPOs) that depend only on which computer the user logs on to.

In this scenario we want to apply special options, the availability of the **Start** menu options and Control Panel utilities, for the Administrators on the IT computers.

**Reference:**

Loopback Processing of Group Policy, Microsoft Knowledge Base Article - Q231287  
Description of Group Policy Restricted Groups, Microsoft Knowledge Base Article - Q279301

**Incorrect Answers**

- A:** The **Restricted Groups** policy is used to control the members of the Administrators group. This does not address the problem of this scenario.
- B:** This would give the administrators full administrative to the computers in the IT\_Computers OU. However, this is not related to the requirements of this scenario.
- C:** **Loopback Processing** is applied on computers, not on users.

**QUESTION NO: 8**

You are the network administrator for Chinatag. The network consists of a Windows 2000 Active Directory domain. The domain contains a Windows 2000 Server computer

named ChinatagSrv. ChinatagSrv runs Microsoft SQL Server 2000 and contains databases that are used by all company employees. ChinatagSrv is configured as shown in the following table.

Configuration option	Parameter
Server role	Domain member server
SQL Authentication mode	Mixed mode
MSSQLServer service account	LocalSystem
SQL system administrator account name	sa SQL
system administrator account password	password

ChinatagSrv is configured to use domain groups as login accounts. Company users access ChinatagSrv by means of membership in the appropriate domain group.

The written security policy for Chinatag prohibits the use of SQL Server login accounts on ChinatagSrv. The written policy also prohibits any user from accessing ChinatagSrv by means of the sa login account.

You need to ensure that ChinatagSrv complies with the written policy, while continuing to allow access to authorized users.

**Which action or actions should you take? (Choose all that apply)**

- A. Configure ChinatagSrv to use Windows authentication.
- B. Configure ChinatagSrv as a member of a workgroup.
- C. Configure the MSSQLServer service in ChinatagSrv to use the local Administrator account.
- D. Configure the MSSQLServer service on ChinatagSrv to use the local non-administrative accounts.

**Answer: A, C**

**Explanation:**

**A:** By changing SQL Authentication mode from Mixed Mode to Windows Authentication mode sql logins, including the sa login, could not be used to access the SQL Server computer.

**C:** As Chinatag1 is a Domain member server we should use the local Administrator account, not the LocalSystem, account for the MSSQLServer service.

**Reference:** SQL Server Books Online, Authentication Modes

**Incorrect Answers**

**B:** The SQL Server computer is already a member of the domain. We should not make it a member of a workgroup.

**D:** ChinatagSrv needs local administrative rights and permissions.

**QUESTION NO: 9**

You are the network administrator for Chinatag. The network consists of a Windows 2000 Active directory domain. The domain contains a Windows 2000 Server computer named Chinatag1 that is running Microsoft SQL Server. The domain also contains an organizational unit (OU) named TestK. Chinatag is the TestK OU. The written security policy for Chinatag requires that you create all Group Policy objects (GPOs) for the domain.

The administrator for the TestK OU is named Tess. Tess is responsible for the user accounts and computer accounts in the OU. Tess submits a list of configurations that he wants to be applied to Chinatag in the TestK OU by means of a GPO. You create a GPO that complies with Tess's request.

You want to give Tess the ability to link the GPO to the TestK OU, but you need to ensure that Tess cannot create GPOs.

**What should you do?**

- A. Add Tess's user account to the Group Policy Creator Owners group.
- B. Run the Delegation of Control wizard on the TestK OU and assign Tess's user account the **Manage Group Policy links** task.
- C. Move Tess's user account to the North OU.
- D. Configure the permissions on the GPO so that Tess's account has **Read** and **Apply Group Policy** permissions.

**Answer: B**

**Explanation:** The Manage Group Policy links common task common task assigns the delegate(s) the permission to edit, add or delete Group Policy links of the selected Organizational Unit. We use the Delegation of Control wizard to assign the appropriate permissions to Bruno.

**Reference:** Step-by-Step Guide to Using the Delegation of Control Wizard HOW TO: Delegate Authority for Editing a Group Policy Object (GPO), Microsoft Knowledge Base Article - Q221577

**Incorrect Answers**

- A:** As a member of the Group Policy Creator Owners Bruno would be able to create GPOs.
- C:** Moving the user account to the OU would not automatically give the user account any permissions or rights.
- D:** Read and Apply Group Policy permissions would ensure that GPOs in the OU would apply to Bruno. However, it would allow Bruno to link GPOs to the OU.

**QUESTION NO: 10**

You are the network administrator for Chinatag International. The network consists of a Windows 2000 Active Directory domain. The domain contains five Windows 2000 Server domain controllers and 20 Windows 2000 Professional computers. The computer

accounts for all client computers are contained in an organizational unit (OU) named Chinatag.

Four Group Policy objects (GPOs) are linked to the Chinatag OU. The Chinatag OU properties are configured as shown in the following exhibit.



The administrator of the Chinatag OU customizes each GPO by using several settings and a different security template, as shown in the following table.

Group Policy object	Policy	Policy setting
GPO A	Maximum security log size	8,000 KB
GPO B	Maximum security log size	20,032 KB
GPO C	Maximum security log size	6,016 KB
GPO D	Maximum security log size	8,000 KB

On average, the security logs increase by 1,000 KB per day. When you inspect the logs on one of the desktops, you find that approximately eight days of security logs are being retained. You want to retain approximately 20 days of security log settings.

**What should you do?**

- A. Make GPO B the highest in the GPO list.
- B. Make GPO B the lowest in the GPO list.
- C. Create a new domain security group and add the users of the desktops to the new group.  
Grant the security group **Read** and **Apply Group Policy** permissions on GPO B.
- D. Create a new domain security group and add the desktop computers to the new group. Grant the security group **Read** and **Apply Group Policy** permissions on GPO B.

**Answer: B**

**Explanation:** The last GPO applied overrides the earlier GPOs whenever there is a conflict between them. Currently the GPOs are applied in the following order: GPO A, GPO B, GPO C, GPO D. We need to move GPO B lowest in the GPO list to ensure GPO B's policy setting is applied.

**Incorrect Answers**