

GlobalTcert

GLOBALTCERT.COM
Your gateway to success



Demo
STUDY GUIDE

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

QUESTION 1

You are the network administrator for GlobalitcerT. The network consists of a Windows 2000 Active Directory domain named GlobalitcerT.com.

You have deployed a new Windows 2000 Server computer as a Web server in the perimeter network (also known as the DMZ). The Web server is not a member of GlobalitcerT.com. A firewall between the network and the DMZ is configured to allow only HTTP traffic to be sent from the DMZ to the private network.

Your Web server administrator creates a security template named Webserver.inf that defines the default security settings required for the Web server. The security template settings must be enforced at the Web server and applied at regular intervals.

What should you do?

A. Make the Web server a member of the GlobalitcerT.com domain and place the Web server computer account into a new organizational unit (OU).

Import the Webserver.inf security template to the Default Domain Policy.

B. Create a batch file that applies the security template by using the `secedit /configure /cfg Webserver.inf /db web.sdb` command.

In Scheduled Tasks, create a new task to run the batch file daily.

C. Apply the security template using the Security Configuration and Analysis console on the Web server.

Create a batch file that updates the security policy of the Web server by using the `secedit /refreshpolicy machine_policy /enforce` command.

In Scheduled Tasks, create a new task to run the batch file daily.

D. Import the Webserver.inf security template to the Local Computer policy of the Web server.

Create a batch file that updates the security policy of the Web server by using the `secedit /refreshpolicy machine_policy /enforce` command.

In Scheduled Tasks, create a new task to run the batch file daily.

Answer: C

Explanation:

We apply the security template using the Security Configuration and Analysis console. We then update the security policy at regular intervals using a scheduled task.

Incorrect Answers

A: We do not want to apply the Webserver.inf to all computers in the domain.

B: We do repeatedly have to apply the security template.

D: The initial template applied to a computer is called the Local Computer Policy. It is not a good practice to change this template.

QUESTION 2

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

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

The user accounts for all administrators are located in the IT_Users organizational unit (OU). All other user accounts are located in the Employee_Users OU. The client computer accounts for the administrators' computers are located in the IT_Computers OU. All other client computer accounts are located in the Employee_Computers OU. You company employs 10 security auditors to ensure that servers and client computers comply with the written security policy of GlobalitcerT . You create a domain security group named Security_Audit. You add the computer accounts for each security auditor to this group.

You create several Group Policy objects (GPOs) and link them to the Employees OU. The GPOs configure security settings to enforce the written policy. The priority and configuration of each GPO are shown in the following table.

GPO name	Policy	Setting	Object with Read and Apply Group Policy Permissions	Priority	No Override
GPO1	Audit object access	Success and Failure	Authenticated Users Security_Audit	1	
GPO2	Audit logon events	Failure	Security_Audit	2	

GPO3	Audit account logon events	Success	Authenticated Users Security_Audit	3	X
------	----------------------------	---------	---------------------------------------	---	---

You discover that the Security logs on many client computers are full of successful object access events from the users of the client computers. You do not want users to be audited when they access files on their own computers. However, you want the security auditors to be audited when they access any file on any client computer.

What should you do?

- A. Clear the No Override check box in GPO3.
- B. Remove the Authenticated Users group from the DACL for GPO1.
- C. Configure the policy settings for GPO3 so that success and failure events are audited.
- D. Configure the DACL for GPO1 so that the Authenticated Users group has Deny - Apply Group Policy permission.

Answer: B

Explanation:

By removing the Authenticated Users group from the DACL of GPO1, only members of the Security_Audit group would be audited for Object Access.

Incorrect Answers

A, C: GPO1 would still be applied, and object Access by the Authenticated Users group would still be audited.

D: The auditors, like all users, belong to the Authenticated Users group. They would also be receive Deny - Apply Group Policy permission, and they would not be audited contrary to the requirements in this scenario.

QUESTION 3

You are the network administrator for GlobalitcerT . The network consists if a Windows 2000 Active Directory domain. The domain contains five Windows 2000 Server domain controllers and 50 Windows NT Workstation 4.0 computers.

You perform a clean installation of Windows 2000 Professional on four client computers. You do not install Internet Information Services (IIS) on these computers.

The written security policy for GlobalitcerT allows Windows 2000 Professional users to install and run IIS. Every computer running IIS must be configured to meet the written policy before the computer can be connected to GlobalitcerT network.

You want to ensure that the written policy for IIS is enforced automatically if IIS is installed on a Windows 2000 Professional computer.

What should you do before the user receive their computers?

- A. On each Windows 2000 Professional computer, modify the Ocfilesw.inf security template to comply with the written policy.