

GlobalTcert.com

GLOBALTCERT.COM
Your gateway to success



Demo
STUDY GUIDE

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

B. Create a startup script that adds the Domain Users group to the local Power Users group when the client computer starts.

Link the startup script to the Workstation OU.

C. Create a new Group Policy object (GPO) named GPO1.

Configure the Restricted Groups option in GPO1 to add the Domain Users group to the Power Users group.

Link GPO1 to the Workstation OU.

D. Create a new Group Policy object (GPO) named GPO1.

Configure the Restricted Groups option in GPO1 to add the Domain Users group to the Power Users group.

Link GPO1 to the domain.

Answer: C

Explanation: We need to move all users to the Power users group. We can do this by using the Restricted Groups option of a GPO to add the Domain Users group to the Power Users group. Restricted Groups ensures that group memberships are set as specified. Groups and users not specified in Restricted Groups are removed from the group. In addition, the reverse membership configuration option ensures that each restricted group is a member of only those groups specified in the Member Of column. This GPO must be linked to all client computers as users must not have any administrative rights to member servers or domain controllers in the domain. The client computers are in the Workstations OU.

Incorrect Answers:

A, B: Using the Restricted Groups option would be a better solution than using logon scripts or startup scripts.

D: We should link the GPO the Workstations OU, not the domain as it should only be applied to client computers and not server computers. Linking the GPO to the domain will result in the GPO being applied to client computers as well as to server computers.

Reference:

Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-Paced Training Kit (Exam 70-294); Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, pp. 10-40 to 10-41, 13-6 to 13-7

QUESTION 379

You are the network administrator for GlobalitcerT .com. The network consists of a single Active Directory domain named GlobalitcerT .com. All servers that are not domain controllers are located in an organizational unit (OU) named Servers.

The security department is responsible for defining security requirements for servers. You are responsible for configuring GlobalitcerT 's servers. The security department provides you with security settings that you must apply to new and existing servers that are not domain controllers. You configure a Windows Server 2003 computer named GlobalitcerT 1 with these settings.

You need to apply the security settings in compliance with the security department's requirements.

What should you do?

A. Export the security settings for GlobalitcerT 1.

Import the settings to a Group Policy object (GPO) linked to the Servers OU.

B. Create a script by running the netsh dump command on GlobalitcerT 1.

Create a Group Policy object (GPO), link to the GPO to the Servers OU, and configure the GPO to

apply the script as a startup script.

C. Configure Synchronization Manager on GlobalitcerT 1 to perform a synchronization task daily. D. Export the security settings for GlobalitcerT 1.

Configure File Replication service (FRS) to copy the .ini file to the systemroot on each server.

Answer: A

Explanation: You need to apply the settings to all servers that are not domain controllers. All these servers are in the Servers OU and you have applied the security settings to GlobalitcerT 1. All you need to do now is export the

settings to a custom template and import to a GPO that is linked to the Servers OU.

Incorrect Answers:

B: The netsh dump command dumps the network configuration to a file, not the security settings.

C: We need to apply the security settings to the other servers. This can't be accomplished by synchronizing.

D: Copying the exported file to the systemroot of each server will not apply the settings to the server. We need to apply it through a GPO.

Reference:

Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-Paced Training Kit (Exam 70-294); Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, pp. 10-40 to 10-41, 13-57 to 13-62

QUESTION 380

You are the network administrator for GlobalitcerT .com. The network consists of a single Active Directory domain named GlobalitcerT .com. The domain contains an organizational unit (OU) named Research. All users who have user accounts in the Research OU use portable computers that run Windows XP Professional.

You create a Group Policy object (GPO) named PowerManagement and link it to the Research OU. You configure the PowerManagement GPO to enable the Prompt for password on resume from hibernate /suspend policy.

A user named Sandra has a user account in the Research OU. Sandra reports that she is not prompted for a password when her computer resumes hibernation.

You need to ensure that Sandra immediately has password protection for her portable computer when resuming from hibernation mode.

What should you do?

A. Instruct Sandra to run the gpupdate command from her computer.

B. Instruct Sandra to run the gpresult command from her computer.

C. Instruct Sandra to send a Remote Assistance invitation to you.

Take control of Sandra's compute and run the secdit /analyze command.

D. Instruct Sandra to send a Remote Assistance invitation to you.

Take control of Sandra's computer and run the gpresult command.

Answer: A

Explanation: Although the GPO has been configured, some laptops may have not been online to be updated with the GPO policy or there could have been network connectivity problems that prevented some laptops from

getting the policy. All problems aside, Sandra's laptop should get the update at the next GPO refresh interval or Sandra can get refresh immediately by running the gpupdate command from her computer.

Incorrect answers:

B: The gpresult command will yield a text report of the resultant set of policy, i.e. the policy that is already applied. You rather want to enforce a new GPO and that can be done through the use of the gpupdate command that enforces a GPO without having to restart the computer.

C: This command is usually utilized when analyzing system security on a large number of computers. This will not ensure that Sandra will have immediate password protection for her portable computer when resuming from hibernation mode. She needs to have the GPO updated on her computer.

D: This would be the wrong command to use (see B explanation). First sending Remote Assistance invitation is not an immediate process as is required by the question.

Reference:

Michael Cross, Jeffery

A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.

Shinder, MCSE: Exam 70-294: Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 9, p. 623

Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-Paced Training Kit (Exam 70-294); Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, pp. 10-44 to 10-21, 11-4, 11-6, 11-19 to 11-22

QUESTION 381

You are the network administrator for GlobalitcerT .com. The network consists of a single Active Directory domain named GlobalitcerT .com. All servers run Windows Server 2003. Each client computer runs either Windows 2000 Professional or Windows XP Professional.

All desktop computers have computer accounts in an organizational unit (OU) named GlobalitcerT Desktops, and all portable computers have computer accounts in an OU named GlobalitcerT Portables. All employees have user accounts in an OU named GlobalitcerT Users.

A written GlobalitcerT policy requires that different Encrypting File System (EFS) policies be applied to portable computers and to desktop computers. In addition, policy settings in the Default Domain Policy Group Policy object (GPO) must apply to all computers.

You create two new GPOs named DesktopEFSPolicy and PortableEFSPolicy to be applied to desktop computers and portable computers, respectively. You configure each GPO to contain the policy settings required by the written GlobalitcerT policy.

You need to ensure that the written GlobalitcerT policy is enforced.

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

A. Link the DesktopEFSPolicy GPO to the GlobalitcerT Desktops OU. Link the PortableEFSPolicy GPO to the GlobalitcerT Portables OU.

B. In the Default Domain Policy GPO, assign the Domain Users security group the Deny - Full Control permission.

Assign the Domain Admins security group the Allow - Full Control permission.

C. Link the DesktopEFSPolicy GPO and the PortableEFSPolicy to the domain.

Configure the GlobalitcerT Desktops OU and the GlobalitcerT Portables OU to block Group Policy inheritance.

D. Enable the No Override setting for the Default Domain Policy GPO, the DesktopEFSPolicy GPO, and the PortableEFSPolicy OU.

Answer: A, D

Explanation: You want the Default Domain Policy settings to apply to all computers, so you must configure the No Override, or else lower GPO settings with the Block Policy Inheritance will negate the particular policy from above. Also the same is true for the OU level GPOS that are configured. Any lower GPOs configured on child OUs with Block Policy inheritance will negate policy from a higher level set GPO policy.

Incorrect Answers:

B: The GPO must be applied based to computer type, not user group.

C: Lower GPO settings with the Block Policy Inheritance will negate the particular policy from above.

Reference:

Jill Spealman, Kurt Hudson & Melissa Craft, MCSE Self-Paced Training Kit (Exam 70-294), Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Microsoft Press, Redmond, Washington, 2004, pp. 10-16 to 10-20, 10-40 to 10-41

QUESTION 382

You are the network administrator for GlobalitcerT .com. The network consists of a single Active Directory domain named GlobalitcerT .com. All servers run Windows Server 2003. One of the domain controllers is configured as an enterprise root certification authority (CA). All client computers run Windows XP Professional.

GlobalitcerT uses IPsec to secure communications between computers in GlobalitcerT and computers at other companies. These IPsec connections require computer certificates. Your IPsec policies require every computer to be able to make an IPsec connection when connecting to other computers.

You need to configure the network so that all computers can make IPsec connections.

What should you do?

E. In the computer settings section of the Default Domain Policy Group Policy object (GPO), configure the domain members to always digitally encrypt or sign secure channel data.

F. Create a new automatic certificate request in the computer settings section of the Default Domain Policy Group Policy object (GPO),

G. Obtain a new computer certificate from a public C

A. Import a copy of this certificate into the Trusted

Root Certification Authorities section of the Default Domain Policy Group Policy object (GPO).

H. Issue a new computer certificate from your enterprise C

A. Place a copy if this certificate on an internal

Web page. Instruct users to install this certificate in their trusted certificate store the first time they need to make an IPsec connection.

Answer: D

Explanation: Enterprise CAs is integrated into the Active Directory directory service. They use certificate templates, publish their certificates and CRLs to Active Directory, and use the information in the Active Directory database to approve or deny certificate enrollment requests automatically. Because the clients of an enterprise CA must have access to Active Directory to receive certificates, enterprise CAs are not suitable for issuing certificates to clients outside the enterprise. Enterprise CAs requires and uses Active Directory to issue

certificates, often automatically. AN IPSec connection comprises of two modes: Main mode and Quick mode. Main Mode is the first part of an IPSec connection. In Main Mode, each computer authenticates to the other and then IKE is used to calculate the master key. All other keys are generated from the master key. An IKE security association (SA) is created over which Quick Mode can be negotiated.

Quick Mode is the second phase of IPSec. In Quick Mode, agreement is reached for the encryption, integrity algorithms, and other policy settings. Two SAs are created, one incoming and one outgoing.

Incorrect answers:

A: Always digitally encrypting or signing secure channel data does not necessarily ensure the ability to make IPSec connections.

B: An automatic certificate request in the computer settings section of the Default Domain GPO is not the solution.

C: Obtaining a new certificate from a public CA is not going to ensure that all computers will have the ability to make IPSec connections. What is needed is to have a new computer certificate issued from your enterprise CA which should be installed on users' trusted certificate store.

Reference:

J. C. Mackin, Ian McLean, MCSA/MCSE self-paced training kit (exam 70-291): Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Microsoft Press, Redmond, Washington, 2004, p.11: 88

James Chellis, Paul Robichaux, and Matthew Sheltz, MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex Inc., Alameda, 2004, p. 11: 15

Michael Cross, Jeffery

A. Martin, Todd

A. Walls, Martin Grasdal, Debra Littlejohn Shinder & Dr. Thomas W.

Shinder, MCSE: Exam 70-294: Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory Infrastructure Study Guide & DVD Training System, Syngress Publishing, Rockland, MA, 2003, Chapter 9, p. 612

QUESTION 383

You are the network administrator for GlobalitcerT . The network consists of a single Active Directory domain named GlobalitcerT .com. All servers run Windows Server 2003. All client computers run Windows XP Professional.

User accounts are configured as local administrators so that users can install software. A desktop support team supports end users. The desktop support team's user accounts are all members of a group named Support.

You create a software restriction policy that only prevents users from running registry editing tools by file hash rule. You apply the policy to all user accounts in the domains.

The desktop support team reports that when they attempt to run registry editing tools, they receive the following error message:

"Windows cannot open this program because it has been prevented by a software restriction policy. For more information, open Event Viewer or contact your system administrator".

You need to ensure that only the desktop support team can run registry editing tools.

What should you do?

A. Configure the software restriction policies to be enforced for all users except local administrators.

B. Make users members of the Power Users group instead of the Administrators group.