Exam Report: 8.1.9 Practice Questions

Date: 11/23/2019 4:28:31 pm
Time Spent: 11:01

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 30%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

You have created a group policy that prevents users in the accounting department from accessing records in a database that has confidential information. The group policy is configured to disable the search function for all users in the Accounting OU no matter which workstation is being used.

After you configure and test the policy, you learn that several people in the Accounting OU have valid reasons for using the search function. These users are part of a security group named Managers.

What can you do to prevent the Group Policy object (GPO) that you have configured from applying to members of the Managers group?

- Move members of the Managers group to their own OU beneath the Accounting OU. Enable Block Policy inheritance for the new OU.
- ~~Make sure that the Managers group is not on the GPO's discretionary access control list (DACL).~~
- Add the Managers group to the Accounting OU's discretionary access control list (DACL). Deny the apply Group Policy and read permissions to the Managers group.
- Add the Managers group to the GPO's discretionary access control list (DACL). Deny the apply Group Policy and read permissions to the Managers group.

Explanation

Users must have the apply Group Policy and read permissions to a GPO for that GPO to be applied to the user. You can prevent a group from receiving a GPO by denying the group the required permissions to the GPO. By denying the permissions for the Managers group, you can prevent the GPO settings from applying to group members.

References

LabSim for Server Pro 2016, Section 8.1.
[AllQuestions_ServerPro_2017.exm GPO FOUNDATION 01]

Question 2: Correct

You are the security administrator for a large metropolitan school district. You are reviewing security standards with the network administrators for the high school. The school's computer center has workstations for anyone's use. All computers in the computer center are members of the Computer Center Computers global group. All workstations are currently located in the Computers container.

The computer center computers have access to the Internet so users can perform research. Any user who uses these computers should be able to run Internet Explorer only. Other computers in the high school should not be affected. To address this security concern, you create a Group Policy object (GPO) named Computer Center Security.

How can you configure and apply this GPO to enforce the computer center's security?

- Configure the User Configuration node of the Computer Center Security GPO to restrict software to Internet Explorer only. Link the GPO to the Computers container and allow access to the Computer Center Computers group only.
- Configure the Computer Configuration node of the Computer Center Security GPO to restrict software to Internet Explorer only. Link the GPO to the domain and allow access to the Computer Center Computers group only.
- Configure the User Configuration node of the Computer Center Security GPO to restrict software to Internet Explorer only. Link the GPO to the domain and allow access to the Computer Center Computers group only.
- Configure the Computer Configuration node of the Computer Center Security GPO to restrict software to Internet Explorer only. Link the GPO to the Computers container and allow access to the Computer Center Computers group only.

Explanation

To apply settings that apply to computers without regard to the user who is using them, you need to configure the Computer Configuration node of a Group Policy object (GPO). You also need to link the GPO to a domain, site, or organizational unit (OU) that contains the relevant computer accounts. Because the GPO is linked to the domain but should apply to computer center computers only, you need to filter access to the GPO so it applies to the Computer Center Computers group only.

You cannot link GPOs to the Computers container because it is not an OU. Therefore, you should link the GPO to the domain in this scenario.

References

LabSim for Server Pro 2016, Section 8.1.
[AllQuestions_ServerPro_2017.exm GPO FOUNDATION 02]

Question 3: Incorrect

You are the administrator for a network with a single Active Directory domain named widgets.local. The widgets.local domain has an organizational unit object for each major department in the company, including the information systems department. User objects are located in their respective departmental OUs. Users who are members of the Domain Admins group belong to the Information Systems department. However, not all employees in the Information Systems department are members of the Domain Admins group.

To simplify employees' computing environment and prevent problems, you link a Group Policy object (GPO) to the widgets.local domain that disables the control panel for users.

How can you prevent this Group Policy object from applying to members of the Domain Admins group?

- On the Group Policy object's access control list, deny the read permission for members of the Domain Admins group.
- Link the Group Policy object to each organizational unit rather than to the domain.
- On the Group Policy object's access control list, deny the apply Group Policy permission for members of the Domain Admins group.
- ~~Configure the Information Systems OU to block policy inheritance.~~
- Link the Group Policy object to each organizational unit (except the Information Systems OU) rather than to the domain.

Explanation

Because the Information Systems OU has users to which the GPO should apply as well as those to which the GPO should not apply, the GPO must be linked to the domain or each individual OU. Linking the GPO to the domain is a simpler solution than linking it to each individual OU,

and is the best solution. Then, to prevent the Group Policy object from applying to members of the Domain Admins group, you need to deny that group the Apply Group Policy permission to the GPO. Do not deny the Read permission, or Domain Administrators will not be able to edit the GPO.

References

LabSim for Server Pro 2016, Section 8.1.
[AllQuestions_ServerPro_2017.exm GPO FOUNDATION 03]

Question 4: Correct

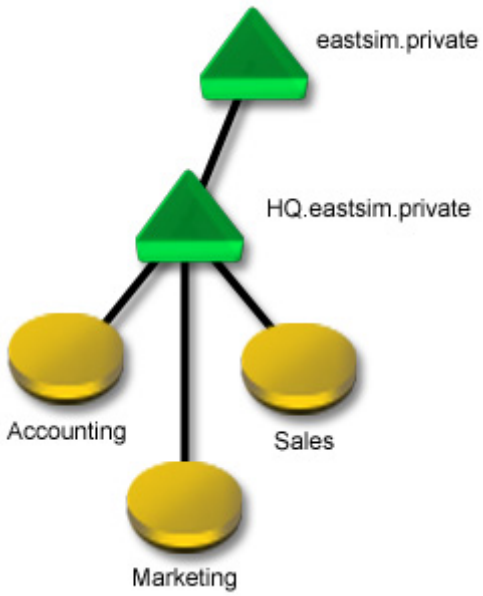
Your network has a single Active Directory forest with two domains, eastsim.private and HQ.eastsim.private. The organizational units Accounting, Marketing, and Sales represent departments of the HQ domain. Additional OUs (not pictured) exist in both the eastsim.private and HQ.eastsim.private domains. All user and computer accounts for all departments company-wide are in their respective departmental OUs.

You are in the process of designing Group Policy for the network. You want to accomplish the following goals:

- You want to enforce strong passwords throughout the entire forest for all computers. All computers in both domains should use the same password settings.
- The Accounting department has a custom software application that needs to be installed on computers in that department.
- Computers in the marketing and sales departments need to use a custom background and prevent access to the **Run** command.

You create the following three GPOs with the appropriate settings: Password Settings, Accounting App, and Desktop Settings.

How should you link the GPOs to meet the design objectives? To answer, drag the label corresponding to the GPO to the appropriate boxes.



eastsim.private

✔ Password Settings		
	(leave blank)	(leave blank)

HQ.eastsim.private

✔ Password Settings		
	(leave blank)	(leave blank)

Accounting

✔ Accounting App	~~Password Settings~~

(leave blank)

Marketing

✓ Desktop Settings	~~Password Settings~~

(leave blank)

Sales

✓ Desktop Settings	~~Password Settings~~

(leave blank)

Explanation

To meet the requirements, link the GPOs as follows:

- Link the Password Settings GPO to both the eastsim.private and HQ.eastsim.private domains. Password policies must be set in a GPO linked to a domain and apply only to the domain for which they are linked. You want the password settings to apply to both domains.
- Link the Accounting App GPO to the Accounting OU. The GPO will apply only to computers in the Accounting OU.
- Link the Desktop Settings GPO to both the Marketing and Sales OUs.

Do not apply the GPO to the domain, as this would apply the settings to computers in the Accounting OU as well.

References

LabSim for Server Pro 2016, Section 8.1.
[AllQuestions_ServerPro_2017.exm GPO FOUNDATION 04]

Question 5: Correct

You are the administrator for the widgets.com domain. Organizational Units (OUs) have been created for each company department. User and computer accounts for each department have been moved into their respective departmental OUs.

From your workstation, you create a GPO that configures settings from a custom .admx file. You link the GPO to the Sales OU.

You need to make some modifications to the GPO settings from the server console. However, when you open the GPO, the custom administrative template settings are not shown.

What should you do?

- ○ On the Administrative Template node, right-click the node and choose Add/Remove Templates.... Browse and select the .admx file to add.
- ○ Right-click the Security Settings node and select Import Policy....
- ➡ ◉ Enable the Administrative Templates central store in Active Directory. Copy the .admx file to the central store location.
- ○ Install PowerShell on the server.

Explanation

When using .admx files, custom .admx files must be located on the local system or stored in Active Directory in the central store. If the central store is enabled, Group Policy Object Editor reads the .admx files from that location.

The Security Settings node allows you to import a predefined security policy. The Administrative Template node allows you to add .adm template files. Powershell is installed on the server by default.

References

LabSim for Server Pro 2016, Section 8.1.
[AllQuestions_ServerPro_2017.exm GPO FOUNDATION 05]

Question 6: Incorrect

You are the administrator for the widgets.com domain. Organizational units (OUs) have been created for each company department. User and computer accounts for each department have been moved into their respective departmental OUs.

As part of your security plan, you have analyzed the use of Internet Explorer in your organization. You have defined three different groups of users. Each group has different needs for using Internet Explorer. For example, one group needs ActiveX controls enabled, and you want to disable ActiveX for the other two groups.

You would like to create three templates that contain the necessary settings for each group. When you create a GPO, you want to apply the settings in the corresponding template rather than manually set the corresponding Administrative Template settings for Internet Explorer.

What should you do?

- ○ Create three custom .admx files. Copy these files to the central store location. When creating the GPOs, select the necessary .admx file.
- ○ Create three custom .admx files. Copy these files to the local workstation that you use to manage GPOs. Use the Add/Remove Templates... feature to add the necessary template when creating the GPO.
- ◉ ~~Identify three GPOs with the necessary settings. Take a backup of these GPOs. After creating a new GPO, right-click the GPO and choose Restore from Backup....~~
- ➡ ○ Create three starter GPOs with the necessary settings. When creating the GPOs, select the starter GPO with the desired settings.

Explanation

Because all settings are stored in the Administrative Templates portion of the GPO, you can use starter GPOs. Create the starter GPOs with the necessary settings, and then use a starter GPO when creating the new GPO. Settings in the starter GPO will be copied into the new GPO.

.admx files are templates that identify possible Administrative Template settings; the files do not contain specific settings. You can only restore a GPO to the same GPO that was backed up. To restore settings to a different GPO, import the settings from a backup.

References

LabSim for Server Pro 2016, Section 8.1.
[AllQuestions_ServerPro_2017.exm GPO FOUNDATION 06]

Question 7: Incorrect

You are the administrator for the widgets.com domain. Organizational units (OUs) have been created for each company department. User and computer accounts for each department have been moved into their respective departmental OUs.

As you manage Group Policy objects (GPOs), you find that you often make similar user rights, security options, and Administrative Template settings in different GPOs. Rather than make these same settings each time, you would like to create some templates that contain your most common settings.

What should you do? (Select two. Each choice is a possible solution.)

- ☐ Create starter GPOs. When creating new GPOs, select the appropriate starter GPO.
- ☑ ~~Create custom .admx files with the necessary settings. Copy these files to the central store. After creating the GPO, import the settings from the .admx files.~~
- ➡ ☐ Create GPOs with the common settings. When creating new GPOs, copy one of the existing GPOs.
- ➡ ☐ Create GPOs with the common settings. Take a backup of each GPO. After creating new GPOs, import the settings from one of the backed up GPOs.

Create GPOs with the common settings. Take a backup of each GPO. After creating new GPOs, restore one of the backed up GPOs.

Explanation

Because the settings you want to copy include user rights and security options, you can copy an existing GPO or import settings from a backup of another GPO.

Starter GPOs only contain administrative template settings, not other GPO settings, such as software installation, user rights, or security options. .admx files are templates that identify possible administrative template settings; the files do not contain specific settings. You can only restore a GPO to the same GPO that was backed up.

References

LabSim for Server Pro 2016, Section 8.1.
[AllQuestions_ServerPro_2017.exm GPO FOUNDATION 07]

Question 8: Incorrect

You are the administrator for the widgets.com domain. Organizational units (OUs) have been created for each company department. User and computer accounts for each department have been moved into their respective departmental OUs.

You have two OUs that contain temporary users, TempSales and TempMarketing. For all users within these OUs, you want to restrict what the users are able to do. For example, you want to prevent them from shutting down the system or accessing computers through a network connection.

Which GPO category would you edit to make the necessary changes?

- User Rights
- Security Options
- Restricted Groups
- ~~Account Policies~~

Explanation

Configure user rights to determine what actions a user can perform on a computer or domain. User rights settings identify users or groups with the corresponding privileges.

Configure security options to control actions that everyone can perform. Use restricted groups to limit the membership of specific security groups. Use account policies to control password and account lockout settings for all users.

References

LabSim for Server Pro 2016, Section 8.1.
[AllQuestions_ServerPro_2017.exm GPO FOUNDATION 08]

Question 9: Incorrect

You are the administrator for the widgets.com domain. Organizational units (OUs) have been created for each company department. User and computer accounts for each department have been moved into their respective departmental OUs.

You would like to configure all computers in the Sales OU to prevent the installation of unsigned drivers.

Which GPO category would you edit to make the necessary changes?

- User Rights
- ~~Restricted Groups~~
- Security Options

Account Policies

Explanation

Configure security options to control actions that everyone can perform, such as preventing the installation of unsigned drivers.

Configure user rights to determine what actions a user can perform on a computer or domain. User rights settings identify users or groups with the corresponding privileges. Use restricted groups to limit the membership of specific security groups. Use account policies to control password and account lockout settings for all users.

References

LabSim for Server Pro 2016, Section 8.1.
[AllQuestions_ServerPro_2017.exm GPO FOUNDATION 09]

Question 10: Incorrect

You are the network administrator for eastsim.com. The network consists of a single Active Directory domain. The company has a main office in New York and several international locations, including facilities in Germany and France.

You have been asked to build a domain controller that will be deployed to the eastsim.com office in Germany. The network administrators in Germany plan to use Group Policy administrative templates to manage Group Policy in their location. You need to install the German version of the Group Policy administrative templates so they will be available when the new domain controller is deployed to Germany.

What should you do?

- Copy the German .ADM files to the appropriate directory in the SYSVOL on a local domain controller.
- Copy the German .ADMX files to the appropriate directory in the SYSVOL on a local domain controller.
- ~~Copy the NTDS.dit file to the appropriate directory in the SYSVOL on a local domain controller.~~
- Copy the German .ADML files to the appropriate directory in the SYSVOL on a local domain controller.

Explanation

You should copy the German .ADML files to the appropriate directory in the SYSVOL on a local domain controller.

The Group Policy administrative templates come in 34 different languages. When you have extracted the appropriate language, you copy the ADML files to the appropriate directory in the SYSVOL share on a local domain controller. They will then replicate to the other domain controllers in the domain. The appropriate directory would be PolicyDefinitions*LANGUAGE* where *LANGUAGE* would be the appropriate code for the language being installed. For example, for the German language, the directory would be de-DE; for the French language, it would be fr-FR.

ADM files were the older version of Administrative templates used in Windows Server 2003. Windows Server 2008 introduced ADMX files, which are based on XML coding. However, the language files are .ADML files. The NTDS.dit file is the file that contains the Active Directory database. It is located in the **%systemroot%\NTDS** folder on the domain controller. It should not be copied to the SYSVOL.

References

LabSim for Server Pro 2016, Section 8.1.
[AllQuestions_ServerPro_2017.exm GPO FOUNDATION 10]