Lesson 8

CONFIGURING THE USER AND COMPUTER ENVIRONMENT USING GROUP POLICY

Knowledge Assessment

Fill in the Blank

1. In a case where multiple PSOs are configured for a particular user, Active Directory will determine which one to apply by using the PSO's \_precedence\_. P160

2. You can automatically add a technical support user to the local Administrators group of each domain workstation by using \_Restricted Groups\_. P168

3. The \_gpupate.exe\_ command allows you to manually refresh Group Policy settings on a particular computer. P177

4. \_\_Tattooing\_\_ refers to a Group Policy setting that is not removed when the GPO setting reverts to "Not Configured." P173

5. You would audit \_\_Account Logon Events\_\_ to determine who is authenticating against your Active Directory domain controllers. P165

6. Each Active Directory domain controller acts as a(n) \_\_Key Distribution Center (KDC)\_\_ to enable the distribution of Kerberos tickets. P161

7. \_\_Folder Redirection\_\_ allows you to configure a user's Documents, Desktop, and other folders so that they are stored on a network drive rather than the local computer. P170

8. Settings in the \_Kerberos Policies\_ section of Group Policy allow you to configure the maximum allowable clock skew between a client and a domain controller. P161

9. Auditing for \_\_Policy Change events\_\_ will alert you when a change is made to User Rights assignments, IPSec policies, or trust relationships. P165

10. You can create a consistent service startup configuration for multiple computers by using the \_\_System Services\_\_ node in Group Policy. P169

Multiple Choice

1. What type of object will you create to enable multiple password policies within a Windows Server 2008 domain?

a. msDS-MinimumPasswordLength

b. msDS-MultiplePasswordPolicies

c. PasswordSettingsObject (PSO)

d. msDS-PasswordObject

Windows Server 2008 introduces a new object type called a PasswordSettingsObject (PSO) that allows you to configure multiple password policies and account policies within a Windows Server 2008 domain. P160

2. Which configuration item has a default value of 90 minutes for workstations and member servers, with a random offset of 0 to 30 minutes to optimize network performance?

a. Refresh time

b. Refresh interval

c. Clock skew

d. Clock interval

The default Group Policy refresh interval for workstations and member servers in an Active Directory is 90 minutes; for domain controllers, the refresh interval is every 2 minutes. P177

3. To determine which users are accessing resources on a particular member server in an Active Directory domain, which event type would you audit?

a. Account logon event

b. Policy change event

c. Account management event

d. Logon event

Logon events are logged when a user authenticates to a member server or workstation in an Active Directory domain. Account logon events are logged whenever a user authenticates against an Active Directory domain controller. P165

4. Monitoring a system such as Active Directory for the success and/or failure of specific user actions is called

a. auditing

b. inspecting

c. scanning

d. sniffing

You can audit numerous types of system events including account logon events, logon events, object access, directory service access, and account management events. Within each event category, you can audit success events, failure events, or both. P163

5. Which audit category includes events such as server startup and shutdown, time changes, and clearing the security log within the Windows Event Viewer?

a. Process tracking

b. Privileged use

c. System Events

d. Policy management

By default, the System Events audit category is set to log success events in the Default Domain Controllers Policy. P165

6. Which feature allows you to control how much space a user can take on a particular hard drive volume, configurable via Group Policy?

a. Disk quotas

b. Folder redirection

c. Offline files

d. Object access auditing

Disk quotas can be configured at the volume level using Active Directory Group Policy Objects and can be more granularly controlled using the File Services role installed on a Windows Server 2008 member server. Additional information about managing the File Services role can be found in the MOAC 70-642 and MOAC 70-643 textbooks and lab manuals. P174

7. To prevent users from re-using a certain number of network passwords, what can you configure as part of a domain-wide policy or as part of a Fine-Grained Password Policy?

a. Minimum password length

b. Minimum password age

c. Maximum password age

d. Enforce password history

By configuring the “Enforce password history” setting, you can configure all users who receive a particular password policy so that they cannot re-use a specified number of passwords. This means that users must create new network passwords rather than simply re-using old passwords when their passwords expire. P160

8. A PasswordSettingsObject (PSO) within Active Directory is also known as which type of object?

a. msDS-PasswordSettingsPrecedence

b. msDS-PasswordSettings

c. msDS-PasswordComplexityEnabled

d. msDS-MinimumPasswordLength

Windows Server 2008 introduces Fine-Grained Password Policies, which are enabled by the addition of a new object type within Active Directory referred to as a PasswordSettingsObject (PSO) or msDS-PasswordSettings object.P160

9. Which Group Policy feature allows users to access user files when the user is disconnected from the corporate network?

a. Folder redirection

b. Disk quotas

c. Offline files

d. Object access auditing

When the Offline Files feature is enabled, users can access their network files as though they were still connected to the network; any changes made while offline will be applied when the user reconnects. Combining this feature with Folder Redirection creates a balanced solution between centralization of user data and enabling convenient access for remote and travelling users.P173

10. Which audit event type is triggered when user or group accounts are created, deleted, renamed, enabled, or disabled?

a. Account logon events

b. Account management events

c. Privileged use events

d. Policy management events

This policy is set to audit Success events by default in the Default Domain Controller Policy of Windows Server 2008. P165

CASE SCENARIOS

Scenario 8-1: Lucerne Publishing and Offline Files

You are a computer consultant. Linda Randall, Chief Information Officer of Lucerne Publishing, has asked for your help. The Lucerne Publishing network consists of a single Active Directory domain with four domain controllers running Windows Server 2008, three file servers, and 300 clients that are evenly divided between Windows XP Professional and Windows Vista.

Recently, several publishing projects stored in electronic format were lost when an employee's laptop was stolen from a publishing convention. Previously, another employee lost important publishing project files during a fire sprinkler system incident in which the employee's computer was destroyed.

Employees typically store documents in the Documents folder on their local systems. Linda wants all employees to store their data on the network servers. The data on the network servers is backed up regularly. Linda tells you that her editors tend to work on sensitive data that requires special handling. She is especially worried that the data is backed up and secured.

All client computers have P drive mappings that are supposed to be used for storing files. However, many employees do not understand drive mappings. They often store files in their Documents folder and then copy them over to the P drive. This is also an issue because many employees forget to copy their files to the server until something occurs, such as a data loss.

Given Lucerne Publishing's concerns, answer the following questions:

a. How would you address Linda's concern that some employees do not understand drive mappings and others forget to store their data on the server?

Deploy Automatic Folder Redirection so that users do not need to remember to save their files and folders to a network server.

b. How can you address the situation concerning the sensitive data editors use?

Deploy EFS to encrypt files and folders for individual users.

c. How would you address the users with mobile computers so that they could work on their files while traveling?

Deploy Offline Folders.

d. Linda warns that some users may have huge amounts of data already stored in the My Documents folder on their local computer. How might this affect your recommendations?

The user's first logon after configuring Folder Redirection will appear significantly slower because their existing files are uploaded to the network location.