

CIS131 – Homework 6 - (Account Policies, Groups, Local Policies)

Account Policies

1. Display the domain-wide password policy settings for your domain.
 - a. Provide a print-screen image of the current settings.
 - b. Explain each of the current settings.

2. Change the domain-wide policy to conform with the following:
 - Users must change their password every 90 days
 - They cannot change their password unless they've had it for at least 2 days
 - Their password must be at least 10 characters long
 - The system should not allow them to reuse any of the last 5 passwords used
 - Complex passwords must be used
 - a. Provide a print-screen image which displays these values.

3. Display the domain-wide account lockout policy settings for your domain.
 - a. Provide a print-screen image of the current settings.
 - b. Explain what each means.

4. Change the domain-wide account lockout policy to conform with the following:
 - a. If a user attempts to logon incorrectly at least 5 times within 20 minutes, their account should be locked for 20 minutes.
 - b. Provide a print-screen image which displays these values.
 - c. Explain how you could configure the account to lock until it's reset by an administrator.

5. At one of the clients in your domain, attempt to logon as one of your users. Do not enter the correct password. Do this 6 times.
 - a. What message did you receive after the 6th attempt?
 - b. Explain why you received this message.

6. Logon as administrator and display the Account Tab for the user you used in step 5. The account should be locked.
 - a. Provide a print-screen image which confirms that the account is locked. (You can unlock the account.)

Local Policies

This part of the assignment will have you define some User Rights Assignments for all computers in the domain and some for just domain controllers in the domain. The objective is to understand the different locations where this would be set and to be able to confirm that the policy was configured as defined. You must complete these tasks using the existing GPOs on the system; do not create new GPOs

7. Using Group Policy Management, modify the “*Perform Volume Maintenance Tasks*” user’s right for all computers in the domain. Add the “Backup Operator’s” group to the list of

existing groups who have this right locally – be sure you are adding and not wiping out any existing entries at the client.

- a. Provide a bulleted list of all the steps used to configure this as well as the steps used to confirm the setting was applied. Be very specific in your list; assume someone will be using the steps you provide to complete this task.
 - b. At the server, open Group Policy Management and drill down to the “User Rights Assignment” node and, while this node is selected, provide a screenshot. Make sure the “Policy Setting” column in the right pane is wide enough to display the full value of the “*Perform Volume Maintenance Tasks*” item. I want the entire Group Policy Management Screen; don’t crop anything out.
 - c. At each of the client machines, open Local Security Settings, drill down to the “User Rights Assignment” node and, while this node is selected, provide a screenshot. Make sure the “Security Setting” column in the right pane is wide enough to display the full value of the “*Perform Volume Maintenance Tasks*” item. I want the entire Local Policy Security screen; don’t crop anything out. Submit one screenshot for each client; label each accordingly.
 - d. What group(s) had this right at the client machines prior to configuring this group policy setting?
8. Using Group Policy Management, modify the “*Allow log on through Remote Desktop Services*” user’s right for all Domain Controllers in the domain. Administrators and the Remote Desktop Users group should be allowed this right.
- a. Provide a bulleted list of all the steps used to configure this as well as the steps used to confirm the setting was applied. Be very specific in your list; assume someone will be using the steps you provide to complete this task.
 - b. At the server, open Group Policy Management and drill down to the “User Rights Assignment” node and, while this node is selected, provide a screenshot. Make sure the “Policy Setting” column in the right pane is wide enough to display the full value of the “*Allow log on through Remote Desktop Services*” item. I want the entire Group Policy Management Screen; don’t crop anything out.
 - c. At the server, open Local Security Settings, drill down to the “User Rights Assignment” node and, while this node is selected, provide a screenshot. Make sure the “Security Setting” column in the right pane is wide enough to display the full value of the “*Allow log on through Remote Desktop Services*” item. I want the entire Local Policy Security screen; don’t crop anything out.
 - d. At either one of the client machines, open Local Security Settings, drill down to the “User Rights Assignment” node and, while this node is selected, provide a screenshot. Make sure the “Security Setting” column in the right pane is wide enough to display the full value of the “*Allow log on through Remote Desktop Services*” item. I want the entire Local Policy Security screen; don’t crop anything out.
 - e. Test your policy: from one of the client machines, remote control the server as the Administrator and as a user who is a member of the remote desktop user’s group. What user did you test this as? Was the administrator and the user able to remote control the server?

Groups

You should currently have 10 users in *your* container. (If you have more, that's fine, if you have less, create as many as is necessary to make 10.) The goal of the next few problems in this assignment is to split those users into two departments. Assume half of these users work in the Sales department and the other half work in the Finance department and that you'll later be assigning permissions shared uses to all users in the Sales department and all users in the Finance Department.

9. Create an organizational unit within *your* container for each department (Finance and Sales).
 - a. Provide a print-screen image which confirms the containers were created in the appropriate location.
10. Use Active Directory Users and computers to move half of your users from *your* container to the Sales container and the other half to the Finance container.
 - a. Provide a print-screen image of each department's container to confirm the users were moved.
11. In this problem you must create the appropriate number of groups with the appropriate scopes and memberships to represent users in each department (Finance and Sales). The group objects must be created within the respective containers (i.e., Finance groups must be stored in the Finance container... Sales groups must be stored in the Sales container). When completing this task you ***must*** conform to the best practice covered in class (AGDLP). You must also use a consistent naming convention when naming groups. (Please do not use Universal Groups.)
 - a. Explain the naming convention you used for domain local groups? For global groups?
 - b. Provide a print-screen image that displays the sales container's contents. Be sure that the '*Type*' column is fully displayed.
 - c. Provide a print-screen image that displays the finance container's contents. Be sure that the '*Type*' column is fully displayed.
 - d. Provide a print-screen image that displays the *Members* property for *each* of the groups you created. The number of print-screens you include should match the number of groups you created.
12. Rename your template object – it's name must be `_SalesTemplate`. Copy the object to a new object named `_FinanceTemplate`. Assume this `_SalesTemplate` object will be used when creating new accounts for employees in the Sales department and assume the `_FinanceTemplate` will be used when creating new accounts for employees in the Finance department. Configure each template to include the appropriate group membership for any new sales or finance employees employees. Move the `_SalesTemplate` object to the sales container and move the `_FinanceTemplate` object to the Finance container.
 - a. Provide a screenshot of the *Member of* tab of the `SalesTemplate` object.
 - b. Provide a screenshot of the *Member of* tab of the `_FinanceTemplate` object.
 - c. Use each of the templates to create a new user in each department. Explain the process you used to create these new users and provide a screenshot of the following tabs for each user: profile tab, member of tab.
 - d. Provide a screenshot of the Finance container and a screenshot of the Sales container.

13. Create a new user in *your* container. Use your name as the user's account name. When naming your user, be sure to use the same naming convention used when creating your existing users. The new user must be configured as follows:
- This user must have full administrative rights throughout the domain.
 - Same home folder requirements as existing users
 - No logon time or station restrictions
 - Password should never expire
- a. Provide a print-screen image of the user's *Member Of* page.
 - b. Provide a print-screen image of the user's *Profile* tab.
 - c. Provide a print-screen image of the user's *Account* tab.
14. Confirm that your newly created 'administrative account' does in fact have administrative rights in the domain.
- a. Explain *exactly* how you confirmed this account worked.

In the next two problems you should be adding a user to an appropriate built-in group.

15. Create a new container directly within *your* container. Name the container ITS. Create a new user in this container. Assume that you want this user to be able to create, delete and modify user and group accounts in the domain. You do not however want him/her to be able to manage anything else on the server. Add the user to the appropriate group and confirm that you've appropriately configured the account.
- a. What user did you use – provide his/her name.
 - b. To which group did you add this user?
 - c. Provide a print-screen image of the user's *member of* tab
 - d. Explain how you confirmed that this account was appropriately configured? (Do not just show me that the user is a member of the group you selected.... Confirm by testing the user's rights and explain how you did it.)
16. Create another user in the ITS container. Assume that you want this user to be able to administer all the printers in your domain. Add the user to the appropriate group.
- a. What user did you use – provide his/her name.
 - b. To which group did you add this user?
 - c. Provide a print-screen image of the user's *member of* tab