Experiment No.5

Security Group Policies Management

Objectives

Group Policy management is a Windows Server 2003 features in which it allows administrators to define policies for both servers and user machines. Group policies ensure that all computers in the network are secure and ease the process of deployment by keeping the network safe. They allow the definition of user and computer related policies, network settings and security settings. In this lab, we will go over implementing group policy object, configuring group policies and determining applied group policies objects. In addition, we are going to apply different security policies to groups.

Group Policies

Group Policy is a management solution in Windows Server 2003 which allows the administrator to implement security and networking policies' settings across the company. In addition, it enables the management of domain controllers as well as desktop user machines.

Group policies allow the administrator to configure the settings of a computer or a group of users. Several security settings located under Group Policy Editor, Windows settings, and security settings can be used to configure IP security and specify different settings. For example, user rights. Group policies can be applied on domains, sites, organizational units, users or computers and these configuration can be all done from the server. The benefit of a group policy that is applied on an organizational unit is the inheritance that the computers and users get benefit from. For example, we can configure an OU to assign permissions to a registry key in which this policy will be applied to all computers under this OU. Yet, there is one exception which is the Account Policies Settings that only applies to the domain level by default.

Implementing Group Policy Objects

Group policies are usually linked to multiple objects of the Active directory (sites, domains or organizational unit). Yet, they can’t be linked directly to a user of security group.

When linking multiple GPOs (Group Policy Object) to a single object (domain, site, OU), the lowest link order in the list has the highest precedence and overwrites all other GPOs. Site and domain GPOs and GPOs that are lined to the domain or site are processed next which means that the highest order is processed first and the lowest link order is processed last.

Organizational units GPOs are processed according to the hierarchy, so the highest OU is processed first, then its children OUs, until it reaches the computer of the user. The OU that is processed last has the highest priority and it overcomes all the previous settings.
Group Policy is processed in this order

![Group Policy Processing Hierarchy](image)

Fig 1 Group Policy Processing Hierarchy

*NOTE* To view the precedence of Group Policies on any site, domain or OU go to Group Policy inheritance tab. The first object applies last and takes precedence over all others.

Implementing Group Policy on a Organizational Unit

First of all make sure that you have the group policy management installed in the administrative tools. If not, go to run >GPMC and install the group policy settings. Otherwise follow these steps:

1. Go to administrative tools > **Group Policy Management**
2. Right-click on *Group Policy Objects* and select **New**
3. Name your policy
4. Click on **Link an Existing GPO** to Link a GPO to an Organizational Unit
5. Select the Group Policy Object you want to link

*Note: you can edit the GPO by right clicking and clicking edit.*
Configuring Group Policy Settings

A Group Policy Object (GPO) is a collection of Group Policy settings. Normally, a user can edit GPOs which are locally installed on each computer, yet an administrator can create any non local GPOs.

To disable Windows Messenger from running, for example, follow these steps:

1. Create GPO as mentioned above
2. Right click and edit the **Group Policy settings**.
3. Your new GPO will appear to the right. Right-click on the GPO and select **edit**.
4. **Group Policy Object Editor** will open. Navigate to **User Configuration>Administrative Templates>Windows Components>Windows Messenger**.
5. Two Group Policies setting will appear. Double-click on **“Do not allow Windows Messenger to be run”**.
6. There are three options: Not configured, enabled and disabled. Not configured means that the GPO takes precedence and would allow users to use windows messenger. Enable means that you are not allowing windows messenger to run. And disabled allows users to run windows messengers. (In Case you forget what each means, you can press explain tab and a clear description will show).

*Note: After configuring the GPO, you can still link it to OU, Domain, or site by right-clicking on one of the objects and choosing link an existing GPO*.

Determining Applied GPOs

To determine what effective Group Policies are applied to a user or computer, The **Group Policy Results Wizard** allows you to target configured settings. To do so, open the group policy management, then:

1. Right-click on **Group Policy Results** and select **Group Policy Results Wizard**.
2. Select a user or computer.
3. A report will be displayed under **Group Policy Results**.
4. Click show the report to identify section of interest.

Security Policies

Some of the other popular security options you can set in Group Policy are:
1. Password Policy

Go to Group Policy Object Editor >Computer Configuration >Windows Settings: >Security Settings> Account Policies >Password Policy. There are six options:

a. **Enforce password history** (keep a history of all passwords assigned and don’t allow repetition)

b. **Maximum password age** (Allows a maximum amount of time a password can be kept before changed. After it expires, the user has to assign a new password)

c. **Minimum password age** (Determines the minimum amount of times a user can keep his/her password)

d. **Password must meet complexity requirements** (lower case, upper case, numbers and special characters)

e. **Store passwords using reversible encryption** (stores passwords in the equivalent of plaintext.)

2. Account Lockout Policy


a. **Account lockout duration** (A defined number of times in which the user is allowed to enter the correct password).

b. **Account lockout threshold** – (A defined number of times in which the user can enter an incorrect password).

c. **Reset account lockout counter after** (resets the counter for lockouts after a predetermined time).

3. User Rights Assignment

Go to Computer Configuration> Windows Settings>Security Settings> Local Policies> User Rights Assignment. You can choose either to deny or grant a right for users.

4. Security Options

Go to Computer Configuration>Windows Settings>Security Settings>Local Policies> Security Options. You can choose to grant or deny a number of security options to certain users or groups.
Conclusion

There are numerous security settings that can be configured in a single Group Policy Object. Yet, you have to make sure that all security settings are tested before pushing them into production. In this lab, we have introduced group policies and we have applied it on one of the windows components of the administrative templates in addition to other security policies. In the next lab, we will go over security templates which are essential for applying network security policy. In addition, to auditing which keeps track of all actions of computers and users.