Lab 7: Group Policy

East Tennessee State University

CSCI 4417/5417: Introduction to System Administration

Spring 2016

Pramod Nepal

Lab 7: Group Policy
CSCI 4417/5417 – Introduction to System Administration

Pramod Nepal
12 April 2016

Purpose

The focus of this lab was to learn to setup Group Policy. Two Group Policy Objects (GPO) were created and the access to resources of each group at different authentication level was tested.

Materials

- Lab Instructions
- PuTTY
- Two Windows instances i.e., AD Domain Server (DS) and Member Server (MS).

Procedure and Results

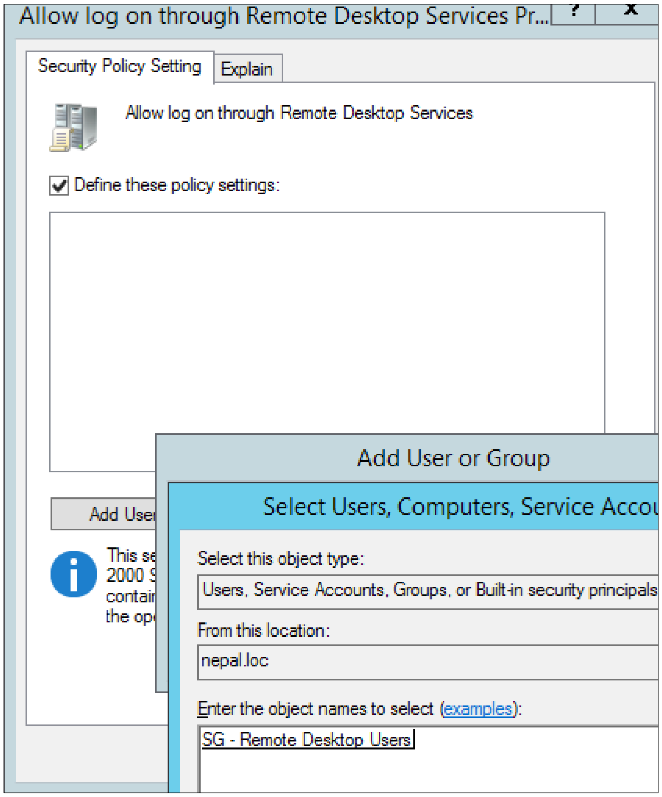
Setup

As a preventive measure for not bricking both DS and MS instances' images were created. To create the image in the EC2 dashboard the respective images were selected and 'Create Image' option was selected from actions Image menu. One of the objectives of the Lab was to create a GPO that would have restricted access to the server. Users under this group would not have administrative privileges. The test to verify that the access worked was by making sure that the user failed to edit the registry after the user was assigned to a group that had restricted access to the domain server. First the domain server was RDP into. In the Active Directory Users and Computers new Organizational Unit was created using the domain created in previous labs. This object was named 'Domain – Groups'. Two more hierarchical Organizational Units were created under 'Domain – Groups' called 'Security' and under which 'SG - Remote Desktop Users'. The group access was set as 'Global'. As noted from lecture, 'Global' groups have access within multiple domains. The 'Group type' was set as 'Security' since the intention was to create a security group.

Group Policy Object

Group Policy Management Console was started and the domain created in previous labs was selected. The domain name was right-clicked and 'Create a GPO in this domain, and Link it here...” option was selected. In an organization these settings would be more pertinent to an OU rather than for the entire domain. The GPO was named 'Enable RDP'. In the 'Group Policy Objects' directory of the domain Edit menu option of 'Enable RDP GPO' was selected from right-click menu. This opened the 'Group Policy Management Editor'. Since the purpose of this GPO was to allow Remote Desktop Connection 'Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Users Rights Assignment\Allow Log on through Remote Desktop Services' was selected and 'Define these policy settings' was clicked. 'Add Users and Group…' was clicked and 'SG – Remote Desktop users' OU created previously was searched and added (see Fig 1.).

Figure 1: Adding 'SG – Remote Desktp users' OU for remote login



Allow log on through Remote Desktop Services Pr...

Allow log on through Remote Desktop Services

☑ Define these policy settings:

Add User or Group

Select Users, Computers, Service Accou

Select this object type:
Users, Service Accounts, Groups, or Built-in security principals

From this location:
nepal.loc

Enter the object names to select (examples):
SG - Remote Desktop Users

Next, 'Computer Configuration\Policies\Windows Settings\Security Settings\Restricted Groups' was selected and 'Add Group...' menu option was selected after right-clicking on the blank area that opens up. 'SG – Remote Desktp Users' was added for the 'Members of this Group' of Remote Desktop Users option. Few more options like Firewall, allowing remote connection through Remote Desktop Services were enabled. However, 'Require user authentication for remote connections by using Network Level Authentication' was disabled. After these settings, users of this group would be able to RDP into the server.

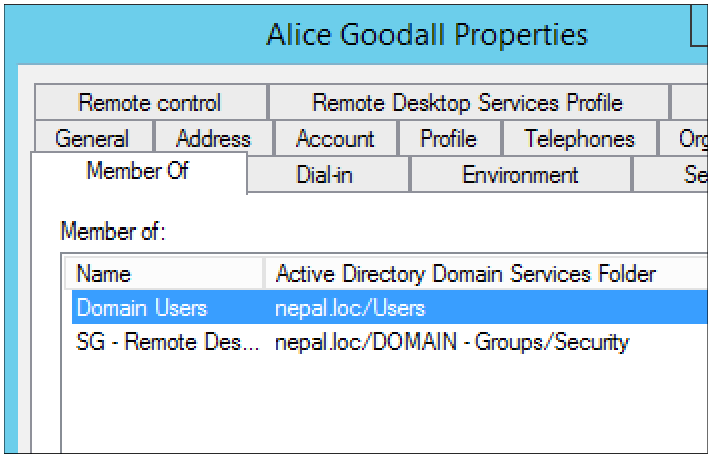
Using similar steps another GPO was created. The GPO was named 'LockRegistry'. GPMC was opened by right clicking this GPO from Group Policy Objects of the domain and selecting Edit. 'User Configuration\Policies\Administrative Templates\System\Prevent access to registry editing tools' was Enabled. This would prevent users of this group from editing the registry.

Next the rules were set by executing 'gpupdate /force' command from PowerShell. The Group Policy settings' output was exported to a html file named 'GPResult.html' for viewing the settings. All the enabled settings were visible in this file.

Remote Connection Setup

A new user named 'Alice Goodall' with logon name of agoodall was added using New → User from right click menu of Users in 'Active Directory Users and Computers'. Alice was added to 'SG – Remote Desktop Users' group that was created above by right-clicking on Alice and selecting Properties and clicking on Add from 'Member of' tab (see Fig 2.). In addition to adding Alice to 'SC – Remote Desktop Users' the user Bob was added to this group. This way Bob who is an Administrator can connect to the member server and do administrative tasks.

Figure 2: Adding groups to Alice Goodall



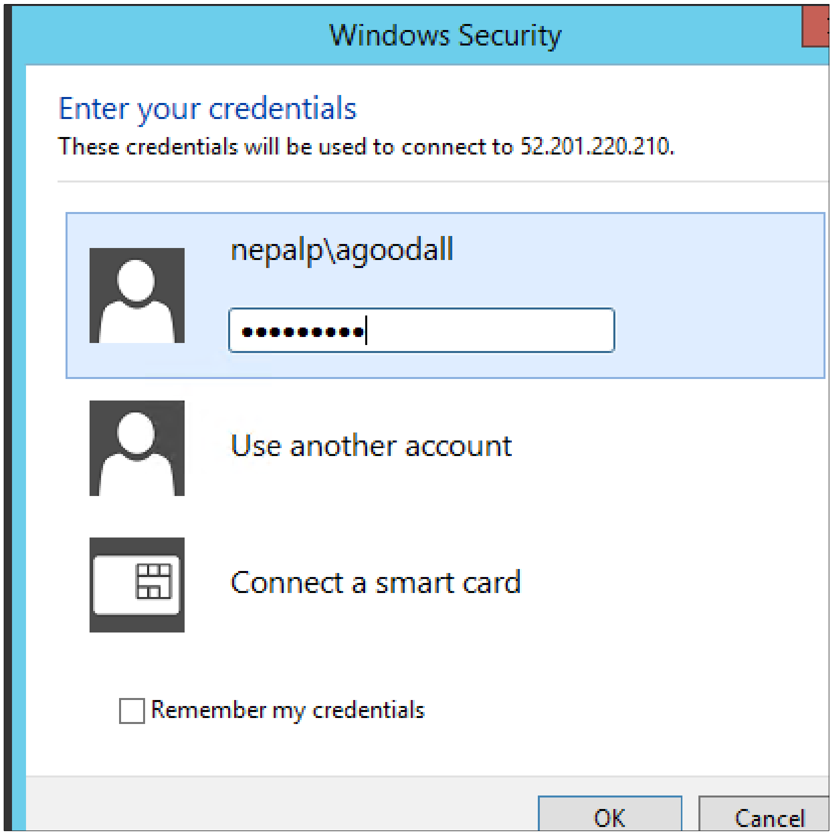
Alice Goodall Properties

Member of:

Name	Active Directory Domain Services Folder
Domain Users	nepal.loc/Users
SG - Remote Des...	nepal.loc/DOMAIN - Groups/Security

Member server was next configured to accept remote connections. The member server would be logged in using account and access created above. The member server was RDP into from the domain server. And Remote Settings was selected from 'System' window that opened by right-click Start button. It was made sure that 'Allow remote connections to this computer' was selected. 'Select Users …' button was clicked and 'SG – Remote Desktop Users' GPO was searched and added. The RDP from the member server was exited back to domain server. The member server was again connected through remote connection, but this time using Alice Goodall's login credentials (see Fig 3.)

Figure 3: Login using agoodall account into member server



Windows Security

Enter your credentials

These credentials will be used to connect to 52.201.220.210.

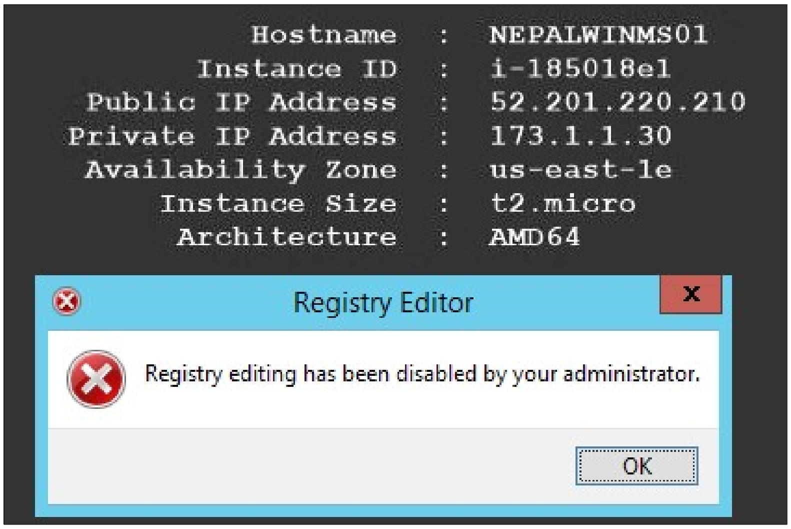
nepalp\agoodall

••••••••••

□ Remember my credentials

If the user tried to edit the registry by typing regedit.exe from PowerShell an error dialog would pop-up indicating that registry editing had been disabled for this account (see Fig 4.). However an Administrator (Bob) would be able to change the registry.

Figure 4: Registry editing disabled



```
             Hostname  :  NEPALWINMS01
          Instance ID  :  i-185018e1
    Public IP Address  :  52.201.220.210
   Private IP Address  :  173.1.1.30
    Availability Zone  :  us-east-1e
        Instance Size  :  t2.micro
         Architecture  :  AMD64
```

Registry Editor

Registry editing has been disabled by your administrator.

Observations

This lab experimented with Group Policy and authorization of resources to different groups. A user was created and added to a specific group that had some restrictions in terms of what the user could do on the computer. As could be seen throughout the lab and different options the focal point or main components of Group Policy was Users and Computers. Access to resources was configured for users that were part of certain group. Group Policy settings are organized using a Processing Order. First the Local GP objects are processed. Then Site, Domain and Organizational Unit objects are processed in sequence. Software and Windows settings and administrative templates can be applied to each components of the Group Policy Object. Local Group Policy is one of the group policies applied to each computer. However, domain object can have access to multiple domain-linked GPO. In the Member Server unless added as Domain Admin the user cannot have Administrative privileges. This signifies that a computer/resource added to a group has access to members associated with that group. In this lab few policies were applied. There are other settings that and Administrator can utilize. One of them is 'Custom

User Interface'. The Admin can setup Custom User Interface to a group so that it applies to a certain group. Another option that can be useful to an Admin would be preventing access to the command prompt. If the users of a group use specific software, it might be a good idea to prevent them from running any scripts from the command line. The last option for such users could be enabling 'Run only specified Windows applications'. It prevents the users from running applications other than specified by the admin.