

Introduction to System Administration

CSCI 4417/5417

ETSU - Department of Computing

Lab 7 - Group Policy

Spring 2016

Jack Ramsey, Lecturer

Introduction

In this lab, we will create a couple of Group Policy Objects on our Windows Domain Controller, push them out to the Member Server, and test them.

The GPOs will need to do the following:

- Enable Remote Desktop Service
- Open the Firewall to allow Remote Desktop
- Only allow certain users to logon remotely
- Restrict domain users from editing servers' registries

Backup Instances

In previous labs, some of us managed to brick our instances so that we couldn't recover (or log in to) them. So, we'll start this lab with a little preventative maintenance.

1. Log in to the AWS service and navigate to the EC2 dashboard
2. Select your Windows DC instance
3. Click on actions -> Image -> Create Image
4. In the dialog that launches, give your image a name and description

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination	Encrypted
Root	/dev/sda1	snap-f38cdb84	30	General Purpose SSD (GP2)	90 / 3000	<input checked="" type="checkbox"/>	Not Encrypted

Figure 1: Creating machine images (AMIs)

Note I used today's date as part of the name to keep it easily distinguishable from other images that may exist.

5. Click 'Create Image'
6. Repeat Steps 2-4 for your (public) Windows MS instance. You can create a third image for the MS instance on your private subnet if you wish, but today we'll just be using the two public subnet instances

CREATE A SECURITY GROUP (WINDOWS, NOT AWS)

When we created user Bob during the Active Directory lab, we made him a member of the Domain Admins group, which by default has remote access permission. But what if we want to allow selected users permission to access our servers remotely *without* giving them admin permissions? To accomplish this, we'll create a new security group and configure it so that its members can access the servers on our domain remotely. Then, we'll create a new user and make her a member of that group. We'll create a second GPO that prevents domain users from editing the servers' registries. Then, we'll test our new GPOs by logging in to the Windows member server and trying to run the registry editor.

1. Launch both your Windows Domain Controller and Member Server instances. Once the DC server is up and running, RDP to it
2. Open up Active Directory Users and Computers (under Tools in the Server Manager). Note: Some of these screen shots are a little old – your domain's TLD should be 'loc,' not 'local,' as is pictured below.

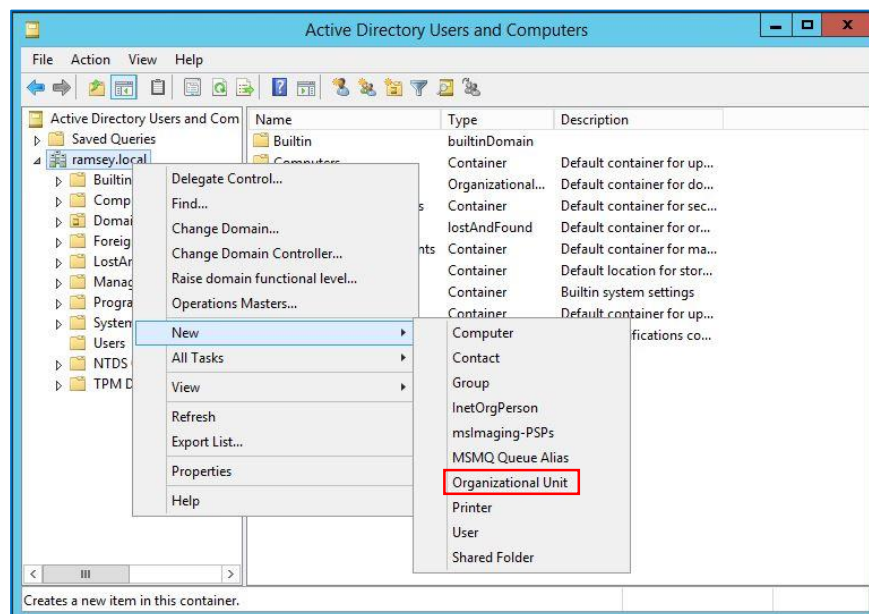


Figure 2: Creating a new OU

3. Create an Organizational Unit (OU) called "DOMAIN – Groups" by right-clicking on your domain and selecting New -> Organizational Unit

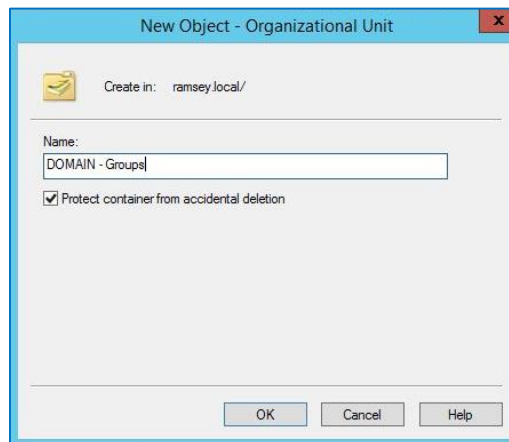


Figure 3: Naming the new OU

4. Under your DOMAIN - Groups OU create another OU called "Security" by right-clicking on 'DOMAIN - Groups, and selecting New -> Organizational Unit. This is where we will hold all of our security groups
5. Right-click on Security and select New -> Group
6. Give the group a name. Name it "SG – Remote Desktop Users" – Leave the scope 'Global'

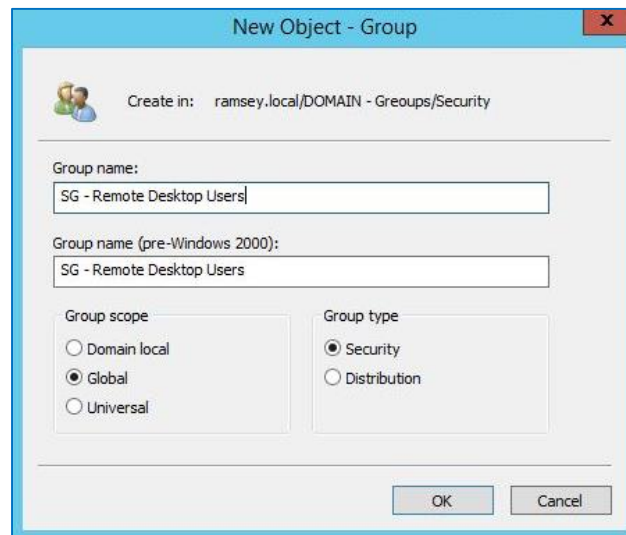


Figure 4: RD Users Group

Create the GPO

Now that we have a security group, we need to enable RDP and allow only members of this group to connect to our systems.

1. On the Run Screen (Right-click the Metro button, select 'Run') type: **gpmc.msc**. This will pull up the Group Policy Management Console. Alternatively, you can launch the Server Manager, click on 'Tools' and select 'Group Policy Management'

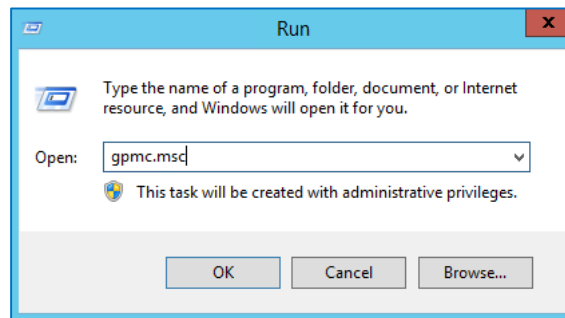


Figure 5: Running gpmc.msc from the Run Menu

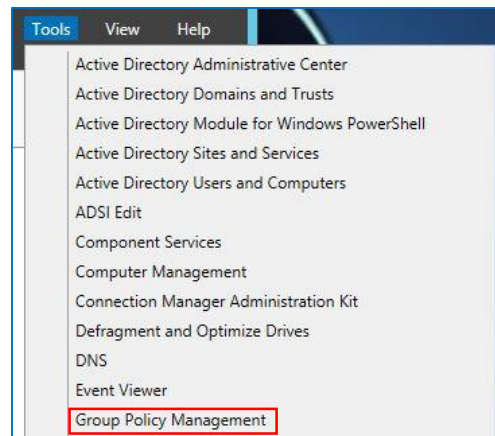


Figure 6: Launching the GPMC from the Server Manager

2. Expand the Forest and Domains containers on the left. Right click on your domain and select "Create a GPO in this domain, and Link it here...". Creating this GPO at the root of the domain allows access to all servers and computers in the domain. This might not be exactly what you

want to do. If your situation happened to be different, then you'd select the OU you want this policy to apply to, rather than the entire domain

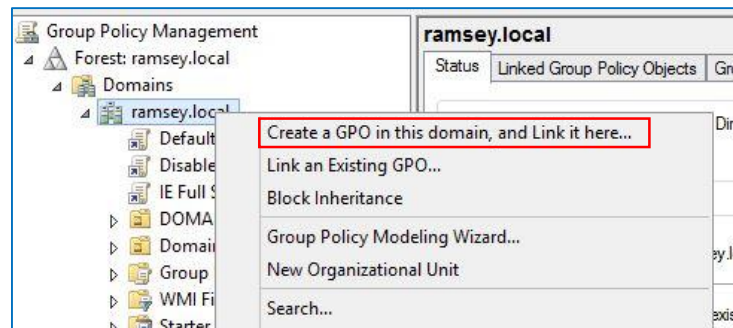


Figure 7: Creating and linking a GPO to a domain

3. Name the GPO "Enable RDP". This will create a blank GPO and a link to it
4. Expand the lastname.loc domain on the left, if necessary, to display the Group Policy Objects. Select Group Policy Objects. Right click the Enable RDP GPO and select "Edit..."

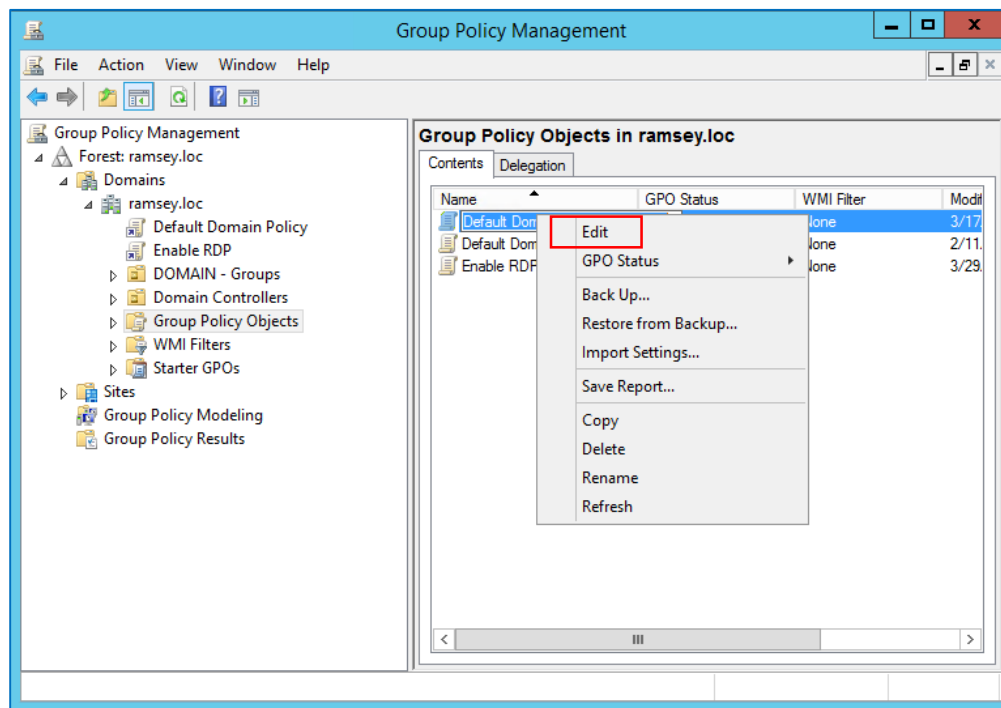


Figure 8: Editing the new GPO

5. This will pull up the Group Policy Management Editor

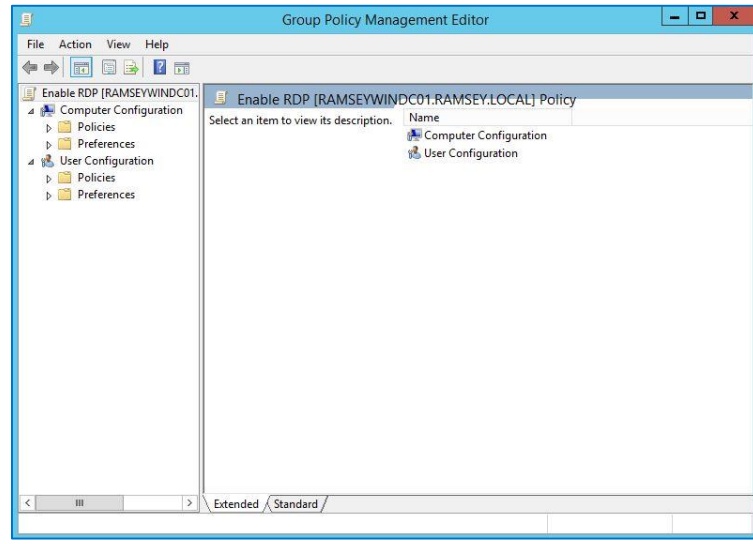
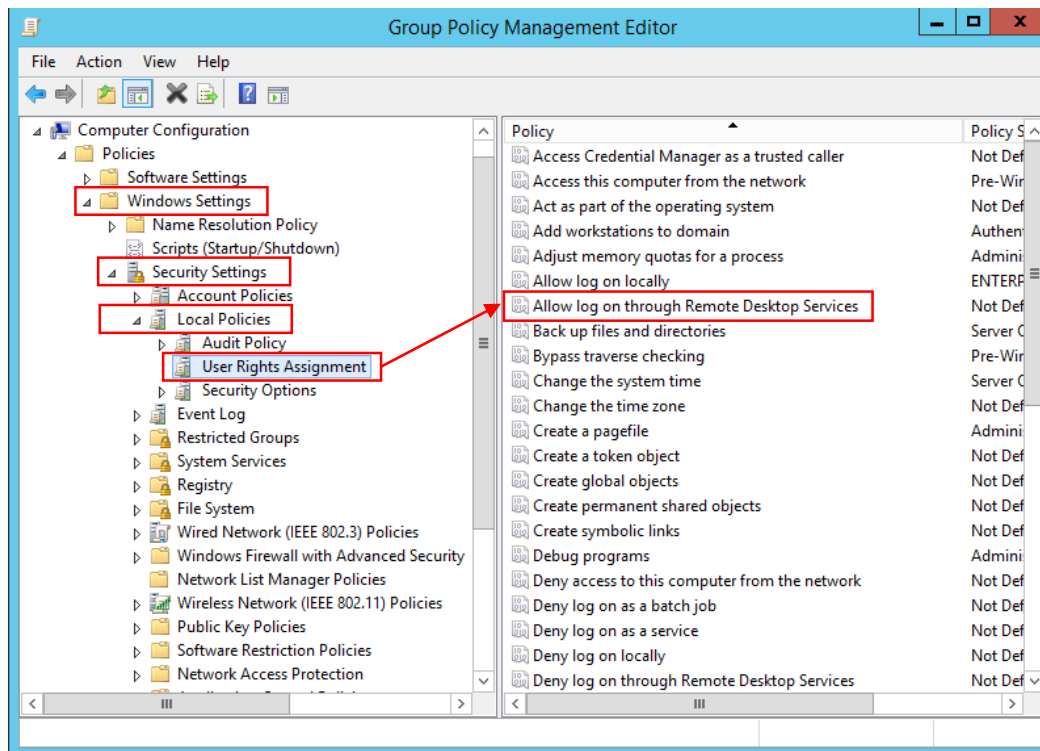


Figure 9: Group Policy Management Editor

6. Navigating the GPMC can be tricky because it is so granular. For this GPO, we are only going to be modifying Computer Settings. We need to enable RDP, open the Firewall, and allow the security group members. Set the following:
 - A. Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow Log on through Remote Desktop Services



B. Check 'Define these policy settings:'

C. Add Users or Group...

- D. Click 'Browse'. Click 'Advanced...' and then 'Find Now'. Browse and search for your Security Group, 'SG – Remote Desktop users'. Select it and click 'OK' until you're back at the Group Policy Management Editor

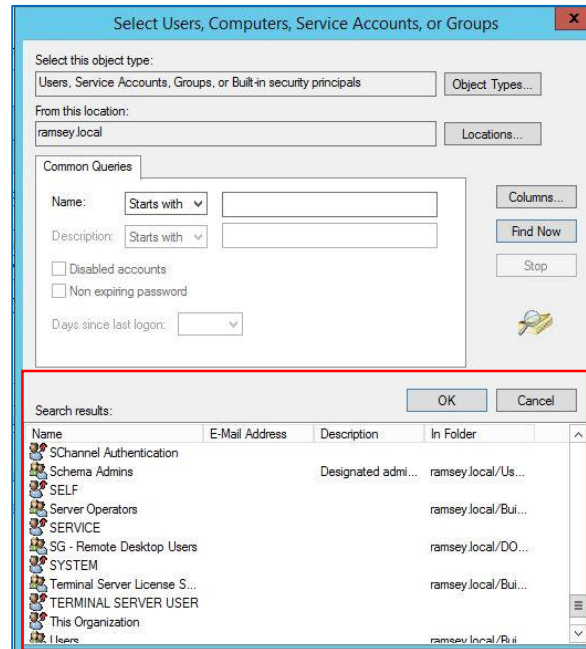


Figure 10: Browsing for Security Group

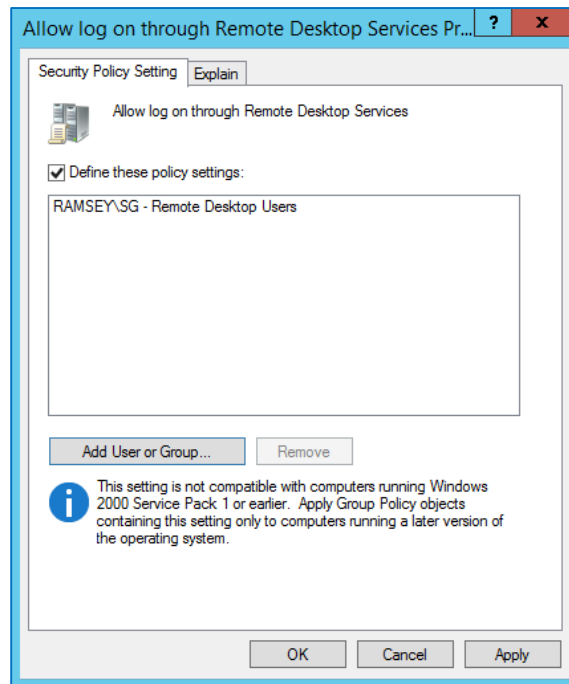


Figure 11: Applying group to new policy object

- E. Navigate to Computer Configuration\Policies\Windows Settings\Security Settings\Restricted Groups
- F. Right Click in the blank area and select Add Group...

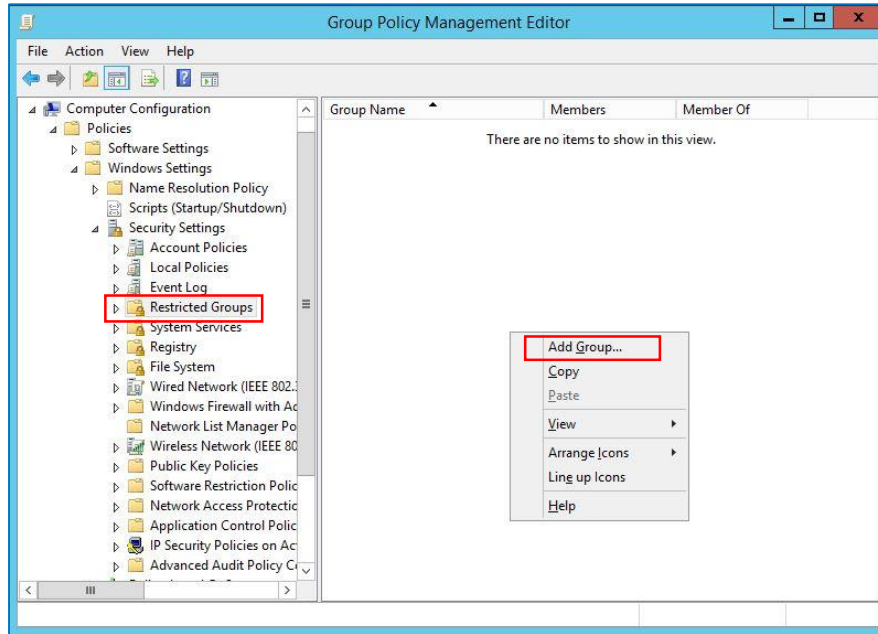


Figure 12: Adding the security group to the GPO

G. Browse and find “Remote Desktop Users”

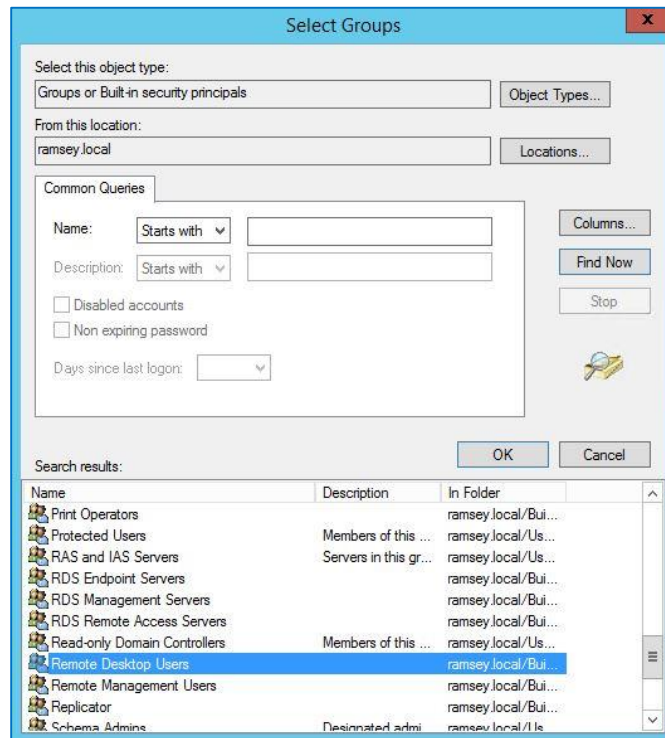


Figure 13: Adding Remote Desktop Users group to the GPO

H. Select OK

I. Select Add for “Members of this Group”

J. Browse and find your Security group. (This may throw an error the first time you select the group. Try again and it should work). Click OK

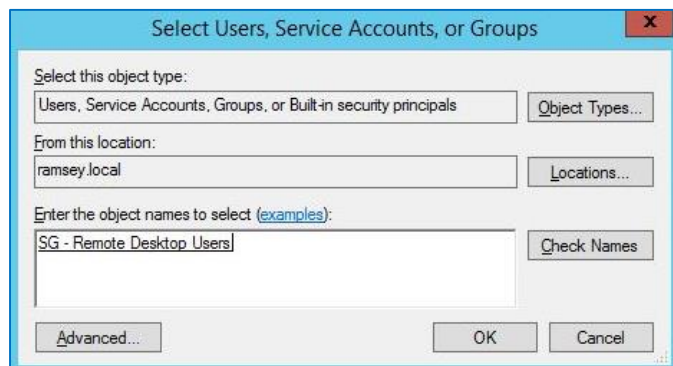


Figure 14: Browsing for the security group

- K. Navigate to Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile\Windows Firewall: Allow Inbound Remote Desktop exceptions (Double-click) and select **Enable**. Click OK

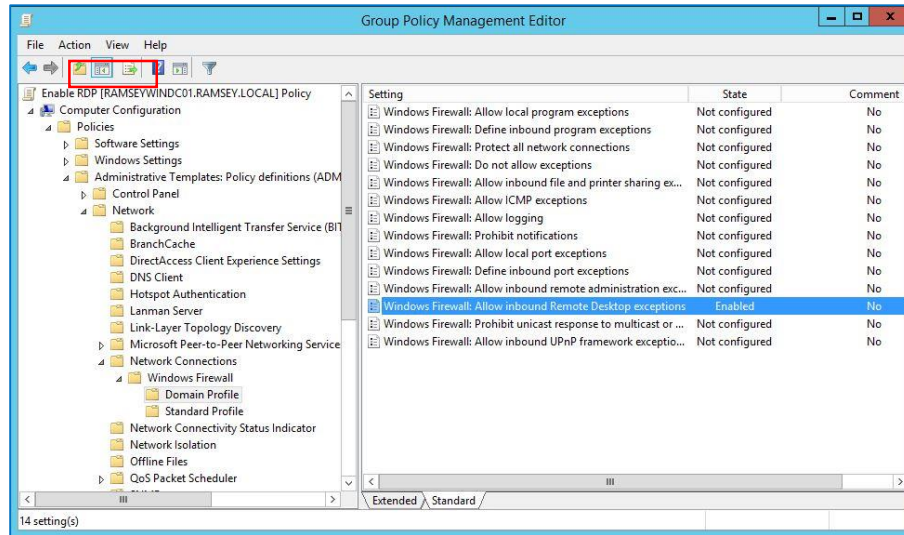


Figure 15: Allowing inbound Remote Desktop

- L. Navigate to Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections\Allow users to connect remotely by using Remote Desktop Services (Double-click): **Enabled** -> **OK**

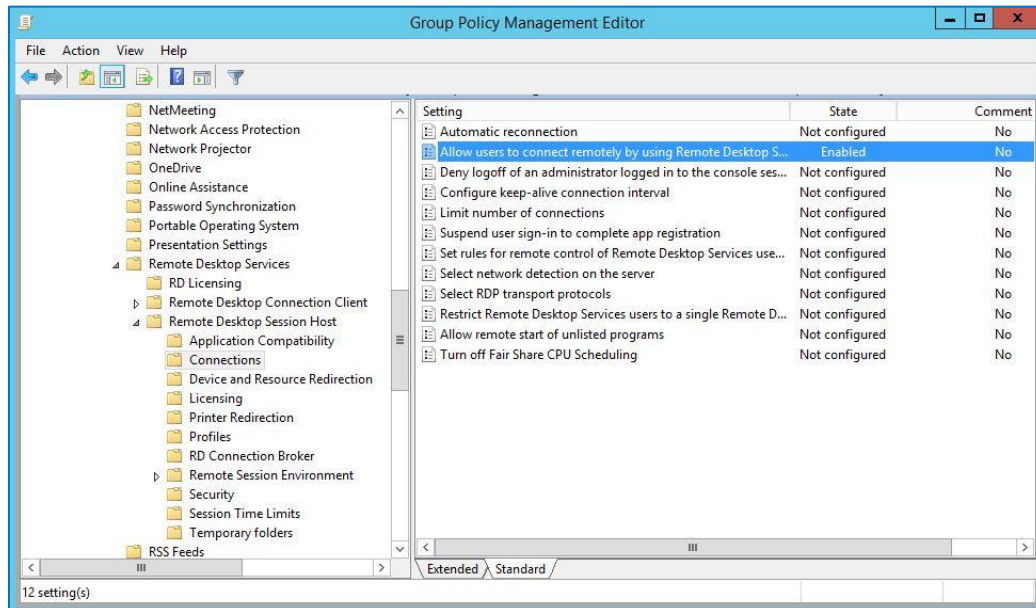


Figure 16: Allowing users to connect remotely

- M. Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require user authentication for remote connections by using Network Level Authentication. (Double-click): **Disabled** -> **OK**

N. RDP is now configured for domain users. **Close the GP Management Editor**

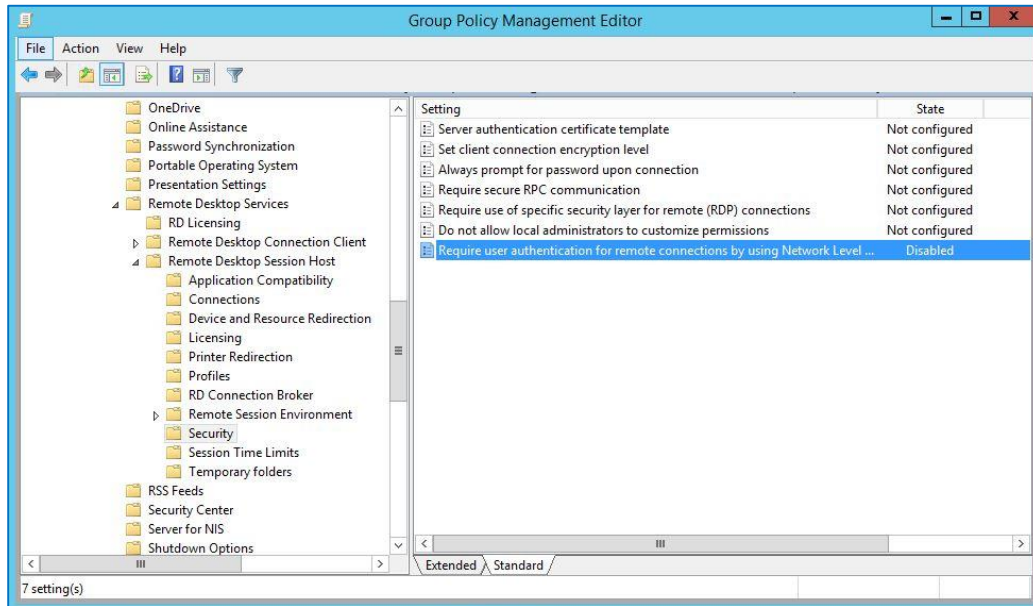


Figure 17: Disabling Network Level Authentication

GPO DISABLING REGEDIT

1. Time for the second GPO. This one will prevent domain users from altering the servers' registries. Once again, right-click on your domain in the GPMC and select 'Create a GPO in this domain, and Link it here...'
2. Name your new GPO 'LockRegistry'. Return to lastname.loc\Group Policy Objects and right-click on 'LockRegistry' in the GPMC and select 'Edit'.
3. Navigate to User Configuration\Policies\Administrative Templates\System\Prevent access to registry editing tools (Double-click): **Enable**. Close the GP Management Editor and the Group Policy Management Console

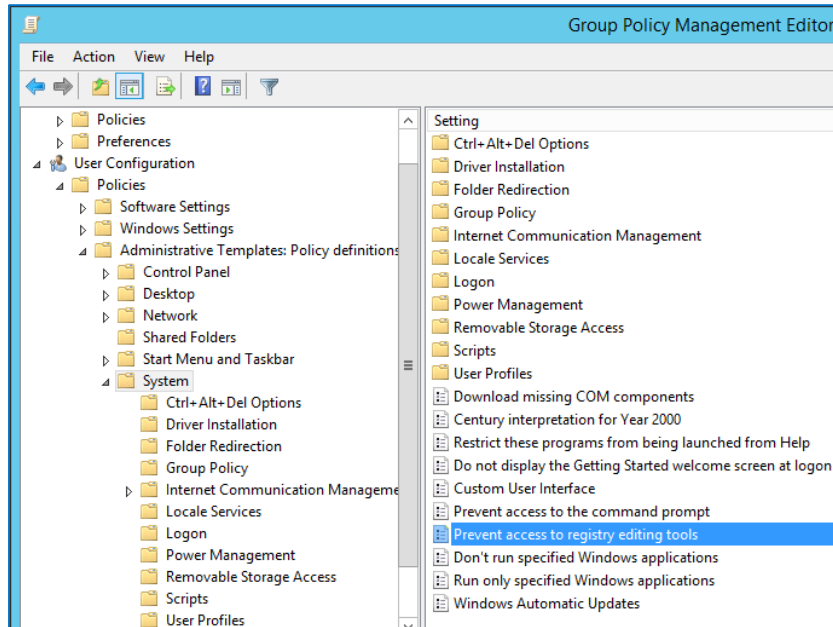


Figure 18: Preventing users' access to registry editor

4. Launch PowerShell as Administrator and enter

gpupdate /force

5. When Step 7 is complete, enter

gpresult /H C:\Users\Administrator\Desktop\GPResult.html

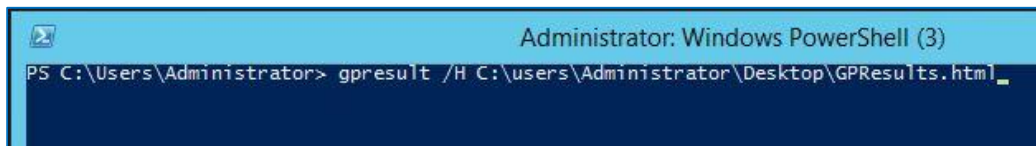
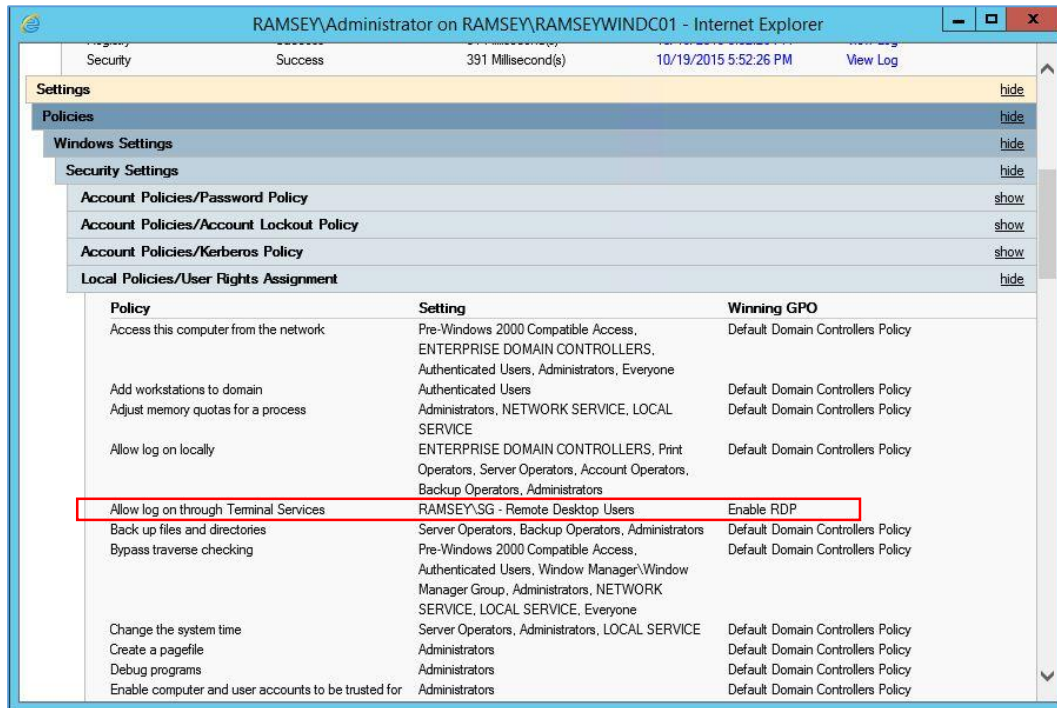


Figure 19: Generating GP result report

This will generate an .html-formatted report of the current state of your Group Policy and save it on your Desktop. Open the report by double-clicking on it. Observe the following:



Policy	Setting	Winning GPO
Access this computer from the network	Pre-Windows 2000 Compatible Access, ENTERPRISE DOMAIN CONTROLLERS, Authenticated Users, Administrators, Everyone	Default Domain Controllers Policy
Add workstations to domain	Authenticated Users	Default Domain Controllers Policy
Adjust memory quotas for a process	Administrators, NETWORK SERVICE, LOCAL SERVICE	Default Domain Controllers Policy
Allow log on locally	ENTERPRISE DOMAIN CONTROLLERS, Print Operators, Server Operators, Account Operators, Backup Operators, Administrators	Default Domain Controllers Policy
Allow log on through Terminal Services	RAMSEY\SG - Remote Desktop Users	Enable RDP
Back up files and directories	Server Operators, Backup Operators, Administrators	Default Domain Controllers Policy
Bypass traverse checking	Pre-Windows 2000 Compatible Access, Authenticated Users, Window Manager\Window Manager Group, Administrators, NETWORK SERVICE, LOCAL SERVICE, Everyone	Default Domain Controllers Policy
Change the system time	Server Operators, Administrators, LOCAL SERVICE	Default Domain Controllers Policy
Create a pagefile	Administrators	Default Domain Controllers Policy
Debug programs	Administrators	Default Domain Controllers Policy
Enable computer and user accounts to be trusted for	Administrators	Default Domain Controllers Policy

Figure 20: Local Policies/User Rights Assignment

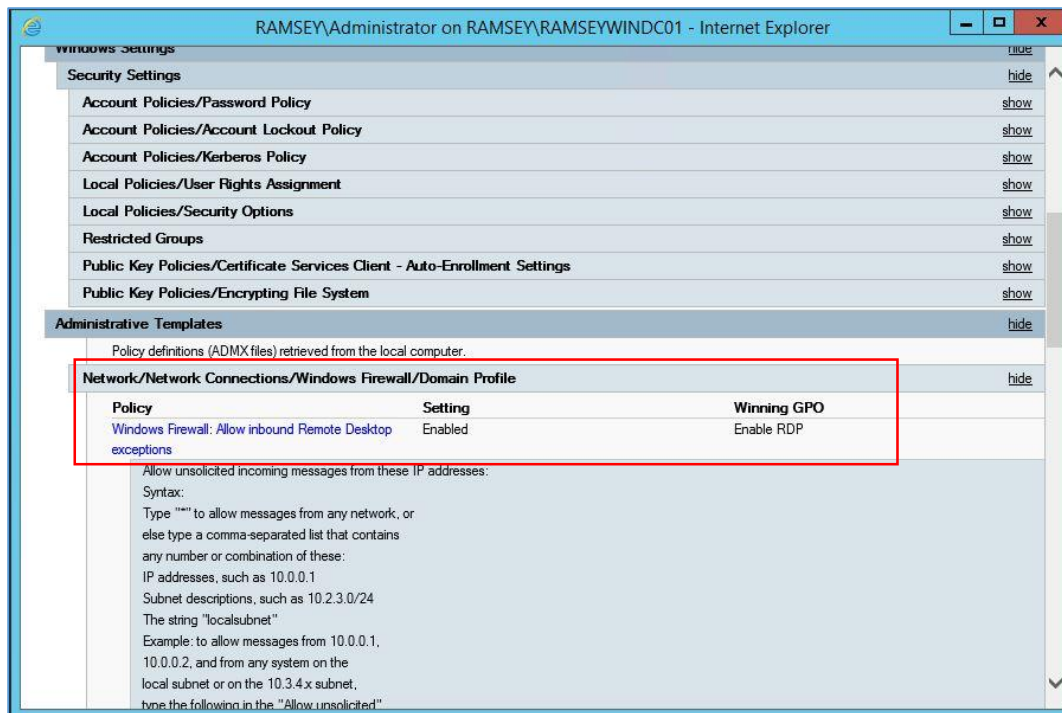


Figure 21: Administrative Templates



Figure 22: GPO to enable RDP

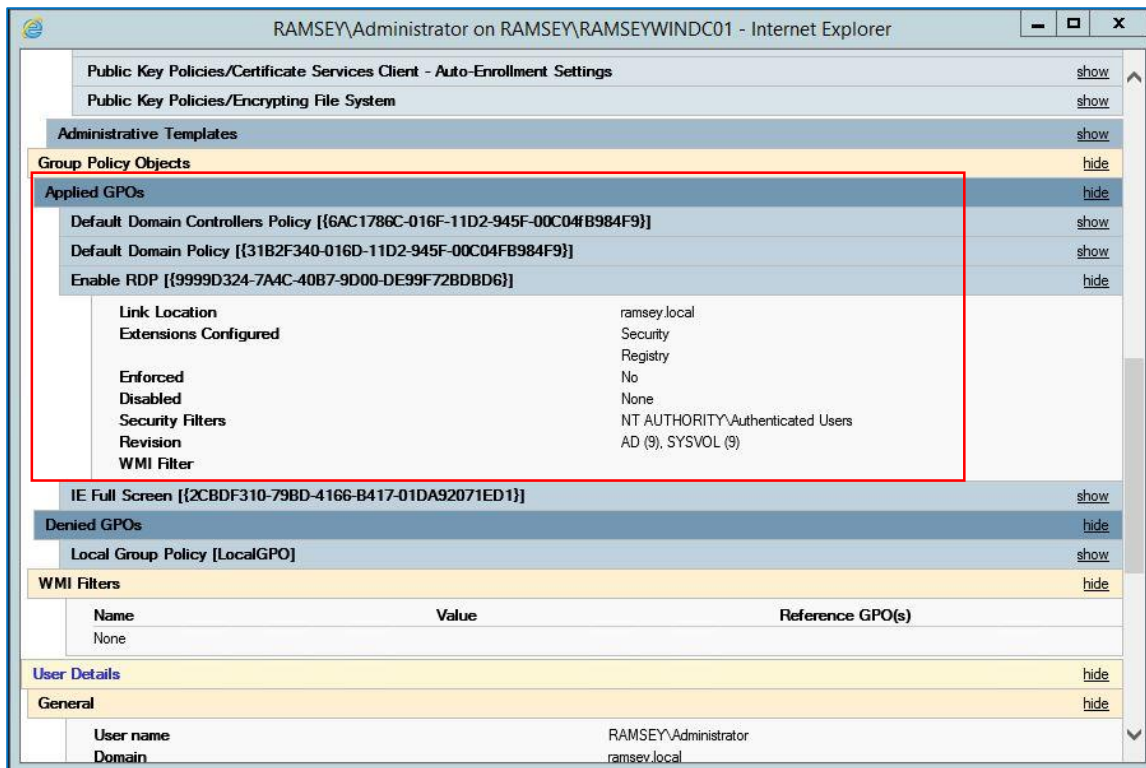


Figure 23: Applied GPOs

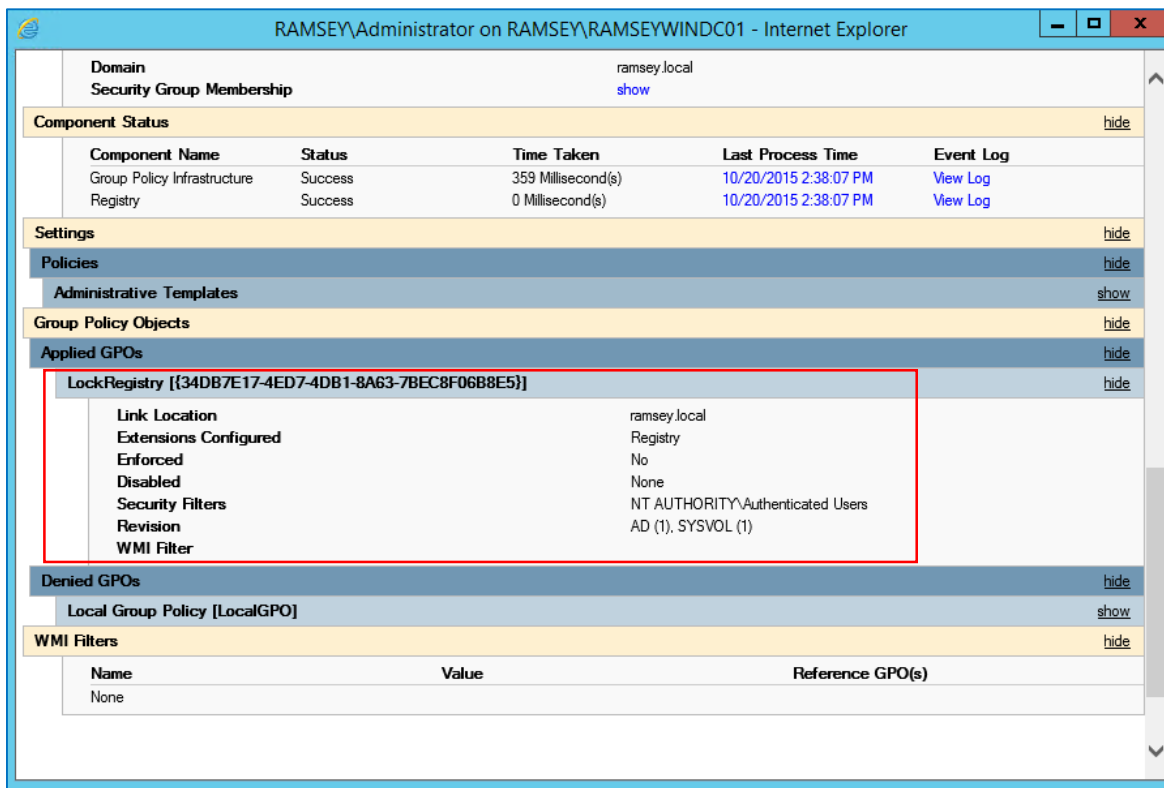


Figure 24: LockRegistry GPO

Create a new user

1. Launch Active Directory Users and Computers
2. Right-click on Users, select 'New' and 'User'
3. Make your new user's name 'Alice Goodall' with a user logon name of 'agoodall'
4. Give Alice a password (PasswOrd!) and set it to never expire. Click 'OK'
5. Right-click on Alice and select Properties. Select the 'Member of' tab
6. Click 'Add'
7. Type 'SG' into the search window and click 'Check Names'
8. Select the 'SG - Remote Desktop Users' group and click 'OK'. Click 'OK' again
9. **Add the Domain Admins group to the new security group as well.** If you don't, the only person who'll be able to log in to your instances will be Alice

Configure Member Server to Accept Remote Connections

Now, we have to tell the member server to accept remote connections.

1. Log in to the member server as Administrator from your Domain Controller
2. Right-click on the Start button and select 'System'
3. Click on 'Remote Settings'
4. Make sure 'Allow remote connections to this computer' is selected and click on 'Select Users...'

- Click 'Add...' Once again, navigate to your 'SG - Remote Desktop Users' group and select it and click 'OK'

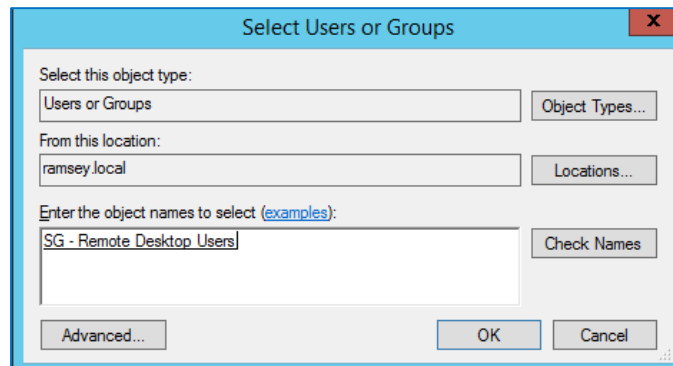


Figure 25: Selecting domain security group for authorization of remote access

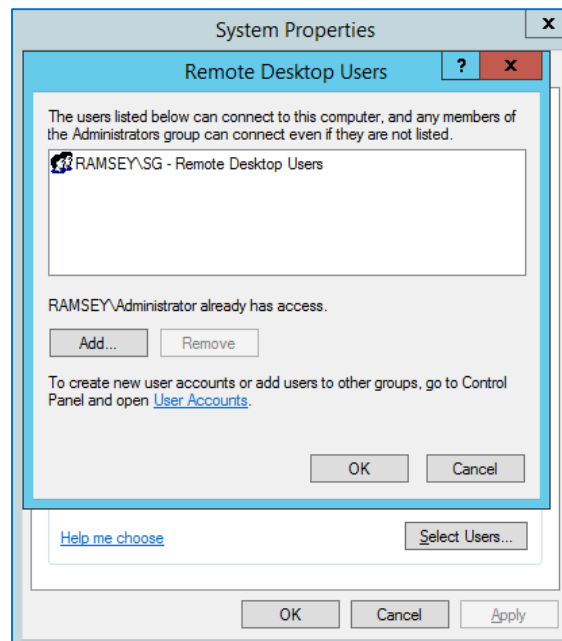


Figure 26: Adding the security group to authorized users list

- Click 'OK' and 'OK' again to exit
- Exit RDP
- Launch RDP again, but this time, try to log in as *lastname\agoodall* (you have to specify the domain name in order to log in as a domain user). If all goes well, you should be authenticated.
- Once agoodall is logged on, launch PowerShell and enter

regedit.exe

10. If we were successful in deploying our GPOs, you should be blocked from running the registry editor

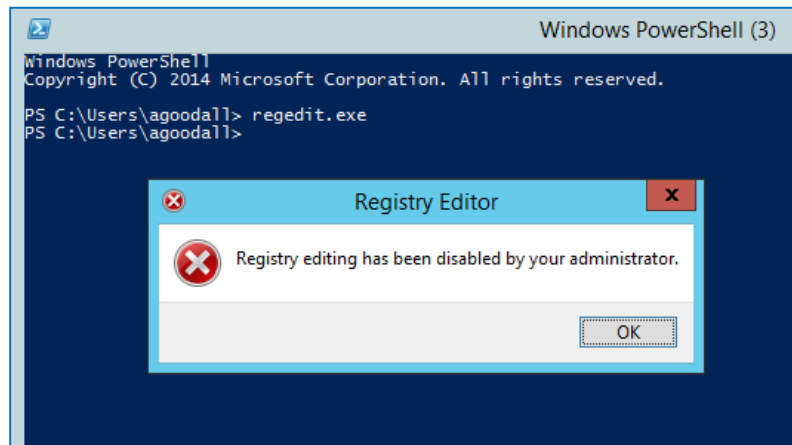


Figure 27: Editing member server's registry blocked

11. Exit all of your instances and stop them.

12. Your lab report should be prepared in accordance with the lab guide and submitted by the beginning of class next Tuesday, April 5, 2016. While preparing your report, consider the following questions:
- What are the two main components of Group Policy?
 - What are the three settings that can be applied to each component?
 - How are Group Policy settings organized?
 - What is the difference between Local Group Policy and Domain-based (or Active Directory-based) Group Policy?
 - If you log in to your Member Server as Administrator and try to run regedit.exe, you'll find that the new GPO even prevents Domain Admins from running the Registry Editor. What could you do to allow Administrators to run regedit.exe while still denying access to the Registry Editor to all other users?
 - We've explored a couple of GPOs in this lab that might be useful in a production environment. Name three other policies that might be of use to system administration; that would protect the infrastructure and/or limit permissions to appropriate user groups.