Lab 5: Managing Group Policies

By: Ethan Holmes

Contents

Activity 5-2. Working with GPO Inheritance Blocking and Enforcement

In this activity, we will create a GPO for blocking access to features such as control panel and other parts of our window's system.

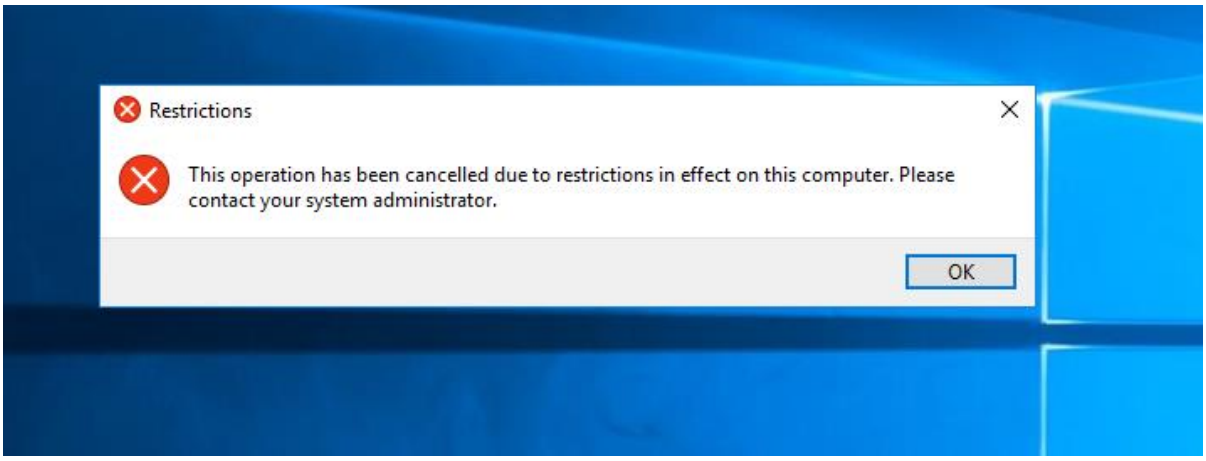
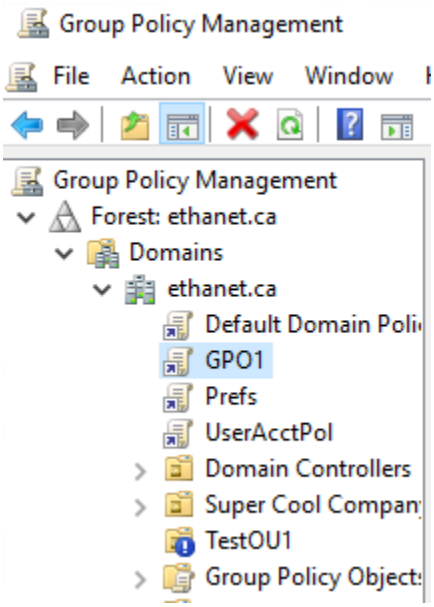


Figure 1: Domuser1 is blocked from accessing control panel



Here, we will block Inheritance on TestOU1 so that users in this group aren't subject to the group policy.

Figure 2: Inheritance disabled on TestOU1

Domuser1 can now access the control panel

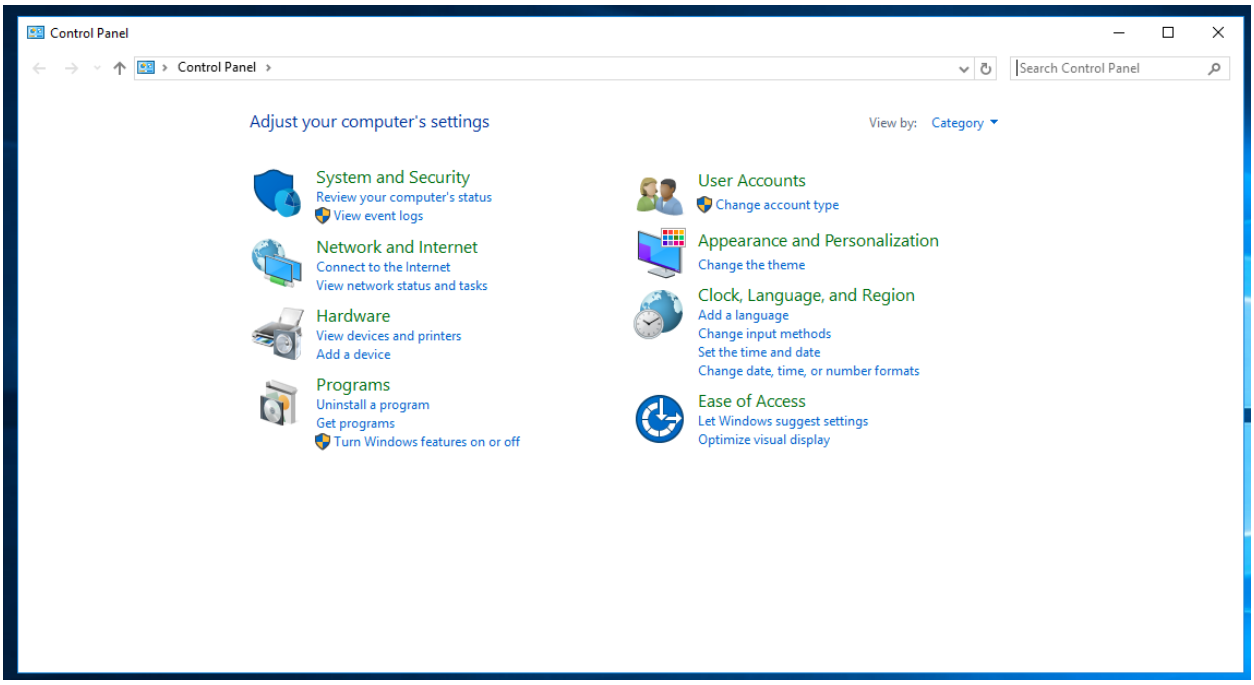
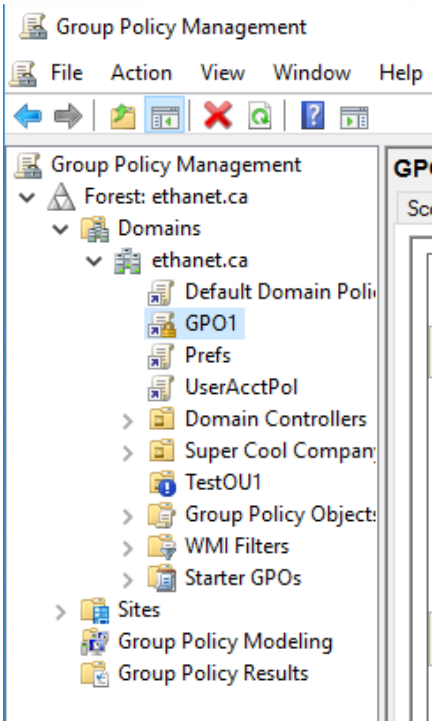


Figure 3: domuser1 can access the control panel because inheritance is disabled



We have now enforced the GPO1, which should overrule the disabled inheritance and once again disable control panel for all users in TestOU1

Figure 4: Enforcing TestOU1

Domuser1 on dm1 can now no longer access control panel because of the enforcement of the GPO1

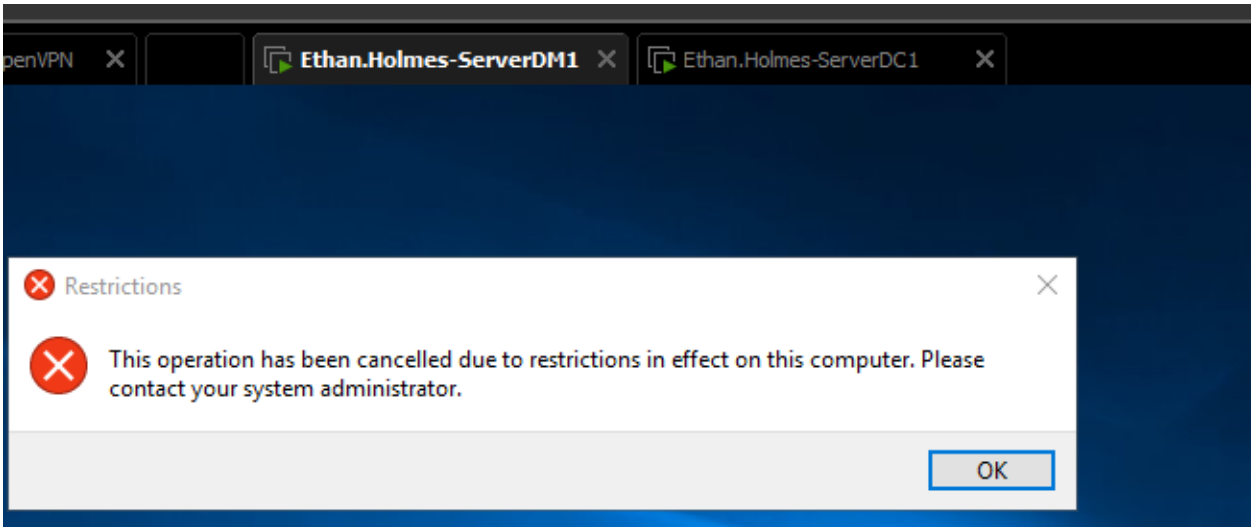


Figure 5: Enforcement overrules inheritance

Activity 5-3. Using GPO Security Filtering

In this activity, we will be using GPO filtering to change the default inheritance behavior of GPO processing.

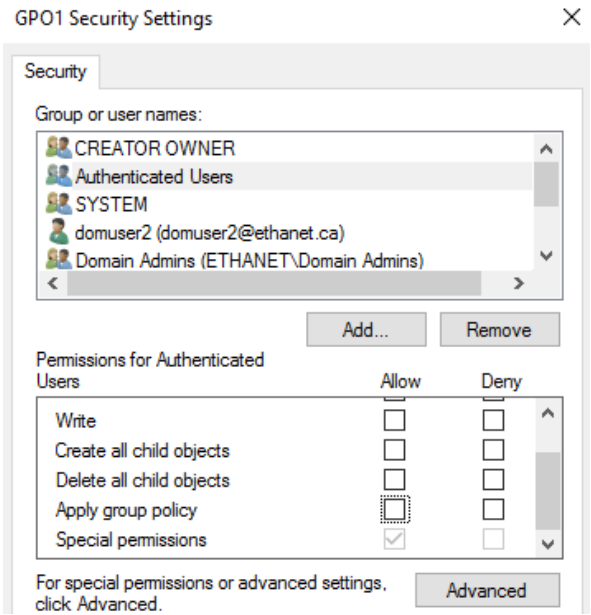


Figure 6: Disabling the application of group policy to all authenticated users

Here, in figure 6 and 7 below, we can see that we are disabling authenticated users from the GP, while adding domuser2 to the security filter, thus making domuser2 the only authenticated user who will have the GP applied to them.

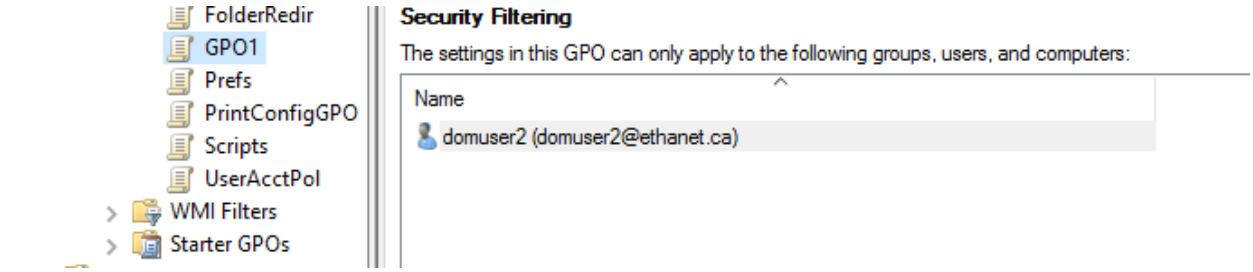


Figure 7: domuser2 apart of the security filtering

We can now demonstrate the control panel being disabled and GPO1 being in effect.

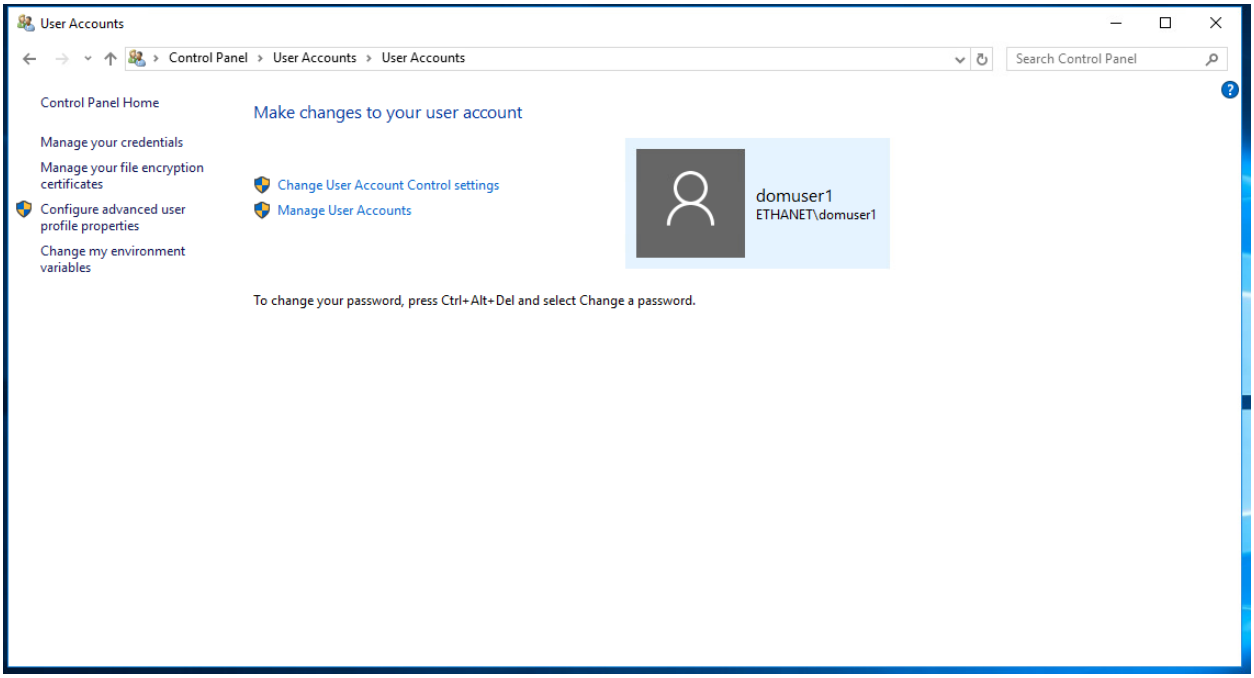


Figure 8: domuser1 can see control panel succesfully

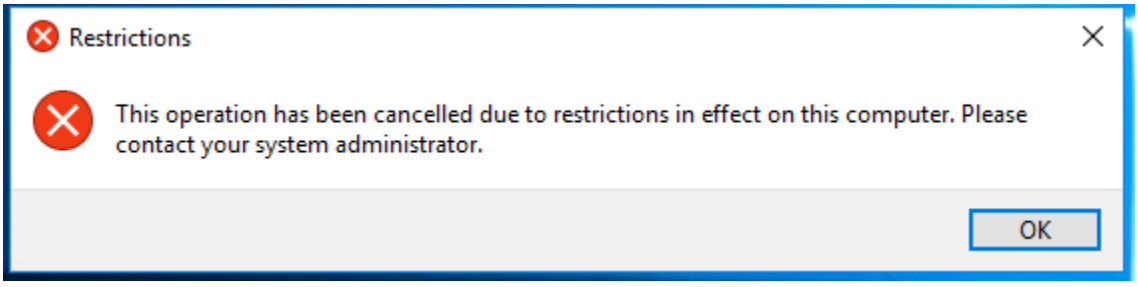


Figure 9: domuser2 cannot access control panel because of the security filtering

Activity 5-4. Using GPO Security Filtering for a Computer Account

Doing the same steps as the previous activity, but this time we will do it with computer accounts rather than user accounts.

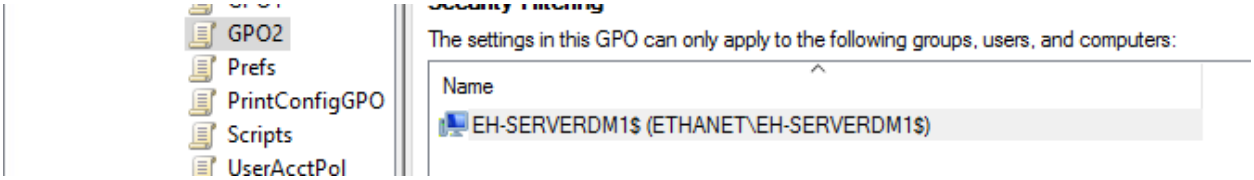
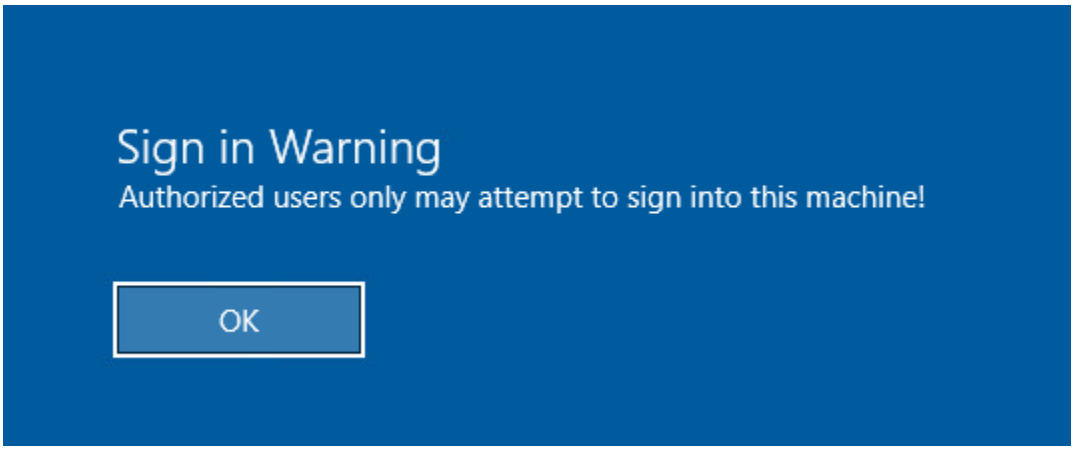


Figure 10: Security Filtering on GPO2 specific to serverdm1

Message we get when we add a warning messages that apply to the DM1 machine



Activity 5-5. Configuring Loopback Policy Processing

In this activity, we will configure loopback policies

After creating the MembersServers OU and applying ServerDM1 to it, we then made GPO3 which had various windows desktop policies applied to it.

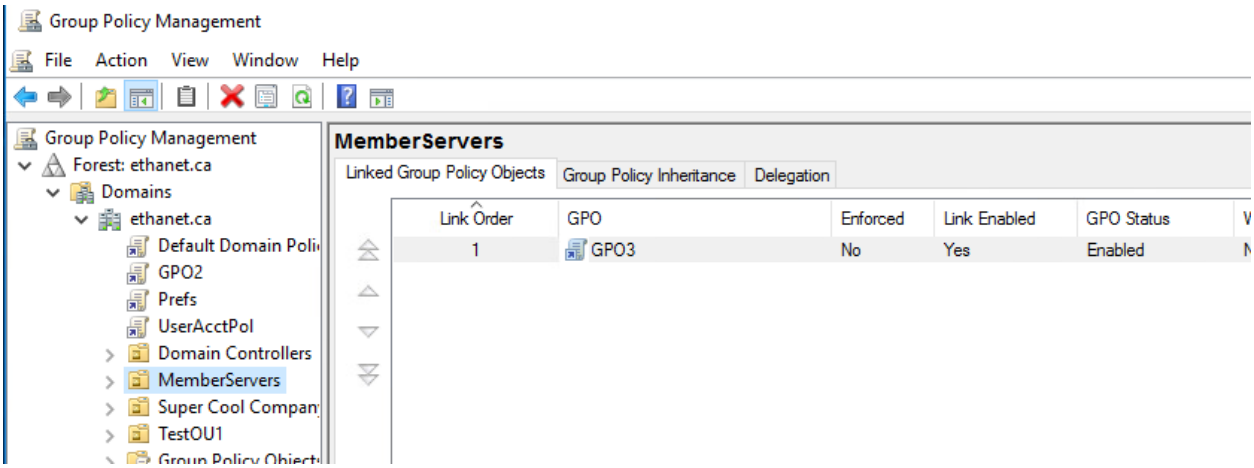


Figure 11: GPO3 created

However, after doing a gpupdate we still don't have our changes made, this is because we need to enable our Loopback processing, which allows us to apply user settings based on the computer, rather than where the user is

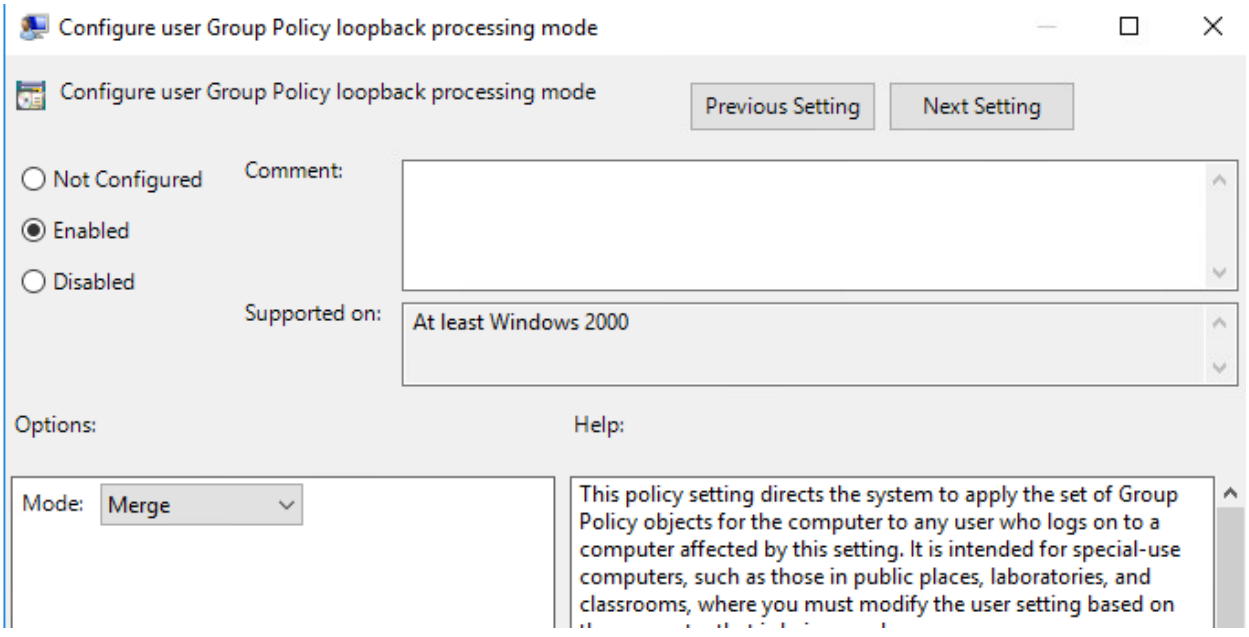
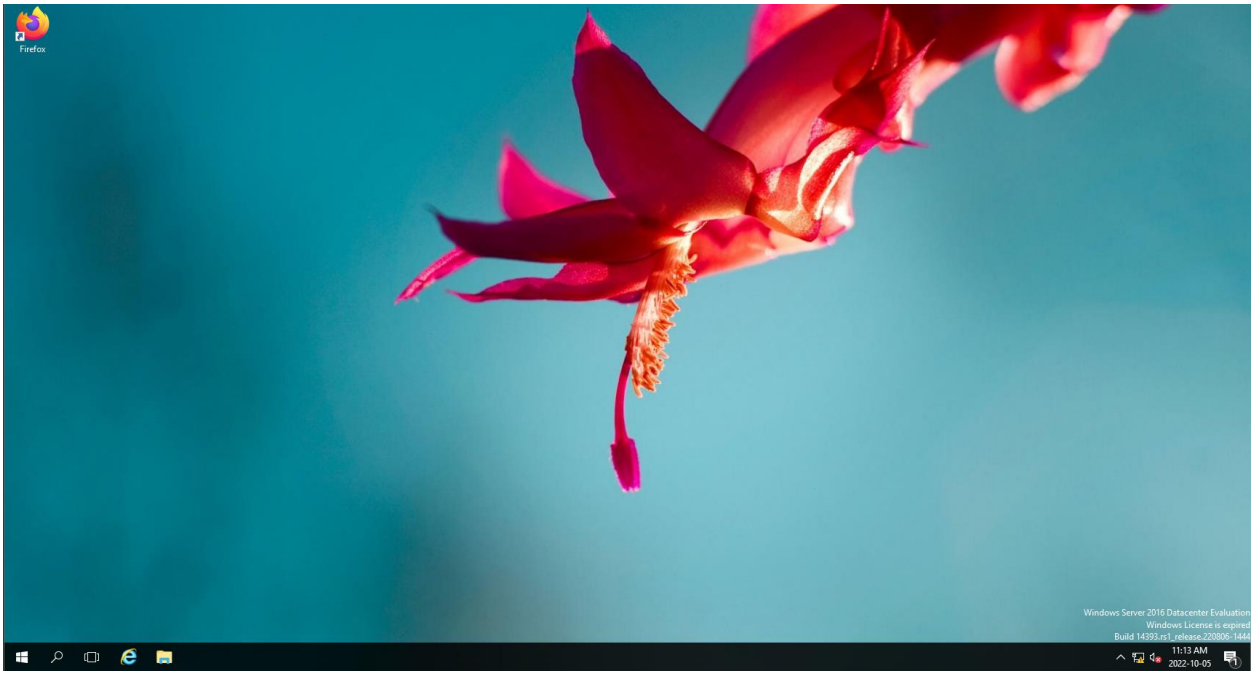


Figure 12: Enabling loopback policies

When we restart and sign into the machine again, we can see that the policies have taken effect.



Activity 5-6. Using Remote Group Policy Updates

In this activity, we will Configure the firewall for a remote group policy update on ServerDM1

The first thing that we will do is change some firewall rules, these are the following ones that we will change

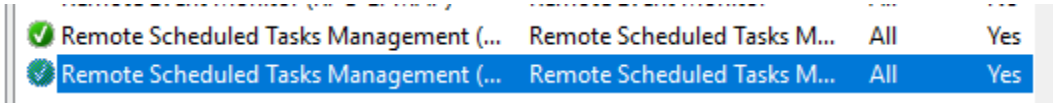


Figure 13: Firewall tasks being changed

We will now force a group policy update from our DC1

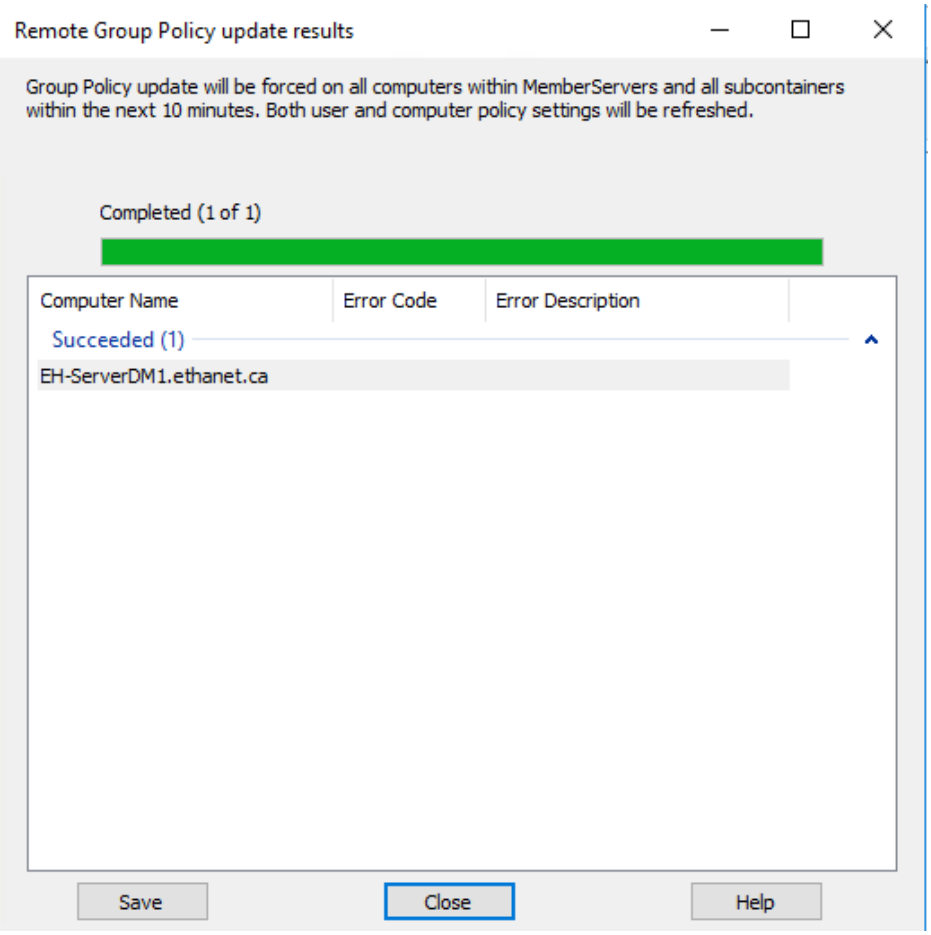
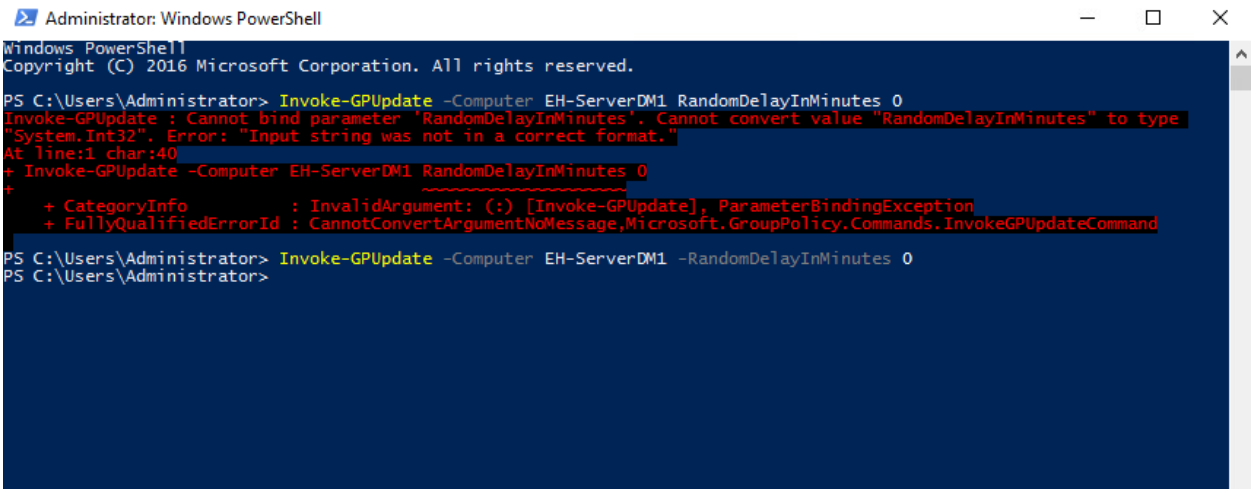


Figure 14: Remote GP policy update

We can also push the GPUpdate through PowerShell with the following command



Activity 5-7. Using Group Policy Results and Group Policy Modeling

In this activity, use the Group Policy Results Wizard to see how user and computer accounts are affected by group policy settings. Then you use the Group Policy Modeling Wizard to create a what-if scenario to see how accounts are affected if they're moved to a different OU

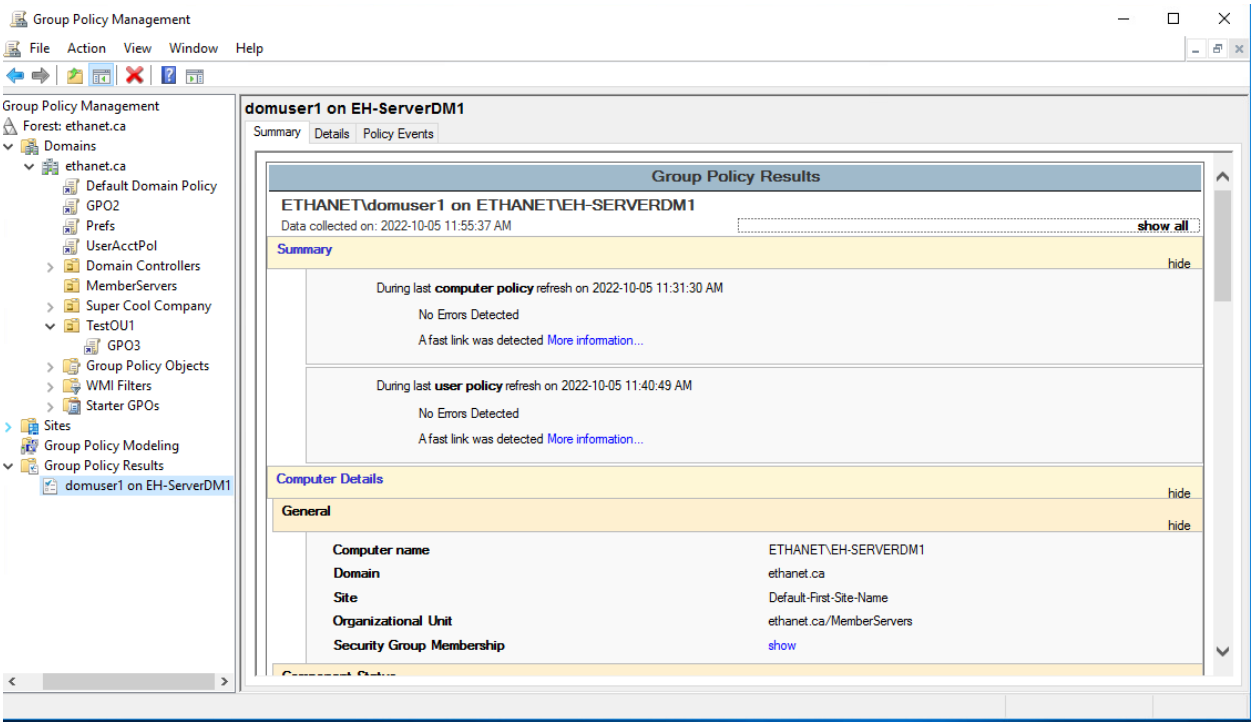


Figure 15: Policy results from scan

When we do a modelling scan, we get a second user report to look at

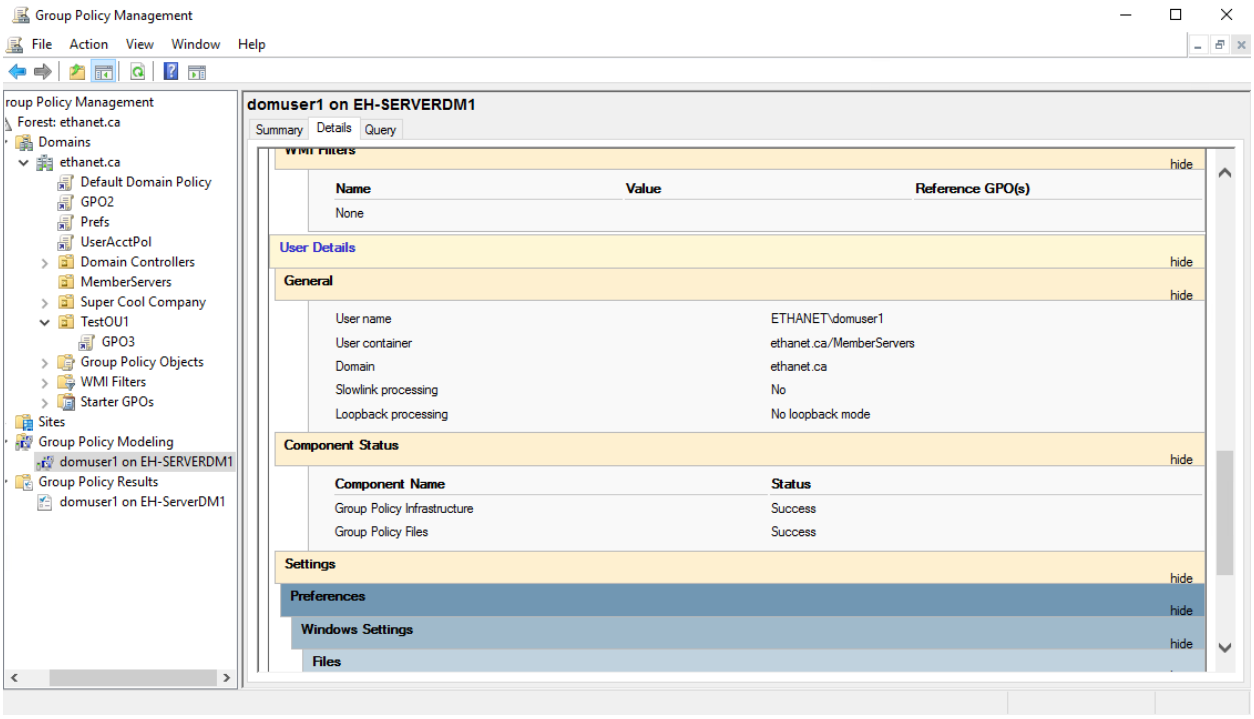


Figure 16: GP Modeling scan

Activity 5-8: Backing Up and Restoring a GPO

In this activity, we will create a backup and restore our GPO from that backup.

To start, I used the following command in PowerShell to save GPO1

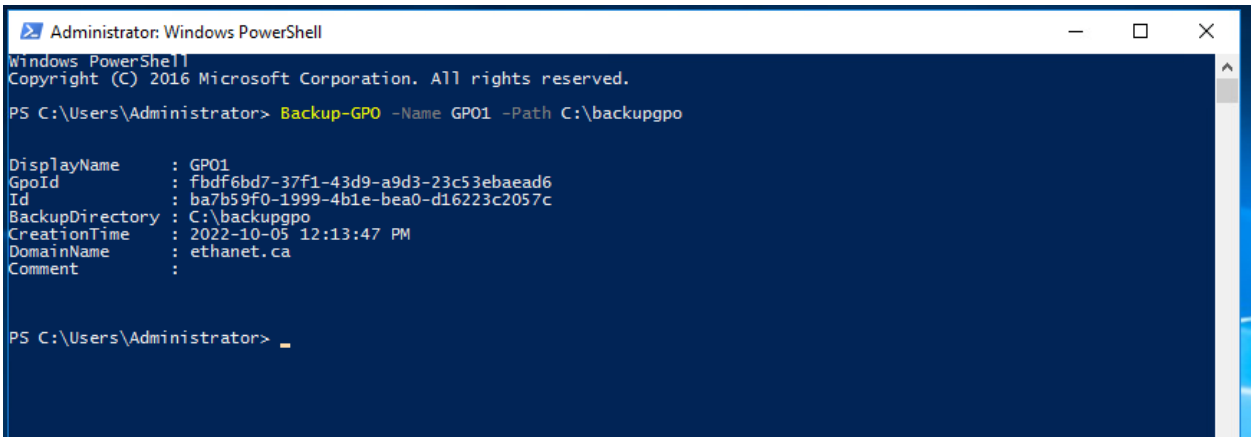


Figure 17: PowerShell command to save GPO1

We will make the following changes to GPO1

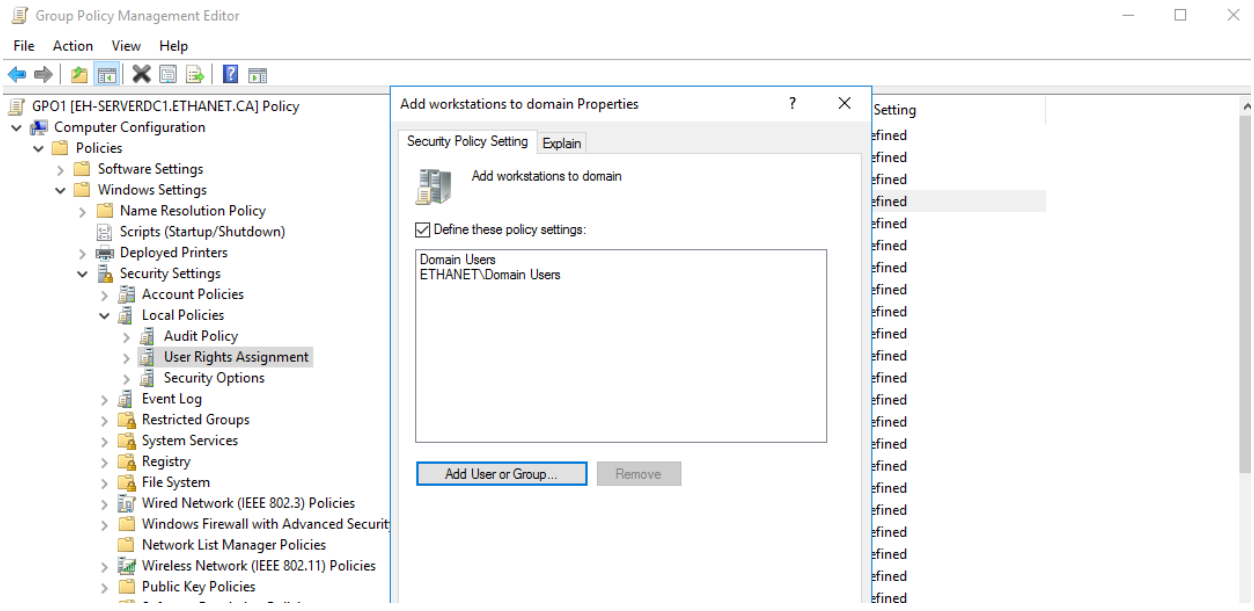


Figure 18: Changing the "Add workstations to domain" property

Once this is done, we can then use the following PowerShell command to revert to our previous GPO options

```
PS C:\Users\Administrator> Restore-GPO -Name GPO1 -Path C:\backupgpo

DisplayName      : GPO1
DomainName       : ethanet.ca
Owner            : ETHANET\Domain Admins
Id               : fbdf6bd7-37f1-43d9-a9d3-23c53ebaead6
GpoStatus        : AllSettingsEnabled
Description      :
CreationTime     : 2022-09-28 11:54:45 AM
ModificationTime : 2022-10-05 12:20:25 PM
UserVersion      : AD Version: 2, SysVol Version: 2
ComputerVersion  : AD Version: 6, SysVol Version: 6
WmiFilter        :


PS C:\Users\Administrator>
```

Figure 19: Restore GPO command to restore the GPO1

We can now see that we have reverted to our previous GPO1 before we made those changes,

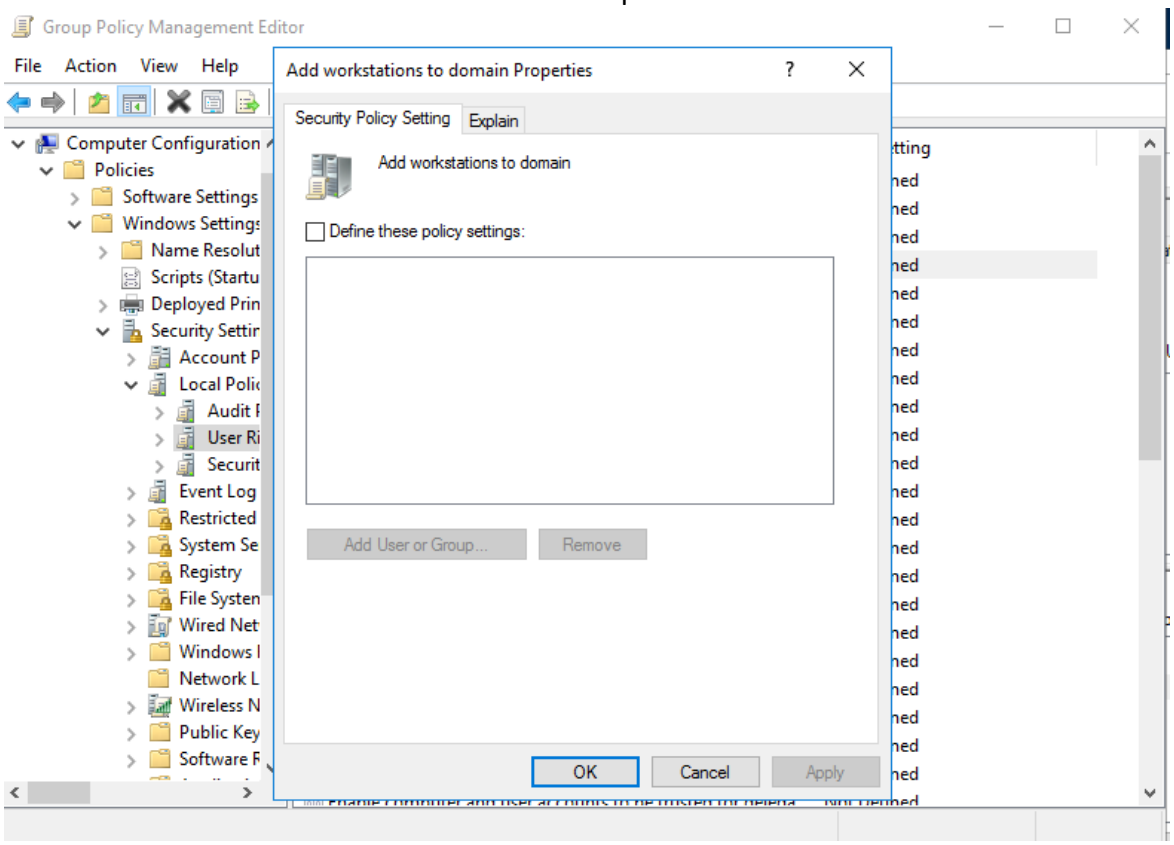


Figure 20: Reverted changes to our GPO1 after running the command

Conclusion

In this Lab, I learned lots about how to make loopback policies, and applying more Group Policies and how I can affect user start-up as well as computer start-up with these policies, as well as policy precedence using inheritance and enforcing, these were all neat policies to learn and I'm sure I will use them lots in my career.