Lab Report - Lab 9

Name: Tyler Burleson Date: 3/25/2024

Summary

In this lab we were tasked with creating a Group Policy Object in our Windows Domain Controller. Once our object is created, we need to push it to our member server and test if it is effective. Our objective Group Policy Object we wanted to create was “Restrict domain users from editing servers’ registries.” We started by logging on to AWS and RDP’ing into our Domain Controller. Once we were connected, we opened our Server Manager, clicked on the Tools drop down menu and selected Group Policy Management. Next, we right clicked our domain and created a GPO and linked it in the domain. Once we named our new GPO, “LockRegistry,” we opened its editor. We then navigated through the folders and added “Prevent access to registry editing tools.” Next, we opened PowerShell and forced updated our Group Policy. To check that our changes were made we ran “gpresult” to output an html file containing a report of all the new changes. Once we confirmed our changes, we needed to add them to a user and test it on our Member Server.

To do this we followed the same steps we’ve done in a previous lab; we opened our Server Manager, clicked the Tools dropdown menu, and selected Active Directory Users and Computers. Once inside we created a new user named Charles Tuna. Next, we navigated to our Member Server via RDP. Inside our server we navigated into the Advanced system settings. We clicked the Remote Settings, allowed remote connections to the computer, and clicked Select Users. Inside this box we added “ctuna,” Charles Tuna, and clicked Check Names. This converted the entry into a valid format for Charles and we saved the settings. Now that Charles is able to RDP into the Member Server we can attempt to test our new GPO. We connected back to our Member Server using Charles’ credentials and this time we were able to connect. Once we were in, we opened PowerShell and typed “regedit.exe.” After hitting enter an error message appeared saying the Registry Editor has been disabled by you administrator. This meant our

new Policy was successful. To wrap this lab up we went back to our Domain Controller and created a new User Group called Remote Users. We then gave this group to a new user and navigated back to the Member Server. The same way we added “ctuna” to be allowed remote access, we added the “Remote Users” group, now anyone with this group can access the server without us having to add each one manually.

Screen Shots

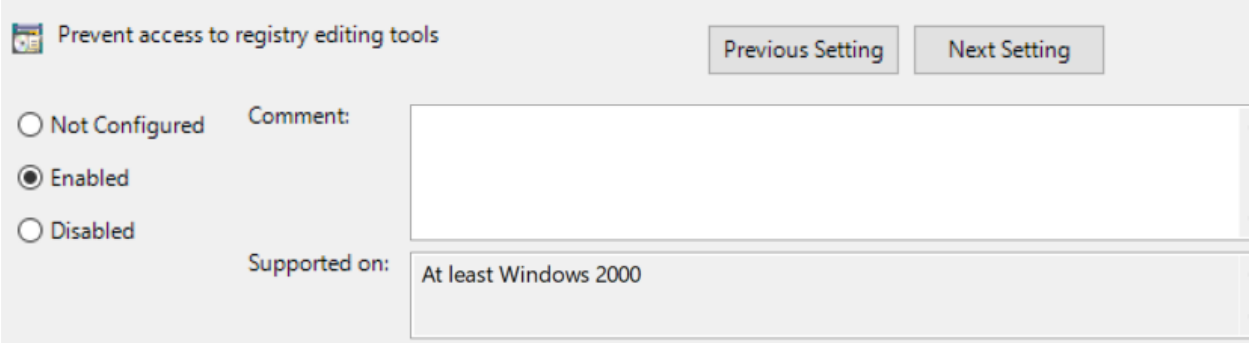

Figure 1

Figure 2

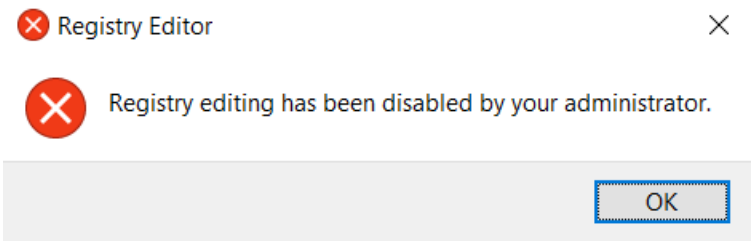

Figure 3

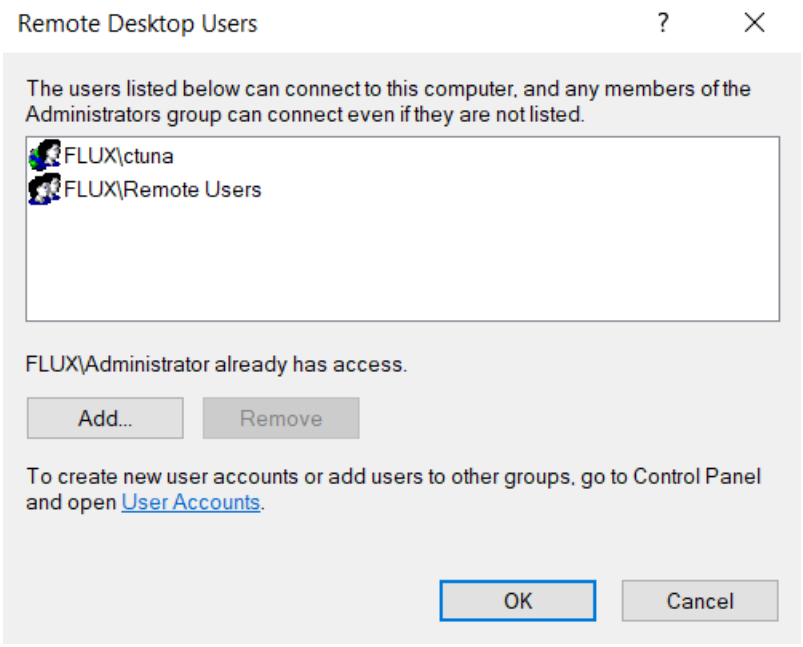

Figure 4

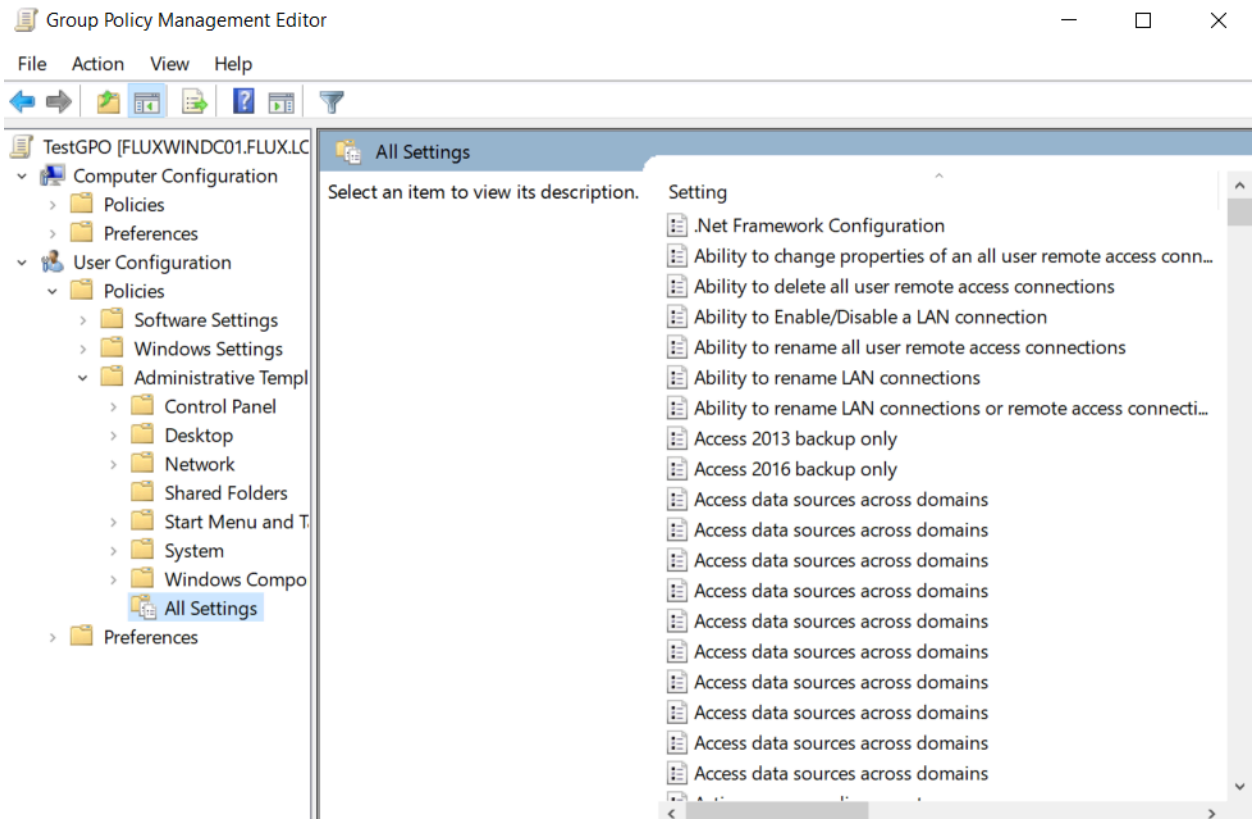

Figure 5

Research Questions

1. What are the two main components of Group Policy?
   Computer Configuration and User Configuration are the two main configurations.

2. What are the three settings that can be applied to each component?
   Software settings, Windows settings, and Administrative templates are the three components.

3. How are Group Policy settings organized?
   The processing order is the following local GP objects, site, domain, organizational unit, and forest.

4. What is the difference between Local Group Policy and Domain-based (or Active Directory-based) Group Policy?
   The Local Group Policy is applied first and settings in a child OU can override settings in a parent OU.

5. 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 Administrators 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?
   You would disable the policy for Administrators.

6. We've explored a GPO 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?
   There are several examples, some of these include: not allowing users to download software, creating .msi packages to push allowed software out to clients, and removing the ability to run commands on a machine.

7. What is Local GPOs/policy?
   Local GPO is a collection of objects that only apply to a local machine rather than the entire domain or OU.

8. What is the GPO Apply Order?
   The local policy is applied first. Next the AD policies are applied onto the site level, then into the OU.