**CSI3670**

**Winter 2021**

**Lab 6: Group Policy**

**Due April 18th at 11:59pm**

**Synopsis:**

In this lab, we’ll create a local user and destroy their self-confidence by locking down their machine. We’ll also do some file sharing.

**New User Creation**

First, let’s create a user that you’ll manage. Congratulations, you are now supervising somebody else. You should get a bump in pay, but unfortunately we don’t have the available budget for raises at the moment.

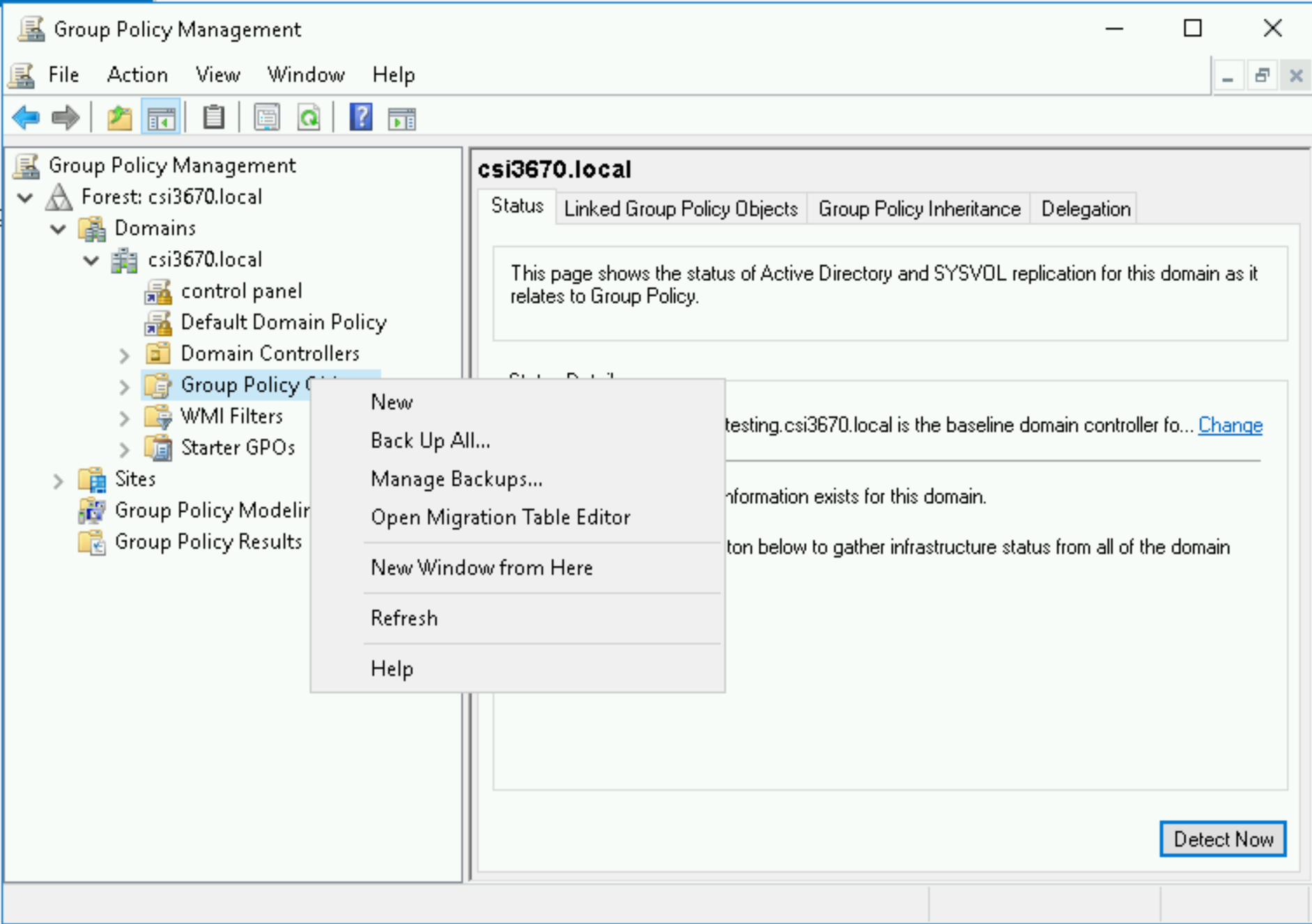
1) Login to your **GCP** VM (you should have ADDS installed on there from a prior lab).

2) Under Tools in the top right of your Server Manager window, open up the AD Users and Computers window. Right click the Users folder and create a new User. Give this user a unique name, something like <yourlastname>-TempUser for the login name. Use your last name for the first name, and TempUser for the last name. Hopefully by now it is obvious that you have to replace <yourlastname>, including the angle brackets.

3) Give this user a password that’s easy for you to remember. Ch@ng3M31mm3d1@t3ly will suffice. Uncheck ‘User must change password at next logon. (Temp12345 used to be the choice, but it turned out that GCP is a target for bots and that was broken into in prior years!)

**4) Take a screenshot of the user in your Active Directory Users and Computers window after successfully adding and paste into Q5.**

5) Now, let’s create a Group Policy. Go back to your Server Manager window, click Tools, and open up the Group Policy Management window. Expand Forest (csi3670.local), Domains, and your domain (probably csi3670.local from another lab). Right click on Group Policy Objects (the directory nested inside your domain) and click New. Name it <yourlastname>-GPO and leave the Source Starter GPO as (none). **Take a screenshot of your newly-created GPO inside your Group Policy Management window (make sure to include the left pane) and paste it into Q5.**



6) Right-click on your new GPO and click Edit. For this one, assign the following policies (not preferences) to the **User Configuration.**

(Remember, to set or restrict a restriction, find it in the tree of possible objects, right-click → Edit, and set to enabled).

This is an incredibly annoying process, but I’m doing it this way for a reason. When you set group policies in a system administration job, you will not always know where they’re located, and so therefore you need the practice of stumbling around to find the one you’re looking for. Also, while stumbling around, you’ll see what types of policies are available, even if they’re not the ones we’re looking for.

**If you get lost in the tree, searching for the right attribute can be… difficult. There are several tools out there, such as** [**https://gpsearch.azurewebsites.net/**](https://gpsearch.azurewebsites.net/) **or simple Googling. Here is a list of methods for finding them:** [**https://4sysops.com/archives/four-ways-to-search-for-group-policy-settings/**](https://4sysops.com/archives/four-ways-to-search-for-group-policy-settings/)

*(This is not an easy task … Googling may give you the fastest result). The HowToGeek website seems to be a decent repository for answers if you search for, say, "disable access to registry, group policy"*

a) Disable access to the registry editing tools

b) Prohibit access to the Control Panel and PC settings

c) Prevent access to the Command Prompt

d) Require password prompt on resume from hibernate/suspend

e) Password-protect the screensaver

**Go back to the Group Policy Management Window, select your GPO, and navigate to the Settings tab. Expand all of the User Configuration policies and take a screenshot showing it is being enforced and paste into Q5.**

That’s probably good for now. As you can see, you can enable/disable nearly everything in Windows via a GPO.

7) Now, we need to apply this GPO to your new user. In the Group Policy Management window, right-click your domain (in this case, csi3670.local) and ‘Link an Existing GPO...’ Add the newly created GPO. Now you should see it appear under your domain, not just under Group Policy Objects.

Left-click on your GPO in the left pane. Under Security Filtering, remove ‘Authenticated Users’ and add in your newly-created user. Mine looks like this when I’m done:

Graphical user interface, text, application

Description automatically generated

IMPORTANT NOTE: If you followed the slides and created the NoCtrl policy, you will need to make sure that it is enabled. The NoCtrl policy, if disabled, will override your new GPO settings.

8) We need to allow the new user to login locally. Right click on your group policy and choose “Edit”. In the Group Policy Management Editor, follow the screenshot:

Graphical user interface, table

Description automatically generated with medium confidence

Right click → Properties → Check “Define the policy settings”. Add your username by clicking ‘Add User or Group’ then Browse. Add your username, check names, and OK. You’ll also need to add the Administrators group. Click Apply and OK.

Graphical user interface, text, application

Description automatically generated

To allow this user access to login locally, we’ll need to add them to the Administrators group. Seems to be a bit of a workaround/hack, but fairly common when trying to login to a DC locally. Open up AD Users and Computers (from the Server Manager 🡪 Tools 🡪 Active Directory Users and Computers), right click on your user and click Add to a Group. Add ‘Domain Admins’ to the field, Check Names, and click OK.

Lastly, open up a command prompt (PowerShell 7) as an Administrator and run: gpupdate /force. You should hopefully see a message like this:

Text

Description automatically generated

If you receive an error logging in (that the method is not allowed), reboot the machine. If that still did not work, do the exact same set of steps (in 8) for the Default Domain Policy instead of your new GPO.

9) Now, logout and log back in as your new user (you’ll probably need to login as CSI3670\<new username> or <new-username>@csi3670.local). If you’re using Microsoft Remote Desktop like me, you may need to add a new user to your VM. Go to the settings for your VM inside Microsoft Remote Desktop and add a User Account for your new username.

**Take a screenshot of you:**

**a) Trying to access the Control Panel.**

**b) Trying to access the Registry.**

**c) Trying to access the Command Prompt (NOTE: PowerShell is different than the Command Prompt application!)**

**Lab Report (100 points)**

All of the answers to the following questions can be found in the slides we went over in class. The PDF is uploaded to Moodle under Group Policy Objects. If you prefer to supplement with Googling, make sure to (1) cite your source and (2) rephrase in your own words.

To complete the assignment, type your responses below, paste in the appropriate screenshots, and upload the completed Word/PDF document to Moodle.

1. (10 points) What is the difference between applying a GPO to a User vs. a Computer?
2. (10 points)What is the order that GPOs are applied? What happens if an **enforced** policy is higher in the application level than one that **blocks inheritance**?
3. (10 points) What is the difference between a Group Policy **setting** vs a Group Policy **preference**?
4. (10 points) In terms of group policy, what is required if we are dealing with Windows machines that are different versions? How would you ensure that you can support both the newest and oldest versions of Windows on your network?
5. (60 points, 10 points per screenshot) Make sure you read through carefully and supply all necessary screenshots here (should be six).