Robert Carpenter
github.com/robertmcarpenter
Fri November 16th 2024

Lab 4.5.7 Hardening Local Accounts using a Active Directory Group Policy Object

In this lab, I will be hardening User Accounts on a Windows Server/Active Directory Domain using a Group Policy Object and applying that to the domain so that the changes are reflected across our MS/Windows Infrastructure.

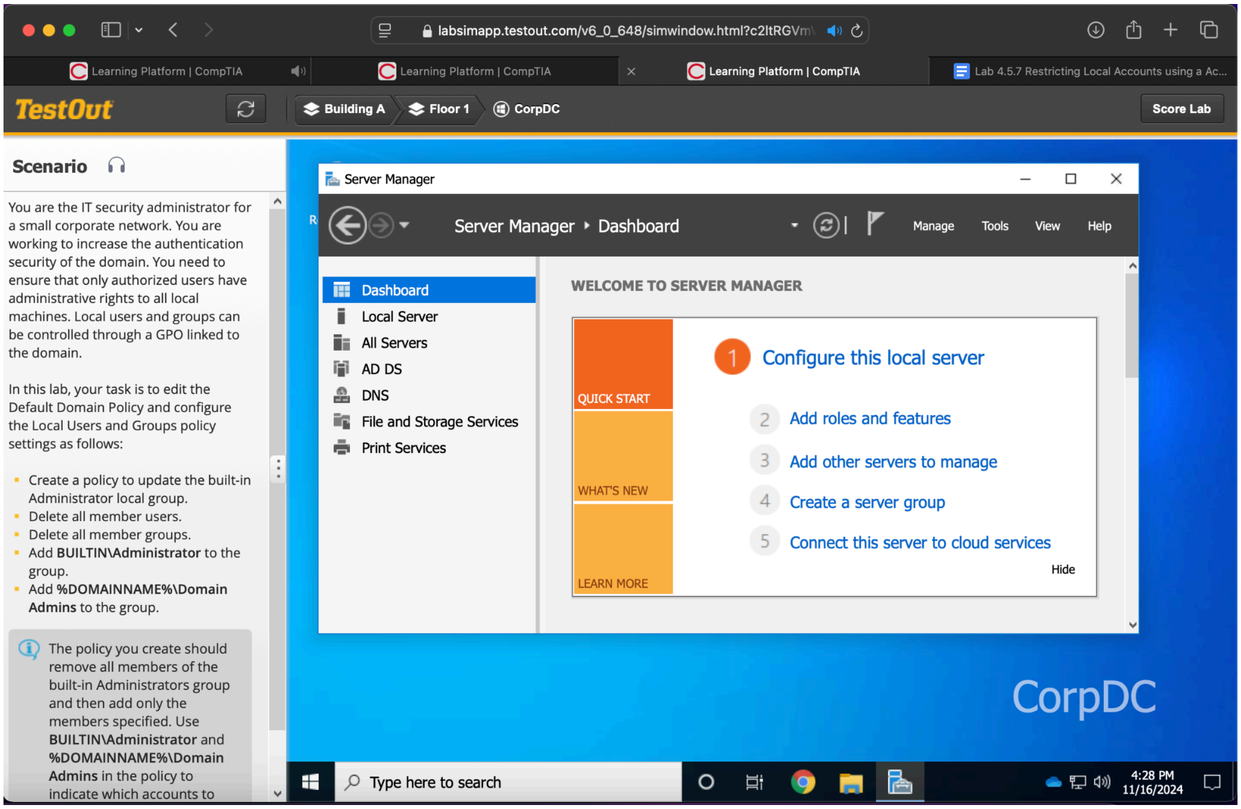
The scenario for this lab is as follows:

"You are the IT security administrator for a small corporate network. You are working to increase the authentication security of the domain. You need to ensure that only authorized users have administrative rights to all local machines. Local users and groups can be controlled through a GPO linked to the domain.

In this lab, your task is to edit the Default Domain Policy and configure the Local Users and Groups policy settings as follows:

- Create a policy to update the built-in Administrator local group.
- Delete all member users.
- Delete all member groups.
- Add **BUILTIN\Administrator** to the group.
- Add **%DOMAINNAME%\Domain Admins** to the group. "

Robert Carpenter
github.com/robertmcarpenter
Fri November 16th 2024


labsimapp.testout.com/v6_0_648/simwindow.html?c2ltRGVm
Learning Platform | CompTIA
Learning Platform | CompTIA
Learning Platform | CompTIA
Lab 4.5.7 Restricting Local Accounts using a Ac...
TestOut
Building A
Floor 1
CorpDC
Score Lab
Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
Print Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
CorpDC
Type here to search
4:28 PM
11/16/2024

Scenario

You are the IT security administrator for a small corporate network. You are working to increase the authentication security of the domain. You need to ensure that only authorized users have administrative rights to all local machines. Local users and groups can be controlled through a GPO linked to the domain.

In this lab, your task is to edit the Default Domain Policy and configure the Local Users and Groups policy settings as follows:

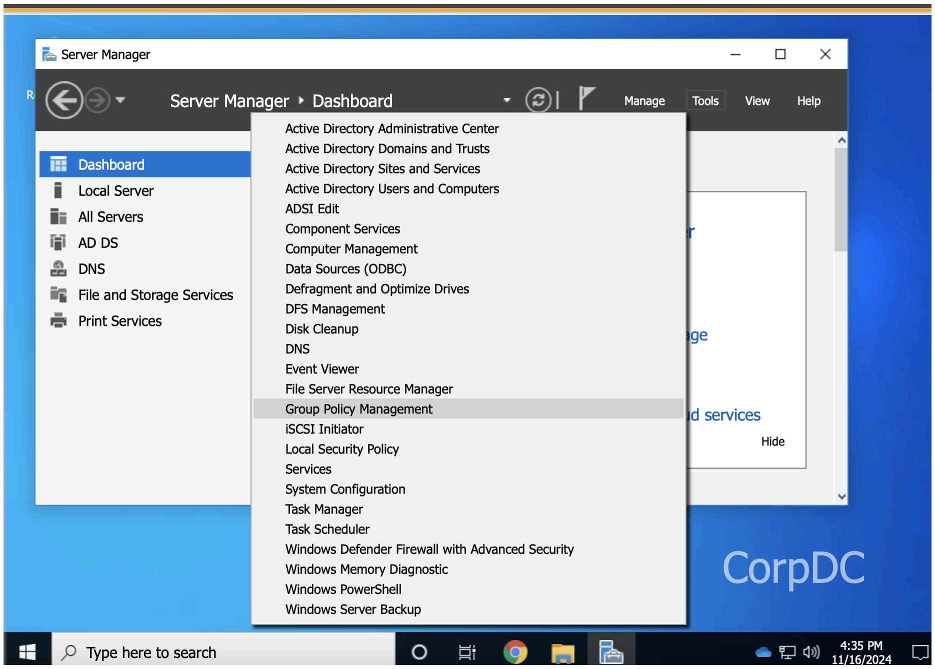
- Create a policy to update the built-in Administrator local group.
- Delete all member users.
- Delete all member groups.
- Add **BUILTIN\Administrator** to the group.
- Add **%DOMAINNAME%\Domain Admins** to the group.

The policy you create should remove all members of the built-in Administrators group and then add only the members specified. Use **BUILTIN\Administrator** and **%DOMAINNAME%\Domain Admins** in the policy to indicate which accounts to

Our first task is to create a policy on our Windows Server Manager in order to update the Local Admin accounts that are created by default. Having the default Administrator (and Guest) accounts can grant an attacker the possibility of elevating privileges in the event of a breach. We want to make sure that the Admin account for all computers in this domain is assigned to the actual Administrator of the system and also obfuscate the account so it's not obvious that the account holds the privileges it does.

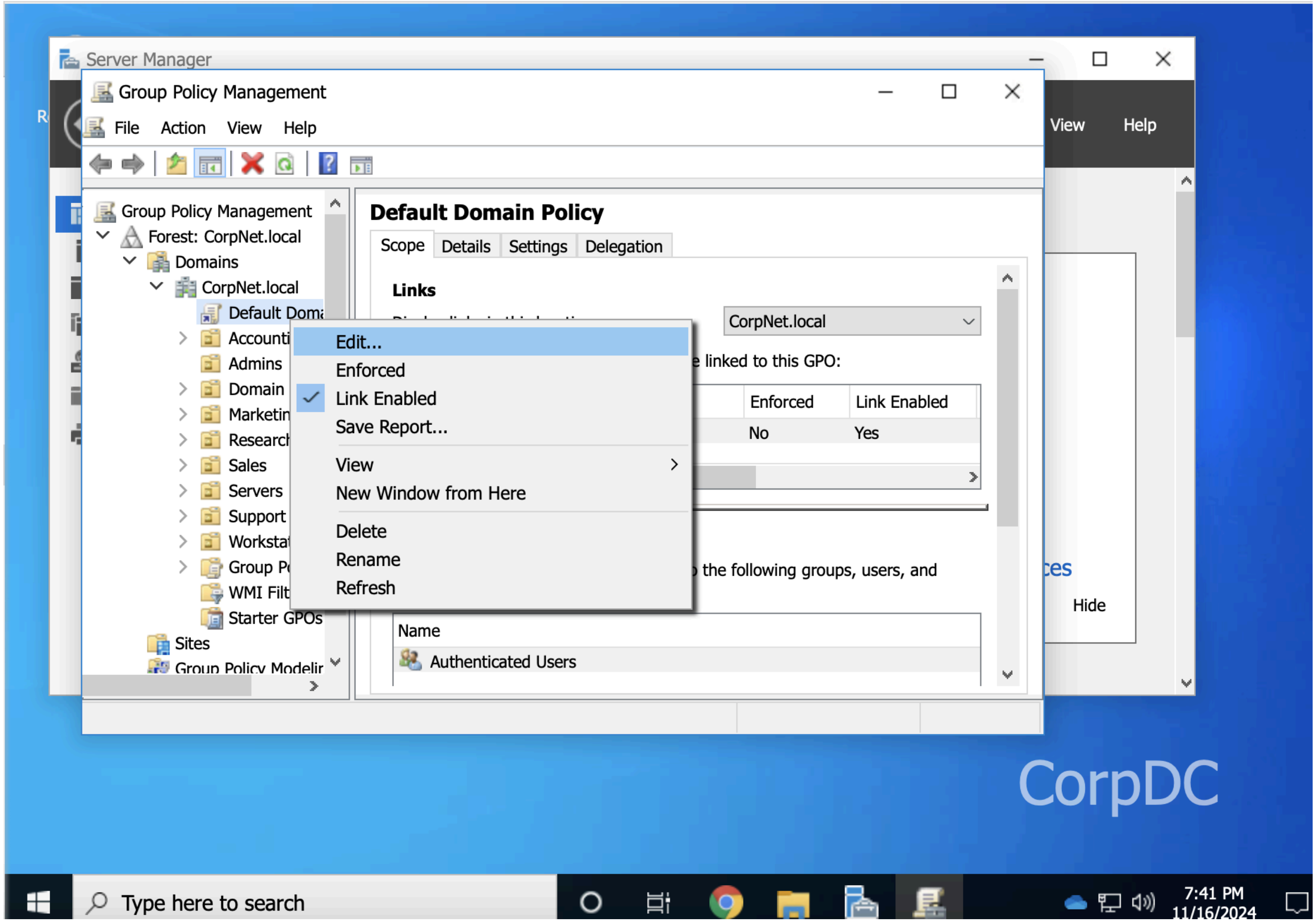
Lets click Tools > Group Policy Management on our Windows Server Manager:

Robert Carpenter
github.com/robertmcarpenter
Fri November 16th 2024



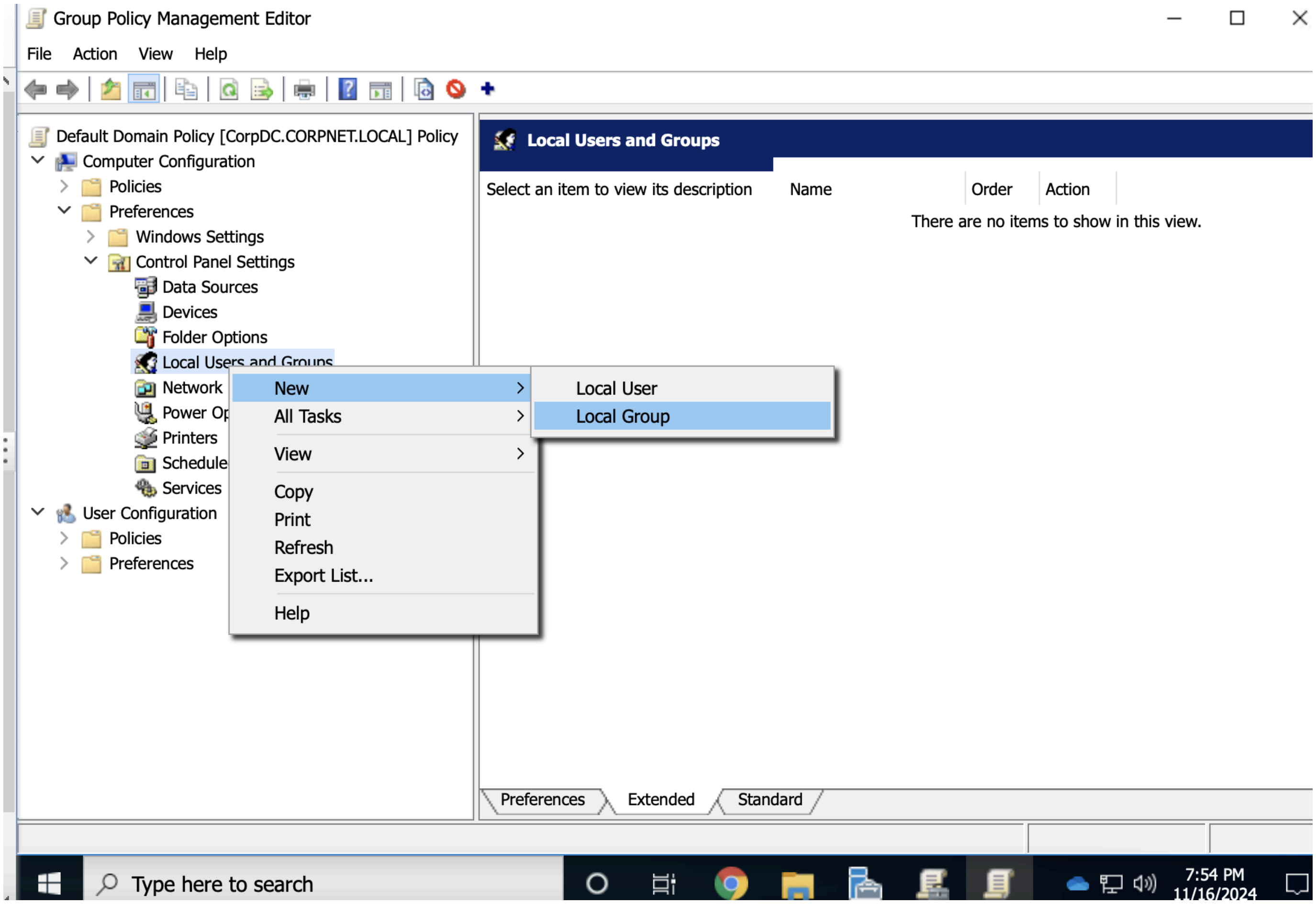
Now that we have it open let’s navigate to Group Policy Objects and Create a new policy.

Robert Carpenter
github.com/robertmcarpenter
Fri November 16th 2024



We will want to set a Computer Configuration policy that is applied to every machine in the domain instead of individual accounts.Upon clicking the “Edit” button we get the following screen:

Robert Carpenter
github.com/robertmcarpenter
Fri November 16th 2024

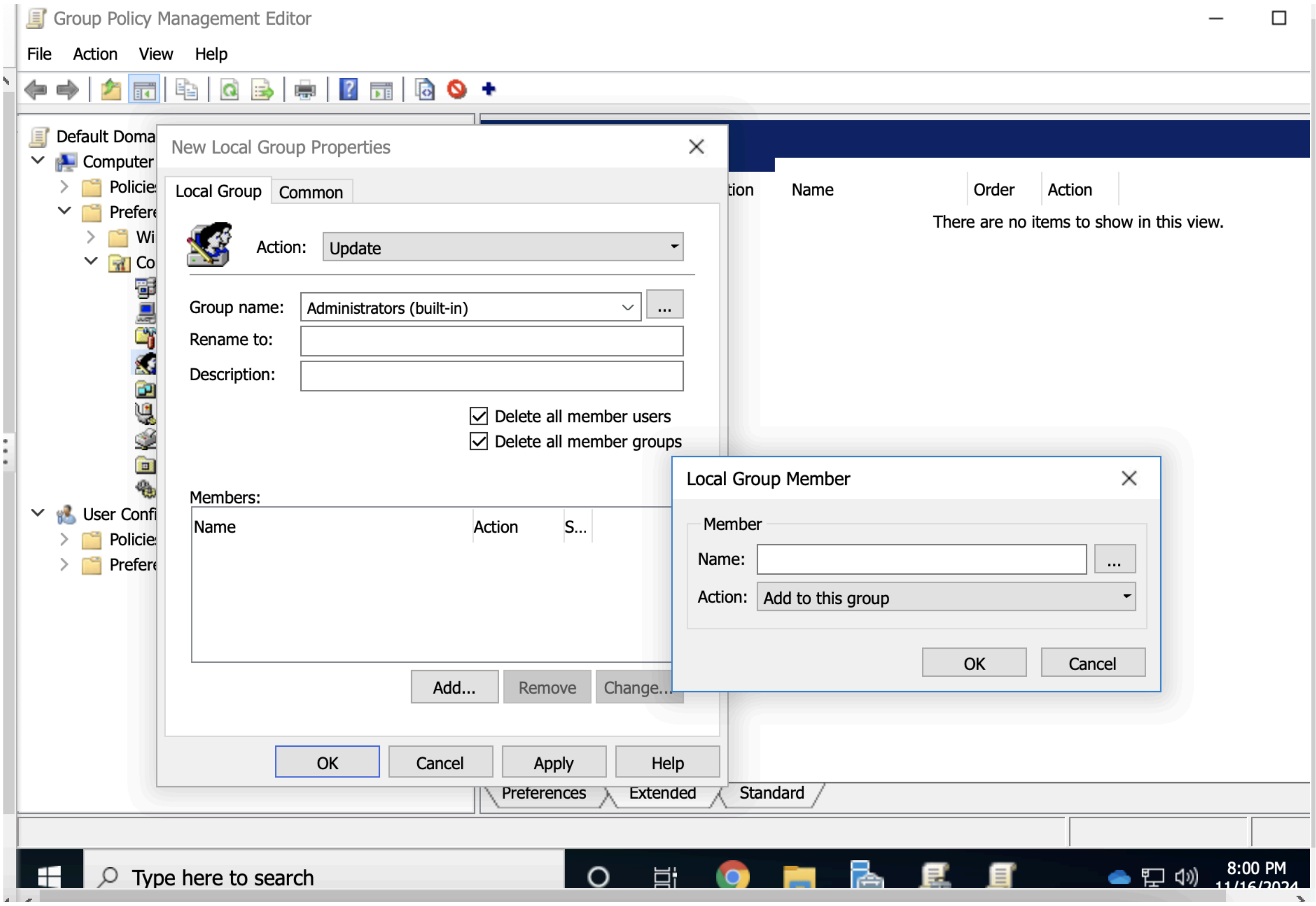


Select an item to view its description

There are no items to show in this view.

We are going to create a Local Group for our Admins. We will want to check the boxes in the dialog box that pops up that states “Delete all Member users.” The reason is because we will need to remove all traces of the built in “Administrators” group and replace with our defined “Domain Admins” aka. Our actual IT admins of the company. Should look like this:

Robert Carpenter
github.com/robertmcarpenter
Fri November 16th 2024



There are no items to show in this view.

Action: Update

Group name: Administrators (built-in)

Rename to:

Description:

☑ Delete all member users

☑ Delete all member groups

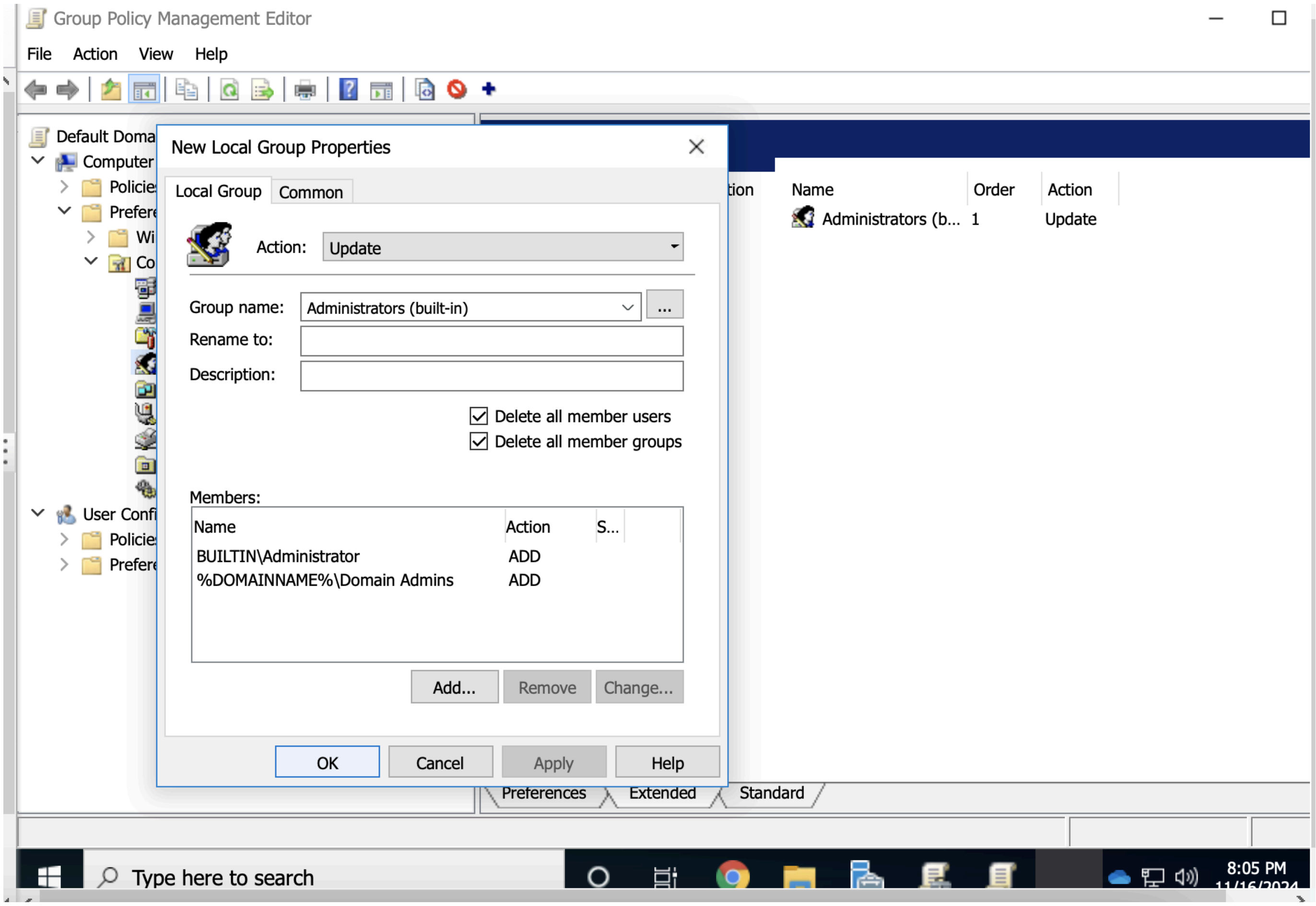
Members:

Name	Action	S...

Name:

Action: Add to this group

Robert Carpenter
github.com/robertmcarpenter
Fri November 16th 2024



New Local Group Properties

Local Group | Common

Action: Update

Group name: Administrators (built-in)

Rename to:

Description:

☑ Delete all member users

☑ Delete all member groups

Members:

Name	Action	S...
BUILTIN\Administrator	ADD	
%DOMAINNAME%\Domain Admins	ADD	

Name	Order	Action
Administrators (b...	1	Update

After click Apply and then OK. This will now push out the update to our domain controller. This concludes this lab.