CS312 :: Lab Week 7 :: Windows Server and Active Directory

In this lab, we'll install and configure a couple Docker containers, link them together, and start them running.

Supplies needed

- Personal laptop with VirtualBox installed
- Our **WinServer2016Router**, **WindowsServer2016_Reference**, and **Win10_DomainPC** virtual machines, downloadable from our Canvas website. These are quite large, totaling about 18GB.

Perform the Procedure and answer the Questions in order, as given below.

Procedure

In this Lab, we'll be doing the following:

1. Enable DHCP client protocol tracking in the logs of a Windows 10 Pro PC
2. Create a reserved mapping in DHCP for the PC
3. Join the Windows 10 Pro PC to a Windows Server 2016 domain controller
4. Create a Group Policy Object on the server and apply it to the PC
5. See the effect of the GPO on the PC

Getting Started

The first thing we are going to do is record the DHCP information given to our Windows PC by the Windows 10 Server.

To get started, we'll need to turn everything on. Import and then boot the VMs in the following order, waiting for each to complete booting before starting the next (just to make things easier):

1. WinServer2016Router
2. WindowsServer2016_Reference
3. Win10_DomainPC

It's possible that you receive an error message about USB, where the error message suggests that you need to install a VirtualBox extension pack. This is very easy to do! Simply go here and download the Extension pack that matches your installed VirtualBox version (Help -> About VirtualBox *OR* VirtualBoxVM -> About VirtualBox MV):

https://www.virtualbox.org/wiki/Download_Old_Builds_5_2

Once you have the file downloaded, which will have a .extpack file extension, just double click on it to install it. That should enable you to run the VMs.

Note that I am developing these labs and VMs with VirtualBox version 5.2.6.

Enable and Track DHCP Assignments

Once everything is running, log to the PC using the "User" account (password is: "password") and follow these instructions to turn on DHCP event tracking:

1. Fire up the Event Viewer by hitting WINDOWS+X and clicking on "Event Viewer"
2. Inside the program, expand the tree, in the left side bar, like this: Applications and Services Logs -> Microsoft -> Windows -> Dhcp-Client
3. With Dhcp-Client selected, two options will appear inside of it. Click on the "Microsoft-Windows-DHCP Client Events/Operational" entry, and then click on "Enable Log" on the right sidebar.

Now we can track DHCP events in these logs! Let's see what happens when we get a DHCP address:

1. Open up a command prompt (cmd.exe)
2. Type this to release your DHCP address:

   ```
   ipconfig /release
   ```

   And then this to get a new one:

   ```
   ipconfig /renew
   ```

3. Now, head back to the Event Viewer and refresh the log view using the "Refresh" button on the right.

You should have about a hundred entries to look through. Here's a few questions about what you're seeing. Note that you can use the "Filter Current Log" tool on the right sidebar to filter out everything but the Event IDs you want:

QUESTION: Go answer Questions 1 through 3 now.

Reserve IP Address in DHCP

Next, we're going to reserve whatever IP address our PC gets as its permanent IP address.

1. Log into the Windows 2016 server VM
2. When you log in, the Server Manager should be displayed. If not, it's pinned to the start menu: click on it to start it up.
3. On the top menu bar, click Tools, then select DHCP.
4. In the DHCP manager that starts up, on the left side bar, click the little arrows to expand the path like so: <server name> -> IPv4 -> Scope [192.168.1.0], then click on Address Leases.
5. You should see the name of our PC in the list, which is something like "DESKTOP-74J...". There may be more than one lease allocated to this PC. Go ahead and right-click on the one that has the Lease Expiration timestamp furthest into the future, and click "Add to Reservation". Click OK on the confirmation message.
6. Expand the Reservations sub menu on the left sidebar, and verify that our PC has a reservation for the IP address you selected above.

Add PC to Domain Controller

Now we're going to add our Windows 10 Pro PC to the domain!

1. Back on the PC, open up a command lind.
2. Get our IP information in detail:

   ```
   ipconfig /all
   ```

3. In the data that's returned, look for a section with Description as "Red Hat VirtIO Ethernet Adapter". This is the interface we've defined in VirtualBox itself. This is the ethernet interface that should be getting an IP address.
4. Verify that "Connection-Specific DNS Suffix" has "cs312domain.local" as its value, and that the "DNS servers" entry lists 192.168.1.2. This is the Domain Controller address, and it needs to be what our PC is listening to before we attempt to join.
5. Now we'll do the join to the domain. From the Start Menu, type "System" and click the "System Control panel" item returned.
6. In the middle of the System windows is a section labeled, "Computer name, domain, and workgroup settings". Click on the Change settings link on the right side.
7. In the System Properties dialog box that appears, click the Change button.

8. In the new “Computer Name/Domain Changes” dialog box that appears, click the radio button that says, “Domain”, and enter “CS312DOMAIN”. Click the OK button and cross your fingers - this’ll take a minute!
9. When presented, use the Domain Administrator credentials to log in (Username: “CS312DOMAIN\Administrator”, with password “Password!”).
10. Click OK on the “Welcome to the Domain” dialog box, and close out of the rest of the windows.
11. Restart the PC, then log in (Click “Other user” at the login screen first) as as the Domain Administrator.

Create Group Policy Object

Now that our PC is on the domain, let’s enforce a policy onto this PC. We’re going to create a Group Policy Object on the server, and then apply it to this PC.

1. On the server, in the Server Manager tool, click the Tools menu and select Group Policy Management.
2. Now we need to create container for our computer to live in: only then can we assign a Policy to that container. In AD, these containers are called “Organizational Units” (OU). Let’s create one and get our PC in:
    a. In the Group Policy Management window, drill down using the little arrows on the left sidebar: “Forest: cs312domain.local” -> Domains, and then right click on the next one, “cs312domain.local”. Select “New Organizational Unit”.
    b. Enter in “My Test PCs” for the Name, and click OK.
    c. Now, right-click on the “cs312domain.local” entry in the tree on the left, and select, “Active Directory Users and Computers...”. This is the classic tool for organizing Users, Groups, and Computers.
    d. In the AD U&C window that appears, locate the Computers folder on the next sidebar. Click on it.
    e. You should see our Domain PC, called “DESKTOP-74J...”, Left-click it, then drag it into the “My Test PCs” OU that is also on the left side bar. AD will warn you, but click OK anyway. This adds our PC to this OU.
3. Now we can create and assign a Group Policy Object (GPO) to this Organizational Unit (OU). Back in the Group Policy Management tool, right-click on “My Test PCs”, and select “MyCreate a GPO in this domain, and Link it here...”.
4. Enter the name “MyTestGPO” and click OK. You’ll note that the actual GPO lives in a separate folder outside “My Test PCs” called “Group Polocy Objects”, but this is fine. You can see that there’s a shortcut/link to the GPO in our “My Test PCs” OU, and that is sufficient.
5. Click on “MyTestGPO”. A little warning box will appear: read it, check the box to never see it again, and hit OK.
6. Now, let’s make some changes to this policy. By default, the policy contains all possible settings, all of which are set to the “Not Configured” value, which means it’s up to each individual PC and User to control things. We’re going to set just a few things.
    a. Right-click on MyTestGPO and select “Edit...”.
    b. Maximize the window, then expand the tree in the left side-bar like this: MyTestGPO -> Computer Configuration -> Policies -> Administrative Templaces... -> System, then click on Group Policy. This will make a bunch of options appear on the right.
    c. Click on the option called, “Turn off Local Group Policy Objects processing”. By setting this option, we’ll prevent users from setting their own Group Policy Objects on their computers that might override our (admittedly heavy-handed) oversight. Let’s set the settting:
        i. Right-click on this option and click Edit.
        ii. Click the Enabled circle option, then click OK.

d. Now, click on the option labeled as, “Configure user Group Policy loopback processing mode” We’re going to use this to replace whatever settings the *User* has configured, with these ones we’re setting up for the *Computer*.
    i. Right-click this option and click Edit.
    ii. Click the Enabled circle option.
    iii. Down in Options, Set the Mode to “Replace”., then click OK.
e. The change we’re going to make is fairly boring: we’re going to add a new entry to the PATH variable on our PC by way of this GPO. To get started, drill down to MyTestGPO -> Computer Configuration -> Preferences -> Windows Settings and click on Environment. A page will appear that looks suspiciously like Windows XP. Here’s how we’ll add the Registry keys we want:
    i. Right-click on the Environment item in the left side-bar.
    ii. Select New -> Environment Variable
    iii. In the window that appears set these values:

    Action: Create
    System Variable: Checked
    PATH checkbox: Checked (this also sets the Name to PATH)
    Partial checkbox: Checked
    Value: “C:\Users\Public\Documents”

    This is going to add the Public User docs to the PATH for all users. If you had programs stored in there, they could now be run in the command line from any folder.

7. Now we can go check our settings on the PC! Log into the PC with the Domain Administrator account, and fire up a command prompt.
8. Run the following command on the PC to get the policies we just set in the Server, and apply them:

    ```
    gpupdate /force
    ```

9. Log out, then log back in to the PC (or restart).
10. In the PC, open up a command prompt, and run this command:

    ```
    path
    ```

    You should see the “C:\Users\Public\Documents” in the path listing! If not, go back through the instructions and see what you might have missed.

    QUESTION: Go answer Question 4 now.

Questions

1) What is happening in the entry with Event ID 50059? What are the two IP addresses reported in the log entry, and what machines are likely at those IP addresses? *(5 points)*
2) Similarly, what is happening in the entry with Event ID 60001? What are the two IP addresses reported in the log entry, and what machines are likely at those IP addresses? *(5 points)*
3) What does the entry in Event ID 50058 say? *(5 points)*
4) Get the TAs initials, showing that your PATH contains “C:\Users\Public\Documents” *(25 points)*

You’re done! To receive credit for this lab, you must turn in your answer sheet.