|  |  |
| --- | --- |
| **Networking Infrastructure**  Diploma in CSF/IT  Year 2 (2020/21) Semester 3 | Week **16** |
| **2** hours |
| **Windows 2016: Group Policy Management** | |

## A. Objective:

At the end of this practical, students would be able to use Group Policy in Windows 2016 to complete the following tasks:

* Configure a group policy for a specific OU.
* Configure a domain policy for user account login.
* Configure a domain policy for software deployment.

**B. Resources**

* Machine with Microsoft Windows 2016 Server (domain controller).
* Client PC running Windows 10.

(Form team of 3/4 students. Each team will work on a server and 2 client PCs.)

### C. Lab Setup

In this Practical, ensure the following before you proceed:

* VMware Windows 2016 Server as a **domain controller** with Domain Name: NI**T**.com
* VMware Windows 10 Client joined the NI**T**.com Domain and login as NI**T**\administrator.
* The date and time on the PC (Host machine) is set correctly.

Settings for Server and Client PCs should be as follows:

|  |  |
| --- | --- |
| TCP/IP Domain Name | NI**T**.com, T is the team number 2-9  (to be assigned by tutor) |
| Restore Mode Administrator Password | **p@ssw0rd** |
| Static IP address /Subnet mask | **For Server,** WinSvr2016**:**  172.16.**T**.**1**  **For Client PC,** NI**T**client**101**  172.16.**T**.**101**  **Subnet mask for all machines: 255.255.255.0** |

If you have already configured the above settings in the earlier lab, check that the IP/DNS settings are correct.

This practical is a continuation of the earlier practical.

**On the PC where the Server is installed:**

Login to Windows 10 with username “Administrator” and password “p@ssw0rd”.

Start VMware program.

Locate the Windows 2016 server VM (WinSvr2016\_X where X is your tutorial group number) that you have created in the earlier practical lesson.

Start the virtual machine-server. After the server is running, ensure the domain settings and IP settings are correct.

**Tasks to achieve:**

**Task 1: Create a Group Policy for SHOWROOM OU**

* Upon successful login, the **SHOWROOM** users will have:
  + **No icons on Desktop**.
  + On **Start menu**, no **Run menu** and **no logoff**.

**Task 2: Domain Policy for User Account Login**

* Create a password and account lockout policy for all users configured with following settings:
* Account will automatically **lock out for 2 minutes, after 3 failed attempts** to login.
* Account Lockout **will automatically reset** after 2 minutes.
* Minimum Password length: **8 characters**
* Minimum Password age: **0 days**

**Task 3: Domain Policy for Software Deployment**

* To deploy a windows application automatically when the user logs on.

**Task 1: Create a Group Policy for SHOWROOM OU**

**D. Create the SHOWROOM OU and SHOWROOM User account**

1. Login to the Windows 2016 domain as an administrator.

2. Use the **Active Directory Users and Computer Tool** to create an organizational unit called **SHOWROOM**.

3. Create a user account called **showroom01** in the new OU (with the password "**p@ssw0rd**")

### E. Create Group Policy to control the Desktop

Next, we will create the GPO (group policy object) that will be linked to this **SHOWROOM** OU.

1. In the Server Manager Dashboard, at the tool bar, click the **Tools** tab then select **Group Policy Management**. In the Forest: NI**T**.com, expand Domains and expand NI**T**.com.
2. Right click on the **SHOWROOM** OU and select “Create a GPO in this domain and link it here”. Rename the new GPO as **Showroom Policy Object** and click **OK**.
3. Select the **Showroom Policy Object** in **SHOWROOM** OU. Right click on it and then select **Edit**.
4. Navigate to **User Configuration** (not Computer Configuration)

**Note:** Each GPO is built from 2 sections:

* **Computer configuration** contains the settings that configure the computer prior to the user login combo-box.
* **User configuration** contains the settings that configure the user after the login.

1. Expand **Policies**, then the **Administrative Templates**, expand on **Desktop.**

**Note: Administrative templates** are settings that configure the local registry of the machine.

1. Click on **Desktop** under **Desktop**.
2. Double click on “**Enable Active Desktop**” and select “**Enabled”** option. Click **OK**.
3. On the **Group Policy Management Editor**, navigate to **User Configuration -> Administrative Templates** **-> Desktop,** enable **“Hide and disable all items on the Desktop”** feature.
4. On the **Group Policy Management Editor**, navigate to **Administrative Templates -> Start Menu and Taskbar.**

Find and enable the following options:

* **Remove Run menu from Start Menu.**
* **Remove Logoff on the Start Menu.**

## In File menu, click Exit. Click OK when completed.

### F. Updating the new Group Policy

### To ensure that the group policy settings are updated, type the following command using Windows PowerShell:

**gpupdate /force**

**G. Showroom Group Policy Test**

### 11. To test whether the group policy is working for showroom users, login from Windows 10 client as showroom user: showroom01.

What do you see on the desktop after logging on?

Can you access the Run menu?

Can you **Sign out**/log off?

### 12. All users created in the SHOWROOM OU will have the same Group Policy applied. You may create another user e.g. showroom02 in this OU, login to test the effect of the Group Policy.

**Task 2: Domain Policy for User Account Login**

**H. Configuring Password and Account Lockout Policy**

Next, we are going to configure the following settings:

* Minimum Password length**: 8 characters**
* Account will automatically **lock out for 2 minutes, after 3 failed attempts** to login.
* Account lock out **will automatically reset** after 2 minutes.

1. In the Server Manager Dashboard, at the tool bar, click the **Tools** tab then select **Group Policy Management**.

As this policy affects the whole domain (everyone in the domain), we will edit the **default domain** **policy**.

**Note:** Domain security policy is the policy of the entire network. When a security setting is set on domain security policy every user and computer that resides in that domain is affected by that policy.

1. Click on **the domain object** (NI**T**.com). Right click on **Default Domain Policy** and select **Edit**. The Default Domain Security Settings console will open.
2. Under **Computer Configuration,** expand **Policies,** expand **Windows Settings,** expand **Security Settings,** expand **Account Policies** and select **Password Policy**.
3. Double-click the relevant settings and **set them to the settings as given above**.
4. Under **Account Policies** select **Account Lockout Policy.**
5. Double-click the relevant settings and **set them to the settings as given** (e.g. Account Lockout Duration, Account Lockout threshold and Reset Account Lockout counter after).
6. Right-click the NIT on the “Default Domain Policy” page, select “Enforced” and “Link Enabled”
7. Update the group policy settings by typing **gpupdate /force** command **using** Windows PowerShell.

**I. Testing the configured Domain Policy**

1. Reboot the **Windows 10 Client** and re-login to the Windows domain.

When the user logs in, test out the password and account lockout policy to determine whether the Group policy is working. For example, use a user account to enter a wrong password three times and check if the account is locked out.

**Task 3: Domain Policy for Software Deployment**

**J. Software Deployment Group Policy**

Next, we will create a new group policy that would install/deploy windows software to the Windows 10 clients automatically. Any windows program with an .MSI extension can be installed using this method. You can also use Group Policy to upgrade or remove the original program.

Software installation using GPO provides users with immediate access to the software they need to perform their jobs. With software installation policies you can rollout programs like Word, Access and Excel to local machines, while retaining central control of all such desktop applications.  Users no longer need to look for a network share or install, fix and upgrade software themselves.

Some basic terms regarding to software deployment:

**Assigning Applications:**

* Assign an application when you want everyone to have the application on his or her computer. An application can be **assigned to both computers and users**. The assigned applications are installed on the first reboot of the computer or when the user logs on.

**Publishing Applications:**

* Publish an application when you want the **application to be available** to people managed by the GPO, should they want the application. With published applications it is up to each person to **decide whether or not to install the published application**. An application can only be published **to users**. With Publish, the user would have to go to the Control Panel, Add or Remove Programs before they could install the program.

In this case, we will **assign the application** – install the software **putty.msi** when the user logs on.

1. Create a folder, **INSTALLATION** in **c:\users\public\ of Windows 2016 Server**.

Share this **INSTALLATION** folder with the following settings:

* **Share permissions (Sharing tab) set to “Full Control” for Everyone**
* **NTFS permissions (Security tab), add “Everyone” built-in group and set to “Full Control”**

If permissions are not set correctly, this may prevent the installation process from starting.

1. Copy the software package, **putty.msi** into the folder.

The software package, **putty.zip** (zipped up) is available in Mel-NI-Learning Materials-Week16. **Unzip** the file and copy **putty.msi** into the **INSTALLATION** folder.

1. In the Server Manager Dashboard, at the tool bar, click the **Tools** tab then select **Group Policy Management**.

As this software policy affects the whole domain (everyone in the domain), we will edit the **default domain** **policy**.

1. Click on **the domain object** (NI**T**.com). Right click on **Default Domain Policy** and select **Edit**. The Default Domain Security Settings console will open.
2. Under **User Configuration,** expand **Policies,** expand **Software Settings.** Right-click the **Software Installation** node, then click **Properties**.
3. In the **General tab** of the Software Installation Properties dialog box type the path to the default Software Distribution Point for packages (.msi files) in the Default Package Location box **(\\<IP\_Address\_Windows\_Server>\INSTALLATION)**. This is the location of the share you created earlier on. Select the option “**Assign”** and click **OK** to exit.

**Note:** On the **General** tab you will find the following information.

* **Display the Deploy Software Dialog Box:** to specify that when you add a new package, the Deploy Software dialog box will display, allowing you to assign, publish, or configure package properties.
* **Publish:** Packages can only be published to users, not computers.
* **Assign:** Packages can be assigned to users and computers.
* **Advanced:** to specify that when you add a new package, the Configure Package Properties form should appear.
* **Basic:** to provide only a basic display of the install process to users.
* **Maximum:** provide all installation messages and screens during the package installation to users.

1. To create software package to deploy, right click **software installation** node, click **New** and click **Package.**

The File Name list in the Open dialog box shows those Windows Installer packages located at **\\<IP\_Address\_of\_Server>\Installation** which you specified as the default. Select the **putty.msi** software that you want to deploy, click **Open**. You have just added a software package to deploy. (Wait a while for the **putty.msi** package to appear).

1. To set the software package properties, right click on the software package (**Putty release 0.70**) and click **Properties**. Click on the **deployment tab**.

**Check** the option **“Install this application at login”.** Click **OK** when completed**.**

**Notes:**

* **General tab** gives you some general information about the package.
* **Deployment tab** allows you to set appropriate deployment type (Publish or Assigned). If this is an application under the Computer Configuration node of the Group Policy snap-in, the Published choice appears dimmed, because packages can only be assigned to computers, not published.
* You can check the **Uninstall this application** **when it falls out of the scope of management** check box to specify that the package should be removed when the GPO no longer applies to users or computers. For instance, if they get a promotion and move to a different OU.
* **Do not display this package in The Add/Remove Programs control panel** option is used to specify that this package should not be displayed in Add/Remove Programs in Control Panel.
* **Upgrade** tab allows you to add the package to be upgraded for this package.
* In the **Categories** tab of the Properties dialog box for the application, click the category you want to specify for this software from the Available Categories list, then click **Select**.
* The **Modifications** tab lists the modifications (that is, transforms) to be applied to the package.
* On the **Security** tab you can set security for this package. Make sure that all the users that this GPO is applying on must have Read access on the package.

**K. Testing the Software Deployment Group Policy**

1. On **Server**, check whether Putty application is installed using search. If installed, uninstall it.

On **Windows 10 client**, login using a valid domain user account (e.g. Sales002).

Check whether Putty application is installed and uninstall if it is installed.

1. On Server, update the group policy settings by typing the **gpupdate /force** command.

(When prompted to logoff on Server, answer **“Y”** to install software package on the Server when you login again)

1. Re-login to Server and check whether Putty application is automatically installed/deployed.
2. On **Windows 10 client**, logoff from the domain user account and **re-login**. Check whether Putty application is automatically installed/deployed (as specified in the group policy).

\*\*\*\*\* End of Practical \*\*\*\*\*