Lab 6 – Active Directory

In this lab, you will create a new domain by installing Active Directory, and moving your Windows Server from a server in a Workgroup to a Domain Controller of a Domain. You will then set up a second Domain Controller and you will have your Windows Client VM join your domain. You will also create Domain users and groups.

This lab should take approximately 90 minutes to complete.

BEFORE YOU BEGIN:

You will be using Server 2 for most of this lab. Ensure that TCP/IP is statically configured with your ***10.0.xxx.20*** address with a subnet mask of ***255.255.0.0***.

If the DNS Role is not installed on your server, you can skip step 0. If the DNS Role is installed on your computer, from Lab 2, use the instructions in Step 0 to remove it before installing Active Directory.

0.0 Remove DNS Role – Server2

Because we configured DNS to resolve a name for our installation of the Web Server Role in Lab 4, we must delete DNS and then reinstall it with the Active Directory role to ensure that DNS is properly configured for AD DS.

1. Use the Server Manager to Remove Roles and remove the DNS Role. Restart your server, if prompted, to complete the role removal.

1.0 Install Active Directory

1. Logon to the Server2. Open **Server Manager**, click **Add Roles and Features** from the Dashboard.

   Click the checkbox for ***Active Directory Domain Services*** and click **Next**.

   You may be asked to install some additional Roles or Features to support AD. Ensure to click OK to confirm that these other Roles and Features will be installed.

2. Read the information about *Active Directory Domain Services* then click **Next**. Click **Install**.
3. Review the installation results window to ensure that you see *Active Directory Domain Services* and *Active Directory Domain Controller*. Click **Close**.

2.0 Promote Your Server to a Domain Controller

Installing the Active Directory Domain Services role, does not immediately make your server a Domain Controller. More configuration is required.

1. On the Server Manager, top right corner, you will see a Warning Label (yellow triangle with an exclamation point). Click this icon and select “Promote this server to a domain controller”.
2. Click the option button to ***Add a new forest***, enter your domain name (***SenecaID*.com,** where ***SenecaID*** is your Seneca username), and click **Next**.
3. In ***Domain Controller Options*** window*:* for the ***Forest functional level***, you select ***Windows Server 2016 (default).*** Assign a password of ***P@ssw0rd*** to use in case the domain controller needs to be started in the *Directory Services Restore Mode*, confirm the password and click **Next**.
4. In the ***Additional Options*** window, take the defaults and click **Next**.
5. In the ***Paths*** window, take the defaults and click Next.
6. Review your selections and click **Next**.
7. Review the ***Prerequisites Check***. Don’t worry about the warnings. They are just warnings. Click **Install**.

- The installation will complete and your server will restart. It takes a bit of time to complete this procedure.

3.0 Managing Active Directory

The Local Users and Groups tool that you used in the previous lab cannot be used to set up users in your domain because they are local to the server where they were created. We must create Domain Users and Groups, using the **Active Directory Users and Computers** tool. The process is very similar, but you will be creating these users and groups in the AD DS database that is used by all users and computers in the domain, not just on the local server.

1. From the **Tools** menu, select the tool called, **Active Directory Users and Computers.**
2. When the tool opens, you should see the name of your domain in the left pane. Click your domain name to view the contents of the domain in the right pane of the tool. You will see several containers, including **Users**
3. Double-click the **Users** container to view the contents. You should only the built-in user and group accounts since the Local Users and Groups you created in Lab 7 were created on Server1.

3.1 Creating a New OU

Continue from above

1. Right-click your Domain name in the left pane. From the pop-up menu, select **New** and then **Organizational Unit**.
   We are going to create a new OU for our Head Office and create users, groups and computers within that OU. This would allow us to delegate administration of our Head Office to a particular group of Administrators at that office.
2. Type in ***Head Office*** for the name of the OU, and click OK. The Head Office OU should appear in your list.

3.2 Creating Computer Accounts

Computer accounts can be created as the computers join the domain, or an administrator can create the accounts for the computers ahead of time, which is what we are going to do now.

1. Right-click the **Head Office** OU and select **New** and then **Computer**. Enter the name ***HO-FileServer1*** in the computer name field.
2. Create 3 more computer accounts called: ***HO-ACCT1, HO-MGMT2, HO-SALES3***

3.3. Creating Domain Users

1. Right-click the **Head Office** OU, select **New** and then **User**. The ***New Object – User*** dialog box will appear.
2. Create a new user by filling in the fields with the following information:
   First Name: ***Danny***
   Last Name: ***Roy***
   username: ***droy1***
   Click **Next**.
3. On the Password screen, type a password of ***P@ssw0rd***, confirm it, and place a checkmark next to ***Password Never Expires***. Click **Next**, and then click **Finish**.
4. Create 3 more users in Head Office with the same password settings as above and using the following information:
   Jane Doe, jdoe23
   Marge Simpson, msimpson
   Super Man, sman45

3.4 Creating Domain Local Groups

A domain local security group is used when Active Directory is deployed. This type of group is typically used to manage resources in a domain and to give global groups from the same and other domains access to those resources. A Domain Local Group can contain user accounts, global groups and universal groups, but it is a good practice to only add groups to a local group.

1. In *Active Directory Users and Computers*, right-click the **Head Office** OU and select **New** and then **Group**. Enter ***Executives*** as the Group Name, the select **Domain Local** group for the ***Group Scope***, and leave the ***type*** as **Security**.
2. Create 2 more Domain Local Groups named ***SalesReps*** and ***Designers***.

3.5 Creating Domain Global Groups

Creating Domain Global Groups is exactly the same as Domain Local Groups. Typically, Global Groups contain user accounts then the Global Groups are added to the Local Groups to gain access to resources who list the Local Group in the ACL.

1. In *Active Directory Users and Computers*, right-click the **Head Office** OU and select **New** and then **Group**. Enter ***HO-Executives*** as the Group Name, the select **Global** group for the ***Group Scope***, and leave the ***type*** as **Security**.
2. Create 2 more Domain Global Groups named ***HO-SalesReps*** and ***HO-Designers***.

3.6 Modifying Group Membership

We will add users to a Global Group and then place the Global Group into a Domain Local Group.

1. Click the **Head Office** OU in the left pane so the contents of Head Office are displayed in the right pane.
2. Double-click your **HO-SalesReps** Global Group, and the groups **Properties** dialog will appear.
3. Click the **Members** Then click **Add** to add users to the Global Group. Click the **Advanced** button and then select **Object Types**. Ensure that only **Users** has a checkmark beside it. Then click **Find Now**. All of the user accounts should appear in the list. These user accounts will be a combination of Local Users in the Users folder and Domain Users which we have created in the Head Office OU.
4. Select any three users from the Head Office OU then click **OK**. The users should be added to your Global Group.
5. Now click the **Member Of** tab, and select **Add** to Add this Global Group to a Domain Local Group. Click **Advanced**, then **Object Types**. Make sure only **Groups** is selected. Then **Find Now** to see a list that contains only groups.
6. Find your Domain Local Group called **SalesReps**. Select it and then click **OK**, then **OK** Then **OK** again on the *HO-SalesReps Properties* dialog box.
7. To verify that you have added your Global Group to the Domain Local Group, double-click your **SalesReps** Local Group and click the **Members** Tab to see the Global Group listed.

4.0 Creating a Second Domain Controller for your Domain

1. Create a new Virtual Machine with the following specifications:
   Server4
   - Guest Operating System: Microsoft Windows: **Windows Server 2012**
   - Virtual machine name: **Server4**
   - Location: Make sure to browse and find your SSD just as you did in lab 1
   - Maximum Disk Size: **40GB**; Store virtual disk as a single file
   - Customize Hardware: Memory: **4096 MB**
   - Make sure your network card is set to **Bridged**.
2. Install Windows Server Datacenter (with a GUI) and use the information from your Prelab Chart to

configure the computer name and **manually configure TCP/IP, using the information from the PreLab Chart. Make sure your Preferred DNS is set to the IP address of Server 2.**

3. Install the Active Directory role on your server (section 1.0 from this lab).
4. Promote your server to be a Domain Controller (section 2.0 from this lab), but instead of creating a new domain in a new forest, you will **join an existing domain**. You will need to enter your domain name (**SenecaID.com**) and the credentials of the domain Administrator username and password for the domain to prove you have administrative privileges on the domain. The format of the CREDENTIALS is: **SenecaID.COM\Administrator** and the password should be **P@ssw0rd**.
5. You will need to restart your server to complete the procedure. Once you have restarted, login as the Administrator of the domain. You should see all of the domain users and computers in the OU that was previously created.
6. Create a new **domain user account** from Active Directory Users and computers on Server 4, with the following specifications:
   First Name: ***Hans***
   Last Name: ***Heim***
   username: ***hheim***
   Password: P@ssw0rd

5.0 Adding a Windows Client to your Domain

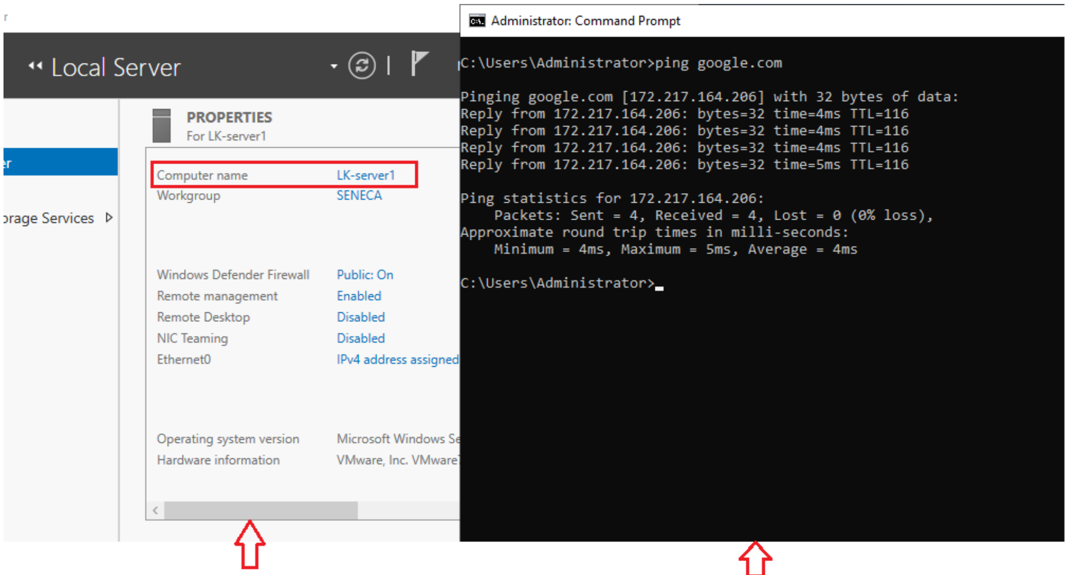
1. Open your Windows Client VM and login using the local account you created in Lab 1. This user account has administrative privileges on the local computer.
2. **Verify your TCP/IP settings before continuing**. Make sure your IP address, and subnet mask are correct (from the PreLab chart), and your preferred DNS server is your Server2's IP address.
3. Click the Windows key and type PC into the search field. Select **PC Info** from the list.
4. You will see a button at the top that will allow you to **Join a domain**.
5. Enter the domain name and the domain Administrator username and password (same as above).
6. Once you have joined the domain, you will need to restart the client VM. Login using the **hheim** user account that was created in the previous section.

For this lab to be marked as complete, you will have to do the following. From either Server2 or Server 4:

- **Take a screenshot that shows the Organizational Unit is created**
- **Take a screenshot that shows your Domain Local Group with your Domain Global Group as a member.**
- **Take a screenshot that shows your Domain Global Group containing the Domain User accounts.**
- **Take a screenshot that shows the Computer Accounts you created.**

Whenever you take a screenshot of your actual work that you are asked to demonstrate, please make sure you take a

screenshot of your computer name along with the actual work together (side by side). For reference, please see the screenshot below:



Computer name LK-server1
Workgroup SENECA

Windows Defender Firewall Public: On
Remote management Enabled
Remote Desktop Disabled
NIC Teaming Disabled
Ethernet0 IPv4 address assigned

Operating system version Microsoft Windows Se
Hardware information VMware, Inc. VMware

```
C:\Users\Administrator>ping google.com

Pinging google.com [172.217.164.206] with 32 bytes of data:
Reply from 172.217.164.206: bytes=32 time=4ms TTL=116
Reply from 172.217.164.206: bytes=32 time=4ms TTL=116
Reply from 172.217.164.206: bytes=32 time=4ms TTL=116
Reply from 172.217.164.206: bytes=32 time=5ms TTL=116

Ping statistics for 172.217.164.206:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 5ms, Average = 4ms

C:\Users\Administrator>_
```

Window to show your computer name

Window for Actual work asked to demonstrate

Insert all screenshots in a word file, save the file as Domain.docx. Upload the word file into the blackboard

From Client1:

- login to the domain using the *hheim* domain user account. Take a screenshot that shows that your client logins into the domain. Upload the screenshot into blackboard