# Lab 2 – Configuring a Server

Upon completion of this Lab you will have Windows Server 2019 configured and be familiar with several Windows Server Configuration Tools.

BEFORE YOU BEGIN:

Before you begin Lab 2, please make sure you have installed one more virtual machine, Server2 and install **Windows Server 2019 (Desktop Experience)**.

Configure your installation of Windows Server 2019 on Server2 statically and assign the IP address from the table in the prelab. If you use ***ipconfig*** to check, you should see an IP address similar to this: **10.0.xxx.20**

Check to make sure that Server 1 has TCP/IP Automatically configured. If you use ***ipconfig*** to check, you should see an IP address that comes from the Seneca DHCP servers. It should be something like this: **142.204.x.x.**

Make these corrections before starting the lab, or you will have problems.

Complete this lab on Server 2 unless otherwise noted in the instructions

Approximate completion time: 90 minutes.

### *1.0 Installing and Removing Roles*

In this activity, you will use three different methods to Install and Remove Roles on your Windows Server installed on Server2.

### *1.1 Install and Remove Roles with Server Manager*

1. Open **Server Manager**. From the Dashboard, click **Add Roles and Features**. Click Next. Select **Role based or feature-based installation**, click Next. Select your server name from the list. Click Next.
2. Place a checkmark in the checkbox next to the following Roles: **Print and Document Services, Web Server (IIS) and DNS Server**. Click Next. As you select each role, add any necessary features that it prompts you to install. Take all default settings. Select the option to restart if required. Click Install and wait for the installation to complete.
3. In the Server Manager, under Roles and Server Groups, review the installed roles.

4. Select **Remove Roles and Features** from the **Manage** menu (upper right). Click next until your reach the list of roles. Remove the checkmarks next to Print and Document Services. Click **Remove Features**. Click Next. Accept the default settings. Click **Remove**. Click **Close**.
5. View the Roles and Server Groups area, and ensure that only the **File and Storage, Web Server (IIS)** and **DNS Server** Roles are installed. We will be using these roles later in the lab.

### *1.2 Install and Remove Roles with PowerShell*

Server Manager's command-line counterpart is the **ServerManager** module for Windows PowerShell. This module is not imported into Windows PowerShell by default. Instead, you need to import the module before you can use the cmdlets it provides.

To import the Server Manager module, enter **Import-Module ServerManager** at the Windows PowerShell prompt.

Once the module is imported, you can use it with the currently running instance of Windows PowerShell. The next time you start Windows PowerShell, you'll need to import the module again if you want to use its features.

1. Open a Windows PowerShell session with elevated user rights.

   To do this, from the Windows Start Screen (Winkey) or on the Task Bar – blue parallelogram with a >_

   Verify that the window that appears is labelled as **Administrator: Windows PowerShell**

2. Load the Server Manager module into the Windows PowerShell session before working with Server Manager cmdlets

   Type the following, and then press Enter.

   ```
   Import-Module Servermanager
   ```

3. If you do not know the command name of the role, role service, or features you want to install type the following, and then press Enter to return a list of all command names in the Name column.

   The command name is required for the next step.

```
Get-WindowsFeature
```

The **X** next to the role/feature, indicates that it is currently installed. Look up the name for the Print and Document Services Role.

4. Type the following, in which name represents the command name of the role, role service, or feature that was obtained in the previous step, and then press Enter to install the File Services role.

   The -restart parameter restarts the computer automatically after installation is complete, if a restart of the computer is required by the role or feature.

   ```
   Add-WindowsFeature print-services –restart
   ```

   You can install multiple roles, role services, and features by using commas to separate the command names.

5. Type the following command to Remove the File Services Role, and then press Enter.
   ```
   Remove-WindowsFeature print-services –restart
   ```
6. Exit PowerShell by typing **exit**.

## 2.0 Configure Web Server (IIS) and DNS Server.

The Web Services and DNS Services Roles were installed in section 1.1 of this lab. In this activity, you will do some basic configuration of your Web Server and you will configure DNS to resolve a name to gain access to your web server.

### *2.1 Personalize Your Website and Test*

1. In Server Manager, from the Tools pull-down menu (upper right), find and run **Internet Information Services (IIS) Manager**.
2. In the left pane, expand the tree under your server name until the **Default Web Site** appears.
3. Right-click on the **Default Web Site** and choose **Explore**.
4. From the new Window you can modify your starter web site by opening the file **iisstart** in Notepad. You will be editing HTML code in this file.

To make a basic modification to the site, change the title of the page by modifying the text that appears between the <title> tags to include your name. You may also make any other modifications you like (not required). Save and exit the file.

5. To view your web page locally, open Internet Explorer, and type 127.0.0.1 in the browser address bar. (Note: 127.0.0.1 is the loopback address and not your IP address. It just finds the local host, regardless of the IP) The default IIS7 webpage should appear, and the tab title should be the title you entered above.

### *2.2 Configure a New Domain Name*

1. In Server Manager, from the Tools pull-down menu*, select **DNS**. The DNS Manager will appear, displaying your server name, which should be your SenecaID (not a name that starts with WIN) in both the left and right panes.*
2. *Expand the tree for your server [>], then right-click **Forward Lookup Zone**, and select **New Zone**. Click **Next**. Make the zone a Primary Zone. Click **Next**.*

   *Type in a zone name for your web server. Use your **Seneca ID + .com**. Click **Next** and allow the wizard to create the zone file for you. Click **Next**.*

   *We will not require dynamic updates. Click **Next** and click Finish.*

3. Expand the Forward Lookup Zone in the left pane until you see your zone name (SenecaID.com). Right-click on your new domain name and choose to **Add New Host**. The New Host dialog box will appear. Leave the name blank, and add the IP address of your web server (the IP address that was manually configured for your installation of Windows Server on Server2) to the IP address field. You do not need to create a pointer record. Click **Add Host**, and then **OK** when you get your success message. Click **Done** to close the window.
4. Modify your TCP/IP settings to include the IP address of your DNS server in the Preferred DNS Servers field. Your Preferred DNS server is also the IP address assigned to your server. Once we installed the DNS Role, it turns your server into a DNS Server.
5. To test the new domain name locally, open Internet Explorer and type the domain name you entered above (SenecaID.com), in the address bar field. Your webpage should display as it did before. This proves that your DNS Server (that you just configured) is resolving the name (SenecaID.com) to the correct IP address to find the web page on your web server. If your webpage does not appear, check your Preferred DNS settings to make sure you have entered the correct IP address. It should be your server’s IP address: 10.0.xxx.20

## 2.3 Adding Authentication to Your Web Site

1. Using Server Manager on Server2, click IIS in the left pane. Your server name should appear in the right pane. Right-click the server and select Add Roles and Features from the menu. Select Next a couple of times until you reach the screen with the roles displayed. Scroll down to your Web Server Role and expand it [>] to see the available roles and features. Select Web Server. Then select Security. Place a checkmark next to Basic Authentication. Click Next, Next and Install. Close the window once the installation completes.
2. Open the **IIS Manager**. Expand the tree to find your Default Web Site. Click on the **Authentication** icon in the middle pane. **Disable** Anonymous Authentication, and **Enable** Basic Authentication.
3. Test your website again. What is the difference now? You should be able to use your **Administrator** account to login to gain access to the website. This is the only user account currently available on your server.

## 2.4 Configuring Your Client to use DNS on your Server

1. Start your Client1 VM and login with your **SenecaID** username.
2. In your TCP/IPv4 settings, configure the **Preferred DNS server** address with the IP address of Server2 (this is where your DNS server is installed and configured to resolve your website)
3. Using Internet Explorer, test that you can access the website on Server2 from the client VM by entering ***SenecaID.com*** in the address bar of your browser. When prompted for a username and password, you will use **Administrator** and P@**ssw0rd**.

## 3.0 Editing the Registry (Server2)

The Registry is a protected database, which stores all computer, system, application and user settings. In this activity, you will use **RegEdit** to make server configuration changes. Be very careful when making these changes as you can cripple your server by making errors. The changes we are making are not critical, but we will still Export registry keys for a backup, and we can Import them afterwards if we cause a problem.

### *3.1 Export Registry Key*

1. Open the Run command field by typing ***Winkey+R***. Type **regedit** from the Run command to open the registry editor.
2. Use the navigation tree to navigate to the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system

3. Click on the **File** menu, then **Export**

   In the File name, save to the C: drive of your VM and enter a name for the saved registry key.

   Save the key as **RegistryLegalNotice.reg.** This will allow us to save the original settings so we can revert back if there is a problem.

### *3.2 Display a Legal Notice Message*

You will add a special message to users that this computer is secure. Only authorized users are allowed to the company network. Many companies use such a message to deter non-authorized users. It is also a good way to display a common message to all users who log in, such as “Please submit your time sheets today.”

1. Use the registry path from #2 above and double click on the **legalnoticecaption** key.

   Enter the value **This is a Secure PC**.

2. Double click on the **legalnoticetext**.

   Enter the value **Only authorized users can log into this computer and use this network. Non-authorized users will be recorded and prosecuted.**

3. Under the **View** menu, select **Refresh**.

4. Close the registry editor and log off. To log off, go to the Start Screen (Winkey), select Administrator from the top right corner and Sign Out.

5. Log in to your server again. You should see a new splash screen with your secure message before you are presented with the Login screen.

### 4.0 More Registry Editing

Using the procedure from the previous exercise, make the following changes to the registry. Do the EXPORT of the individual registry keys, but do not IMPORT them at the end unless you have made a mistake.

### *4.1 Change the Registered Owner*

You can change the registered owner's name and organization that's stored by Windows, viewable via the Windows winver.exe program. This is useful, for example, if your organization changes its name or is bought out, or if they buy used PCs. Changing the registration info isn't extremely important, but can be useful as some program installers prefill their registration details with those from Windows.

1. *Use the following key:*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
2. *Change the following registry value: Value name:* ***RegisteredOwner*** *Value data:* ***Your_Name***
3. ***Change the following registry value:*** *Value name:* ***RegisteredOrganization*** *Value data:* ***Your_Organization***
4. *Exit Registry Editor.*
5. *Type* ***winver.exe*** *at the Run command to view your changes.*

### *4.2 Disable Shutdown Event Tracker*

The Shutdown Event Tracker dialog box is used to track intentional and unintentional shutdowns of the server. Servers are usually required to be up and running as much as possible and servers being shut down means employees are unable to do their work, therefore it may be necessary to audit when and why servers have been shut down. In our lab environment, this is not necessary, so we can make the following change in our registry so the Shutdown Event Tracker window does not appear each time we shut down the server.

1. Use the following key in the registry:**HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT**

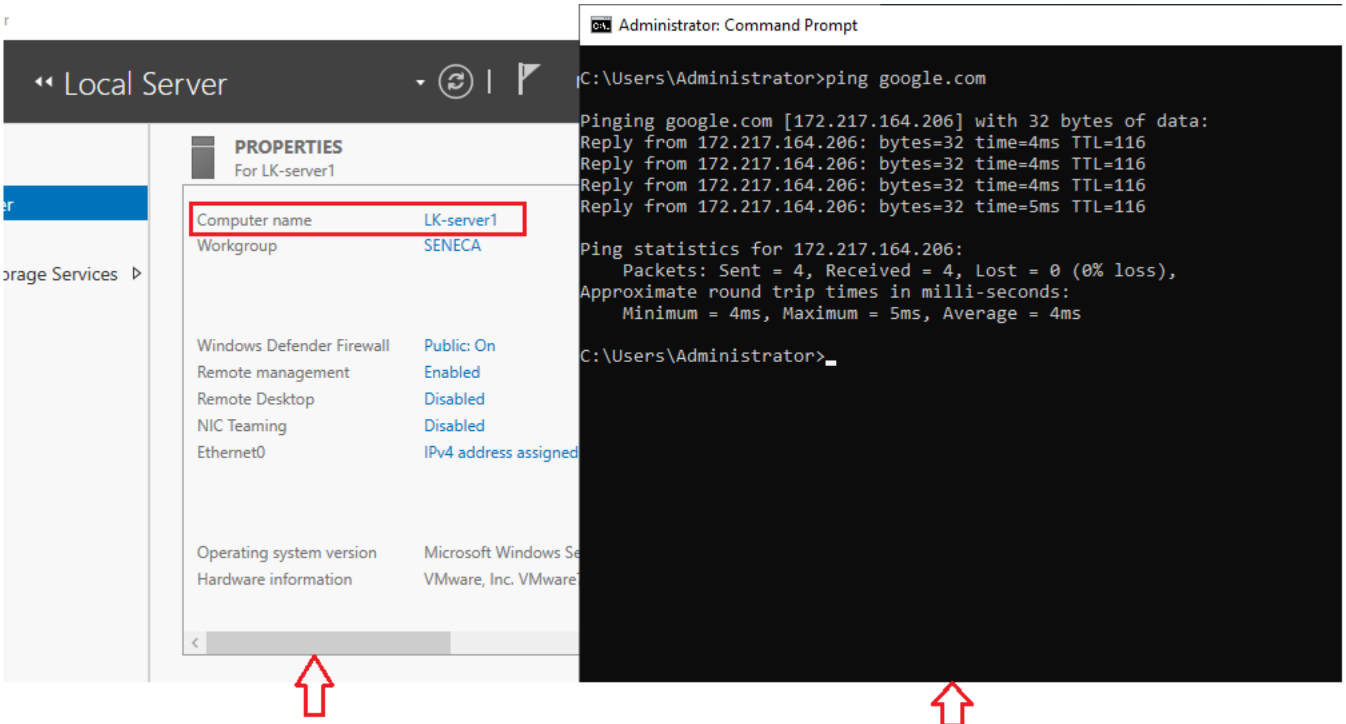
*****Be very careful when navigating through the path. Many students make a mistake with this registry path.**

1. Create a new key called **Reliability** by highlighting **WindowsNT**, then on the **Edit** menu, point to **New** and then **key.** Type **Reliability** into the name.
2. Then highlight **Reliability,** on the **Edit** menu, click **New** and **DWORD** Value, and then add the following registry values:Value name: **ShutdownReasonOn**
3. Exit Registry Editor.
4. Test your change by shutting down your server. Notice if the Shutdown Event Tracker Window appears or not.

For this lab to be complete, you must demonstrate the following

- In Server 2, take a screenshot that shows your DNS server is resolving the domain name typed into your browser and authentication enabled on the website by opening Internet Explorer and typing in your domain name. Save the screenshot as Lab2-DNSResolve.jpg
- Show that you can do the above with your Client VM and save the screenshot as Lab2-DNSResolveC1.jpg
- Take a screenshot that displays the change in name of the Registered Owner by typing Winver.exe from the run command. Save the screenshot as Lab2-RegisteredOwnerReg.jpg
- Take a screenshot that demonstrates that the Shutdown Event Tracker does not appear when you shutdown your server. Save the screenshot as Lab2-ShutdownReg.jpg

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**

Upload Lab2-DNSResolve.jpg, Lab2-DnsResolveC1.Jpg, Lab2-RegisteredOwnerReg.jpg, Lab2-ShutdownReg.jpg into the Lab 2 submission link in blackboard.