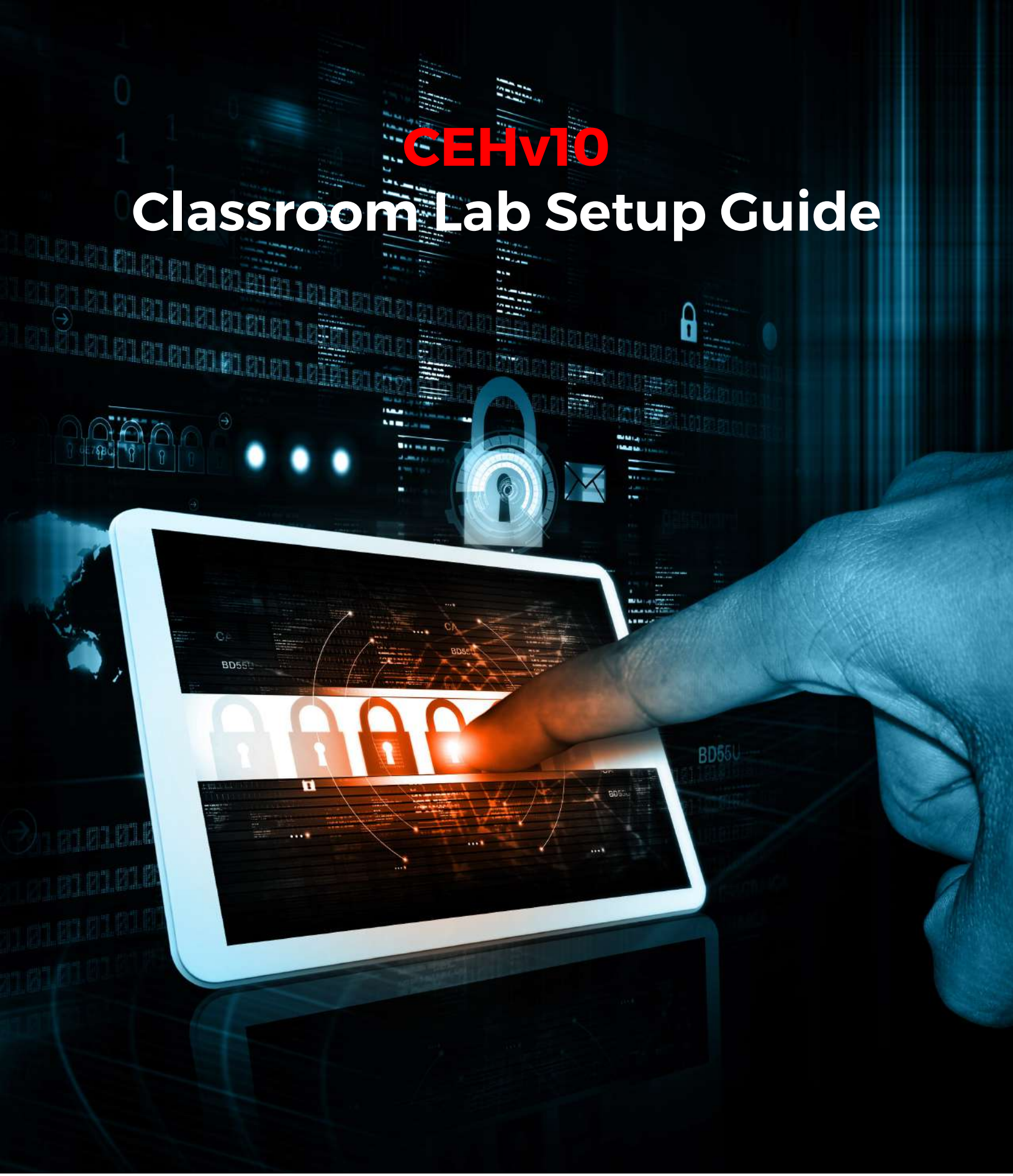
CEHv10

Classroom Lab Setup Guide



EC-Council

www.eccouncil.org

Table of Contents

Classroom Setup Instructions: CEHv10

This document contains setup instructions for the EC-Council Certified Ethical Hacker (CEH) course. The course requires a standard modular classroom seating configuration, one computer for each student, one computer for the instructor, a dedicated hub or switch (hub preferred), dedicated firewall, and Internet connection. This class teaches network attack and penetration methodologies. It is imperative that network used for this class be separated both logically and physically from any other networks in the training facility to preclude students "accidentally" conducting exploits on other computers within accessible networks.

Before beginning the class, install and configure all computers using the information and instructions that follow.

Classroom Requirements

This section describes classroom equipment required for the EC-Council Certified Ethical Hacker course.

Classroom Equipment

The following equipment is required for the general classroom setup:

- Climate control system adjustable within the classroom
- Lighting controls, adjustable within the classroom
- Whiteboard, 3 feet X 6 feet (1m X 2m) or larger
- Markers, whiteboard, assorted colors
- Eraser, whiteboard cleaner liquid (3 oz minimum)
- Towels, paper
- Easel with flipchart or butcher paper pad, 24 inches X 36 inches
- Felt tip pens, blue and black required, other colors optional, chisel tip (not fine-point)
- Screen, projection, 6 feet diagonal measurement (non-reflective whiteboard surface may be substituted)
- Instructor station:
  - Desk, chair, and ergonomic
  - Power outlet
  - Network jack
  - Projector, LCD, capable of 740 X 1280 pixels minimum w/ all connecting cables
- Student station (per student)
  - Chair, ergonomic
  - Workstation, minimum horizontal workspace 9 square feet (3 feet X 3 feet)
  - Power outlet, one per student station
  - Network jack, one per student station

Hardware

Hardware requirements for instructor, student and victim computers are identical:

- Intel Core i5 or equivalent CPU with minimum CPU speed of 3.2 GHz
- Minimum of 8 GB RAM or more (16 GB recommended)
- Hard disk, 500 GB or larger, 7200 RPM or faster
- DVD drive (DVD R/W drive preferred)
- 1 Network adapter (minimum of a 10/100 NIC, but a 10/100/1000 is preferred), full duplex (disable any additional network adapters installed)
- Monitor (minimum requirement is 17-inch LCD)
- Mouse or compatible pointing device, and sound card with amplified speakers
- Internet access
- 2 Wireless Network adapter (PCI or USB)*

The following additional hardware is also required:

- A switch with sufficient ports to allow connection of all instructor and student workstations plus at least 5 additional, unused ports for connection of additional equipment or for use as "spares."

---

*If wireless network adapters are not available for all classroom machines, at least the Instructor machine must be so equipped.

Software

All computers in the class require the following software:

- Any Windows or Linux OS capable of running VMware Workstation
- VMware Workstation Pro
- CEH Tools downloadable from Aspen portal

Classroom Connectivity

As this class teaches network attack methodologies, the network for the class must be logically and physically separated from any other networks present in the training facility and must have its own connection to the Internet.

Configuration

This section describes the procedures for setting up the instructor, victim and student computers as well as general directions for the configuration of the firewall appliance.

This guide assumes that you will use disk-imaging software to create images of the classroom computers for future use. To that end, configuration tasks common to all computers are presented first. Perform these tasks on the computer that will become the Instructor computer. Create a disk image after setting up a single student computer. You may then deploy this image to remaining classroom machines while completing configuration of the Instructor computer.

Because the Instructor computer is configured as a DHCP server that provides IP addresses to the student machines, the installation and configuration of the Instructor computer must be completed before final configuration of the student machines can begin. The Victim machine uses a static IP address and so can be configured at any time after the base image has been deployed.

Setup Document Overview

This document provides background information for technical staff responsible for setting up a training room facility for the CEH course. This guide describes the requirements for the network equipment and computer stations that are installed and configured by the facilities personnel for the training courses.

Training Room Environment

The training room environment consists primarily of the following equipment:

- Instructor's Computer
- Student Workstation

Equipment	Number (Class of 12 Students)	Operating System	Minimum System Requirements
Instructor's Computer	1	Any Windows/Linux OS	Intel Core i5 or equivalent PC with 200 GB free disk space, minimum of 8 GB RAM, 1 NIC, 17-inch monitor, 2 Wireless Network adapter (PCI or USB) and compatible mouse
Student Workstations	12	Any Windows/Linux OS	Intel Core i5 or equivalent PC with 200 GB free disk space, minimum of 8 GB RAM, 1 NIC, 17-inch monitor, Wireless Network adapter (PCI or USB) and compatible mouse

Instructor's Computer

The instructor's computer must:

- Be installed with Windows Server 2016, latest service packs and full patches applied
- Download all CEH Tools from Aspen to your hard drive in **D:\CEH-Tools** folder for easy access (See CT#1 in Configuration Task section)
- Be installed with VMware Workstation Pro in Host Machine (See CT#2 in Configuration Task section)
- Be Configured with Virtual Network in the VMware Virtual Network Editor (See CT#3 in Configuration Task Section)
- Be installed with a Windows Server 2016 Guest Operating System in VMware Workstation (See CT#4 in Configuration Task section)
- Be configured with **Internet Explorer Enhanced Security Configuration** (See CT#5 in Configuration Task section)
- Be running IP protocol
- Be installed with IIS (Internet Information Services), File Services, SNMP and Remote Access roles in Windows Server 2016 (Virtual Machine) (See CT#6 in Configuration Task section)
- Be installed with guest operating systems (Kali Linux, Ubuntu and Android) (See CT#7, CT#8, and CT#9 in Configuration Task section)
- Be configured with the logon account to username: *administrator*, password: *Pa$$w0rd* in all the Windows virtual machines
- Be installed with ES File Explorer File Manager in Android machine (See CT#9 in Configuration Task section)
- Have CEH-Tools shared as '**Z:**' drive in Windows Machines (Mapping Z:\ drive) (See CT#10 in Configuration Task section)
- Have CEH-Tools shared in Kali Linux (See CT#11 in Configuration Task section)
- Have CEH-Tools shared in Ubuntu (See CT#12 in Configuration Task section)
- Have CEH-Tools shared in Android (See CT#13 in Configuration Task section)
- Have Adobe Acrobat and WinRAR installed in all the Windows machines (both can be found in Lab Prerequisites directory in **Z:\CEH-Tools** folder) (See CT#14 and CT#15 in Configuration Task section)
- Have Windows Explorer set to show all files, file types and extensions (See CT#16 in Configuration Task section)
- Have installed latest versions of Web browsers: Firefox, and Chrome (See CT#17 in Configuration Task section)
- Have password complexity disabled in all the Windows virtual machines (See CT#18 in Configuration Task section)

- Have demo user accounts created in all the machines (See CT#19 in Configuration Task section)
- Be installed with Active Directory and Create User Accounts in Windows Server 2012 virtual machine (See CT#20 in Configuration Task section)
- Be installed and configured with SNMP Services in Windows Server 2016 and Windows Server 2012 virtual machines (See CT#21 in Configuration Task Section)
- Be installed with SQL Server Express 2017 in Windows Server 2016 virtual machine (See CT#22 in Configuration Task section)
- Have firewall Turned off in all the Windows virtual Machines (See CT#23 in Configuration Task section)
- Have Remote Desktop Connection enabled in all Windows virtual machines (See CT#24 in Configuration Task section)
- Screen Savers turned off in the Windows Server 2012 and Windows 8 virtual Machines (See CT#25 in Configuration Task section)
- Ping test verified between all the machines in your Network (See CT#26 in Configuration Task section)
- FTP Server enabled and configured in Windows 10 virtual machine (See CT#27 in Configuration Task section)
- Be installed with GoodShopping and Moviescope demo websites in Windows Server 2016 virtual machine (See CT#28 and CT#29 in Configuration Task section)
- Be Configured the hosts file in all the virtual machines (See CT#30 in Configuration Task section)
- Be installed with WAMP Server, WordPress, and DVWA websites in Windows Server 2012 virtual machine (See CT#31, CT#32, and CT#33 in Configuration Task section)
- Be configured Windows Components (See CT#34 in Configuration Task section)
- Be disabled Server Manager on Startup in Windows Server 2016 and Windows Server 2012 (See CT#35 in Configuration Task section)
- Have snapshots taken for virtual machines (See CT#36 in Configuration Task section)
- Have an LCD Projector connected to instructor's machine

Student Workstations

Student workstations must:

- Be installed with Windows Server 2016, latest service packs and full patches applied
- Download all CEH Tools from Aspen to your hard drive in **D:\CEH-Tools** folder for easy access (See CT#1 in Configuration Task section)
- Be installed with VMware Workstation Pro in Host Machine (See CT#2 in Configuration Task section)
- Be Configured with Virtual Network in the VMware Virtual Network Editor (See CT#3 in

Configuration Task Section)

- Be installed with a Windows Server 2016 Guest Operating System in VMware Workstation (See CT#4 in Configuration Task section)
- Be configured with **Internet Explorer Enhanced Security Configuration** (See CT#5 in Configuration Task section)
- Be running IP protocol
- Be installed with IIS (Internet Information Services), File Services, SNMP and Remote Access roles in Windows Server 2016 (Virtual Machine) (See CT#6 in Configuration Task section)
- Be installed with guest operating systems (Kali Linux, Ubuntu and Android) (See CT#7, CT#8, and CT#9 in Configuration Task section)
- Be configured with the logon account to username: *administrator*, password: *Pa$$w0rd* in all the Windows virtual machines
- Be installed with ES File Explorer File Manager in Android machine (See CT#9 in Configuration Task section)
- Have CEH-Tools shared as '**Z:**' drive in Windows Machines (Mapping Z:\ drive) (See CT#10 in Configuration Task section)
- Have CEH-Tools shared in Kali Linux (See CT#11 in Configuration Task section)
- Have CEH-Tools shared in Ubuntu (See CT#12 in Configuration Task section)
- Have CEH-Tools shared in Android (See CT#13 in Configuration Task section)
- Have Adobe Acrobat and WinRAR installed in all the Windows machines (both can be found in Lab Prerequisites directory in **Z:\CEH-Tools** folder) (See CT#14 and CT#15 in Configuration Task section)
- Have Windows Explorer set to show all files, file types and extensions (See CT#16 in Configuration Task section)
- Have installed latest versions of Web browsers: Firefox, and Chrome (See CT#17 in Configuration Task section)
- Have password complexity disabled in all the Windows virtual machines (See CT#18 in Configuration Task section)
- Have demo user accounts created in all the machines (See CT#19 in Configuration Task section)
- Be installed with Active Directory and Create User Accounts in Windows Server 2012 virtual machine (See CT#20 in Configuration Task section)
- Be installed and configured with SNMP Services in Windows Server 2016 and Windows Server 2012 virtual machines (See CT#21 in Configuration Task Section)
- Be installed with SQL Server Express 2017 in Windows Server 2016 virtual machine (See CT#22 in Configuration Task section)
- Have firewall Turned off in all the Windows virtual Machines (See CT#23 in Configuration

Task section)

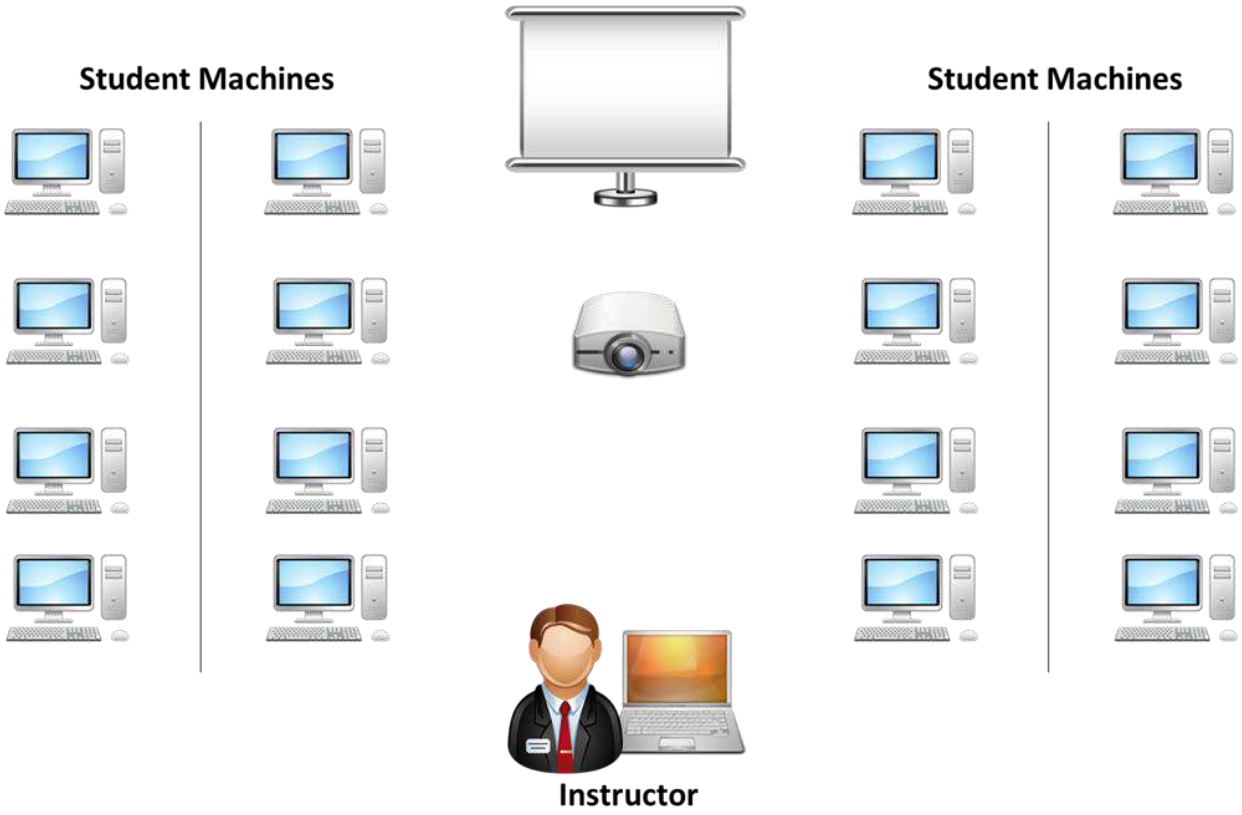
- Have Remote Desktop Connection enabled in all Windows virtual machines (See CT#24 in Configuration Task section)
- Screen Savers turned off in the Windows Server 2012 and Windows 8 virtual Machines (See CT#25 in Configuration Task section)
- Ping test verified between all the machines in your Network (See CT#26 in Configuration Task section)
- FTP Server enabled and configured in Windows 10 virtual machine (See CT#27 in Configuration Task section)
- Be installed with Goodshopping and Moviescope demo websites in Windows Server 2016 virtual machine (See CT#28 and CT#29 in Configuration Task section)
- Be Configured the hosts file in all the virtual machines (See CT#30 in Configuration Task section)
- Be installed with WAMP Server, WordPress, and DVWA websites in Windows Server 2012 virtual machine (See CT#31, CT#32, and CT#33 in Configuration Task section)
- Be configured Windows Components (See CT#34 in Configuration Task section)
- Be disabled Server Manager on Startup in Windows Server 2016 and Windows Server 2012 (See CT#35 in Configuration Task section)
- Have snapshots taken for virtual machines (See CT#36 in Configuration Task section)

Room Environment

- The room must contain a whiteboard measuring a minimum of 1 yard by 2-3 yards in length (1 meter by 2-3 meters)
- The room should contain an easel and large tablet (optional)
- The room must be equipped with legible black and blue felt tip pens (CHISEL-Point, not fine-tip)

Classroom Configuration

The configuration of this classroom is modular. Computers can be added or removed by either row or column, depending on the needs of the particular class. The following is a sample room setup that provides optimal support. This setup allows for ease of access to "***troublespots***" by the instructor, and allows students to break into functional small and larger teams.



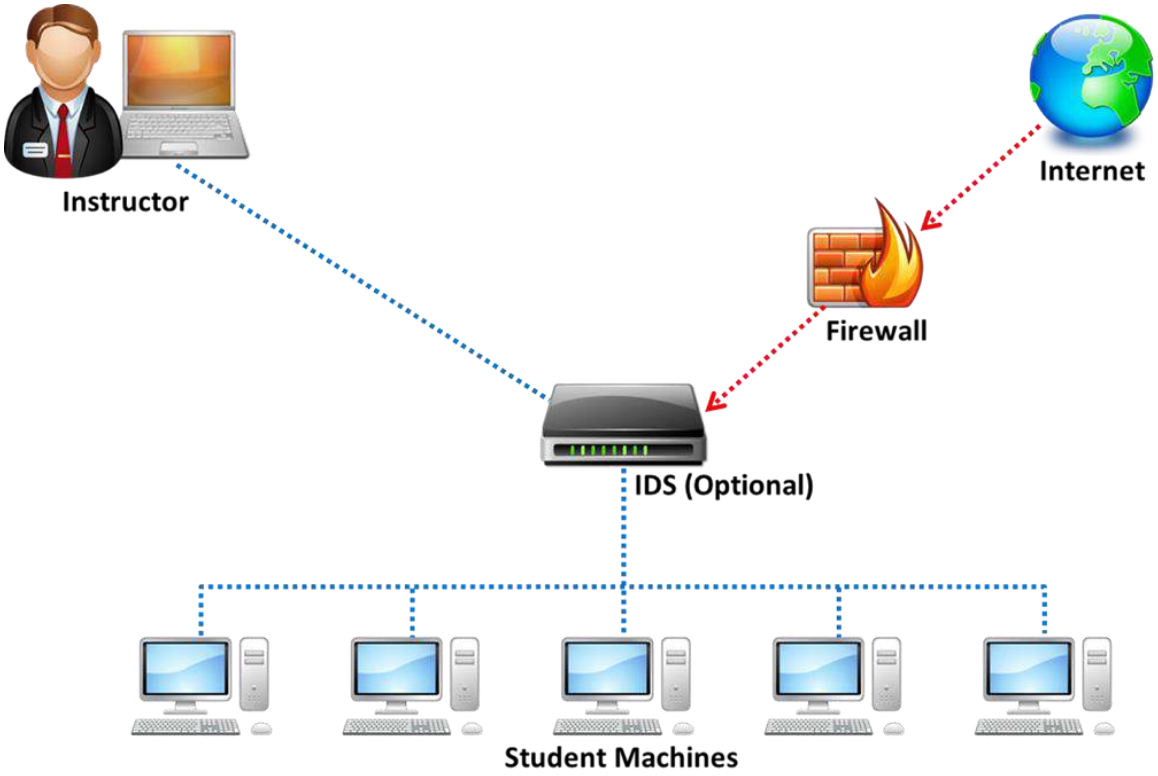
Computer Names

Assign computer names to student machines like CEHSTUDENT1, CEHSTUDENT2, CEHSTUDENT3, and so on. Instructor machine should be named as INSTRUCTOR and victim machine as VICTIM.

Network Topology

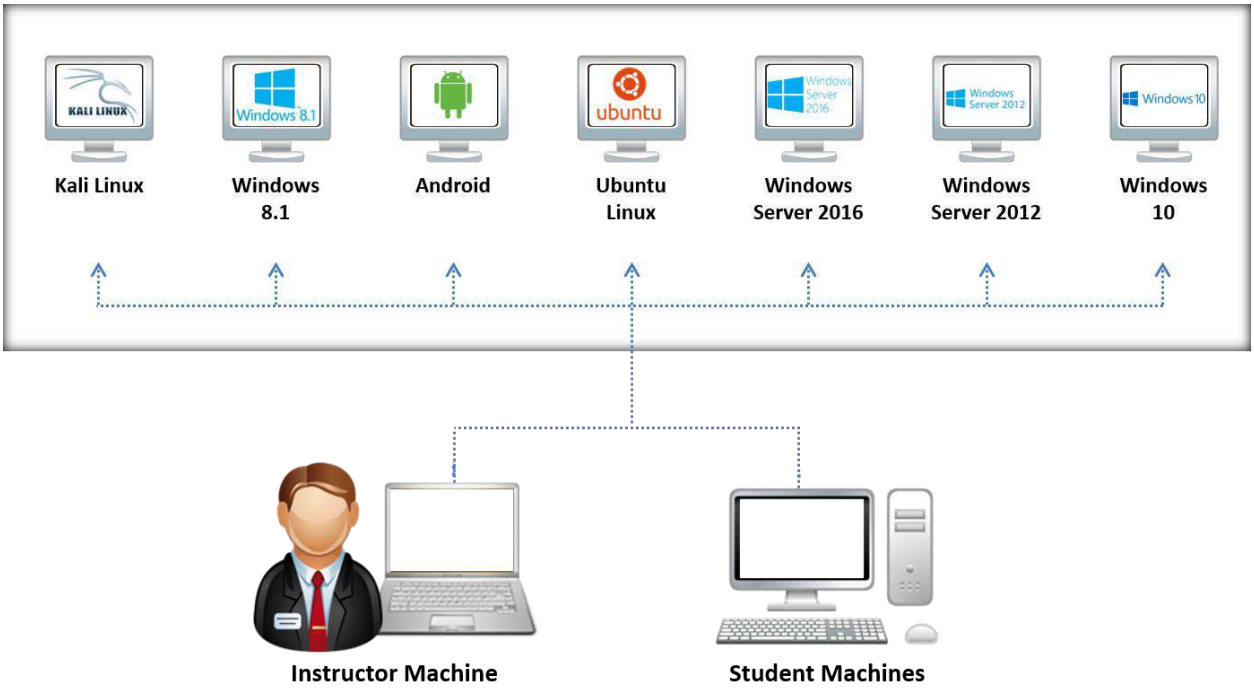
The training room must be physically isolated from any production network. Students must be able to access the Internet from their PCs. All computers are connected as one isolated network and domain. The common protocol is IP. All computers should have dynamic IP addresses using DHCP server. Configure the DHCP server scope to 10.0.0.0/24 IP addresses. This reduces potential problems when booting the virtual machines. NICs can be 10Mbit or 100Mbit (100Mbit is recommended). Layer-3 switch is recommended but not required instead of a standard switch (helpful for demonstrating tools in **Sniffer/Session Hijacking** modules). Cables must be bundled and tied out of pathways and work areas, and must be of sufficient length to avoid stress.

The training room must also have a wireless network (victim network) to demonstrate wireless hacking labs. The wireless network should be configured to use WEP keys for demonstration purposes. This network could be a part of above network subnet. Configure the wireless router for DHCP server scope.



Set up the machines based on the classroom setup diagram. The lab exercises for the students are instructor led and they are based on the hacking tools in the trainer slides. The instructors are encouraged to demonstrate and guide the students on the usage of the hacking tools against the Victim machines (virtual machines). Do not encourage live hacking on the Internet using these tools in the classroom. Please feel free to include your own exercises.

CEH VM Setup in Instructor and Students' Machines



Instructor and Student Machine Operating System: Any Machine Capable of Running VMWare (Fully Patched)

NDA Document

Download and print the student NDA document and have them ready for students to sign before the class starts on day 1. (Contact your ATC/EC-Council representative for download links)

Note: DONOT CONDUCT THE CLASS WITHOUT STUDENT SIGNING THIS DOCUMENT. Training Centers (ATC) should file the NDA document at their facility.

Instructor Acceptance

Before the training class is scheduled to begin, the instructor will visit the training facility to inspect and accept the setup. The technical contact (System Administrator) for the facility must be available to answer questions and correct any setup issues. Both the instructor and the facility technical contact will ensure completion of the following checklists before the training setup is deemed acceptable.

Firewall Settings

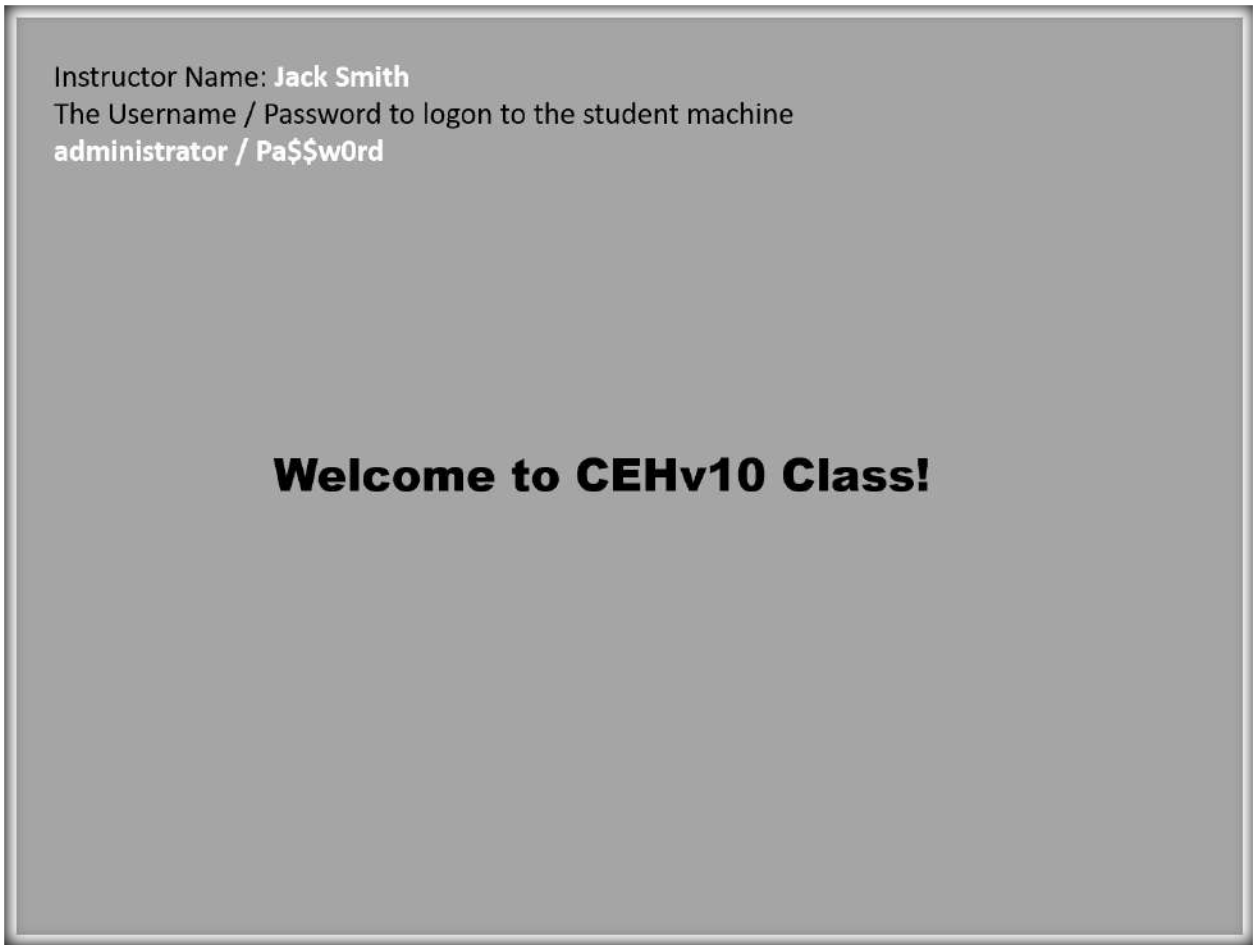
Do not block any ports while accessing the Internet through the firewall. You should be able to ping servers on the Internet

Blackboard

Write the following on the blackboard top left corner:

Instructor name: <Name of the instructor>

Provide Username/Password to logon to the student machine



Setup Checklist

The arrangement of items in the setup checklists is designed to allow the process to be completed in the most efficient manner possible and also validate that the setup has been done correctly. Before beginning the setup checklist, log off any connected users.

Tick Here	List
❑	Verify that VMware Workstation Pro Installed
❑	Verify that all CEH tools are on the computer in CEH-Tools folder in the D:\
❑	Verify that Internet access is available
❑	Visit https://www.eccouncil.org and view the page to check Internet access
❑	Open Command Prompt and type nslookup certifiedhacker.com and look for connection to the server
❑	Verify Acrobat Reader and WinRAR and command prompt extensions are installed
❑	Verify that the Instructor computer can image through the overhead projector
❑	Verify each computer has 200 GB or more free disk space
❑	Verify if you can successfully boot Windows Server 2016, Windows Server 2012, Windows 10, Windows 8, Kali Linux, Ubuntu, and Android VMs using VMware Workstation
❑	Cable wiring organized and labeled
❑	Student workstations and chair placement is satisfactory
❑	Placement of LCD (overhead) projector is appropriate
❑	Whiteboard and dry erase markers and erasers are available
❑	Instructor station is properly organized and oriented
❑	Computers are labeled with client number
❑	EC-Council courseware (Official EC-Council CEHv10 Box) is available for students
❑	Student NDA agreement downloaded and printed for every student in the class and placed on each student's desk
❑	Write down the facility's technical contact person's hand phone number. Contact him in case of network problem
❑	That the Internal network adapter is configured for the virtual machines and host

Instructor Acceptance

The technical contact (System Administrator) for the facility must be available to answer questions and correct any setup issues.

The Instructor will inspect both the classroom and the items covered in the setup checklist(s) to ensure that the classroom and setup meet EC Council standards. Any deficiencies discovered by the Instructor must be corrected before the scheduled start time for the class.

Assistance

If you have problems or require assistance in setting up the Lab for your CEH class, please e-mail partnersupport@eccouncil.org.

Detailed Setup Instructions - Configuration Tasks (CT)

CT#1: Download CEH Tools

1. Create a folder in the Drive **D:** named **CEH-Tools**
2. Login to your **Aspen** account (You will see your course listed under **My Courses**) → Click **TRAINING** button under the course to access the e-Courseware, Lab Manuals, and Tools in the **Training** area → Click **Download Tools** tab from the left-pane
3. Click the module names from the right-pane and download all the **CEH Tools** files to the **D:\CEH-Tools** folder
4. Right-click the .zip files in the **D:\CEH-Tools** folder and select **Extract Here** option

Note: Please download all the CEHv10 Lab Prerequisites.zip part files (Total 7 Parts) before extracting them in a **D:\CEH-Tools** folder.

[Back to Configuration Task Outline]

CT#2: Install VMware Workstation Pro in Host Machine

1. Download VMware Workstation Pro from https://www.vmware.com/in/products/workstation-pro/workstation-pro-evaluation.html
2. Navigate to downloaded location of the VMware Workstation pro, and double-click downloaded setup file of the VMware Workstation
3. Installation wizard appears, click Next and follow the wizard driven installation steps to install VMware Workstation Pro

   Note: While installing VMware Workstation Pro, Custom Setup wizard appears, check **Enhanced Keyboard Driver** option and click **Next**.

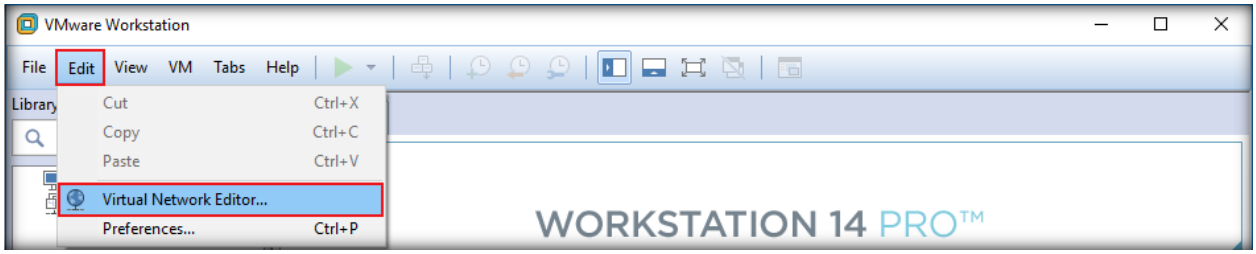
   If you have downloaded the latest version of the VMware Workstation Pro then screenshots will differ.
4. On completion of the installation, the machine will restart
5. Once the machine got rebooted launch the VMware Workstation Pro

   Note: If the VMware Workstation Pro prompts for the Activation key, then provide the activation key if you have purchased one or continue with the trial version of the VMware Workstation Pro

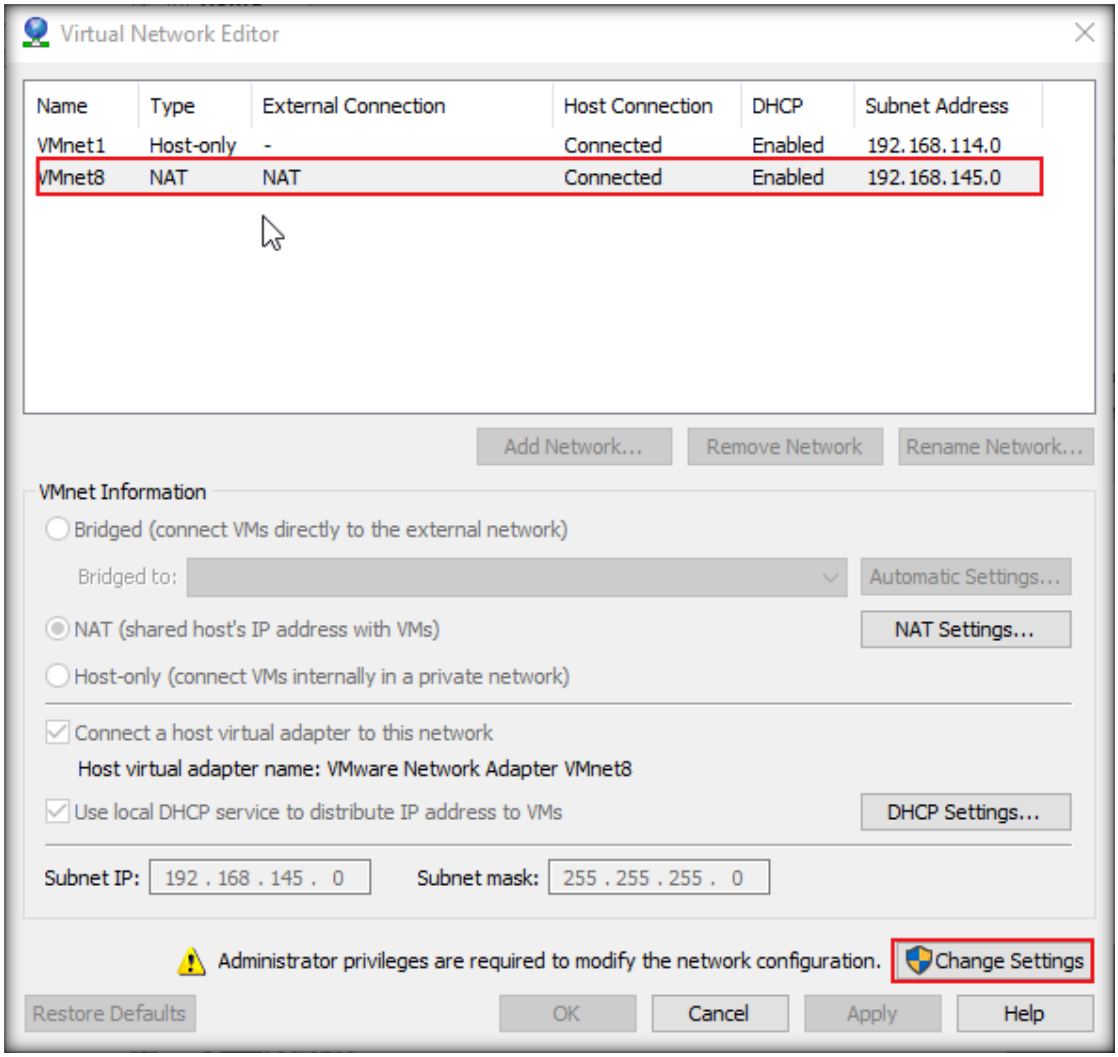
[Back to Configuration Task Outline]

CT#3: Configuring Virtual Network in the VMware Virtual Network Editor

1. Launch **VMware** Workstation
2. Navigate to **Edit** and click **Virtual Network Editor** as shown in the screenshot

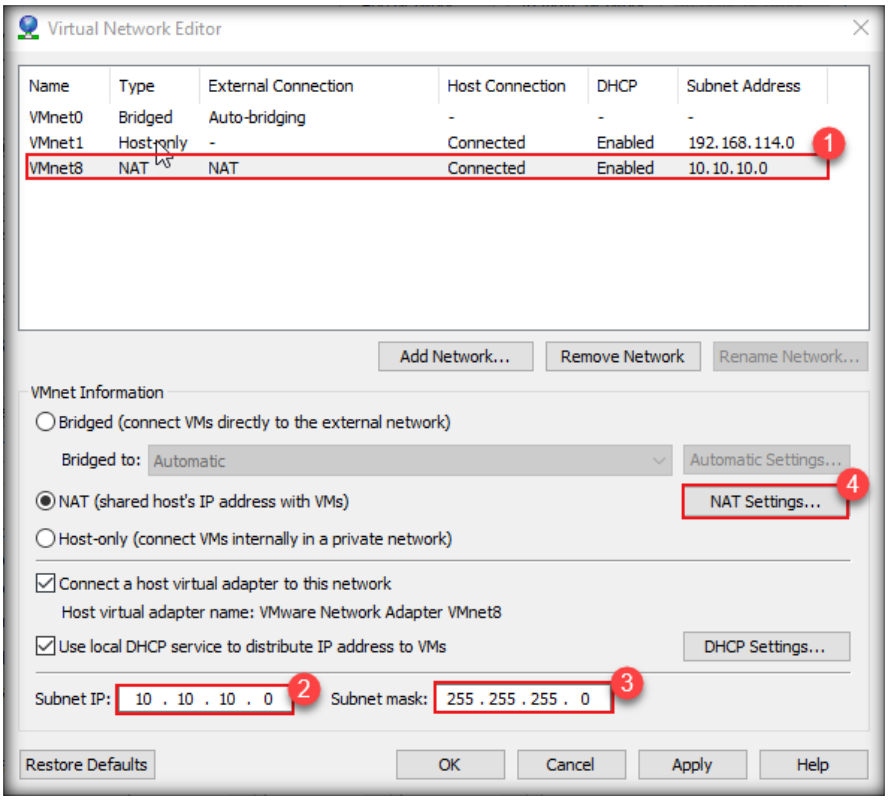


3. Virtual Network Editor window appears, choose **VMnet8 NAT** network, and click **Change Settings**

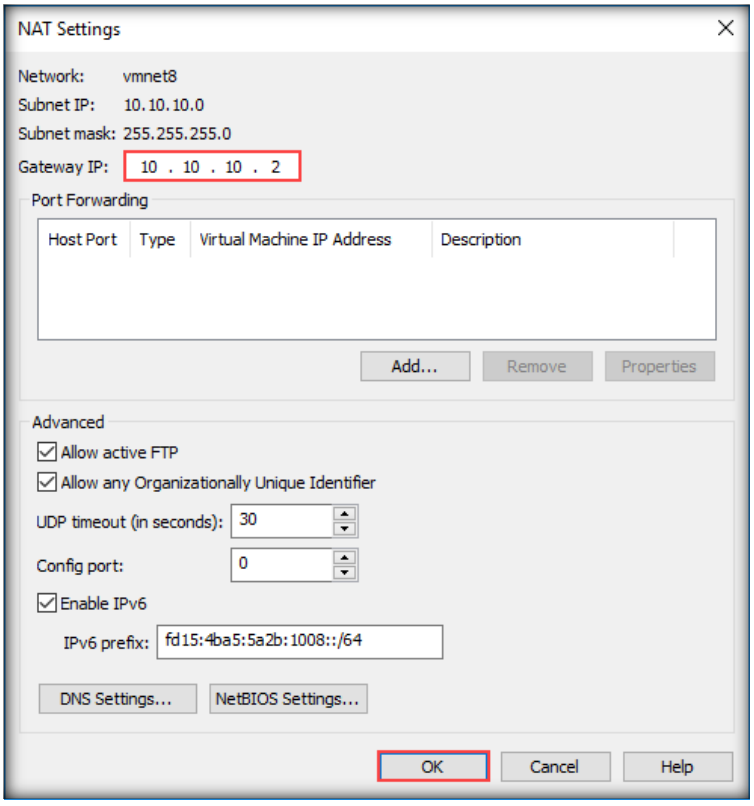


4. If User Access Control pop-up appears, click **Yes**.

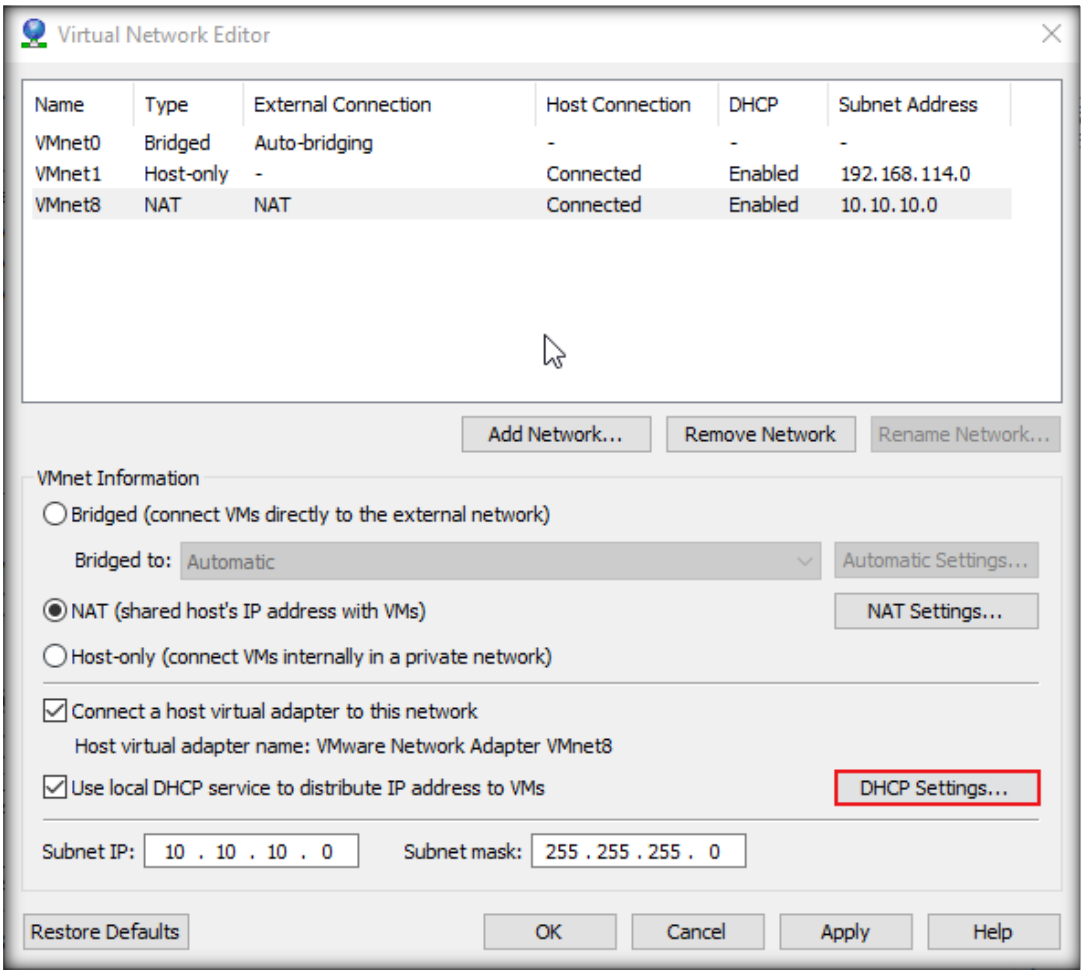
5. Define Subnet IP as **10.10.10.0**, Subnet Mask as **255.255.255.0**, and click **NAT Settings**



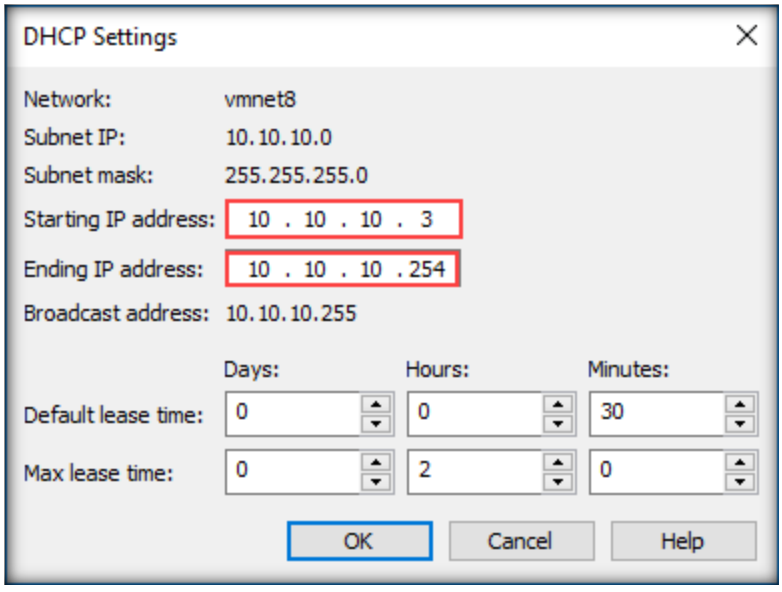
6. NAT Settings window appears, Enter Gateway IP as **10.10.10.2** and click **OK**



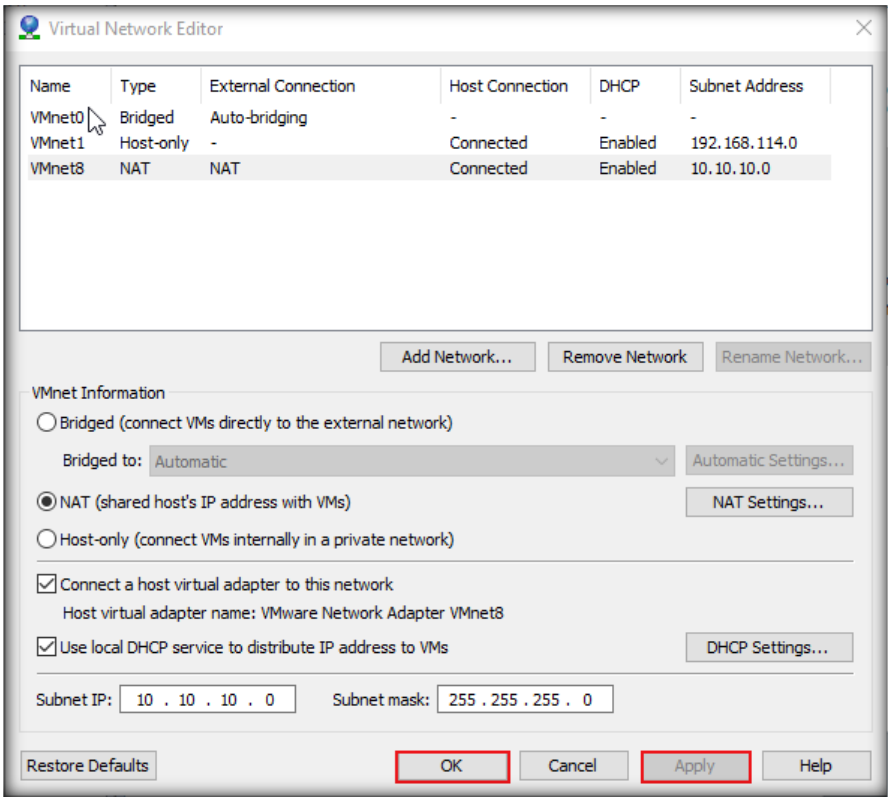
7. Now we keep **VMnet8** selected and click **DHCP Settings**



8. In DHCP Settings window, define Starting IP as **10.10.10.3** and ending IP as **10.10.10.254** and click **OK**



9. Click **Apply** and **OK** on Virtual Network Editor to complete the configuration

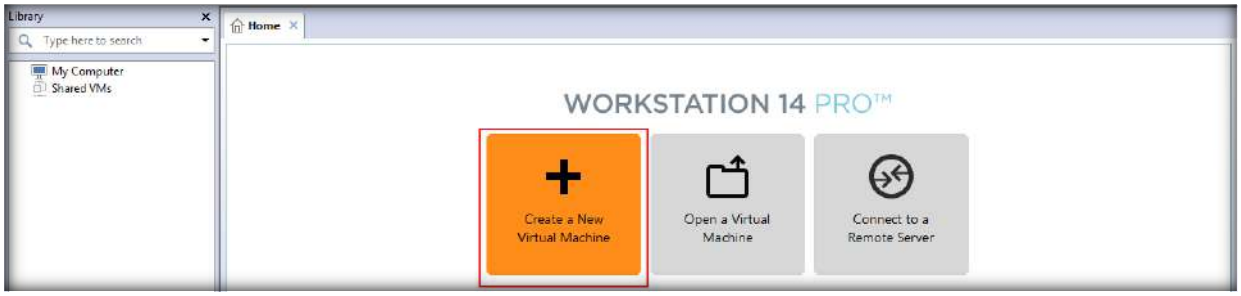


[Back to Configuration Task Outline]

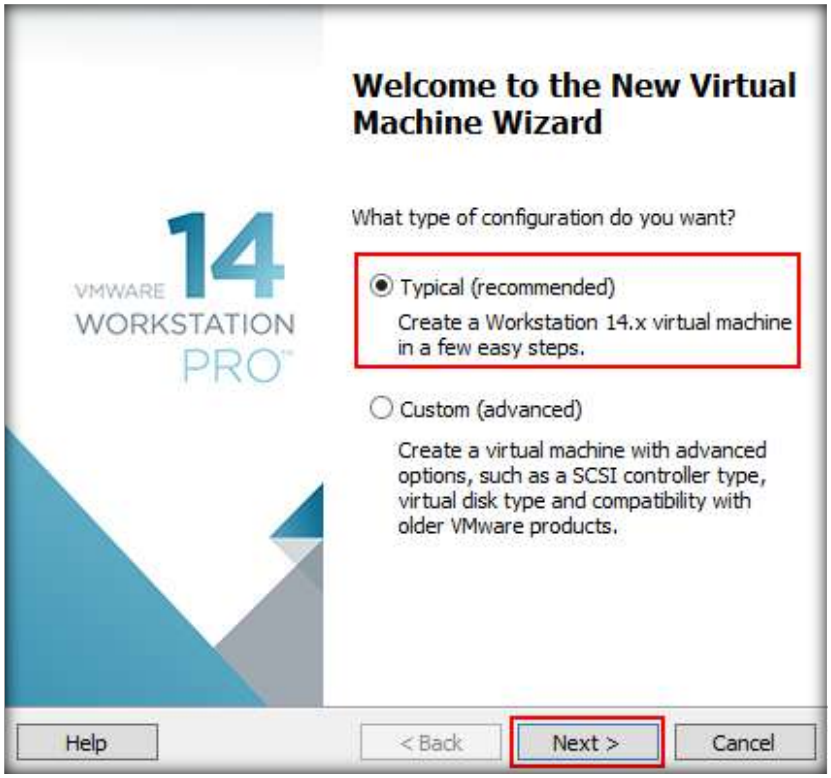
CT#4: Installing Virtual Machines (Windows)

Install Windows Server 2016 Virtual Machine

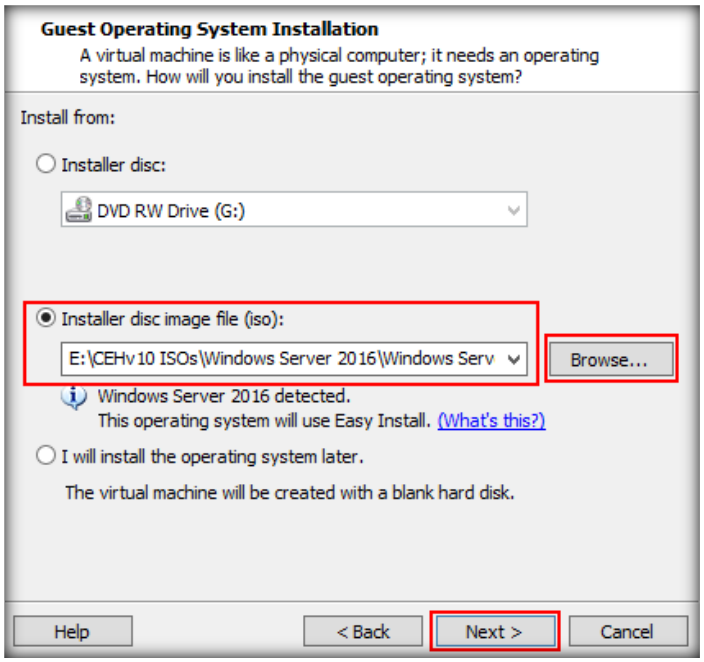
1. In VMware Workstation window, click **Create a New Virtual Machine**



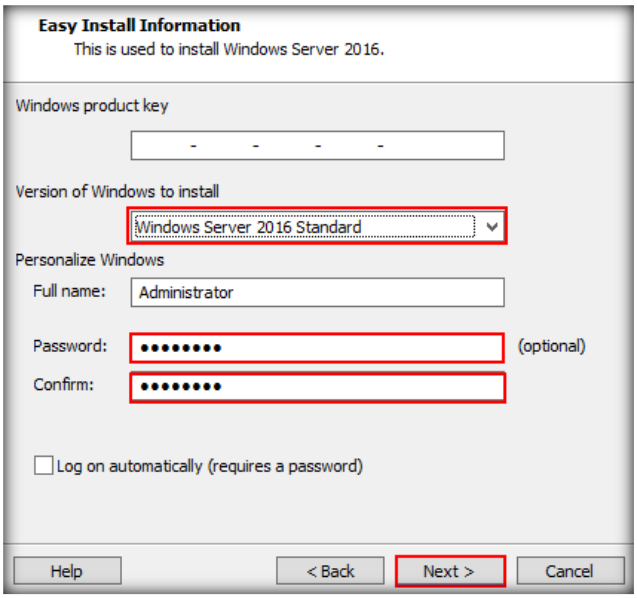
2. In the New Virtual Machine wizard, leave the settings to default and click **Next**



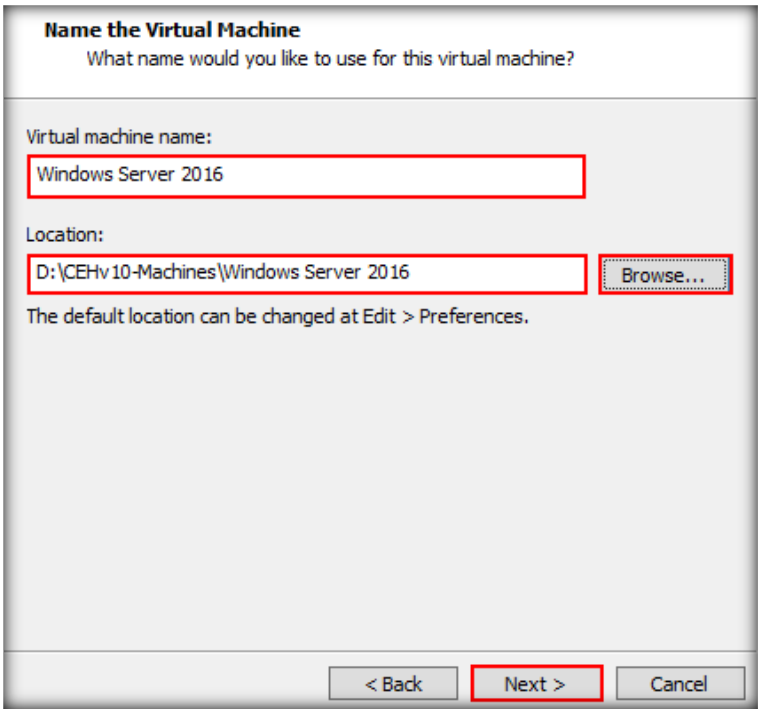
3. In Guest Operating System Installation wizard, choose **Installer disc image file (iso)**: radio button (if you have an ISO of the Windows Server 2016) and then click Browse button to provide the ISO path and click **Next**



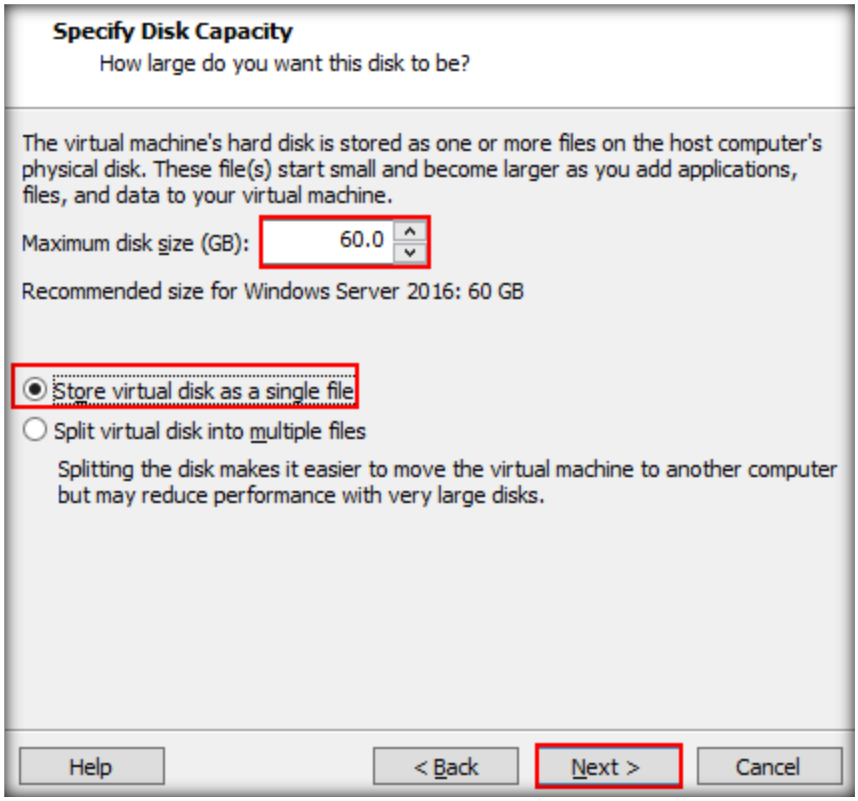
4. Easy Install Information wizard appears. If you have Windows Server 2016 product key then enter the product key or leave it blank
5. Choose **Windows Server 2016 Standard** in the Version of Windows to install section
6. Leave the Username as **Administrator** and type **Pa$$w0rd** in Password and Confirm fields under Personalize Windows section and click **Next**
7. VMware Workstation Warning appears, stating to enter the product key, click **Yes** to continue if you donot have product key



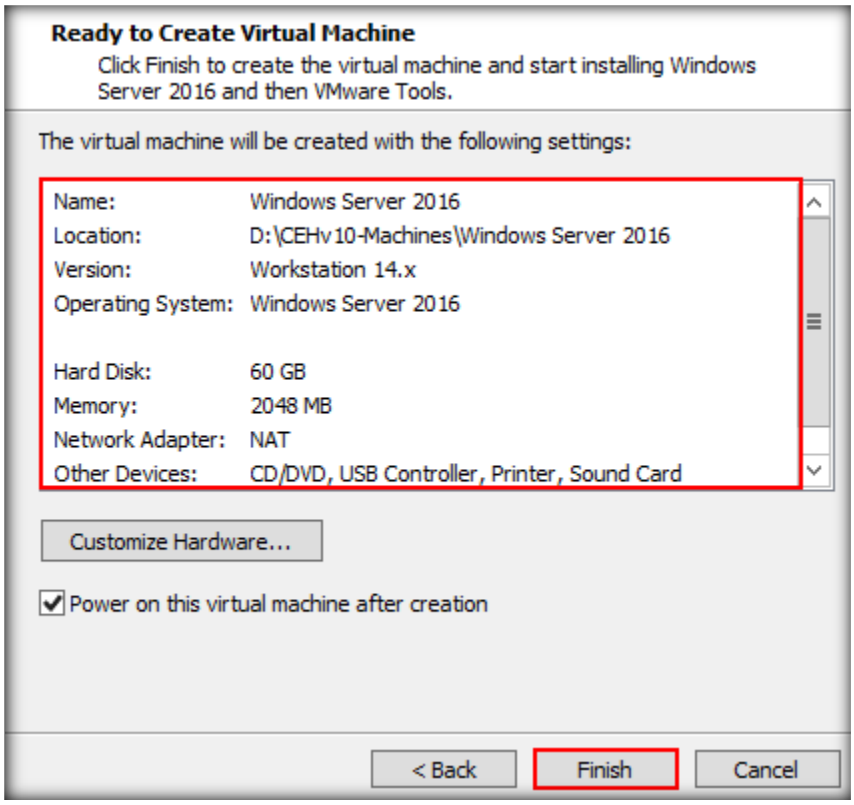
8. Name the Virtual Machine wizard appears, type **Windows Server 2016** in the Virtual machine name field and click **Browse** button to store the virtual hard disk, you can choose the desired location to store the hard disk and then click **Next**



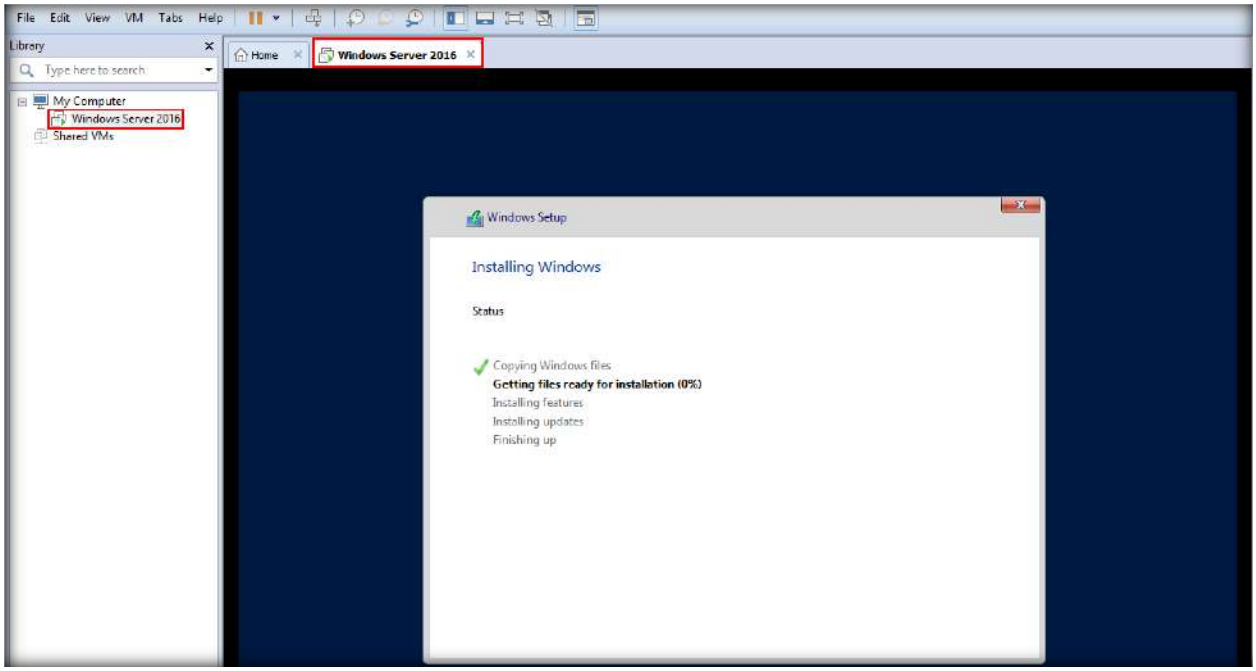
9. Specify Desk Capacity wizard appears, leave the Maximum disk size to default (i.e., **60 GB** recommended) and choose **Store virtual disk as a single file** and click **Next**



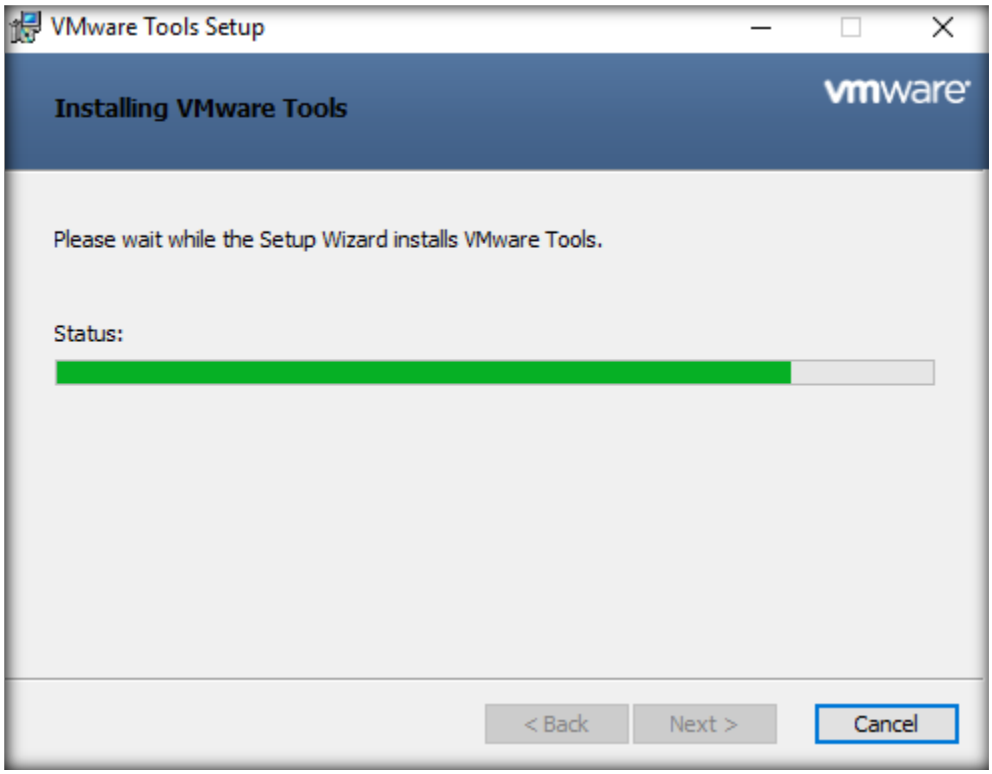
10. Ready to Create Virtual Machine wizard appears, confirm with the settings and click **Finish**



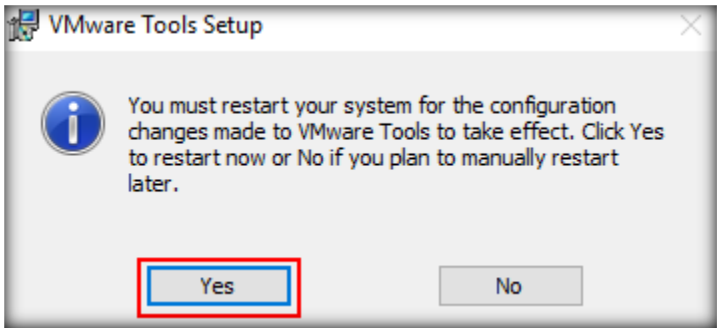
11. As soon as you click **Finish** button, Windows Server 2016 virtual machine pane opens in the VMware Workstation pro and start installing the operating system
12. The machine will restart once the installation is completed



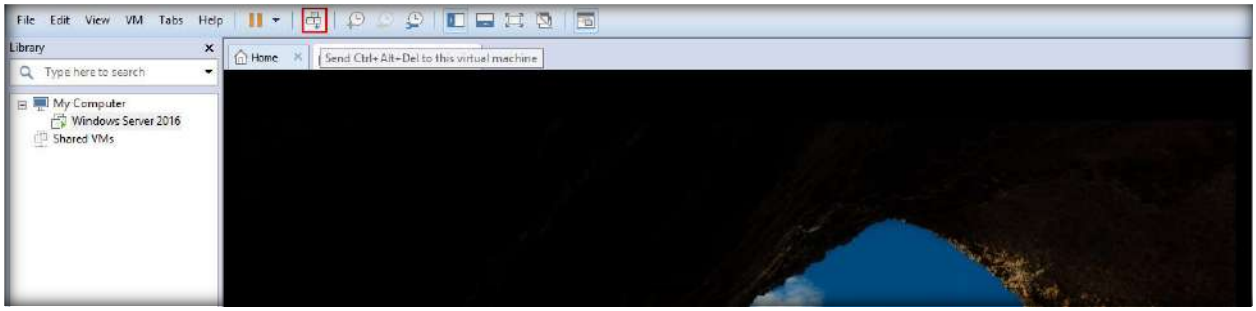
13. The machine will automatically login with the provided credentials. Once the machine is logged in Server Manager window appears, close the Server Manager window
14. VMware Tools Setup wizard will install the required wait until it completes the installation



15. After installation is completed it will prompt you to restart the machine click **Yes** to restart

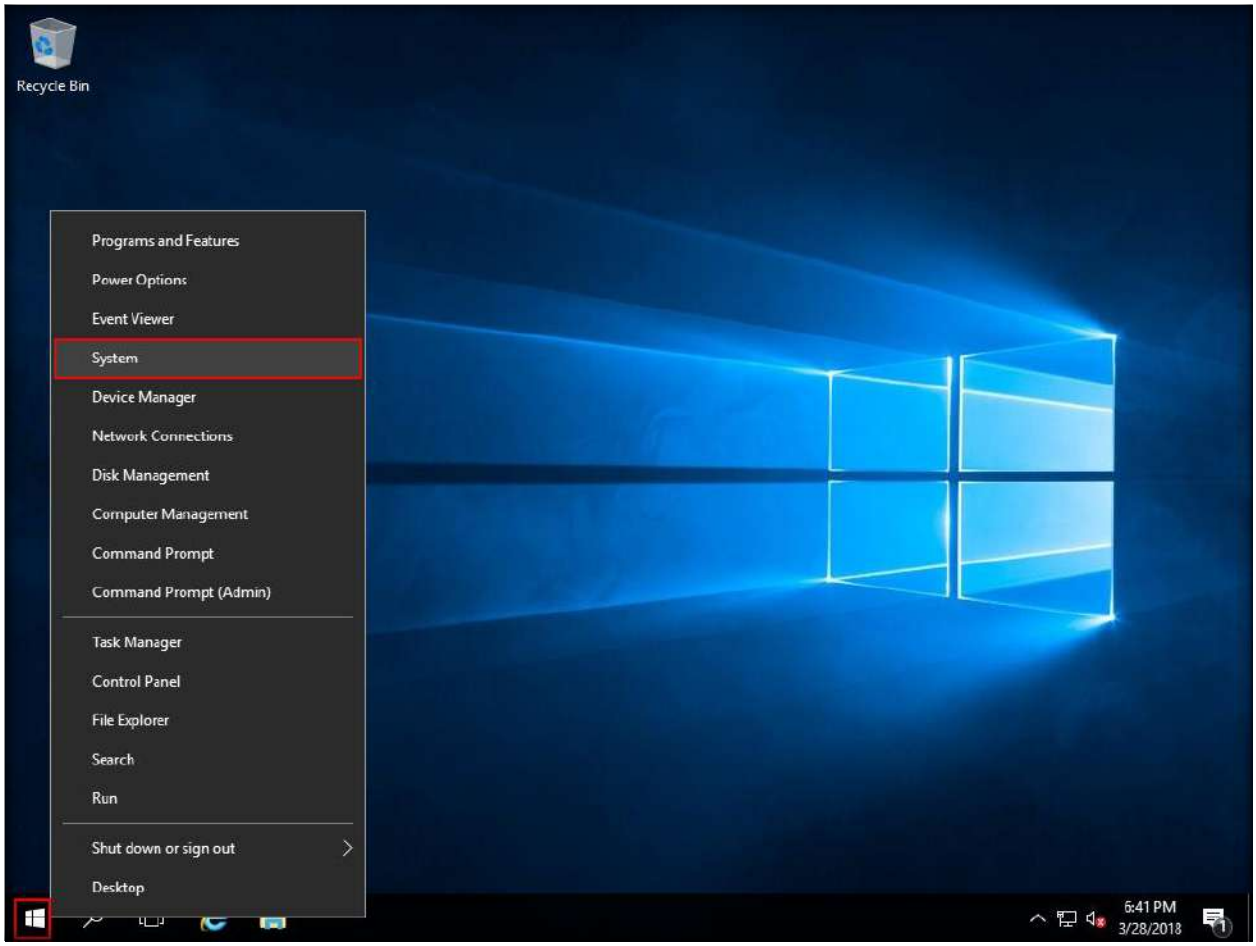


16. Once the installation is finished, the lock screen appears, press the **Send Ctrl+Alt+Delete to this virtual machine** icon from the menu bar



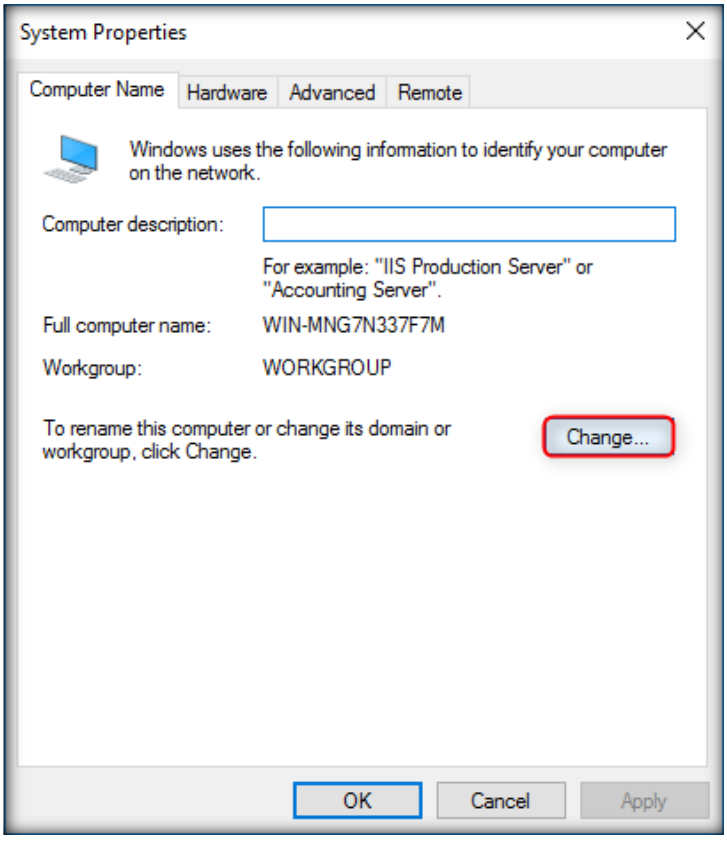
17. **Log In** to the Administrator account by typing **Pa$$w0rd** as the password and press **Enter**

18. Windows Server 2016 desktop appears, close the **Server Manager** window that appears. Right click the **Start** button on the bottom-left and click **System** from the context menu

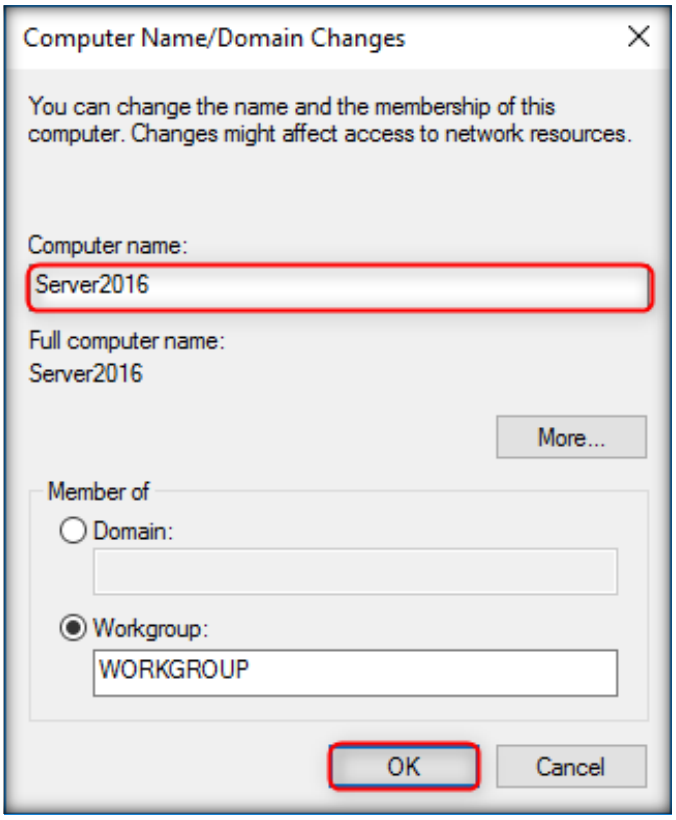


19. System window appears, click **Change settings** as shown in the screenshot:

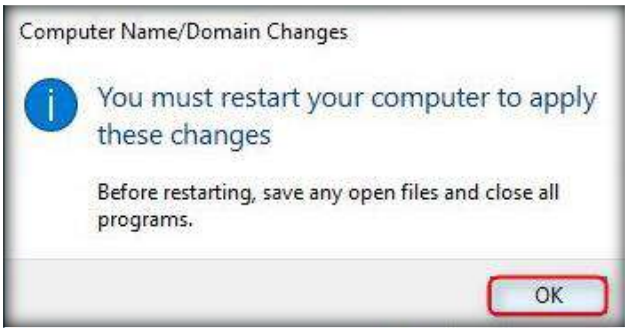
20. System Properties window appears, click **Change...** as shown in the following screenshot:



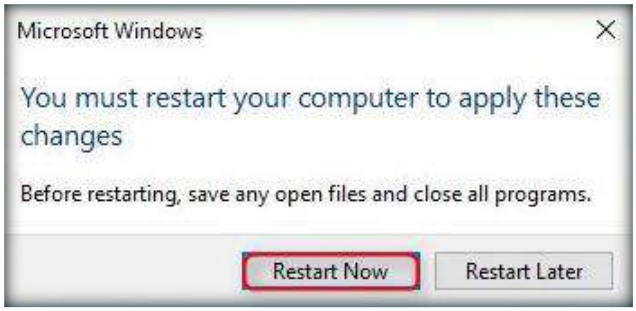
21. Type a computer name (here, **Server2016**) and click **OK** as shown in the following screenshot



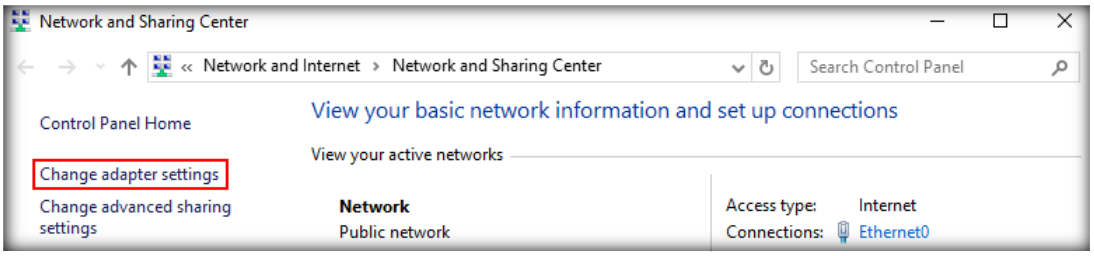
22. You must restart your computer to apply these changes pop-up appears, click **OK**
23. **Close** any open windows



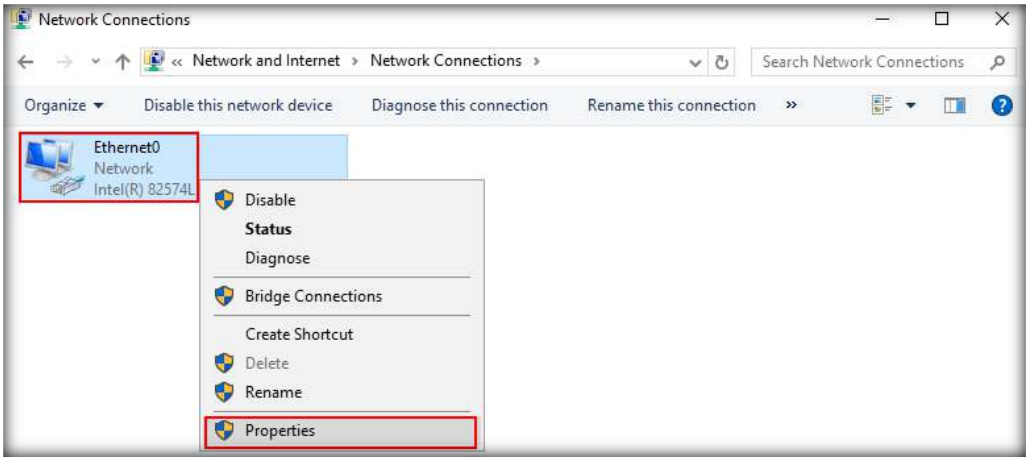
24. Microsoft Windows pop-up appears, click **Restart Now**



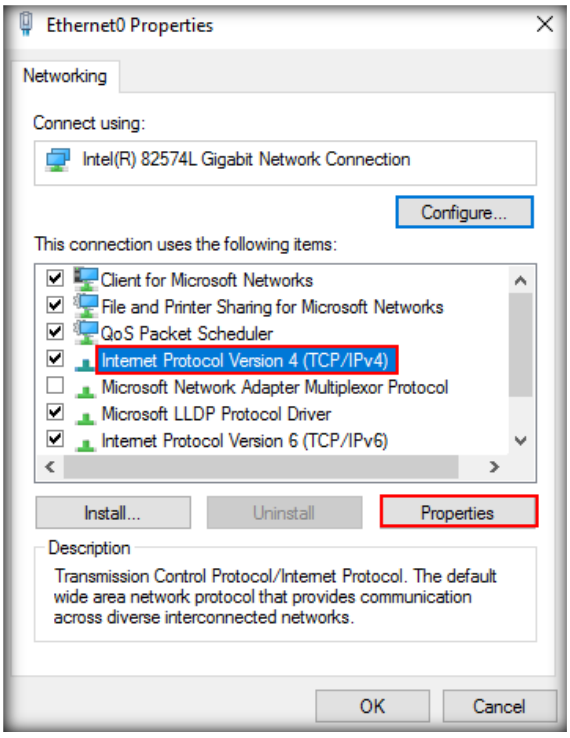
25. After the virtual machine restarts, login to virtual machine and close the Server Manager window. Open **Network and Sharing Center** and click **Change adapter settings** link from the left pane



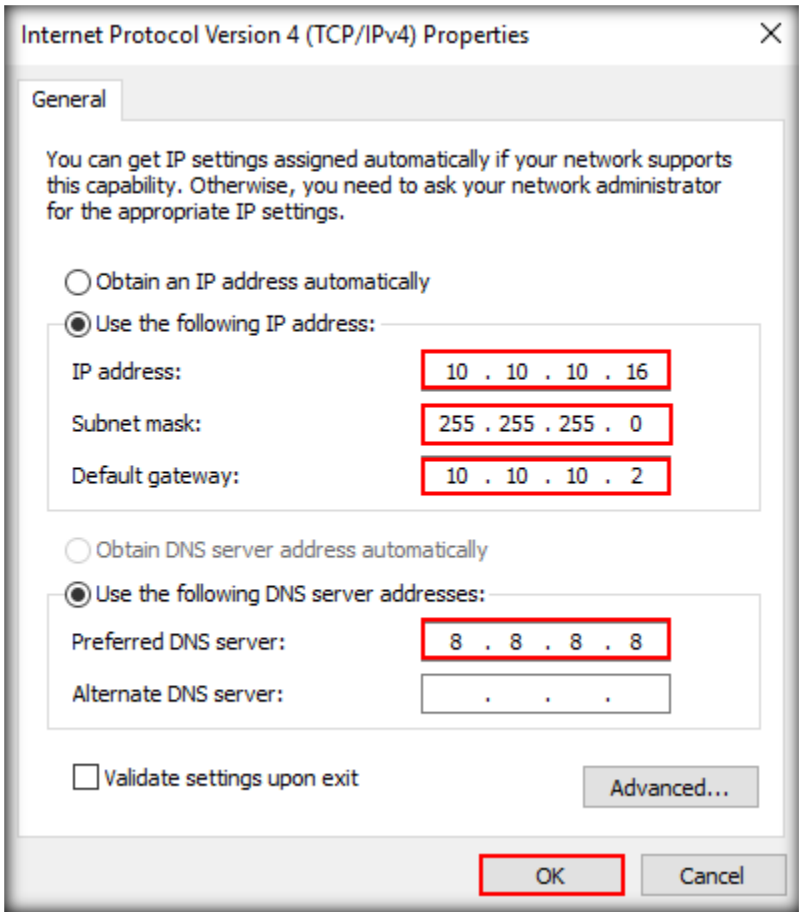
26. Right-click the network interface (here, **Ethernet0**) and click **Properties**



27. **Ethernet0 Properties** window appears; scroll down the list, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**



28. Select **Use the following IP address** radio button, assign **10.10.10.16** as **IP address**, **255.255.255.0** as **Subnet mask** and **10.10.10.2** as **Default gateway**
29. Assign **8.8.8.8** as the **Preferred DNS server** address and click **OK**



30. **Close** the **Ethernet0 Properties** window
31. Similarly, Create and Install **Windows Server 2012 R2 (64-bit)**, **Windows 10**, and **Windows 8**, Virtual Machines with default hard disk space and 2048MB of RAM memory, with the following credentials as mentioned below:
    - Windows Server 2012 (10.10.10.12, 255.255.255.0, 10.10.10.2 and 8.8.8.8)

      Username: Administrator

      Password: Pa$$w0rd
    - Windows 10 (10.10.10.10, 255.255.255.0, 10.10.10.2 and 8.8.8.8)

      Username: Admin

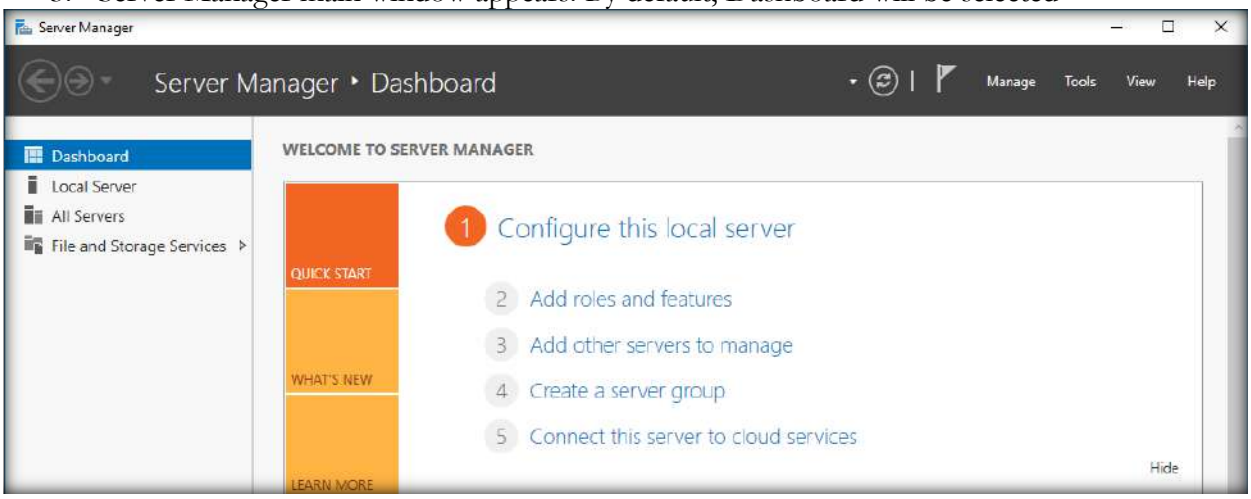
      Password: Pa$$w0rd
    - Windows 8 (10.10.10.8, 255.255.255.0, 10.10.10.2 and 8.8.8.8)

      Username: Admin

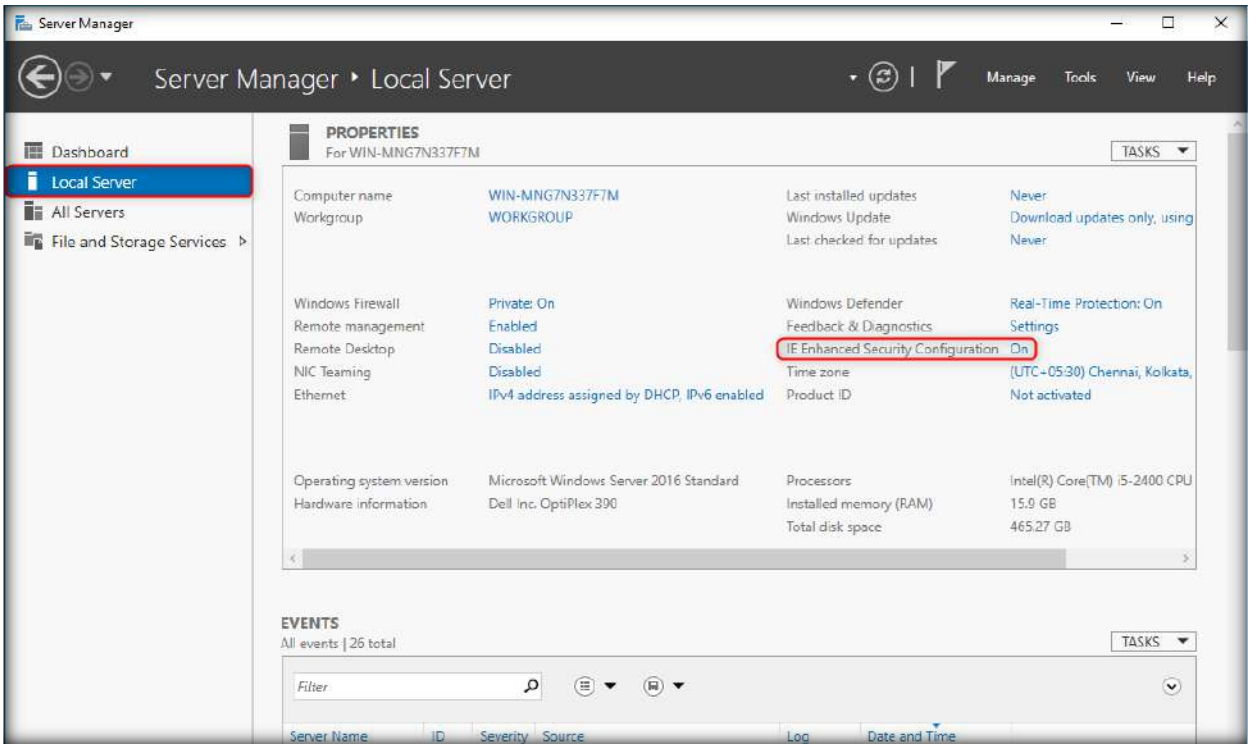
      Password: Pa$$w0rd

CT#5: Configure Internet Explorer (IE) Enhanced Security Configuration in Windows Server 2016

1. Start and log in to the Windows Server 2016 virtual machine
2. To configure Internet Explorer Enhanced Security Configuration, go to Start menu→ Server Manager App
3. Server Manager main window appears. By default, Dashboard will be selected



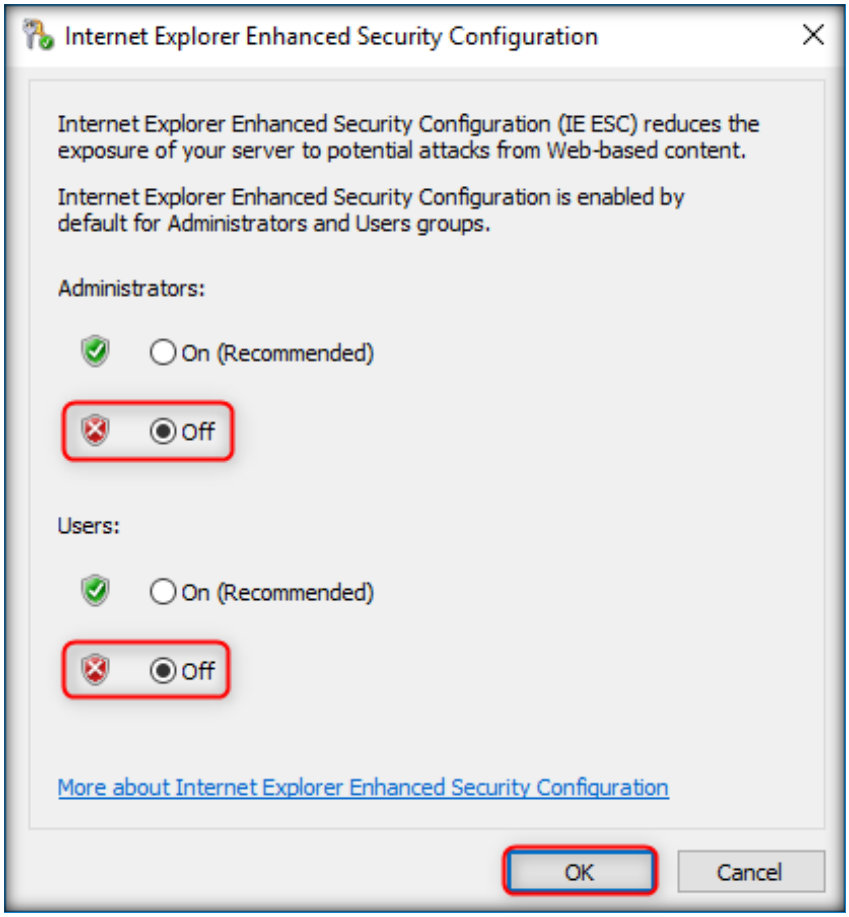
4. Select Local Server in the left pane of the window. In the right pane, click On for IE Enhanced Security Configuration



5. **Internet Explorer Enhanced Security Configuration** window appears

6. Select **Off** radio button for both **Administrators** and **Users** sections and click **OK**

   Note: Configure IE Explorer Enhanced Security Configuration in Windows Server 2012 also.

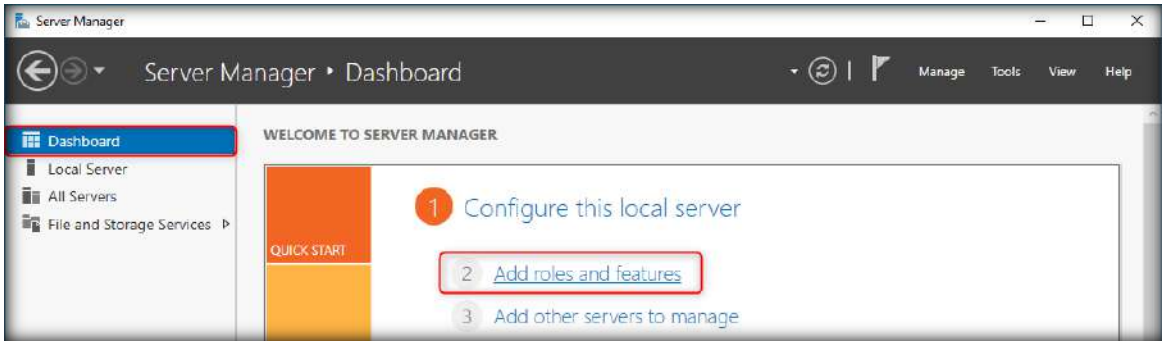


[Back to Configuration Task Outline]

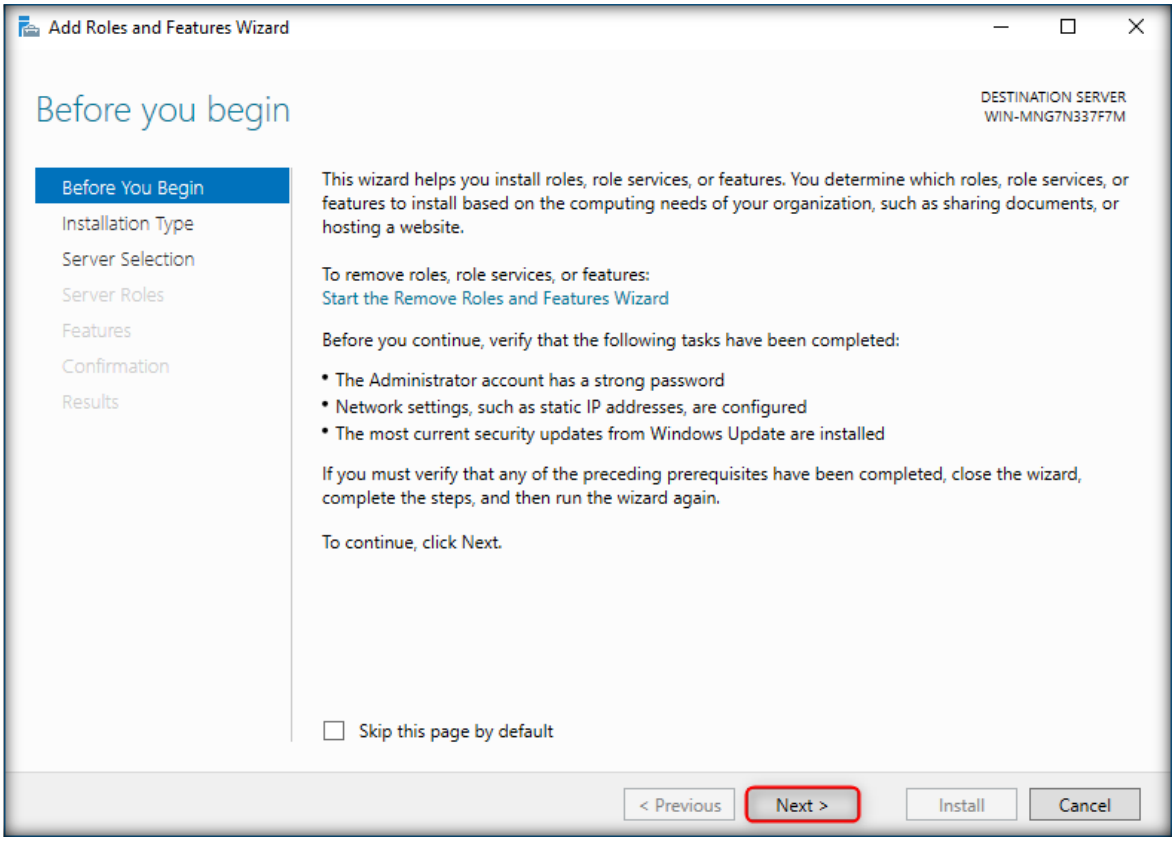
CT#6: Adding Roles IIS (Internet Information Services), File Services, SNMP and Remote Access roles in Windows Server 2016 (Virtual Machine)

Adding IIS (Internet Information Services) roles in Server Manager

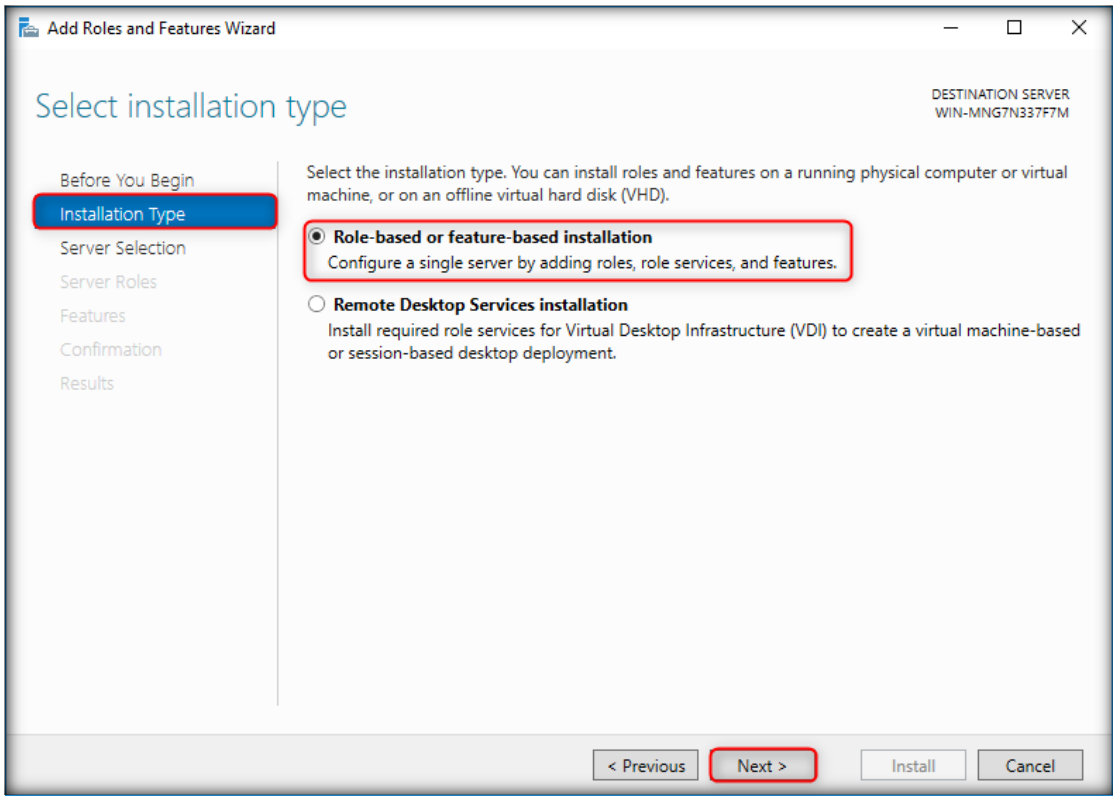
1. Add **Internet Information Services (IIS)** roles in Server Manager
2. To open Server Manager, click **Start → Server Manager App**
3. In Server Manager **Dashboard**, click **Add Roles and Features**



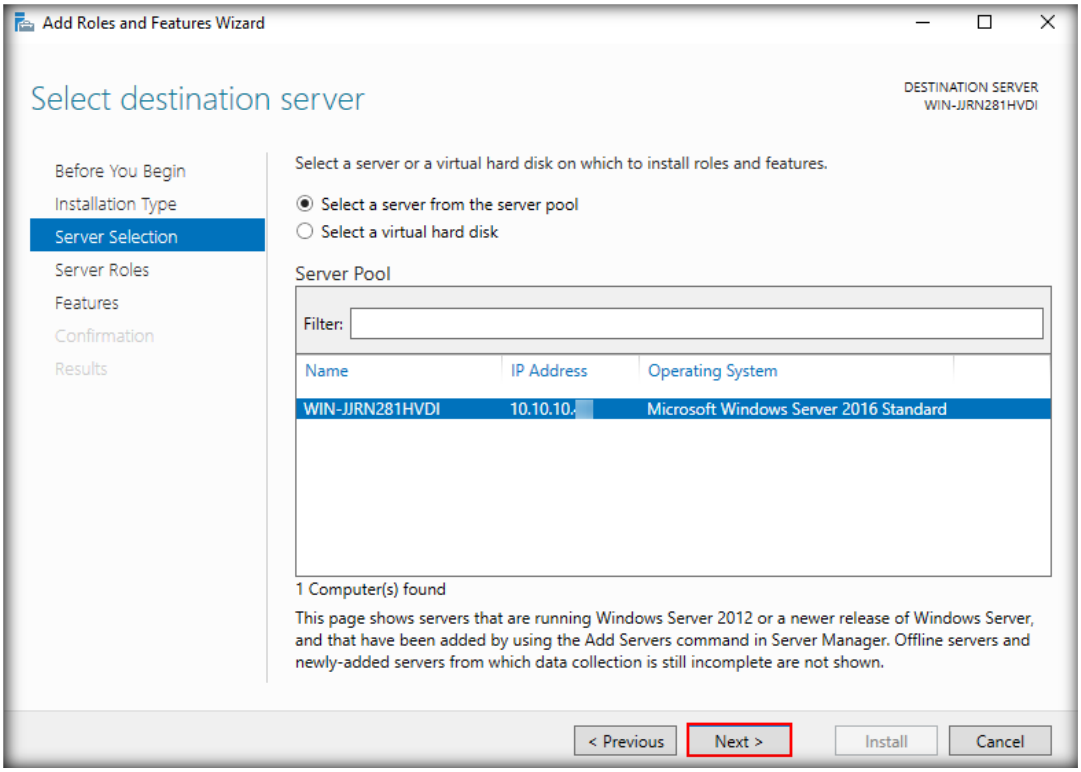
4. **Add Roles and Features Wizard** appears, click **Next**



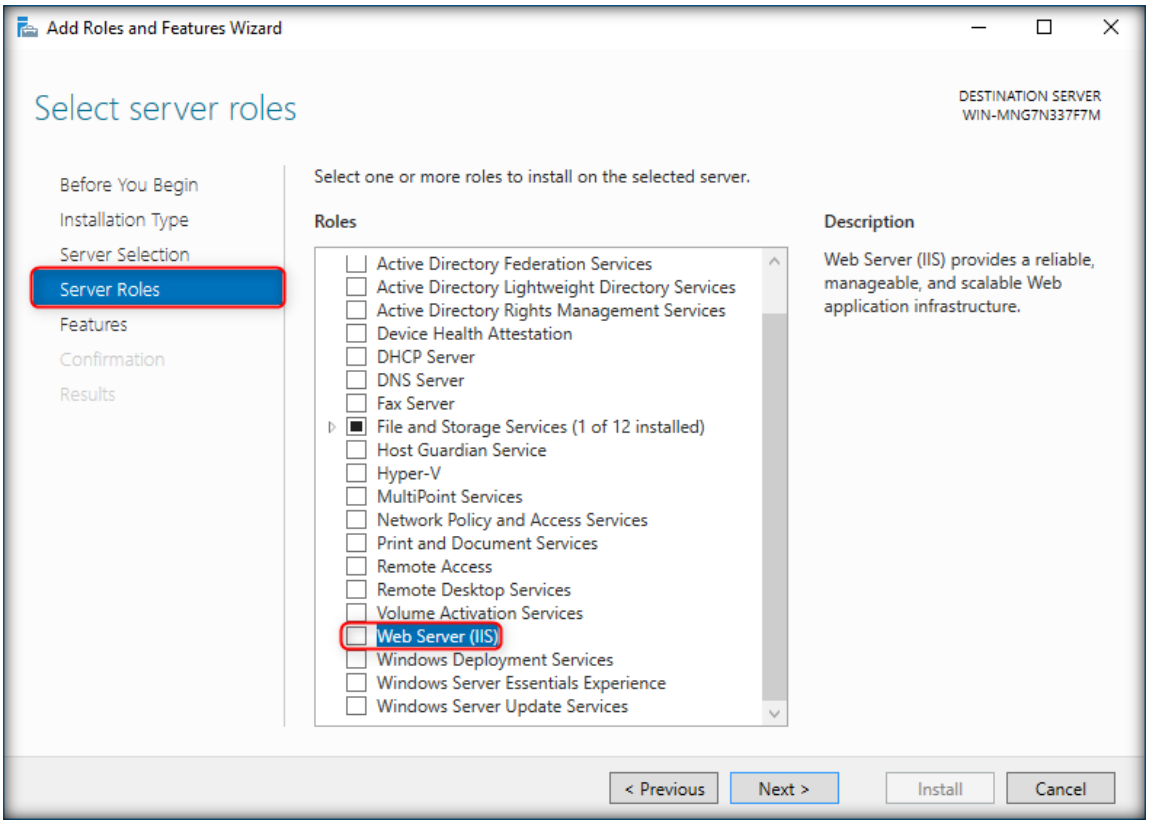
5. In **Installation Type** section of the wizard, select **Role-based or feature-based installation** radio button and click **Next**



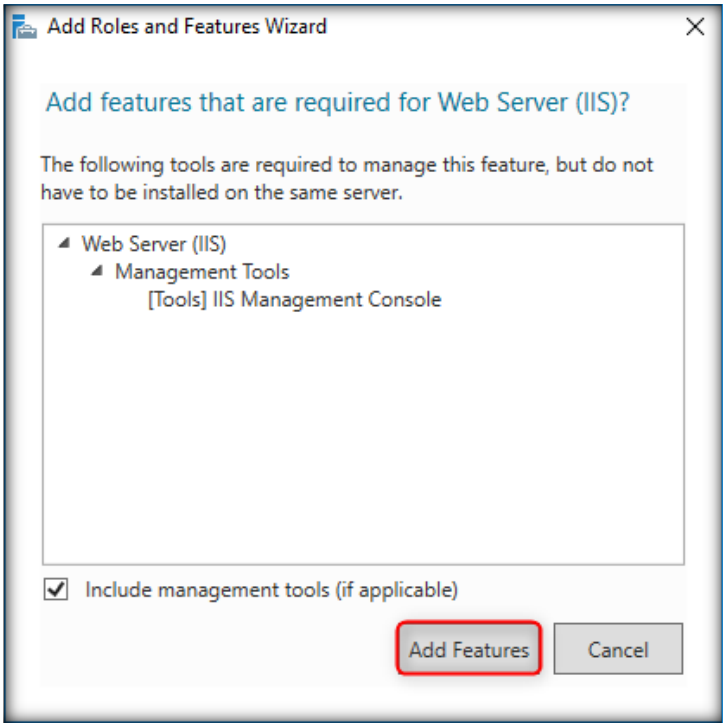
6. In **Server Selection** section, leave the selections to default and click **Next**



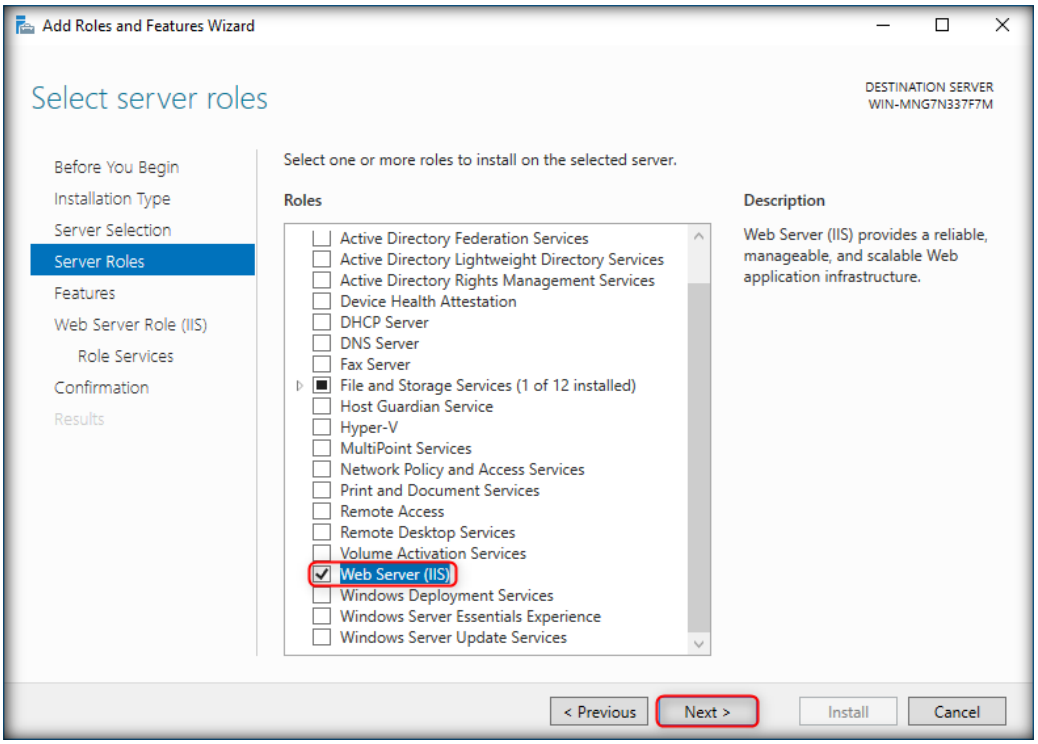
7. **Server Roles** section appears, click the check box of **Web Server (IIS)** role



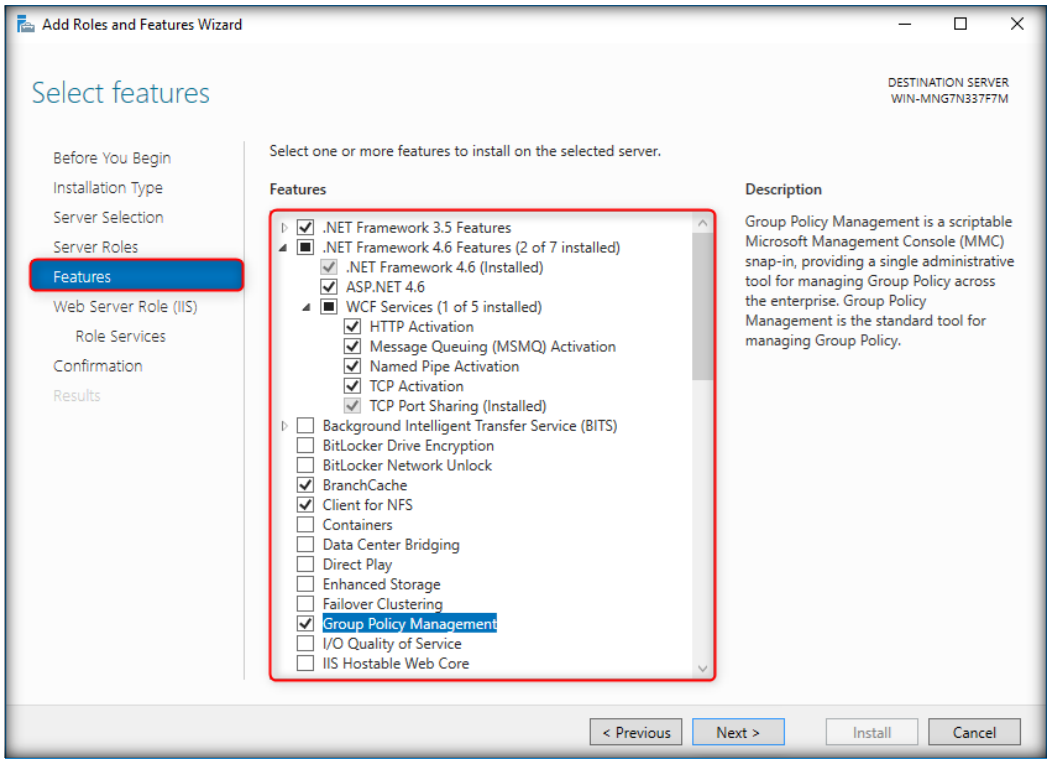
8. **Add Roles and Features wizard** window appears, click **Add Features**



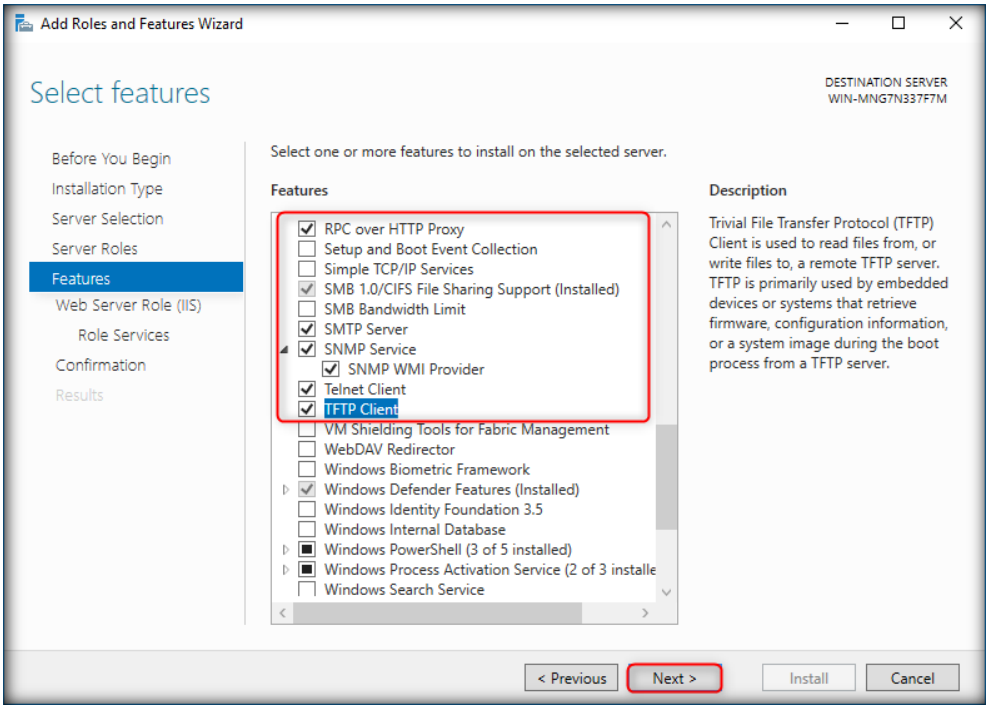
9. In the **Server Roles** section, you will observe the Web Server (IIS) option is checked. Click **Next**



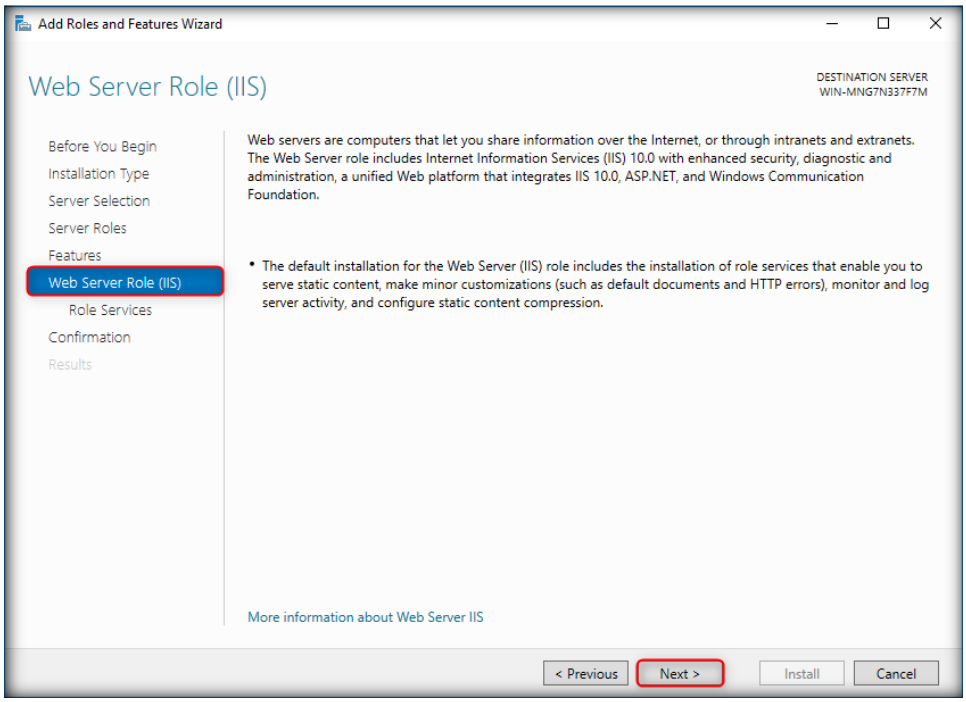
10. **Features** section appears, select the checkboxes for **.NET Framework 3.5**, **Branch Cache**, **Client for NFS** and **Group Policy Management** Features, as well as all the checkboxes under **.NET Framework 4.6** Features



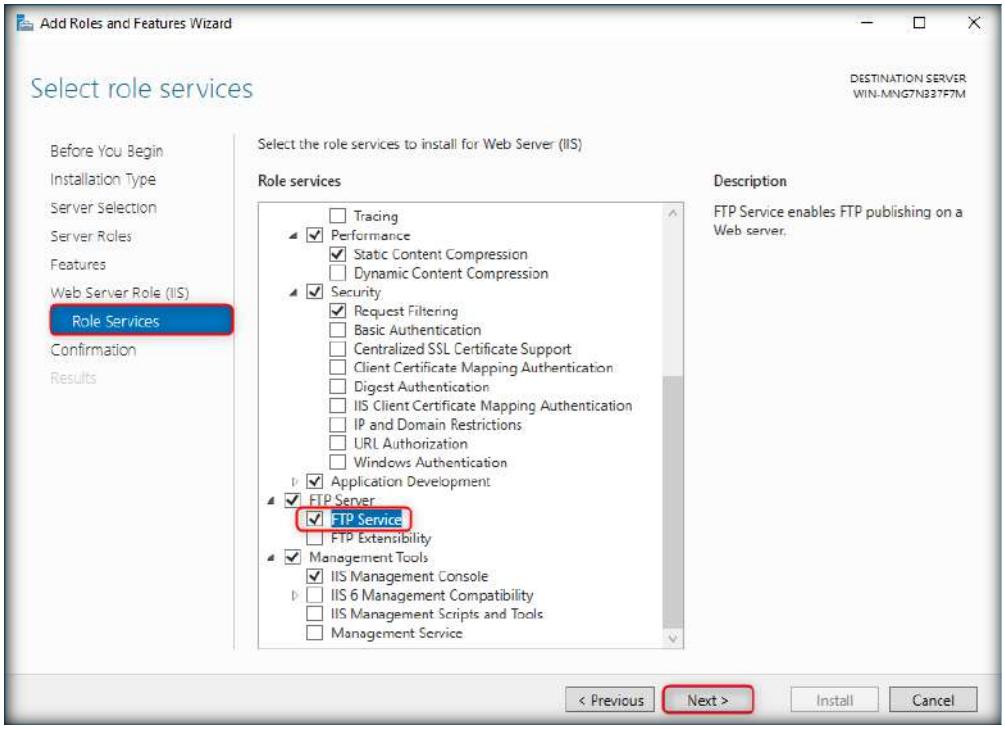
11. Scroll down the section and check **RPC over HTTP Proxy**, **SMTP Server**, **SNMP WMI Provider** under **SNMP Service** feature, **Telnet Client** and **TFTP Client** roles. Click **Add Features** button if you get a prompt for the features to be added while selecting few of the features.
12. Click **Next**



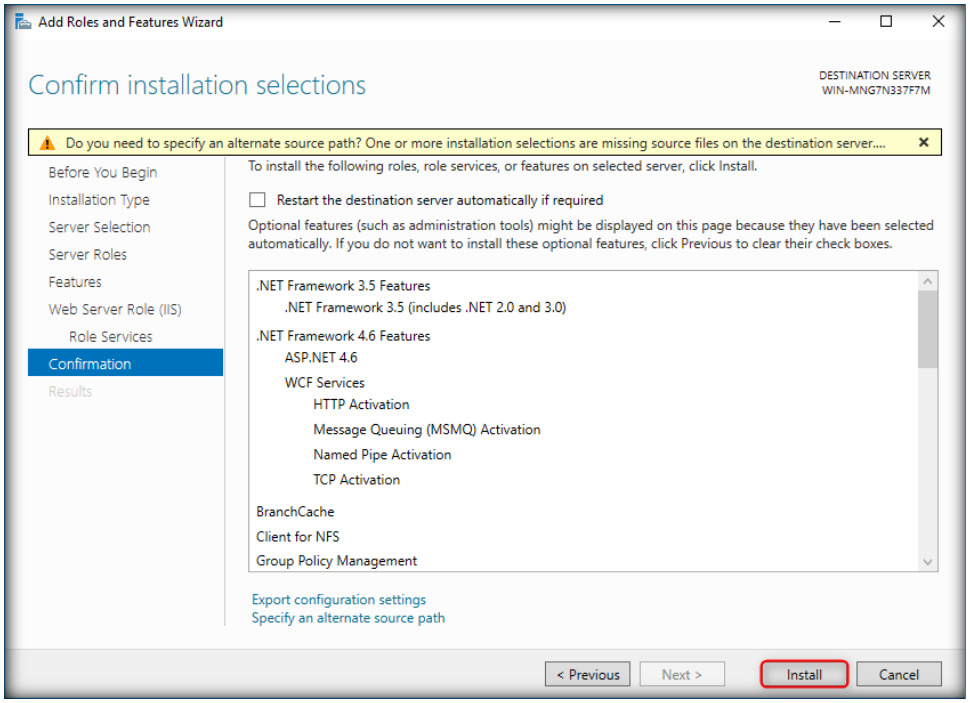
13. Click **Add Features** button if you get a prompt for the features to be added, while selecting any features. Click **Next**.
14. **Web Server Role (IIS)** section appears in the wizard, click **Next**.



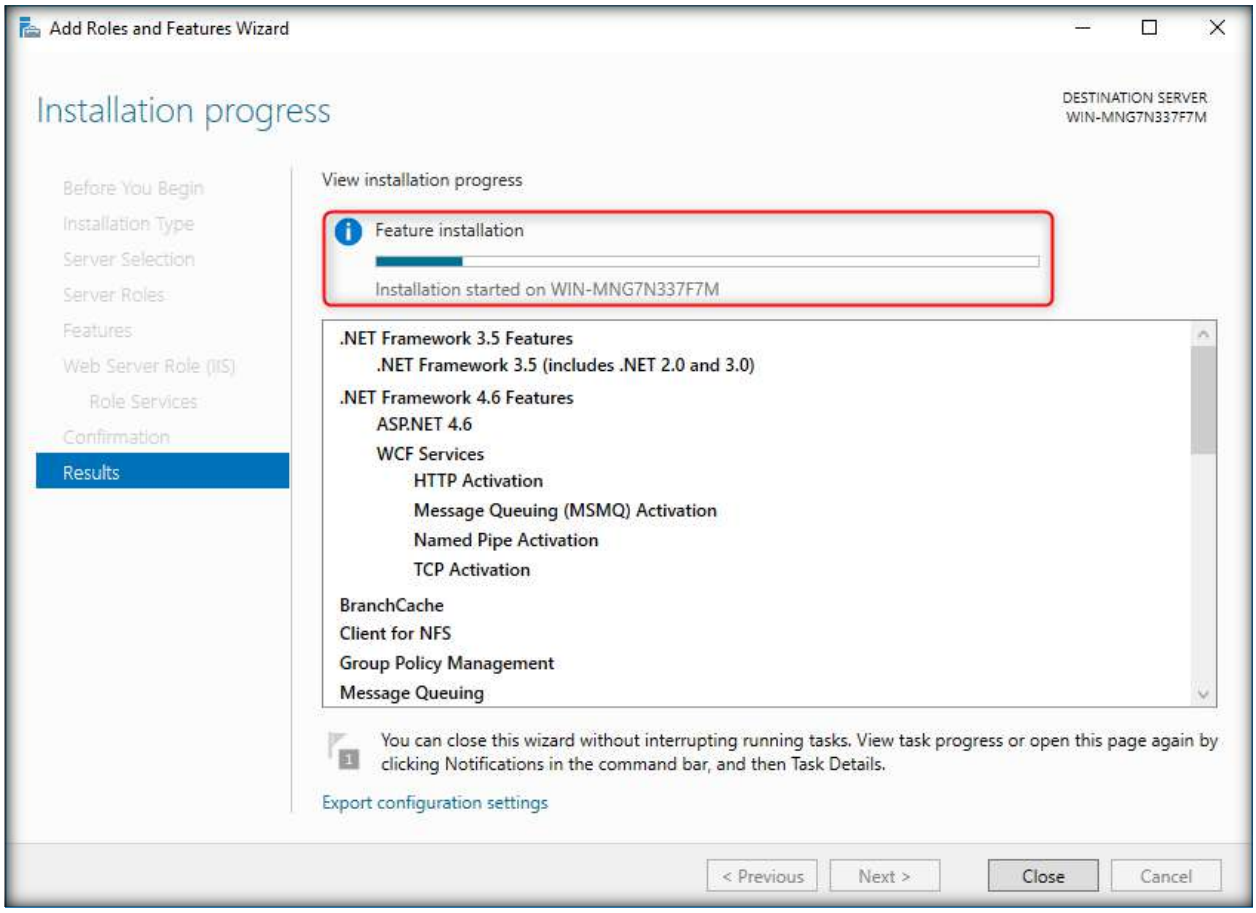
15. **Role Services** section appears in the wizard. Scroll down the Role services and check **FTP Service** under **FTP Server** role.
16. Click **Next**



17. **Confirmation** section appears in the wizard, click **Install** (Ignore the warning under the Custom installation selections wizard).



18. In Add Roles and Features Wizard, **View Installation progress** will show the installation progress of the features. It will take a while to **complete** the installation of selected roles

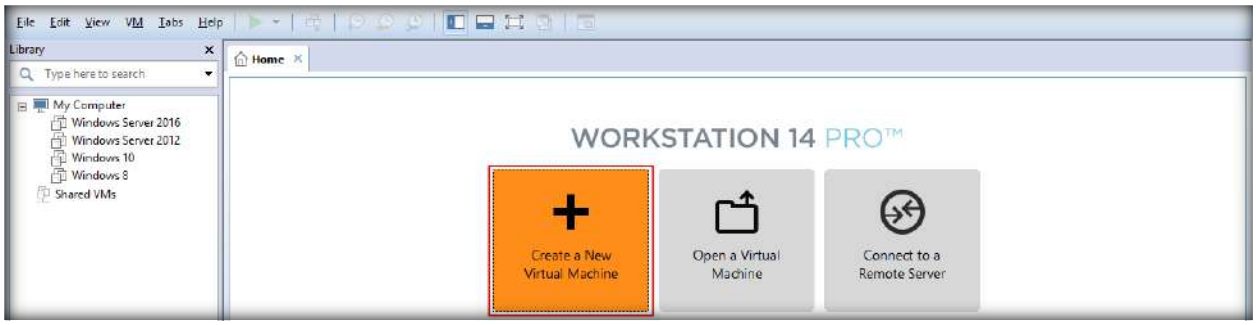


19. After the completion of installation, click **Close** button and restart the machine
20. Similarly install all the above roles and services in the Windows Server 2012 machine
21. After installing all the services Windows Server 2012. Stop the **World Wide Web Publishing Service** and **IIS Admin service**. To do this navigate to **Start → Administrative Tools**. Administrative Tools window appears, double-click **Services**. Service window appears, scroll down to **World Wide Web Publishing Service** and right-click and click **Properties** from the context menu
22. **World Wide Web Publishing Service** properties window appears, choose Startup type as **Disabled** and click **Stop** button under Service Status section and then click **Apply** and **OK**
23. Similarly Stop the **IIS Admin Service** also

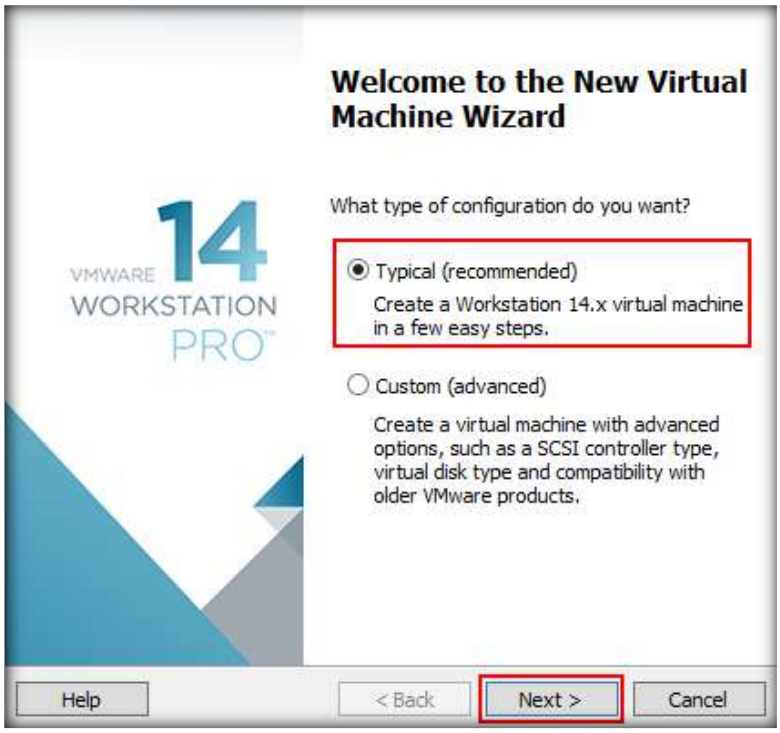
[Back to Configuration Task Outline]

CT#7: Install Kali Linux in VMware

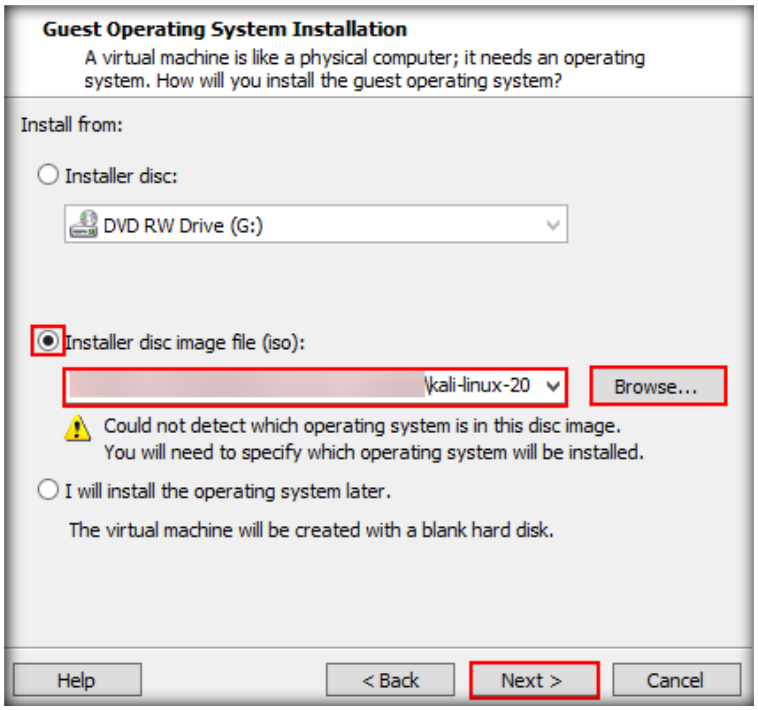
1. In VMware Workstation window, click **Create a New Virtual Machine**



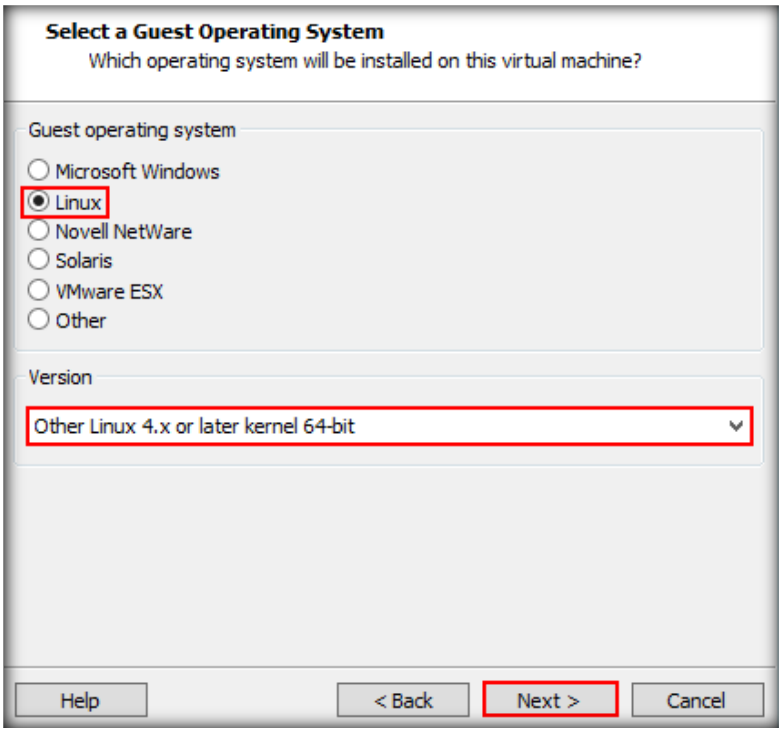
2. In the New Virtual Machine wizard, leave the settings to default and click **Next**



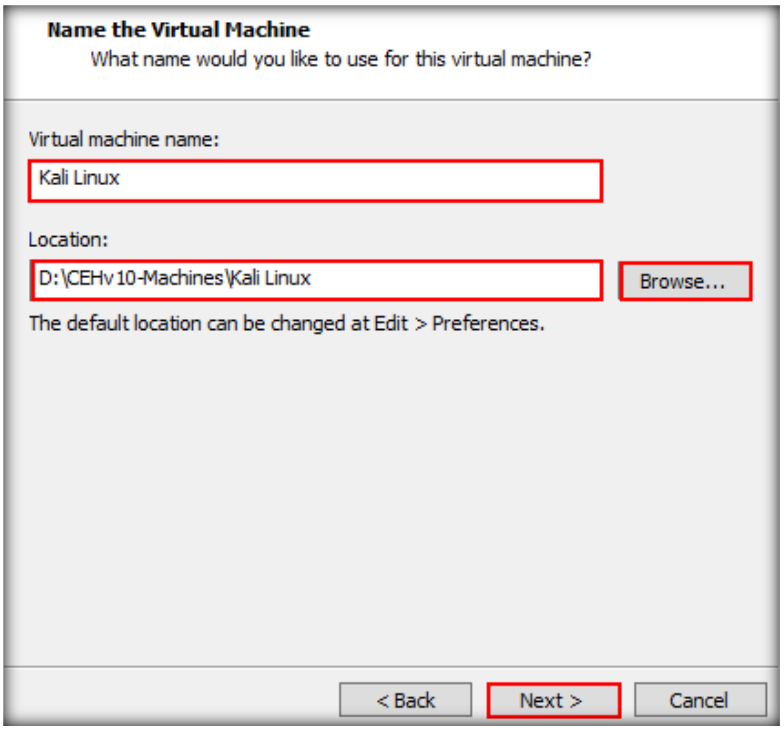
3. In Guest Operating System Installation wizard, choose **Installer disc image file (iso)**: radio button. Click **Browse** and navigate to D:\CEH-Tools\CEHv10 Lab Prerequisites\ISO's\Kali Linux and select **kali-linux-2017.3-amd64.iso** to provide the ISO path and click **Next**



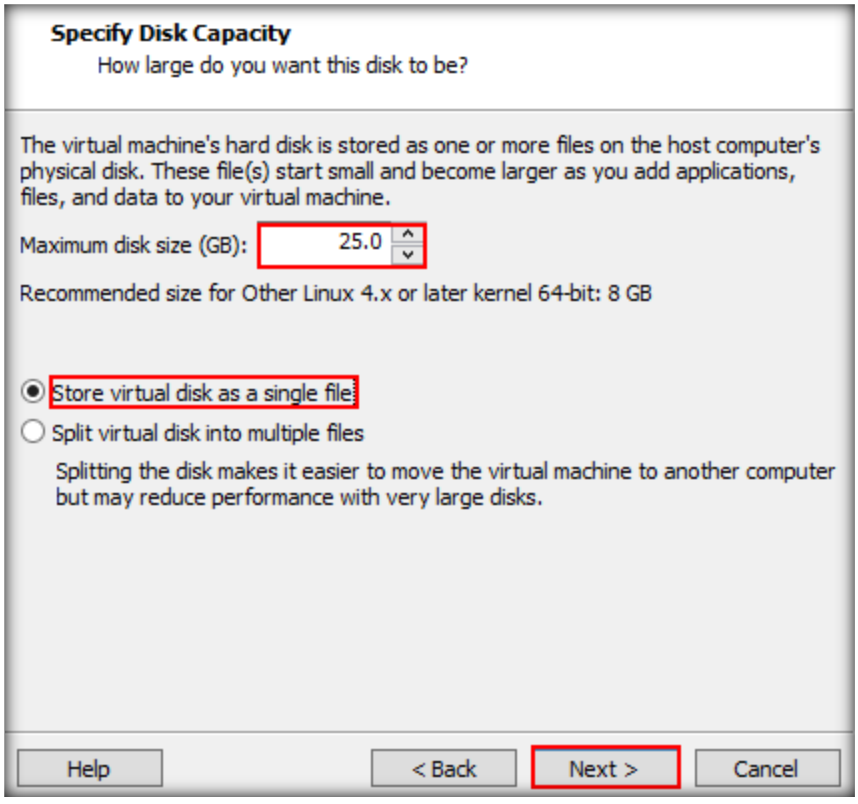
4. Select a Guest Operating System wizard appears, choose **Linux** radio button under Guest operating system type and select **Other Linux 4.x or later kernel 64-bit** in the Version drop down and click **Next** as shown in the screenshot



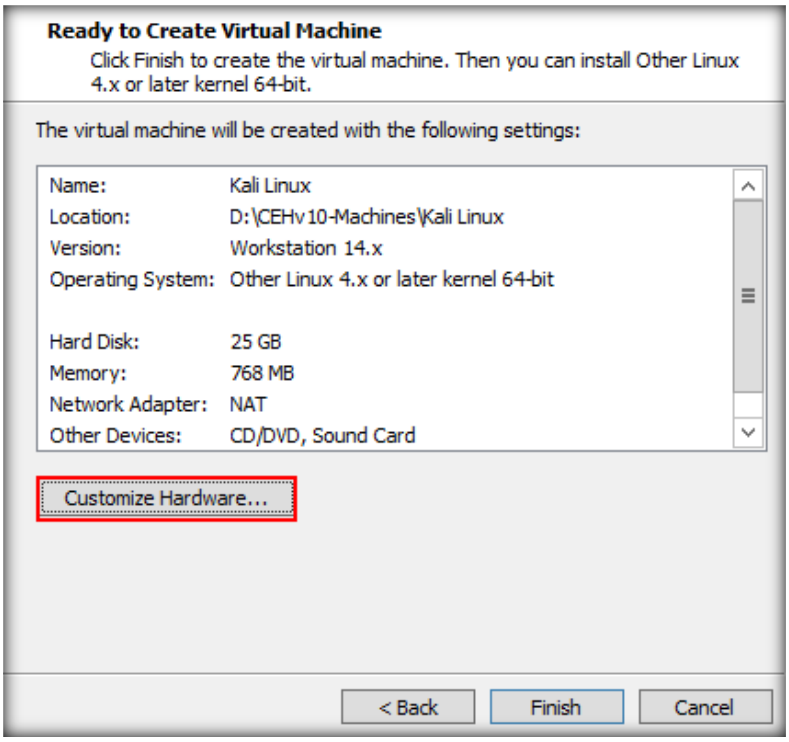
5. Name the Virtual Machine wizard appears, type **Kali Linux** in the Virtual machine name field, and click **Browse** button to store the virtual hard disk and click **Next**



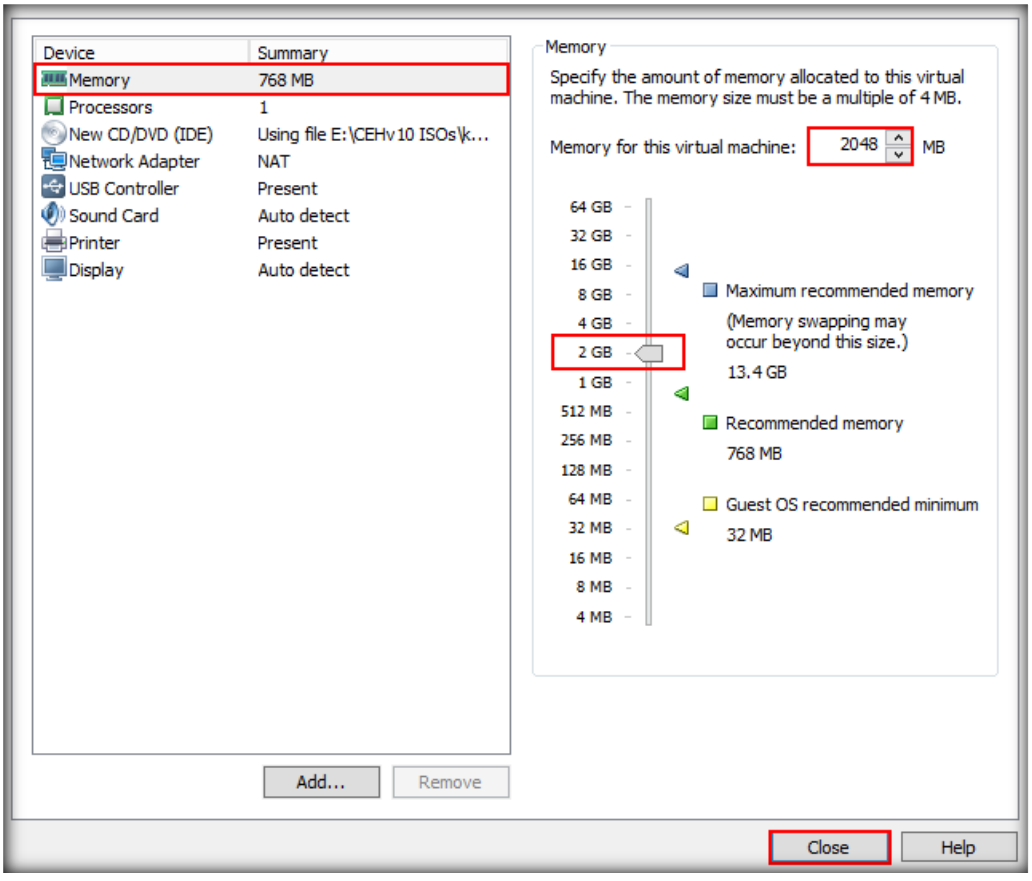
6. Specify Disk Capacity wizard appears, type **25.0 GB** in the Maximum disk size, and choose **Store virtual disk as a single disk** radio button and click **Next**



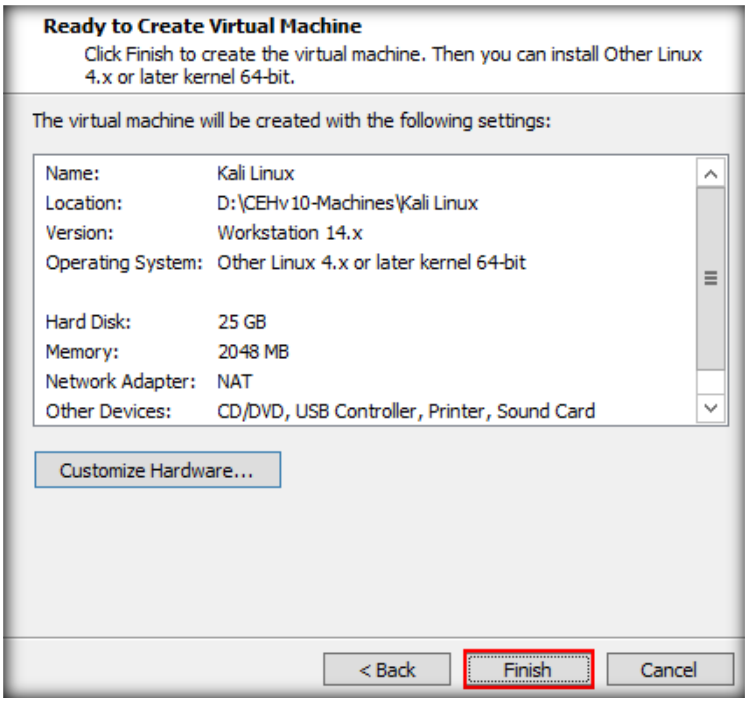
7. Click **Customize Hardware** button in the Ready to Create Virtual Machine wizard



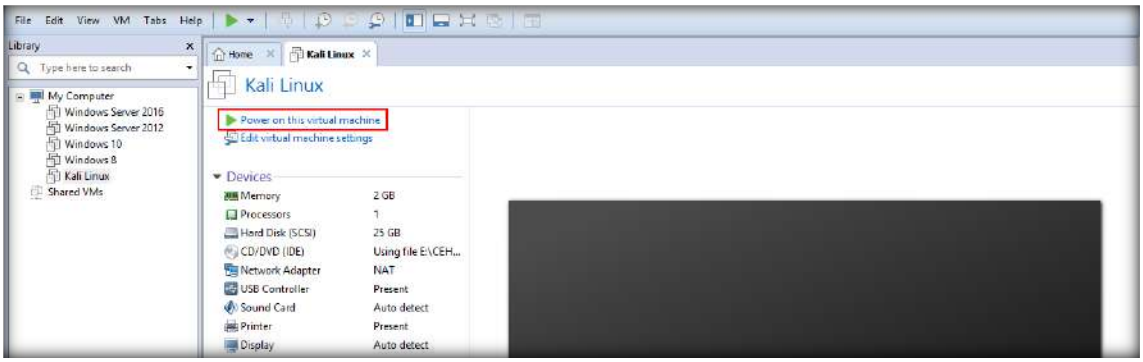
8. Hardware window appears, toggle the memory option to **2 GB** and click **Close**



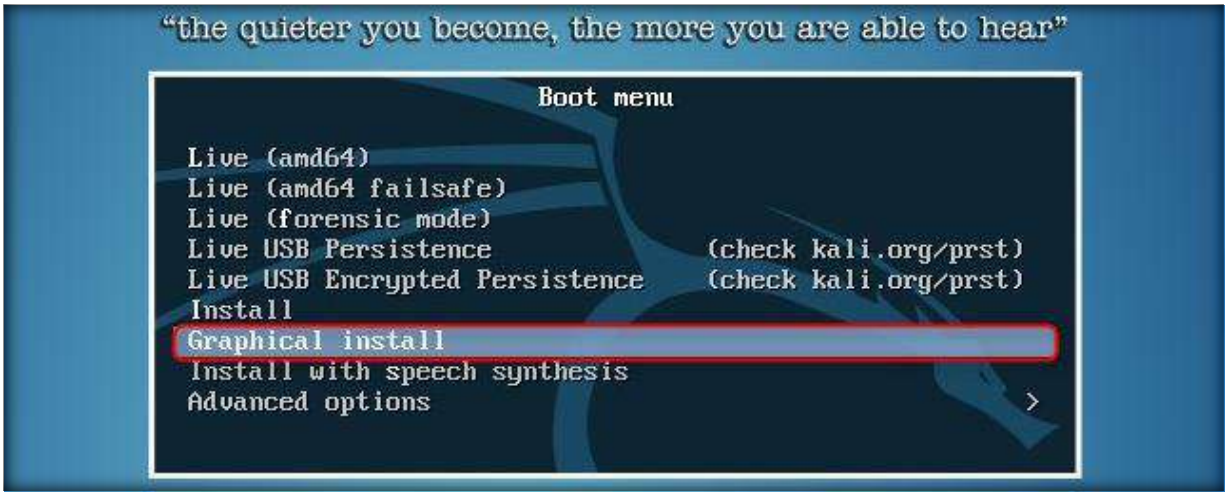
9. Click **Finish** in the Ready to Create Virtual Machine wizard



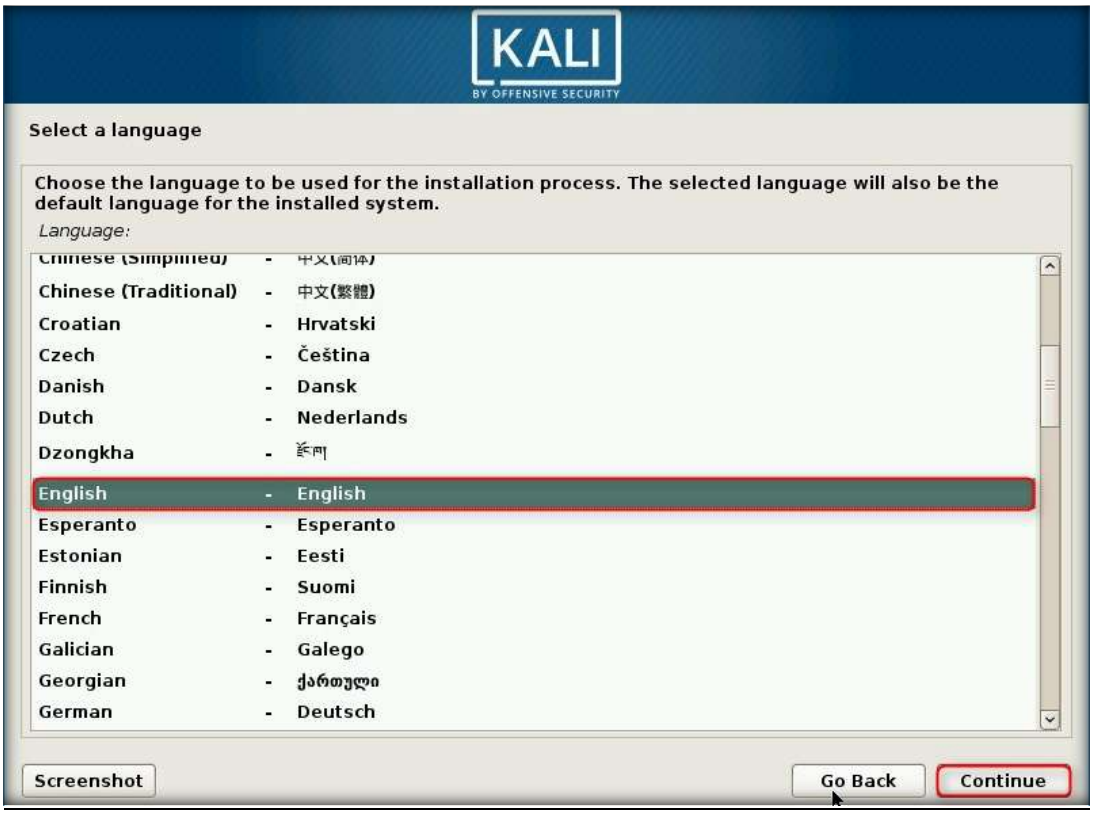
10. Click **Power on this virtual machine** link in the Kali Linux tab as shown in the screenshot



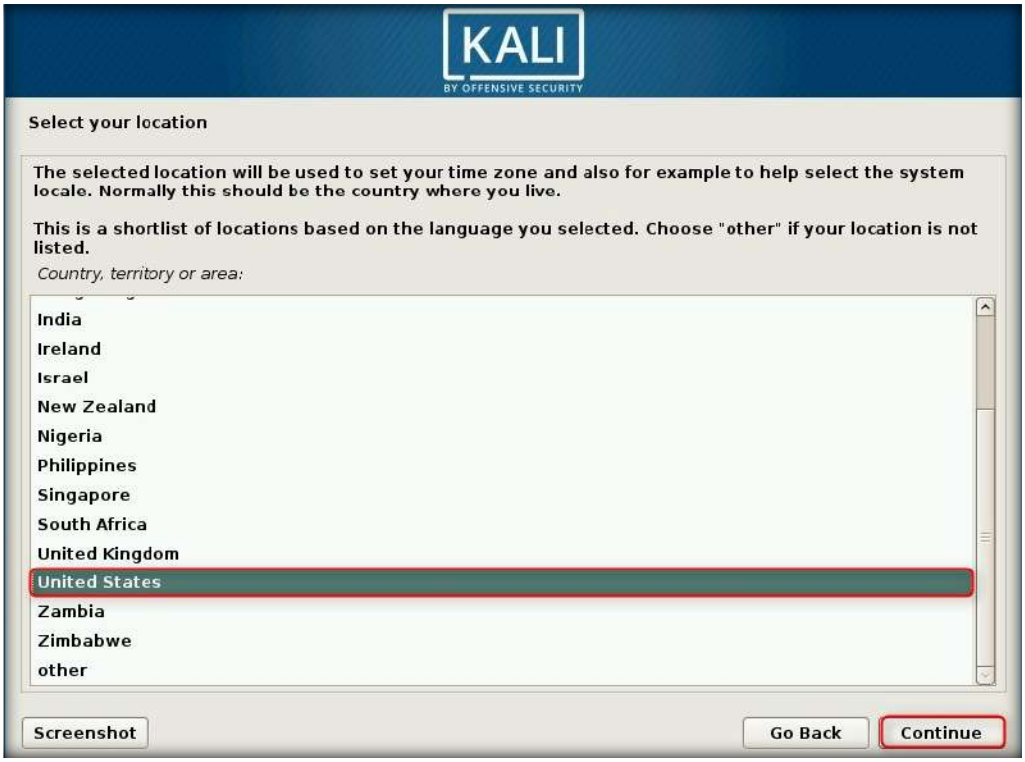
11. Kali Linux **Boot menu** appears, select **Graphical install** and press **Enter**



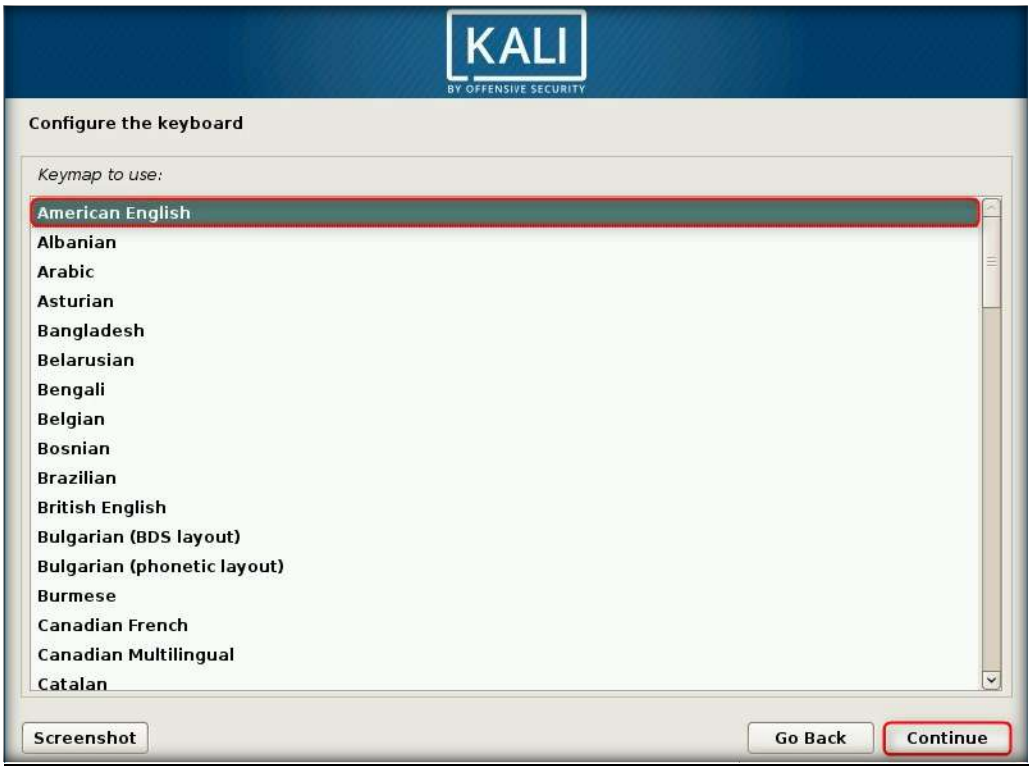
12. **Select a language** window appears, choose a language (here, **English**) and click **Continue**



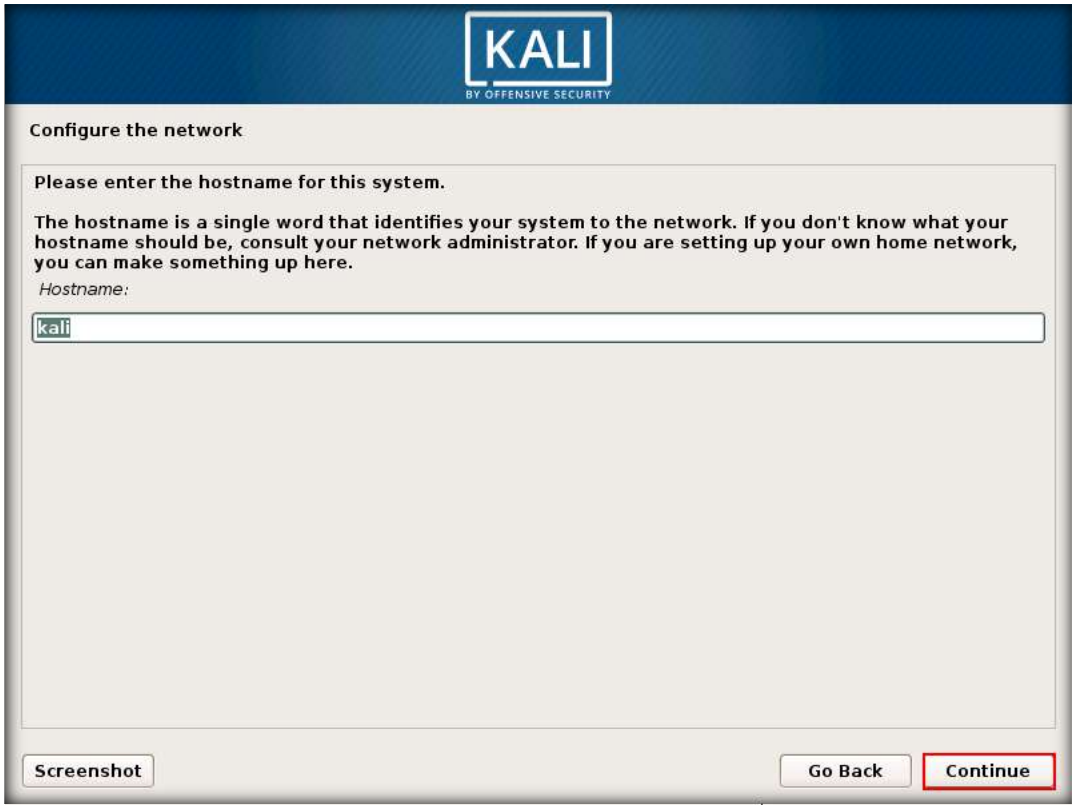
13. In the **Select your location** section, choose a location (here, **United States**) and click **Continue**



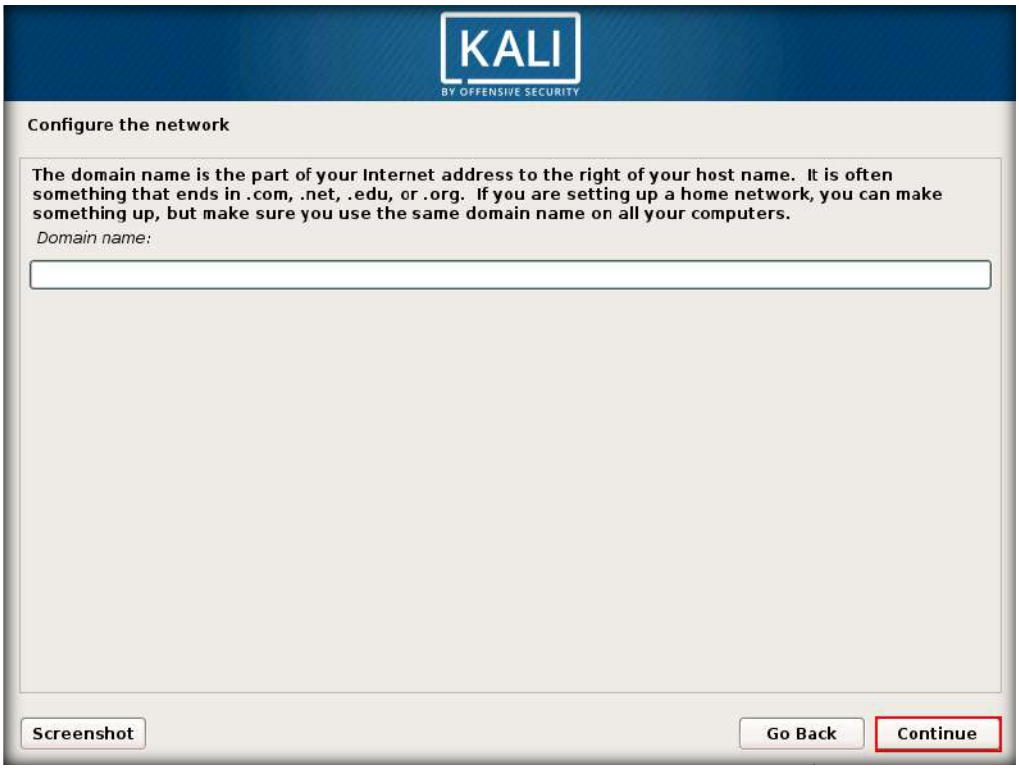
14. **Configure the keyboard** section appears, choose a language (here, **American English**) and click **Continue**



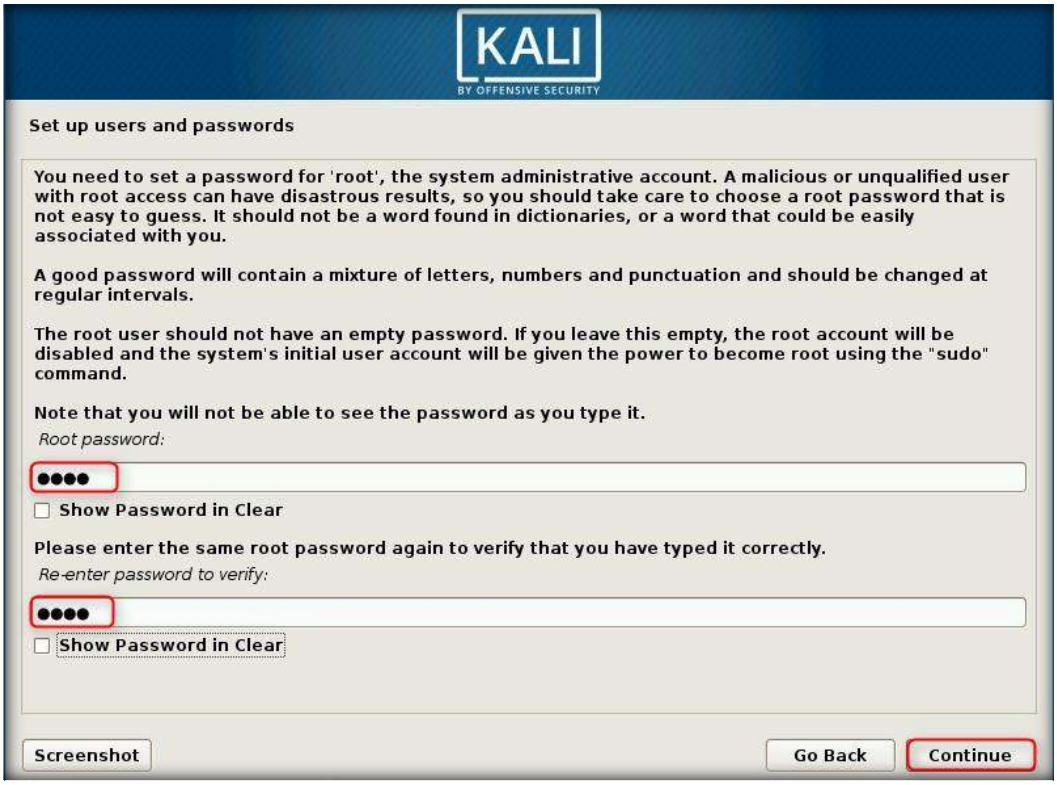
15. **Configure the network** section appears, leave the Hostname to default and click **Continue**



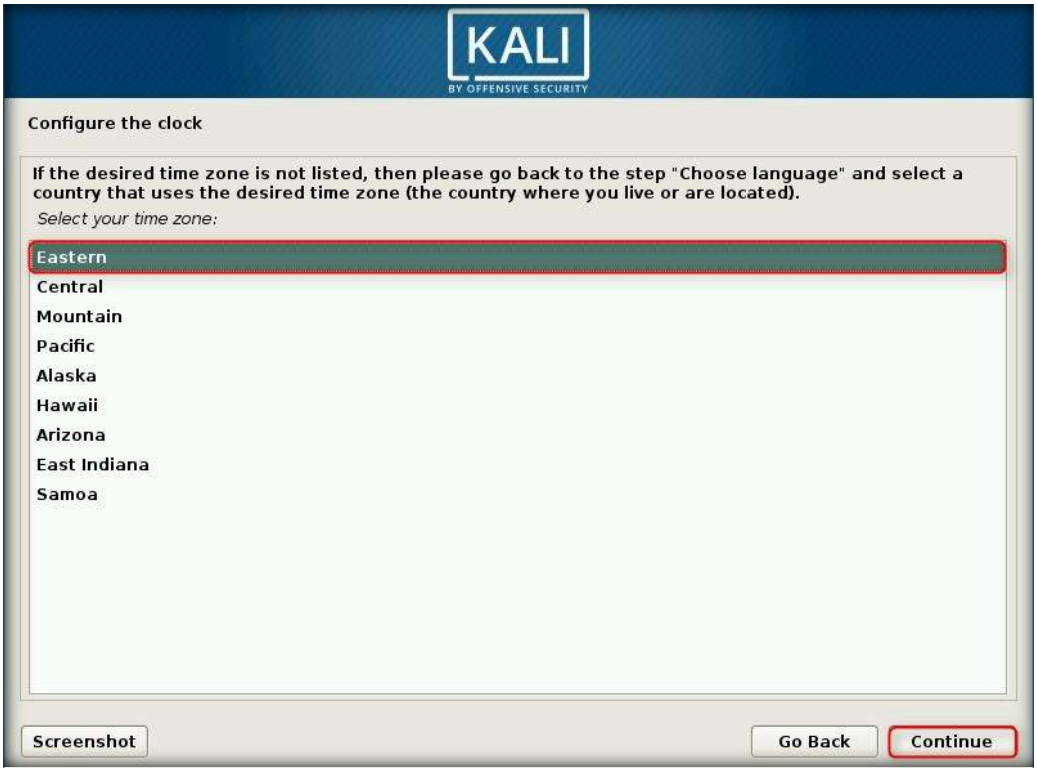
16. **Configure the network** section appears, leave the Domain name: field blank and click **Continue**



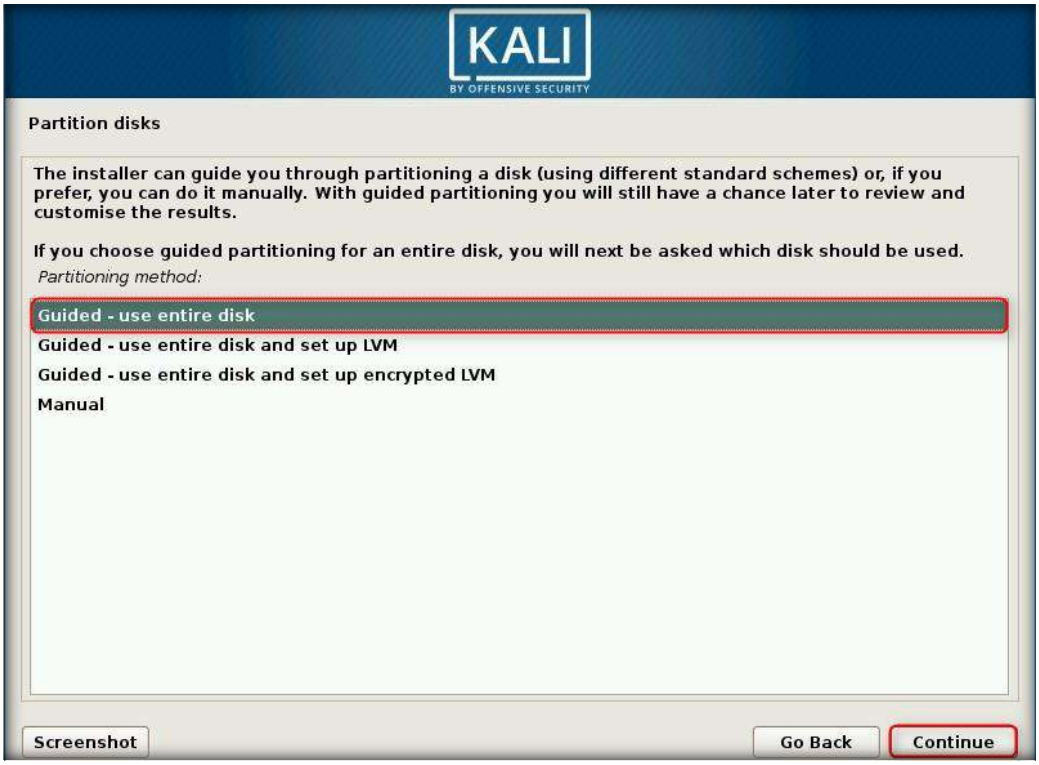
17. **Set up users and passwords** section appears, enter **toor** in both the **Root password** as well as **re-enter password to verify** fields and click **Continue**



18. In **Configure the clock** window, choose the time zone (here, **Eastern**) and click **Continue**
19. Wait until the installer fetches time from the network time server

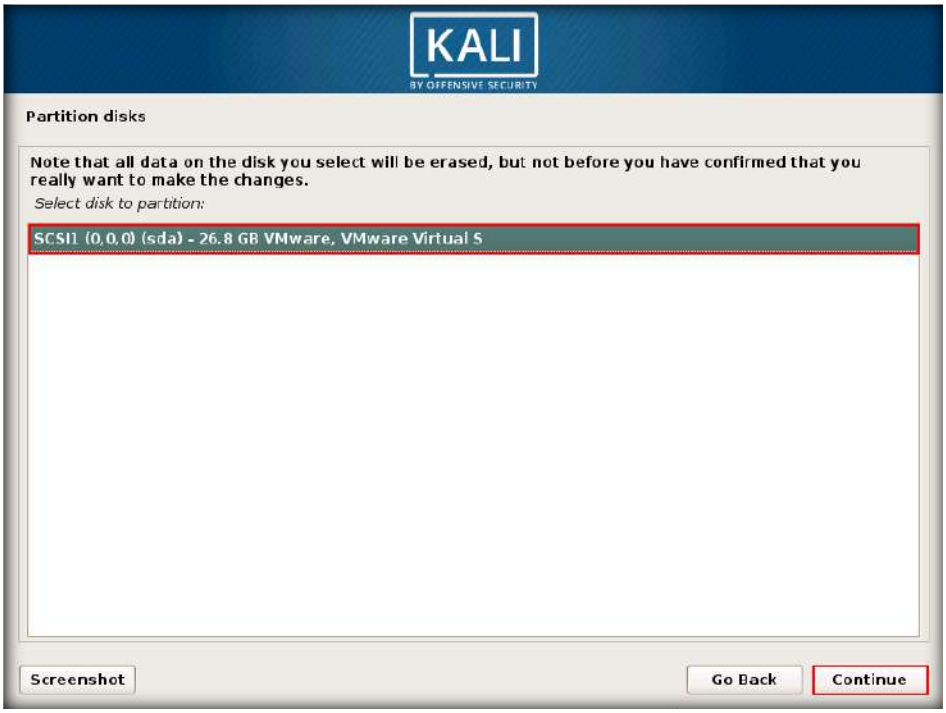


20. **Partition disks** window appears, choose the Partitioning method: **Guided – use entire disk** and click **Continue**

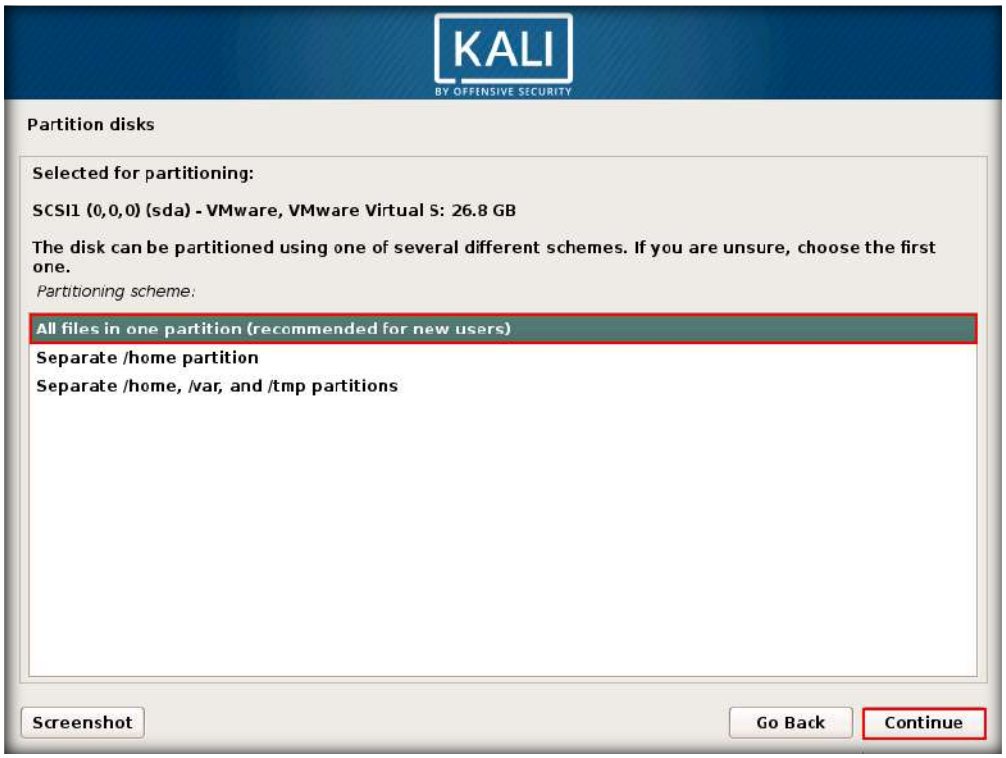


21. Another **Partition disks** window appears, select the disk **SCSI1 (0,0,0) (sda) – 26.8 GB VMware, VMware Virtual S** and click **Continue**

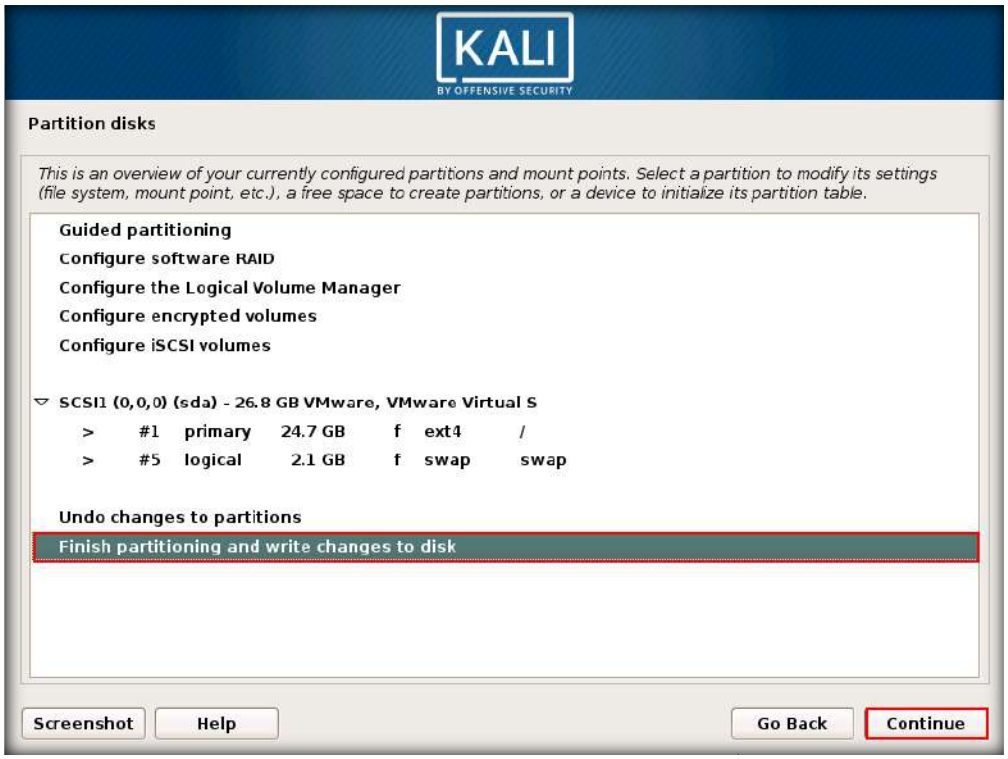
    Note: The size of the disk (**26.8 GB**) may vary in your lab environment



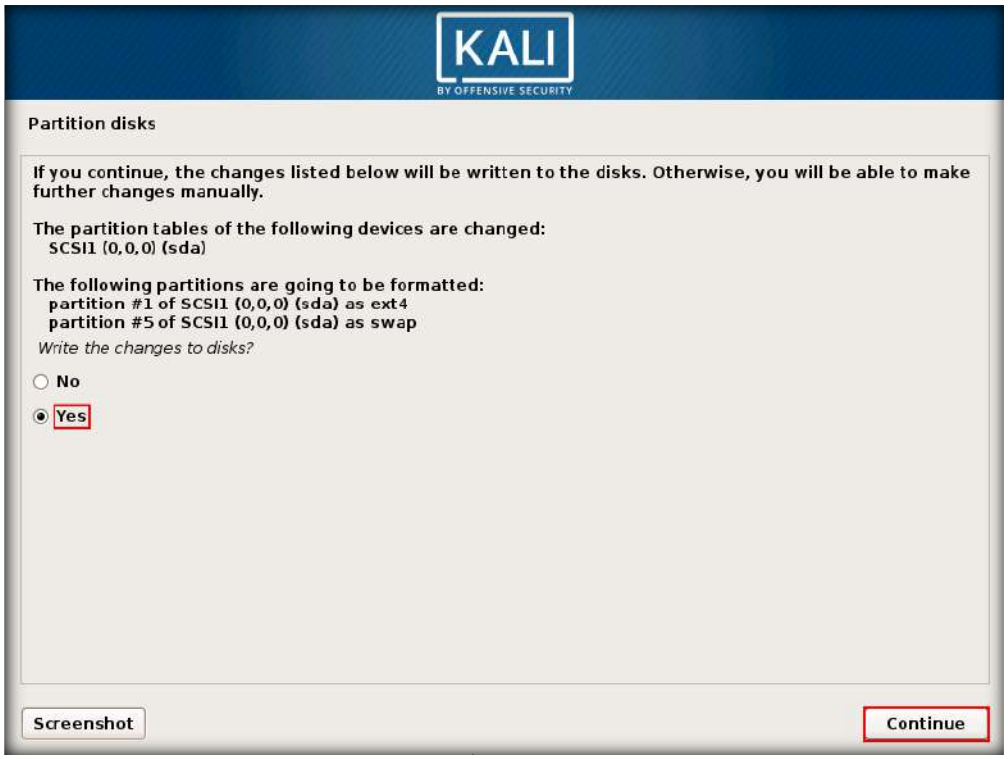
22. In the **Partition disks** window, choose the Partitioning scheme: **All files in one partition (recommended for new users)** and click **Continue**



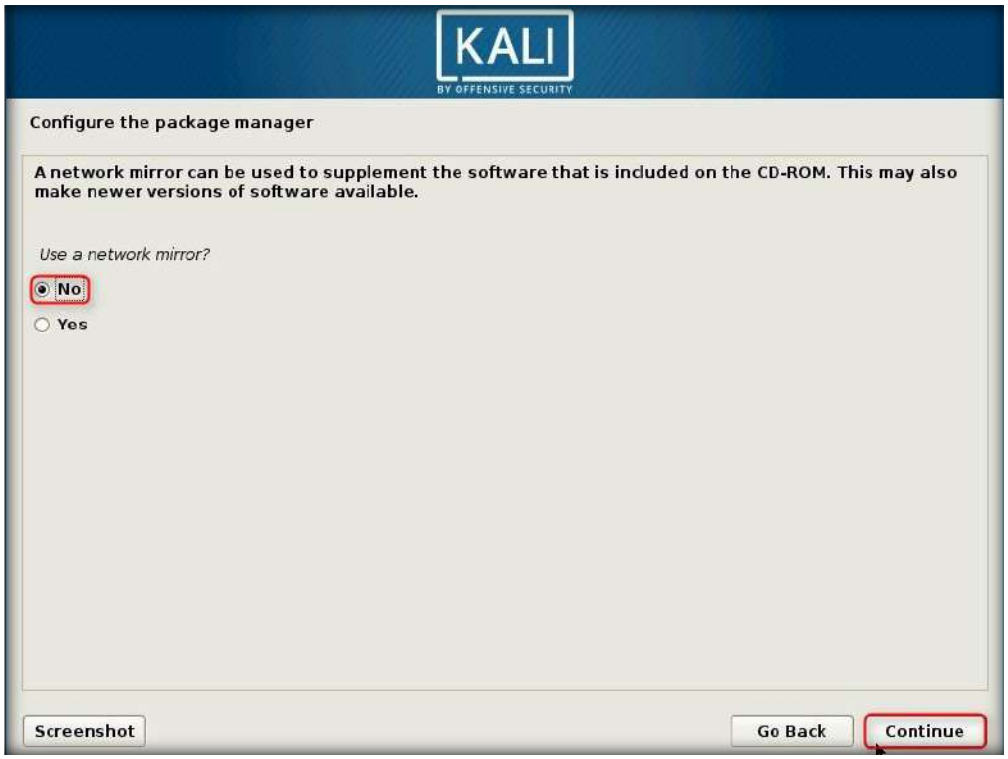
23. **Partition disks** window appears displaying the overview of your currently configured partitions, choose **Finish partitioning and write changes to disk** and click **Continue**



24. A **Partition disks** window appears stating that the changes will be written to the disk, select **Yes** and click **Continue**

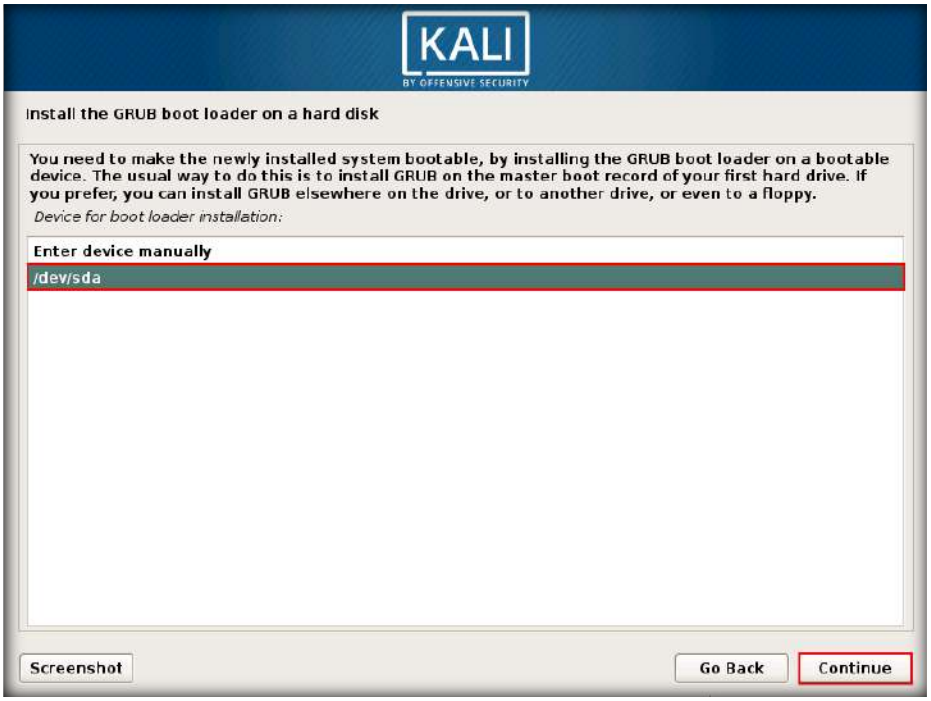


25. On completion of installation, **Configure the package manager** window appears, select **No** and click **Continue**



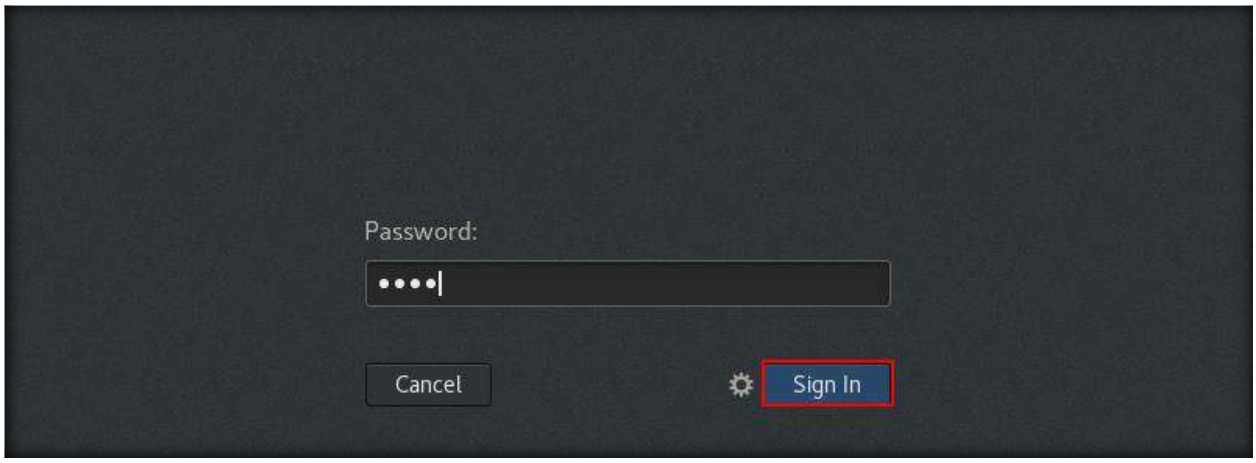
26. **Install the GRUB boot loader on a hard disk** window appears, select **Yes** in order to install the GRUB boot loader to the master boot record and click **Continue**

27. Select the available device in Device for boot loader installation (here, **/dev/sda**) and click **Continue**
28. Wait until the GRUB boot loader is installed

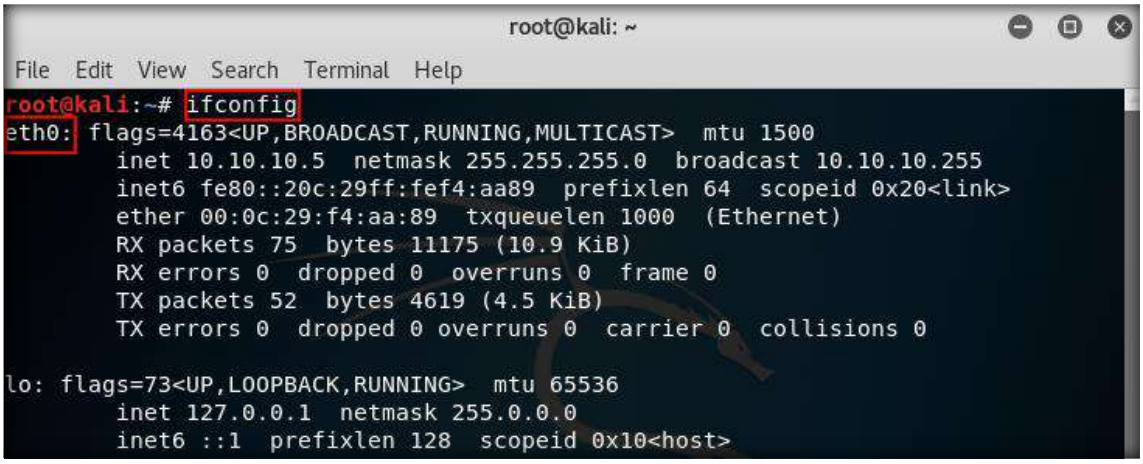


29. Wait until the partitions are formatted and the operating system is installed
30. It takes some time for the installation to complete. Finish the installation window appears, click **Continue**

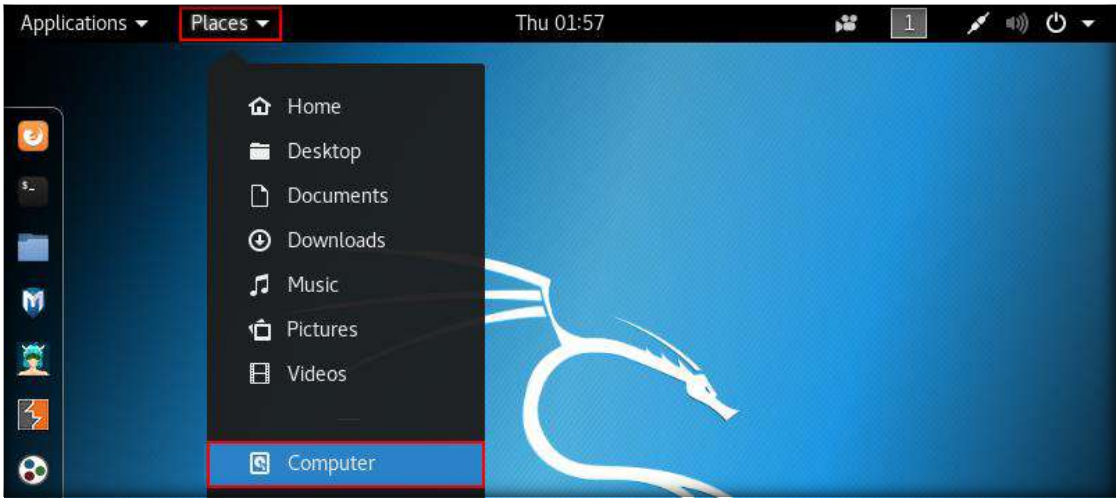
31. Once the installation is finished the machine will get restarted, and after the restart it will come to the login screen. Login to the machine with Username: **root** and Password: **toor**



32. Click **Terminal** icon from the left-hand side of the **Favorites** bar, and type **ifconfig** and press **Enter** to check with the network adapter, here it is **eth0** (it might differ in your lab environment). Close the terminal window after making a note of the adapter

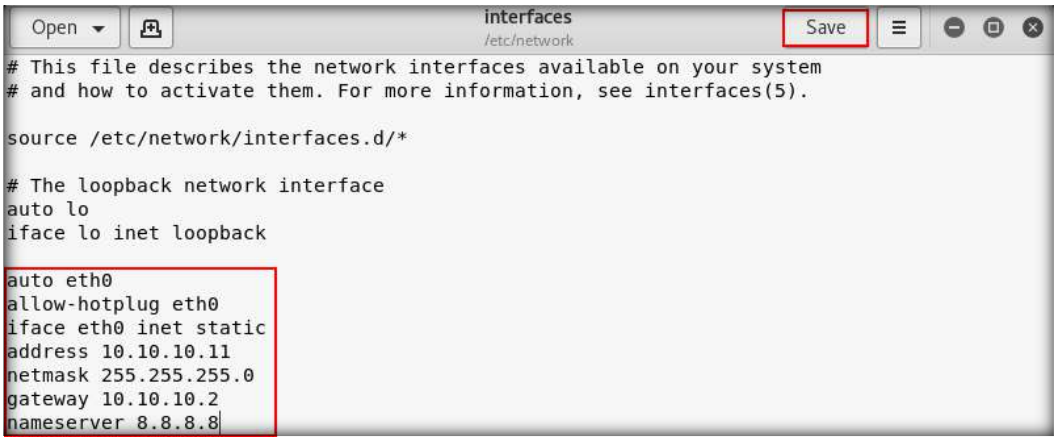


33. Now you need to configure the Network. To do this navigate to **Places** and click **Computer**

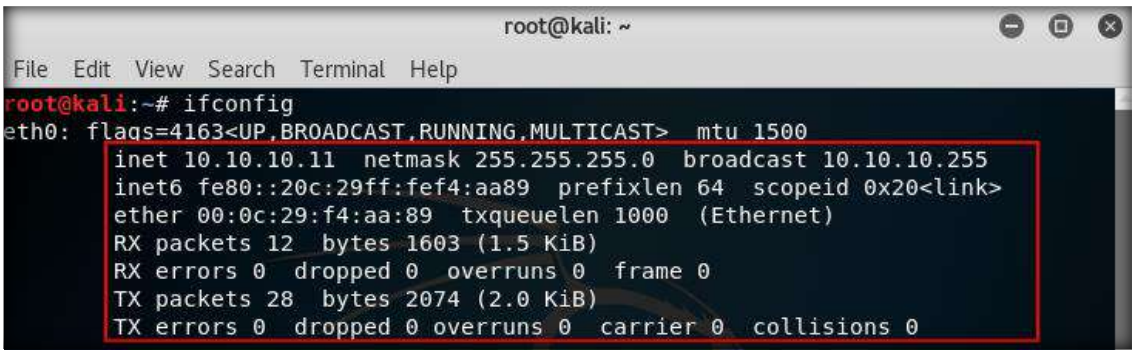


34. Computer window appears, navigate to etc → network and double-click **Interfaces** file

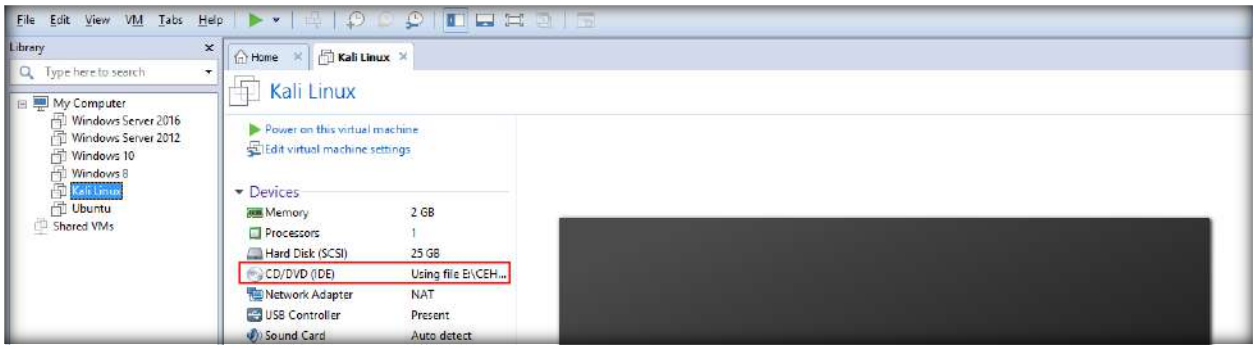
35. In the Interfaces file type, the following details to assign the static IP address and click **Save**
    - **auto eth0**
    - **allow-hotplug eth0**
    - **iface eth0 inet static**
    - **address 10.10.10.11**
    - **netmask 255.255.255.0**
    - **gateway 10.10.10.2**
    - **nameserver 8.8.8.8**



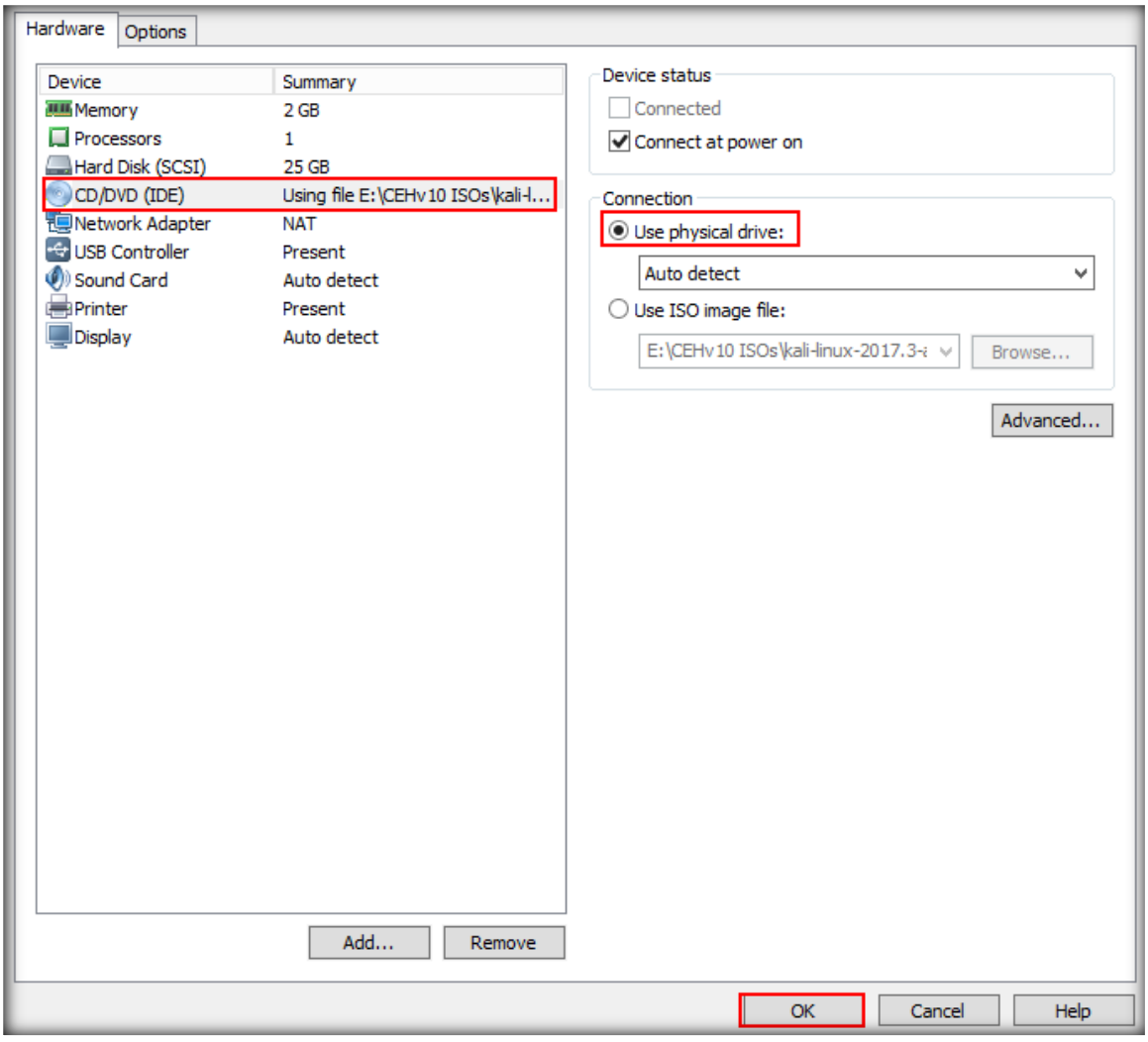
36. **Restart/Reboot** the machine to configure the IP address
37. Once the machine is restarted, login to the machine and open a **terminal** from the **Favorites** bar and type **ifconfig** and press **Enter** to verify the IP configuration. Close the terminal window and shutdown the machine



38. Once the machine is turned off, select Kali Linux in the left pane and click CD\DVD (IDE) under devices section



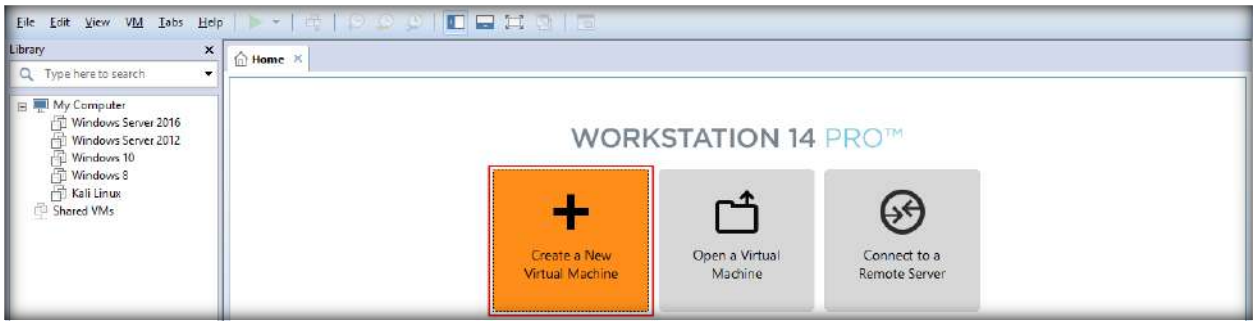
39. Virtual Machine Settings window appears, choose **Use physical drive:** radio button under Connection section and click **OK**



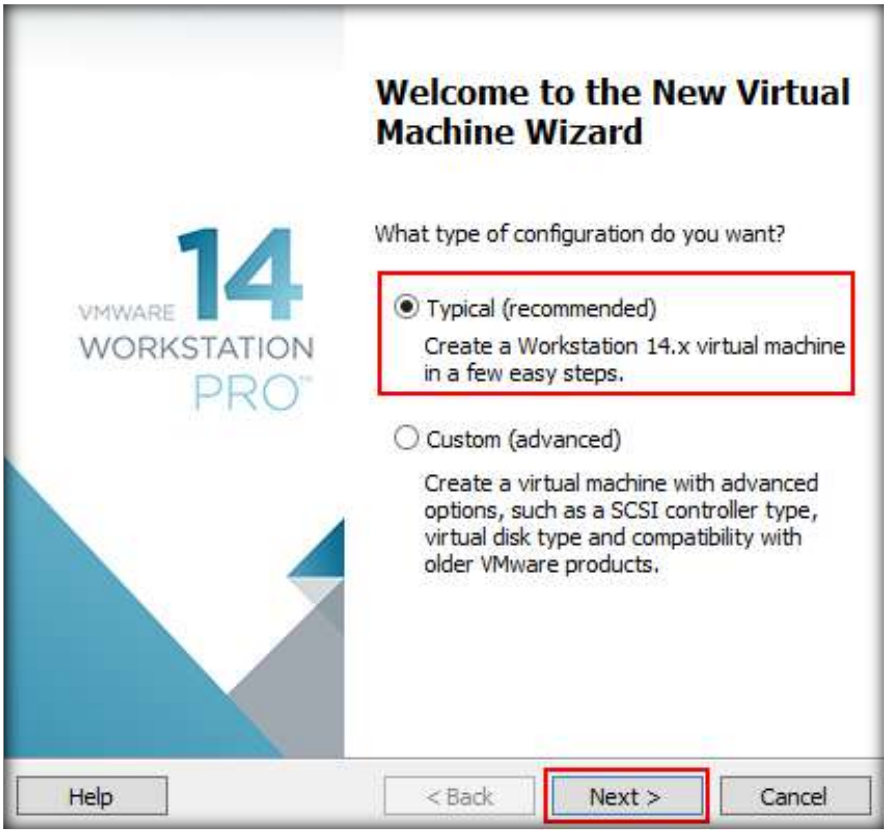
[Back to Configuration Task Outline]

CT#8: Install Ubuntu in VMware

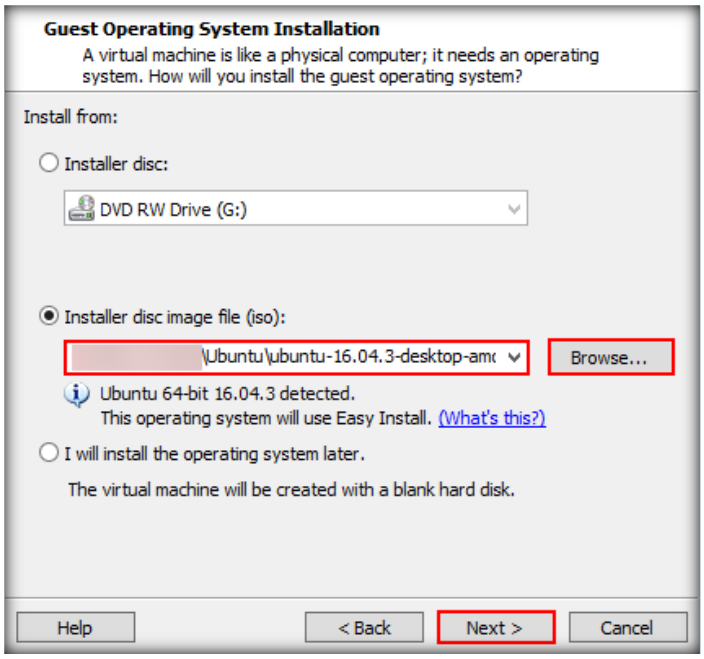
1. In VMware Workstation window, click **Create a New Virtual Machine**



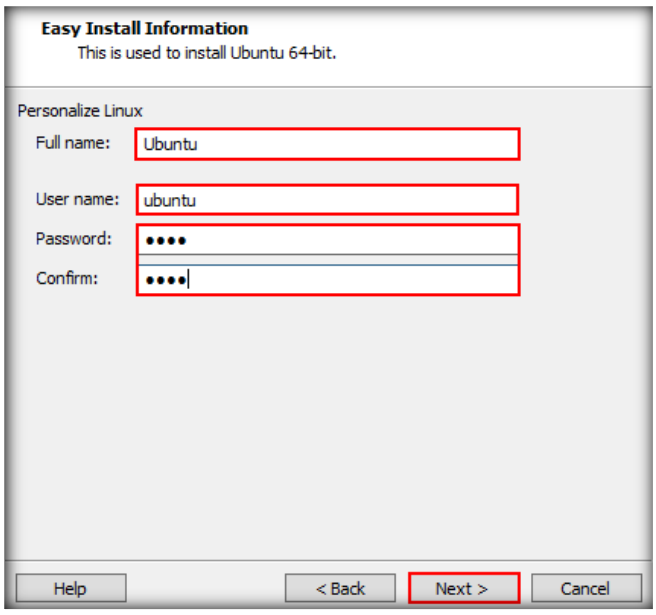
2. In the New Virtual Machine wizard, leave the settings to default and click **Next**



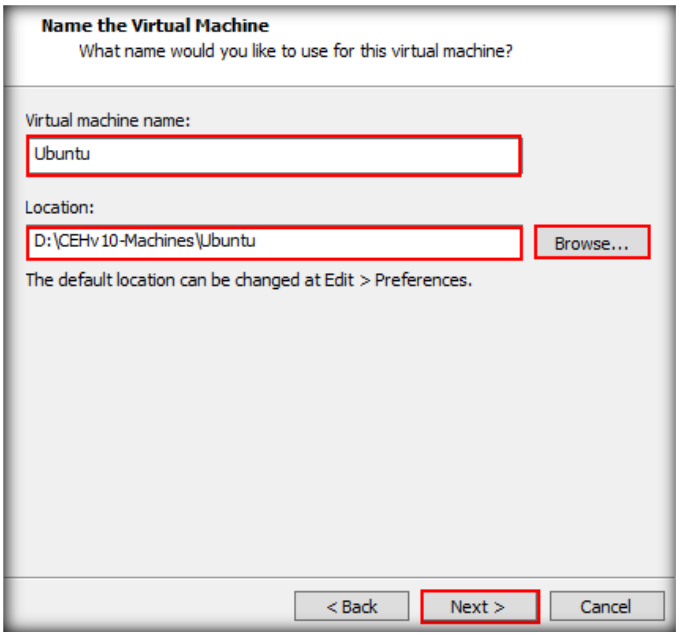
3. In Guest Operating System Installation wizard, choose **Installer disc image file (iso)**: radio button. Click **Browse** and navigate to D:\CEH-Tools\CEHv10 Lab Prerequisites\ISO's\Ubuntu and select **ubuntu-16.04.3-desktop-amd64.iso** to provide the ISO path and click **Next**



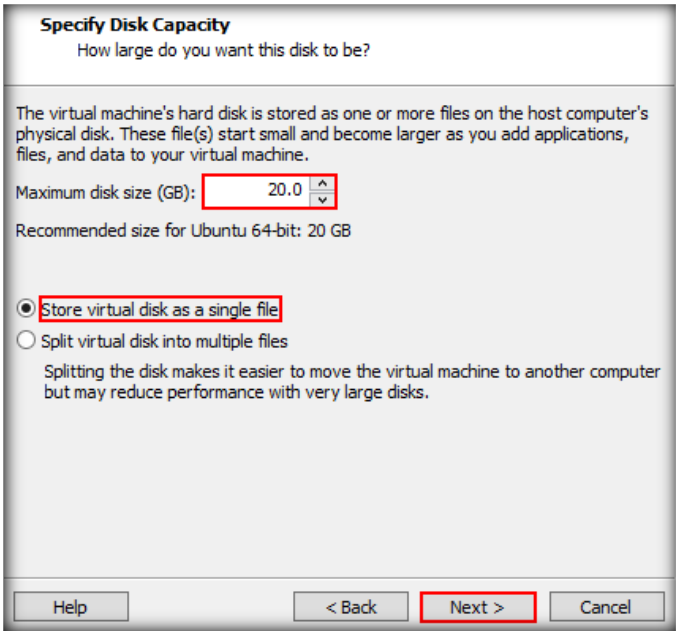
4. Easy Install Information wizard appears, type the following information in the Personalize Linux section and click **Next**
   - Full name: **Ubuntu**
   - User name: **ubuntu**
   - Password: **toor**
   - Confirm: **toor**



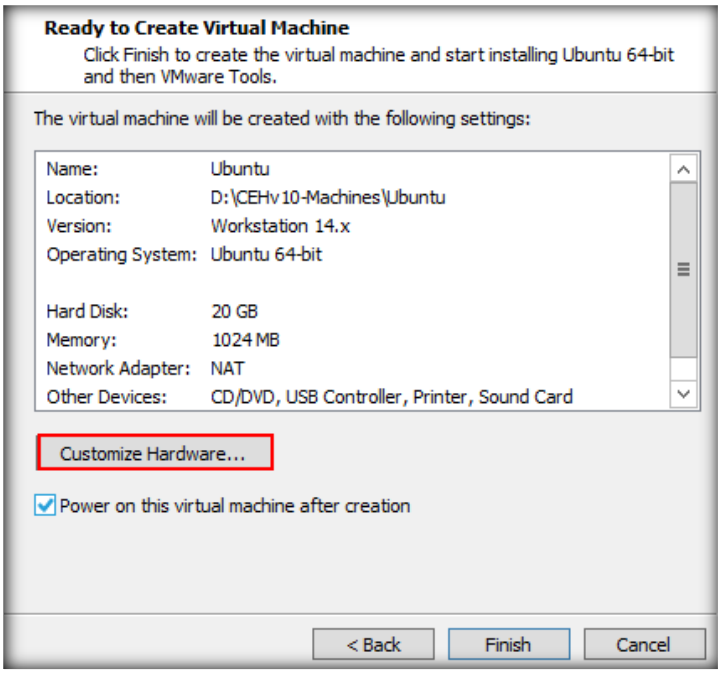
5. Name the Virtual Machine wizard appears, type **Ubuntu** in the Virtual machine name field, and click **Browse** button to store the virtual hard disk and click **Next**



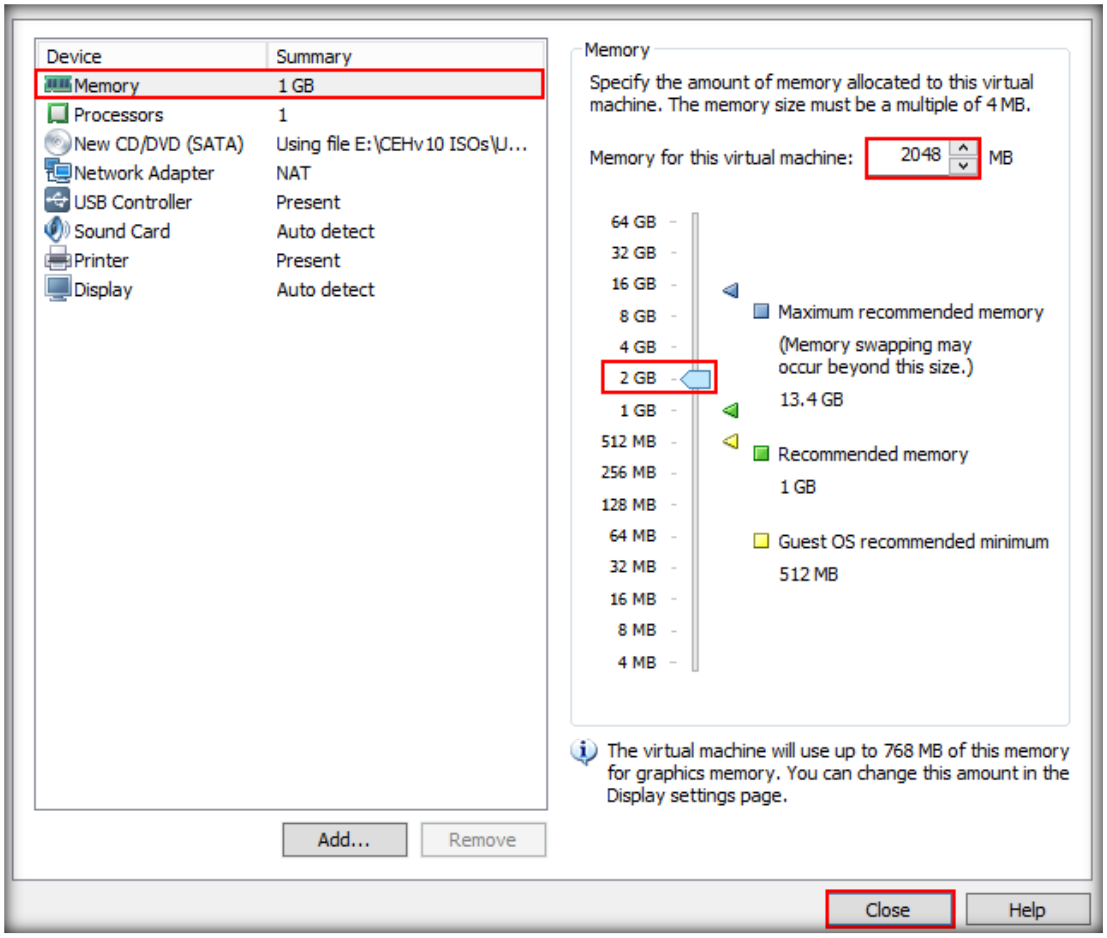
6. Specify Disk Capacity wizard, leave the Maximum disk size as recommended (i.e., **20 GB**) and select **Store virtual disk as a single file** and click **Next**



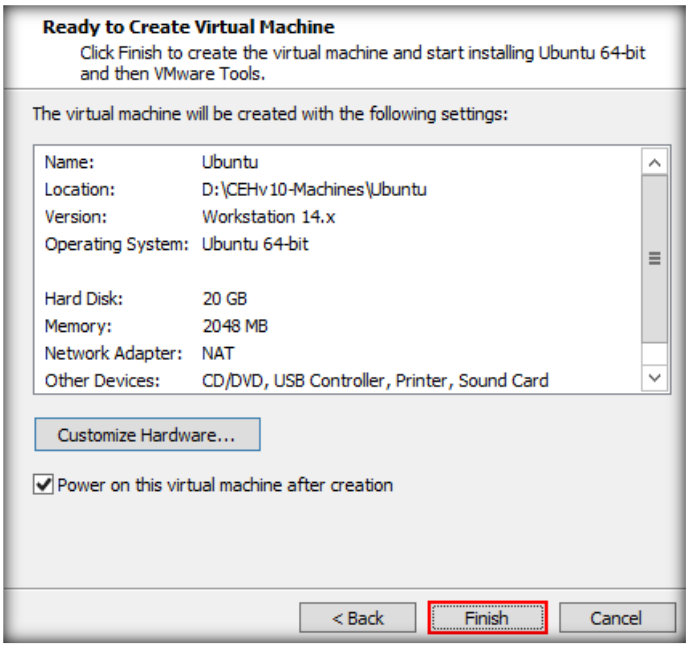
7. Click **Customize Hardware** button in the Ready to Create Virtual Machine wizard



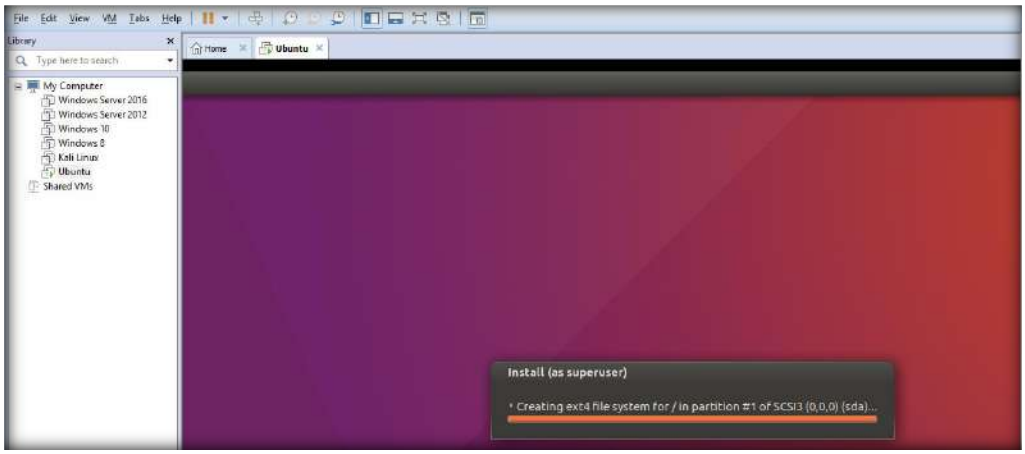
8. Hardware window appears, toggle the memory option to **2 GB** and click **Close**



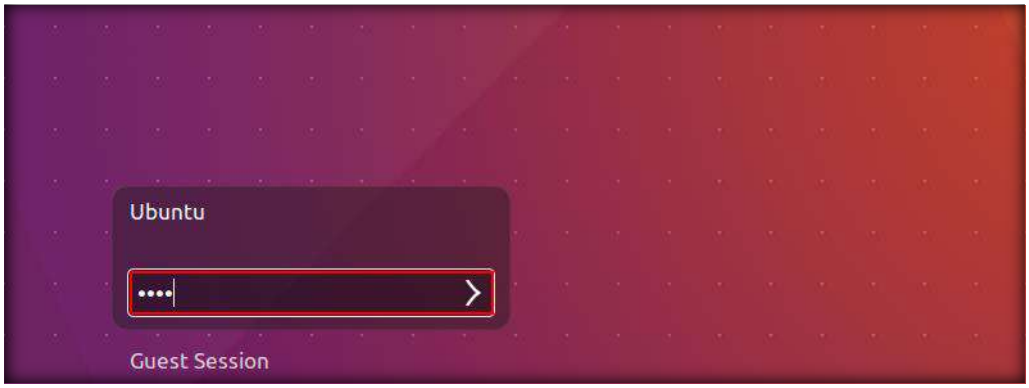
9. Click **Finish** in the Ready to Create Virtual Machine wizard



10. As soon as you click **Finish** button VMware Workstation starts installing the Ubuntu OS as shown in the screenshot. Wait until installation is completed

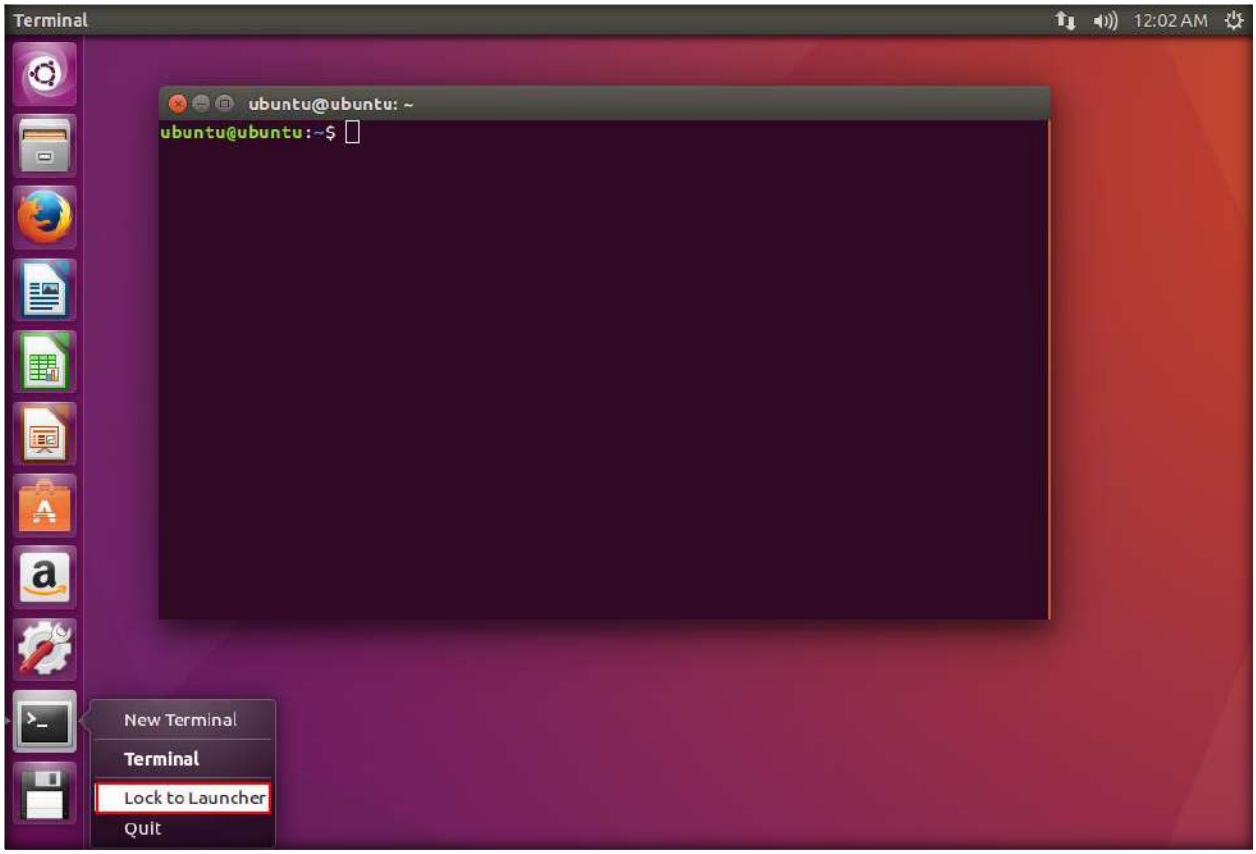


11. Once the installation is finished, the machine will get restarts and provide you with the login screen, with the Username Ubuntu. Type **toor** in the Password field and press **Enter**



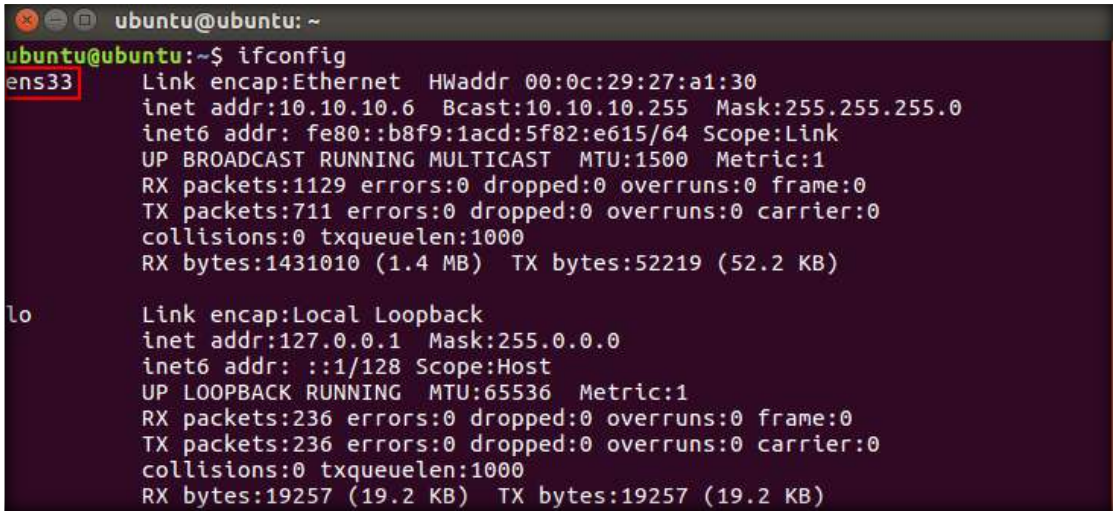
12. Click **Search your computer** icon, and type **terminal** in the search bar. From the search results click **Terminal** icon to launch

13. Terminal window appears, right-click on Terminal icon on the Launcher and click **Lock to Launcher** as shown in the screenshot to lock the terminal on the launcher



14. In the terminal window, type **ifconfig** and press **Enter** to check with the enabled network adapter. Here the network adapter is **ens33** as shown in the screenshot

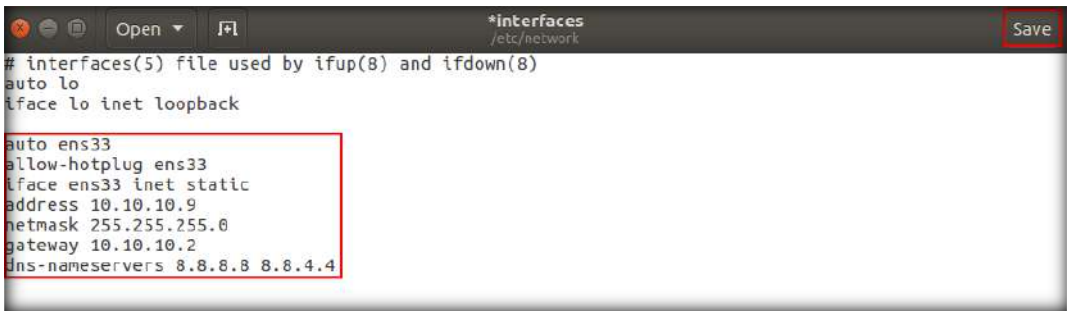
    Note: Network adapter may vary in your lab environment



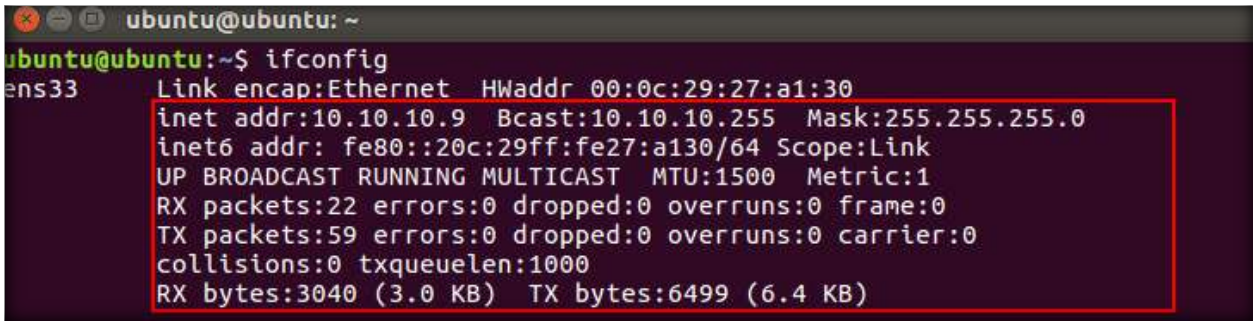
15. Configure Static IP. In the terminal window type **sudo gedit /etc/network/interfaces** and press **Enter** type **toor** in the password for ubuntu to open **Interfaces** file with root user

16. Interfaces file opens in the text editor, type the following IP configuration details in the text editor and click **Save**
    - **auto ens33**
    - **allow-hotplug ens33**
    - **iface ens33 inet static**
    - **address 10.10.10.9**
    - **netmask 255.255.255.0**
    - **gateway 10.10.10.2**
    - **dns-nameservers 8.8.8.8 8.8.4.4**

17. **Reboot** or **Restart** the machine to apply the network configuration

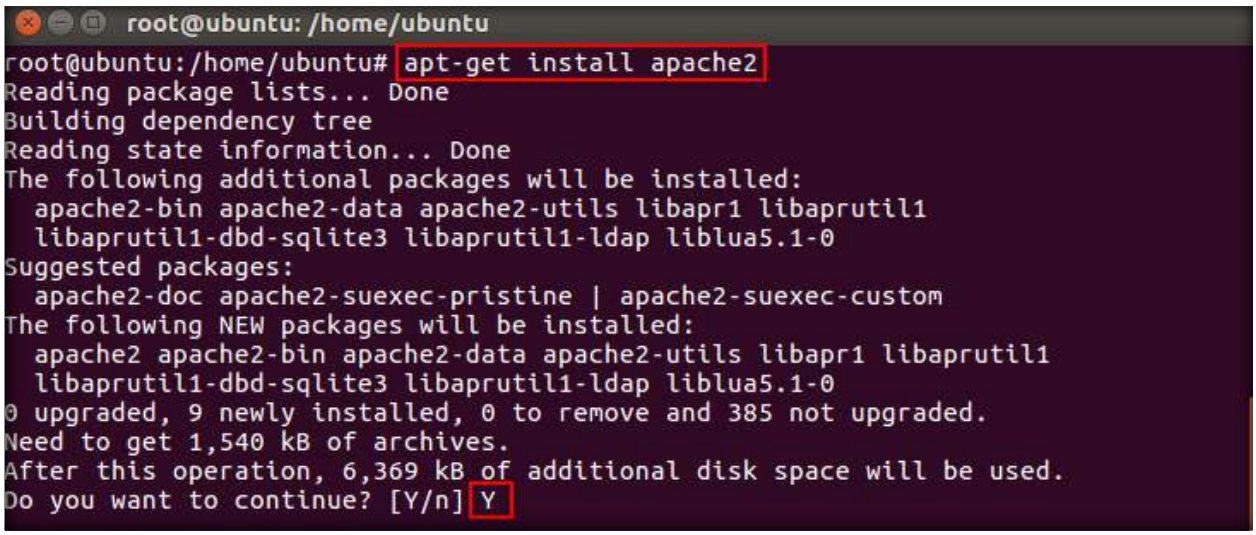


18. Once the machine is restarted, login to the machine and open a **terminal** from the **Launcher** bar and type **ifconfig** and press **Enter** to verify the IP configuration. Close the terminal window and shutdown the machine



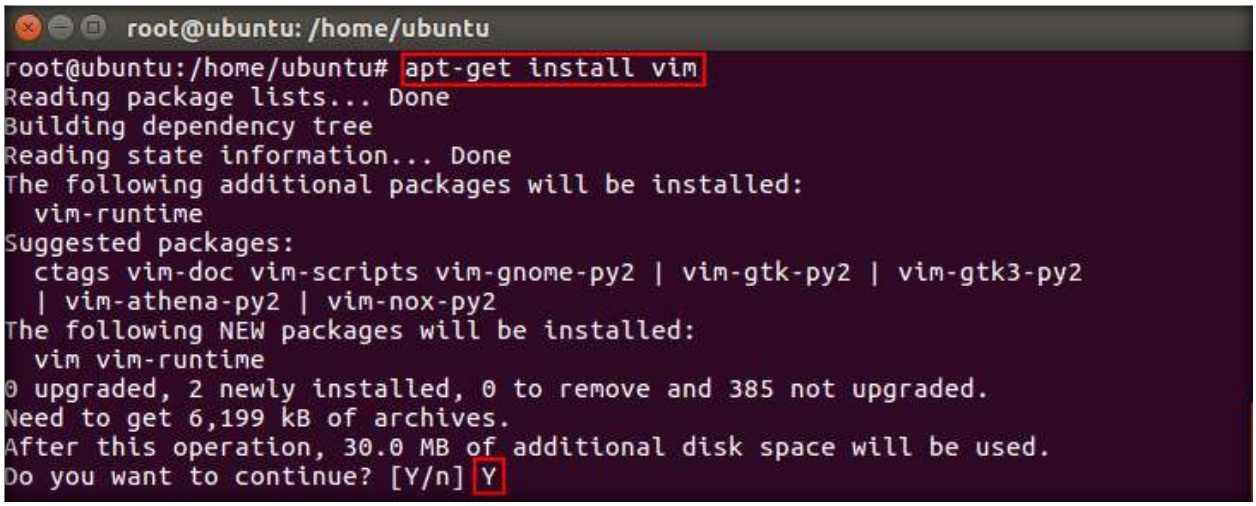
19. In the terminal window type **sudo su** and press **Enter**
20. You will be prompted to enter a password. Type the password as **toor** and press **Enter**. The password which you type will not be visible

21. Type the command **apt-get install apache2** and press **Enter**. This command is issued to install apache web server
22. While installing the server, a notification appears saying additional disk space will be used. Type **y** and press **Enter**



23. Type the command **apt-get install vim** and press **Enter**. This command in issued in order to install vim editor

24. While installing, a notification appears saying additional disk space will be used. Type **y** and press **Enter**

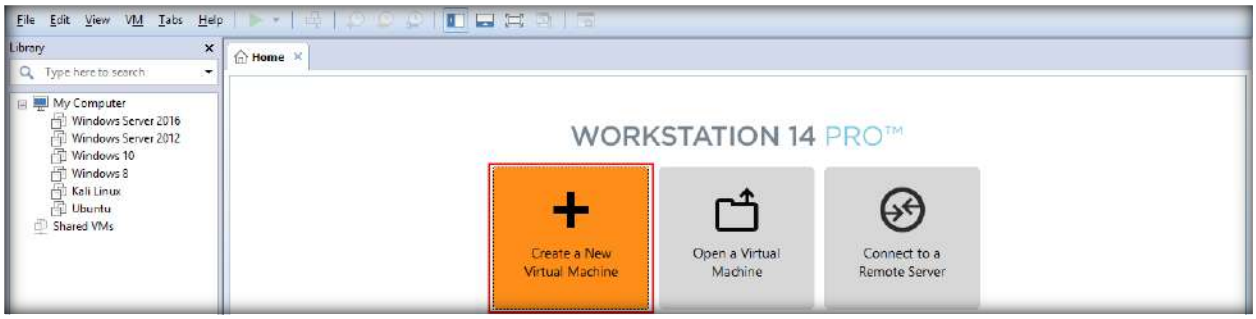


25. Close the terminal window after installation completes, shut down the machine

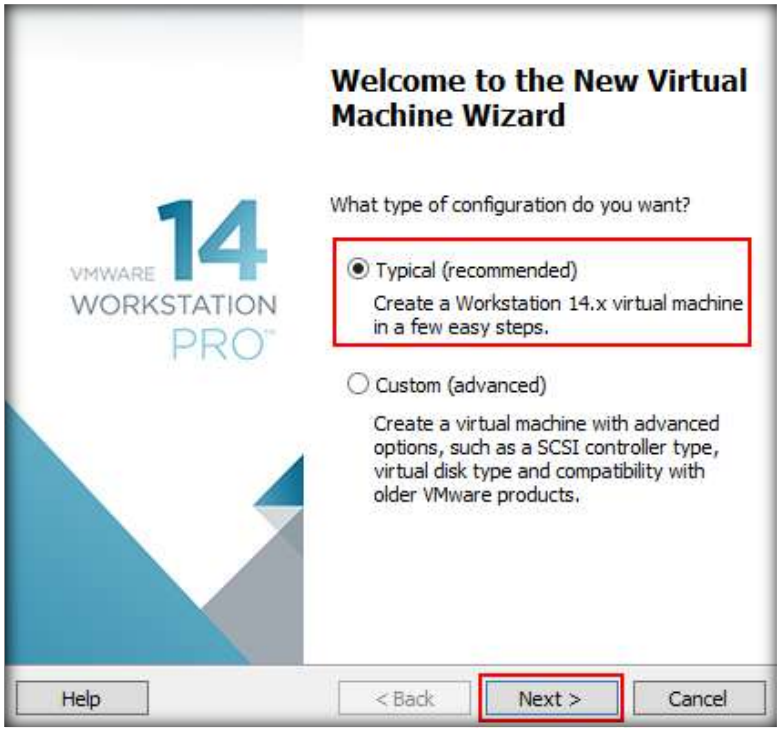
[Back to Configuration Task Outline]

CT#9: Install Android in VMware Workstation

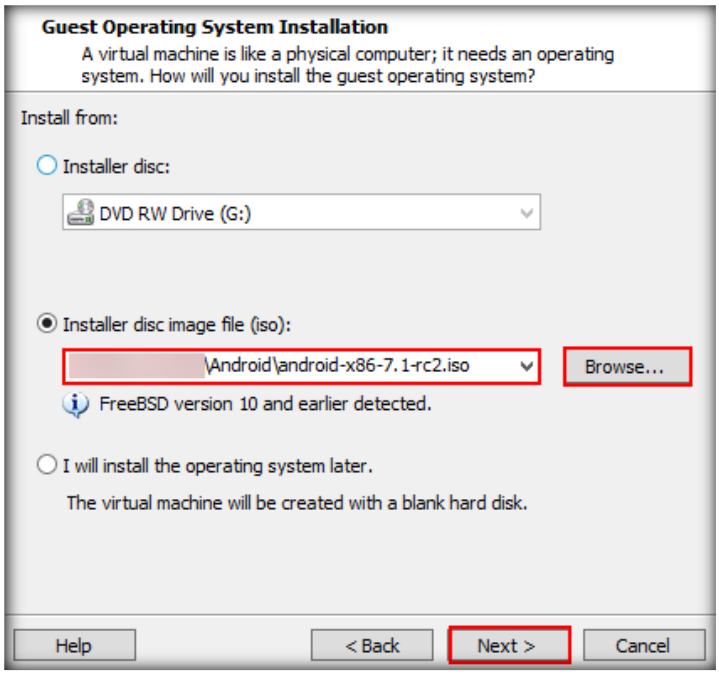
1. In VMware Workstation window, click **Create a New Virtual Machine**



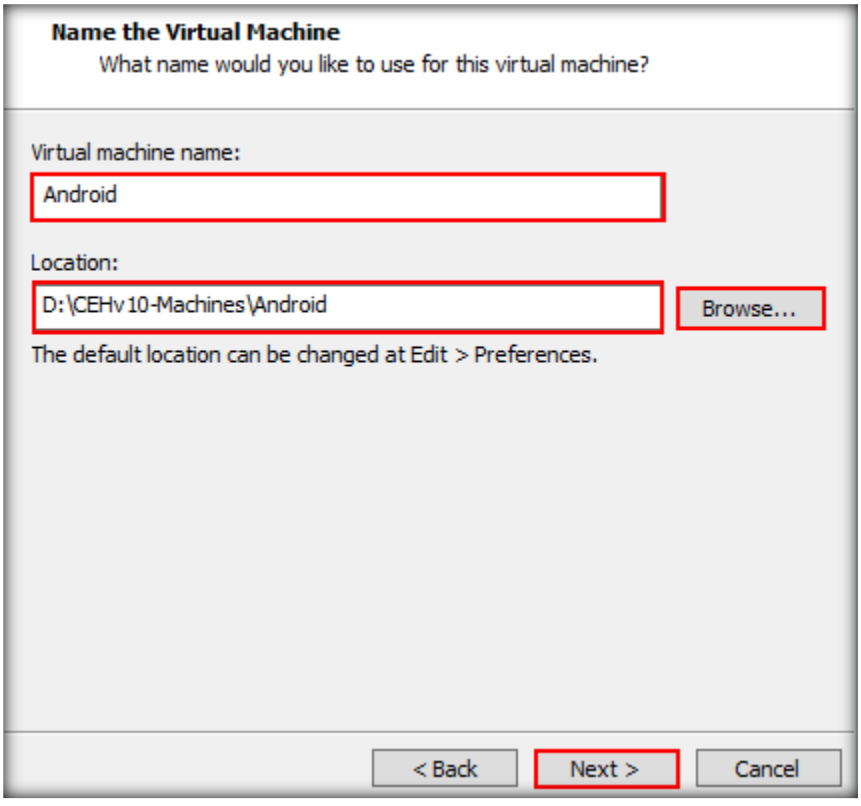
2. In the New Virtual Machine wizard, leave the settings to default and click **Next**



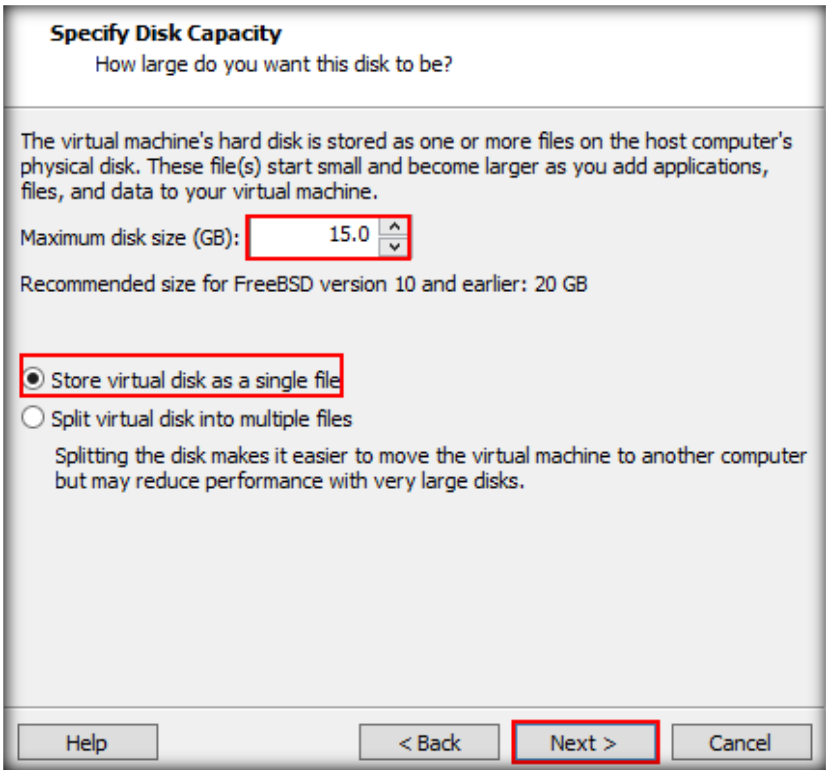
3. In Guest Operating System Installation wizard, choose **Installer disc image file (iso)**: radio button. Click **Browse** and navigate to D:\CEH-Tools\CEHv10 Lab Prerequisites\ISO's\Android and select **android-x86-7.1-rc2.iso** to provide the ISO path and click **Next**



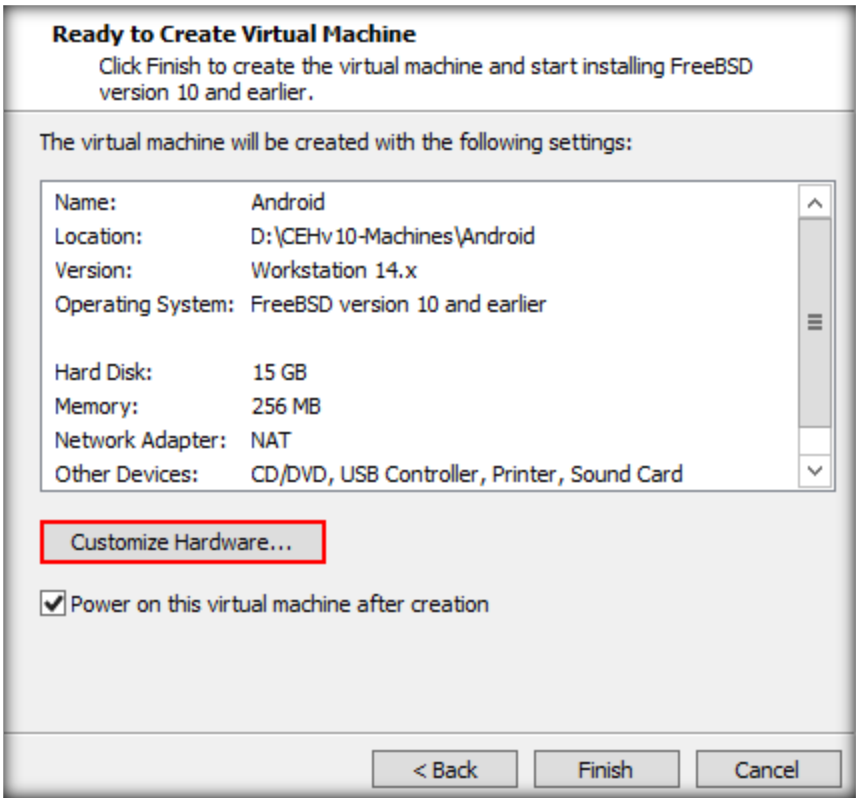
4. Name the Virtual Machine wizard appears, type **Android** in Virtual machine name field, and click Browse to store the virtual hard disk and click **Next**



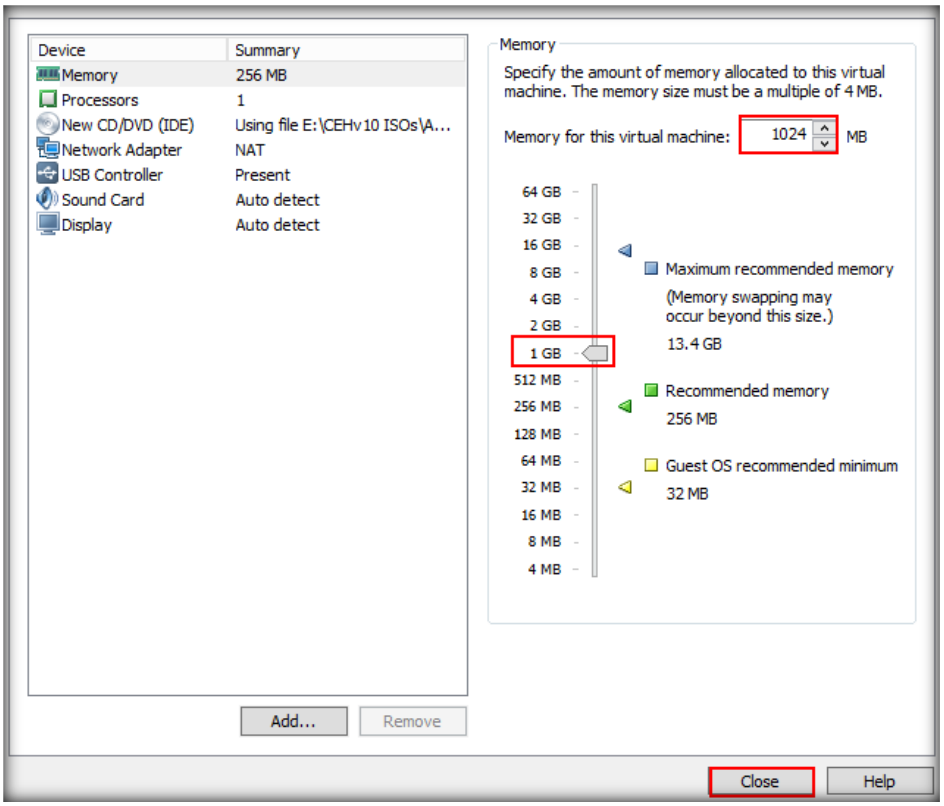
5. Specify Disk Capacity wizard appears, type **15.0 GB** in the Maximum disk size, and choose Store virtual disk as a single file radio button and click **Next**



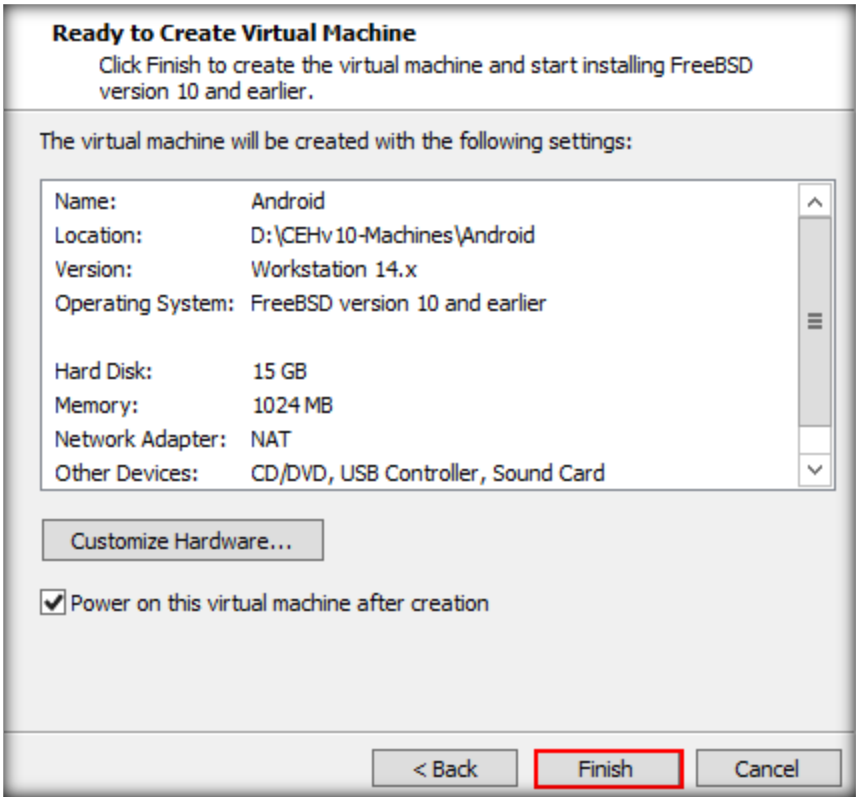
6. Click **Customize Hardware** button in the Ready to Create Virtual Machine wizard



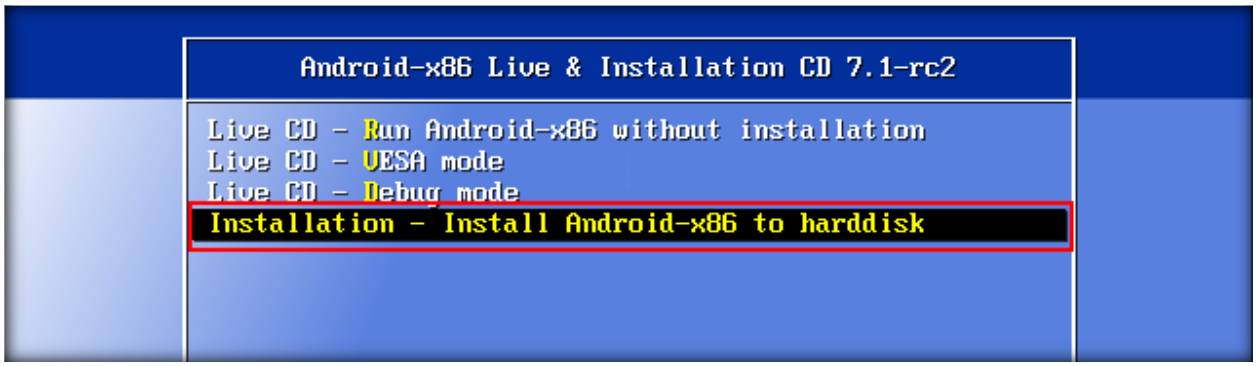
7. Hardware window appears, toggle the memory option to **1 GB** and click **Close**



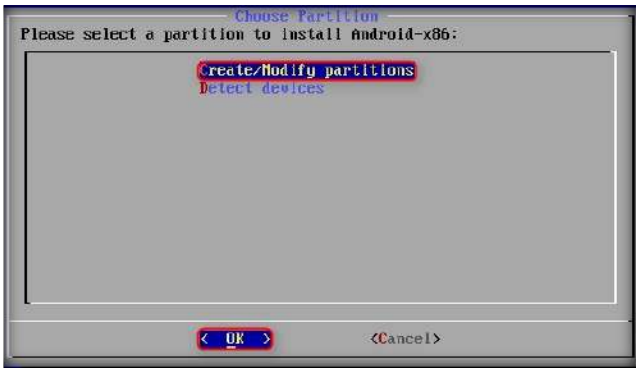
8. Click **Finish** in the Ready to Create Virtual Machine wizard



9. Android virtual machine installation GUI appears on the screen, select **Installation - Install Android-x86 to harddisk** option and press **Enter**

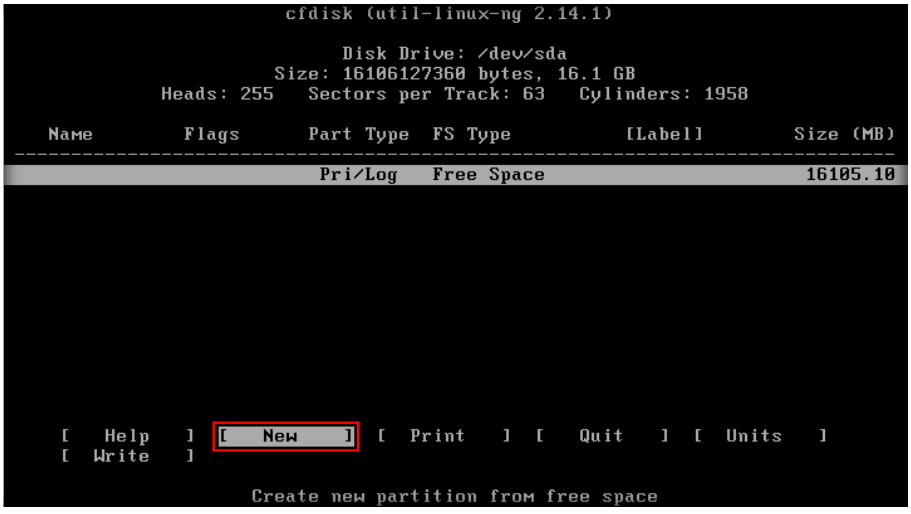


10. **Choose Partition** window appears. By default, **Create/Modify partitions** is selected, select **OK**



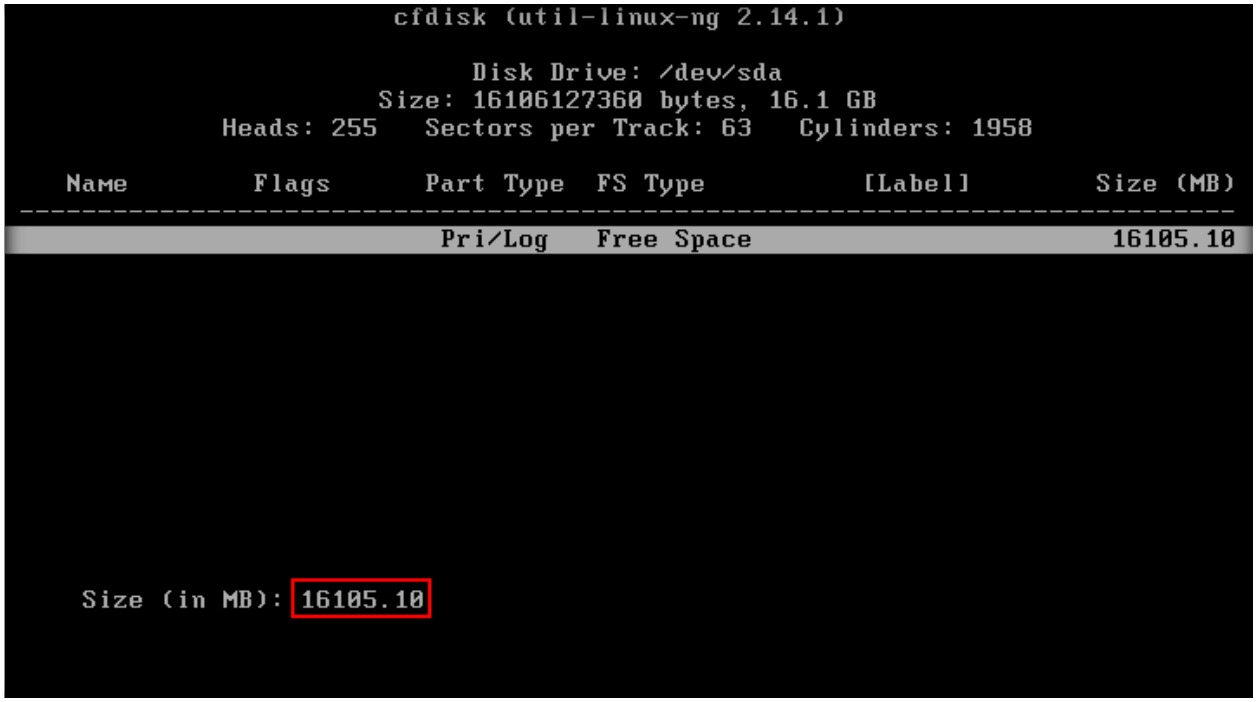
11. Confirm pop-up appears. Do you want to use GPT? select **No** and press **Enter**

12. Partitions window appears as on the screen, select **New** option and press **Enter**



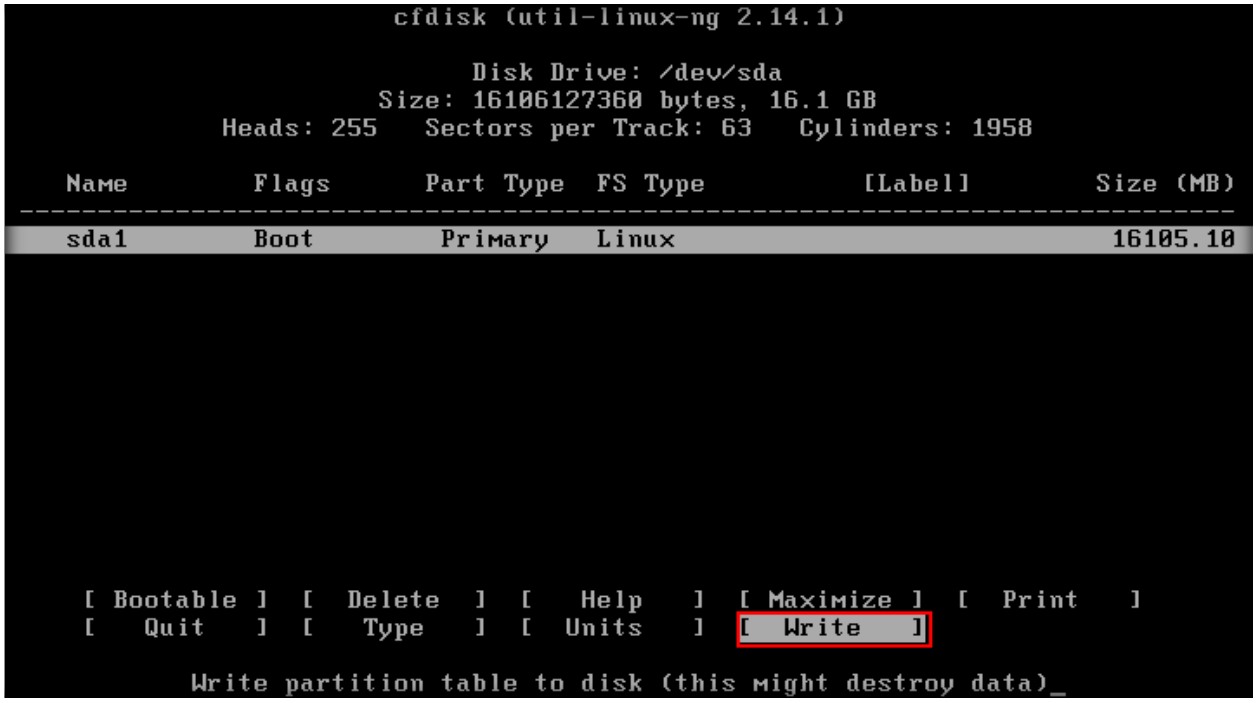
13. Select **Primary** and press **Enter**

14. Leave the Size to default and press **Enter**

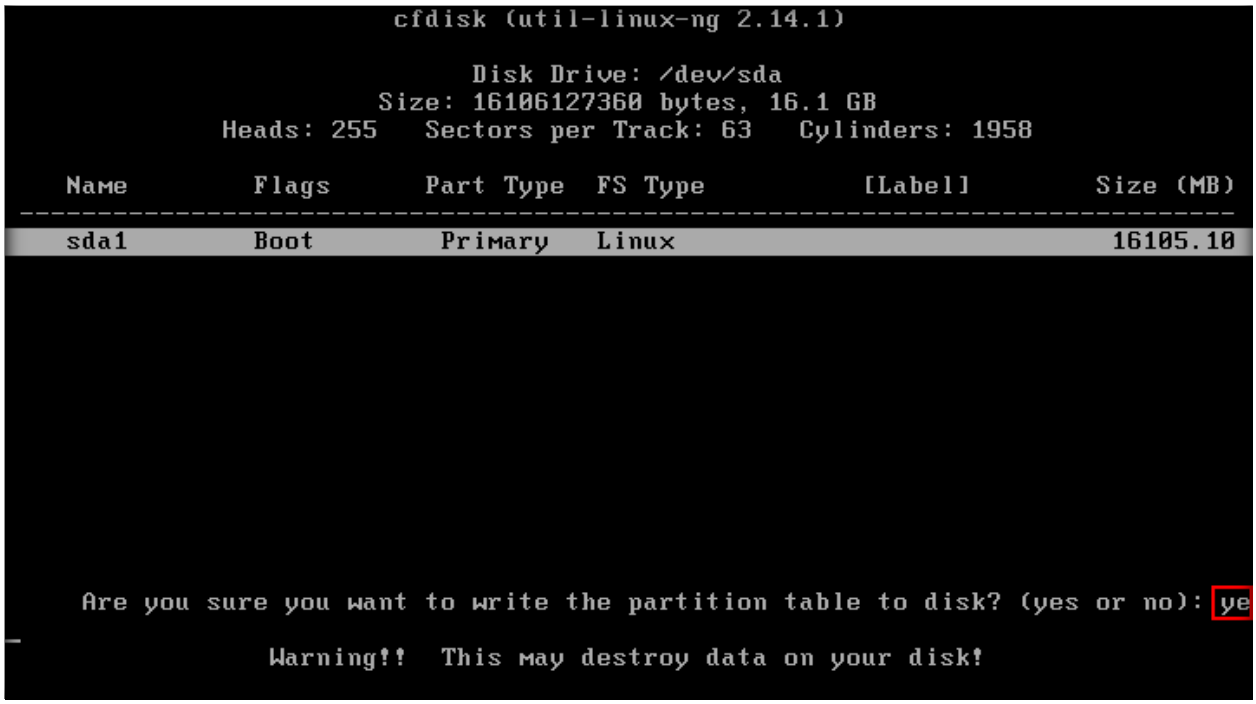


15. Select **Bootable** and press **Enter**

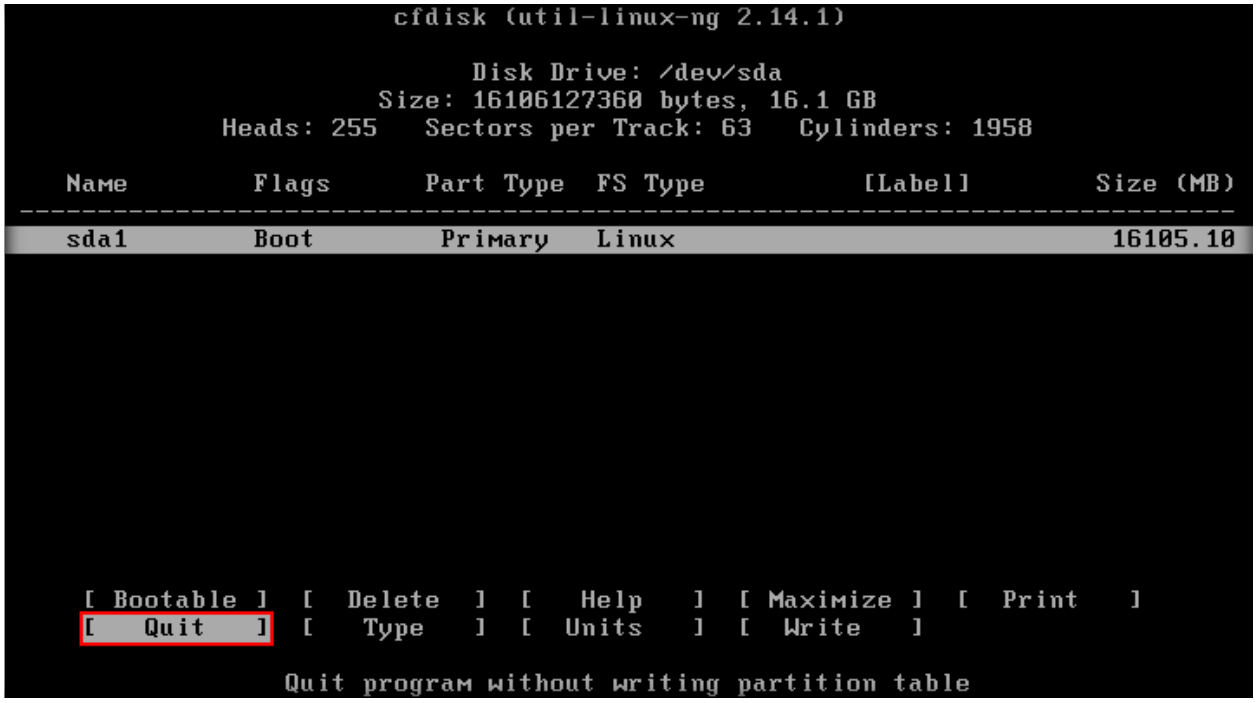
16. Select **Write** and press **Enter**



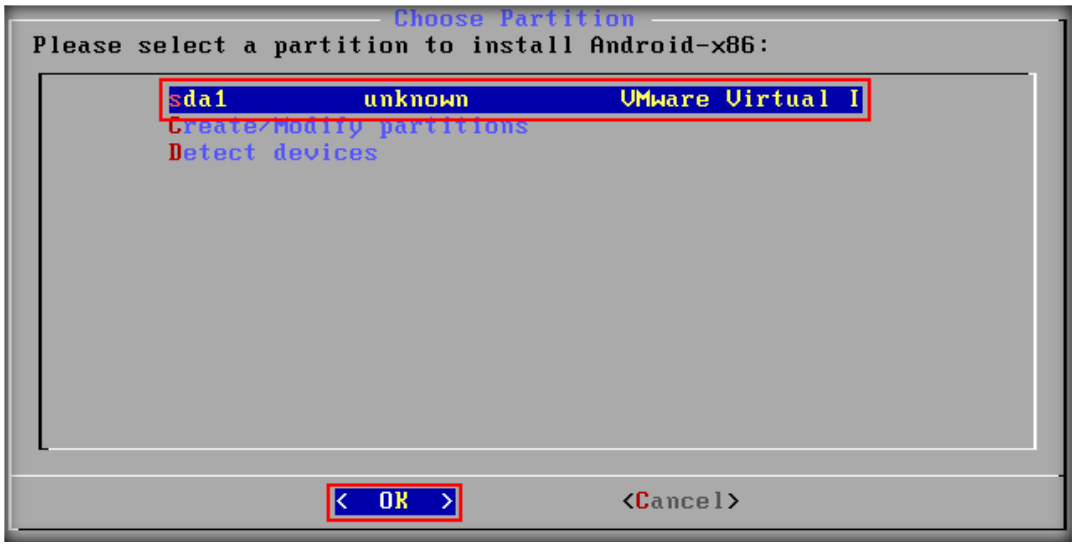
17. Type **yes** and press **Enter**



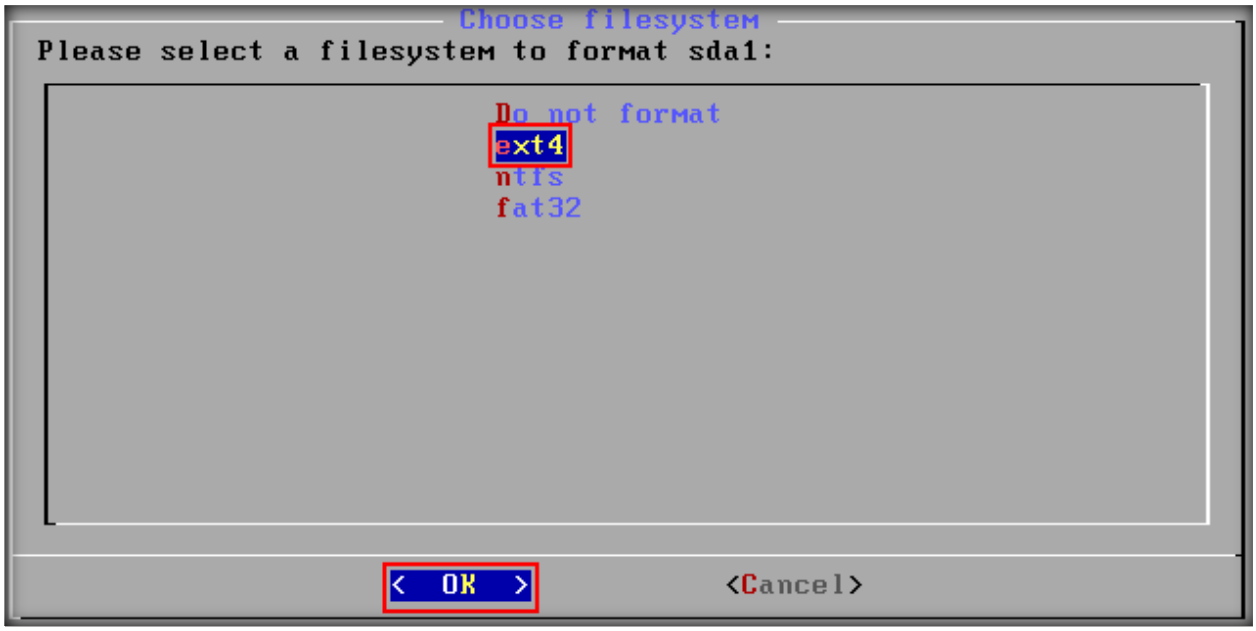
18. Select **Quit** and press **Enter**



19. **Choose Partition** window appears with the virtual hard disk (**sda1**) selected by default, select **OK** and press **Enter**

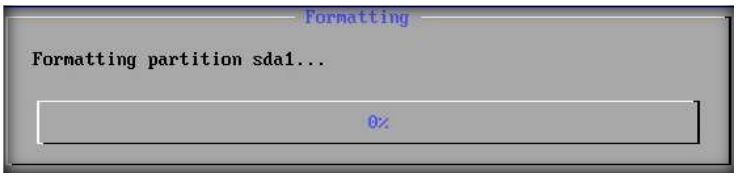


20. Choose a filesystem (here, **ext4**) and select **OK** and press **Enter**

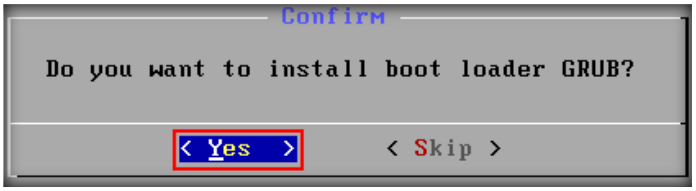


21. A **Confirm** dialog box appears, select **Yes** and press **Enter**

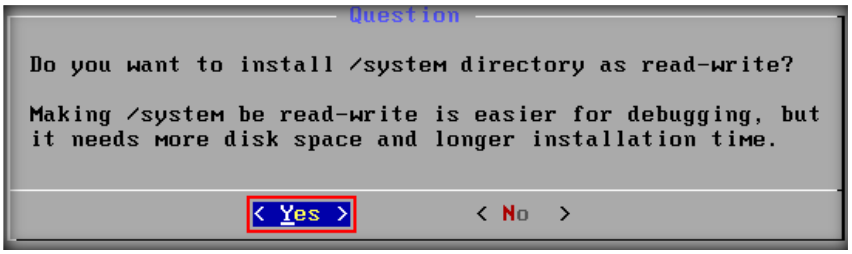
22. Partition formatting begins as shown in the screenshot



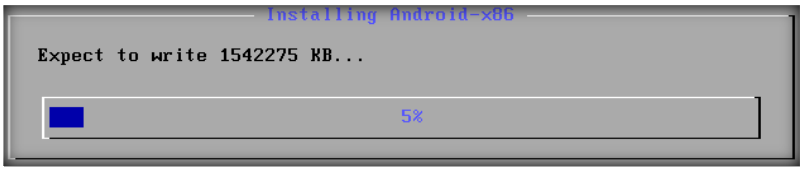
23. Once the partition is formatted, a **Confirm** dialog-box appears asking you to install boot loader **GRUB**, select **Yes** and press **Enter**



24. A **Question** dialog box appears; select **Yes** and press **Enter**

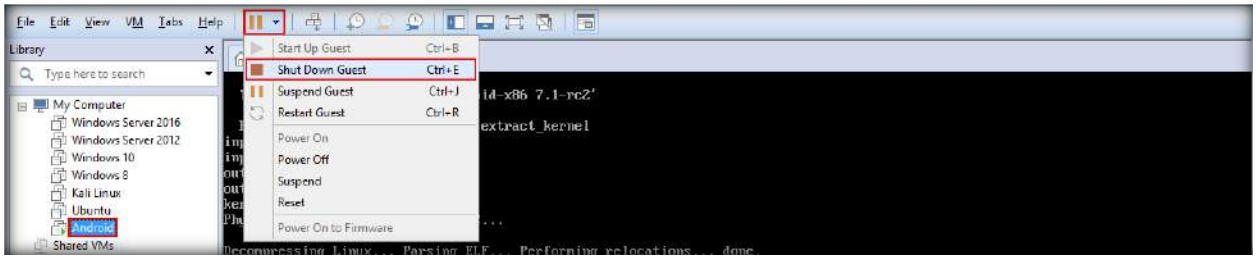


25. Android installation begins as shown in the following screenshot

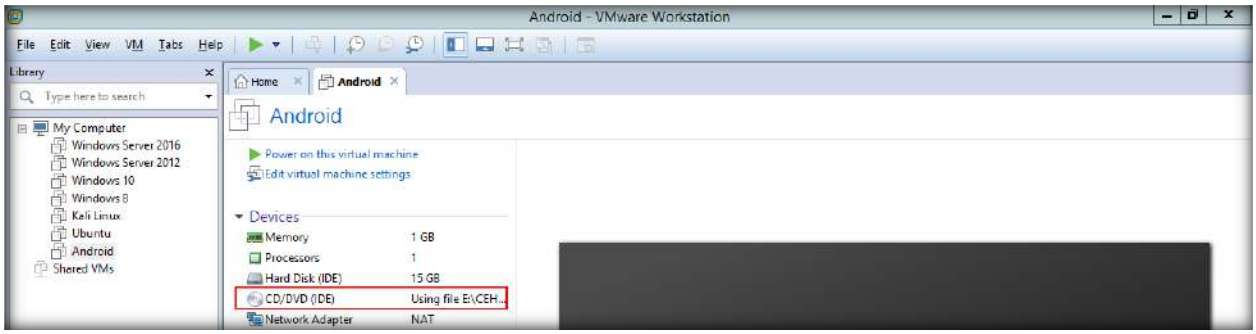


26. Once the image is created, a **Congratulations!** dialog box appears, select **Reboot** option and then select **OK** and press **Enter**

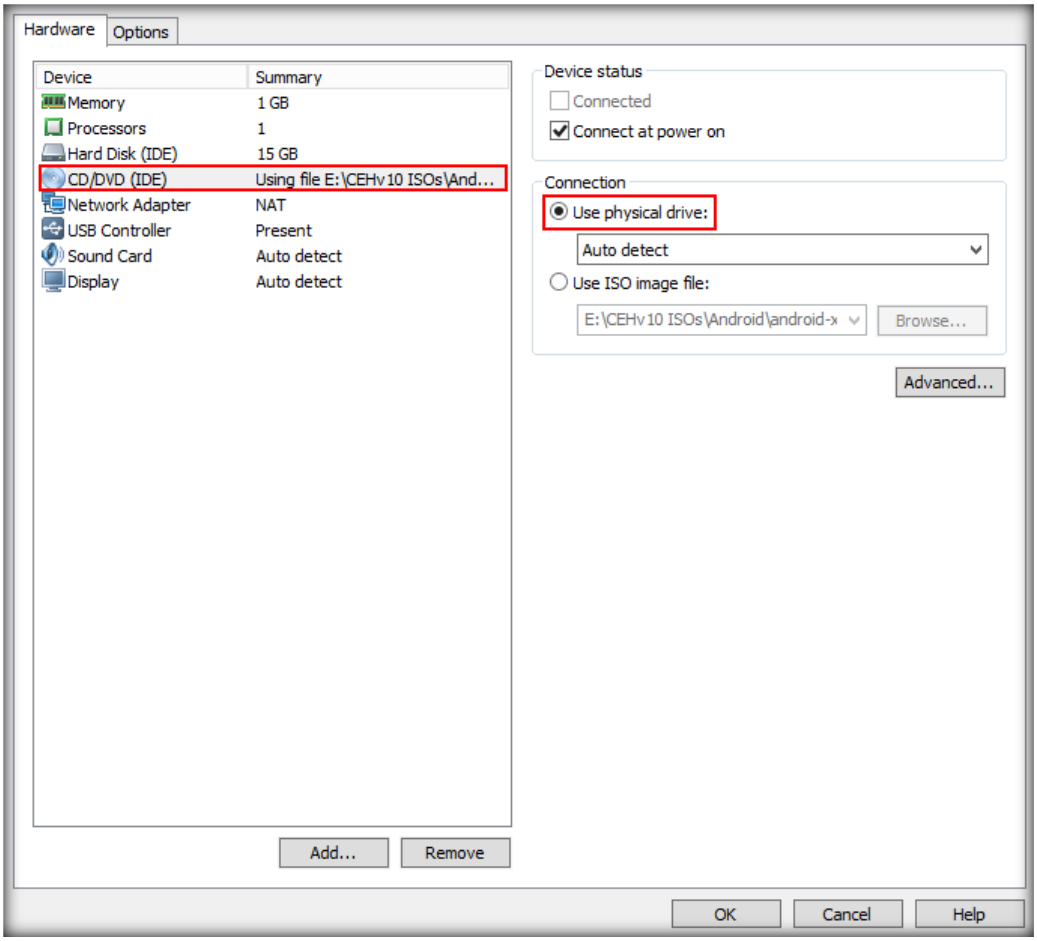
27. Once the machine is restarted, click **Shut Down Guest** as shown in the screenshot



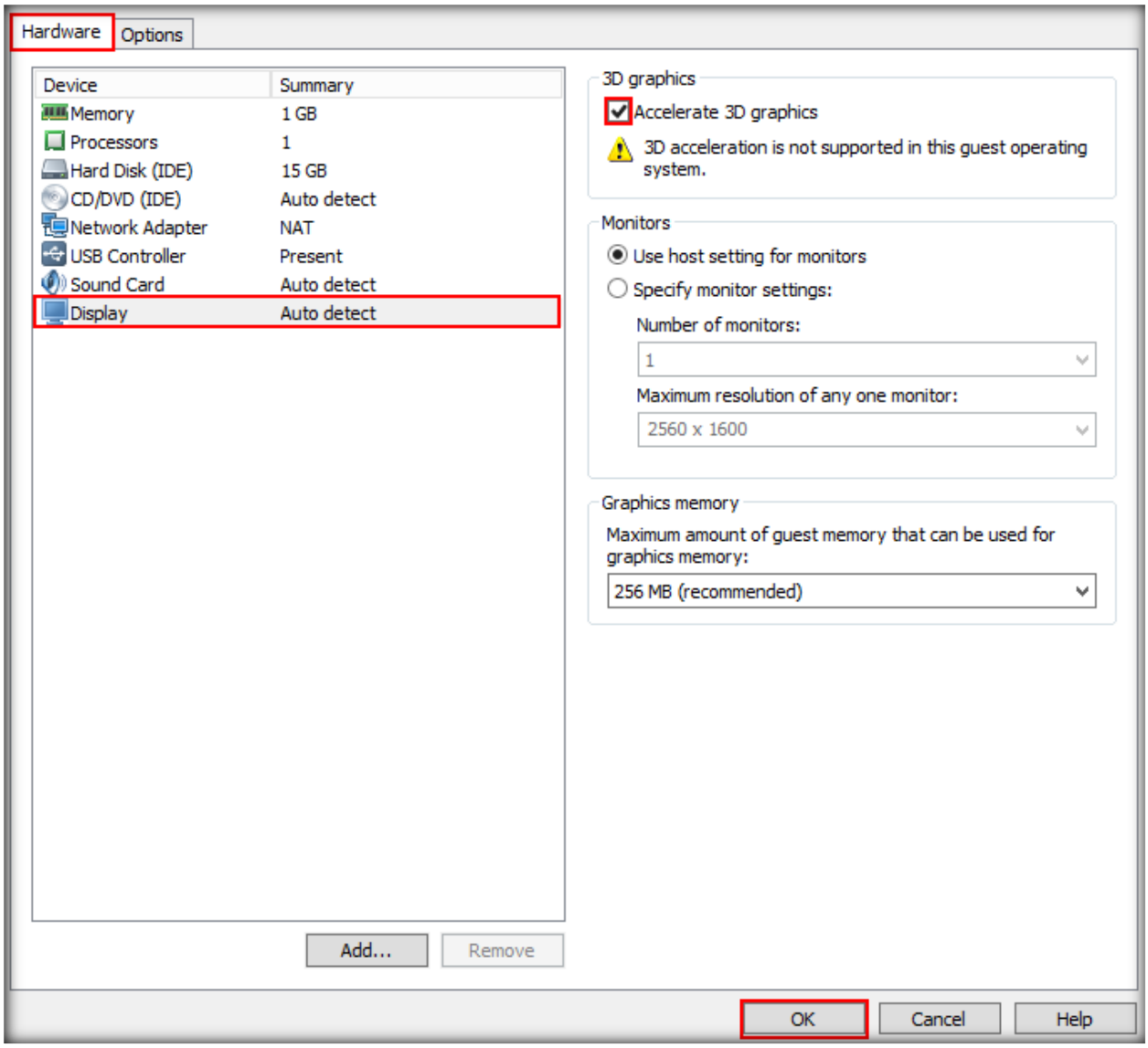
28. Once the machine is shut down, click CD/DVD (IDE) under Devices section as shown in the screenshot



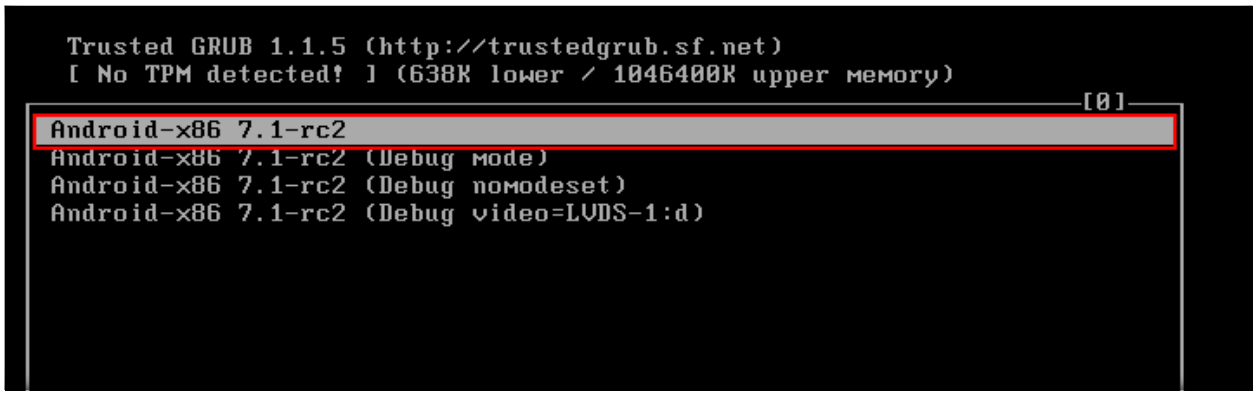
29. Virtual Machine Settings window appears, choose **Use physical drive** radio button and then click **Display** option in the left pane



30. Display options appears, check **Accelerate 3D graphics** check box, and then click **OK**



31. Android boot menu appears, leave the window intact
32. Wait until android machine gets booted

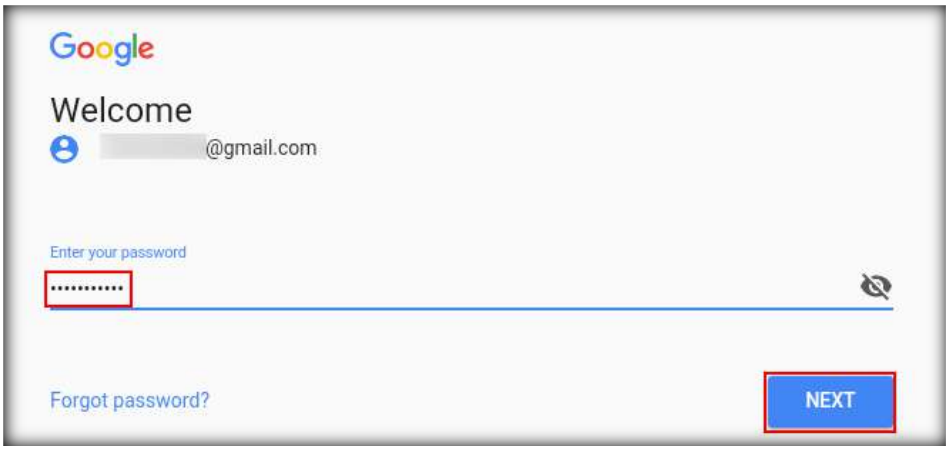


33. Welcome screen appears, click **LET'S GO**

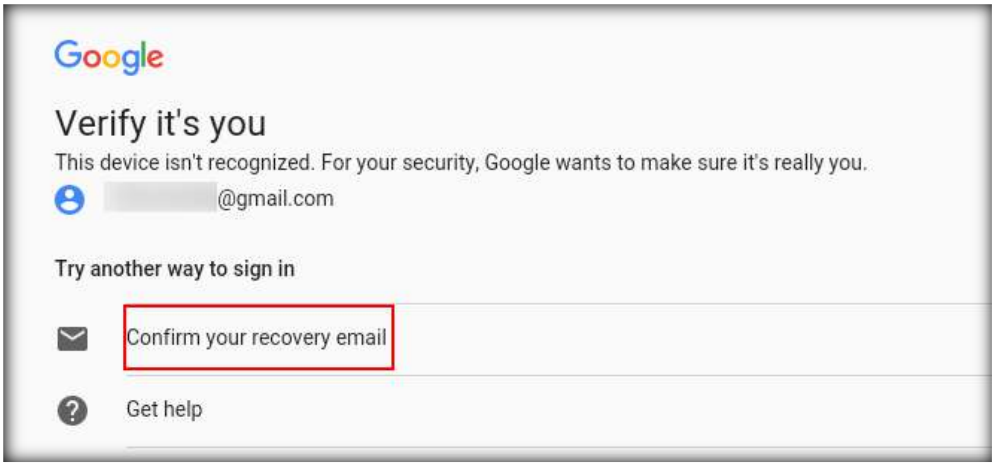
34. Welcome to your VMware Virtual Platform screen appears, click **Set up as new**
Note: If Google Play services has stopped pop-up appears, click **Close app**

35. Google Sign in page appears, provide the working email ID to sign in and click **Next**
Note: If you donot have an email account Create a new account by clicking Create account link

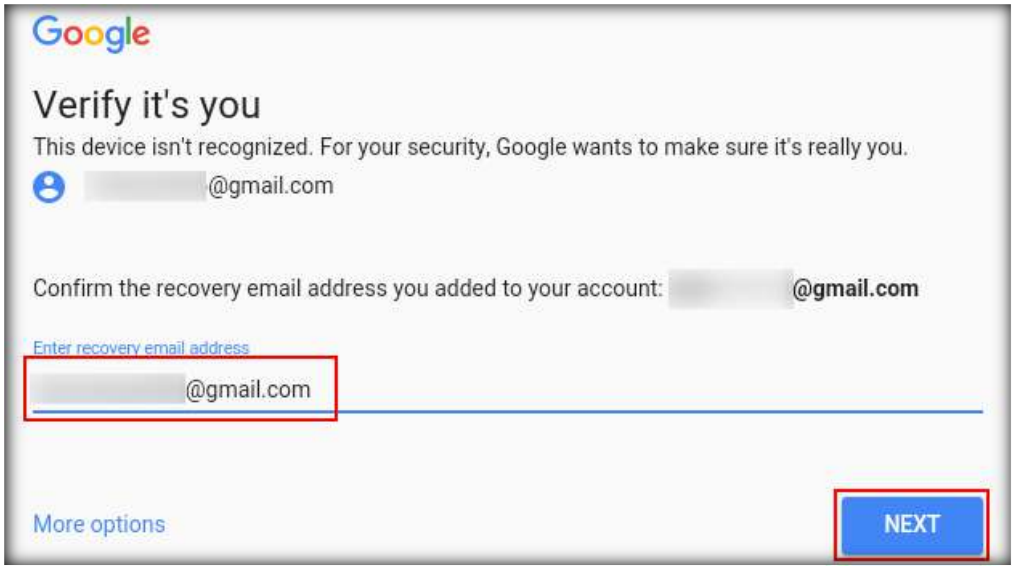
36. Type in your email account password and click **Next**



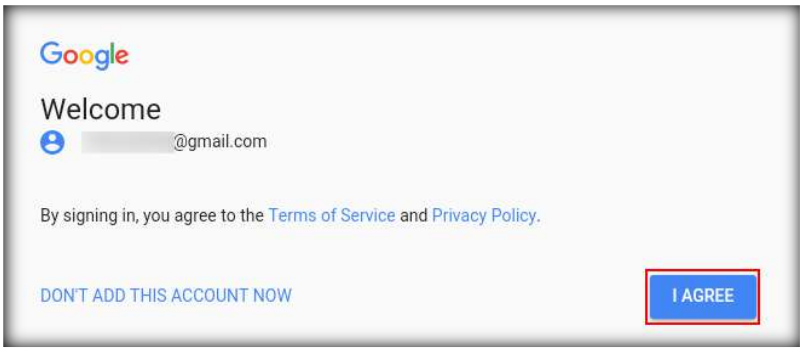
37. If Verify it's you screen appears, click **Confirm your recovery email**



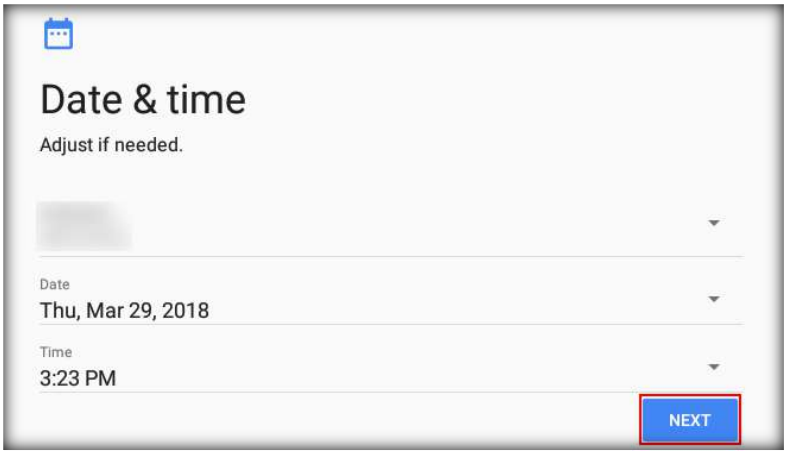
38. Confirm your recovery email address screen appears, type the recovery email address that you have assigned at the time of creating the email ID, and then click **Next**



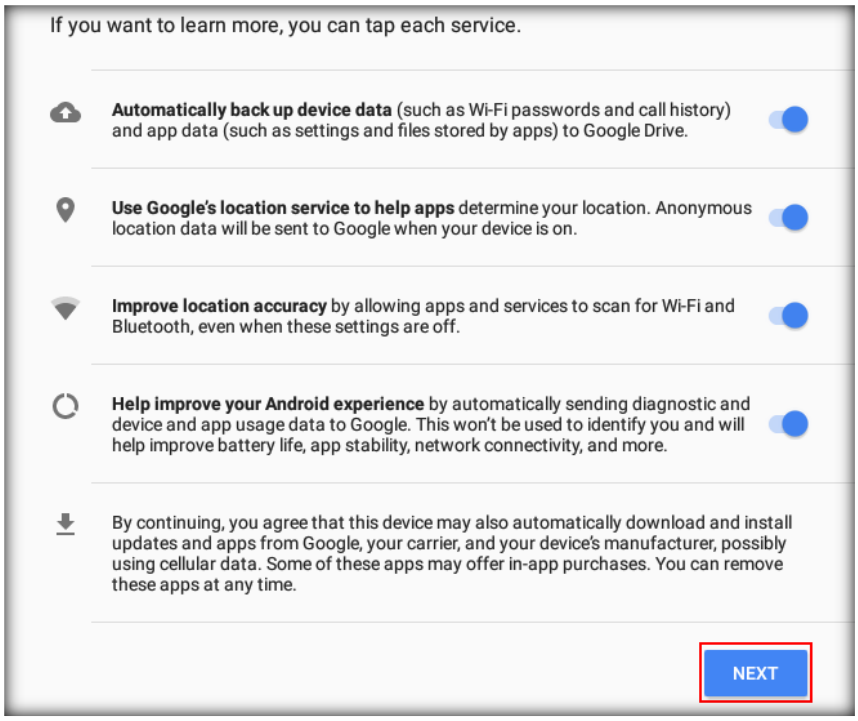
39. Welcome screen appears, click **I AGREE**. Wait until the configuration is completed



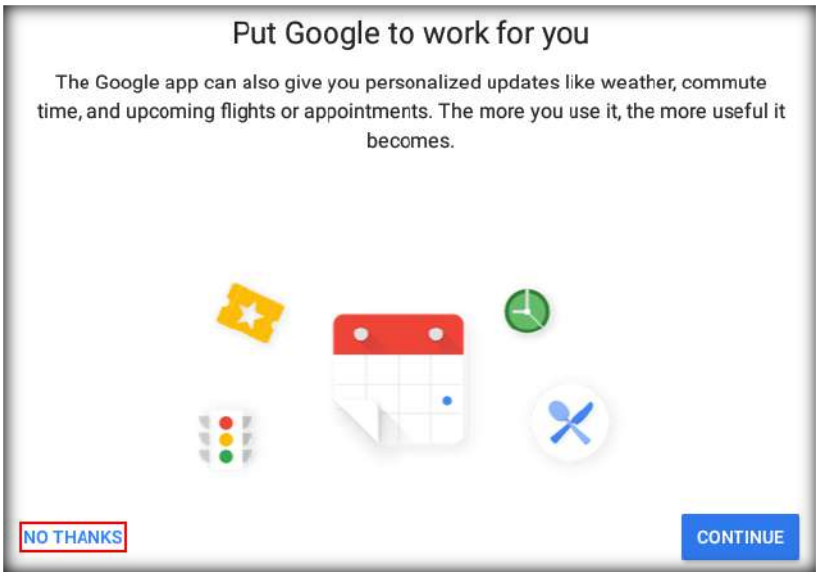
40. Date & time screen appears, leave the settings to default and click **Next**



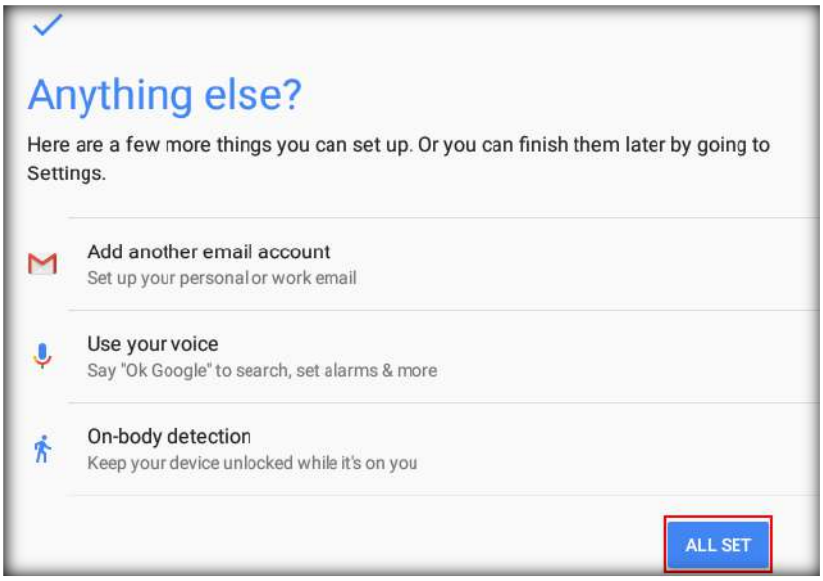
41. In Google Services screen, leave the settings to default, scroll down and click **Next**



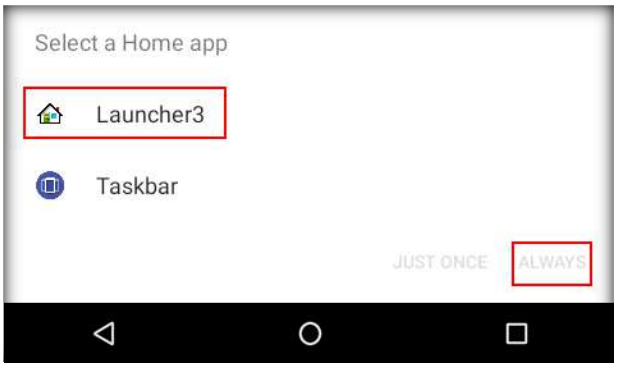
42. Put Google to work for you screen appears, click **NO THANKS**



43. Anything else? screen appears, click **ALL SET** to continue

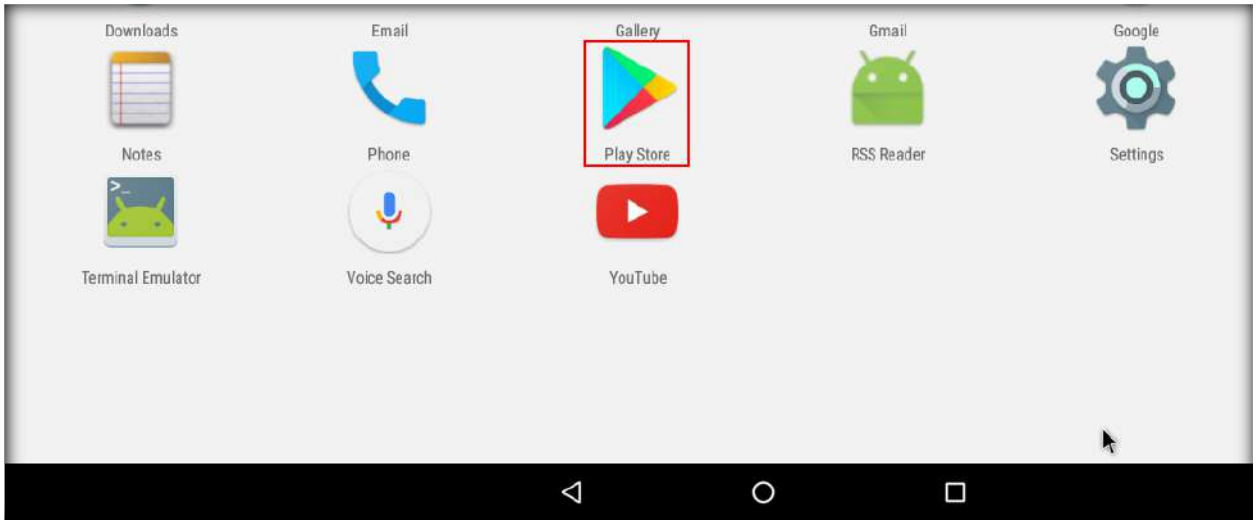


44. Select a Home app pop-up appears, click **Launcher3** and click **ALWAYS** as shown in the screenshot

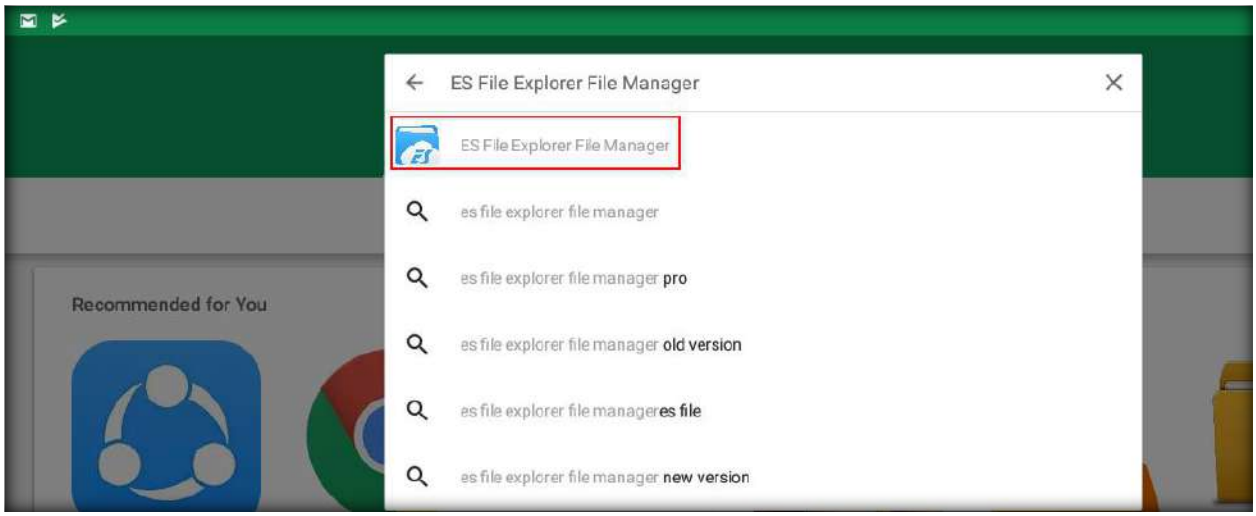


45. Thus, you have successfully installed Android machine as shown in the screenshot. Click **app drawer** icon (^) to view menu

46. Click **Play Store** icon in the menu

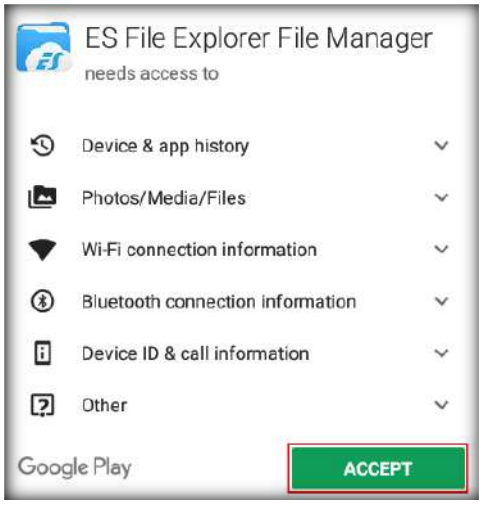


47. Type **es file explorer** in the search bar of Play Stor. **ES File Explorer File Manager** application appears in the search result. Click on it



48. Click **INSTALL** button to begin the application installation

49. **ES File Explorer File Manager** pop-up appears, click **ACCEPT**

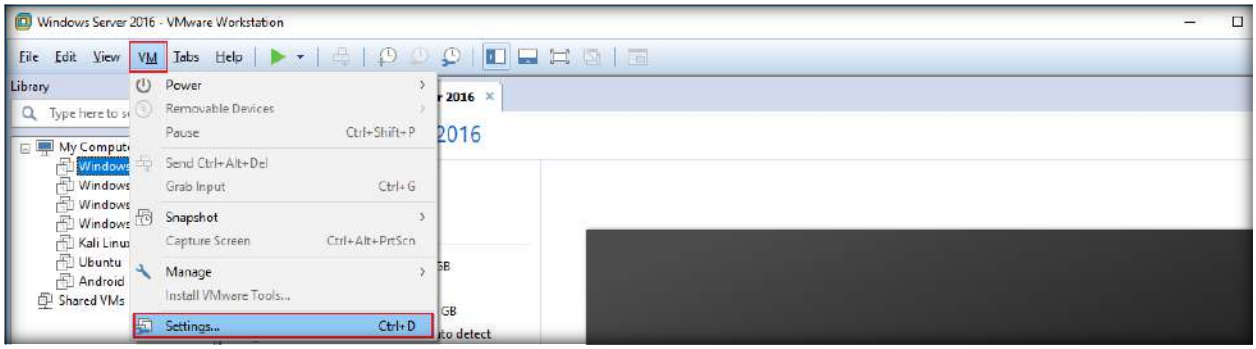


50. Wait for the application to install. On completing the installation close all the applications

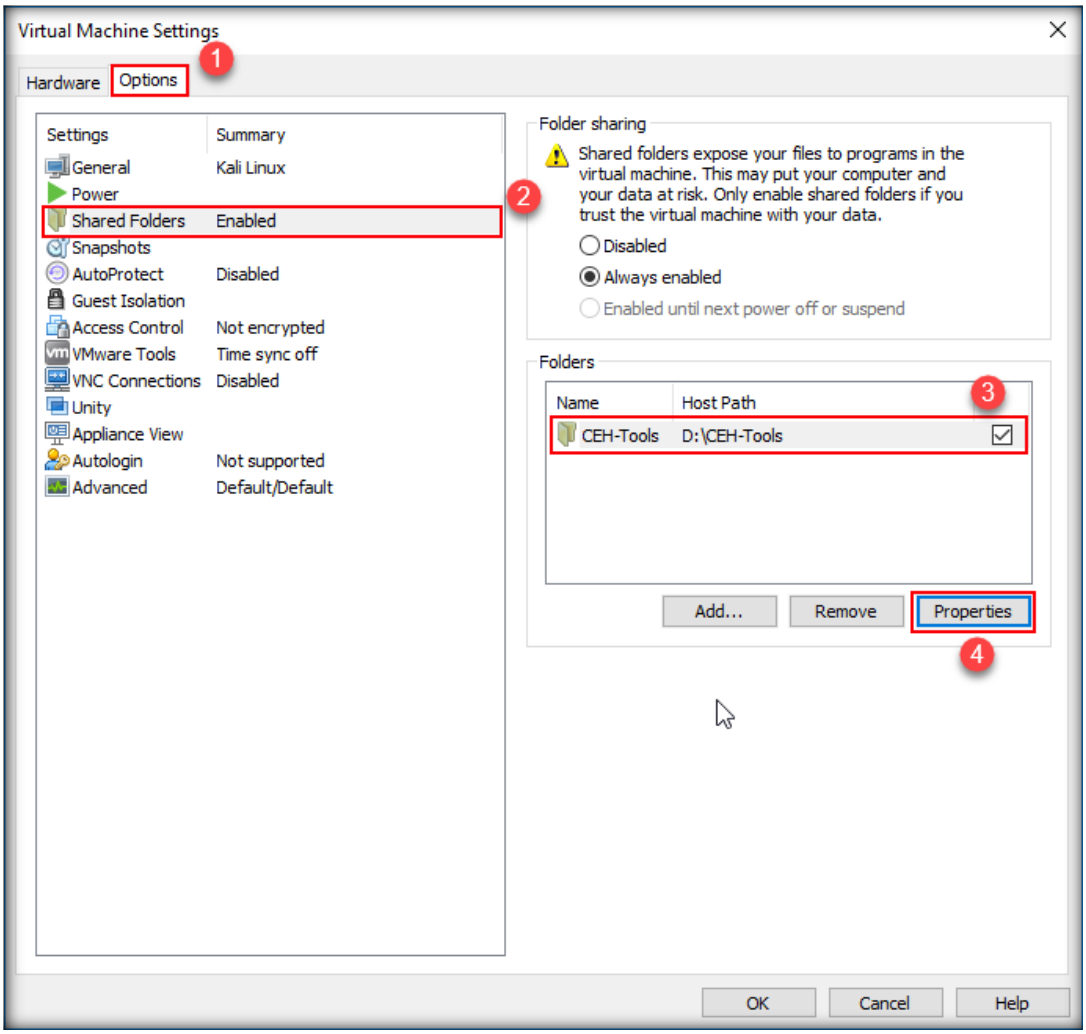
[Back to Configuration Task Outline]

CT#10: Share CEH-Tools Folder to Windows VMs

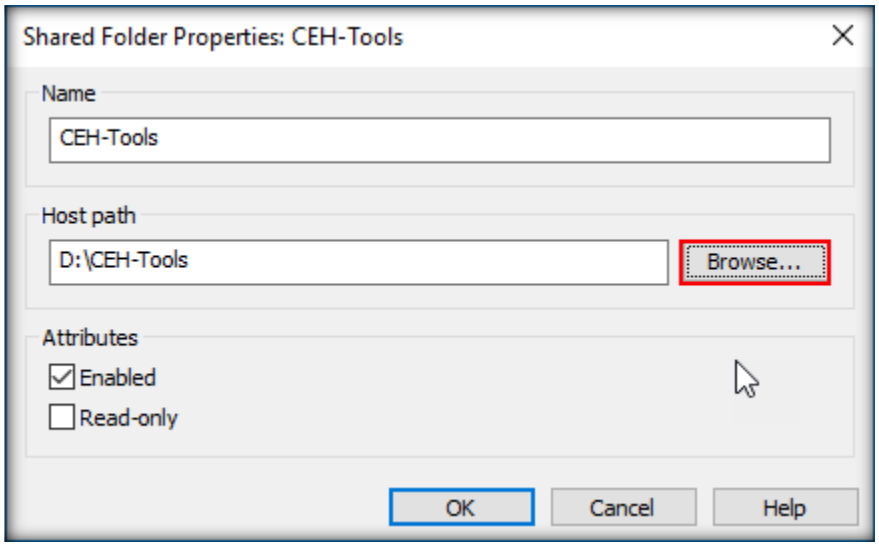
1. Make sure that all the Virtual Machines are turned off
2. Select any Windows VM (here, Windows Server 2016) from the left pane, and go to **VM** and click **Settings**



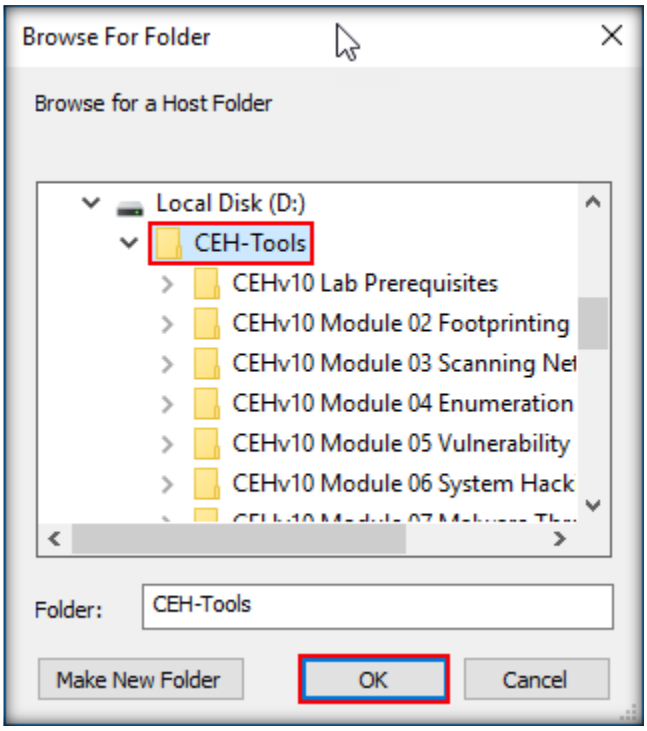
3. Go to **Options** tab in the Virtual Machine Settings window. Select **Shared Folders** from the left pane, select **Always enabled** radio button, choose the **CEH-Tools** folder and click **Properties**



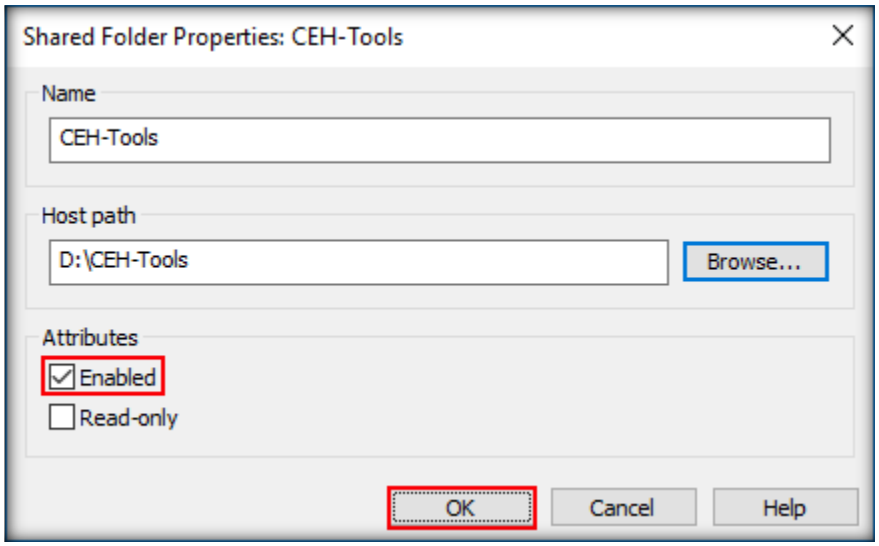
4. Shared Folder Properties window appears, click **Browse**



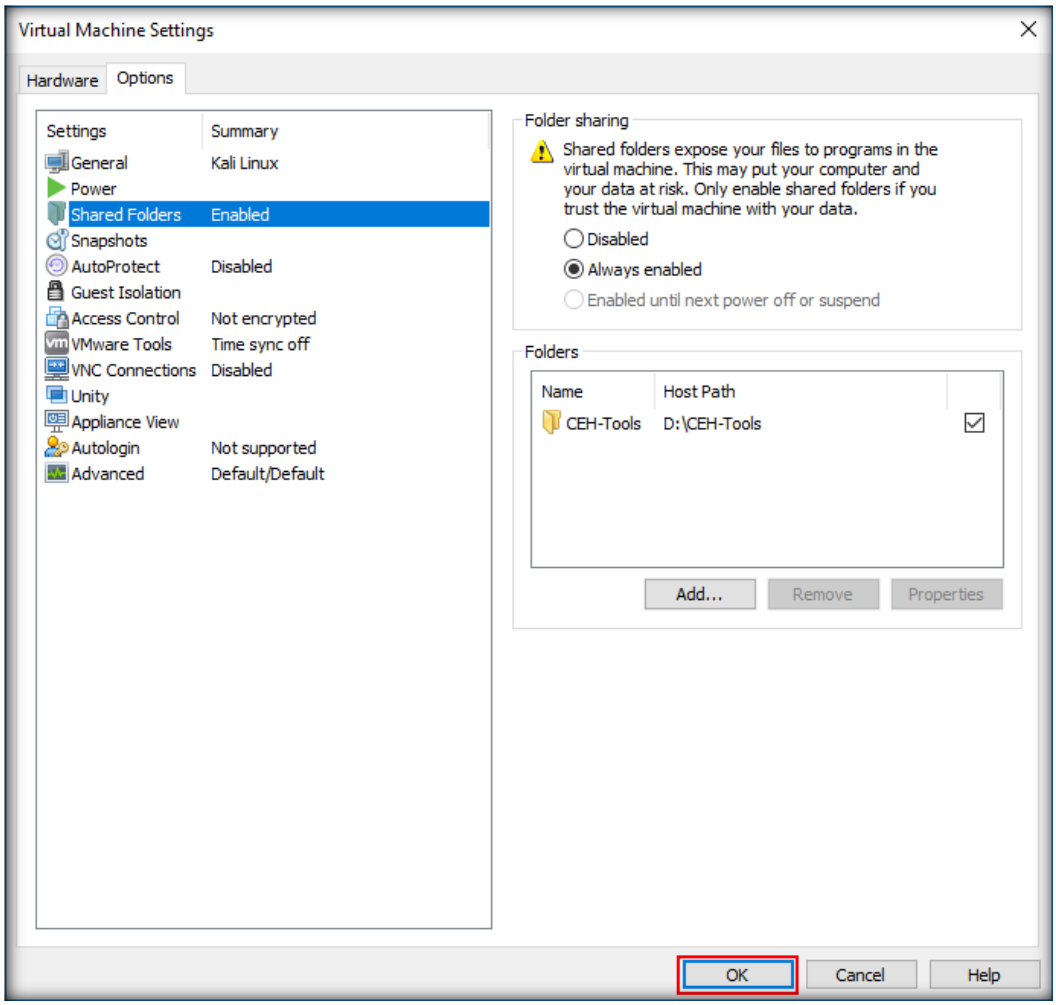
5. Browse to the **CEH-Tools** directory in your host system and click **OK**



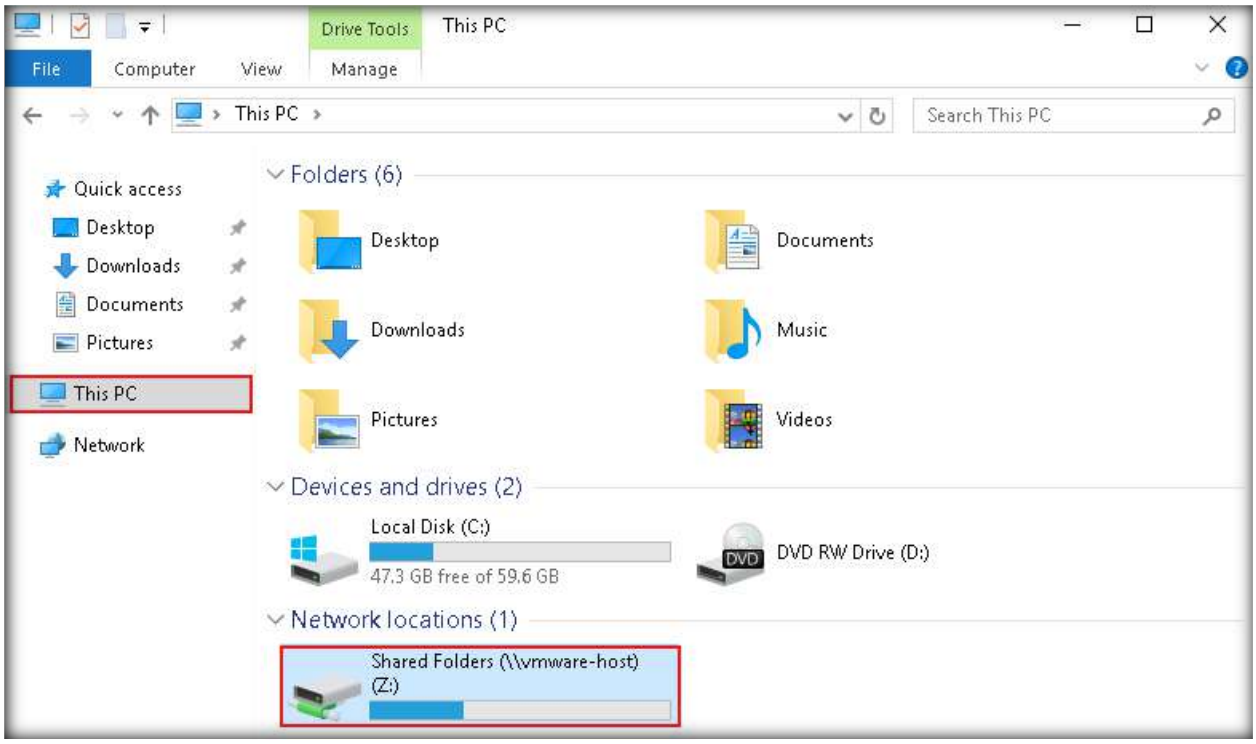
6. Make sure that the **Enabled** checkbox is selected and click **OK**



7. Shared folder will be added as shown below: click **OK** to close the Virtual Machine Settings window



8. Now, login to the Windows Server 2016 virtual machine **close** the Server Manager window if appears, you will see the **Shared Folder** attached in the Windows Explorer



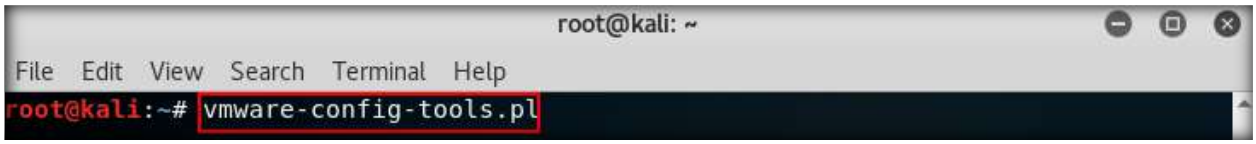
9. Repeat the above steps with Windows Server 2012, Windows 10 and Windows 8 virtual machines

[Back to Configuration Task Outline]

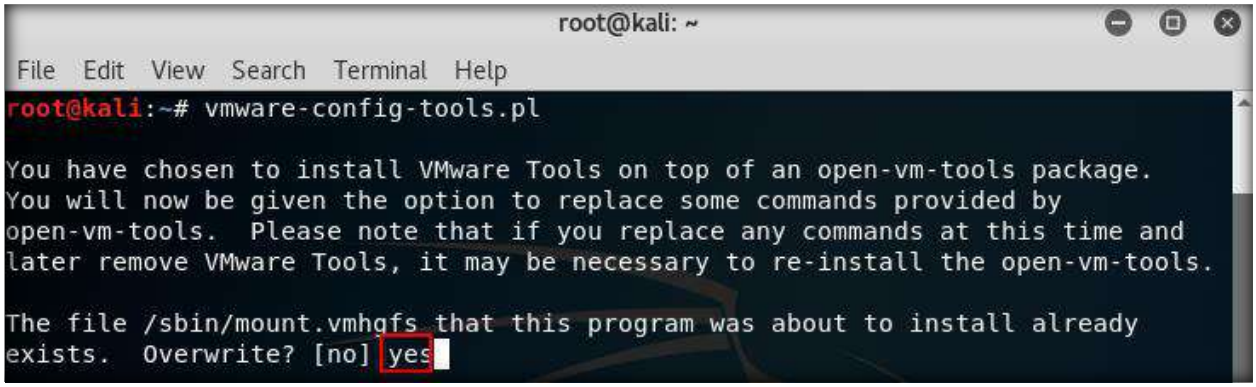
CT#11: Mapping CEH-Tools with Kali Linux Machine

1. Follow the steps of CT#10 from 1 to 7
2. Now, Login to Kali Linux machine
3. Launch Terminal window and type **vmware-hgfsclient** and press **Enter**. This will show you the shared folder list of your host machine

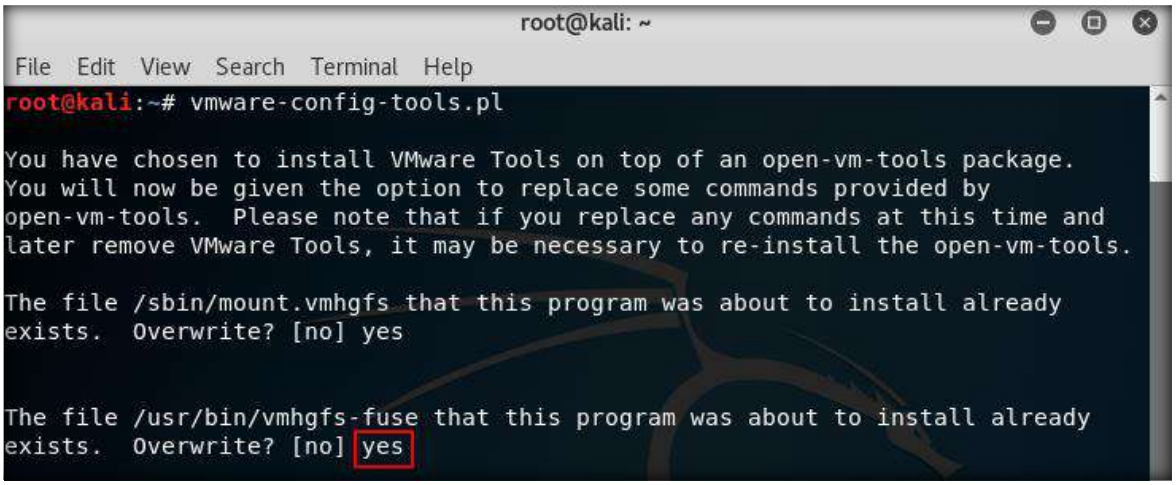
4. Now, type **vmware-config-tools.pl** and press **Enter**, type **toor** as the password and press **Enter**



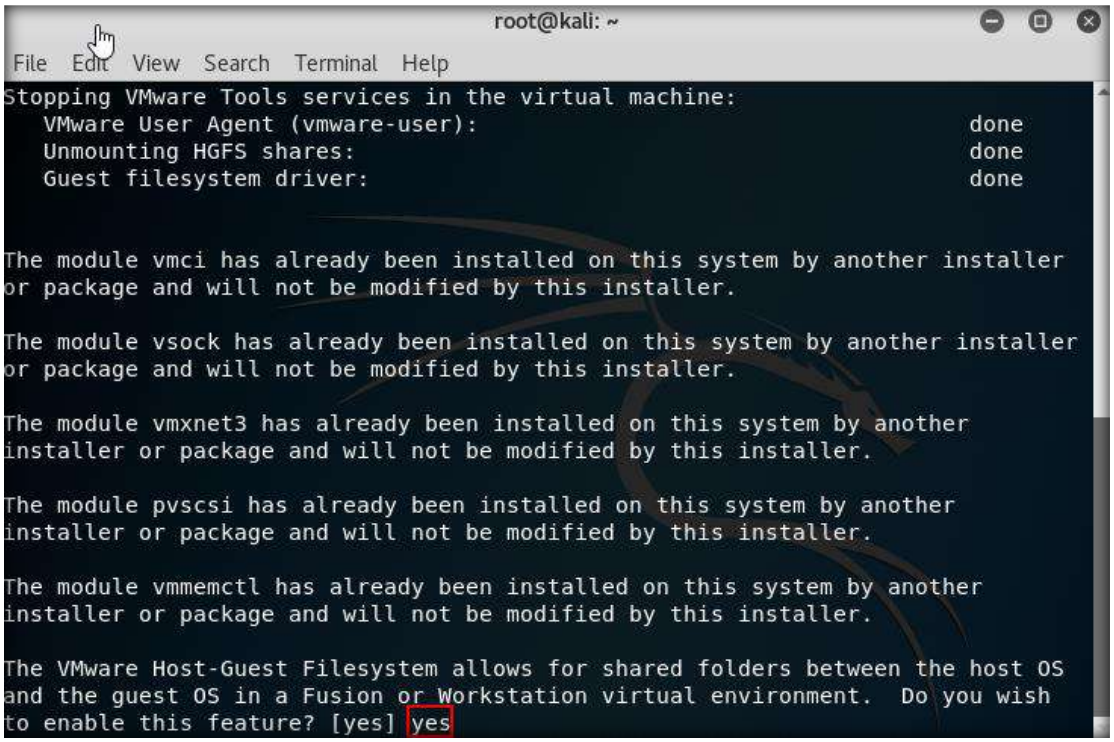
5. The file already exists warning appears, type **Yes** and press **Enter**



6. The fuse program already exists warning appears, type **Yes** and press **Enter**

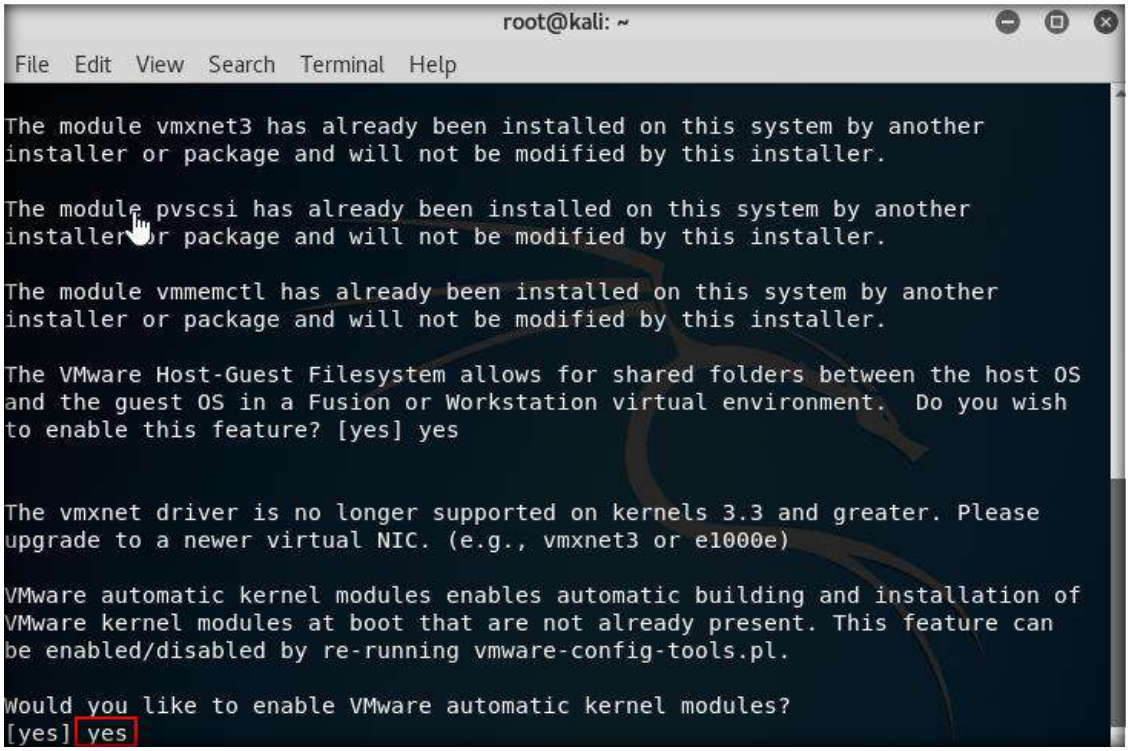


7. The VMware Host-Guest Filesystem allows for shared folders between the host OS and the guest OS in Fusion or Workstation virtual environment appears, type **Yes** and press **Enter**

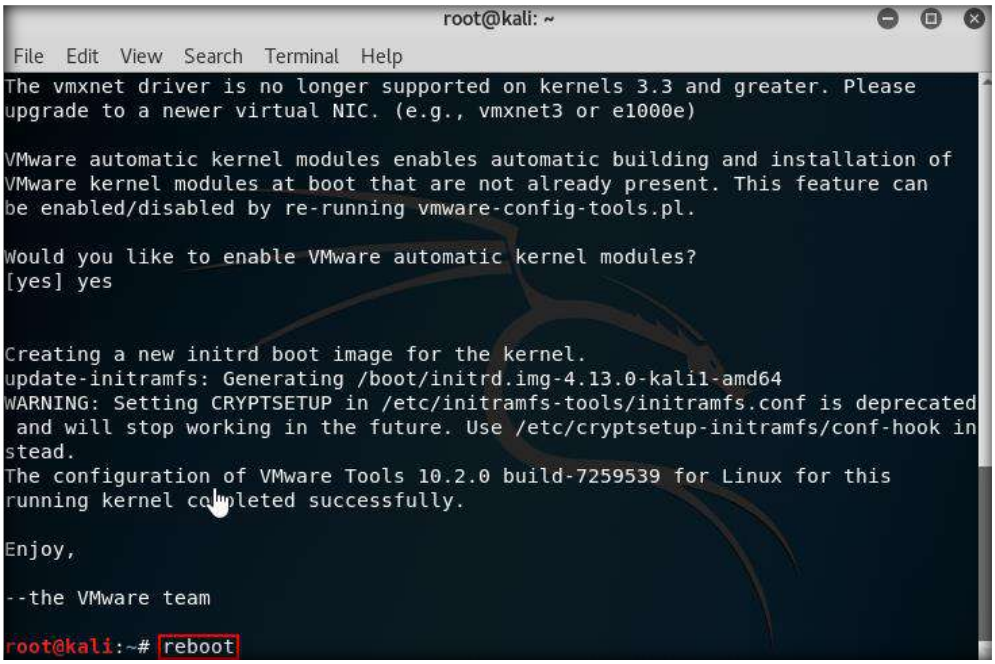


8. If the vmblock enables dragging or copying files between host and guest in a Fusion or Workstation virtual environment appears, type **Yes** and press **Enter**

9. Type **Yes** and press **Enter** in Would you like to enable VMware automatic kernel modules?



10. If the Thinprint provides driver-free printing warning appears, type **Yes** and press **Enter**
11. If Do you want enable Guest Authentication (vgauth) warning appears, type **Yes** and press **Enter**
12. If Do you want to enable Common Agent (caf) warning appears, type **Yes** and press **Enter**
13. Now, the installation was successful, type **reboot** and press **Enter** to restart the Kali Linux machine



14. Login to the Kali Linux machine
15. Now, we need to mount the shared directory, open a terminal window and type **ln –s /mnt/hgfs/CEH-Tools ~/Desktop/CEH-Tools** press **Enter**
16. This will mount the shared directory on the Desktop

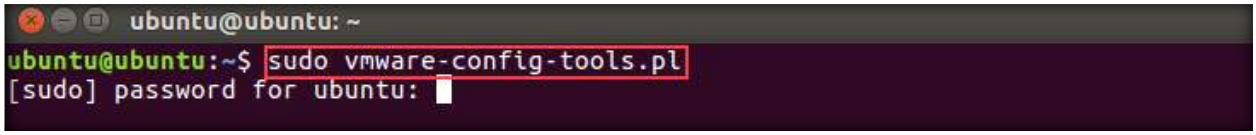
17. Shared CEH-Tools directory

[Back to Configuration Task Outline]

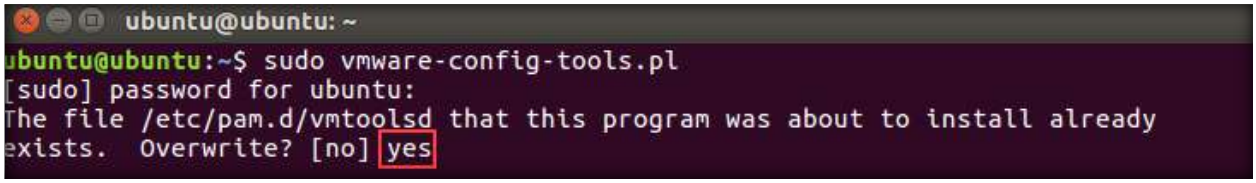
CT#12: Mapping CEH-Tools with Ubuntu Machine

1. Follow the steps of CT#10 from 1 to 7
2. Now, Login to Ubuntu machine
3. Launch Terminal window and type **vmware-hgfsclient** and press **Enter**. This will show you the shared folder list of your host machine

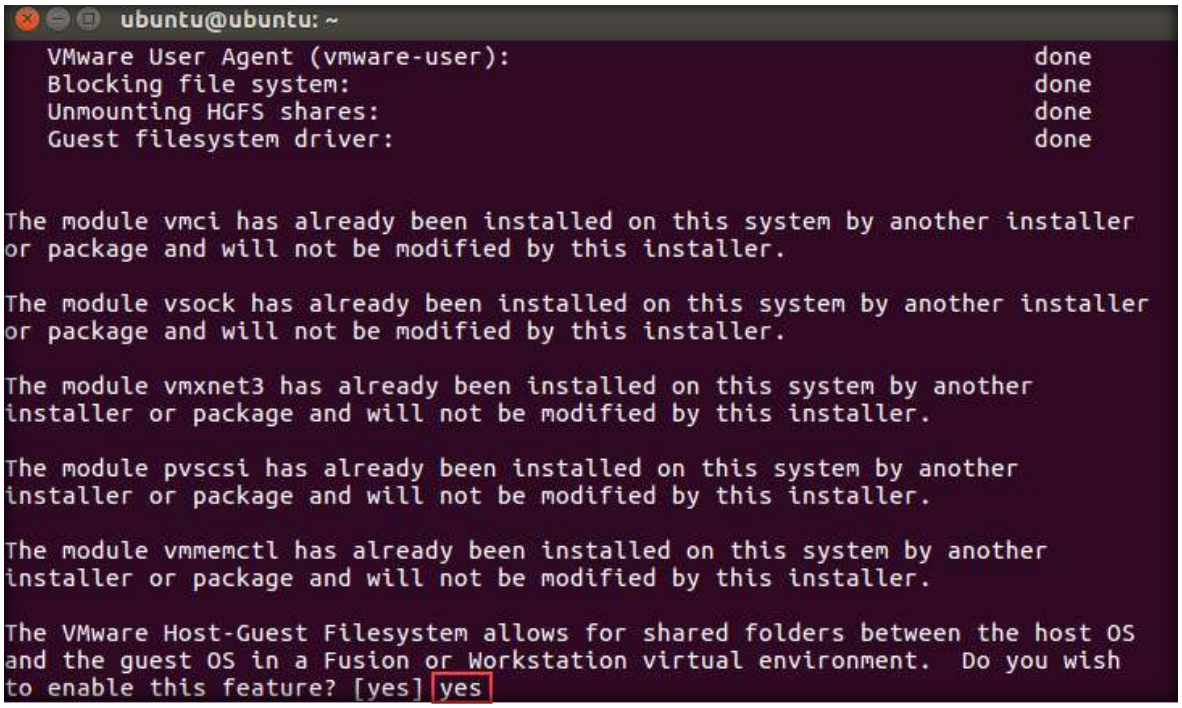
4. Now, type **sudo vmware-config-tools.pl** and press **Enter**, type **toor** as the password and press **Enter**



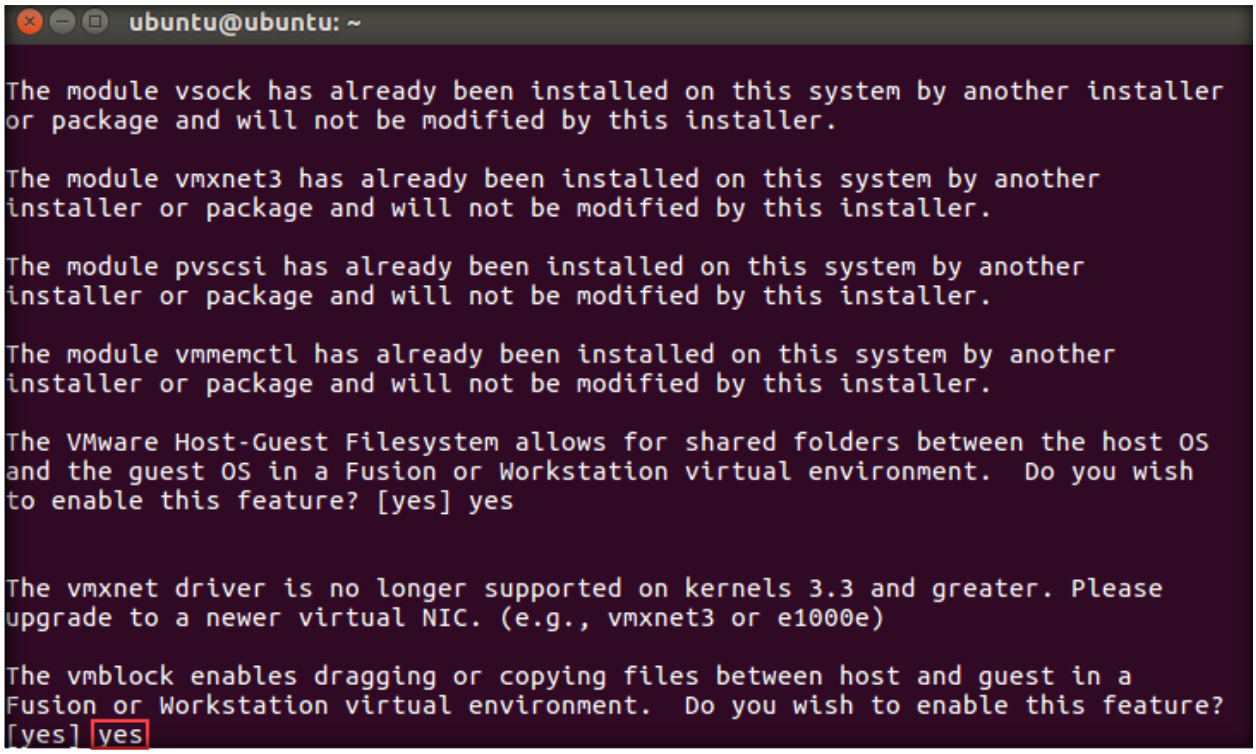
5. The file already exists warning appears, type **Yes** and press **Enter**



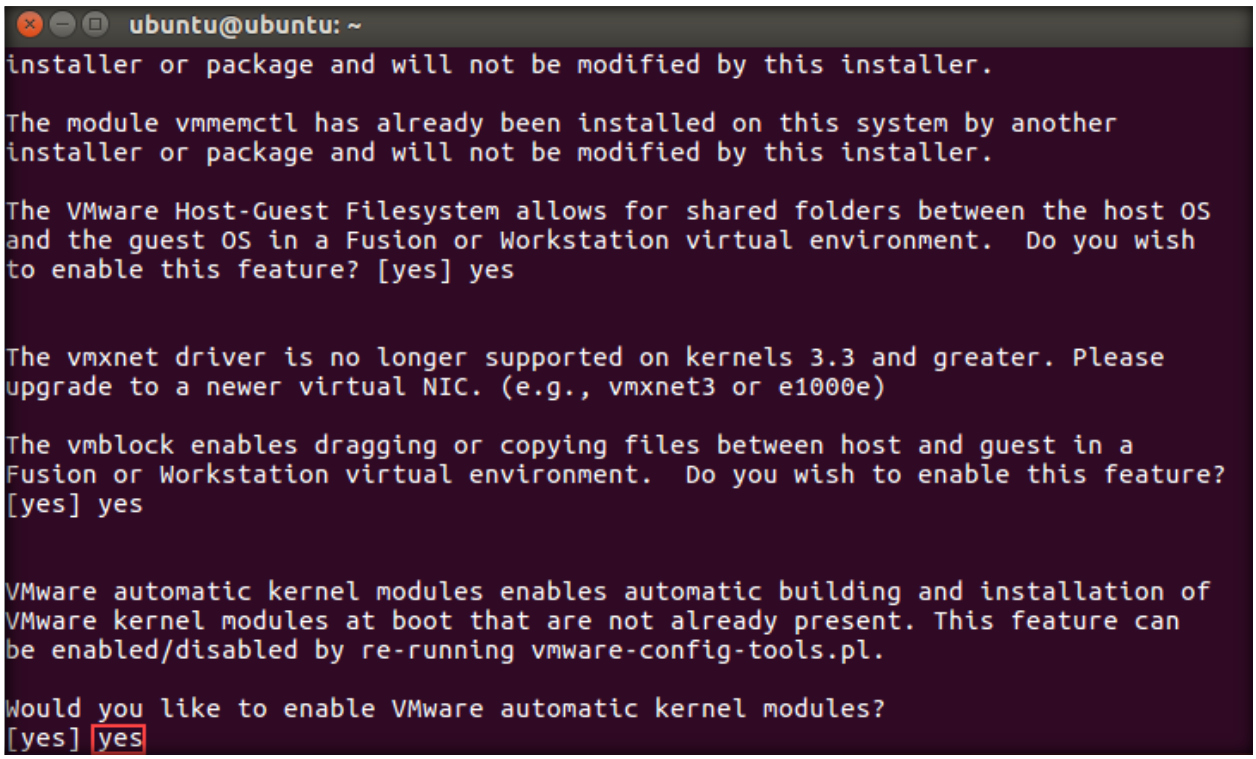
6. The VMware Host-Guest Filesystem allows for shared folders between the host OS and the guest OS in Fusion or Workstation virtual environment appears, type **Yes** and press **Enter**



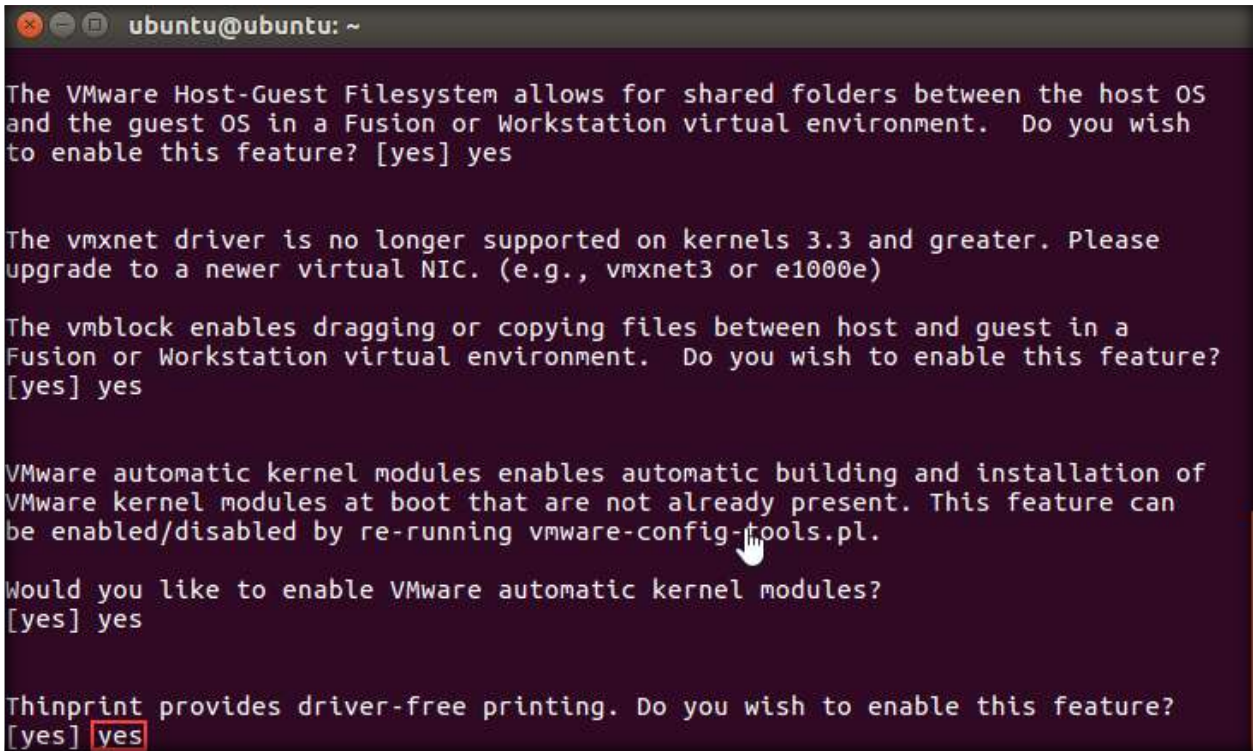
7. The vmblock enables dragging or copying files between host and guest in a Fusion or Workstation virtual environment appears, type **Yes** and press **Enter**



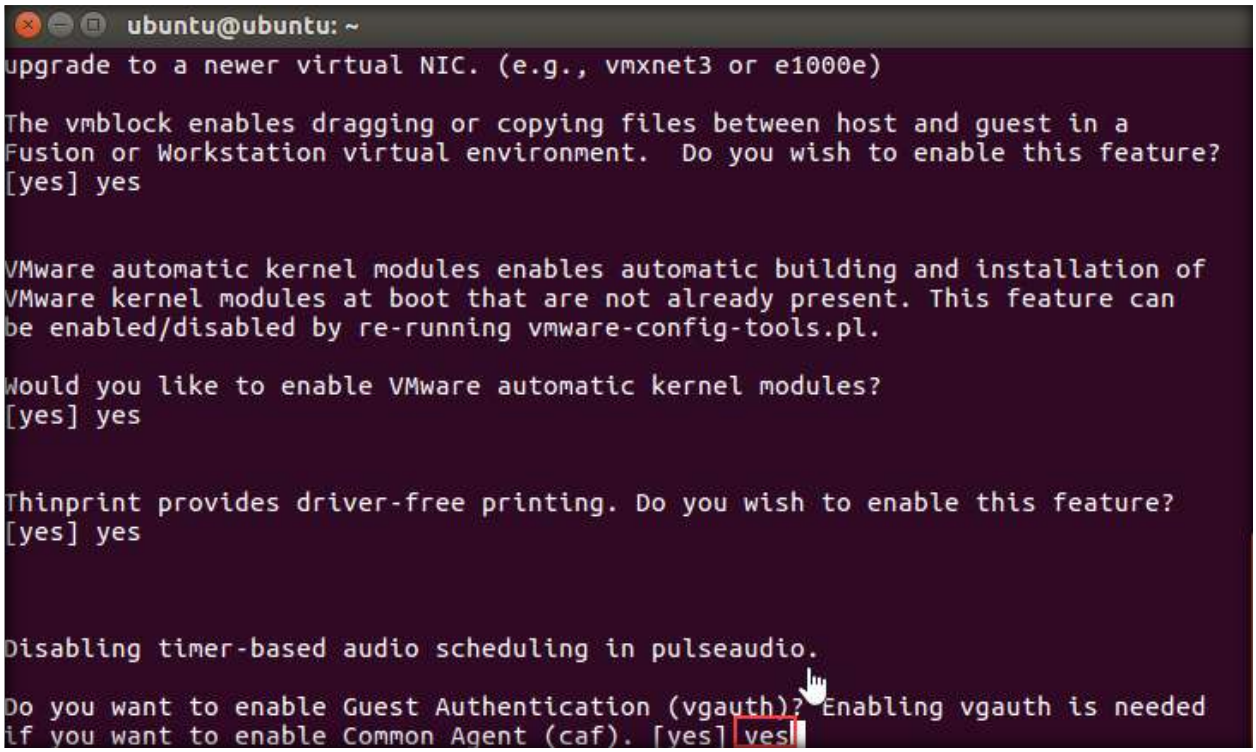
8. Type **Yes** and press **Enter** in Would you like to enable VMware automatic kernel modules?



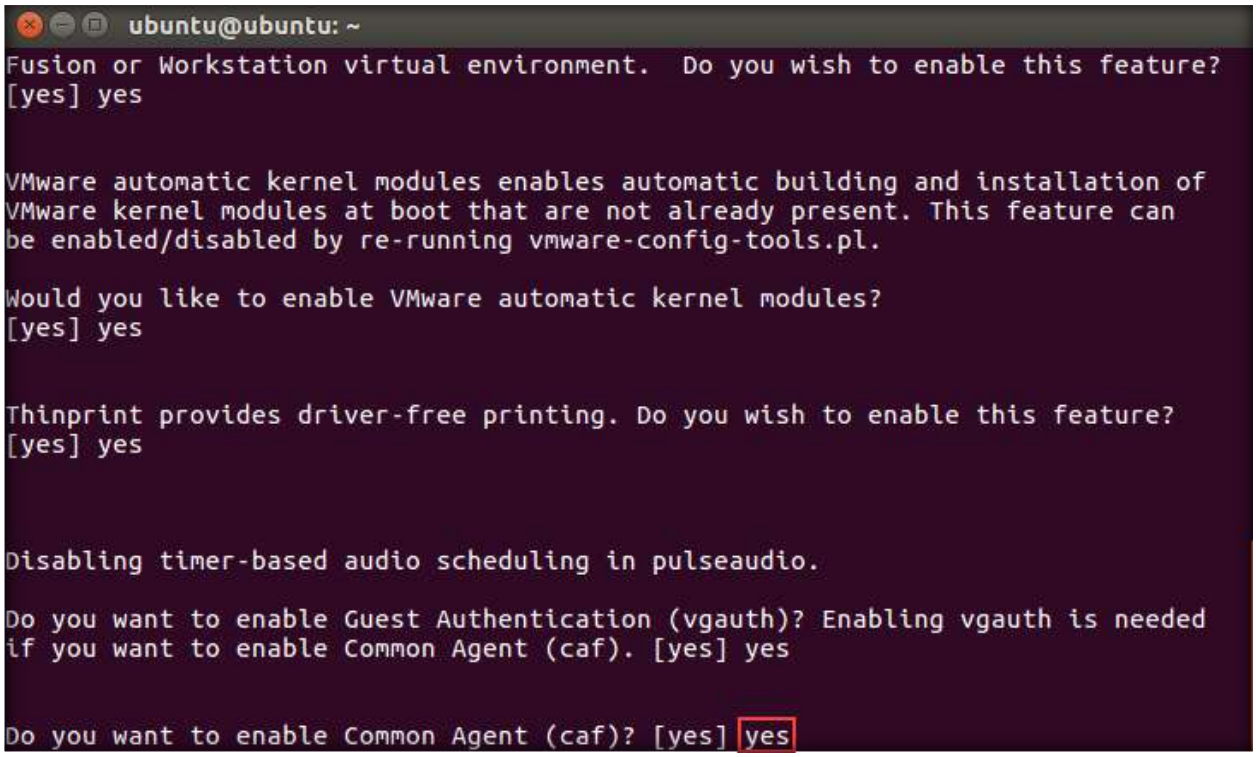
9. Thinprint provides driver-free printing warning appears, type **Yes** and press **Enter**



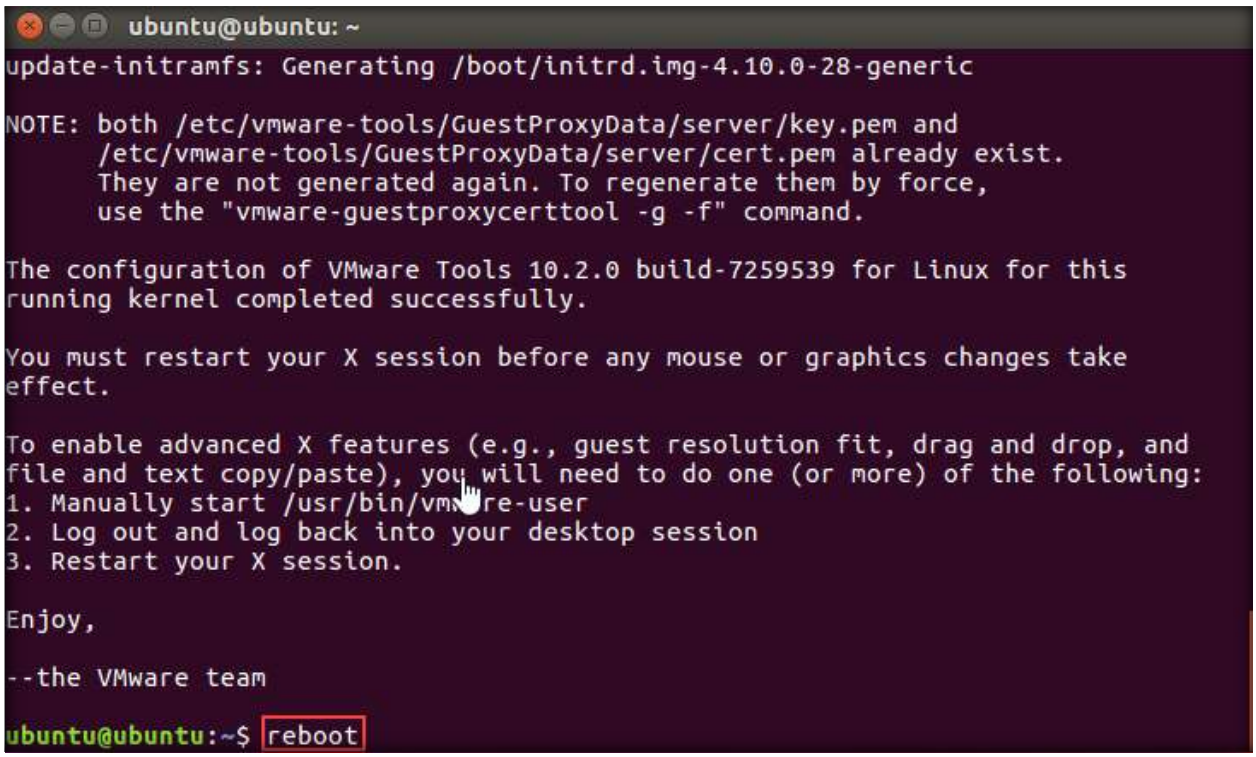
10. Do you want enable Guest Authentication (vgauth) warning appears, type Yes and press **Enter**



11. Do you want to enable Common Agent (caf) warning appears, type **Yes** and press **Enter**

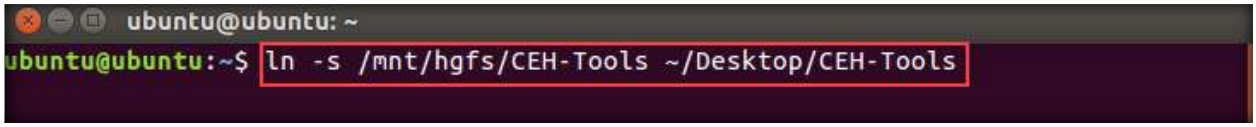


12. Now, the installation was successful, type **reboot** and press **Enter** to restart the Ubuntu machine



13. Login to the Ubuntu machine

14. Now, we need to mount the shared directory, open a terminal window and type **ln –s /mnt/hgfs/CEH-Tools ~/Desktop/CEH-Tools** press **Enter**
15. This will mount the shared directory on the Desktop

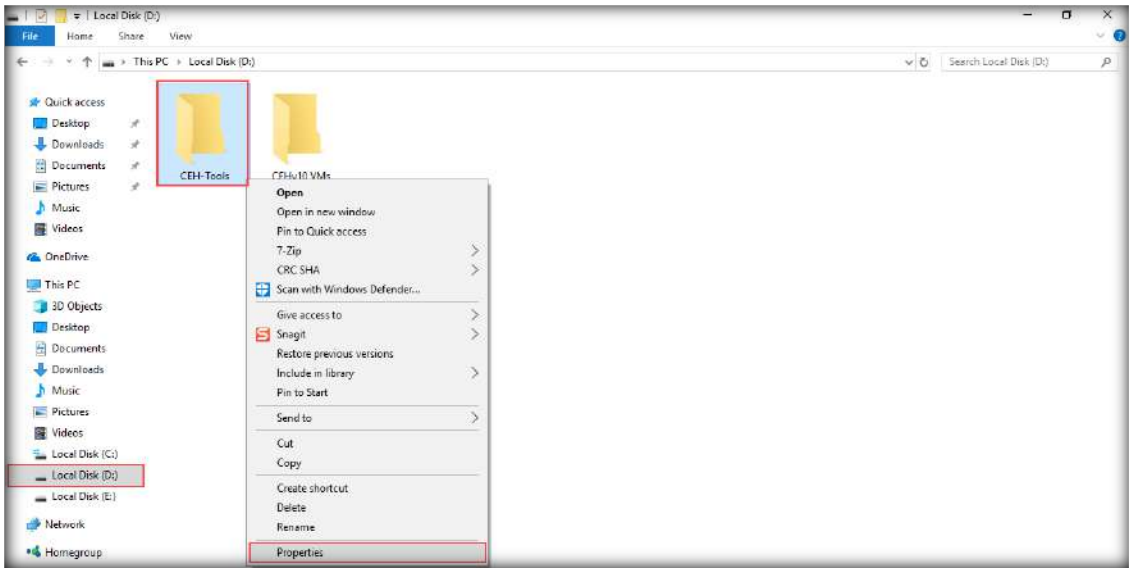


16. Shared CEH-Tools directory

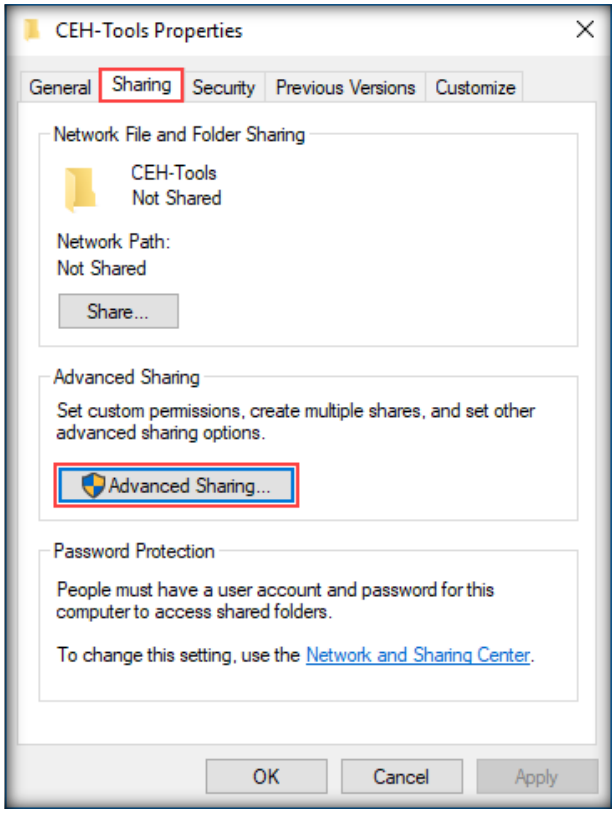
[Back to Configuration Task Outline]

CT#13: Mapping CEH-Tools with Android Machine

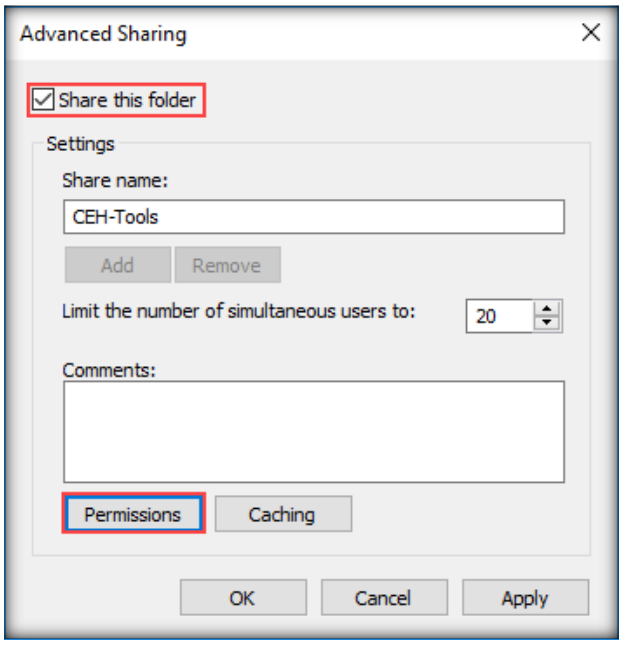
1. Before the performing this configuring task for Android, in your host machine navigate to the **CEH-Tools** folder location
2. Right-click on CEH-Tools folder, and click **Properties** from the context menu



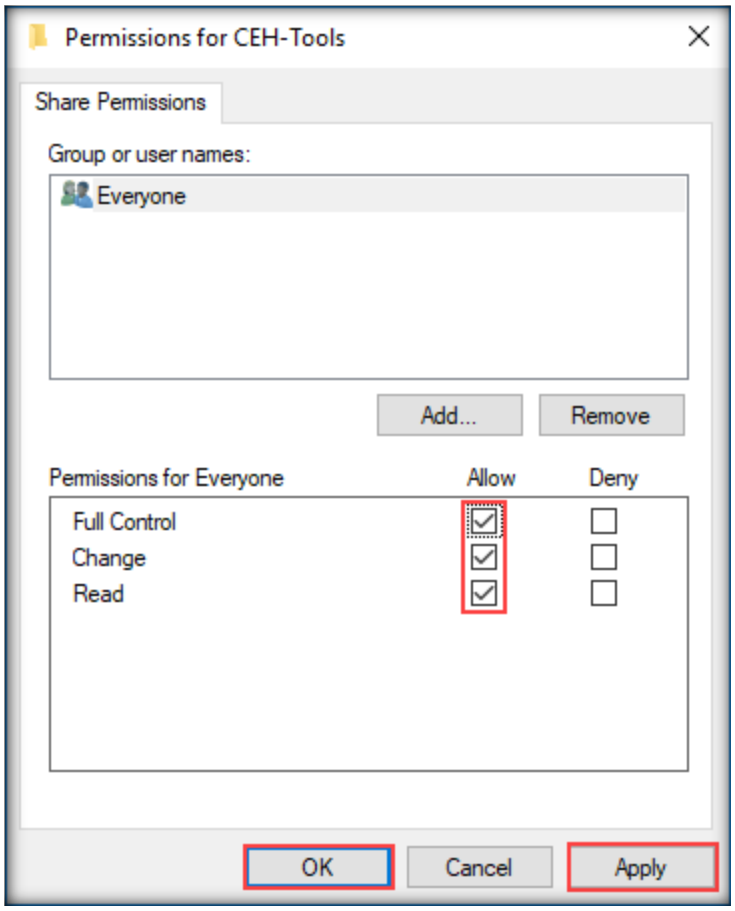
3. CEH-Tools Properties window appears, click **Sharing** tab, and click **Advanced Sharing** under Advanced Sharing section



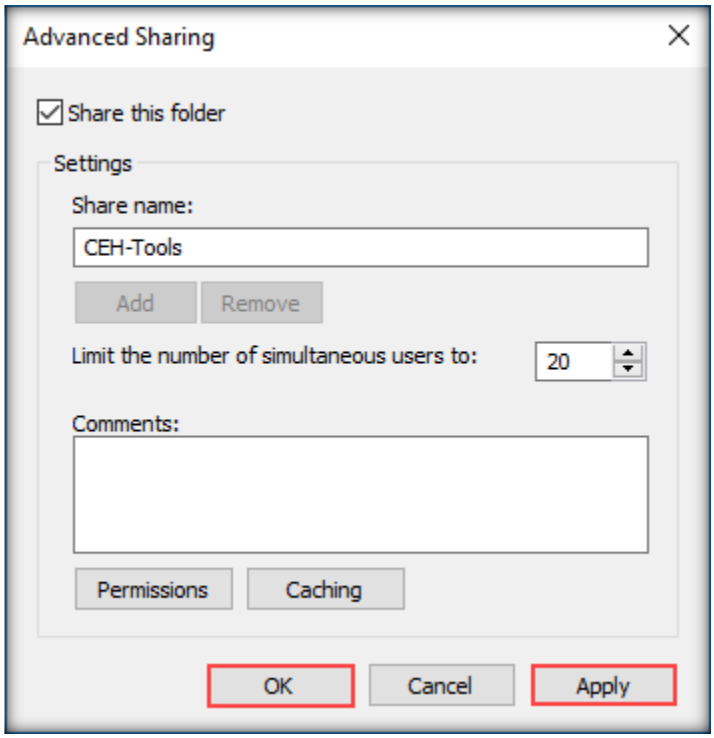
4. Advanced Sharing pop-up appears, check **Share this folder** option, and click **Permissions** as shown in the screenshot



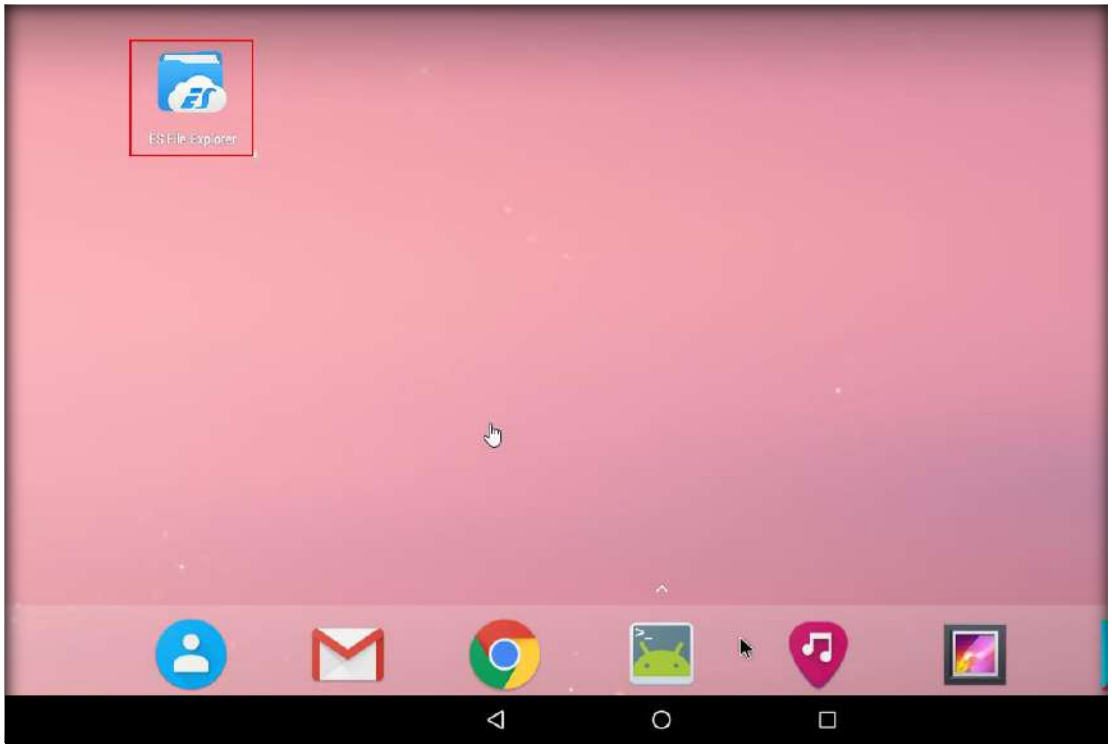
5. Permissions for CEH-Tools pop-up appears, check all the options under **Allow** in the **Permissions for Everyone** section. Click **Apply** and **OK**



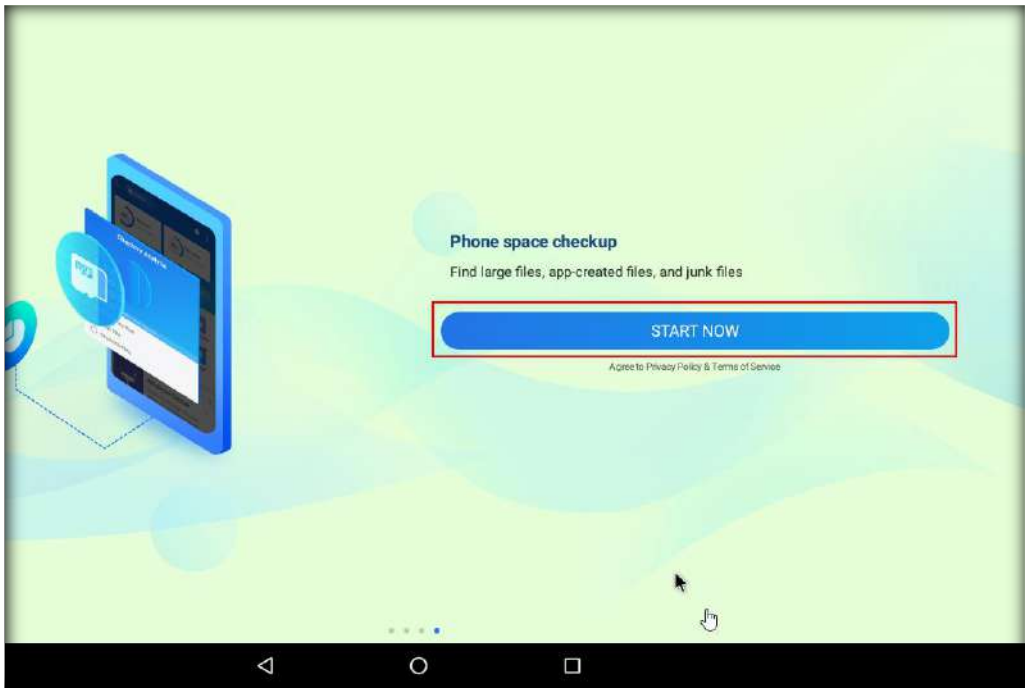
6. Click **Apply** and **OK** in the Advanced Sharing pop-up.



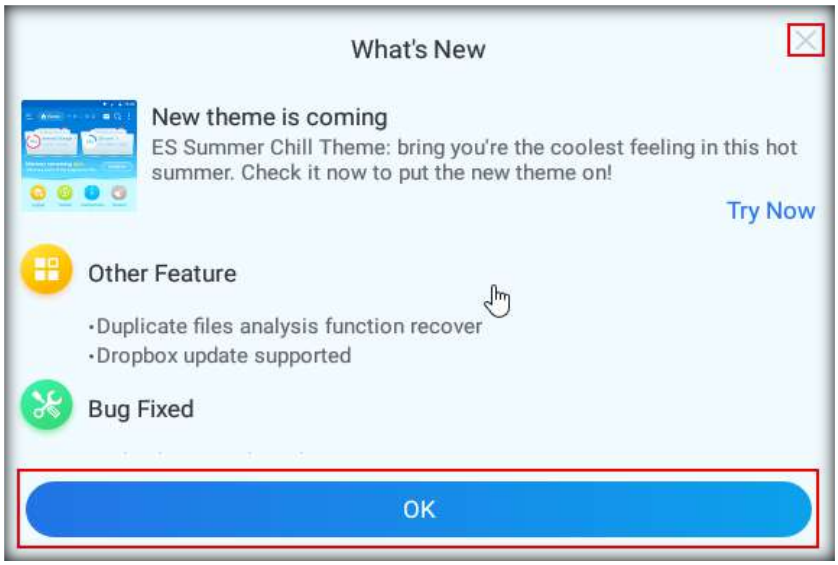
7. Click **Close** on the CEH-Tools Properties window
8. Power on **Android** machine from VMware Workstation
9. Click **ES File Explorer** icon present on the **Home** screen (hold the screen with mouse and move to left hand side)



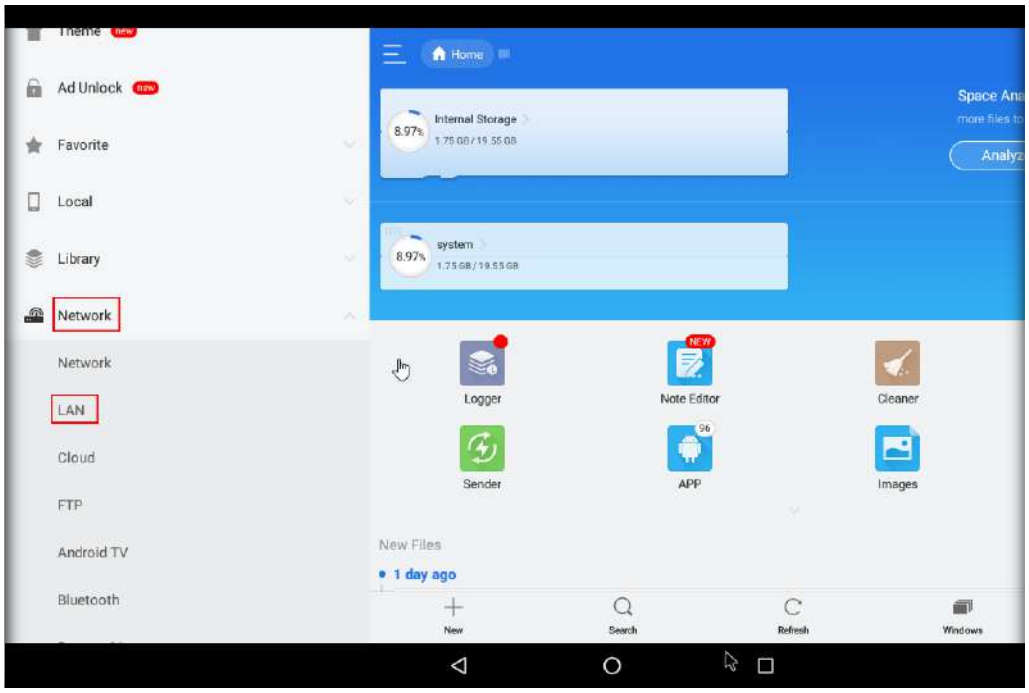
10. If ES File Explorer usage options and features appears, toggle the screen to left hand-side and click **START NOW** as shown in the screenshot



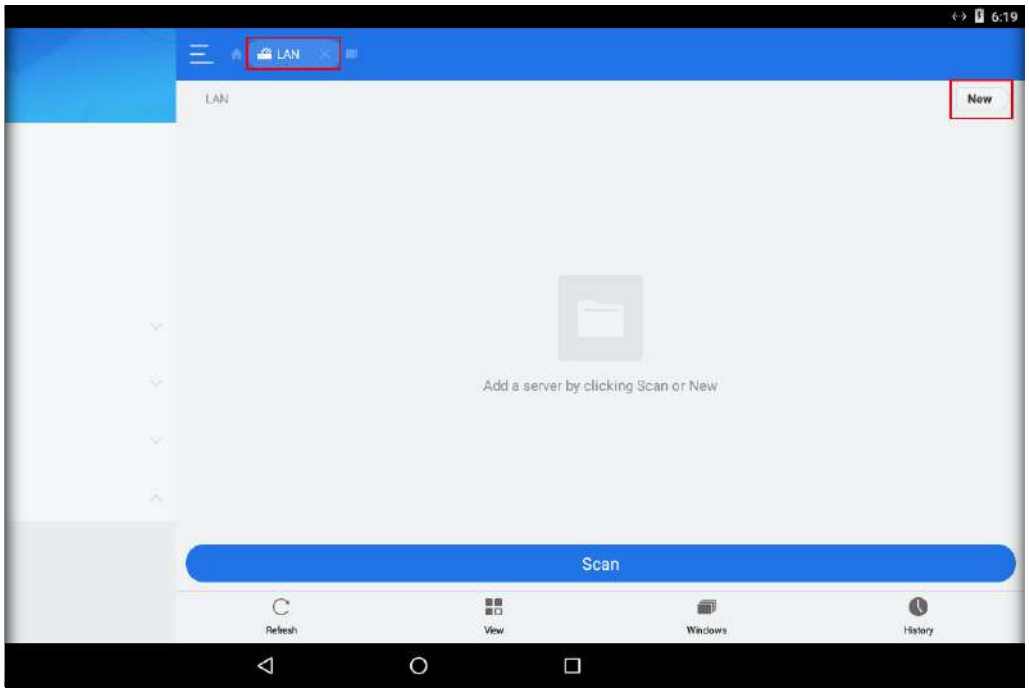
11. ES File Explorer window appears along with What's New pop-up, click **X** or **OK** to close the pop-up



12. Click **Network** to expand, and then click **LAN** in the left pane

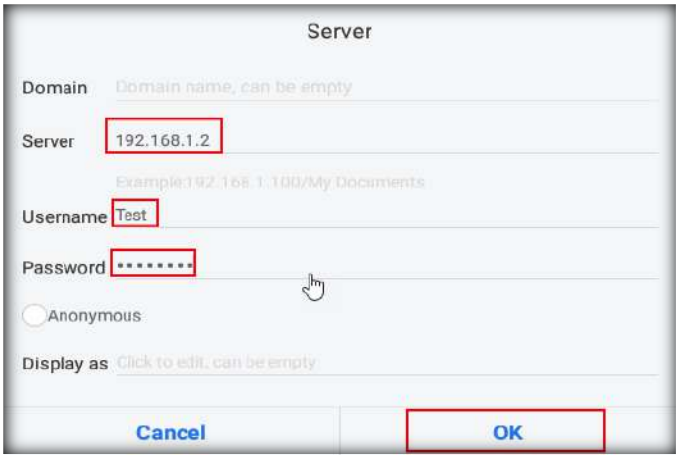


13. LAN screen appears along with the systems connected in the network, click **New**

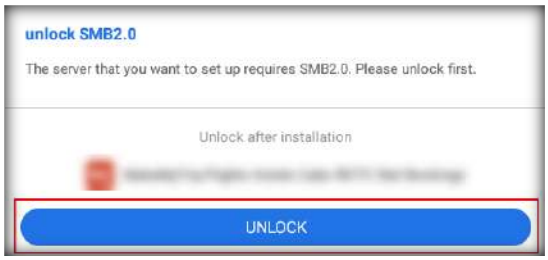


14. Server pop-up appears, enter your **Host machine IP address** in the Server field, and enter the credentials of your host machine and click **OK**

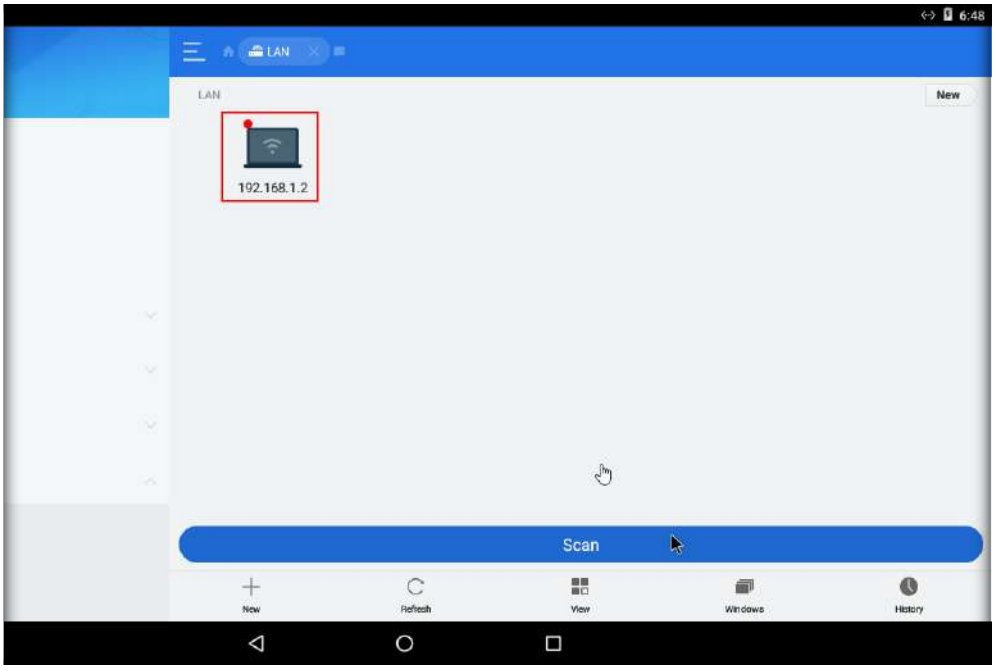
    Note: IP address will vary in your lab environment



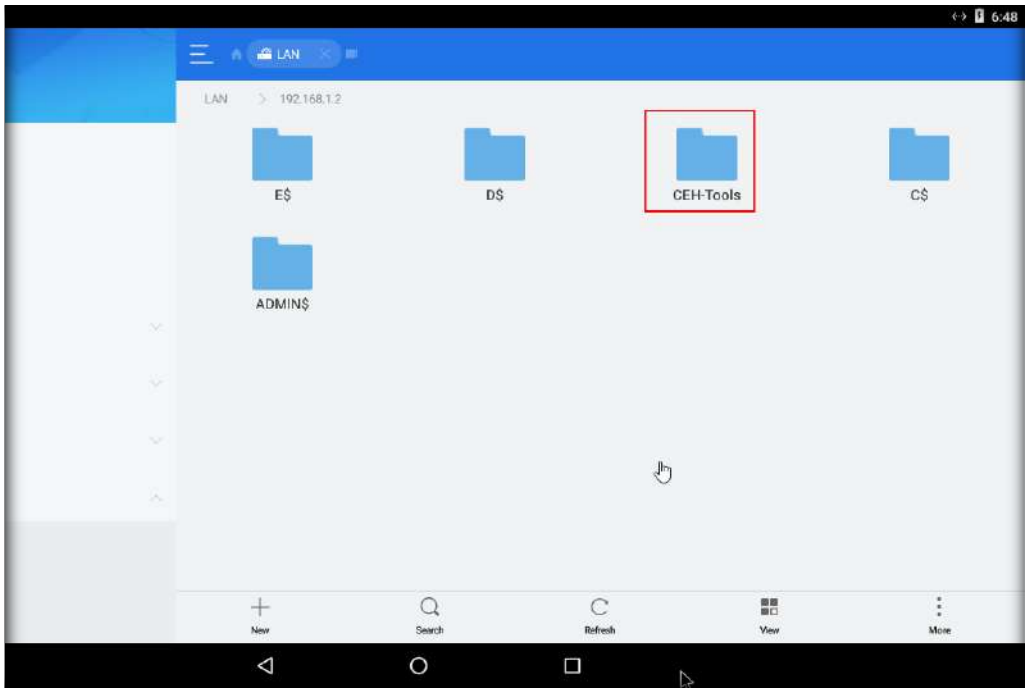
15. If unlock SMB2.0 pop-up appears, click UNLOCK to install the third party application
16. This will redirect you to play store window, and install the third party application



17. Switch back to EX File Explorer app, click on the **Host Machine IP** address icon as shown in the screenshot



18. This will display the shared folders of the Host Machine as shown in the screenshot. Shut down the machine



[Back to Configuration Task Outline]

CT#14: Install Adobe Acrobat Reader in Windows VMs

1. Select Windows Server 2016 in the left pane and click Power on this virtual machine in the left pane of the VMware Workstation window and login
2. Navigate to **Z:\CEH-Tools\CEHv10 Lab Prerequisites\Adobe Reader** folder
3. Alternatively, you may download the latest version of **Adobe Reader** from **Adobe** website
4. Double-click the **.exe** install file to begin the installation
5. Follow **wizard-driven** installation steps and **complete** the install by choosing **default** options throughout the installation process
6. While installing make sure that if any Anti-Virus add on option is select, uncheck the option and install adobe reader
7. In the same way, install the application in Windows Server 2012, Windows 10 and Windows 8

[Back to Configuration Task Outline]

CT#15: Install WinRAR in Windows VMs

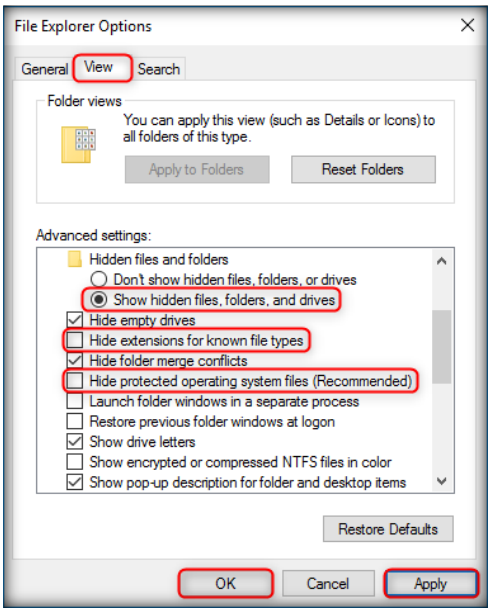
1. Navigate to **Z:\CEH-Tools\CEHv10 Lab Prerequisites\WinRAR** folder
2. Alternatively, you can also download the latest version of **WinRAR** from **Aspen Portal**
3. Double click on .exe setup file to begin the installation
4. **WinRAR setup** window appears
5. In the WinRAR setup window, click **Install**
6. Complete the **install** by choosing **defaults** throughout the installation process
7. After completing the installation, the installation **location** of WinRAR files window opens **automatically**
8. **Close** the window
9. In the same way, install the application in Windows Server 2012, Windows 10 and Windows 8

[Back to Configuration Task Outline]

CT#16: Configure Windows Explorer

1. Open the **Control Panel and** click **File Explorer Options**
2. **File Explorer Options** window appears, click the **View** tab
3. In the **Advanced Settings** section, under Hidden files and folders, select **Show hidden files, folders, and drives** radio button, uncheck **Hide extensions for known file types** and **Hide protected operating system files (Recommended)** options, click **Apply** and then click **OK**.

   Note: If a Warning pop-up appears, click **Yes**.



4. In the same way, configure these settings in Windows Server 2012, Windows 8 and Windows 10

   Note: In different version of windows, File Explorer Options may be named as Folder Options

[Back to Configuration Task Outline]

CT#17: Install Web Browsers in Windows VMs

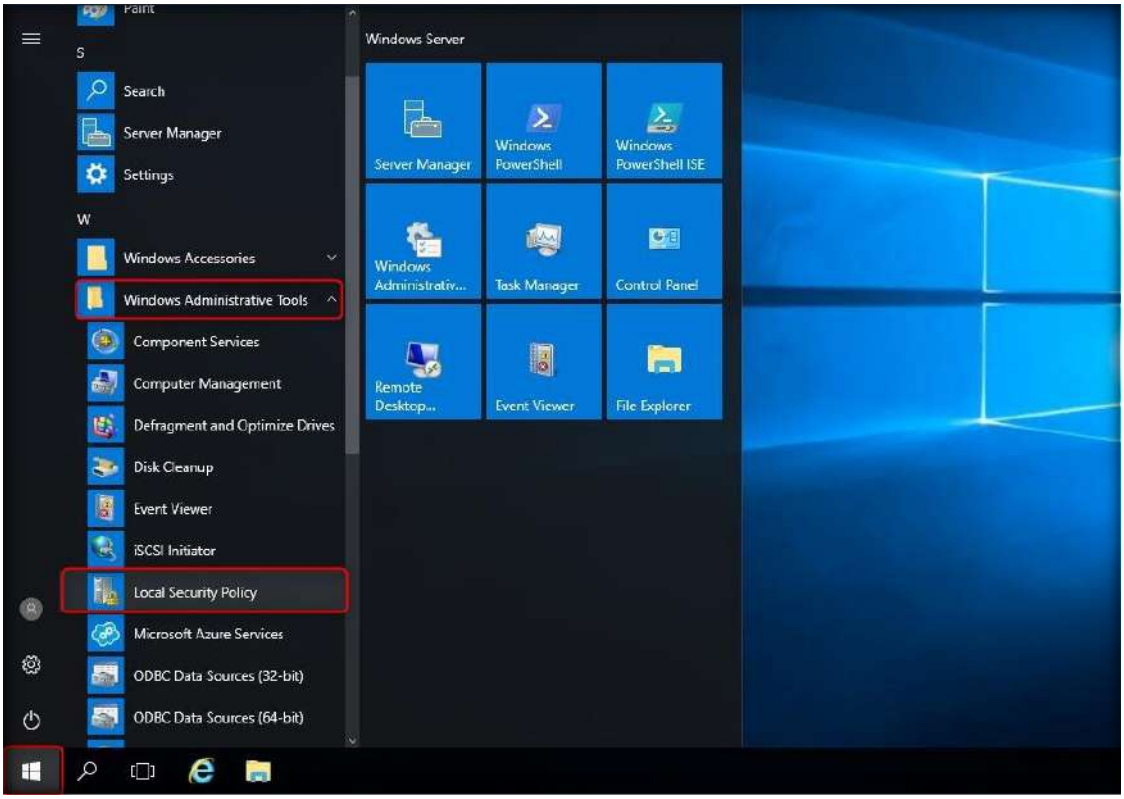
1. Navigate to **Z:\CEH-Tools\CEHv10 Lab Prerequisites** in guest operating systems
2. Open **Web Browsers** folder
3. Follow **wizard-driven** installation steps to install **Firefox** and **Chrome** web browsers
4. You can also download **latest** version of web browsers from respective **vendors**

[Back to Configuration Task Outline]

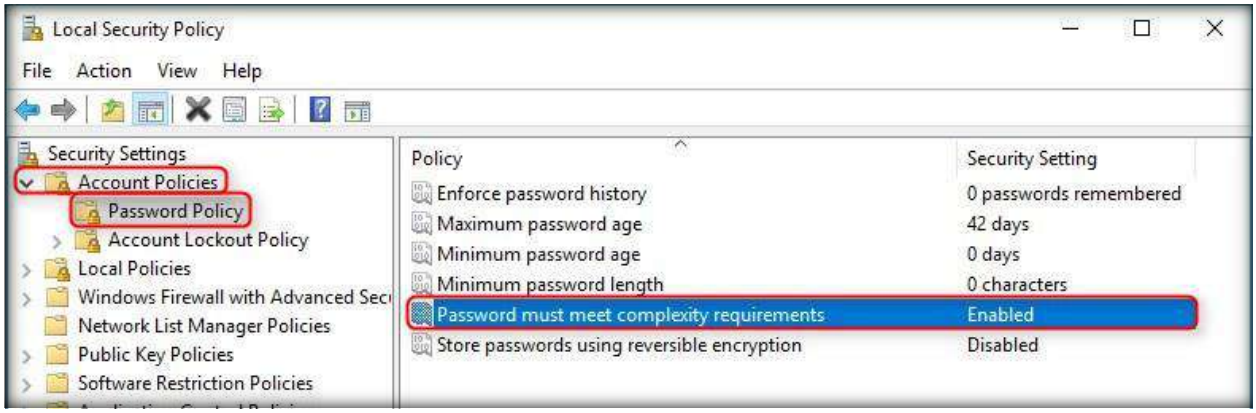
CT#18: Removing Password Complexity from Guest Operating Systems

Remove Password Complexity in Windows Server 2016 (Virtual machine)

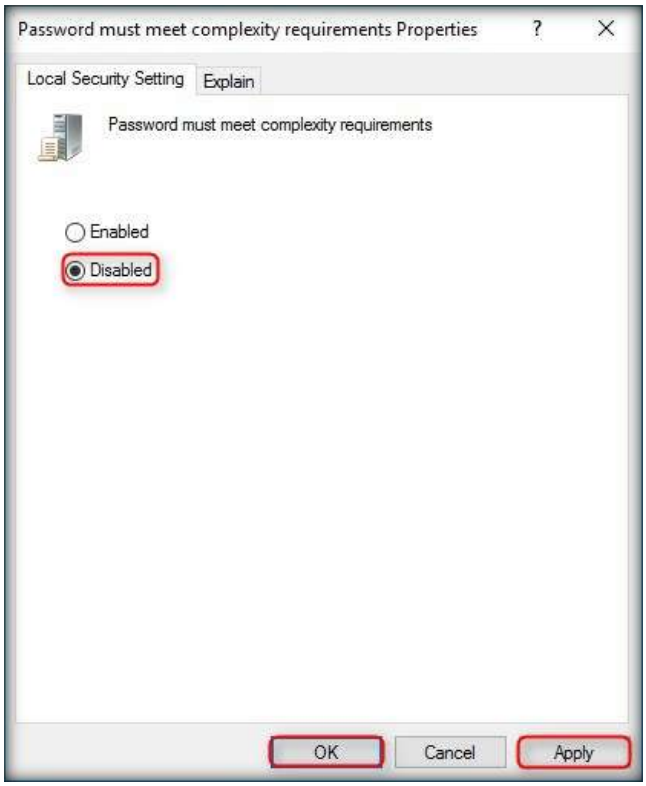
1. To remove password complexity in Windows Server 2016 virtual machine
2. In the Windows Server 2016 virtual machine, click the **Windows** icon at the lower left corner of the screen
3. **Start** menu appears, click **Windows Administrative Tools** → **Local Security Policy**



4. **Local Security Policy** window appears, expand **Account Policies** node, click **Password Policy** in the left pane and in the right pane double-click **Password must meet complexity requirements**

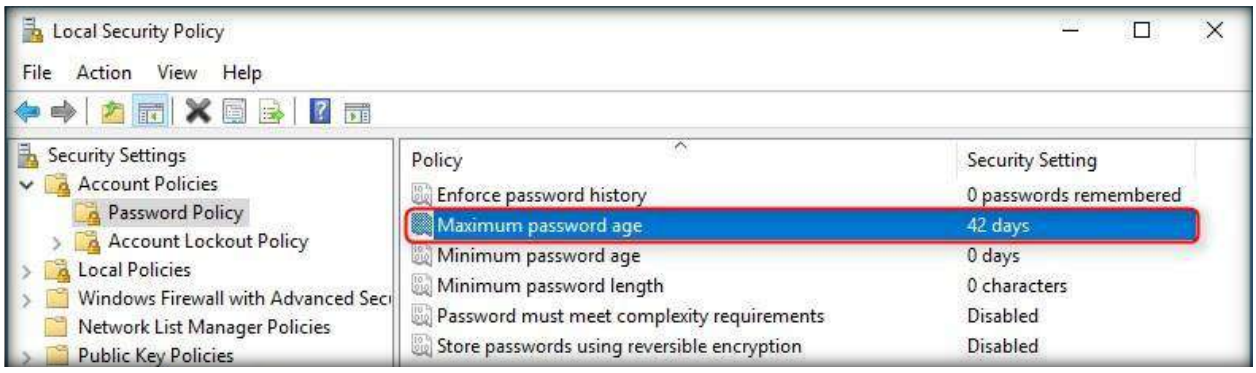


5. **Password must meet complexity requirements Properties** window appears, select **Disabled** radio button and click **Apply** and **OK**

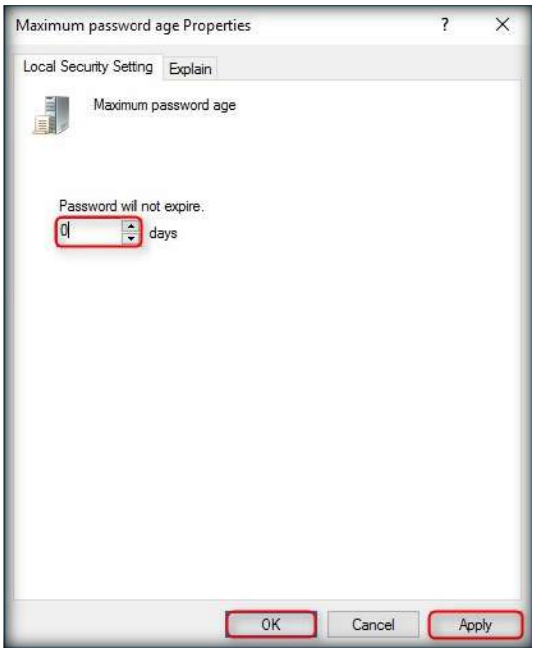


Remove Maximum Password Age in Windows Server 2016 (Virtual Machine)

1. In the right pane double-click **Maximum password age**



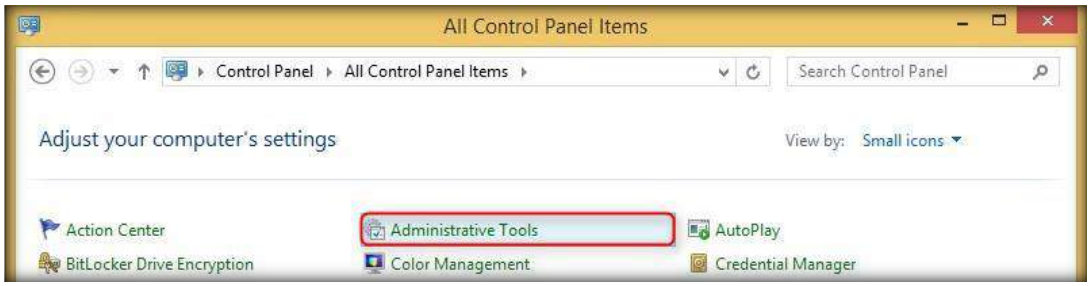
2. **Maximum password age Properties** window appears; enter **0** days under **Password will expire in** section. As soon as **0** is entered, the section name changes to **Password will not expire**. Click **Apply** and click **OK**



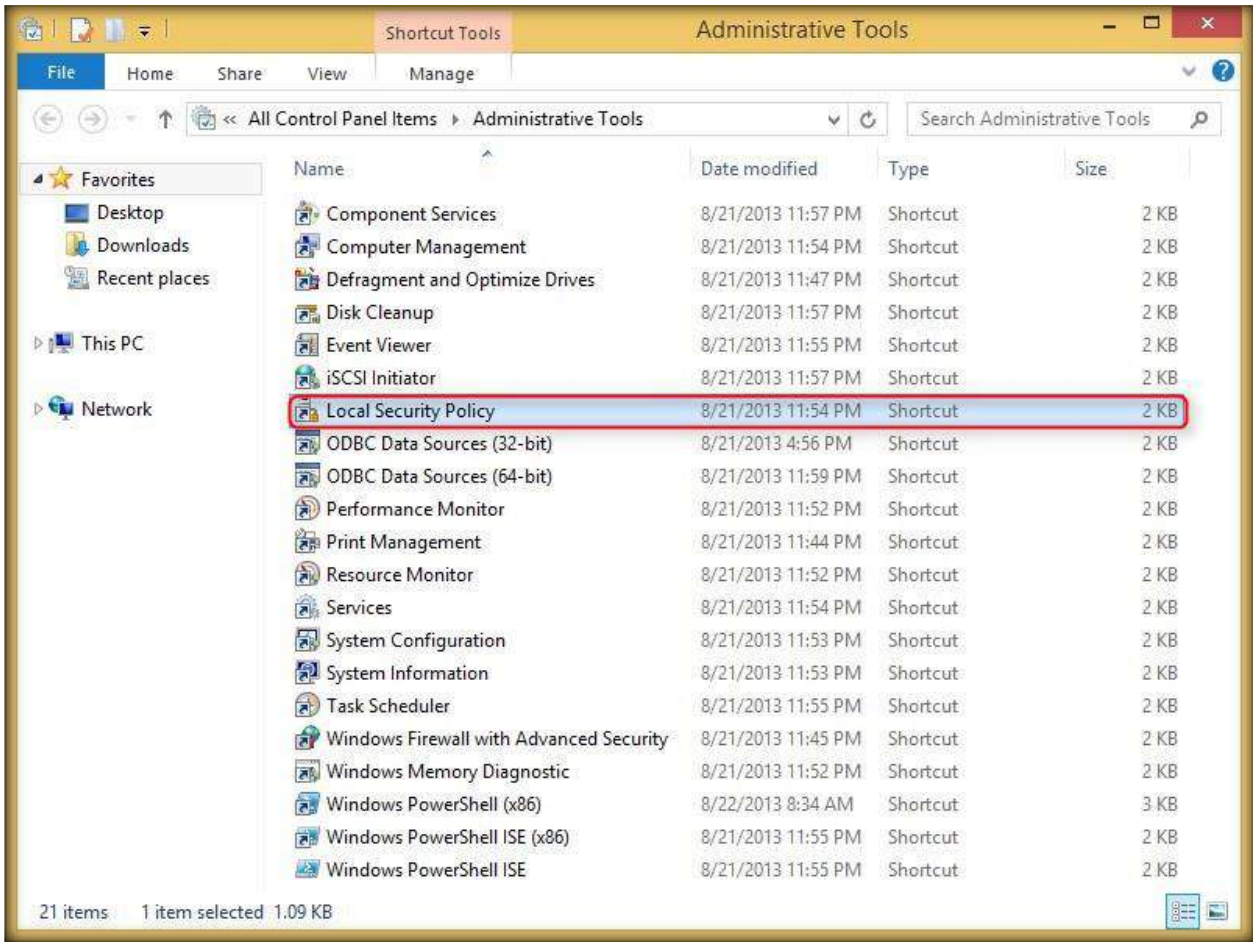
Remove Password Complexity in Windows 8 (Virtual Machine)

1. To remove password complexity in Windows 8 virtual machine, Power on and **Log On** to Windows 8 virtual machine
2. In the Windows 8 virtual machine, open **Control Panel**
3. Control Panel window appears on the screen, select **Small icons** from the **Category** drop down list to see all the control panel options

4. In **All Control Panel Items** window click **Administrative Tools**



5. **Administrative Tools** window appears, double-click **Local Security Policy**

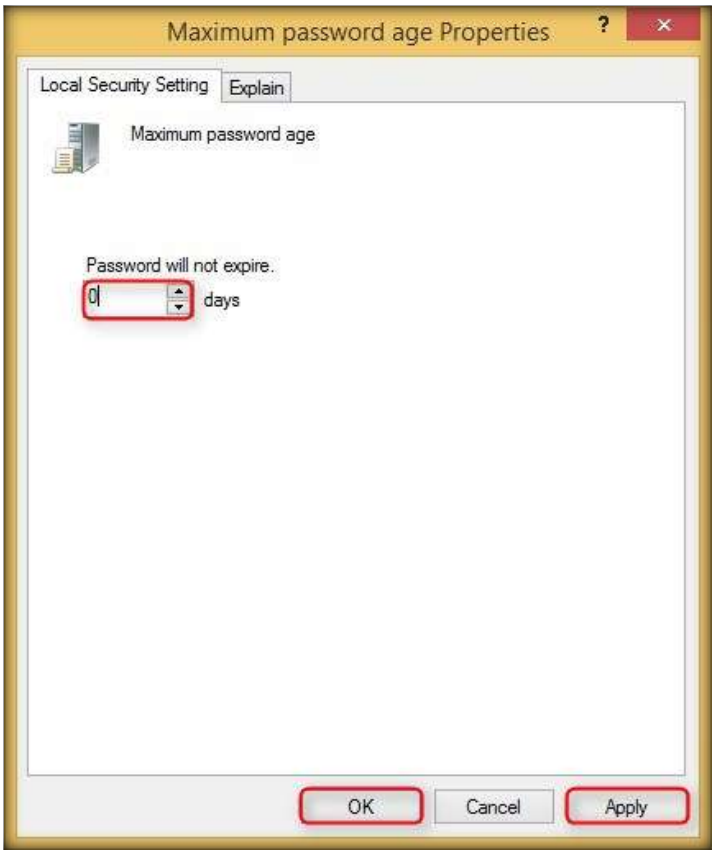


6. **Local Security Policy** window appears, expand **Account Policies** node, click **Password Policy** in the left pane and in the right pane double-click **Password must meet complexity requirements**
7. **Password must meet complexity requirements Properties** window appears, select **Disabled** radio button and click **Apply** and **OK**

Remove Maximum Password Age in Windows 8 (Virtual Machine)

1. In the right pane double-click **Maximum password age**

2. **Maximum password age Properties** window appears; enter **0** days under **Password will expire in** section. As soon as **0** is entered, the section name changes to **Password will not expire**. Click **Apply** and then click **OK**. Then close all the windows.



3. Similarly configure the **Maximum password age** and **Password must meet complexity requirements** options Windows 10 virtual machine

[Back to Configuration Task Outline]

CT#19: Creating Demo User Accounts in Windows Server 2016, Windows 10, and Windows 8

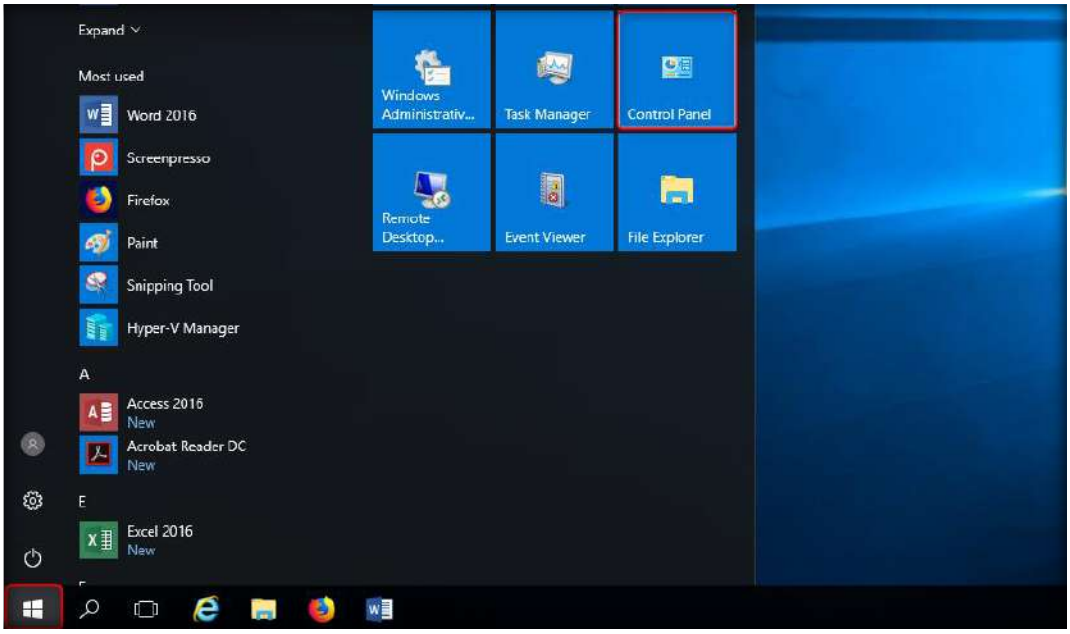
Create user accounts in Windows Server 2016, Windows 10, and Windows 8.

For demonstration purpose, we are creating three different accounts. Create all three user accounts in all the machines. Below are the user account details:

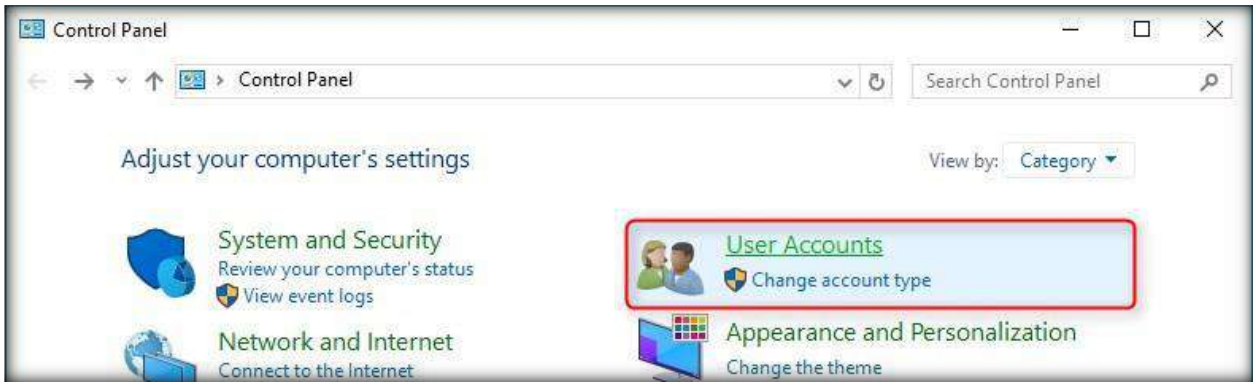
(i) Username: **Martin**; Password: **apple**
(ii) Username: **Jason**; Password: **qwerty**
(iii) Username: **Shiela**; Password: **test**

Creating User Accounts in Windows Server 2016

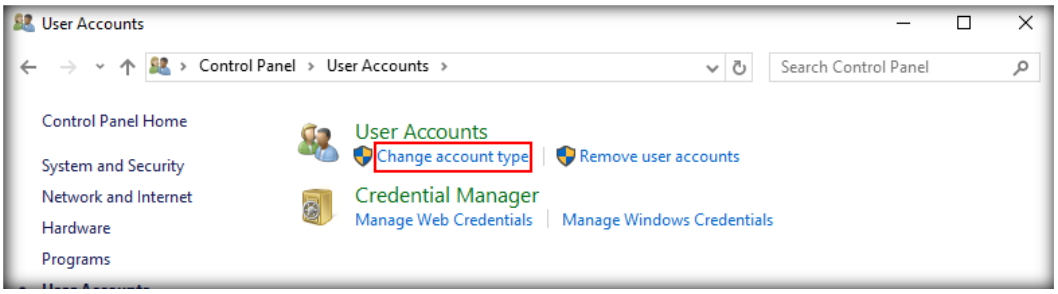
1. To create a user account in Windows Server 2016, click **Start** menu icon at the lower left corner of the screen and click **Control Panel**



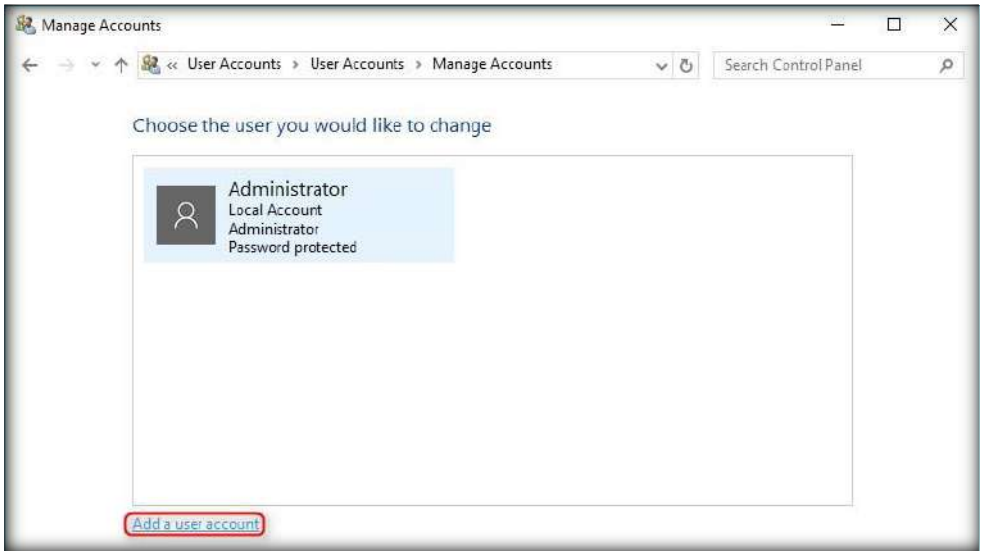
2. **Control Panel** window appears click **User Accounts**



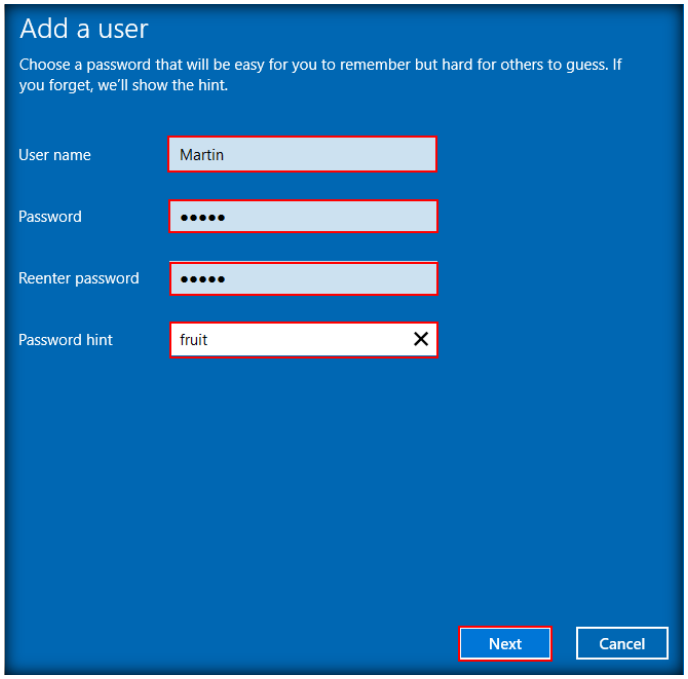
3. In User Accounts window, click **Change account type** or **Remove user accounts** link



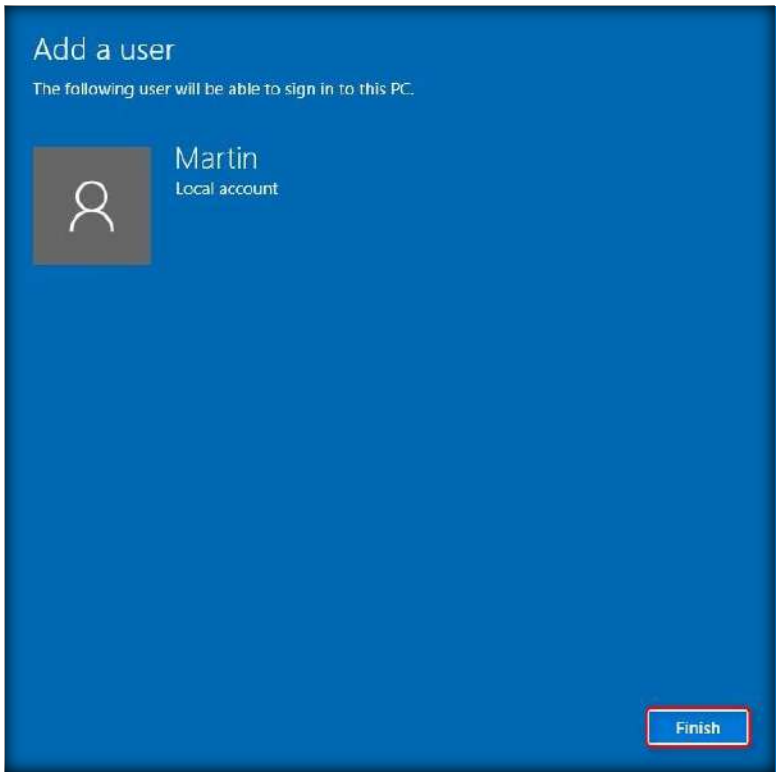
4. Click **Add a user account** in Manage Accounts window



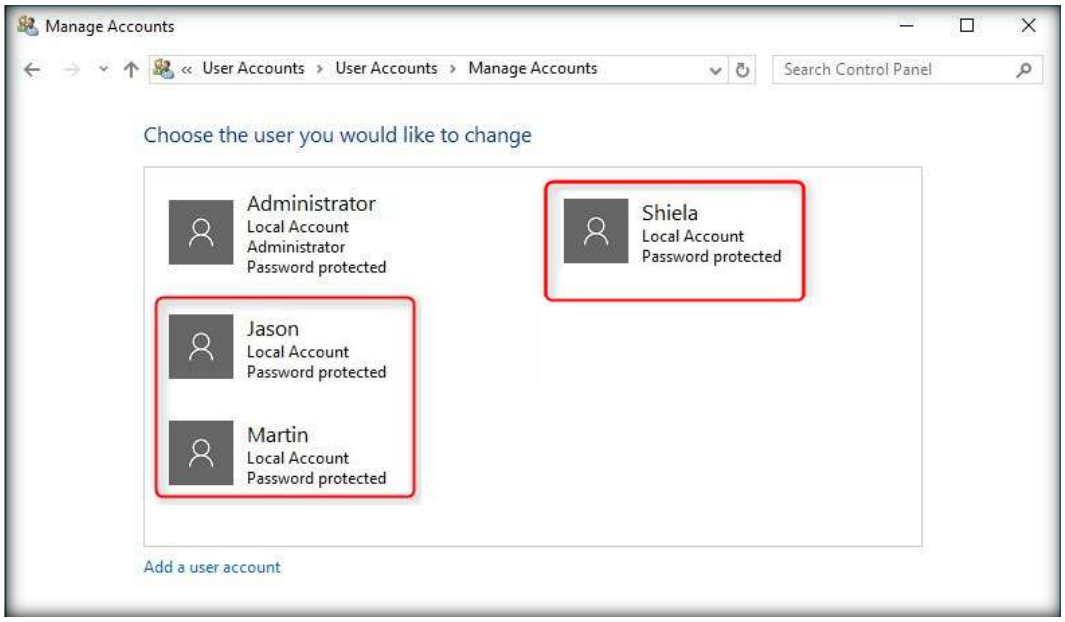
5. **Add a user** wizard appears, fill in the following fields and click **Next**



6. Click **Finish** after user account is created



7. Follow steps 4-6 and create the other users as well
8. Below screenshot shows the user accounts created in Windows Server 2016 virtual machine



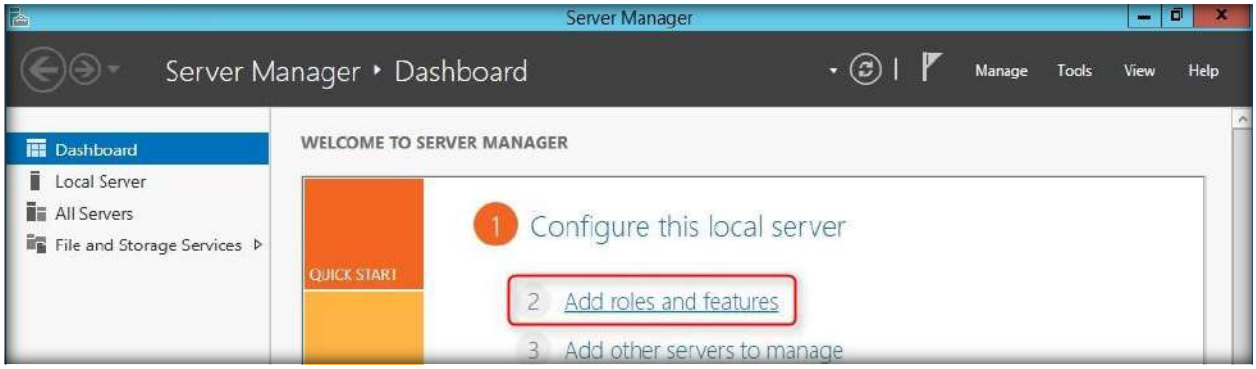
Note: Create these three user accounts in **Windows 10** and **Windows 8** virtual machines.

[Back to Configuration Task Outline]

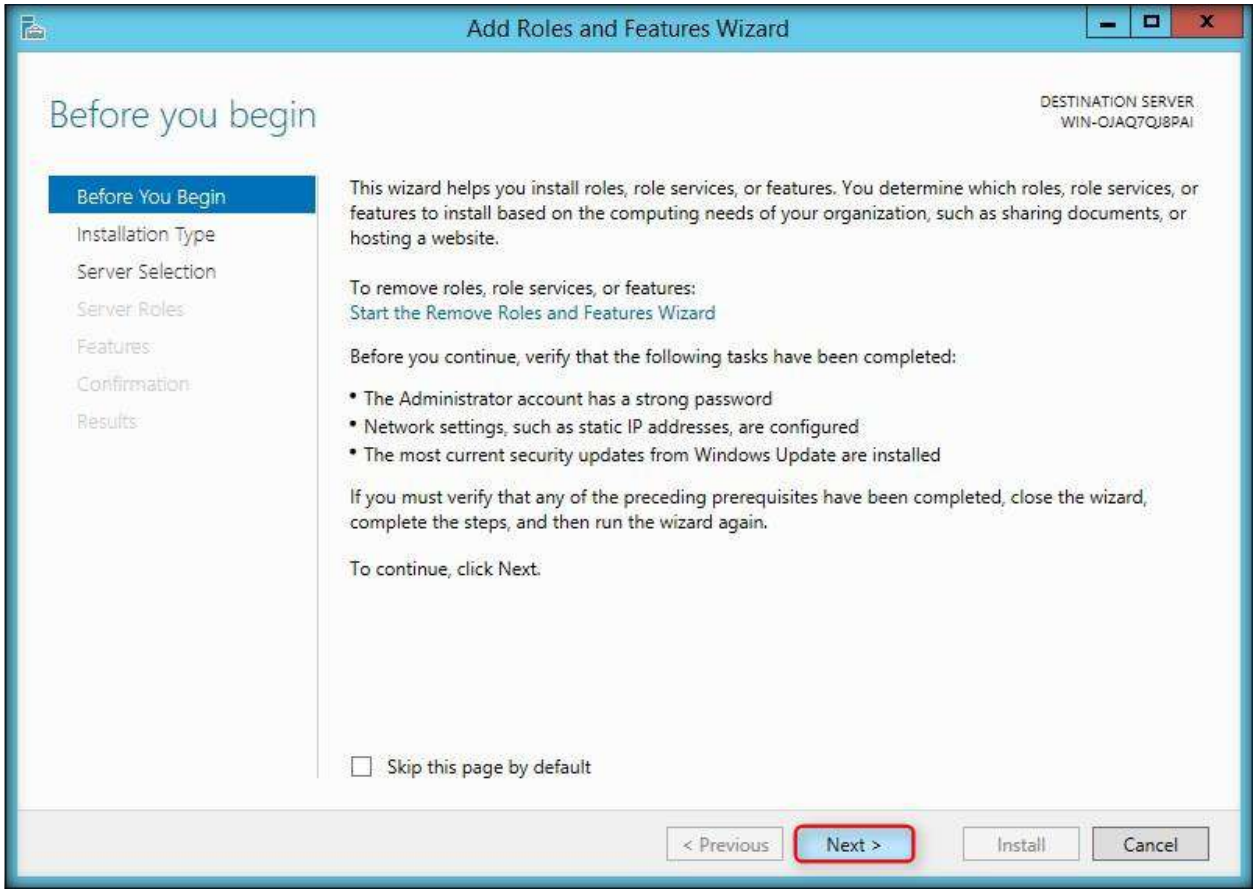
CT#20: Install Active Directory and Create User Accounts in Windows Server 2012

Install Active Directory in Windows Server 2012 virtual machine

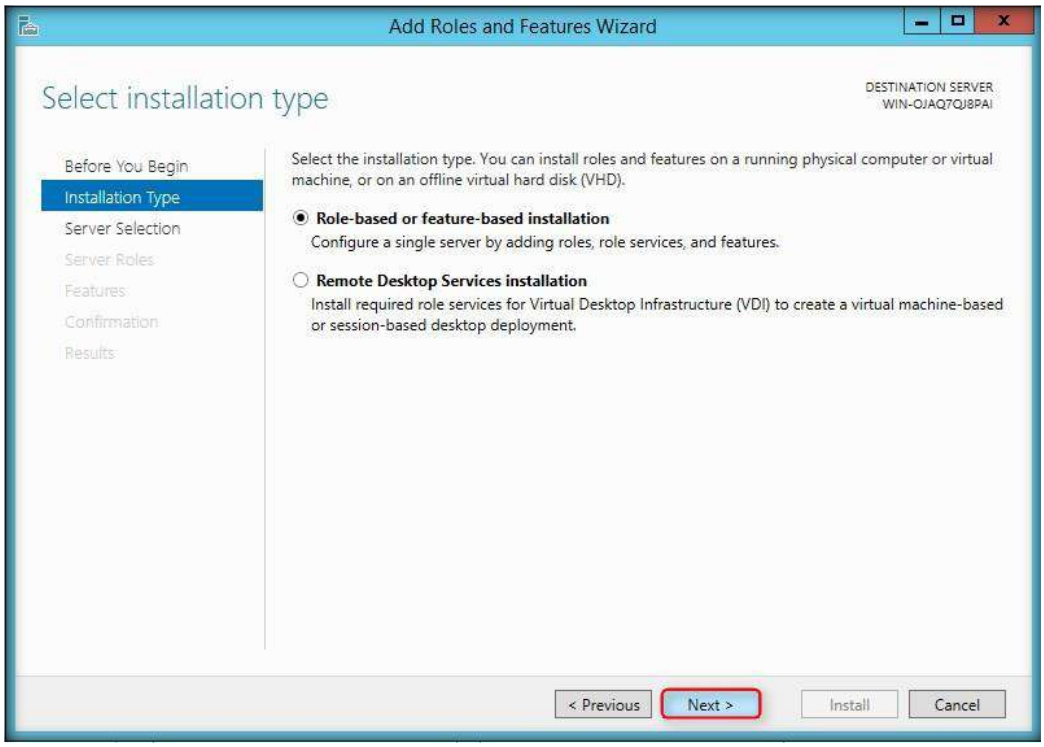
1. To install Active Directory (AD) in Windows Server 2012 machine, click Windows Server 2012 machine in the left pane and click Power on this virtual machine and then login to the machine
2. After successful logon, Server Manager window appears, click **Add roles and features** from the Server Manager Dashboard



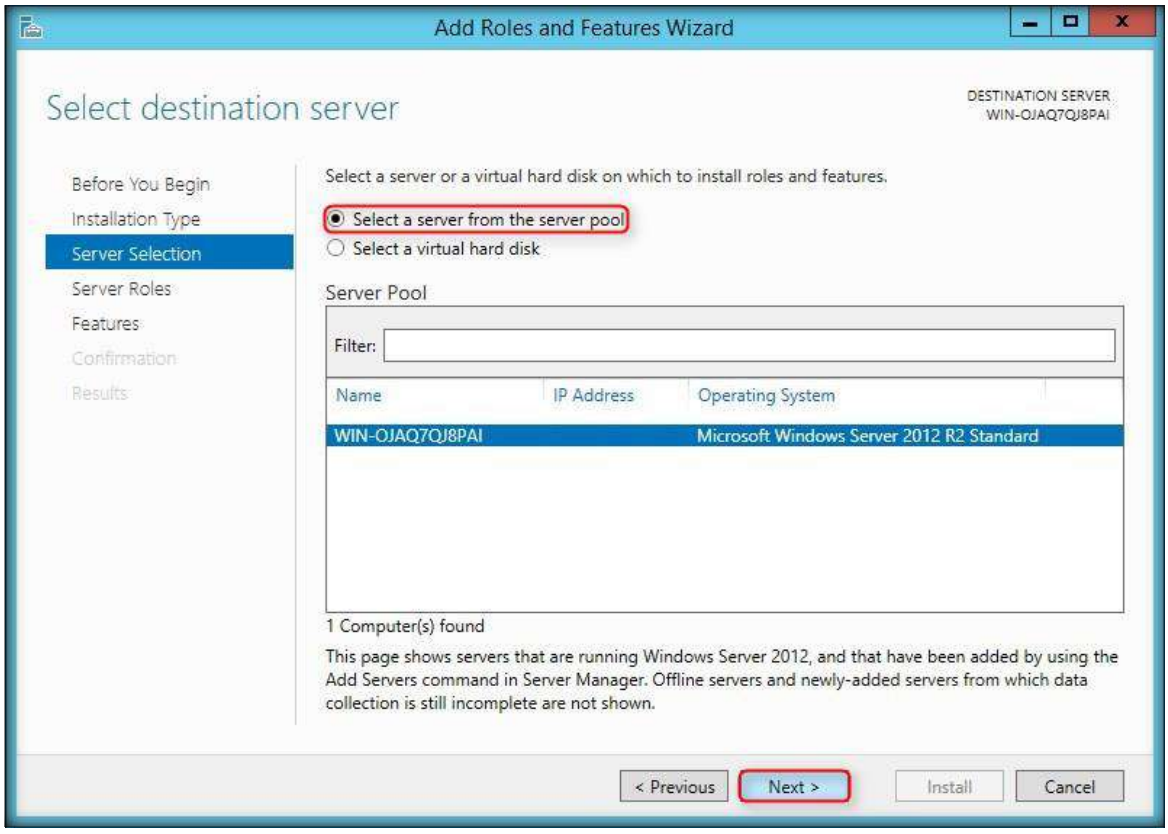
3. Before You Begin wizard appears click **Next** to continue



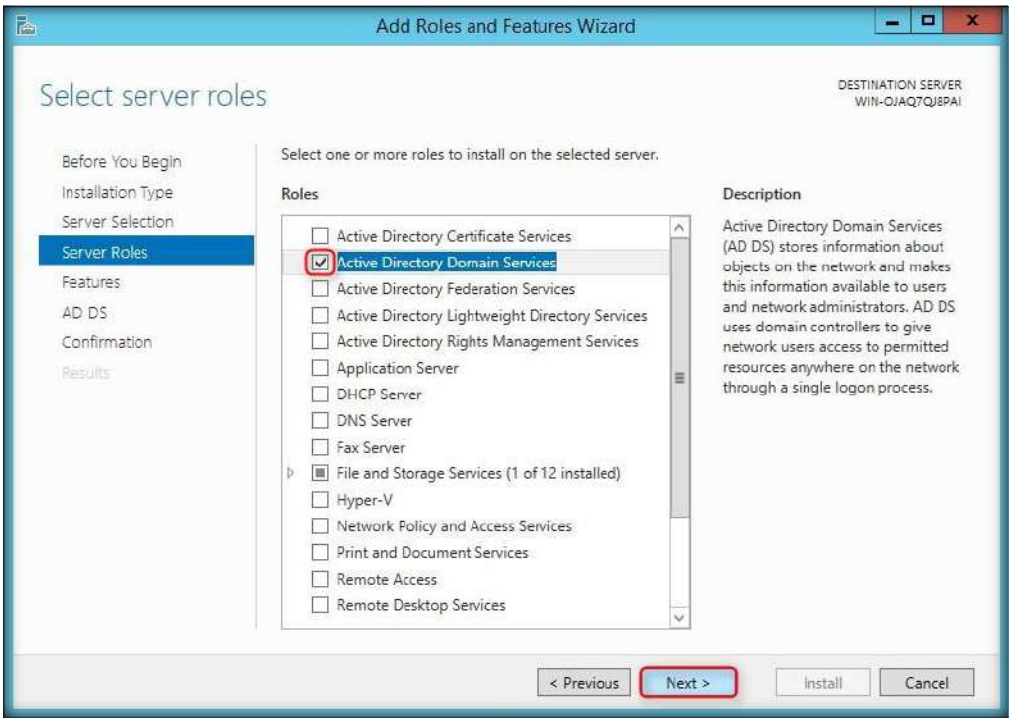
4. Select Installation type section appears, leave the options to default and click **Next**



5. Select destination server section appears, choose the **Select a server from the server pool** radio-button and click **Next**

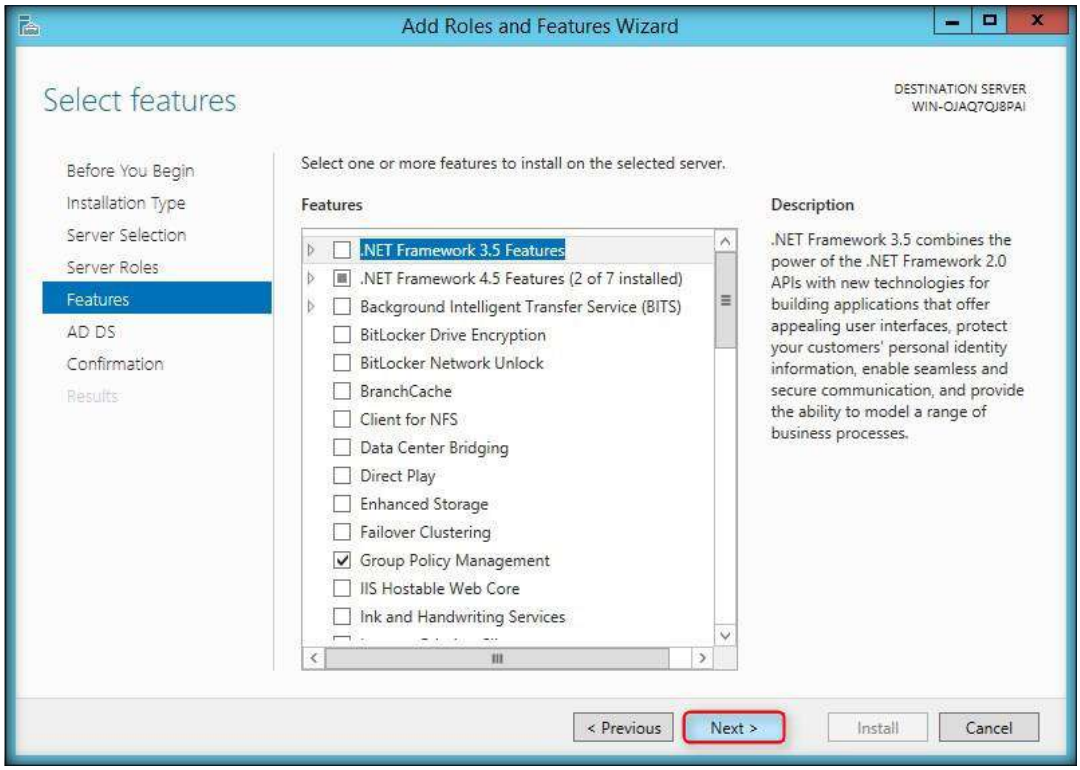


6. Check Active Directory Domain Services from Roles section in Select Server Roles wizard and click Next

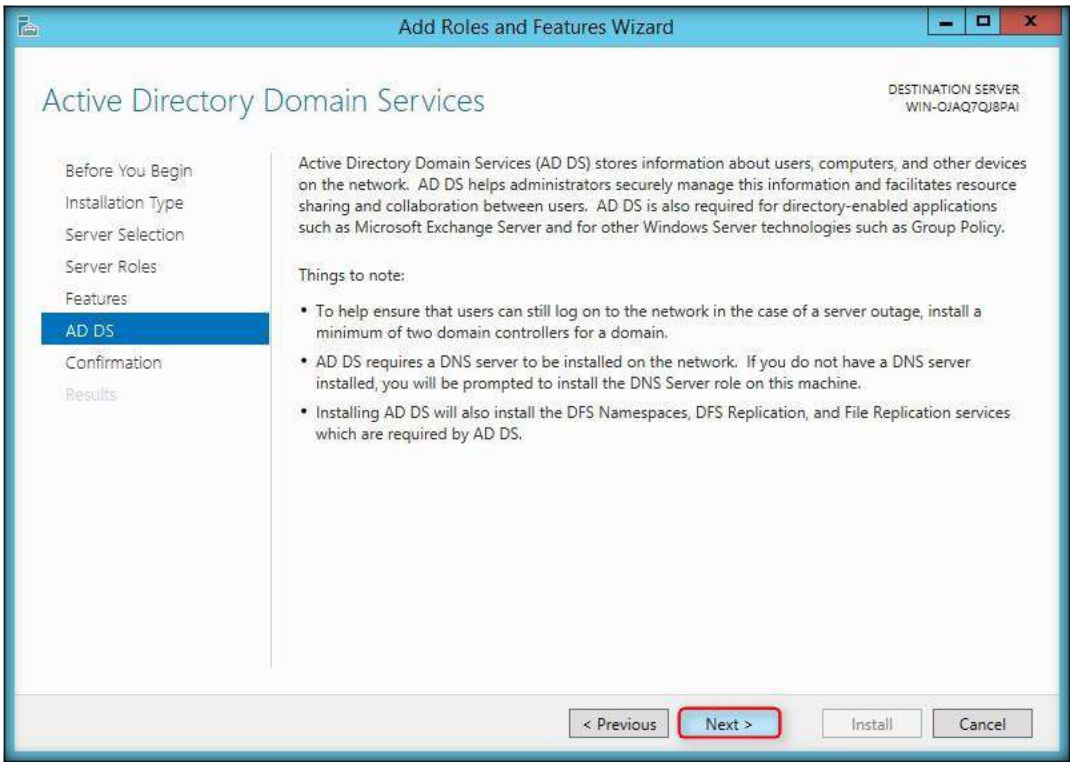


Note: If Add Roles and Features Wizard pop-up appears, click **Add Features**

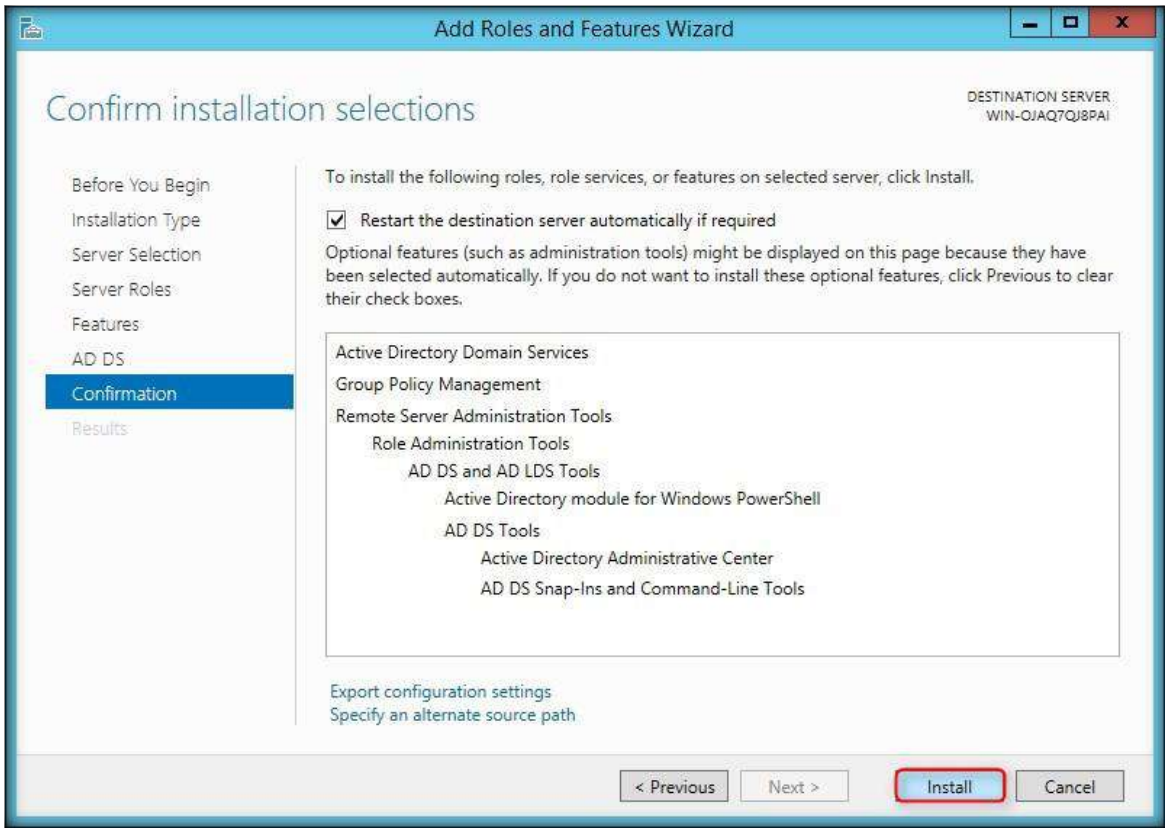
7. In Select Features section click **Next** to continue



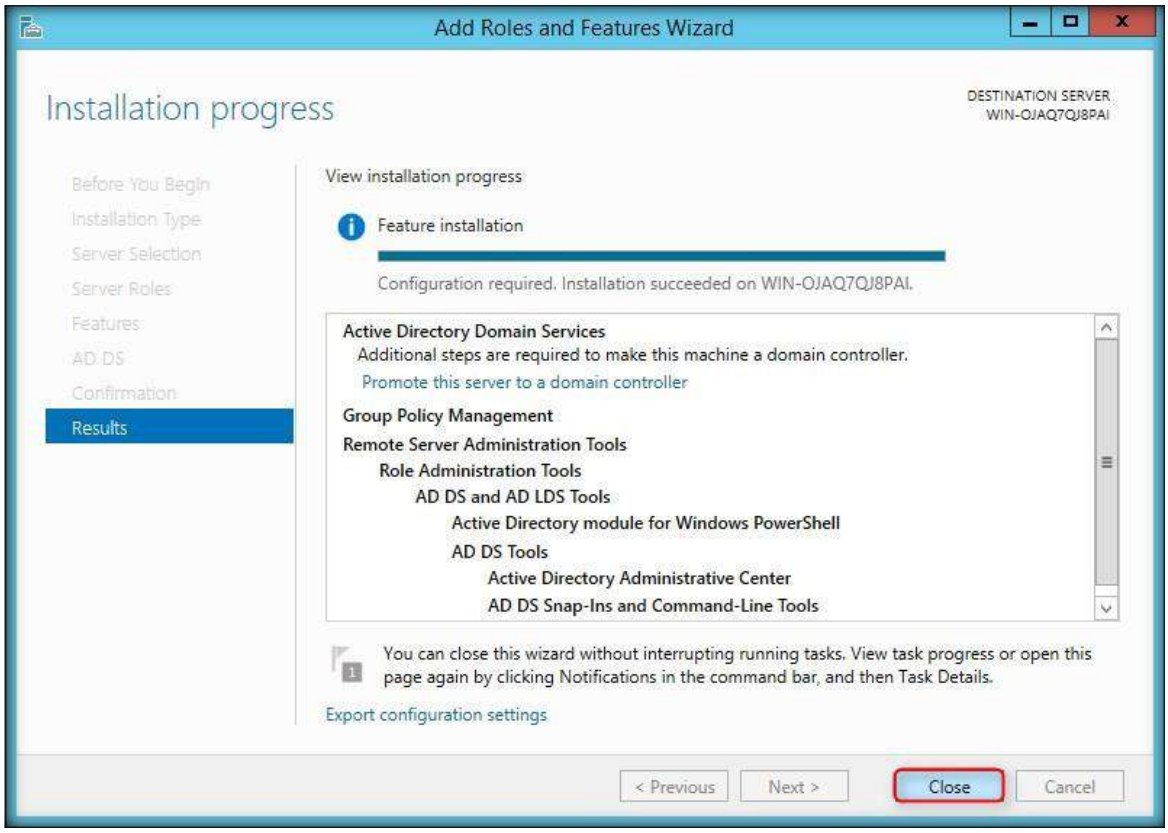
8. Active Directory Domain Services section appears click **Next** to continue



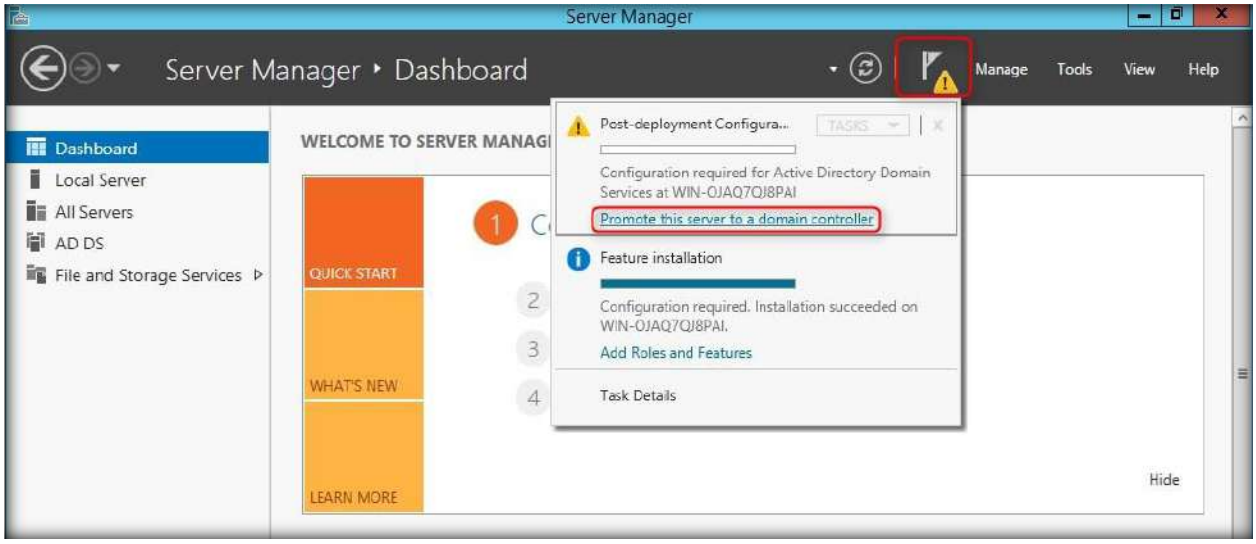
9. **Confirm Installation Selections** section appears, click **Install**



10. Once the installation is finished click **Close** in the Add Roles and Features Wizard window

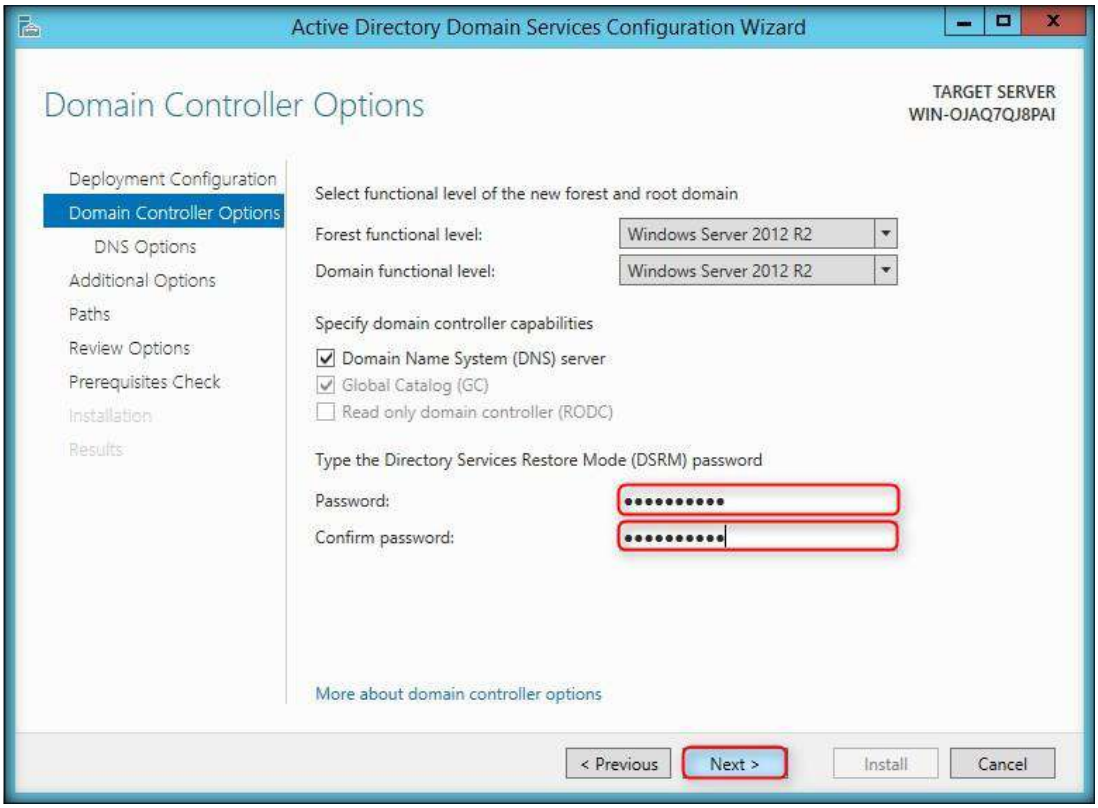


11. In the Server Manager Dashboard, click the **Flag** icon and click **Promote this server to a domain controller** link as shown in the screenshot below

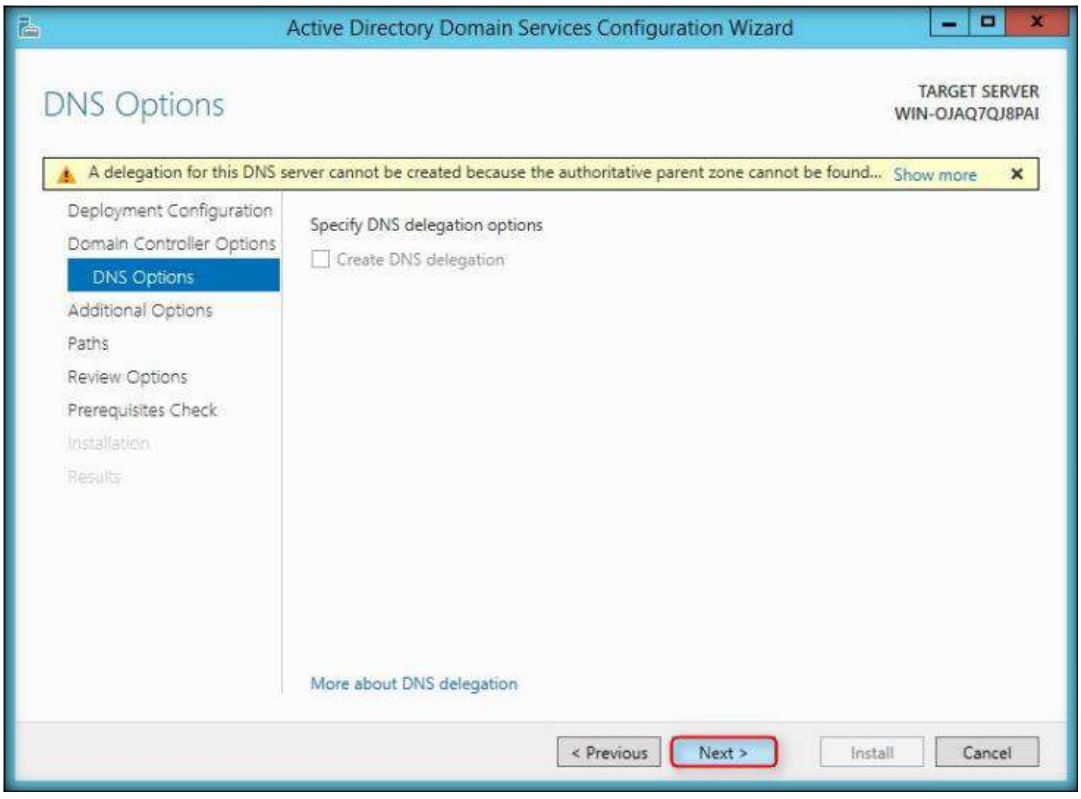


12. Active Directory Domain Services Configuration Wizard window appears, fill in the following Password and Confirm password field and click Next

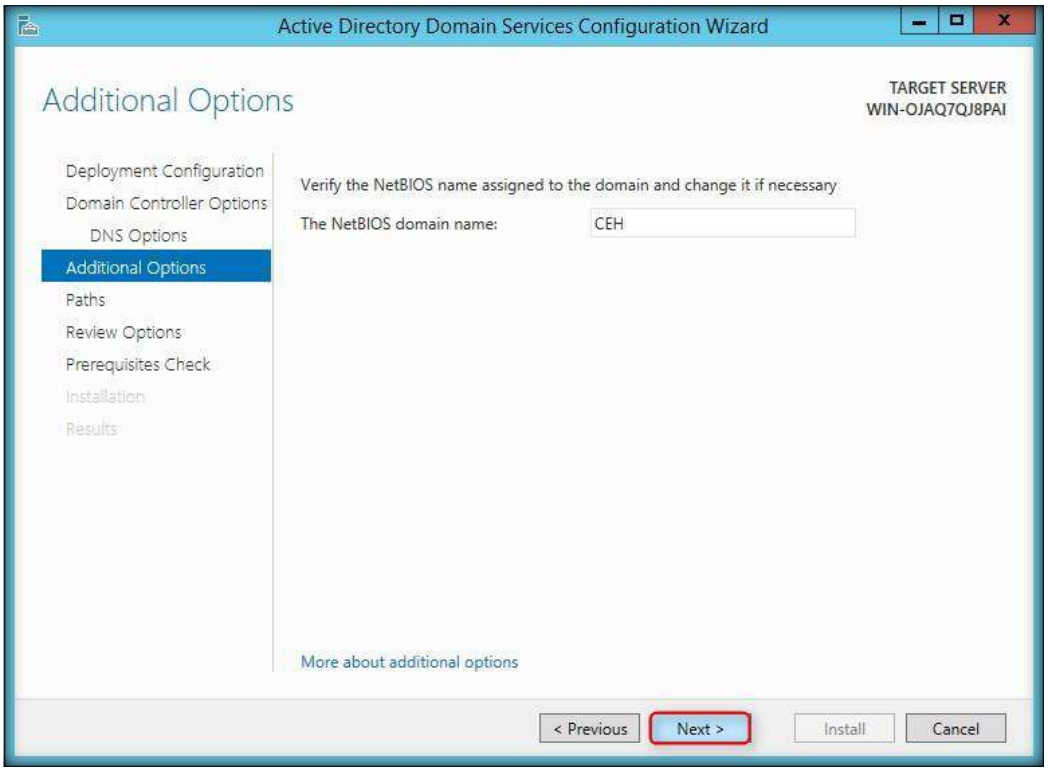
13. In this lab environment we have provided password as Pa$$w0rd



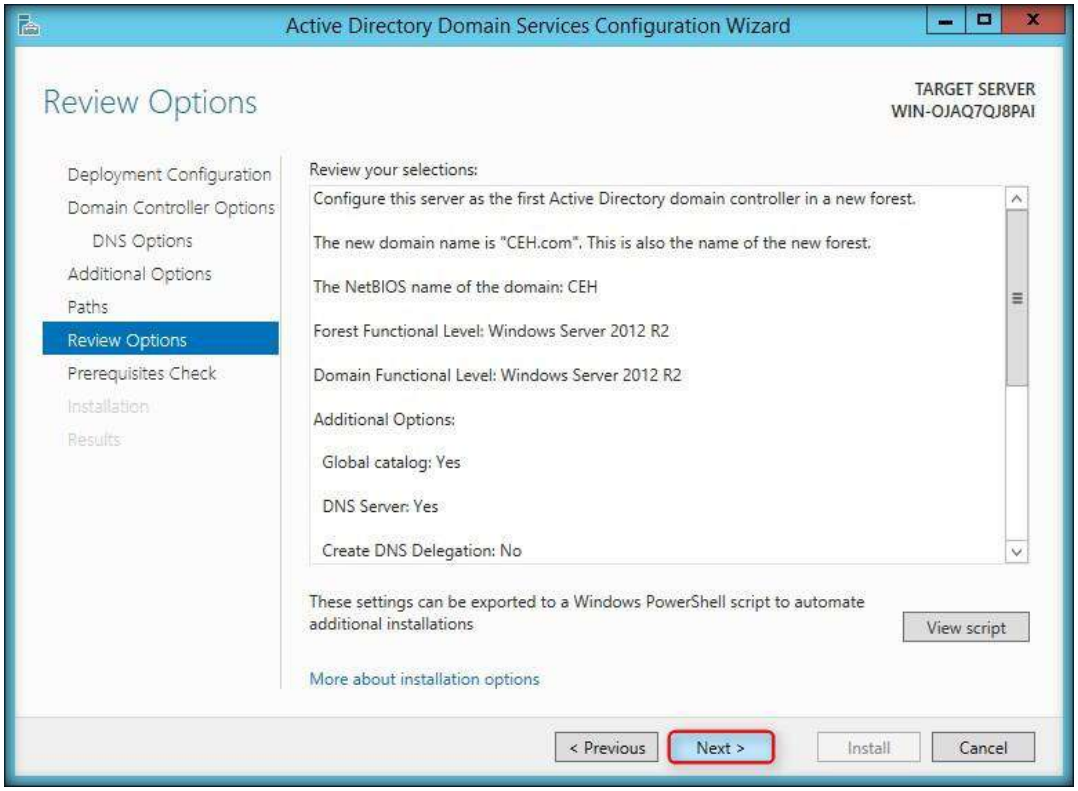
14. DNS Options section appears, ignore any alerts and click **Next**



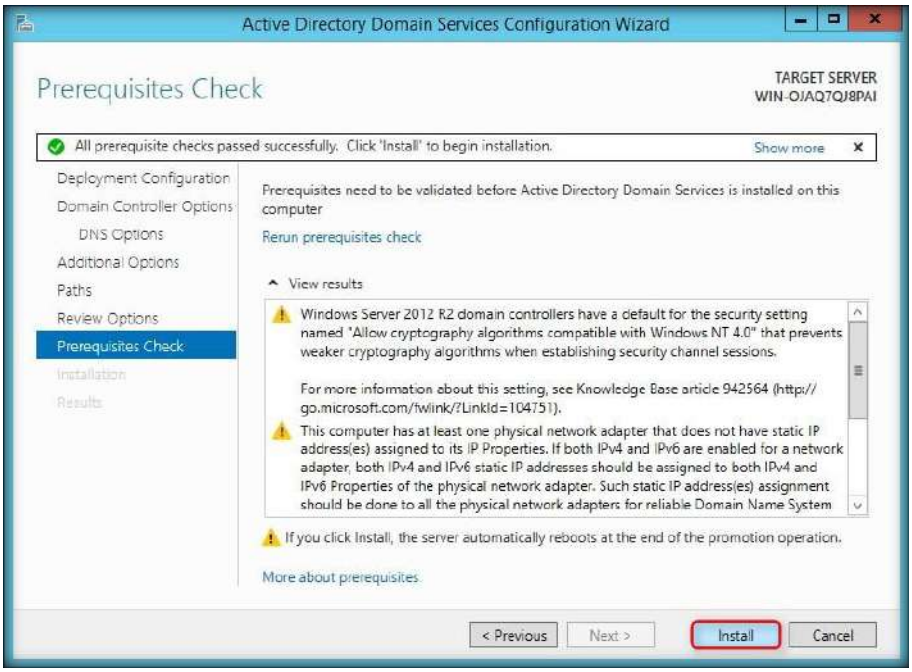
15. Additional Options section appears, verify the NetBIOS domain name is CEH and click **Next**



16. Review Options section appears, click Next

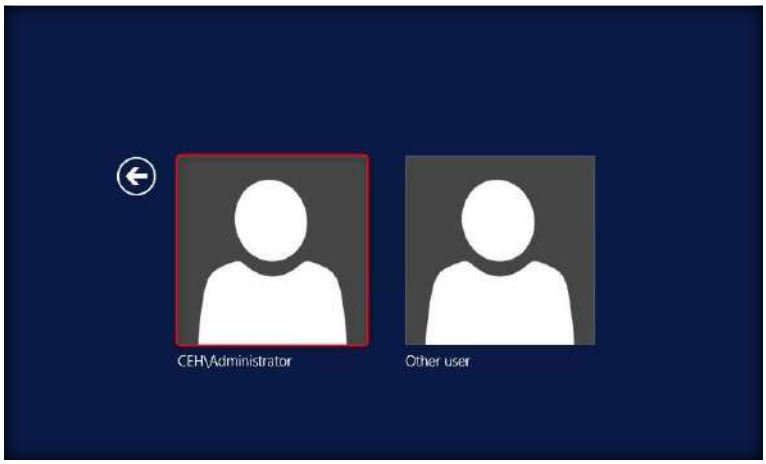


17. In Prerequisites Check section, click **Install**



18. You're about to be signed out pop-up appears click **Close**

19. To login to Windows Server 2012 machine go to Action and click **Ctrl+Alt+Delete** option.



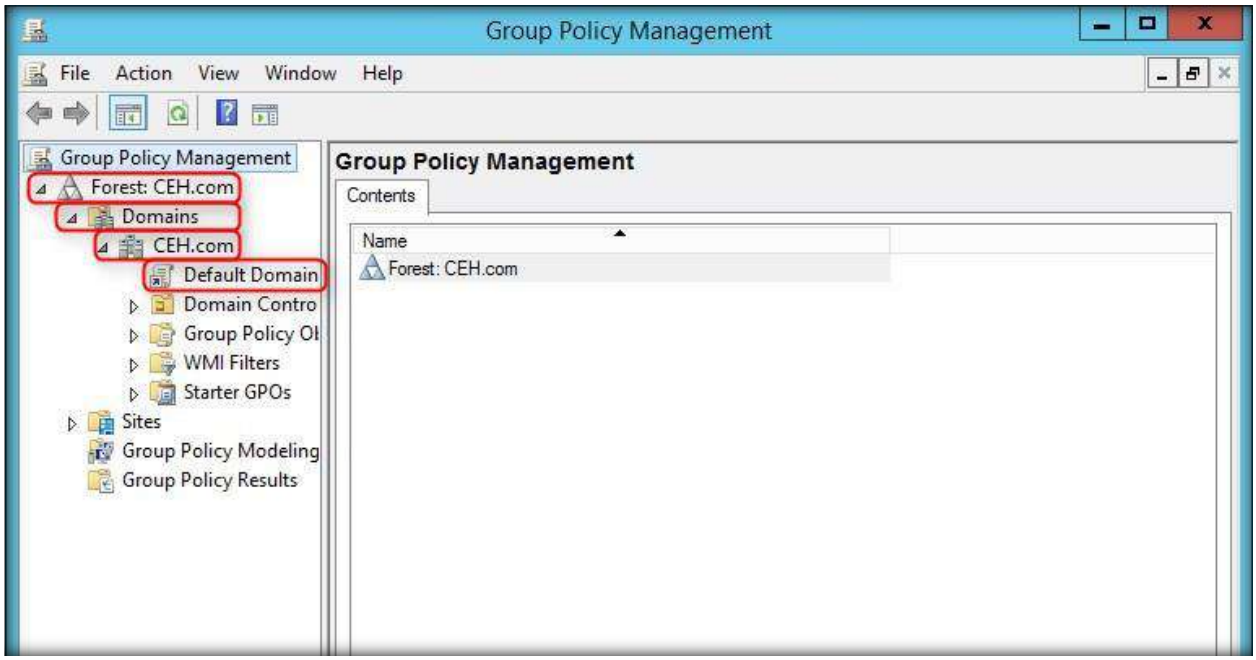
20. Type the password **Pa$$w0rd** and click **Login** button

21. **Close** the Server Manager window once you logged in

Configure Group Policy Management

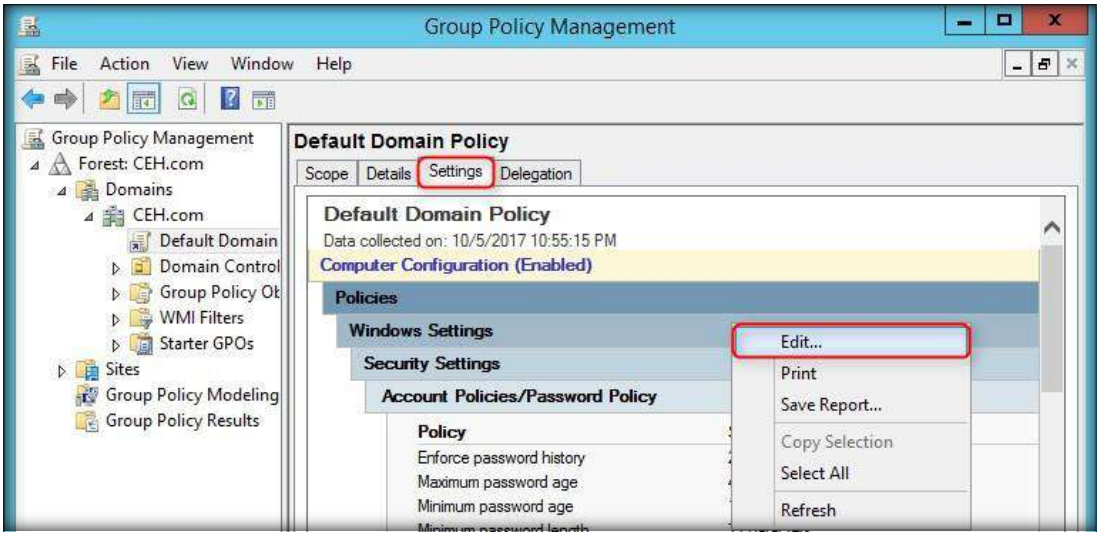
22. Navigate to **Start → Apps → Administrative Tools → Group Policy Management**

23. **Group Policy Management** window appears, expand **Group Policy Management → Forest: CEH.com → Domains → CEH.com** and select **Default Domain**



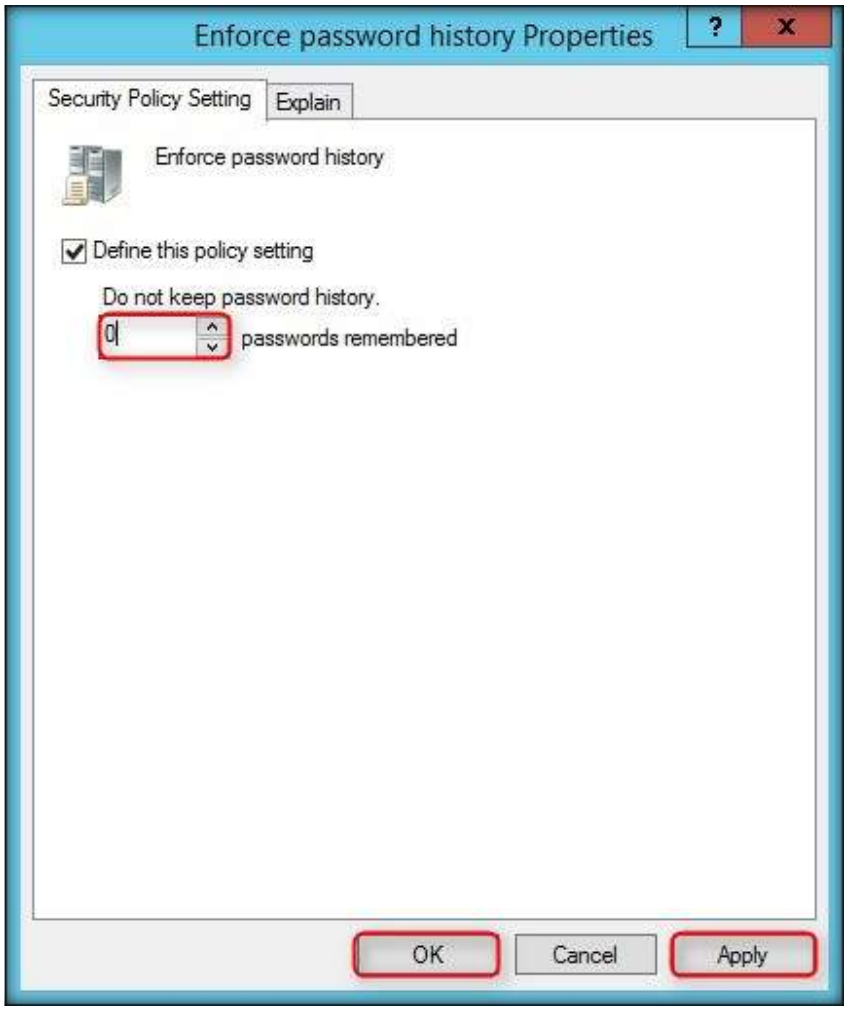
24. **Group Policy Management Console** dialog-box appears, click **OK**

25. **Default Domain Policy** window appears, select **Settings** tab
26. Right-click anywhere in the section, and then select **Edit...** option from the context menu

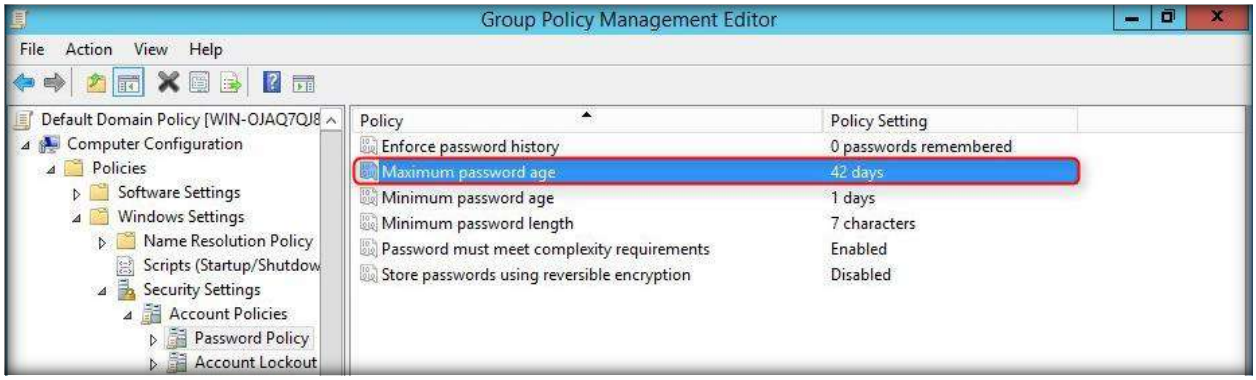


27. **Group Policy Management Editor** window appears, expand **Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies** and select **Password Policy**
28. Password policies appear in the right pane, double-click **Enforce password history**

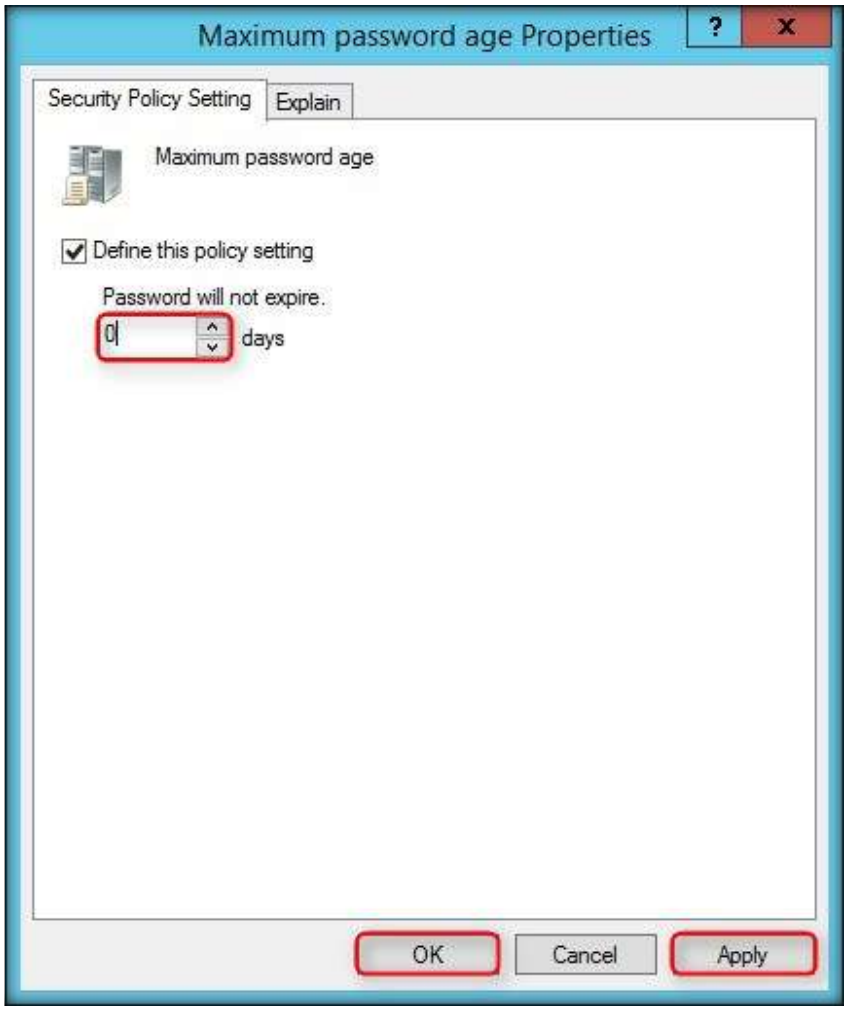
29. **Enforce password history Properties** window appears, type **0** in the **passwords remembered** field; click **Apply**, and then click **OK**



30. Double-click **Maximum password age** option in the right-pane

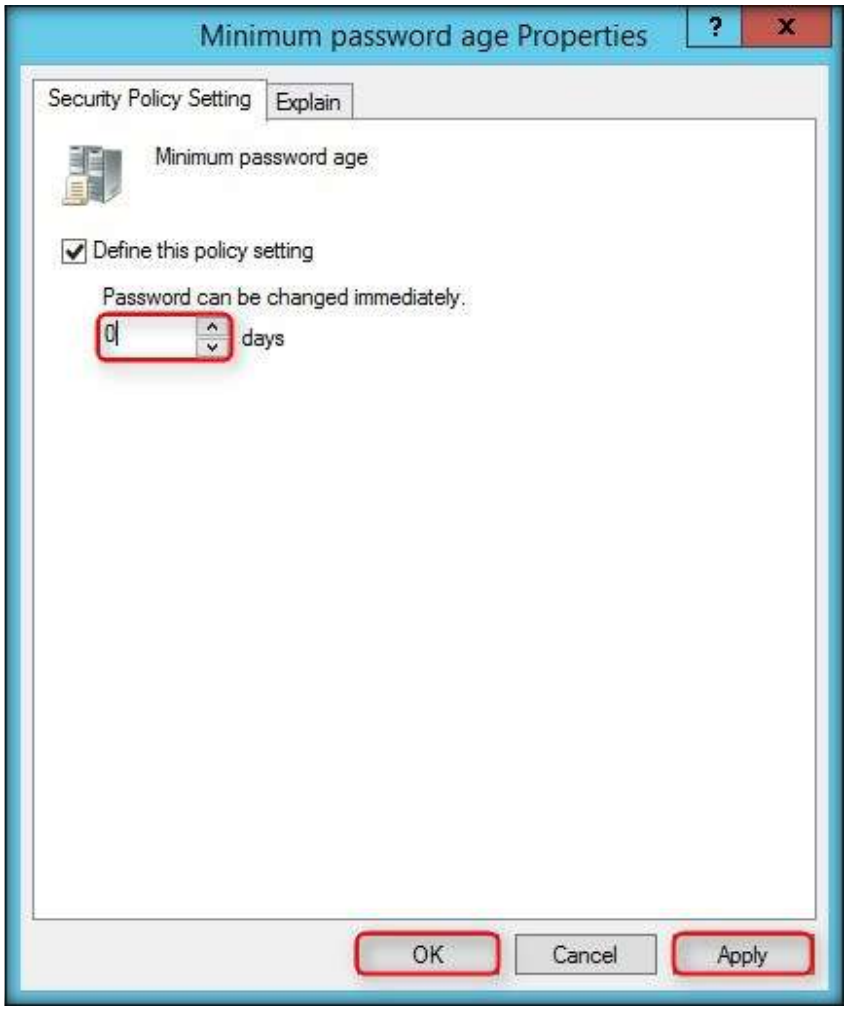


31. **Maximum password age Properties** window appears, type **0** in the **days** field; click **Apply**, and then click **OK**



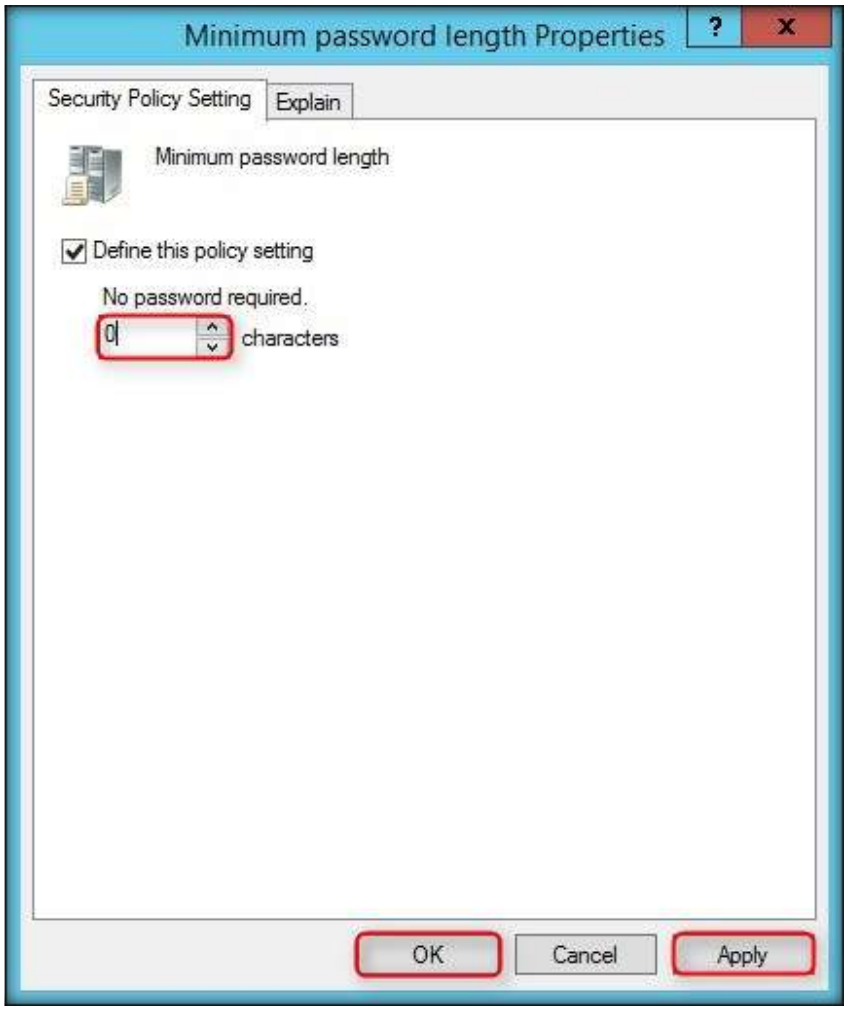
32. Double-click **Minimum password age** option in the right-pane

33. **Minimum password age Properties** window appears, type **0** in the **days** field; click **Apply**, and then click **OK**

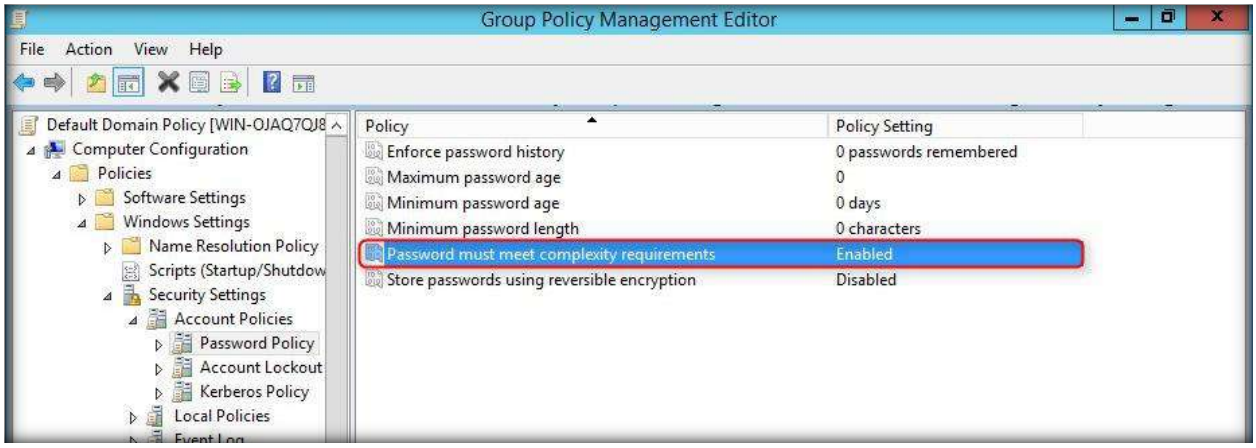


34. Double-click **Minimum password length** option in the right-pane

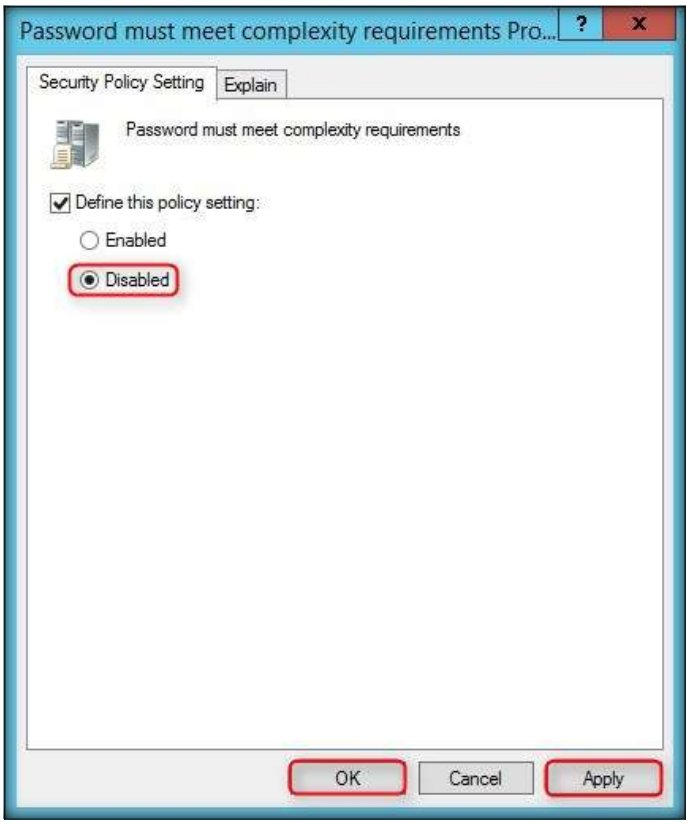
35. **Minimum password lengths Properties** window appears, type **0** in the **characters** field; click **Apply**, and then click **OK**



36. Double-click **Password must meet complexity requirements** option in the right-pane



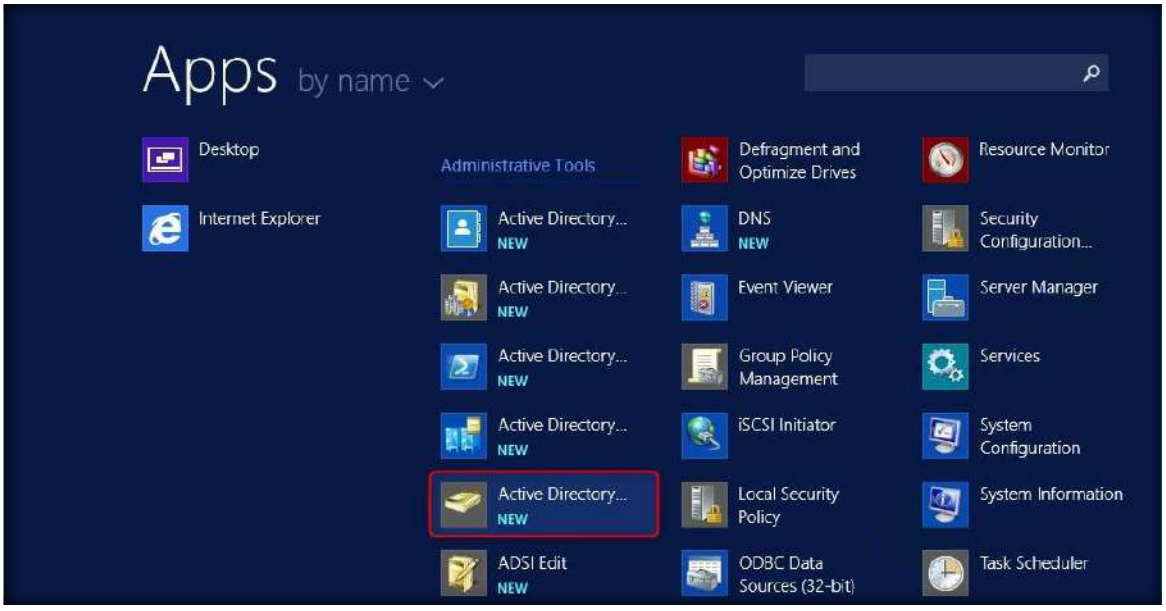
37. **Password must meet complexity requirements Properties** window appears, select **Disabled** radio button; click **Apply**, and then click **OK**



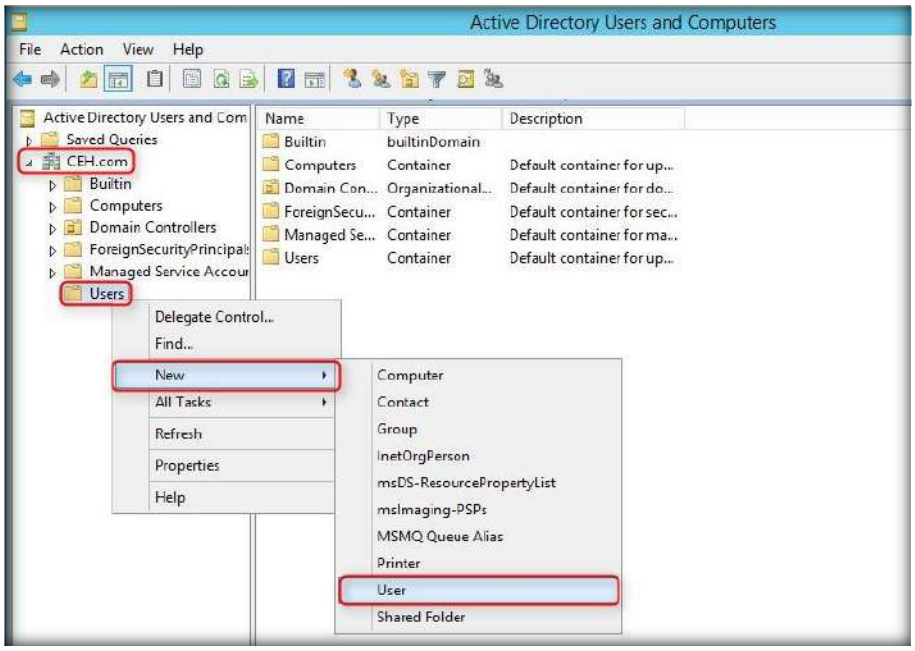
38. Once done, close all the windows

Create User Accounts and Configure Them

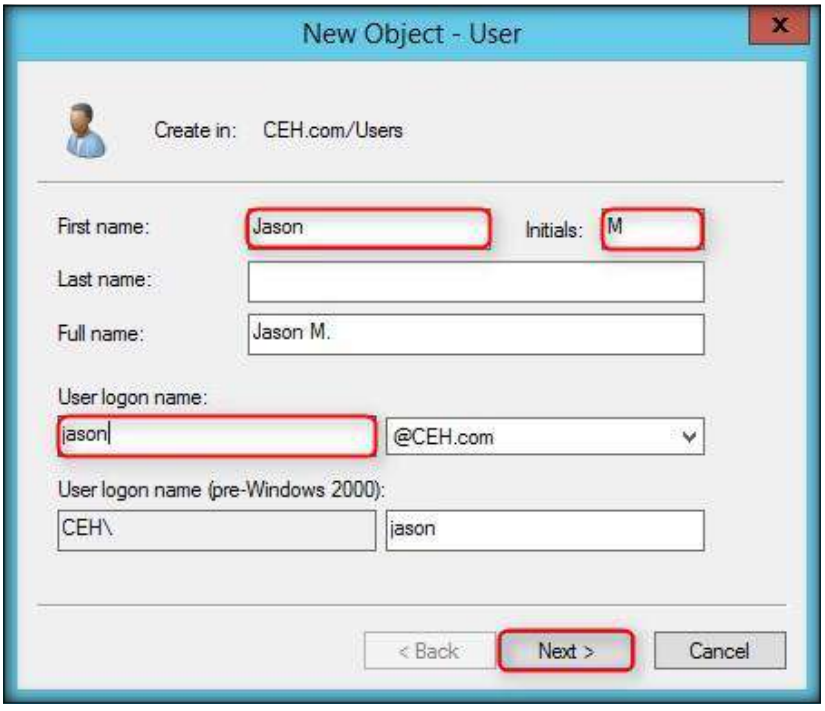
39. Now navigate to **Start → Apps → Administrative Tools → Active Directory Users and Computers**



40. In Active Directory Users and Computers expand **CEH.com** node and right-click **Users** and click **New** and **User** from the context menu as shown in the below figure.

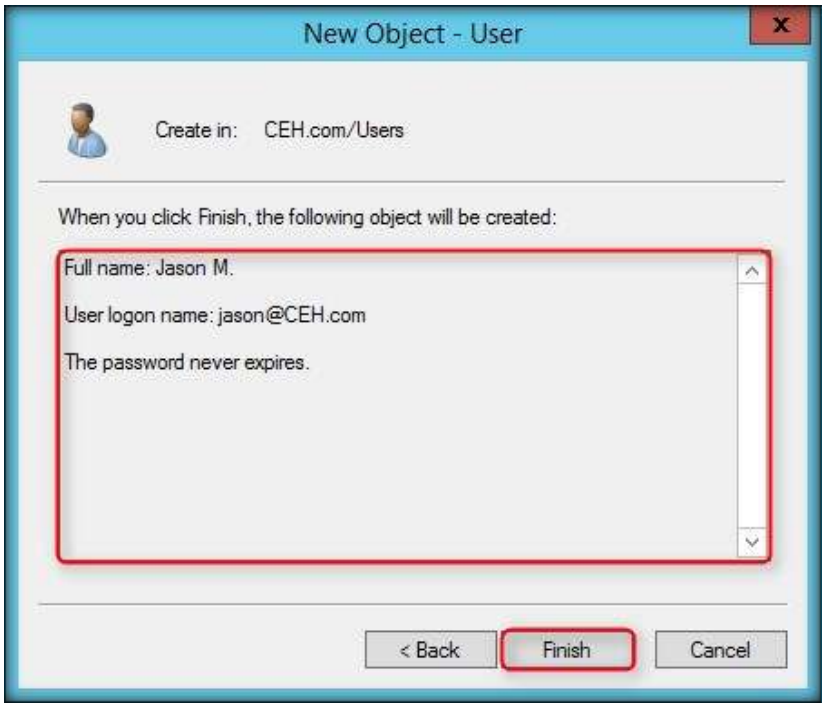


41. **New Object** - **User** dialog box appears fill in the required fields
42. Type **Jason** in First name: field, Initial of your choice, type **jason** in **User logon name:** field and click **Next**

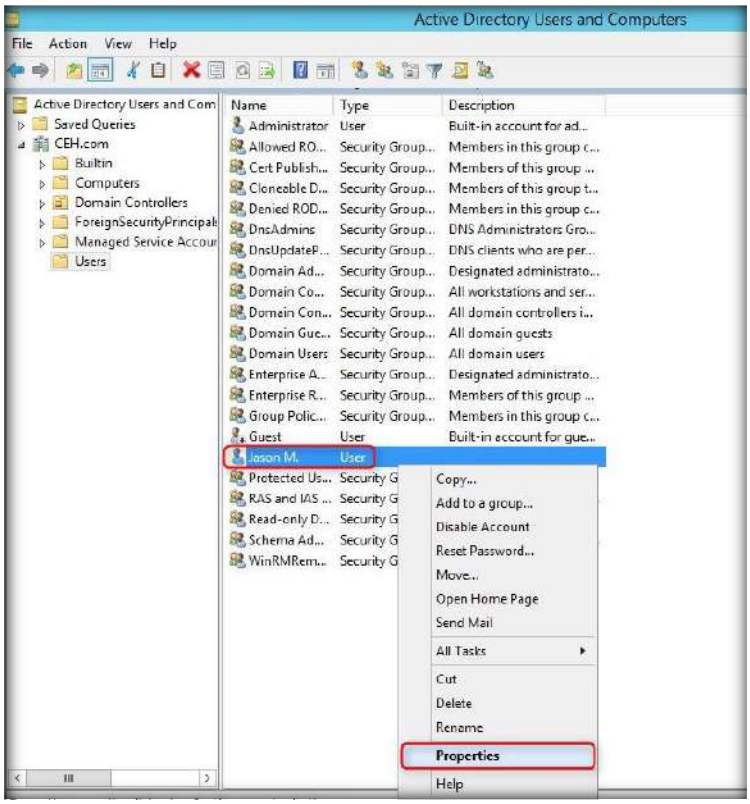


43. Type **qwerty** in Password and Confirm password fields and uncheck User must change password at next logon and check Password never expires option and click **Next**

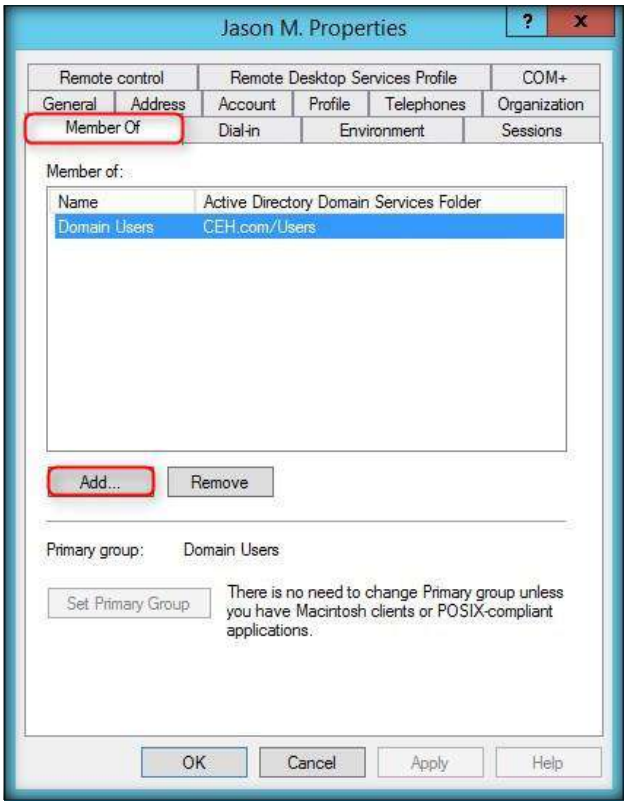
44. Once **User** is successfully created click **Finish**



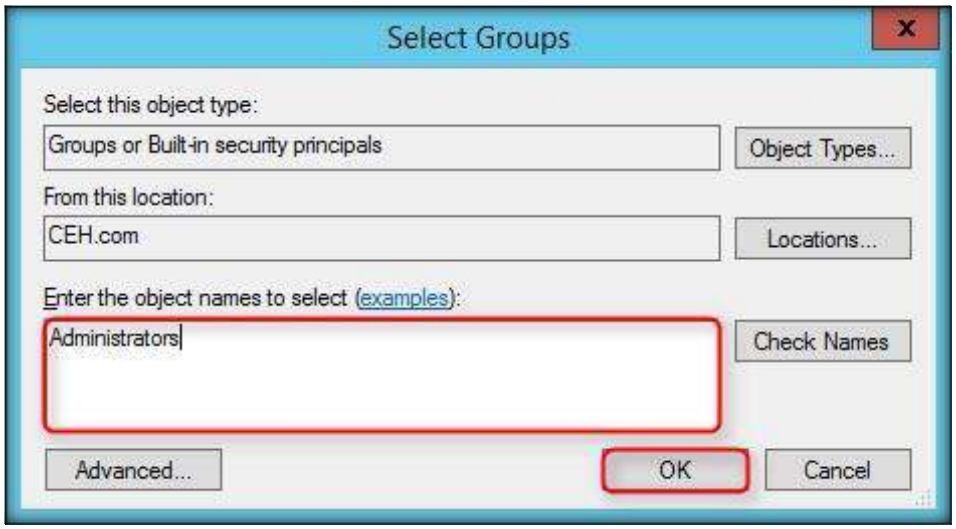
45. Now right-click on created user and click **Properties** from the context menu



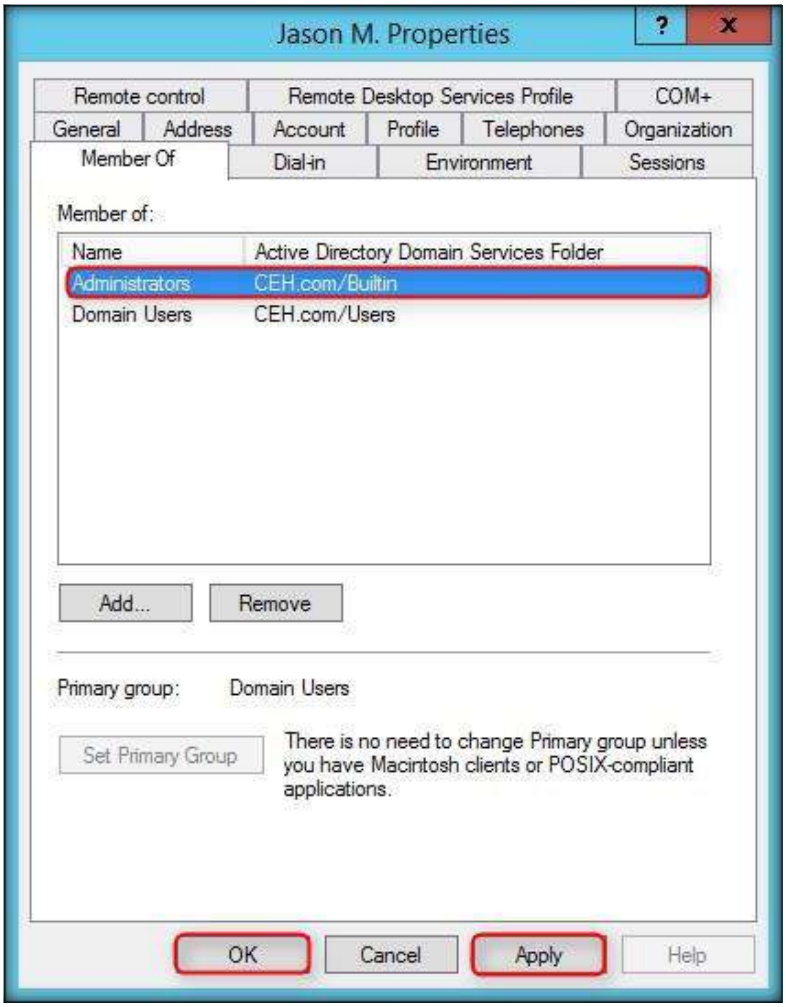
46. In select user properties click **Member Of** tab and click **Add** button



47. In Select Groups wizard type **Administrators** and click **OK**. This will make the user as member of the Administrators



48. Click **Apply** and **OK** in the Users Properties

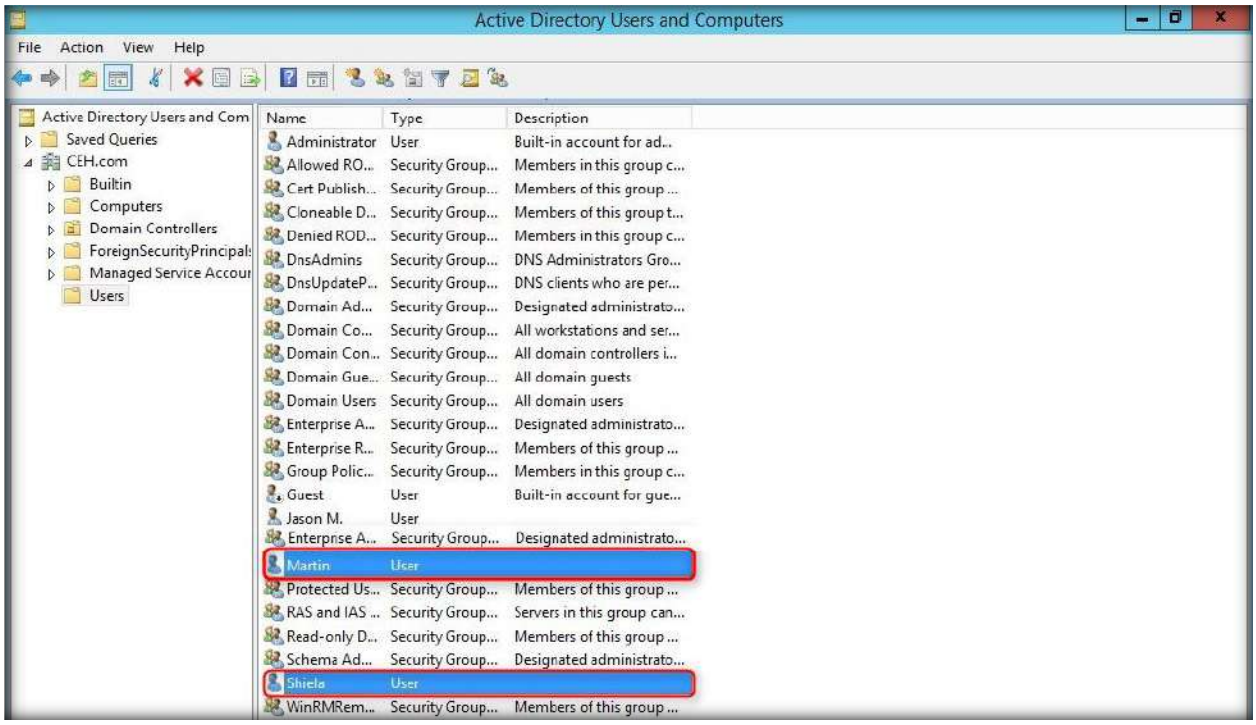


49. Similarly create the following users in Active Directory by following the steps **40** to **44**

    I. Username: **Martin**; Password: **apple**

    II. Username: **Shiela**; Password: **test**

Note: You may assign admin privileges to any of these accounts as well, by following the steps **45** to **48**.



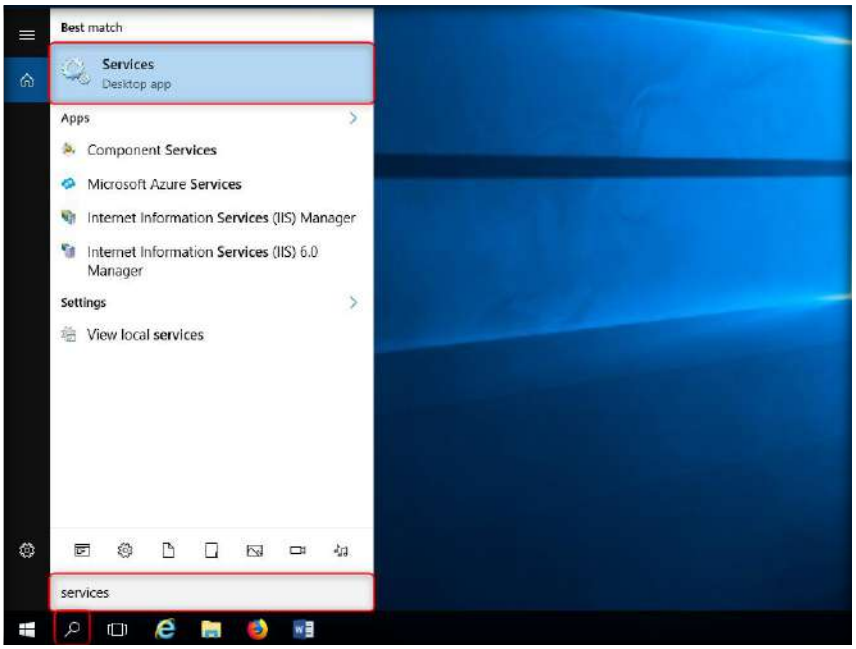
[Back to Configuration Task Outline]

CT#21: Configure SNMP Service in Windows Server 2016 and Windows Server 2012

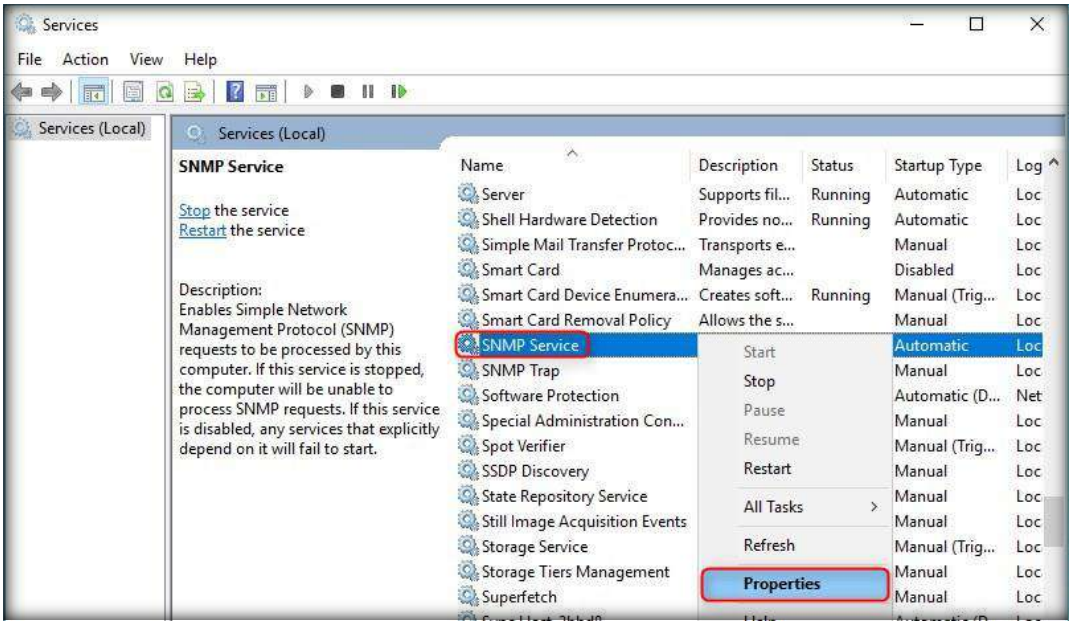
Configuring SNMP Service in Windows Server 2016

As you have already installed SNMP service in Windows Server 2016 virtual machine, you just need to configure it in this machine. For this, launch **Services**.

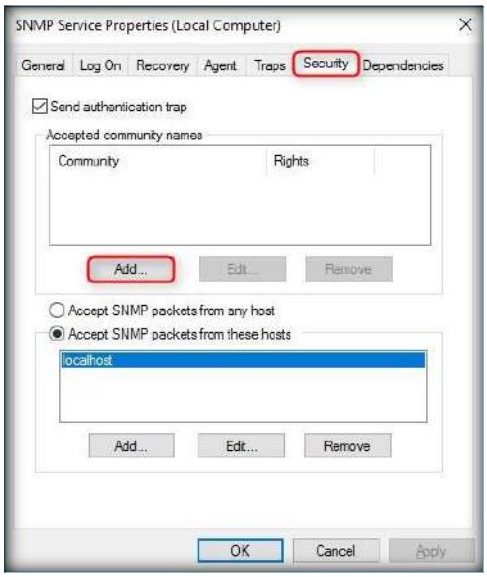
1. Click the **Search** icon in the taskbar and type **services** in the search field. Click the **Services** Desktop app



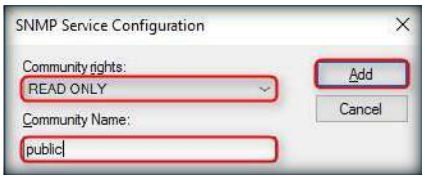
2. Services window appears, right-click **SNMP Service** and click **Properties** from context menu



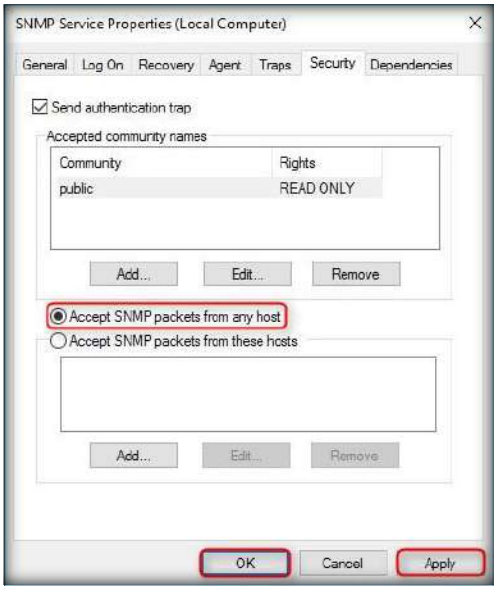
3. Click **Security** tab in **SNMP Service Properties** wizard and click **Add** button under **Accepted community names** section



4. SNMP Service Configuration wizard appears, Community Rights should **READONLY**, and in Community Name section type **public** (lowercase only) and click **Add** button



5. After adding Accepted community name details, select **Accept SNMP packets from any host** radio button, click **Apply** and then click **OK**



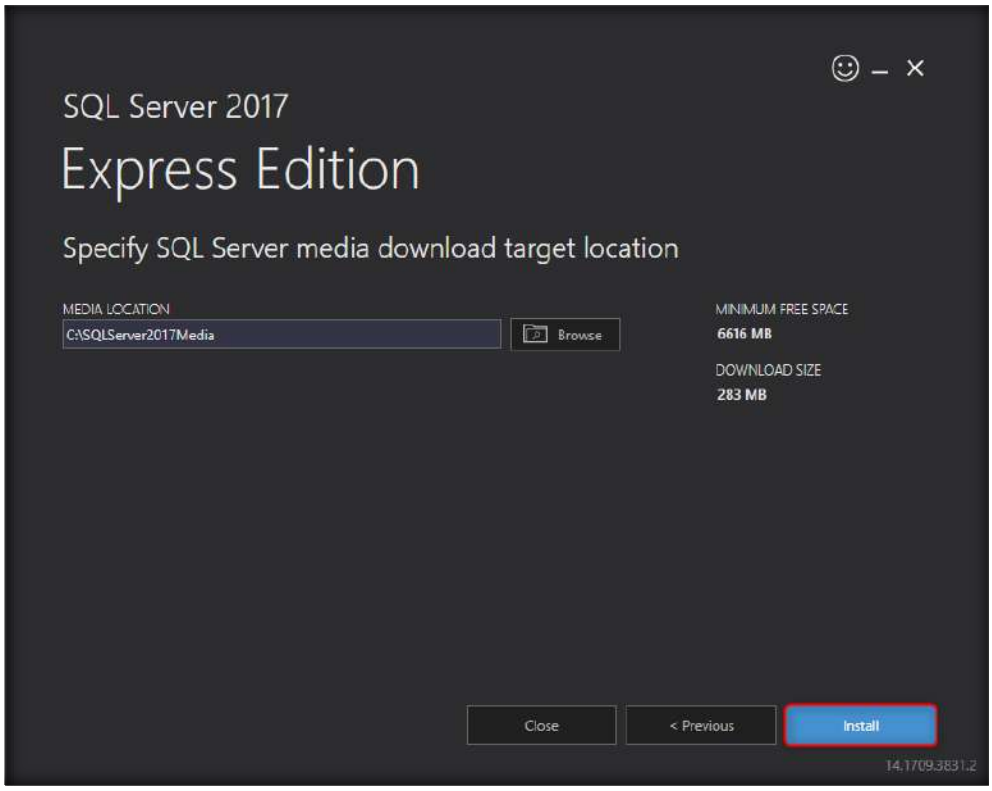
6. Follow the same steps to configure the SNMP service in Windows Server 2012

[Back to Configuration Task Outline]

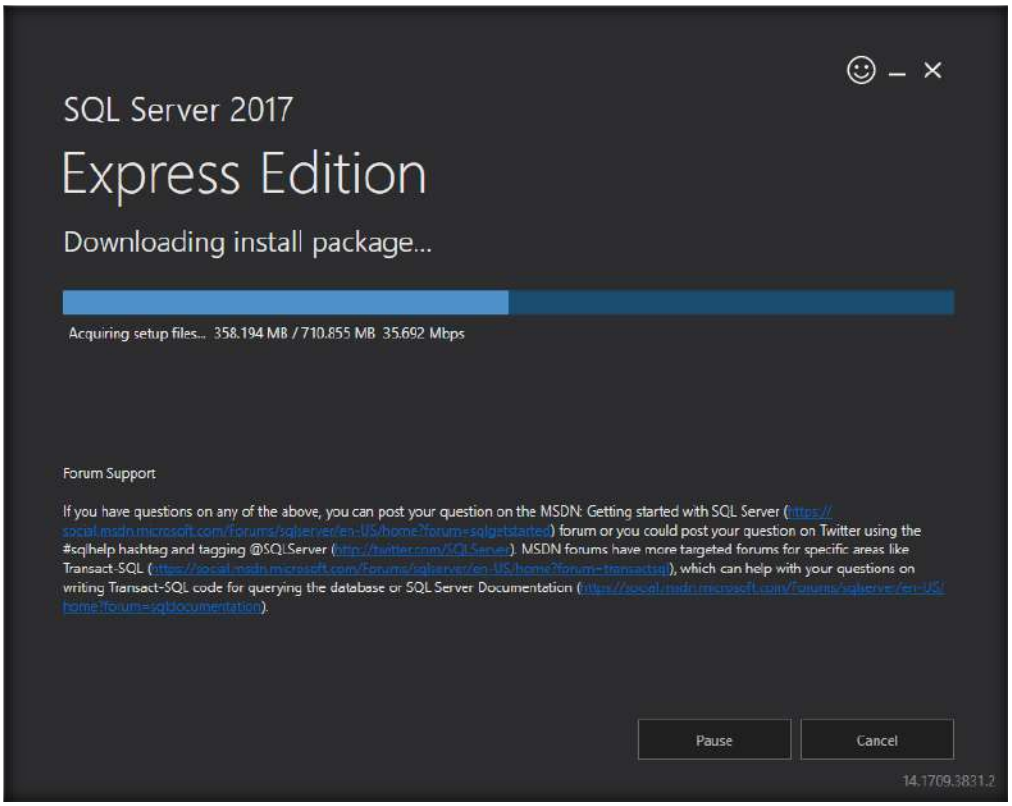
CT#22: Install MS SQL Server 2017 Express Edition on Windows Server 2016 Virtual Machine

1. Navigate to **Z:\CEH-Tools\CEHv10 Lab Prerequisites\SQL Server** and double-click **SQLServer2017-SSEI-Expr.exe**
2. If a User Account Control pop-up appears, click **Yes**
3. SQL Server 2017 window appears click **Custom**

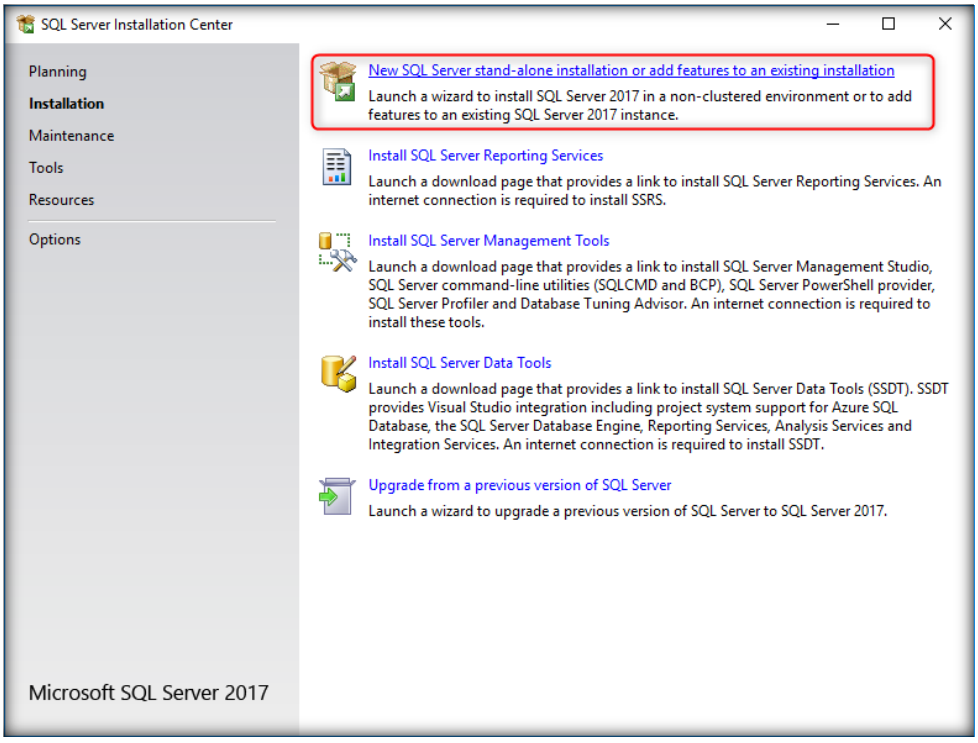
4. Specify SQL Server media download target location section appears, click **Install**



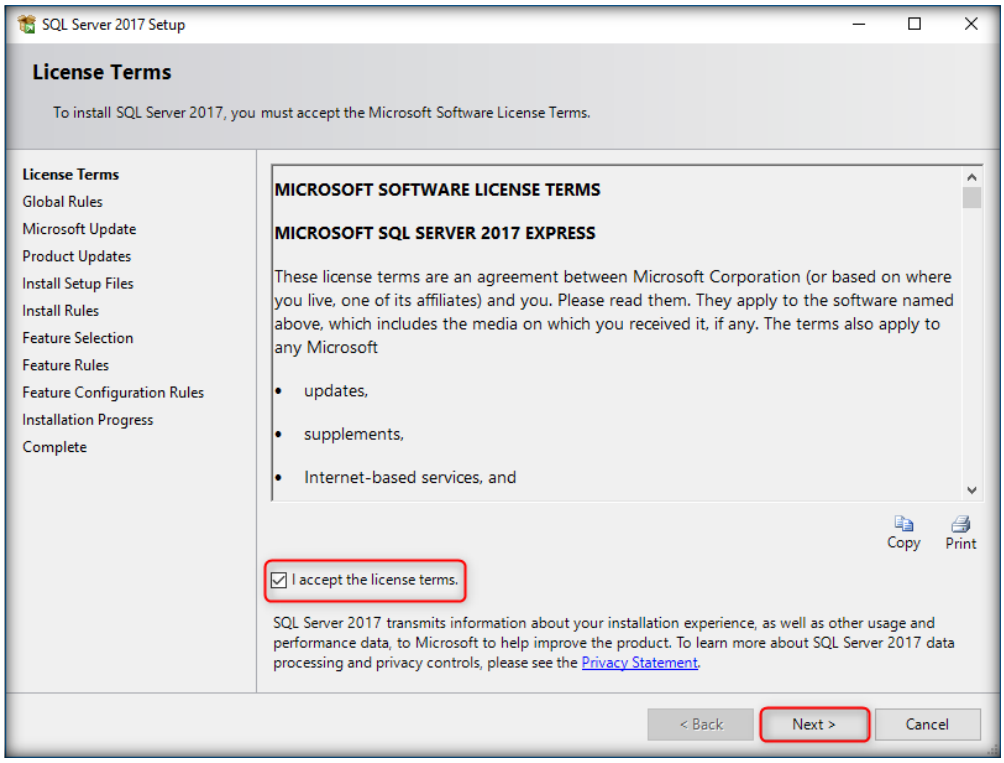
5. The program starts downloading the setup files, wait for the Installation Center to launch



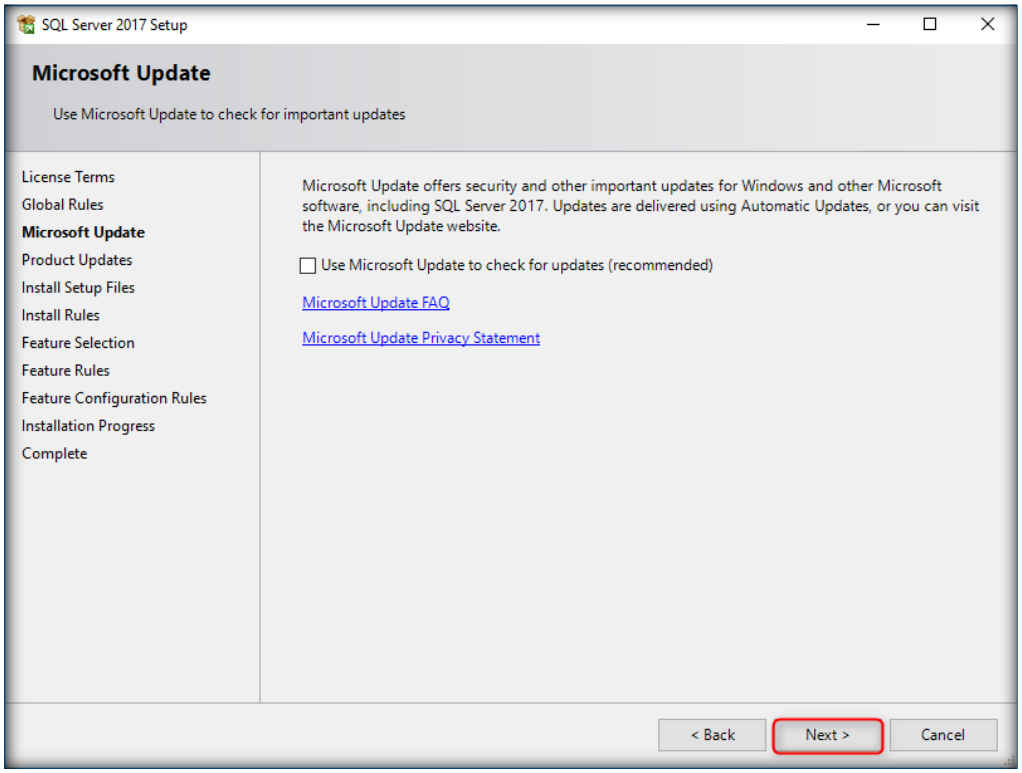
6. SQL Server Installation Center window appears with **Installation** section displayed by default, click **New SQL Server stand-alone installation or add features to an existing installation** link and wait for some time



7. Read the Software License Terms in the **License Terms** section, check the option **I accept the license terms** and click **Next**

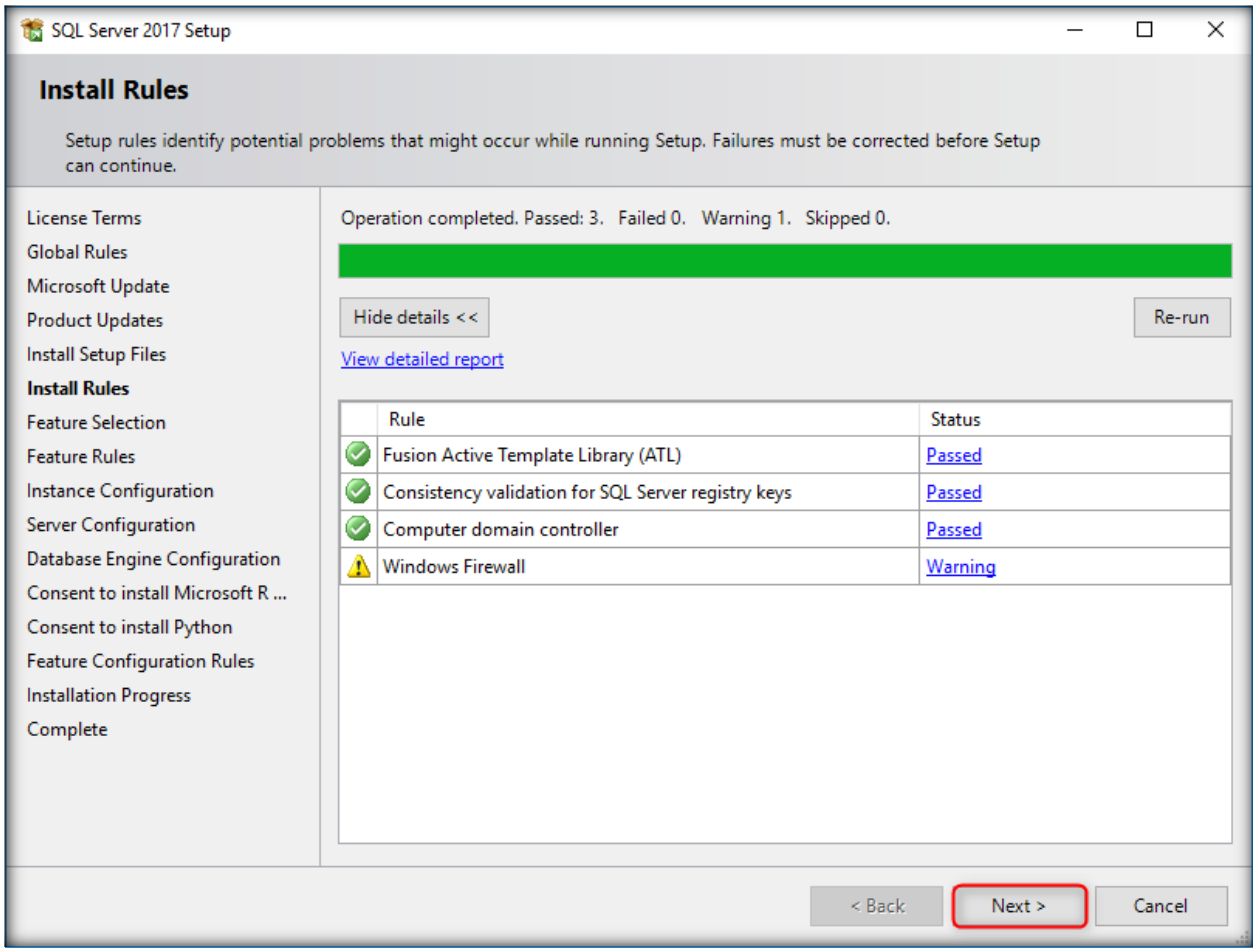


8. SQL Server 2017 Setup **Microsoft Update** section appears, click **Next**



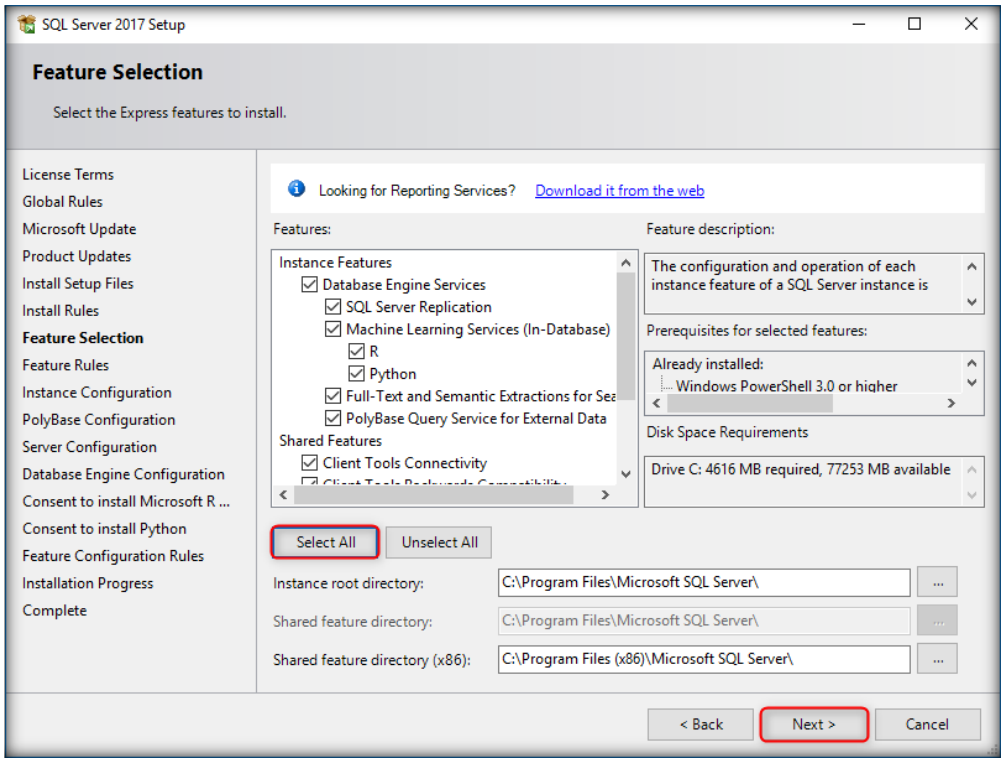
9. The **Install Rules** verifies the system state of your computer before Setup continues

10. After verification is finished, click **Next**

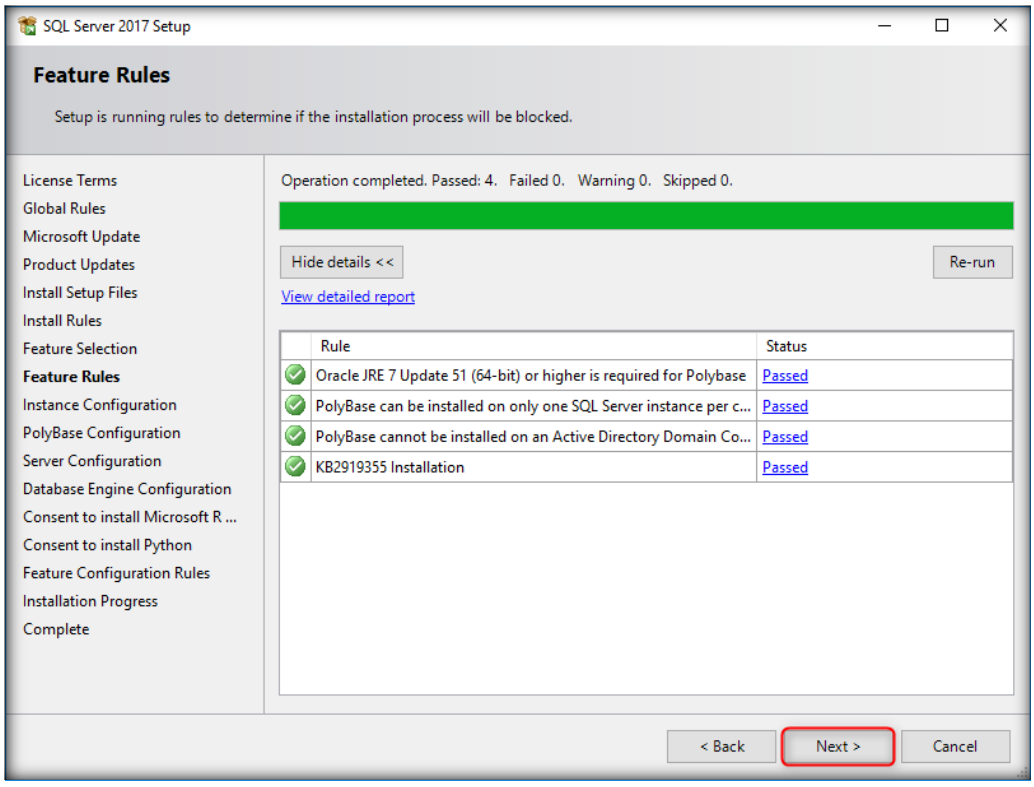


11. On the **Feature Selection** window, select the **Features** for installation (**Select All**)
12. A **description** for each feature group appears in the **right pane** after you select the feature
13. You can select any **combination** of check boxes
14. To change the **installation path** for shared components, either **update** the path in the field for Shared feature directory/Shared feature directory (x86), or click **Browse** button to select another installation directory
15. The default installation path for Shared feature directory is **C:\Program Files\Microsoft SQL Server**
16. The default installation path for Shared feature directory (x86) is **C:\Program Files (x86)\Microsoft SQL Server**

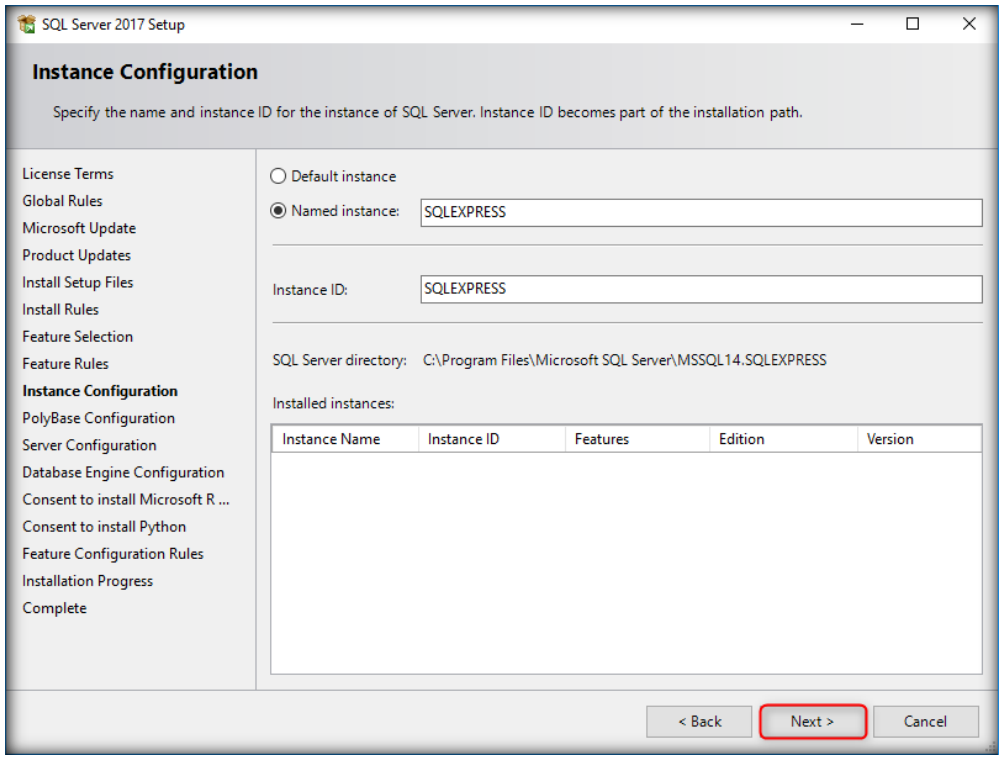
17. Click **Next**



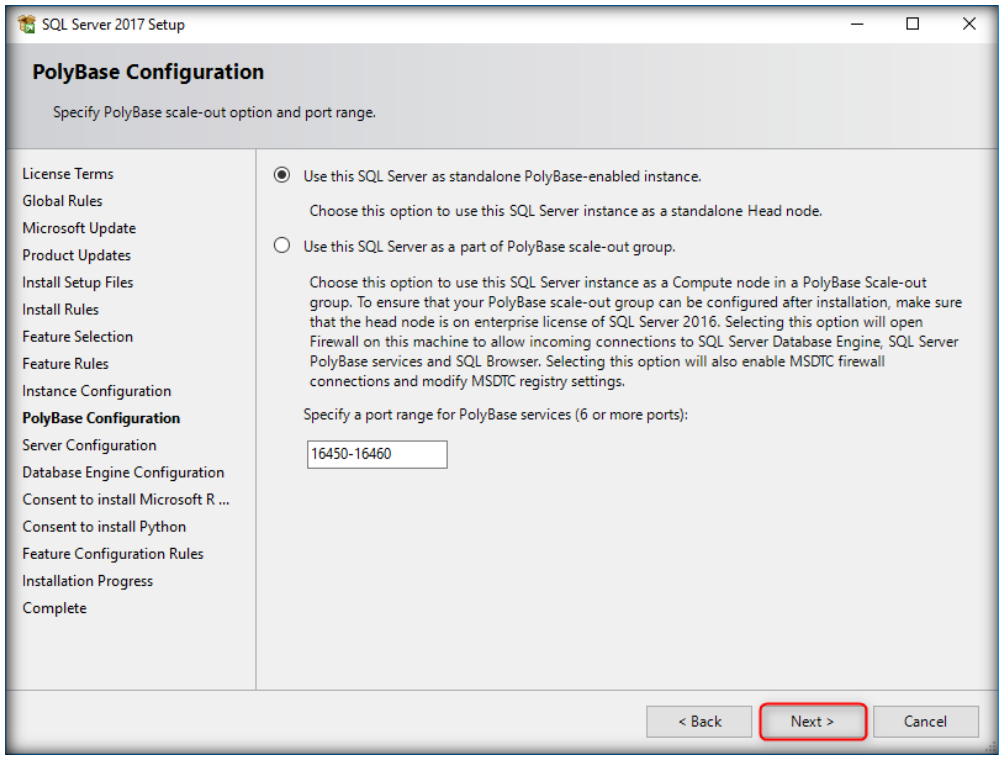
18. **Feature Rules** section appears, and verifies the prerequisites for the installation.
19. If all the prerequisites are present, click **Next**



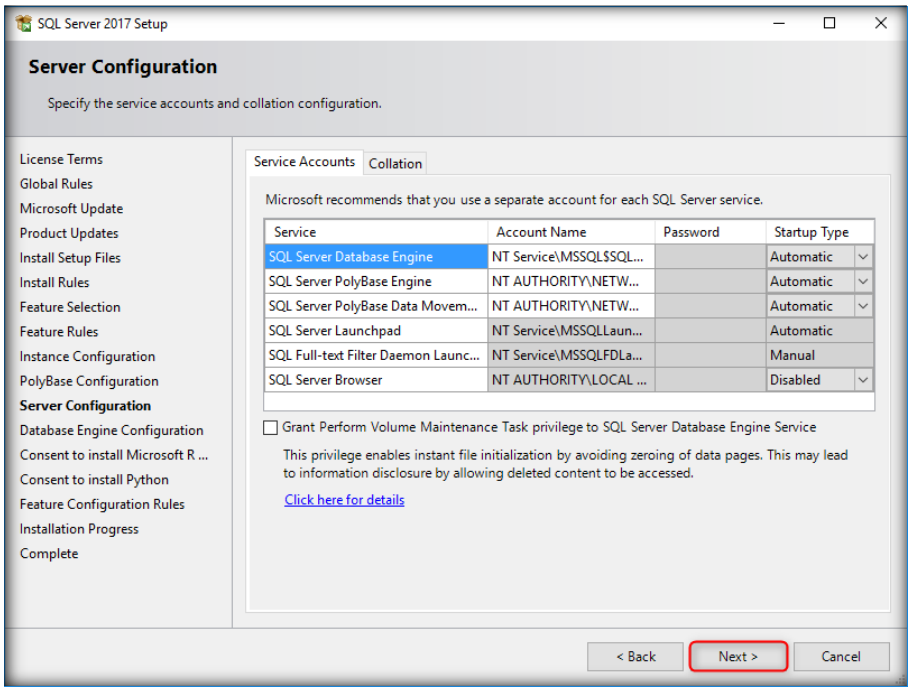
20. In the **Instance Configuration** section, check that **Named instance** is specified, leave the **Instance ID** and **Instance root directory** options set to default, and click **Next** to continue



21. **PolyBase Configuration** section appears, select **Use this SQL Server as standalone PolyBase-enabled instance** option and click **Next**

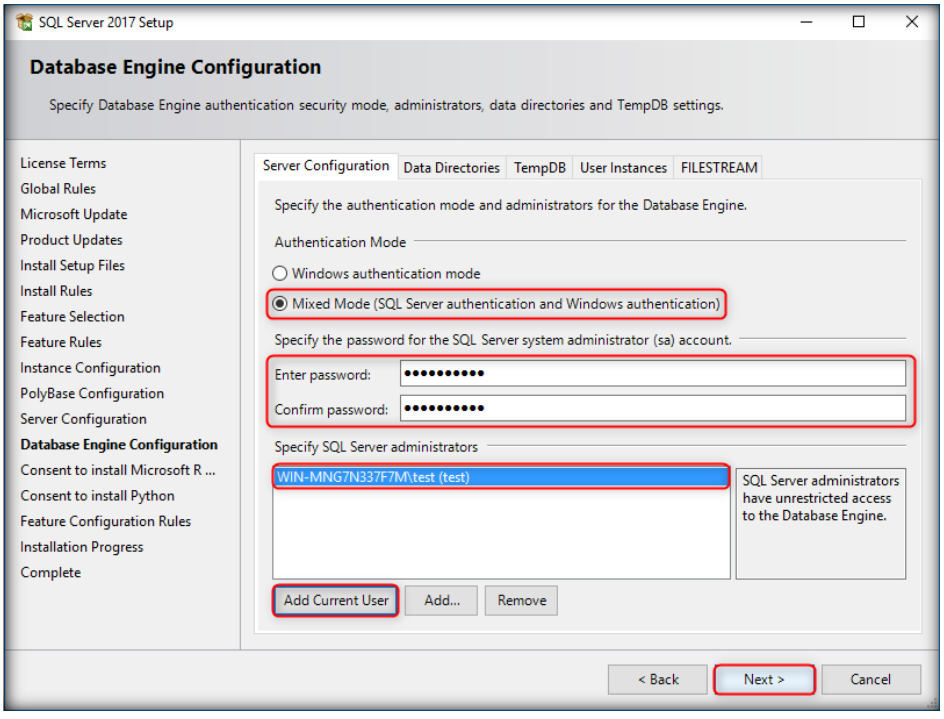


22. **Server configuration** section appears, leave the Account Names and Passwords set to default and click **Next**

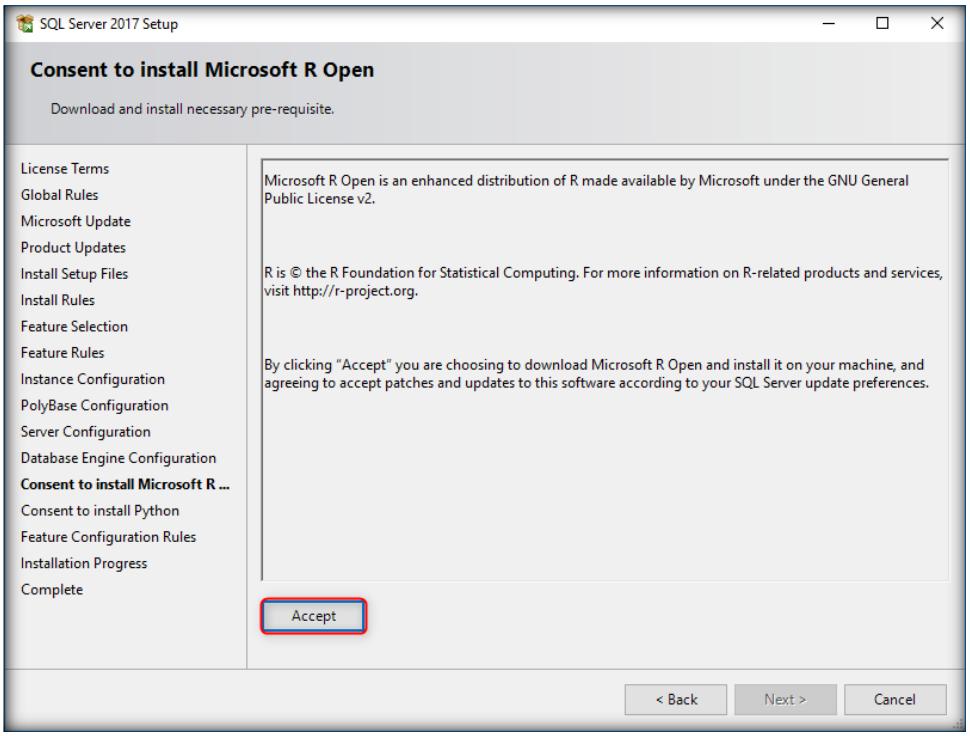


23. **Database Engine Configuration** section appears, select **Mixed Mode (SQL Server authentication and Window authentication)** radio button and input the password **qwerty@123** in both **Enter password** and **Confirm password** text fields

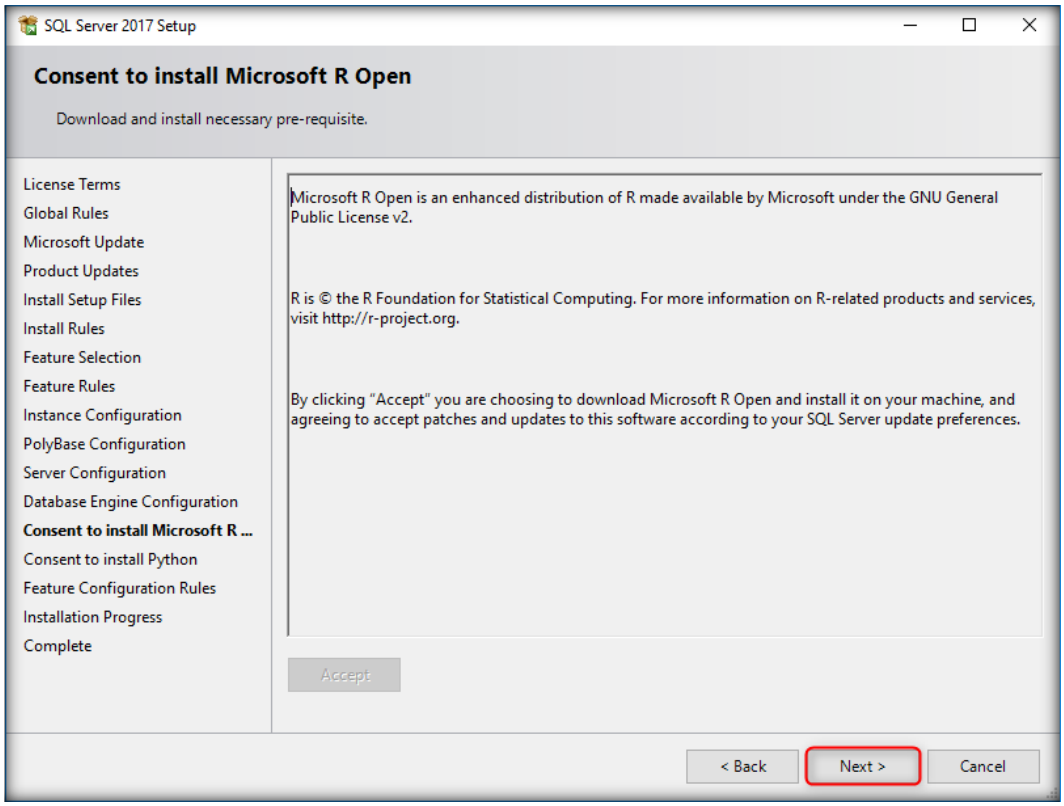
24. Click **Add Current User** button. You are added as the user (here, test) and is displayed under **Specify SQL Server administrators**. Click **Next**



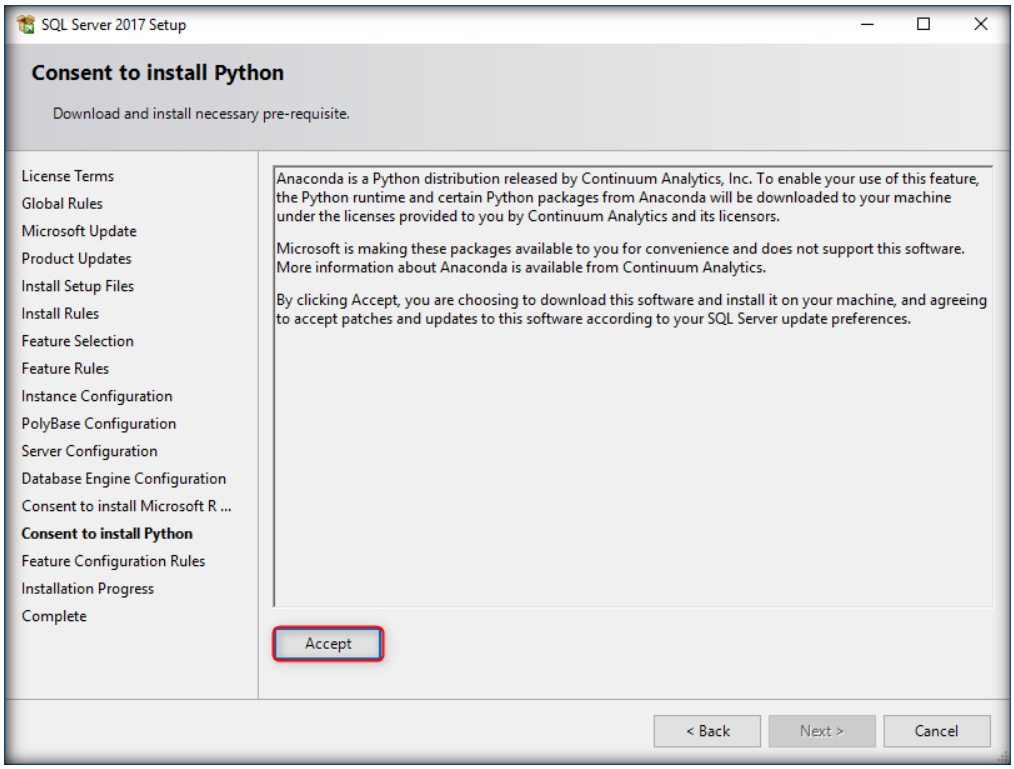
25. **Consent to install Microsoft R Open** section appears, click the **Accept** button



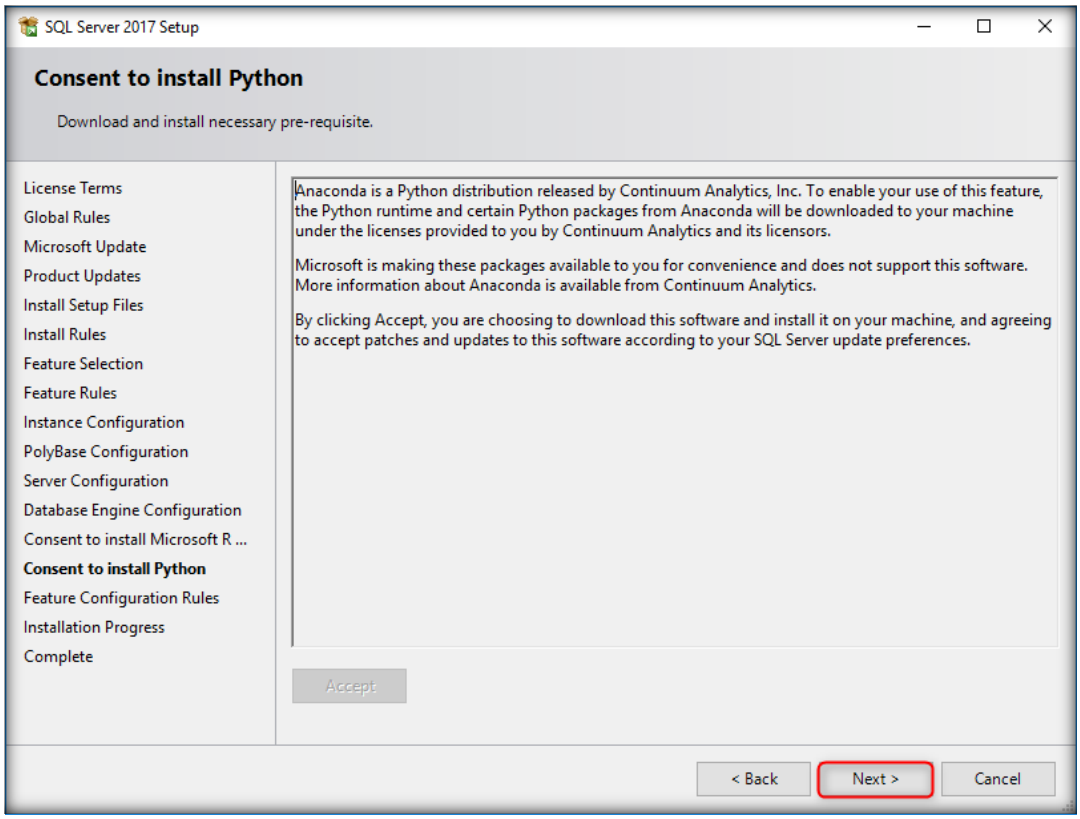
26. In the **Consent to install Microsoft R Open** section wait for the **Next** button to be active and then click it



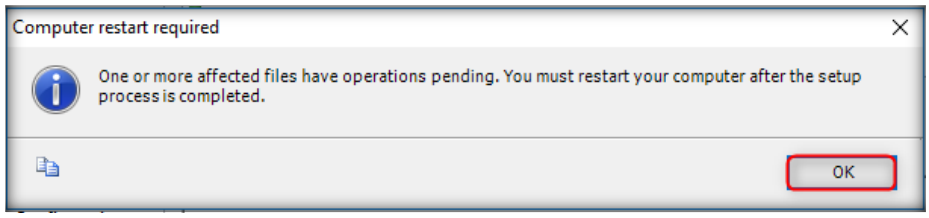
27. **Consent to install Python** section appears, click the **Accept** button



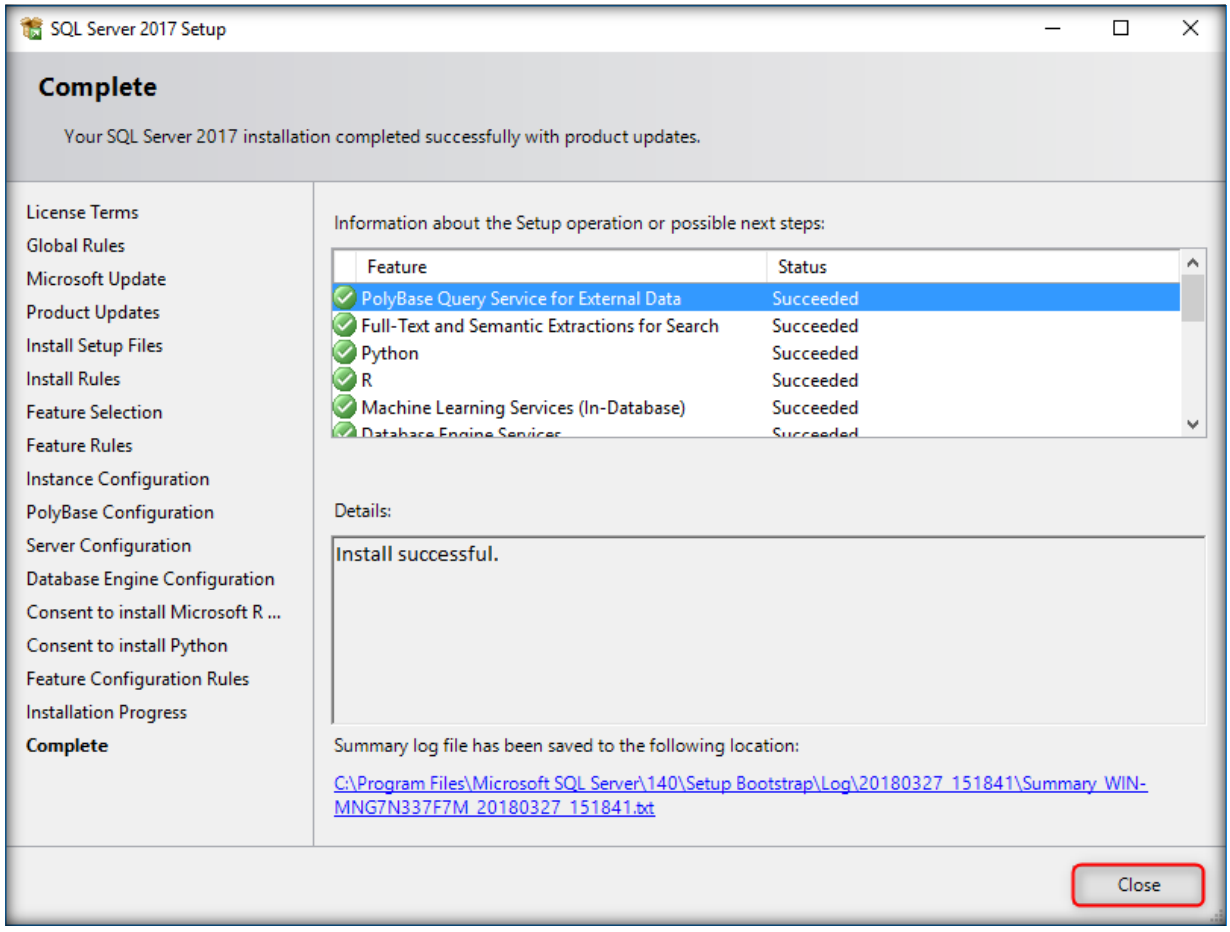
28. **In the Consent to install Python** section wait for the **Next** button to be active and then click it



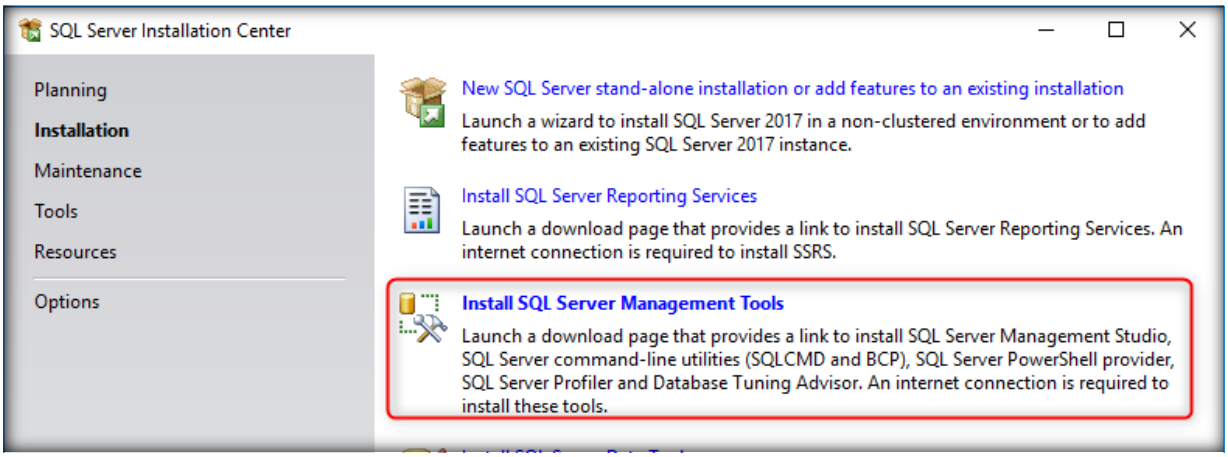
29. The setup starts to install the SQL server, showing you the progress in the **Installation Progress** section.
30. Wait for the installation to complete
31. Computer restart required pop-up appears, click **OK**



32. **Complete** window appears, providing a link that redirects to the location of the **summary log file** for the installation and other **important notes**
33. Click **Close** to finish the installation setup

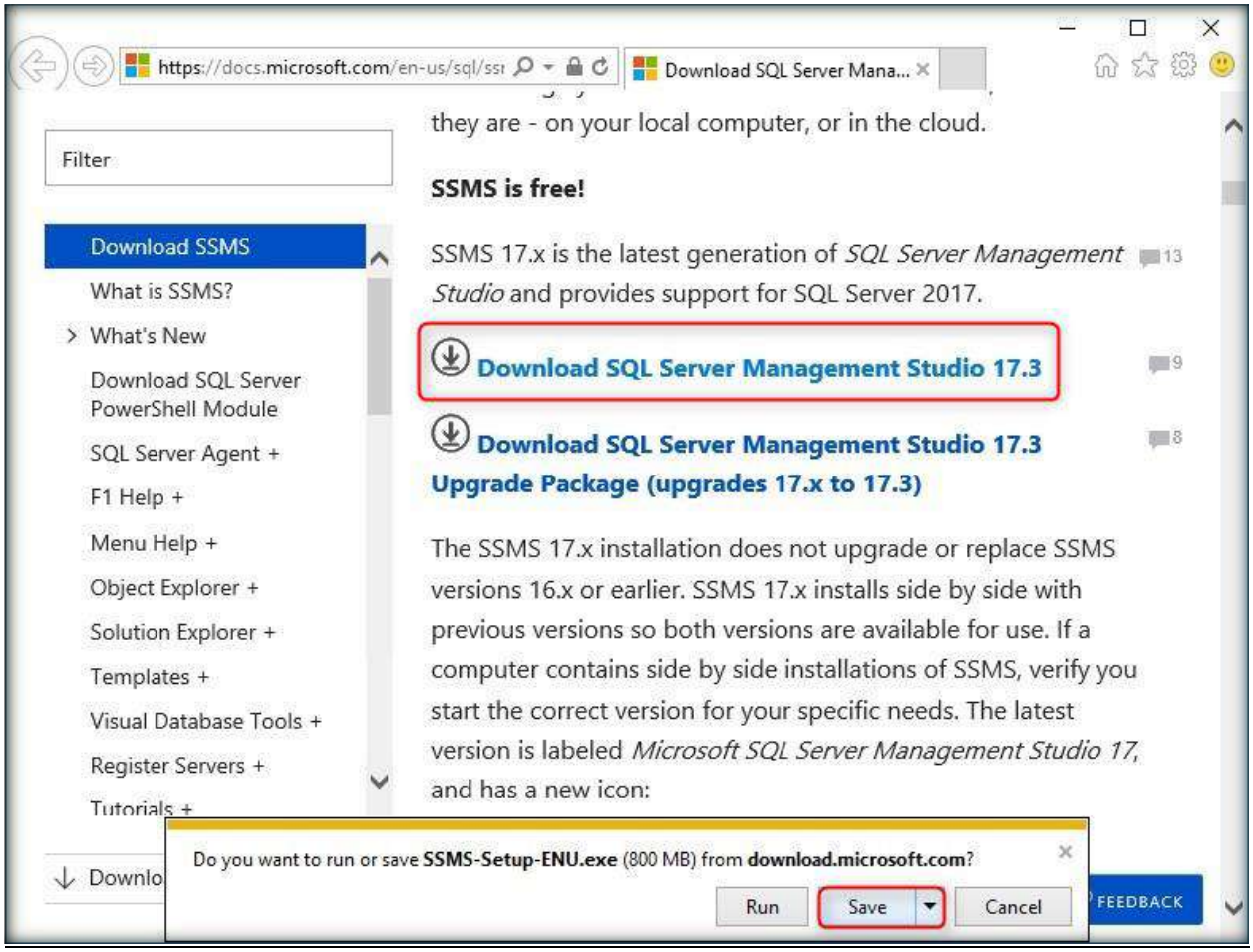


34. Open the SQL Server Installation Center window and click **Install SQL Server Management Tools** link

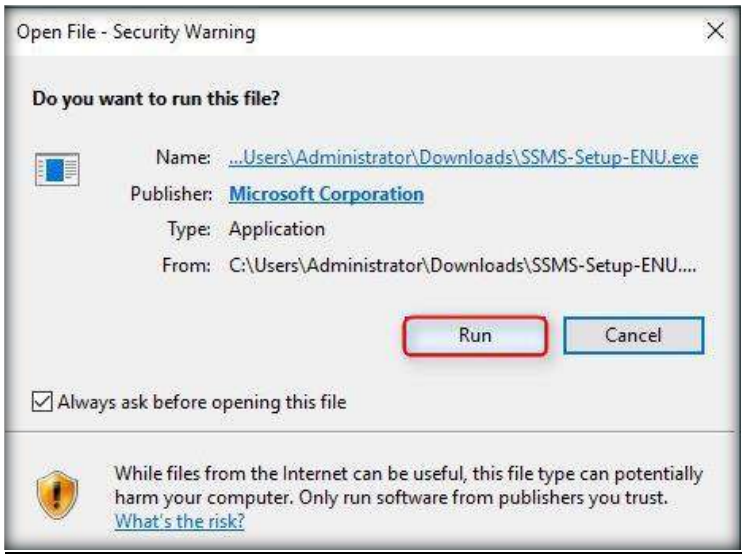


35. The link opens in your browser, click **Download SQL Server Management Studio 17.3** and save the file in your system

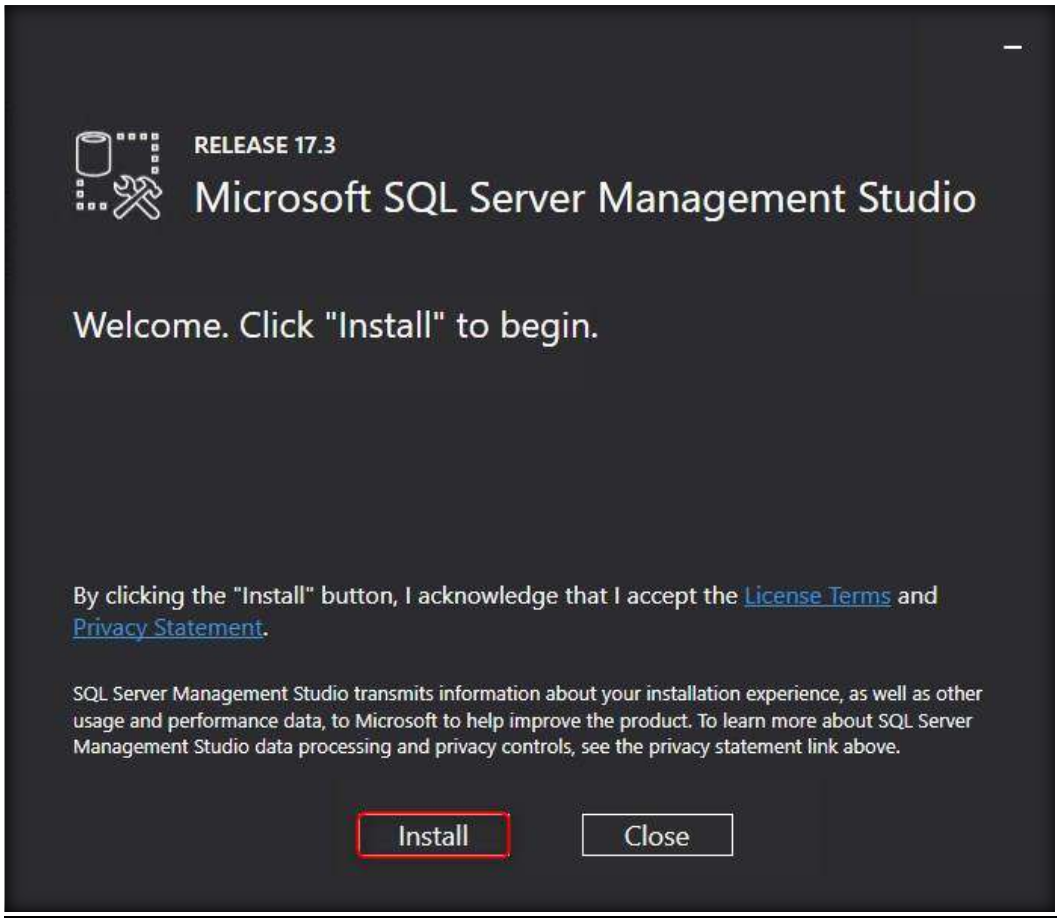
Note: The software version may vary in your lab environment



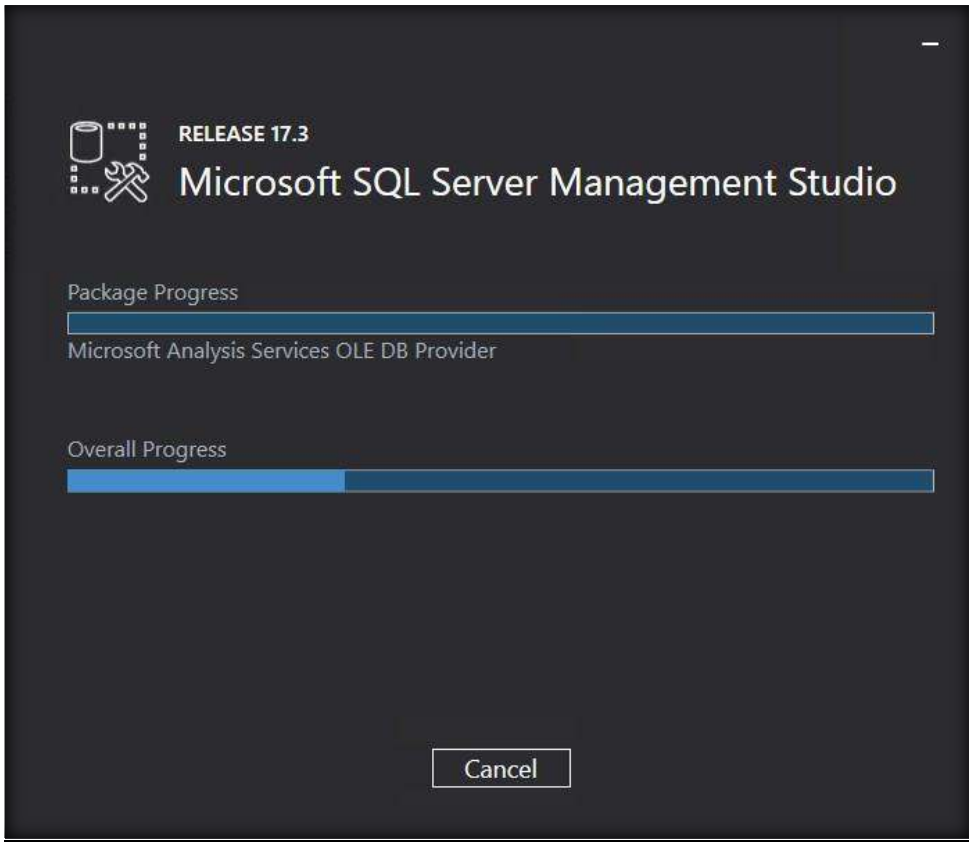
36. Open your downloads folder and double-click the application downloaded in the previous step. Click **Run** if security waring pop-up appears



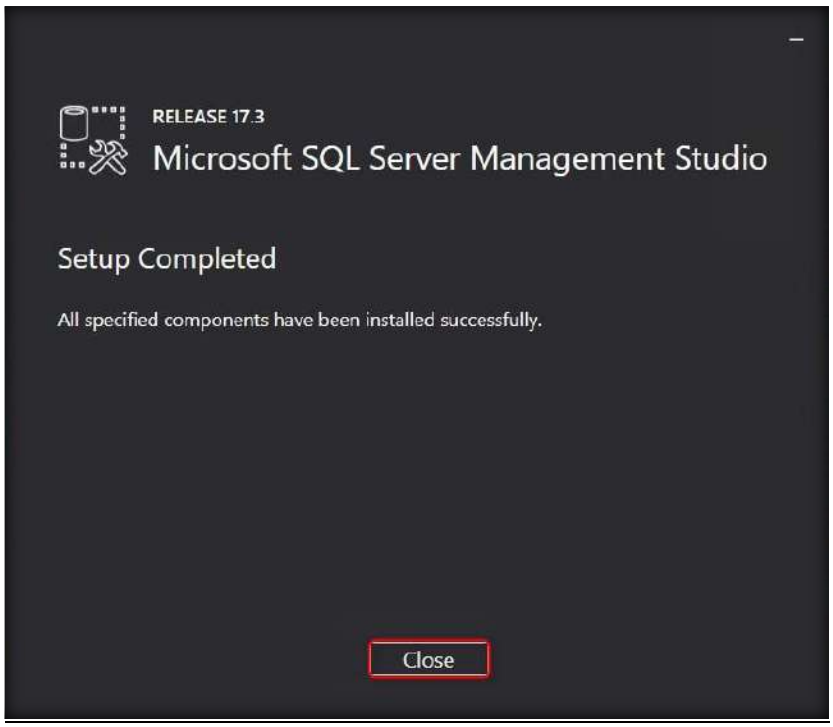
37. Microsoft SQL Server Management Studio welcome screen appears, click **Install** to begin the setup



38. Microsoft SQL Server Management Studio begins the setup. Wait for the setup to finish



39. Microsoft SQL Server Management Studio Setup Completed screen appears, click **Close** to finish



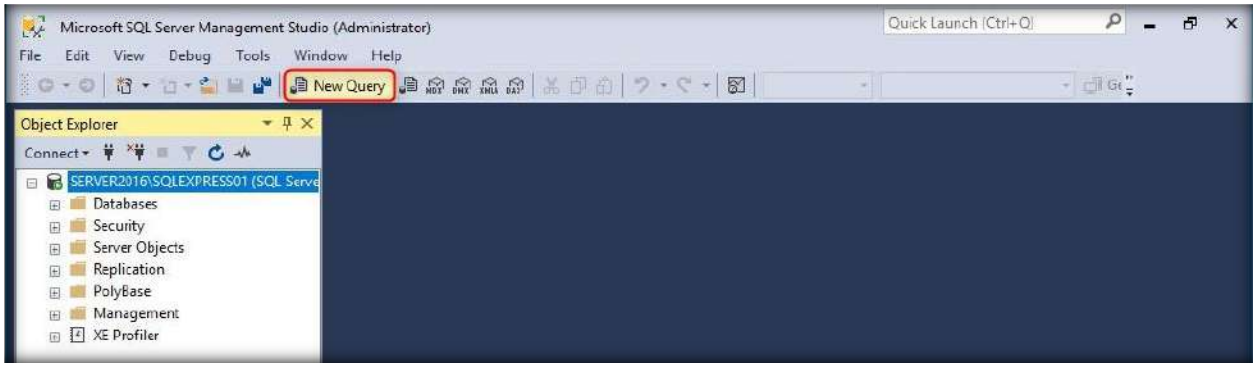
40. Close the **SQL Server Installation Center** window

Important Note:

To execute **XP command shell scripts** in CEH demo websites, you need to run the below query in your **SQL Server Management Studio** or otherwise all the XP command shell labs exercise will not work accordingly.

1. To launch SQL Server Management Studio, click Windows icon at the lower left corner of the screen
2. **Start** menu appears, click **SQL Server Management Studio** icon in order to launch the application
3. Main window of **SQL Server Management Studio** appears along with a **Connect to Server** dialog-box
4. Ensure that the name of the Windows machine is pre-written in the **Server name** field and click **Connect**
5. If the server name is not already written, then navigate to **Control Panel → All Control Panel Items → System**, make a note of the machine's name written in the **Computer name** field and write it in the **Server name** field of **Connect to Server** dialog-box

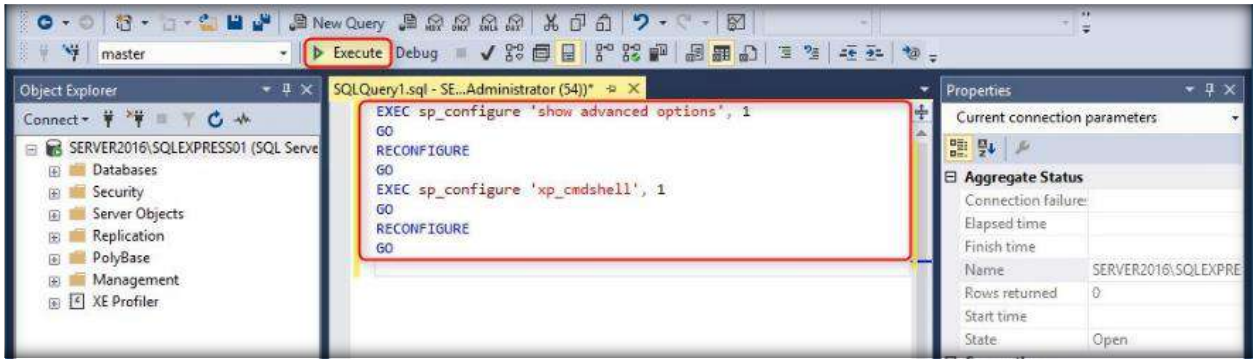
6. When the server is connected, click **New Query** button from menu bar



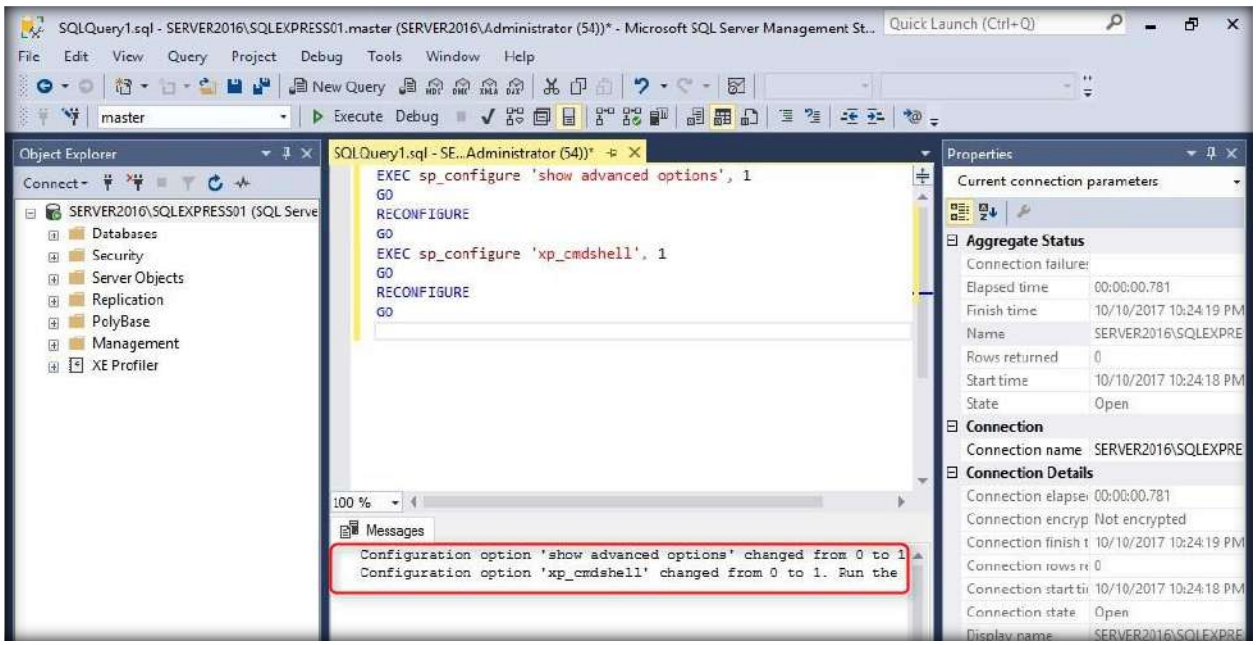
7. **SQL Query** window appears in the right pane of the window

8. Now, in this query page type the below **query** and then click **Execute** button

```
EXEC sp_configure 'show advanced options', 1
GO
RECONFIGURE
GO
EXEC sp_configure 'xp_cmdshell', 1
GO
RECONFIGURE
GO
```



9. After the query is **executed successfully**, close SQL Server Management Studio



10. If prompted to save the query, click **No** and **exit** from SQL Server Management Studio

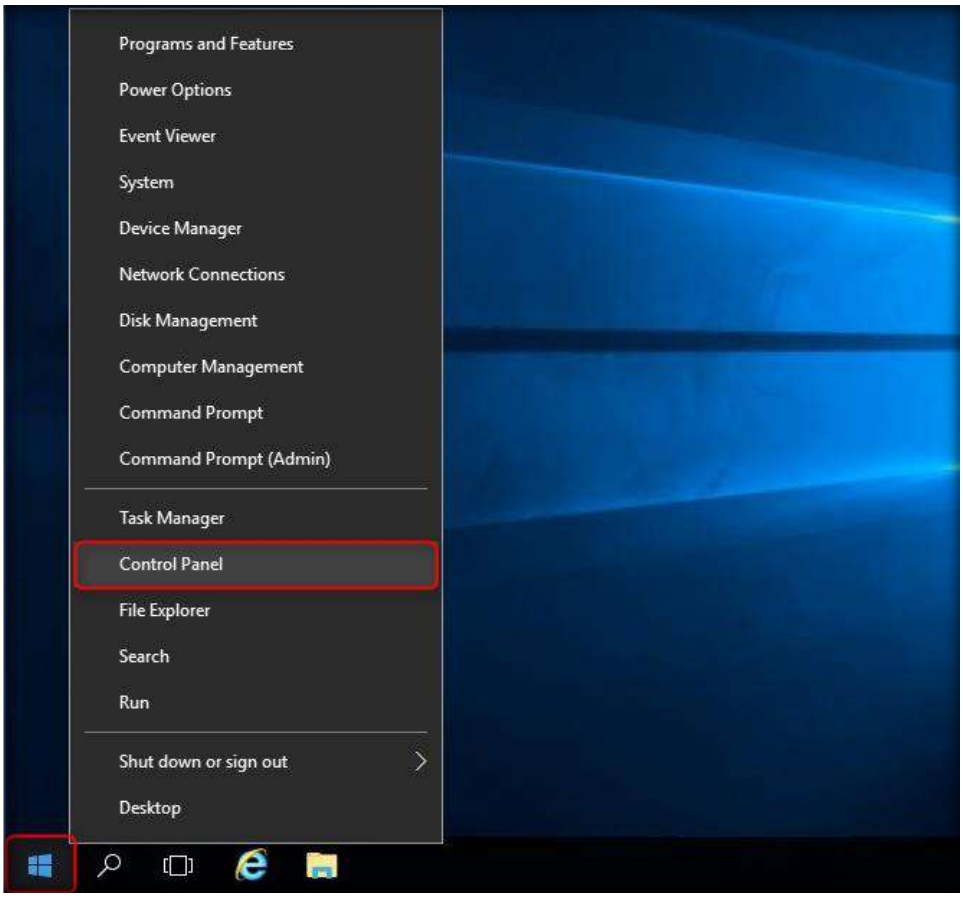
[Back to Configuration Task Outline]

CT#23: Turn off Firewall in all the Machines

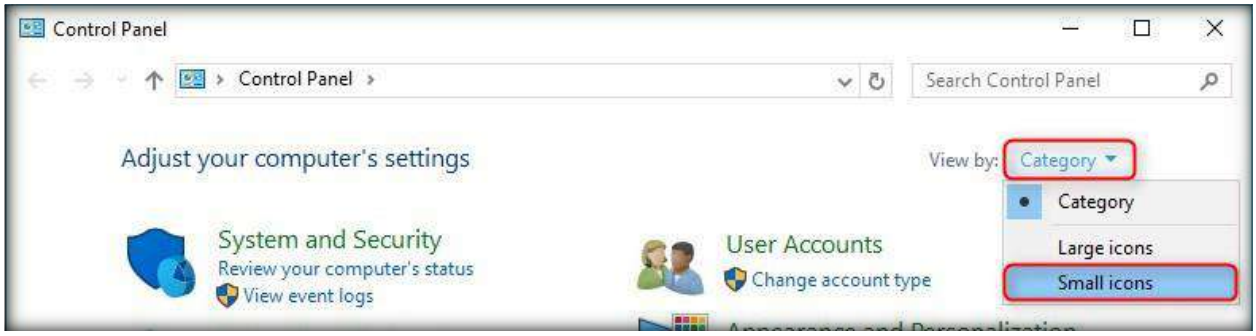
Windows Server 2016 (virtual machine)

To turn off Windows Firewall Settings in **Windows Server 2016**:

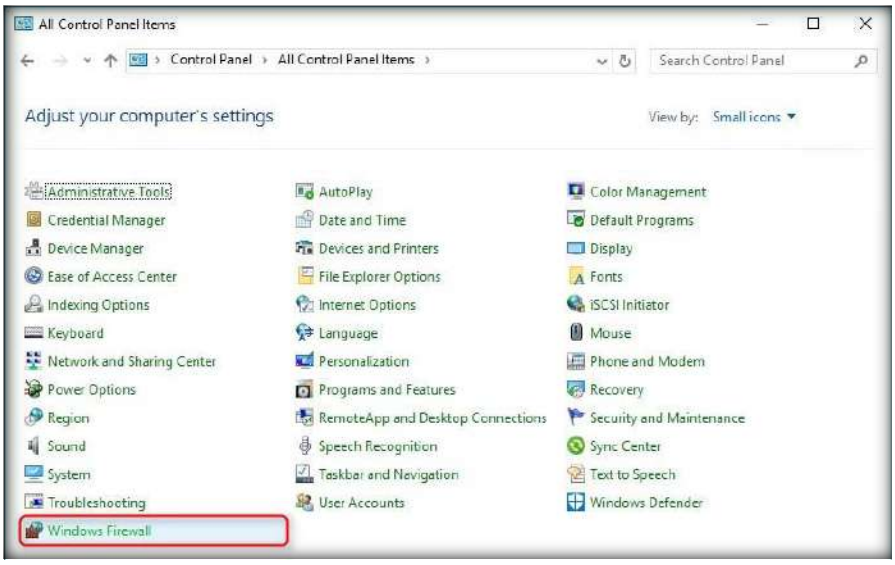
1. Right-click **Windows** icon at the lower left corner of the screen, click **Control Panel** from the context menu



2. Control Panel appears on the screen, select **Small icons** from the **Category** drop down list to see all the control panel options

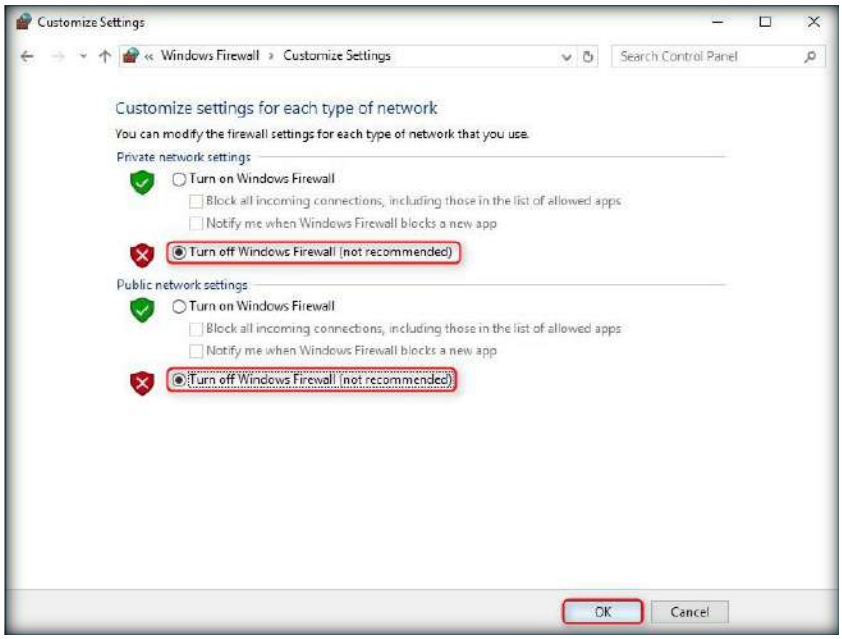


3. **All Control Panel Items** Window, click **Windows Firewall**



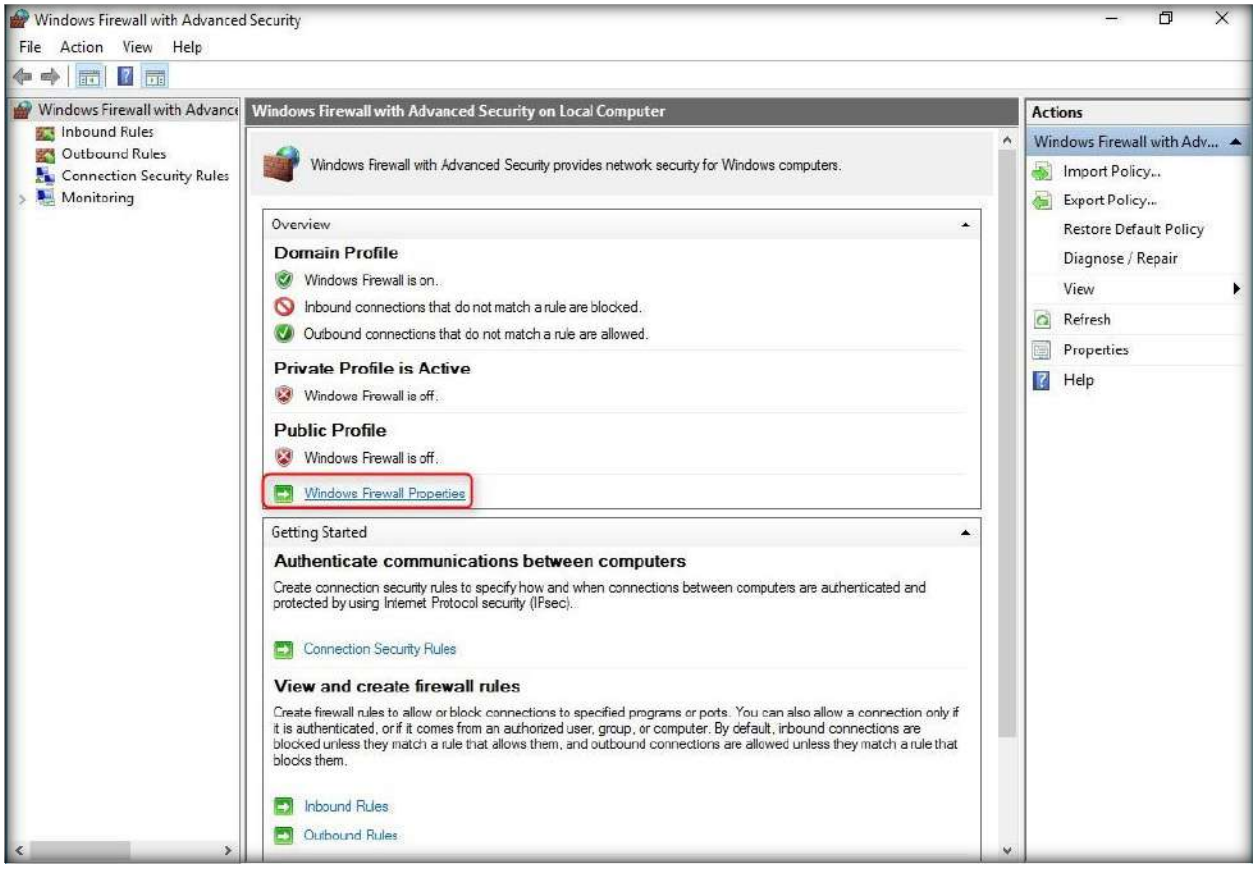
4. **Windows Firewall** control panel appears on the screen, click **Turn Windows Firewall on or off** link in the left pane of the window

5. In **Customize Settings** window, select the radio button **Turn off Windows Firewall (not recommended)** for both Private and Public network settings and click **OK**

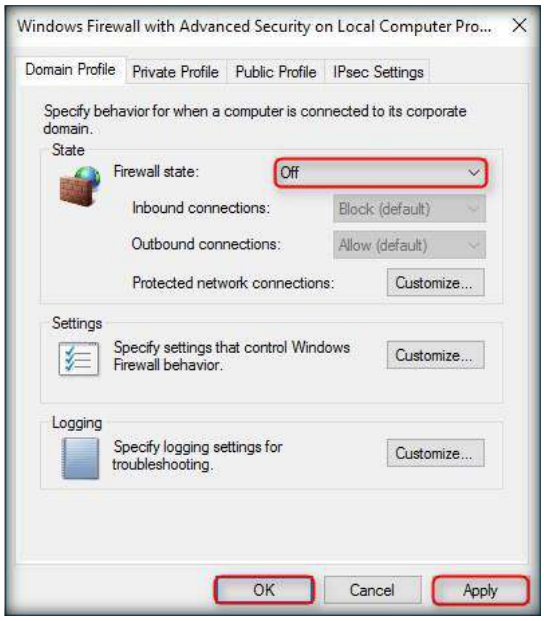


6. In the Windows Firewall control panel, click **Advanced settings** link in the left pane

7. A window named **Windows Firewall with Advanced Security** appears on the screen, click **Windows Firewall Properties** link in the Overview section



8. **Windows Firewall with Advanced Security on Local Computer Properties** window appears, choose **Off** from the **Firewall state** drop-down list, click **Apply** and then click **OK**

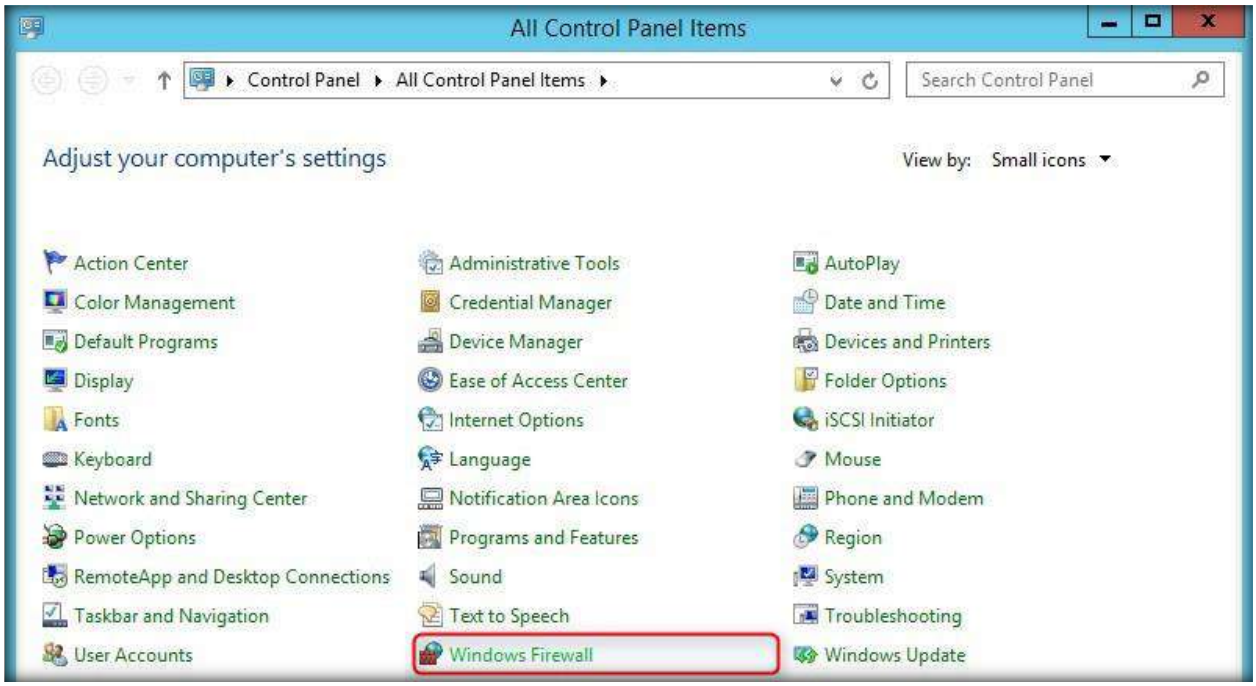


9. Ensure that Firewall state under **Private Profile** tab is also turned off.
10. **Close** all the windows

Windows Server 2012

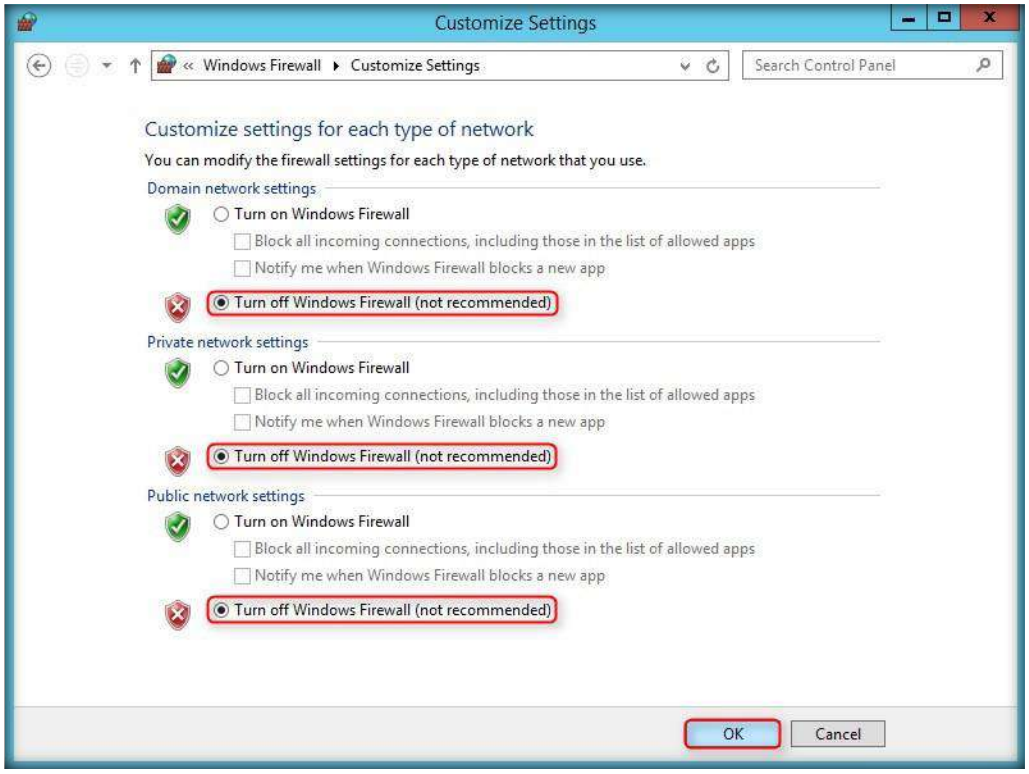
To Turn off Windows Firewall Settings in **Windows Server 2012**:

1. Go to **Start → Control Panel → All Control Panel Items**
2. Click **Windows Firewall** icon in Control Panel to launch Windows Firewall



3. Click **Turn Windows Firewall on or off** link in the left pane of the Windows Firewall window

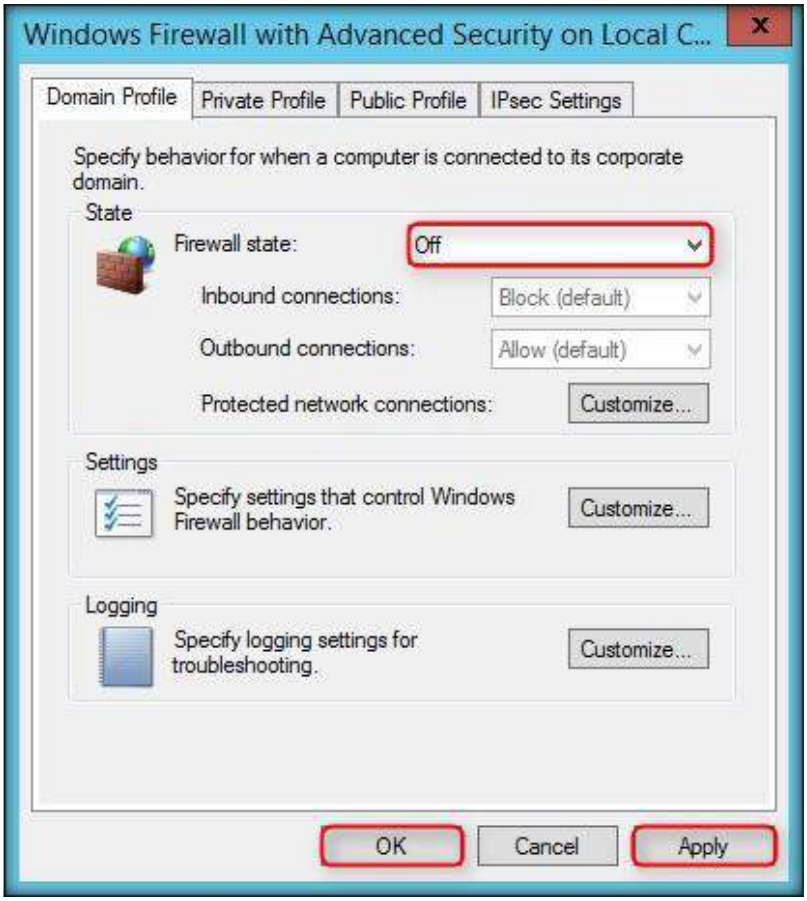
4. In **Customize Settings** window, select the radio button **Turn off Windows Firewall (not recommended)** for Private, Public and Domain network settings and click **OK**



5. In the Windows Firewall control panel, click **Advanced settings** link in the left pane

6. **Windows Firewall with Advanced Security** window appears, click **Windows Firewall Properties** link under **Overview** section

7. **Windows Firewall with Advanced Security on Local Computer Properties** window appears, choose **Off** from the **Firewall state** drop-down list, click **Apply** and then click **OK**



8. Ensure that Firewall state under **Private Profile** tab is also turned off.
9. **Close** all the windows

Windows 10

To turn off Windows Defender Firewall settings in **Windows 10**:

1. Follow the same steps as in Windows Server 2016/Windows Server 2012 to turn off Windows Defender Firewall in Windows 10

Windows 8

To turn off Windows Firewall settings in **Windows 8**:

1. Follow the same steps as in Windows Server 2016/Windows Server 2012 to turn off Windows Firewall in Windows 8

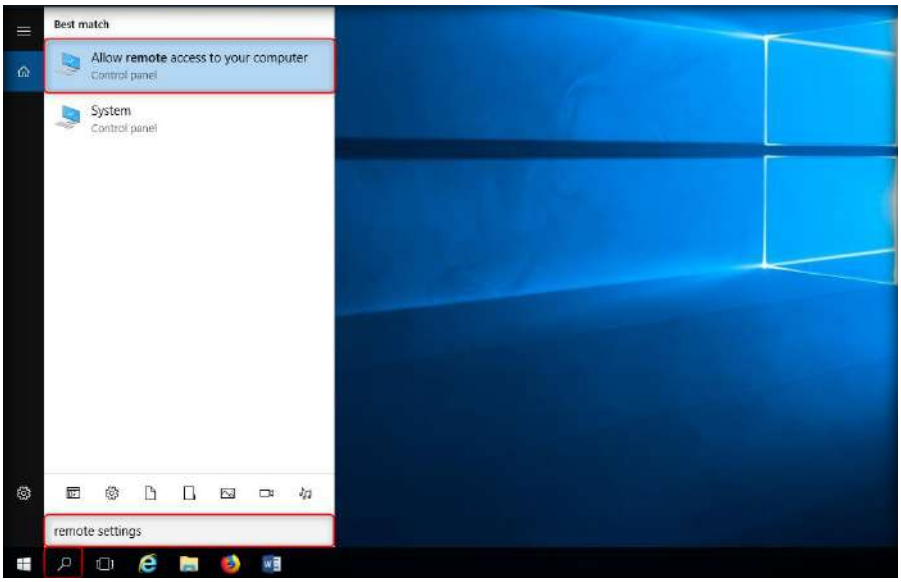
[Back to Configuration Task Outline]

CT#24: Enabling Remote Desktop Connection in all Windows Virtual Machines

Windows Server 2016

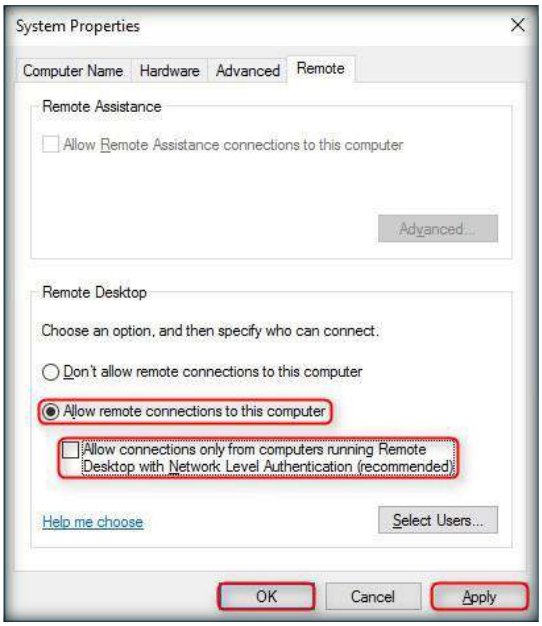
To enable remote desktop connection in **Windows Server 2016**:

1. Click **Search** icon at the lower left corner of the screen and type **remote settings**
2. Click **Allow remote access to your computer** Control panel option obtained in the search result



3. **System properties** dialog-box appears, click **Allow remote connections to this computer** radio button
4. A **Remote Desktop Connection** pop-up appears, click **OK**
5. You will observe that **Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)** is checked. Uncheck the option
6. Click **Apply** and then click **OK**

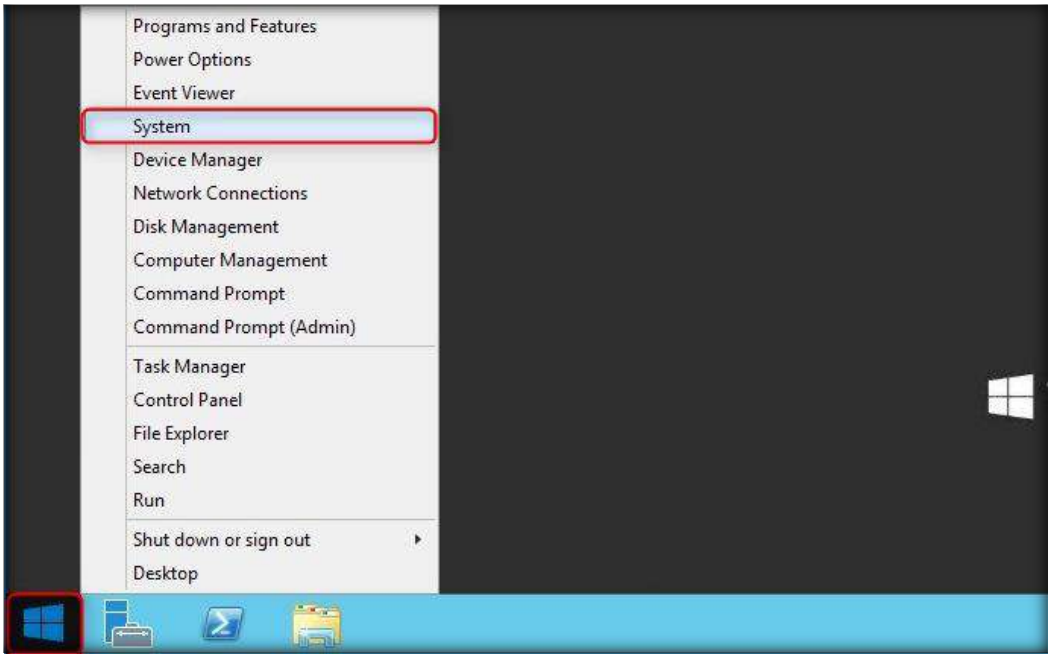
7. Repeat the same steps for **windows 10**



Windows Server 2012

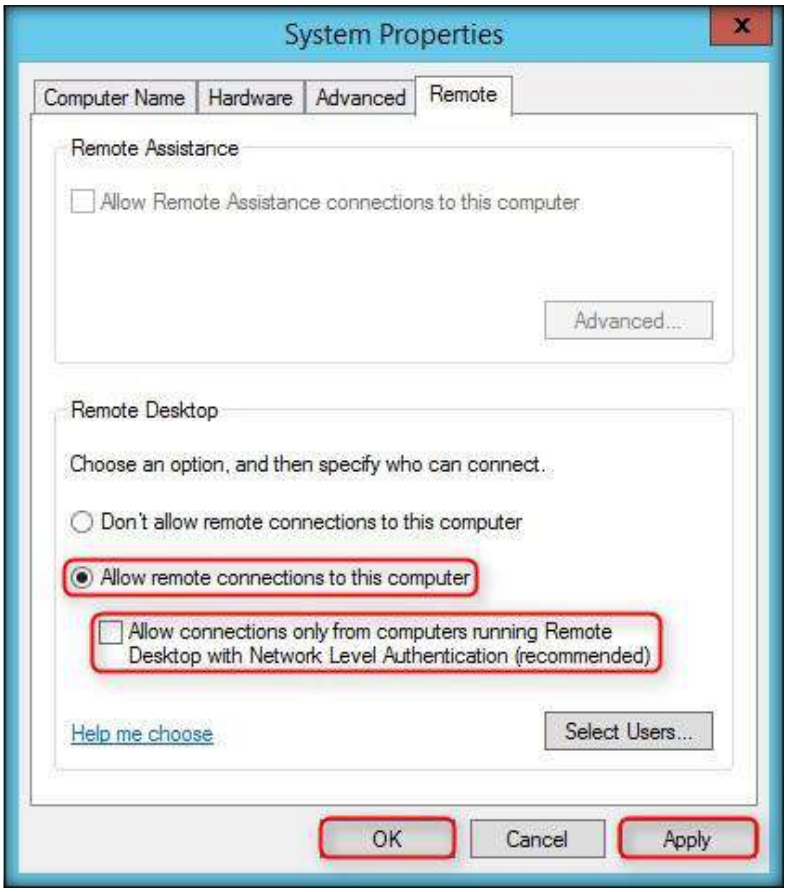
To enable remote desktop connection in **Windows Server 2012**:

1. Right-click **Start** button and click **System**



2. **System** control panel appears on the screen, click **Remote settings** link from the left pane

3. **System properties** dialog-box appears, click **Allow connections from computers running any version of Remote Desktop (less secure)** radio button
4. A **Remote Desktop** pop-up appears, click **OK**
5. You will observe that **Allow connections from computers running any version of Remote Desktop (less secure)** radio button is selected. Uncheck it
6. Click **Apply** and then click **OK**
7. Repeat the same steps for **windows 8**



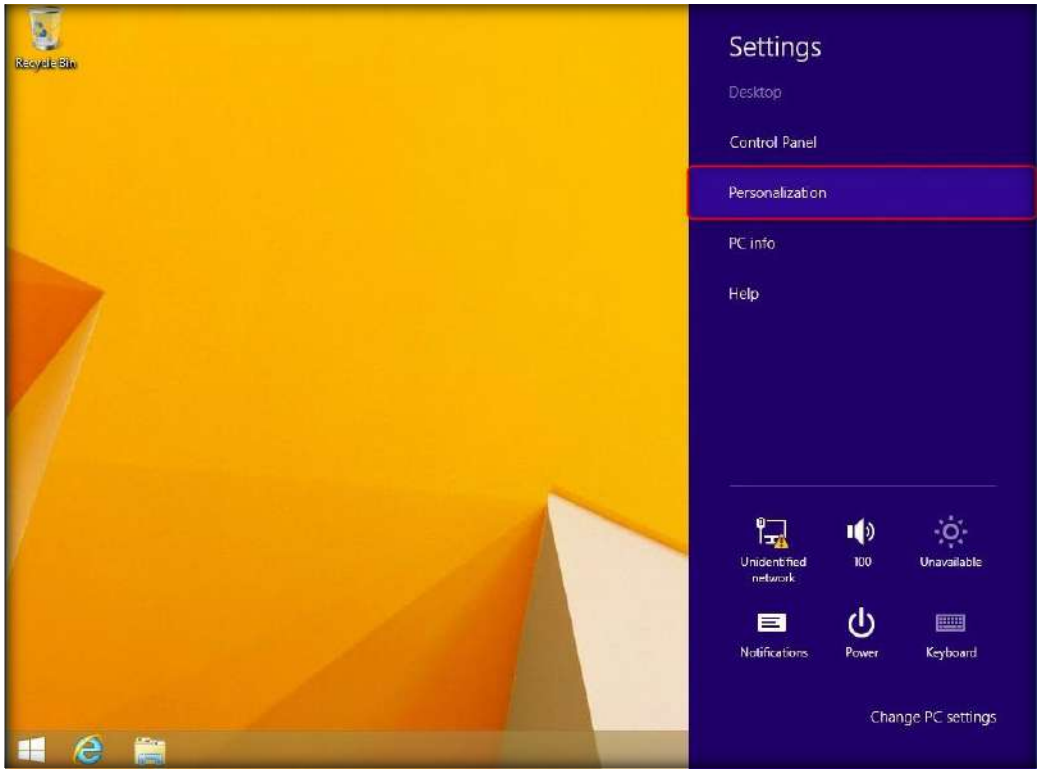
[Back to Configuration Task Outline]

CT#25: Turn off Screen Savers in all the Machines

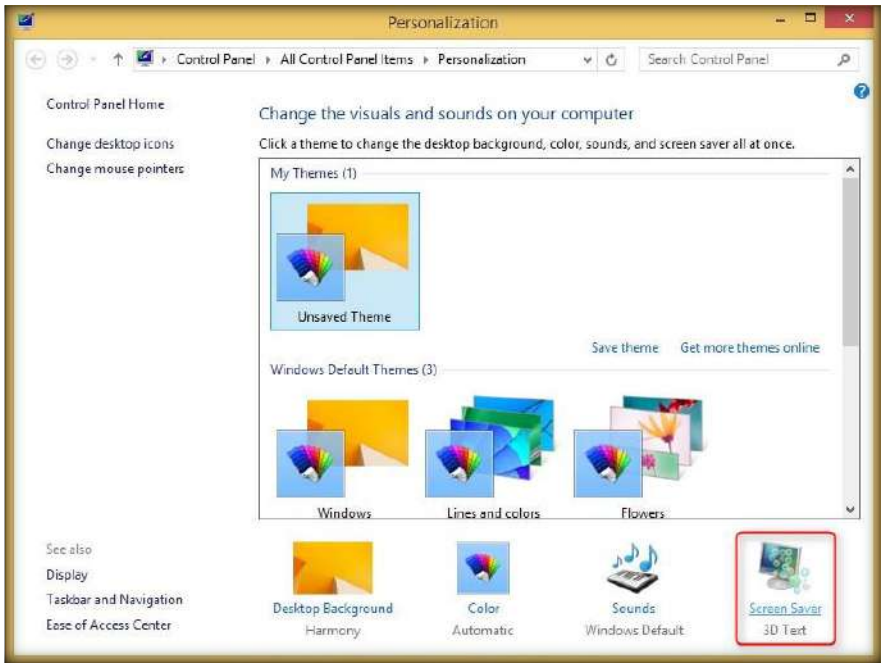
Windows 8

1. Move your mouse on the right side of the desktop screen to get the menu pane, select **Settings**

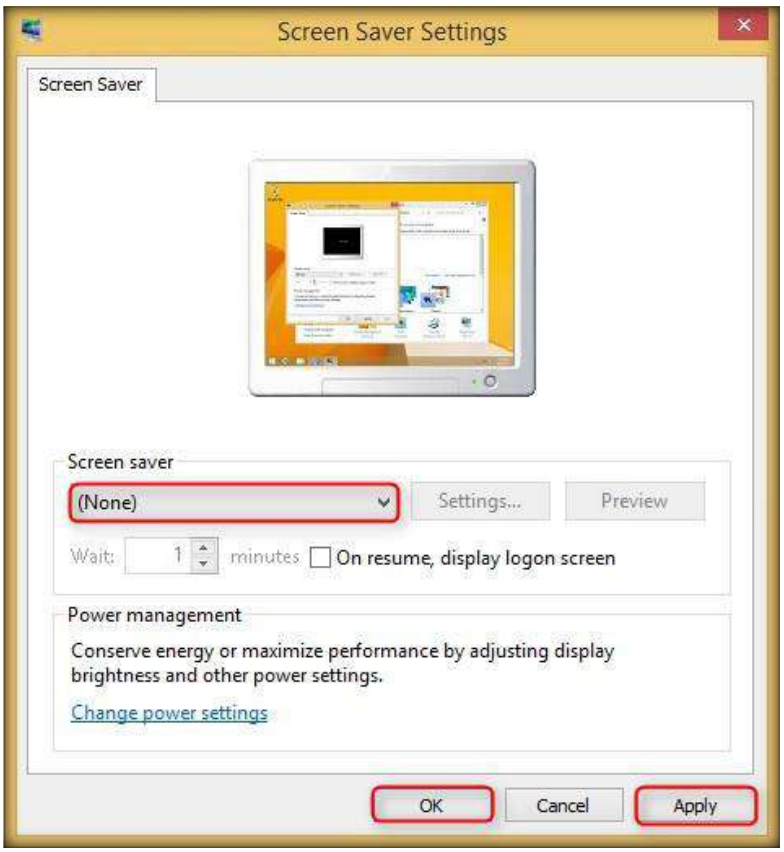
2. In the Settings menu, click **Personalization**



3. Personalization window appears, click **Screen Saver** link as shown in the screenshot below:



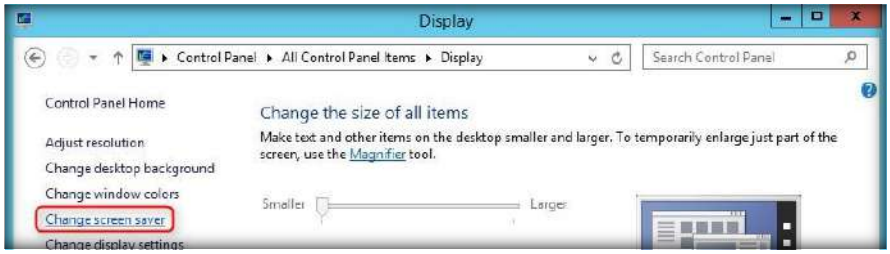
4. In Screen Saver Settings wizard, select **None** from the drop-down list of Screen Saver. Click **Apply** and then click **OK**



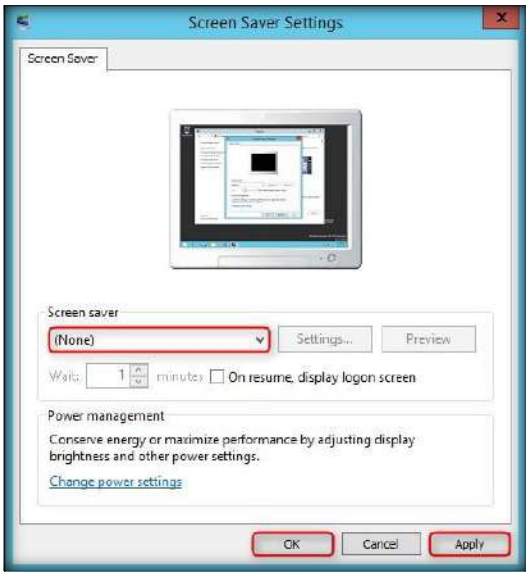
Windows Server 2012

1. In the Windows Server 2012 virtual machine, navigate to **Start → Control Panel → All Control Panel Items**
2. Click **Display** as shown in the screenshot below

3. Display window appears, click **Change screen saver** link on the left pane



4. In **Screen Saver Settings** wizard, select **None** from the drop-down list of Screen Saver. Click **Apply** and then click **OK**

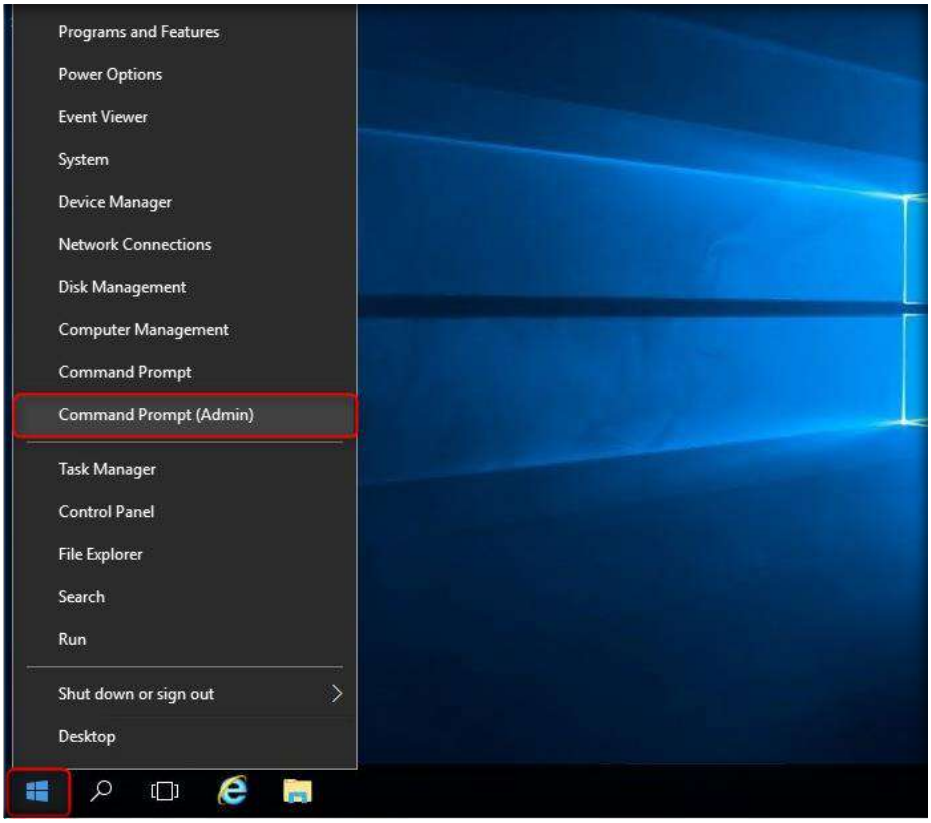


5. In some windows operating systems such as Windows Server 2016 and Windows 10, you are not able to change the personalization settings unless your system is activated

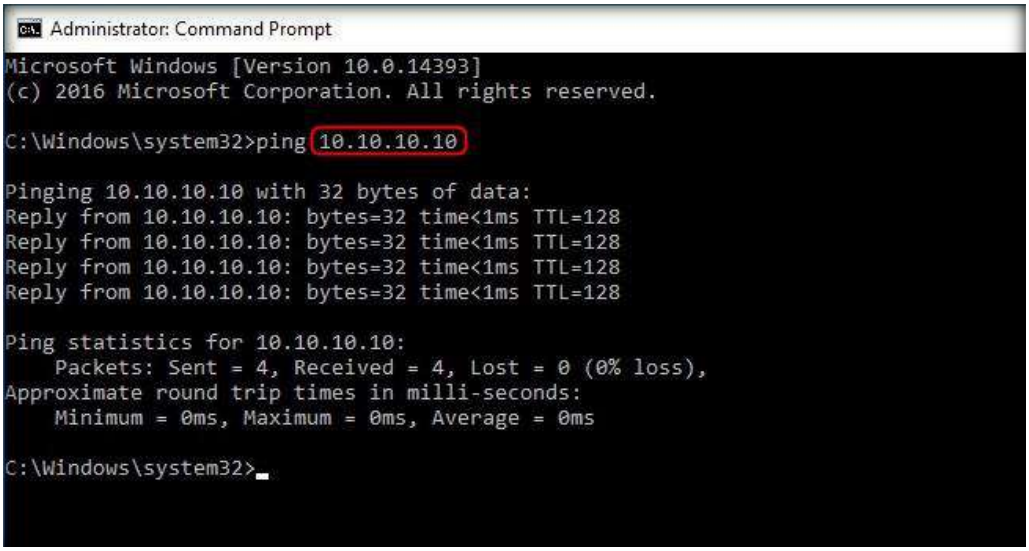
[Back to Configuration Task Outline]

CT#26: Test for Pinging each other

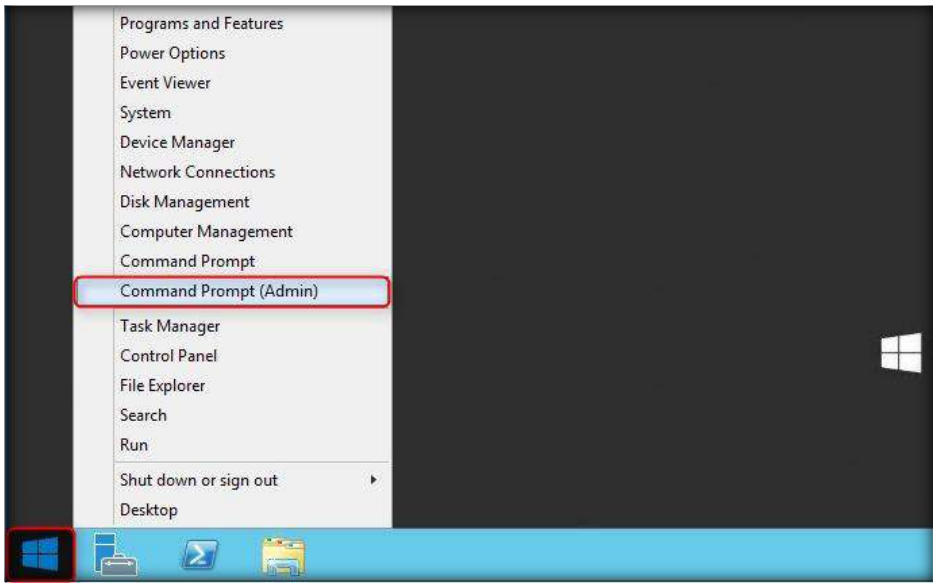
1. Click **Windows** icon at the lower left corner of the screen and click **Command Prompt (Admin)**



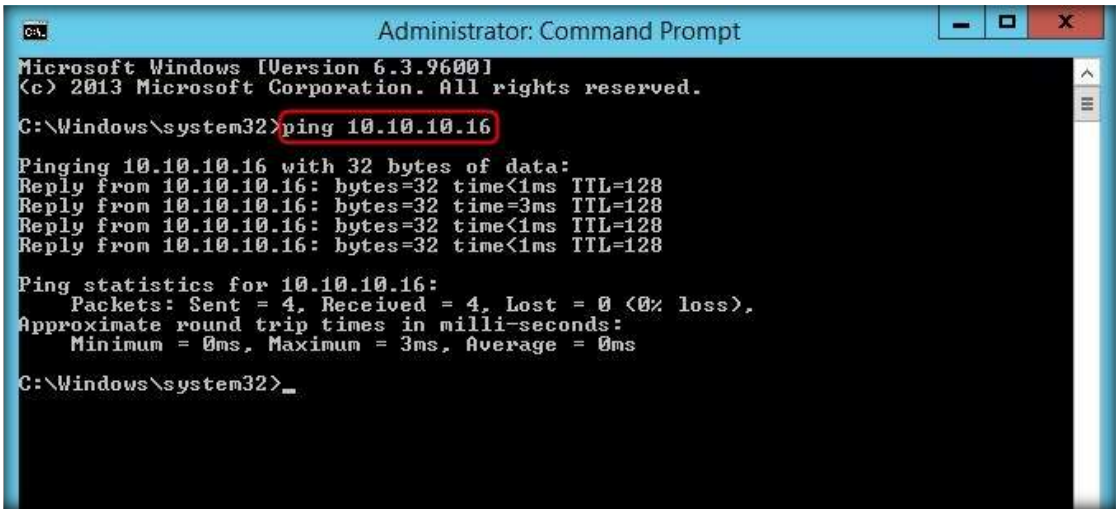
2. Before pinging the virtual machines make sure that the **Virtual Machines are running**
3. Check for the reply from the Virtual Machines. Here as an example, we are using **Windows 10** Virtual Machine IP address **10.10.10.10** (this IP address may be different in your Lab network)



4. Open command prompt in another one of the **Virtual Machines**. Here as an example, we are using **Windows Server 2012** virtual machine



5. Here as an example, we are pinging between **Windows Server 2012** and **Windows Server 2016**
6. Open Command Prompt in one of your **Virtual Machines** and type the ping command as **Ping <IP address of Virtual Machine>**
7. Here we are pinging Windows Server 2016 with Windows Server 2012 (this IP address will be different in your Lab network)

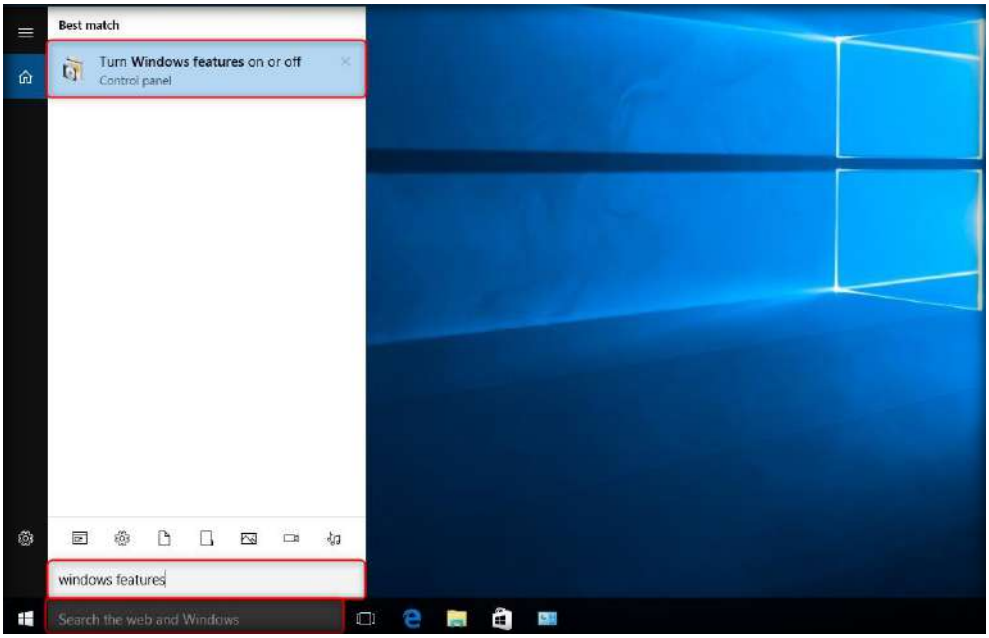


8. **Repeat** the above steps to ping all the Virtual Machines

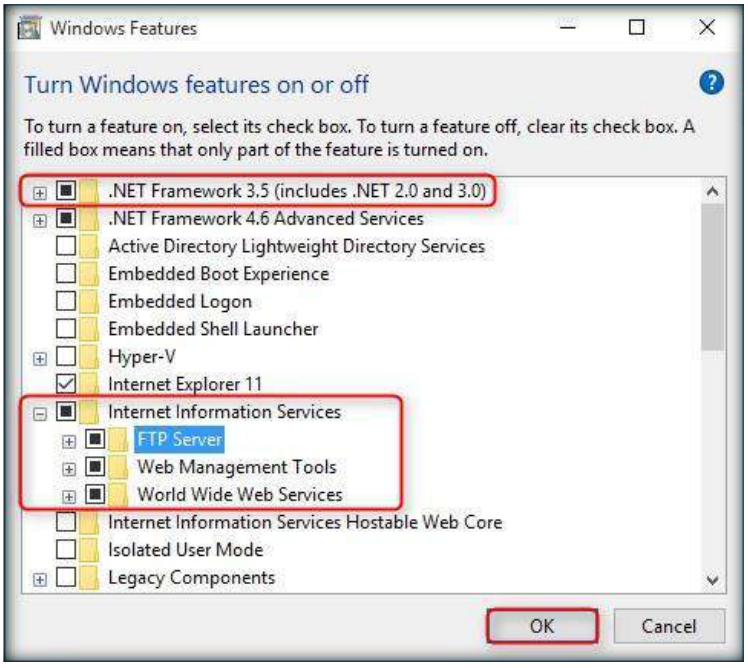
[Back to Configuration Task Outline]

CT#27: Enabling and Configuring FTP Server in Windows 10 Virtual Machine

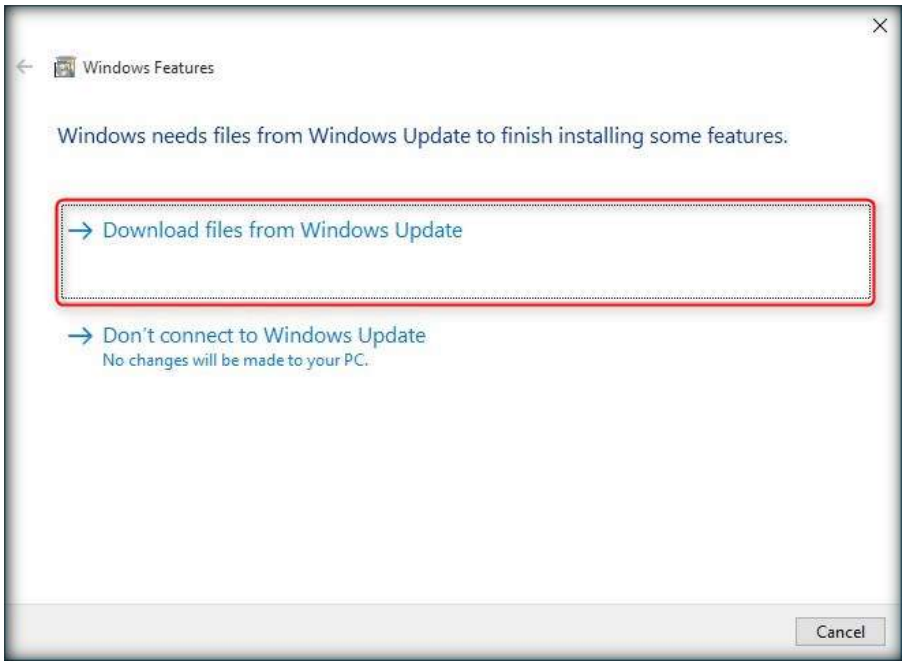
1. Login into your **Windows 10** virtual machine and in Search the web and Windows bar type **windows features**
2. Click **Turn Windows features on or off** as shown in the screenshot below



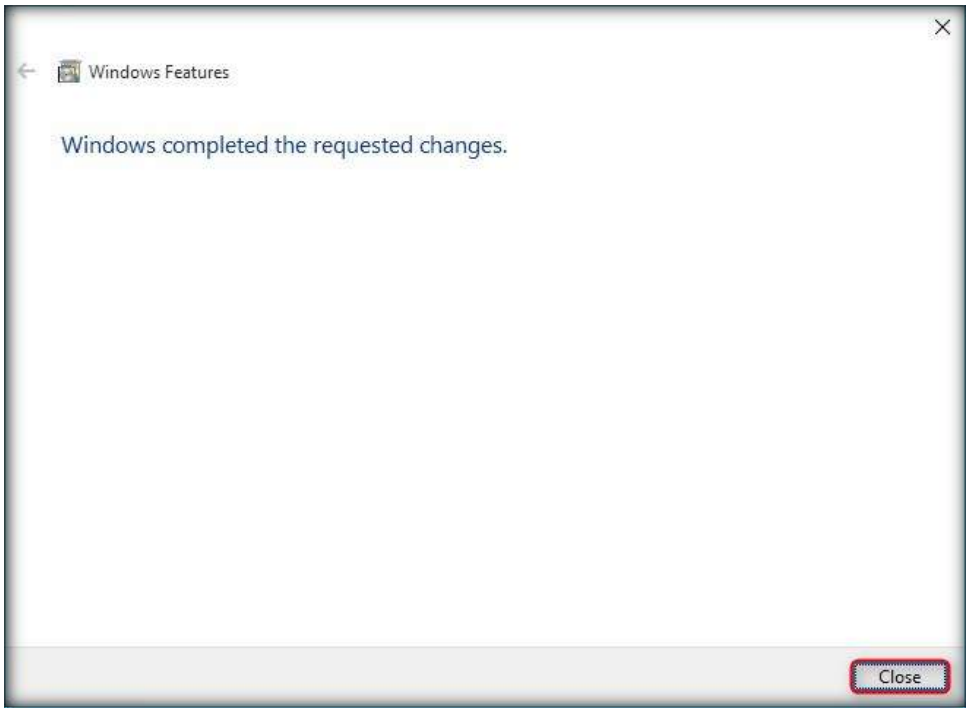
3. Windows Features window appears, select **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** and **FTP Server**, **Web Management Tools** and **World Wide Web Services** under **Internet Information Services**. Click **OK** to install these features



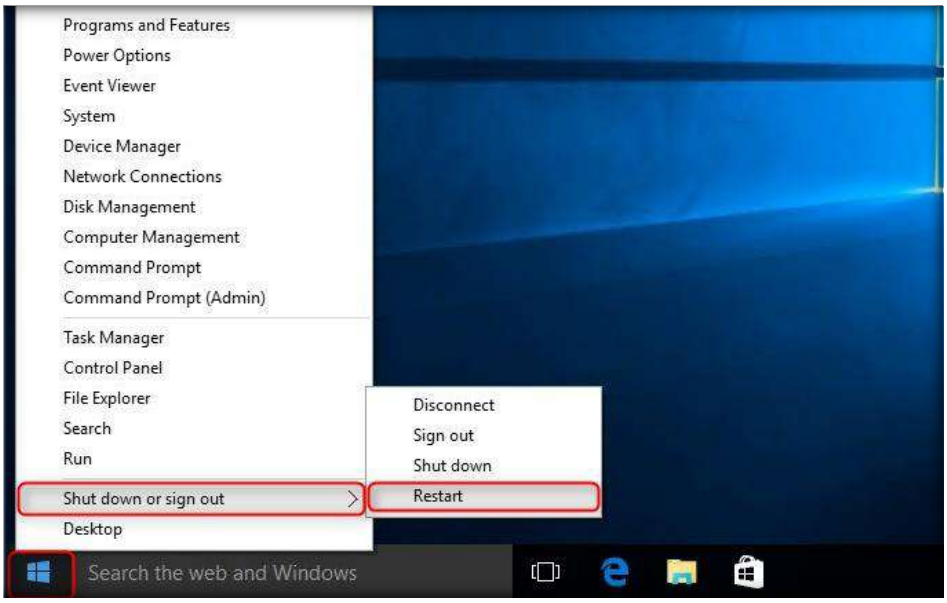
4. Click **Download files from Windows Update** as shown in the screenshot below:



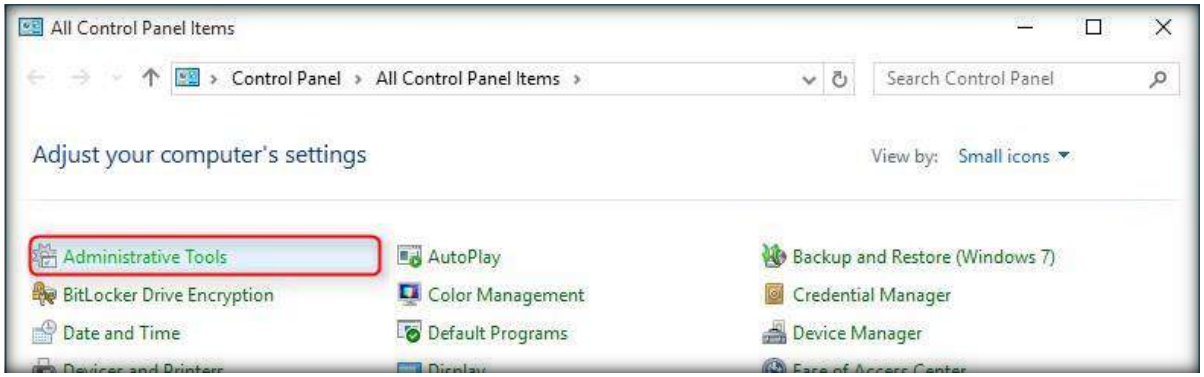
5. After the features have been successfully installed, click **Close** to exit Windows Features window



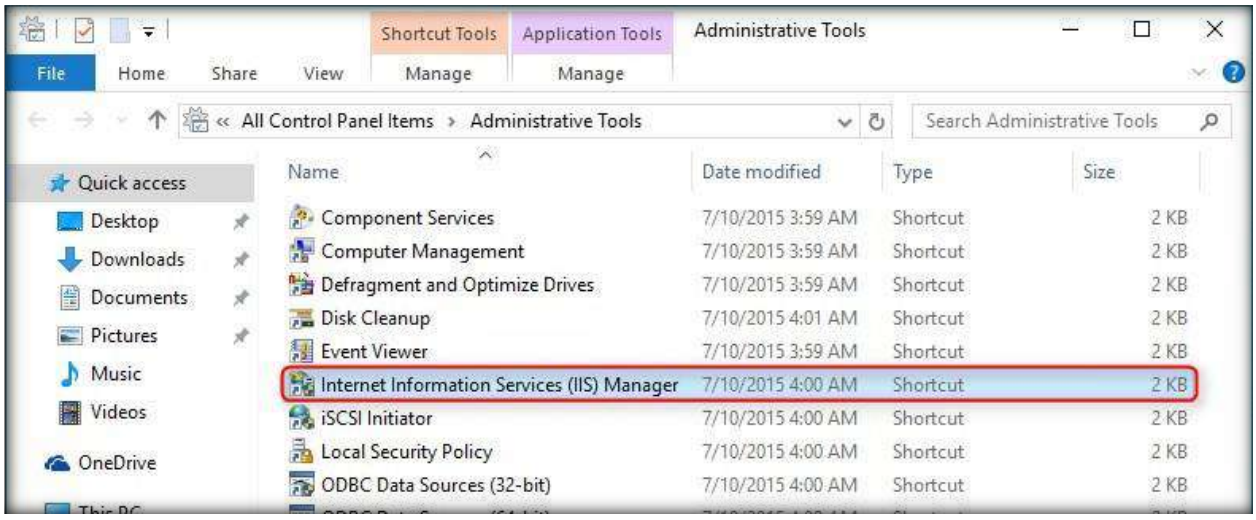
6. Once done, close all the windows and restart **Windows 10** virtual machine



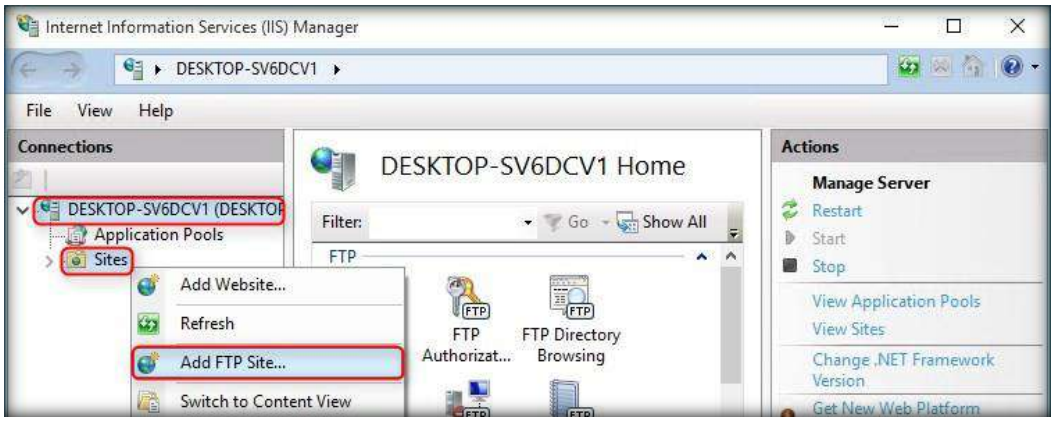
7. Once Windows 10 machine is restarted navigate to **Control Panel → All Control Panel Items → Administrative Tools**



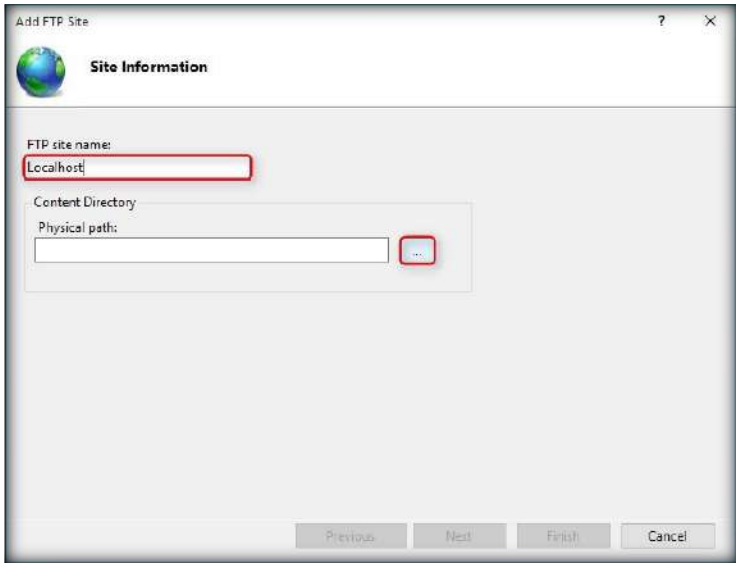
8. In Administrative Tools window double-click **Internet Information Services (IIS) Manager**



9. Internet Information Services (IIS) Manager window appears, expand the **root** folder, right-click **Sites** and select **Add FTP Site** from the context menu

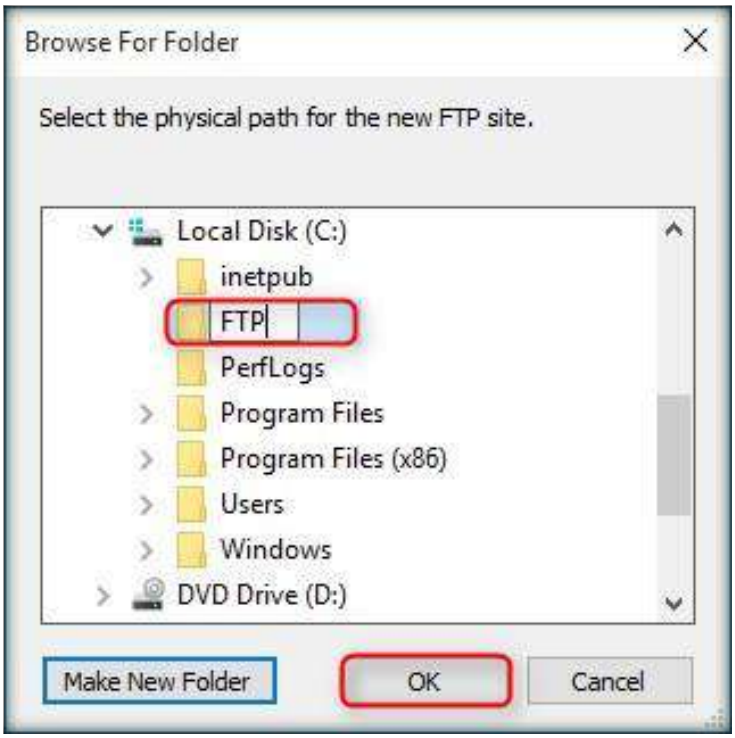


10. Add FTP Site wizard appears, in **FTP site name:** field type **Localhost** and in **Content Directory** section click **Browse** button

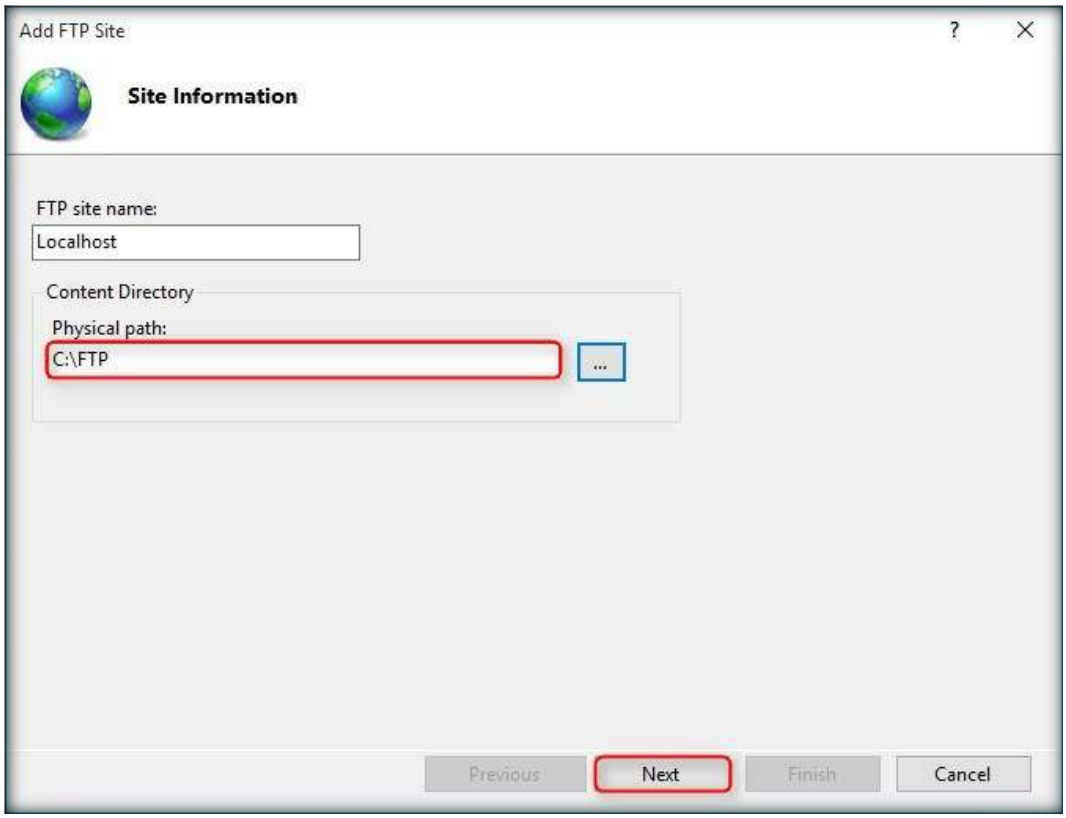


11. **Browse For Folder** wizard appears choose **C:** (or any drive) click **Make New Folder**

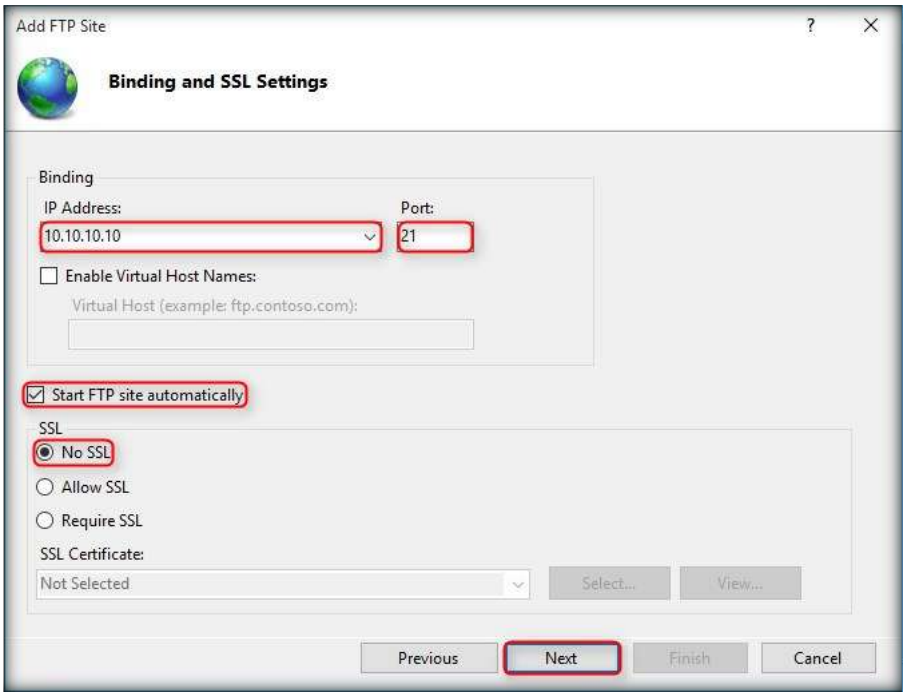
12. A New Folder will be created. Rename it as **FTP** and click **OK**



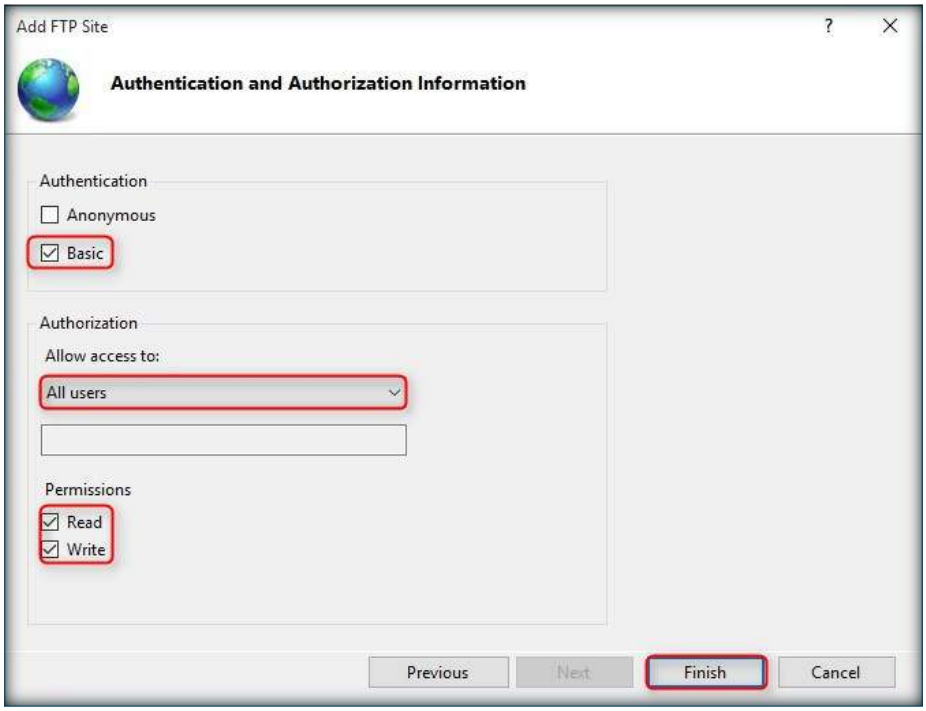
13. After Physical path is provided click **Next** button



14. In **Binding and SSL Settings** section, Enter the IP address of **Windows 10** virtual machine under IP Address field, specify port number as **21** under **Port** field, check **Start FTP site automatically** option, choose **No SSL** option under **SSL** section and leave the rest of the settings to default then click **Next**



15. In **Authentication and Authorization Information** options Check **Basic** under Authentication and choose **All users** under Authorization section, and check **Read** and **Write** options under Permissions and click **Finish**



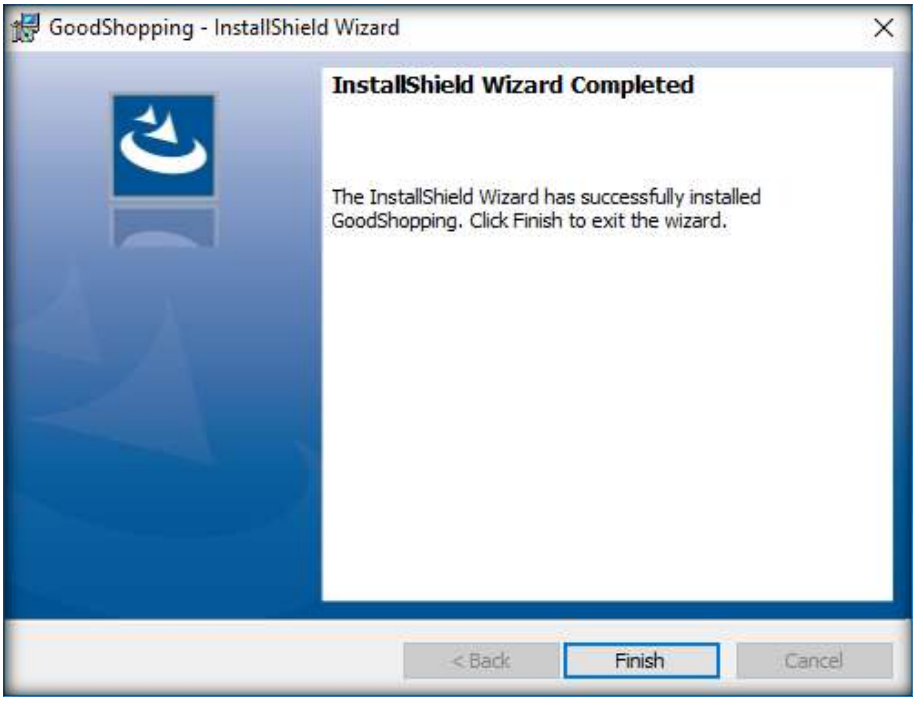
16. **Localhost** site will have created under **Sites** folder as shown in the following screenshot:

[Back to Configuration Task Outline]

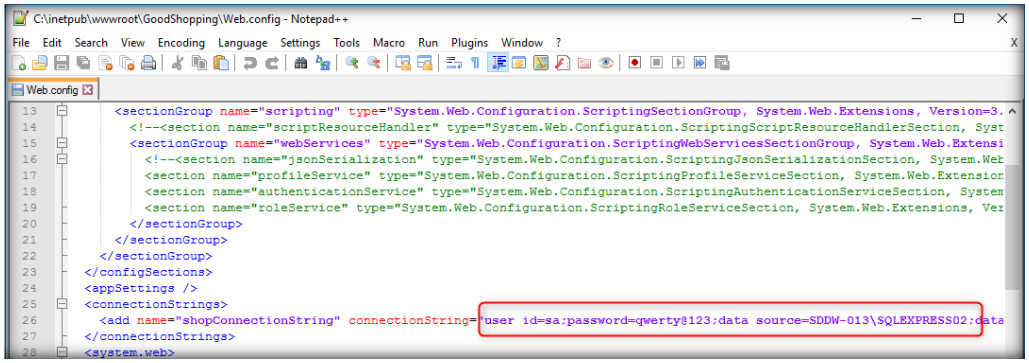
CT#28: Configure the GoodShopping Website Windows Server 2016 (Virtual Machine)

1. Navigate to **Z:\CEH-Tools\CEHv10 Lab Prerequisites\Websites**
2. Open **GoodShopping** folder. Double click on **setup.exe** and follow the wizard driven installation steps

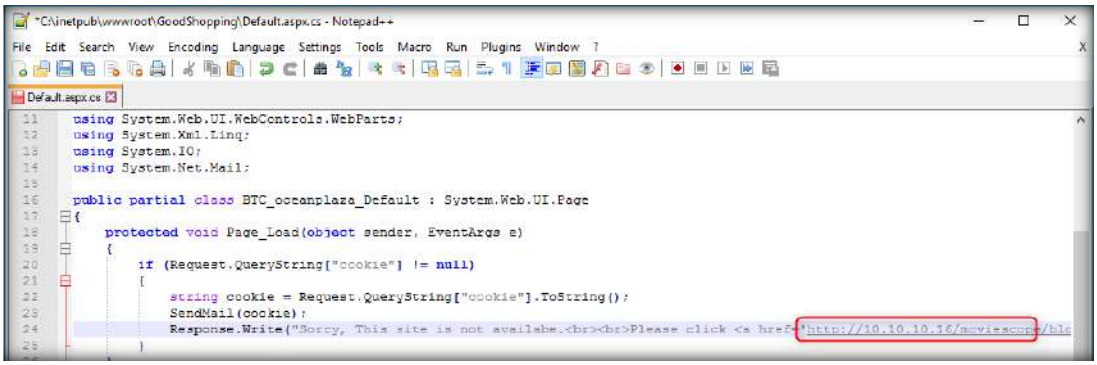
3. After completing the installation click **Finish**



4. Open **GoodShopping** folder from **C:\inetpub\wwwroot\GoodShopping** and open **Web.config** file in notepad++ or in notepad
5. Scroll down to **connectionstring** tag, enter your machine's name **data source=[Provide Your Host Machine Name]**, provide a user id after **user id=sa**, and a password after **Password=qwerty@123**

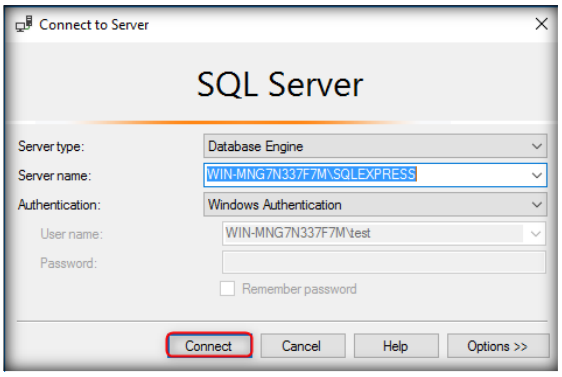


6. **Save** the file and **close** it
7. Open **GoodShopping** folder from **C:\inetpub\wwwroot\GoodShopping** and open **Default.aspx.cs** file in notepad++ or in notepad
8. Scroll down to **line no. 24** and replace localhost with the IP address of the Windows Server 2016 machine, i.e., the IP address of the machine where you are hosting the website.

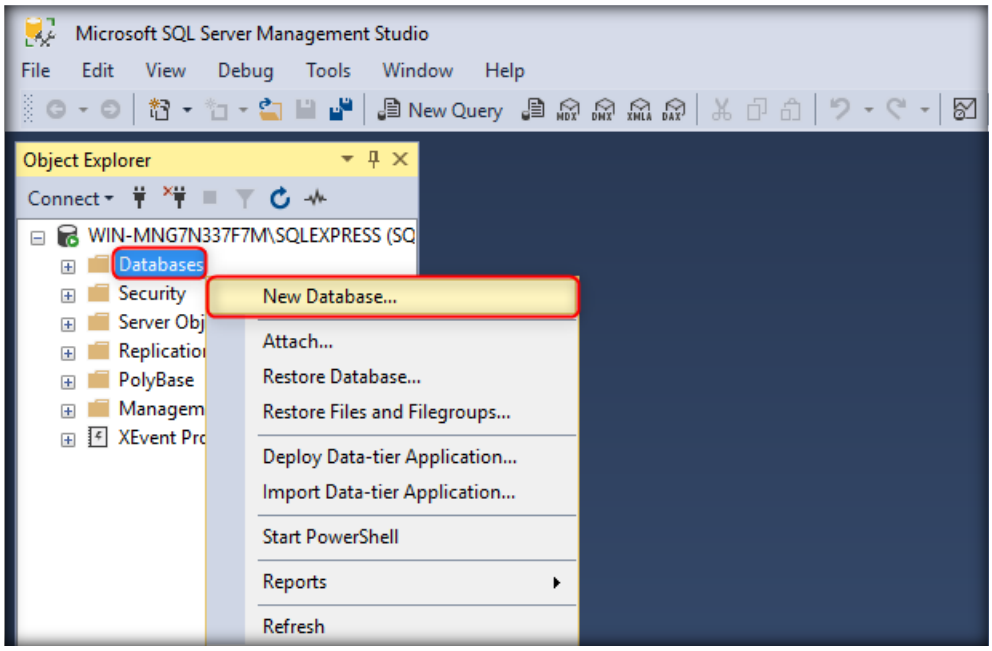


Note: The IP address of Windows Server 2016 machine might vary in your lab environment.

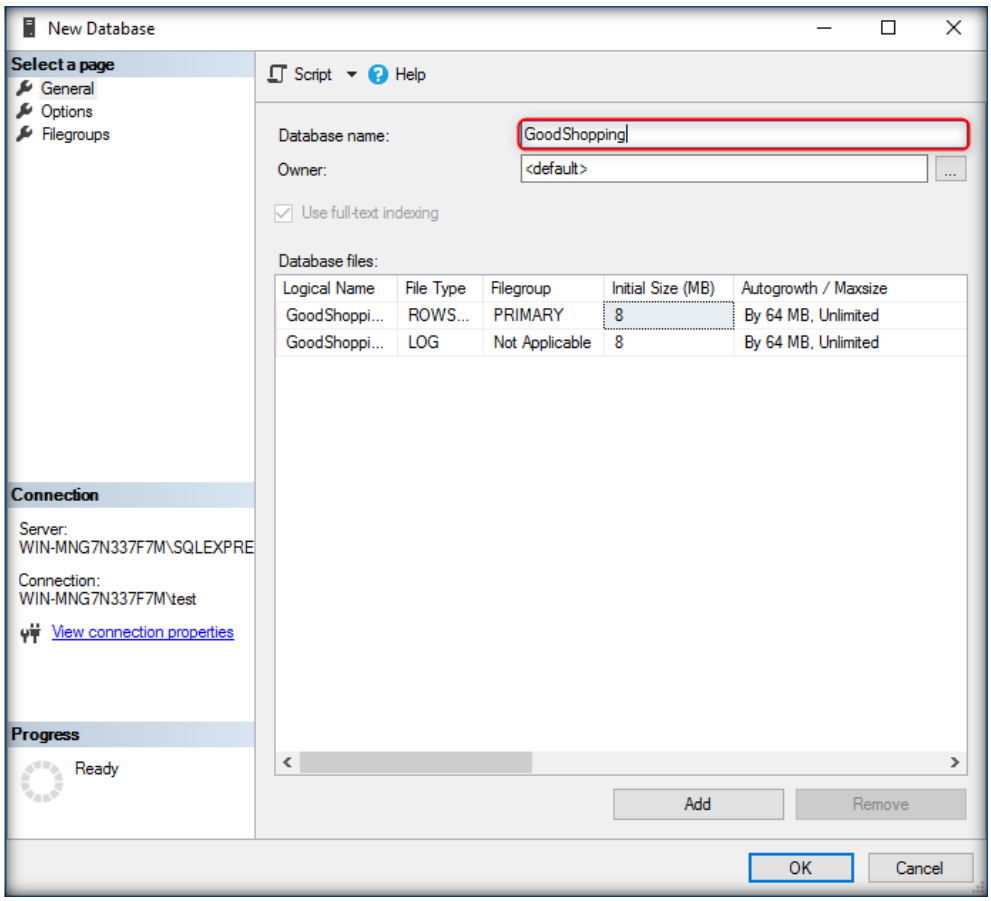
9. **Save** the file and **close** it
10. Now, **Launch** SQL Server 2017 Management Studio click **Connect**



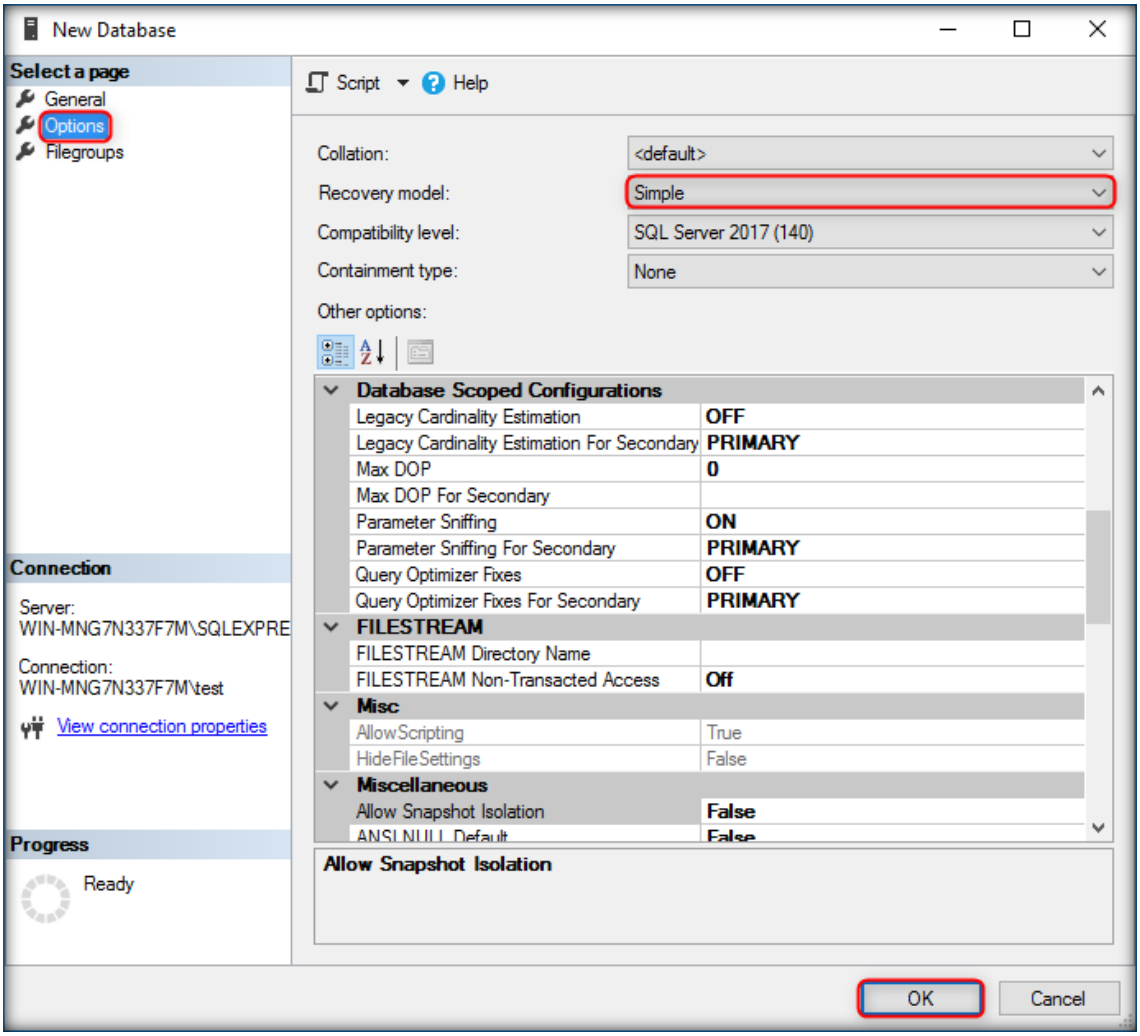
11. **Microsoft SQL Server Management Studio** window, right-click on **Databases** and select **New Database...**



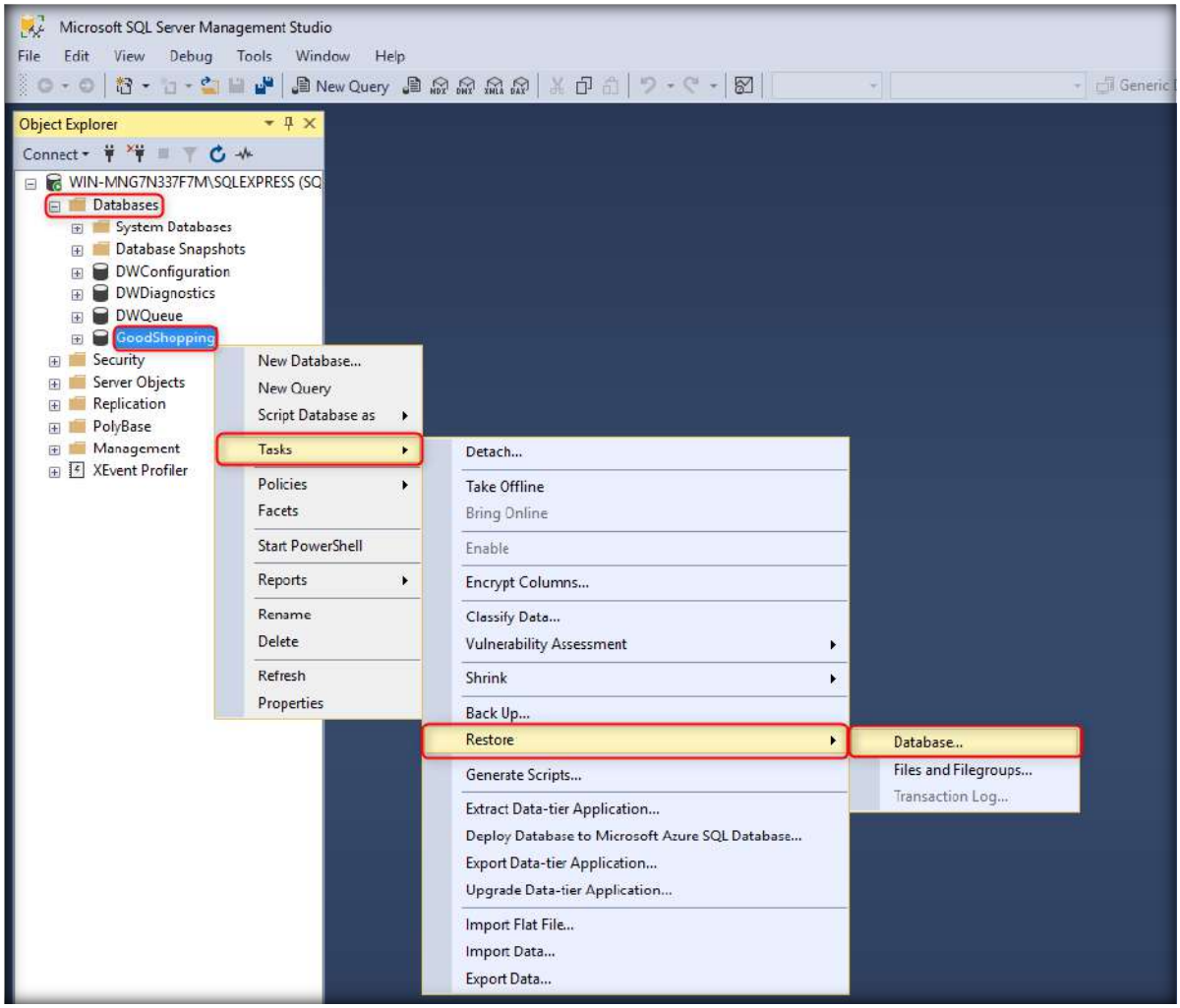
12. **New Database** window appears, specify **Database name** as **GoodShopping**



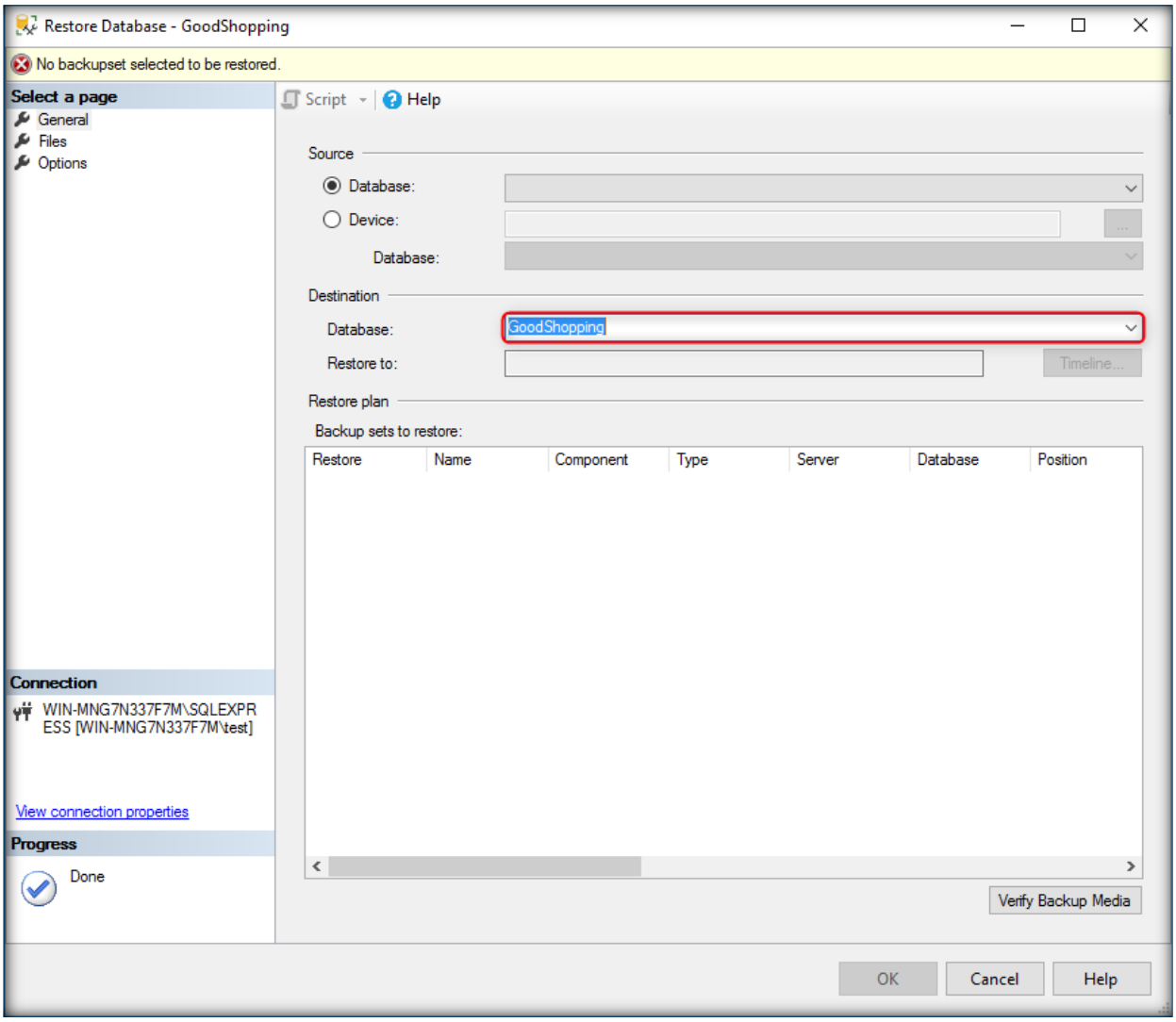
13. Select **Options** from the left pane.
14. Select **Simple** from the **Recovery model** drop-down list and click **OK**.



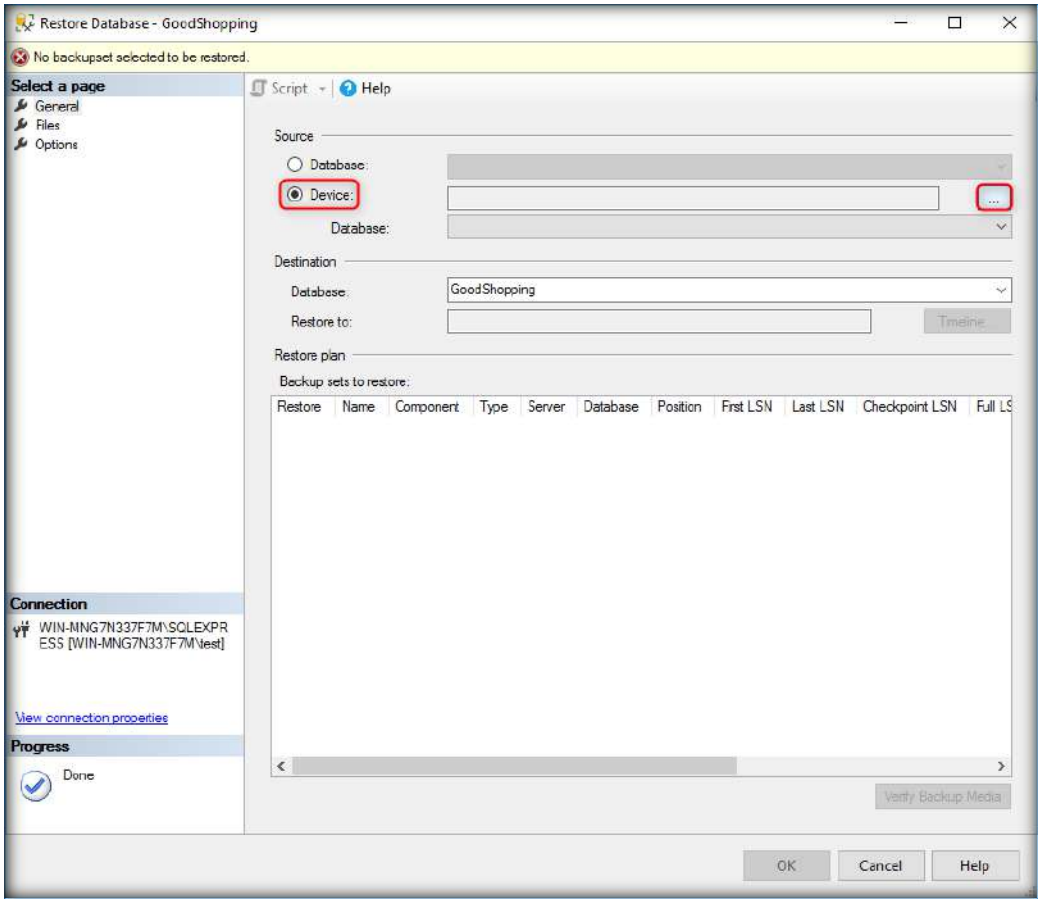
15. Now expand the **Databases** node. You will observe that **GoodShopping** database folder appears under the **Object Explorer** section, which implies that GoodShopping database has been **successfully** created.
16. **Right-Click** on GoodShopping database and go to **Tasks → Restore → Database...**



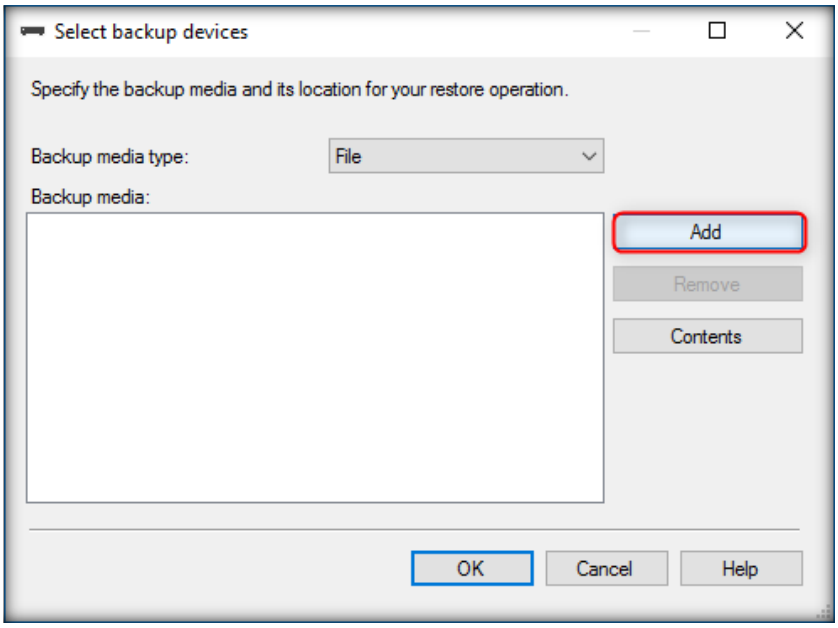
17. **Restore Database – GoodShopping** window appears displaying the database name (**GoodShopping**) in the **Database** field under **Destination** section.



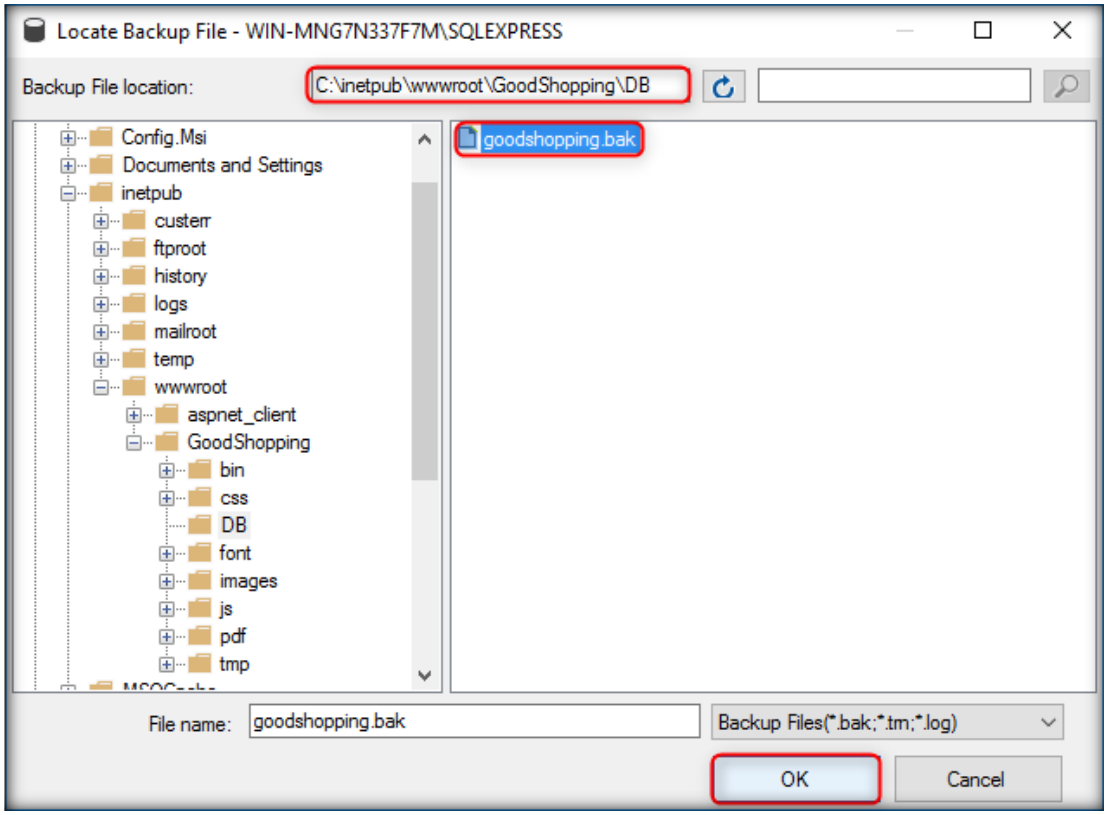
18. Click **Device** radio button under **Source** section and click  button located parallel to **Device** field



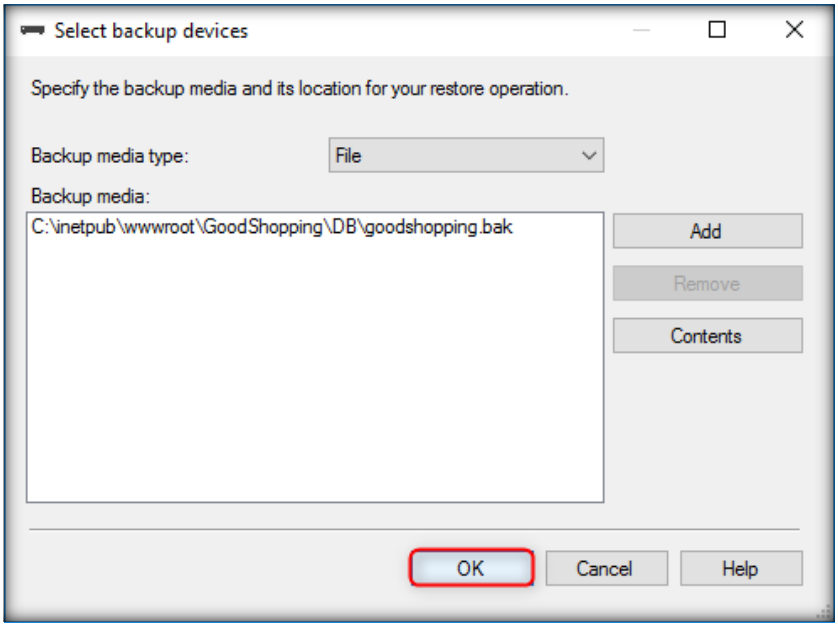
19. **Select backup devices** dialog-box appears, click **Add** button



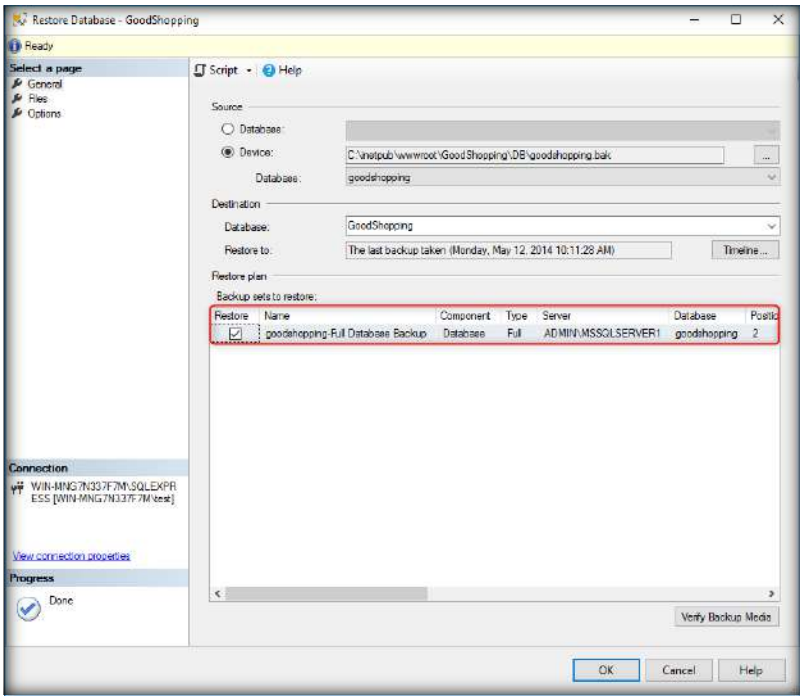
20. Navigate to the backup file (**goodshopping.bak**) located in **C:\inetpub\wwwroot\GoodShopping\DB**
21. Select the backup file and then click **OK**. Locate Backup File window exits



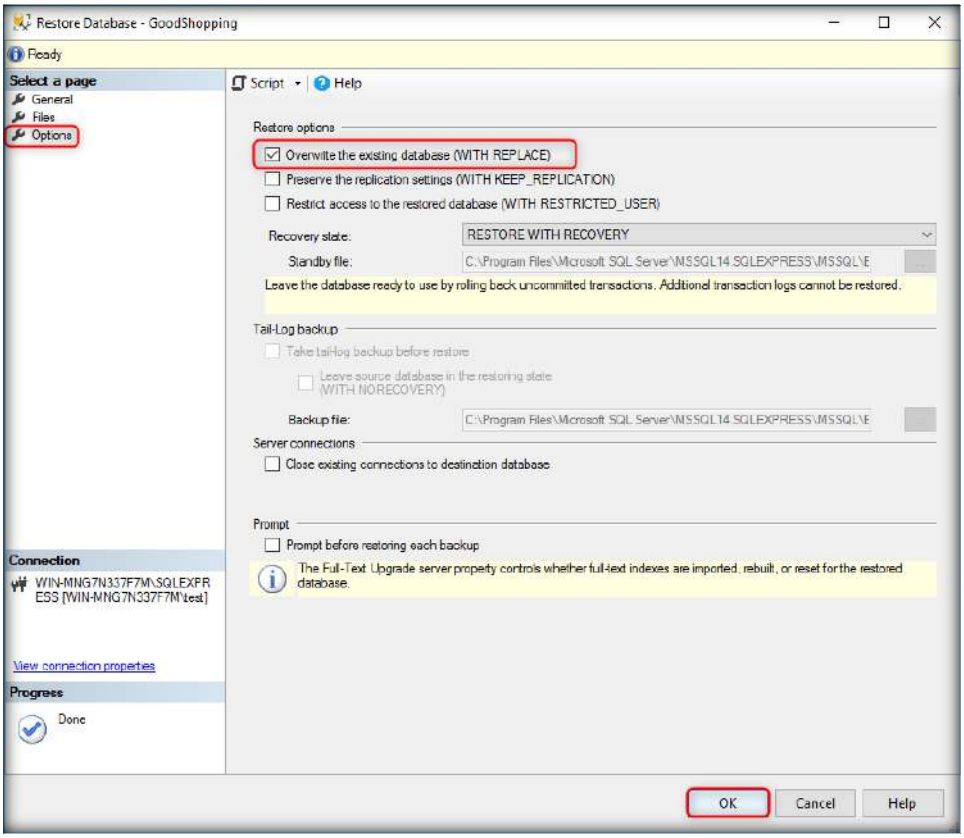
22. Under Backup media section, the location of **goodshopping.bak** website is listed
23. Click **OK**, Select backup devices window exits



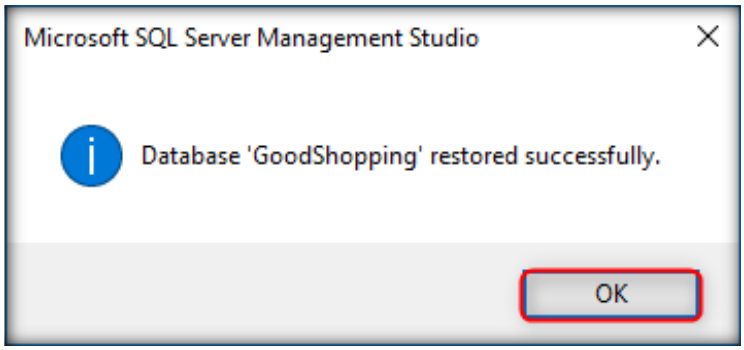
24. You will observe that the backup file has been successfully added. Ensure that the backup file is checked.



25. Click **Options** in left pane, check **Overwrite existing database** under **Restore options** section and the click **OK**

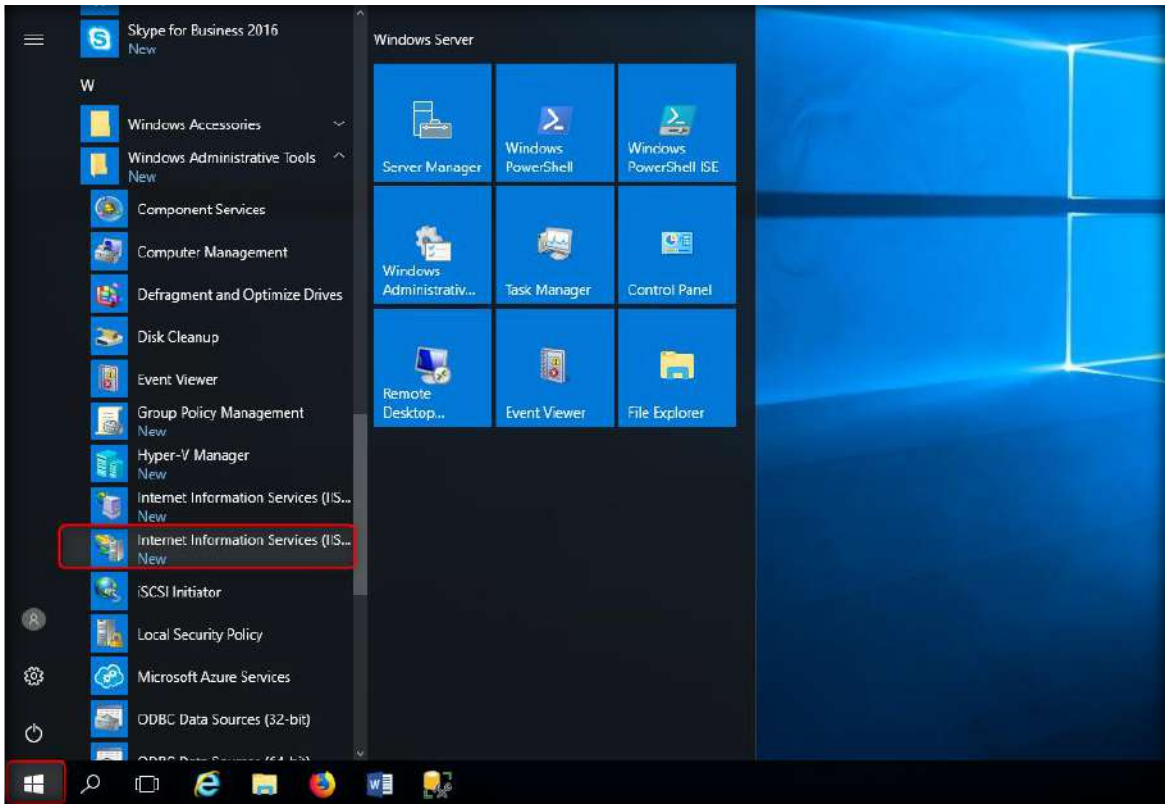


26. **Microsoft SQL Server Management Studio** pop-up appears stating that the database has been successfully created. Click **OK**

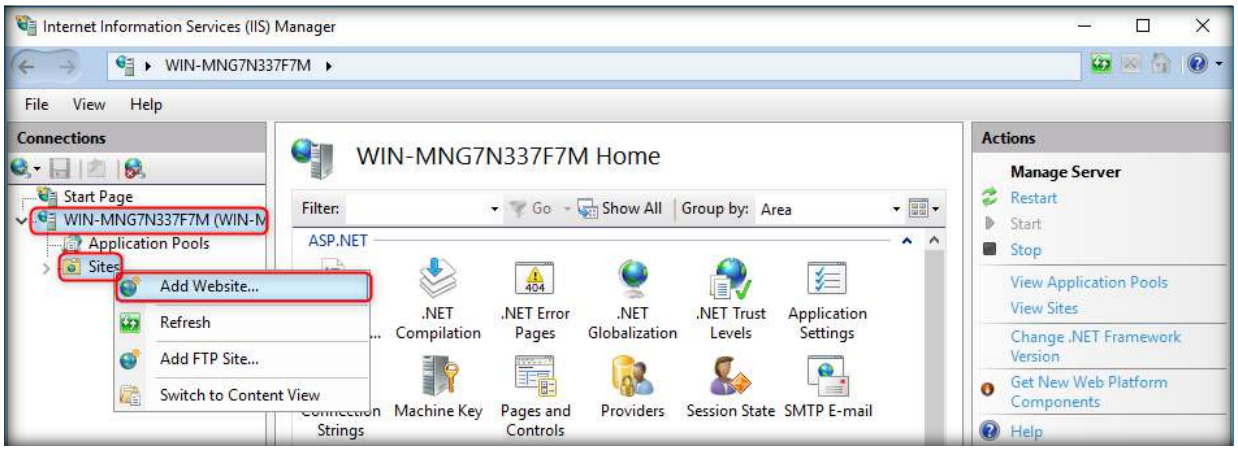


27. You have successfully **restored** the **database** of GoodShopping in your machine, GoodShopping website is now hosted in your local machine

28. Now click **Start** menu button, click **Windows Administrative Tools → Internet Information Services (IIS) Manager**

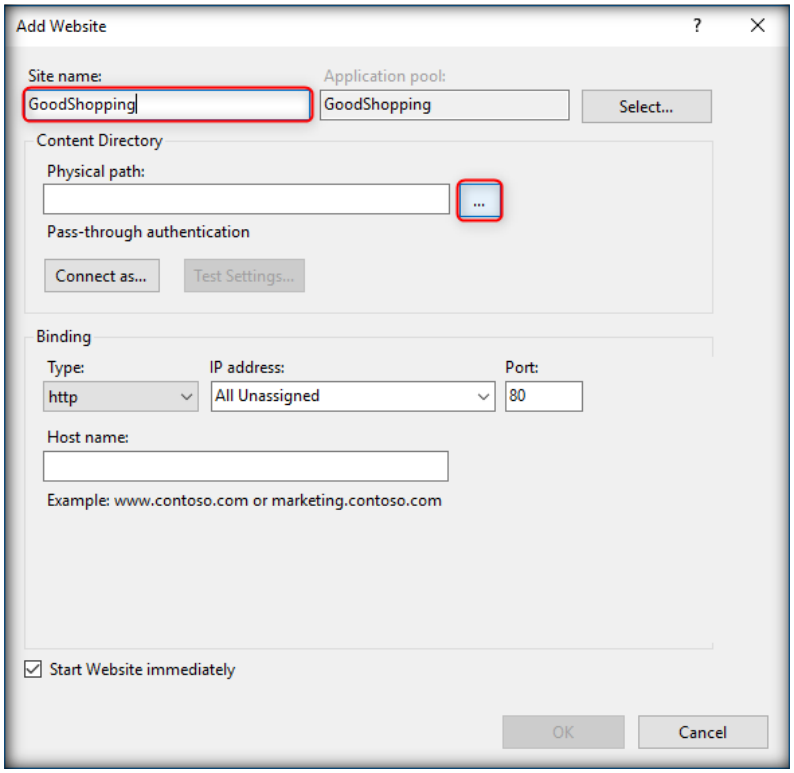


29. Internet Information Services (IIS) Manager main window appears, now in left pane of the window expand **Machine Name** and right click on **Sites** and click **Add Website...** from context menu.

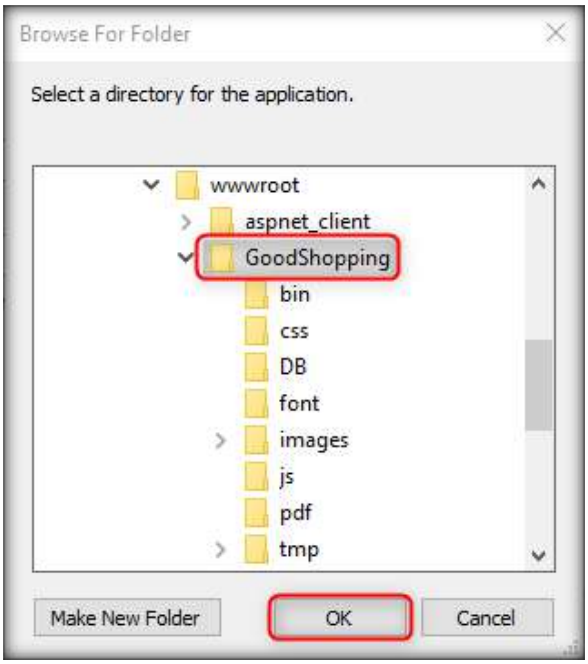


30. Add Website wizard appears, type the **Site** name in **Site name:** field and click on **Browse** button near **Physical path:** section

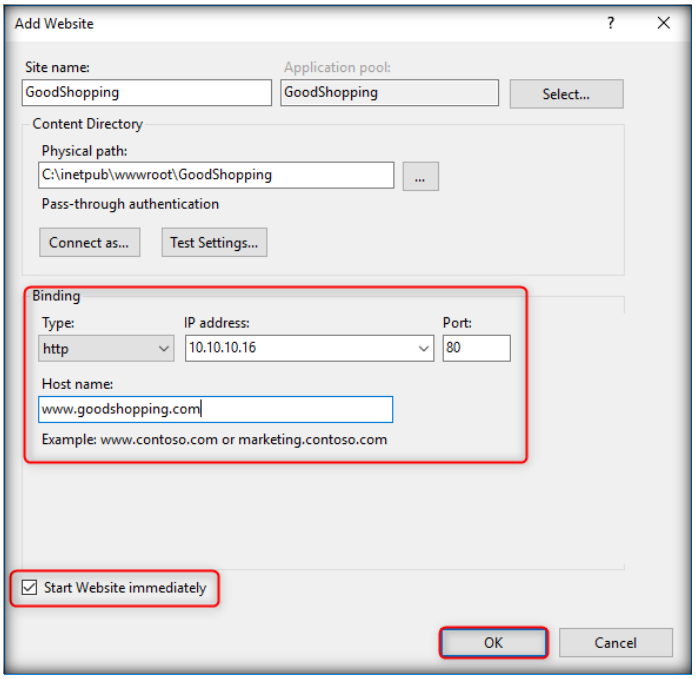
31. Here we are installing GoodShopping site, so we have provided **GoodShopping** in the Site name: field



32. **Browse** for Folder pop-up appears, navigate to C:\inetpub\wwwroot and choose **GoodShopping** folder and click **OK**.



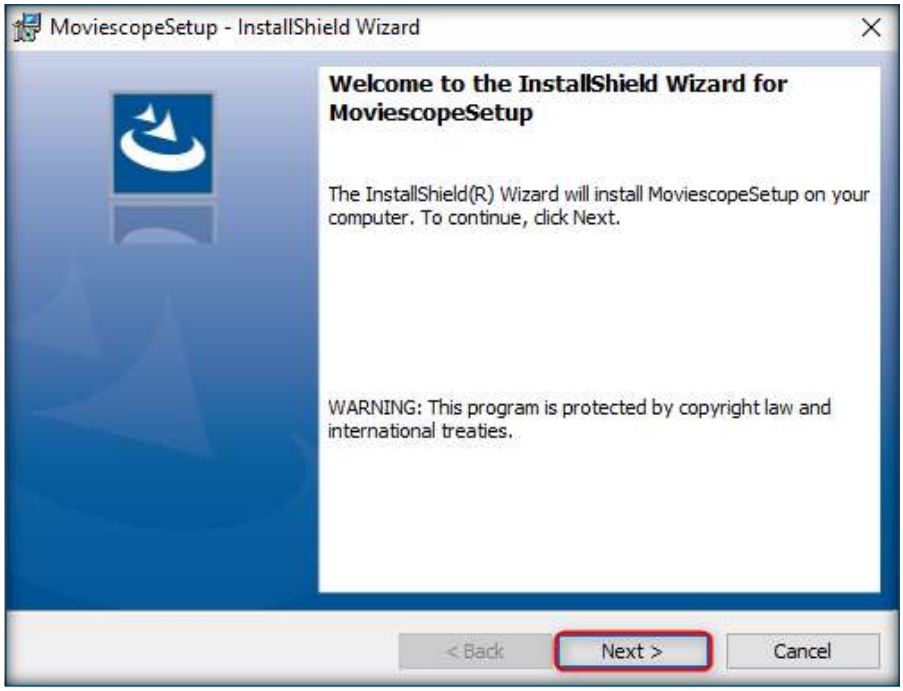
33. Now in Binding section choose **http** in Type: field. Choose the **Host machine IP address** from IP address: field, and choose **80** in Port: field.
34. Type www.goodshopping.com in Hostname: field, make sure that **Start Website immediately** is checked and click **OK**.



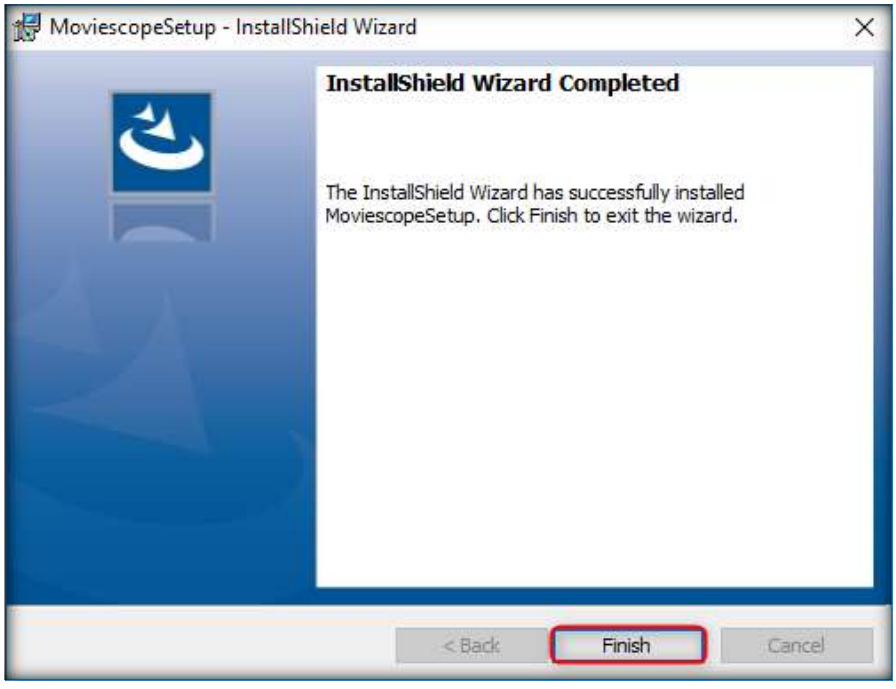
[Back to Configuration Task Outline]

CT#29: Configure the moviescope Website in Windows Server 2016 (Virtual Machine)

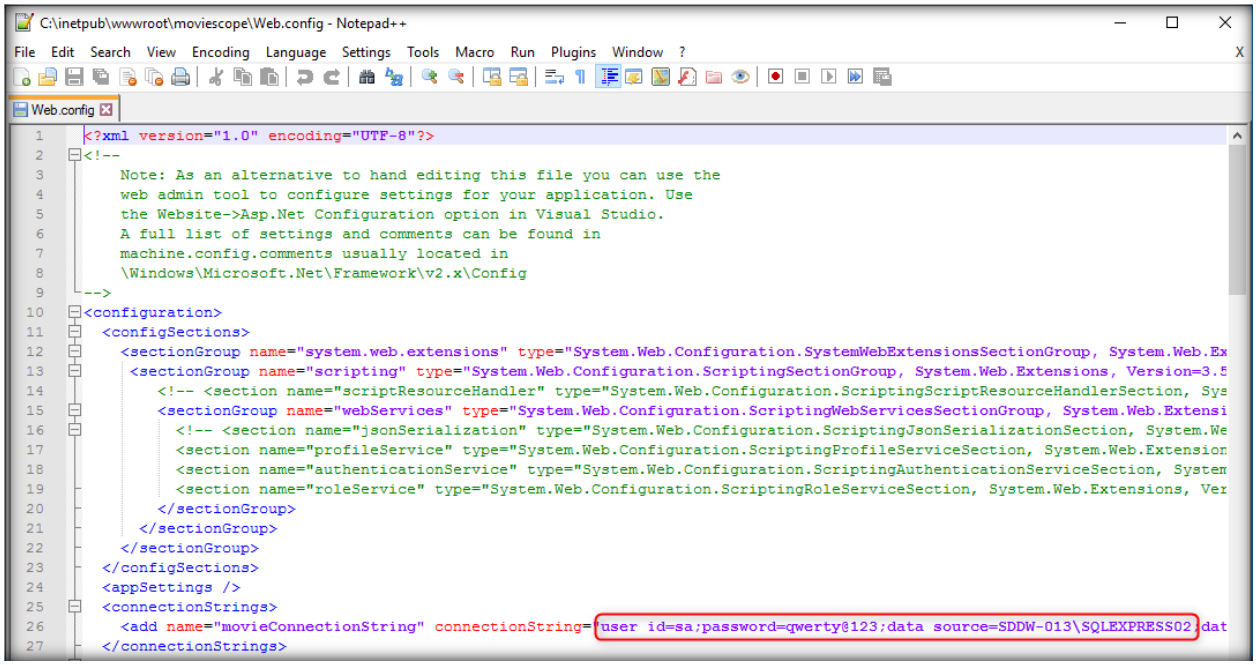
1. Open **Z:\CEH-Tools\CEHv10 Lab Prerequisites\Websites\moviescope**
2. Open **moviescope** folder. Double click on **Moviescope.exe** and follow the wizard driven installation steps to install



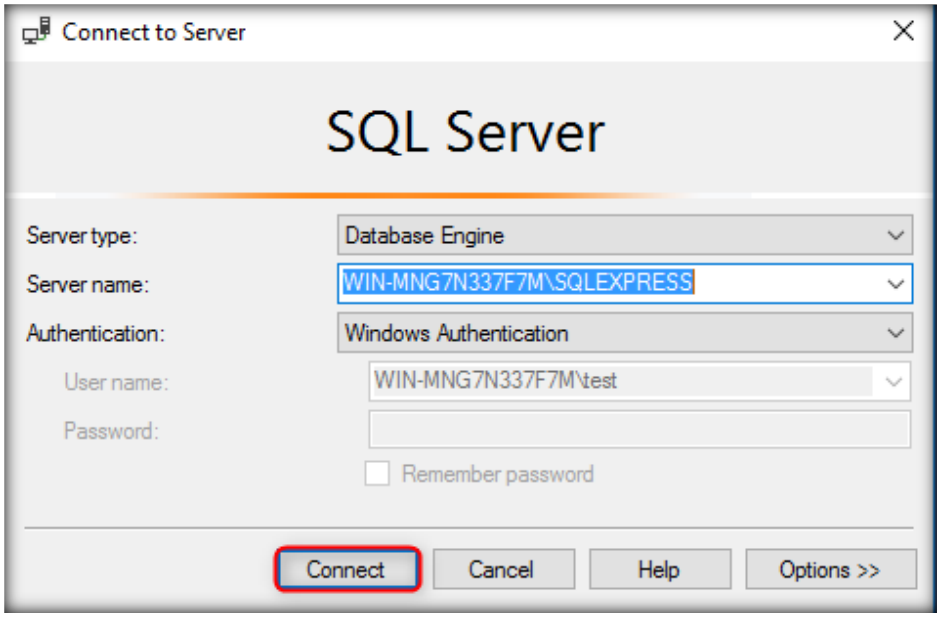
3. After completing the installation click **Close**



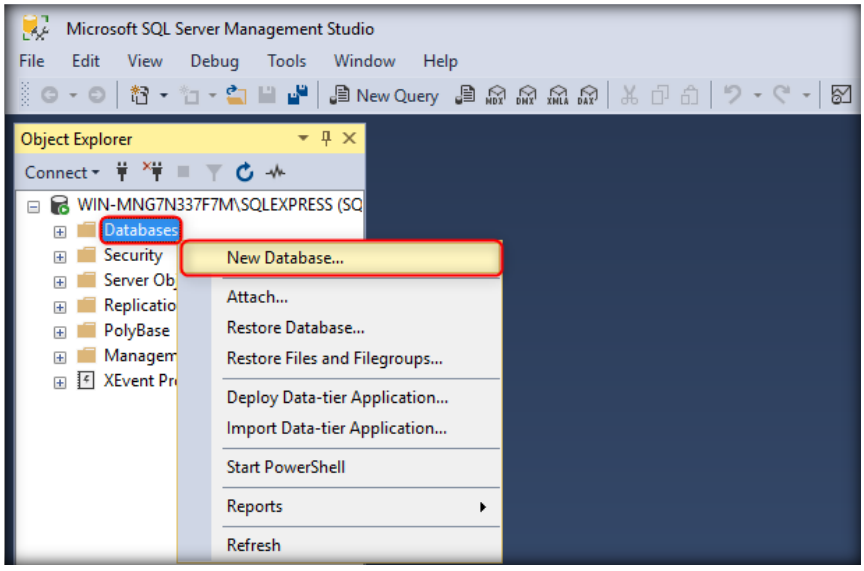
4. Open **moviescope** folder from **C:\inetpub\wwwroot\moviescope** and open **Web.config** file in notepad++ or in notepad
5. Scroll down to **connectionstring** tag in **line no. 26**, enter your machine's name in **data source=[Provide Your Host Machine Name]**, provide a user id after **User ID=sa**, and a password after **Password=qwerty@123**



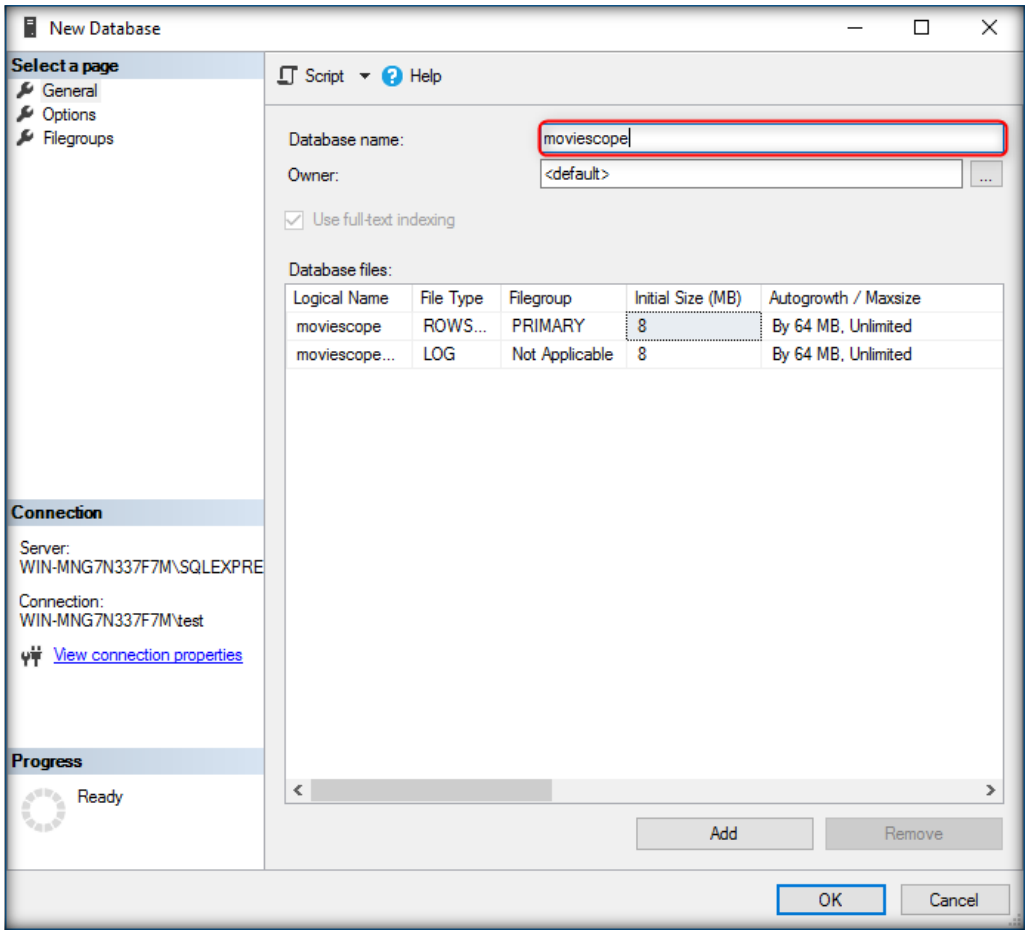
6. **Save** the file and **close** it
7. Now, **Launch** SQL Server 2017 Management Studio and click **Connect** to connect to the SQL Server



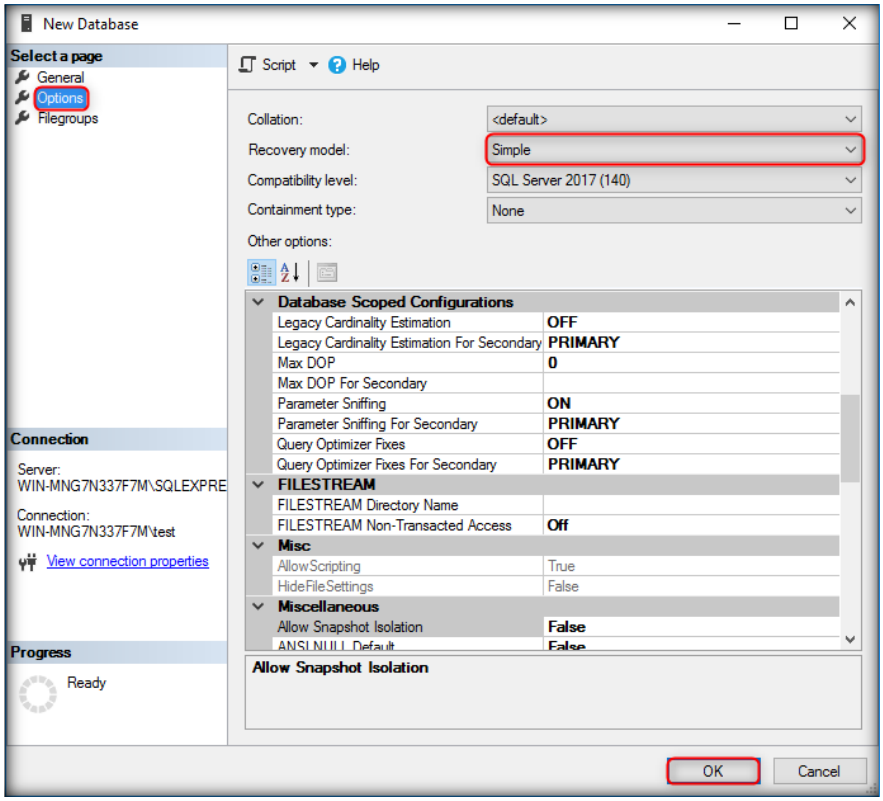
8. **Microsoft SQL Server Management Studio** window appears as shown in the following screenshot:
9. Right-click on **Databases** and select **New Database...**



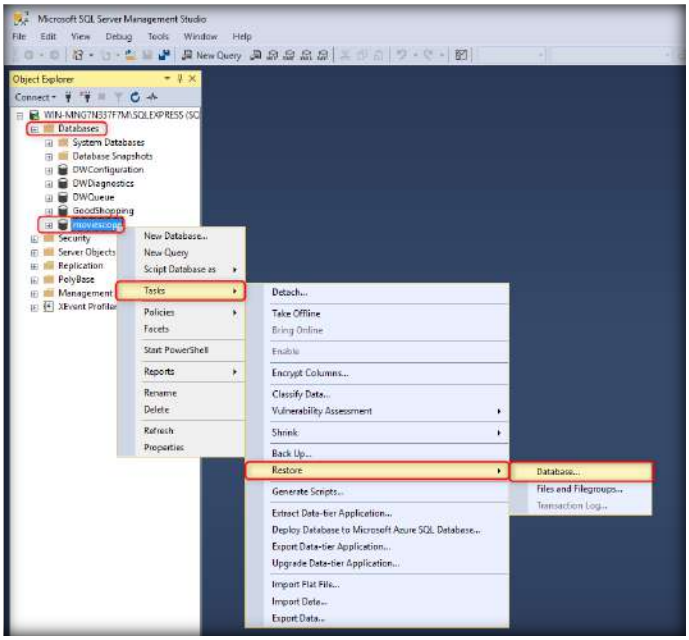
10. **New Database** window appears, specify **Database name** as **moviescope**



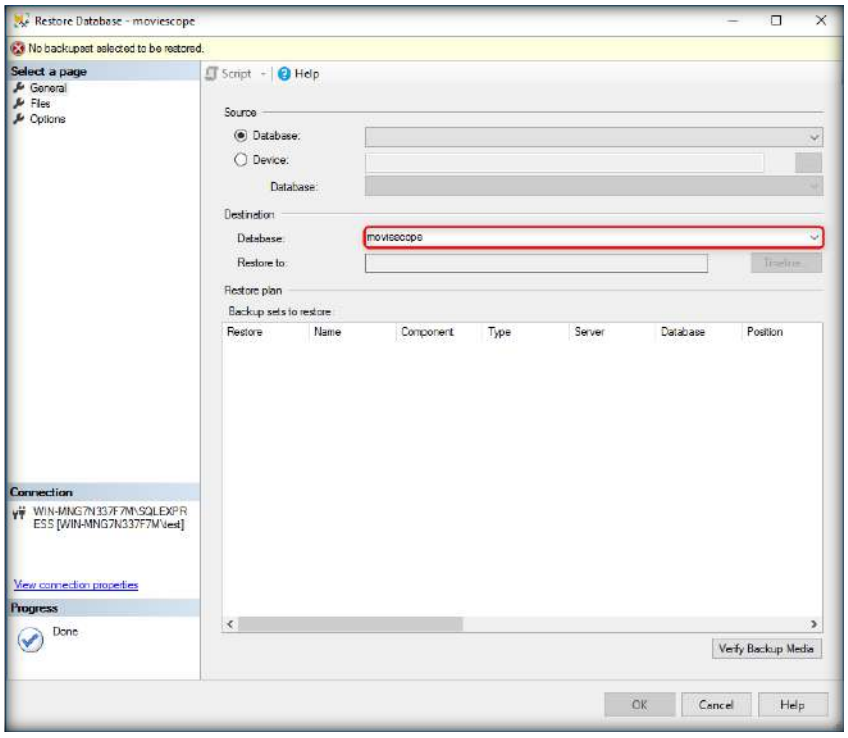
11. Select **Options** from the left pane.
12. Select **Simple** from the **Recovery model** drop-down list and click **OK**.



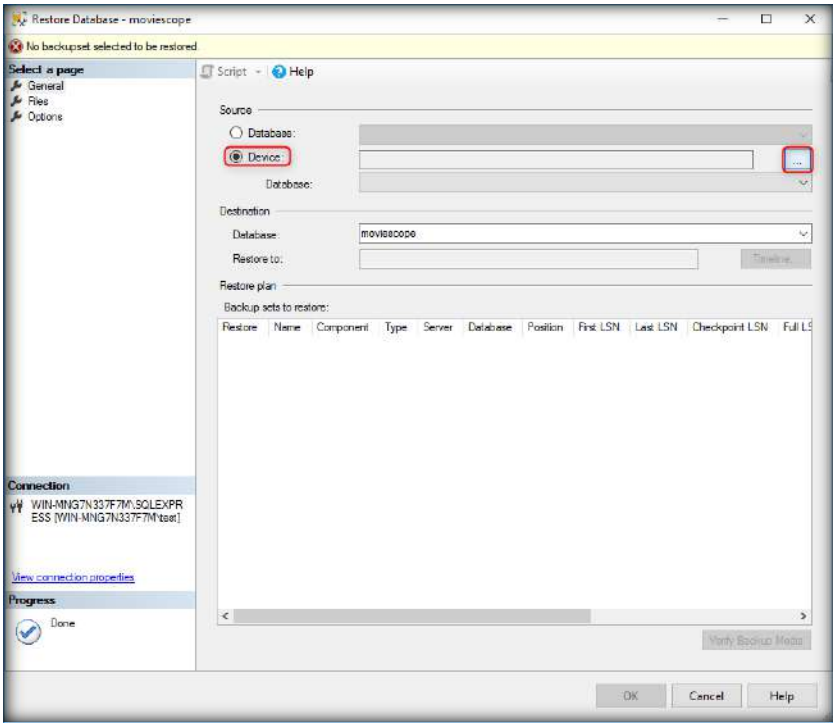
13. Now expand the **Databases** node. You will observe that **moviescope** database folder appears under the **Object Explorer** section, which implies that moviescope database has been **successfully** created.
14. **Right-Click** on **moviescope** database and go to **Tasks → Restore → Database...**



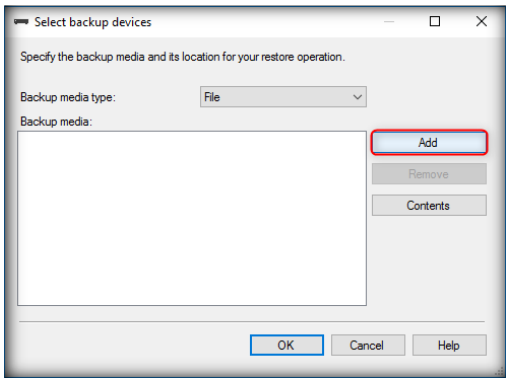
15. **Restore Database - moviescope** window appears displaying the database name (**moviescope**) in the **Database** field under **Destination** section



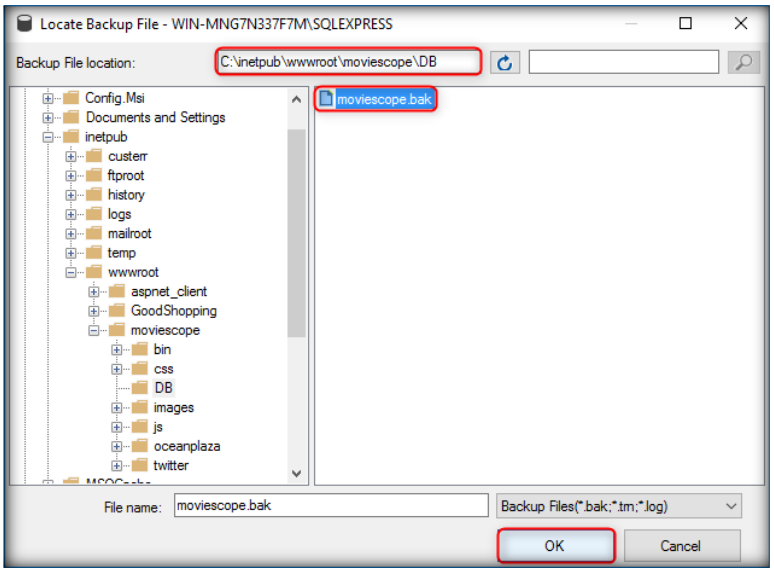
16. Click **Device** radio button under **Source** section and click  button located parallel to **Device** field



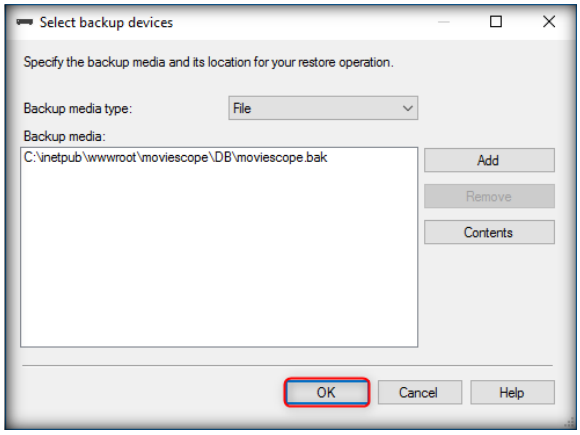
17. **Select backup devices** dialog-box appears, click **Add** button



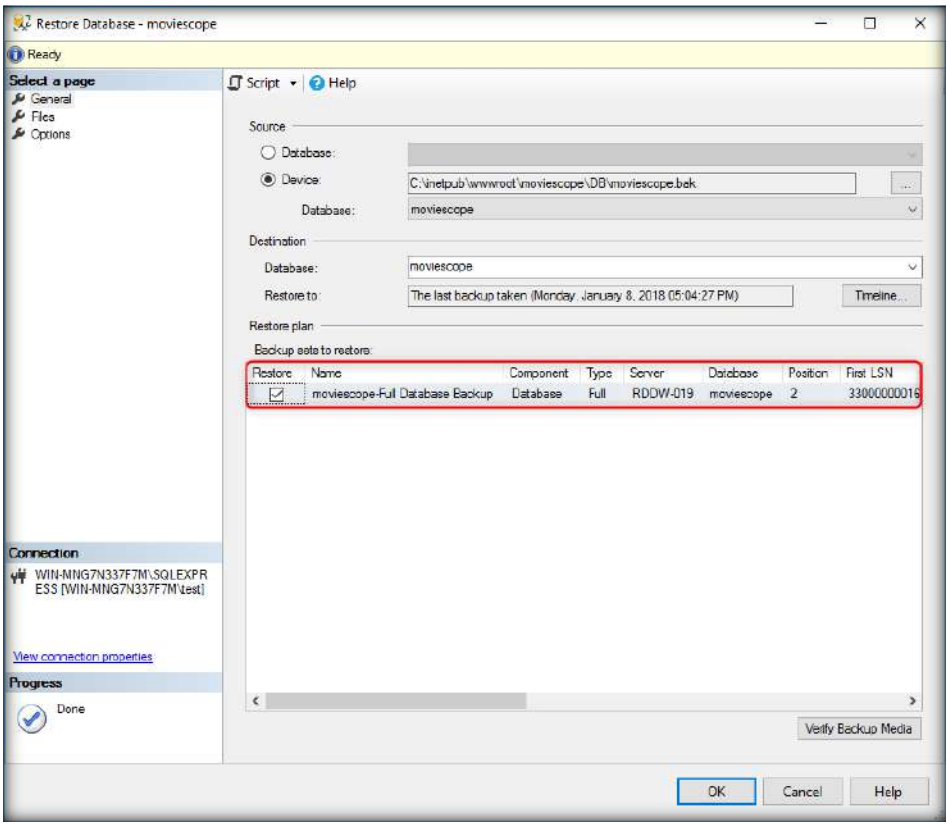
18. Navigate to the backup file (**moviescope.bak**) located in **C:\inetpub\wwwroot\moviescope\DB**
19. Select the backup file and then click **OK**. Locate Backup File window exits.



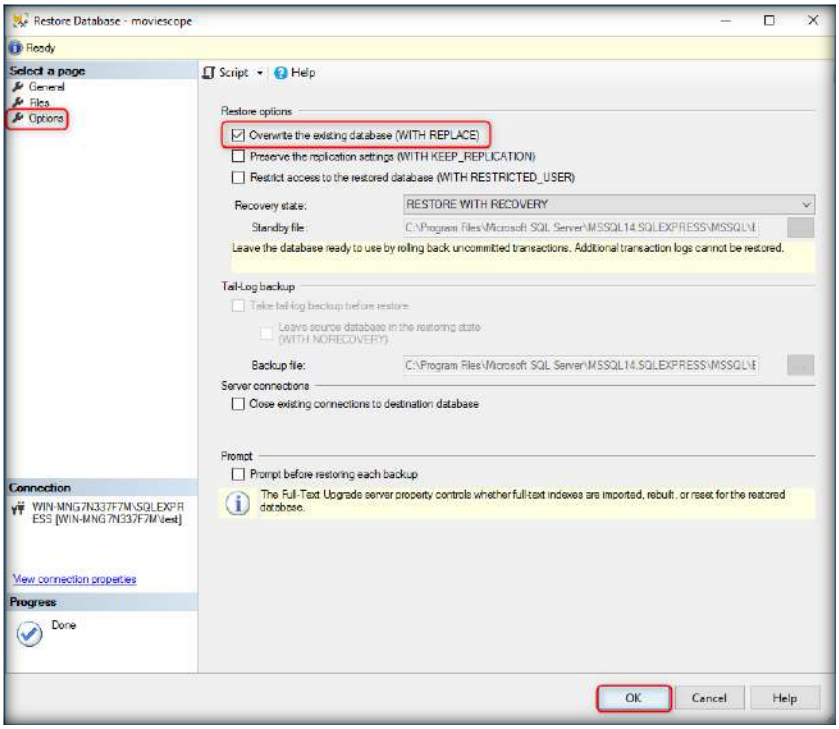
20. Under Backup media section, the location of **moviescope.bak** website is listed
21. Click **OK**, Select backup devices window exits



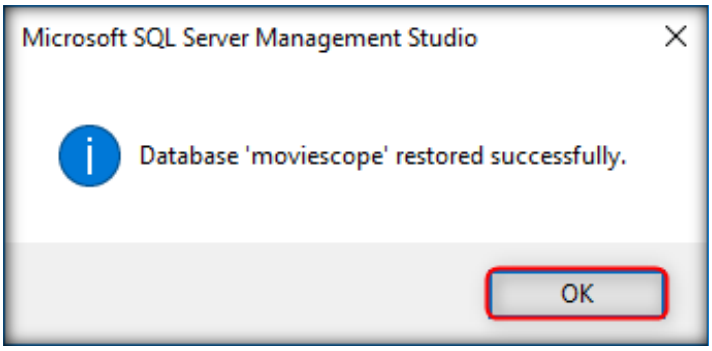
22. You will observe that the backup file has been successfully added. Ensure that the backup file is checked.



23. Click **Options** in left pane, check **Overwrite existing database** under **Restore options** section and the click **OK**



24. **Microsoft SQL Server Management Studio** pop-up appears stating that the database has been successfully created. Click **OK**



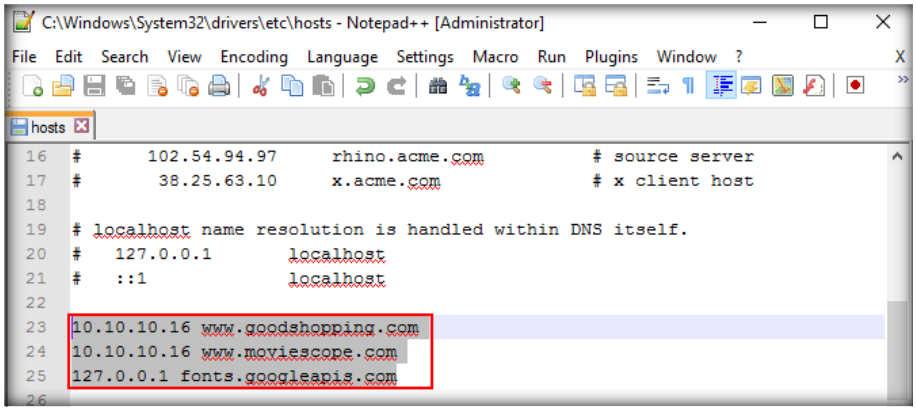
25. You have successfully **restored** the **database** of moviescope in your machine
26. Similarly follow the steps from **28** to **34** from the previous configuration task of GoodShopping to configure MovieScope site as www.moviescope.com

[Back to Configuration Task Outline]

CT#30: Configure Hosts file in all the Virtual Machines

Configuring Hosts File in Windows Server 2016 and Windows Server 2012

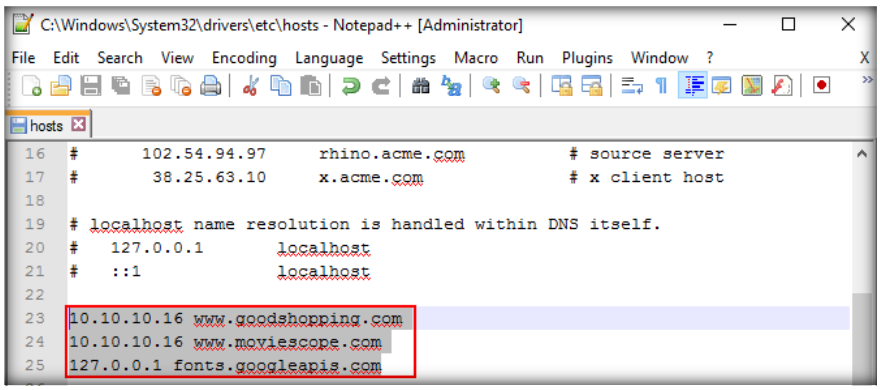
1. In Windows Server 2016 navigate to C:\Windows\System32\drivers\etc and right click on **hosts** file and click **Edit with Notepad++** from context menu
2. Hosts file opens in Notepad++ type **<IP Address of the Windows Server 2016> www.goodshopping.com, <IP Address of the Windows Server 2016> www.moviescope.com,** and **127.0.0.1 fonts.googleapis.com** then click **Save** button and close the Notepad++ window.



3. Similarly, follow the above 2 steps to configure the hosts file in Windows Server 2012

Configuring Hosts File in Windows 10 and Windows 8

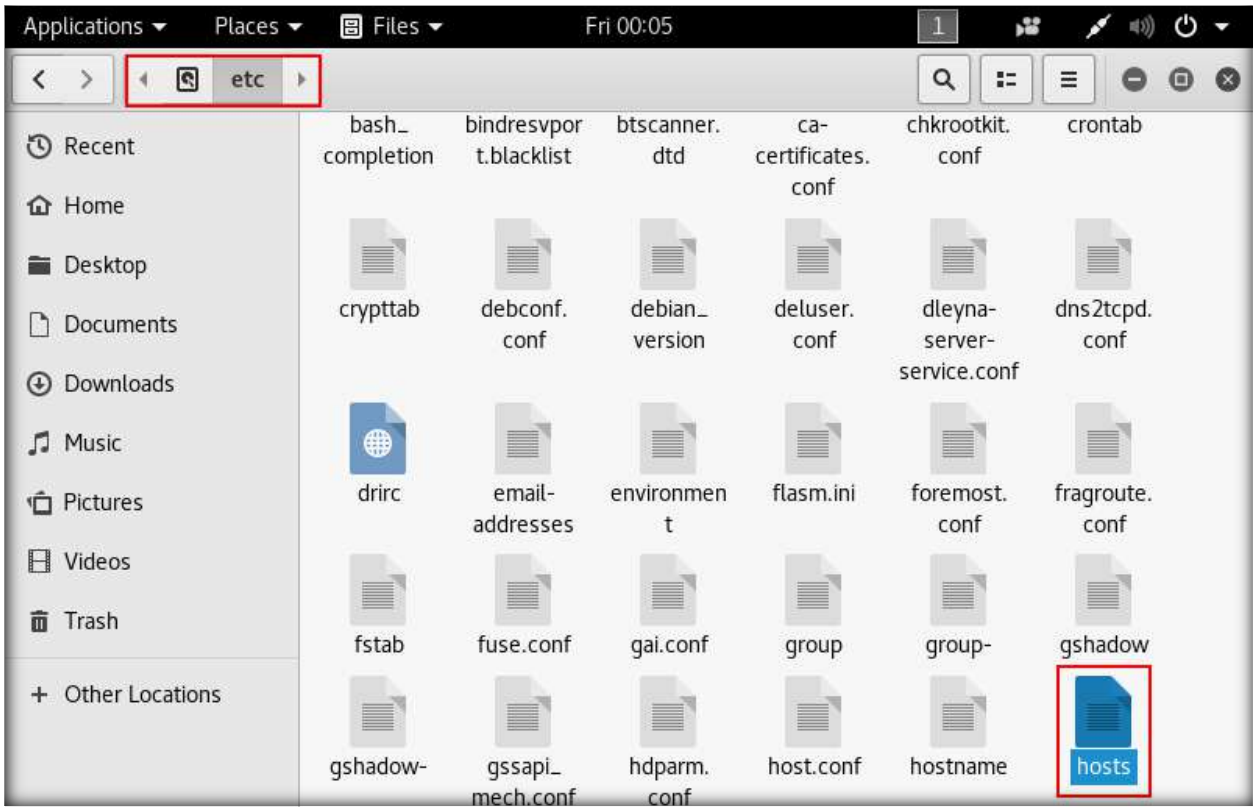
1. In Windows 10 navigate to C:\Windows\System32\drivers\etc and copy the hosts file to Desktop and right click on **hosts** file and click **Edit with Notepad++** from context menu
2. Hosts file opens in Notepad++ type **<IP Address of the Windows Server 2016> www.goodshopping.com, <IP Address of the Windows Server 2016> www.moviescope.com,** and **127.0.0.1 fonts.googleapis.com** then click **Save** button and close the Notepad++ window.



3. Paste the hosts file in the following location C:\Windows\System32\drivers\etc
4. Similarly, follow the above 3 steps to configure the hosts file in Windows 8

Configuring Hosts File in Kali Linux

1. Launch and login to Kali Linux machine, and navigate to **Places → Computer → etc** and double click **hosts** file

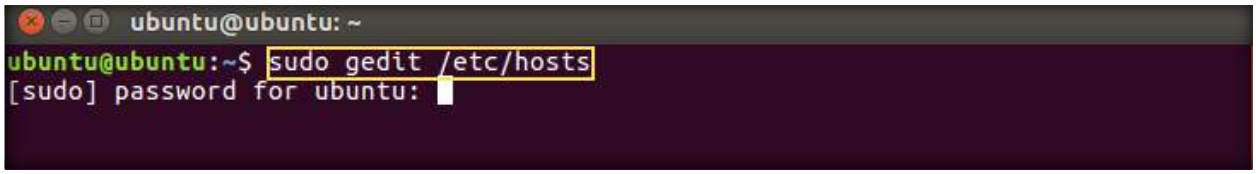


2. Hosts file opens in a text editor window, type <**IP Address of the Windows Server 2016**> **www.goodshopping.com**, <**IP Address of the Windows Server 2016**> **www.moviescope.com**, and **127.0.0.1 fonts.googleapis.com** then click **Save** button and close

Configuring Hosts File in Ubuntu

1. Launch and login to Ubuntu machine, click terminal icon from the launcher bar to launch

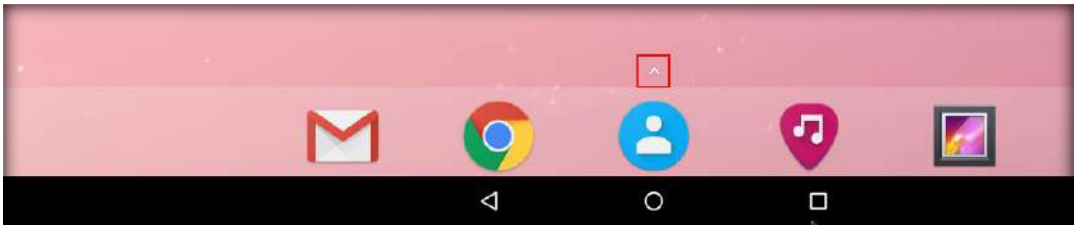
2. Type **sudo gedit /etc/hosts** and press **Enter**. It will prompt you to enter the root password, type **toor** in the password field and press **Enter**



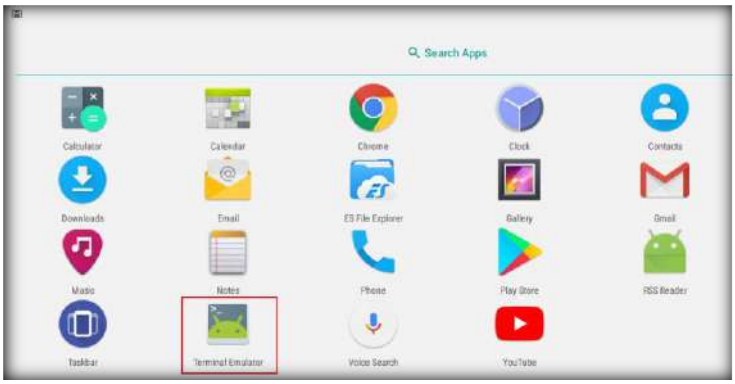
3. Hosts file opens in the text editor window, type <**IP Address of the Windows Server 2016**> **www.goodshopping.com**, <**IP Address of the Windows Server 2016**> **www.moviescope.com**, and **127.0.0.1 fonts.googleapis.com** then click **Save** button and close

Configuring Hosts File in Android

1. Launch and power on the Android virtual machine in the VMware Workstation. Click **App Drawer** (^) icon as shown in the screenshot

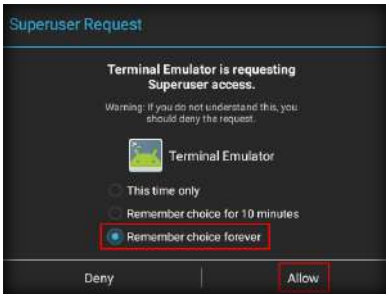


2. Click **Terminal Emulator** icon to launch terminal



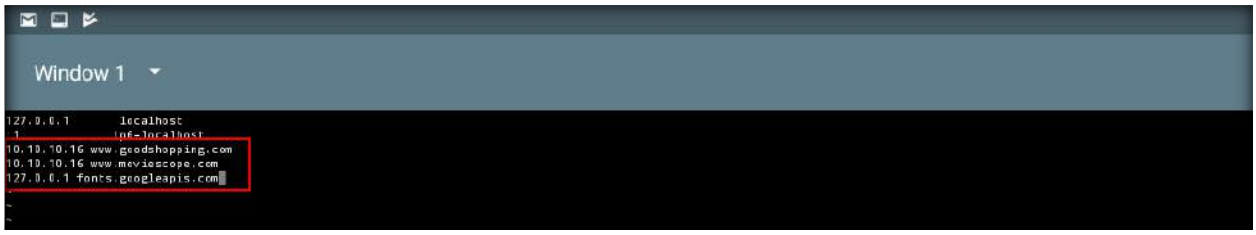
3. Type **su** and press **Enter** to gain the root access

4. Superuser Request pop-up appears, choose **Remember choice forever** radio button and click **Allow**

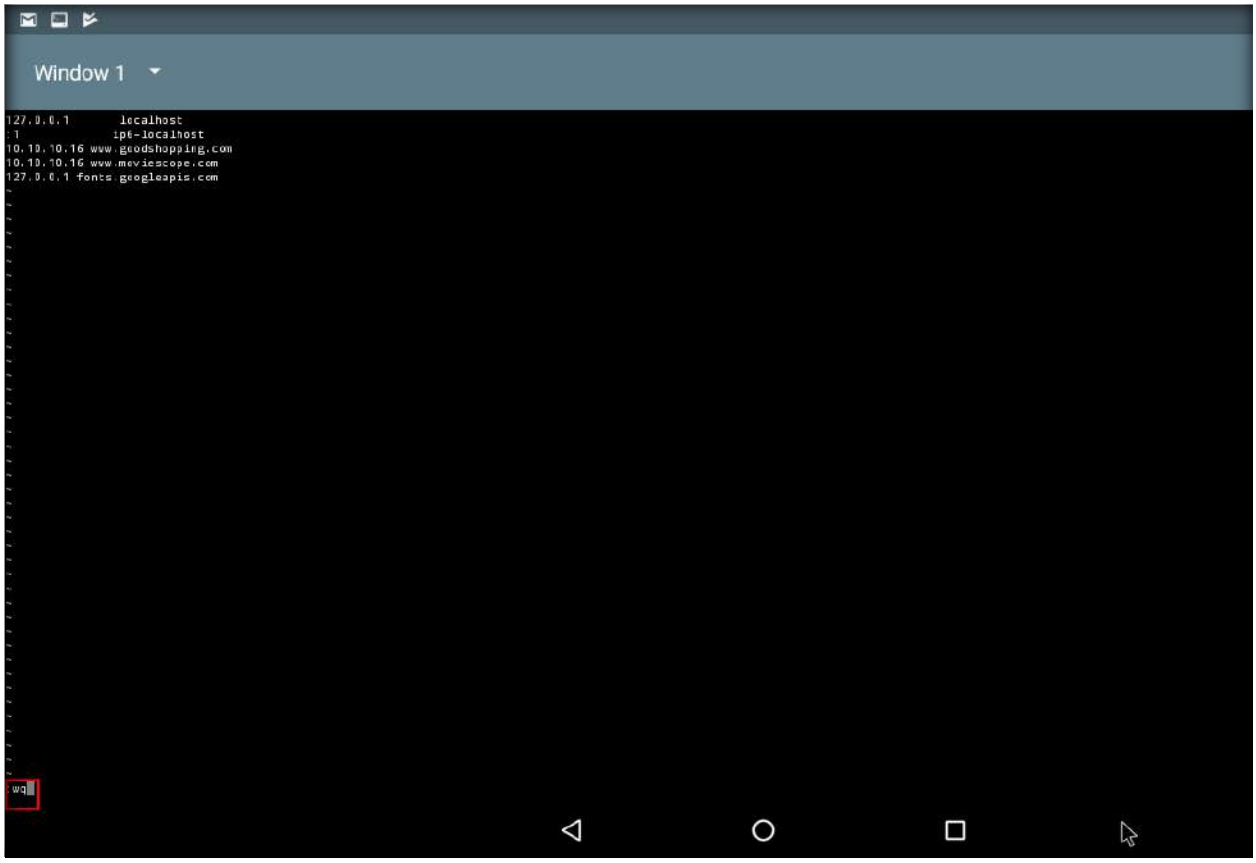


5. Type **vi /etc/hosts** in the terminal and press **Enter** to edit hosts file

6. In the text editor window press **Shift+I** on your keyboard to allow editing. Type <**IP Address of the Windows Server 2016**> **www.goodshopping.com**, <**IP Address of the Windows Server 2016**> **www.moviescope.com**, and **127.0.0.1 fonts.googleapis.com**



7. Press **Esc** button on keyboard and type **:wq** and press **Enter** to write and quit from the text editor window

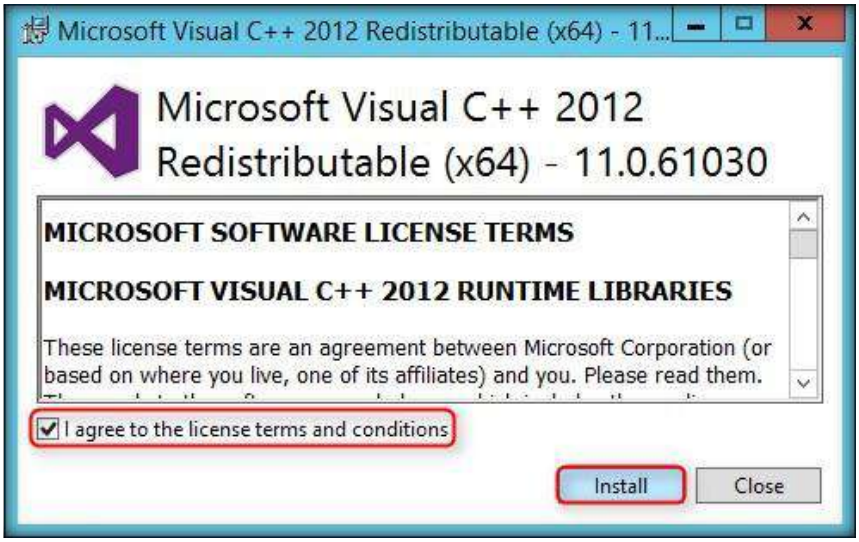


Note: Once you have configured hosts file in all the machines, open any browser and browse the local websites i.e., www.goodshopping.com and www.moviescope.com in all the virtual machines.

[Back to Configuration Task Outline]

CT#31: Install WampServer in Windows Server 2012

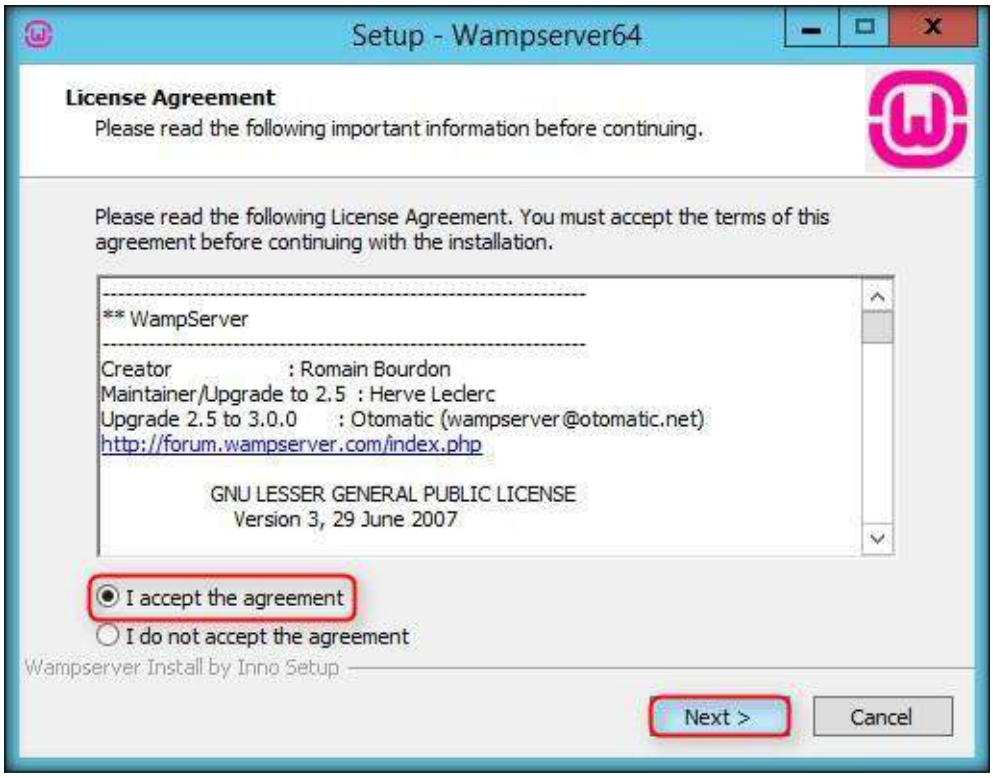
1. Launch **Windows Server 2012** virtual machine
2. To install Wamp server without any errors, you need to install **Microsoft Visual C++ 2012 Redistribute** first
3. Navigate to **Z:\CEH-Tools\CEHv10 Lab Prerequisites\Microsoft Visual C++ 2012** and double-click **vcredist_x64.exe**
4. **Microsoft Visual C++ 2012 x64 Redistributable Setup** window appears. Accept the license terms and click **Install**.



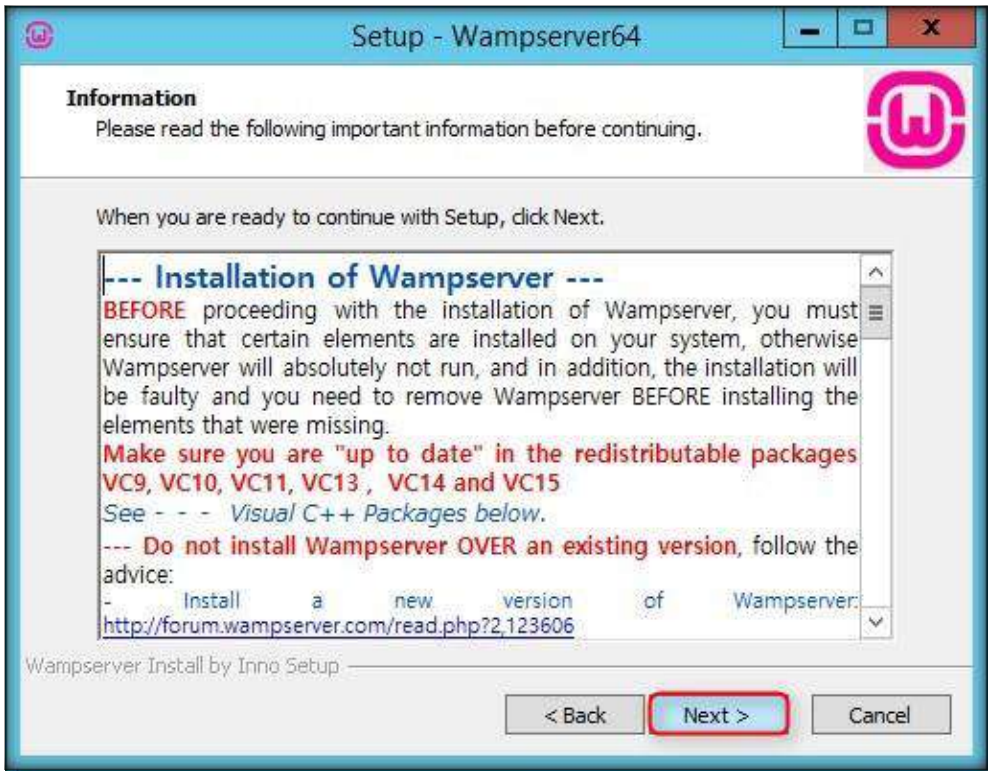
5. On completion of installation, click **Close**
6. In the same way, follow the wizard driven steps to install **Microsoft Visual C++ 2008 Redistribute, Microsoft Visual C++ 2010 Redistribute, Microsoft Visual C++ 2013 Redistribute, Microsoft Visual C++ 2015 Redistribute, Microsoft Visual C++ 2017 Redistribute** packages

   Note: If you are running a x64 bit system, you have to install both x64 and x86 versions of the packages
7. Navigate **Z:\CEH-Tools\CEHv10 Module 18 Cloud Computing\WAMP Server** and double-click **wampserver3.1.0_x64.exe**
8. Select Setup Language window appears, click **OK**

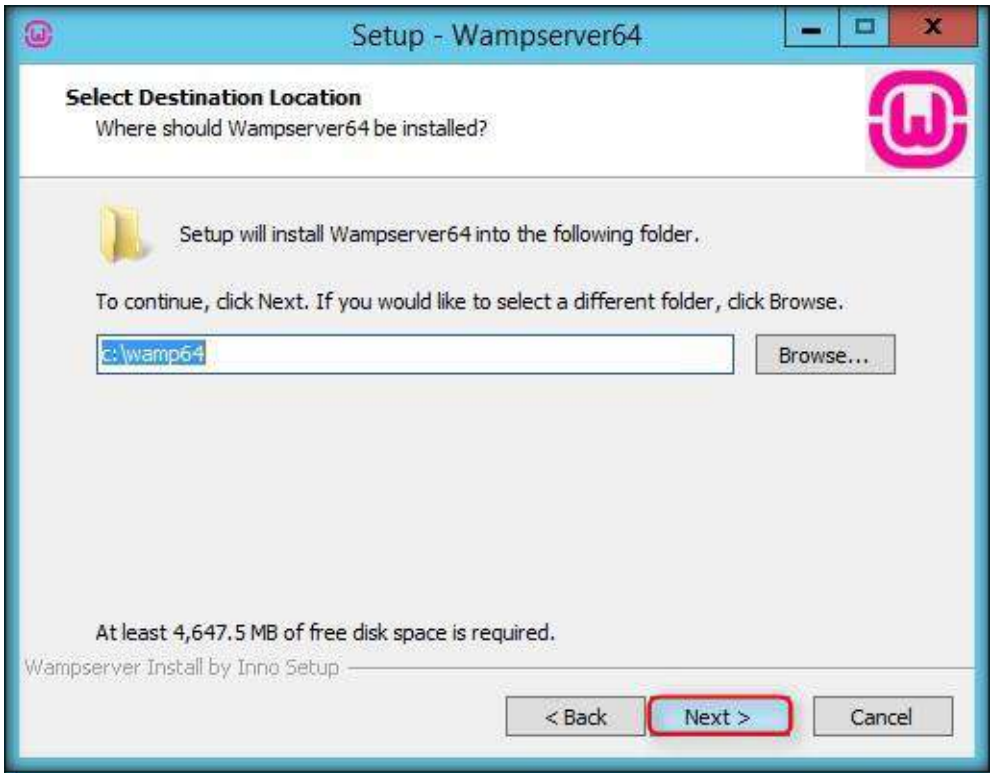
9. In the **License Agreement** section, accept the license agreement and click **Next**



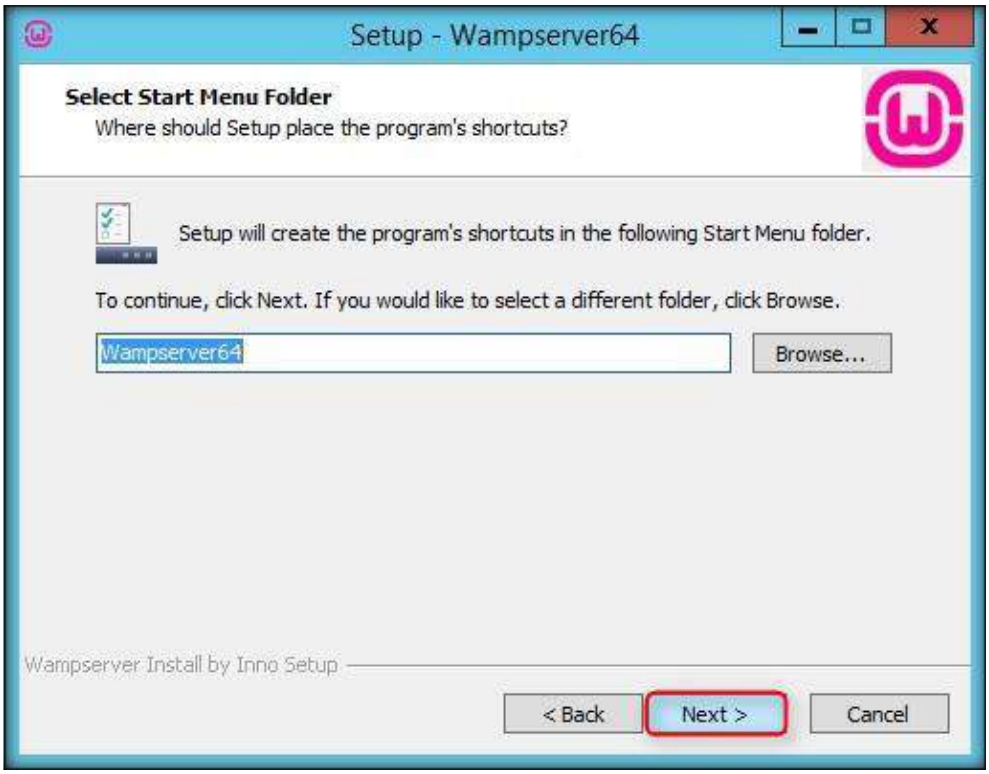
10. **Information** section appears, make sure you have the redistributable packages mentioned here and click **Next**



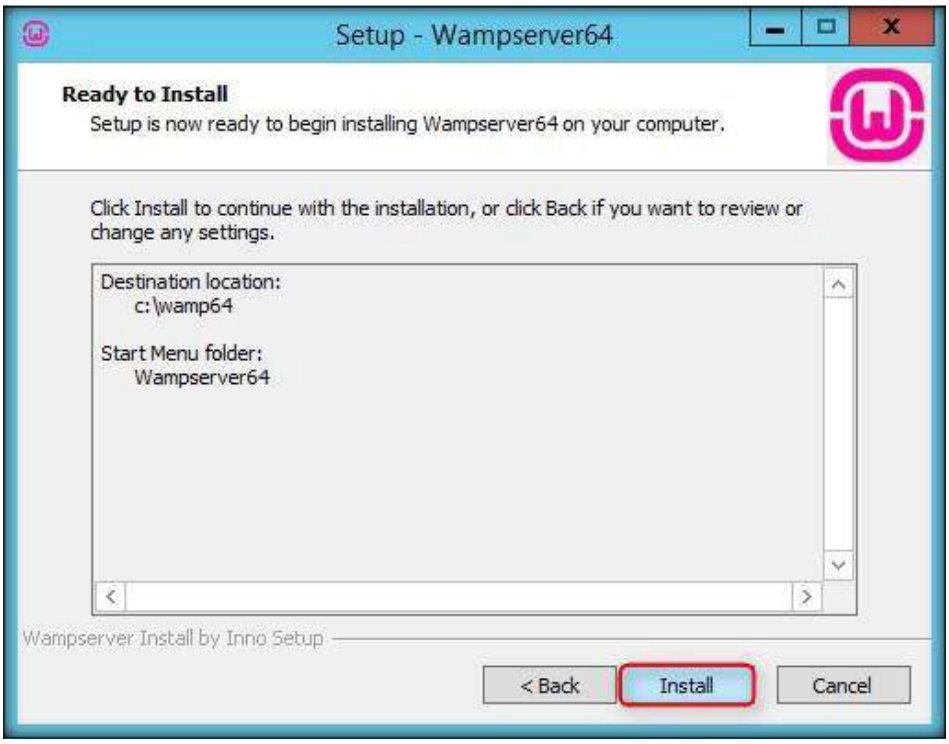
11. **Select Destination Location** section appears, specify a location where you want to install the server and click **Next**



12. **Select Start Menu Folder** section appears, click **Next**

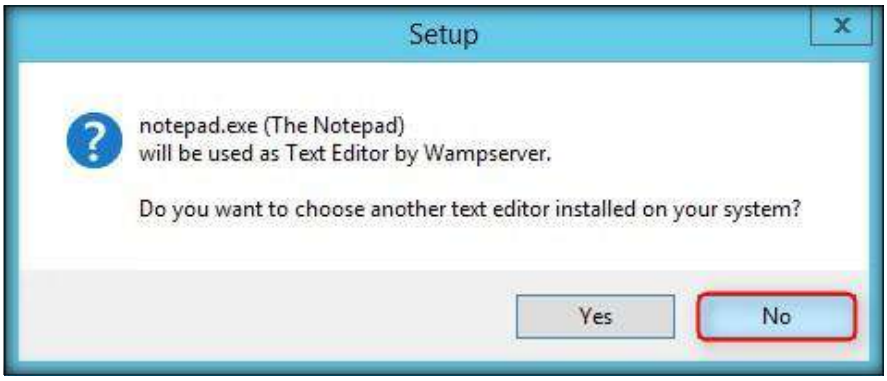


13. Ready to Install section appears, click **Install**

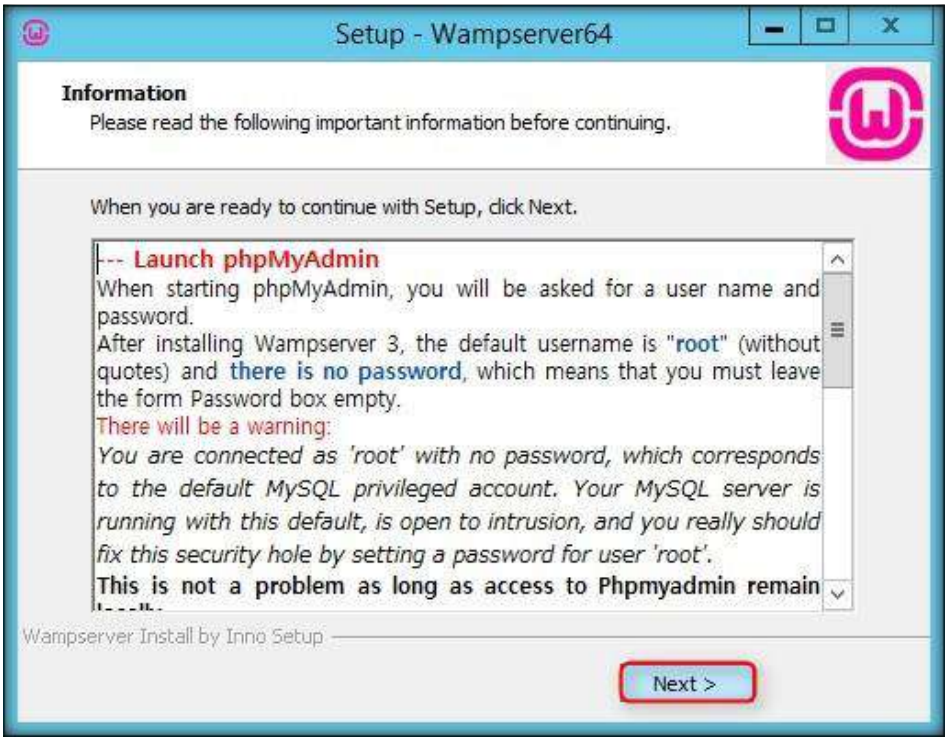


14. Setup pop-up appears, asking to choose the browser to be used by Wampserver, click **No**

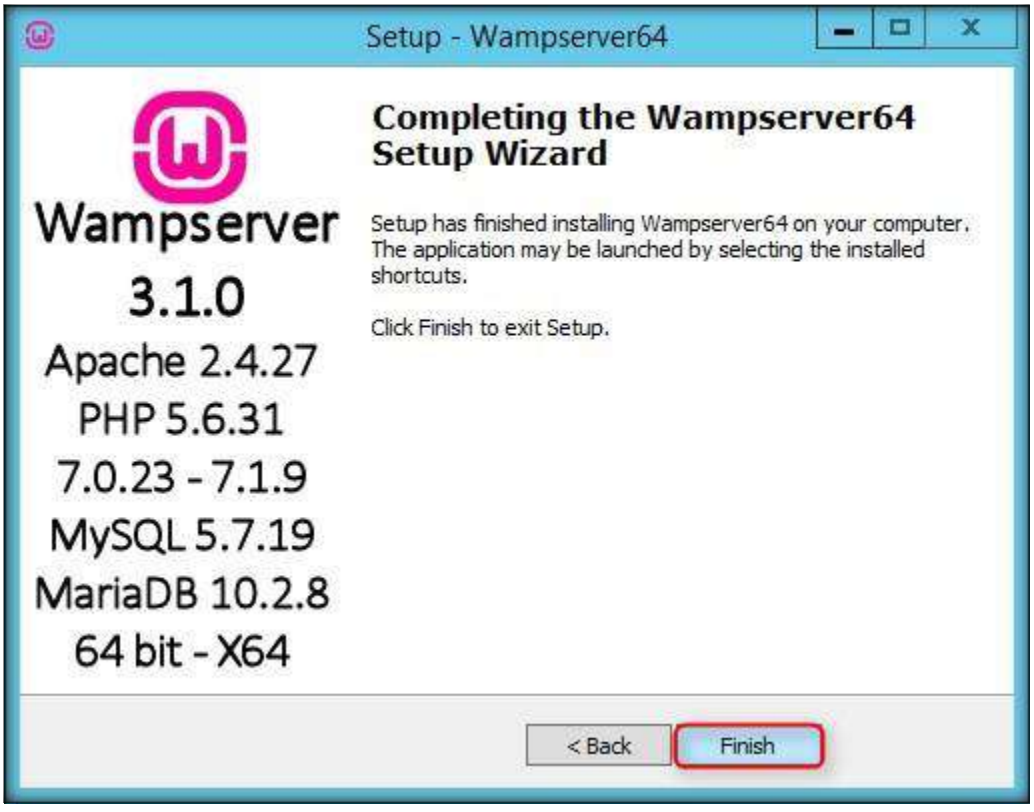
15. Another Setup pop-up appears, asking to choose the text editor to be used by Wampserver, click **No**



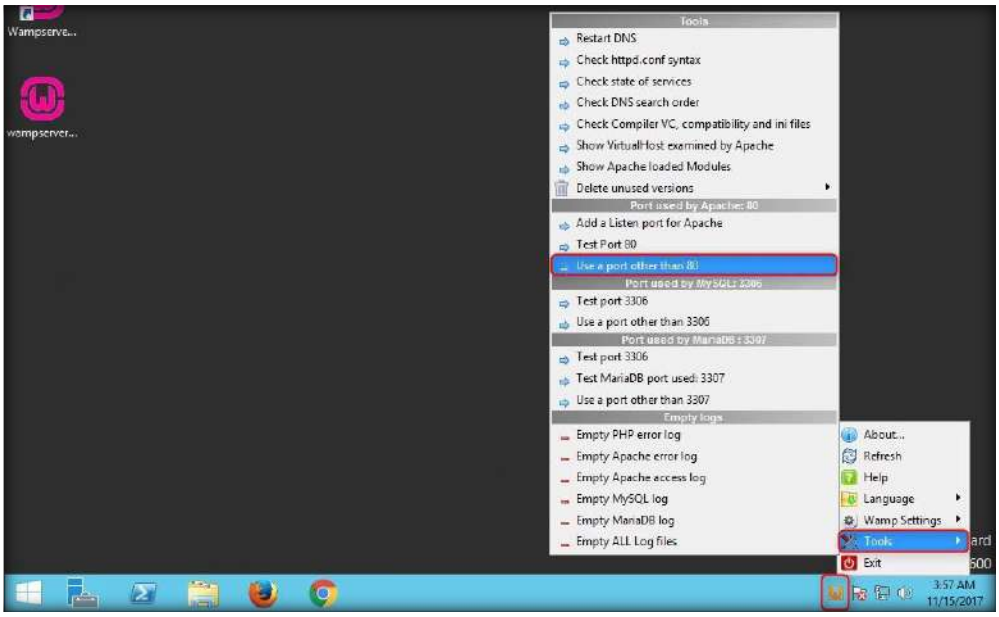
16. Information section appears, click **Next**
17. It takes some time for the server to install



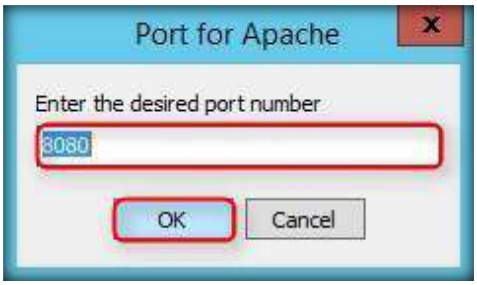
18. Completing the Wampserver64 Setup Wizard section appears, click **Finish**



19. Right-click the Wampserver icon from the taskbar notification area and go to **Tools → Port used by Apache → Use a port other than 80**

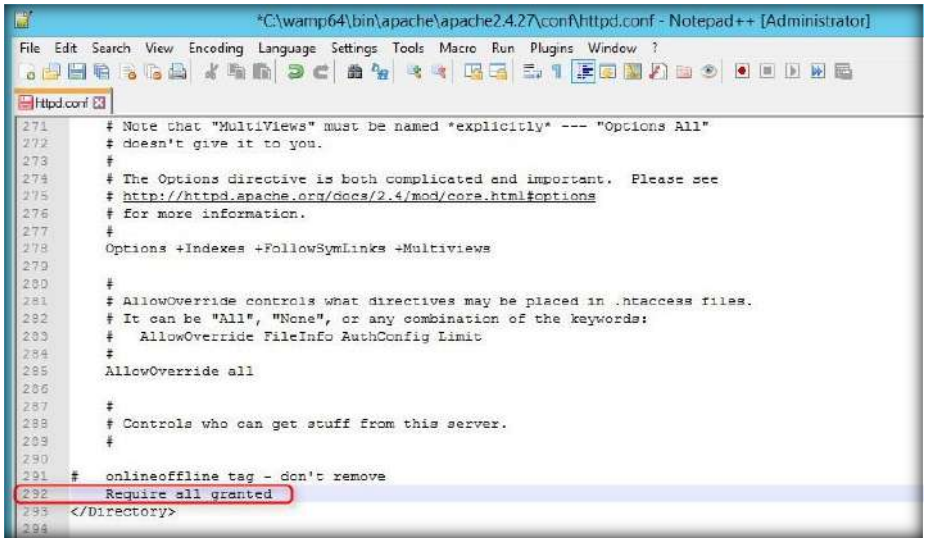


20. Port for Apache window appears, type **8080** as the new port number and click **OK**



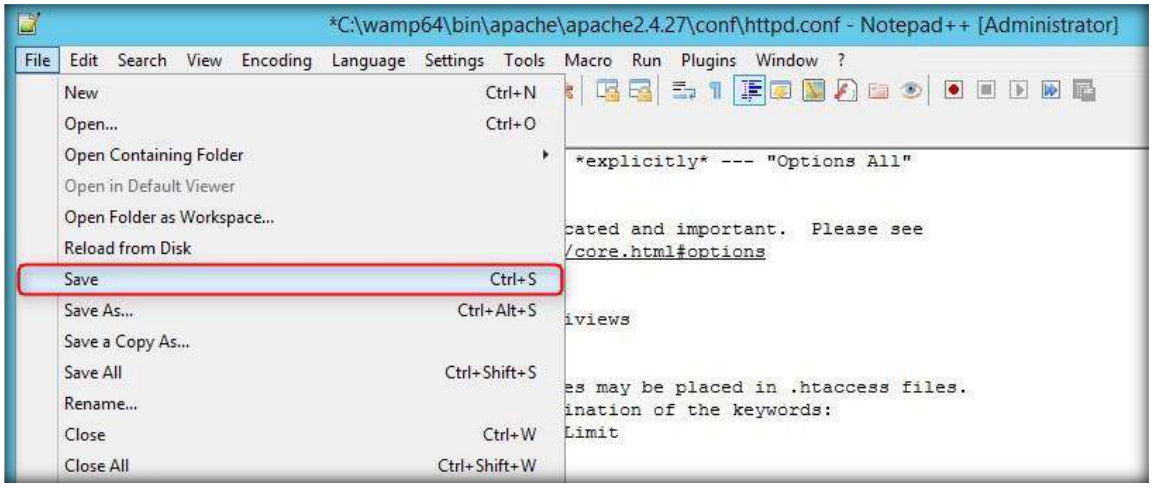
21. Navigate to the location **C:\wamp64\bin\apache\apache2.4.27\conf**, open **httpd.conf** file with **Notepad++** i.e., right-click on **httpd.conf** file and select **Edit with Notepad++**.

22. Scroll down to **line no. 292** and change the script from **Require local** to **Require all granted**



23. Click **File** from the menu bar and then click **Save**

    Note: You can also press **Ctrl+S** on the keyboard to save the file



24. **Close** the file and all the other folders that were open. Click **Wamp server** icon from the system tray, and then click **Restart All Services**

25. Wait until the icon turns green

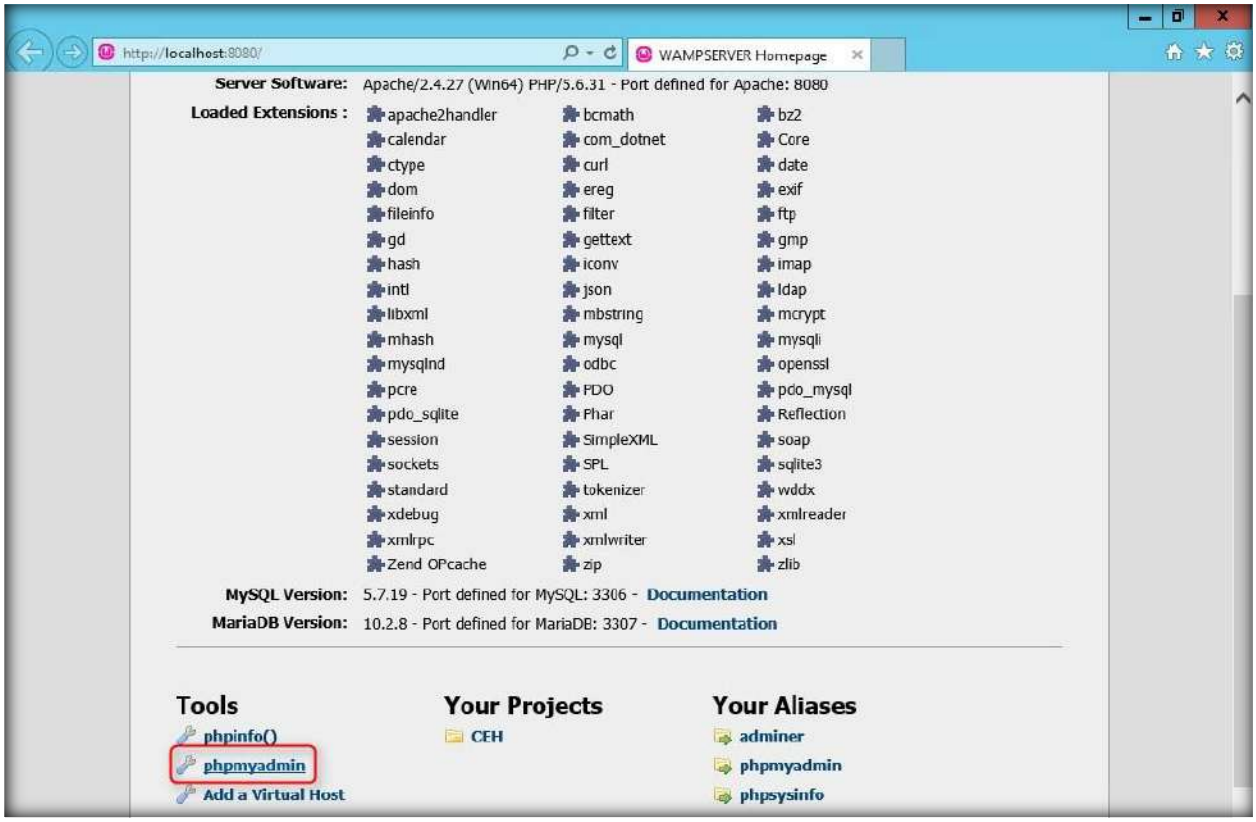
[Back to Configuration Task Outline]

CT#32: Install and Configure WordPress Website

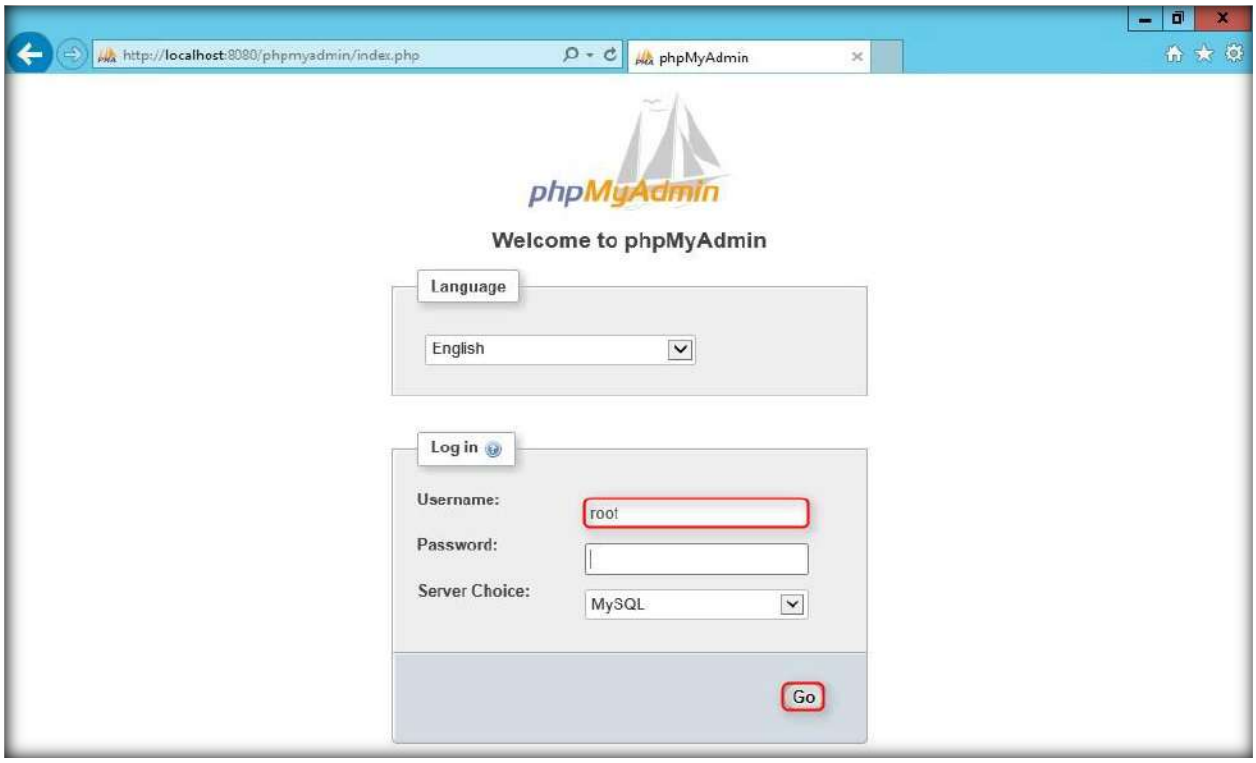
1. Click the **WampServer** icon in the notification area and select **Localhost**

2. As soon as you click the icon, the WAMPSERVER home page appears in the default browser. Click **phpmyadmin** link under **Tools** section.

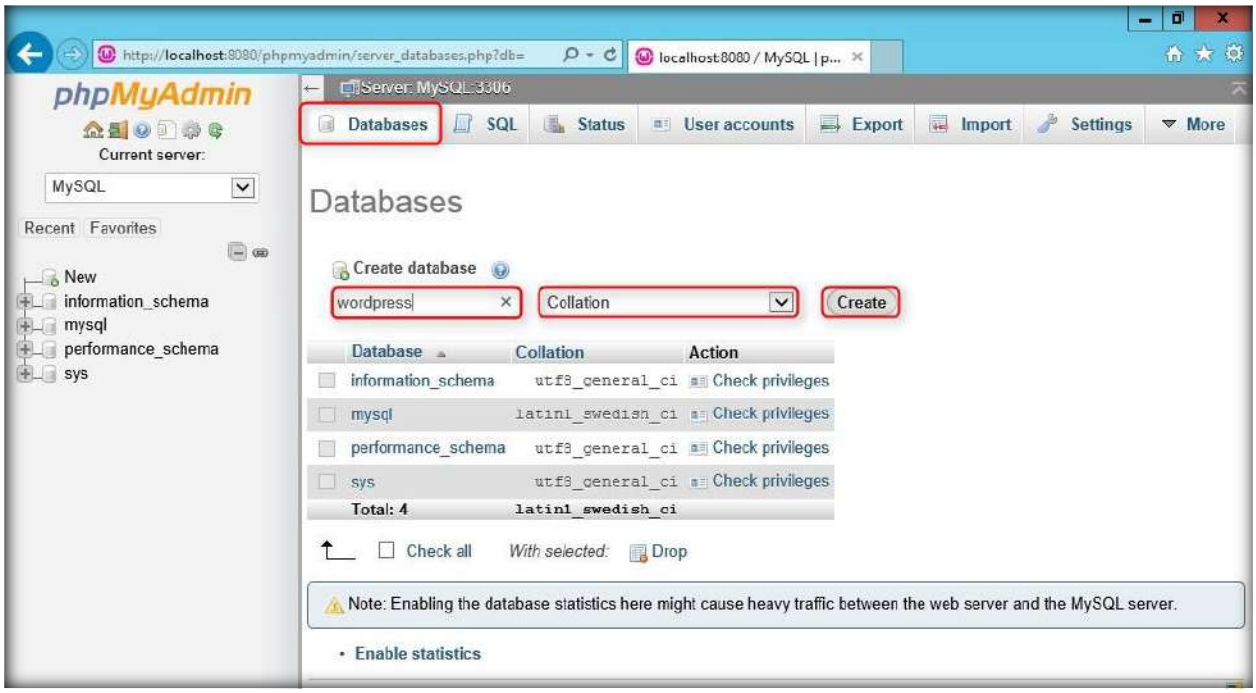
   Note: Screenshots may differ if you are using different browser



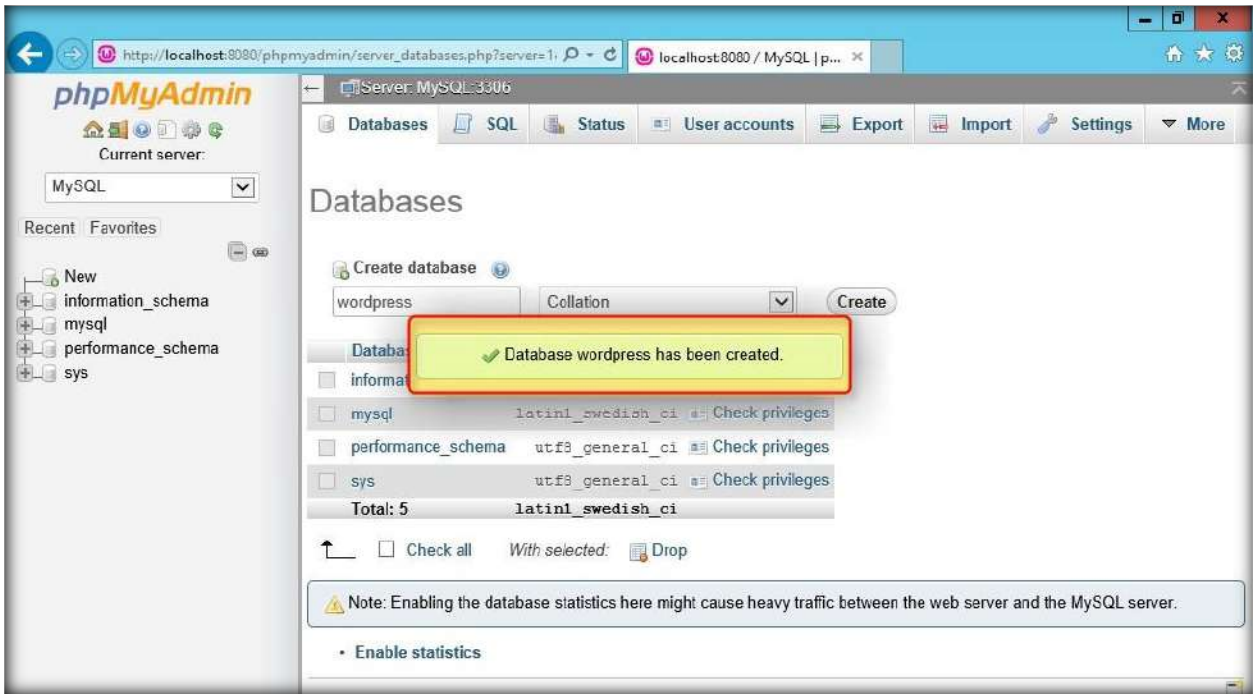
3. phpMyAdmin login page appears, type **root** as the Username and click **Go**



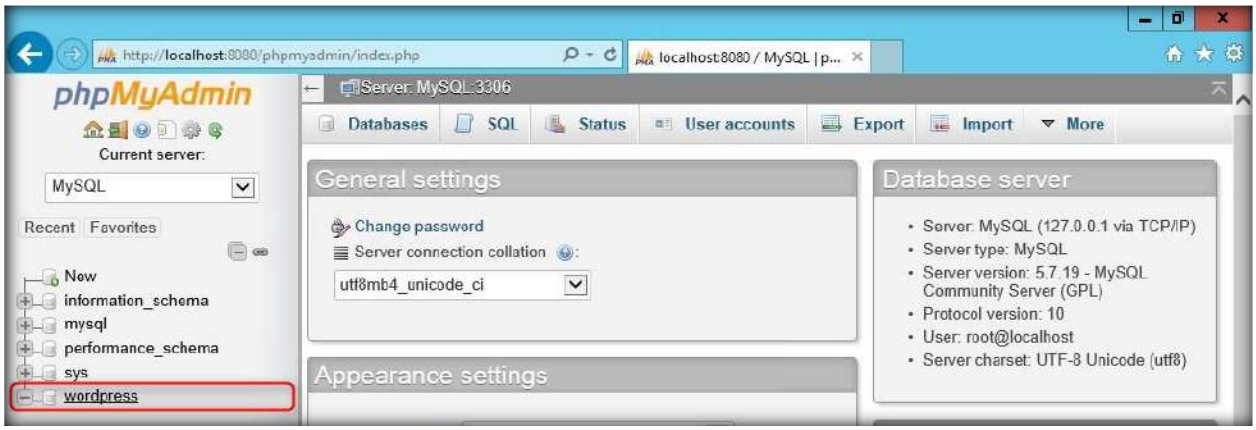
4. **phpMyAdmin** webpage appears, click **Databases** tab.
5. **Databases** webpage appears, type **wordpress** in the **Create database** text field, leave the drop-down list set to default as **Collation** and click **Create** to create a database named wordpress



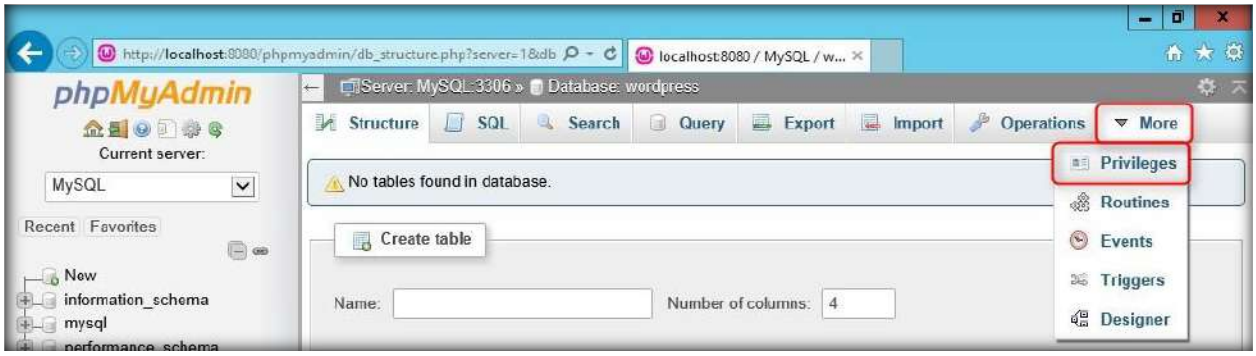
6. On successful creation of the database, a pop-up appears stating that the database has been created



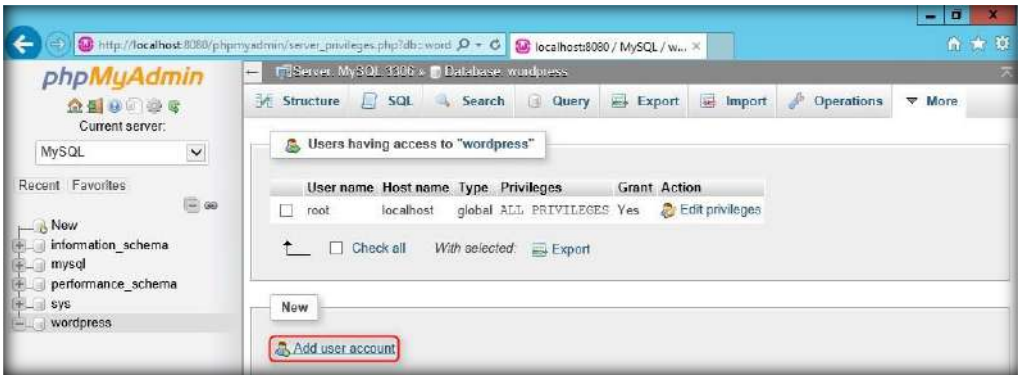
7. The newly added database appears in the left pane, click on it



8. Wordpress database's webpage appears, click **Privileges**



9. Here, you will be adding a user to the database. To add, click the **Add user account** link.



10. Add user page appears,

    Under **Login Information** section:

    Type **admin** in the **User name** text field,

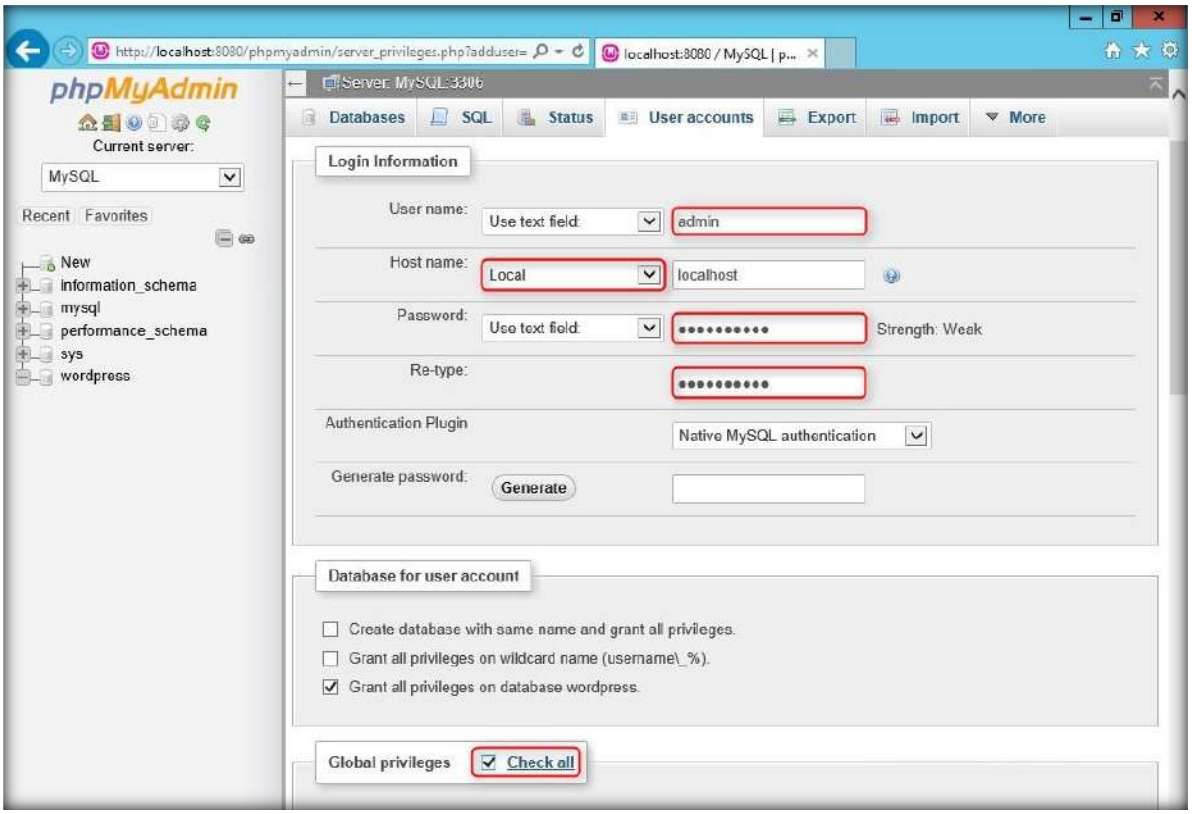
    Select **Local** from the **Host** drop-down list

    Type the password as **qwerty@123** in **Password** and **Re-type** password fields

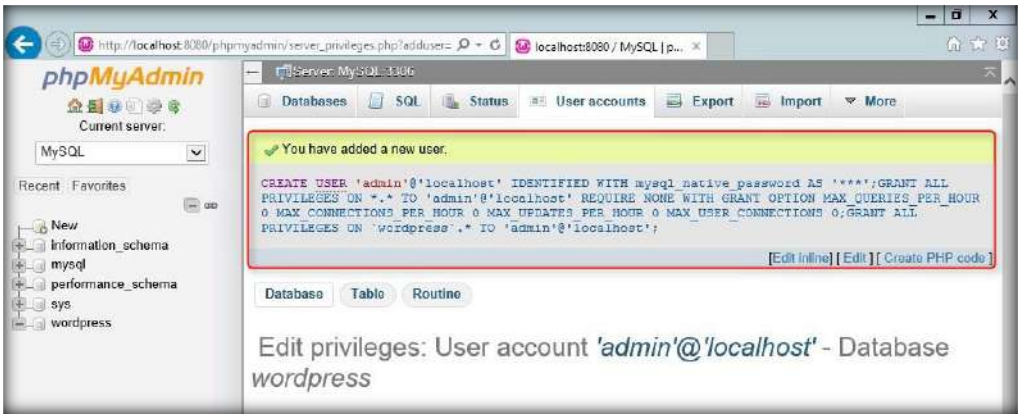
    In the **Global privileges** section:

    Click **Check All** link

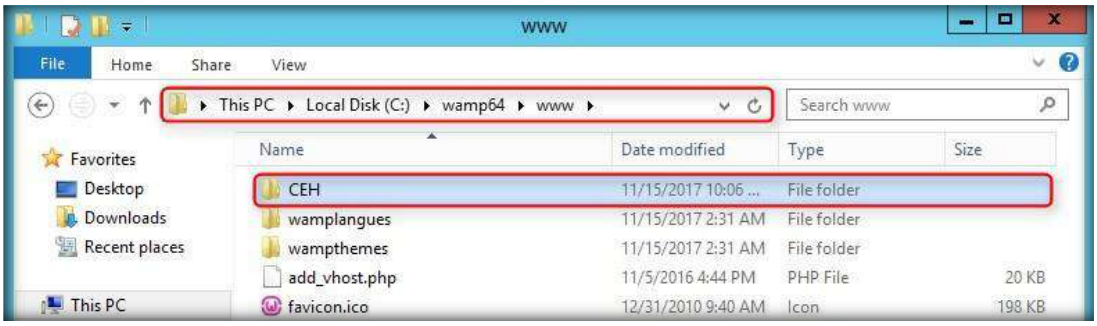
11. Click **Go** button at the bottom of the page



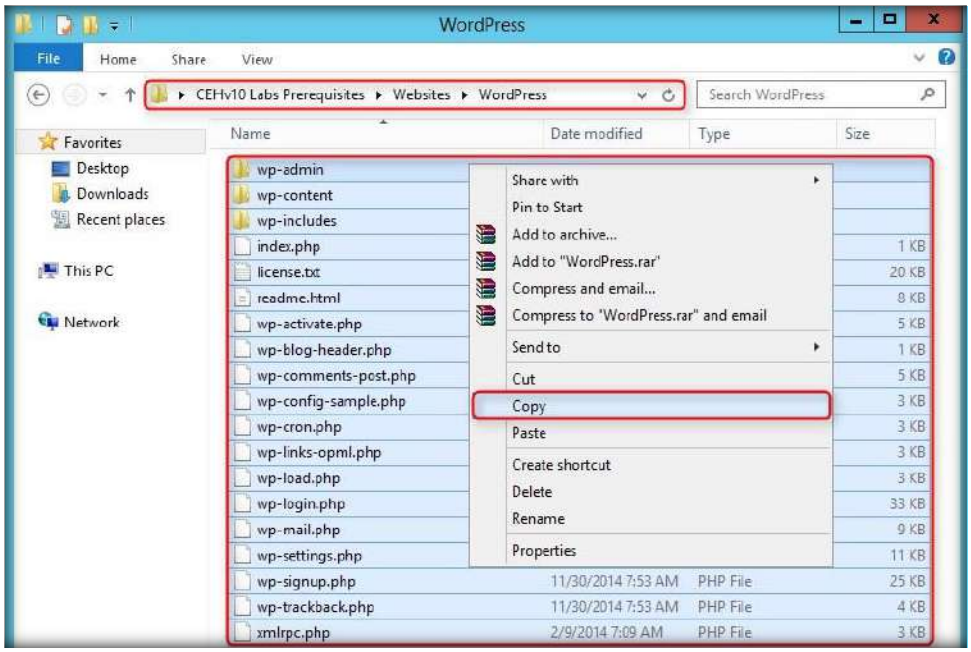
12. You will observe the newly added user in the wordpress database's webpage as shown in the following screenshot:



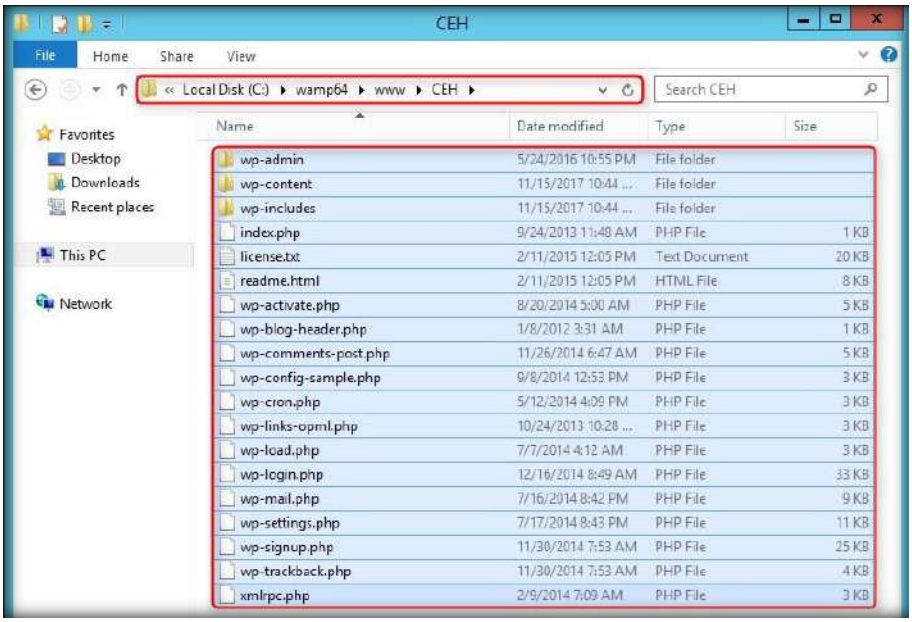
13. Close the Web browser
14. Navigate to **C:\wamp64\www** and create a new folder named **CEH**



15. Navigate to **Z:\CEH-Tools\CEHv10 Lab Prerequisites\Websites\WordPress** and copy all the contents in the location

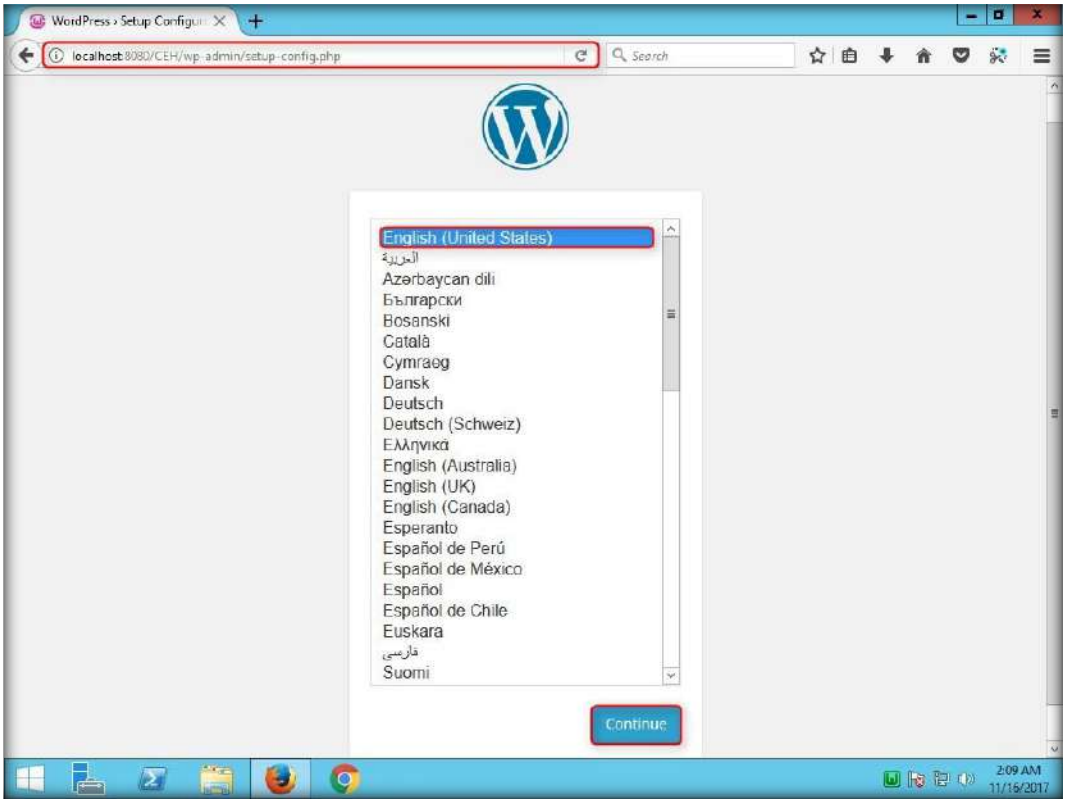


16. Navigate to **C:\wamp64\www\CEH** and paste all the contents that were copied from **Z:\CEH-Tools\CEHv10 Lab Prerequisites\Websites\WordPress**

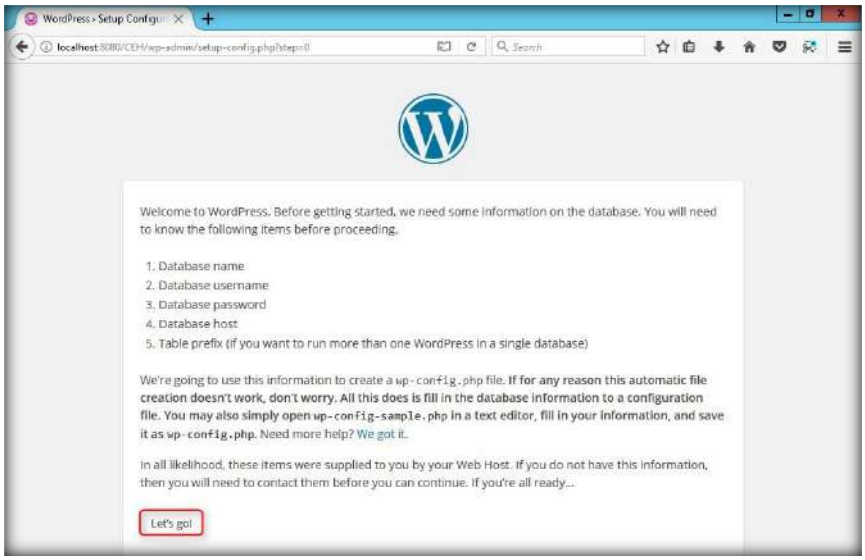


17. Launch a web browser, type the URL **http://localhost:8080/CEH** and press **Enter**
18. **Setup Configuration** webpage appears, click **Continue**

Note: Screenshots may differ if you are using different browser or a different version of wordpress.



19. **Setup Configuration** webpage appears, click **Let's go!** Button



20. Now, you need to specify the database connection details
21. Type:

    wordpress in **Database Name** field

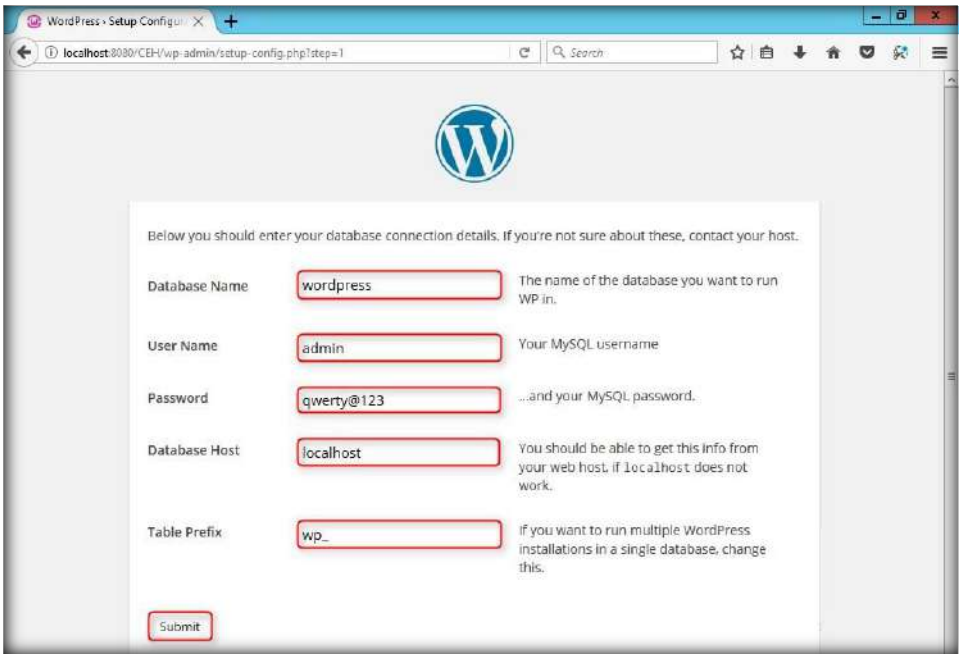
    admin in **User Name** field

    qwerty@123 in **Password** field

    localhost in **Database Host** field

    wp_ in the **Table Prefix** field

22. Click **Submit** button



23. Click **Run the install** button

24. Welcome page appears, scroll down the webpage, type:

    CEH Demo Website in **Site Title** field

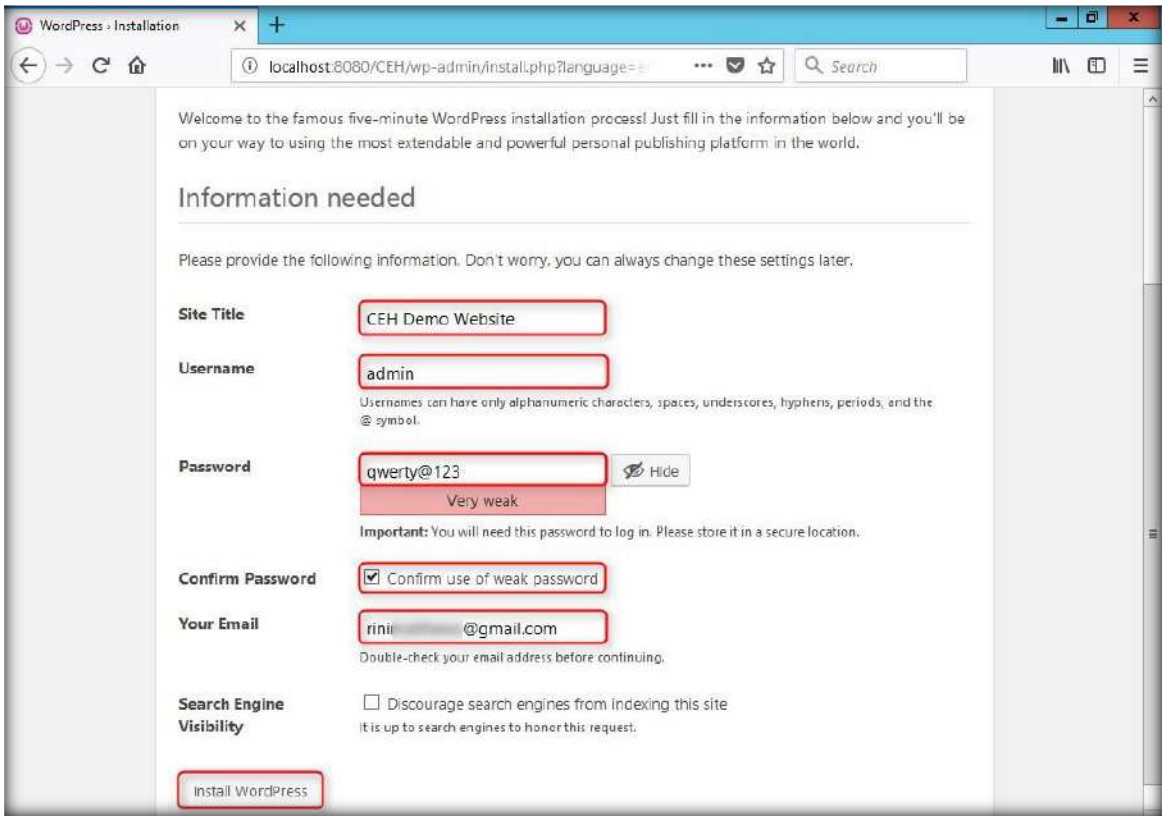
    admin in the **Username** field

    qwerty@123 in **Password** and **Re-type password** field

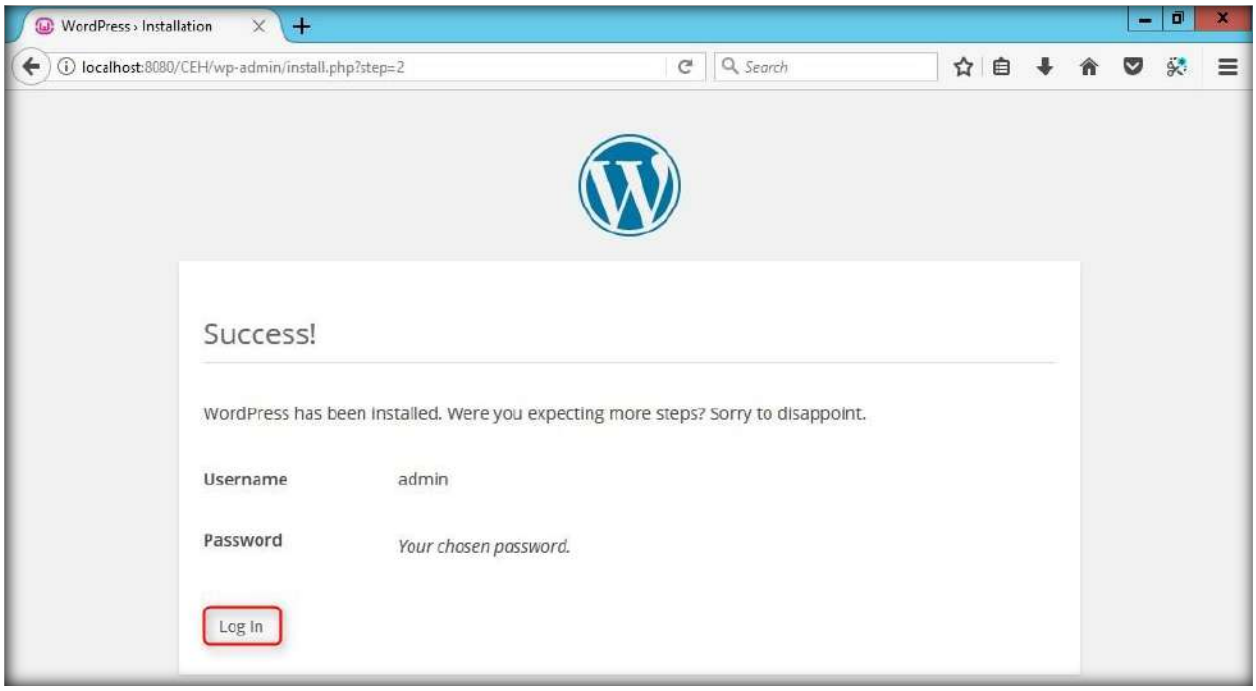
    Tick the checkbox in the **Confirm Password** field

    an email ID in **Your E-mail** text field

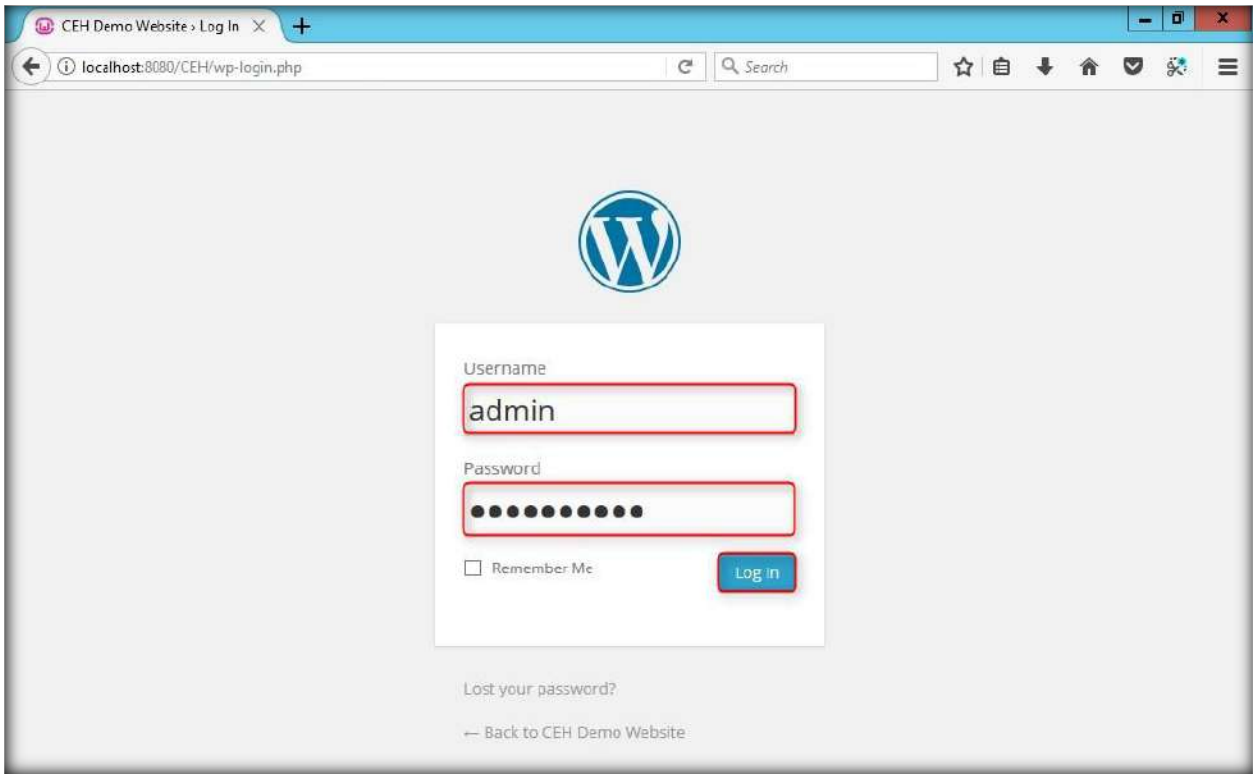
25. Click **Install WordPress** button



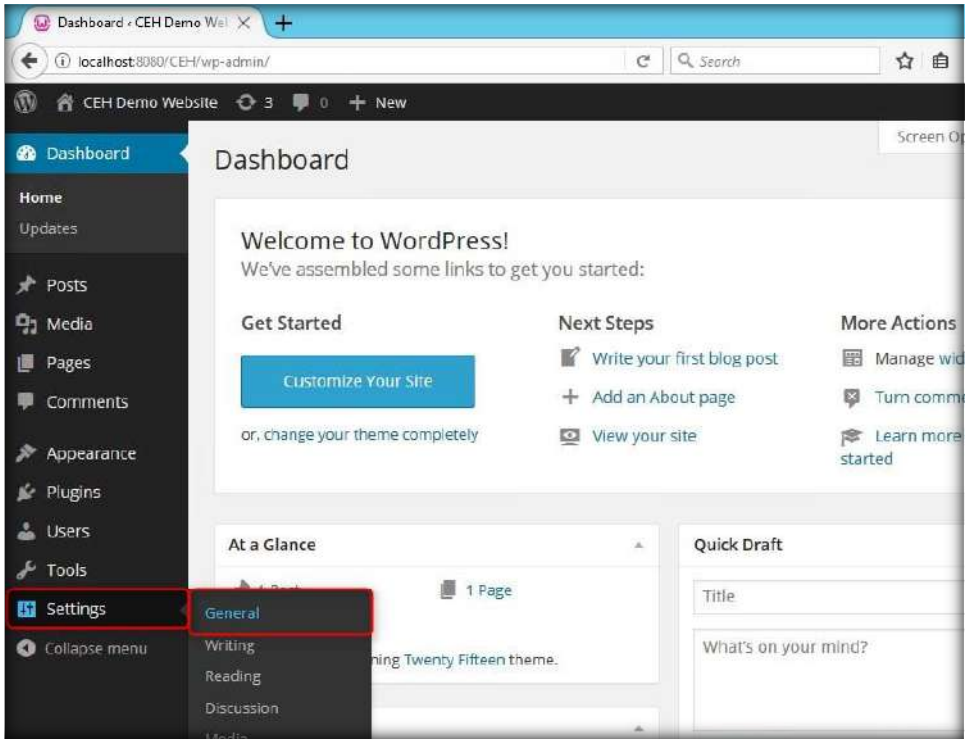
26. On successful installation, a webpage appears stating that the installation is successful. Click **Log in** button



27. Log In webpage appears, type **admin** in **Username** field, **qwerty@123** in **Password** field and click **Log In** button

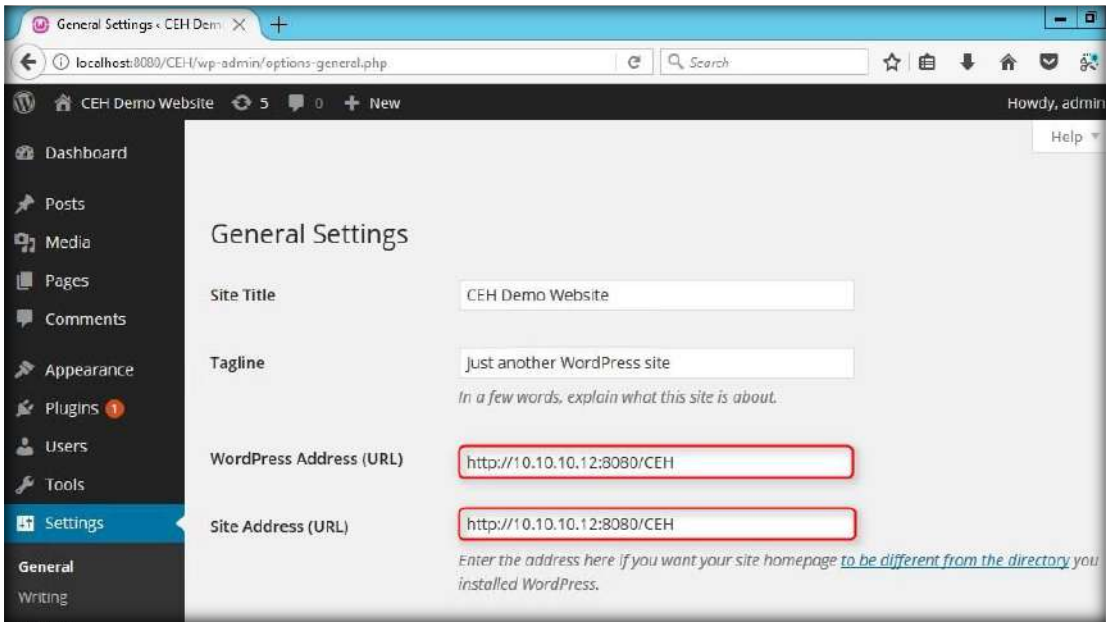


28. Once you have logged in to the website, **WordPress Dashboard** appears
29. Hover the mouse cursor on **Settings** and click **General**

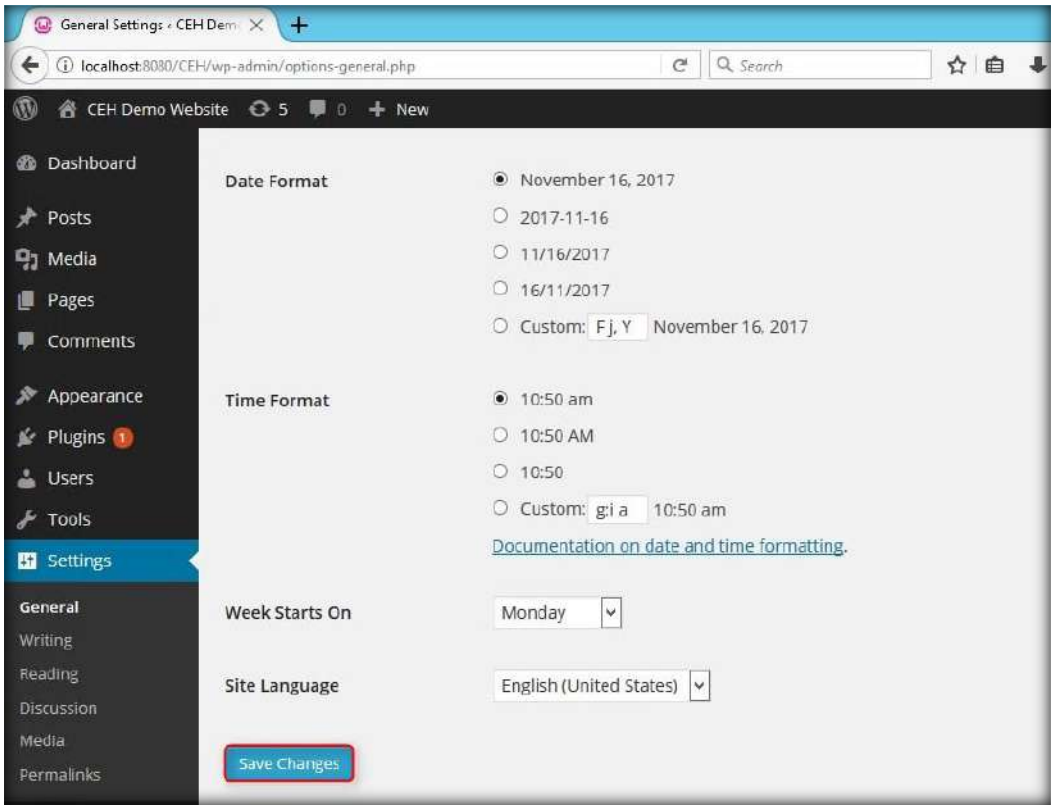


30. WordPress Settings webpage appears, type **http://[IP Address of Windows Server 2012]:8080/CEH** in **WordPress Address (URL)** and **Site Address (URL)** fields

    Note: In this lab setup, the IP Address of **Windows Server 2012** is **10.10.10.12** and the port on which the **apache web server** is running is **8080**. This address and port may vary in your lab environment

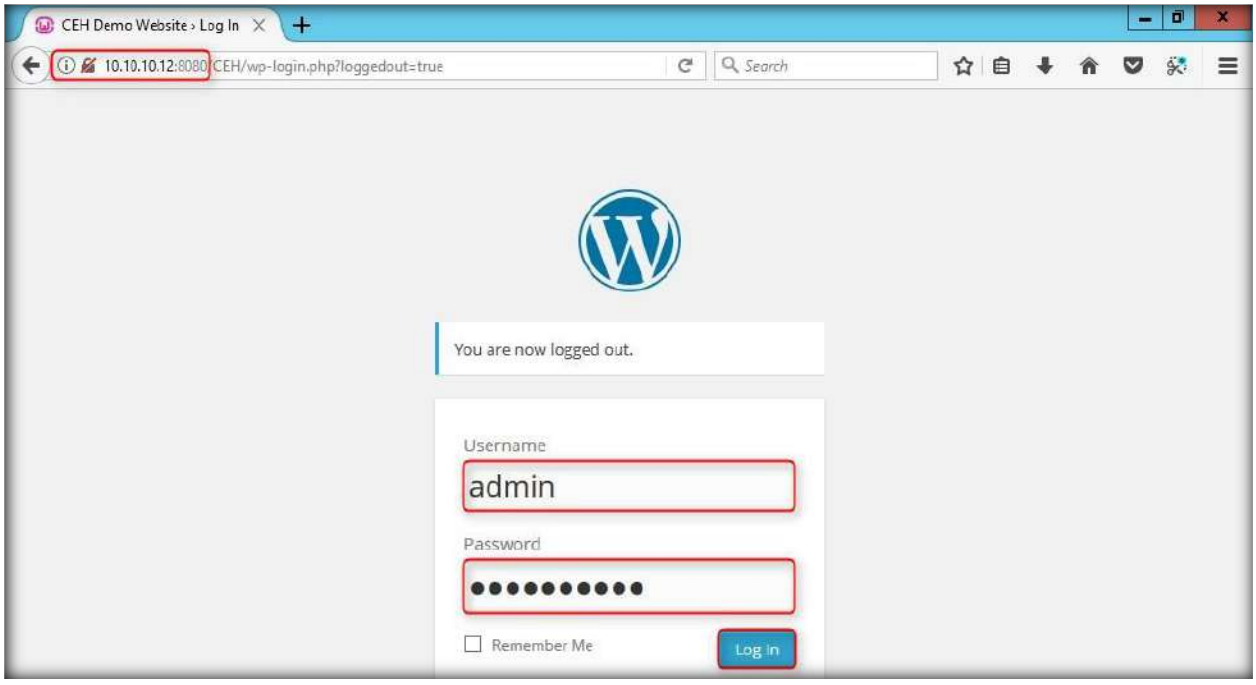


31. Scroll down the webpage and click **Save Changes** button

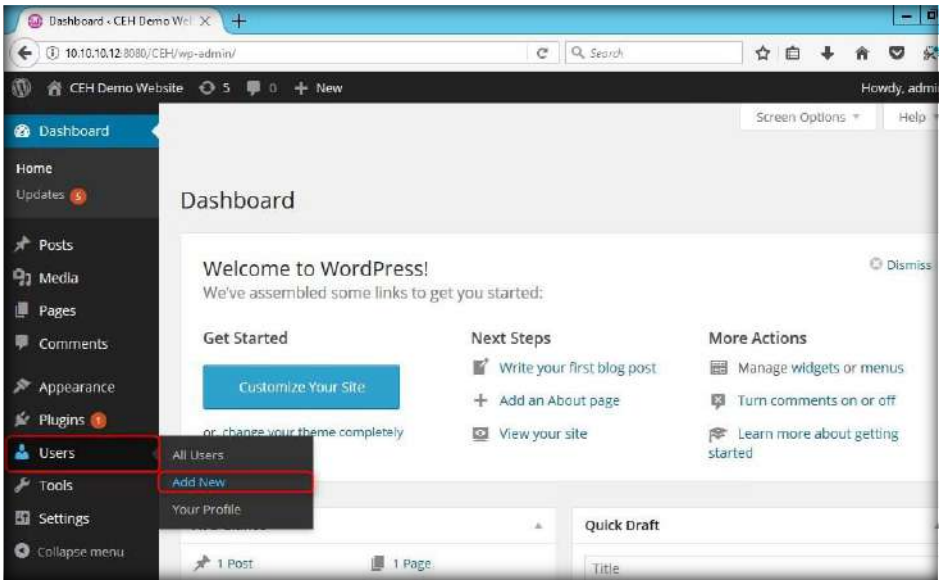


32. On clicking the button, you will be redirected back to the login page. Here, you can observe the IP address of **Windows Server 2012** in the URL field instead of localhost.

33. Enter the user credentials (**admin**/ **qwerty@123**) and click **Log in** button



34. Once you are logged in to the website, hover the mouse cursor on **Users** and then click **Add New**



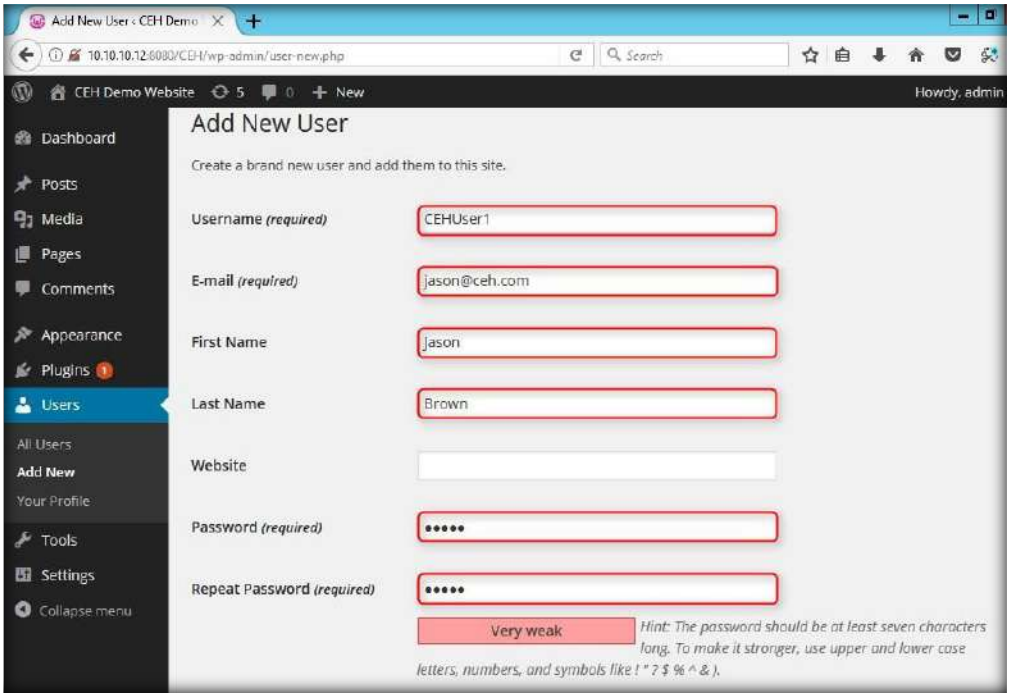
35. **Add New User** webpage appears, enter:

    CEHUser1 in the **Username** field

    An Email ID in **E-mail** field

    First and **Last Names**

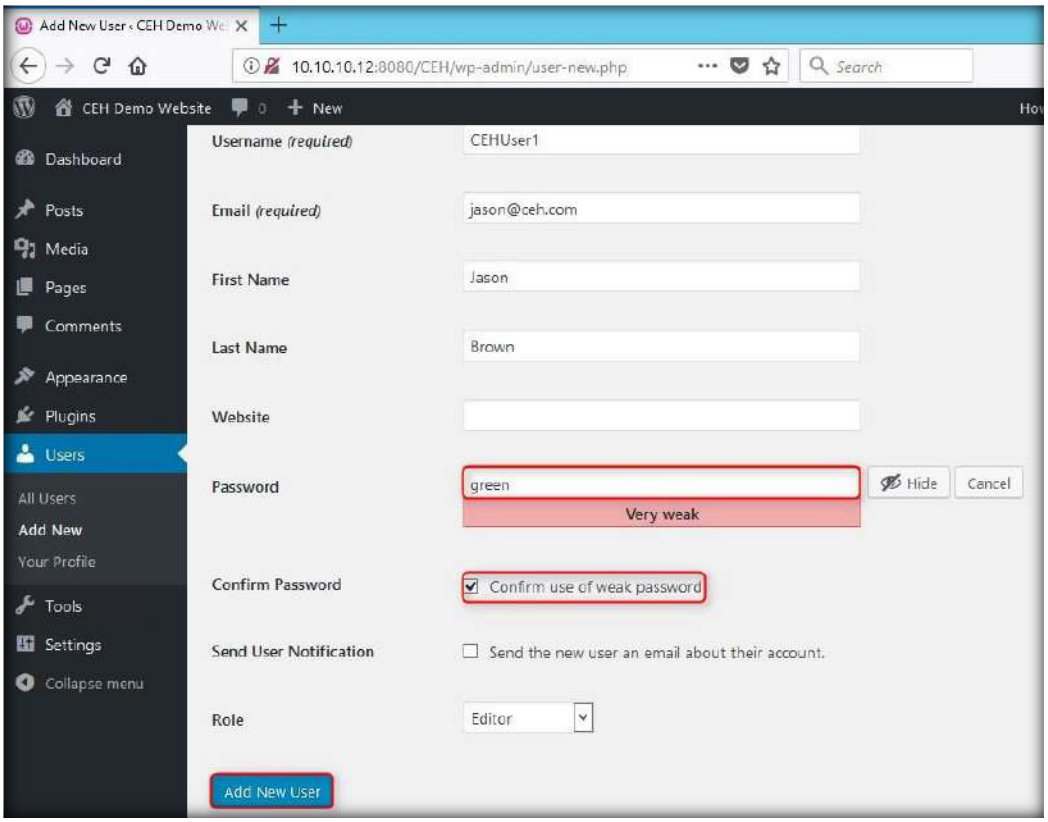
    green in **Password** and **Repeat Password** fields



36. So, you are creating a user account with Username **CEHUser1** and Password **green**

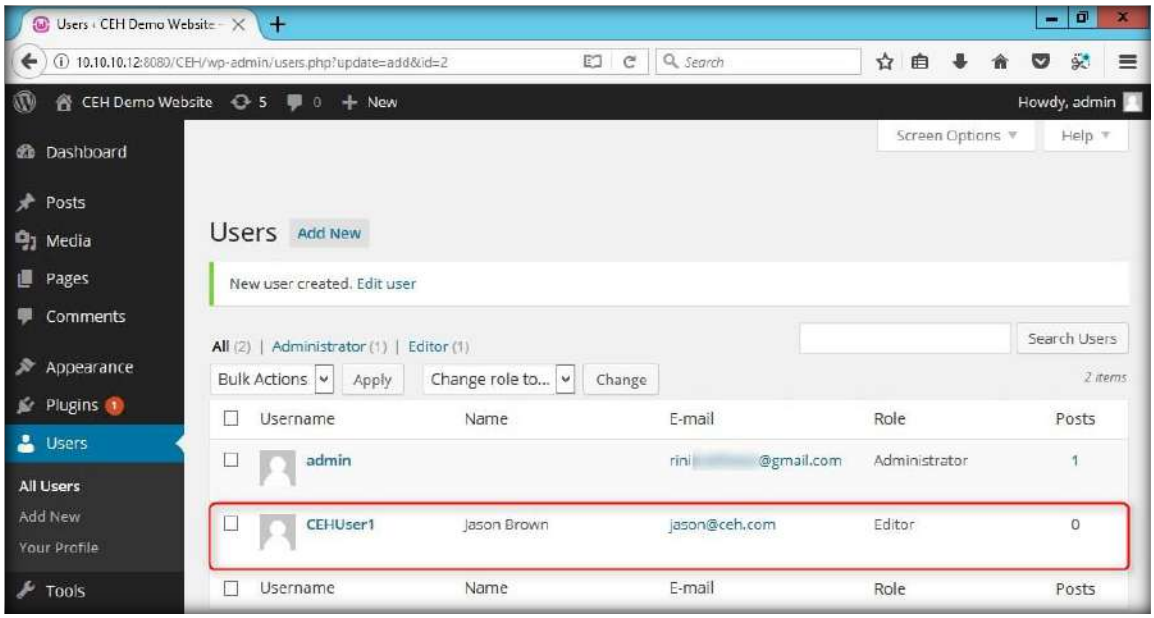
37. **Tick** the checkbox in the **Confirm Password** field

38. Scroll down the webpage, assign a role to the user (here, **Editor**) and click **Add New User**



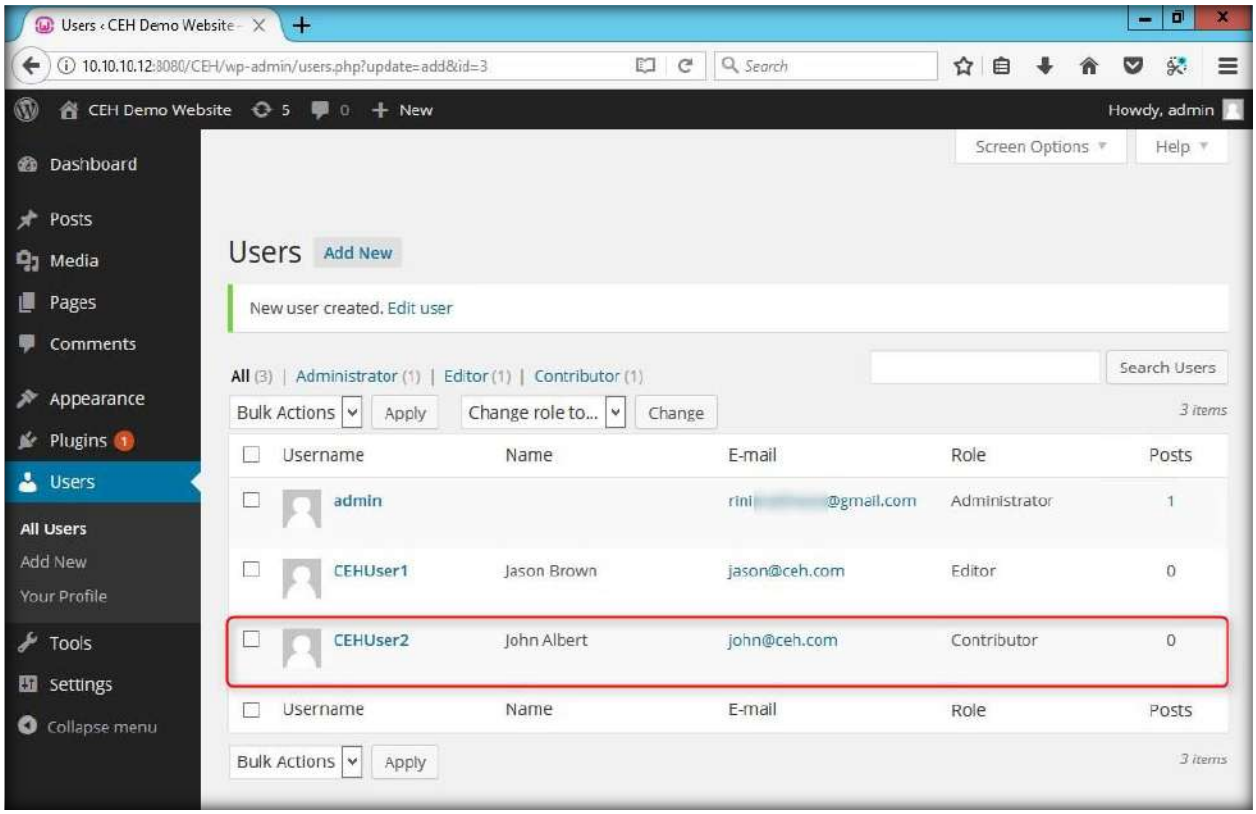
39. This creates a user account

40. Now, click **Add New** to create another user account



41. In the same way, follow the steps **34** and **38** and create a user account with the credentials (**CEHUser2**/ **alpha**)

42. Once done, the added user appears as shown in the following screenshot:



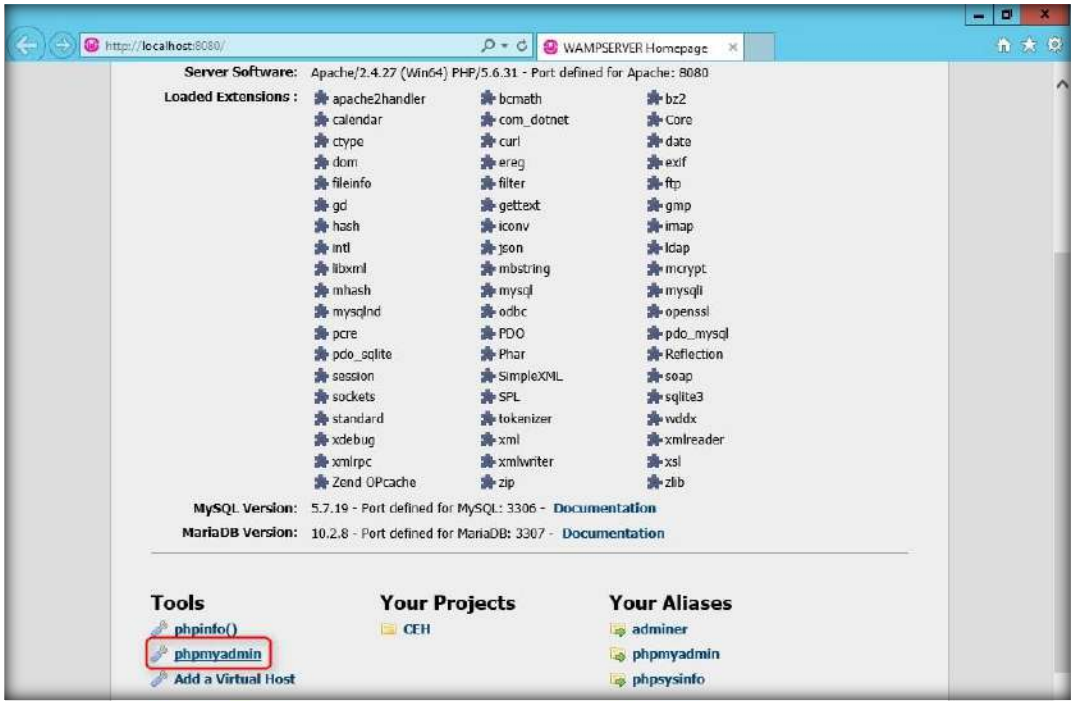
43. Once the users are successfully added, hover the mouse cursor on the admin account field and click **Log Out**

[Back to Configuration Task Outline]

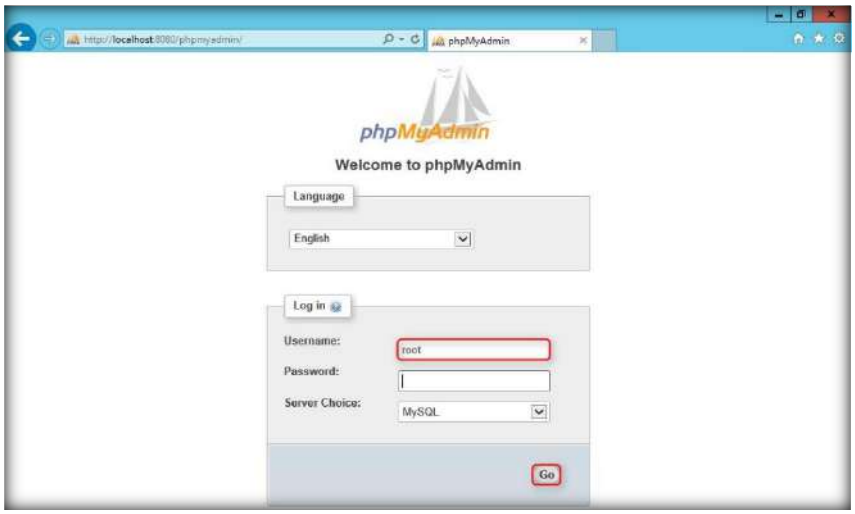
CT#33: Install and Configure Damn Vulnerable Web Application

1. Click **WampServer** icon from the notification area
2. Choose **Localhost** from the context menu

3. As soon as you click the icon, the WAMPSERVER home page appears in the default browser. Click **phpmyadmin** link under **Tools** section.

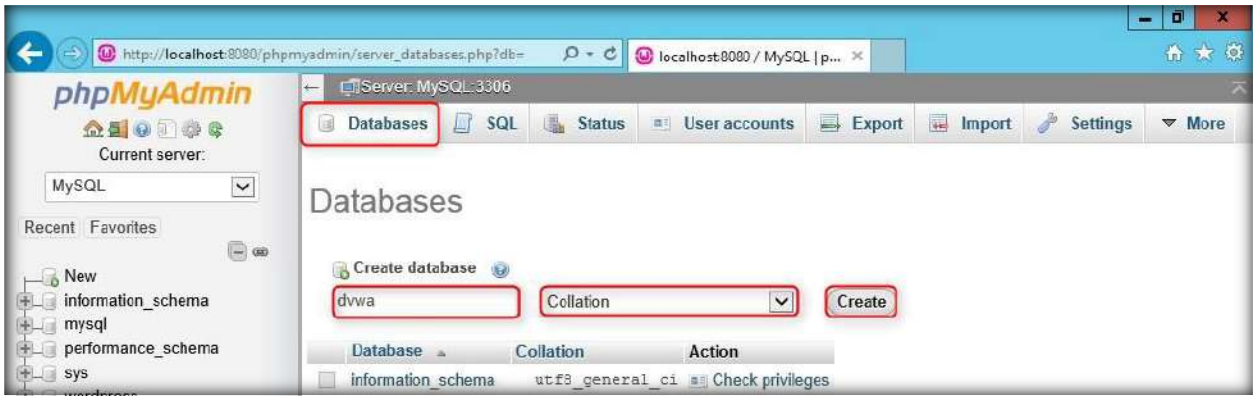


4. **phpMyAdmin** login page appears, type root as the Username and click Go

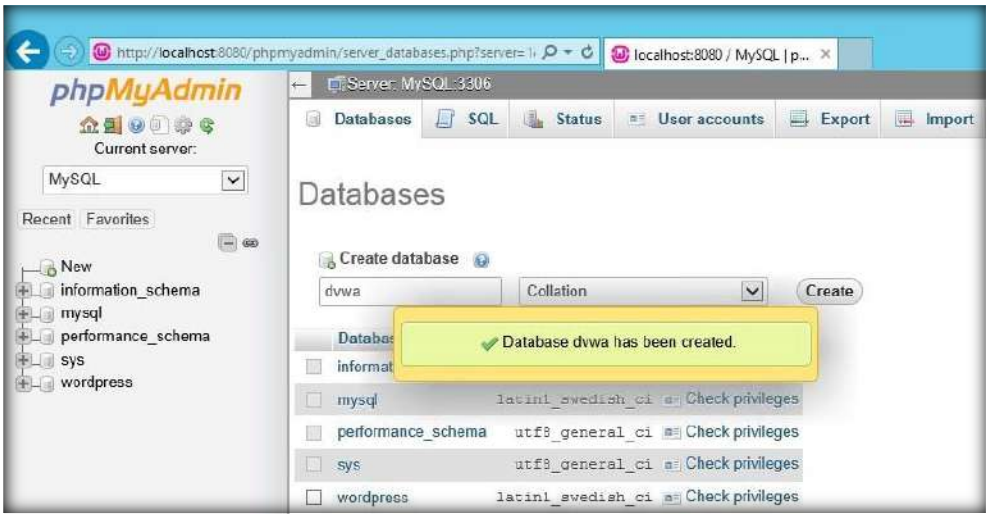


5. **phpMyAdmin** webpage appears, click **Databases** tab

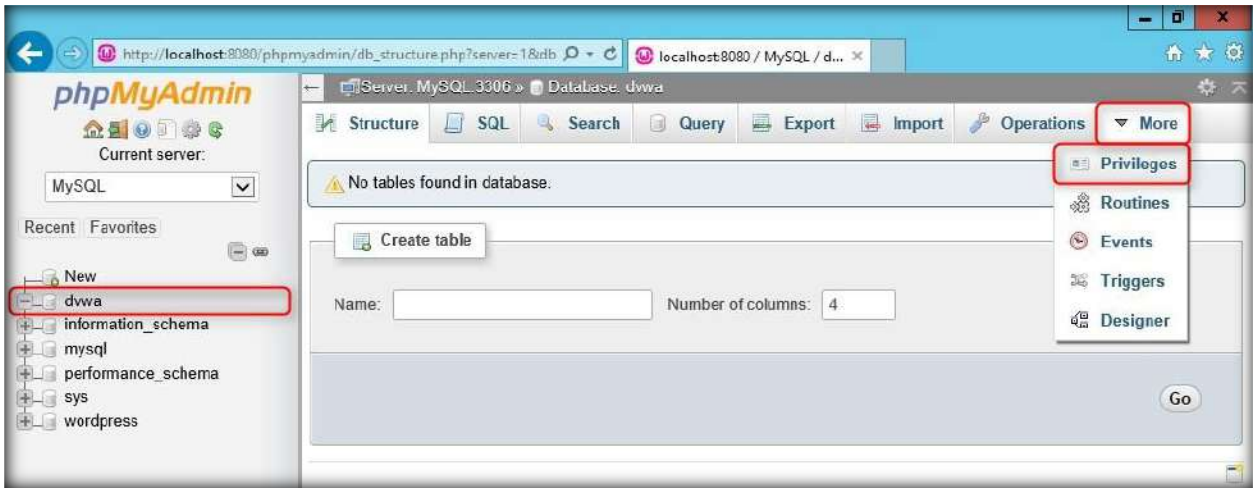
6. **Databases** webpage appears, type **dvwa** in the **Create database** text field, leave the drop-down list set to default as **Collation** and click **Create** to create a database named dvwa



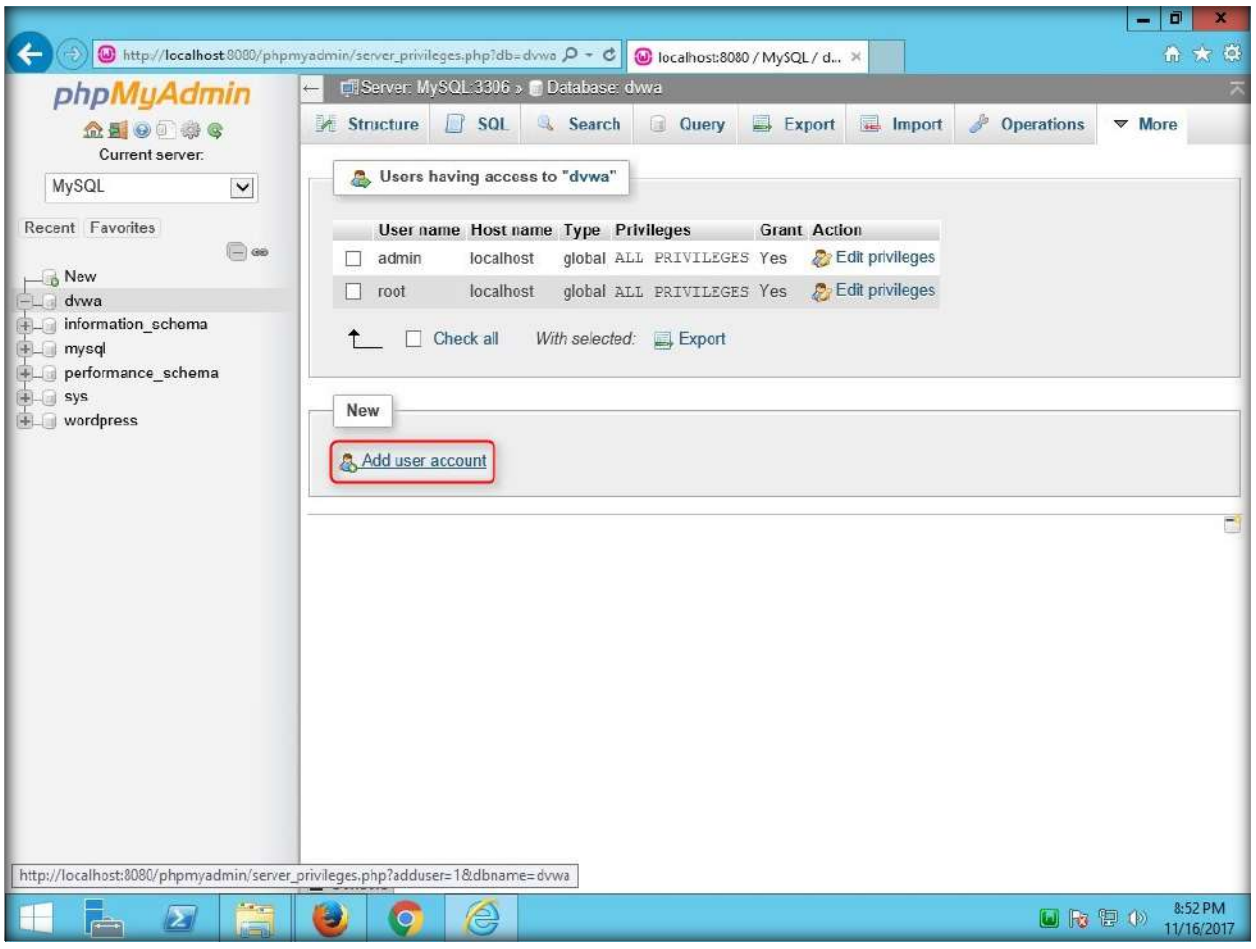
7. On successful creation of the database, a pop-up appears stating that the database has been created



8. The newly added database appears in the left pane, click on it. DVWA database's webpage appears, click **Privileges**



9. Here, you will be adding a user to the database. To add, click the **Add user account** link.



10. Add user page appears,

    Under **Login Information** section:

Type **dvwa_user** in the **User name** text field,

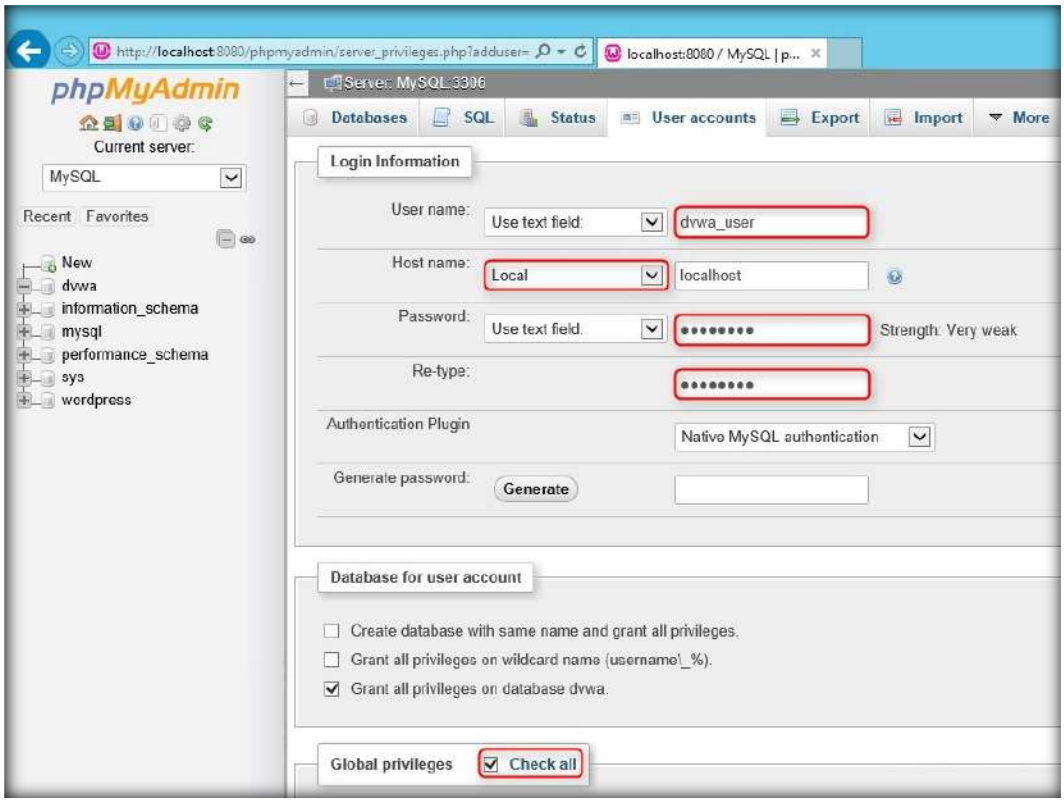
Select **Local** from the **Host name** drop-down list

Type the password as **test@123** in **Password** and **Re-type** password fields

In the **Global privileges** section:

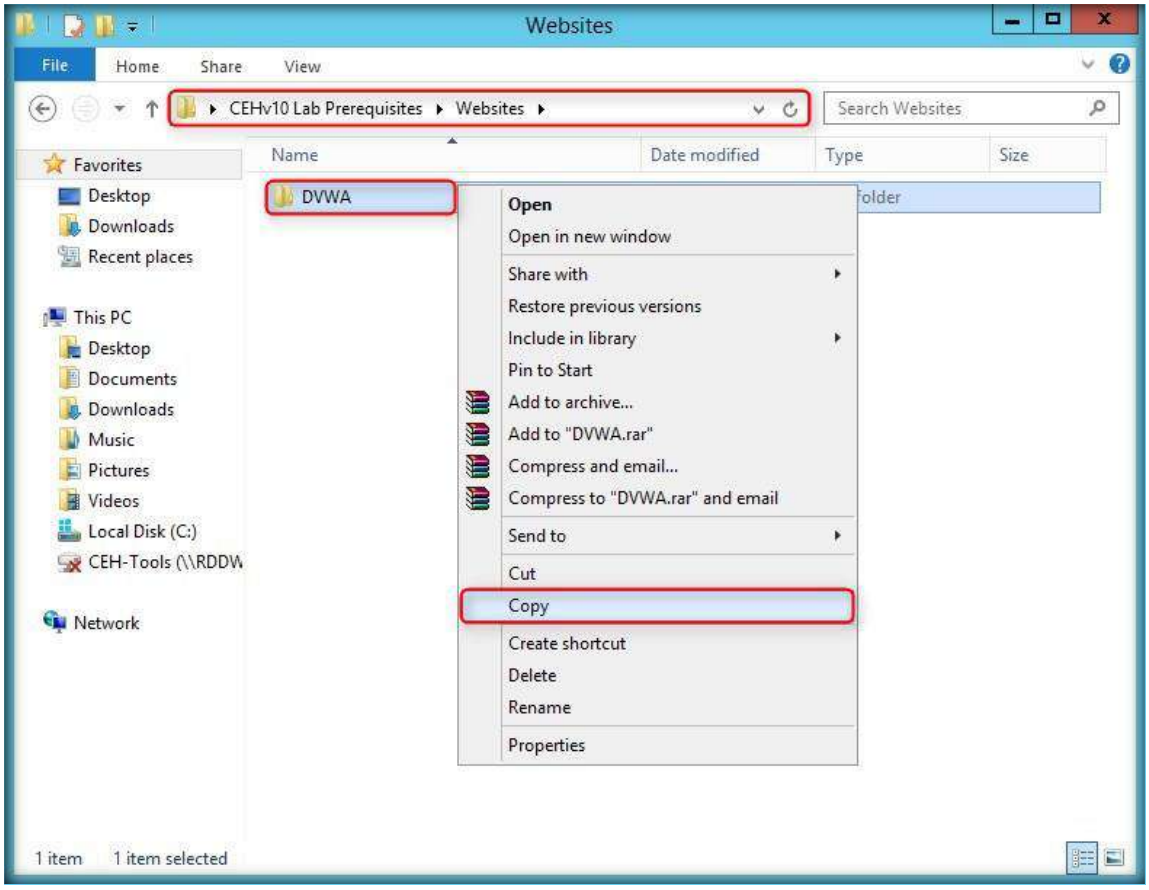
Click **Check All** link

11. Click **Go** button at the bottom of the page

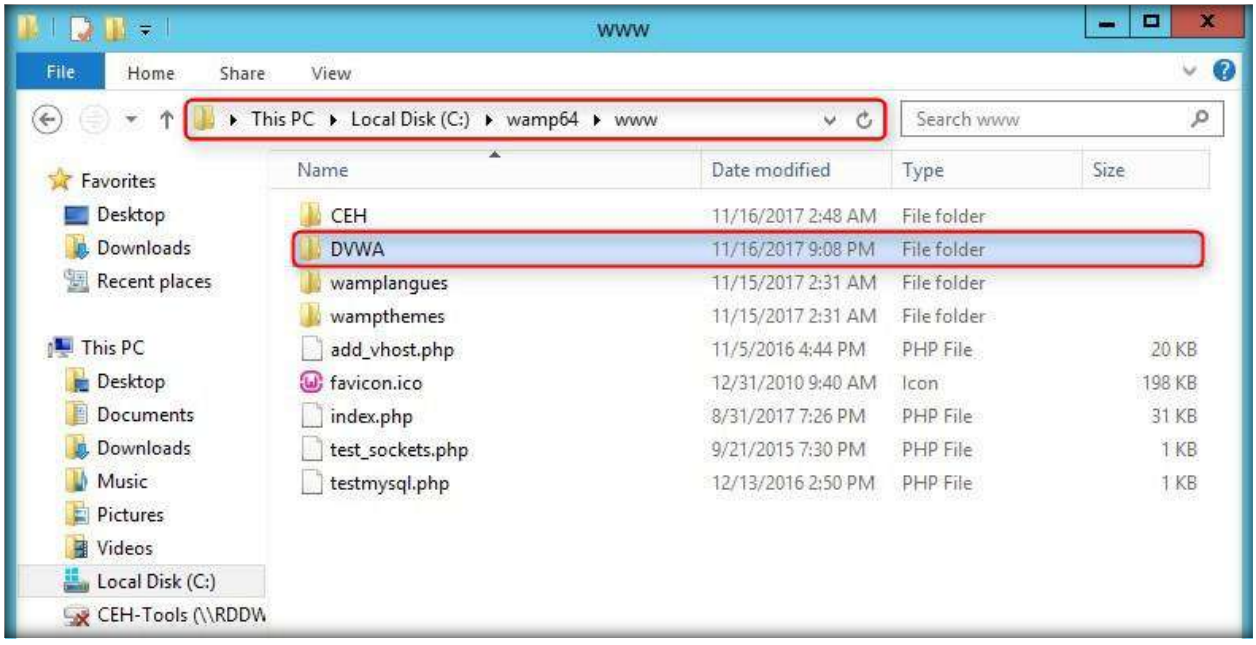


12. You will observe the newly added user in the dvwa database's webpage as shown in the following screenshot:

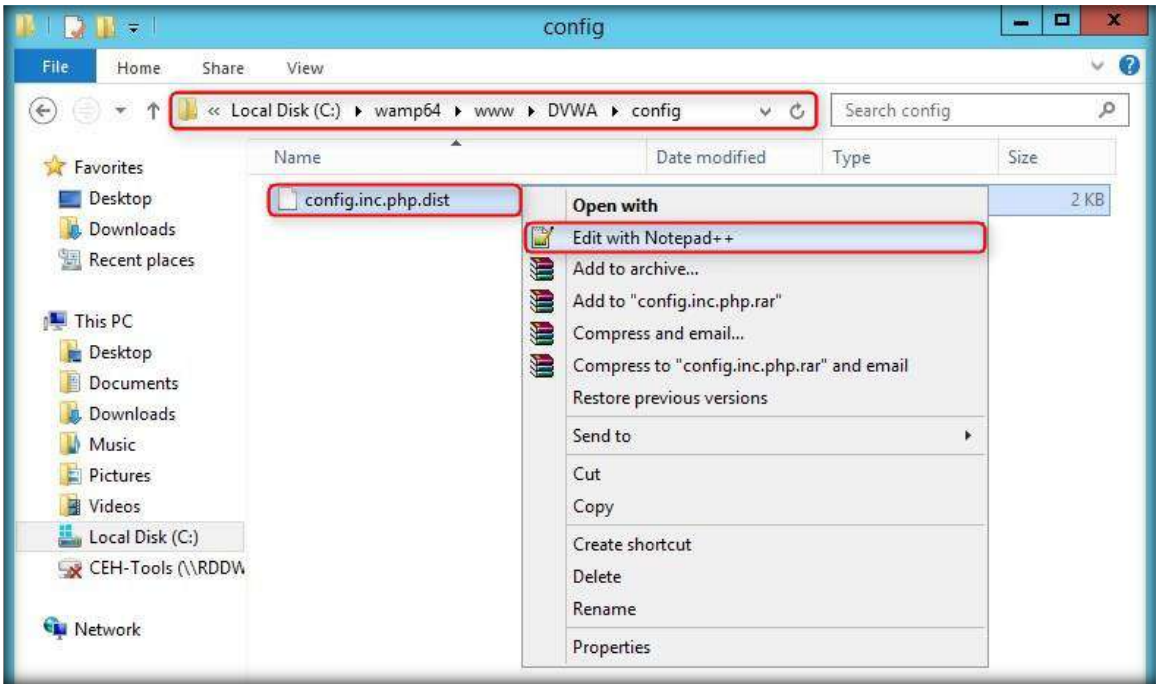
13. Close the Web browser
14. Navigate to **Z:\CEH-Tools\CEHv10 Lab Prerequisites\Websites** and copy the **DVWA** folder



15. Navigate to **C:\wamp64\www** and paste the **DVWA** folder which you have copied in the previous step



16. Navigate to **C:\wamp64\www\DVWA\config** and open **config.inc.php.dist** file with **Notepad++**



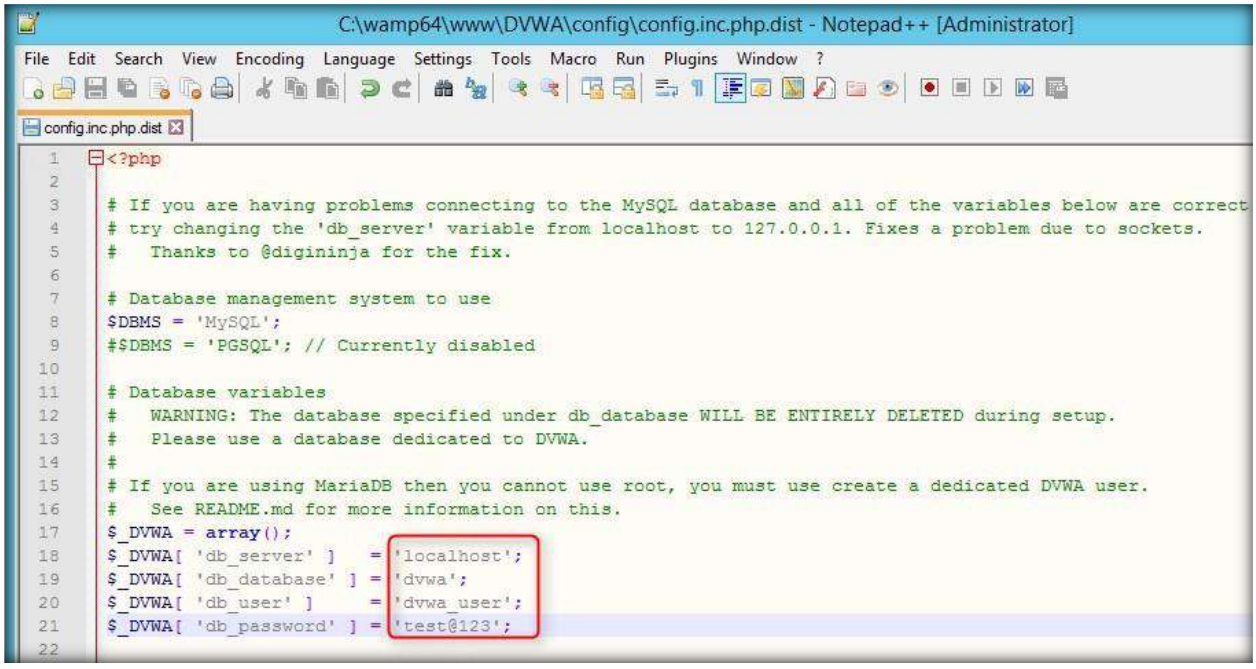
17. **config.php** file appears in Notepad++. Now:

    a. In **line no. 18**, assign the mysql database server host as **localhost** in single quotes.

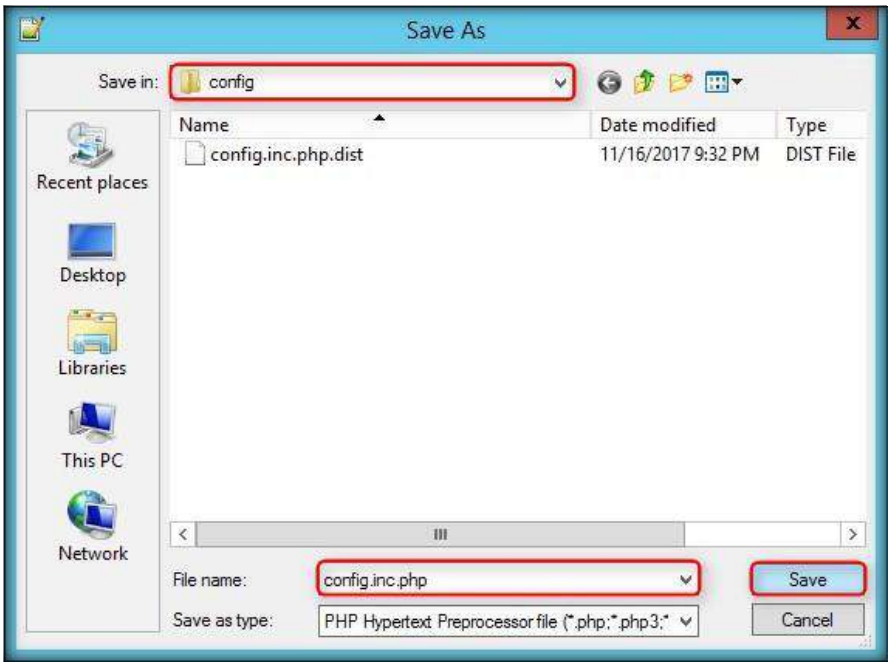
    b. In **line no. 19**, assign the database name as **dvwa** in single quotes.

    c. In **line no. 20**, assign the mysql database username as **dvwa_user** in single quotes.

    d. In **line no. 21**, assign the mysql database password as **test@123** in single quotes.

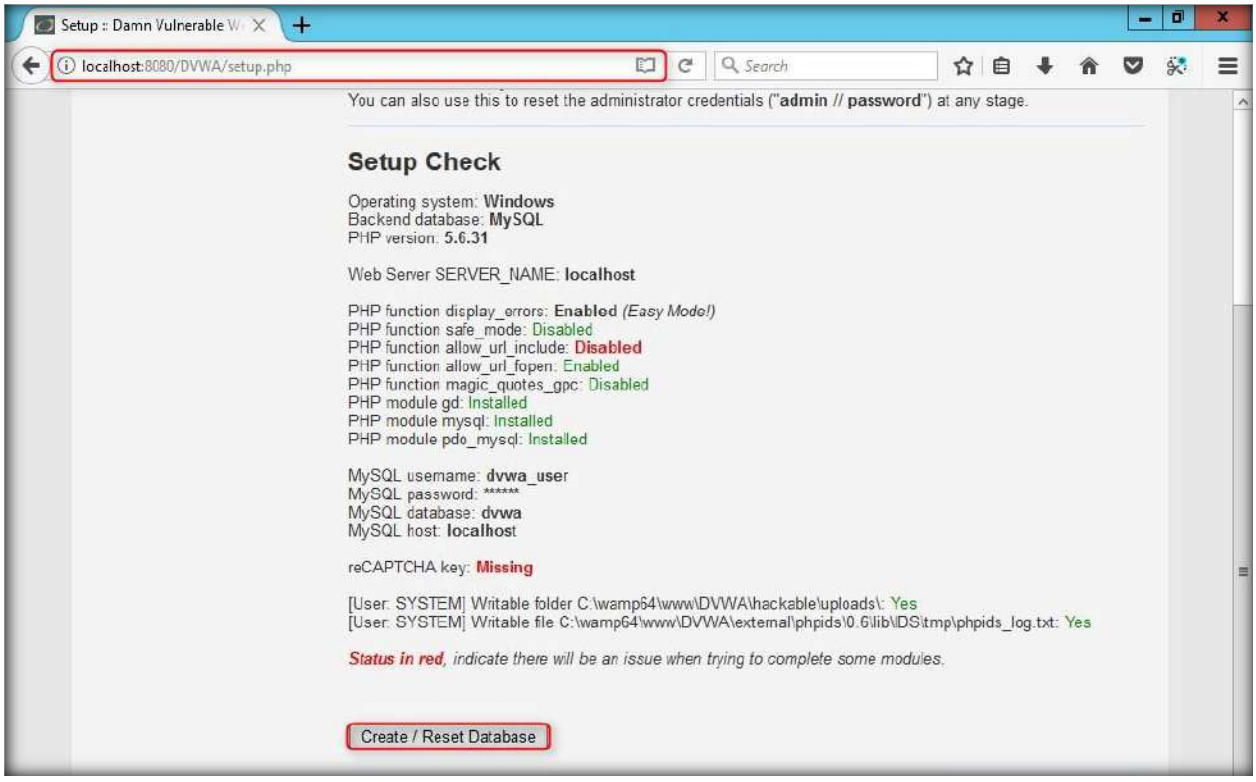


18. Once done, save the file in the **config** folder as **config.inc.php**

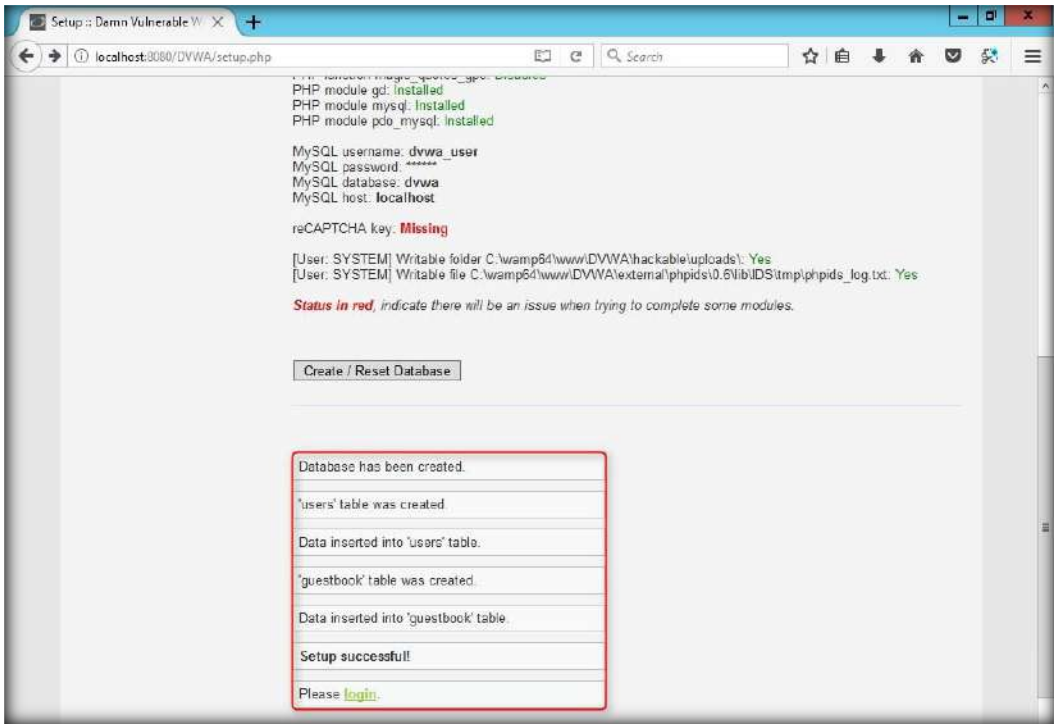


19. Launch a web browser, type the URL **http://localhost:8080/DVWA/setup.php** in the address bar and press **Enter**

20. Database setup webpage appears, click **Create / Reset Database** button

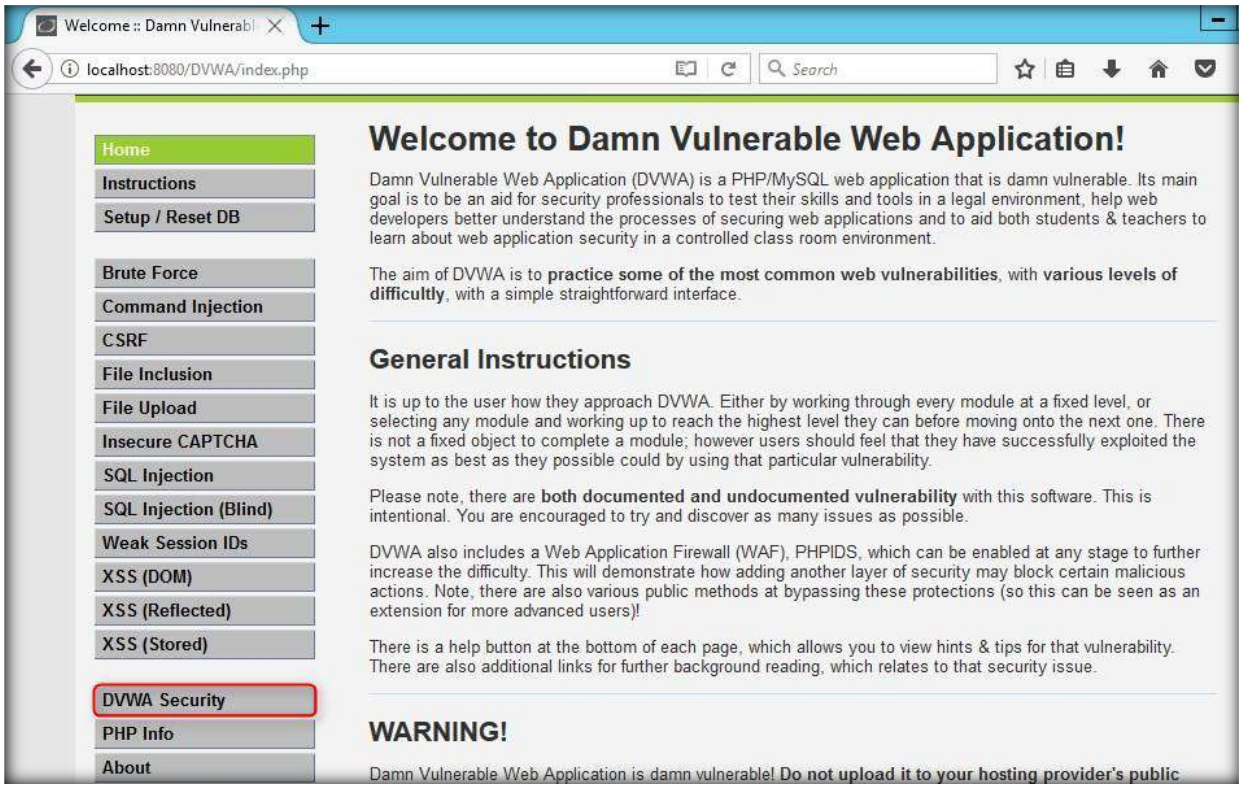


21. Databases will be successfully created, close the web browser.



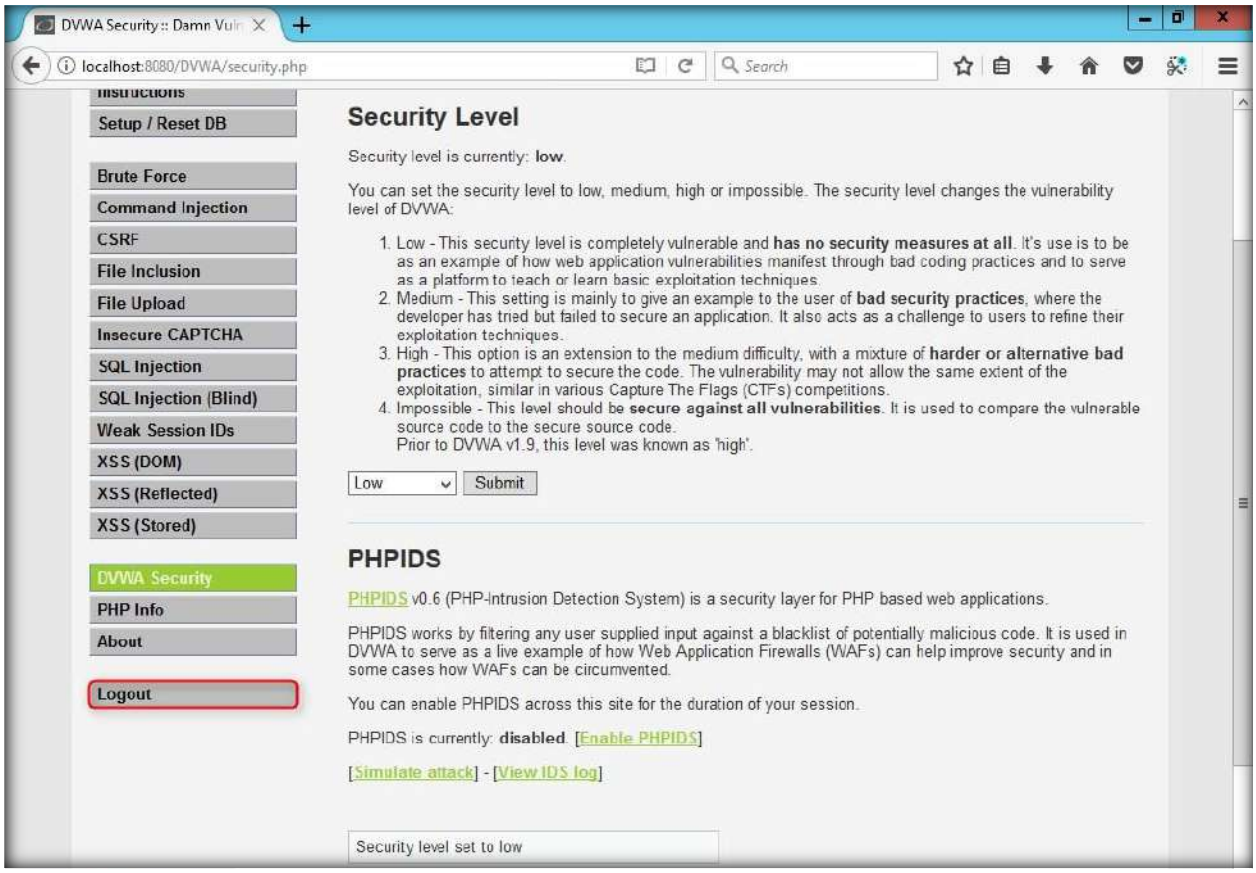
22. Now, type **http://localhost:8080/DVWA/login.php** in the address bar and press **Enter**. **DVWA** login page appears, type **admin** in **Username** field, **password** in **Password** field and click **Login** button.

23. Admin page appears, click **DVWA Security** in the left pane



24. **DVWA Security** webpage appears, select **Low** option from the drop-down list and click **Submit**

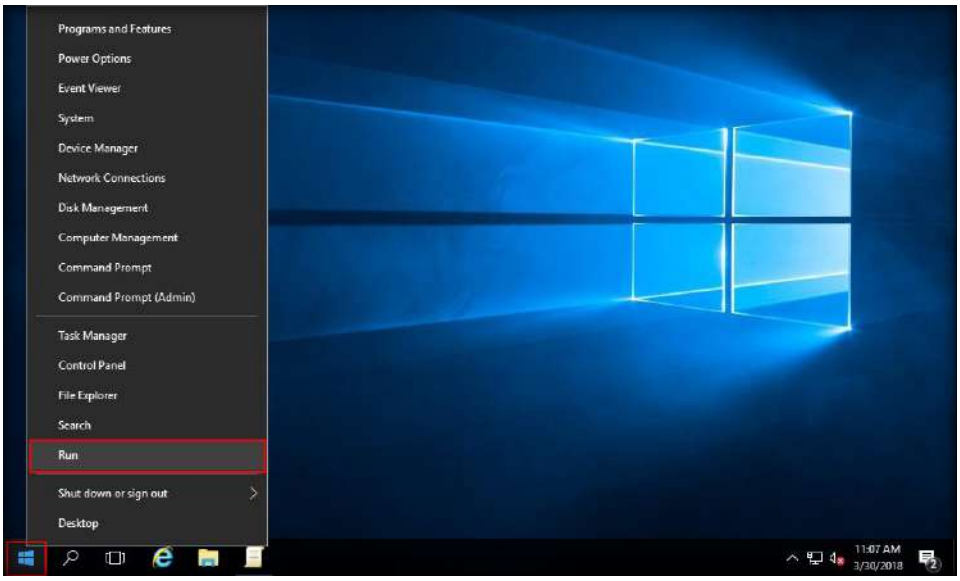
25. On configuring the security setting, click **Logout** in the left pane



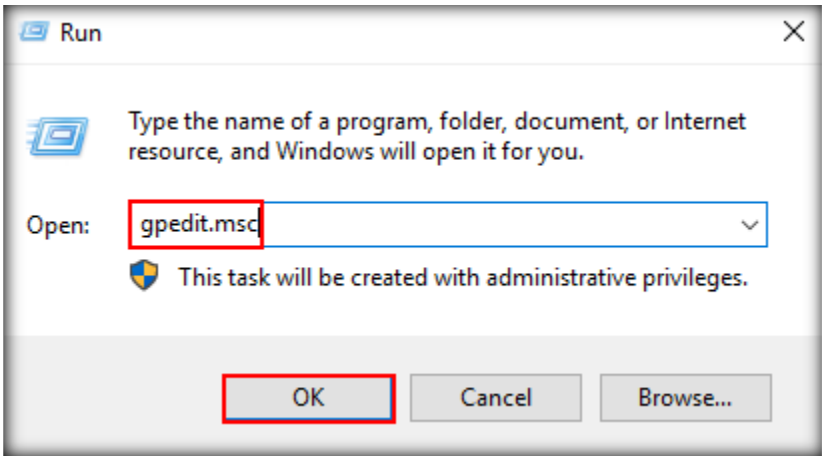
[Back to Configuration Task Outline]

CT#34: Configure Windows Components

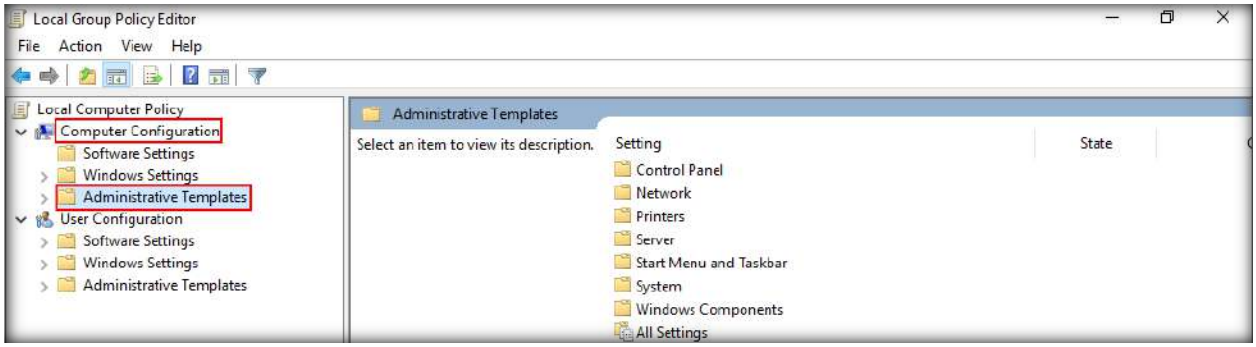
1. Login to Windows Server 2016 machine, right-click on Start and click Run as shown in the screenshot



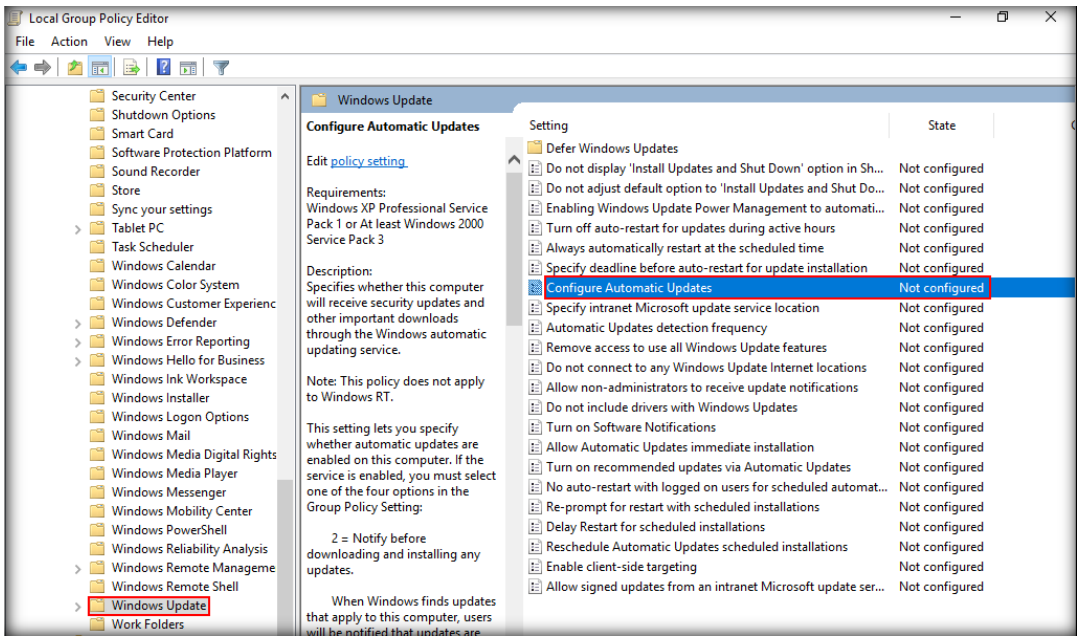
2. Run Command window appears, type gpedit.msc and click OK



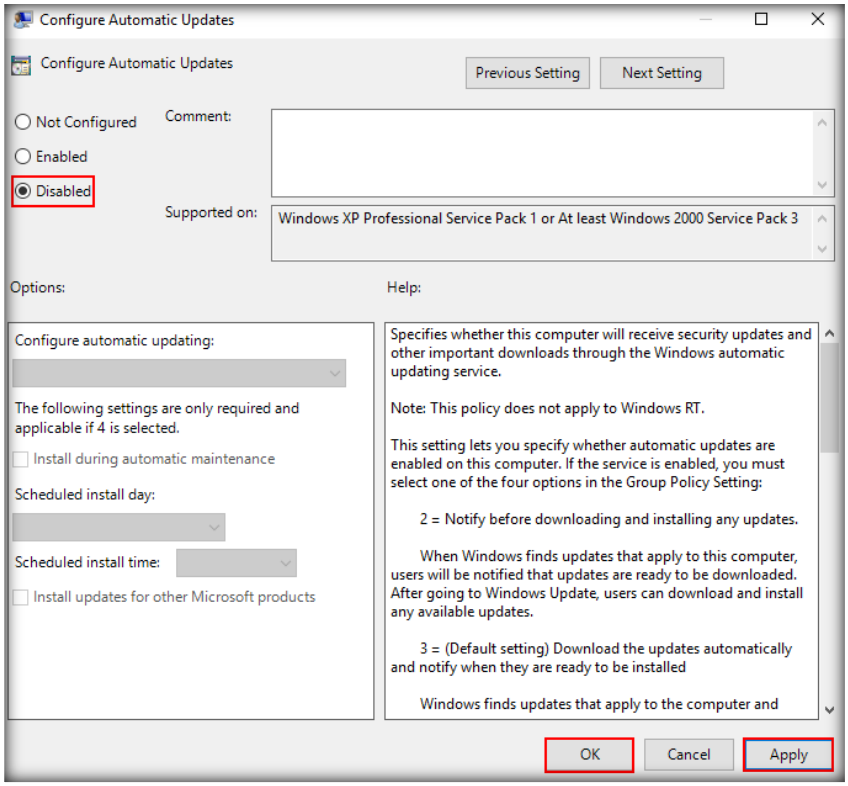
3. Local Group Policy Editor window appears, expand Administrative Templates under Computer Configuration in the left pane



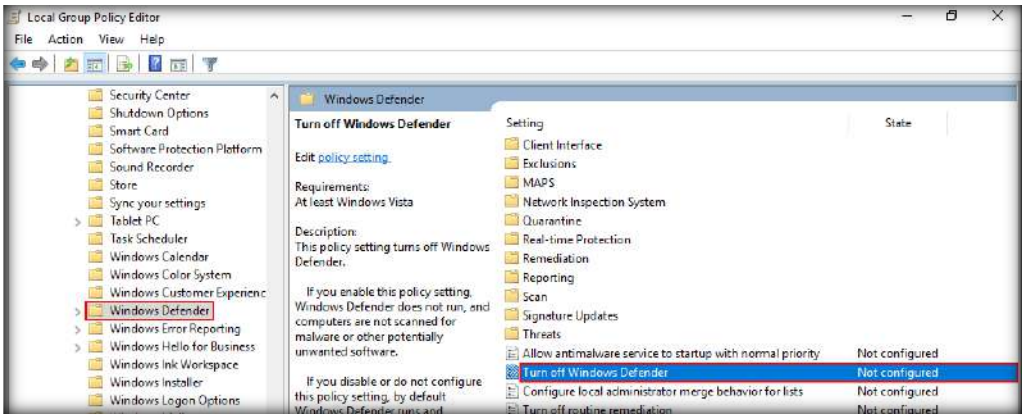
4. In Administrative Templates expand Windows Components and scroll down and click Windows Update in the left pane and double-click Configure Automatic Updates in the right-pane as shown in the screenshot



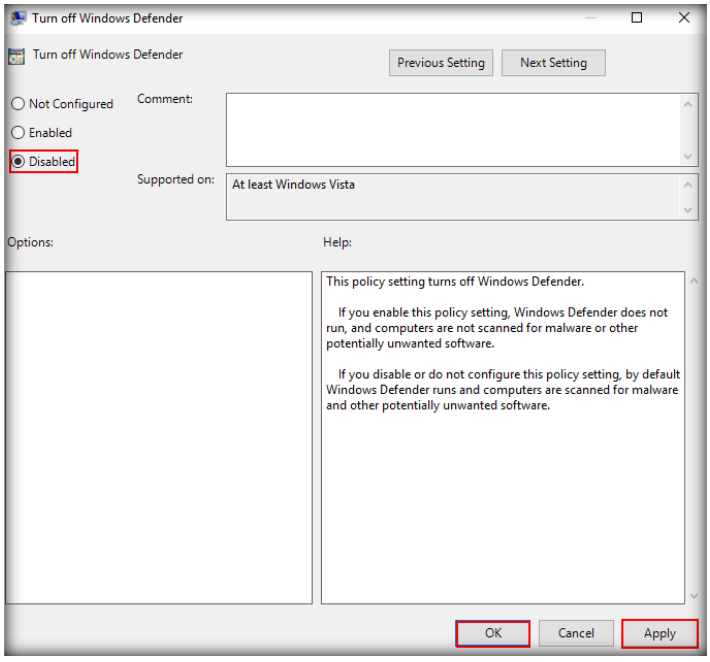
5. Configure Automatic Updates window appears, select **Disabled** radio button and click **Apply** and **OK**



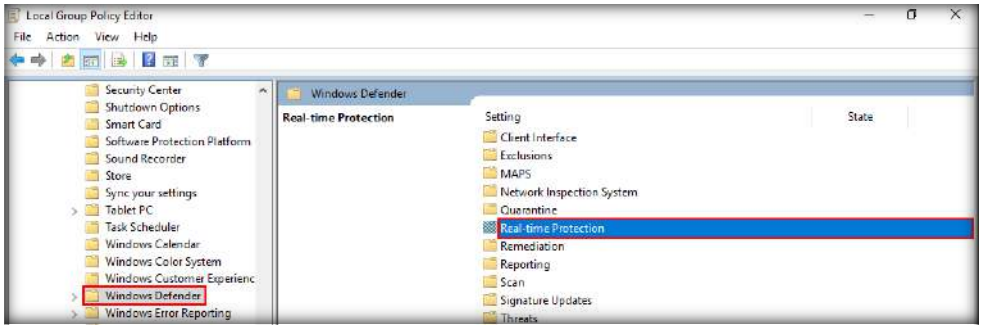
6. In the left pane click Windows Defender and double-click Turn off Windows Defender in the right-pane of the window as shown in the screenshot



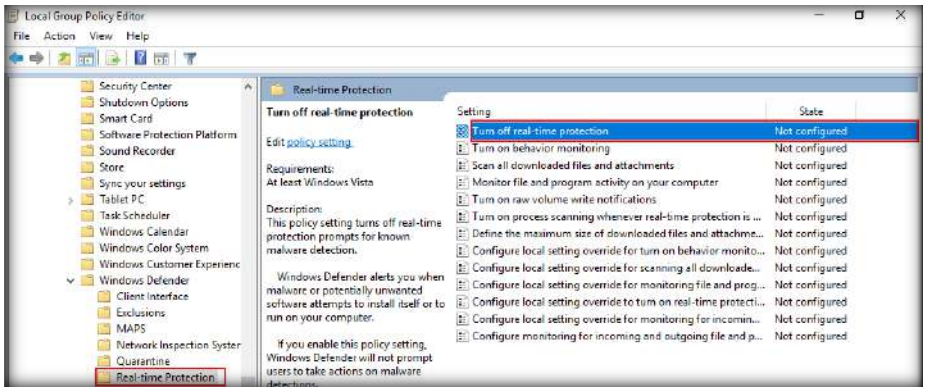
7. Turn off Windows Defender window appears, select Disabled radio button and click Apply and OK



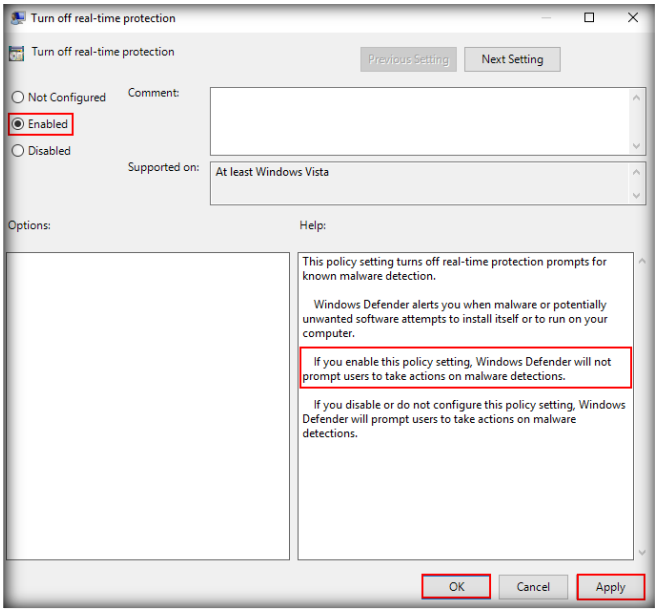
8. Double-click Real-time Protection in the Windows Defender as shown in the screenshot



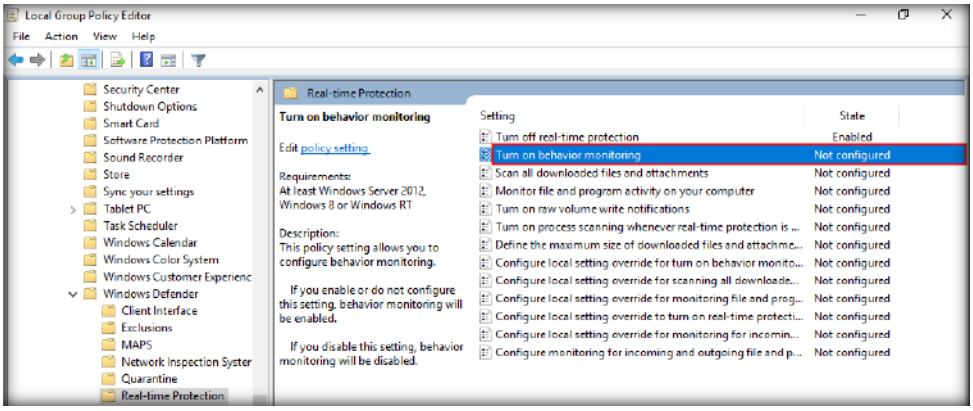
9. Real-time Protection settings appears, double-click Turn off real-time protection to configure in the right pane



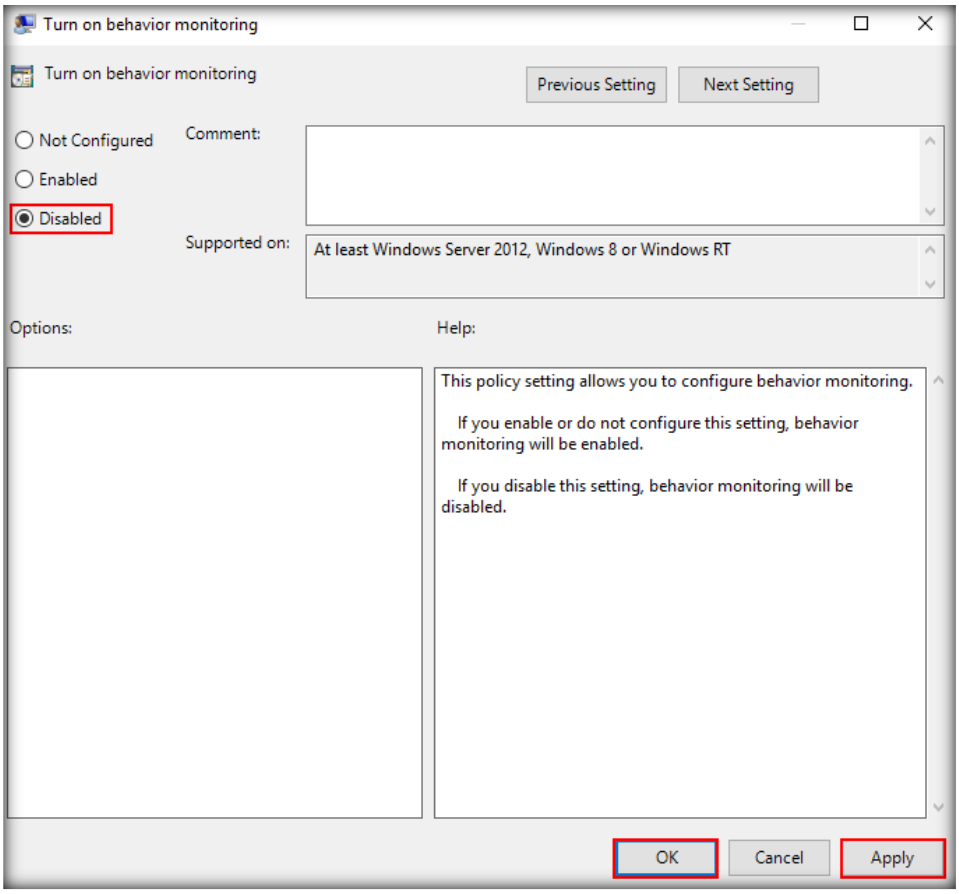
10. Turn off real-time protection window appears, select Enabled radio button and click Apply and OK



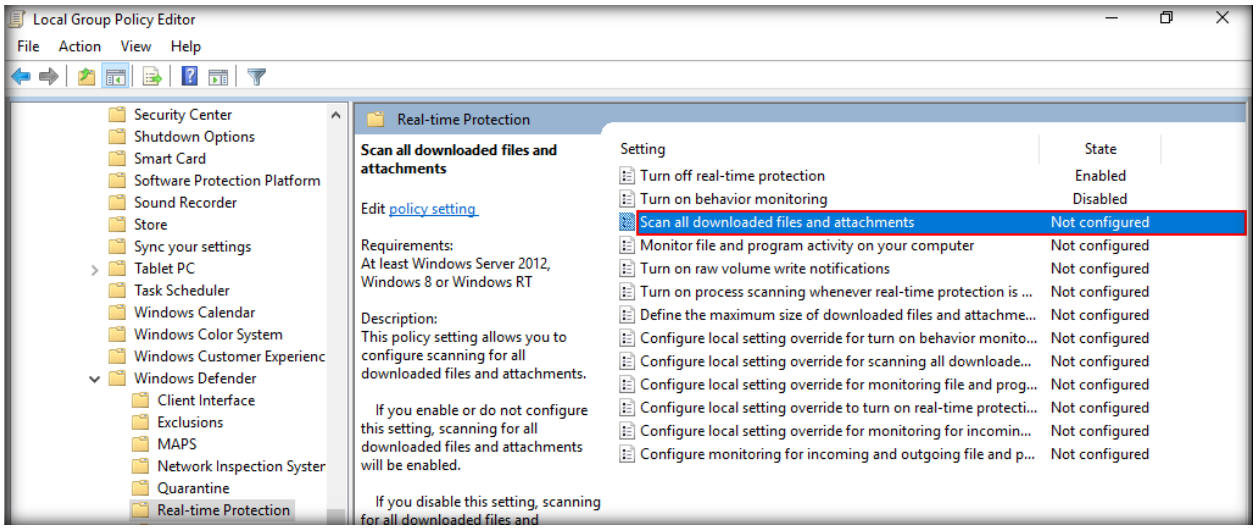
11. Double-click **Turn on behavior monitoring** setting to configure



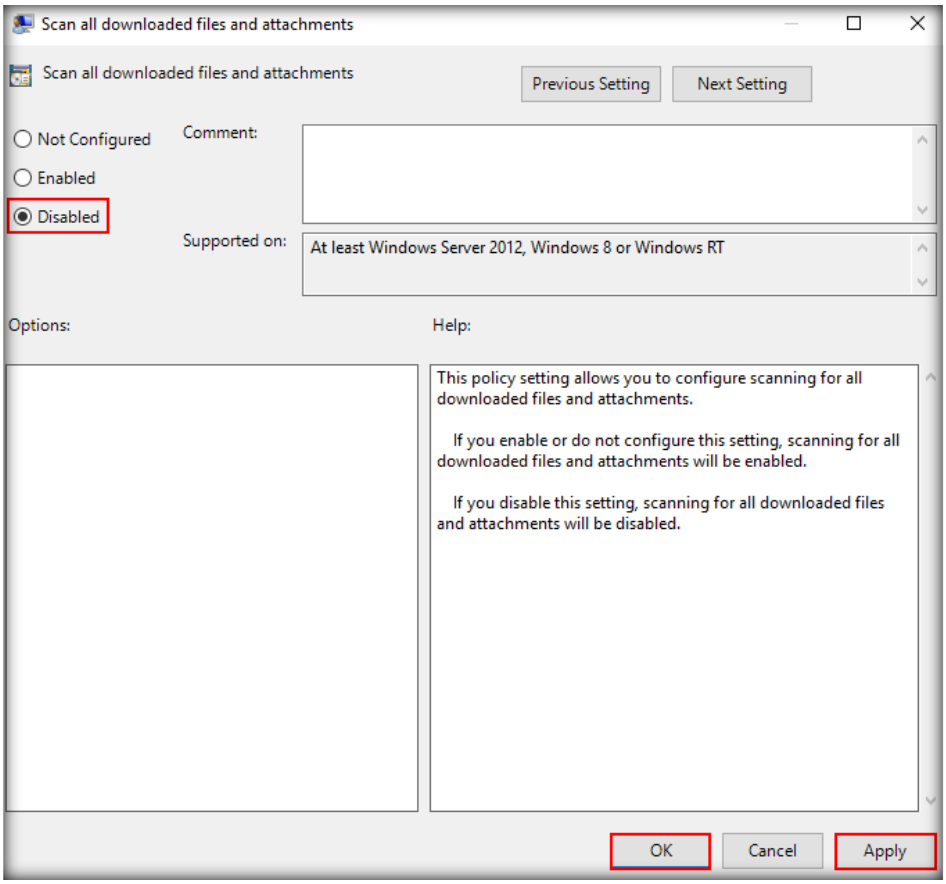
12. Turn on behavior monitoring settings window appears, select **Disabled** radio button and click **Apply** and **OK**



13. Double-click **Scan all downloaded files and attachments** setting as shown in the screenshot



14. Scan all downloaded files and attachments window appears, select Disabled radio button and click **Apply** and **OK**

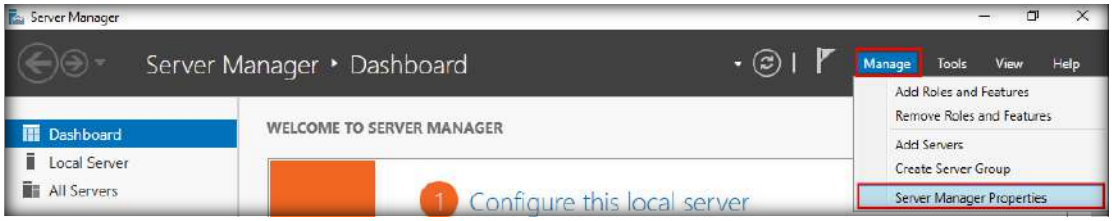


15. Similarly follow the above steps to configure Windows Components in all the Windows machines.

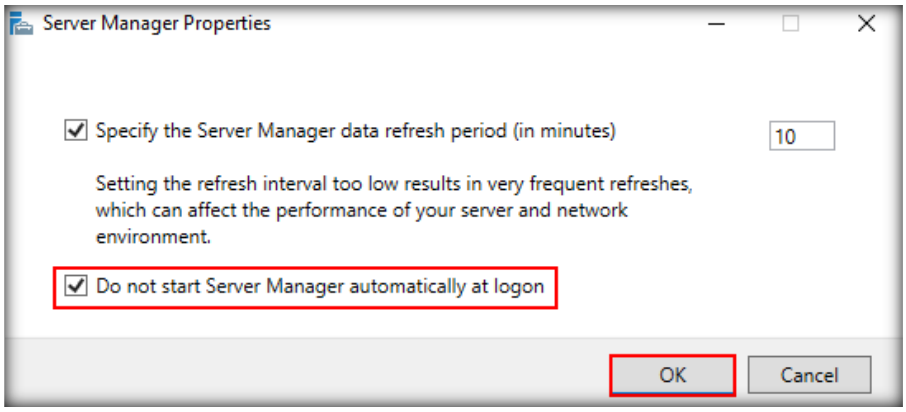
[Back to Configuration Task Outline]

CT#35: Disable Server Manager on Startup in Windows Server 2016 and Windows Server 2012

1. Login to Windows Server 2016 virtual machine, Server Manager window appears
2. Navigate to **Manage** and click **Server Manager Properties**



3. Server Manager Properties window appears, check **Do not start Server Manager automatically at logon** option and click **OK**
4. **Close** the Server Manager window

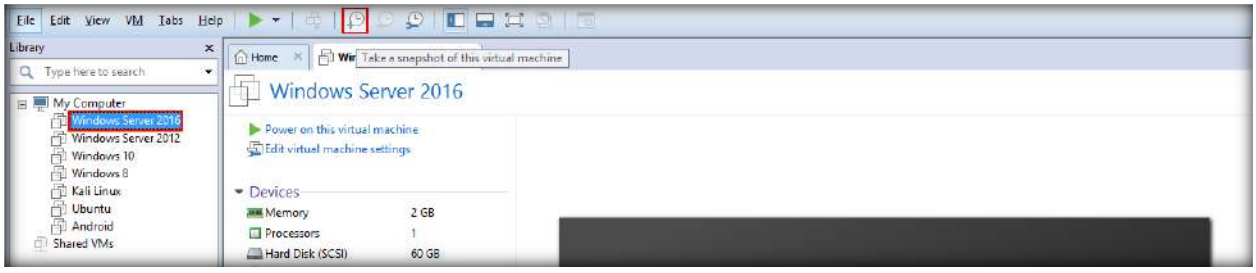


Note: Similarly follow the above steps to configure Server Manager properties in Windows Server 2012 machine

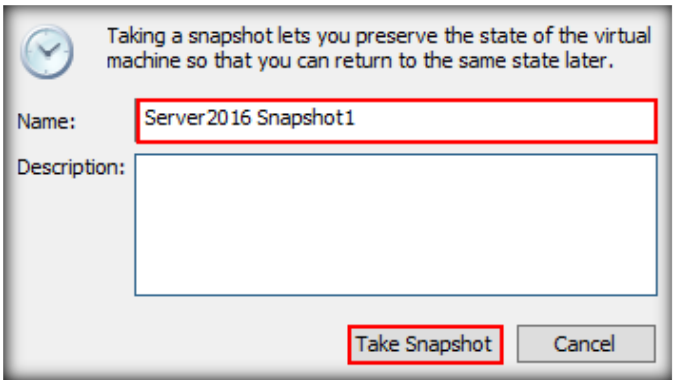
[Back to Configuration Task Outline]

CT#36: Taking Snapshots of Virtual Machines

1. Make sure that all the virtual machines are turned off, click **Windows Server 2016** in the left pane and click **Take a snapshot of the virtual machine** icon as shown in the screenshot



2. Windows Server 2016 – Take Snapshot pop-up appears, type a name for the snapshot in the Name field, leave the description field to default and click **Take Snapshot**



Note: Similarly take snapshots of the all virtual machines once all the configuration tasks are completed

[Back to Configuration Task Outline]

End of the Document