

CEHv10

Classroom Lab Setup Guide

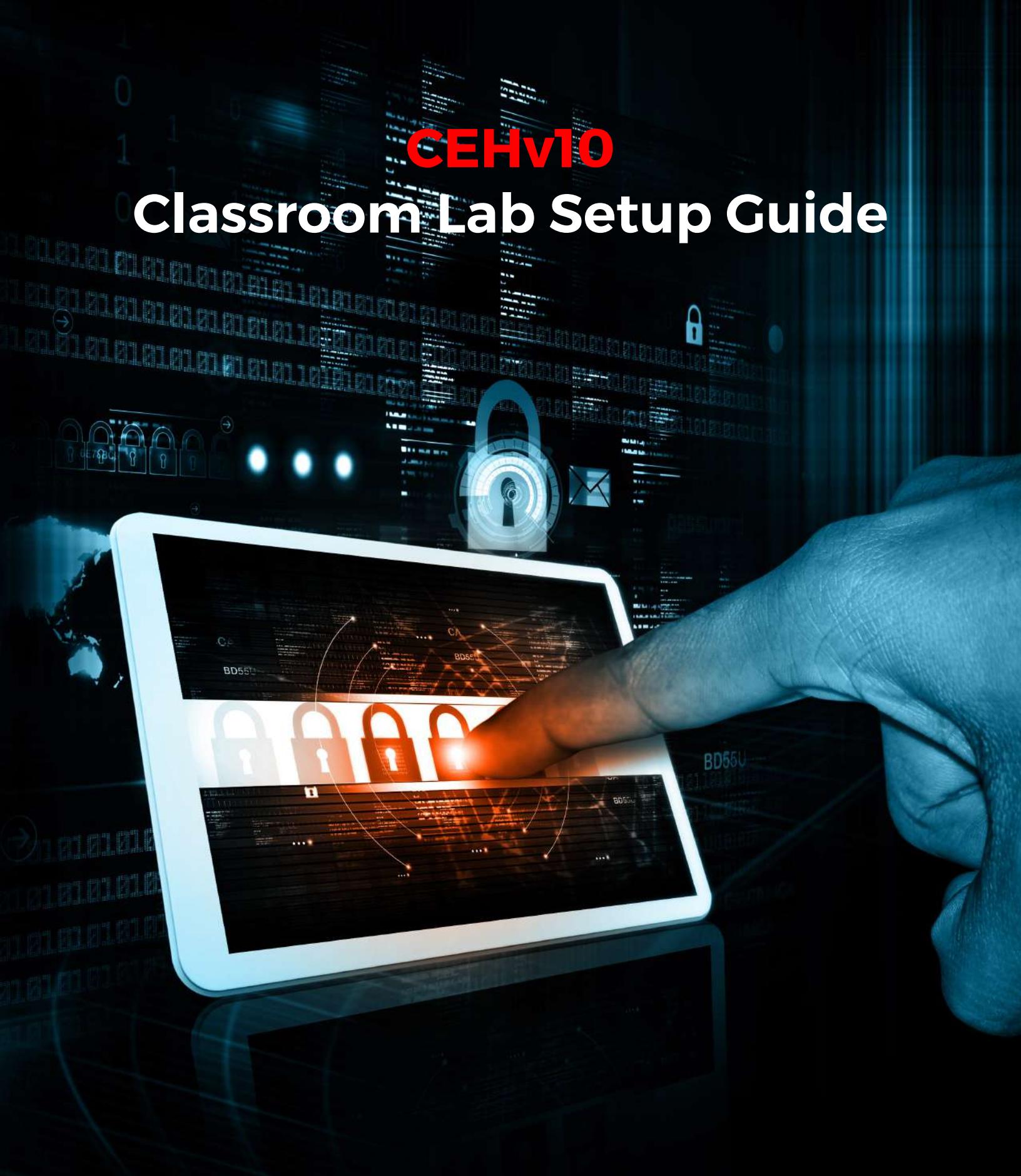


Table of Contents

Classroom Setup Instructions: CEHv10	3
Classroom Requirements	4
Hardware.....	5
Software.....	5
Classroom Connectivity	5
Configuration.....	6
Setup Document Overview.....	6
Training Room Environment	6
Instructor's Computer.....	7
Student Workstations	8
Room Environment	11
Classroom Configuration.....	11
Computer Names.....	11
Network Topology	12
CEH VM Setup in Instructor and Students' Machines.....	13
NDA Document.....	13
Instructor Acceptance.....	13
Firewall Settings	13
Blackboard	14
Setup Checklist.....	15
Instructor Acceptance	16
Assistance.....	16
Detailed Setup Instructions - Configuration Tasks (CT).....	17
CT#1: Download CEH Tools.....	17
CT#2: Install VMware Workstation Pro in Host Machine.....	17
CT#3: Configuring Virtual Network in the VMware Virtual Network Editor.....	18
CT#4: Installing Virtual Machines (Windows)	22
CT#5: Configure Internet Explorer (IE) Enhanced Security Configuration in Windows Server 2016.....	32
CT#6: Adding Roles IIS (Internet Information Services), File Services, SNMP and Remote Access roles in Windows Server 2016 (Virtual Machine)	34
CT#7: Install Kali Linux in VMware.....	41
CT#8: Install Ubuntu in VMware.....	57
CT#9: Install Android in VMware Workstation.....	66
CT#10: Share CEH-Tools Folder to Windows VMs	84
CT#11: Mapping CEH-Tools with Kali Linux Machine.....	88

CT#12: Mapping CEH-Tools with Ubuntu Machine.....	91
CT#13: Mapping CEH-Tools with Android Machine	96
CT#14: Install Adobe Acrobat Reader in Windows VMs	103
CT#15: Install WinRAR in Windows VMs	103
CT#16: Configure Windows Explorer.....	104
CT#17: Install Web Browsers in Windows VMs	104
CT#18: Removing Password Complexity from Guest Operating Systems.....	105
CT#19: Creating Demo User Accounts in Windows Server 2016, Windows 10, and Windows 8....	110
CT#20: Install Active Directory and Create User Accounts in Windows Server 2012	113
CT#21: Configure SNMP Service in Windows Server 2016 and Windows Server 2012	133
CT#22: Install MS SQL Server 2017 Express Edition on Windows Server 2016 Virtual Machine.	135
CT#23: Turn off Firewall in all the Machines.....	150
CT#24: Enabling Remote Desktop Connection in all Windows Virtual Machines.....	157
CT#25: Turn off Screen Savers in all the Machines.....	160
CT#26: Test for Pinging each other.....	163
CT#27: Enabling and Configuring FTP Server in Windows 10 Virtual Machine	165
CT#28: Configure the GoodShopping Website Windows Server 2016 (Virtual Machine)	172
CT#29: Configure the moviescope Website in Windows Server 2016 (Virtual Machine)	184
CT#30: Configure Hosts file in all the Virtual Machines	192
CT#31: Install WampServer in Windows Server 2012	197
CT#32: Install and Configure WordPress Website	204
CT#33: Install and Configure Damn Vulnerable Web Application	218
CT#34: Configure Windows Components.....	228
CT#35: Disable Server Manager on Startup in Windows Server 2016 and Windows Server 2012..	234
CT#36: Taking Snapshots of Virtual Machines.....	234

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.

The information contained in this document is subject to change without notice. Unless otherwise noted, the names of companies, products, people and data used in this document are fictional. Their use is not intended in any way to represent any real company, person, product or event. Users of this document are responsible for compliance with all applicable copyright laws. No part of this document may be reproduced or transmitted by any means, electronic or mechanical, for any purpose, without the express written consent of the International Council of Electronic-Commerce Consultants, herein after referred to as the EC Council. If, however, your only means of access is electronic, permission is hereby granted to print one copy.

The EC-Council may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering the material in this document. Except as expressly provided in any written license agreement from the EC-Council, providing this document does not give you any license to those patents, trademarks, copyrights or other intellectual property.

EC-Council Certified Ethical Hacker and CEH are either registered trademarks or trademarks of the EC-Council in the USA and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

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)

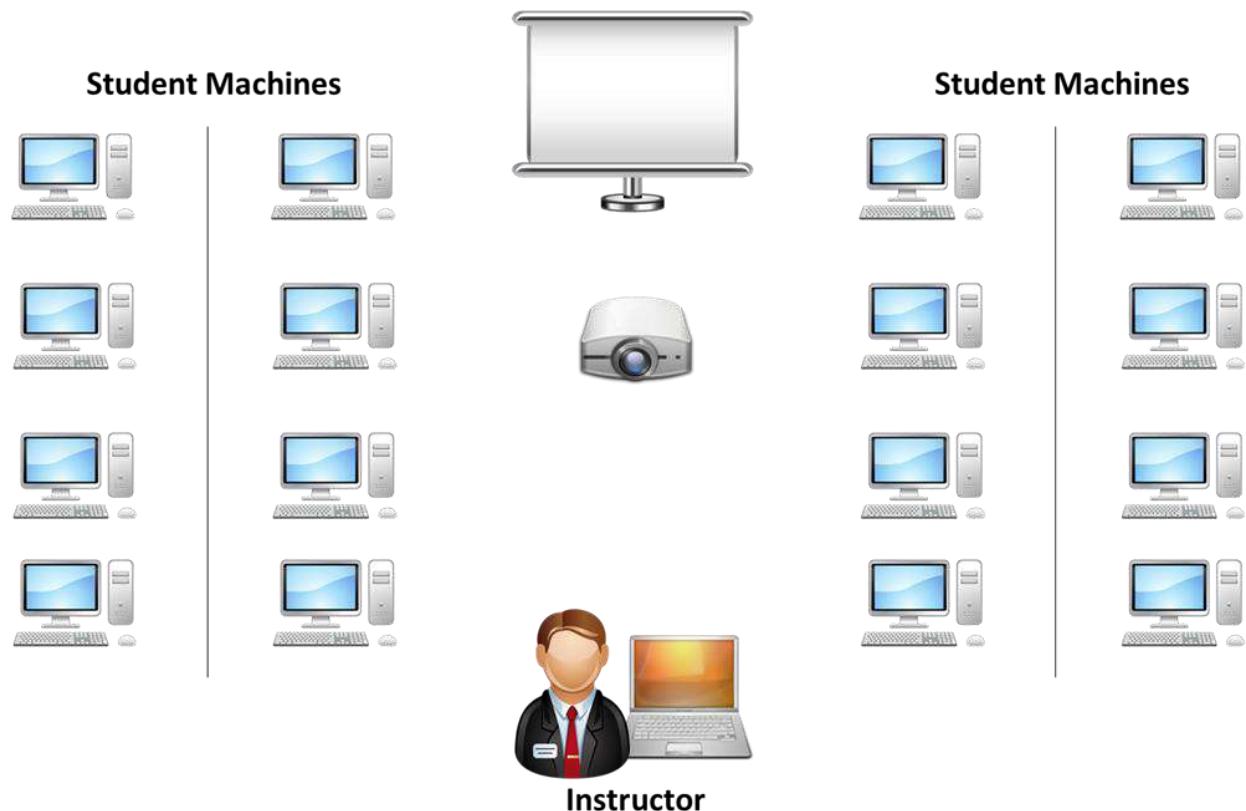
- Have Remote Desktop Connection enabled in all Windows virtual machines (See [CT#24](#) in Configuration Task section)
- Screen Savers turned off in the Windows Server 2012 and Windows 8 virtual Machines (See [CT#25](#) in Configuration Task section)
- Ping test verified between all the machines in 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.



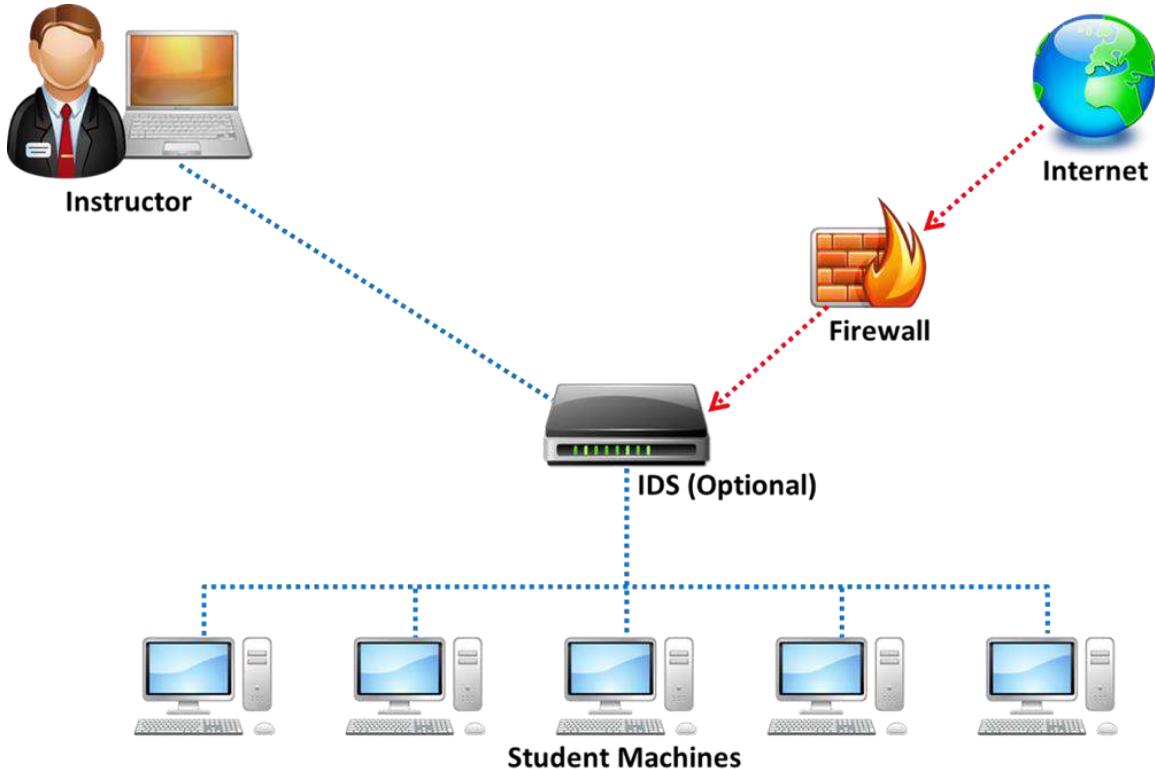
Computer Names

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

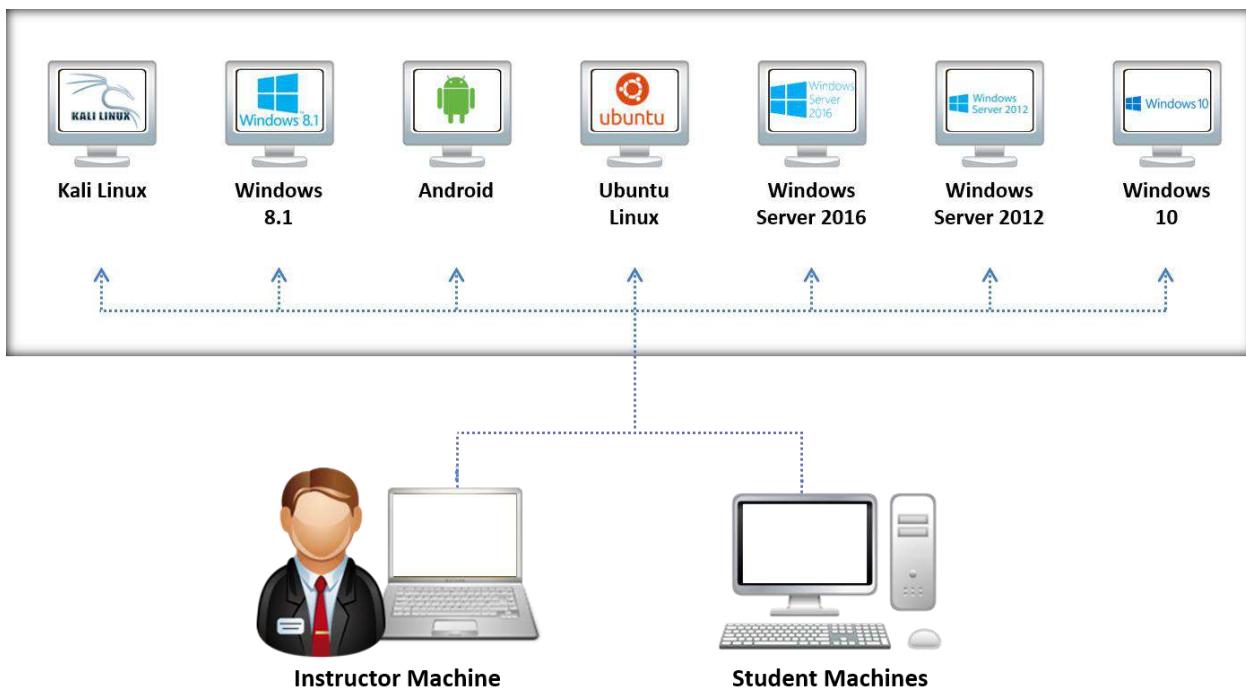
The training room must be physically isolated from any production network. Students must be able to access the Internet from their PCs. All computers are connected as one isolated network and domain. The common protocol is IP. All computers should have dynamic IP addresses using DHCP server. Configure 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

Instructor Name: Jack Smith

The Username / Password to logon to the student machine

administrator / Pa\$\$w0rd

Welcome to CEHv10 Class!

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
<input type="checkbox"/>	Verify that VMware Workstation Pro Installed
<input type="checkbox"/>	Verify that all CEH tools are on the computer in CEH-Tools folder in the D:\
<input type="checkbox"/>	Verify that Internet access is available
<input type="checkbox"/>	Visit https://www.eccouncil.org and view the page to check Internet access
<input type="checkbox"/>	Open Command Prompt and type nslookup certifiedhacker.com and look for connection to the server
<input type="checkbox"/>	Verify Acrobat Reader and WinRAR and command prompt extensions are installed
<input type="checkbox"/>	Verify that the Instructor computer can image through the overhead projector
<input type="checkbox"/>	Verify each computer has 200 GB or more free disk space
<input type="checkbox"/>	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
<input type="checkbox"/>	Cable wiring organized and labeled
<input type="checkbox"/>	Student workstations and chair placement is satisfactory
<input type="checkbox"/>	Placement of LCD (overhead) projector is appropriate
<input type="checkbox"/>	Whiteboard and dry erase markers and erasers are available
<input type="checkbox"/>	Instructor station is properly organized and oriented
<input type="checkbox"/>	Computers are labeled with client number
<input type="checkbox"/>	EC-Council courseware (Official EC-Council CEHv10 Box) is available for students
<input type="checkbox"/>	Student NDA agreement downloaded and printed for every student in the class and placed on each student's desk
<input type="checkbox"/>	Write down the facility's technical contact person's hand phone number. Contact him in case of network problem
<input type="checkbox"/>	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.

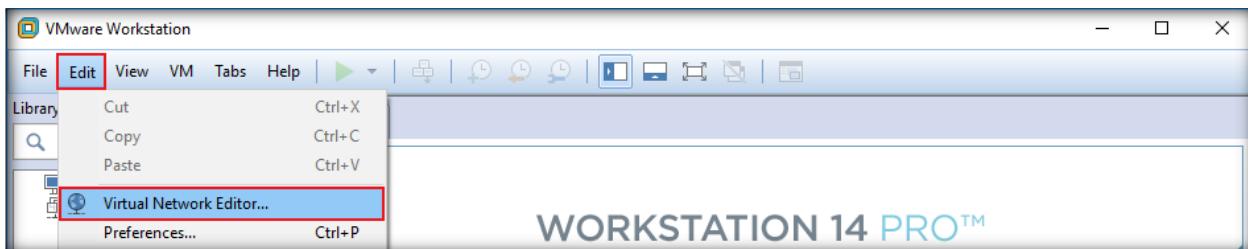
4. On completion of the installation, the machine will restart
5. Once the machine got rebooted launch the VMware Workstation Pro

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

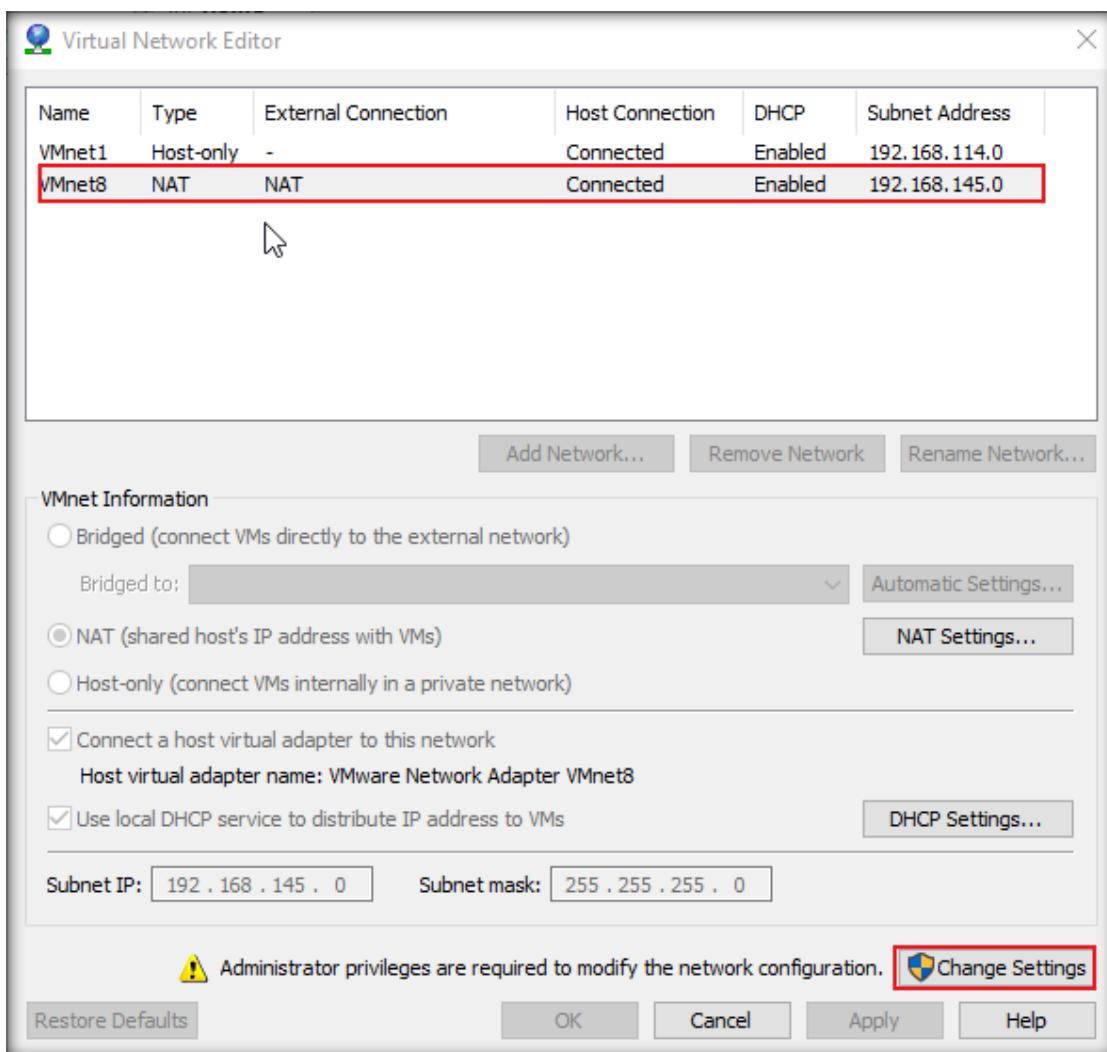
[\[Back to Configuration Task Outline\]](#)

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

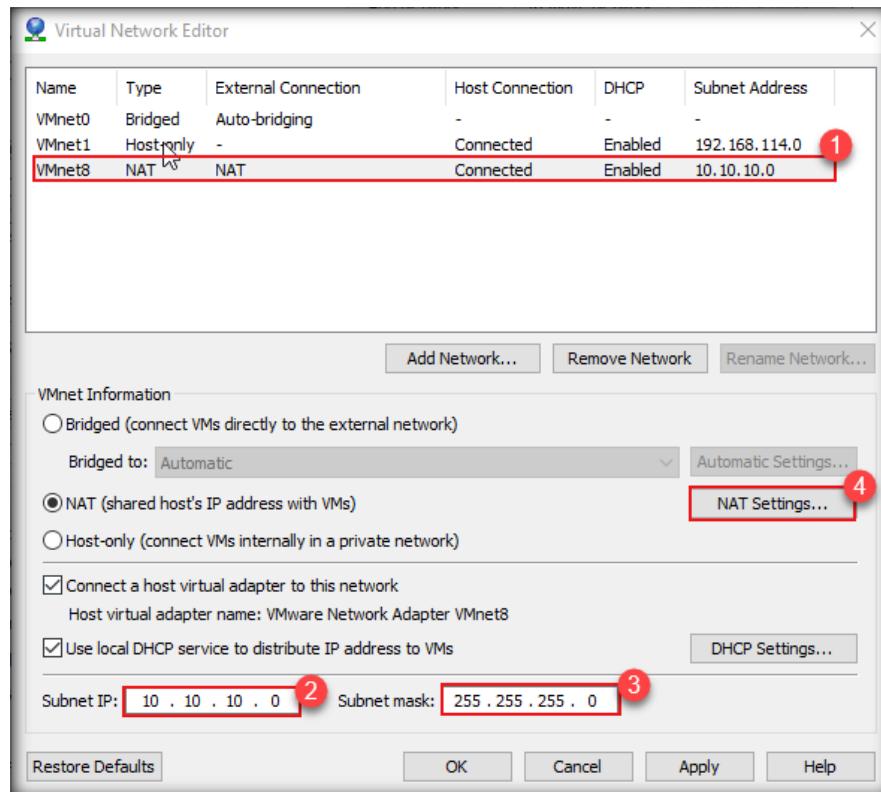


3. Virtual Network Editor window appears, choose **VMnet8 NAT** network, and click **Change Settings**

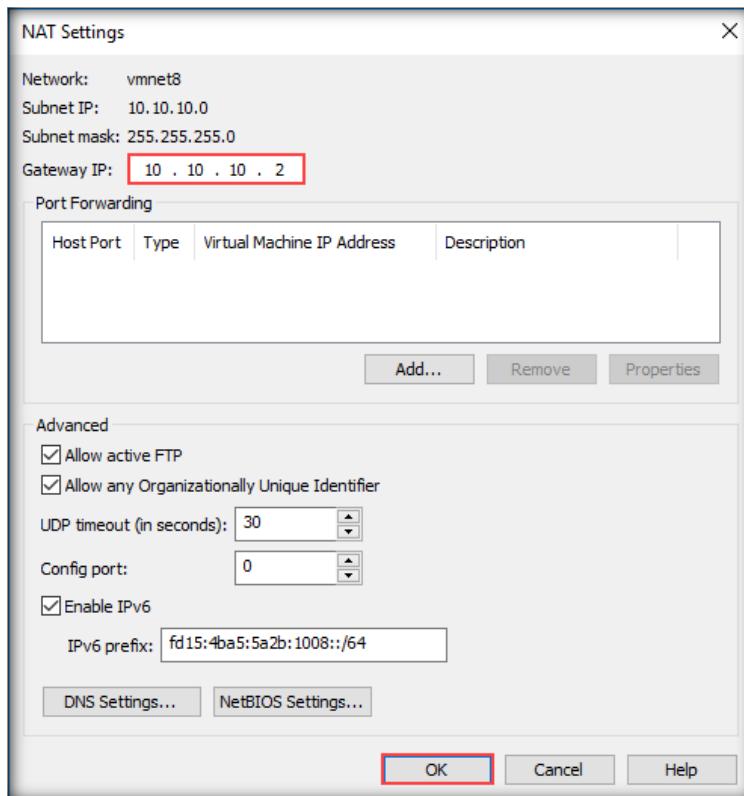


4. If User Access Control pop-up appears, click **Yes**.

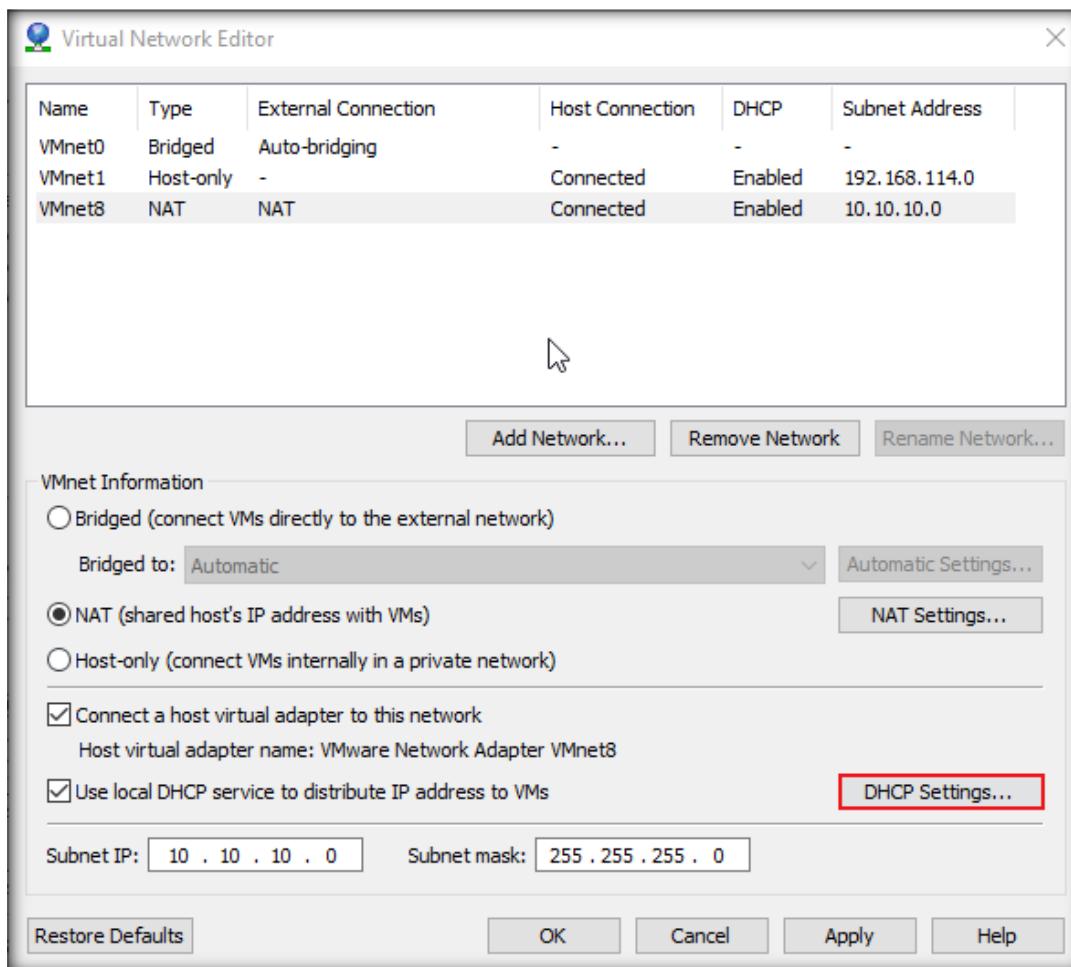
5. Define Subnet IP as **10.10.10.0**, Subnet Mask as **255.255.255.0**, and click **NAT Settings**



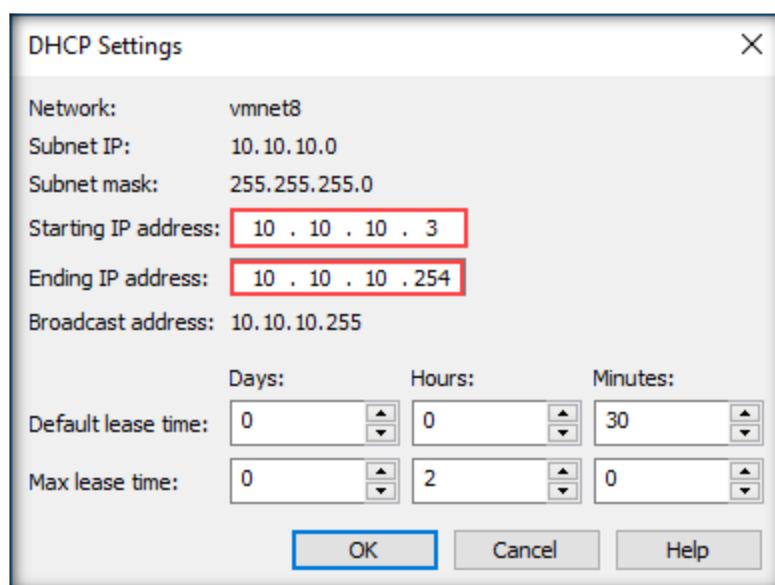
6. NAT Settings window appears, Enter Gateway IP as **10.10.10.2** and click **OK**



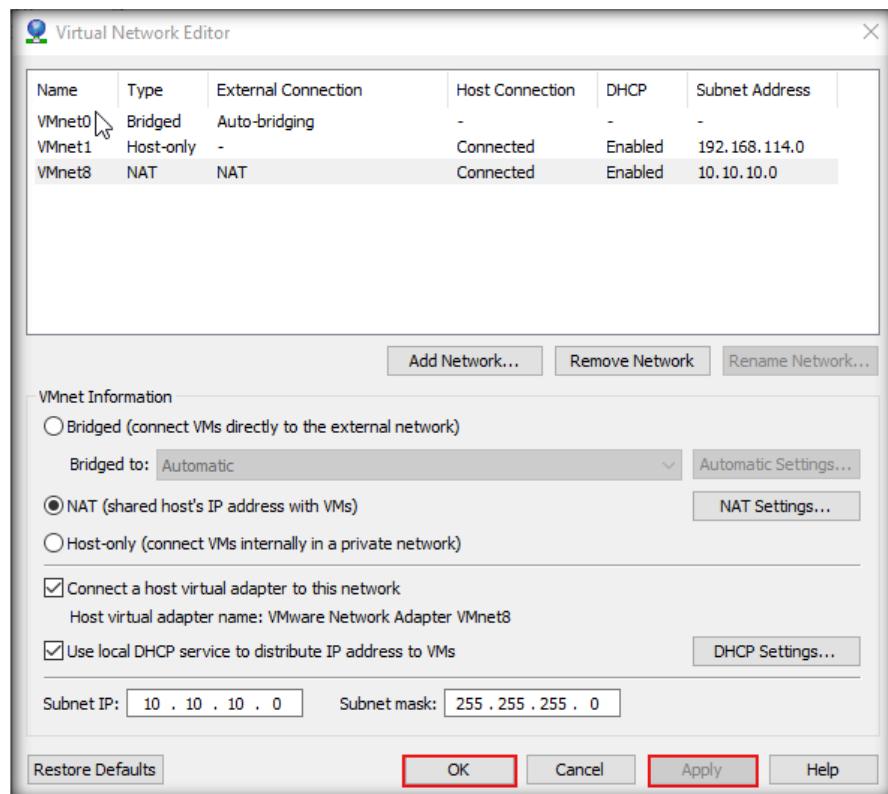
7. Now we keep **VMnet8** selected and click **DHCP Settings**



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](#)]

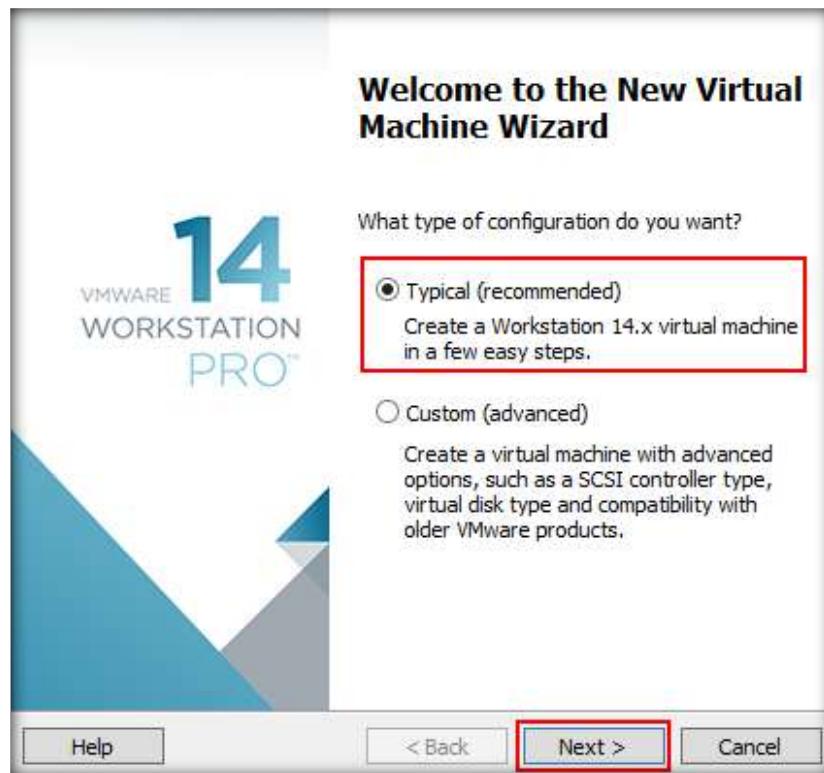
CT#4: Installing Virtual Machines (Windows)

Install Windows Server 2016 Virtual Machine

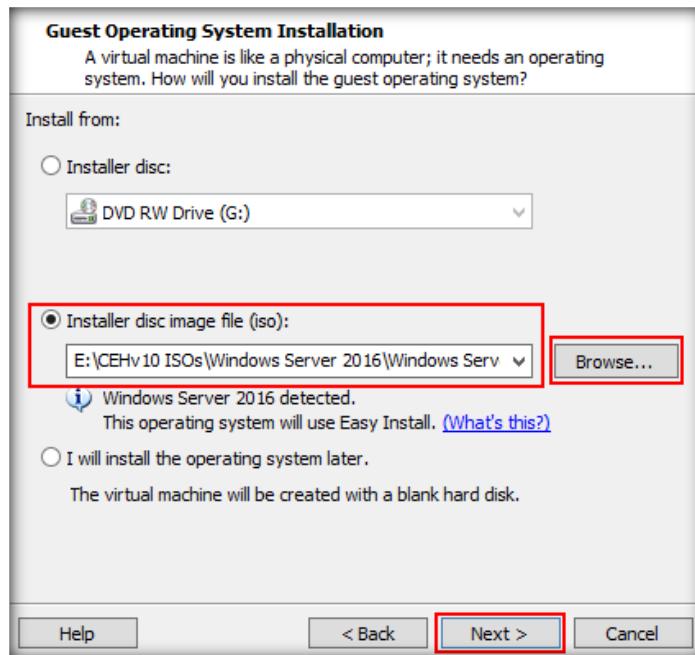
1. In VMware Workstation window, click **Create a New Virtual Machine**



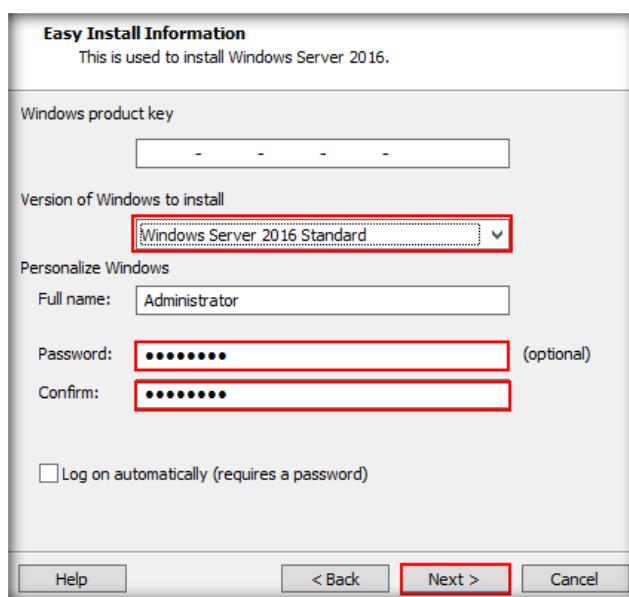
2. In the New Virtual Machine wizard, leave the settings to default and click **Next**



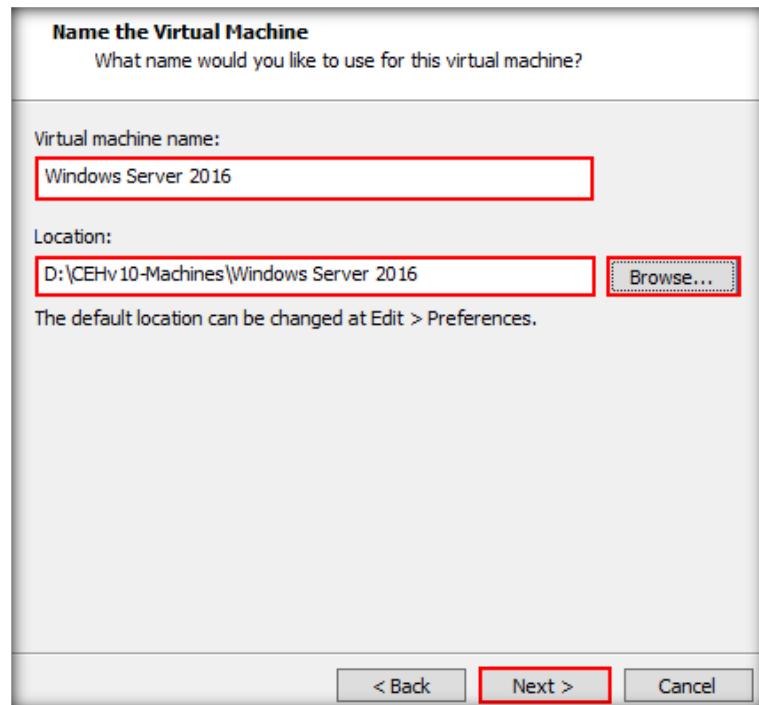
3. In Guest Operating System Installation wizard, choose **Installer disc image file (iso)**: radio button (if you have an ISO of the Windows Server 2016) and then click Browse button to provide the ISO path and click **Next**



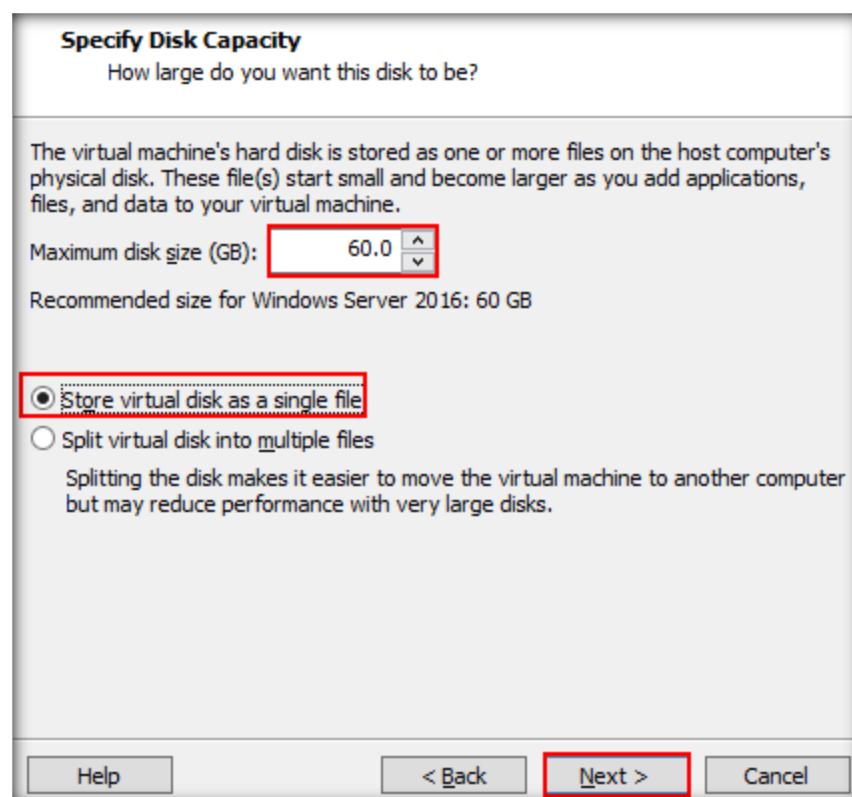
4. Easy Install Information wizard appears. If you have Windows Server 2016 product key then enter the product key or leave it blank
5. Choose **Windows Server 2016 Standard** in the Version of Windows to install section
6. Leave the Username as **Administrator** and type **Pa\$\$w0rd** in Password and 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 do not have product key



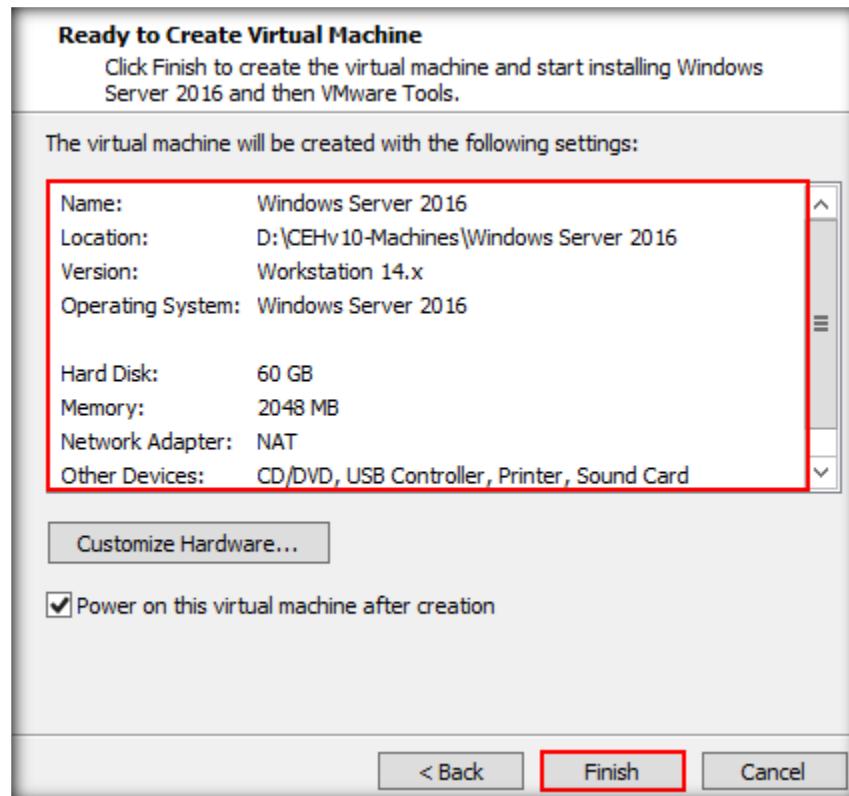
8. Name the Virtual Machine wizard appears, type **Windows Server 2016** in the Virtual machine name field and click **Browse** button to store the virtual hard disk, you can choose the desired location to store the hard disk and then click **Next**



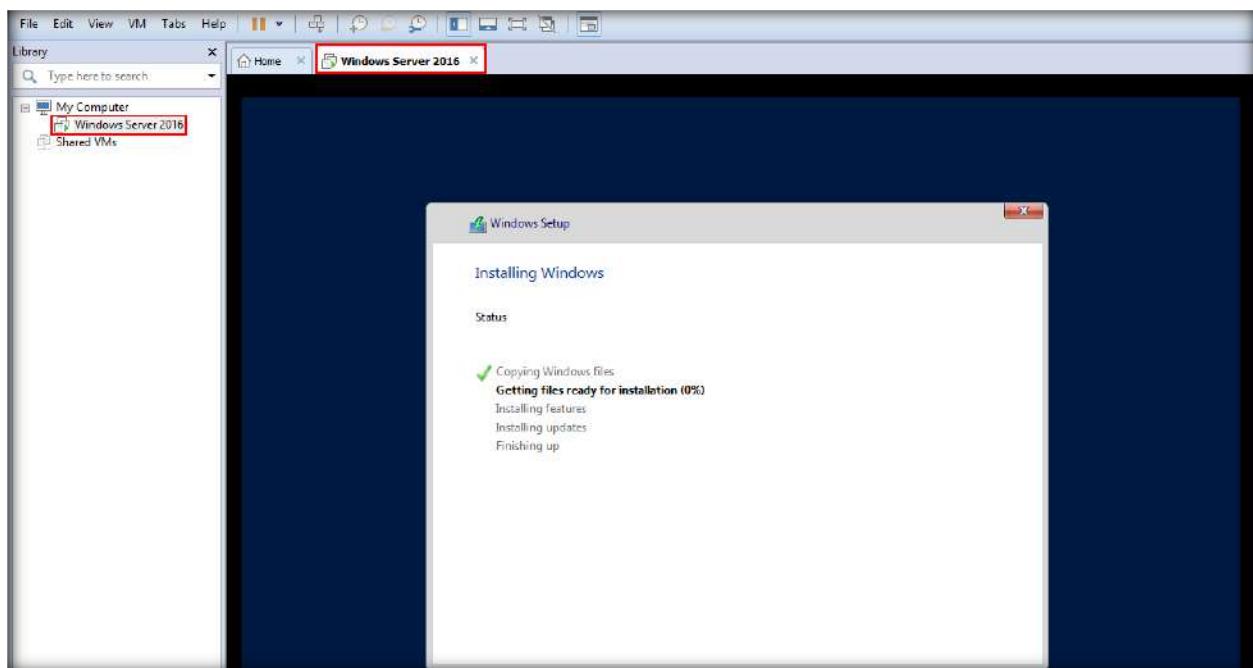
9. Specify Disk Capacity wizard appears, leave the Maximum disk size to default (i.e., **60 GB** recommended) and choose **Store virtual disk as a single file** and click **Next**



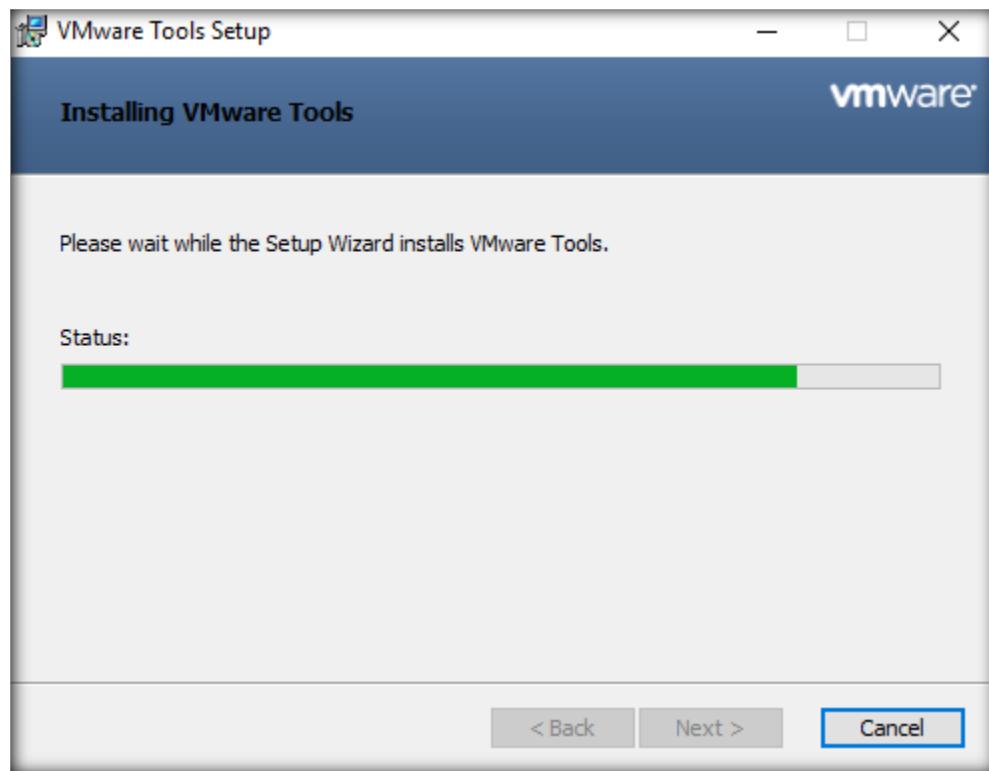
10. Ready to Create Virtual Machine wizard appears, confirm with the settings and click **Finish**



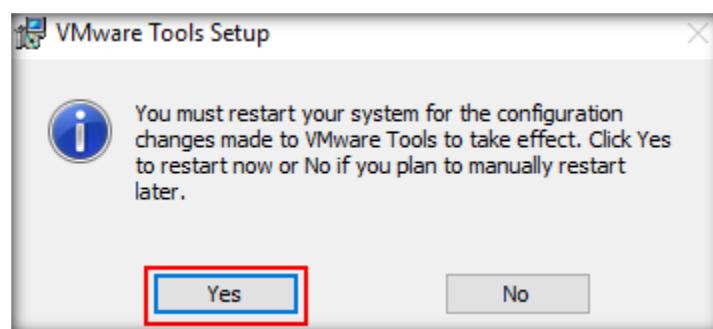
11. As soon as you click **Finish** button, Windows Server 2016 virtual machine pane opens in the VMware Workstation pro and start installing the operating system
12. The machine will restart once the installation is completed



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



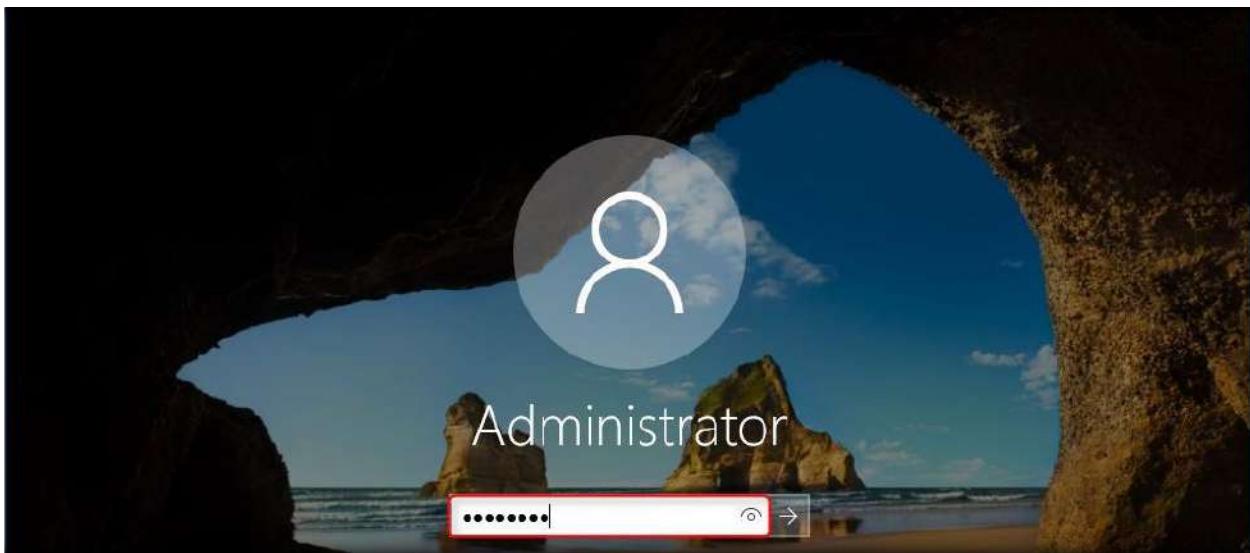
15. After installation is completed it will prompt you to restart the machine click **Yes** to restart



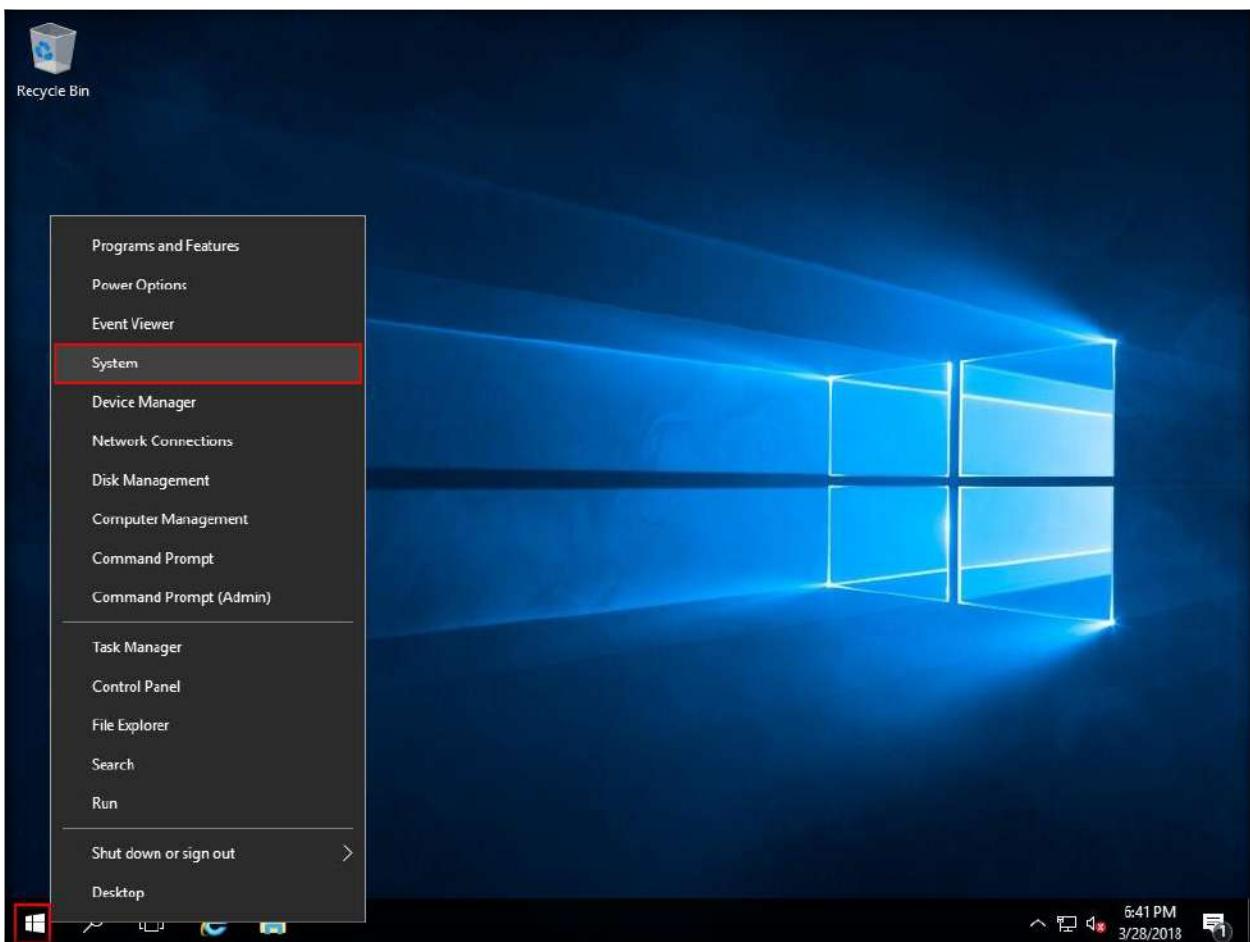
16. Once the installation is finished, the lock screen appears, press the **Send Ctrl+Alt+Delete to this virtual machine** icon from the menu bar



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



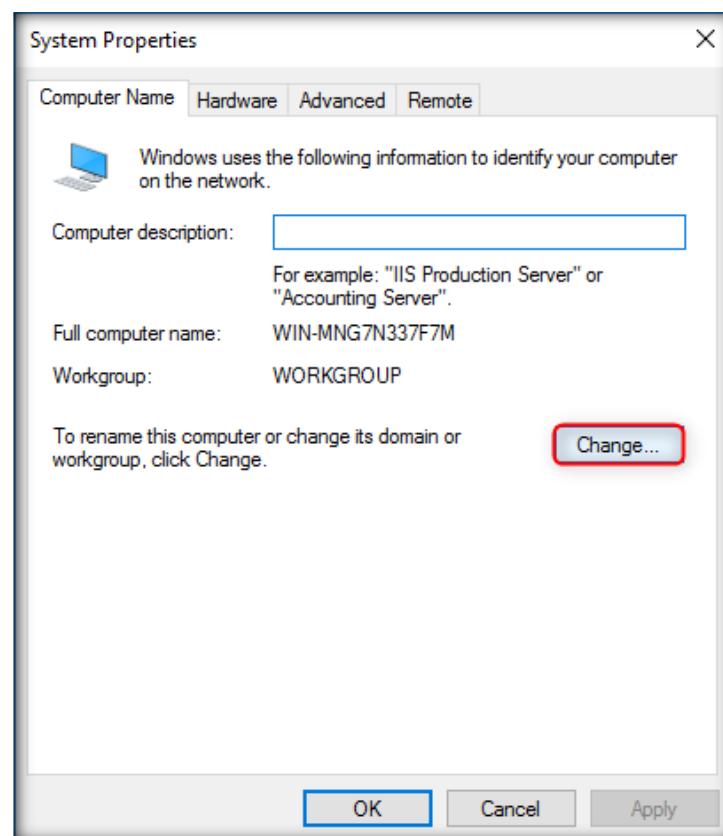
18. Windows Server 2016 desktop appears, close the **Server Manager** window that appears. Right click the **Start** button on the bottom-left and click **System** from the context menu



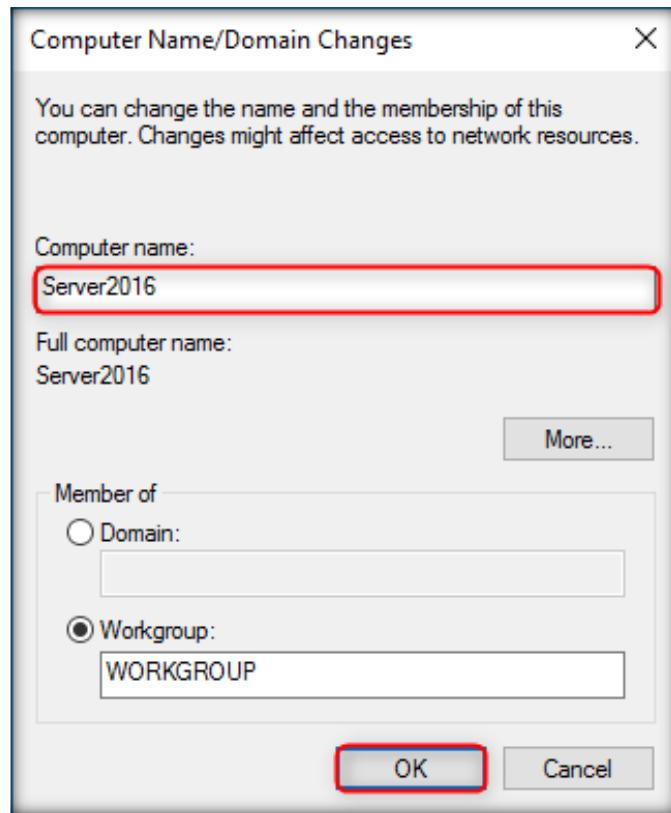
19. System window appears, click **Change settings** as shown in the screenshot:



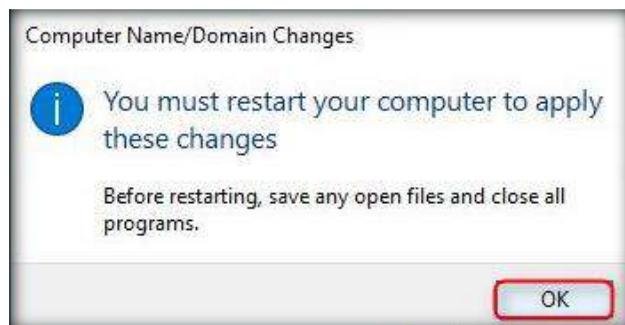
20. System Properties window appears, click **Change...** as shown in the following screenshot:



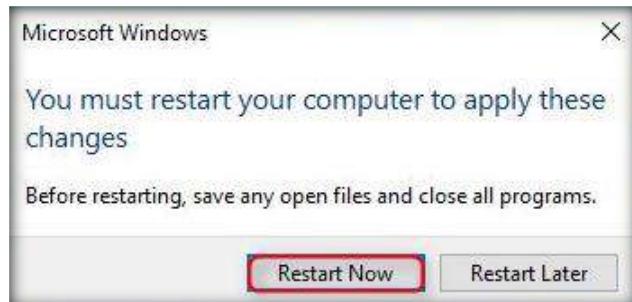
21. Type a computer name (here, **Server2016**) and click **OK** as shown in the following screenshot



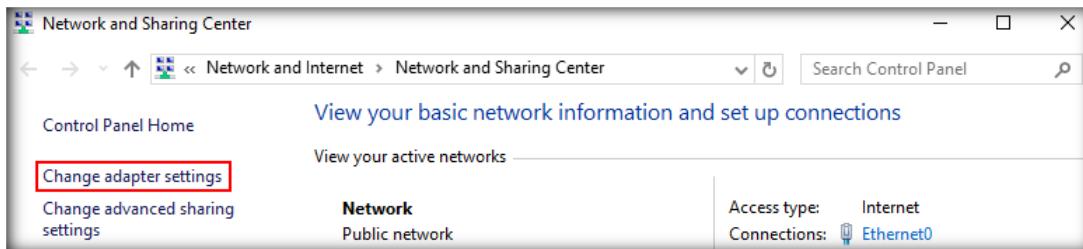
22. You must restart your computer to apply these changes pop-up appears, click **OK**
23. **Close** any open windows



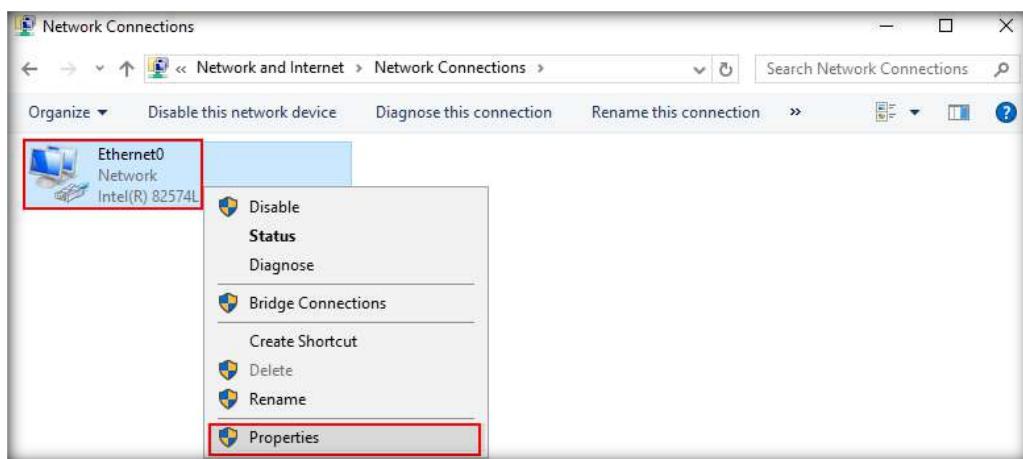
24. Microsoft Windows pop-up appears, click **Restart Now**



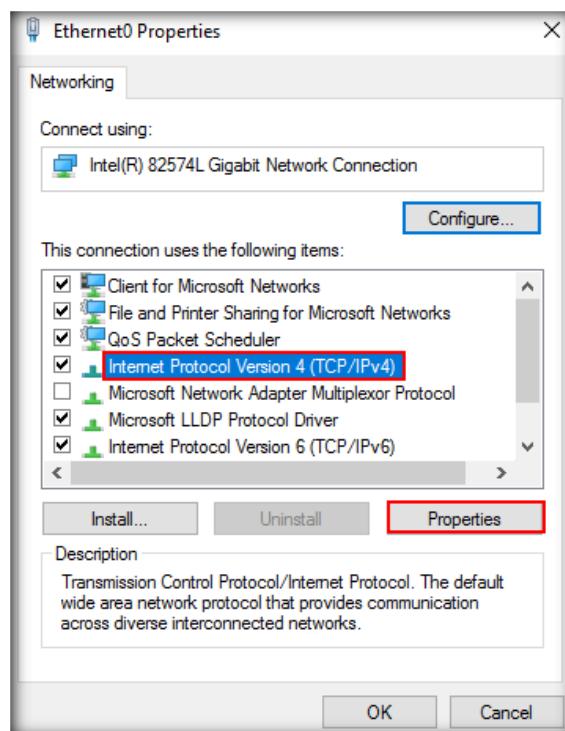
25. After the virtual machine restarts, login to virtual machine and close the Server Manager window. Open **Network and Sharing Center** and click **Change adapter settings** link from the left pane



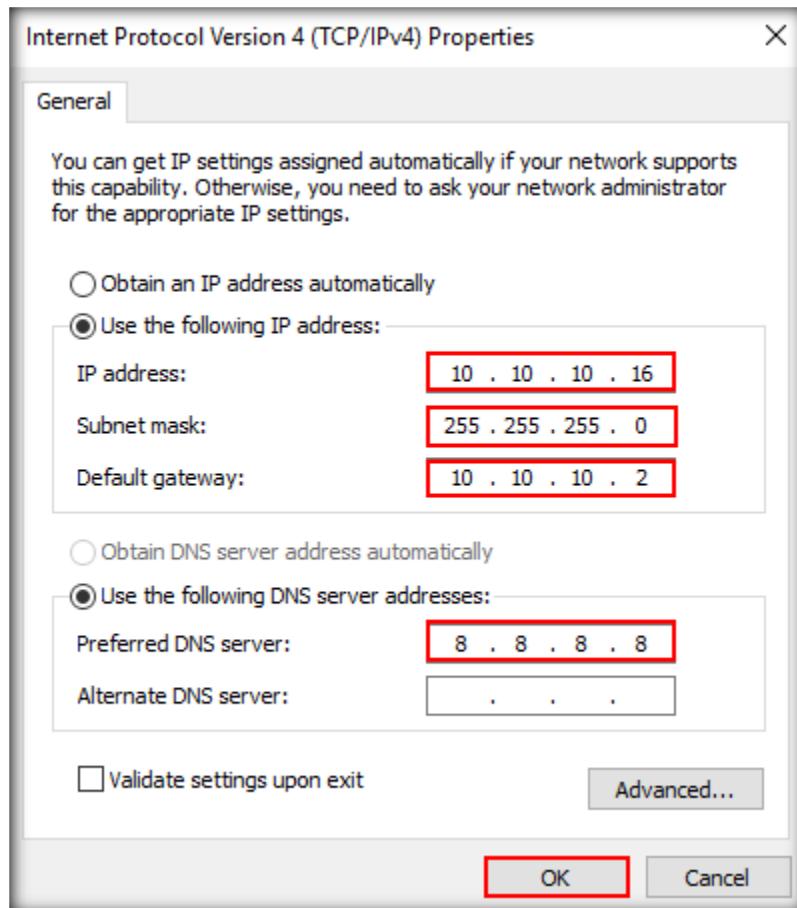
26. Right-click the network interface (here, **Ethernet0**) and click **Properties**



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



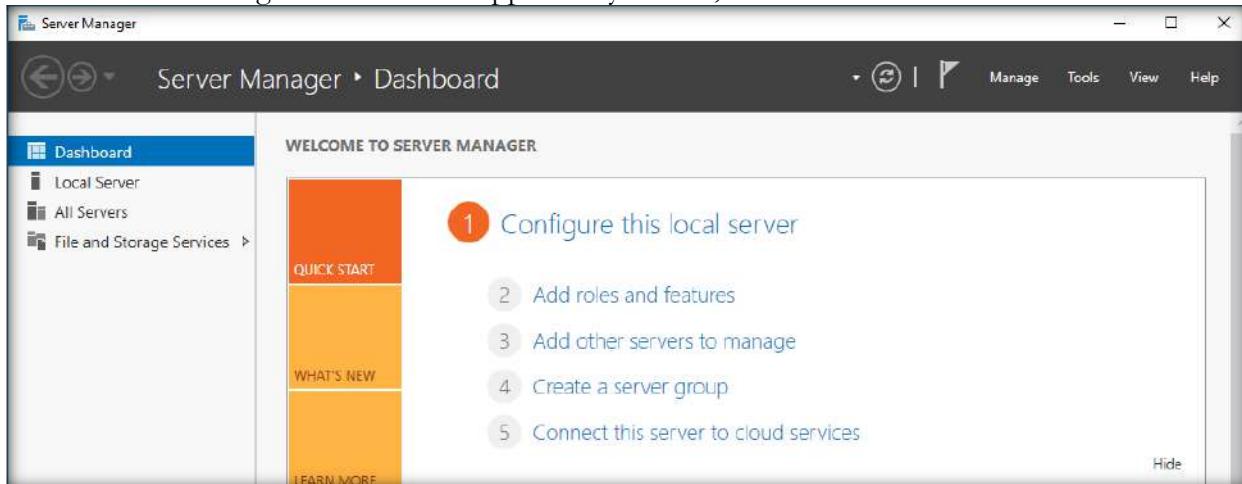
28. Select **Use the following IP address** radio button, assign **10.10.10.16** as **IP address**, **255.255.255.0** as **Subnet mask** and **10.10.10.2** as **Default gateway**
 29. Assign **8.8.8.8** as the **Preferred DNS server** address and click **OK**



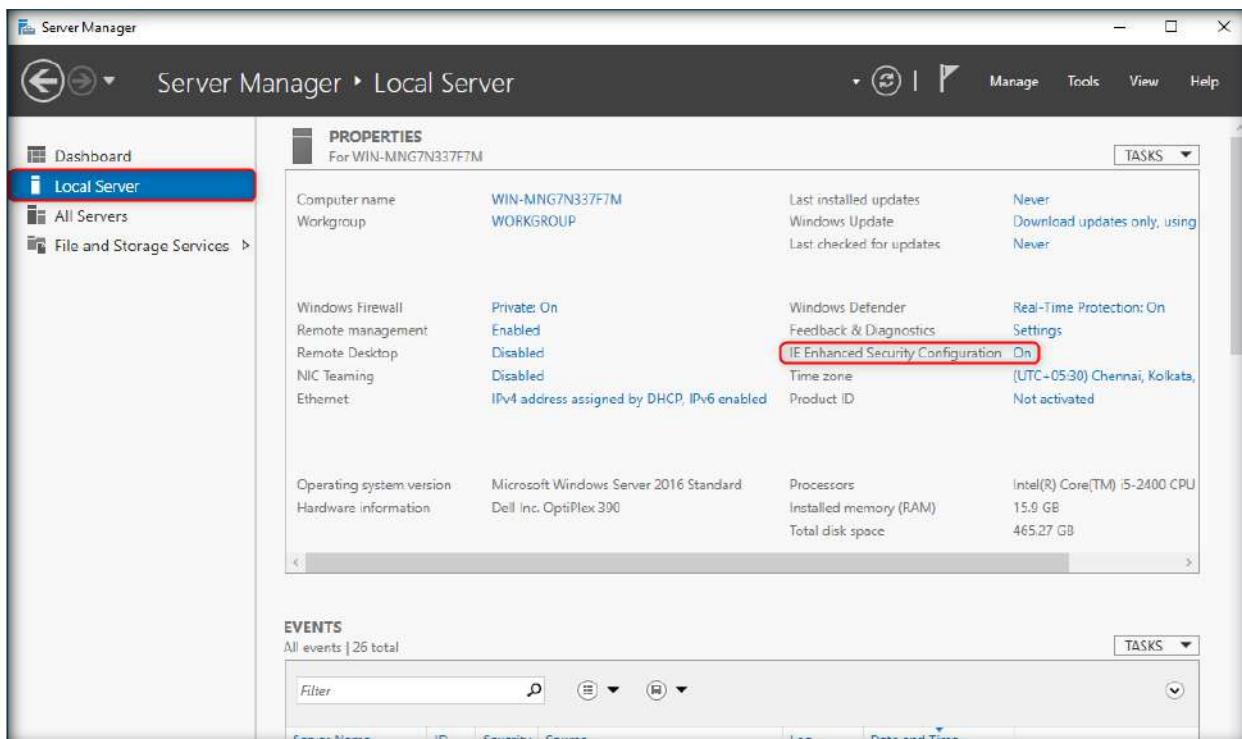
30. Close the **Ethernet0 Properties** window
 31. Similarly, Create and Install **Windows Server 2012 R2 (64-bit)**, **Windows 10**, and **Windows 8**, Virtual Machines with default hard disk space and 2048MB of RAM memory, with the following credentials as mentioned below:
- Windows Server 2012 (10.10.10.12,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



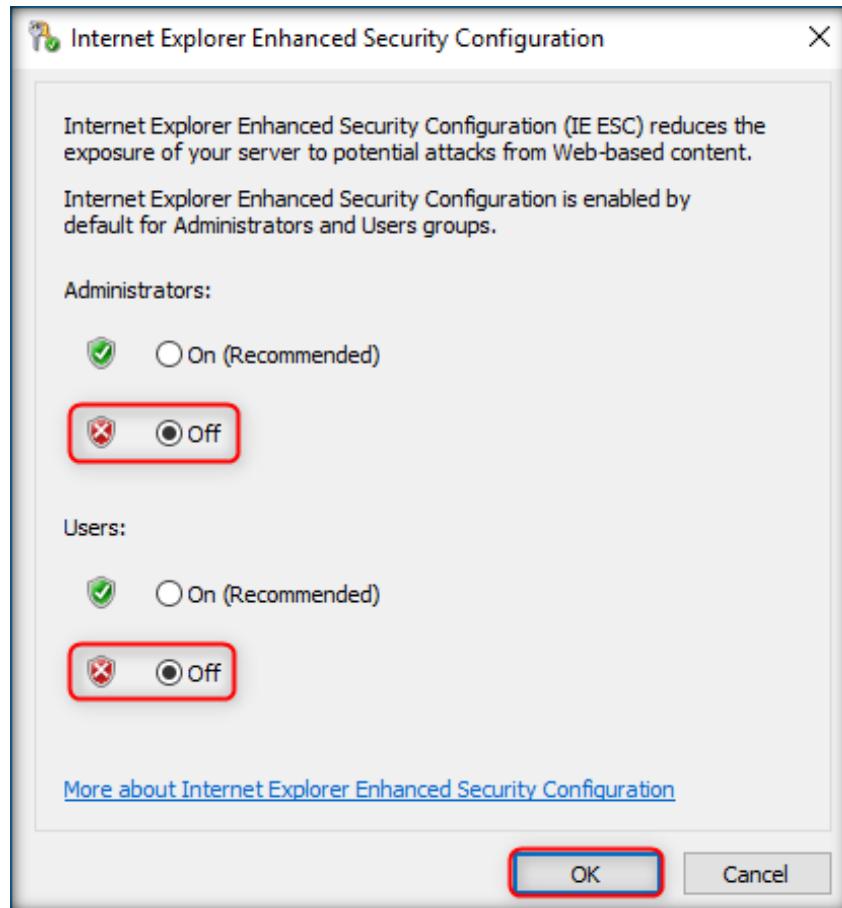
4. Select Local Server in the left pane of the window. In the right pane, click On for IE Enhanced Security Configuration



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.

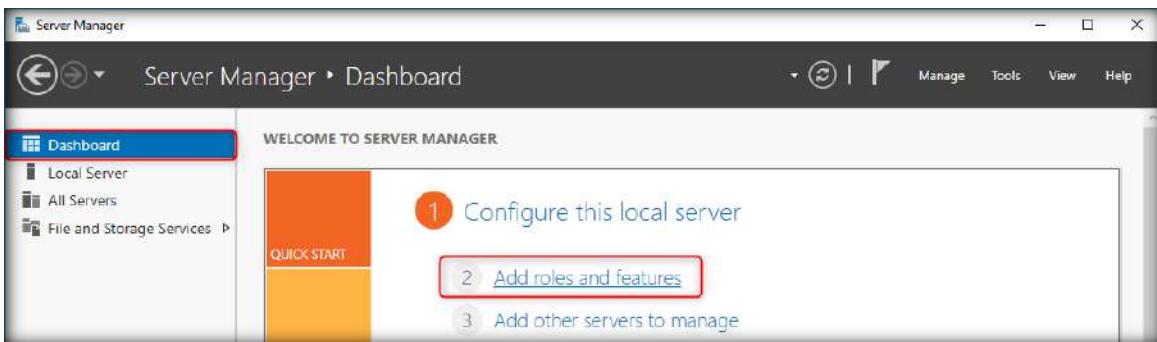


[Back to Configuration Task Outline]

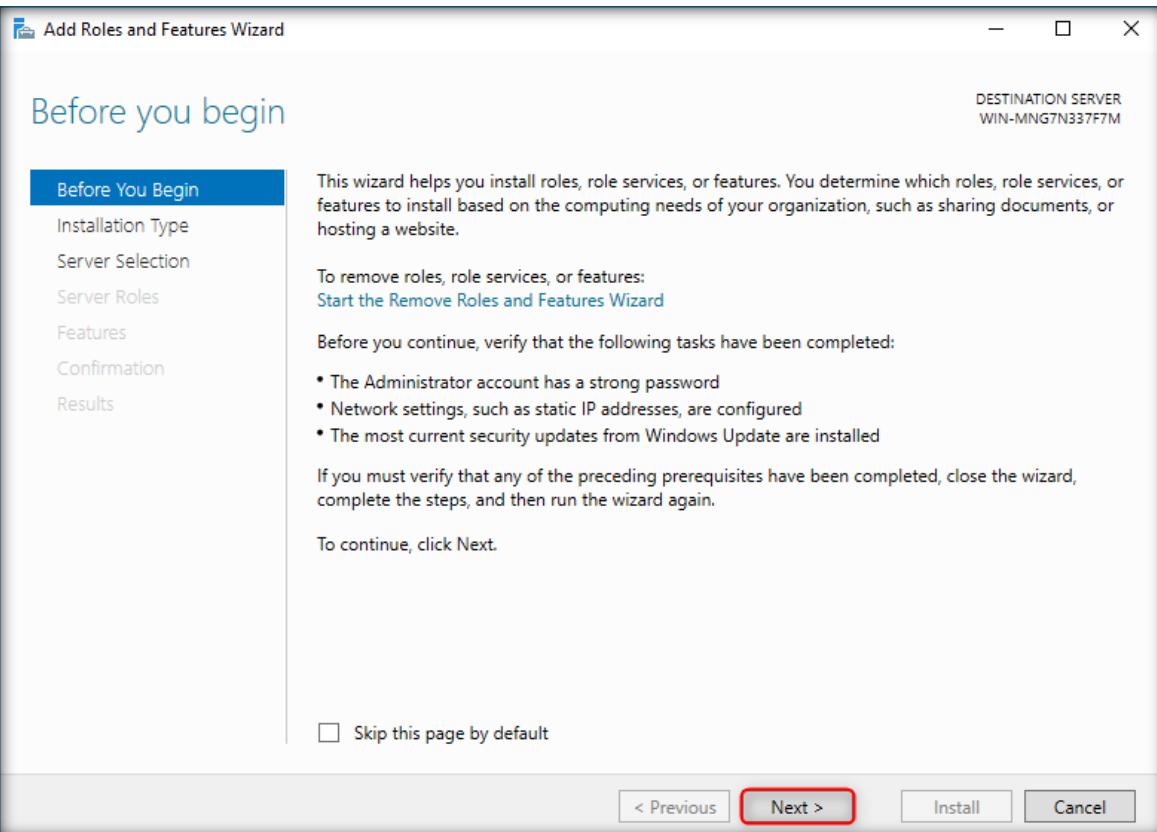
CT#6: Adding Roles IIS (Internet Information Services), File Services, SNMP and Remote Access roles in Windows Server 2016 (Virtual Machine)

Adding IIS (Internet Information Services) roles in Server Manager

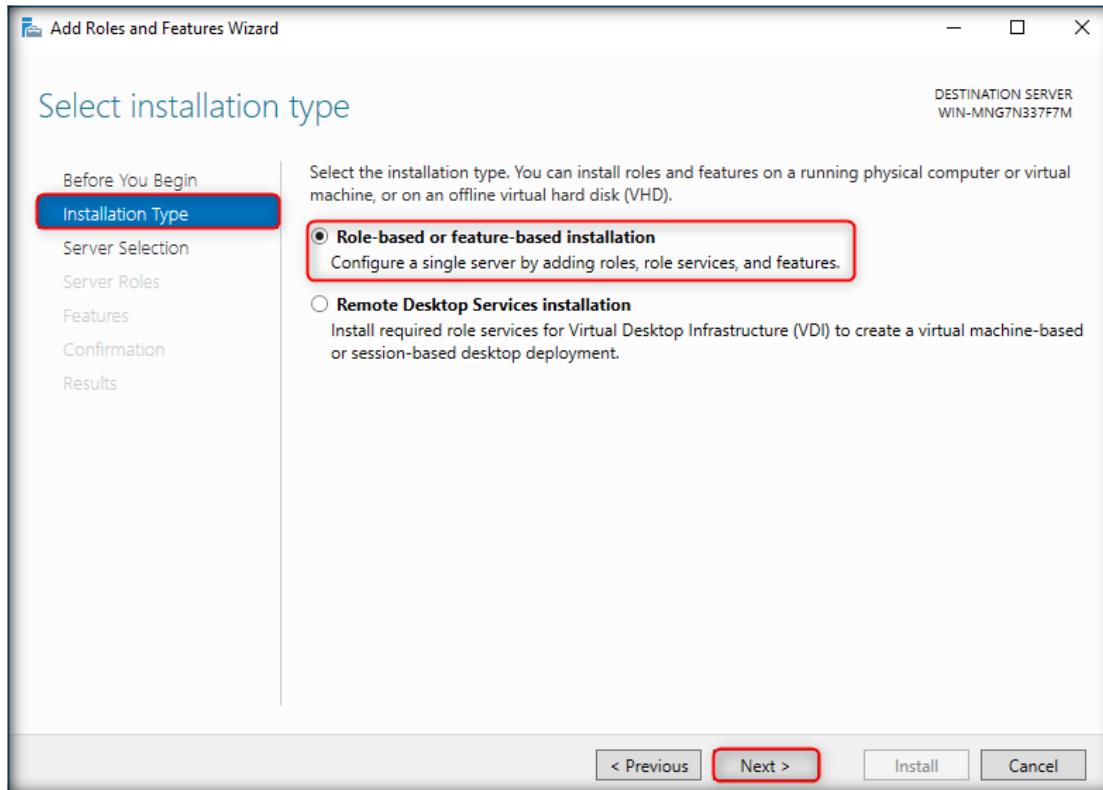
1. Add **Internet Information Services (IIS)** roles in Server Manager
2. To open Server Manager, click **Start → Server Manager App**
3. In Server Manager **Dashboard**, click **Add Roles and Features**



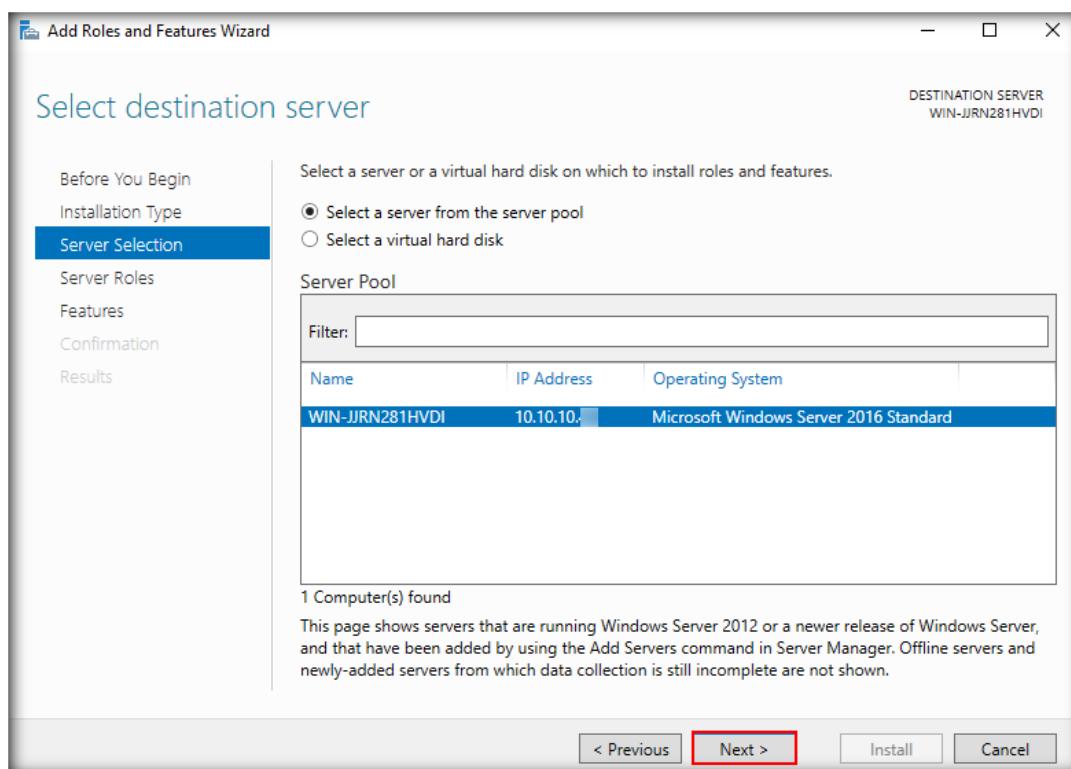
4. **Add Roles and Features Wizard** appears, click **Next**



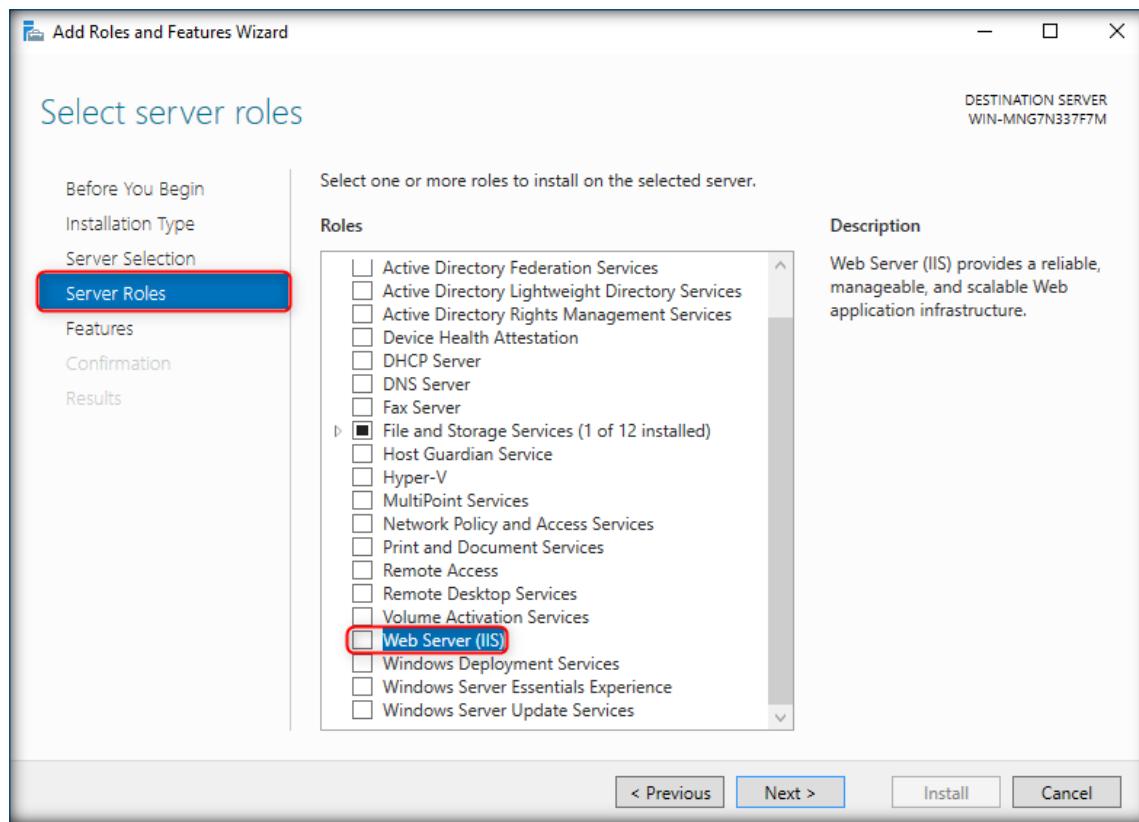
5. In **Installation Type** section of the wizard, select **Role-based or feature-based installation** radio button and click **Next**



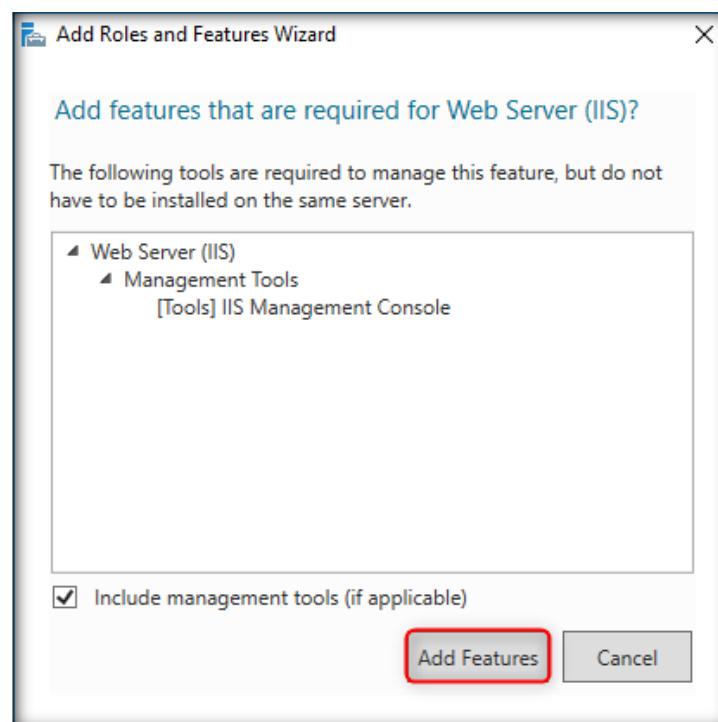
6. In **Server Selection** section, leave the selections to default and click **Next**



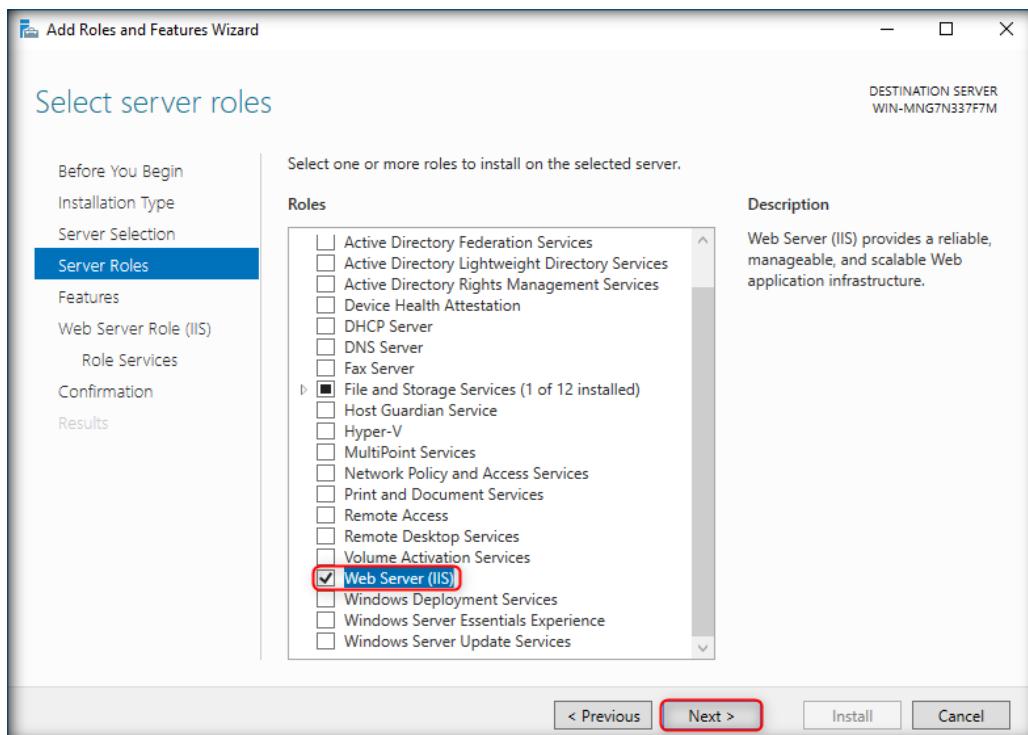
7. **Server Roles** section appears, click the check box of **Web Server (IIS)** role



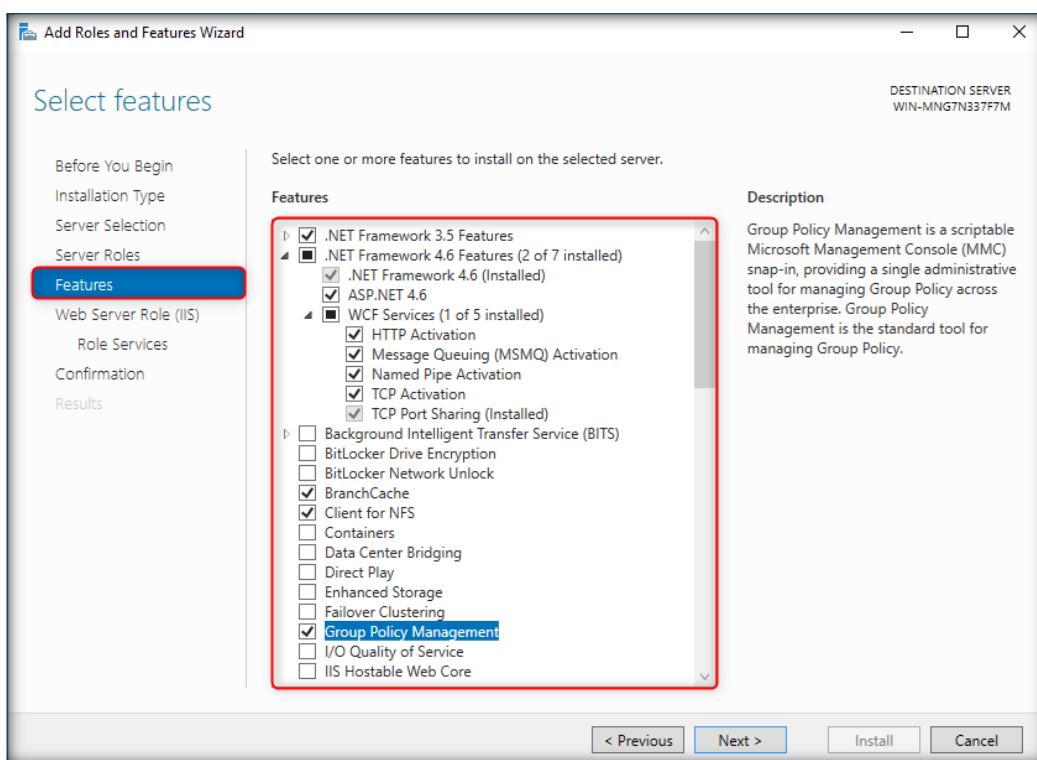
8. **Add Roles and Features wizard** window appears, click **Add Features**



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

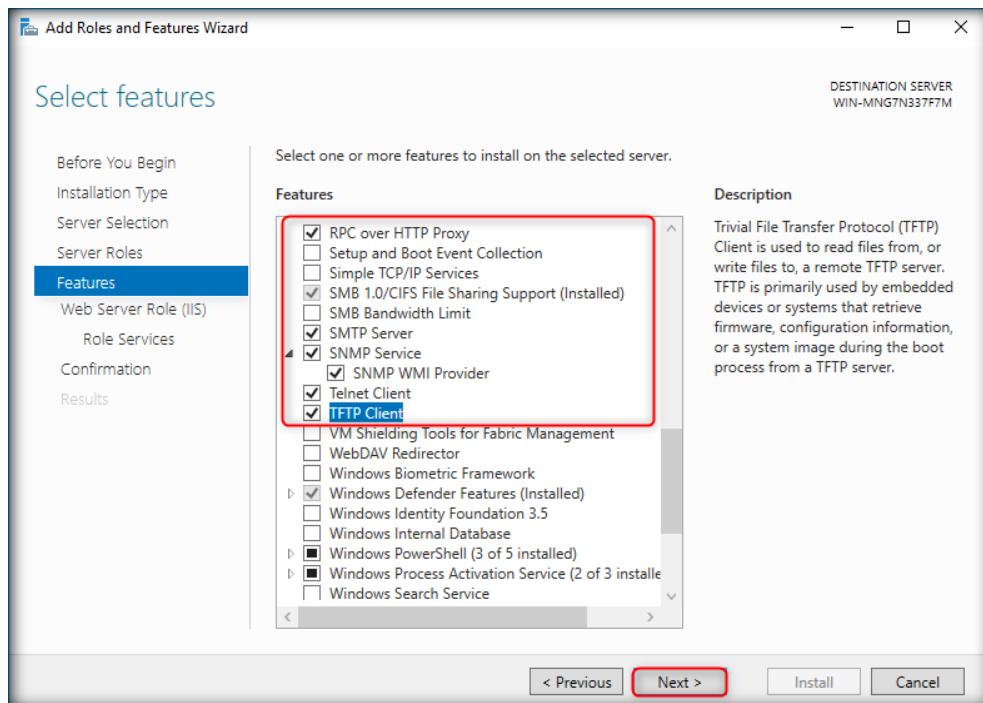


10. **Features** section appears, select the checkboxes for **.NET Framework 3.5, Branch Cache, Client for NFS** and **Group Policy Management** Features, as well as all the checkboxes under **.NET Framework 4.6 Features**



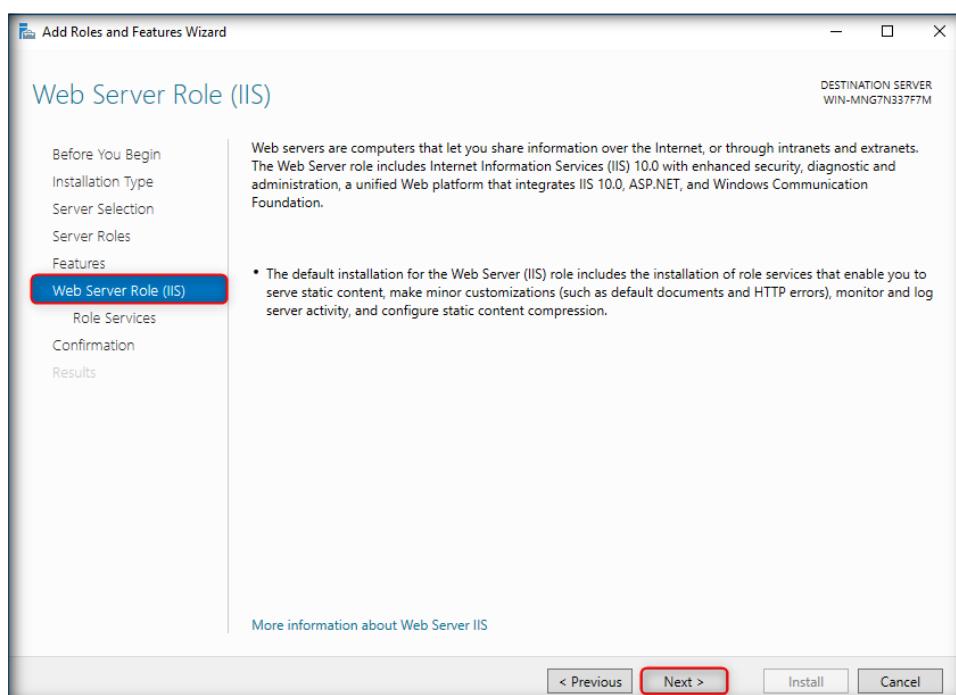
11. Scroll down the section and check **RPC over HTTP Proxy, SMTP Server, SNMP WMI Provider** under **SNMP Service** feature, **Telnet Client** and **TFTP Client** roles. Click **Add Features** button if you get a prompt for the features to be added while selecting few of the features.

12. Click **Next**



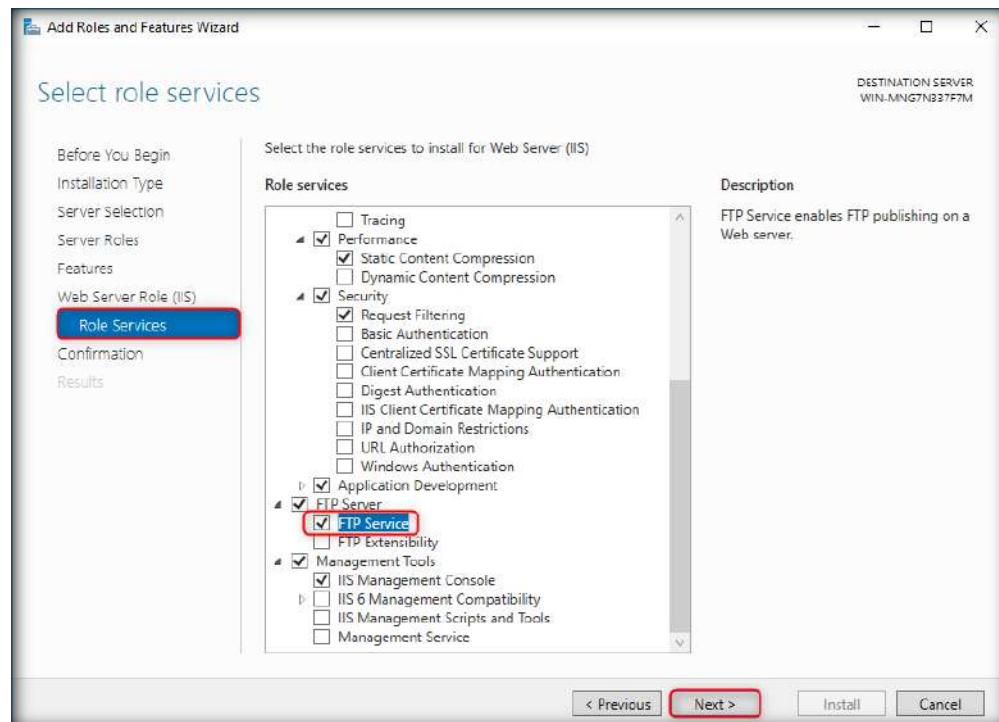
13. Click **Add Features** button if you get a prompt for the features to be added, while selecting any features. Click **Next**.

14. **Web Server Role (IIS)** section appears in the wizard, click **Next**.

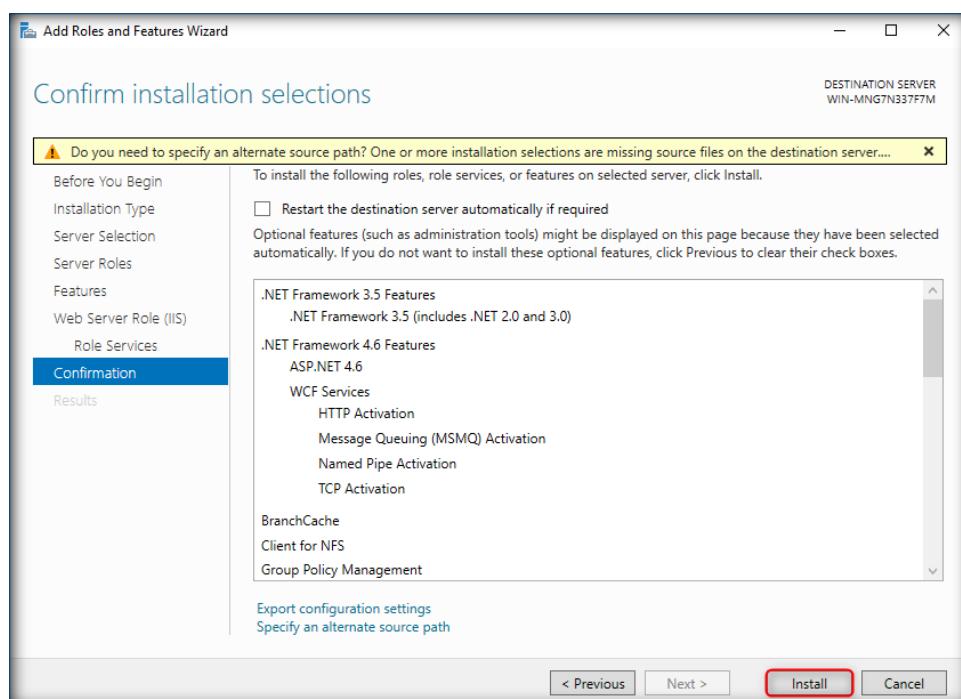


15. **Role Services** section appears in the wizard. Scroll down the Role services and check **FTP Service** under **FTP Server** role.

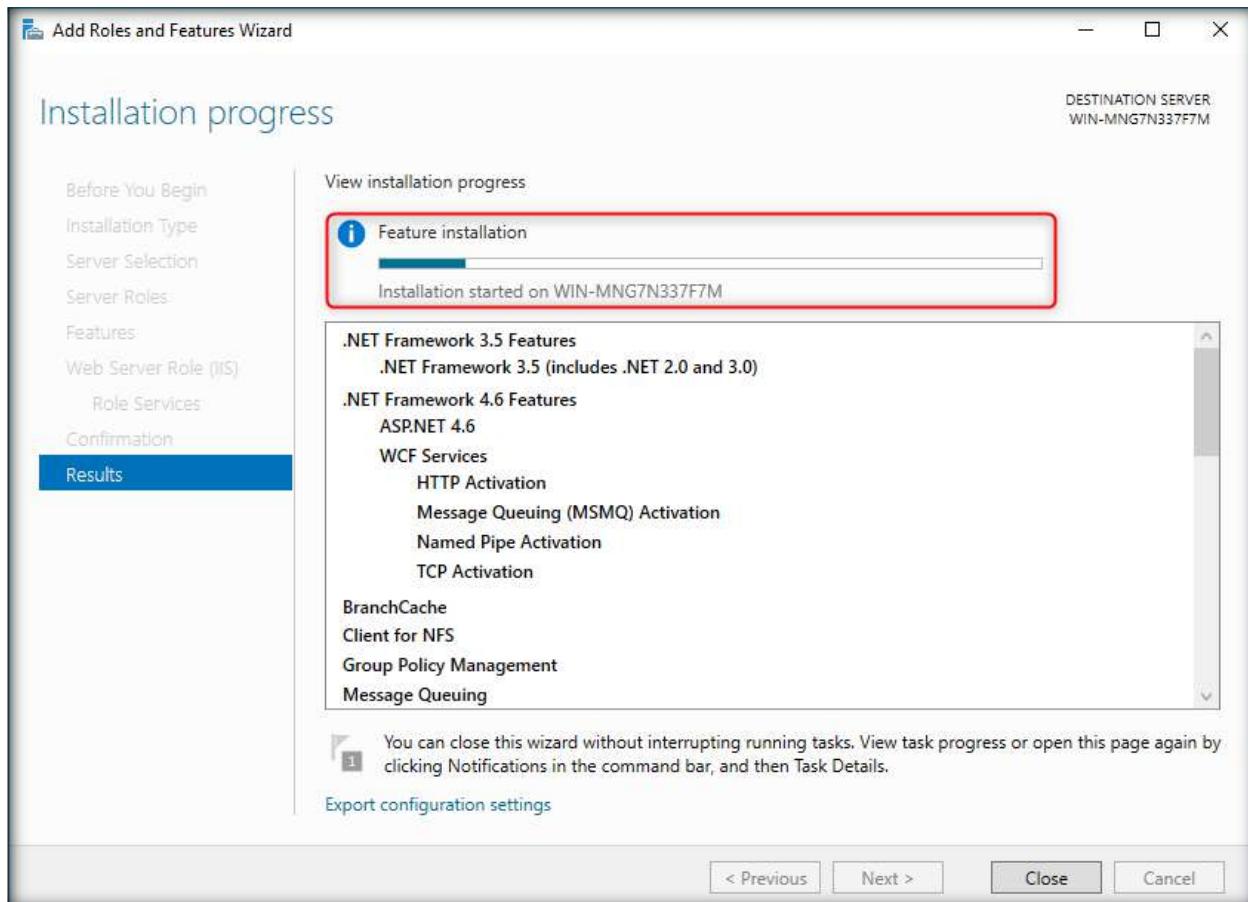
16. Click **Next**



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

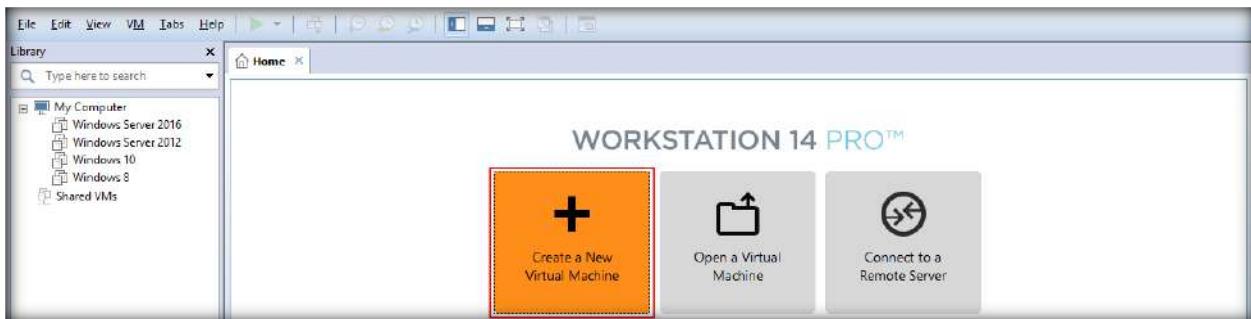


19. After the completion of installation, click **Close** button and restart the machine
20. Similarly install all the above roles and services in the Windows Server 2012 machine
21. After installing all the services Windows Server 2012. Stop the **World Wide Web Publishing Service** and **IIS Admin 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

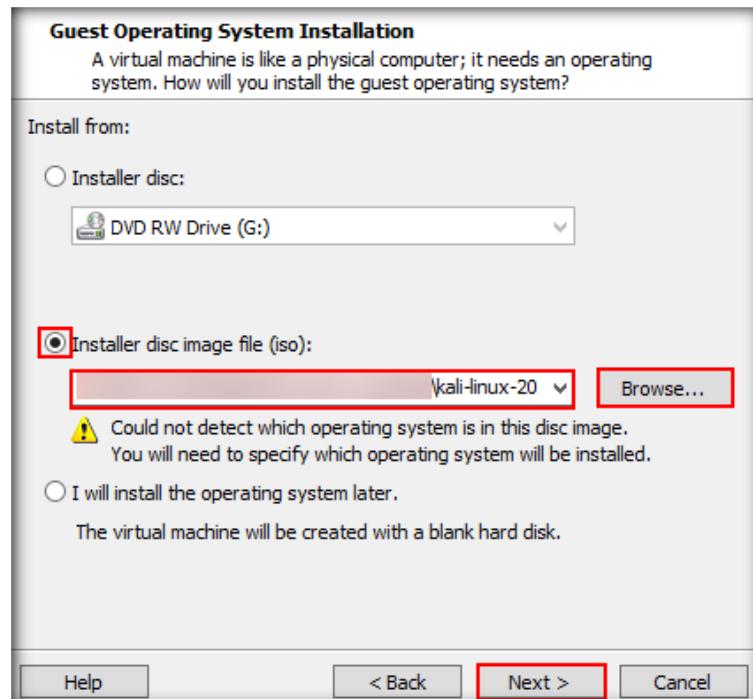
1. In VMware Workstation window, click **Create a New Virtual Machine**



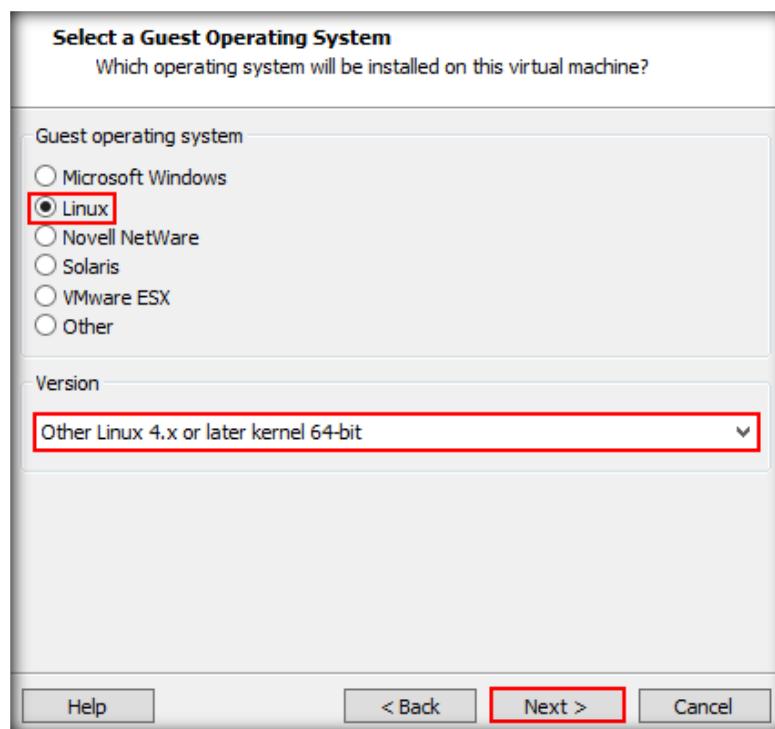
2. In the New Virtual Machine wizard, leave the settings to default and click **Next**



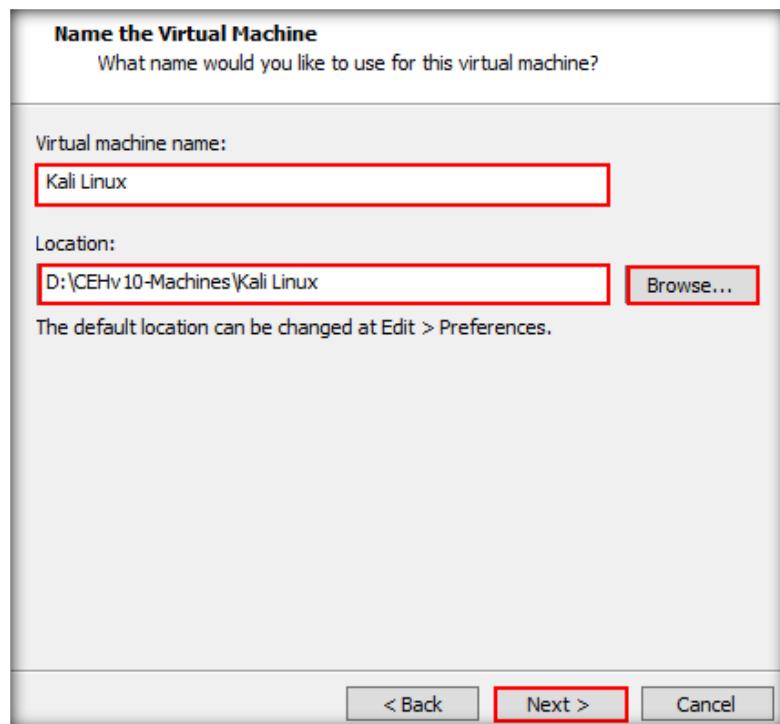
3. In Guest Operating System Installation wizard, choose **Installer disc image file (iso)**: radio button. Click **Browse** and navigate to D:\CEH-Tools\CEHv10 Lab Prerequisites\ISO's\Kali Linux and select **kali-linux-2017.3-amd64.iso** to provide the ISO path and click **Next**



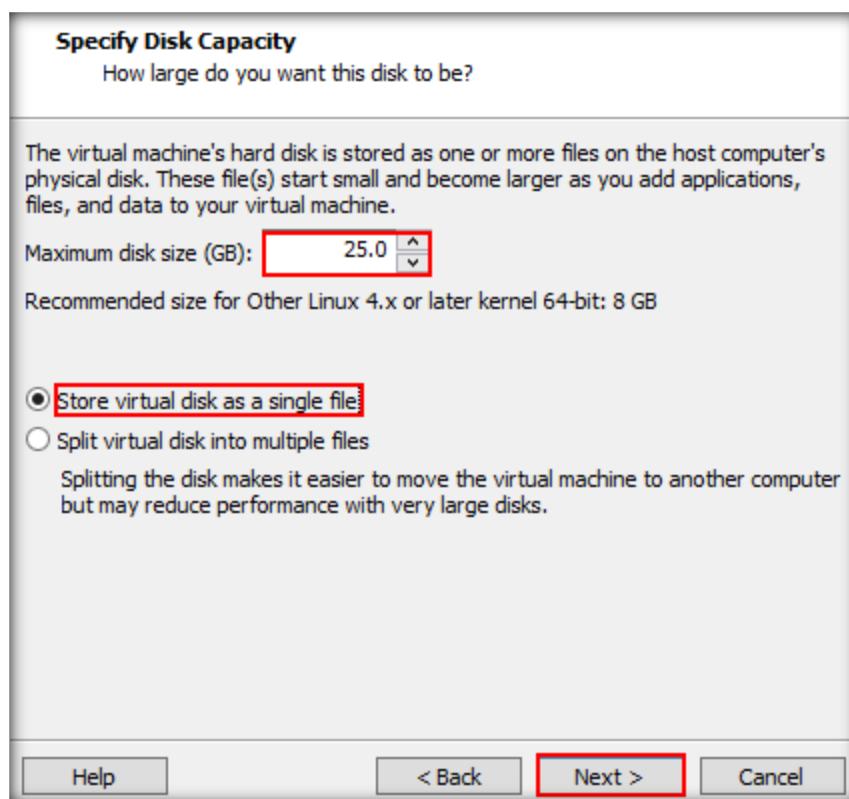
4. Select a Guest Operating System wizard appears, choose **Linux** radio button under Guest operating system type and select **Other Linux 4.x or later kernel 64-bit** in the Version drop down and click **Next** as shown in the screenshot



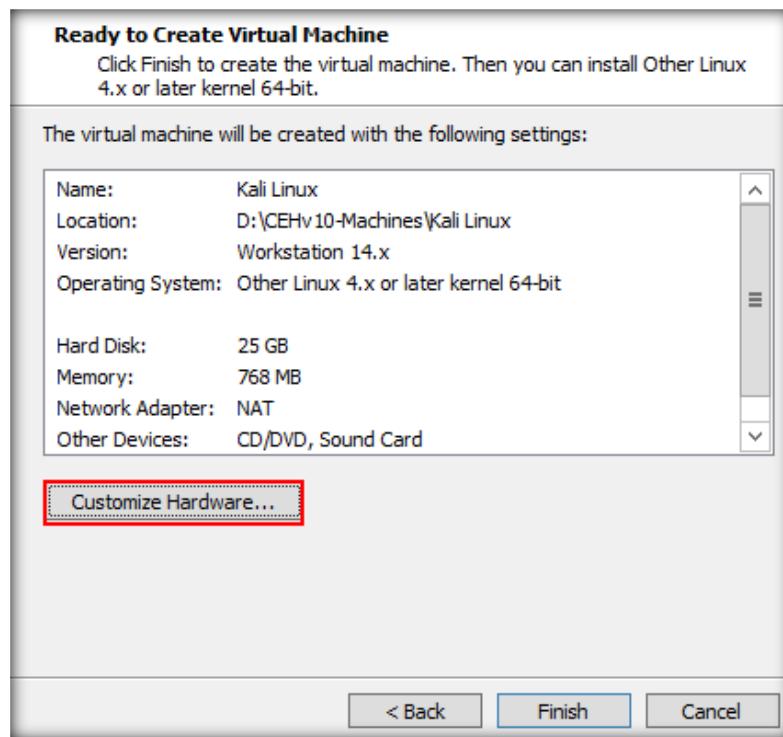
5. Name the Virtual Machine wizard appears, type **Kali Linux** in the Virtual machine name field, and click **Browse** button to store the virtual hard disk and click **Next**



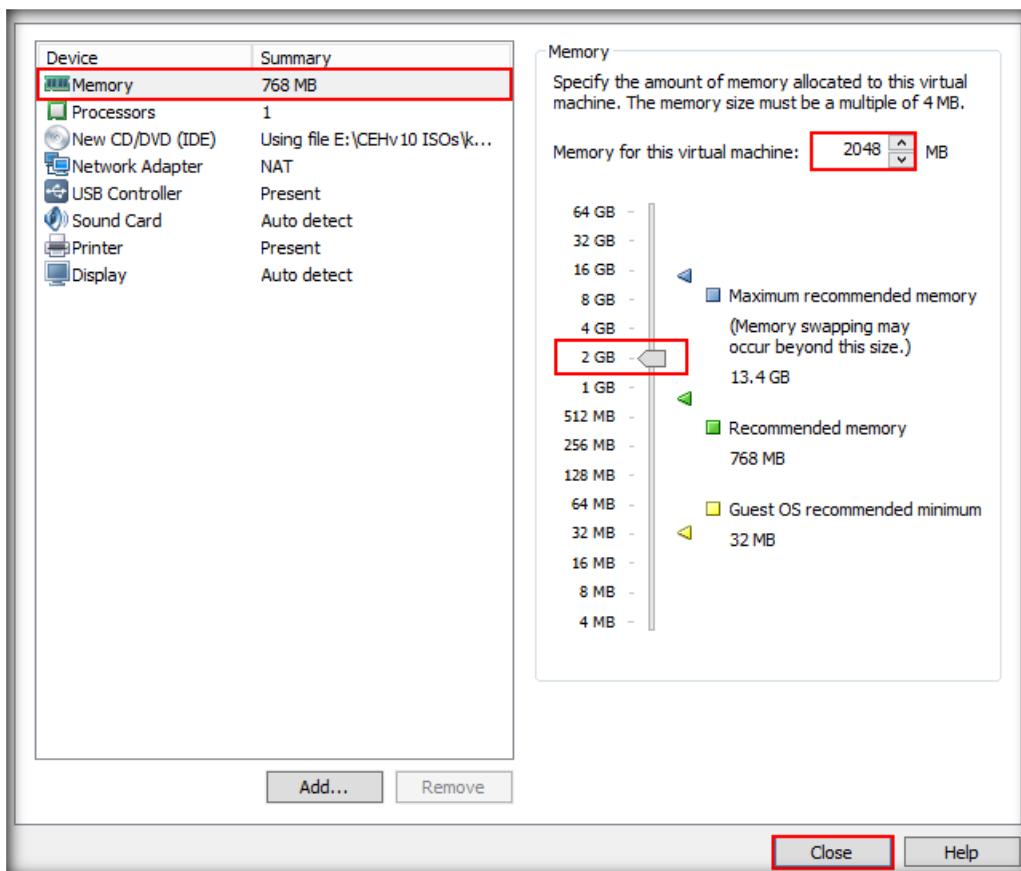
6. Specify Disk Capacity wizard appears, type **25.0 GB** in the Maximum disk size, and choose **Store virtual disk as a single disk** radio button and click **Next**



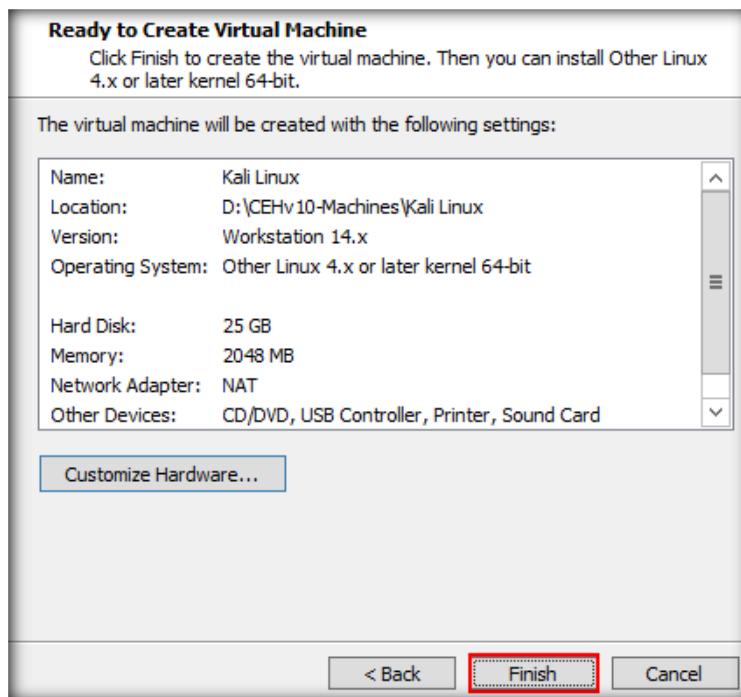
7. Click **Customize Hardware** button in the Ready to Create Virtual Machine wizard



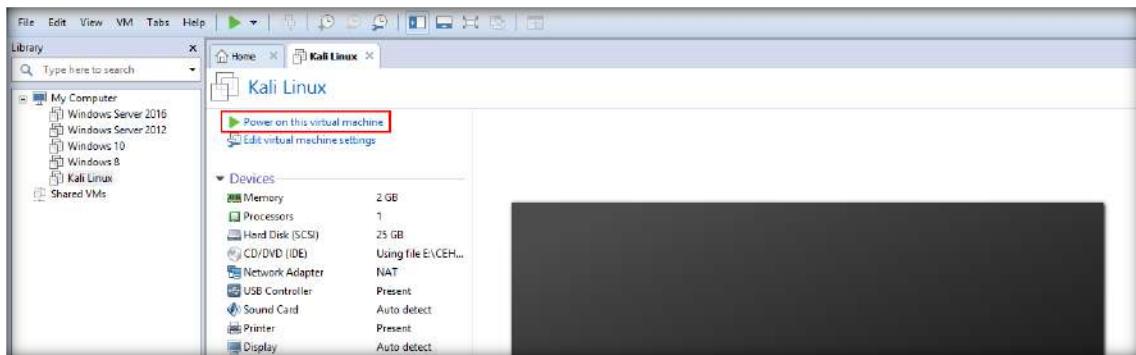
8. Hardware window appears, toggle the memory option to **2 GB** and click **Close**



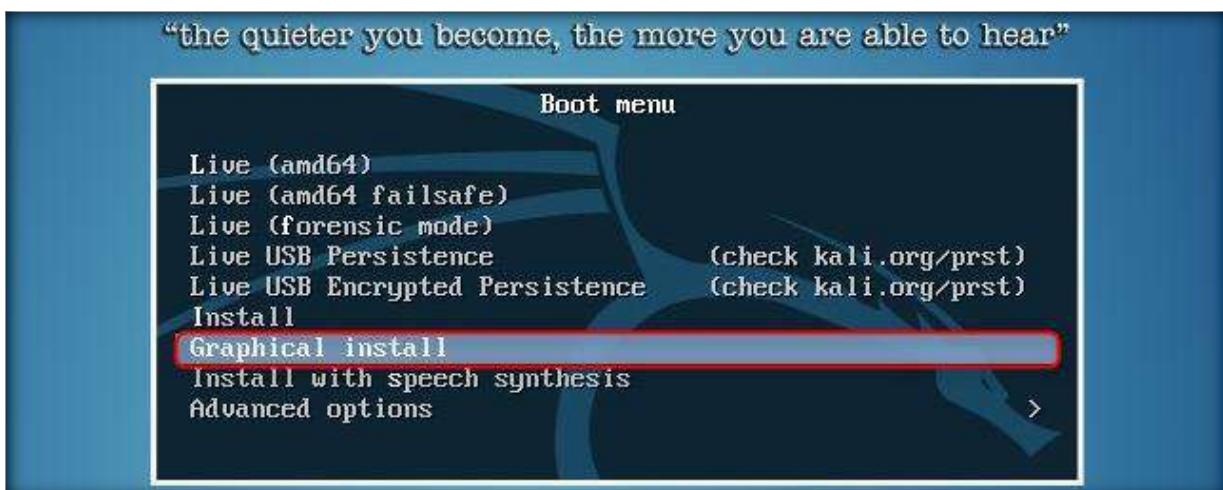
9. Click **Finish** in the Ready to Create Virtual Machine wizard



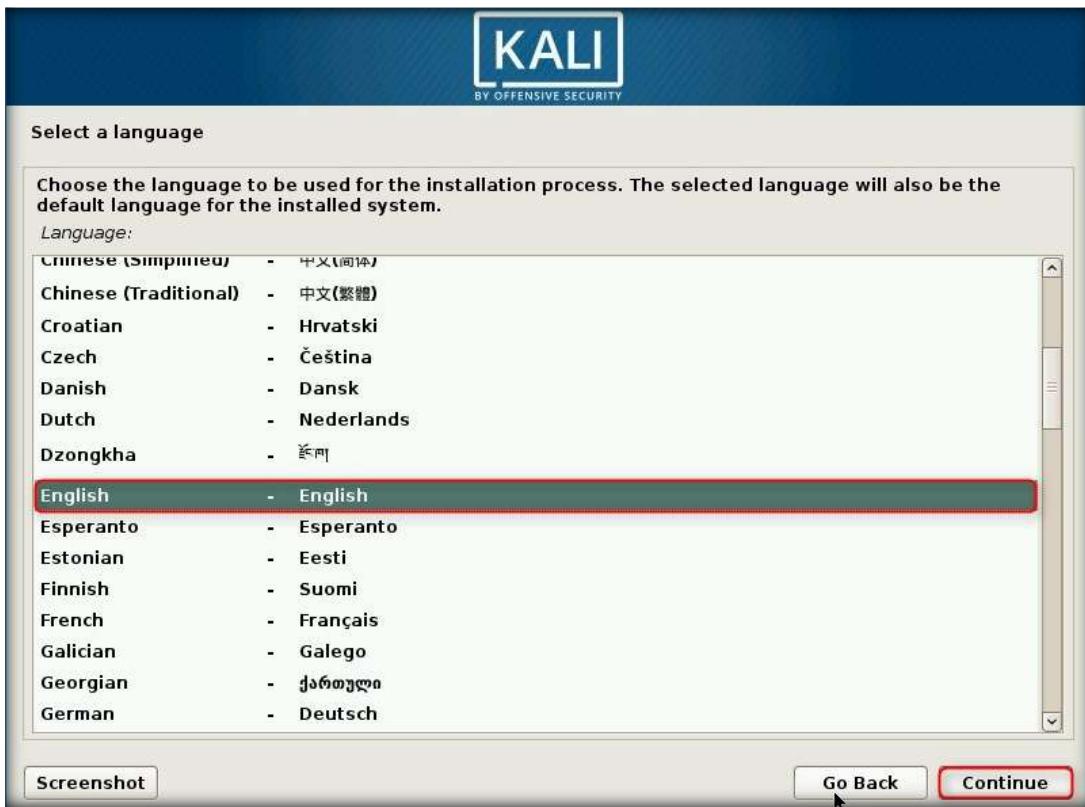
10. Click **Power on this virtual machine** link in the Kali Linux tab as shown in the screenshot



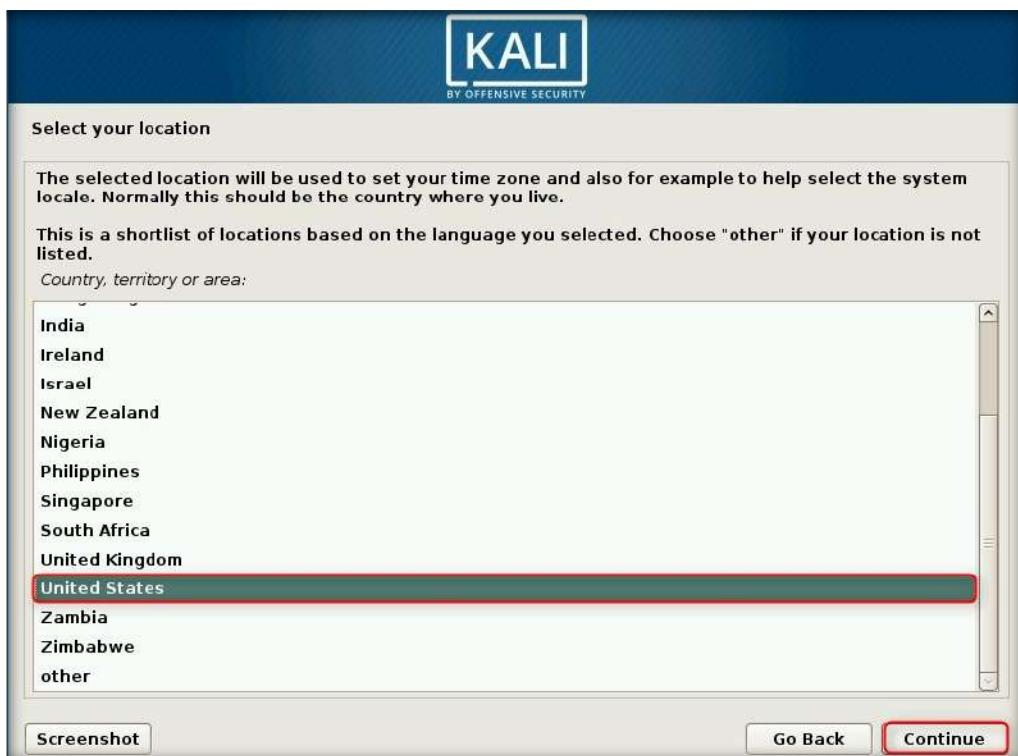
11. Kali Linux **Boot menu** appears, select **Graphical install** and press **Enter**



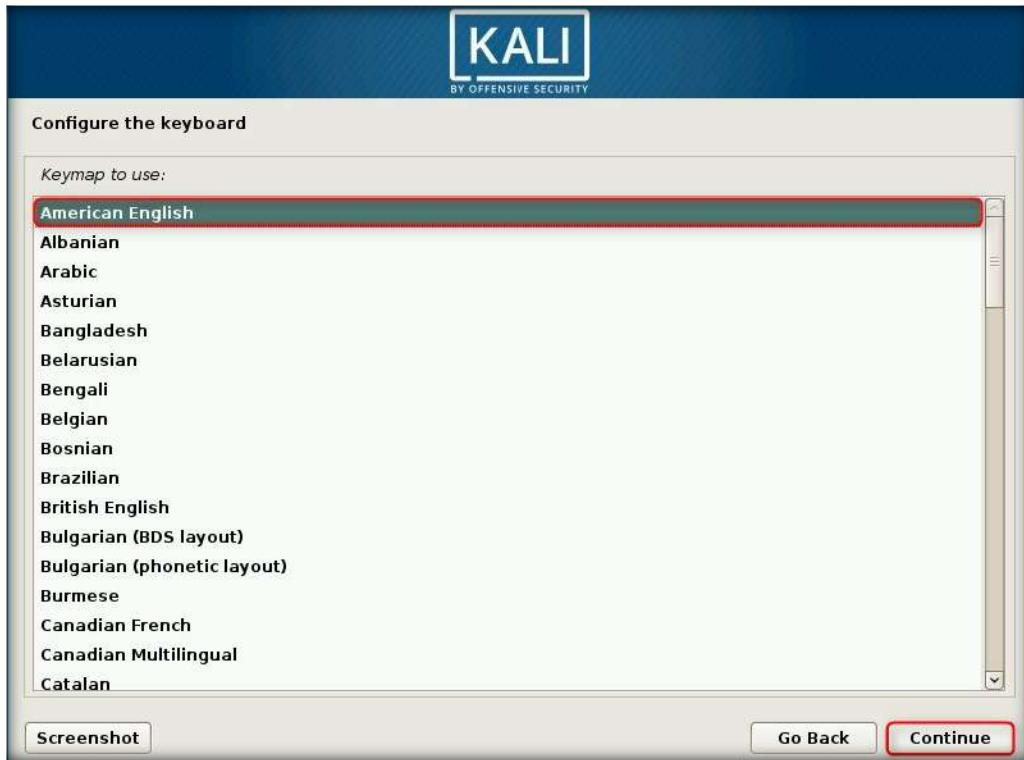
12. **Select a language** window appears, choose a language (here, **English**) and click **Continue**



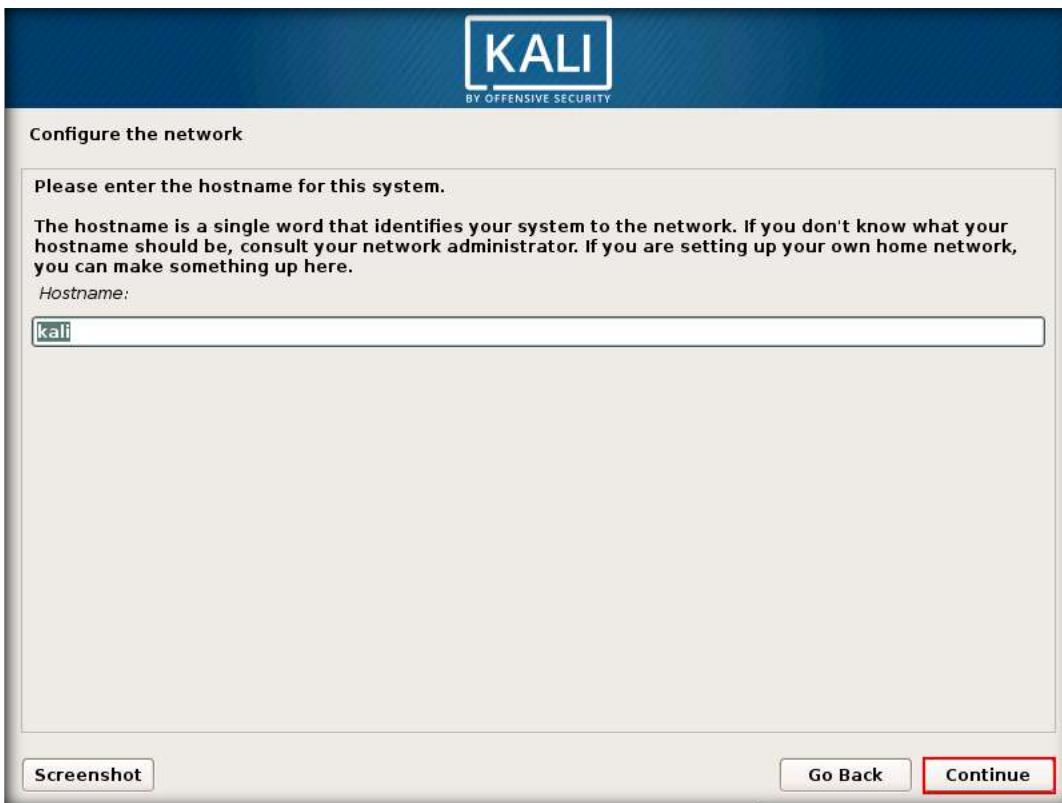
13. In the **Select your location** section, choose a location (here, **United States**) and click **Continue**



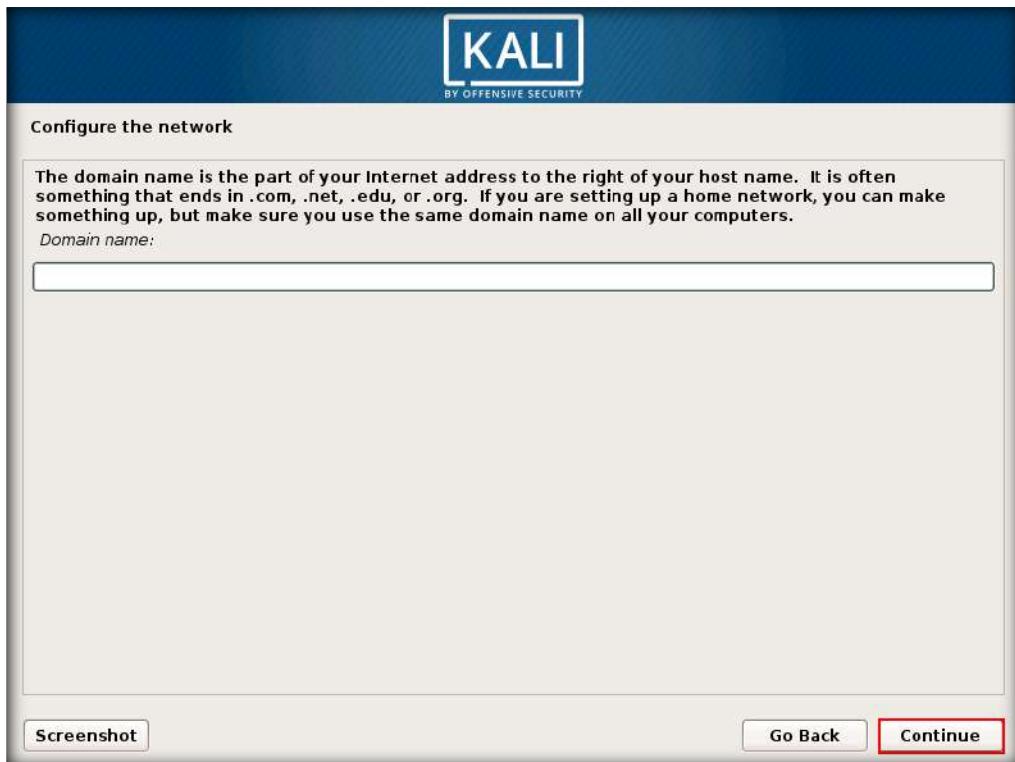
14. **Configure the keyboard** section appears, choose a language (here, **American English**) and click **Continue**



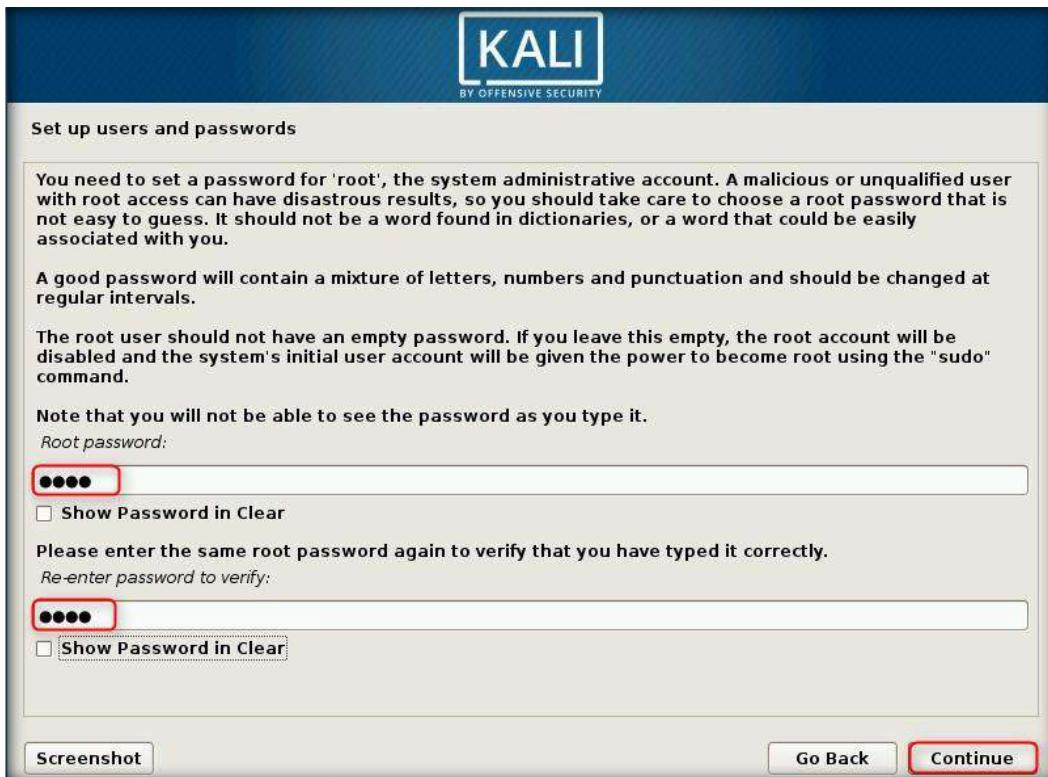
15. **Configure the network** section appears, leave the Hostname to default and click **Continue**



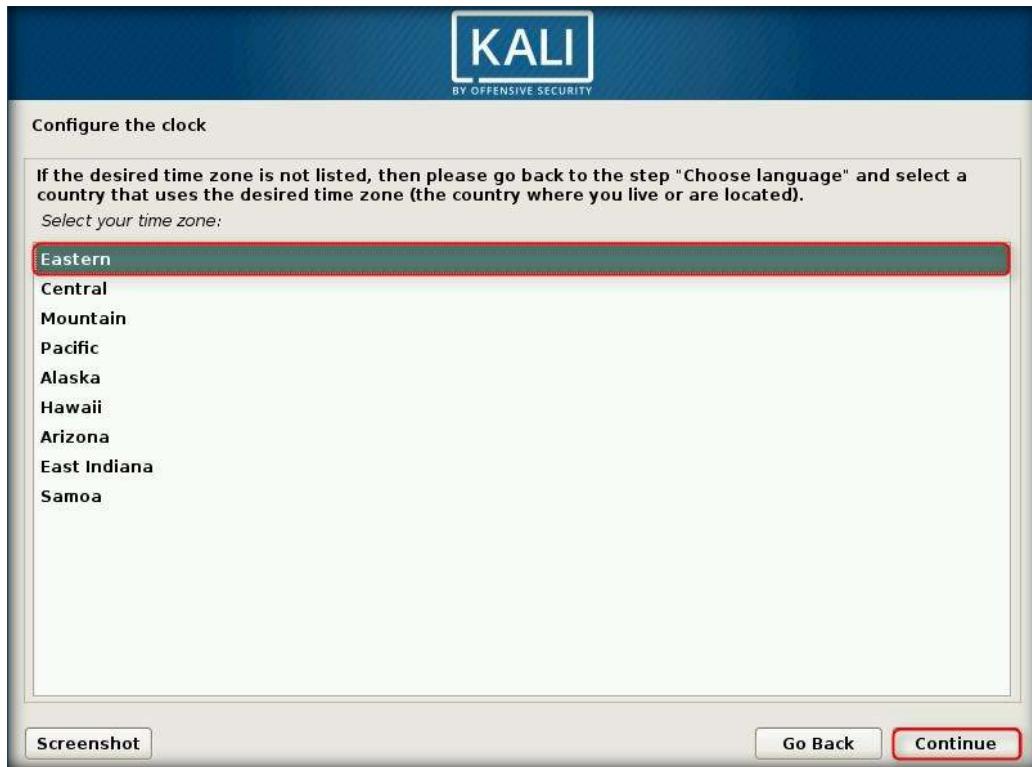
16. **Configure the network** section appears, leave the Domain name: field blank and click **Continue**



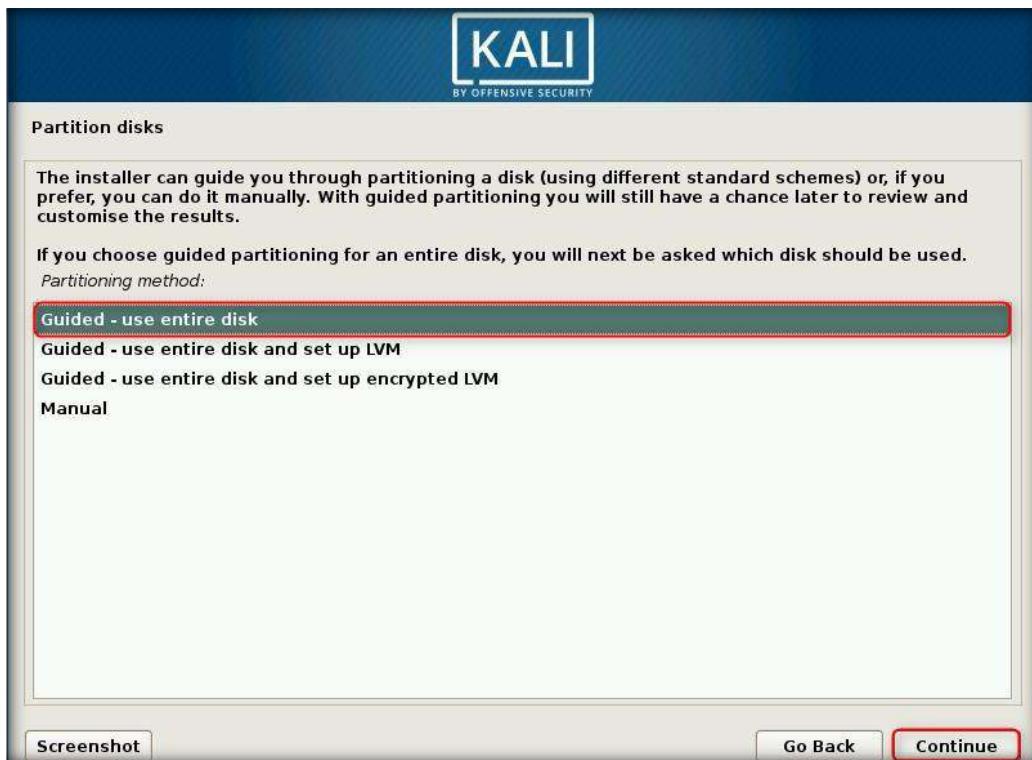
17. **Set up users and passwords** section appears, enter **toor** in both the **Root password** as well as **re-enter password to verify** fields and click **Continue**



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**

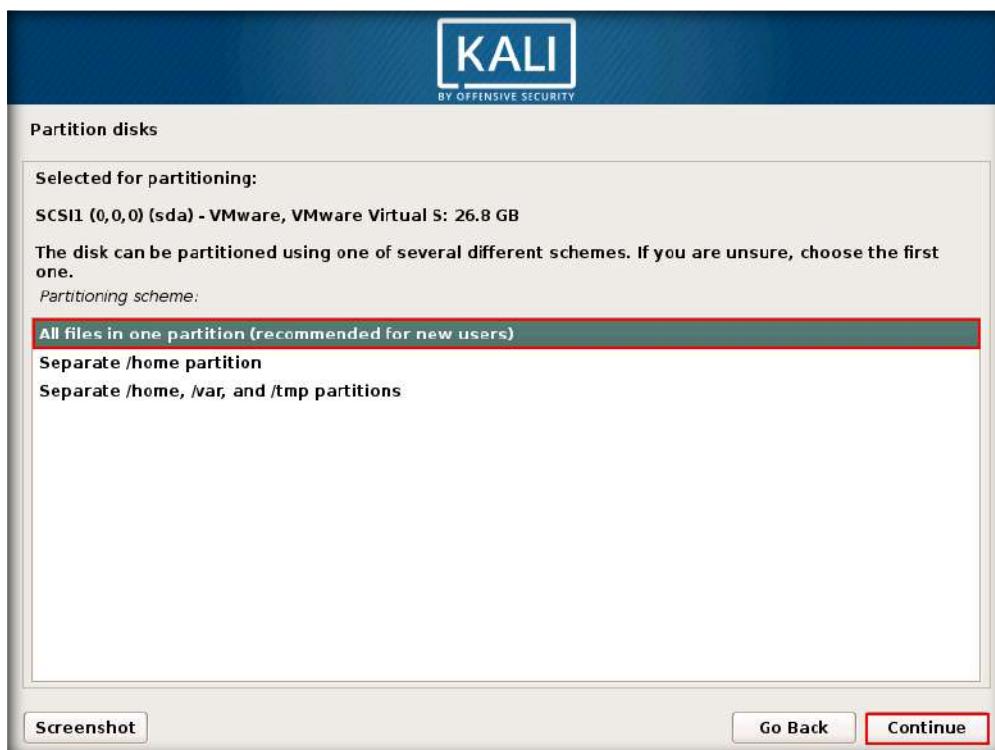


21. Another **Partition disks** window appears, select the disk **SCSI1 (0,0,0) (sda) – 26.8 GB VMware, VMware Virtual S** and click **Continue**

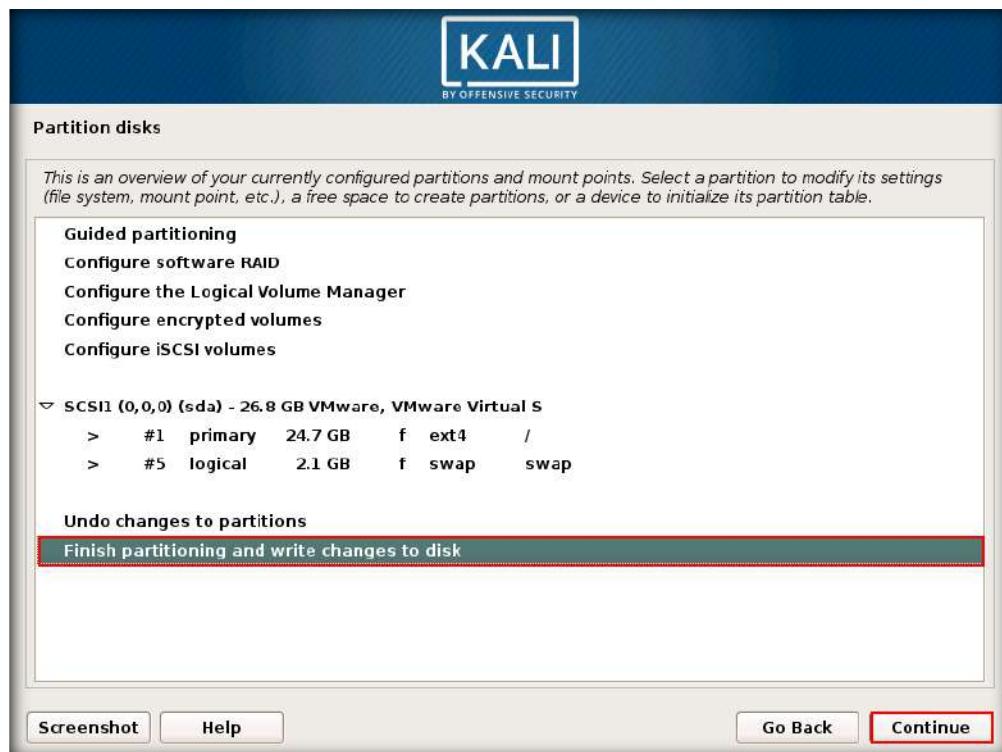
Note: The size of the disk (**26.8 GB**) may vary in your lab environment



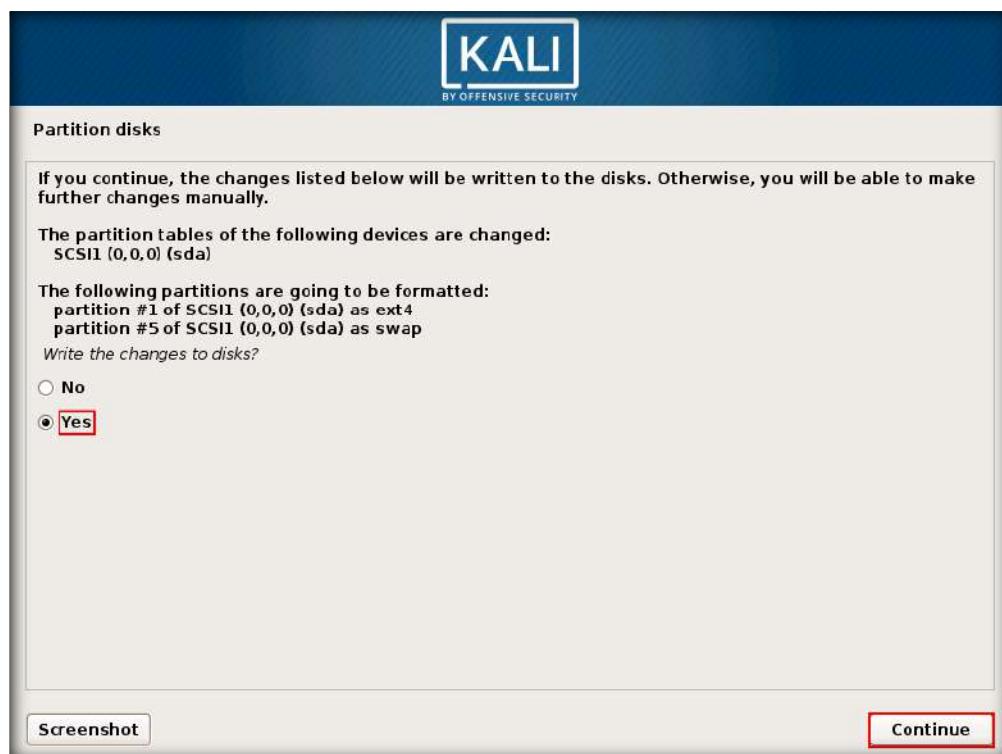
22. In the **Partition disks** window, choose the Partitioning scheme: **All files in one partition (recommended for new users)** and click **Continue**



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

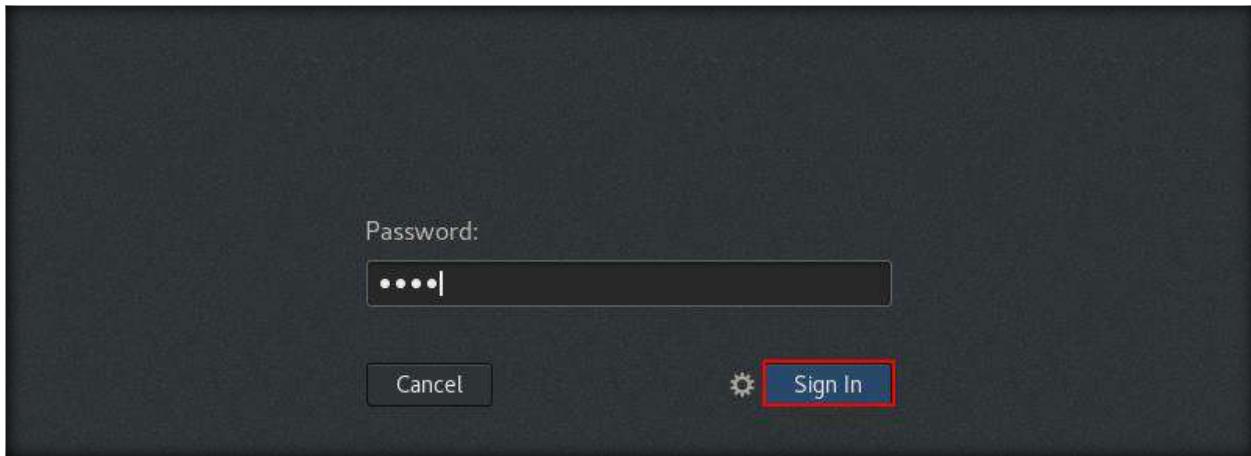


29. Wait until the partitions are formatted and the operating system is installed

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**



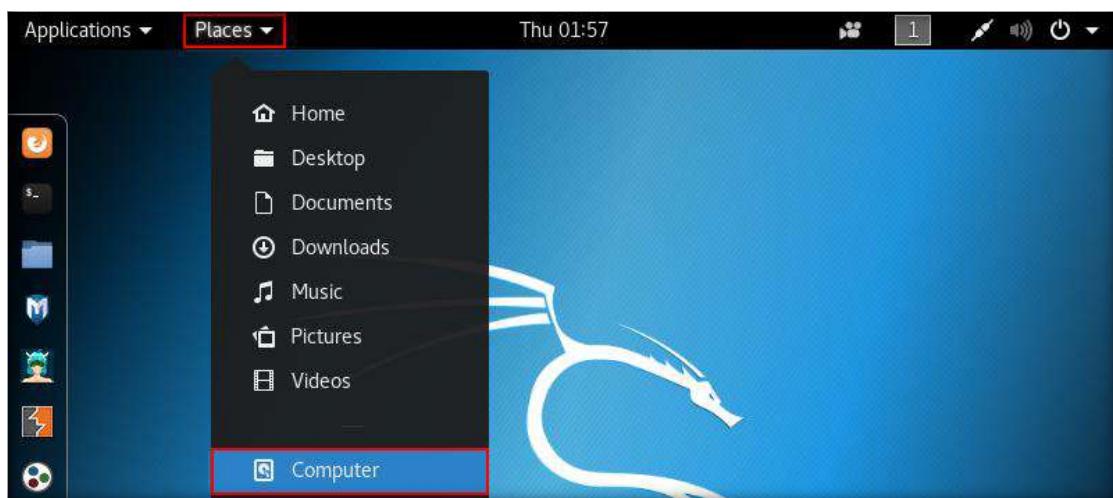
32. Click **Terminal** icon from the left-hand side of the **Favorites** bar, and type **ifconfig** and press **Enter** to check with the network adapter, here it is **eth0** (it might differ in your lab environment). Close the terminal window after making a note of the adapter

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.5  netmask 255.255.255.0  broadcast 10.10.10.255
              inet6 fe80::20c:29ff:fe4:aa89  prefixlen 64  scopeid 0x20<link>
                ether 00:0c:29:f4:aa:89  txqueuelen 1000  (Ethernet)
                  RX packets 75  bytes 11175 (10.9 KiB)
                  RX errors 0  dropped 0  overruns 0  frame 0
                  TX packets 52  bytes 4619 (4.5 KiB)
                  TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
              inet6 ::1  prefixlen 128  scopeid 0x10<host>
```

A terminal window titled 'root@kali: ~'. The command 'ifconfig' is run, displaying network interface information. The 'eth0' interface is shown with an IP of 10.10.10.5 and a MAC address of 00:0c:29:f4:aa:89. The 'lo' interface is shown with an IP of 127.0.0.1. The terminal window has a red box around the command 'ifconfig' and another red box around the 'eth0' interface information.

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**

```

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces/*

# The loopback network interface
auto lo
iface lo inet loopback

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

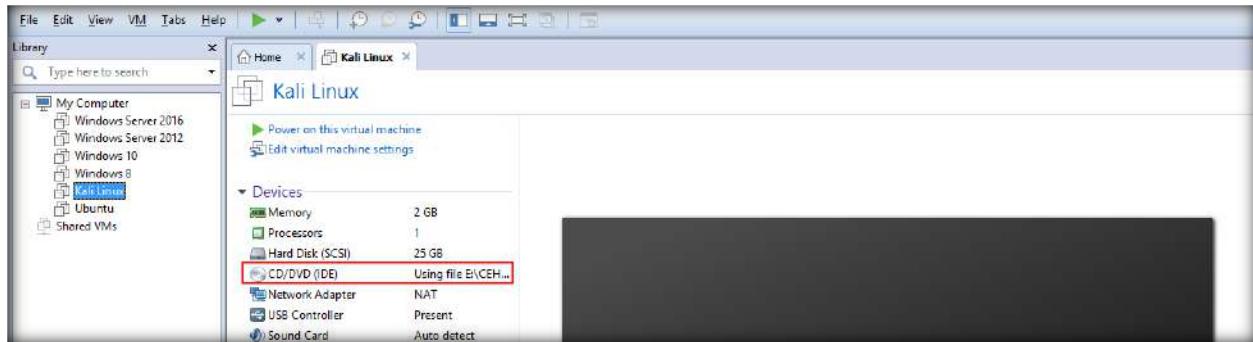
37. Once the machine is restarted, login to the machine and open a **terminal** from the **Favorites** bar and type **ifconfig** and press **Enter** to verify the IP configuration. Close the terminal window and shutdown the machine

```

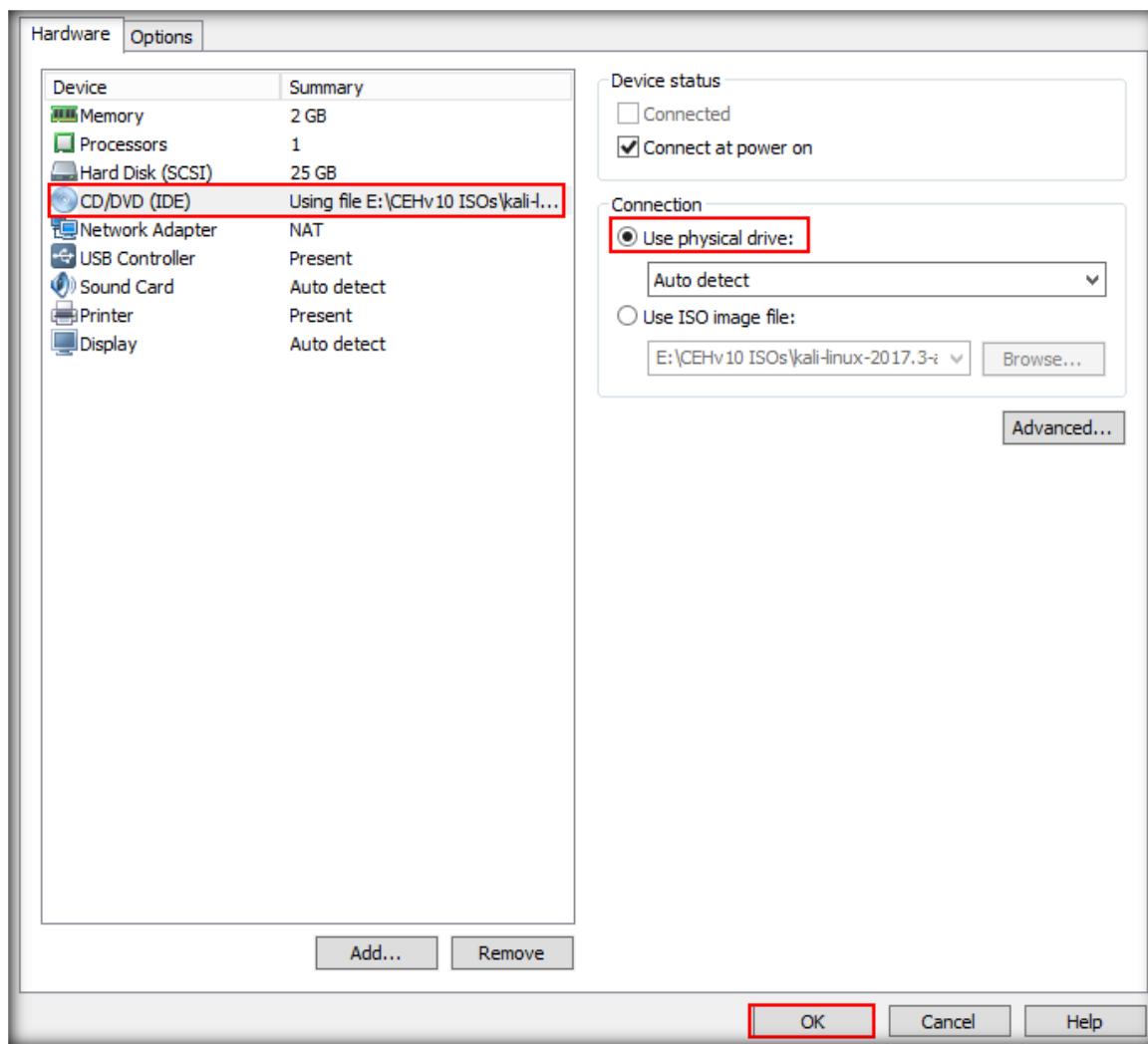
root@kali:~#
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 10.10.10.11 netmask 255.255.255.0 broadcast 10.10.10.255
              inet6 fe80::20c:29ff:fe00:aa89 prefixlen 64 scopeid 0x20<link>
                ether 00:0c:29:f4:aa:89 txqueuelen 1000 (Ethernet)
                  RX packets 12 bytes 1603 (1.5 KiB)
                  RX errors 0 dropped 0 overruns 0 frame 0
                  TX packets 28 bytes 2074 (2.0 KiB)
                  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

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



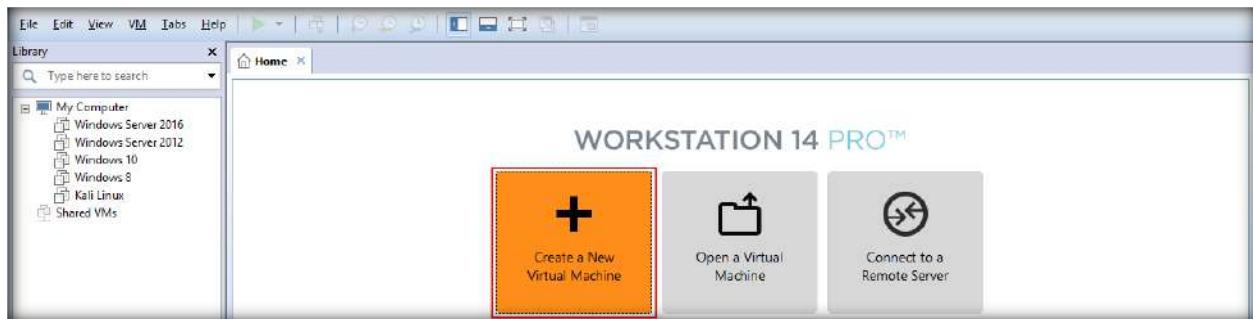
39. Virtual Machine Settings window appears, choose **Use physical drive:** radio button under Connection section and click **OK**



[\[Back to Configuration Task Outline\]](#)

CT#8: Install Ubuntu in VMware

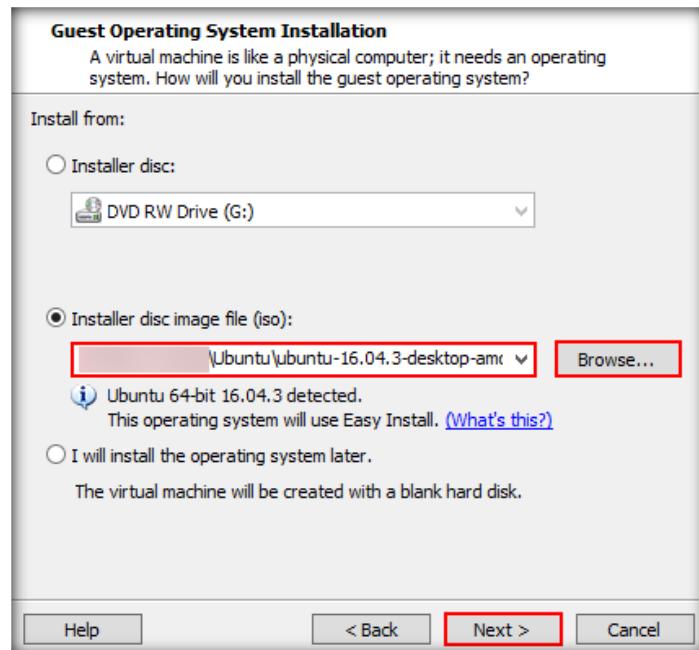
1. In VMware Workstation window, click **Create a New Virtual Machine**



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

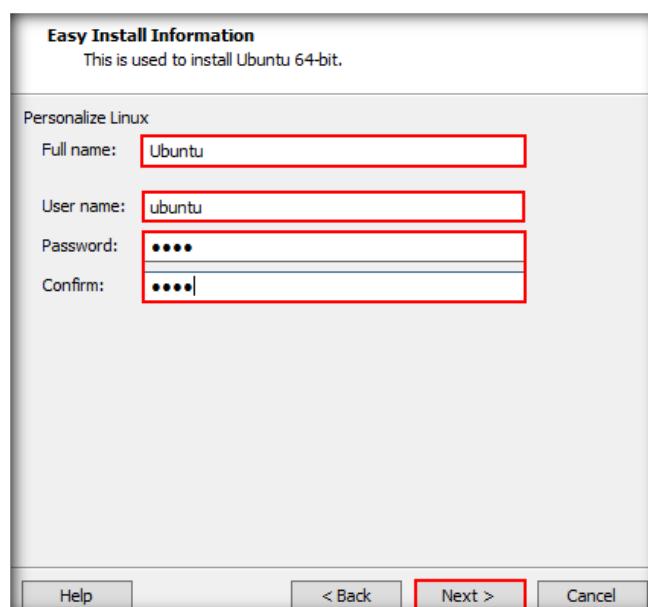


3. In Guest Operating System Installation wizard, choose **Installer disc image file (iso)**: radio button. Click **Browse** and navigate to D:\CEH-Tools\CEHv10 Lab Prerequisites\ISO's\Ubuntu and select **ubuntu-16.04.3-desktop-amd64.iso** to provide the ISO path and click **Next**

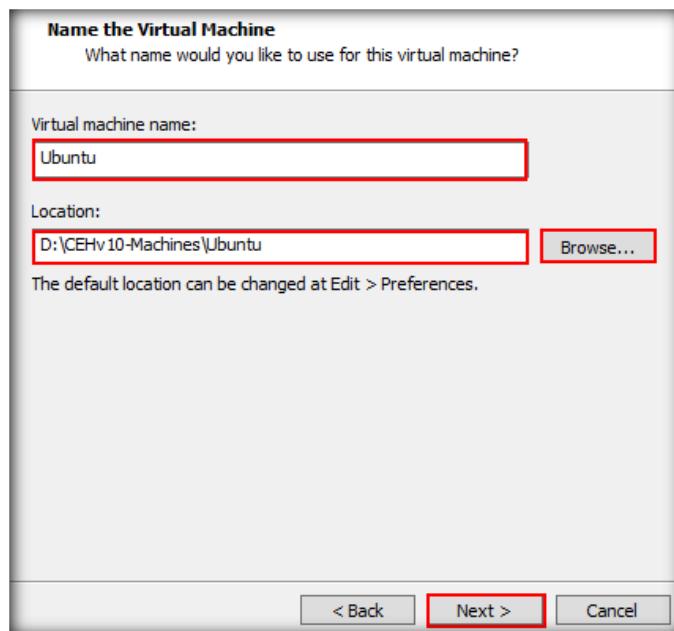


4. Easy Install Information wizard appears, type the following information in the Personalize Linux section and click **Next**

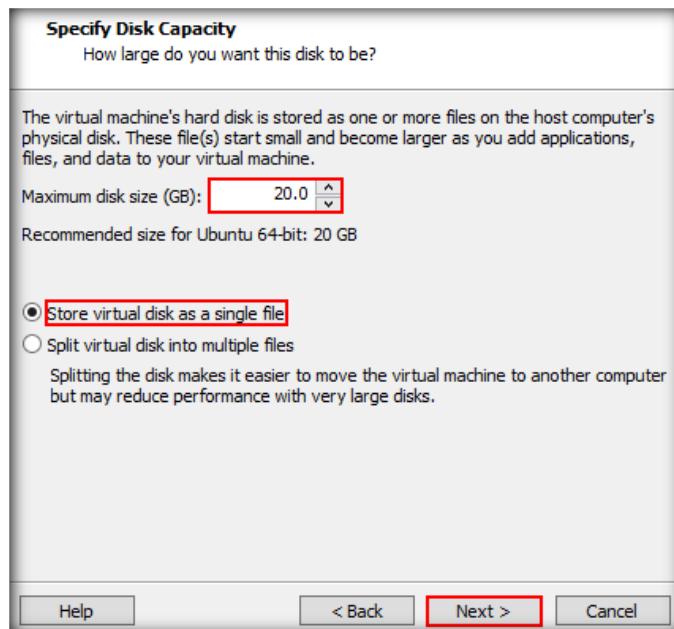
- Full name: **Ubuntu**
- User name: **ubuntu**
- Password: **toor**
- Confirm: **toor**



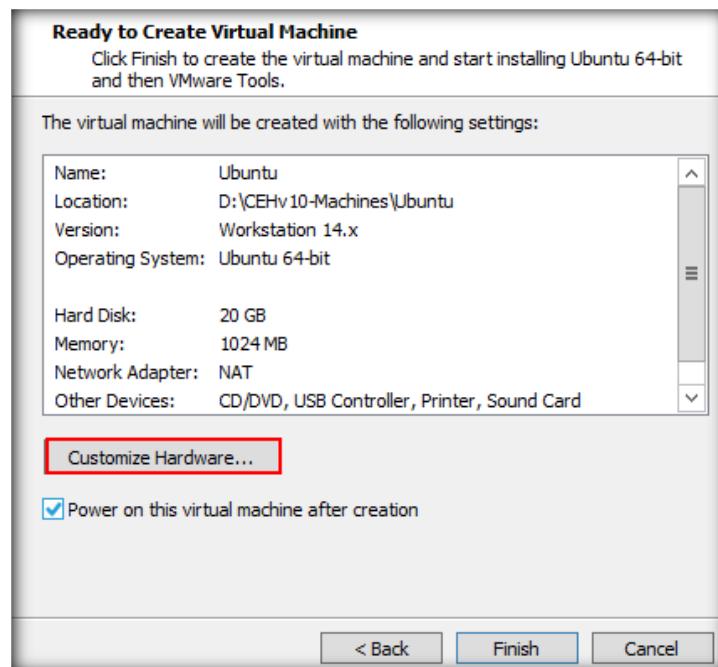
5. Name the Virtual Machine wizard appears, type **Ubuntu** in the Virtual machine name field, and click **Browse** button to store the virtual hard disk and click **Next**



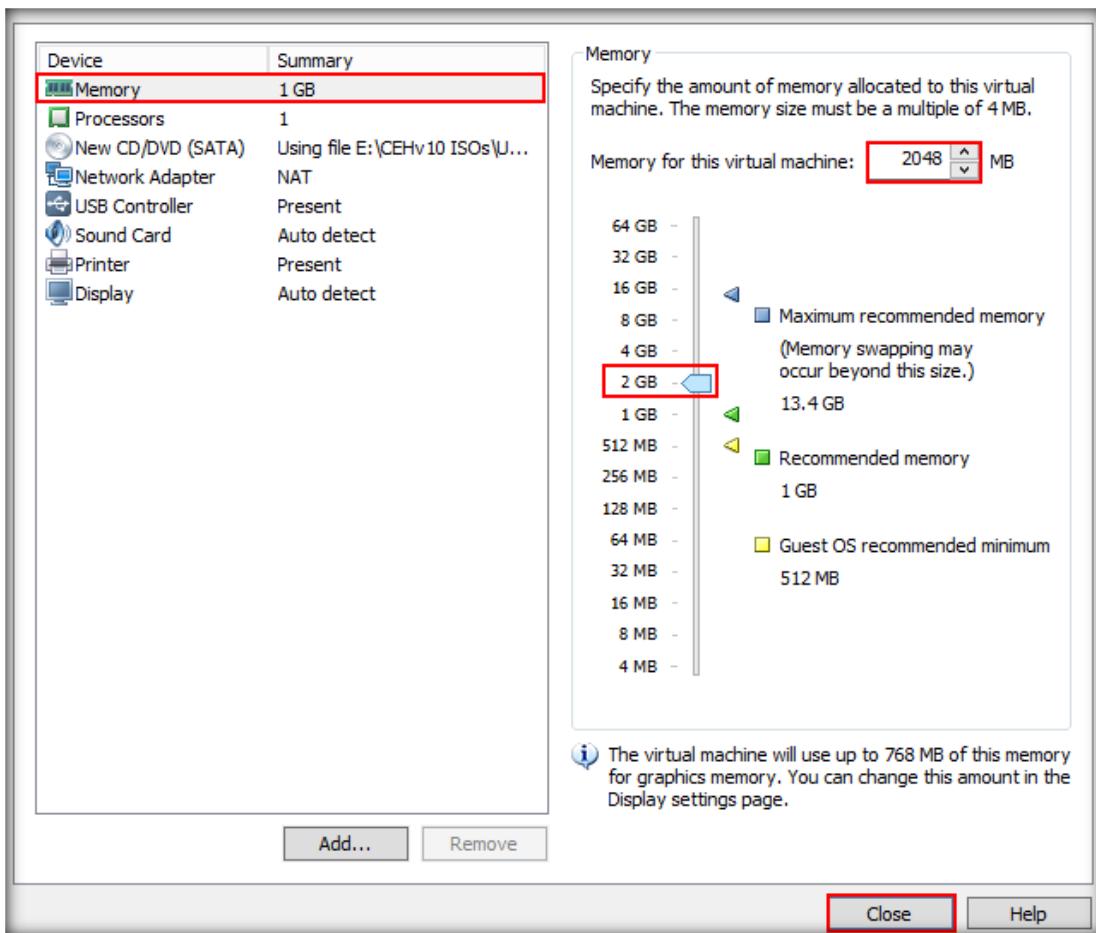
6. Specify Disk Capacity wizard, leave the Maximum disk size as recommended (i.e., **20 GB**) and select **Store virtual disk as a single file** and click **Next**



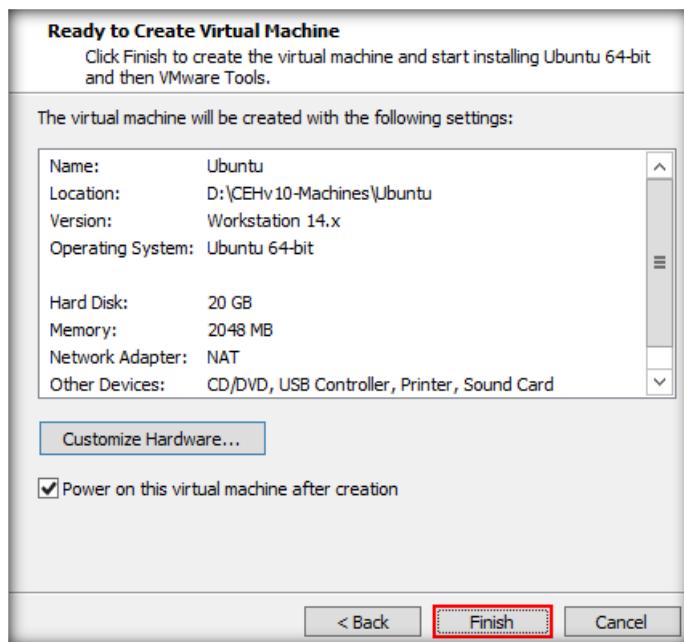
7. Click **Customize Hardware** button in the Ready to Create Virtual Machine wizard



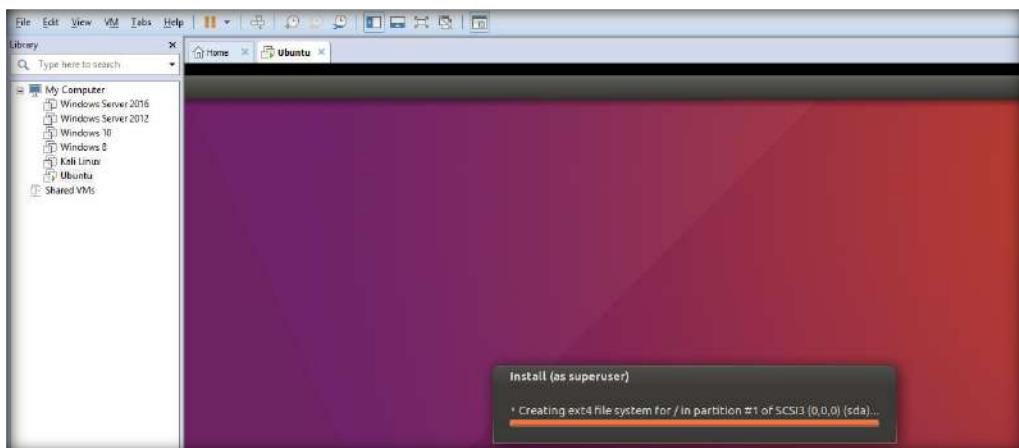
8. Hardware window appears, toggle the memory option to **2 GB** and click **Close**



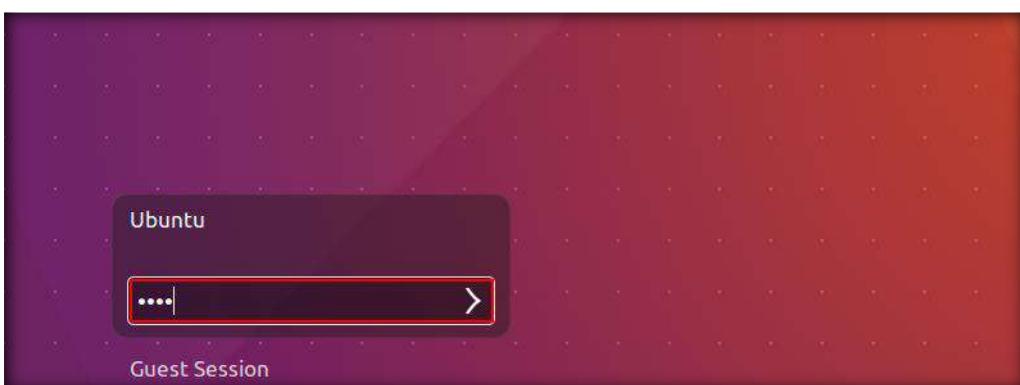
9. Click **Finish** in the Ready to Create Virtual Machine wizard



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



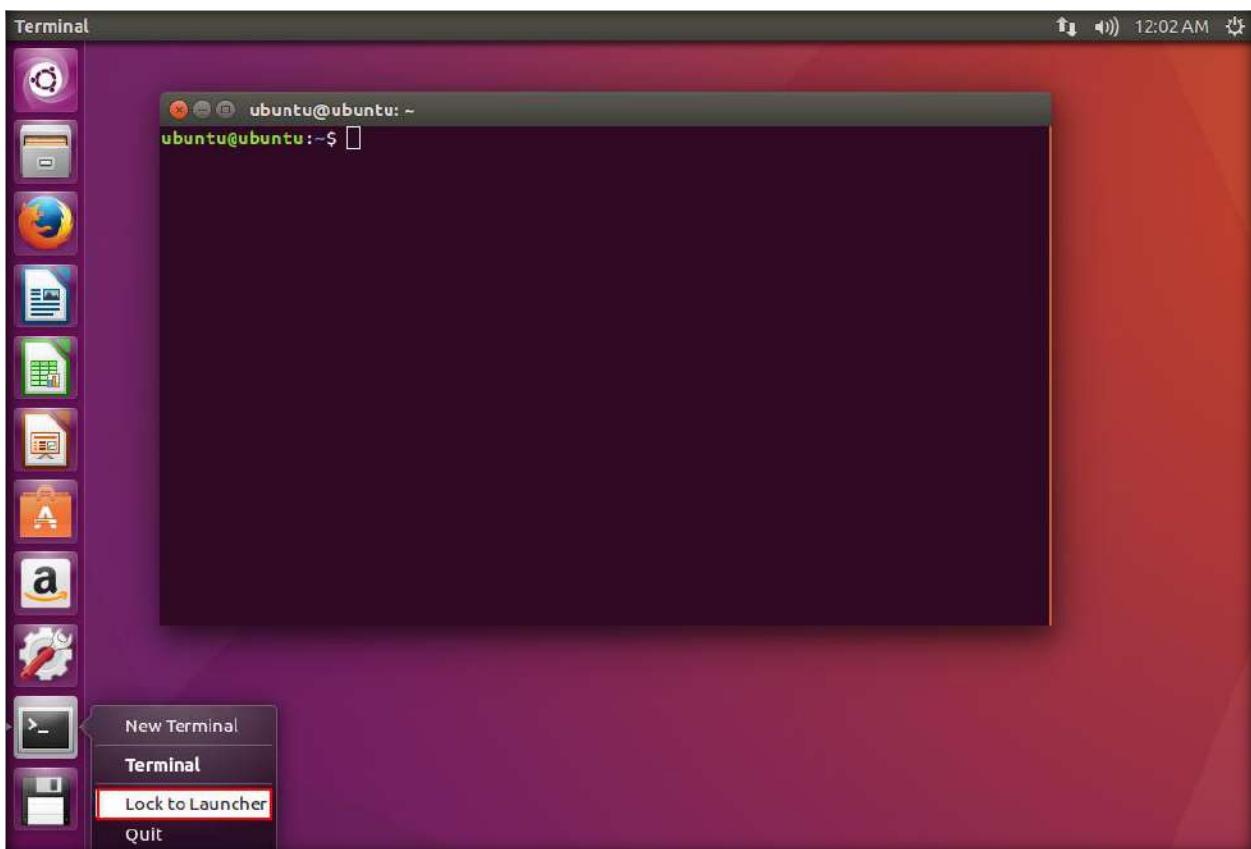
11. Once the installation is finished, the machine will get restarts and provide you with the login screen, with the Username **Ubuntu**. Type **toor** in the Password field and press **Enter**



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

```
ubuntu@ubuntu:~$ ifconfig
ens33      Link encap:Ethernet HWaddr 00:0c:29:27:a1:30
           inet addr:10.10.10.6 Bcast:10.10.10.255 Mask:255.255.255.0
             inet6 addr: fe80::b8f9:1acd:5f82:e615/64 Scope:Link
                   UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                   RX packets:1129 errors:0 dropped:0 overruns:0 frame:0
                   TX packets:711 errors:0 dropped:0 overruns:0 carrier:0
                   collisions:0 txqueuelen:1000
                   RX bytes:1431010 (1.4 MB) TX bytes:52219 (52.2 KB)

lo         Link encap:Local Loopback
           inet addr:127.0.0.1 Mask:255.0.0.0
             inet6 addr: ::1/128 Scope:Host
                   UP LOOPBACK RUNNING MTU:65536 Metric:1
                   RX packets:236 errors:0 dropped:0 overruns:0 frame:0
                   TX packets:236 errors:0 dropped:0 overruns:0 carrier:0
                   collisions:0 txqueuelen:1000
                   RX bytes:19257 (19.2 KB) TX bytes:19257 (19.2 KB)
```

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

```
ubuntu@ubuntu:~$ sudo gedit /etc/network/interfaces
[sudo] password for ubuntu: [REDACTED]
```

16. Interfaces file opens in the text editor, type the following IP configuration details in the text editor and click **Save**

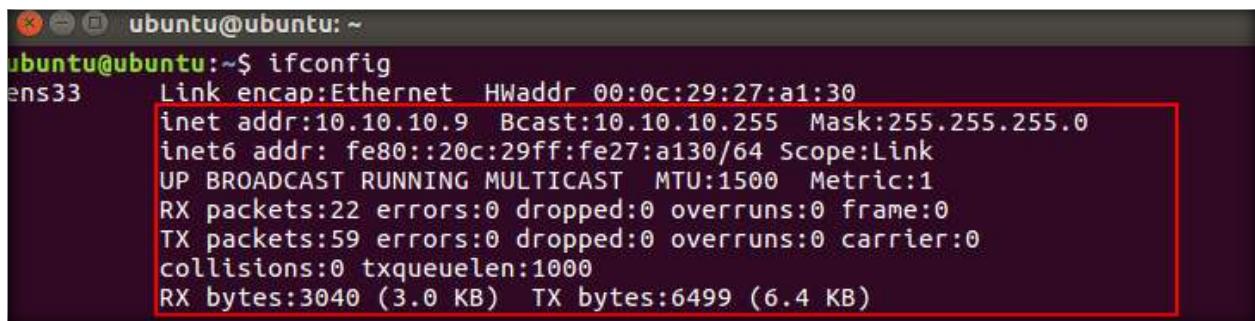
- auto ens33**
- allow-hotplug ens33**
- iface ens33 inet static**
- address 10.10.10.9**
- netmask 255.255.255.0**
- gateway 10.10.10.2**
- dns-nameservers 8.8.8.8 8.8.4.4**

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

```
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

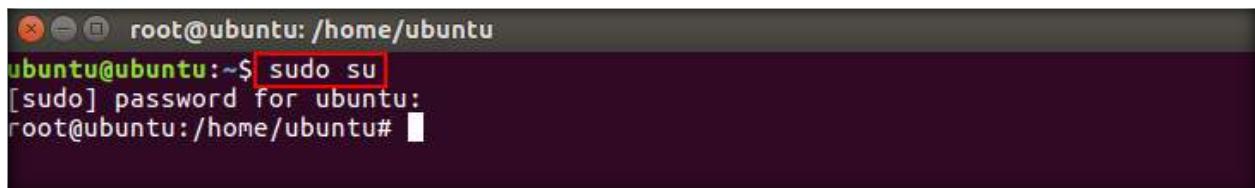
auto ens33
allow-hotplug ens33
iface ens33 inet static
    address 10.10.10.9
    netmask 255.255.255.0
    gateway 10.10.10.2
    dns-nameservers 8.8.8.8 8.8.4.4
```

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



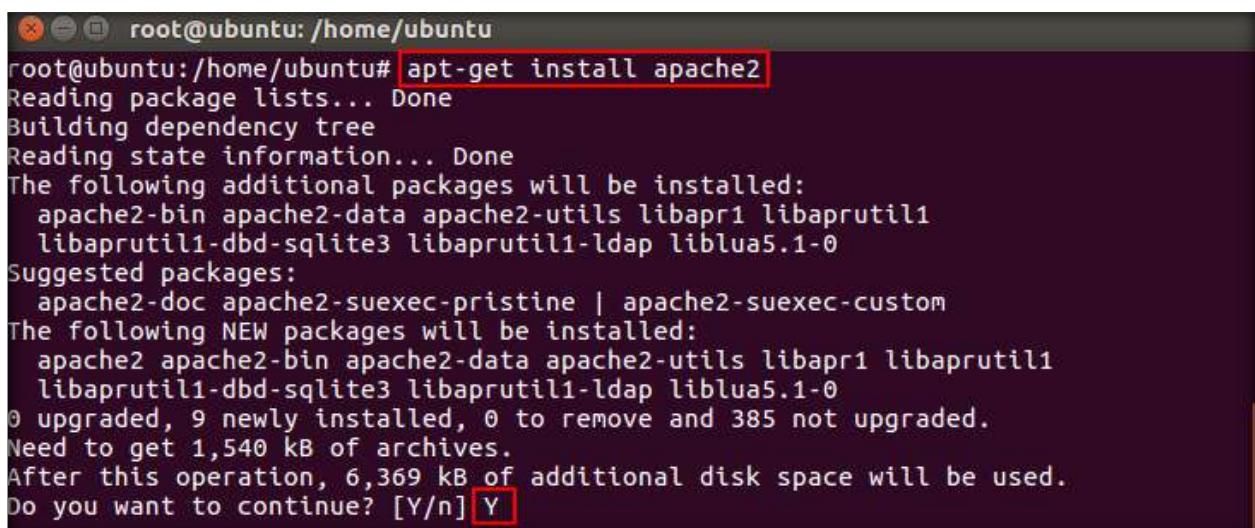
```
ubuntu@ubuntu:~$ ifconfig
ens33      Link encap:Ethernet HWaddr 00:0c:29:27:a1:30
           inet addr:10.10.10.9 Bcast:10.10.10.255 Mask:255.255.255.0
             inet6 addr: fe80::20c:29ff:fe27:a130/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                  RX packets:22 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:59 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:3040 (3.0 KB) TX bytes:6499 (6.4 KB)
```

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



```
root@ubuntu:/home/ubuntu
ubuntu@ubuntu:~$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu#
```

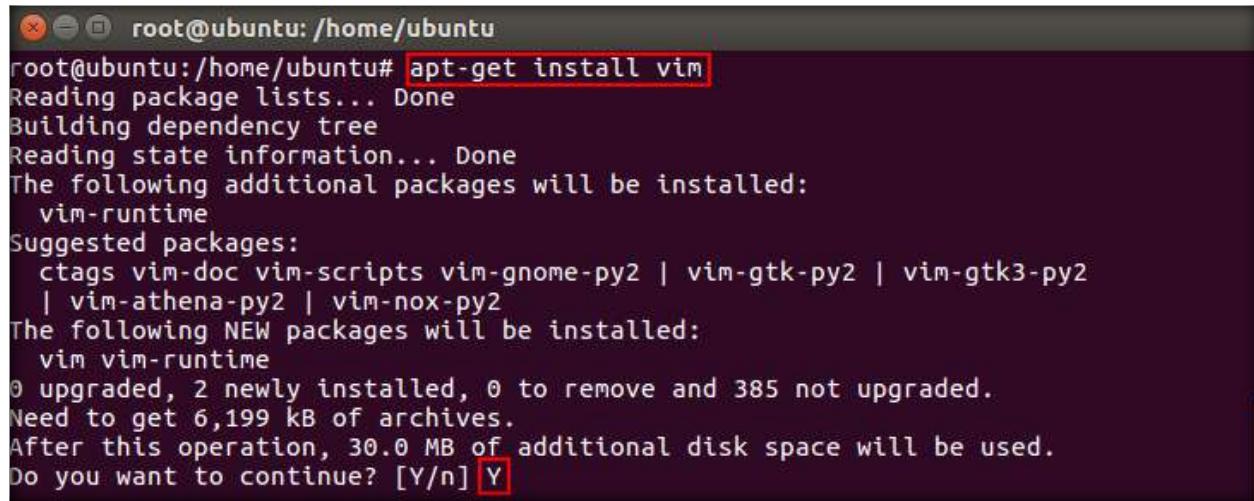
21. Type the command **apt-get install apache2** and press **Enter**. This command is issued to install apache web server
22. While installing the server, a notification appears saying additional disk space will be used. Type **y** and press **Enter**



```
root@ubuntu:/home/ubuntu#
root@ubuntu:/home/ubuntu# apt-get install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.1-0
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1
  libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.1-0
0 upgraded, 9 newly installed, 0 to remove and 385 not upgraded.
Need to get 1,540 kB of archives.
After this operation, 6,369 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

23. Type the command **apt-get install vim** and press **Enter**. This command is 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**



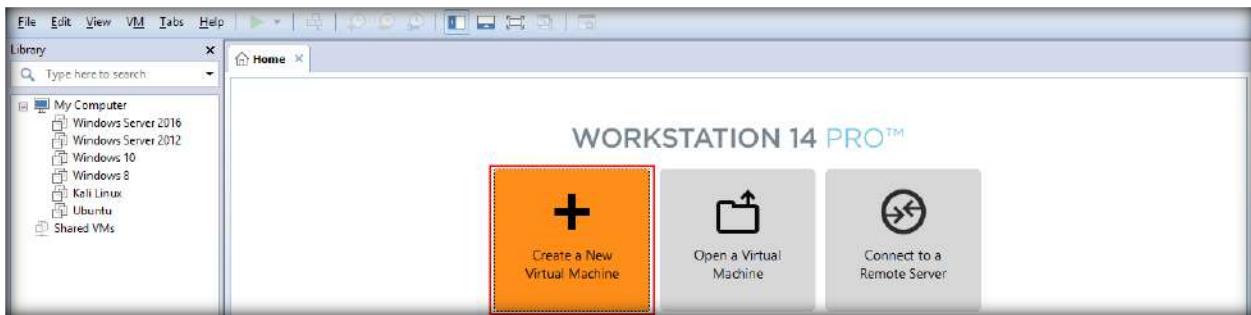
```
root@ubuntu:/home/ubuntu
root@ubuntu:/home/ubuntu# apt-get install vim
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  vim-runtime
Suggested packages:
  ctags vim-doc vim-scripts vim-gnome-py2 | vim-gtk-py2 | vim-gtk3-py2
  | vim-athena-py2 | vim-nox-py2
The following NEW packages will be installed:
  vim vim-runtime
0 upgraded, 2 newly installed, 0 to remove and 385 not upgraded.
Need to get 6,199 kB of archives.
After this operation, 30.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

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

[\[Back to Configuration Task Outline\]](#)

CT#9: Install Android in VMware Workstation

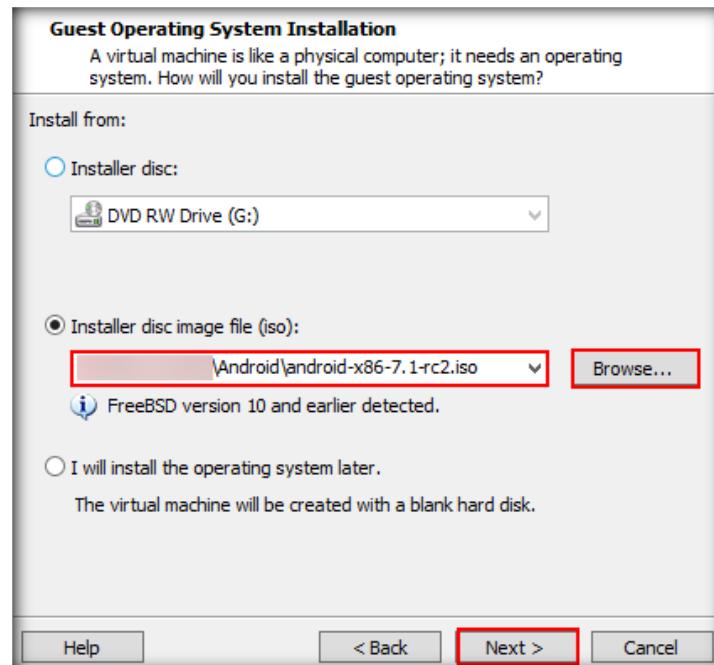
1. In VMware Workstation window, click **Create a New Virtual Machine**



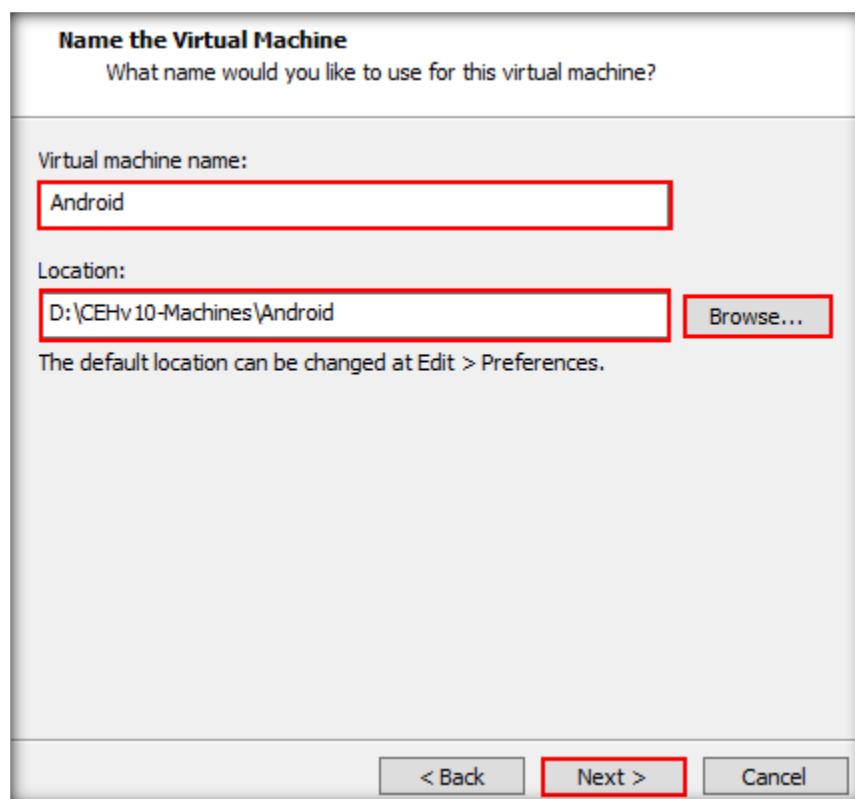
2. In the New Virtual Machine wizard, leave the settings to default and click **Next**



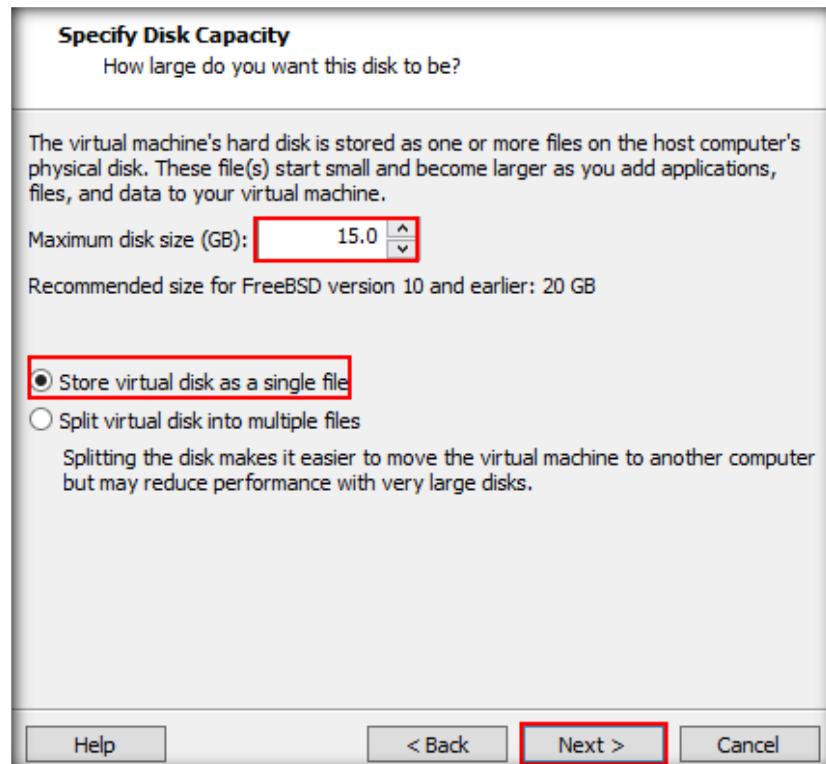
3. In Guest Operating System Installation wizard, choose **Installer disc image file (iso)**: radio button. Click **Browse** and navigate to D:\CEH-Tools\CEHv10 Lab Prerequisites\ISO's\Android and select **android-x86-7.1-rc2.iso** to provide the ISO path and click **Next**



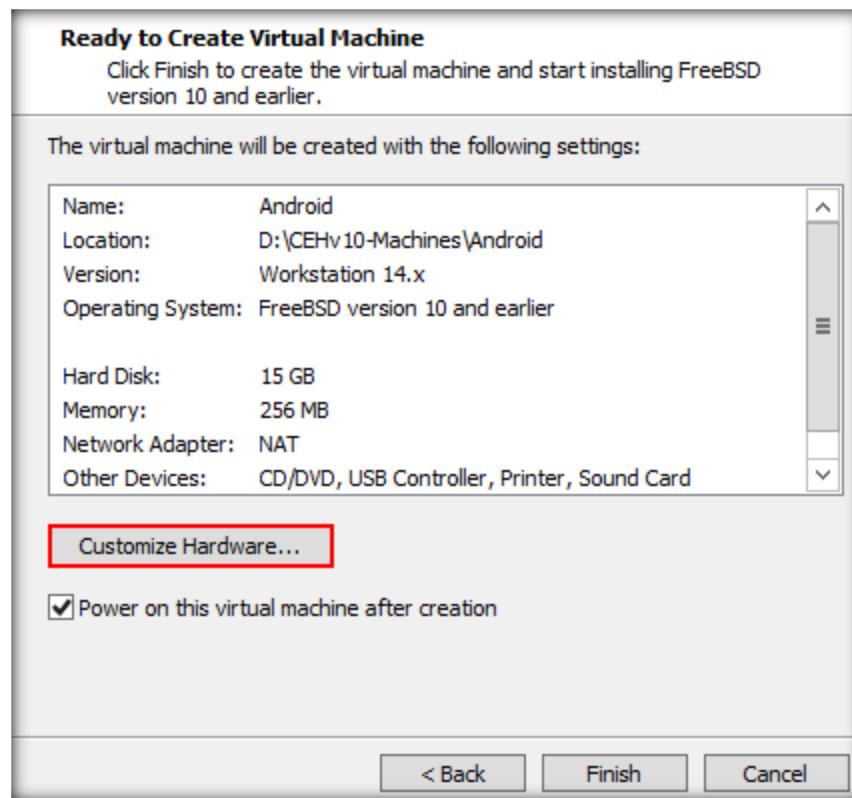
4. Name the Virtual Machine wizard appears, type **Android** in Virtual machine name field, and click **Browse** to store the virtual hard disk and click **Next**



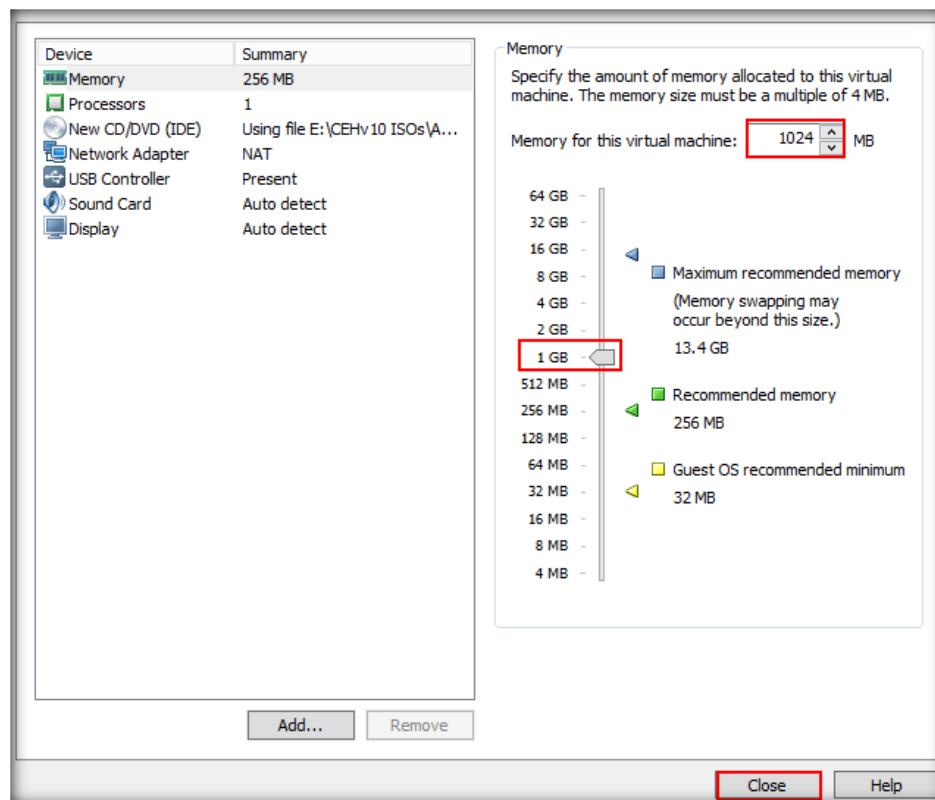
5. Specify Disk Capacity wizard appears, type **15.0 GB** in the Maximum disk size, and choose Store virtual disk as a single file radio button and click **Next**



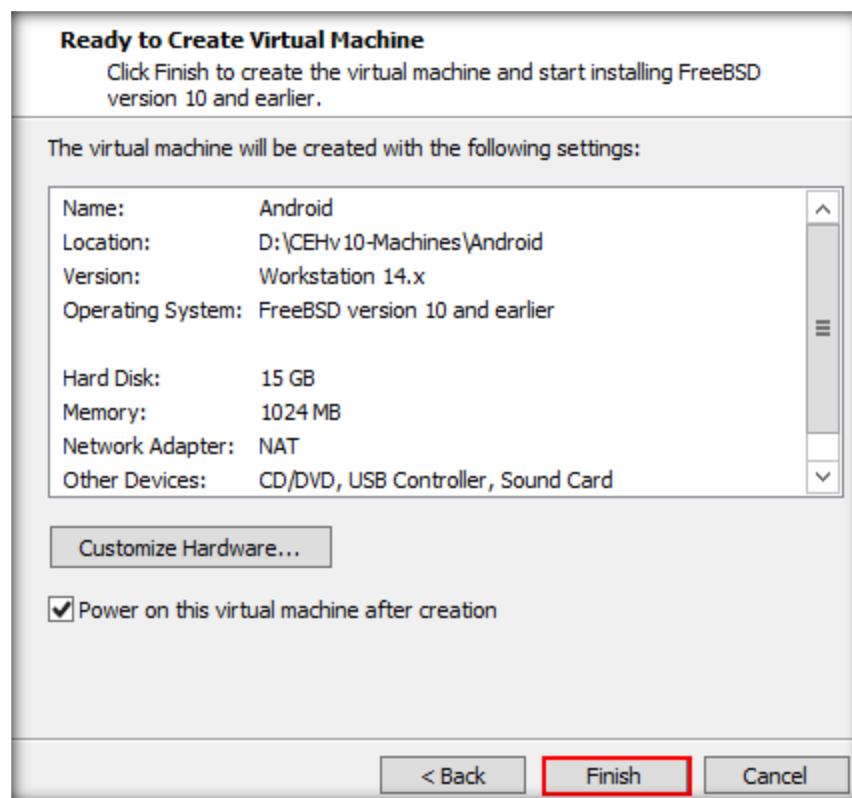
6. Click **Customize Hardware** button in the Ready to Create Virtual Machine wizard



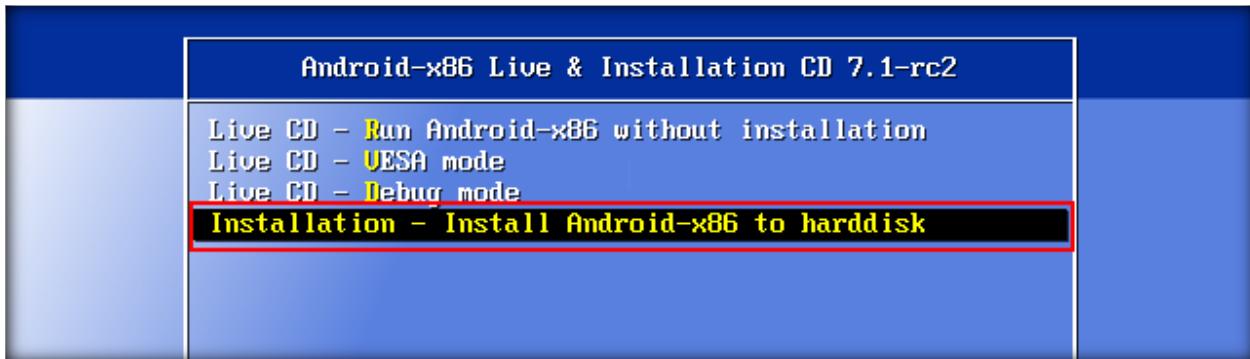
7. Hardware window appears, toggle the memory option to **1 GB** and click **Close**



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**



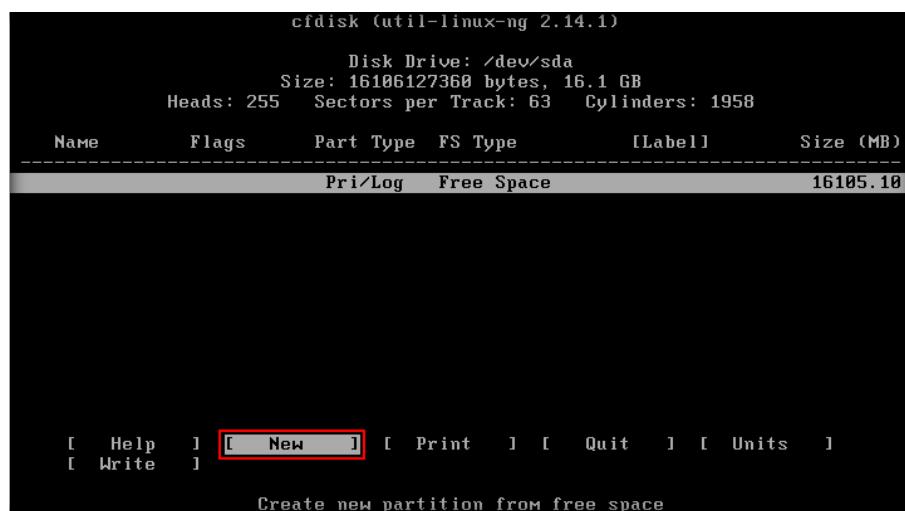
10. **Choose Partition** window appears. By default, **Create/Modify partitions** is selected, select **OK**



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**

```
cfdisk (util-linux-ng 2.14.1)

Disk Drive: /dev/sda
Size: 16106127360 bytes, 16.1 GB
Heads: 255  Sectors per Track: 63  Cylinders: 1958

Name      Flags     Part Type   FS Type      [Label]      Size (MB)
-----  -----
          Pri/Log   Free Space           16105.10

[Primary] [Logical] [Cancel]

Create a new primary partition_
```

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

```
cfdisk (util-linux-ng 2.14.1)

Disk Drive: /dev/sda
Size: 16106127360 bytes, 16.1 GB
Heads: 255  Sectors per Track: 63  Cylinders: 1958

Name      Flags     Part Type   FS Type      [Label]      Size (MB)
-----  -----
          Pri/Log   Free Space           16105.10

Size (in MB): 16105.10
```

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

```
cfdisk (util-linux-ng 2.14.1)

Disk Drive: /dev/sda
Size: 16106127360 bytes, 16.1 GB
Heads: 255  Sectors per Track: 63  Cylinders: 1958

Name      Flags     Part Type   FS Type        [Label]    Size (MB)
-----
sda1          Primary   Linux           16105.10
```

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

```
cfdisk (util-linux-ng 2.14.1)

Disk Drive: /dev/sda
Size: 16106127360 bytes, 16.1 GB
Heads: 255    Sectors per Track: 63    Cylinders: 1958

Name      Flags     Part Type   FS Type        [Label]     Size (MB)
-----
sda1      Boot      Primary   Linux          16105.10
```

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

```
cfdisk (util-linux-ng 2.14.1)

Disk Drive: /dev/sda
Size: 16106127360 bytes, 16.1 GB
Heads: 255  Sectors per Track: 63  Cylinders: 1958

Name      Flags     Part Type   FS Type      [Label]      Size (MB)
-----  -----
sda1      Boot      Primary  Linux          16105.10

Are you sure you want to write the partition table to disk? (yes or no): ye
Warning!! This may destroy data on your disk!
```

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

```
cfdisk (util-linux-ng 2.14.1)

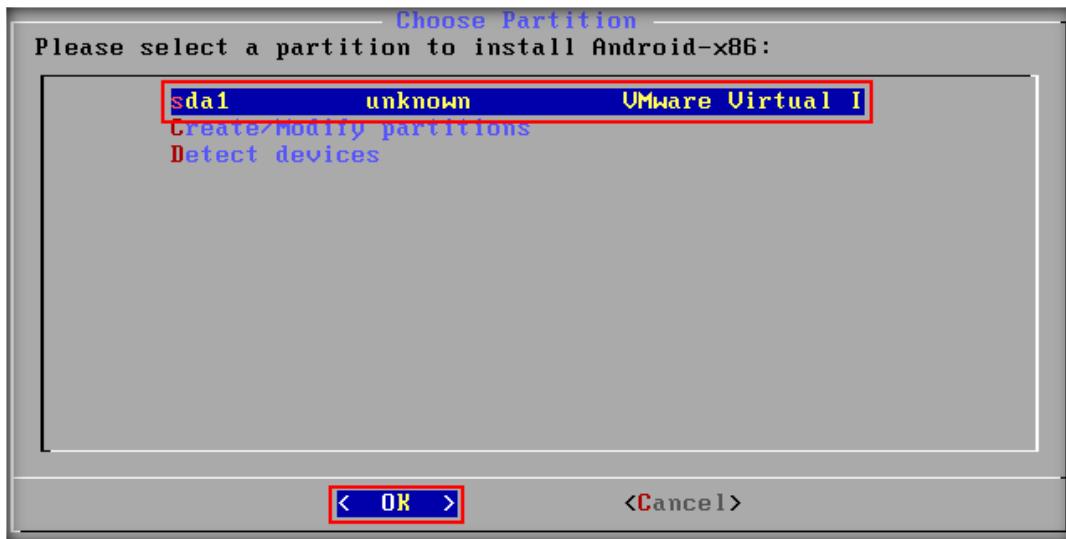
Disk Drive: /dev/sda
Size: 16106127360 bytes, 16.1 GB
Heads: 255  Sectors per Track: 63  Cylinders: 1958

Name      Flags     Part Type   FS Type      [Label]      Size (MB)
-----  -----
sda1      Boot      Primary  Linux          16105.10

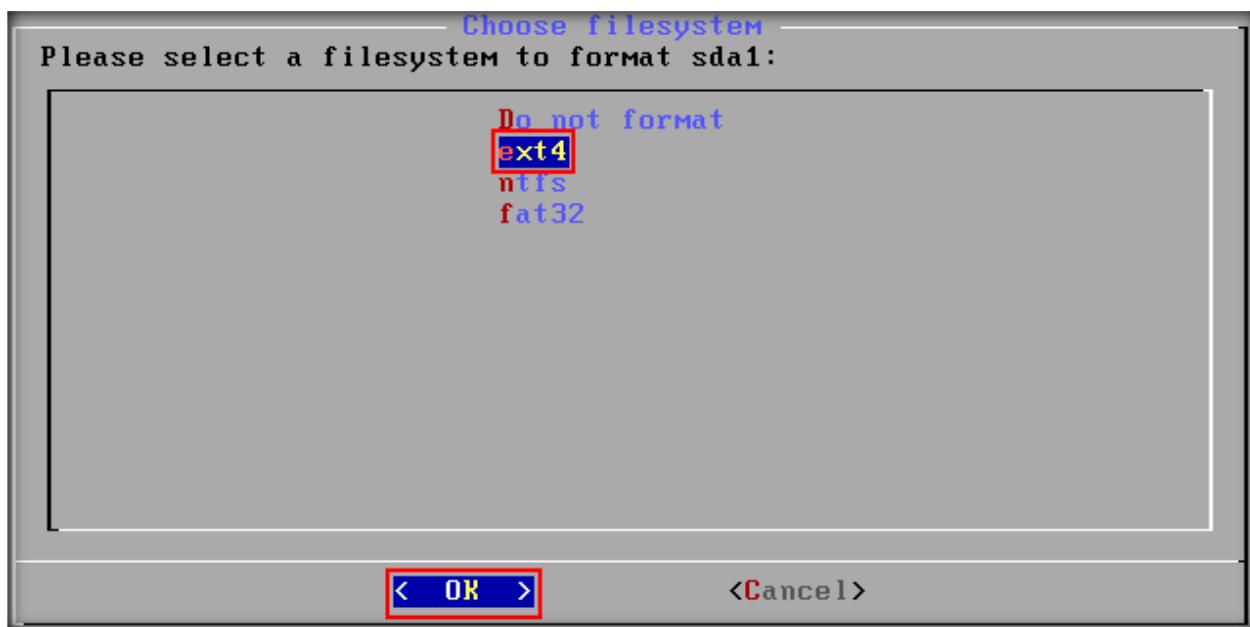
[ Bootable ] [ Delete ] [ Help ] [ Maximize ] [ Print ] 
[ Quit ] [ Type ] [ Units ] [ Write ] 

Quit program without writing partition table
```

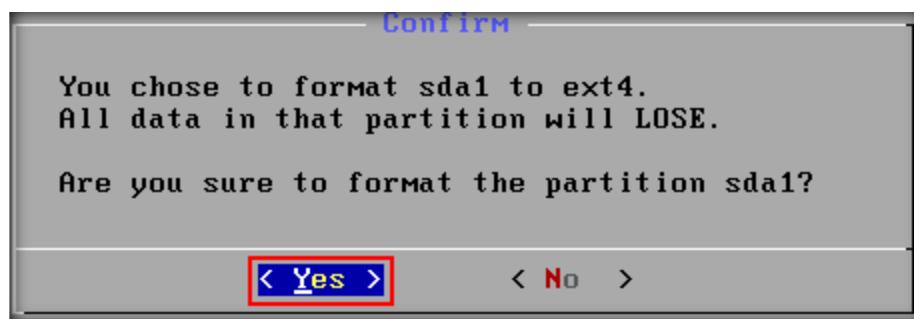
19. **Choose Partition** window appears with the virtual hard disk (**sda1**) selected by default, select **OK** and press **Enter**



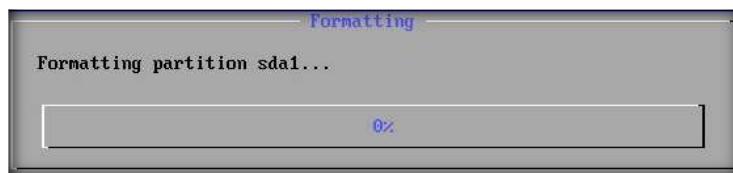
20. Choose a filesystem (here, **ext4**) and select **OK** and press **Enter**



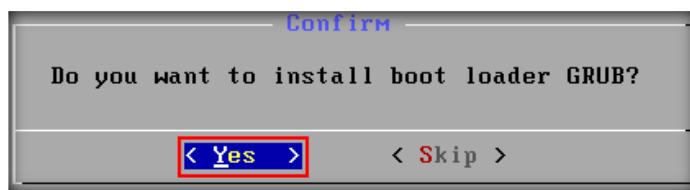
21. A **Confirm** dialog box appears, select **Yes** and press **Enter**



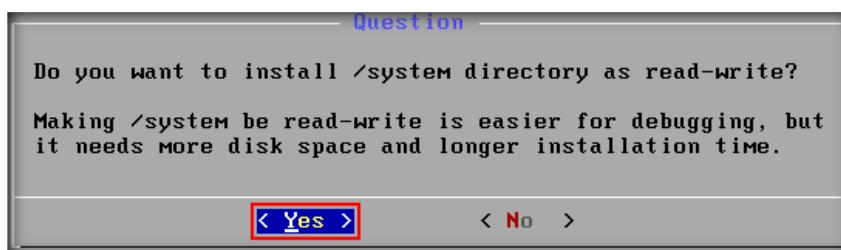
22. Partition formatting begins as shown in the screenshot



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



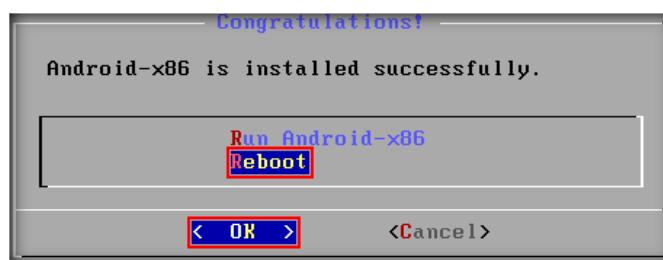
24. A **Question** dialog box appears; select **Yes** and press **Enter**



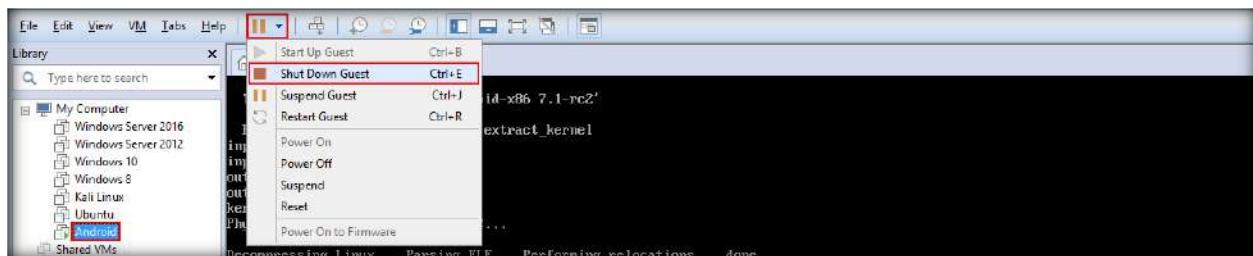
25. Android installation begins as shown in the following screenshot



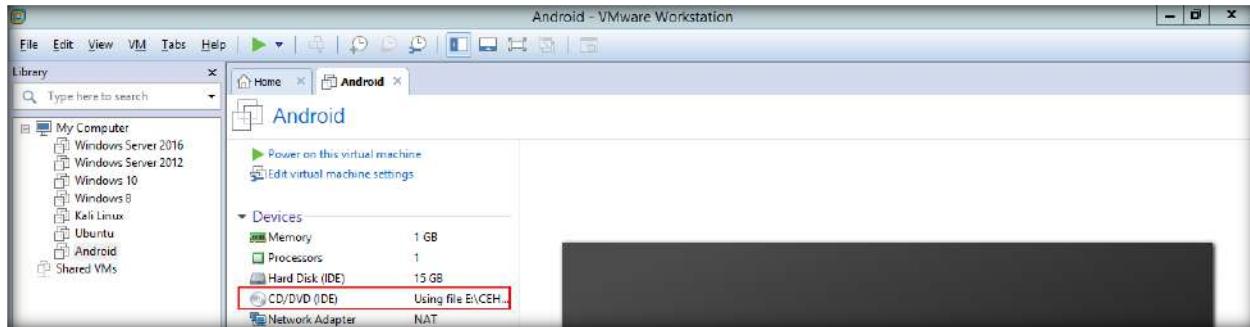
26. Once the image is created, a **Congratulations!** dialog box appears, select **Reboot** option and then select **OK** and press **Enter**



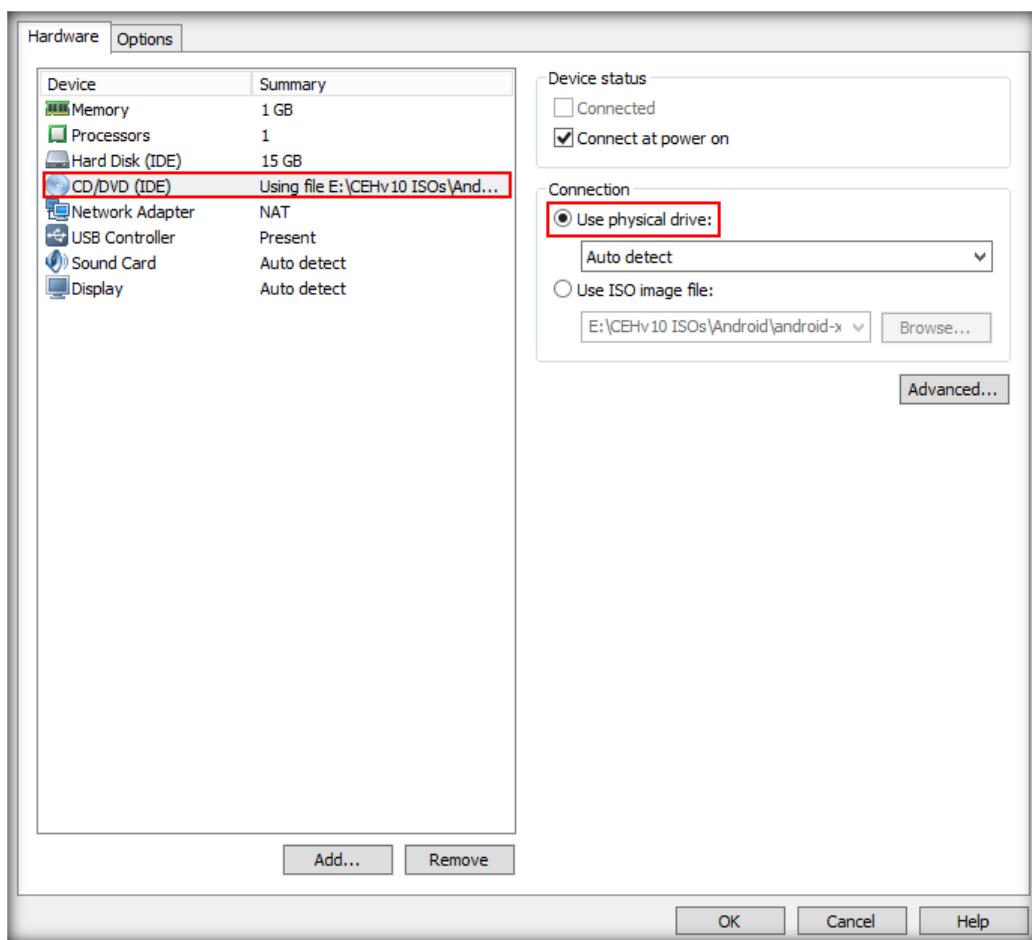
27. Once the machine is restarted, click **Shut Down Guest** as shown in the screenshot



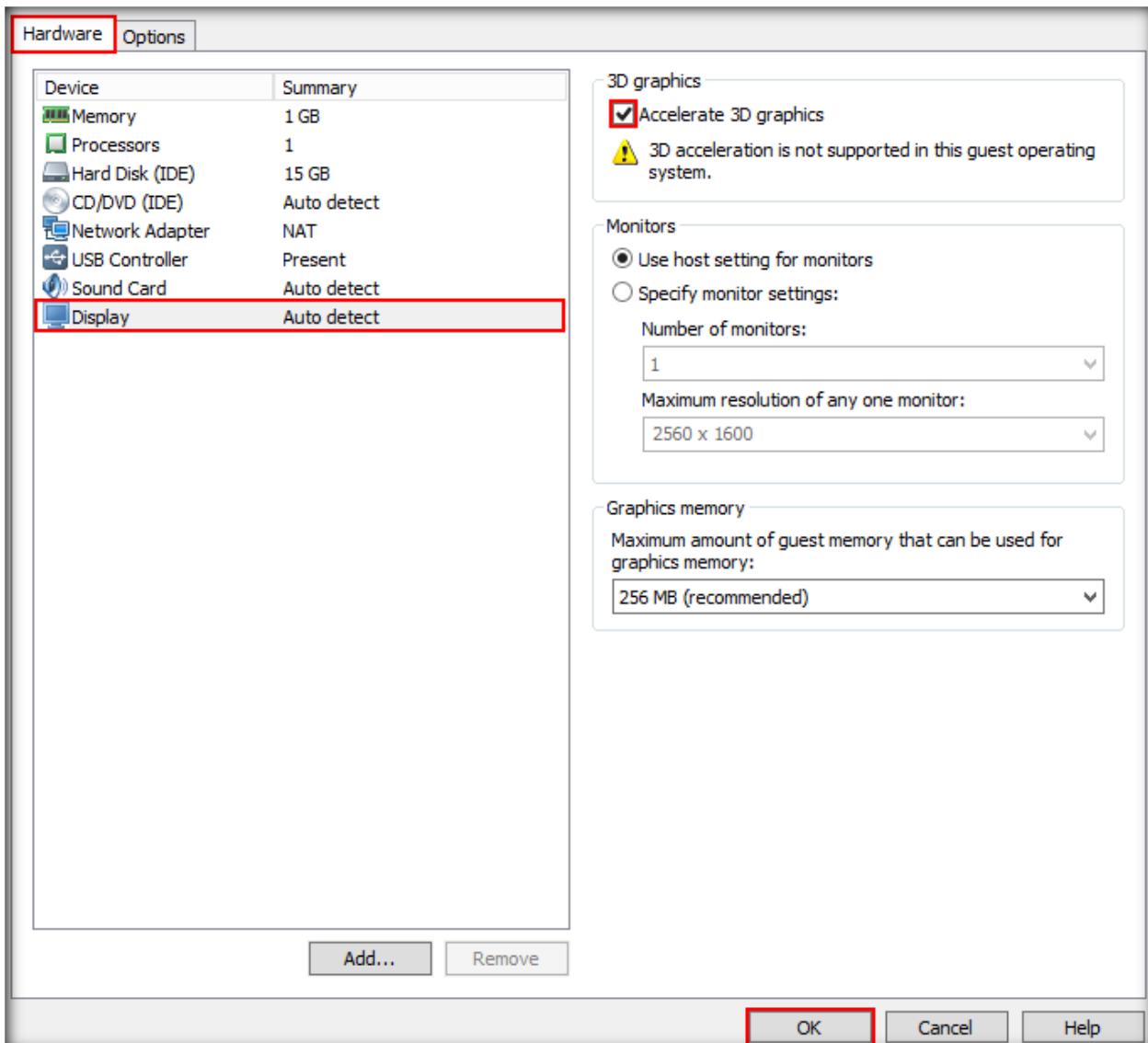
28. Once the machine is shut down, click CD/DVD (IDE) under Devices section as shown in the screenshot



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

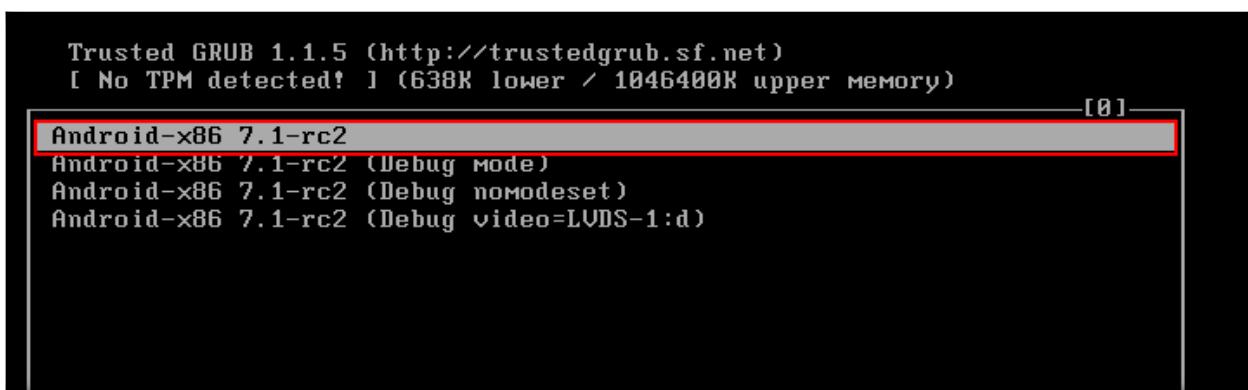


30. Display options appears, check **Accelerate 3D graphics** check box, and then click **OK**



31. Android boot menu appears, leave the window intact

32. Wait until android machine gets booted

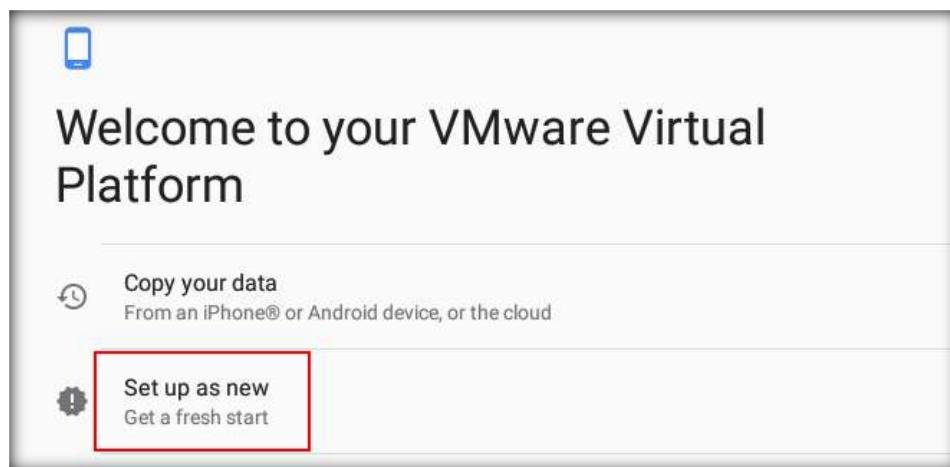


33. Welcome screen appears, click **LET'S GO**



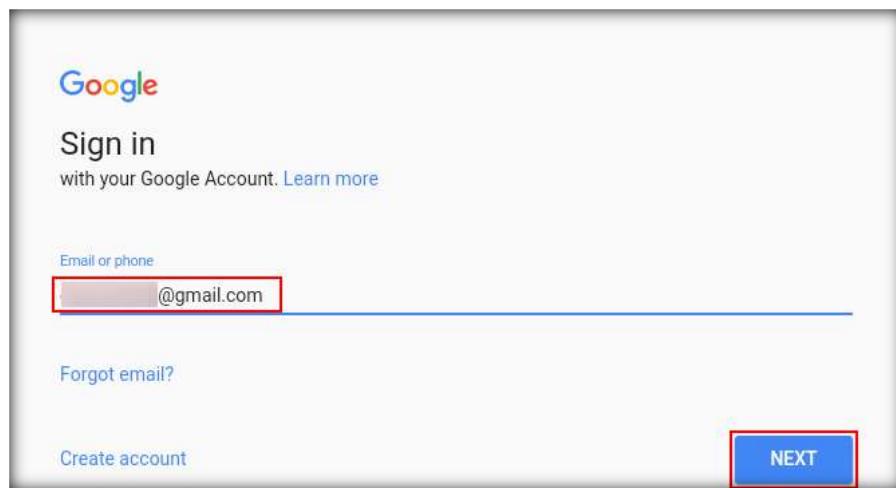
34. Welcome to your VMware Virtual Platform screen appears, click **Set up as new**

Note: If Google Play services has stopped pop-up appears, click **Close app**

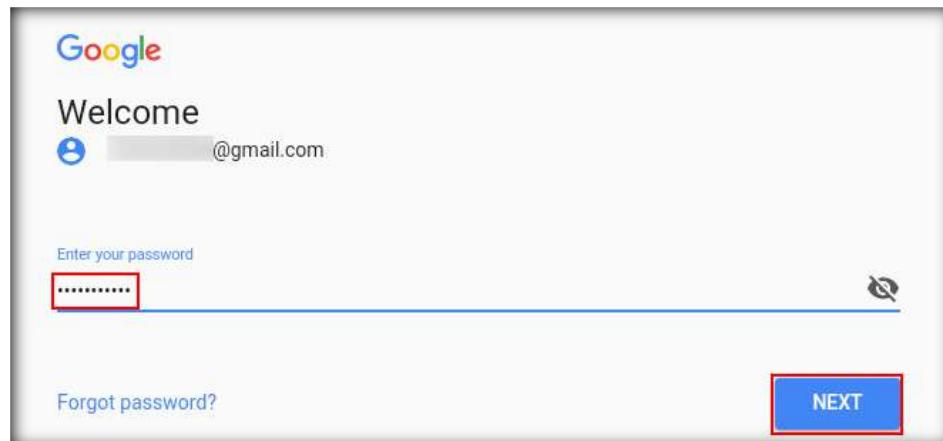


35. Google Sign in page appears, provide the working email ID to sign in and click **Next**

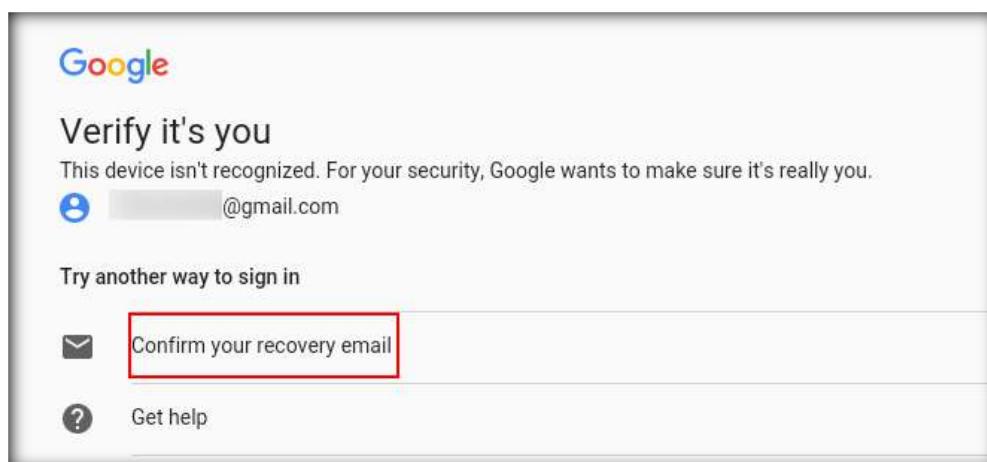
Note: If you do not have an email account Create a new account by clicking Create account link



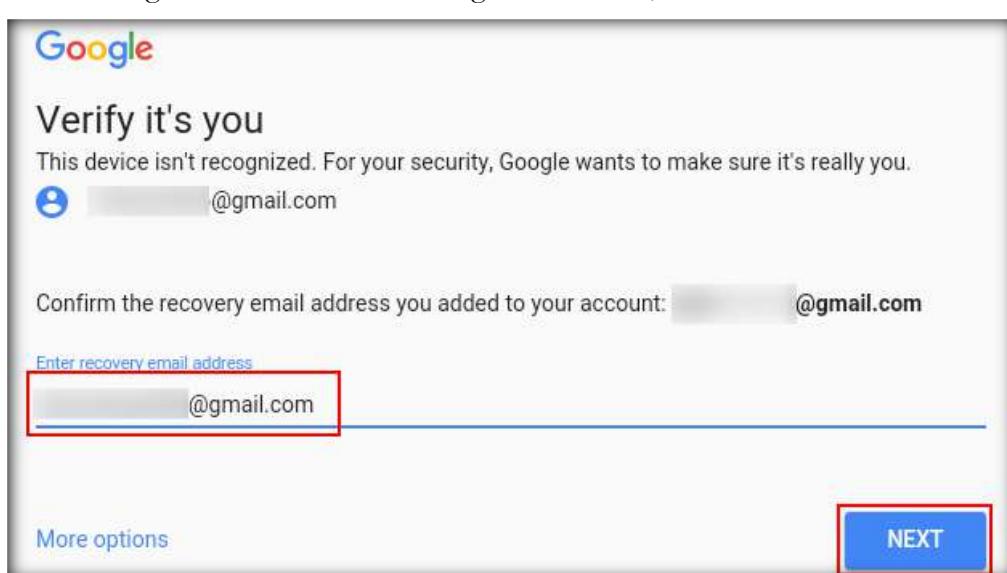
36. Type in your email account password and click **Next**



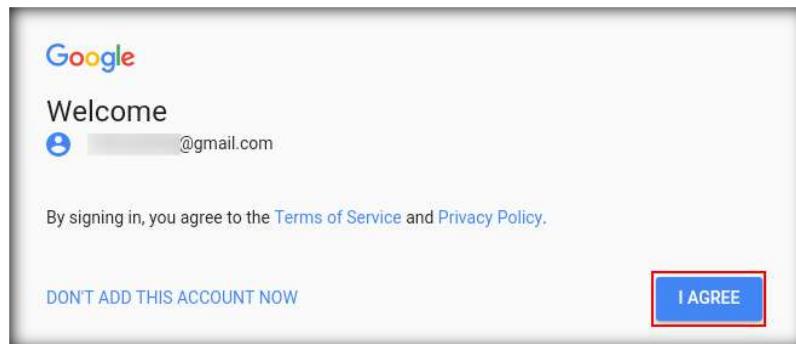
37. If Verify it's you screen appears, click **Confirm your recovery email**



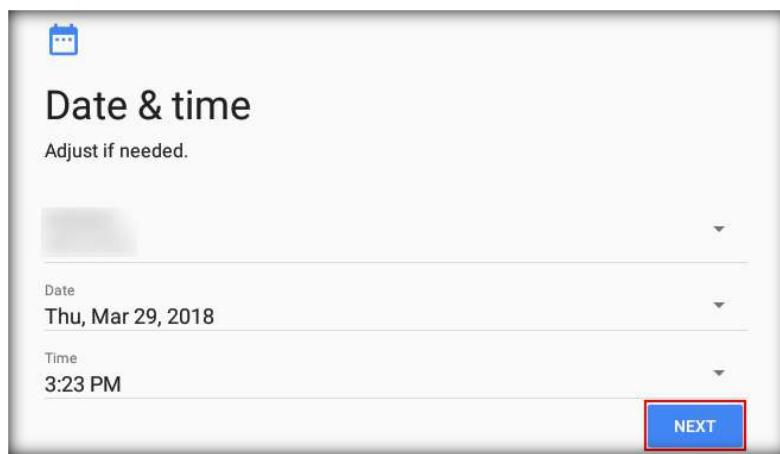
38. Confirm your recovery email address screen appears, type the recovery email address that you have assigned at the time of creating the email ID, and then click **Next**



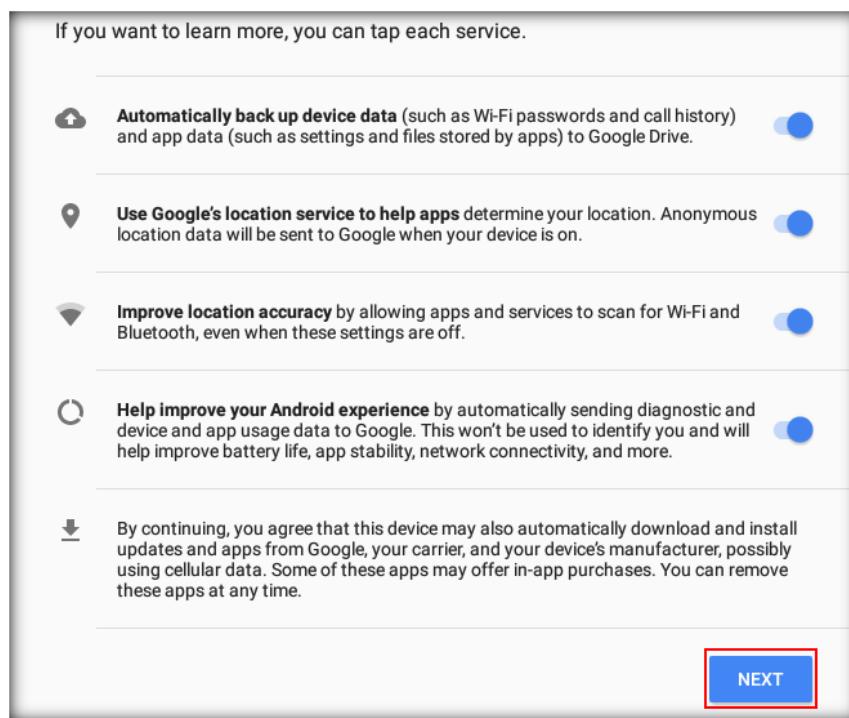
39. Welcome screen appears, click **I AGREE**. Wait until the configuration is completed



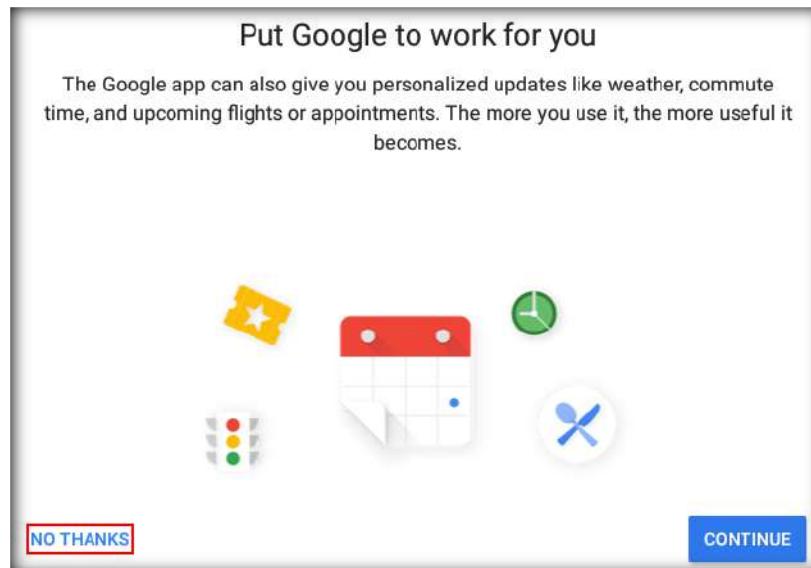
40. Date & time screen appears, leave the settings to default and click **Next**



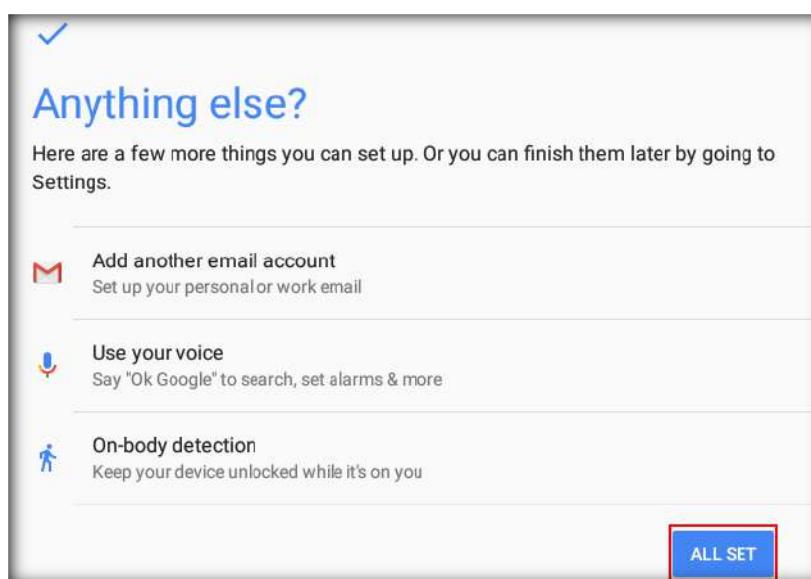
41. In Google Services screen, leave the settings to default, scroll down and click **Next**



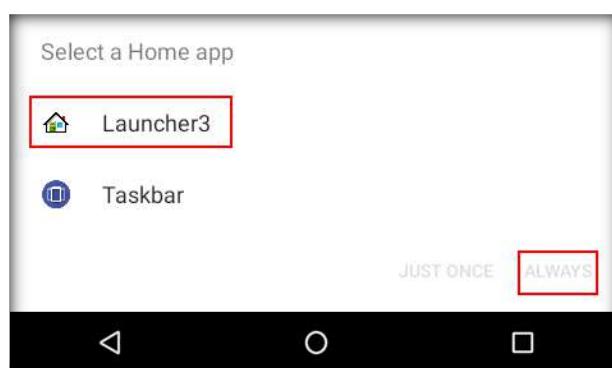
42. Put Google to work for you screen appears, click **NO THANKS**



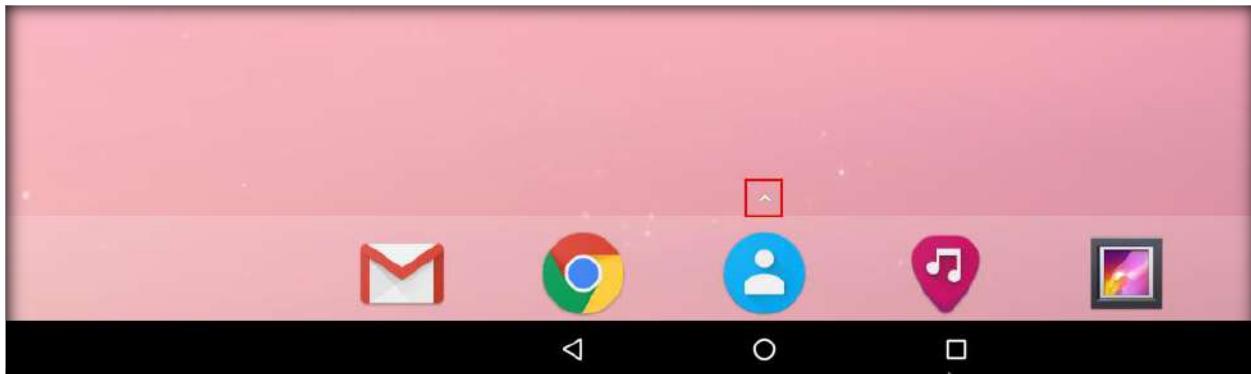
43. Anything else? screen appears, click **ALL SET** to continue



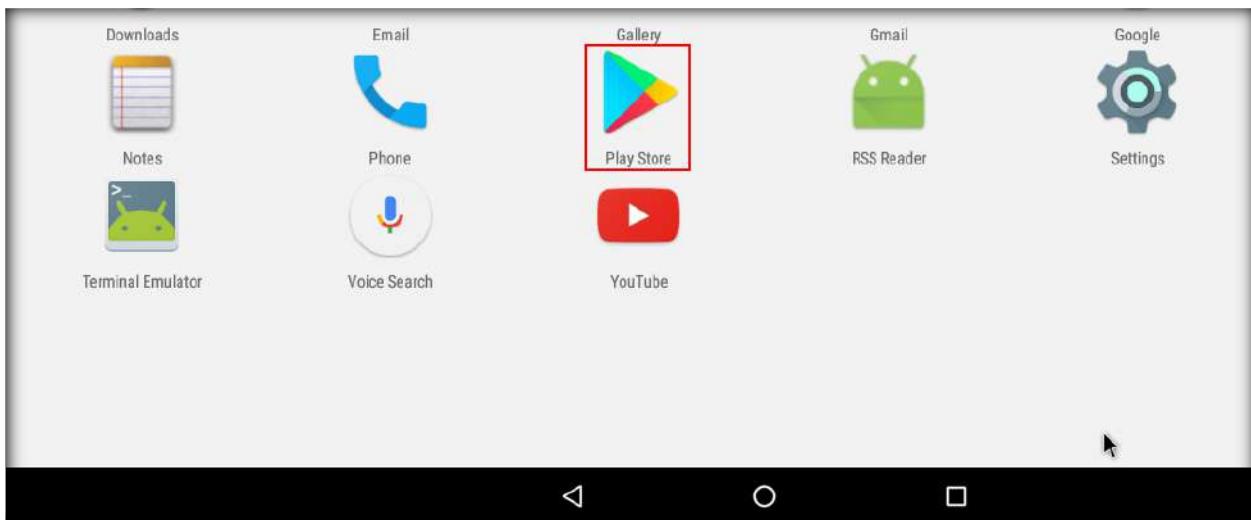
44. Select a Home app pop-up appears, click **Launcher3** and click **ALWAYS** as shown in the screenshot



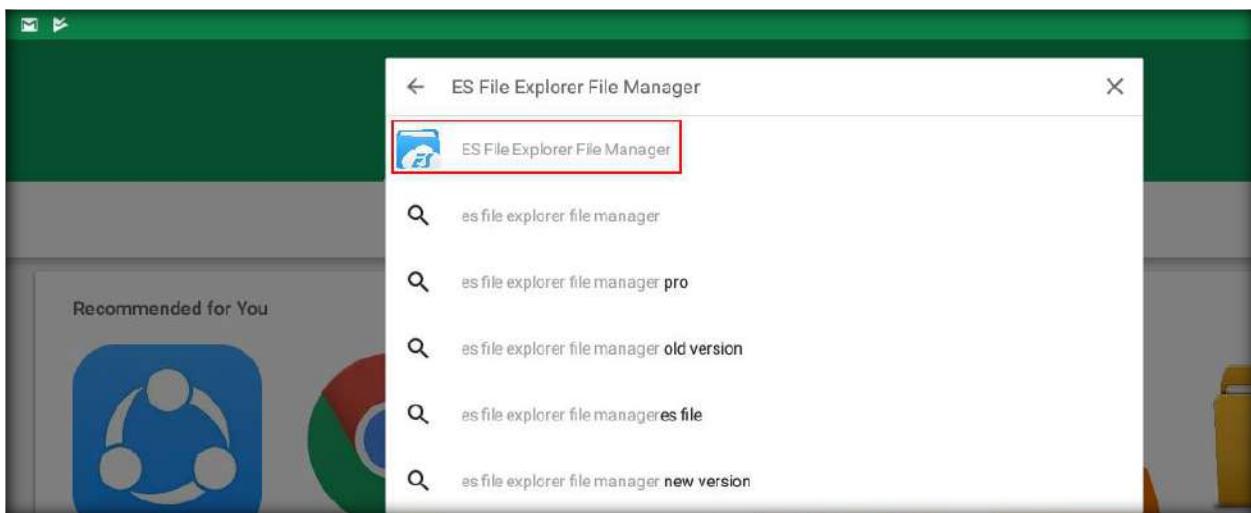
45. Thus, you have successfully installed Android machine as shown in the screenshot. Click **app drawer** icon (^) to view menu



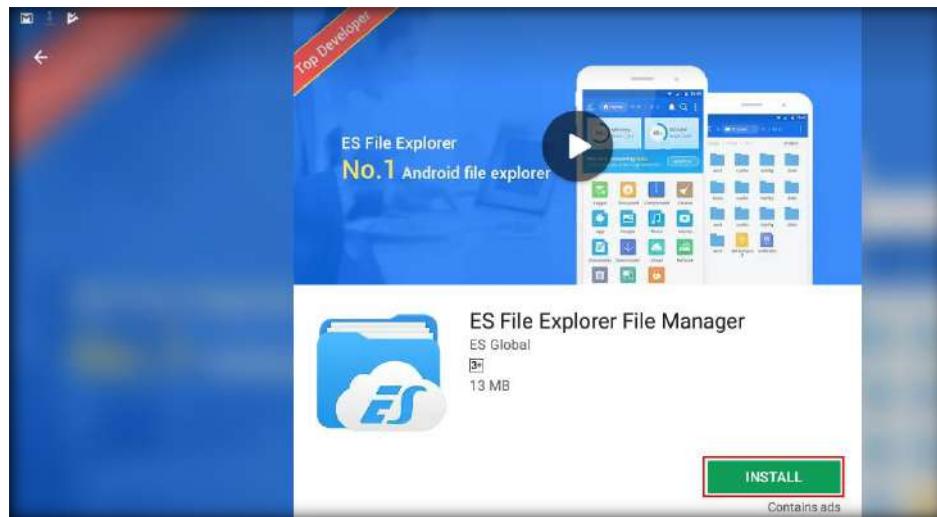
46. Click **Play Store** icon in the menu



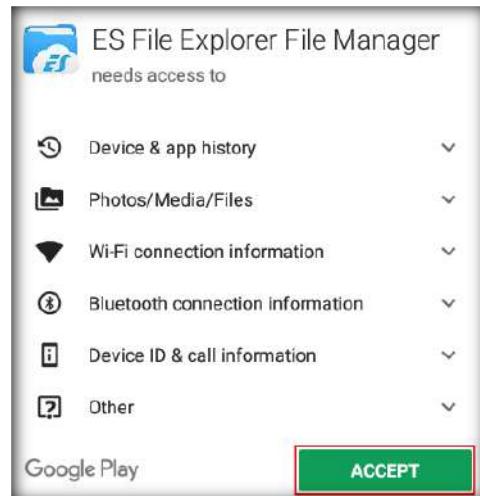
47. Type **es file explorer** in the search bar of Play Stor. **ES File Explorer File Manager** application appears in the search result. Click on it



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



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



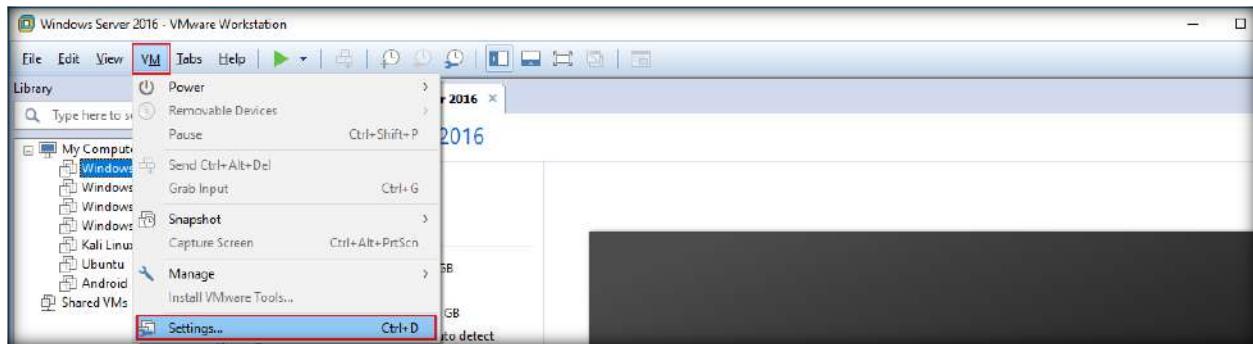
50. Wait for the application to install. On completing the installation close all the applications



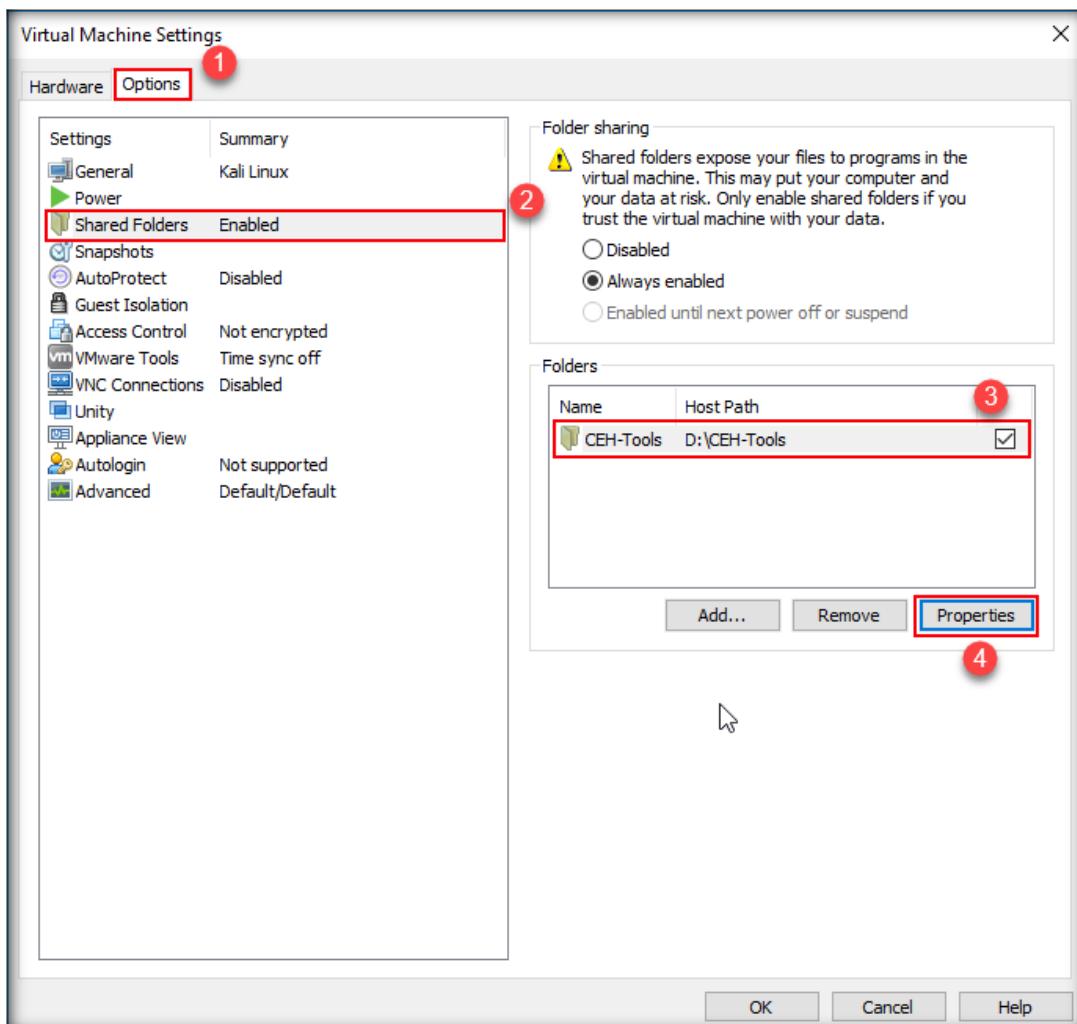
[\[Back to Configuration Task Outline\]](#)

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

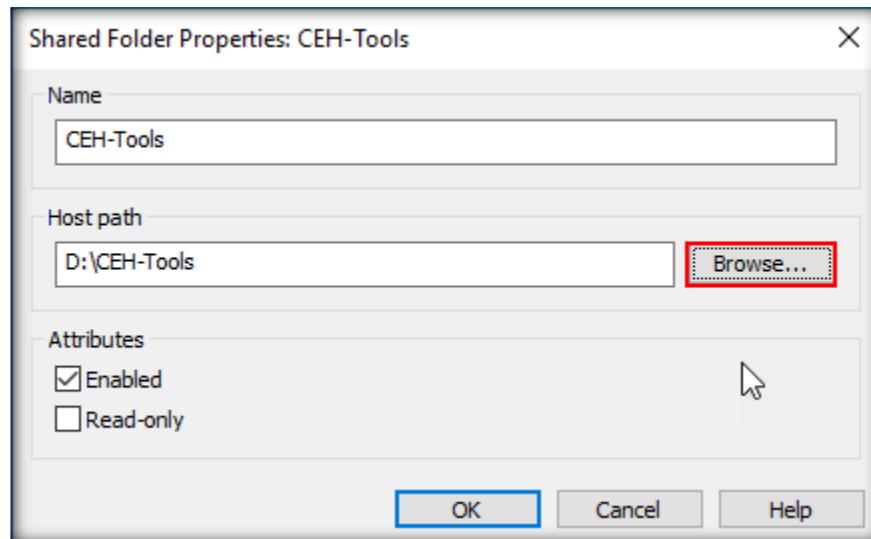
1. Make sure that all the Virtual Machines are turned off
2. Select any Windows VM (here, Windows Server 2016) from the left pane, and go to **VM** and click **Settings**



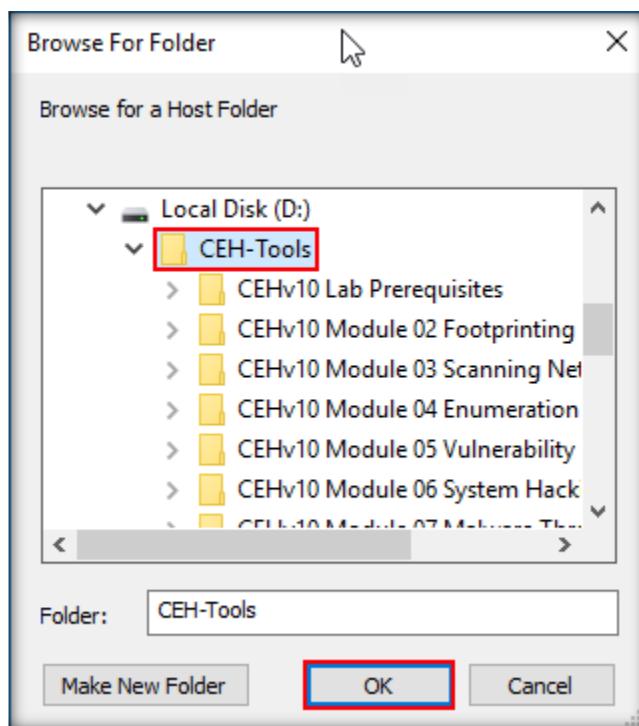
3. Go to **Options** tab in the Virtual Machine Settings window. Select **Shared Folders** from the left pane, select **Always enabled** radio button, choose the **CEH-Tools** folder and click **Properties**



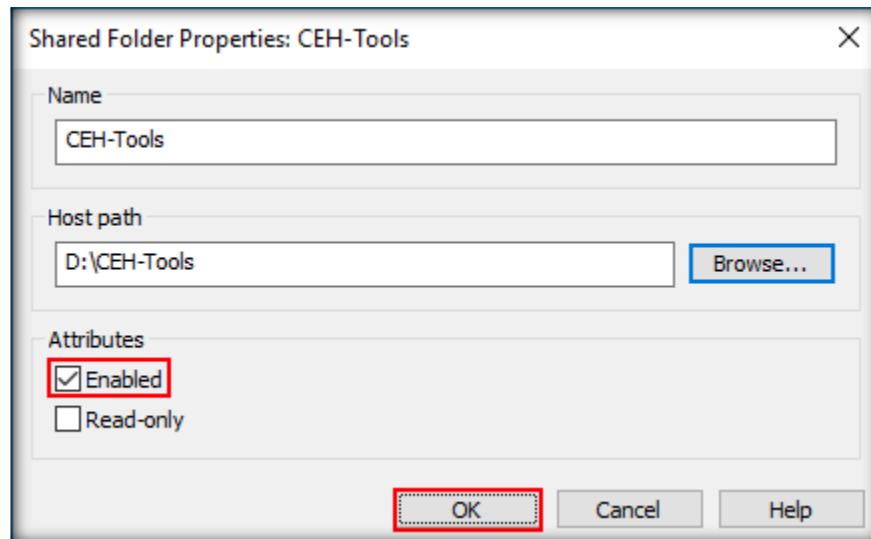
4. Shared Folder Properties window appears, click **Browse**



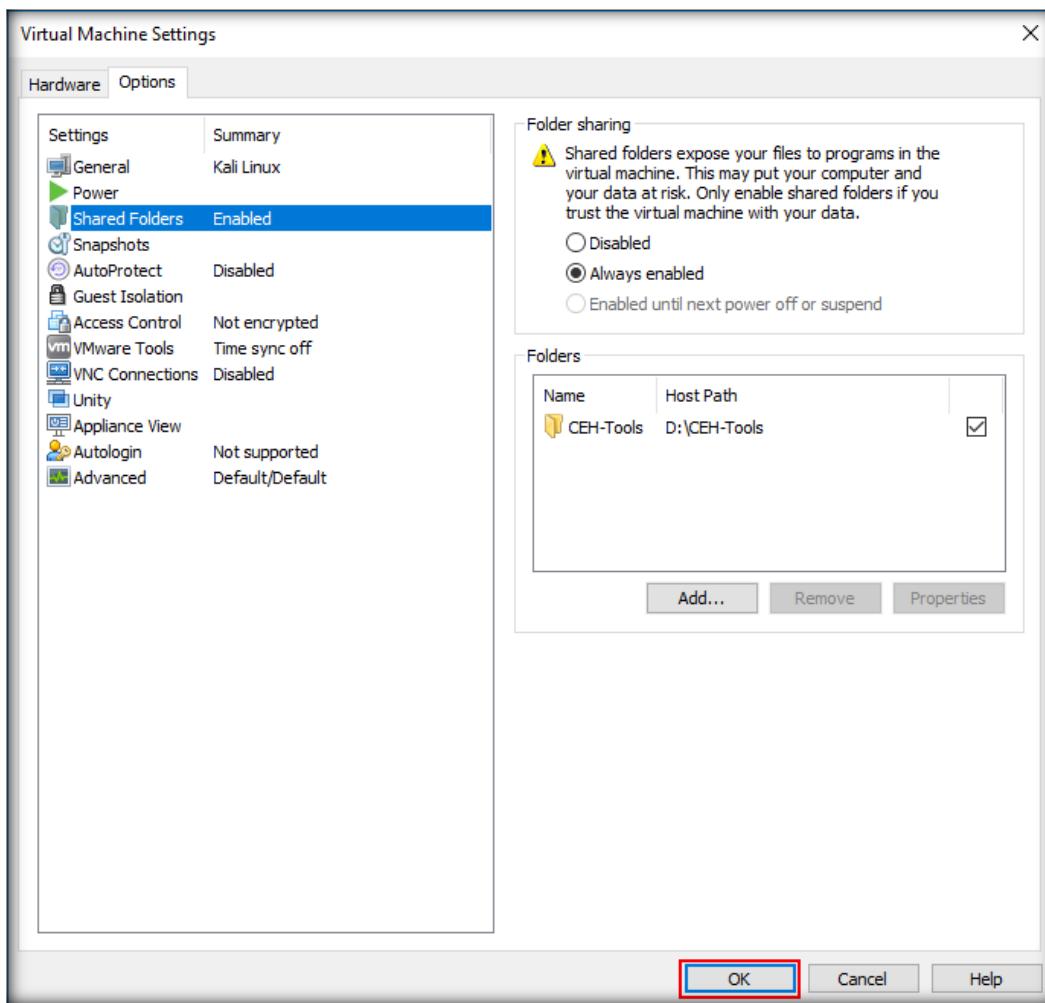
5. Browse to the **CEH-Tools** directory in your host system and click **OK**



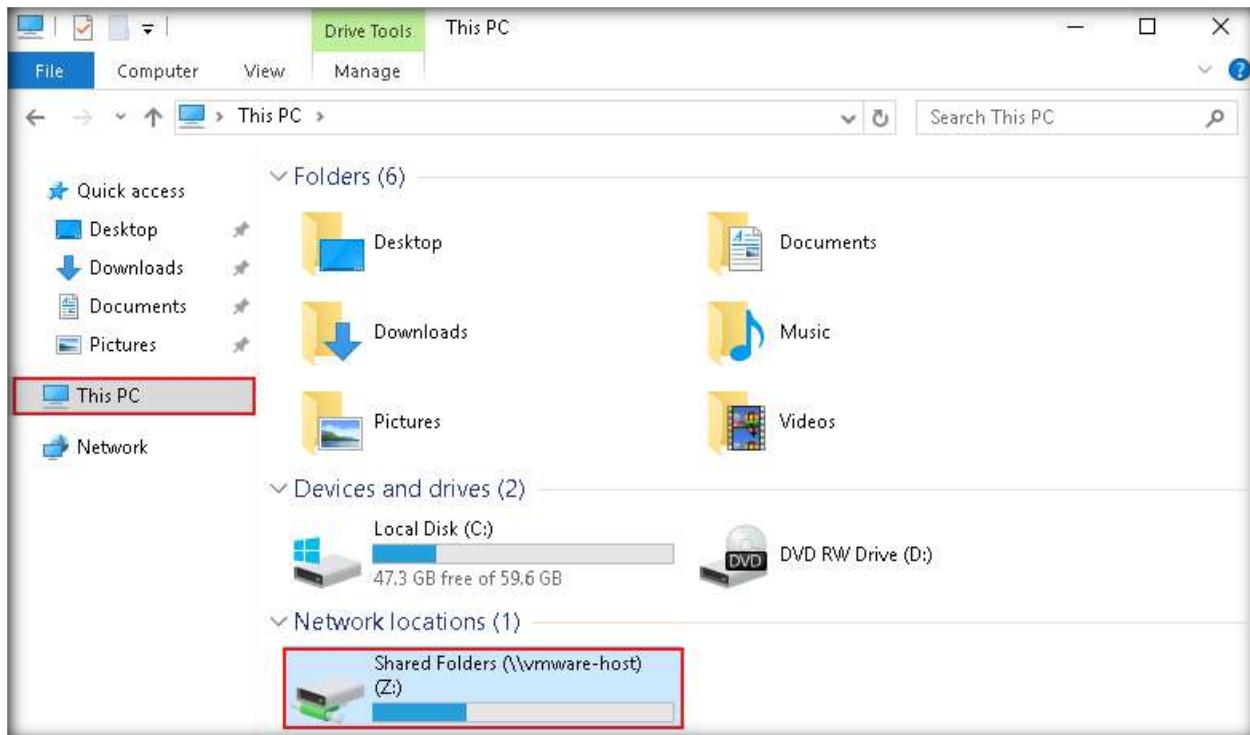
6. Make sure that the **Enabled** checkbox is selected and click **OK**



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

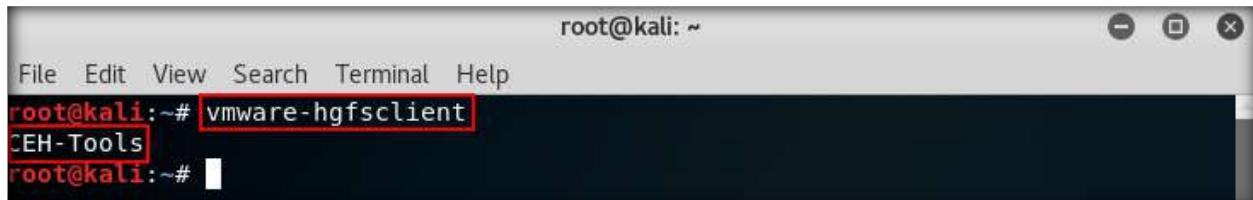


9. Repeat the above steps with Windows Server 2012, Windows 10 and Windows 8 virtual machines

[\[Back to Configuration Task Outline\]](#)

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

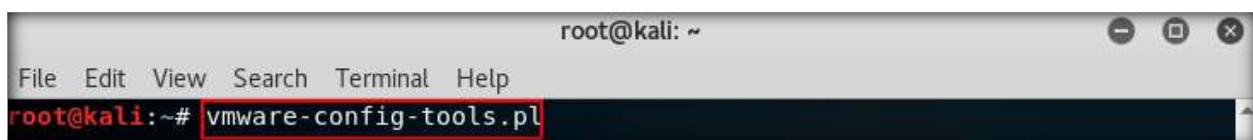


root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# vmware-hgfsclient
CEH-Tools
root@kali:~#
```

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

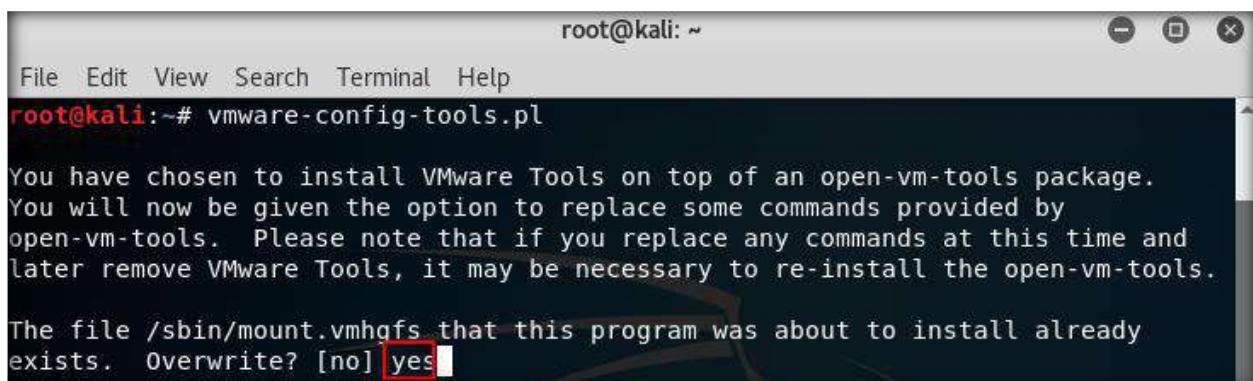


root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# vmware-config-tools.pl
```

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



root@kali: ~

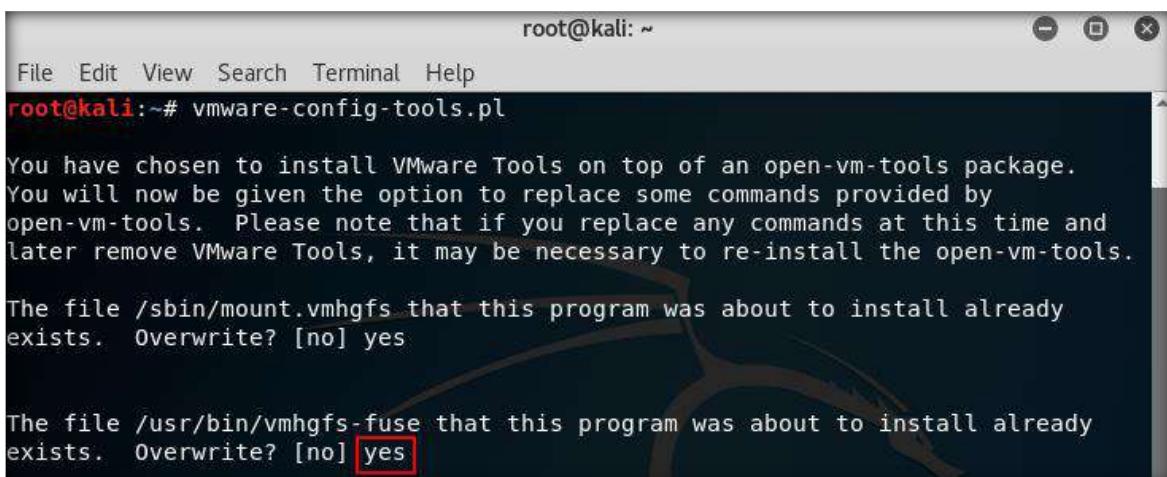
File Edit View Search Terminal Help

```
root@kali:~# vmware-config-tools.pl
```

You have chosen to install VMware Tools on top of an open-vm-tools package.
You will now be given the option to replace some commands provided by
open-vm-tools. Please note that if you replace any commands at this time and
later remove VMware Tools, it may be necessary to re-install the open-vm-tools.

The file /sbin/mount.vmhgfs that this program was about to install already
exists. Overwrite? [no] yes

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



root@kali: ~

File Edit View Search Terminal Help

```
root@kali:~# vmware-config-tools.pl
```

You have chosen to install VMware Tools on top of an open-vm-tools package.
You will now be given the option to replace some commands provided by
open-vm-tools. Please note that if you replace any commands at this time and
later remove VMware Tools, it may be necessary to re-install the open-vm-tools.

The file /sbin/mount.vmhgfs that this program was about to install already
exists. Overwrite? [no] yes

The file /usr/bin/vmhgfs-fuse that this program was about to install already
exists. Overwrite? [no] yes

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**

```
root@kali: ~
File Edit View Search Terminal Help
Stopping VMware Tools services in the virtual machine:
  VMware User Agent (vmware-user): done
  Unmounting HGFS shares: done
  Guest filesystem driver: done

The module vmci has already been installed on this system by another installer
or package and will not be modified by this installer.

The module vsock has already been installed on this system by another
installer or package and will not be modified by this installer.

The module vmxnet3 has already been installed on this system by another
installer or package and will not be modified by this installer.

The module pvscsi has already been installed on this system by another
installer or package and will not be modified by this installer.

The module vmmemctl has already been installed on this system by another
installer or package and will not be modified by this installer.

The VMware Host-Guest Filesystem allows for shared folders between the host OS
and the guest OS in a Fusion or Workstation virtual environment. Do you wish
to enable this feature? [yes] yes
```

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?

```
root@kali: ~
File Edit View Search Terminal Help
The module vmxnet3 has already been installed on this system by another
installer or package and will not be modified by this installer.

The module pvscsi has already been installed on this system by another
installer or package and will not be modified by this installer.

The module vmmemctl has already been installed on this system by another
installer or package and will not be modified by this installer.

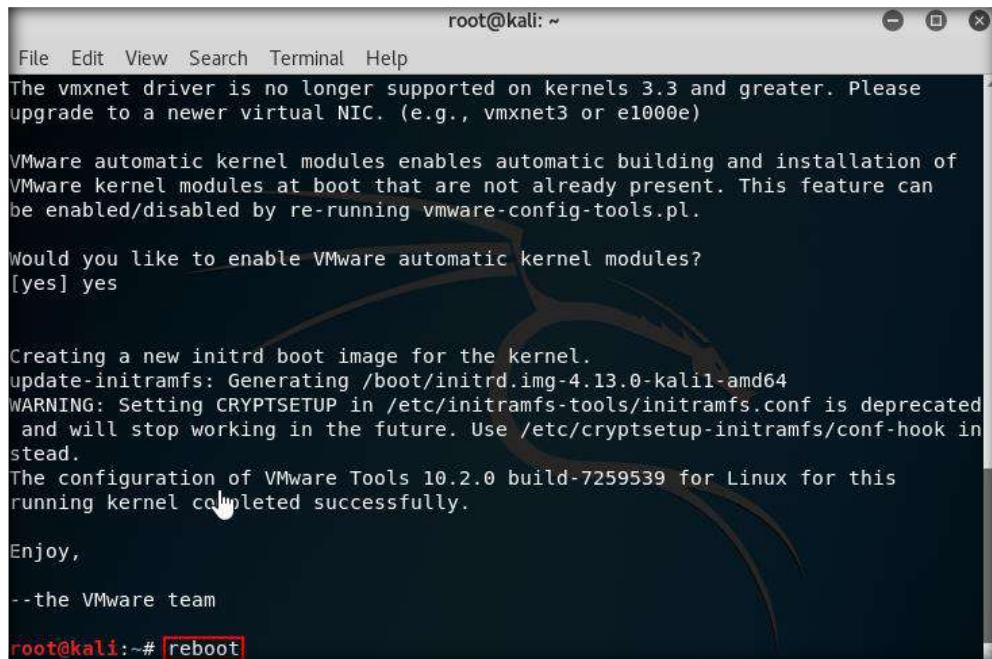
The VMware Host-Guest Filesystem allows for shared folders between the host OS
and the guest OS in a Fusion or Workstation virtual environment. Do you wish
to enable this feature? [yes] yes

The vmxnet driver is no longer supported on kernels 3.3 and greater. Please
upgrade to a newer virtual NIC. (e.g., vmxnet3 or e1000e)

VMware automatic kernel modules enables automatic building and installation of
VMware kernel modules at boot that are not already present. This feature can
be enabled/disabled by re-running vmware-config-tools.pl.

Would you like to enable VMware automatic kernel modules?
[yes] yes
```

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



```
root@kali: ~
File Edit View Search Terminal Help
The vmxnet driver is no longer supported on kernels 3.3 and greater. Please
upgrade to a newer virtual NIC. (e.g., vmxnet3 or e1000e)

VMware automatic kernel modules enables automatic building and installation of
VMware kernel modules at boot that are not already present. This feature can
be enabled/disabled by re-running vmware-config-tools.pl.

Would you like to enable VMware automatic kernel modules?
[yes] yes

Creating a new initrd boot image for the kernel.
update-initramfs: Generating /boot/initrd.img-4.13.0-kali1-amd64
WARNING: Setting CRYPTSETUP in /etc/initramfs-tools/initramfs.conf is deprecated
and will stop working in the future. Use /etc/cryptsetup-initramfs/conf-hook instead.
The configuration of VMware Tools 10.2.0 build-7259539 for Linux for this
running kernel completed successfully.

Enjoy,
--the VMware team

root@kali:~# reboot
```

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



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# ln -s /mnt/hgfs/CEH-Tools ~/Desktop/CEH-Tools
```

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

```
ubuntu@ubuntu:~$ vmware-hgfsclient
```

The terminal shows the command `vmware-hgfsclient` being typed in. The output below it is "CEH-Tools".

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

```
ubuntu@ubuntu:~$ sudo vmware-config-tools.pl
```

The terminal shows the command `sudo vmware-config-tools.pl` being typed in. A password prompt "[sudo] password for ubuntu:" is shown below.

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

```
ubuntu@ubuntu:~$ sudo vmware-config-tools.pl
[sudo] password for ubuntu:
The file /etc/pam.d/vmtoolsd that this program was about to install already
exists. Overwrite? [no] yes
```

The terminal shows a warning message: "The file /etc/pam.d/vmtoolsd that this program was about to install already exists. Overwrite? [no] yes". The user has typed "yes".

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**

```
ubuntu@ubuntu:~$ sudo vmware-config-tools.pl
VMware User Agent (vmware-user): done
Blocking file system: done
Unmounting HGFS shares: done
Guest filesystem driver: done

The module vmci has already been installed on this system by another installer
or package and will not be modified by this installer.

The module vsock has already been installed on this system by another installer
or package and will not be modified by this installer.

The module vmxnet3 has already been installed on this system by another
installer or package and will not be modified by this installer.

The module pvscsi has already been installed on this system by another
installer or package and will not be modified by this installer.

The module vmmemctl has already been installed on this system by another
installer or package and will not be modified by this installer.

The VMware Host-Guest Filesystem allows for shared folders between the host OS
and the guest OS in a Fusion or Workstation virtual environment. Do you wish
to enable this feature? [yes] yes
```

The terminal shows the configuration process for the VMware Host-Guest Filesystem. It lists several modules that have already been installed and are not being modified. At the end, it asks if the user wants to enable the VMware Host-Guest Filesystem, and the user has responded "yes".

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**

```
ubuntu@ubuntu: ~  
The module vsock has already been installed on this system by another installer  
or package and will not be modified by this installer.  
The module vmxnet3 has already been installed on this system by another  
installer or package and will not be modified by this installer.  
The module pvscsi has already been installed on this system by another  
installer or package and will not be modified by this installer.  
The module vmmemctl has already been installed on this system by another  
installer or package and will not be modified by this installer.  
The VMware Host-Guest Filesystem allows for shared folders between the host OS  
and the guest OS in a Fusion or Workstation virtual environment. Do you wish  
to enable this feature? [yes] yes  
  
The vmxnet driver is no longer supported on kernels 3.3 and greater. Please  
upgrade to a newer virtual NIC. (e.g., vmxnet3 or e1000e)  
The vmblock enables dragging or copying files between host and guest in a  
Fusion or Workstation virtual environment. Do you wish to enable this feature?  
[yes] yes
```

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

```
ubuntu@ubuntu: ~  
installer or package and will not be modified by this installer.  
The module vmmemctl has already been installed on this system by another  
installer or package and will not be modified by this installer.  
The VMware Host-Guest Filesystem allows for shared folders between the host OS  
and the guest OS in a Fusion or Workstation virtual environment. Do you wish  
to enable this feature? [yes] yes  
  
The vmxnet driver is no longer supported on kernels 3.3 and greater. Please  
upgrade to a newer virtual NIC. (e.g., vmxnet3 or e1000e)  
The vmblock enables dragging or copying files between host and guest in a  
Fusion or Workstation virtual environment. Do you wish to enable this feature?  
[yes] yes  
  
VMware automatic kernel modules enables automatic building and installation of  
VMware kernel modules at boot that are not already present. This feature can  
be enabled/disabled by re-running vmware-config-tools.pl.  
Would you like to enable VMware automatic kernel modules?  
[yes] yes
```

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

```
ubuntu@ubuntu: ~  
The VMware Host-Guest Filesystem allows for shared folders between the host OS  
and the guest OS in a Fusion or Workstation virtual environment. Do you wish  
to enable this feature? [yes] yes  
  
The vmxnet driver is no longer supported on kernels 3.3 and greater. Please  
upgrade to a newer virtual NIC. (e.g., vmxnet3 or e1000e)  
  
The vmblock enables dragging or copying files between host and guest in a  
Fusion or Workstation virtual environment. Do you wish to enable this feature?  
[yes] yes  
  
VMware automatic kernel modules enables automatic building and installation of  
VMware kernel modules at boot that are not already present. This feature can  
be enabled/disabled by re-running vmware-config-tools.pl.  
  
Would you like to enable VMware automatic kernel modules?  
[yes] yes  
  
Thinprint provides driver-free printing. Do you wish to enable this feature?  
[yes] yes
```

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

```
ubuntu@ubuntu: ~  
upgrade to a newer virtual NIC. (e.g., vmxnet3 or e1000e)  
  
The vmblock enables dragging or copying files between host and guest in a  
Fusion or Workstation virtual environment. Do you wish to enable this feature?  
[yes] yes  
  
VMware automatic kernel modules enables automatic building and installation of  
VMware kernel modules at boot that are not already present. This feature can  
be enabled/disabled by re-running vmware-config-tools.pl.  
  
Would you like to enable VMware automatic kernel modules?  
[yes] yes  
  
Thinprint provides driver-free printing. Do you wish to enable this feature?  
[yes] yes  
  
Disabling timer-based audio scheduling in pulseaudio.  
  
Do you want to enable Guest Authentication (vgauth)? Enabling vgauth is needed  
if you want to enable Common Agent (caf). [yes] yes
```

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

```
ubuntu@ubuntu:~  
Fusion or Workstation virtual environment. Do you wish to enable this feature?  
[yes] yes  
  
VMware automatic kernel modules enables automatic building and installation of  
VMware kernel modules at boot that are not already present. This feature can  
be enabled/disabled by re-running vmware-config-tools.pl.  
  
Would you like to enable VMware automatic kernel modules?  
[yes] yes  
  
Thinprint provides driver-free printing. Do you wish to enable this feature?  
[yes] yes  
  
Disabling timer-based audio scheduling in pulseaudio.  
  
Do you want to enable Guest Authentication (vgauth)? Enabling vgauth is needed  
if you want to enable Common Agent (caf). [yes] yes  
  
Do you want to enable Common Agent (caf)? [yes] yes
```

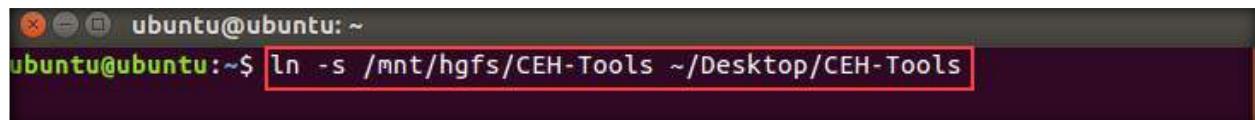
12. Now, the installation was successful, type **reboot** and press **Enter** to restart the Ubuntu machine

```
ubuntu@ubuntu:~  
update-initramfs: Generating /boot/initrd.img-4.10.0-28-generic  
  
NOTE: both /etc/vmware-tools/GuestProxyData/server/key.pem and  
/etc/vmware-tools/GuestProxyData/server/cert.pem already exist.  
They are not generated again. To regenerate them by force,  
use the "vmware-guestproxycerttool -g -f" command.  
  
The configuration of VMware Tools 10.2.0 build-7259539 for Linux for this  
running kernel completed successfully.  
  
You must restart your X session before any mouse or graphics changes take  
effect.  
  
To enable advanced X features (e.g., guest resolution fit, drag and drop, and  
file and text copy/paste), you will need to do one (or more) of the following:  
1. Manually start /usr/bin/vmware-user  
2. Log out and log back into your desktop session  
3. Restart your X session.  
  
Enjoy,  
--the VMware team  
ubuntu@ubuntu:~$ reboot
```

13. Login to the Ubuntu machine

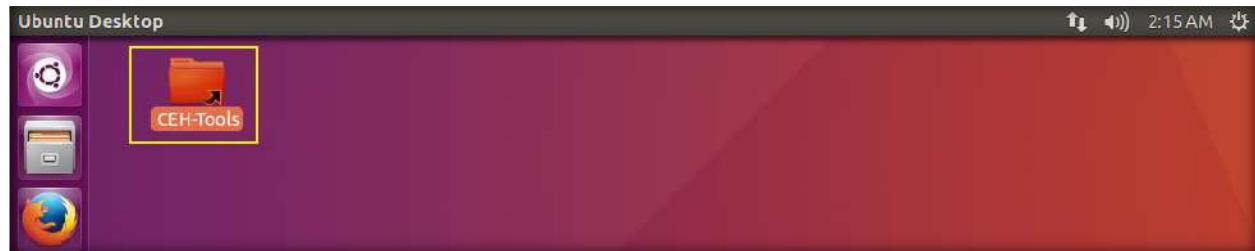
14. Now, we need to mount the shared directory, open a terminal window and type **ln -s /mnt/hgfs/CEH-Tools ~/Desktop/CEH-Tools** press **Enter**

15. This will mount the shared directory on the Desktop



```
ubuntu@ubuntu: ~
ubuntu@ubuntu:~$ ln -s /mnt/hgfs/CEH-Tools ~/Desktop/CEH-Tools
```

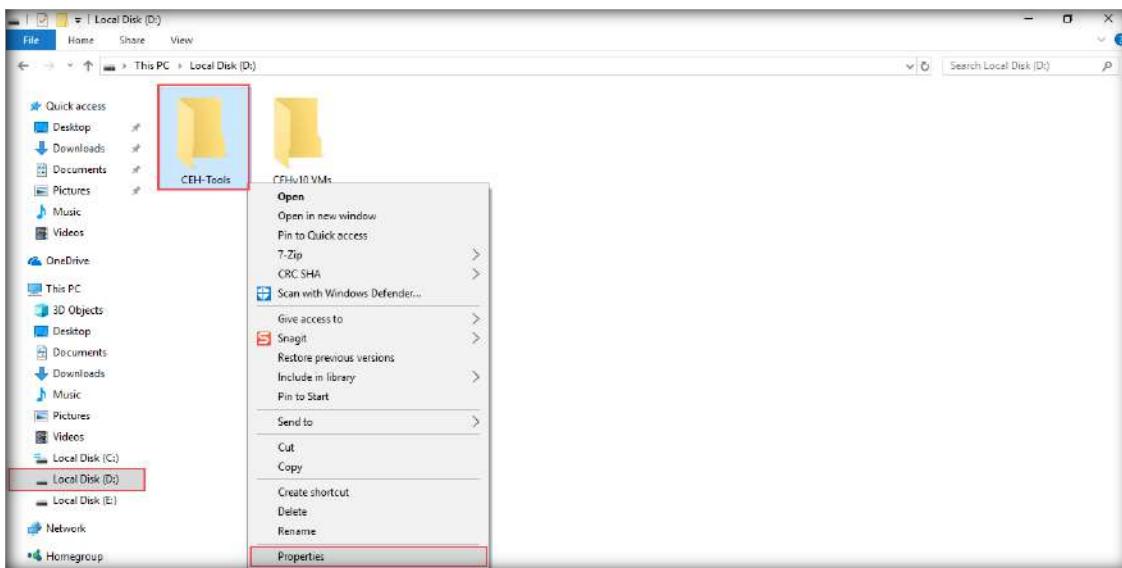
16. Shared CEH-Tools directory



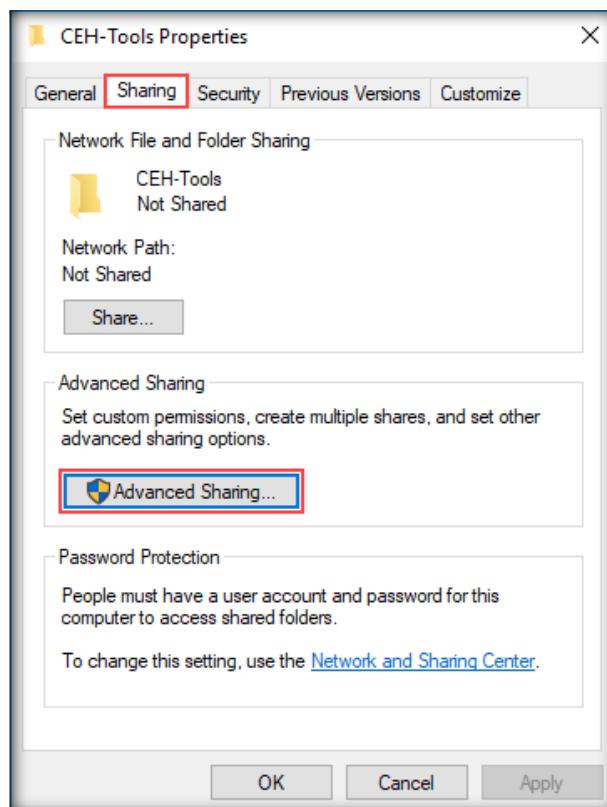
[\[Back to Configuration Task Outline\]](#)

CT#13: Mapping CEH-Tools with Android Machine

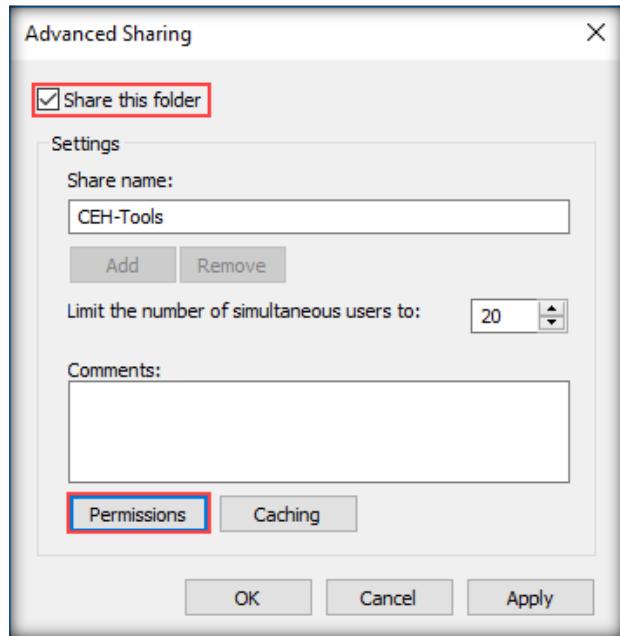
1. Before performing this configuring task for Android, in your host machine navigate to the **CEH-Tools** folder location
2. Right-click on CEH-Tools folder, and click **Properties** from the context menu



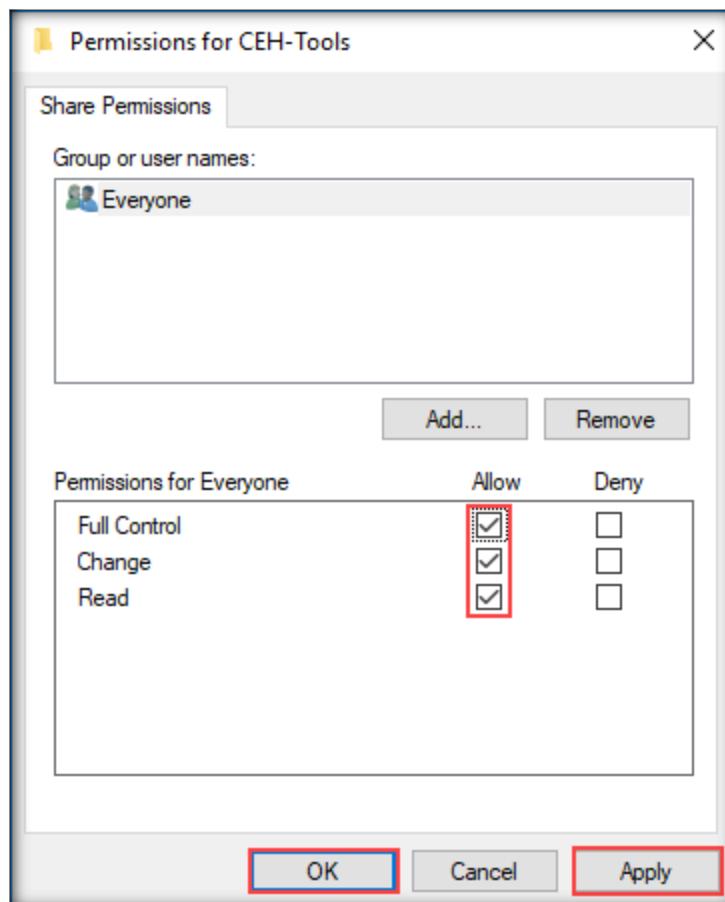
3. CEH-Tools Properties window appears, click **Sharing** tab, and click **Advanced Sharing** under Advanced Sharing section



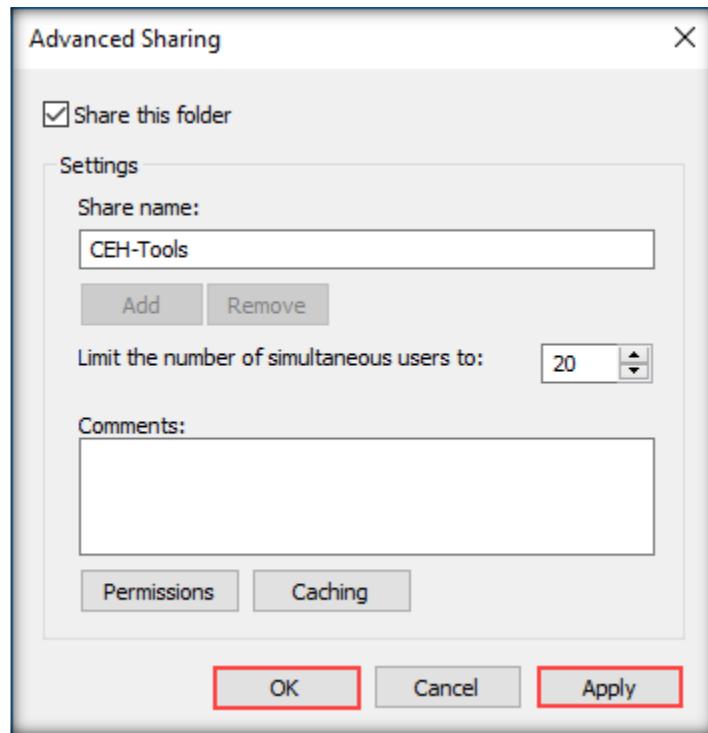
4. Advanced Sharing pop-up appears, check **Share this folder** option, and click **Permissions** as shown in the screenshot



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



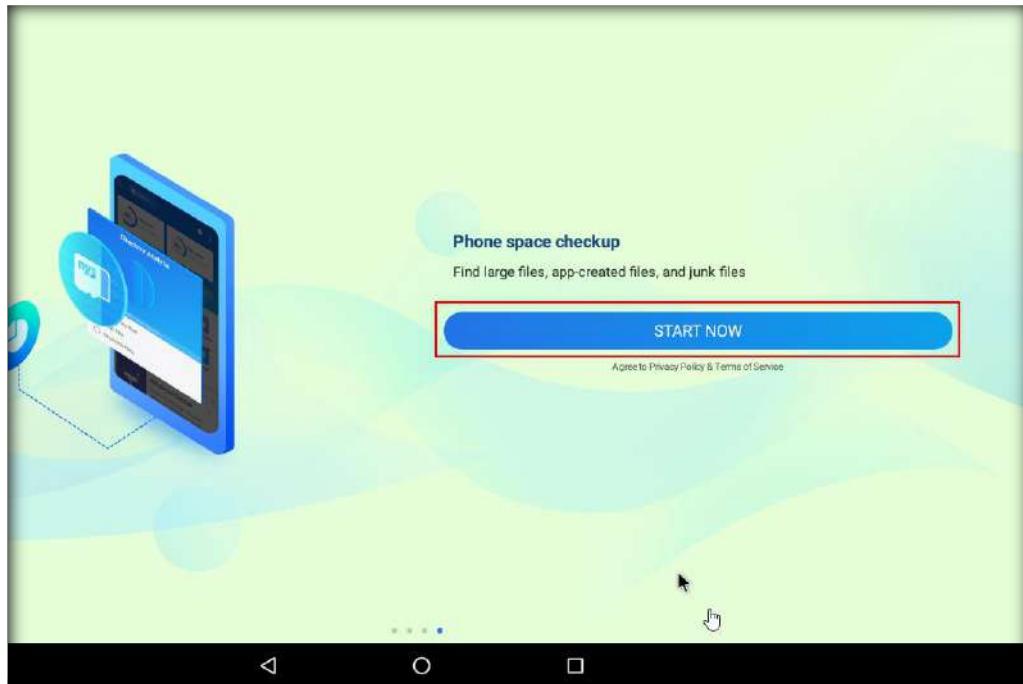
6. Click **Apply** and **OK** in the Advanced Sharing pop-up.



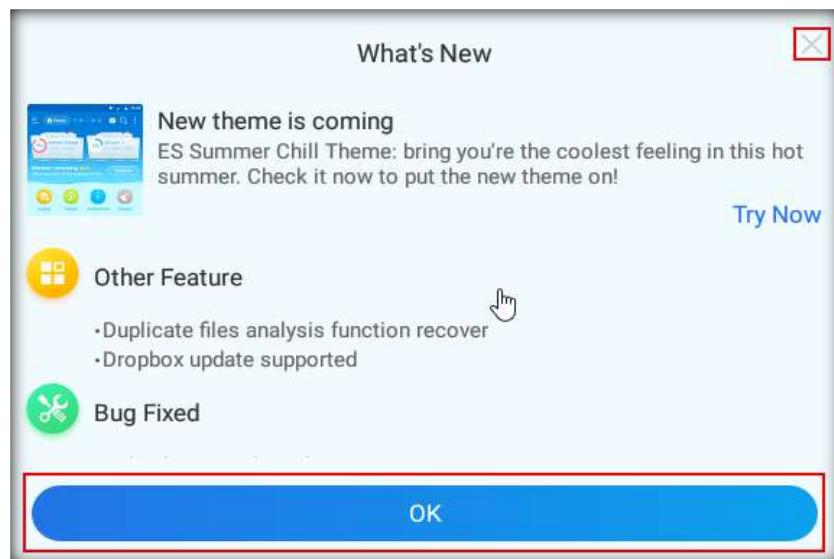
7. Click **Close** on the CEH-Tools Properties window
8. Power on **Android** machine from VMware Workstation
9. Click **ES File Explorer** icon present on the **Home** screen (hold the screen with mouse and move to left hand side)



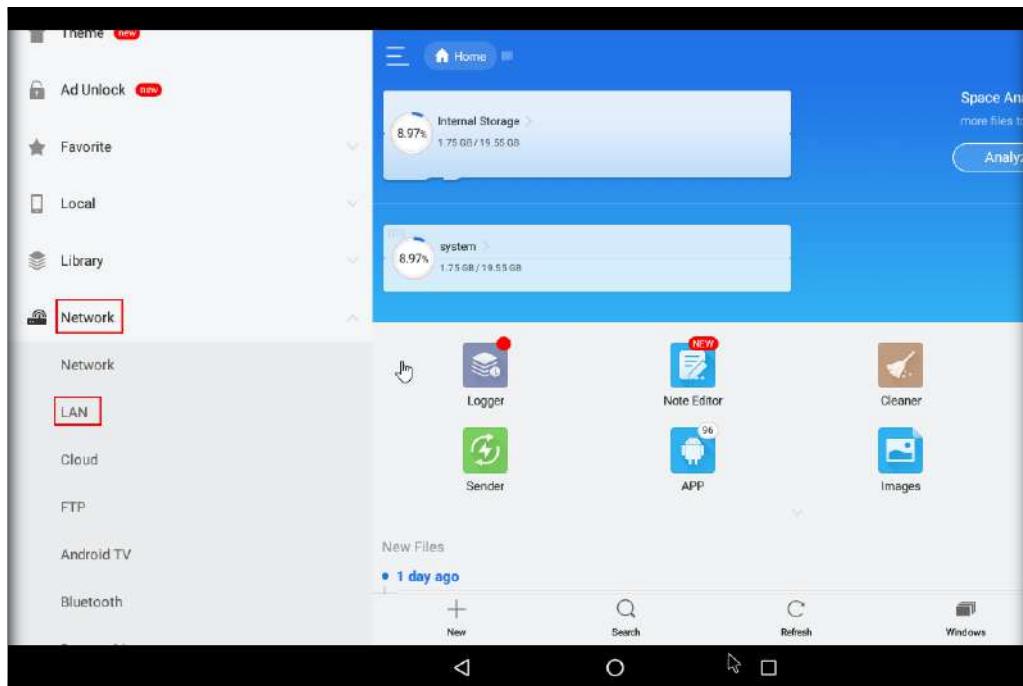
10. If ES File Explorer usage options and features appears, toggle the screen to left hand-side and click **START NOW** as shown in the screenshot



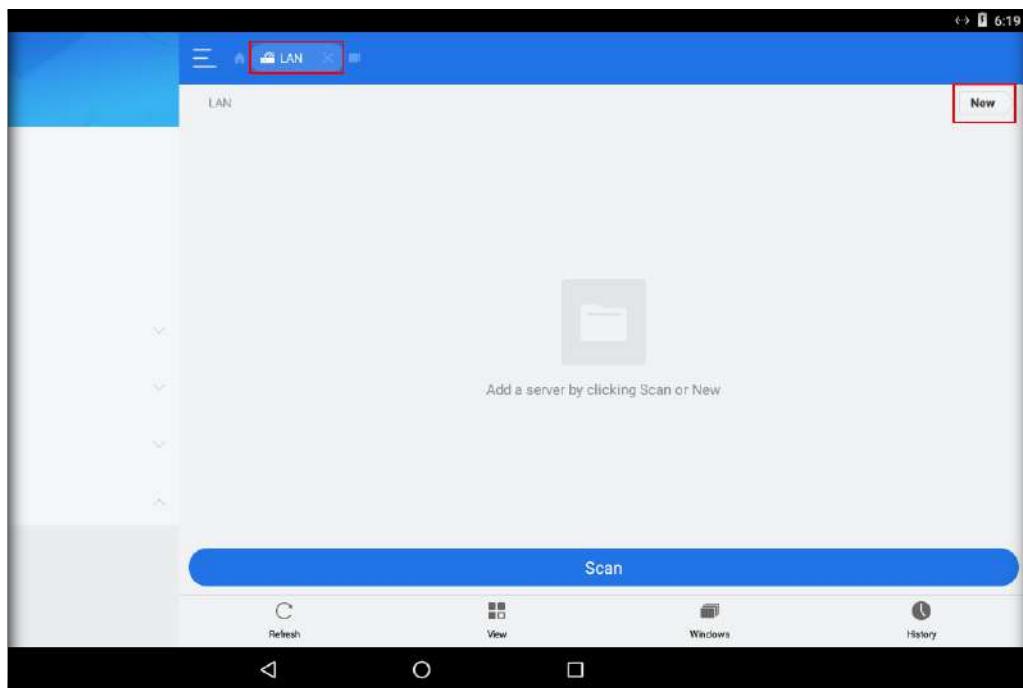
11. ES File Explorer window appears along with What's New pop-up, click **X** or **OK** to close the pop-up



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**

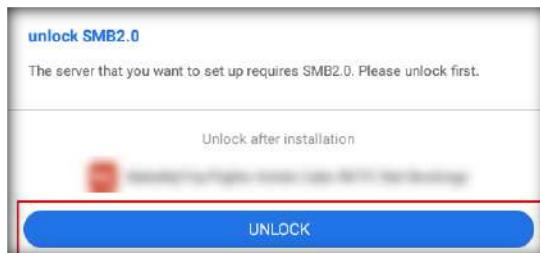


14. Server pop-up appears, enter your **Host machine IP address** in the Server field, and enter the credentials of your host machine and click **OK**

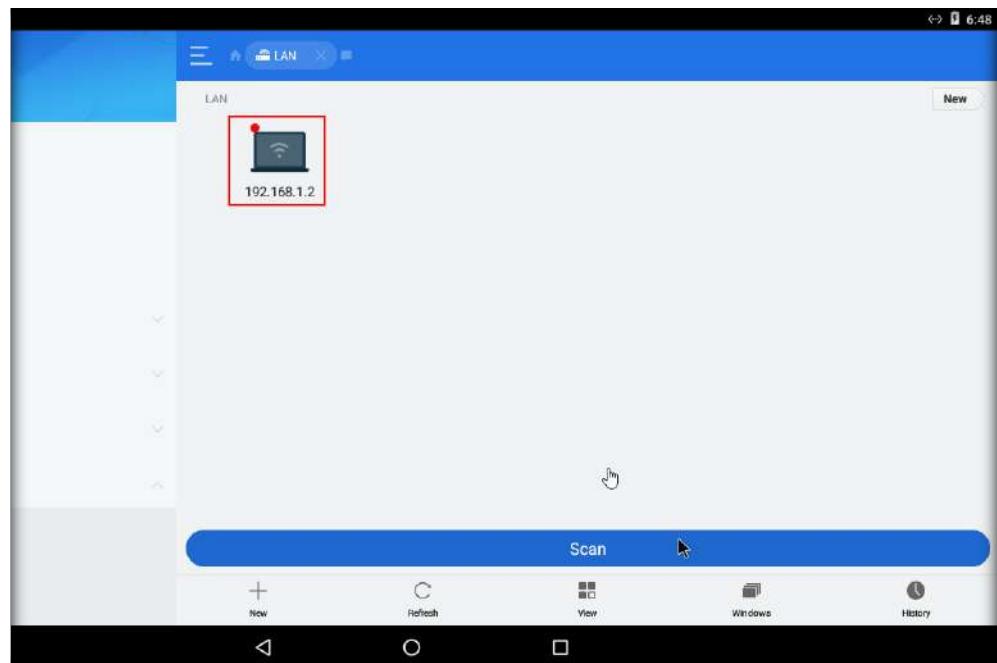
Note: IP address will vary in your lab environment



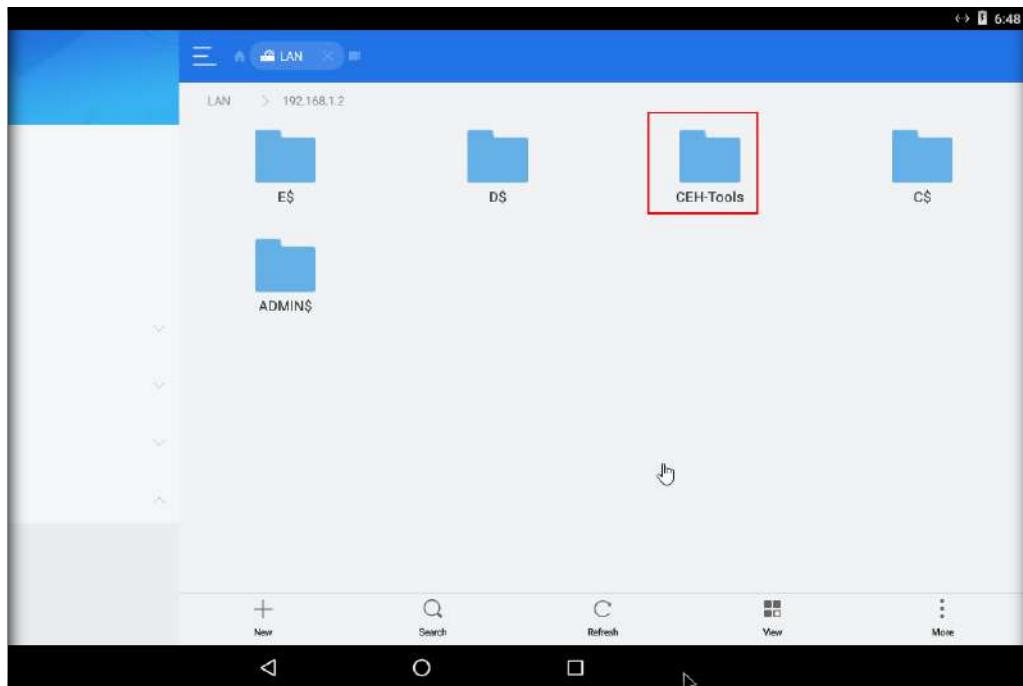
15. If unlock SMB2.0 pop-up appears, click UNLOCK to install the third party application
16. This will redirect you to play store window, and install the third party application



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

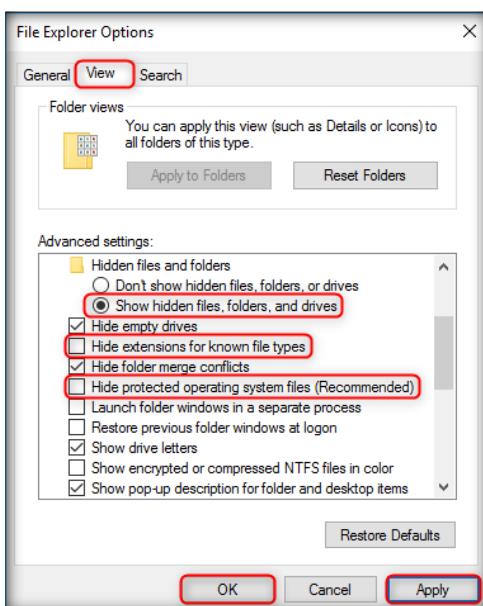
1. Navigate to **Z:\CEH-Tools\CEHv10 Lab Prerequisites\WinRAR** folder
2. Alternatively, you can also download the latest version of **WinRAR** from **Aspen Portal**
3. Double click on .exe setup file to begin the installation
4. **WinRAR setup** window appears
5. In the WinRAR setup window, click **Install**
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

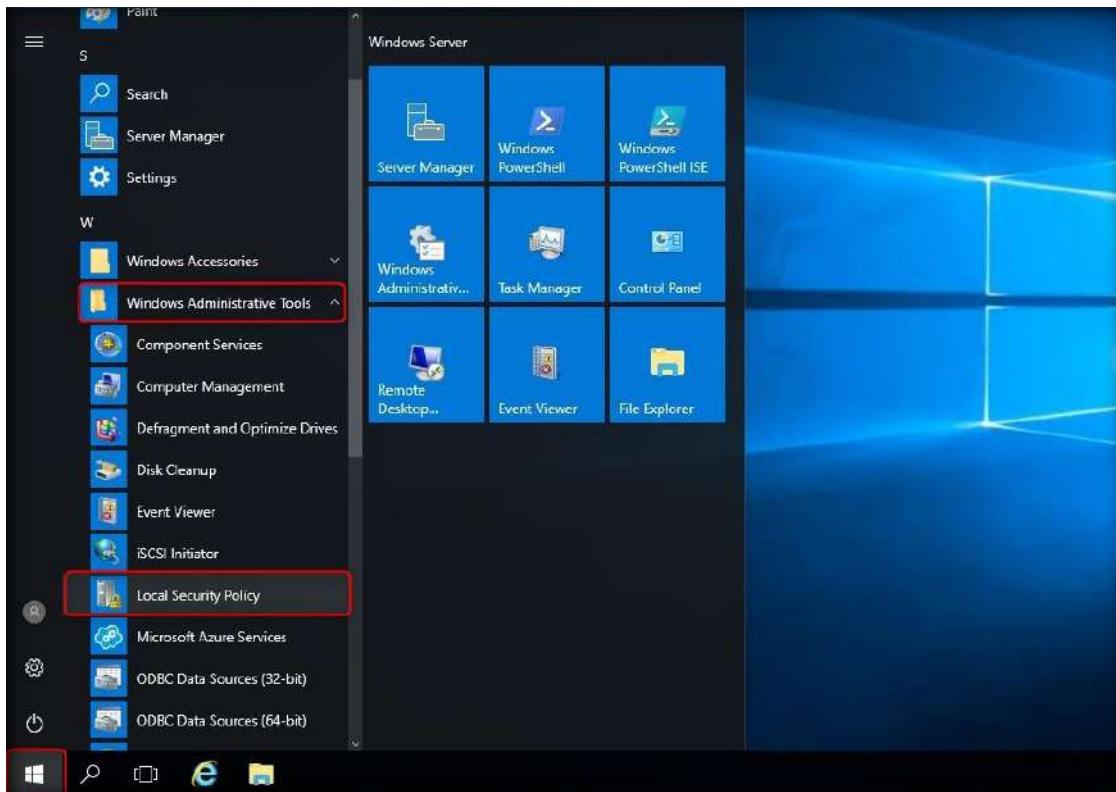
1. Navigate to **Z:\CEH-Tools\CEHv10 Lab Prerequisites** in guest operating systems
2. Open **Web Browsers** folder
3. Follow **wizard-driven** installation steps to install **Firefox** and **Chrome** web browsers
4. You can also download **latest** version of web browsers from respective **vendors**

[\[Back to Configuration Task Outline\]](#)

CT#18: Removing Password Complexity from Guest Operating Systems

Remove Password Complexity in Windows Server 2016 (Virtual machine)

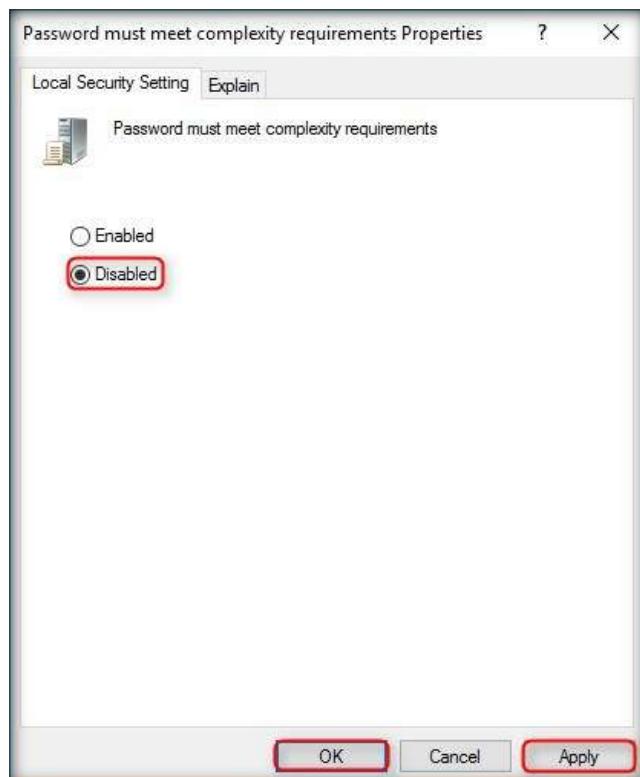
1. To remove password complexity in Windows Server 2016 virtual machine
2. In the Windows Server 2016 virtual machine, click the **Windows** icon at the lower left corner of the screen
3. **Start** menu appears, click **Windows Administrative Tools → Local Security Policy**



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)

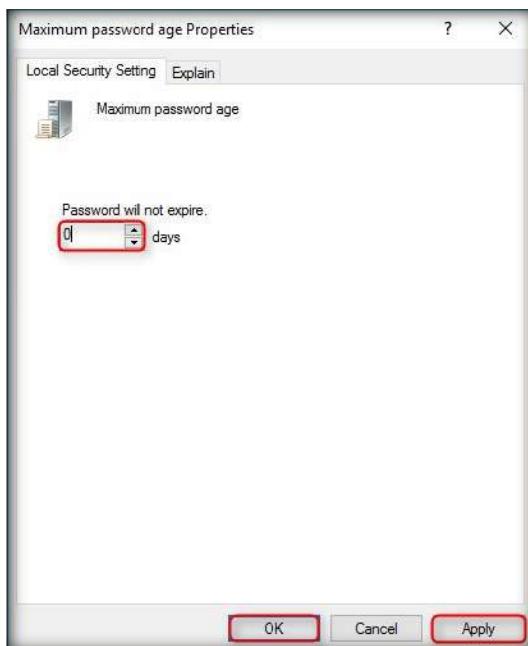
1. In the right pane double-click **Maximum password age**

The screenshot shows the 'Local Security Policy' snap-in window. The left pane displays a tree view of security settings: 'Security Settings' > 'Account Policies' > 'Password Policy' > 'Account Lockout Policy'. The right pane lists various policies with their current settings:

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

The 'Maximum password age' row is selected and highlighted with a red border.

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)

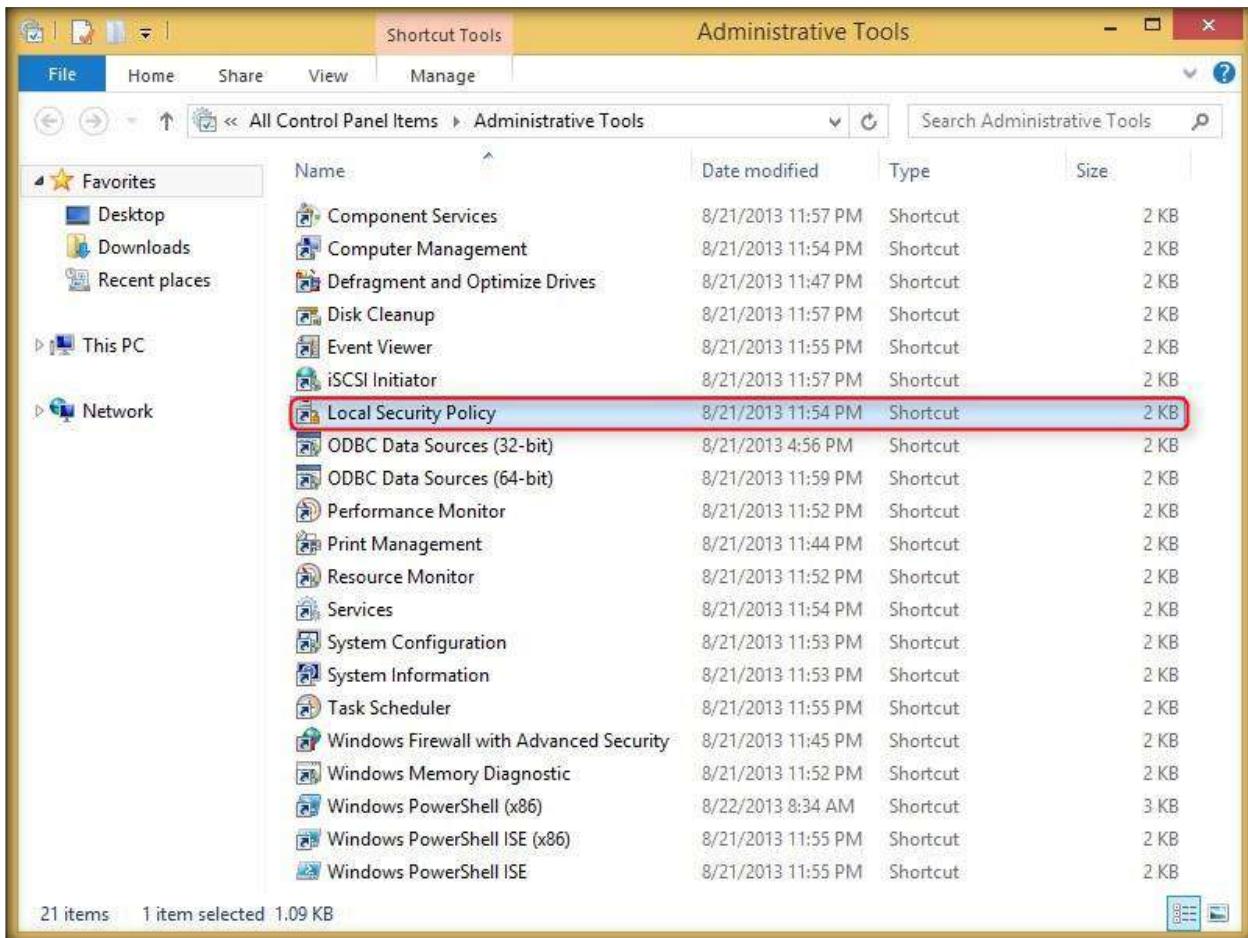
1. To remove password complexity in Windows 8 virtual machine, Power on and **Log On** to Windows 8 virtual machine
2. In the Windows 8 virtual machine, open **Control Panel**
3. Control Panel window appears on the screen, select **Small icons** from the **Category** drop down list to see all the control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



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



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



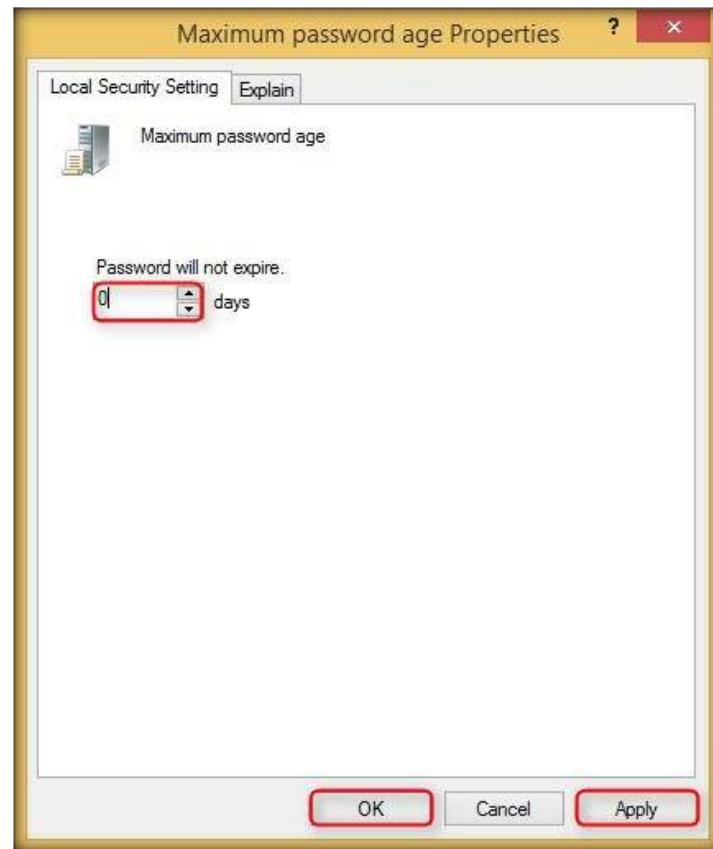
6. **Local Security Policy** window appears, expand **Account Policies** node, click **Password Policy** in the left pane and in the right pane double-click **Password must meet complexity requirements**
 7. **Password must meet complexity requirements Properties** window appears, select **Disabled**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

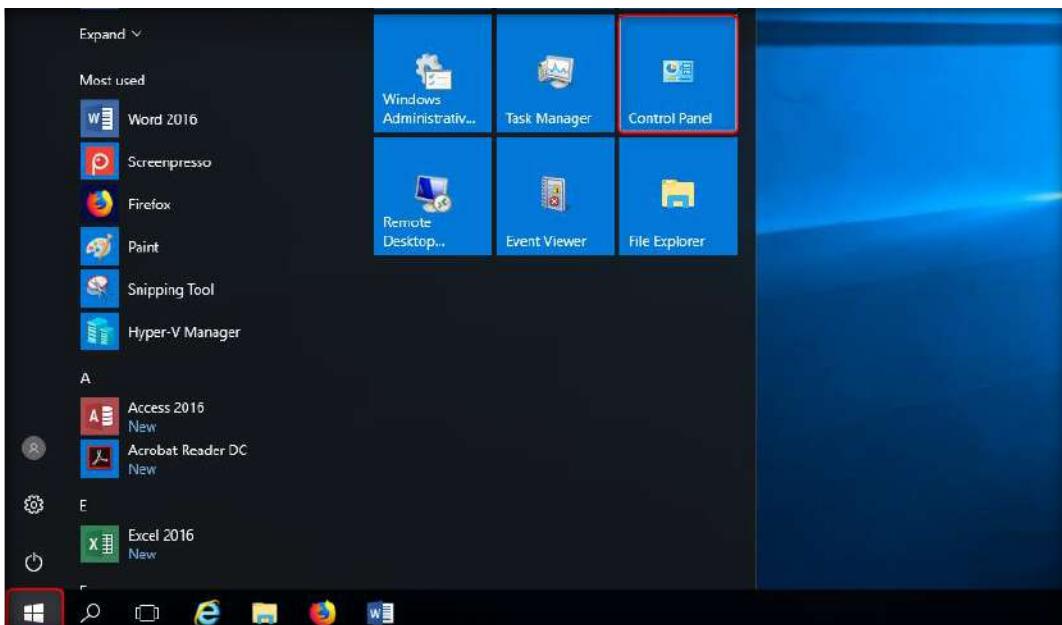
Create user accounts in Windows Server 2016, Windows 10, and Windows 8.

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

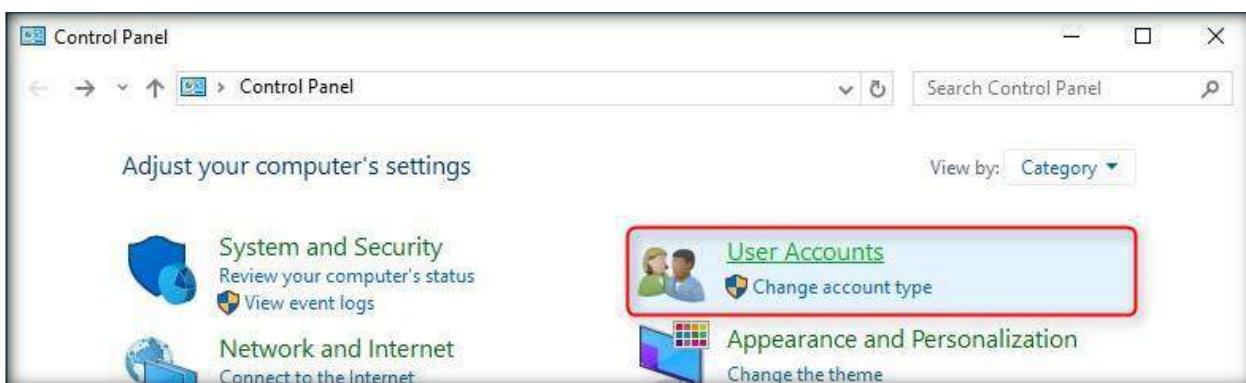
- (i) Username: **Martin**; Password: **apple**
- (ii) Username: **Jason**; Password: **qwerty**
- (iii) Username: **Shiela**; Password: **test**

Creating User Accounts in Windows Server 2016

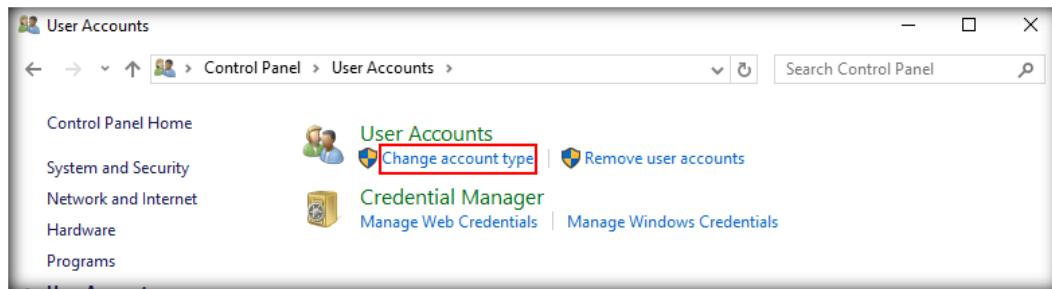
1. To create a user account in Windows Server 2016, click **Start** menu icon at the lower left corner of the screen and click **Control Panel**



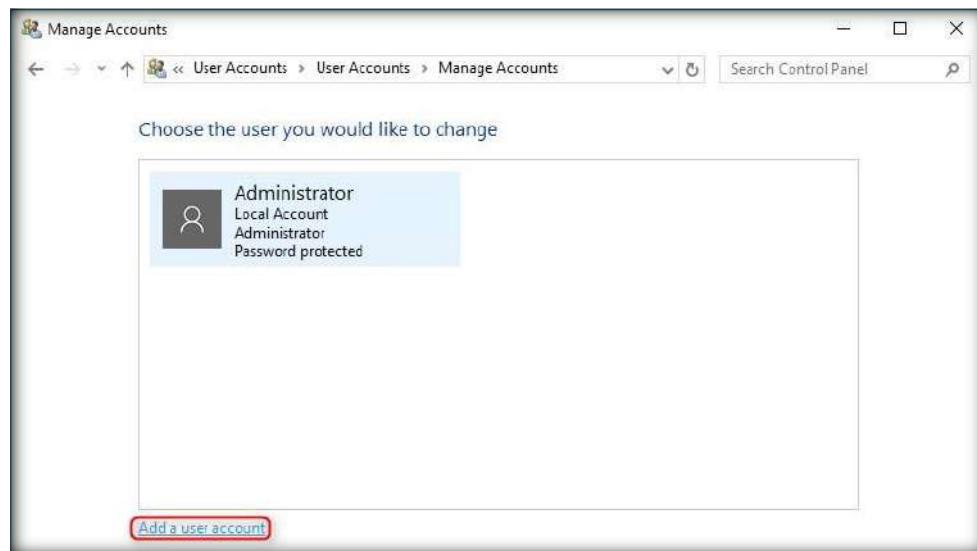
2. **Control Panel** window appears click **User Accounts**



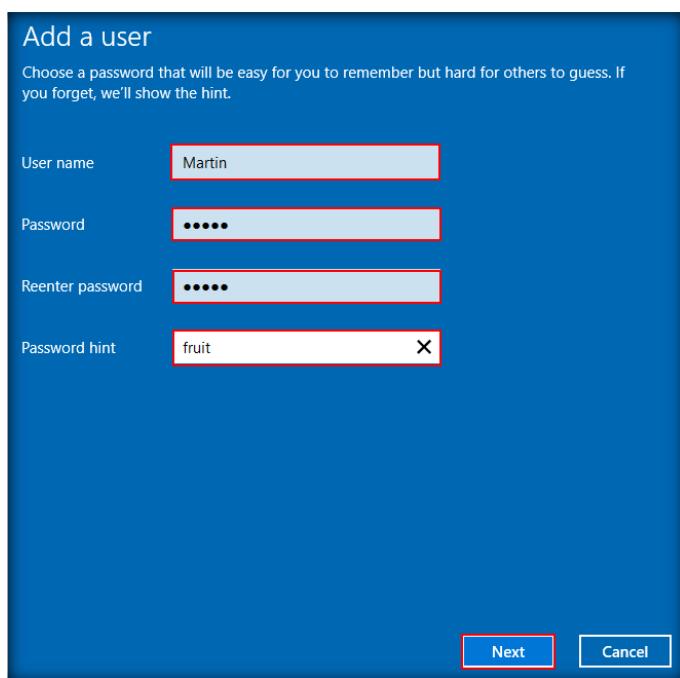
3. In User Accounts window, click **Change account type** or **Remove user accounts** link



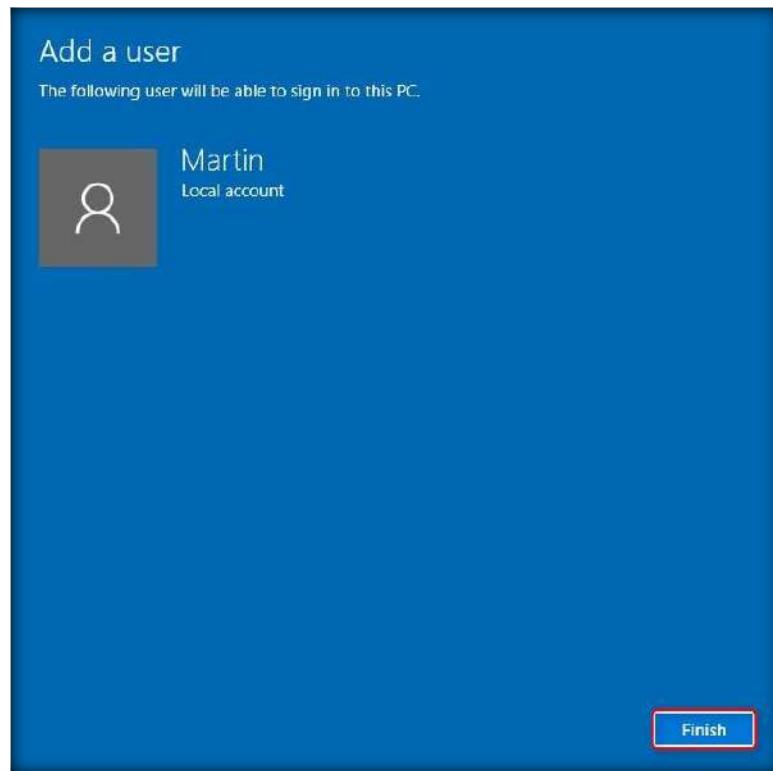
4. Click **Add a user account** in Manage Accounts window



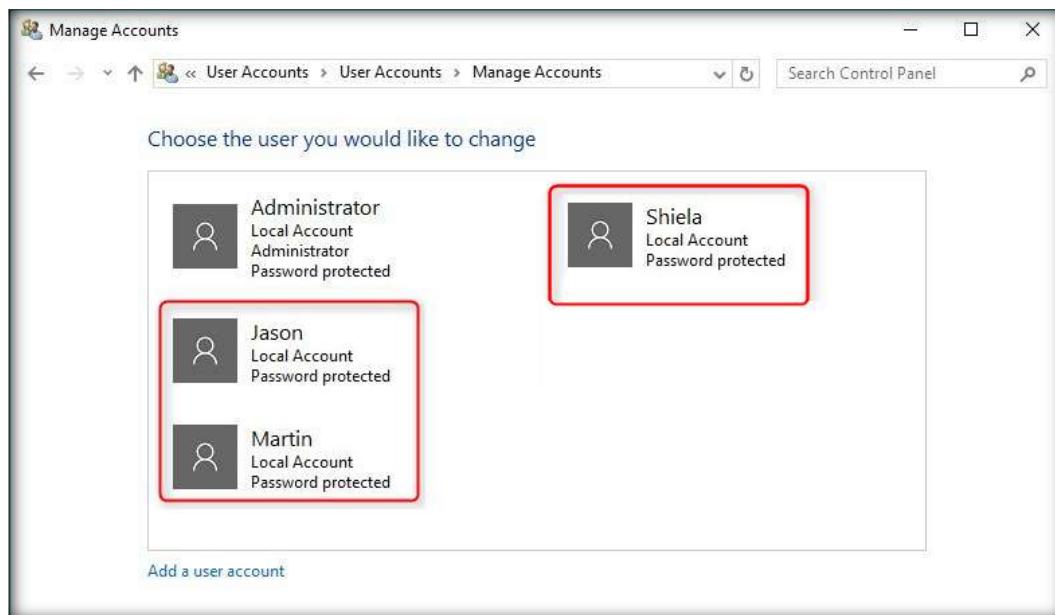
5. **Add a user** wizard appears, fill in the following fields and click **Next**



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



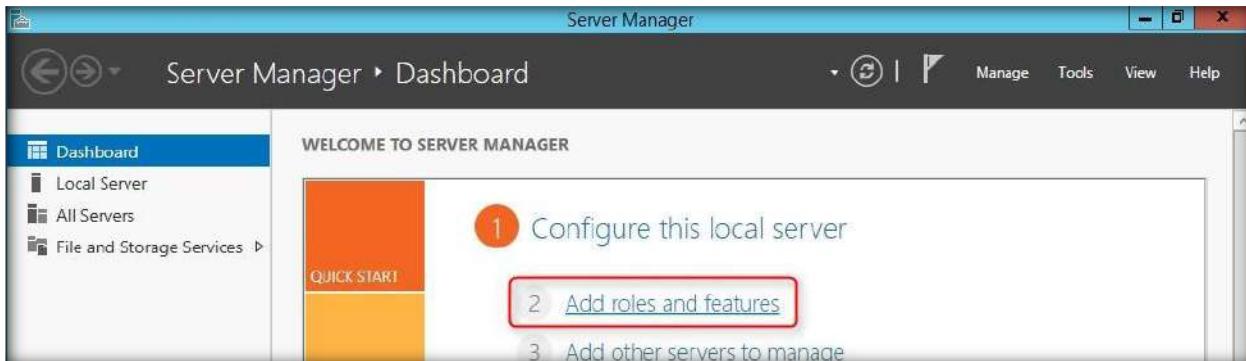
Note: Create these three user accounts in **Windows 10** and **Windows 8** virtual machines.

[\[Back to Configuration Task Outline\]](#)

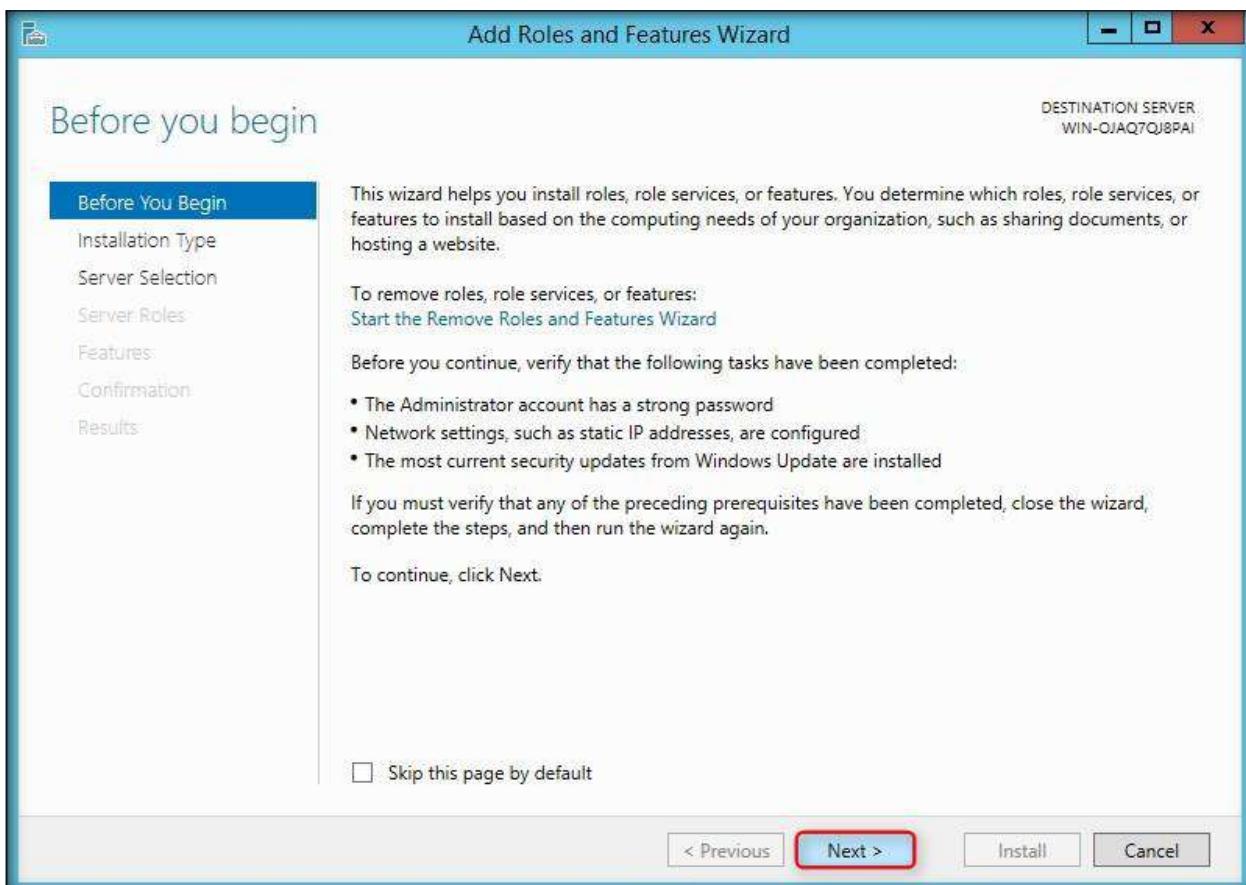
CT#20: Install Active Directory and Create User Accounts in Windows Server 2012

Install Active Directory in Windows Server 2012 virtual machine

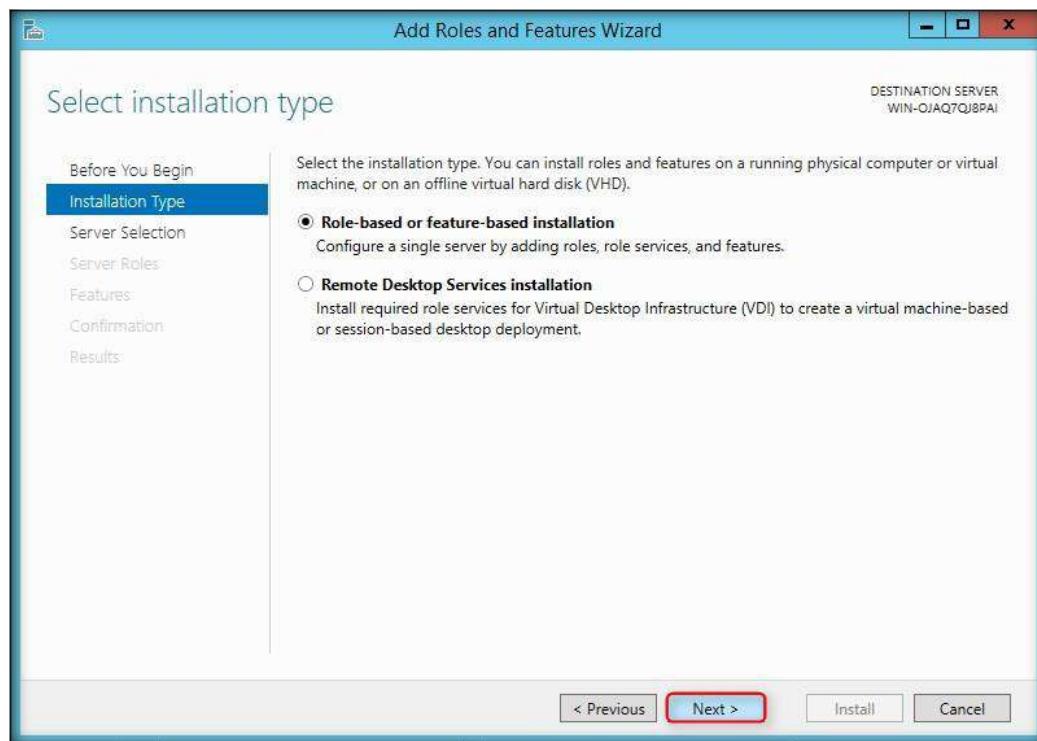
1. To install Active Directory (AD) in Windows Server 2012 machine, click Windows Server 2012 machine in the left pane and click Power on this virtual machine and then login to the machine
2. After successful logon, Server Manager window appears, click **Add roles and features** from the Server Manager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



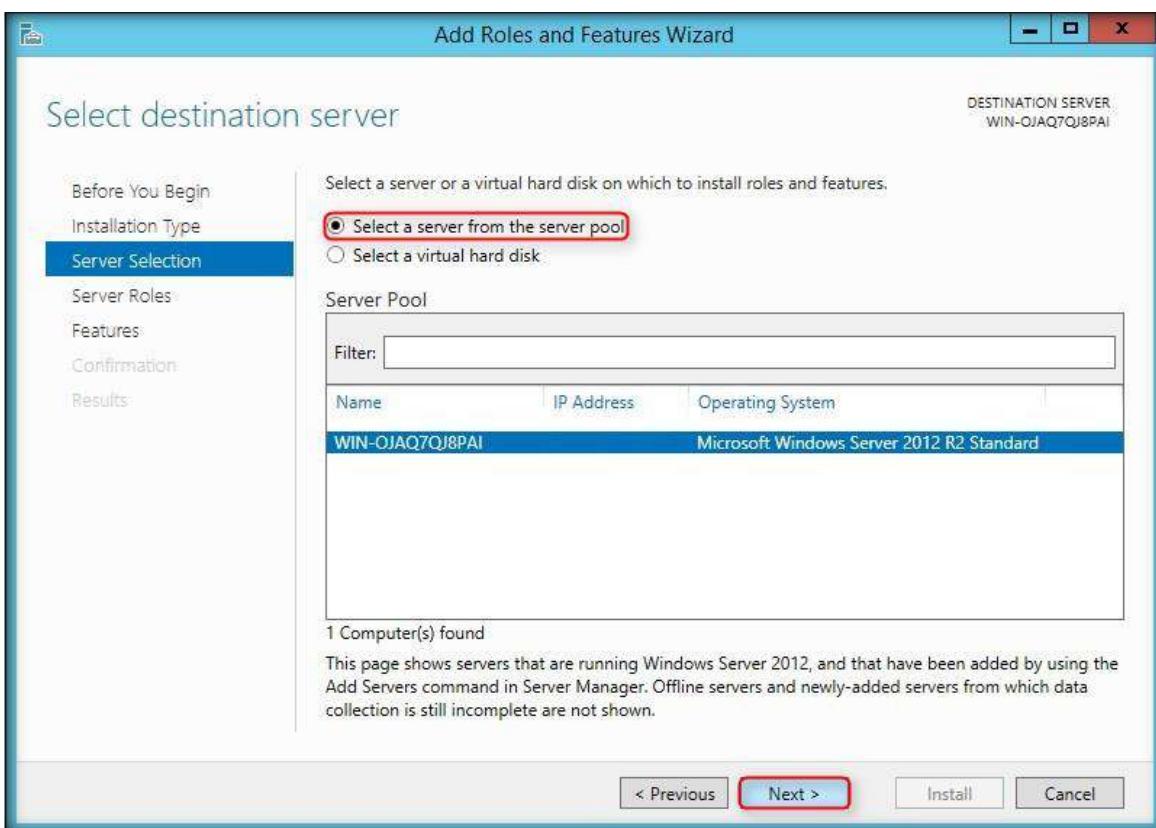
3. Before You Begin wizard appears click **Next** to continue



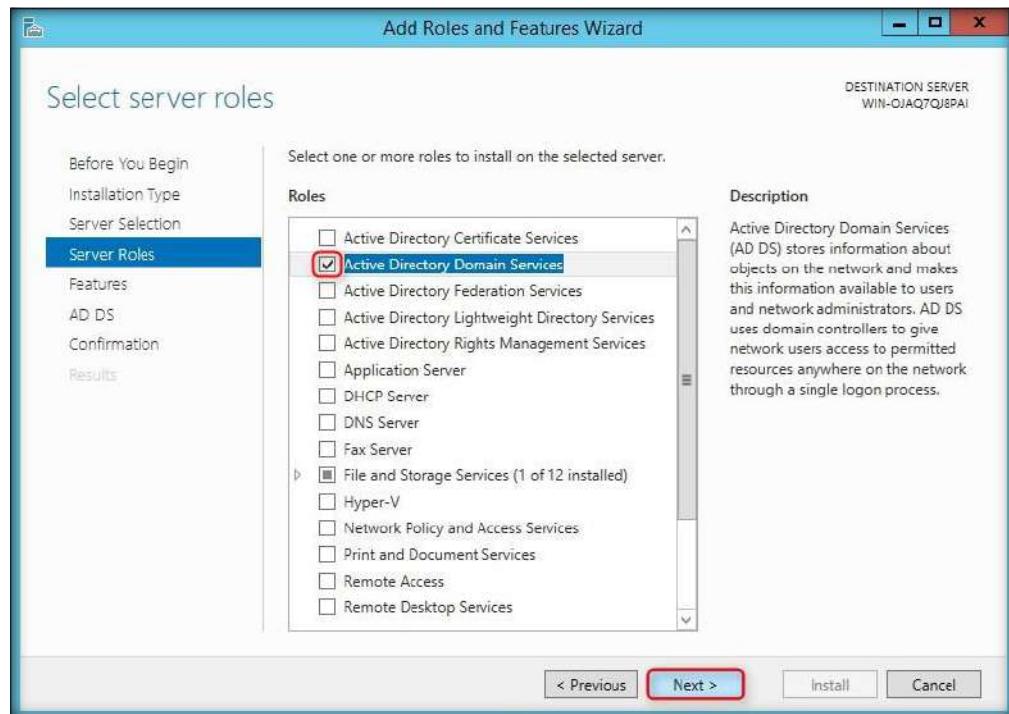
4. Select Installation type section appears, leave the options to default and click **Next**



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

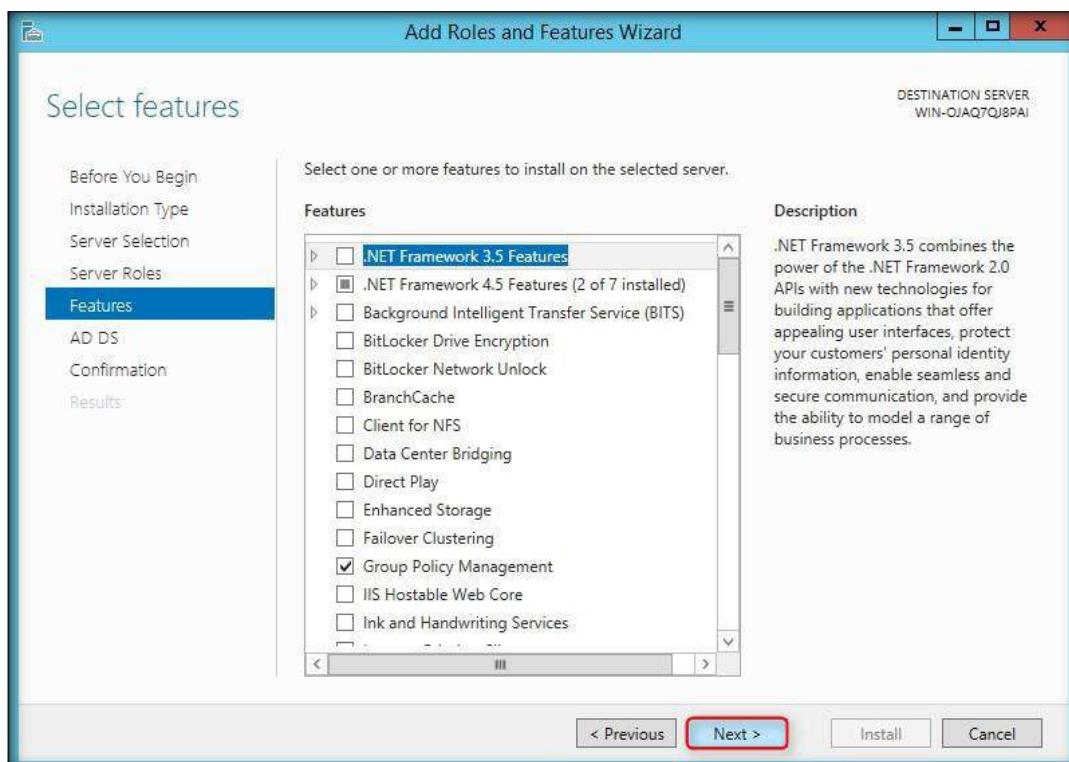


6. Check Active Directory Domain Services from Roles section in Select Server Roles wizard and click Next

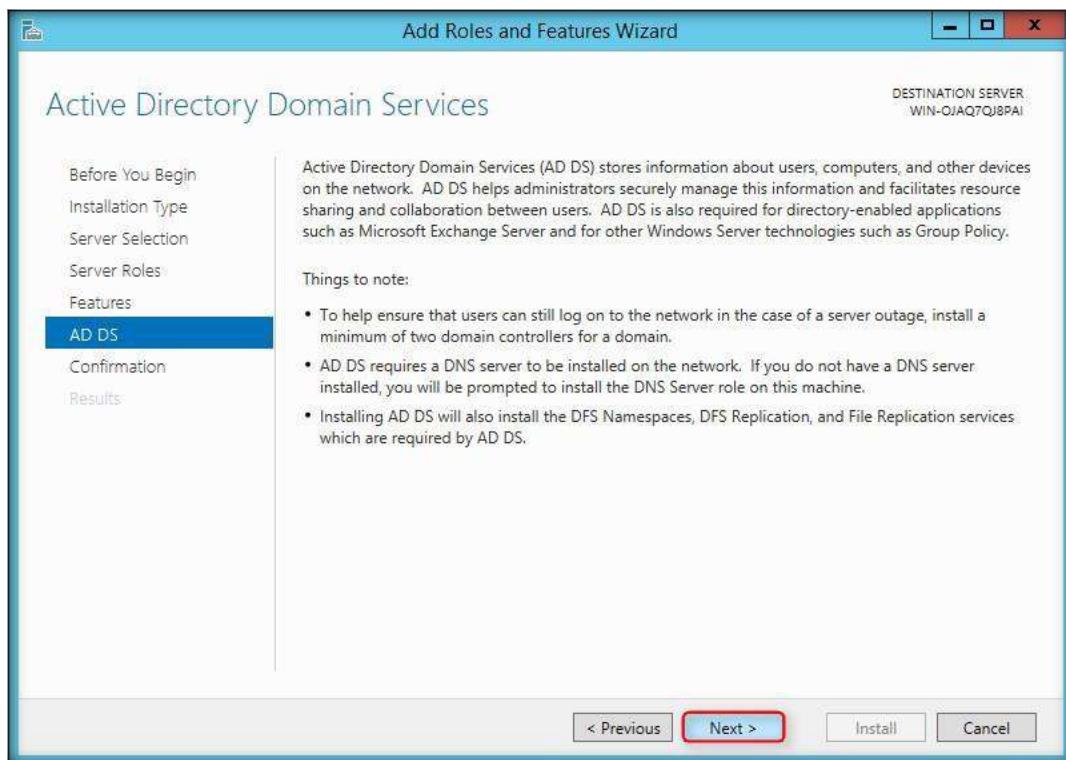


Note: If Add Roles and Features Wizard pop-up appears, click **Add Features**

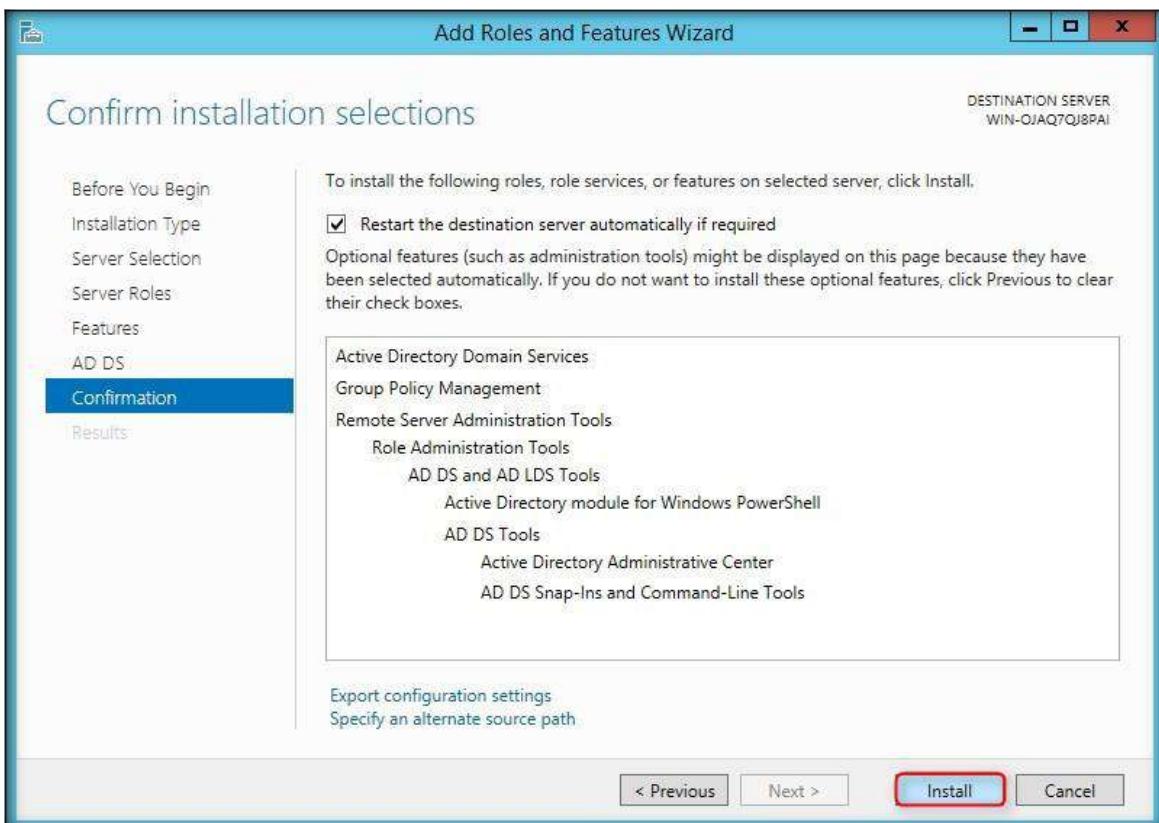
7. In Select Features section click **Next** to continue



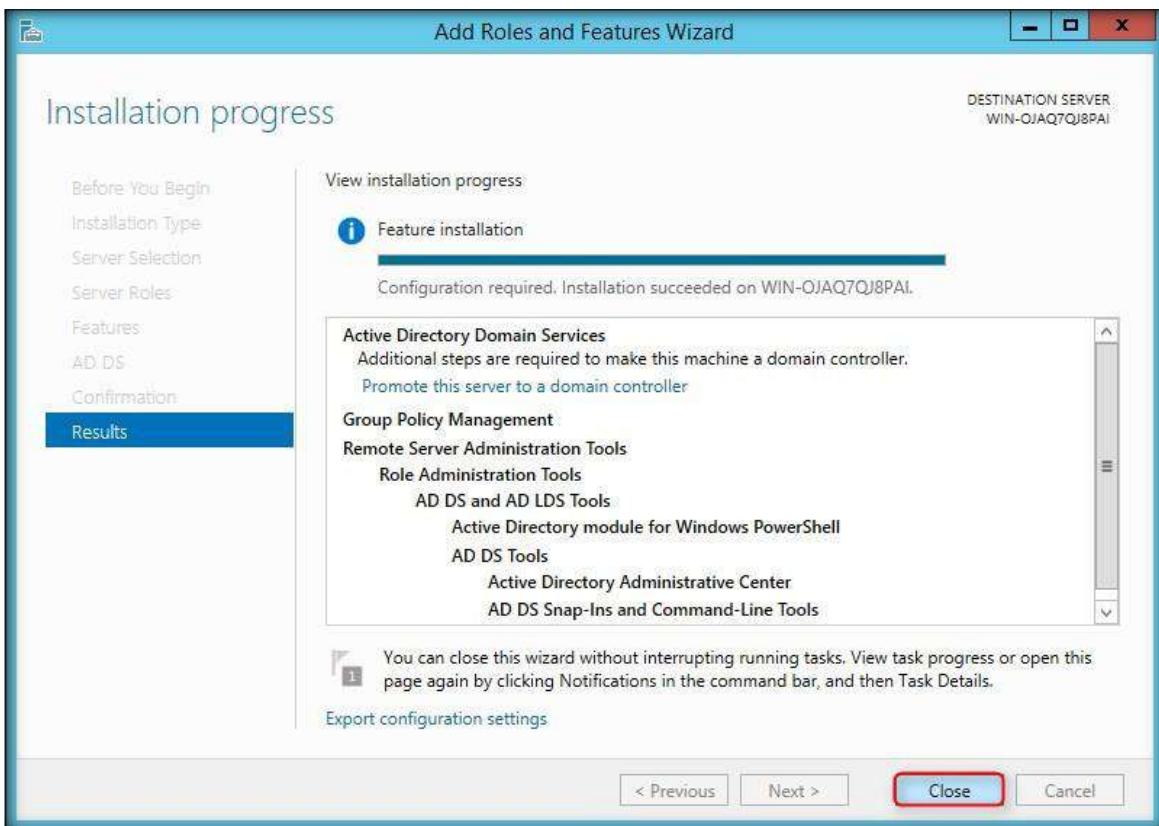
8. Active Directory Domain Services section appears click **Next** to continue



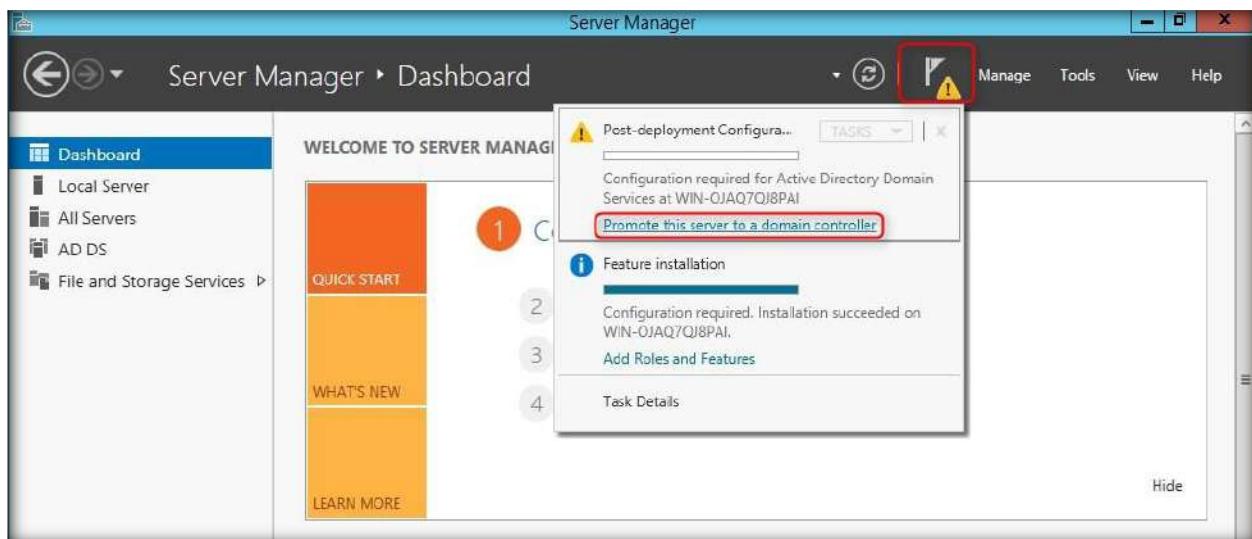
9. **Confirm Installation Selections** section appears, click **Install**



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

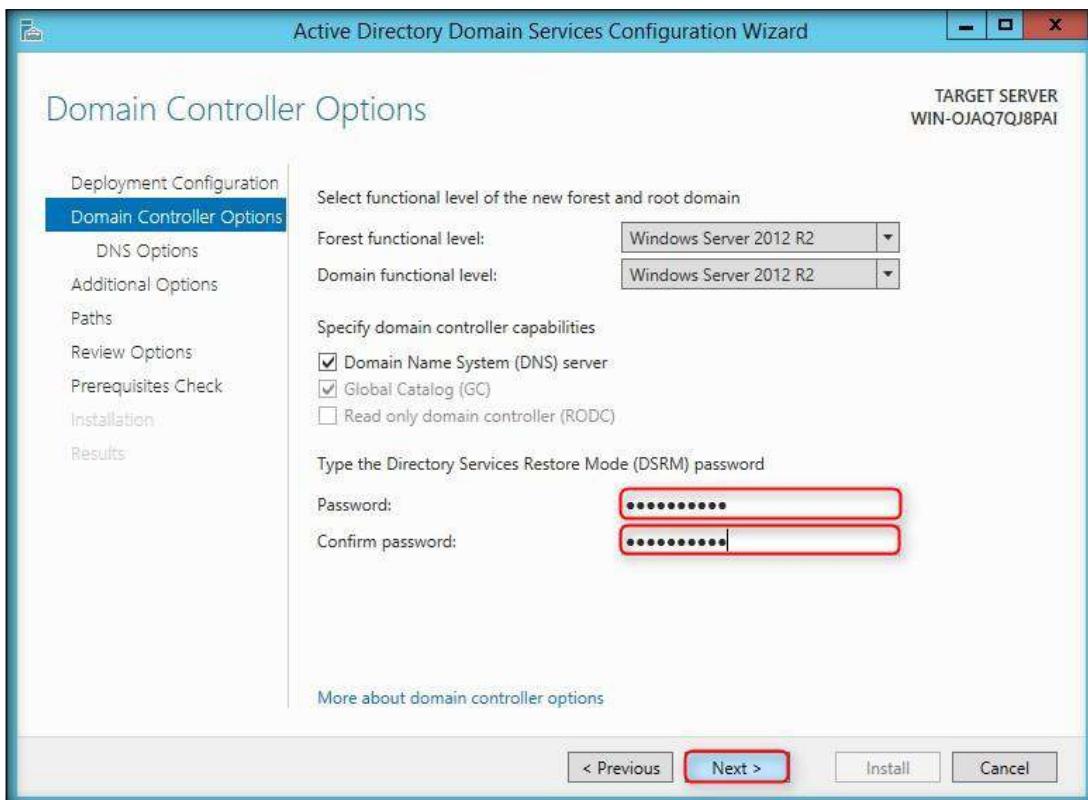


11. In the Server Manager Dashboard, click the **Flag** icon and click **Promote this server to a domain controller** link as shown in the screenshot below

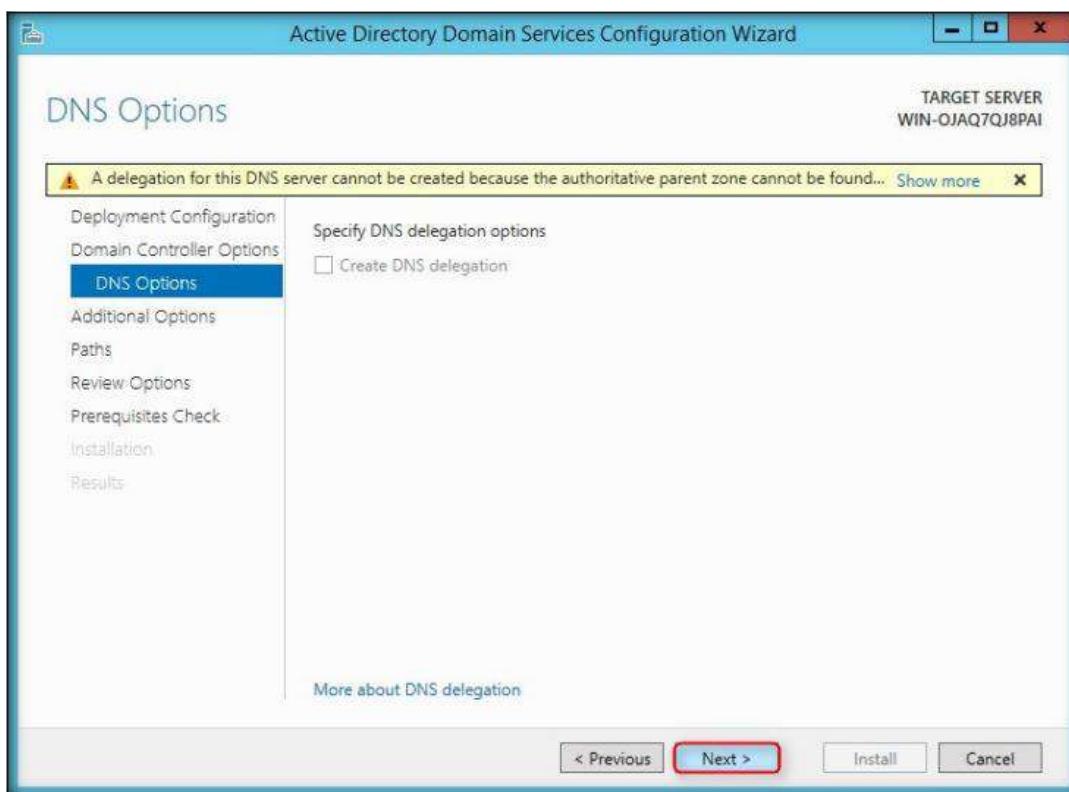


12. Active Directory Domain Services Configuration Wizard window appears, fill in the following Password and Confirm password field and click Next

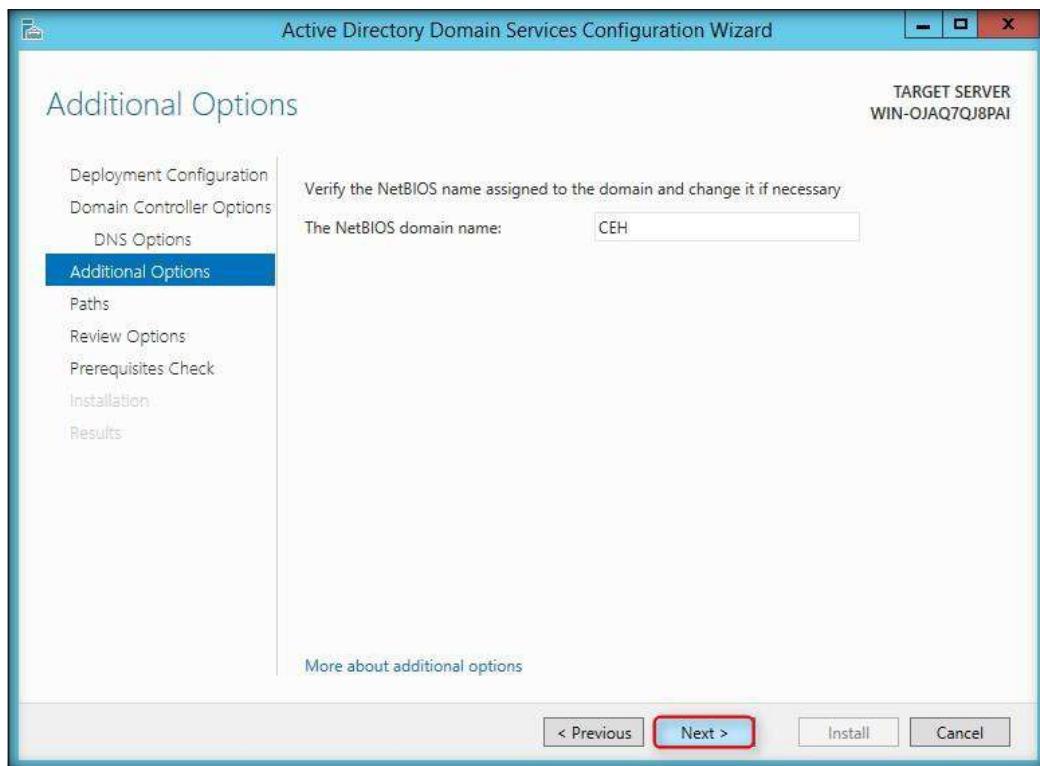
13. In this lab environment we have provided password as Pa\$\$w0rd



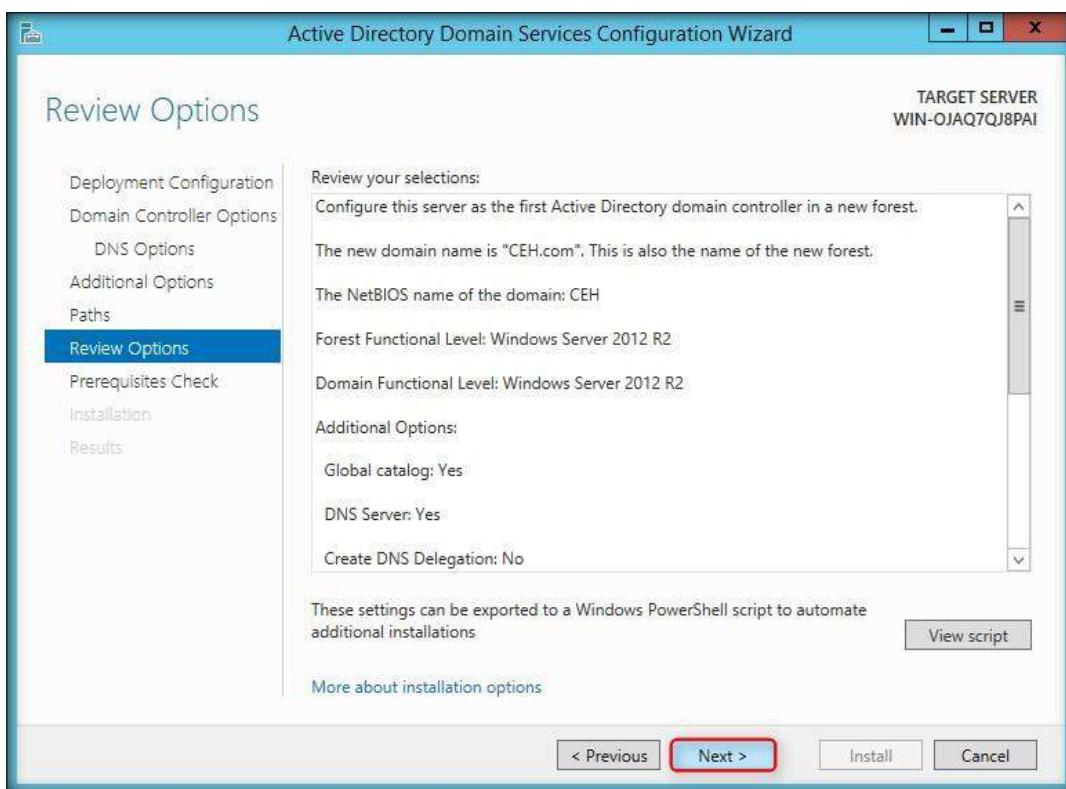
14. DNS Options section appears, ignore any alerts and click **Next**



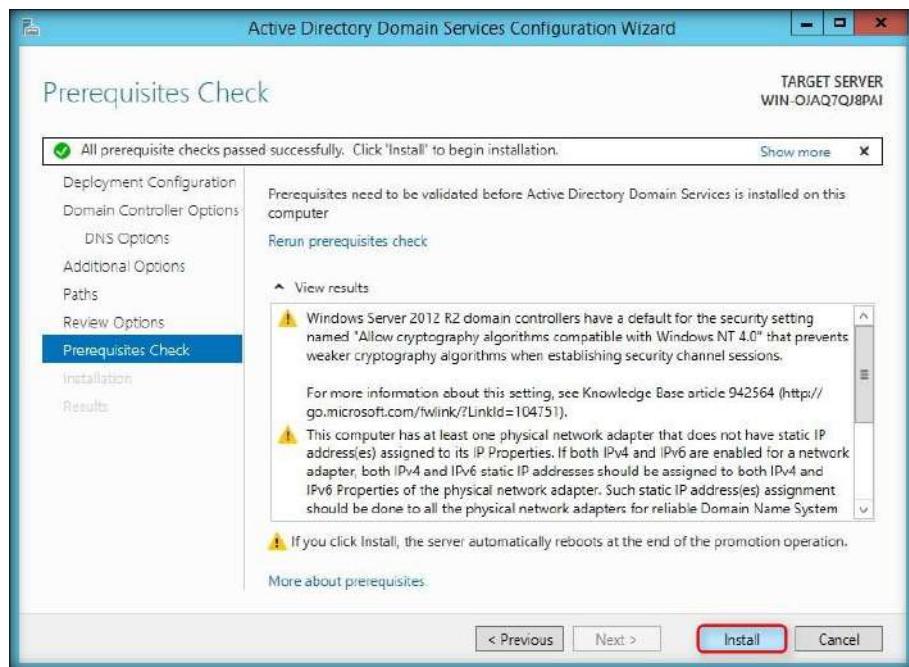
15. Additional Options section appears, verify the NetBIOS domain name is CEH and click **Next**



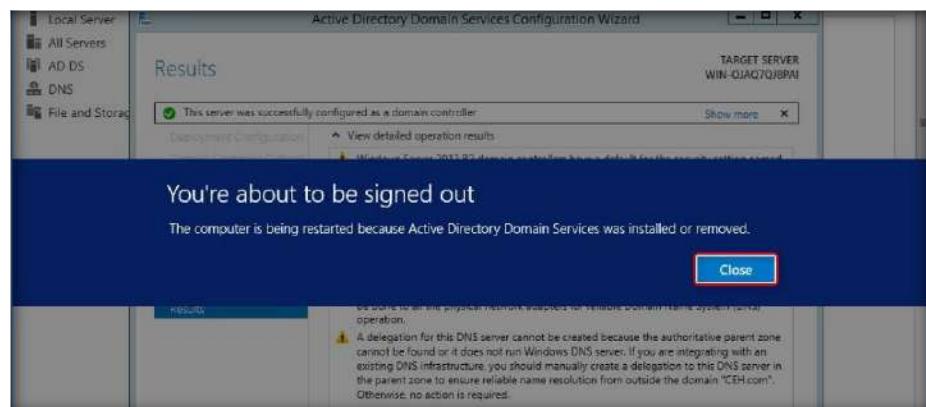
16. Review Options section appears, click Next



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



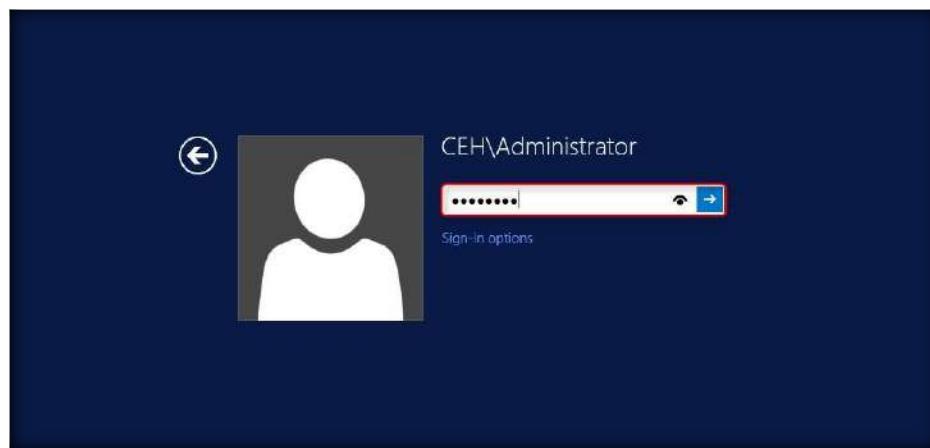
18. You're about to be signed out pop-up appears click **Close**



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



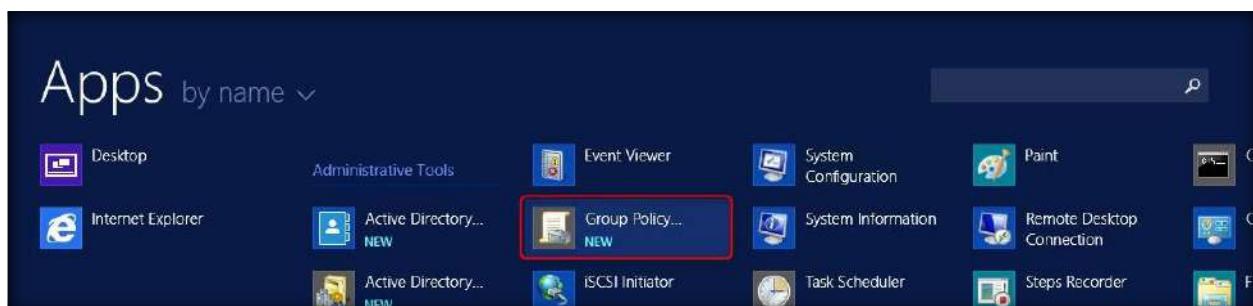
20. Type the password **Pa\$\$w0rd** and click **Login** button



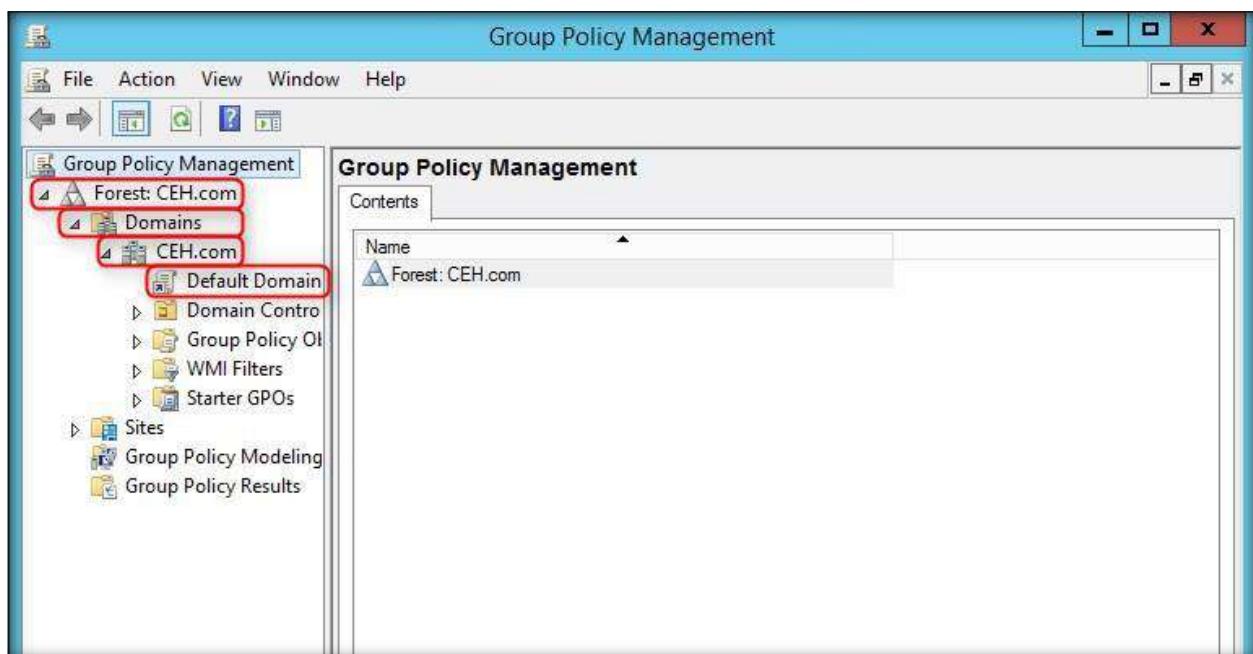
21. **Close** the Server Manager window once you logged in

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**

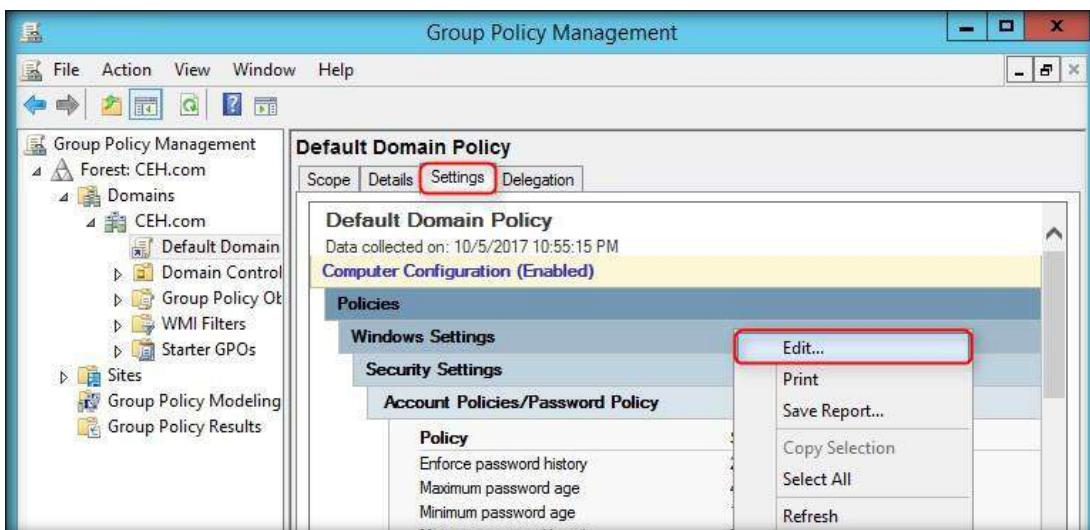


24. **Group Policy Management Console** dialog-box appears, click **OK**



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

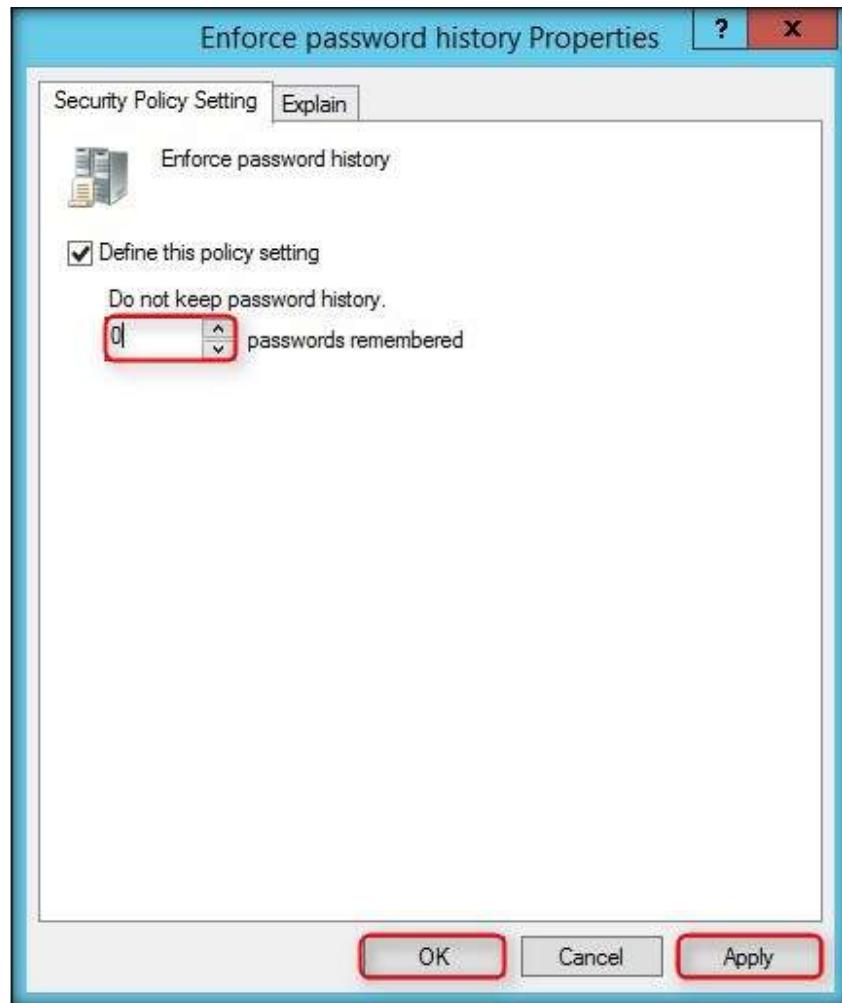


27. **Group Policy Management Editor** window appears, expand **Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies** and select **Password Policy**

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**



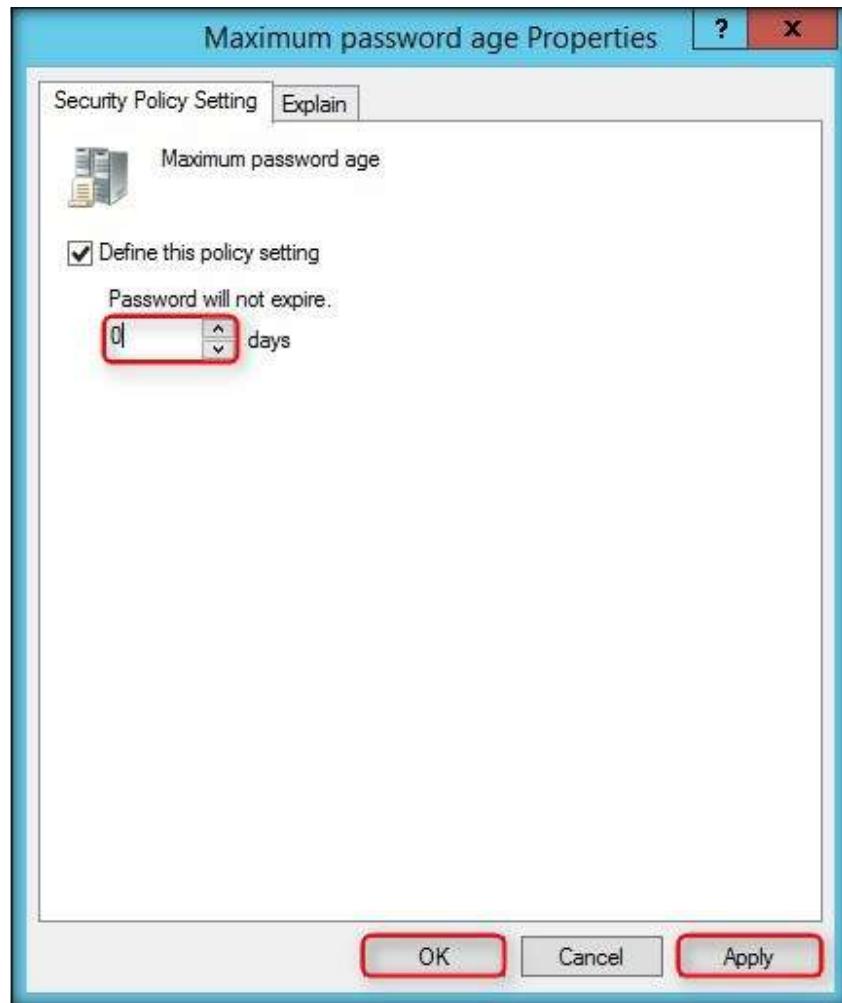
30. Double-click **Maximum password age** option in the right-pane

A screenshot of the 'Group Policy Management Editor' window. The title bar says 'Group Policy Management Editor'. The left pane shows a tree structure with 'Default Domain Policy [WIN-OJAQ7QJ8]' expanded, revealing 'Computer Configuration' and 'Policies'. Under 'Policies', 'Account Policies' is expanded, showing 'Password Policy' and 'Account Lockout'. The right pane is titled 'Policy' and lists several policy settings with their values:

Policy	Policy Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

The 'Maximum password age' row is highlighted with a blue selection bar and has a red box around its value '42 days'.

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

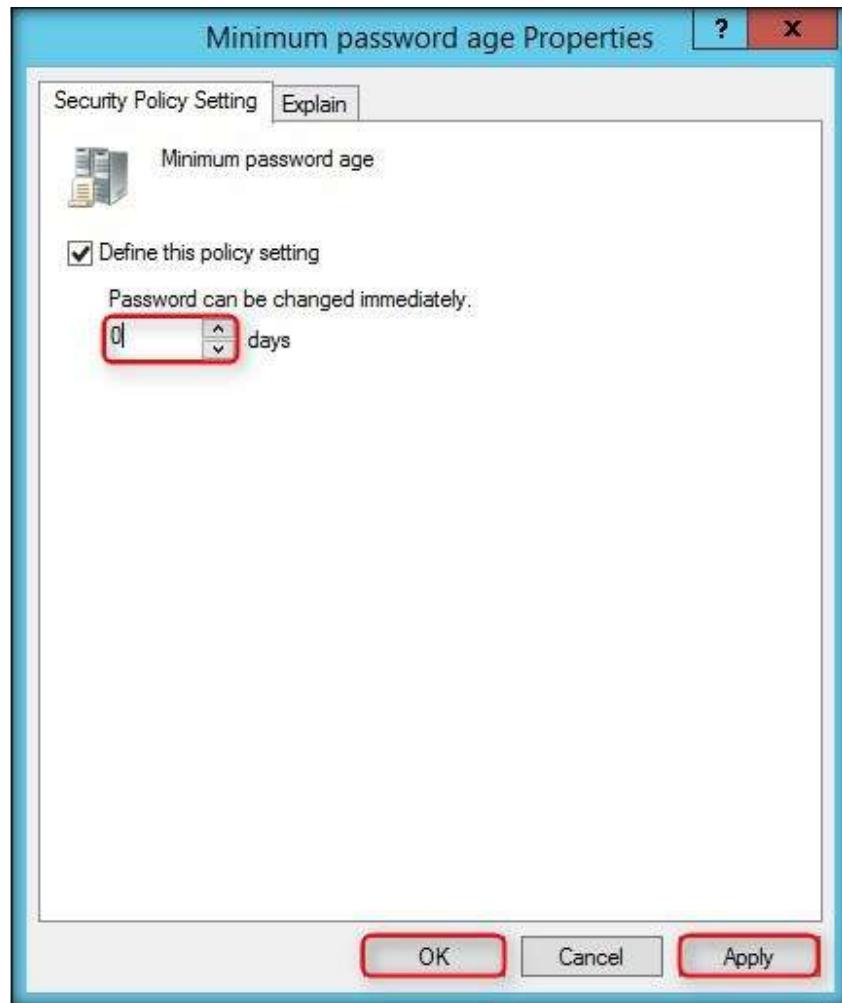


32. Double-click **Minimum password age** option in the right-pane

The screenshot shows the 'Group Policy Management Editor' window. On the left, the navigation pane shows 'Default Domain Policy [WIN-OJAQ7QJ8]'. Under 'Computer Configuration / Policies / Windows Settings / Security Settings / Account Policies / Password Policy', several policy items are listed in a table:

Policy	Policy Setting
Enforce password history	0 passwords remembered
Maximum password age	0
Minimum password length	1 days
Password must meet complexity requirements	7 characters
Store passwords using reversible encryption	Enabled

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

A screenshot of the 'Group Policy Management Editor' window. The left pane shows a tree structure with 'Default Domain Policy [WIN-OJAQ7QJ8]' expanded, showing 'Computer Configuration' and 'Policies' nodes. The right pane is titled 'Policy' and contains a table of policy settings. The 'Minimum password length' row is selected and highlighted with a blue box. The table data is as follows:

Policy	Policy Setting
Enforce password history	0 passwords remembered
Maximum password age	0
Minimum password age	0 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

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

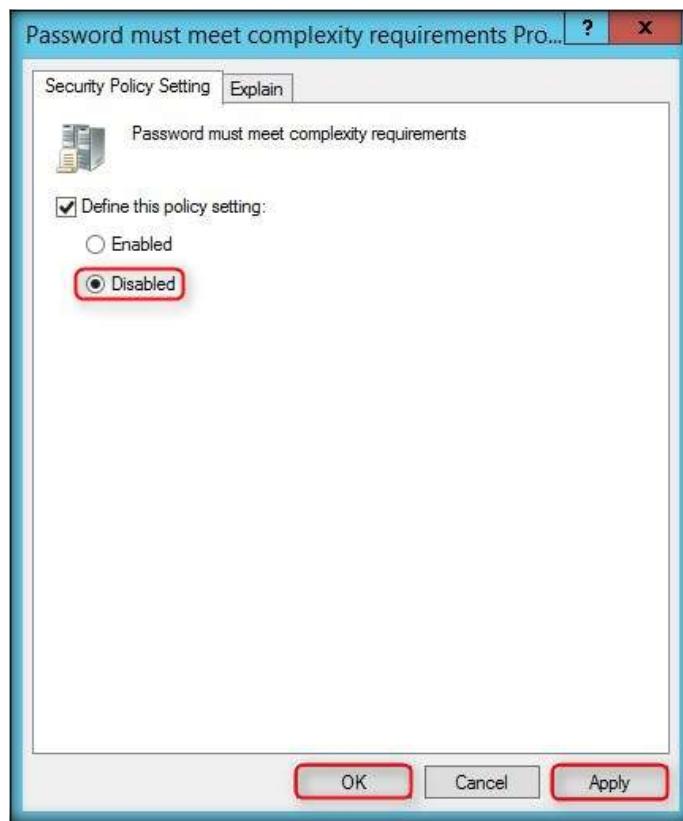


36. Double-click **Password must meet complexity requirements** option in the right-pane

The screenshot shows the 'Group Policy Management Editor' window. The left pane displays a tree structure under 'Default Domain Policy [WIN-OJAQ7QJ8]': Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy. The right pane lists policy settings with their values:

Policy	Policy Setting
Enforce password history	0 passwords remembered
Maximum password age	0 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

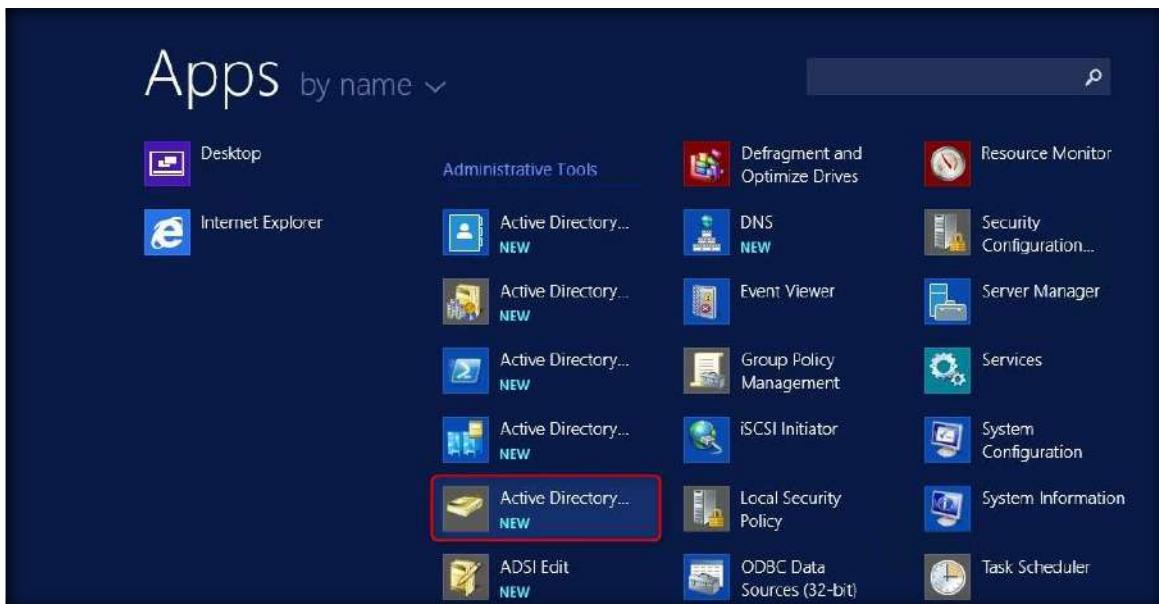
37. **Password must meet complexity requirements Properties** window appears, select **Disabled** radio button; click **Apply**, and then click **OK**



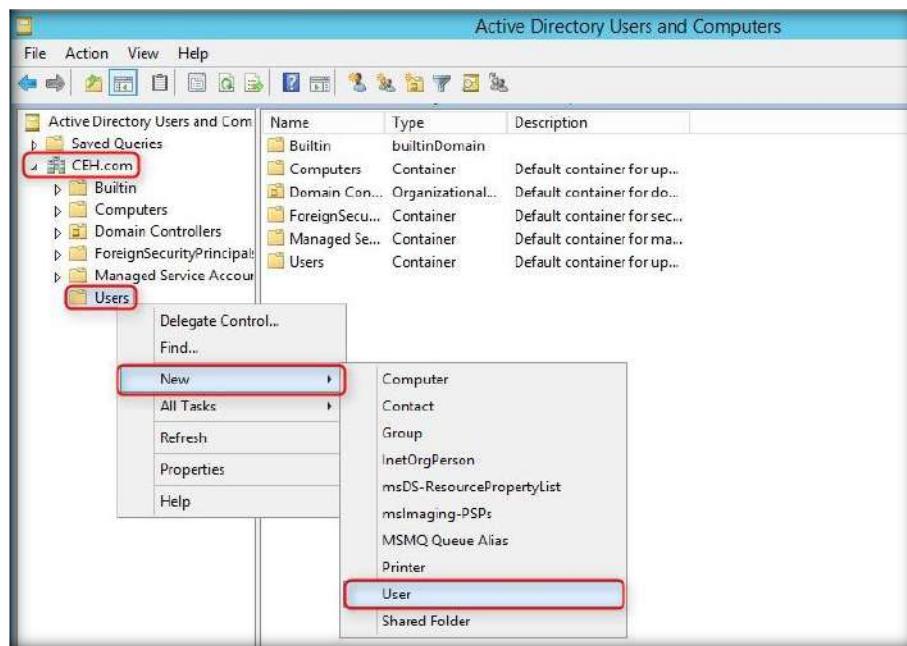
38. Once done, close all the windows

Create User Accounts and Configure Them

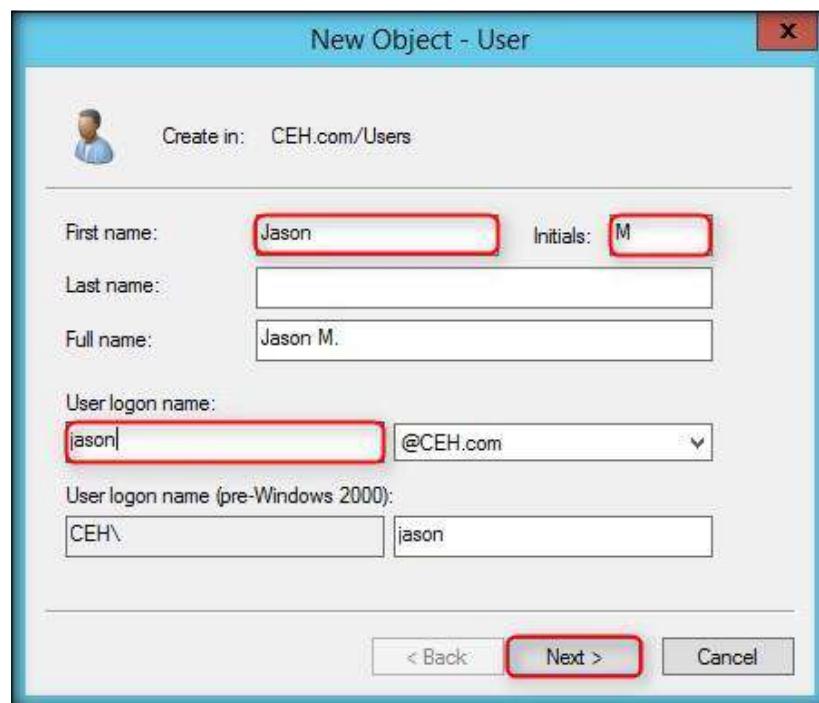
39. Now navigate to **Start → Apps → Administrative Tools → Active Directory Users and Computers**



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.



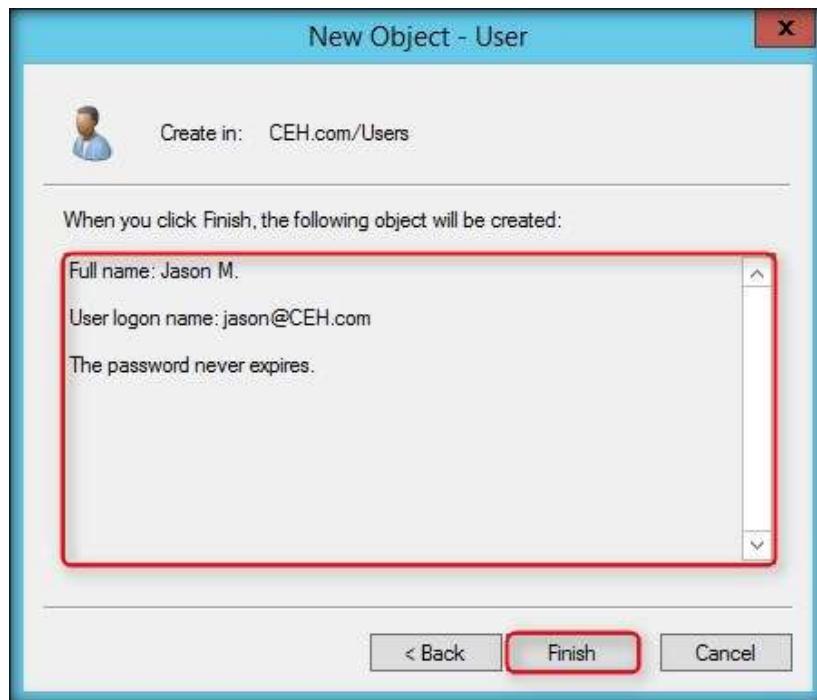
41. **New Object - User** dialog box appears fill in the required fields
42. Type **Jason** in First name: field, Initial of your choice, type **jason** in **User logon name:** field and click **Next**



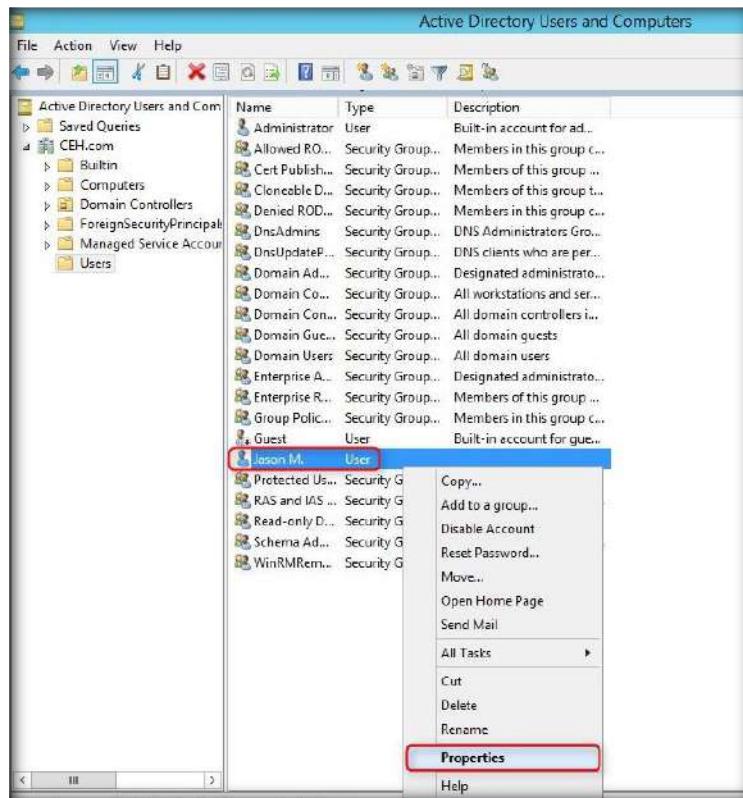
43. Type **qwerty** in Password and Confirm password fields and uncheck User must change password at next logon and check Password never expires option and click **Next**



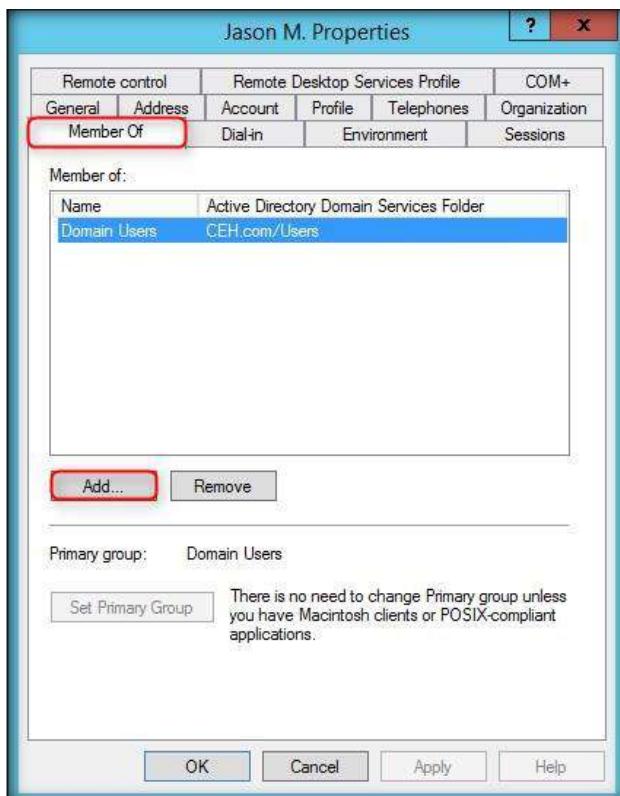
44. Once **User** is successfully created click **Finish**



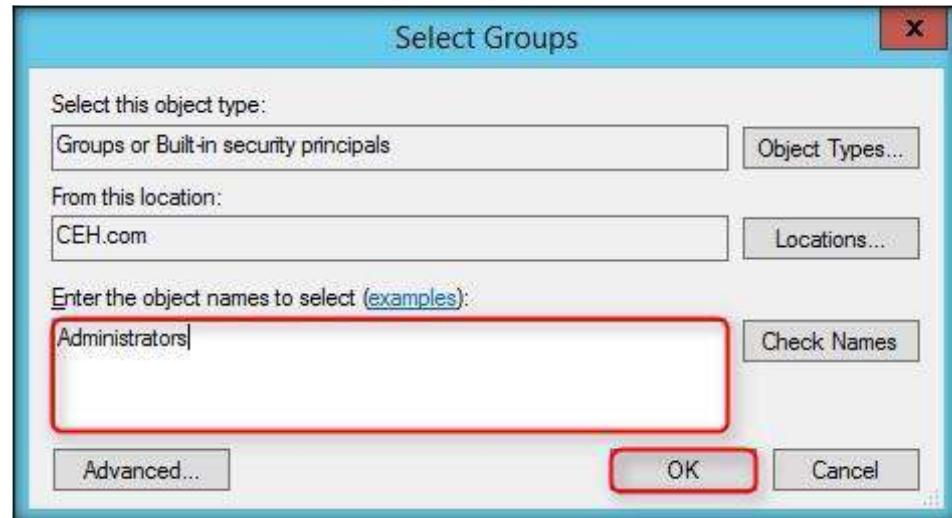
45. Now right-click on created user and click **Properties** from the context menu



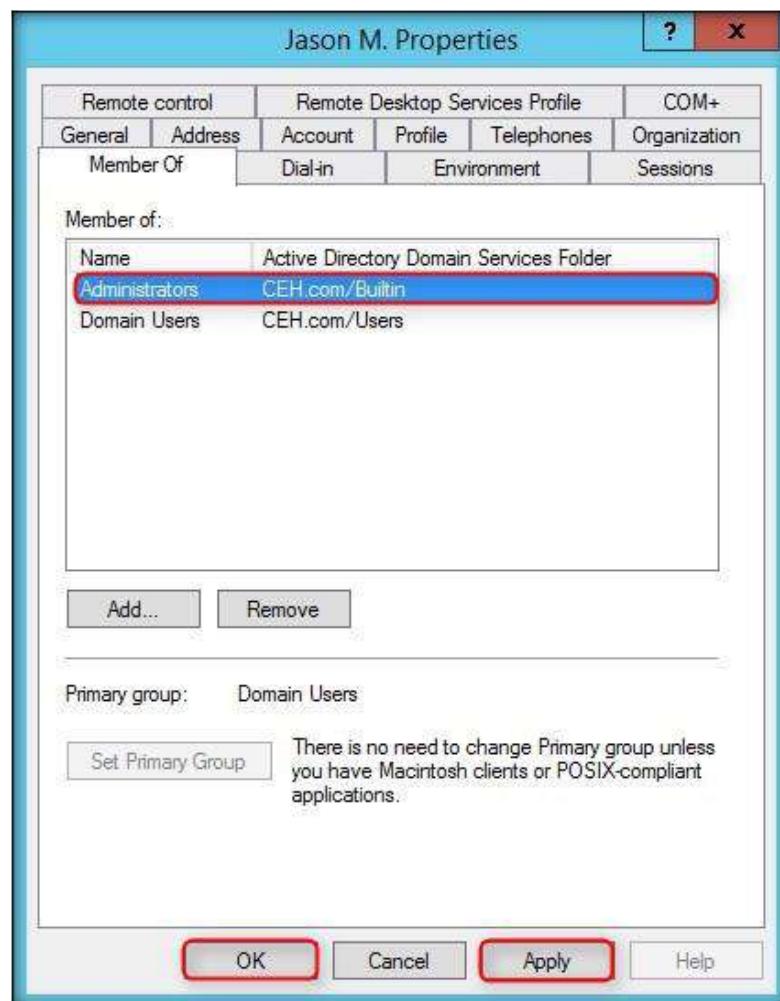
46. In select user properties click **Member Of** tab and click **Add** button



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**.

The screenshot shows the Windows Active Directory Users and Computers management console. The left navigation pane shows the tree structure of the domain: Active Directory Users and Com, Saved Queries, CEH.com, and its sub-objects like Builtin, Computers, Domain Controllers, ForeignSecurityPrincipal, Managed Service Account, and Users. The main pane displays a table of users and groups. Two specific users are highlighted with blue rounded rectangles: 'Martin' (User) and 'Shiela' (User). Both entries show their account type as 'User'. The table includes columns for Name, Type, and Description.

Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are pe...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Jason M.	User	
Enterprise A...	Security Group...	Designated administrato...
Martin	User	
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group ca...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...
Shiela	User	
WinRMRem...	Security Group...	Members of this group ...

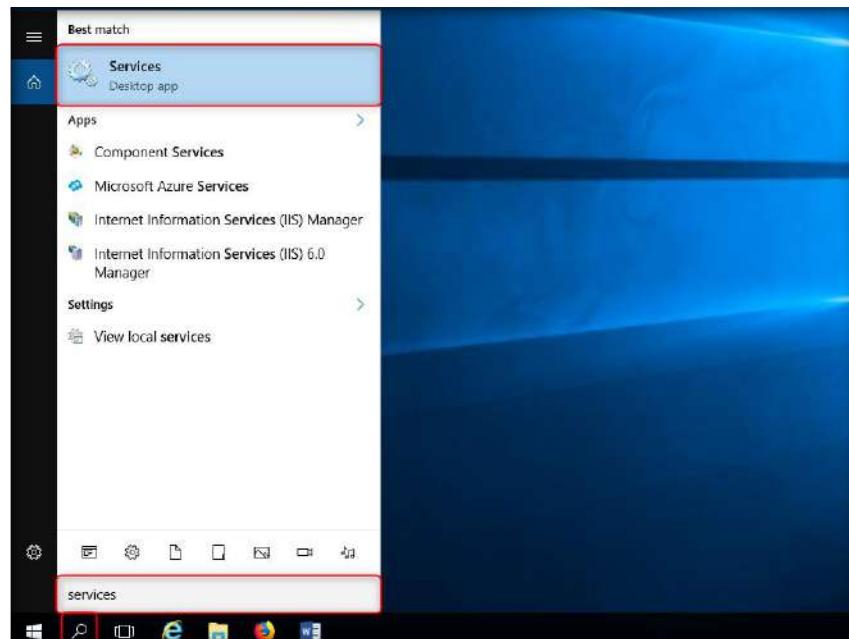
[[Back to Configuration Task Outline](#)]

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

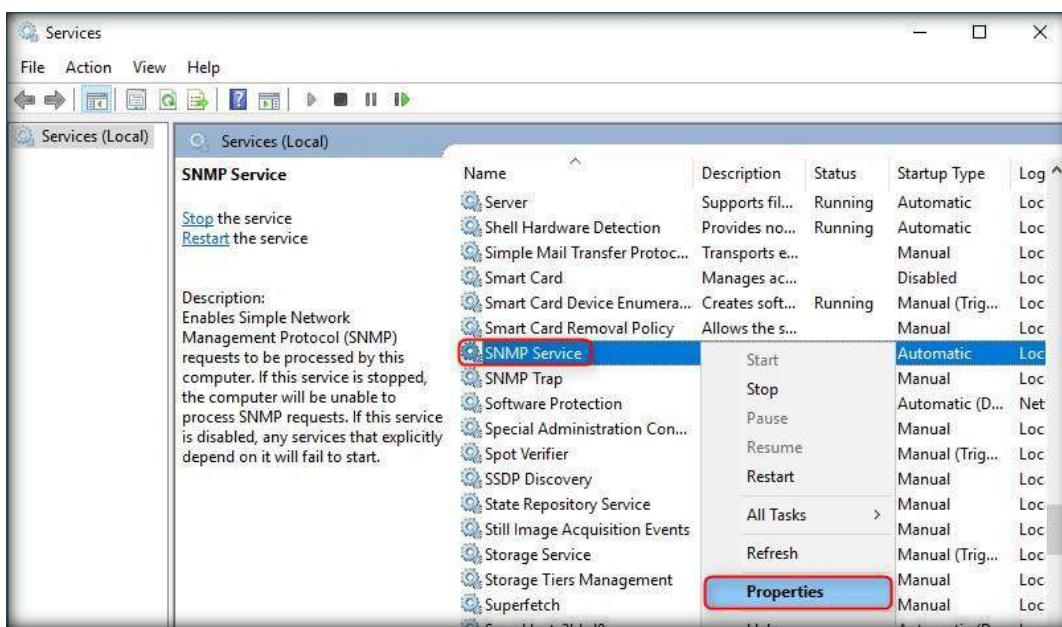
Configuring SNMP Service in Windows Server 2016

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**.

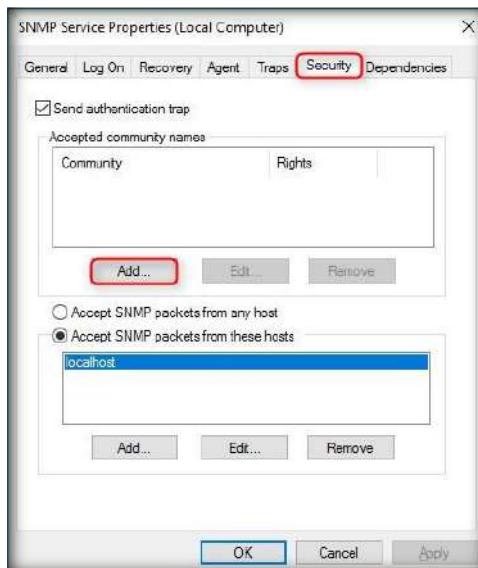
1. Click the **Search** icon in the taskbar and type **services** in the search field. Click the **Services** Desktop app



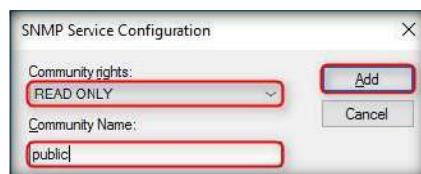
2. Services window appears, right-click **SNMP Service** and click **Properties** from context menu



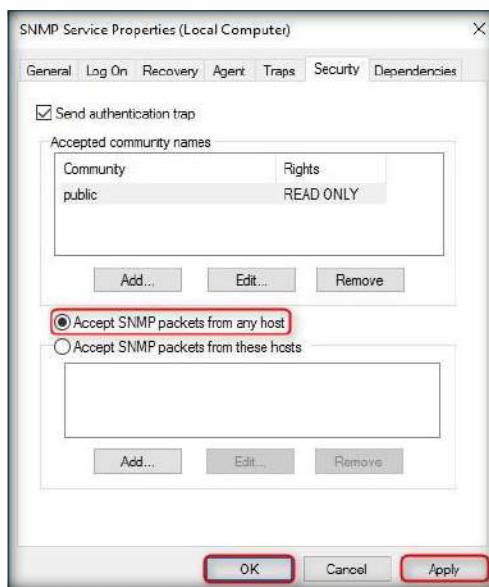
3. Click **Security** tab in **SNMP Service Properties** wizard and click **Add** button under **Accepted community names** section



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

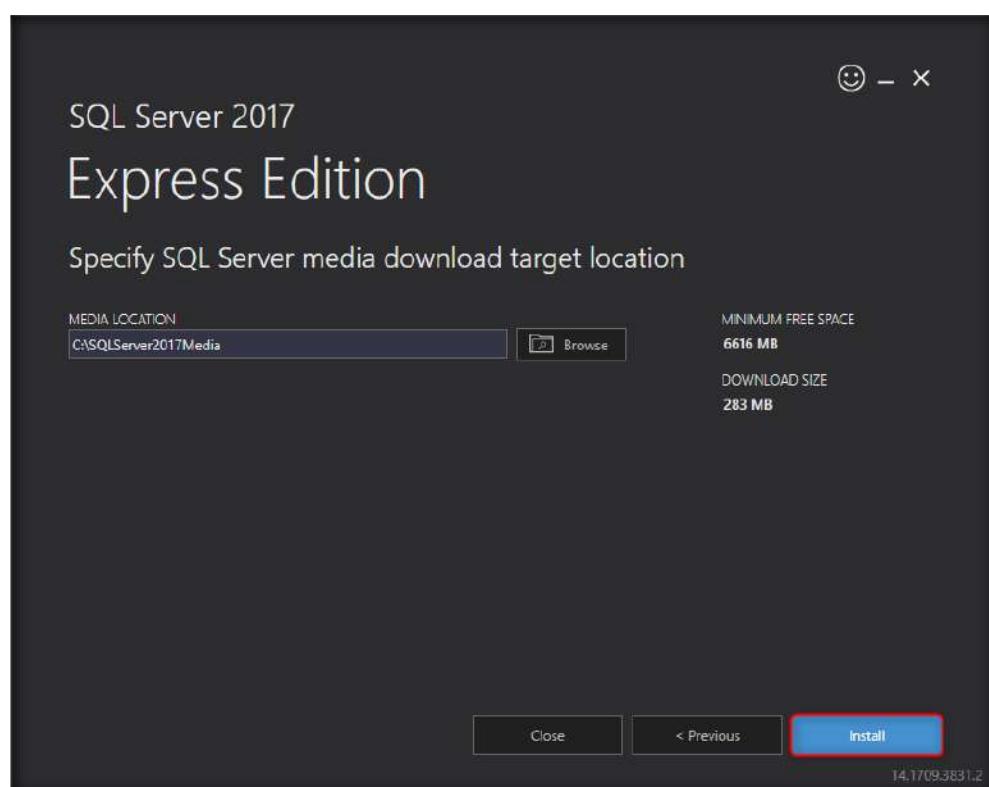
[\[Back to Configuration Task Outline\]](#)

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

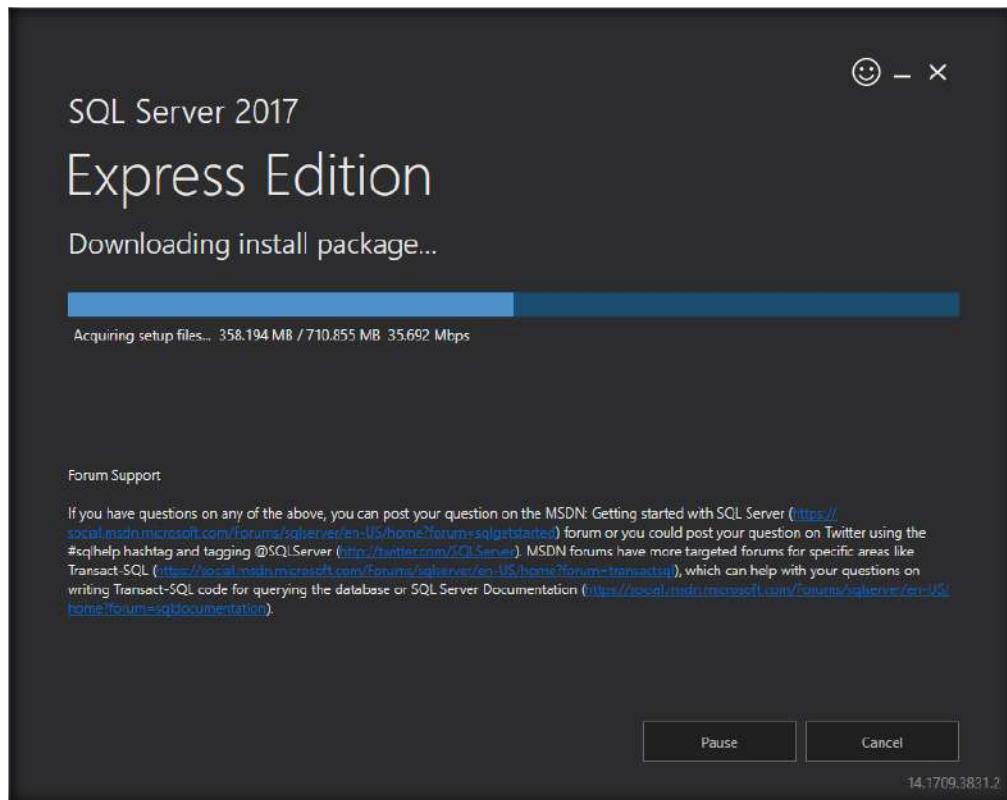
1. Navigate to **Z:\CEH-Tools\CEHv10 Lab Prerequisites\SQL Server\SQLServer2017-SSEI-Expr.exe** and double-click **SQLServer2017-SSEI-Expr.exe**
2. If a User Account Control pop-up appears, click **Yes**
3. SQL Server 2017 window appears click **Custom**



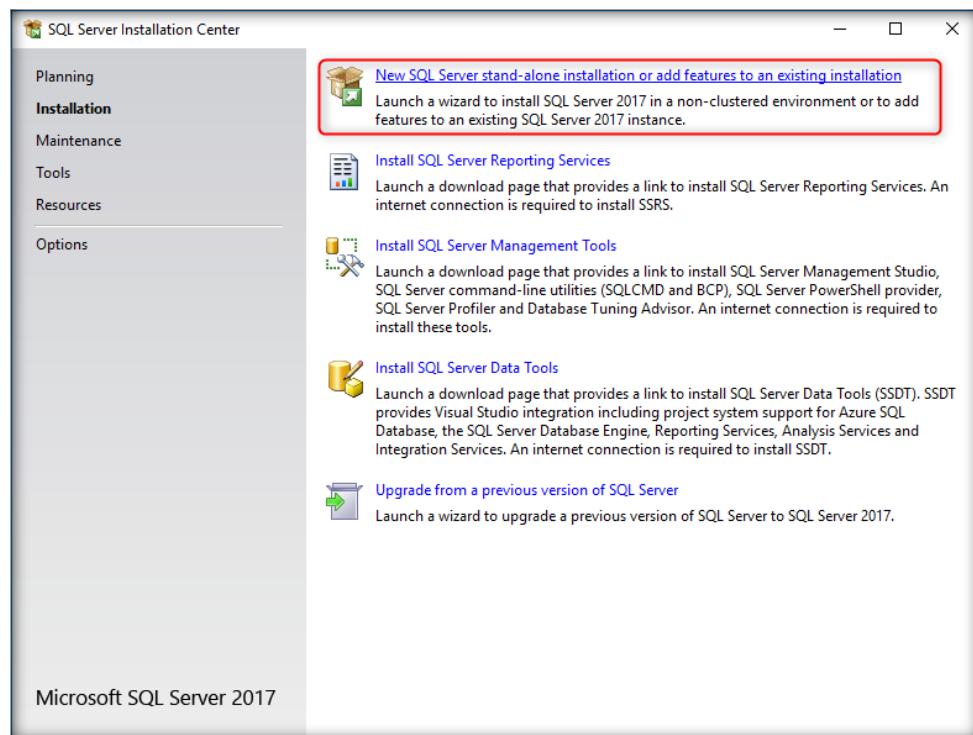
4. Specify SQL Server media download target location section appears, click **Install**



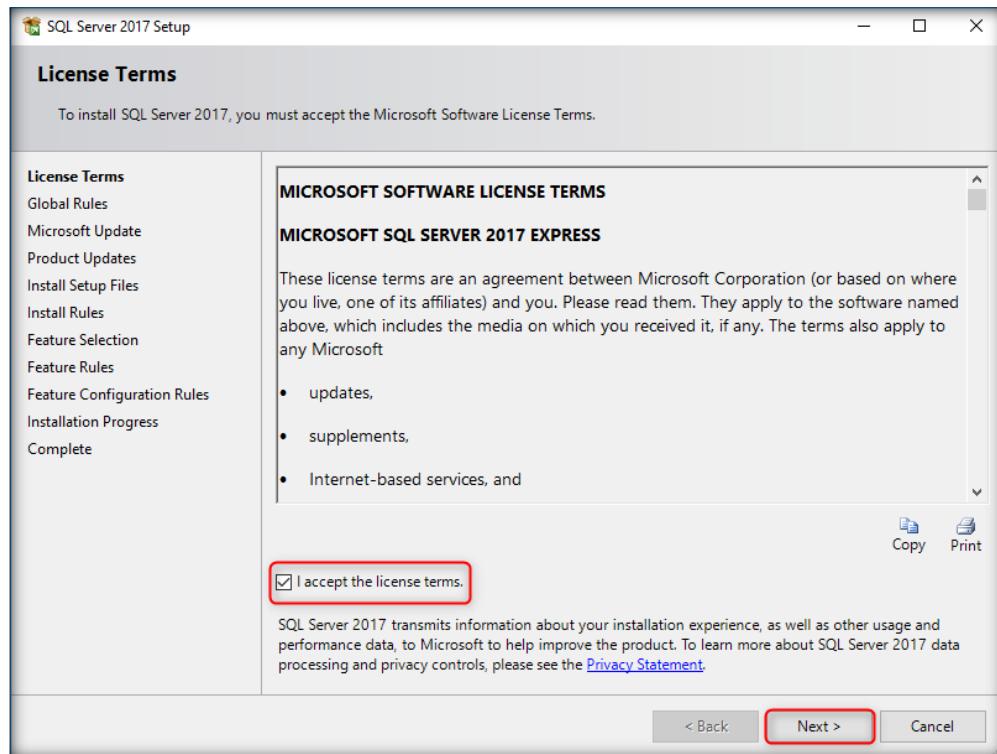
5. The program starts downloading the setup files, wait for the Installation Center to launch



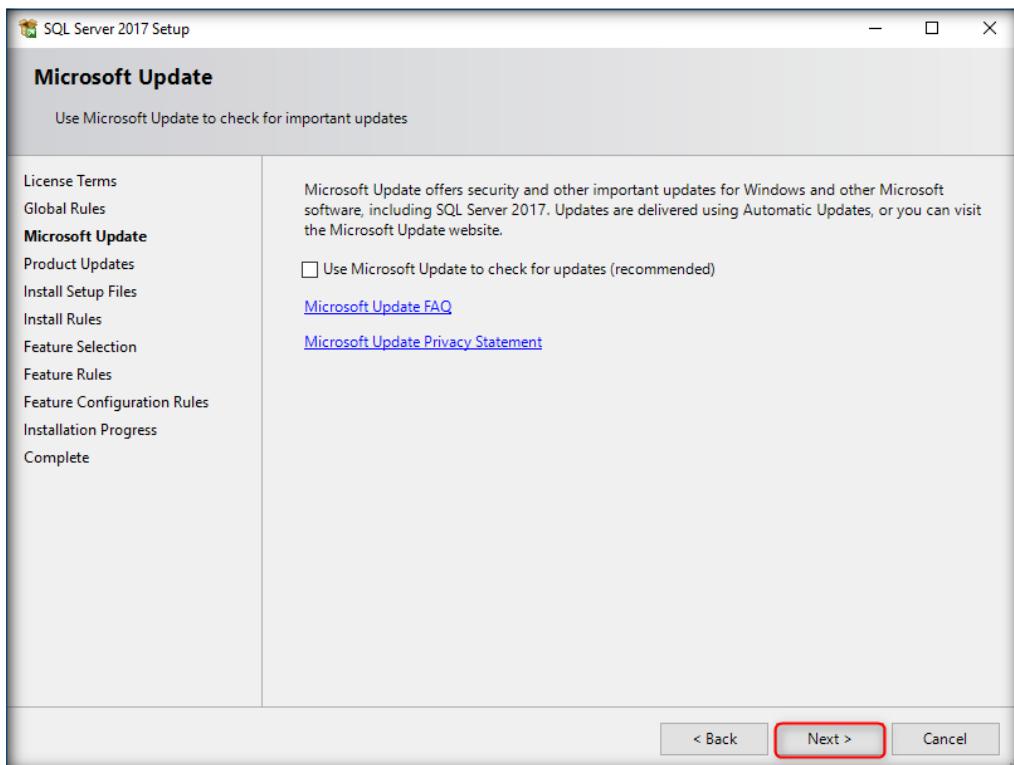
6. SQL Server Installation Center window appears with **Installation** section displayed by default, click **New SQL Server stand-alone installation or add features to an existing installation** link and wait for some time



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

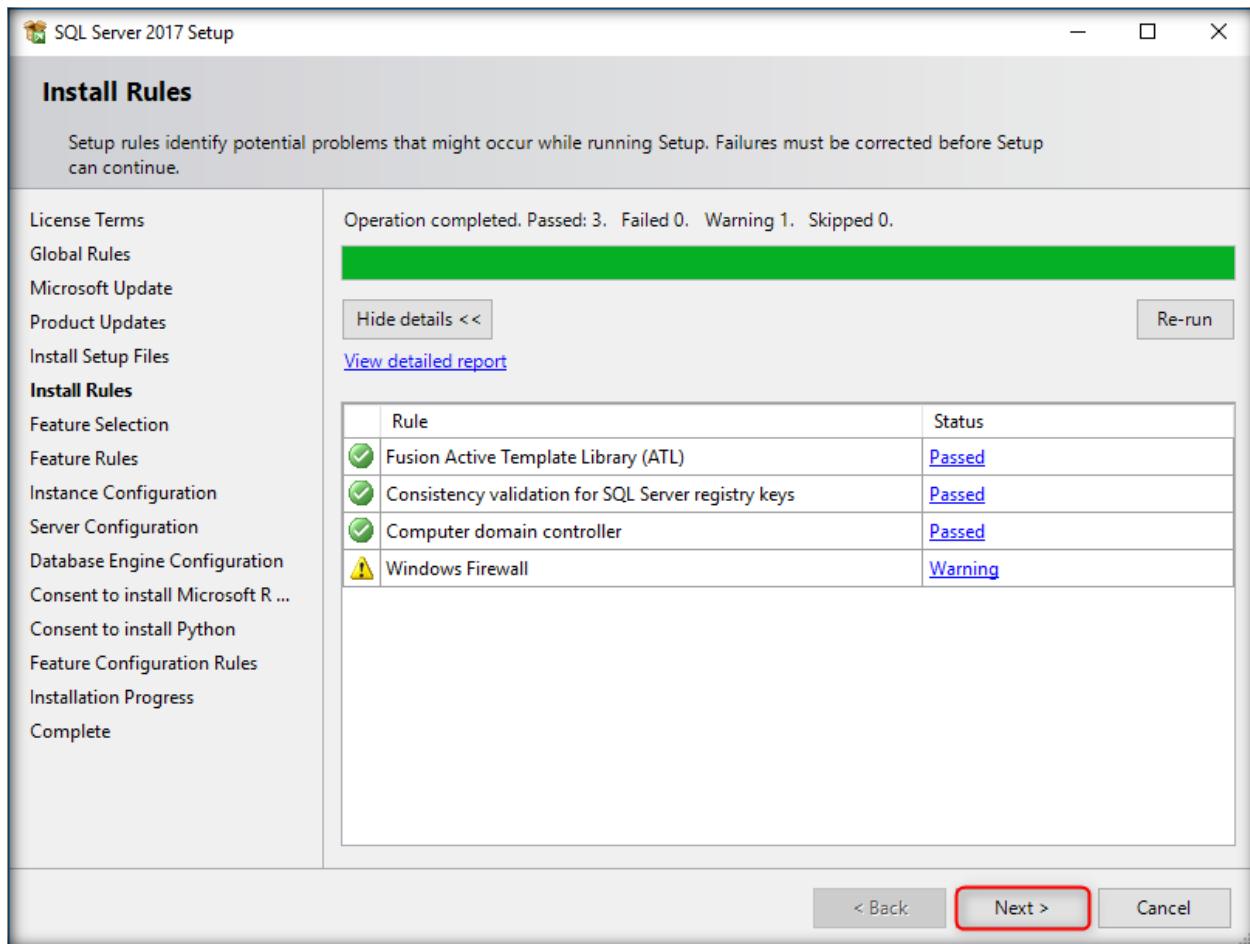


8. SQL Server 2017 Setup **Microsoft Update** section appears, click **Next**



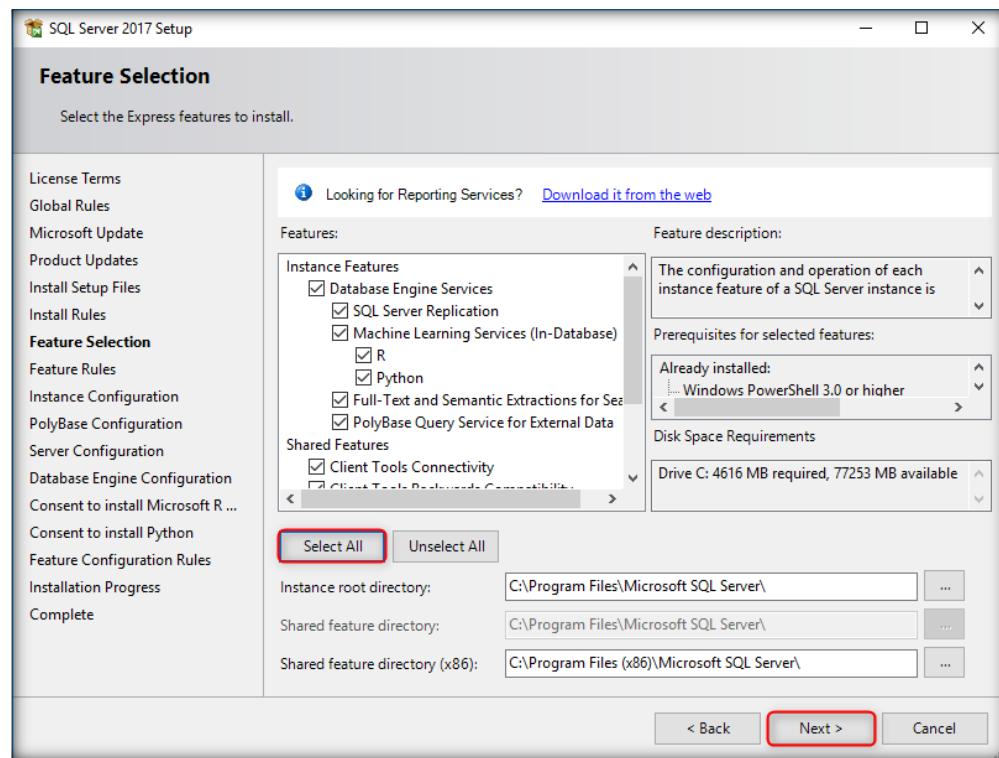
9. The **Install Rules** verifies the system state of your computer before Setup continues

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



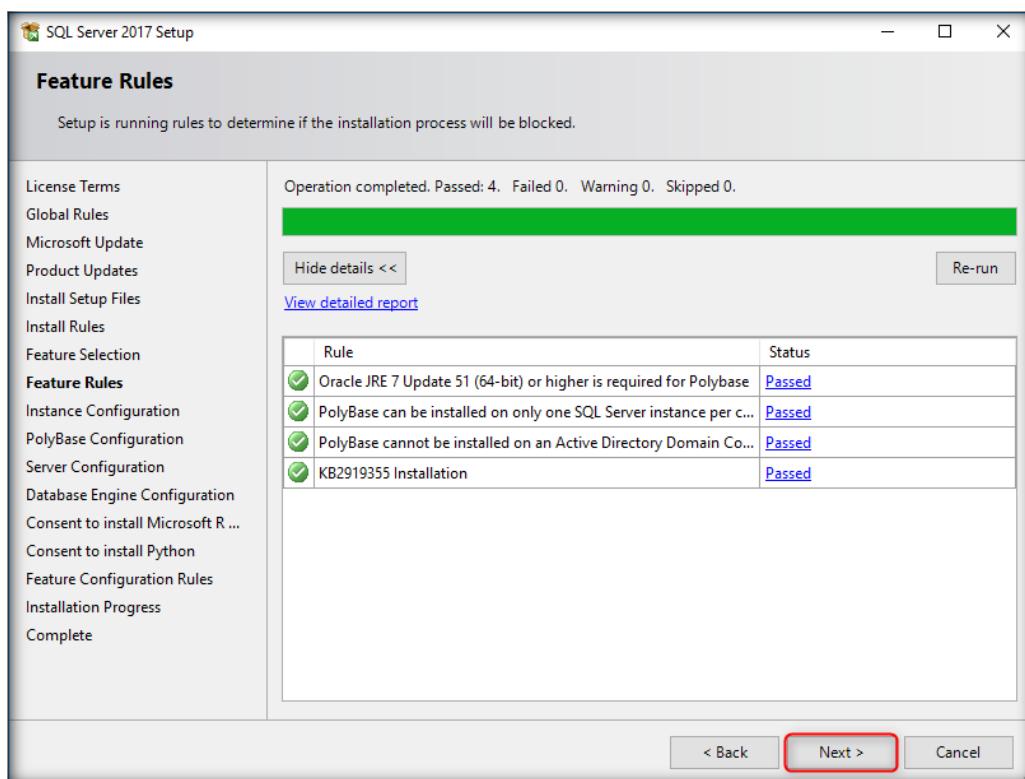
11. On the **Feature Selection** window, select the **Features** for installation (**Select All**)
12. A **description** for each feature group appears in the **right pane** after you select the feature
13. You can select any **combination** of check boxes
14. To change the **installation path** for 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**

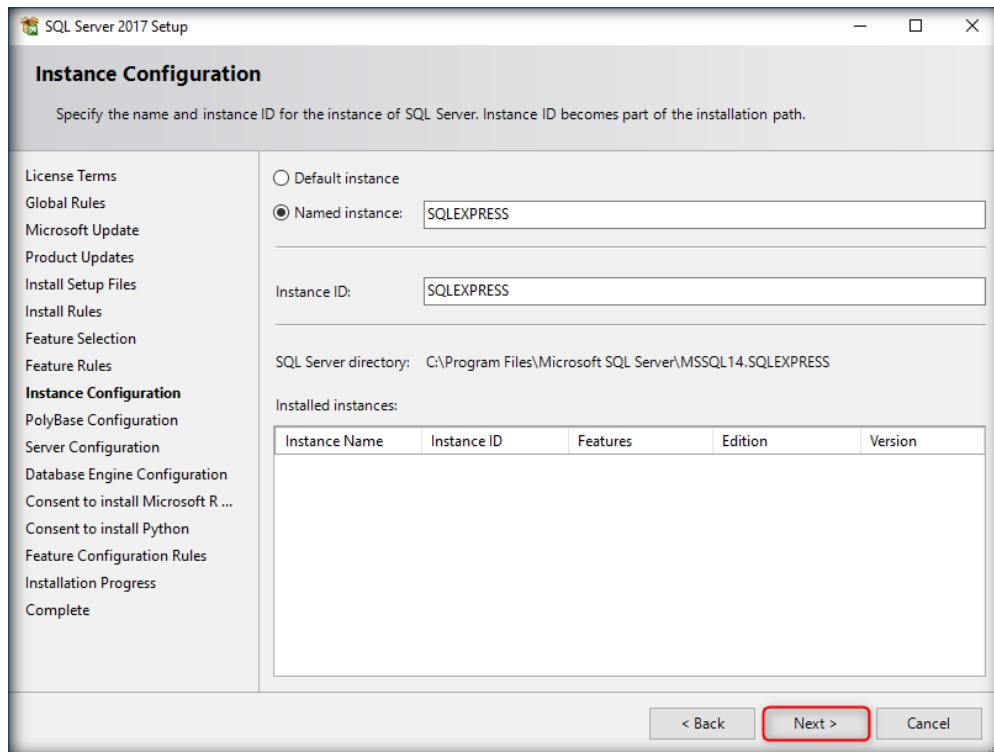


18. **Feature Rules** section appears, and verifies the prerequisites for the installation.

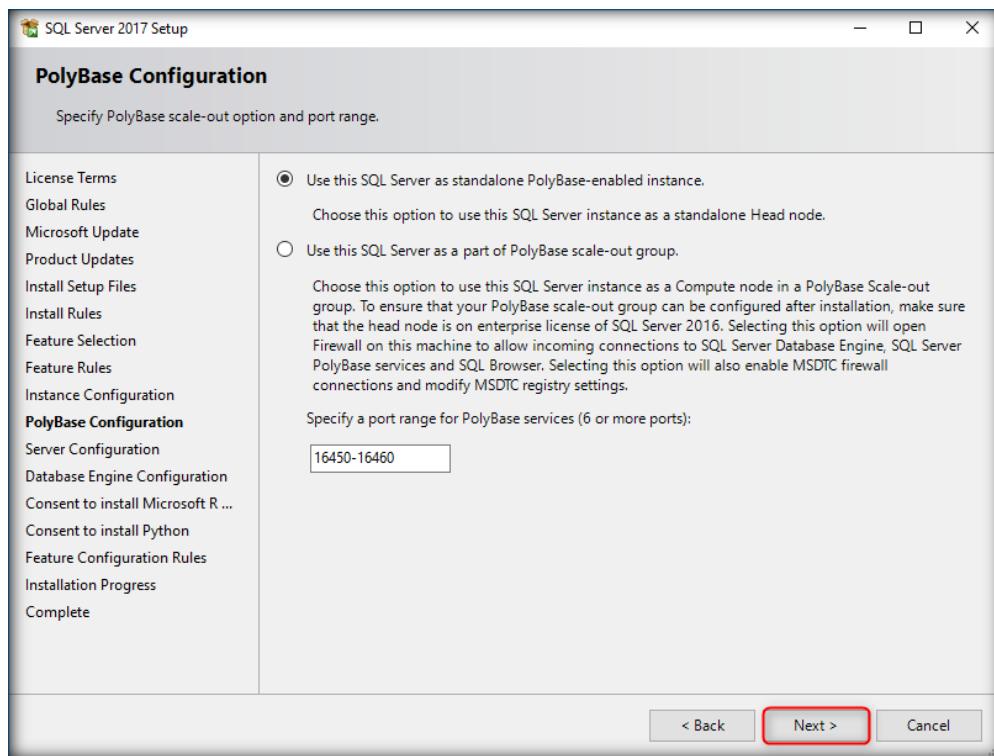
19. If all the prerequisites are present, click **Next**



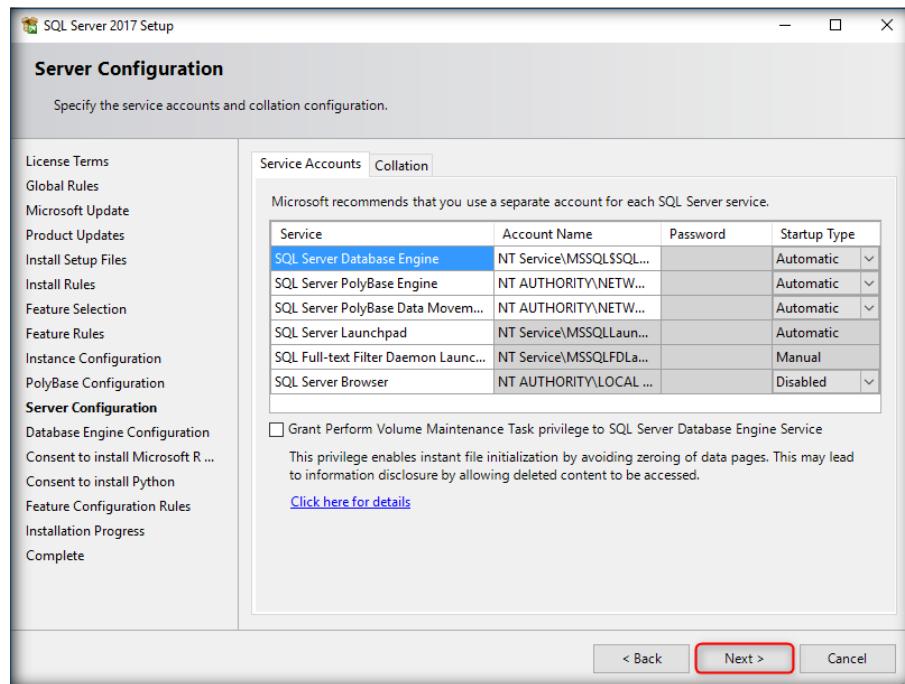
20. In the **Instance Configuration** section, check that **Named instance** is specified, leave the **Instance ID** and **Instance root directory** options set to default, and click **Next** to continue



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

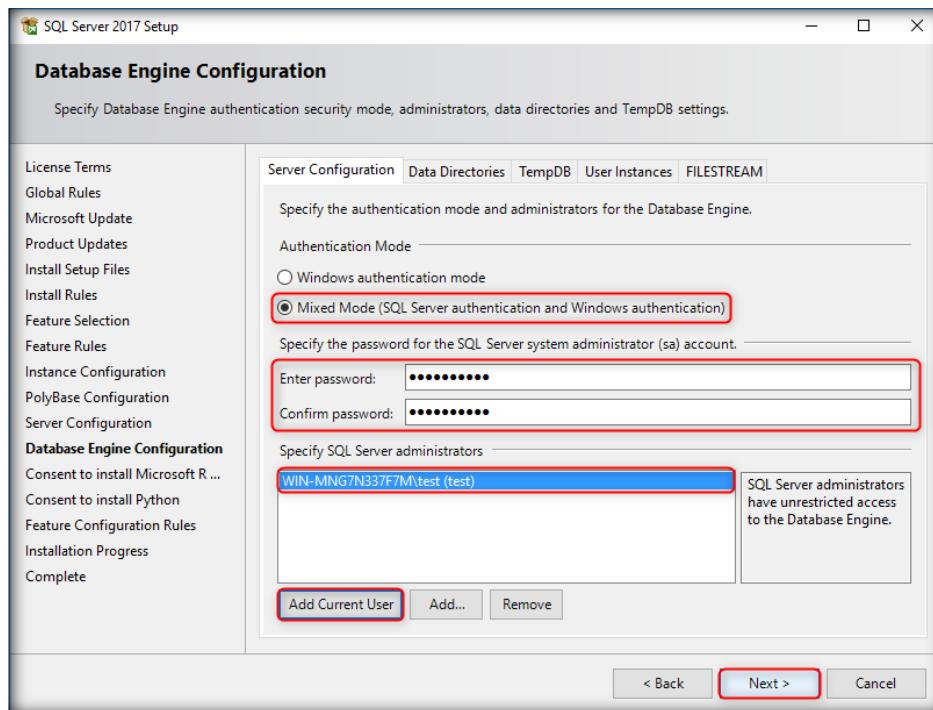


22. **Server configuration** section appears, leave the Account Names and Passwords set to default and click **Next**

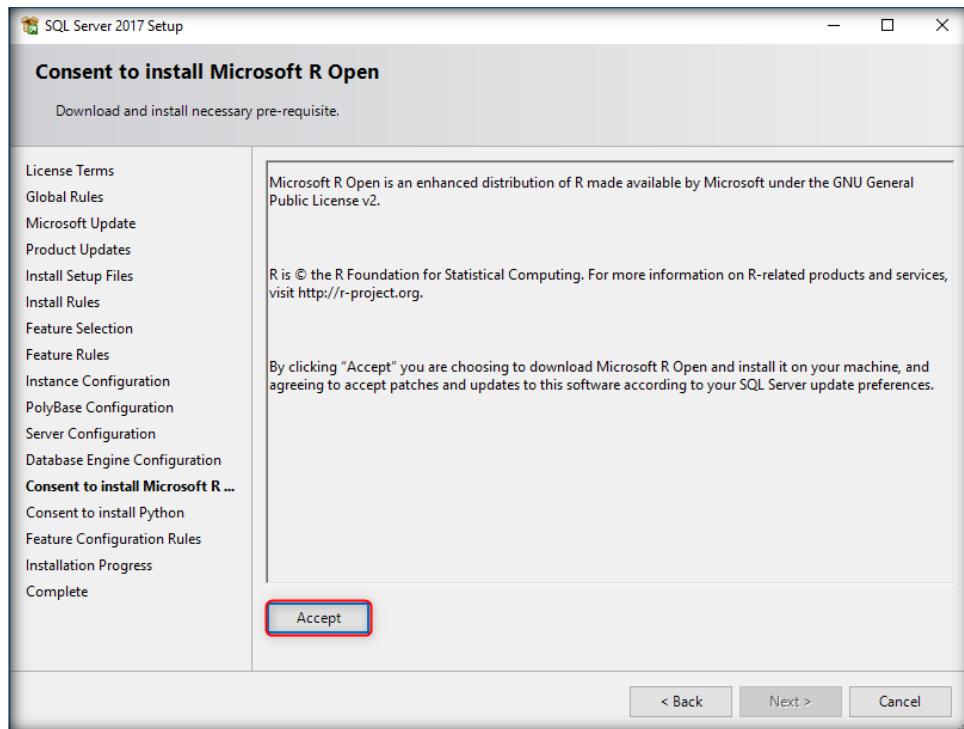


23. **Database Engine Configuration** section appears, select **Mixed Mode (SQL Server authentication and Window authentication)** radio button and input the password **qwert@123** in both **Enter password** and **Confirm password** text fields

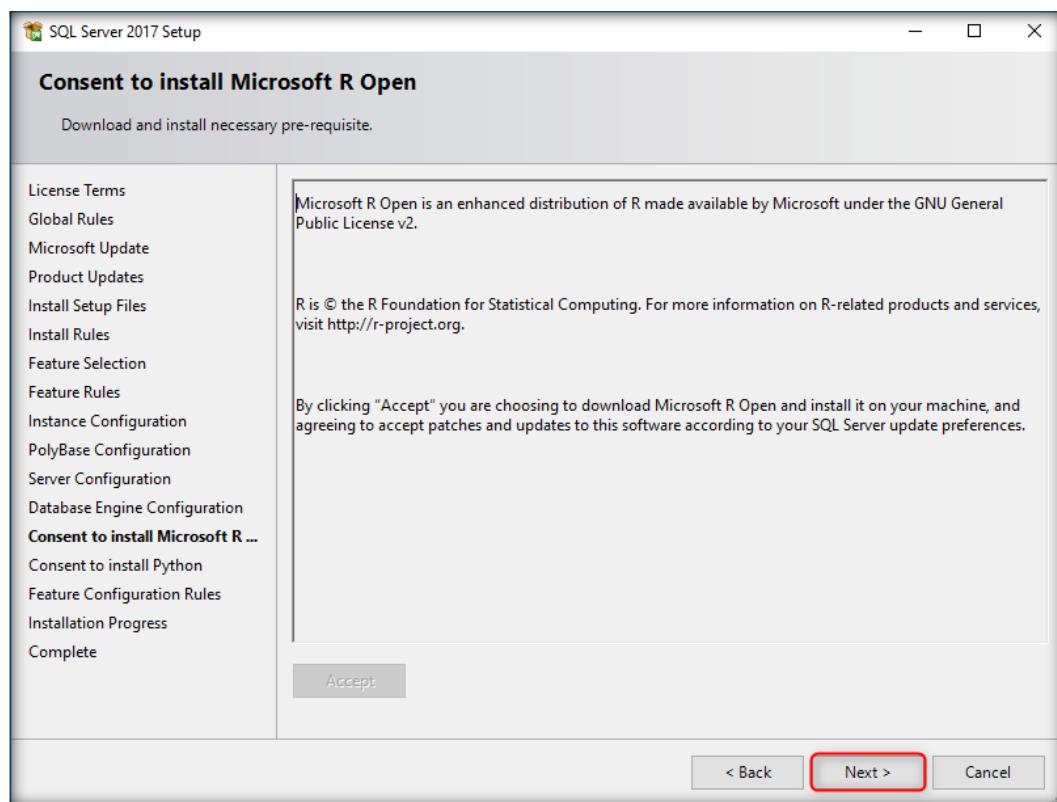
24. Click **Add Current User** button. You are added as the user (here, test) and is displayed under **Specify SQL Server administrators**. Click **Next**



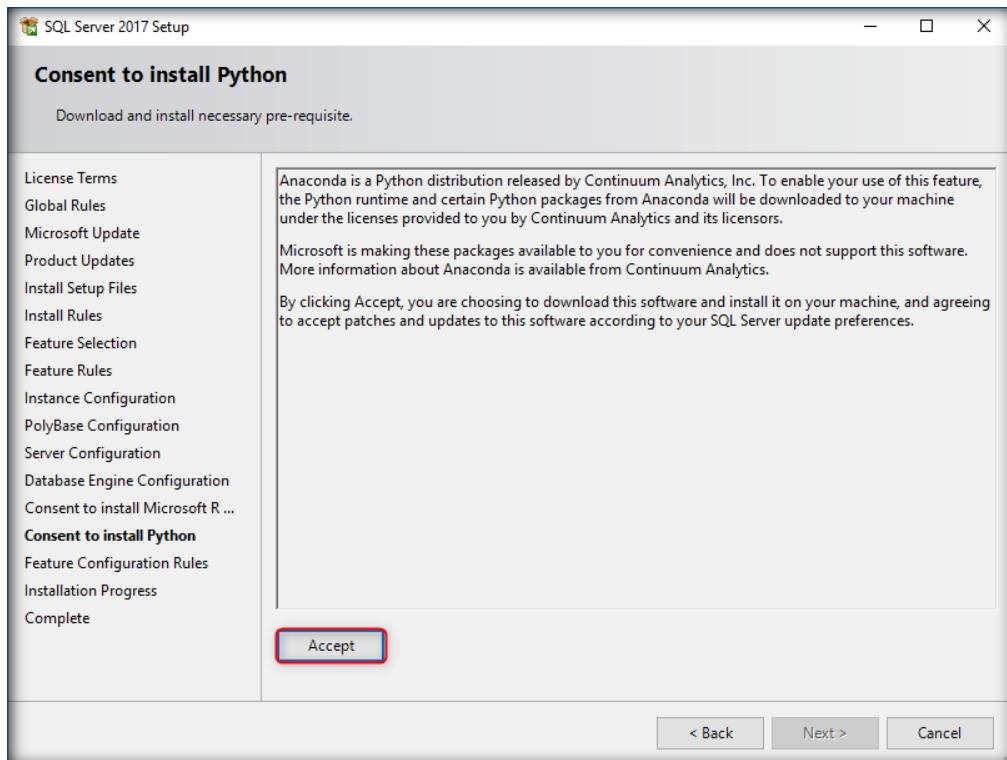
25. **Consent to install Microsoft R Open** section appears, click the **Accept** button



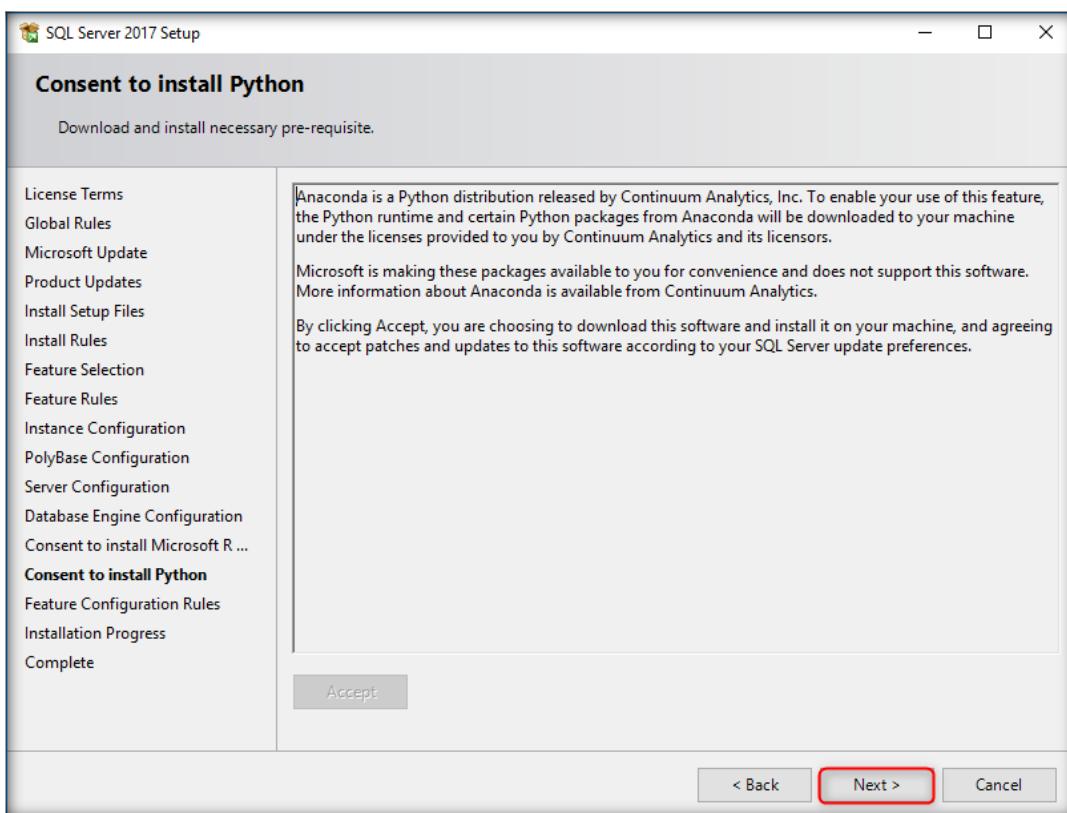
26. In the **Consent to install Microsoft R Open** section wait for the **Next** button to be active and then click it



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



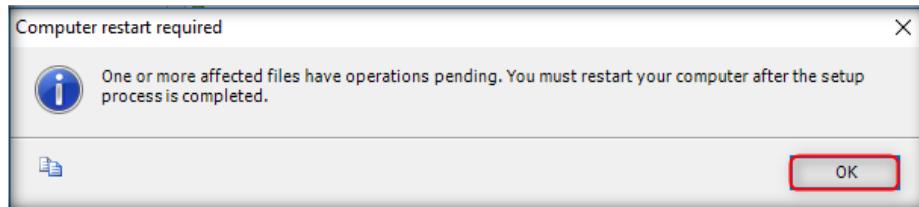
28. In the **Consent to install Python** section wait for the **Next** button to be active and then click it



29. The setup starts to install the SQL server, showing you the progress in the **Installation Progress** section.

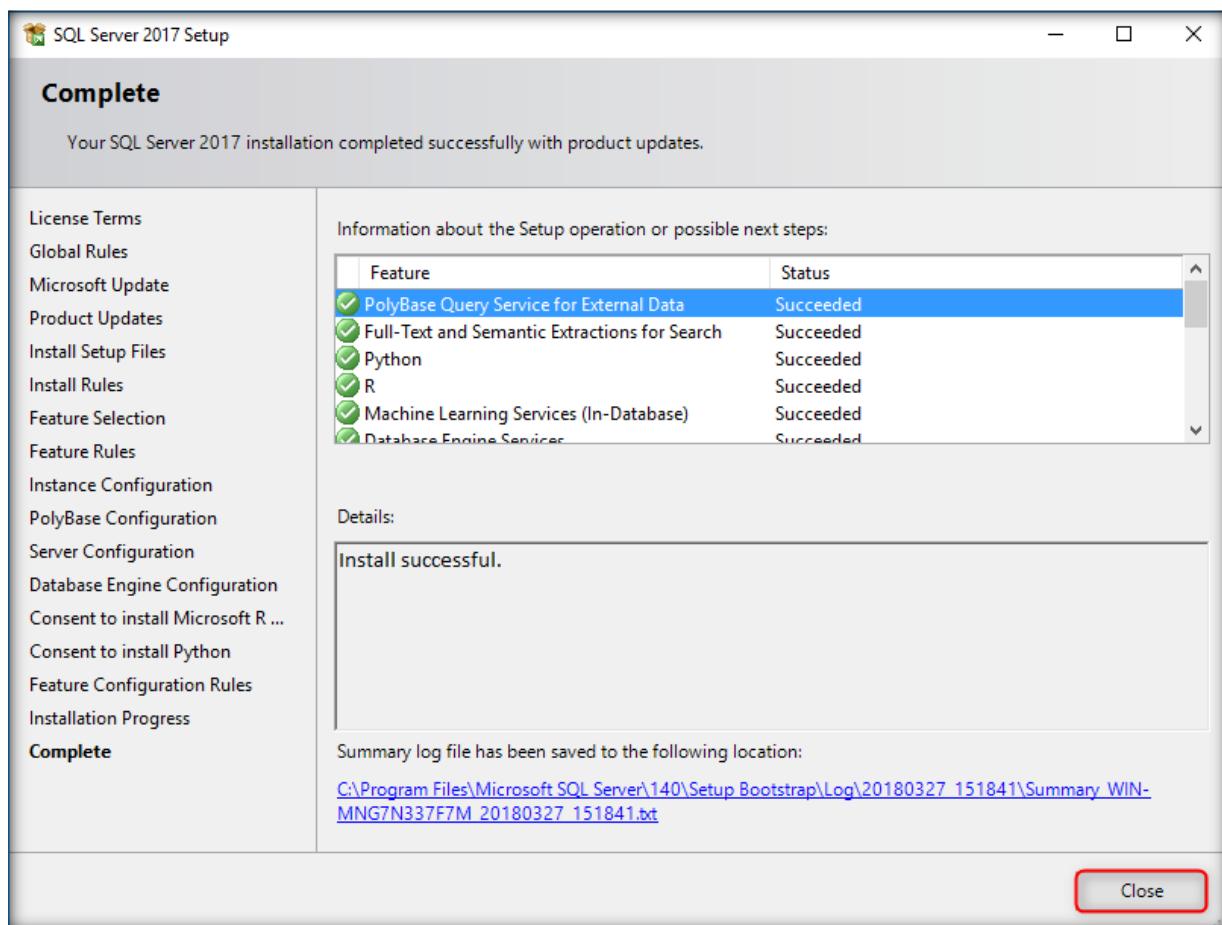
30. Wait for the installation to complete

31. Computer restart required pop-up appears, click **OK**

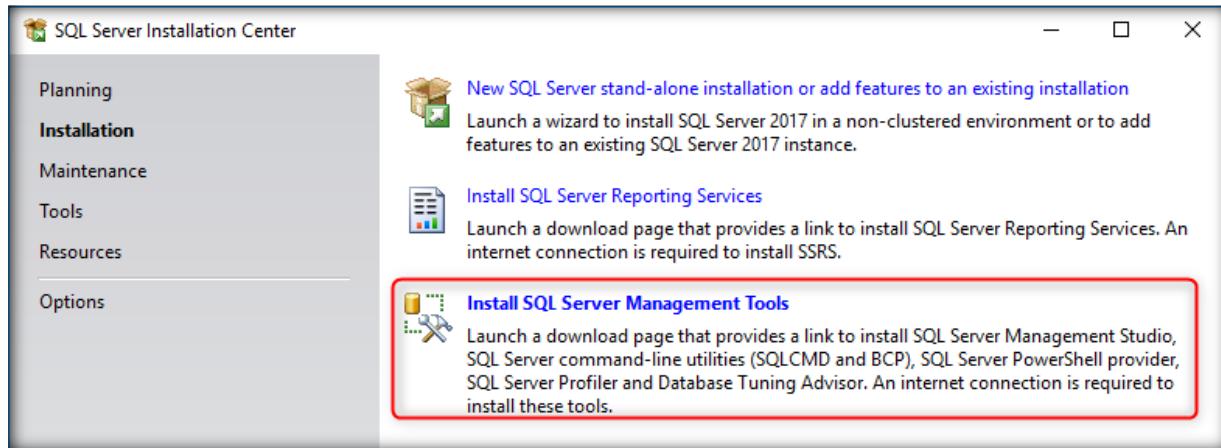


32. **Complete** window appears, providing a link that redirects to the location of the **summary log file** for the installation and other **important notes**

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

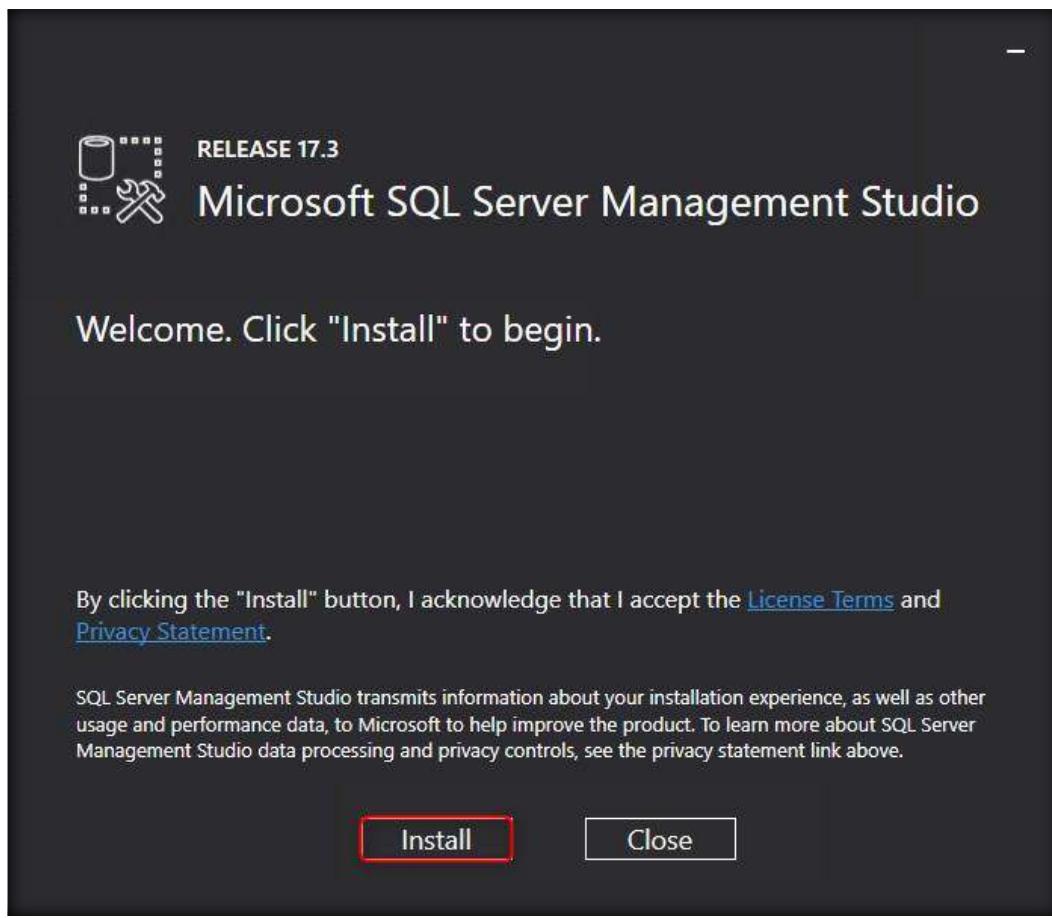
Note: The software version may vary in your lab environment

The screenshot shows a web browser displaying a Microsoft page about SSMS. The URL in the address bar is <https://docs.microsoft.com/en-us/sql/ssms/>. The page content includes a sidebar with 'Download SSMS' and various tools like Object Explorer, Solution Explorer, and Visual Database Tools. The main content area starts with 'SSMS is free!' and describes SSMS 17.x. Two download links are shown: 'Download SQL Server Management Studio 17.3' and 'Download SQL Server Management Studio 17.3 Upgrade Package (upgrades 17.x to 17.3)'. A red box highlights the first download link. At the bottom, a download dialog box asks 'Do you want to run or save SSMS-Setup-ENU.exe (800 MB) from download.microsoft.com?'. The 'Save' button is highlighted with a red box.

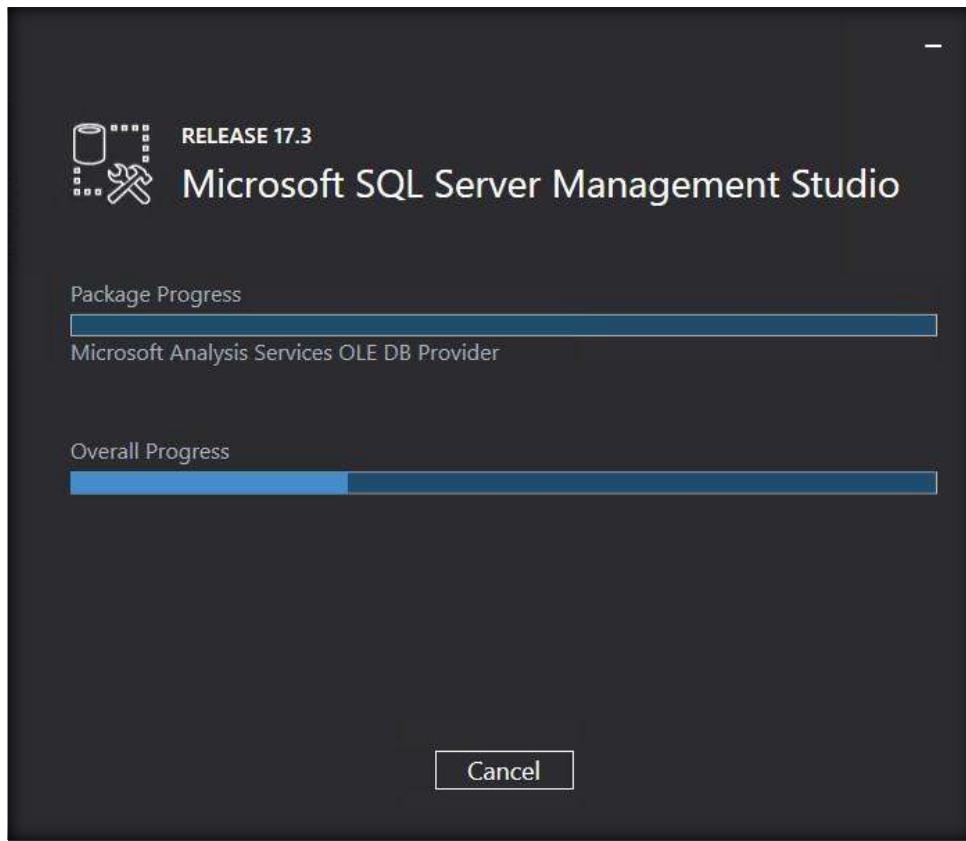
36. Open your downloads folder and double-click the application downloaded in the previous step. Click **Run** if security warning pop-up appears



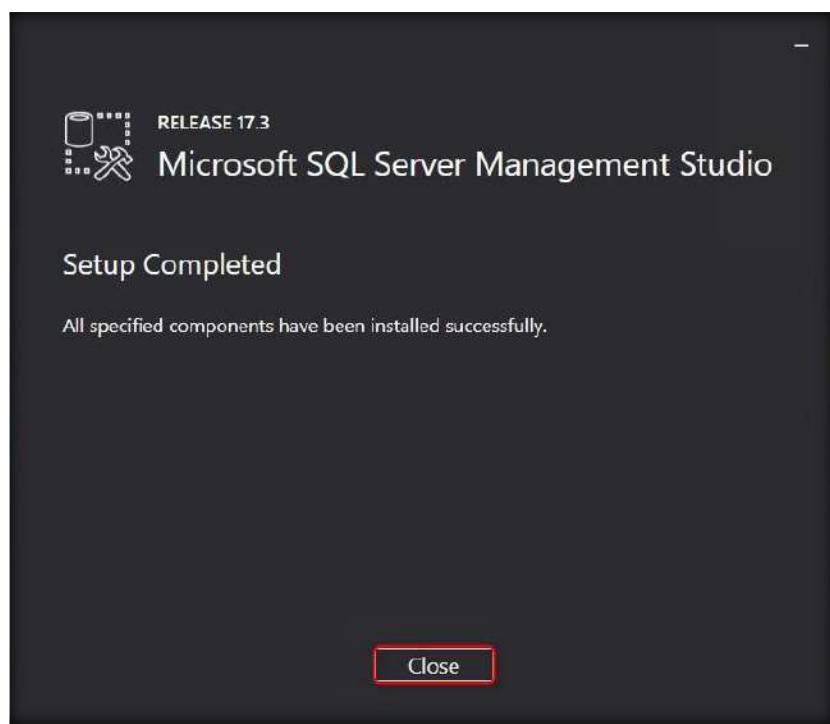
37. Microsoft SQL Server Management Studio welcome screen appears, click **Install** to begin the setup



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

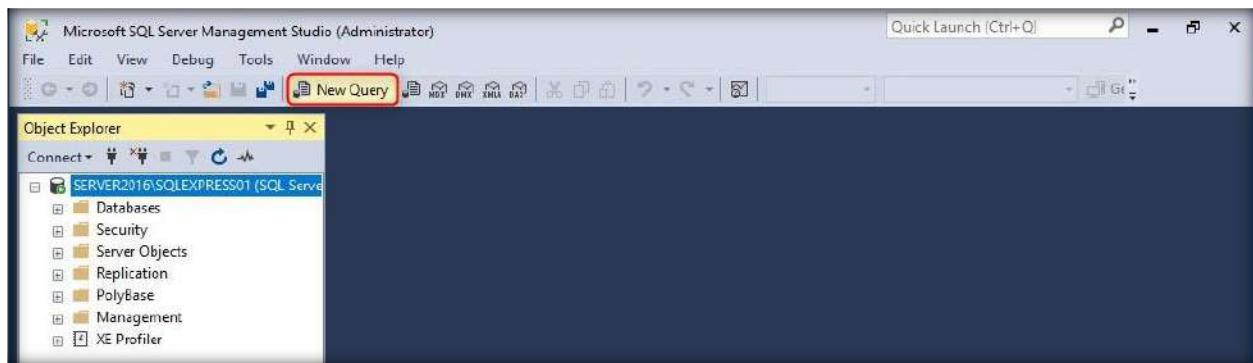
Important Note:

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



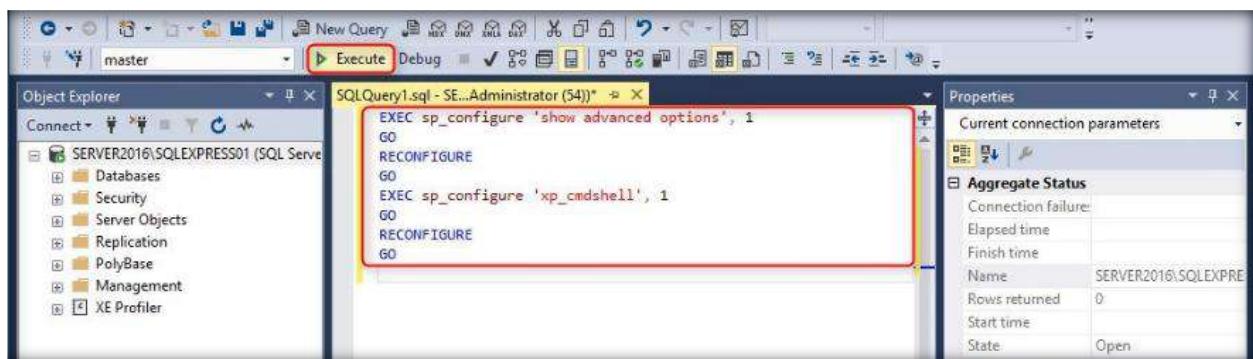
6. When the server is connected, click **New Query** button from menu bar



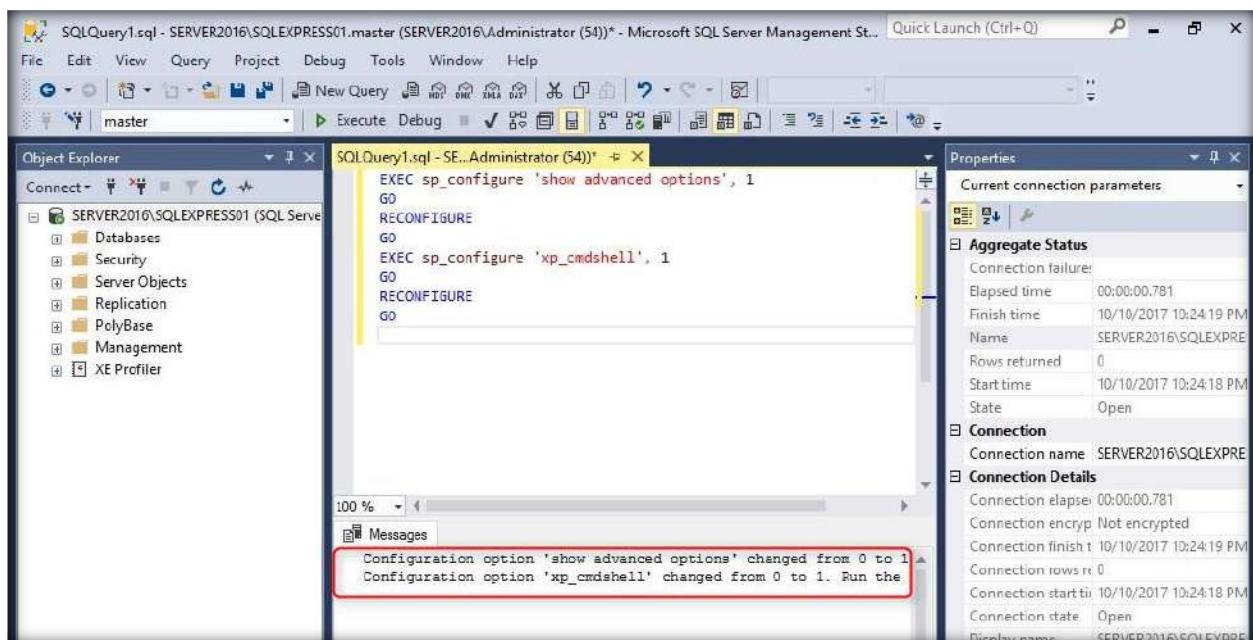
7. **SQL Query** window appears in the right pane of the window

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

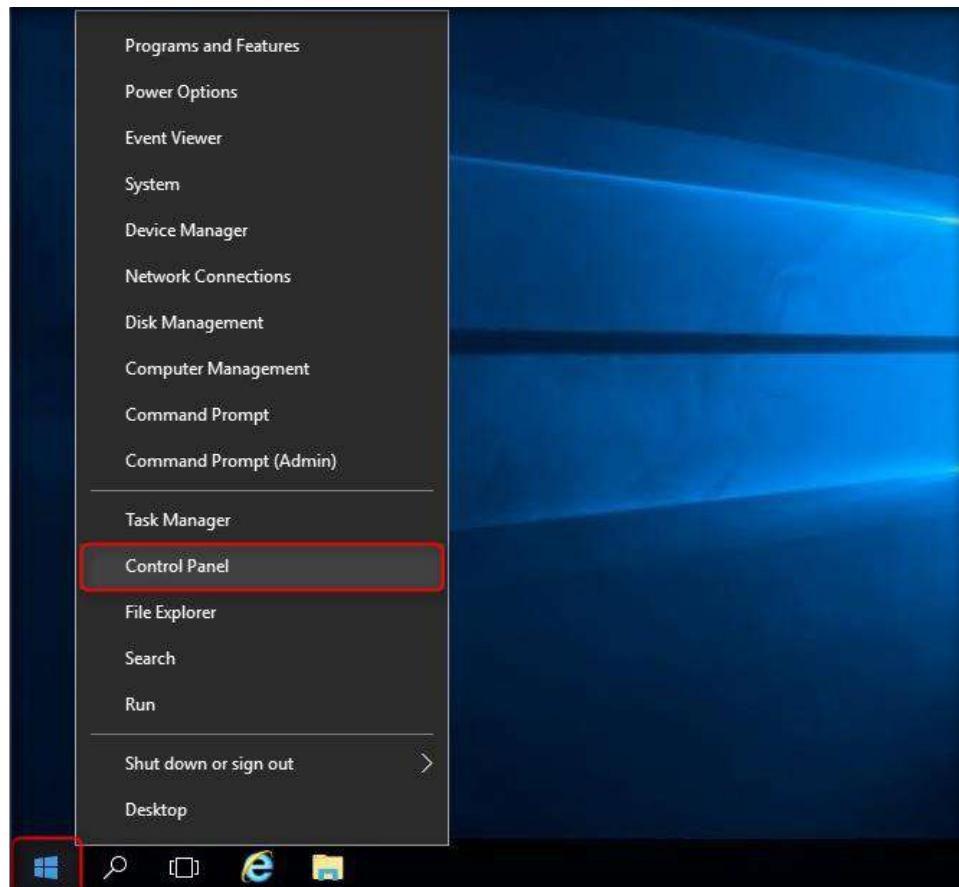
[\[Back to Configuration Task Outline\]](#)

CT#23: Turn off Firewall in all the Machines

Windows Server 2016 (virtual machine)

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

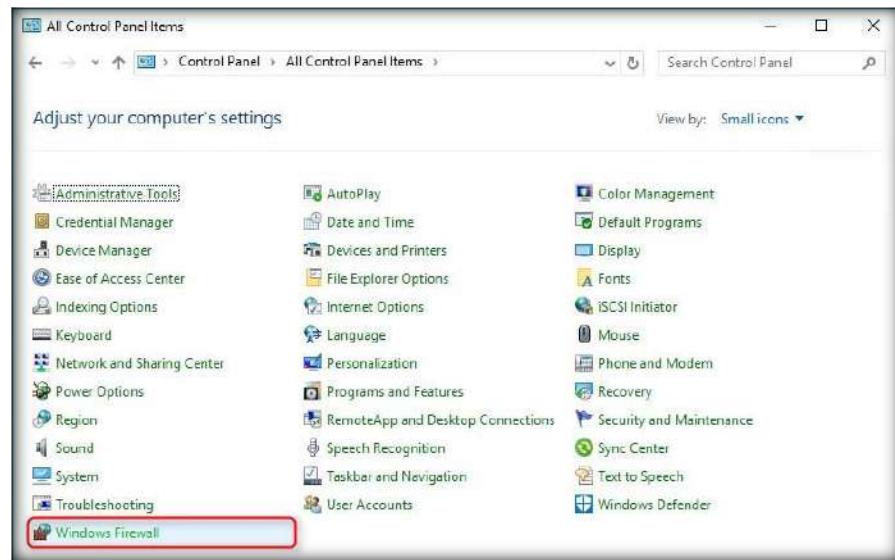
1. Right-click **Windows** icon at the lower left corner of the screen, click **Control Panel** from the context menu



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



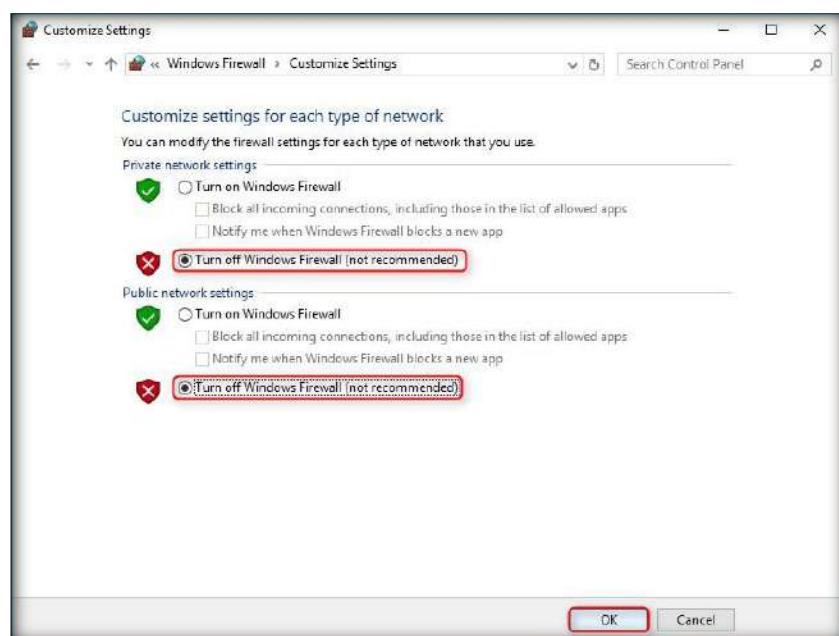
3. All Control Panel Items Window, click **Windows Firewall**



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



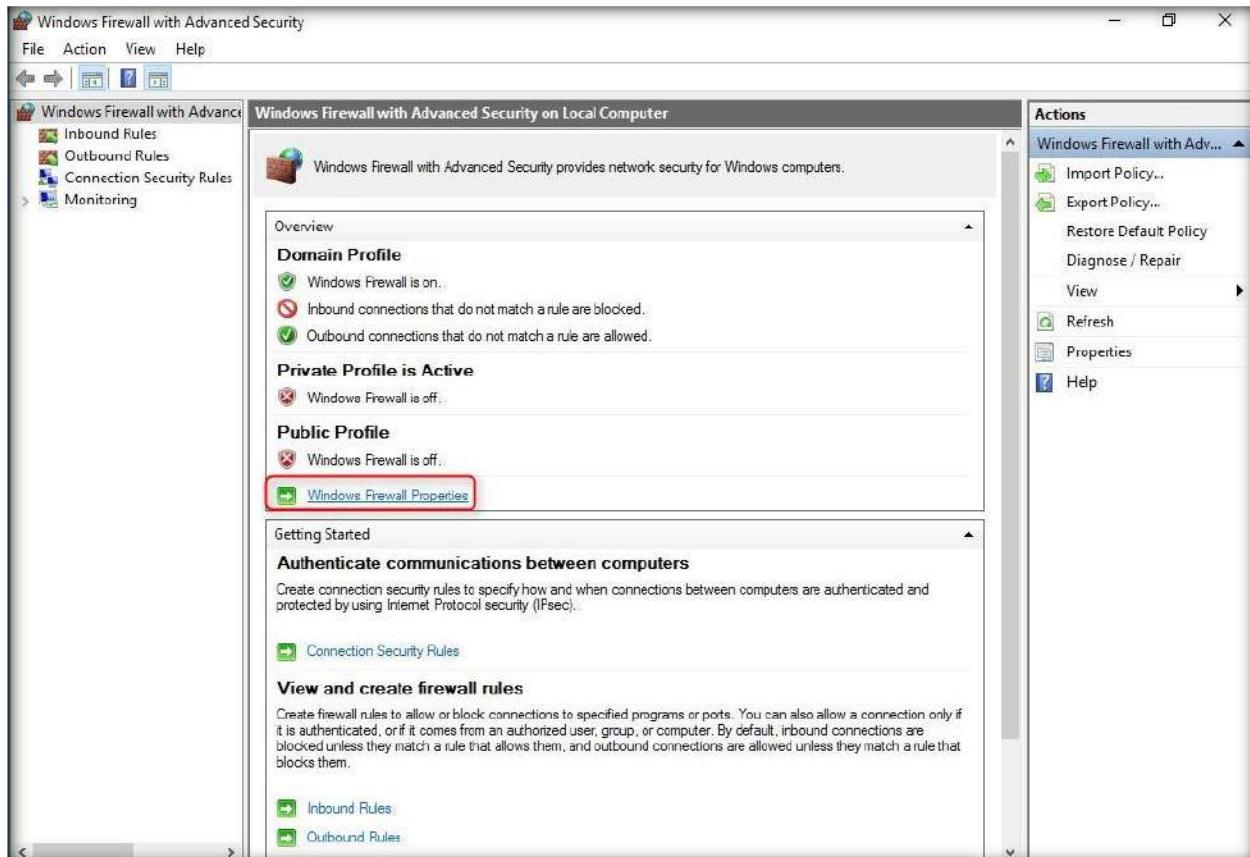
5. In **Customize Settings** window, select the radio button **Turn off Windows Firewall (not recommended)** for both Private and Public network settings and click **OK**



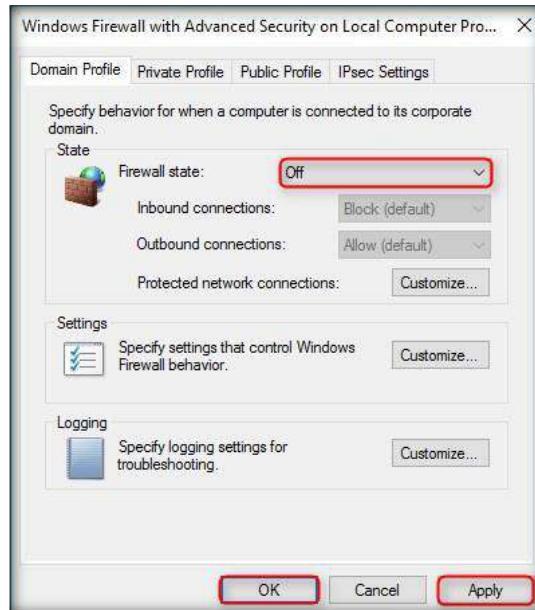
6. In the Windows Firewall control panel, click **Advanced settings** link in the left pane



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**:

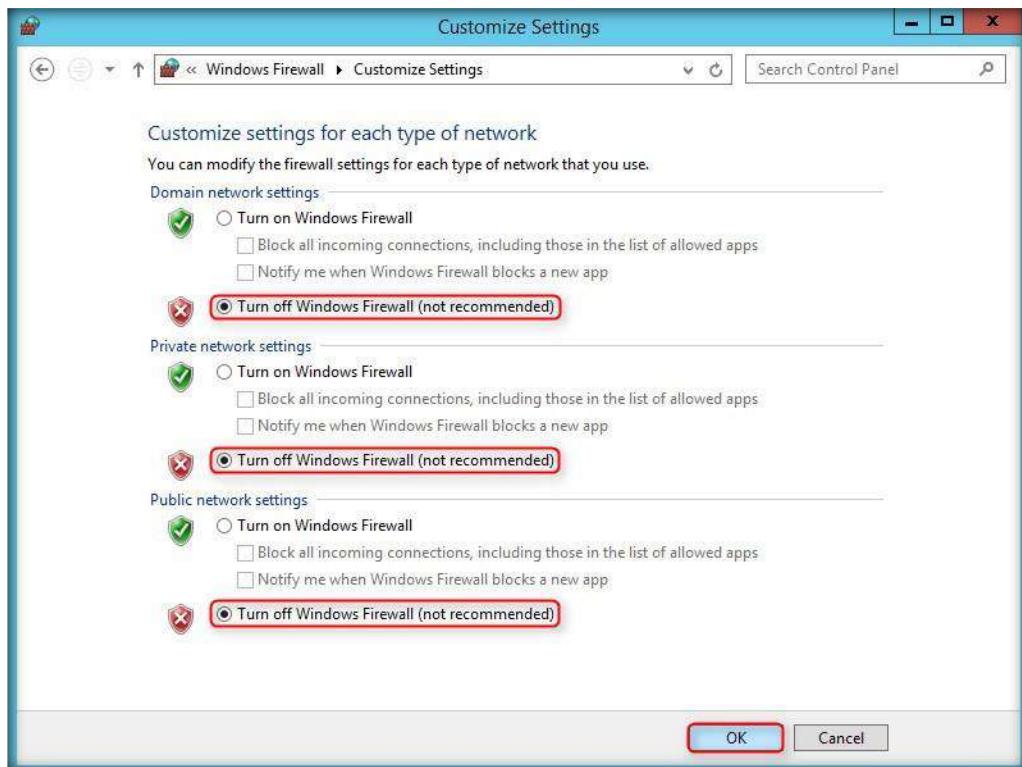
1. Go to **Start → Control Panel → All Control Panel Items**
2. Click **Windows Firewall** icon in Control Panel to launch Windows Firewall



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**



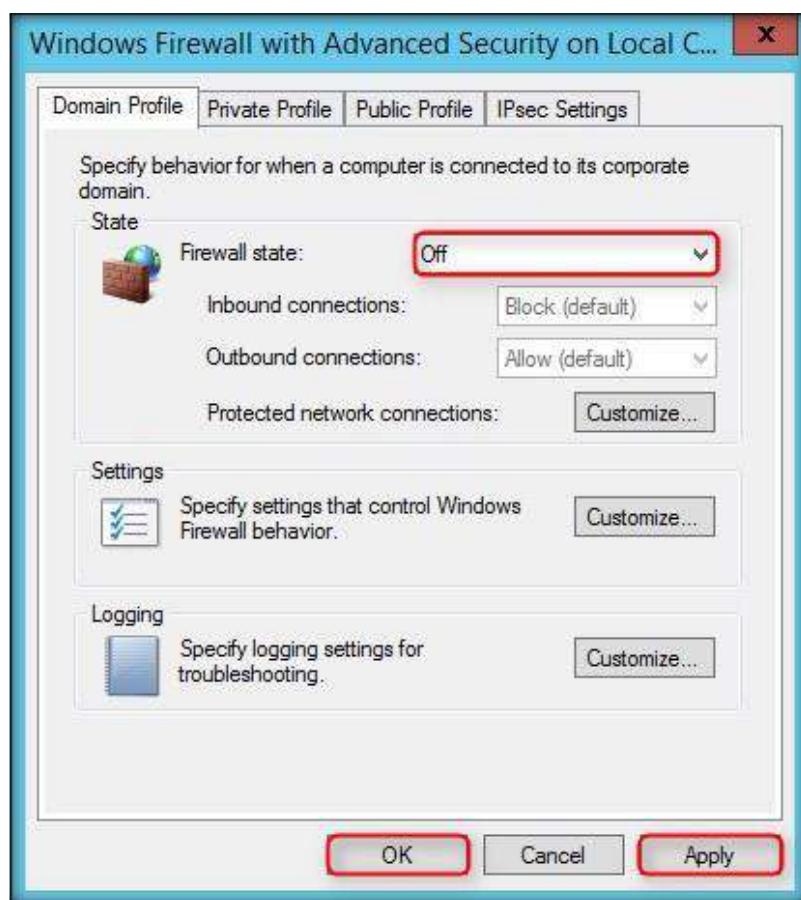
5. In the Windows Firewall control panel, click **Advanced settings** link in the left pane



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**:

- 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**:

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



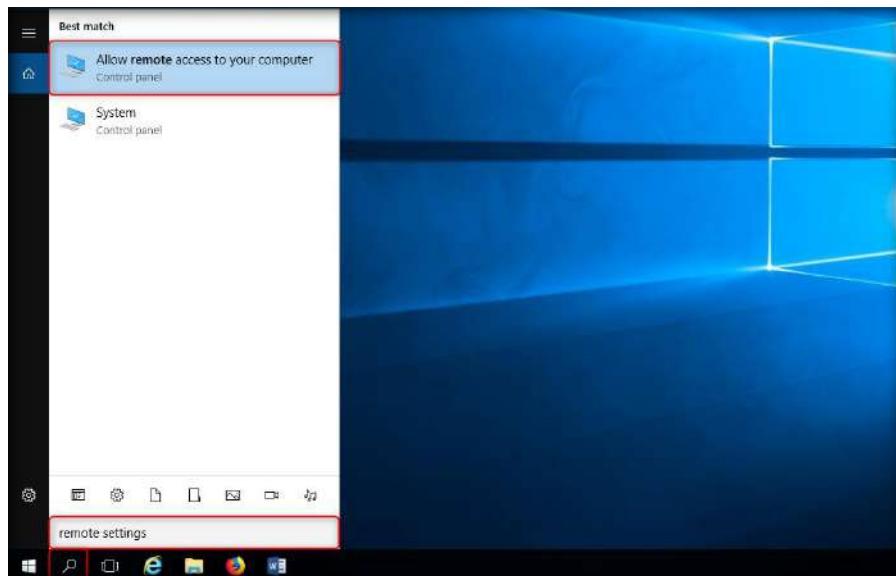
[\[Back to Configuration Task Outline\]](#)

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

Windows Server 2016

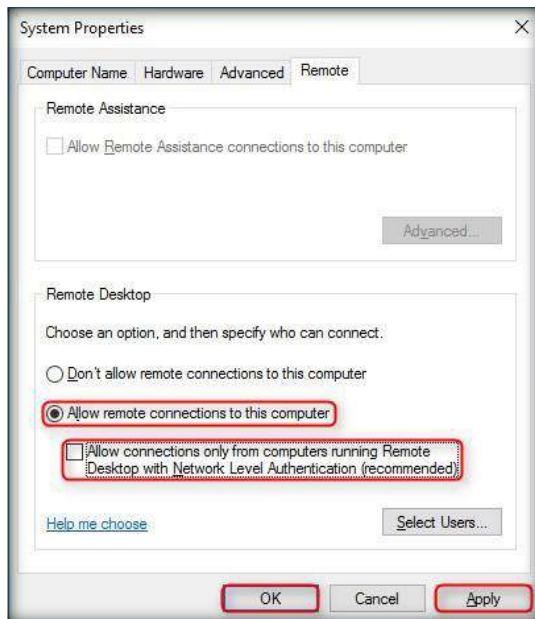
To enable remote desktop connection in **Windows Server 2016**:

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**

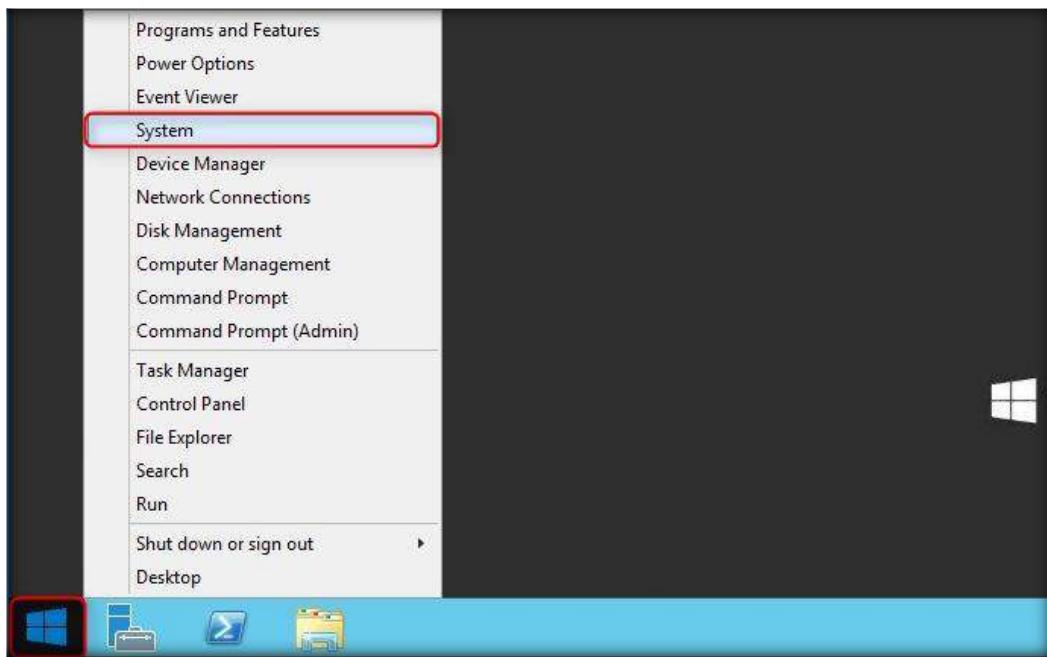
7. Repeat the same steps for **windows 10**



Windows Server 2012

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

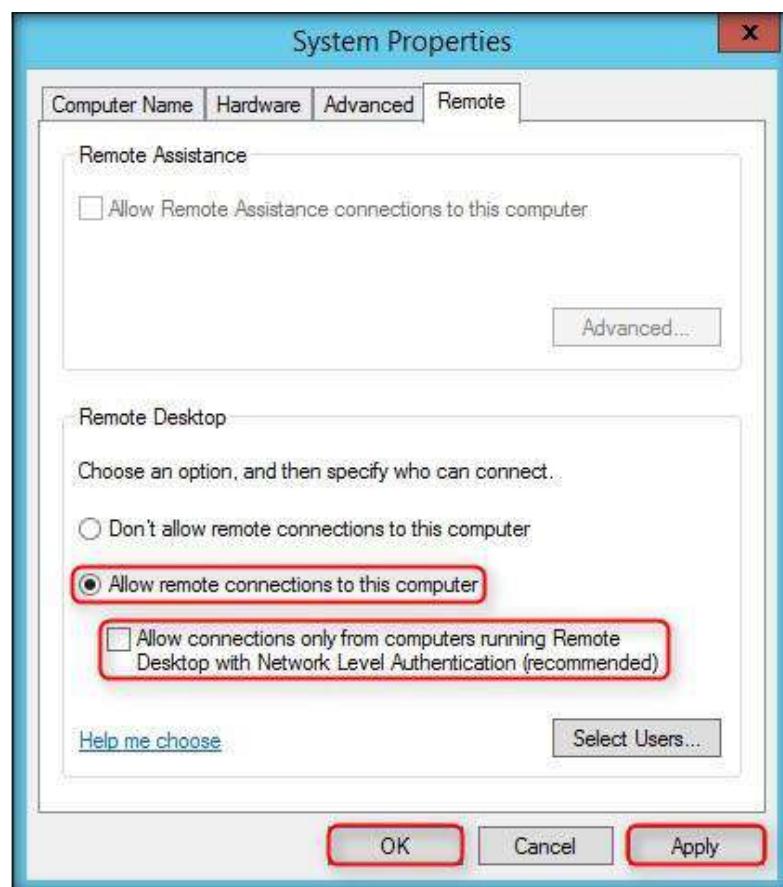
1. Right-click **Start** button and click **System**



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**

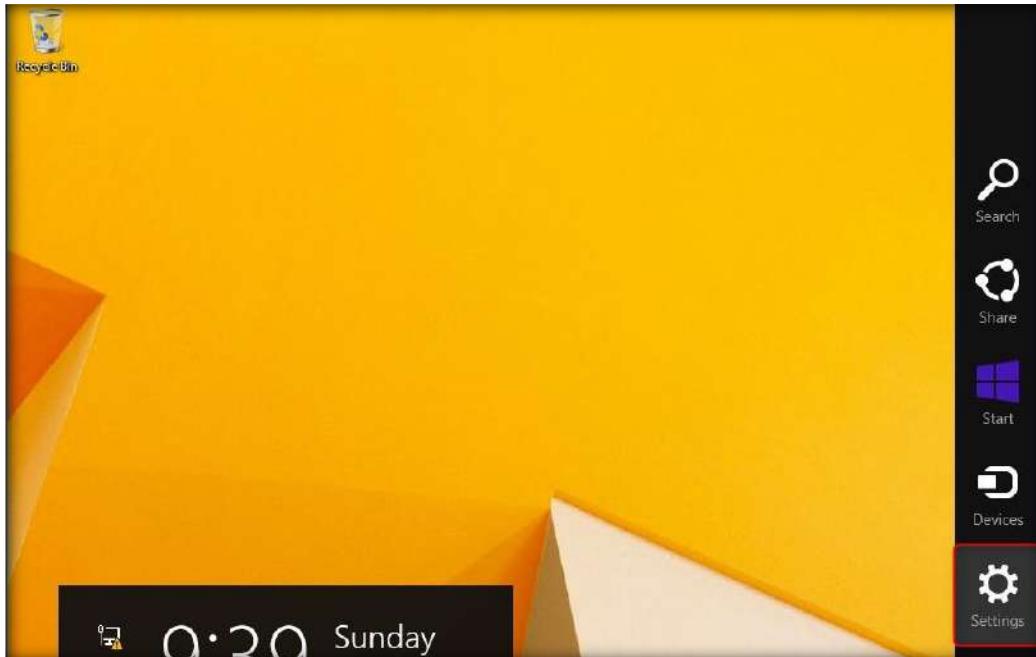


[\[Back to Configuration Task Outline\]](#)

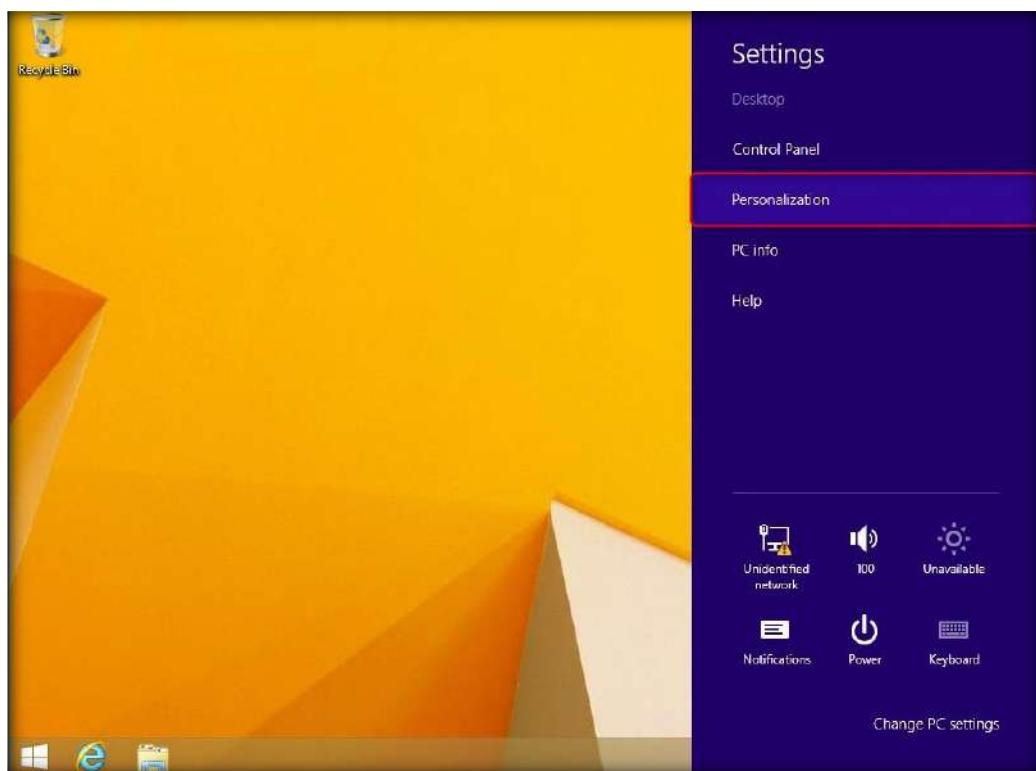
CT#25: Turn off Screen Savers in all the Machines

Windows 8

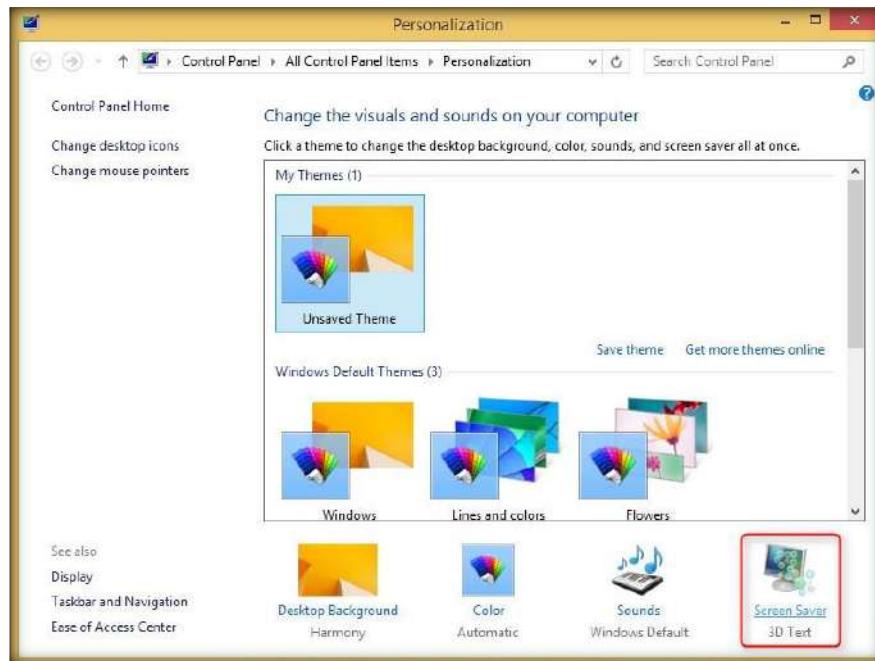
1. Move your mouse on the right side of the desktop screen to get the menu pane, select **Settings**



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**

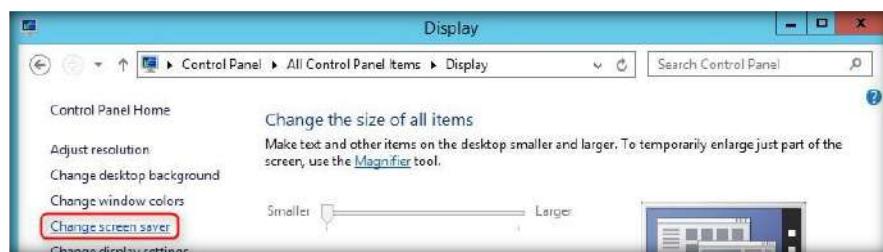


Windows Server 2012

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**

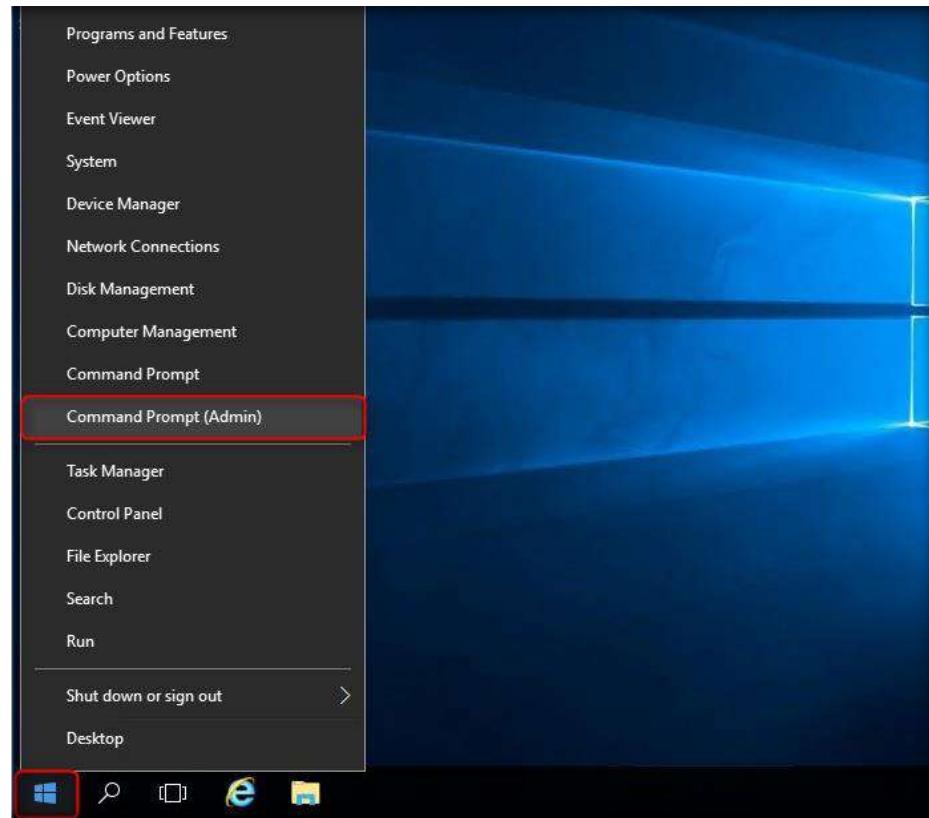


5. In some windows operating systems such as Windows Server 2016 and Windows 10, you are not able to change the personalization settings unless your system is activated

[\[Back to Configuration Task Outline\]](#)

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)

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 10.10.10.10

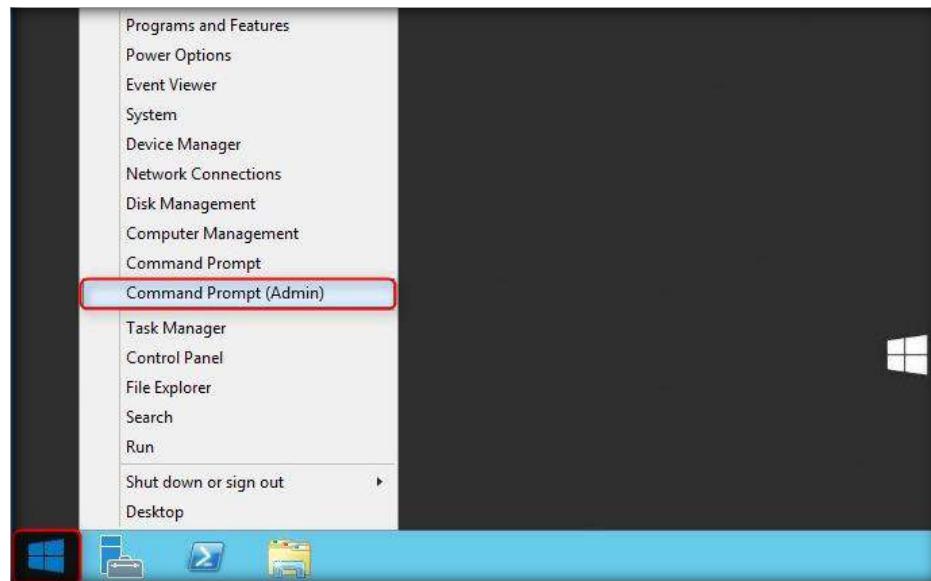
Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\system32>
```

A screenshot of a Windows Command Prompt window titled "Administrator: Command Prompt". The window shows the command "ping 10.10.10.10" being run. The output shows four successful replies from the target IP address. Below the ping results, the "Ping statistics for 10.10.10.10:" section provides details about the packet exchange. The entire window is framed by a black border.

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)

```

Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ping 10.10.10.16
Pinging 10.10.10.16 with 32 bytes of data:
Reply from 10.10.10.16: bytes=32 time<1ms TTL=128
Reply from 10.10.10.16: bytes=32 time=3ms TTL=128
Reply from 10.10.10.16: bytes=32 time<1ms TTL=128
Reply from 10.10.10.16: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.16:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 0ms

C:\Windows\system32>

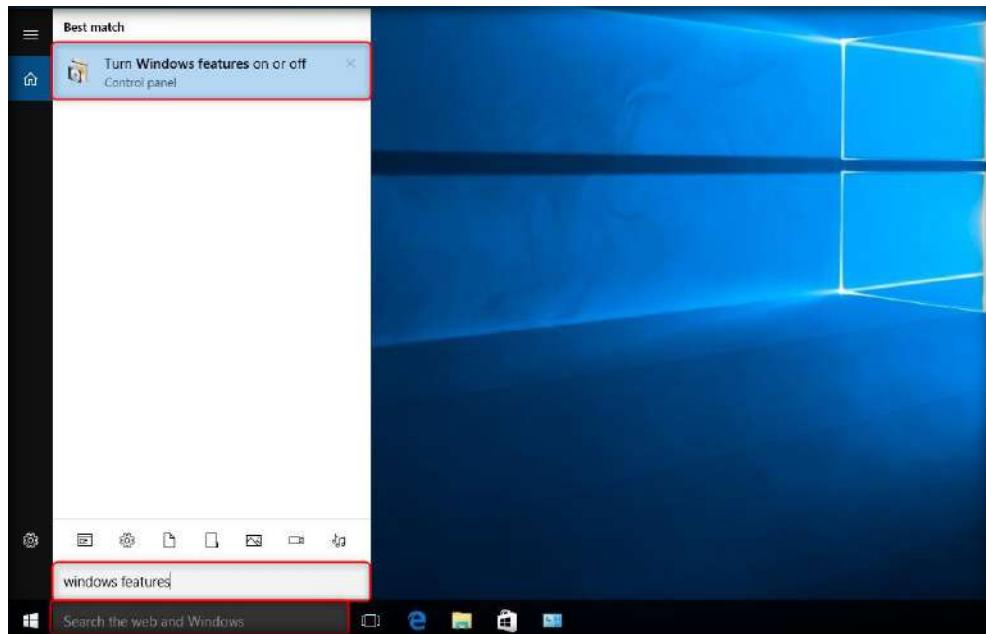
```

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

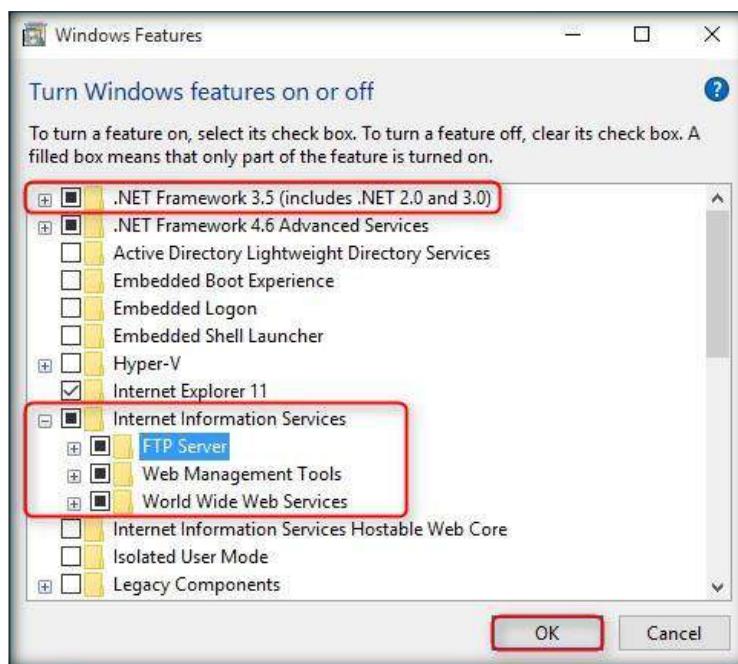
[\[Back to Configuration Task Outline\]](#)

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

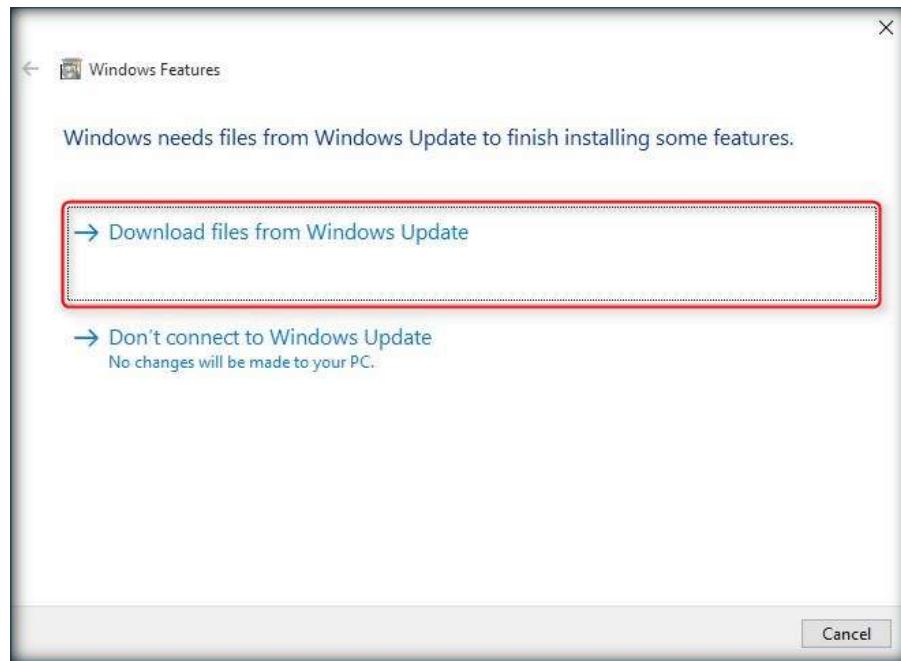
1. Login into your **Windows 10** virtual machine and in Search the web and Windows bar type **windows features**
2. Click **Turn Windows features on or off** as shown in the screenshot below



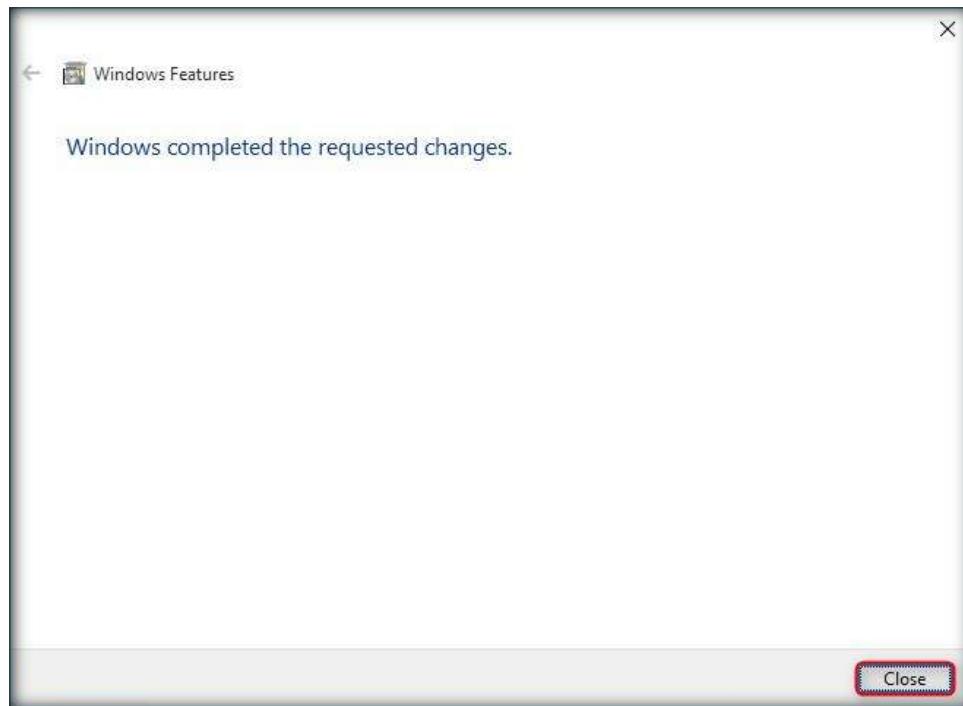
3. Windows Features window appears, select **.NET Framework 3.5 (includes .NET 2.0 and 3.0)** and **FTP Server, Web Management Tools** and **World Wide Web Services** under **Internet Information Services**. Click **OK** to install these features



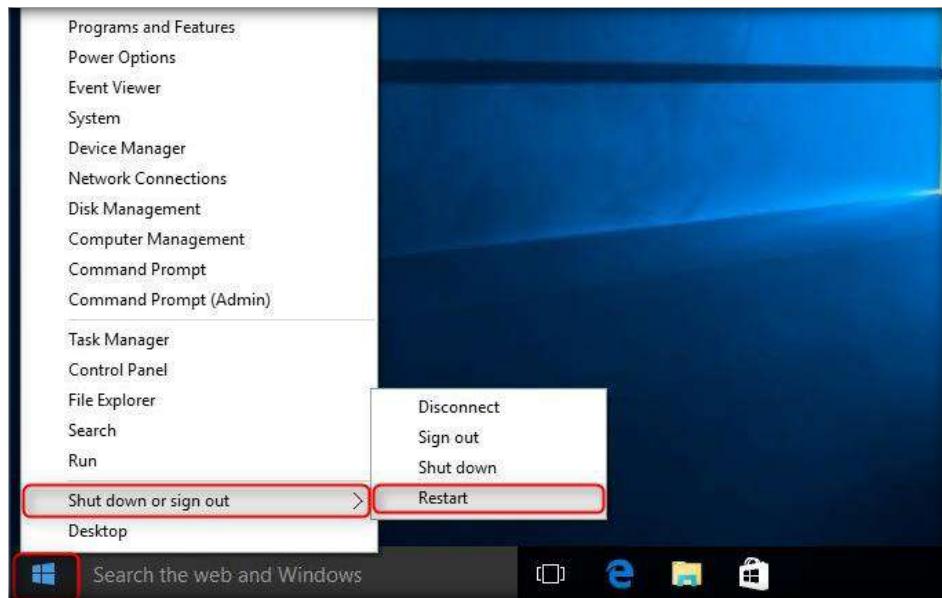
4. Click **Download files from Windows Update** as shown in the screenshot below:



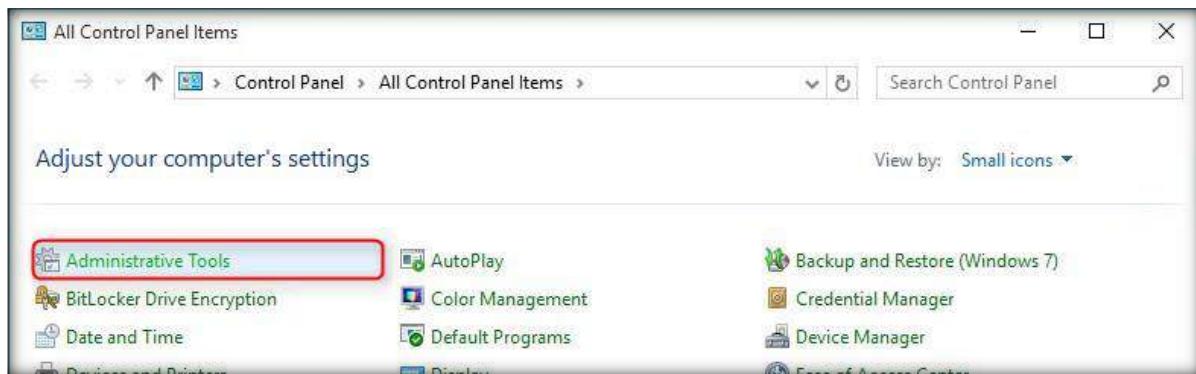
5. After the features have been successfully installed, click **Close** to exit Windows Features window



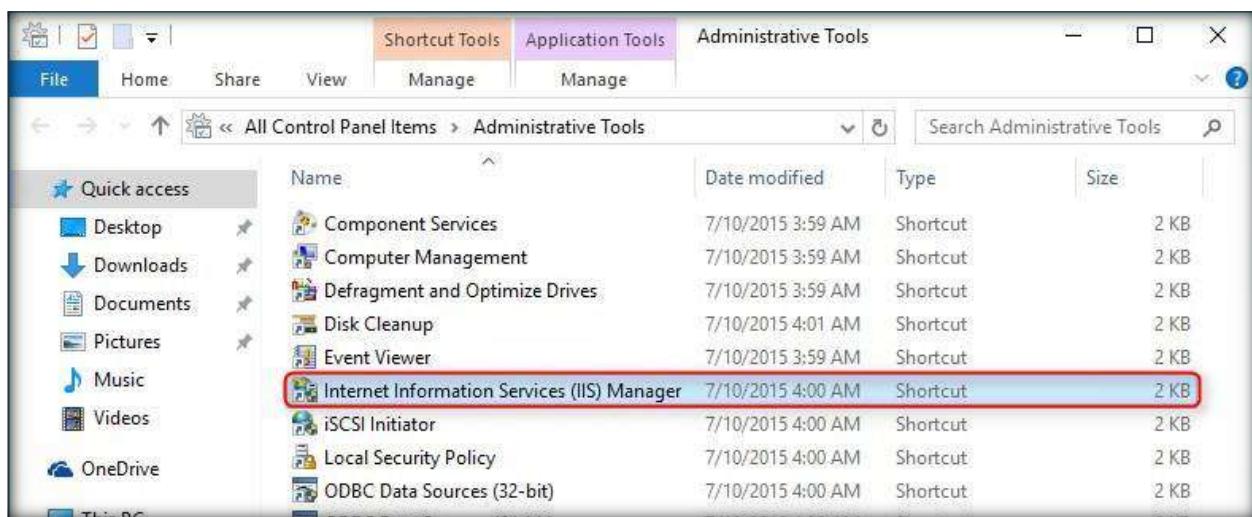
6. Once done, close all the windows and restart **Windows 10** virtual machine



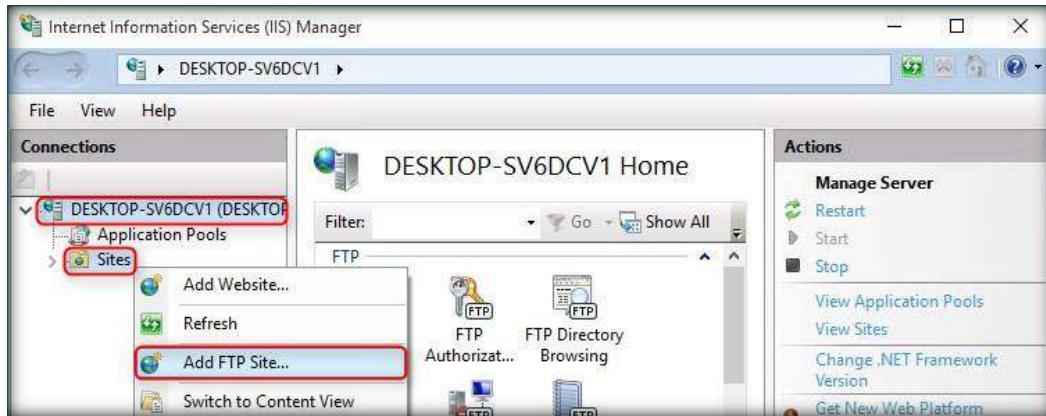
7. Once Windows 10 machine is restarted navigate to **Control Panel → All Control Panel Items → Administrative Tools**



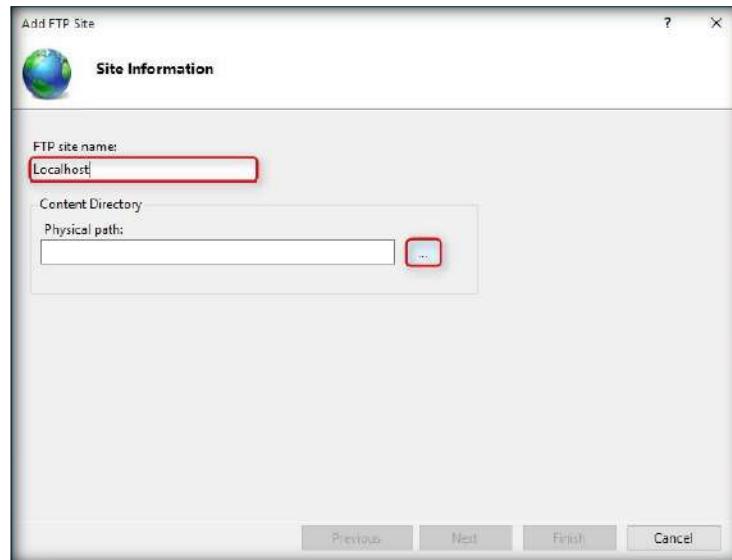
8. In Administrative Tools window double-click **Internet Information Services (IIS) Manager**



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



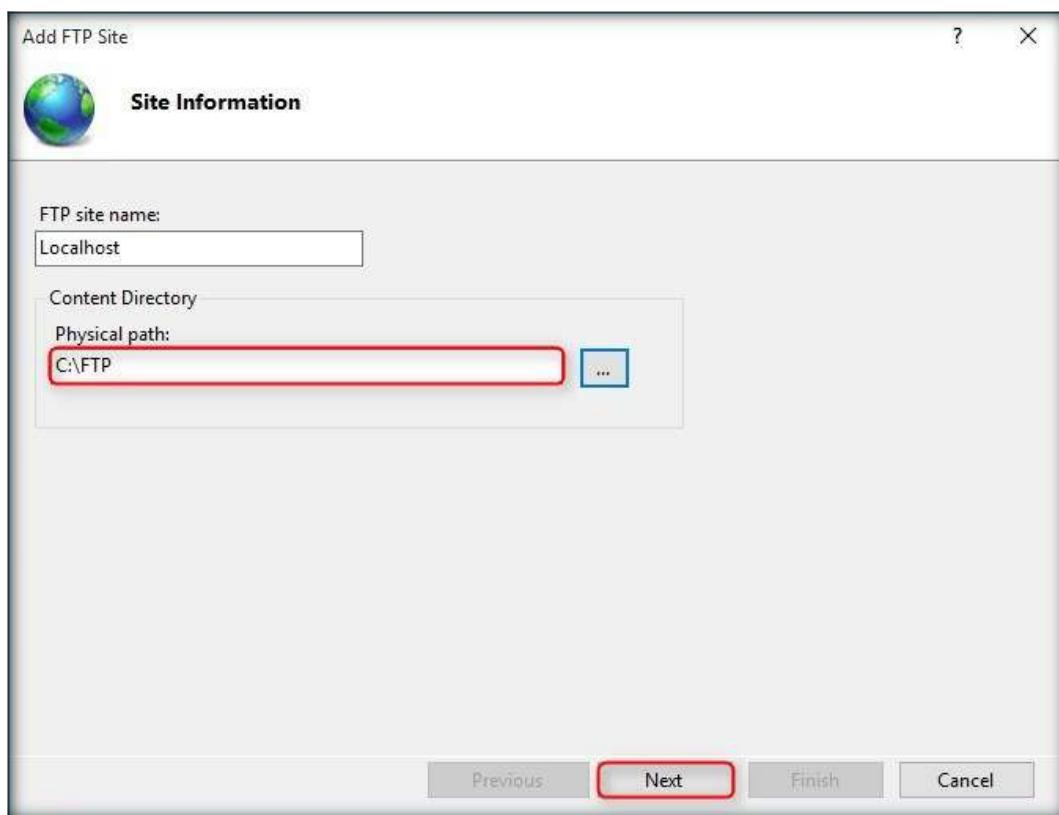
11. **Browse For Folder** wizard appears choose **C:** (or any drive) click **Make New Folder**



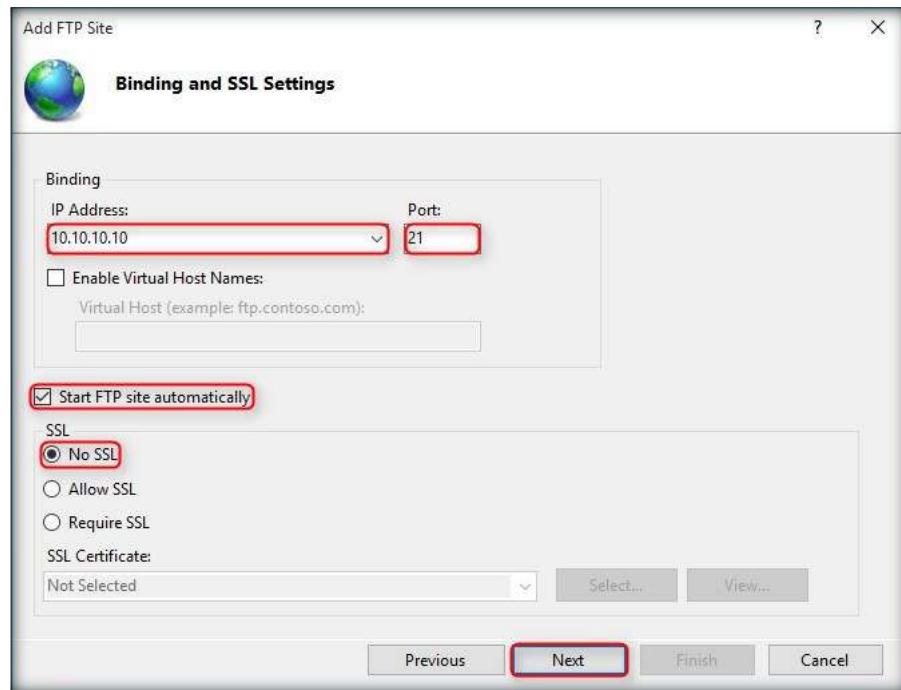
12. A New Folder will be created. Rename it as **FTP** and click **OK**



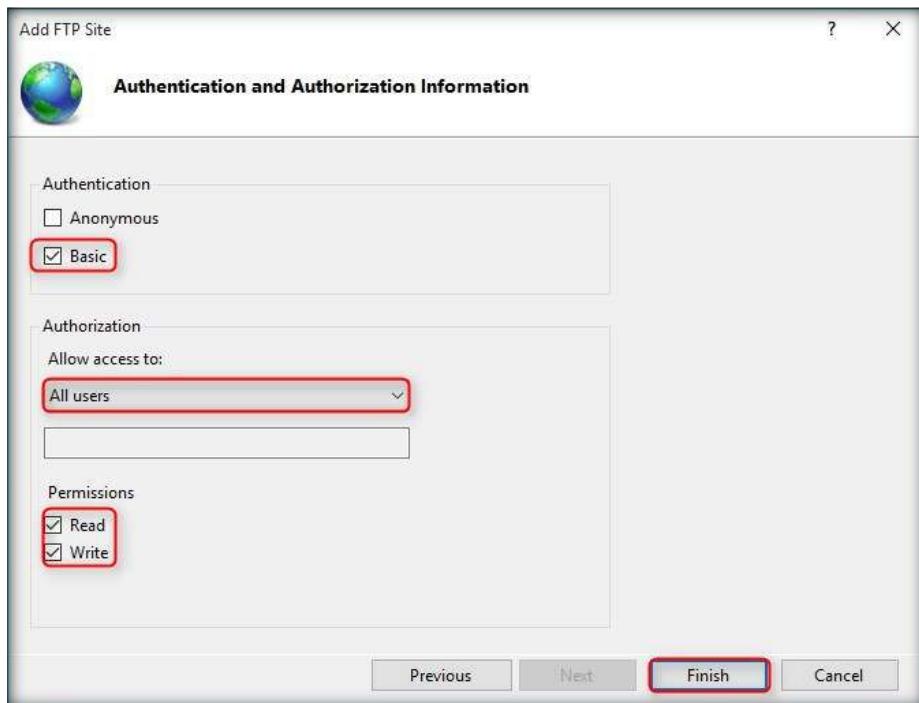
13. After Physical path is provided click **Next** button



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 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:



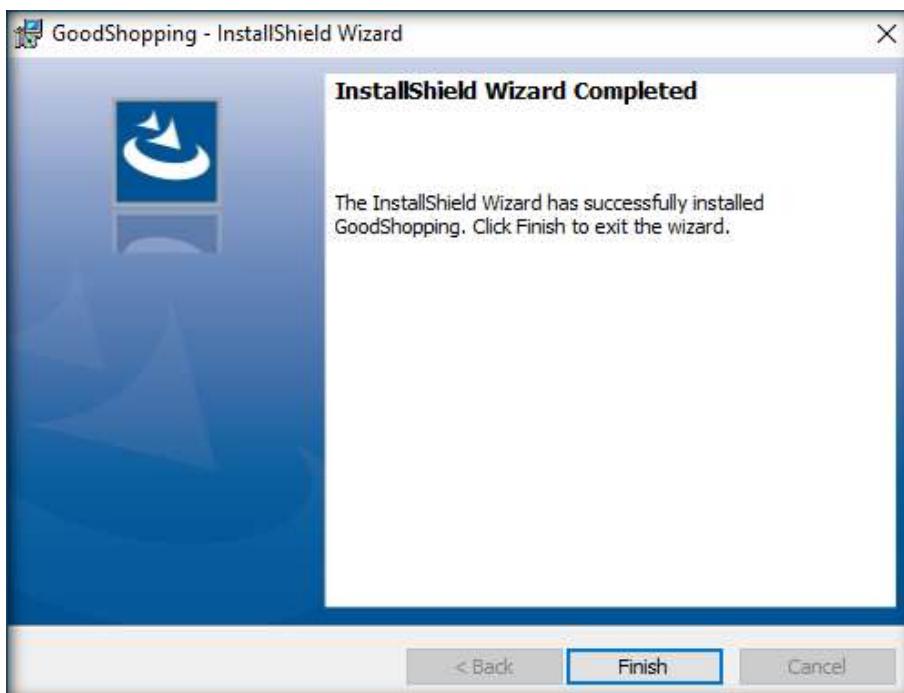
[\[Back to Configuration Task Outline\]](#)

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

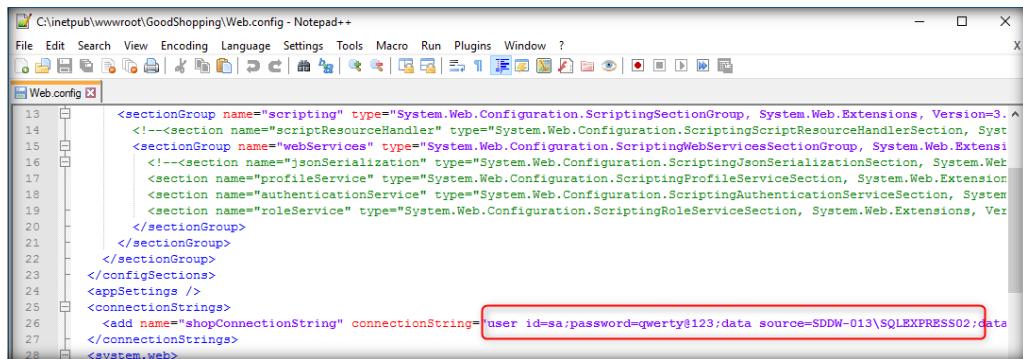
1. Navigate to **Z:\CEH-Tools\CEHv10 Lab Prerequisites\Websites**
2. Open **GoodShopping** folder. Double click on **setup.exe** and follow the wizard driven installation steps



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**

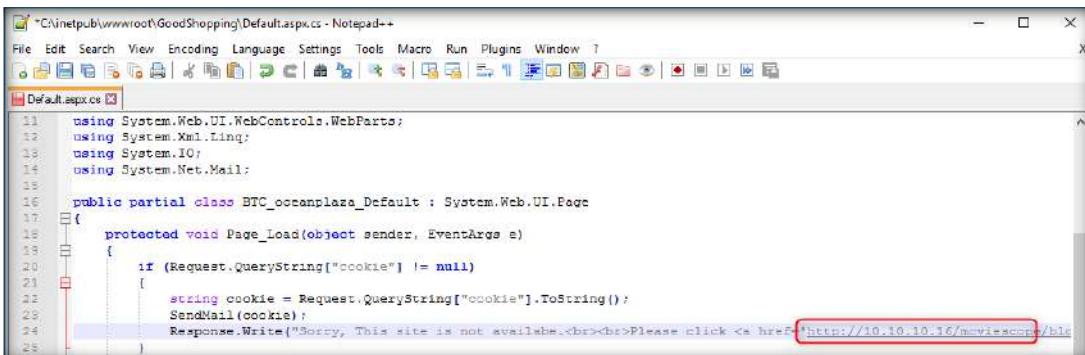


```

C:\inetpub\wwwroot\GoodShopping\Web.config - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Web.config [x]
<sectionGroup name="scripting" type="System.Web.Configuration.ScriptingSectionGroup, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35">
  <!--<section name="scriptResourceHandler" type="System.Web.Configuration.ScriptingScriptResourceHandlerSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35">
  <sectionGroup name="webServices" type="System.Web.Configuration.ScriptingWebServicesSectionGroup, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35">
    <!--<section name="jsonSerialization" type="System.Web.Configuration.ScriptingJsonSerializationSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35">
    <section name="authenticationService" type="System.Web.Configuration.ScriptingProfileServiceSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35">
      <section name="roleService" type="System.Web.Configuration.ScriptingRoleServiceSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35">
        </section>
      </sectionGroup>
    </sectionGroup>
  </configSections>
<appSettings />
<connectionStrings>
  <add name="shopConnectionString" connectionString="user id=sa:password=qwerty@123:data source=SDDW-013\SQLEXPRESS02:port=1433;integrated security=true;multipleactiveresultsets=true;packet size=4096;"/>
</connectionStrings>
<system.web>

```

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.



```

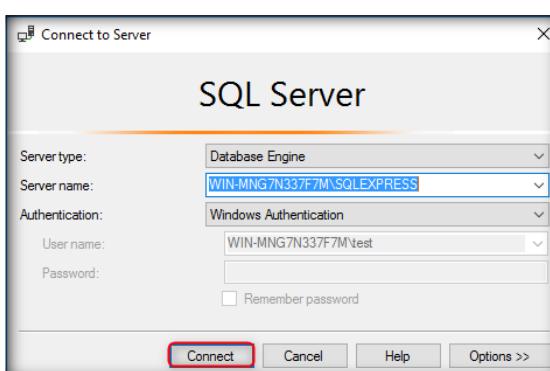
C:\inetpub\wwwroot\GoodShopping\Default.aspx.cs - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Default.aspx.cs [x]
using System;
using System.Web.UI.WebControls;
using System.Xml.Linq;
using System.IO;
using System.Net.Mail;

public partial class BTC_occanplaza_Default : System.Web.UI.Page
{
    protected void Page_Load(object sender, EventArgs e)
    {
        if (Request.QueryString["cookie"] != null)
        {
            string cookie = Request.QueryString["cookie"].ToString();
            SendMail(cookie);
            Response.Write("Sorry, This site is not available.  
  
Please click <a href='http://10.10.10.16/moviescopy/blo");
        }
    }
}

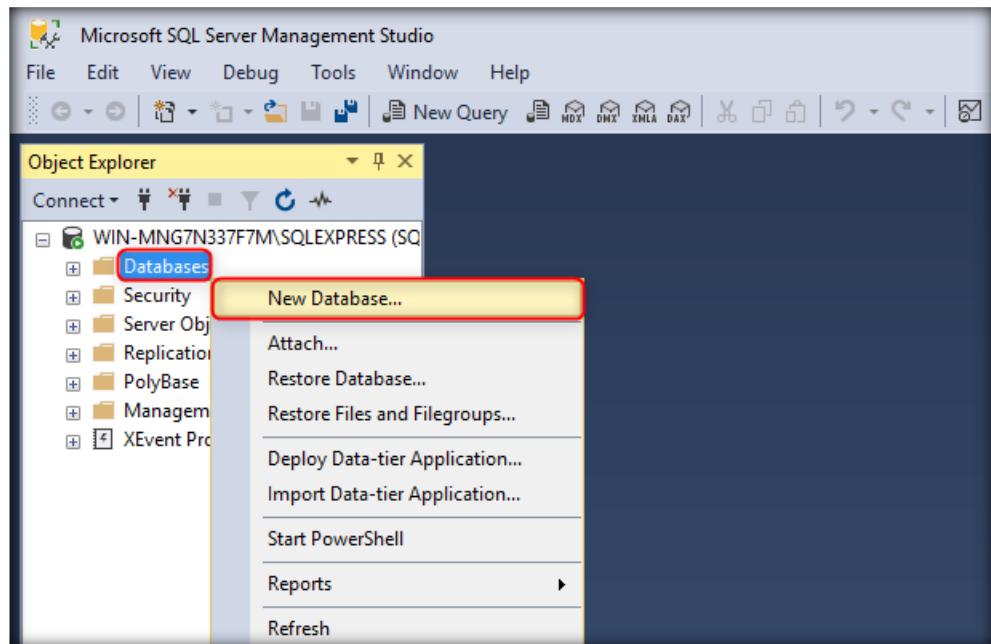
```

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

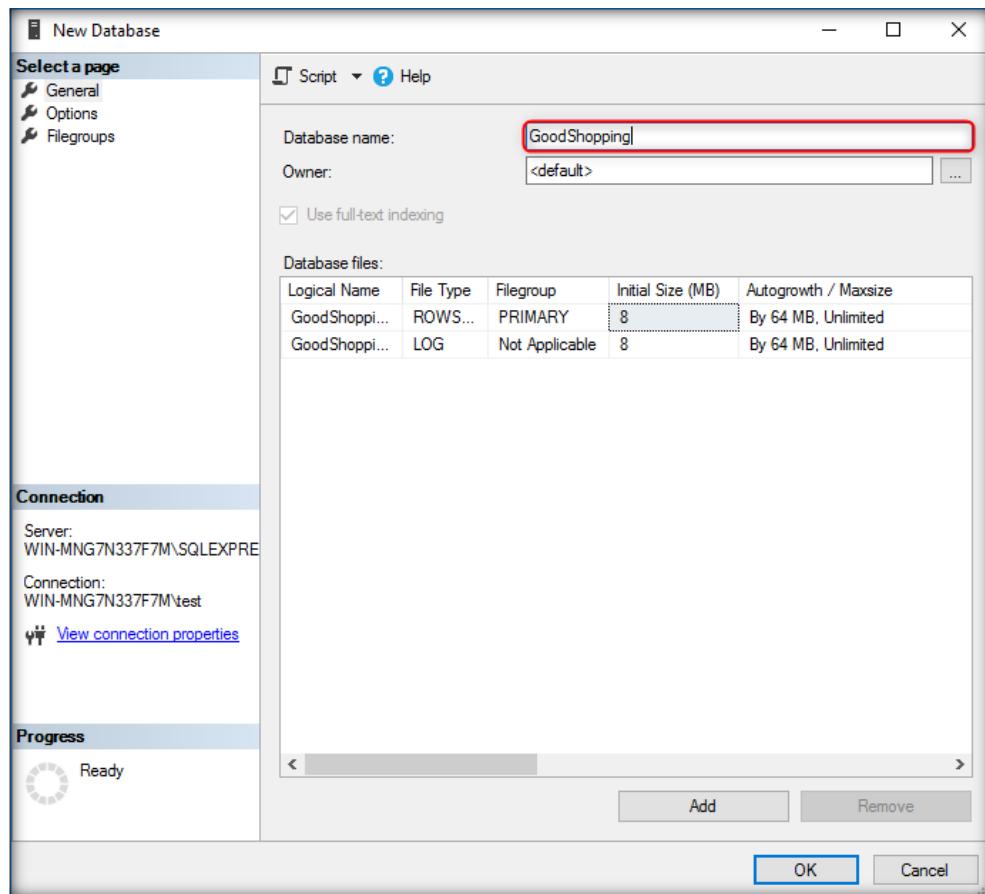
9. **Save** the file and **close** it
10. Now, **Launch** SQL Server 2017 Management Studio click **Connect**



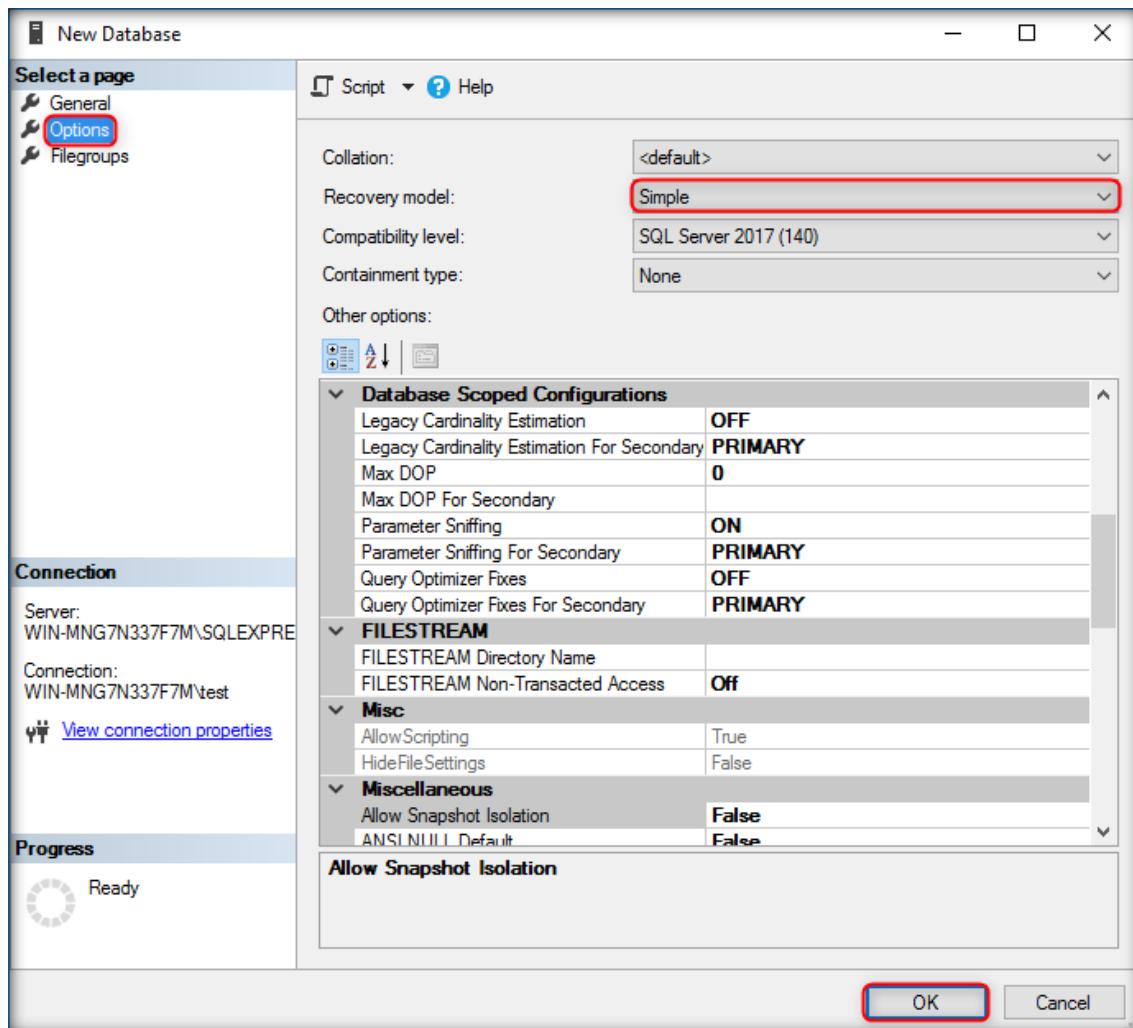
11. Microsoft SQL Server Management Studio window, right-click on **Databases** and select **New Database...**



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

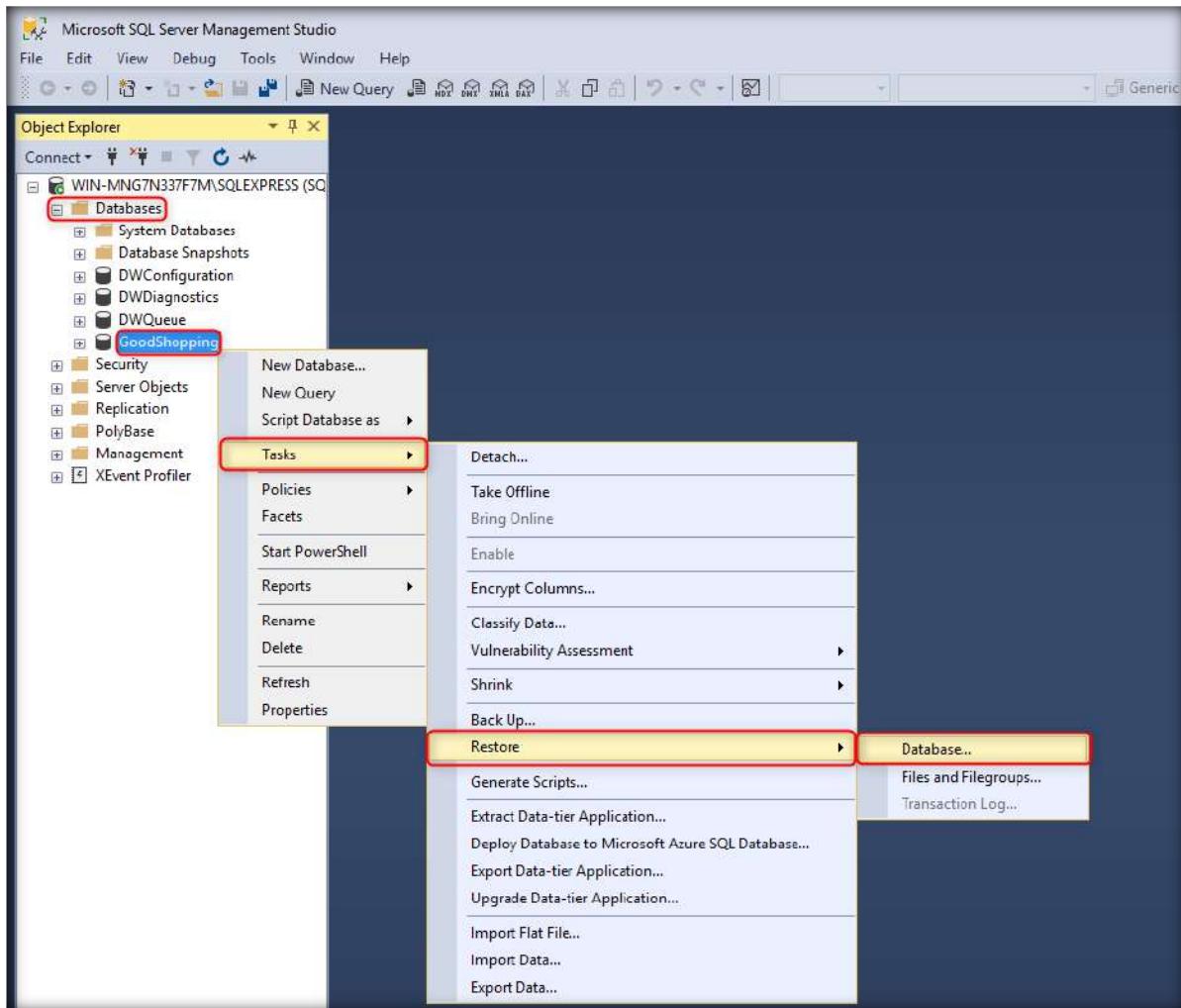


13. Select **Options** from the left pane.
14. Select **Simple** from the **Recovery model** drop-down list and click **OK**.

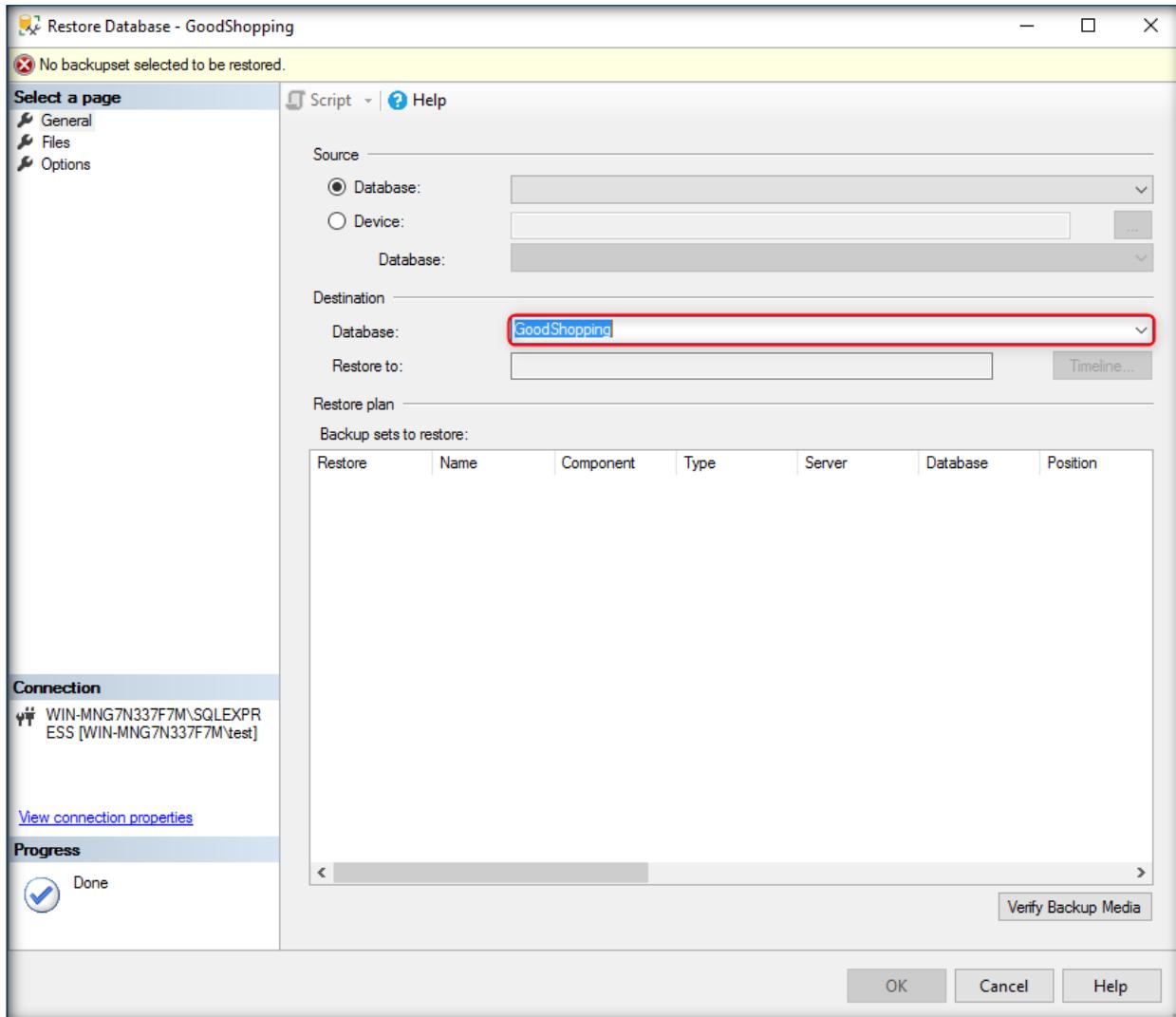


15. Now expand the **Databases** node. You will observe that **GoodShopping** database folder appears under the **Object Explorer** section, which implies that GoodShopping database has been **successfully** created.

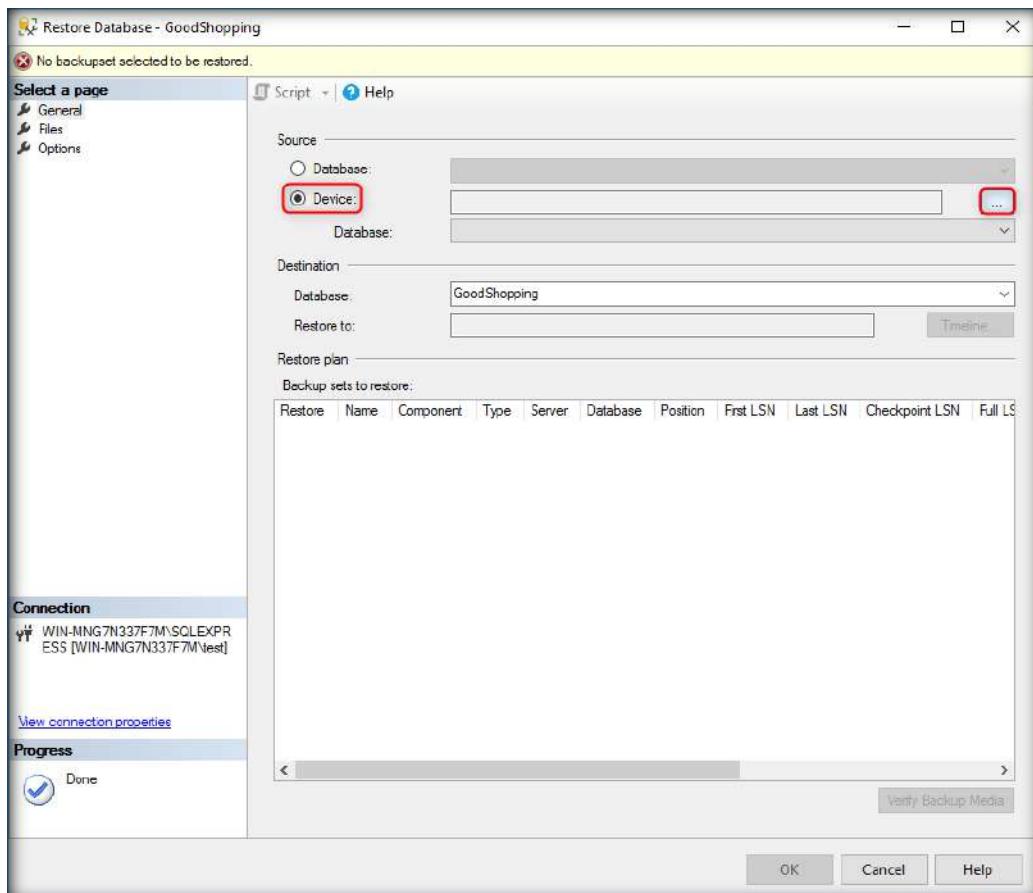
16. **Right-Click** on GoodShopping database and go to **Tasks → Restore → Database...**



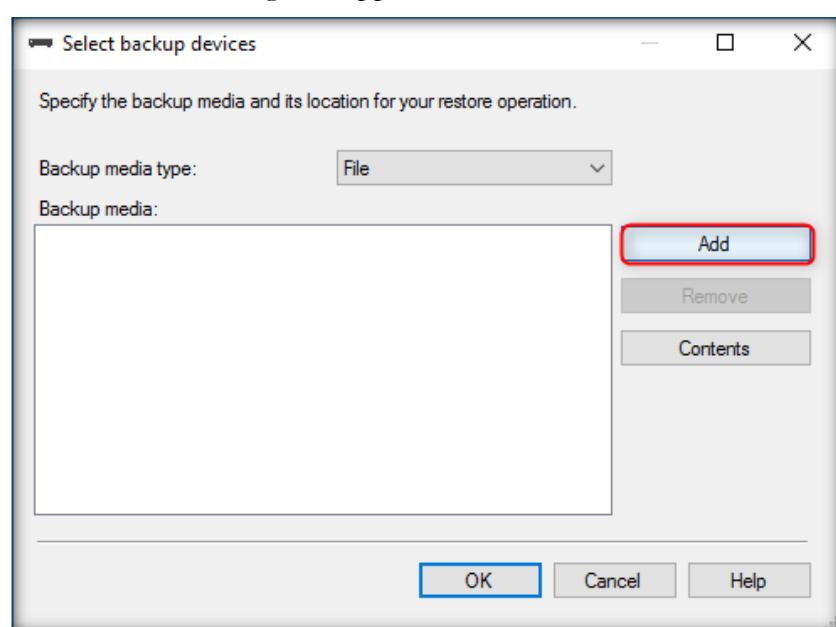
17. **Restore Database – GoodShopping** window appears displaying the database name (**GoodShopping**) in the **Database** field under **Destination** section.



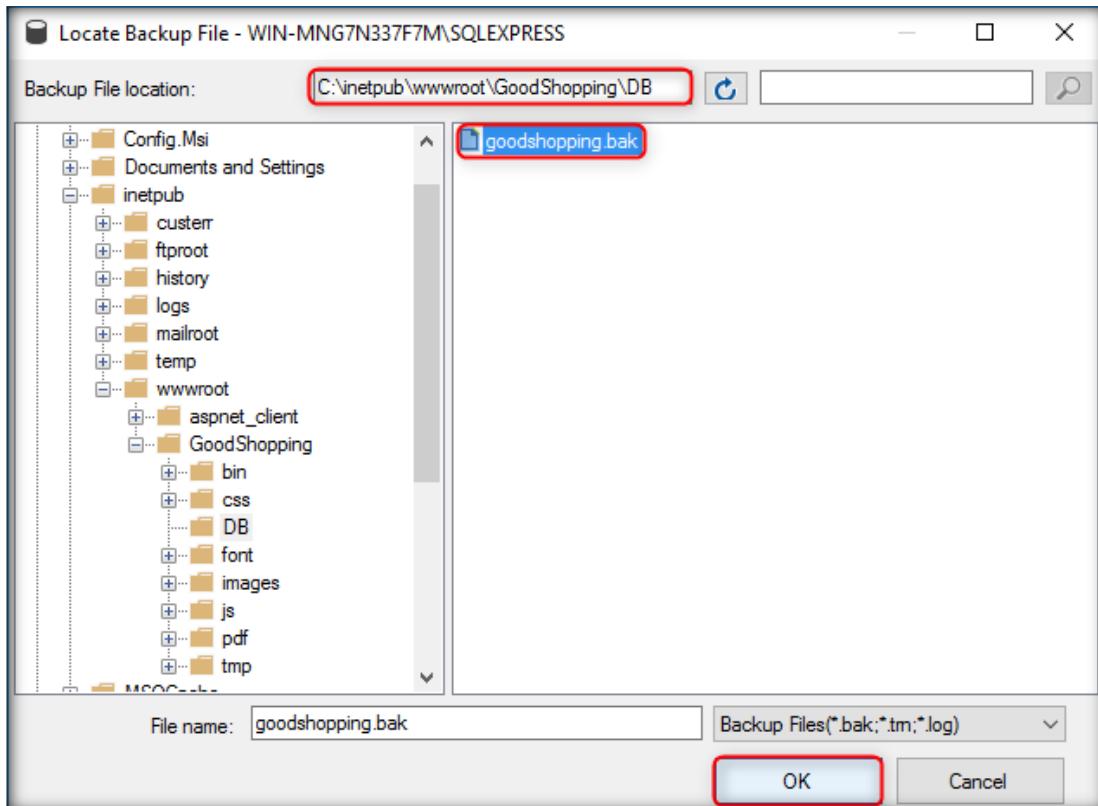
18. Click **Device** radio button under **Source** section and click  button located parallel to **Device** field



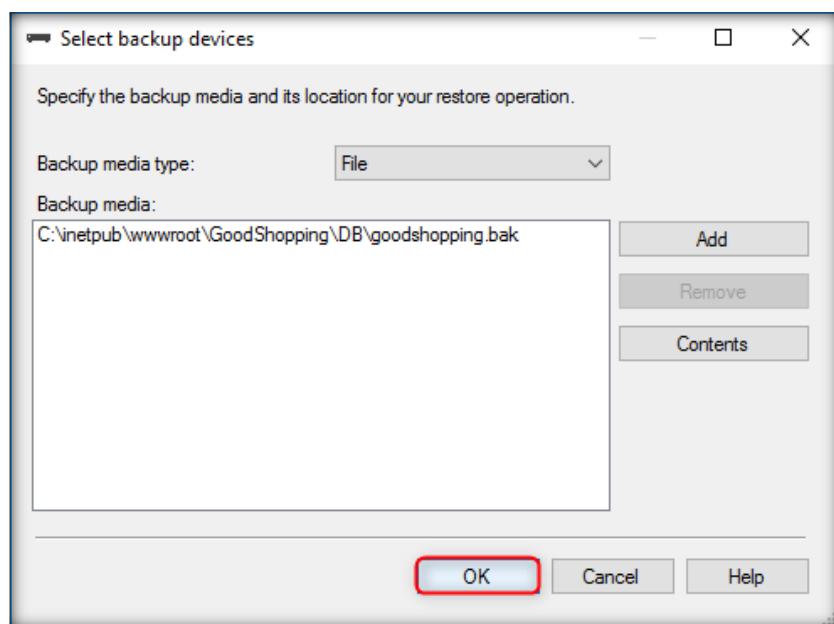
19. **Select backup devices** dialog-box appears, click **Add** button



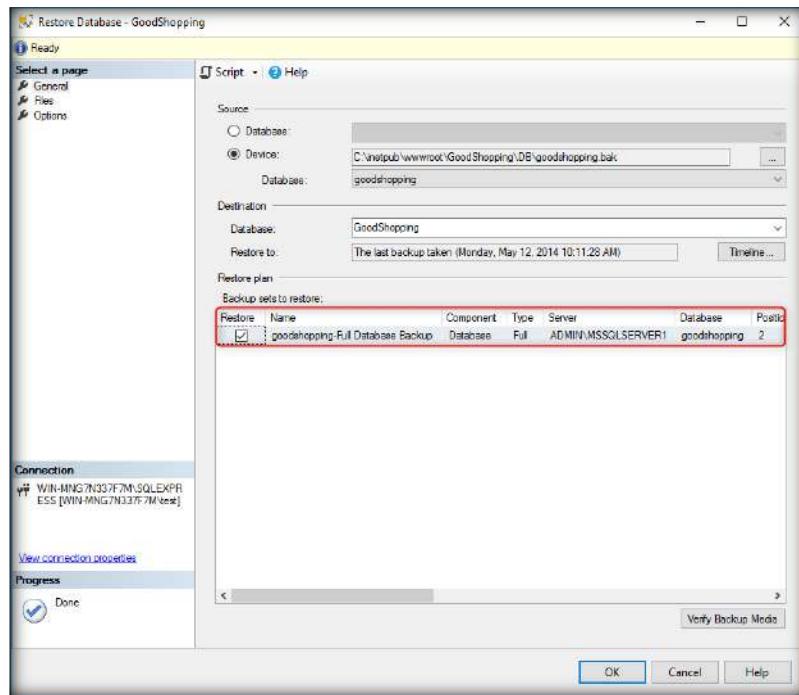
20. Navigate to the backup file (**goodshopping.bak**) located in
C:\inetpub\wwwroot\GoodShopping\DB
21. Select the backup file and then click **OK**. Locate Backup File window exits



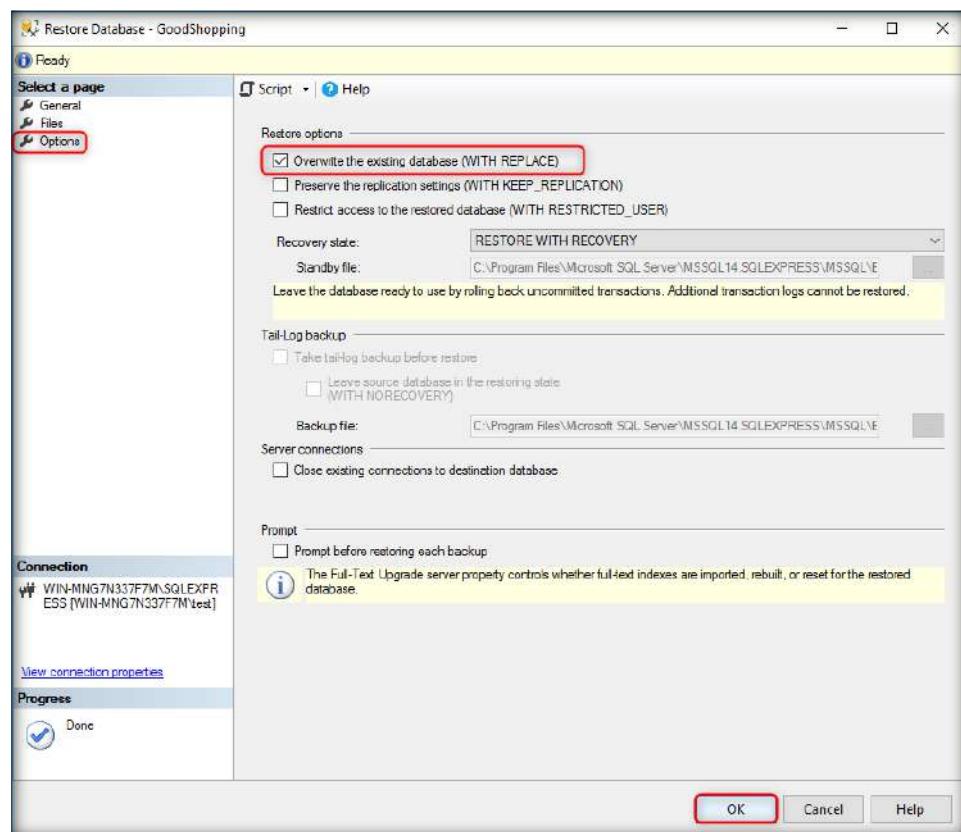
22. Under Backup media section, the location of **goodshopping.bak** website is listed
23. Click **OK**, Select backup devices window exits



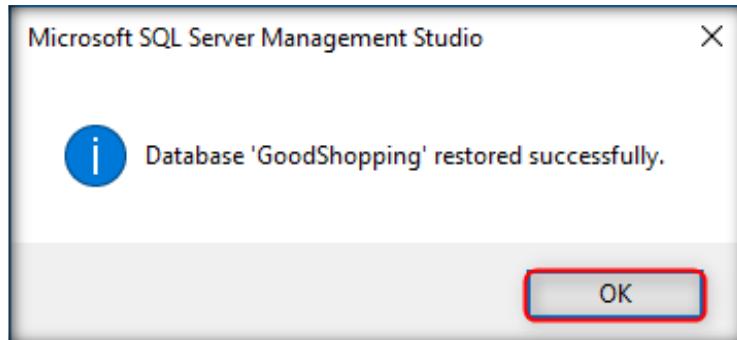
24. You will observe that the backup file has been successfully added. Ensure that the backup file is checked.



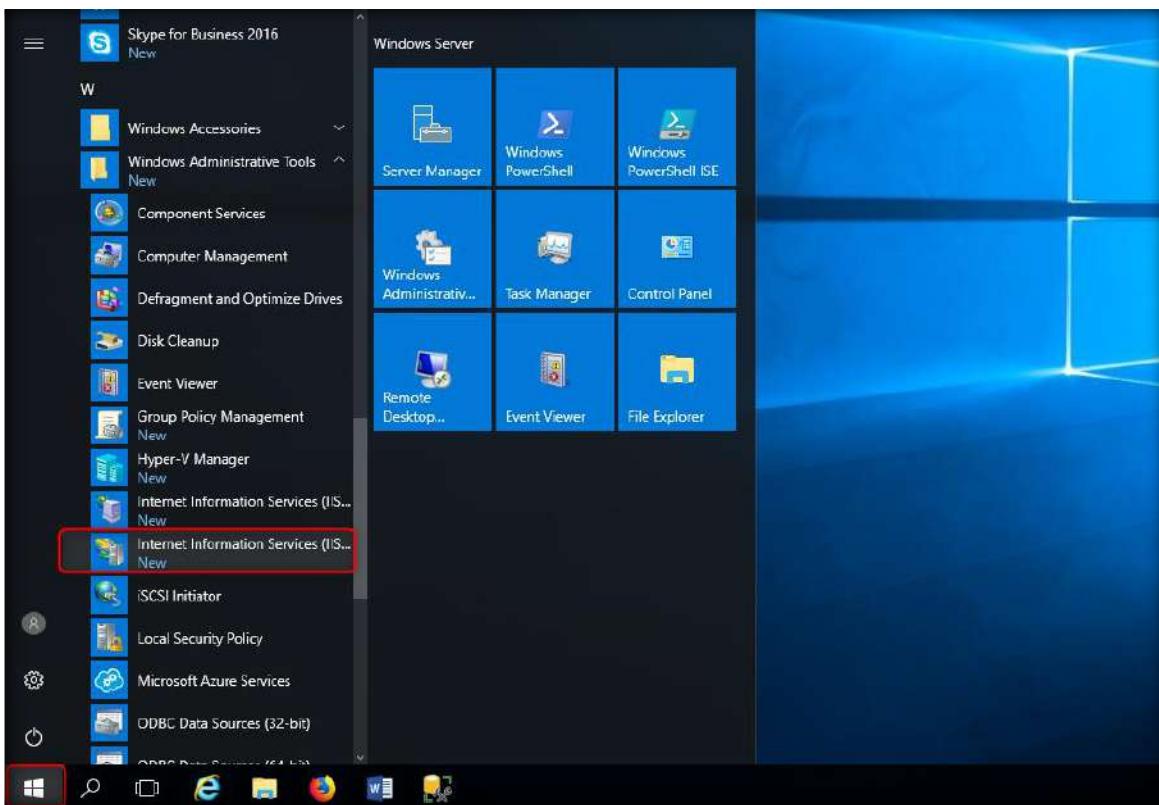
25. Click **Options** in left pane, check **Overwrite existing database (WITH REPLACE)** under **Restore options** section and the click **OK**



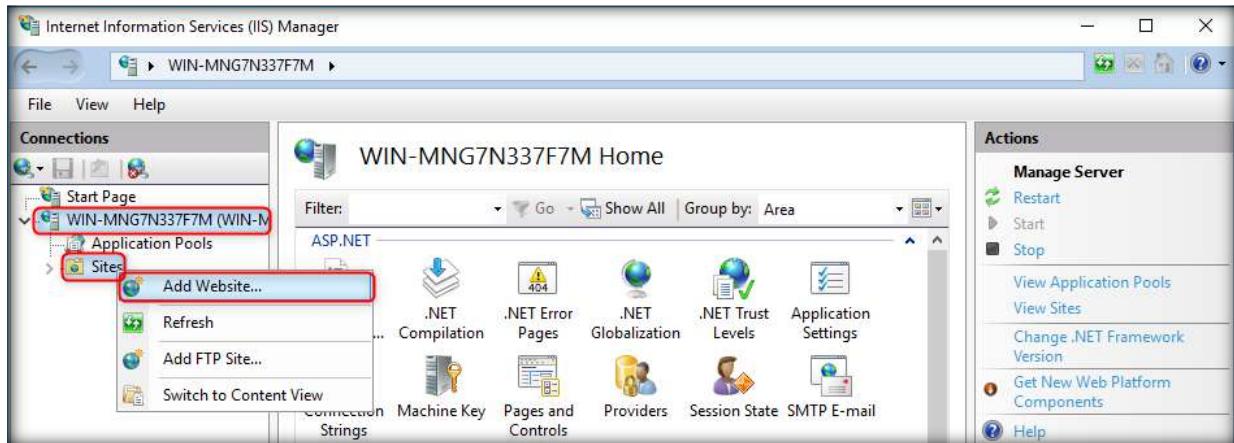
26. **Microsoft SQL Server Management Studio** pop-up appears stating that the database has been successfully created. Click **OK**



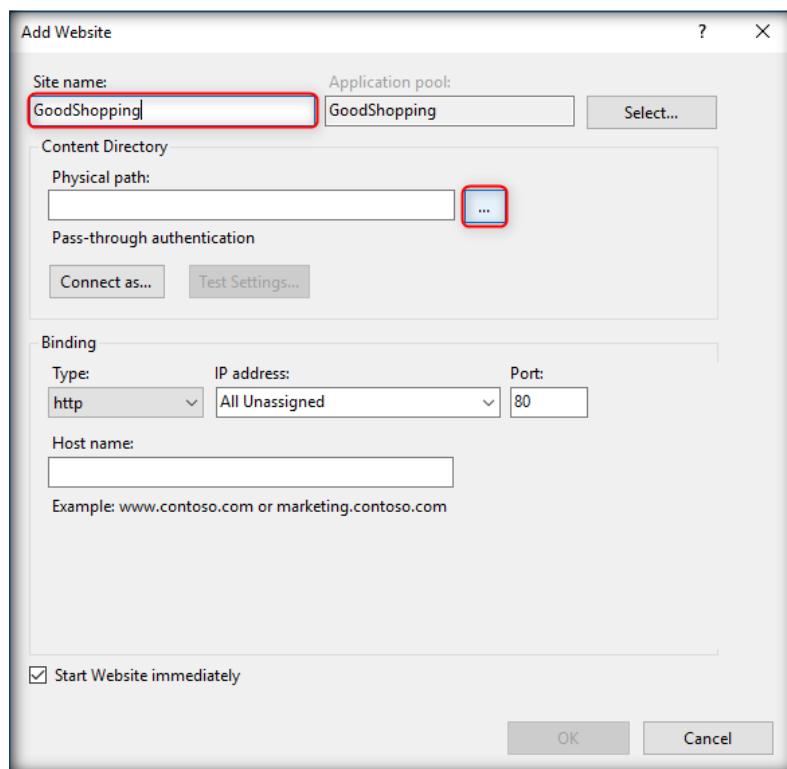
27. You have successfully **restored** the **database** of GoodShopping in your machine, GoodShopping website is now hosted in your local machine
28. Now click **Start** menu button, click **Windows Administrative Tools** → **Internet Information Services (IIS) Manager**



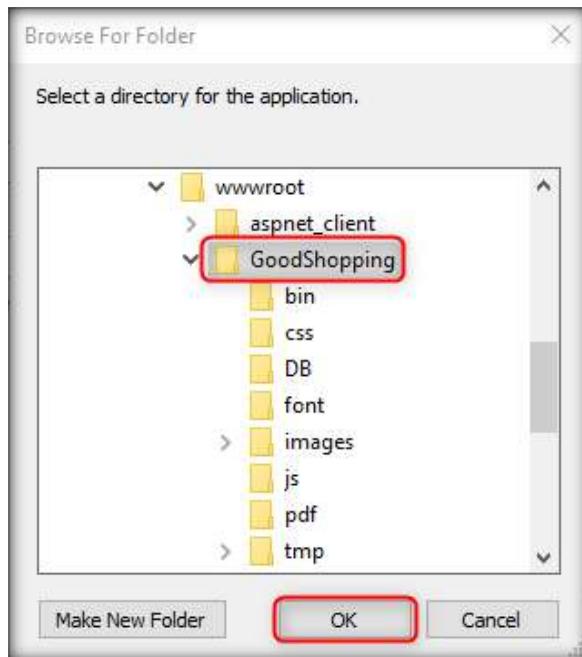
29. Internet Information Services (IIS) Manager main window appears, now in left pane of the window expand **Machine Name** and right click on **Sites** and click **Add Website...** from context menu.



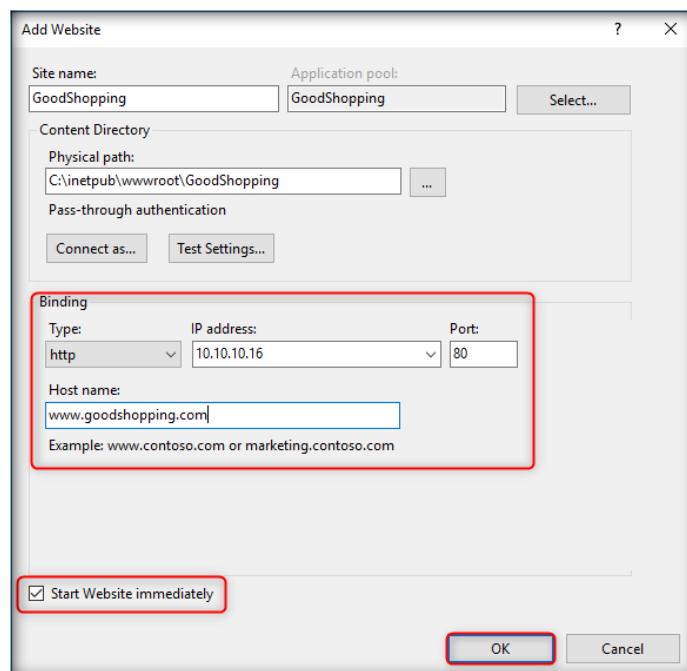
30. Add Website wizard appears, type the **Site name:** field and click on **Browse** button near **Physical path:** section
31. Here we are installing GoodShopping site, so we have provided **GoodShopping** in the Site name: field



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



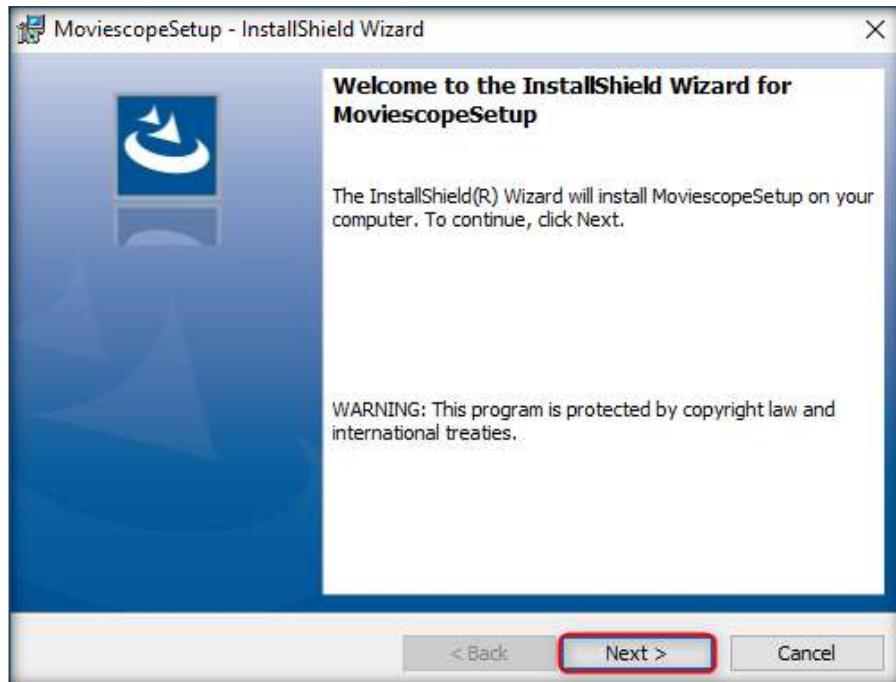
33. Now in Binding section choose **http** in Type: field. Choose the **Host machine IP address** from IP address: field, and choose **80** in Port: field.
34. Type www.goodshopping.com in Hostname: field, make sure that **Start Website immediately** is checked and click **OK**.



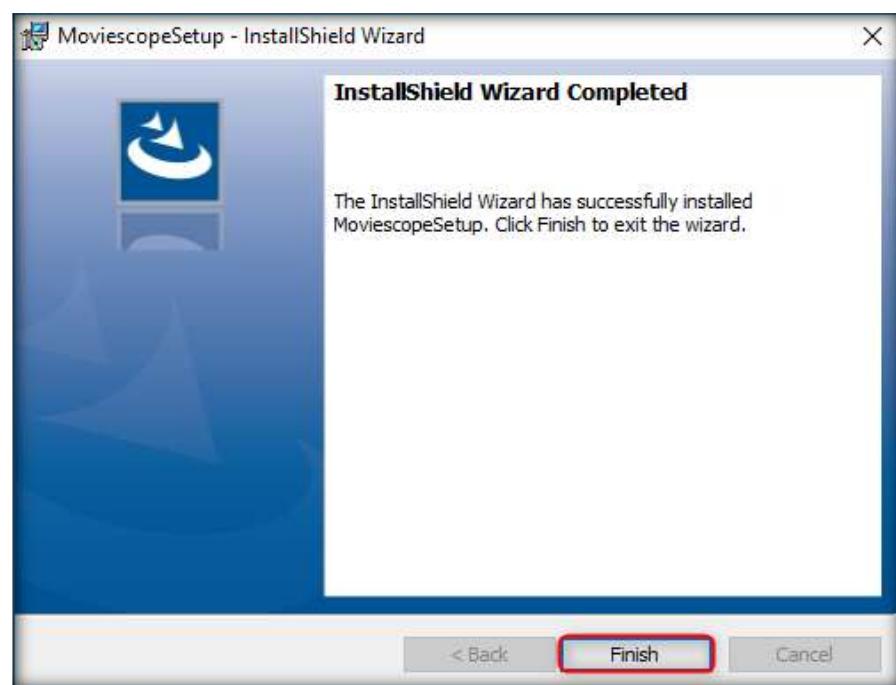
[\[Back to Configuration Task Outline\]](#)

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**



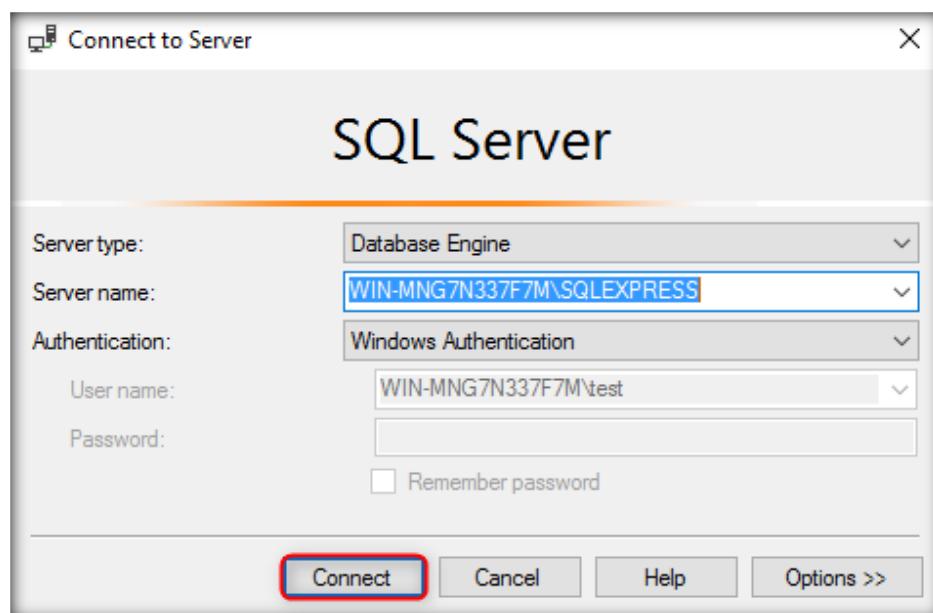
4. Open **moviescope** folder from **C:\inetpub\wwwroot\moviescope** and open **Web.config** file in notepad++ or in notepad
5. Scroll down to **connectionstring** tag in **line no. 26**, enter your machine's name in **data source=[Provide Your Host Machine Name]**, provide a user id after **User ID=sa**,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

```

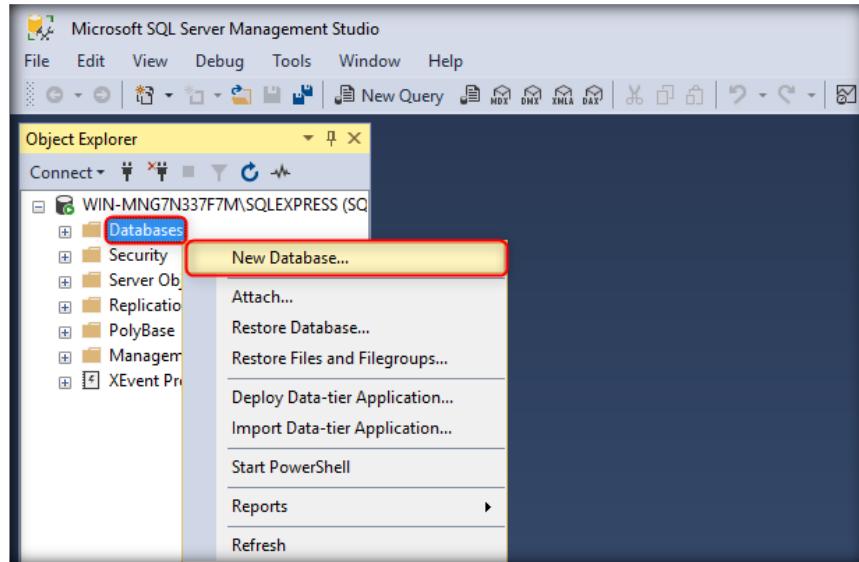
C:\inetpub\wwwroot\moviescope\Web.config - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Web.config
<?xml version="1.0" encoding="UTF-8"?>
<!--
  Note: As an alternative to hand editing this file you can use the
  web admin tool to configure settings for your application. Use
  the Website->Asp.Net Configuration option in Visual Studio.
  A full list of settings and comments can be found in
  machine.config.comments usually located in
  \Windows\Microsoft.NET\Framework\v2.0\Config
-->
<configuration>
  <configSections>
    <sectionGroup name="system.web.extensions" type="System.Web.Configuration.SystemWebExtensionsSectionGroup, System.Web.Extensions, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434493e">
      <section name="scripting" type="System.Web.Configuration.ScriptingSectionGroup, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434493e">
        <!-- <section name="scriptResourceHandler" type="System.Web.Configuration.ScriptingScriptResourceHandlerSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434493e" />
        <!-- <section name="webServices" type="System.Web.Configuration.ScriptingWebServicesSectionGroup, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434493e" />
        <!-- <section name="jsonSerialization" type="System.Web.Configuration.ScriptingJsonSerializationSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434493e" />
        <!-- <section name="profileService" type="System.Web.Configuration.ScriptingProfileServiceSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434493e" />
        <!-- <section name="authenticationService" type="System.Web.Configuration.ScriptingAuthenticationServiceSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434493e" />
        <!-- <section name="roleService" type="System.Web.Configuration.ScriptingRoleServiceSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434493e" />
      </sectionGroup>
    </sectionGroup>
  </configSections>
  <appSettings />
  <connectionStrings>
    <add name="movieConnectionString" connectionString="user id=sa;password=qwerty@123;data source=SDDW-013\SQLEXPRESS02;dat" />
  </connectionStrings>
</configuration>

```

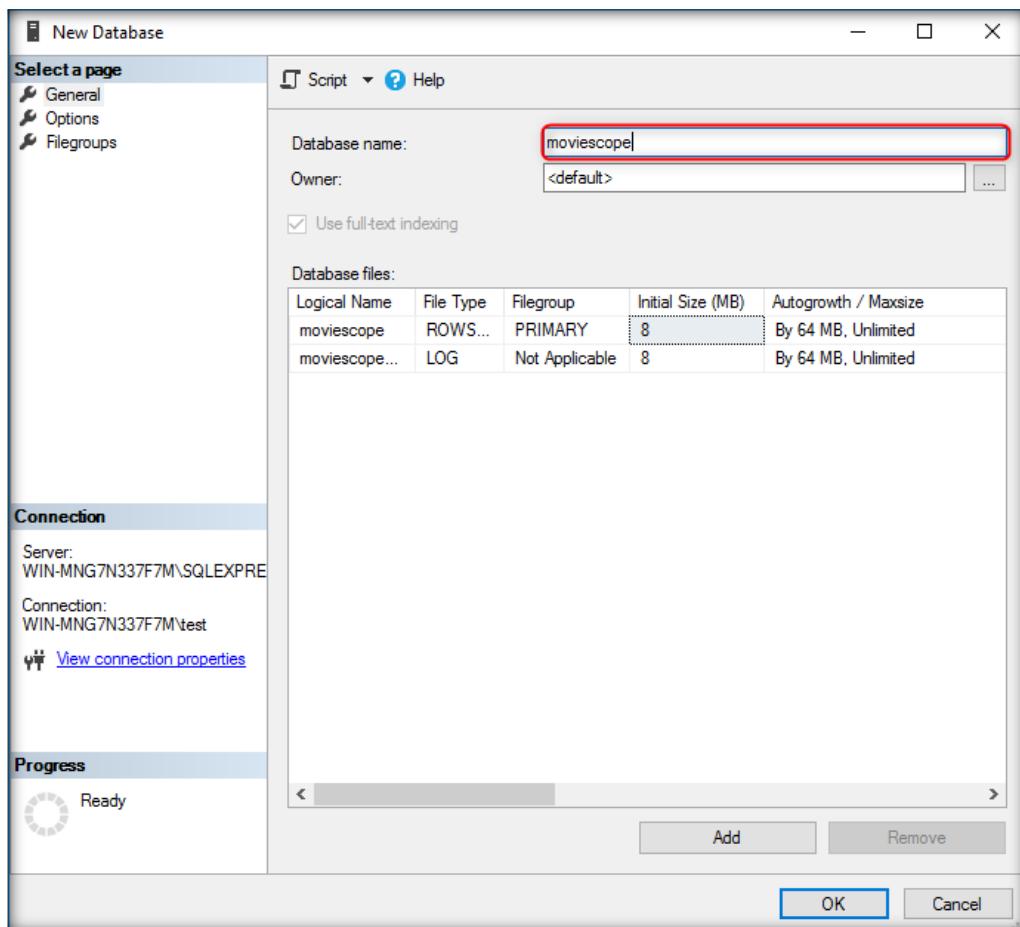
6. **Save** the file and **close** it
7. Now, **Launch** SQL Server 2017 Management Studio and click **Connect** to connect to the SQL Server



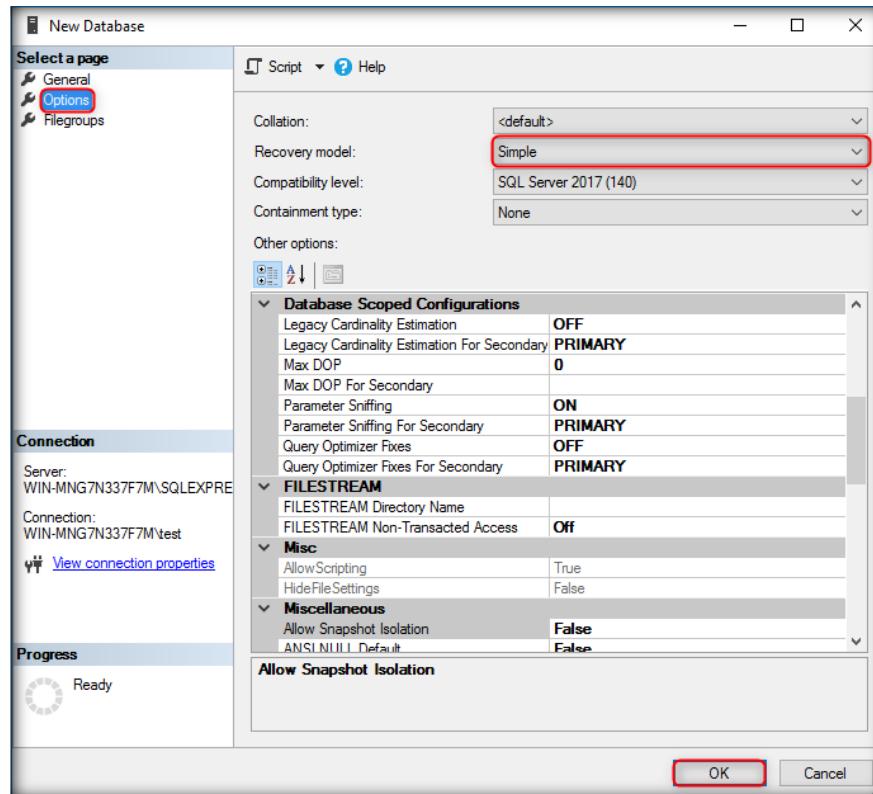
8. Microsoft SQL Server Management Studio window appears as shown in the following screenshot:
9. Right-click on **Databases** and select **New Database...**



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

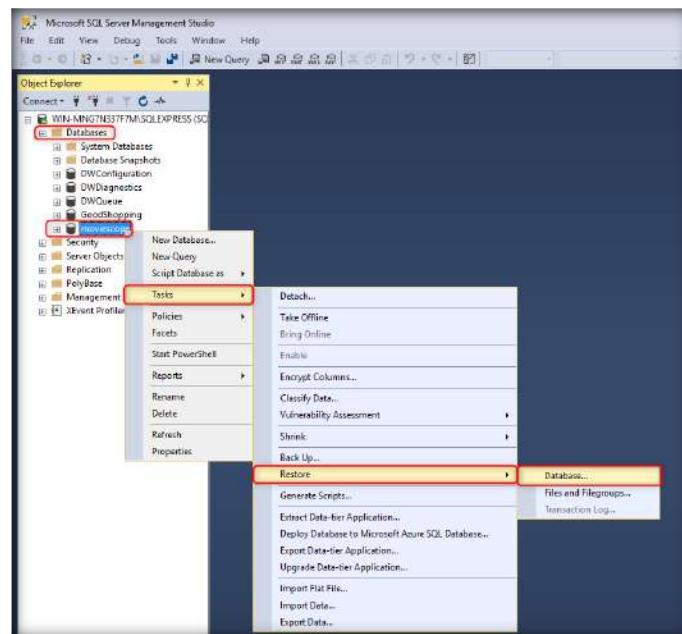


11. Select **Options** from the left pane.
12. Select **Simple** from the **Recovery model** drop-down list and click **OK**.

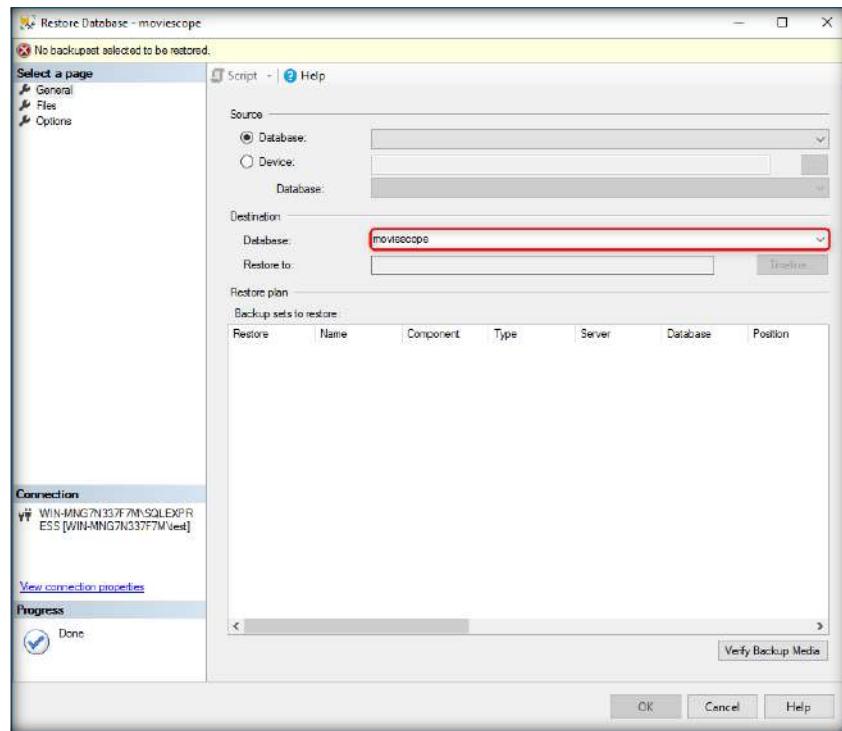


13. Now expand the **Databases** node. You will observe that **moviescope** database folder appears under the **Object Explorer** section, which implies that moviescope database has been **successfully** created.

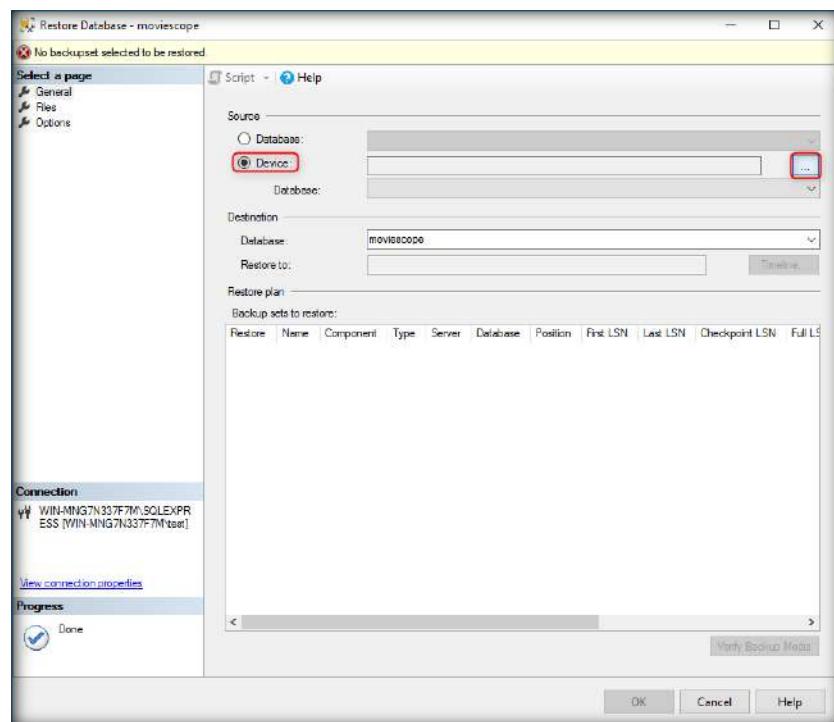
14. **Right-Click** on **moviescope** database and go to **Tasks** → **Restore** → **Database...**



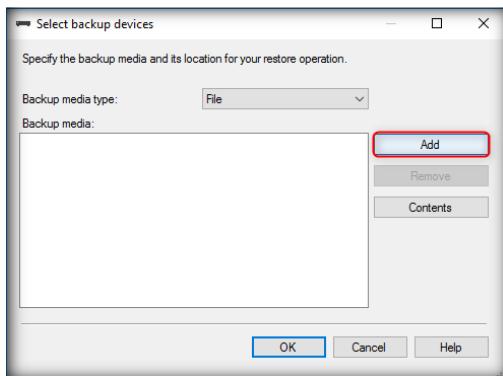
15. **Restore Database - moviescope** window appears displaying the database name (**moviescope**) in the **Database** field under **Destination** section



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

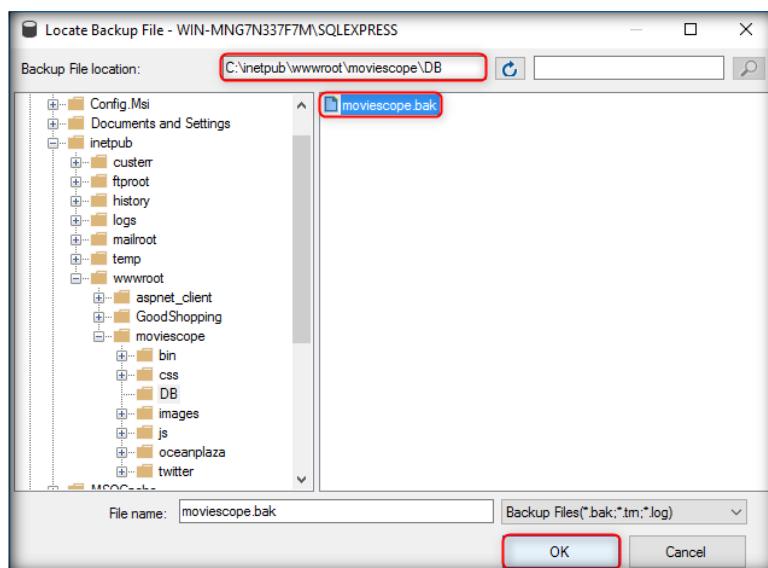


17. **Select backup devices** dialog-box appears, click **Add** button



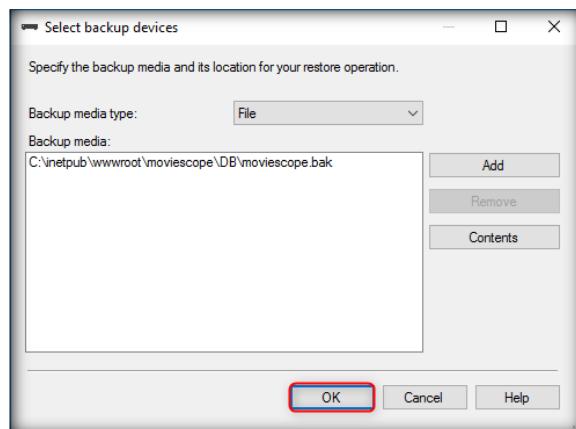
18. Navigate to the backup file (**moviescope.bak**) located in
C:\inetpub\wwwroot\moviescope\DB

19. Select the backup file and then click **OK**. Locate Backup File window exits.

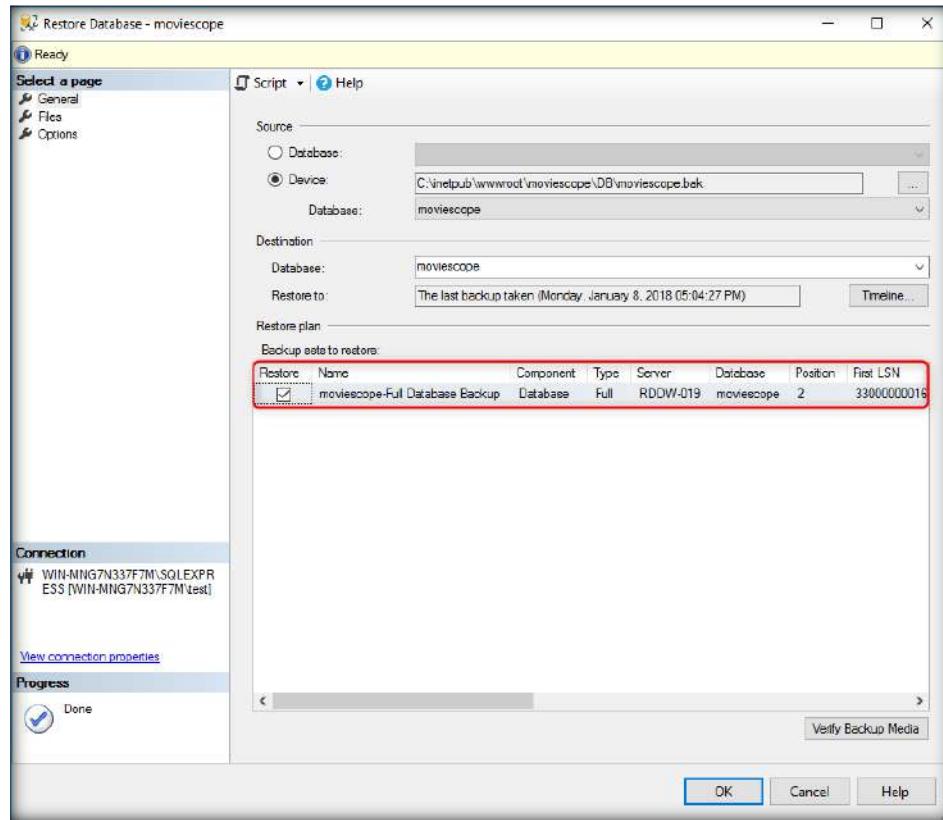


20. Under Backup media section, the location of **moviescope.bak** website is listed

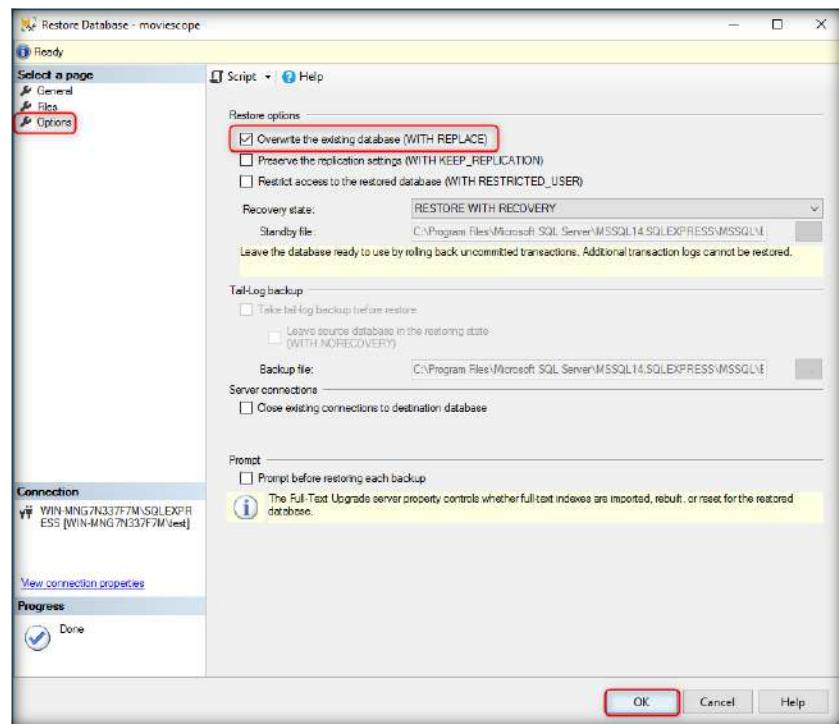
21. Click **OK**, Select backup devices window exits



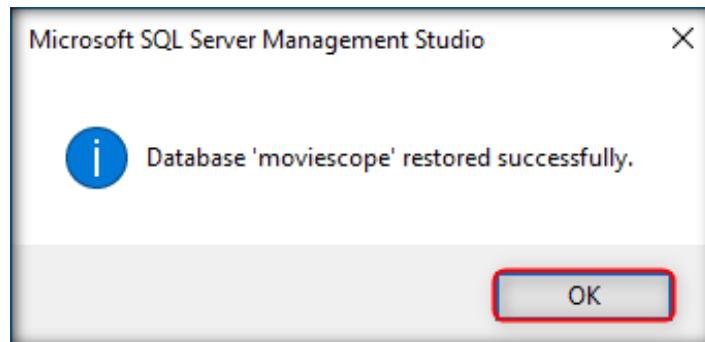
22. You will observe that the backup file has been successfully added. Ensure that the backup file is checked.



23. Click **Options** in left pane, check **Overwrite existing database (WITH REPLACE)** 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.

```

C:\Windows\System32\drivers\etc\hosts - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
hosts x
16 # 102.54.94.97 rhino.acme.com # source server
17 # 38.25.63.10 x.acme.com # x client host
18
19 # localhost name resolution is handled within DNS itself.
20 # 127.0.0.1 localhost
21 # ::1 localhost
22
23 10.10.10.16 www.goodshopping.com
24 10.10.10.16 www.moviescope.com
25 127.0.0.1 fonts.googleapis.com
26

```

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.

```

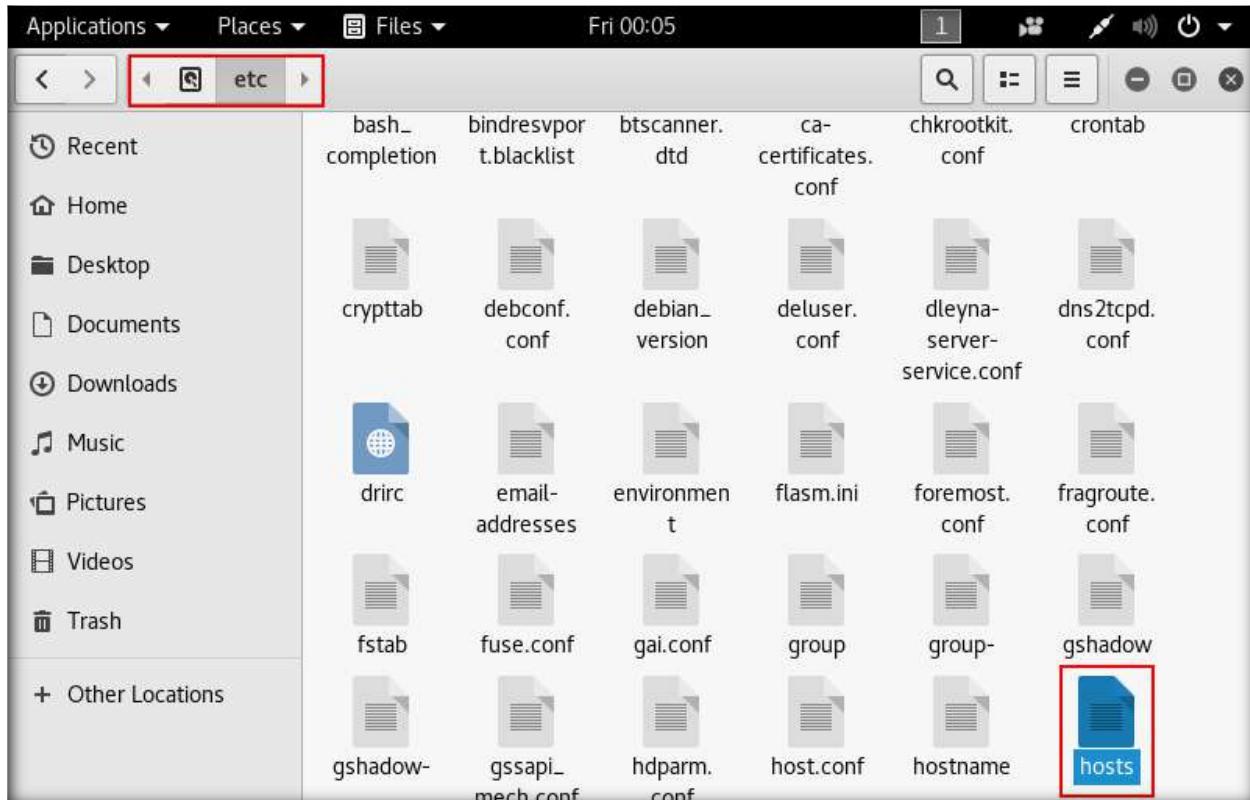
C:\Windows\System32\drivers\etc\hosts - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
hosts x
16 # 102.54.94.97 rhino.acme.com # source server
17 # 38.25.63.10 x.acme.com # x client host
18
19 # localhost name resolution is handled within DNS itself.
20 # 127.0.0.1 localhost
21 # ::1 localhost
22
23 10.10.10.16 www.goodshopping.com
24 10.10.10.16 www.moviescope.com
25 127.0.0.1 fonts.googleapis.com
26

```

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

```

Open *hosts /etc Save ×
127.0.0.1      localhost
127.0.1.1      kali

# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters

10.10.10.16 www.goodshopping.com
10.10.10.16 www.moviescope.com
127.0.0.1 fonts.googleapis.com

```

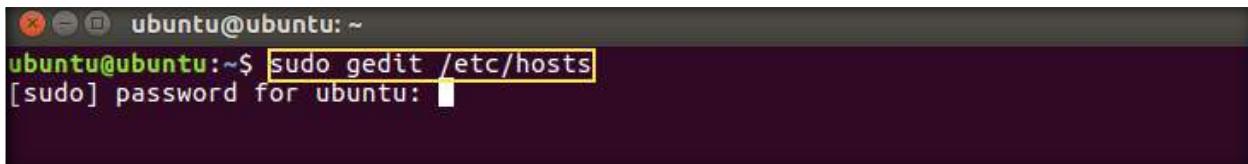
The screenshot shows a text editor window with the file name '*hosts' and the path '/etc'. The content of the file is displayed. The last three lines, which are the additions to the hosts file, are highlighted with a red box. The 'Save' button in the top right is also highlighted with a red box.

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**

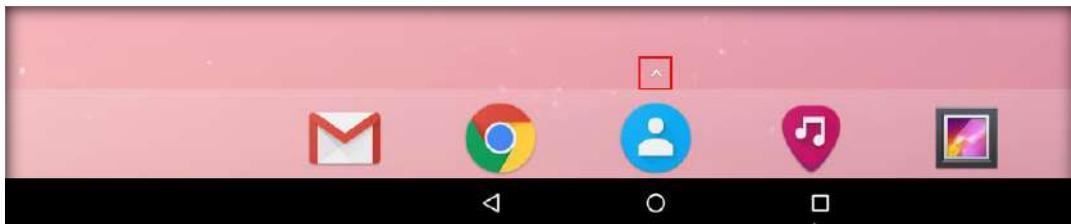


3. Hosts file opens in the text editor window, type <IP Address of the Windows Server 2016> www.goodshopping.com, <IP Address of the Windows Server 2016> www.moviescope.com, and **127.0.0.1 fonts.googleapis.com** then click **Save** button and close

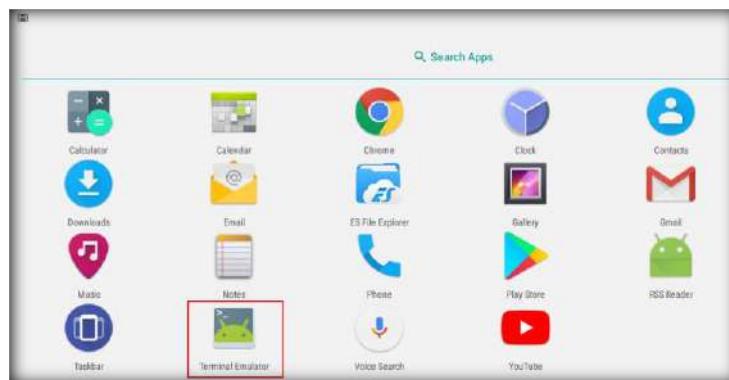


Configuring Hosts File in Android

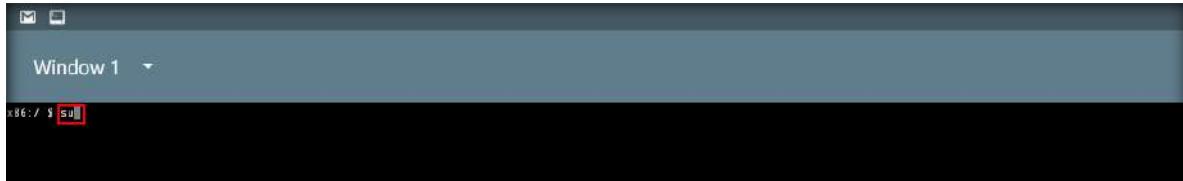
1. Launch and power on the Android virtual machine in the VMware Workstation. Click **App Drawer** (^) icon as shown in the screenshot



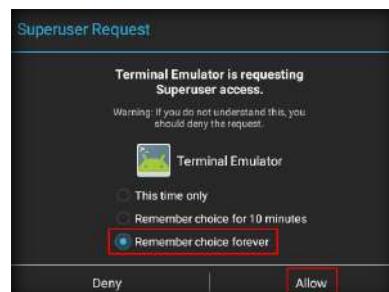
2. Click **Terminal Emulator** icon to launch terminal



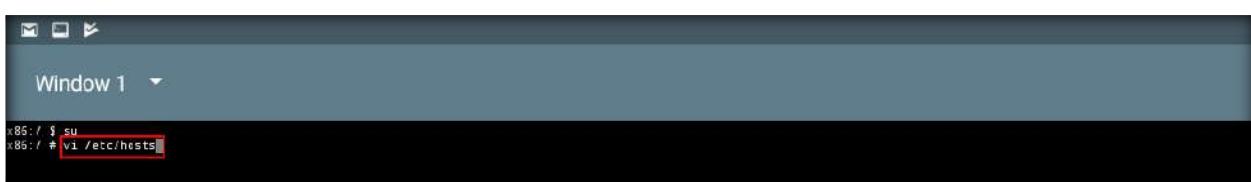
3. Type **su** and press **Enter** to gain the root access



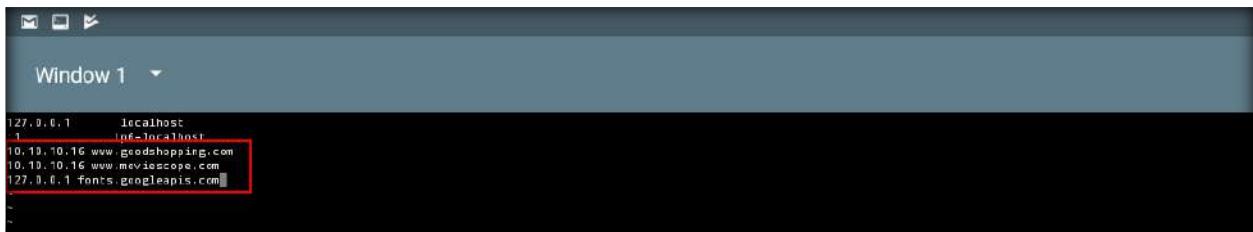
4. Superuser Request pop-up appears, choose **Remember choice forever** radio button and click **Allow**



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

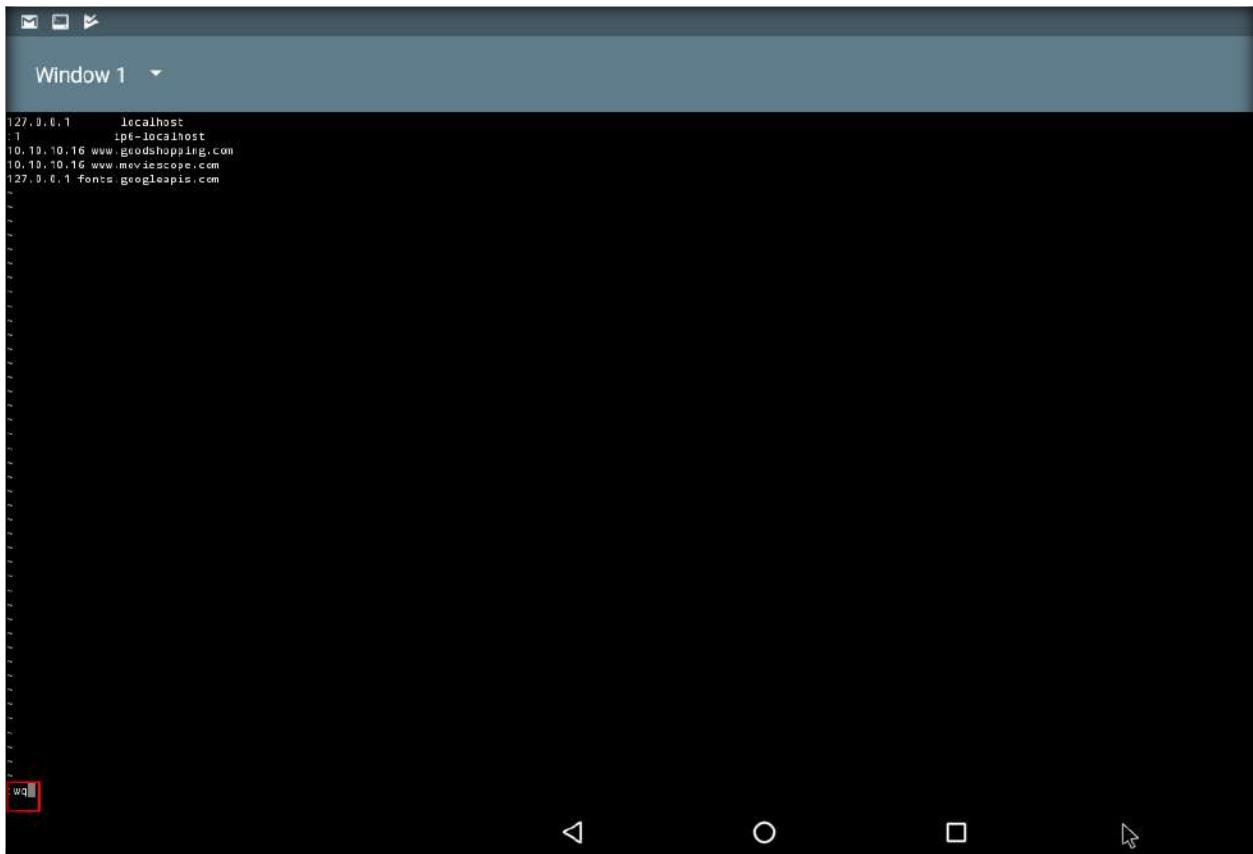


6. In the text editor window press **Shift+I** on your keyboard to allow editing. Type <IP Address of the Windows Server 2016> www.goodshopping.com, <IP Address of the Windows Server 2016> www.moviescope.com, and **127.0.0.1 fonts.googleapis.com**



```
127.0.0.1      localhost
1              ip6-localhost
10.10.10.16   www.goodshopping.com
10.10.10.16   www.moviescope.com
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



```
127.0.0.1      localhost
1              ip6-localhost
10.10.10.16   www.goodshopping.com
10.10.10.16   www.moviescope.com
127.0.0.1     fonts.googleapis.com
```

wq

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**.



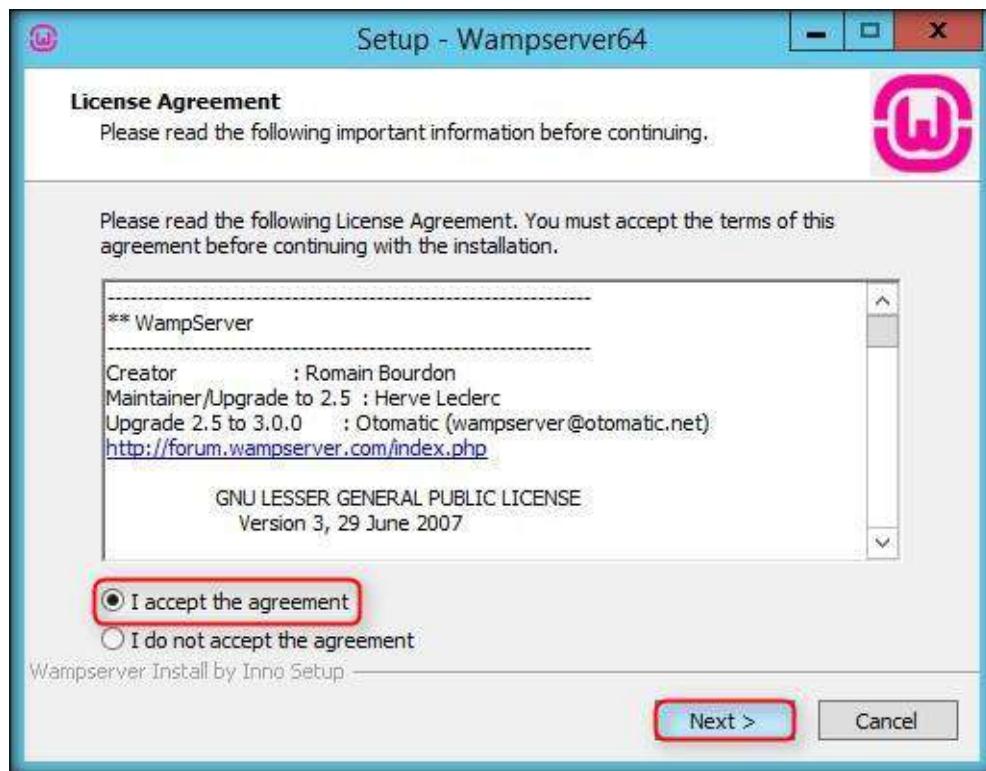
5. On completion of installation, click **Close**
6. In the same way, follow the wizard driven steps to install **Microsoft Visual C++ 2008 Redistribute**, **Microsoft Visual C++ 2010 Redistribute**, **Microsoft Visual C++ 2013 Redistribute**, **Microsoft Visual C++ 2015 Redistribute**, **Microsoft Visual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



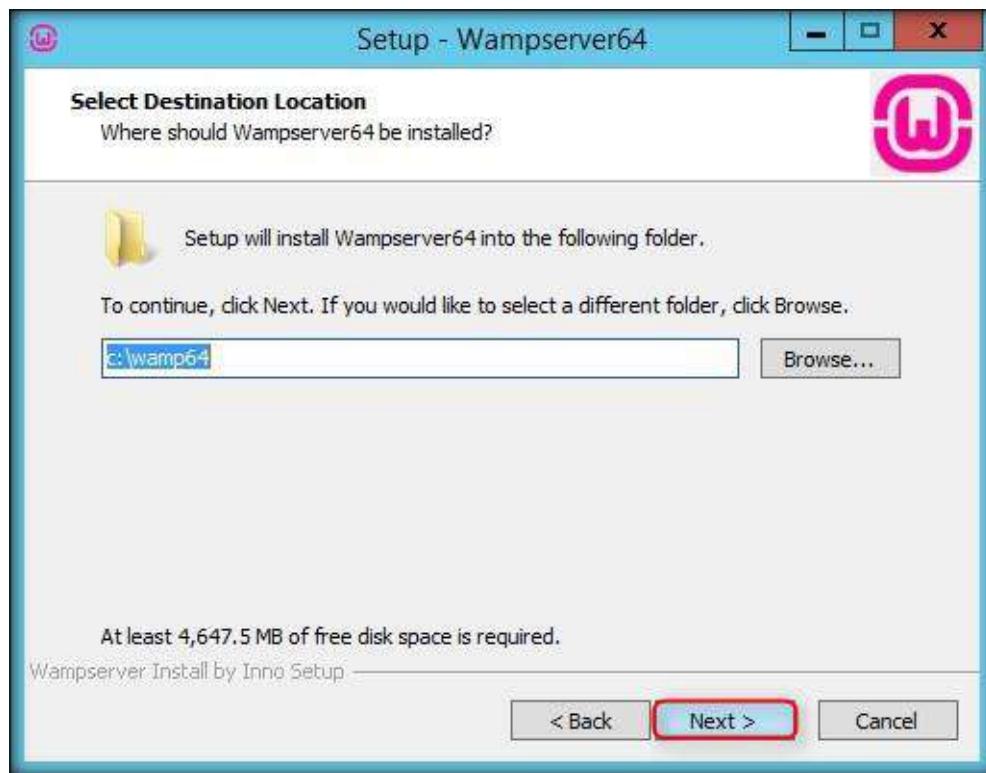
9. In the **License Agreement** section, accept the license agreement and click **Next**



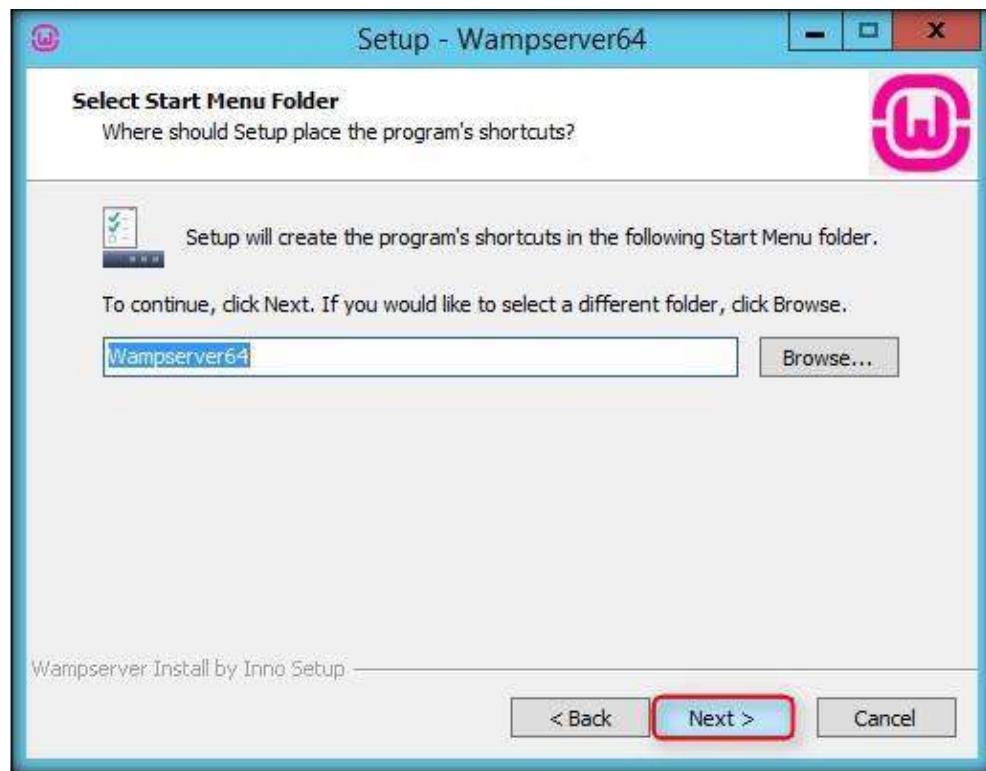
10. **Information** section appears, make sure you have the redistributable packages mentioned here and click **Next**



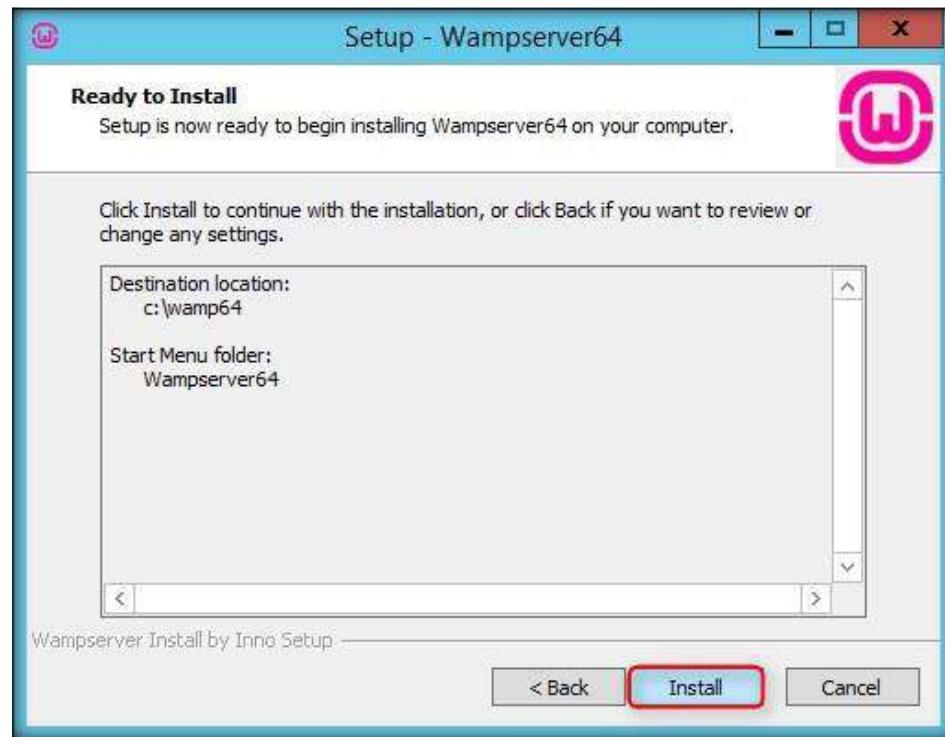
11. **Select Destination Location** section appears, specify a location where you want to install the server and click **Next**



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



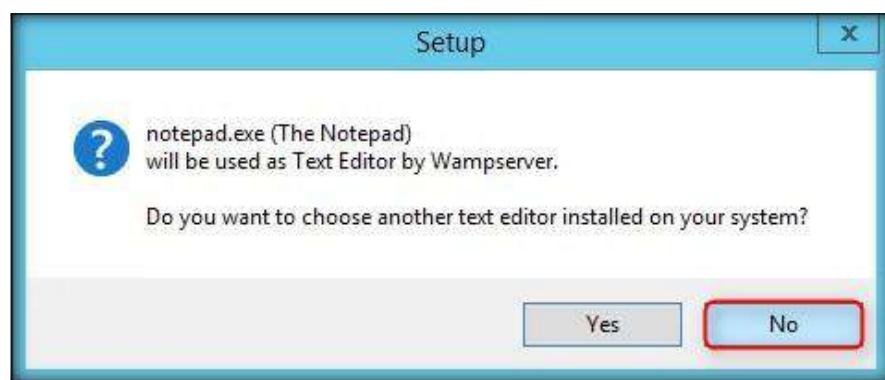
13. Ready to Install section appears, click **Install**



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



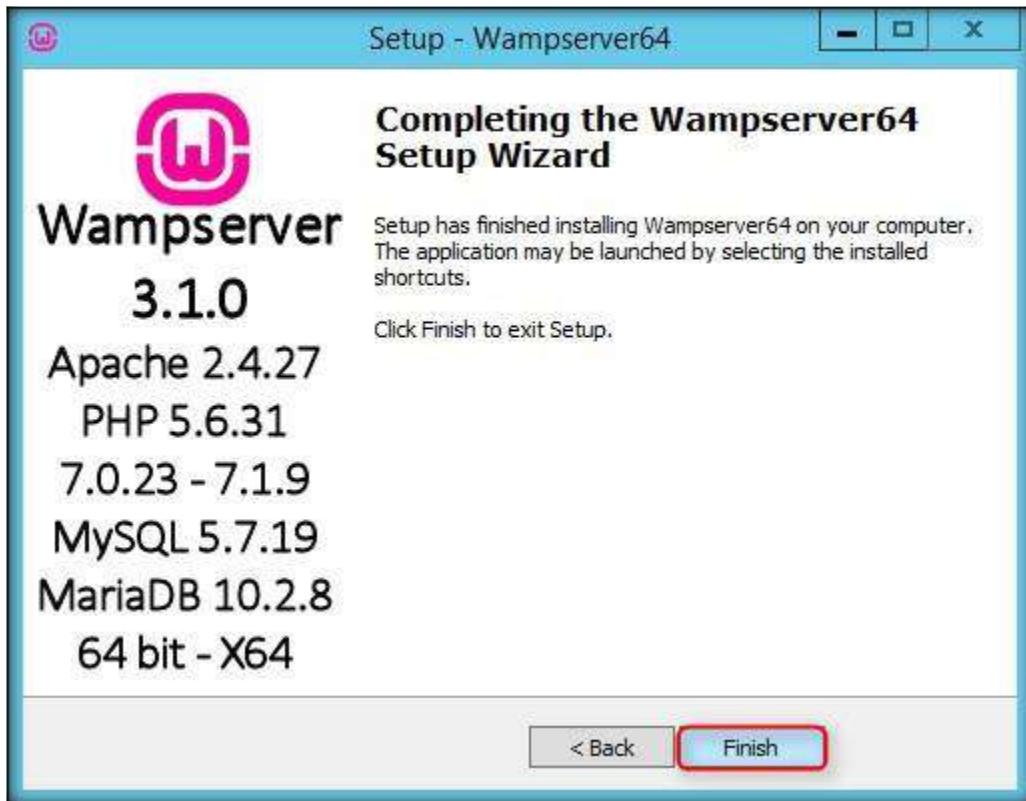
15. Another Setup pop-up appears, asking to choose the text editor to be used by Wampserver, click **No**



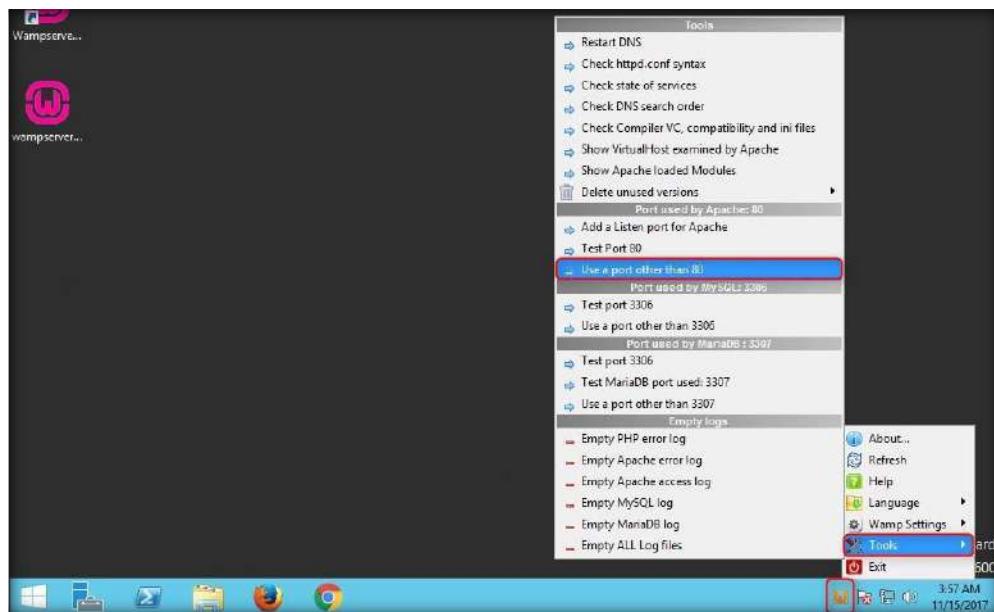
16. Information section appears, click **Next**
17. It takes some time for the server to install



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++**.

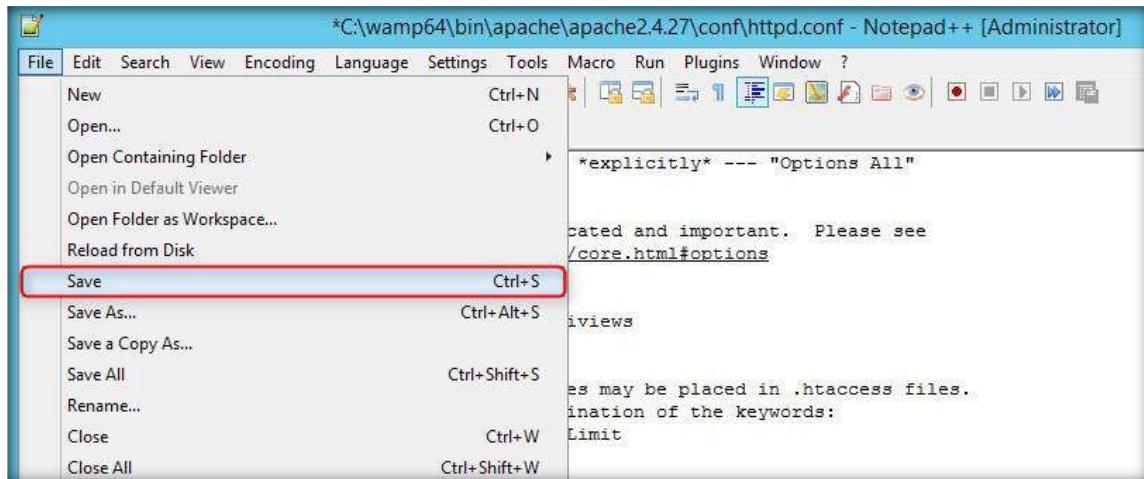
22. Scroll down to **line no. 292** and change the script from **Require local** to **Require all granted**

```
*C:\wamp64\bin\apache\apache2.4.27\conf\httpd.conf - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Httpd.conf

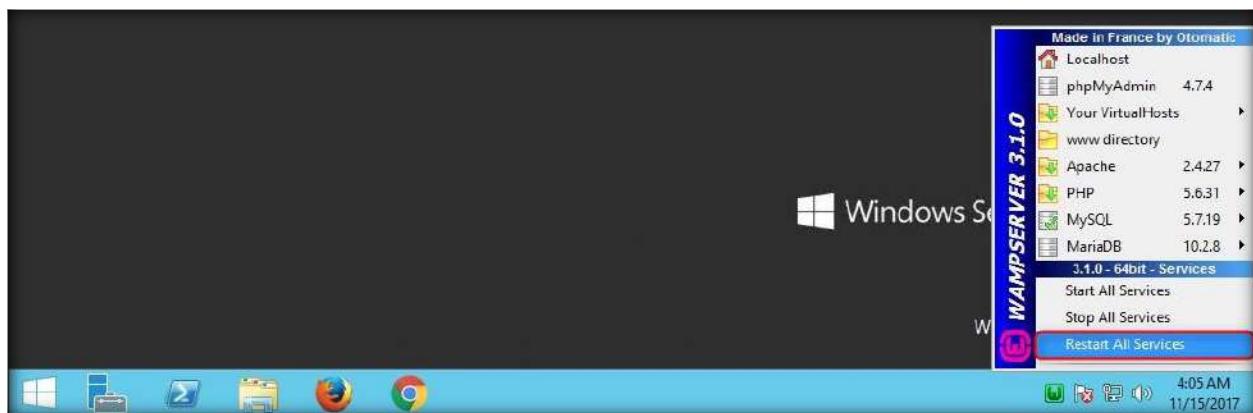
271 # Note that "MultiViews" must be named *explicitly* --- "Options All"
272 # doesn't give it to you.
273 #
274 # The Options directive is both complicated and important. Please see
275 # http://httpd.apache.org/docs/2.4/mod/core.html#options
276 # for more information.
277 #
278 Options +Indexes +FollowSymLinks +Multiviews
279 #
280 # AllowOverride controls what directives may be placed in .htaccess files.
281 # It can be "All", "None", or any combination of the keywords:
282 # AllowOverride FileInfo AuthConfig Limit
283 #
284 AllowOverride all
285 #
286 #
287 # Controls who can get stuff from this server.
288 #
289 #
290 #
291 # onlineoffline tag - don't remove
292 Require all granted
293 </Directory>
294
```

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**

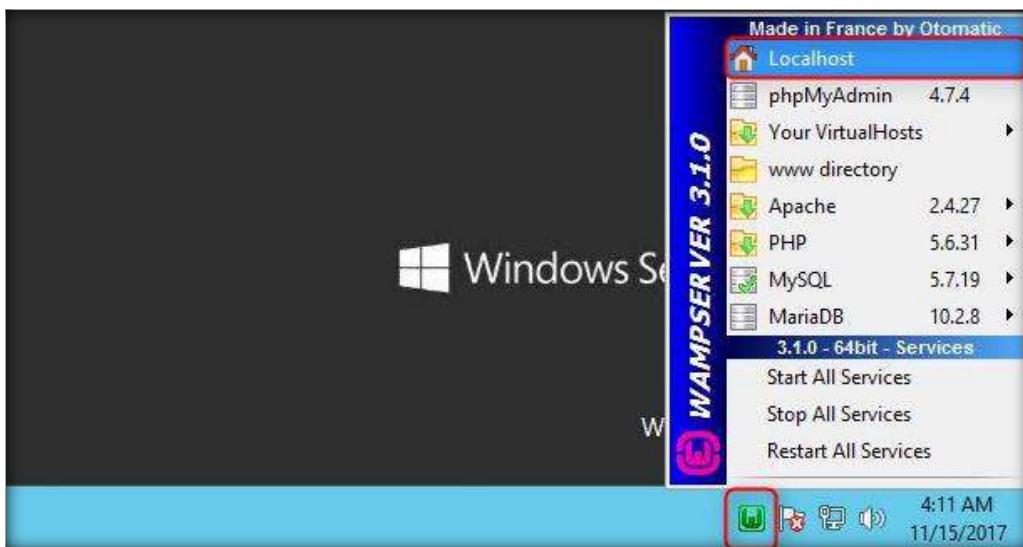


25. Wait until the icon turns green

[\[Back to Configuration Task Outline\]](#)

CT#32: Install and Configure WordPress Website

- Click the **WampServer** icon in the notification area and select **localhost**



- 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

Server Software: Apache/2.4.27 (Win64) PHP/5.6.31 - Port defined for Apache: 8080

Loaded Extensions :

apache2handler	bcmath	bz2
calendar	com_dotnet	Core
ctype	curl	date
dom	ereg	exif
fileinfo	filter	ftp
gd	gettext	gmp
hash	iconv	imap
intl	json	ldap
libxml	mbstring	mcrypt
mhash	mysql	mysqli
mysqlnd	odbc	openssl
pcre	PDO	pdo_mysql
pdo_sqlite	Phar	Reflection
session	SimpleXML	soap
sockets	SPL	sqlite3
standard	tokenizer	wddx
xdebug	xml	xmlreader
xmlrpc	xmlwriter	xsl
Zend OPcache	zip	zlib

MySQL Version: 5.7.19 - Port defined for MySQL: 3306 - [Documentation](#)

MariaDB Version: 10.2.8 - Port defined for MariaDB: 3307 - [Documentation](#)

Tools

- [phpinfo\(\)](#)
- [**phpmyadmin**](#)
- [Add a Virtual Host](#)

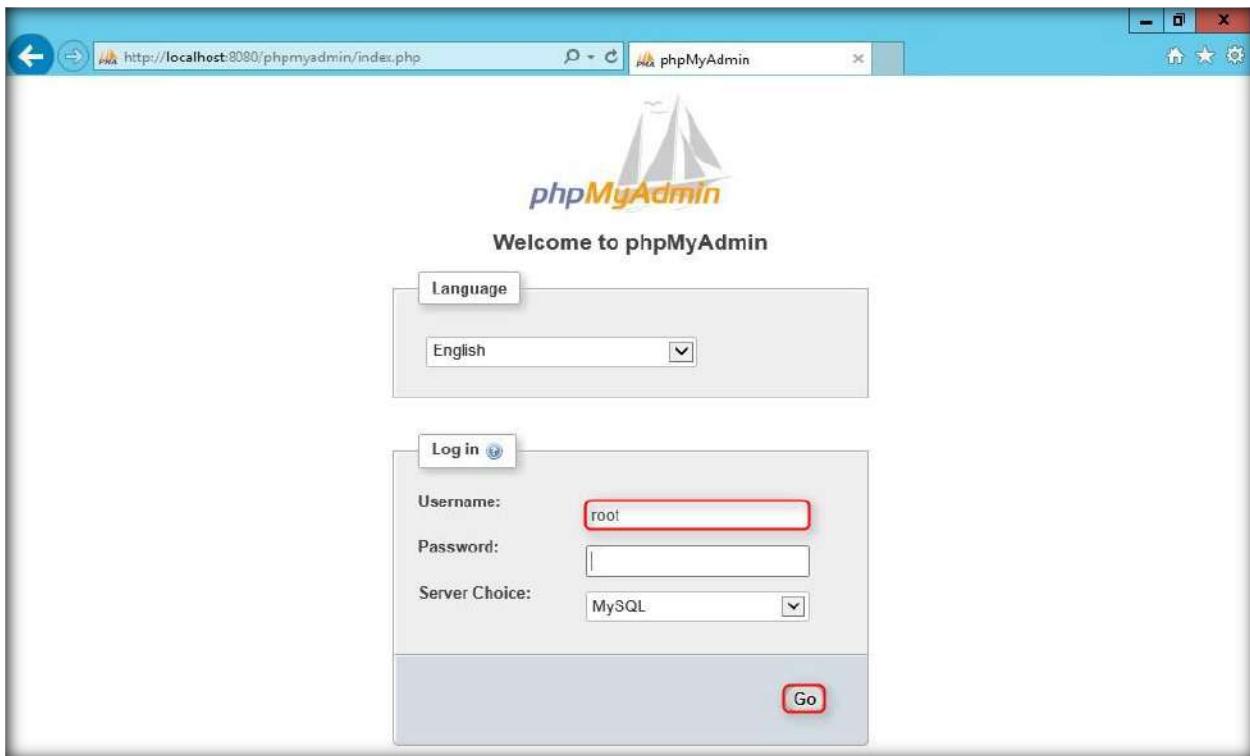
Your Projects

- [CEH](#)

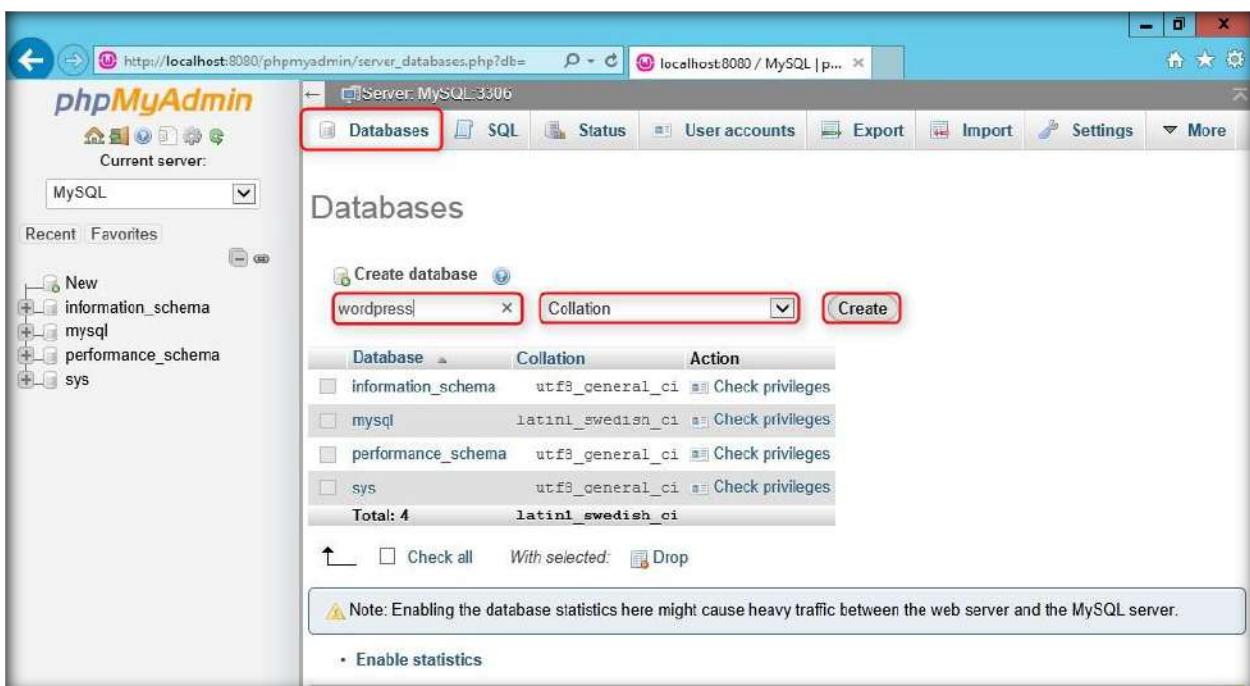
Your Aliases

- [adminer](#)
- [phpmyadmin](#)
- [phpsysinfo](#)

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

The screenshot shows the 'Databases' section of phpMyAdmin. In the center, there is a message box with a green checkmark and the text 'Database wordpress has been created.' Below this message, a list of databases is shown: information_schema, mysql, performance_schema, sys, and the newly created wordpress database. The 'Create database' button is visible above the list. At the bottom, there is a note about enabling statistics and a link to enable it.

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

The screenshot shows the 'General settings' and 'Database server' panes. The 'wordpress' database is selected in the left sidebar, highlighted with a red box. The 'Database server' pane displays various MySQL server details.

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

The screenshot shows the 'Operations' tab selected in the top navigation bar. In the dropdown menu on the right, the 'Privileges' option is highlighted with a red box. The main area shows a message 'No tables found in database.' and a 'Create table' form.

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

The screenshot shows the phpMyAdmin interface for managing users in a MySQL database named 'wordpress'. The main table lists a single user entry: 'root' with 'localhost' as the host and 'ALL PRIVILEGES' granted. Below the table are buttons for 'Check all', 'With selected', 'Export', and 'Edit privileges'. At the bottom left, there is a 'New' button and a prominent red-bordered 'Add user account' button.

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

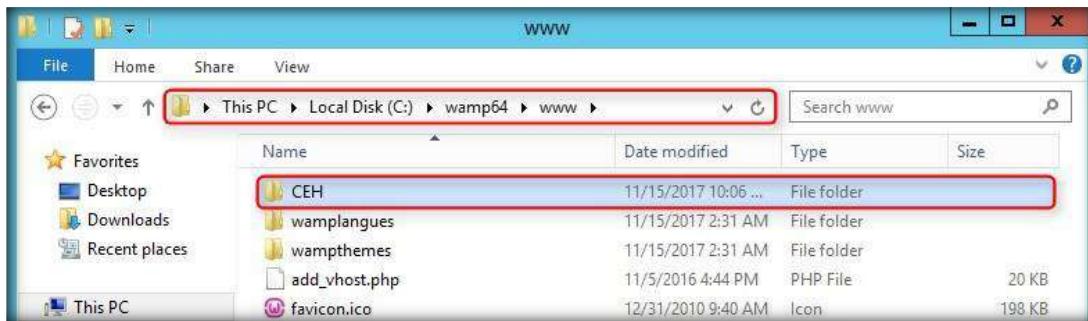
This screenshot shows the 'User accounts' tab in phpMyAdmin with the 'Login Information' section active. The 'User name' is set to 'admin', 'Host name' is 'Local', and both 'Password' and 'Re-type' fields contain masked text. In the 'Global privileges' section, the 'Check all' checkbox is checked. Other options like 'Create database with same name and grant all privileges' and 'Grant all privileges on wildcard name (username_%)' are unchecked.

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

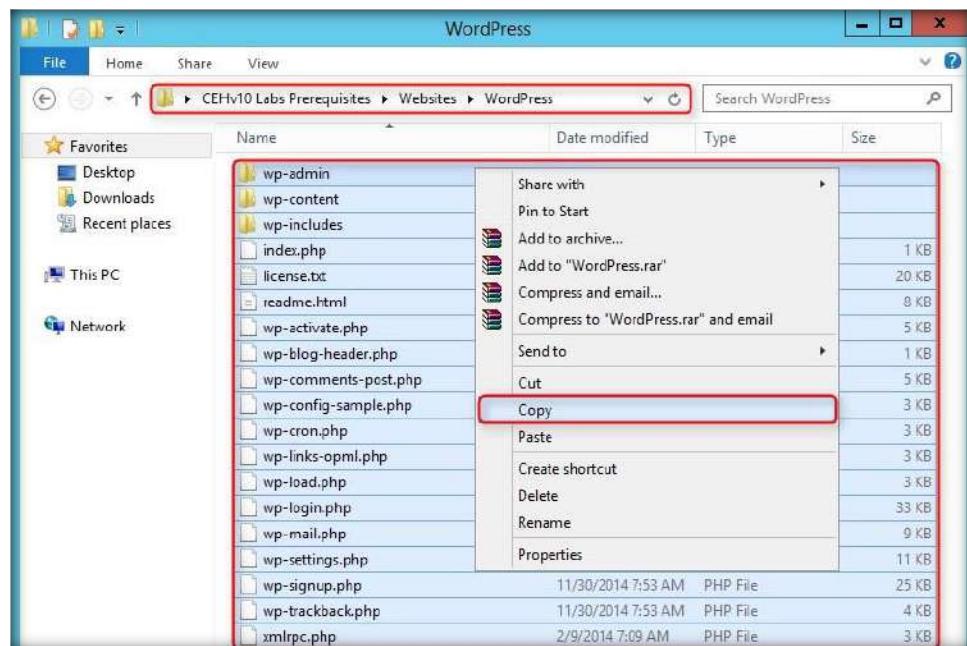


13. Close the Web browser

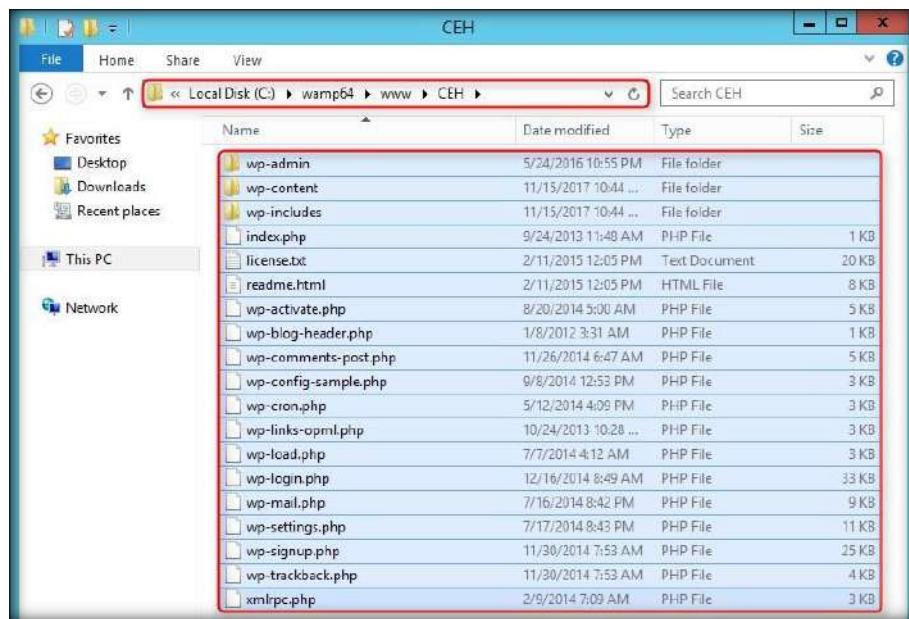
14. Navigate to **C:\wamp64\www** and create a new folder named **CEH**



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



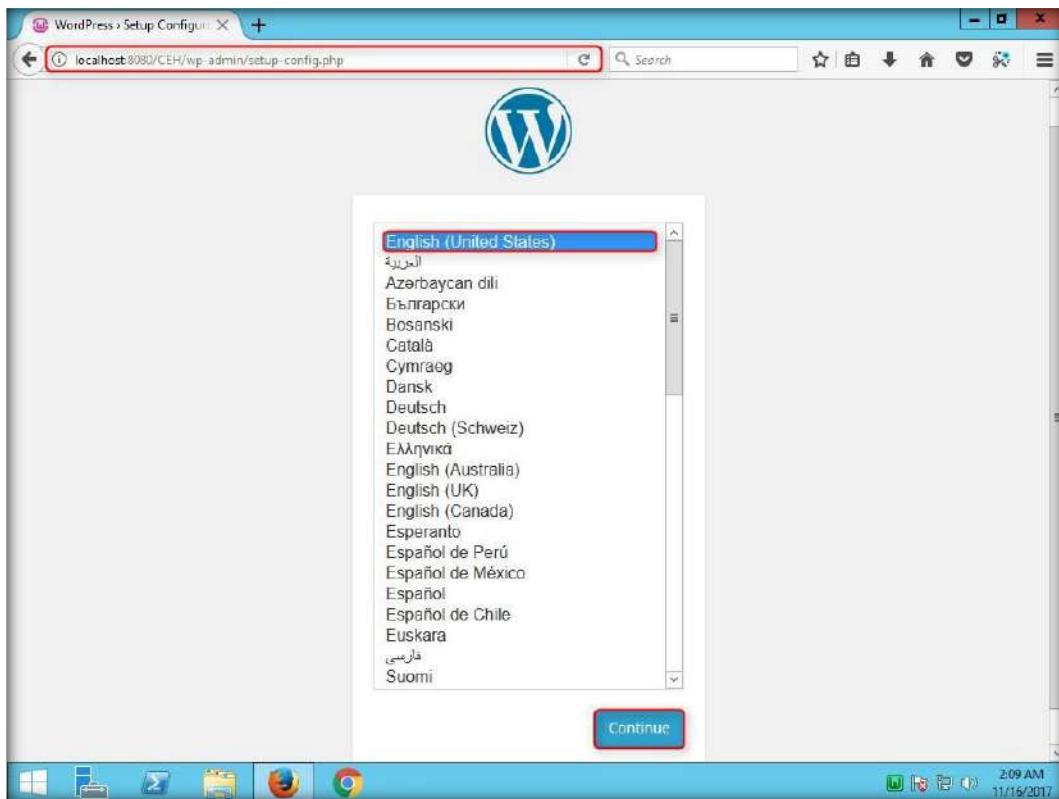
16. Navigate to **C:\wamp64\www\CEH** and paste all the contents that were copied from **Z:\CEH-Tools\CEHv10 Lab Prerequisites\Websites\WordPress**



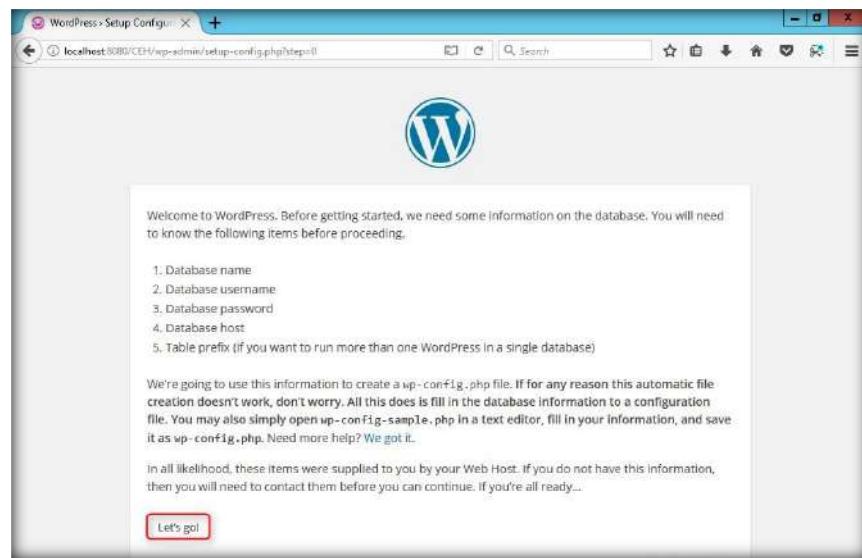
17. Launch a web browser, type the URL **http://localhost:8080/CEH** and press **Enter**

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

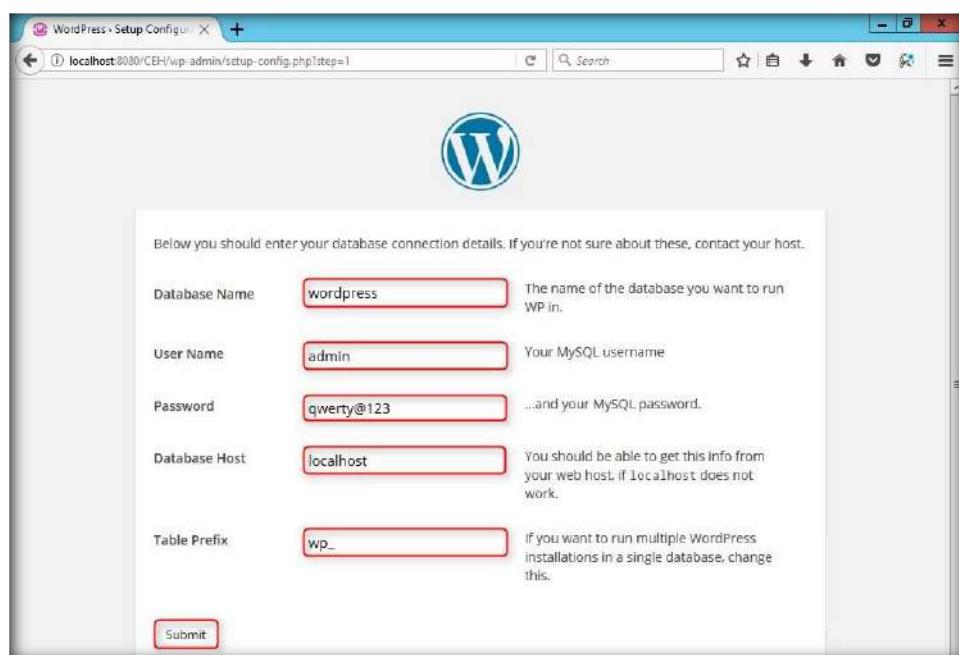
admin in **User Name** field

qwerty@123 in **Password** field

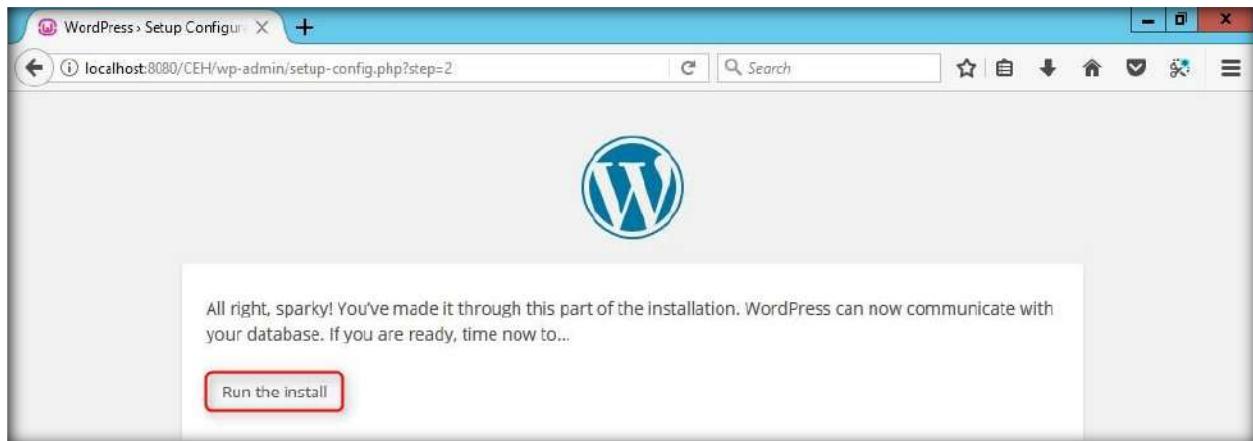
localhost in **Database Host** field

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

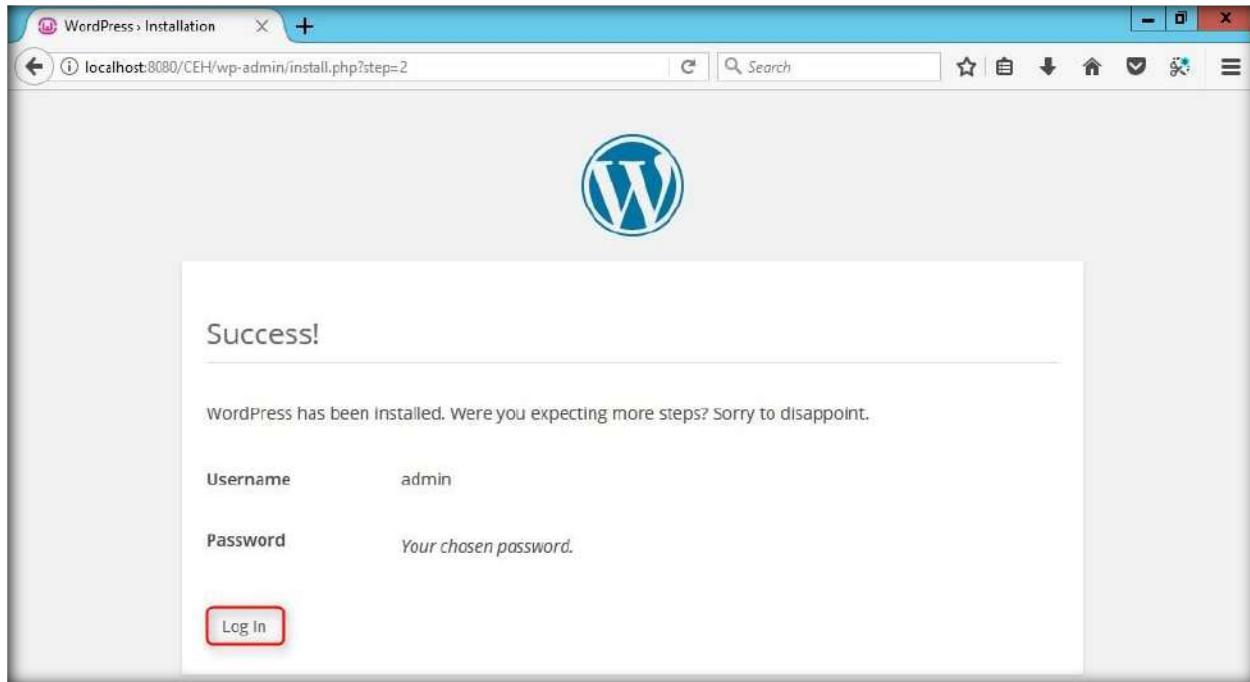
25. Click **Install WordPress** button

A screenshot of a web browser window titled "WordPress : Installation". The URL in the address bar is "localhost:8080/CEH/wp-admin/install.php?language=en". The page has a heading "Welcome to the famous five-minute WordPress installation process! Just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world." Below this is a section titled "Information needed" with the sub-instruction "Please provide the following information. Don't worry, you can always change these settings later.". The form contains the following fields:

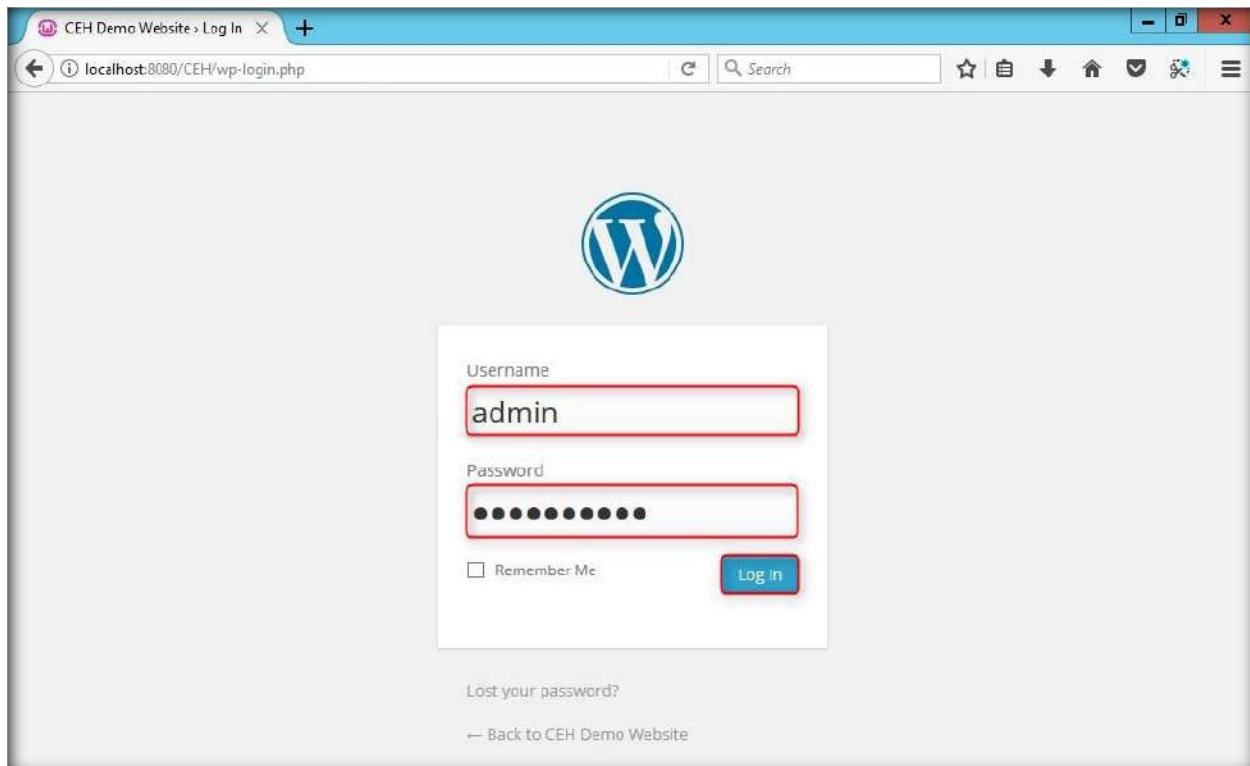
- Site Title:** CEH Demo Website
- Username:** admin
- Password:** qwerty@123 (status: Very weak)
- Confirm Password:** Confirm use of weak password
- Your Email:** rini@gmail.com
- Search Engine Visibility:** Discourage search engines from indexing this site

At the bottom of the form is a red-bordered "Install WordPress" button.

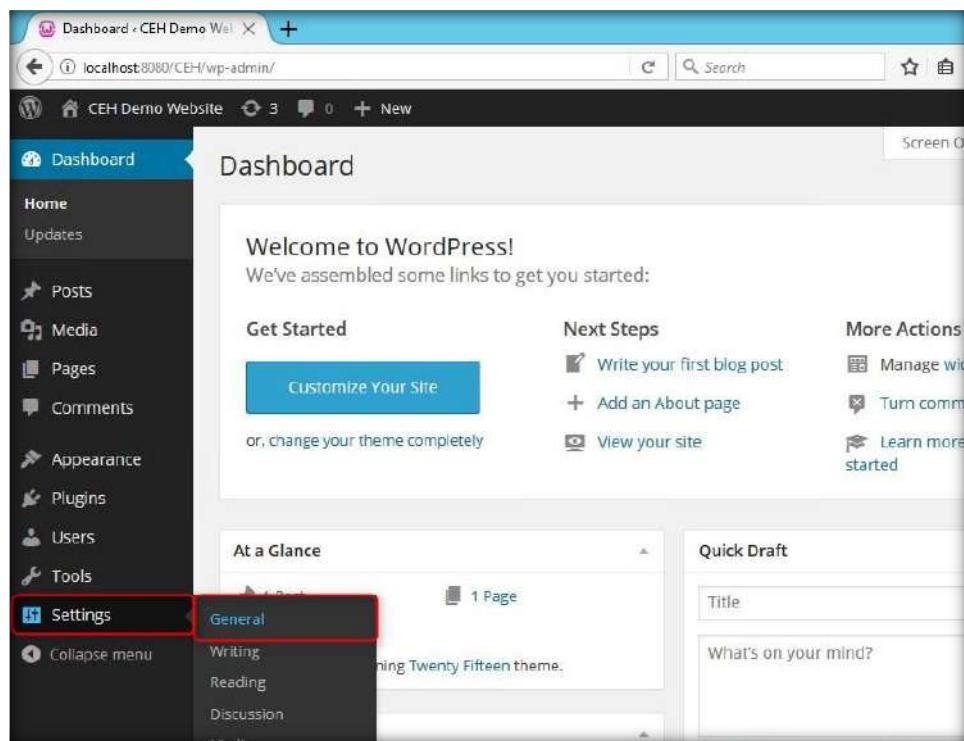
26. On successful installation, a webpage appears stating that the installation is successful. Click **Log in** button



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

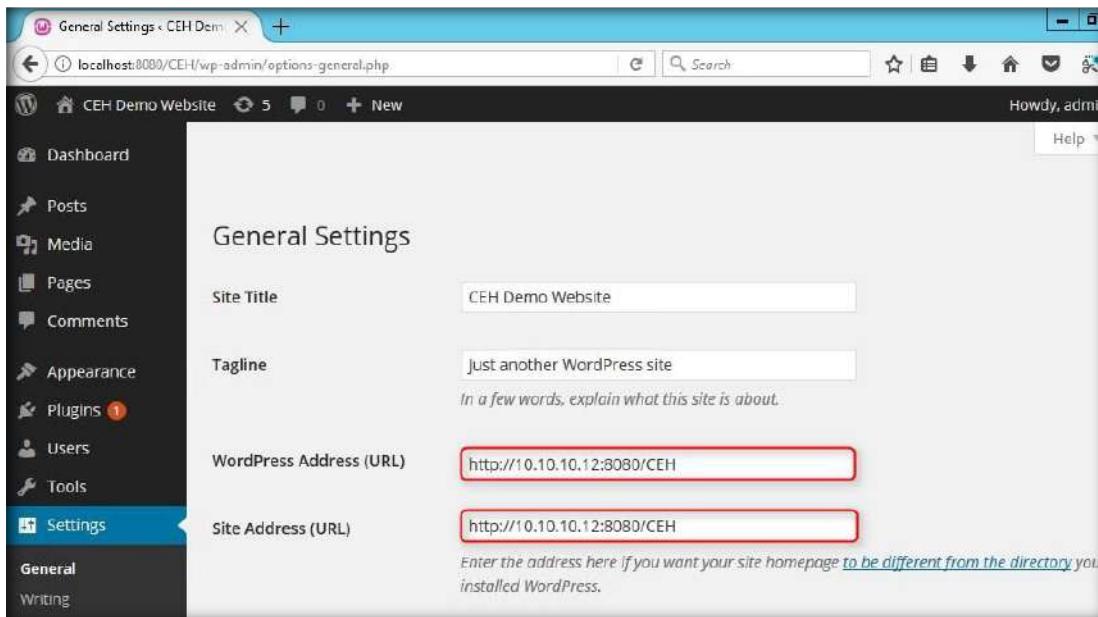


28. Once you have logged in to the website, **WordPress Dashboard** appears
 29. Hover the mouse cursor on **Settings** and click **General**

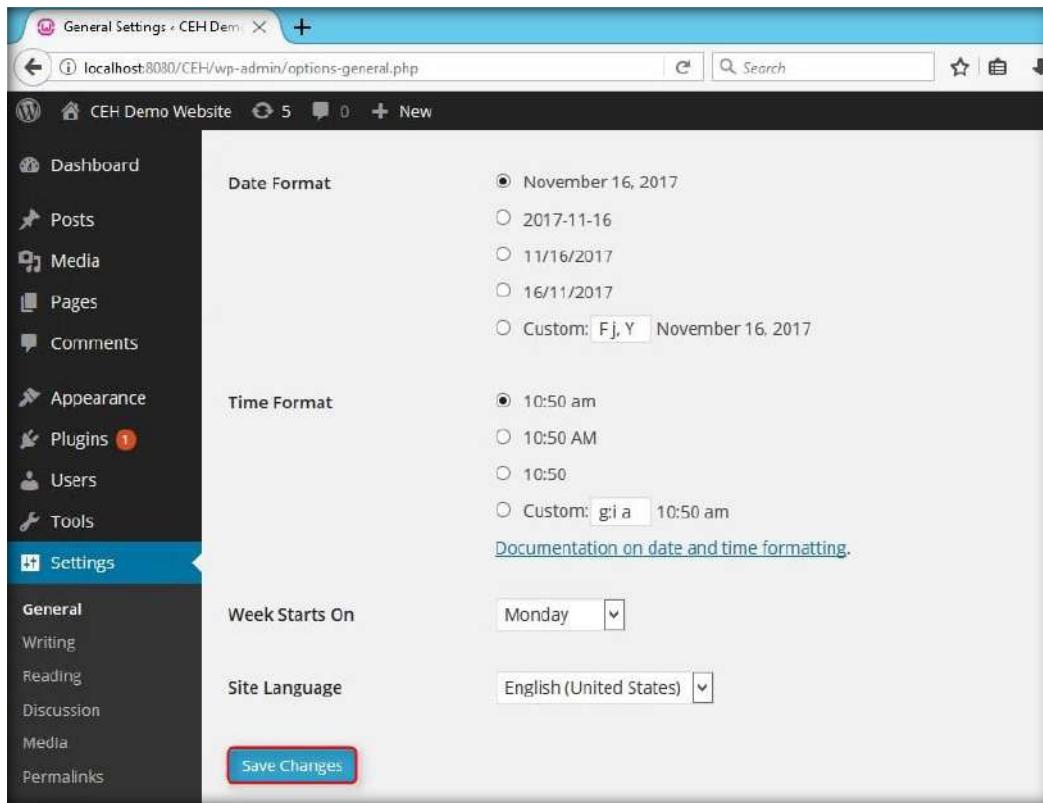


30. WordPress Settings webpage appears, type **http://[IP Address of Windows Server 2012]:8080/CEH** in **WordPress Address (URL)** and **Site Address (URL)** fields

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

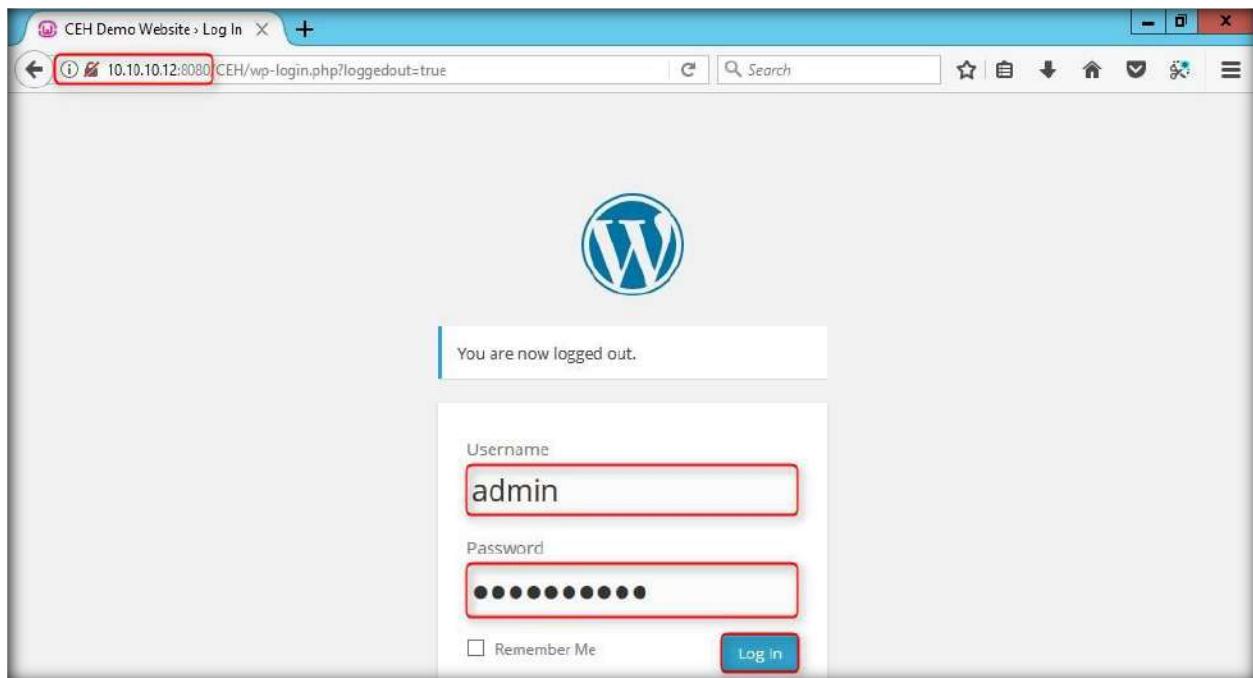


31. Scroll down the webpage and click **Save Changes** button

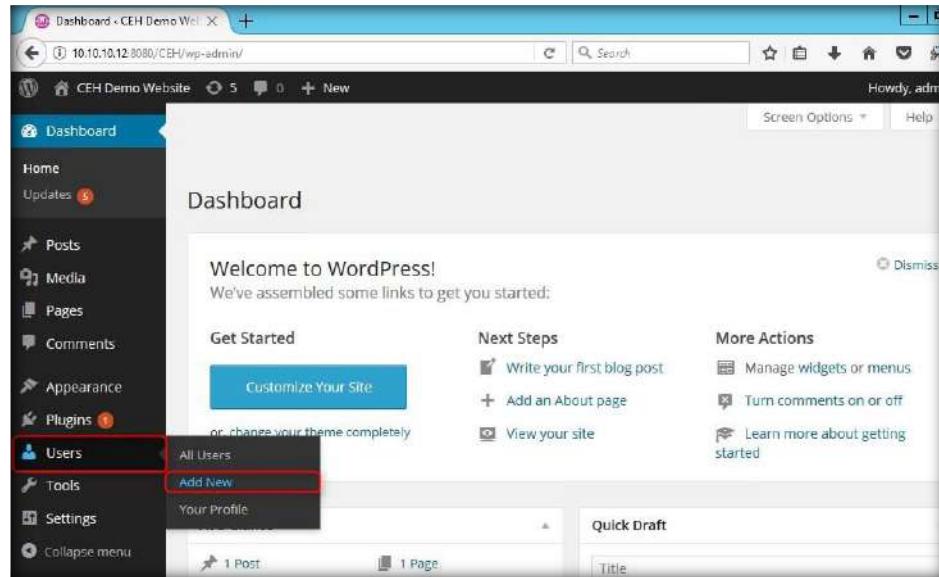


32. On clicking the button, you will be redirected back to the login page. Here, you can observe the IP address of **Windows Server 2012** in the URL field instead of localhost.

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

 A screenshot of a web browser displaying the 'Add New User' page at the URL 10.10.10.12:8080/CEH/wp-admin/user-new.php. The left sidebar shows the 'Users' menu item selected. The main form has the following fields: 'Username (required)' with value 'CEHUser1', 'E-mail (required)' with value 'jason@ceh.com', 'First Name' with value 'jason', 'Last Name' with value 'Brown', 'Website' (empty), 'Password (required)' with value '*****', and 'Repeat Password (required)' with value '*****'. A note below the password fields says: 'Very weak Hint: The password should be at least seven characters long. To make it stronger, use upper and lower case letters, numbers, and symbols like ! @ # % ^ &.'.

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**

The screenshot shows the 'Add New User' form in the WordPress admin interface. The 'Users' menu item is highlighted in blue. The form fields are as follows:

- Username (required): CEHUser1
- Email (required): jason@ceh.com
- First Name: Jason
- Last Name: Brown
- Website: (empty)
- Password: green (highlighted with a red border and labeled 'Very weak')
- Confirm Password: (checkbox checked, labeled 'Confirm use of weak password')
- Send User Notification: (checkbox unchecked)
- Role: Editor (selected from a dropdown menu)

At the bottom is a blue 'Add New User' button.

39. This creates a user account

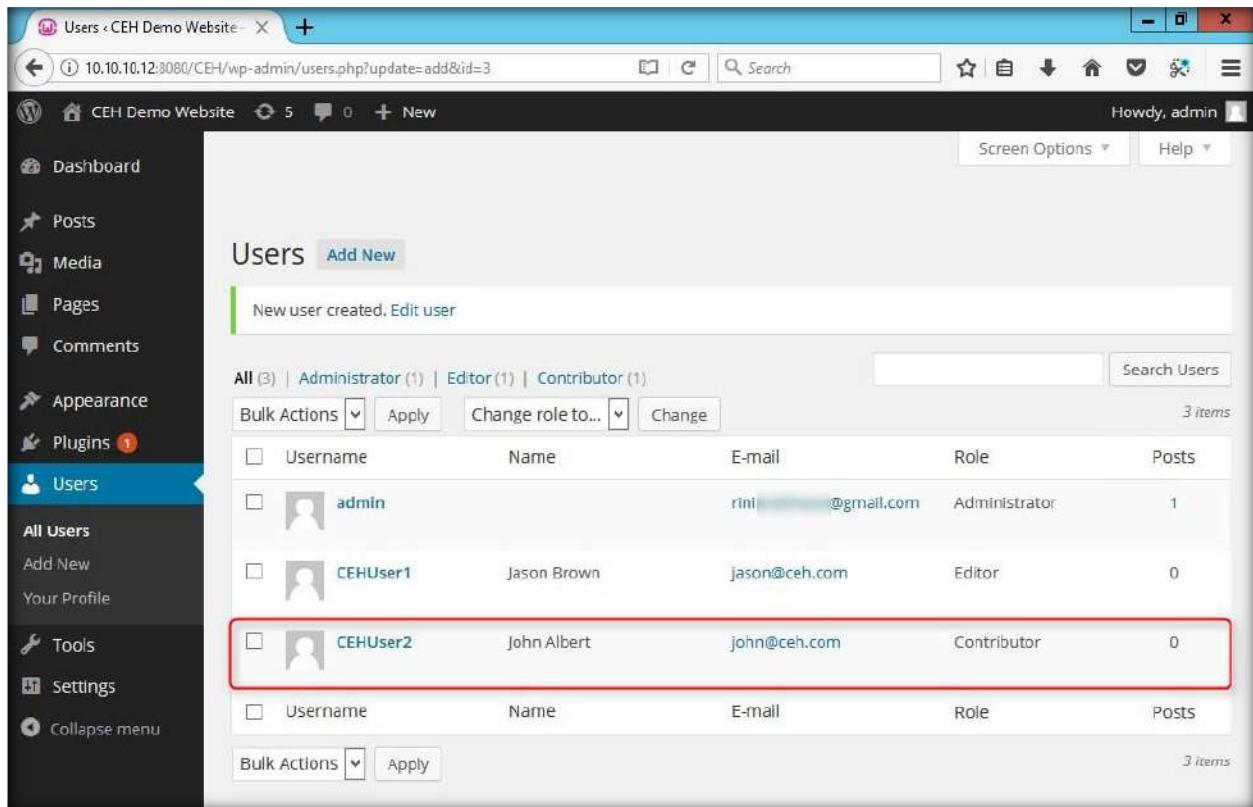
40. Now, click **Add New** to create another user account

The screenshot shows the 'Users' page in the WordPress admin interface. The 'Users' menu item is highlighted in blue. The table displays the following user information:

All (2) Administrator (1) Editor (1)	Search Users			
Bulk Actions				
Username	Name	E-mail	Role	Posts
admin	rini	@gmail.com	Administrator	1
CEHUser1	Jason Brown	jason@ceh.com	Editor	0

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:



The screenshot shows the WordPress Admin interface under the 'Users' section. The left sidebar has 'Users' selected. The main area displays a table of users with columns: Username, Name, E-mail, Role, and Posts. There are three users listed: 'admin' (Name: rini, E-mail: rini@gmail.com, Role: Administrator, Posts: 1), 'CEHUser1' (Name: Jason Brown, E-mail: jason@ceh.com, Role: Editor, Posts: 0), and 'CEHUser2' (Name: John Albert, E-mail: john@ceh.com, Role: Contributor, Posts: 0). The row for 'CEHUser2' is highlighted with a red box.

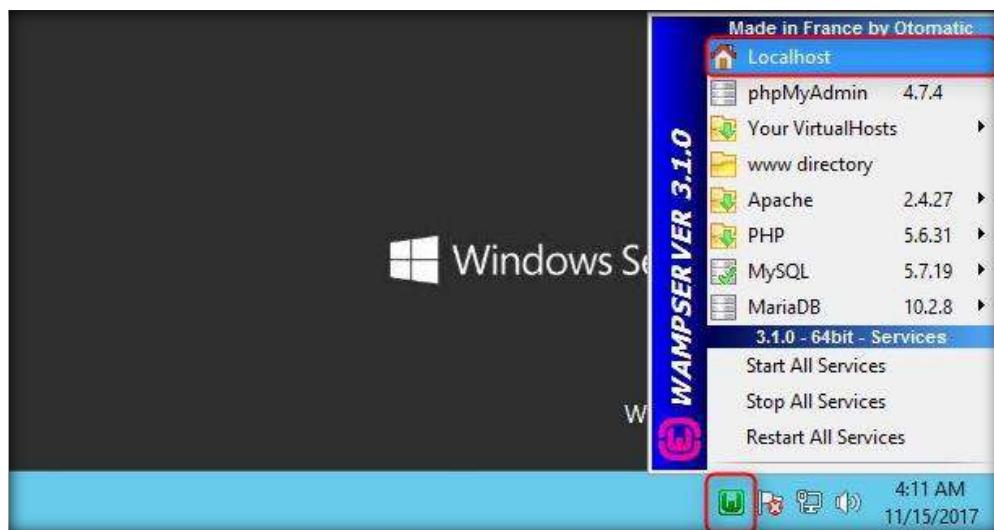
Username	Name	E-mail	Role	Posts
admin	rini	rini@gmail.com	Administrator	1
CEHUser1	Jason Brown	jason@ceh.com	Editor	0
CEHUser2	John Albert	john@ceh.com	Contributor	0
Username	Name	E-mail	Role	Posts

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

[\[Back to Configuration Task Outline\]](#)

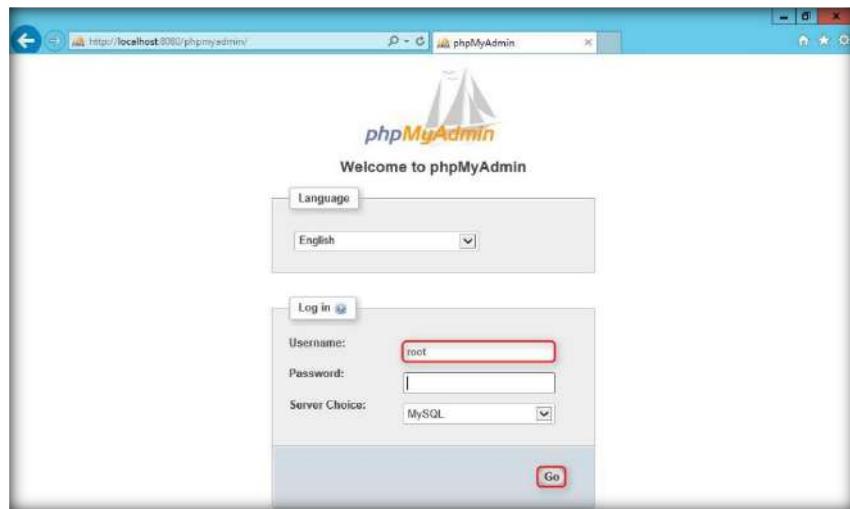
CT#33: Install and Configure Damn Vulnerable Web Application

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.

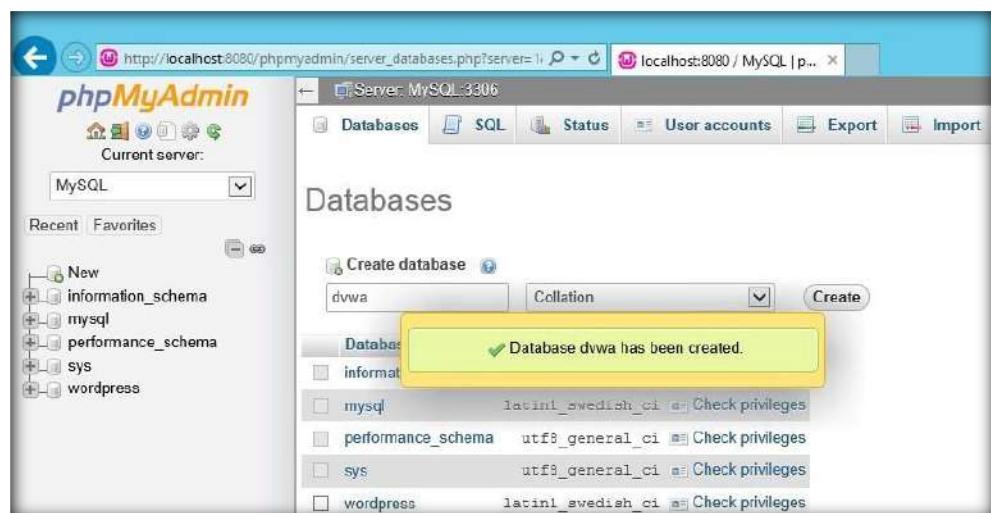
4. **phpMyAdmin** login page appears, type root as the Username and click Go



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**

The screenshot shows the phpMyAdmin interface. In the left sidebar, under 'Current server: MySQL', the 'dwa' database is selected and highlighted with a red box. The main panel shows a message: 'No tables found in database.' Below it is a 'Create table' form. On the right, the 'Operations' menu is open, with 'Privileges' highlighted and also outlined in red. Other options in the menu include 'Routines', 'Events', 'Triggers', and 'Designer'.

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

The screenshot shows the phpMyAdmin interface with the 'dwa' database selected. The main panel displays a table titled 'Users having access to "dwa"'. It contains two rows: one for 'admin' (host: localhost, type: global, privileges: ALL PRIVILEGES, grant: Yes) and one for 'root' (host: localhost, type: global, privileges: ALL PRIVILEGES, grant: Yes). Below the table, there is a 'New' button and a link labeled 'Add user account'. The URL in the address bar is http://localhost:8080/phpmyadmin/server_privileges.php?adduser=1&dbname=dvwa. The taskbar at the bottom shows various application icons and the date/time: 8:52 PM 11/16/2017.

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

The screenshot shows the 'phpMyAdmin' interface for adding a new user. In the 'Login Information' section, the 'User name' is set to 'dvwa_user', 'Host name' is set to 'Local' (with 'localhost' in the dropdown), and the 'Password' and 'Re-type' fields both contain '*****'. In the 'Database for user account' section, the 'Grant all privileges on database dvwa' checkbox is checked. At the bottom, the 'Global privileges' section has a 'Check all' checkbox which is checked.

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

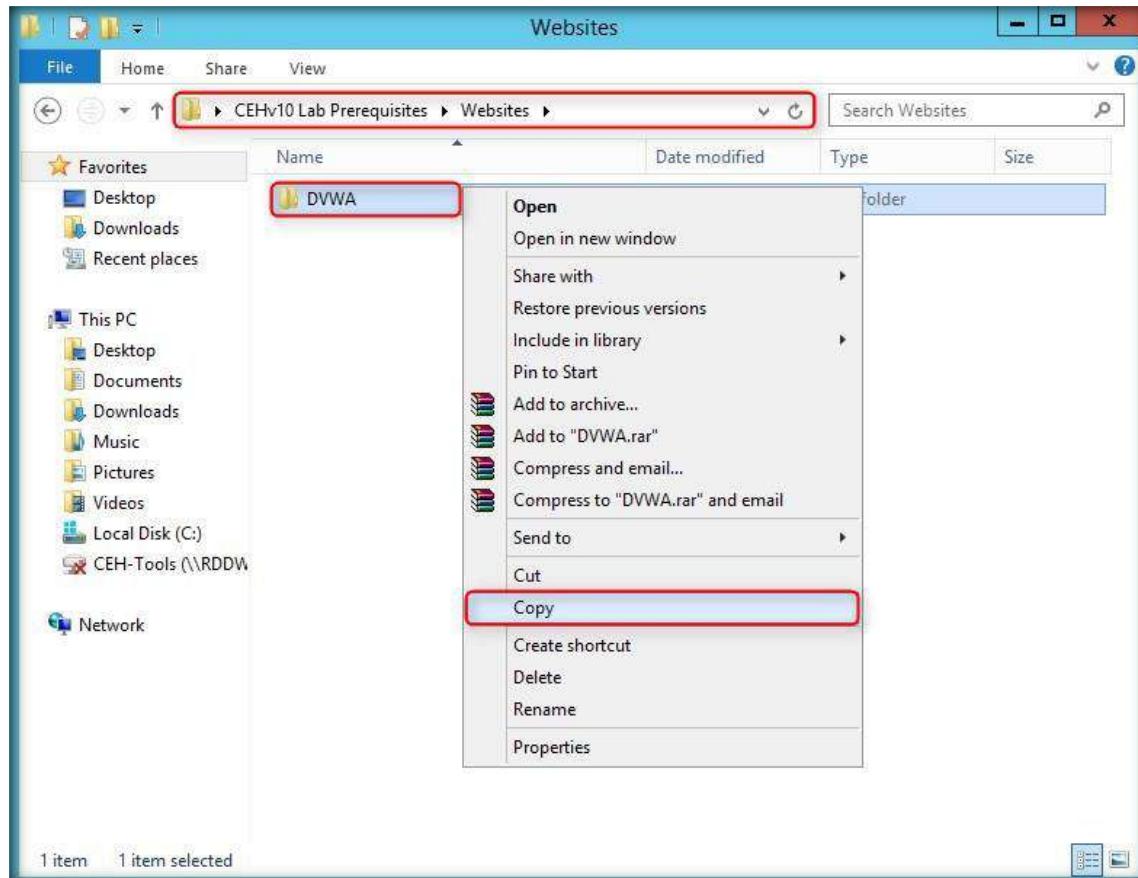
The screenshot shows the 'Edit privileges' page for the 'dvwa_user' account. It displays a success message: 'You have added a new user.' Below this is a SQL command for creating the user:

```
CREATE USER 'dvwa_user'@'localhost' IDENTIFIED WITH mysql_native_password AS '*****';GRANT ALL PRIVILEGES ON *.* TO 'dvwa_user'@'localhost' REQUIRE NONE WITH GRANT OPTION;
MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR 0
MAX_USER_CONNECTIONS 0;GRANT ALL PRIVILEGES ON `dvwa`.* TO 'dvwa_user'@'localhost';
```

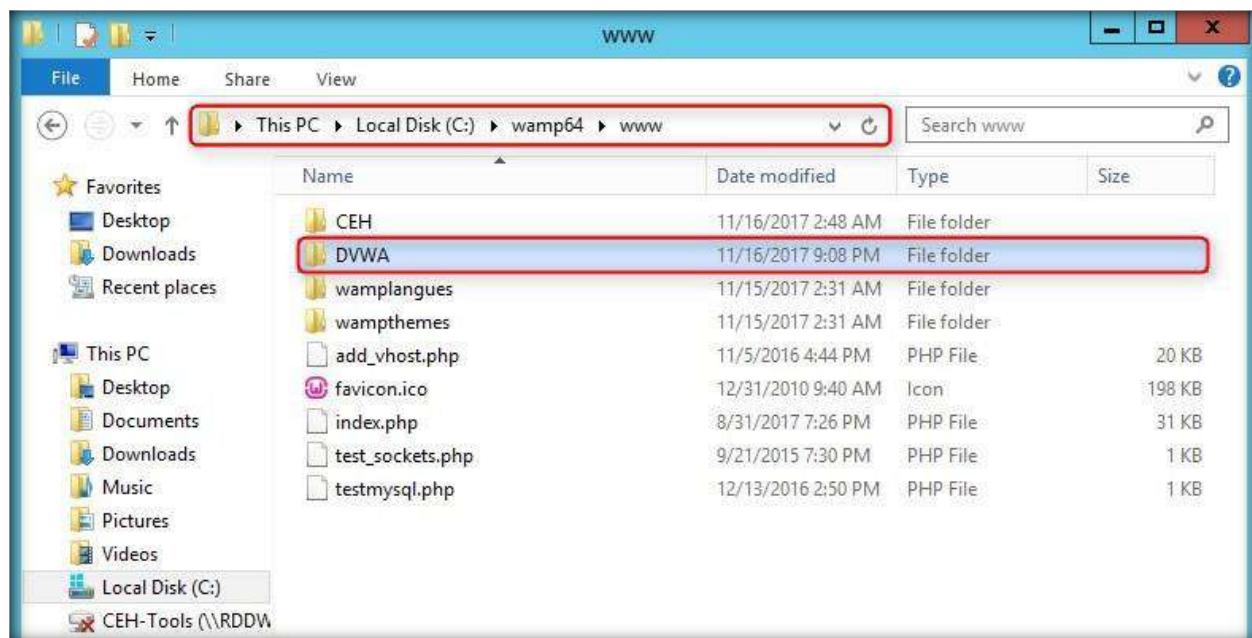
At the bottom, there is a note: 'Edit privileges: User account 'dvwa_user'@'localhost' - Database dvwa'.

13. Close the Web browser

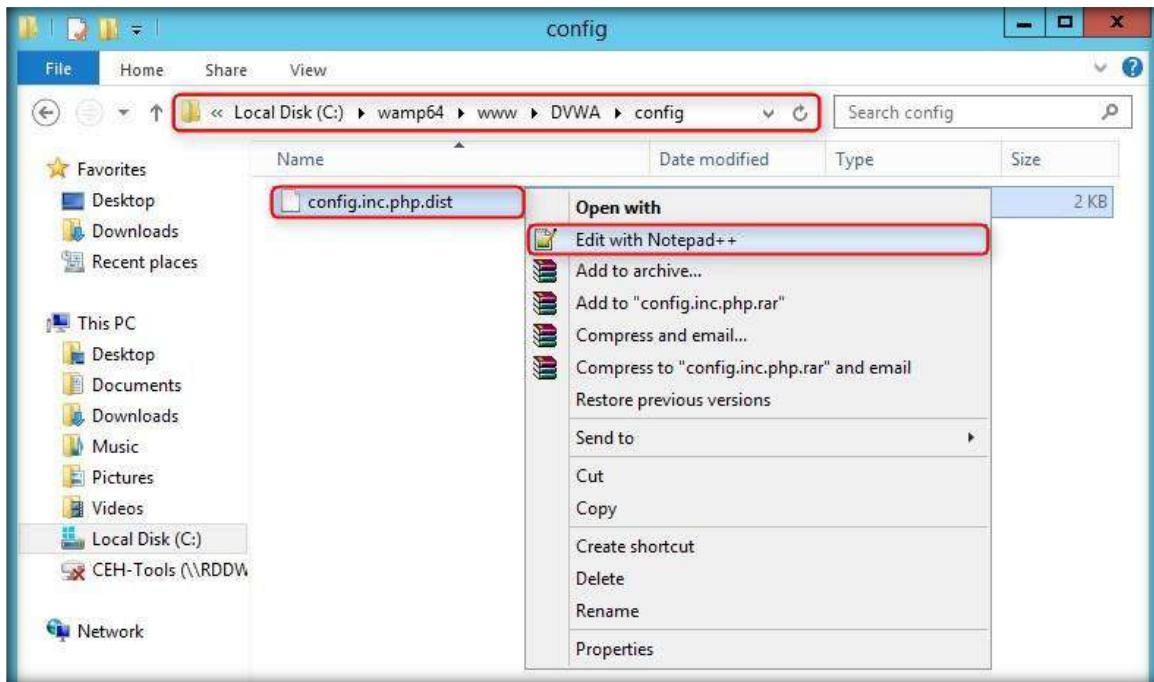
14. Navigate to **Z:\CEH-Tools\CEHv10 Lab Prerequisites\Websites** and copy the **DVWA** folder



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:

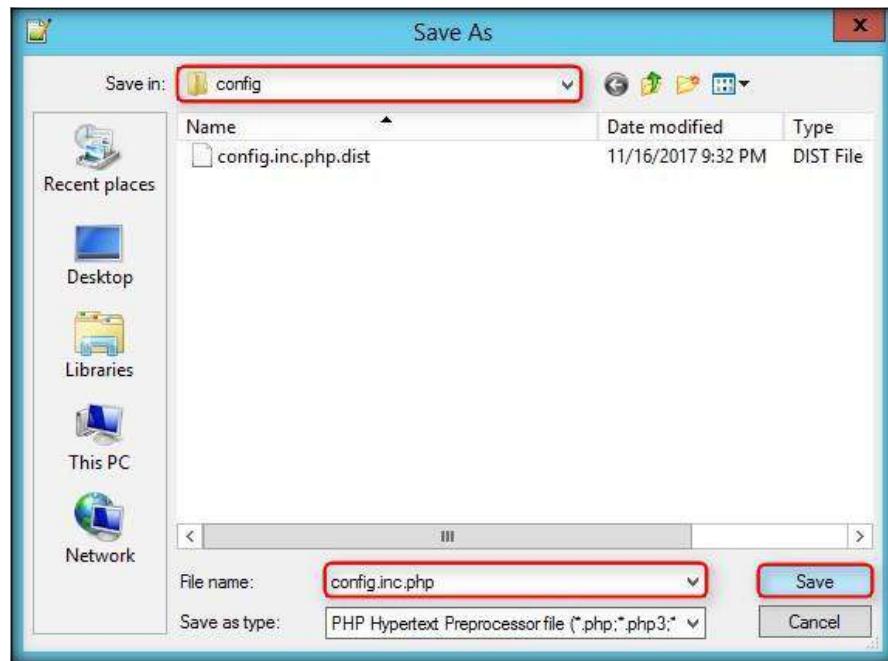
- In **line no. 18**, assign the mysql database server host as **localhost** in single quotes.
- In **line no. 19**, assign the database name as **dvwa** in single quotes.
- In **line no. 20**, assign the mysql database username as **dvwa_user** in single quotes.
- In **line no. 21**, assign the mysql database password as **test@123** in single quotes.

```

1 <?php
2
3 # If you are having problems connecting to the MySQL database and all of the variables below are correct
4 # try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
5 # Thanks to @digininja for the fix.
6
7 # Database management system to use
8 $DBMS = 'MySQL';
9 #$DBMS = 'PGSQL'; // Currently disabled
10
11 # Database variables
12 # WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
13 # Please use a database dedicated to DVWA.
14 #
15 # If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
16 # See README.md for more information on this.
17 ${_DVWA} = array();
18 ${_DVWA['db_server']} = 'localhost';
19 ${_DVWA['db_database']} = 'dvwa';
20 ${_DVWA['db_user']} = 'dvwa_user';
21 ${_DVWA['db_password']} = 'test@123';
22

```

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

A screenshot of a web browser window titled 'Setup :: Damn Vulnerable Web Application'. The address bar shows 'localhost:8080/DVWA/setup.php'. The page content includes a 'Setup Check' section with the following details:

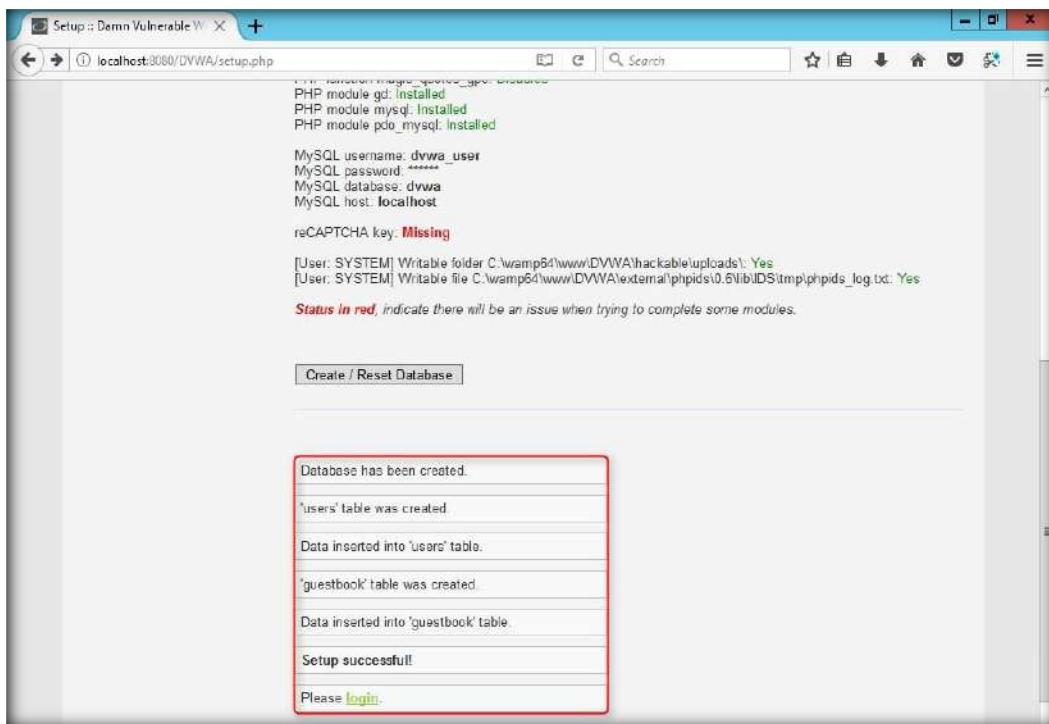
Operating system:	Windows
Backend database:	MySQL
PHP version:	5.6.31
Web Server SERVER_NAME:	localhost
PHP function display_errors:	Enabled (Easy Mode)
PHP function safe_mode:	Disabled
PHP function allow_url_include:	Disabled
PHP function allow_url_fopen:	Enabled
PHP function magic_quotes_gpc:	Disabled
PHP module gd:	Installed
PHP module mysql:	Installed
PHP module pdo_mysql:	Installed
MySQL username:	dvwa_user
MySQL password:	*****
MySQL database:	dvwa
MySQL host:	localhost
reCAPTCHA key:	Missing

[User: SYSTEM] Writable folder C:\wamp64\www\DVWA\hackable\uploads: Yes
[User: SYSTEM] Writable file C:\wamp64\www\DVWA\external\phpids\0.6\lib\DS\tmp\phpids_log.txt: Yes

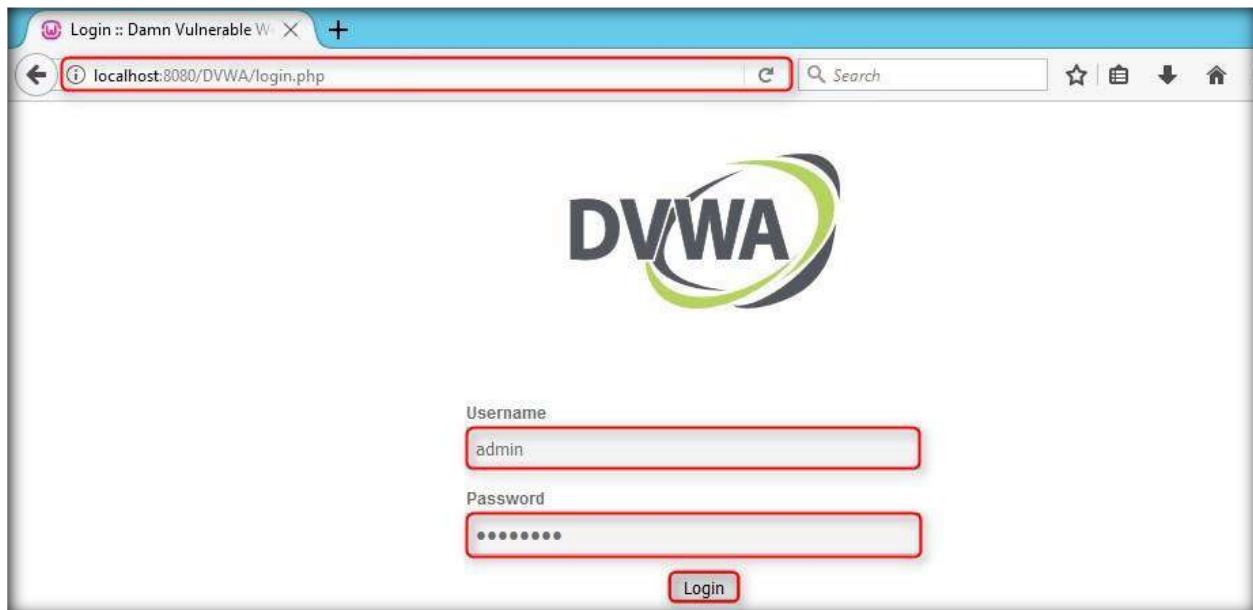
Status in red, indicate there will be an issue when trying to complete some modules.

Create / Reset Database

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

Welcome :: Damn Vulnerable Web Application! [+/-](#)

localhost:8080/DVWA/index.php

General Instructions

The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are both documented and undocumented vulnerability with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users)!

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public

DVWA Security

- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- DVWA Security**
- PHP Info
- About

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

DVWA Security :: Damn Vulnerable Web Application! [+/-](#)

localhost:8080/DVWA/security.php

DVWA Security

Security Level

Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

(Low)

- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)

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

The screenshot shows a web browser window for DVWA Security. The URL is `localhost:8080/DVWA/security.php`. The left sidebar has a 'Logout' button highlighted with a red border. The main content area is titled 'Security Level'. It says 'Security level is currently: low.' Below this, it states: 'You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:' followed by a numbered list of four options. At the bottom, there is a dropdown menu set to 'Low' and a 'Submit' button. A message at the bottom of the page says 'Security level set to low'.

INSTRUCTIONS

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

DVWA Security

PHP Info

About

Logout

Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. Its use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

Low

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently: **disabled**. [[Enable PHPIDS](#)]

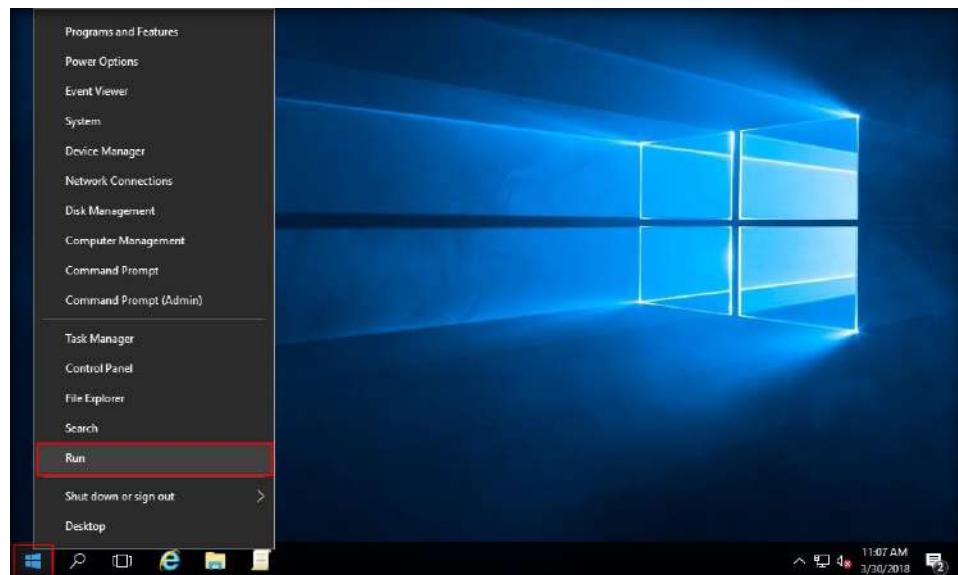
[[Simulate attack](#)] - [[View IDS log](#)]

Security level set to low

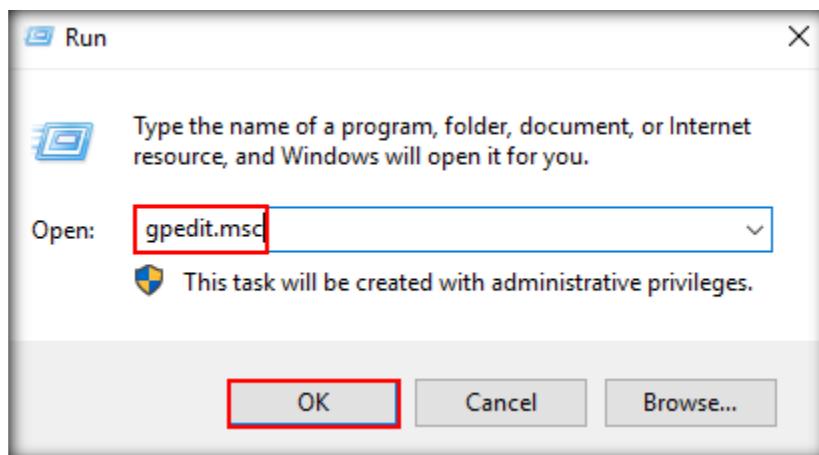
[\[Back to Configuration Task Outline\]](#)

CT#34: Configure Windows Components

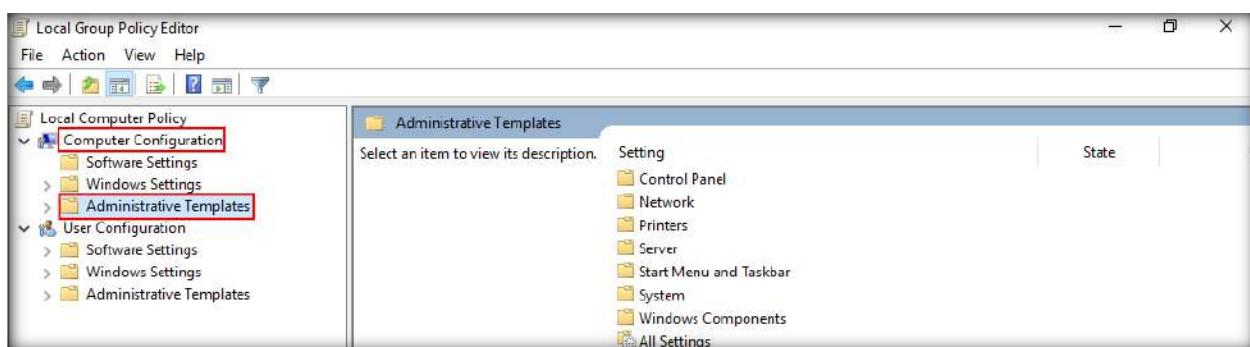
1. Login to Windows Server 2016 machine, right-click on Start and click Run as shown in the screenshot



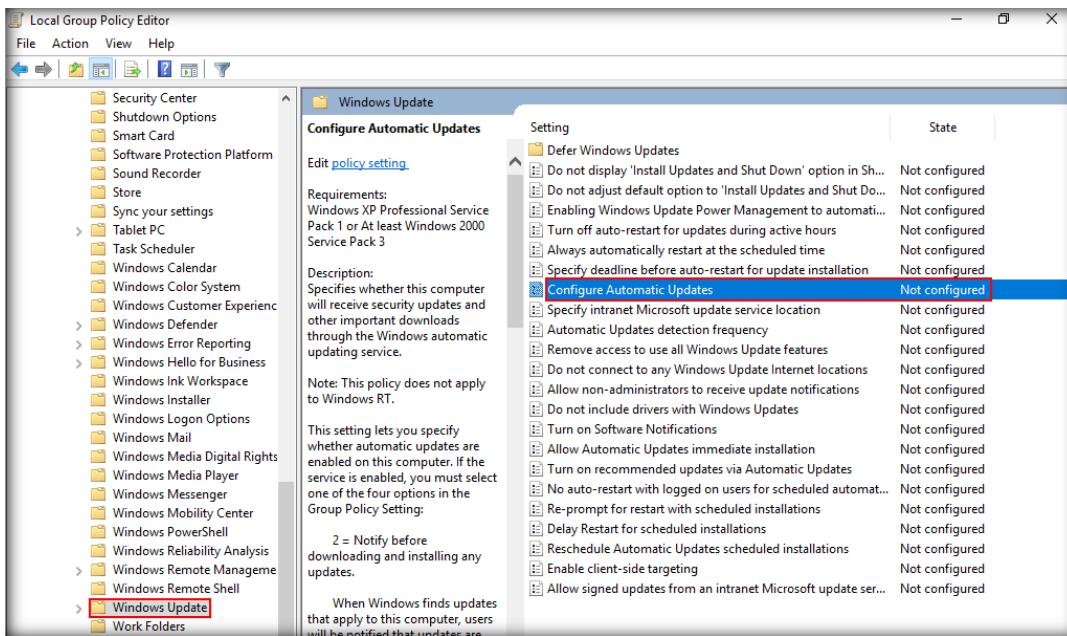
2. Run Command window appears, type gpedit.msc and click OK



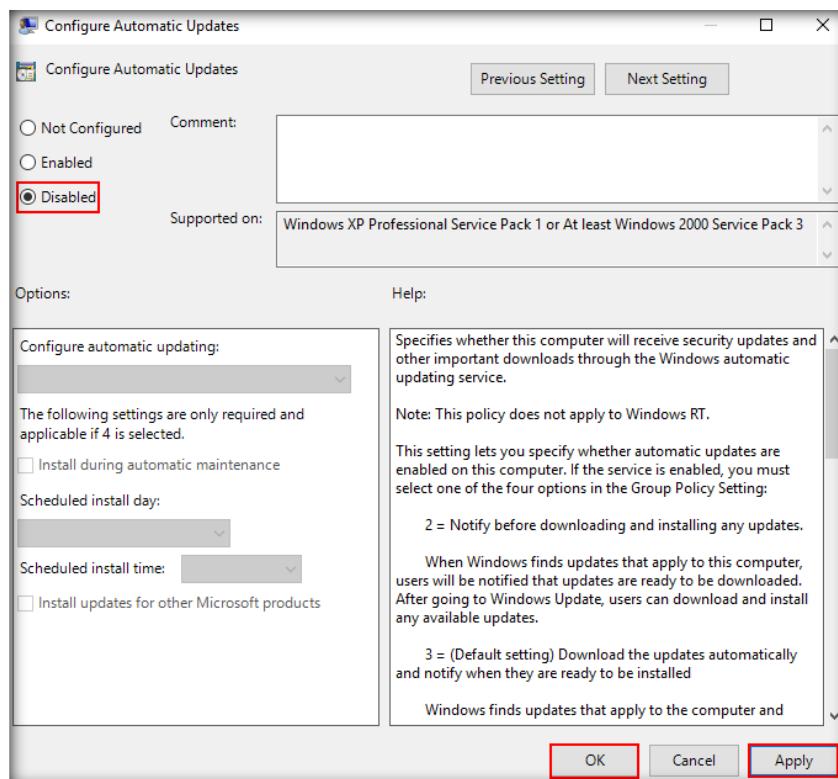
3. Local Group Policy Editor window appears, expand Administrative Templates under Computer Configuration in the left pane



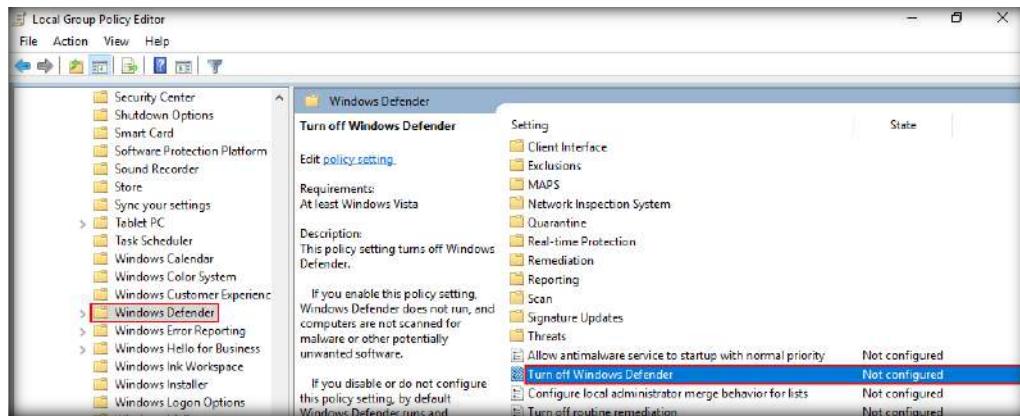
4. In Administrative Templates expand Windows Components and scroll down and click Windows Update in the left pane and double-click Configure Automatic Updates in the right-pane as shown in the screenshot



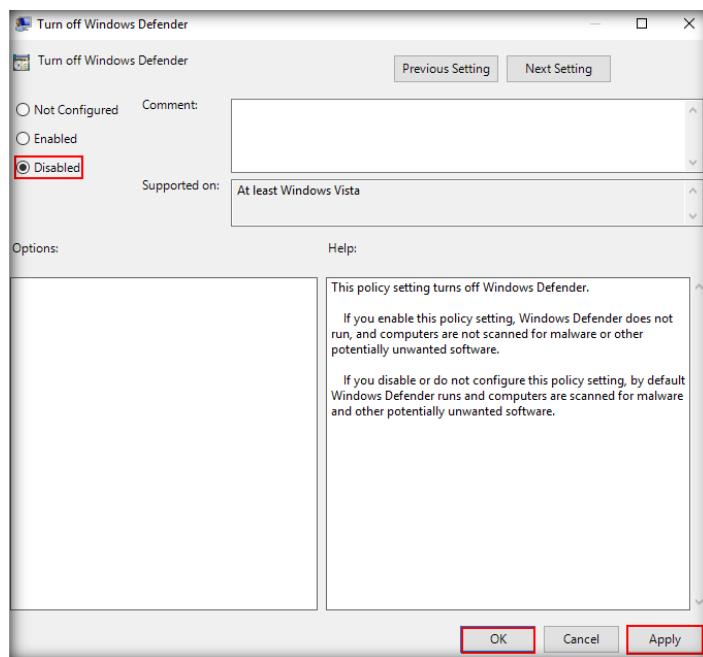
5. Configure Automatic Updates window appears, select **Disabled** radio button and click **Apply** and **OK**



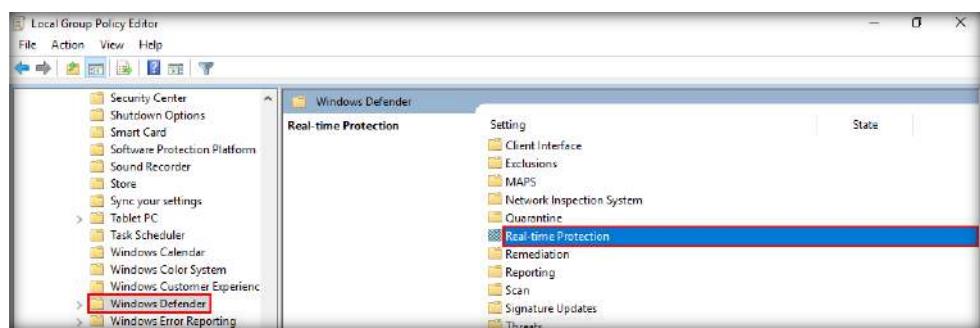
6. In the left pane click Windows Defender and double-click Turn off Windows Defender in the right-pane of the window as shown in the screenshot



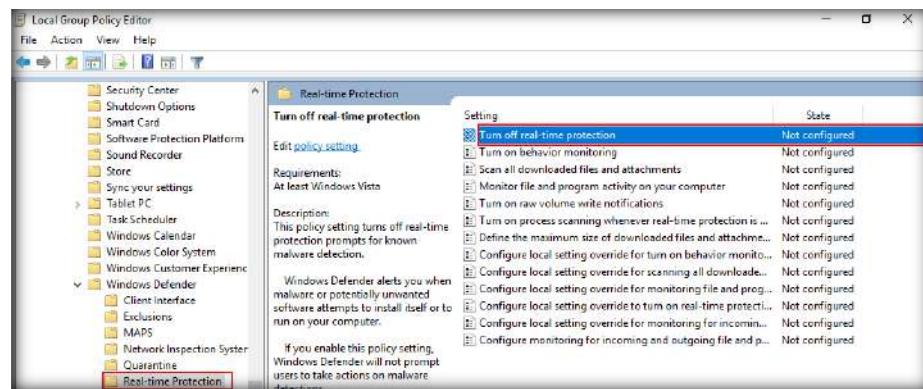
7. Turn off Windows Defender window appears, select Disabled radio button and click Apply and OK



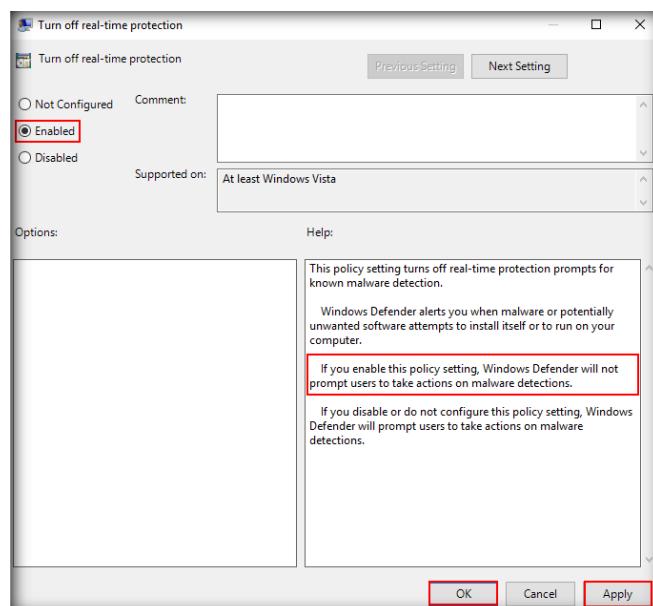
8. Double-click Real-time Protection in the Windows Defender as shown in the screenshot



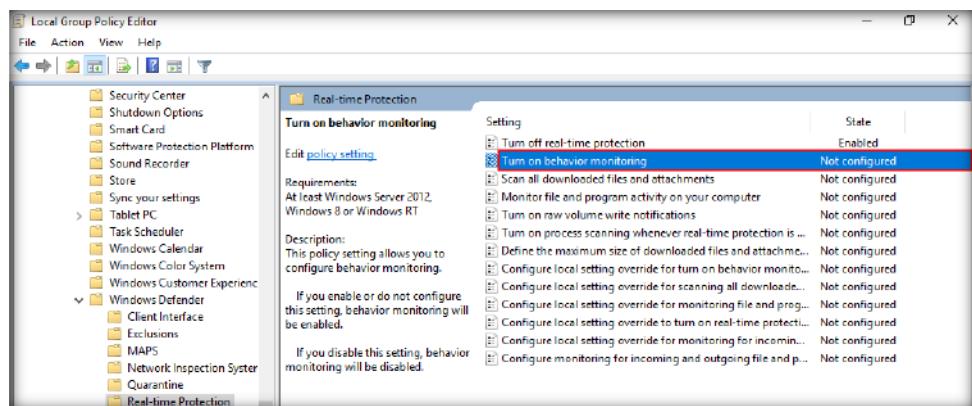
9. Real-time Protection settings appears, double-click Turn off real-time protection to configure in the right pane



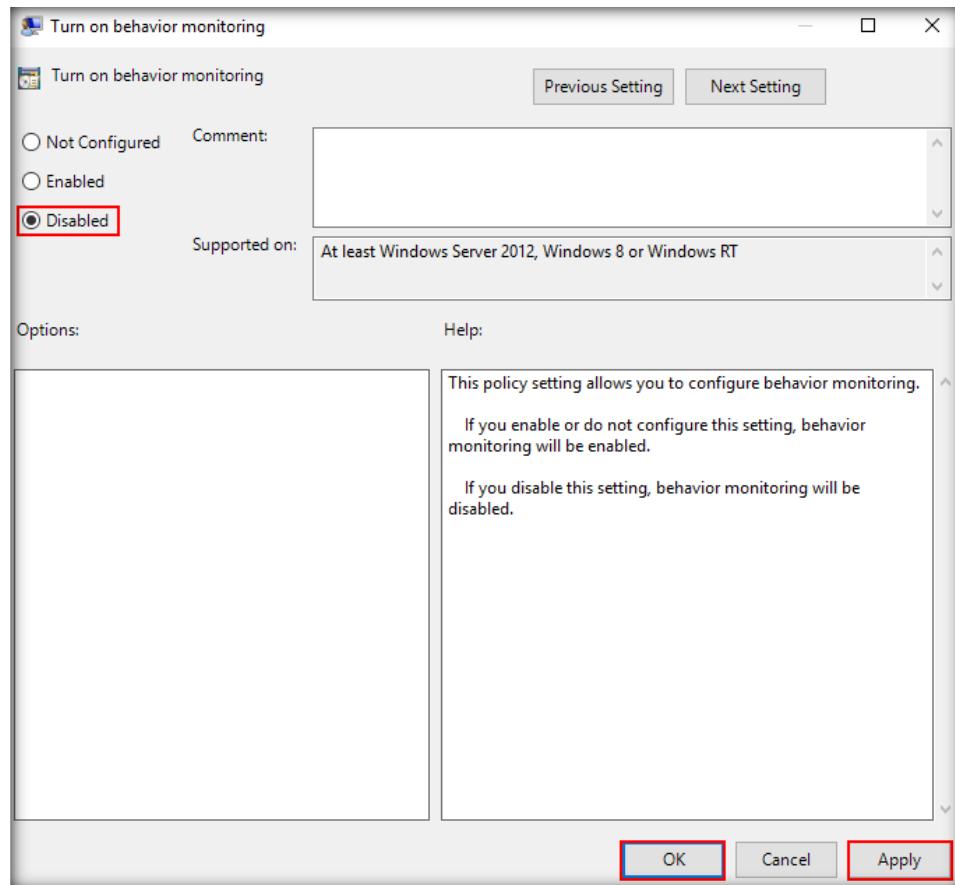
10. Turn off real-time protection window appears, select Enabled radio button and click Apply and OK



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

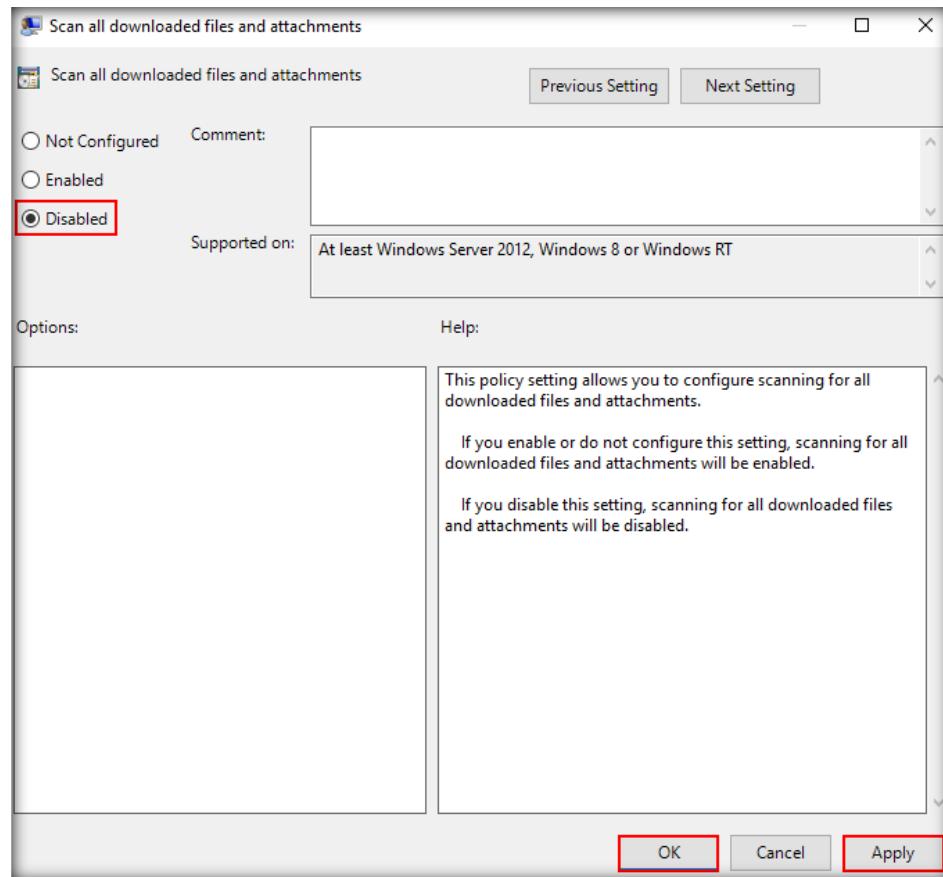
The screenshot shows the Local Group Policy Editor interface. The left pane displays a tree structure of policy settings, including Security Center, Real-time Protection, and Windows Defender. The 'Real-time Protection' node is expanded, showing the 'Scan all downloaded files and attachments' setting. This setting is described as follows:

Setting: Scan all downloaded files and attachments
Requirements: At least Windows Server 2012, Windows 8 or Windows RT
Description: This policy setting allows you to configure scanning for all downloaded files and attachments. If you enable or do not configure this setting, scanning for all downloaded files and attachments will be enabled.

The 'State' column for this setting shows 'Not configured', which is highlighted with a red box. The right pane lists several sub-options for this setting, each with its own state:

Setting	State
Turn off real-time protection	Enabled
Turn on behavior monitoring	Disabled
Scan all downloaded files and attachments	Not configured
Monitor file and program activity on your computer	Not configured
Turn on raw volume write notifications	Not configured
Turn on process scanning whenever real-time protection is ...	Not configured
Define the maximum size of downloaded files and attachme...	Not configured
Configure local setting override for turn on behavior monito...	Not configured
Configure local setting override for scanning all download...	Not configured
Configure local setting override for monitoring file and prog...	Not configured
Configure local setting override to turn on real-time protect...	Not configured
Configure local setting override for monitoring for incomin...	Not configured
Configure monitoring for incoming and outgoing file and p...	Not configured

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

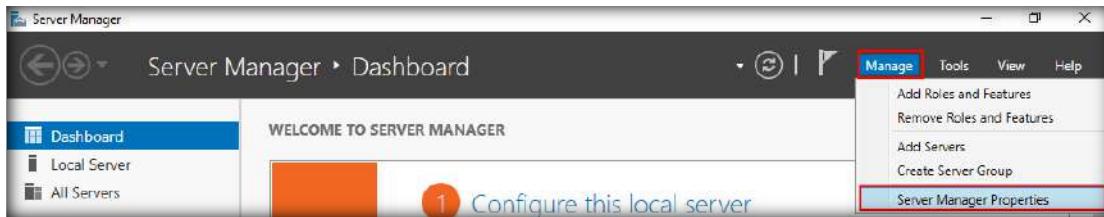


15. Similarly follow the above steps to configure Windows Components in all the Windows machines.

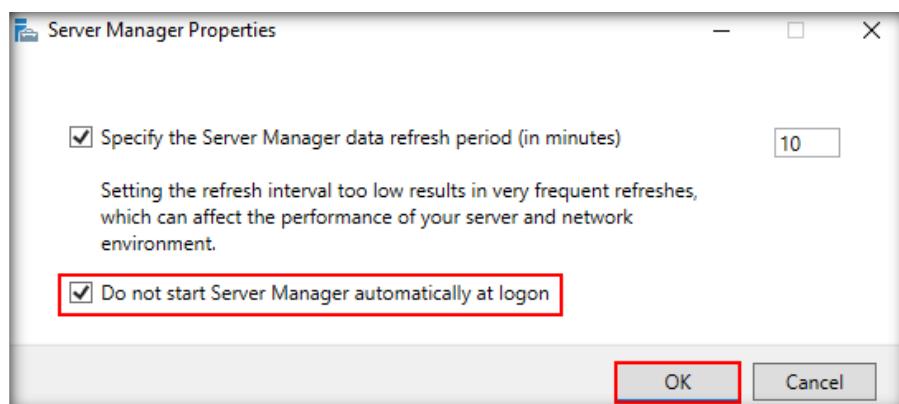
[\[Back to Configuration Task Outline\]](#)

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

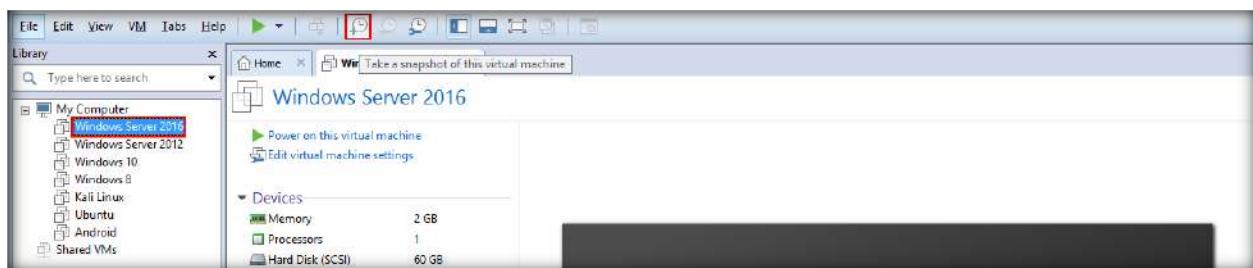


Note: Similarly follow the above steps to configure Server Manager properties in Windows Server 2012 machine

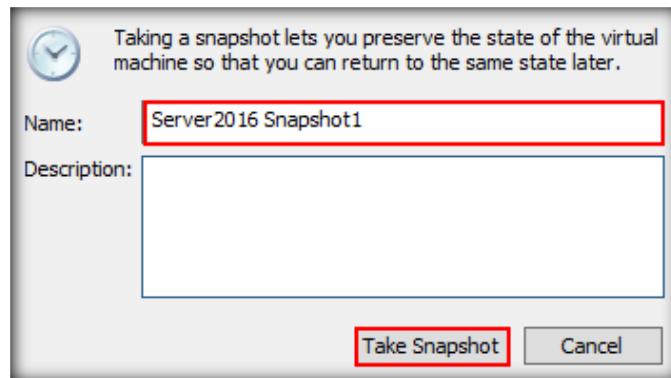
[\[Back to Configuration Task Outline\]](#)

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