

BUILDBOOK
BY
GULDZHAKHON KHUDZHABEKOVA



SOC CYBERSECURITY ANALYST

Training Program

LAB WORK 1

Install Oracle VM VirtualBox

LAB WORK 2

Install Windows Server 2016 on VirtualBox

LAB WORK 3

Install Active Directory on Windows Server 2016

LAB WORK 4

Join Domain Controller

LAB WORK 5

Sumologic

LAB WORK 6

Nessus

LAB WORK 7

Sophos

LAB WORK 8

pfSense

LAB WORK 1

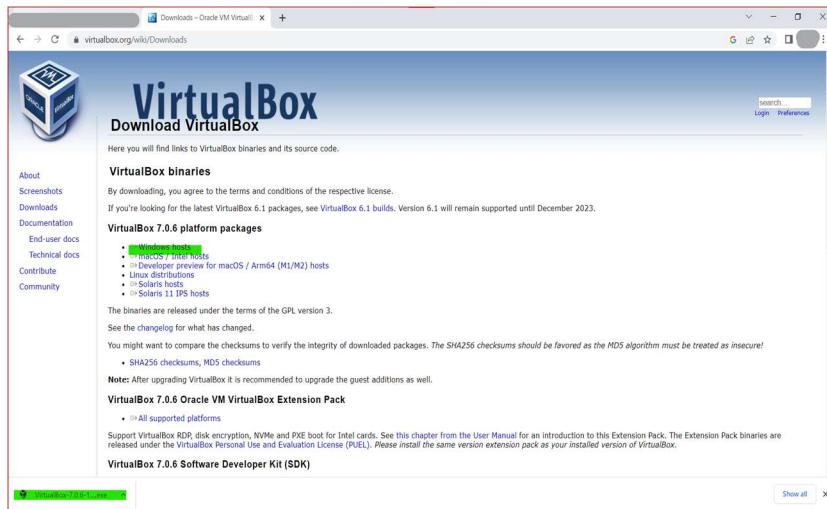
Install Oracle VM VirtualBox

LAB WORK 1

Install Oracle VM VirtualBox

Follow the link to download and install:

<https://www.virtualbox.org/wiki/Downloads>



1. Click on the compatible with your device version.
2. Run setup file.
3. When Installation is completed, open VirtualBox Manager page.

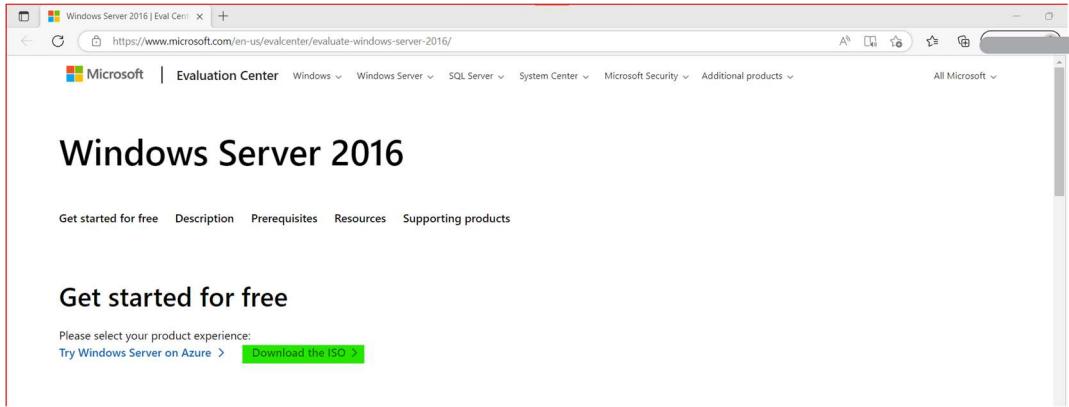


LAB WORK 1 COMPLETED

LAB WORK 2
Install Windows Server 2016 on VirtualBox

LAB WORK 2

Install Windows Server 2016 on VirtualBox



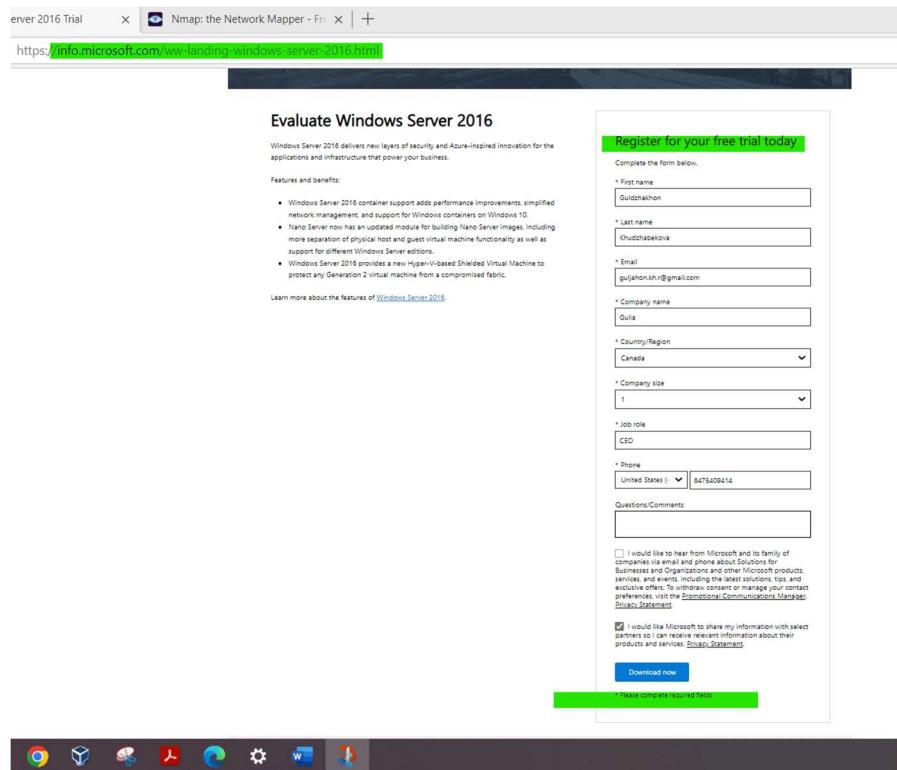
The screenshot shows a web browser window with the URL <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2016/>. The page title is "Windows Server 2016". The main content area features a section titled "Get started for free" with a green button labeled "Download the ISO >". Above this button, there is a link "Try Windows Server on Azure >". The browser's navigation bar includes links for Microsoft Evaluation Center, Windows, Windows Server, SQL Server, System Center, Microsoft Security, and Additional products.

Follow the link to download ISO file for Windows Server 2016:

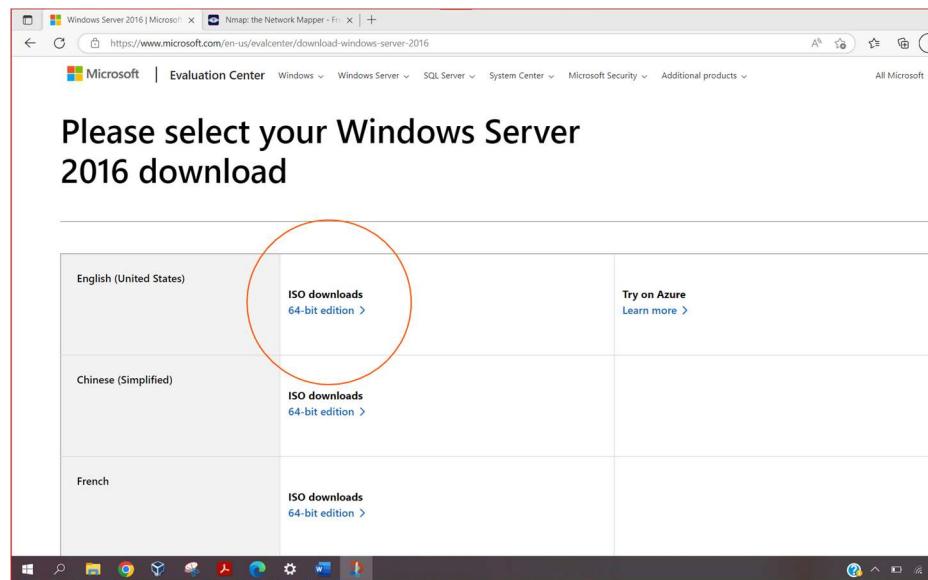
[Windows Server 2016 Trial \(microsoft.com\)](https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2016/)

LAB WORK 2

Install Windows Server 2016 on VirtualBox



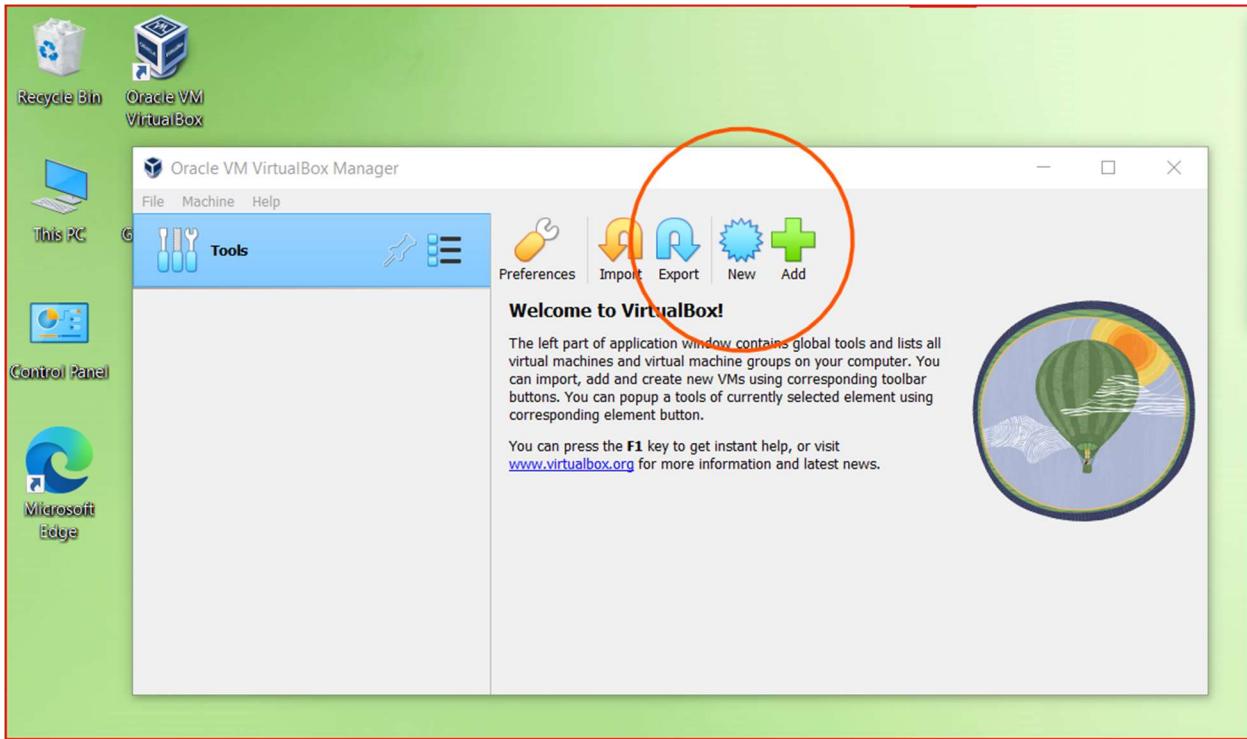
Fill out the form and click **Download**.



Follow the instruction.

LAB WORK 2

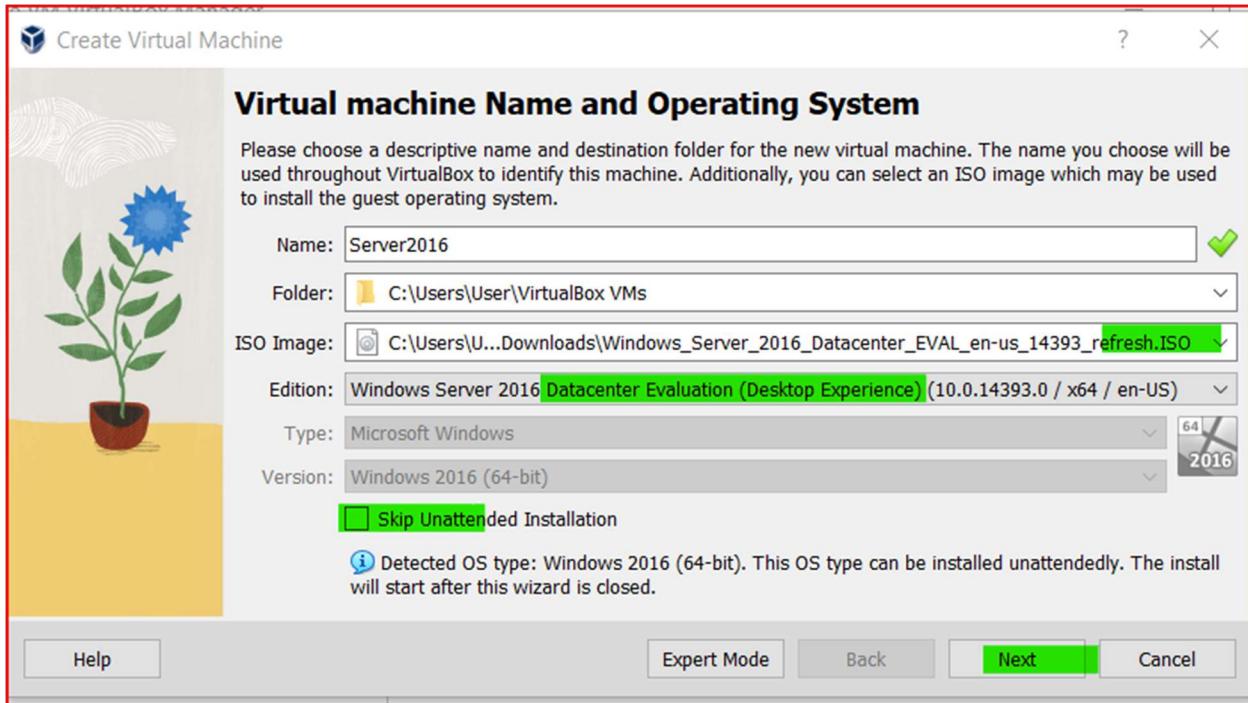
Install Windows Server 2016 on VirtualBox



Open VirtualBox icon on the desktop and click **New**.

LAB WORK 2

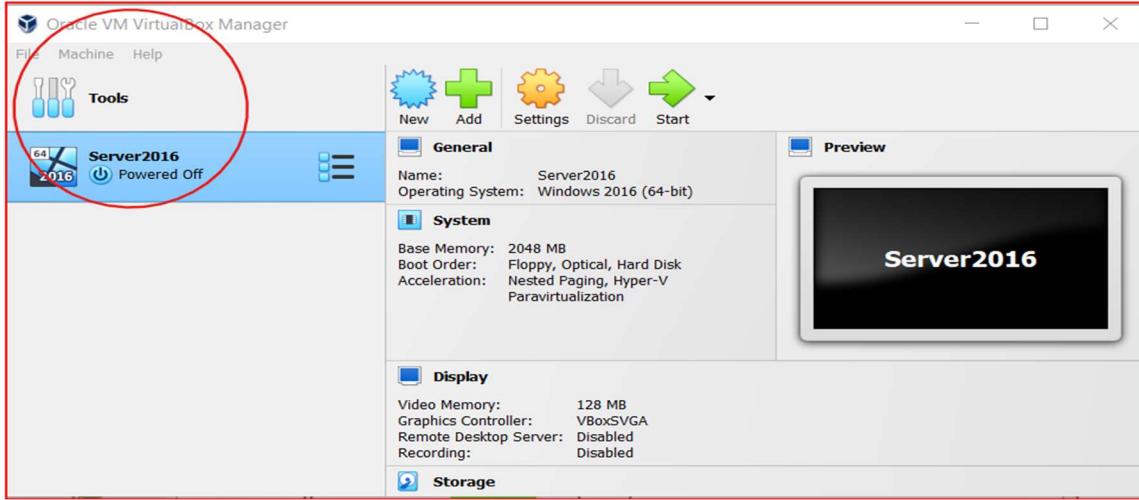
Install Windows Server 2016 on VirtualBox



1. Enter desired name.
2. Choose ISO file
3. Click on “Datacenter Evaluation (Desktop Experience)”
4. Skip unattended installation.
5. leave options by default

LAB WORK 2

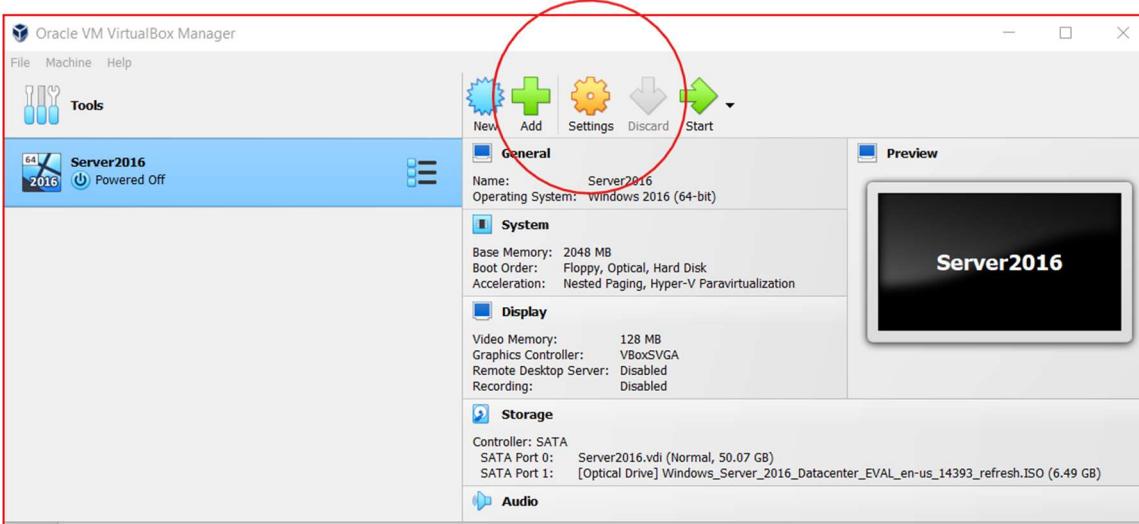
Install Windows Server 2016 on VirtualBox



VirtualBox manager:

All virtual machines will be appeared under **Tools**.

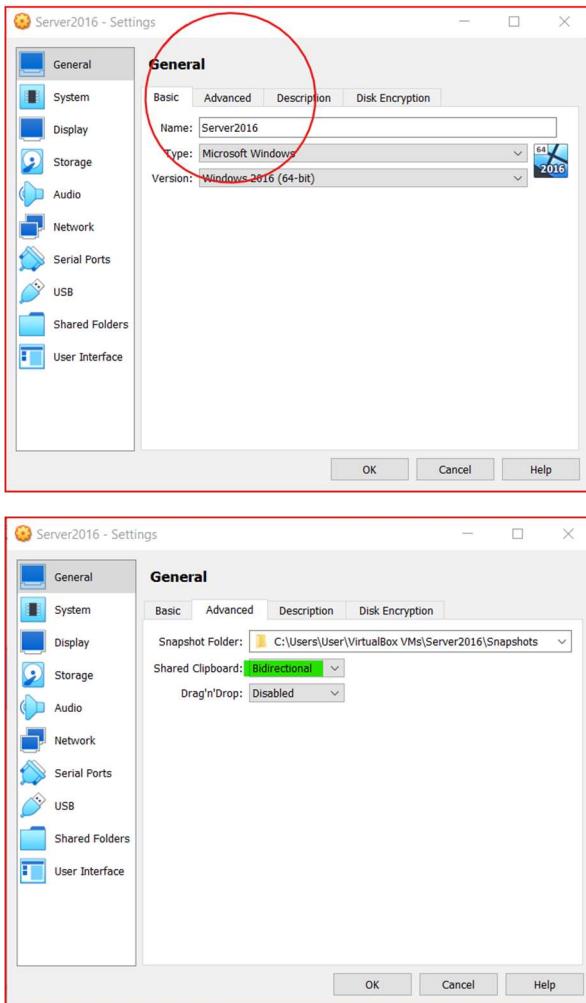
Next, we will apply configurations.



Go to **Settings**.

LAB WORK 2

Install Windows Server 2016 on VirtualBox

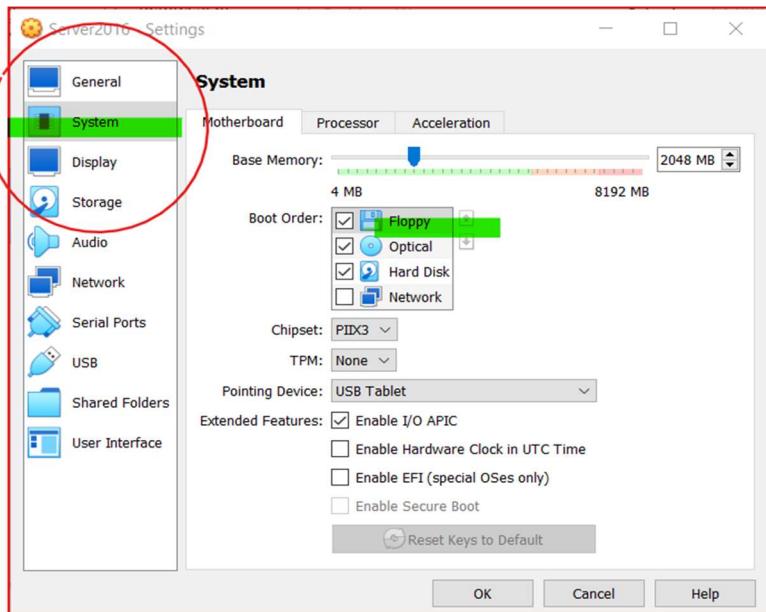


Shared clipboard means the ability to copy and paste from host machine onto virtual.

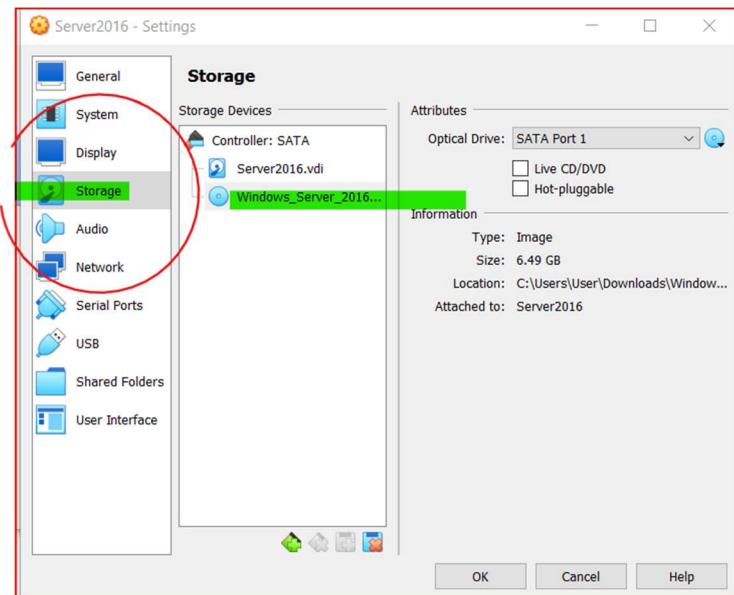
- If shared clipboard is disabled, virtual machine is completely isolated from host machine.
- You will not be able to copy and paste anything from host machine, which is recommended for the security reason.
- For this lab bidirectional shared clipboard is safe, and easy.

LAB WORK 2

Install Windows Server 2016 on VirtualBox



From boot order disable **Floppy**.



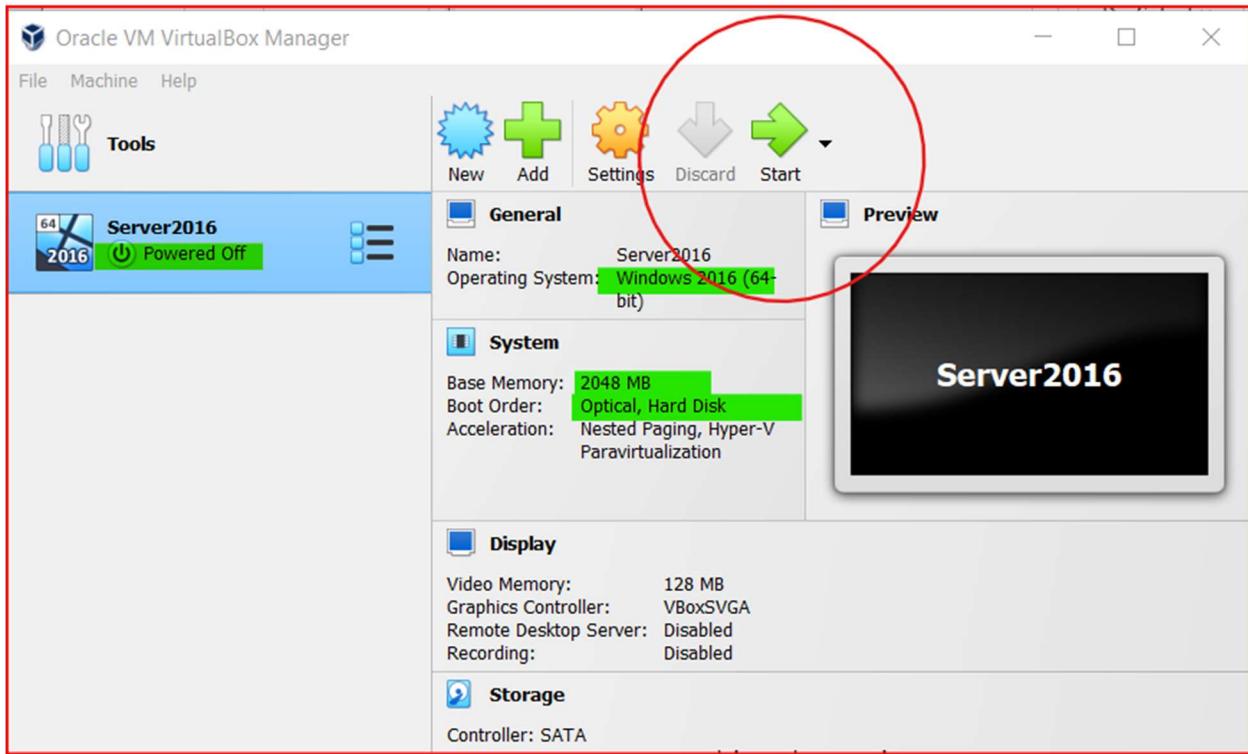
Leave other options by default.

Under SATA Controller on **Empty** disk click and choose the **iso** file you downloaded and remembered where it was stored.

Click **OK**

LAB WORK 2

Install Windows Server 2016 on VirtualBox

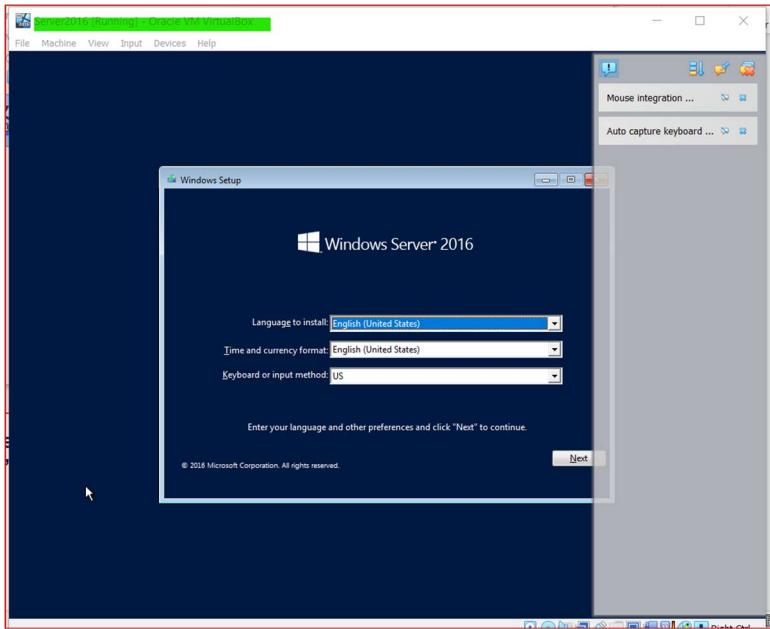


Windows Server 2016 is set to go.

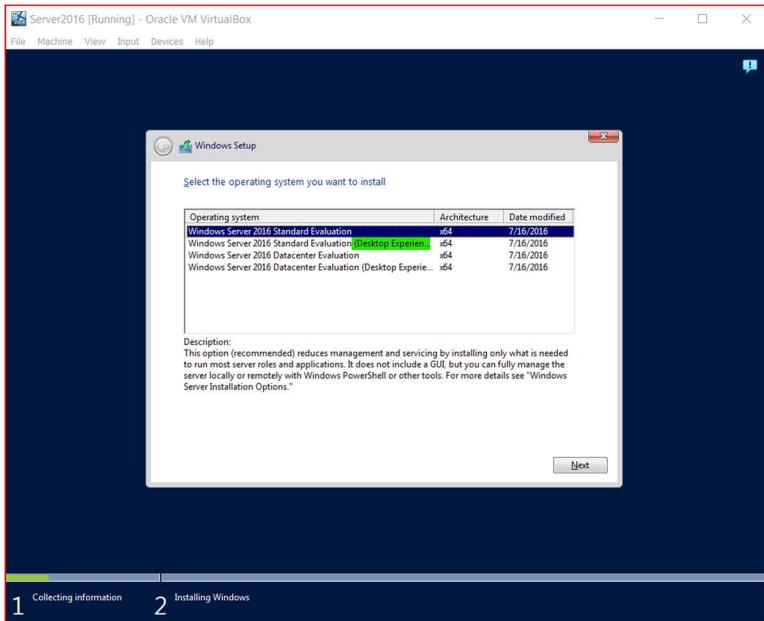
Click **Start** to run installation.

LAB WORK 2

Install Windows Server 2016 on VirtualBox



Follow instruction – **Next, Install Now, Next,**



Operating system	Architecture	Date modified
Windows Server 2016 Standard Evaluation	x64	7/16/2016
Windows Server 2016 Standard Evaluation (Desktop Experience)	x64	7/16/2016
Windows Server 2016 Datacenter Evaluation	x64	7/16/2016
Windows Server 2016 Datacenter Evaluation (Desktop Experience)	x64	7/16/2016

Description:
This option (recommended) reduces management and servicing by installing only what is needed to run most server roles and applications. It does not include a GUI, but you can fully manage the server locally or remotely with Windows PowerShell or other tools. For more details see "Windows Server Installation Options."

Next >

1 Collecting information

2 Installing Windows

It is important to install “Standard Evaluation Desktop Experience” to use GUI.

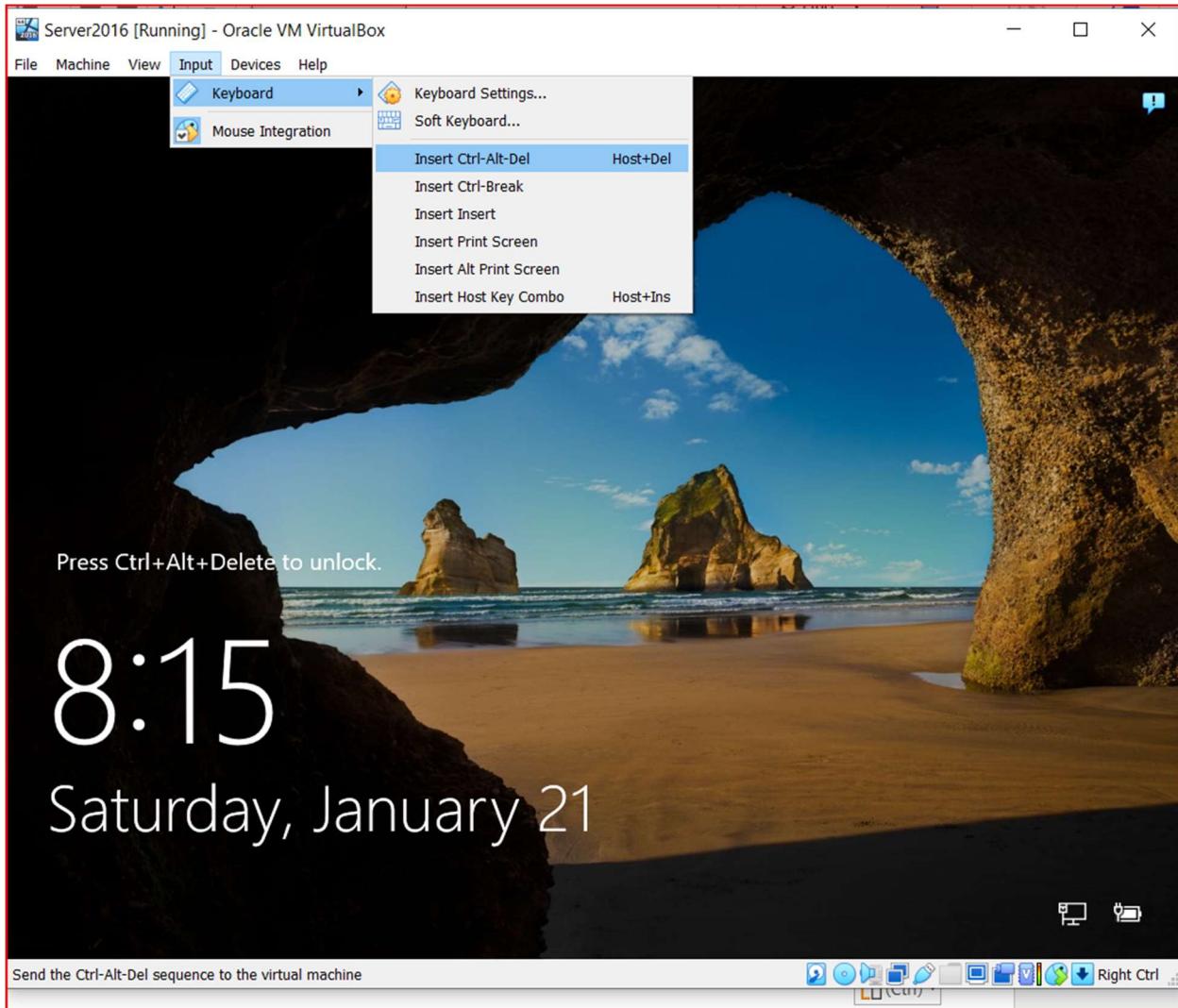
Next> Accept the software license agreement.

Next> Select **Custom**.

Next> Create an account/strong password.

LAB WORK 2

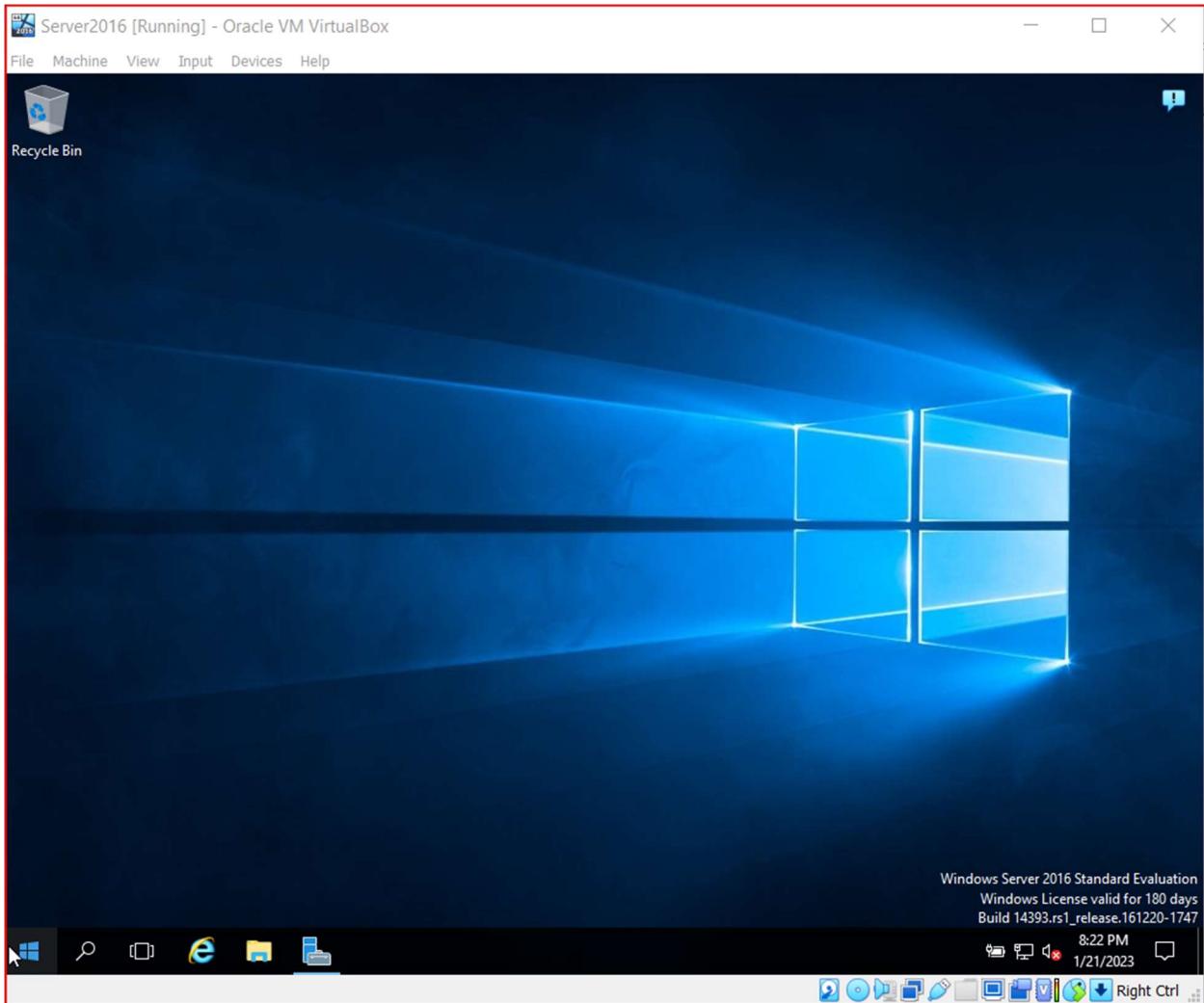
Install Windows Server 2016 on VirtualBox



Insert password for default built-in administrator account.

LAB WORK 2

Install Windows Server 2016 on VirtualBox



Windows Server 2016 desktop.

LAB WORK 2 COMPLETED

LAB WORK 3

Install Active Directory on Windows Server 2016

LAB WORK 3

Install Active Directory on Windows Server 2016

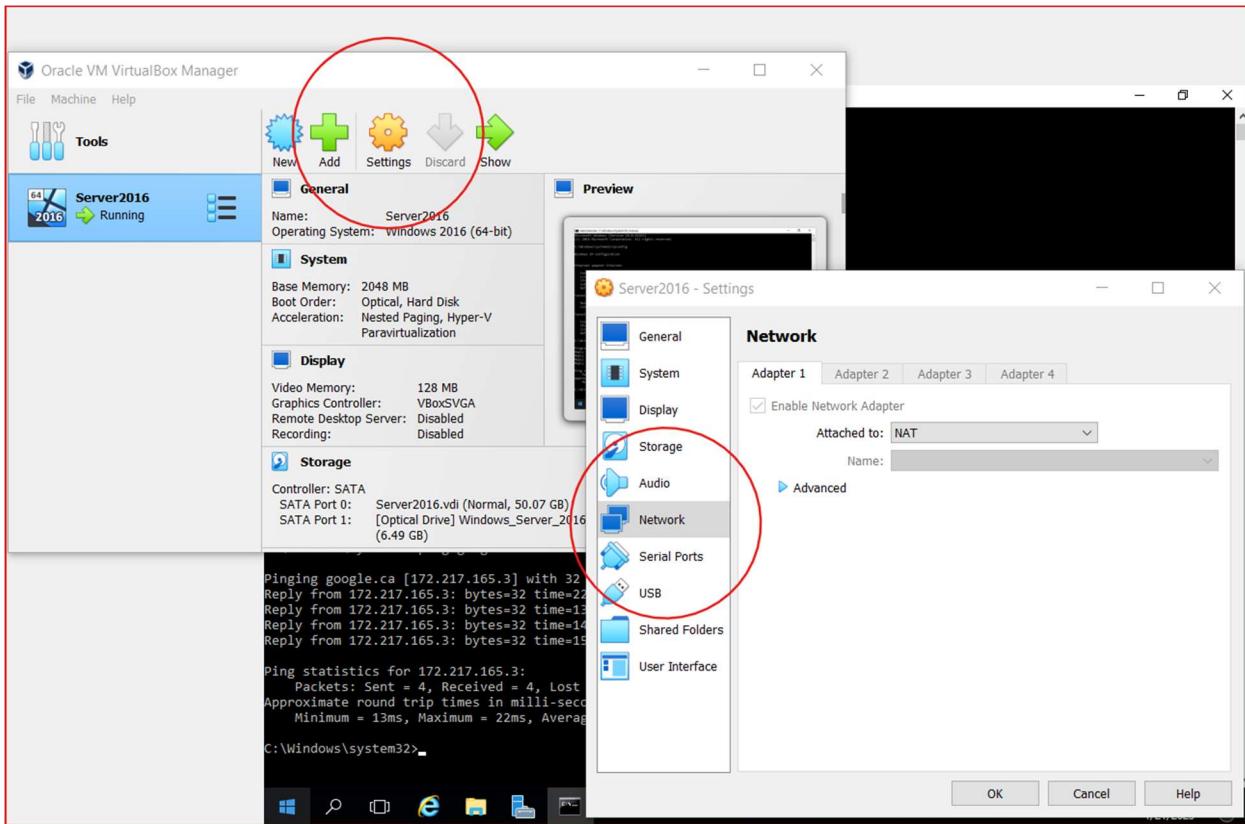
Prepare the environment before the installation process of Active Directory Domain Controller (*AD DC)

- ✓ Configure static IP address.
- ✓ Change PC name, reboot the system.
- ✓ Install Active Directory Domain Service (*AD DS) by using Server Manager
- ✓ Add Users

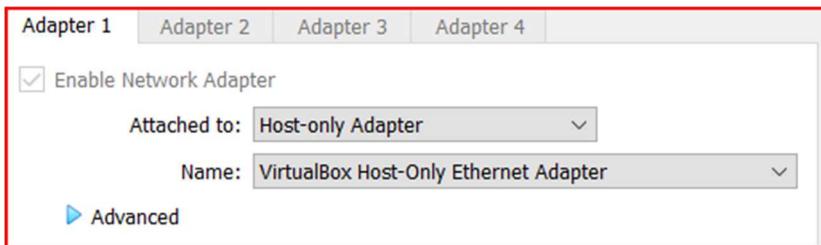
LAB WORK 3

Install Active Directory on Windows Server 2016

Static IP address.

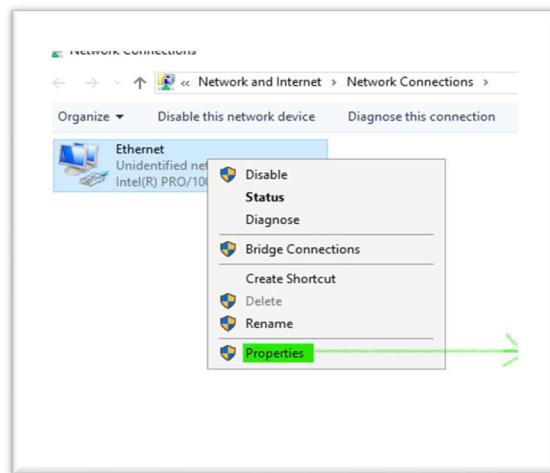
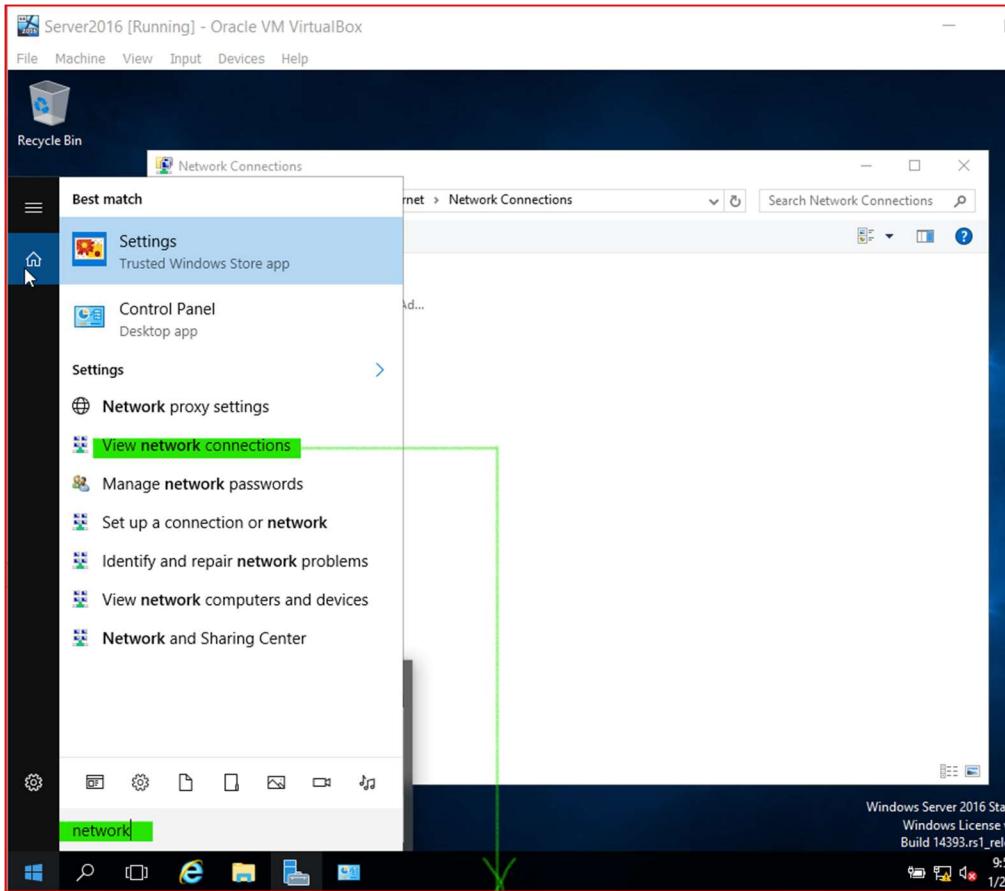


VirtualBox>Settings>Network>Adapter 1>Host-only Adapter>OK.



LAB WORK 3

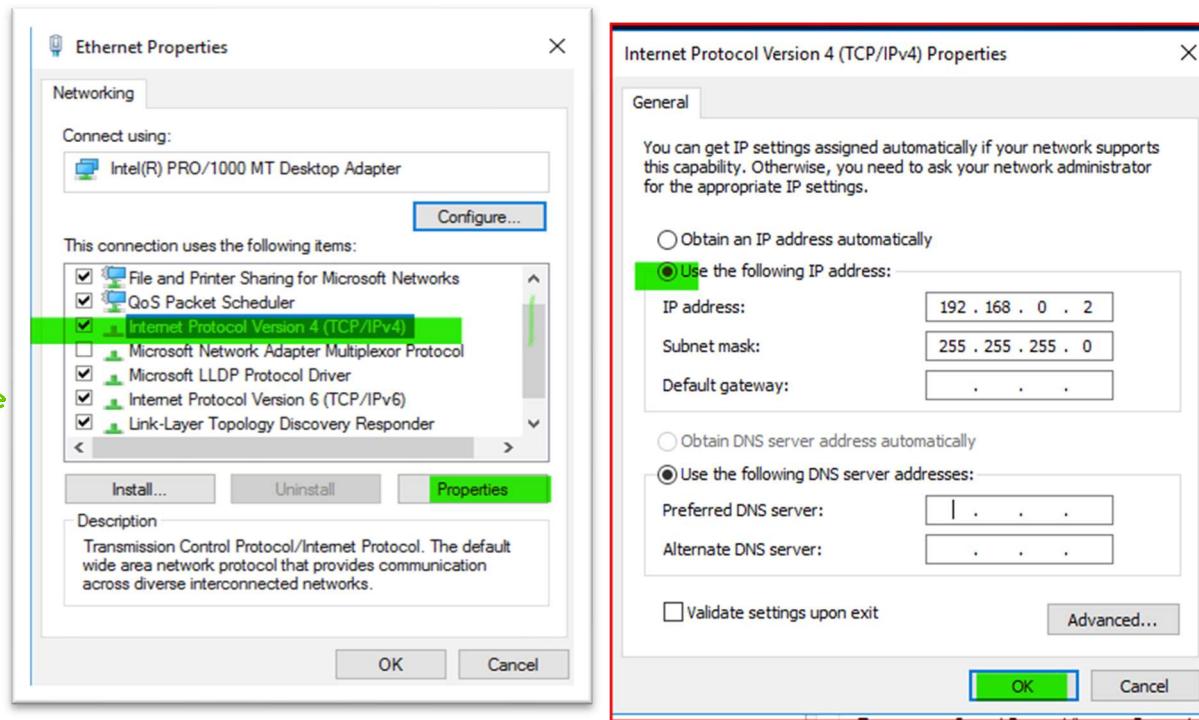
Install Active Directory on Windows Server 2016



Start>View network connections>Ethernet>Property>Internet Protocol Version 4(TCP/IPv4)>Properties

LAB WORK 3

Install Active Directory on Windows Server 2016

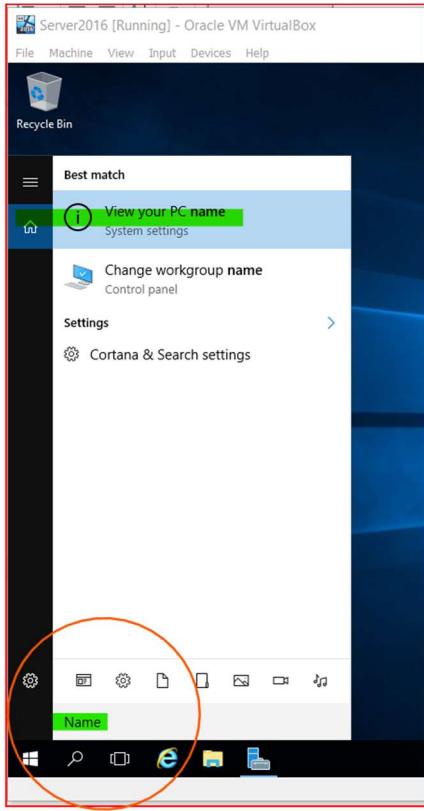


Set Static IP address **192.168.0.2**

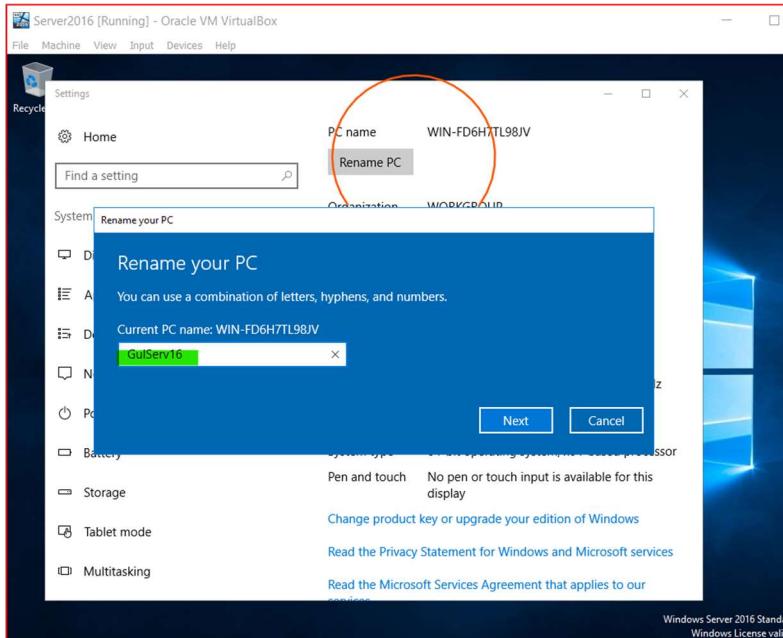
LAB WORK 3

Install Active Directory on Windows Server 2016

Rename PC



Click on **Start** button, type in **Name>View your PC Name**



Click **Rename PC/Restart Now**

LAB WORK 3

Install Active Directory on Windows Server 2016

Install Active Directory

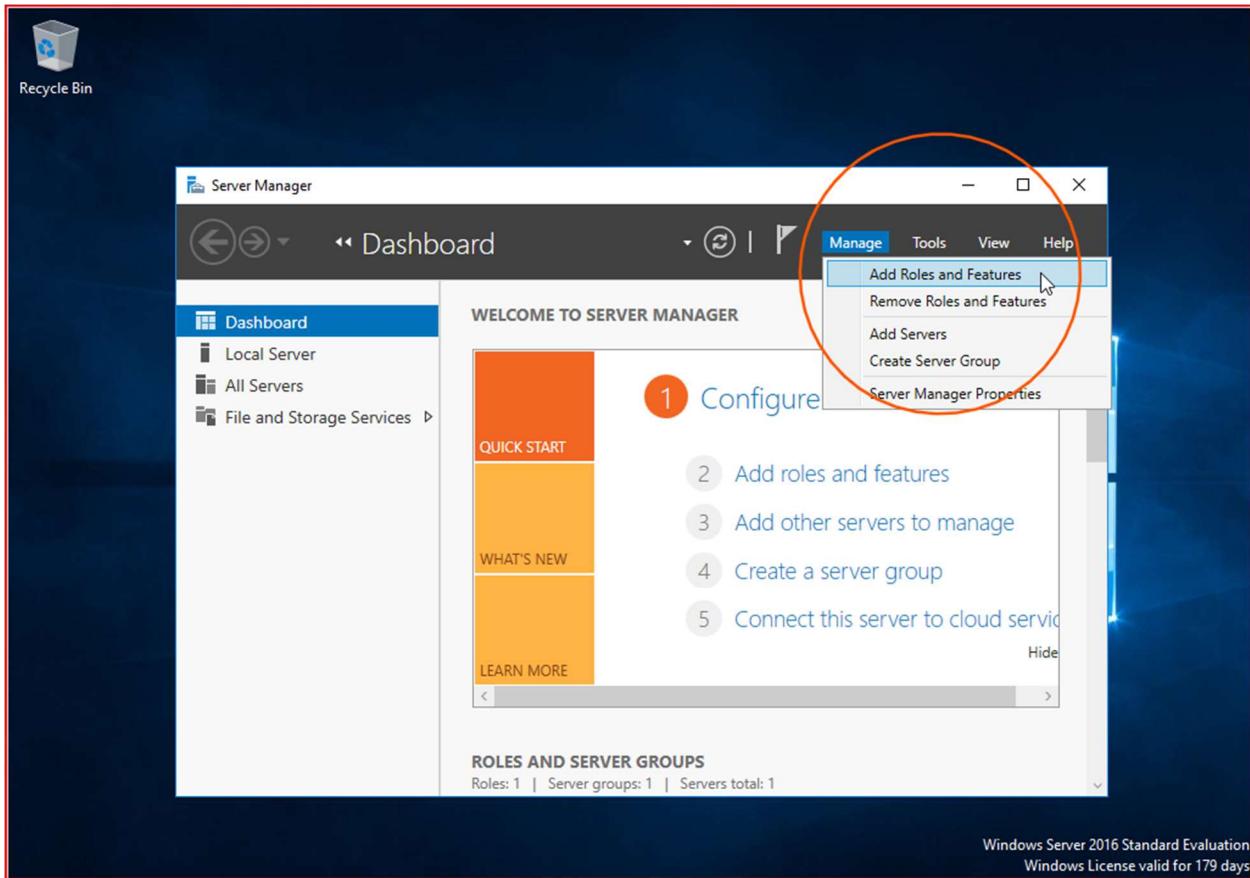
Follow the link to learn how to install AD DS by using Server Manager:

https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100-#BKMK_GUI

The screenshot shows a Microsoft Learn article page. The URL in the address bar is https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100-#BKMK_GUI. The page title is "Install Active Directory Domain Services (Level 100)". The left sidebar contains a navigation tree with topics like "Directory Child or tree Domain", "Install a Windows Server 2012 Active Directory Read-Only Domain Controller (RODC)", and "Demoting Domain Controllers". The main content area describes the steps to install AD DS in Windows Server 2012 using various methods, including "Adprep.exe", "Windows PowerShell", "Server Manager", and "Graphical User Interface". A sidebar on the right lists "In this article" sections such as "Credential requirements to run Adprep.exe and install Active Directory Domain Services", "Installing AD DS by Using Windows PowerShell", and "Performing a Staged RODC Installation using the Graphical User Interface".

LAB WORK 3

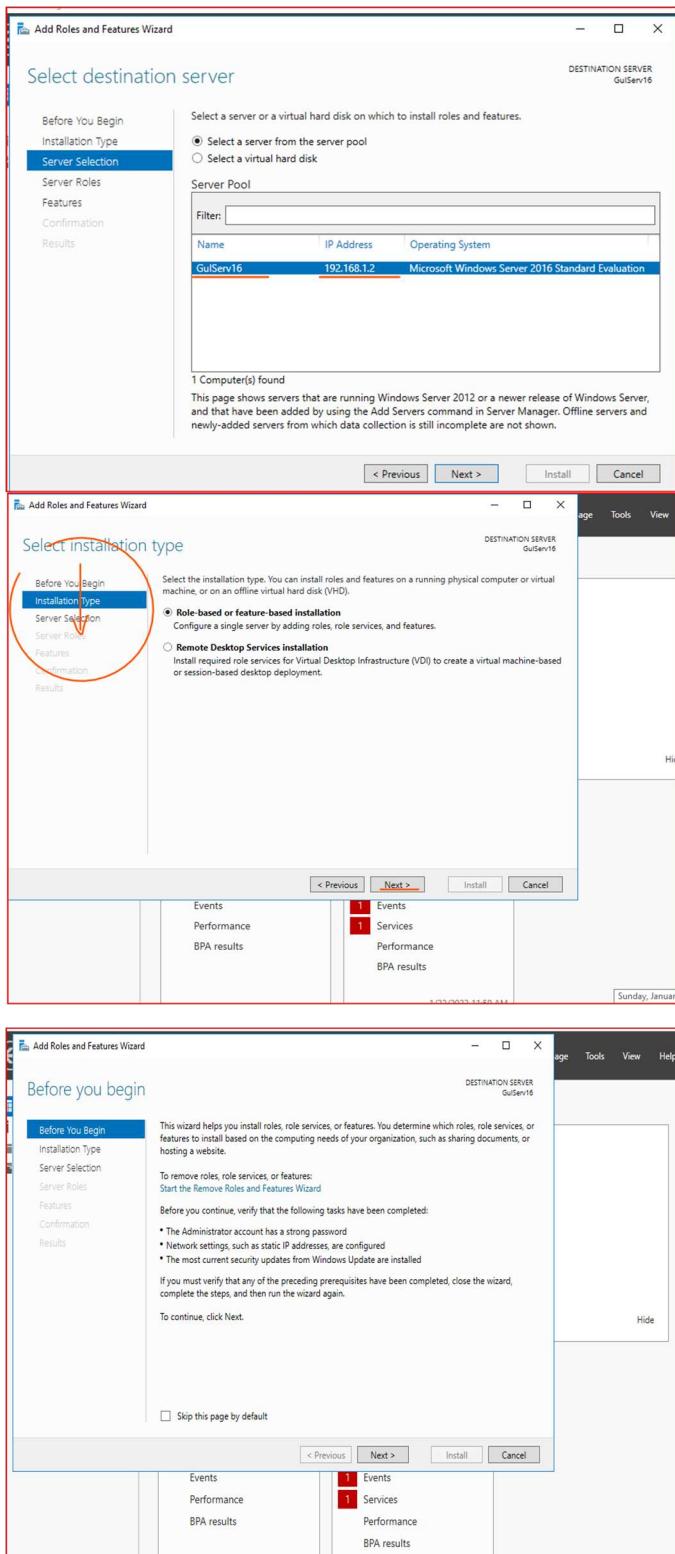
Install Active Directory on Windows Server 2016



In Server Manager, click **Manage** and click **Add Roles and Features** to start the Add Roles Wizard.

LAB WORK 3

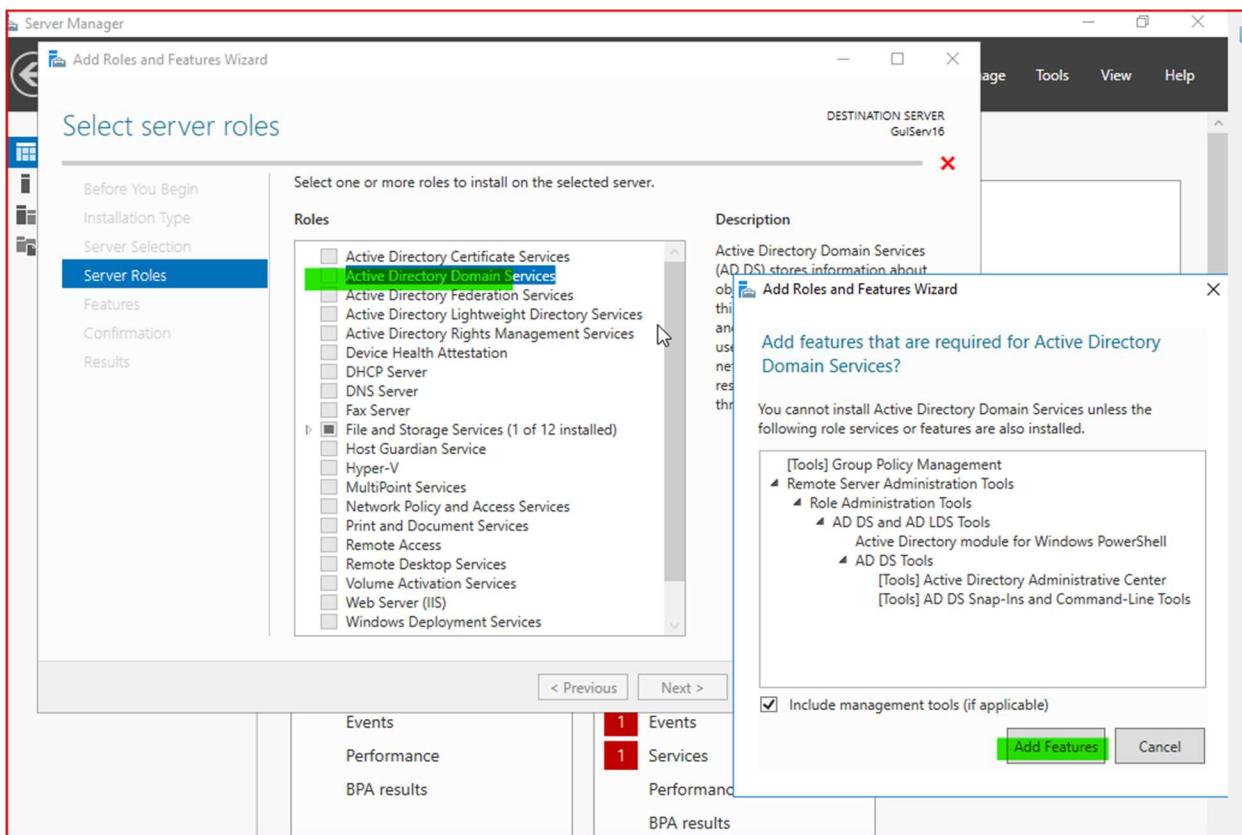
Install Active Directory on Windows Server 2016



Click **Next>**

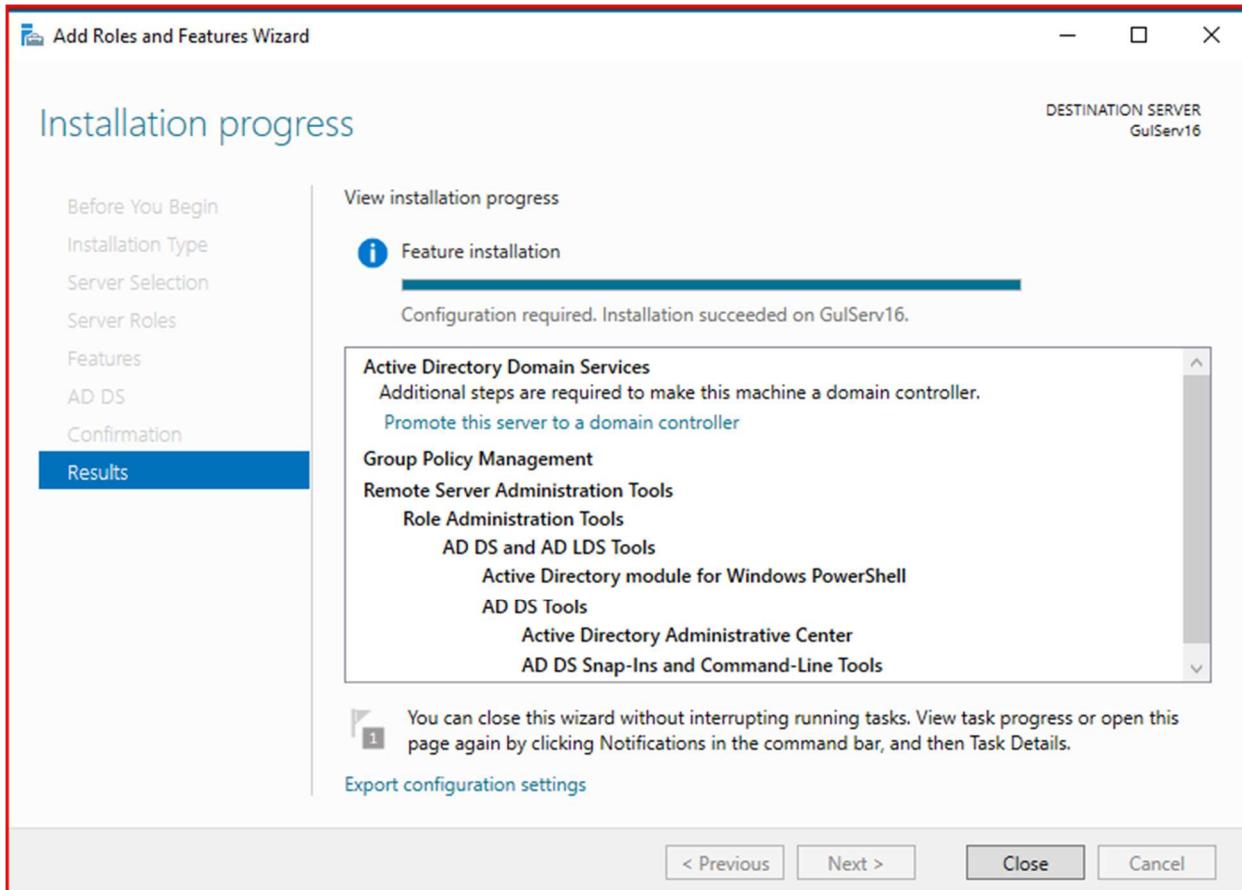
LAB WORK 3

Install Active Directory on Windows Server 2016



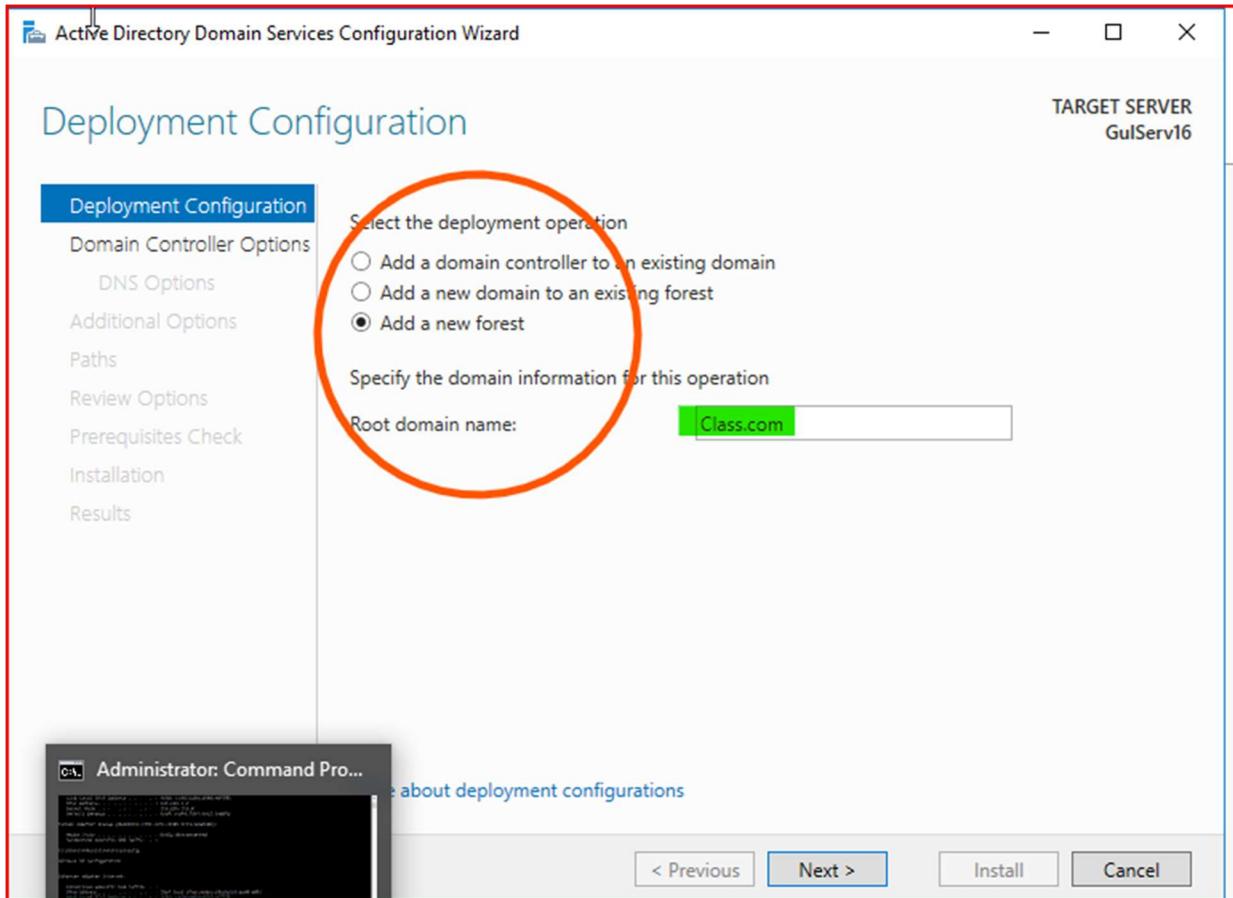
Click **AD DS**> pop-up **Add Features**> **Next**> **.NET Framework**> **Next**> It will prompt to install DNS. Click **Next**> **Install**>

LAB WORK 3



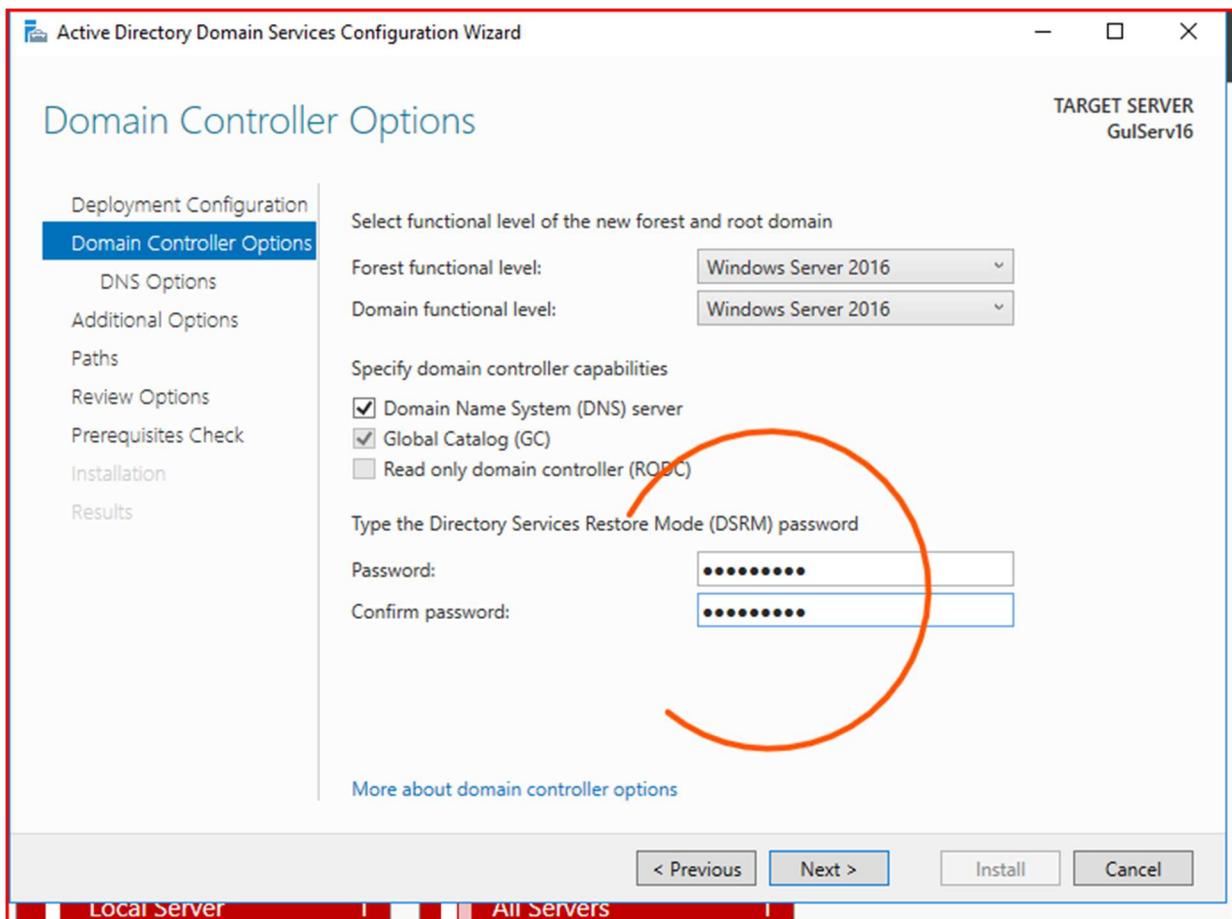
Manager is promoting **this server to a domain controller**. Double click to accept.

LAB WORK 3



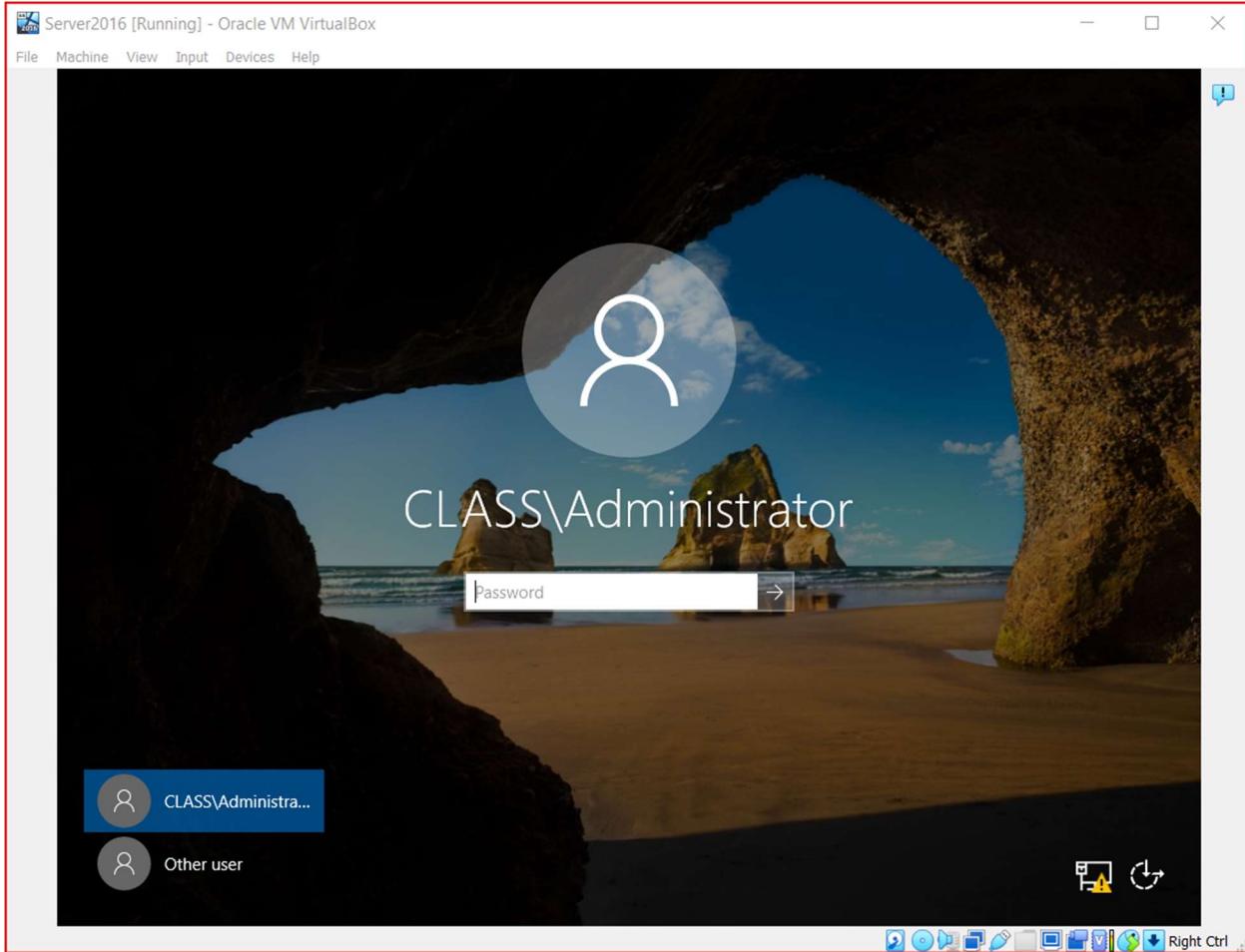
Enter domain **Class.com**

LAB WORK 3



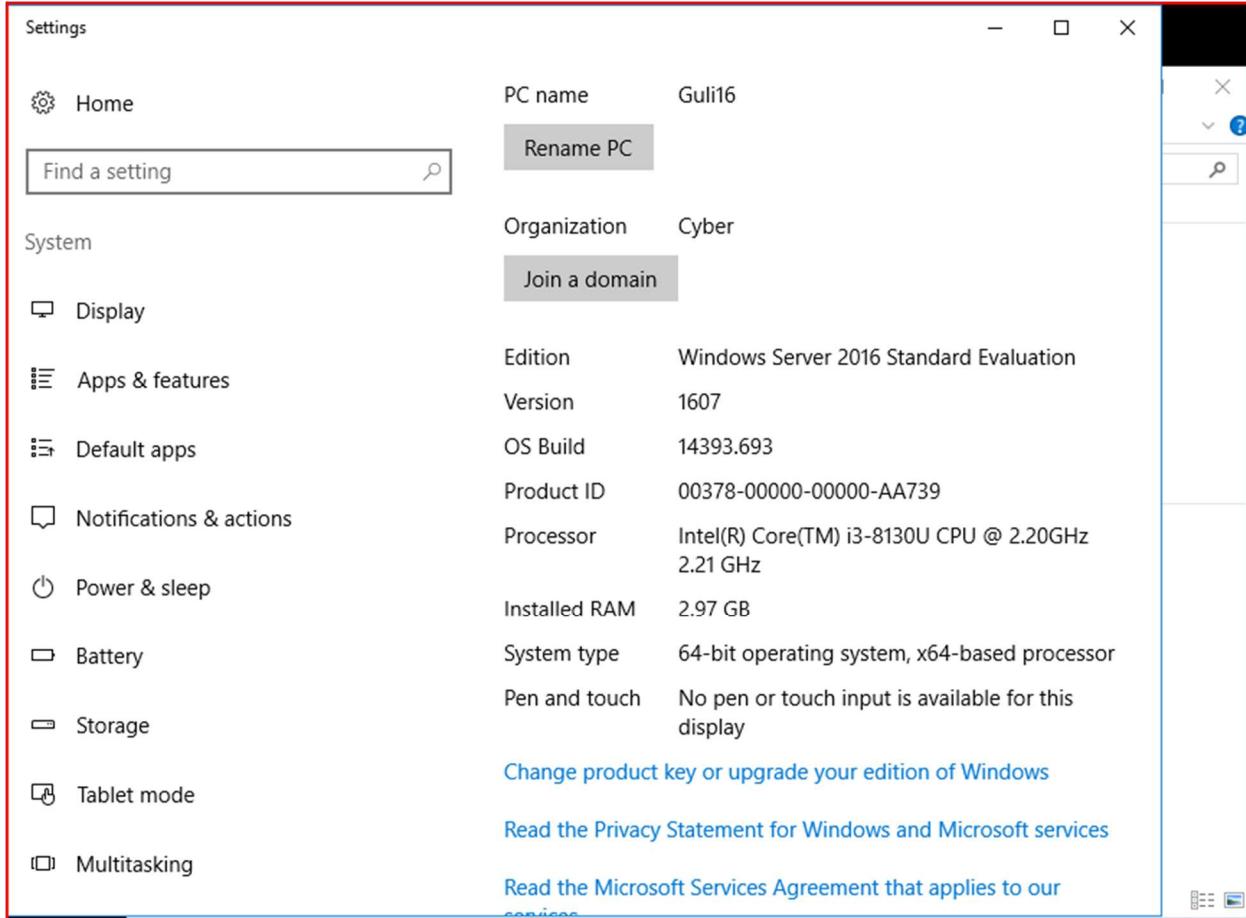
Leave default configuration for future options by clicking **Next > Install**, until installation is finished, and the system starts **reboot**.

LAB WORK 3



AD DC installed successfully.

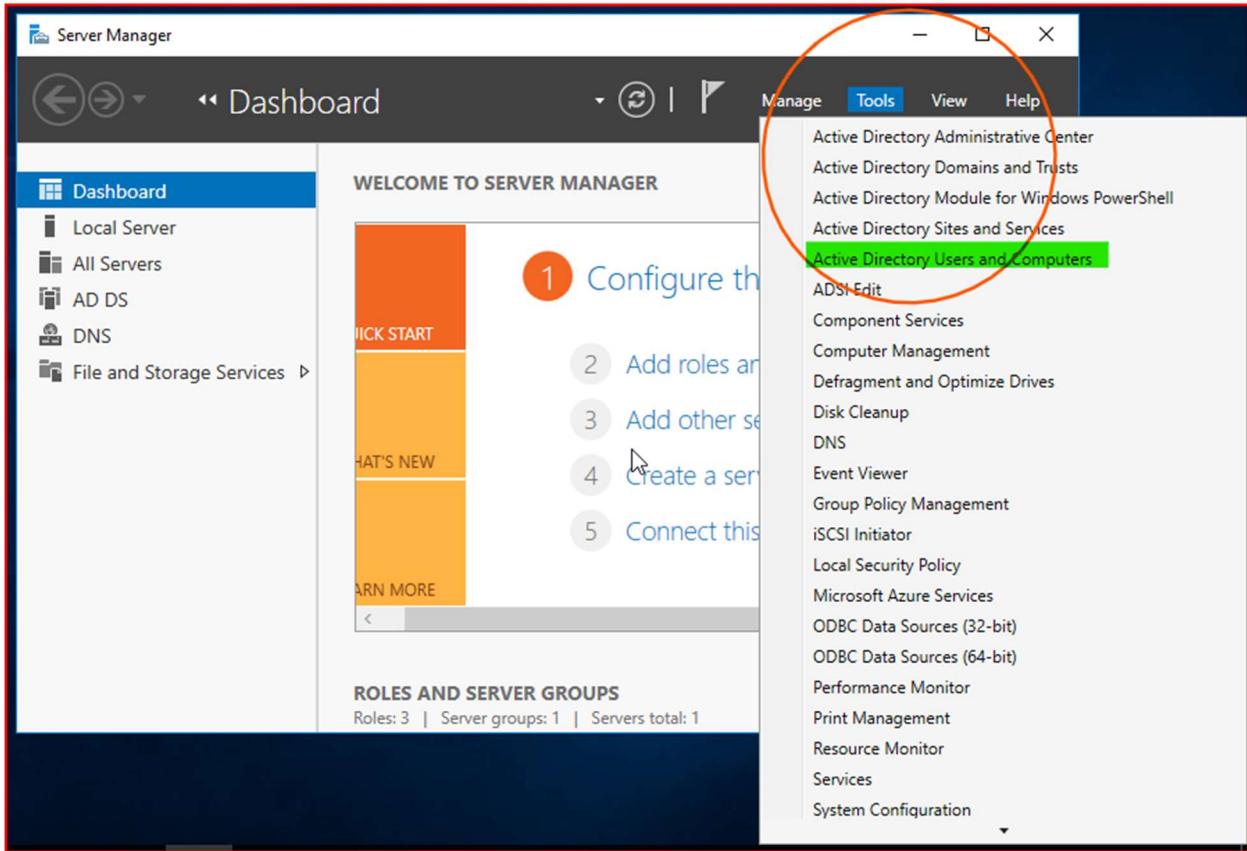
LAB WORK 3



The latest version of Server 2016.

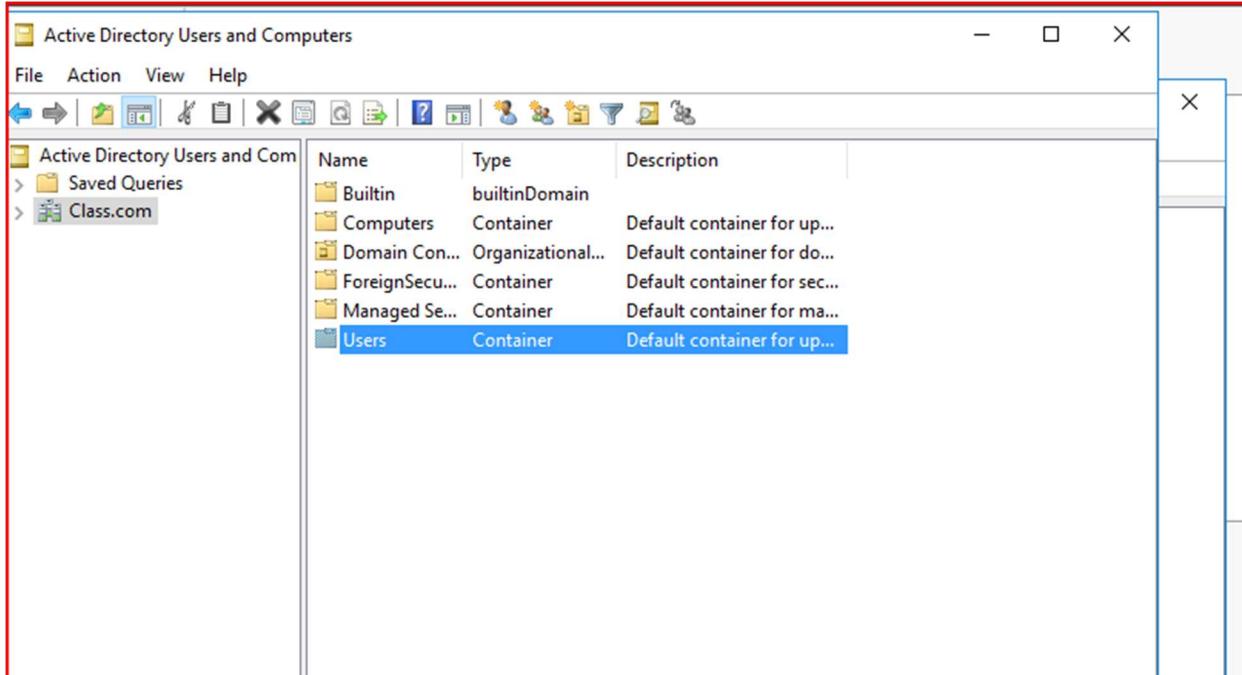
LAB WORK 3

Create Users



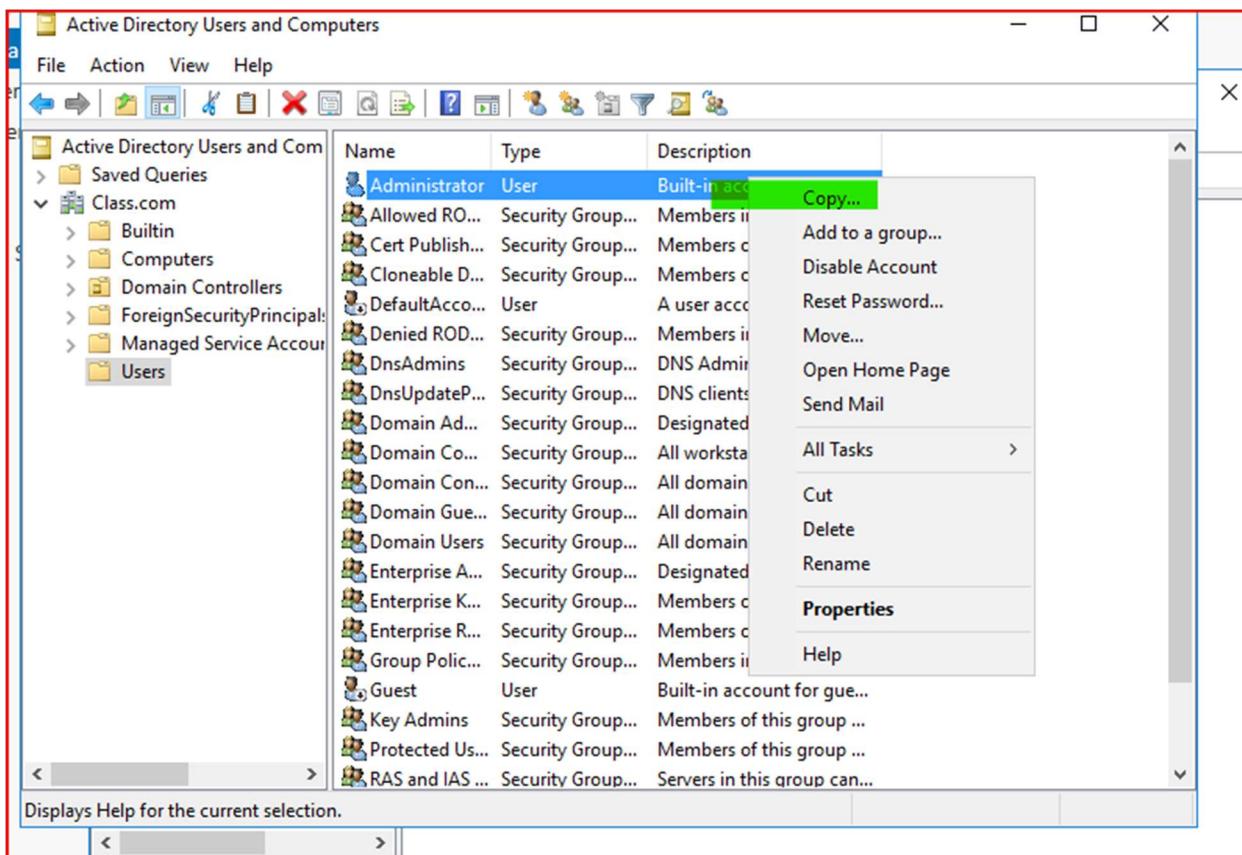
Under “Tools” on the Server Manager open “Active Directory Users and Computers”

LAB WORK 3



The screenshot shows the 'Active Directory Users and Computers' window. The left pane displays a tree view of the directory structure under 'Class.com'. The 'Users' container is selected and highlighted with a blue border. The right pane is a grid view showing the following data:

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational...	Default container for do...
ForeignSecu...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
Users	Container	Default container for up...



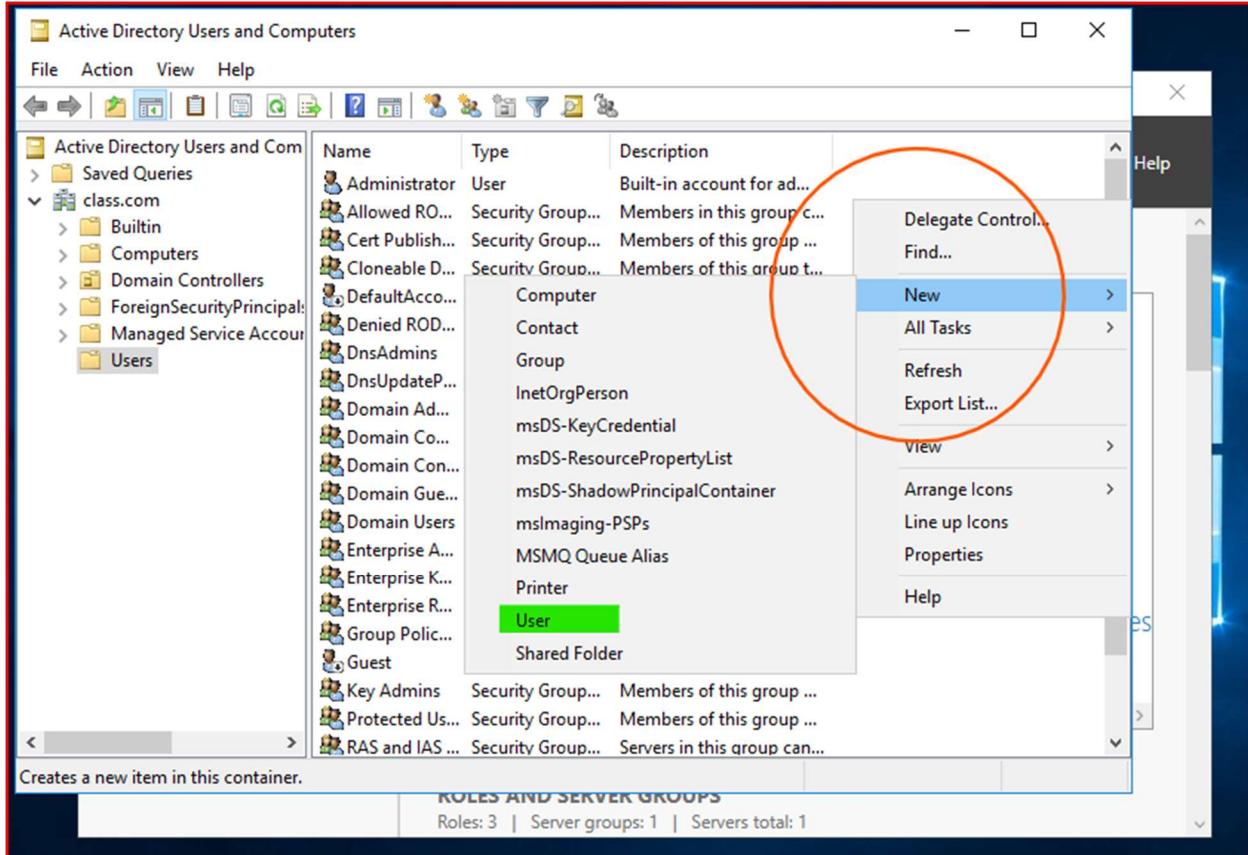
The screenshot shows the 'Active Directory Users and Computers' window with the 'Administrator' user selected. A context menu is open over the 'Administrator' row. The menu items include:

- Copy...
- Add to a group...
- Disable Account
- Reset Password...
- Move...
- Open Home Page
- Send Mail
- All Tasks >
- Cut
- Delete
- Rename
- Properties**
- Help

A tooltip at the bottom of the window says: 'Displays Help for the current selection.'

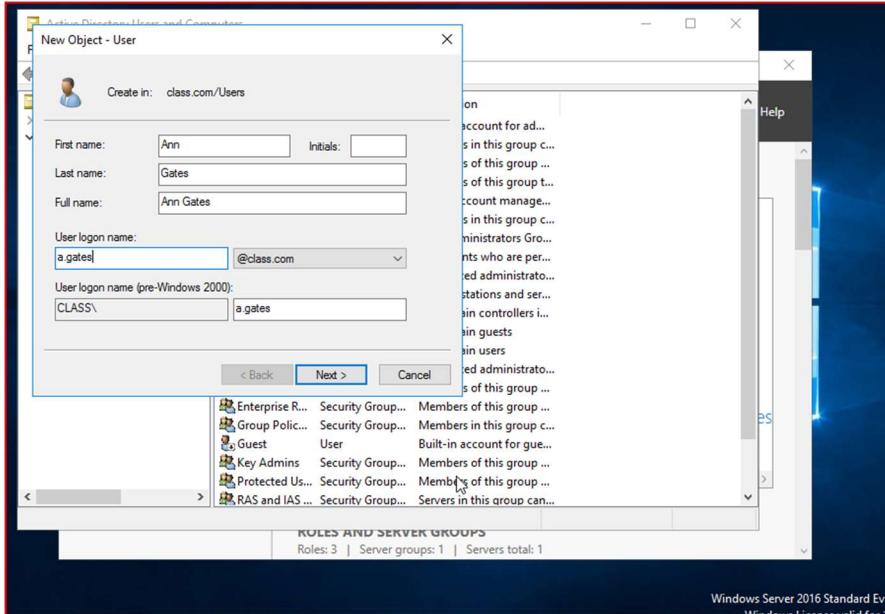
If you want to create a new user with administrator properties (or with any other group policy) right click on the user and “**Copy**”

LAB WORK 3

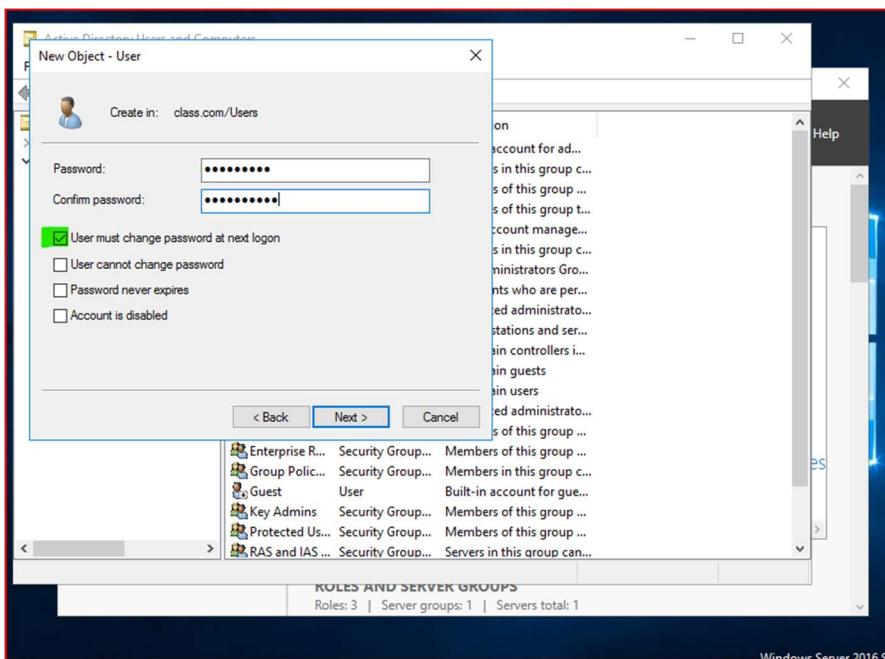


Or right click>New>User

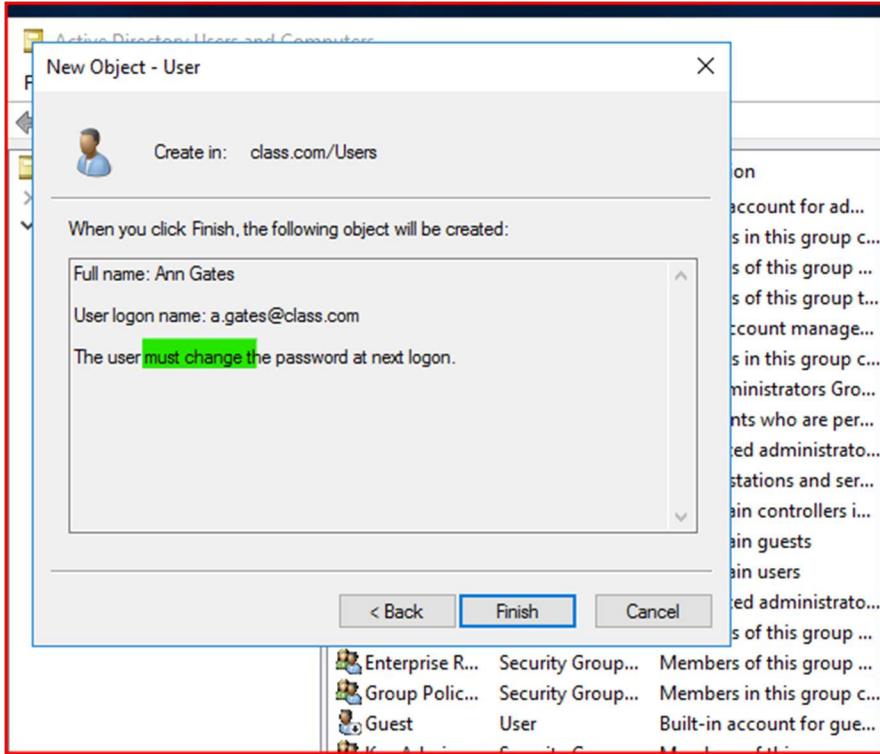
LAB WORK 3



Give it name and create a password.



LAB WORK 3



"Finish" adding Users

LAB WORK 3 COMPLETED

LAB WORK 4
Join Domain Controller

LAB WORK 4

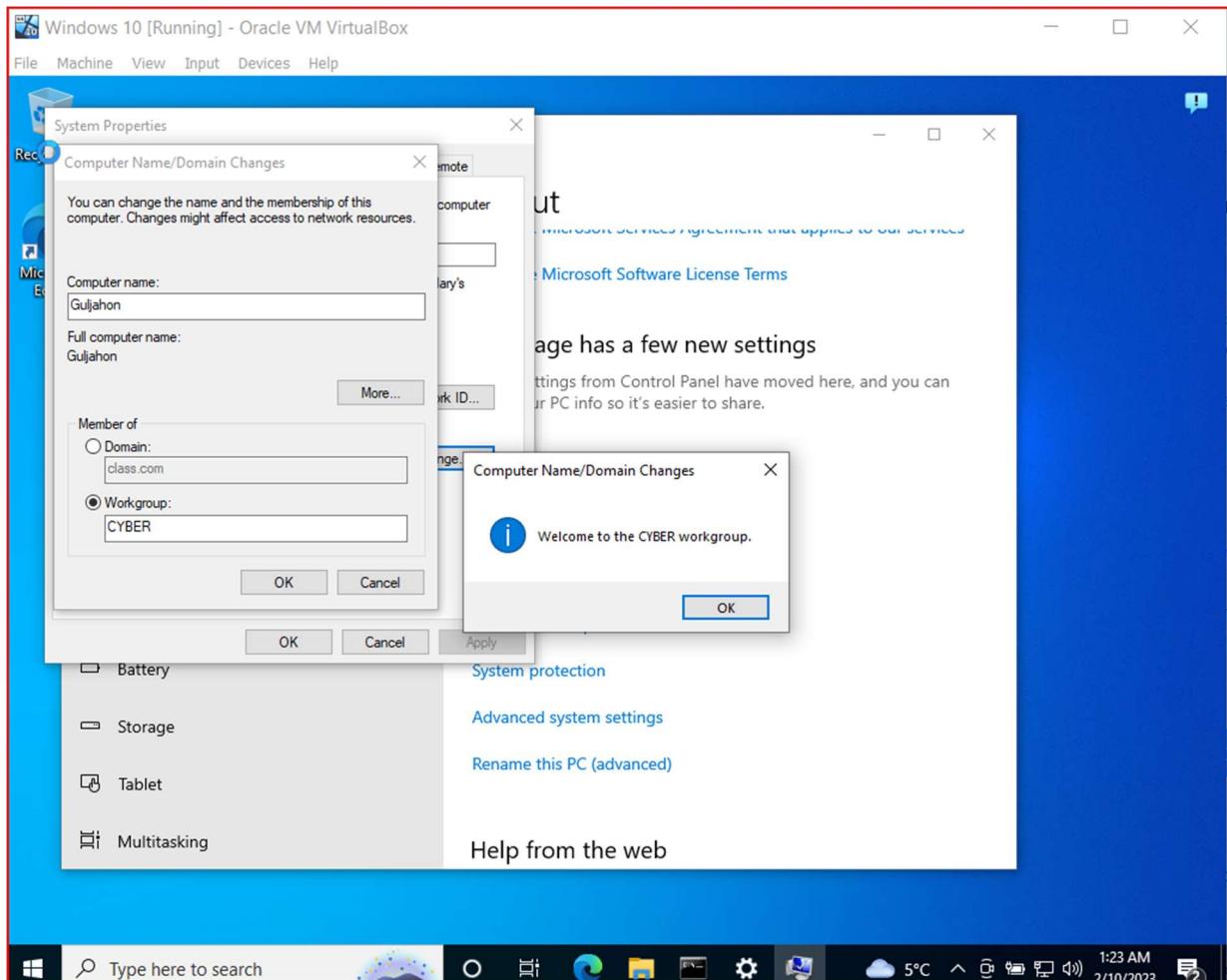
Join Domain Controller

- ✓ Configure machines Adapters to “Host-only” mode.
- ✓ Give machines static IP address.
- ✓ Join Windows 10 client to the domain.

After **LAB WORK 4** I faced some problems with:

- Joining Domain and connecting client to the Server.
- Troubleshooting took more than 4 weeks.
- The main problem was related to **misconfiguration on Active Directory** and my device's low hard disk and memory.
- I built several virtual machines from scratch, connected client to the server and my machines continued crashing or corrupting files.

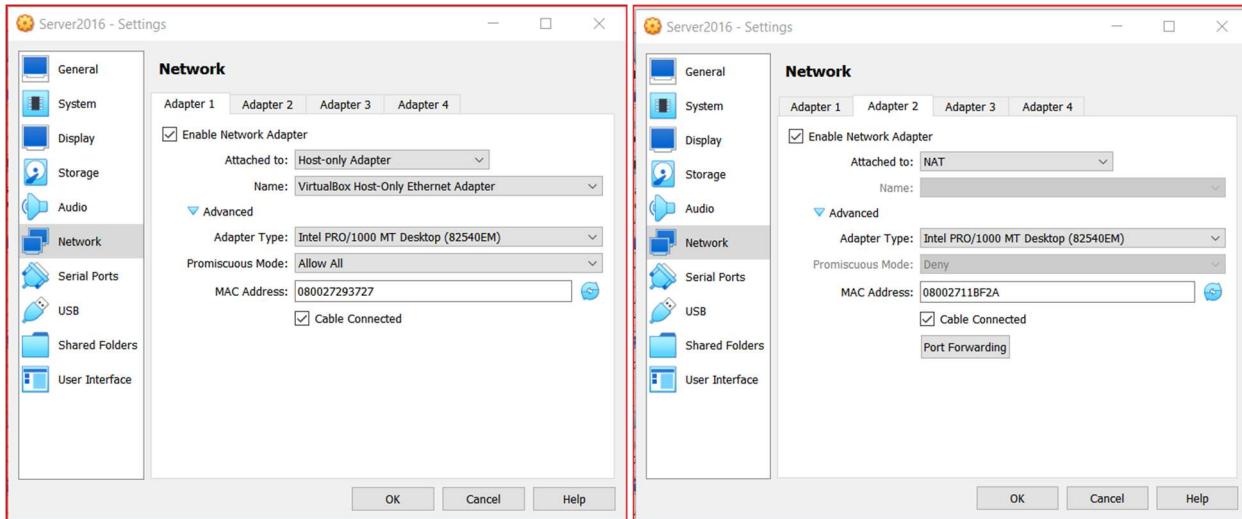
Below you will see the final screenshots of successfully joining domain controller.



LAB WORK 4

Join Domain Controller

✓ Windows Server 2016



Windows 2016 server's Network configuration.

The screenshot shows a Windows Server 2016 [Running] - Oracle VM VirtualBox window with an Administrator: Command Prompt. The command `ipconfig` is run, displaying network configuration details for several adapters:

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

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::e02c:8a4c:d01:7657%14
  IPv4 Address. . . . . : 192.168.0.15
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Ethernet adapter Ethernet 2:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::6c1d:ea89:35dc:efb7%12
  IPv4 Address. . . . . : 192.168.0.5
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Tunnel adapter isatap.{C4BFD718-49B5-48A6-8200-6ECA08663907}:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Tunnel adapter Reusable ISATAP Interface {22040D20-9743-441E-A127-55E96566BD73}:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

C:\Users\Administrator>whoami
cyber\administrator

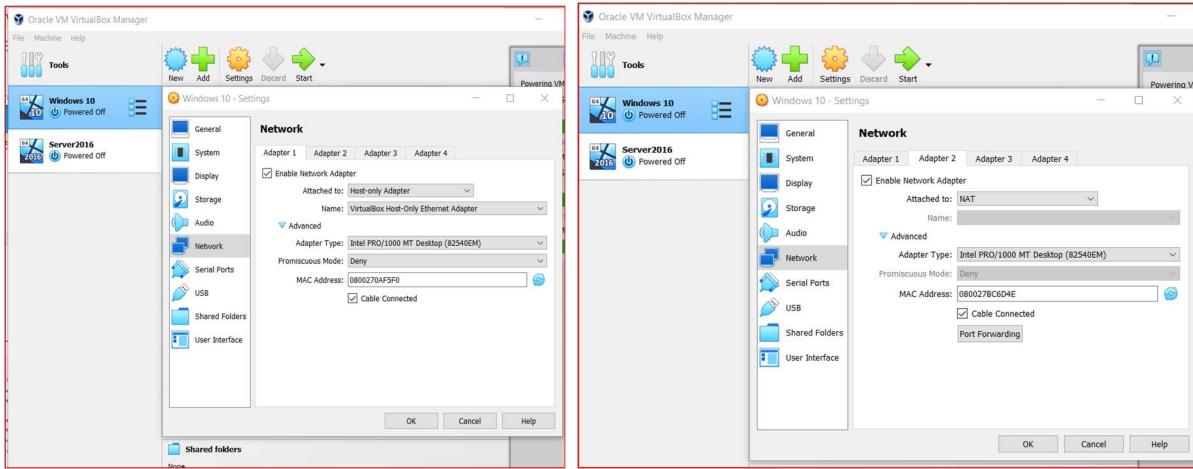
C:\Users\Administrator>
```

Static IP address assigned.

LAB WORK 4

Join Domain Controller

✓ Windows 10 client



```
cmd Command Prompt
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::3550:b200:a8d6:6045%13
  IPv4 Address . . . . . : 192.168.0.25
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Ethernet adapter Ethernet 2:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::5db0:7ec4:6a8b:87f7%3
  IPv4 Address . . . . . : 10.0.3.15
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.0.3.2

C:\Users\User>whoami
guljahon\user

C:\Users\User>ping class.com

Pinging class.com [23.185.0.2] with 32 bytes of data:
Reply from 23.185.0.2: bytes=32 time=47ms TTL=57
Reply from 23.185.0.2: bytes=32 time=10ms TTL=57
Reply from 23.185.0.2: bytes=32 time=11ms TTL=57
Reply from 23.185.0.2: bytes=32 time=8ms TTL=57

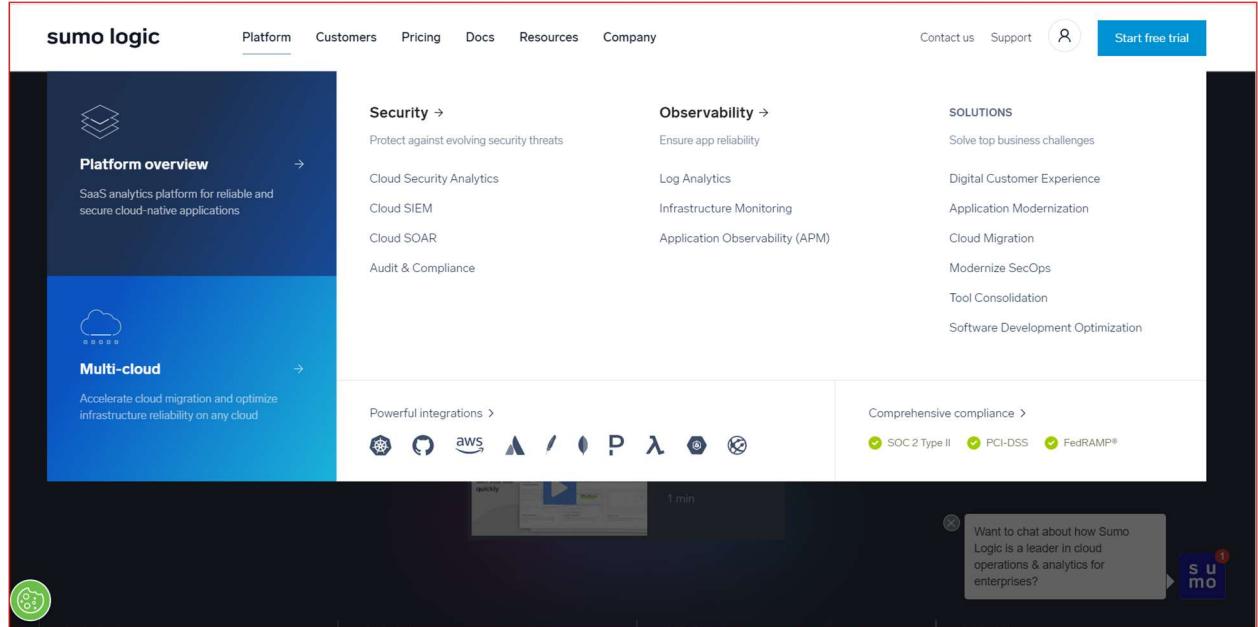
Ping statistics for 23.185.0.2:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 47ms, Average = 19ms

C:\Users\User>
```

Static IP assigned.

SUMOLOGIC

- ✓ Authorization
- ✓ Installation
- ✓ Data Parsing
- ✓ Save the Search
- ✓ Configure an Email Alert



LAB WORK 5

Sumologic

✓ Authorization

Follow the link to register for free trial:
<https://www.sumologic.com>



Or:

The image shows two views of the Sumologic platform. On the left, a dark-themed landing page highlights 'Cloud Monitoring, Log Management, SIEM' and 'Quickly detect application and security incidents'. It includes a 'Start free trial' button and a 'Logs Metrics Traces Events' navigation bar. On the right, a detailed application monitoring dashboard for 'the coffee-bar app' displays various metrics like 'Avg. Latency [ms]', 'Avg. Requests [per sec]', and 'Avg. Errors Percentage [per sec]'. A specific chart for 'Latency [ms]' shows several data series with distinct peaks. A small callout bubble in the bottom right corner asks if there are any questions before getting started, with a 'Human' button nearby.

LAB WORK 5

Sumologic

✓ Installation

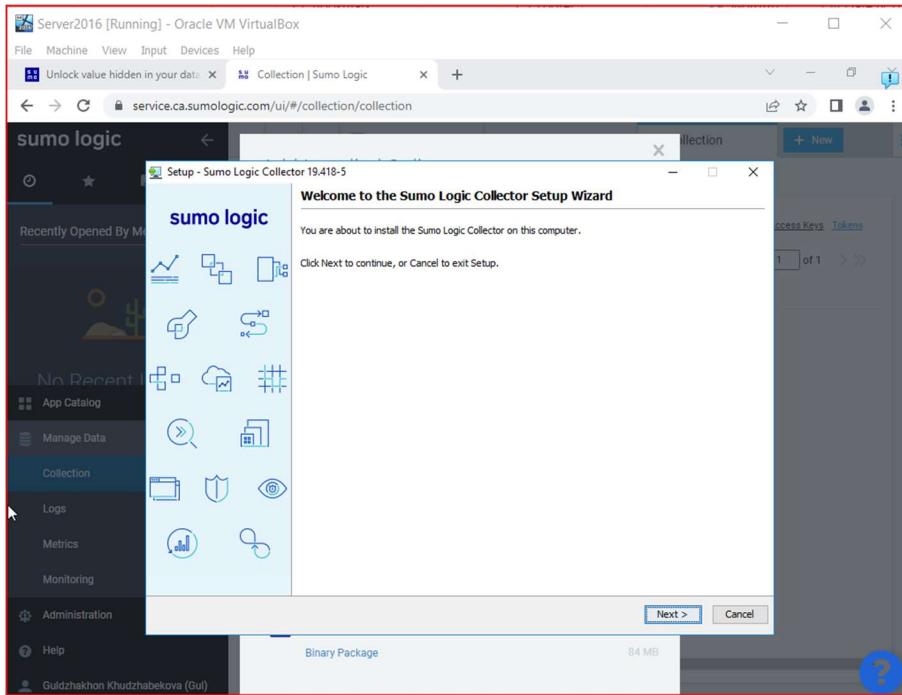
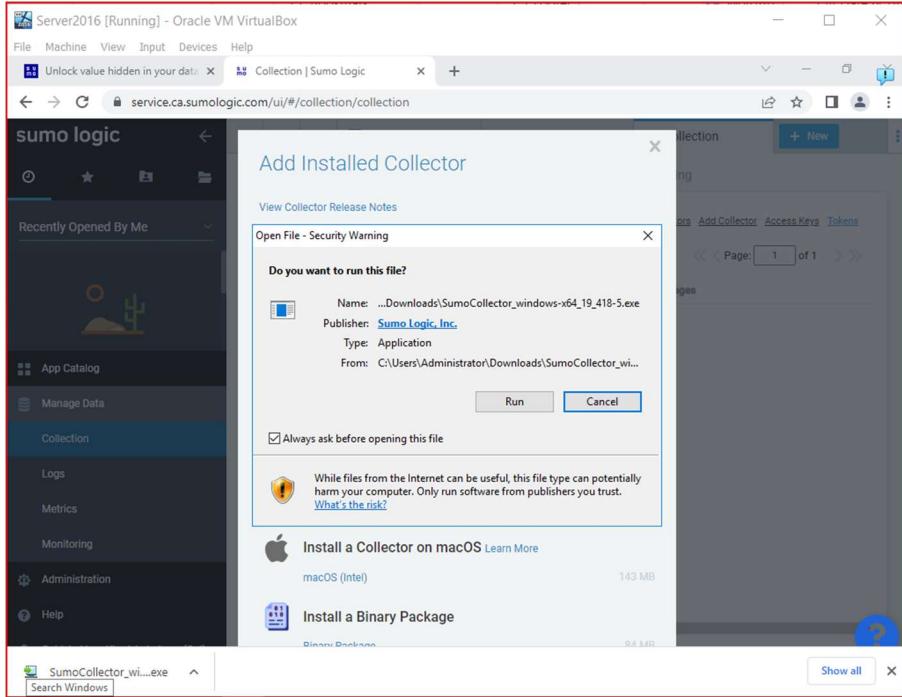
The screenshot shows the Sumologic interface with a red box highlighting the 'Collection' tab in the navigation bar. A modal window titled 'Select Collector Type' is open. It contains two sections: 'Installed Agent' and 'Hosted Collector'. Under 'Installed Agent', there are two options: 'Sumo Logic Distribution for OpenTelemetry Collector' and 'Installed Collector'. The 'Installed Collector' option is described as a Java agent that receives logs and metrics from its sources and then encrypts, compresses, and sends the data to the Sumo service. Under 'Hosted Collector', there is one option: 'Hosted Collector', which is described as Select to set up a Collector in the Sumo Logic Cloud.

The screenshot shows the Sumologic interface with a red box highlighting the 'Collection' tab in the navigation bar. A modal window titled 'Add Installed Collector' is open. It displays the following information:

- View Collector Release Notes
- Version 19.418 Build 5
- Install a Collector on Linux
 - Linux (64-bit/x86_64/amd64) - 94 MB
 - Linux Debian (64-bit/x86_64/amd64) - 134 MB
 - Linux RPM (64-bit/x86_64/amd64) - 134 MB
 - Linux Arm (64-bit/aarch64) - 77 MB
 - Linux RPM (64-bit/aarch64) - 126 MB
 - Linux Debian (64-bit/arm64) - 126 MB
- Install a Collector on Windows
 - Windows (32-bit) - 132 MB
 - Windows (64-bit) - 133 MB
- Install a Collector on macOS
 - macOS (Intel) - 143 MB
- Install a Binary Package
 - Binary Package - 84 MB

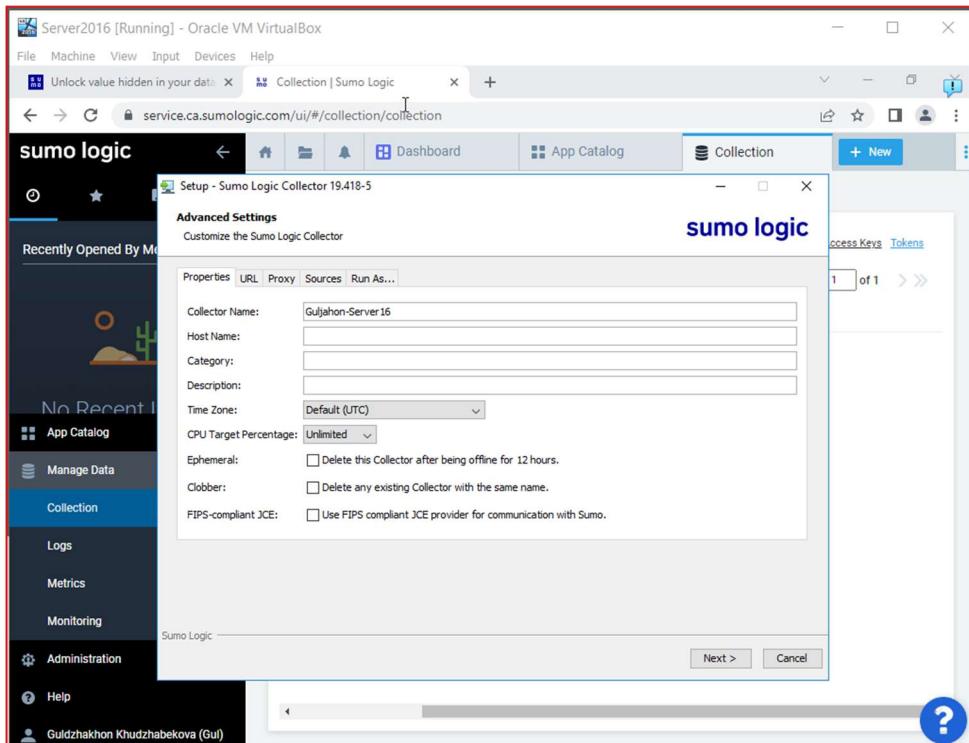
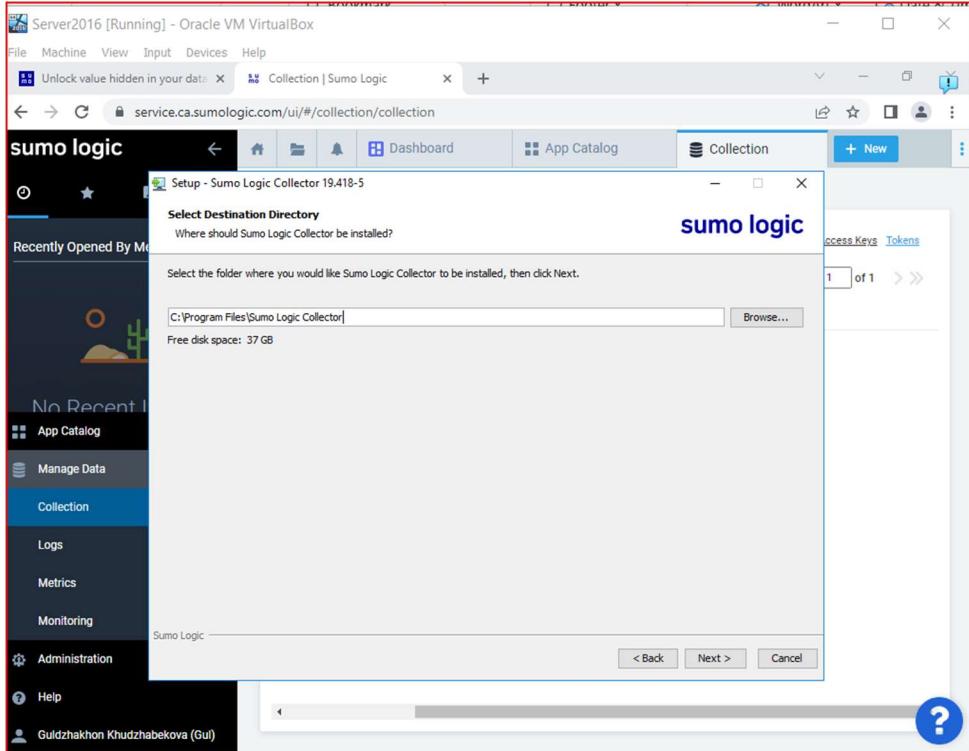
LAB WORK 5

Sumologic



LAB WORK 5

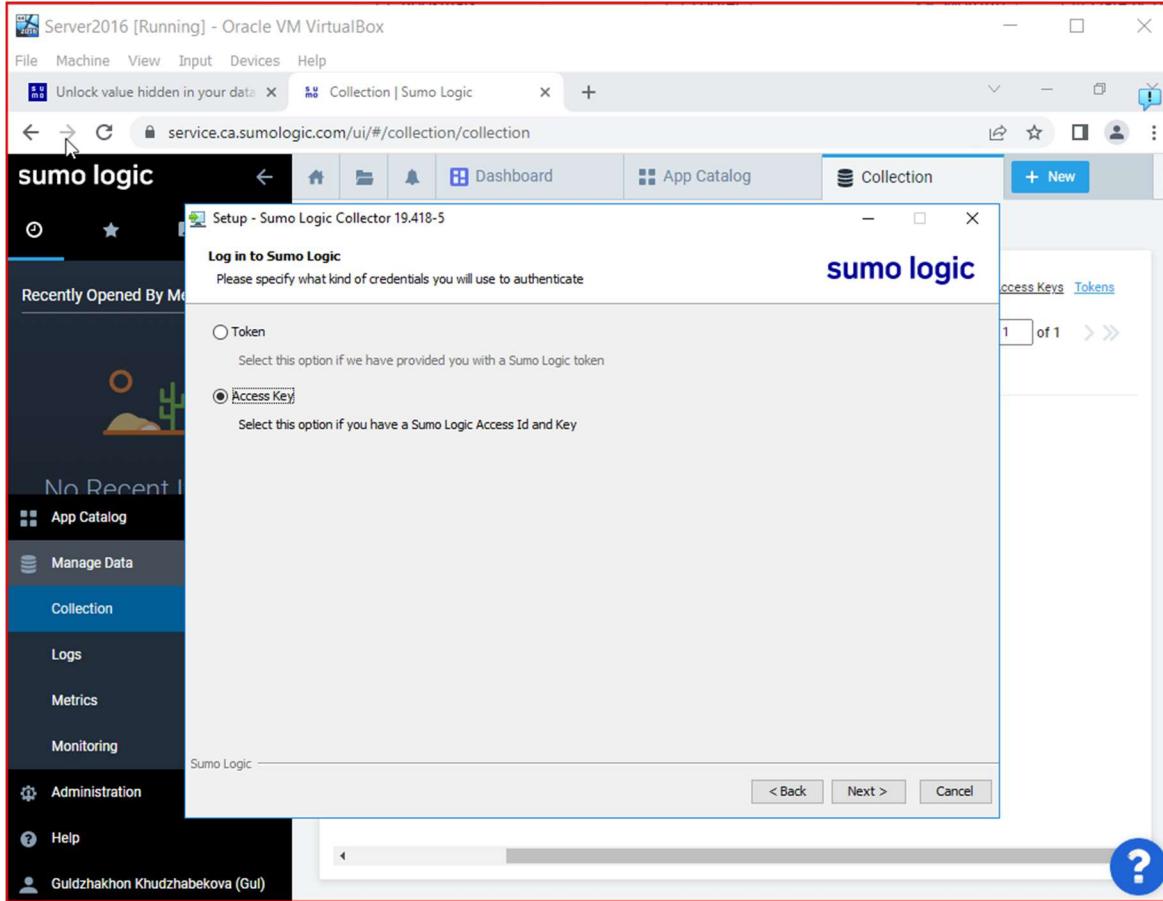
Sumologic



Next>Advanced options>

LAB WORK 5

Sumologic



Access Key>Next>

Activate MFA using Google Authenticator

LAB WORK 5

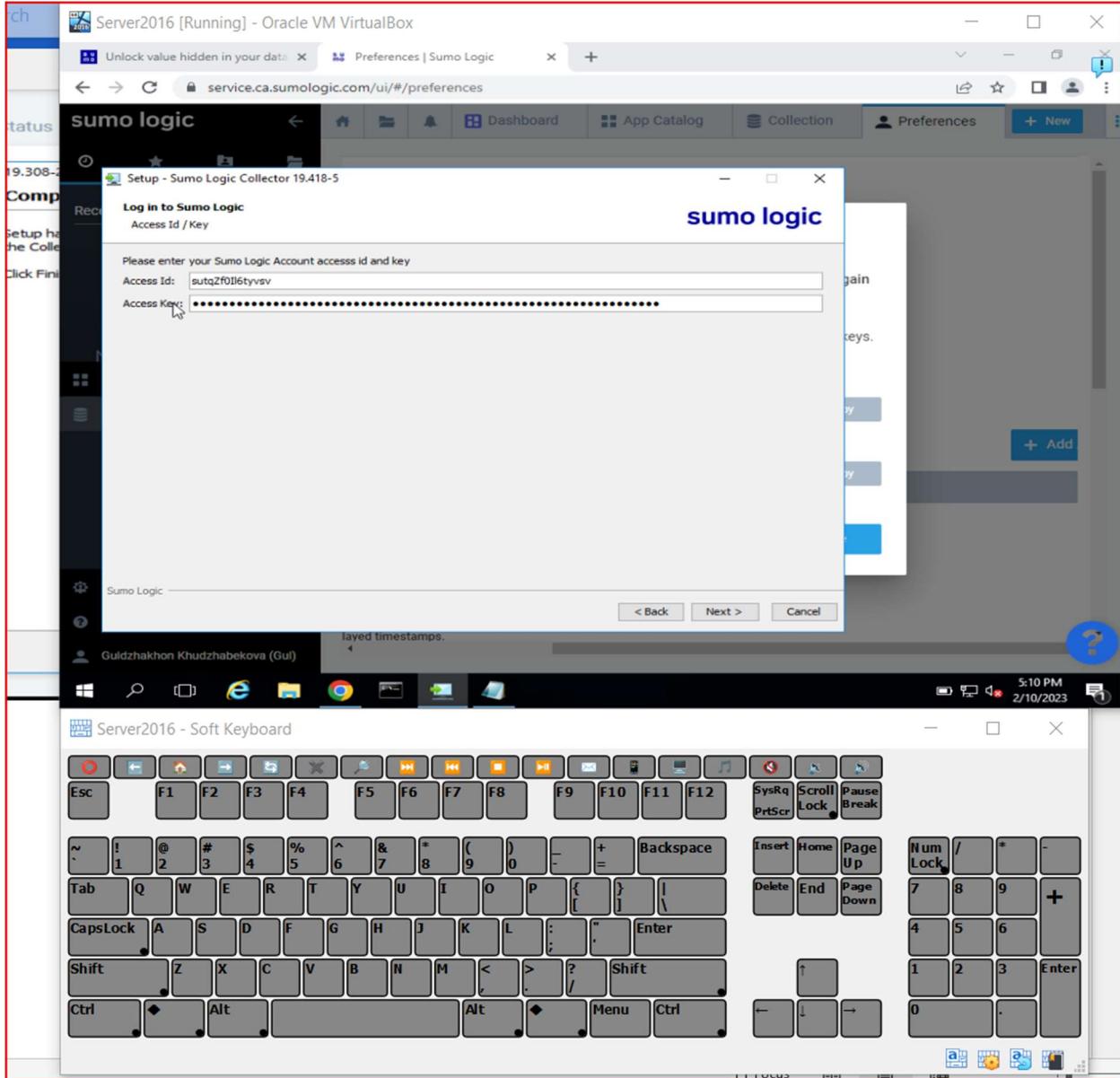
Sumologic

The screenshot shows the Sumologic interface with a red border around the main content area. At the top, there are two tabs: 'Unlock value hidden in your data' and 'Preferences | Sumo Logic'. Below the tabs, the URL is service.ca.sumologic.com/ui/#/preferences. The navigation bar includes icons for Home, File, Bell, Dashboard, App Catalog, Collection, Preferences (which is selected), and a New button. On the left, a sidebar titled 'sumo logic' lists 'Recently Opened By Me' with a cactus icon, followed by 'No Recent Items'. The sidebar also contains links for App Catalog, Manage Data, Collection, Logs, Metrics, Monitoring, Administration, Help, and a user profile for Guldzhakon Khudzhabekova (Gul). The main content area is titled 'Access Keys' and displays a message: 'Unlock value hidden in your data. Click the Add button to generate your first key.' A blue '+ Add' button is visible. Below this, there is a table header with columns: ACCESS ID, CREATED, and STATUS. A note at the bottom says 'Your access keys are displayed timestamps.' and a question mark icon is in the bottom right corner.

+Add access key

LAB WORK 5

Sumologic



LAB WORK 5

Sumologic

The image contains two screenshots of the Sumologic web interface, both titled "Collection | Sumo Logic".

Screenshot 1: This screenshot shows the "Collection" tab selected. The left sidebar lists "Recently Opened By Me" dashboards: Windows - Overview, Windows - Login Status, Windows - Event Errors, Windows - Default, and Windows - Application. The main area displays a table of collectors. The table has columns: Name, Health, Type, Status, Source Category, Sources, Last Hour, and Messages. One row is visible: "Guli16" (Healthy, Installed, Windows 2016). A blue question mark icon is in the bottom right corner.

Name	Health	Type	Status	Source Category	Sources	Last Hour	Messages
Guli16	Healthy	Installed		Windows 2016	None	None	

Screenshot 2: This screenshot also shows the "Collection" tab selected. The left sidebar includes "Manage Data" under "Collection", "Logs", "Metrics", and "Monitoring". The main area shows the same collector table as Screenshot 1. An orange circle highlights the "Page: 1" dropdown in the top navigation bar. A blue question mark icon is in the bottom right corner.

Name	Health	Type	Status	Source Category	Sources	Last Hour	Messages
Guljahan Server 2...	Healthy	Installed		Windows 2016	None	None	

Add Source.

LAB WORK 5

Sumologic

The screenshots illustrate the process of configuring a Windows Event Log source in Sumologic:

- Screenshot 1:** Shows the "Collection" tab selected in the navigation bar. The "Windows Event Log" icon is highlighted and circled in red.
- Screenshot 2:** The "Ingest Budgets" tab is selected. The "Windows Event Log" configuration page is displayed, showing fields for Name (Server 2016), Description (Windows Log Event From Server 2016), and Windows hosts (left blank). A FAQ panel on the right provides information about remote Windows event collection.
- Screenshot 3:** The "Collector" tab is selected. The "Windows Event Log" configuration page is shown, detailing the event format (Collect using legacy format), event types (Security checked), and event IDs. The "Processing Rules for Logs" section is visible at the bottom.

The same procedure for Windows 10 workstation data (Security, Application and Systems) and Windows 10 performance data (CPU, Logical Disk, Physical Disk, Memory, Network).

LAB WORK 5

Sumologic

✓ Data Parsing

The screenshot shows the Sumologic interface with a search results page. A log entry is selected, and a context menu is open over it. The menu options are:

- Expand Row
- Copy Selected Text
- Parse Selected Text
- Add selected text as AND
- Add selected text as AND NOT
- Add selected text as OR
- Add selected text as OR NOT

Right click>Parse Selected Text

LAB WORK 5

Sumologic

The screenshot shows the Sumologic interface with a red border around the central workspace. In the top left, there's a sidebar with 'RECENTLY OPENED DASHBOARDS' and 'RECENTLY RUN SEARCHES'. The main area has a title 'Parse Text' with the instruction 'Select the text to parse, then click the action popup.' Below this is a text input field containing 'EventCode = 4634;'. A yellow callout box points to the number '4634' with the text 'Click to extract this value'. To the right of the input field are 'Cancel' and 'Submit' buttons. At the bottom of the dialog, there's some event log data: 'RecordNumber = 9281; SourceName = "Microsoft-Windows-Security-Auditing"; TimeGenerated = "20230213100428.000000-000"; TimeWritten = "20230213100428.000000-000"; Type = "Audit Success"; EventType = 4;'. The background shows a dashboard with various metrics and a search bar.

Extract selected value.

Provide the Field Name (Event ID) and Submit.

LAB WORK 5

Sumologic

The screenshot shows the Sumologic search interface. On the left is a sidebar with navigation links like 'Recently Opened By Me' and 'RECENTLY RUN SEARCHES'. The main area has a search bar at the top with the query: '(_collector="Guljahon Server 2016") "EventCode = *" as EventID "EventCode = *" as EventID "EventCode =*;" as EventID'. Below the search bar is a histogram chart showing event counts over time from 1:00 AM to 5:00 AM. A red circle highlights the search bar area. The bottom half of the screen shows a table of event results. The first row has columns '#', 'Time', 'EventID', and 'Message'. The 'EventID' column shows the value '4634' for the first event. A red circle highlights this value. The 'Message' column displays a detailed log entry for event ID 4634, which is an Audit Success event. The log includes fields like Computer, EventCode, EventIdentifier, Logfile, RecordNumber, SourceName, TimeGenerated, TimeWritten, Type, EventType, Category, and CategoryString. At the bottom of the table, there are filters for Host, Name, and Category.

Event ID parsed.

The procedure is same for any Event ID parsing.

LAB WORK 5

Sumologic

✓ Save the Search

The figure consists of three vertically stacked screenshots of the Sumologic web interface.

Screenshot 1: Shows a search results page for a query involving EventCode. A context menu is open over a specific event log entry, with the "Save" option highlighted. An orange circle highlights the "Save As..." option in the menu.

Screenshot 2: Shows the "Save Item" dialog box. The "Name" field contains "Parsed Event code by EventID". The "Description (optional)" field is empty. The "QUERY" field displays the search query: `(((_collector="Guljahon Server 2016")) | parse "EventCode = *" as EventID)`. Below the query are fields for "Time range" (set to -6h), "Search By" (Receipt Time), and "Search Mode" (Auto Parse Mode). The "Location to save to" dropdown shows "All Folders" with a single item, "Personal", selected. At the bottom are "Cancel" and "Save" buttons. An orange circle highlights the "Save" button.

Screenshot 3: Shows the search results page again, but now the saved search "Parsed Event code by EventID" is visible in the left sidebar under the "Recently Opened By Me" section. An orange circle highlights the search entry in the sidebar.

The Search is saved under Personal Folder

LAB WORK 5

Sumologic

✓ Configure an Email Alert

Save Item

Name: Collector - Guljalon Server 2016

Description (optional)

QUERY: _collector="Guljalon Server 2016"

Time range: -15m

Location to save to:

Name	Description
Personal	My saved searches and dashboards

Schedule this search > Cancel Save

Collection>Collector >Schedule this search>Provide all details.

If the following condition is met

Alert condition: Greater than > Number of results: 0

Alert Type: Email

Send email on failure to search owner.

Recipients: gulia@cloud-it.biz, guljalon.kh.r@gmail.com

Email Subject: Search Alert: {{TriggerCondition}} found for {{SearchName}}

Include in email:

- Search Query
- Result Set
- Histogram
- Results as a CSV attachment (max 5MB or 1,000 results)

< Back Cancel Save

LAB WORK 5

Sumologic

Search Alert: More than 0 found for Collector - Guljahon Server 2016

SL Sumo Logic <service@sumologic.com>
To Guldzhakon Khudzhabekova; guljahon.kh.r@gmail.com

Collector - Guljahon Server 2016_2023-02-13T004600.000-0800.csv
119 KB

Saved Search	Collector - Guljahon Server 2016
Search String	_collector="Guljahon Server 2016"
Time Range	02/13/2023 03:30:00 AM EST to 02/13/2023 03:45:00 AM EST
Run Frequency	Every 15 minutes
Notification Threshold	More than 0
Run At	02/13/2023 03:47:56 AM EST
Scheduled By	Guldzhakon Khudzhabekova <gulia@cloud-it.biz>

Message Distribution (View results in Sumo Logic)

Result Set
Displaying 25 out of 70 or more results. Click [here](#) to view full results in Sumo Logic.

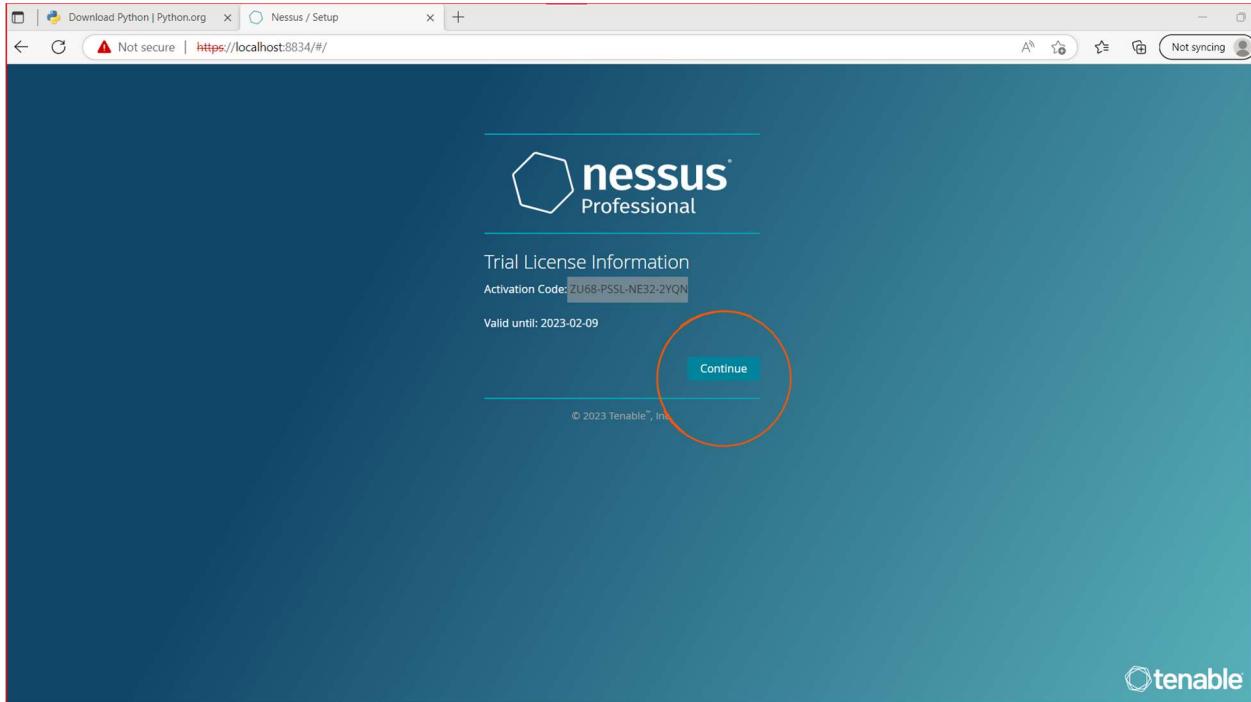
#	Time	Message
1	02/13/2023 06:44:45 AM EST	instance of Win32_NTLogEvent { Computer = "Guli16.class.com"; EventCode = 4634; EventIdentifier = 4634; LogFile = "Security"; RecordNumber = 10021; SourceName = "Microsoft-Windows-Security-Auditing"; TimeGenerated = "20230213114445.000000-000";

An alert was received as soon as new user was created.

LAB WORK 5 COMPLETED

NESSUS

- ✓ Deploy application
- ✓ Vulnerability screening
- ✓ How to read the Report

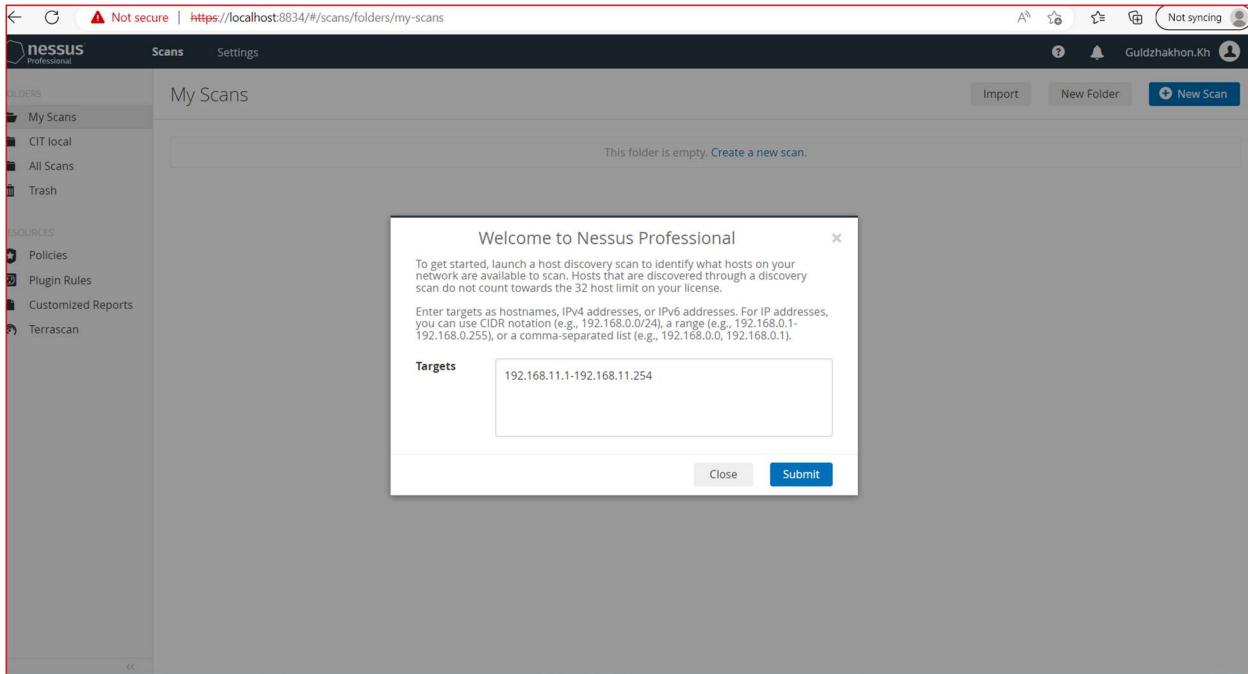


Guldzhakhon.Kh

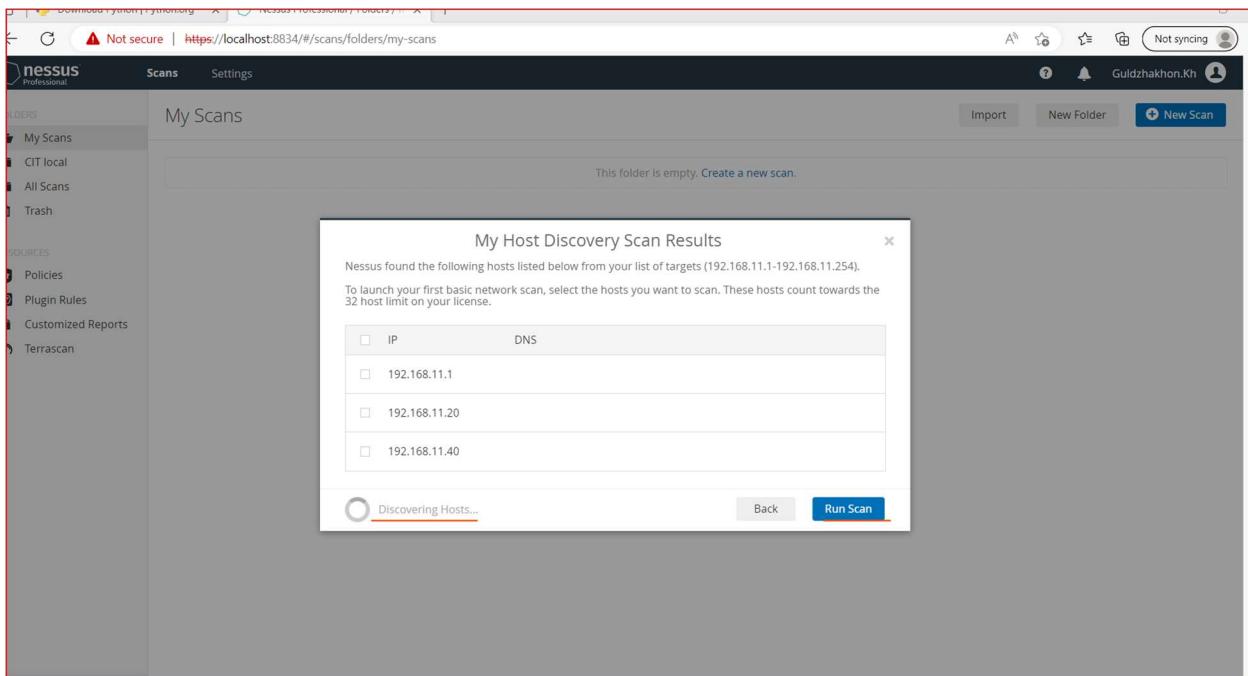
A screenshot of the Nessus Professional interface. The top navigation bar shows "Scans" and "Settings". The left sidebar has sections for "FOLDERS" (My Scans, All Scans, Trash) and "RESOURCES" (Policies, Plugin Rules, Customized Reports, Terrascan). The main content area is titled "My Scans" and contains the message "This folder is empty. Create a new scan." A large orange circle highlights the main content area. In the top right, there are two notifications: one about plugins compiling and another about the trial expiration on Feb 9, 2023. The user name "Guldzhakhon.Kh" is visible in the top right corner.

LAB WORK 6

Nessus



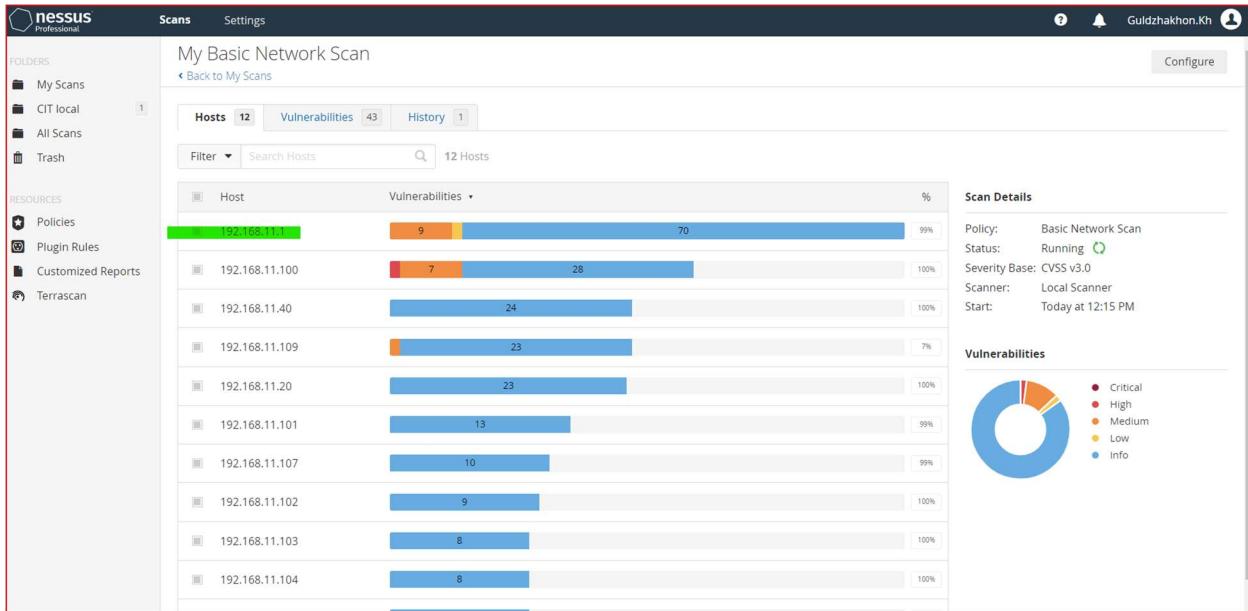
Enter IP range.



Nessus is discovering all devices. When discovering is completed Run Scan

LAB WORK 6

Nessus



It takes time to complete screening.

LAB WORK 6

Nessus

Not secure | https://localhost:8834/#/scans/reports/9/scan-summary

Scans Settings

Guildzhakhon.Kh

My Basic Network Scan

Scan Summary Hosts 31 Vulnerabilities 63 Remediations 1 VPR Top Threats 0 History 1

Scan Details

Critical Vulnerabilities	High Vulnerabilities
0	10

Medium Vulnerabilities	Low Vulnerabilities
69	2

Details

Scan Name: My Basic Network Scan
Plugin Set: 202302021412
CVSS_Score: CVSS_V3
Scan Template: Basic Network Scan
Scan Start: Today at 12:15 PM
Scan End: Today at 1:36 PM

Authentication / Credential Info (Hosts)

0 SUCCEEDED	31 FAILED
-------------	-----------

Top 5 Operating Systems Detected During Scan

Scan Durations

01:21:10 SCAN DURATION	00:09:27 MEDIAN SCAN TIME PER HOST	00:32:00 MAX SCAN TIME
------------------------	------------------------------------	------------------------

Saved to this PC | https://localhost:8834/#/scans/reports/9/vulnerabilities

There's an error with your feed. Click here to view your license information.

Scans Settings

Guildzhakhon.Kh

My Basic Network Scan

Scan Summary Hosts 31 Vulnerabilities 63 Remediations 1 VPR Top Threats 0 History 1

Filter Search Vulnerabilities 63 Vulnerabilities

Sev	Score	Name	Family	Count
MIXED	...	SSL (Multiple Issues)	General	119
MIXED	...	Qnap Qtz (Multiple Issues)	Misc.	10
MIXED	...	IETF Md5 (Multiple Issues)	General	6
MEDIUM	6.5	IP Forwarding Enabled	Firewalls	2
MEDIUM	6.1	JQuery 1.2 < 3.5.0 Multiple XSS	CGI abuses : XSS	1
MIXED	...	TLS (Multiple Issues)	Service detection	45
MIXED	...	SSL (Multiple Issues)	Service detection	9
MIXED	...	SMB (Multiple Issues)	Misc.	7
MIXED	...	Microsoft Windows (Multiple Issues)	Service detection	4
LOW	3.3 *	DHCP Server Detection	Service detection	1

Scan Details

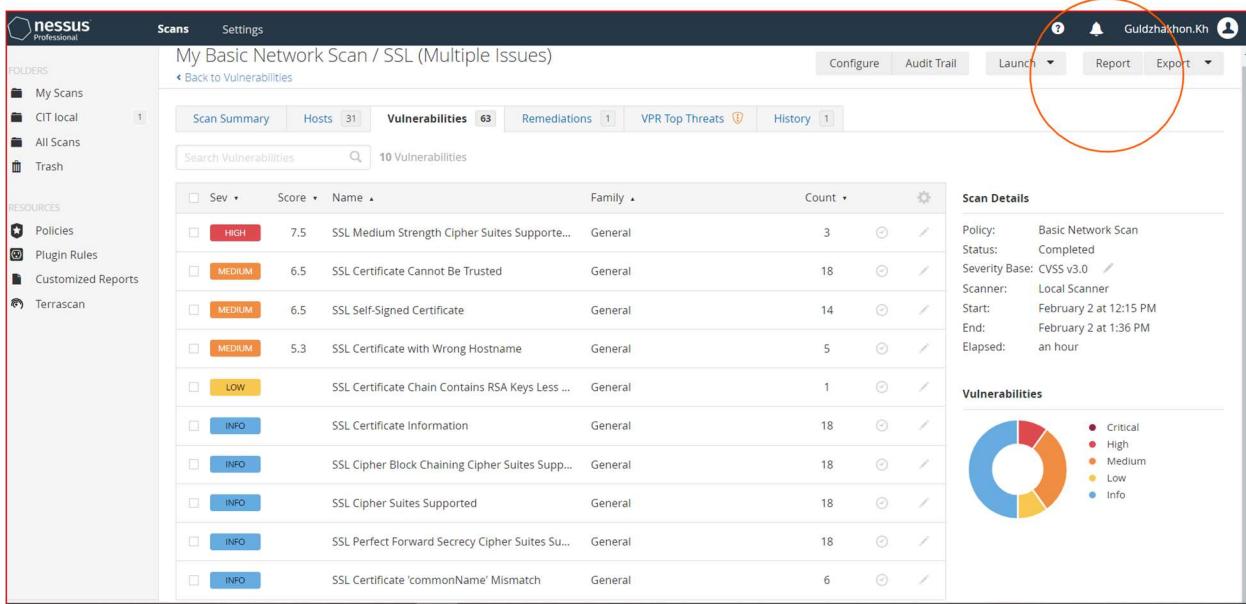
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: February 2 at 12:15 PM
End: February 2 at 1:36 PM
Elapsed: an hour

Vulnerabilities

54

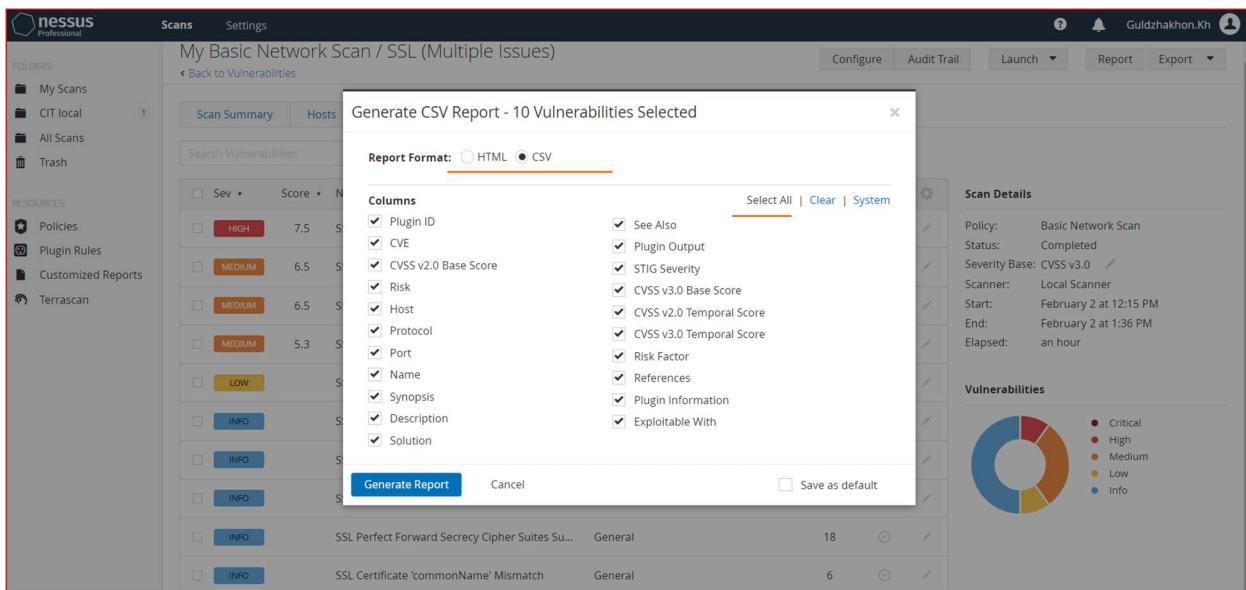
LAB WORK 6

Nessus



The screenshot shows the Nessus Professional interface. On the left, there's a sidebar with 'Folders' (My Scans, CIT local, All Scans, Trash) and 'Resources' (Policies, Plugin Rules, Customized Reports, Terrascan). The main area displays a scan titled 'My Basic Network Scan / SSL (Multiple Issues)' with 63 vulnerabilities found across 31 hosts. The vulnerabilities are listed in a table with columns for Severity (High, Medium, Low, Info), Score, Name, Family, and Count. A search bar at the top allows filtering by vulnerability name. To the right, there's a 'Scan Details' section with information about the scan (Policy: Basic Network Scan, Status: Completed, etc.) and a 'Vulnerabilities' section with a pie chart showing the distribution of severity levels (Critical, High, Medium, Low, Info).

Click on report to create a report. You can save it in any type of document you need. HTML, PDF or CVS.



This screenshot shows the same Nessus interface as above, but with a modal dialog overlaid. The dialog is titled 'Generate CSV Report - 10 Vulnerabilities Selected' and has 'Report Format: CSV' selected. It lists various 'Columns' to include in the report, such as Plugin ID, CVE, CVSS v2.0 Base Score, Risk, Host, Protocol, Port, Name, Synopsis, Description, Solution, See Also, Plugin Output, STIG Severity, CVSS v3.0 Base Score, CVSS v2.0 Temporal Score, CVSS v3.0 Temporal Score, Risk Factor, References, Plugin Information, and Exploitability. At the bottom, there are 'Generate Report', 'Cancel', and 'Save as default' buttons. The background of the main interface is dimmed.

Generate report.

LAB WORK 6

Nessus

✓ How to read the Report

2/6/23, 11:02 AM My Basic Network Scan

 Report generated by Nessus™

My Basic Network Scan

Thu, 02 Feb 2023 13:36:32 Eastern Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.11.1
- 192.168.11.20
- 192.168.11.40
- 192.168.11.100
- 192.168.11.101
- 192.168.11.102
- 192.168.11.103
- 192.168.11.104
- 192.168.11.105
- 192.168.11.107
- 192.168.11.109
- 192.168.11.111
- 192.168.11.112
- 192.168.11.113
- 192.168.11.114
- 192.168.11.116
- 192.168.11.122
- 192.168.11.131
- 192.168.11.137
- 192.168.11.146
- 192.168.11.147
- 192.168.11.149
- 192.168.11.158
- 192.168.11.159
- 192.168.11.163
- 192.168.11.167
- 192.168.11.169
- 192.168.11.172
- 192.168.11.191
- 192.168.11.196
- 192.168.11.250

Vulnerabilities by Host

Collapse All | Expand All

[file:///C:/Users/User/Downloads/My Basic Network Scan_1si0ow.html](file:///C:/Users/User/Downloads/My%20Basic%20Network%20Scan_1si0ow.html) 1/28

After scanning Nessus provides wide information and solutions on how to resolve detected issues.

Expand on interested field and find very detailed information about every single issue.

LAB WORK 6

Nessus

2/6/23, 11:02 AM My Basic Network Scan

192.168.11.147

0 1 3 27

Critical High Medium Low Info

Severity	CVSS v3.0	Plugin	Name
HIGH	7.5	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.9	31705	SSL Anonymous Cipher Suites Supported
LOW	N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	87242	TLS NPN Supported Protocol Enumeration
INFO	N/A	62564	TLS Next Protocols Supported

file:///C:/Users/User/Downloads/My Basic Network Scan_1st0ow.html 18/28

The interface is user friendly.

LAB WORK 6

Nessus

68	57582	6.4	Medium	192.168.1:tcp	21 SSL Self-Signed The SSL	The X.509 Purchase or generate a proper SSL certificate for this service.	Medium
69	57582	6.4	Medium	192.168.1:tcp	443 SSL Self-Signed The SSL	The X.509 Purchase or generate a proper SSL certificate for this service.	Medium
70	57608	5	Medium	192.168.1:tcp	445 SMB Signing is n/a	Enforce message signing in the host's configuration. On Windows, this	Medium
71	60119	None	192.168.1:tcp	445 Microsoft It was possible to use n/a	0 Patch Rep. The remote host	Install the patches listed below.	None
72	66334	None	192.168.1:tcp	21 SSL Cipher The	The	n/a	None
73	70544	None	192.168.1:tcp	443 SSL Cipher The	The	n/a	None
74	70544	None	192.168.1:tcp	22 SSH Algorithm An SSH server This script	n/a	n/a	None
75	70657	None	192.168.1:tcp	443 HSTS Missing The remote host	Configure the remote web server to use HSTS.	n/a	None
76	84502	None	192.168.1:tcp	0 Ethernet Network This	This	n/a	None
77	86420	None	192.168.1:tcp	21 SSL Root Certificate Authority root	The	Ensure that use of this root Certification Authority certificate	None
78	94761	None	192.168.1:tcp	443 SSL Root Certificate Authority root	The	Ensure that use of this root Certification Authority certificate	None
79	94761	None	192.168.1:tcp	445 Server Misconfiguration The remote host	Disable SMBv1 according to the vendor instructions in Microsoft	n/a	None
80	96982	None	192.168.1:tcp	445 Microsoft It was Nessus	n/a	n/a	None
81	100871	6.1	Medium	192.168.1:tcp	21 TLS Version The remote host	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.	Medium
82	104743	6.1	Medium	192.168.1:tcp	443 TLS Version The remote host	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.	Medium
83	104743	6.1	Medium	192.168.1:tcp			Medium

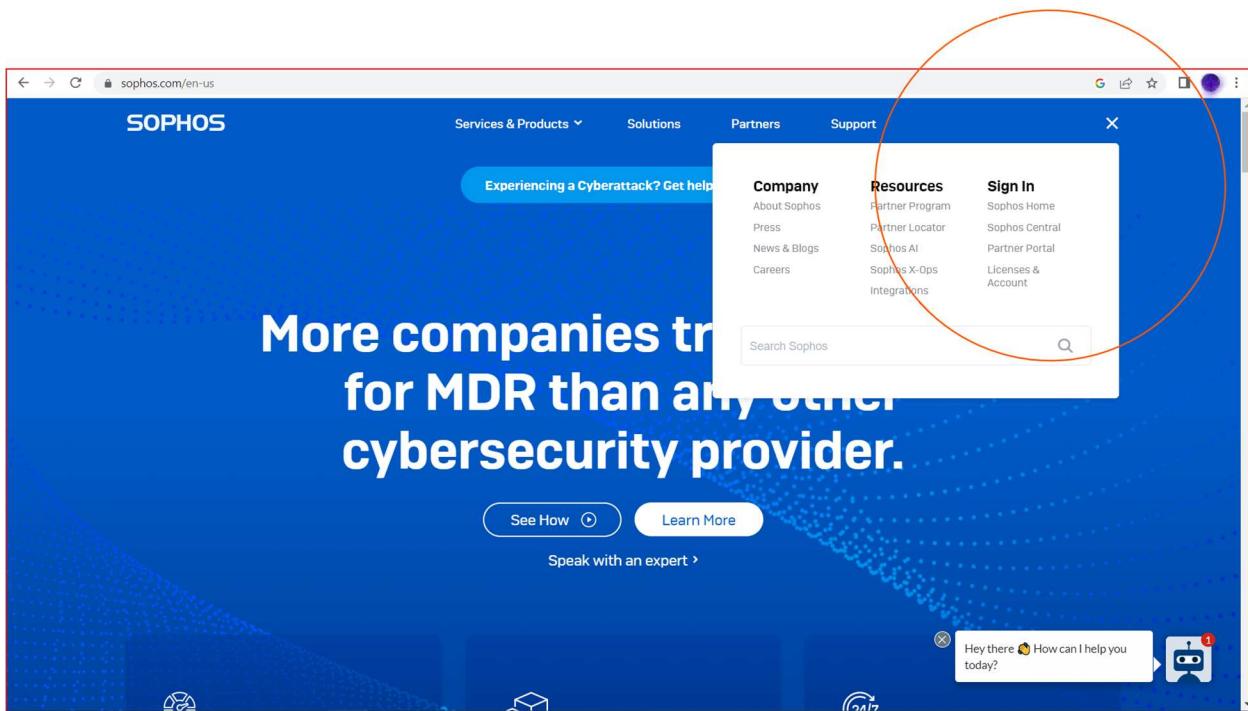
Open created reports and click on specific vulnerability.

You can easily apply patches and push recommendations following active links provided by Nessus.

LAB WORK 6 COMPLETED

SOPHOS

- ✓ Activate Sophos Central free trial.
- ✓ Install Server Protection on Windows Server 2016
- ✓ Push Website management rules



Follow the link to get started with the Sophos free Trial version:
www.sophos.com

LAB WORK 7

Sophos

The screenshot shows the Sophos Partner Dashboard. At the top, there's a header with the Sophos logo, user information (Gulia Khudzhabekova), and a 'Help' dropdown. Below the header is a 'Dashboard' section titled 'See a snapshot of your customers'. It features an 'Alerts' section with three cards: 'High Alerts' (116), 'Medium Alerts' (166), and 'Info Alerts' (220). Below this is a 'Usage For My Monthly Customers' section with a table of data. To the right, there are two promotional sections: 'Sophos Central' (with a cloud icon) and 'Sophos Central - Firewalls' (with a network diagram).

Alerts

For My Managed Customers

Category	Count
High Alerts	116
Medium Alerts	166
Info Alerts	220

Usage For My Monthly Customers

Category	Value
Endpoint...	0
Intercep...	52
Intercep...	0
Intercep...	190
Intercep...	25
Server ...	0
Intercep...	5
Intercep...	12
Intercep...	7
Mobile ...	0
Mobile ...	6
Sophos ...	0
Web	0
Phish T...	0
Zero Tr...	0
Central ...	0
Extende...	0

Sophos Central

Sophos Central - Firewalls

My Sophos Partner Dashboard.

LAB WORK 7

Sophos

The screenshot shows the Sophos Central Dashboard. The left sidebar contains a navigation menu with the following items:

- Dashboard
- Alerts
- Threat Analysis Center
- Logs & Reports
- People
- Devices
- Global Settings
- Protect Devices
- Account Health Check
- MY PRODUCTS
 - Endpoint Protection
 - Server Protection
 - Mobile
 - Encryption
 - Wireless

A red circle highlights the "Protect Devices" and "Account Health Check" sections under "MY PRODUCTS". A second red circle highlights the "Server Protection" item. Below the sidebar, the URL is https://central.sophos.com/manage/bulk-users.

The main dashboard area displays the following statistics:

- Total Alerts: 0
- High Alerts: 0
- Medium Alerts: 0
- Low Alerts: 0

Below these stats is a section titled "Most Recent Alerts" with a message: "You currently do not have any alerts." and a "View all Alerts" link.

On the right side, there are two sections: "Devices and users: summary" and "Web control". The "Devices and users: summary" section includes a pie chart titled "Endpoint Computer Activity Status" showing the following data:

Status	Count
Active	5
Inactive 2+	3
Inactive 2+	0

The "Web control" section shows a message: "No pages blocked or warned about in the last 30 days."

My free trial Sophos Central Dashboard

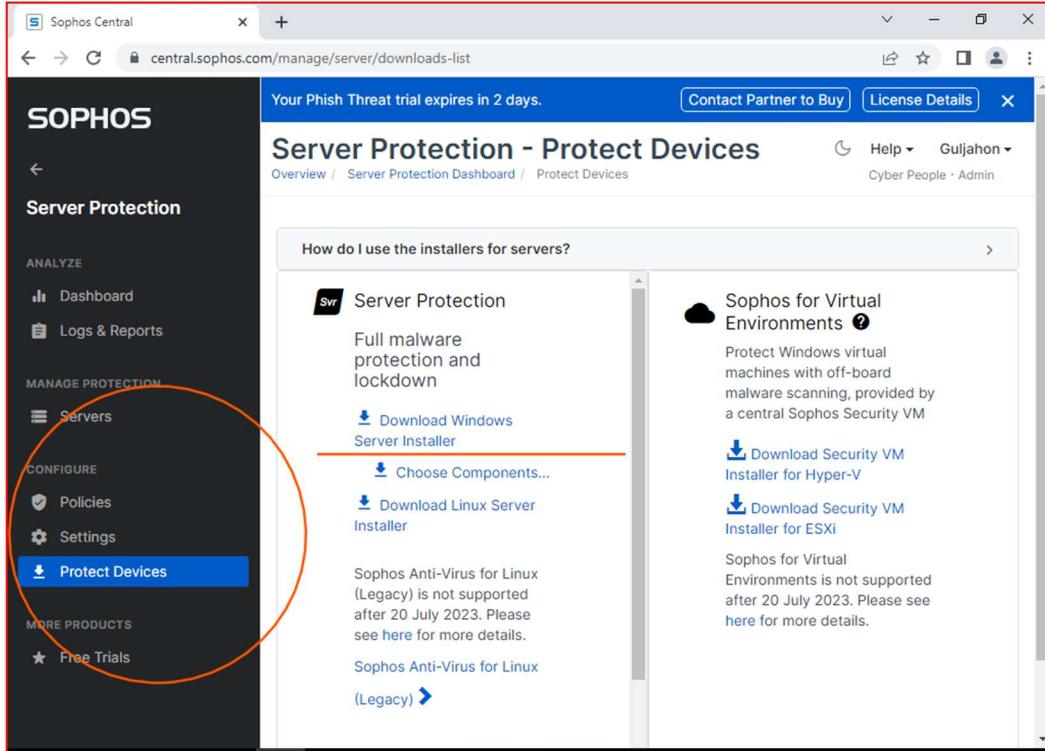
The screenshot shows the "People" management interface in Sophos Central. The left sidebar has the same navigation menu as the previous screenshot, with "People" selected. The main area is titled "People" and "Manage your users". It shows a list of users:

Name	Email	Action
Miceal White	alexcyber23@consultant.com	Actions
Parisa2	heregavahi@yahoo.com	Actions
Parisa3	gavahi@yahoo.com	Actions
Sadiq	sadiqali@hotmail.ca	Actions
Tolu	tolulopeoogun@gmail.com	Actions

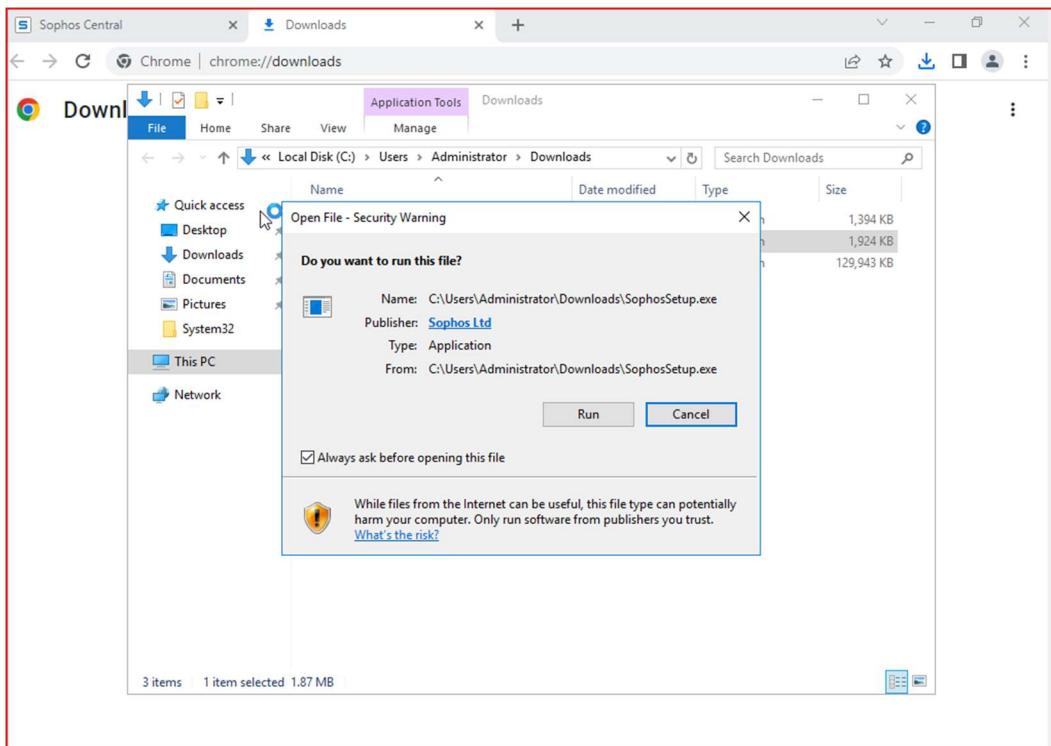
At the top of the main area, it says "Your Phish Threat trial expires in 2 days." and has "Contact Partner to Buy" and "License Details" buttons. The URL in the browser bar is https://central.sophos.com/manage/overview/users-list.

LAB WORK 7

Sophos



The screenshot shows the Sophos Central interface for Server Protection. On the left, a sidebar titled 'Server Protection' includes options like 'Dashboard', 'Logs & Reports', 'Servers' (which is highlighted with a red circle), 'Policies', 'Settings', and 'Protect Devices'. The main content area is titled 'Server Protection - Protect Devices' and contains sections for 'How do I use the installers for servers?' and 'Sophos for Virtual Environments'. It features links to download Windows and Linux server installers, and a note about legacy Linux support.

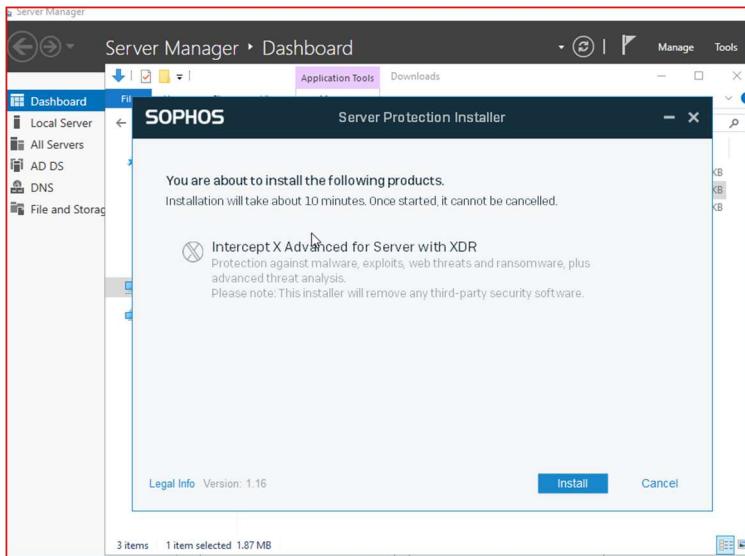


The screenshot shows a Chrome browser window with a download progress bar for 'SophosSetup.exe' from Sophos Ltd. The file is 1,924 KB in size. A warning dialog box is overlaid on the download interface, asking if the user wants to run the file. The dialog provides details about the file (Name: C:\Users\Administrator\Downloads\SophosSetup.exe, Publisher: Sophos Ltd, Type: Application, From: C:\Users\Administrator\Downloads\SophosSetup.exe) and includes 'Run' and 'Cancel' buttons, as well as a checkbox for 'Always ask before opening this file'.

Run Setup.

LAB WORK 7

Sophos



Complete installation.

The screenshot shows the Sophos Server Protection - Servers dashboard. The left sidebar has sections for ANALYZE (Dashboard, Logs & Reports), MANAGE PROTECTION (Servers, Policies), and CONFIGURE (Policies). The main area is titled "Server Protection - Servers" and shows a table of servers. One server, "Guli16", is selected and highlighted with a green checkmark. The table columns include Name, IP, OS, Protection, Last active, and Group. The "Protection" column for Guli16 shows "Intercept X Advanced for Server with XDR".

The screenshot shows the Sophos Central - Guli16 server summary page. The left sidebar has sections for ANALYZE (Dashboard, Logs & Reports), MANAGE PROTECTION (Servers, Policies), and CONFIGURE (Policies, Settings, Protect Devices). The main area is titled "Server Protection - Guli16". It shows an "Agent Summary" table with rows for Last Sophos Central Activity, Last Agent Update, Assigned Products (Core Agent, Sophos Intercept X, Server Protection, XDR), and Installed component versions (10.0.2.15, 10.0.3.15). It also shows system details like IPv4 Addresses (10.0.2.15, 10.0.3.15), Operating System (Windows Server 2016 Standard Evaluation), Processor Architecture (x64), Lockdown Status (Not installed), Group (No group, Change group), and Tamper Protection (Off). A yellow warning box states: "⚠ You can't turn on tamper protection here because it has been turned off for all your devices. To turn it on, go to System Settings > Tamper Protection." Other sections include Windows Firewall (Active(Domain, Private, Public)), Managed by Windows Group Policy (No), Last Active Profiles (Domain), and Other Registered Firewalls (This feature is not available on this Operating System).

The Server is added to a Sophos Central Dashboard.

LAB WORK 7

Sophos

The screenshot shows the Sophos Central interface for a server named Guli16. The left sidebar has a dark theme with the following navigation:

- SOPHOS**
- Server Protection**
- ANALYZE**: Dashboard, Logs & Reports
- MANAGE PROTECTION**:
 - Servers** (selected)
 - Configure: Policies, Settings, Protect Devices
 - More Products: Free Trials

The main content area is titled "Server Protection - Guli16". It includes the following sections:

- Agent Summary**: Shows activity (Last Sophos Central Activity: 3 hours ago), agent update (Last Agent Update: 3 hours ago, Update Successful), assigned products (Core Agent, Sophos Intercept X, Server Protection, XDR), and component versions (IPv4 Addresses: 10.0.2.15, 10.0.3.15; Operating System: Windows Server 2016 Standard Evaluation, x64; Lockdown Status: Not installed; Group: No group, Change group; Tamper Protection: Off). A note says: "⚠ You can't turn on tamper protection here because it has been turned off for all your devices. To turn it on, go to System Settings > Tamper Protection."
- Windows Firewall**: Active(Domain, Private, Public), Managed by Windows Group Policy: No, Last Active Profiles: Domain.
- Other Registered Firewalls**: This feature is not available on this Operating System.

Overview.

LAB WORK 7

Sophos

The screenshot shows the Sophos Central interface with a red border around the main content area. A modal window titled "Add Website Customization" is open in the center. The URL in the address bar is "central.sophos.com/manage/server/config/settings/websites-tagged". The modal has fields for "ENTER URLs, DOMAINS, TLDs, IP ADDRESSES, OR CIDR RANGES" containing "https://www_lcbo_com/en/", "CATEGORY OVERRIDE" set to "Alcohol & Tobacco", and "ADD TAGS" with "Alcohol" and "Tobacco" listed. There's also a "COMMENTS" field and "Cancel" and "Save" buttons.

Add blocklisted website.

The screenshot shows the Sophos Central interface with a red border around the main content area. The URL in the address bar is "central.sophos.com/manage/server/config/settings/websites-tagged". The main page title is "Server Protection - Website Management". It lists websites with their tags and categories. The row for "www_lcbo_com/en/" is highlighted with an orange border. The table columns are "WEBSITE", "TAGGED AS", and "CATEGORY". The data is as follows:

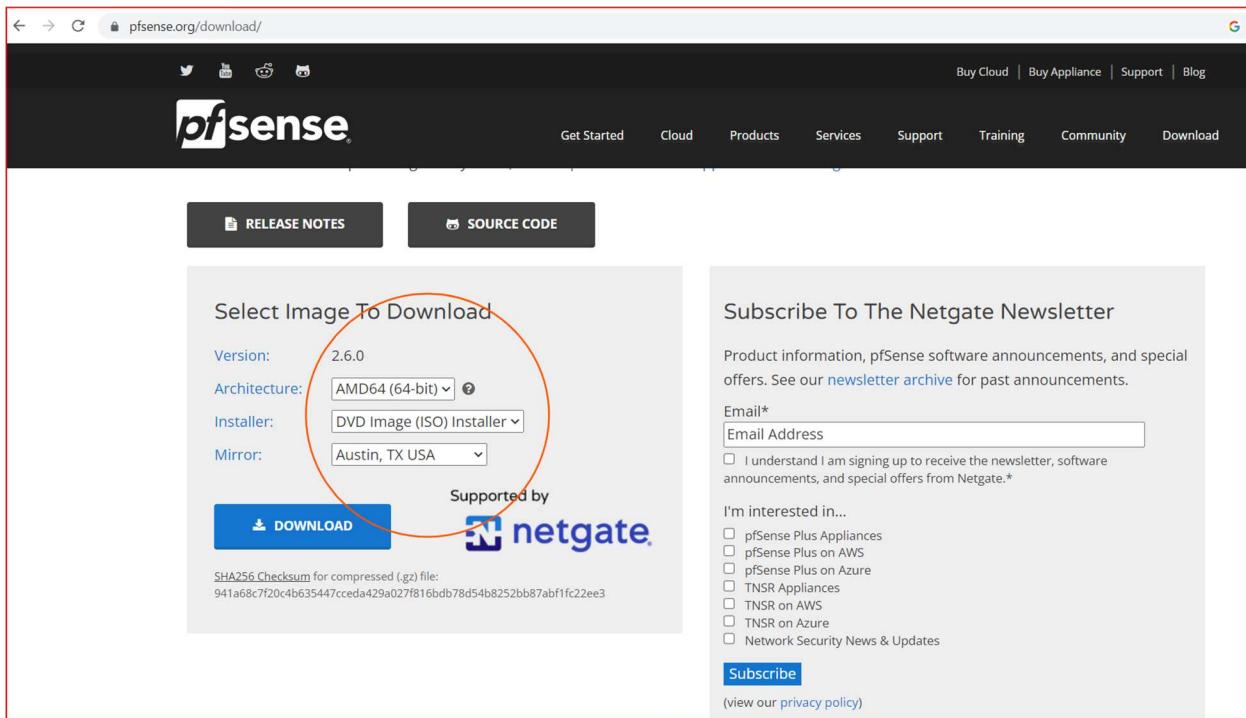
WEBSITE	TAGGED AS	CATEGORY
www.facebook.com	facebook allowed	Blogs & Forums
www.instagram.com	Allow Instagram	Blogs & Forums
www_lcbo_com/en/	Tobacco, Alcohol	Alcohol & Tobacco

LAB WORK 7 COMPLETED

PFSENSE

Deploy pfSense firewall:

- ✓ Setup WAN and LAN Interface
- ✓ Use Default Gateway for Internet Access on Server and Workstation
- ✓ Set up Deny Rule for Social Media
- ✓ Install Snort Package
- ✓ Setup Snort IPS using OinkCode



Follow the link to download iso file of pfSense operating system:

<https://www.pfsense.org>

Selected parameters:

Architecture: AMD 64 (64bit)

Installer: DVD Image (ISO) Installer

Mirror: Austin, TX USA