BUILDBOOK

BY

GULDZHAKHON KHUDZHABEKOVA

SOC CYBERSECURITY ANALYST

Training Program

LAB WORK 1

Install Oracle WM 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

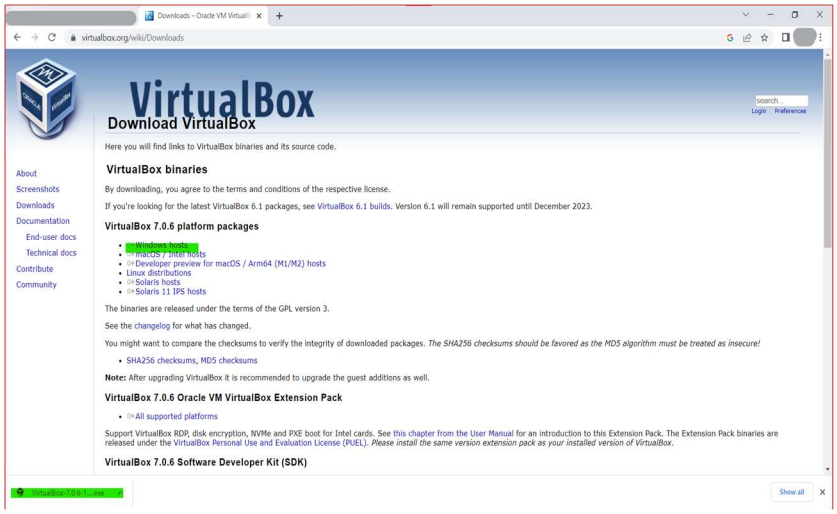
pfSense

LAB WORK 1

Install Oracle WM VirtualBox

Follow the link to download and install:

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

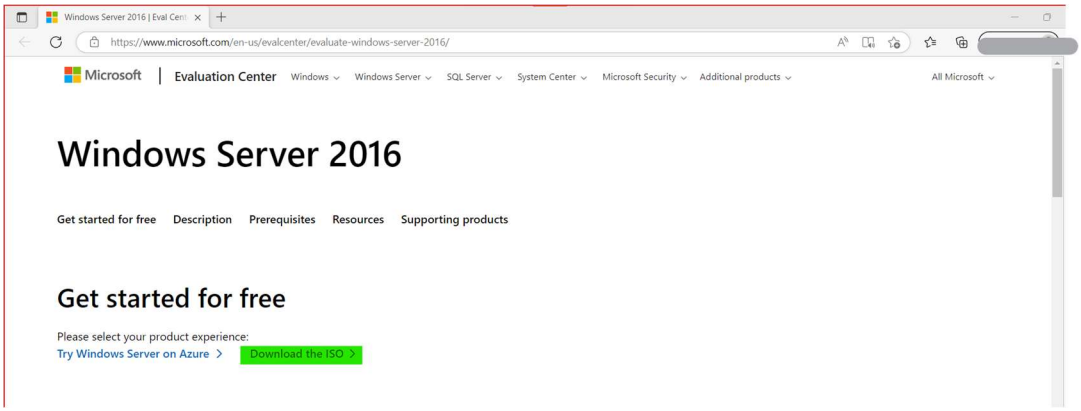


1. Click on the compatible with your device version.
2. Run setup file.
3. When Installation is completed, open VirtualBox Manager page.

LAB WORK 1 COMPLETED

LAB WORK 2

Install Windows Server 2016 on VirtualBox

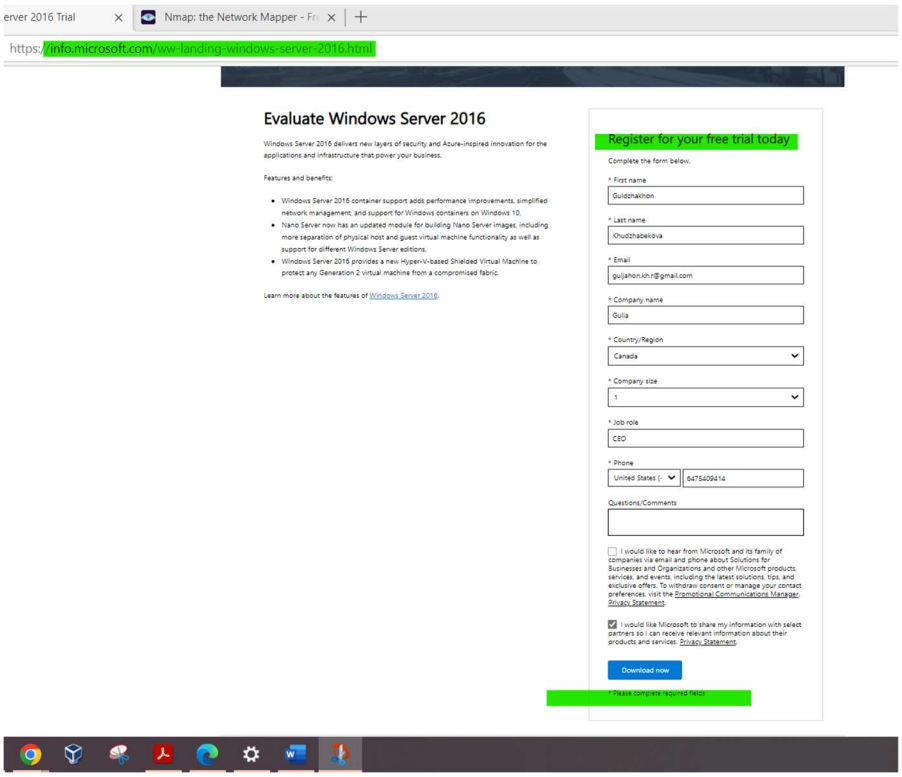


Follow the link to download ISO file for Windows Server 2016:

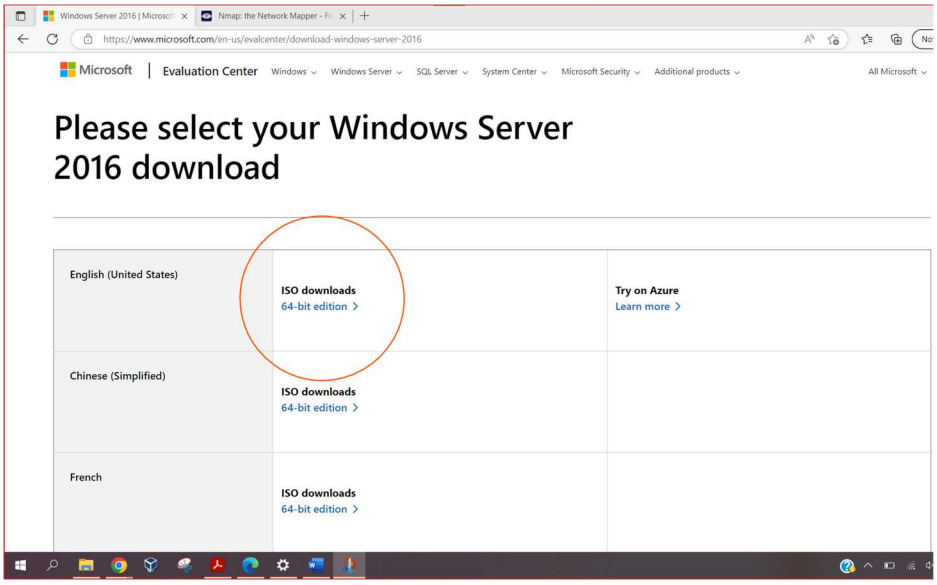
Windows Server 2016 Trial (microsoft.com)

LAB WORK 2

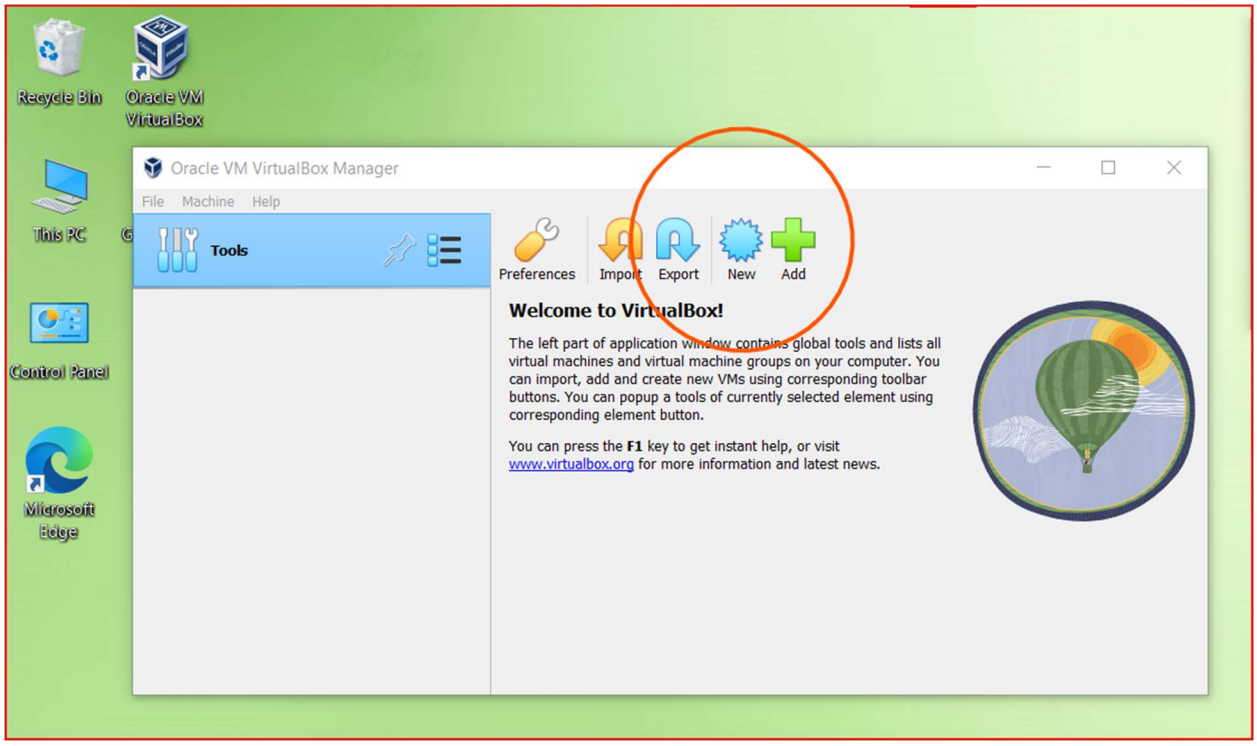
Install Windows Server 2016 on VirtualBox



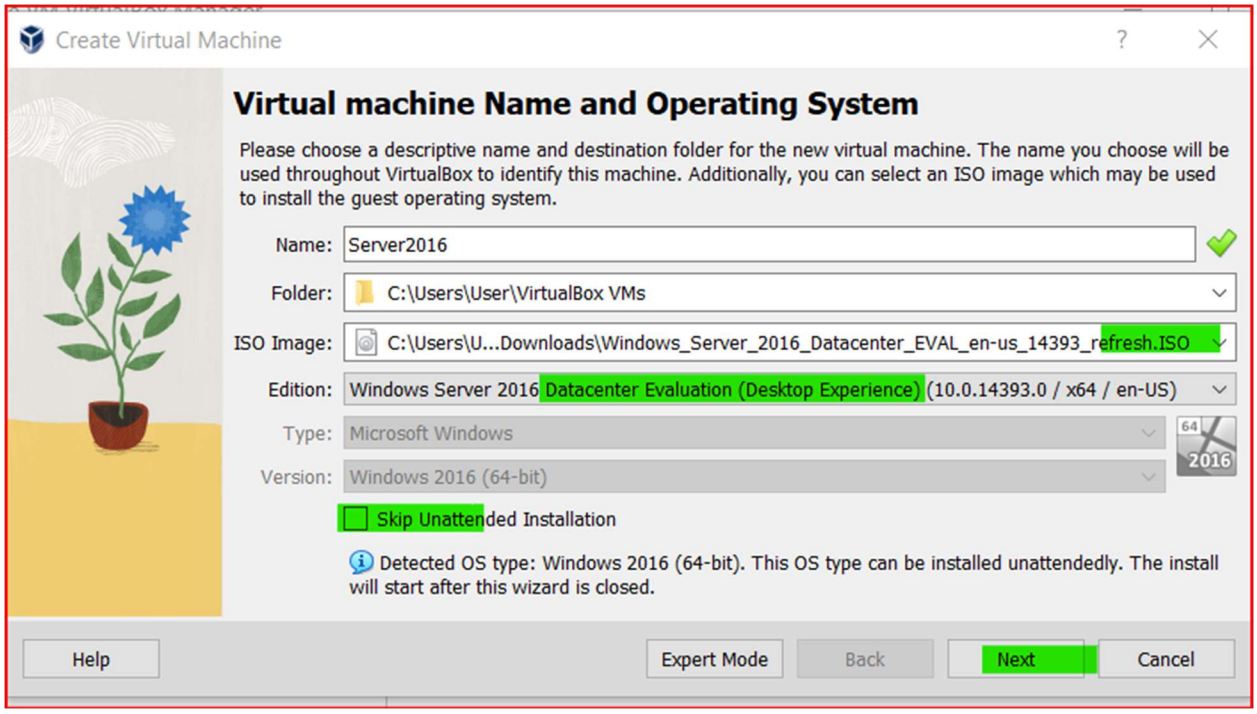
Fill out the form and click **Download.**



Follow the instruction.



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



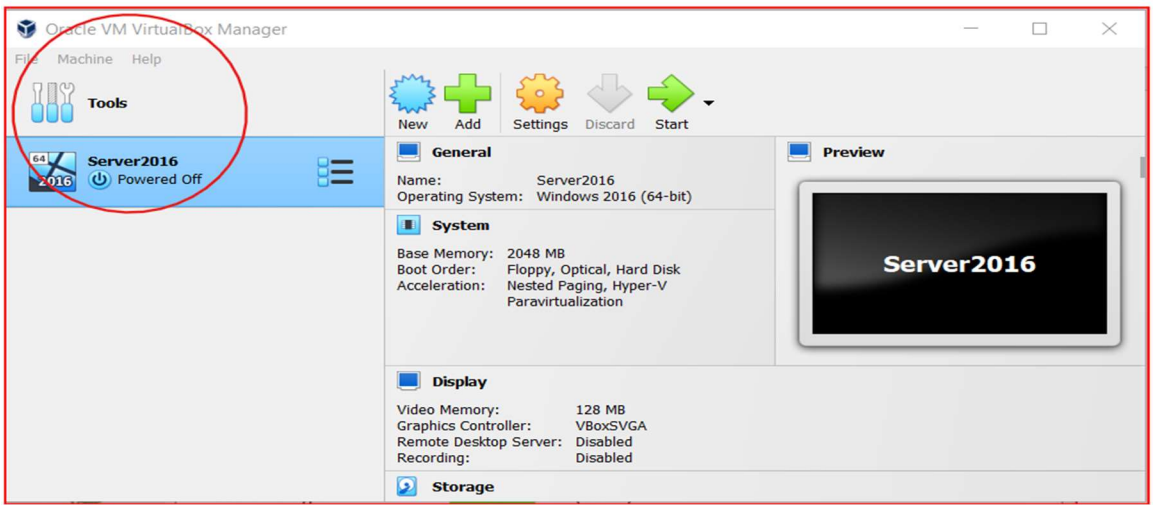
1. Enter desired name.

2. Choose ISO file

3. Click on **“Datacenter Evaluation (Desktop Experience)”**

4. Skip unattended installation.

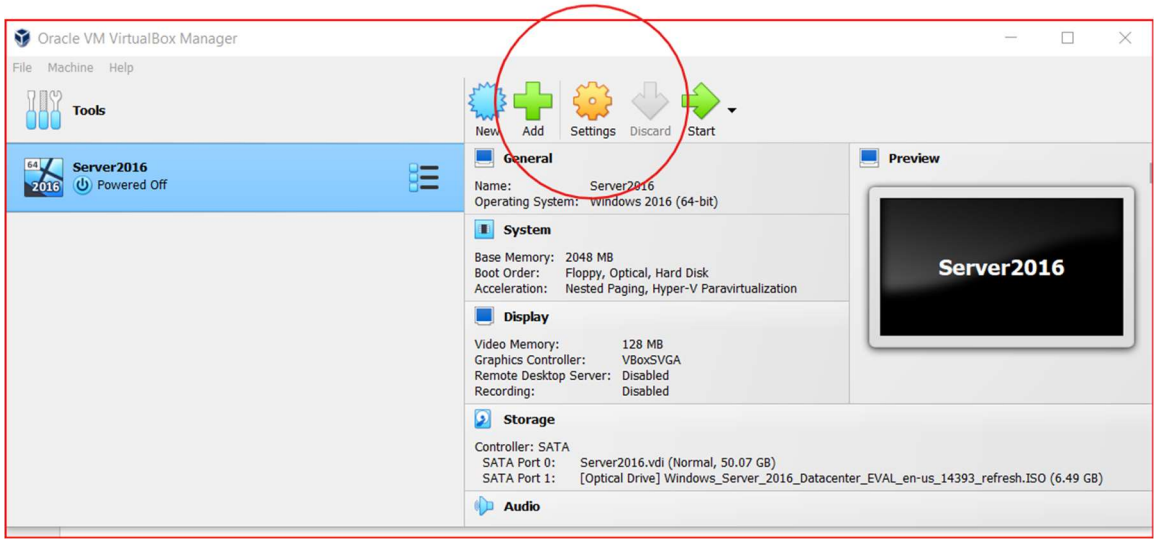
5. leave options by default



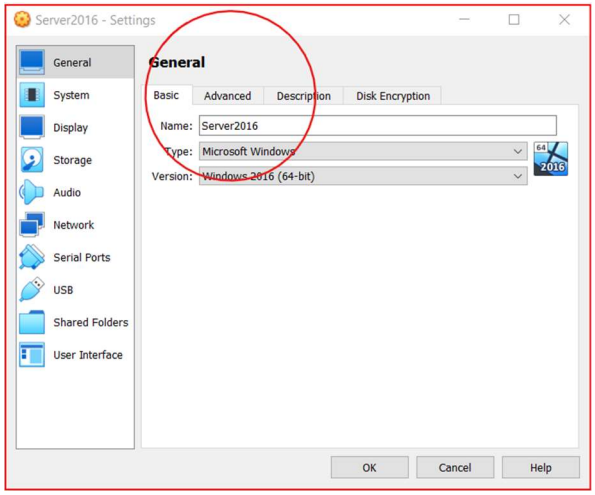
VirtualBox manager:

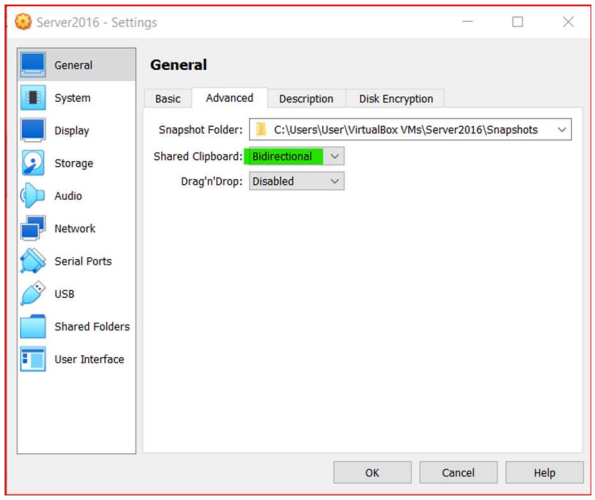
All virtual machines will be appeared under **Tools**.

Next, we will apply configurations.



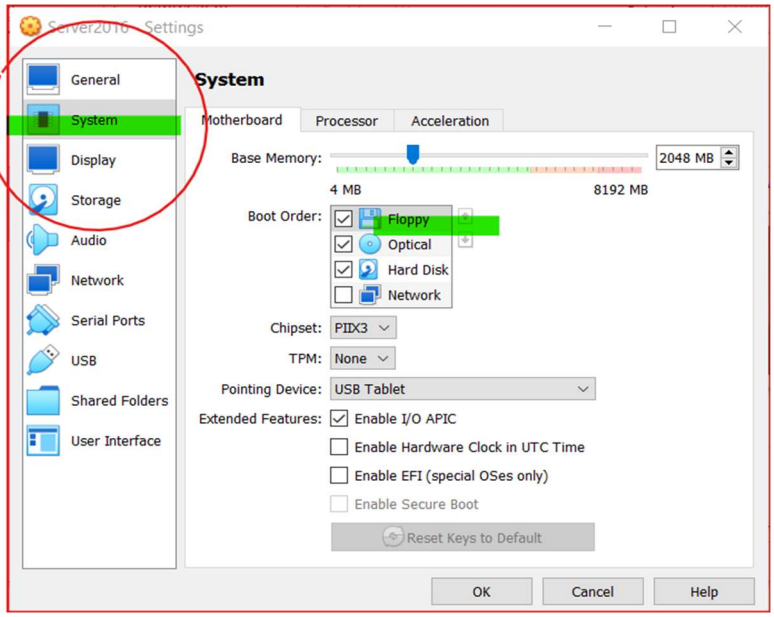
Go to Settings.



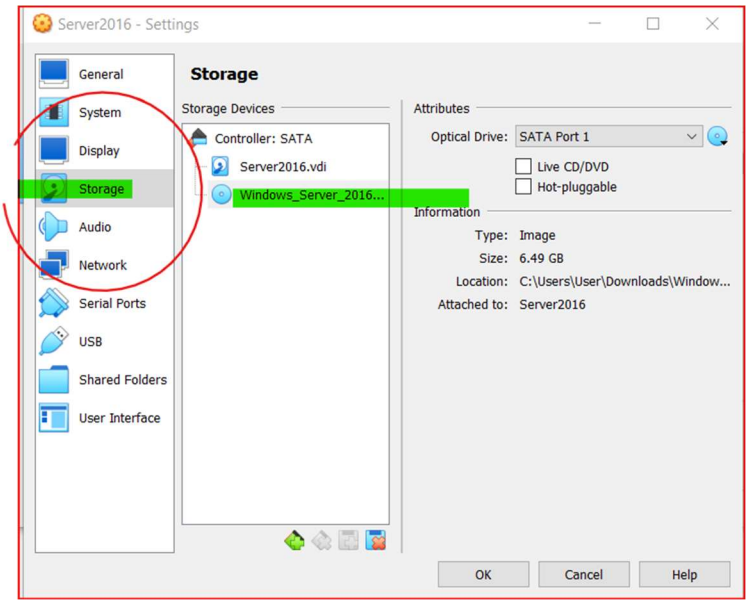


Shared clipboard means the ability to copy and paste from host machine onto virtual.

- 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.



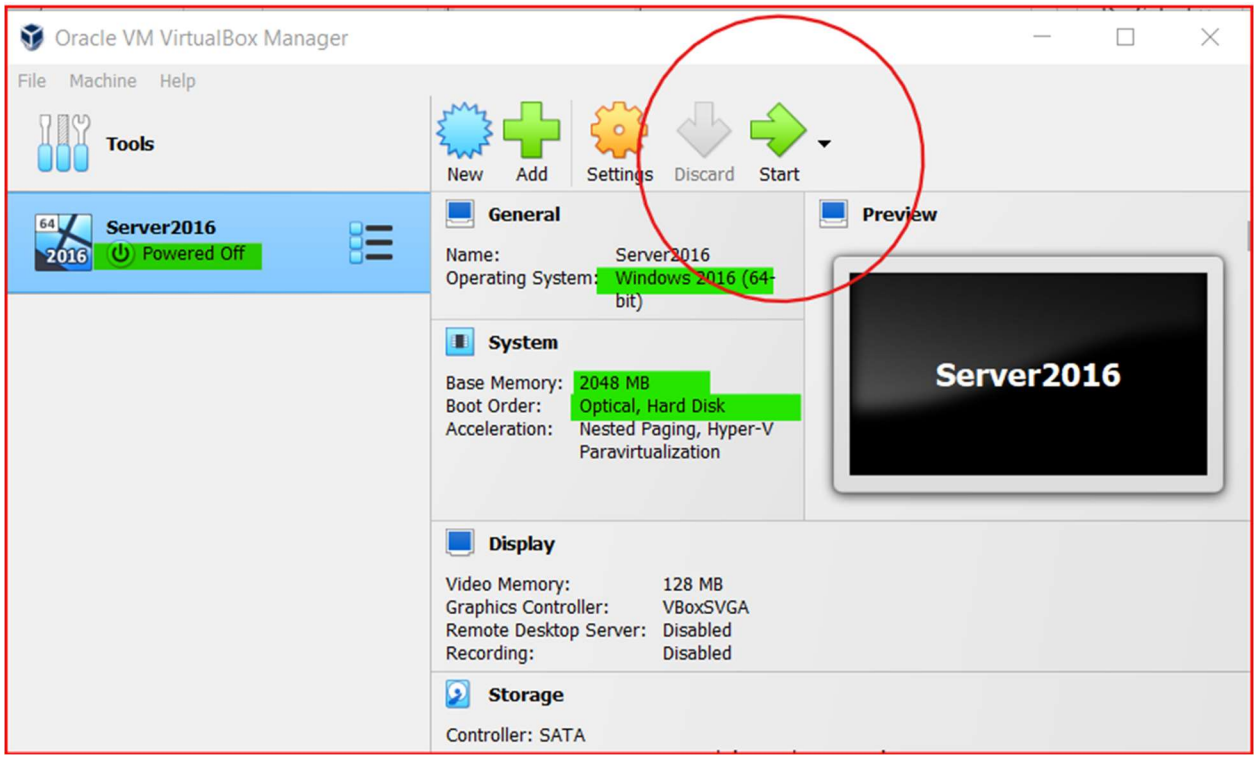
From boot order disable **Floppy.**



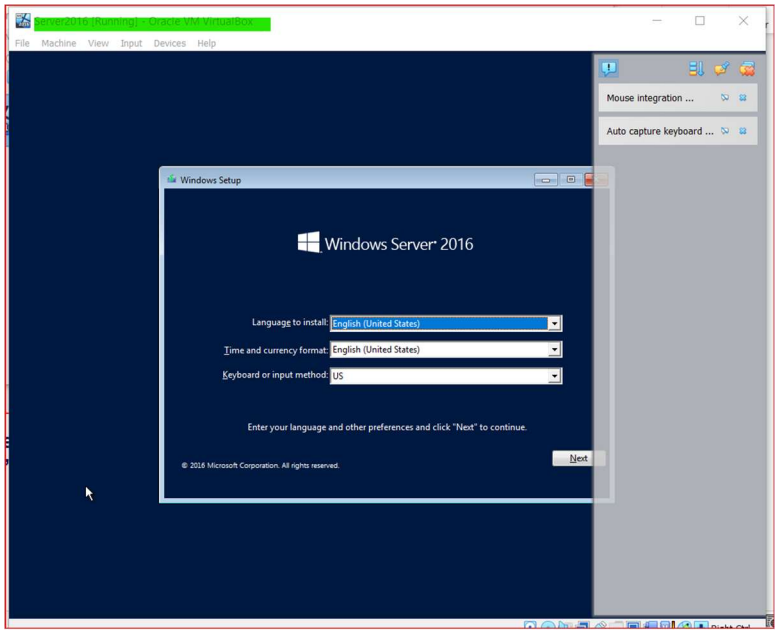
Leave other options by default.

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

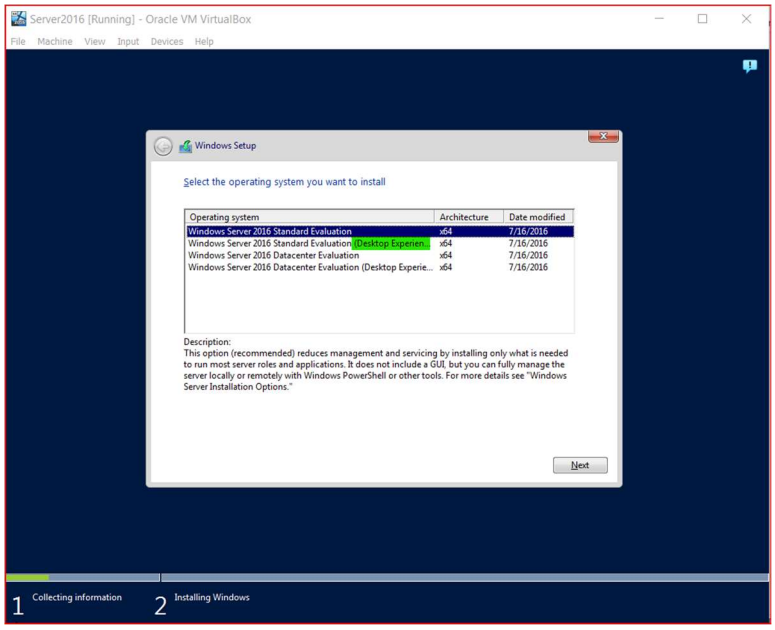
Click **OK**



Windows Server 2016 is set to go.
Click **Start** to run installation.

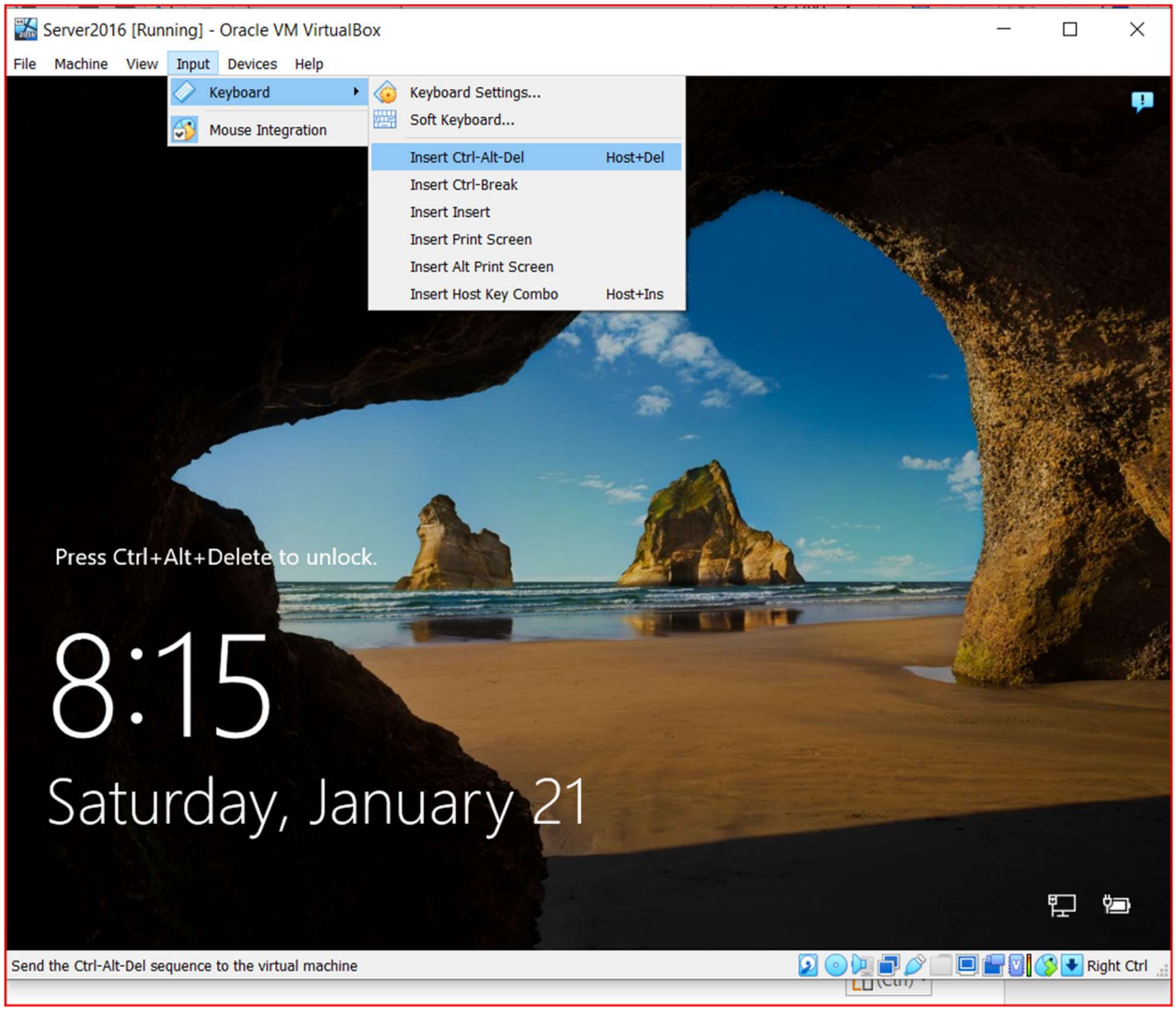


Follow instruction – **Next, Install Now, Next,**

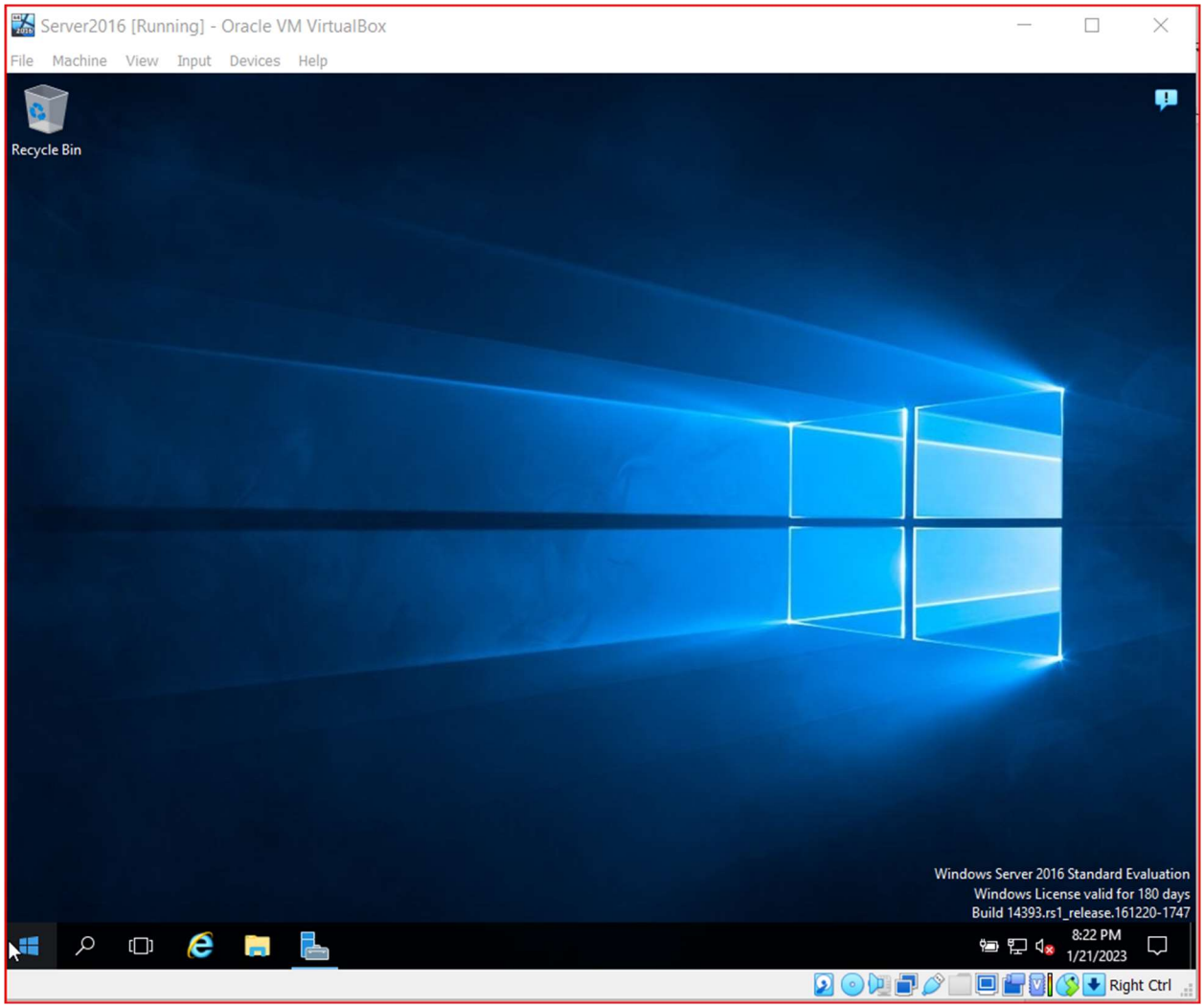


It is important to install “Standard Evaluation Desktop Experience” to use GUI.
Next> Accept the software license agreement.
Next> Select **Custom**.

Next> Create an account/strong password.



Insert password for default built-in administrator account.



Windows Server 2016 desktop.

LAB WORK 2 COMPLETED

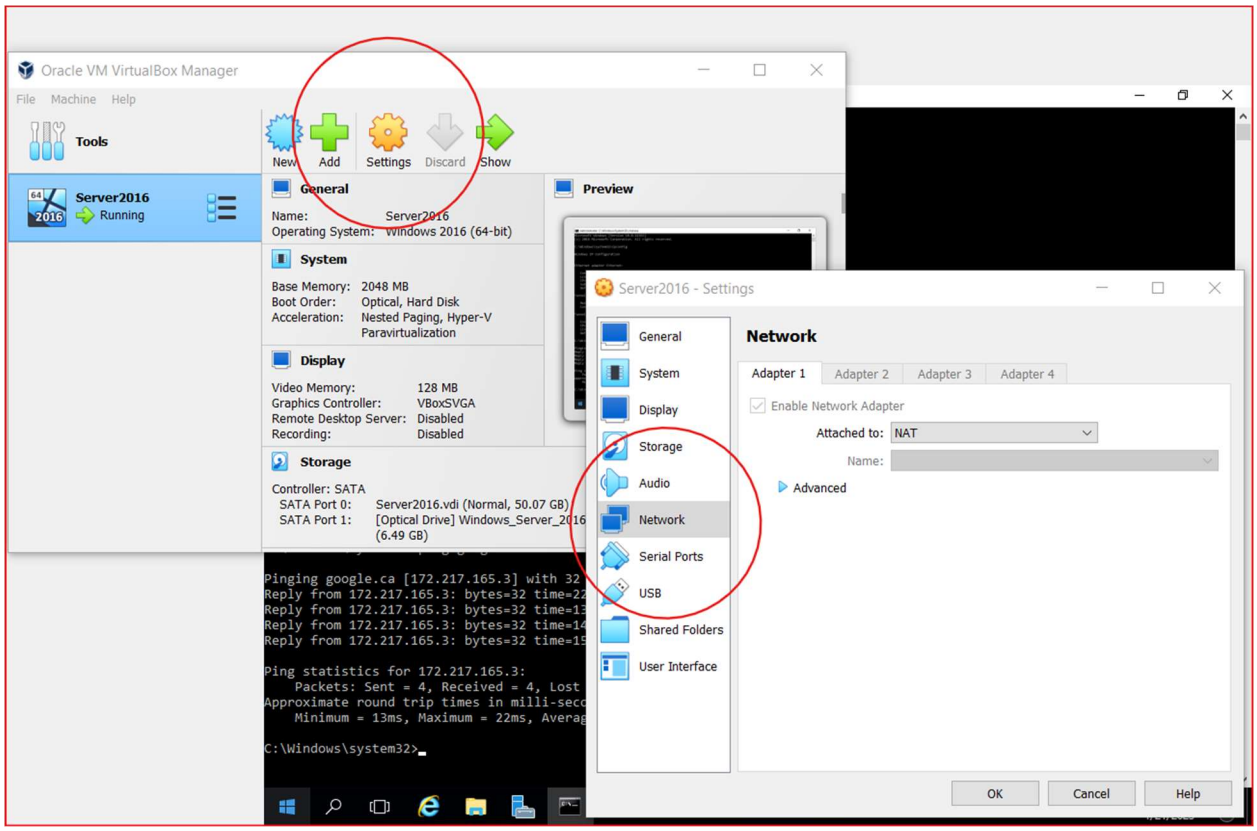
LAB WORK 3

Install Active Directory on Windows Server 2016

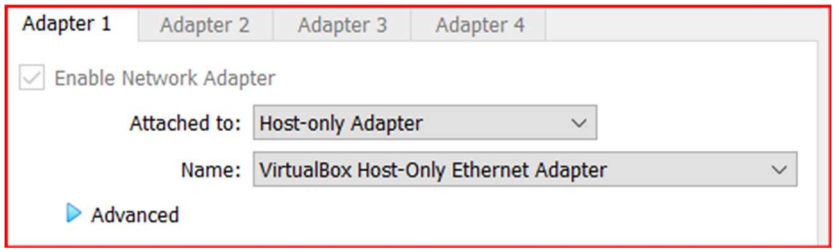
Prepare the environment before the installation process of Active Directory Domain Controller (*AD DC)

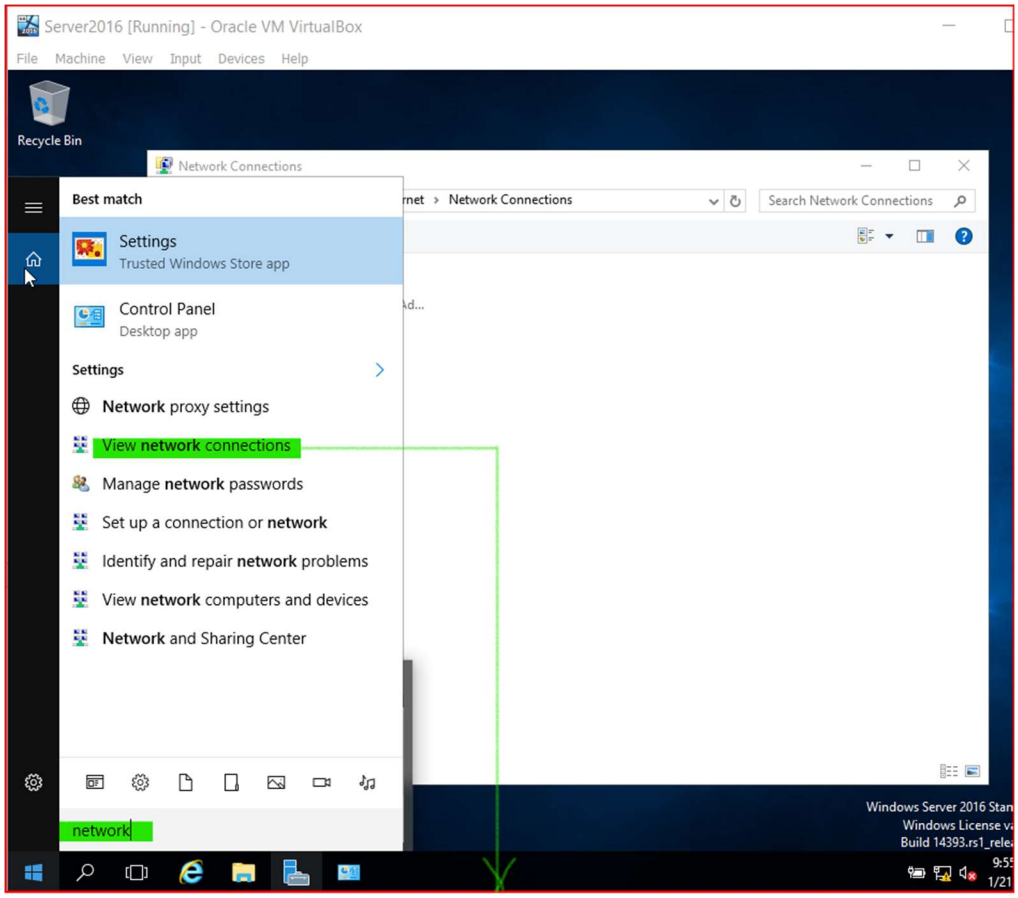
- ✓ Configure static IP address.
- ✓ Change PC name, reboot the system.
- ✓ Install Active Directory Domain Service (*AD DS) by using Server Manager
- ✓ Add Users

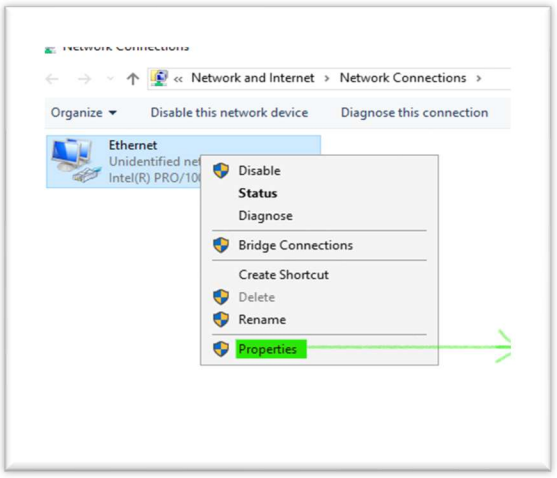
Static IP address.



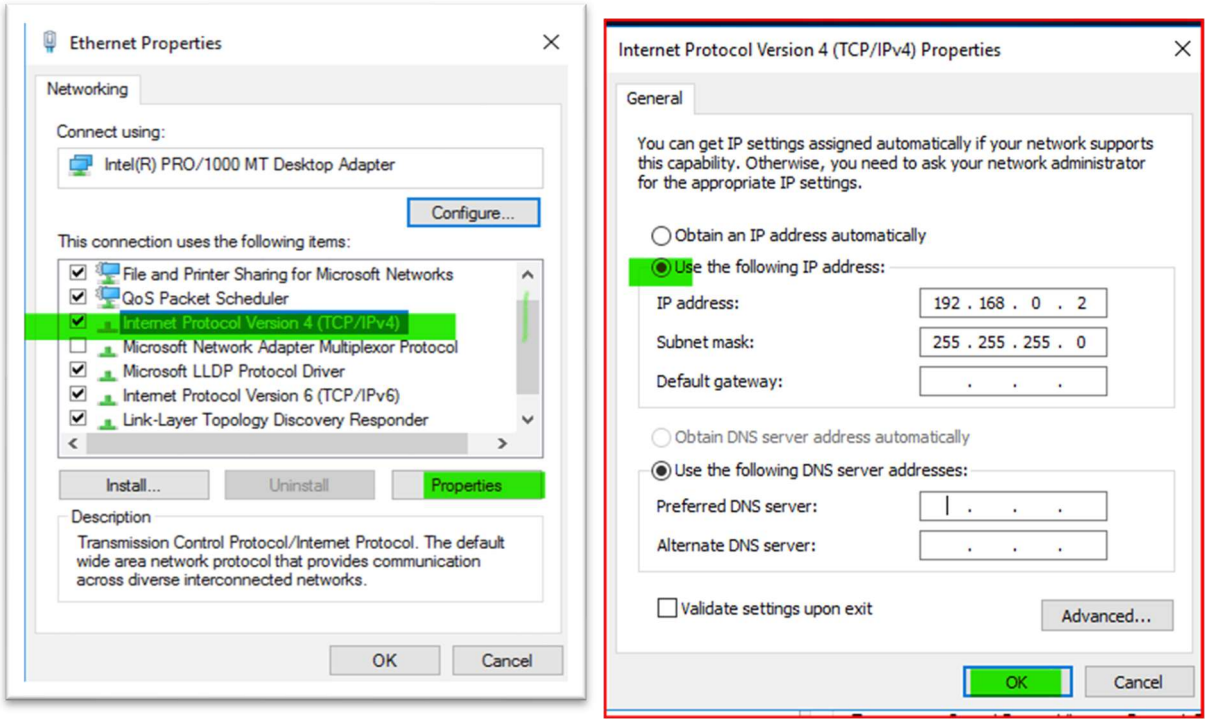
VirtualBox>Settings>Network>Adapter 1>Host-only Adapter>OK.





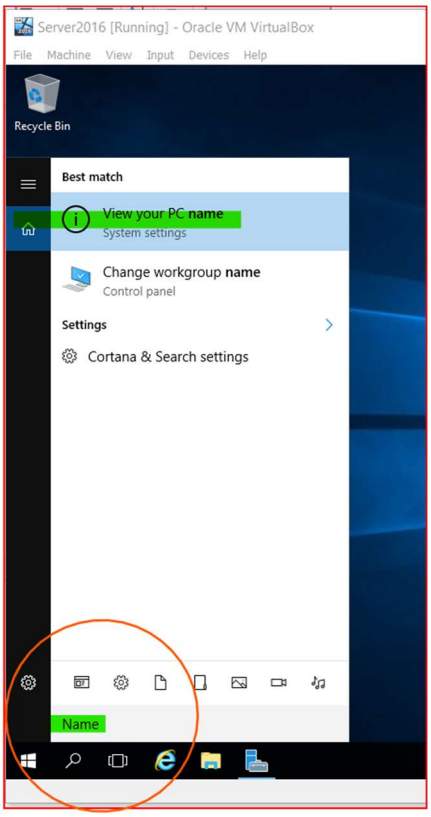


Start>View network connections>Ethernet>Property>Internet Protocol Version 4(TCP/IPv4)>Properties

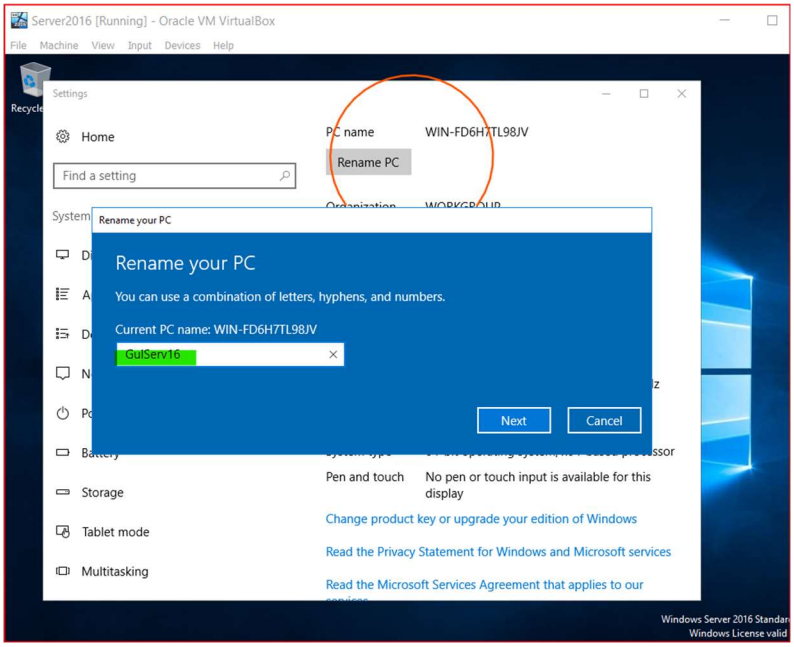


Set Static IP adress **192.168.0.2**

Rename PC



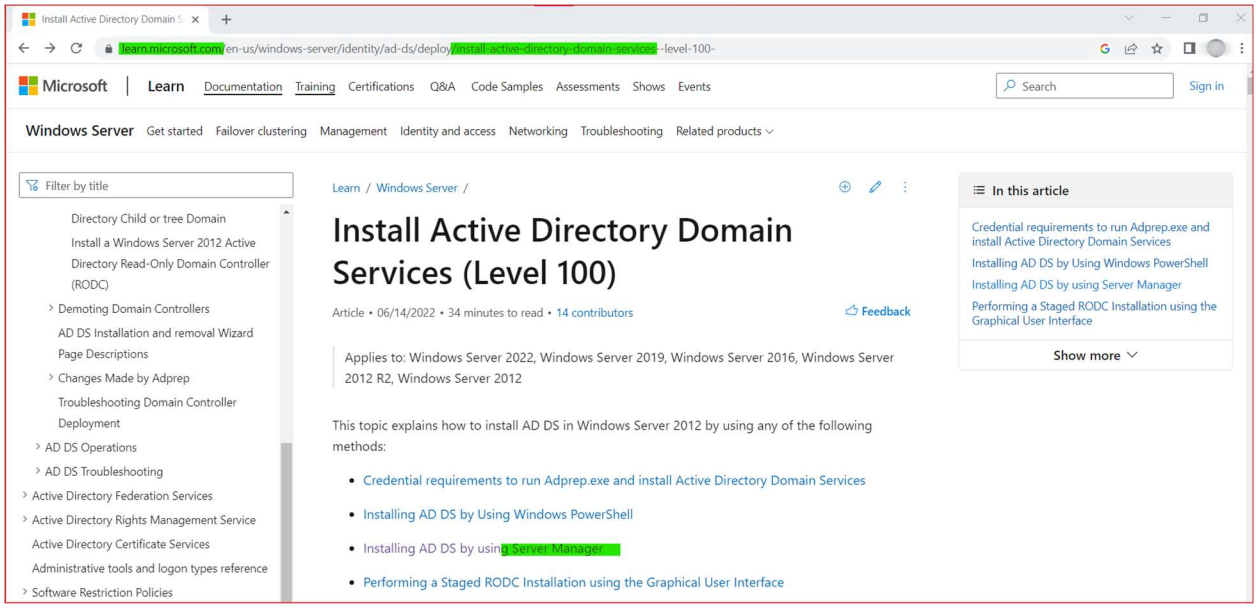
Click on **Start** button, type in **Name**>**View your PC Name**

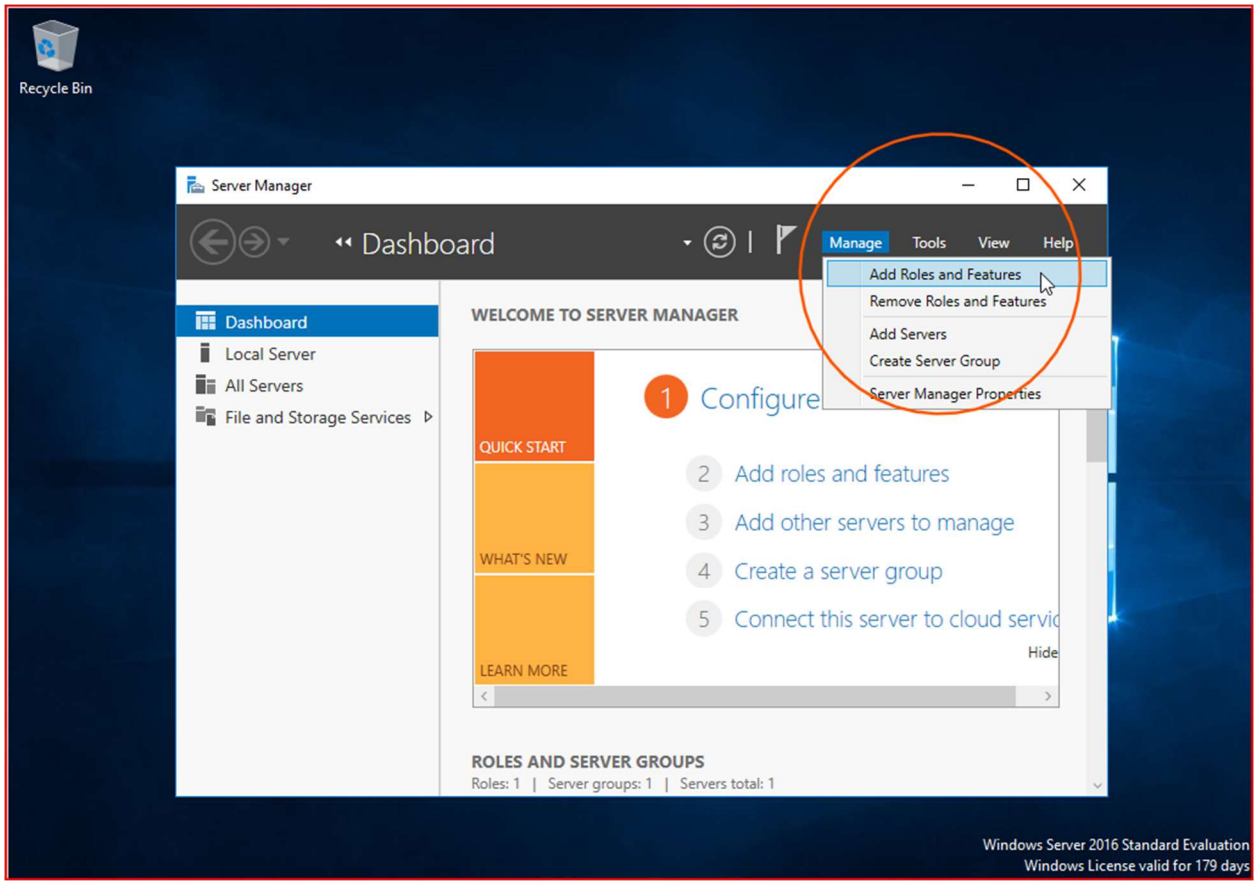


Click **Rename PC/Restart Now**

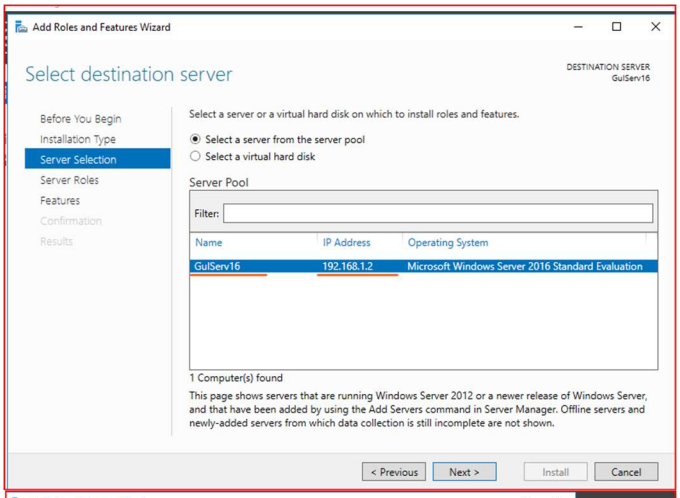
Install Active Directory

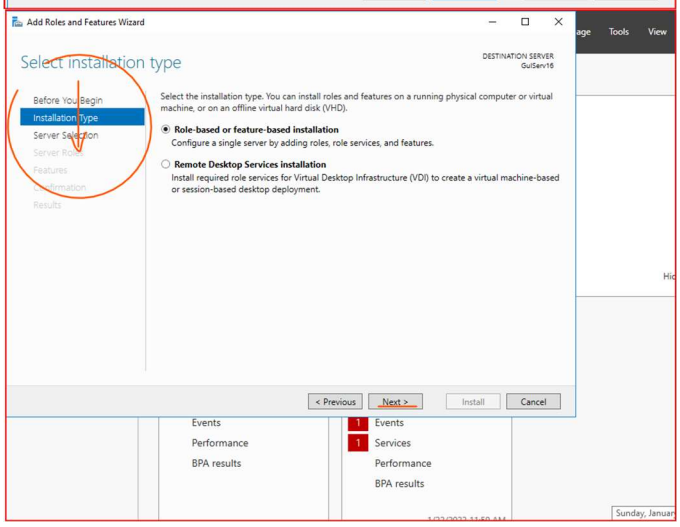
Follow the link to learn how to install AD DS by using Server Manager:
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100-#BKMK_GUI

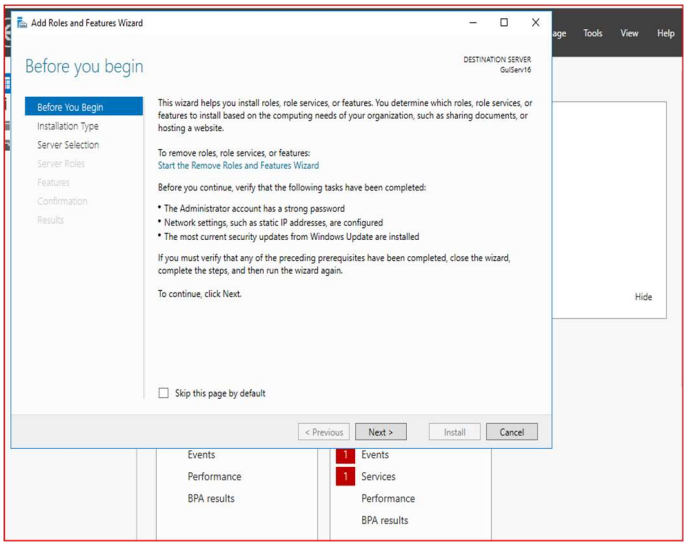




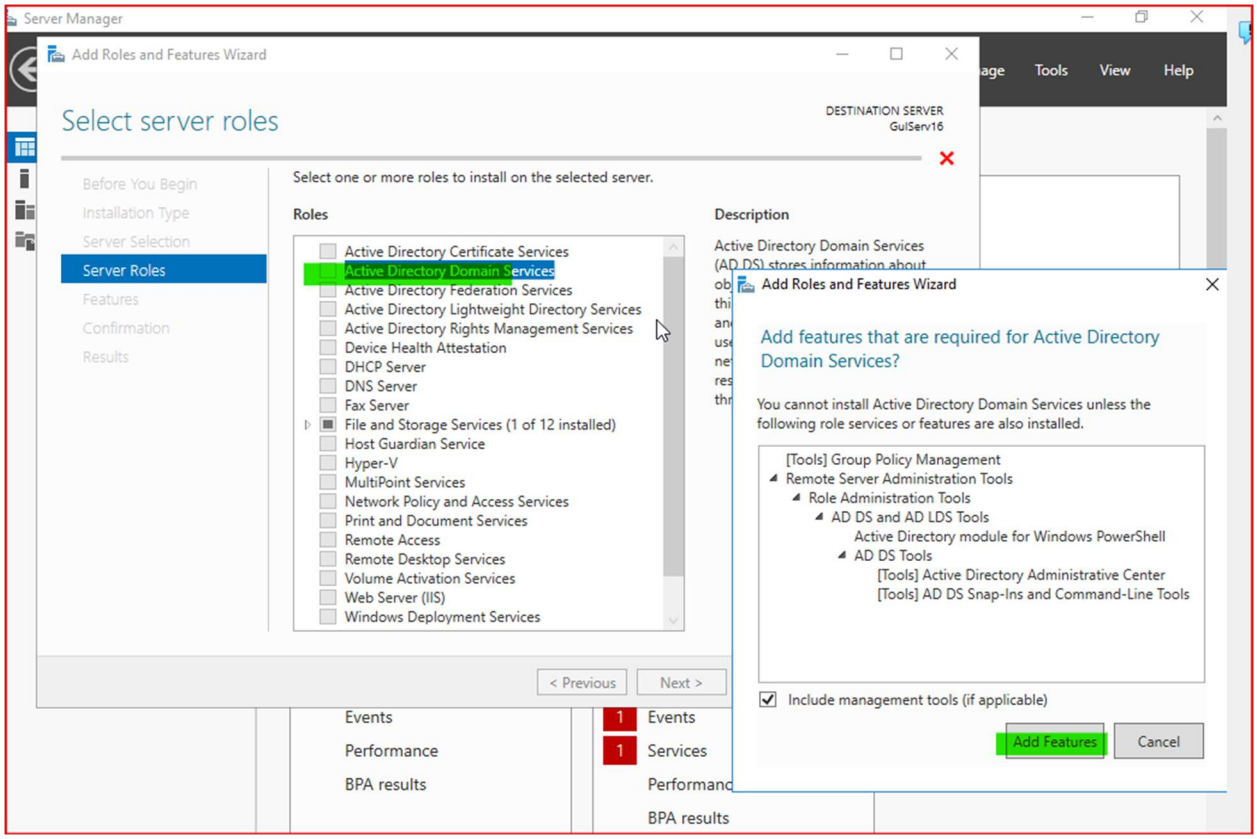
In Server Manager, click **Manage** and click **Add Roles and Features** to start the Add Roles Wizard.


Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
GulServ16
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
GulServ16
192.168.1.2
Microsoft Windows Server 2016 Standard Evaluation
1 Computer(s) found
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel

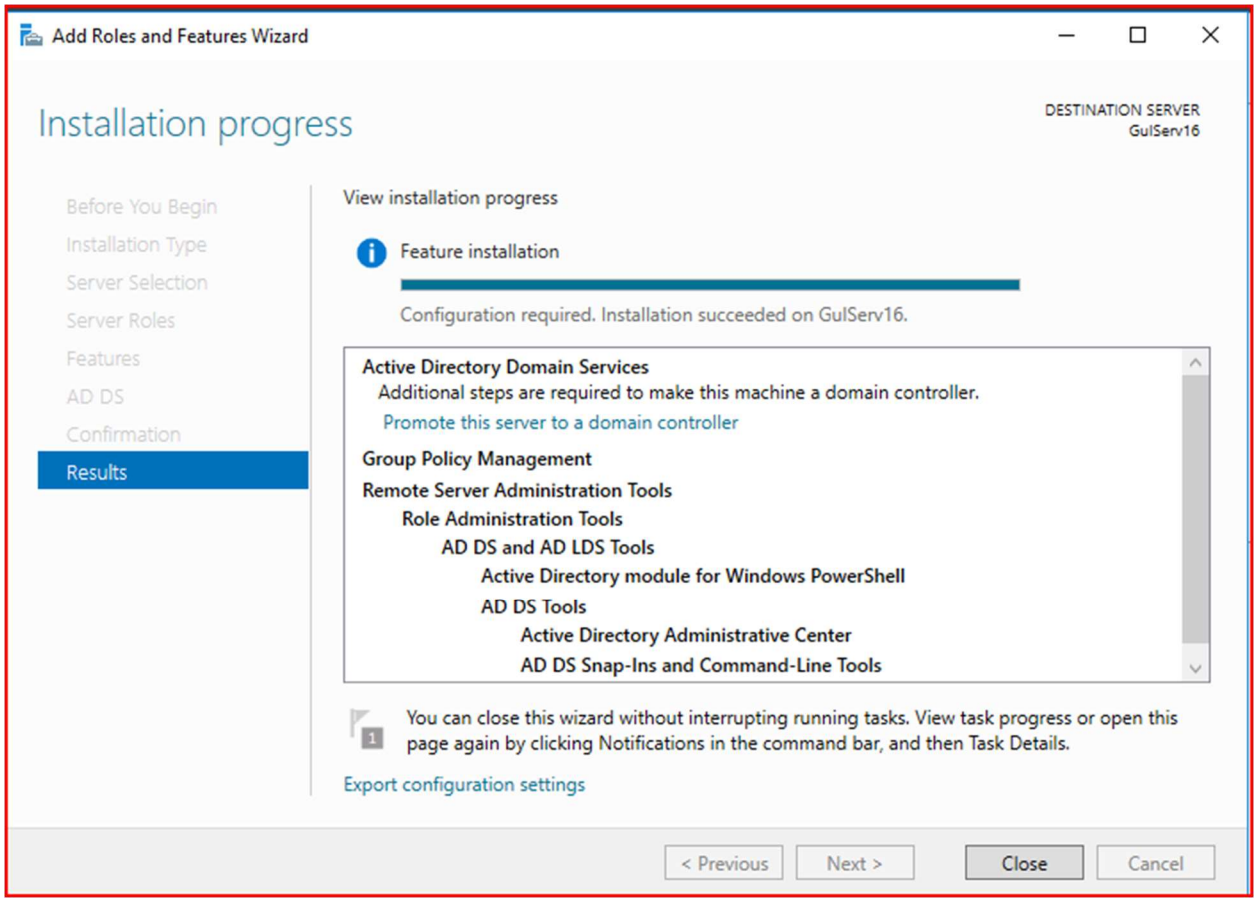

Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
GulServ16
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel
Tools
View
Events
Performance
BPA results
Services
Sunday, Januar


Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
GulServ16
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.
To remove roles, role services, or features:
Start the Remove Roles and Features Wizard
Before you continue, verify that the following tasks have been completed:
* The Administrator account has a strong password
* Network settings, such as static IP addresses, are configured
* The most current security updates from Windows Update are installed
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.
To continue, click Next.
Skip this page by default
< Previous
Next >
Install
Cancel
Tools
View
Help
Hide
Events
Performance
BPA results
Services

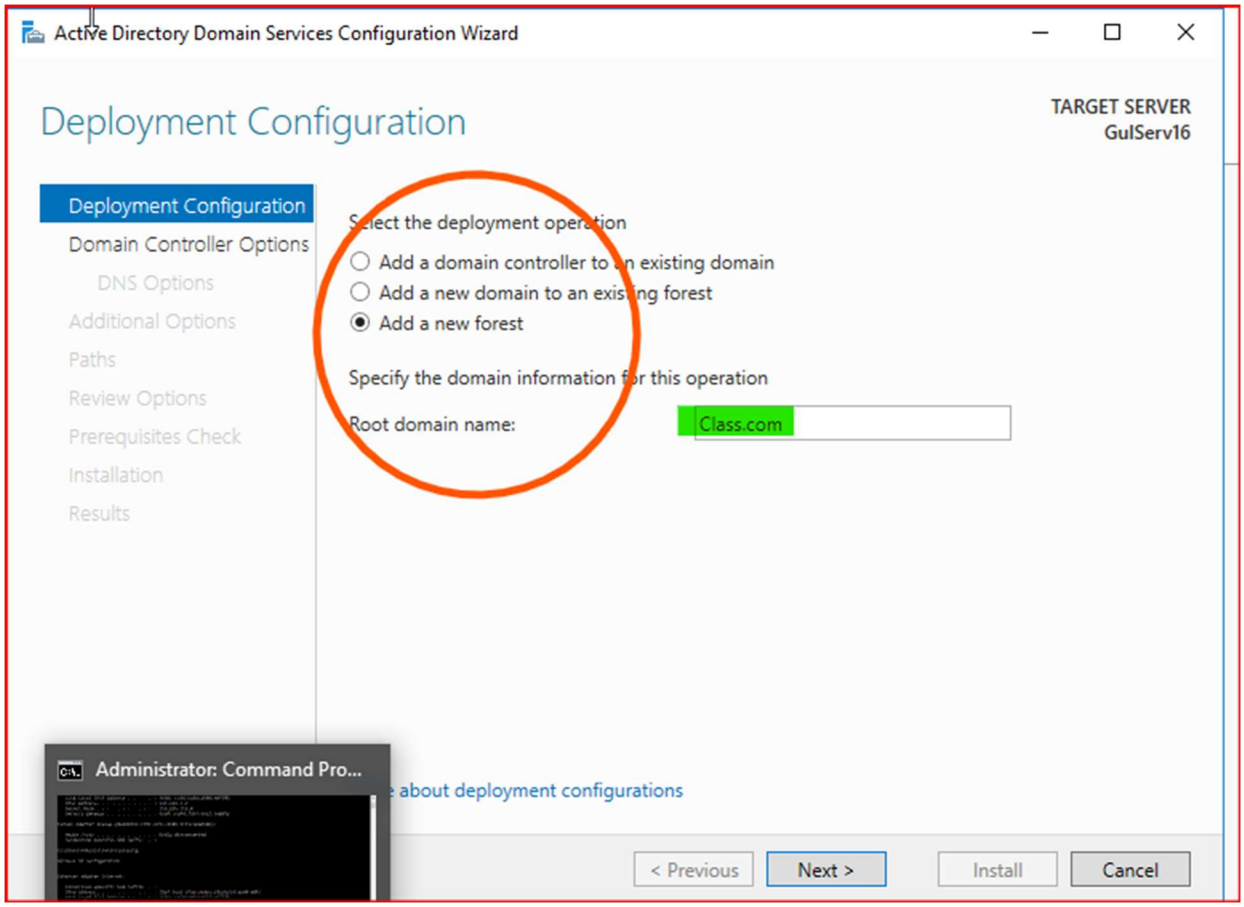
Click **Next>**



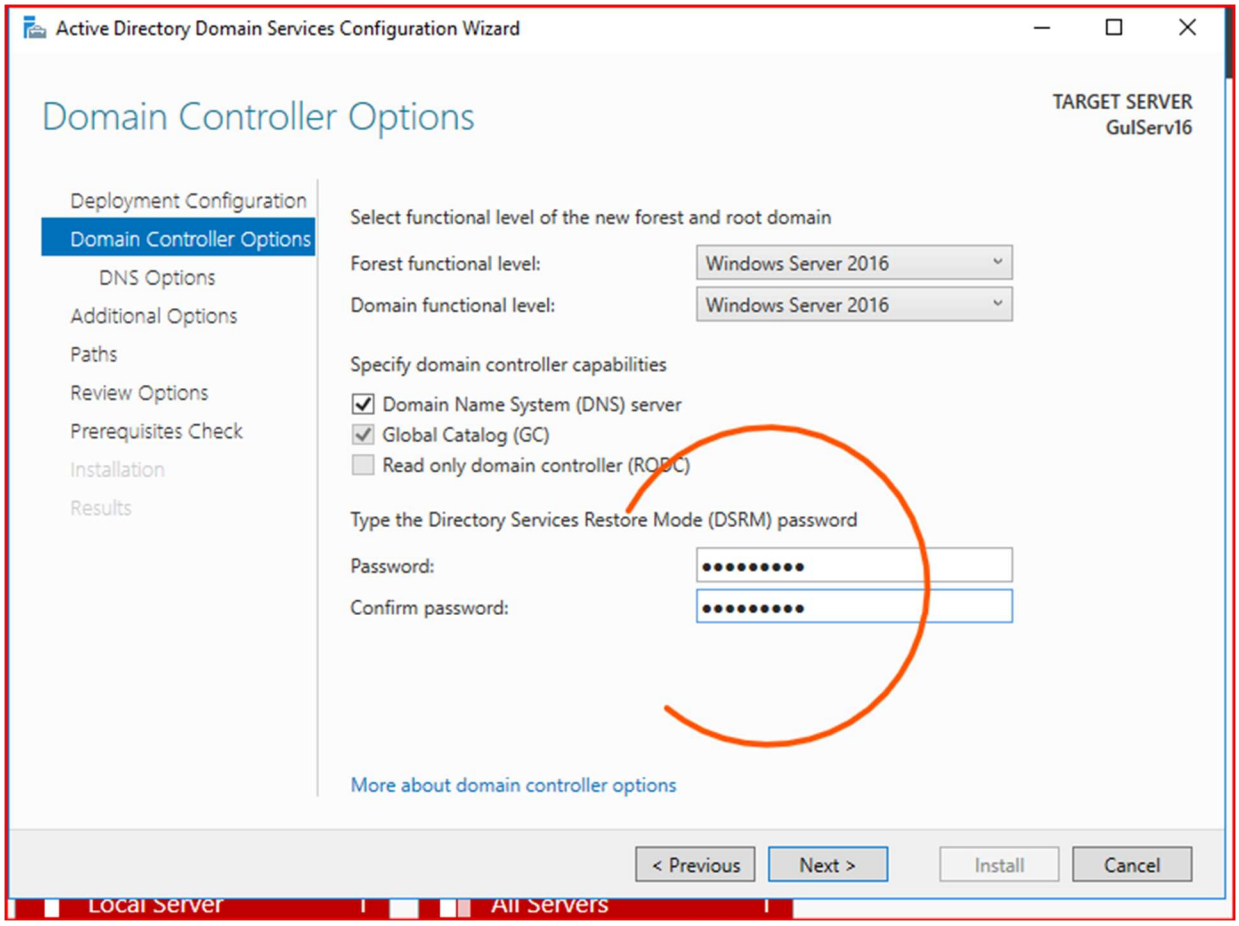
Click **AD DS>** pop-up **Add Features> Next> NET Framework> Next>** It will prompt to install DNS. Click **Next> Install>**



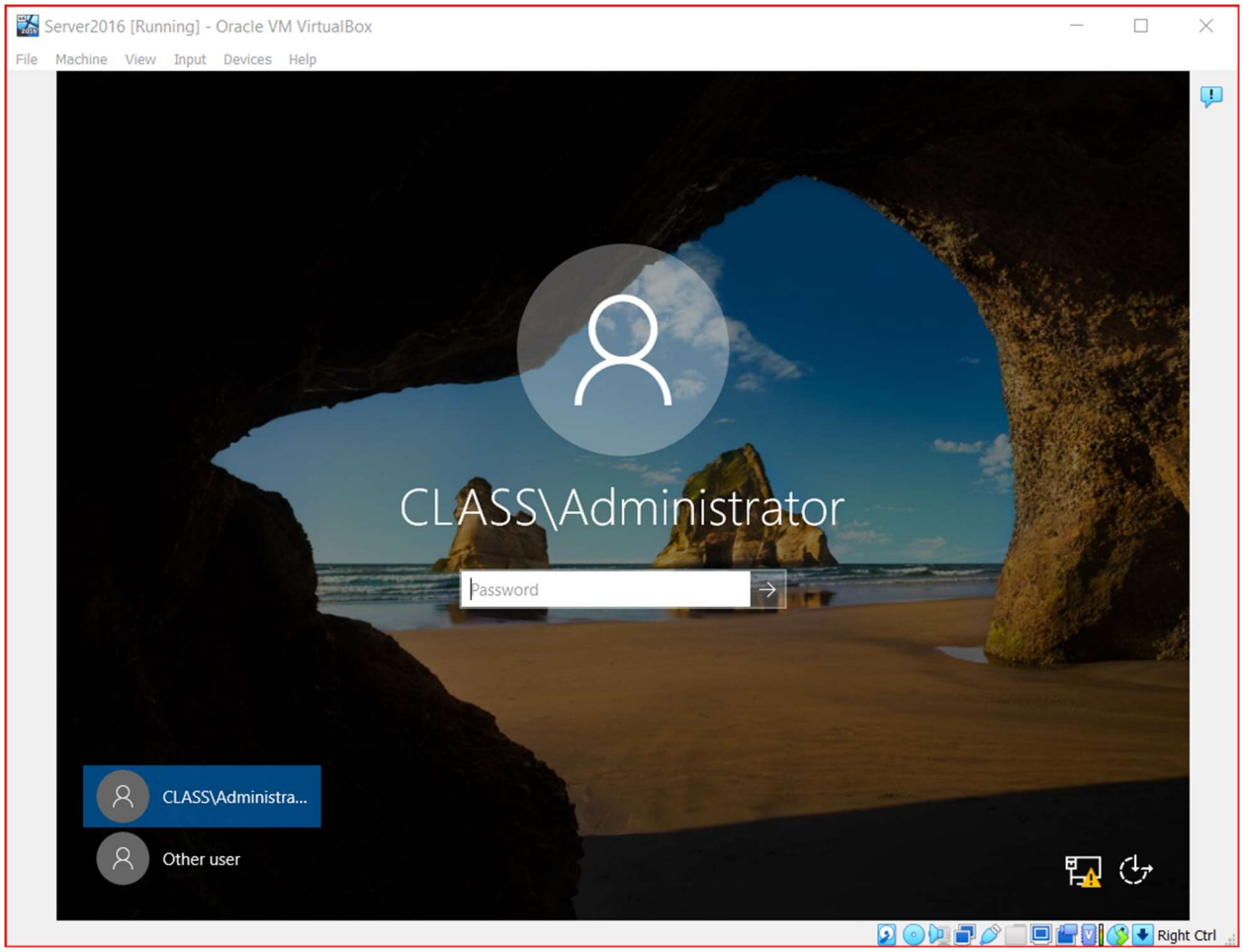
Manager is promoting **this server to a domain controller**. Double click to accept.



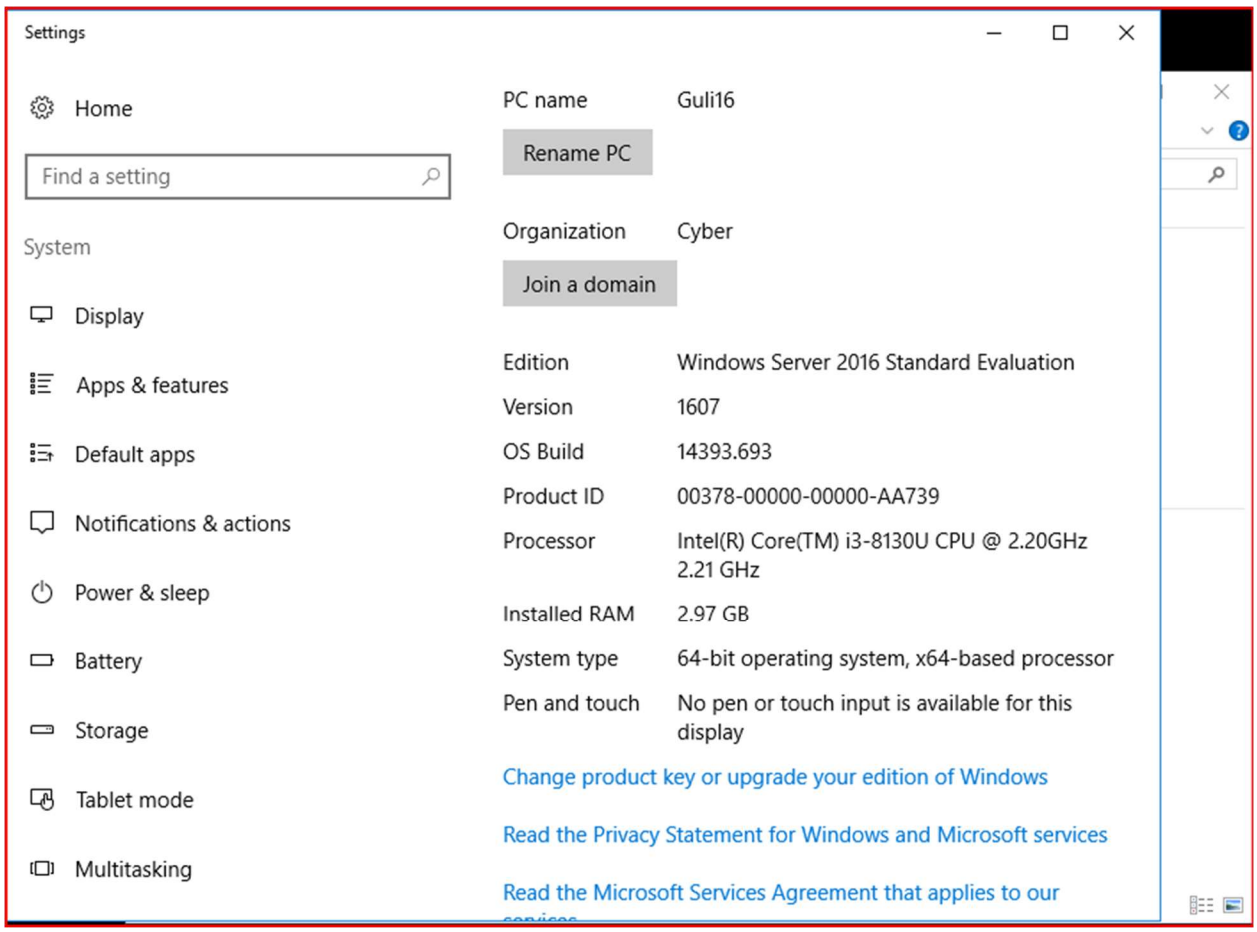
Enter domain **Class.com**



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

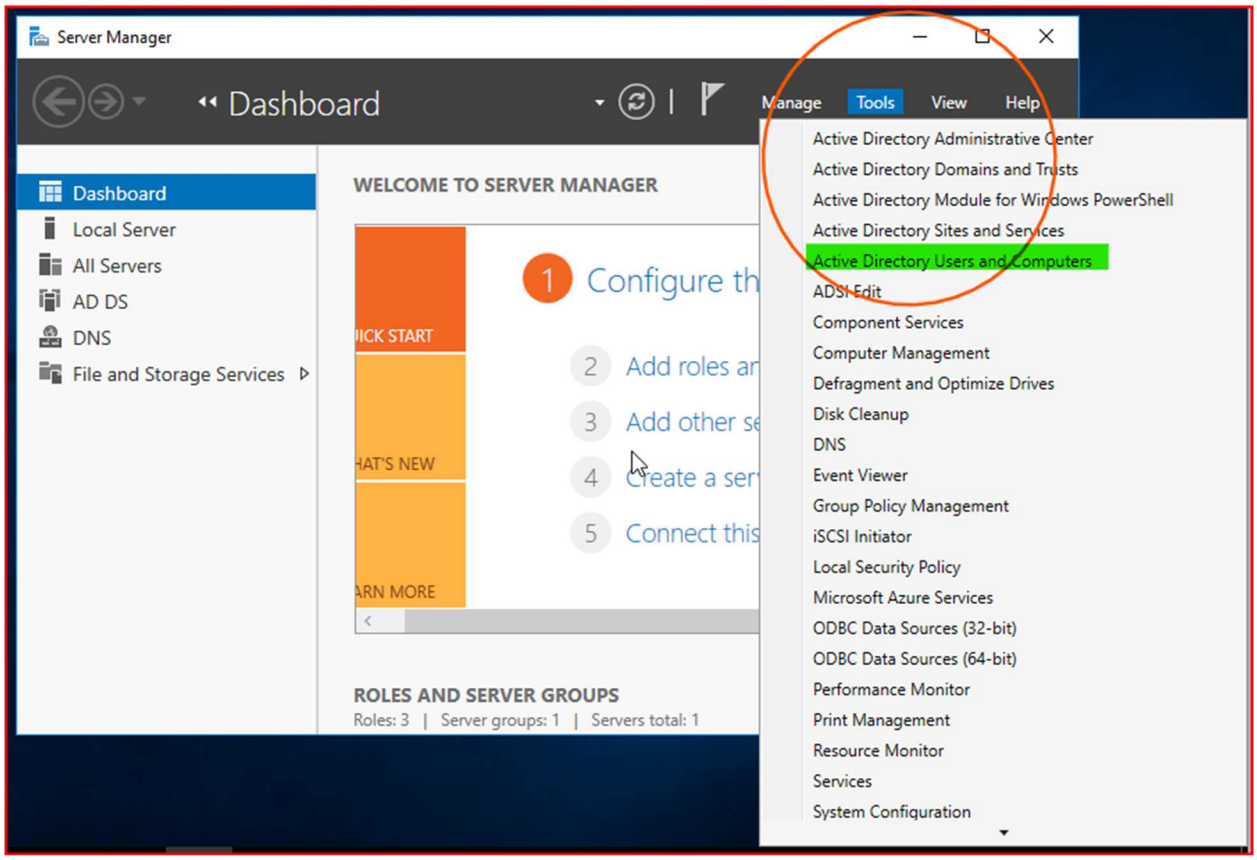


AD DC installed successfully.

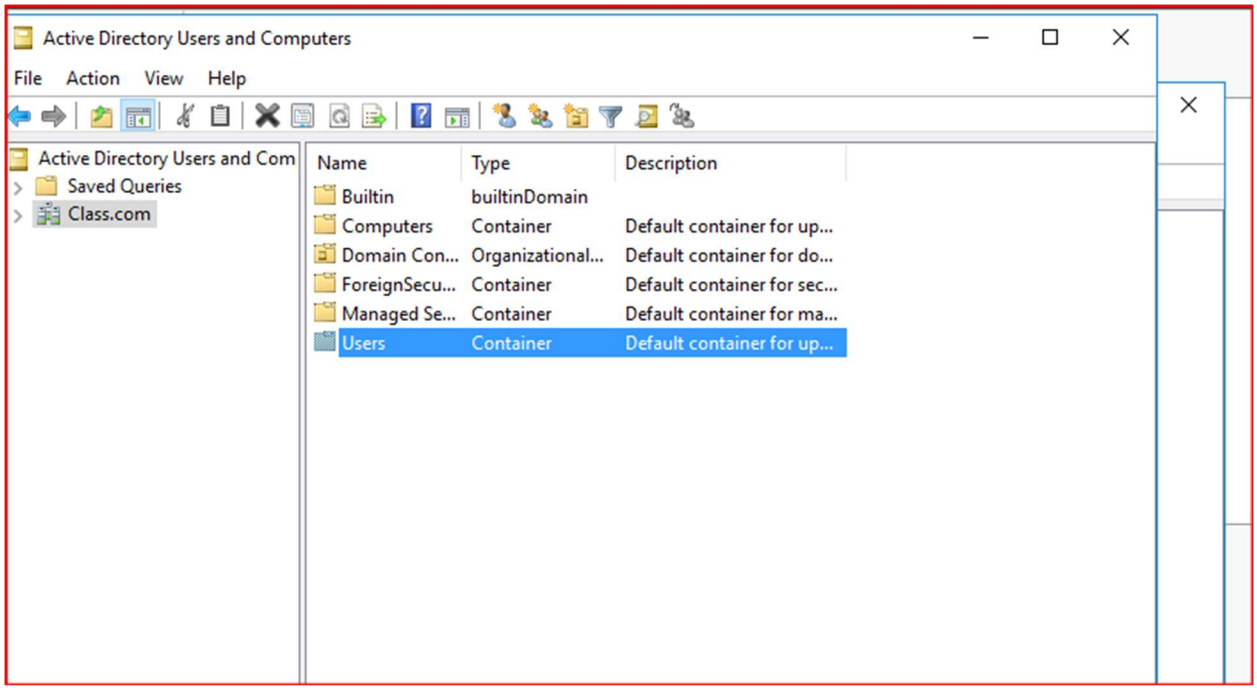


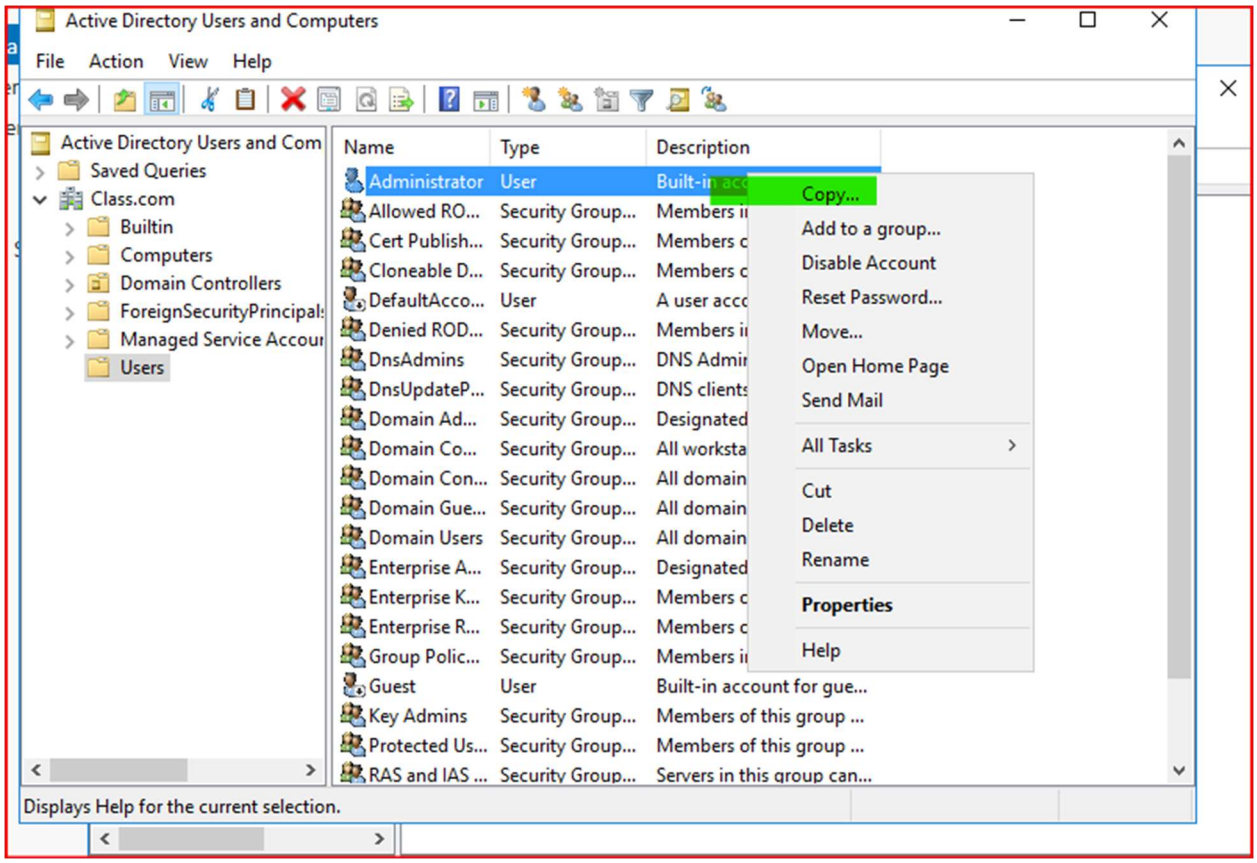
The latest version of Server 2016.

Create Users

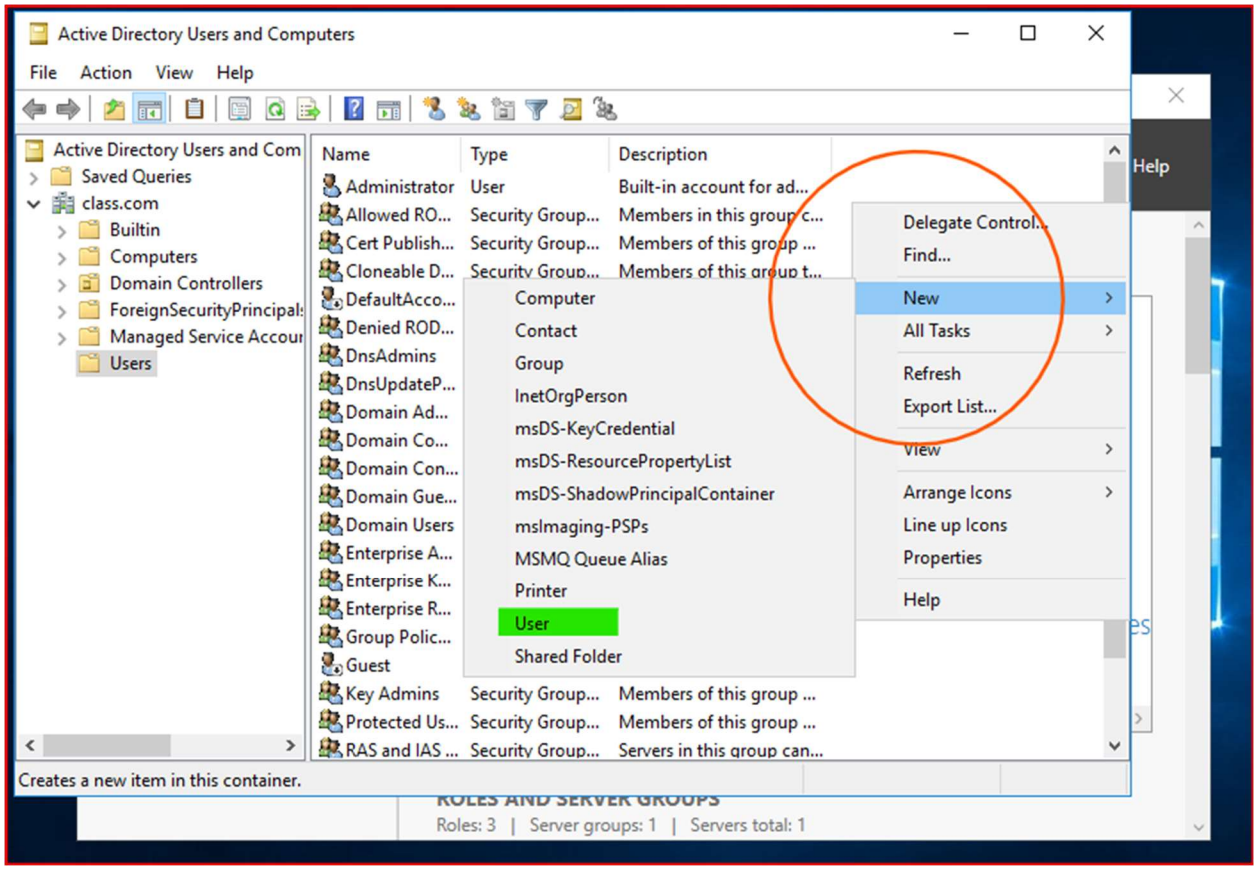


Under **“Tools”** on the Server Manager open **“Active Directory Users and Computers”**

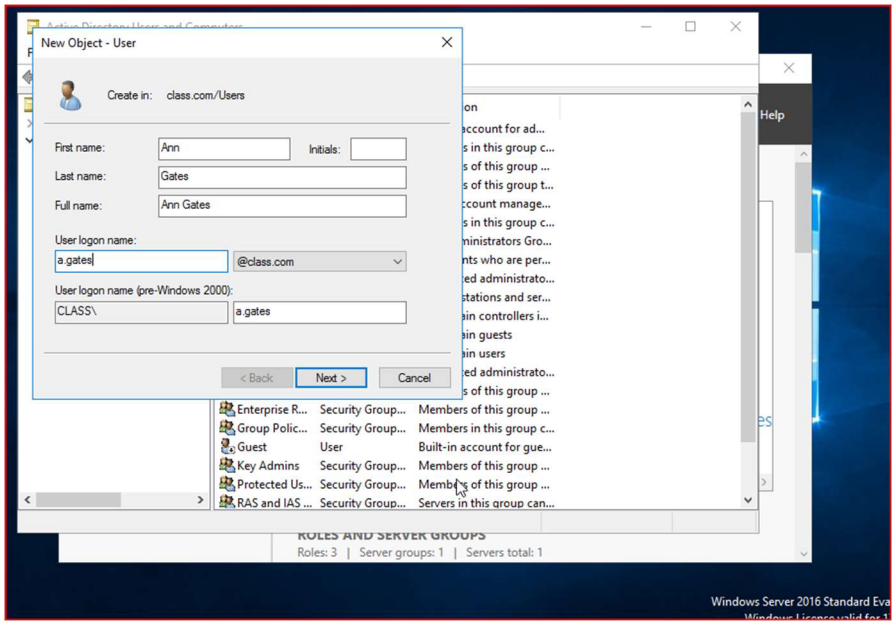




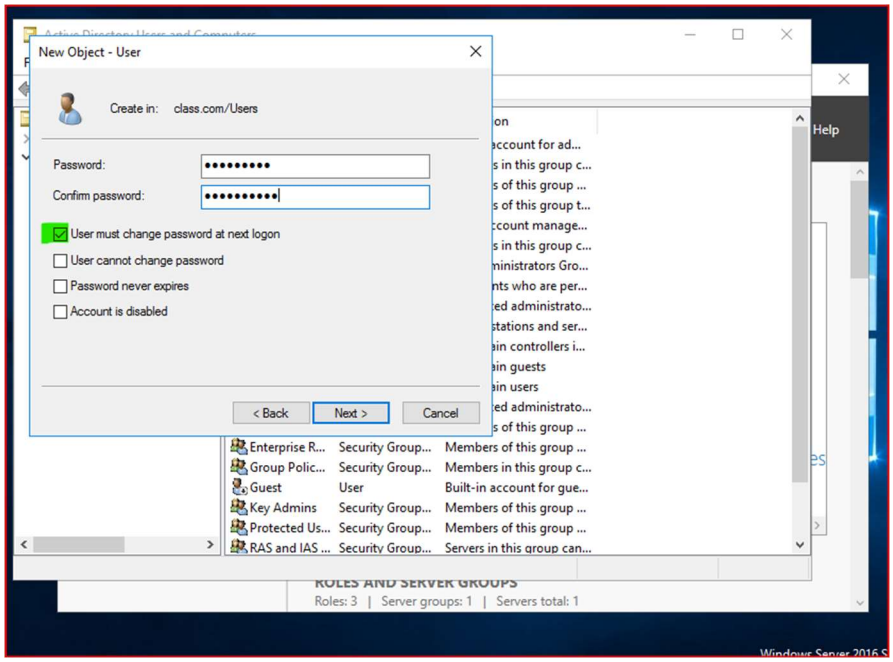
If you want to create a new user with administrator properties (or with any other group policy) right click on the user and "**Copy**"

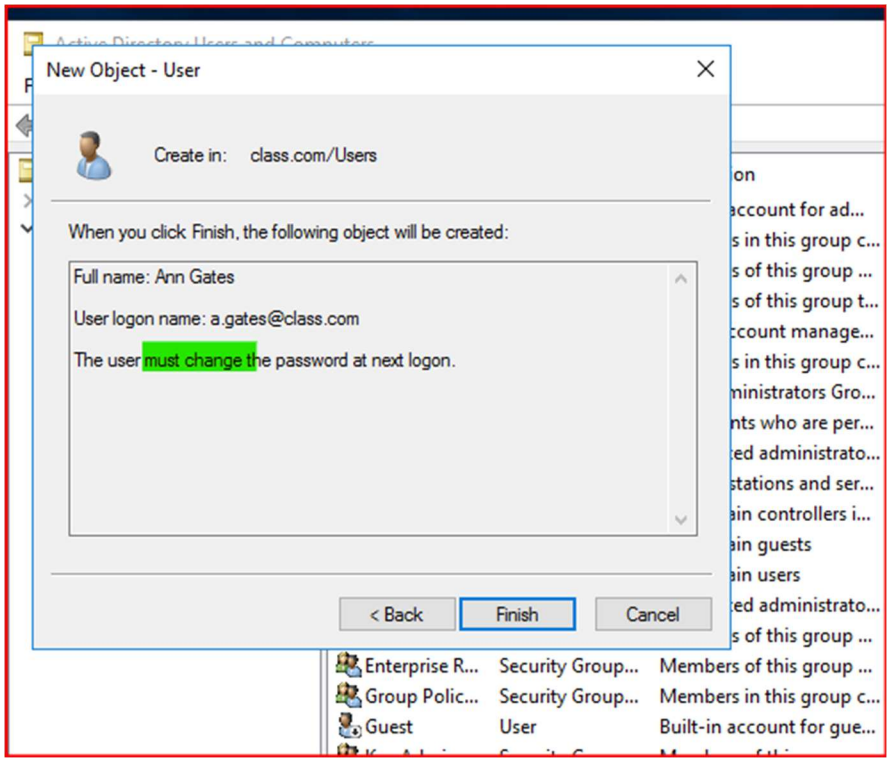


Or **right click>New>User**



Give it name and create a password.





"Finish" adding Users

LAB WORK 3 COMPLETED

LAB WORK 4

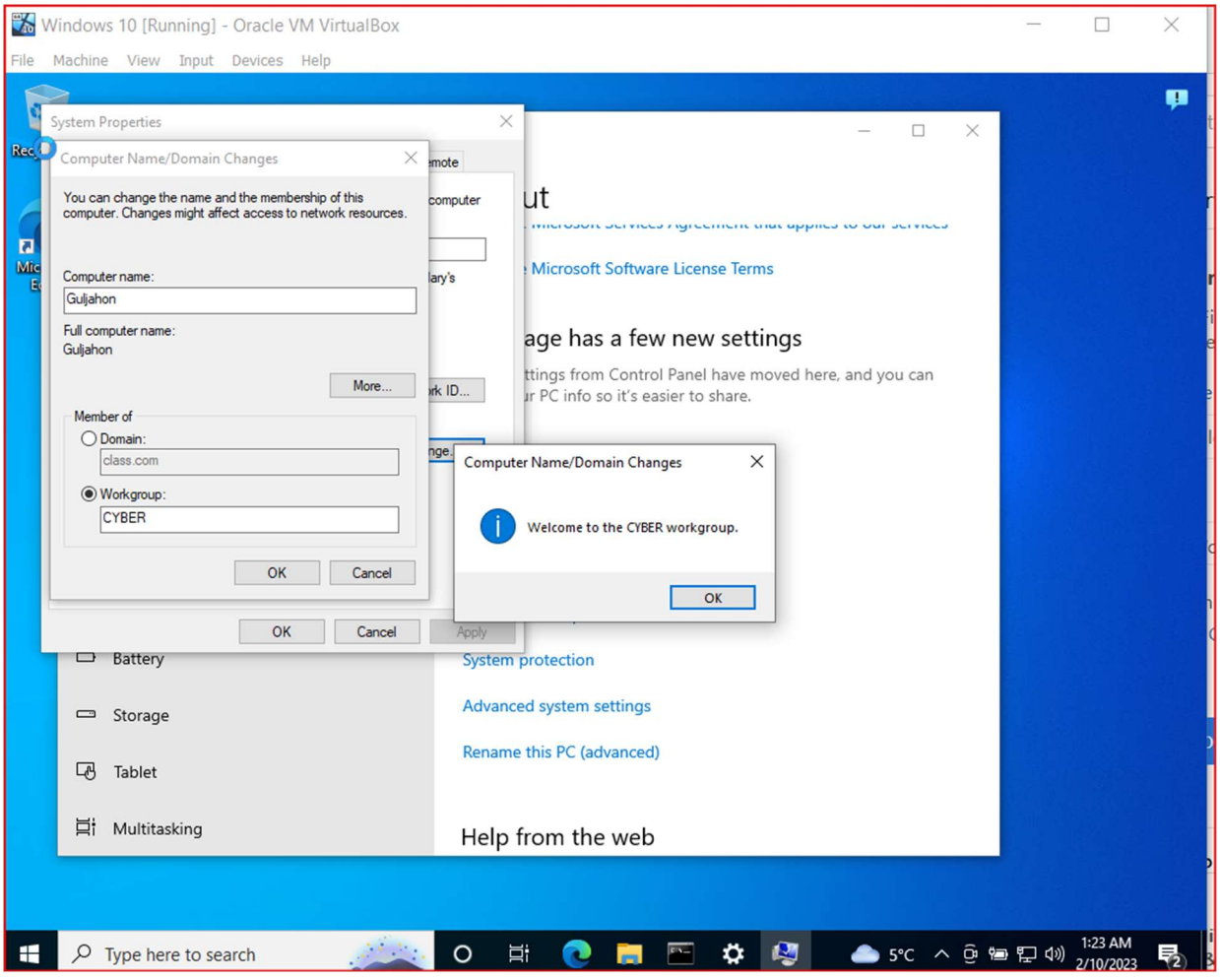
Join Domain Controller

- ✓ **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.

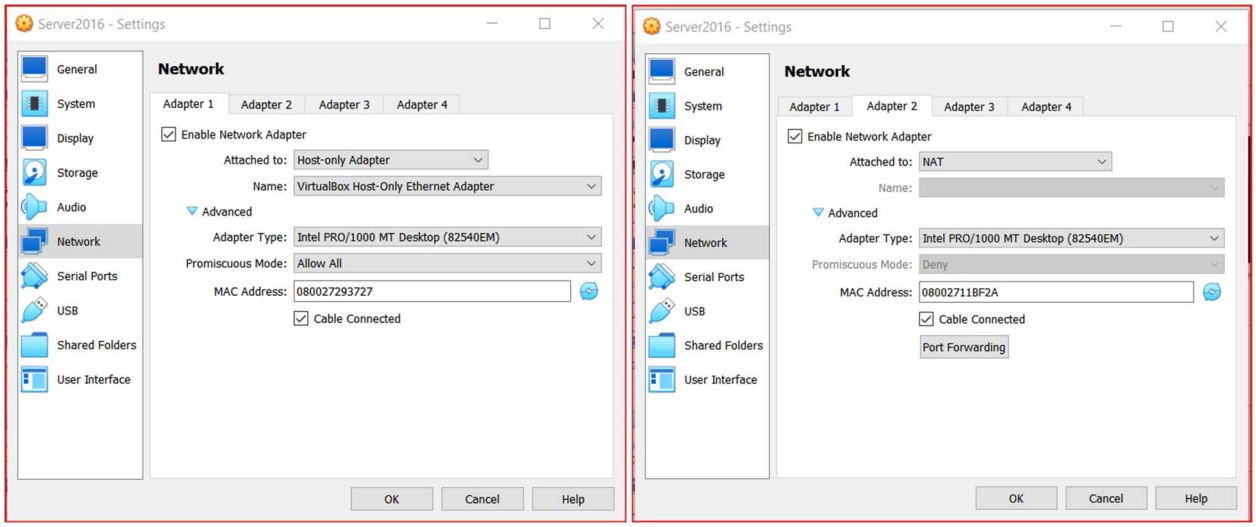
Below you will see the final screenshots of successfully joining domain controller.



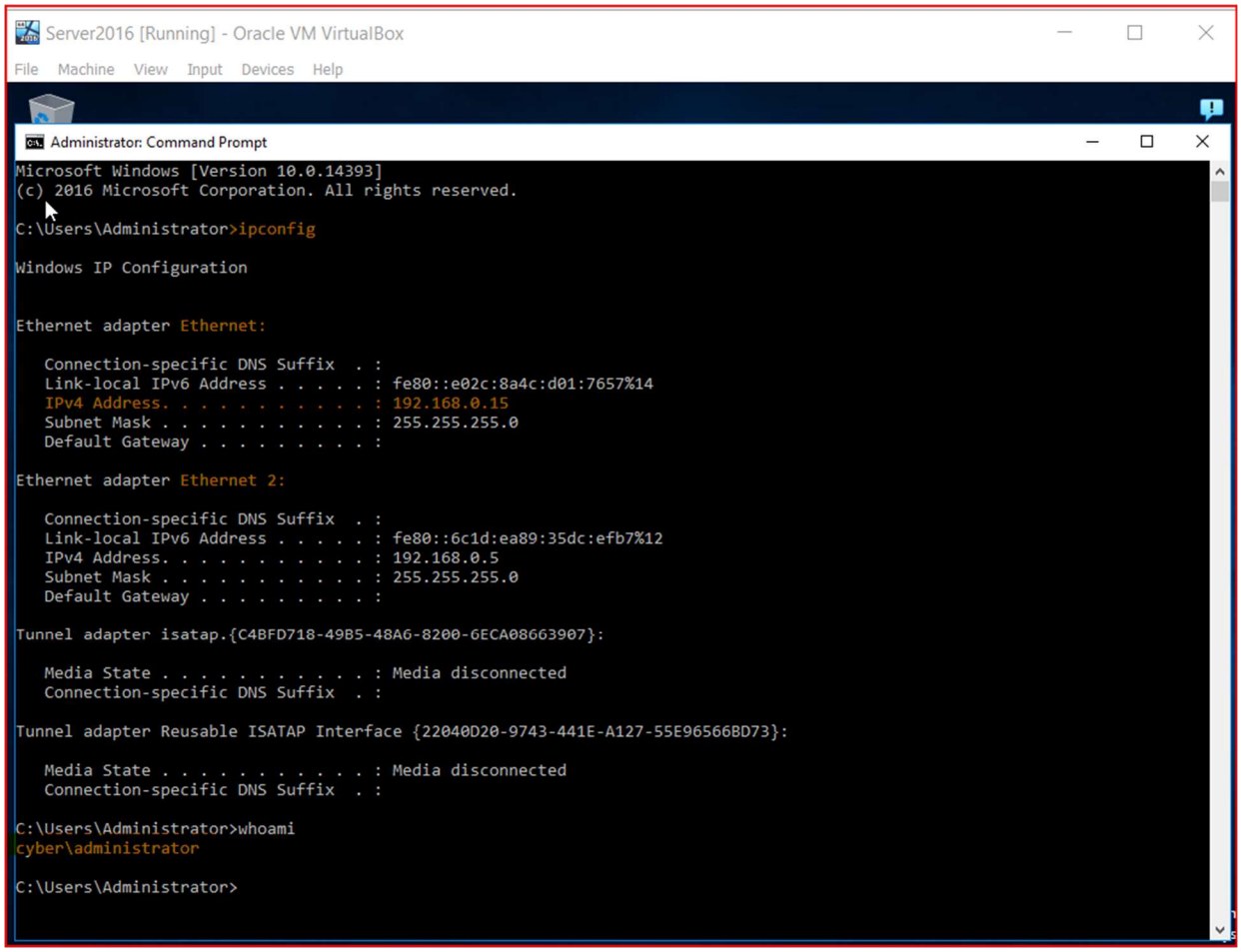
LAB WORK 4

Join Domain Controller

- ✓ **Windows Server 2016**



Windows 2016 server's Network configuration.

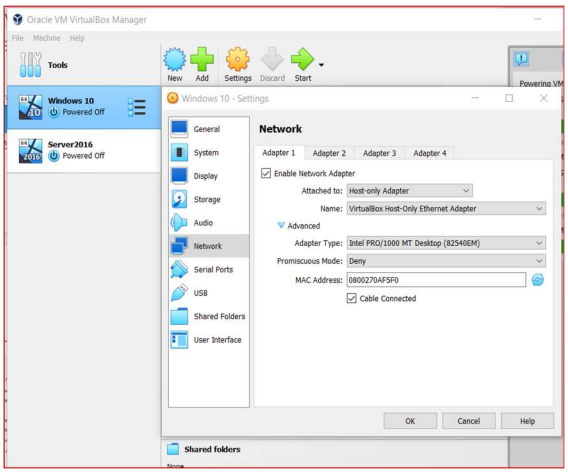


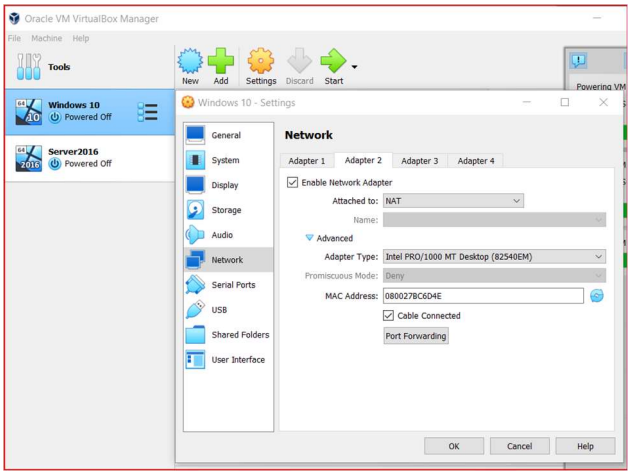
Static IP address assigned.

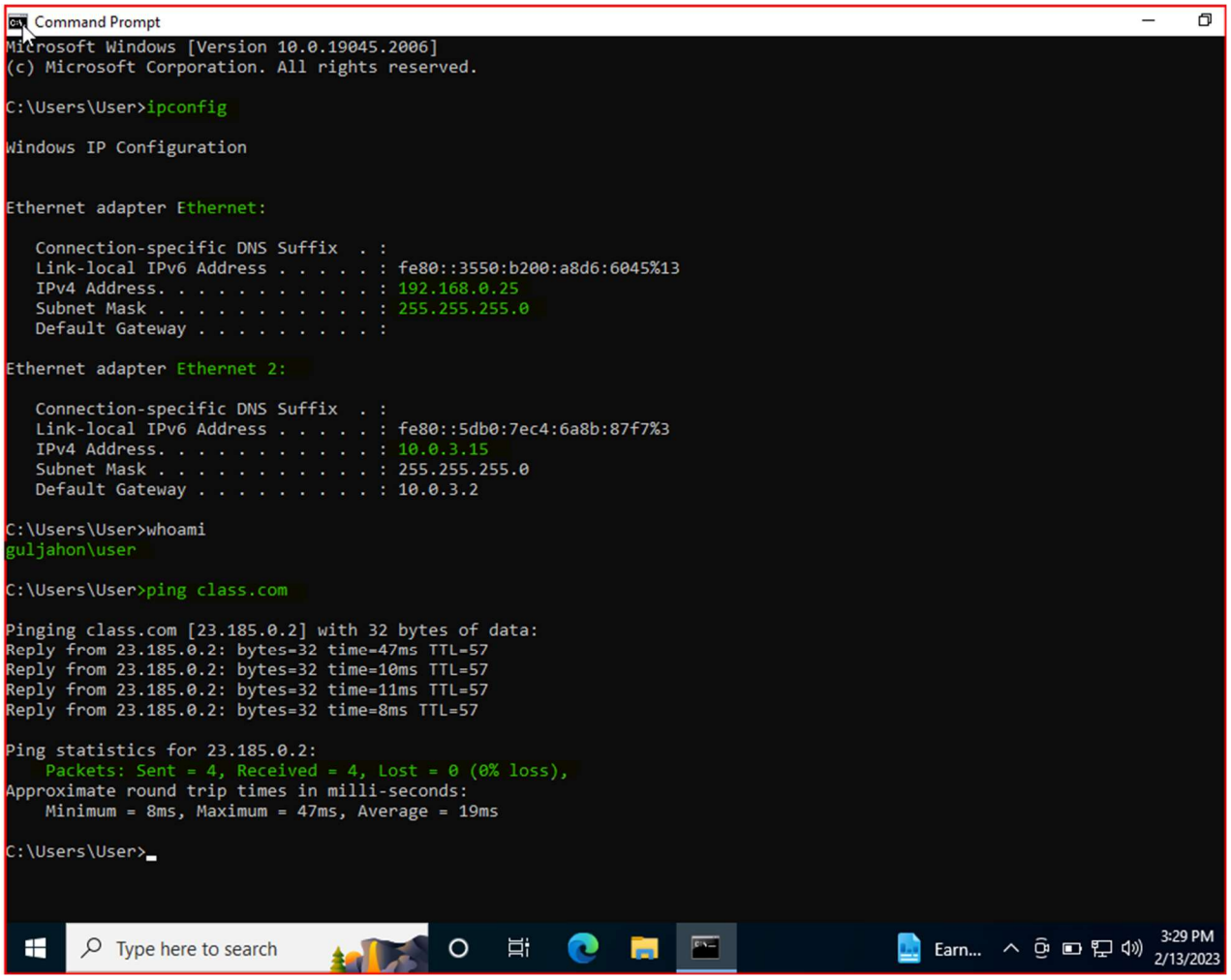
LAB WORK 4

Join Domain Controller

- ✓ **Windows 10 client**



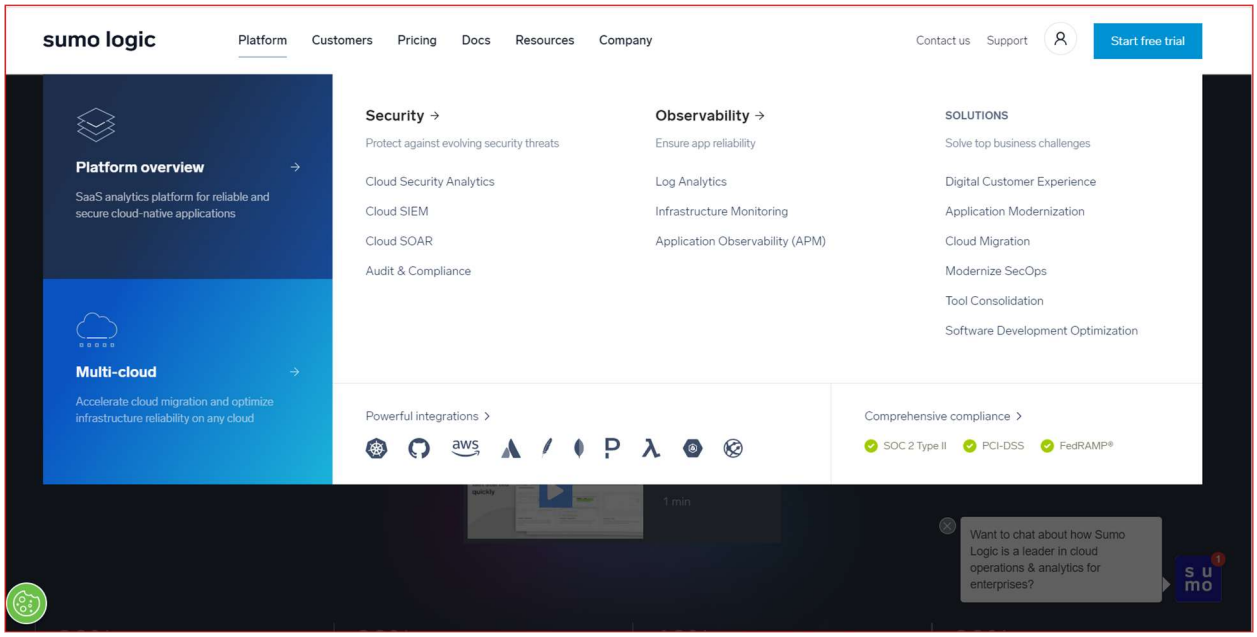




Static IP assigned.

SUMOLOGIC

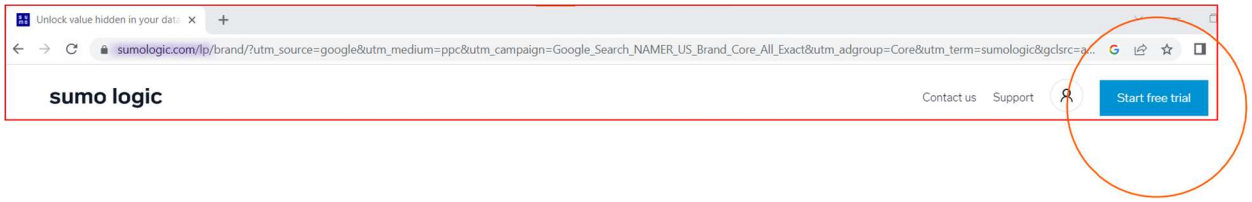
- ✓ **Authorization**
- ✓ **Installation**
- ✓ **Data Parsing**
- ✓ **Save the Search**
- ✓ **Configure an Email Alert**



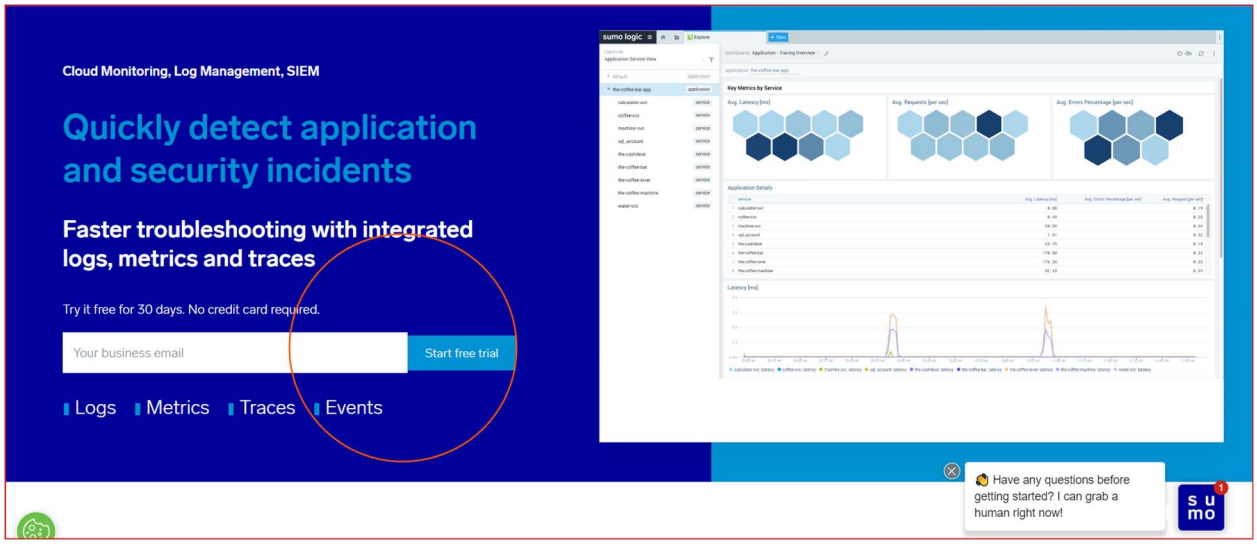
LAB WORK 5
Sumologic

- ✓ **Authorization**

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



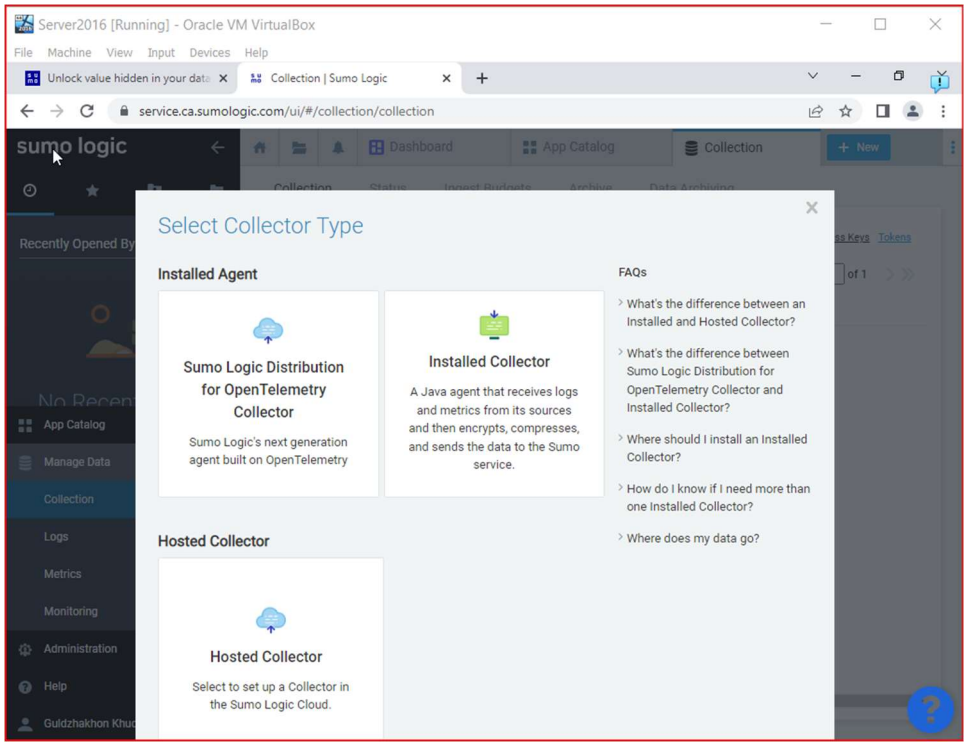
Or:

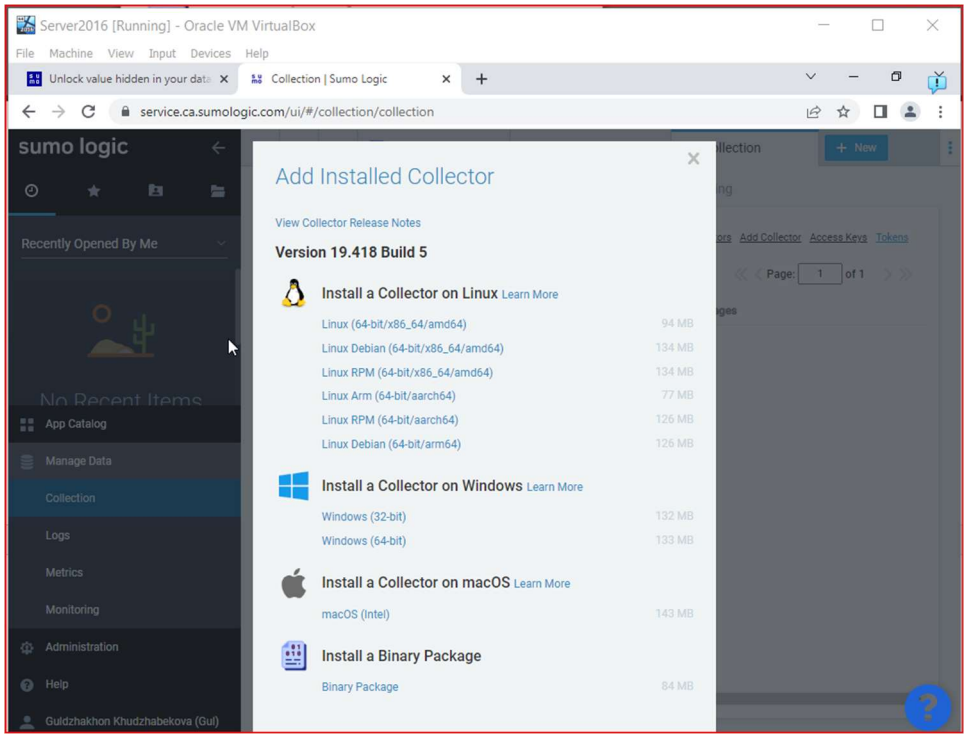


LAB WORK 5

Sumologic

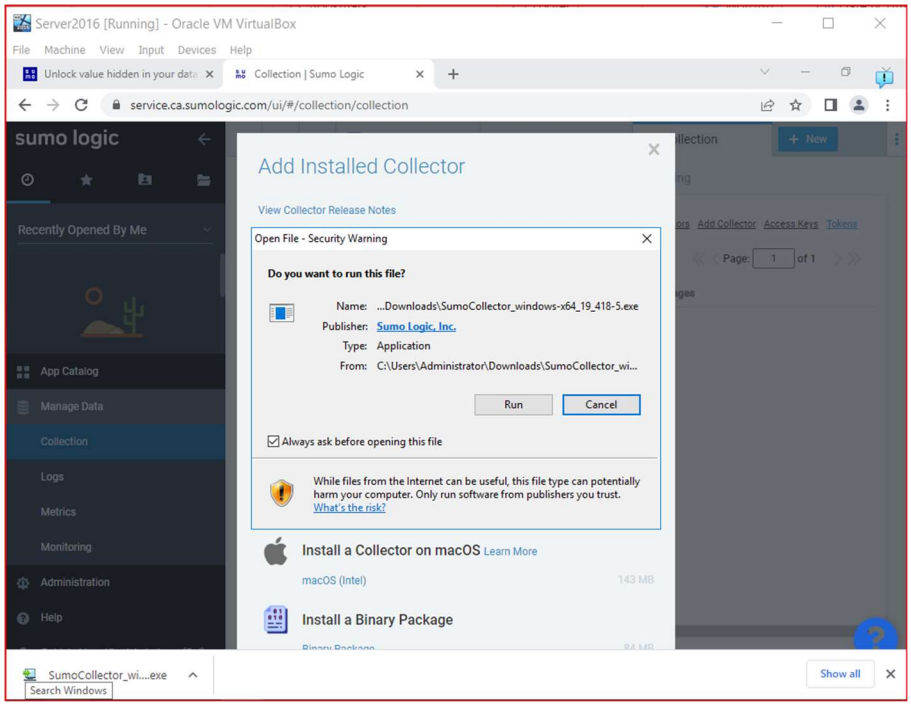
- ✓ **Installation**

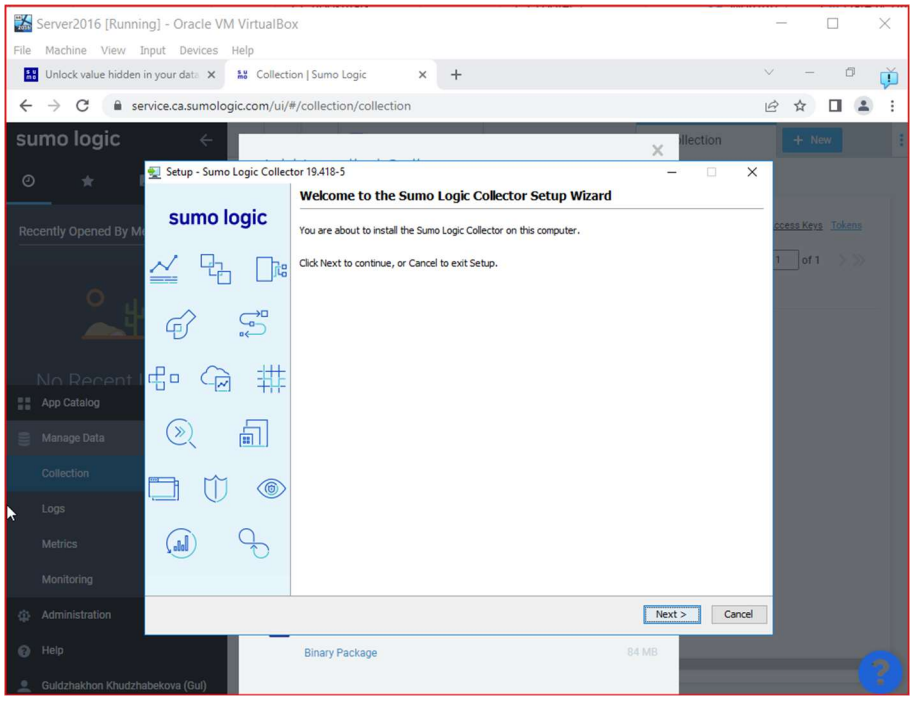




LAB WORK 5

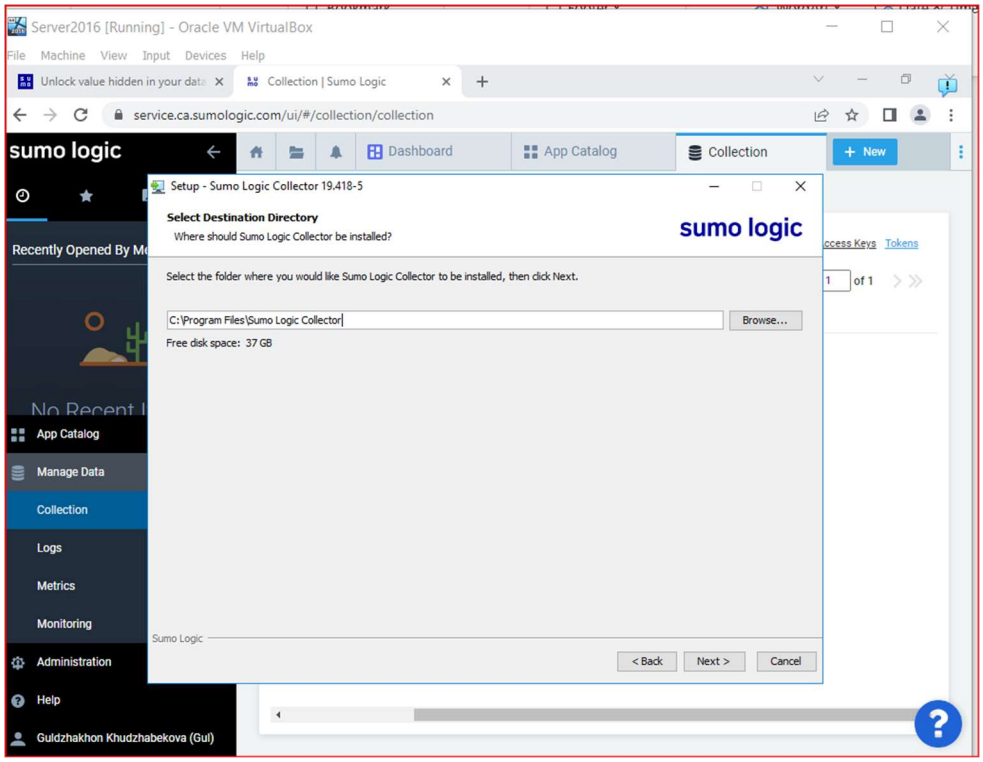
Sumologic

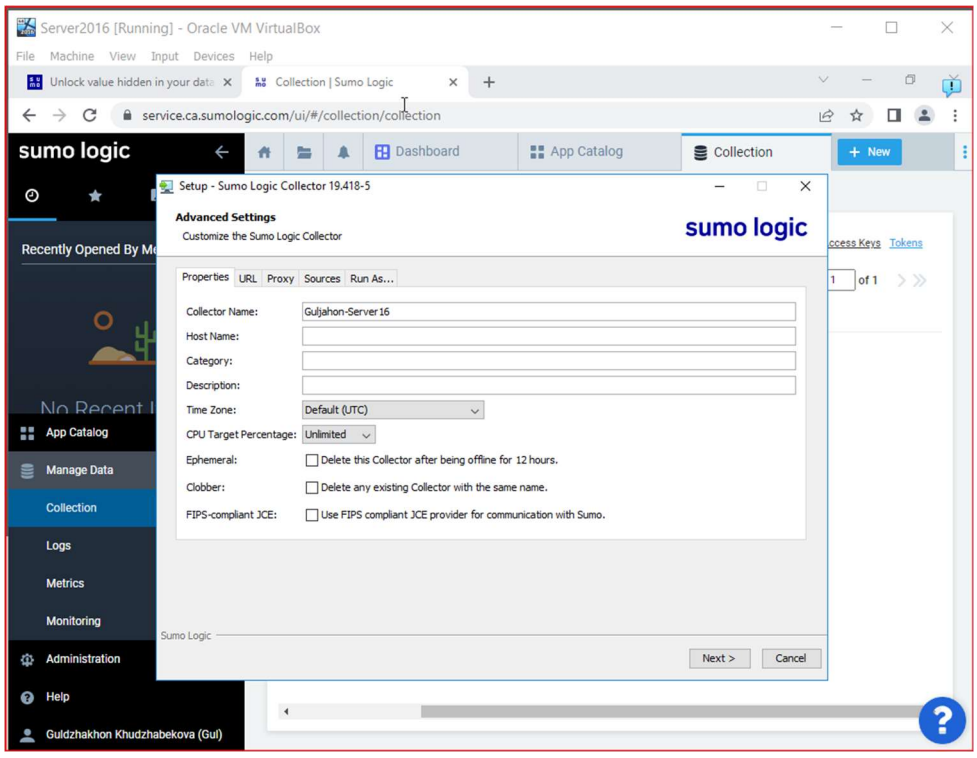




LAB WORK 5

Sumologic

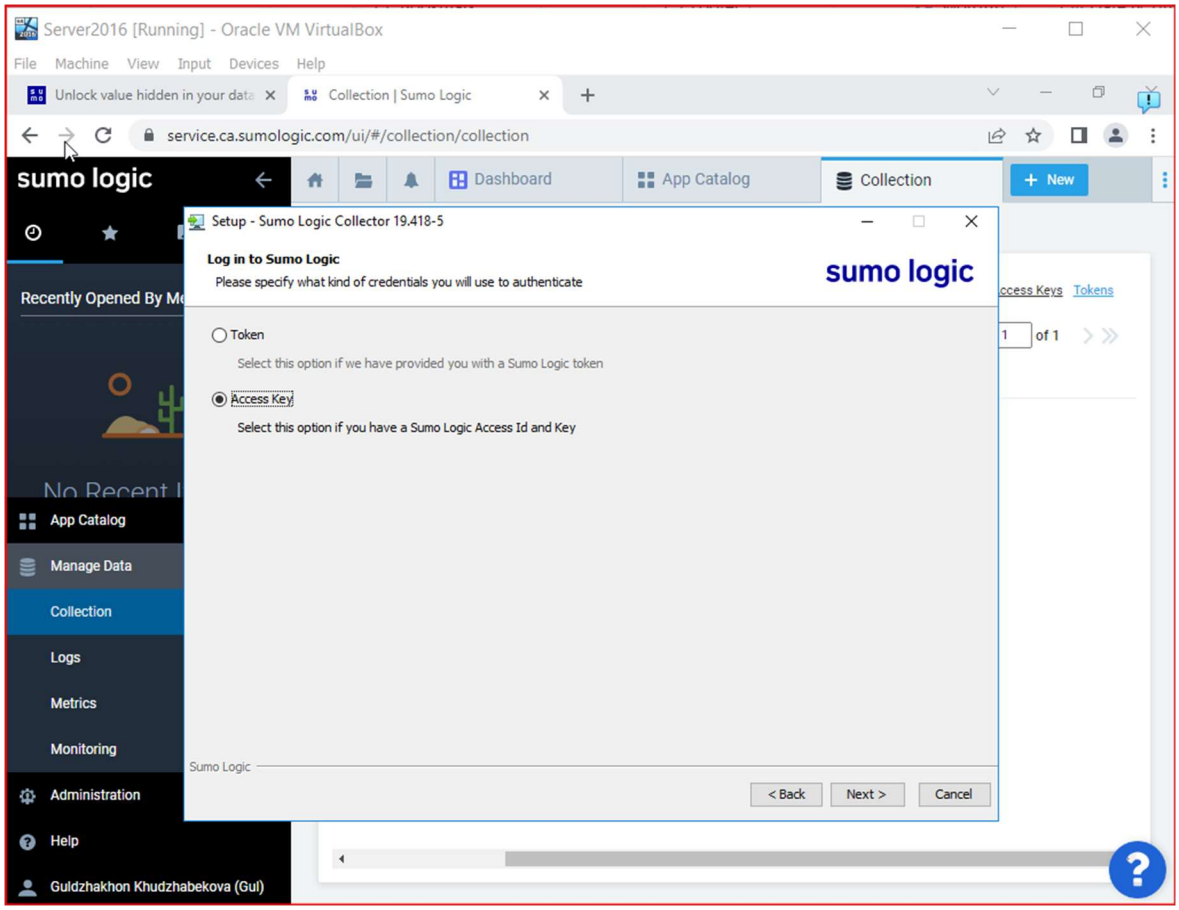




Next>Advanced options>

LAB WORK 5

Sumologic

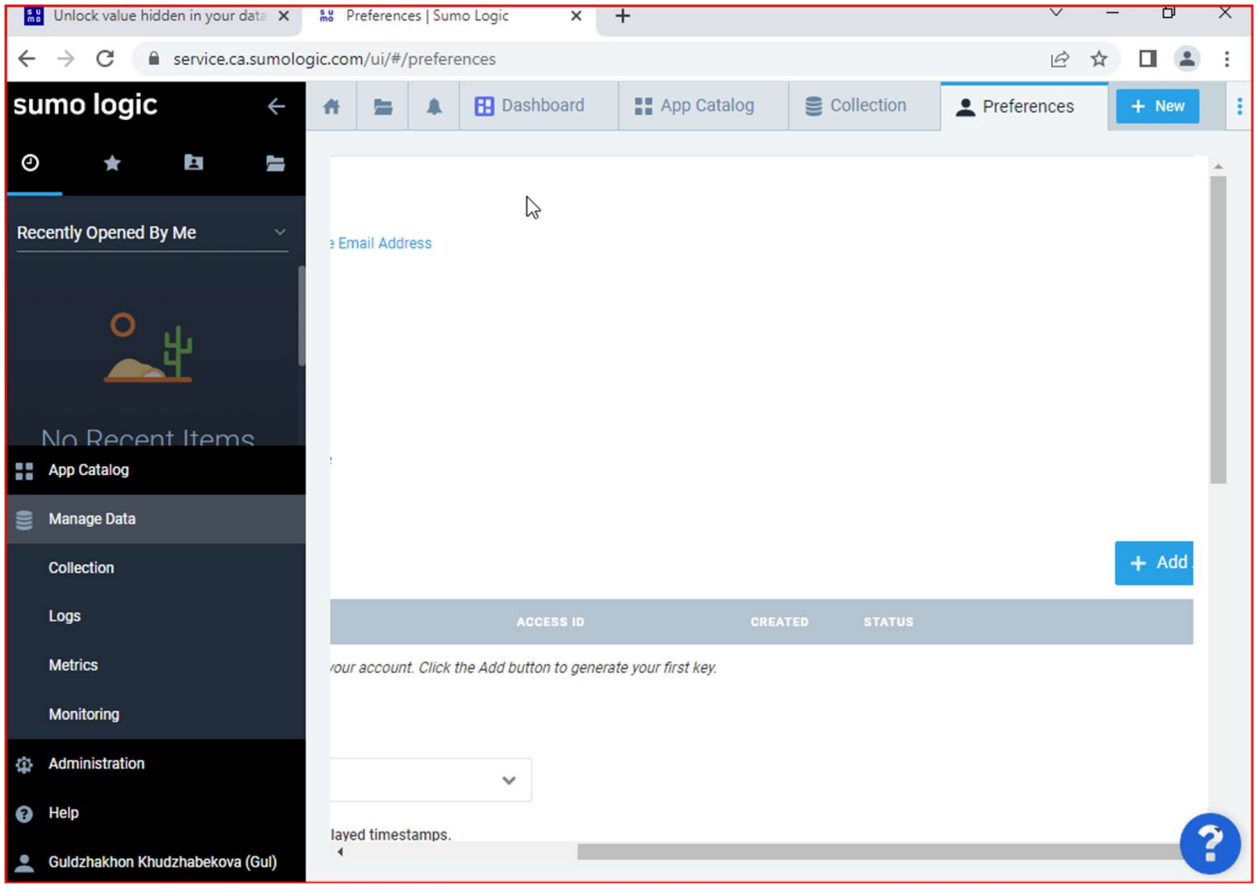


Access Key>Next>

Activate MFA using Google Authenticator

LAB WORK 5

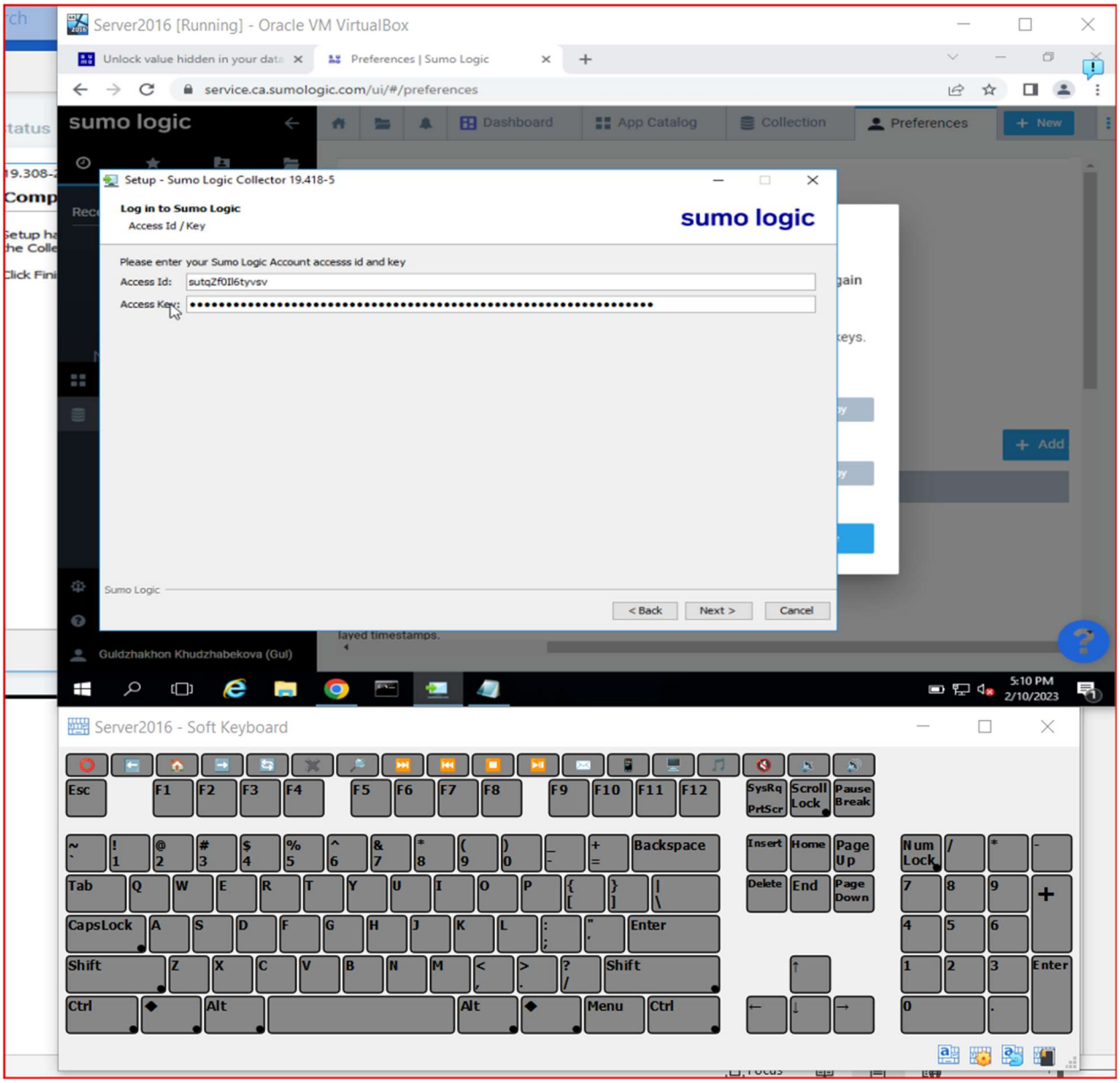
Sumologic



+Add access key

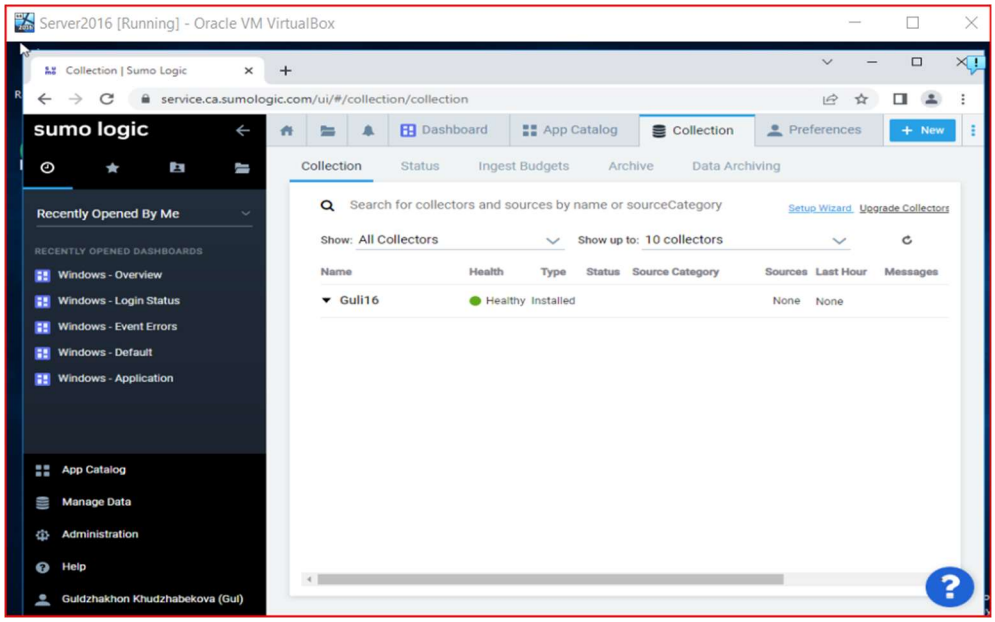
LAB WORK 5

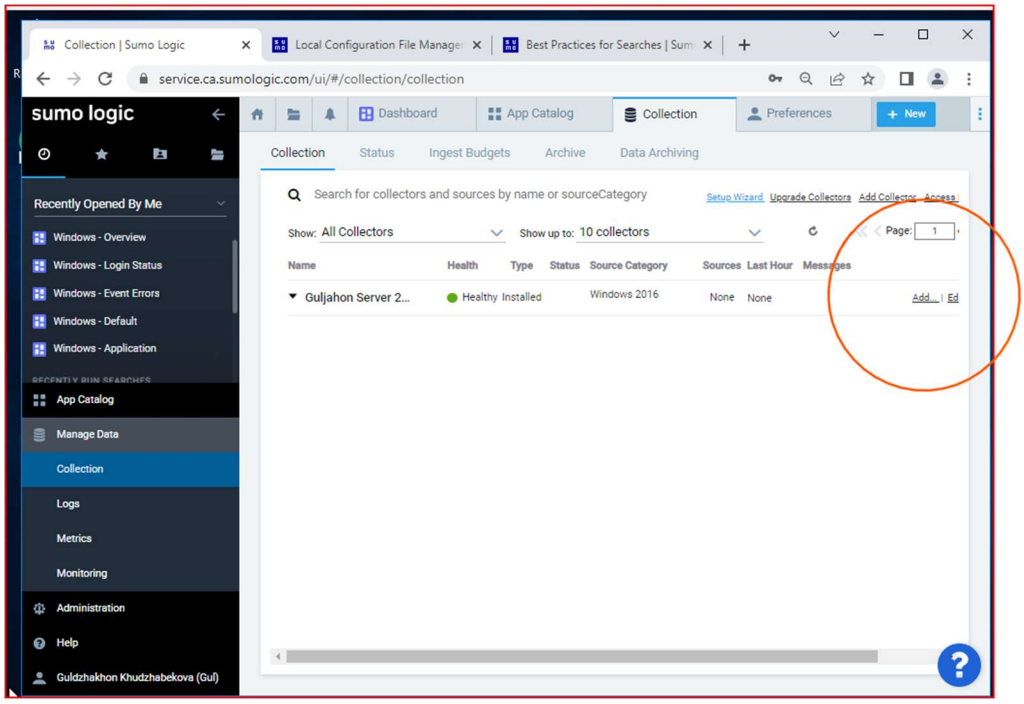
Sumologic



LAB WORK 5

Sumologic

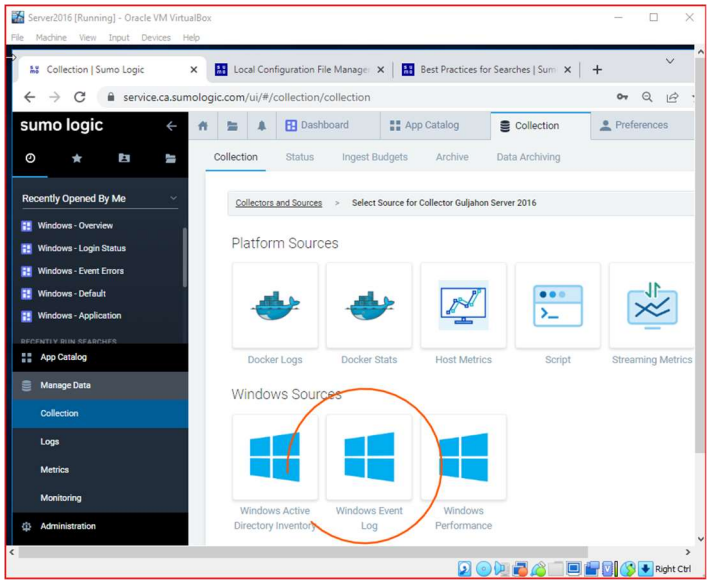


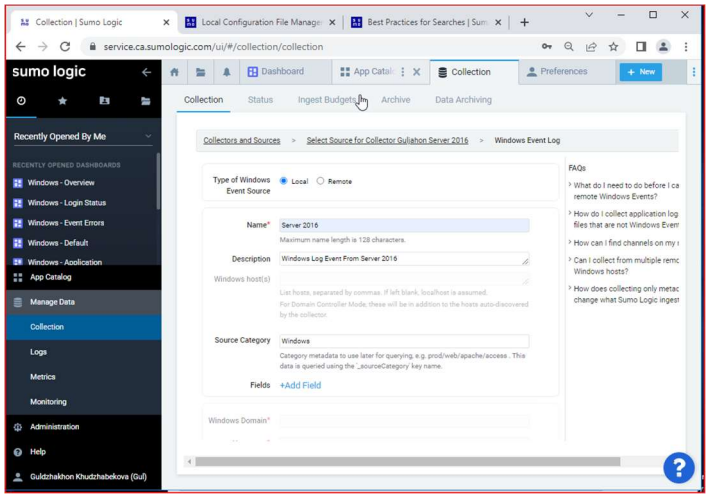


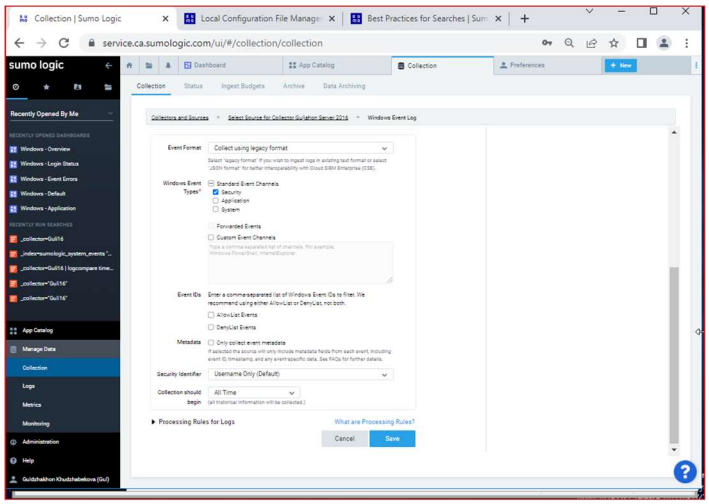
Add Source.

LAB WORK 5

Sumologic





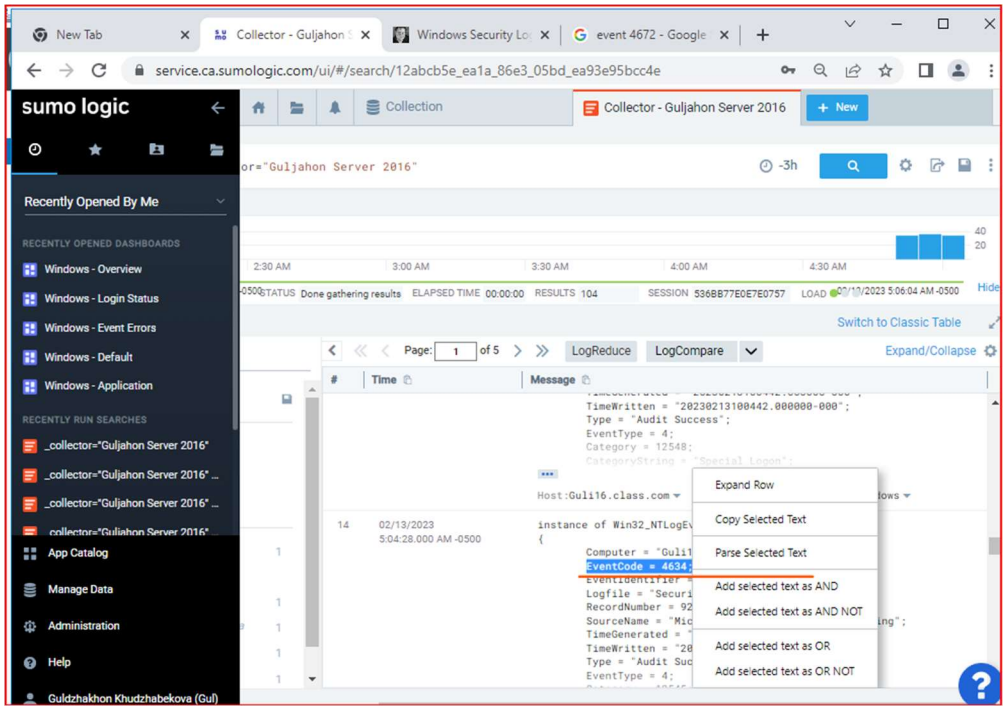


The same procedure for Windows 10 workstation data (Security, Application and Systems) and Windows 10 performance data (CPU, Logical Disk, Physical Disk, Memory, Network).

LAB WORK 5

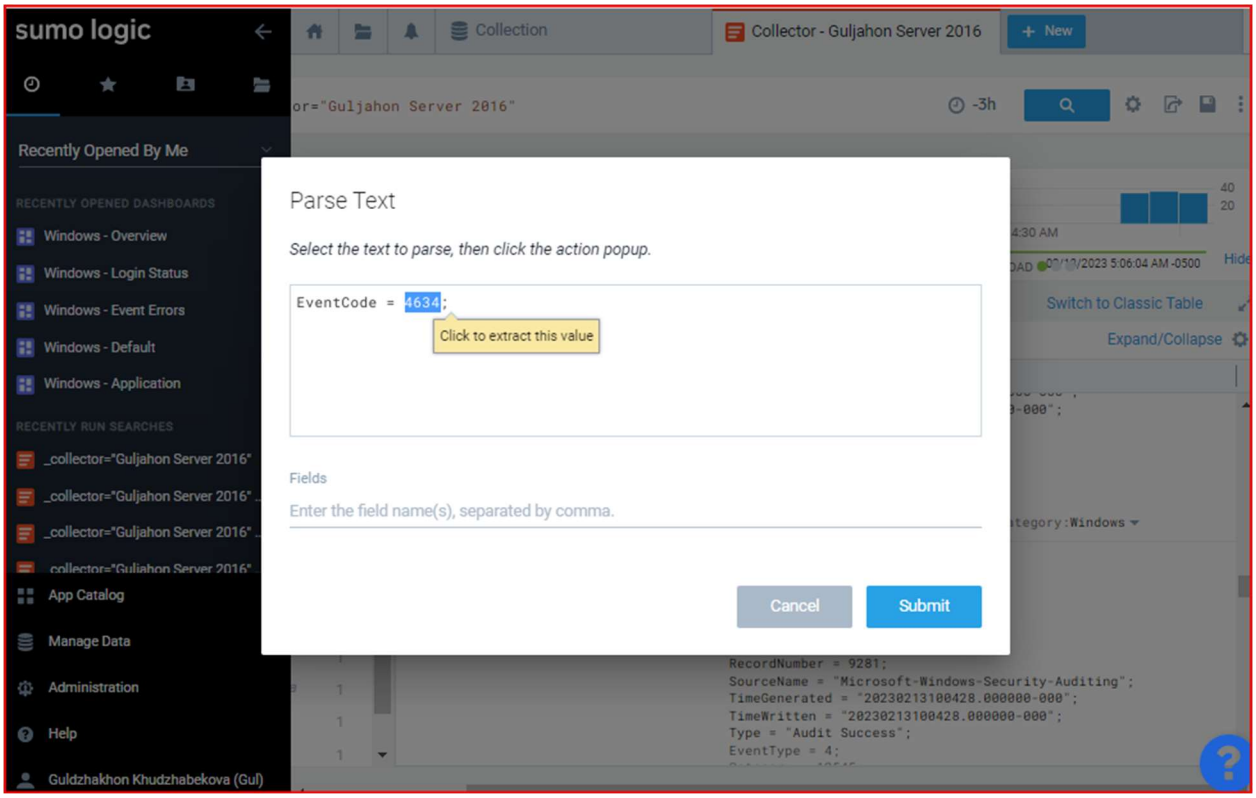
Sumologic

- ✓ **Data Parsing**



Right click>Parse Selected Text

Sumologic

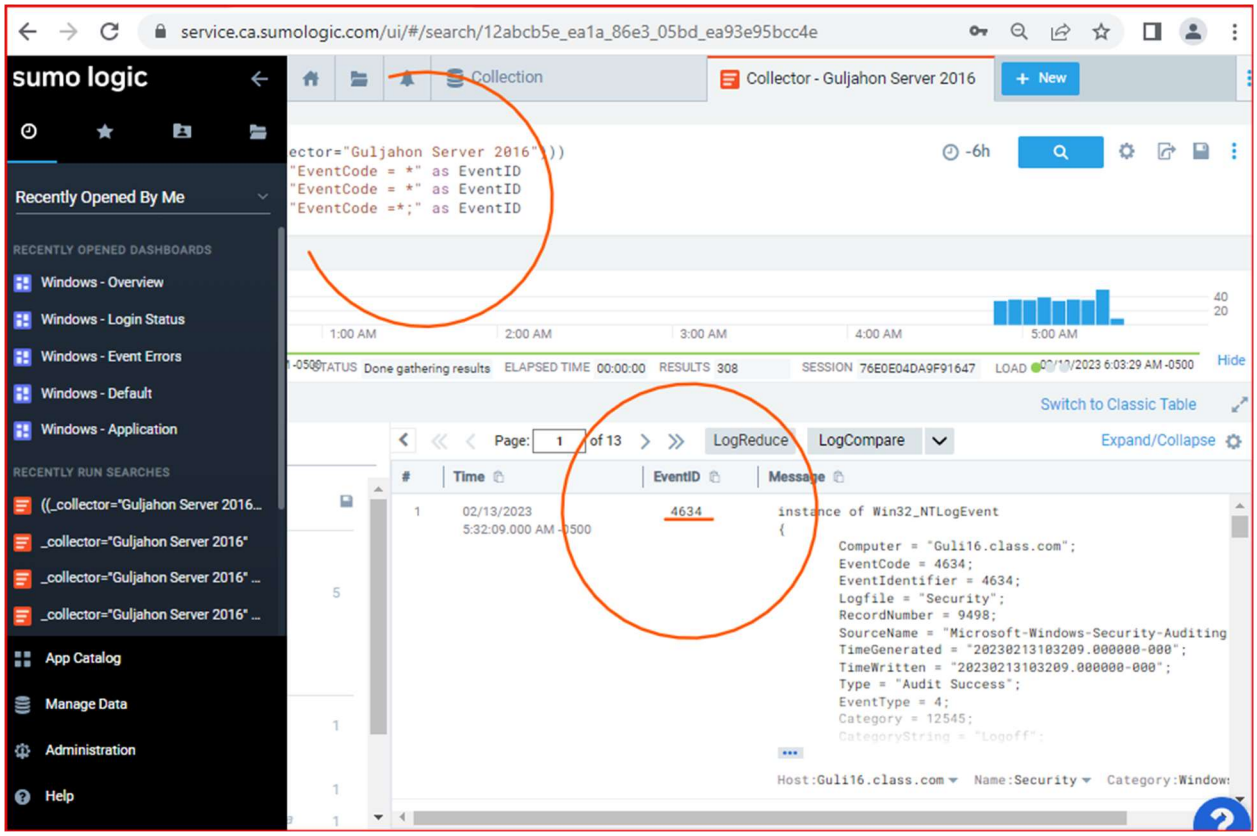


Extract selected value.

Provide the Field Name (Event ID) and Submit.

LAB WORK 5

Sumologic



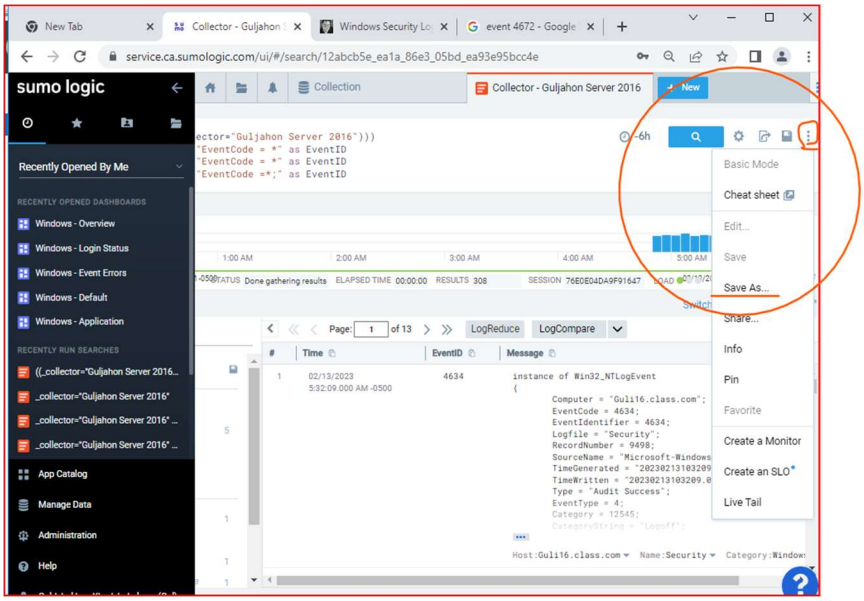
Event ID parsed.

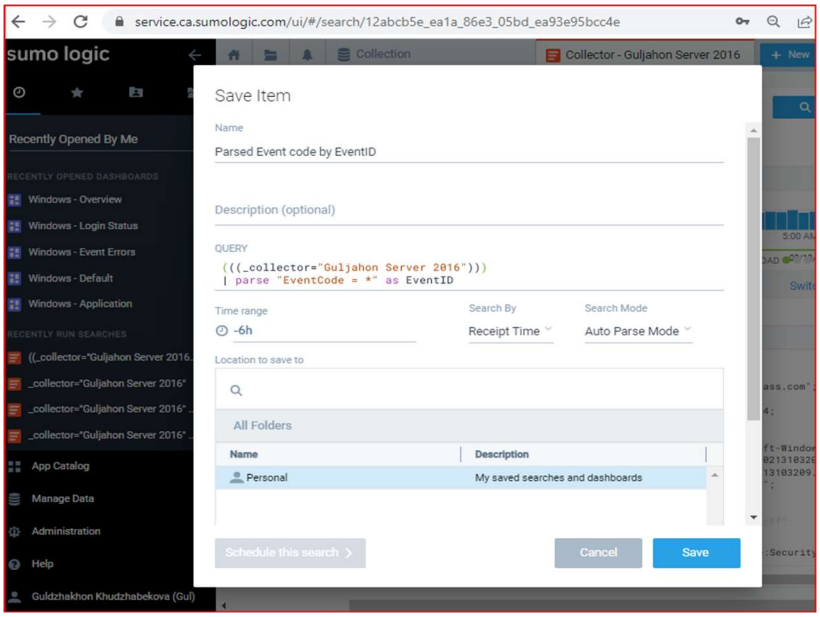
The procedure is same for any Event ID parsing.

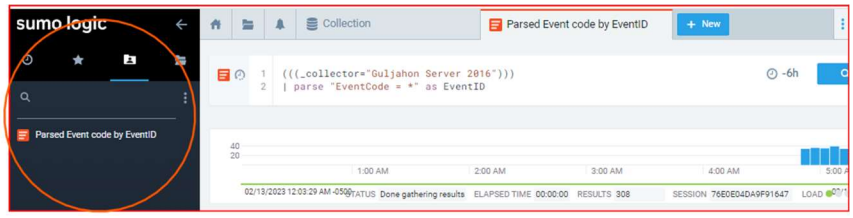
LAB WORK 5

Sumologic

- ✓ **Save the Search**





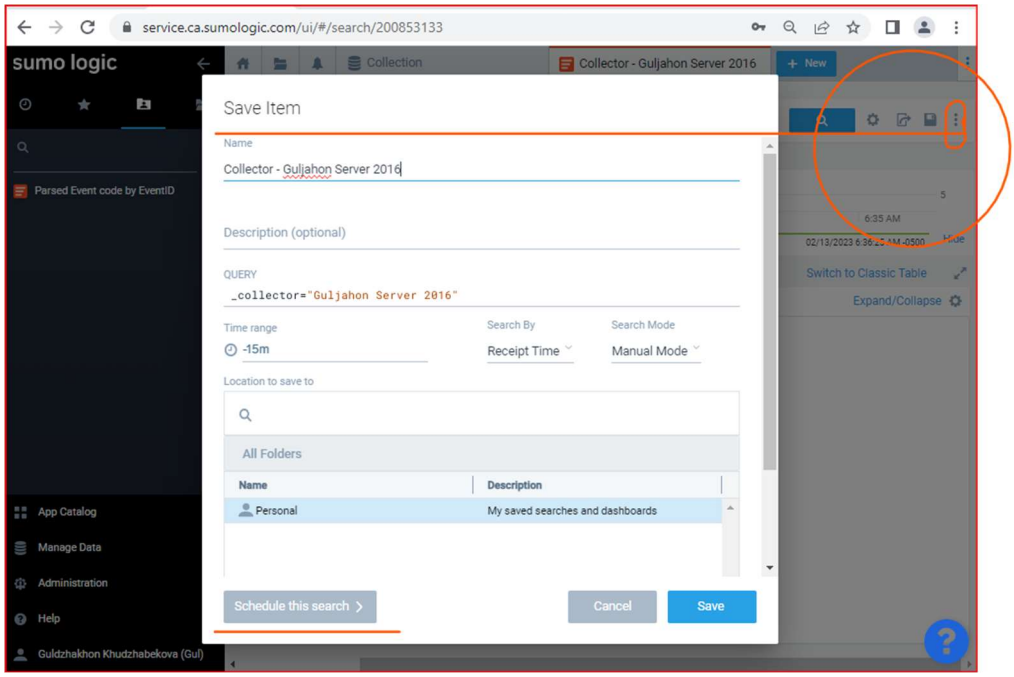


The Search is saved under Personal Folder

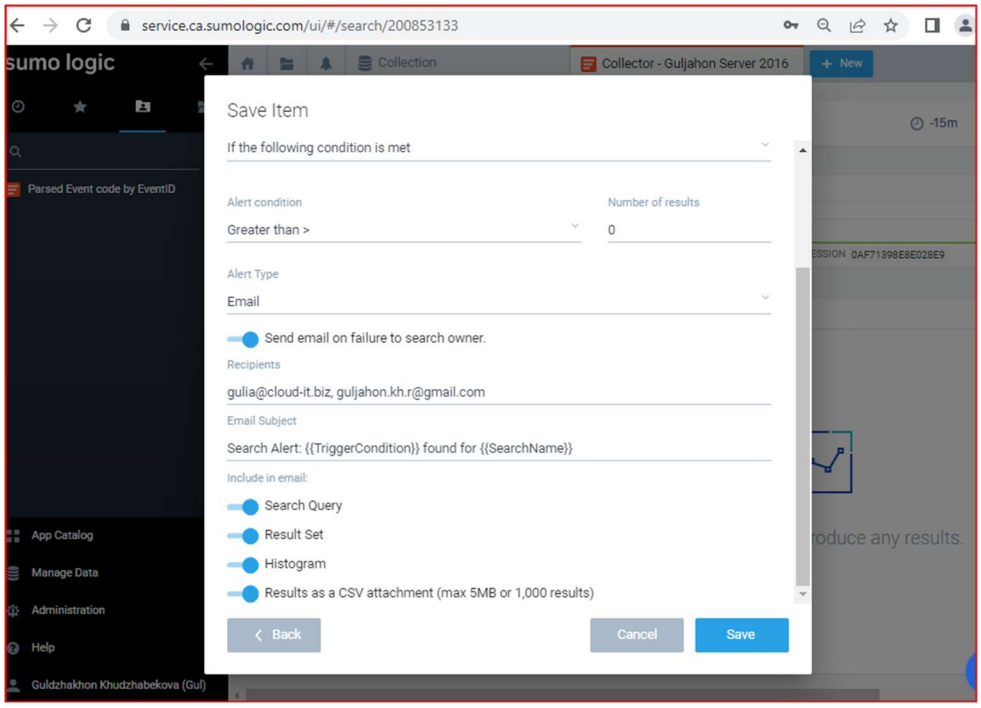
LAB WORK 5

Sumologic

- ✓ **Configure an Email Alert**

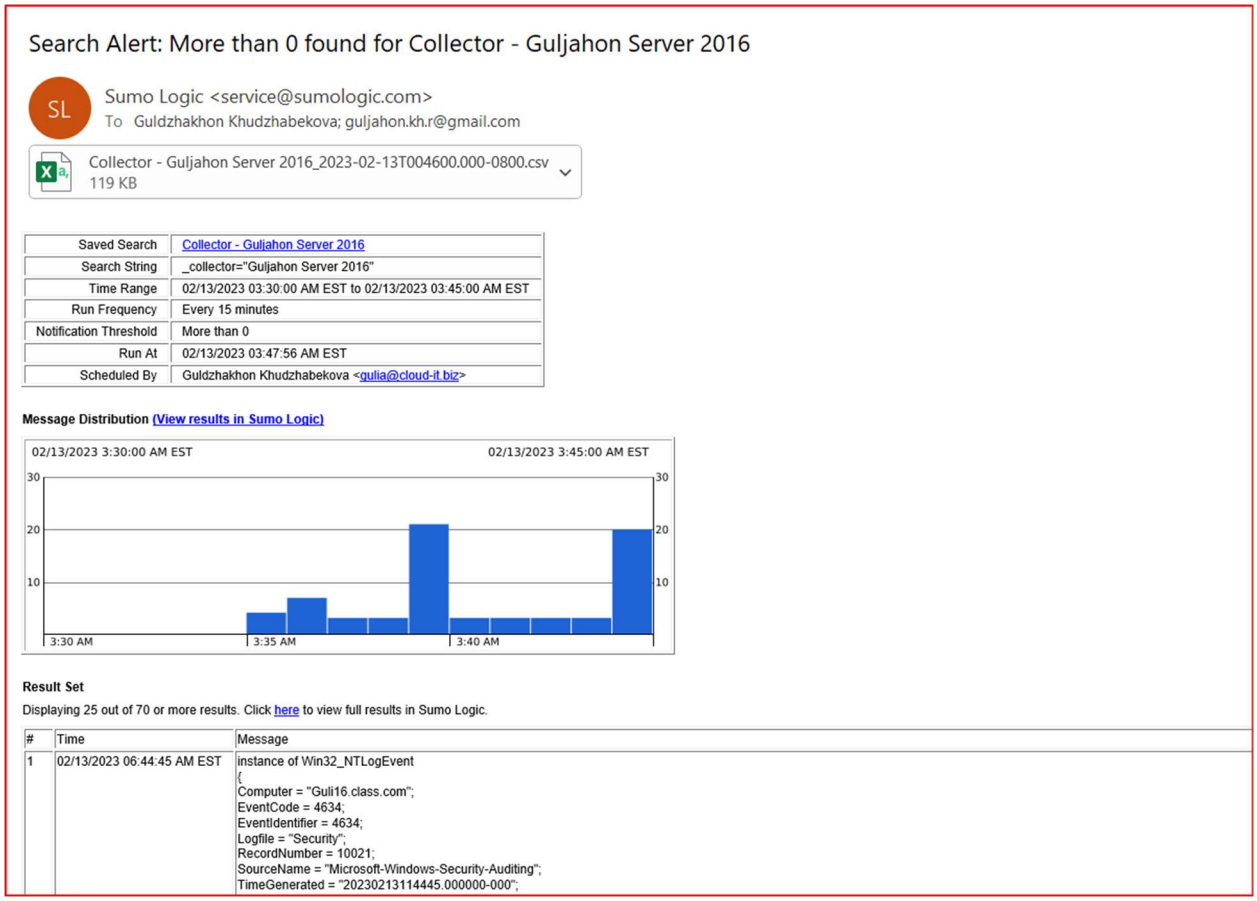


Collection>Collector >Schedule this search>Provide all details.



LAB WORK 5

Sumologic



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

SL

Sumo Logic <service@sumologic.com>
To Guldzhakhon 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	Guldzhakhon 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.

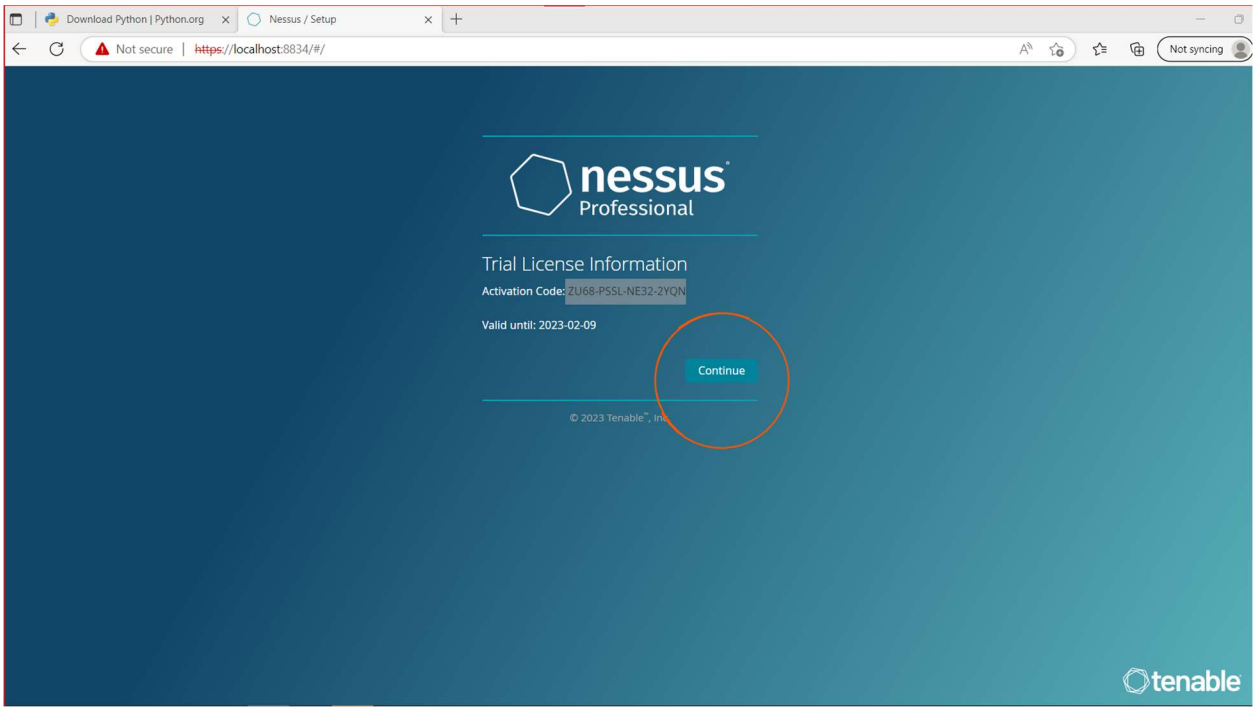
#	Time	Message
1	02/13/2023 06:44:45 AM EST	instance of Win32_NTLogEvent { Computer = "Guli16.class.com"; EventCode = 4634; EventIdentifier = 4634; Logfile = "Security"; RecordNumber = 10021; SourceName = "Microsoft-Windows-Security-Auditing"; TimeGenerated = "20230213114445.000000-000";

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

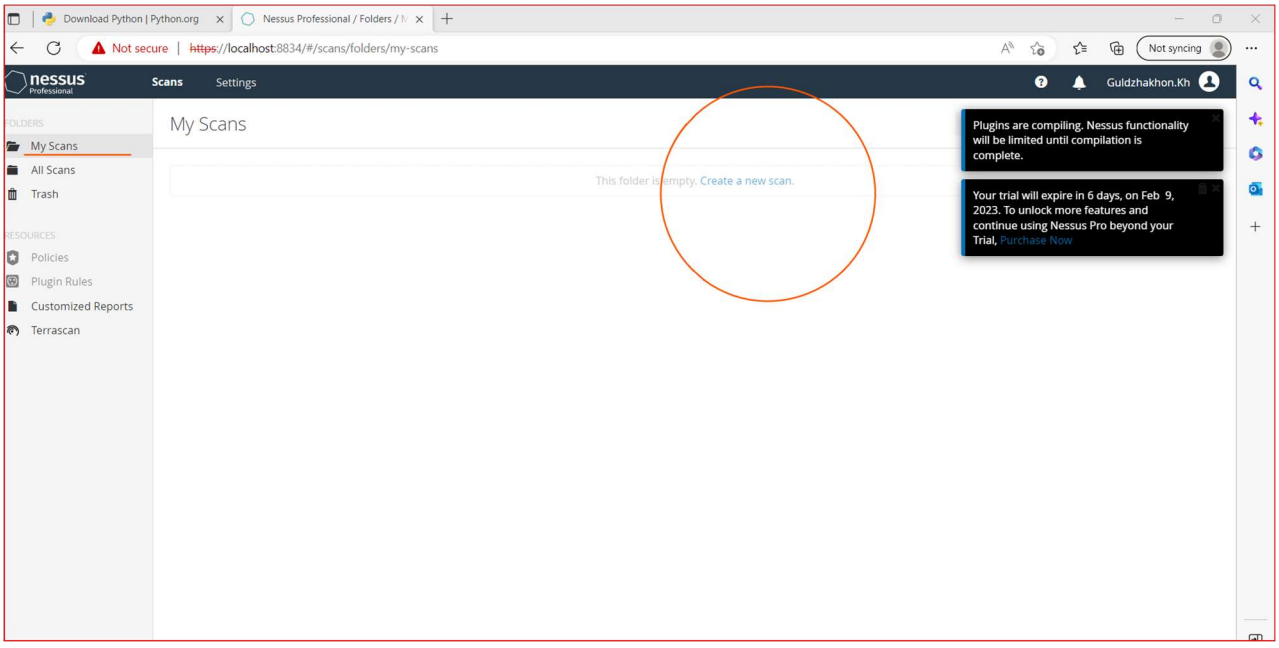
LAB WORK 5 COMPLETED

NESSUS

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

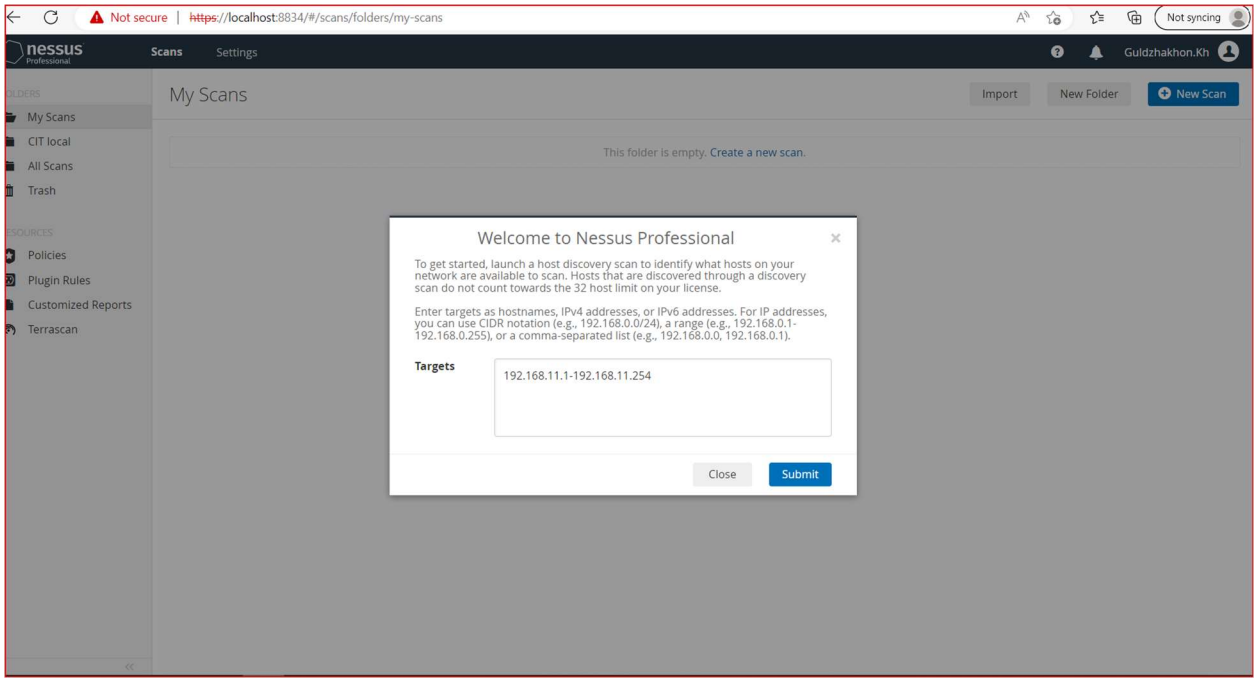


Guldzhakhon.Kh

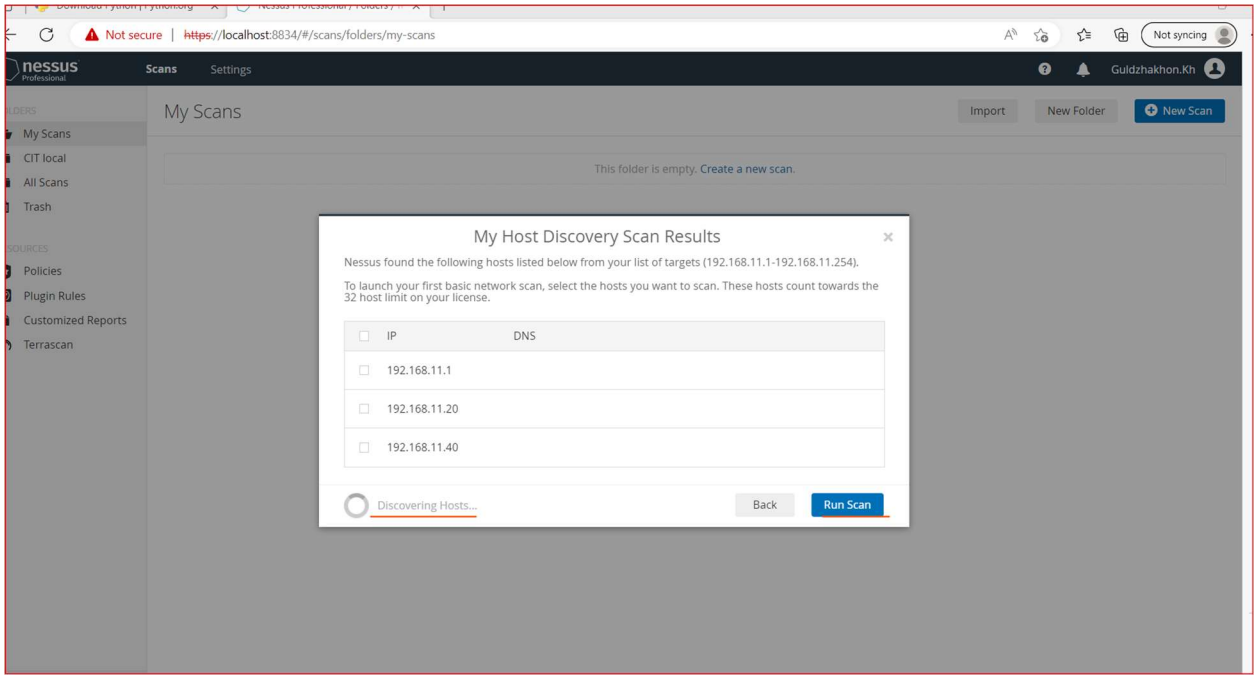


LAB WORK 6

Nessus



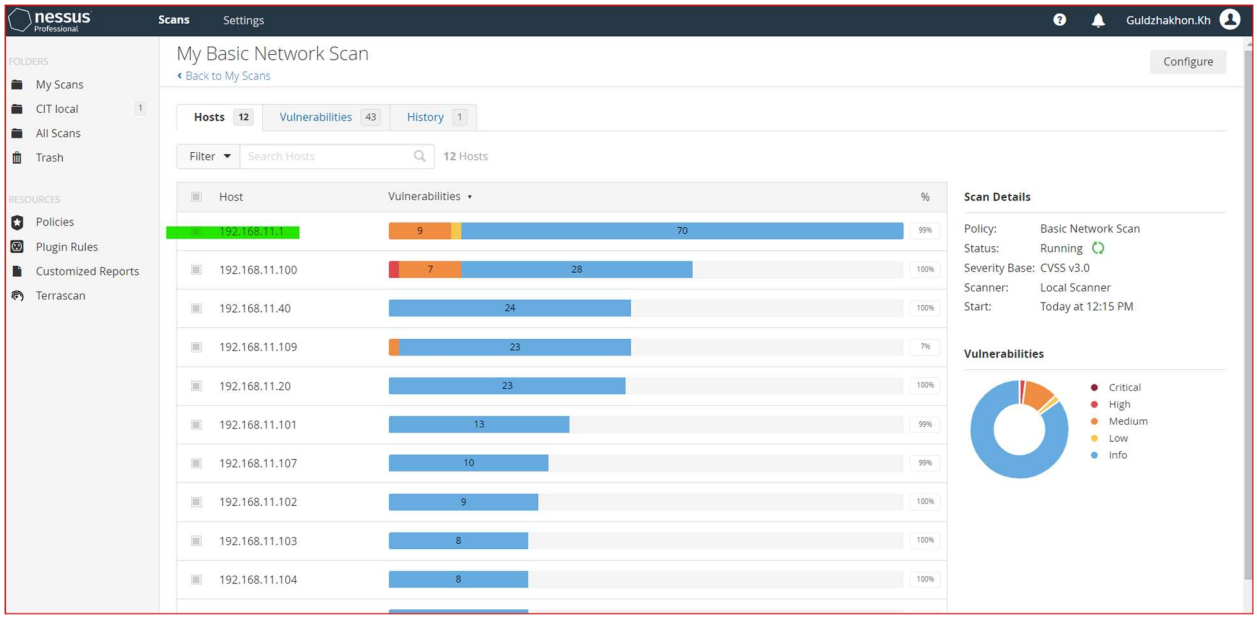
Enter IP range.



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

LAB WORK 6

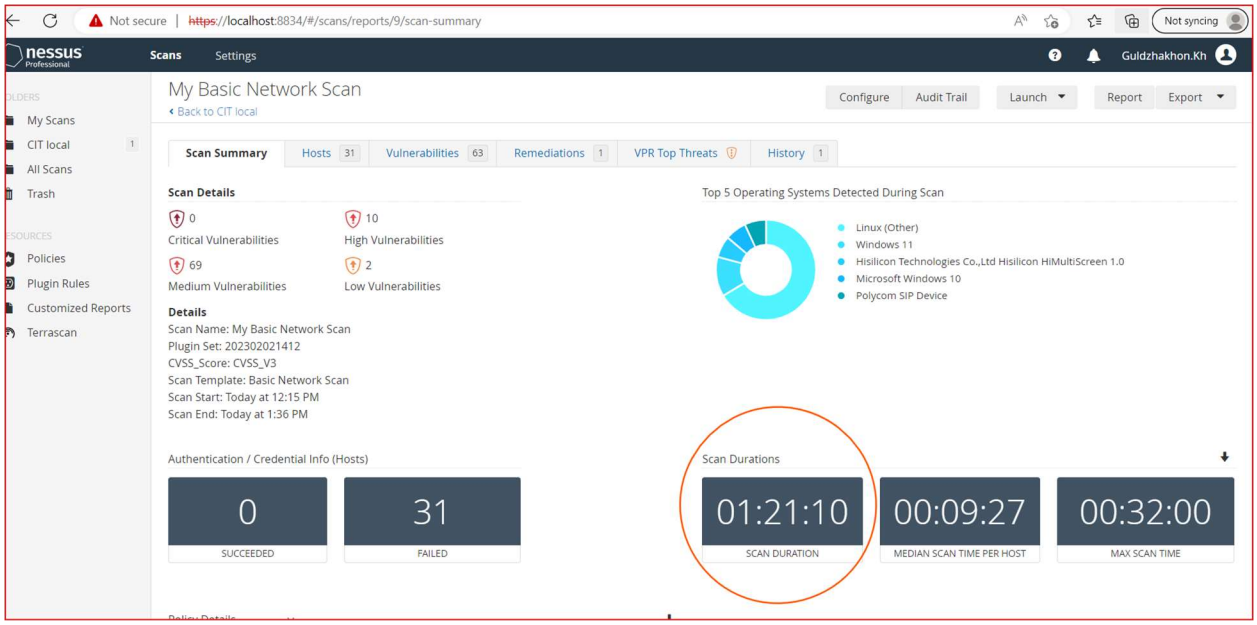
Nessus

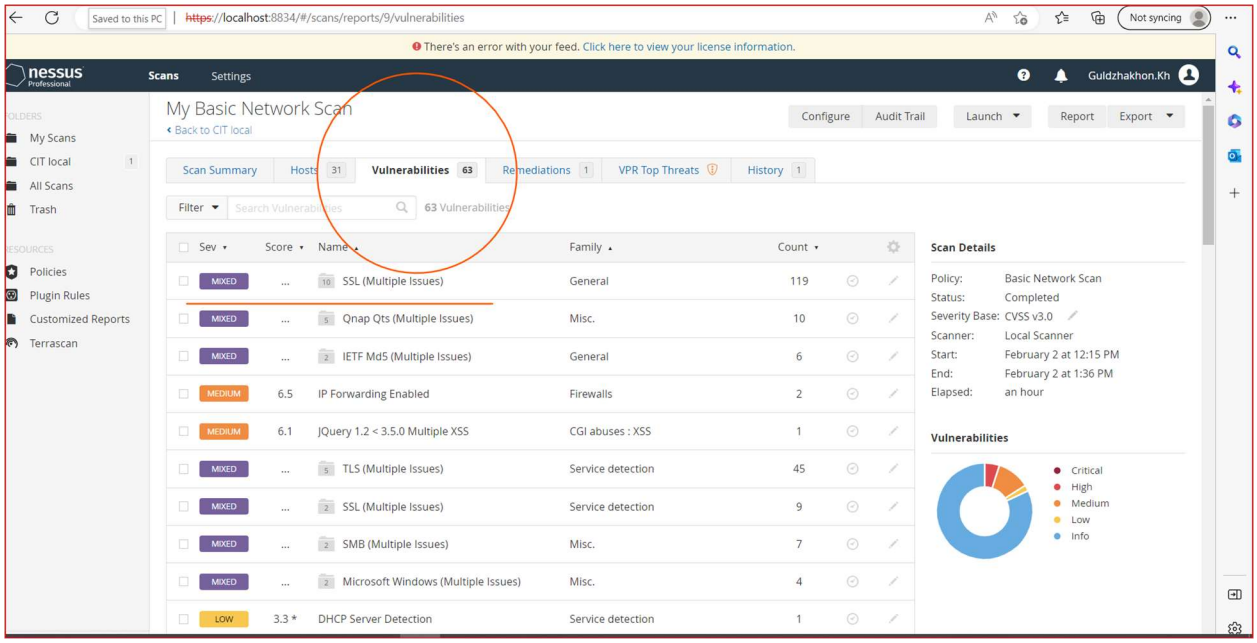


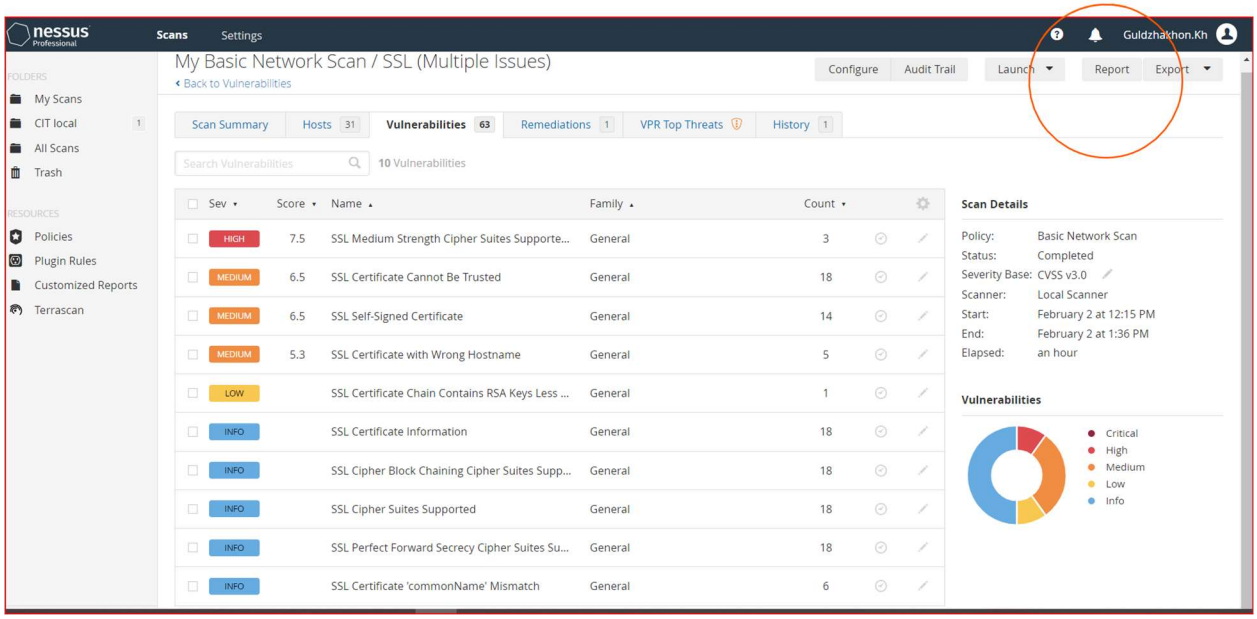
It takes time to complete screening.

LAB WORK 6

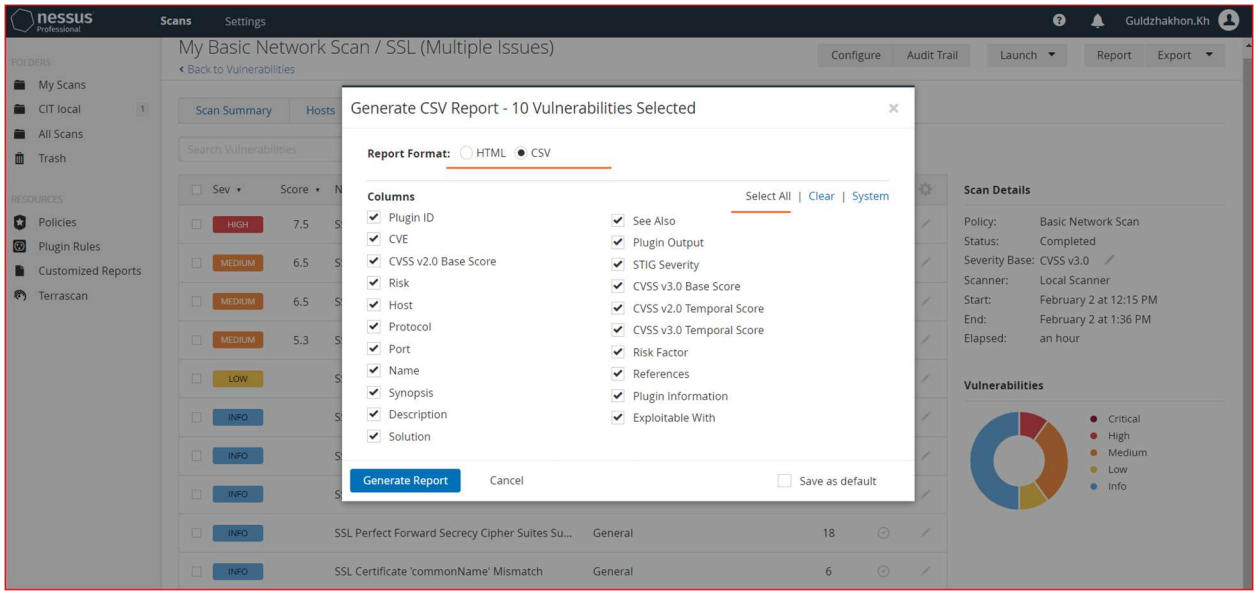
Nessus







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



Generate report.

✓ **How to read the Report**

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

nessus

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_lsi0ow.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.

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

192.168.11.147

0	1	3	1	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_lsi0ow.html 18/28

The interface is user friendly.

68	57582	6.4	Medium	192.168.1	tcp	21	SSL Self-Si	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-Si	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 Signir	Signing is n	Signing is	Enforce message signing in the host's configuration. On Windows, this	Medium
71	60119		None	192.168.1	tcp	445	Microsoft	It was pos	By using	n/a	None
72	66334		None	192.168.1	tcp	0	Patch Rep	The remot	The	Install the patches listed below.	None
73	70544		None	192.168.1	tcp	21	SSL Cipher	The	The	n/a	None
74	70544		None	192.168.1	tcp	443	SSL Cipher	The	The	n/a	None
75	70657		None	192.168.1	tcp	22	SSH Algorit	An SSH ser	This script	n/a	None
76	84502		None	192.168.1	tcp	443	HSTS Missi	The remot	The	Configure the remote web server to use HSTS.	None
77	86420		None	192.168.1	tcp	0	Ethernet M	This	This	n/a	None
78	94761		None	192.168.1	tcp	21	SSL Root C	A root	The	Ensure that use of this root Certification Authority certificate	None
79	94761		None	192.168.1	tcp	443	SSL Root C	A root	The	Ensure that use of this root Certification Authority certificate	None
80	96982		None	192.168.1	tcp	445	Server Me	The remot	The	Disable SMBv1 according to the vendor instructions in Microsoft	None
81	100871		None	192.168.1	tcp	445	Microsoft	It was	Nessus	n/a	None
82	104743	6.1	Medium	192.168.1	tcp	21	TLS Versio	The remot	The	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	443	TLS Versio	The remot	The	Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.	Medium

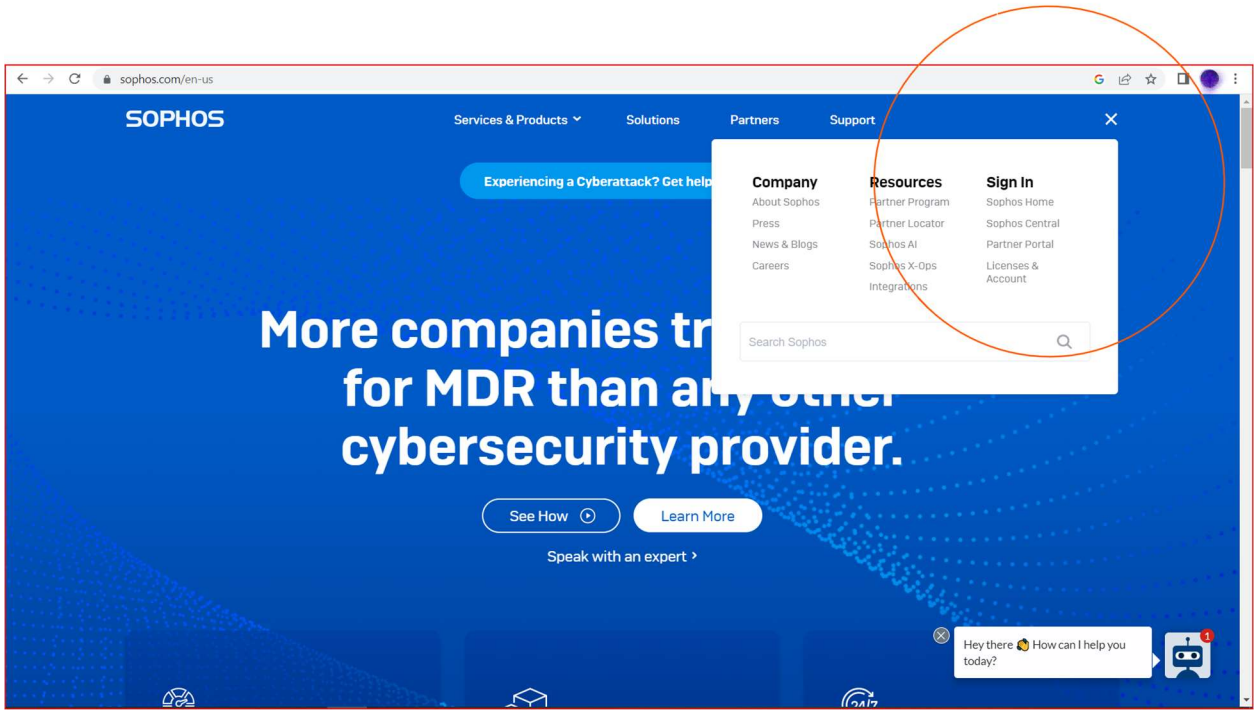
Open created reports and click on specific vulnerability.

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

LAB WORK 6 COMPLETED

SOPHOS

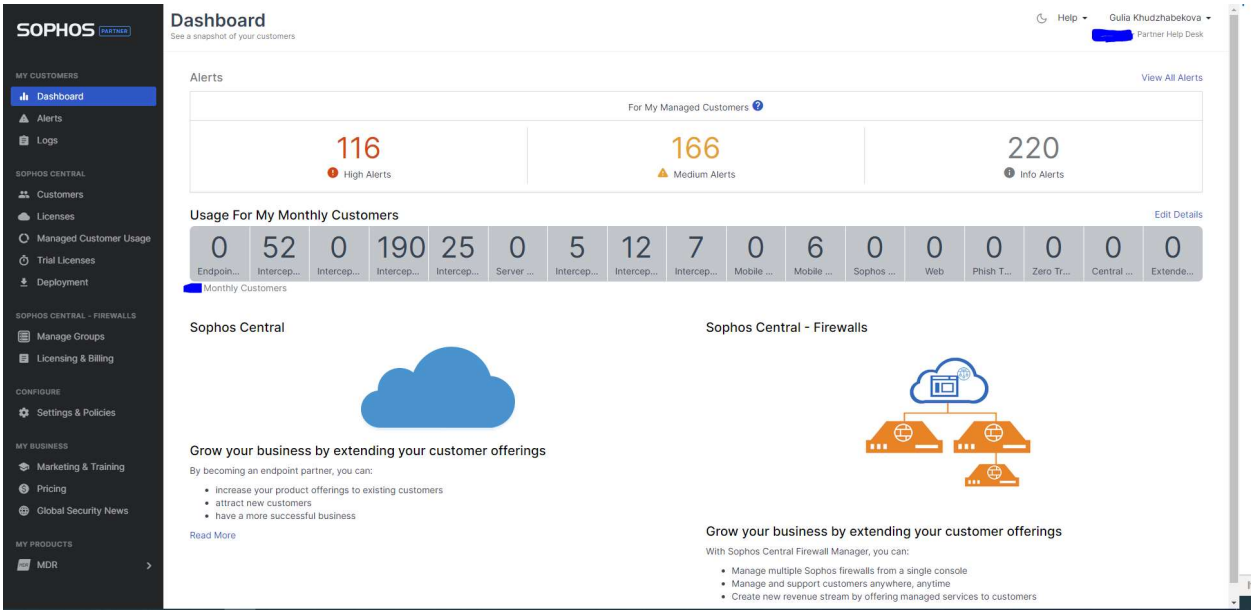
- ✓ **Activate Sophos Central free trial.**
- ✓ **Install Server Protection on Windows Server 2016**
- ✓ **Push Website management rules**



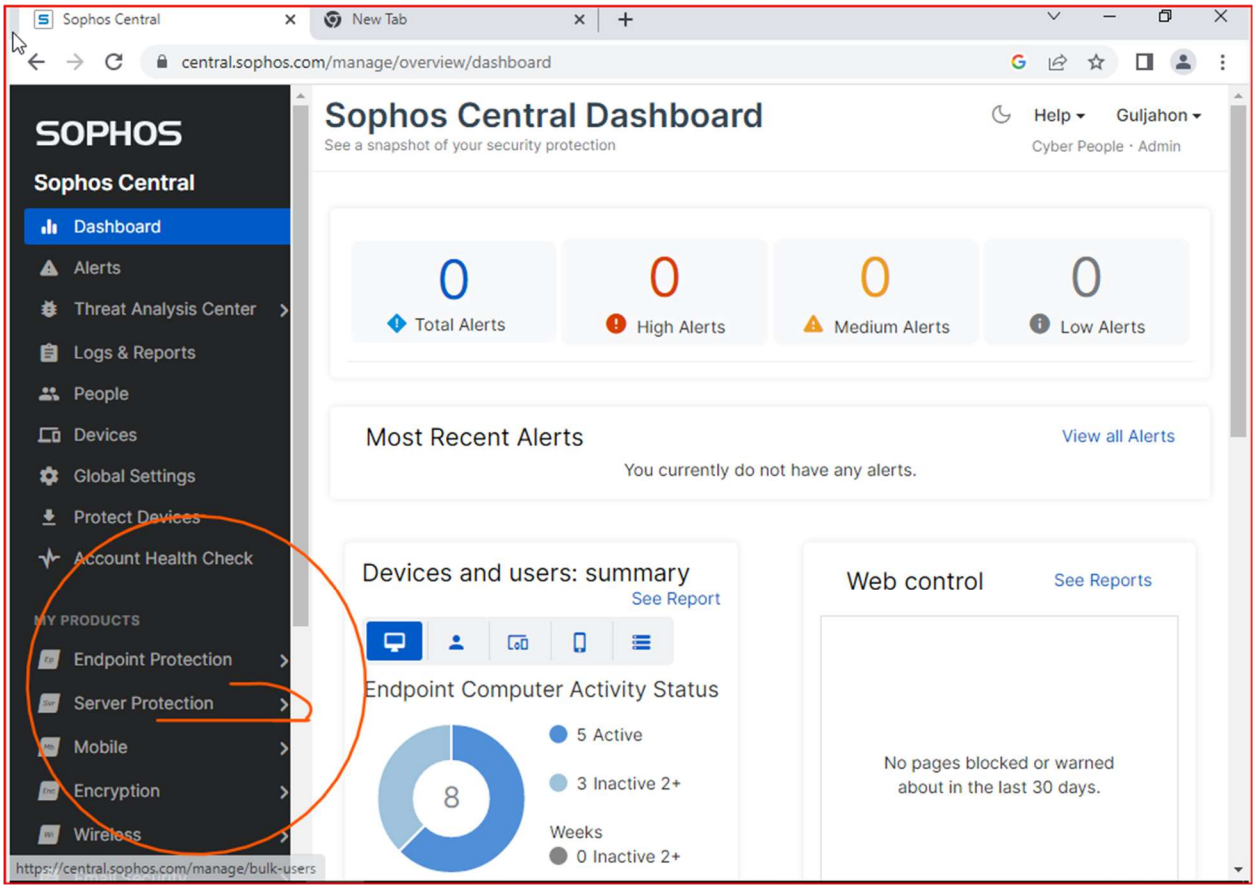
Follow the link to get started with the Sophos free Trial version:
www.sophos.com

LAB WORK 7

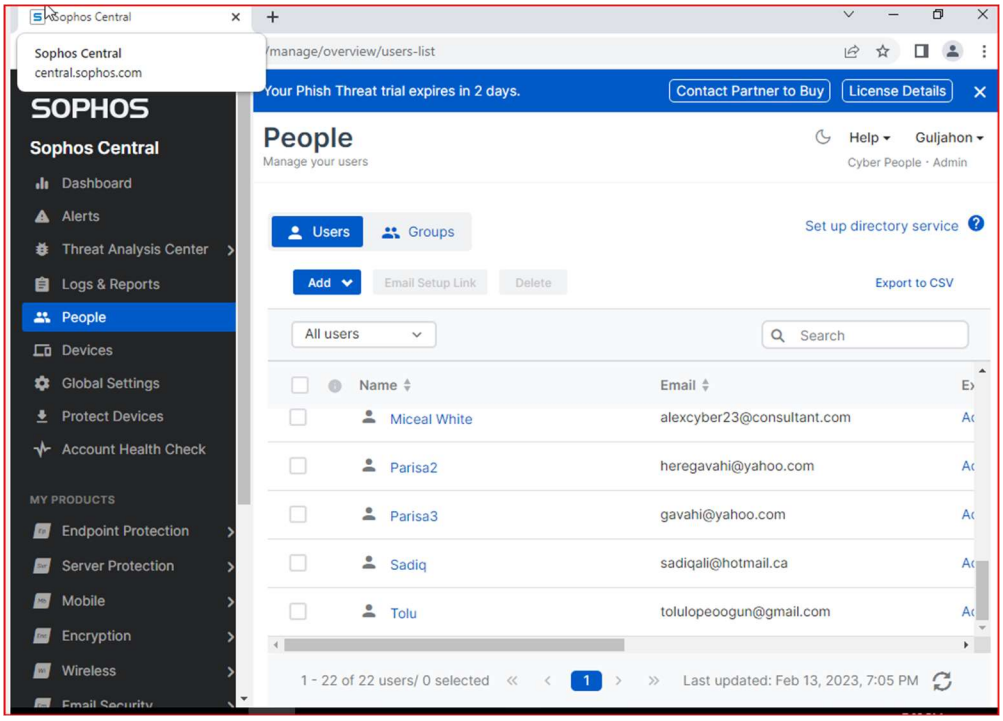
Sophos

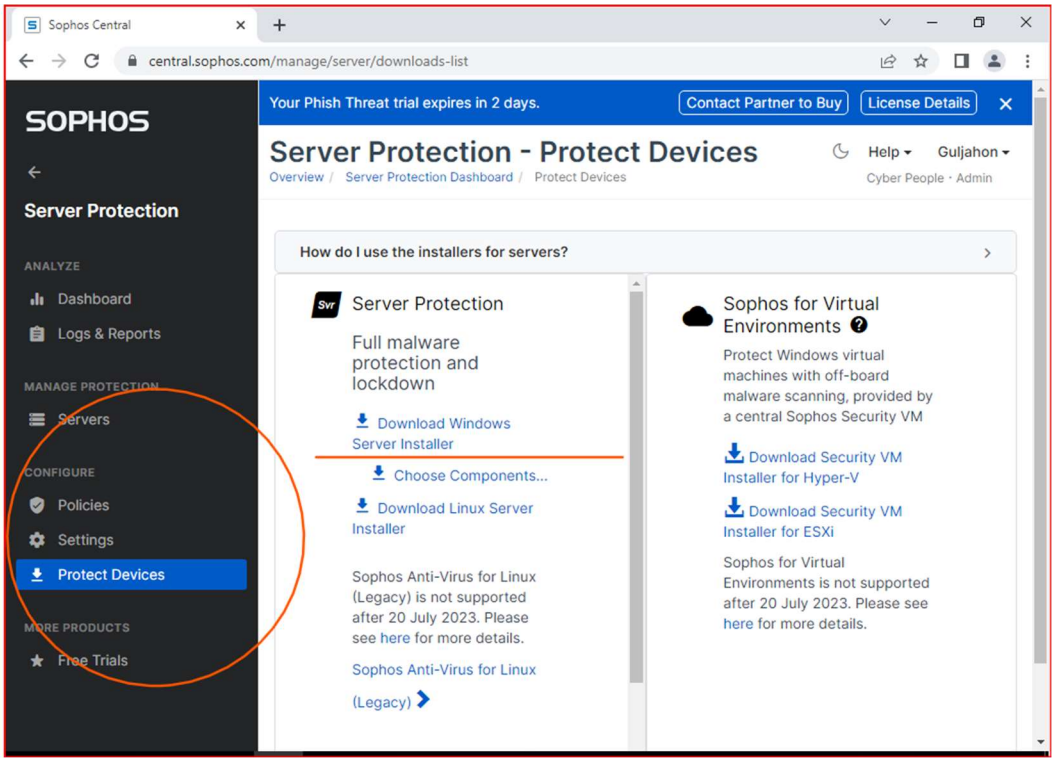


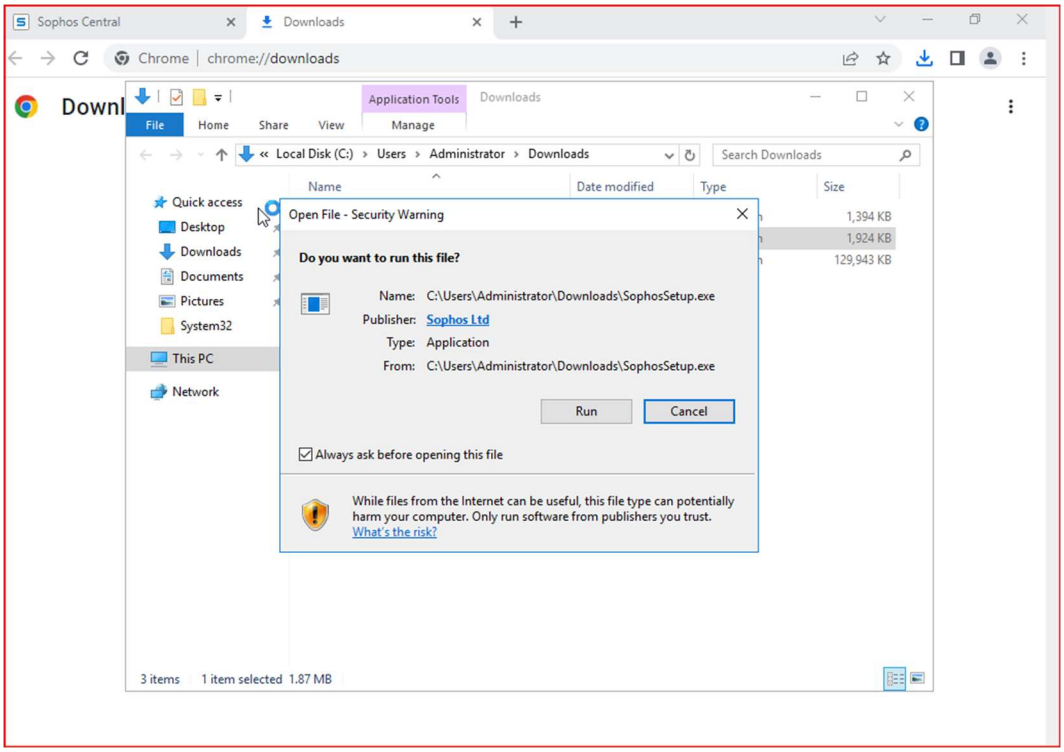
My Sophos Partner Dashboard.



My free trial Sophos Central Dashboard



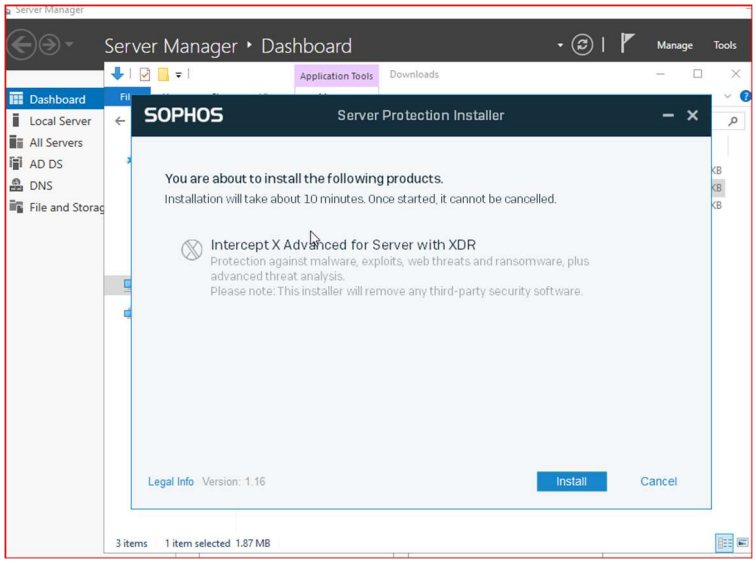

Sophos Central
central.sophos.com/manage/server/downloads-list
SOPHOS
Your Phish Threat trial expires in 2 days.
Contact Partner to Buy
License Details
Server Protection - Protect Devices
Overview / Server Protection Dashboard / Protect Devices
Help
Guljahon
Cyber People · Admin
Server Protection
ANALYZE
Dashboard
Logs & Reports
MANAGE PROTECTION
Servers
CONFIGURE
Policies
Settings
Protect Devices
MORE PRODUCTS
Free Trials
How do I use the installers for servers?
Server Protection
Full malware protection and lockdown
Download Windows Server Installer
Choose Components...
Download Linux Server Installer
Sophos Anti-Virus for Linux (Legacy) is not supported after 20 July 2023. Please see here for more details.
Sophos Anti-Virus for Linux (Legacy)
Sophos for Virtual Environments
Protect Windows virtual machines with off-board malware scanning, provided by a central Sophos Security VM
Download Security VM Installer for Hyper-V
Download Security VM Installer for ESXi
Sophos for Virtual Environments is not supported after 20 July 2023. Please see here for more details.


Sophos Central
Downloads
Chrome | chrome://downloads
Application Tools
Downloads
File
Home
Share
View
Manage
Local Disk (C:) › Users › Administrator › Downloads
Search Downloads
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Name
Date modified
Type
Size
1,394 KB
1,924 KB
129,943 KB
Open File - Security Warning
Do you want to run this file?
Name: C:\Users\Administrator\Downloads\SophosSetup.exe
Publisher: Sophos Ltd
Type: Application
From: C:\Users\Administrator\Downloads\SophosSetup.exe
Run
Cancel
Always ask before opening this file
While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust.
What's the risk?
3 items
1 item selected 1.87 MB

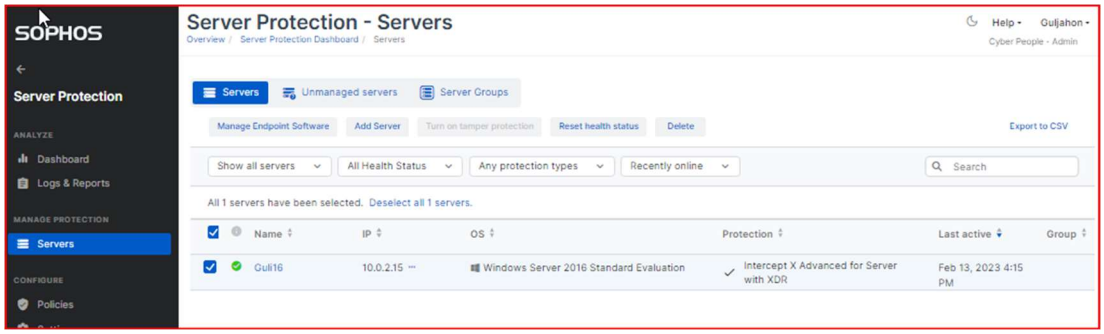
Run Setup.

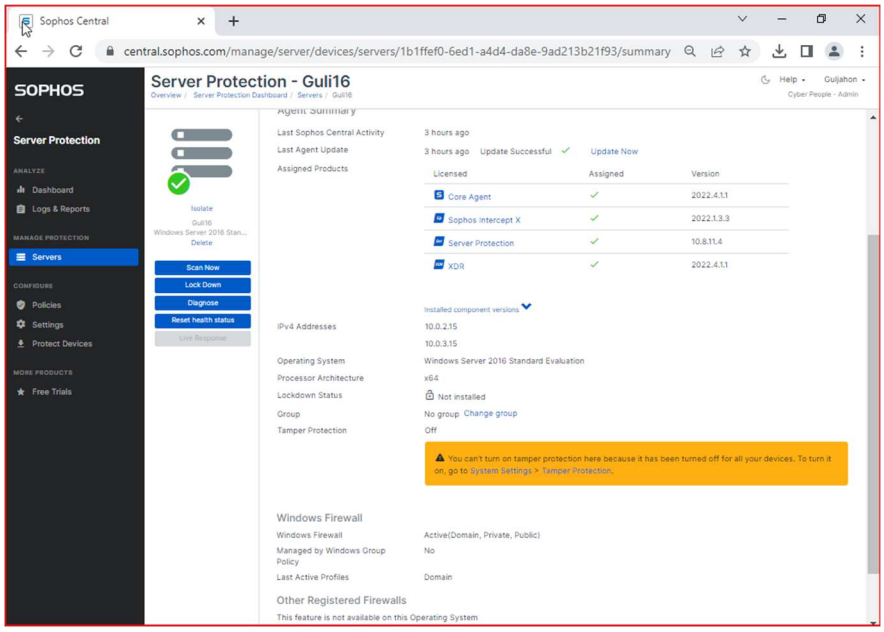
LAB WORK 7

Sophos

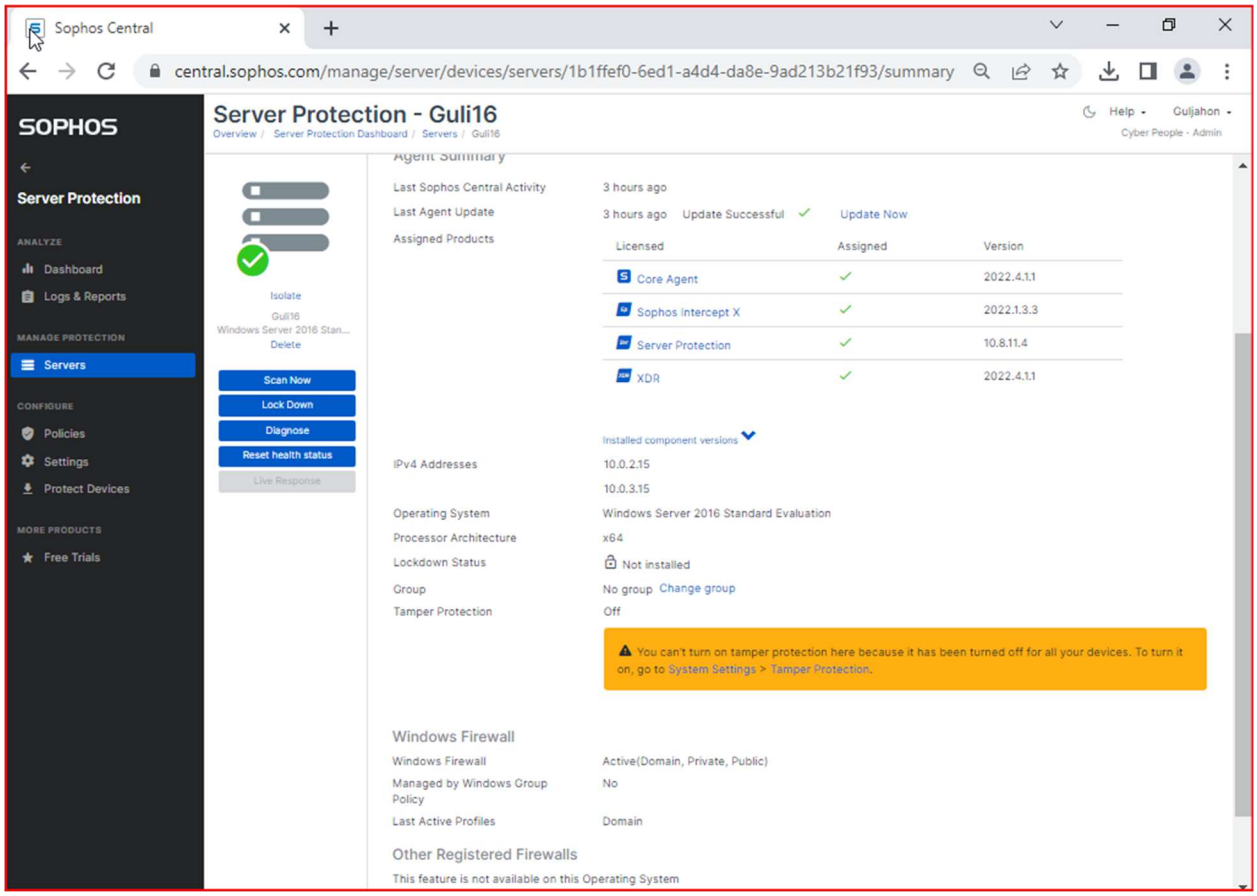


Complete installation.



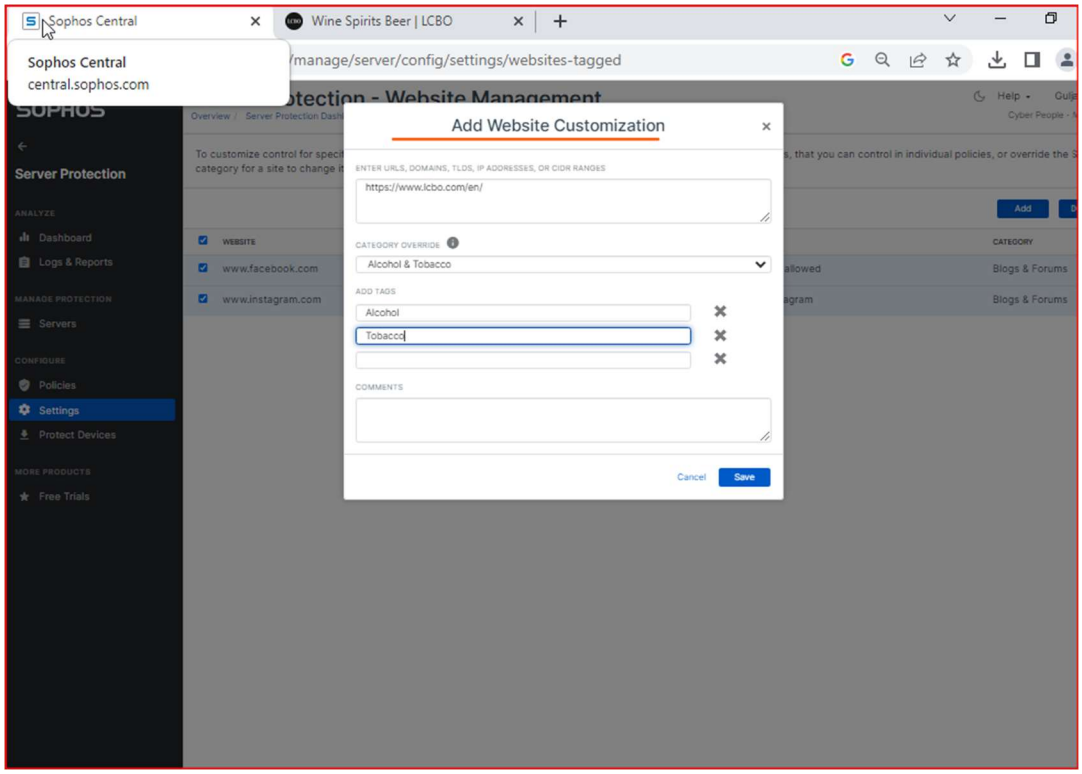


The Server is added to a Sophos Central Dashboard.

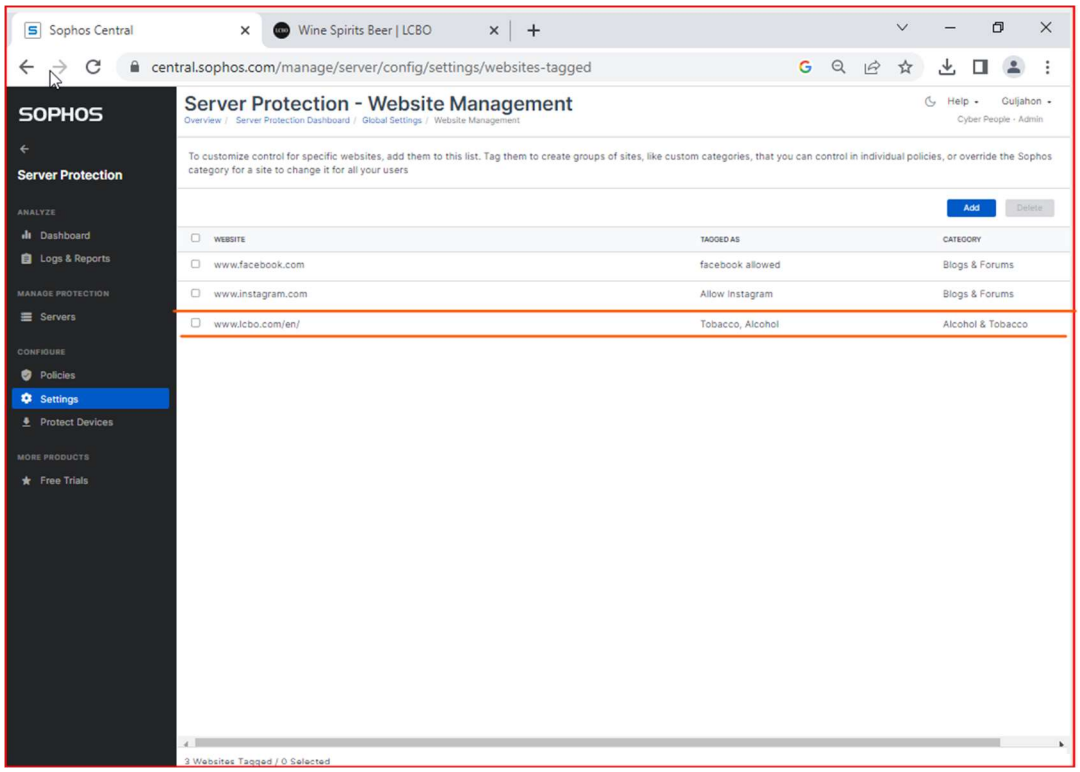

Sophos Central
central.sophos.com/manage/server/devices/servers/1b1ffef0-6ed1-a4d4-da8e-9ad213b21f93/summary
SOPHOS
Server Protection
ANALYZE
Dashboard
Logs & Reports
MANAGE PROTECTION
Servers
CONFIGURE
Policies
Settings
Protect Devices
MORE PRODUCTS
Free Trials
Server Protection - Guli16
Overview / Server Protection Dashboard / Servers / Guli16
Help
Guljahon
Cyber People - Admin
Isolate
Guli16
Windows Server 2016 Stan...
Delete
Scan Now
Lock Down
Diagnose
Reset health status
Live Response
Agent Summary
Last Sophos Central Activity
3 hours ago
Last Agent Update
3 hours ago
Update Successful
Update Now
Assigned Products
Licensed
Assigned
Version
Core Agent
2022.4.1.1
Sophos Intercept X
2022.1.3.3
Server Protection
10.8.11.4
XDR
2022.4.1.1
Installed component versions
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
Tamper Protection
Off
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
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



Add blocklisted website.

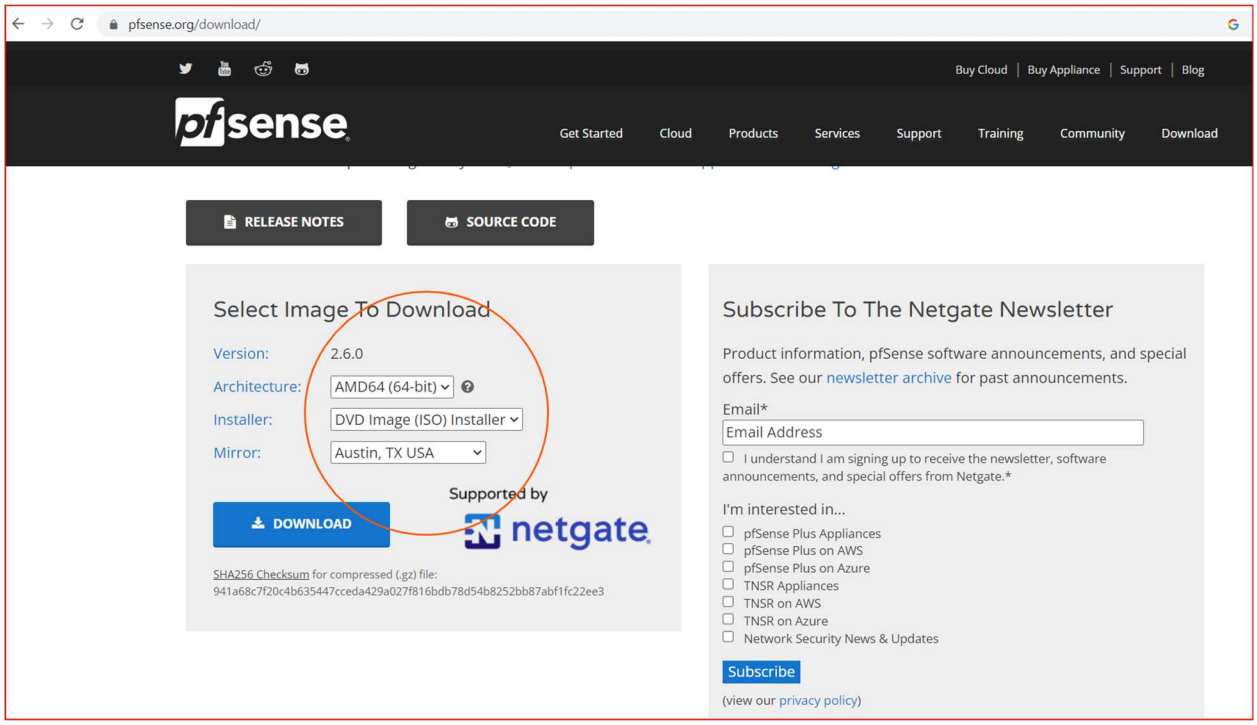


LAB WORK 7 COMPLETED

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