Active Directory Home Lab

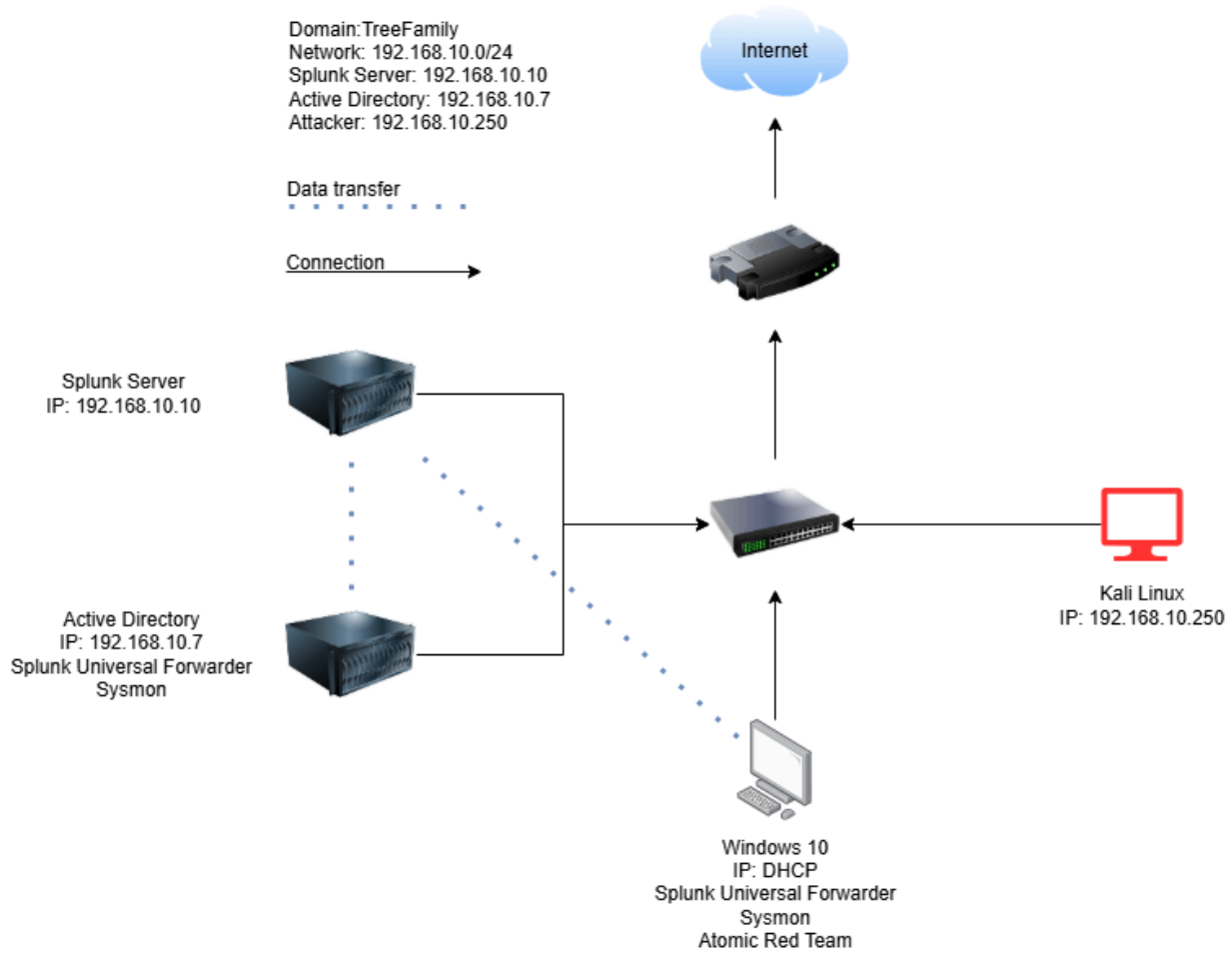
Creating Logical Diagram

Tool: Draw.io

Splunk Universal Forwarder: allow us to send data over to Splunk Server

Sysmon: collect Telemetry on the server and send it over to Splunk Server

Telemetry: automatically collects, transmits and measures data from remote sources, using sensors and other devices to collect data. It uses communication systems to transmit the data back to a central location.



Install Virtual Machines

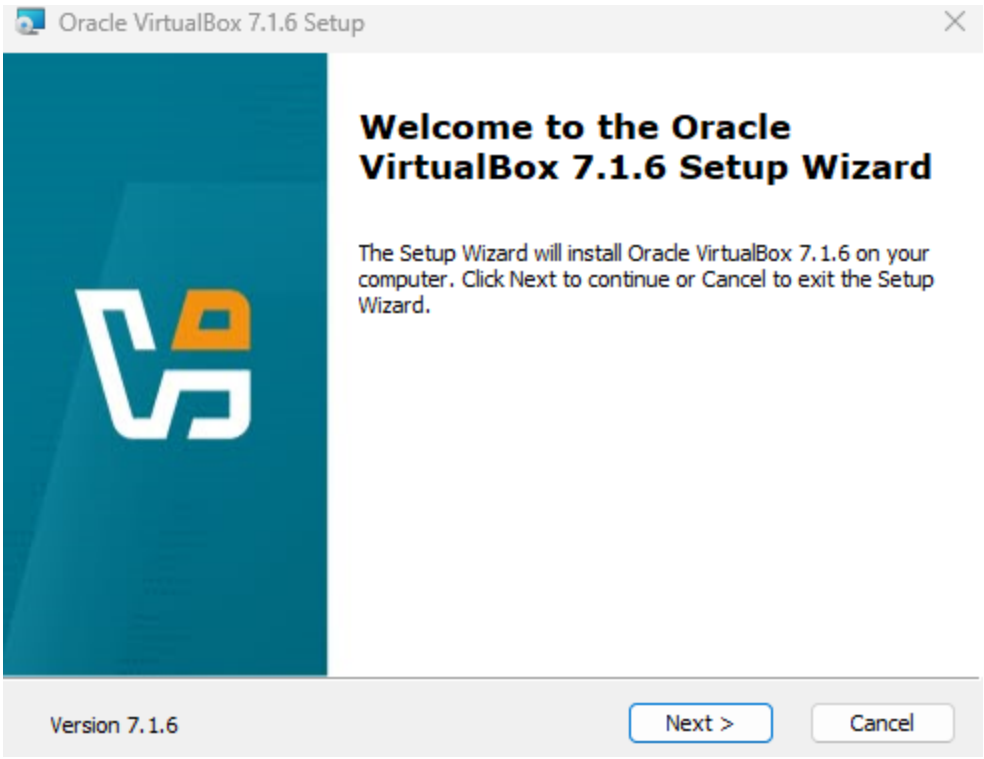
Our virtual machine set-up will include:

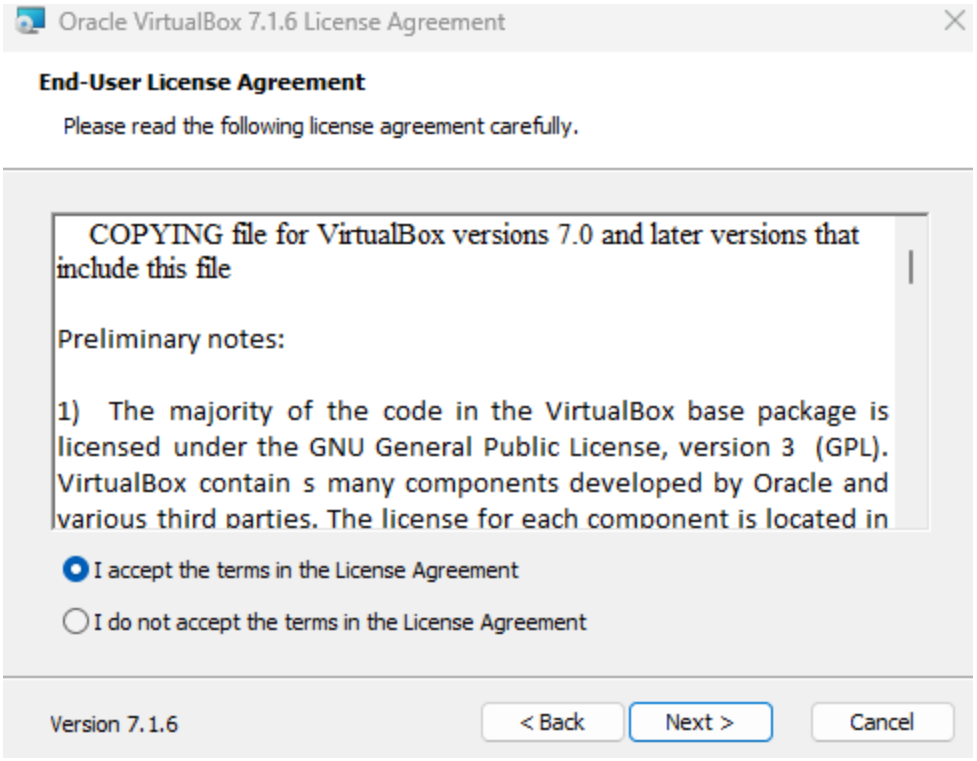
- Windows 10
- Kali Linux
- Ubuntu Server
- Windows Server 2022

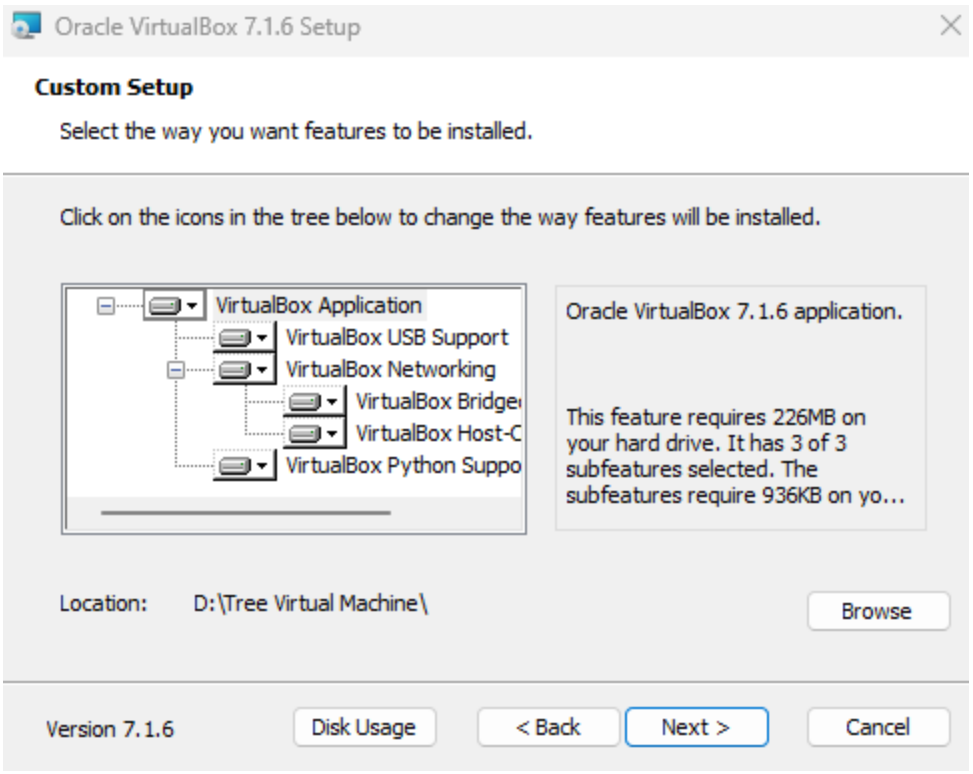
1. Install Virtual Box

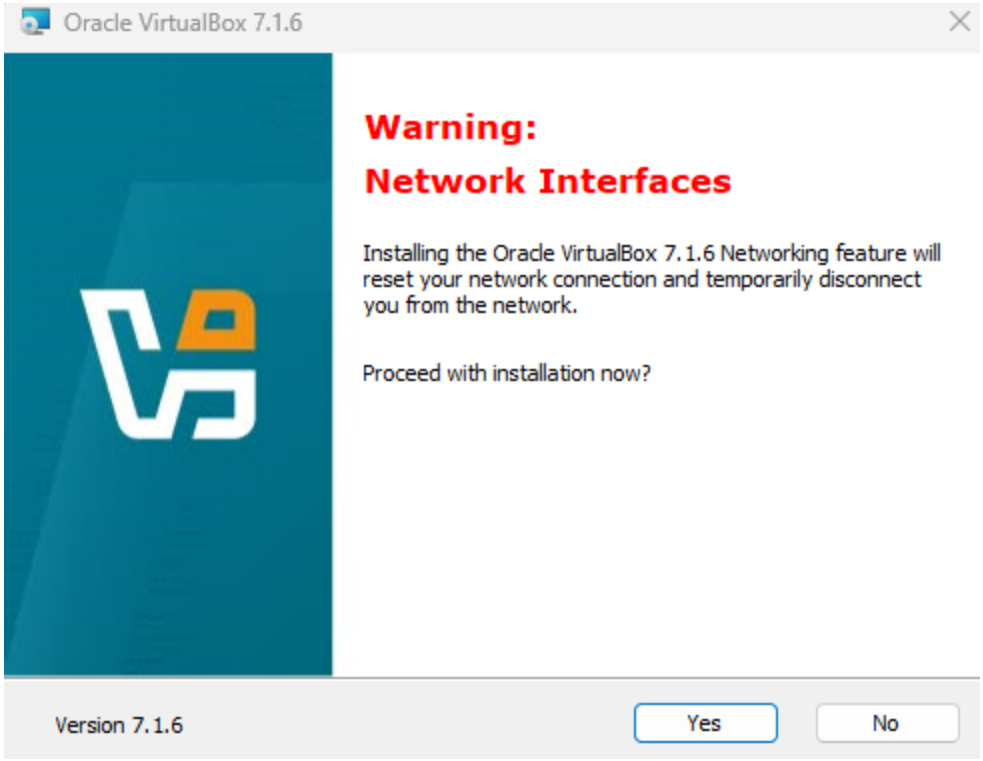
https://www.oracle.com/ca-en/virtualization/technologies/vm/downloads/virtualbox-downloads.html

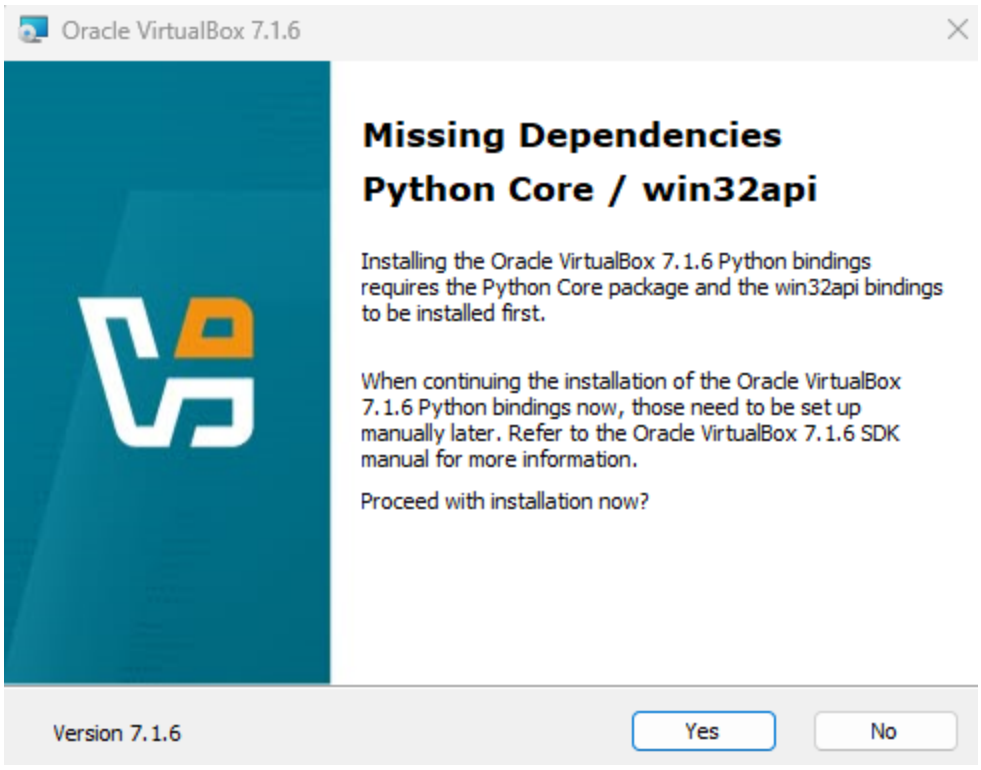
After that run the .exe installer file

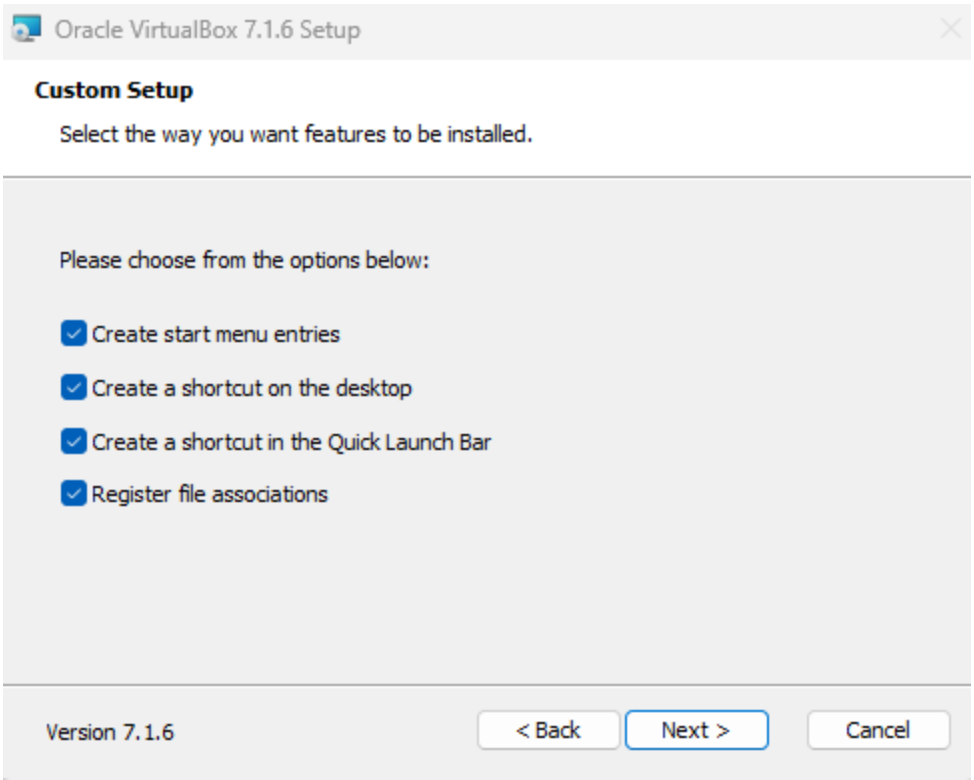

Oracle VirtualBox 7.1.6 Setup
Welcome to the Oracle VirtualBox 7.1.6 Setup Wizard
The Setup Wizard will install Oracle VirtualBox 7.1.6 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.
Version 7.1.6
Next >
Cancel

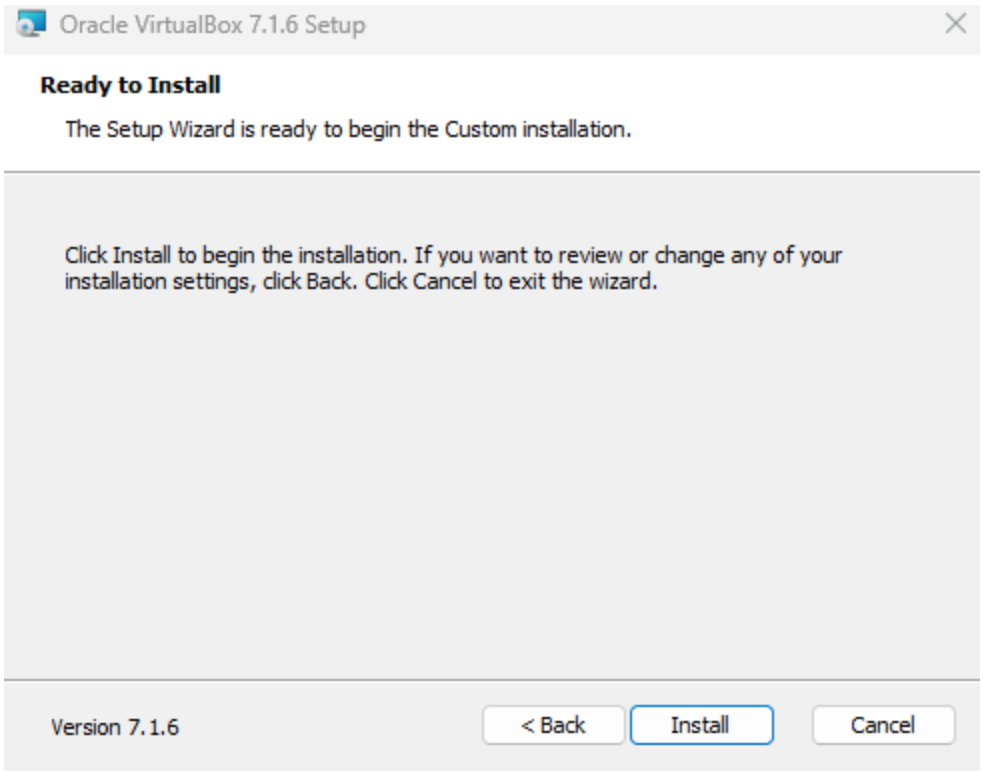

Oracle VirtualBox 7.1.6 License Agreement
End-User License Agreement
Please read the following license agreement carefully.
COPYING file for VirtualBox versions 7.0 and later versions that include this file
Preliminary notes:
1) The majority of the code in the VirtualBox base package is licensed under the GNU General Public License, version 3 (GPL). VirtualBox contain s many components developed by Oracle and various third parties. The license for each component is located in
I accept the terms in the License Agreement
I do not accept the terms in the License Agreement
Version 7.1.6
< Back
Next >
Cancel

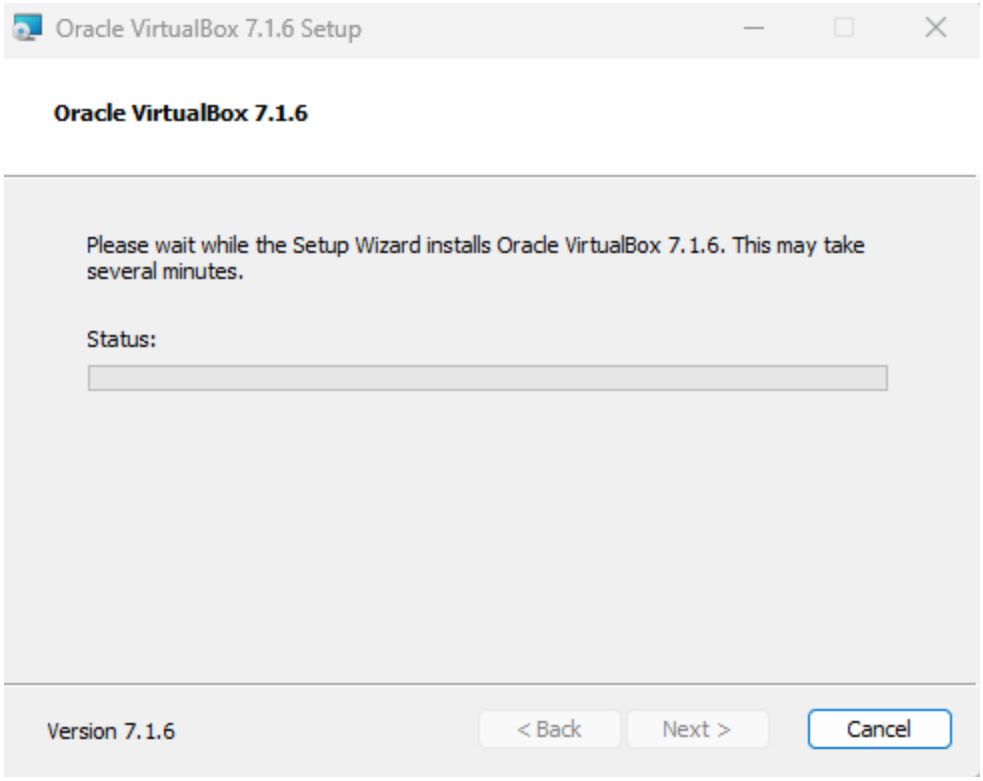

Oracle VirtualBox 7.1.6 Setup
Custom Setup
Select the way you want features to be installed.
Click on the icons in the tree below to change the way features will be installed.
VirtualBox Application
VirtualBox USB Support
VirtualBox Networking
VirtualBox Bridge
VirtualBox Host-C
VirtualBox Python Suppo
Oracle VirtualBox 7.1.6 application.
This feature requires 226MB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 936KB on yo...
Location:
D:\Tree Virtual Machine\
Browse
Version 7.1.6
Disk Usage
< Back
Next >
Cancel

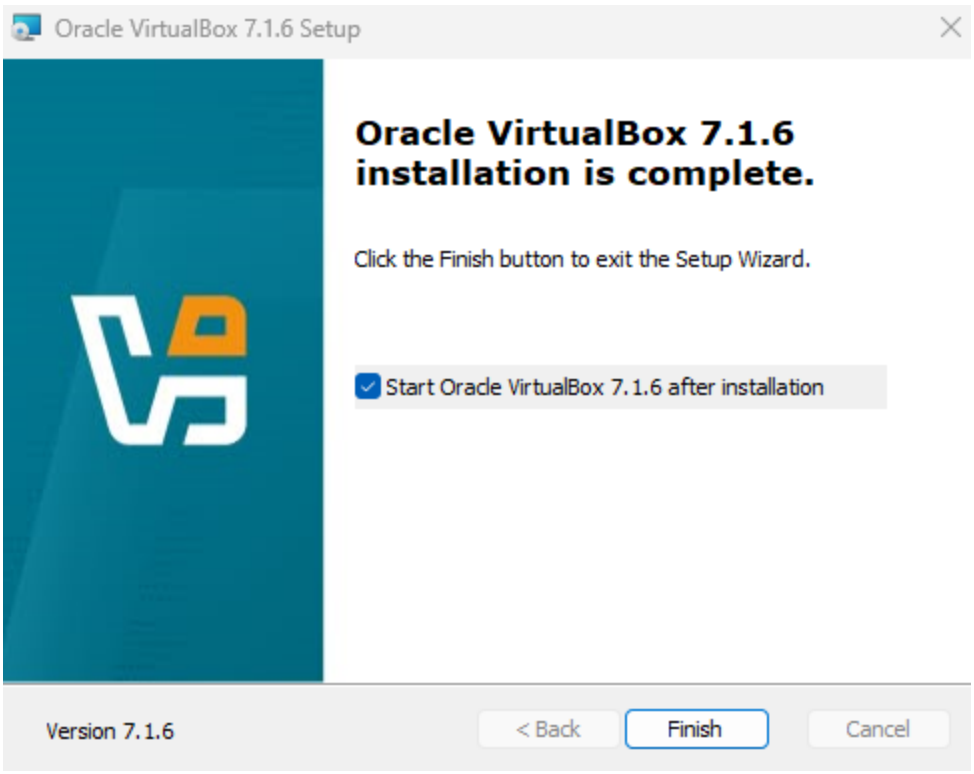

Oracle VirtualBox 7.1.6
Warning:
Network Interfaces
Installing the Oracle VirtualBox 7.1.6 Networking feature will reset your network connection and temporarily disconnect you from the network.
Proceed with installation now?
Version 7.1.6
Yes
No

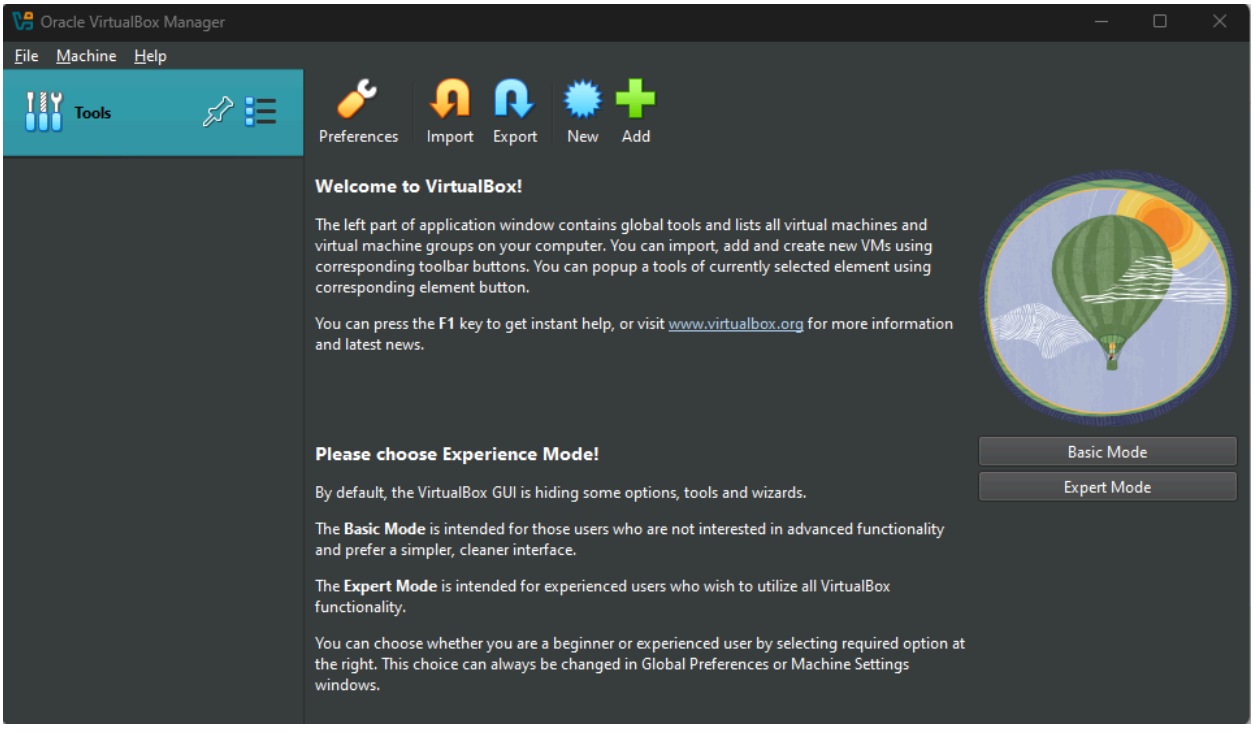

Oracle VirtualBox 7.1.6
Missing Dependencies
Python Core / win32api
Installing the Oracle VirtualBox 7.1.6 Python bindings requires the Python Core package and the win32api bindings to be installed first.
When continuing the installation of the Oracle VirtualBox 7.1.6 Python bindings now, those need to be set up manually later. Refer to the Oracle VirtualBox 7.1.6 SDK manual for more information.
Proceed with installation now?
Version 7.1.6
Yes
No


Oracle VirtualBox 7.1.6 Setup
Custom Setup
Select the way you want features to be installed.
Please choose from the options below:
Create start menu entries
Create a shortcut on the desktop
Create a shortcut in the Quick Launch Bar
Register file associations
Version 7.1.6
< Back
Next >
Cancel


Oracle VirtualBox 7.1.6 Setup
Ready to Install
The Setup Wizard is ready to begin the Custom installation.
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Version 7.1.6
< Back
Install
Cancel

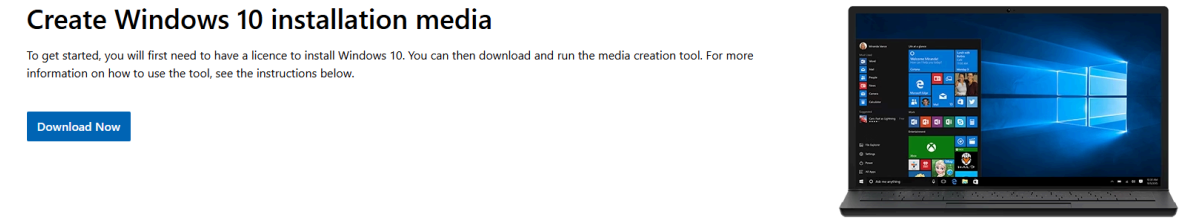

Oracle VirtualBox 7.1.6 Setup
Oracle VirtualBox 7.1.6
Please wait while the Setup Wizard installs Oracle VirtualBox 7.1.6. This may take several minutes.
Status:
Version 7.1.6
< Back
Next >
Cancel



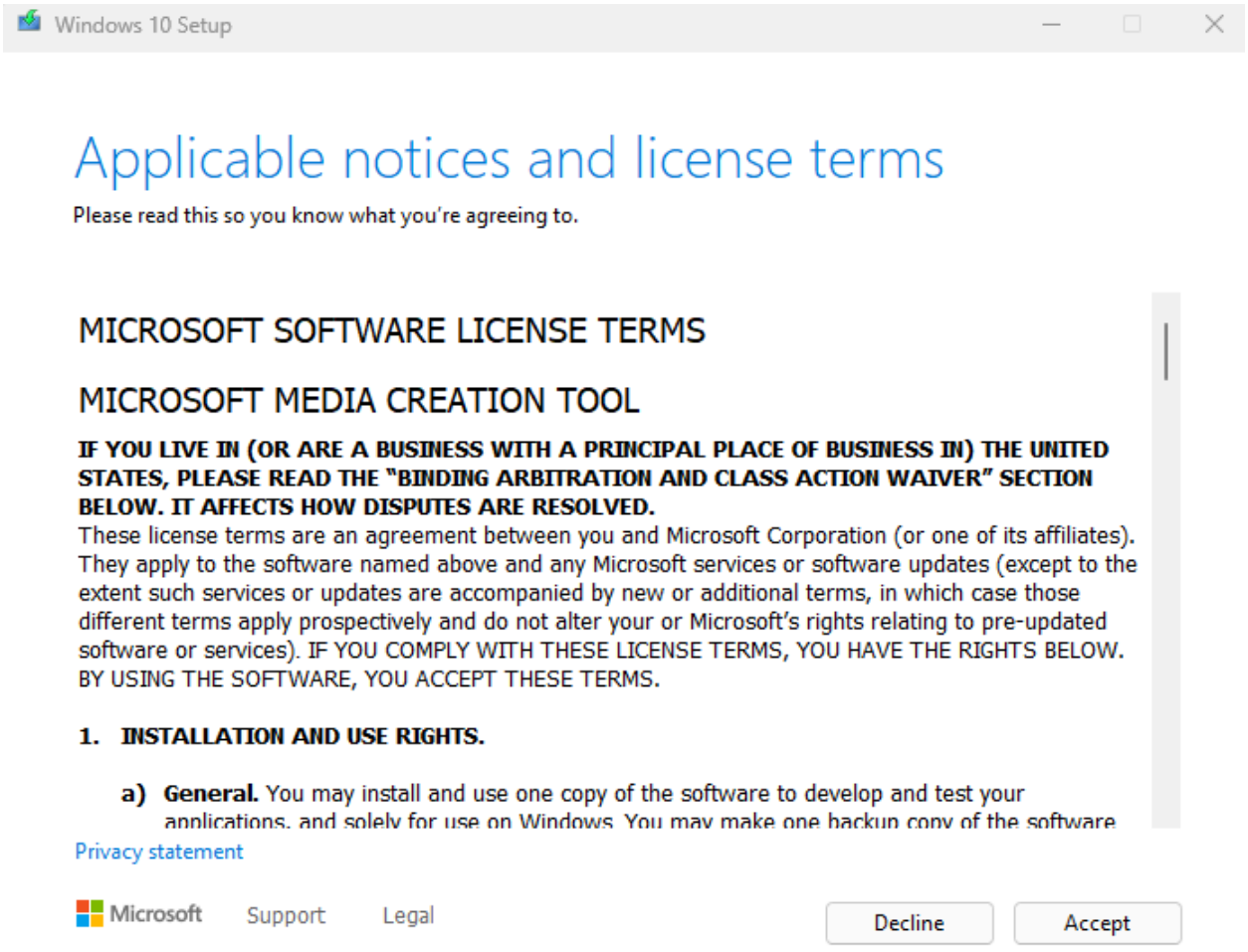


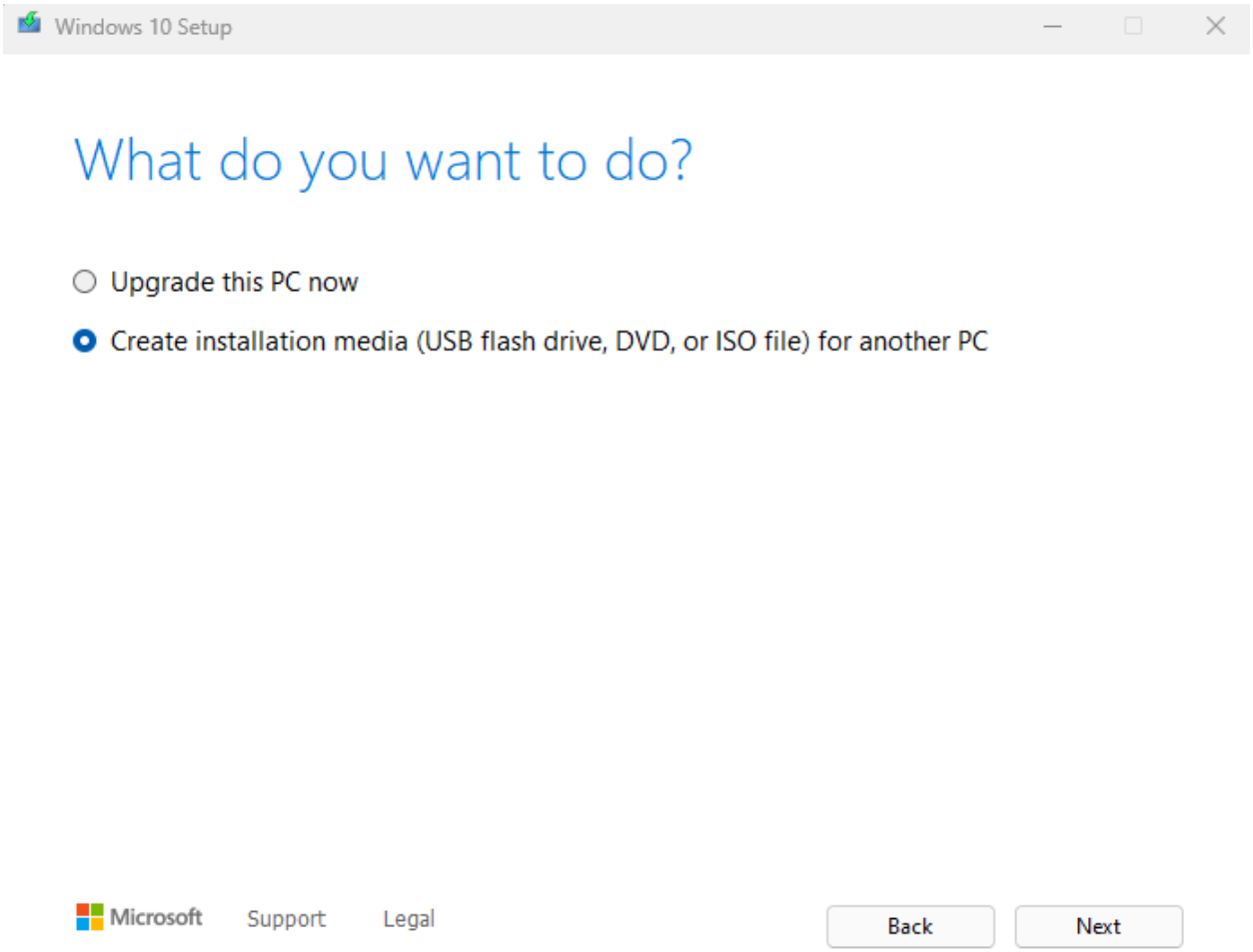
2. Install Windows 10

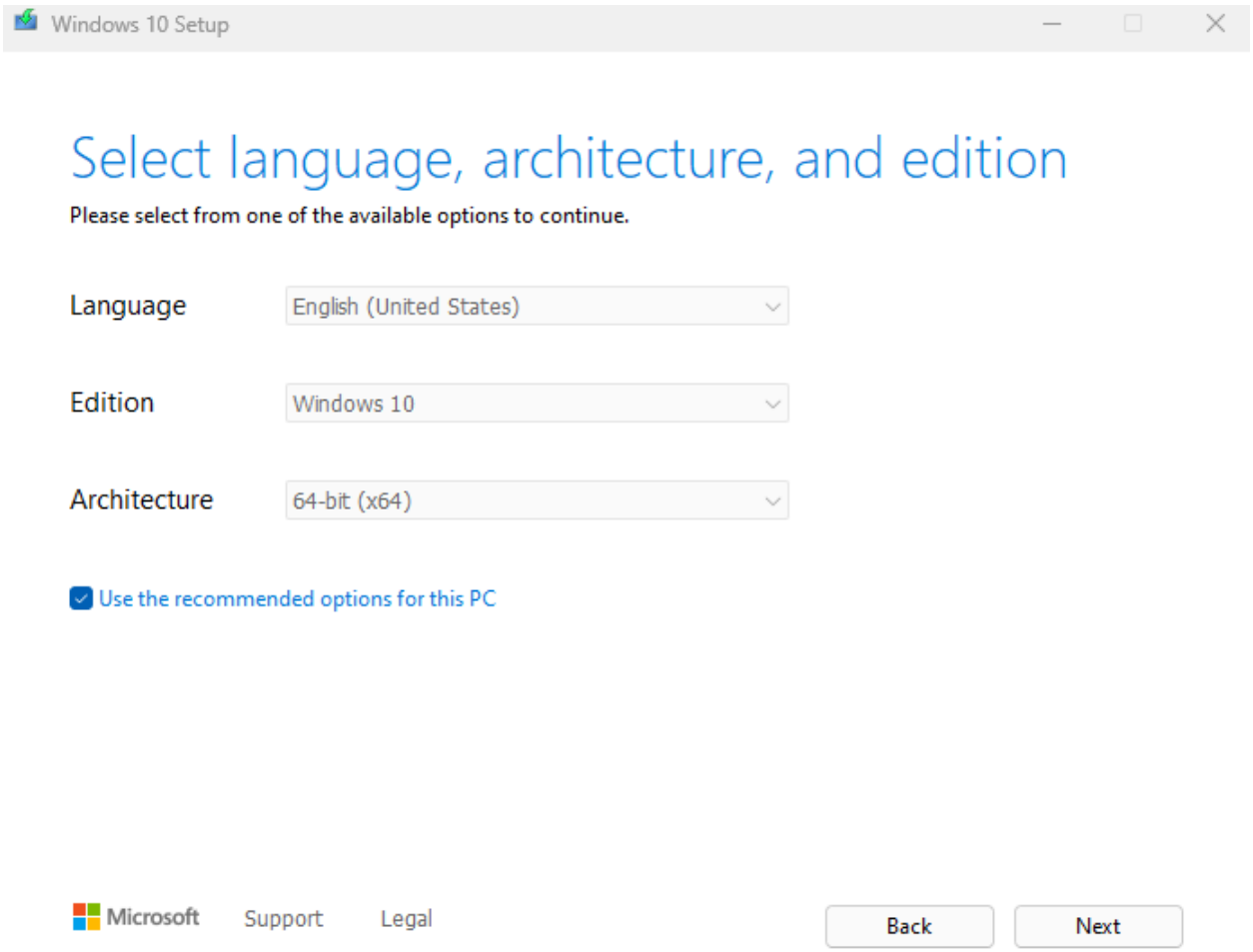
Download Window ISO Image through this link (https://www.microsoft.com/en-ca/software-download/windows10)

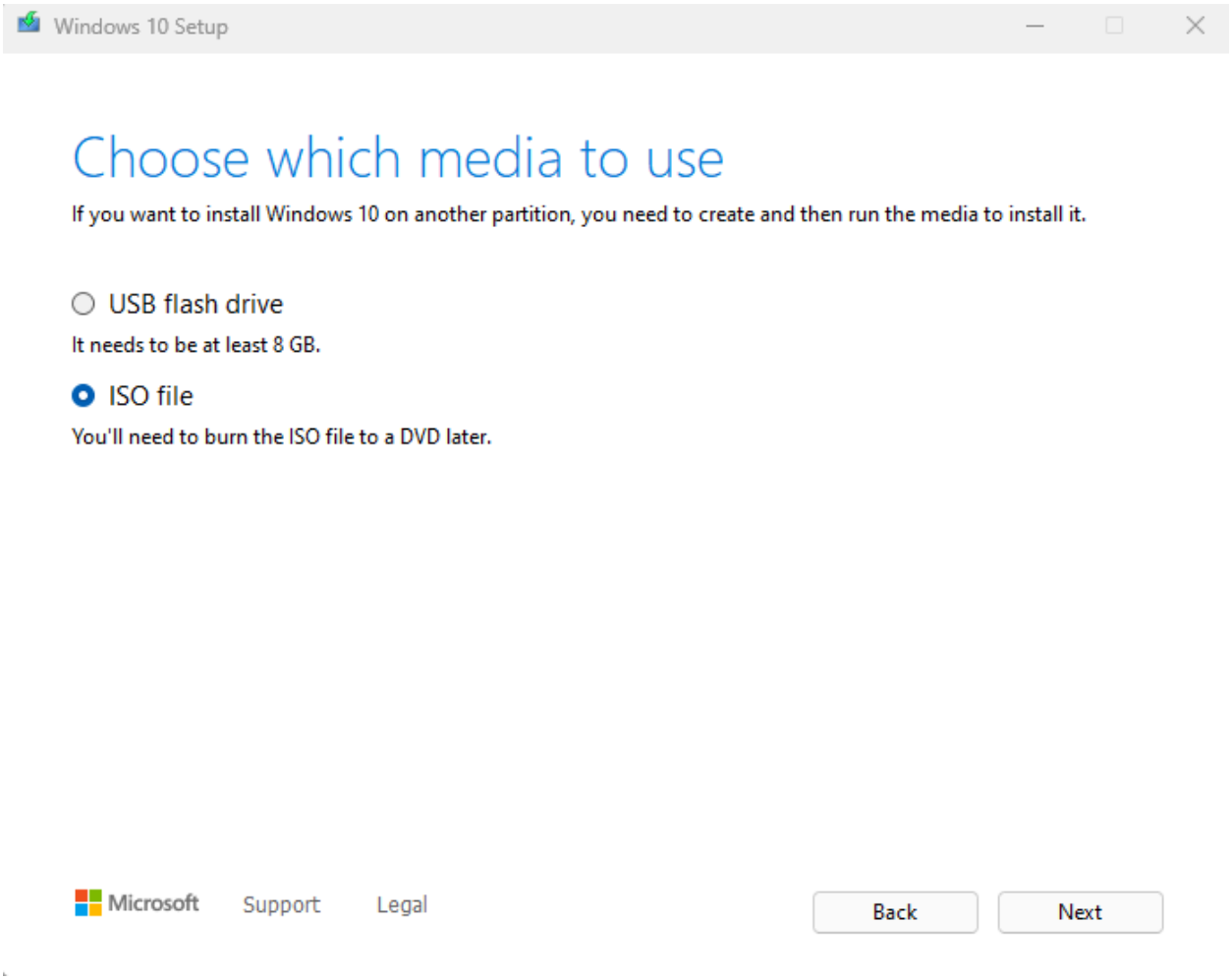


After that run the .exe installer file

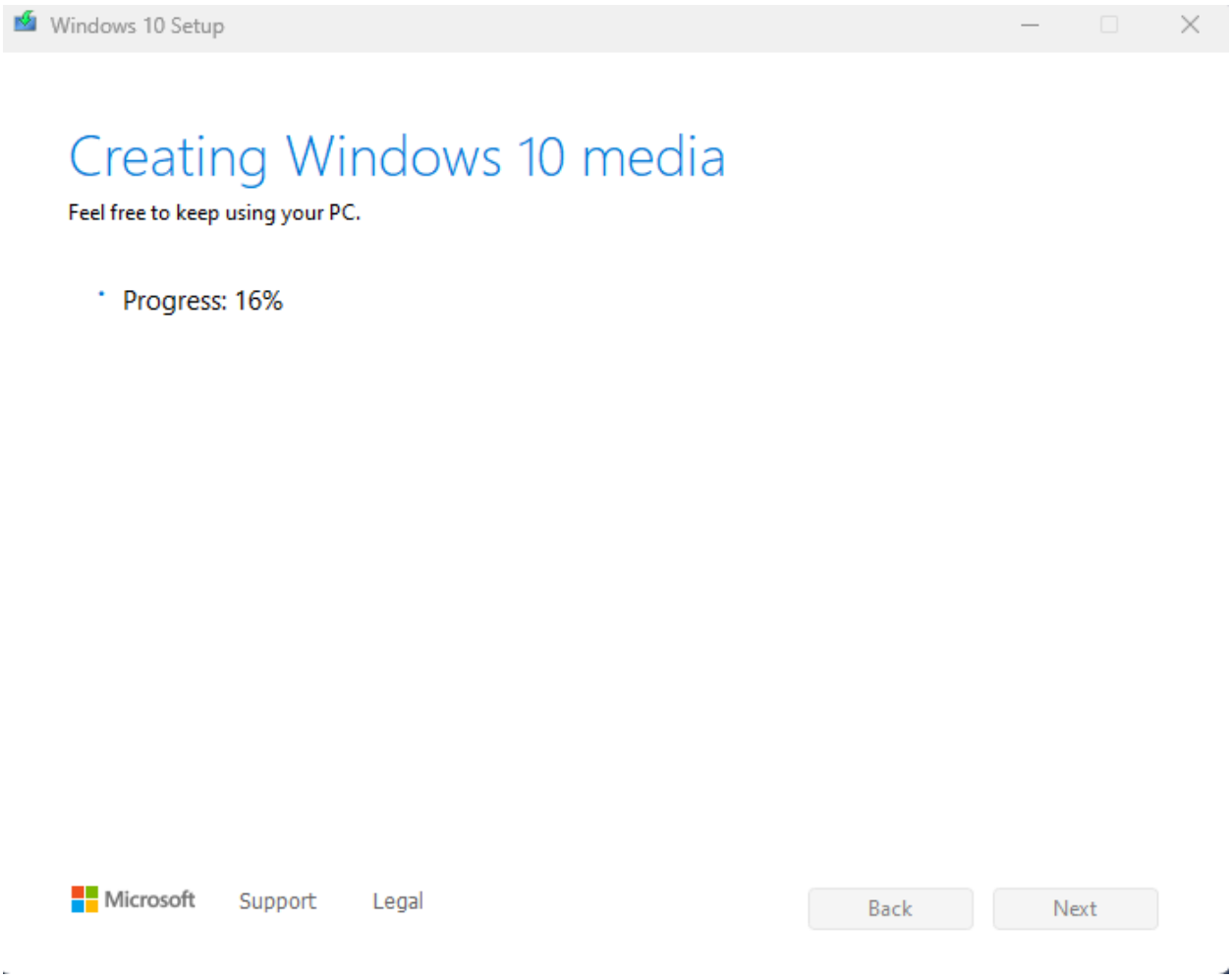


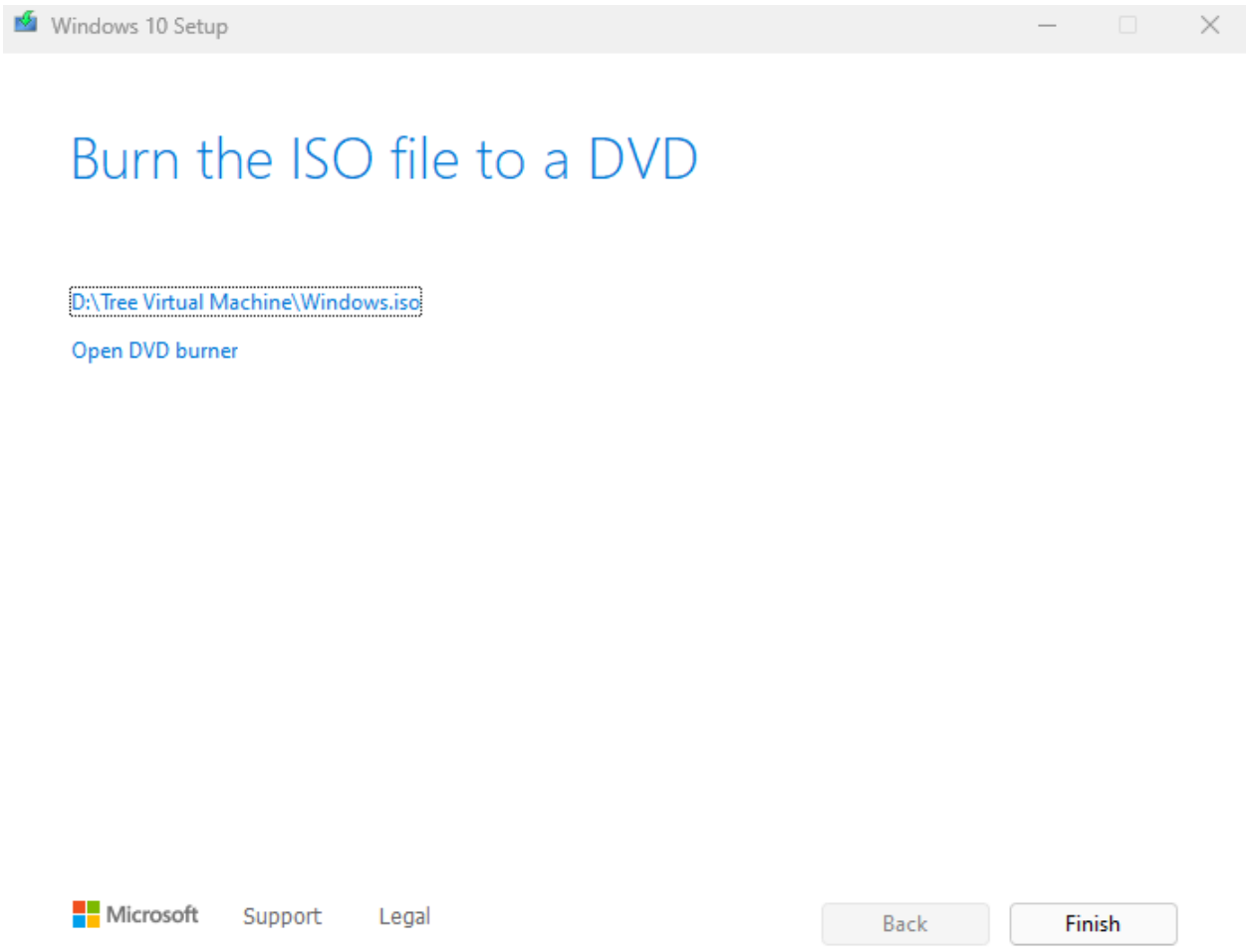

Windows 10 Setup
What do you want to do?
Upgrade this PC now
Create installation media (USB flash drive, DVD, or ISO file) for another PC
Microsoft
Support
Legal
Back
Next


Windows 10 Setup
Select language, architecture, and edition
Please select from one of the available options to continue.
Language
English (United States)
Edition
Windows 10
Architecture
64-bit (x64)
Use the recommended options for this PC
Microsoft
Support
Legal
Back
Next

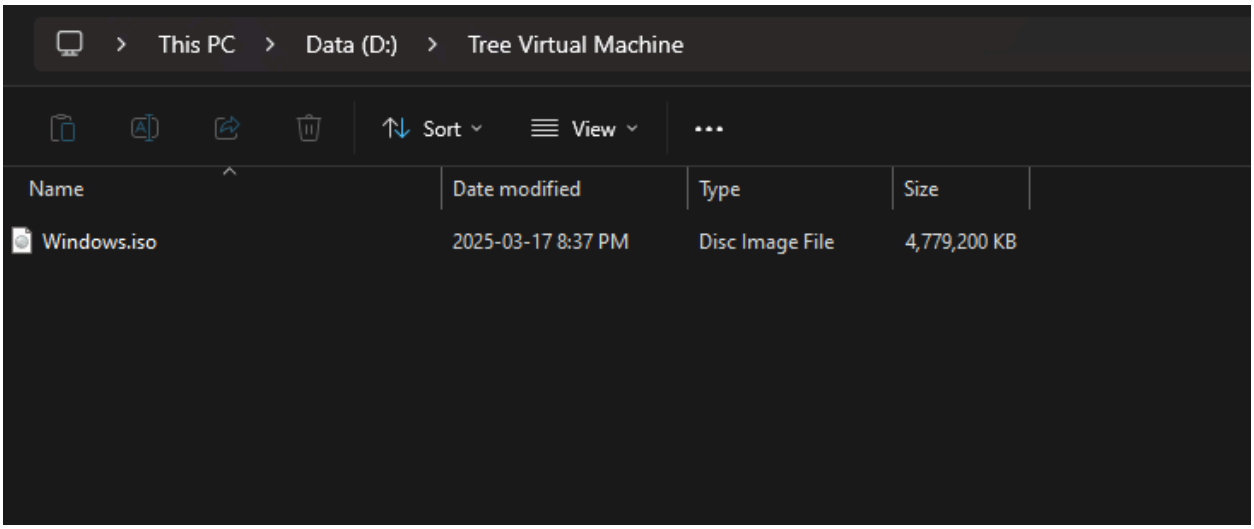


After Next, it will ask you to install the windows.iso to folder location you prefer, choose your location then install.

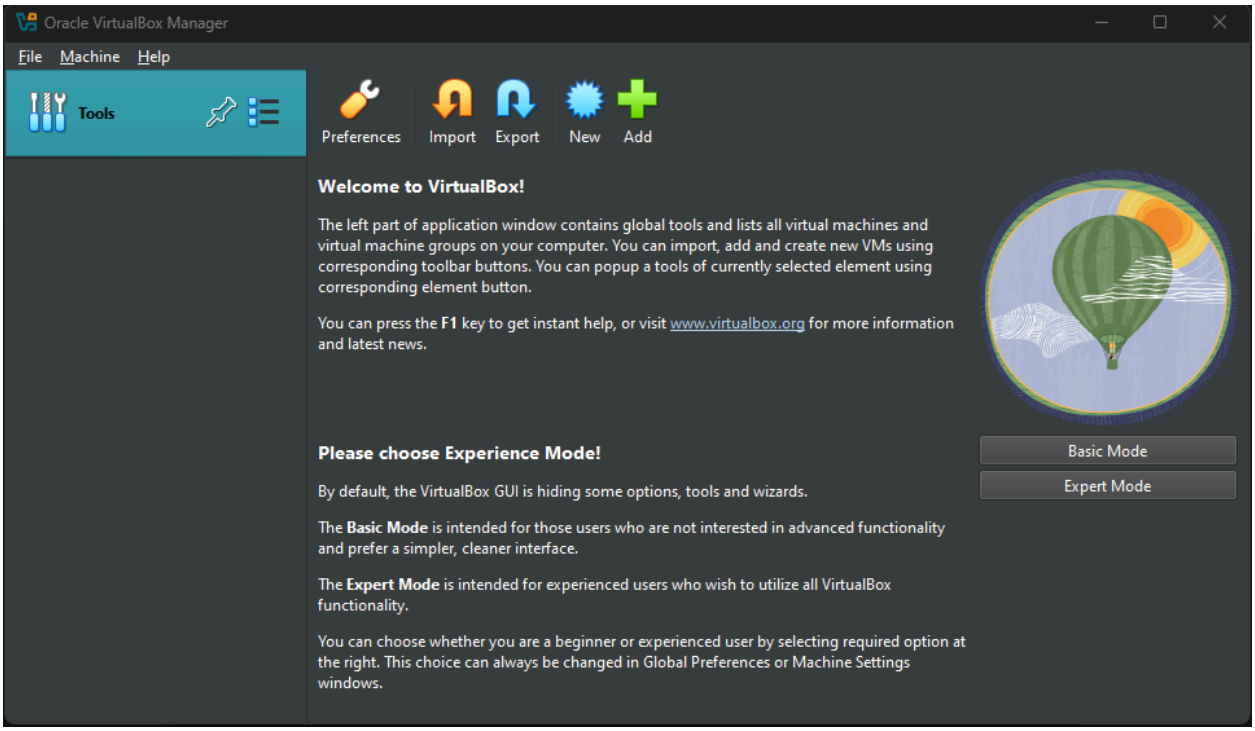

Windows 10 Setup
Creating Windows 10 media
Feel free to keep using your PC.
Progress: 16%
Microsoft
Support
Legal
Back
Next

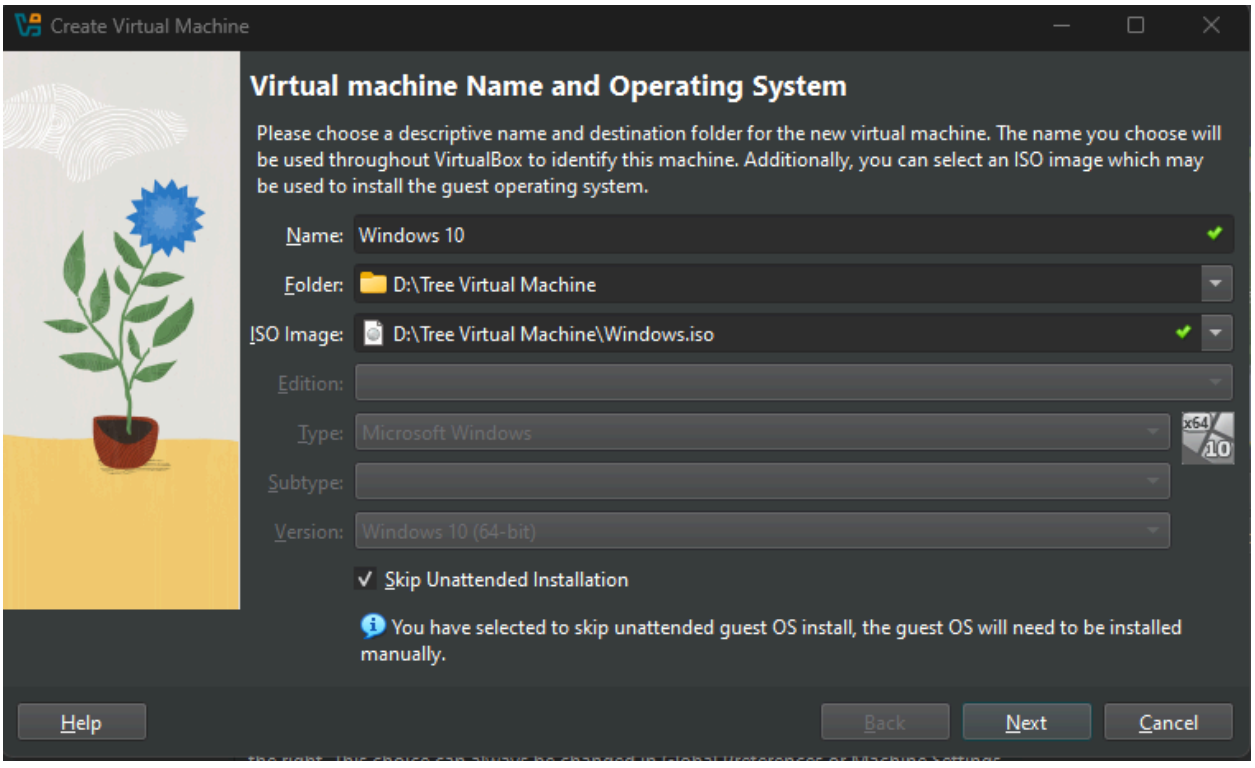


After finish you should see the windows.iso in your prefer folder:



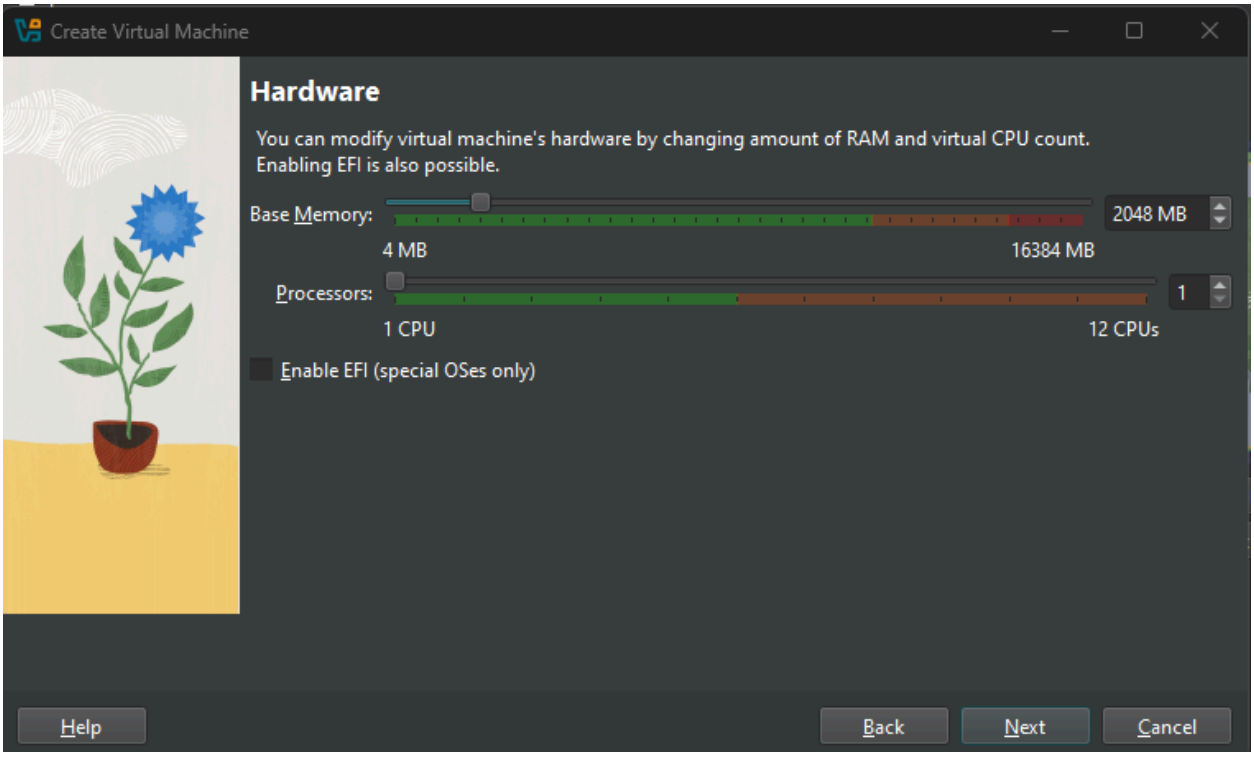
Time to create a Windows 10 Virtual Machine



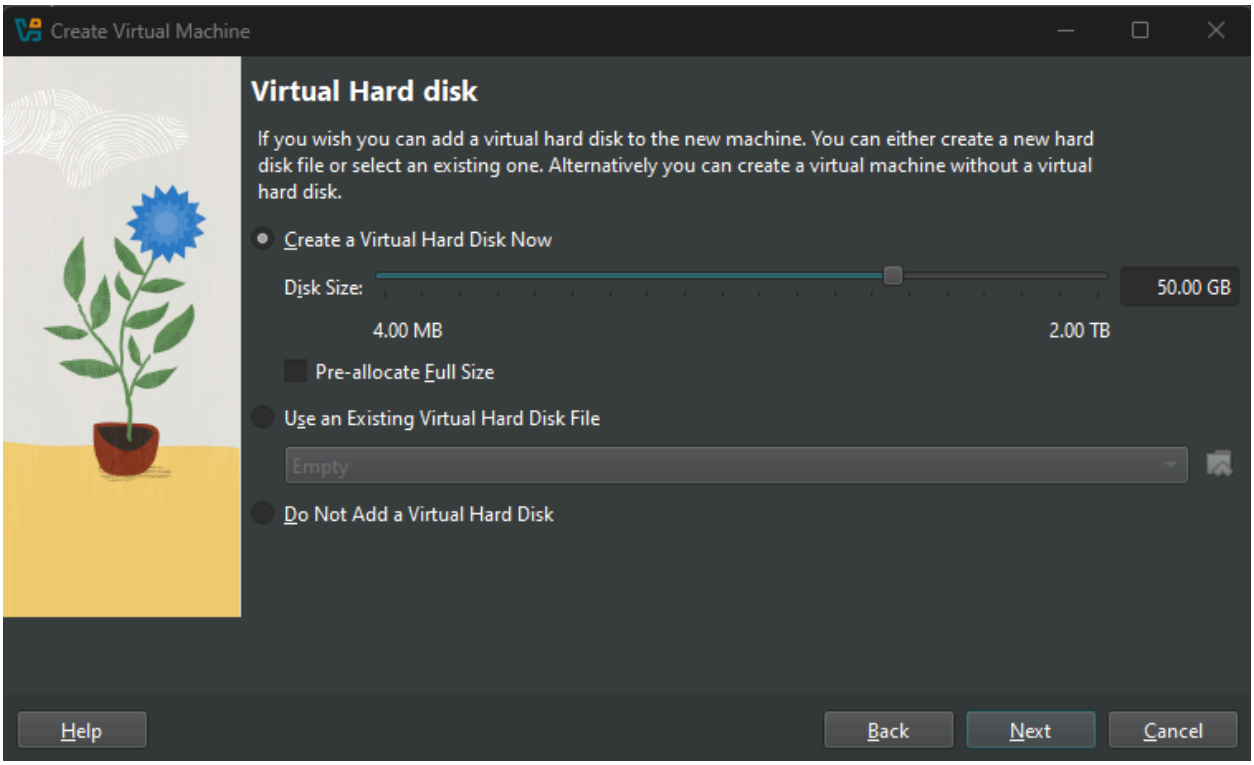


- Set up your VM Name

- Choose folder to store the VM storage and file
- Choose the windows.iso file we install earlier for the ISO Image section
- Select “Skip Unattended Installation” so that you can install the Operate System manually (Option)

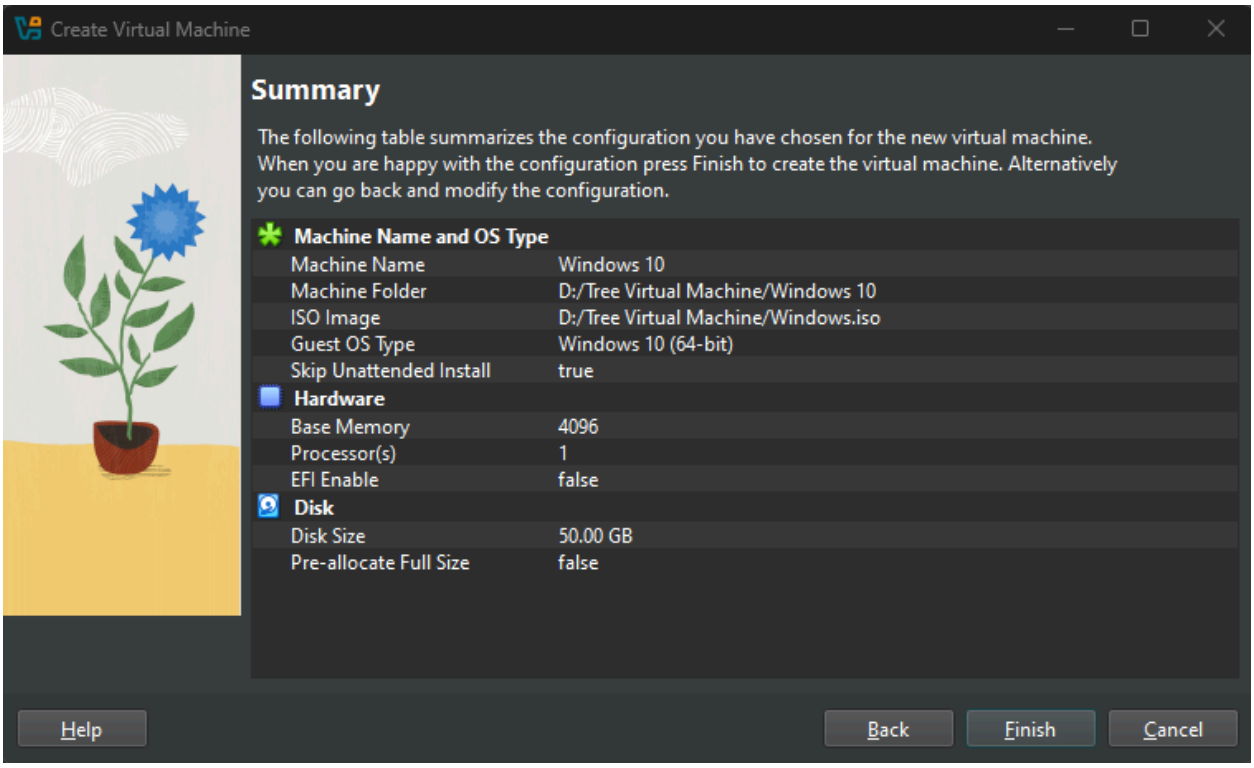


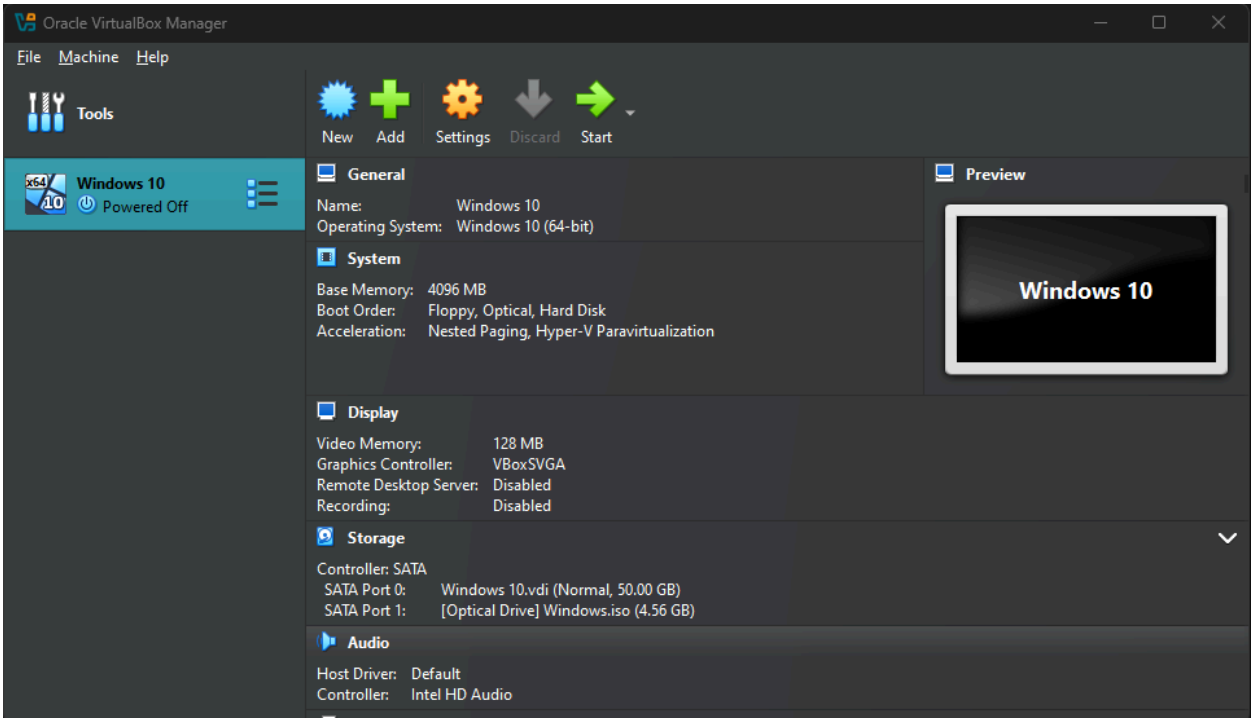
Please note that for this section we will configurate our VM (Virtual Machine) specifications, base on your computer specifications so be aware of how you adjust the memory and disk space.

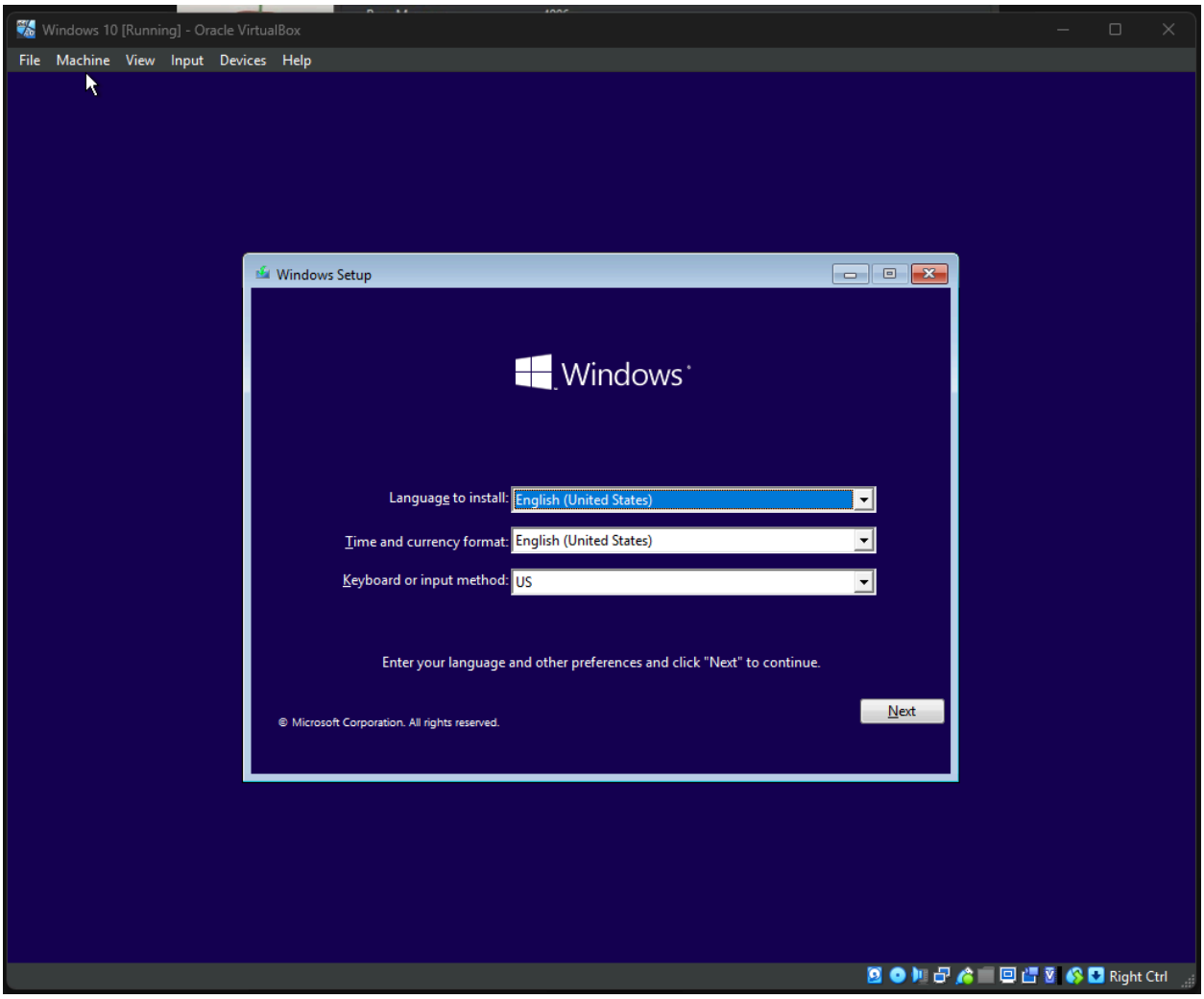


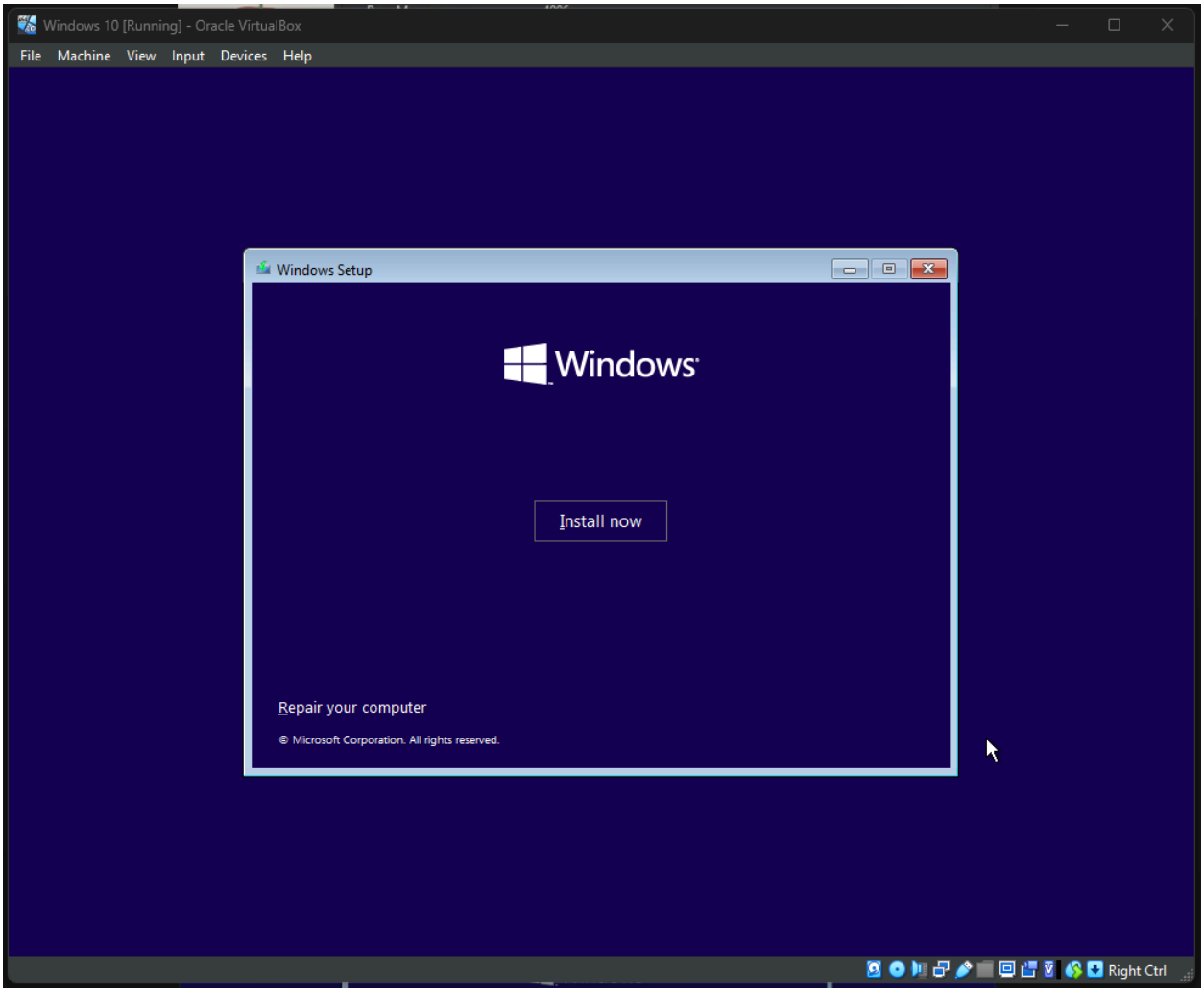
In summary, my Windows 10 VM Specification will be:

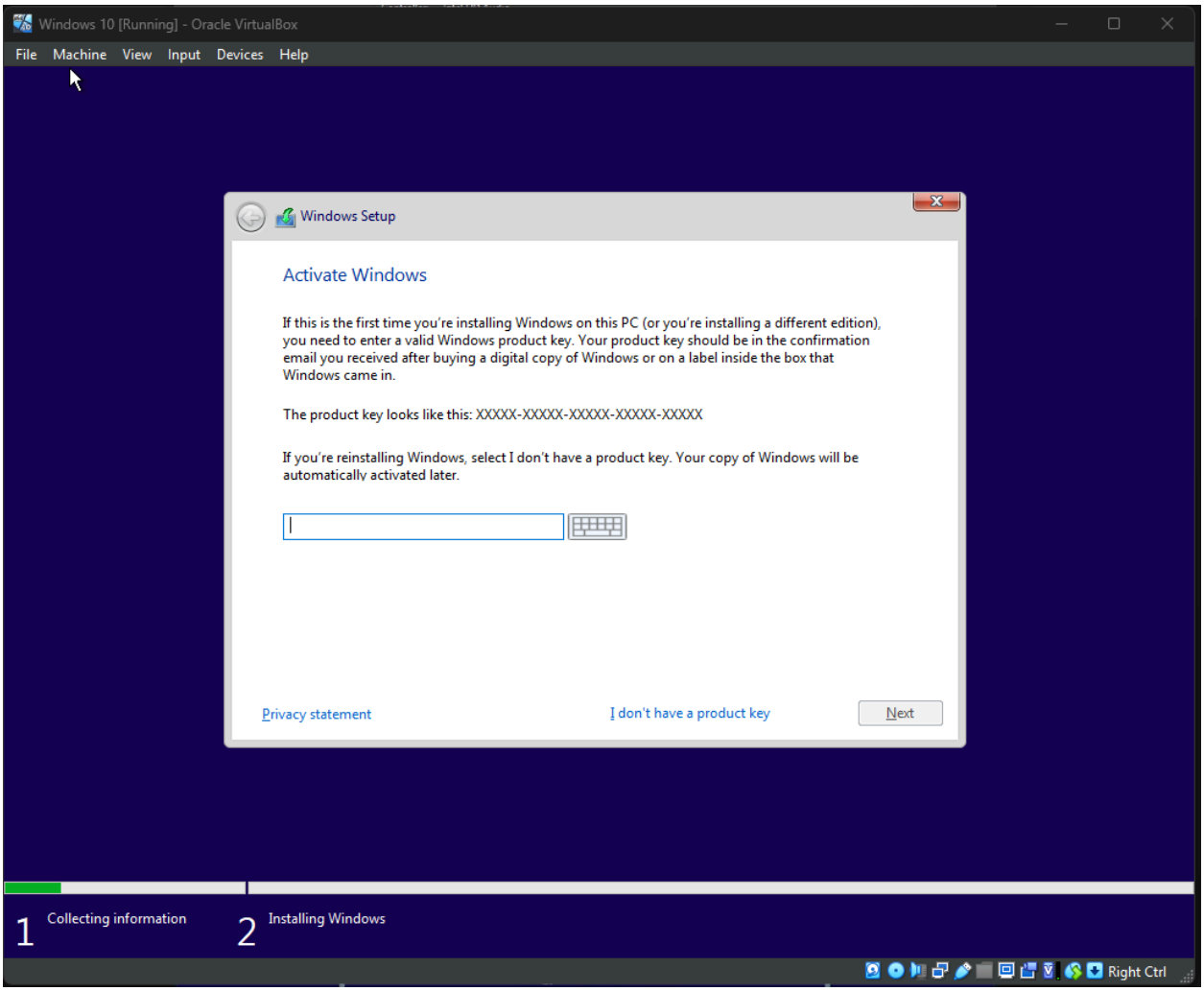
- Memory: 4GBs
- CPU: 1
- Hard Disk: 50Gbs


Create Virtual Machine
Summary
The following table summarizes the configuration you have chosen for the new virtual machine. When you are happy with the configuration press Finish to create the virtual machine. Alternatively you can go back and modify the configuration.
Machine Name and OS Type
Machine Name Windows 10
Machine Folder D:/Tree Virtual Machine/Windows 10
ISO Image D:/Tree Virtual Machine/Windows.iso
Guest OS Type Windows 10 (64-bit)
Skip Unattended Install true
Hardware
Base Memory 4096
Processor(s) 1
EFI Enable false
Disk
Disk Size 50.00 GB
Pre-allocate Full Size false
Help
Back
Finish
Cancel

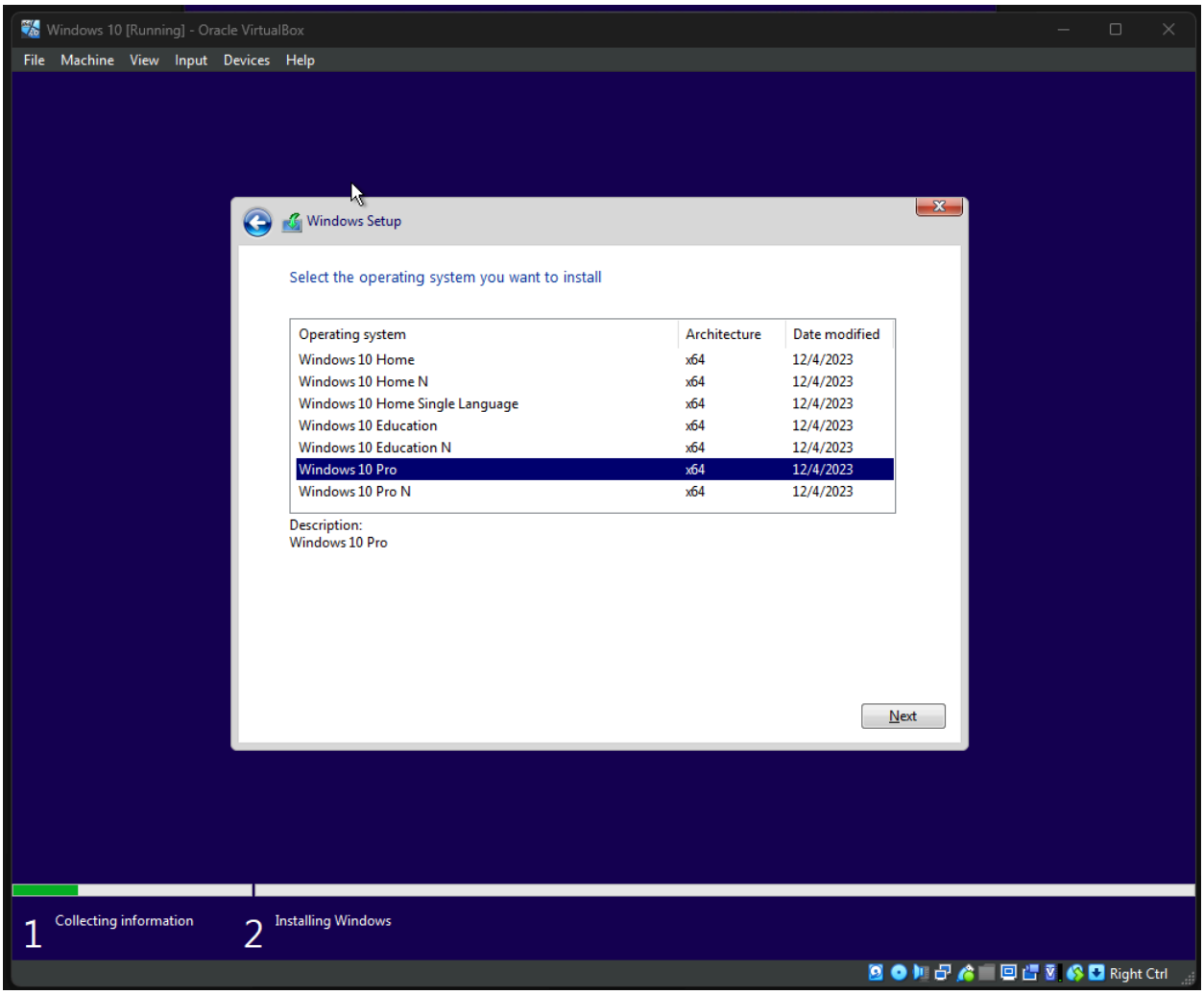

Oracle VirtualBox Manager
File Machine Help
Tools
New Add Settings Discard Start
Windows 10
Powered Off
General
Name: Windows 10
Operating System: Windows 10 (64-bit)
System
Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, Hyper-V Paravirtualization
Preview
Windows 10
Display
Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: SATA
SATA Port 0: Windows 10.vdi (Normal, 50.00 GB)
SATA Port 1: [Optical Drive] Windows.iso (4.56 GB)
Audio
Host Driver: Default
Controller: Intel HD Audio


Windows 10 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Windows Setup
Windows
Language to install: English (United States)
Time and currency format: English (United States)
Keyboard or input method: US
Enter your language and other preferences and click "Next" to continue.
© Microsoft Corporation. All rights reserved.
Next
Right Ctrl

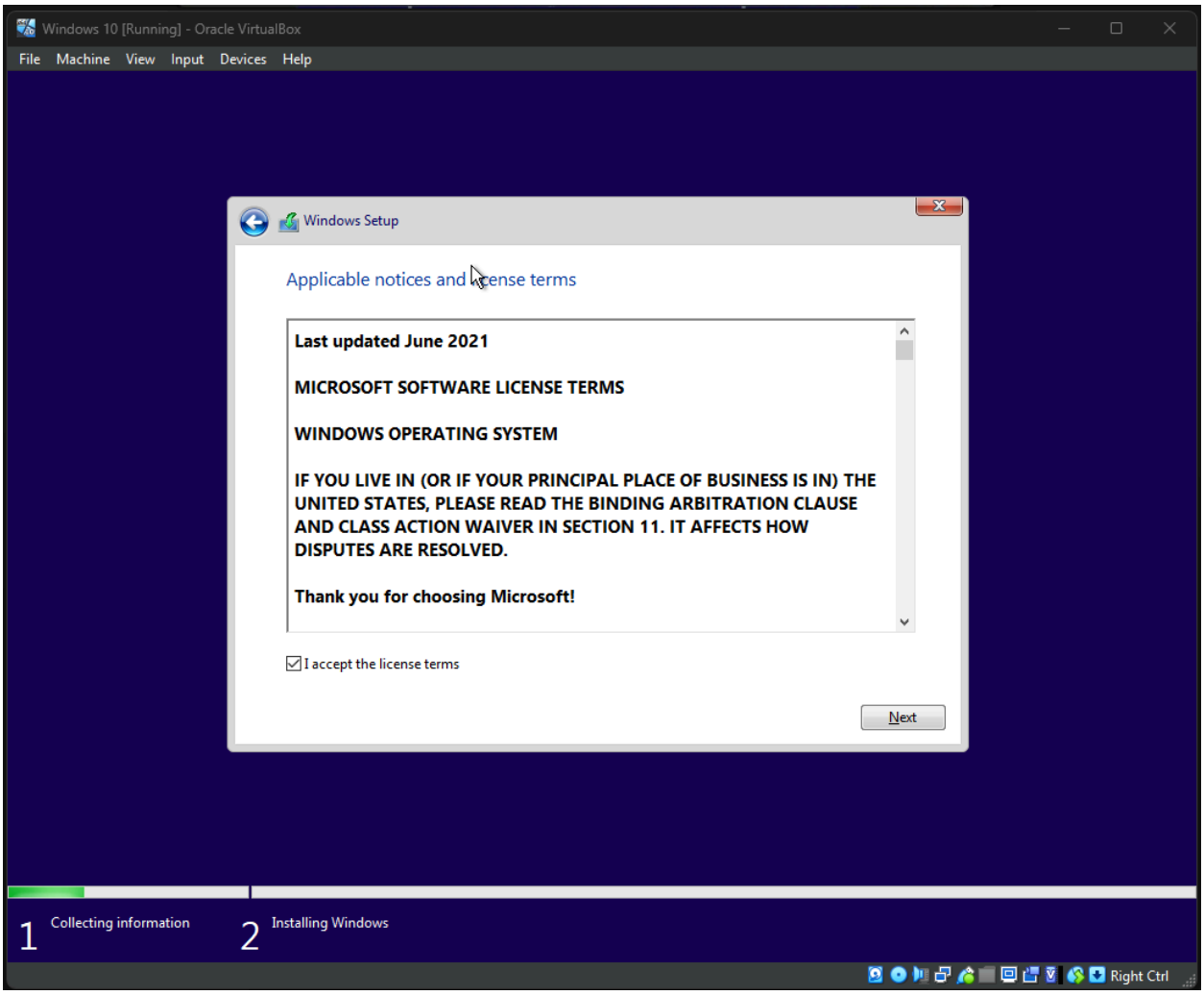

Windows 10 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Windows Setup
Windows
Install now
Repair your computer
© Microsoft Corporation. All rights reserved.
Right Ctrl

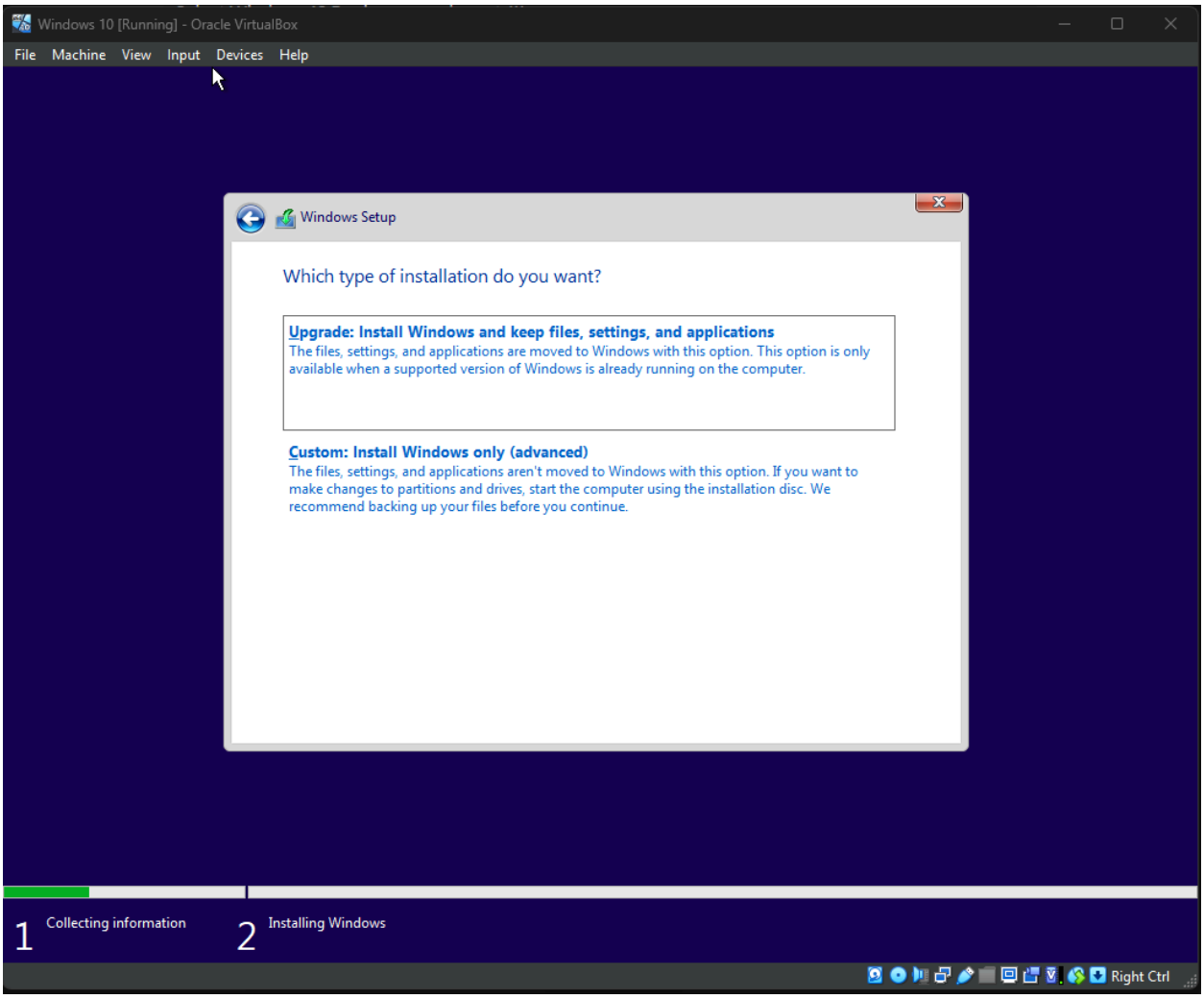


Click “I don’t have a product key”

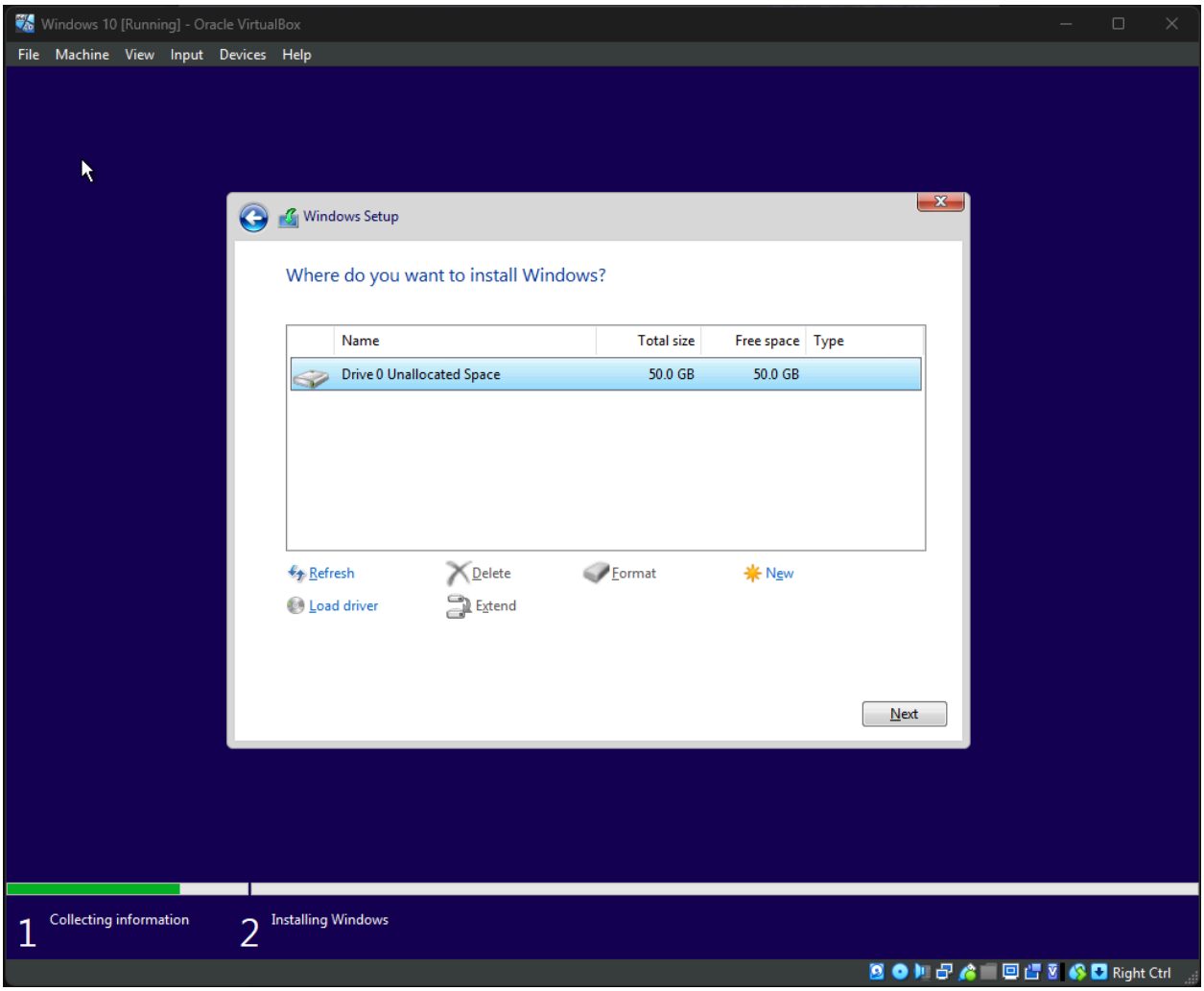


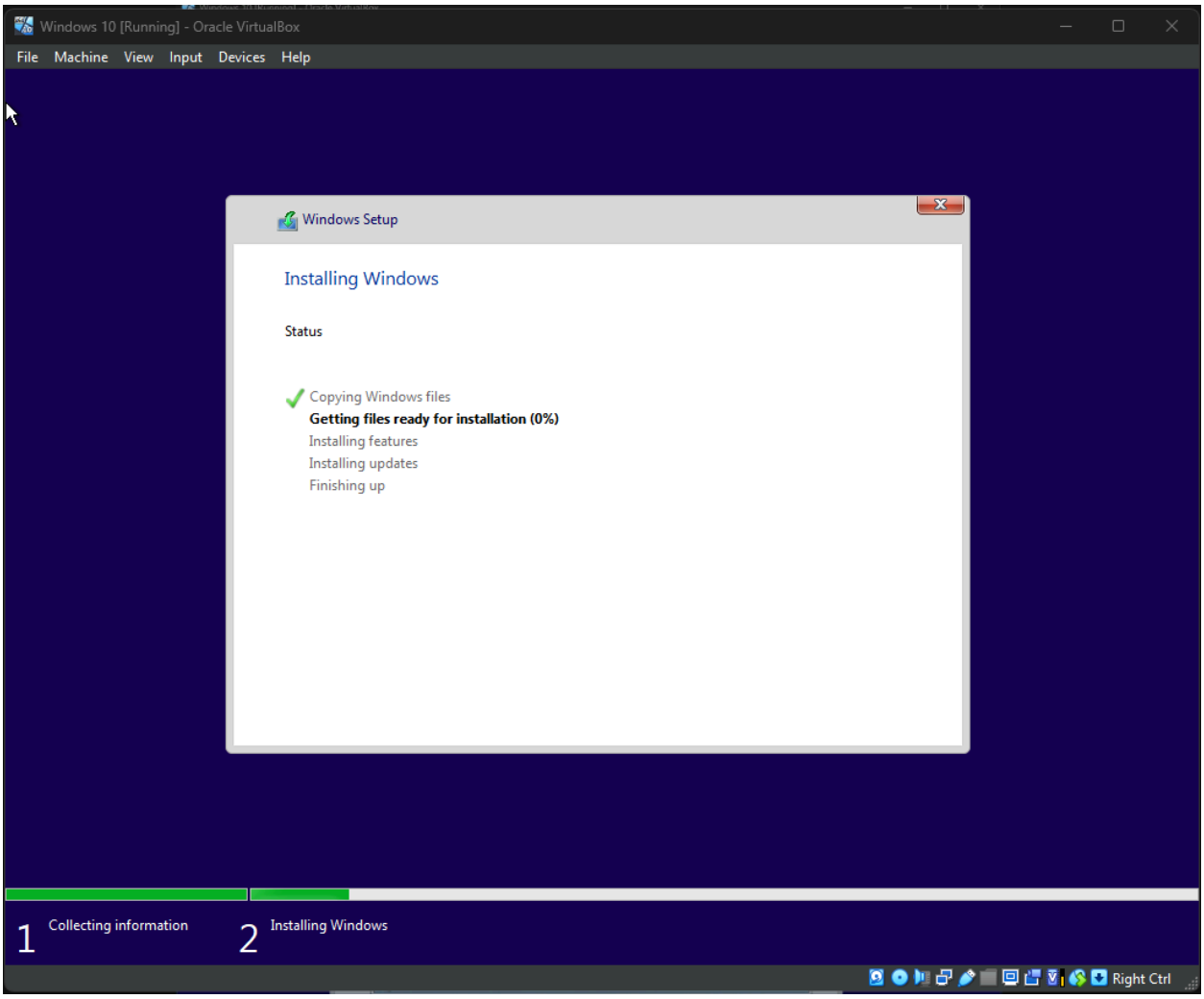
Select Windows 10 Pro because why not :)))


Windows 10 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Windows Setup
Applicable notices and license terms
Last updated June 2021
MICROSOFT SOFTWARE LICENSE TERMS
WINDOWS OPERATING SYSTEM
IF YOU LIVE IN (OR IF YOUR PRINCIPAL PLACE OF BUSINESS IS IN) THE UNITED STATES, PLEASE READ THE BINDING ARBITRATION CLAUSE AND CLASS ACTION WAIVER IN SECTION 11. IT AFFECTS HOW DISPUTES ARE RESOLVED.
Thank you for choosing Microsoft!
I accept the license terms
Next
1 Collecting information
2 Installing Windows
Right Ctrl



Click “Custom: Install Windows only (advanced)”

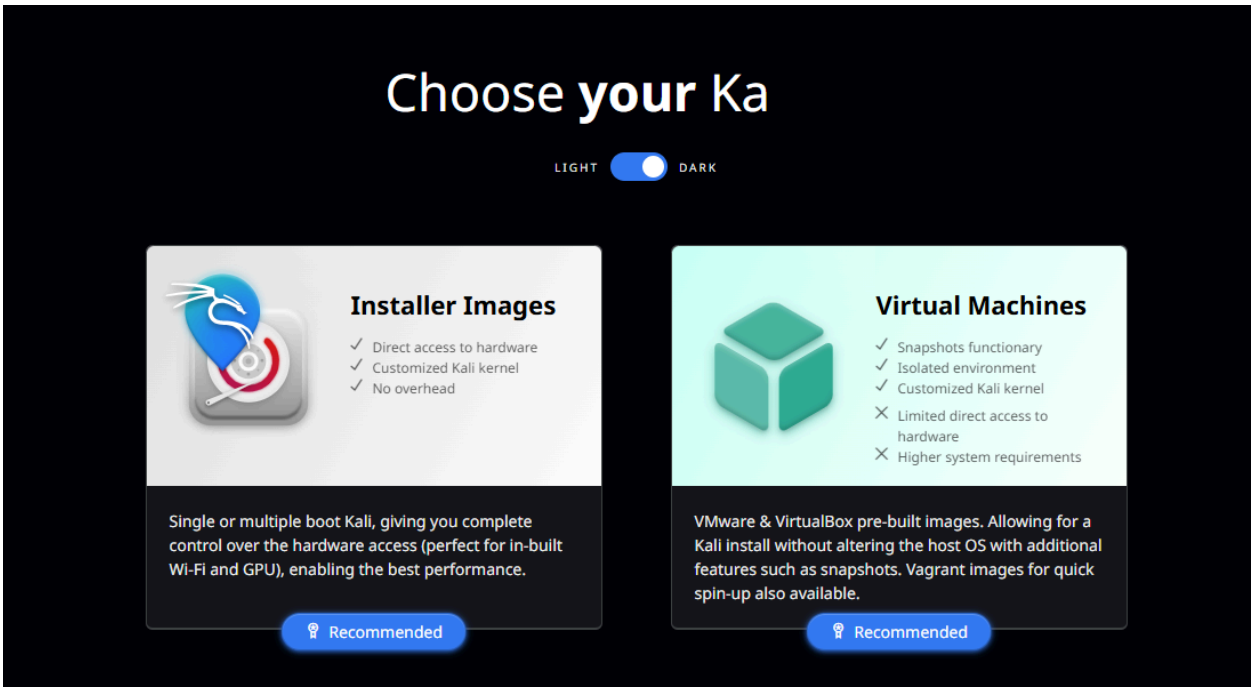

Windows 10 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Windows Setup
Where do you want to install Windows?
Name
Total size
Free space
Type
Drive 0 Unallocated Space
50.0 GB
50.0 GB
Refresh
Delete
Format
New
Load driver
Extend
Next
1 Collecting information
2 Installing Windows
Right Ctrl



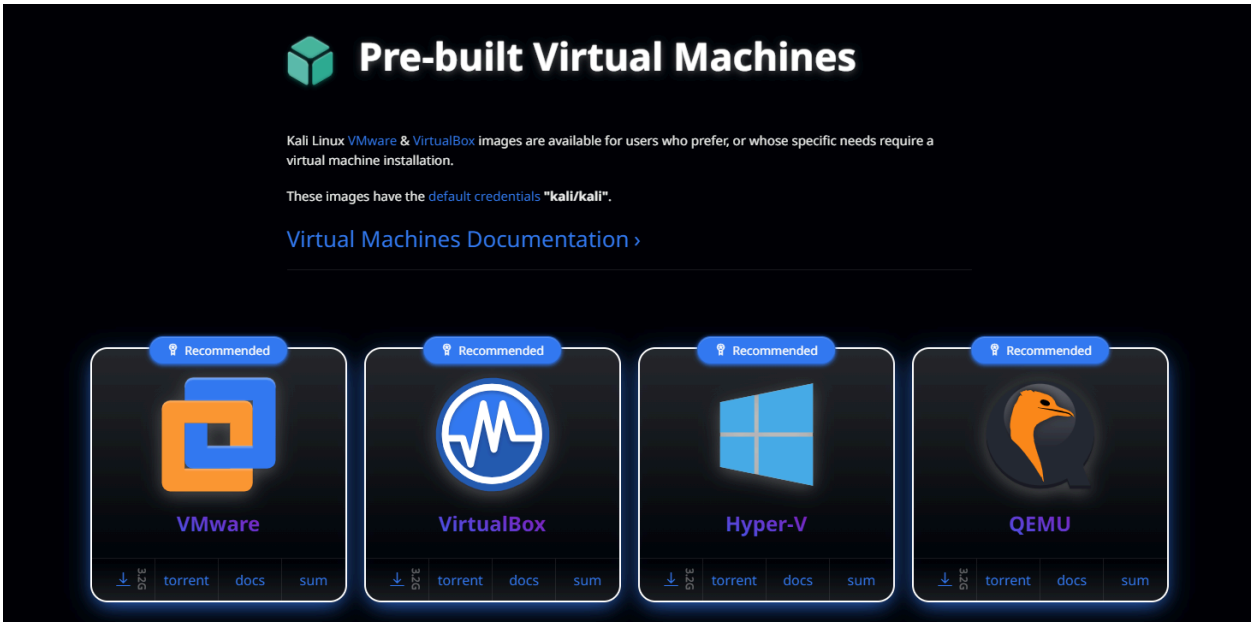
Your Windows 10 VM should be install

3. Install Kali (for adversary side)

Download Kali for Attack VM here https://www.kali.org/get-kali/#kali-platforms

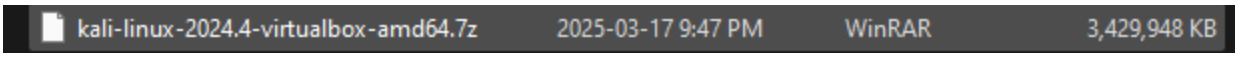


With Installer Images you can install Kali VM manually just how we did with Windows 10 VM. In this case I will choose the Virtual Machine for the Pre-built Virtual Machines.



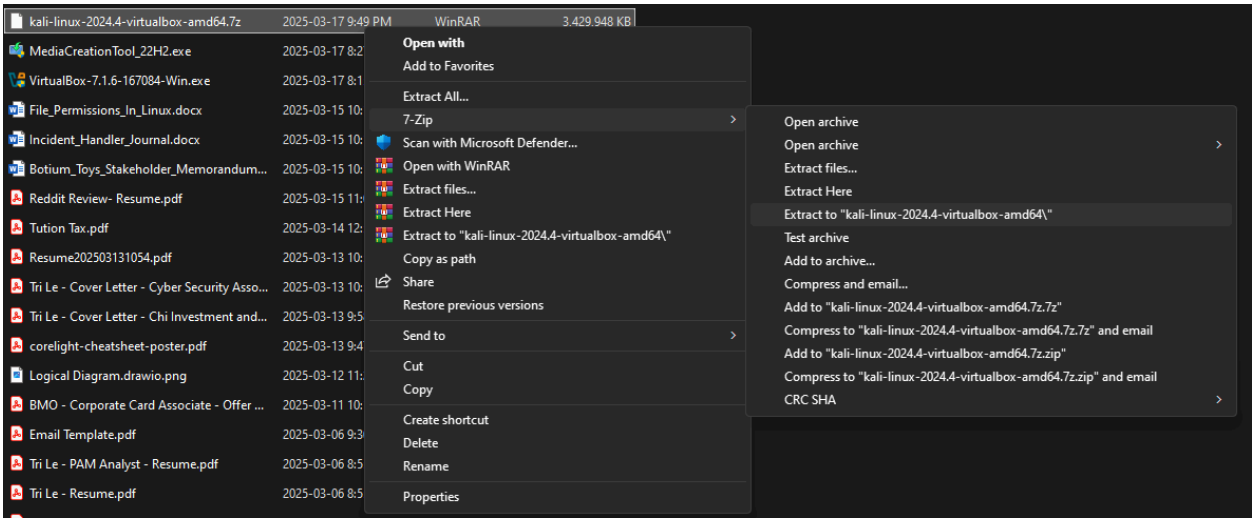
We will choose the Virtual Box option

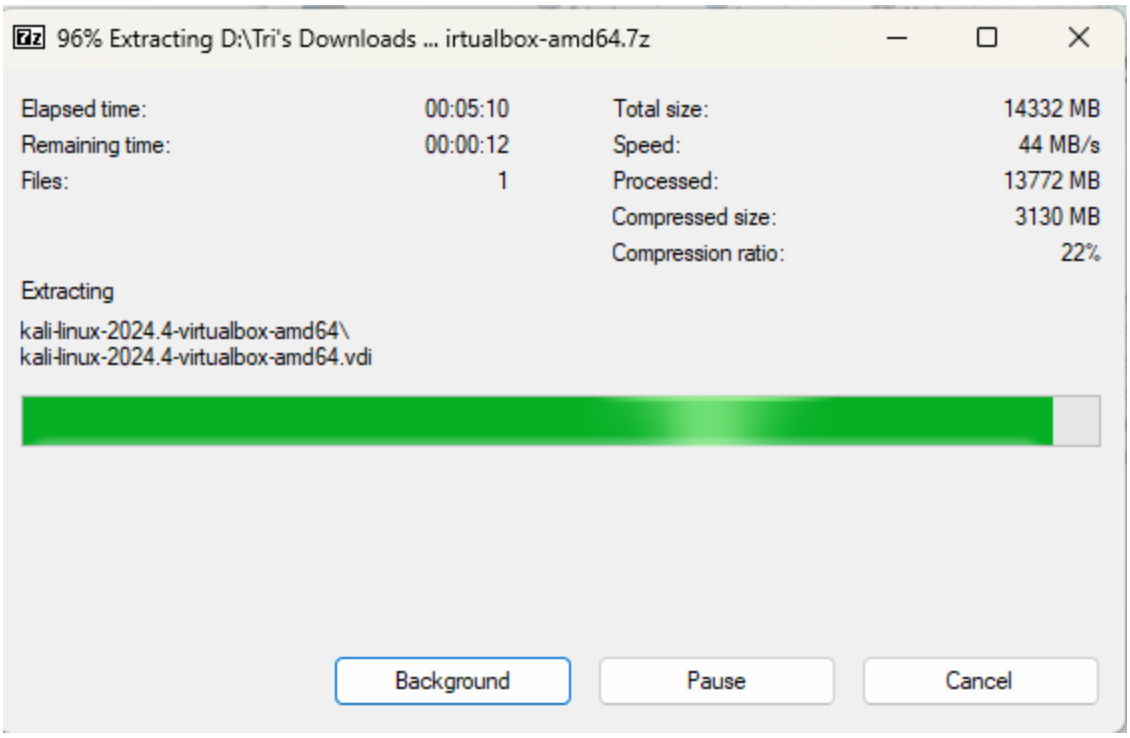
You will need 7-zip install on your machine in order to run the Kali Installer we just download:



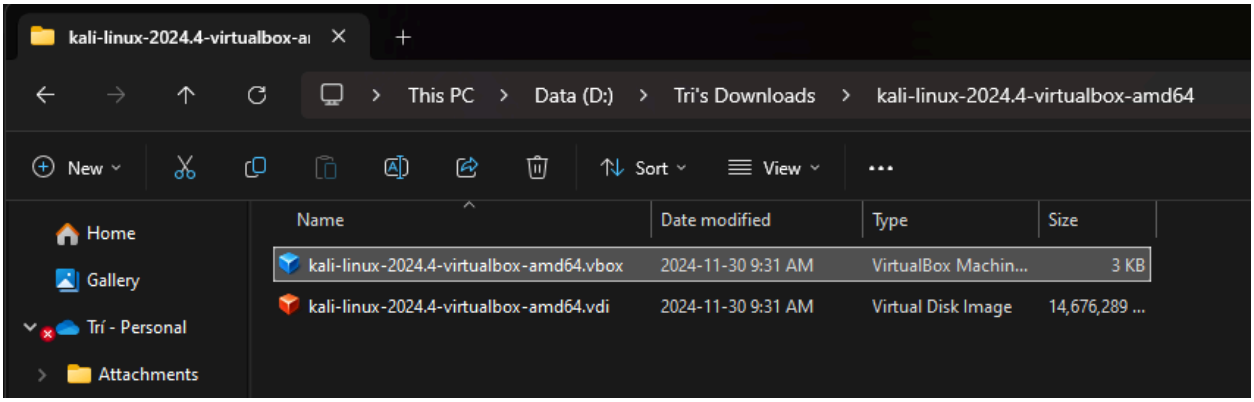
Pleas go to this link to download it, make sure to choose the correct version (it will be 64-bit x64 for me): https://www.7-zip.org/

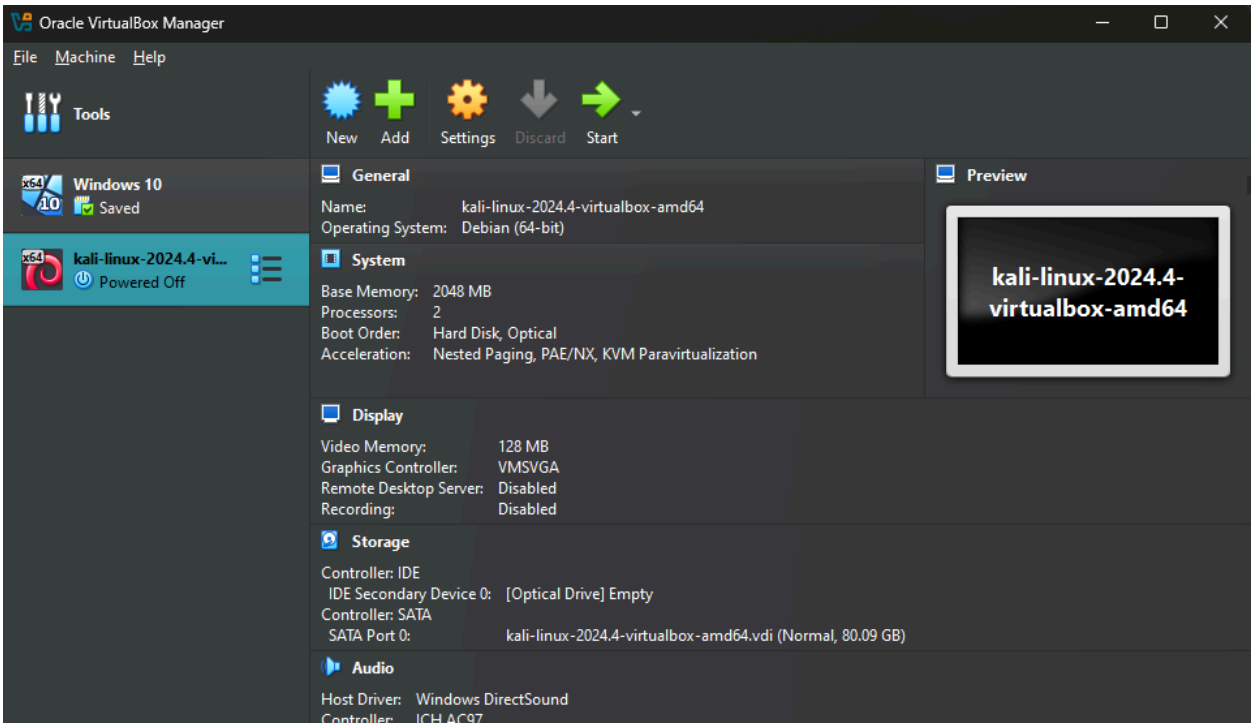
After download 7-zip run the kali virtual box installer using 7-zip:
Right click to “kali-linux-2024.4-virtualbox-amd64.7z”- > Show more options (If applicable) → 7-Zip → Extract to “kali-linux-2024.4-virtualbox-amd64\”





Locate the extract folder and select the vbox extenstion





Kali Virtual Machine will instantly appear for you in Virtual Box.

We can start the Kali VM, for log-in please use this default credentials:

- Username: kali
- Password: kali

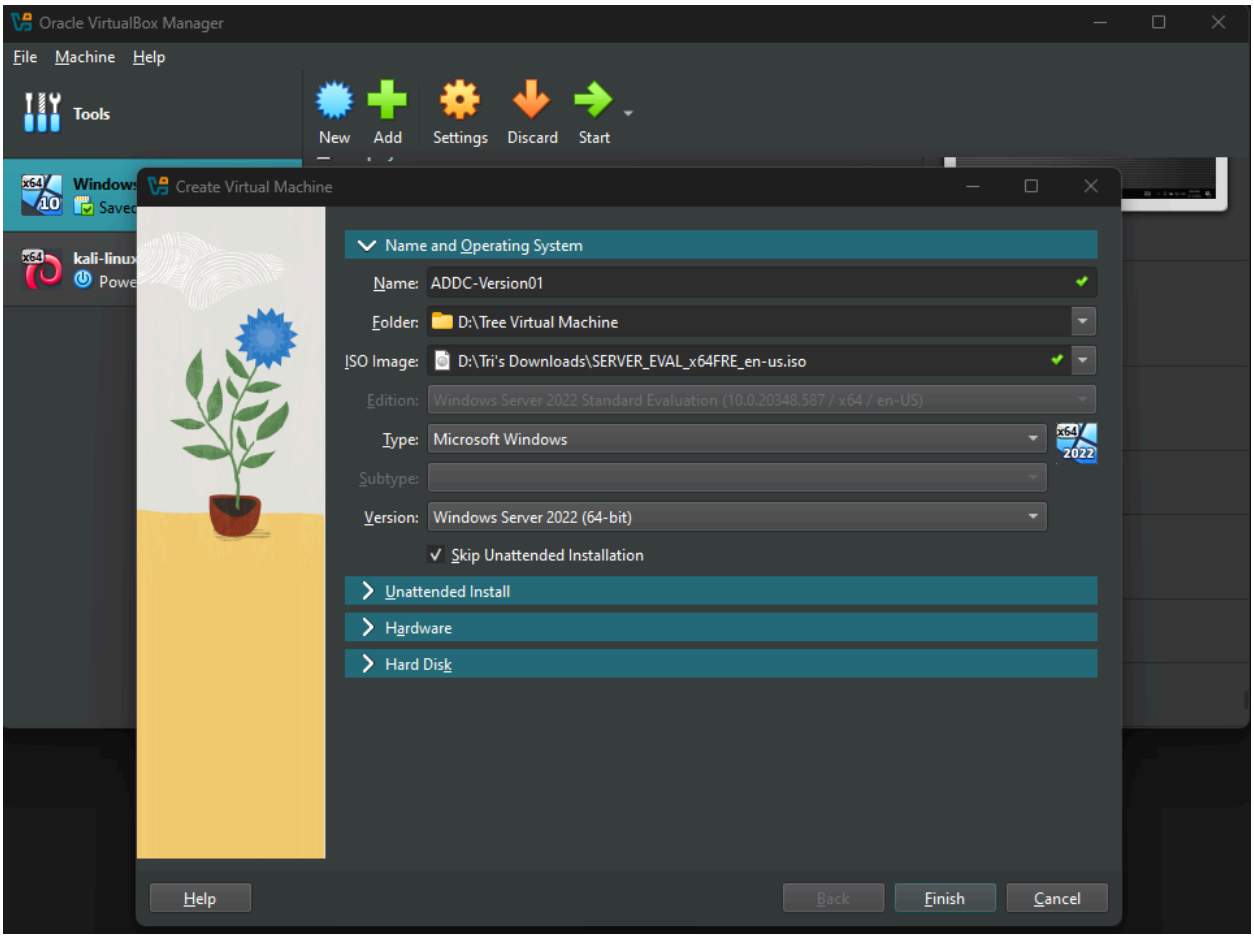
4. Install Windows Server

Download the Windows Server 2022 from this link https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022

Download the ISO

File the information then hit Download Now. Click ISO downloads - 64-bit edition and run the installed iso file.

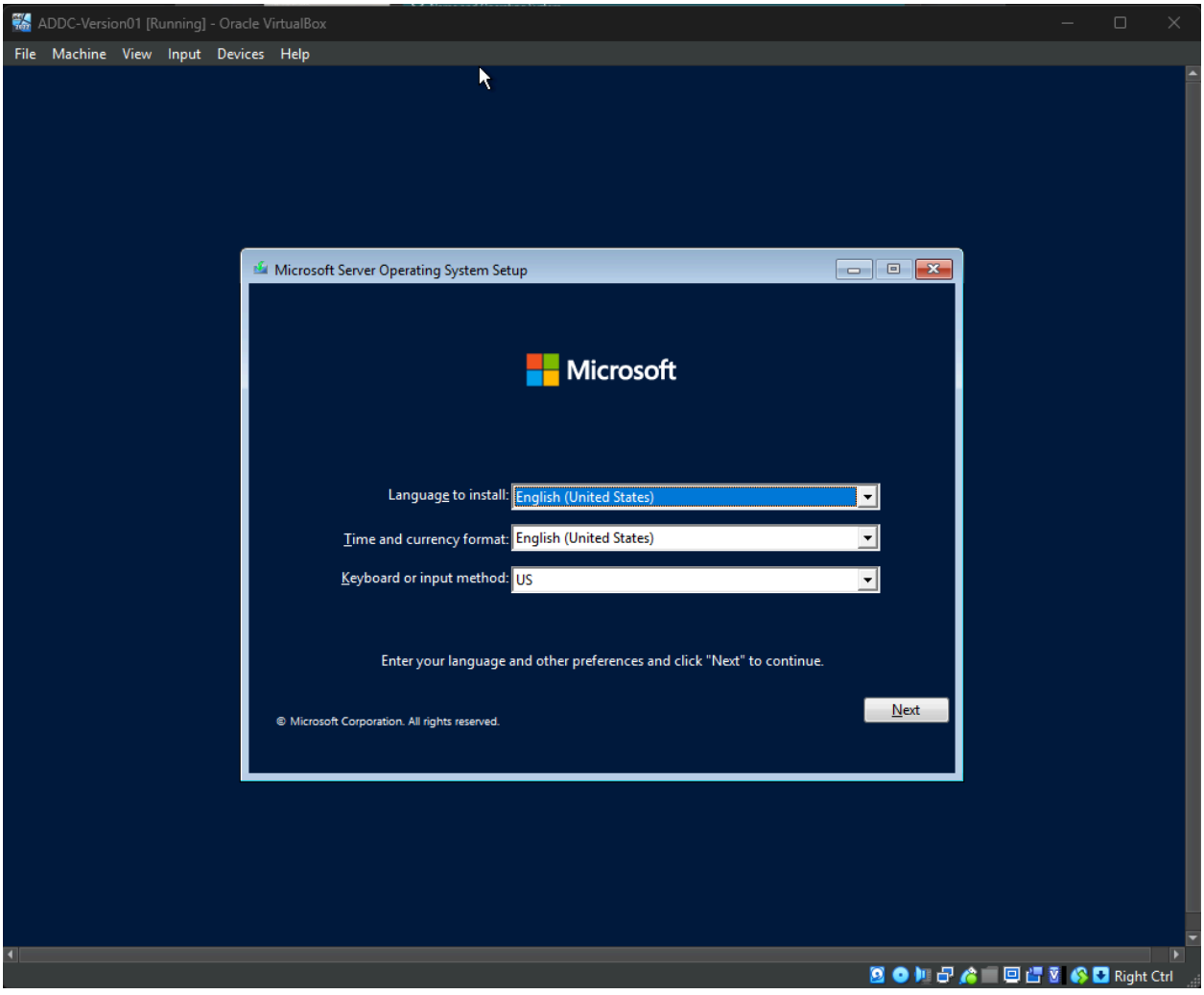
Time to to add the server to our Virtual Box:

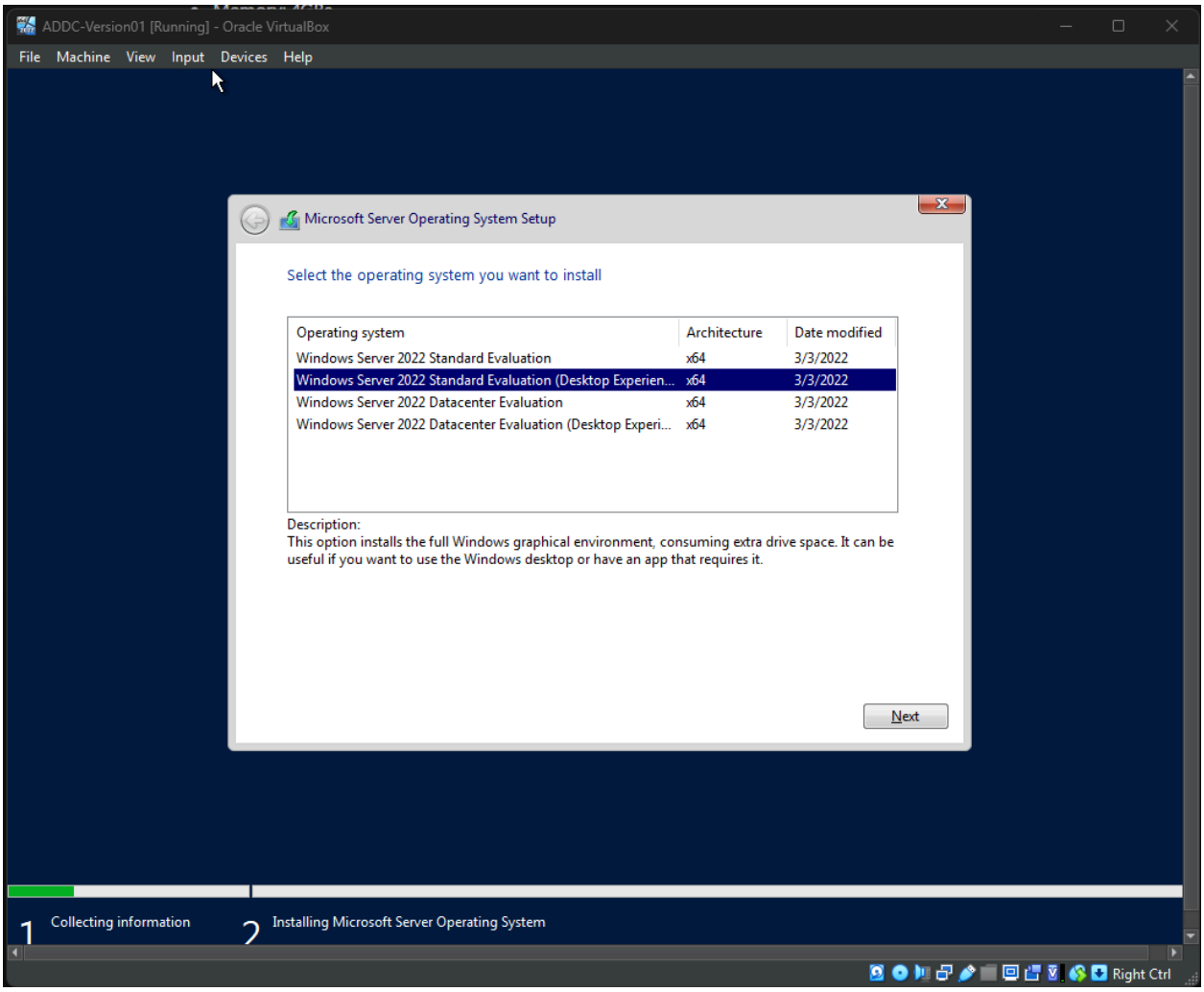


Please note: check the “Skip Unattended Installation” box so we won’t get any “unattended” error in the future if we let the Virtual Box automatically install the server.

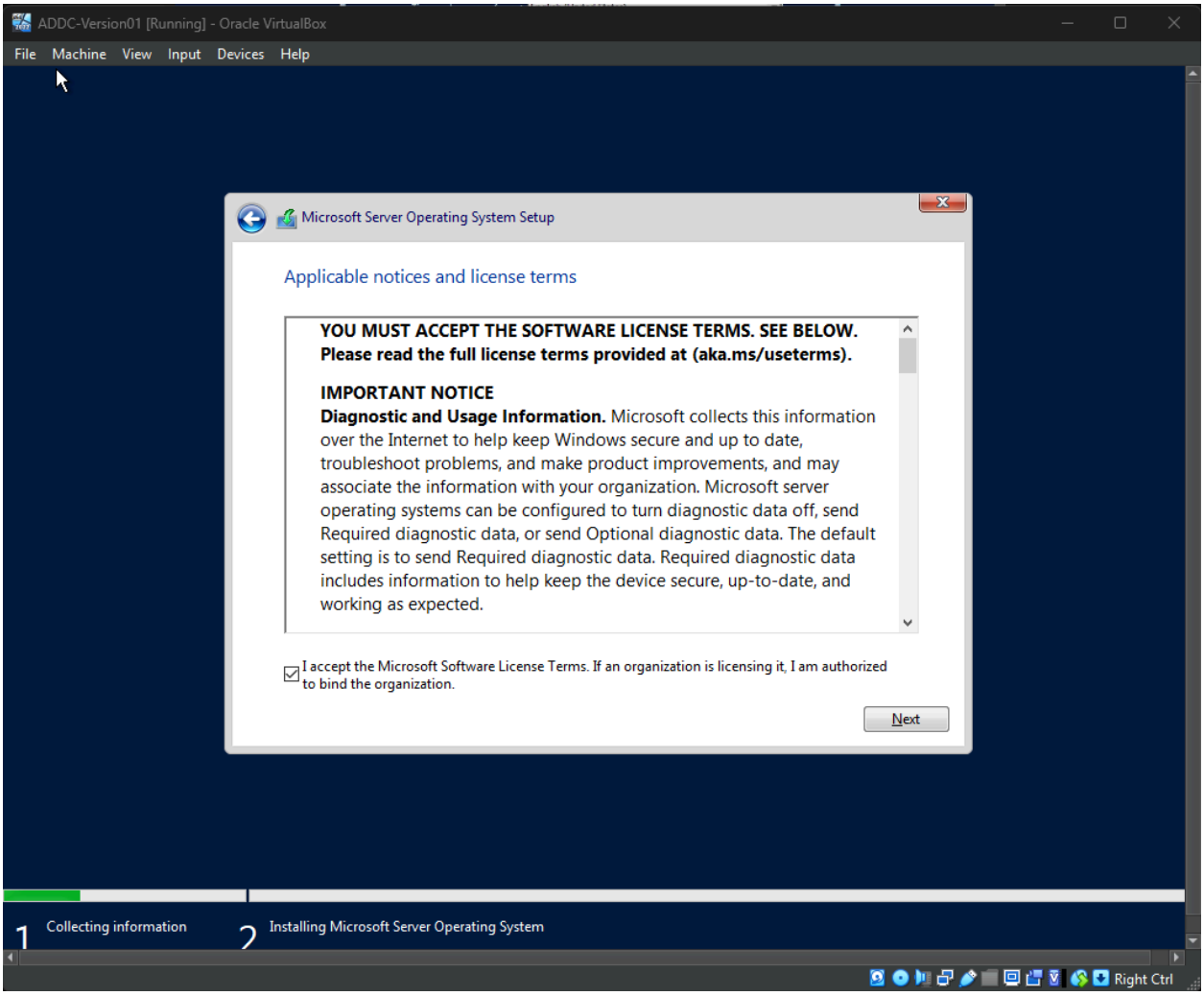
For configure specification, my Windows Server 2022 will have:

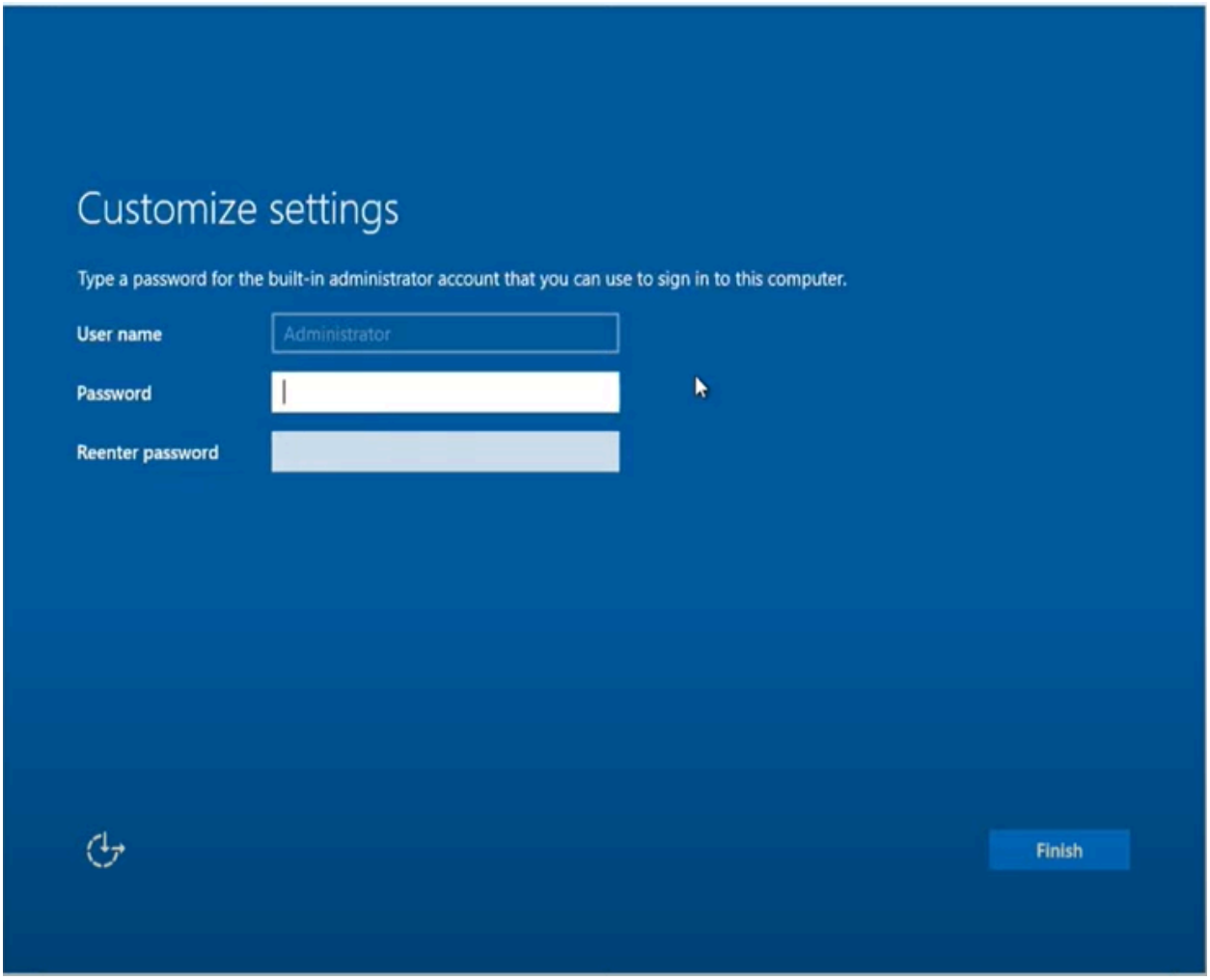
- Memory: 4GBs
- CPU: 1
- Hard Disk: 50Gbs





Please note make sure to choose the Windows Server 2022 Standard Evaluation (Desktop Experience) if you don’t want to work with CLI (Command Line Interface) server


ADDC-Version01 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Microsoft Server Operating System Setup
Applicable notices and license terms
YOU MUST ACCEPT THE SOFTWARE LICENSE TERMS. SEE BELOW.
Please read the full license terms provided at (aka.ms/useterms).
IMPORTANT NOTICE
Diagnostic and Usage Information. Microsoft collects this information over the Internet to help keep Windows secure and up to date, troubleshoot problems, and make product improvements, and may associate the information with your organization. Microsoft server operating systems can be configured to turn diagnostic data off, send Required diagnostic data, or send Optional diagnostic data. The default setting is to send Required diagnostic data. Required diagnostic data includes information to help keep the device secure, up-to-date, and working as expected.
I accept the Microsoft Software License Terms. If an organization is licensing it, I am authorized to bind the organization.
Next
1 Collecting information
2 Installing Microsoft Server Operating System
Right Ctrl



After it finish installing, create a Administrator password.

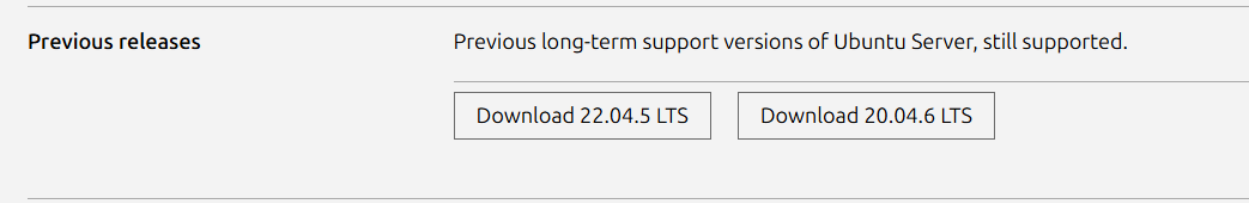
Unlock the screen and enter your password.

Please note in VM sometime you will not be able to do Ctrl - Alt - Del, you can use these input feature on the top of

5. Install Splunk Server

Download Ubuntu Server through this link https://ubuntu.com/download/server#system-requirements-latest to set up Splunk server

For compatible reason we will download any form of Ubuntu 22.04 version (not the latest one)



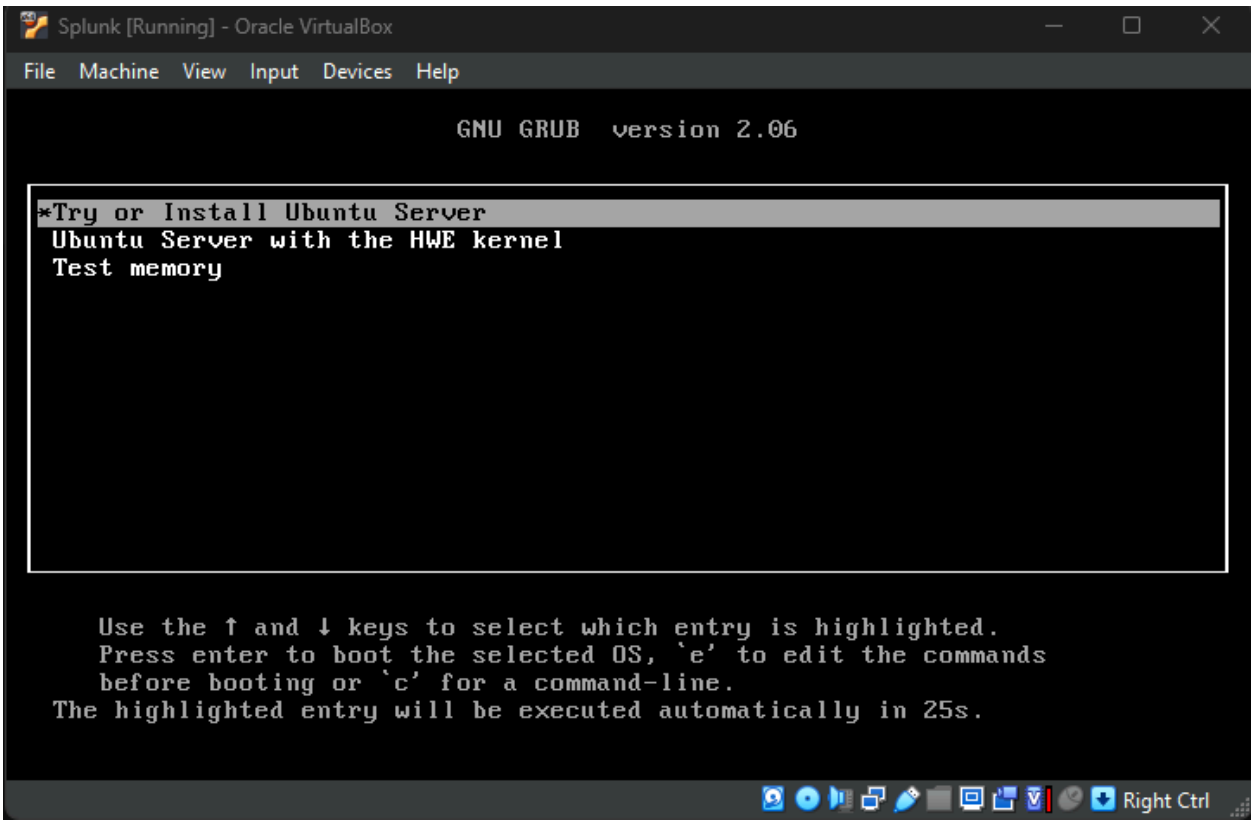
The way to install this to Virtual Box will be the same for Windows 10 and Windows Server 2022 so I won't show fully here.

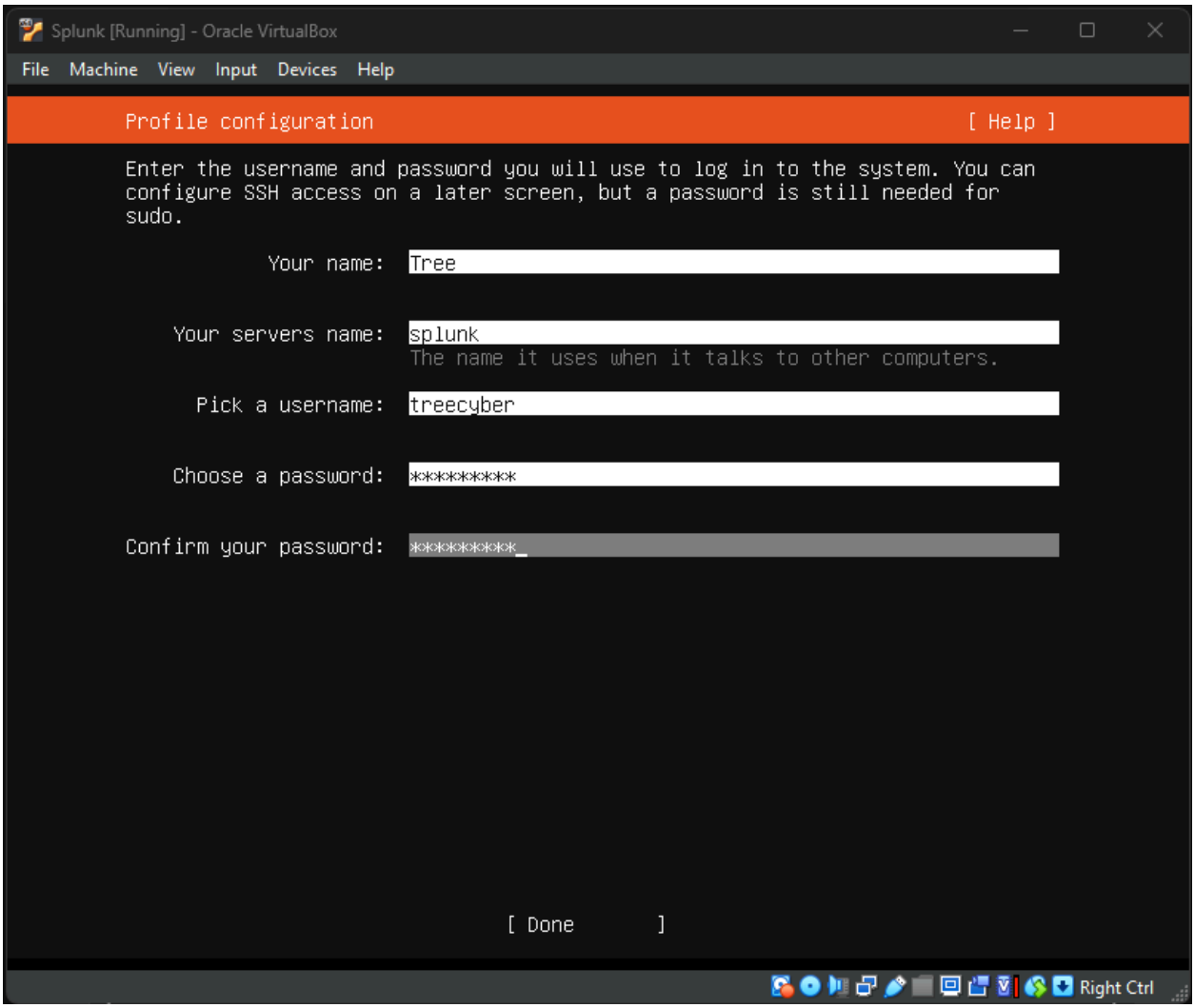
For configure specification, my Windows Server 2022 will have:

- Memory: 8GBs
- CPU: 2
- Hard Disk: 100Gbs

Please note that for Splunk Server, it will going to be ingesting data and running search so the spec will be higher compare to other VM.

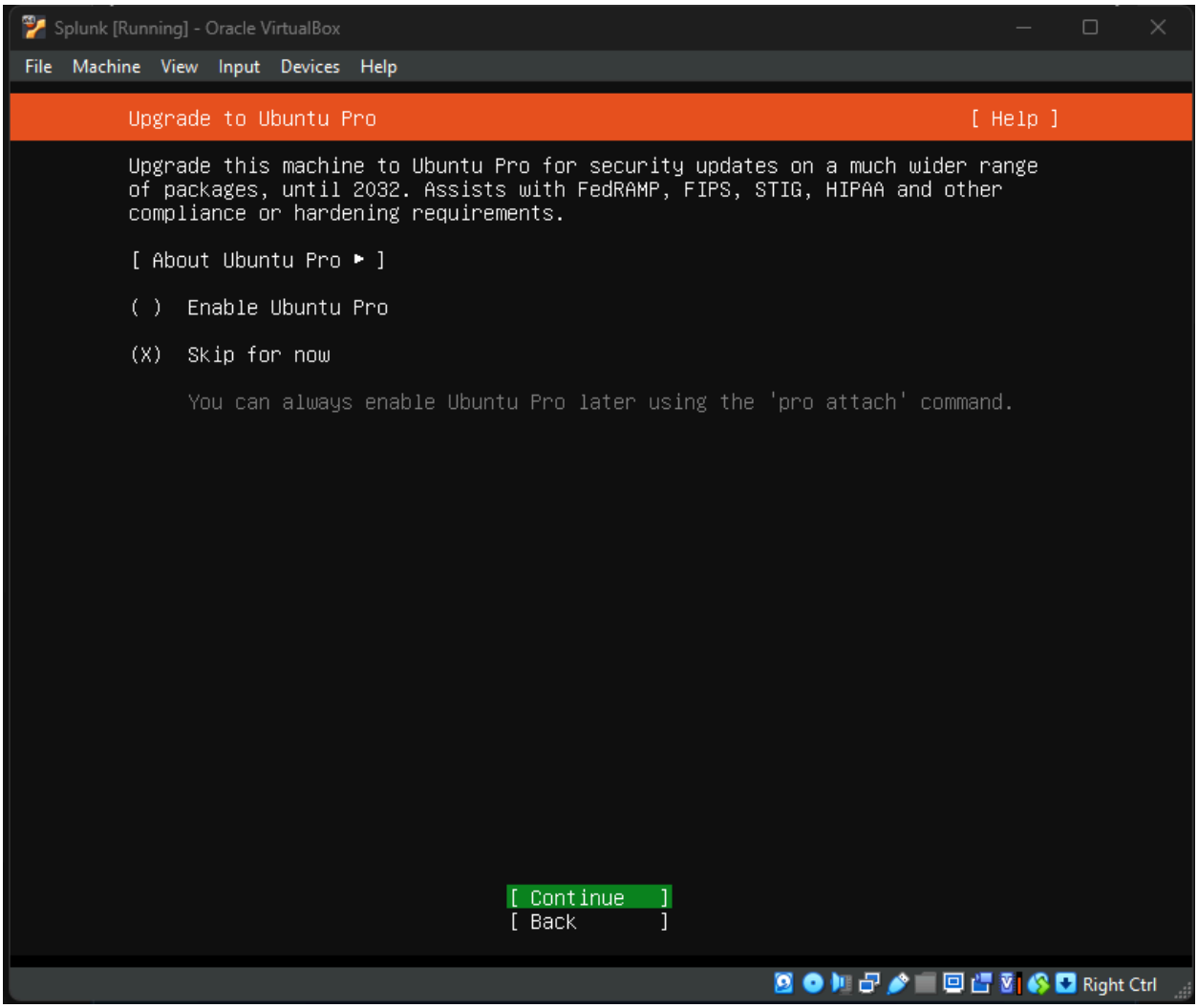
After configuration, let run Ubuntu

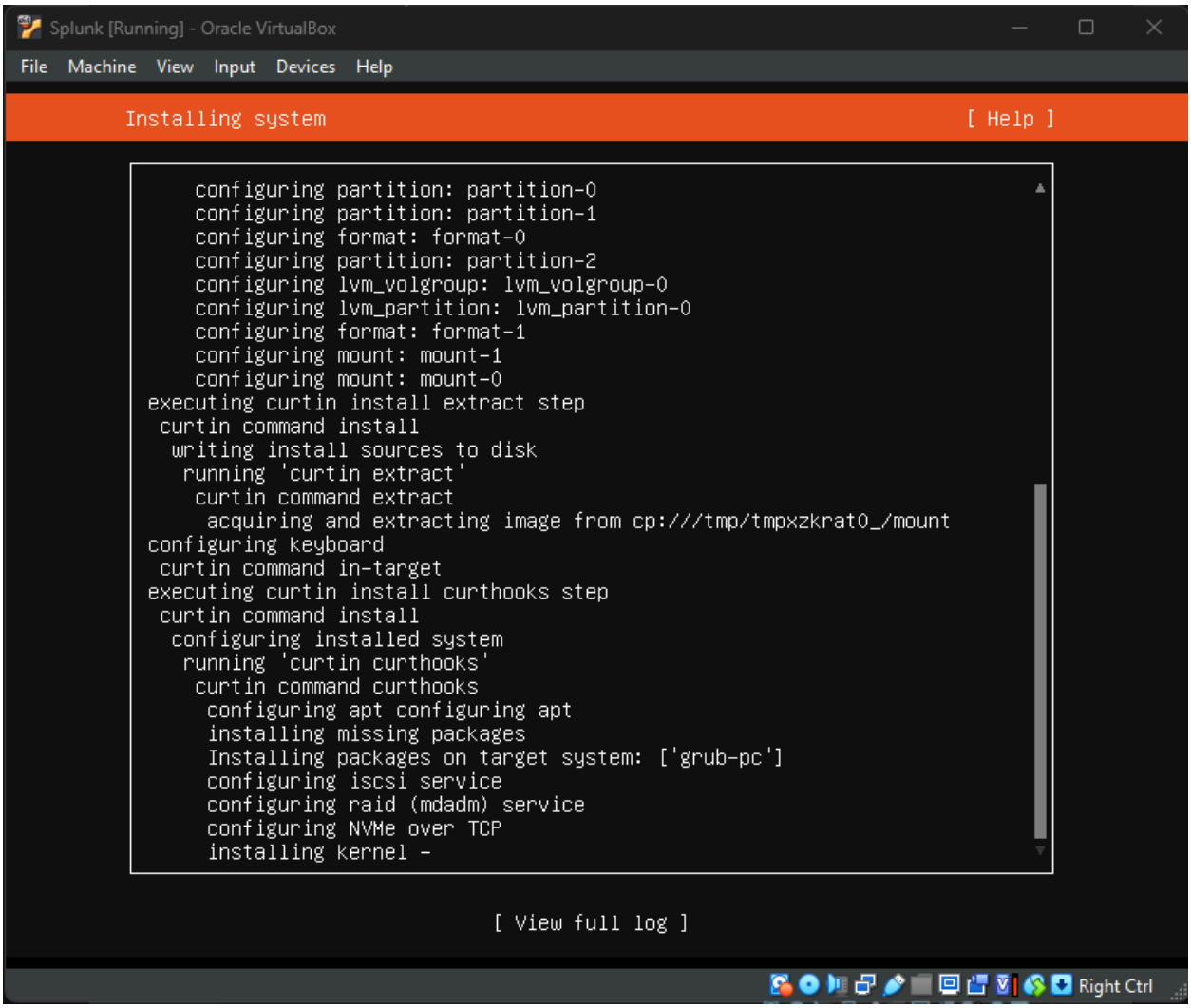


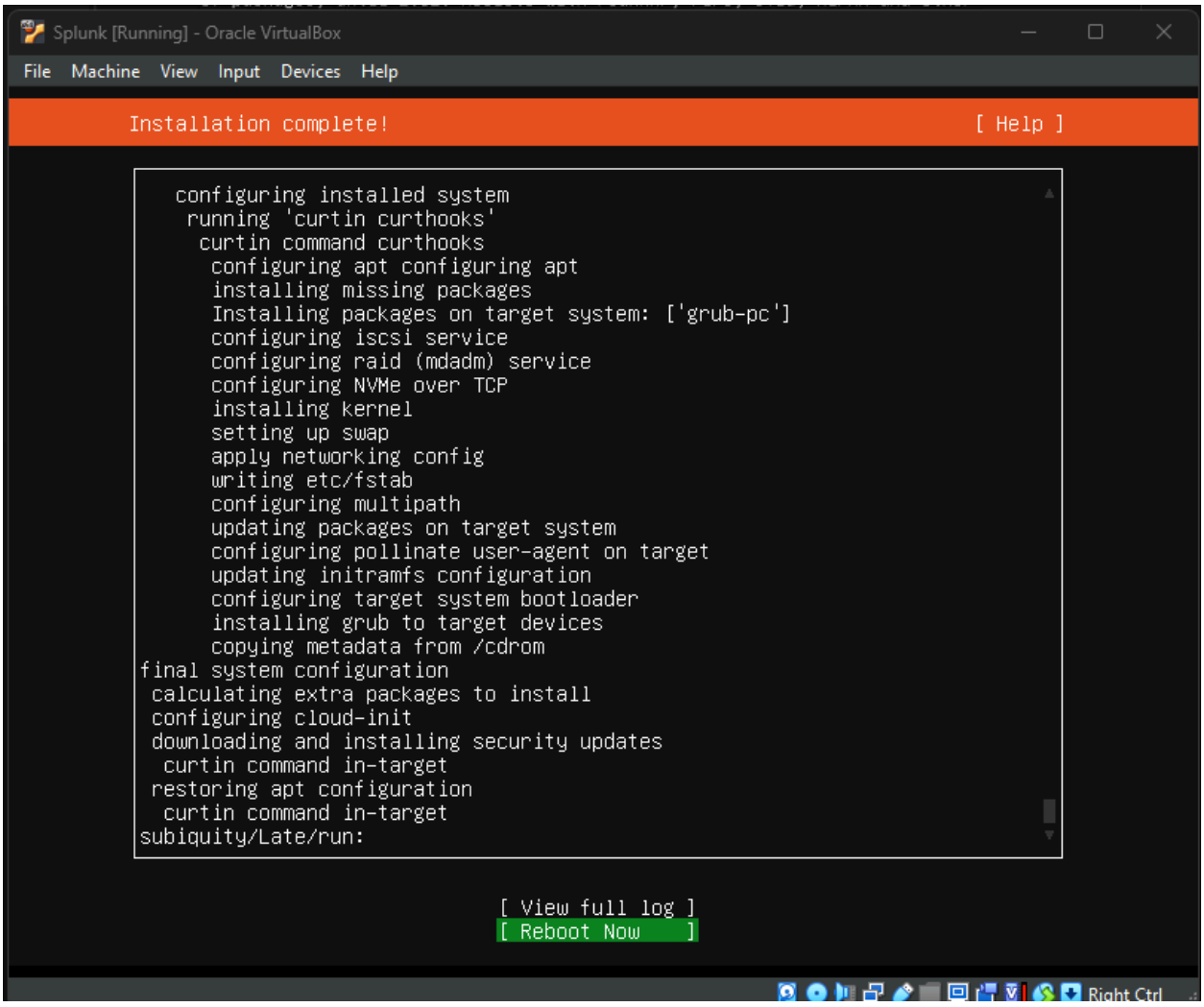


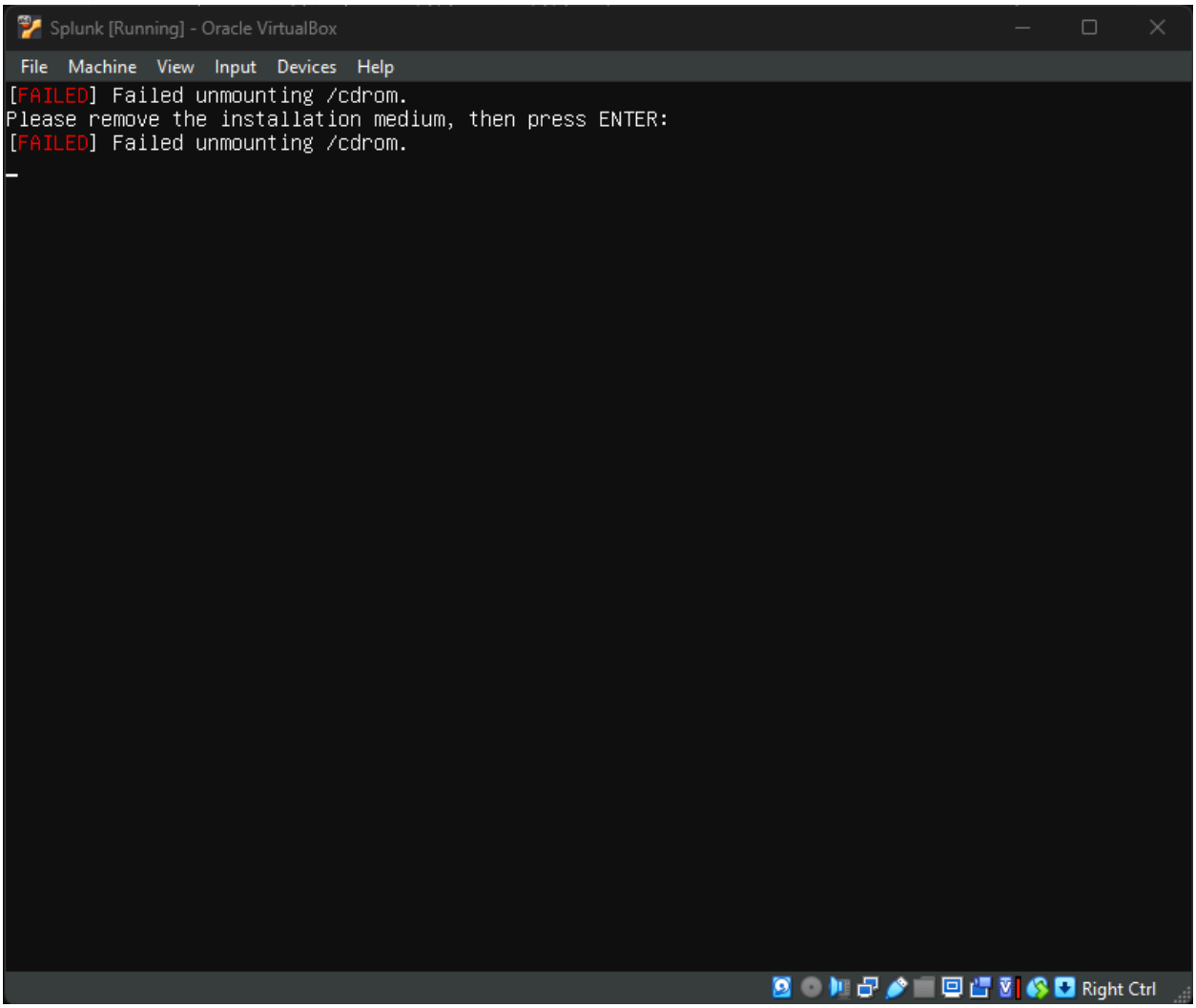
Username: treecyber

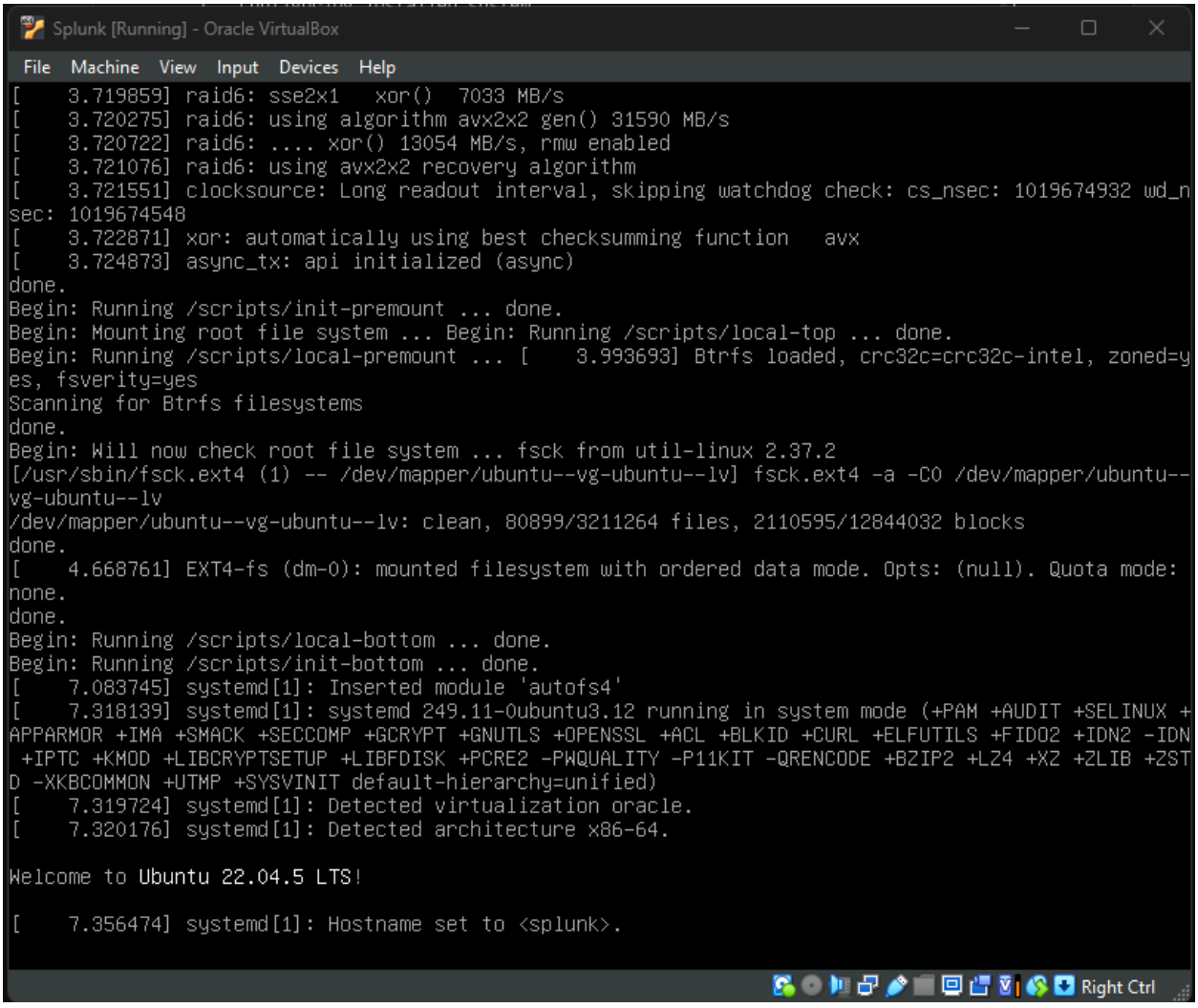
Password: Kim12345$

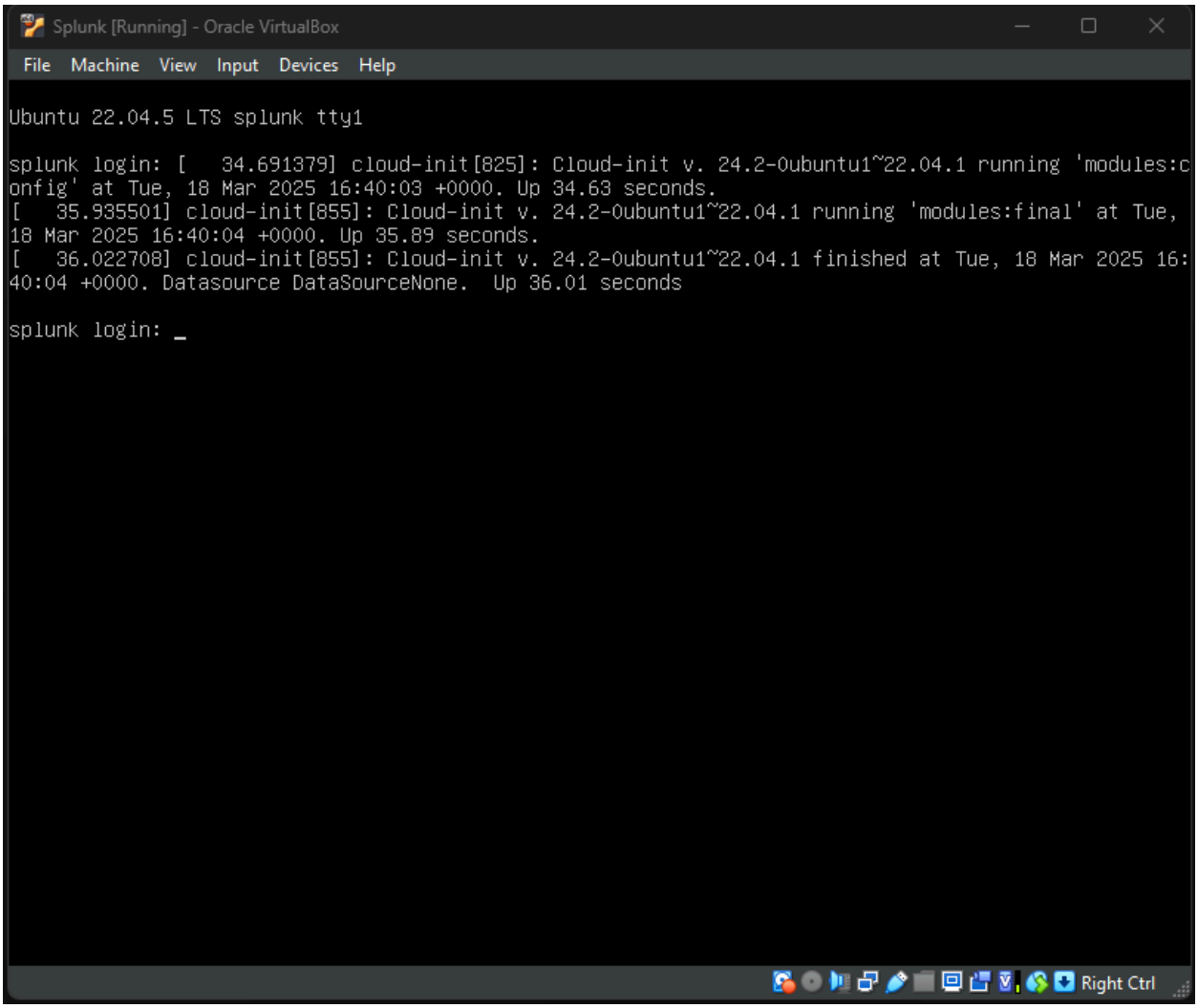

Splunk [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Upgrade to Ubuntu Pro [Help]
Upgrade this machine to Ubuntu Pro for security updates on a much wider range of packages, until 2032. Assists with FedRAMP, FIPS, STIG, HIPAA and other compliance or hardening requirements.
[About Ubuntu Pro ▸]
( ) Enable Ubuntu Pro
(X) Skip for now
You can always enable Ubuntu Pro later using the 'pro attach' command.
[Continue]
[Back]
Right Ctrl

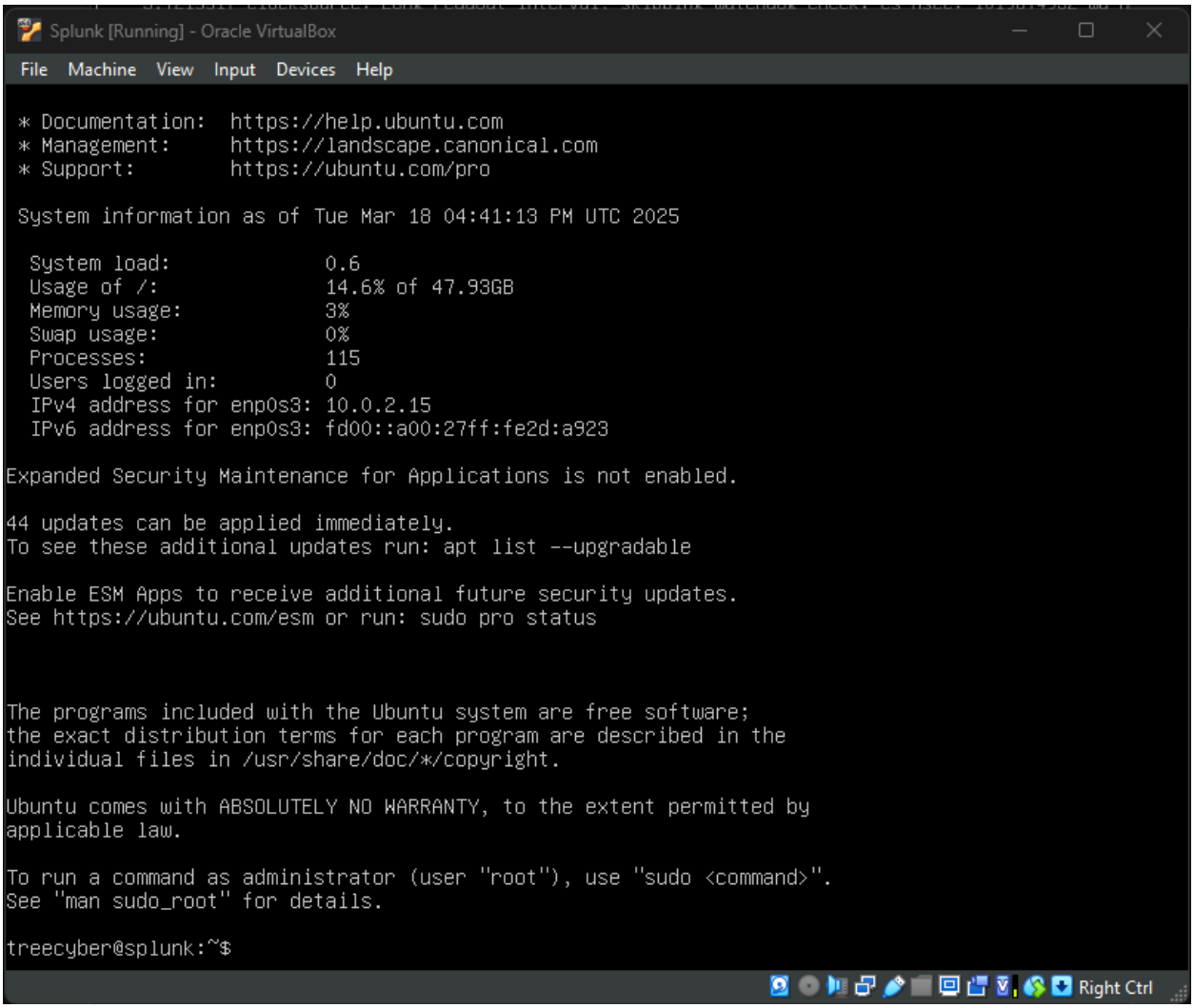

Splunk [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Installing system [Help]
configuring partition: partition-0
configuring partition: partition-1
configuring format: format-0
configuring partition: partition-2
configuring lvm_volgroup: lvm_volgroup-0
configuring lvm_partition: lvm_partition-0
configuring format: format-1
configuring mount: mount-1
configuring mount: mount-0
executing curtin install extract step
curtin command install
writing install sources to disk
running 'curtin extract'
curtin command extract
acquiring and extracting image from cp:///tmp/tmpxzkrat0_/mount
configuring keyboard
curtin command in-target
executing curtin install curthooks step
curtin command install
configuring installed system
running 'curtin curthooks'
curtin command curthooks
configuring apt configuring apt
installing missing packages
Installing packages on target system: ['grub-pc']
configuring iscsi service
configuring raid (mdadm) service
configuring NVMe over TCP
installing kernel -
[View full log]
Right Ctrl


Splunk [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Installation complete!
[Help]
configuring installed system
running 'curtin curthooks'
curtin command curthooks
configuring apt configuring apt
installing missing packages
Installing packages on target system: ['grub-pc']
configuring iscsi service
configuring raid (mdadm) service
configuring NVMe over TCP
installing kernel
setting up swap
apply networking config
writing etc/fstab
configuring multipath
updating packages on target system
configuring pollinate user-agent on target
updating initramfs configuration
configuring target system bootloader
installing grub to target devices
copying metadata from /cdrom
final system configuration
calculating extra packages to install
configuring cloud-init
downloading and installing security updates
curtin command in-target
restoring apt configuration
curtin command in-target
subiquity/Late/run:
[View full log]
[Reboot Now]
Right Ctrl


Splunk [Running] - Oracle VirtualBox
File Machine View Input Devices Help
[FAILED] Failed unmounting /cdrom.
Please remove the installation medium, then press ENTER:
[FAILED] Failed unmounting /cdrom.
Right Ctrl

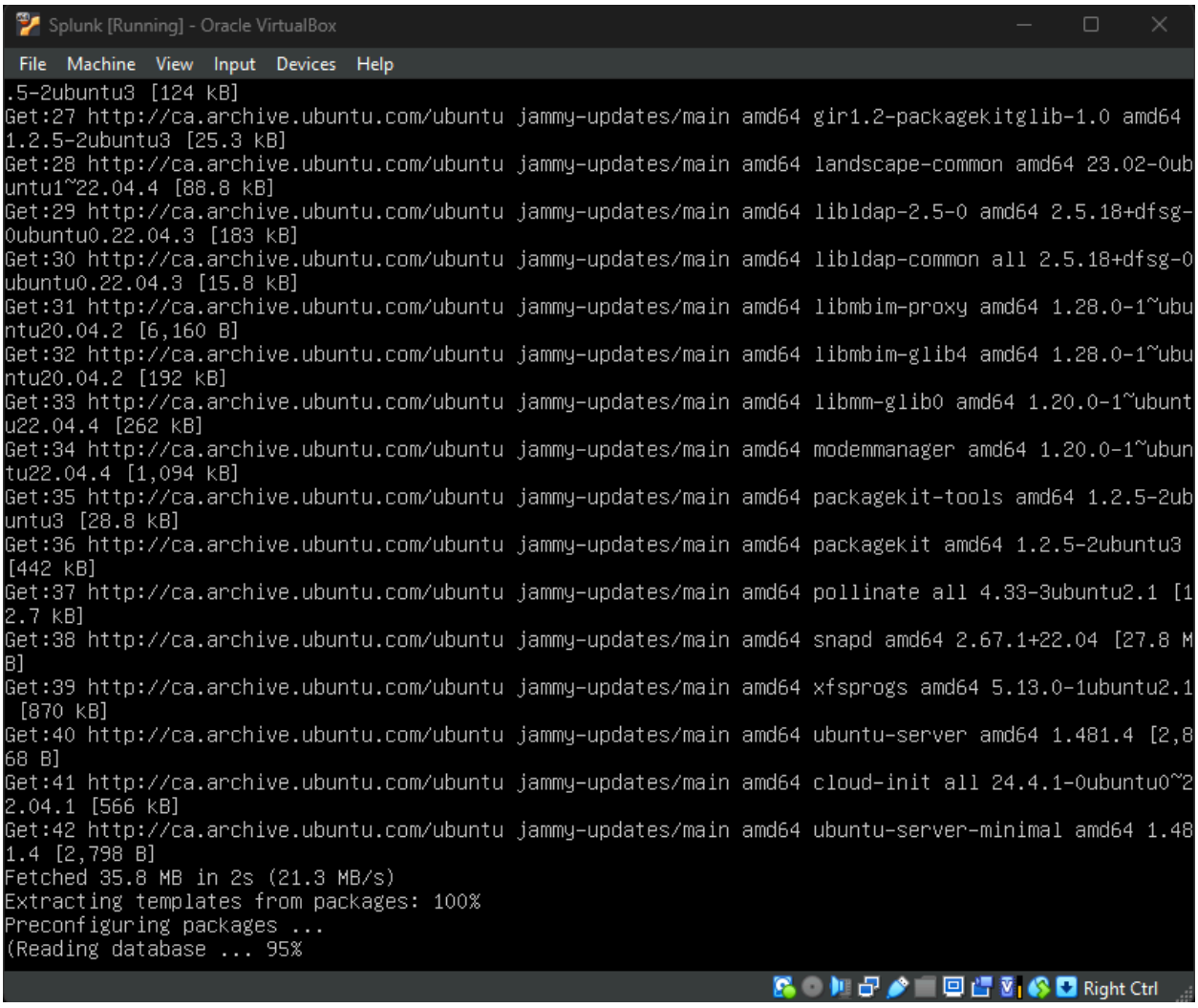

Splunk [Running] - Oracle VirtualBox
File Machine View Input Devices Help
[3.719859] raid6: sse2x1 xor() 7033 MB/s
[3.720275] raid6: using algorithm avx2x2 gen() 31590 MB/s
[3.720722] raid6: .... xor() 13054 MB/s, rmw enabled
[3.721076] raid6: using avx2x2 recovery algorithm
[3.721551] clocksource: Long readout interval, skipping watchdog check: cs_nsec: 1019674932 wd_nsec: 1019674548
[3.722871] xor: automatically using best checksumming function avx
[3.724873] async_tx: api initialized (async)
done.
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... Begin: Running /scripts/local-top ... done.
Begin: Running /scripts/local-premount ... [3.993693] Btrfs loaded, crc32c=crc32c-intel, zoned=yes, fsverity=yes
Scanning for Btrfs filesystems
done.
Begin: Will now check root file system ... fsck from util-linux 2.37.2
[/usr/sbin/fsck.ext4 (1) -- /dev/mapper/ubuntu--vg-ubuntu--lv] fsck.ext4 -a -C0 /dev/mapper/ubuntu--vg-ubuntu--lv
/dev/mapper/ubuntu--vg-ubuntu--lv: clean, 80899/3211264 files, 2110595/12844032 blocks
done.
[4.668761] EXT4-fs (dm-0): mounted filesystem with ordered data mode. Opts: (null). Quota mode: none.
done.
Begin: Running /scripts/local-bottom ... done.
Begin: Running /scripts/init-bottom ... done.
[7.083745] systemd[1]: Inserted module 'autofs4'
[7.318139] systemd[1]: systemd 249.11-0ubuntu3.12 running in system mode (+PAM +AUDIT +SELINUX +APPARMOR +IMA +SMACK +SECCOMP +GCRYPT +GNUTLS +OPENSSL +ACL +BLKID +CURL +ELFUTILS +FIDO2 +IDN2 -IDN +IPTC +KMOD +LIBCRYPTSETUP +LIBFDISK +PCRE2 -PWQUALITY -P11KIT -QRENCODE +BZIP2 +LZ4 +XZ +ZLIB +ZSTD -XKBCOMMON +UTMP +SYSVINIT default-hierarchy=unified)
[7.319724] systemd[1]: Detected virtualization oracle.
[7.320176] systemd[1]: Detected architecture x86-64.
Welcome to Ubuntu 22.04.5 LTS!
[7.356474] systemd[1]: Hostname set to <splunk>.
Right Ctrl

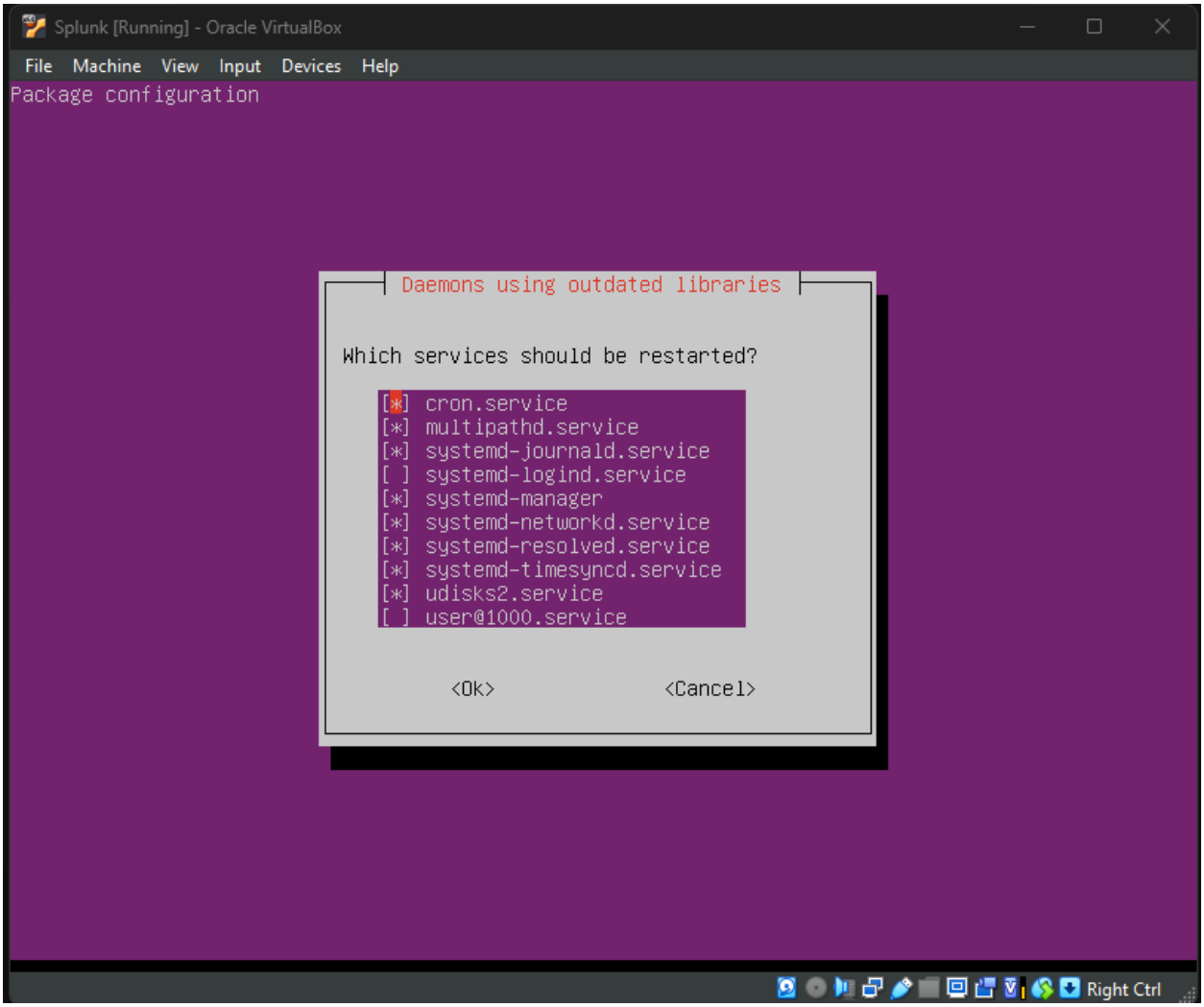

Splunk [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Ubuntu 22.04.5 LTS splunk tty1
splunk login: [34.691379] cloud-init[825]: Cloud-init v. 24.2-0ubuntu1~22.04.1 running 'modules:config' at Tue, 18 Mar 2025 16:40:03 +0000. Up 34.63 seconds.
[35.935501] cloud-init[855]: Cloud-init v. 24.2-0ubuntu1~22.04.1 running 'modules:final' at Tue, 18 Mar 2025 16:40:04 +0000. Up 35.89 seconds.
[36.022708] cloud-init[855]: Cloud-init v. 24.2-0ubuntu1~22.04.1 finished at Tue, 18 Mar 2025 16:40:04 +0000. Datasource DataSourceNone. Up 36.01 seconds
splunk login: _
Right Ctrl



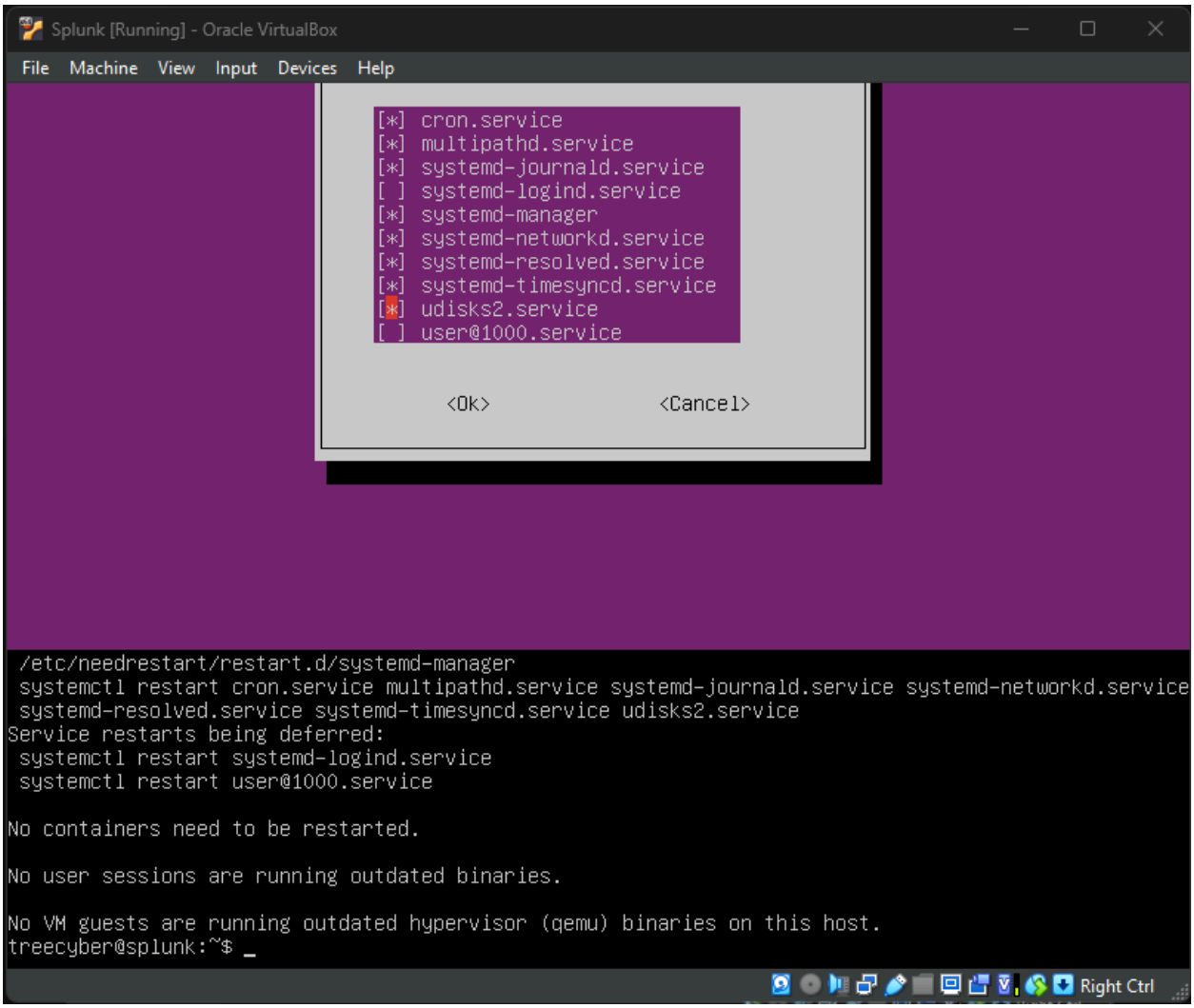
Enter: `sudo apt-get update && sudo apt-get upgrade -y`

This will allow the machine to update and upgrade all of our repository.


Splunk [Running] - Oracle VirtualBox
File Machine View Input Devices Help
.5-2ubuntu3 [124 kB]
Get:27 http://ca.archive.ubuntu.com/ubuntu jammy-updates/main amd64 gir1.2-packagekitglib-1.0 amd64 1.2.5-2ubuntu3 [25.3 kB]
Get:28 http://ca.archive.ubuntu.com/ubuntu jammy-updates/main amd64 landscape-common amd64 23.02-0ubuntu1~22.04.4 [88.8 kB]
Get:29 http://ca.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libldap-2.5-0 amd64 2.5.18+dfsg-0ubuntu0.22.04.3 [183 kB]
Get:30 http://ca.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libldap-common all 2.5.18+dfsg-0ubuntu0.22.04.3 [15.8 kB]
Get:31 http://ca.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libmbim-proxy amd64 1.28.0-1~ubuntu20.04.2 [6,160 B]
Get:32 http://ca.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libmbim-glib4 amd64 1.28.0-1~ubuntu20.04.2 [192 kB]
Get:33 http://ca.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libmm-glib0 amd64 1.20.0-1~ubuntu22.04.4 [262 kB]
Get:34 http://ca.archive.ubuntu.com/ubuntu jammy-updates/main amd64 modemmanager amd64 1.20.0-1~ubuntu22.04.4 [1,094 kB]
Get:35 http://ca.archive.ubuntu.com/ubuntu jammy-updates/main amd64 packagekit-tools amd64 1.2.5-2ubuntu3 [28.8 kB]
Get:36 http://ca.archive.ubuntu.com/ubuntu jammy-updates/main amd64 packagekit amd64 1.2.5-2ubuntu3 [442 kB]
Get:37 http://ca.archive.ubuntu.com/ubuntu jammy-updates/main amd64 pollinate all 4.33-3ubuntu2.1 [12.7 kB]
Get:38 http://ca.archive.ubuntu.com/ubuntu jammy-updates/main amd64 snapd amd64 2.67.1+22.04 [27.8 MB]
Get:39 http://ca.archive.ubuntu.com/ubuntu jammy-updates/main amd64 xfsprogs amd64 5.13.0-1ubuntu2.1 [870 kB]
Get:40 http://ca.archive.ubuntu.com/ubuntu jammy-updates/main amd64 ubuntu-server amd64 1.481.4 [2,868 B]
Get:41 http://ca.archive.ubuntu.com/ubuntu jammy-updates/main amd64 cloud-init all 24.4.1-0ubuntu0~22.04.1 [566 kB]
Get:42 http://ca.archive.ubuntu.com/ubuntu jammy-updates/main amd64 ubuntu-server-minimal amd64 1.481.4 [2,798 B]
Fetched 35.8 MB in 2s (21.3 MB/s)
Extracting templates from packages: 100%
Preconfiguring packages ...
(Reading database ... 95%
Right Ctrl


Splunk [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Package configuration
Daemons using outdated libraries
Which services should be restarted?
[*] cron.service
[*] multipathd.service
[*] systemd-journald.service
[ ] systemd-logind.service
[*] systemd-manager
[*] systemd-networkd.service
[*] systemd-resolved.service
[*] systemd-timesyncd.service
[*] udisks2.service
[ ] user@1000.service
<Ok>
<Cancel>
Right Ctrl

Hit enter



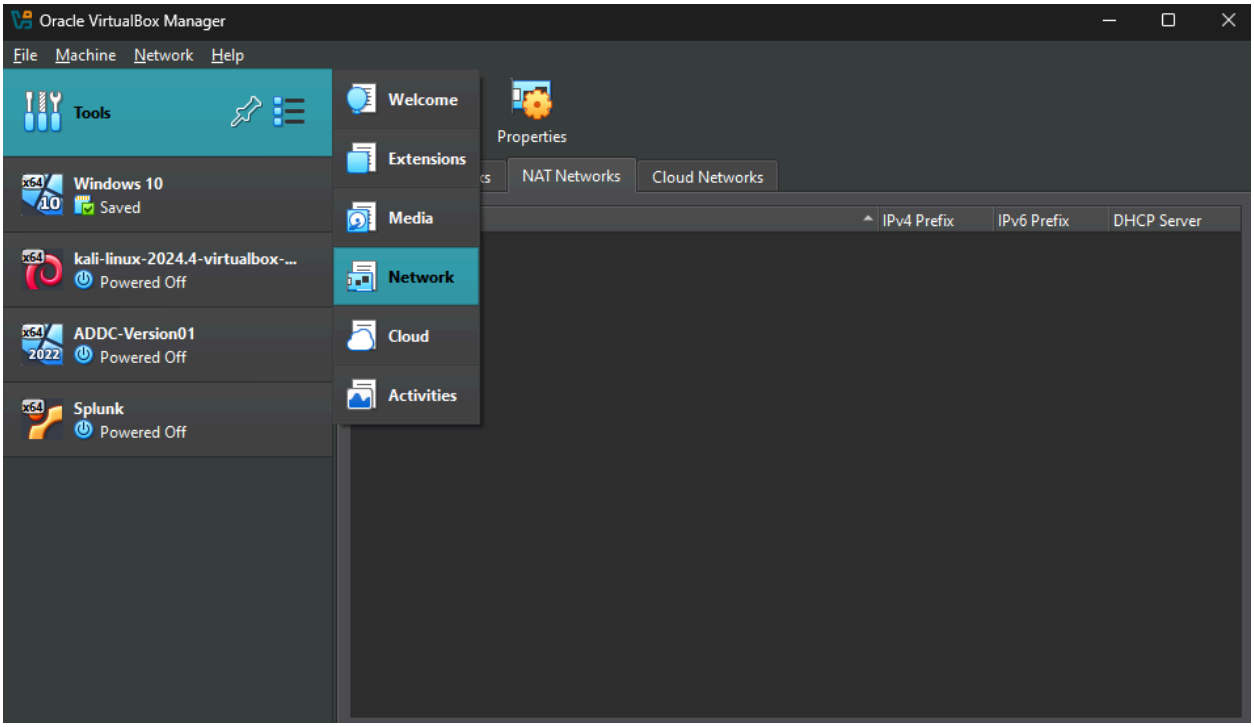
Splunk Server is good to go!

Install & Configure (Sysmon & Splunk) to Windows 10 machine and Windows Server.

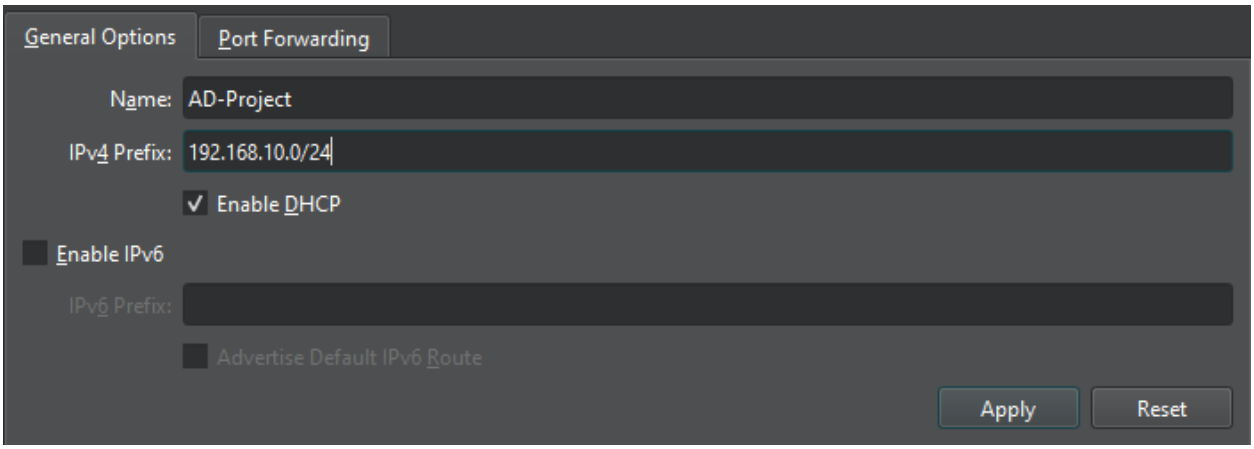
Network configure:

Please note that we need to make sure our network setting is NAT Network, this way our VM still can be on the same network and still have access to internet.

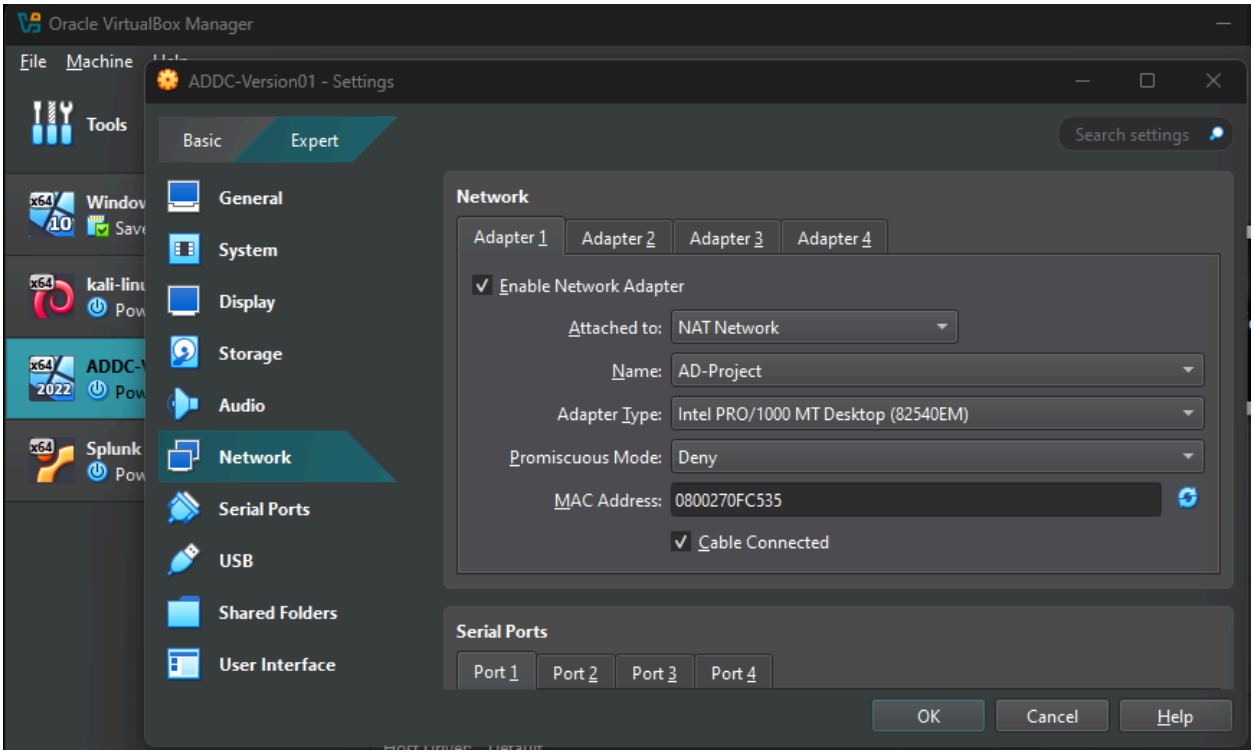
Network Address Translation (NAT): is **a process that allows multiple devices on a private network to share a single public IP address**, enabling them to communicate with devices on the internet without requiring each device to have its own unique public IP address.



Press
Create, edit Name and IPv4 Prefix, hit apply. Please note that for IPv4 Prefix, it should be how we plan with the diagram chart which will be 192.168.10.0/24.



After that we will setup network for each Virtual Machine (VM) to use NAT Network by click **Setting → Network → Adapter 1 → Attached to → NAT Network.** Make sure that the Name of NAT Network is the one you just create in case if you have different network, for me will be AD-Project.



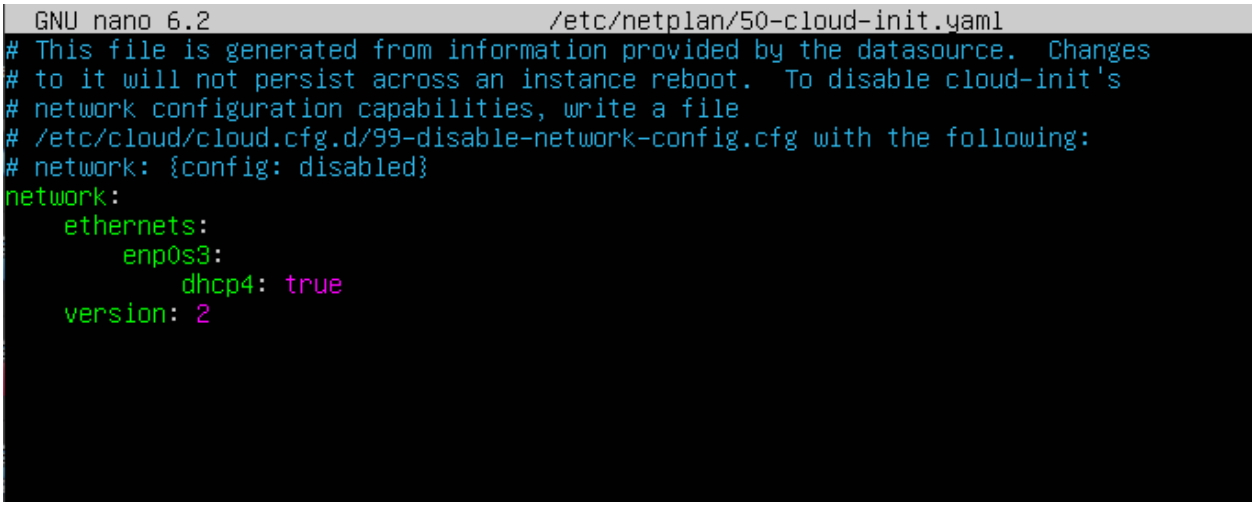
Set up to NAT Network for all machine include Splunk, Kali, ADDC and Windows 10.

Splunk configure:

Splunk server will have a different IP then what we plan on our diagram, type `ip a` under Splunk Server VM and you can see:

Splunk Server IP currently is `192.168.10.4` and what we plan is `192.168.10.10` . Time to set up a static IP on our Splunk Server.

Type `sudo nano /etc/netplan/50-cloud-init.yaml` and this should show up for you



This is how you will configure:

- For `nameserver`, we will set up DNS IP that you want. In this case I will use Google DNS (8.8.8.8)
- Set `no` for DHCP since we want our Splunk Server to have static IP
- We will want to add default routes for Splunk Server network setting

Save the file and start enter `sudo netplan apply` . You can ignore the warning, after that you can check the IP again with `ip a`

```
treecyber@splunk:~$ sudo netplan apply
[sudo] password for treecyber:
WARNING:root:Cannot call Open vSwitch: ovsdb-server.service is not running.
treecyber@splunk:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
    link/ether 08:00:27:2d:a9:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.10/24 brd 192.168.10.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe2d:a923/64 scope link
       valid_lft forever preferred_lft forever
treecyber@splunk:~$ _
```

Try to `ping google.com` if there is a connection, if yes you are successfully configure Splunk Server IP setting:

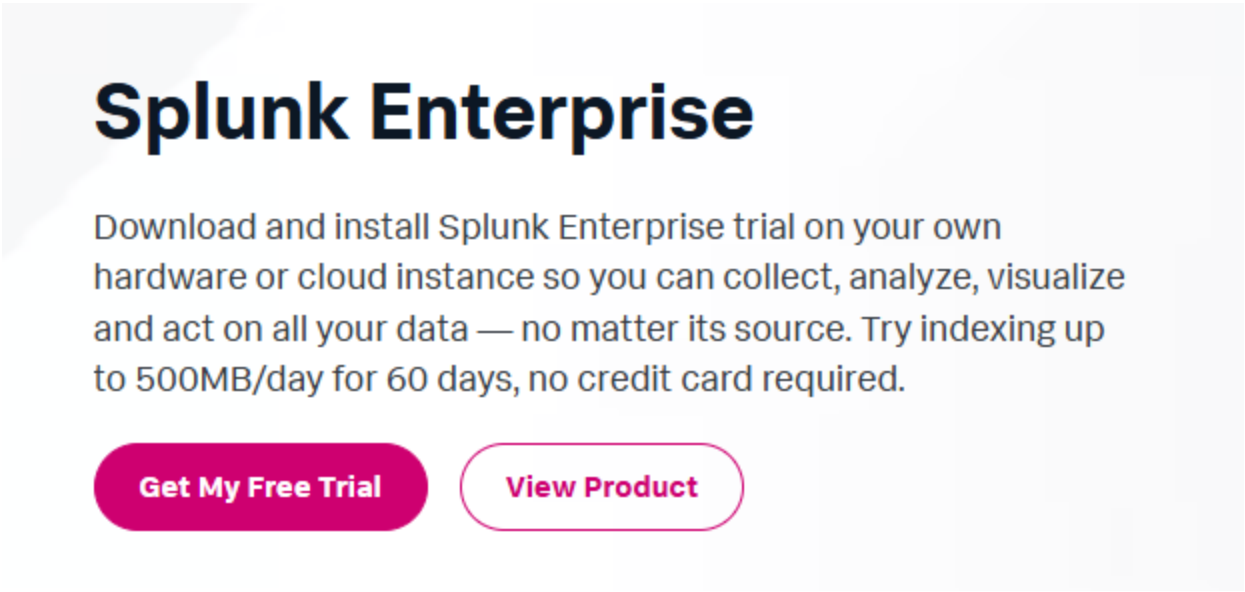
```
treecyber@splunk:~$ ping google.com
PING google.com (142.251.32.78) 56(84) bytes of data.
64 bytes from yyz12s07-in-f14.1e100.net (142.251.32.78): icmp_seq=1 ttl=115 time=17.2 ms
64 bytes from yyz12s07-in-f14.1e100.net (142.251.32.78): icmp_seq=2 ttl=115 time=11.8 ms
64 bytes from yyz12s07-in-f14.1e100.net (142.251.32.78): icmp_seq=3 ttl=115 time=14.1 ms
64 bytes from yyz12s07-in-f14.1e100.net (142.251.32.78): icmp_seq=4 ttl=115 time=11.1 ms
64 bytes from yyz12s07-in-f14.1e100.net (142.251.32.78): icmp_seq=5 ttl=115 time=15.2 ms
64 bytes from yyz12s07-in-f14.1e100.net (142.251.32.78): icmp_seq=6 ttl=115 time=20.0 ms
64 bytes from yyz12s07-in-f14.1e100.net (142.251.32.78): icmp_seq=7 ttl=115 time=16.9 ms
64 bytes from yyz12s07-in-f14.1e100.net (142.251.32.78): icmp_seq=8 ttl=115 time=17.5 ms
64 bytes from yyz12s07-in-f14.1e100.net (142.251.32.78): icmp_seq=9 ttl=115 time=16.8 ms
^C
--- google.com ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8010ms
rtt min/avg/max/mdev = 11.147/15.645/20.049/2.698 ms
treecyber@splunk:~$
```

Troubleshooting:

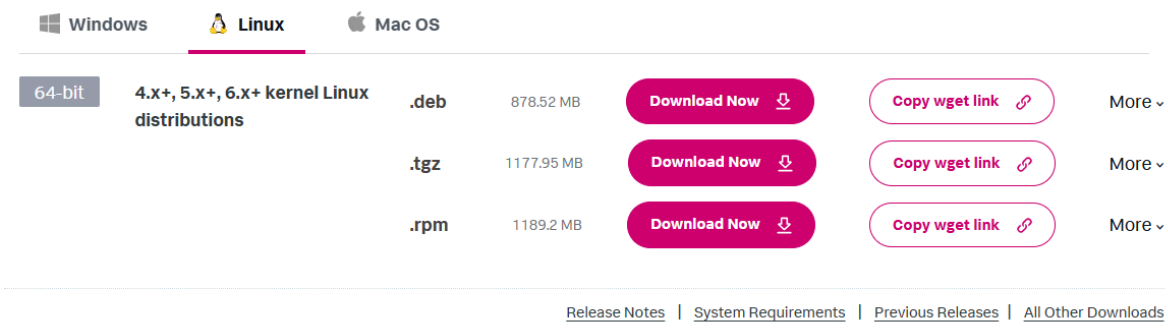
If every time you reboot the Server and the IP change back to old address then you will need to add `99-disable-network-config.cfg` file by `sudo nano /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg` and add `network: {config: disabled}` , save the file, set up the static IP again and it should good to go.

Time to install Splunk for our Splunk Server VM. Sign up an account with Splunk to download the package we need for this step.

We will look to download Splunk Enterprise



Choose Linux and down load the .deb extension one. Save to the directory of your choice.



Go back to your Splunk Server VM then install the guest add-ons for virtual box.

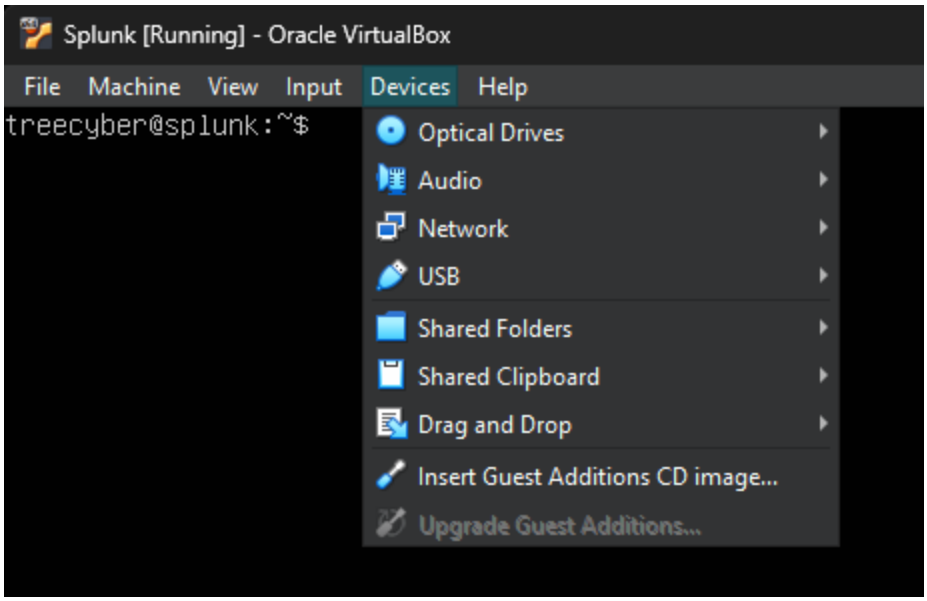
Enter `sudo apt-get install virtualbox-guest-additions-iso`

```
treecyber@splunk:~$ sudo apt-get install virtualbox
virtualbox                      virtualbox-guest-utils          virtualbox-qt
virtualbox-dkms                 virtualbox-guest-utils-hwe      virtualbox-source
virtualbox-ext-pack             virtualbox-guest-x11
virtualbox-guest-additions-iso  virtualbox-guest-x11-hwe
treecyber@splunk:~$ sudo apt-get install virtualbox-guest-additions-iso _
```

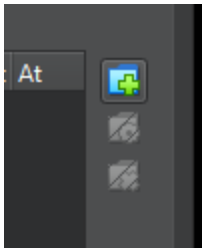
And type enter download it. Make sure to type Y if they ask you

```
After this operation, 891 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

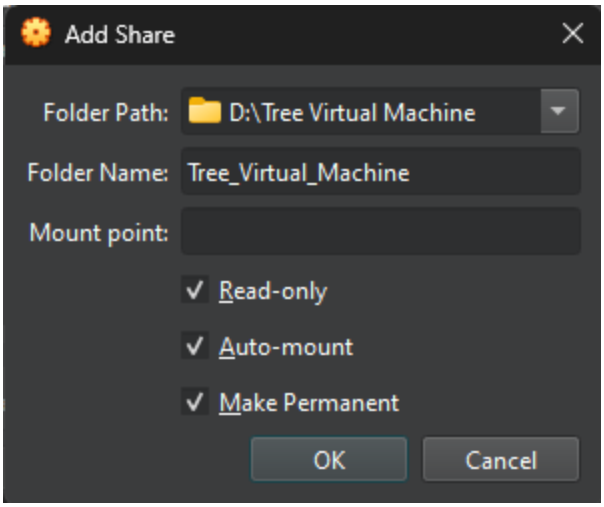
Let add the Splunk .deb file we just download. Head over to Devices → Shared Folders → Shared Folders Setting



Add folder



Choose the path for Folder Path where you put your Splunk .deb installer file and tick all the options



Back to our VM, type `sudo reboot` to restart the VM. After reboot, we would like to add user to the vbox SF group by type `sudo adduser [username] vboxsf` , hit Enter

```
treecyber@splunk:~$ sudo adduser treecyber vboxsf
[sudo] password for treecyber:
adduser: The group `vboxsf' does not exist.
treecyber@splunk:~$
```

If error, we will need to install vboxsf by type `sudo apt-get install virtualbox-guest-utils` and reboot again. Try to add user again and it should work:

```
treecyber@splunk:~$ sudo adduser treecyber vboxsf
[sudo] password for treecyber:
Adding user `treecyber' to group `vboxsf' ...
Adding user treecyber to group vboxsf
Done.
treecyber@splunk:~$ _
```

Let create a new directory call *share* with `mkdir share` and we will run a command to mount our shared folder onto our *share* directory we just create.

Type `sudo mount -t vboxsf -o uid=1000,gid=1000 [Folder Name] share/` and hit Enter. You can see the *share* directory highlighted.

```
treecyber@splunk:~$ mkdir share
treecyber@splunk:~$ ls
share
treecyber@splunk:~$ sudo mount -t vboxsf -o uid=1000,gid=1000 Tree_Virtual_Machine share/
treecyber@splunk:~$ ls
share
treecyber@splunk:~$
```

Change your location to the *share* directory with `cd share` and type `ls -la` to see all the file in there.

```
treecyber@splunk:~$ cd share
treecyber@splunk:~/share$ ls -la
total 5678828
drwxrwxrwx 1 treecyber treecyber       4096 Mar 24 21:44  .
drwxr-x--- 5 treecyber treecyber       4096 Mar 24 22:34  ..
drwxrwxrwx 1 treecyber treecyber       4096 Mar 24 20:47  ADDC-Version01
drwxrwxrwx 1 treecyber treecyber       4096 Mar 24 22:10  Splunk
-rwxrwxrwx 1 treecyber treecyber  921195836 Mar 24 21:44  splunk-9.4.1-e3bdab203ac8-linux-amd64.deb
drwxrwxrwx 1 treecyber treecyber       4096 Mar 24 20:48 'Windows 10'
-rwxrwxrwx 1 treecyber treecyber 4893900800 Mar 18 00:37  Windows.iso
treecyber@splunk:~/share$
```

You will see the file and folder that we save in our directory, including our Splunk .deb install file. We will install Splunk with `sudo dpkg -i splunk...(hit Tab)`

```
treecyber@splunk:~/share$ sudo dpkg -i splunk-9.4.1-e3bdab203ac8-linux-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 94824 files and directories currently installed.)
Preparing to unpack splunk-9.4.1-e3bdab203ac8-linux-amd64.deb ...
no need to run the pre-install check
Unpacking splunk (9.4.1) ...
Setting up splunk (9.4.1) ...
complete
treecyber@splunk:~/share$ _
```

We change the directory location to where Splunk is installed with `cd /opt/splunk` and type ls -la to check what we have.

```
treecyber@splunk:~/share$ cd /opt/splunk
treecyber@splunk:/opt/splunk$ ls -la
total 5260
drwxr-xr-x 11 splunk splunk    4096 Mar 24 22:50 .
drwxr-xr-x  3 root   root      4096 Mar 24 22:47 ..
drwxr-xr-x  4 splunk splunk   12288 Mar 24 22:50 bin
-r--r--r--  1 splunk splunk      57 Feb 20 17:58 copyright.txt
drwxr-xr-x 17 splunk splunk    4096 Mar 24 22:50 etc
-rw-r--r--  1 splunk splunk     426 Mar 24 22:50 ftr
drwxr-xr-x  4 splunk splunk    4096 Mar 24 22:50 include
drwxr-xr-x 10 splunk splunk    4096 Mar 24 22:50 lib
-r--r--r--  1 splunk splunk   59708 Feb 20 17:58 license-eula.txt
-r--r--r--  1 splunk splunk    1090 Dec 11 20:50 LICENSE.txt
drwxr-xr-x  3 splunk splunk    4096 Mar 24 22:50 openssl
drwxr-xr-x  4 splunk splunk    4096 Mar 24 22:49 opt
drwxr-xr-x  2 splunk splunk    4096 Mar 24 22:50 quarantined_files
-r--r--r--  1 splunk splunk     522 Feb 20 18:03 README-splunk.txt
drwxr-xr-x  5 splunk splunk    4096 Mar 24 22:50 share
-r--r--r--  1 splunk splunk 5255133 Feb 20 18:30 splunk-9.4.1-e3bdab203ac8-linux-amd64-manifest
drwxr-xr-x  2 splunk splunk    4096 Mar 24 22:50 swidtag
treecyber@splunk:/opt/splunk$ _
```

We will change user to Splunk with `sudo -u splunk bash`

```
treecyber@splunk:/opt/splunk$ sudo -u splunk bash
splunk@splunk:~$
```

Change directory to bin with `cd bin` , type `./splunk start` to run the install

```
splunk@splunk:~$ cd bin
splunk@splunk:~/bin$ ./splunk start_
```

Hit Enter and it will prompt the license, term and agreement

```
Splunk General Terms (v4 August 2024)

These Splunk General Terms ("General Terms") between Splunk Inc., a Delaware
corporation, with its principal place of business at 250 Brannan Street, San
Francisco, California 94107, USA ("Splunk" or "we" or "us" or "our") and you
("Customer" or "you" or "your") govern your acquisition, access to, and use of
Splunk's Offerings, regardless of how accessed or acquired, whether directly
from us or from another Approved Source. By clicking on the appropriate button,
or by downloading, installing, accessing, or using any Offering, you agree to
these General Terms. If you are entering into these General Terms on behalf of
Customer, you represent that you have the authority to bind Customer. If you do
not agree to these General Terms, or if you are not authorized to accept the
General Terms on behalf of Customer, do not download, install, access, or use
any Offering. The "Effective Date" of these General Terms is: (i) the date of
Delivery; or (ii) the date you access or use the Offering in any way, whichever
is earlier. Capitalized terms are defined in the Definitions section below.
Effective September 23, 2024, and unless the context otherwise requires, any
reference in these General Terms to "Splunk Inc.", "Splunk", "we", "us" or "our"
will be deemed to refer to "Splunk LLC".

1. Your Use Rights and Limits

1.1. Your Use Rights. We grant you a non-exclusive, worldwide, non-transferable
and non-sublicensable right, subject to your compliance with these General Terms
and payment of applicable Fees, to use acquired Offerings only for your Internal
Business Purpose during the Term, up to the Capacity, and, if applicable, in
accordance with the Order ("Use Rights"). You have the right to make a
reasonable number of copies of On-Premises Products for archival and back-up
purposes.

1.2. Limits on Your Use Rights. Except as expressly permitted in the Order,
these General Terms or Documentation, your Use Rights exclude the right to, and
you agree not to (nor allow any user or Third Party Provider to): (i) reverse
engineer, decompile, disassemble or otherwise attempt to discover source code or
underlying structures, ideas, protocols or algorithms of, or used by, any
Offering; (ii) modify, translate or create derivative works based on any
3% viewed, press Space for next page or Enter for next line...
```

Read the agreement (I bet you won't) and hit y to agree with the license. Setup administrator username and password for Splunk.

We will setup the machine to run Splunk with user Splunk every time we reboot Splunk by `exit` user Splunk, change directory to bin with `cd bin` . Type `sudo ./splunk enable boot-start -user splunk`

```
splunk@splunk:~/bin$ exit
exit
treecyber@splunk:/opt/splunk$ cd bin
treecyber@splunk:/opt/splunk/bin$ sudo ./splunk enable boot-start -user splunk
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
treecyber@splunk:/opt/splunk/bin$
```

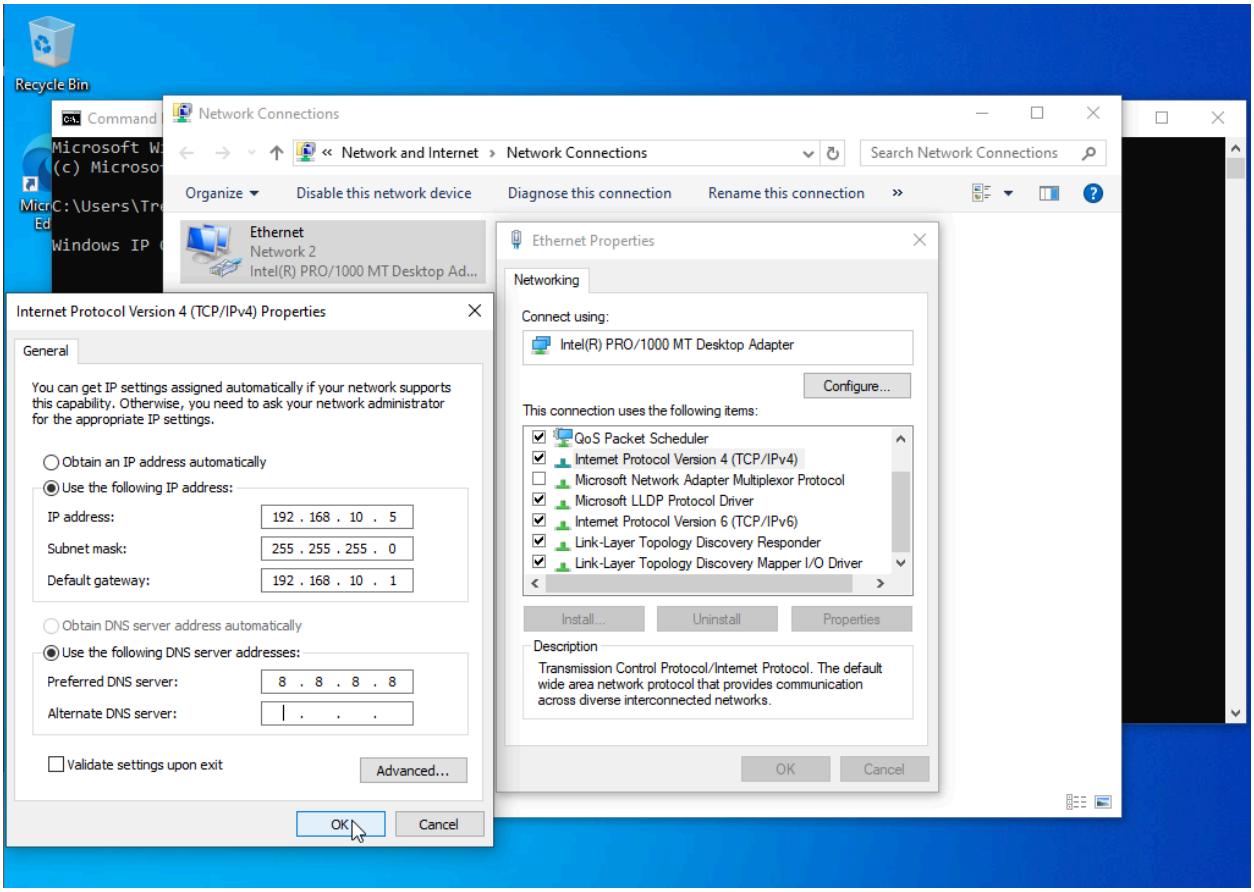
We had successfully install Splunk to our Splunk Server VM

Windows 10 Configure:

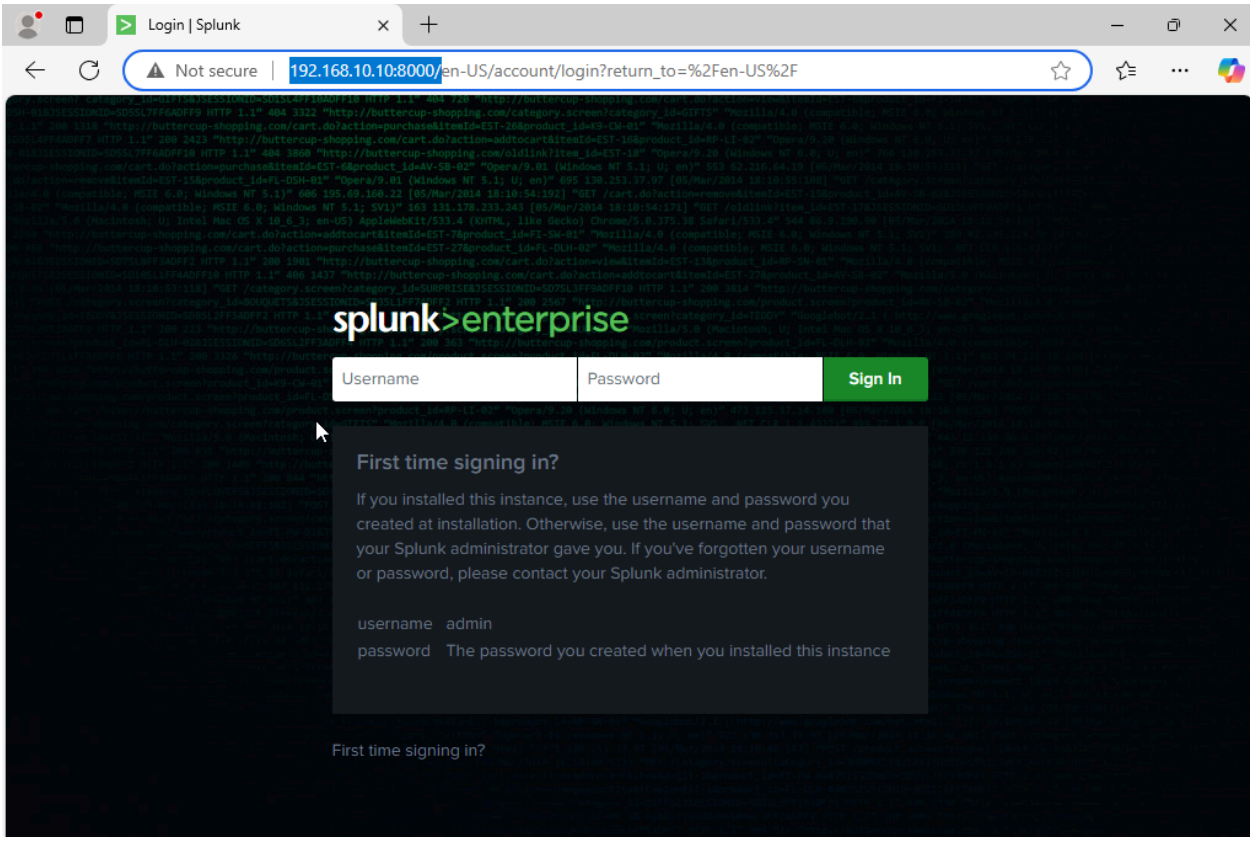
We will install Splunk Universal Forwarder and Sysmon on the Windows 10 VM

Start by changing the name and/or IP of the Windows PC (Make sure the IP of the PC is not conflict with any Server or Machine that we have drawn). This I believed you can do a little bit research on google and do it yourself, good luck!

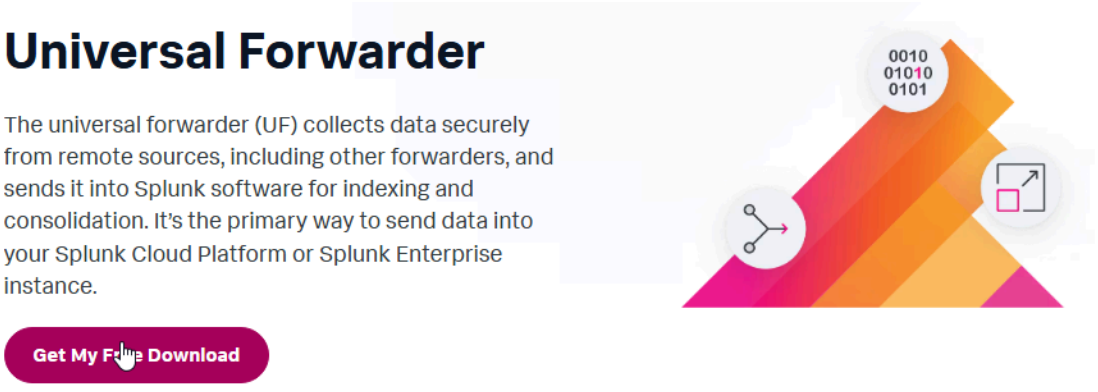
Here is my IP setup for Windows 10 VM

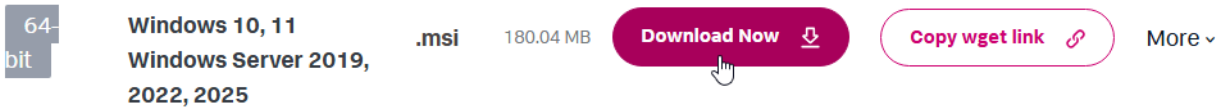


We can check if our Splunk Server is running by enter the IP of Splunk Server with port 8000 (Please note, Splunk listens on port 8000)

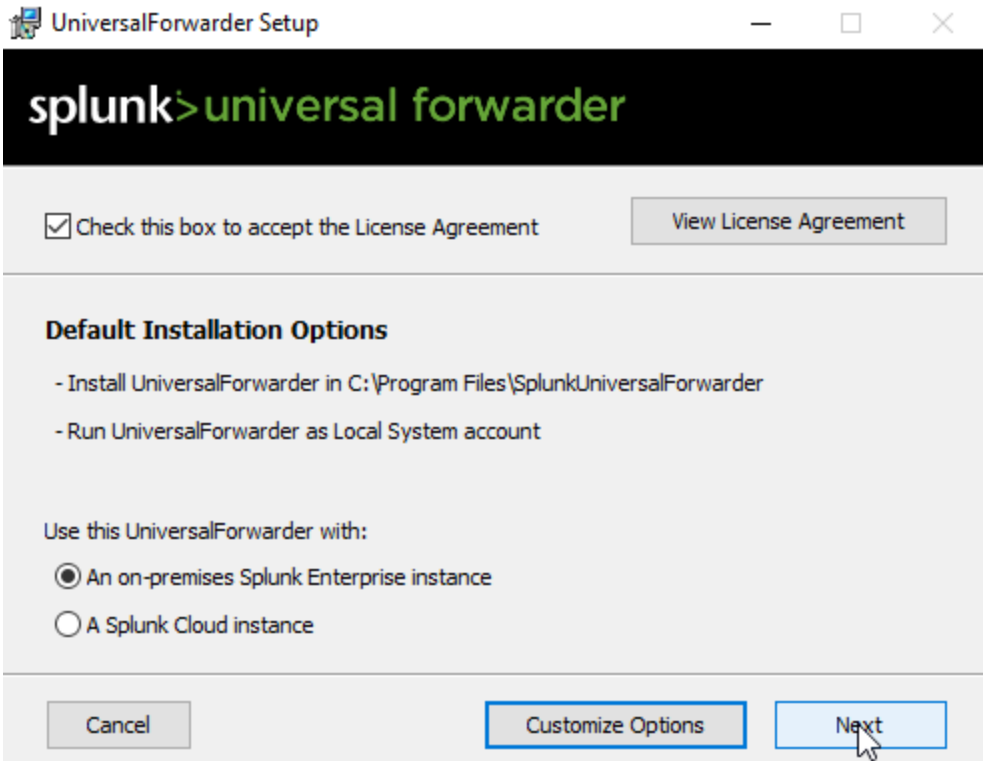


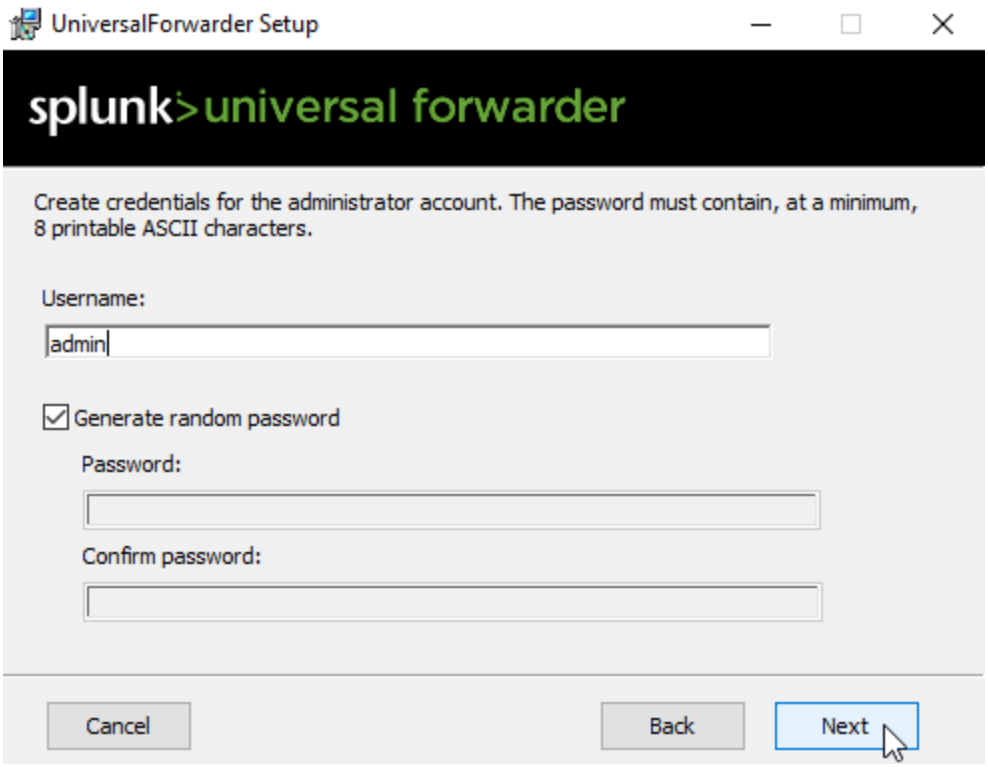
We will go ahead download the Splunk Universal Forwarder straight up on the Windows 10 VM:

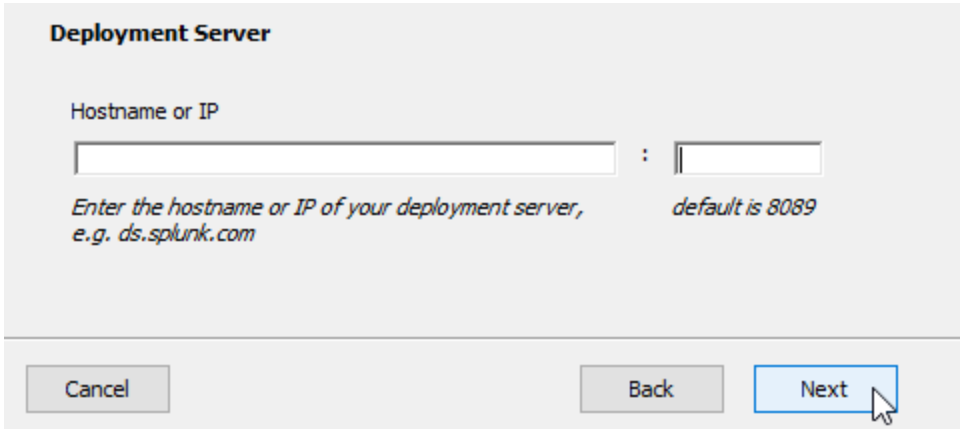


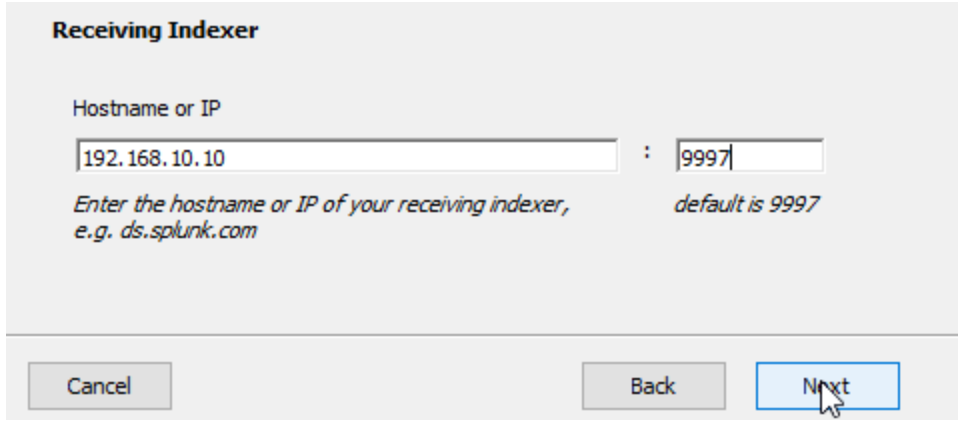


Double click on the Splunk file we just download and setup like the images below:

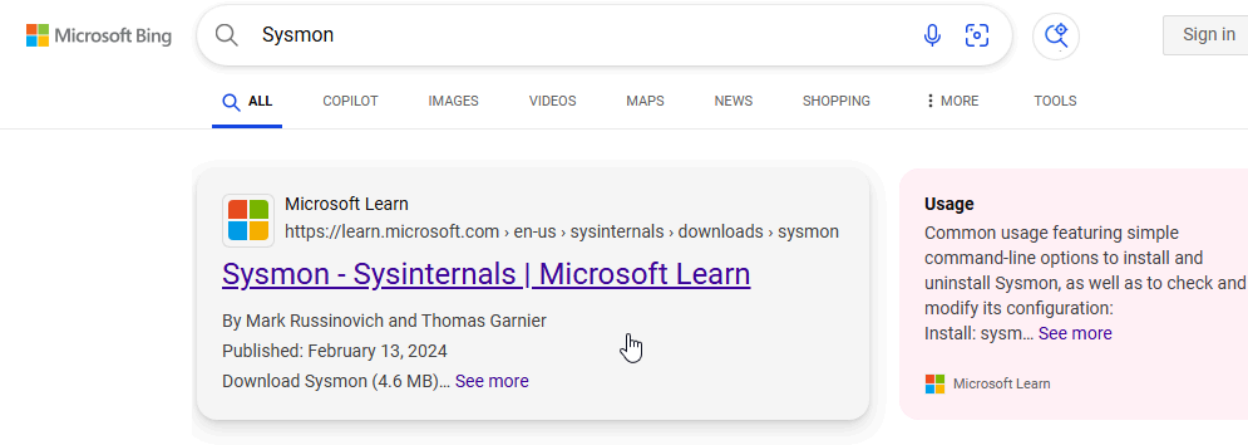


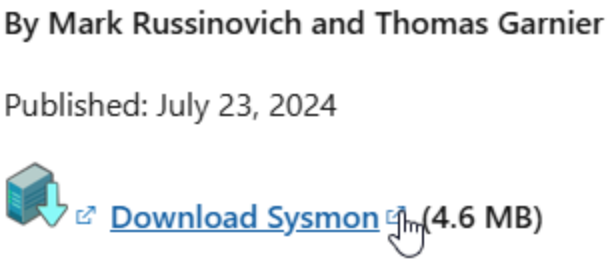

UniversalForwarder Setup
splunk>universal forwarder
Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.
Username:
admin
Generate random password
Password:
Confirm password:
Cancel
Back
Next


Deployment Server
Hostname or IP
:
Enter the hostname or IP of your deployment server, e.g. ds.splunk.com
default is 8089
Cancel
Back
Next


Receiving Indexer
Hostname or IP
192.168.10.10
:
9997
Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com
default is 9997
Cancel
Back
Next

Start downloading Sysmon after:

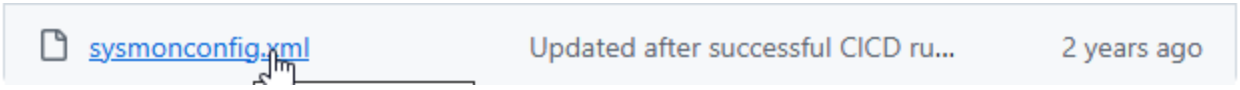




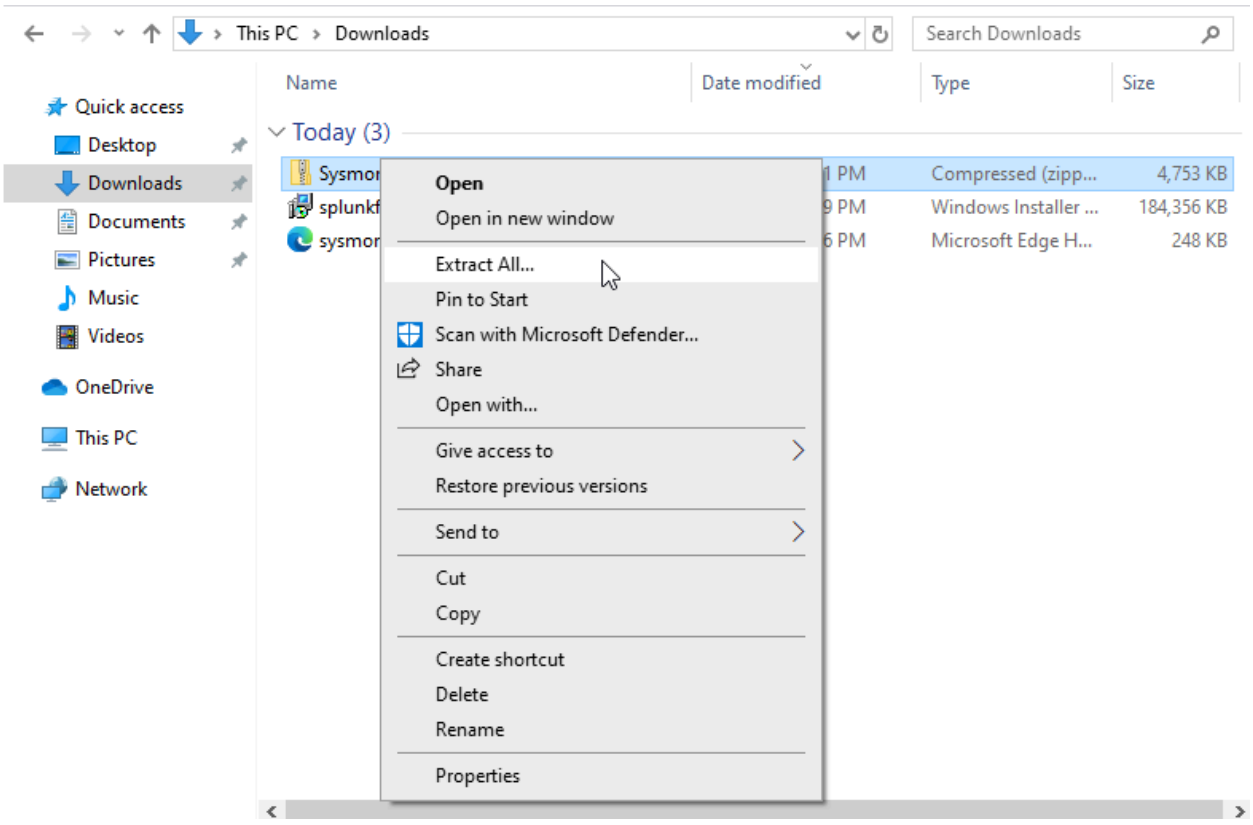
We also will need to configure Sysmon so we can download pre-configuration Sysmon file by Olaf

> https://github.com/olafhartong/sysmon-modular

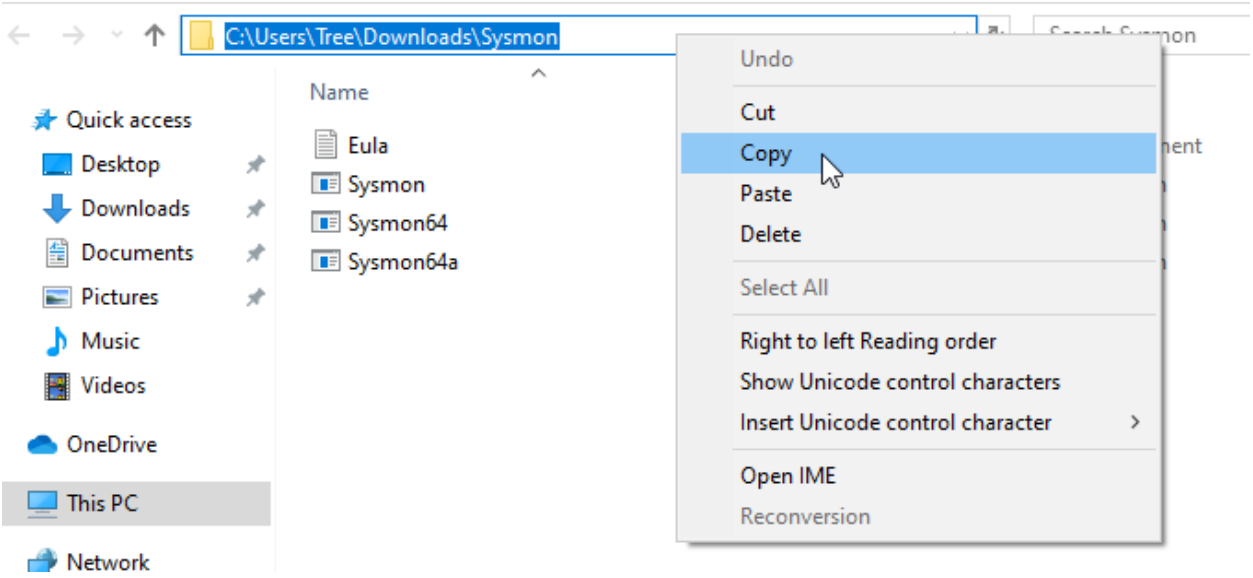
This will be the file we want to dowload:



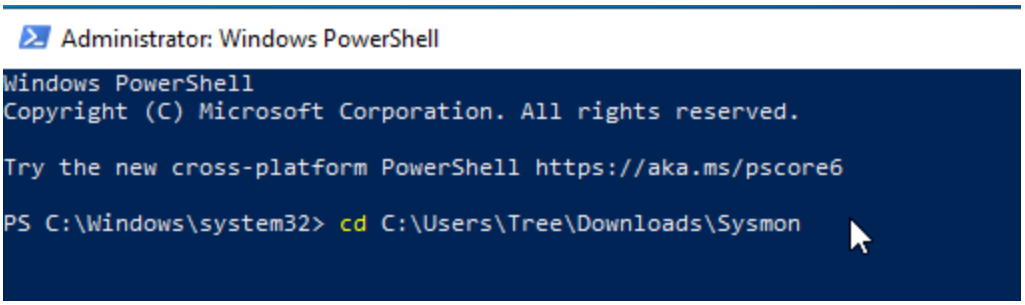
Go to the folder where you place your Splunk Universal Forward downloaded file and extract it:



Copy and paste the extract folder path:



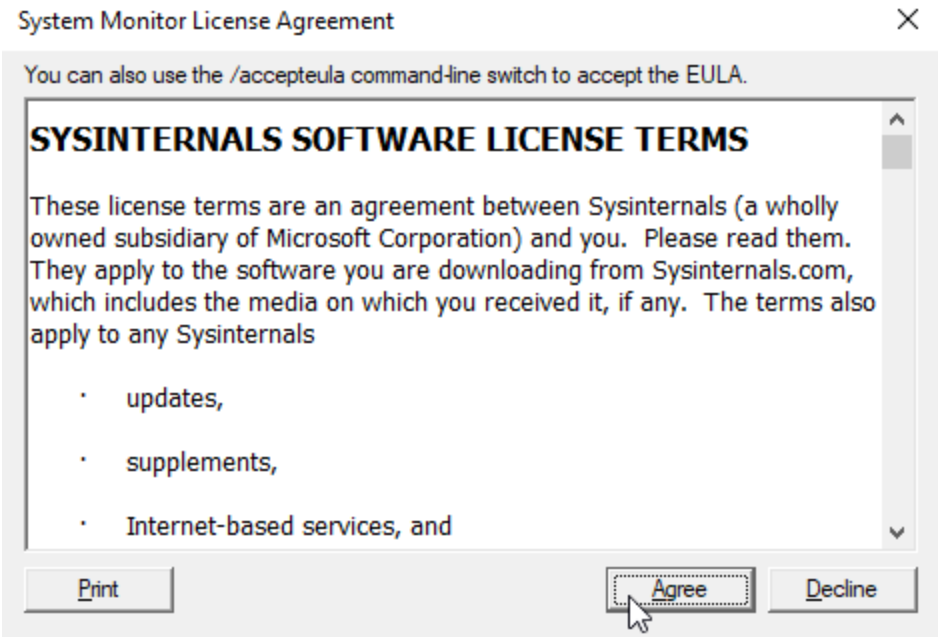
Open Windows PowerShell and run as administrator and change directory to the path you just copy:



Then we will run `.\Sysmon64.exe -i ..\sysmonconfig.xml`

-i: Indicate that I want to specify a configuration file

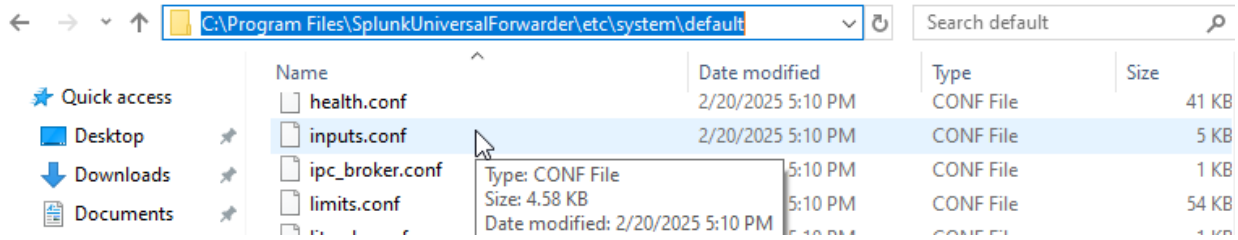
..\sysmonconfig.xml: To go back one directory and specify the configuration file we want to configure



```
PS C:\Users\Tree\Downloads\Sysmon> .\Sysmon64.exe -i ..\sysmonconfig.xml


System Monitor v15.15 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2024 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
PS C:\Users\Tree\Downloads\Sysmon>
```

Here come the most *important part:*

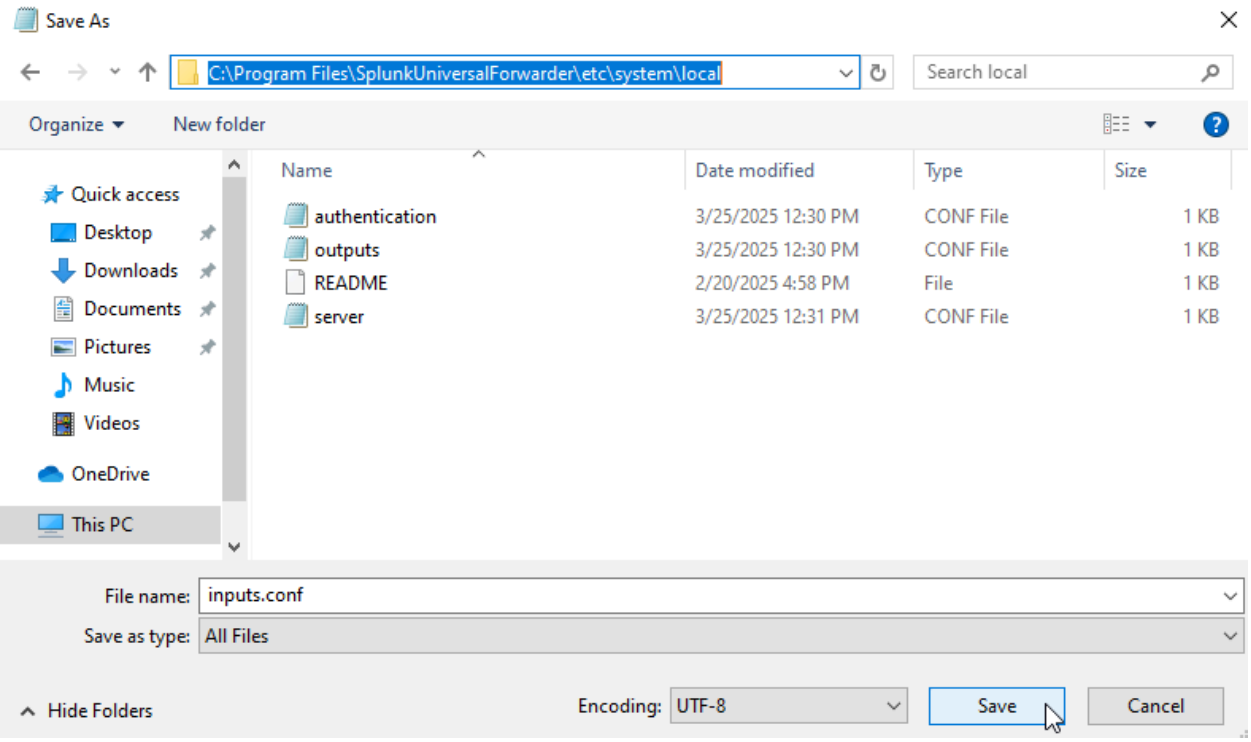
We want to inform our Splunk Universal Forwarder on what we want to send over to our Splunk Server. We will need to configure a file called inputs.conf located in C:\Program Files\SplunkUniversalForwarder\etc\system\default



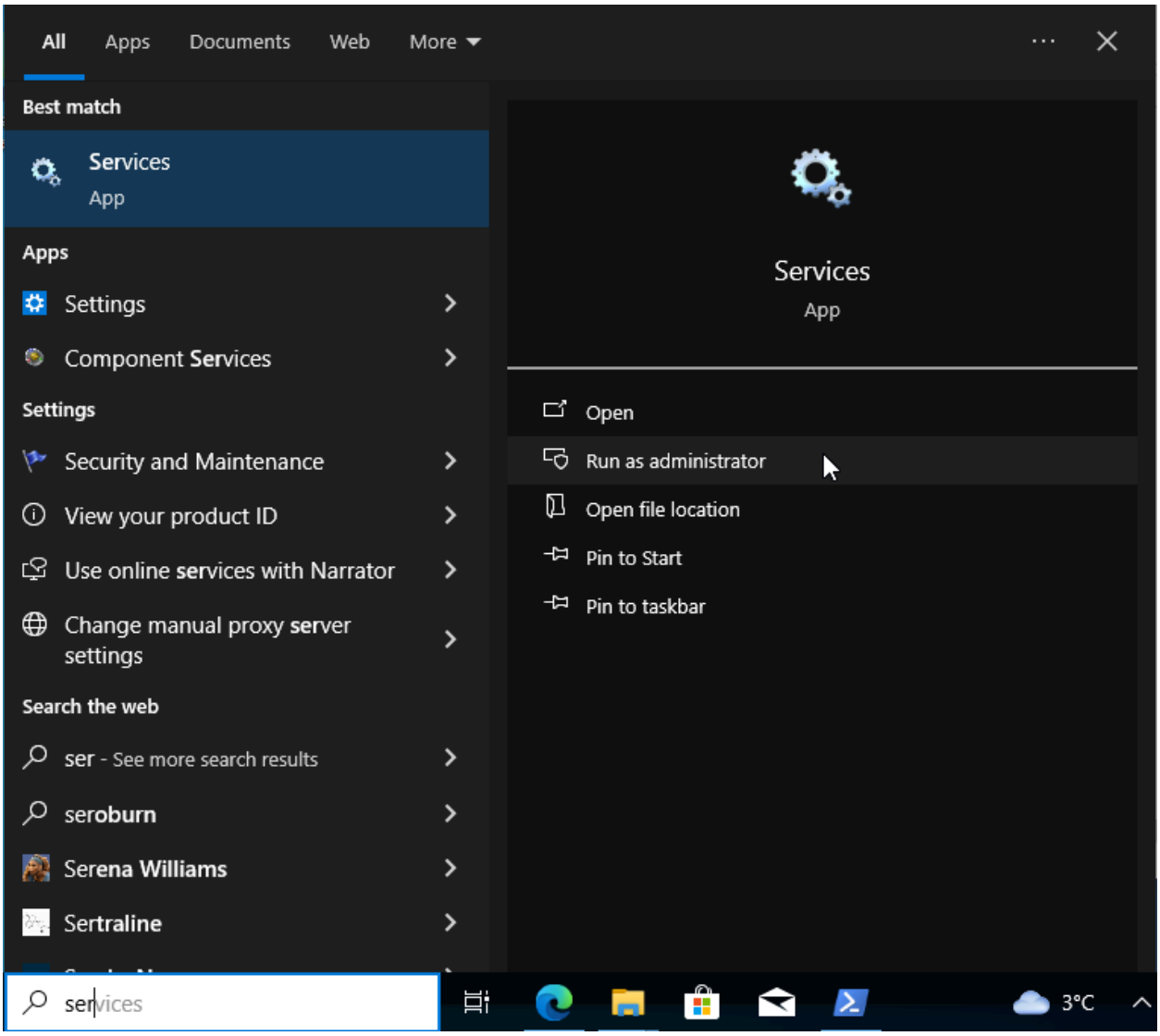
But we will not configure that inputs.conf file under *default* folder since you will need the default as a back up incase if you mess up the configuration. Instead you will create your own inputs.conf file under *local* folder. You can't directly create a new file under *local* folder since it require the admin privilege access. You can open Notpad, run as administrator and paste these configuration into it:

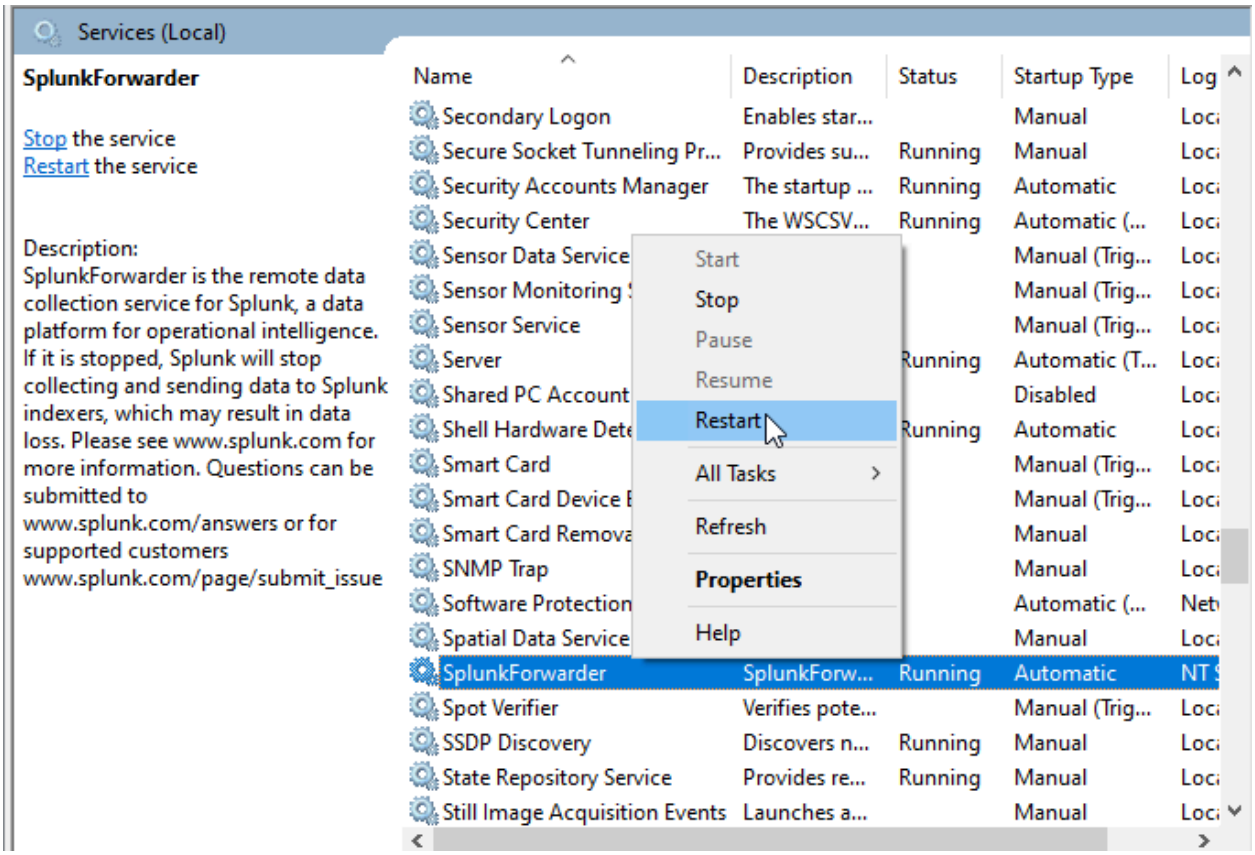
```
[WinEventLog://Application]
index = endpoint
disabled = false
```

```
[WinEventLog://Security]
index = endpoint
disabled = false

[WinEventLog://System]
index = endpoint
disabled = false

[WinEventLog://Microsoft-Windows-Sysmon/Operational]
index = endpoint
disabled = false
renderXml = true
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
```

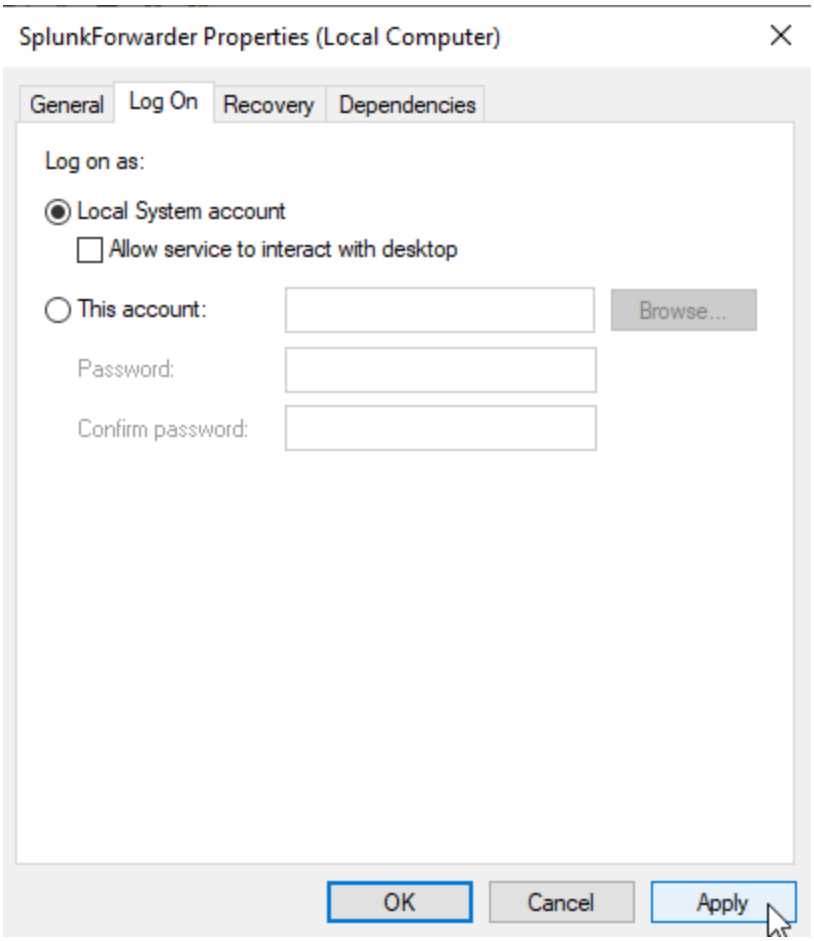


After every time we make a change on our inputs.conf, you must restart the Splunk UF services by:


All
Apps
Documents
Web
More
Best match
Services
App
Apps
Settings
Component Services
Settings
Security and Maintenance
View your product ID
Use online services with Narrator
Change manual proxy server settings
Search the web
ser - See more search results
seroburn
Serena Williams
Sertraline
services
Services
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar
3°C

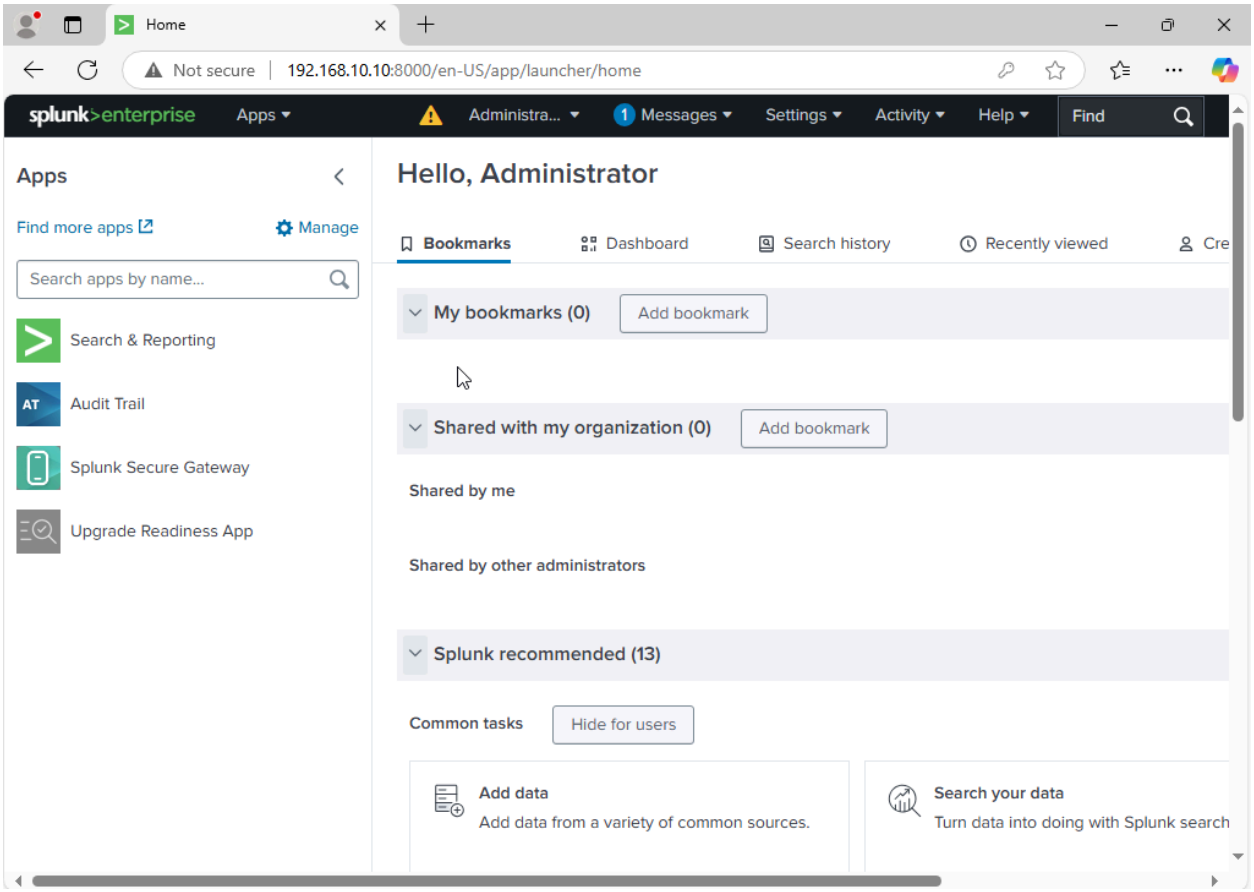


Before we restart, we will need to configure the Log on as Local System account for SplunkForwarder due to collects log permissions:

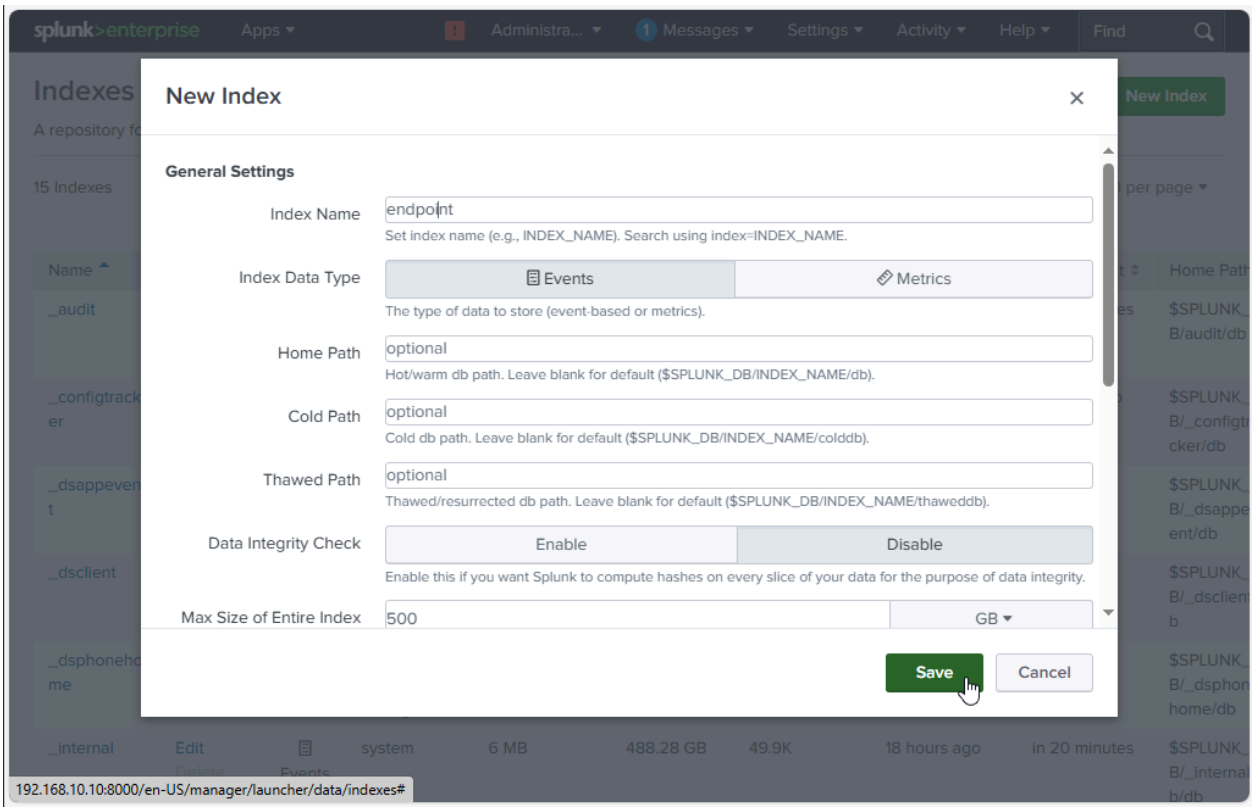


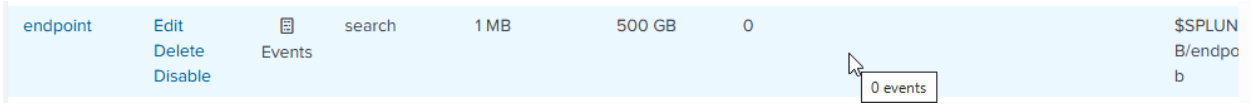
Please note: ignore the warning or error

Let head back to the Splunk Server browser and enter your credential:

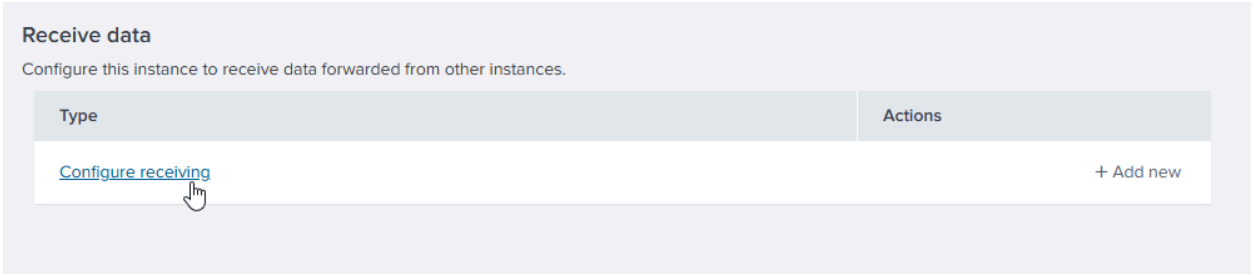


Remember the inputs.conf we configured had a indexed of endpoint? We will add the endpoint index by clicking Settings → Indexes → New Index

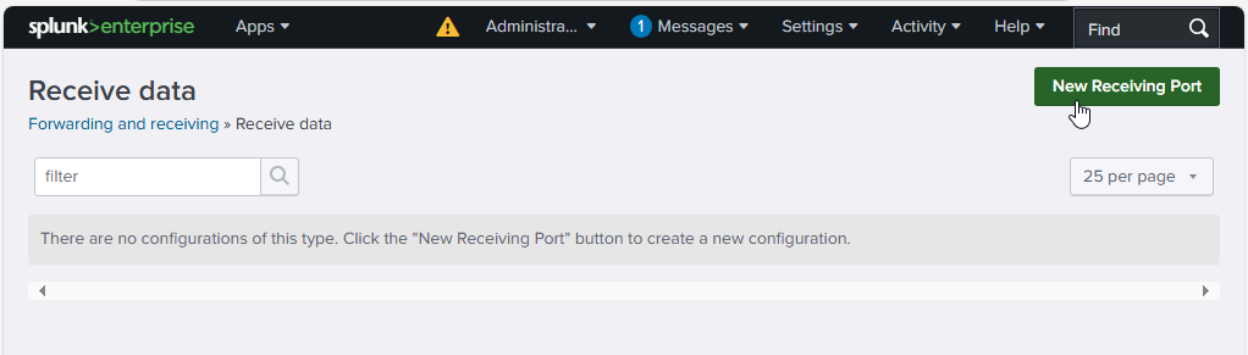




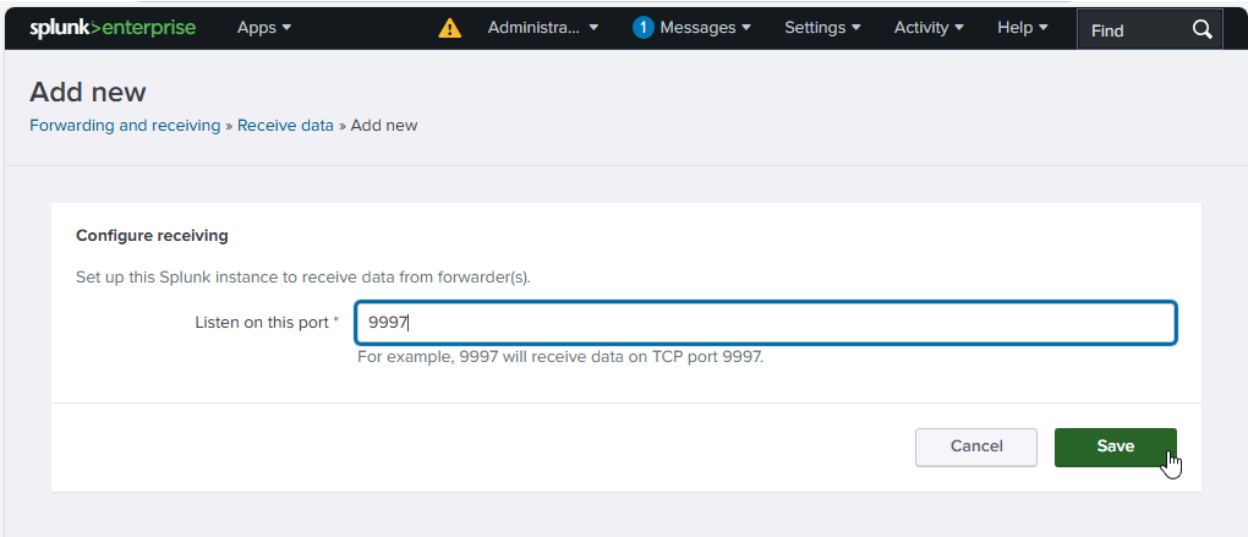
Next we will need to unable our Splunk Server to receive the data by go to Settings → Forwarding and receiving. We will want to click the Configure receiving under Receive data:



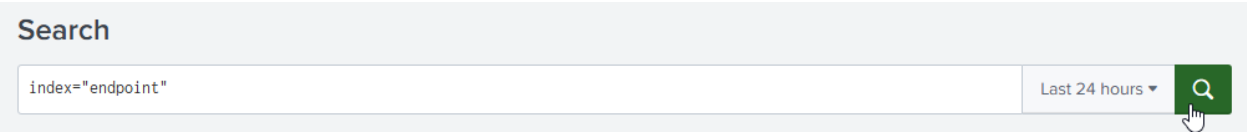
Click New Receiving Port:



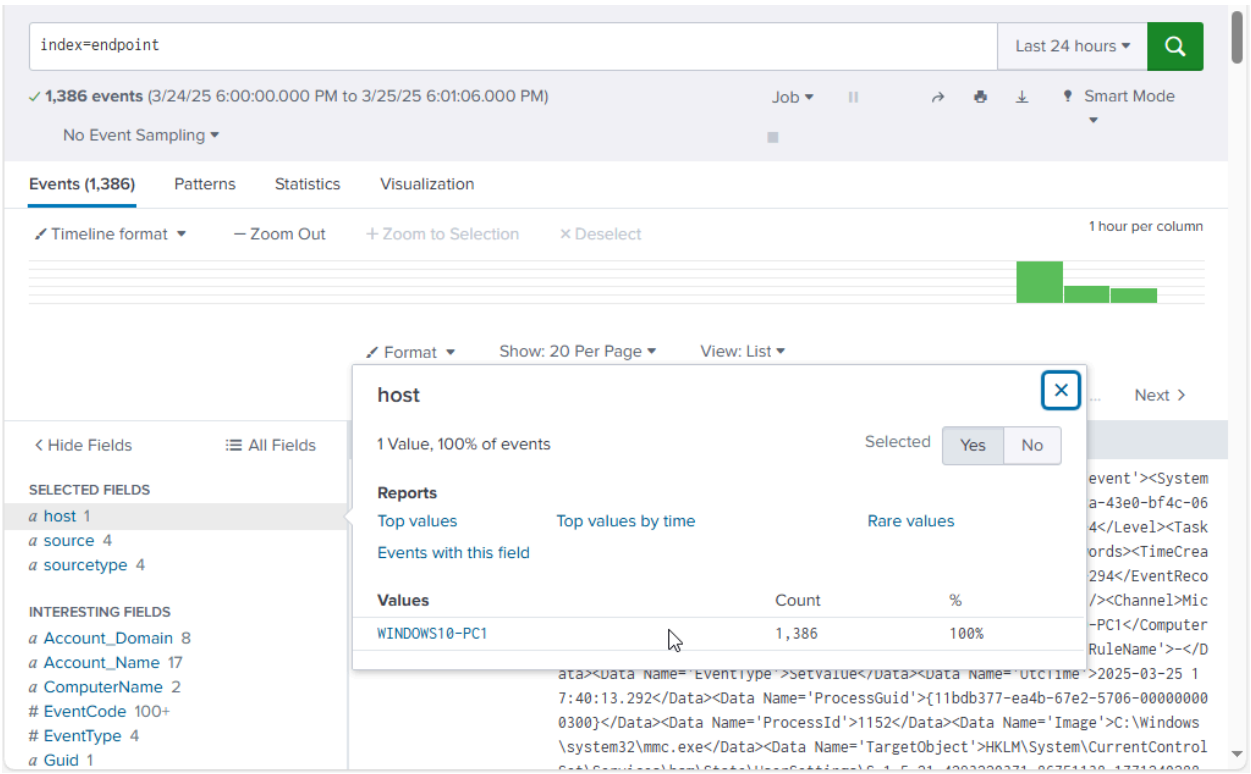
During our Splunk Universal Forwarder setup, we set the port as default port 9997 so we will enter port 9997 for the Listen on this port:



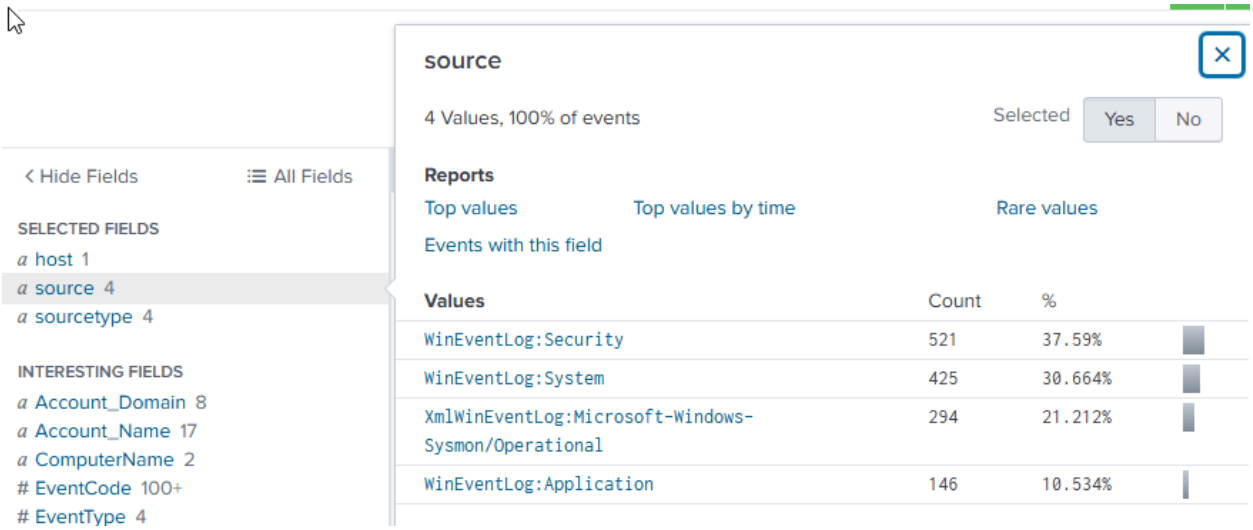
If everything setup and configure correctly, you should see all the events data coming in from our Windows 10 VM. You can check it by click on Apps → Search & Reporting. Skip the tutorial and tour if needed, search up for index=”endpoint” with a timeframe of 24 hours:



You will see all the events happen within 24 hours in the WINDOWS10-PC1 host which is the name of my Windows 10 VM:



Our the data that you configure in inputs.conf to receive from Windows 10 VM will show under *source*



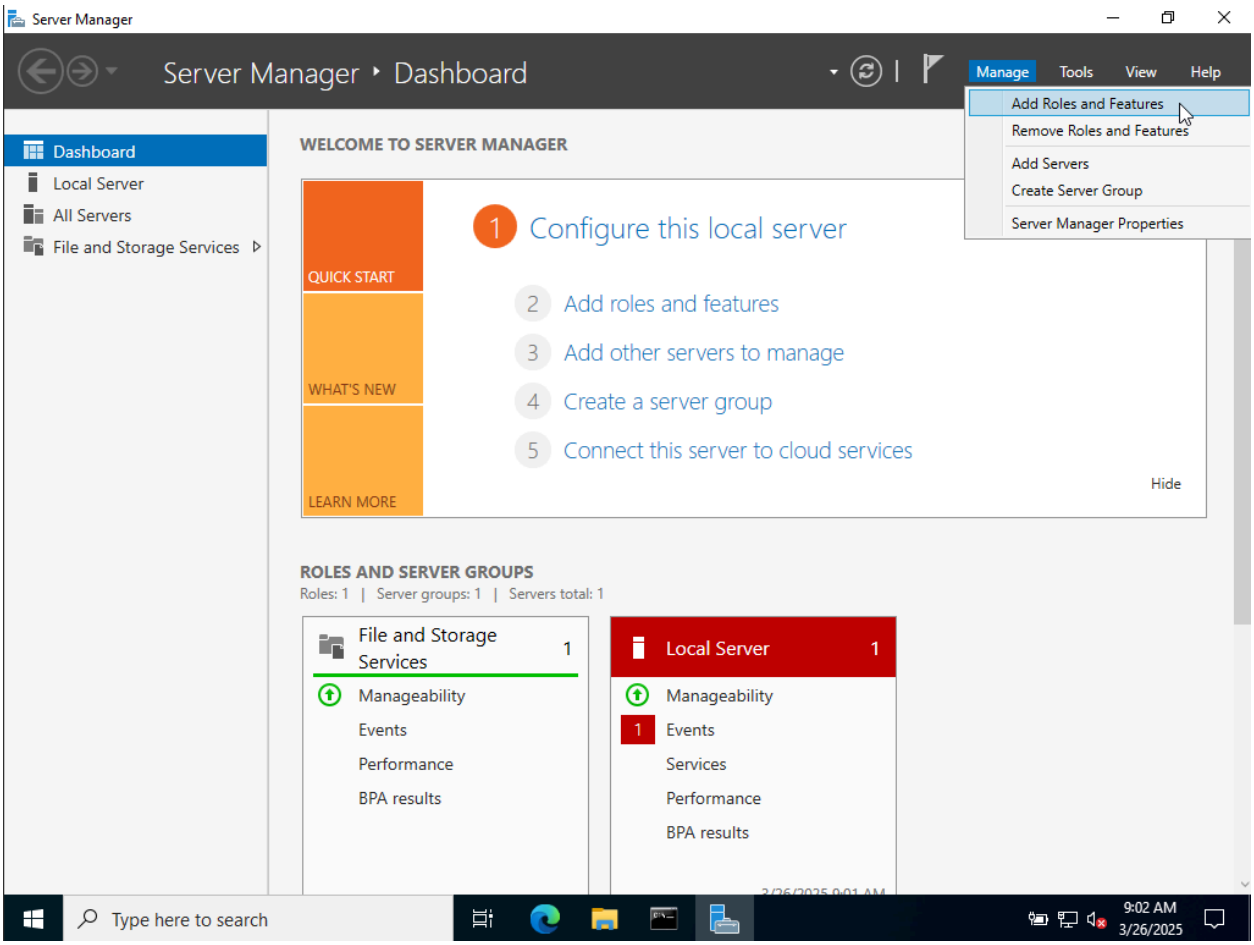
You had complete install and configure Sysmon and Splunk to Windows 10 VM. You will need to do the same for the Active Directory Server VM also to monitor the log. The process will be similar for Windows 10 machine.

Active Directory Server Configure:

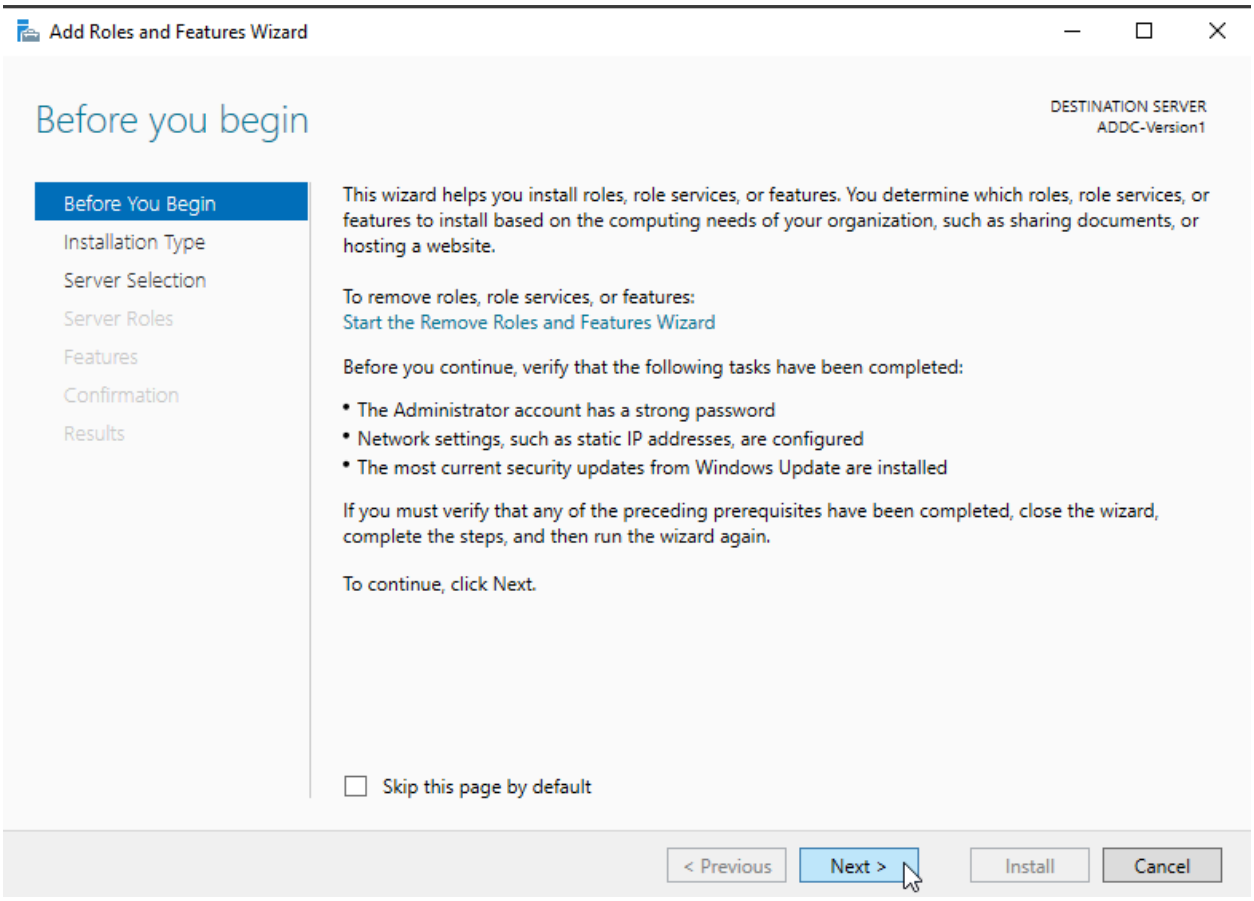
- Similar with Windows 10 Configuration, you will want to setup Splunk Universal Forwarder and Sysmon.
- Make sure to change the name and IP match with the diagram we plan

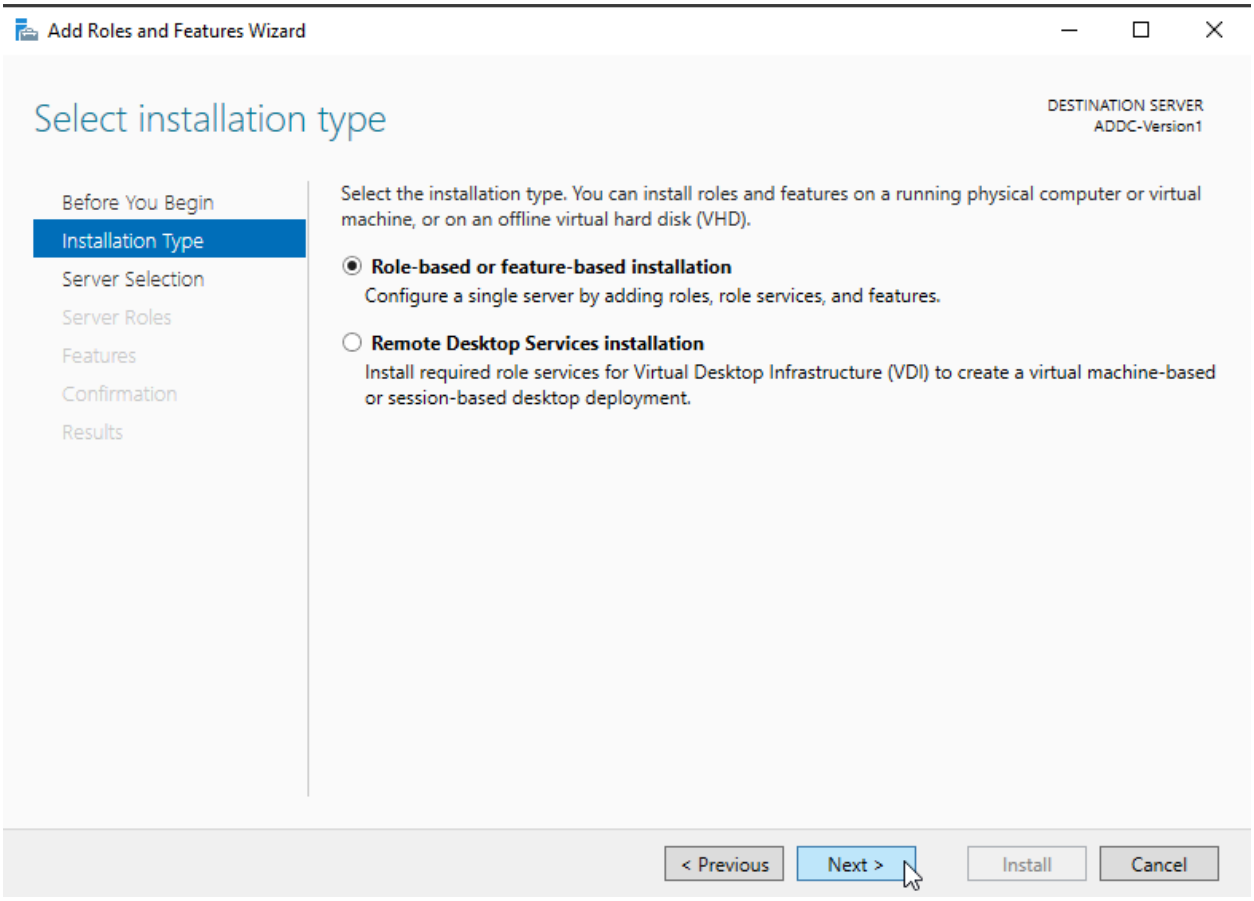
Setup Active Directory

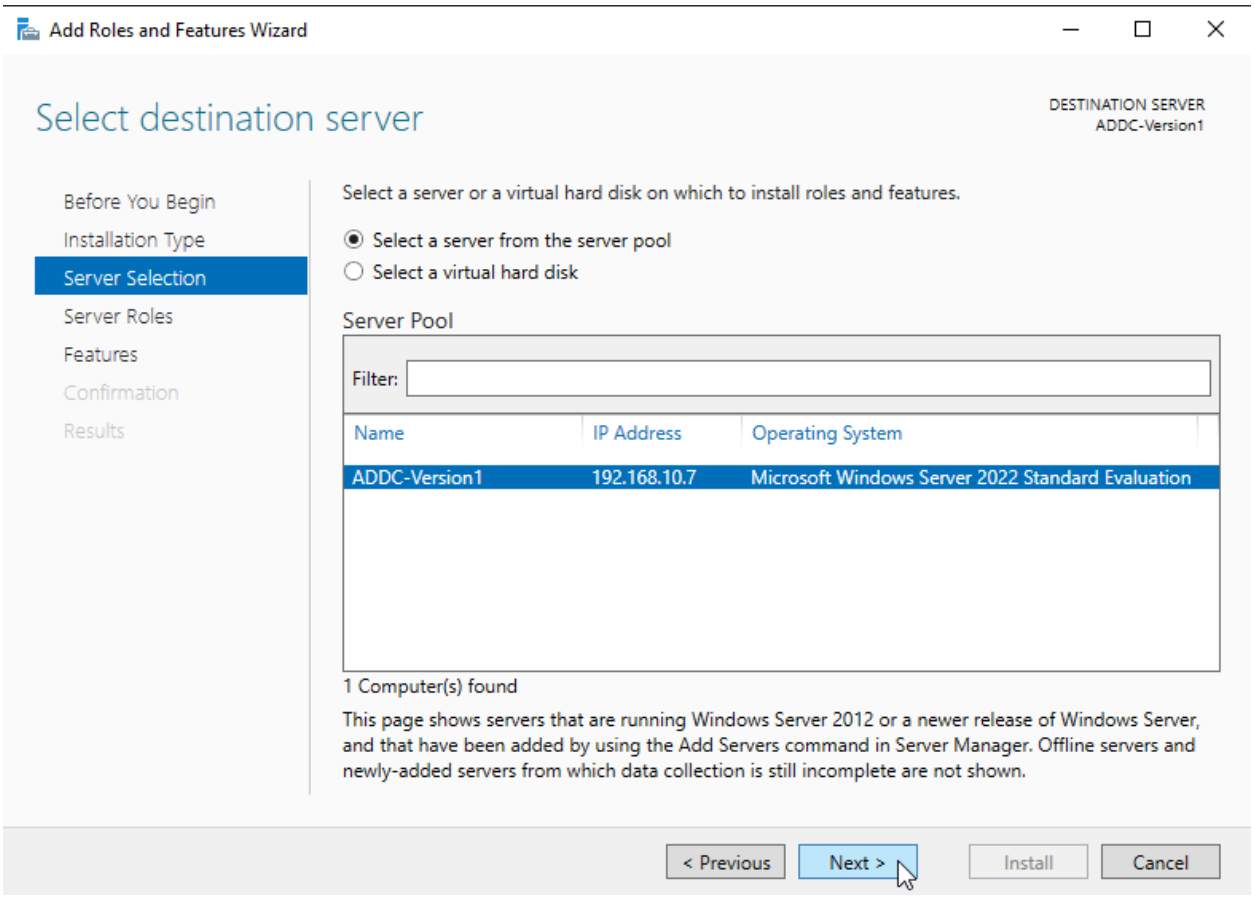
Head to Server Manager → Manage → Add Roles and Feautures:



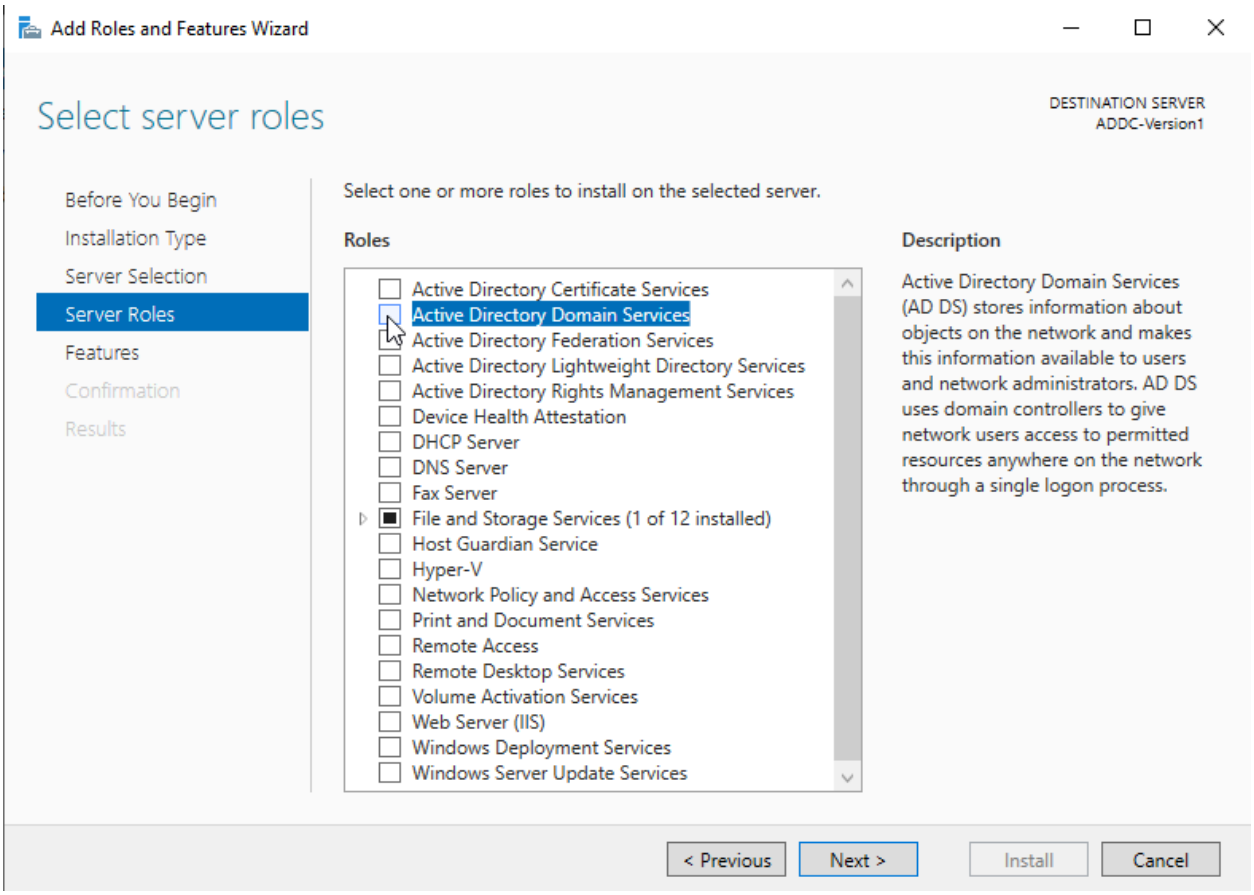
Setup the setting like this:

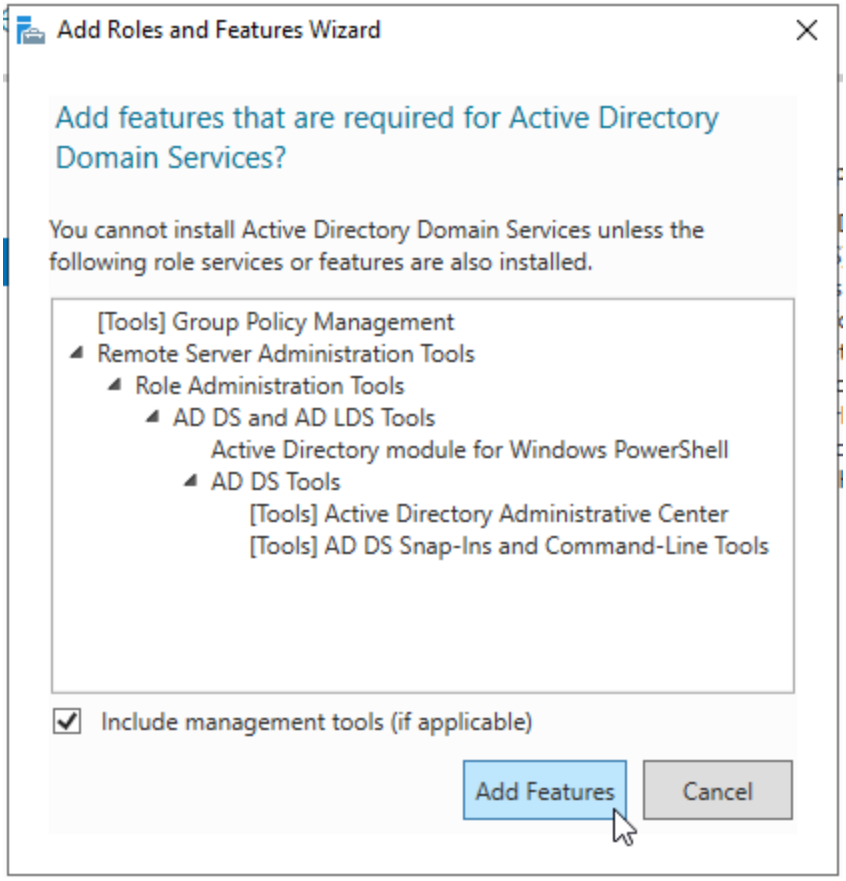

Add Roles and Features Wizard
Before you begin
DESTINATION SERVER
ADDC-Version1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install 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

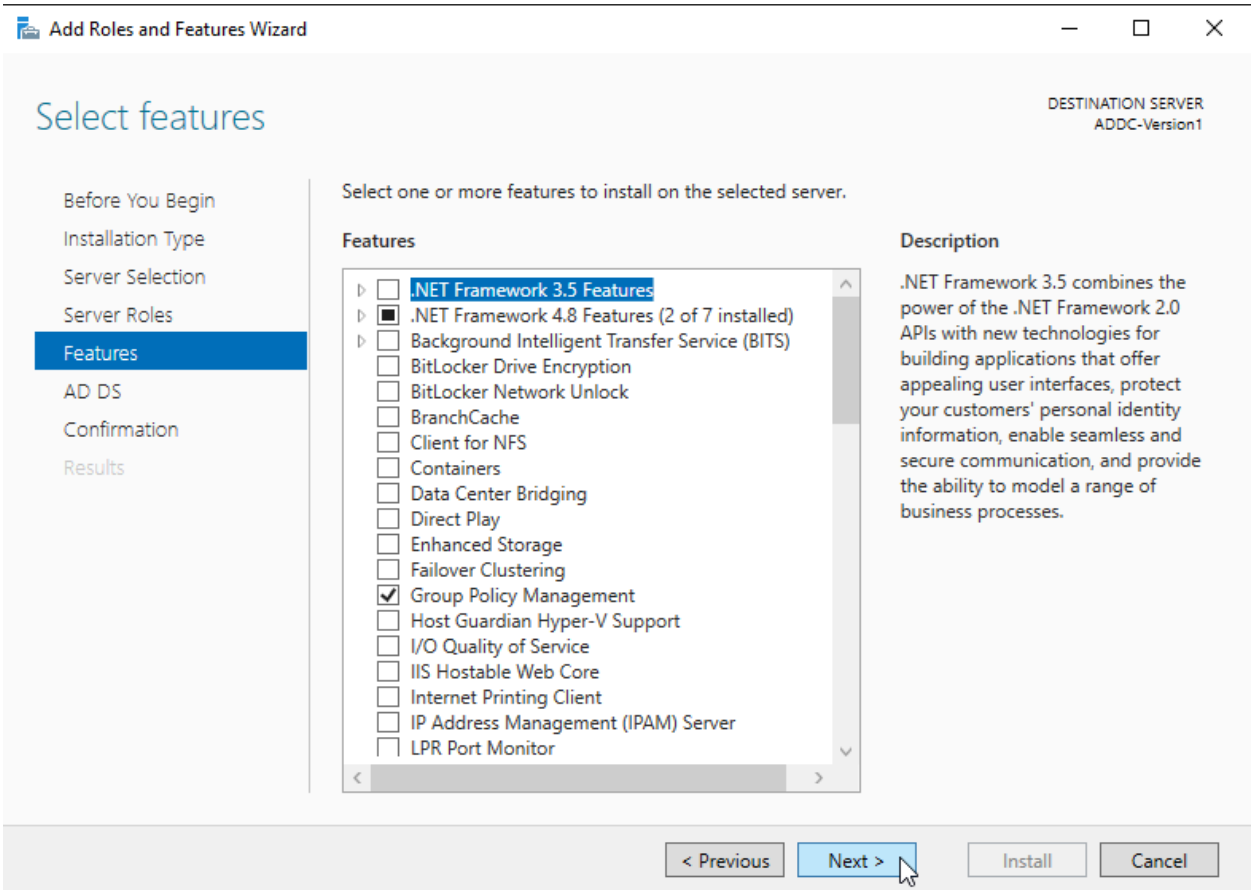

Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
ADDC-Version1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or 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

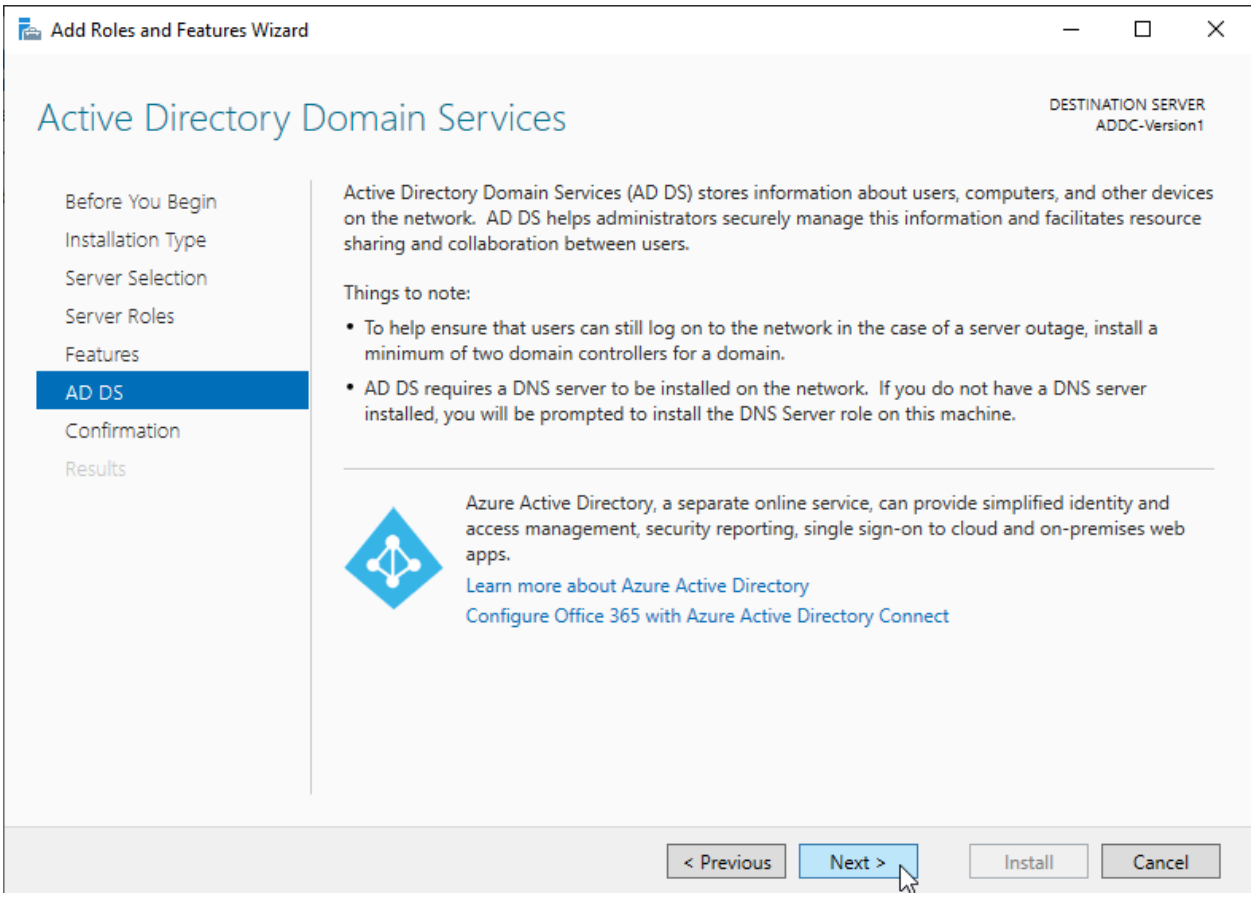


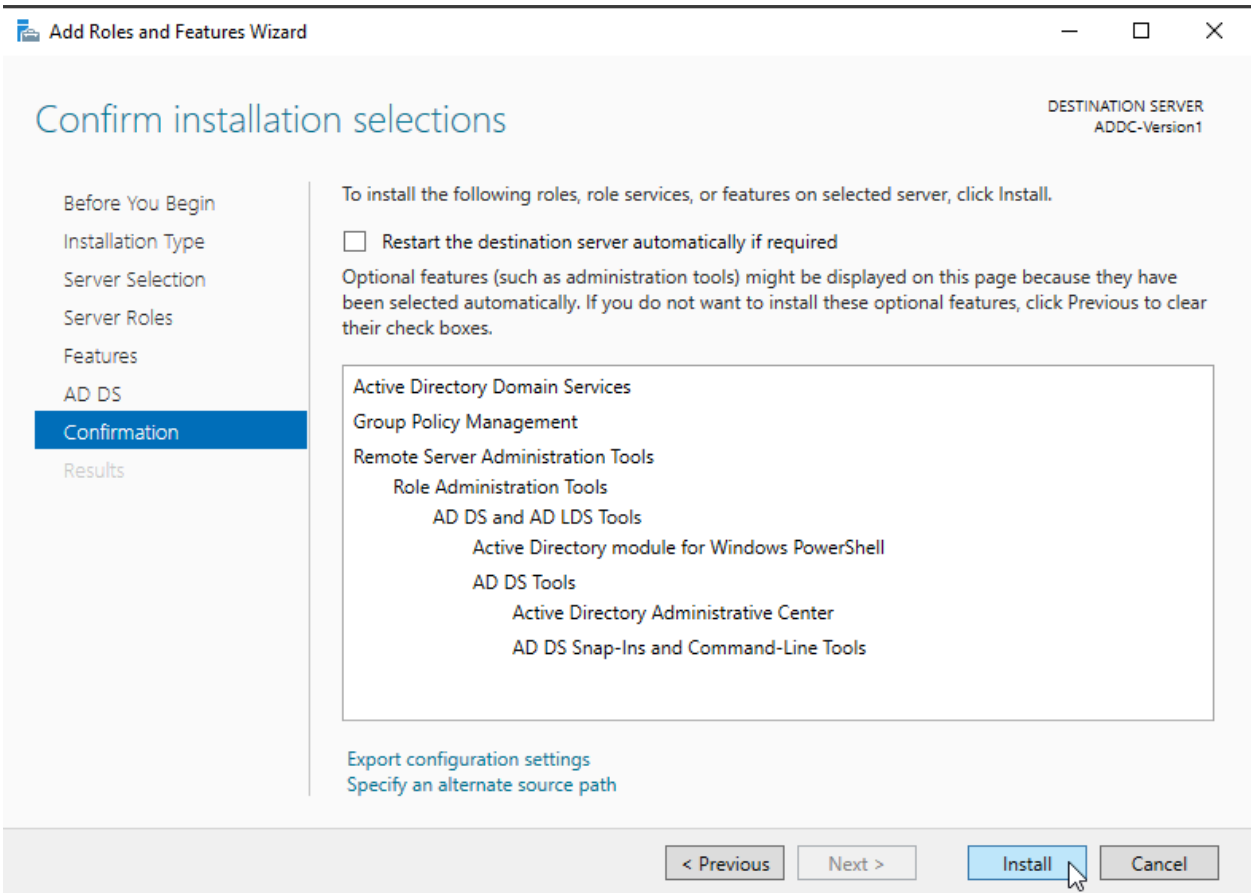
This is where you can see the company servers (not include Splunk)


Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
ADDC-Version1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Windows Server Update Services
Description
Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
< Previous
Next >
Install
Cancel

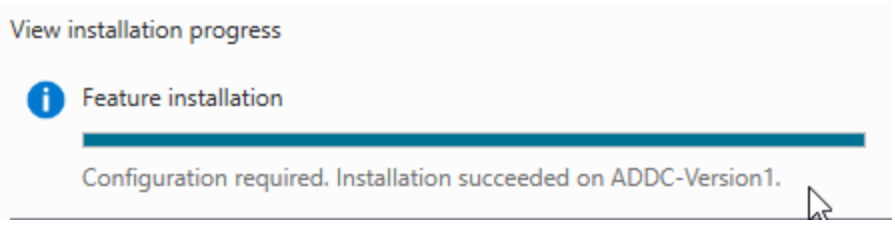

Add Roles and Features Wizard
Add features that are required for Active Directory Domain Services?
You cannot install Active Directory Domain Services unless the following role services or features are also installed.
[Tools] Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
[Tools] Active Directory Administrative Center
[Tools] AD DS Snap-Ins and Command-Line Tools
Include management tools (if applicable)
Add Features
Cancel


Add Roles and Features Wizard
Select features
DESTINATION SERVER
ADDC-Version1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features
.NET Framework 4.8 Features (2 of 7 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache
Client for NFS
Containers
Data Center Bridging
Direct Play
Enhanced Storage
Failover Clustering
Group Policy Management
Host Guardian Hyper-V Support
I/O Quality of Service
IIS Hostable Web Core
Internet Printing Client
IP Address Management (IPAM) Server
LPR Port Monitor
Description
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
< Previous
Next >
Install
Cancel

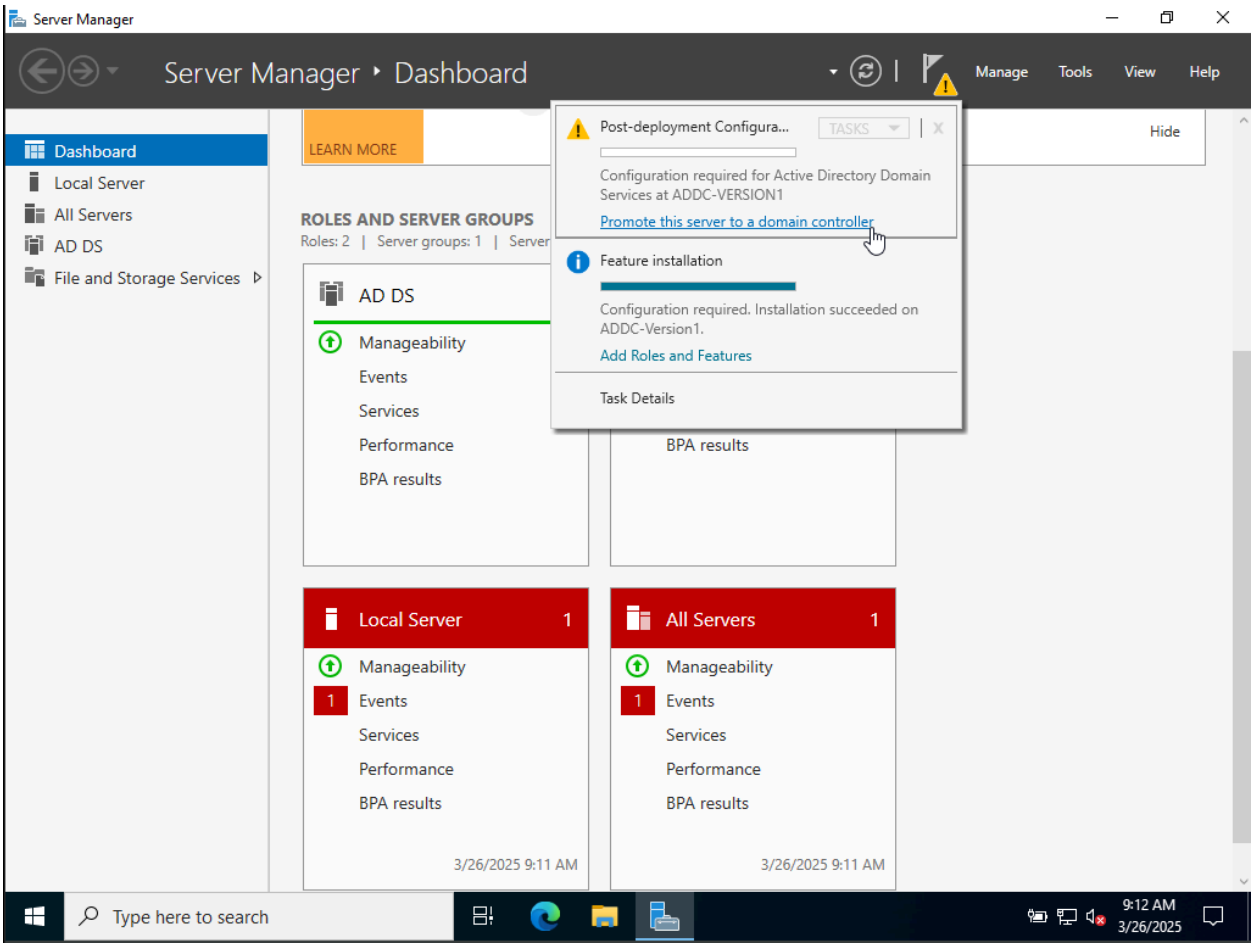

Add Roles and Features Wizard
Active Directory Domain Services
DESTINATION SERVER
ADDC-Version1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.
Things to note:
To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.
Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.
Learn more about Azure Active Directory
Configure Office 365 with Azure Active Directory Connect
< Previous
Next >
Install
Cancel

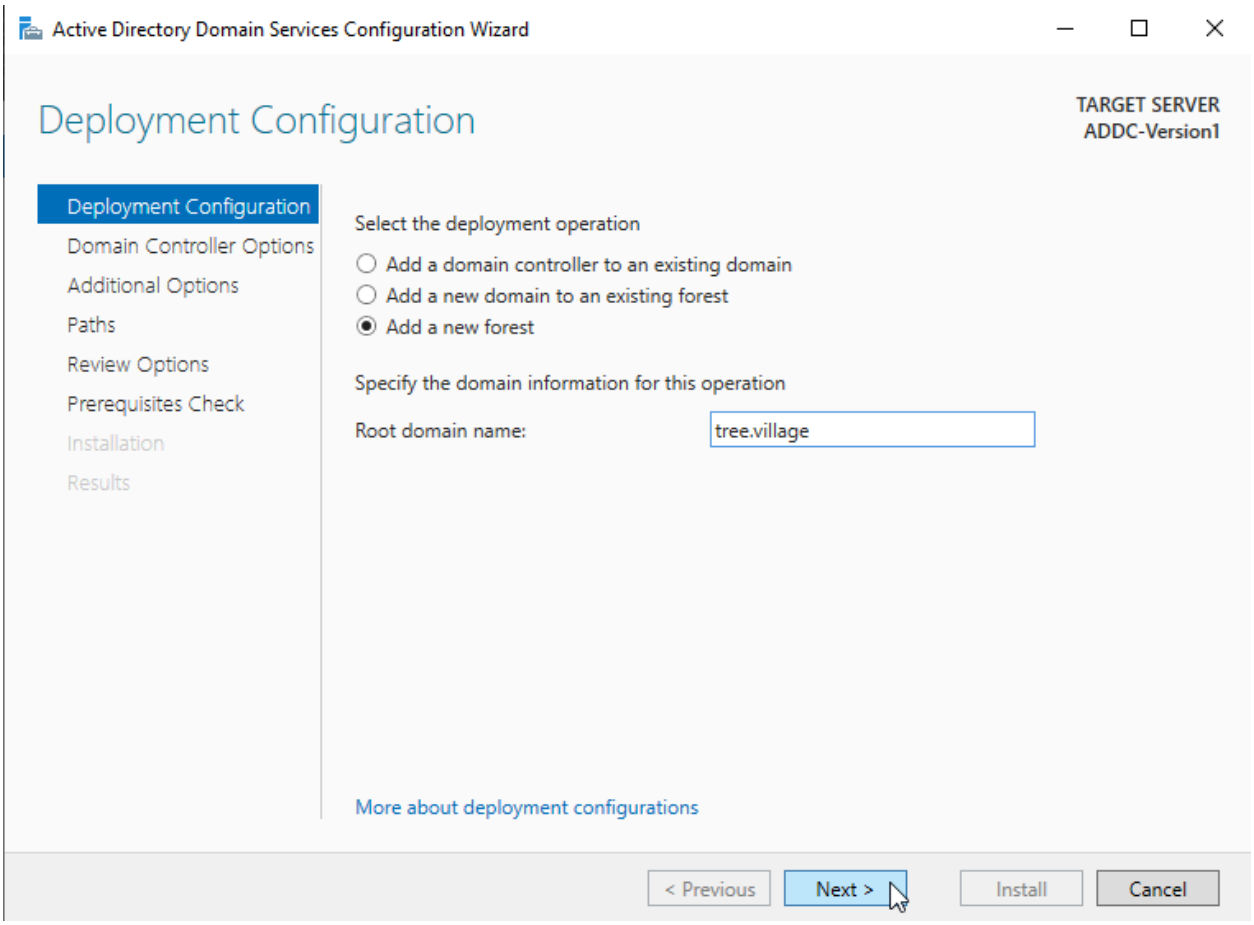


Wait for it to install until you see *Installation succeeded on "Name".*

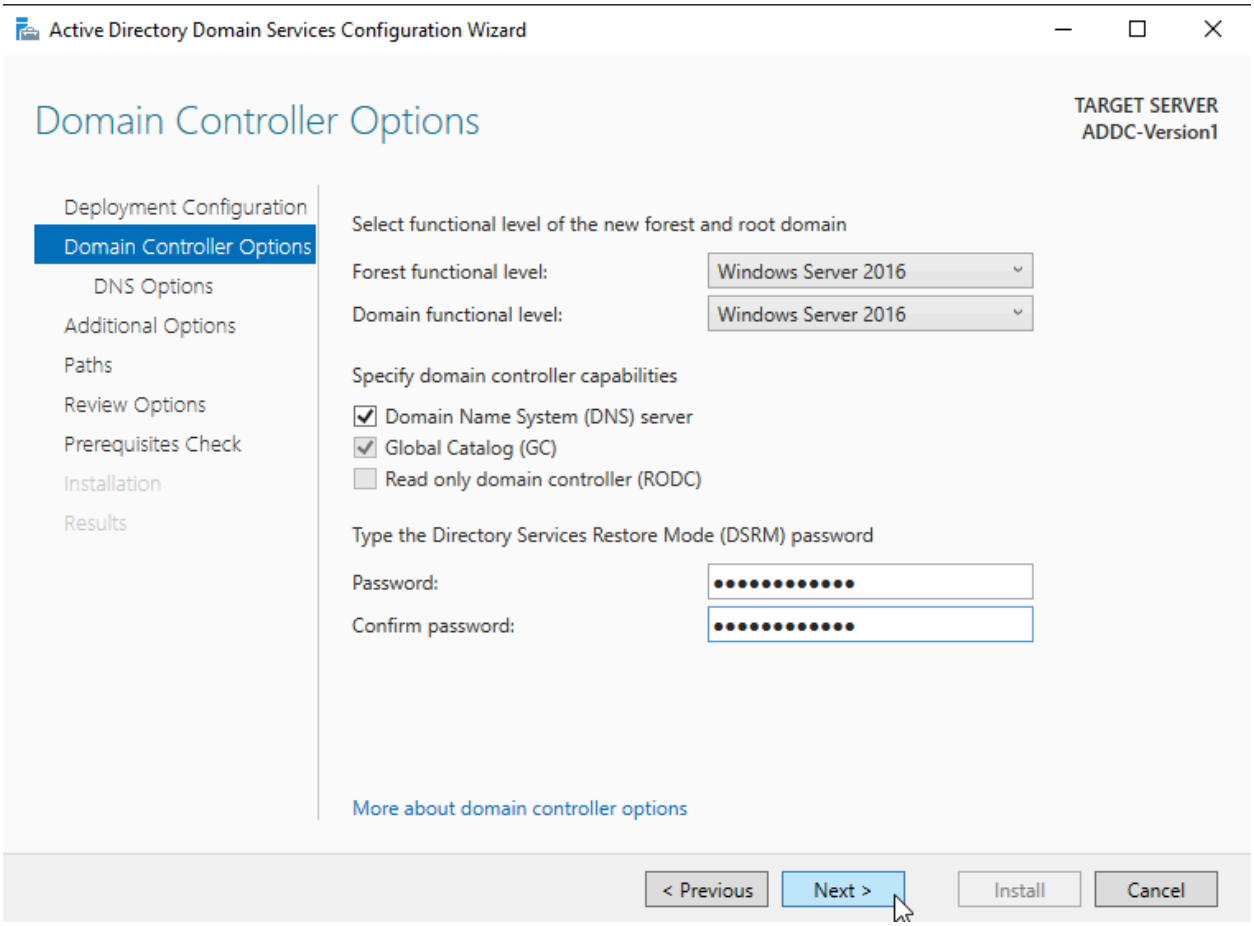


It time to setup the server into domain controller. Click to the Warning Icon above:

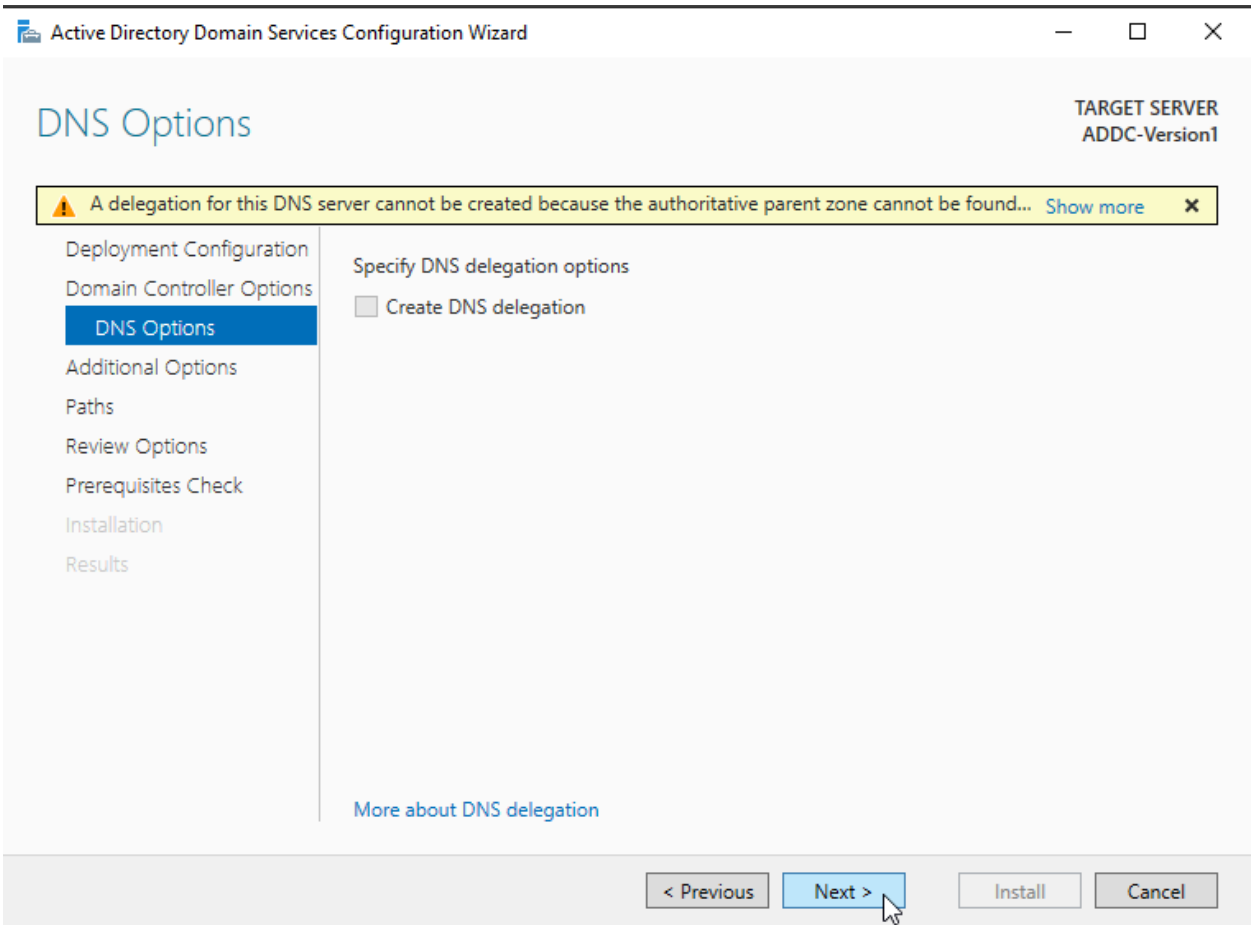

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
File and Storage Services
LEARN MORE
Hide
Post-deployment Configura...
TASKS
Configuration required for Active Directory Domain Services at ADDC-VERSION1
Promote this server to a domain controller
Feature installation
Configuration required. Installation succeeded on ADDC-Version1.
Add Roles and Features
Task Details
ROLES AND SERVER GROUPS
Roles: 2 | Server groups: 1 | Server
AD DS
Manageability
Events
Services
Performance
BPA results
BPA results
Local Server 1
Manageability
1 Events
Services
Performance
BPA results
3/26/2025 9:11 AM
All Servers 1
Manageability
1 Events
Services
Performance
BPA results
3/26/2025 9:11 AM
Type here to search
9:12 AM
3/26/2025

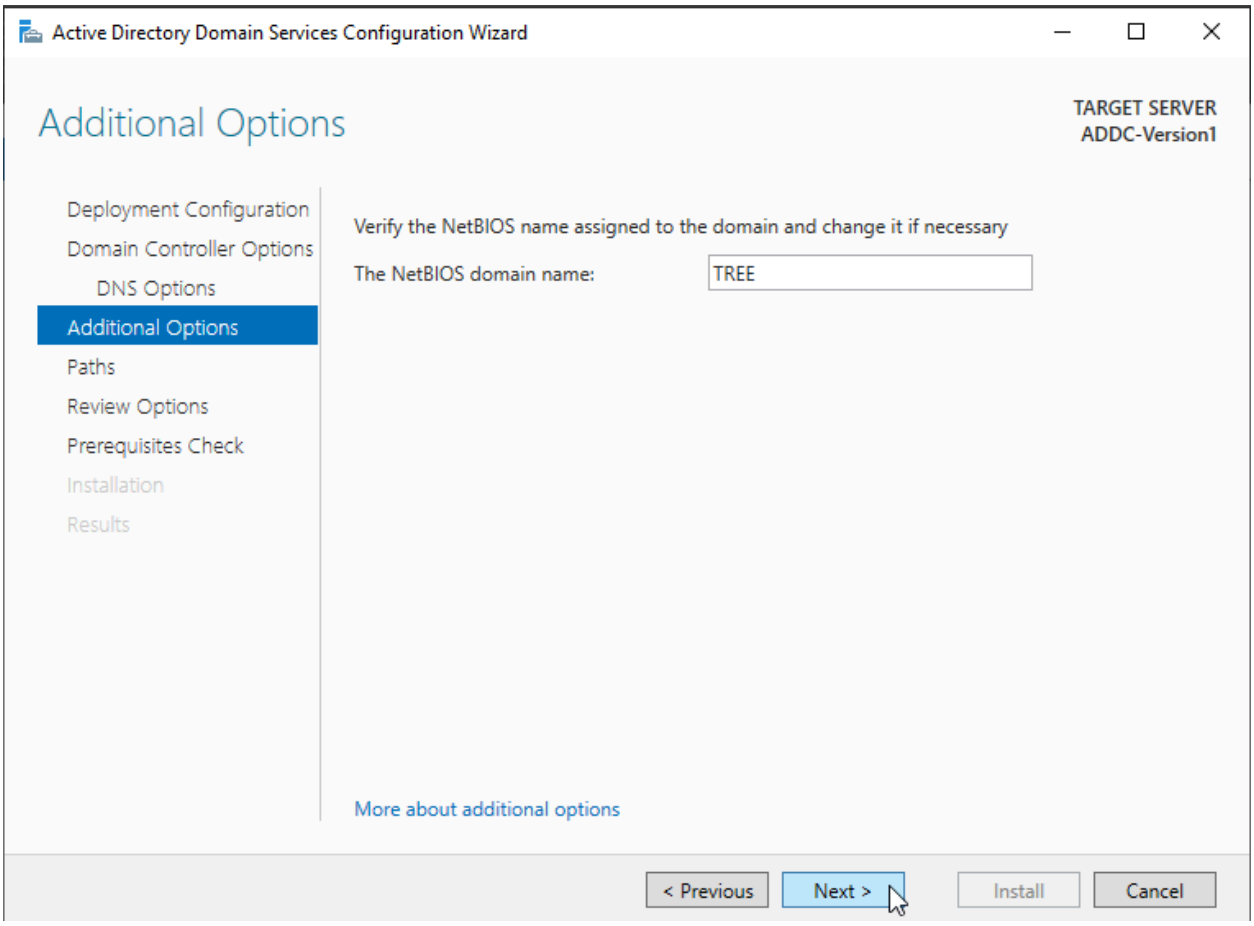


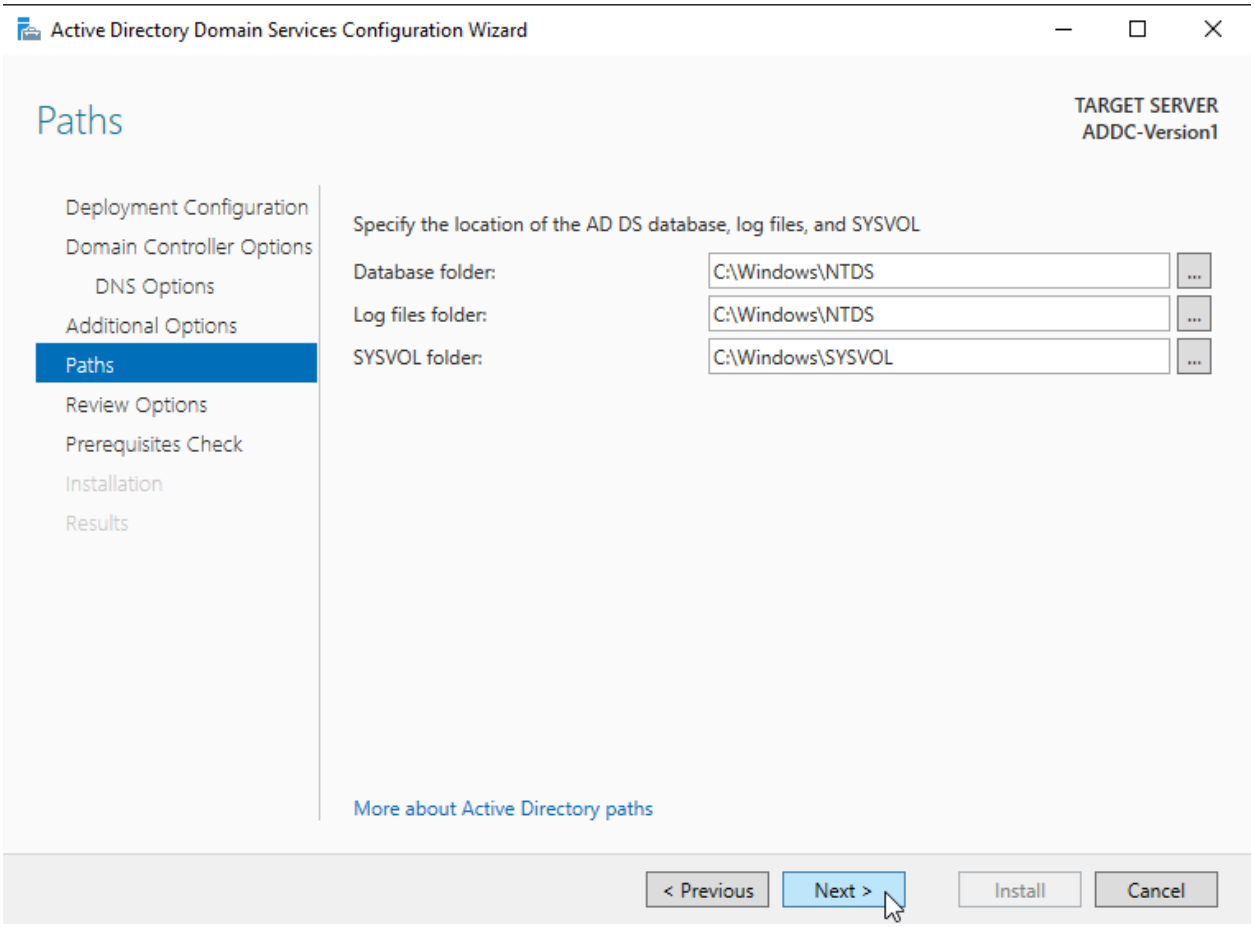
- We choose the *Add a new forest* because we want to create a brand new domain.
- The domain name must have a top level domain so the name must be `something.something`



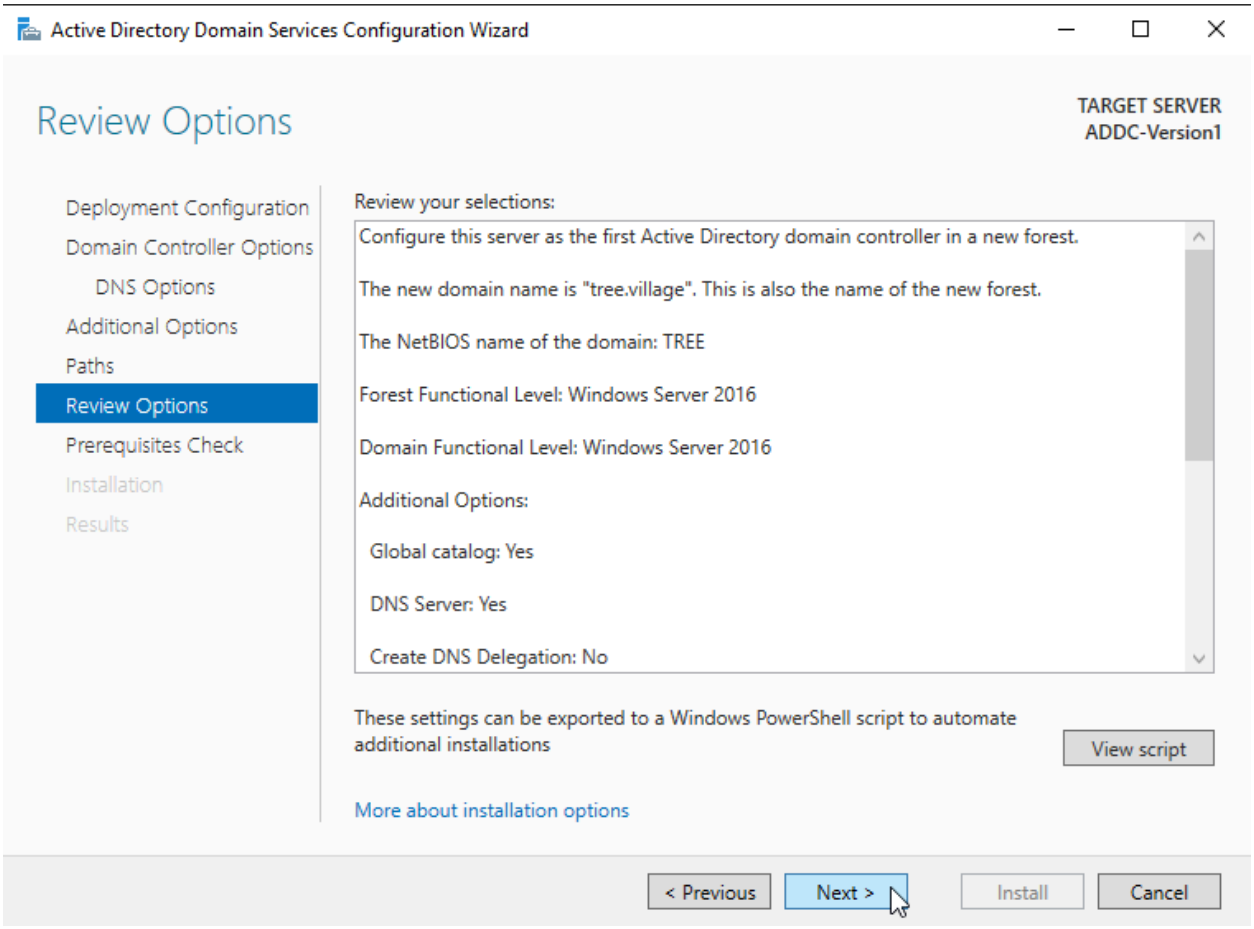
Password is Kirsten1230$


Active Directory Domain Services Configuration Wizard
DNS Options
TARGET SERVER
ADDC-Version1
A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found...
Show more
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify DNS delegation options
Create DNS delegation
More about DNS delegation
< Previous
Next >
Install
Cancel

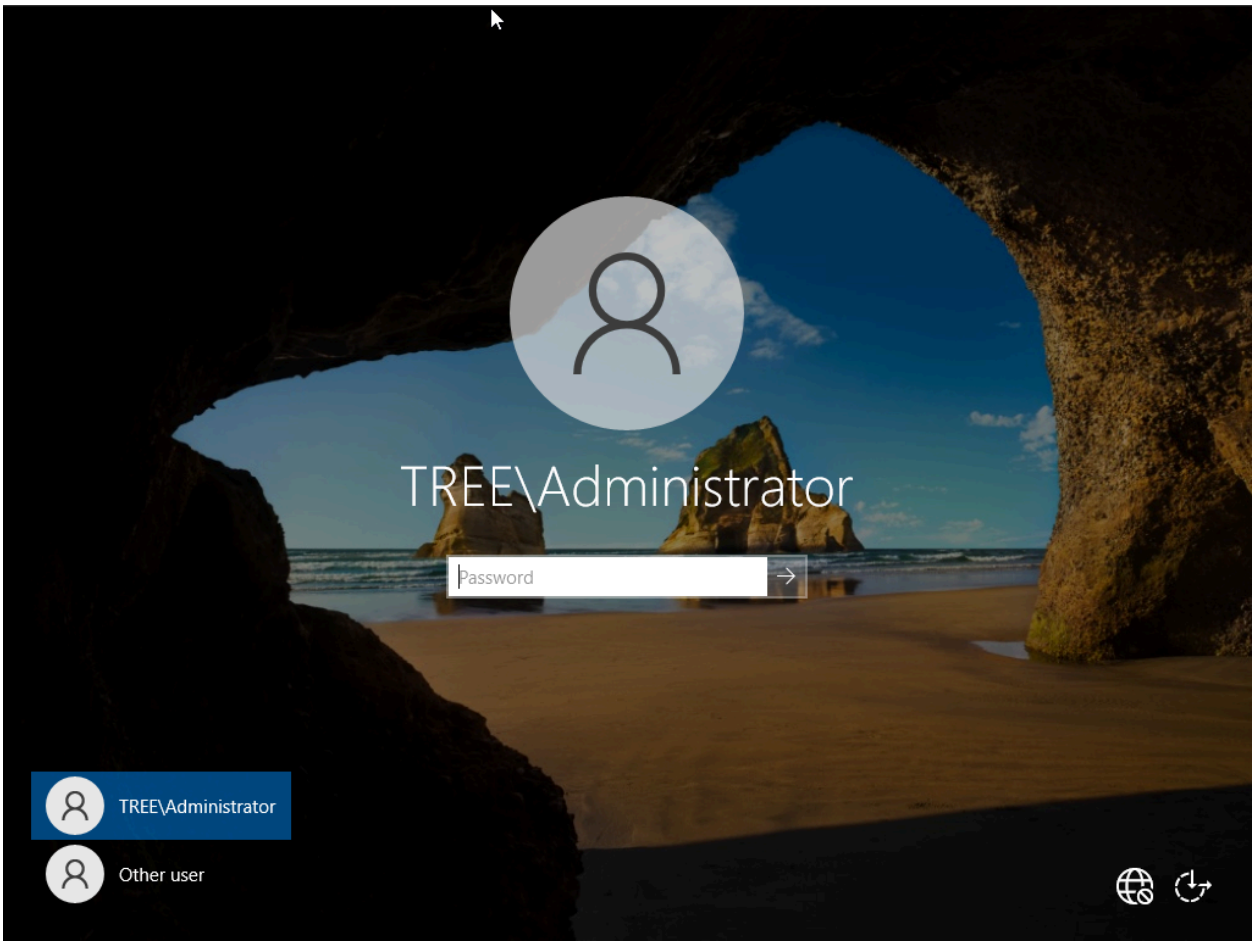

Active Directory Domain Services Configuration Wizard
Additional Options
TARGET SERVER
ADDC-Version1
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Verify the NetBIOS name assigned to the domain and change it if necessary
The NetBIOS domain name:
TREE
More about additional options
< Previous
Next >
Install
Cancel



- This will be the path use to store the database file name ntds.dit.
- FYI love to target DC (Domain Controllers) not only because it has access to everything but also because of ntds.dit since it contains everything related to active directory including password hashes.
- If any unauthorized activity towards ntds.dit, you can assume that your entire domain is unfortunately compromised.

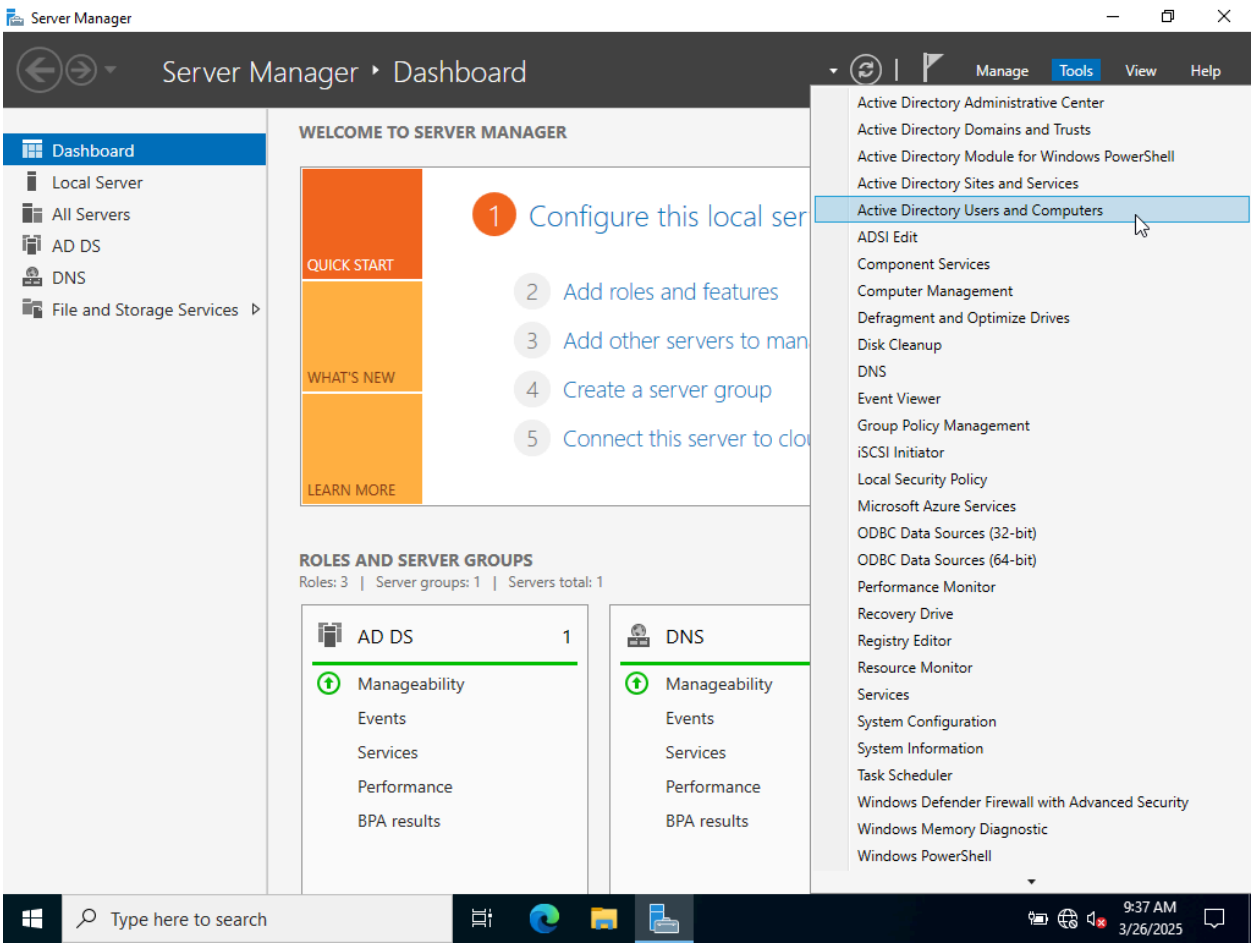


After you see this screen mean that we successfully installed ADDC and promoted our server to DC (Domain Controller):

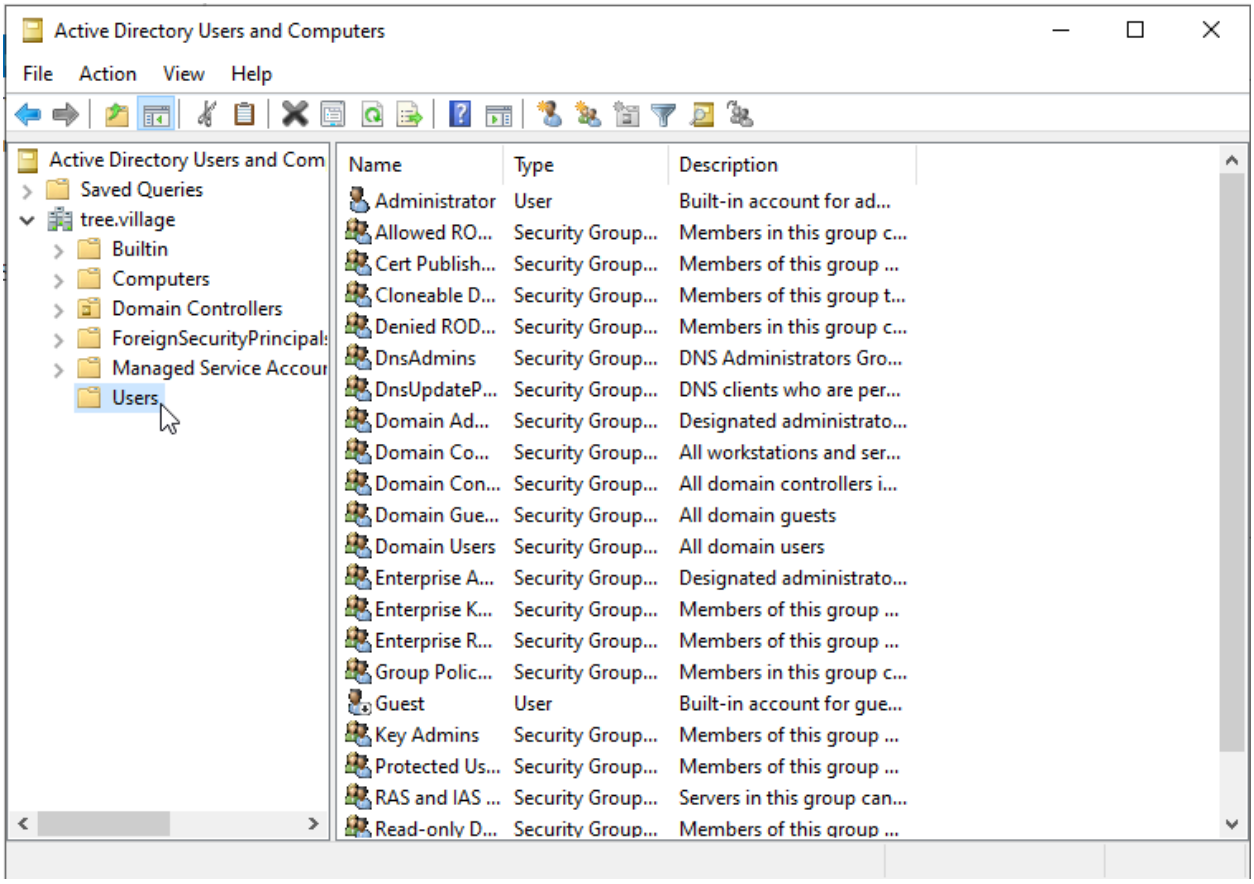


Create Users

Head to Server Manager → Tools → Active Directory Users and Computers

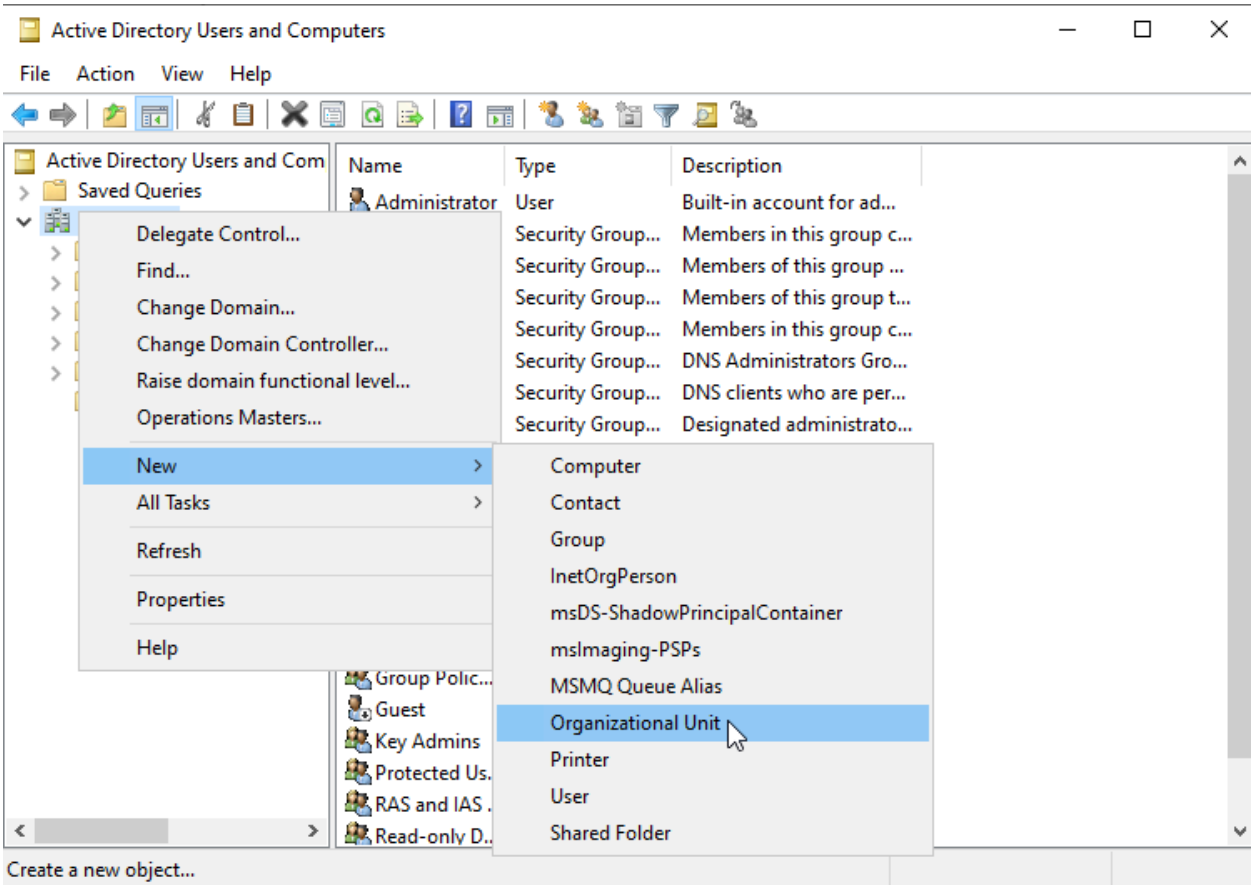


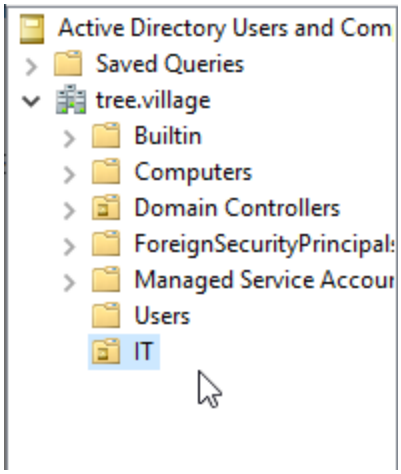
- This is where we can create objects such as User, Computer, Groups,...



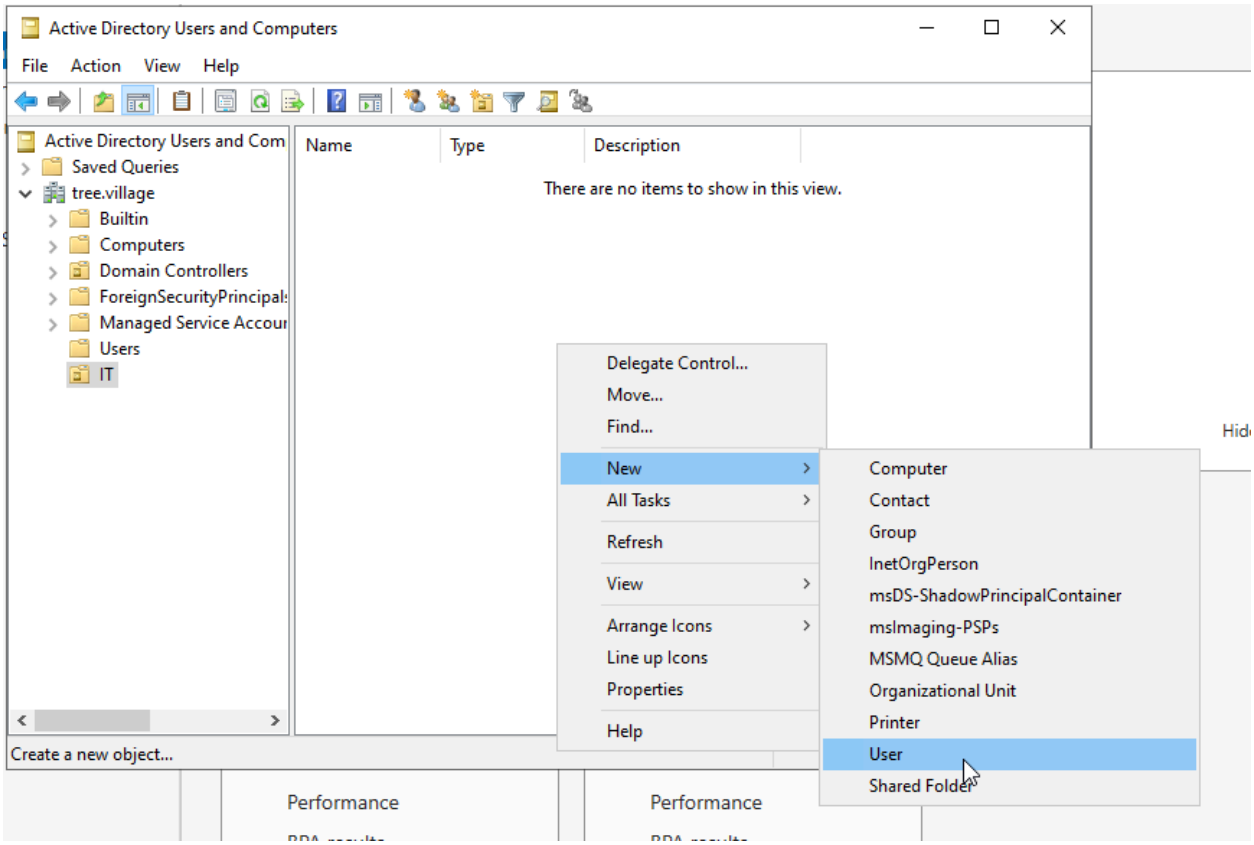
This is where all the prebuilt User in here, now we want to create organizational units since a company usually gonna gave different departments such as HR, IT, Finace,...

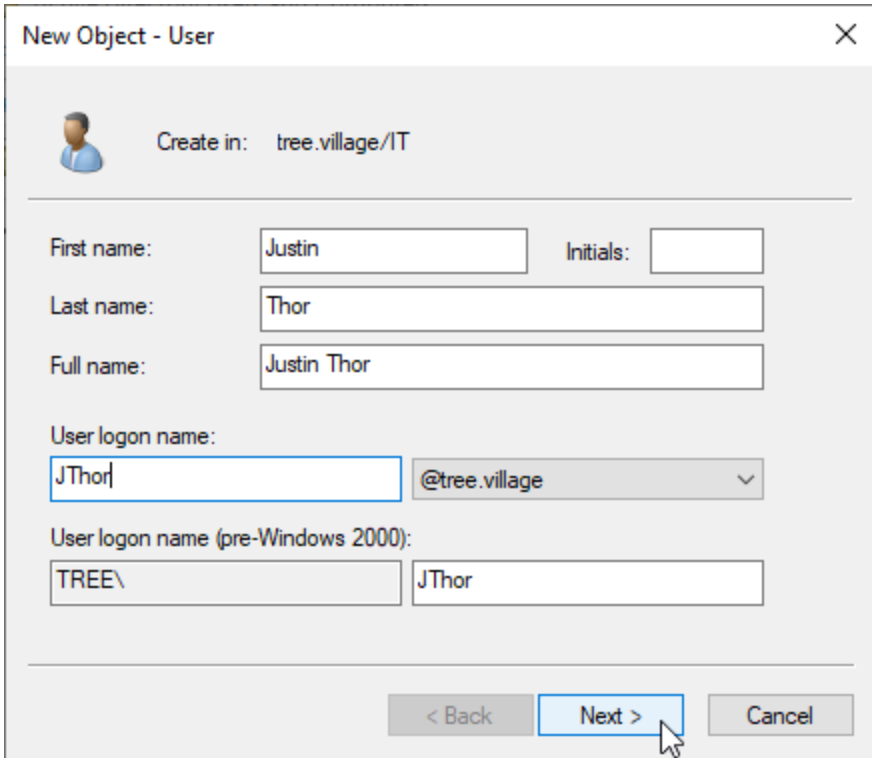
Right click the domain → New → Organizational Unit

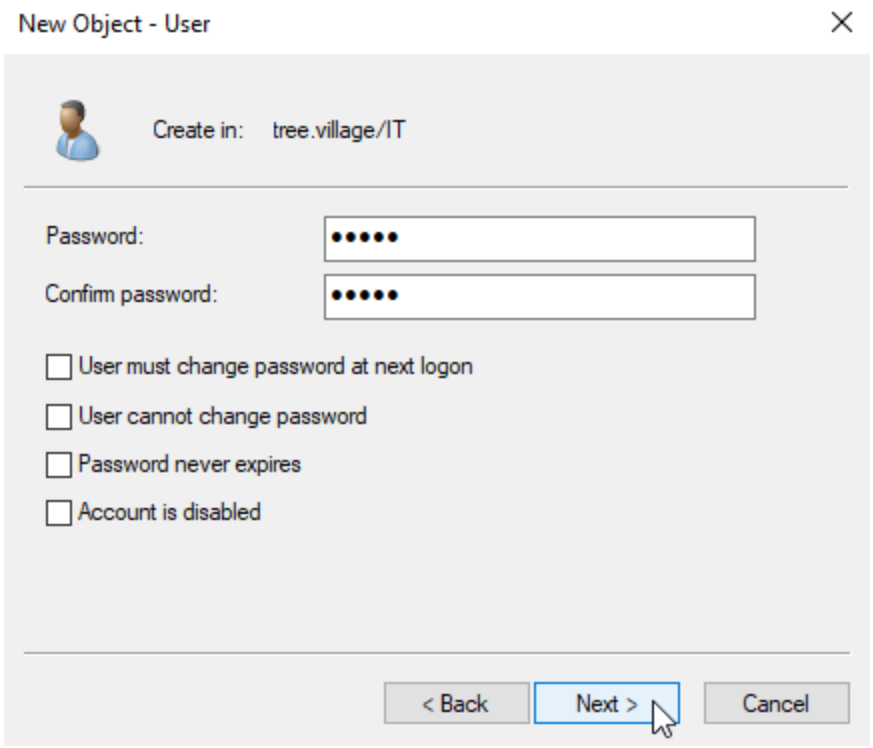




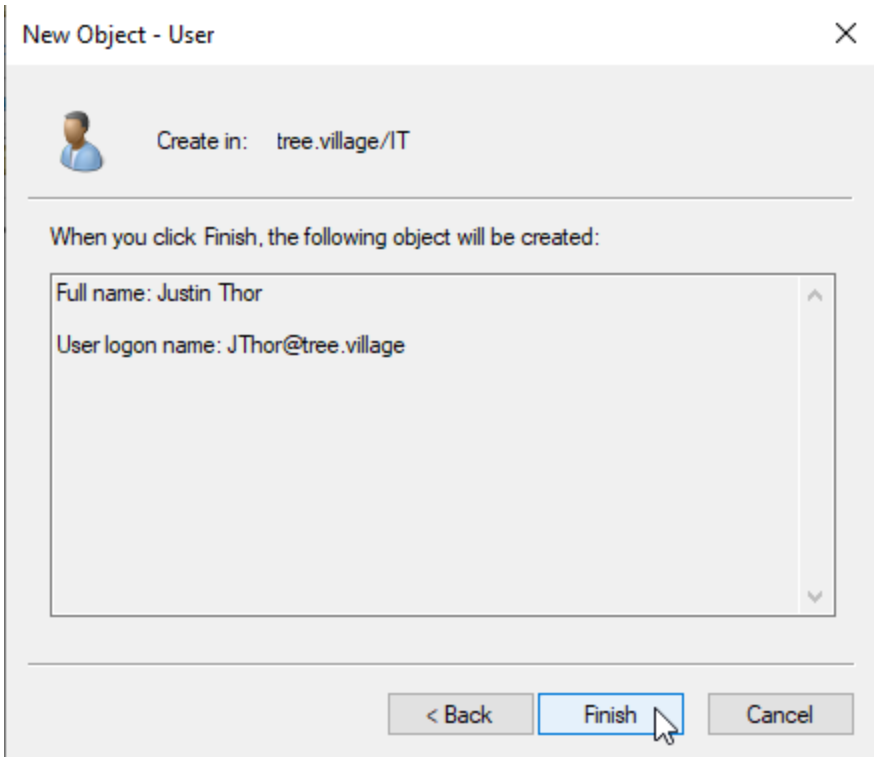
Let create a user:

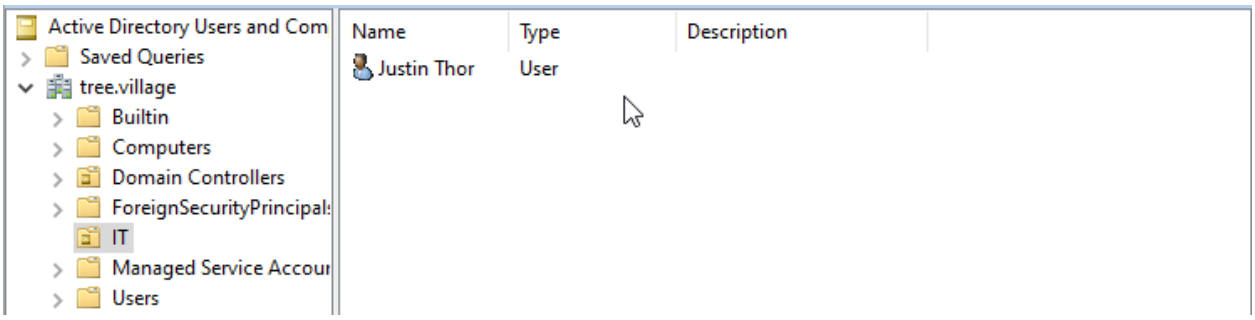

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
tree.village
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
IT
Name
Type
Description
There are no items to show in this view.
Delegate Control...
Move...
Find...
New
All Tasks
Refresh
View
Arrange Icons
Line up Icons
Properties
Help
Computer
Contact
Group
InetOrgPerson
msDS-ShadowPrincipalContainer
msImaging-PSPs
MSMQ Queue Alias
Organizational Unit
Printer
User
Shared Folder
Create a new object...
Performance
Performance


New Object - User
Create in: tree.village/IT
First name:
Justin
Initials:
Last name:
Thor
Full name:
Justin Thor
User logon name:
JThor
@tree.village
User logon name (pre-Windows 2000):
TREE\
JThor
< Back
Next >
Cancel

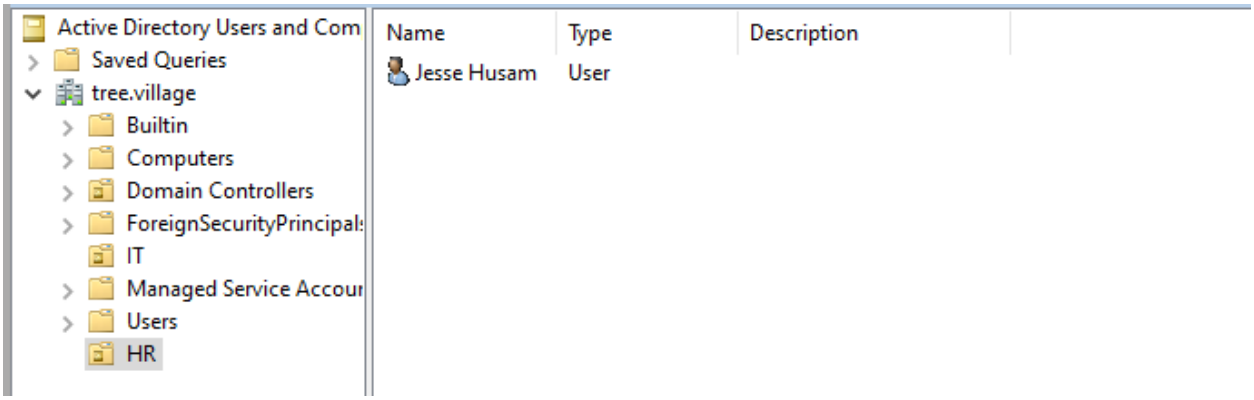


Password: Jaisie123$

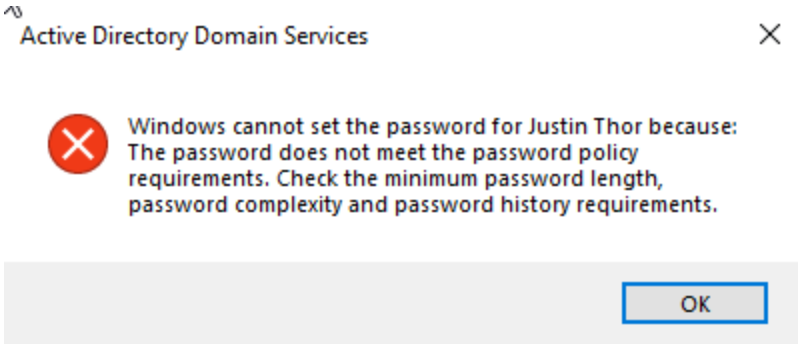


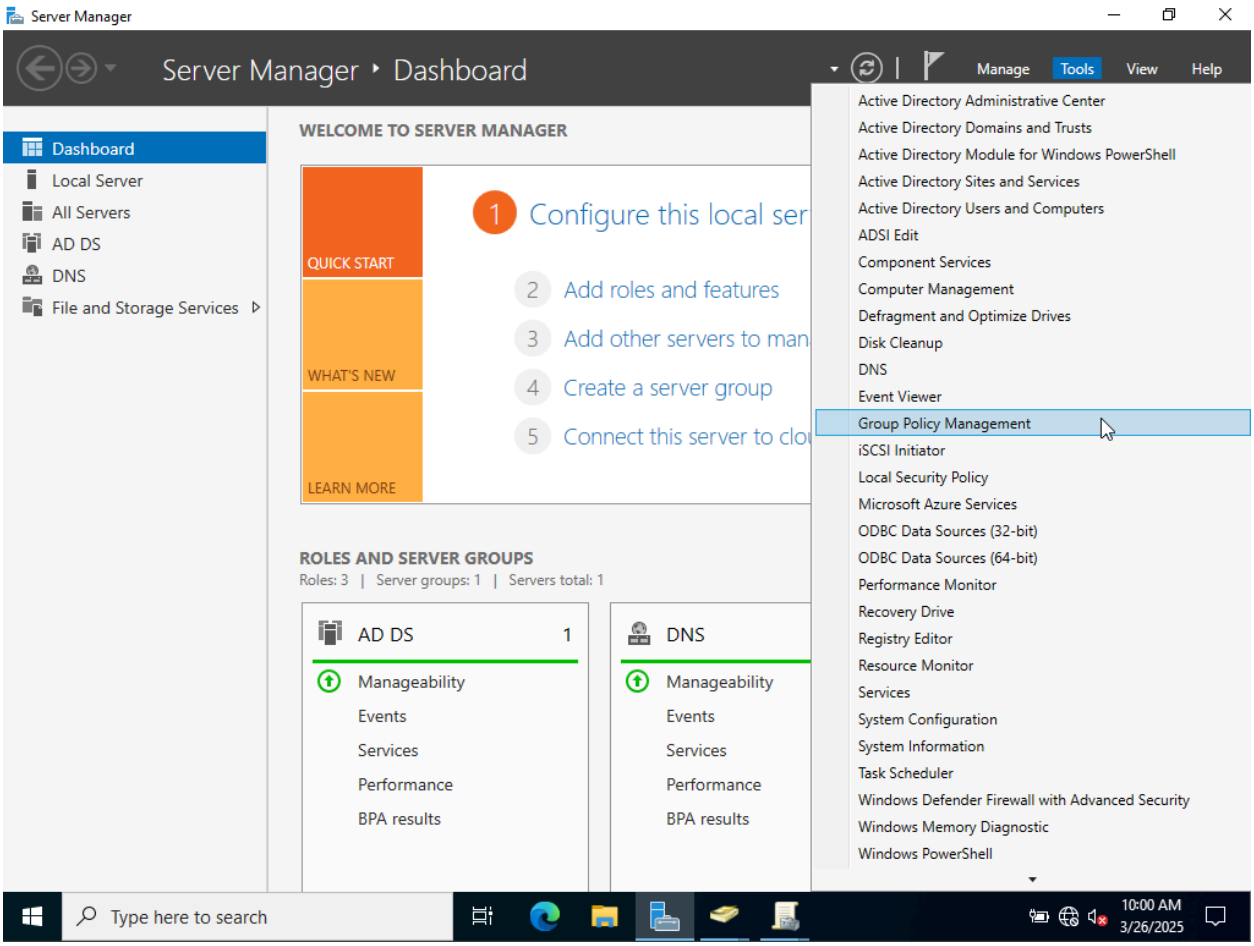


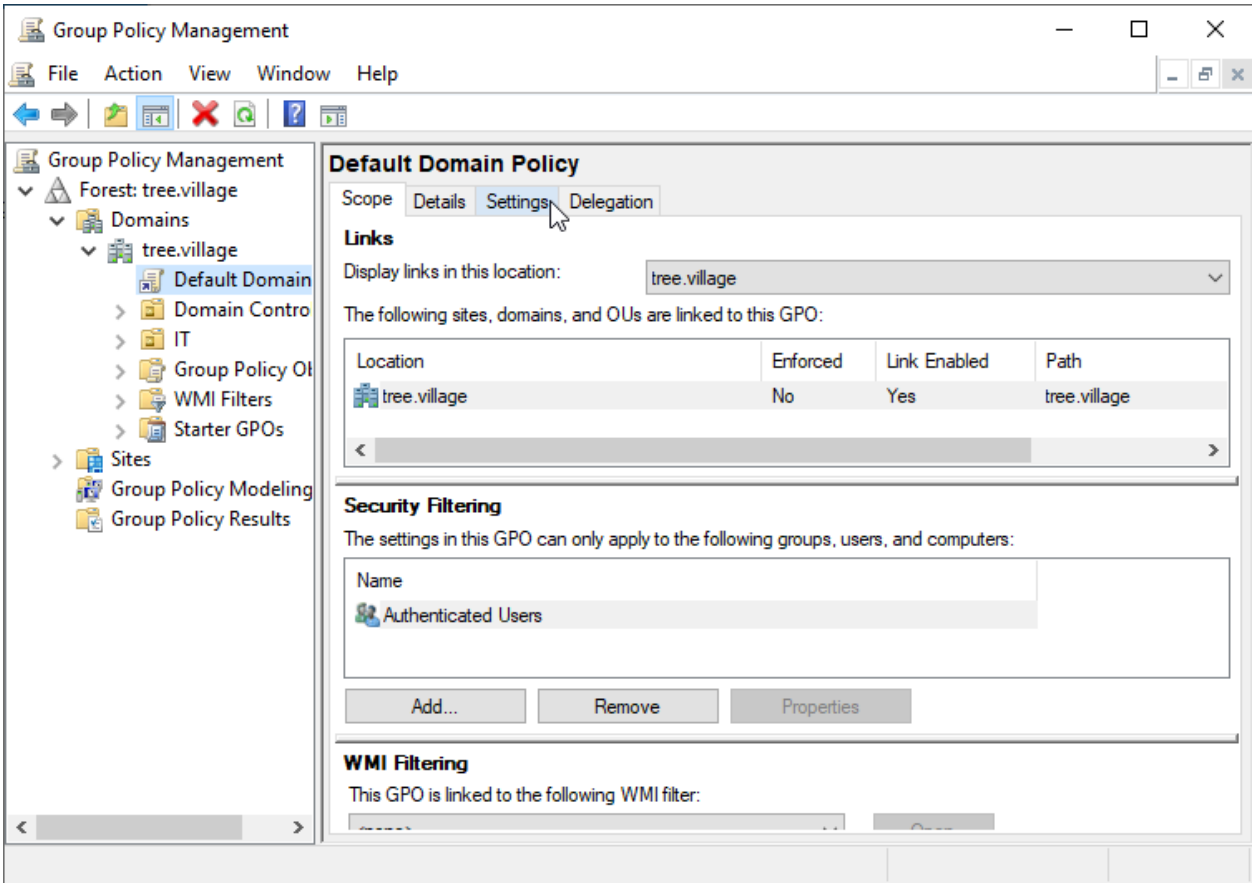
Let create another user under HR department:



BONUS PART:



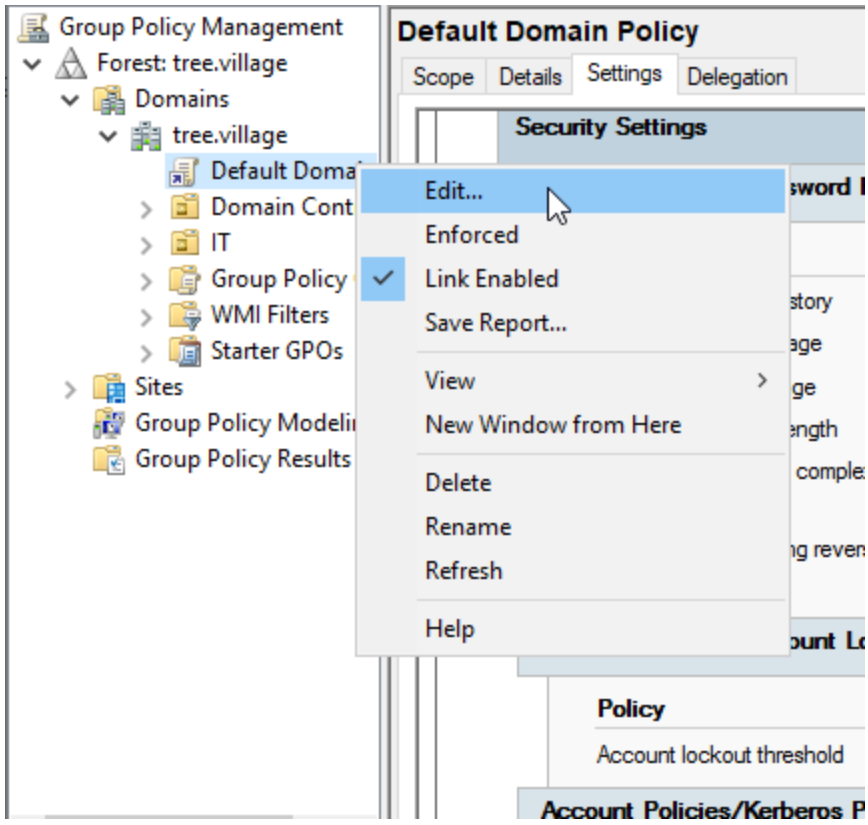

Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local ser
2 Add roles and features
3 Add other servers to man
4 Create a server group
5 Connect this server to clo
ROLES AND SERVER GROUPS
Roles: 3 | Server groups: 1 | Servers total: 1
AD DS 1
Manageability
Events
Services
Performance
BPA results
DNS
Manageability
Events
Services
Performance
BPA results
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Recovery Drive
Registry Editor
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Defender Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Type here to search
10:00 AM
3/26/2025

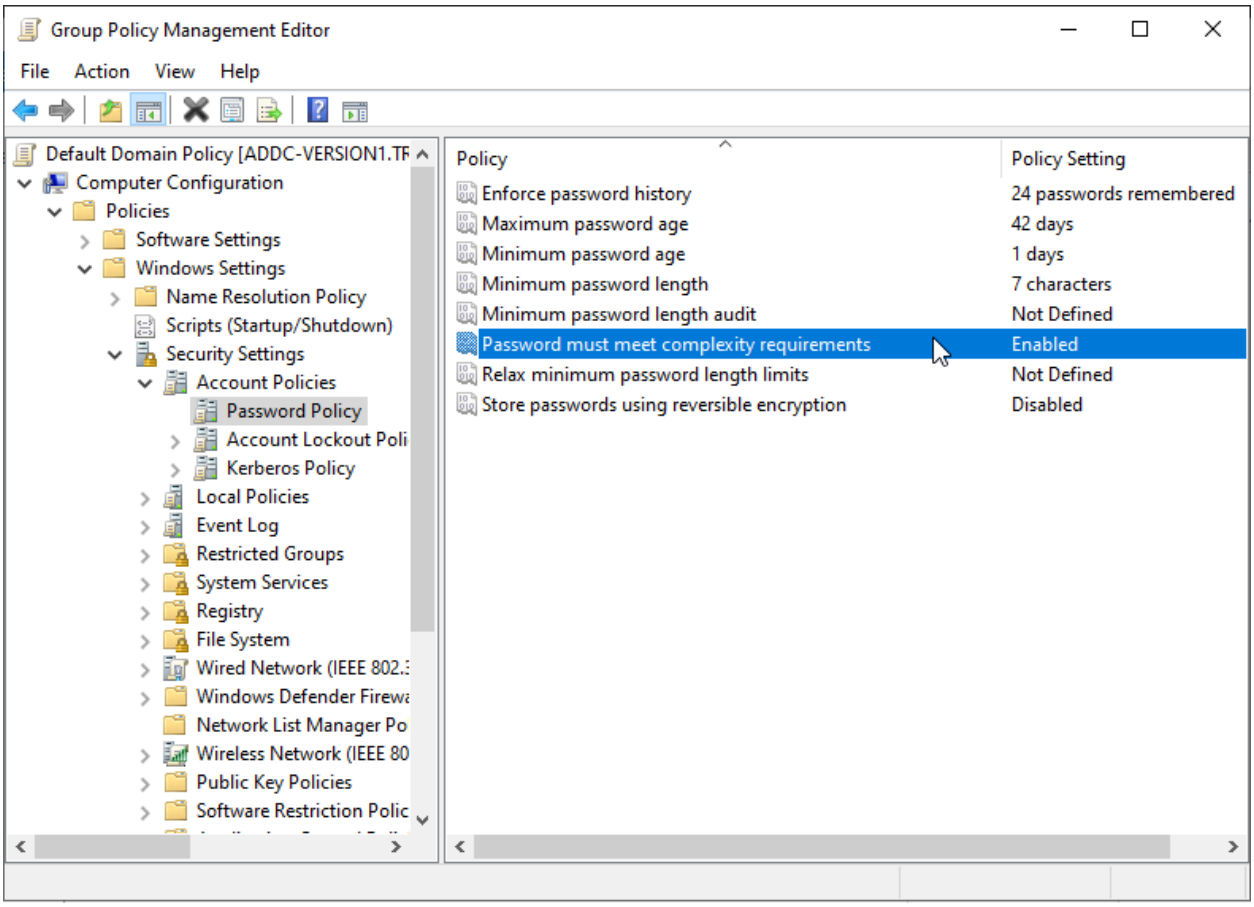


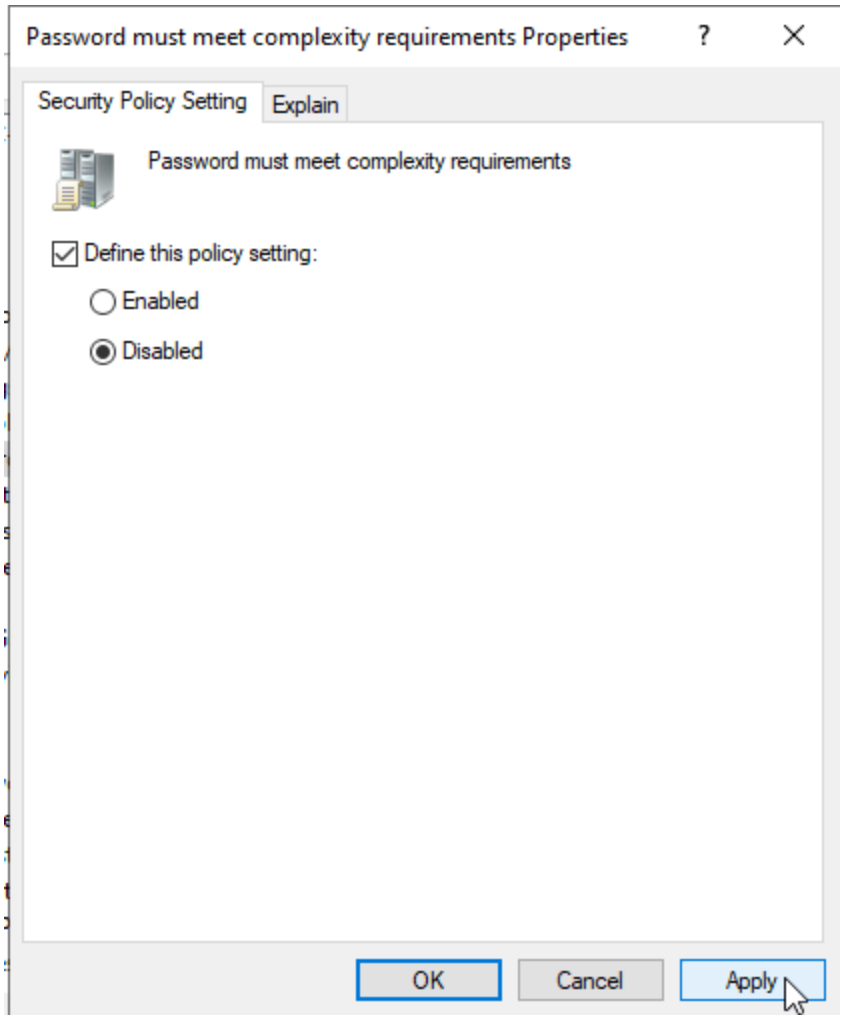
Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled


Group Policy Management
Forest: tree.village
Domains
tree.village
Default Doma
Domain Cont
IT
Group Policy
WMI Filters
Starter GPOs
Sites
Group Policy Modeli
Group Policy Results
Default Domain Policy
Scope
Details
Settings
Delegation
Security Settings
Edit...
Enforced
Link Enabled
Save Report...
View
New Window from Here
Delete
Rename
Refresh
Help
Policy
Account lockout threshold
Account Policies/Kerberos P


Group Policy Management Editor
File Action View Help
Default Domain Policy [ADDC-VERSION1.TF
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Password Policy
Account Lockout Poli
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.
Windows Defender Firewa
Network List Manager Po
Wireless Network (IEEE 80
Public Key Policies
Software Restriction Polic
Policy
Policy Setting
Enforce password history
24 passwords remembered
Maximum password age
42 days
Minimum password age
1 days
Minimum password length
7 characters
Minimum password length audit
Not Defined
Password must meet complexity requirements
Enabled
Relax minimum password length limits
Not Defined
Store passwords using reversible encryption
Disabled



Join Windows 10 VM to ADDC Server VM