Splunk & Sysmon Configuration

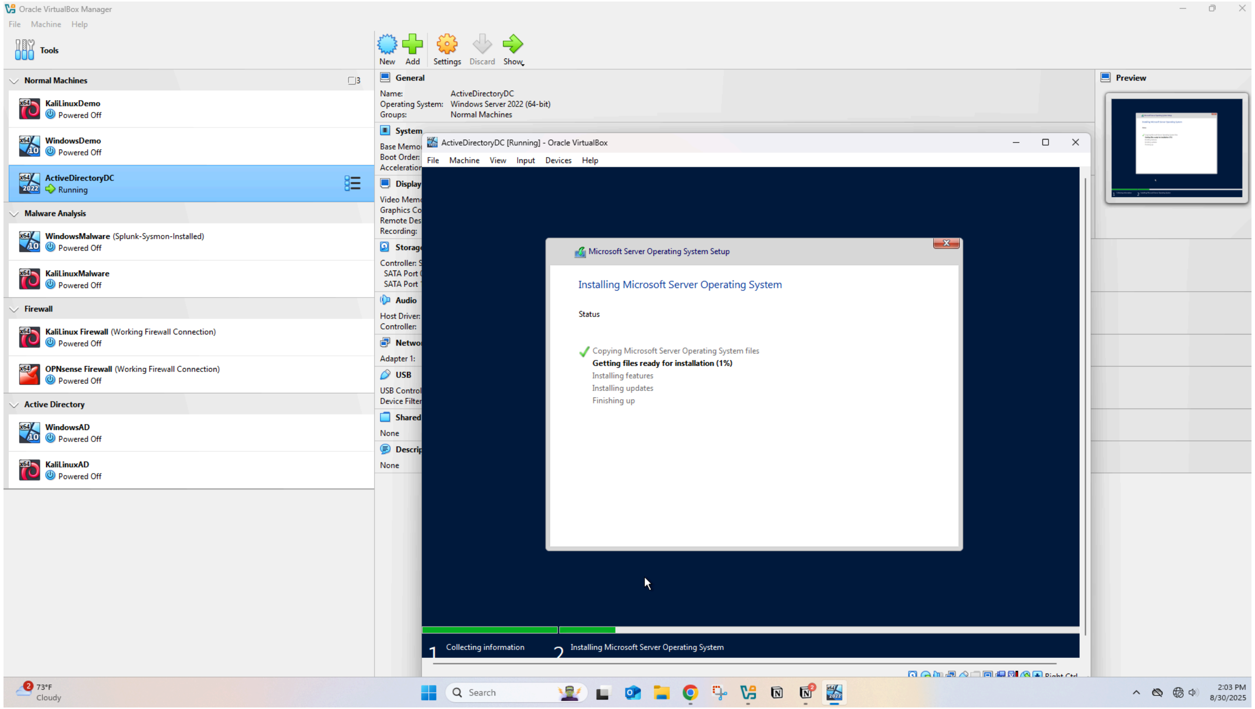
Active Directory - a database that contains users, computers, groups, etc.

Windows Server 2022 Installation

- In order to use active director a server must install a service called active directory domain services (ADDS). The service must be promoted to a Domain Controller (DC) to grant us capability of performing authentication using a protocol called Kerberos and authorization for our domain. All iso files are downloadable online and will be placed into our virtual box machines
- AD DS Objects
  - Users
  - Computer
  - Groups
- The objects will contain attributes (information about the object like metadata)
- ex: **Object**: **User**-Bob , **Atribute** - first name: Bob, last name: Smith

Tools

- Windows 10 (target machine)
- Kali Linux (attacker machine)
- Windows Server 2022 (Active Directory)
- Ubuntu Server (Splunk)
- Virtual Box


Oracle VirtualBox Manager
File Machine Help
Tools
New Add Settings Discard Show
Normal Machines
KaliLinuxDemo Powered Off
WindowsDemo Powered Off
ActiveDirectoryDC Running
Malware Analysis
WindowsMalware (Splunk-Sysmon-Installed) Powered Off
KaliLinuxMalware Powered Off
Firewall
KaliLinux Firewall (Working Firewall Connection) Powered Off
OPNsense Firewall (Working Firewall Connection) Powered Off
Active Directory
WindowsAD Powered Off
KaliLinuxAD Powered Off
Preview
ActiveDirectoryDC [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Microsoft Server Operating System Setup
1 Collecting information
2 Installing Microsoft Server Operating System

General

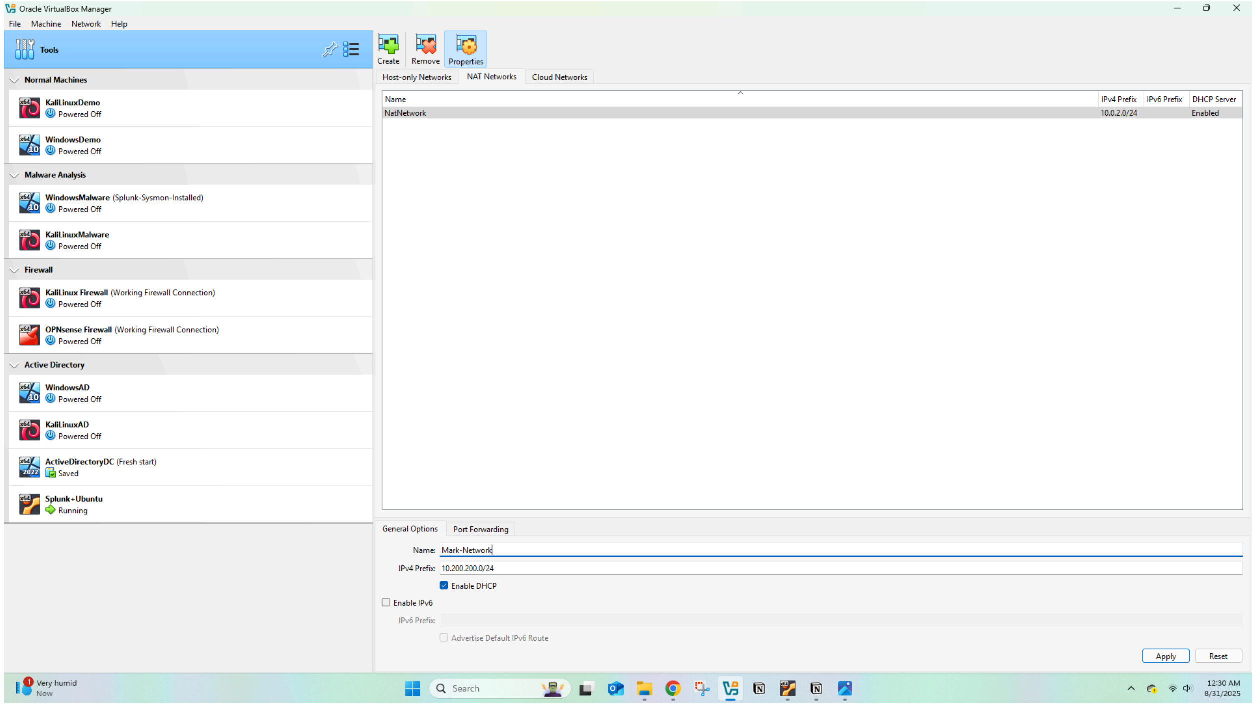
Name: ActiveDirectoryDC
Operating System: Windows Server 2022 (64-bit)
Groups: Normal Machines

Installing Microsoft Server Operating System

Status

✓ Copying Microsoft Server Operating System files
Getting files ready for installation (1%)
Installing features
Installing updates
Finishing up

- After downloading the Windows Server 2022 ISO file I import it into virtual box.
- We will then make sure ubuntu is downloaded and splunk is configured



Normal Machines
- KaliLinuxDemo — Powered Off
- WindowsDemo — Powered Off

Malware Analysis
- WindowsMalware (Splunk-Sysmon-Installed) — Powered Off
- KaliLinuxMalware — Powered Off

Firewall
- KaliLinux Firewall (Working Firewall Connection) — Powered Off
- OPNsense Firewall (Working Firewall Connection) — Powered Off

Active Directory
- WindowsAD — Powered Off
- KaliLinuxAD — Powered Off
- ActiveDirectoryDC (Fresh start) — Saved
- Splunk+Ubuntu — Running

Name	IPv4 Prefix	IPv6 Prefix	DHCP Server
NatNetwork	10.0.2.0/24		Enabled

Name: Mark-Network

IPv4 Prefix: 10.200.200.0/24

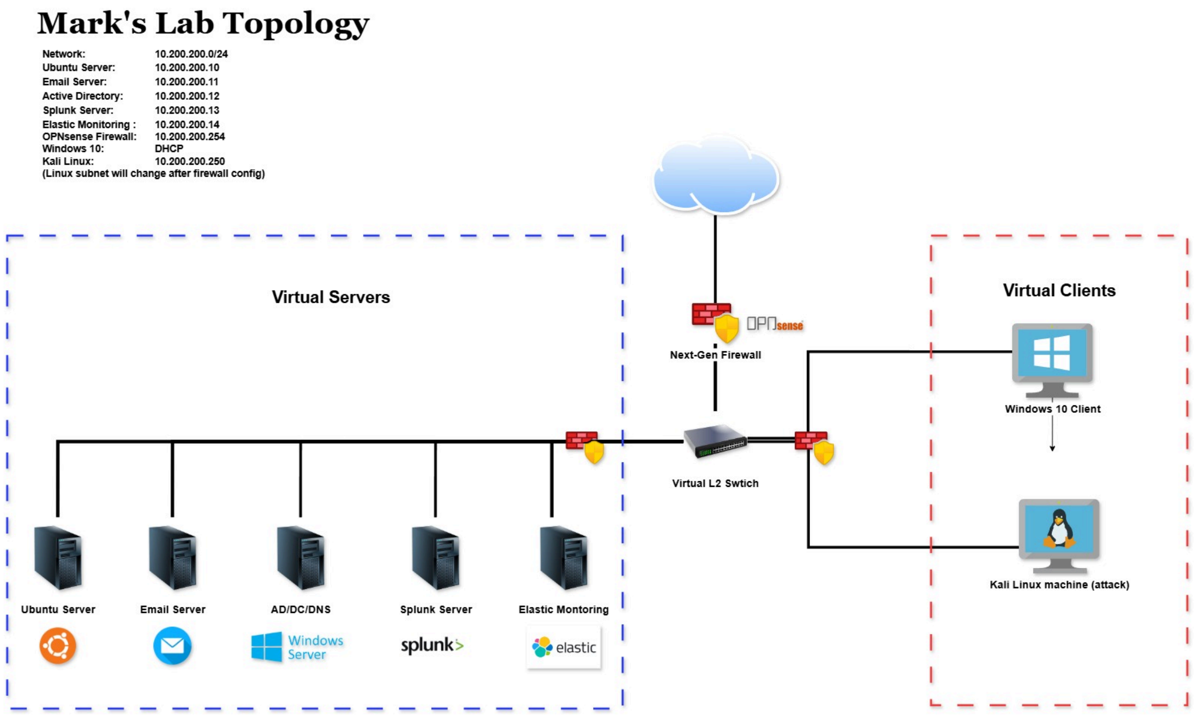
☑ Enable DHCP

☐ Enable IPv6

IPv6 Prefix:

☐ Advertise Default IPv6 Route

- In the screen shot above I am creating a network called Marks-Network where I will house the Active directory VMs and other servers and devices within my lab.
- This is also on my lab topology below

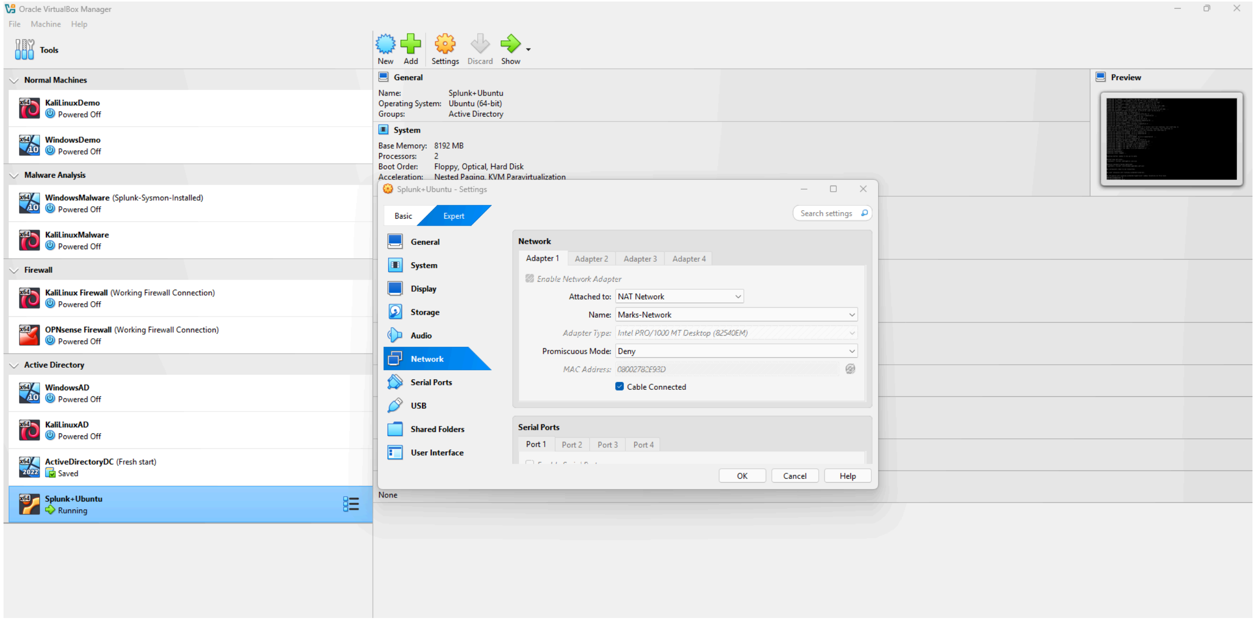


Mark's Lab Topology

Network:	10.200.200.0/24
Ubuntu Server:	10.200.200.10
Email Server:	10.200.200.11
Active Directory:	10.200.200.12
Splunk Server:	10.200.200.13
Elastic Monitoring :	10.200.200.14
OPNsense Firewall:	10.200.200.254
Windows 10:	DHCP
Kali Linux:	10.200.200.250

(Linux subnet will change after firewall config)

For this specific project since its our first time working with AD we are going to choose a different network set up. After this project I will connect everything to follow the lap toplogy above



Normal Machines
- KaliLinuxDemo — Powered Off
- WindowsDemo — Powered Off

Malware Analysis
- WindowsMalware (Splunk-Sysmon-Installed) — Powered Off
- KaliLinuxMalware — Powered Off

Firewall
- KaliLinux Firewall (Working Firewall Connection) — Powered Off
- OPNsense Firewall (Working Firewall Connection) — Powered Off

Active Directory
- WindowsAD — Powered Off
- KaliLinuxAD — Powered Off
- ActiveDirectoryDC (Fresh start) — Saved
- Splunk+Ubuntu — Running

General
Name: Splunk+Ubuntu
Operating System: Ubuntu (64-bit)
Groups: Active Directory

System
Base Memory: 8192 MB
Processors: 2
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Splunk+Ubuntu - Settings

General | System | Display | Storage | Audio | **Network** | Serial Ports | USB | Shared Folders | User Interface

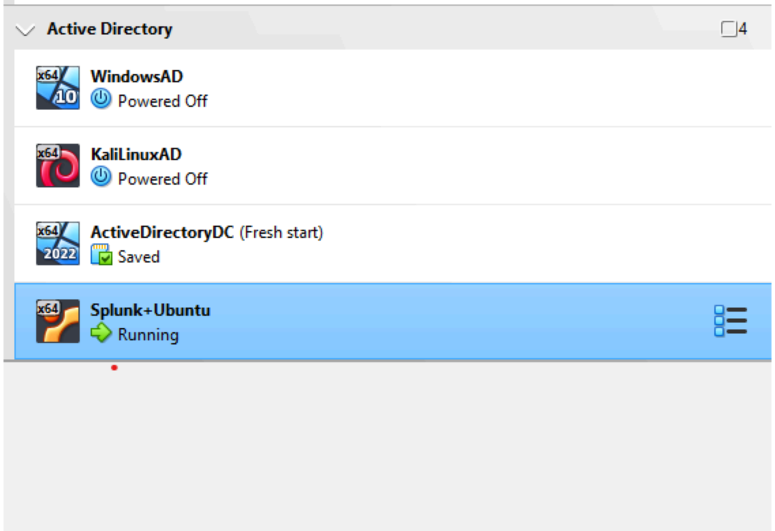
Network
Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter
Attached to: NAT Network
Name: Marks-Network
Adapter Type: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Deny
MAC Address: 08002782E93D
☑ Cable Connected

Serial Ports
Port 1 | Port 2 | Port 3 | Port 4

None

- We will be using a NAT network type for this project which means all the devices including the host machine are on the same network and can communicate to eachother.



Active Directory 4

WindowsAD
Powered Off

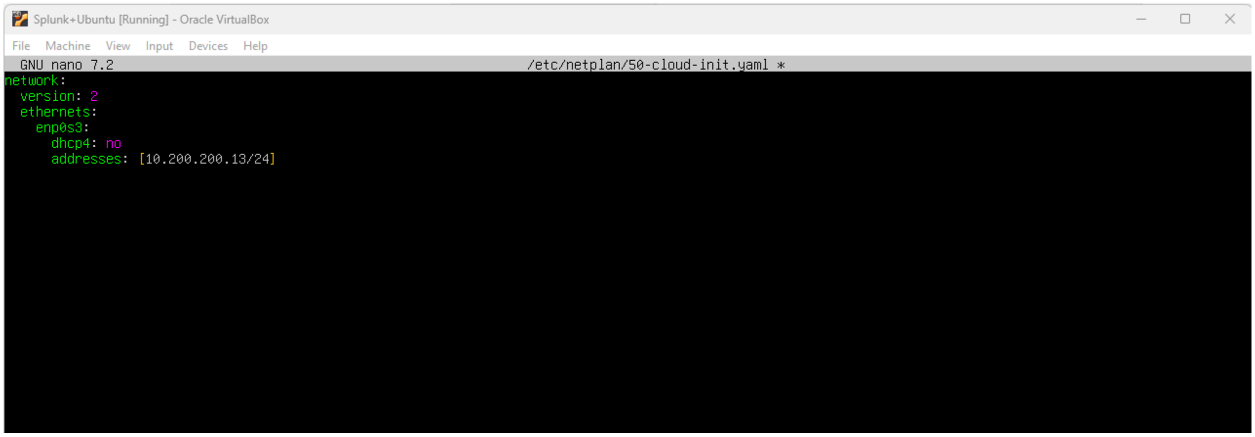
KaliLinuxAD
Powered Off

ActiveDirectoryDC (Fresh start)
Saved

Splunk+Ubuntu
Running

- For this project we will just work with just Active directory, splunk and ubuntu, I only use the VMs I have set up specifically for AD which is in the screenshot above. I will later link the networks to create the original lab topolgoy.
- All of these VMs for now will be set on the NAT network

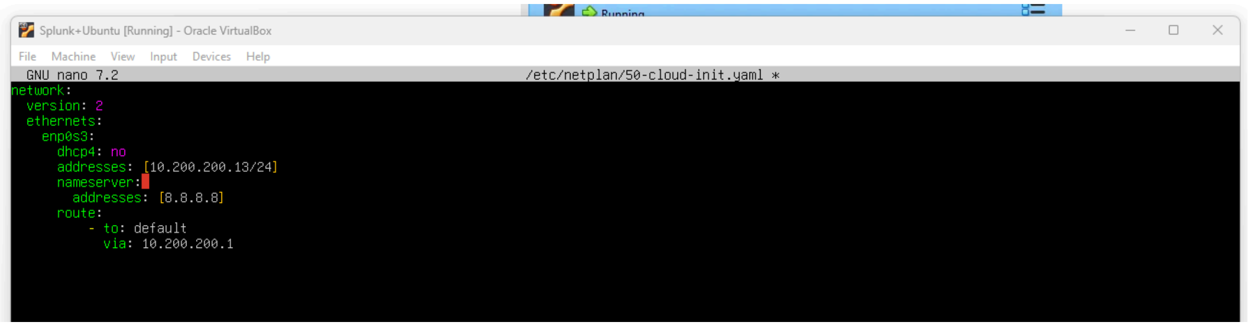
Now in my splunk+ubuntu virtual machine I will create my static IP address which was listed in the lab toplogy.



```
  GNU nano 7.2                                      /etc/netplan/50-cloud-init.yaml *
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [10.200.200.13/24]
```

- Using: sudo nano /etc/netplan/50-cloud-int.yaml
- Allowed me to get into this file and change dhcp4 from no to yes and adding an address section with my new static ip address , in order to change the

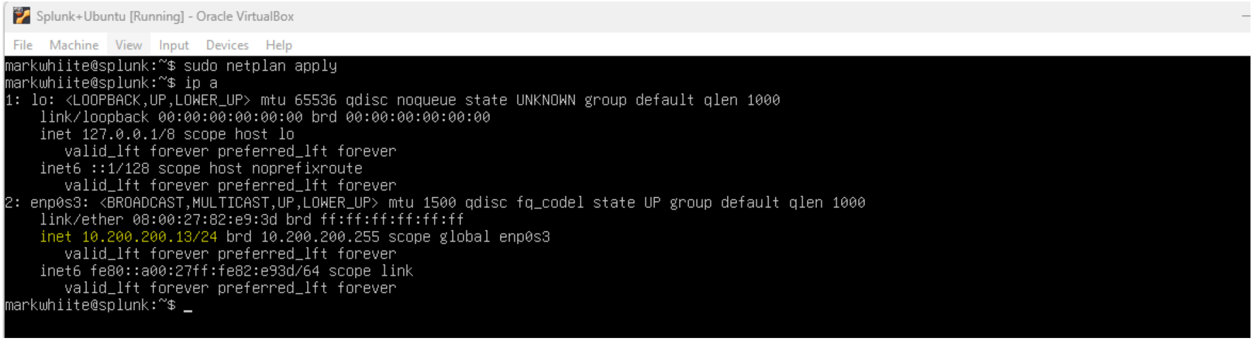
originial ip address that was given



Running
Splunk+Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help

```
 GNU nano 7.2                                  /etc/netplan/50-cloud-init.yaml *
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [10.200.200.13/24]
      nameserver:
        addresses: [8.8.8.8]
      route:
          - to: default
            via: 10.200.200.1
```

- In the image above I am also adding the DNS ip [8.8.8.8] and the gateway 10.200.200.1



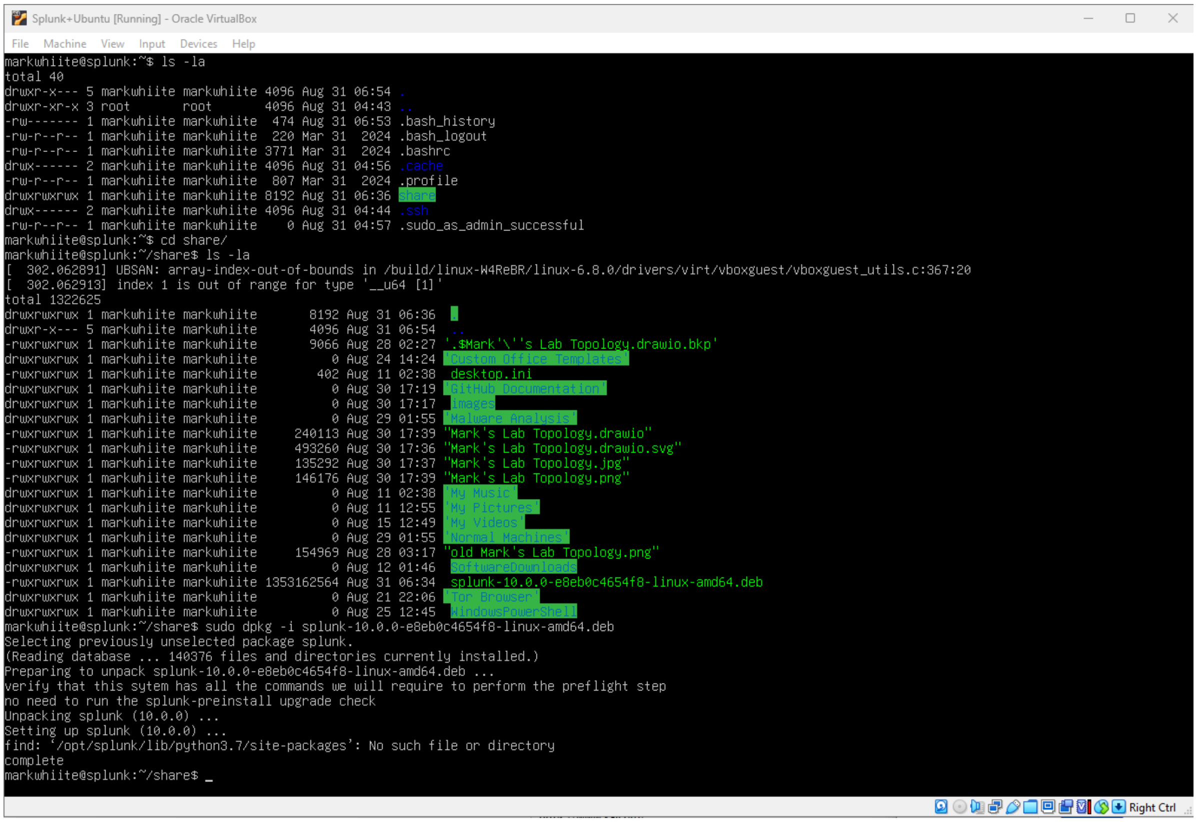
Splunk+Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help

```
markwhiite@splunk:~$ sudo netplan apply
markwhiite@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 noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:82:e9:3d brd ff:ff:ff:ff:ff:ff
    inet 10.200.200.13/24 brd 10.200.200.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe82:e93d/64 scope link
       valid_lft forever preferred_lft forever
markwhiite@splunk:~$ _
```

- I now see my IP address for splunk as updated (which I highlighted in yellow)

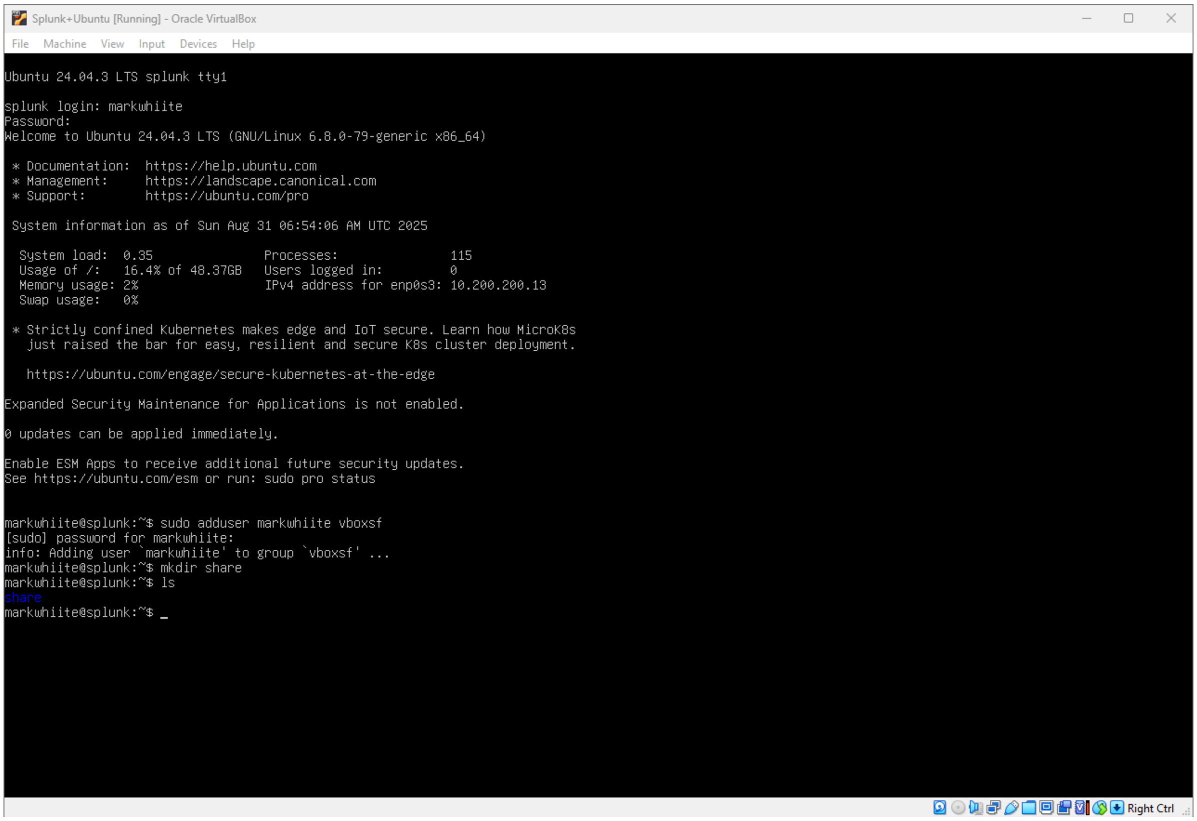
Now at this point I can actually install Splunk

- I will download splunk enterprise, deb file from their website.


Splunk+Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Right Ctrl

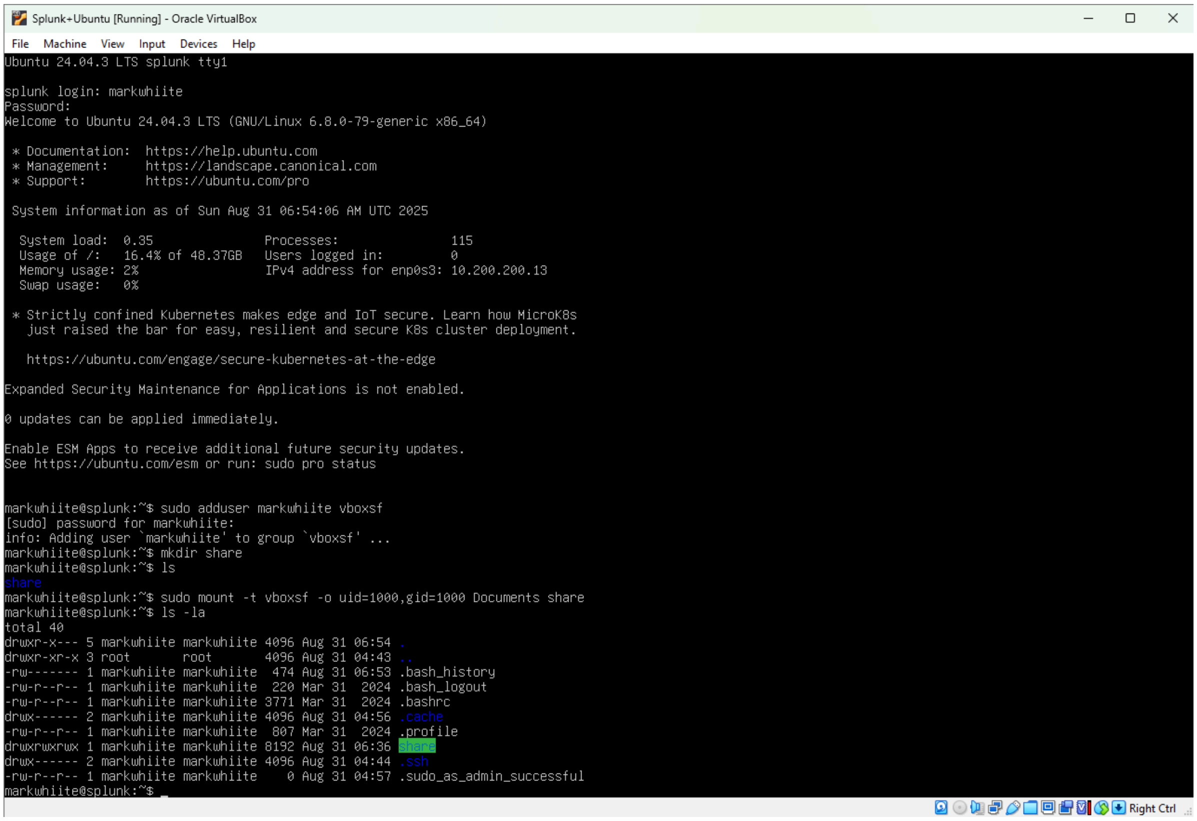
```
markwhiite@splunk:~$ ls -la
total 40
drwxr-x--- 5 markwhiite markwhiite 4096 Aug 31 06:54 .
drwxr-xr-x 3 root       root       4096 Aug 31 04:43 ..
-rw------- 1 markwhiite markwhiite  474 Aug 31 06:53 .bash_history
-rw-r--r-- 1 markwhiite markwhiite  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 markwhiite markwhiite 3771 Mar 31  2024 .bashrc
drwx------ 2 markwhiite markwhiite 4096 Aug 31 04:56 .cache
-rw-r--r-- 1 markwhiite markwhiite  807 Mar 31  2024 .profile
drwxrwxrwx 1 markwhiite markwhiite 8192 Aug 31 06:36 share
drwx------ 2 markwhiite markwhiite 4096 Aug 31 04:44 .ssh
-rw-r--r-- 1 markwhiite markwhiite    0 Aug 31 04:57 .sudo_as_admin_successful
markwhiite@splunk:~$ cd share/
markwhiite@splunk:~/share$ ls -la
[  302.062891] UBSAN: array-index-out-of-bounds in /build/linux-W4ReBR/linux-6.8.0/drivers/virt/vboxguest/vboxguest_utils.c:367:20
[  302.062913] index 1 is out of range for type '__u64 [1]'
total 1322625
drwxrwxrwx 1 markwhiite markwhiite       8192 Aug 31 06:36  .
drwxr-x--- 5 markwhiite markwhiite       4096 Aug 31 06:54  ..
-rwxrwxrwx 1 markwhiite markwhiite       9066 Aug 28 02:27 '.$Mark'\''s Lab Topology.drawio.bkp'
drwxrwxrwx 1 markwhiite markwhiite          0 Aug 24 14:24 'Custom Office Templates'
-rwxrwxrwx 1 markwhiite markwhiite        402 Aug 11 02:38  desktop.ini
drwxrwxrwx 1 markwhiite markwhiite          0 Aug 30 17:19 'GitHub Documentation'
drwxrwxrwx 1 markwhiite markwhiite          0 Aug 30 17:17  images
drwxrwxrwx 1 markwhiite markwhiite          0 Aug 29 01:55 'Malware Analysis'
-rwxrwxrwx 1 markwhiite markwhiite     240113 Aug 30 17:39 "Mark's Lab Topology.drawio"
-rwxrwxrwx 1 markwhiite markwhiite     493260 Aug 30 17:36 "Mark's Lab Topology.drawio.svg"
-rwxrwxrwx 1 markwhiite markwhiite     135292 Aug 30 17:37 "Mark's Lab Topology.jpg"
-rwxrwxrwx 1 markwhiite markwhiite     146176 Aug 30 17:39 "Mark's Lab Topology.png"
drwxrwxrwx 1 markwhiite markwhiite          0 Aug 11 02:38 'My Music'
drwxrwxrwx 1 markwhiite markwhiite          0 Aug 11 12:55 'My Pictures'
drwxrwxrwx 1 markwhiite markwhiite          0 Aug 15 12:49 'My Videos'
drwxrwxrwx 1 markwhiite markwhiite          0 Aug 29 01:55 'Normal Machines'
-rwxrwxrwx 1 markwhiite markwhiite     154969 Aug 28 03:17 "old Mark's Lab Topology.png"
drwxrwxrwx 1 markwhiite markwhiite          0 Aug 12 01:46  SoftwareDownloads
-rwxrwxrwx 1 markwhiite markwhiite 1353162564 Aug 31 06:34  splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb
drwxrwxrwx 1 markwhiite markwhiite          0 Aug 21 22:06 'Tor Browser'
drwxrwxrwx 1 markwhiite markwhiite          0 Aug 25 12:45  WindowsPowerShell
markwhiite@splunk:~/share$ sudo dpkg -i splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 140376 files and directories currently installed.)
Preparing to unpack splunk-10.0.0-e8eb0c4654f8-linux-amd64.deb ...
verify that this sytem has all the commands we will require to perform the preflight step
no need to run the splunk-preinstall upgrade check
Unpacking splunk (10.0.0) ...
Setting up splunk (10.0.0) ...
find: '/opt/splunk/lib/python3.7/site-packages': No such file or directory
complete
markwhiite@splunk:~/share$ _
```

- In the image above I am searching through my file directory using ubuntu (CLI version) to open the installation file



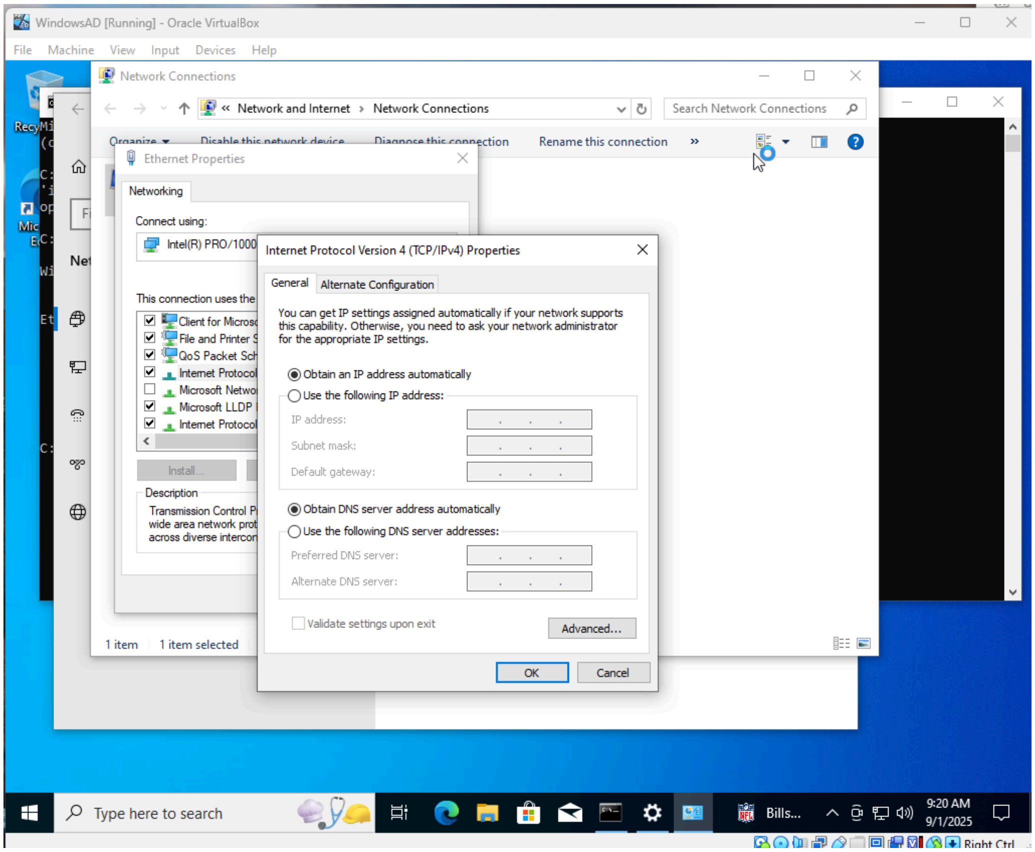
```
Ubuntu 24.04.3 LTS splunk tty1

splunk login: markwhiite
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-79-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun Aug 31 06:54:06 AM UTC 2025

  System load:  0.35               Processes:               115
  Usage of /:   16.4% of 48.37GB   Users logged in:         0
  Memory usage: 2%                 IPv4 address for enp0s3: 10.200.200.13
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


markwhiite@splunk:~$ sudo adduser markwhiite vboxsf
[sudo] password for markwhiite:
info: Adding user `markwhiite' to group `vboxsf' ...
markwhiite@splunk:~$ mkdir share
markwhiite@splunk:~$ ls
share
markwhiite@splunk:~$ _
```

- In this image I am adding necessary users and directories to install splunk


Splunk+Ubuntu [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Right Ctrl

```
Ubuntu 24.04.3 LTS splunk tty1

splunk login: markwhiite
Password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.8.0-79-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun Aug 31 06:54:06 AM UTC 2025

  System load:  0.35               Processes:               115
  Usage of /:   16.4% of 48.37GB   Users logged in:         0
  Memory usage: 2%                 IPv4 address for enp0s3: 10.200.200.13
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


markwhiite@splunk:~$ sudo adduser markwhiite vboxsf
[sudo] password for markwhiite:
info: Adding user `markwhiite' to group `vboxsf' ...
markwhiite@splunk:~$ mkdir share
markwhiite@splunk:~$ ls
share
markwhiite@splunk:~$ sudo mount -t vboxsf -o uid=1000,gid=1000 Documents share
markwhiite@splunk:~$ ls -la
total 40
drwxr-x--- 5 markwhiite markwhiite 4096 Aug 31 06:54 .
drwxr-xr-x 3 root       root       4096 Aug 31 04:43 ..
-rw------- 1 markwhiite markwhiite  474 Aug 31 06:53 .bash_history
-rw-r--r-- 1 markwhiite markwhiite  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 markwhiite markwhiite 3771 Mar 31  2024 .bashrc
drwx------ 2 markwhiite markwhiite 4096 Aug 31 04:56 .cache
-rw-r--r-- 1 markwhiite markwhiite  807 Mar 31  2024 .profile
drwxrwxrwx 1 markwhiite markwhiite 8192 Aug 31 06:36 share
drwx------ 2 markwhiite markwhiite 4096 Aug 31 04:44 .ssh
-rw-r--r-- 1 markwhiite markwhiite    0 Aug 31 04:57 .sudo_as_admin_successful
markwhiite@splunk:~$ _
```

- After we have splunk up and running we will install splunk universal forwader and sysmon on the target machine and server



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

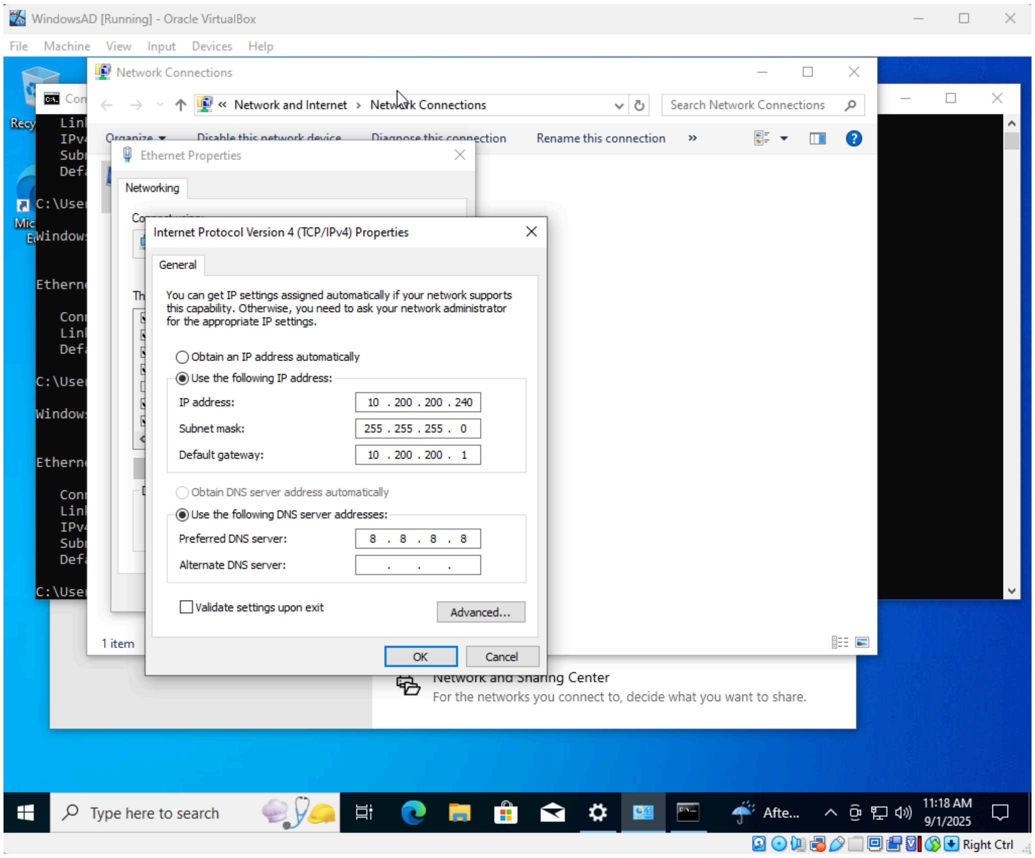
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

- I will then open up my Windows (target machine) and make sure the IP address is set to what I have created in my lab topology.


WindowsAD [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Network Connections
« Network and Internet › Network Connections
Search Network Connections
Organize ▾ Disable this network device Diagnose this connection Rename this connection »
Ethernet Properties
Networking
1 item
Network and Sharing Center
For the networks you connect to, decide what you want to share.
Type here to search
Afte...
11:18 AM
9/1/2025
Right Ctrl

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 10 . 200 . 200 . 240
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 200 . 200 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8
Alternate DNS server: . . .

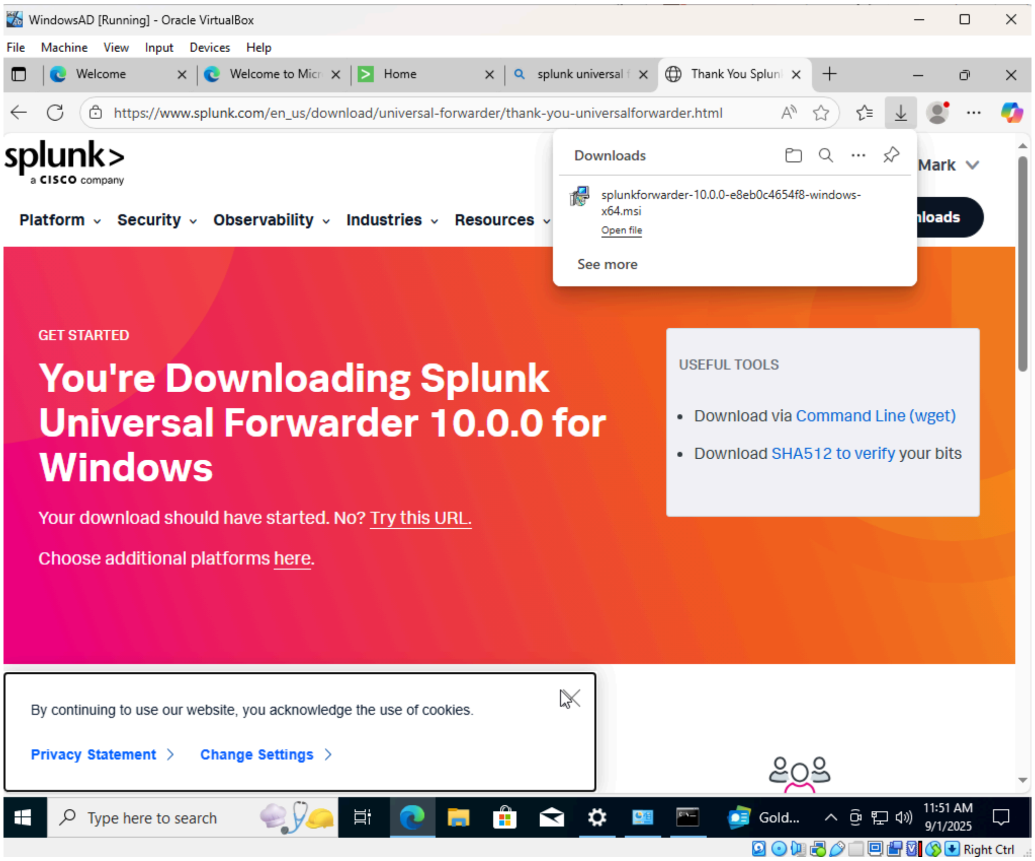
□ Validate settings upon exit

Advanced...

OK Cancel

Once my windows, windows server 2022, and Splunk IP addresses are configured correctly I can continue.

I will next install Splunk universal forwarder, which helps Splunk collect necessary logs and other data. Along with Sysmon, a windows system service and driver mainly used for monitoring and detailed event logs



WindowsAD [Running] - Oracle VirtualBox

https://www.splunk.com/en_us/download/universal-forwarder/thank-you-universalforwarder.html

Downloads

splunkforwarder-10.0.0-e8eb0c4654f8-windows-x64.msi

Open file

See more

GET STARTED

You're Downloading Splunk Universal Forwarder 10.0.0 for Windows

Your download should have started. No? Try this URL.

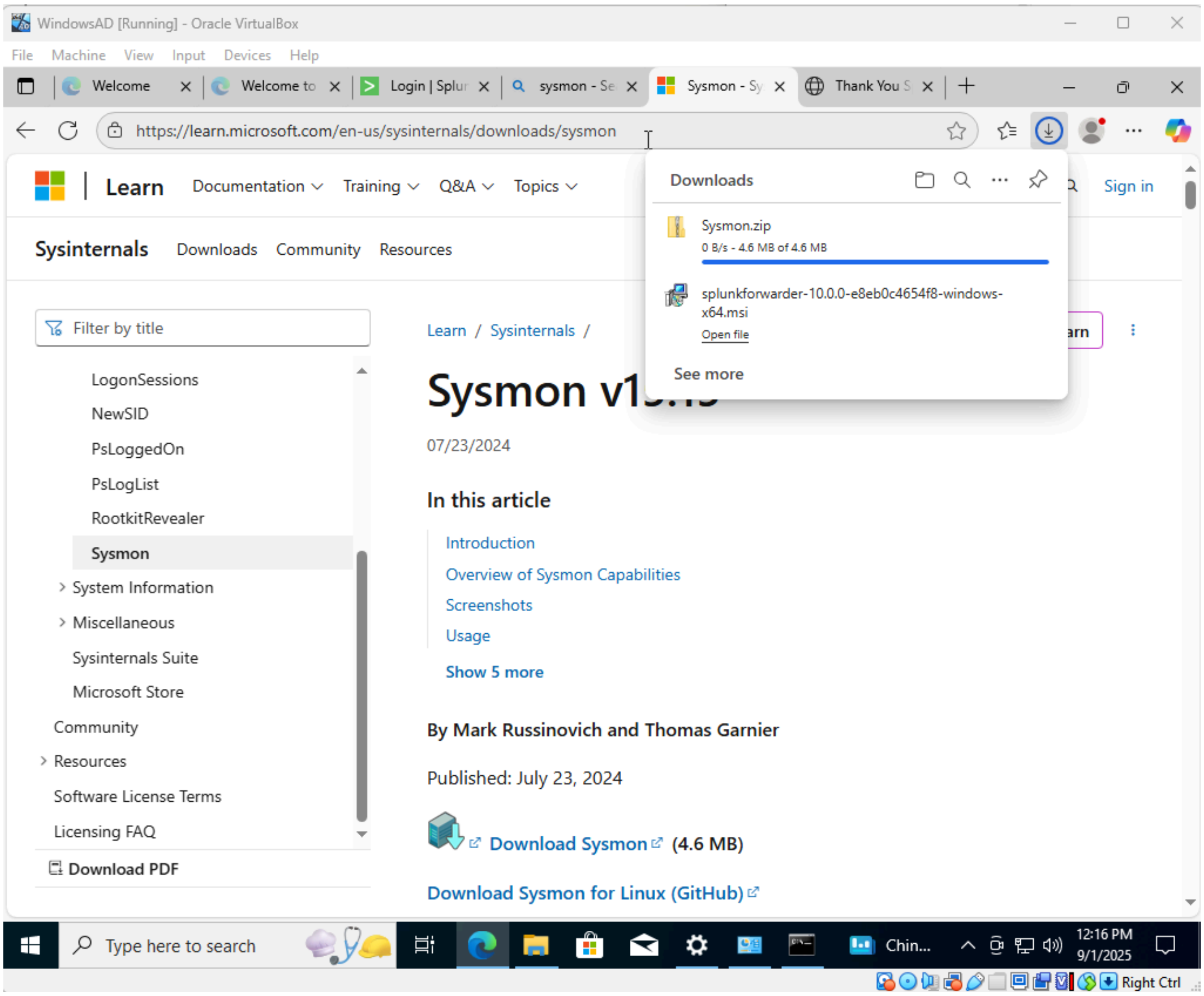
Choose additional platforms here.

USEFUL TOOLS

- Download via Command Line (wget)
- Download SHA512 to verify your bits

By continuing to use our website, you acknowledge the use of cookies.

Privacy Statement > Change Settings >



https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

Downloads

Sysmon.zip
0 B/s - 4.6 MB of 4.6 MB

splunkforwarder-10.0.0-e8eb0c4654f8-windows-x64.msi
Open file

See more

- LogonSessions
- NewSID
- PsLoggedOn
- PsLogList
- RootkitRevealer
- Sysmon
- System Information
- Miscellaneous
- Sysinternals Suite
- Microsoft Store
- Community
- Resources
- Software License Terms
- Licensing FAQ
- Download PDF

Learn / Sysinternals /

Sysmon v1

07/23/2024

In this article

- Introduction
- Overview of Sysmon Capabilities
- Screenshots
- Usage

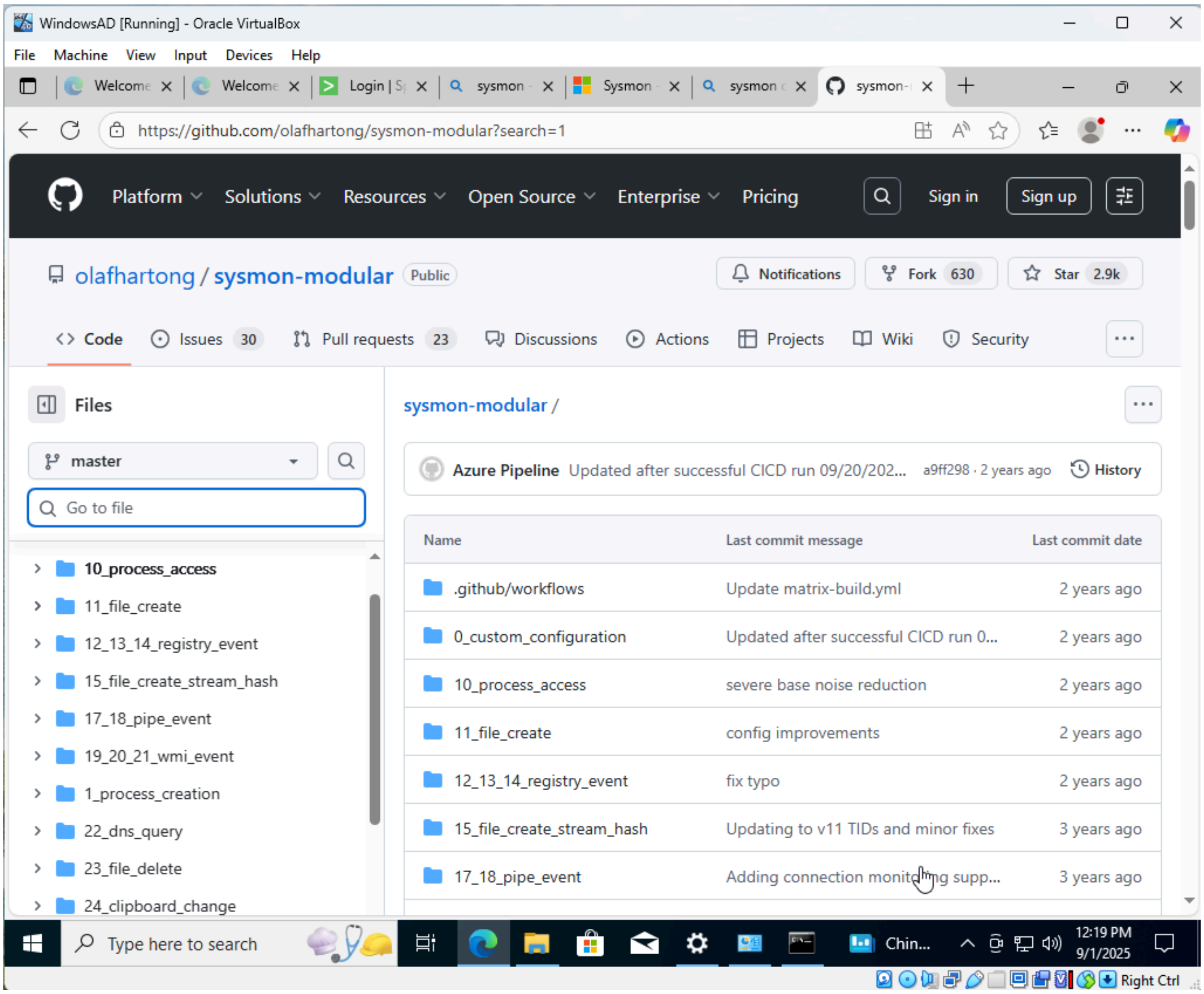
Show 5 more

By Mark Russinovich and Thomas Garnier

Published: July 23, 2024

Download Sysmon (4.6 MB)

Download Sysmon for Linux (GitHub)

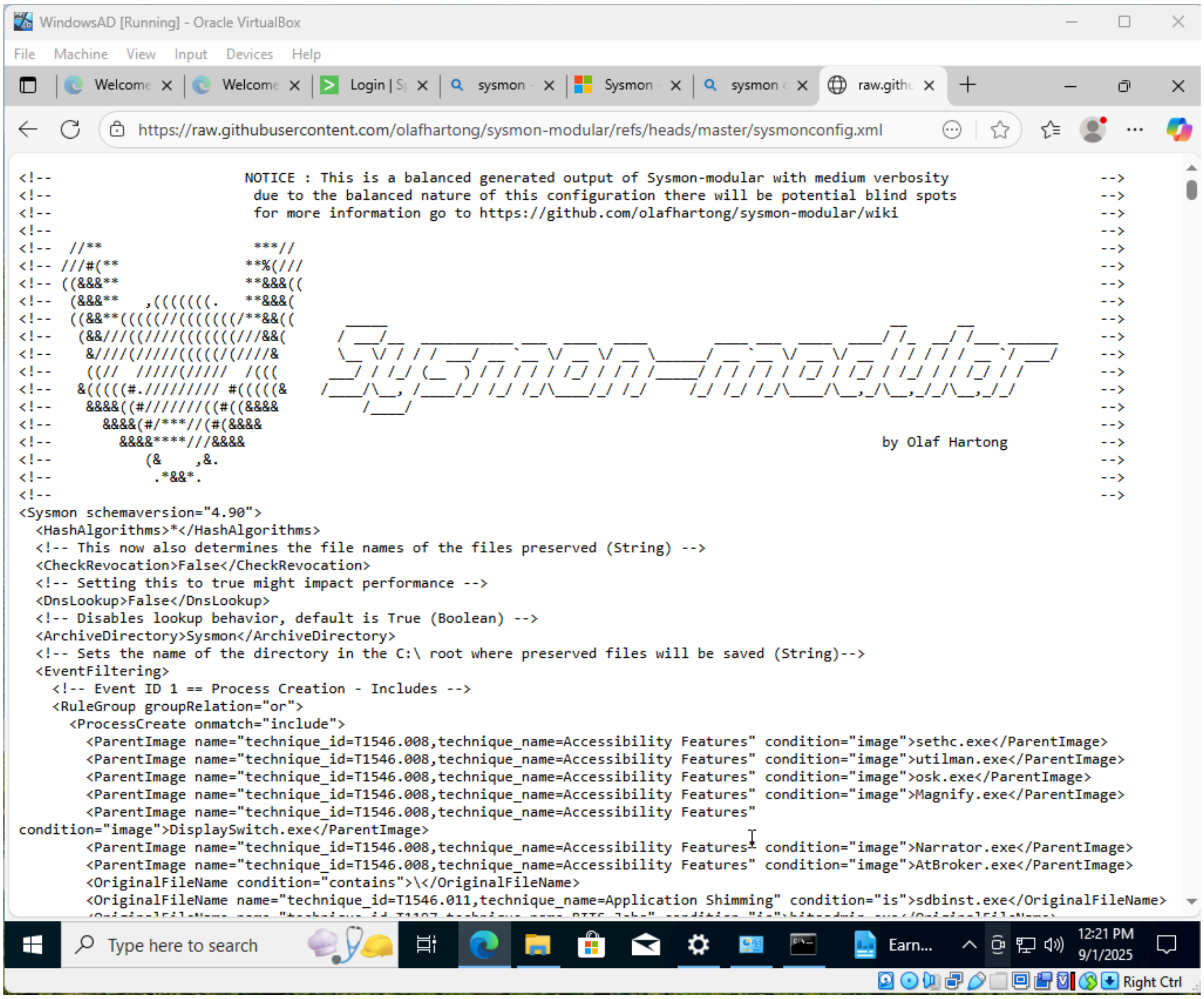


WindowsAD [Running] - Oracle VirtualBox
File Machine View Input Devices Help
https://github.com/olafhartong/sysmon-modular?search=1
Platform Solutions Resources Open Source Enterprise Pricing Sign in Sign up
olafhartong / sysmon-modular Public
Notifications Fork 630 Star 2.9k
Code Issues 30 Pull requests 23 Discussions Actions Projects Wiki Security
Files
master
Go to file
10_process_access
11_file_create
12_13_14_registry_event
15_file_create_stream_hash
17_18_pipe_event
19_20_21_wmi_event
1_process_creation
22_dns_query
23_file_delete
24_clipboard_change
sysmon-modular /
Type here to search
12:19 PM
9/1/2025
Right Ctrl

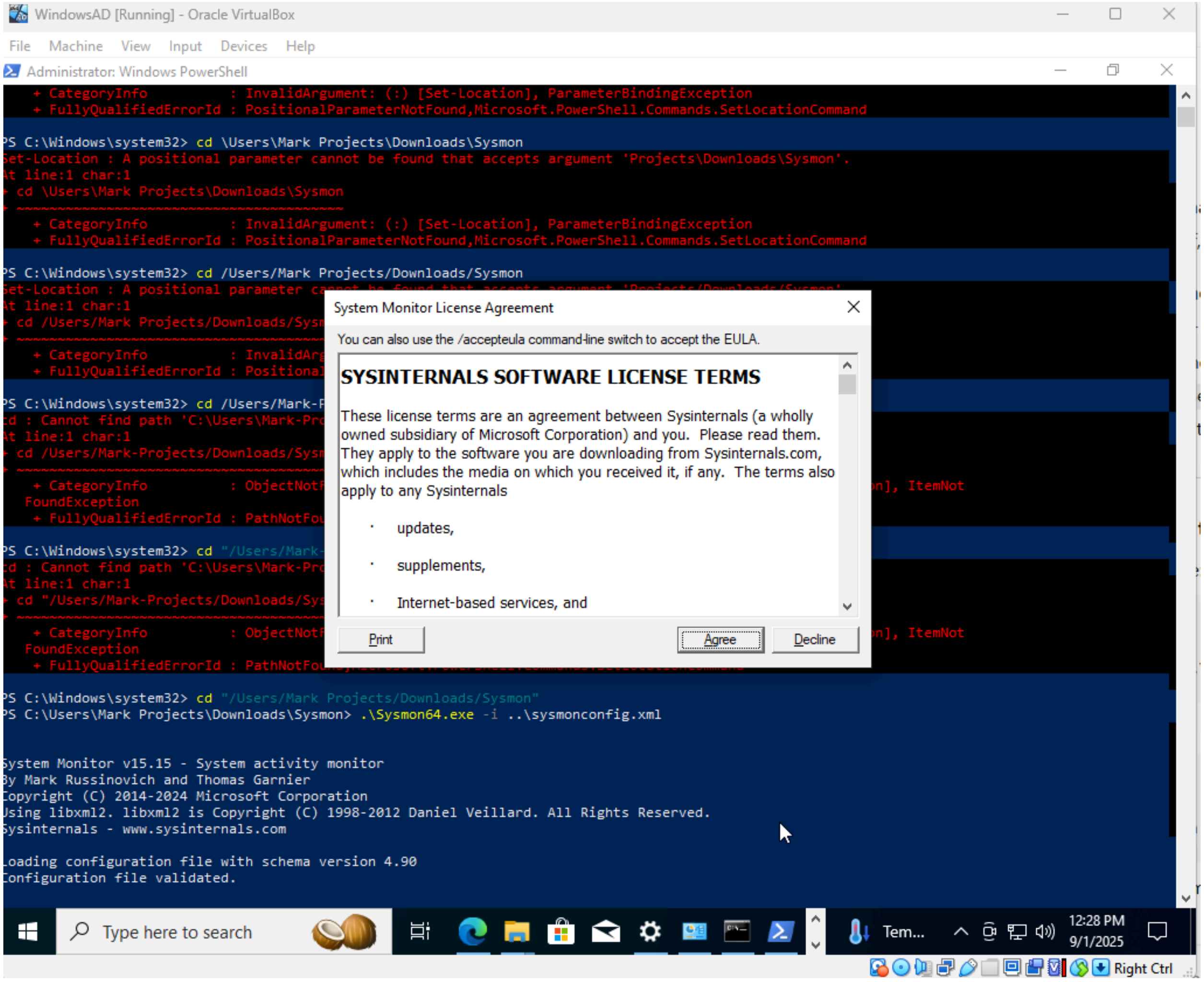
Azure Pipeline Updated after successful CICD run 09/20/202... a9ff298 · 2 years ago History

Name	Last commit message	Last commit date
.github/workflows	Update matrix-build.yml	2 years ago
0_custom_configuration	Updated after successful CICD run 0...	2 years ago
10_process_access	severe base noise reduction	2 years ago
11_file_create	config improvements	2 years ago
12_13_14_registry_event	fix typo	2 years ago
15_file_create_stream_hash	Updating to v11 TIDs and minor fixes	3 years ago
17_18_pipe_event	Adding connection monitoring supp...	3 years ago

- **We will also install a sysmon configuration by Olaf from their github**


WindowsAD [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
Welcome
Welcome
Login | S
sysmon
Sysmon
sysmon
raw.githu
https://raw.githubusercontent.com/olafhartong/sysmon-modular/refs/heads/master/sysmonconfig.xml
Type here to search
Earn...
12:21 PM
9/1/2025
Right Ctrl

```
<!--                          NOTICE : This is a balanced generated output of Sysmon-modular with medium verbosity                  -->
<!--                           due to the balanced nature of this configuration there will be potential blind spots                 -->
<!--                           for more information go to https://github.com/olafhartong/sysmon-modular/wiki                        -->
<!--                                                                                                                                -->
<!--  //**                     ***//                                                                                                -->
<!-- ///#(**                  **%(///                                                                                               -->
<!-- ((&&&**                  **&&&((                                                                                               -->
<!--  (&&&**   ,(((((((.   **&&&(                                                                                                   -->
<!--  ((&&**(((((//(((((((/**&&((       _____                                        __     __                                      -->
<!--   (&&///((////(((((((///&&(      / ___/__  __________ ___  ____  ____        ____ ___  ____  ____/ /_  __/ /___ ______             -->
<!--    &////(/////(((((/(////&       \__ \/ / / / ___/ __ `__ \/ __ \/ __ \______/ __ `__ \/ __ \/ __  / / / / / __ `/ ___/             -->
<!--     ((//  /////(/////  /(((      ___/ / /_/ (__  ) / / / / /_/ / / / /_____/ / / / / / /_/ / /_/ / /_/ / / /_/ / /                 -->
<!--   &(((((#.///////// #(((((&    /____/\__, /____/_/ /_/ /_/\____/_/ /_/     /_/ /_/ /_/\____/\__,_/\__,_/_/\__,_/_/                  -->
<!--    &&&&((#///////((#((&&&&          /____/                                                                                     -->
<!--      &&&&(#/***//(#(&&&&                                                                                                       -->
<!--        &&&&****///&&&&                                                                                    by Olaf Hartong      -->
<!--           (&    ,&.                                                                                                            -->
<!--            .*&&*.                                                                                                              -->
<!--                                                                                                                                -->
<Sysmon schemaversion="4.90">
  <HashAlgorithms>*</HashAlgorithms>
  <!-- This now also determines the file names of the files preserved (String) -->
  <CheckRevocation>False</CheckRevocation>
  <!-- Setting this to true might impact performance -->
  <DnsLookup>False</DnsLookup>
  <!-- Disables lookup behavior, default is True (Boolean) -->
  <ArchiveDirectory>Sysmon</ArchiveDirectory>
  <!-- Sets the name of the directory in the C:\ root where preserved files will be saved (String)-->
  <EventFiltering>
    <!-- Event ID 1 == Process Creation - Includes -->
    <RuleGroup groupRelation="or">
      <ProcessCreate onmatch="include">
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features" condition="image">sethc.exe</ParentImage>
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features" condition="image">utilman.exe</ParentImage>
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features" condition="image">osk.exe</ParentImage>
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features" condition="image">Magnify.exe</ParentImage>
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features"
condition="image">DisplaySwitch.exe</ParentImage>
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features" condition="image">Narrator.exe</ParentImage>
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features" condition="image">AtBroker.exe</ParentImage>
        <OriginalFileName condition="contains">\</OriginalFileName>
        <OriginalFileName name="technique_id=T1546.011,technique_name=Application Shimming" condition="is">sdbinst.exe</OriginalFileName>
        <OriginalFileName name="technique_id=T1197,technique_name=BITS Jobs" condition="is">bitsadmin.exe</OriginalFileName>
```



```
    + CategoryInfo          : InvalidArgument: (:) [Set-Location], ParameterBindingException
    + FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.SetLocationCommand

PS C:\Windows\system32> cd \Users\Mark Projects\Downloads\Sysmon
Set-Location : A positional parameter cannot be found that accepts argument 'Projects\Downloads\Sysmon'.
At line:1 char:1
+ cd \Users\Mark Projects\Downloads\Sysmon
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (:) [Set-Location], ParameterBindingException
    + FullyQualifiedErrorId : PositionalParameterNotFound,Microsoft.PowerShell.Commands.SetLocationCommand

PS C:\Windows\system32> cd /Users/Mark Projects/Downloads/Sysmon
Set-Location : A positional parameter ca
At line:1 char:1
+ cd /Users/Mark Projects/Downloads/Sysm
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArg
    + FullyQualifiedErrorId : Positional

PS C:\Windows\system32> cd /Users/Mark-P
cd : Cannot find path 'C:\Users\Mark-Pro
At line:1 char:1
+ cd /Users/Mark-Projects/Downloads/Sysm
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotF                                        on], ItemNot
   FoundException
    + FullyQualifiedErrorId : PathNotFou

PS C:\Windows\system32> cd "/Users/Mark-
cd : Cannot find path 'C:\Users\Mark-Pro
At line:1 char:1
+ cd "/Users/Mark-Projects/Downloads/Sys
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotF                                        on], ItemNot
   FoundException
    + FullyQualifiedErrorId : PathNotFou

PS C:\Windows\system32> cd "/Users/Mark Projects/Downloads/Sysmon"
PS C:\Users\Mark Projects\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.
```

System Monitor License Agreement

You can also use the /accepteula command-line switch to accept the EULA.

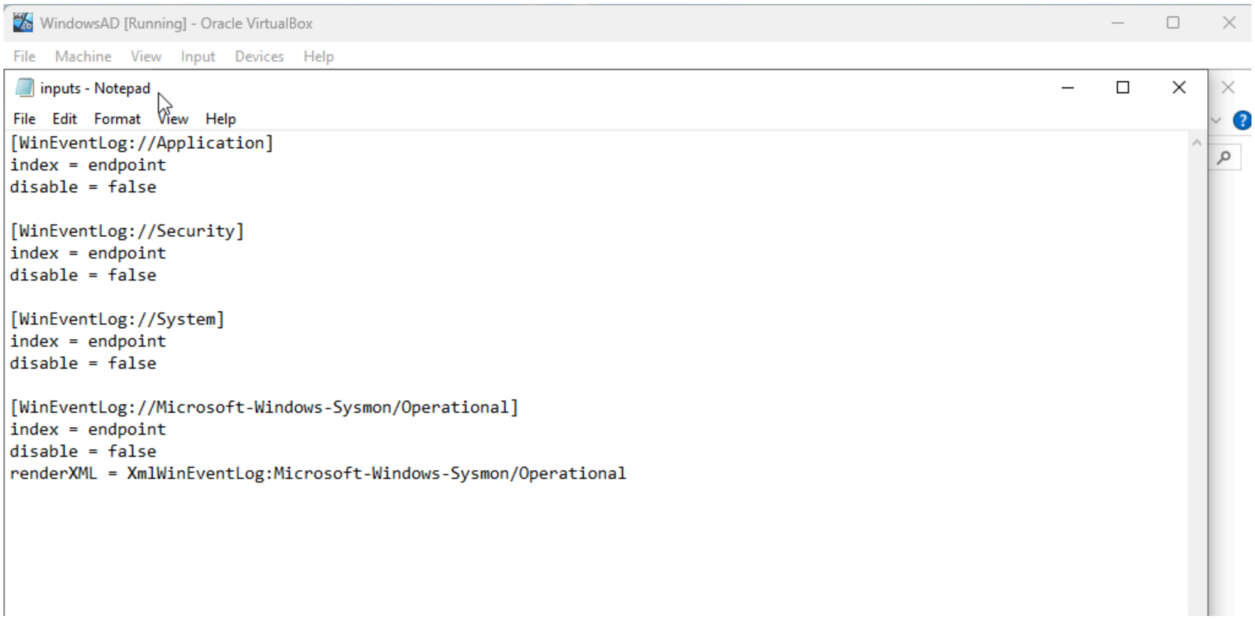
SYSINTERNALS SOFTWARE LICENSE TERMS

These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Sysinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals

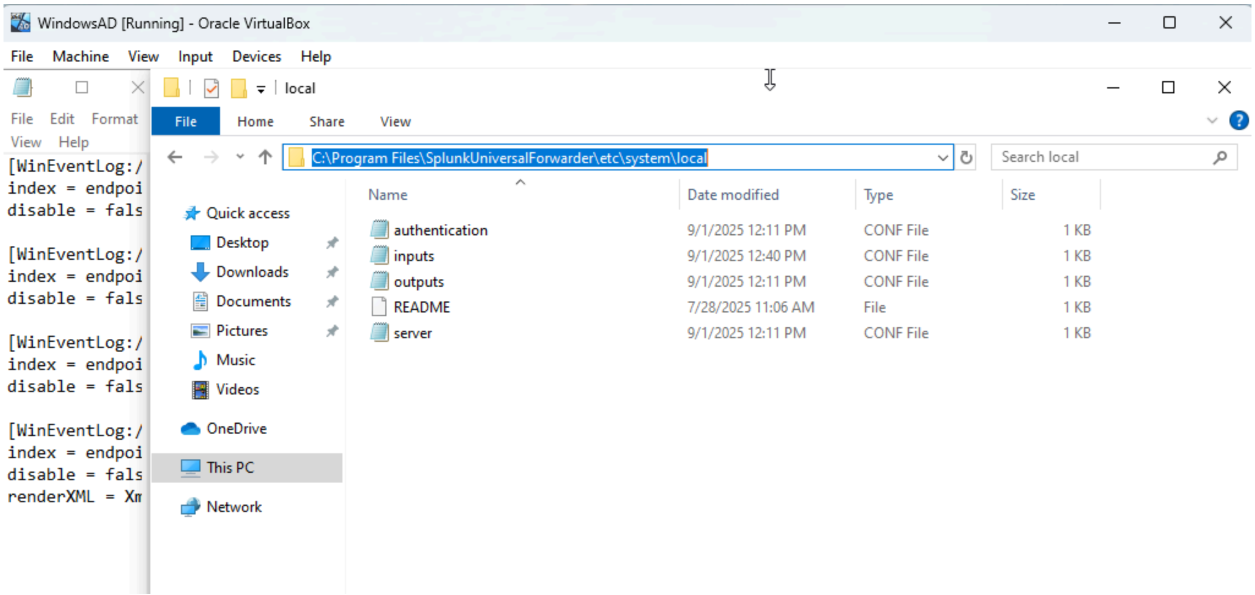
- updates,
- supplements,
- Internet-based services, and

Print Agree Decline

- Now we are officially downloading sysmon through powershell
- We will copy this txt file into Sysmon file folder so it can receive endpoint logs, naming it inputs.conf the restart splunks univseral forwarders service


WindowsAD [Running] - Oracle VirtualBox
File Machine View Input Devices Help
inputs - Notepad
File Edit Format View Help

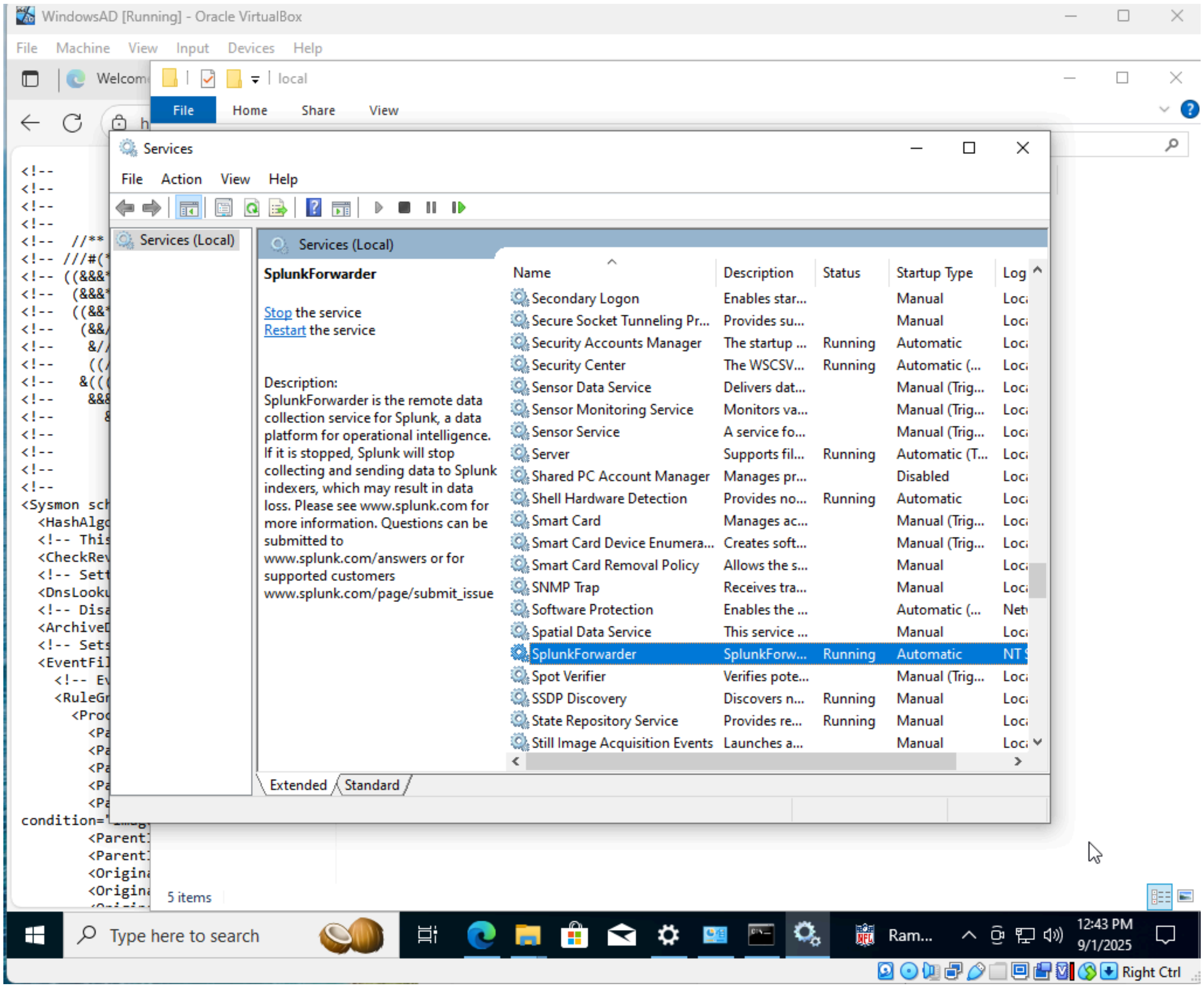
```
[WinEventLog://Application]
index = endpoint
disable = false

[WinEventLog://Security]
index = endpoint
disable = false

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

[WinEventLog://Microsoft-Windows-Sysmon/Operational]
index = endpoint
disable = false
renderXML = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
```



```
[WinEventLog:/
index = endpoi
disable = fals

[WinEventLog:/
index = endpoi
disable = fals

[WinEventLog:/
index = endpoi
disable = fals

[WinEventLog:/
index = endpoi
disable = fals
renderXML = Xm
```

C:\Program Files\SplunkUniversalForwarder\etc\system\local

Name	Date modified	Type	Size
authentication	9/1/2025 12:11 PM	CONF File	1 KB
inputs	9/1/2025 12:40 PM	CONF File	1 KB
outputs	9/1/2025 12:11 PM	CONF File	1 KB
README	7/28/2025 11:06 AM	File	1 KB
server	9/1/2025 12:11 PM	CONF File	1 KB



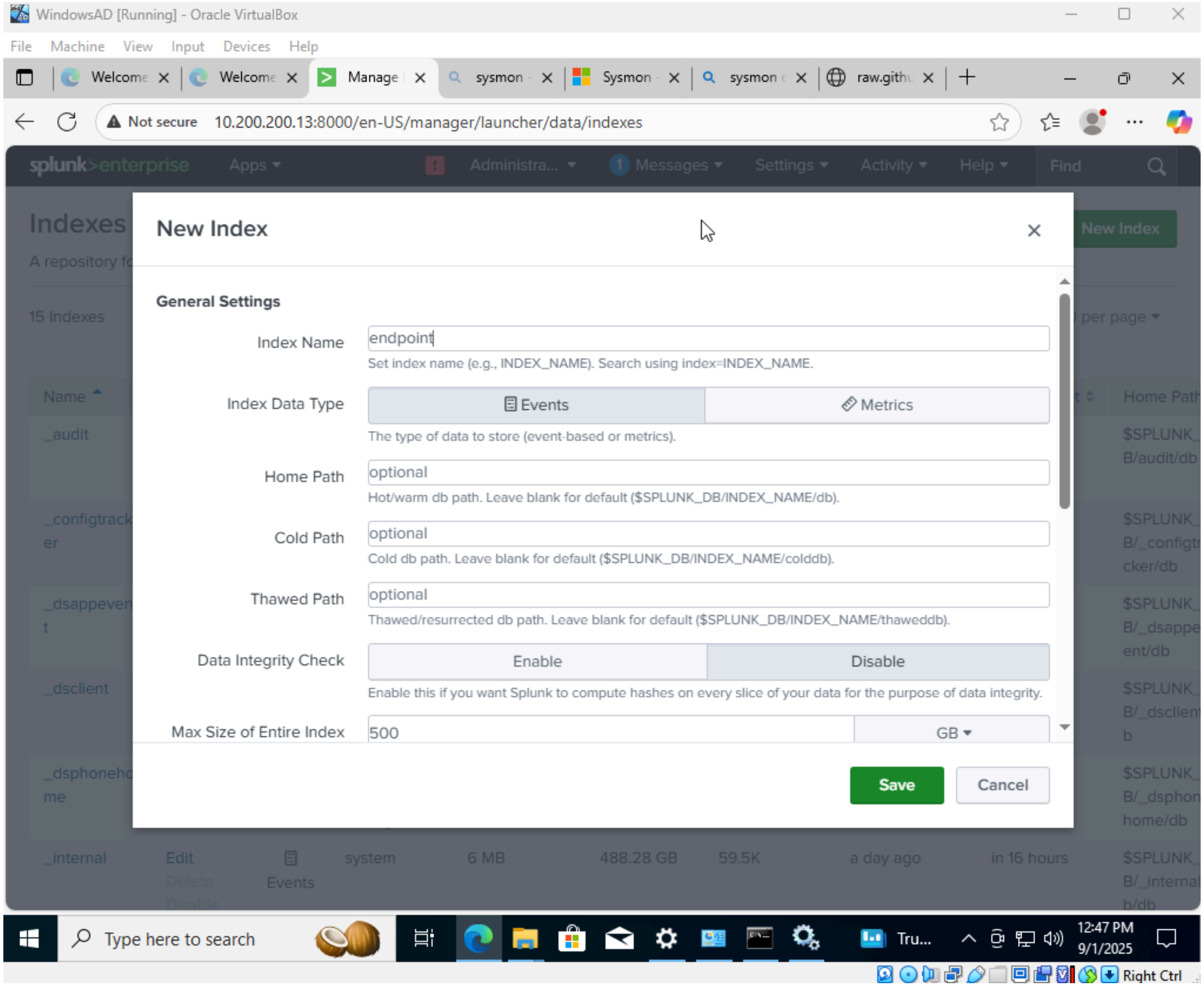
SplunkForwarder

Stop the service
Restart the service

Description:
SplunkForwarder is the remote data collection service for Splunk, a data platform for operational intelligence. If it is stopped, Splunk will stop collecting and sending data to Splunk indexers, which may result in data loss. Please see www.splunk.com for more information. Questions can be submitted to www.splunk.com/answers or for supported customers www.splunk.com/page/submit_issue

Name	Description	Status	Startup Type	Log
Secondary Logon	Enables star...		Manual	Loc
Secure Socket Tunneling Pr...	Provides su...		Manual	Loc
Security Accounts Manager	The startup ...	Running	Automatic	Loc
Security Center	The WSCSV...	Running	Automatic (...	Loc
Sensor Data Service	Delivers dat...		Manual (Trig...	Loc
Sensor Monitoring Service	Monitors va...		Manual (Trig...	Loc
Sensor Service	A service fo...		Manual (Trig...	Loc
Server	Supports fil...	Running	Automatic (T...	Loc
Shared PC Account Manager	Manages pr...		Disabled	Loc
Shell Hardware Detection	Provides no...	Running	Automatic	Loc
Smart Card	Manages ac...		Manual (Trig...	Loc
Smart Card Device Enumera...	Creates soft...		Manual (Trig...	Loc
Smart Card Removal Policy	Allows the s...		Manual	Loc
SNMP Trap	Receives tra...		Manual	Loc
Software Protection	Enables the ...		Automatic (...	Net
Spatial Data Service	This service ...		Manual	Loc
SplunkForwarder	SplunkForw...	Running	Automatic	NT
Spot Verifier	Verifies pote...		Manual (Trig...	Loc
SSDP Discovery	Discovers n...	Running	Manual	Loc
State Repository Service	Provides re...	Running	Manual	Loc
Still Image Acquisition Events	Launches a...		Manual	Loc

- Now the image above is us restarting the SplunkForwader after updating the input locally
- Next, inside of splunk we will create an endpoint index



WindowsAD [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Welcome
Welcome
Manage
sysmon
Sysmon
sysmon
raw.githu
Not secure 10.200.200.13:8000/en-US/manager/launcher/data/indexes
splunk>enterprise Apps Administra... Messages Settings Activity Help Find
Indexes
New Index
Type here to search
12:47 PM
9/1/2025
Right Ctrl

New Index

General Settings

Index Name: endpoint

Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: Events | Metrics

The type of data to store (event-based or metrics).

Home Path: optional

Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

Cold Path: optional

Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path: optional

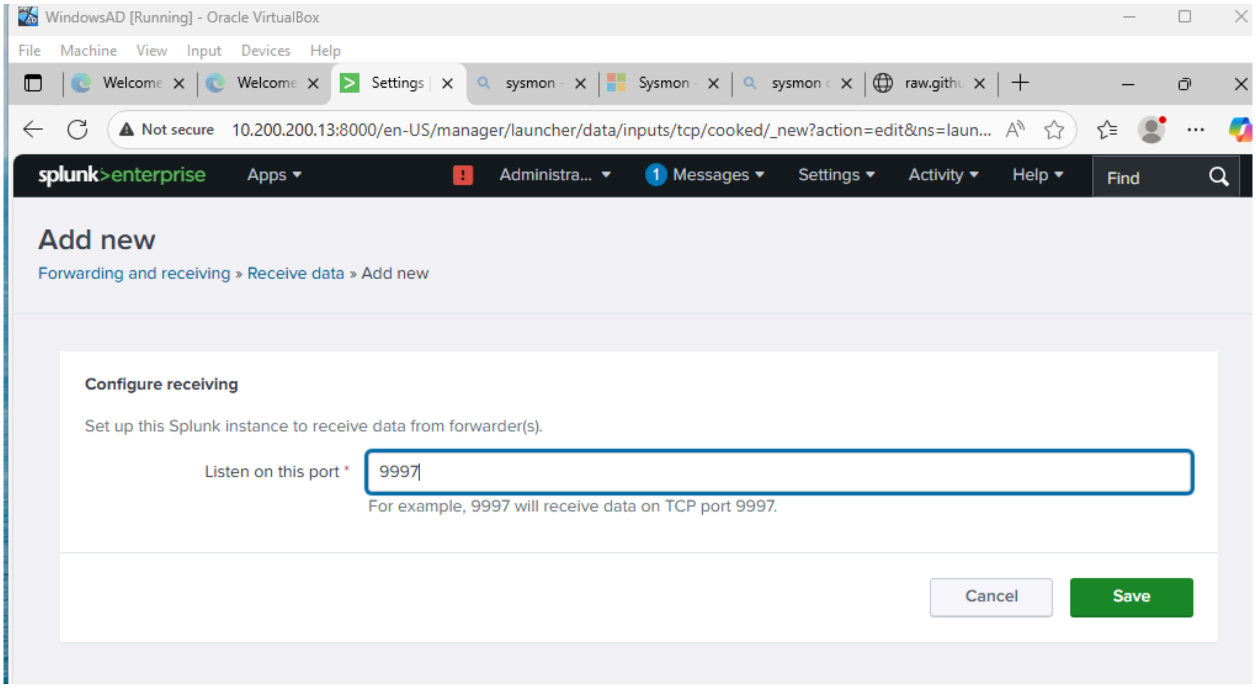
Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check: Enable | Disable

Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index: 500 GB

Save Cancel


WindowsAD [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Welcome
Welcome
Settings
sysmon
Sysmon
sysmon
raw.githu
Not secure 10.200.200.13:8000/en-US/manager/launcher/data/inputs/tcp/cooked/_new?action=edit&ns=laun...
splunk>enterprise
Apps
Administra...
1 Messages
Settings
Activity
Help
Find

Add new

Forwarding and receiving » Receive data » Add new

Configure receiving

Set up this Splunk instance to receive data from forwarder(s).

Listen on this port * 9997

For example, 9997 will receive data on TCP port 9997.

- We will then enable our splunk server to receive the data (settings > forwading & receiveing > configure receiving > enter the port)