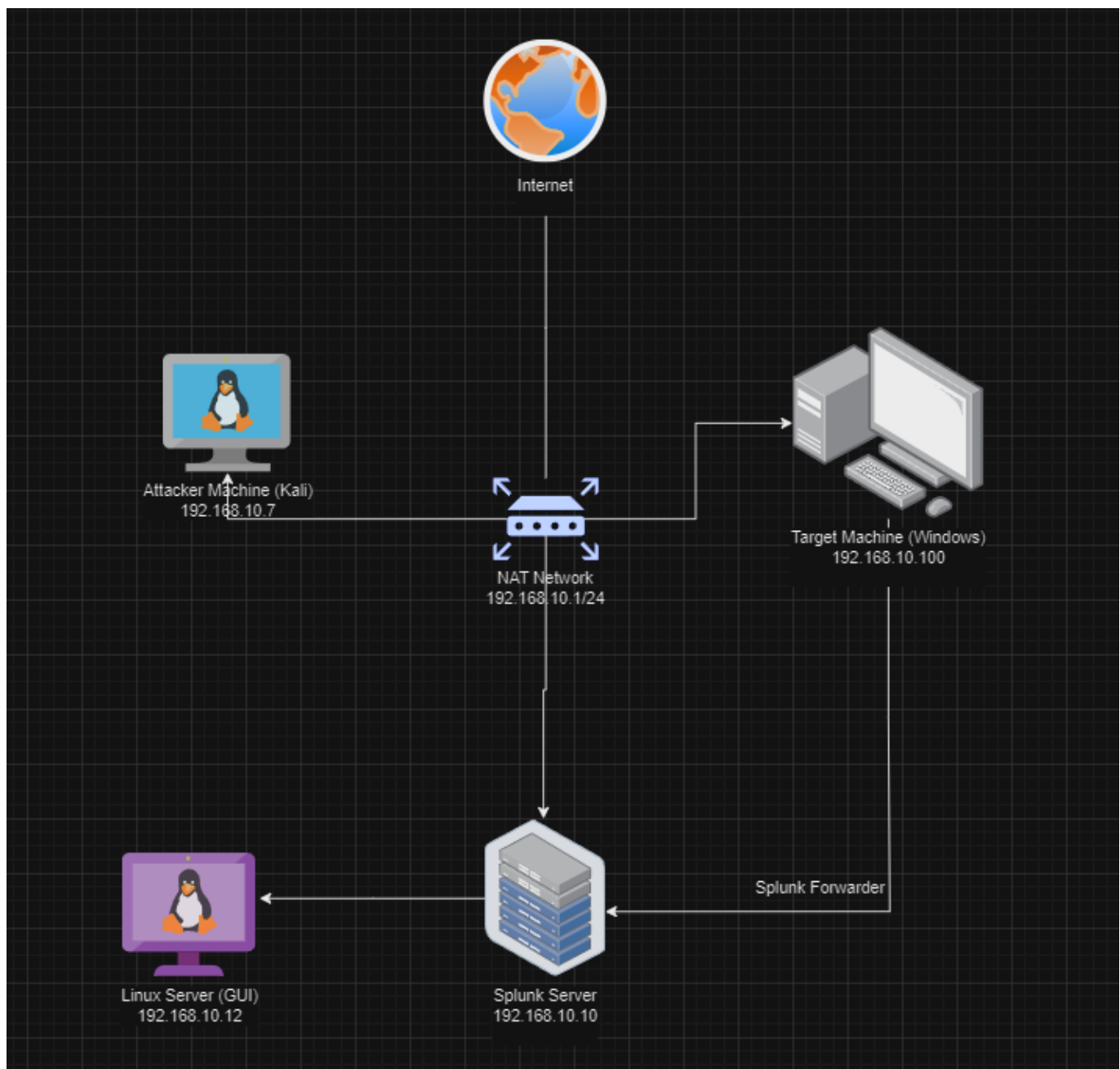


# Security Information and Event Management (SIEM) with Splunk

**SIEM** stands for **Security Information and Event Management**. It is a comprehensive approach to cybersecurity that involves collecting, analyzing, and managing security-related data from across an organization's IT infrastructure. SIEM systems are designed to:

1. **Centralize Data Collection:** SIEM tools gather log data from various sources, such as network devices, servers, applications, and security tools.
2. **Real-time Monitoring:** They provide continuous monitoring of security events and alerts in real-time, allowing for quick detection of potential threats.
3. **Correlation and Analysis:** SIEM systems correlate data from different sources to identify patterns or anomalies that might indicate a security breach or attack.
4. **Incident Detection and Response:** SIEM tools help in detecting security incidents, prioritizing them based on severity, and providing actionable insights for response.
5. **Compliance Reporting:** SIEM solutions often include features for generating reports that help organizations comply with regulatory requirements like GDPR, HIPAA, and PCI-DSS.
6. **Forensic Investigation:** They allow for in-depth analysis of security incidents, helping to trace the origins of an attack and understand its impact.



Setting up the Splunk Enterprises Server:

## 1. Introduction to VirtualBox

VirtualBox is a software virtualization package that allows you to create and manage virtual machines on your operating system. It enables the installation of a second operating system within the virtual environment.

### 1.1 Installation of VirtualBox

To begin, download and install VirtualBox. Detailed installation instructions for different operating systems are available on the [official VirtualBox website](#).

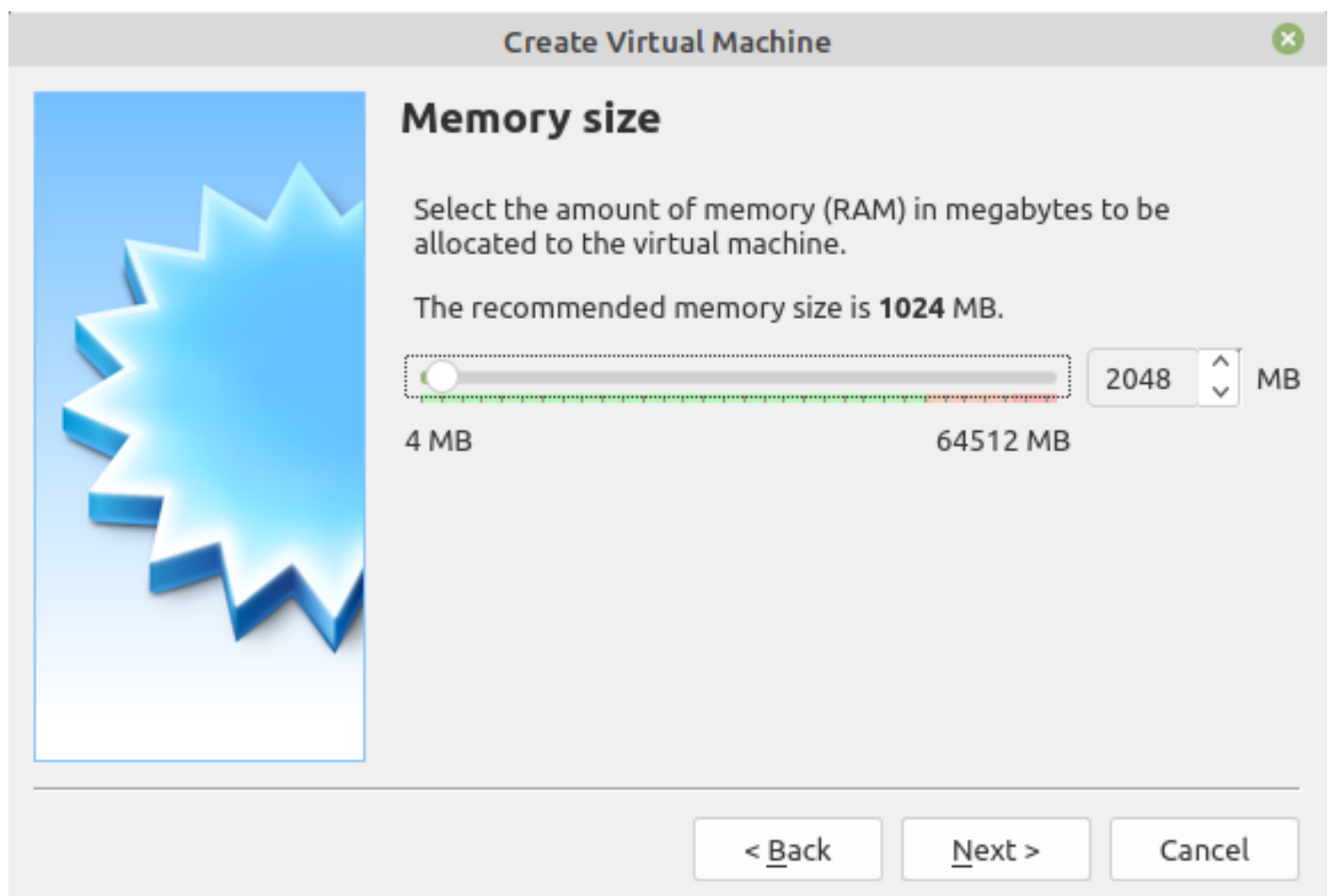
Next, download the Ubuntu Live Server from [Ubuntu's official website](#).

### 1.2 Creating a New Virtual Machine

- Launch VirtualBox, which will open the VirtualBox Manager.
- Click on "New" to create a new virtual machine.




- Provide a name for your virtual machine; the drop-down menus should automatically update based on your selection.
- Click "Next" and allocate 2GB (2048 MB) of RAM to the virtual machine.



- On the next screen, select "Dynamically allocated" for the virtual hard disk and set the size to 40GB to accommodate Splunk Enterprise.

Create Virtual Machine



## Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **1024 MB**.

4 MB64512 MB

2048 MB

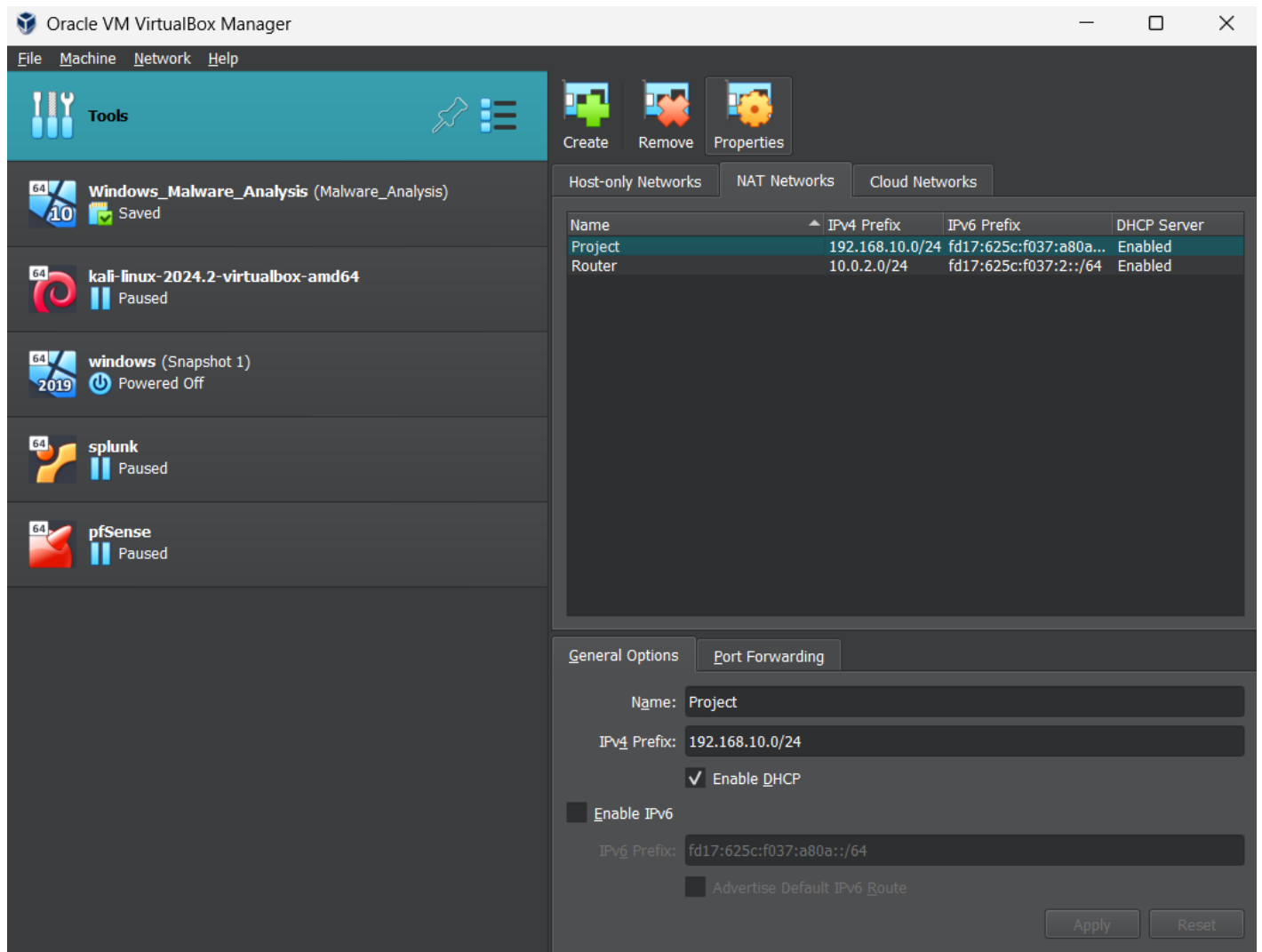
< Back

Next >

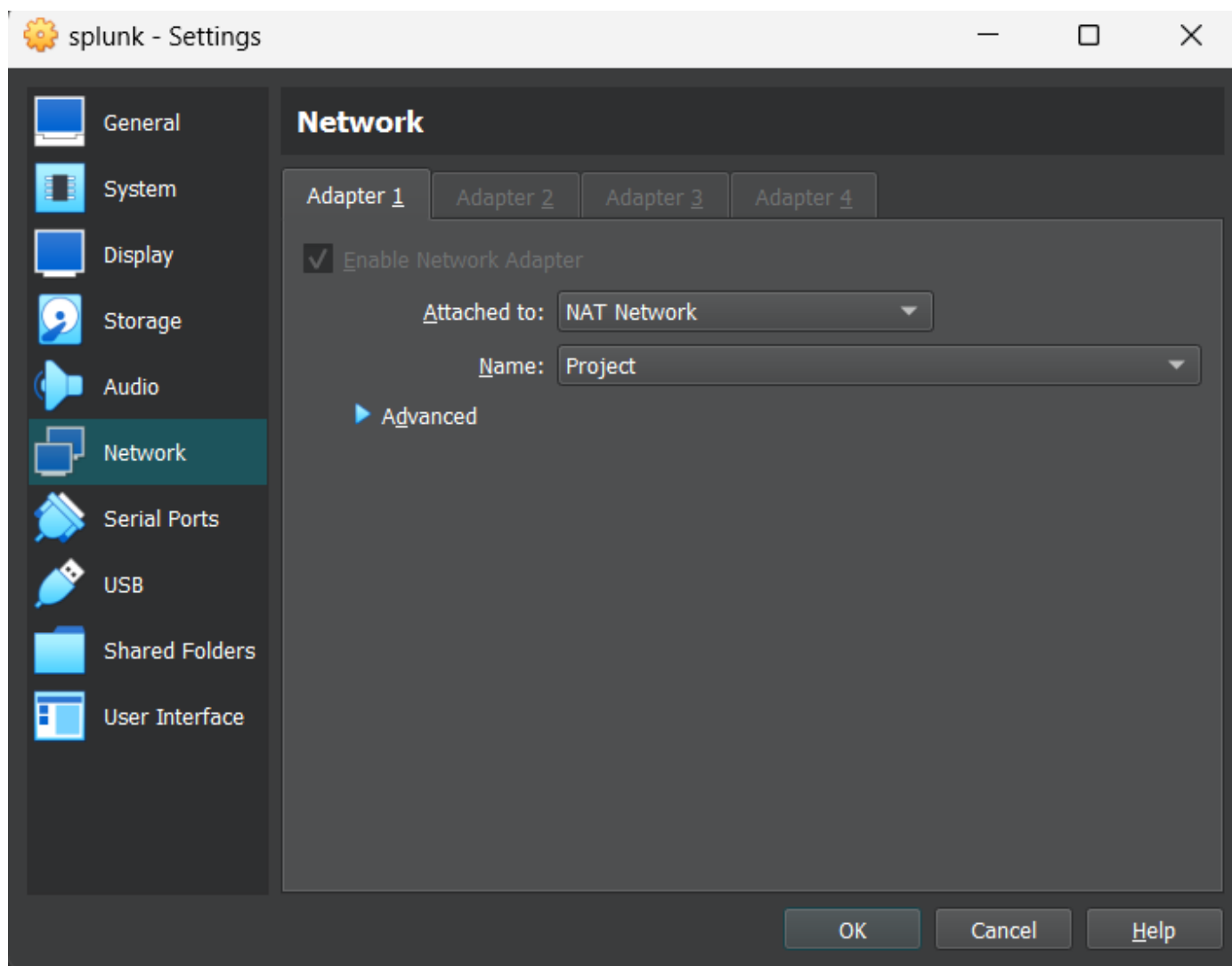
Cancel

### 1.3 Setting Up a Virtual NAT Network

1. Create a NAT network and name it, e.g., "Project," with an IPv4 address of `192.168.10.1/24`. Enable DHCP and save the network.



2. In the Ubuntu Live Server settings, go to "Network" and set Adapter 1 to the newly created NAT network.



#### 1.4 Assigning a Static IP Address to the Splunk Server

```
ip a #For Checking the IP Addr of the Linux Server
```

```
splunk@splunk:/var/log/snort$ 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 pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:e1:5c:64 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:fee1:5c64/64 scope link
        valid_lft forever preferred_lft forever
splunk@splunk:/var/log/snort$
```

Modify the configuration file to assign a static IP of `192.168.10.10` to the server:

```
sudo nano /etc/netplan/00-installer-config.yaml
```

```
#config file
network:
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.10.10/24]
      nameservers:
        addresses: [8.8.8.8]
      routes:
        - to: default
          via: 192.168.10.1
  version: 2
```

Apply the changes with `sudo netplan apply`.

```
sudo netplan apply
```

Done.

## Setting Up Splunk Enterprise (SE):

1. Open a web browser and navigate to the Splunk website (<https://www.splunk.com>).
2. Create an account or login to your account.

3. Under Products, click on "Free Trials & Downloads".

4. Scroll down, under Splunk Enterprise click-on "Get My Free Trial"

5. Select the appropriate version of Splunk Enterprise for Linux (64-bit) and choose the Debian package (`.deb`) format.

**Splunk Enterprise 9.0.5**

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

**Choose Your Installation Package**

Windows **Linux** Mac OS

64-bit	3.x+, 4.x+, or 5.4.x kernel Linux distributions	.tgz	577.34 MB	Download Now
		.deb	448.87 MB	Download Now
		.rpm	577.46 MB	Download Now

```
sudo apt install ./splunk<version>.deb
```

4. After the installation completes, start Splunk Enterprise by running:

```
sudo /opt/splunk/bin/splunk start --accept-license
```

5. Type 'y' to agree with the license.

6. Splunk Enterprise will prompt you to create an administrator password. Follow the instructions to set a secure password.

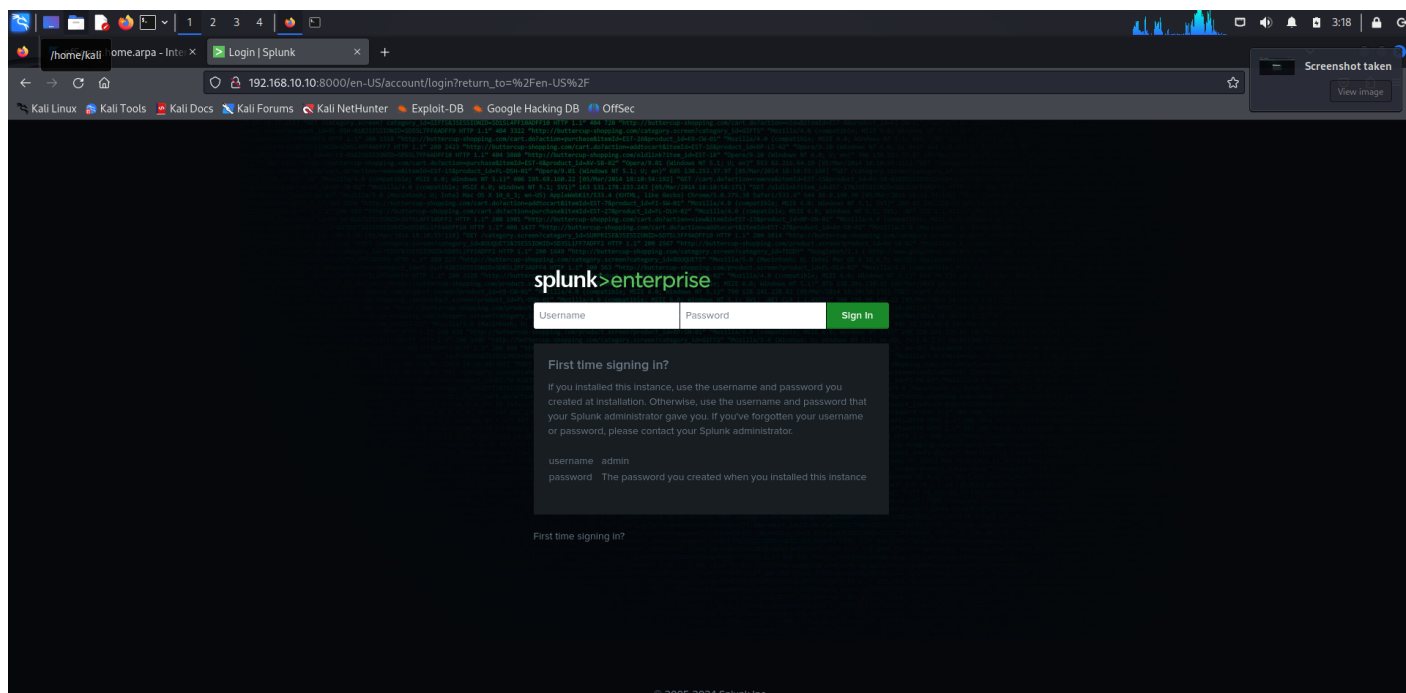
### Access Splunk Enterprise Web Interface

1. Start up the Splunk web interface by running:

```
sudo /opt/splunk/bin/splunk start
```

2. After loading, right click on the link beside "The Splunk web interface is at" and click-on **Open Link**





You Can Access the Splunk GUI Based Web Interface on 192.168.10.10:8000

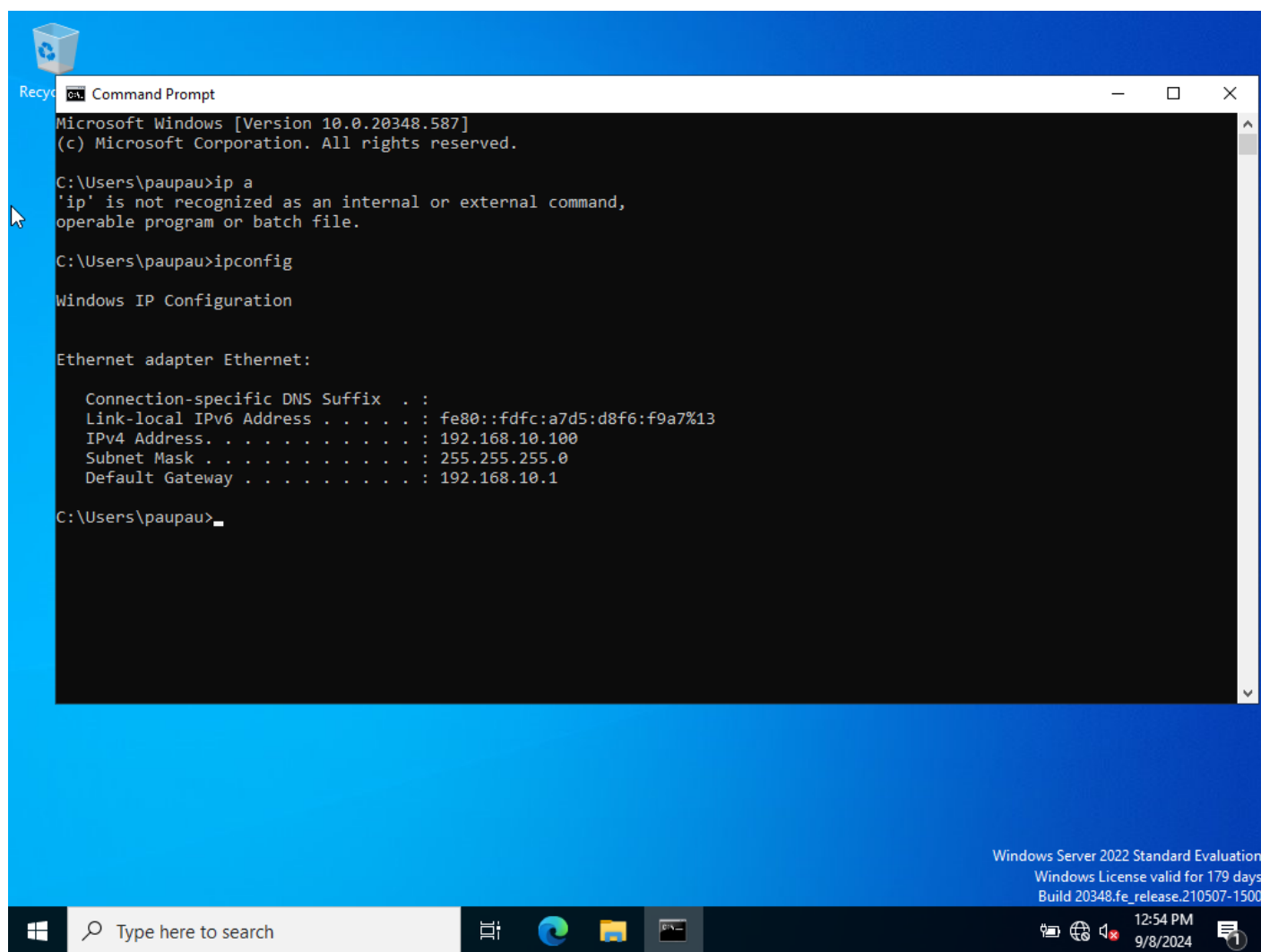
Use the Username and Password set during the installation to log into the administrator page.

## 3. Setting Up the Target Windows Machine

### 3.1 Configuring the IP Address

1. Check the IP address of the Windows machine using `ipconfig`.

```
ipconfig
```



The screenshot shows a Windows Command Prompt window titled "Command Prompt" with a Recycle Bin icon in the title bar. The window displays the following text:

```
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\paupau>ip a
'ip' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\paupau>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

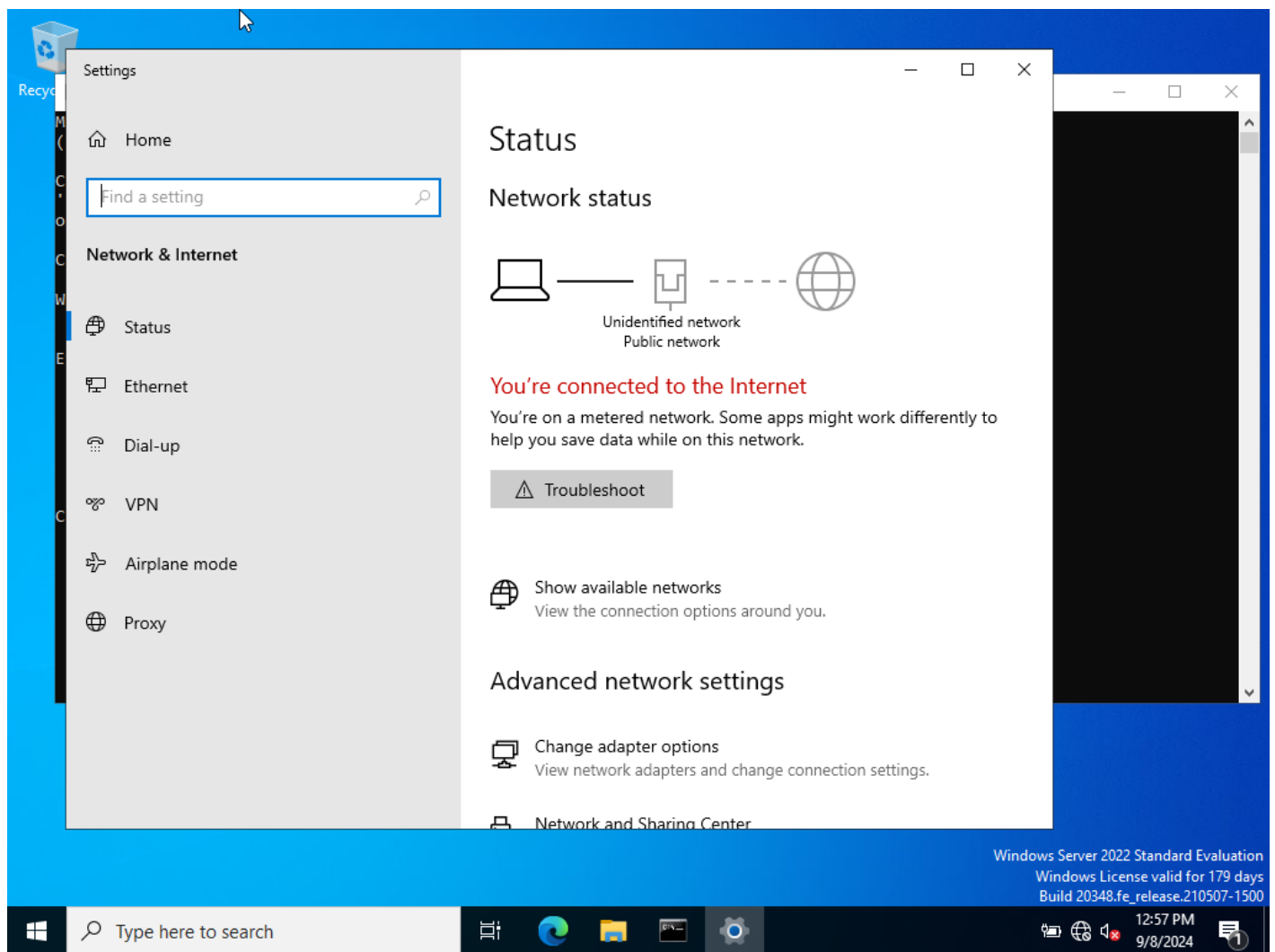
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::fd5d:a7d5:d8f6:f9a7%13
    IPv4 Address. . . . . : 192.168.10.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1

C:\Users\paupau>
```

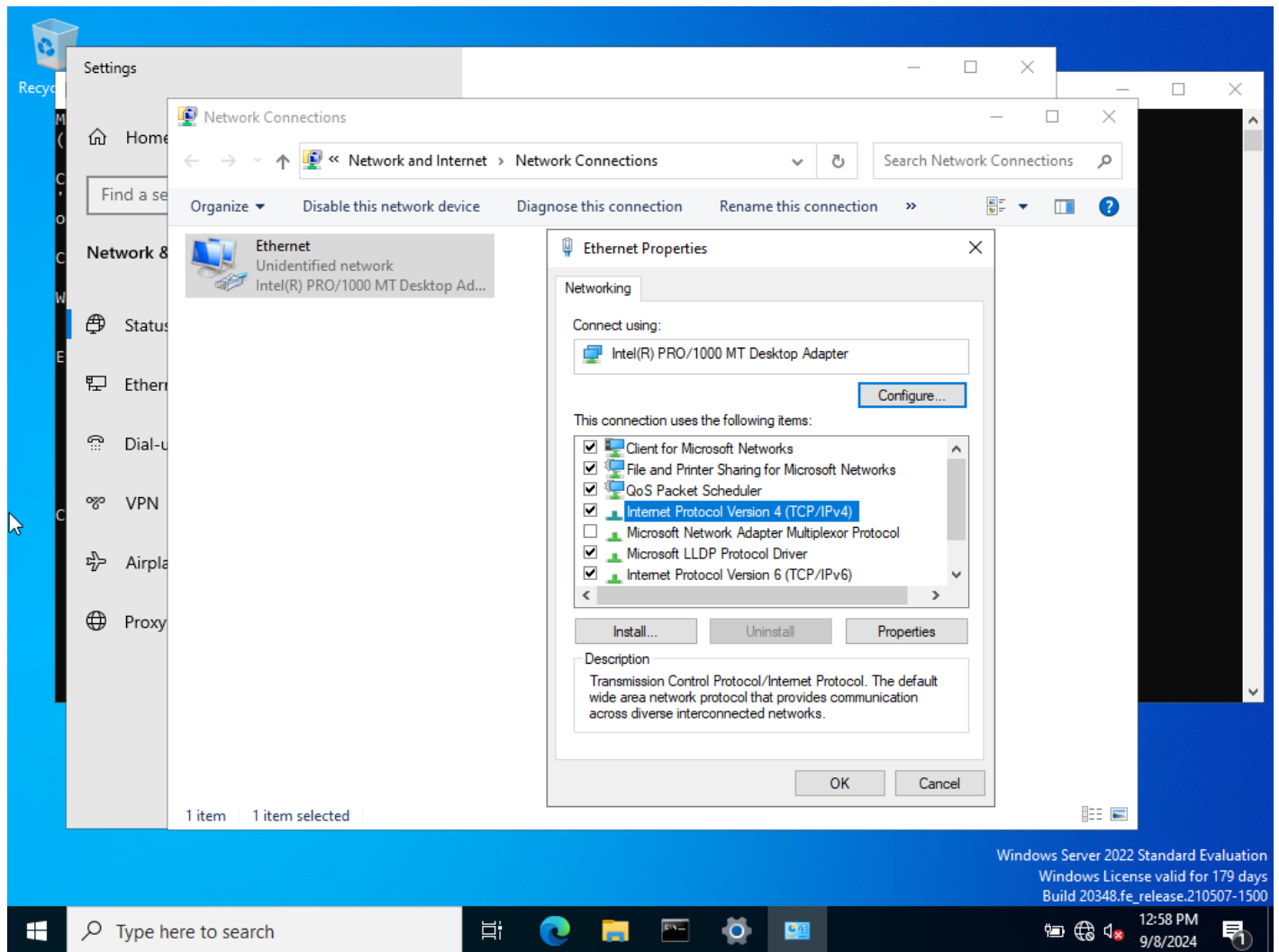
The taskbar at the bottom shows the Windows logo, a search bar with the text "Type here to search", and several application icons. The system tray on the right displays the date and time as "12:54 PM 9/8/2024" and a notification icon.

Set a static IP address, e.g., `192.168.10.100`, in the network adapter settings.

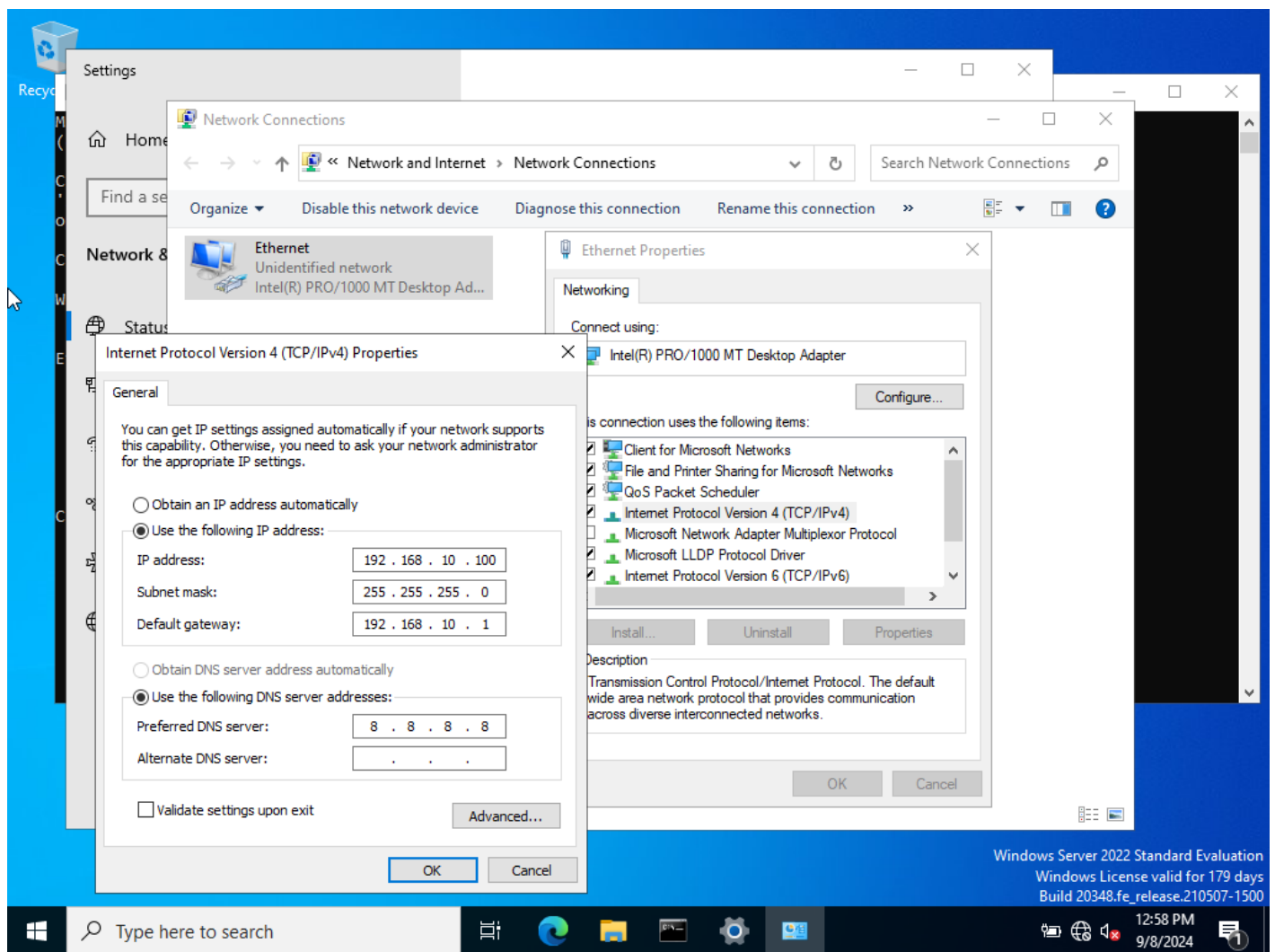
1. Go the Change Network Adapter



2. Select the Properties Section of the Ethernet Adapter.



3. Go to Internet Protocol Version and set the IP address to static based on your need, in my case its 192.168.10.100



## 4. Deploying the Splunk Universal Forwarder on Windows

The [Splunk Universal Forwarder](#) is the best mechanism for collecting logs from servers and end-user systems. In order to collect logs at scale, it is necessary to deploy the Universal Forwarder to every system where log collection is required. Managing the deployment of the Universal Forwarder is best handled via whatever mechanism your organization uses to deploy software packages across machines in your organization. However, if you're doing a one-off installation of the Universal Forwarder or don't have a method of deploying MSIs, the installer may be an acceptable option.

### Installation Steps

#### Obtain the Installation Package

First, download the Splunk Universal Forwarder from Splunk's [download page](#). You will need a [Splunk.com](#) account to access the download. In the event you need to download an older version of the Universal Forwarder, those packages are available on the [older releases](#) page.

# Choose Your Download

## Splunk Universal Forwarder 8.1.2

Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

### Choose Your Installation Package

Windows

Linux

Solaris

Mac OS

FreeBSD

AIX


64-bit

Windows 10

Windows Server 2016, 2019

.msi

70.5 MB


Download Now 

32-bit

Windows 10

.msi

59.04 MB

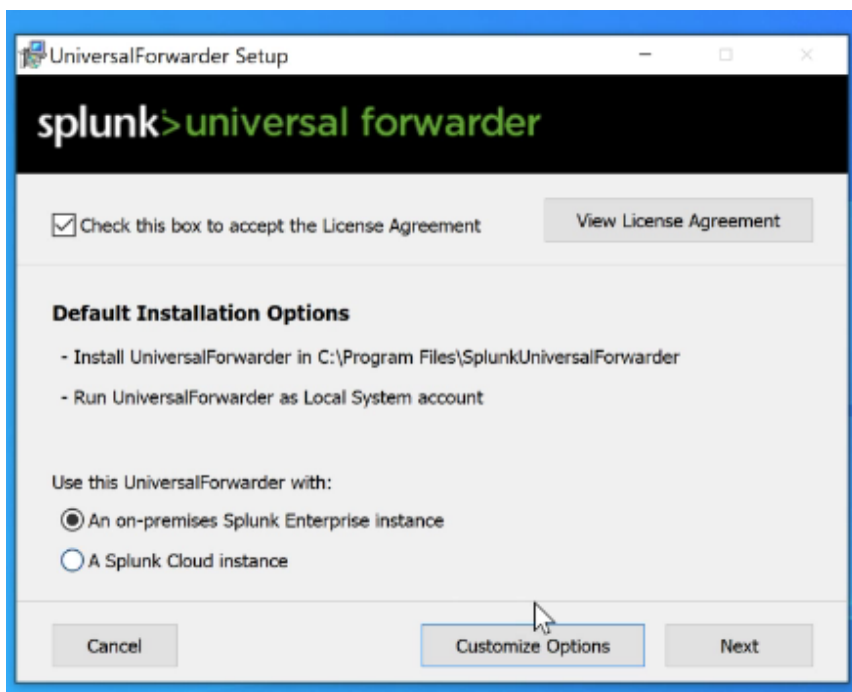
Download Now 

Release Notes

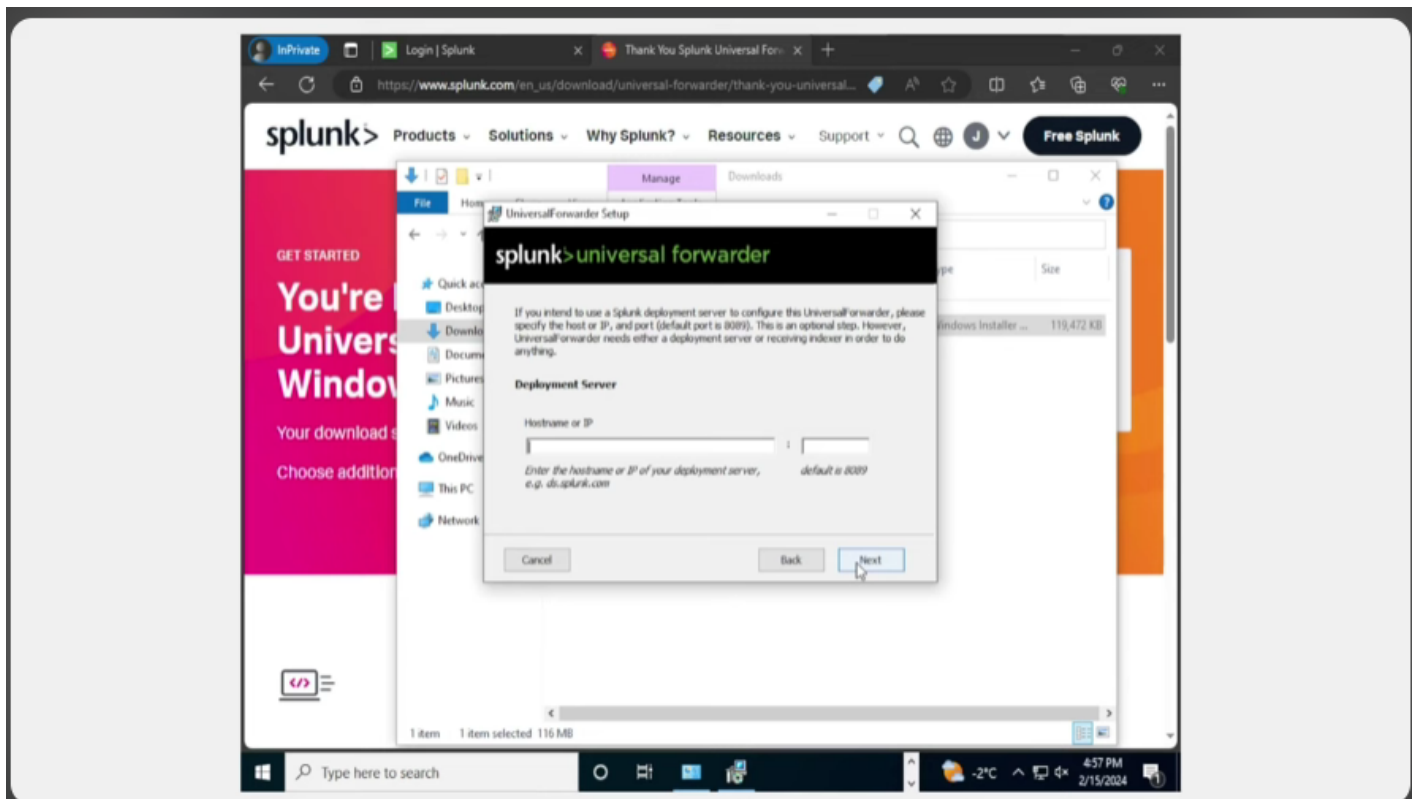
Older Releases

All Other Downloads

When running the installation wizard, you will be asked if you're deploying the Universal Forwarder for an on-premise or Splunk Cloud deployment. If you have an environment managed by Hurricane Labs with a deployment server, you'll always want to choose the on-premise option (even if you're a Splunk Cloud customer), since all of the configurations will be managed by the deployment server.



Set the IP Address to the Splunk Enterprises and the port to Default.

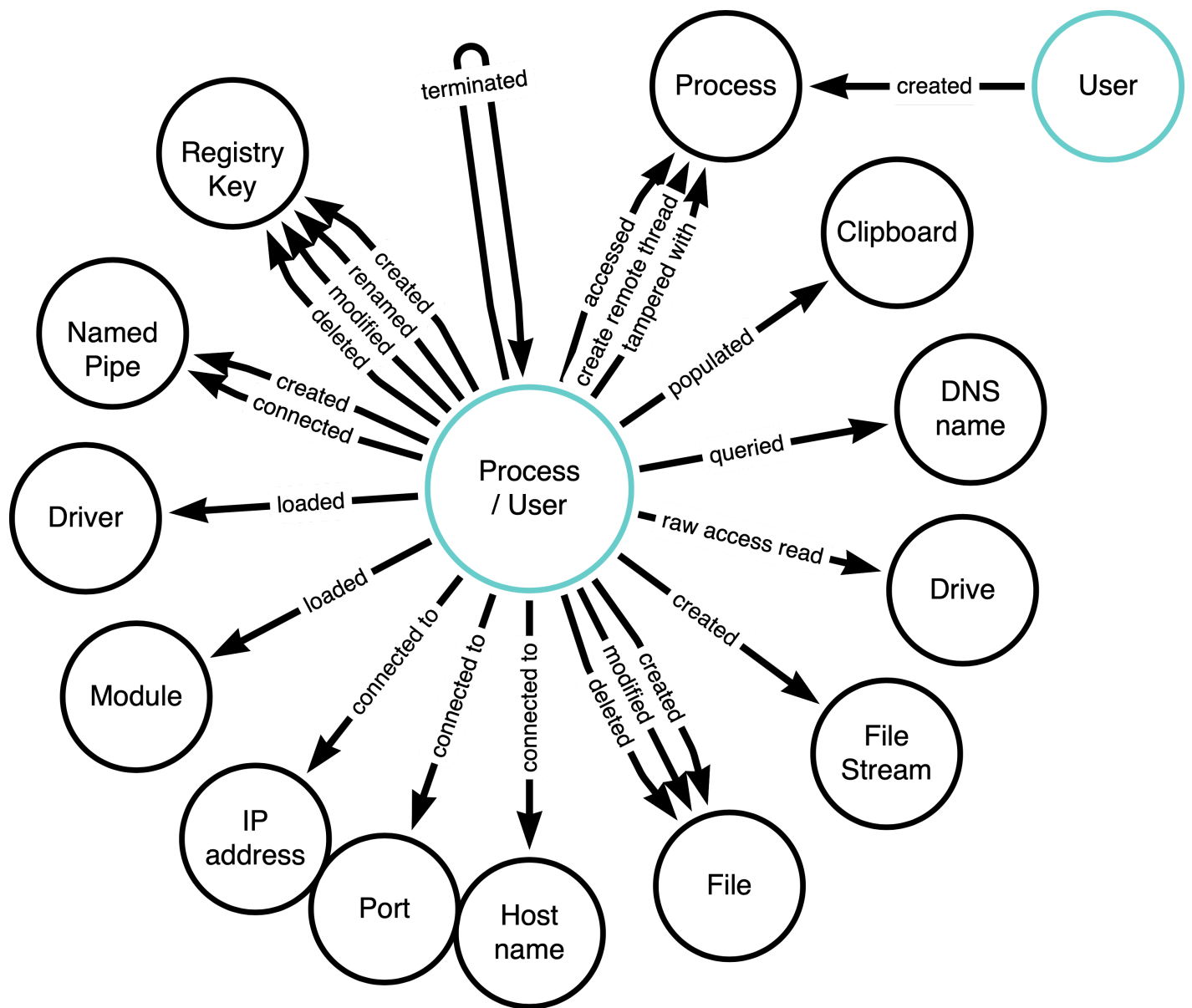


Complete the installation.

## 5. Installing and Configuring Sysmon for Windows

### What is Sysmon?

Sysmon is part of the [Sysinternals suite](#) and is useful for extending the default Windows logs with higher-level monitoring of events and process creations. Sysmon contains detailed information about process creations, networks connections, and file changes.



## Sysmon Event ID's

- Event ID 1: Process creation
- Event ID 2: A process changed a file creation time
- Event ID 3: Network connection
- Event ID 4: Sysmon service state changed
- Event ID 5: Process terminated
- Event ID 6: Driver loaded
- Event ID 7: Image loaded
- Event ID 8: CreateRemoteThread
- Event ID 9: RawAccessRead
- Event ID 10: ProcessAccess
- Event ID 11: FileCreate
- Event ID 12: RegistryEvent (Object create and delete)



- Event ID 13: RegistryEvent (Value Set)
- Event ID 14: RegistryEvent (Key and Value Rename)
- Event ID 15: FileCreateStreamHash
- Event ID 16: ServiceConfigurationChange
- Event ID 17: PipeEvent (Pipe Created)
- Event ID 18: PipeEvent (Pipe Connected)
- Event ID 19: WmiEvent (WmiEventFilter activity detected)
- Event ID 20: WmiEvent (WmiEventConsumer activity detected)
- Event ID 21: WmiEvent (WmiEventConsumerToFilter activity detected)
- Event ID 22: DNSEvent (DNS query)
- Event ID 23: FileDelete (File Delete archived)
- Event ID 24: ClipboardChange (New content in the clipboard)
- Event ID 25: ProcessTampering (Process image change)
- Event ID 26: FileDeleteDetected (File Delete logged)
- Event ID 255: Error

[Learn](#) / [Sysinternals](#) /


⊕

✎

⋮

# Sysmon v15.15

Article • 07/23/2024 • 10 contributors

 [Feedback](#)

## 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 \(GitHub\)](#) 

You can Download the Sysmon From the this Link : <https://download.sysinternals.com/files/Sysmon.zip>

To Run the Sysmon under set of rule for Splunk we are using Sysmon Olaf Config : <https://github.com/olafhartong/sysmon-modular/blob/master/sysmonconfig.xml>

After Downloading both of the File, we will Install Sysmon using the olaf Config

```
.\Sysmon64.exe -i .\sysmonconfig.xml
```

Create `inputs.conf` to define the log sources and save it in `C:\Program Files\SplunkUniversalForwarder\etc\system\local`.

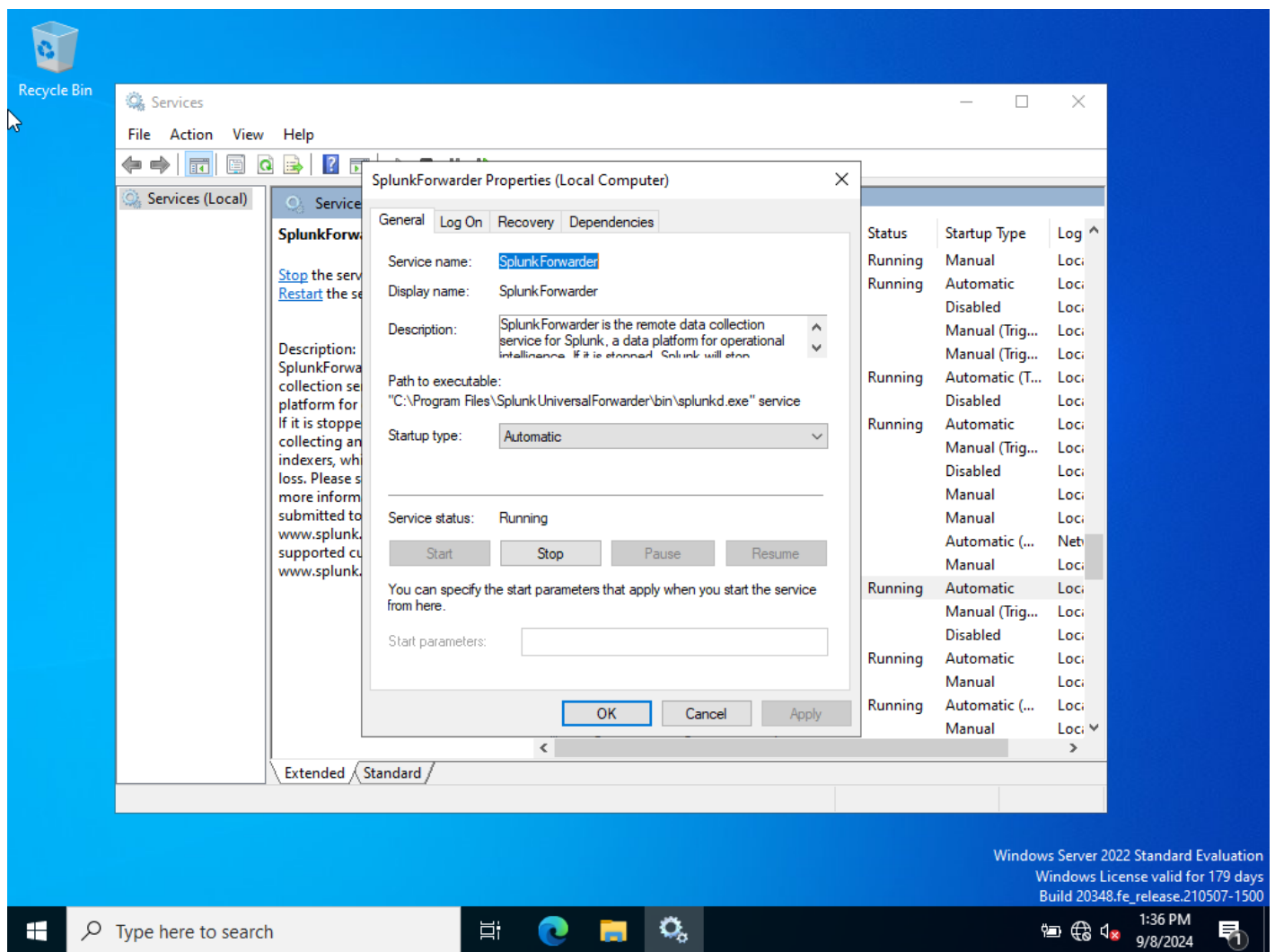
```
[WinEventLog://Application]
index = endpoint
disabled = false

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

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

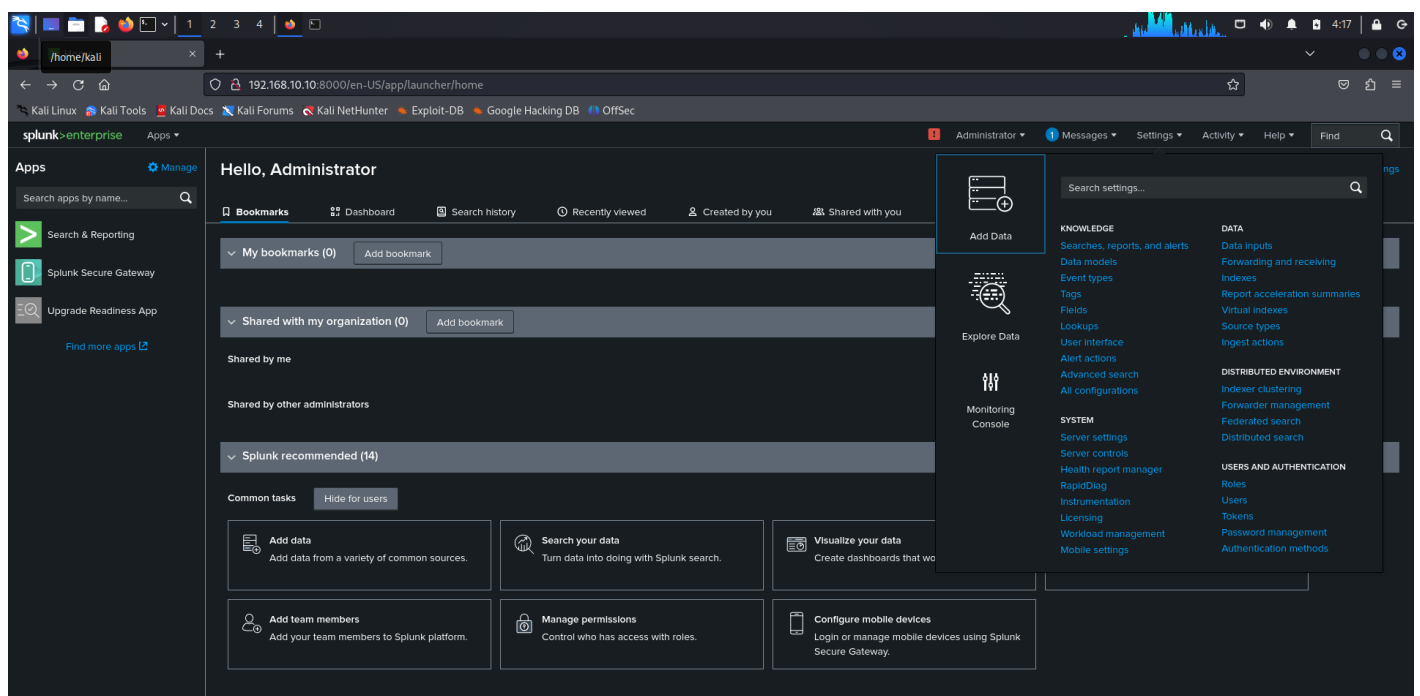
[WinEventLog://Microsoft-Windows-Sysmon/Operational]
index = endpoint
disabled = false
renderXml = true
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
```

Go to the Services Section of the Windows and check if splunk and sysmon are set to automatic Start during the power on of the system.

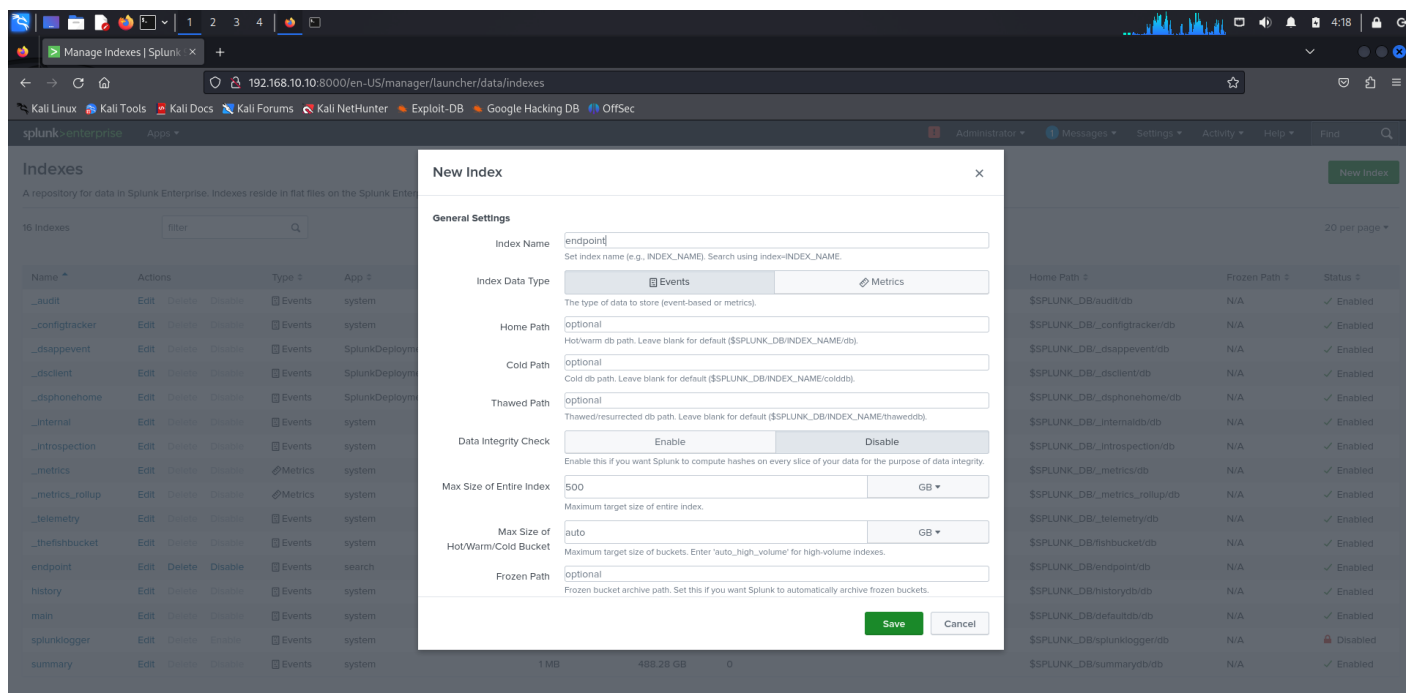


Connecting the Splunk Universal Forwarder to the Enterprise:

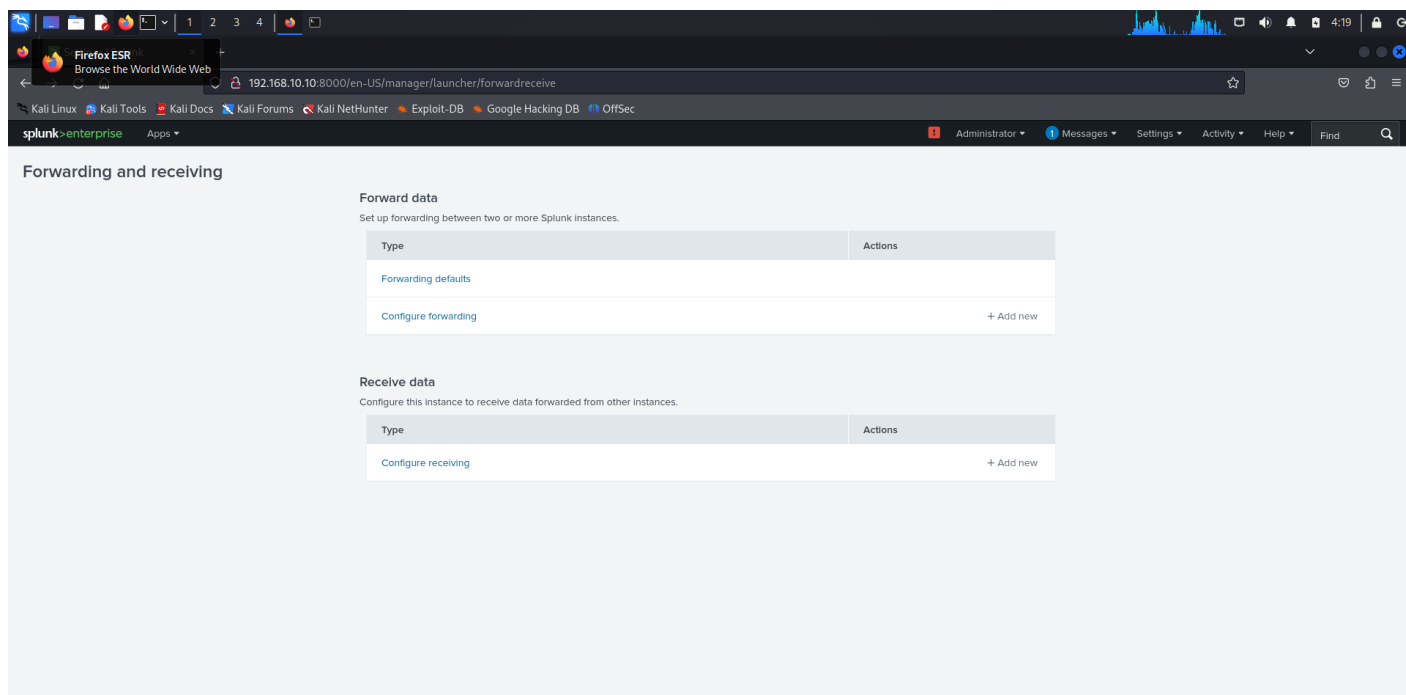
1. In the Setting of the Web GUI , go to the indexes to create a new index for the windows machine.



2. Create a new index named "endpoint" since we are sending all the data of the windows machine using the index "endpoint" in the input.conf.



3. In the Setting of the Web GUI , enter the Forwarding and Receiving tab and add the receiving data from the windows maching by specifying the port 9997.



4. In the Search and reporting section of the Web GUI , Search for the index="endpoint " to get all the data collected from the Windows Machine.

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with 'splunk>enterprise' and various tabs like 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'Search' tab is active, showing a 'New Search' page. The search query is 'index='endpoint'' and it has found 711 events. The search results are displayed in a table with columns for 'Time' and 'Event'. The first event is from 9/7/24 5:15:16.000 PM and contains XML data. The second event is from 9/7/24 5:15:00.000 PM and contains log data. The third event is from 9/7/24 5:15:00.000 PM and contains log data. The interface also includes a sidebar with 'SELECTED FIELDS' and 'INTERESTING FIELDS'.

Time	Event
9/7/24 5:15:16.000 PM	<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385f-c22a-43e0-bf4c-06f5638ffbd9}' /><EventID>11</EventID><Version>2</Version><Level>4</Level><Task>11</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime='2024-09-07T17:15:16.2076289Z' /><EventRecordID>1744</EventRecordID><Correlation></Correlation></System><EventData><Data Name='RuleName'>technique_id=T1574.010,technique_name=Services File Permissions Weakness</Data><Data Name='UtcTime'>2024-09-07 17:15:16.206</Data><Data Name='ProcessGuid'>{aad9370a-896f-66dc-1400-000000000500}</Data><Data Name='ProcessId'>352</Data><Data Name='Image'>C:\Windows\System32\svchost.exe</Data><Data Name='TargetFilename'>C:\Windows\ServiceState\EventLog\Data\lastalive1.dat</Data><Data Name='CreationUtcTime'>2024-09-07 17:13:15.384</Data></EventData></Event>
9/7/24 5:15:00.000 PM	09/07/2024 10:45:00 PM LogName=System EventCode=7036 EventType=4 ComputerName=windows Show all 12 lines host = WINDOWS source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
9/7/24 5:15:00.000 PM	09/07/2024 10:45:00 PM LogName=Application

## 6. Conclusion

This report outlines the setup of Splunk Enterprise in a virtualized environment using VirtualBox, the installation and configuration of Splunk and its Universal Forwarder, and the deployment of Sysmon for enhanced monitoring on Windows. This setup is ideal for collecting and analyzing logs from various systems, providing a robust solution for enterprise-level data analysis and security monitoring.