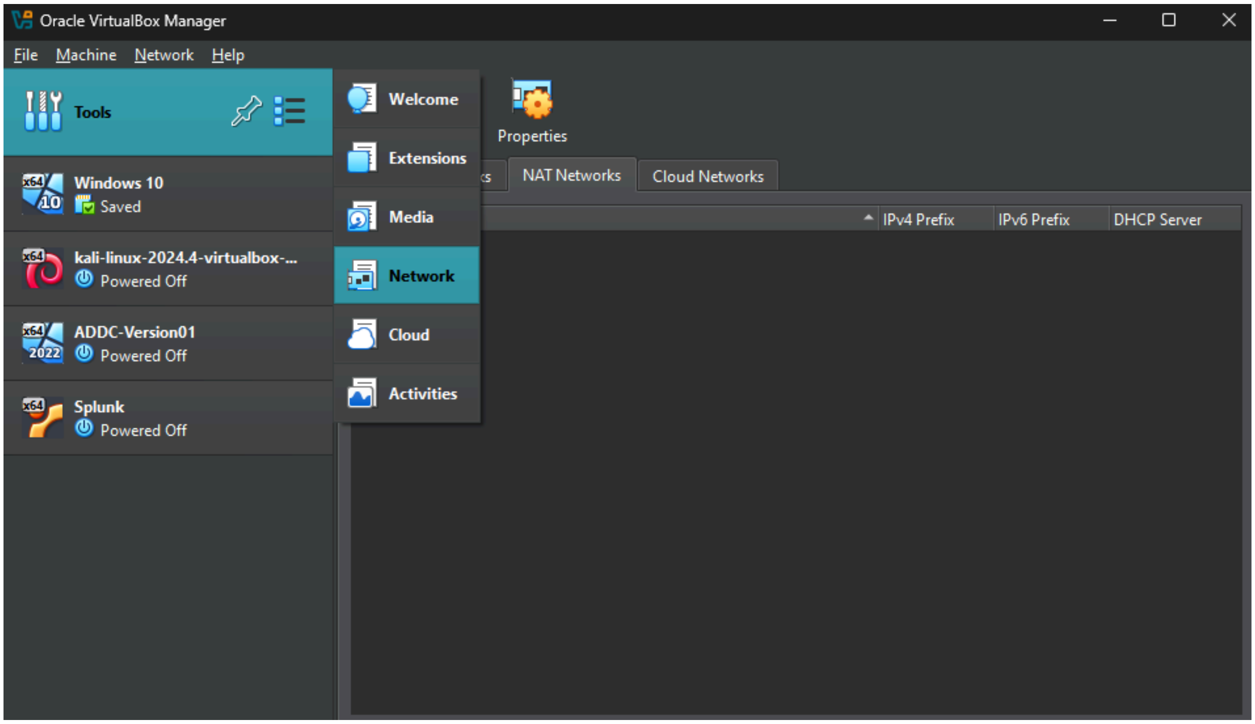
Install & Configure (Sysmon & Splunk) to Windows 10 machine and Windows Server.

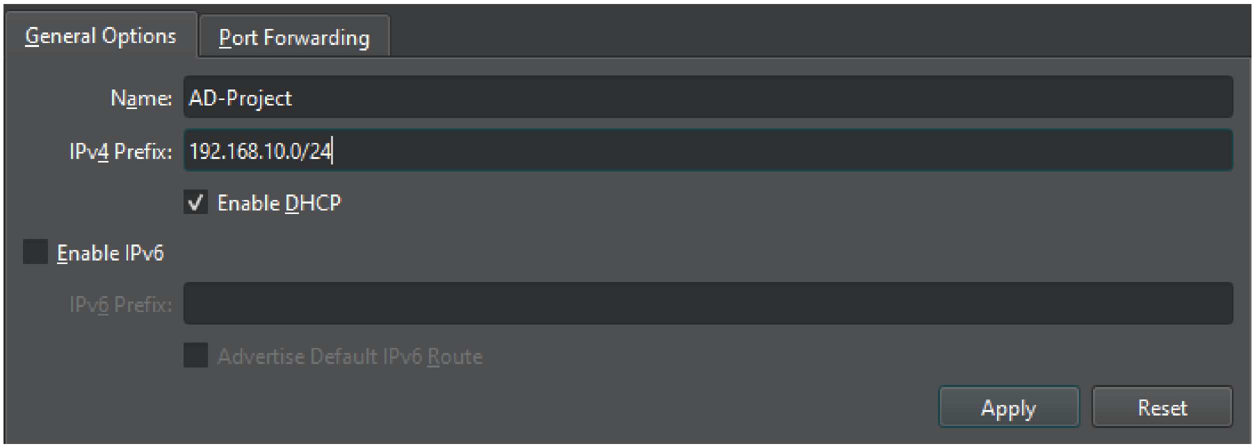
Network configure:

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.



Name: AD-Project

IPv4 Prefix: 192.168.10.0/24

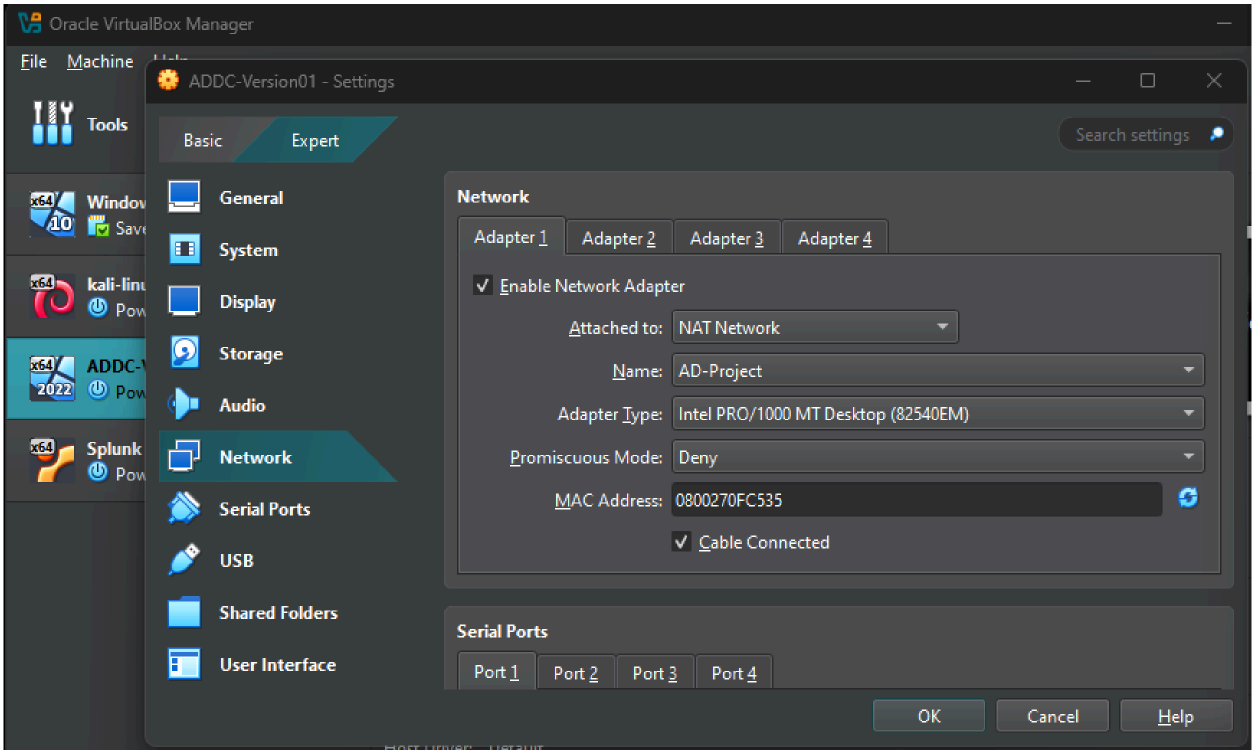
☑ Enable DHCP

□ Enable IPv6

IPv6 Prefix:

□ Advertise Default IPv6 Route

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.



Network

☑ Enable Network Adapter

Attached to: NAT Network

Name: AD-Project

Adapter Type: Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode: Deny

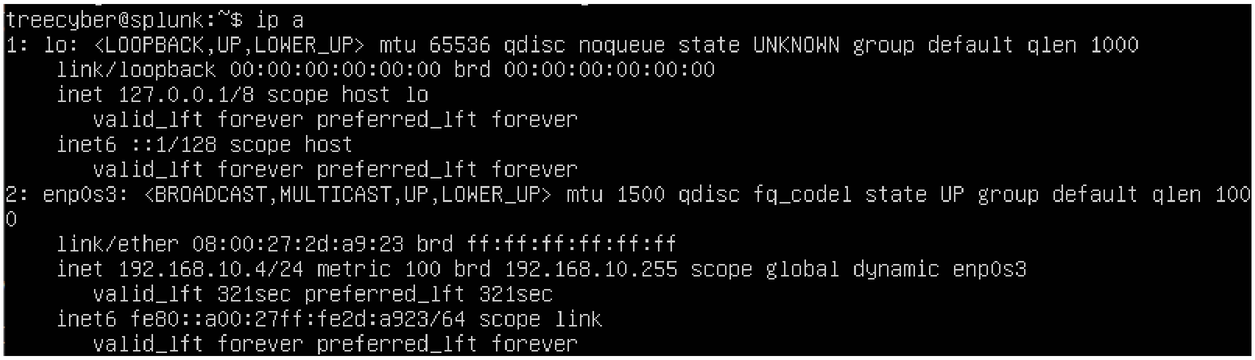
MAC Address: 0800270FC535

☑ Cable Connected

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

Splunk configure:

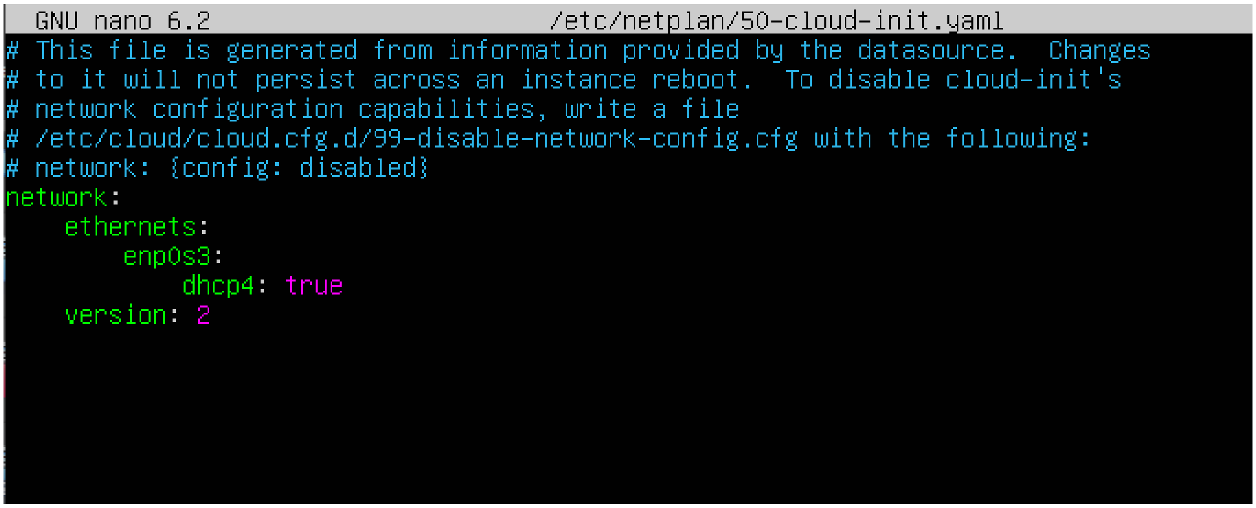
Splunk server will have a different IP then what we plan on our diagram, type `ip a` under Splunk Server VM and you can see:



```
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 192.168.10.4/24 metric 100 brd 192.168.10.255 scope global dynamic enp0s3
       valid_lft 321sec preferred_lft 321sec
    inet6 fe80::a00:27ff:fe2d:a923/64 scope link
       valid_lft forever preferred_lft forever
```

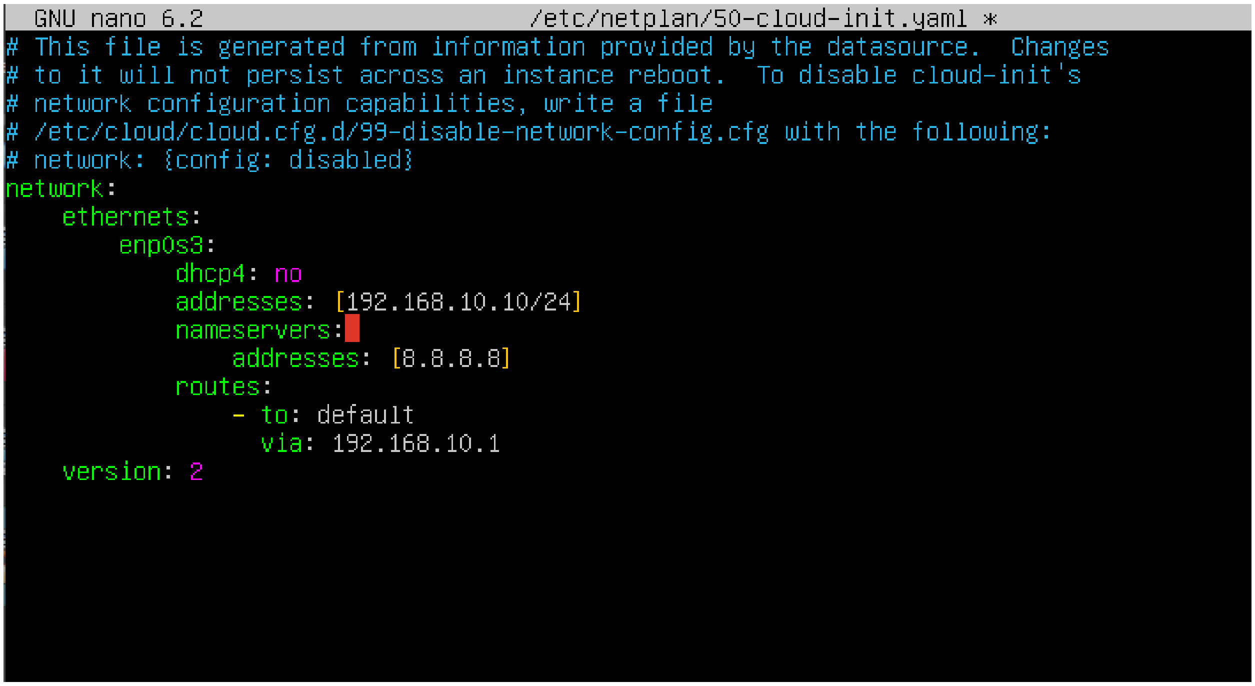
Splunk Server IP currently is `192.168.10.4` and what we plan is `192.168.10.10` . Time to set up a static IP on our Splunk Server.

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



```
  GNU nano 6.2                    /etc/netplan/50-cloud-init.yaml
# This file is generated from information provided by the datasource.  Changes
# to it will not persist across an instance reboot.  To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
    ethernets:
        enp0s3:
            dhcp4: true
    version: 2
```

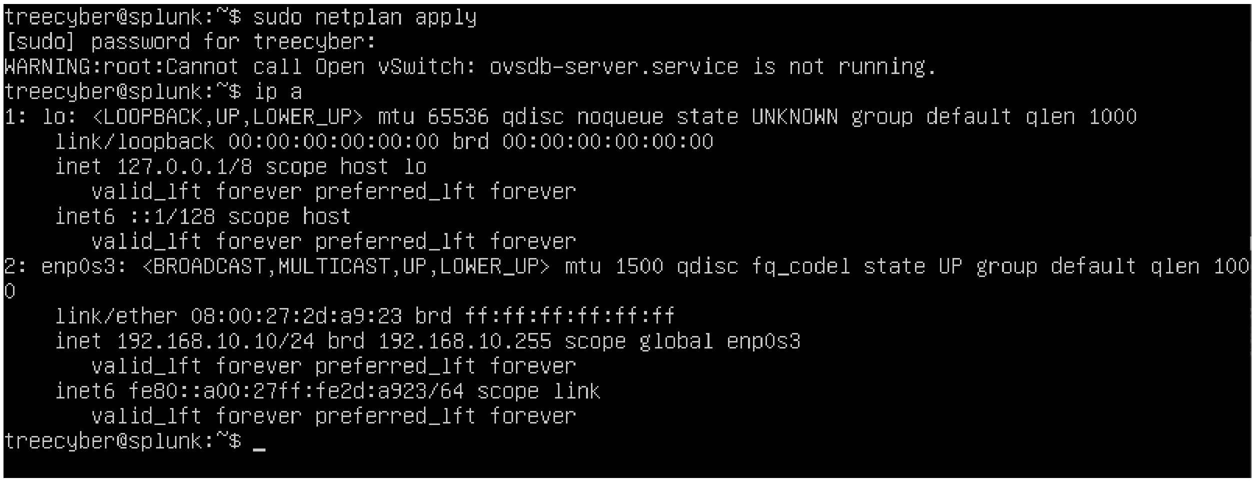
This is how you will configure:



```
  GNU nano 6.2                    /etc/netplan/50-cloud-init.yaml *
# This file is generated from information provided by the datasource.  Changes
# to it will not persist across an instance reboot.  To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
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
```

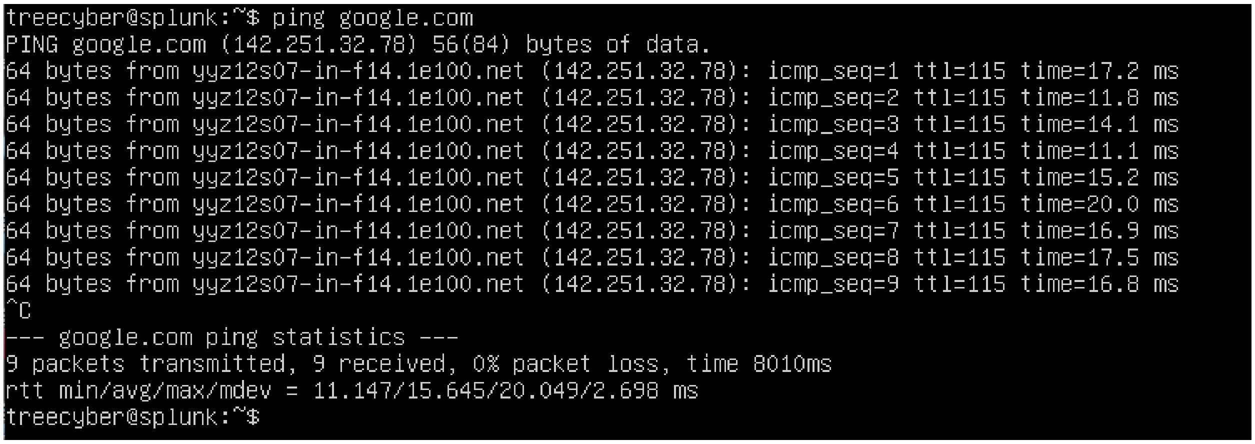
- For `nameserver`, we will set up DNS IP that you want. In this case I will use Google DNS (8.8.8.8)
- Set `no` for DHCP since we want our Splunk Server to have static IP
- We will want to add default routes for Splunk Server network setting

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:



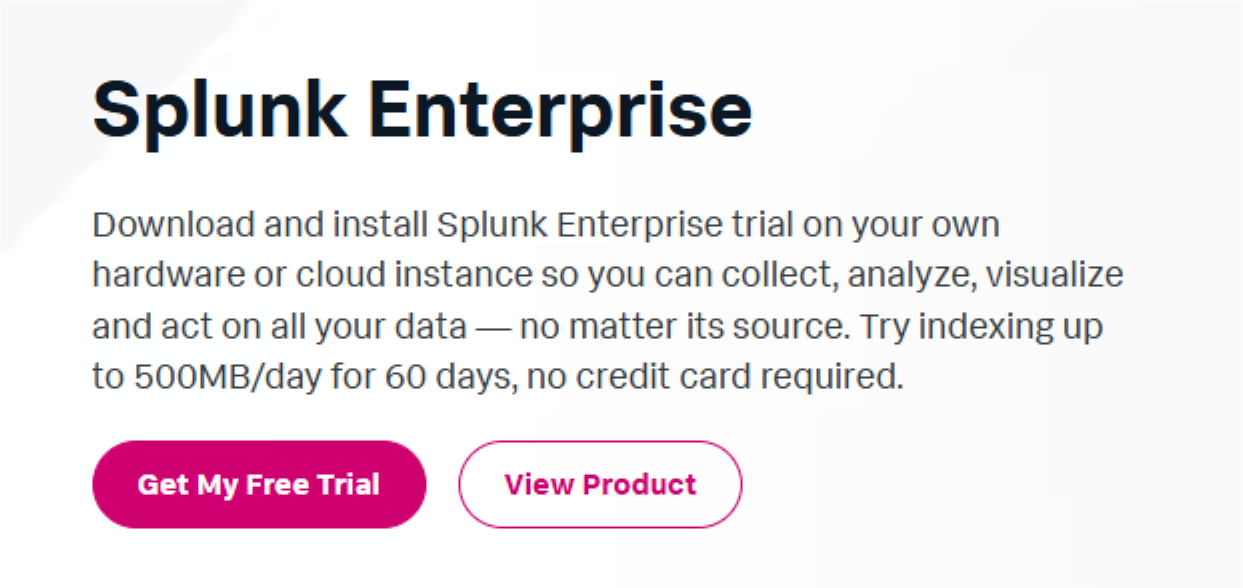
```
treecyber@splunk:~$ ping google.com
PING google.com (142.251.32.78) 56(84) bytes of data.
64 bytes from yyz12s07-in-f14.1e100.net (142.251.32.78): icmp_seq=1 ttl=115 time=17.2 ms
64 bytes from yyz12s07-in-f14.1e100.net (142.251.32.78): icmp_seq=2 ttl=115 time=11.8 ms
64 bytes from yyz12s07-in-f14.1e100.net (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.

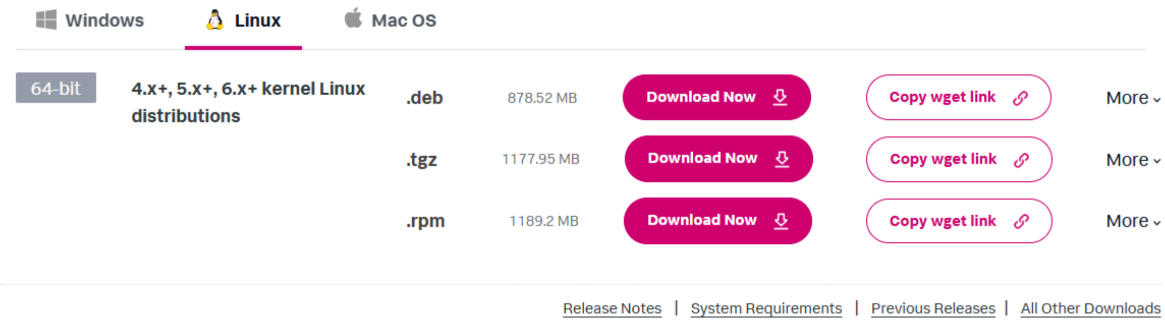
We will look to download Splunk Enterprise



Splunk Enterprise

Download and install Splunk Enterprise trial on your own hardware or cloud instance so you can collect, analyze, visualize and act on all your data — no matter its source. Try indexing up to 500MB/day for 60 days, no credit card required.

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

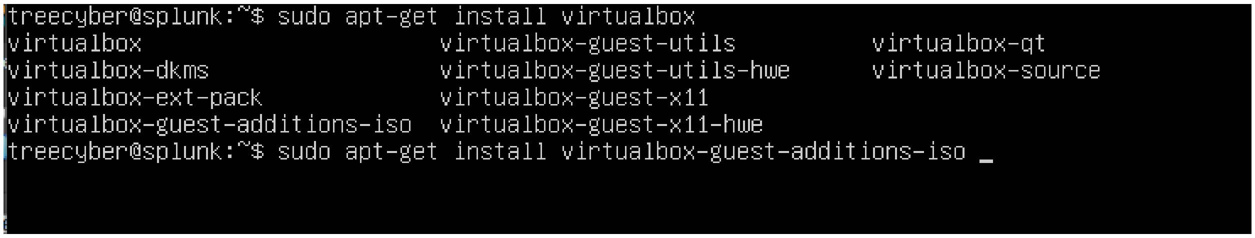


64-bit	4.x+, 5.x+, 6.x+ kernel Linux distributions	.deb	878.52 MB	Download Now	Copy wget link	More
		.tgz	1177.95 MB	Download Now	Copy wget link	More
		.rpm	1189.2 MB	Download Now	Copy wget link	More

Release Notes | System Requirements | Previous Releases | All Other Downloads

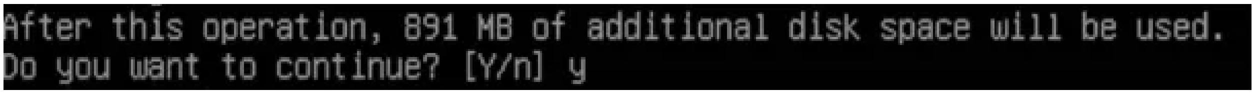
Go back to your Splunk Server VM then install the guest add-ons for virtual box.

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



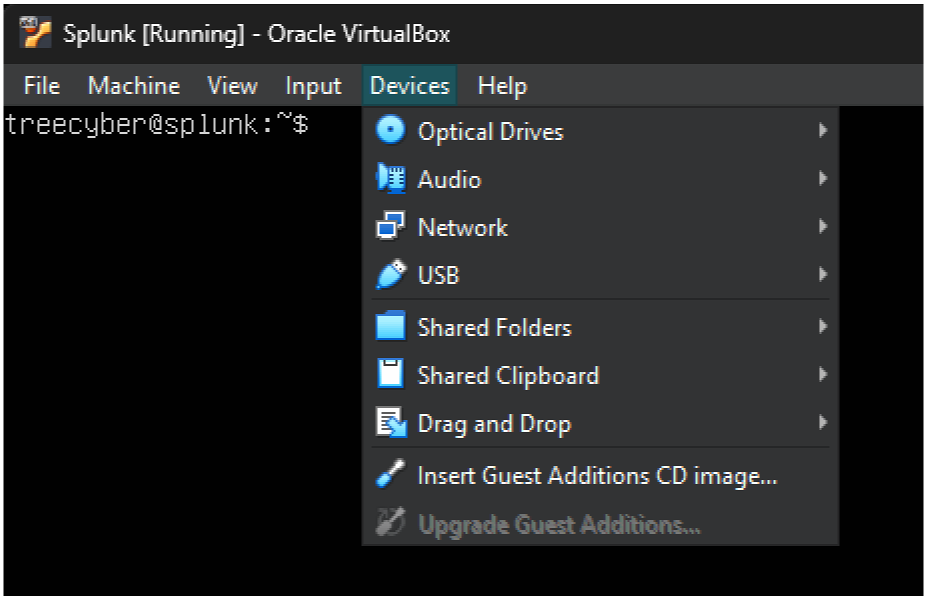
```
treecyber@splunk:~$ sudo apt-get install virtualbox
virtualbox                       virtualbox-guest-utils          virtualbox-qt
virtualbox-dkms                  virtualbox-guest-utils-hwe      virtualbox-source
virtualbox-ext-pack              virtualbox-guest-x11
virtualbox-guest-additions-iso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



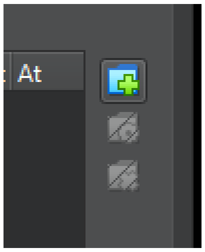
```
After this operation, 891 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

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

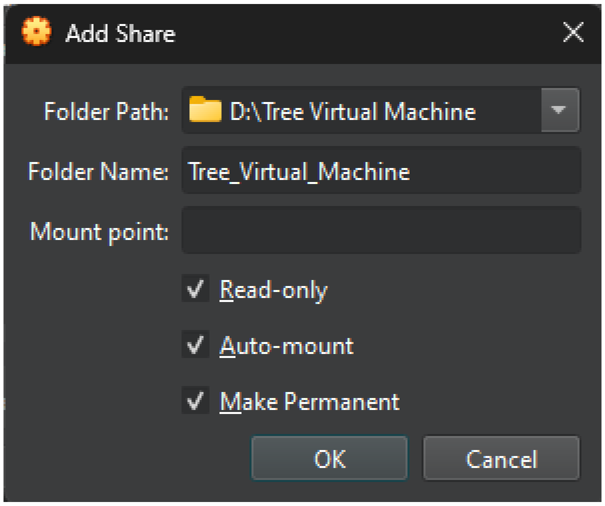


```
treecyber@splunk:~$
```

Add folder



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



Folder Path: D:\Tree Virtual Machine

Folder Name: Tree_Virtual_Machine

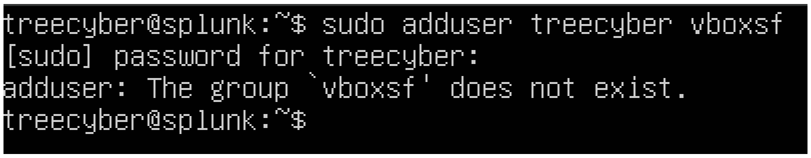
Mount point:

☑ Read-only

☑ Auto-mount

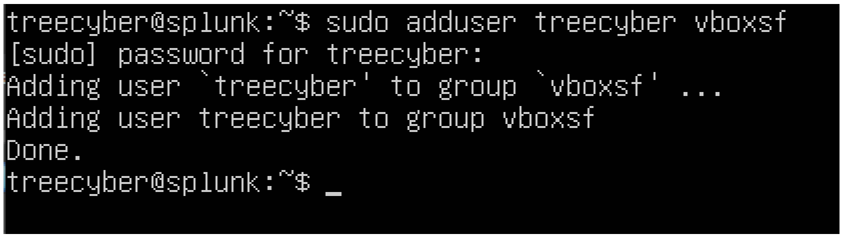
☑ Make Permanent

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:~$
```

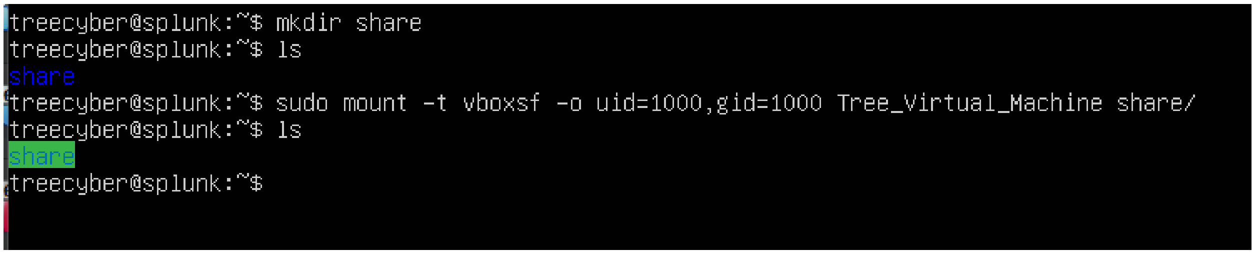
If error, we will need to install vboxsf by type `sudo apt-get install virtualbox-guest-utils` and reboot again. Try to add user again and it should work:



```
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:~$ _
```

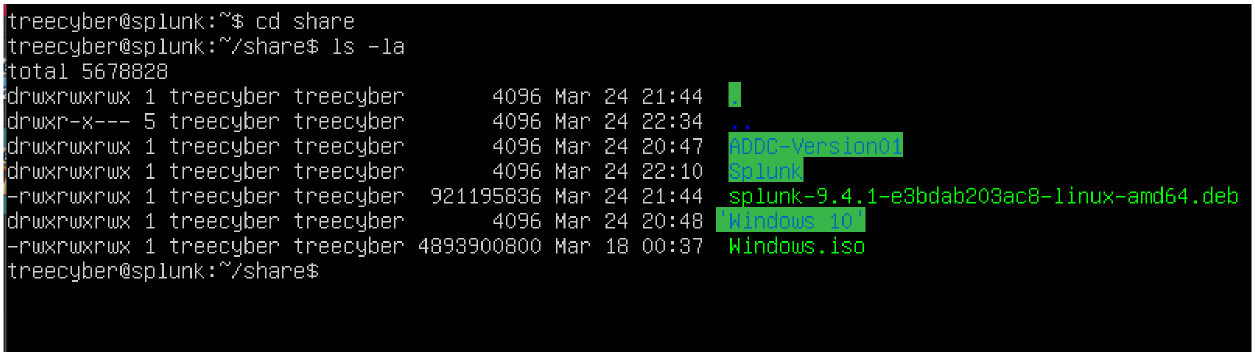
Let create a new directory call *share* with `mkdir share` and we will run a command to mount our shared folder onto our *share* directory we just create.

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



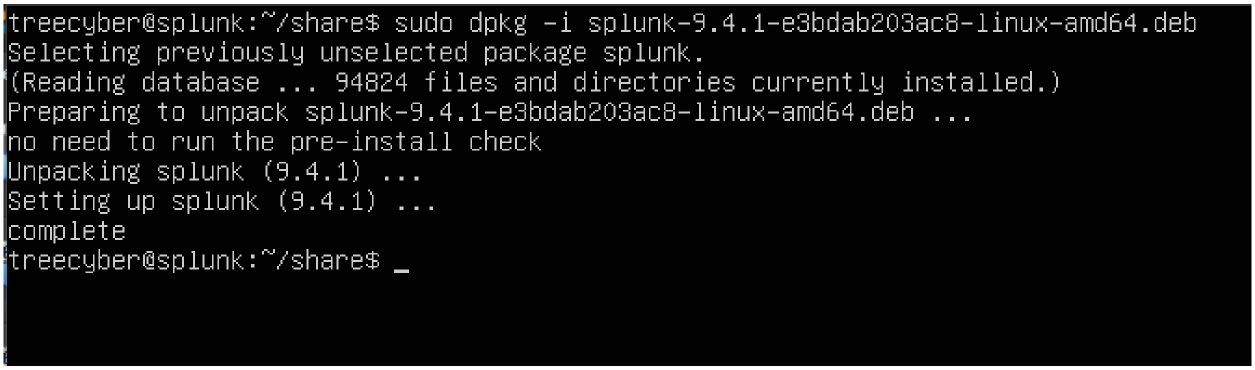
```
treecyber@splunk:~$ mkdir share
treecyber@splunk:~$ ls
share
treecyber@splunk:~$ sudo mount -t vboxsf -o uid=1000,gid=1000 Tree_Virtual_Machine share/
treecyber@splunk:~$ ls
share
treecyber@splunk:~$
```

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



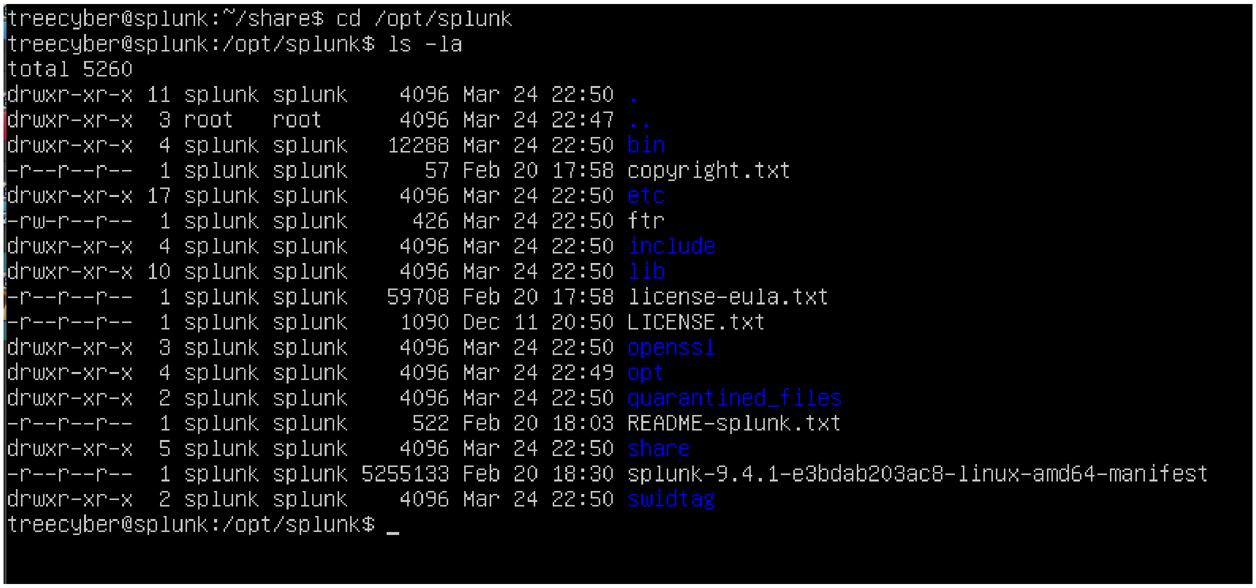
```
treecyber@splunk:~$ cd share
treecyber@splunk:~/share$ ls -la
total 5678828
drwxrwxrwx 1 treecyber treecyber       4096 Mar 24 21:44  .
drwxr-x--- 5 treecyber treecyber       4096 Mar 24 22:34  ..
drwxrwxrwx 1 treecyber treecyber       4096 Mar 24 20:47  ADDC-Version01
drwxrwxrwx 1 treecyber treecyber       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)`



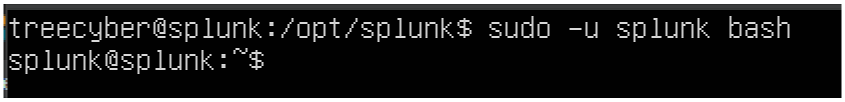
```
treecyber@splunk:~/share$ sudo dpkg -i splunk-9.4.1-e3bdab203ac8-linux-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 94824 files and directories currently installed.)
Preparing to unpack splunk-9.4.1-e3bdab203ac8-linux-amd64.deb ...
no need to run the pre-install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



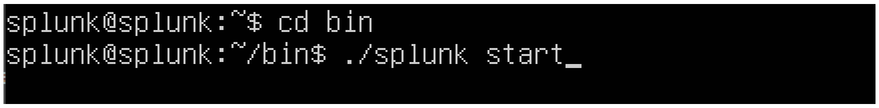
```
treecyber@splunk:~/share$ cd /opt/splunk
treecyber@splunk:/opt/splunk$ ls -la
total 5260
drwxr-xr-x 11 splunk splunk    4096 Mar 24 22:50 .
drwxr-xr-x  3 root   root      4096 Mar 24 22:47 ..
drwxr-xr-x  4 splunk splunk   12288 Mar 24 22:50 bin
-r--r--r--  1 splunk splunk      57 Feb 20 17:58 copyright.txt
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`



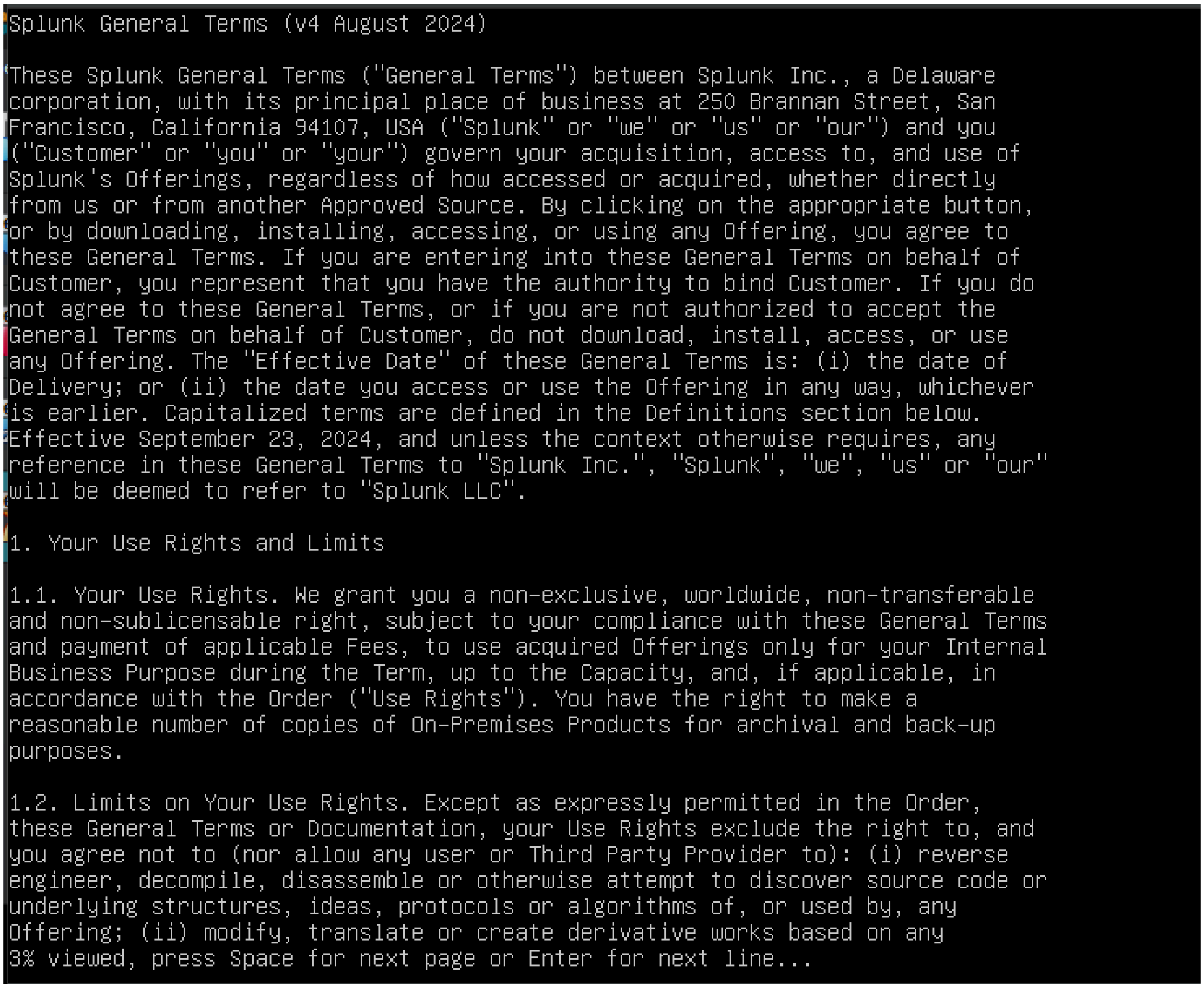
```
treecyber@splunk:/opt/splunk$ sudo -u splunk bash
splunk@splunk:~$
```

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



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

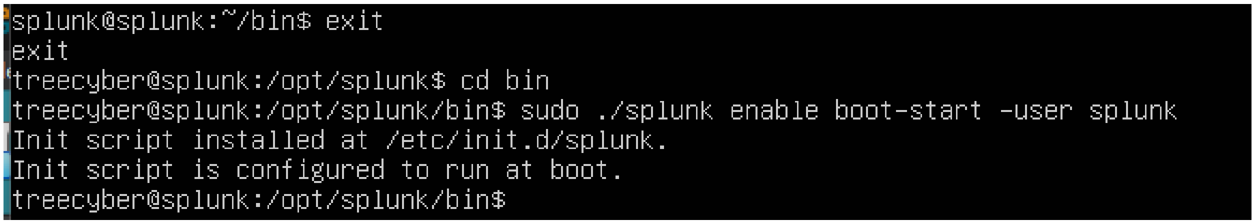
Hit Enter and it will prompt the license, term and agreement



```
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$
```

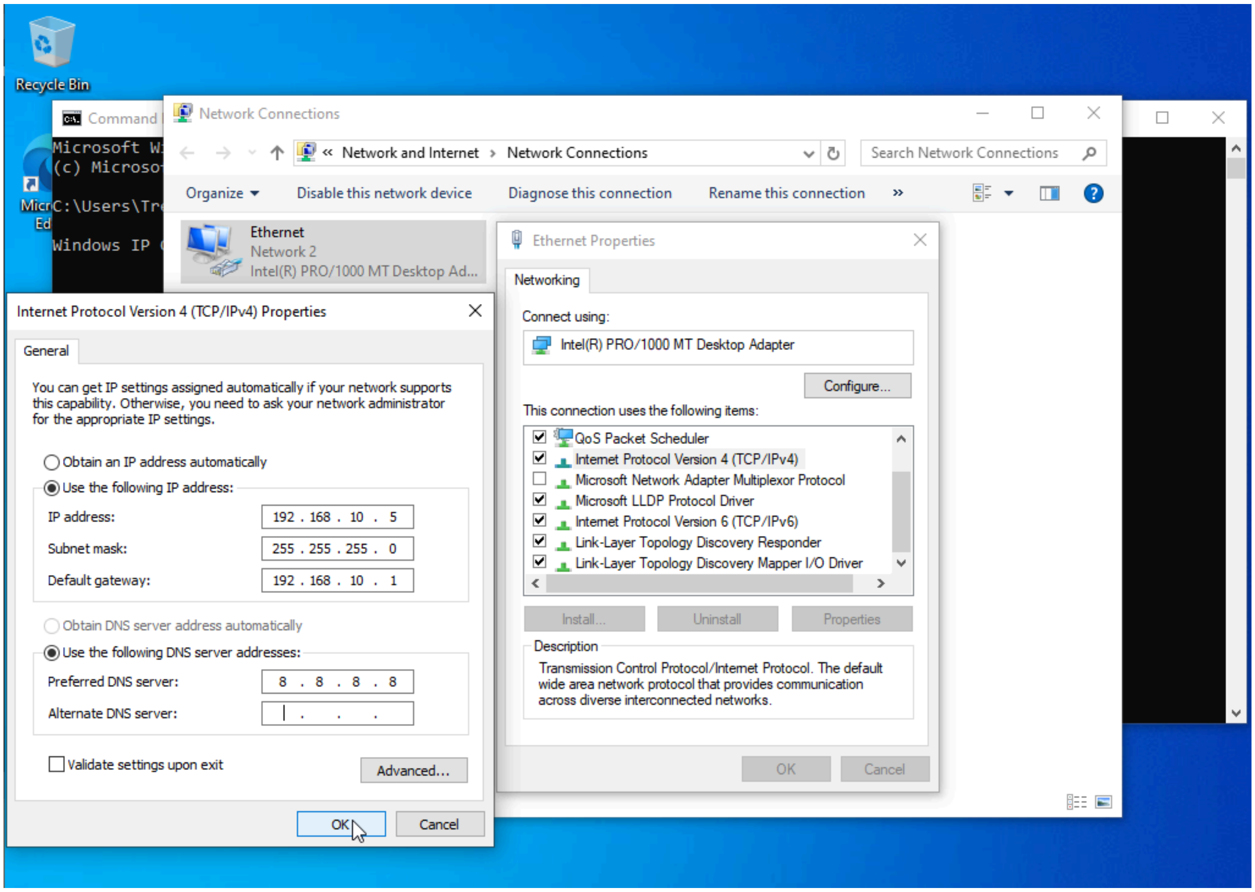
We had successfully install Splunk to our Splunk Server VM

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



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:	192 . 168 . 10 . 5
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 10 . 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

Ethernet Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Desktop Adapter

Configure...

This connection uses the following items:

- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Link-Layer Topology Discovery Responder
- ☑ Link-Layer Topology Discovery Mapper I/O Driver

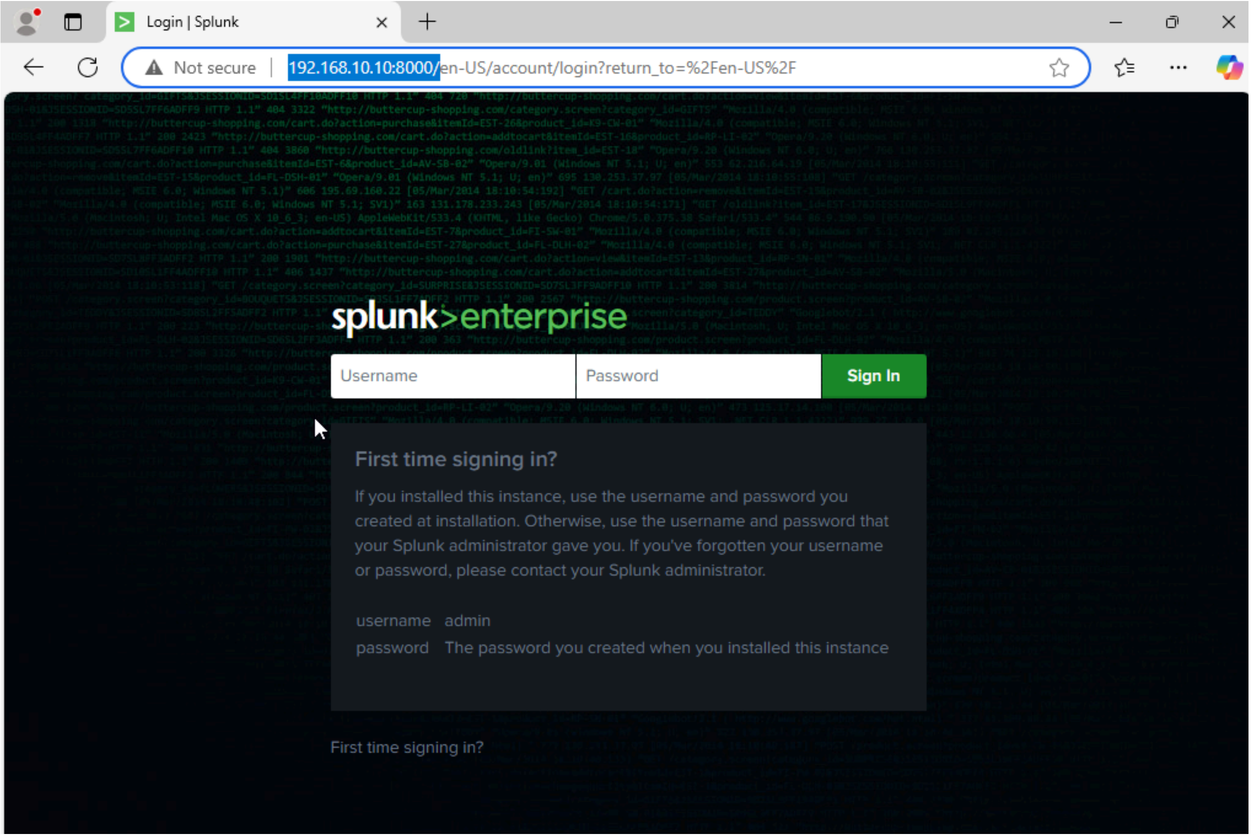
Install... Uninstall Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel

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)



Login | Splunk

Not secure | 192.168.10.10:8000/en-US/account/login?return_to=%2Fen-US%2F

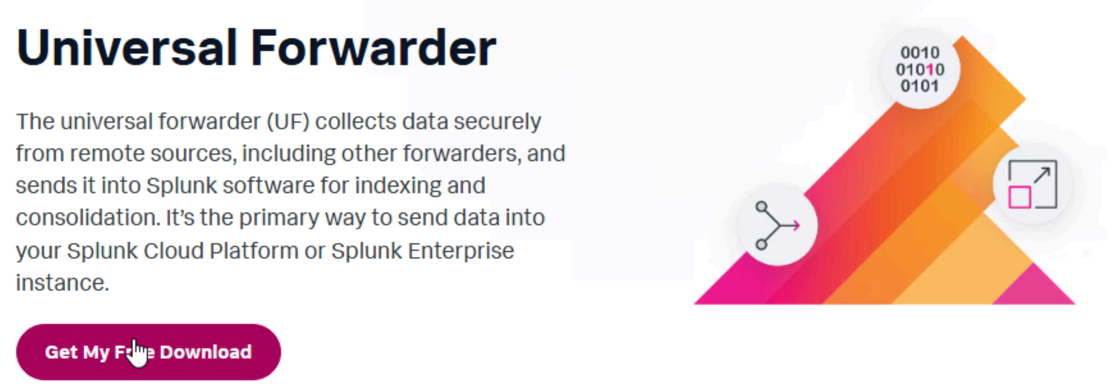
First time signing in?

If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.

username admin
password The password you created when you installed this instance

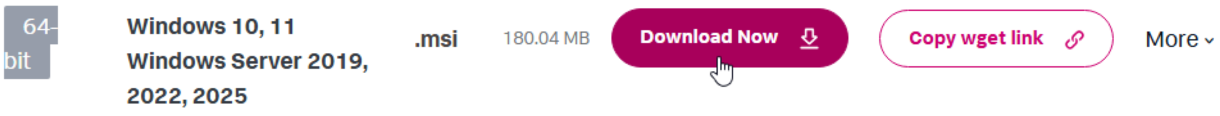
First time signing in?

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



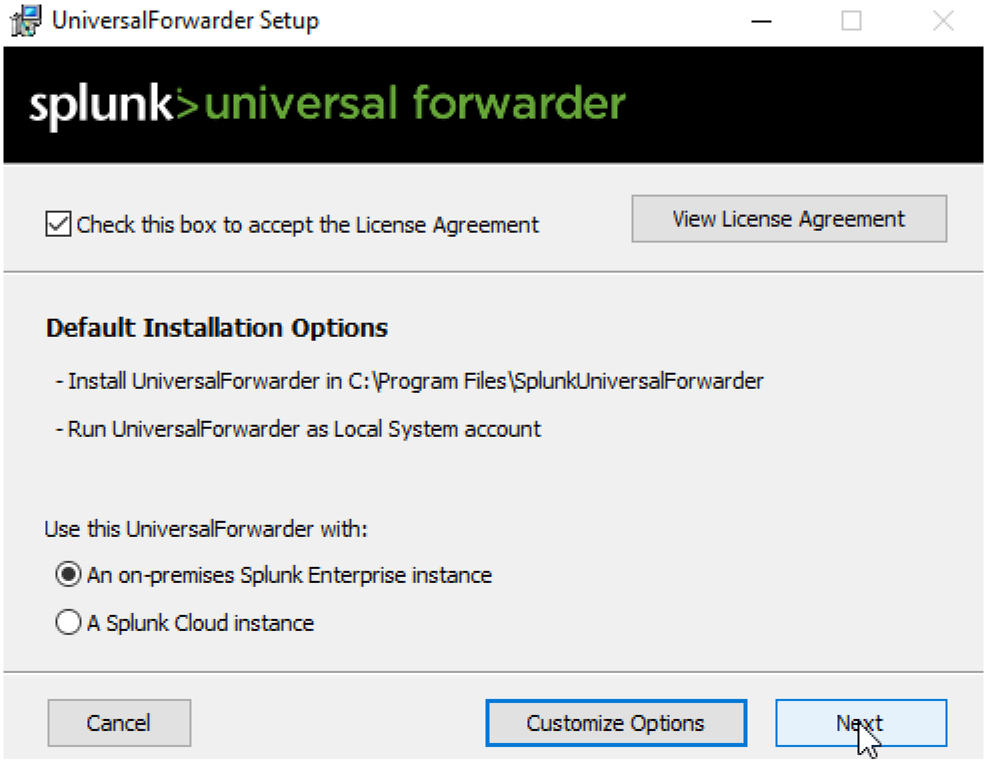
Universal Forwarder

The universal forwarder (UF) collects data securely from remote sources, including other forwarders, and sends it into Splunk software for indexing and consolidation. It's the primary way to send data into your Splunk Cloud Platform or Splunk Enterprise instance.



64-bit	Windows 10, 11 Windows Server 2019, 2022, 2025	.msi	180.04 MB	Download Now	Copy wget link	More ⌄

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



UniversalForwarder Setup

splunk>universal forwarder

☑ Check this box to accept the License Agreement

Default Installation Options

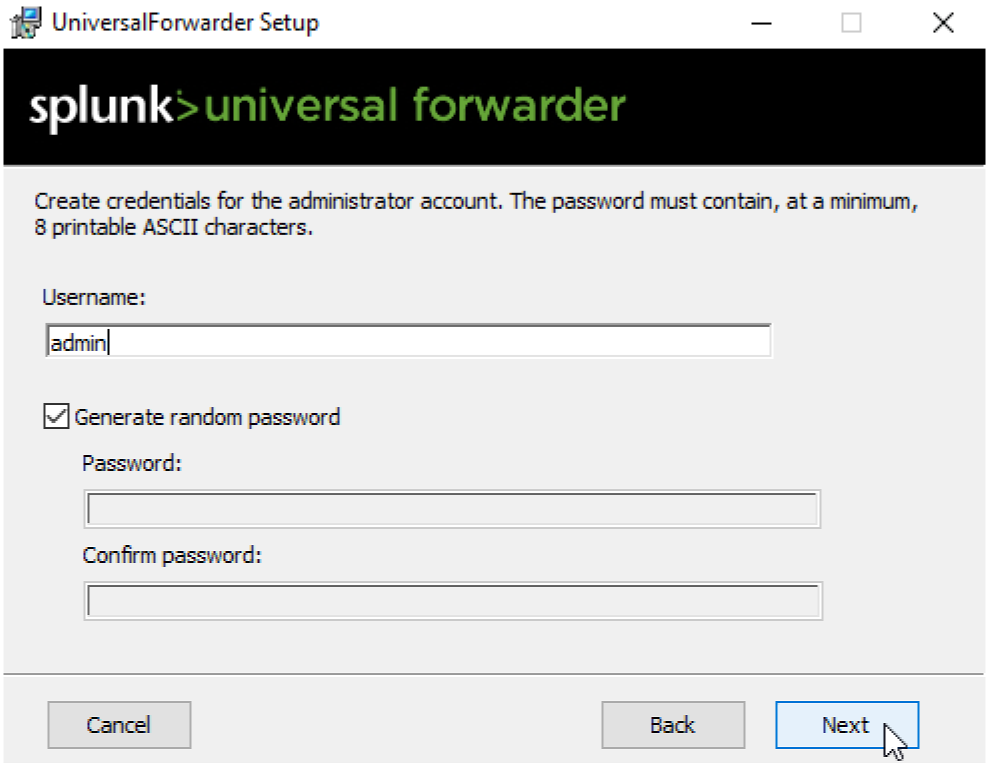
- Install UniversalForwarder in C:\Program Files\SplunkUniversalForwarder

- Run UniversalForwarder as Local System account

Use this UniversalForwarder with:

● An on-premises Splunk Enterprise instance

○ A Splunk Cloud instance



UniversalForwarder Setup

splunk>universal forwarder

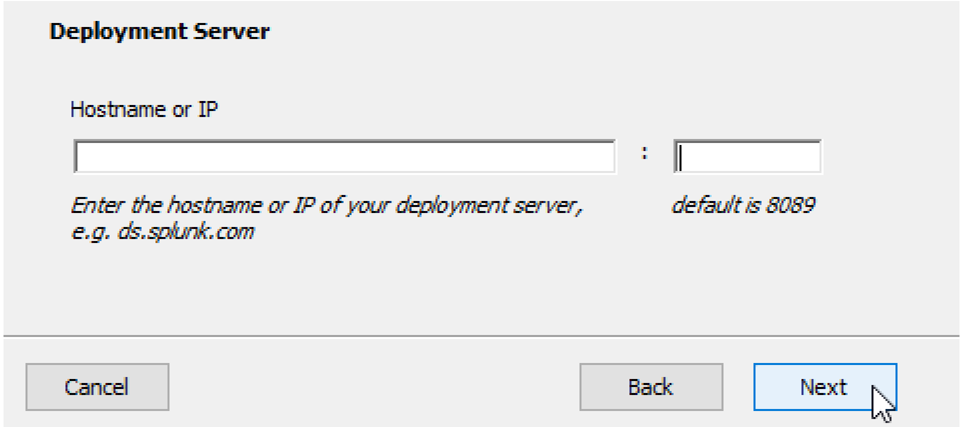
Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

Username: admin

☑ Generate random password

Password:

Confirm password:



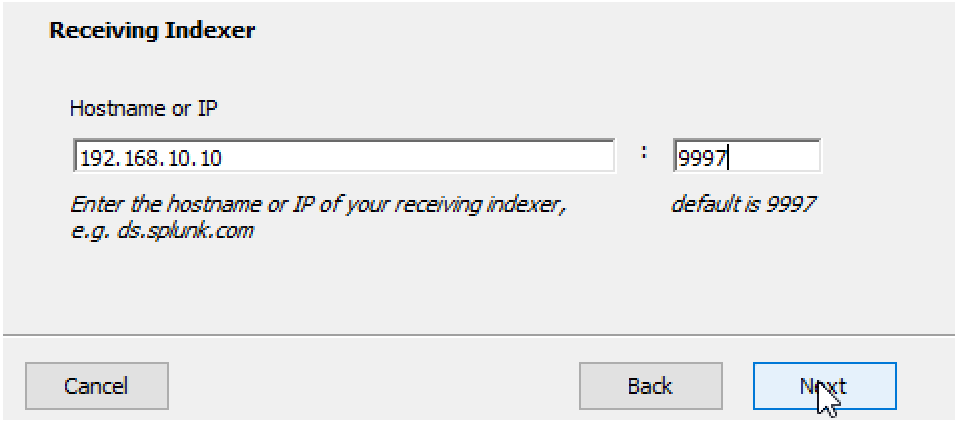
Deployment Server

Hostname or IP

:

Enter the hostname or IP of your deployment server, e.g. ds.splunk.com

default is 8089



Receiving Indexer

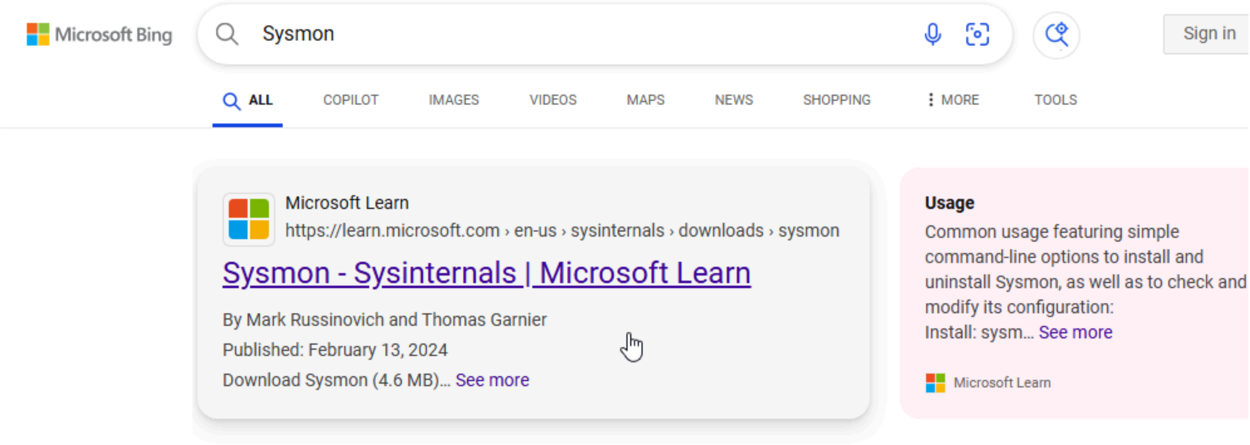
Hostname or IP

192.168.10.10 : 9997

Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com

default is 9997

Start downloading Sysmon after:



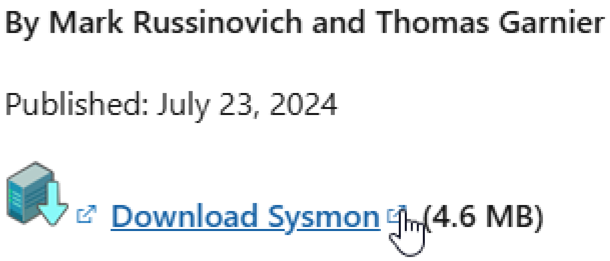
Microsoft Learn
https://learn.microsoft.com › en-us › sysinternals › downloads › sysmon

Sysmon - Sysinternals | Microsoft Learn

By Mark Russinovich and Thomas Garnier
Published: February 13, 2024
Download Sysmon (4.6 MB)... See more

Usage
Common usage featuring simple command-line options to install and uninstall Sysmon, as well as to check and modify its configuration:
Install: sysm... See more

Microsoft Learn



By Mark Russinovich and Thomas Garnier

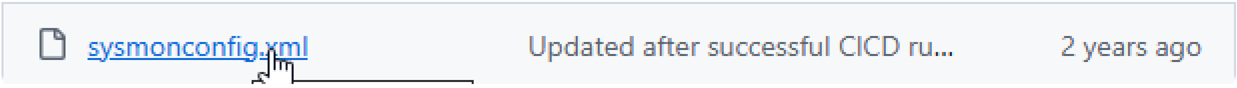
Published: July 23, 2024

Download Sysmon (4.6 MB)

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

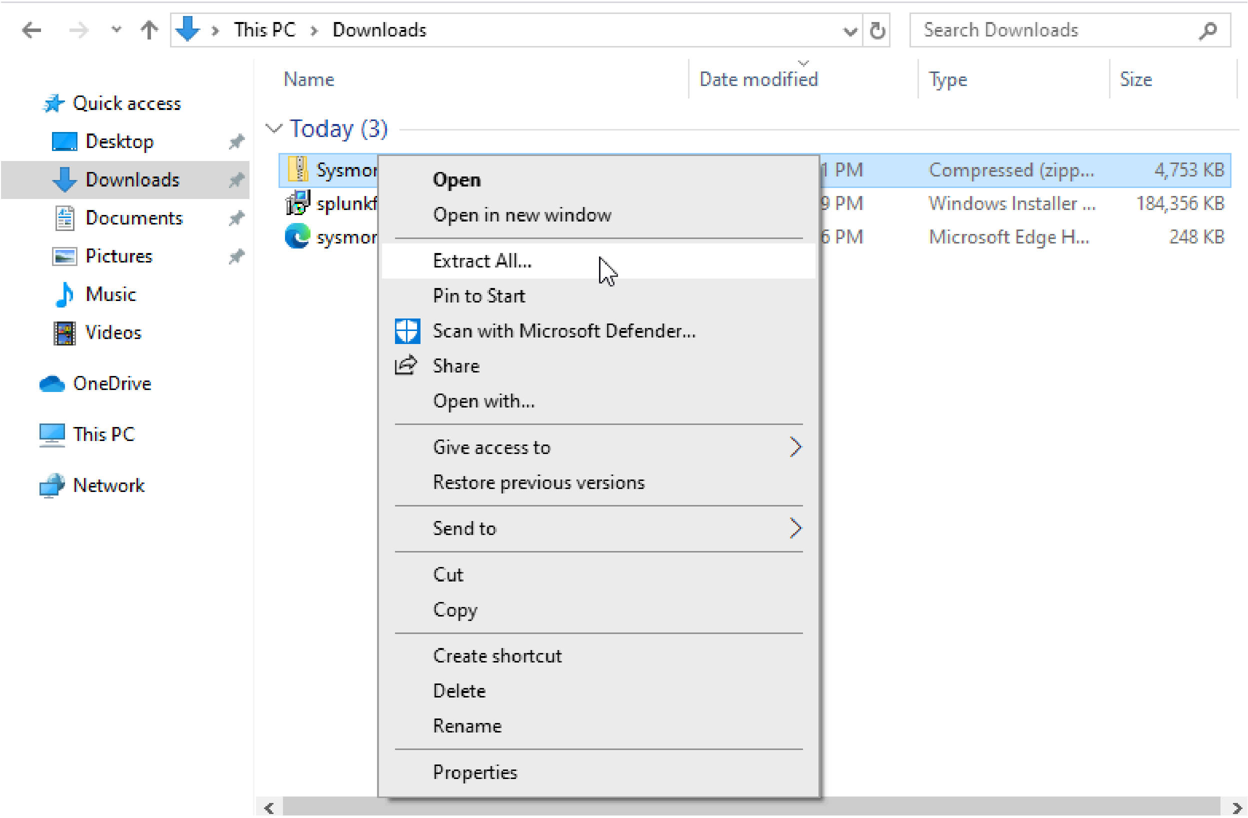
```
https://github.com/olafhartong/sysmon-modular
```

This will be the file we want to dowload:

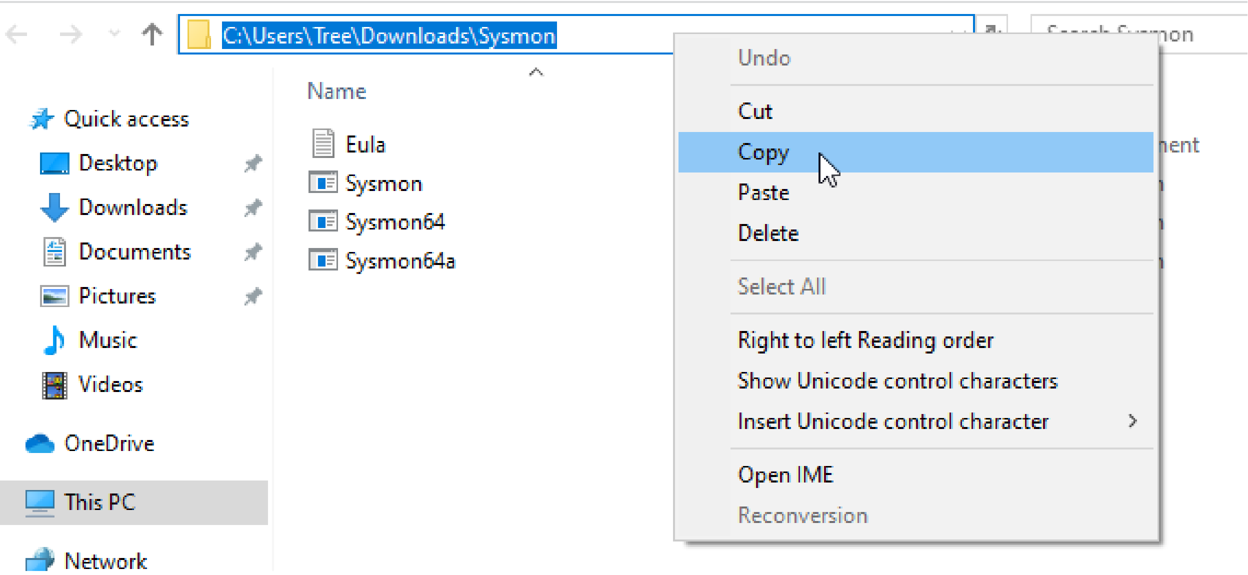


sysmonconfig.xml	Updated after successful CICD ru...	2 years ago

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

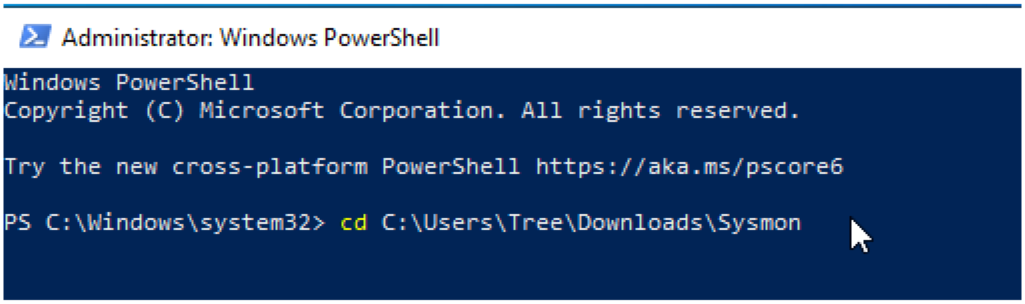


Copy and paste the extract folder path:



C:\Users\Tree\Downloads\Sysmon

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



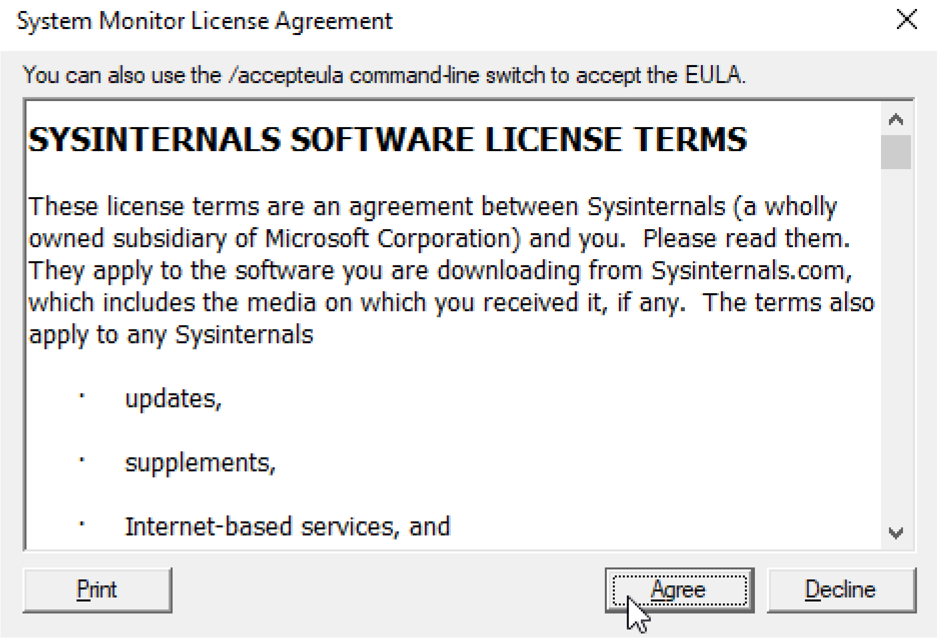
Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> cd C:\Users\Tree\Downloads\Sysmon
```

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



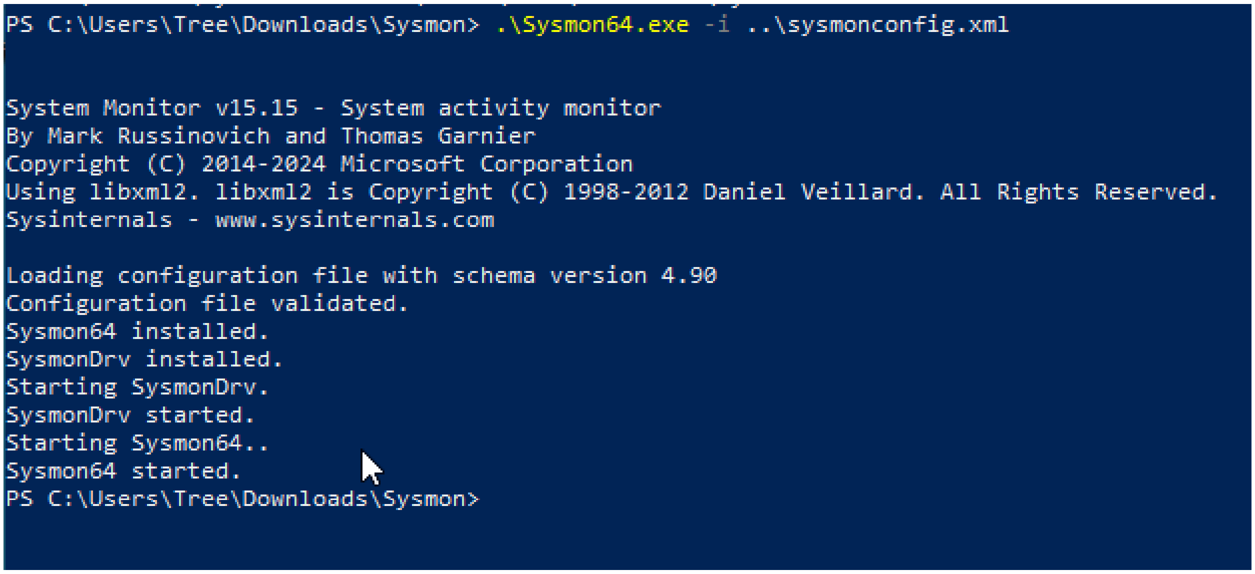
System Monitor License Agreement

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

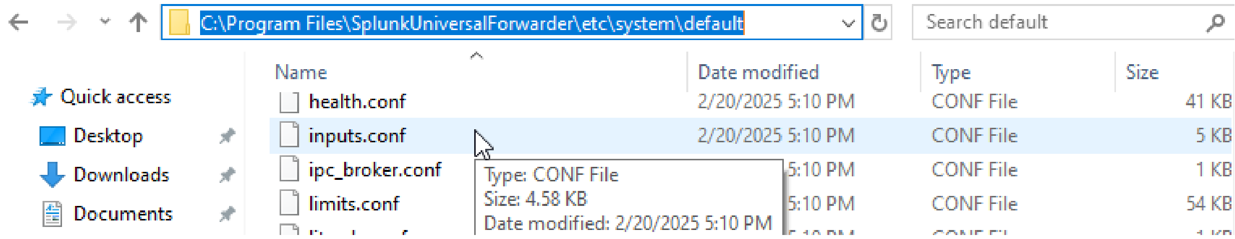
- updates,
- supplements,
- Internet-based services, and



```
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



C:\Program Files\SplunkUniversalForwarder\etc\system\default
Search default
Quick access
Desktop
Downloads
Documents

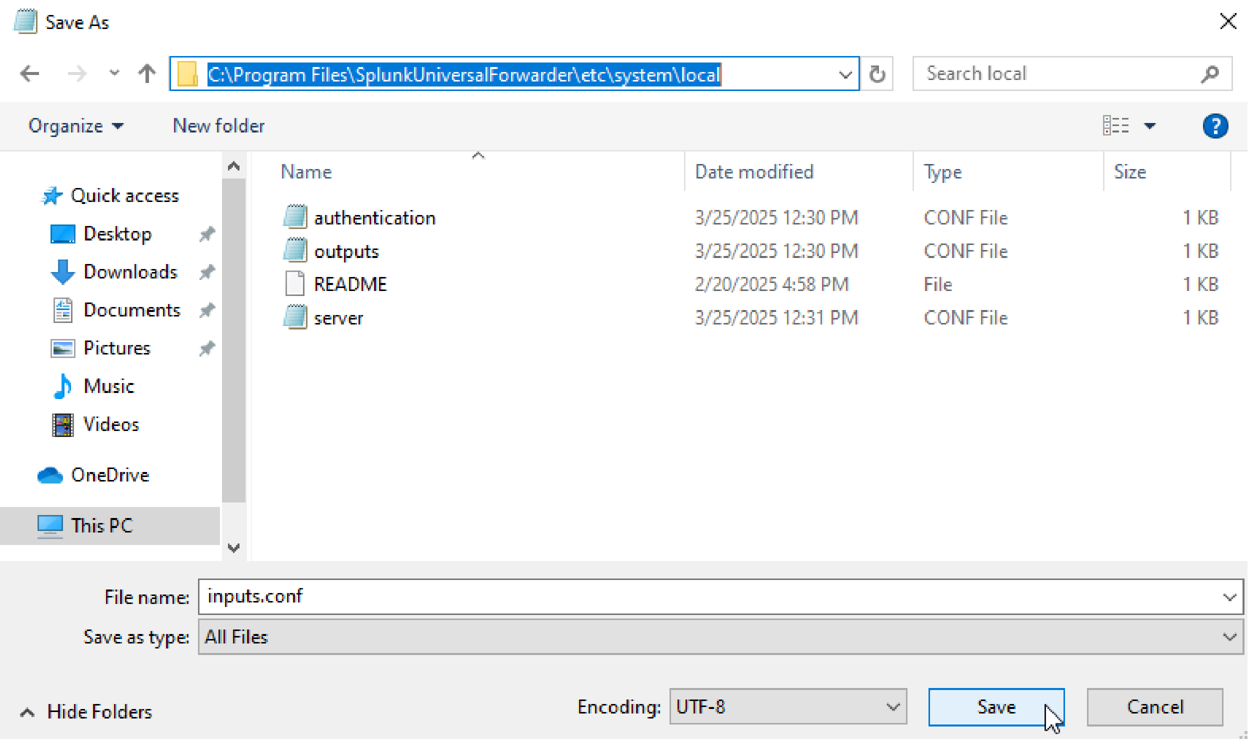
Name	Date modified	Type	Size
health.conf	2/20/2025 5:10 PM	CONF File	41 KB
inputs.conf	2/20/2025 5:10 PM	CONF File	5 KB
ipc_broker.conf	5:10 PM	CONF File	1 KB
limits.conf	5:10 PM	CONF File	54 KB

Type: CONF File
Size: 4.58 KB
Date modified: 2/20/2025 5:10 PM

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
```

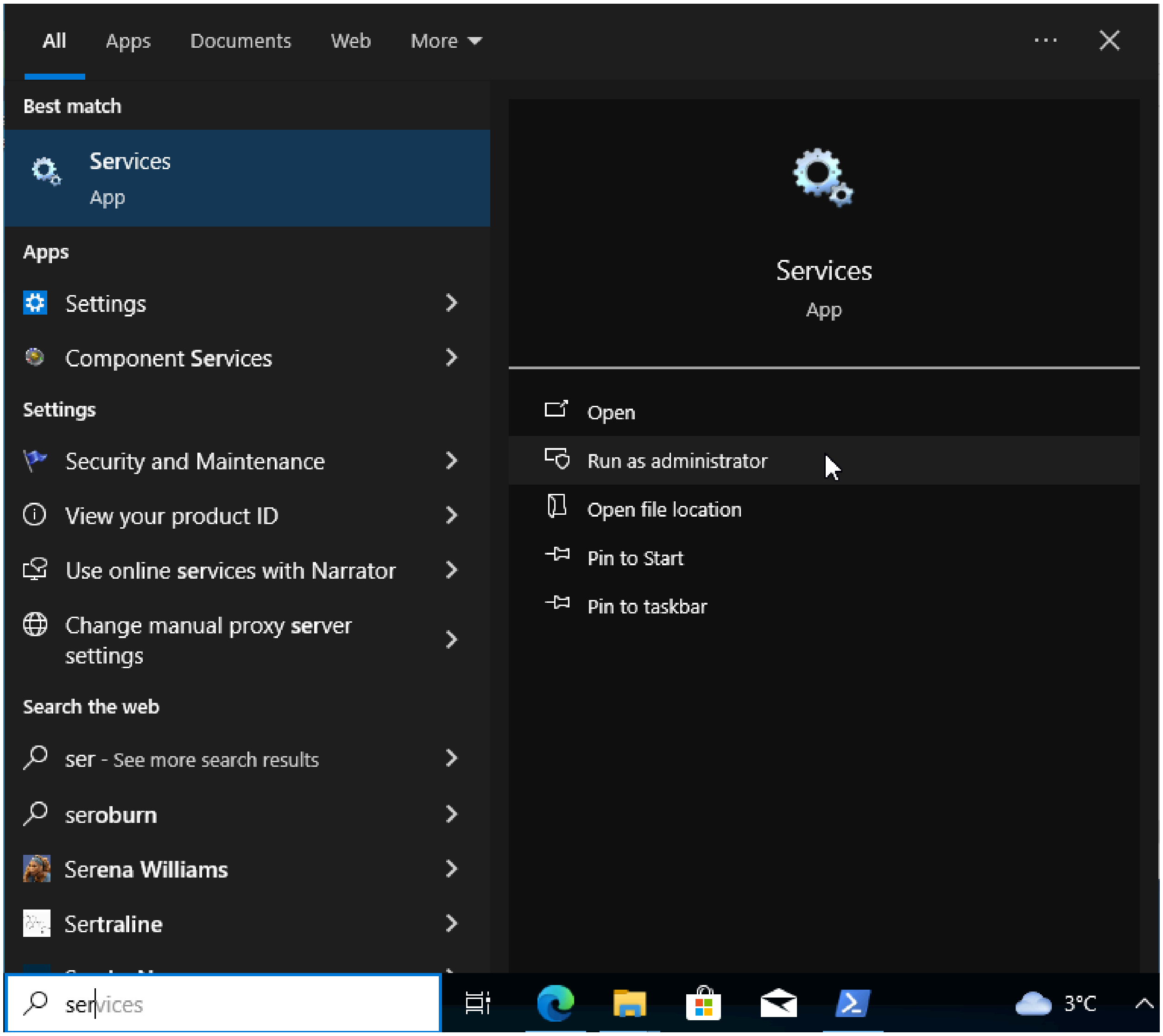


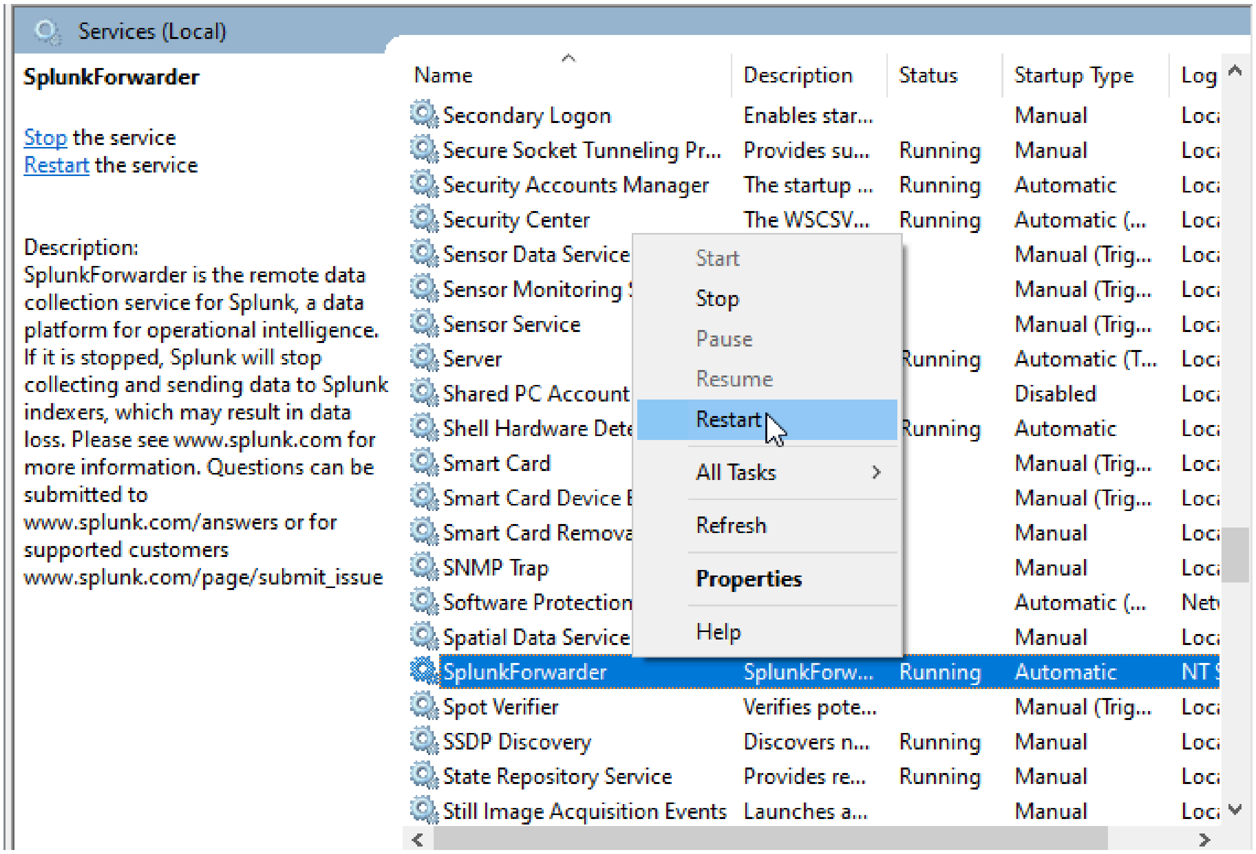
C:\Program Files\SplunkUniversalForwarder\etc\system\local

Name	Date modified	Type	Size
authentication	3/25/2025 12:30 PM	CONF File	1 KB
outputs	3/25/2025 12:30 PM	CONF File	1 KB
README	2/20/2025 4:58 PM	File	1 KB
server	3/25/2025 12:31 PM	CONF File	1 KB

File name: inputs.conf
Save as type: All Files
Encoding: UTF-8

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
App
Open
Run as administrator
Open file location
Pin to Start
Pin to taskbar
services
3°C



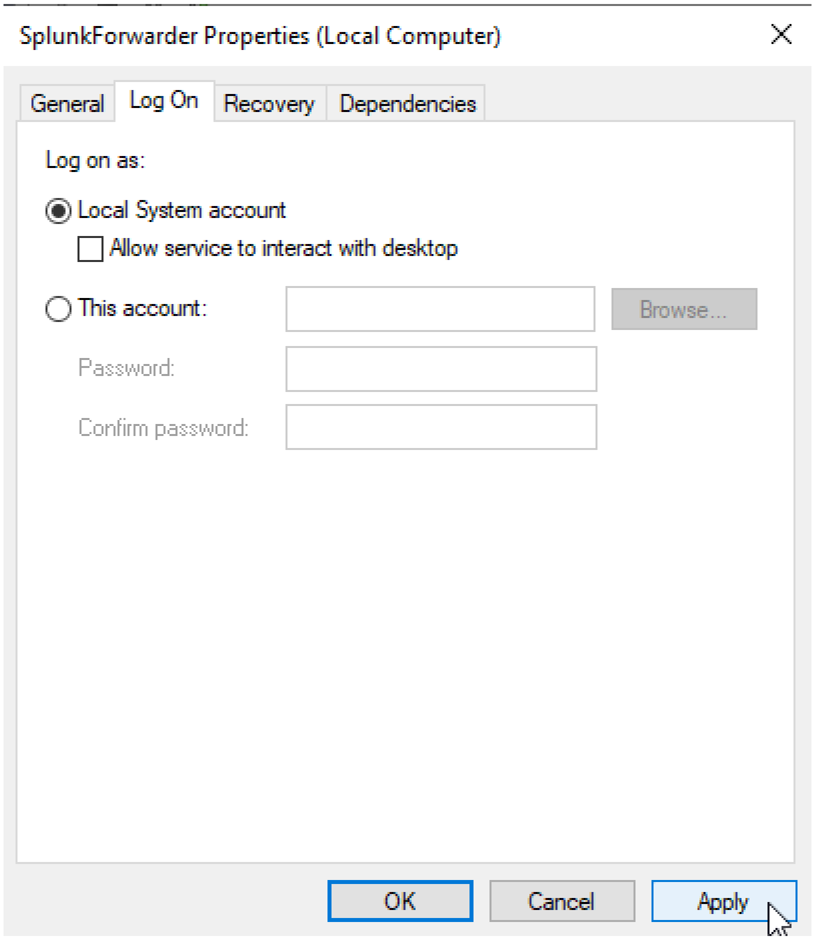
SplunkForwarder

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...	Running	Manual	Loc
Security Accounts Manager	The startup ...	Running	Automatic	Loc
Security Center	The WSCSV...	Running	Automatic (...	Loc
Sensor Data Service			Manual (Trig...	Loc
Sensor Monitoring !			Manual (Trig...	Loc
Sensor Service			Manual (Trig...	Loc
Server		Running	Automatic (T...	Loc
Shared PC Account			Disabled	Loc
Shell Hardware Dete		Running	Automatic	Loc
Smart Card			Manual (Trig...	Loc
Smart Card Device E			Manual (Trig...	Loc
Smart Card Remova			Manual	Loc
SNMP Trap			Manual	Loc
Software Protection			Automatic (...	Net
Spatial Data Service			Manual	Loc
SplunkForwarder	SplunkForw...	Running	Automatic	NT S
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

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



SplunkForwarder Properties (Local Computer)

Log on as:

● Local System account

□ Allow service to interact with desktop

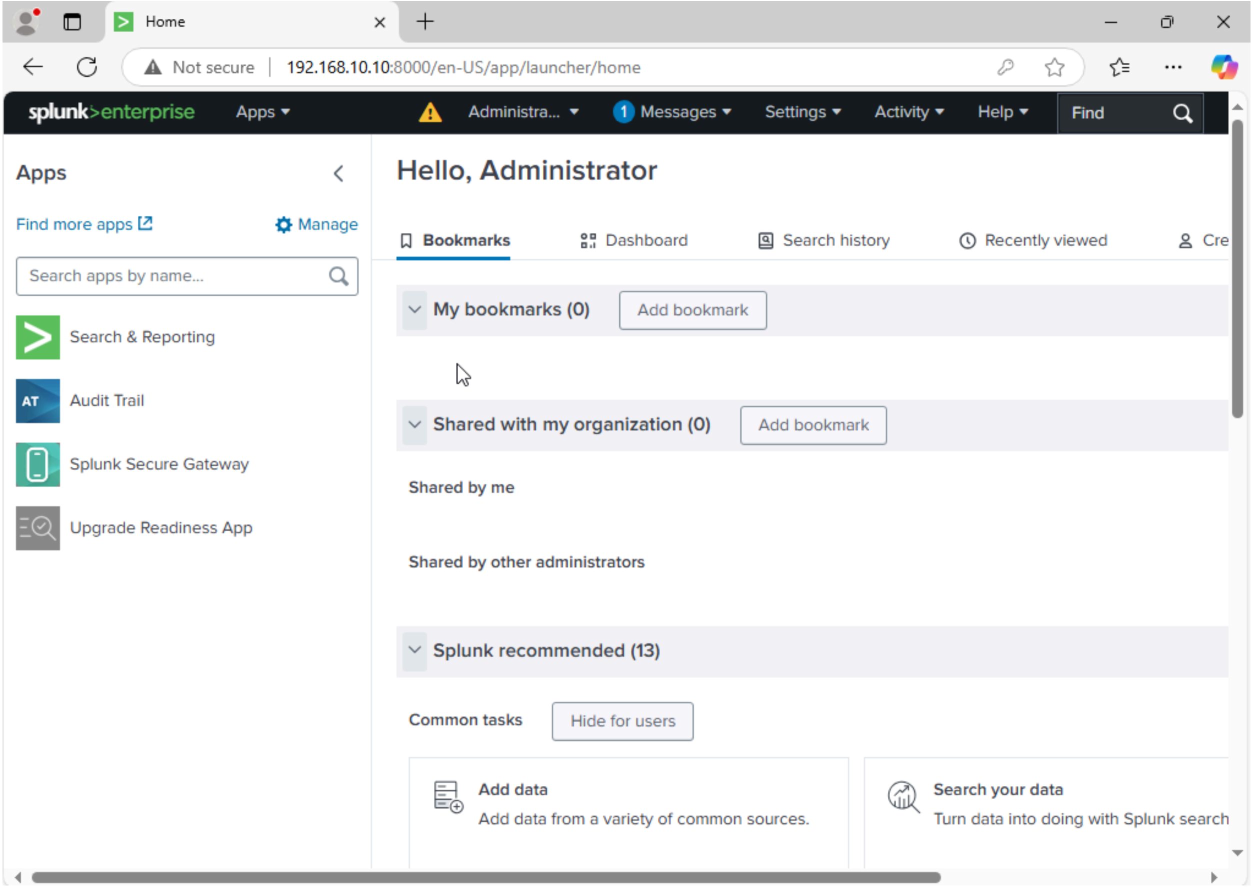
○ This account:

Password:

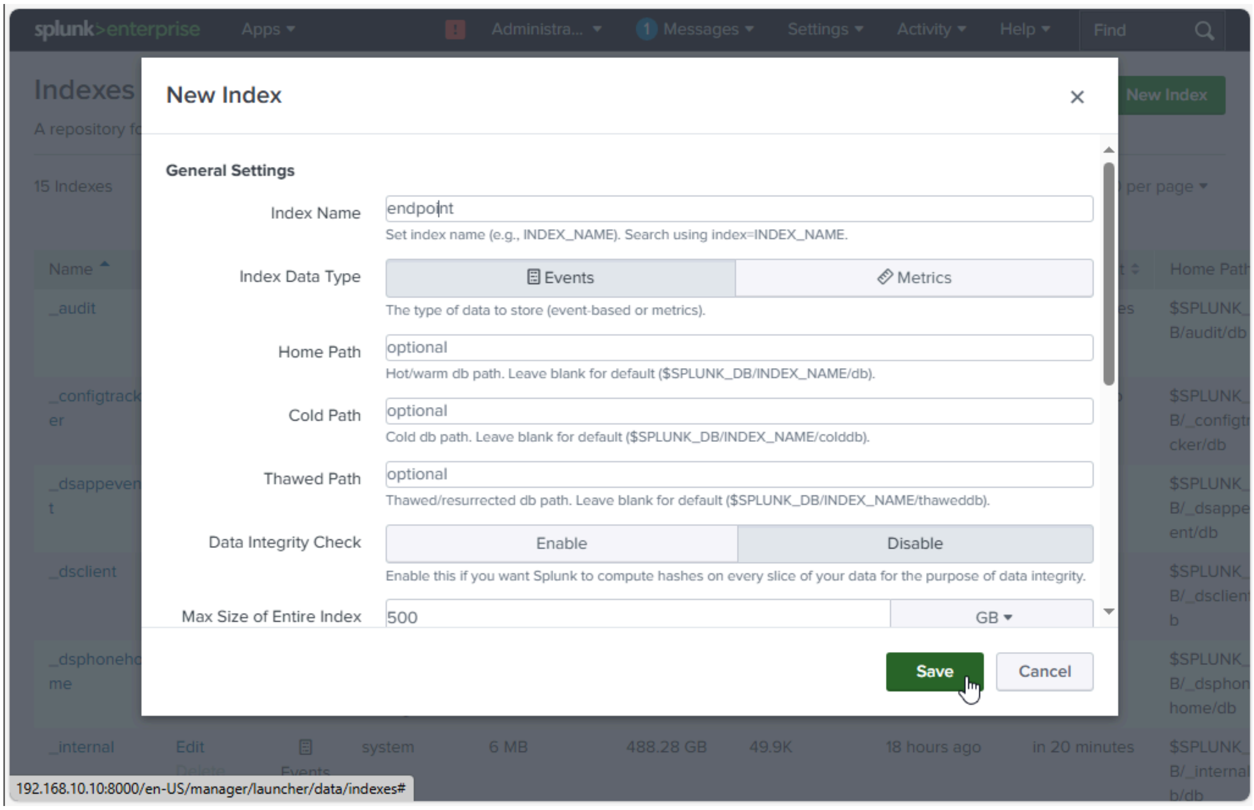
Confirm password:

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



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).

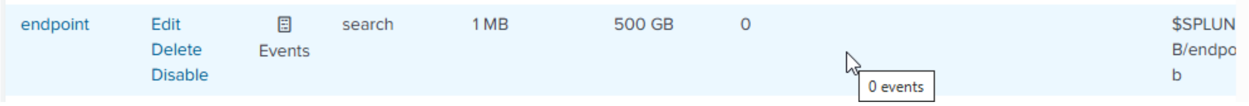
Thawed Path: optional
Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).

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

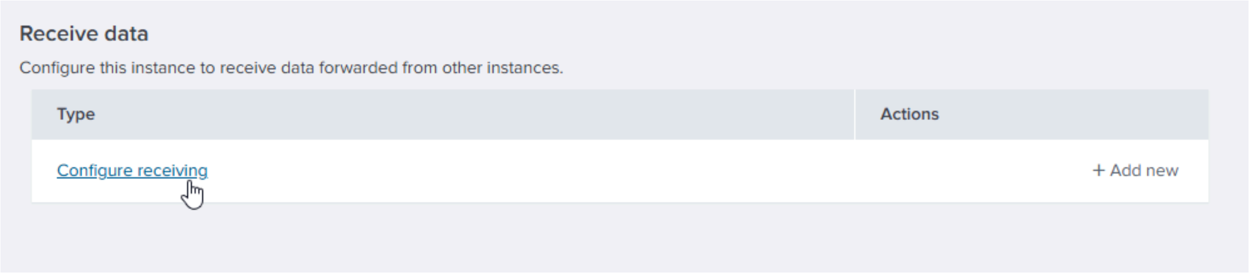
192.168.10.10:8000/en-US/manager/launcher/data/indexes#



endpoint	Edit Delete Disable	Events	search	1 MB	500 GB	0	$SPLUN B/endpo b

0 events

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:

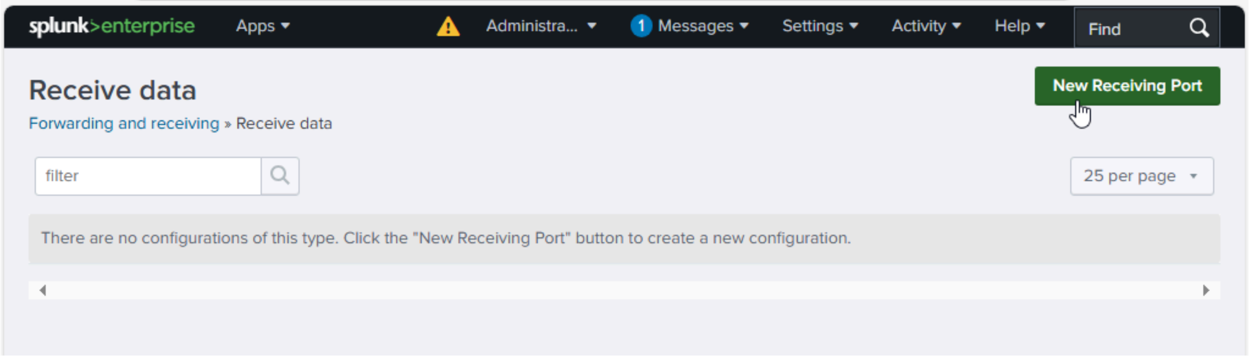


Receive data

Configure this instance to receive data forwarded from other instances.

Type	Actions
Configure receiving	+ Add new

Click New Receiving Port:

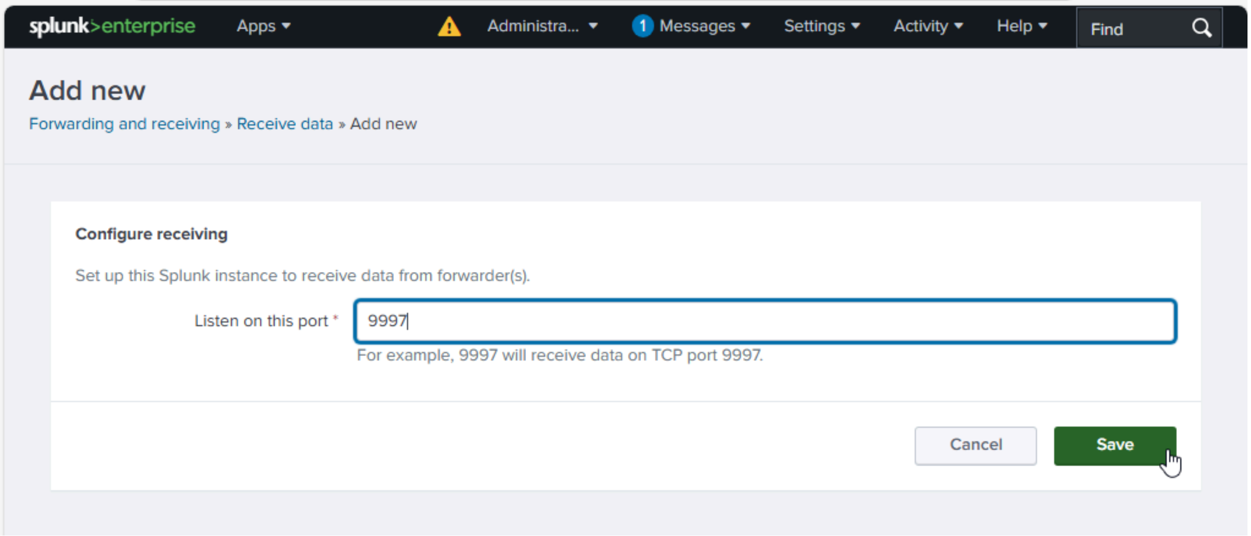


Receive data

Forwarding and receiving » Receive data

There are no configurations of this type. Click the "New Receiving Port" button to create a new configuration.

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:



Add new

Forwarding and receiving » Receive data » Add new

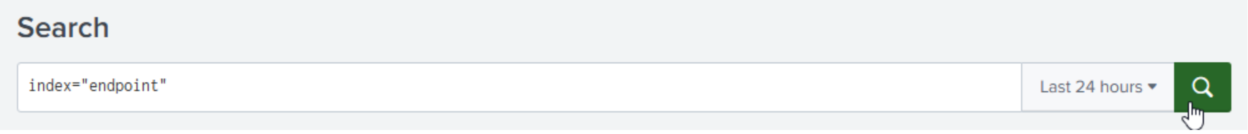
Configure receiving

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

Listen on this port * 9997

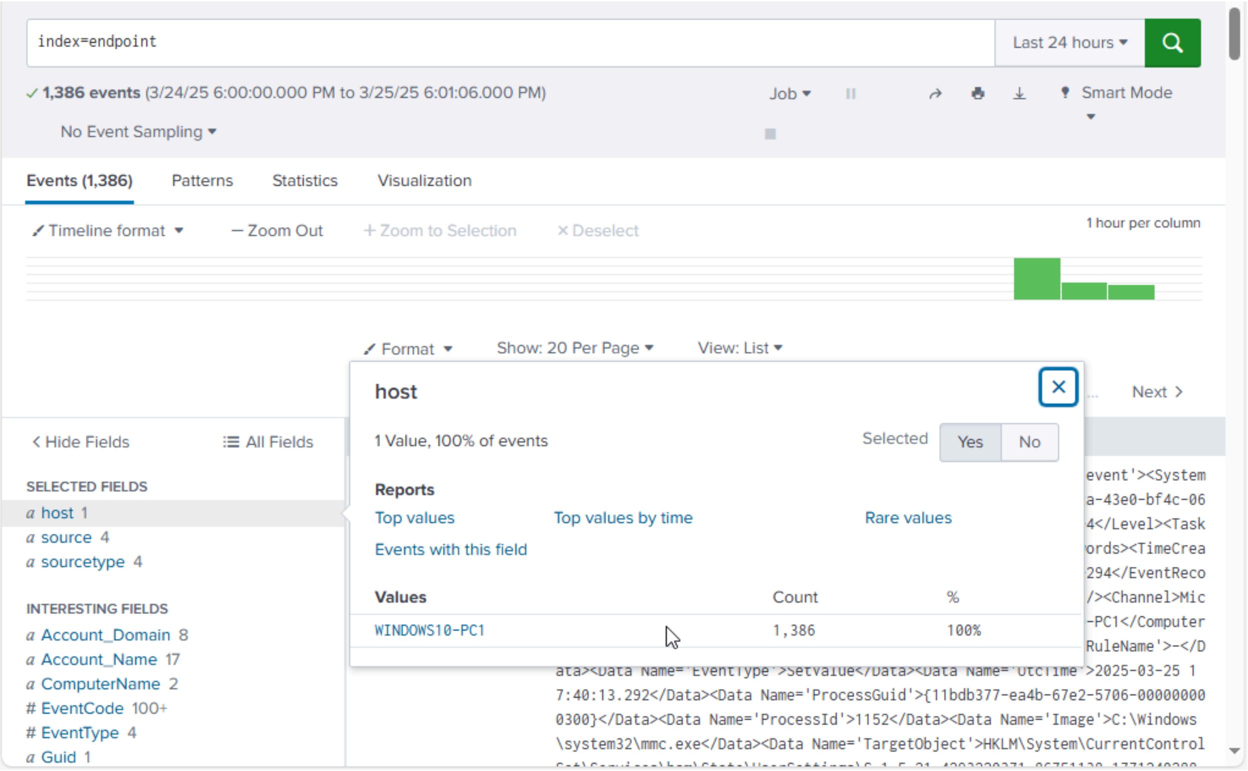
For example, 9997 will receive data on TCP port 9997.

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:


Search

```
index="endpoint"
```

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



```
index=endpoint
```

✓ 1,386 events (3/24/25 6:00:00.000 PM to 3/25/25 6:01:06.000 PM)

SELECTED FIELDS
- *a* host 1
- *a* source 4
- *a* sourcetype 4

INTERESTING FIELDS
- *a* Account_Domain 8
- *a* Account_Name 17
- *a* ComputerName 2
- # EventCode 100+
- # EventType 4
- *a* Guid 1

host

1 Value, 100% of events

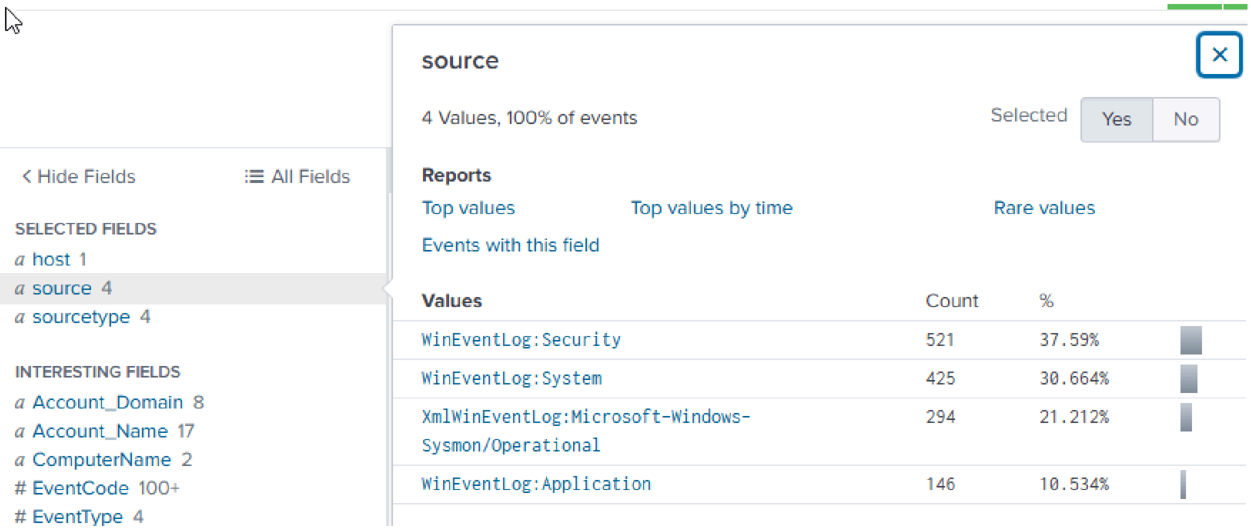
Selected: Yes | No

Reports: Top values · Top values by time · Rare values · Events with this field

Values	Count	%
WINDOWS10-PC1	1,386	100%

```
ata><Data Name='EventType'>SetValue</Data><Data Name='UtcTime'>2025-03-25 1
7:40:13.292</Data><Data Name='ProcessGuid'>{11bdb377-ea4b-67e2-5706-00000000
0300}</Data><Data Name='ProcessId'>1152</Data><Data Name='Image'>C:\Windows
\system32\mmc.exe</Data><Data Name='TargetObject'>HKLM\System\CurrentControl
```

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



SELECTED FIELDS
- *a* host 1
- *a* source 4
- *a* sourcetype 4

INTERESTING FIELDS
- *a* Account_Domain 8
- *a* Account_Name 17
- *a* ComputerName 2
- # EventCode 100+
- # EventType 4

source

4 Values, 100% of events

Selected: Yes | No

Reports: Top values · Top values by time · Rare values · Events with this field

Values	Count	%
WinEventLog:Security	521	37.59%
WinEventLog:System	425	30.664%
XmlWinEventLog:Microsoft-Windows-Sysmon/Operational	294	21.212%
WinEventLog:Application	146	10.534%

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