**SOC Training - Building Splunk lab for Logs ingesting, Monitoring & Alerting**

Part 1: Requirements & Tools:

1. Tools

* Hypervision Software: VMware Workstation, VirtualBox.
* Windows 11 ISO: Download from microsoft official page.
* Ubuntu 22.04 Server/Desktop ISO: Download from Ubuntu official page, Desktop is recommended for visualizing.
* Splunk Enterprise: Download from Splunk official site, free version trial for 60 days (should be enough for a lab project).
* Splunk Universal Forwarder: Download from Splunk official site for logs collecting.
* Other tools: Sysmon, pfSense (optional).

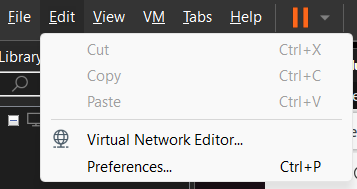
1. Requirements

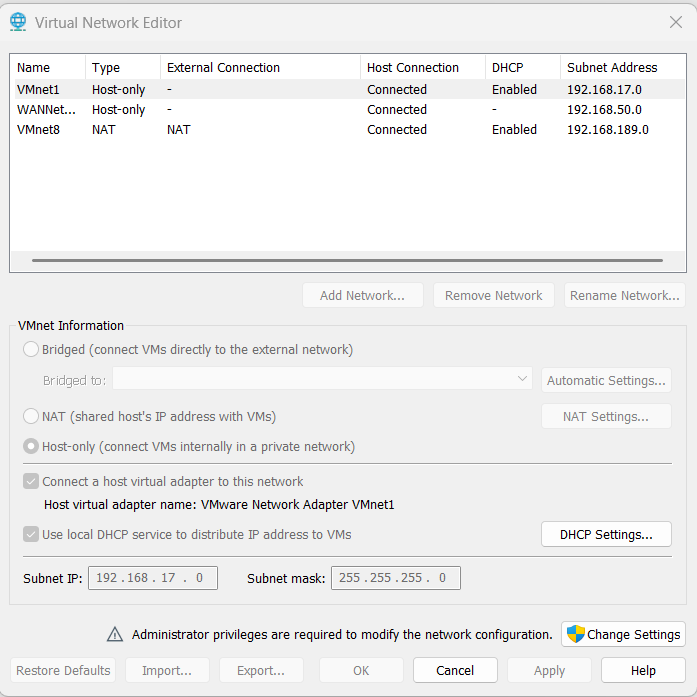
* ROM: >= 90GB spare space
* RAM: >= 16GB for a smooth workflow

Part 2: Implementation

1. Network configuration

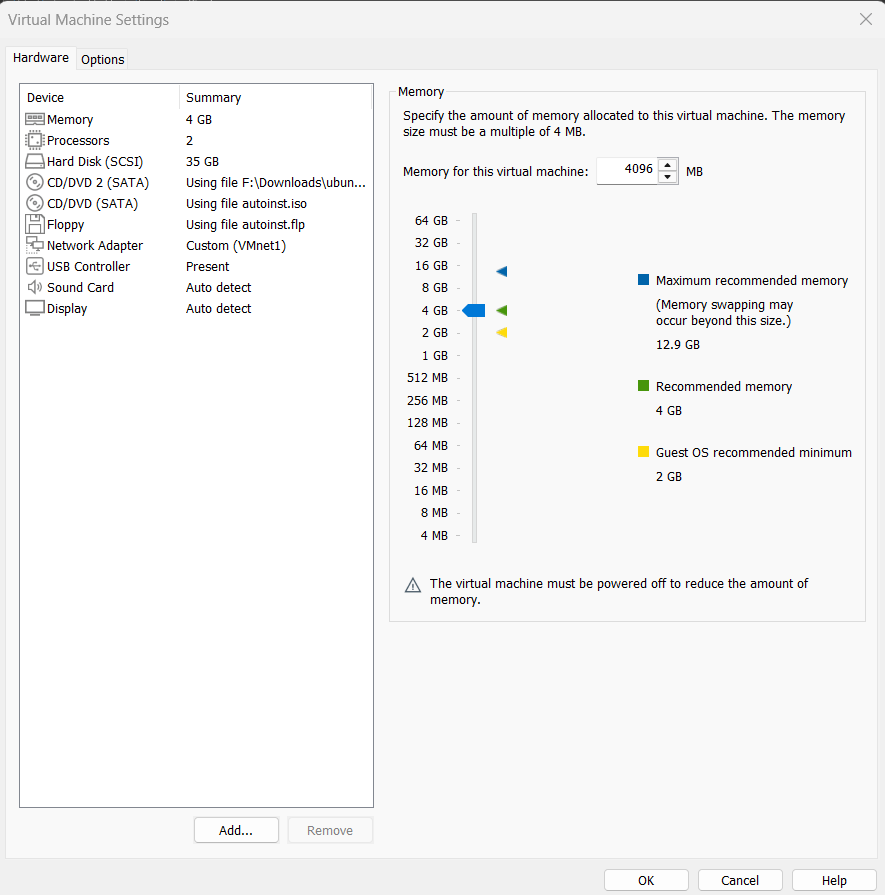
* For this lab, I will be using host-only network to ensure consistency and reliable connection between the VMs.
* Open VMware Workstation Pro, go to Edit -> Virtual Network Editor



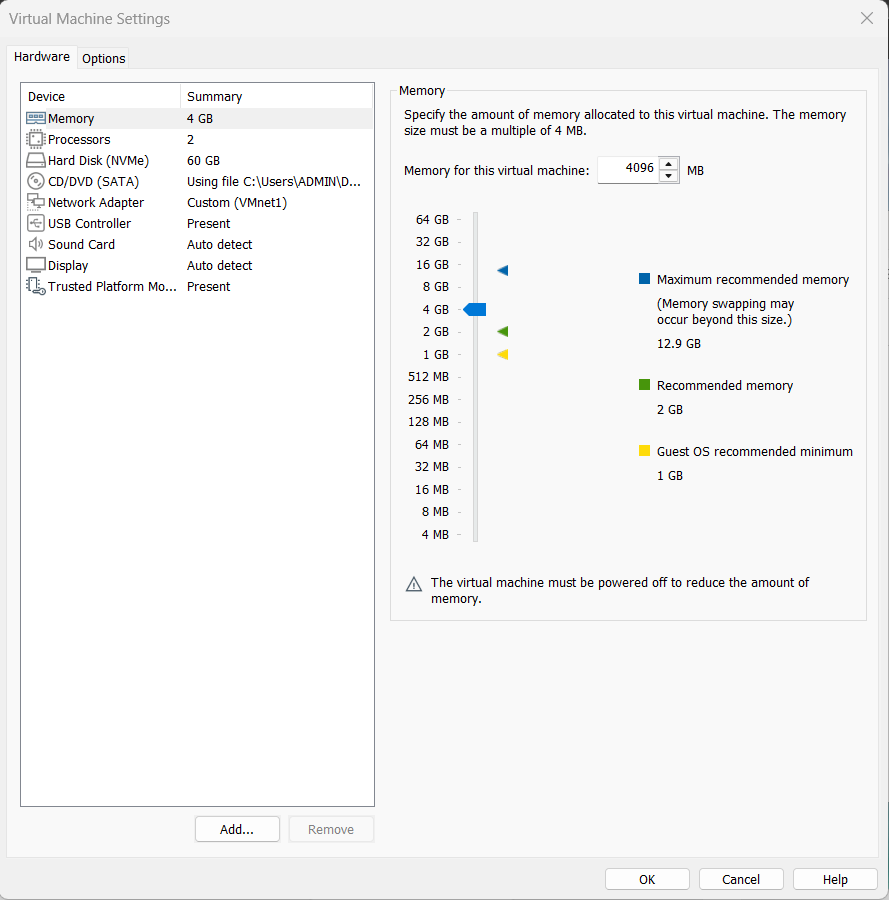


1. Splunk Server

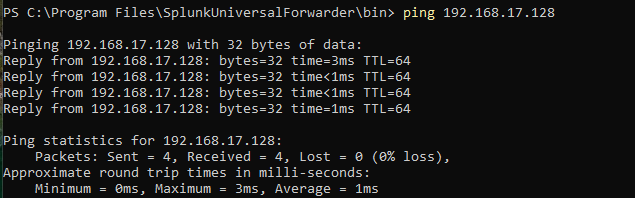
* Before install and configure anything, we need to set up the host virtual machine first, for the Splunk Server, I choose Ubuntu 22.04 as the host OS.
* Ubuntu set up:
* ISO Ubuntu 22.04.05 LTS
* Ram >= 4GB
* CPU >= 2 core
* Storage >= 35GB



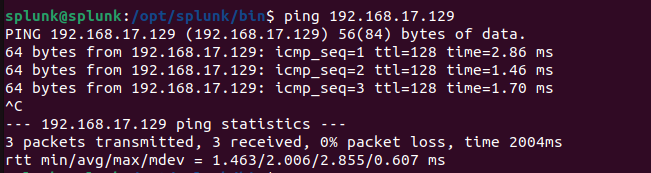
* Windows set up:
* Ram >= 4GB
* CPU >= 2 core
* Storage >= 60GB



* After finish set up the 2 VMs, test their connection



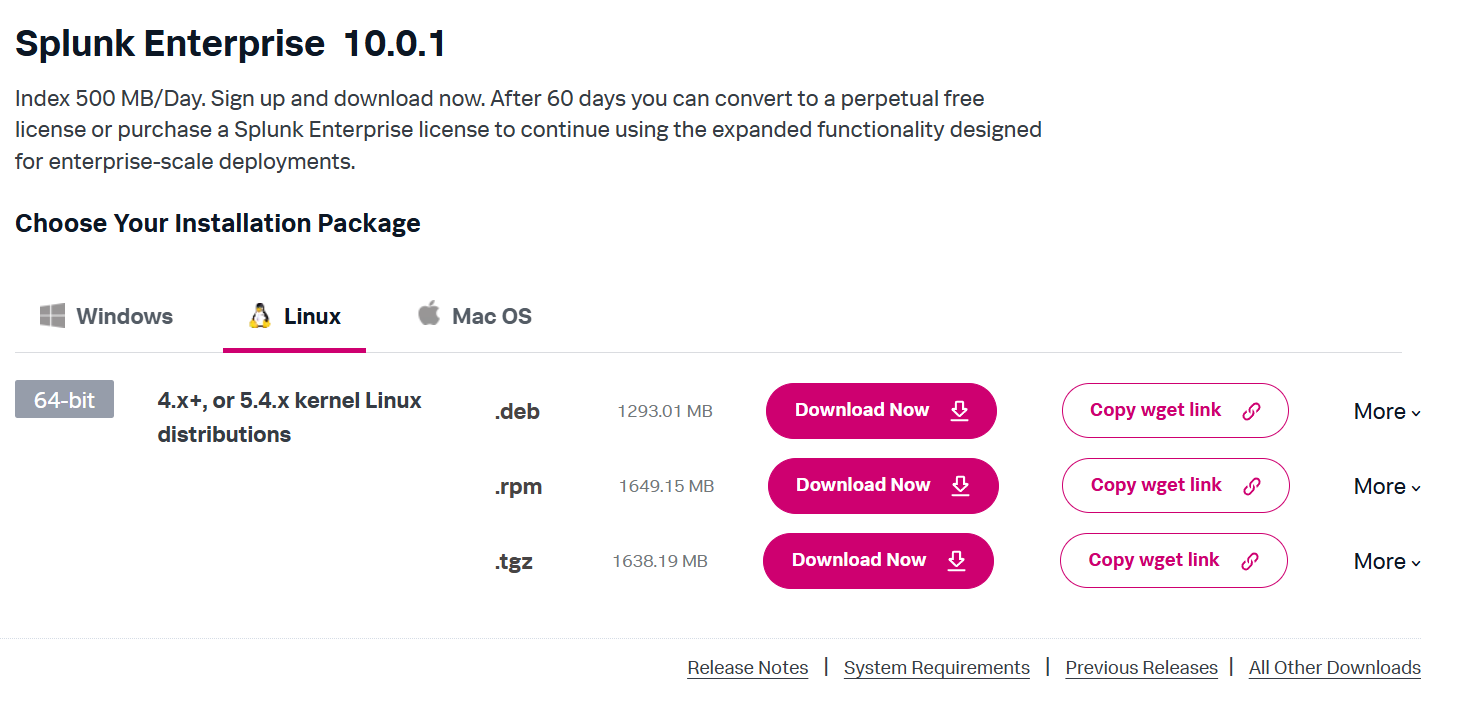
Ping from the Windows machine to Ubuntu



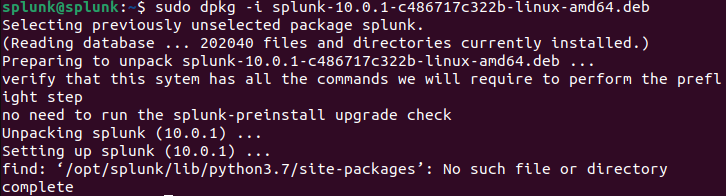
Ping from the Ubuntu machine to the Window machine

Step 1: Splunk Server Download

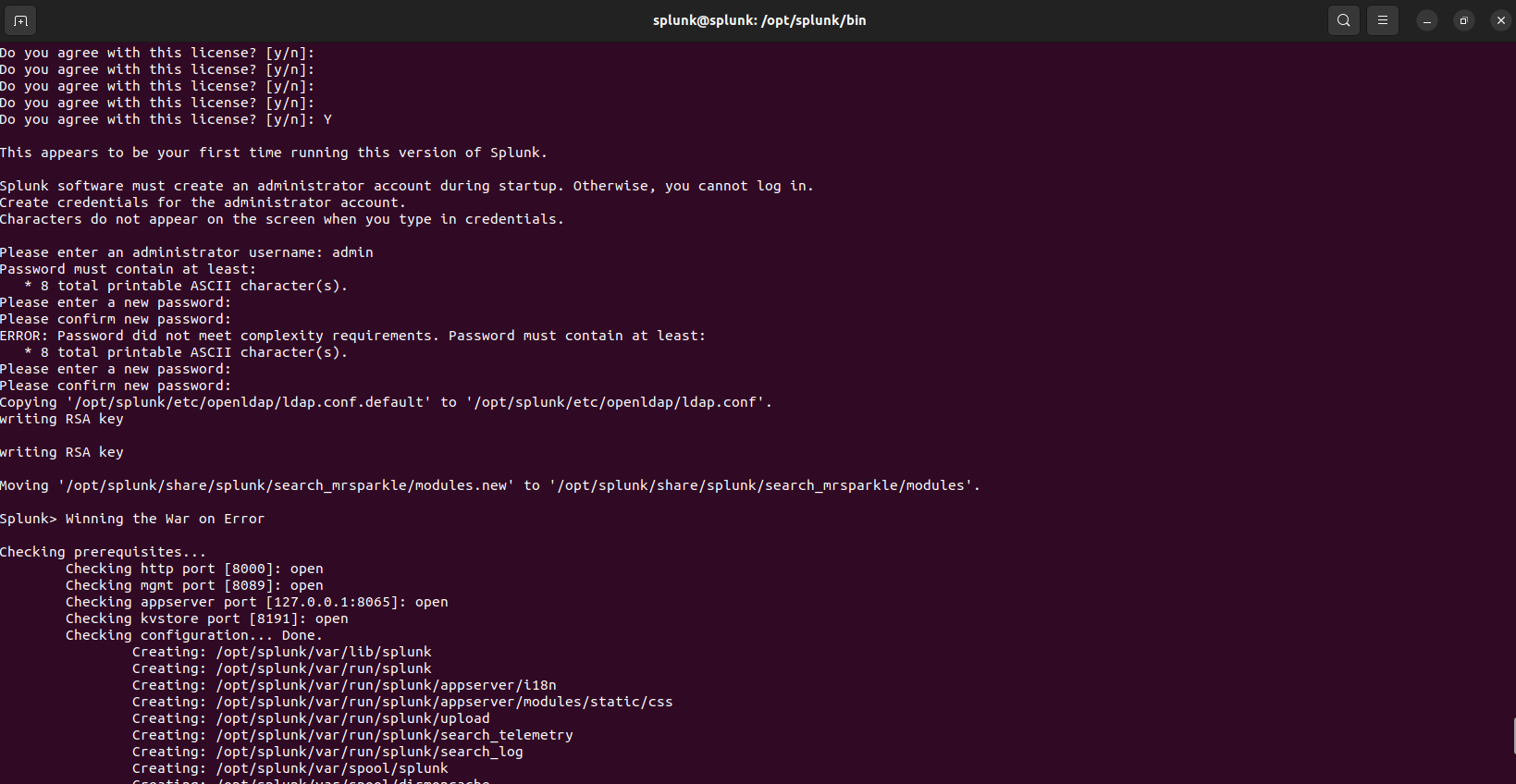
* On Ubuntu machine, access Splunk's official site and create an account (each account only has a 60 days trial).

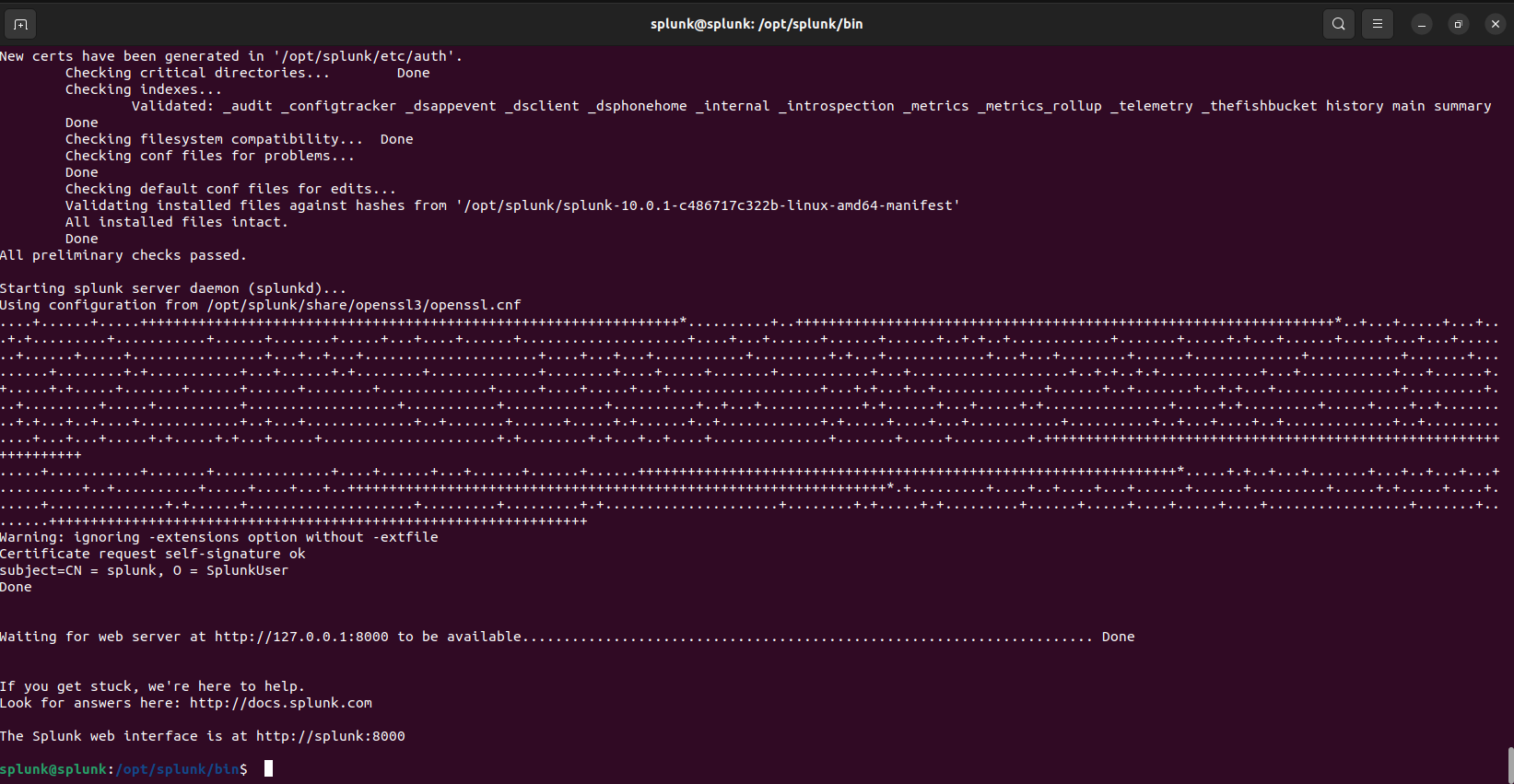


* Copy .deb wget link, then open a terminal and paste it in, it should be something like this: **wget -O splunk-10.0.1-c486717c322b-linux-amd64.deb "**[**https://download.splunk.com/products/splunk/releases/10.0.1/linux/splunk-10.0.1-c486717c322b-linux-amd64.deb**](https://download.splunk.com/products/splunk/releases/10.0.1/linux/splunk-10.0.1-c486717c322b-linux-amd64.deb)**"**
* Extract everything, if everything goes well, it should display a “complete” message as in the picture below.

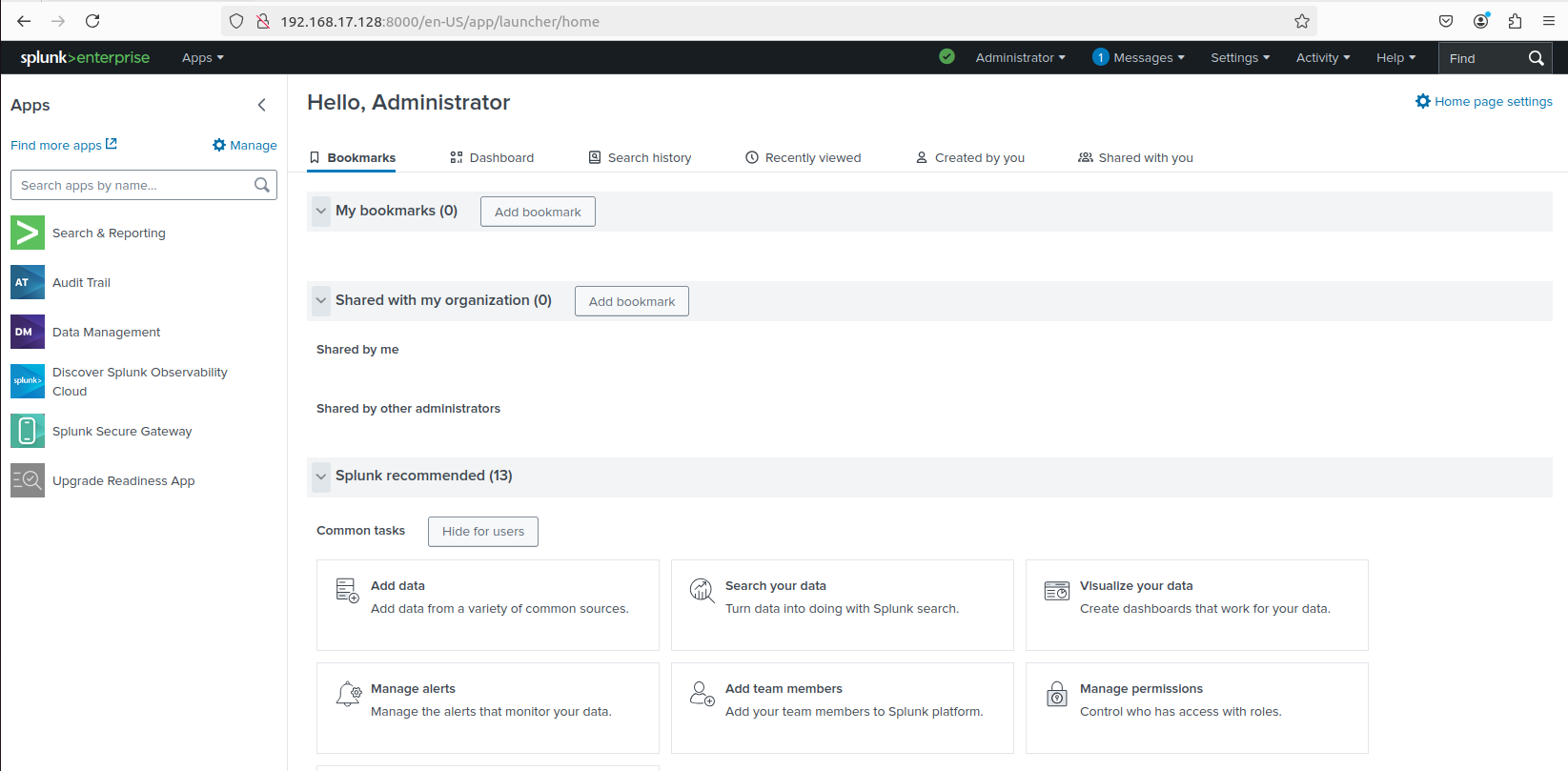


* Run Splunk for the first time using command sudo /opt/splunk/bin/splunk start, accept license, create a username and password to login Splunk.

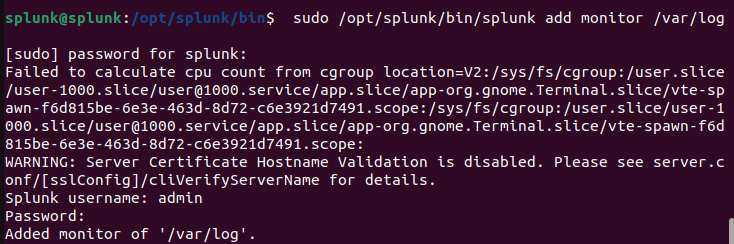




* If everything run smoothly, you can start using the Splunk home page.



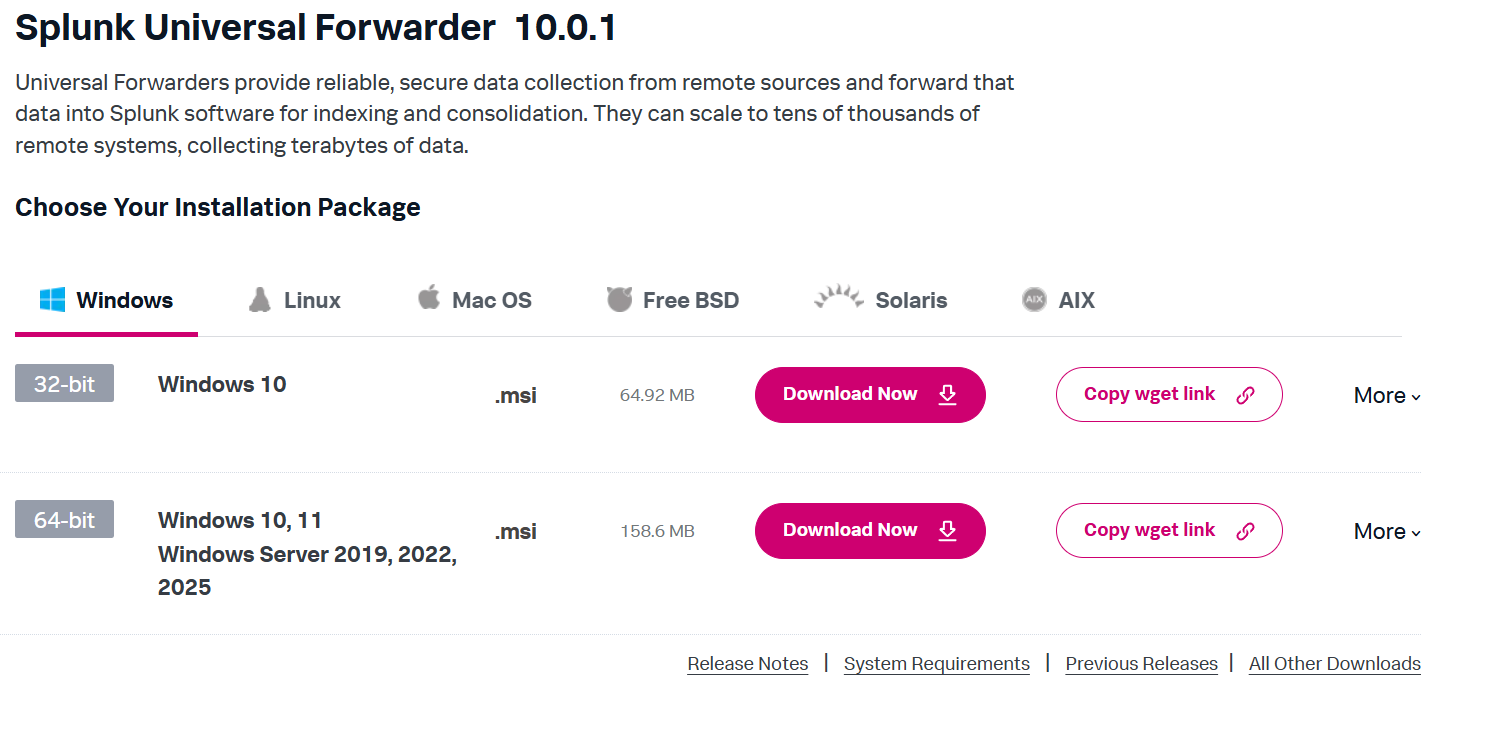
* Next, configure Splunk to monitor the Ubuntu machine (Splunk’s host machine), this will include several system logs such as auth.log, syslog, kern.log,etc.



1. Windows Endpoint

Step 1: Install Splunk Universal Forwarder for remote data collection

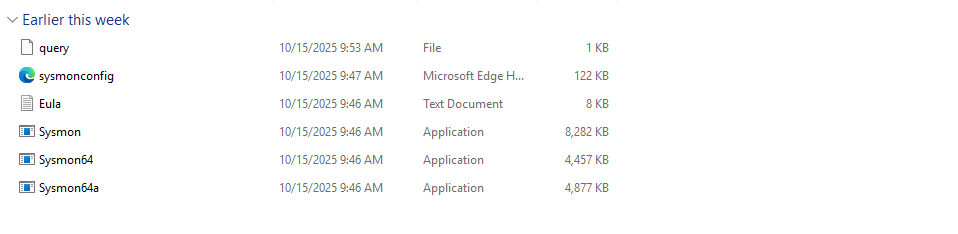
* Download Splunk Universal Forwarder on Splunk official site



* Download and run the .msi file, and configure it to forward data to the Splunk server machine (make sure to get the IP right).

Step 2: Sysmon Installation

* Install Sysmon to have enhanced standard logging capabilities ad Extract it.
* Before running Sysmon, make sure to have a Sysmon configuration file first. Go to SwiftOnSecurity and make a copy of the configuration. [SwiftOnSecurity/sysmon-config: Sysmon configuration file template with default high-quality event tracing](https://github.com/SwiftOnSecurity/sysmon-config)
* Place the configuration file in the same folder as the Sysmon’s exe file



* Finally, run it with command **./Sysmon64.exe -accepeula -i sysmonconfig.xml**

Step 3: Configure Splunk UF to collect data.

* Navigate to **C:\Program Files\SplunkUniversalForwarder\etc\system\local,** you should see a **inputs.conf** file, if not, create one and paste in the following lines.

# Windows platform specific input processor.

#[WinEventLog://Application]

#disabled = 0

#index = wineventlog

[WinEventLog://Security]

disabled = 0

index = wineventlog

#[WinEventLog://System]

#disabled = 0

#index = wineventlog

[WinEventLog://Microsoft-Windows-Sysmon/Operational]

disabled = false

renderXml = true

index = sysmon

sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

* For this project, I configured the UF to collect Windows Security Events Log and Sysmon Log only, that’s why the other events logs are being commented, but you can always enable them if you want.
* **Note**: If you use this configuration, you should create a new index called “sysmon” and “wineventlog” in Splunk, or else you won’t see any logs display on the screen. If you don’t want to configure it, delete the line “index” name in the every section of the above configuration.
* Open a PowerShell or CMD terminal, restart Splunk UF to start sending logs data, make sure the output destination is correct.

**PS C:\Program Files\SplunkUniversalForwarder\bin> .\splunk.exe restart**

With everything set, you can go to the Splunk homepage to start monitoring logs, go to **Search and Report** and check whether or not Splunk have successfully collected logs. If you don’t see any logs display, try to restart splunk with **sudo /opt/splunk/bin/splunk restart.**

