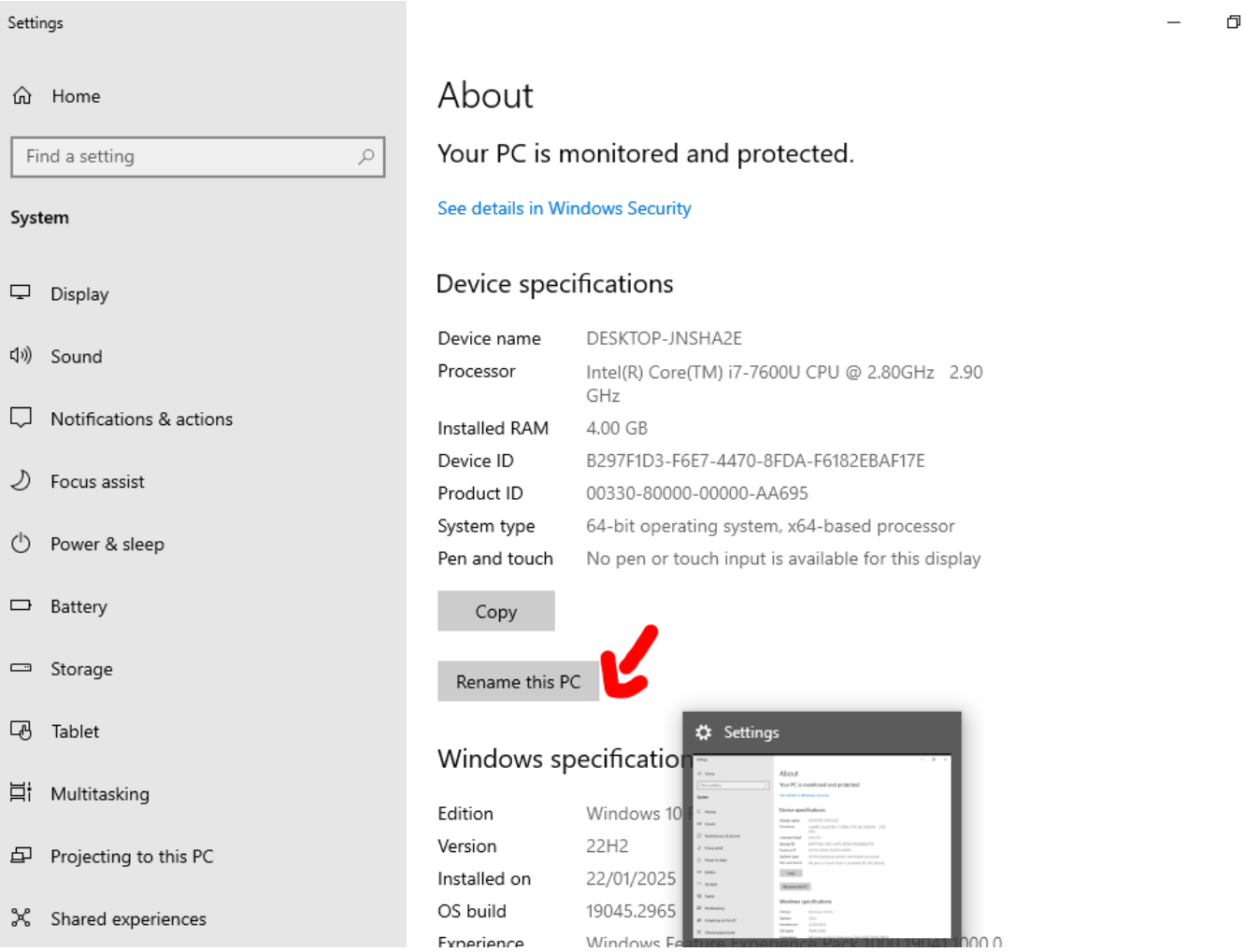
3. Sysmon client domain controller setup

A couple of things we will need to do here is to;

1. Configure the name of our windows client to Target
2. Set a manual IPV4 static address
3. Download and setup Splunk's universal forwarder
4. Download and setup Sysmon
5. Create Endpoint index in Splunk .

1. Rename windows 10 client.

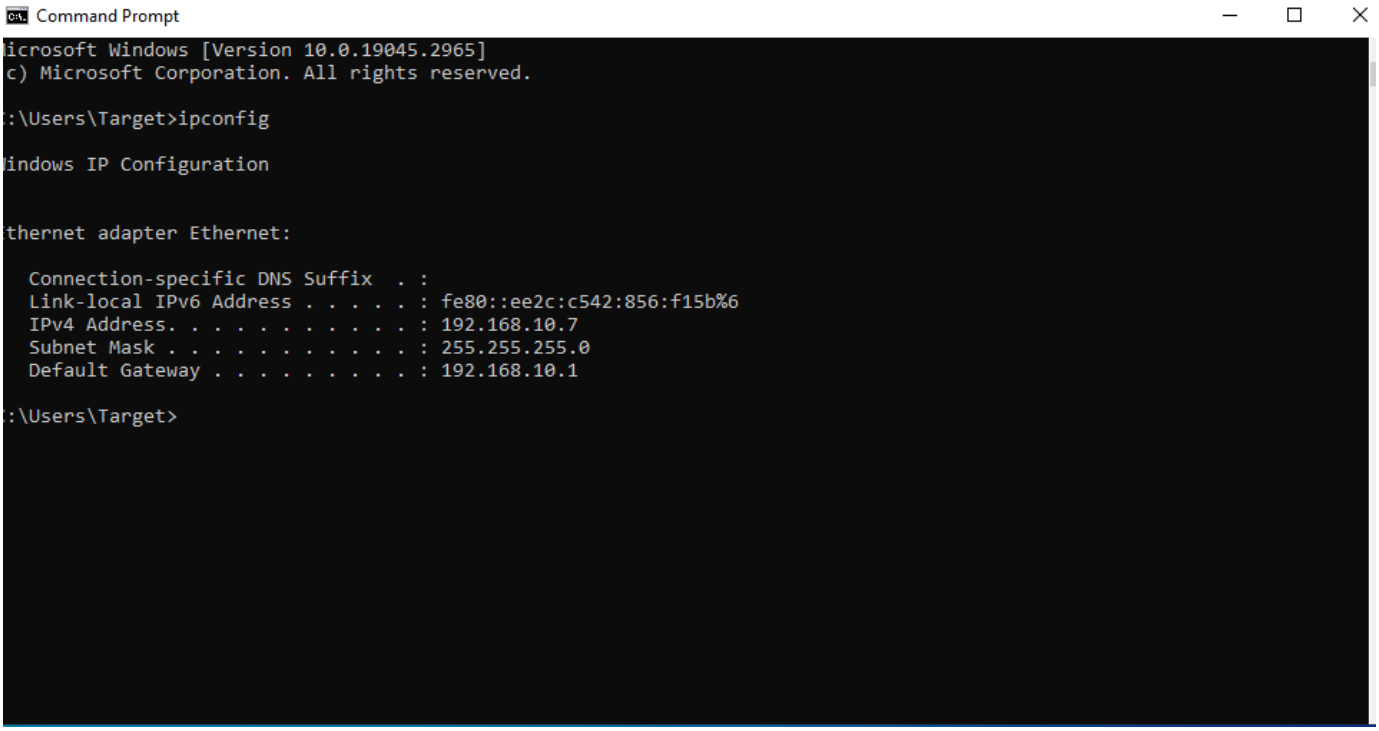
To rename the client simply search for pc in the search box , right-click and go to properties --> Rename this PC :



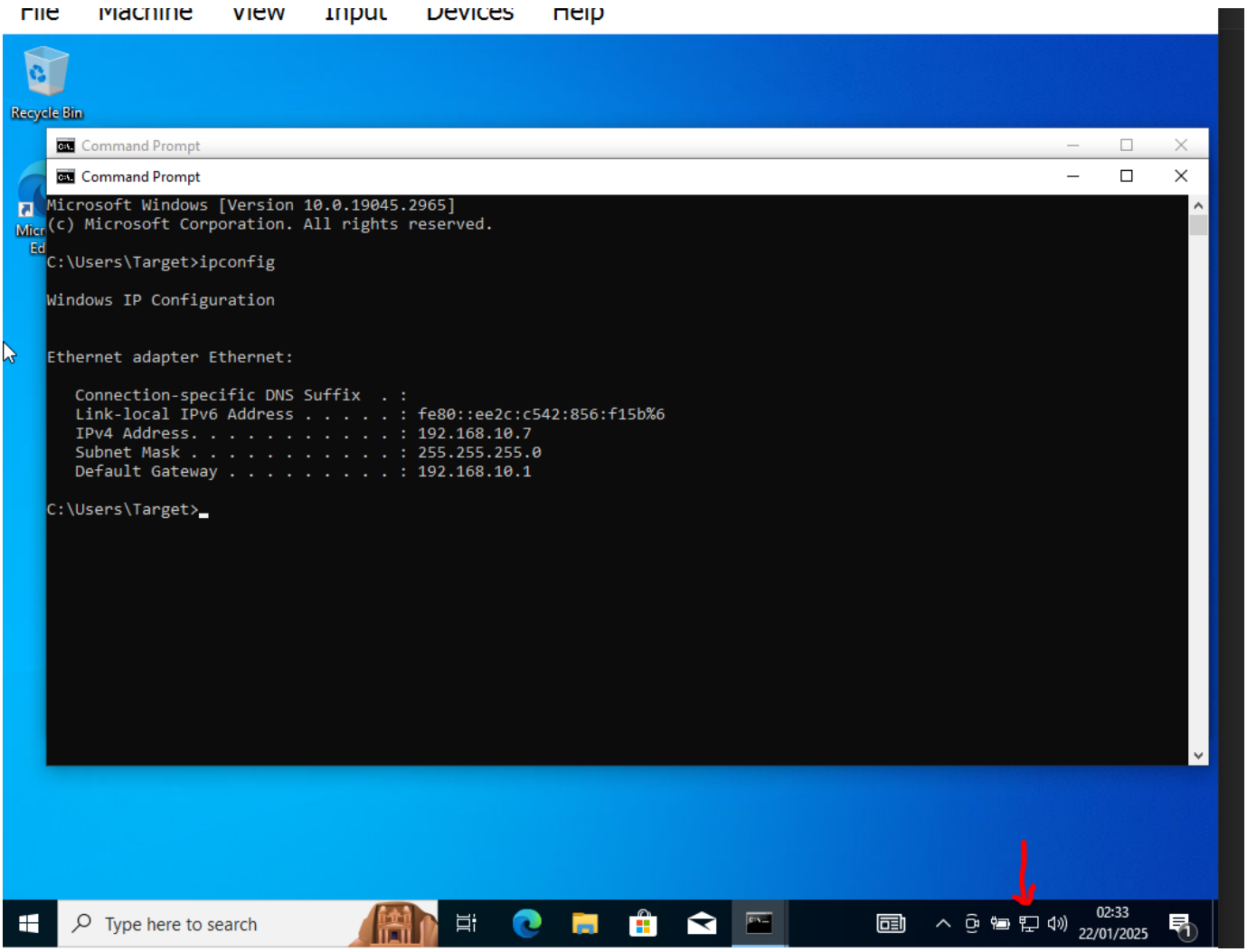
Rename it to "target-PC" and restart the computer.

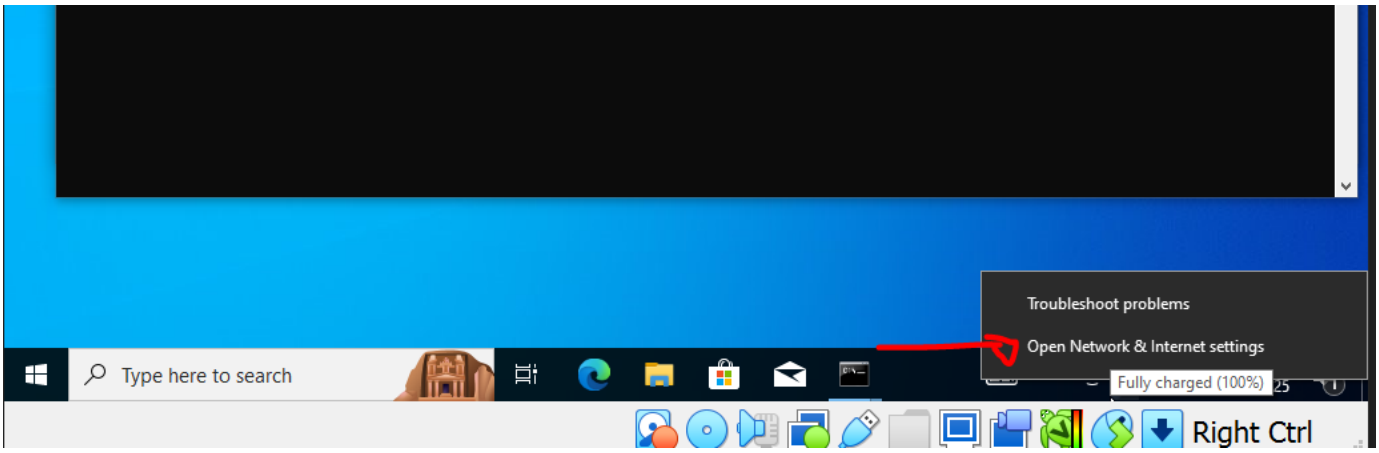
2. Setting static IPV4 Address.

First open up command prompt and run the "ipconfig" command to see what IP we have been dynamically assigned. We are going to change that IP address to the one reflected in the network diagram and different from the DC SERVER(192.168.10.7):

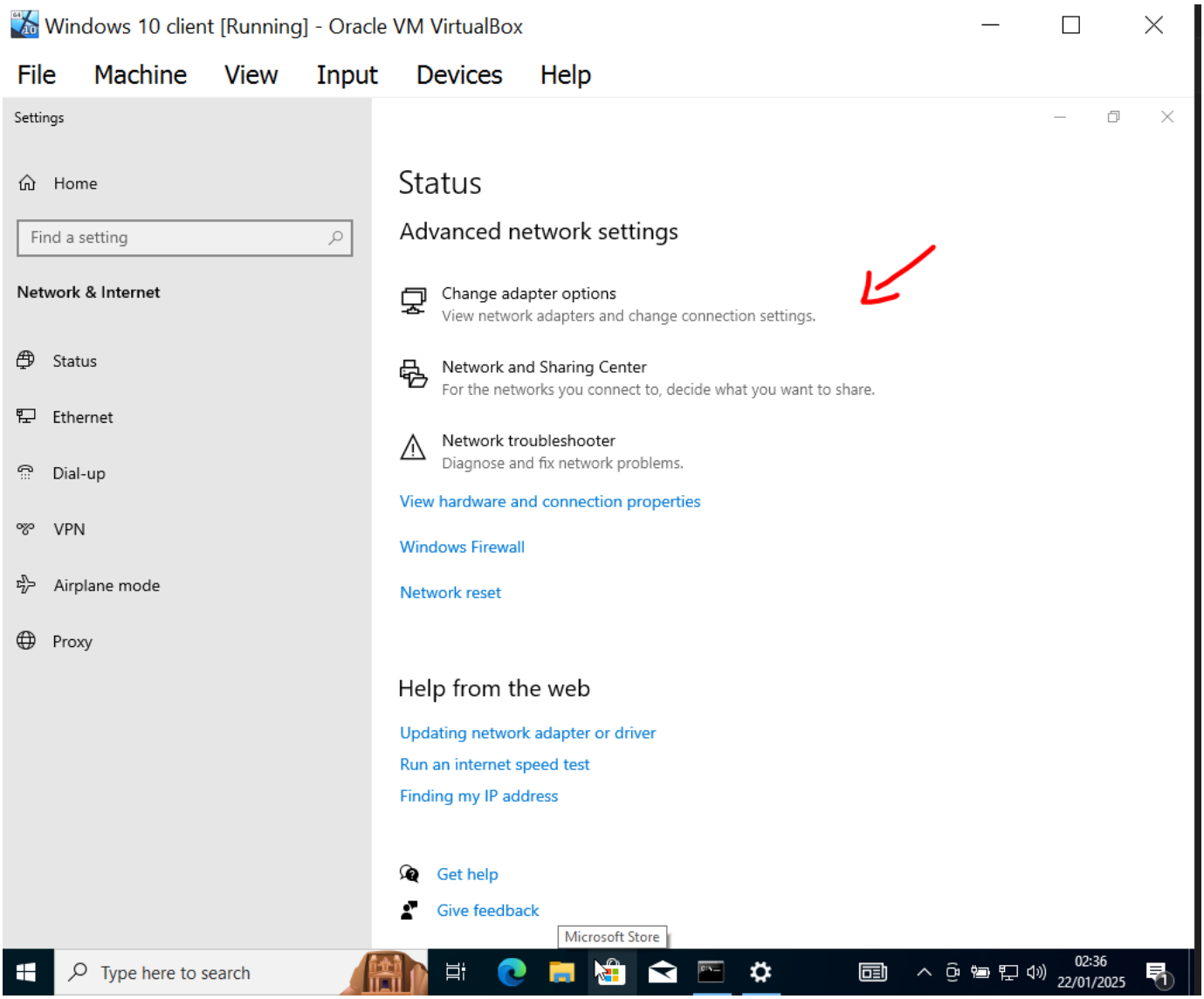


To change that , right-click on the network icon at the bottom right of your windows VM :

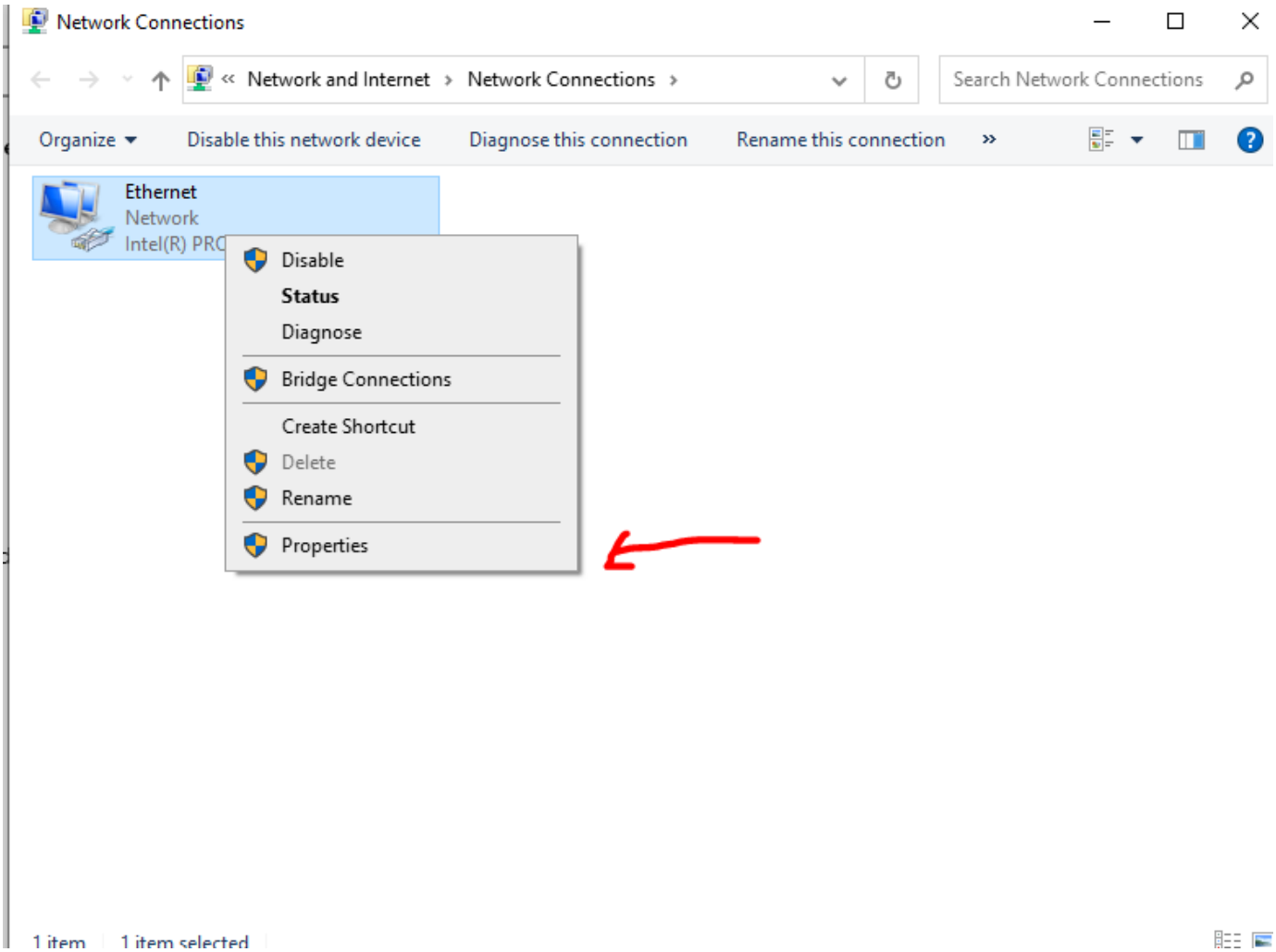




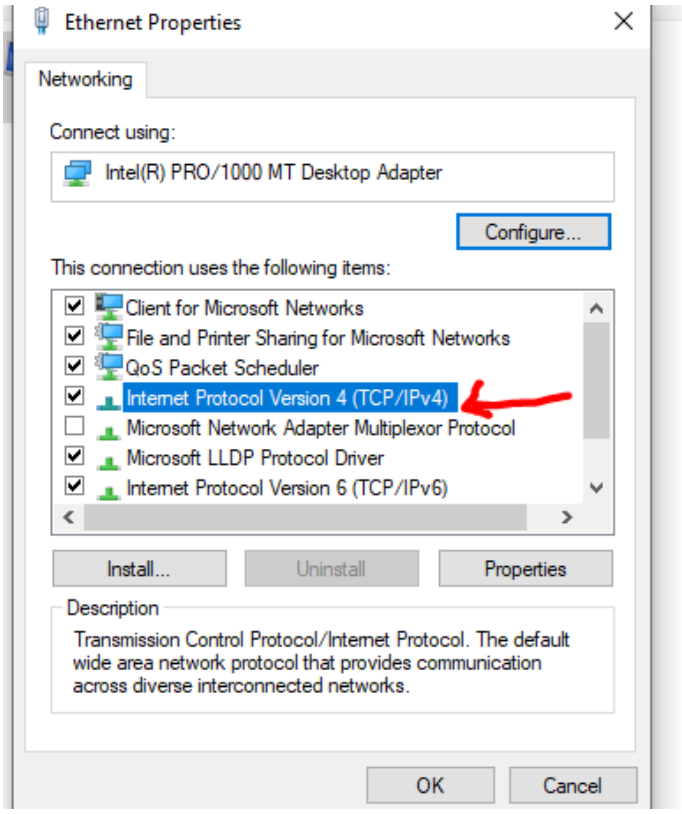
Scroll down and click on Change adapter options :



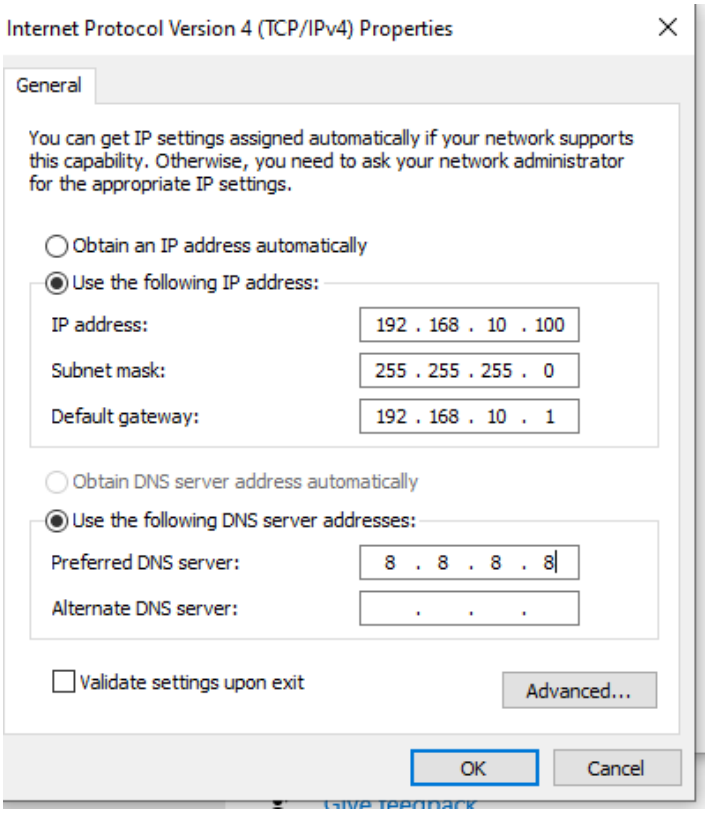
Right-click on the adapter, then click on properties :



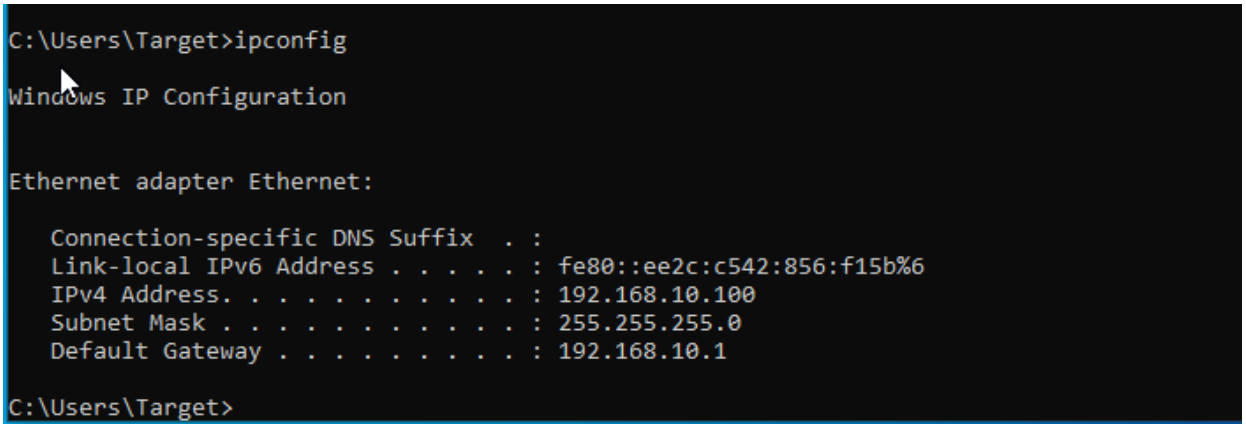
In there , double click on Internet Protocol version 4 :



And click on Use the following IP address and let it match something like the one below :



Click on OK. Go back to command prompt and rerun the ipconfig command and we'll see the new changes made :

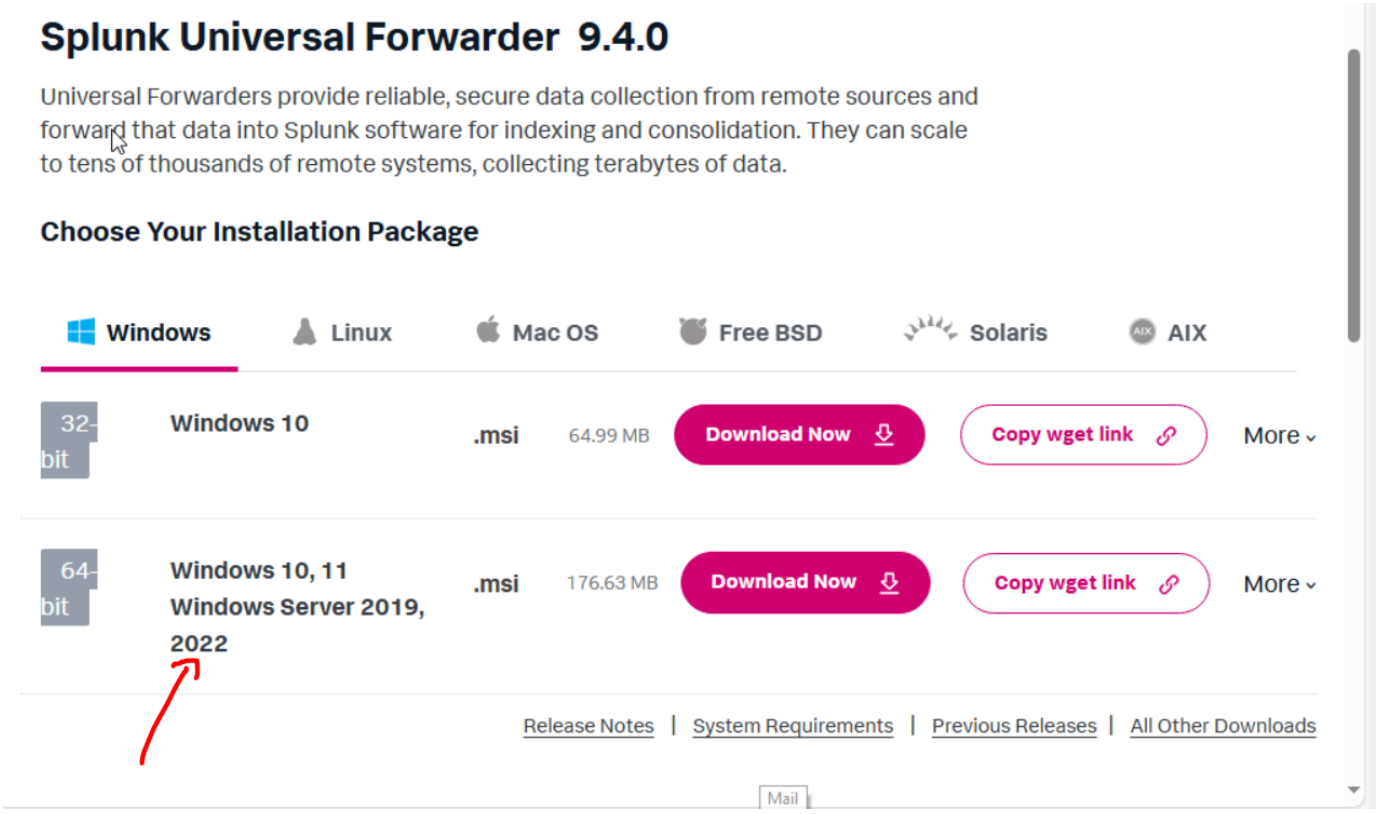


3. Splunk Universal Forwarder.

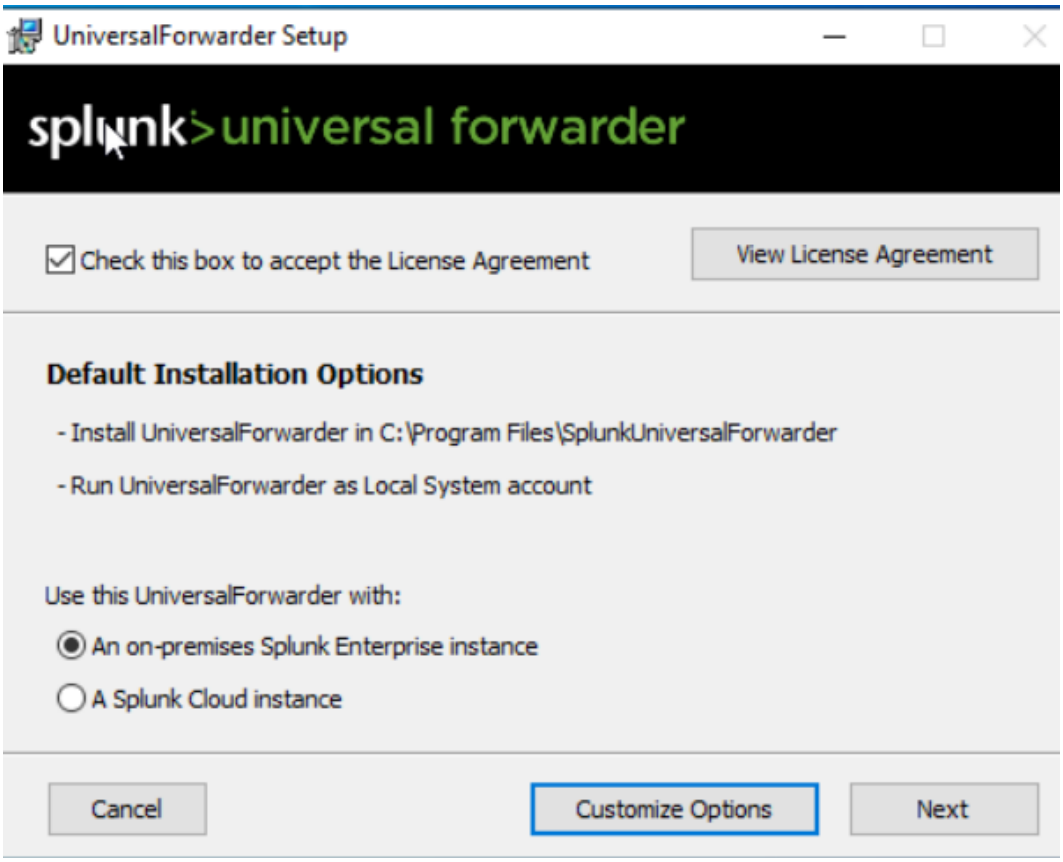
The **Splunk Universal Forwarder** is a small program that collects data, like logs or system information, from computers and sends it to a main Splunk server where the data can be analyzed.

Navigate to the official Splunk website and sign in. Head to products :

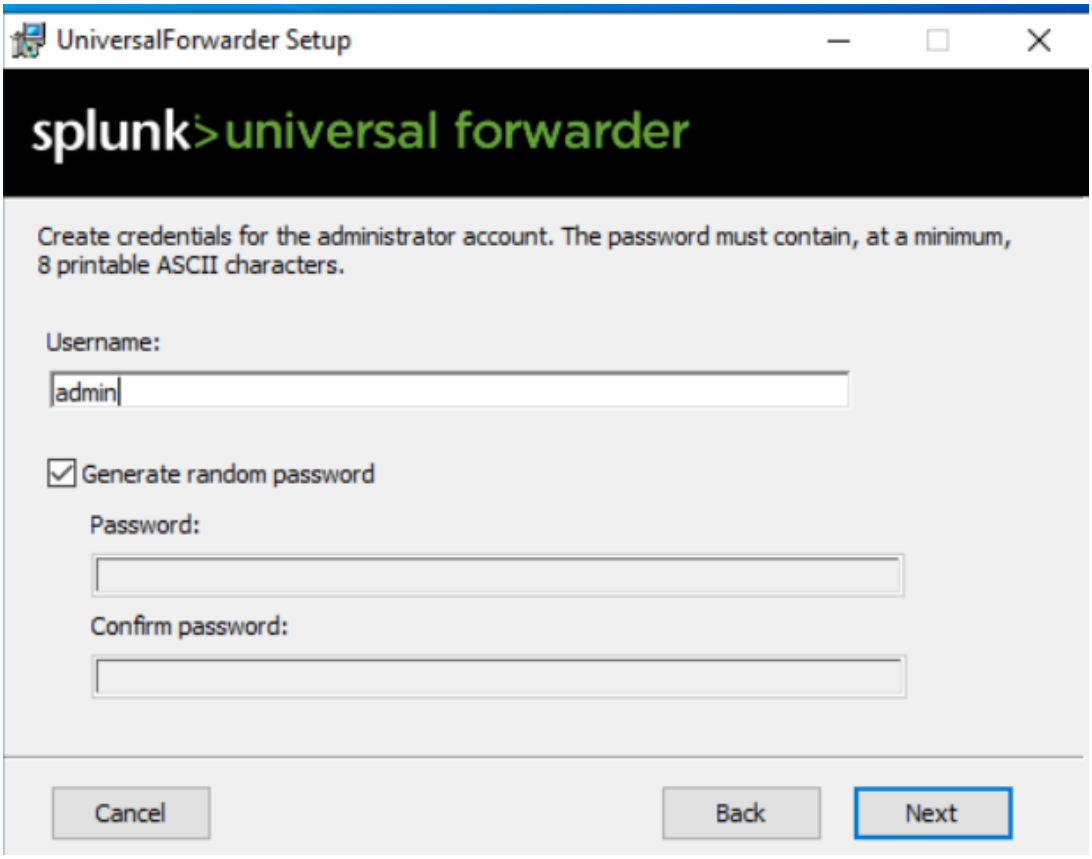
We will select the 64bit windows msi download:



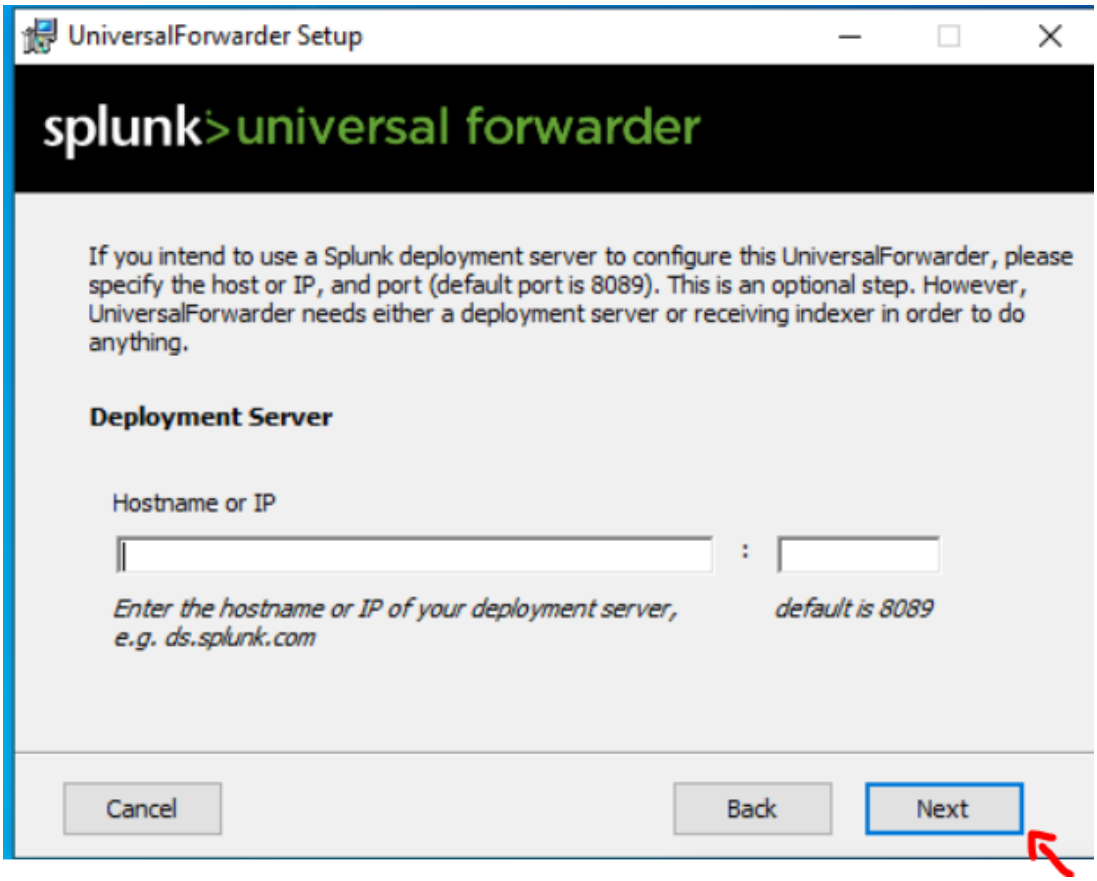
Once the download is completed, navigate to the Downloads folder and double-click on the file to begin installation:



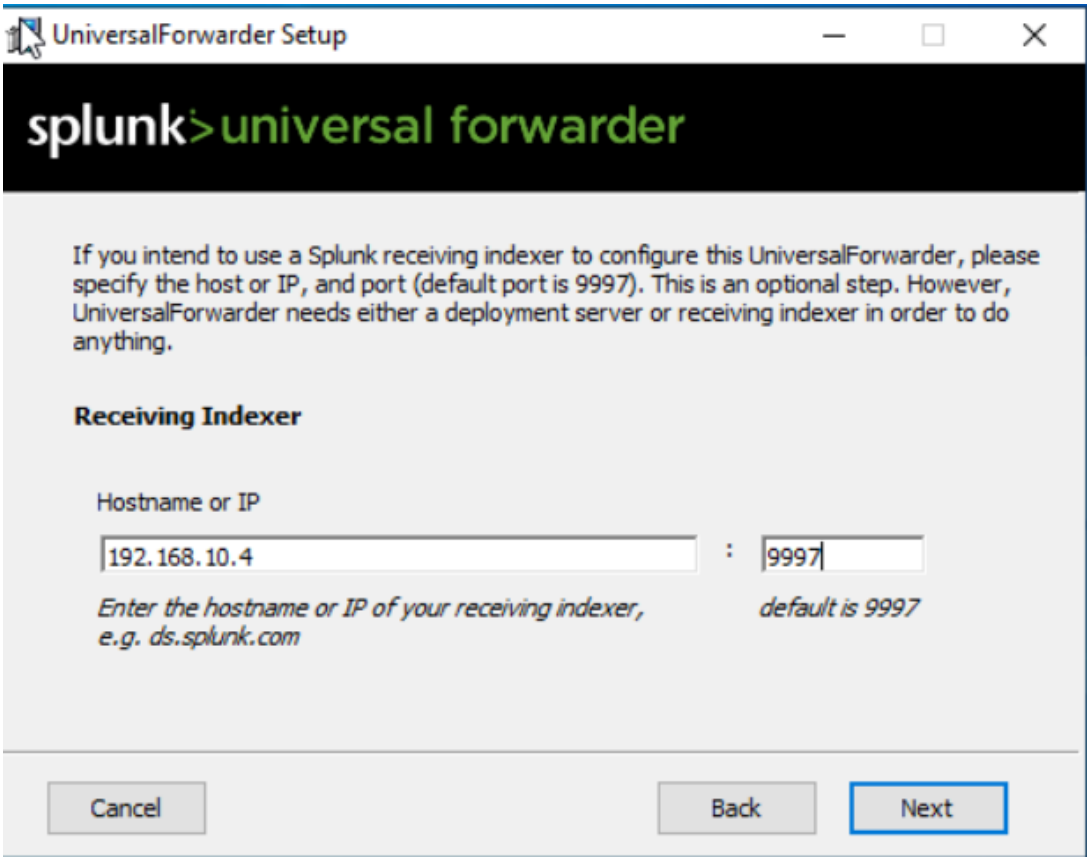
Click on Next:



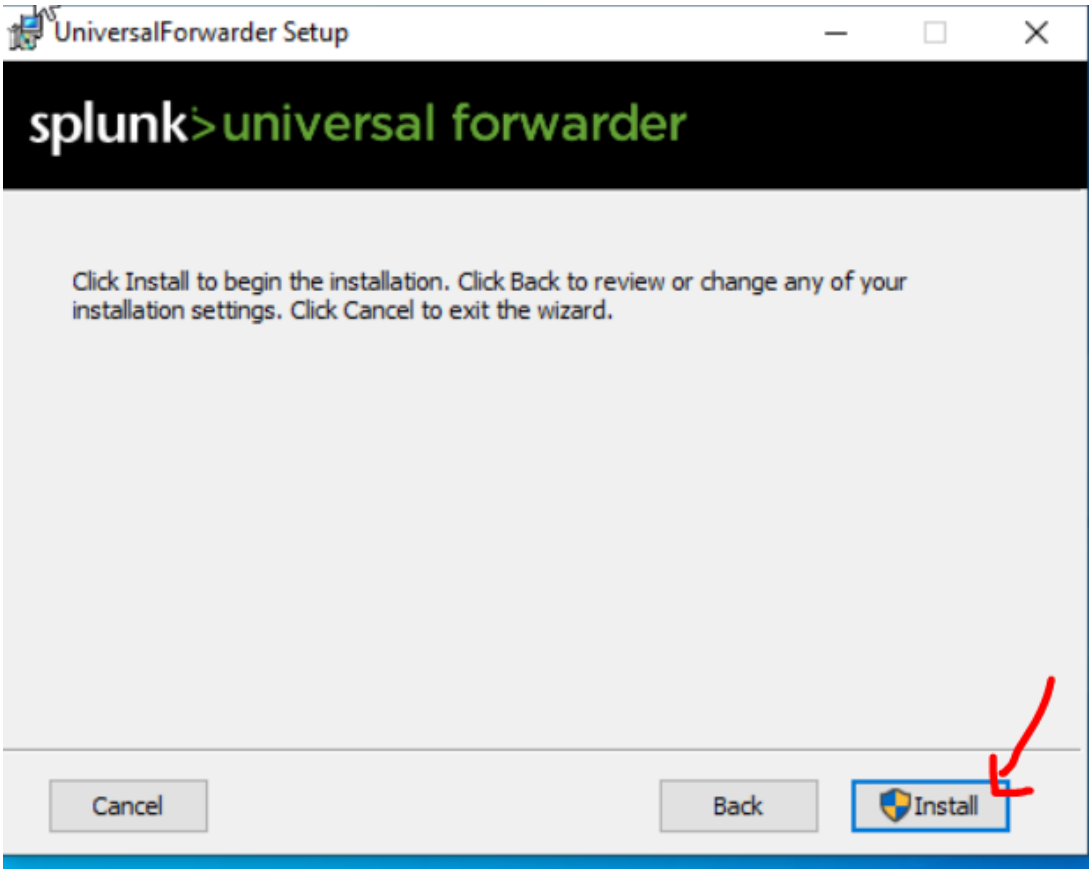
We don't have a deployment server so we will click on Next:



Now we need to input the IP address of the splunk server (in my case 192.168.10.4) and set the default to 9997:



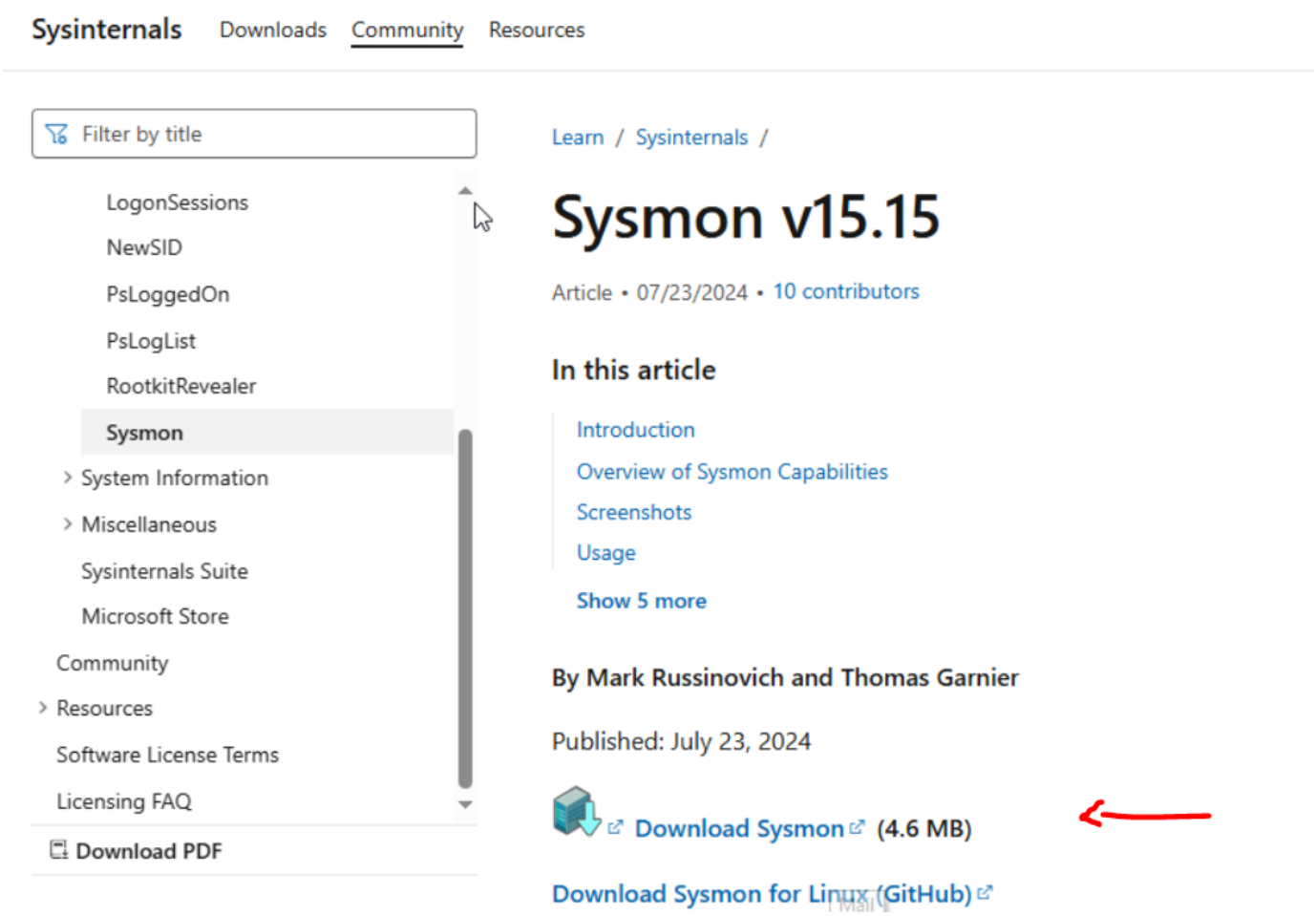
Click Next and select install :



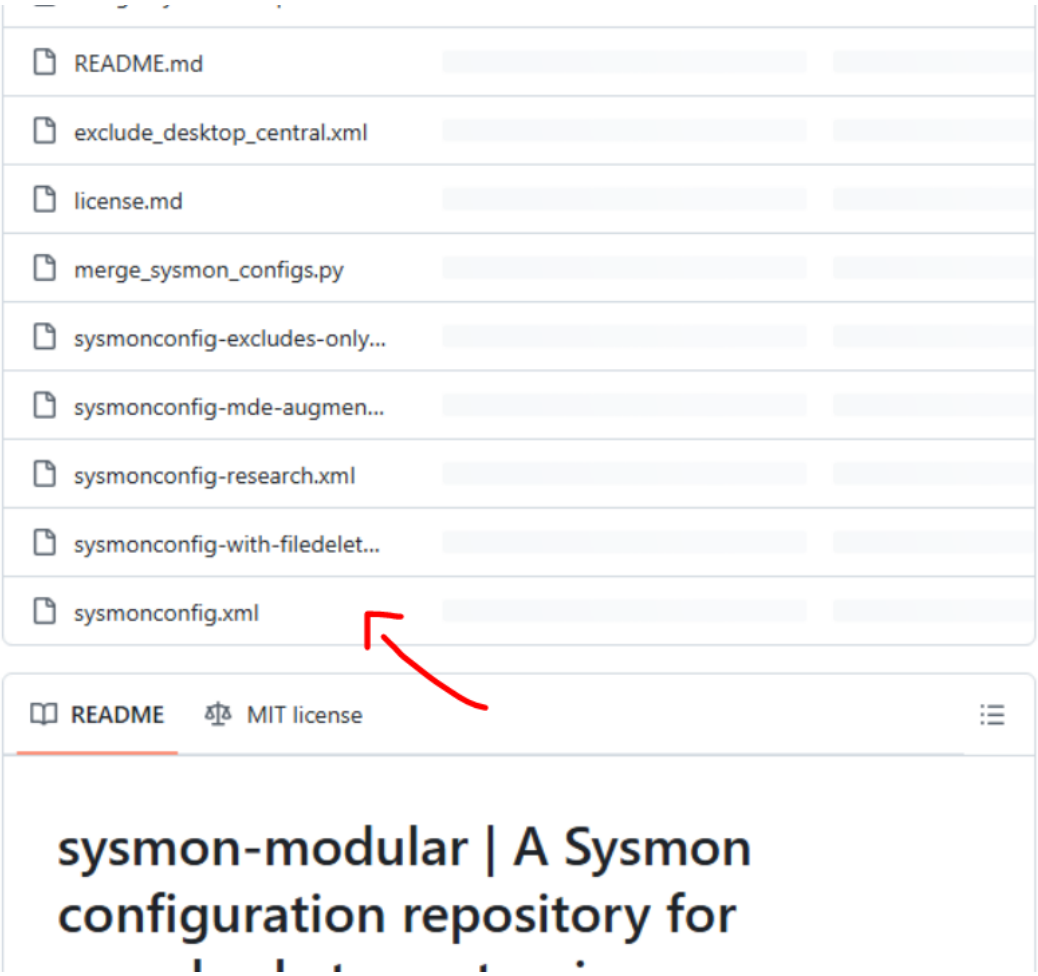
4. Setting up Sysmon

System Monitor (Sysmon) is **a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log**. It provides detailed information about process creations, network connections, and changes to file creation time . Read more here .

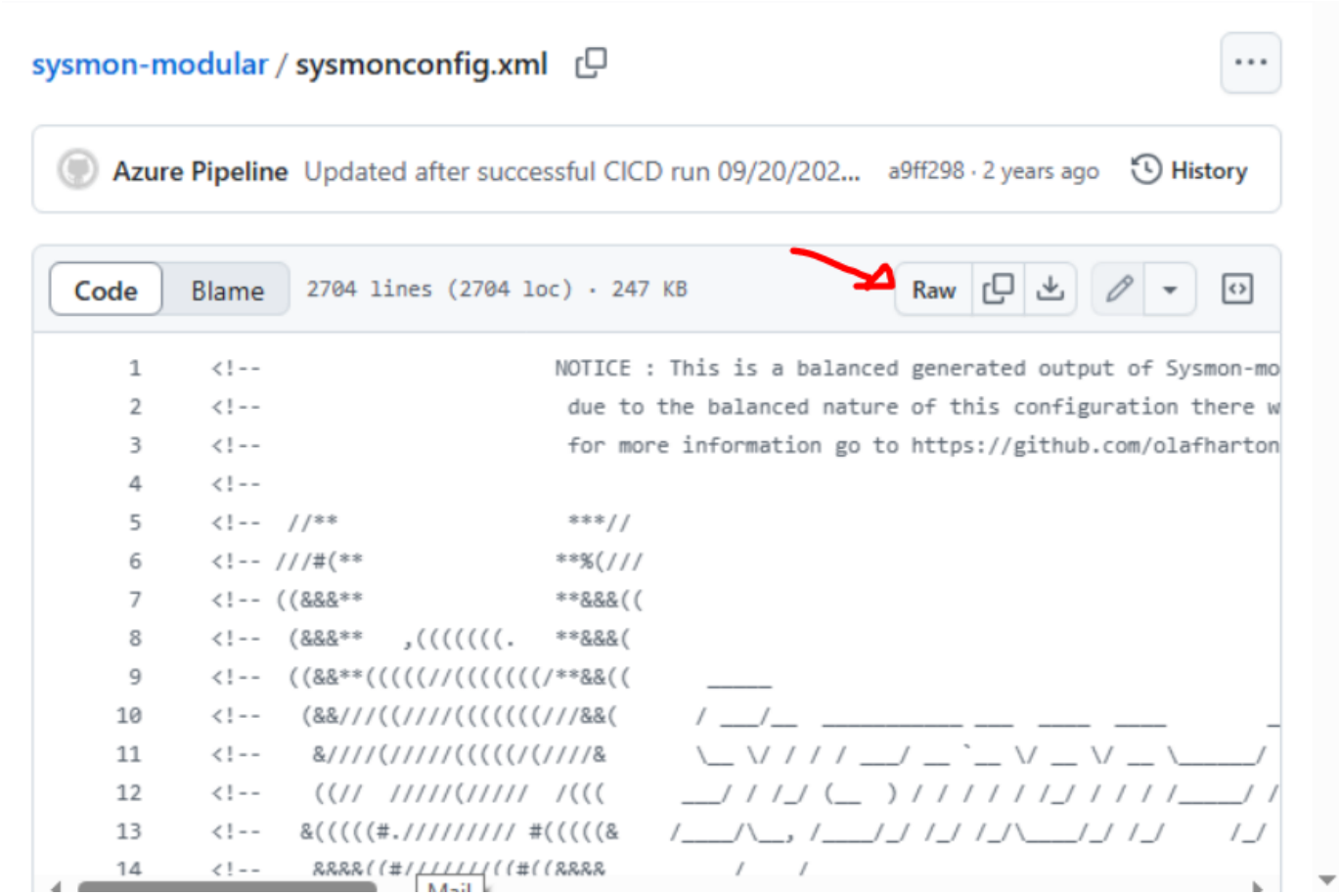
Head over to Sysinternals sysmon download site here and download sysmon:



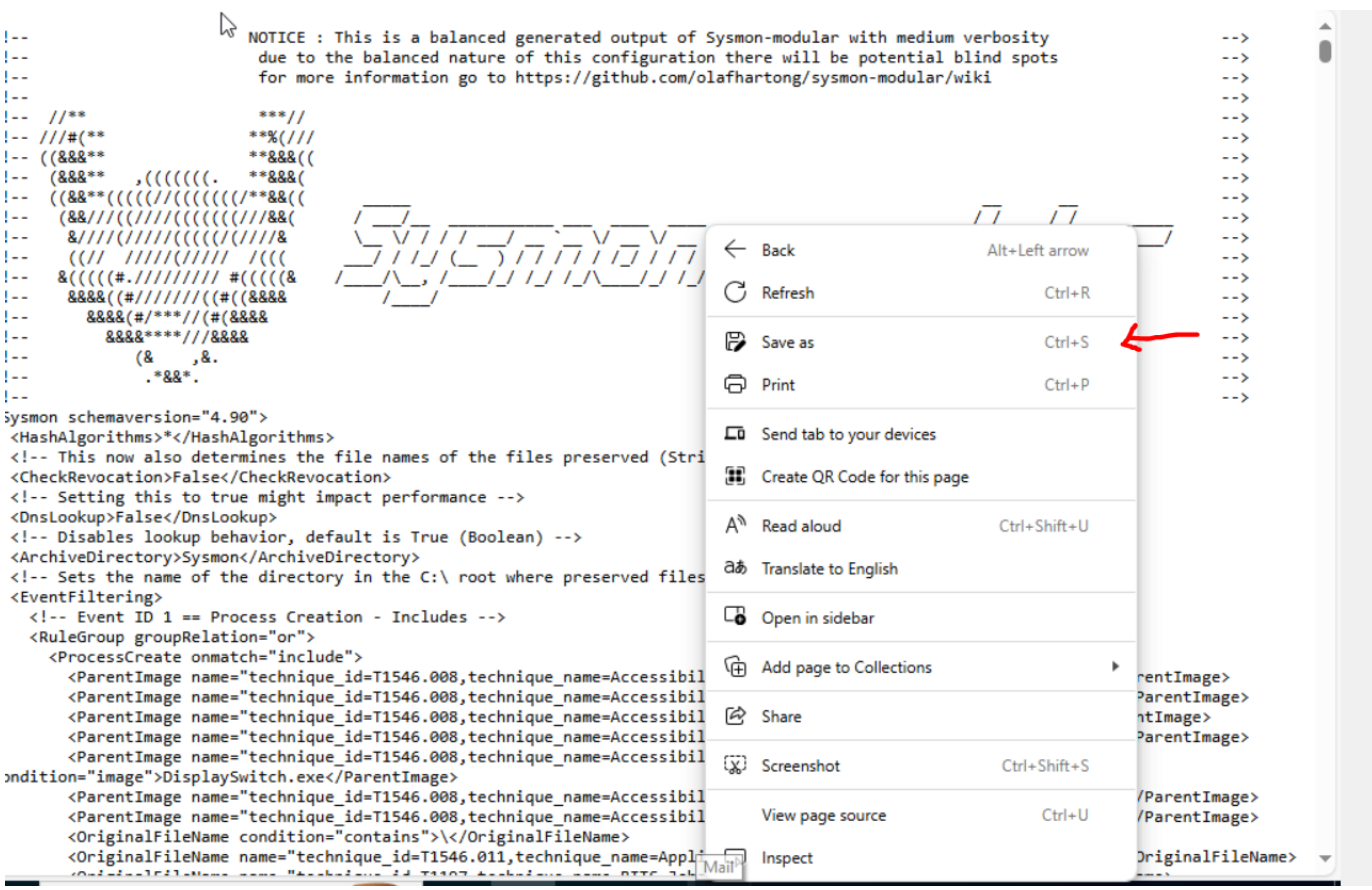
After downloading we now need so download a configuration file , for this lab we will be using the Olaf config and download the RAW sysmonconfig.xml file :
Click and open the sysmonconfig.xml



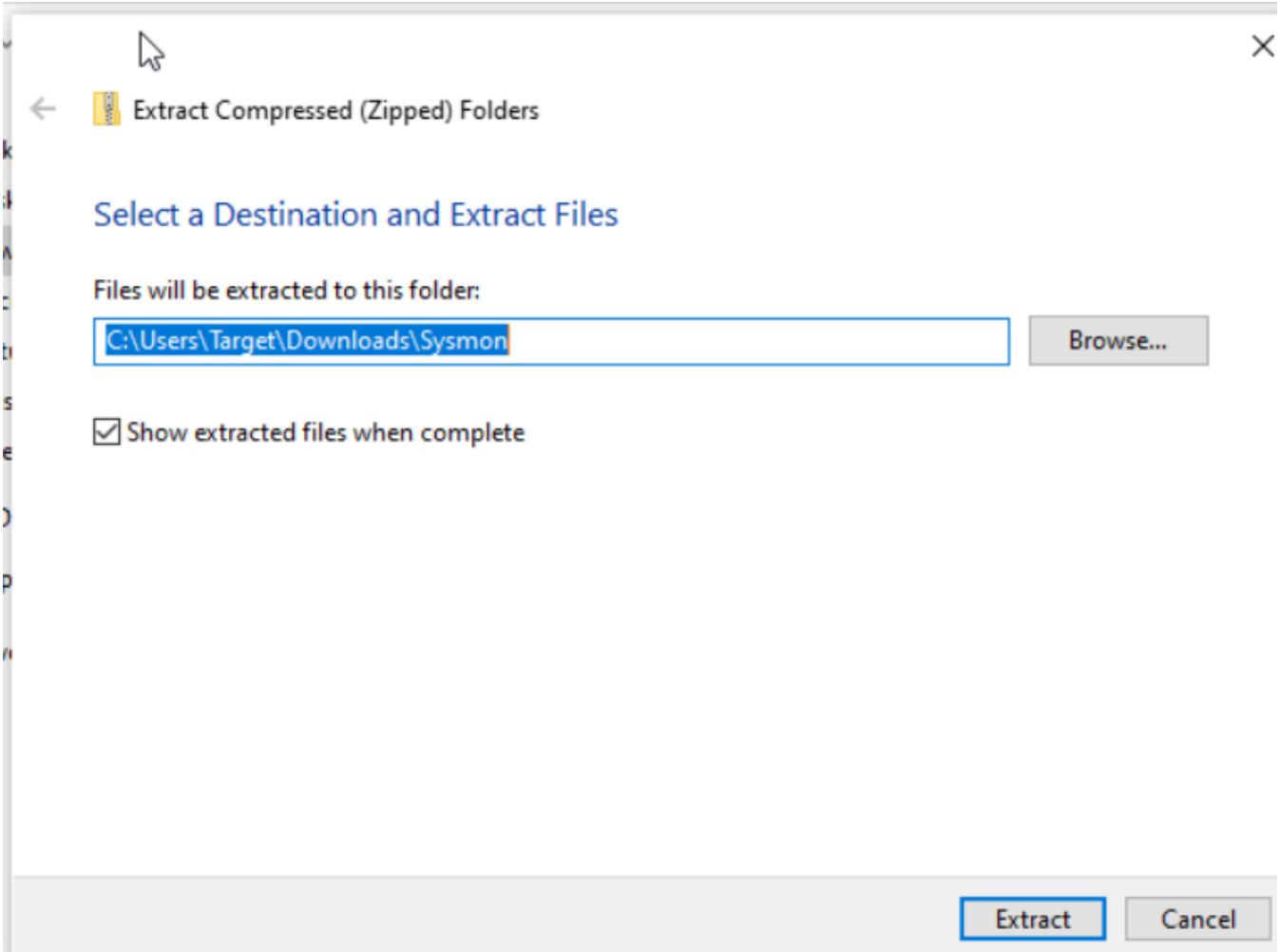
Click on RAW, which will take you to a new page :



Right-click on the page and choose Save as , then select the Downloads directory and save the file :



Now we will need to install sysmon and specify the configuration file we want to use. Navigate to the Downloads directory and extract the sysmon zip file we downloaded :



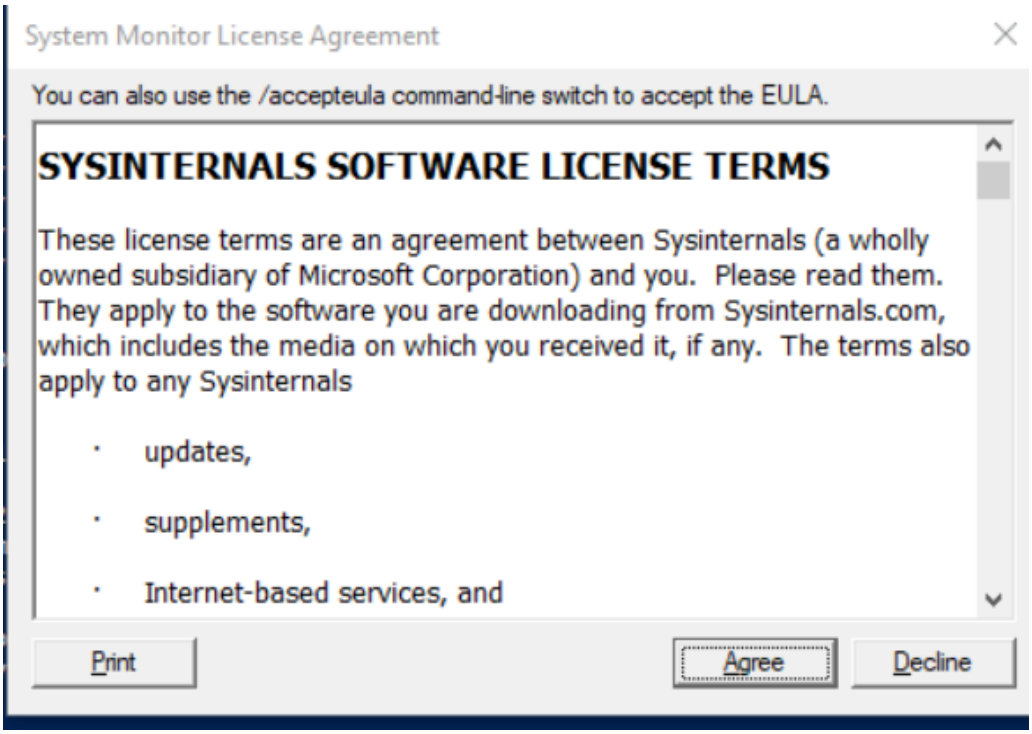
Next copy the sysmonconfig file and paste in the Sysmon directory . After that open up PowerShell with admin rights and navigate to the Sysmon folder we just extracted :

```
PS C:\Users\Target\Downloads\Sysmon> ls

    Directory: C:\Users\Target\Downloads\Sysmon


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         1/22/2025  12:48 PM           7490 Eula.txt
-a----         1/22/2025  12:48 PM        8480560 Sysmon.exe
-a----         1/22/2025  12:48 PM        4563248 Sysmon64.exe
-a----         1/22/2025  12:48 PM        4993440 Sysmon64a.exe
-a----         1/22/2025  12:43 PM         253169 sysmonconfig.xml


PS C:\Users\Target\Downloads\Sysmon>
```

To install Sysmon we run the following command :

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

Agree on the license :




```
PS C:\Users\Target\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\Target\Downloads\Sysmon>
```

Now that Sysmon has been successfully installed, we now need to tell Splunk Universal forwarder what we actually want it to be monitoring . To do this we need to create the input.conf file with the different instructions we want Splunk forwarder to monitor and send to our splunk server . This file will be created in the C ->Program files -> Splunk Universal Forwarder -> etc -> system -> local .

To do this open up notepad as Admin and paste in the following content into it :

" [WinEventLog://Application]

index = endpoint

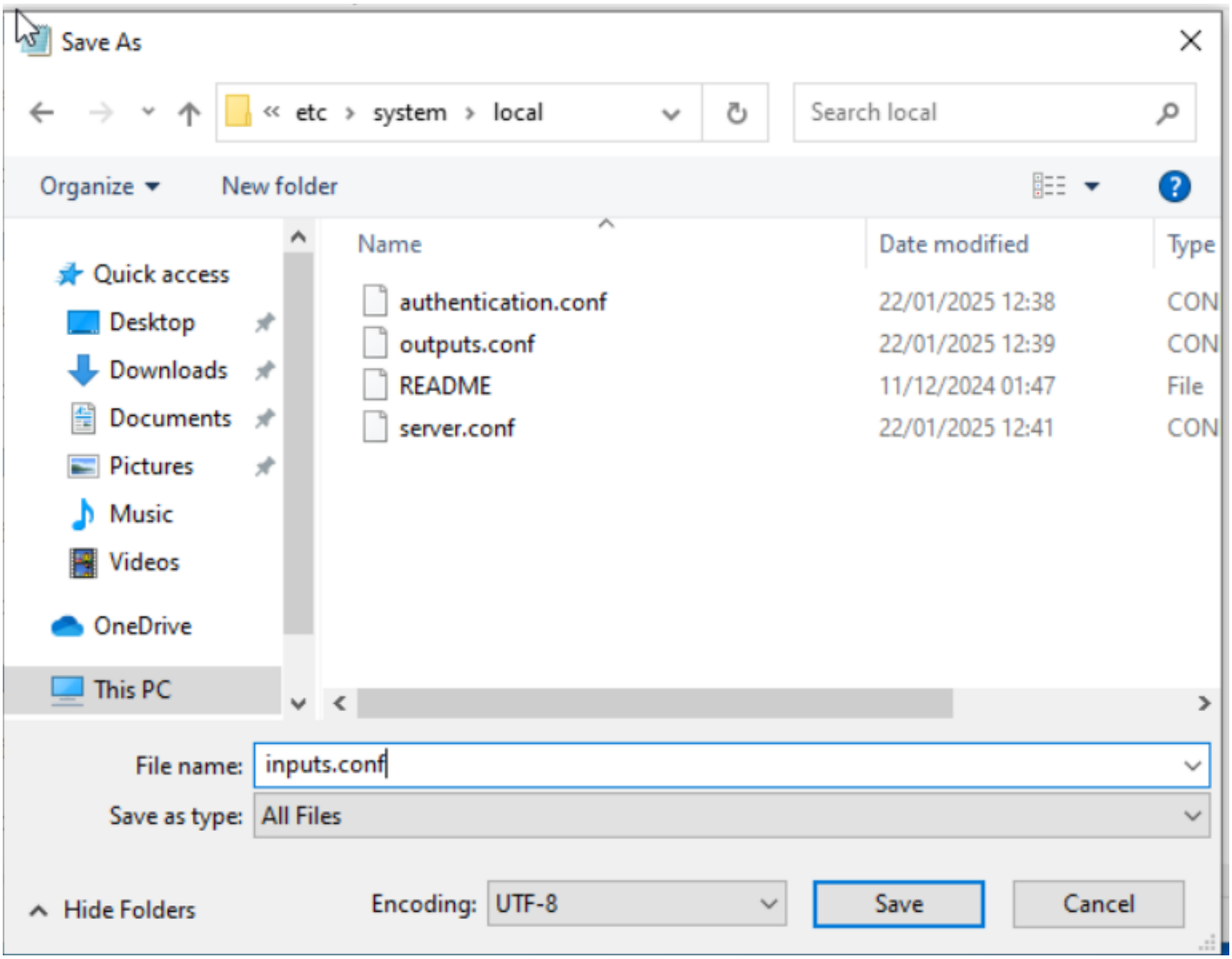
```
disabled = false

[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 "

[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
```

File Edit Format View Help

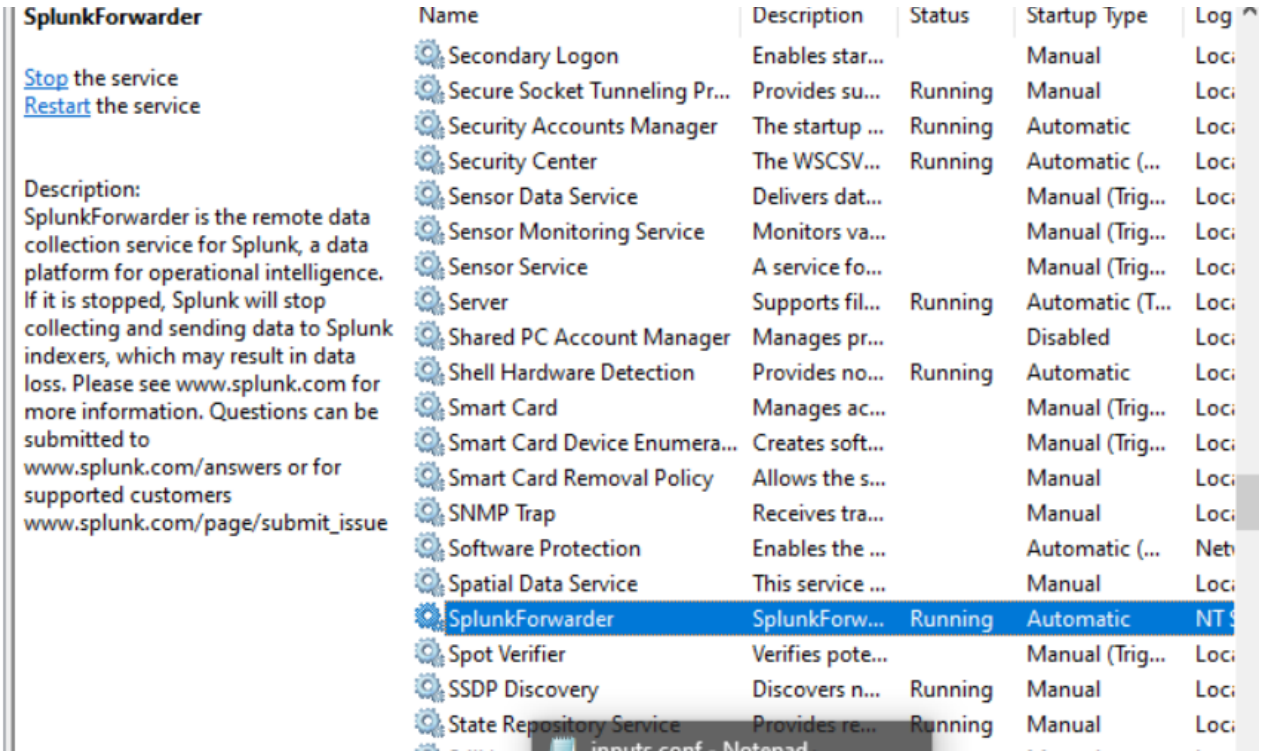
```
[WinEventLog://Application]

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
```

Ln 27, Col 61 100% Windows (CRLF) UTF-8

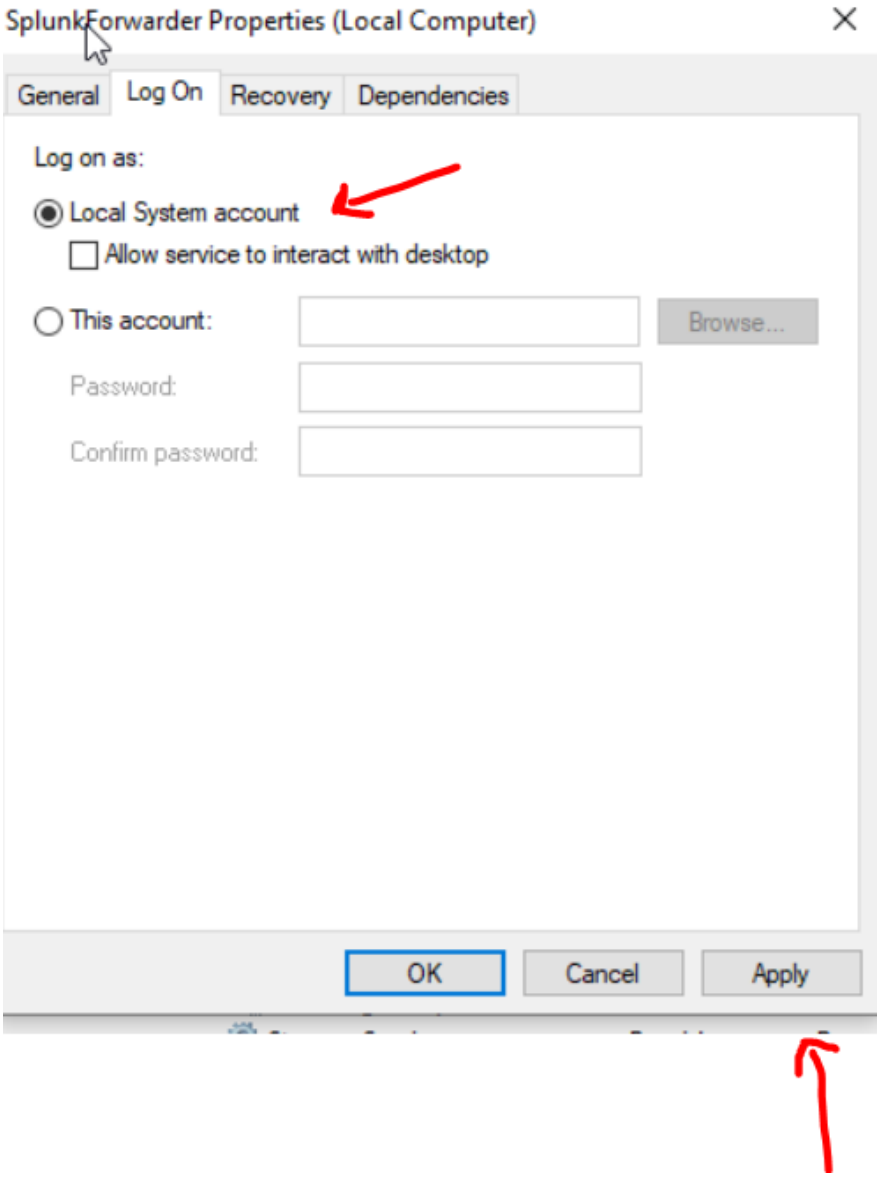
Above the index = endpoint is important because that is where in our splunk server instance we will use to pull logs being forwarded from our target machine to it. Save the file as inputs.conf and paste in the local directory . So at the end it should look like this :



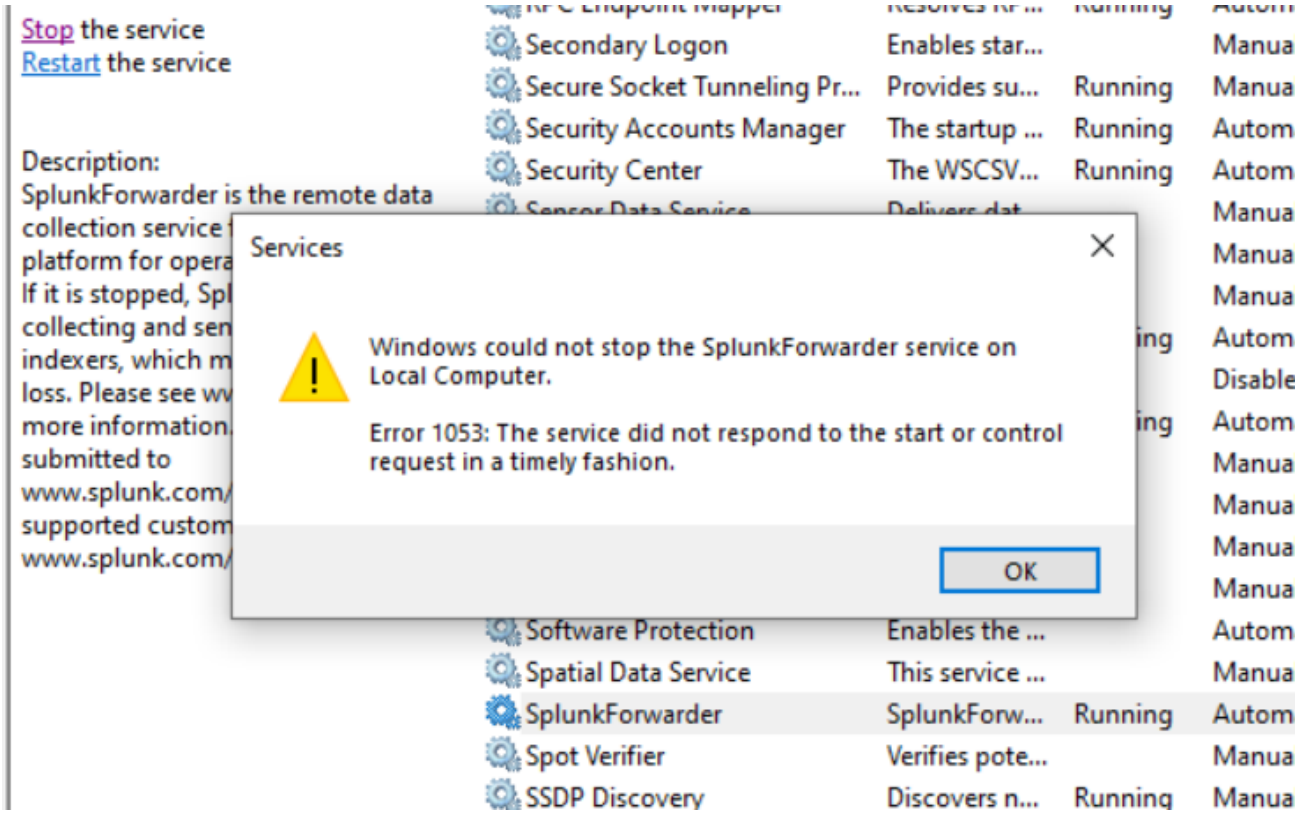
After saving we need to restart the Splunk forwarder service . To do this search for "services" in the windows search box and run it as Administrator . When in it , hit S and look for the Splunk Forwarder service :



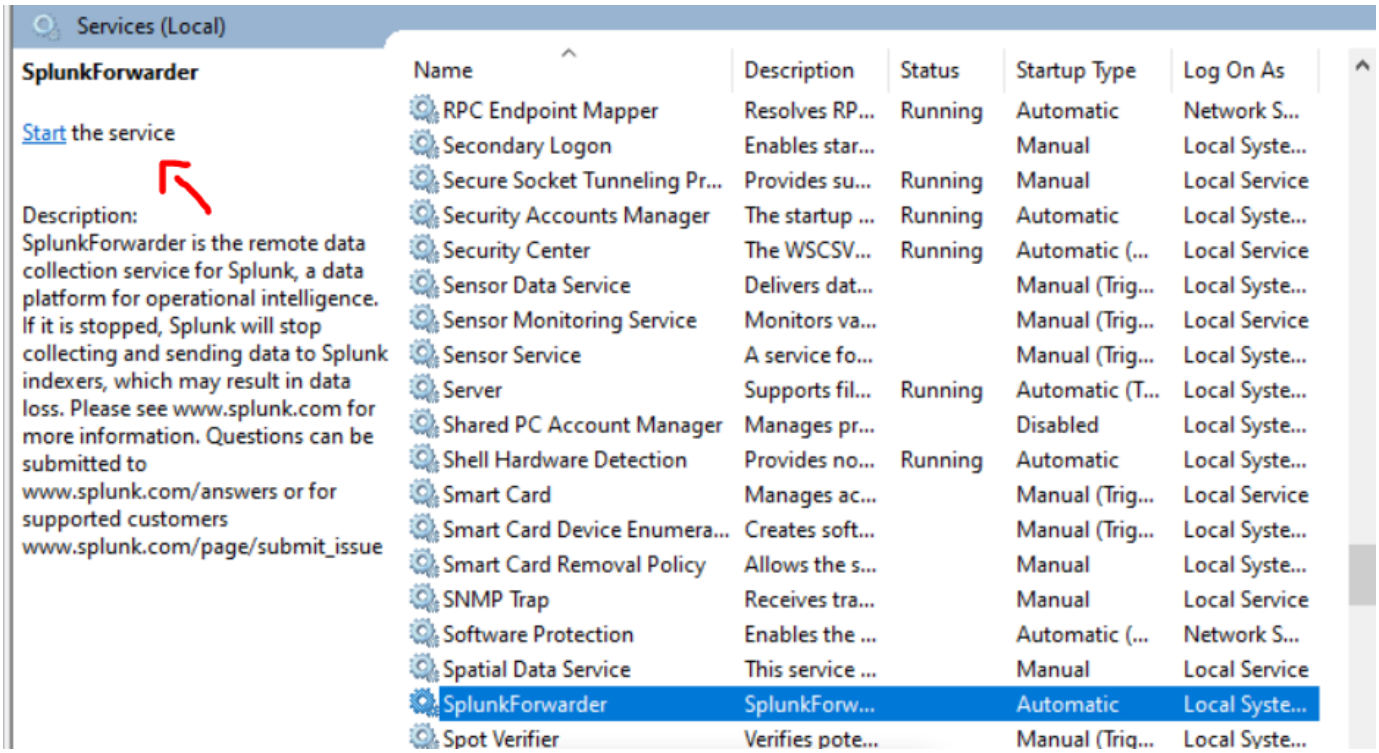
Next we need to change the Logon as type to Local system . To do that double-click on the SplunkForwarder service and navigate to the Logon tab, select Local System account and hit apply :



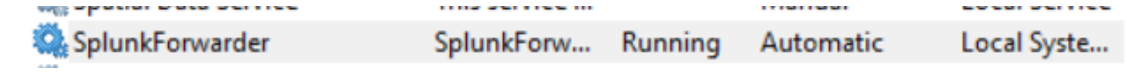
Now we just need to stop the service which will show this :



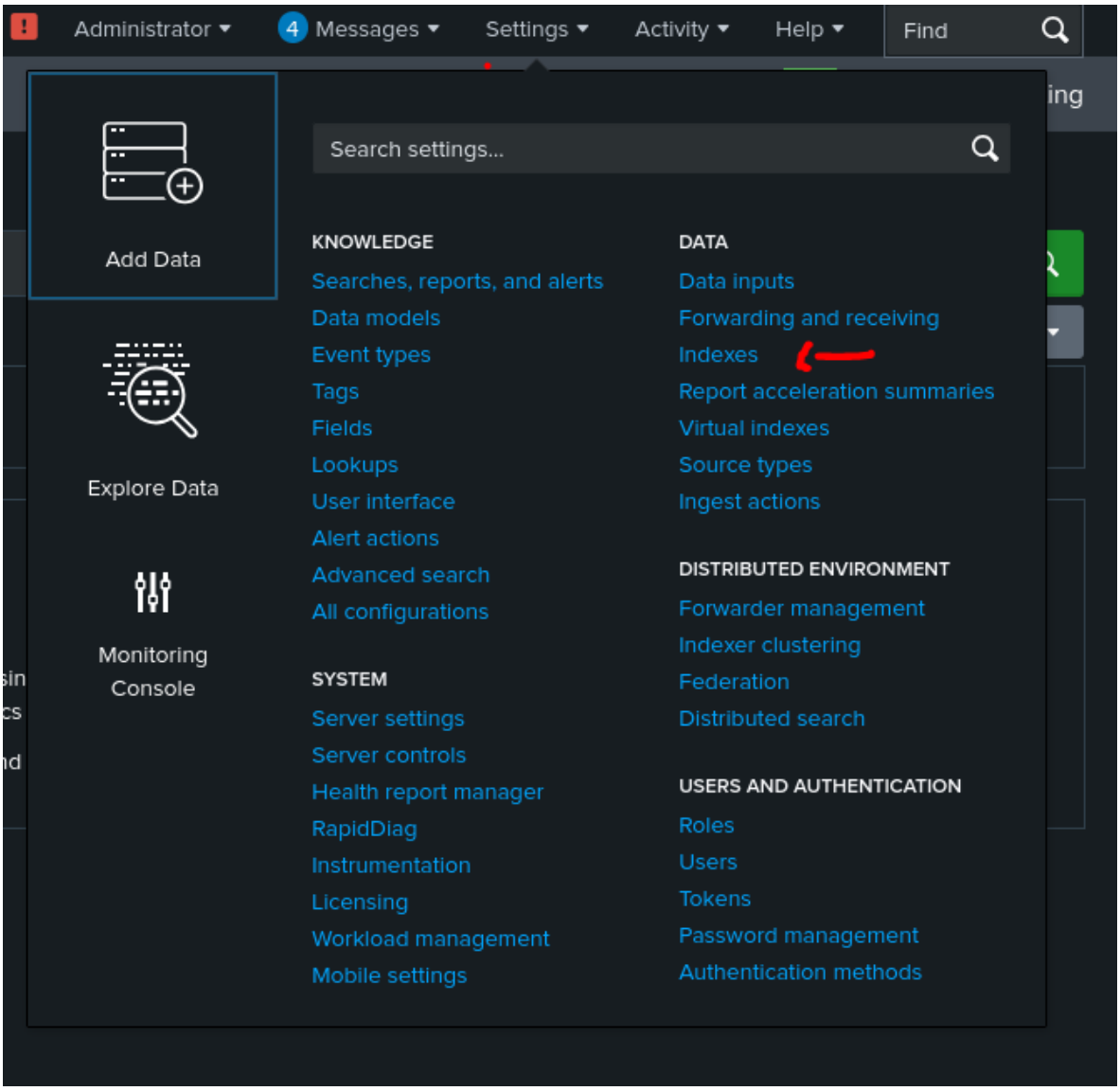
Click on OK and still at your top left you can now click on Start :



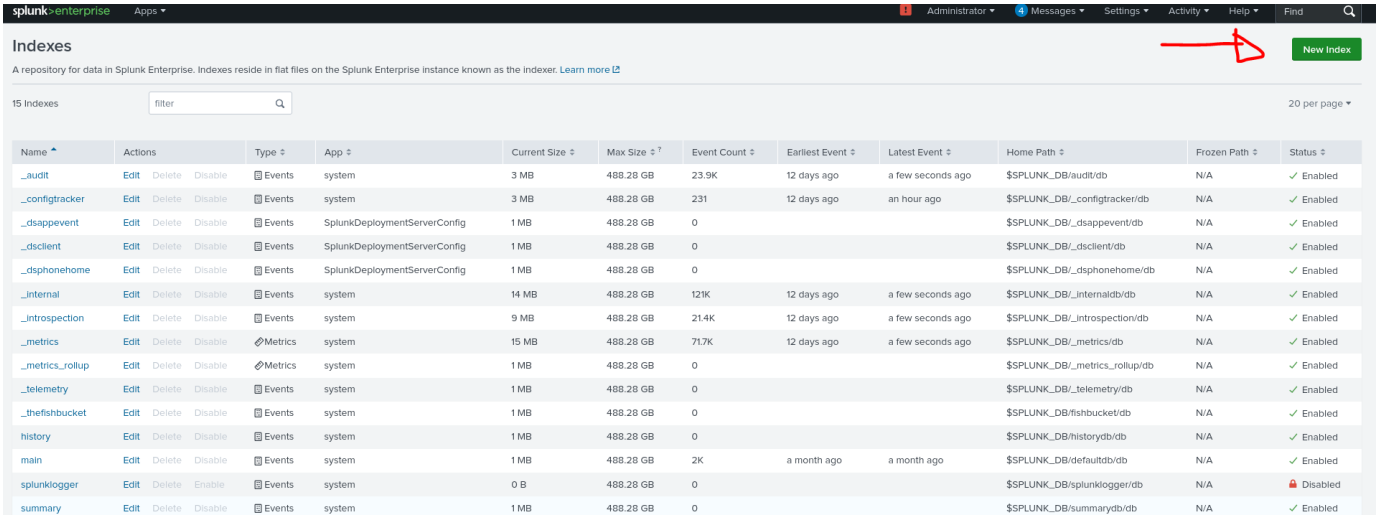
And this is what we will want to see :



After setting up our Forwarder to view the logs coming from this PC we need to login to our Splunk server instance on the browser and Navigate to Settings then indexes :

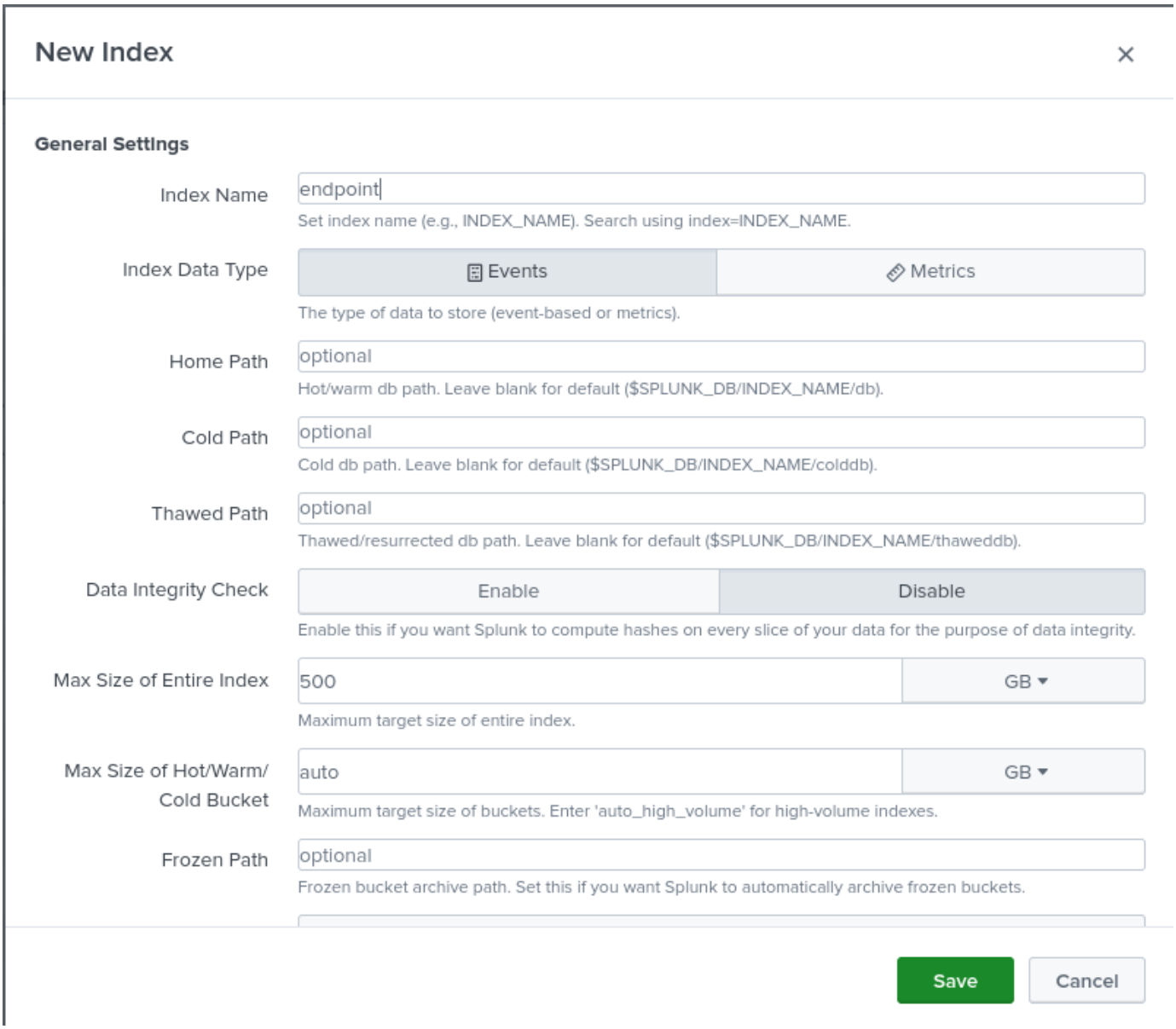


There we can see all the indexes that splunk has but now we will create our own index (the endpoint index) :

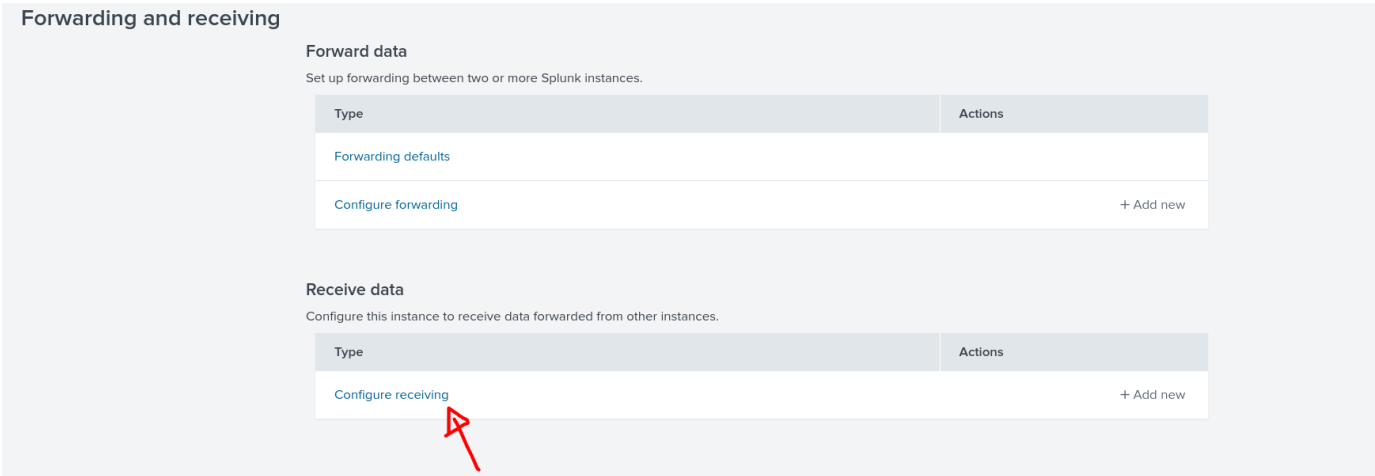


Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen Path	Status
_audit	Edit Delete Disable	Events	system	3 MB	488.28 GB	23.9K	12 days ago	a few seconds ago	$SPLUNK_DB/audit/db	N/A	Enabled
_configtracker	Edit Delete Disable	Events	system	3 MB	488.28 GB	231	12 days ago	an hour ago	$SPLUNK_DB/_configtracker/db	N/A	Enabled
_dsappevent	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0			$SPLUNK_DB/_dsappevent/db	N/A	Enabled
_dsclient	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0			$SPLUNK_DB/_dsclient/db	N/A	Enabled
_dsphonehome	Edit Delete Disable	Events	SplunkDeploymentServerConfig	1 MB	488.28 GB	0			$SPLUNK_DB/_dsphonehome/db	N/A	Enabled
_internal	Edit Delete Disable	Events	system	14 MB	488.28 GB	121K	12 days ago	a few seconds ago	$SPLUNK_DB/_internaldb/db	N/A	Enabled
_introspection	Edit Delete Disable	Events	system	9 MB	488.28 GB	21.4K	12 days ago	a few seconds ago	$SPLUNK_DB/_introspection/db	N/A	Enabled
_metrics	Edit Delete Disable	Metrics	system	15 MB	488.28 GB	71.7K	12 days ago	a few seconds ago	$SPLUNK_DB/_metrics/db	N/A	Enabled
_metrics_rollup	Edit Delete Disable	Metrics	system	1 MB	488.28 GB	0			$SPLUNK_DB/_metrics_rollup/db	N/A	Enabled
_telemetry	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB/_telemetry/db	N/A	Enabled
_thefishbucket	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB/fishbucket/db	N/A	Enabled
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB/historydb/db	N/A	Enabled
main	Edit Delete Disable	Events	system	1 MB	488.28 GB	2K	a month ago	a month ago	$SPLUNK_DB/defaultdb/db	N/A	Enabled
splunklogger	Edit Delete Enable	Events	system	0 B	488.28 GB	0			$SPLUNK_DB/splunklogger/db	N/A	Disabled
summary	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB/summarydb/db	N/A	Enabled

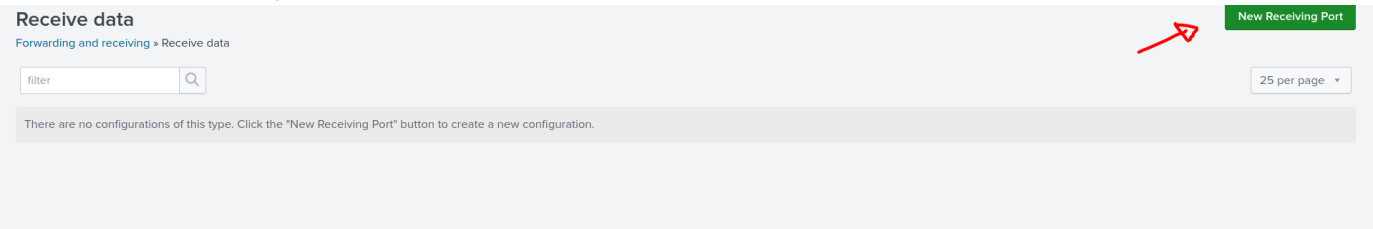
Click on New Index and set the name to endpoint and save :



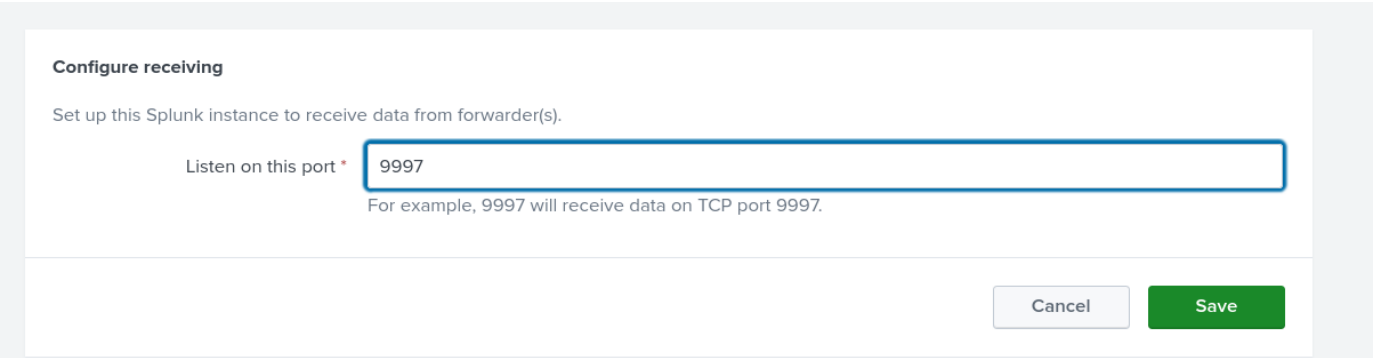
Next we need to enable the splunk server to be able to receive the data. To do that click on Settings at the top tool bar and navigate to "Forwarding and receiving" and click on configure receiving:



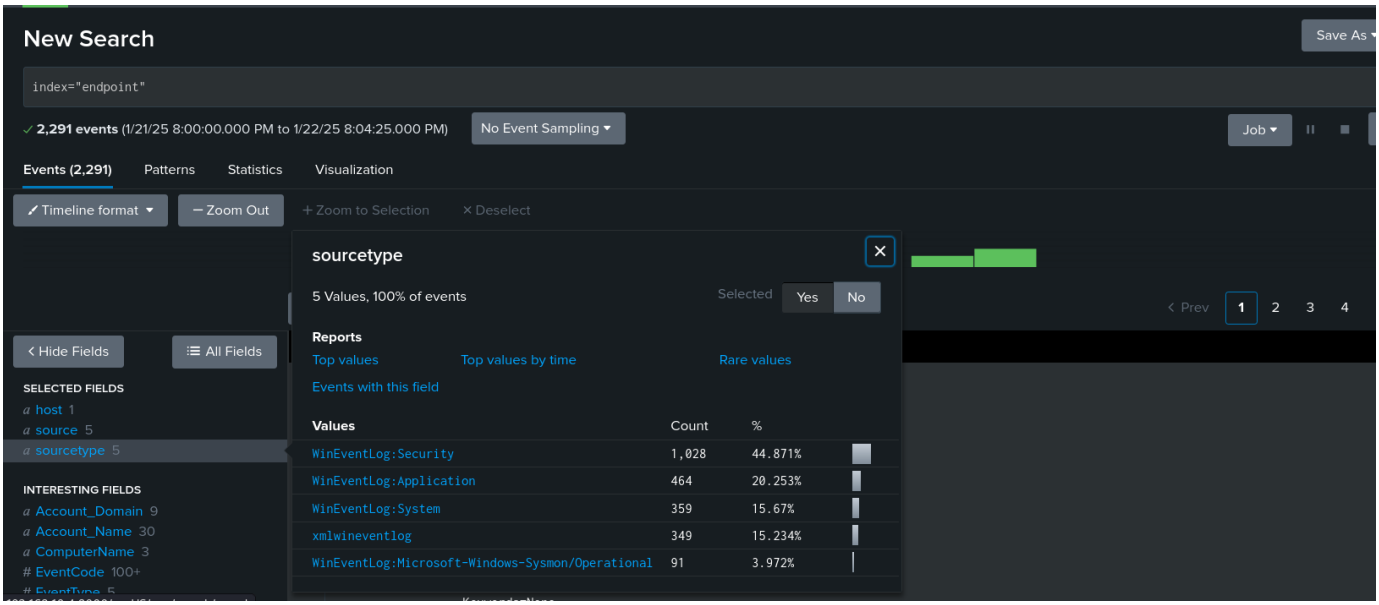
Click on New receiving port :



Input the default port we configured during the forwarder setup i.e. 9997 and click save :



Saving and heading back to Search and Reporting we can query for the endpoint index and here is what it should look like :



The same steps regarding the Splunk Forwarder and sysmon are done on the domain controller too.