

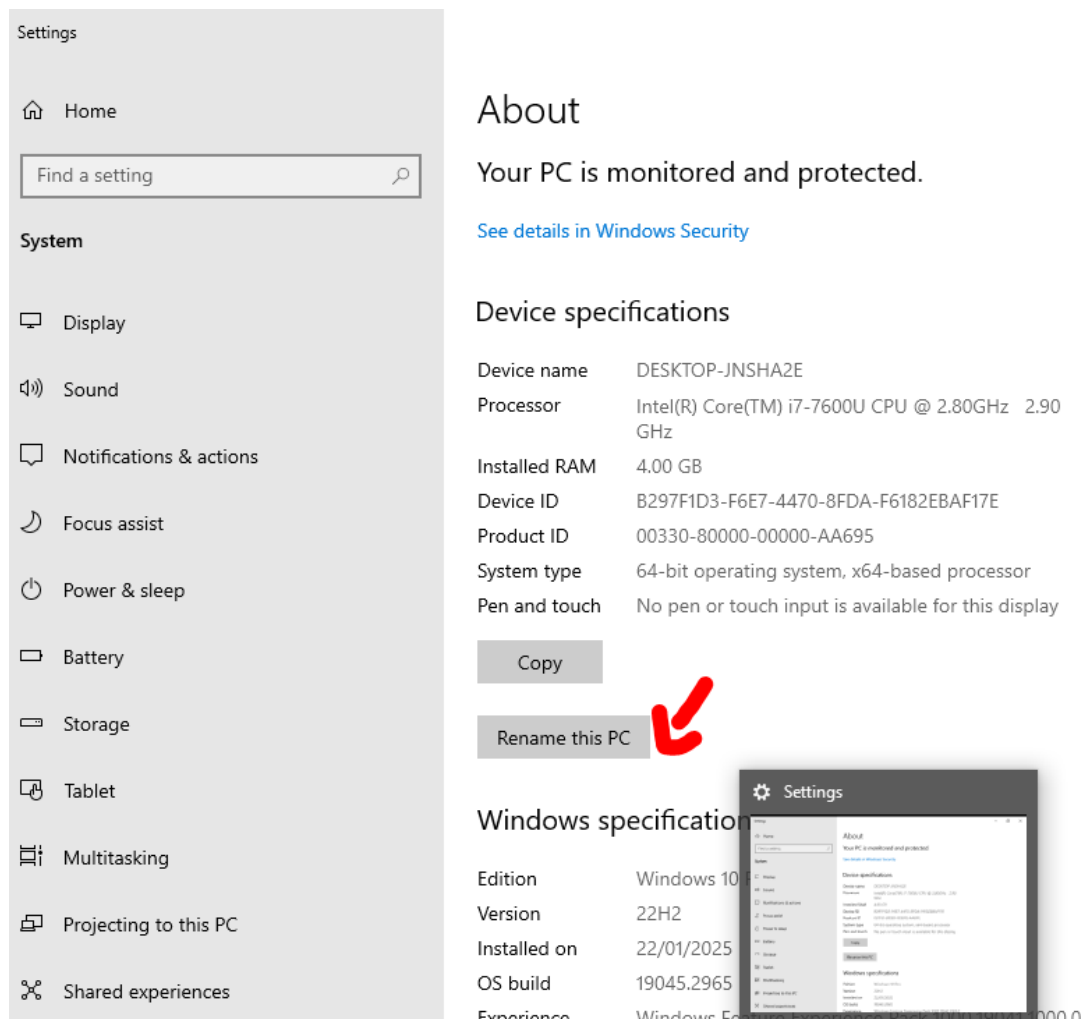
3. Sysmon client domain controller setup

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.

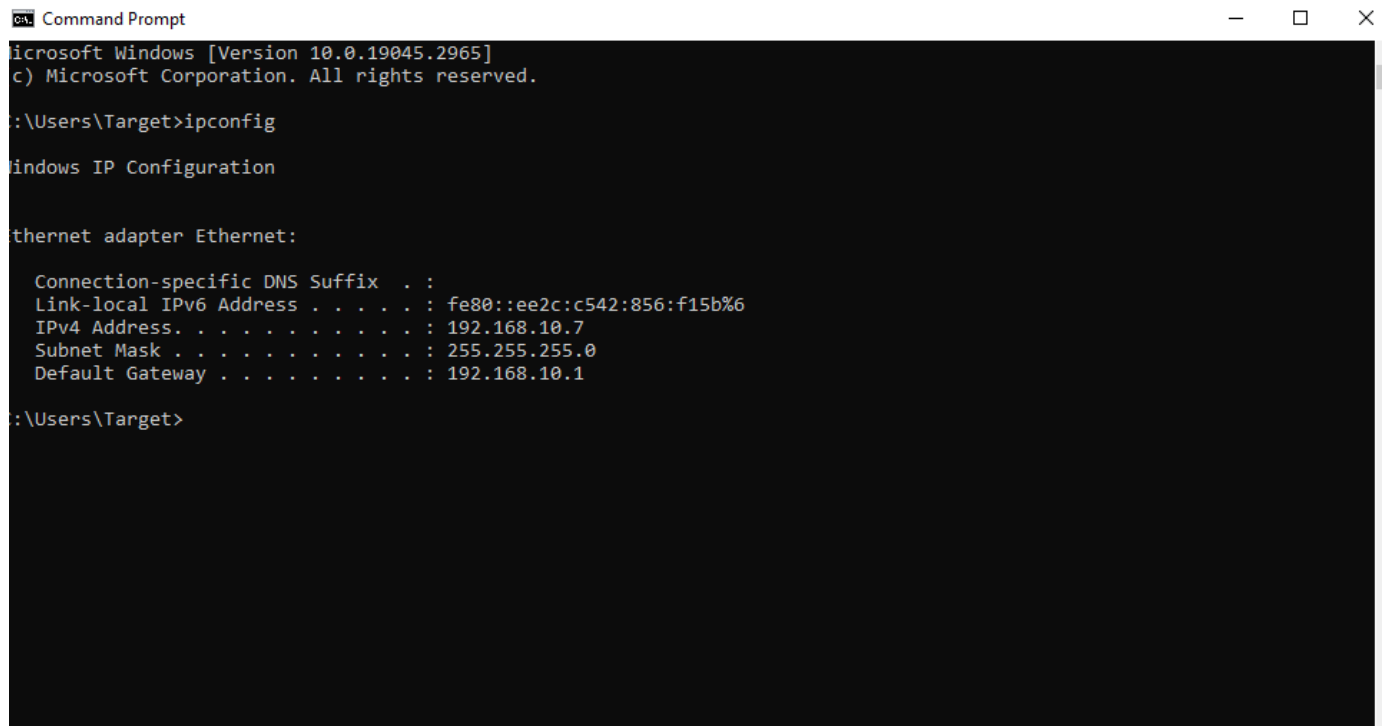
To rename the client simply search for pc in the search box , right-click and go to properties --> Rename this PC :



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):



```
Command Prompt
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Target>ipconfig

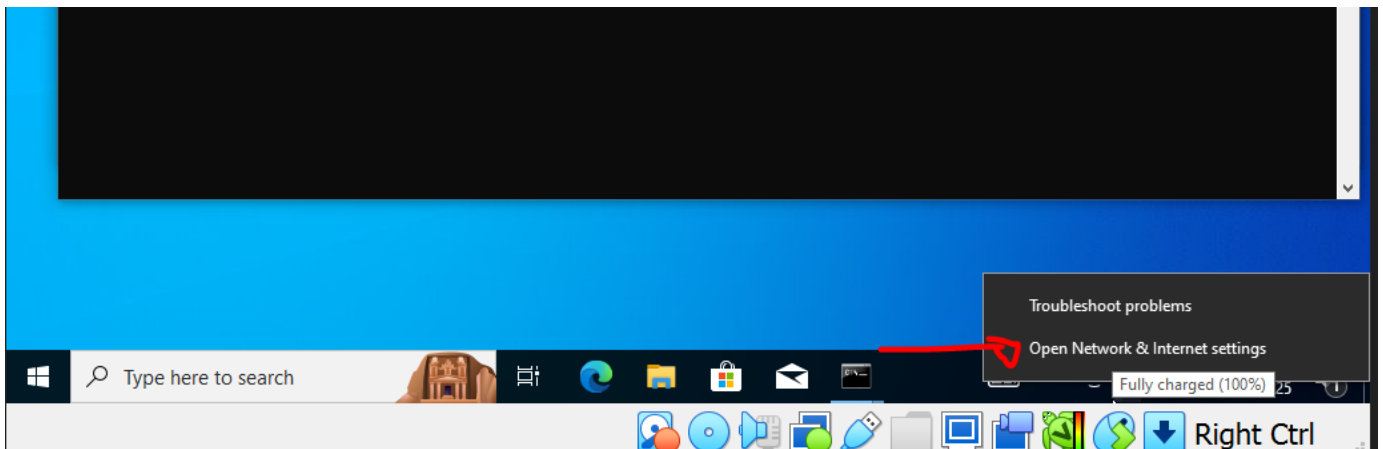
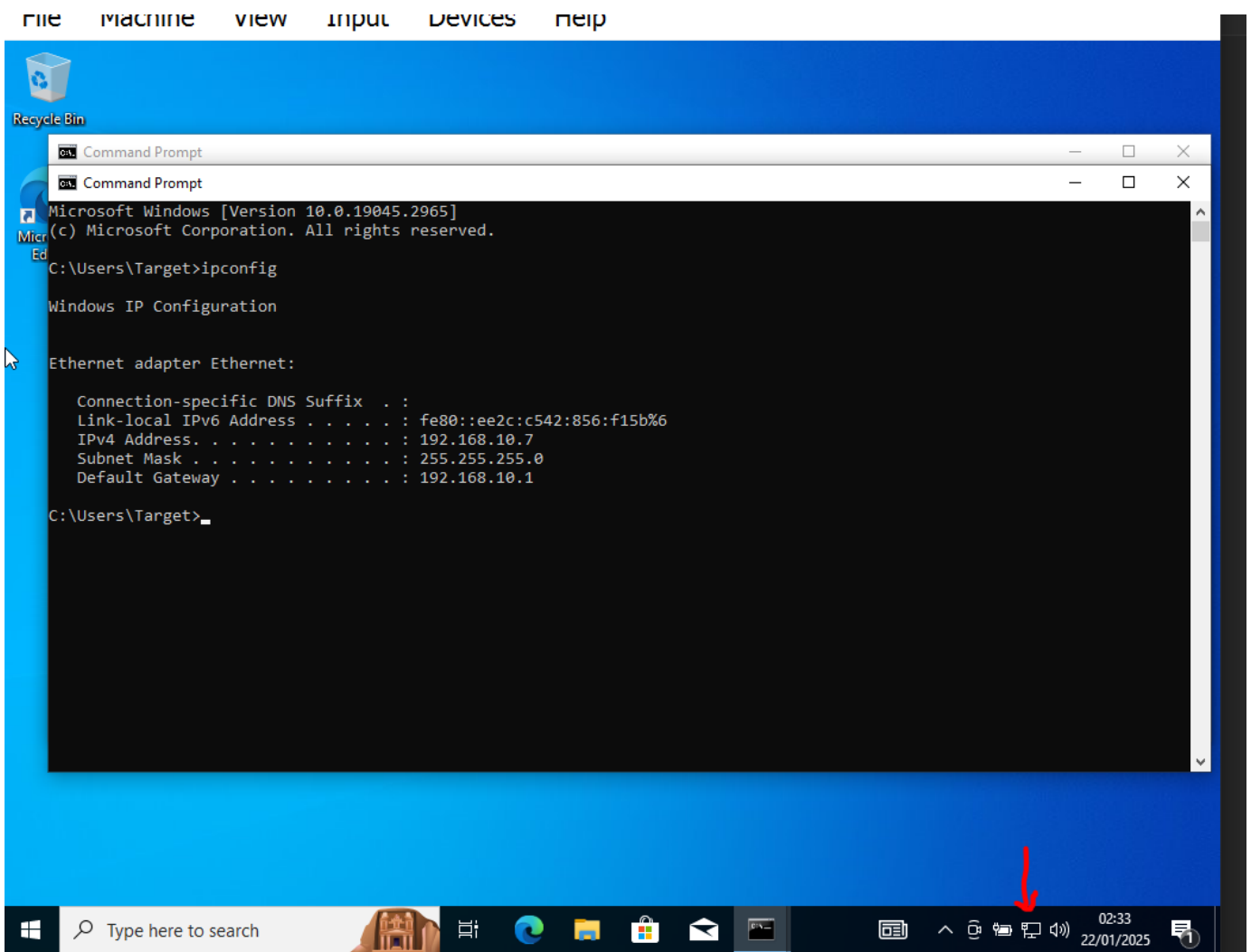
Windows IP Configuration

Ethernet adapter Ethernet:

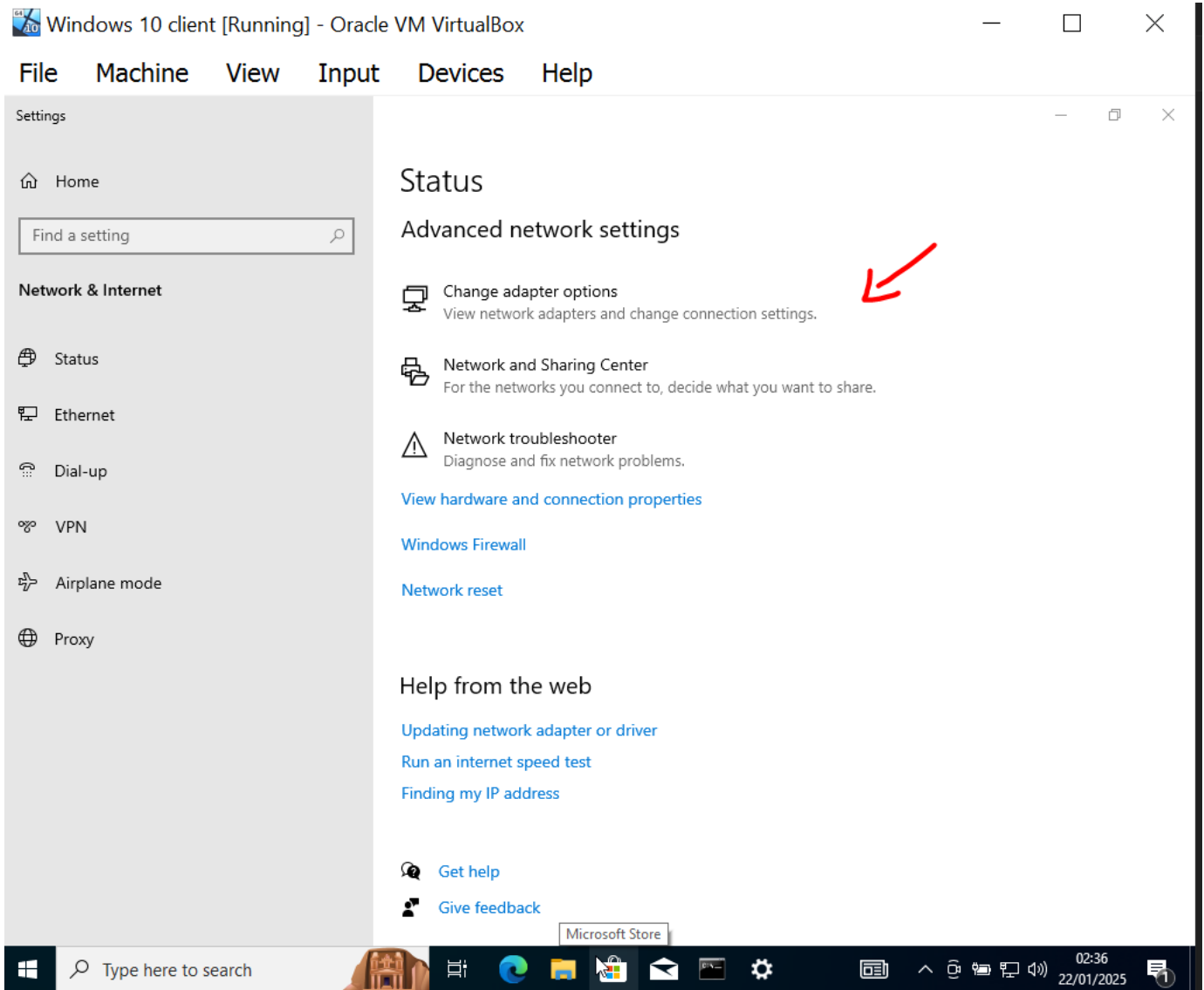
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::ee2c:c542:856:f15b%6
    IPv4 Address. . . . . : 192.168.10.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1

C:\Users\Target>
```

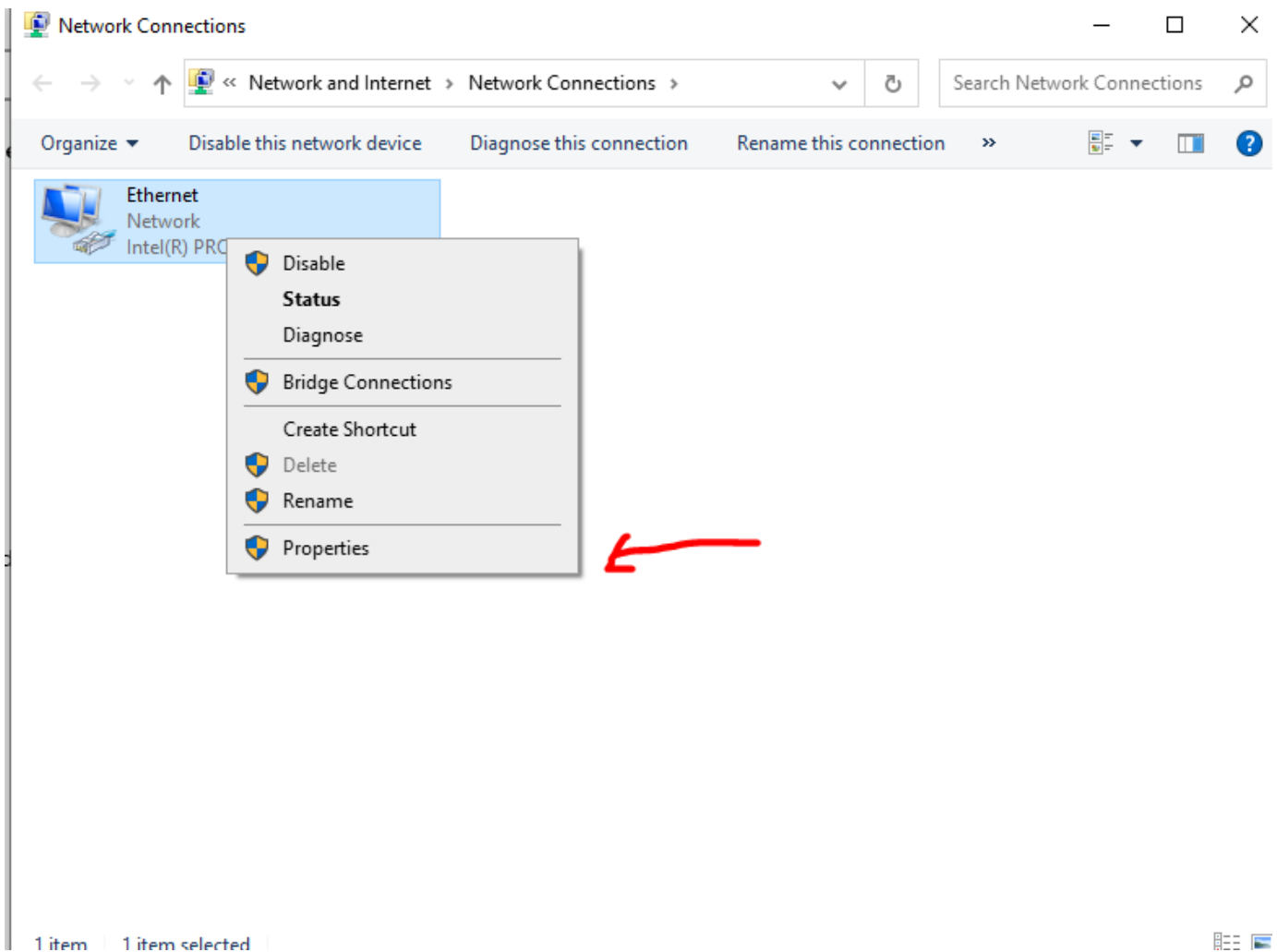
To change that , right-click on the network icon at the bottom right of your windows VM :



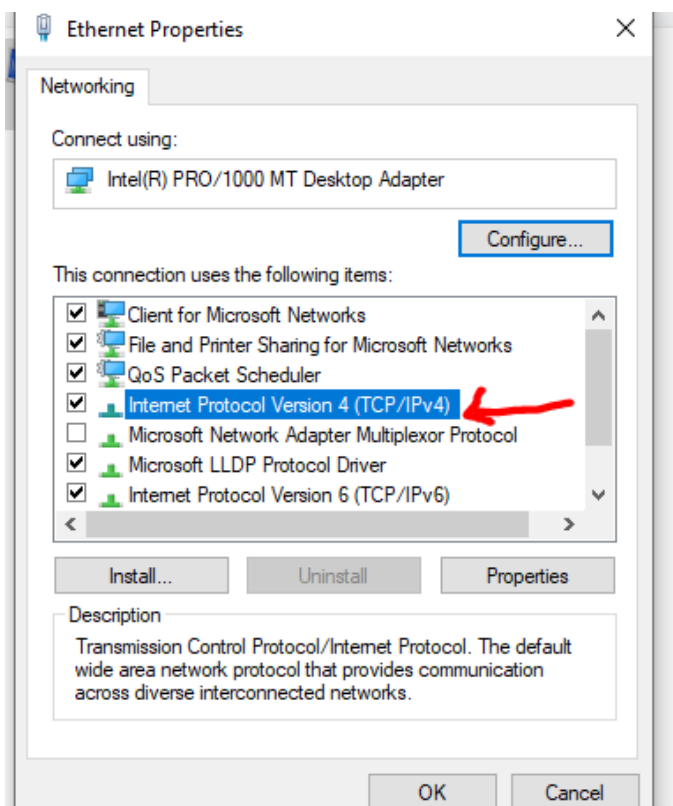
Scroll down and click on Change adapter options :



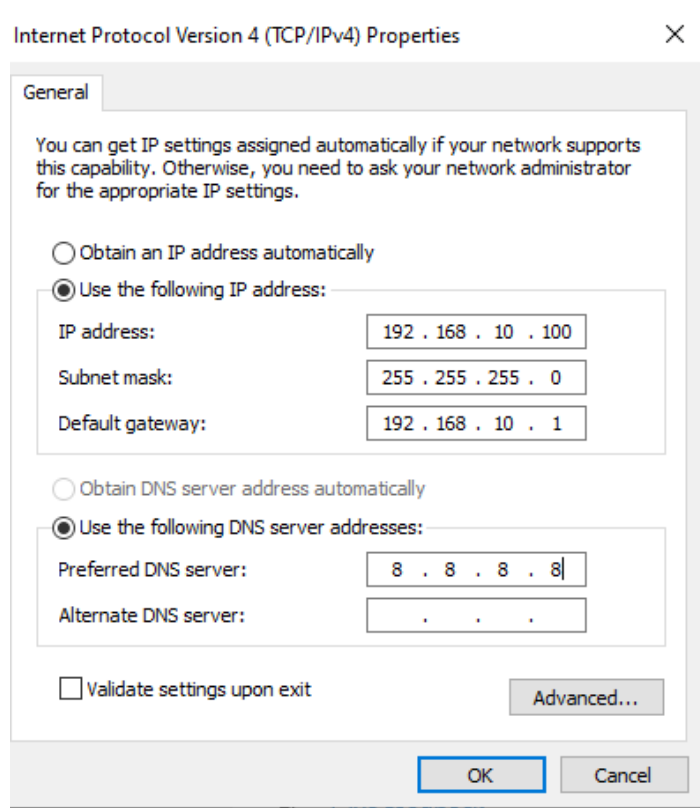
Right-click on the adapter, then click on properties :



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 :

```
C:\Users\Target>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::ee2c:c542:856:f15b%6
    IPv4 Address. . . . . : 192.168.10.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1

C:\Users\Target>
```

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 :

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.



[Get My Free Download](#)

Additional products

Explore more trials and downloads to see which Splunk products are the right fit for you.

We will select the 64bit windows msi download:

Splunk Universal Forwarder 9.4.0

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

 Mac OS

 Free BSD

 Solaris

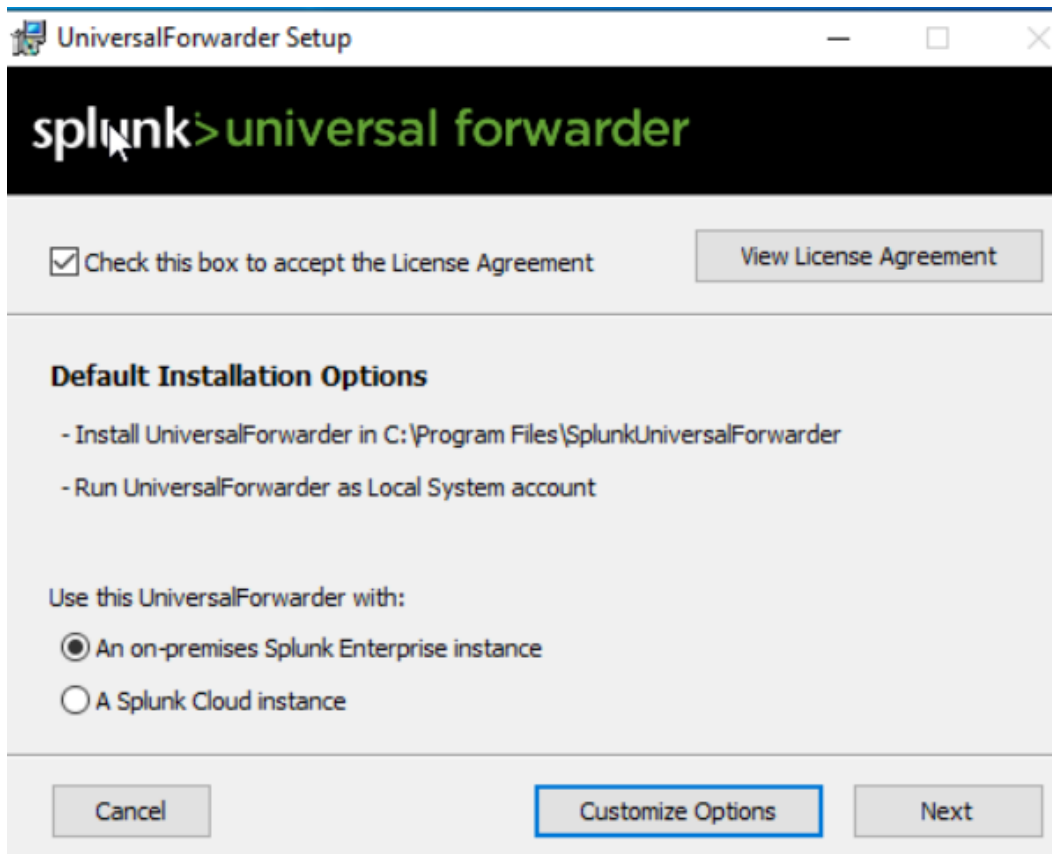
 AIX

32-bit	Windows 10	.msi	64.99 MB	Download Now 	Copy wget link 	More ▾
64-bit	Windows 10, 11 Windows Server 2019, 2022	.msi	176.63 MB	Download Now 	Copy wget link 	More ▾

[Release Notes](#) | [System Requirements](#) | [Previous Releases](#) | [All Other Downloads](#)

[Mail](#)

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



UniversalForwarder Setup

splunk>universal forwarder

☒ Check this box to accept the License Agreement [View License Agreement](#)

Default Installation Options

- Install UniversalForwarder in C:\Program Files\SplunkUniversalForwarder
- Run UniversalForwarder as Local System account

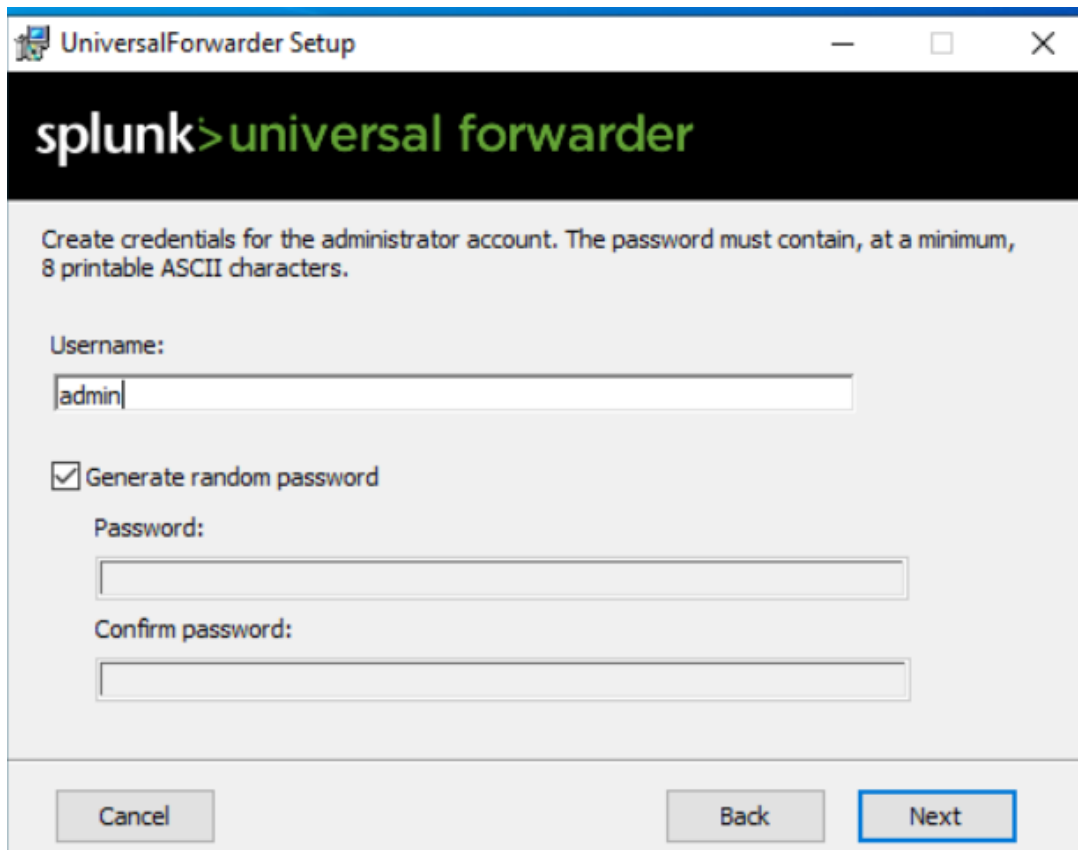
Use this UniversalForwarder with:

☒ An on-premises Splunk Enterprise instance

☐ A Splunk Cloud instance

[Cancel](#) [Customize Options](#) [Next](#)

Click on Next:



UniversalForwarder Setup

splunk>universal forwarder

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

Username:

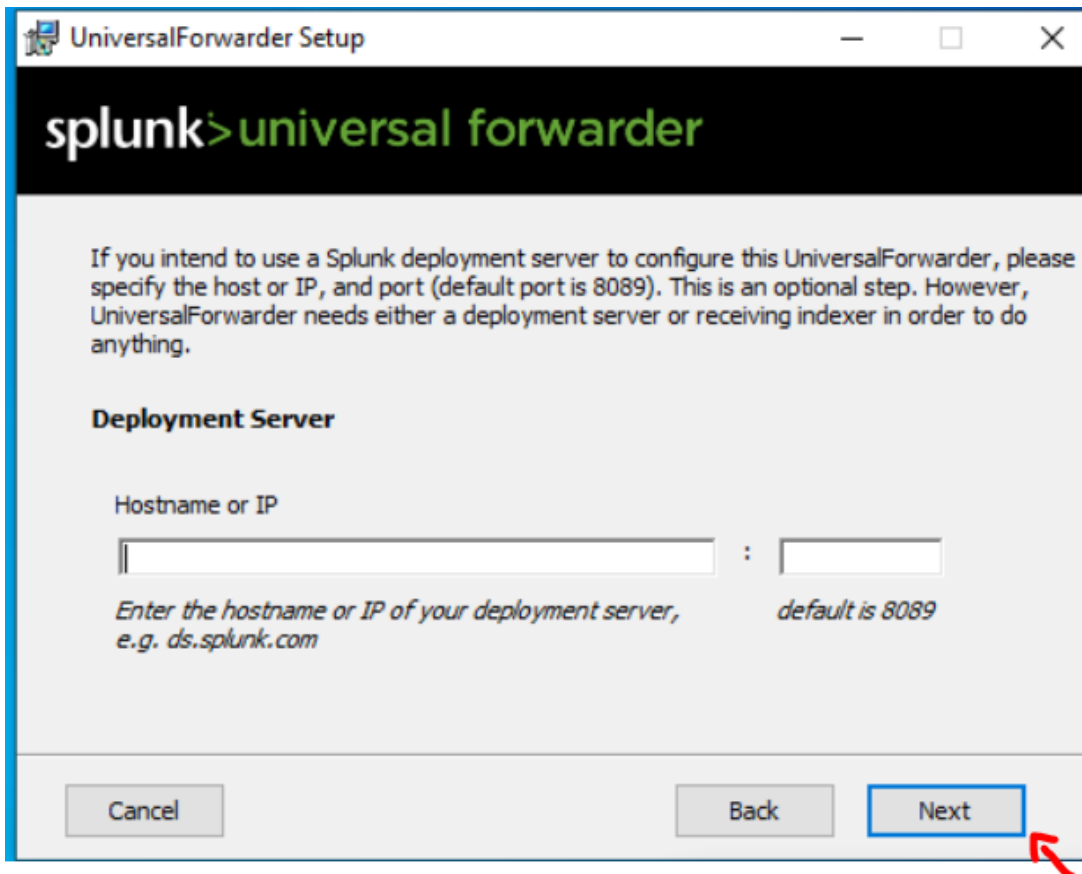
☒ Generate random password

Password:

Confirm password:

[Cancel](#) [Back](#) [Next](#)

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



UniversalForwarder Setup

splunk>universal forwarder

If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Deployment Server

Hostname or IP

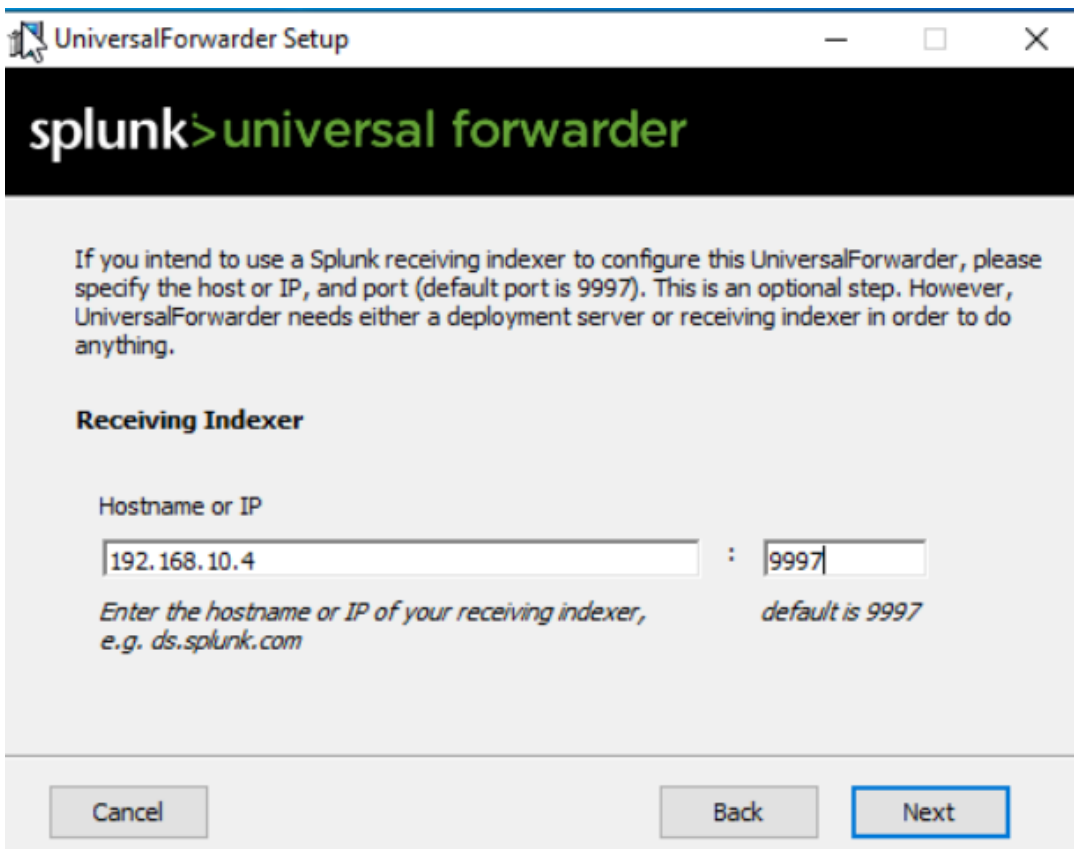
:

Enter the hostname or IP of your deployment server, e.g. ds.splunk.com *default is 8089*

Cancel Back Next

A red arrow points to the 'Next' button.

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:



UniversalForwarder Setup

splunk>universal forwarder

If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Receiving Indexer

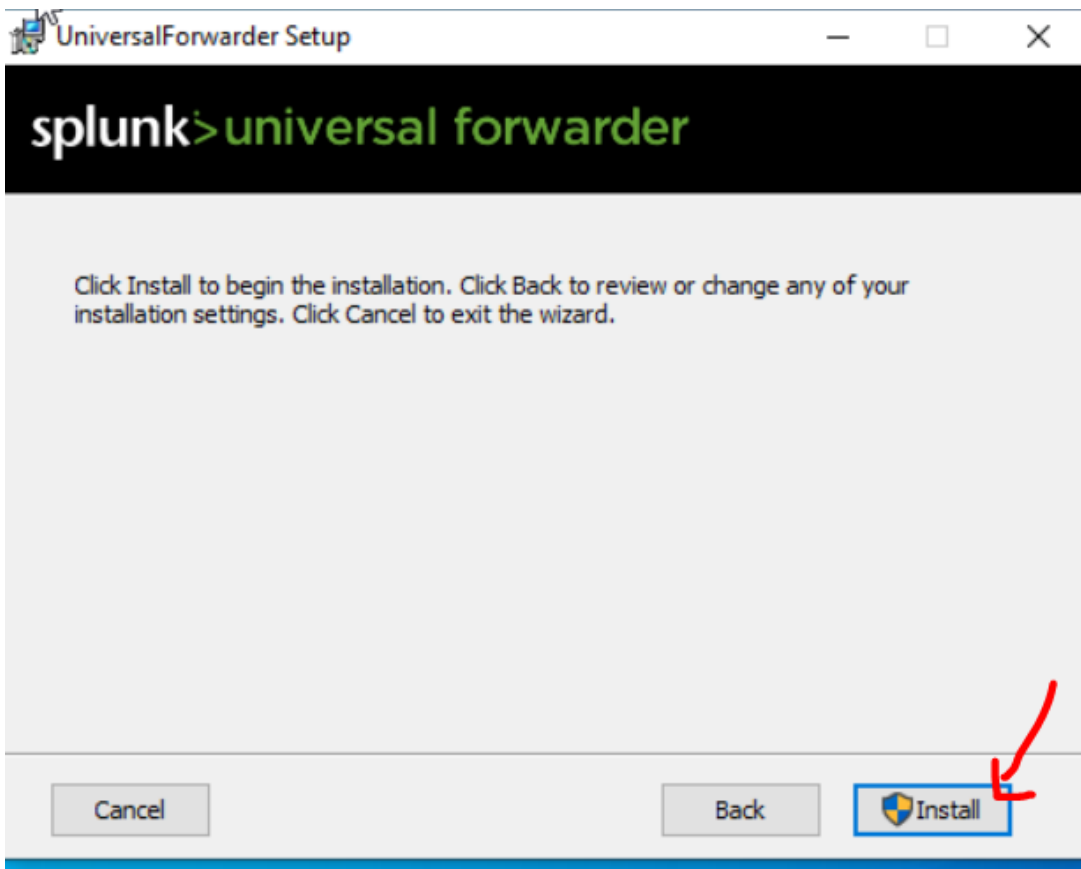
Hostname or IP

:

Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com *default is 9997*

Cancel Back Next

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:

Filter by title

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 v15.15

Article • 07/23/2024 • 10 contributors

In this article

[Introduction](#)
[Overview of Sysmon Capabilities](#)
[Screenshots](#)
[Usage](#)
[Show 5 more](#)

By Mark Russinovich and Thomas Garnier

Published: July 23, 2024

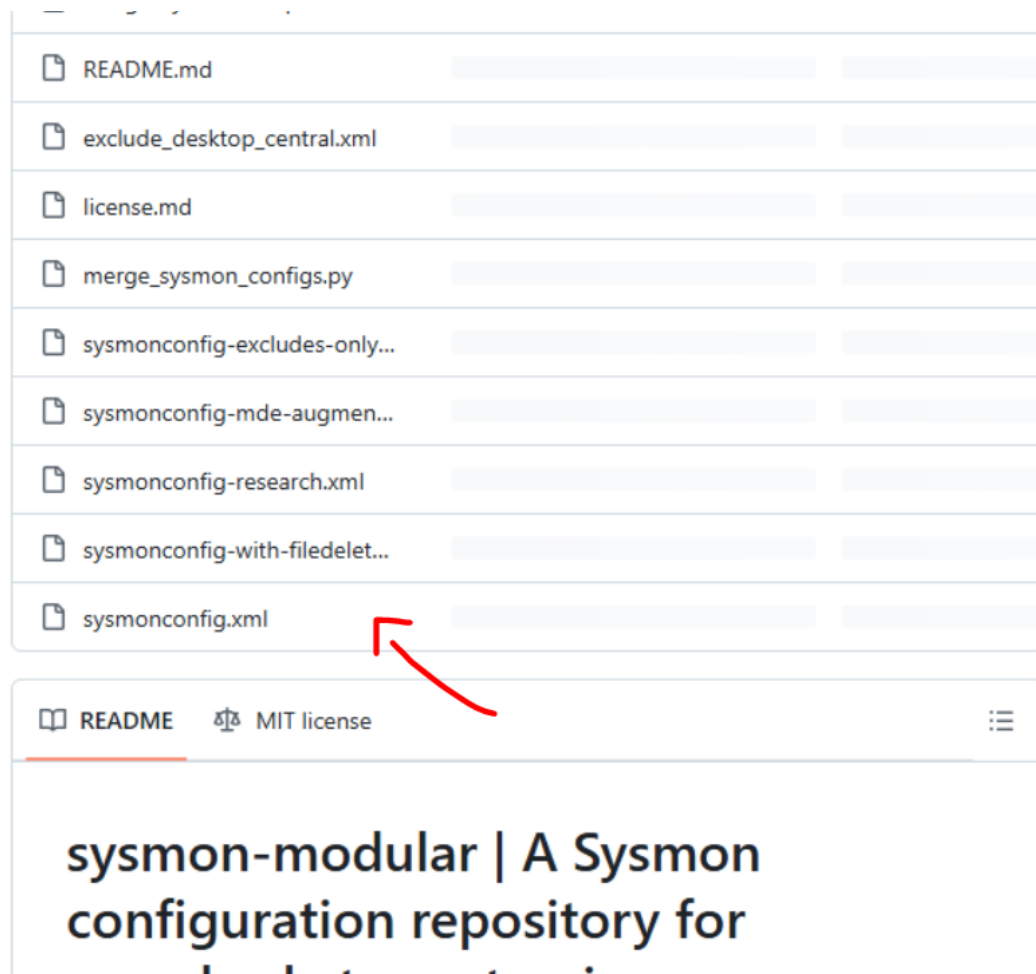


[Download Sysmon](#) (4.6 MB)

[Download Sysmon for Linux \(GitHub\)](#)



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 :



Azure Pipeline Updated after successful CICD run 09/20/202...

a9ff298 · 2 years ago

History

Code

Blame

2704 lines (2704 loc) · 247 KB

Raw

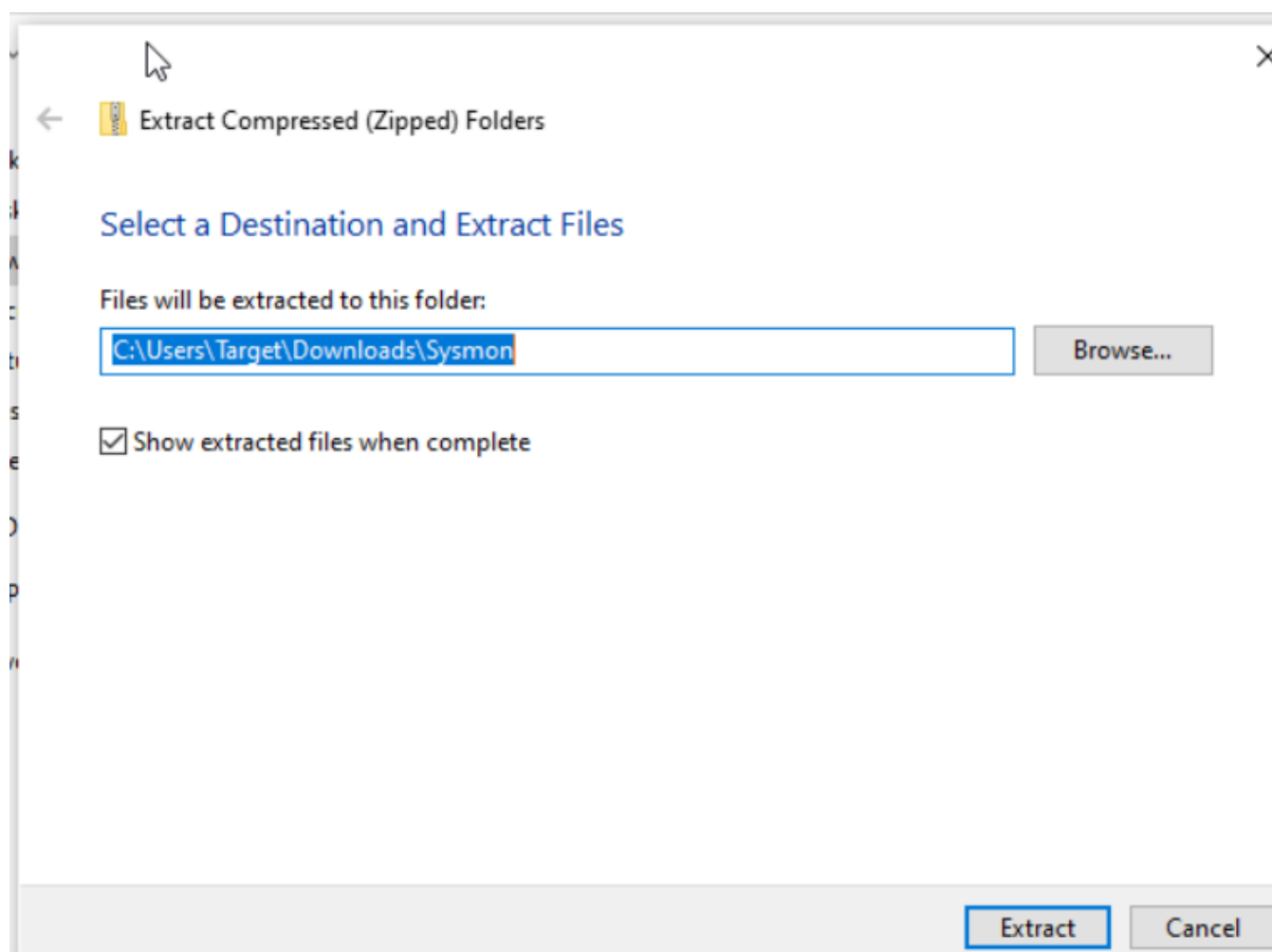


```
1      <!--      NOTICE : This is a balanced generated output of Sysmon-mo
2      <!--      due to the balanced nature of this configuration there w
3      <!--      for more information go to https://github.com/olafharton
4      <!--
5      <!--  /**      ****/
6      <!--  ///#(**      **%(///
7      <!--  ((&&&**      **&&&((
8      <!--  (&&&**      ,(((((((.  **&&&((
9      <!--  ((&&**((((//(((((((//**&&((
10     <!--  (&&///((((//(((((((//&&((
11     <!--  &///((((//(((((((//&
12     <!--  ((//  ///((//  /(((
13     <!--  &((((#.////  /  #((((&
14     <!--  &&&&((#.////  /  #((((&&&&
```

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

```
--      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
--
--  /**      ****/
--  ///#(**      **%(///
--  ((&&&**      **&&&((
--  (&&&**      ,(((((((.  **&&&((
--  ((&&**((((//(((((((//**&&((
--  (&&///((((//(((((((//&&((
--  &///((((//(((((((//&
--  ((//  ///((//  /(((
--  &((((#.////  /  #((((&
--  &&&&((#.////  /  #((((&&&&
--  &&&&****//&&&&
--  (&      ,&.
--  .*&&.
--
sysmon schemaversion="4.90">
<HashAlgorithms>*</HashAlgorithms>
<!-- This now also determines the file names of the files preserved (Stri
<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
<EventFiltering>
<!-- Event ID 1 == Process Creation - Includes -->
<RuleGroup groupRelation="or">
<ProcessCreate onmatch="include">
<ParentImage name="technique_id=T1546.008,technique_name=Accessibil
<ParentImage name="technique_id=T1546.008,technique_name=Accessibil
<ParentImage name="technique_id=T1546.008,technique_name=Accessibil
<ParentImage name="technique_id=T1546.008,technique_name=Accessibil
<ParentImage name="technique_id=T1546.008,technique_name=Accessibil
condition="image">DisplaySwitch.exe</ParentImage>
<ParentImage name="technique_id=T1546.008,technique_name=Accessibil
<ParentImage name="technique_id=T1546.008,technique_name=Accessibil
<OriginalFileName condition="contains">\\</OriginalFileName>
<OriginalFileName name="technique_id=T1546.011,technique_name=App
<OriginalFileName name="technique_id=T1546.011,technique_name=App
```

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

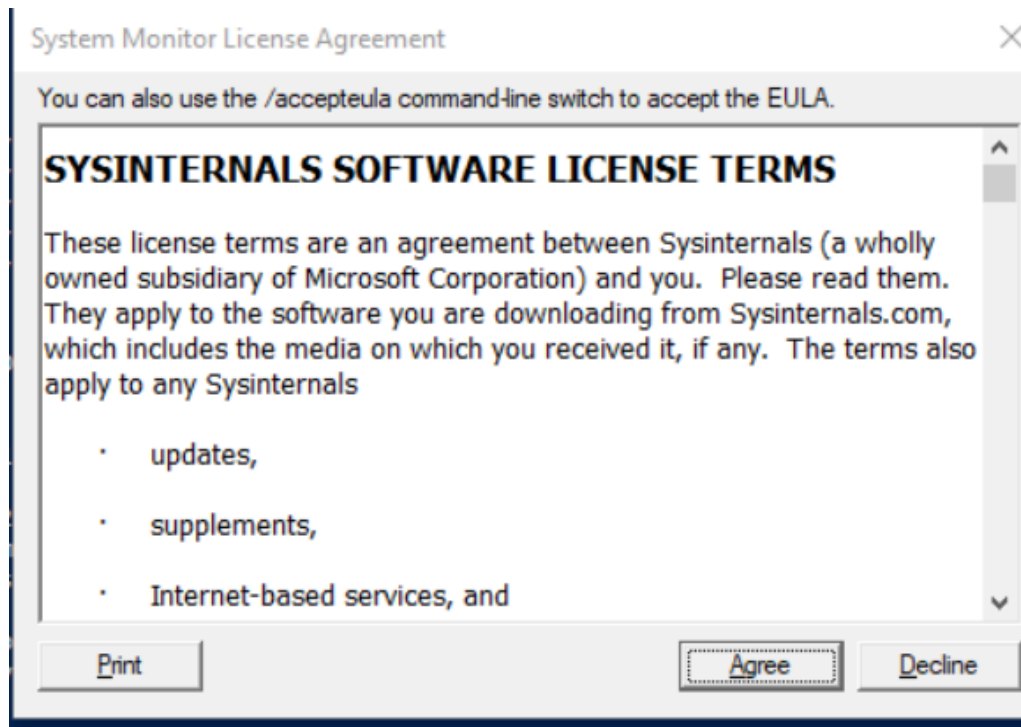
Mode                LastWriteTime         Length Name
----                -
-a----           1/22/2025  12:48 PM             7490 Eula.txt
-a----           1/22/2025  12:48 PM        8480560 Sysmon.exe
-a----           1/22/2025  12:48 PM        4563248 Sysmon64.exe
-a----           1/22/2025  12:48 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

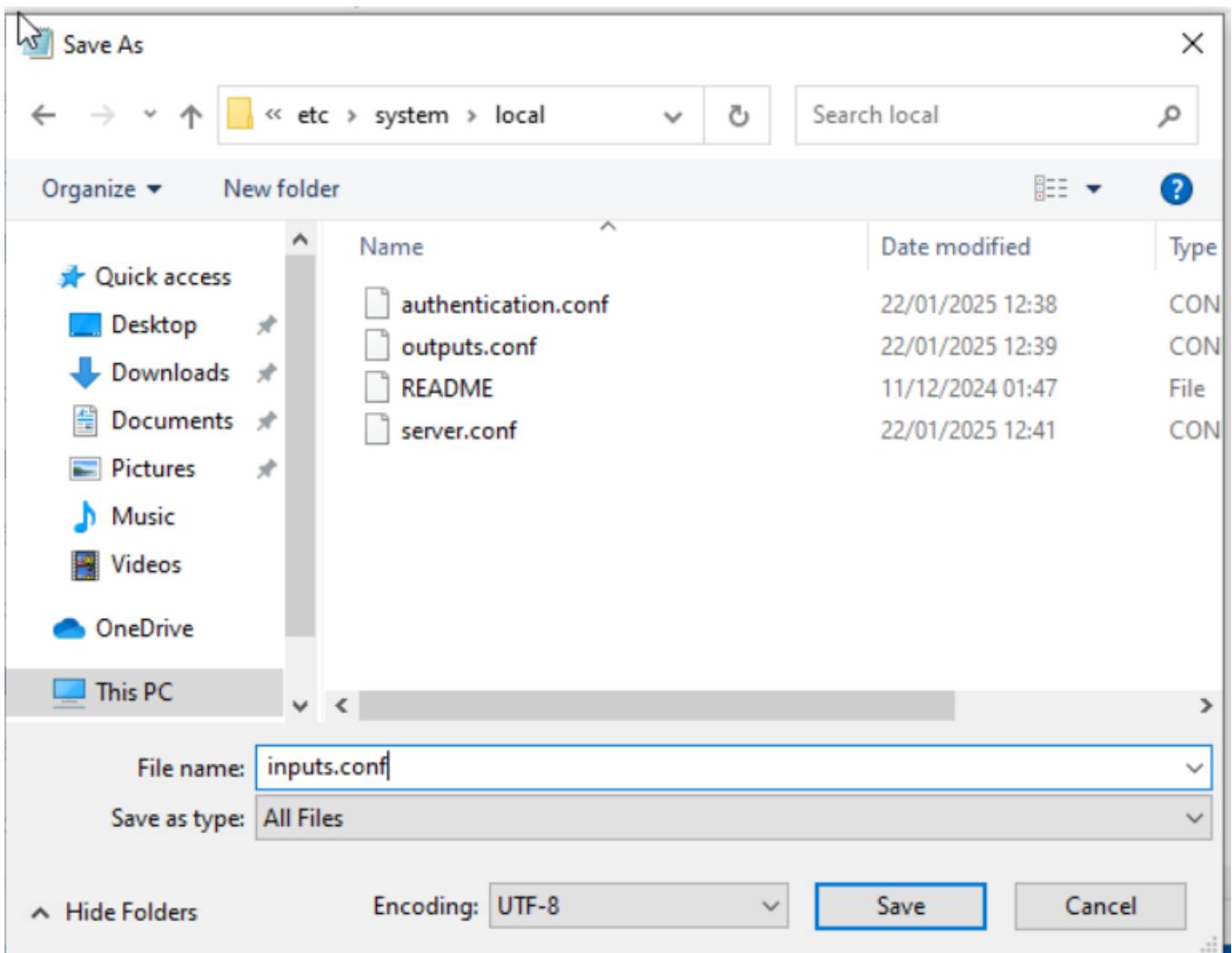
disabled = false

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

index = endpoint

disabled = false
```

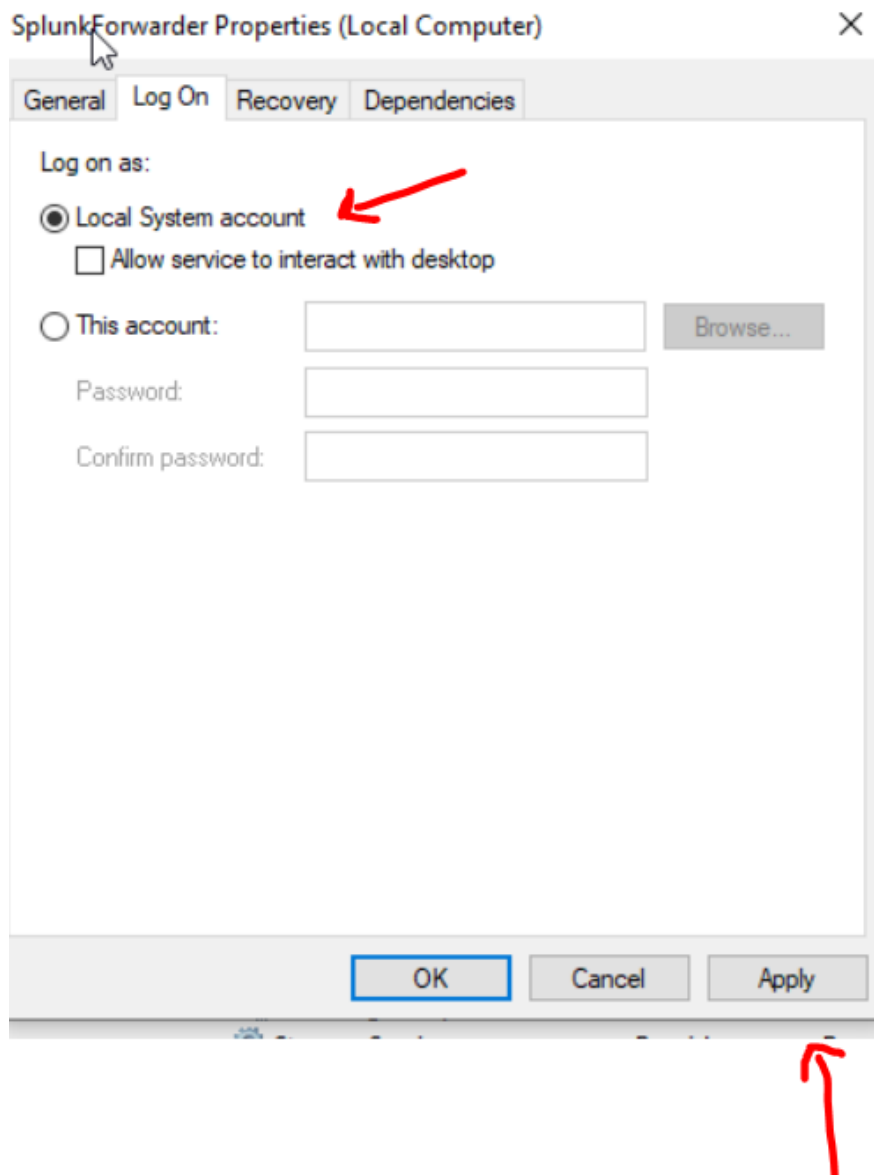
Above the index = endpoint is important because that is where in our splunk server instance we will use to pull logs being forwarded from our target machine to it. Save the file as inputs.conf and paste in the local directory . So at the end it should look like this :



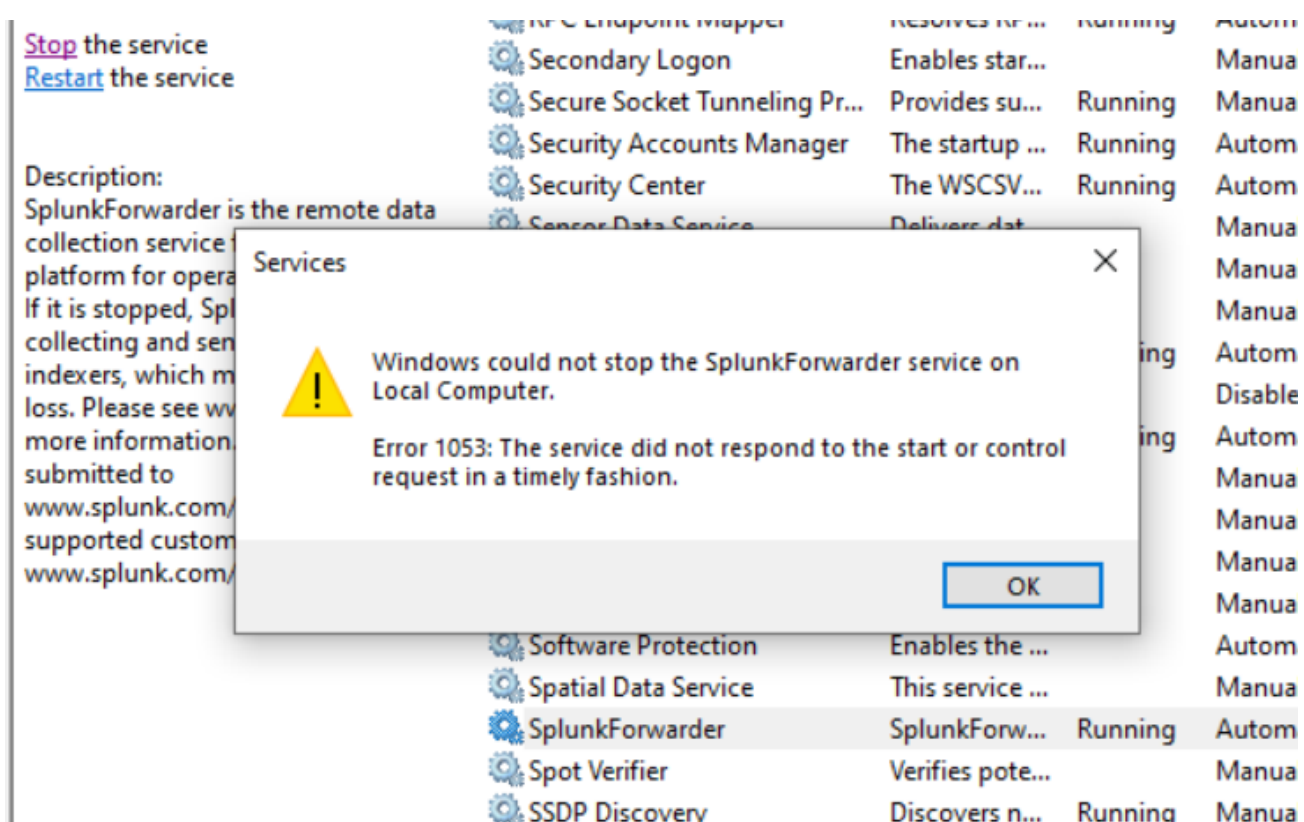
After saving we need to restart the Splunk forwarder service . To do this search for "services" in the windows search box and run it as Administrator . When in it , hit S and look for the Splunk Forwarder service :

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

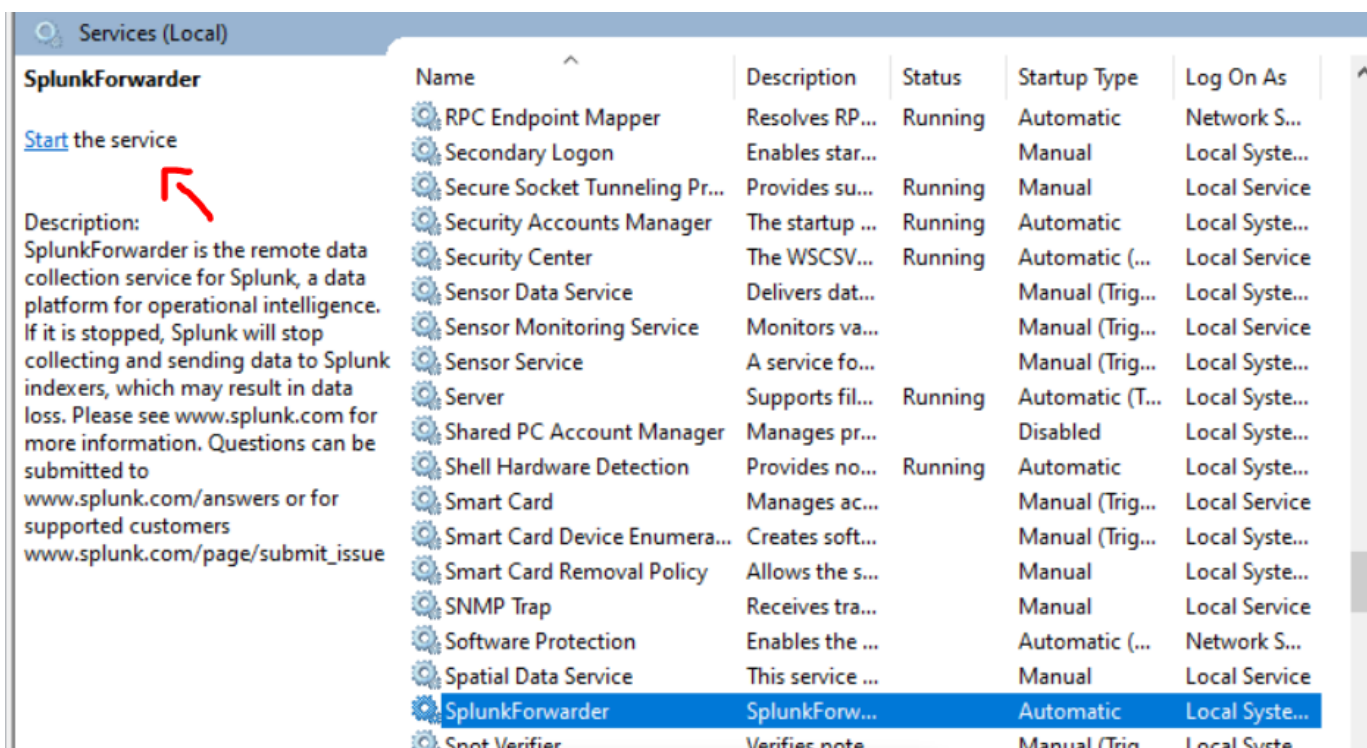
Next we need to change the Logon as type to Local system . To do that double-click on the SplunkForwarder service and navigate to the Logon tab, select Local System account and hit apply :



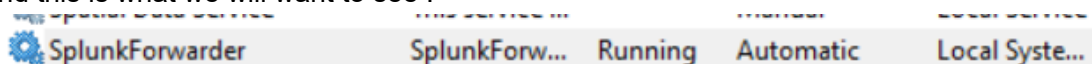
Now we just need to stop the service which will show this :



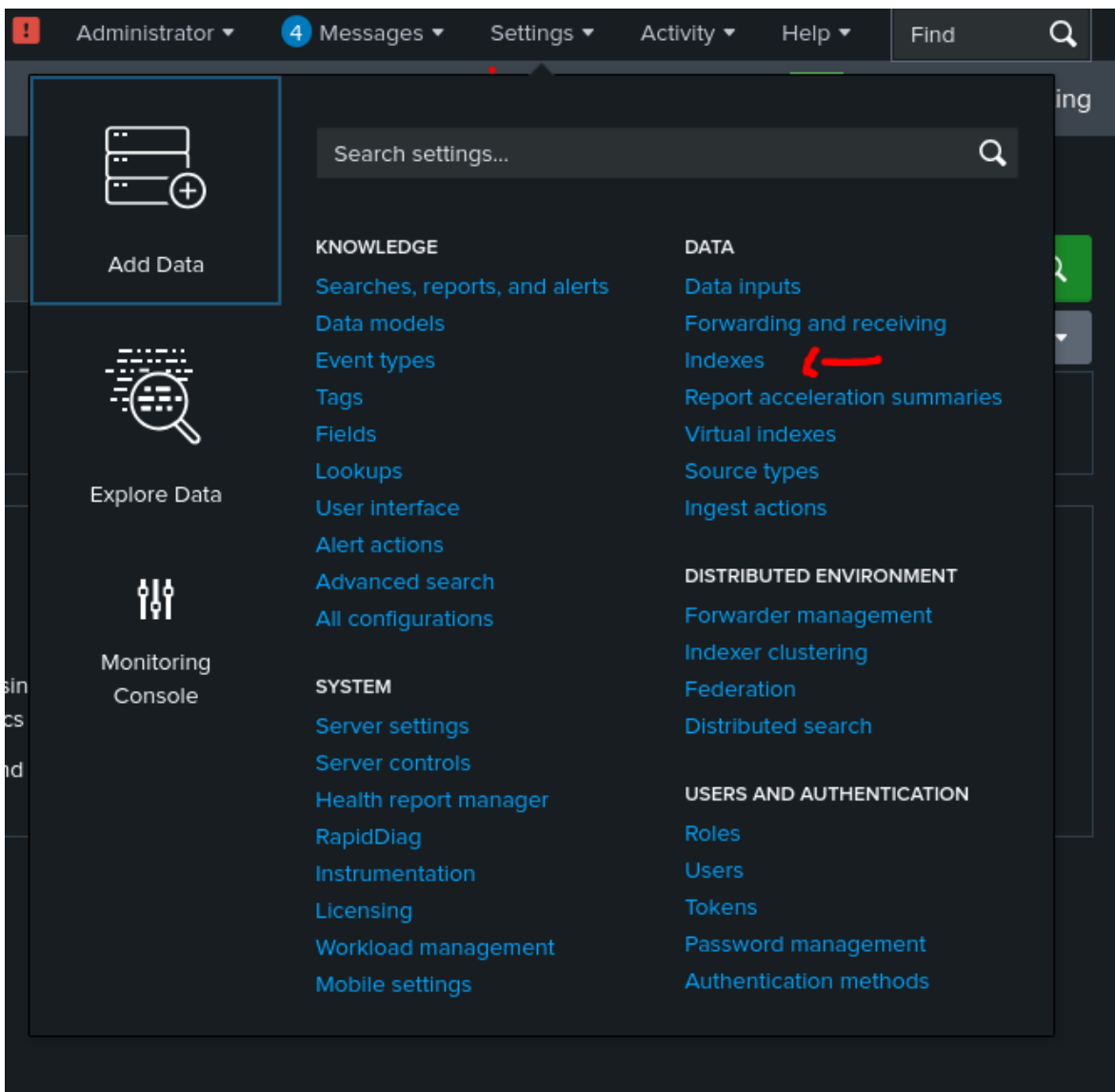
Click on OK and still at your top left you can now click on Start :



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) :

The image shows the Splunk Indexes page. A red arrow points to the 'New Index' button in the top right corner. Below the button is a table listing 15 indexes.

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/_internal/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
theftshbucket	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/_theftshbucket/db	N/A	Enabled
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/_history/db	N/A	Enabled
main	Edit Delete Disable	Events	system	1 MB	488.28 GB	2K	a month ago	a month ago	\$SPLUNK_DB/_default/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/_summary/db	N/A	Enabled

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

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

Maximum target size of entire index.

Max Size of Hot/Warm/
Cold Bucket

auto

GB

Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path

optional

Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

Save

Cancel

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:

Forwarding and receiving

Forward data

Set up forwarding between two or more Splunk instances.

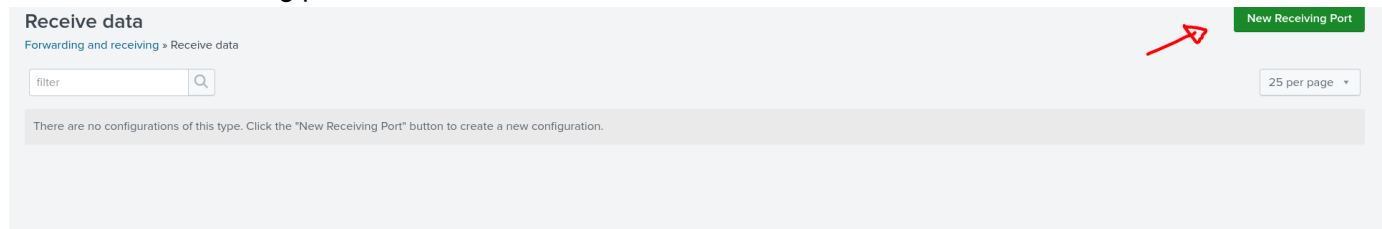
Type	Actions
Forwarding defaults	
Configure forwarding	+ Add new

Receive data

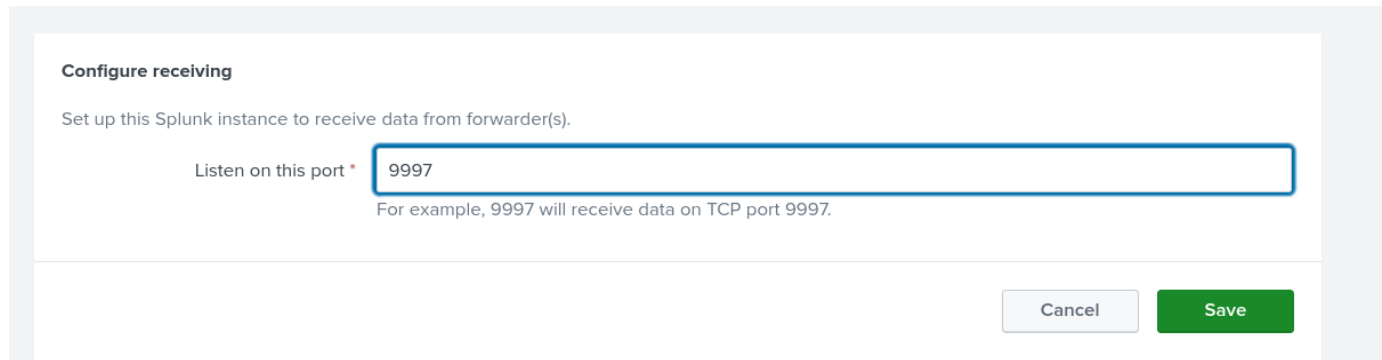
Configure this instance to receive data forwarded from other instances.

Type	Actions
Configure receiving	+ Add new

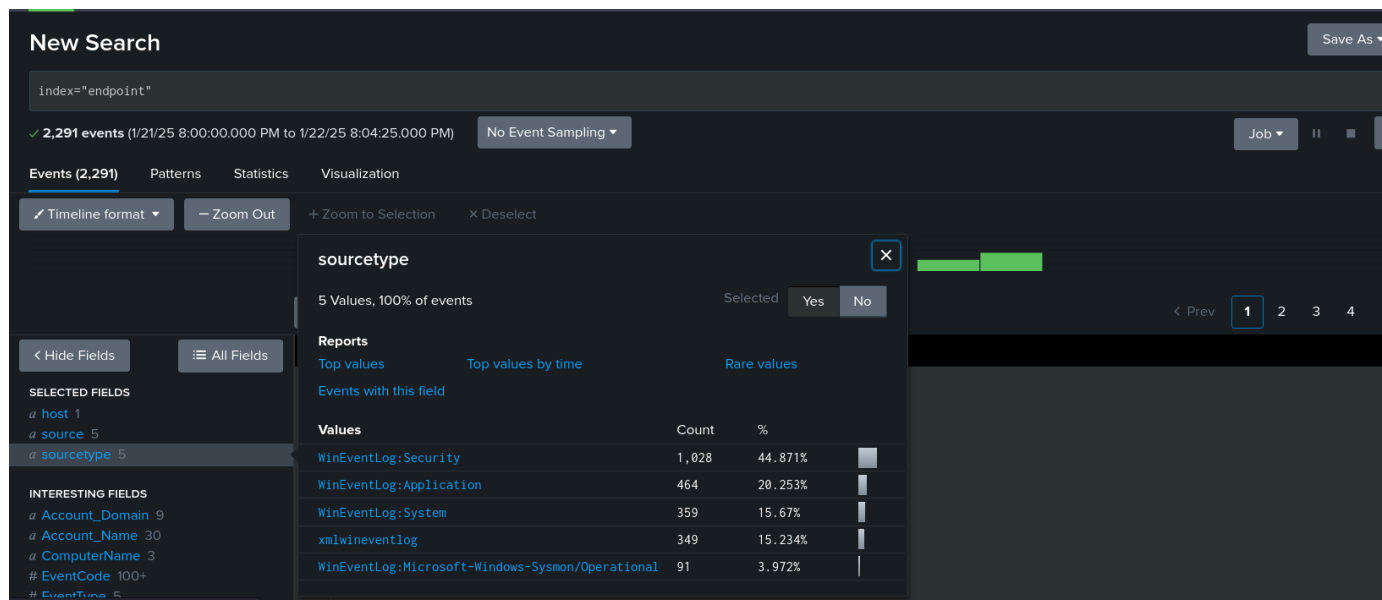
Click on New receiving port :



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.