Splunk Lab Setup Guide

Introduction

This guide provides a detailed walkthrough for setting up a Splunk Lab to facilitate centralized log monitoring and management. By leveraging Splunk Enterprise and the Splunk Universal Forwarder, this lab establishes a robust framework for real-time log analysis and security monitoring. The setup incorporates a virtualized environment with Ubuntu serving as the Splunk server and Windows hosting as a log-generating web server.

Objectives

1. **Setup Virtualized Environment:**
    a. Install VirtualBox
    b. Deploy Ubuntu virtual machine
2. **Install and Configure Splunk Components:**
    a. Set up Splunk Enterprise on the Ubuntu server
    b. Install Splunk Universal Forwarder on the Windows IIS Server
3. **Integrate Log Sources:**
    a. Configure Sysmon for advanced system activity monitoring
    b. Set up IIS logging for web server activity
    c. Set up Apache logging
4. **Enable Data Forwarding:**
    a. Configure Splunk Universal Forwarder to send logs to the Splunk server
    b. Establish indexes for Sysmon, IIS, Apache and other logs
5. **Optimize Monitoring Setup:**
    a. Install Splunk add-ons for IIS, Sysmon, and Apache
6. **Understand Basic Splunk Queries:**
    a. Explore different commands for log analysis

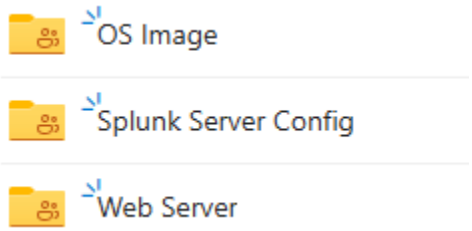
Table of Contents

Contents

Files for Setup

Before we begin, you have two options for obtaining the necessary files for the Splunk Lab setup. You can either use the provided link below, which contains all the required files, or follow the step-by-step instructions in this guide, where download links for each individual file will be provided.

https://1drv.ms/f/c/845eca32a3496e6b/EpWxgyRVVC1BnLe0TbgY5qwB2UdF-L9TqPgkFRTtBAt_6A?e=adnSEQ



The link contains the necessary files for setting up the Splunk Lab, organized into three folders. These files will be used at various stages of the setup process. Below is a description of what each folder contains:

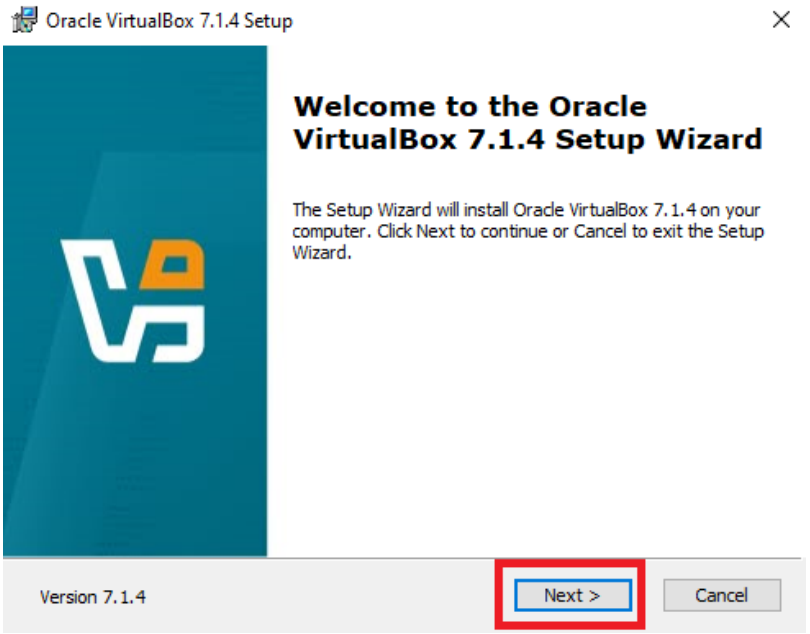
- **OS image:**
  - Contains the Ubuntu 24.04 OS file required for this setup.
- **Splunk Server Config:**
  - Includes the configuration files for Splunk Enterprise and the required apps for this lab.
- **Web Server:**
  - Contains the Splunk Universal Forwarder and Sysmon files for monitoring purposes.

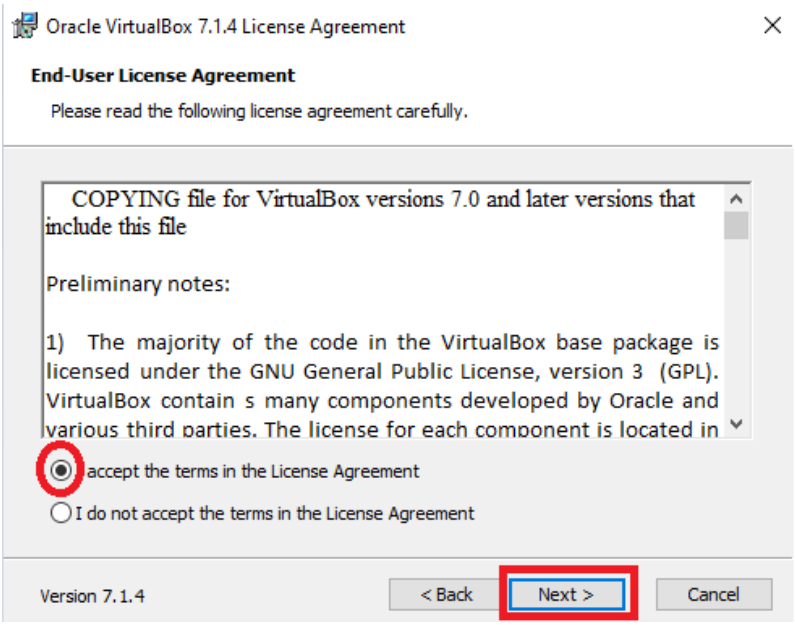
VirtualBox Installation

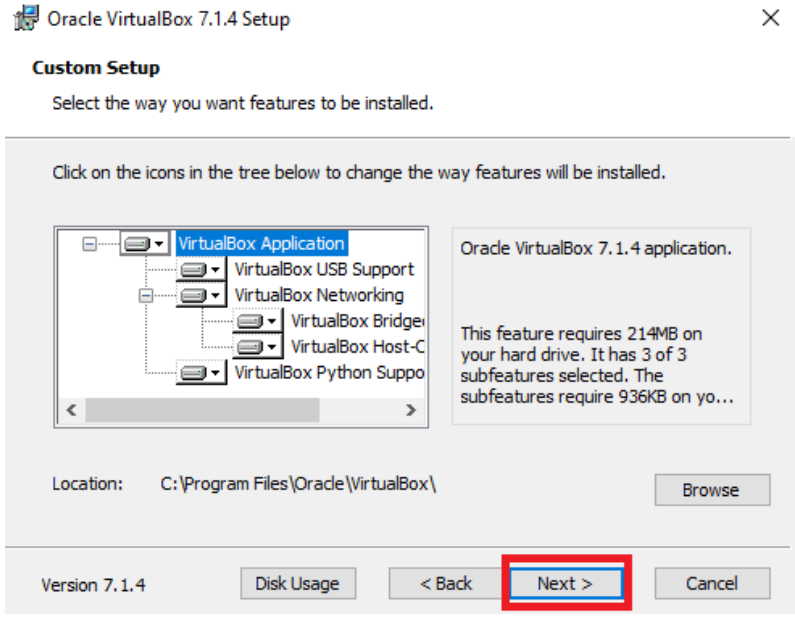
Firstly, we will be downloading VirtualBox, a virtualization software that allows us to run virtual machines on our computers.

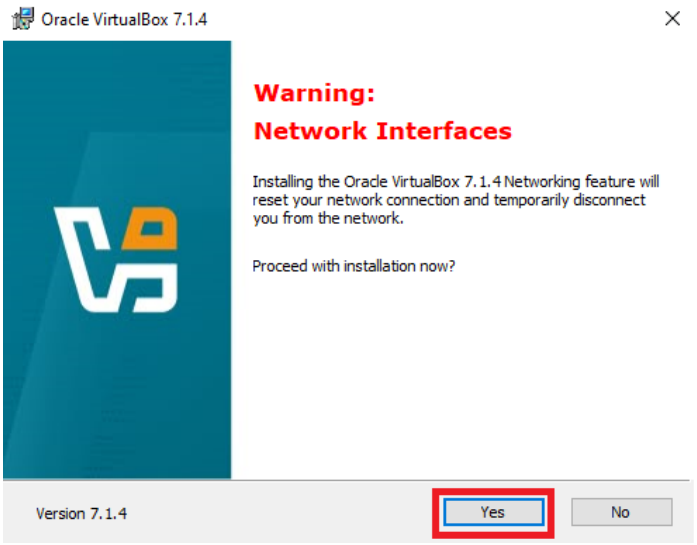
We can download VirtualBox for Windows hosts from the following link: https://www.virtualbox.org/wiki/Downloads

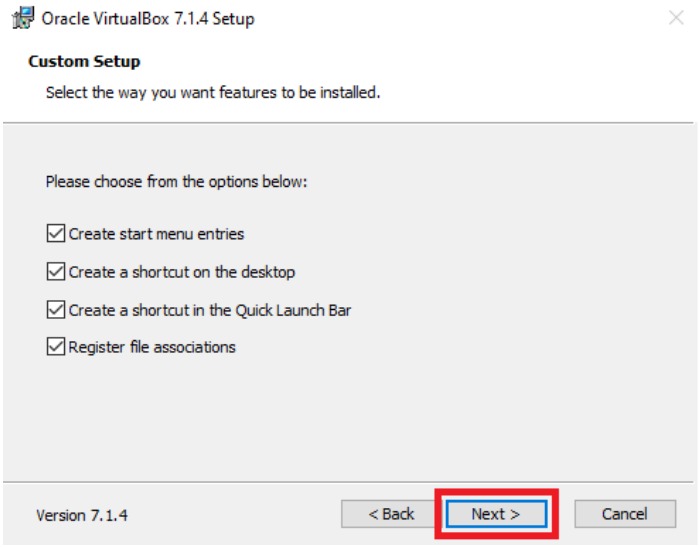
Once the file finishes downloading, run it.

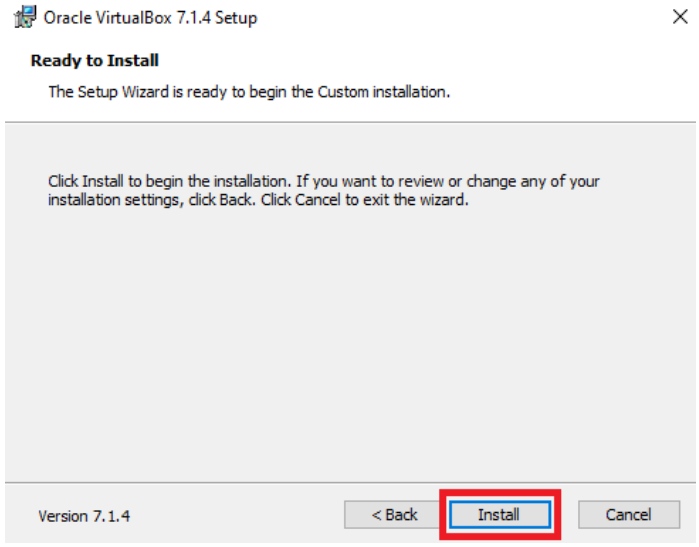



Oracle VirtualBox 7.1.4 License Agreement
End-User License Agreement
Please read the following license agreement carefully.
COPYING file for VirtualBox versions 7.0 and later versions that include this file
Preliminary notes:
1) The majority of the code in the VirtualBox base package is licensed under the GNU General Public License, version 3 (GPL). VirtualBox contain s many components developed by Oracle and various third parties. The license for each component is located in
I accept the terms in the License Agreement
I do not accept the terms in the License Agreement
Version 7.1.4
< Back
Next >
Cancel


Oracle VirtualBox 7.1.4 Setup
Custom Setup
Select the way you want features to be installed.
Click on the icons in the tree below to change the way features will be installed.
VirtualBox Application
VirtualBox USB Support
VirtualBox Networking
VirtualBox Bridge
VirtualBox Host-C
VirtualBox Python Suppo
Oracle VirtualBox 7.1.4 application.
This feature requires 214MB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 936KB on yo...
Location: C:\Program Files\Oracle\VirtualBox\
Browse
Version 7.1.4
Disk Usage
< Back
Next >
Cancel


Oracle VirtualBox 7.1.4
Warning:
Network Interfaces
Installing the Oracle VirtualBox 7.1.4 Networking feature will reset your network connection and temporarily disconnect you from the network.
Proceed with installation now?
Version 7.1.4
Yes
No


Oracle VirtualBox 7.1.4 Setup
Custom Setup
Select the way you want features to be installed.
Please choose from the options below:
Create start menu entries
Create a shortcut on the desktop
Create a shortcut in the Quick Launch Bar
Register file associations
Version 7.1.4
< Back
Next >
Cancel


Oracle VirtualBox 7.1.4 Setup
Ready to Install
The Setup Wizard is ready to begin the Custom installation.
Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Version 7.1.4
< Back
Install
Cancel

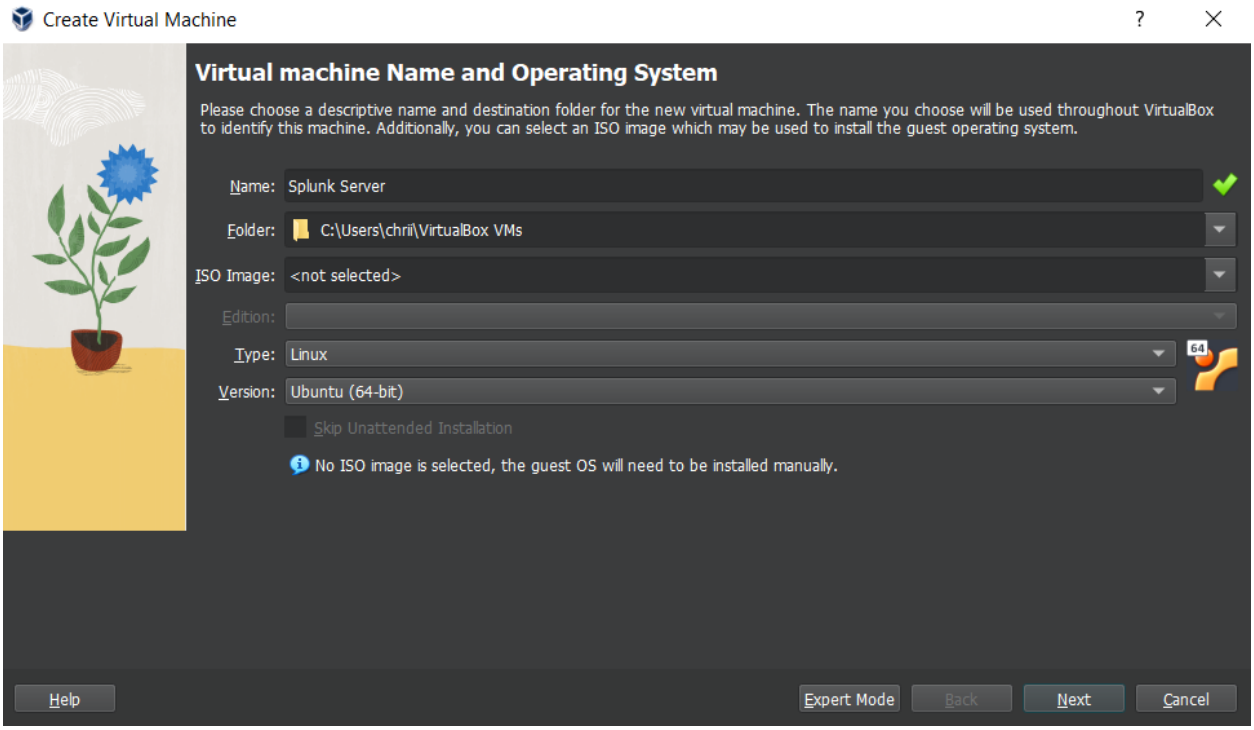
Virtual Machine Setup

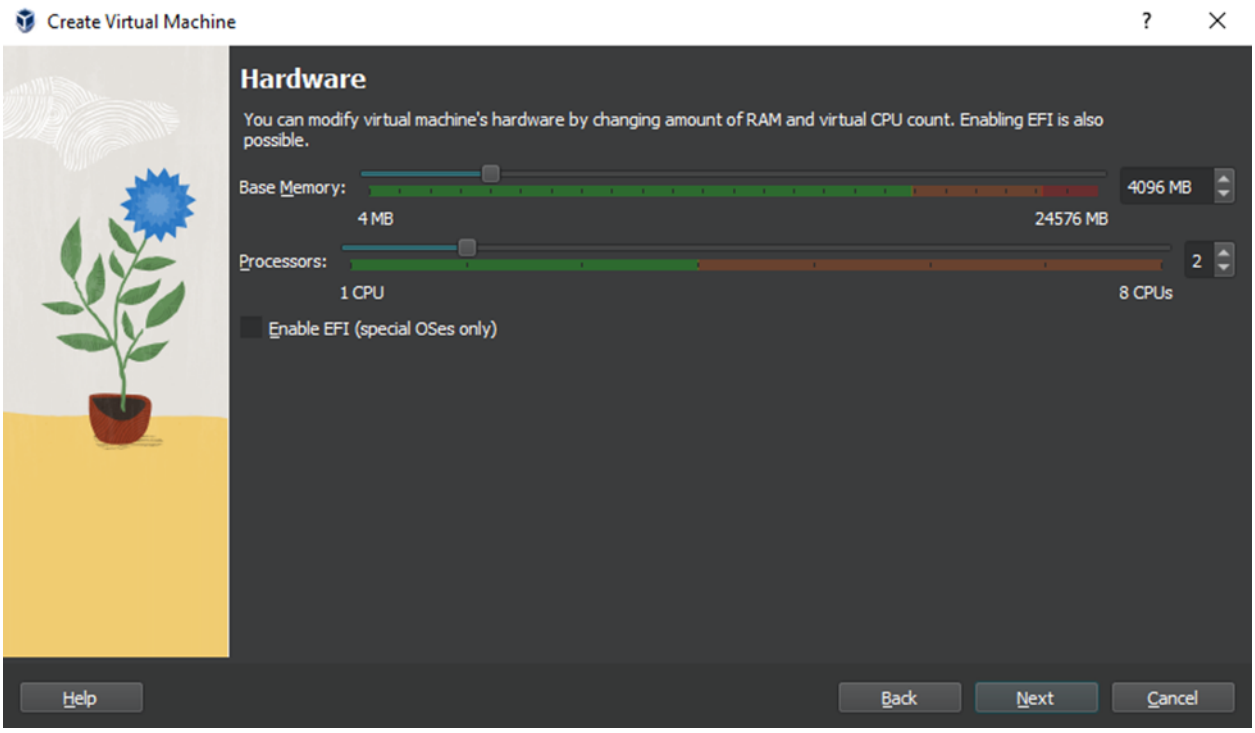
For this lab, we will be using VirtualBox to setup Ubuntu for the Splunk server and Windows for the IIS web server.

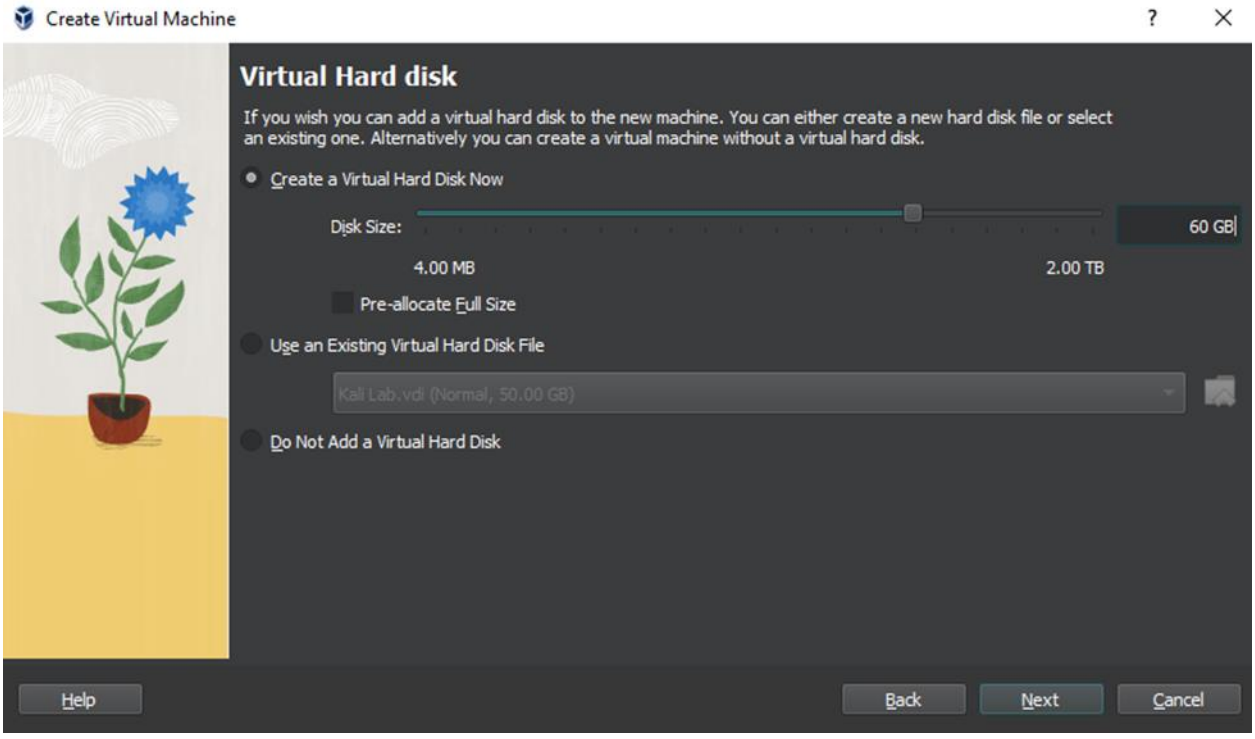
Ubuntu Setup

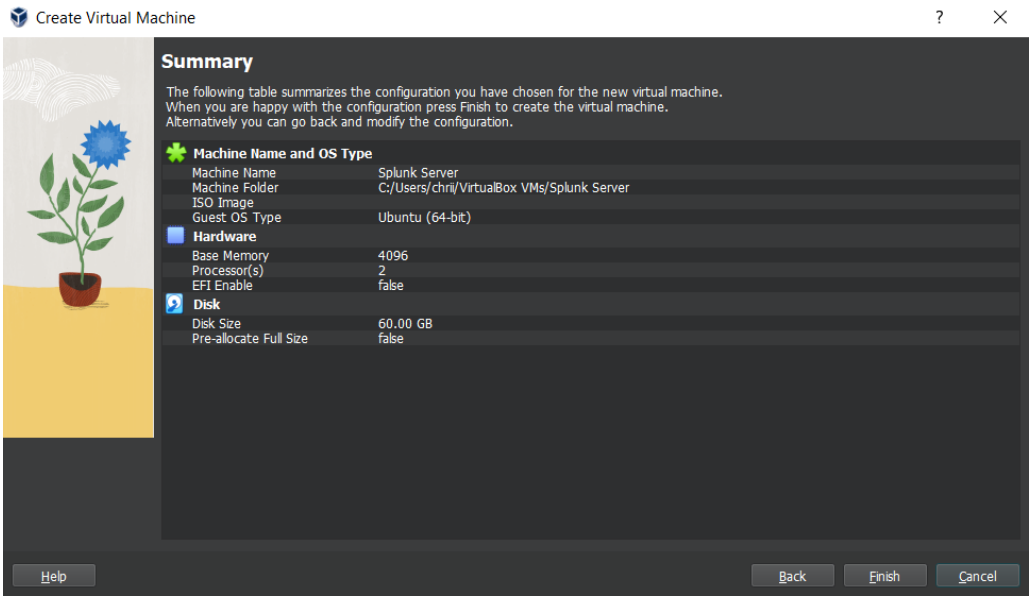
To setup Splunk, we will be using Ubuntu 24.04.1 LTS which can be downloaded with the following link: https://ubuntu.com/download/desktop

Once the ISO image has been installed, create your Ubuntu VM by VirtualBox > Machine > New, and edit based on the provided screenshot below.



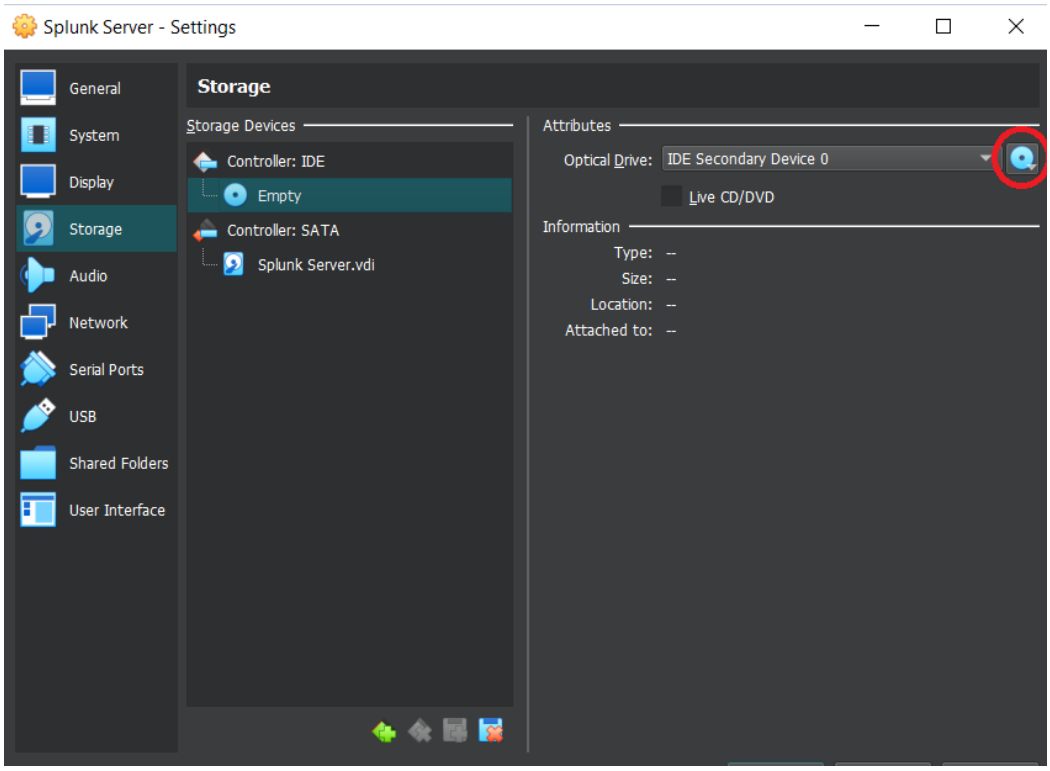

Create Virtual Machine
Hardware
You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.
Base Memory:
4096 MB
4 MB
24576 MB
Processors:
2
1 CPU
8 CPUs
Enable EFI (special OSes only)
Help
Back
Next
Cancel


Create Virtual Machine
Virtual Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.
Create a Virtual Hard Disk Now
Disk Size:
60 GB
4.00 MB
2.00 TB
Pre-allocate Full Size
Use an Existing Virtual Hard Disk File
Kali Lab.vdi (Normal, 50.00 GB)
Do Not Add a Virtual Hard Disk
Help
Back
Next
Cancel



Your summary page should be the same as the picture above.

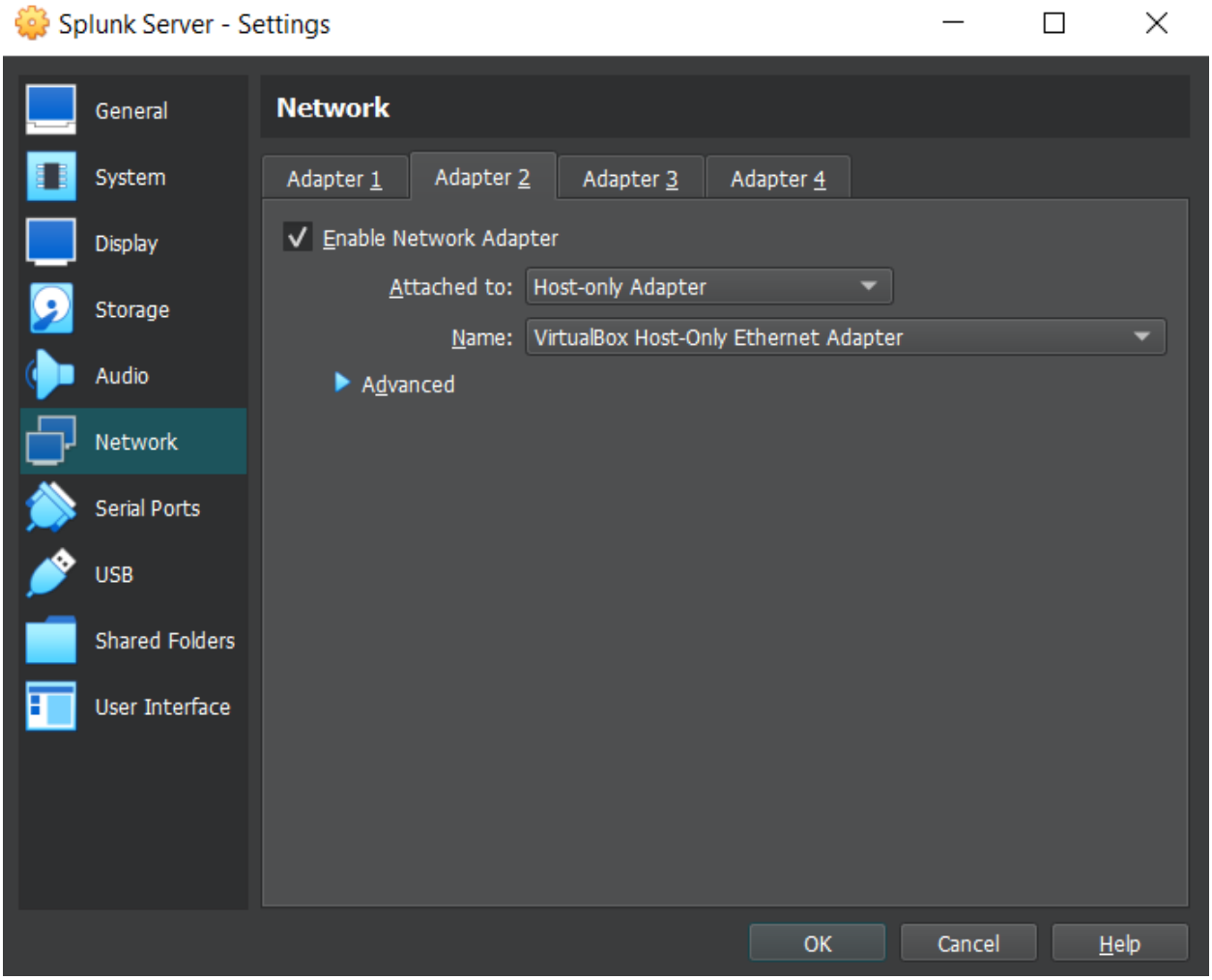
Now we will upload the downloaded Ubuntu ISO file into our VM. Click on the “Splunk Server” VM > Settings > Storage > Empty, and click on the Blue disk on the right > “Choose a disk file…”



Then select the Ubuntu ISO file (ubuntu-24.04.1-desktop-amd64.iso) and click “Ok”

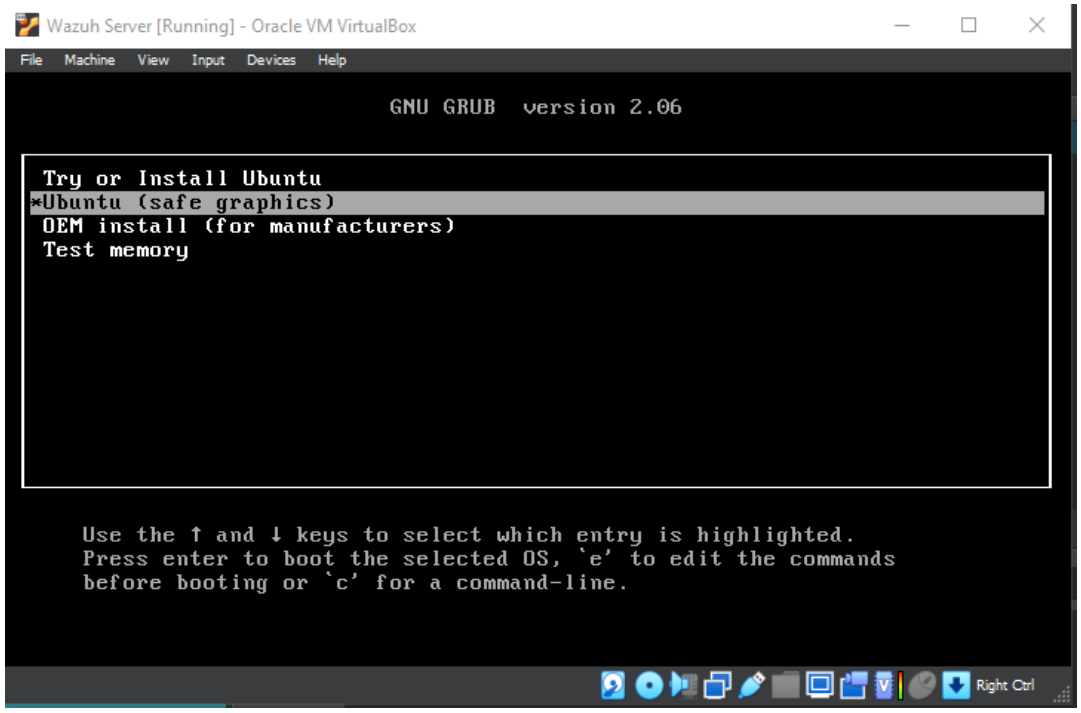
Now, we will have to make a few adjustments for the VM for the setup to run smoothly

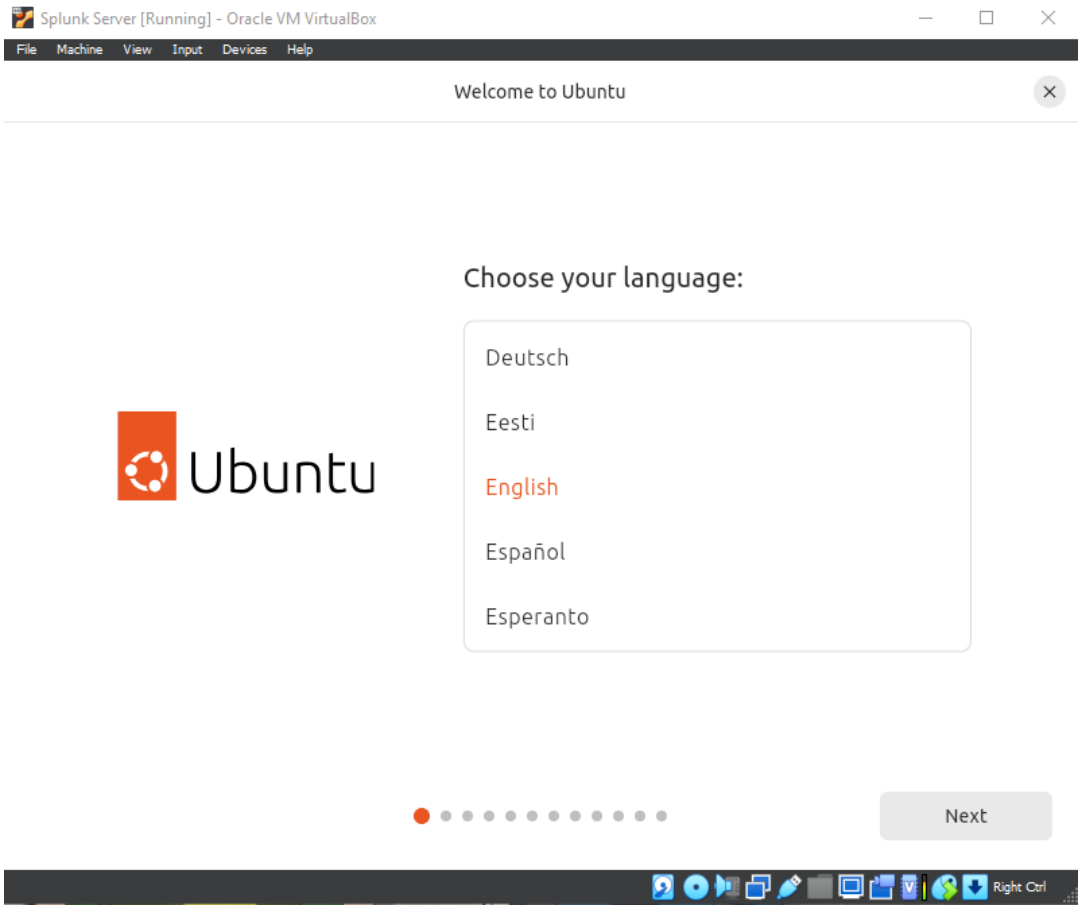
Click on the Splunk Server VM > Settings > Network > Adapter 2, and check “Enable Network Adapter” and change from “Not Attached” to “Host-only Adapter”. This allows our VM to connect to the internet while also providing the VM a unique IP address.



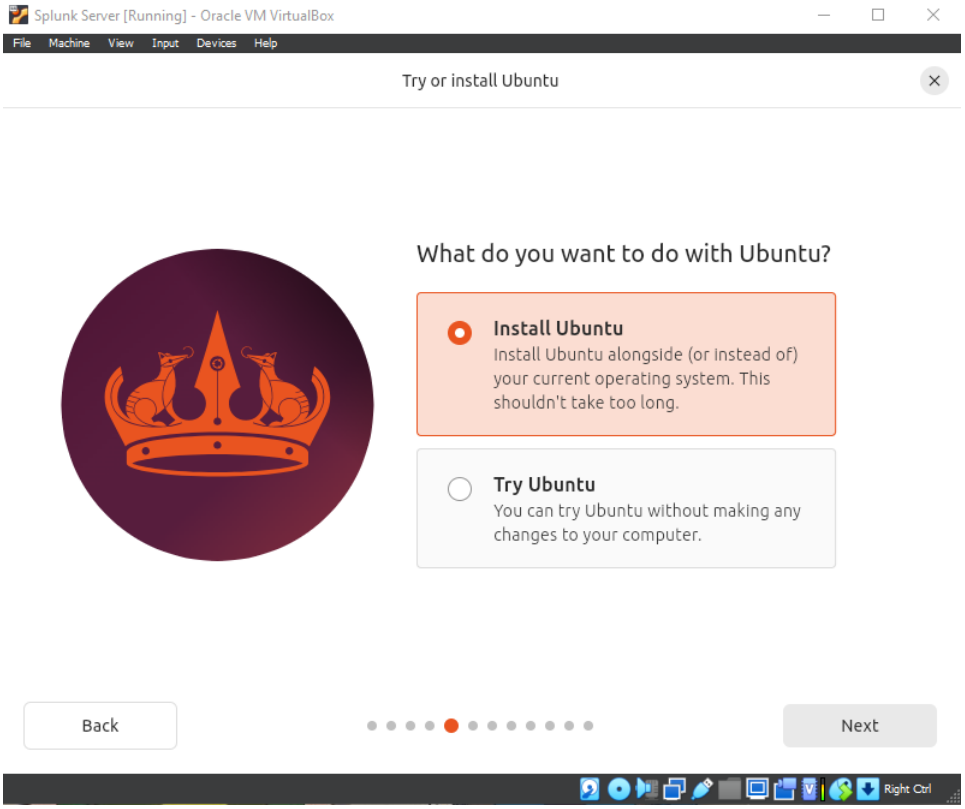
Now, we are ready to start the VM.

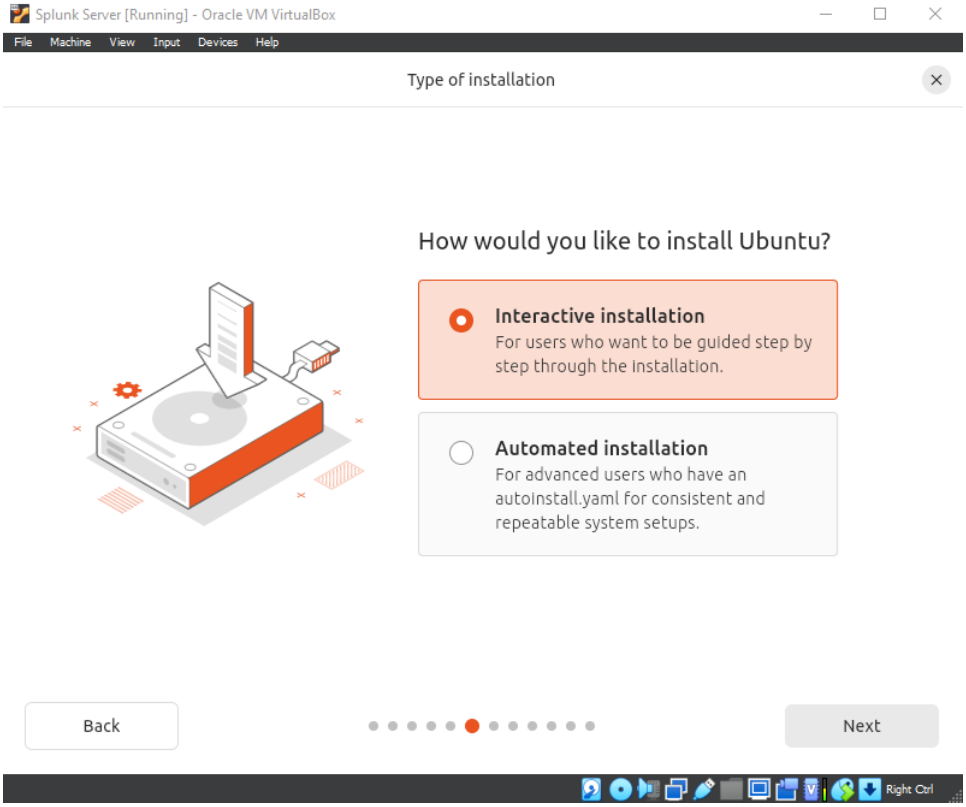
Select Ubuntu (Safe graphics)

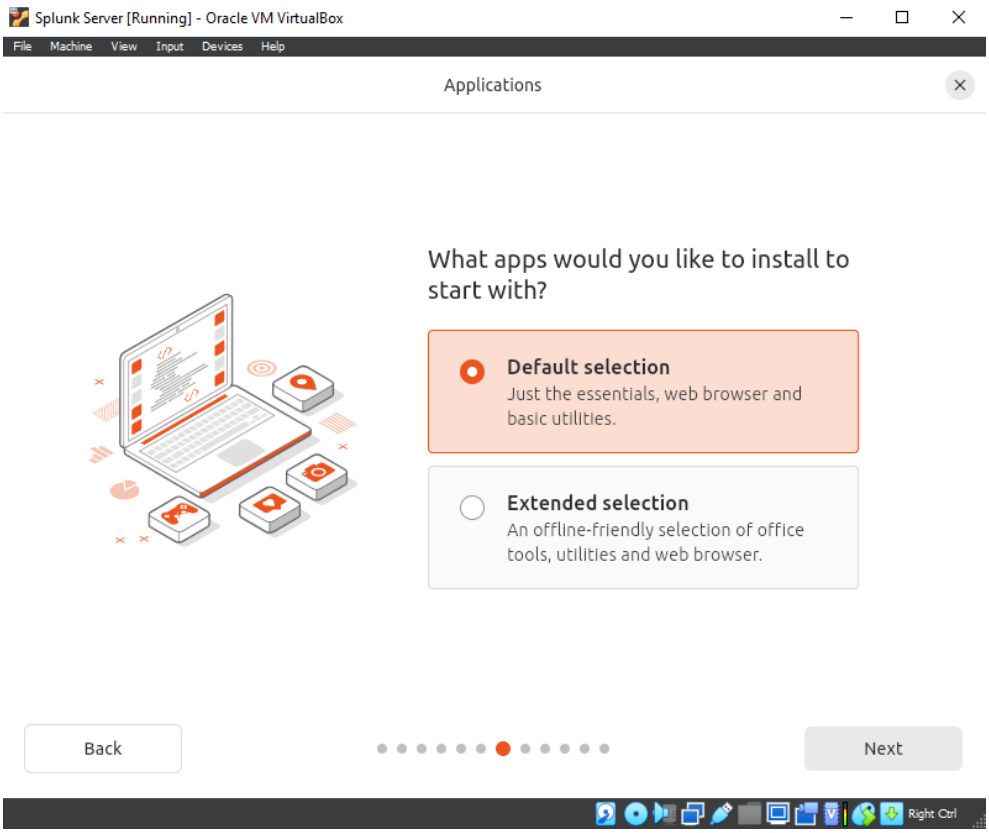




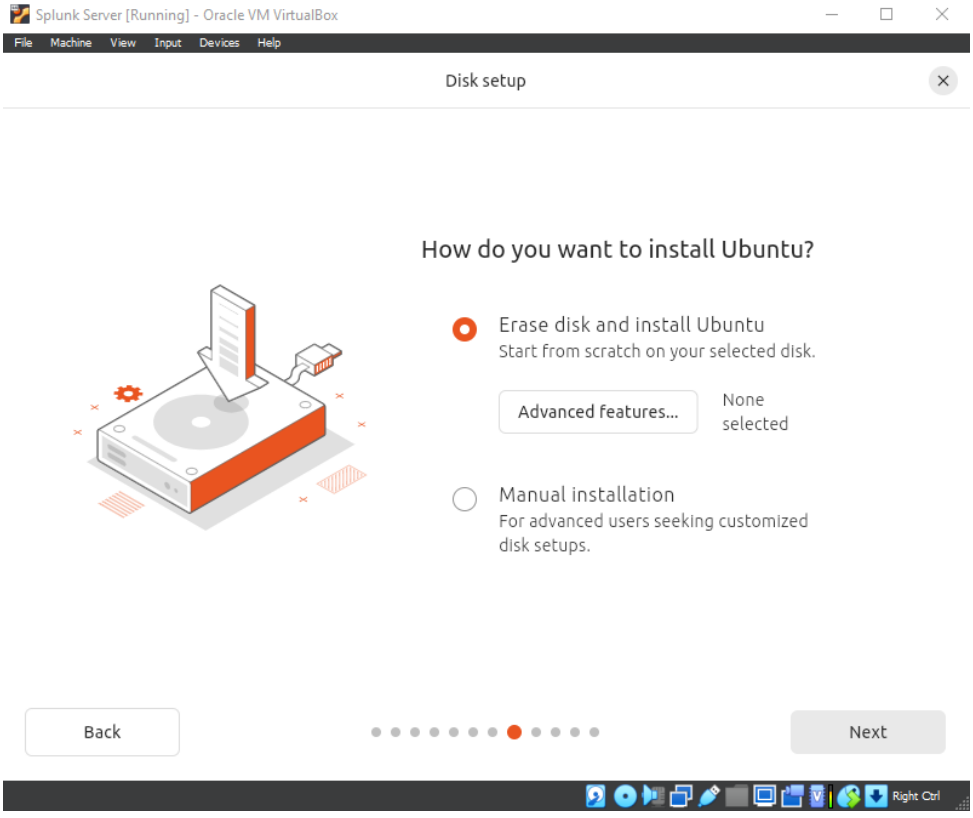
Continue clicking “Next” until you see this page, select “Install Ubuntu” and click Next.



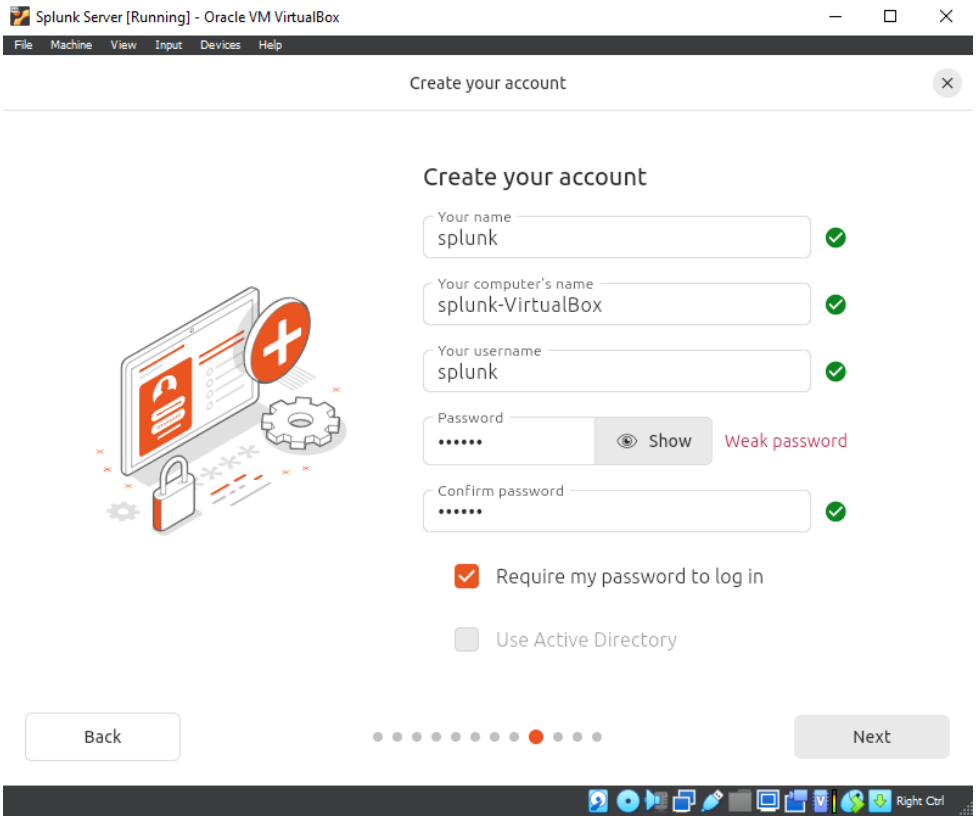


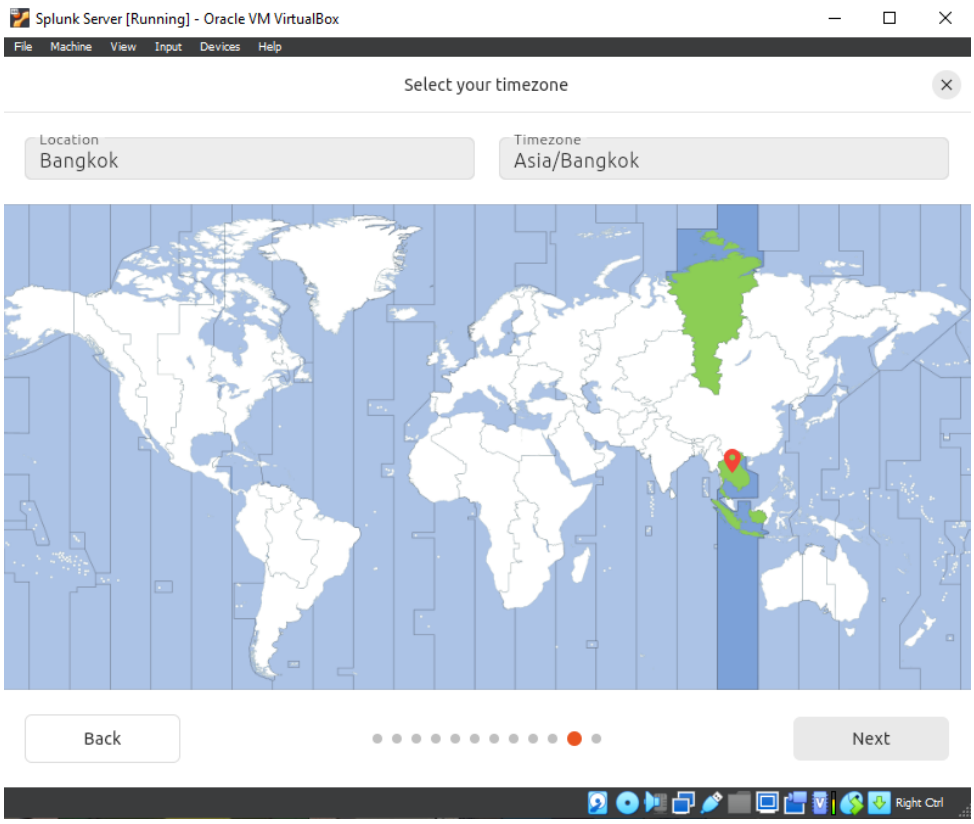


Click Next until you see this page below, and select “Erase disk and install Ubuntu”

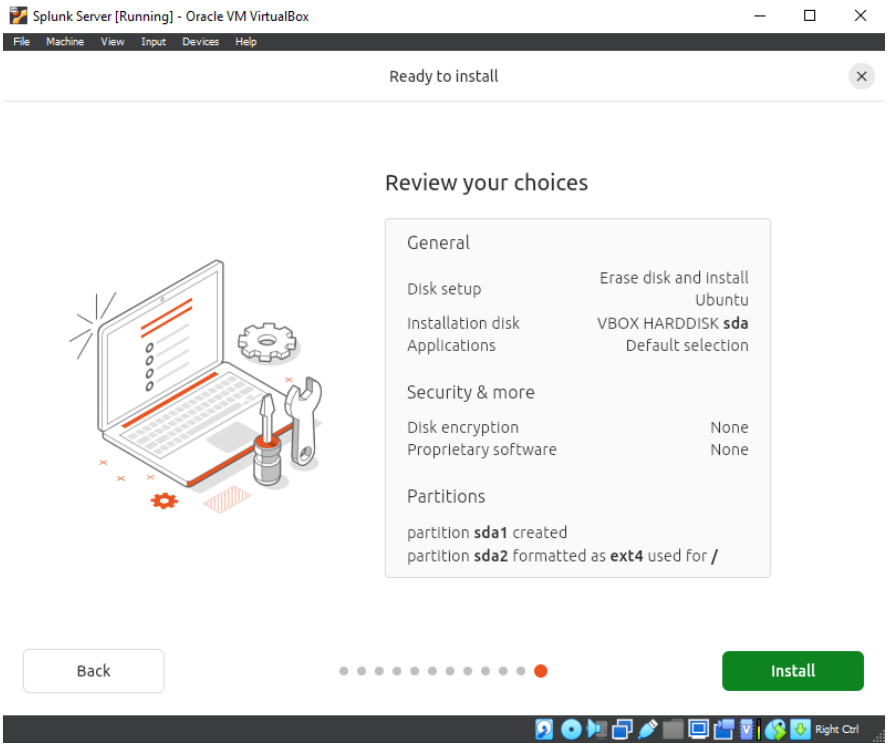


Add in the following, and make sure to pick a password that you can remember.





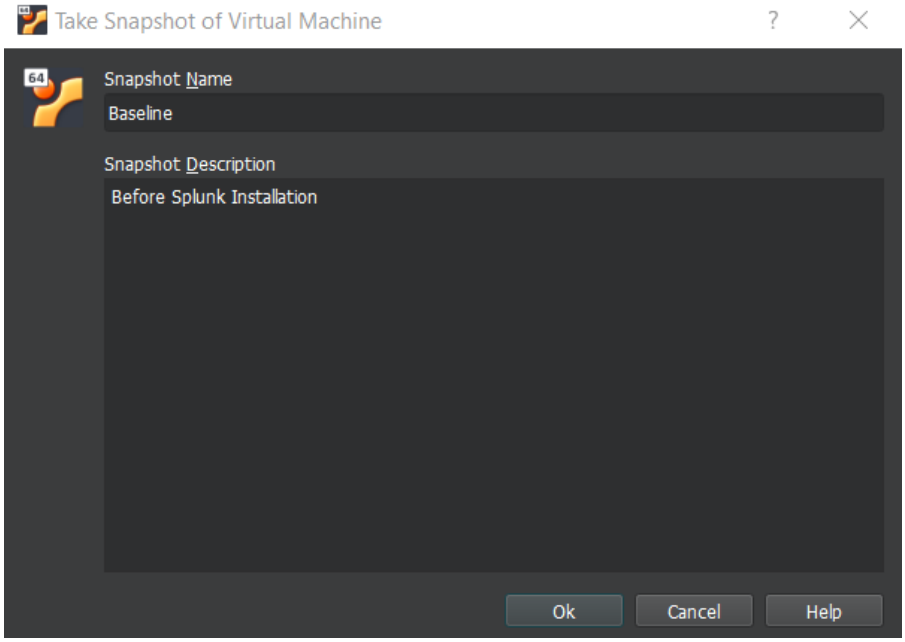
We are now ready to install Ubuntu.



Once the installation is finished, restart the VM.

Now, once we have the VM running, we should take a snapshot of the VM just in case something goes wrong, and we have to go back to the initial setup of Ubuntu.

Machine > Take Snapshot…

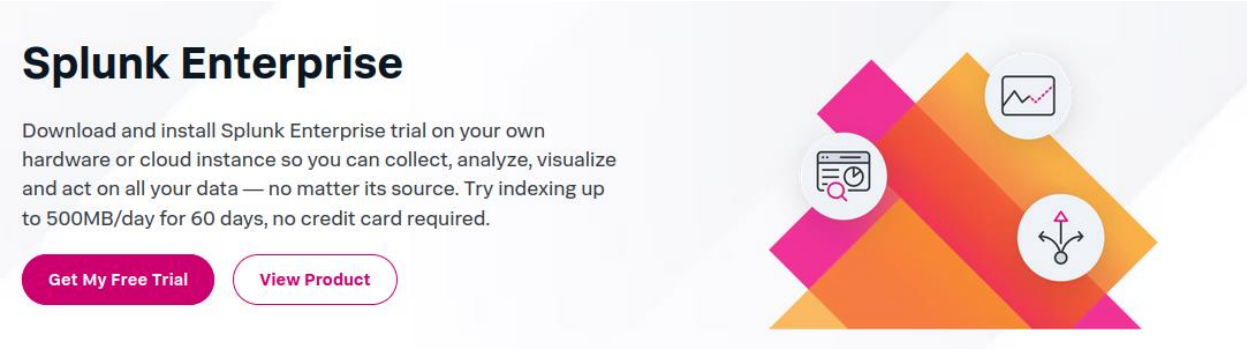


Splunk Server Setup

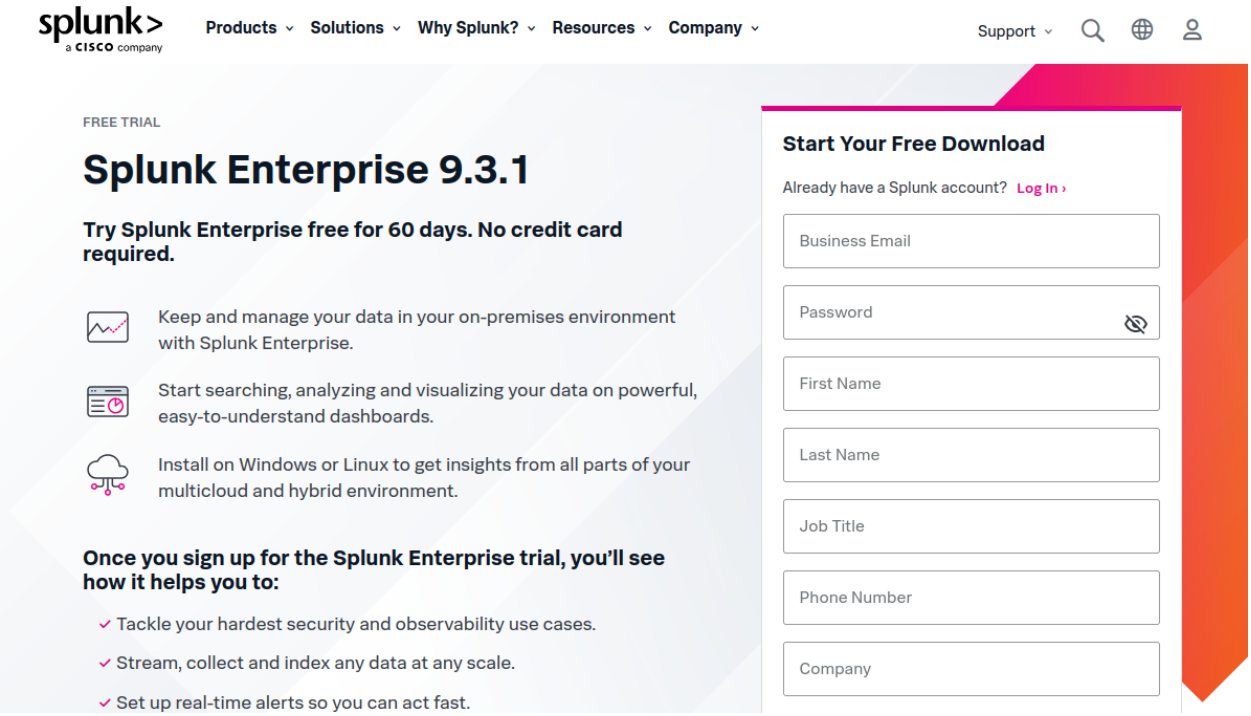
Splunk Installation

We can download Splunk from this link: https://www.splunk.com/en_us/download.html

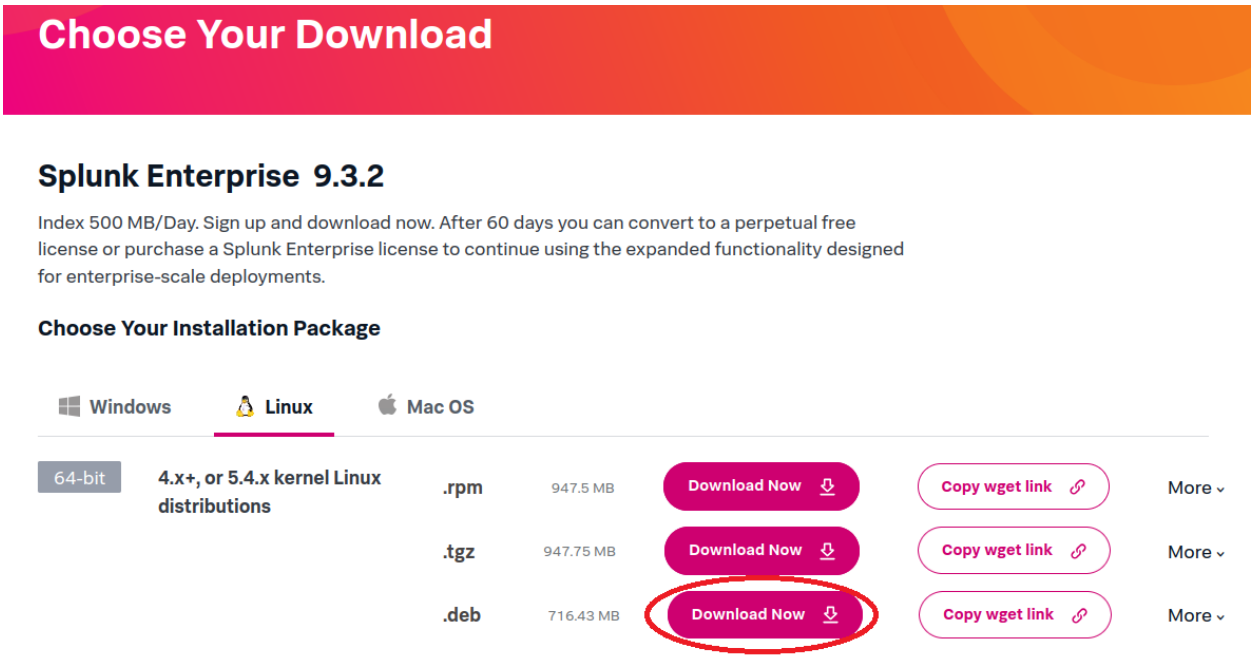
Choose the “Splunk Enterprise” and click on Get My Free Trial



We will be taken to a page where we will have to sign up to download Splunk Enterprise.



Once we sign up, we will be taken to this page. Download the .deb file in the Linux tab



Once the file has been downloaded, run the following commands:

1. sudo apt install curl

```
splunk@splunk-VirtualBox:~$ sudo apt install curl
```

2. cd Downloads/
3. sudo dpkg -i splunk-9.3.2…deb (type in splunk, then press tab)

```
splunk@splunk-VirtualBox:~$ cd Downloads/
splunk@splunk-VirtualBox:~/Downloads$ sudo dpkg -i splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb
```

Once the download is completed, run the command “ls /opt/” and if Splunk shows, that means the download was successful.

```
splunk@splunk-VirtualBox:~/Downloads$ ls /opt/
splunk
```

To run Splunk, run the following commands:

1. cd /opt/splunk/bin/
2. sudo su
3. ./splunk start

```
splunk@splunk-VirtualBox:~/Downloads$ cd /opt/splunk/bin/
splunk@splunk-VirtualBox:/opt/splunk/bin$ sudo su
root@splunk-VirtualBox:/opt/splunk/bin# ./splunk start
```

Keep pressing the space bar until “Do you agree with this license? [y/n]:” shows. Type in “y”

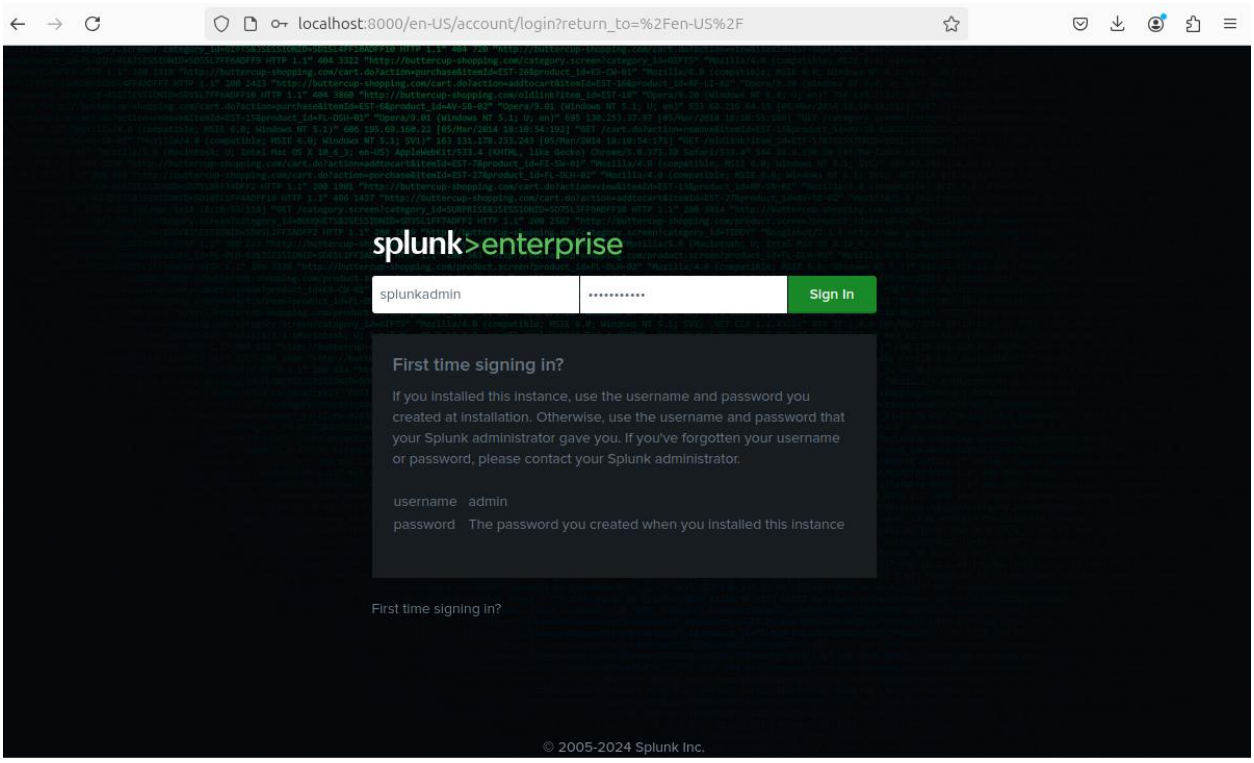
Then, enter the credentials:

```
Please enter an administrator username: splunkadmin
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
```

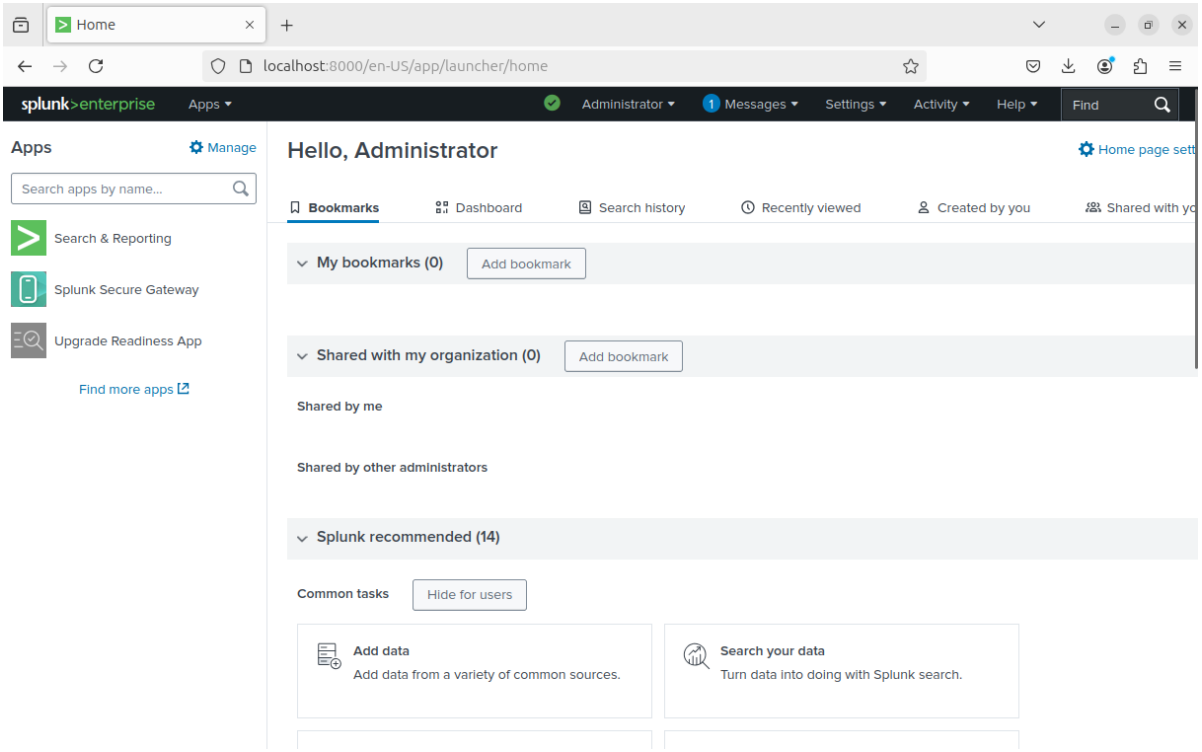
Finally, we should get this as a result where we can enter the Splunk website with the [MachineIP]:8000 or (localhost:8000)

```
Waiting for web server at http://127.0.0.1:8000 to be available..... Done


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://splunk-VirtualBox:8000

root@splunk-VirtualBox:/opt/splunk/bin#
```

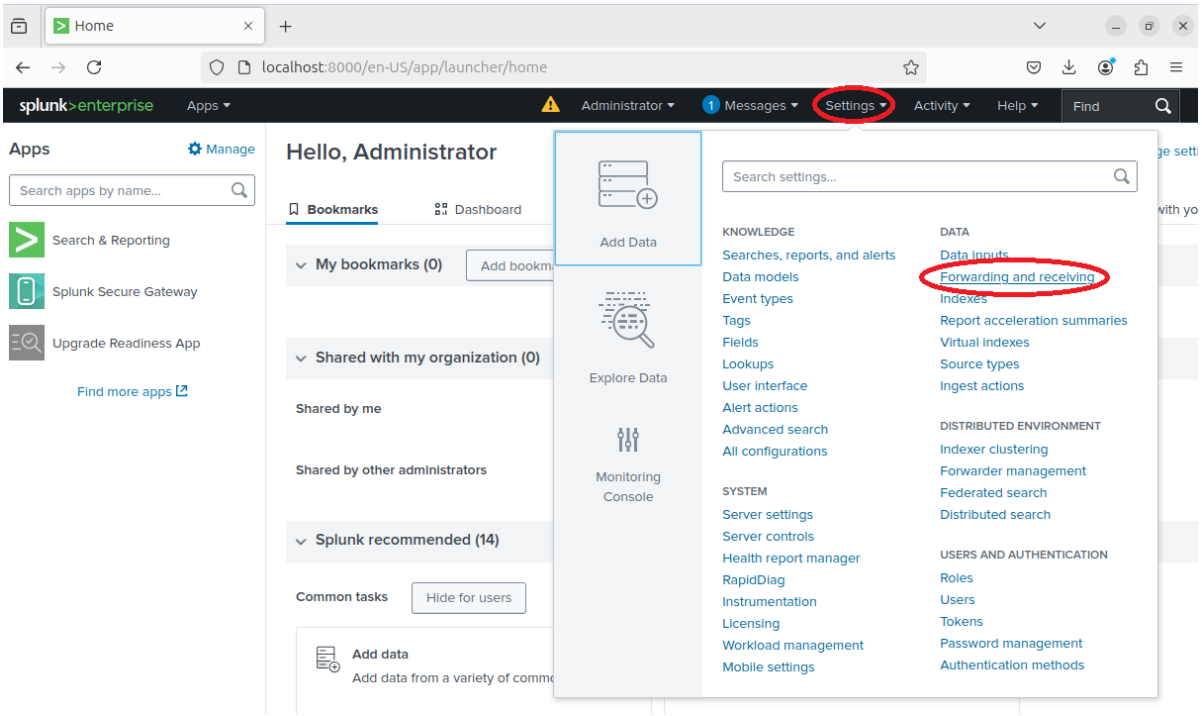
Once we enter the website, we get this page. Sign in with your created credentials

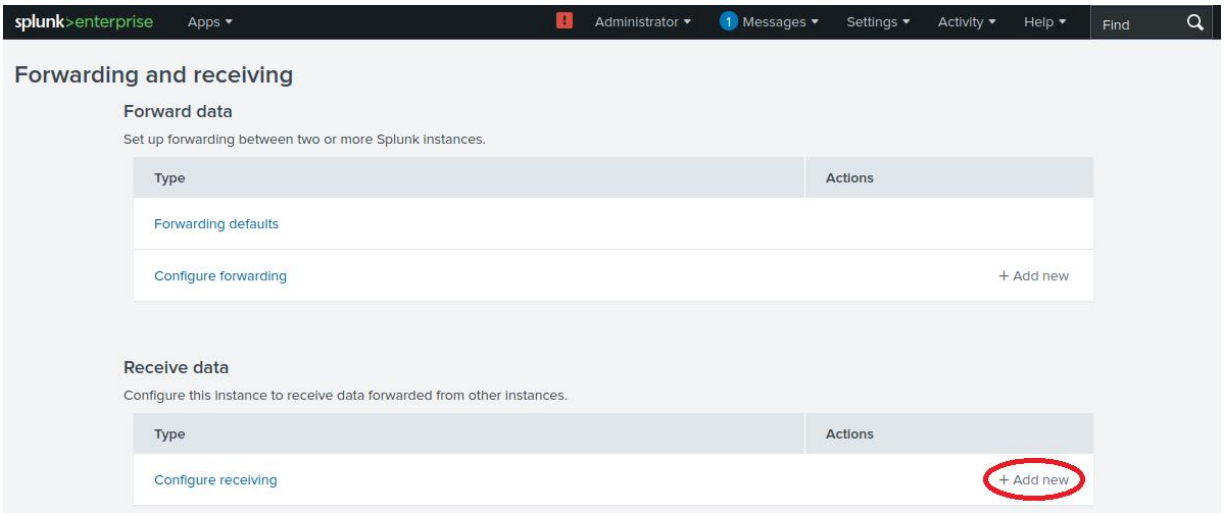


We should be taken to the main page

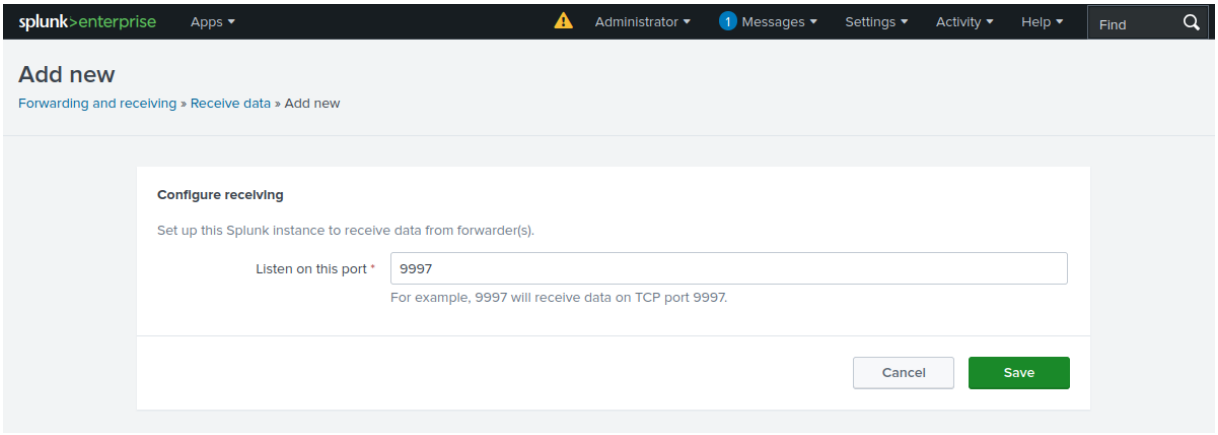


We will have to enable configure the receiving port to receive data forwarded from the Windows server. We can do this by: **Settings > Forwarding and receiving and add a receiving port**





Add port 9997 and save.



Now, we will move to our Windows machine where we will access the Splunk server. We will need the Ubuntu Machine IP which can be done by the command “ip a”

```
splunk@splunk-VirtualBox:/opt/splunk/bin$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:30:b4:9e brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
       valid_lft 86104sec preferred_lft 86104sec
    inet6 fe80::f6c8:a824:ef7e:41e6/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:cc:4c:b2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.108/24 brd 192.168.56.255 scope global dynamic noprefixroute
 enp0s8
```

Splunk Universal Forwarder Setup

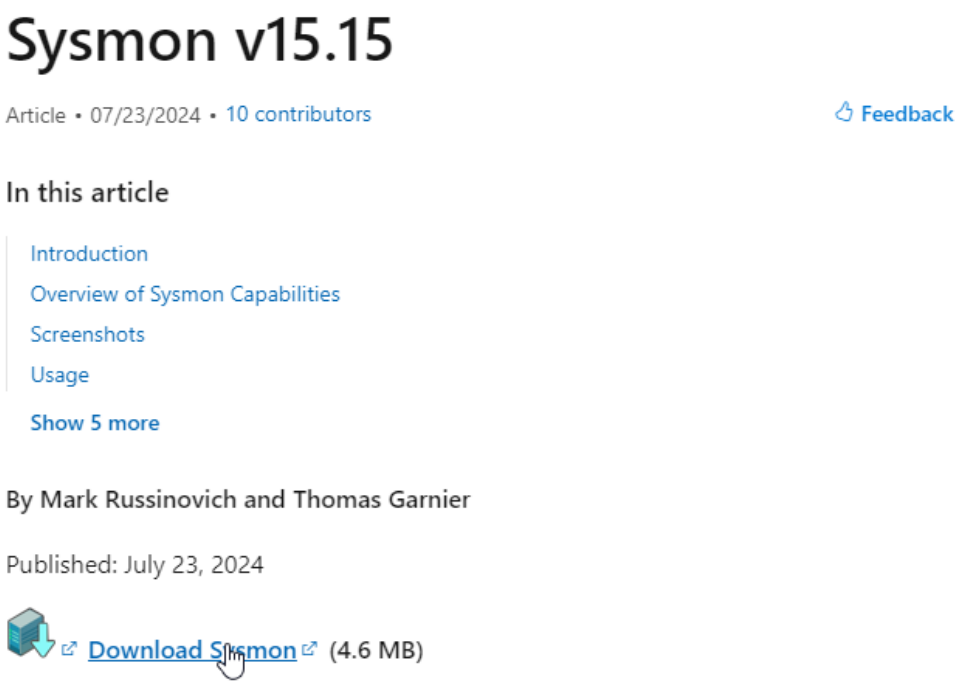
In this section, we install the Splunk Universal Forwarder (UF) agent on the vulnerable Windows IIS Server. Before we install the agent, we will need to download Sysmon, a Microsoft tool that will monitor and log system activity on the Windows IIS server.

Sysmon Integration

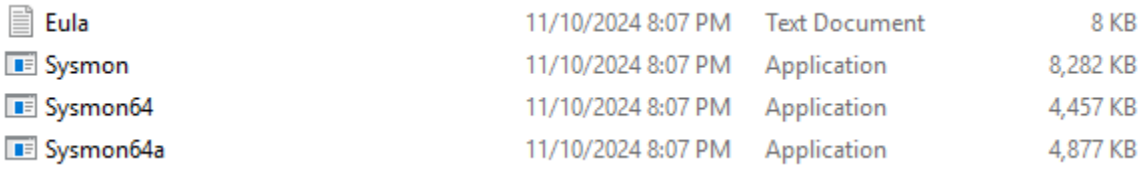
Firstly, we will install and configure Sysmon on the Windows endpoint.

We can download Sysmon from the following link:

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



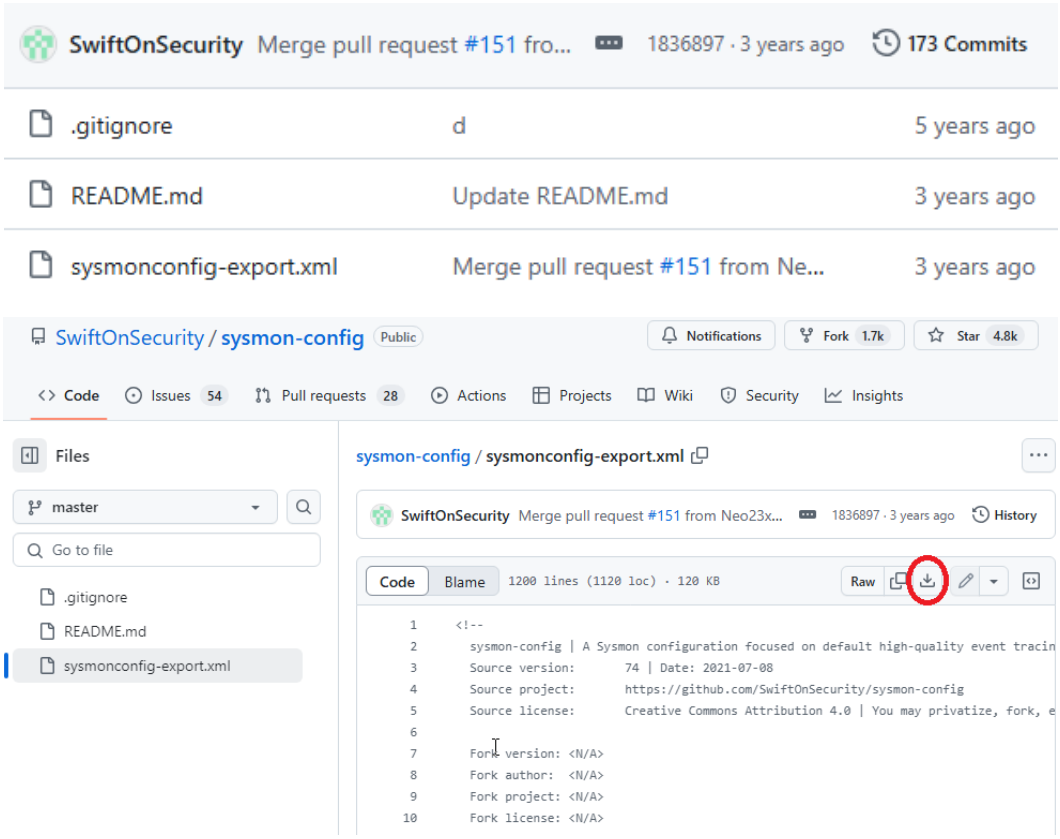
Extract the zip file and we should get this:



We will now need to download the Configuration file from the following link:

https://github.com/SwiftOnSecurity/sysmon-config

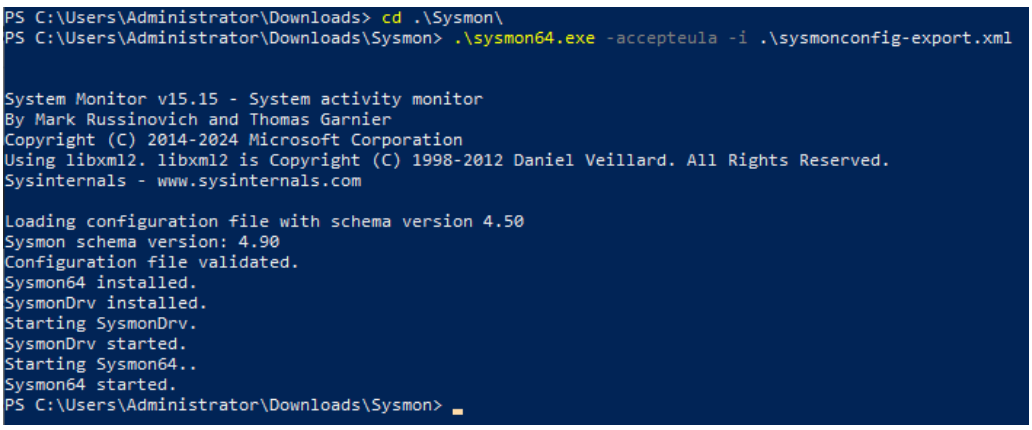
Click on the sysmonconfig-export.xml, and download the file



Once we unzipped the Sysmon file and downloaded the Sysmon configuration file, we should have these two files.

Drag the sysmonconfig-export.xml into the Sysmon folder then run the following command in PowerShell as administrator.

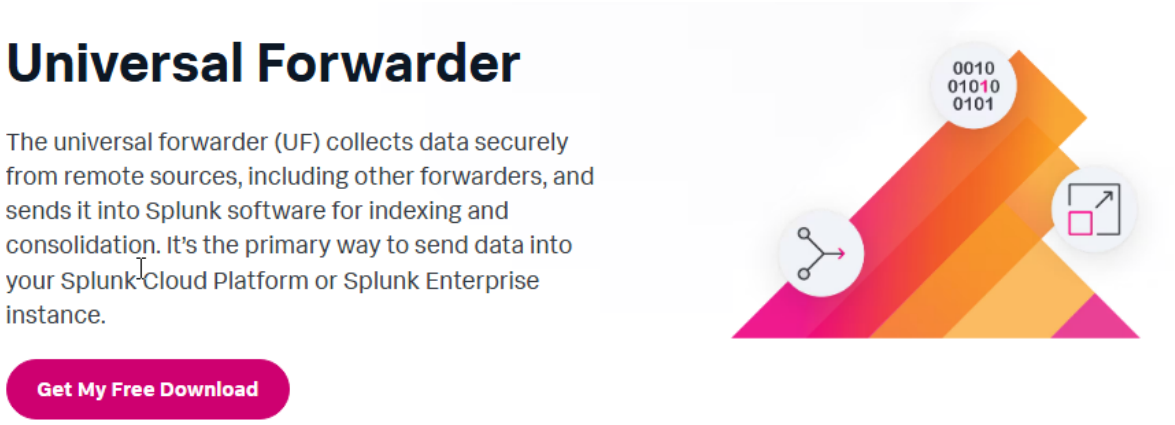
".\sysmon64.exe -accepteula -i .\sysmonconfig-export.xml"

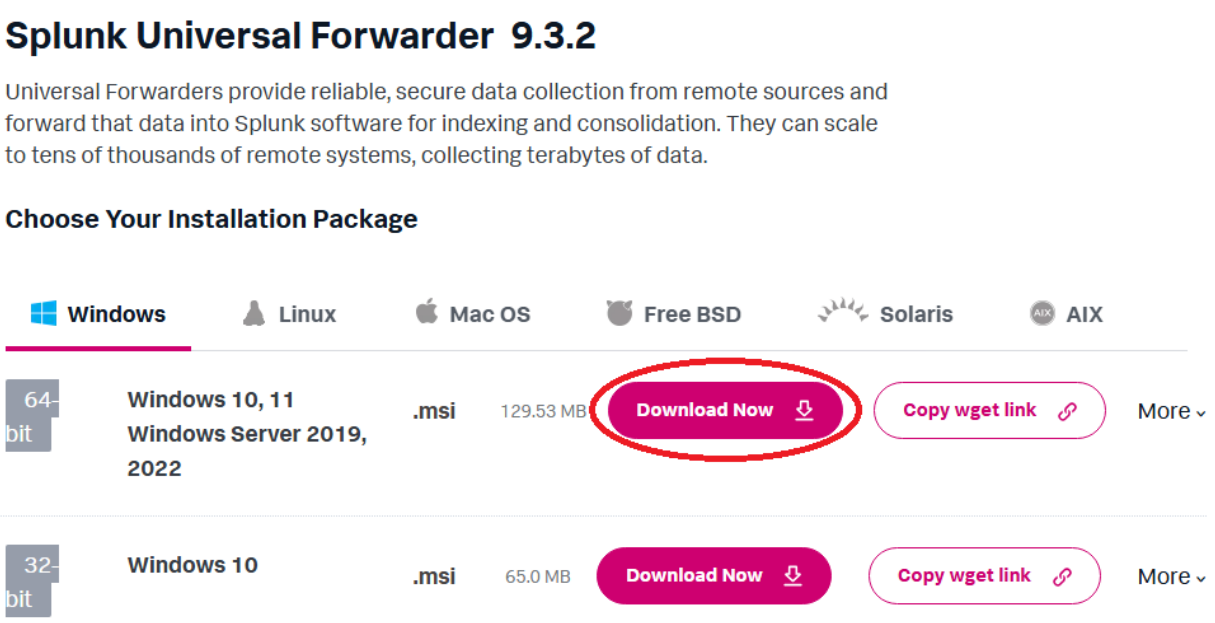


Splunk Universal Forwarder Installation

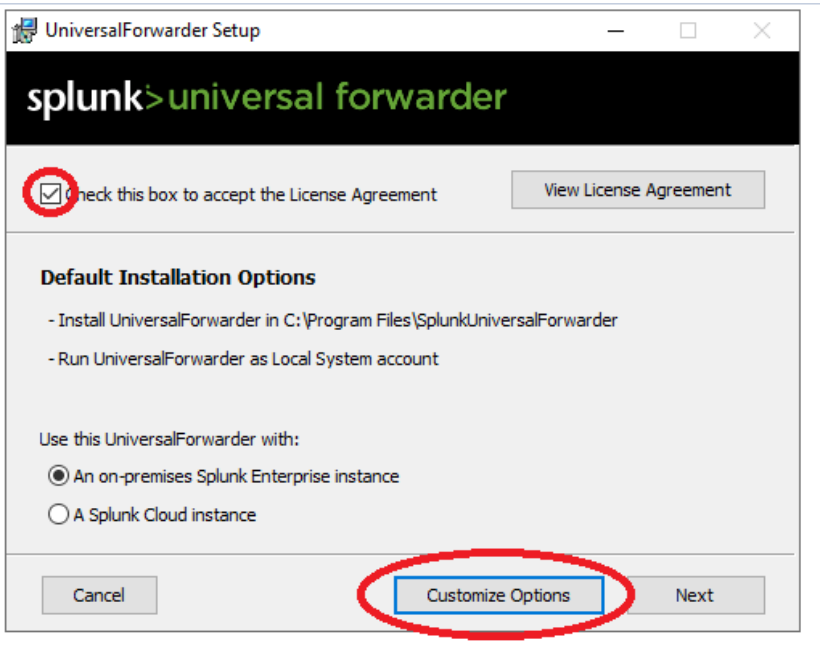
We can download Splunk UF from this link: https://www.splunk.com/en_us/download.html

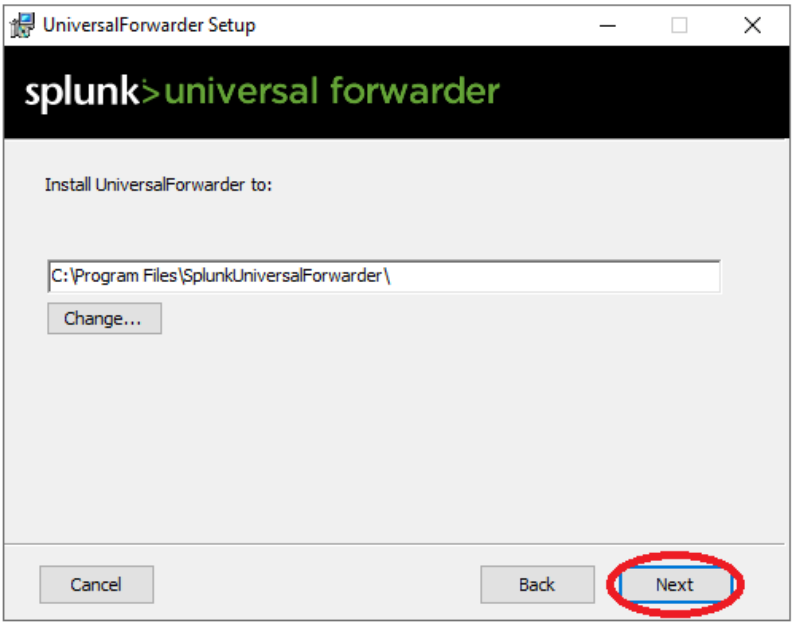
Go to the “Universal Forwarder” section and click on Get My Free Download where you will need to log in with your created account.

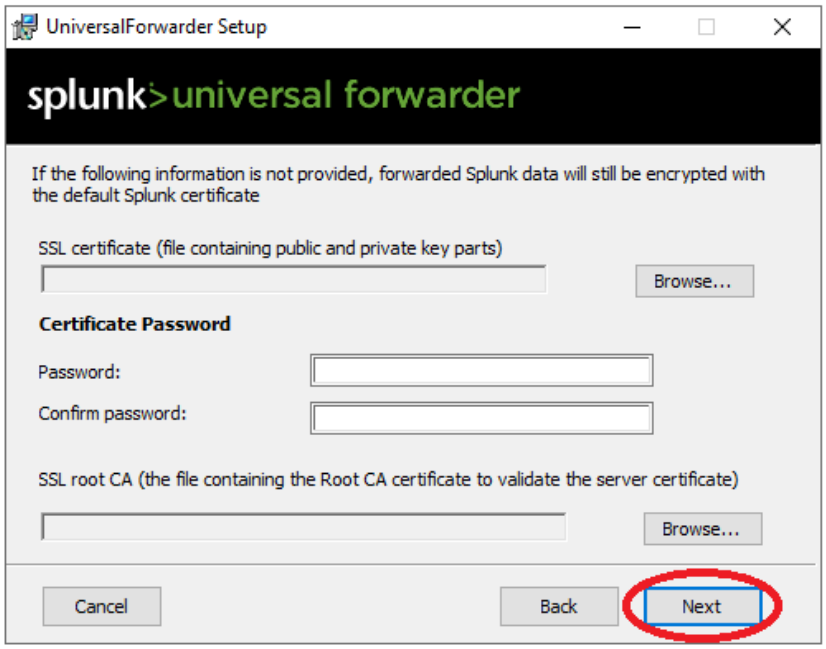


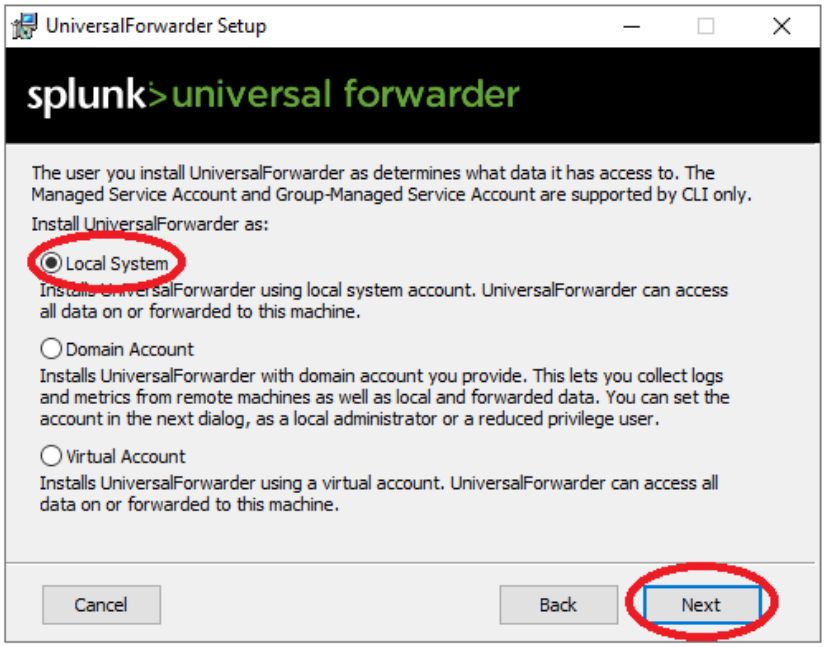


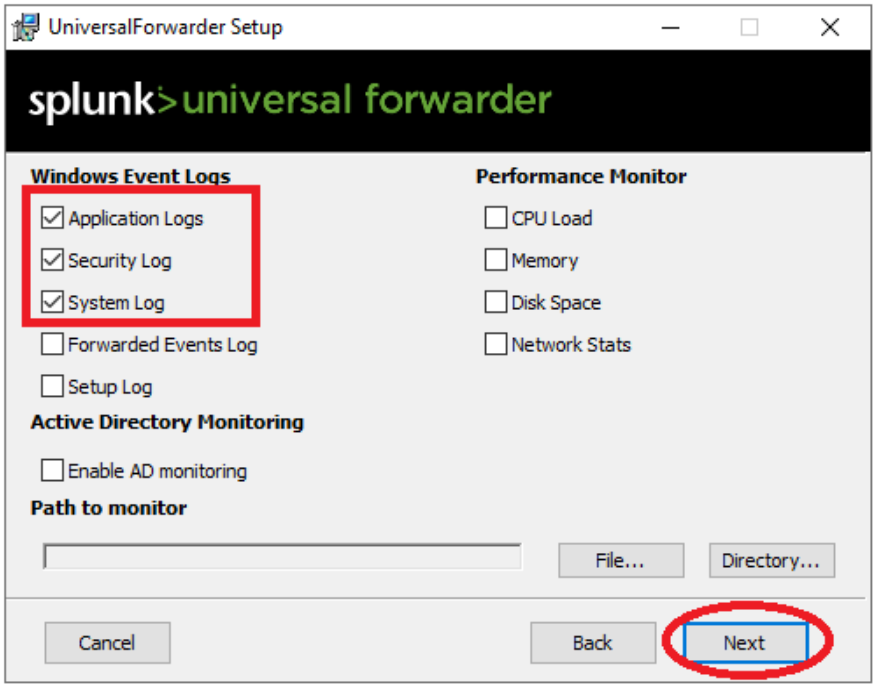
Once the file is downloaded, run the .msi file and follow the instructions below:

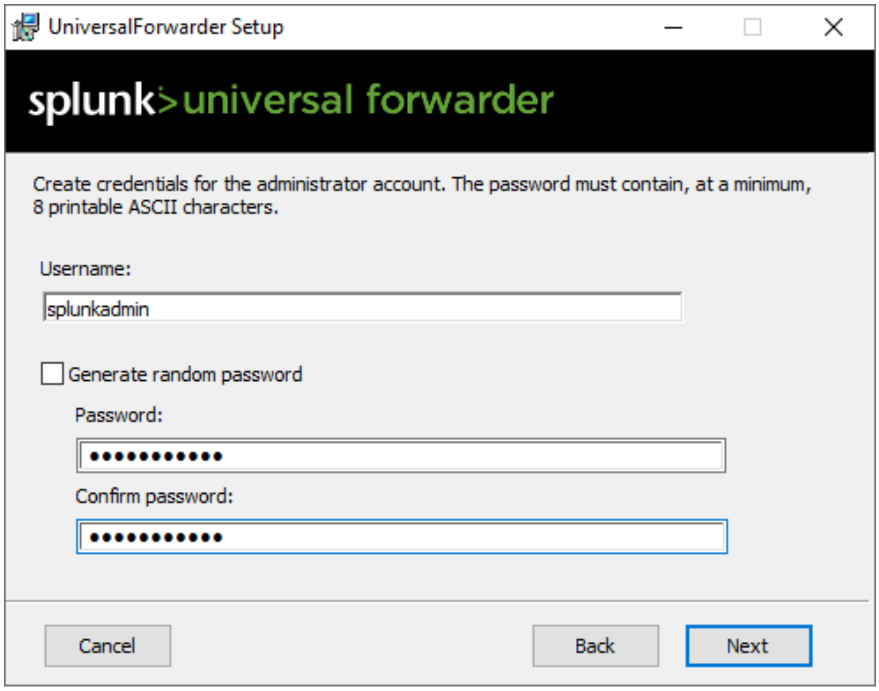




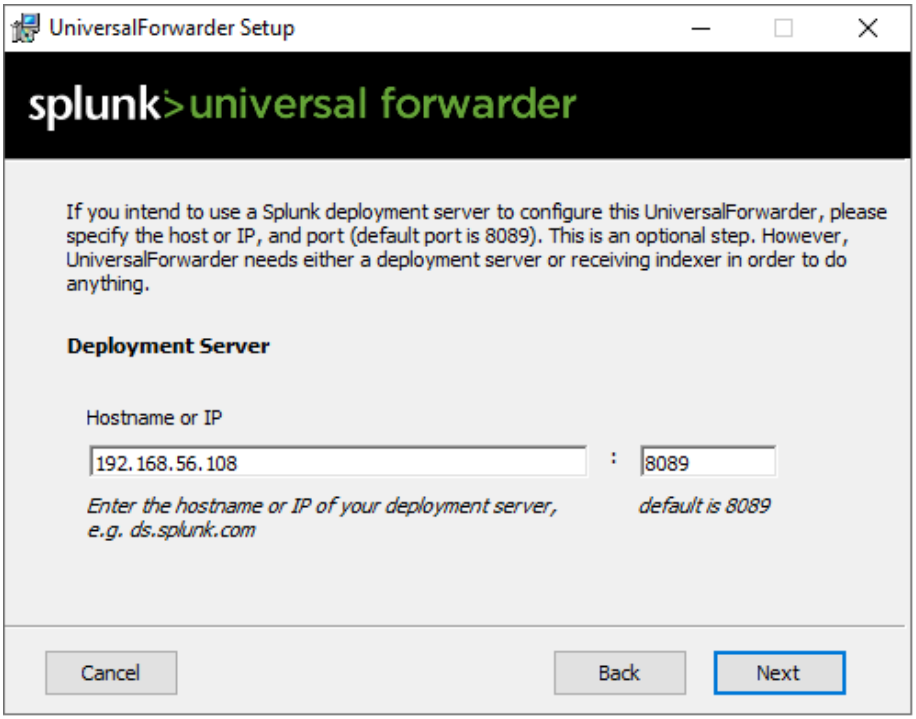

UniversalForwarder Setup
splunk>universal forwarder
If the following information is not provided, forwarded Splunk data will still be encrypted with the default Splunk certificate
SSL certificate (file containing public and private key parts)
Browse...
Certificate Password
Password:
Confirm password:
SSL root CA (the file containing the Root CA certificate to validate the server certificate)
Browse...
Cancel
Back
Next

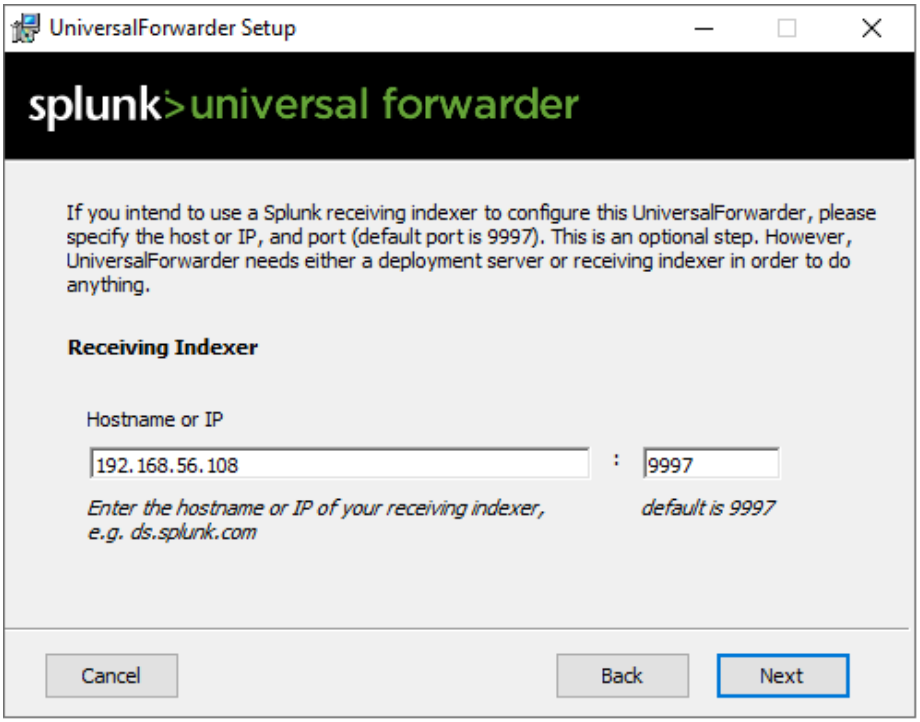

UniversalForwarder Setup
splunk>universal forwarder
The user you install UniversalForwarder as determines what data it has access to. The Managed Service Account and Group-Managed Service Account are supported by CLI only.
Install UniversalForwarder as:
Local System
Installs UniversalForwarder using local system account. UniversalForwarder can access all data on or forwarded to this machine.
Domain Account
Installs UniversalForwarder with domain account you provide. This lets you collect logs and metrics from remote machines as well as local and forwarded data. You can set the account in the next dialog, as a local administrator or a reduced privilege user.
Virtual Account
Installs UniversalForwarder using a virtual account. UniversalForwarder can access all data on or forwarded to this machine.
Cancel
Back
Next


UniversalForwarder Setup
splunk>universal forwarder
Windows Event Logs
Application Logs
Security Log
System Log
Forwarded Events Log
Setup Log
Performance Monitor
CPU Load
Memory
Disk Space
Network Stats
Active Directory Monitoring
Enable AD monitoring
Path to monitor
File...
Directory...
Cancel
Back
Next


UniversalForwarder Setup
splunk>universal forwarder
Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.
Username:
splunkadmin
Generate random password
Password:
Confirm password:
Cancel
Back
Next

Enter the Ubuntu Machine IP as the Deployment Server and the Receiving Indexer with the default ports





Then click **“Next” > “Install” > “Finish”**

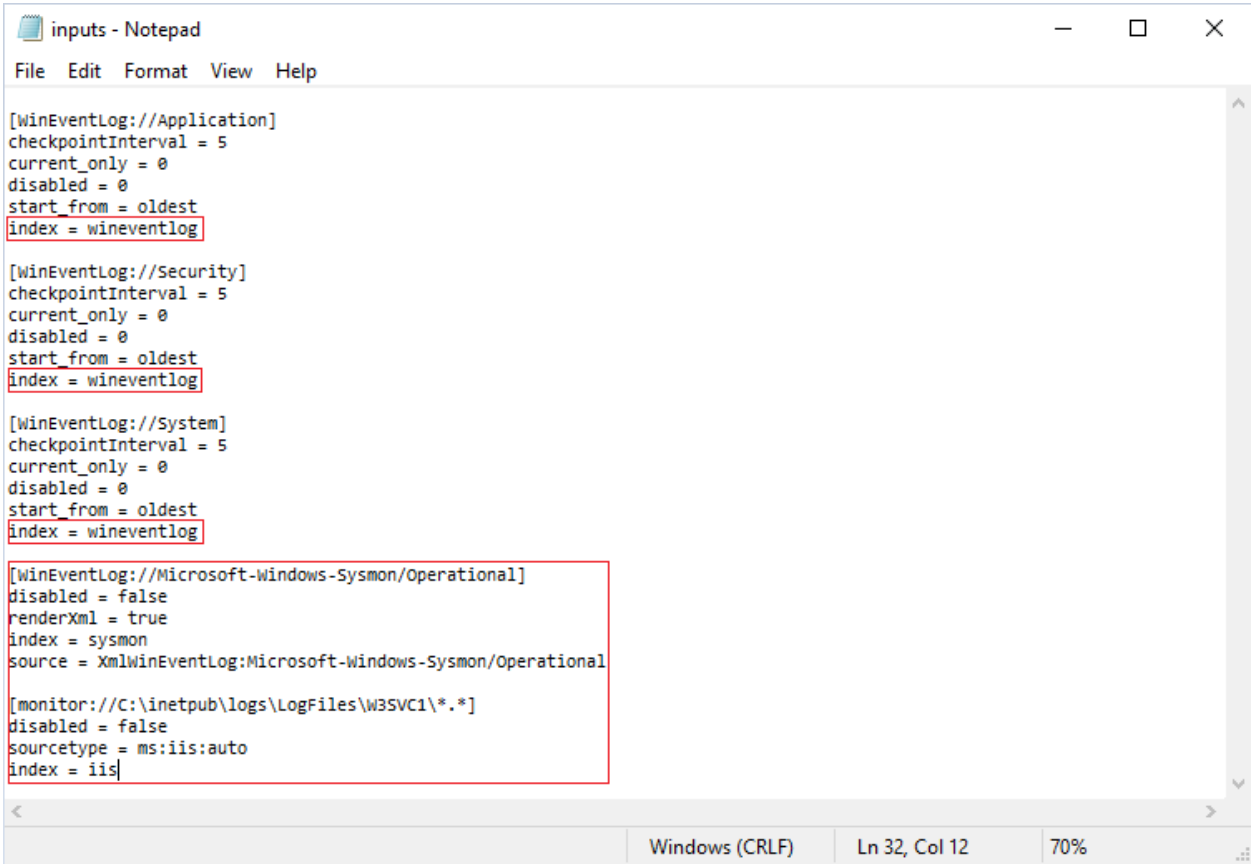
Splunk Universal Forwarder Configuration

In this section, we will be configuring Splunk UF to monitor Sysmon and IIS logs.

Go to the directory:

C:\Program Files\SplunkUniversalForwarder\etc\apps\SplunkUniverslForwarder\local

Then open the **inputs.conf** file with notepad and edit the file according to the red boxes in the screenshot below:



The configuration below allows the Universal Forwarder to monitor the Sysmon Event Log and store the data in the "sysmon" index.

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

disabled = false

renderXml = true

index = sysmon

source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

The configuration below monitors IIS log files in the specified directory, categorizes them using the ms:iis:auto sourcetype, and will store the data in the “iis” index.

Make sure the directory **C:\inetpub\logs\LogFiles\W3SVC1** is correct for your specific machine.

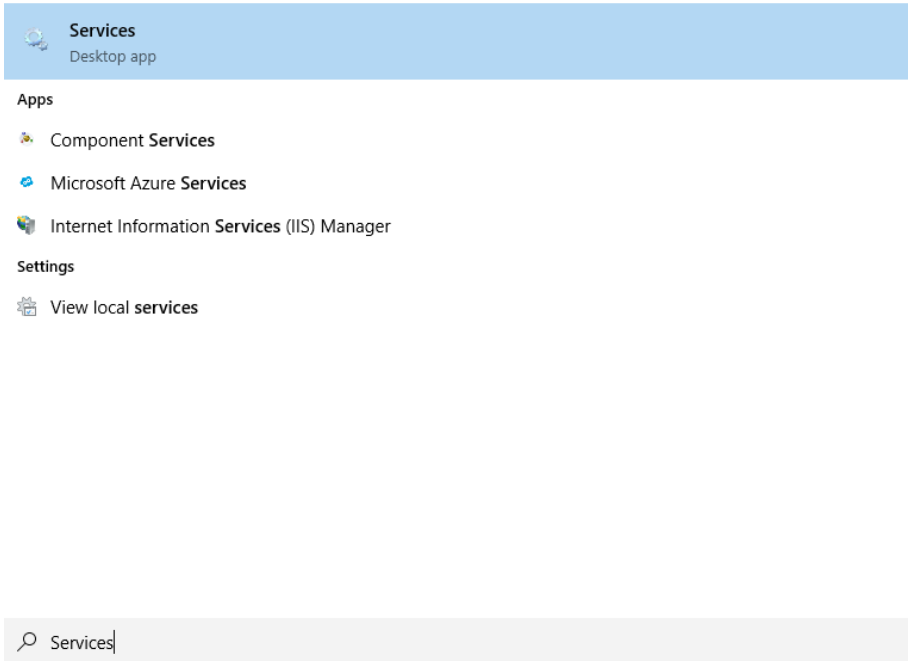
[monitor://C:\inetpub\logs\LogFiles\W3SVC1*.*]

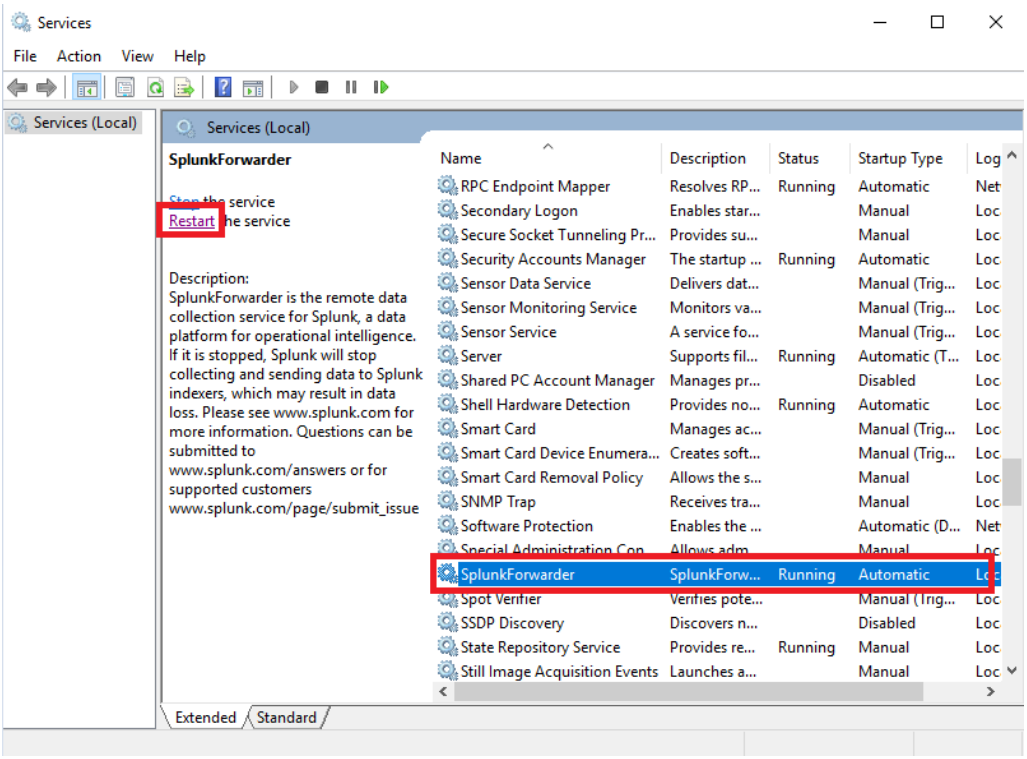
disabled=false

sourcetype=ms:iis:auto

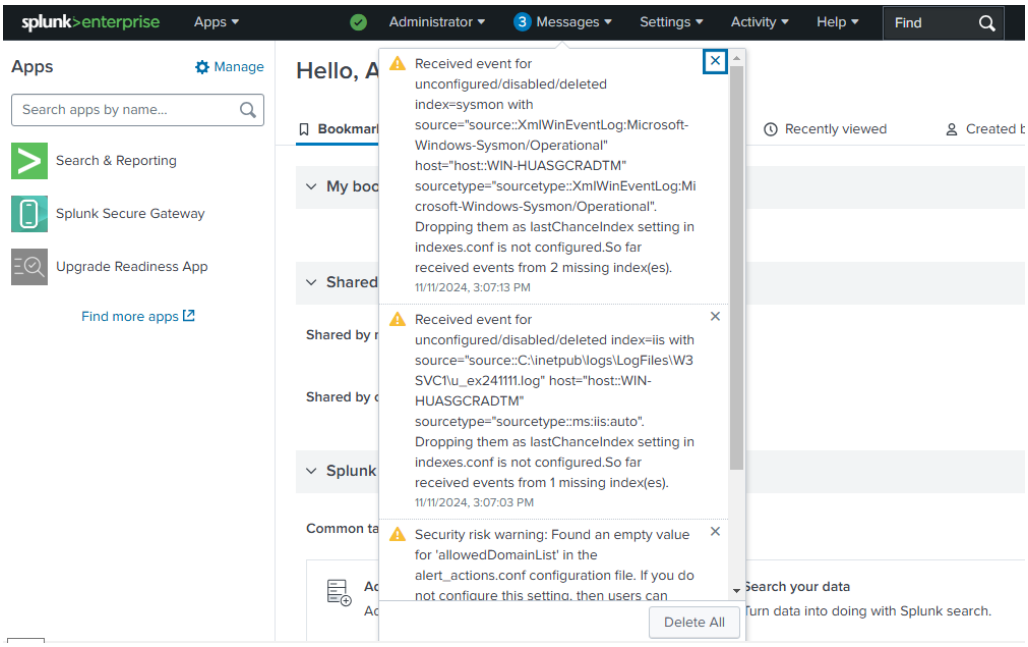
index = iis

Save the inputs.conf file and then restart the SplunkForwarder service by going to the “Services” app (services.msc)

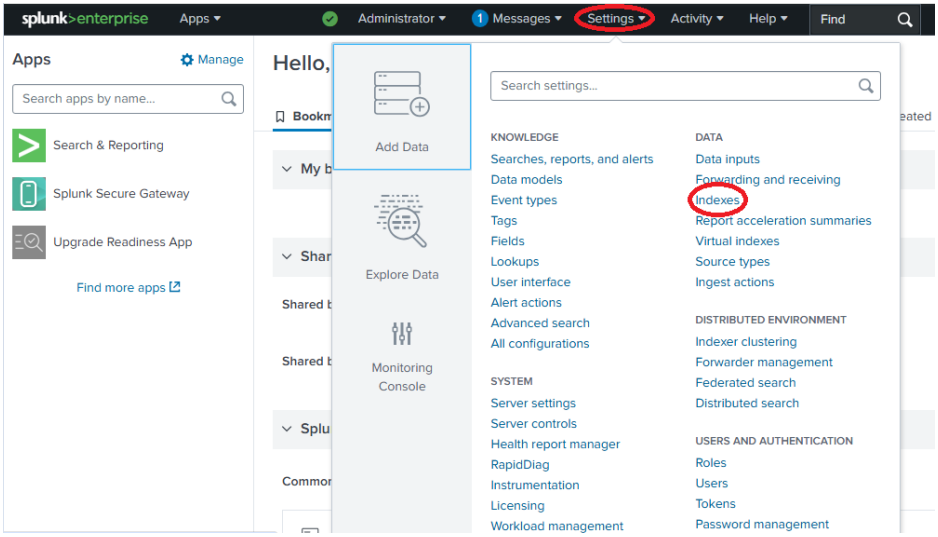


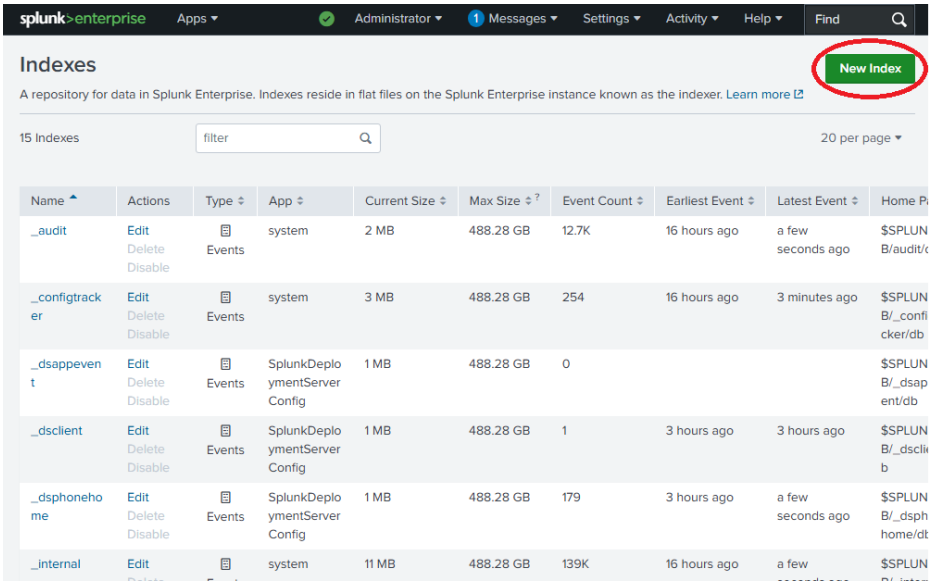


Once SplunkForwarder has restarted, we should get these messages shown below



Now we will log into Splunk from our Windows machine and add extra indexes.

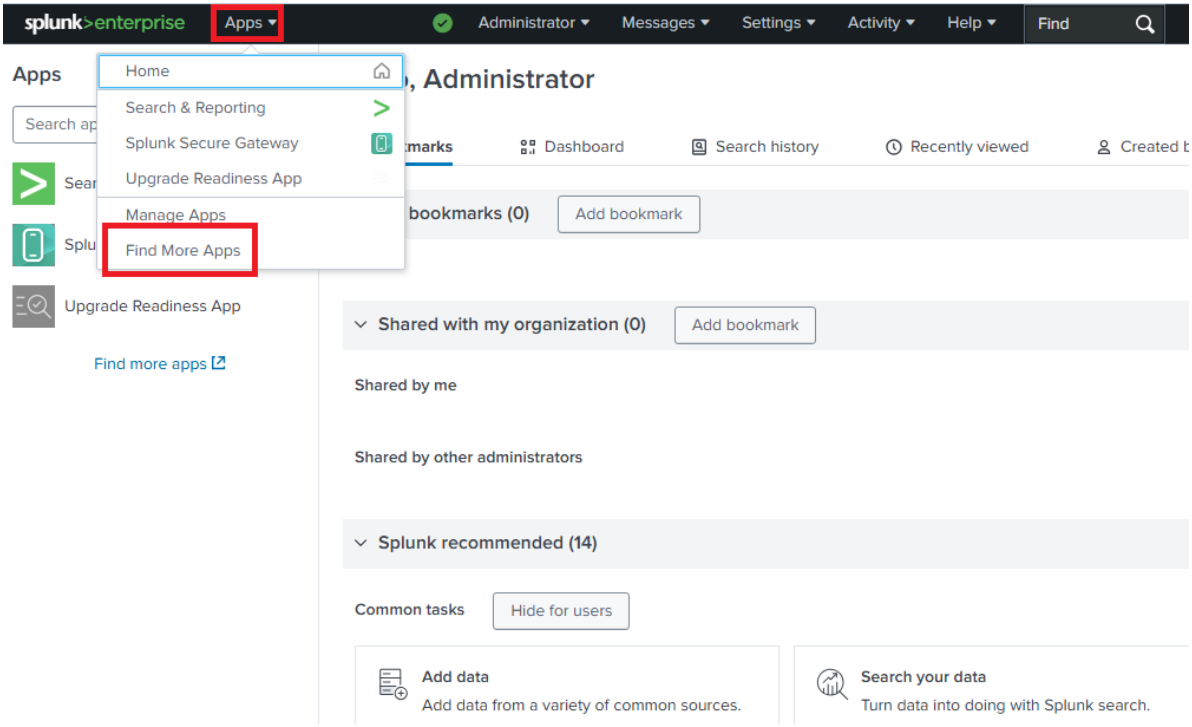




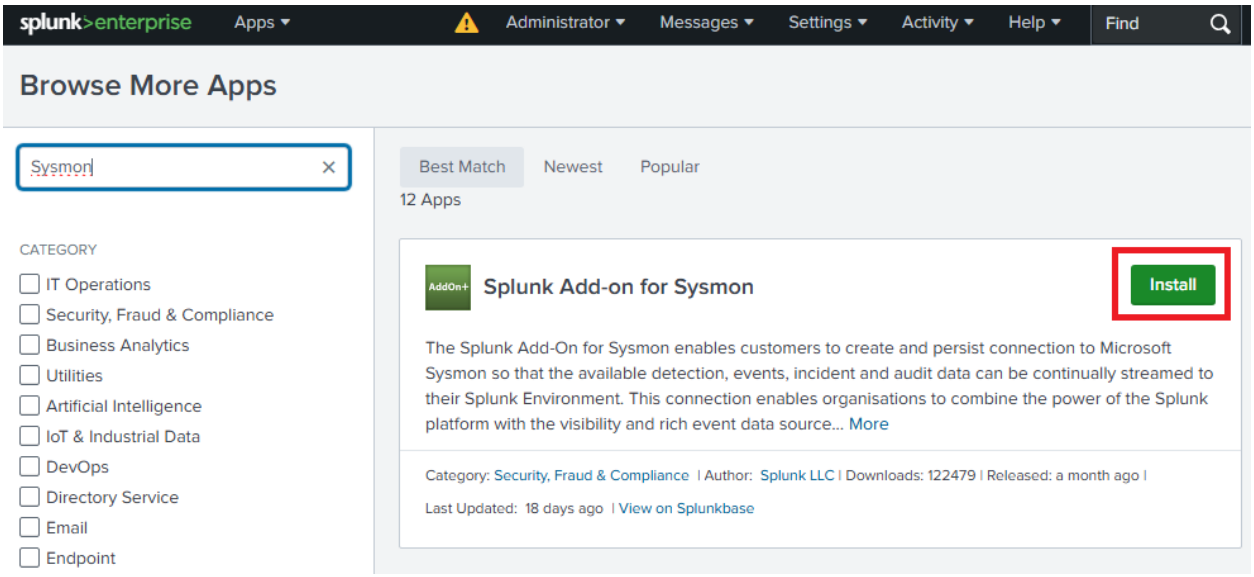
We will add three indexes including sysmon, iis, and wineventlog. Name the indexes accordingly and leave the rest of the settings as default then save them.

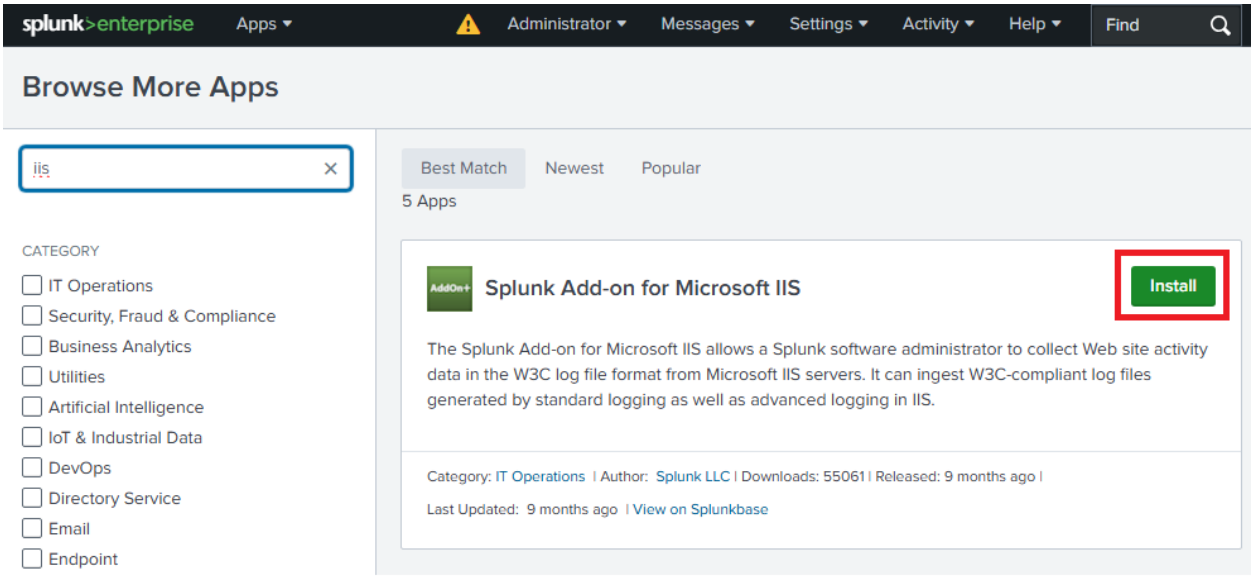
Splunk Universal Forwarder App Installation

In this section, we will install two different apps in Splunk for Sysmon and IIS.



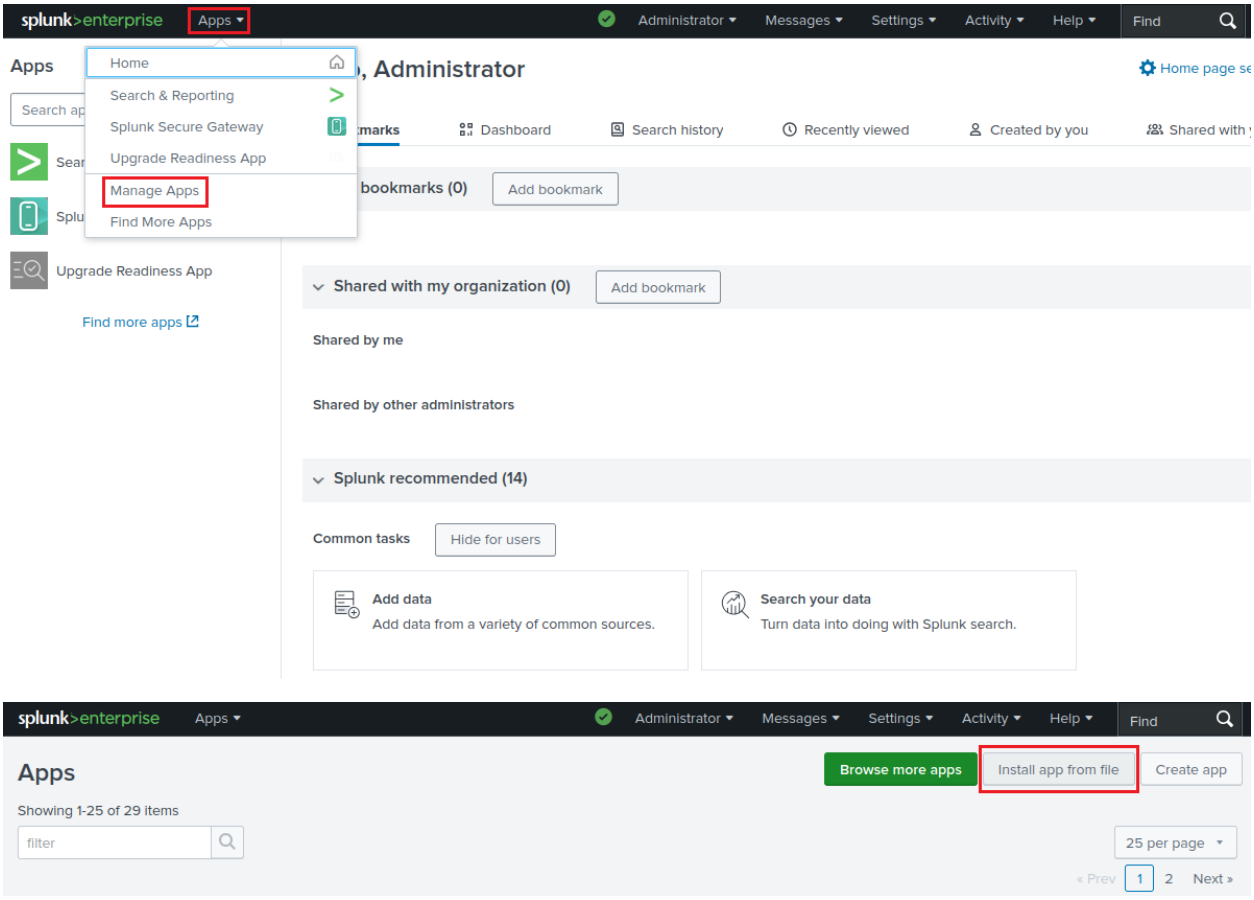
Search for the apps “Splunk Add-on for Sysmon” and “Splunk Add-on for Microsoft IIS”, click Install then log in using your Splunk credentials that you used to download Splunk.



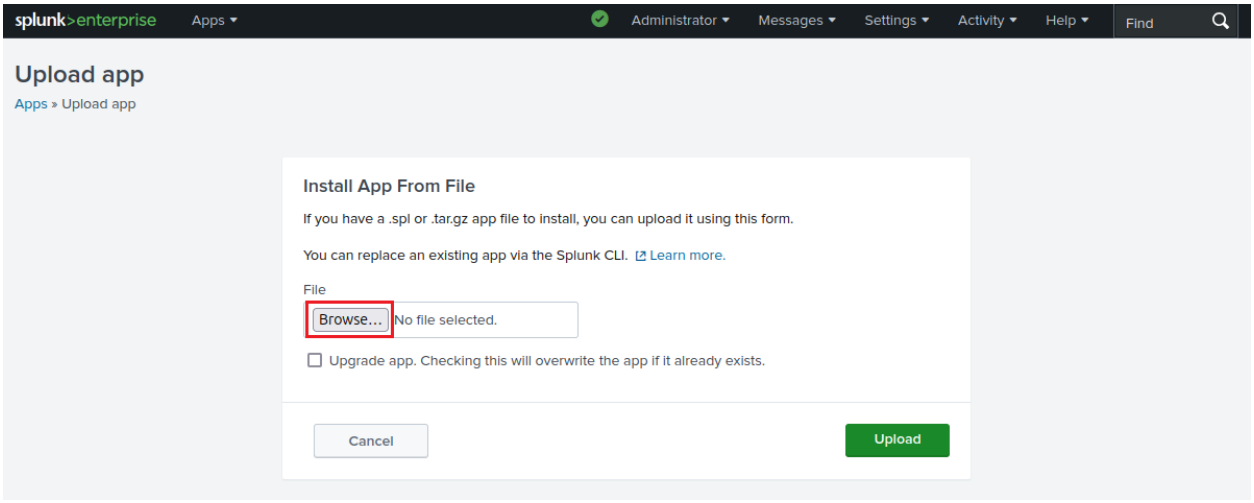


If you are using the provided download files that contains all the files you need for this lab, you can import the apps by following the steps.

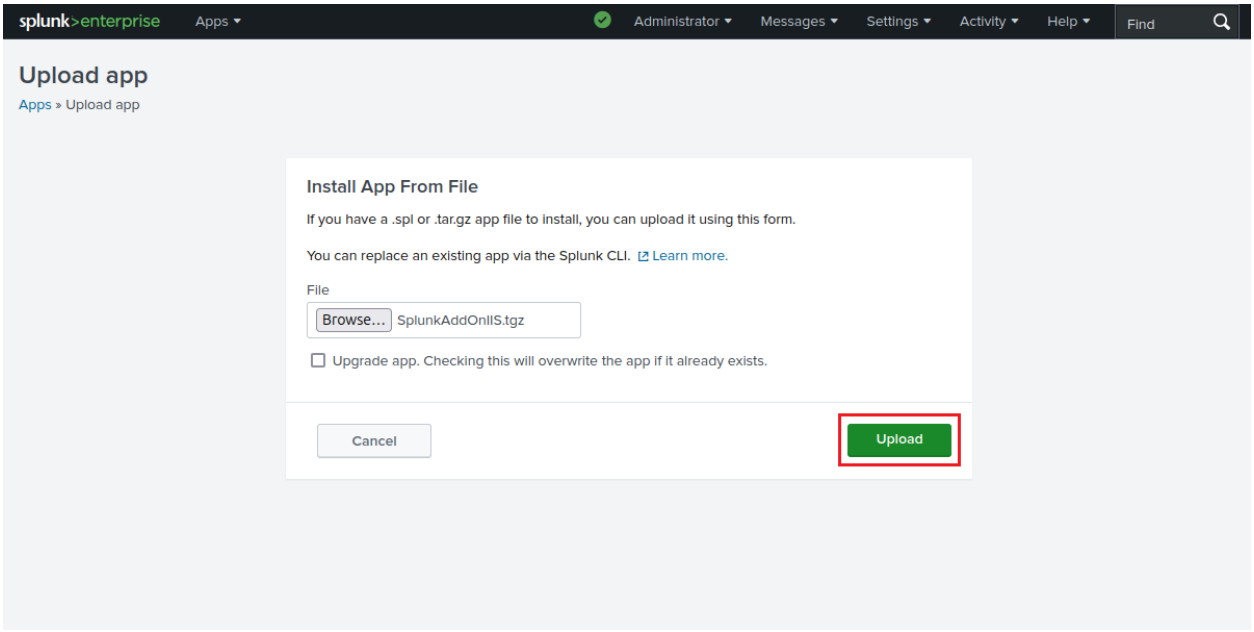
(If you are not using the provided files, then you can skip the steps below)



Select “Browse” and go to the downloaded files in the folder “Splunk Server Config” then import both SplunkAddOnSysmon.tgz and SplunkAddOnIIS.tgz (No need to unzip the files)

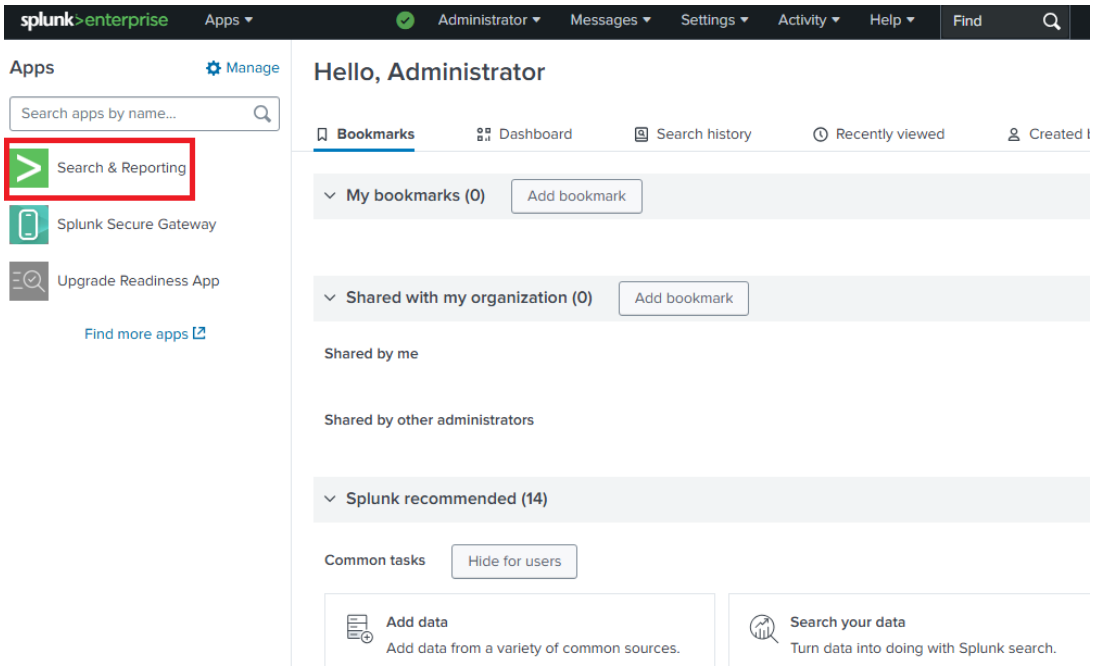


One you have selected the file, click “Upload”

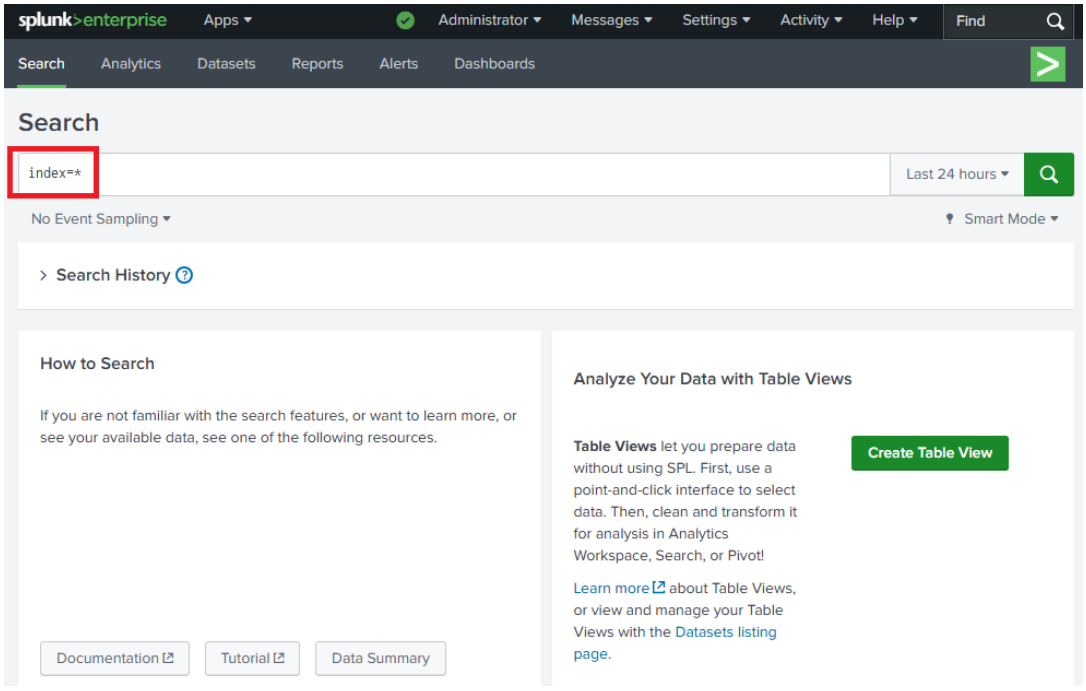


Now we will see if the Sysmon and IIS logs are showing. To do this, enter localhost on your Windows Machine and refresh a couple times to create event logs.

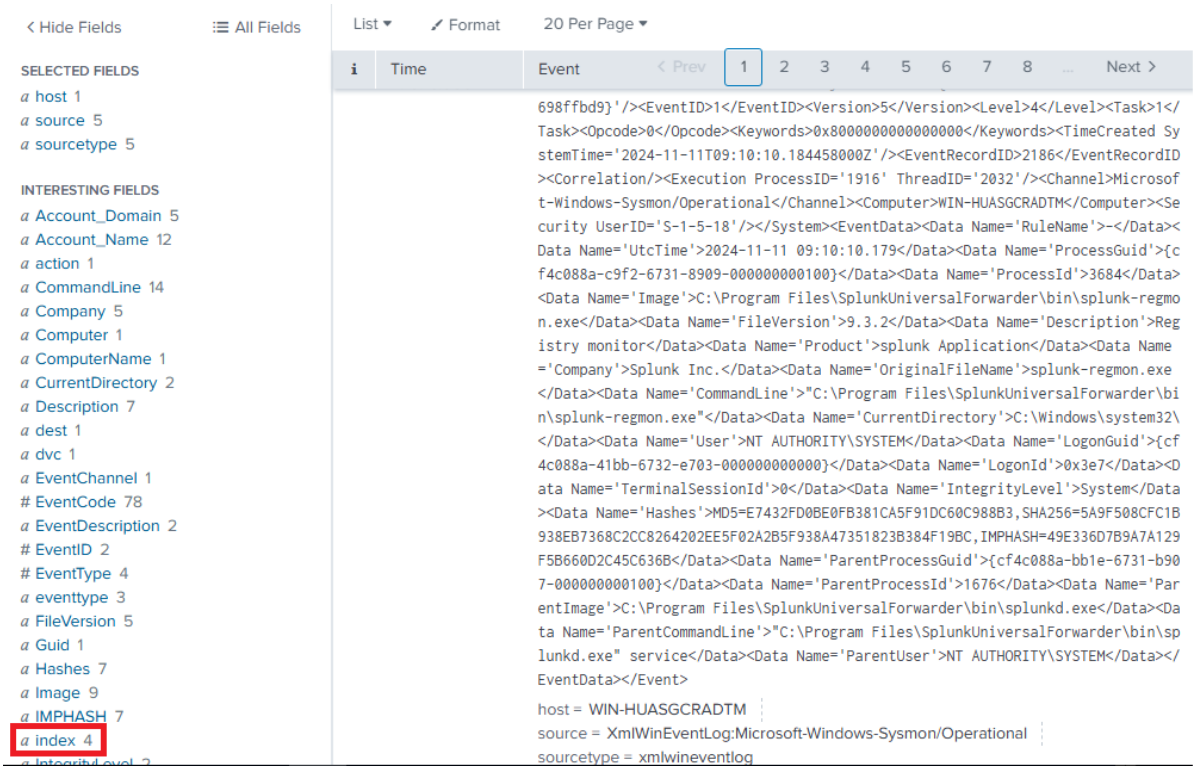
Now on the Splunk website, go to “Search & Reporting” page where we can search and analyze ingested data.



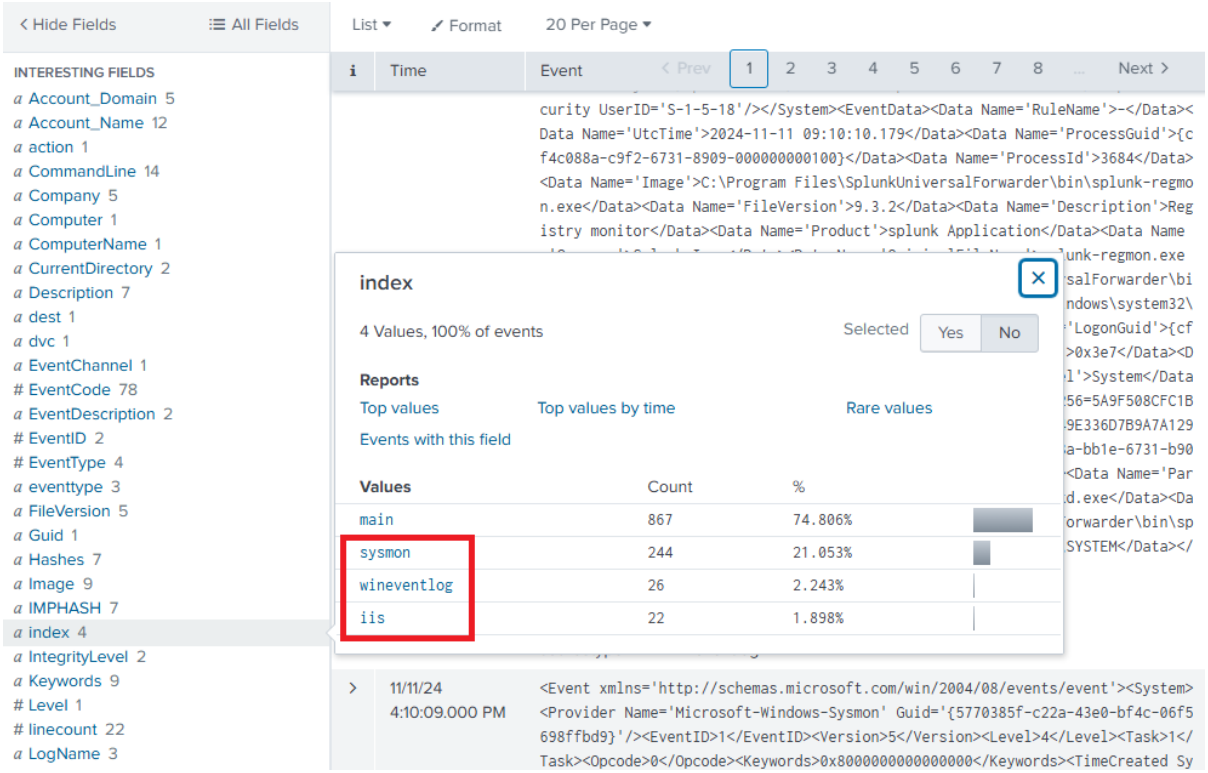
We will be taken to a page where we enter the query: “index=*” which will retrieve all events from all indexes available including the ones we created.



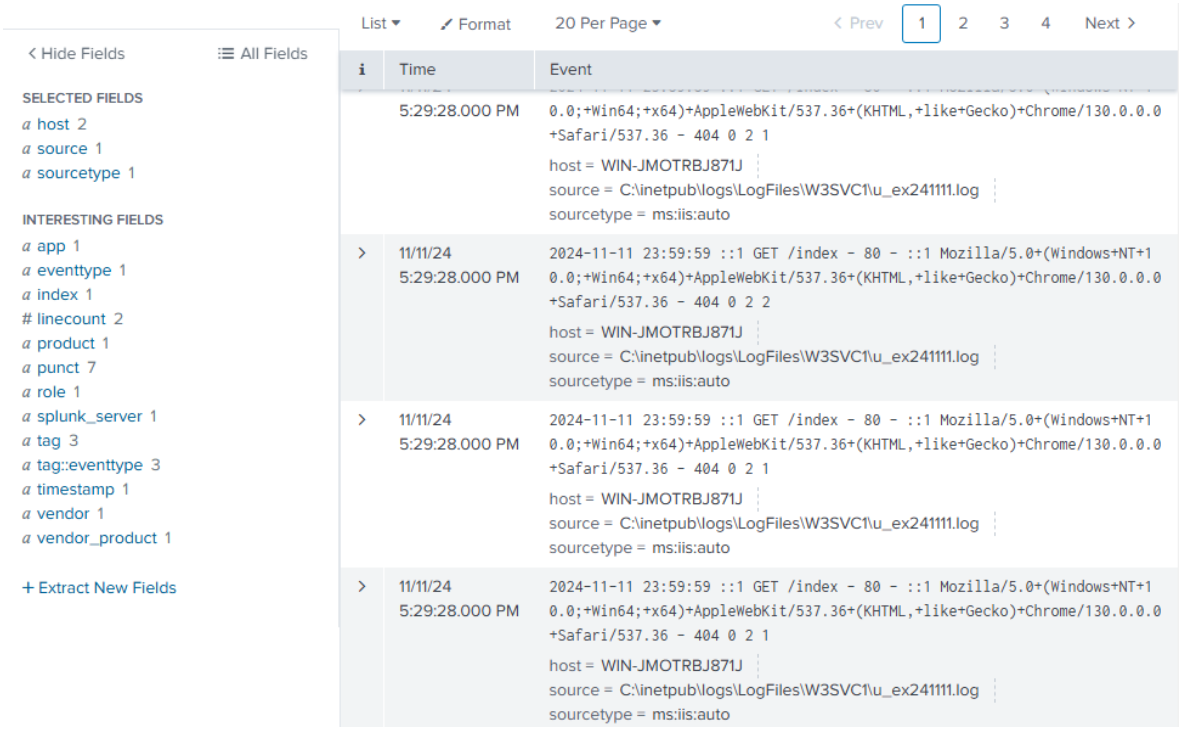
We will get a result like the screenshot below. To see the events stored in different indexes, click on “index” on the left panel.



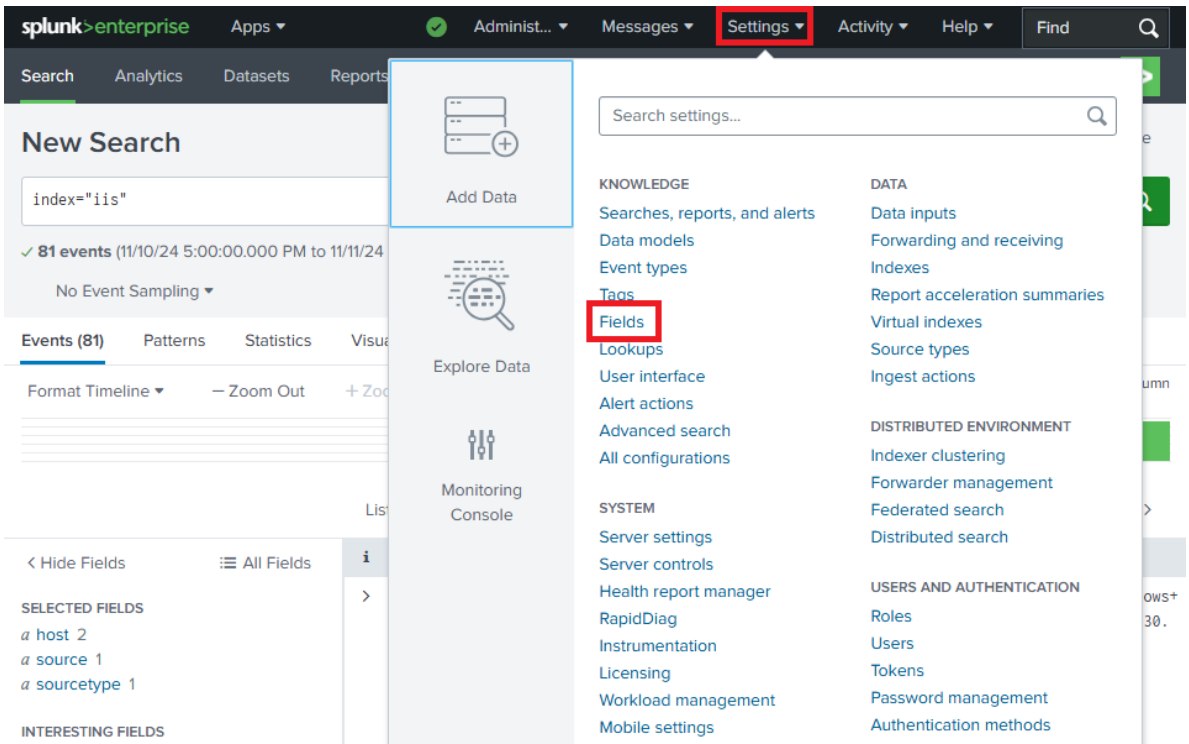
We see that sysmon, wineventlog, and iis shows up in the indexes.

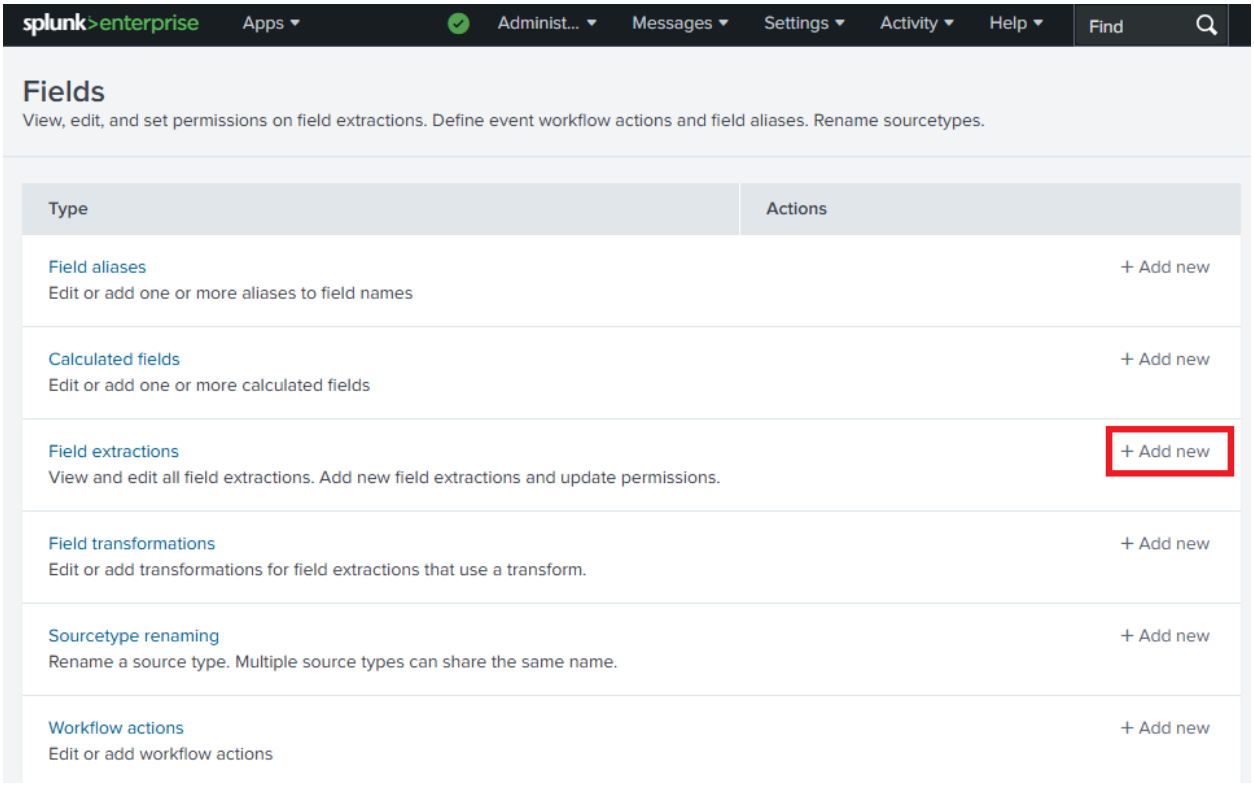


Now, if we search for index=”iis” we will get:



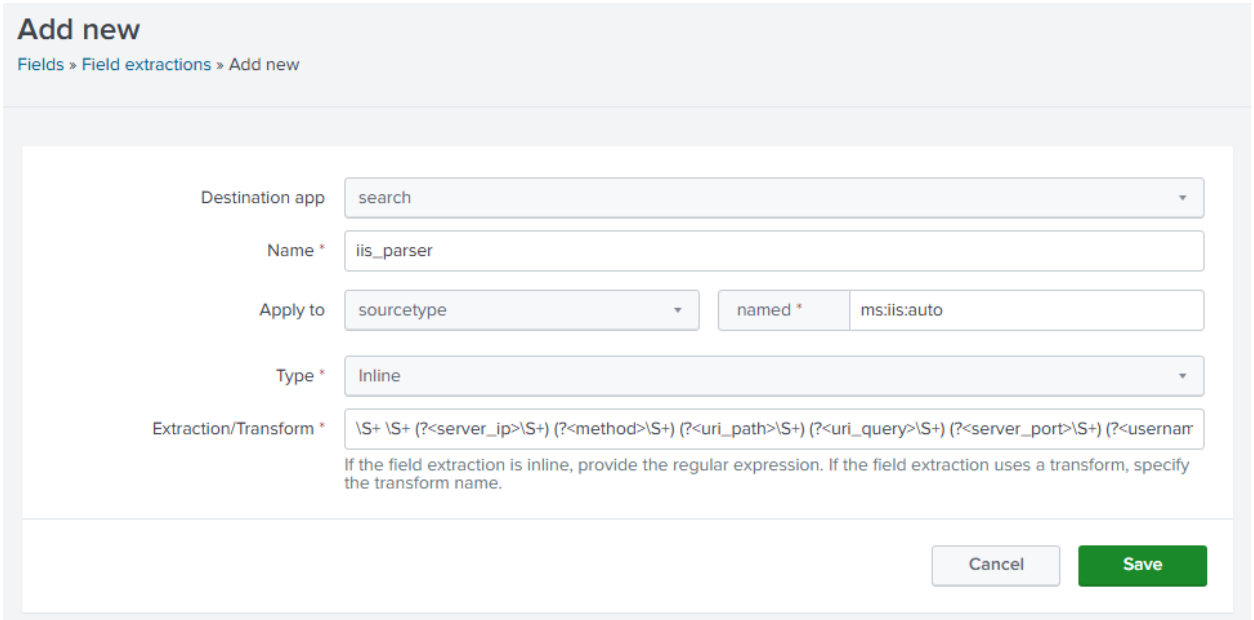
We will add a new field extraction to extract specific fields from the IIS logs

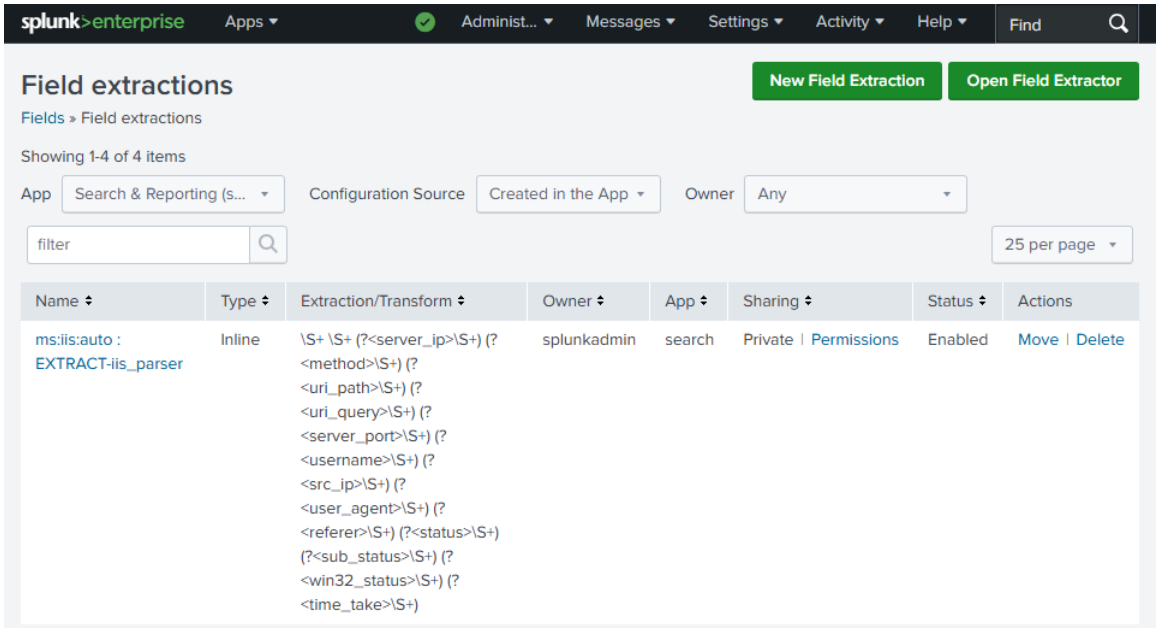




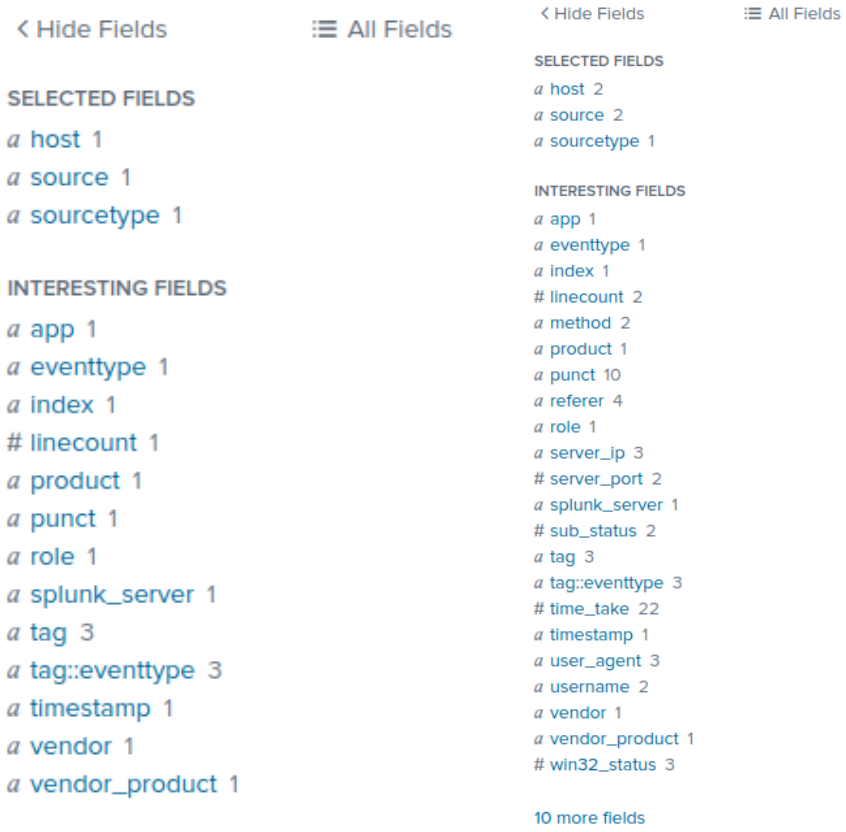
Below is a regular expression (REGEX) for the field extraction.

\S+ \S+ (?<server_ip>\S+) (?<method>\S+) (?<uri_path>\S+) (?<uri_query>\S+) (?<server_port>\S+) (?<username>\S+) (?<src_ip>\S+) (?<user_agent>\S+) (?<referer>\S+) (?<status>\S+) (?<sub_status>\S+) (?<win32_status>\S+) (?<time_take>\S+)





Now that we have added the new Field Extraction, we can see the differences in fields between the old logs and the new logs.

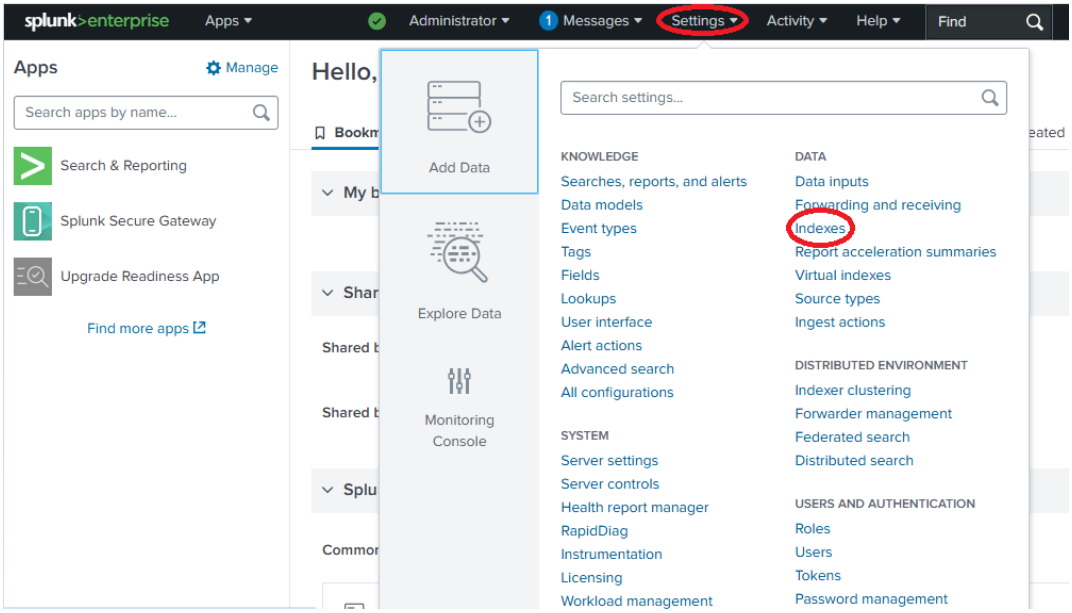


On the left are the fields extracted prior to the added Field Extraction rule, and on the right is after we added the new Field Extraction rule. We can see that more fields are being extracted from the IIS logs.

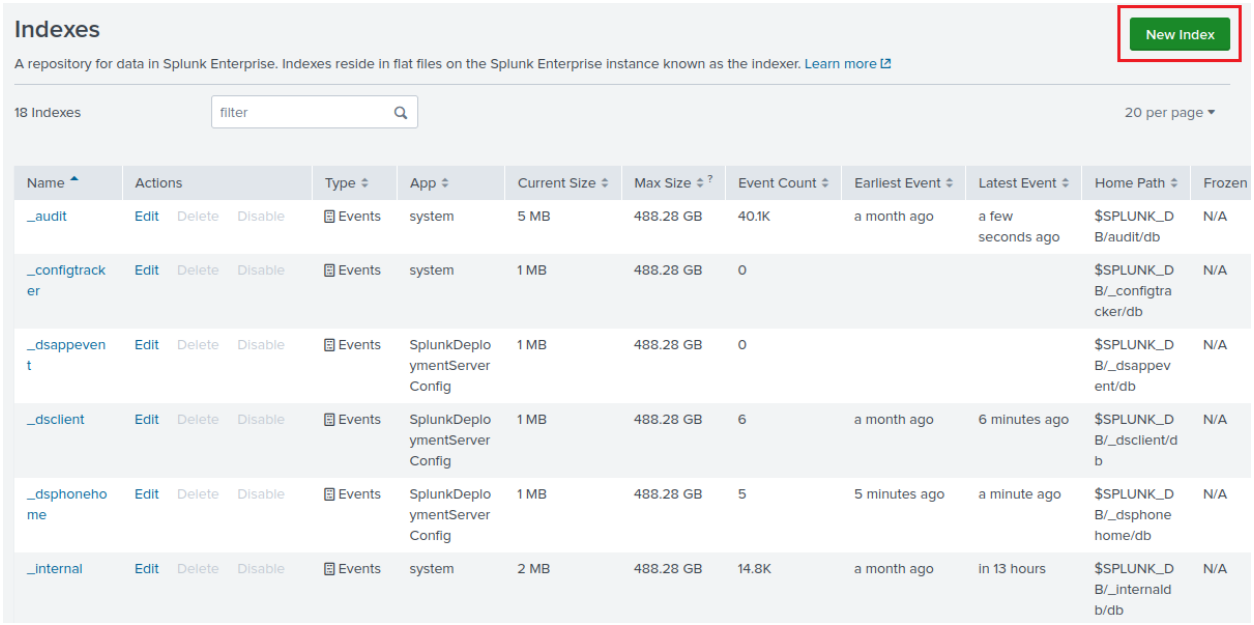
Splunk Setup for Apache Logs

Now that we have successfully set up Splunk to receive forwarded IIS and Sysmon logs, we will do the same for Apache's access logs from XAMPP.

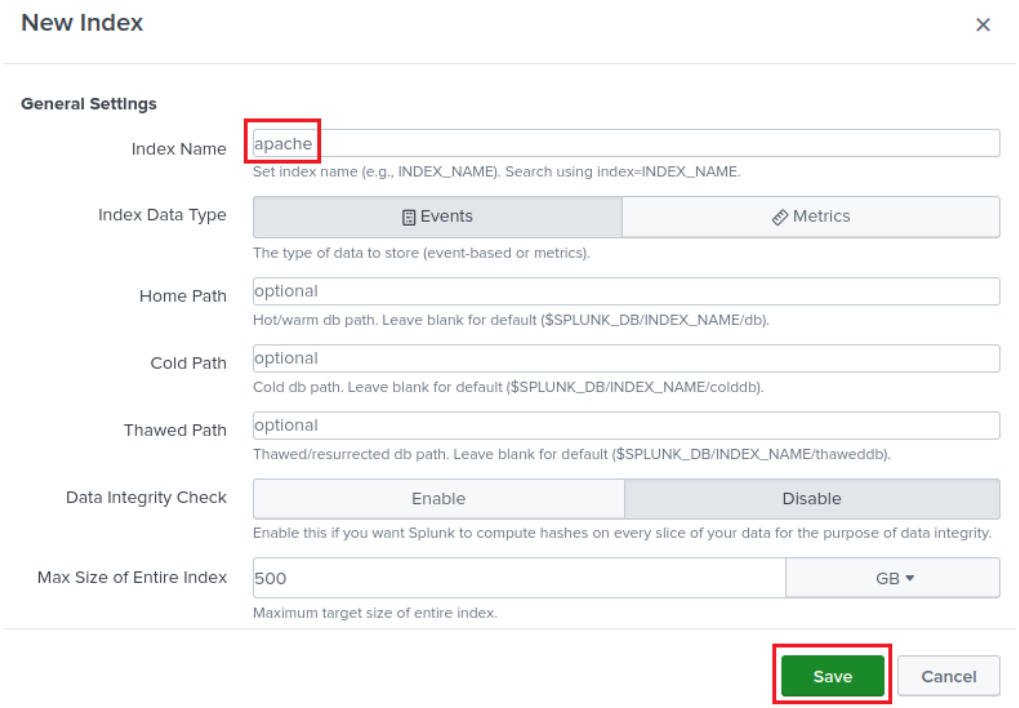
First, we will create an index for access logs from XAMPP. We can do this in Setting > Indexes



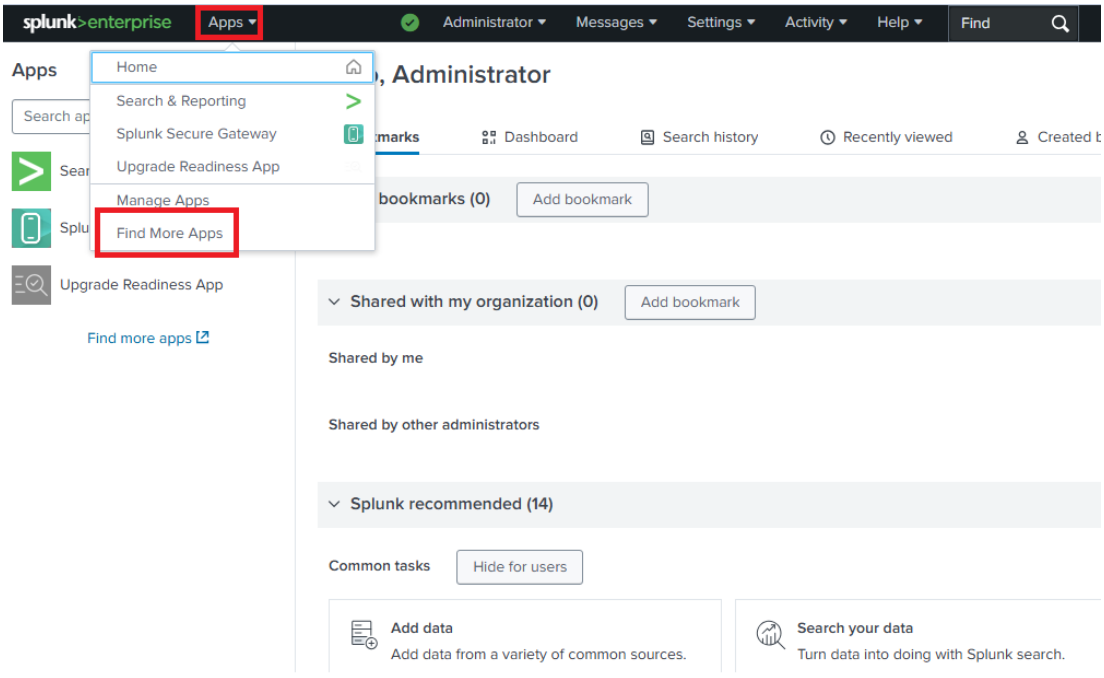
Click on "New Index"



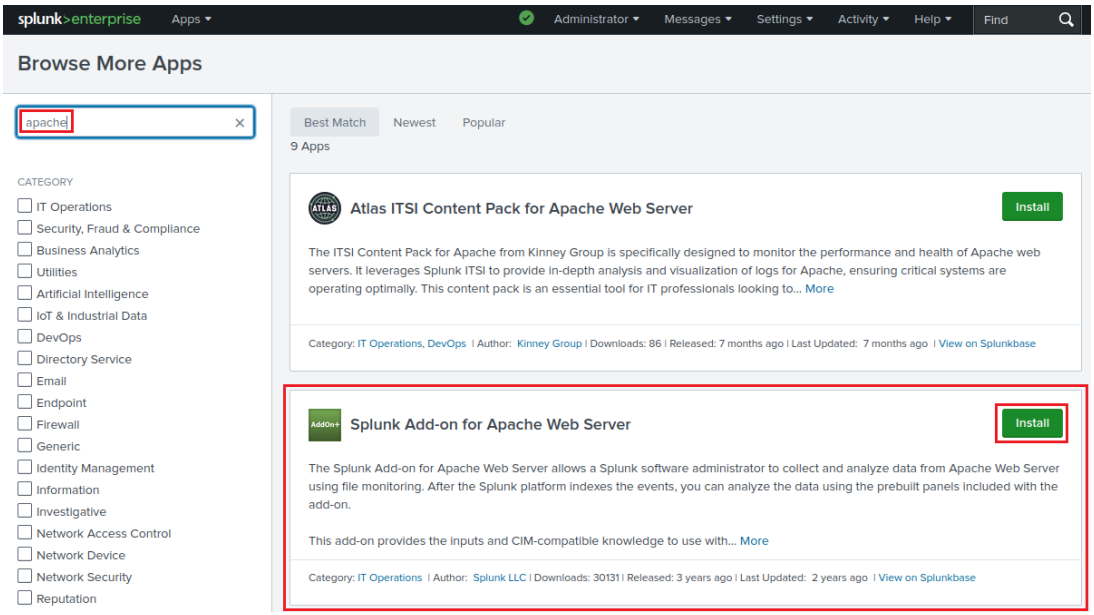
Name the index “apache” and save the new index.



Now, we will download an App to parse the access logs. Go to **Apps > Find More Apps**



Search for “**apache**” where we will install the App “**Splunk Add-on or Apache Web Server**”



On the Windows machine, we will configure Splunk Universal Forwarder to forward Apache logs to the Splunk Server in the following directory:

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

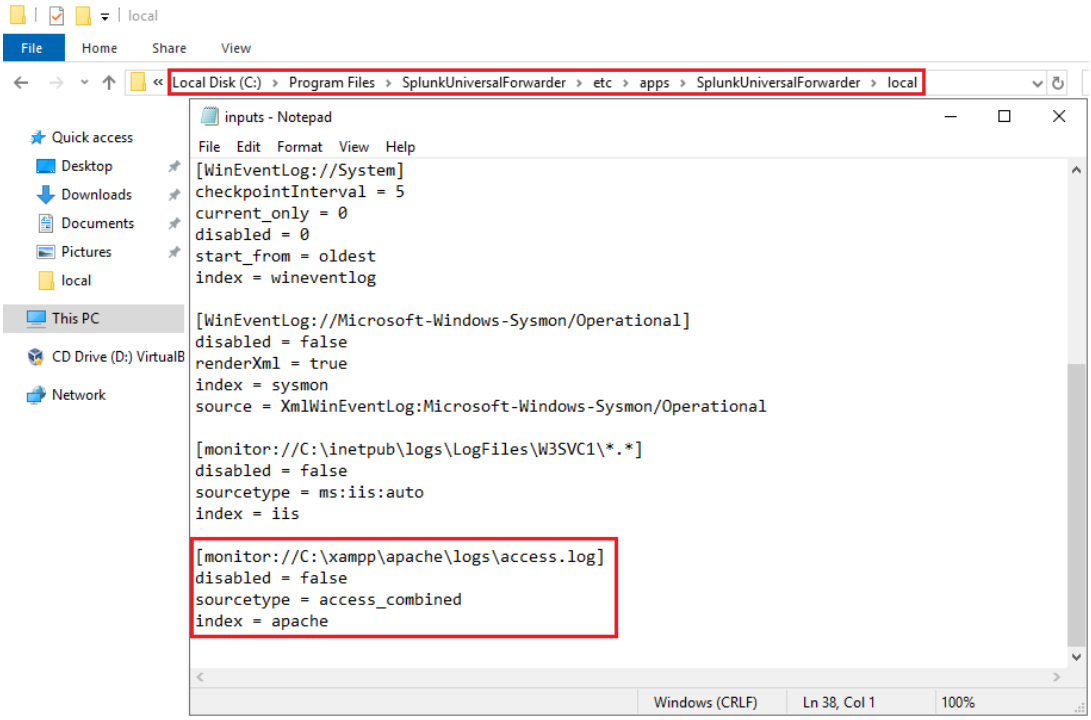
Edit the **inputs.conf** file and add the following:

[monitor://C:\xampp\apache\logs\access.log]

disabled = false

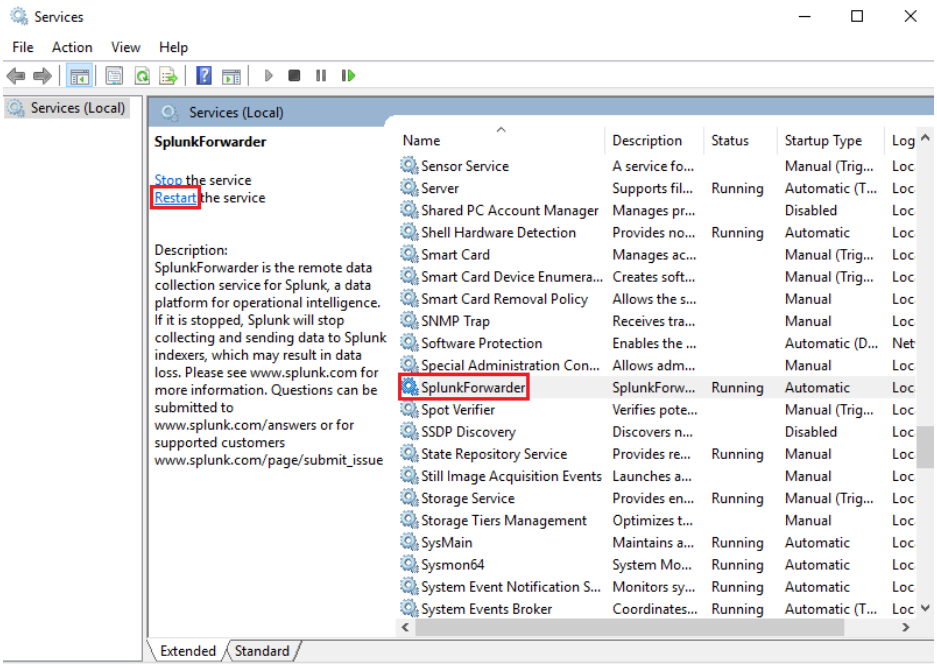
sourcetype = access_combined

index = apache

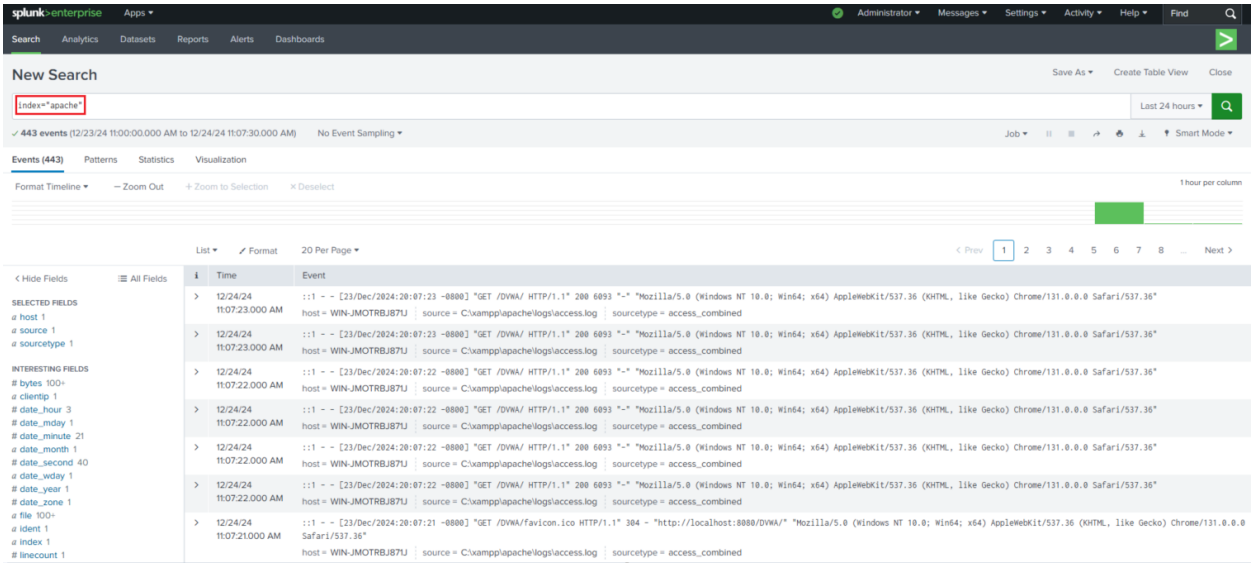


Save the inputs.conf file and then restart the SplunkForwarder service by going to the “Services” app (services.msc).

Find and click on “**SplunkForwarder**” and restart the service

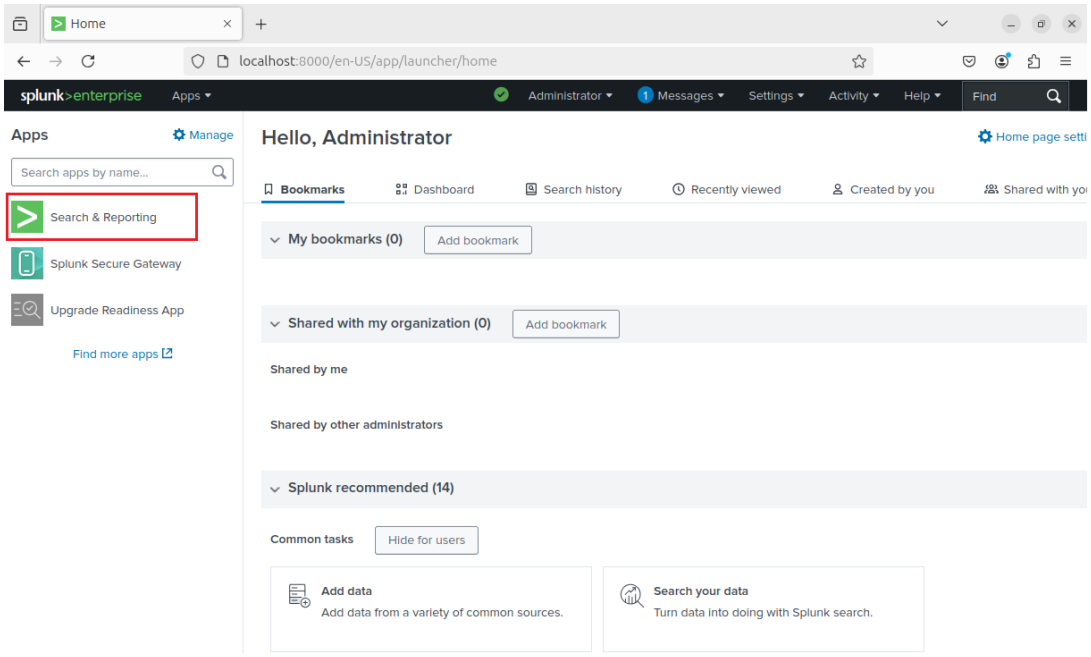


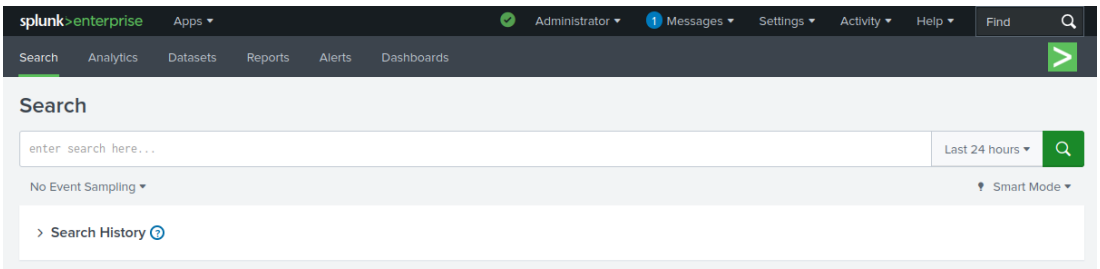
Once SplunkForwarder has been restarted, we can search for apache logs in Splunk with the query “index=apache” where we see



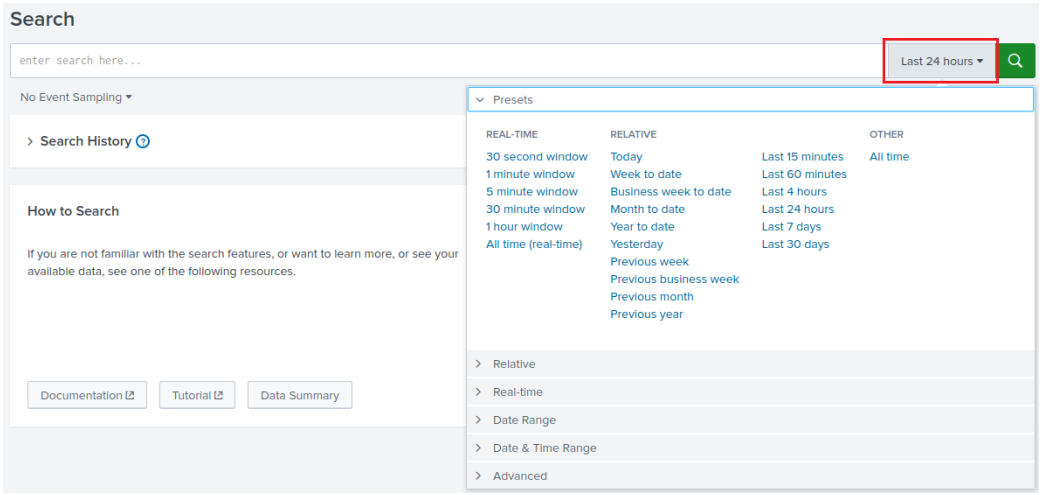
Basic Queries for Splunk

We can use queries to search for specific logs in the “Search & Reporting” page.



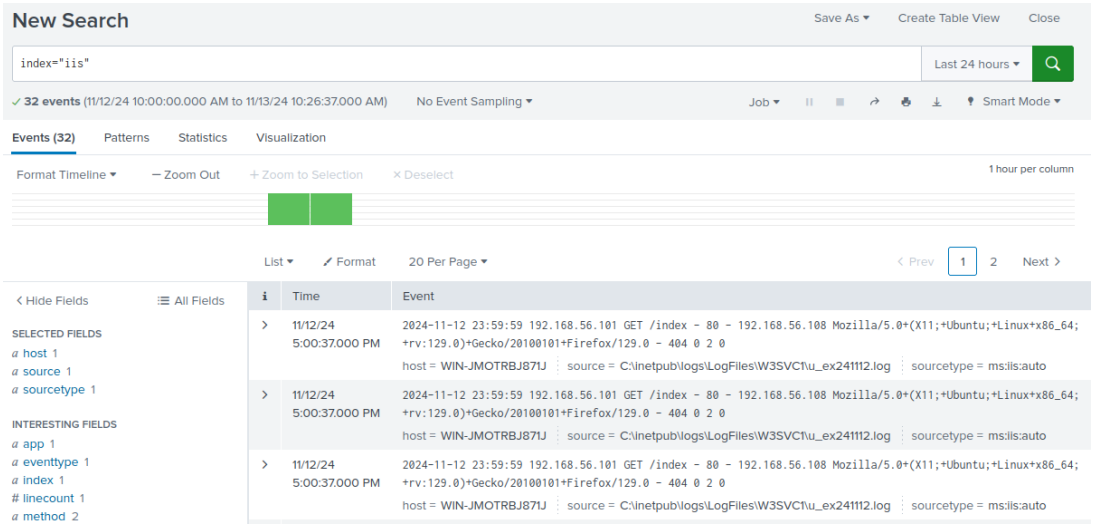


We can add our search queries in the Search bar. We can also filter the logs based on date and time with the presets or with a custom range below.

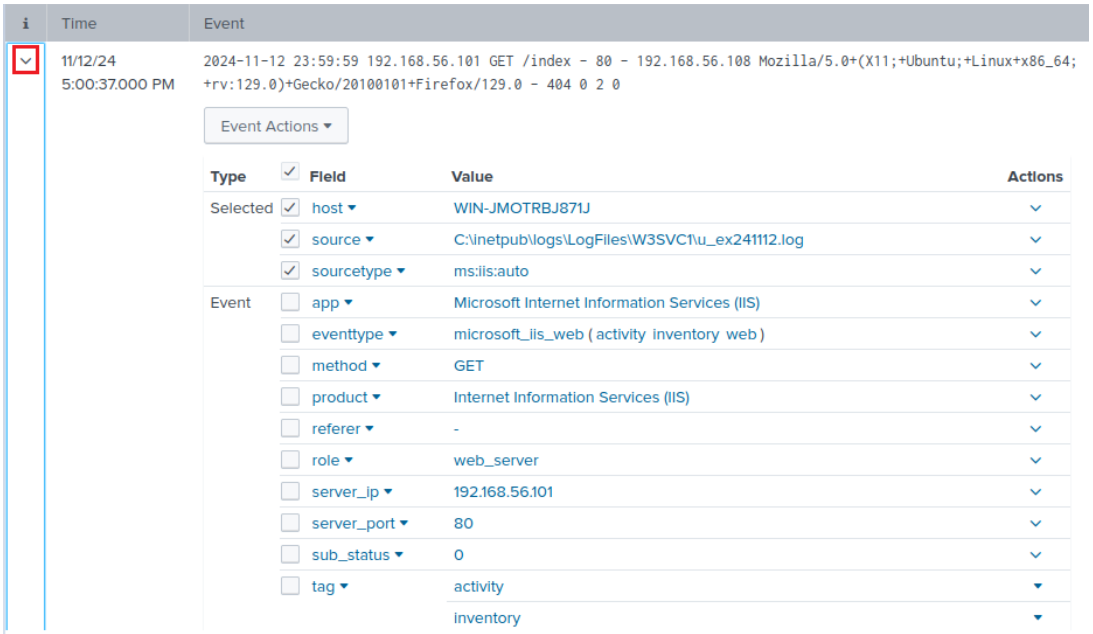


Retrieving Events

Previously, we have tried using the query **index=*** which includes events from all available indexes. This is because the * is a wildcard, so it simply means, any value. If we use the query **index="iis"** then it will filter all the events so that only events from the "iis" index shows.



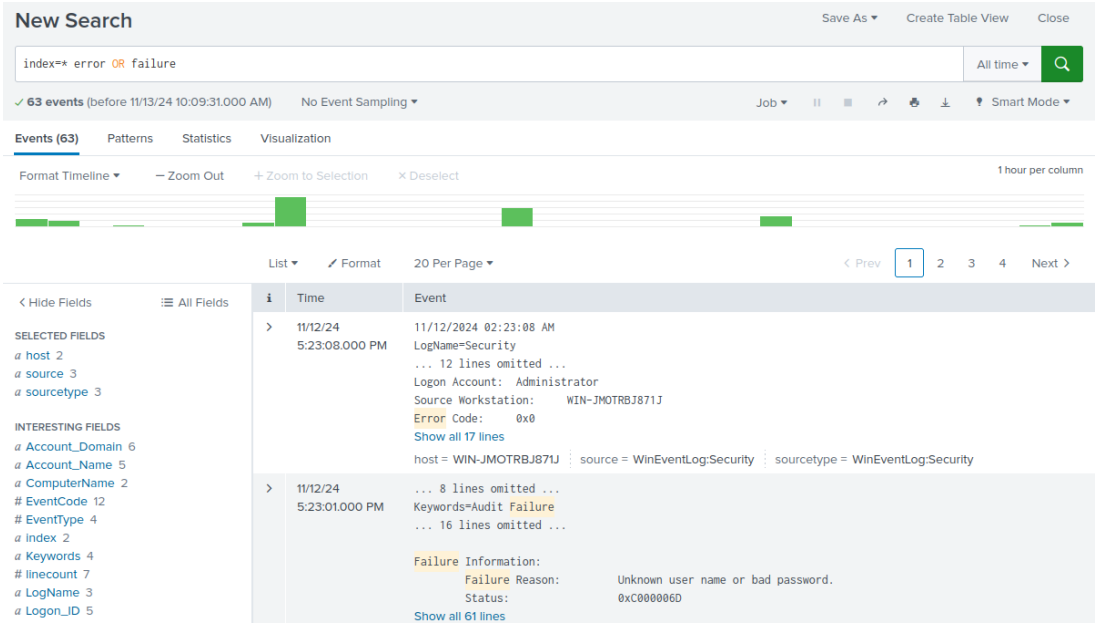
We can click the drop-down arrow to find more information on the specific log which is also easier to read.



Searching with Keywords

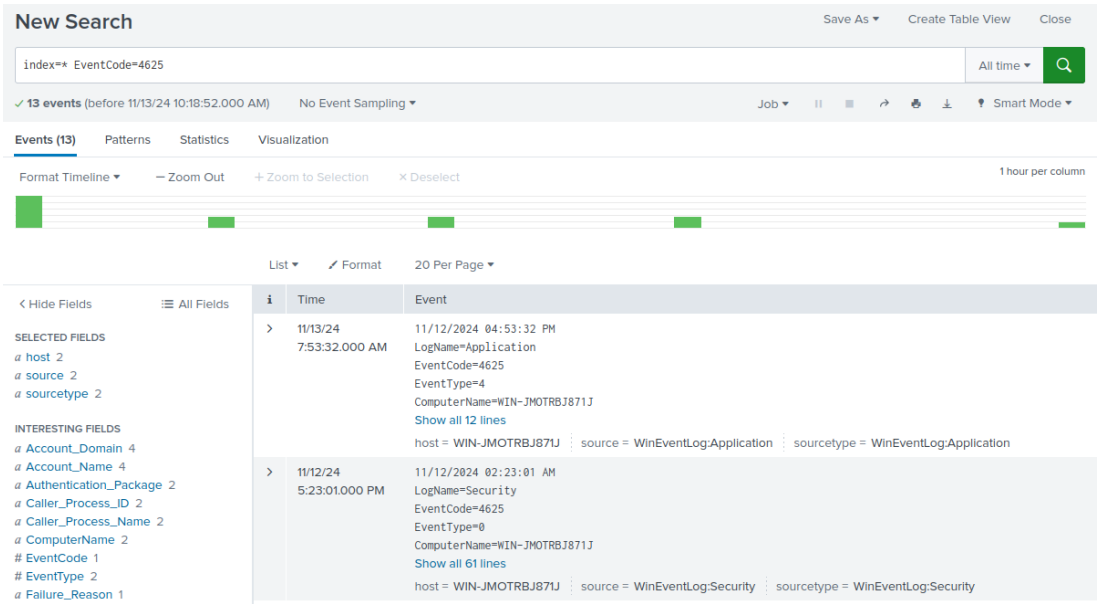
index=* error OR failure

The query above searches for events with specific keywords like “error” or “failure”.



Using Fields

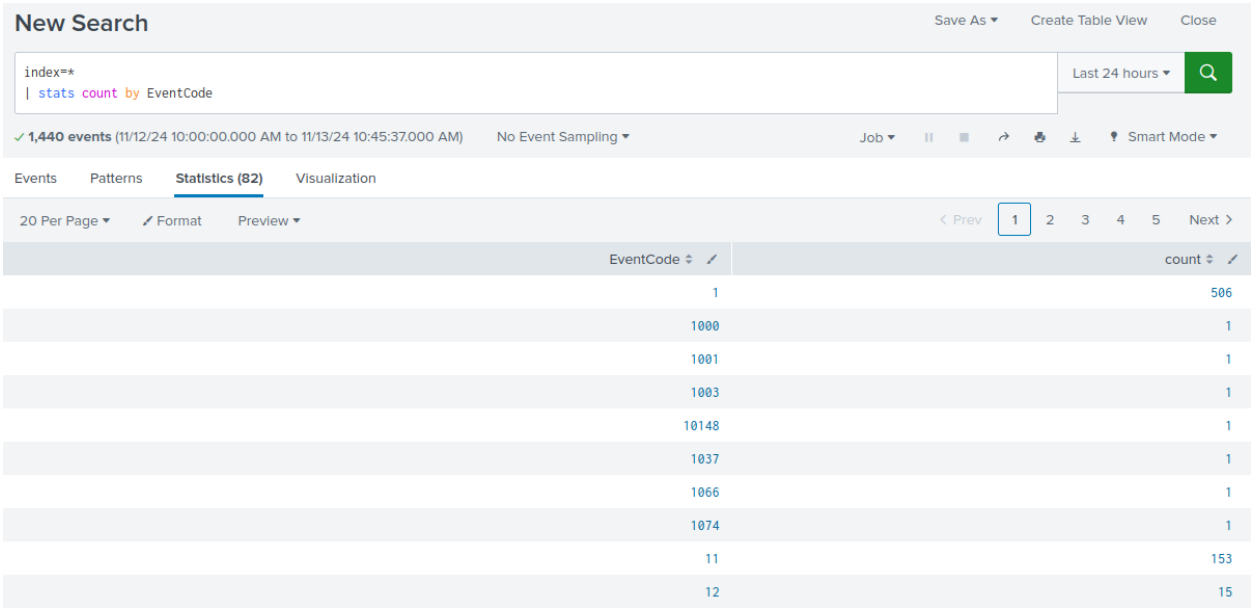
We can search for events with specific field values. For example, a Windows Security Log Event ID 4625 means an account failed to log on. So, if we were to use it in our query, we would use the field “EventCode”. So, our query would look like **index=* EventCode=4625**



Stats for Aggregation

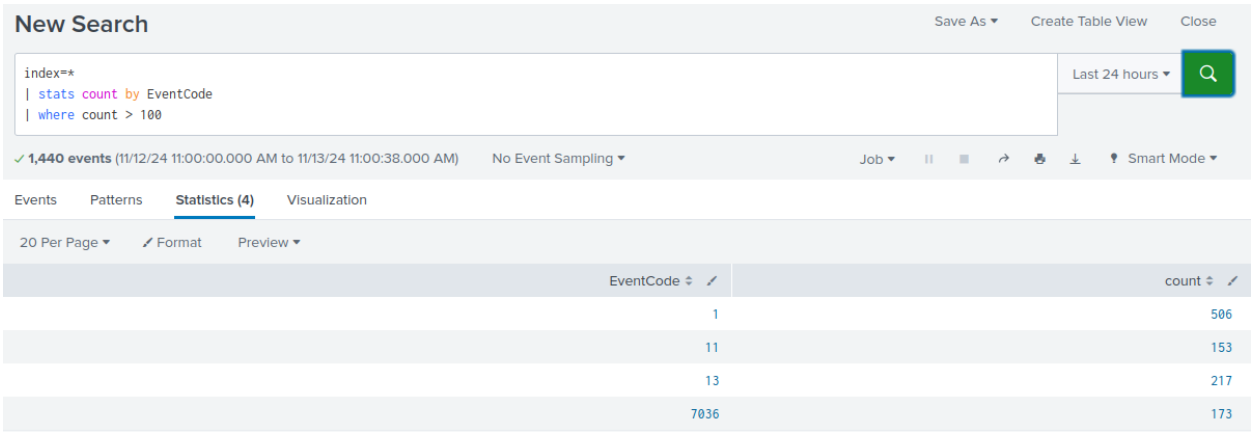
“stats” is a command used to aggregate and summarize data. It helps you perform calculations or create summaries based on fields in your data, such as counting events, finding averages, or grouping results.

The query in the screenshot below groups all events by the values in the EventCode field. For each unique value of EventCode, it counts the number of events and displays them in a table.



Where Clause for Filtering

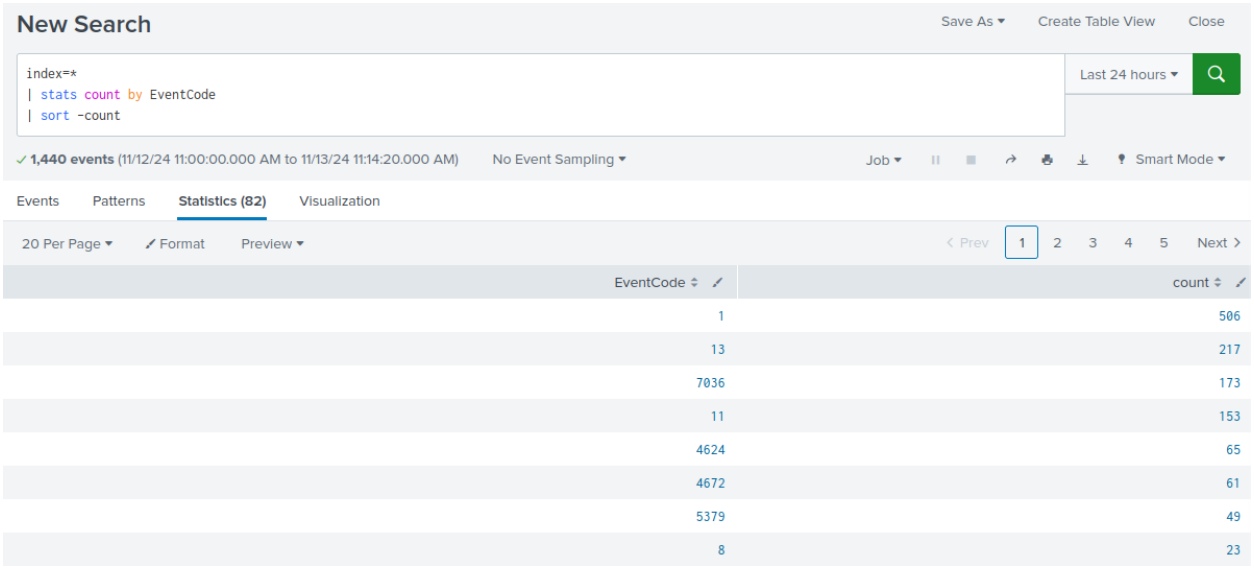
We can filter events with field values that meet specific conditions. Continuing from the previous search, we add **where count > 100**. This searches for EventCodes that has a count of more than 100.



Sorting

The “**sort**” command allows you to sort in ascending or descending order.

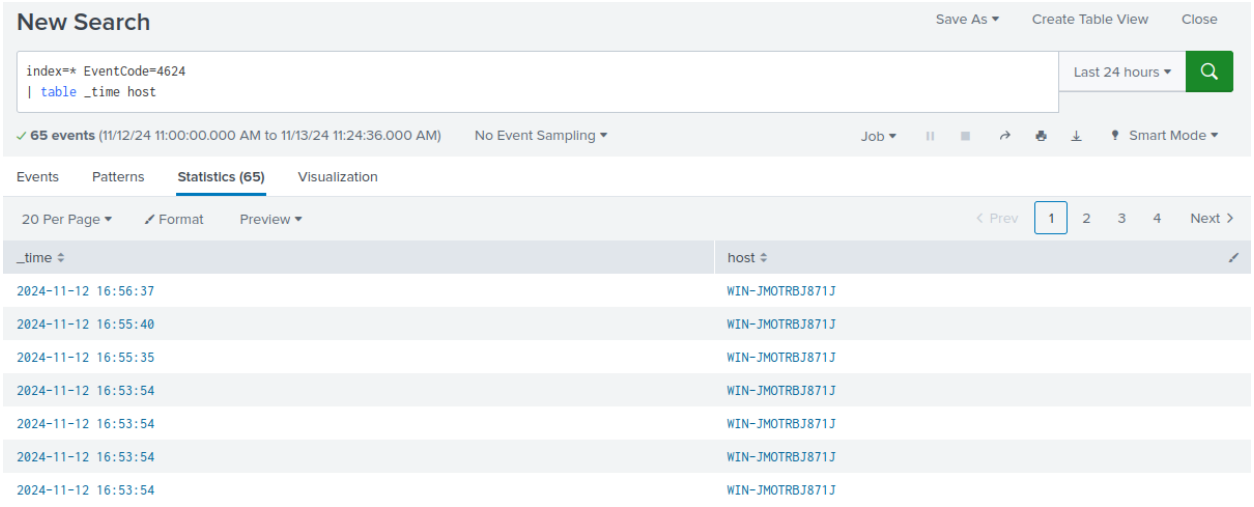
If we want to sort count in ascending order, we use “**sort count**”. Whereas if we want to sort count in descending order, we use “**sort -count**”.



Table

We can use the “**table**” command to display selected fields in a table format.

For example, if we want to find successful logons (EventCode=4624) and only display the time and the host, we can use the command in the screen shot below.



Conclusion

By following this guide, you have successfully set up a Splunk lab environment for centralized log monitoring and management. The lab demonstrates the integration of Splunk Enterprise and Splunk Universal Forwarder to collect, forward, and analyze logs from multiple sources, including Windows IIS, Sysmon, and Apache.