

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

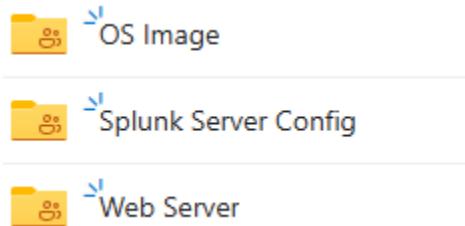
Contents

| | |
|---|----|
| Introduction | 1 |
| Objectives | 1 |
| Table of Contents..... | 2 |
| Files for Setup..... | 3 |
| VirtualBox Installation | 4 |
| Virtual Machine Setup | 7 |
| Ubuntu Setup..... | 7 |
| Splunk Server Setup..... | 16 |
| Splunk Installation..... | 16 |
| Splunk Universal Forwarder Setup..... | 21 |
| Sysmon Integration..... | 21 |
| Splunk Universal Forwarder Installation | 23 |
| Splunk Universal Forwarder Configuration..... | 28 |
| Splunk Universal Forwarder App Installation | 32 |
| Splunk Setup for Apache Logs..... | 40 |
| Basic Queries for Splunk | 45 |
| Conclusion..... | 50 |

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

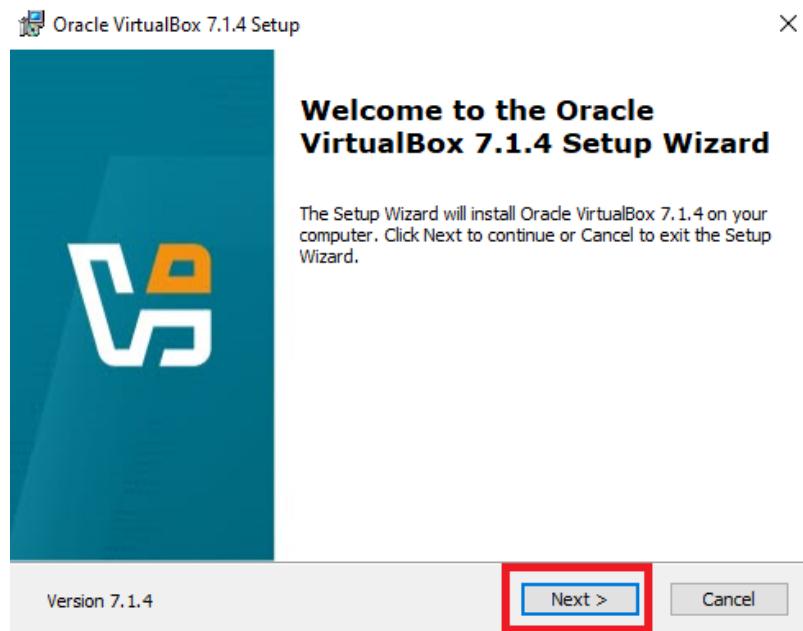
Firstly, we will be downloading VirtualBox, a virtualization software that allows us to run virtual machines on our computers.

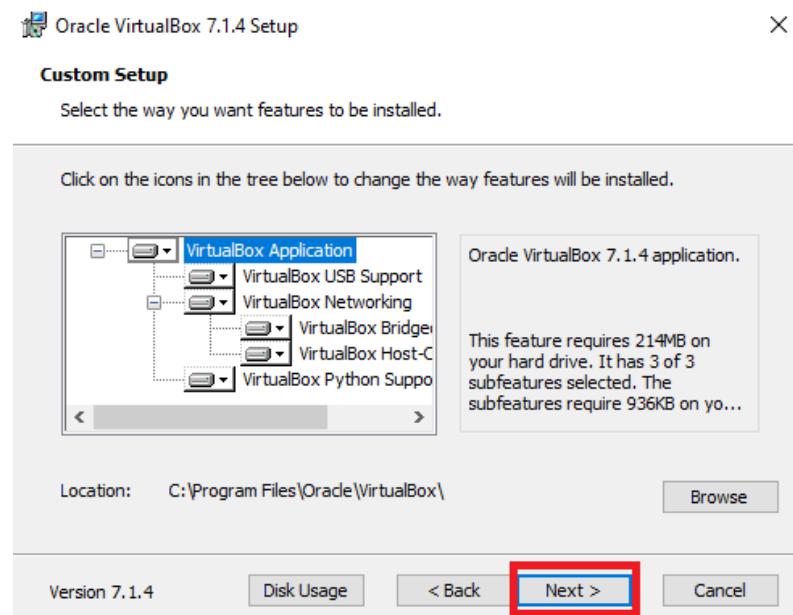
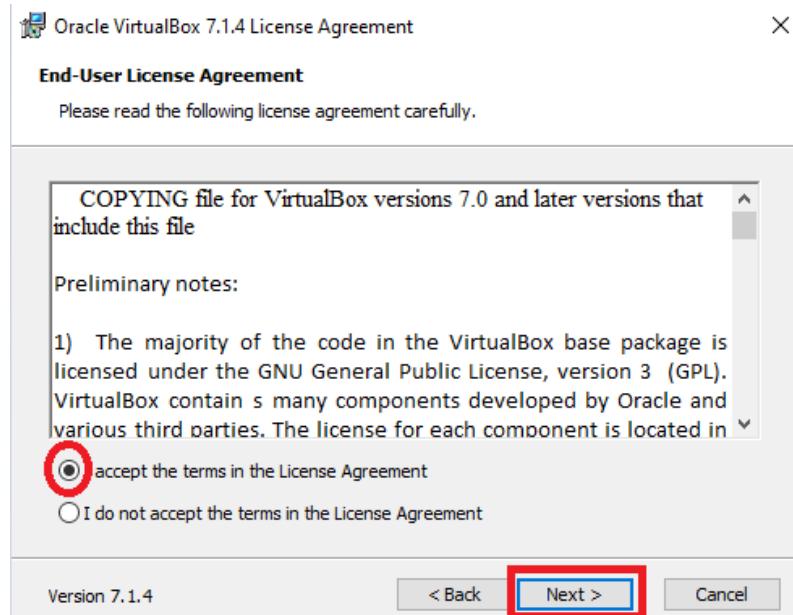
We can download VirtualBox for Windows hosts from the following link:

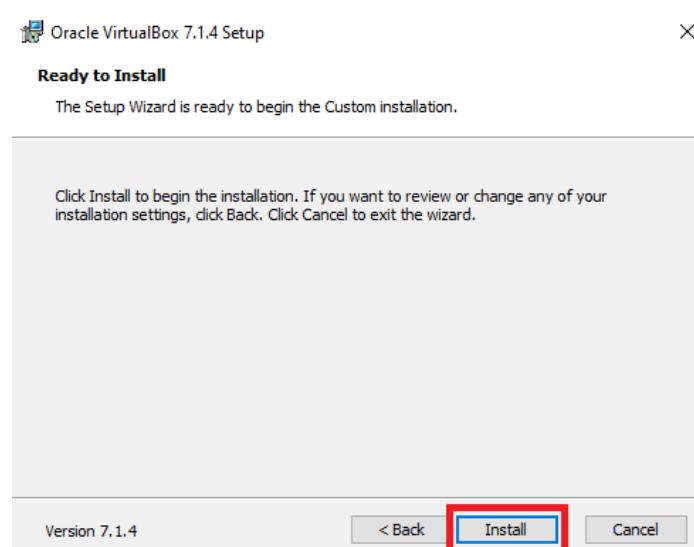
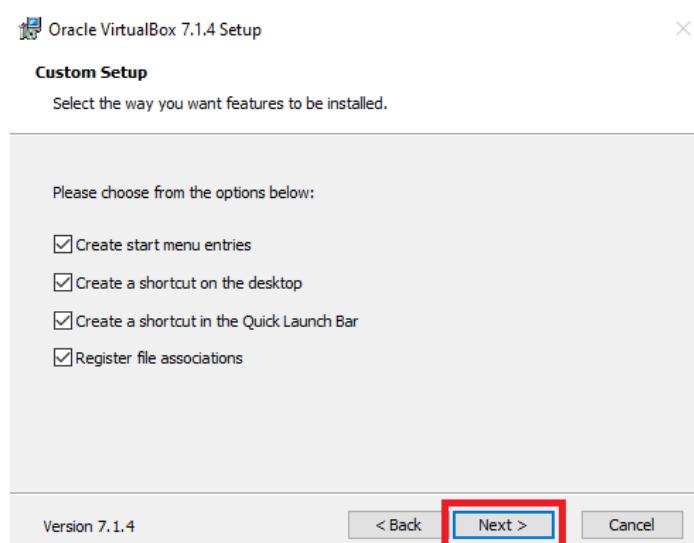
<https://www.virtualbox.org/wiki/Downloads>



Once the file finishes downloading, run it.







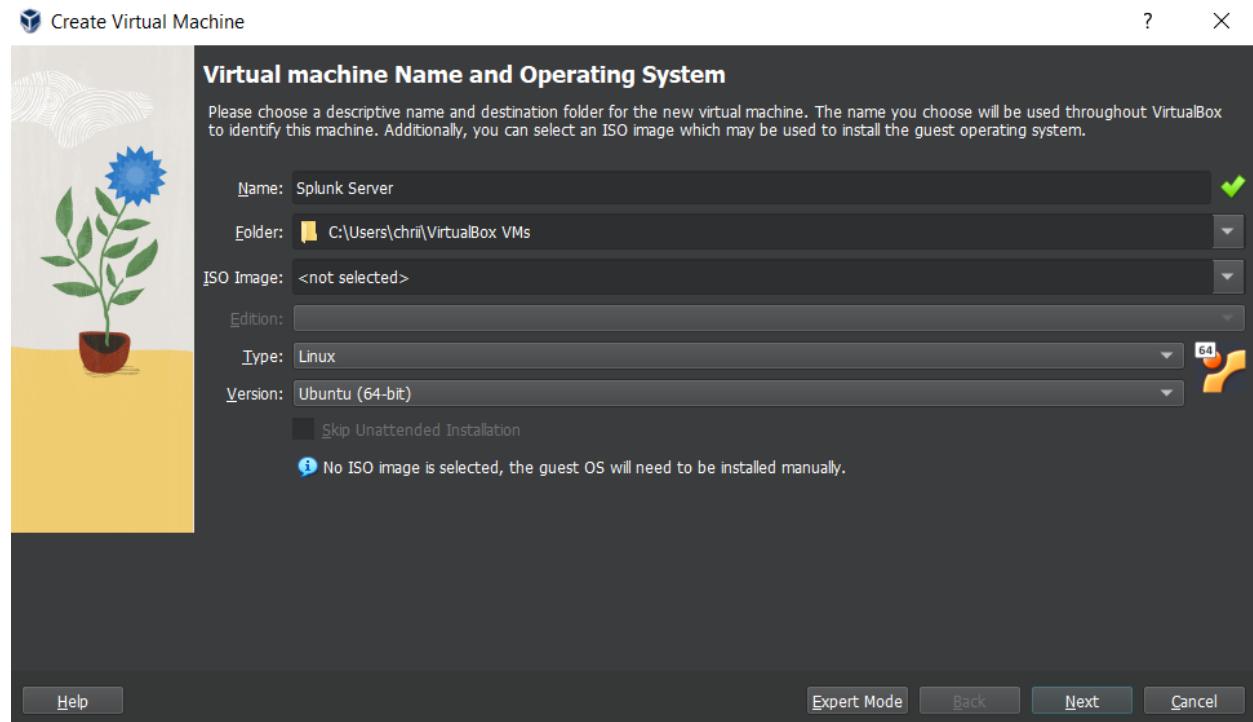
Virtual Machine Setup

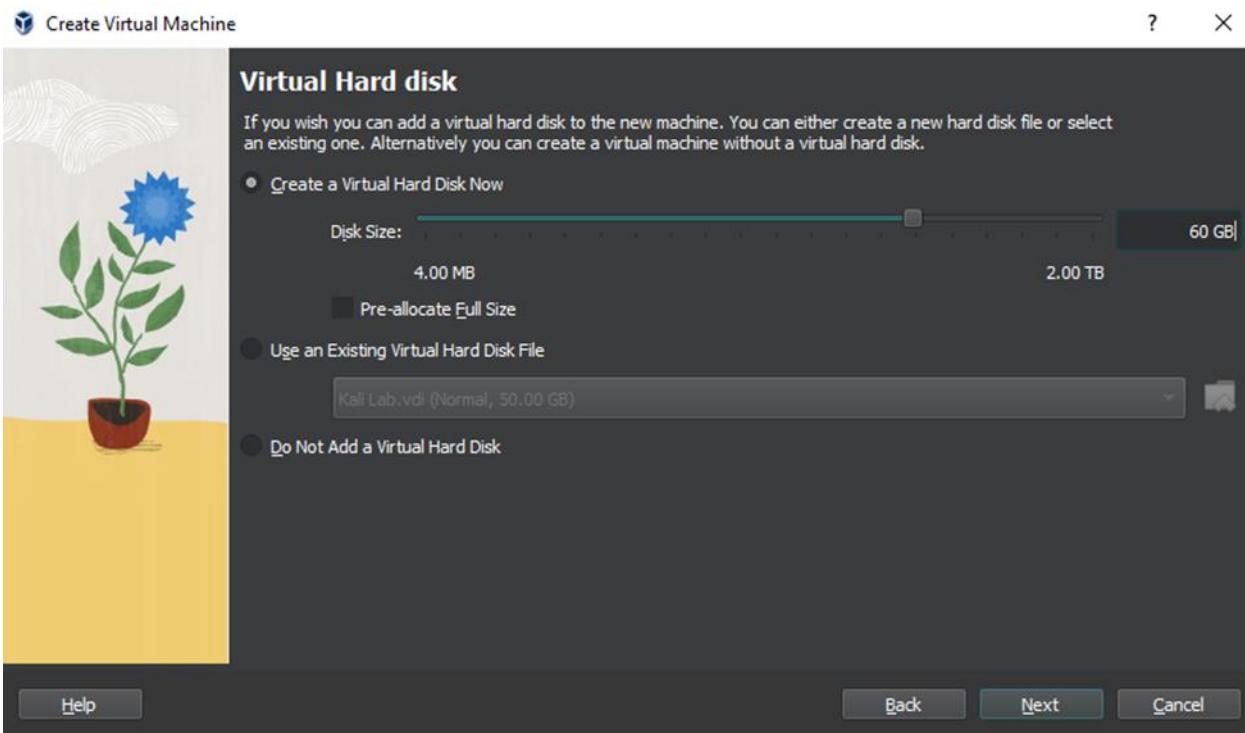
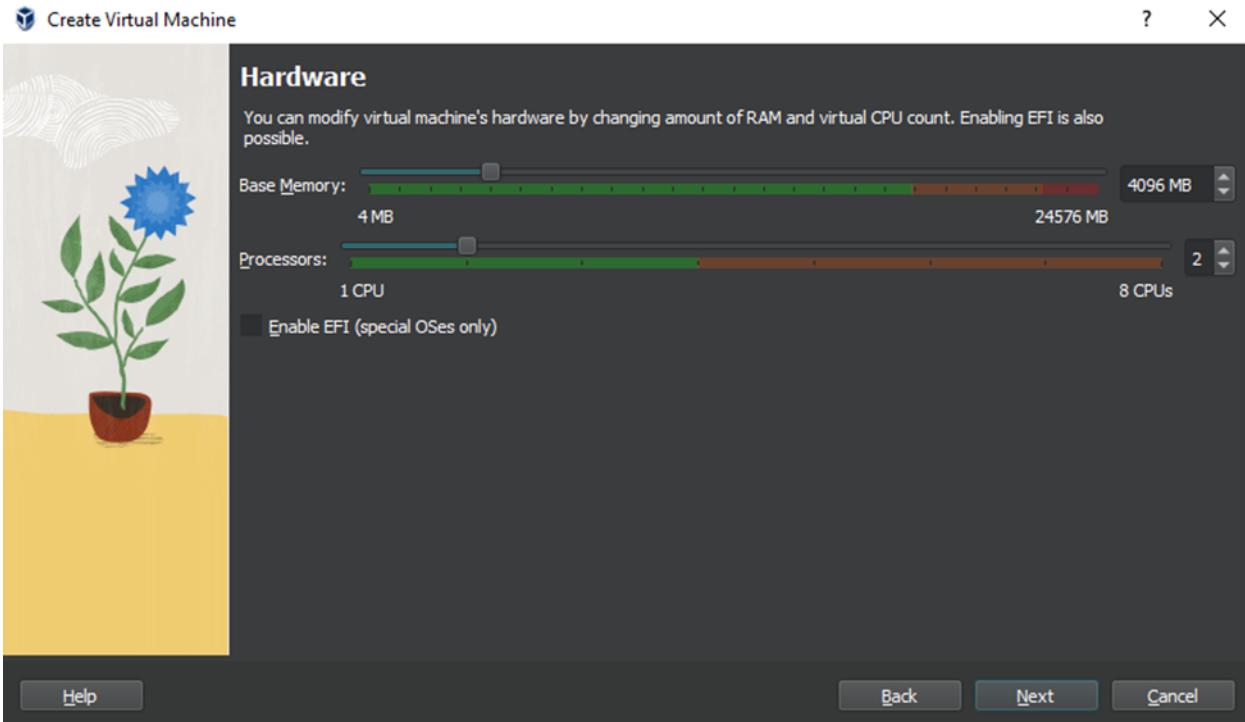
For this lab, we will be using VirtualBox to setup Ubuntu for the Splunk server and Windows for the IIS web server.

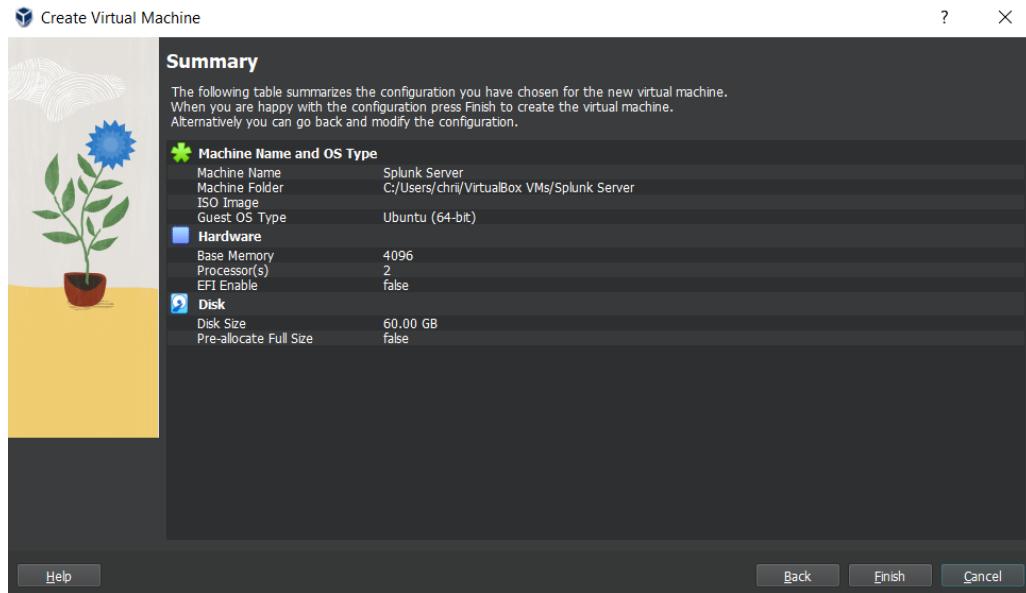
Ubuntu Setup

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.

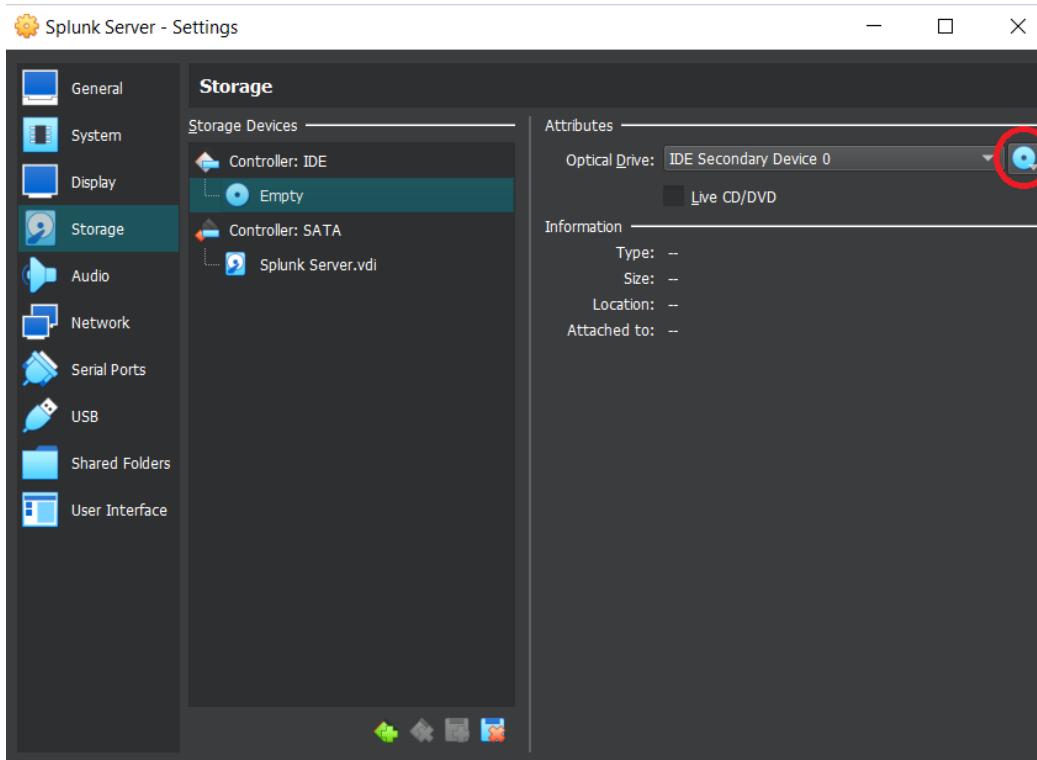






Your summary page should be the same as the picture above.

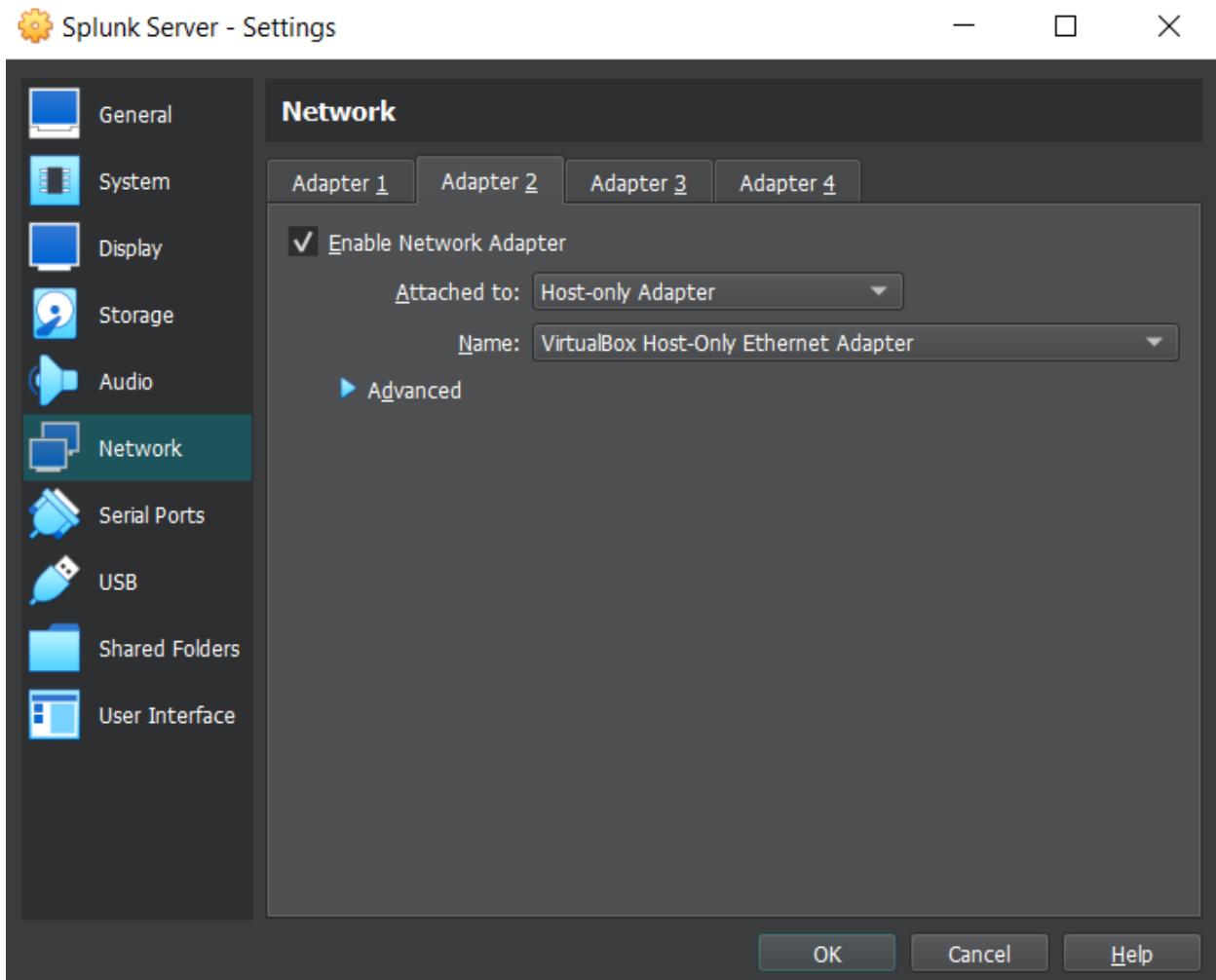
Now we will upload the downloaded Ubuntu ISO file into our VM. Click on the “Splunk Server” VM > Settings > Storage > Empty, and click on the Blue disk on the right > “Choose a disk file...”



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

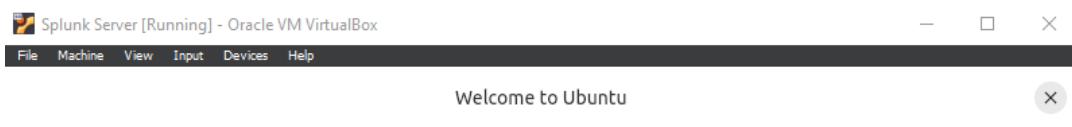
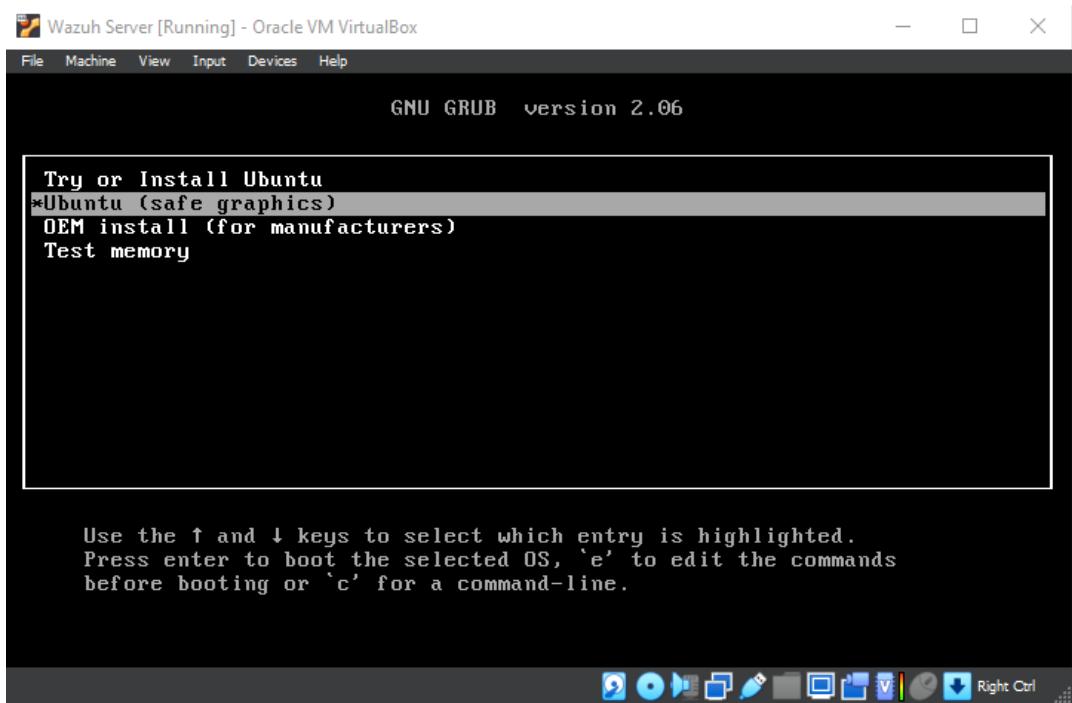
Now, we will have to make a few adjustments for the VM for the setup to run smoothly

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.

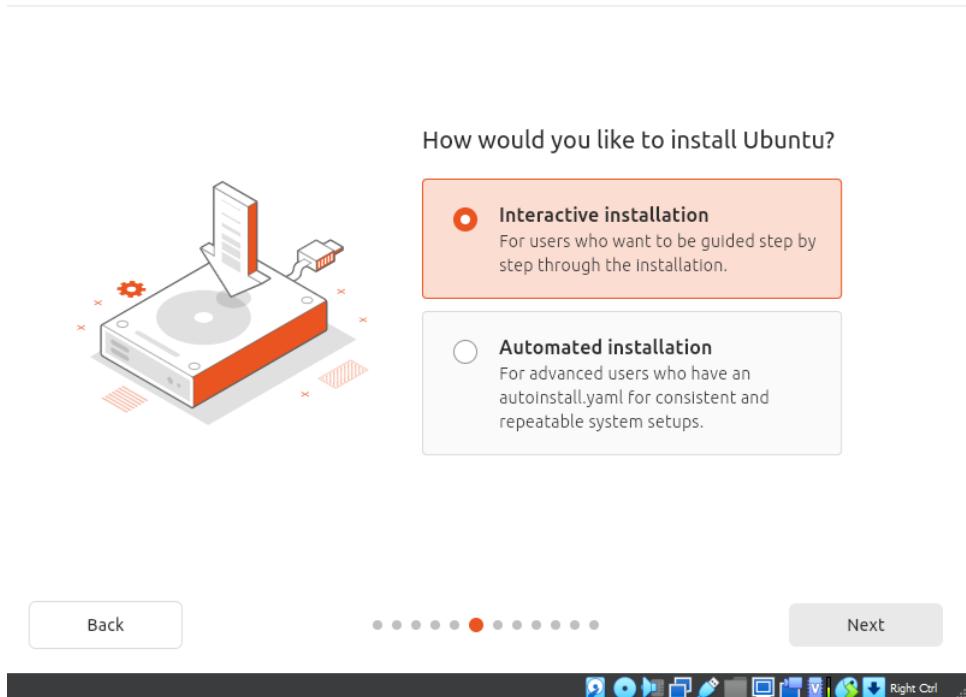
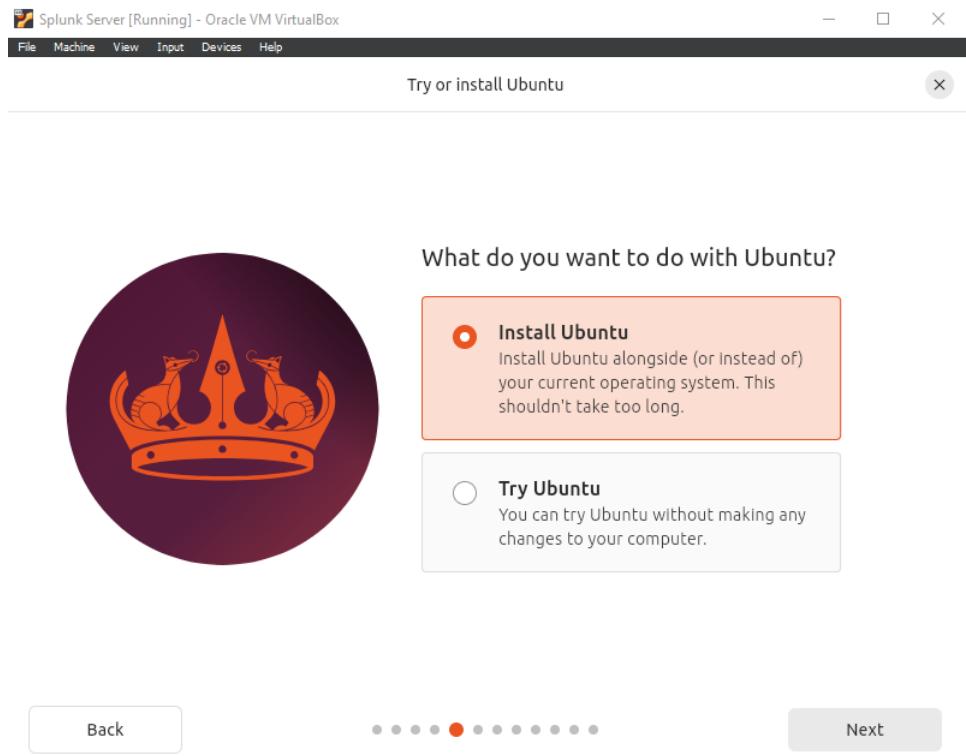


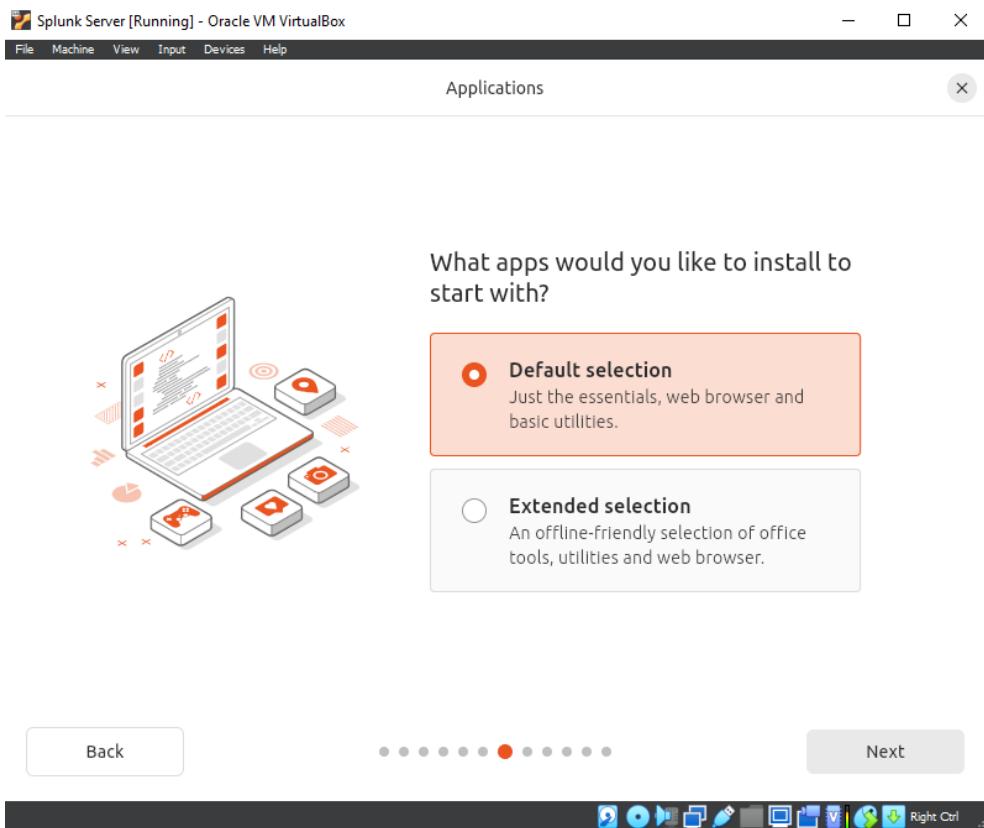
Now, we are ready to start the VM.

Select Ubuntu (Safe graphics)

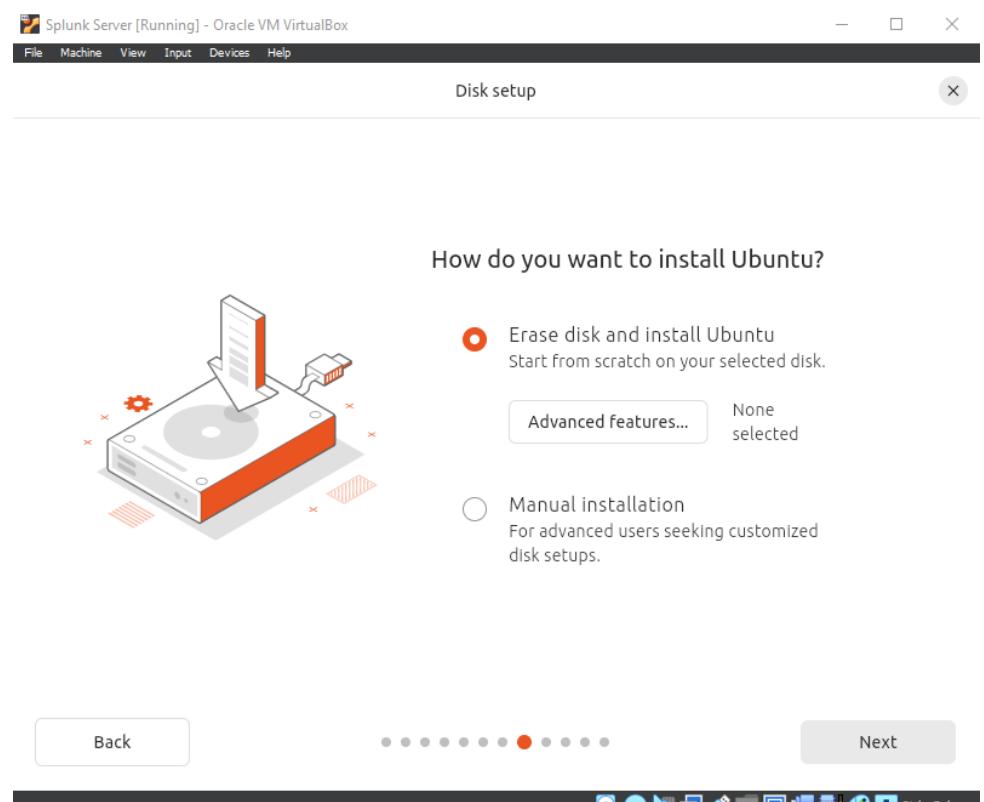


Continue clicking “Next” until you see this page, select “Install Ubuntu” and click Next.

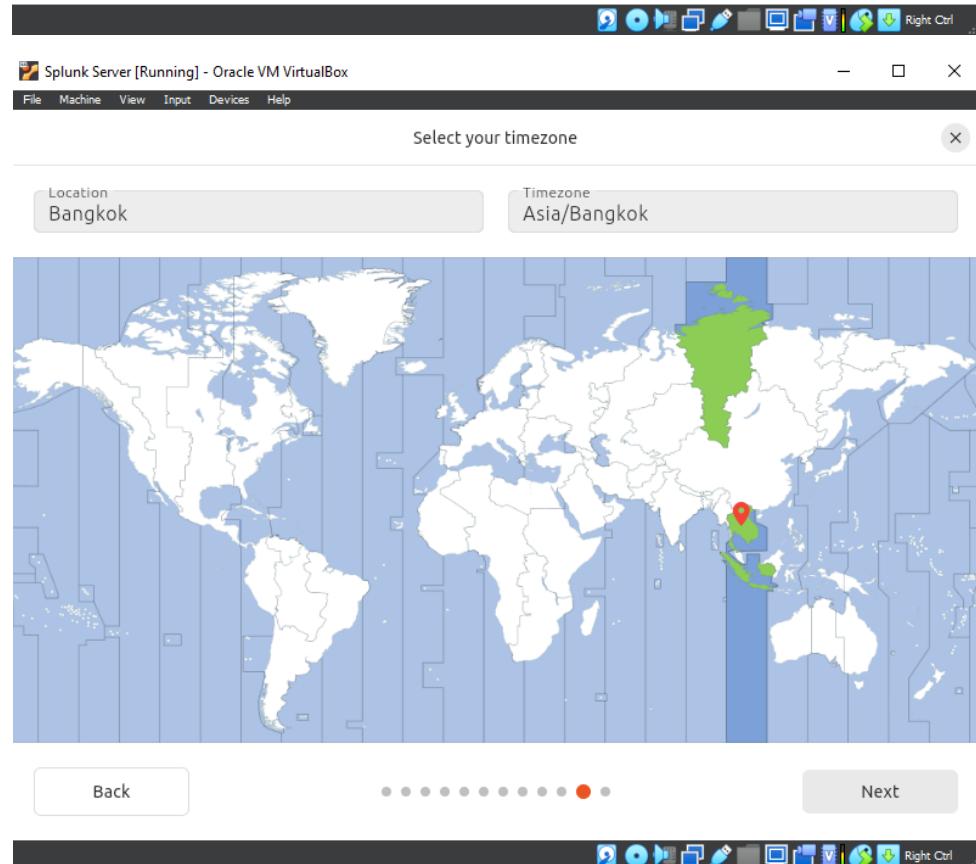
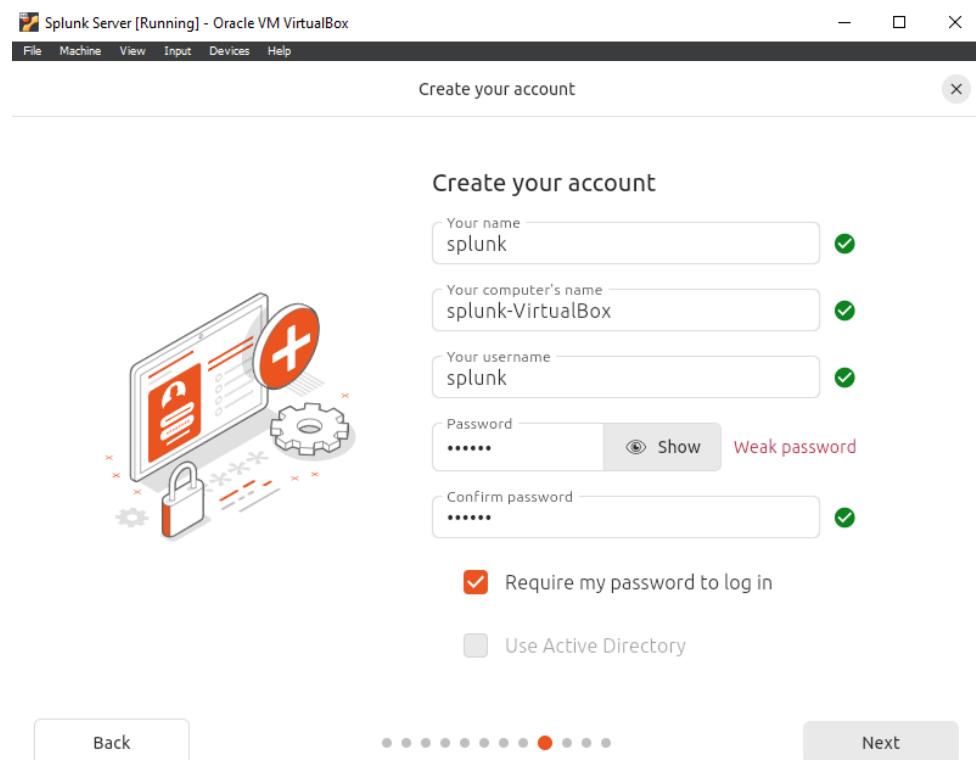




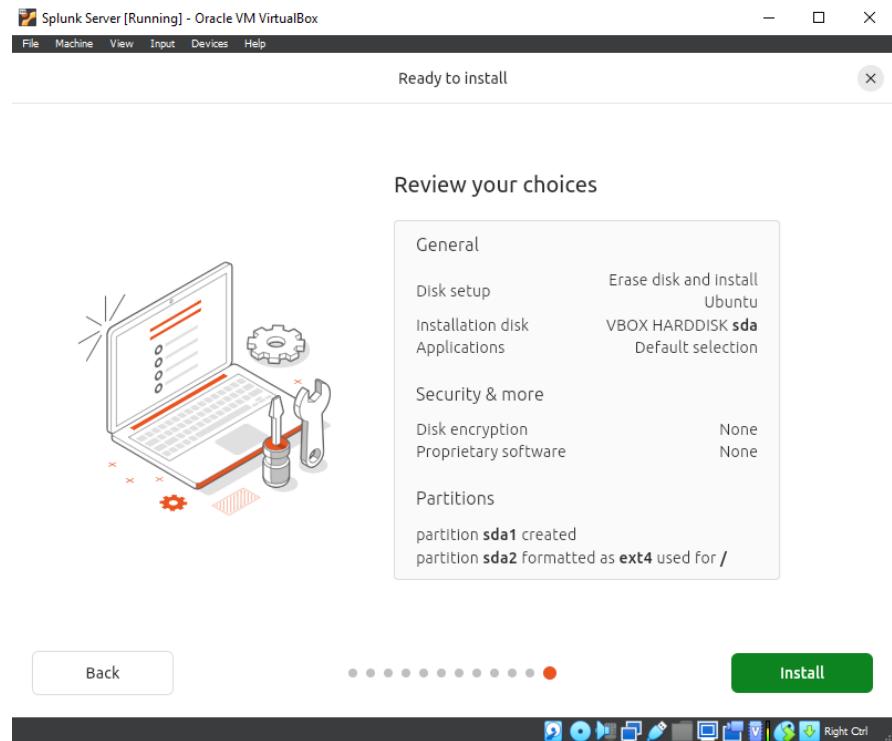
Click Next until you see this page below, and select “Erase disk and install Ubuntu”



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



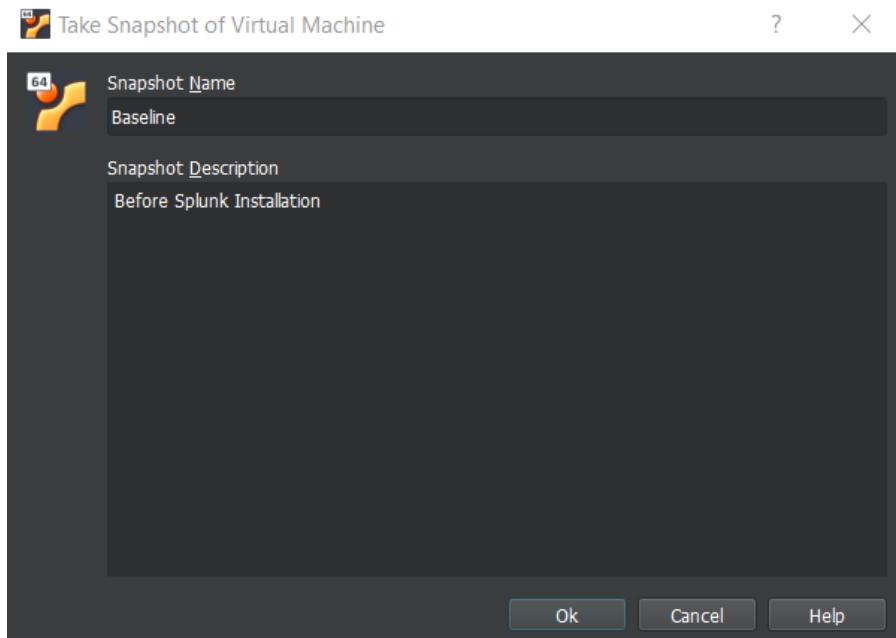
We are now ready to install Ubuntu.



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...

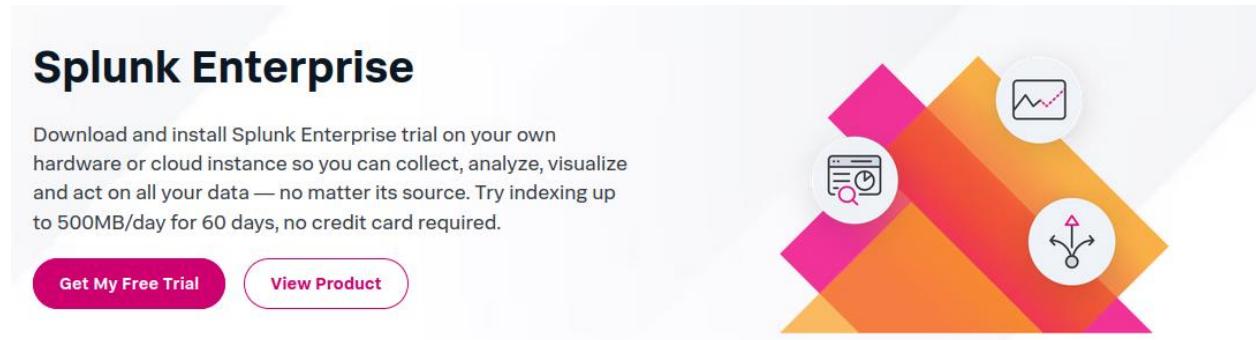


Splunk Server Setup

Splunk Installation

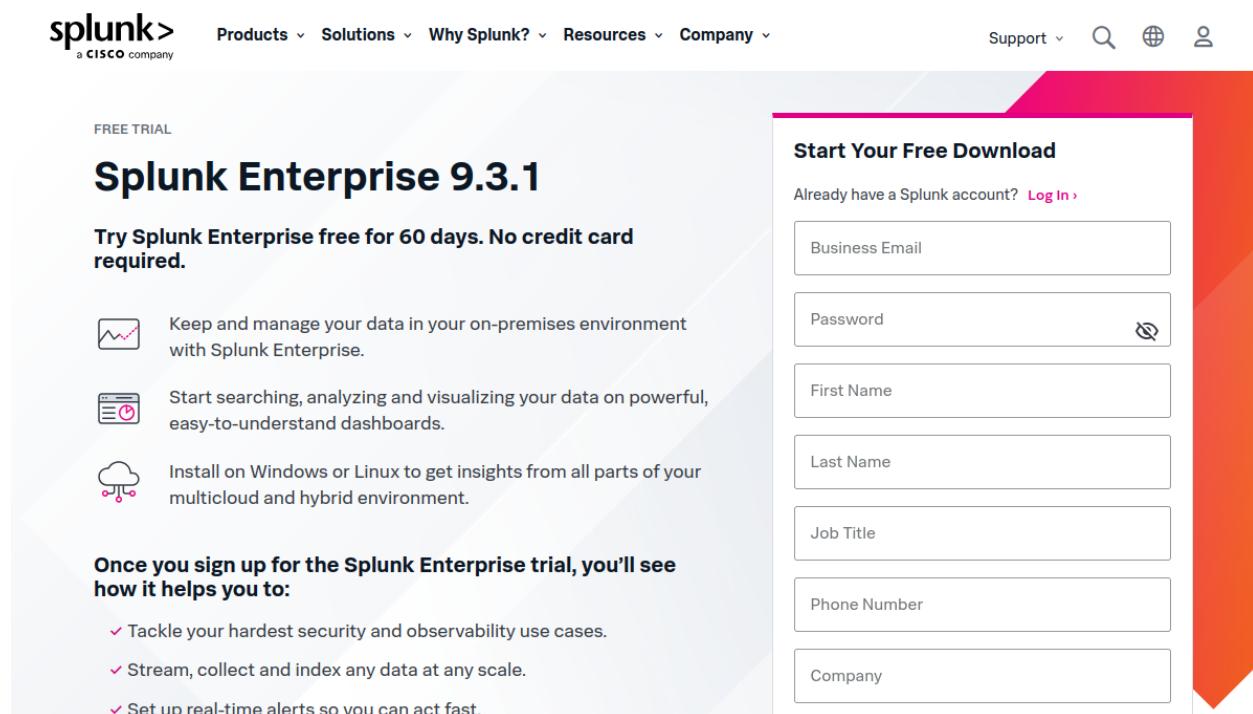
We can download Splunk from this link: https://www.splunk.com/en_us/download.html

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



The image shows the Splunk Enterprise landing page. At the top, it says "Splunk Enterprise". Below that is a description: "Download and install Splunk Enterprise trial on your own hardware or cloud instance so you can collect, analyze, visualize and act on all your data — no matter its source. Try indexing up to 500MB/day for 60 days, no credit card required." There are two buttons: "Get My Free Trial" (in a dark purple box) and "View Product" (in a light blue box). To the right is a graphic featuring three overlapping triangles in pink, orange, and yellow, each containing a white circle with a icon: a graph, a search bar, and a network connection.

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



The image shows the Splunk Enterprise trial sign-up page. At the top, there's a navigation bar with the Splunk logo (a CISCO company), menu items (Products, Solutions, Why Splunk?, Resources, Company), and user options (Support, Log In). Below the navigation is a "FREE TRIAL" button. The main section features the heading "Splunk Enterprise 9.3.1". A callout box says "Try Splunk Enterprise free for 60 days. No credit card required." It lists three benefits with icons: a graph for managing data in an on-premises environment, a search bar for powerful dashboards, and a cloud for multicloud/hybrid environments. Another callout box asks "Once you sign up for the Splunk Enterprise trial, you'll see how it helps you to:" followed by a list of three bullet points: tackling security use cases, streaming data at scale, and setting up real-time alerts. On the right, a large form titled "Start Your Free Download" asks for "Business Email", "Password", "First Name", "Last Name", "Job Title", "Phone Number", and "Company". There's also a link "Already have a Splunk account? Log In".

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

Choose Your Download

Splunk Enterprise 9.3.2

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

| Platform | File Type | Size | Action | More |
|----------|-----------|-----------|------------------------------|--------------------------------|
| Windows | .exe | 947.5 MB | Download Now | Copy wget link |
| Linux | .rpm | 947.5 MB | Download Now | Copy wget link |
| Mac OS | .tgz | 947.75 MB | Download Now | Copy wget link |
| | .deb | 716.43 MB | Download Now | Copy wget link |

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)

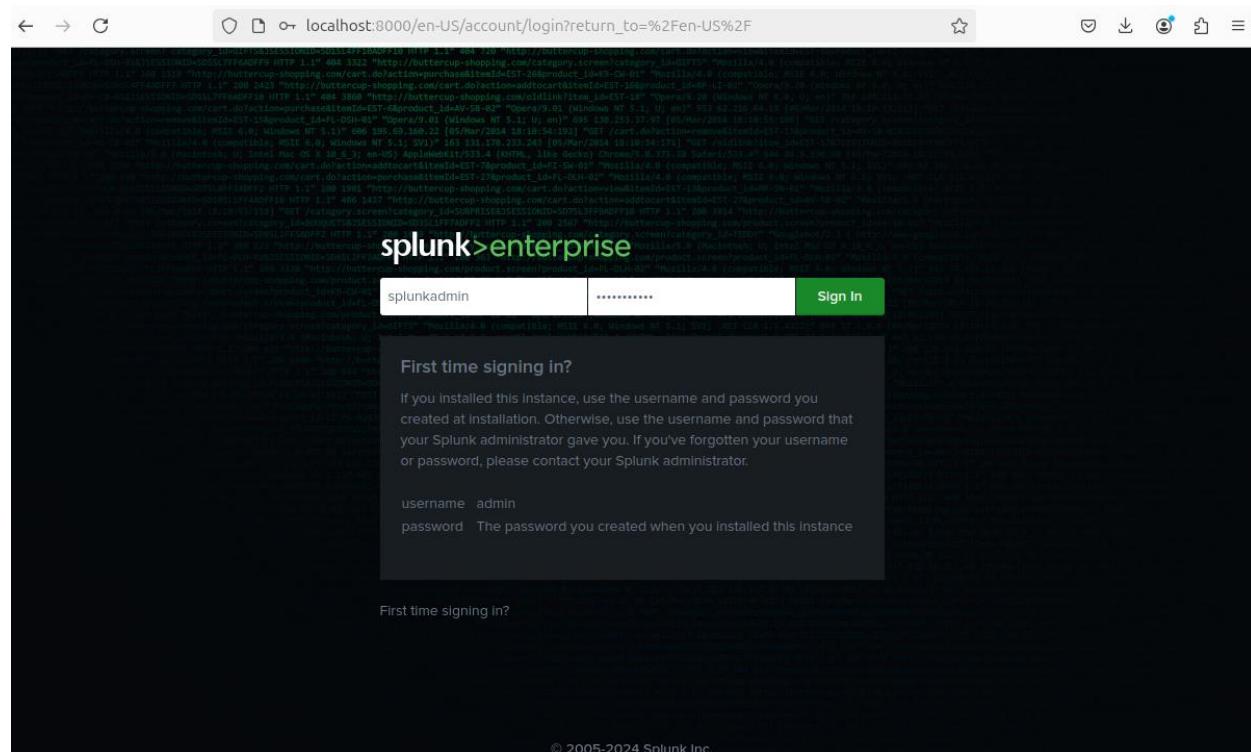
```
Waiting for web server at http://127.0.0.1:8000 to be available..... Done

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

The screenshot shows the Splunk Enterprise main page. At the top, there's a navigation bar with tabs for Home, localhost:8000/en-US/app/launcher/home, and various user and system status indicators. Below the navigation is a search bar and a 'splunk>enterprise' logo. On the left, there's a sidebar titled 'Apps' with a 'Manage' button. The main content area is titled 'Hello, Administrator' and displays a 'Bookmarks' section with categories: 'My bookmarks (0)', 'Shared with my organization (0)', 'Shared by me', and 'Splunk recommended (14)'. Under 'Common tasks', there are two boxes: 'Add data' (with a sub-instruction 'Add data from a variety of common sources.') and 'Search your data' (with a sub-instruction 'Turn data into doing with Splunk search.'). A 'Find' bar at the bottom right includes a magnifying glass icon.

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**

This screenshot is similar to the previous one, showing the Splunk Enterprise main page. However, the 'Settings' menu item in the top navigation bar is highlighted with a red circle. A large callout box is overlaid on the right side of the screen, pointing to the 'DATA' section of the settings menu. Within this section, the 'Forwarding and receiving' link is also circled in red. The callout box lists several other settings categories like 'Data inputs', 'Indexes', 'Report acceleration summaries', etc.

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 |

Add port 9997 and save.

Add new

Forwarding and receiving > Receive data > Add new

Configure receiving

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

Listen on this port * For example, 9997 will receive data on TCP port 9997.

Cancel **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 default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host 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>

Sysmon v15.15

Article • 07/23/2024 • 10 contributors

 Feedback

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)

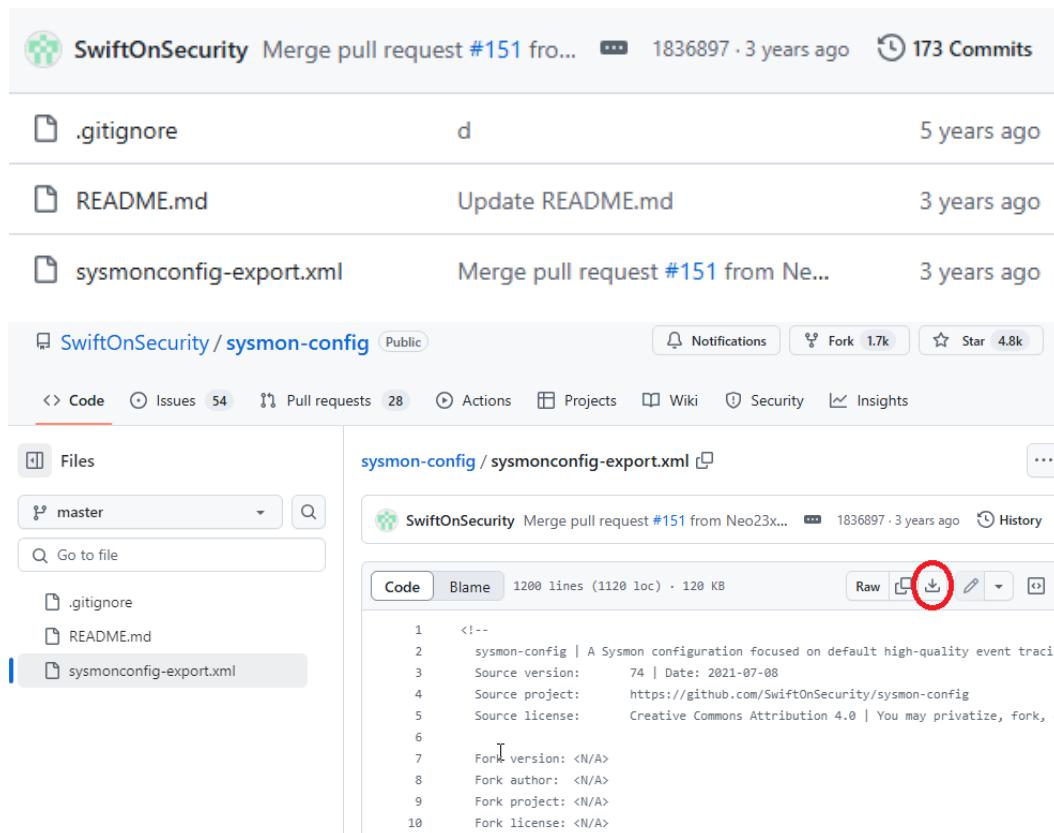
Extract the zip file and we should get this:

| | | | |
|---|--------------------|---------------|----------|
|  Eula | 11/10/2024 8:07 PM | Text Document | 8 KB |
|  Sysmon | 11/10/2024 8:07 PM | Application | 8,282 KB |
|  Sysmon64 | 11/10/2024 8:07 PM | Application | 4,457 KB |
|  Sysmon64a | 11/10/2024 8:07 PM | Application | 4,877 KB |

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



The screenshot shows a GitHub repository page for 'SwiftOnSecurity / sysmon-config'. The repository has 173 commits and 183,689 stars. The 'Code' tab is selected, showing the file structure. On the left, there's a sidebar with a 'Files' section containing '.gitignore', 'README.md', and 'sysmonconfig-export.xml'. On the right, the 'sysmonconfig-export.xml' file is shown in a code viewer. The code content is as follows:

```
1 <!--
2 sysmon-config | A Sysmon configuration focused on default high-quality event tracing
3 Source version: 74 | Date: 2021-07-08
4 Source project: https://github.com/SwiftOnSecurity/sysmon-config
5 Source license: Creative Commons Attribution 4.0 | You may privatize, fork, e
6
7 Fork version: <N/A>
8 Fork author: <N/A>
9 Fork project: <N/A>
10 Fork license: <N/A>
```

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

| | | |
|---|--------------------|--------------|
|  Sysmon | 11/10/2024 8:07 PM | File folder |
|  sysmonconfig-export | 11/10/2024 8:27 PM | XML Document |

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”

```
PS C:\Users\Administrator\Downloads> cd .\Sysmon\
PS C:\Users\Administrator\Downloads\Sysmon> .\sysmon64.exe -accepteula -i .\sysmonconfig-export.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 4.50
Sysmon schema version: 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
PS C:\Users\Administrator\Downloads\Sysmon>
```

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.

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](#)

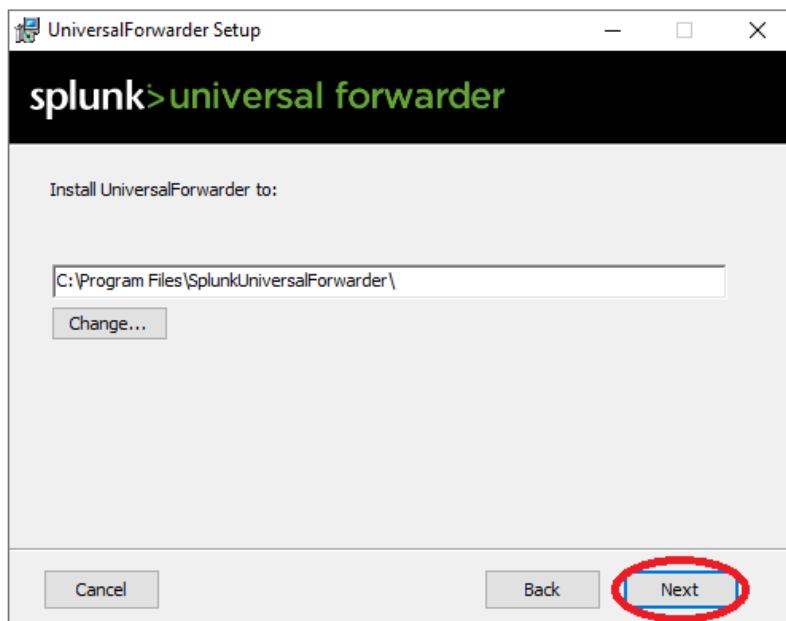
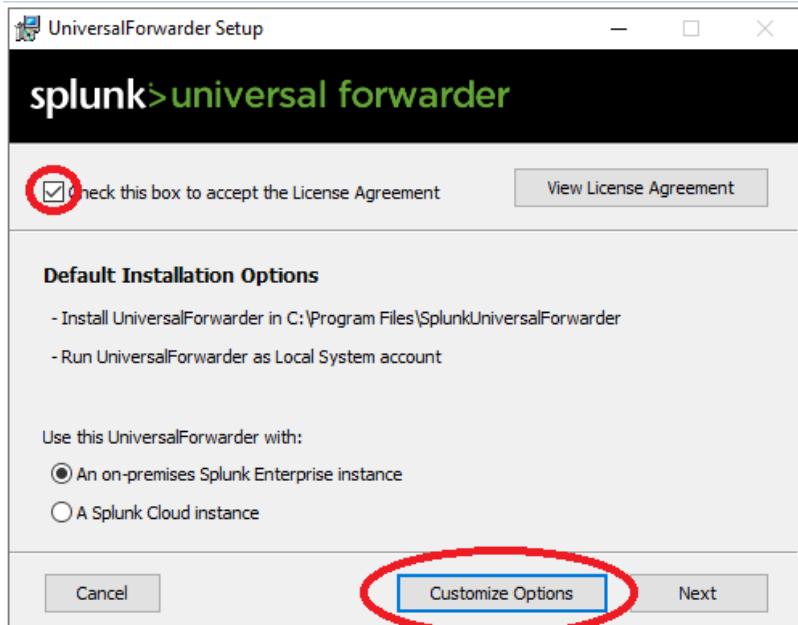
Splunk Universal Forwarder 9.3.2

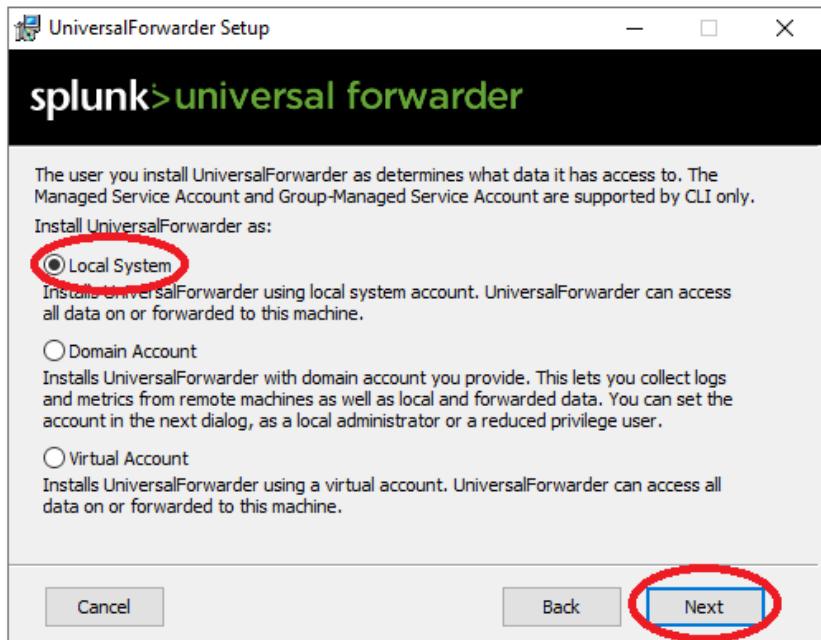
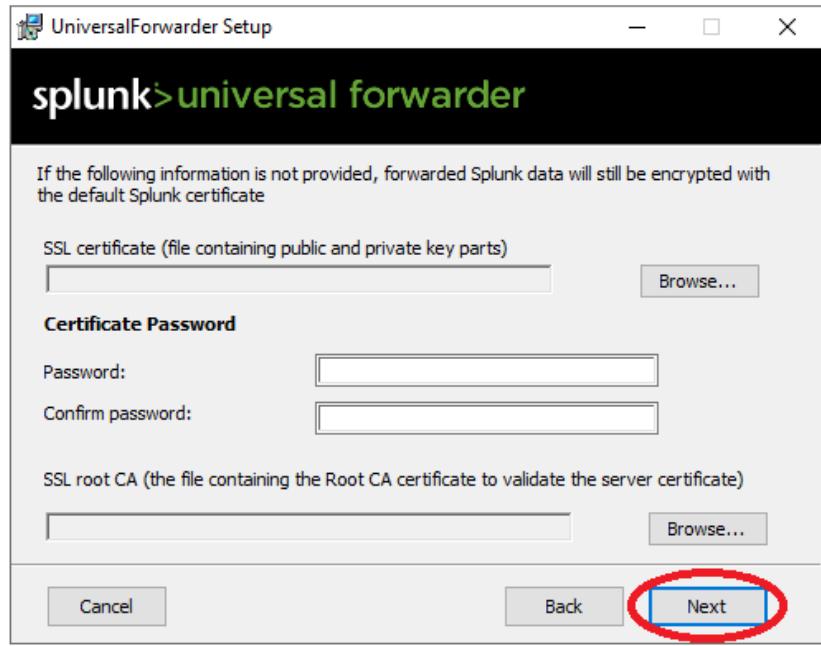
Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

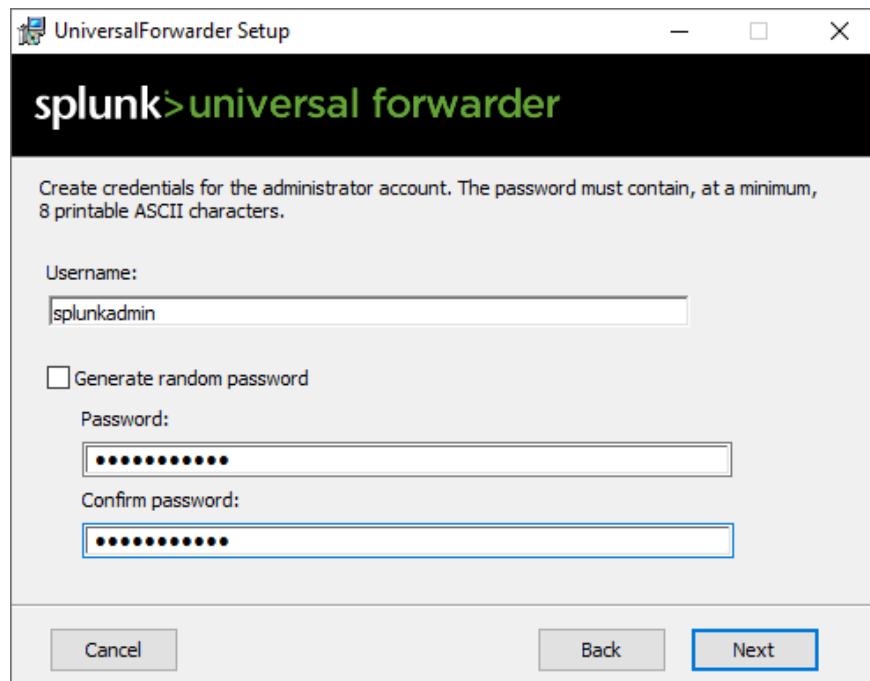
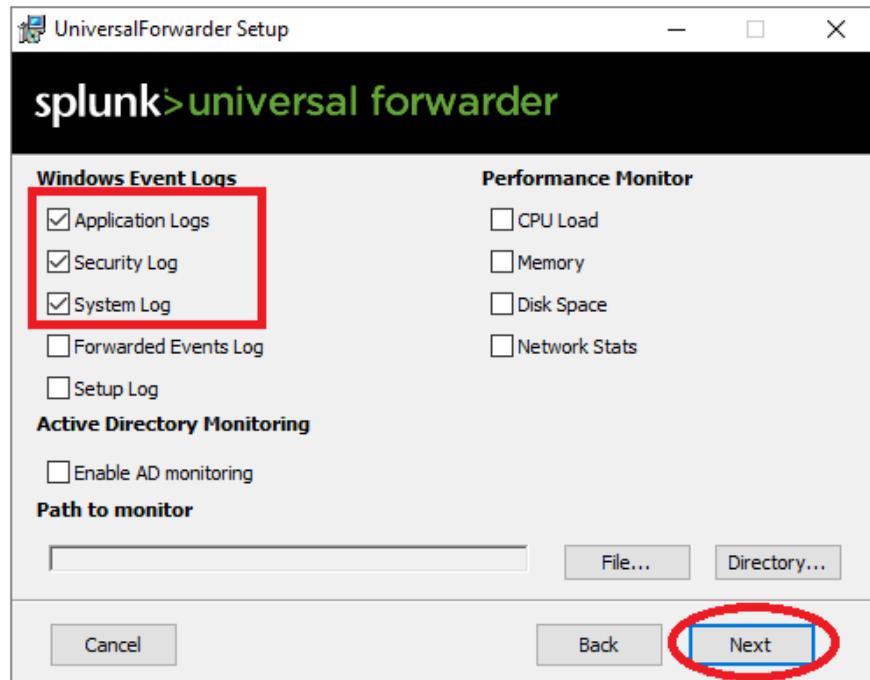
Choose Your Installation Package

| Platform | Version | File Type | Size | Action |
|----------|---|-----------|-----------|------------------------------|
| Windows | Windows 10, 11 Windows Server 2019, 2022 | .msi | 129.53 MB | Download Now |
| Windows | Windows 10 | .msi | 65.0 MB | Download Now |

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







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\SplunkUniversalForwarder\local

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

```
[WinEventLog://Application]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest
index = wineventlog

[WinEventLog://Security]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest
index = wineventlog

[WinEventLog://System]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest
index = wineventlog

[WinEventLog://Microsoft-Windows-Sysmon/Operational]
disabled = false
renderXml = true
index = sysmon
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

[monitor://C:/inetpub/logs/LogFiles/W3SVC1/*.*]
disabled = false
sourcetype = ms:iis:auto
index = iis
```

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

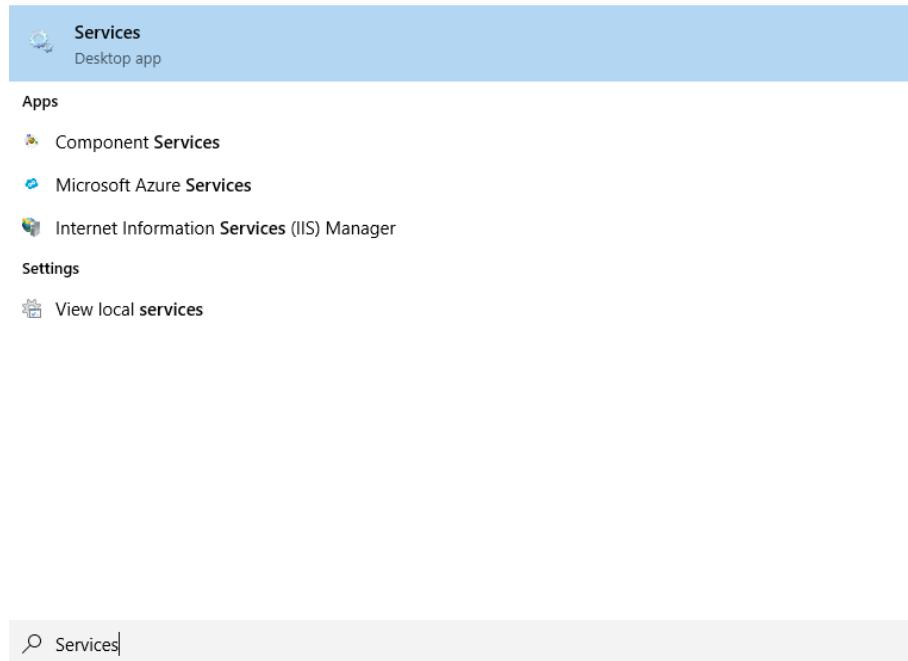
```
[WinEventLog://Microsoft-Windows-Sysmon/Operational]
disabled = false
renderXml = true
index = sysmon
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
```

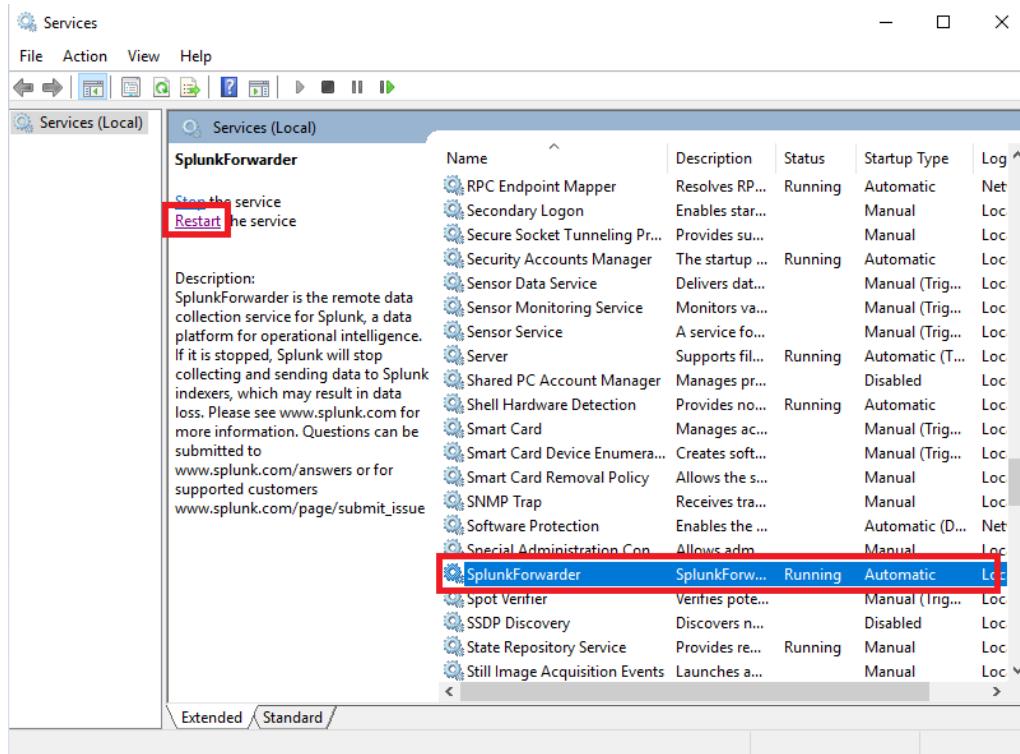
The configuration below monitors IIS log files in the specified directory, categorizes them using the ms:iis:auto sourcetype, and will store the data in the “iis” index.

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)



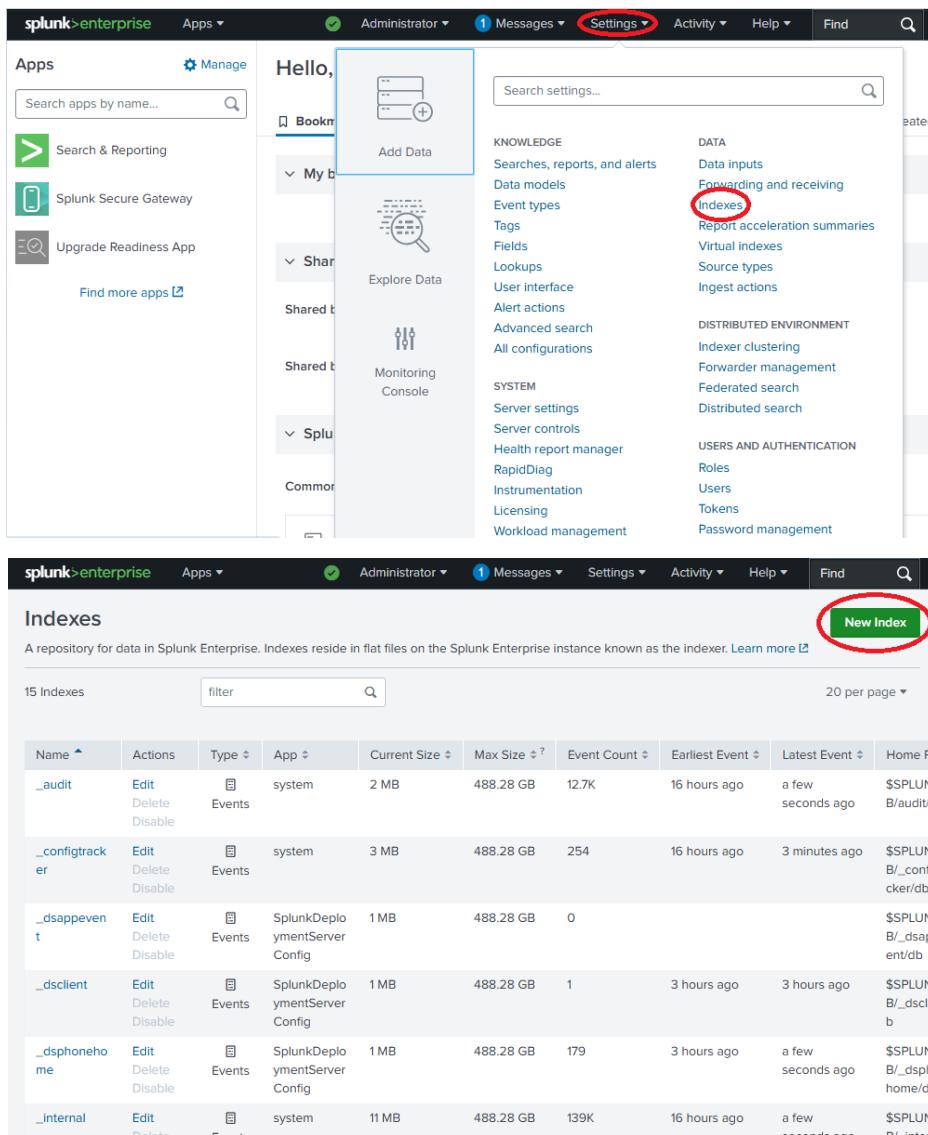


Once SplunkForwarder has restarted, we should get these messages shown below

The screenshot shows the Splunk Enterprise dashboard. Three warning messages are displayed in a sidebar:

- Received event for unconfigured/disabled/deleted index=syomon with source="source:XmlWinEventLog:Microsoft-Windows-Syomon/Operational" host="host:WIN-HUASGCRADTM" sourcetype="sourcetype:XmlWinEventLog:Microsoft-Windows-Syomon/Operational". Dropping them as lastChancelIndex setting in indexes.conf is not configured. So far received events from 2 missing index(es). 11/11/2024, 3:07:13 PM
- Received event for unconfigured/disabled/deleted index=ilis with source="source:C:\inetpub\logs\LogFiles\W3SVC1\lu_ex241111.log" host="host:WIN-HUASGCRADTM" sourcetype="sourcetype::ms:ilis:auto". Dropping them as lastChancelIndex setting in indexes.conf is not configured. So far received events from 1 missing index(es). 11/11/2024, 3:07:03 PM
- Security risk warning: Found an empty value for 'allowedDomainList' in the alert_actions.conf configuration file. If you do not configure this setting, then users can...

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



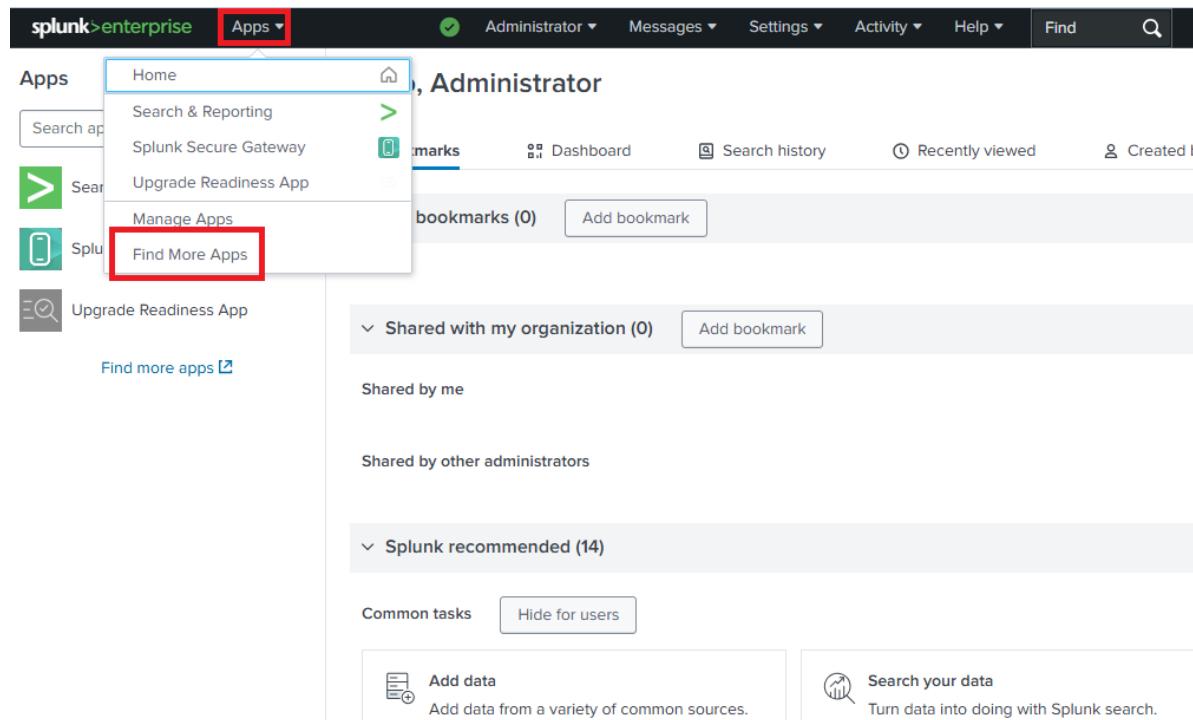
The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk>enterprise', 'Administrator', 'Messages', 'Settings' (which is highlighted with a red circle), 'Activity', 'Help', and a search bar. Below the navigation is a sidebar titled 'Apps' with a 'Manage' icon. The main content area has a 'Hello, Bookr' message and several links: 'Add Data', 'Explore Data', 'Monitoring Console', and 'Shared Content'. To the right is a large 'Search settings...' input field. The main content area is divided into sections: 'KNOWLEDGE' (Searches, reports, and alerts, Data models, Event types, Tags, Fields, Lookups, User interface, Alert actions, Advanced search, All configurations), 'DATA' (Data inputs, Forwarding and receiving, Indexes, Report acceleration summaries, Virtual indexes, Source types, Ingest actions), 'DISTRIBUTED ENVIRONMENT' (Indexer clustering, Forwarder management, Federated search, Distributed search), 'SYSTEM' (Server settings, Server controls, Health report manager, RapidDiag, Instrumentation, Licensing, Workload management), and 'USERS AND AUTHENTICATION' (Roles, Users, Tokens, Password management). Below this is a table titled 'Indexes' with a 'New Index' button highlighted by a red circle. The table lists 15 indexes with columns for Name, Actions, Type, App, Current Size, Max Size, Event Count, Earliest Event, Latest Event, and Home Path. The indexes listed are: _audit, _configtracker, _dsapovenant, _dsclient, _dsphonehome, and _internal.

| Name | Actions | Type | App | Current Size | Max Size | Event Count | Earliest Event | Latest Event | Home Path |
|----------------|---------------------------|--------|-------------------------------|--------------|-----------|-------------|----------------|-------------------|-------------------------|
| _audit | Edit Delete Disable | Events | system | 2 MB | 488.28 GB | 12.7K | 16 hours ago | a few seconds ago | \$SPLUNK/_audit |
| _configtracker | Edit Delete Disable | Events | system | 3 MB | 488.28 GB | 254 | 16 hours ago | 3 minutes ago | \$SPLUNK/_configtracker |
| _dsapovenant | Edit Delete Disable | Events | SplunkDeploymentServer Config | 1 MB | 488.28 GB | 0 | | | \$SPLUNK/_dsapovenant |
| _dsclient | Edit Delete Disable | Events | SplunkDeploymentServer Config | 1 MB | 488.28 GB | 1 | 3 hours ago | 3 hours ago | \$SPLUNK/_dsclient |
| _dsphonehome | Edit Delete Disable | Events | SplunkDeploymentServer Config | 1 MB | 488.28 GB | 179 | 3 hours ago | a few seconds ago | \$SPLUNK/_dsphonehome |
| _internal | Edit Delete Disable | Events | system | 11 MB | 488.28 GB | 139K | 16 hours ago | a few seconds ago | \$SPLUNK/_internal |

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.

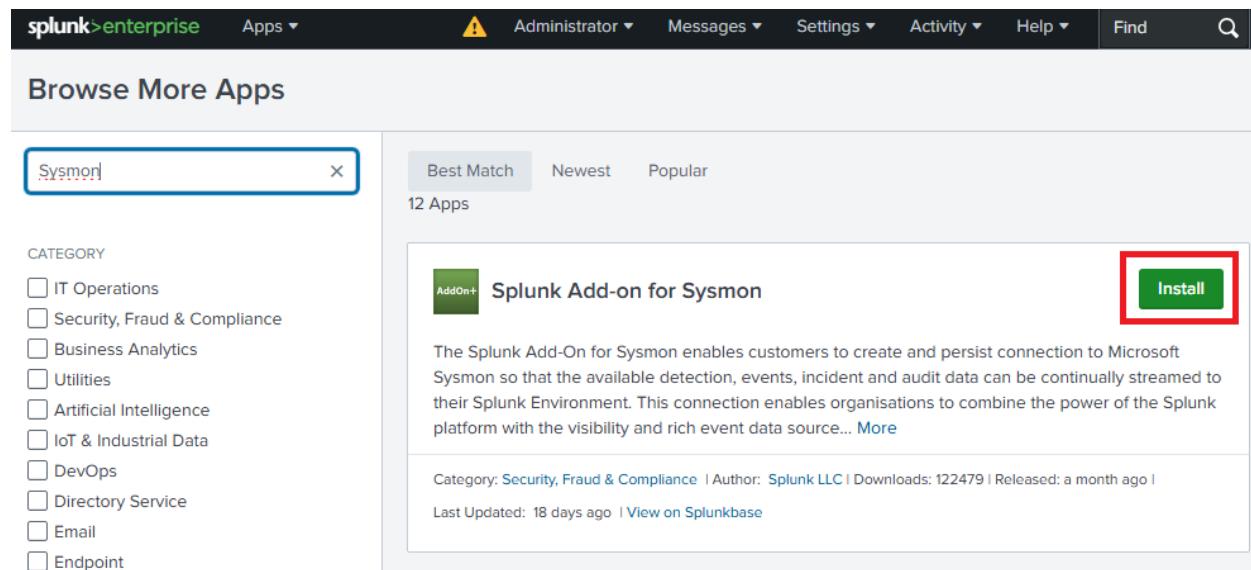
Splunk Universal Forwarder App Installation

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



The screenshot shows the Splunk UI with the 'splunk>enterprise' header. The 'Apps' menu is open, and the 'Find More Apps' option is highlighted with a red box. The main pane displays various app categories and recommended apps.

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.



The screenshot shows the Splunk App Store search results for 'Sysmon'. The search bar contains 'Sysmon'. The 'Splunk Add-on for Sysmon' app is listed, and its 'Install' button is highlighted with a red box. The app details page includes a description, category information, and download statistics.

Browse More Apps

Best Match Newest Popular

5 Apps

CATEGORY

- IT Operations
- Security, Fraud & Compliance
- Business Analytics
- Utilities
- Artificial Intelligence
- IoT & Industrial Data
- DevOps
- Directory Service
- Email
- Endpoint

Splunk Add-on for Microsoft IIS

The Splunk Add-on for Microsoft IIS allows a Splunk software administrator to collect Web site activity data in the W3C log file format from Microsoft IIS servers. It can ingest W3C-compliant log files generated by standard logging as well as advanced logging in IIS.

Category: IT Operations | Author: Splunk LLC | Downloads: 55061 | Released: 9 months ago | Last Updated: 9 months ago | View on Splunkbase

Install

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)

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾

Apps

Home, Administrator

Search app

Manage Apps

Find more apps ↗

Shared with my organization (0) Add bookmark

Shared by me

Shared by other administrators

Splunk recommended (14)

Common tasks Hide for users

Add data Add data from a variety of common sources.

Search your data Turn data into doing with Splunk search.

splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find ▾

Apps

Browse more apps

Install app from file

Create app

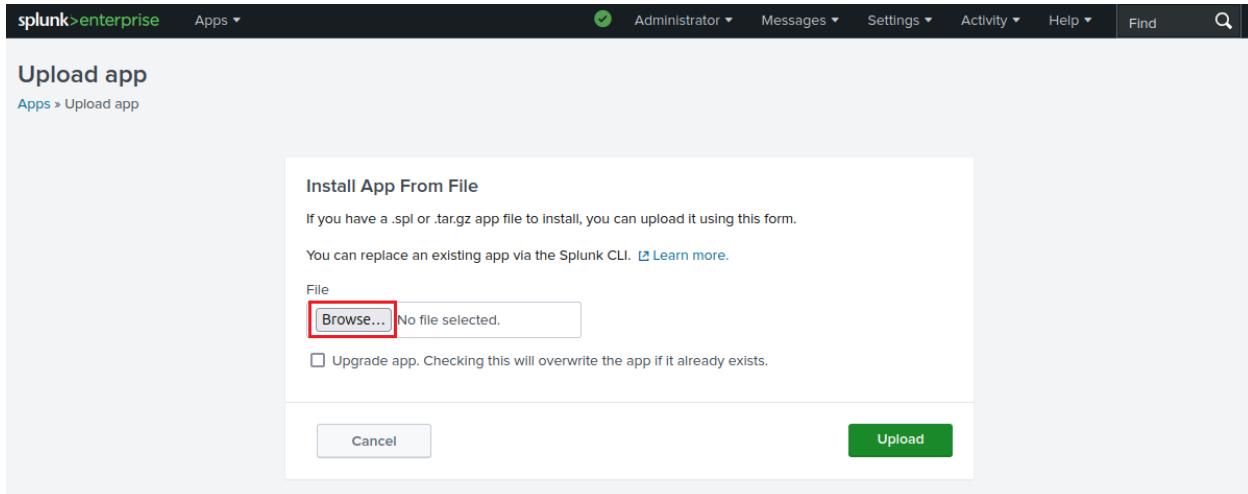
Showing 1-25 of 29 items

filter

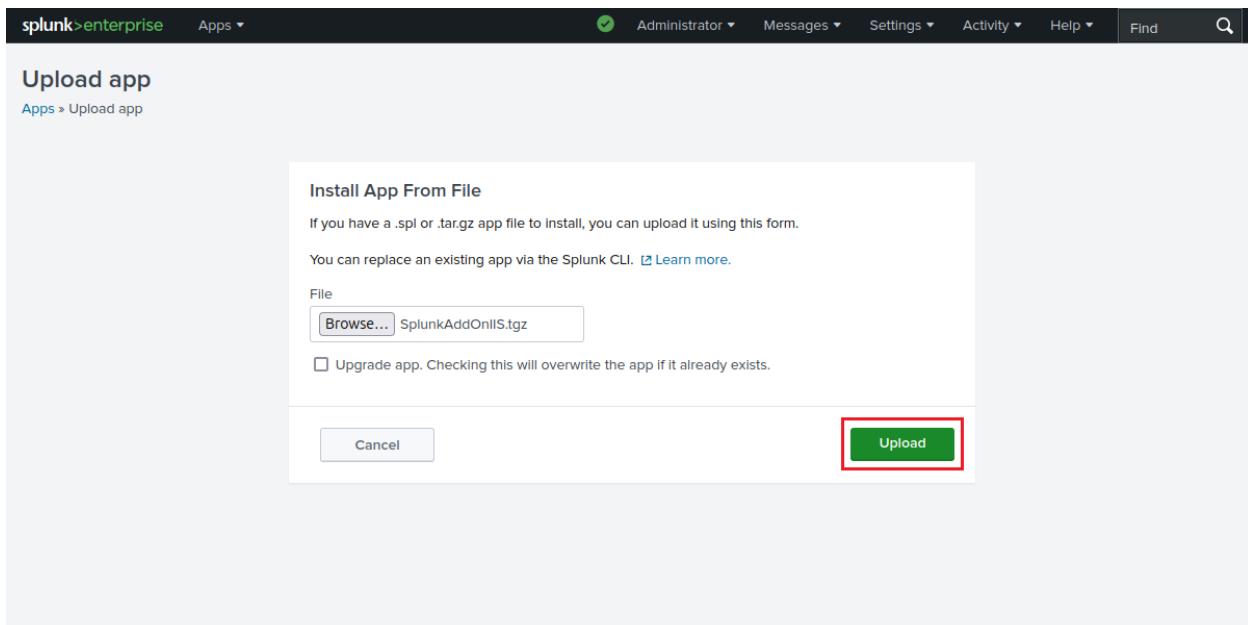
25 per page ▾

< Prev 1 2 Next >

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)



Once 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.

The screenshot shows the Splunk enterprise homepage. At the top, there is a navigation bar with links for 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a search bar. Below the navigation bar, there is a sidebar titled 'Hello, Administrator' with a 'Bookmarks' tab selected. Under 'My bookmarks', there is a link to 'Search & Reporting' which is highlighted with a red box. Other bookmarked items include 'Splunk Secure Gateway' and 'Upgrade Readiness App'. There are also sections for 'Shared with my organization' and 'Splunk recommended' (14). At the bottom of the sidebar, there are 'Common tasks' like 'Add data' and 'Search your 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.

The screenshot shows the Splunk search interface. At the top, there is a navigation bar with links for 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a search bar. Below the navigation bar, there is a search bar containing the query 'index=*'. The search bar has a red box around it. To the right of the search bar are buttons for 'Last 24 hours' and a magnifying glass icon. Below the search bar, there is a 'Search' section with a 'Search History' link. On the left, there is a 'How to Search' section with a link to 'Documentation'. On the right, there is an 'Analyze Your Data with Table Views' section with a 'Create Table View' button. At the bottom, there are buttons for 'Documentation', 'Tutorial', and 'Data Summary'.

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

The screenshot shows a Splunk search interface. On the left, under "SELECTED FIELDS", "a host 1", "a source 5", and "a sourcetype 5" are listed. Under "INTERESTING FIELDS", numerous fields are listed, including "a Account_Domain 5", "a Account_Name 12", "a action 1", "a CommandLine 14", "a Company 5", "a Computer 1", "a ComputerName 1", "a CurrentDirectory 2", "a Description 7", "a dest 1", "a dvc 1", "a EventChannel 1", "# EventCode 78", "a EventDescription 2", "# EventID 2", "# EventType 4", "a eventtype 3", "a FileVersion 5", "a Guid 1", "a Hashes 7", "a Image 9", "a IMPHASH 7", and "a index 4". The "a index 4" field is highlighted with a red box. The main pane displays event details for index 4, including XML event data and metadata such as host = WIN-HUASGCRADTM, source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational, and sourcetype = xmlwineventlog.

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

The screenshot shows a Splunk search interface with a modal window titled "index" open. The modal displays "4 Values, 100% of events" and a "Selected" button with "Yes" and "No" options. Below this, there are sections for "Reports" (Top values, Top values by time, Rare values) and "Events with this field". A table titled "Values" shows the following data:

| Values | Count | % |
|---------------|-------|---------|
| main | 867 | 74.806% |
| sysmon | 244 | 21.053% |
| wineventlog | 26 | 2.243% |
| iis | 22 | 1.898% |

A red box highlights the "sysmon" value in the table. The background search results show event details for index 4, including XML event data and metadata such as host = WIN-HUASGCRADTM, source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational, and sourcetype = xmlwineventlog.

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

| List ▾ | | | Format | 20 Per Page ▾ | < Prev | 1 | 2 | 3 | 4 | Next > |
|---|--|--|--------|---------------|--------|---|---|---|---|--------|
| <i> Hide Fields</i> <i>All Fields</i> | | | | | | | | | | |
| SELECTED FIELDS | | | | | | | | | | |
| <i>a host</i> 2 <i>a source</i> 1 <i>a sourcetype</i> 1 | | | | | | | | | | |
| INTERESTING FIELDS | | | | | | | | | | |
| <i>a app</i> 1 <i>a eventtype</i> 1 <i>a index</i> 1 <i># linecount</i> 2 <i>a product</i> 1 <i>a punct</i> 7 <i>a role</i> 1 <i>a splunk_server</i> 1 <i>a tag</i> 3 <i>a tag:eventtype</i> 3 <i>a timestamp</i> 1 <i>a vendor</i> 1 <i>a vendor_product</i> 1 | | | | | | | | | | |
| <i>+ Extract New Fields</i> | | | | | | | | | | |
| > 11/11/24 5:29:28.000 PM | | | | | | | | | | |
| Event 5:29:28.000 PM 0.0;+Win64;x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/130.0.0.0 +Safari/537.36 - 404 0 2 1 host = WIN-JMOTRBJ871J source = C:\inetpub\logs\LogFiles\W3SVC1\u_ex241111.log sourcetype = ms:iis:auto | | | | | | | | | | |
| > 11/11/24 5:29:28.000 PM | | | | | | | | | | |
| 2024-11-11 23:59:59 ::1 GET /index - 80 - ::1 Mozilla/5.0+(Windows+NT+1 0.0;+Win64;x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/130.0.0.0 +Safari/537.36 - 404 0 2 1 host = WIN-JMOTRBJ871J source = C:\inetpub\logs\LogFiles\W3SVC1\u_ex241111.log sourcetype = ms:iis:auto | | | | | | | | | | |
| > 11/11/24 5:29:28.000 PM | | | | | | | | | | |
| 2024-11-11 23:59:59 ::1 GET /index - 80 - ::1 Mozilla/5.0+(Windows+NT+1 0.0;+Win64;x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/130.0.0.0 +Safari/537.36 - 404 0 2 1 host = WIN-JMOTRBJ871J source = C:\inetpub\logs\LogFiles\W3SVC1\u_ex241111.log sourcetype = ms:iis:auto | | | | | | | | | | |
| > 11/11/24 5:29:28.000 PM | | | | | | | | | | |
| 2024-11-11 23:59:59 ::1 GET /index - 80 - ::1 Mozilla/5.0+(Windows+NT+1 0.0;+Win64;x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/130.0.0.0 +Safari/537.36 - 404 0 2 1 host = WIN-JMOTRBJ871J source = C:\inetpub\logs\LogFiles\W3SVC1\u_ex241111.log sourcetype = ms:iis:auto | | | | | | | | | | |

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

The screenshot shows the Splunk Enterprise interface with the 'Settings' menu open. The 'Fields' option under the 'Data' section is highlighted with a red box. The left sidebar shows a search for 'index="iis"' resulting in 81 events. The main pane displays selected fields like host, source, and sourcetype.

Fields

View, edit, and set permissions on field extractions. Define event workflow actions and field aliases. Rename sourcetypes.

| Type | Actions |
|-----------------------|-----------|
| Field aliases | + Add new |
| Calculated fields | + Add new |
| Field extractions | + Add new |
| Field transformations | + Add new |
| Sourcetype renaming | + Add new |
| Workflow actions | + Add new |

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

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

Add new

Fields » Field extractions » Add new

| | |
|---|---|
| Destination app | search |
| Name * | iis_parser |
| Apply to | sourcetype |
| Type * | Inline |
| Extraction/Transform * | <pre>\\$+ \\$+ (?<server_ip>\\$+) (?<method>\\$+) (?<uri_path>\\$+) (?<uri_query>\\$+) (?<server_port>\\$+) (?<username>\\$+) (?<src_ip>\\$+) (?<user_agent>\\$+) (?<referer>\\$+) (?<status>\\$+) (?<sub_status>\\$+) (?<win32_status>\\$+) (?<time_take>\\$+)</pre> <p>If the field extraction is inline, provide the regular expression. If the field extraction uses a transform, specify the transform name.</p> |
| <input type="button" value="Cancel"/> <input type="button" value="Save"/> | |

The screenshot shows the Splunk Enterprise interface for managing field extractions. At the top, there's a navigation bar with links for Apps, Administ..., Messages, Settings, Activity, Help, and Find. Below the navigation is a search bar with a magnifying glass icon.

The main title is "Field extractions" under the "Fields" section. There are two green buttons at the top right: "New Field Extraction" and "Open Field Extractor".

Below the title, it says "Showing 1-4 of 4 items". There are several filter and search options: "App" set to "Search & Reporting (s...)", "Configuration Source" set to "Created in the App", "Owner" set to "Any", and a search bar with "filter" and a magnifying glass icon. A dropdown menu shows "25 per page".

A table lists the field extraction rules:

| Name | Type | Extraction/Transform | Owner | App | Sharing | Status | Actions |
|-------------------------------------|--------|--|-------------|--------|-----------------------|---------|---------------|
| ms:iis:auto : EXTRACT-iis_parser | Inline | \S+ \S+ (?<server_ip>\S+) (?) <method>\S+ (?) <uri_path>\S+ (?) <url_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+) | splunkadmin | search | Private Permissions | Enabled | Move Delete |

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

The comparison shows two sets of field lists:

- Left (Selected Fields):**
 - SELECTED FIELDS:** host 1, source 1, sourcetype 1
 - INTERESTING FIELDS:** app 1, eventtype 1, index 1, linecount 1, product 1, punct 1, role 1, splunk_server 1, tag 3, tag:eventtype 3, timestamp 1, vendor 1, vendor_product 1
- Right (All Fields):**
 - SELECTED FIELDS:** host 2, source 2, sourcetype 1
 - INTERESTING FIELDS:** app 1, eventtype 1, index 1, linecount 2, method 2, product 1, punct 10, referer 4, role 1, server_ip 3, server_port 2, splunk_server 1, sub_status 2, tag 3, tag:eventtype 3, time_take 22, timestamp 1, user_agent 3, username 2, vendor 1, vendor_product 1, win32_status 3
 - Bottom:** 10 more fields

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

The screenshot shows the Splunk Enterprise interface. At the top, there is a navigation bar with 'splunk>enterprise', 'Apps', 'Administrator', 'Messages' (with a count of 1), 'Settings' (which is highlighted with a red circle), 'Activity', 'Help', 'Find', and a search bar. Below the navigation bar is a sidebar titled 'Apps' with sections for 'Search & Reporting', 'Splunk Secure Gateway', and 'Upgrade Readiness App'. The main content area has a 'Hello, [User]' greeting and several buttons: 'Add Data', 'Explore Data', and 'Monitoring Console'. A large 'Search settings...' input field is also present. On the right, a detailed list of settings categories is shown, with 'Indexes' (under 'DATA') circled in red. Other categories include 'KNOWLEDGE', 'SYSTEM', 'DISTRIBUTED ENVIRONMENT', 'USERS AND AUTHENTICATION', and various sub-options like 'Forwarding and receiving', 'Virtual indexes', etc.

Click on “New Index”

The screenshot shows the 'Indexes' page in Splunk. At the top, it says 'Indexes' and 'A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. Learn more'. There is a green 'New Index' button with a red border. Below this is a table with 18 rows of index data. The columns are: Name, Actions (Edit, Delete, Disable), Type (Events), App (system, SplunkDeploymentServer Config, etc.), Current Size, Max Size, Event Count, Earliest Event, Latest Event, Home Path, and Frozen. The table includes a 'filter' and a '20 per page' dropdown.

| Name | Actions | Type | App | Current Size | Max Size | Event Count | Earliest Event | Latest Event | Home Path | Frozen |
|--------------|---------------------|--------|-------------------------------|--------------|-----------|-------------|----------------|-------------------|--------------------------------|--------|
| _audit | Edit Delete Disable | Events | system | 5 MB | 488.28 GB | 40.1K | a month ago | a few seconds ago | \$SPLUNK_D/B/_audit/db | N/A |
| _configtrack | Edit Delete Disable | Events | system | 1MB | 488.28 GB | 0 | | | \$SPLUNK_D/B/_configtracker/db | N/A |
| _dsappevent | Edit Delete Disable | Events | SplunkDeploymentServer Config | 1MB | 488.28 GB | 0 | | | \$SPLUNK_D/B/_dsappevent/db | N/A |
| _dsclient | Edit Delete Disable | Events | SplunkDeploymentServer Config | 1MB | 488.28 GB | 6 | a month ago | 6 minutes ago | \$SPLUNK_D/B/_dsclient/db | N/A |
| _dsphonehome | Edit Delete Disable | Events | SplunkDeploymentServer Config | 1MB | 488.28 GB | 5 | 5 minutes ago | a minute ago | \$SPLUNK_D/B/_dsphonehome/db | N/A |
| _internal | Edit Delete Disable | Events | system | 2 MB | 488.28 GB | 14.8K | a month ago | in 13 hours | \$SPLUNK_D/B/_internal/db | N/A |

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

New Index

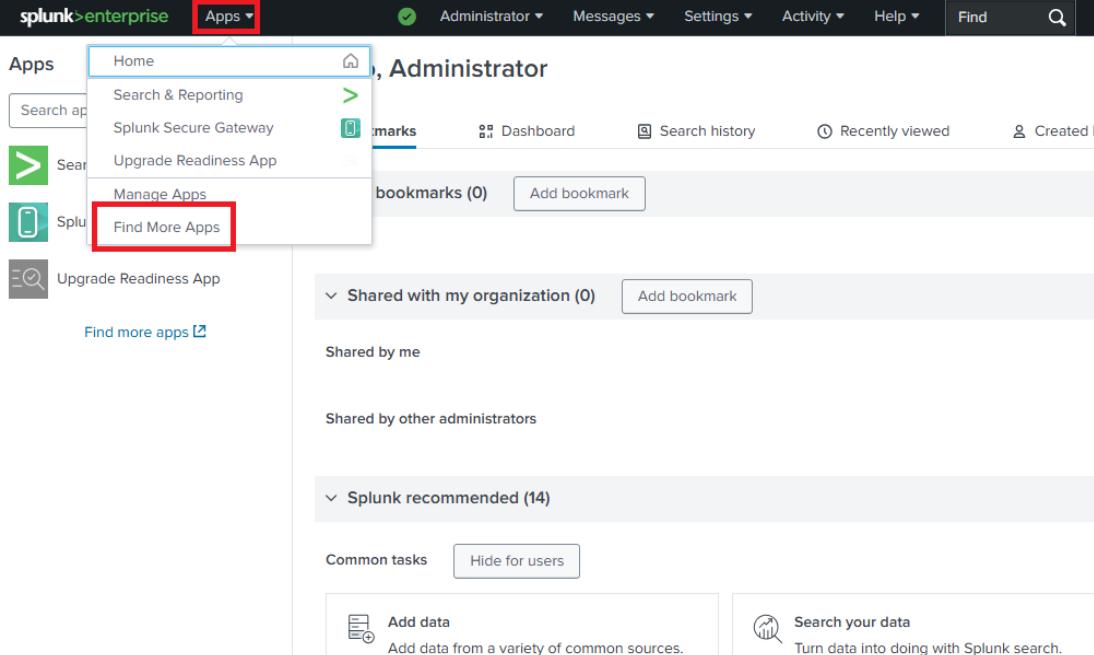
General Settings

| | |
|---|---|
| Index Name | apache |
| Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME. | |
| Index Data Type | <input checked="" type="radio"/> Events <input type="radio"/> 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 | <input checked="" type="radio"/> Enable <input type="radio"/> 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. | |

Action Buttons

Save (Red Box) **Cancel**

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



The screenshot shows the Splunk Enterprise dashboard. At the top, there's a navigation bar with 'splunk>enterprise' on the left, followed by 'Apps ▾'. A dropdown menu is open under 'Apps' with several options: 'Home', 'Search & Reporting', 'Splunk Secure Gateway', 'Upgrade Readiness App', 'Manage Apps', and 'Find More Apps'. The 'Find More Apps' option is highlighted with a red box. To the right of the dropdown, there's a sidebar titled 'Administrator' with sections for 'bookmarks (0)', 'Shared with my organization (0)', 'Shared by me', and 'Splunk recommended (14)'. Below the sidebar, there are two cards: 'Add data' (with a plus icon) and 'Search your data' (with a magnifying glass icon).

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

The screenshot shows the Splunk Enterprise interface with the search bar containing "apache". Below the search bar, there is a sidebar titled "CATEGORY" with various checkboxes for different IT operations categories. The main search results area shows two items:

- Atlas ITSI Content Pack for Apache Web Server**: This item is not highlighted with a red box.
- Splunk Add-on for Apache Web Server**: This item is highlighted with a red box around its entire card. It includes a green "Install" button.

Both items have brief descriptions and links to "View on Splunkbase".

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

```

inputs - Notepad
File Edit Format View Help
[WinEventLog://System]
checkpointInterval = 5
current_only = 0
disabled = 0
start_from = oldest
index = wineventlog

[WinEventLog://Microsoft-Windows-Sysmon/Operational]
disabled = false
renderXml = true
index = sysmon
source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

[monitor://C:/inetpub/logs\LogFiles\W3SVC1\*.*]
disabled = false
sourcetype = ms:iis:auto
index = iis

[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

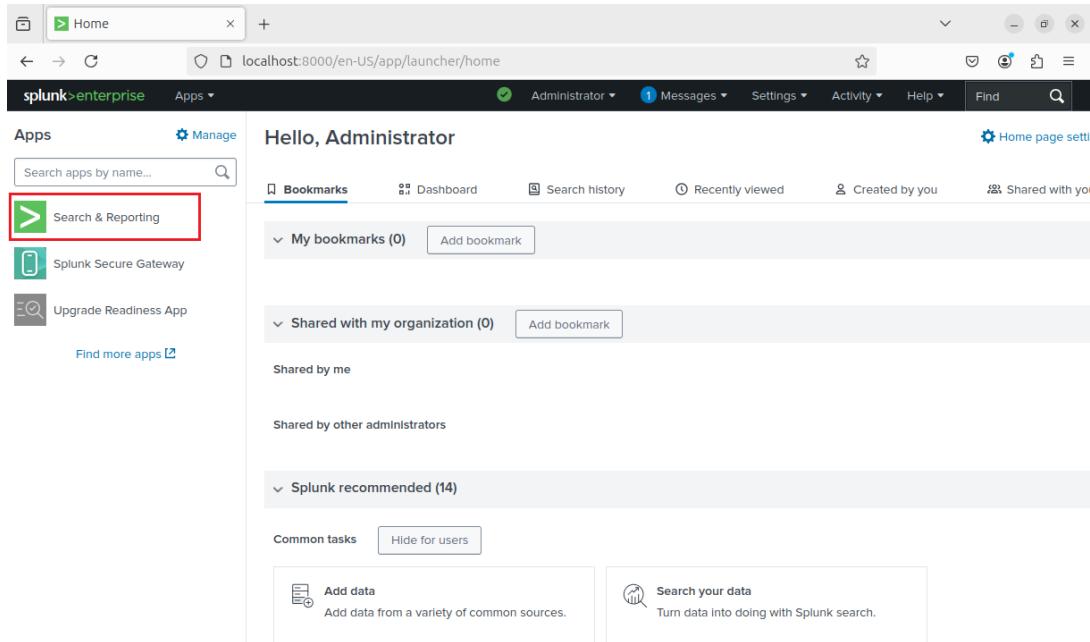
| Name | Description | Status | Startup Type | Log |
|--------------------------------|------------------|-----------------|-----------------|-----|
| Sensor Service | A service fo... | Manual (Trig... | Loc | |
| Server | Supports fil... | Running | Automatic (T... | Loc |
| Shared PC Account Manager | Manages pr... | Disabled | Loc | |
| Shell Hardware Detection | Provides no... | Running | Automatic | Loc |
| Smart Card | Manages ac... | Manual (Trig... | Loc | |
| Smart Card Device Enumera... | Creates soft... | Manual (Trig... | Loc | |
| Smart Card Removal Policy | Allows the s... | Manual | Loc | |
| SNMP Trap | Receives tra... | Manual | Loc | |
| Software Protection | Enables the ... | Automatic (D... | Net | |
| Special Administration Con... | Allows adm... | Manual | Loc | |
| SplunkForwarder | SplunkForw... | Running | Automatic | Loc |
| Spot Verifier | Verifies pote... | Manual (Trig... | Loc | |
| SSDP Discovery | Discovers n... | Disabled | Loc | |
| State Repository Service | Provides re... | Running | Manual | Loc |
| Still Image Acquisition Events | Launches a... | Manual | Loc | |
| Storage Service | Provides en... | Running | Manual (Trig... | Loc |
| Storage Tiers Management | Optimizes t... | Manual | Loc | |
| SysMain | Maintains a... | Running | Automatic | Loc |
| Sysmon64 | System Mo... | Running | Automatic | Loc |
| System Event Notification S... | Monitors sy... | Running | Automatic | Loc |
| System Events Broker | Coordinates... | Running | Automatic (T... | Loc |

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

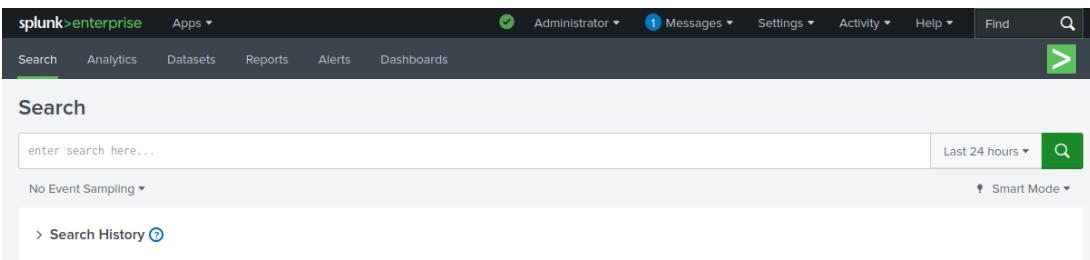
| Time | Event |
|--------------------------|---|
| 12/24/24 11:07:23.000 AM | ::1 - - [23/Dec/2024:20:07:23 -0800] "GET /DVA/ HTTP/1.1" 200 6893 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36" |
| 12/24/24 11:07:23.000 AM | ::1 - - [23/Dec/2024:20:07:23 -0800] "GET /DVA/ HTTP/1.1" 200 6893 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36" |
| 12/24/24 11:07:22.000 AM | ::1 - - [23/Dec/2024:20:07:22 -0800] "GET /DVA/ HTTP/1.1" 200 6893 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36" |
| 12/24/24 11:07:22.000 AM | ::1 - - [23/Dec/2024:20:07:22 -0800] "GET /DVA/ HTTP/1.1" 200 6893 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36" |
| 12/24/24 11:07:22.000 AM | ::1 - - [23/Dec/2024:20:07:22 -0800] "GET /DVA/ HTTP/1.1" 200 6893 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36" |
| 12/24/24 11:07:21.000 AM | ::1 - - [23/Dec/2024:20:07:21 -0800] "GET /DVA/favicon.ico HTTP/1.1" 304 - "http://localhost:8888/DVA/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36" |

Basic Queries for Splunk

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

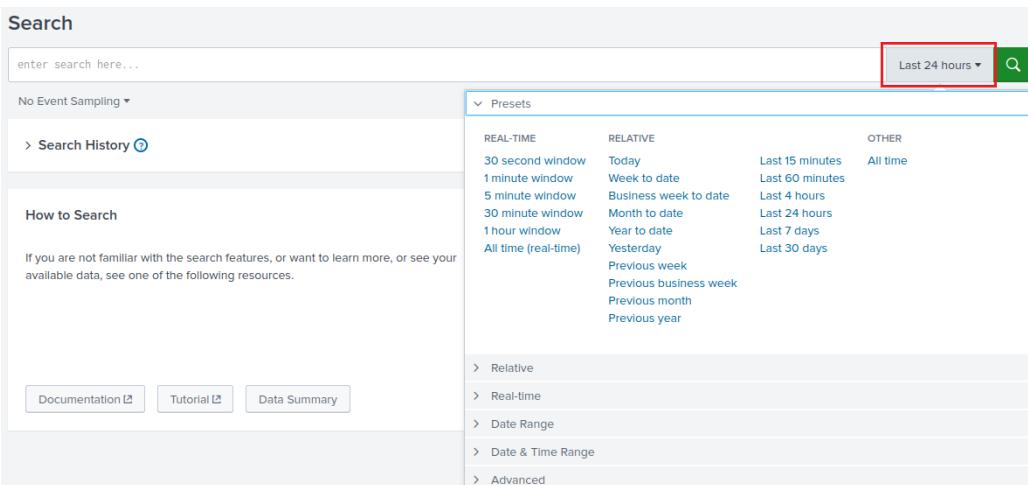


The screenshot shows the Splunk Home page. On the left, there is a sidebar titled "Apps" with a search bar and a list of apps: "Search & Reporting" (highlighted with a red box), "Splunk Secure Gateway", and "Upgrade Readiness App". Below the sidebar, there are sections for "My bookmarks (0)", "Shared with my organization (0)", and "Splunk recommended (14)".



The screenshot shows the Splunk Search page. At the top, there is a search bar with the placeholder "enter search here...". To the right of the search bar is a dropdown menu set to "Last 24 hours". Below the search bar, there is a "No Event Sampling" button and a "Smart Mode" button. A "Search History" link is also visible.

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.



The screenshot shows the Splunk Search page with the search bar and date range dropdown expanded. The dropdown menu is titled "Presets" and includes sections for "REAL-TIME", "RELATIVE", and "OTHER". Under "REAL-TIME", there are options like "30 second window", "1 minute window", etc. Under "RELATIVE", there are options like "Today", "Week to date", etc. Under "OTHER", there are options like "Last 15 minutes", "Last 60 minutes", etc. Below the dropdown, there are links for "Documentation", "Tutorial", and "Data Summary".

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.

The screenshot shows the Splunk interface with a search bar containing "index='iis'". Below the search bar, it says "32 events (11/12/24 10:00:00.000 AM to 11/13/24 10:26:37.000 AM)" and "No Event Sampling". The search results table has columns for Time and Event. The first event is expanded, showing detailed fields like host, source, sourcetype, app, eventtype, index, linecount, and method. The expanded event details are:

| Time | Event |
|-------------------------|--|
| 11/12/24 5:00:37.000 PM | 2024-11-12 23:59:59 192.168.56.101 GET /index - 80 - 192.168.56.108 Mozilla/5.0+(X11;+Ubuntu;+Linux+x86_64;+rv:129.0)+Gecko/20100101+Firefox/129.0 - 404 0 2 0 host = WIN-JMOTRBJ87IJ source = C:\inetpub\logs\LogFiles\W3SVC1\u_ex241112.log sourcetype = ms:ilis:auto |
| 11/12/24 5:00:37.000 PM | 2024-11-12 23:59:59 192.168.56.101 GET /index - 80 - 192.168.56.108 Mozilla/5.0+(X11;+Ubuntu;+Linux+x86_64;+rv:129.0)+Gecko/20100101+Firefox/129.0 - 404 0 2 0 host = WIN-JMOTRBJ87IJ source = C:\inetpub\logs\LogFiles\W3SVC1\u_ex241112.log sourcetype = ms:ilis:auto |
| 11/12/24 5:00:37.000 PM | 2024-11-12 23:59:59 192.168.56.101 GET /index - 80 - 192.168.56.108 Mozilla/5.0+(X11;+Ubuntu;+Linux+x86_64;+rv:129.0)+Gecko/20100101+Firefox/129.0 - 404 0 2 0 host = WIN-JMOTRBJ87IJ source = C:\inetpub\logs\LogFiles\W3SVC1\u_ex241112.log sourcetype = ms:ilis:auto |

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

The screenshot shows the details for the first expanded event. It includes an "Event Actions" section and a table of event fields with dropdown menus for selection. The expanded event details are:

| Type | Field | Value | Actions |
|----------|-------------|--|---------|
| Selected | host | WIN-JMOTRBJ87IJ | ▼ |
| Selected | source | C:\inetpub\logs\LogFiles\W3SVC1\u_ex241112.log | ▼ |
| Selected | sourcetype | ms:ilis:auto | ▼ |
| Event | app | Microsoft Internet Information Services (IIS) | ▼ |
| Event | eventtype | microsoft_iis_web (activity inventory web) | ▼ |
| Event | method | GET | ▼ |
| Event | product | Internet Information Services (IIS) | ▼ |
| Event | referer | - | ▼ |
| Event | role | web_server | ▼ |
| Event | server_ip | 192.168.56.101 | ▼ |
| Event | server_port | 80 | ▼ |
| Event | sub_status | 0 | ▼ |
| Event | tag | activity | ▼ |
| | | inventory | ▼ |

Searching with Keywords

`index=* error OR failure`

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

New Search

index=* error OR failure

63 events (before 11/13/24 10:09:31.000 AM) No Event Sampling

Events (63) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection X Deselect 1 hour per column

List Format 20 Per Page < Prev 1 2 3 4 Next >

Time Event

11/12/24 5:23:08.000 PM host = WIN-JMOTRB871J source = WinEventLog:Security sourcetype = WinEventLog:Security

LogName=Security ... 12 lines omitted ... Logon Account: Administrator Source Workstation: WIN-JMOTRB871J Error Code: 0x0 Show all 17 lines

host = WIN-JMOTRB871J source = WinEventLog:Security sourcetype = WinEventLog:Security

11/12/24 5:23:01.000 PM ... 8 lines omitted ... Keywords=Audit Failure ... 16 lines omitted ... Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Show all 61 lines

INTERESTING FIELDS

- a Account_Domain 6
- a Account_Name 5
- a ComputerName 2
- # EventCode 12
- # EventType 4
- # index 2
- a Keywords 4
- # linecount 7
- a LogName 3
- a Logon_ID 5

SELECTED FIELDS

- a host 2
- a source 3
- a sourcetype 3

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`

New Search

index=* EventCode=4625

13 events (before 11/13/24 10:18:52.000 AM) No Event Sampling

Events (13) Patterns Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection X Deselect 1 hour per column

List Format 20 Per Page < Prev 1 2 3 4 Next >

Time Event

11/12/24 7:53:32.000 AM host = WIN-JMOTRB871J source = WinEventLog:Application sourcetype = WinEventLog:Application

LogName=Application EventCode=4625 EventType=4 ComputerName=WIN-JMOTRB871J Show all 12 lines

host = WIN-JMOTRB871J source = WinEventLog:Application sourcetype = WinEventLog:Application

11/12/24 5:23:01.000 PM host = WIN-JMOTRB871J source = WinEventLog:Security sourcetype = WinEventLog:Security

LogName=Security EventCode=4625 EventType=0 ComputerName=WIN-JMOTRB871J Show all 61 lines

INTERESTING FIELDS

- a Account_Domain 4
- a Account_Name 4
- a Authentication_Package 2
- a Caller_Process_ID 2
- a Caller_Process_Name 2
- a ComputerName 2
- # EventCode 1
- # EventType 2
- a Failure_Reason 1

SELECTED FIELDS

- a host 2
- a source 2
- a sourcetype 2

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.

A screenshot of a Splunk search interface titled "New Search". The search bar contains the command: "index==* | stats count by EventCode". The results show 1,440 events from Nov 12, 2024, to Nov 13, 2024. The "Statistics (82)" tab is selected. The table lists EventCodes and their counts:

| EventCode | count |
|-----------|-------|
| 1 | 506 |
| 1000 | 1 |
| 1001 | 1 |
| 1003 | 1 |
| 10148 | 1 |
| 1037 | 1 |
| 1066 | 1 |
| 1074 | 1 |
| 11 | 153 |
| 12 | 15 |

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.

A screenshot of a Splunk search interface titled "New Search". The search bar contains the command: "index==* | stats count by EventCode | where count > 100". The results show 1,440 events from Nov 12, 2024, to Nov 13, 2024. The "Statistics (4)" tab is selected. The table lists EventCodes and their counts:

| EventCode | count |
|-----------|-------|
| 1 | 506 |
| 11 | 153 |
| 13 | 217 |
| 7036 | 173 |

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**”.

New Search

```
index=*  
| stats count by EventCode  
| sort -count
```

Last 24 hours

1,440 events (11/12/24 11:00:00.000 AM to 11/13/24 11:14:20.000 AM) No Event Sampling ▾ Job ▾ II ■ ▶ ↻ ⌂ ⌄ Smart Mode ▾

Events Patterns Statistics (82) Visualization

20 Per Page ▾ Format Preview ▾

| EventCode | count |
|-----------|-------|
| 1 | 506 |
| 13 | 217 |
| 7036 | 173 |
| 11 | 153 |
| 4624 | 65 |
| 4672 | 61 |
| 5379 | 49 |
| 8 | 23 |

< Prev 1 2 3 4 5 Next >

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.

New Search

```
index=* EventCode=4624  
| table _time host
```

Last 24 hours

65 events (11/12/24 11:00:00.000 AM to 11/13/24 11:24:36.000 AM) No Event Sampling ▾ Job ▾ II ■ ▶ ↻ ⌂ ⌄ Smart Mode ▾

Events Patterns Statistics (65) Visualization

20 Per Page ▾ Format Preview ▾

| _time | host |
|---------------------|-----------------|
| 2024-11-12 16:56:37 | WIN-JMOTRBJ871J |
| 2024-11-12 16:55:40 | WIN-JMOTRBJ871J |
| 2024-11-12 16:55:35 | WIN-JMOTRBJ871J |
| 2024-11-12 16:53:54 | WIN-JMOTRBJ871J |
| 2024-11-12 16:53:54 | WIN-JMOTRBJ871J |
| 2024-11-12 16:53:54 | WIN-JMOTRBJ871J |

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.