Splunk Lab - THM

Introduction

We need your help!

A few weeks ago, Jasmine, the owner of Coffely, had reported a potential data breach resulting in her secret recipe getting stolen by James from the IT department. Before the recipe could get into the hands of the competitors, he was apprehended after finding undeniable evidence in his laptop, thanks to our Forensics team's quick investigation.

Now, Jasmine wants to develop an in-house SOC capability for continuously monitoring the critical logs and events to keep an eye on all the activities within the network. She has contacted our team to provide an on-prem resource who can set up a SIEM locally and ingest necessary logs from the different log sources.

Our choice of SIEM is Splunk for this activity. You are tasked with installing and configuring Splunk and integrating the log sources on Linux and Windows OS.

Prerequisite

This room expects the users to have completed the following rooms:

- Intro to SIEM
- Splunk Basics

About the Lab

In this room, you will be handed over two VMs, Linux and Windows, and your task will be to install Splunk on both Machines and integrate important log sources on each server either through listening ports or by installing forwarders.

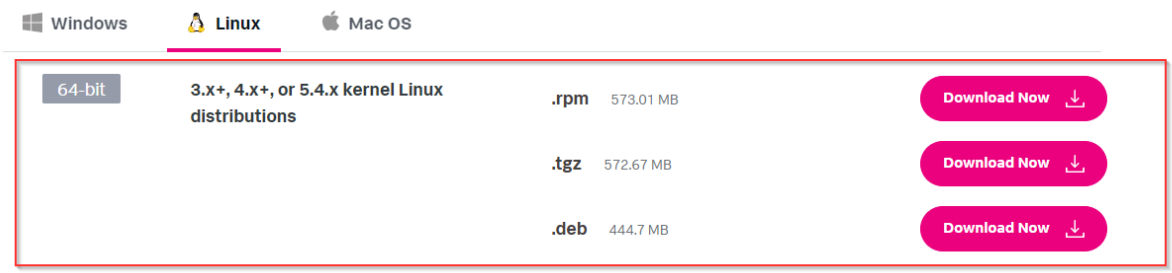
Learning Objectives

This room covers the following learning objectives:

- Dive deep into the Splunk installation process.
- How to install and configure Splunk in Linux and Windows Environments.
- How to integrate different log sources into Splunk.

Splunk: Deployment on Linux Server

Splunk supports all major OS versions, has very straightforward steps to install, and can be up and running in less than 10 minutes on any platform. In this task, we will only focus on installing Splunk Enterprise on the Linux host. Typically, we would create an account on splunk.com and go to this Splunk Enterprise download link to select the installation package for the latest version. As of the time of writing, 9.0.3 is the newest version available on its website.

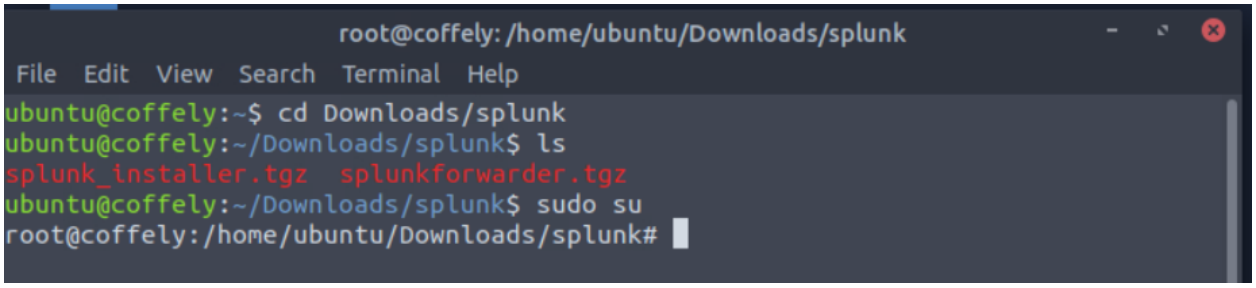


Note: Users are not expected to create an account and download the Splunk Enterprise during this activity. All required executables are already downloaded in relevant paths.

Splunk Installation

For the sake of simplicity, the Splunk installer is already downloaded at the location ~/Downloads/splunk.

Note: Make sure to run sudo su to change to the root user before applying commands.



Splunk installation is as simple as running a command. You will need to uncompress Splunk by running the following command.

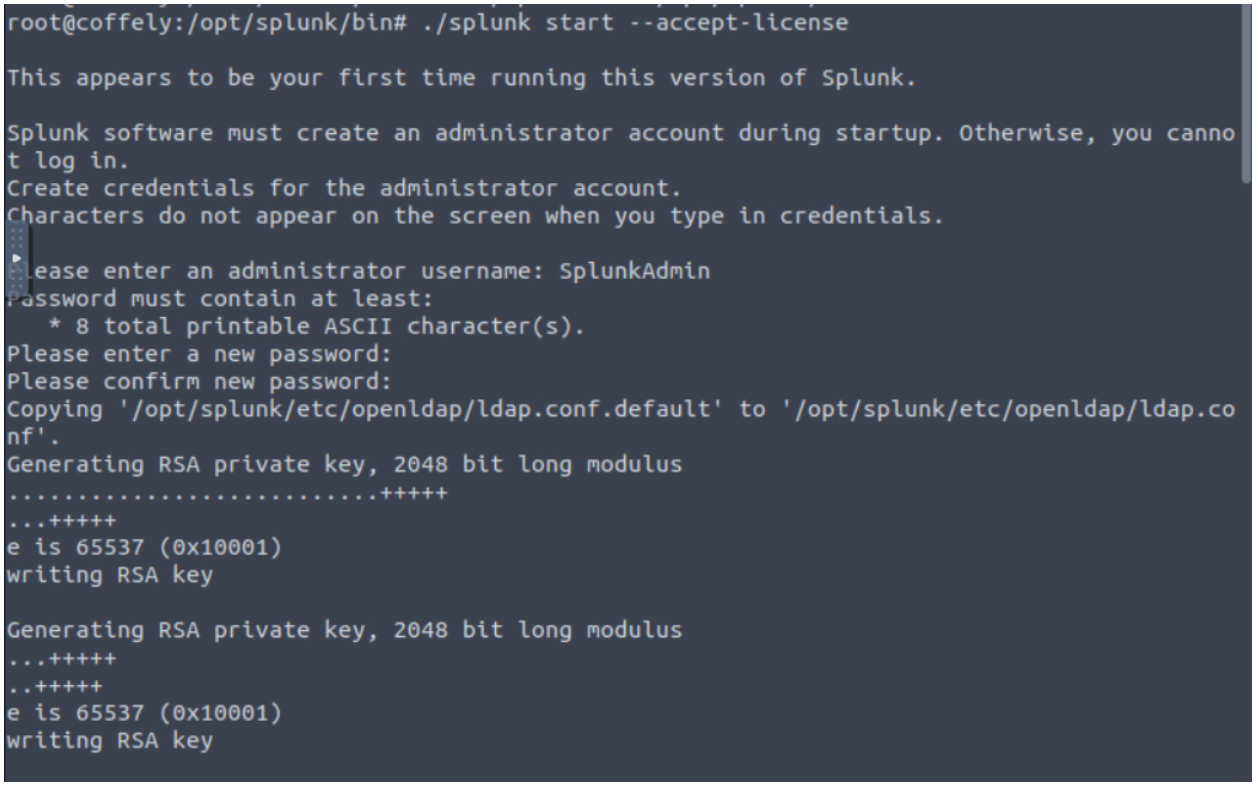
```
root@coffely:/home/ubuntu/Downloads/splunk# tar xvzf splunk_installer.tgz
```

After the installation is complete, a new folder named splunk will be created, as shown below. Let's now move this folder to the /opt/ directory and start working on Splunk from there.

```
root@coffely:/home/ubuntu/Downloads/splunk# ls
splunk  splunk_installer.tgz  splunkforwarder.tgz
root@coffely:/home/ubuntu/Downloads/splunk# mv splunk /opt/
```

Starting Splunk

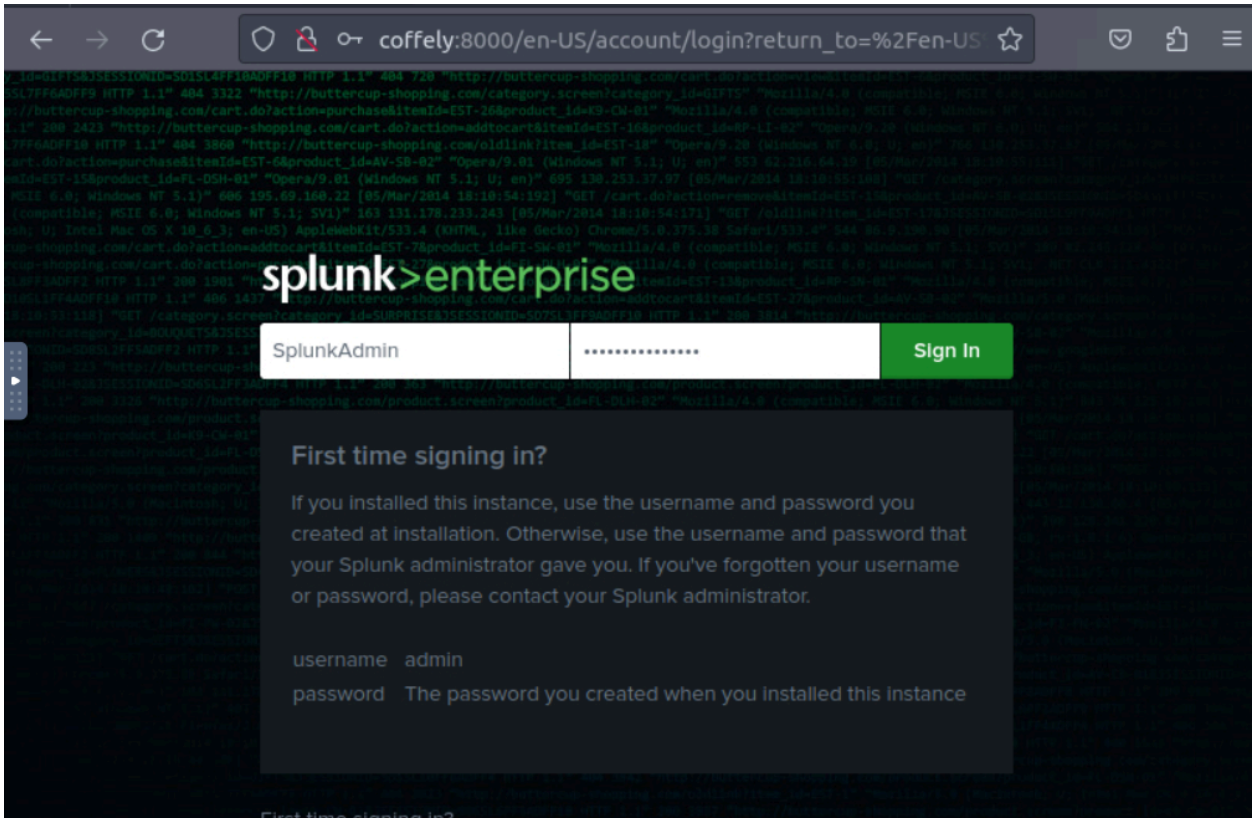
The above step unzips the Splunk installer and installs all the necessary binaries and files on the system. Once installed, go to the directory /opt/splunk/bin and run the following command to start Splunk ./splunk start --accept-license. As it is the first time we are starting the Splunk instance, it will ask the user for admin credentials. Create a user account and proceed.



Accessing Splunk

Congrats! - We successfully installed Splunk on our Linux machine, which took us less than 10 minutes. To access Splunk, open the browser within the VM and go to the address http://coffely:8000. If you are connected to the VPN, you can access Splunk right in your browser by going to the address. http://10.10.217.84:8000.

Use the credentials you created during the installation to access the Splunk dashboard.



****

Answer the questions below:

What is the default port for Splunk?

Answer: 8000

Splunk: Integrating with CLI

Now that we have installed Splunk, it's important to learn some key commands while interacting with Splunk instances through CLI. These commands are run from the /opt/splunk/ directory. It is important to note that we can use the same commands on different platforms.

Some important and commonly used commands are shown below:

Command: splunk start

The splunk start command is used to start the Splunk server. This command starts all the necessary Splunk processes and enables the server to accept incoming data. If the server is already running, this command will have no effect.

```
root@coffely:/opt/splunk/bin# ./splunk start
The splunk daemon (splunkd) is already running.


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

The Splunk web interface is at http://coffely:8000
```

Command: splunk stop

The splunk stop command is used to stop the Splunk server. This command stops all the running Splunk processes and disables the server from accepting incoming data. If the server is not running, this command will have no effect.

```
root@coffely:/opt/splunk/bin# ./splunk stop
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
.........................................
Stopping splunk helpers...

Done.
```

Command: splunk restart

The splunk restart command is used to restart the Splunk server. This command stops all the running Splunk processes and then starts them again. This is useful when changes have been made to the Splunk configuration files or when the server needs to be restarted for any other reason.

```
root@coffely:/opt/splunk/bin# ./splunk restart
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
.........................................
Stopping splunk helpers...

Done.

Splunk> Needle. Haystack. Found.

Checking prerequisites...
        Checking http port [8000]: open
        Checking mgmt port [8089]: open
        Checking appserver port [127.0.0.1:8065]: open
        Checking kvstore port [8191]: open
        Checking configuration... Done.
        Checking critical directories...        Done
        Checking indexes...
                Validated: _audit _configtracker _internal _introspection _metrics _metri
cs_rollup _telemetry _thefishbucket history main summary
        Done
        Checking filesystem compatibility...  Done
        Checking conf files for problems...
                Invalid key in stanza [instrumentation.usage.tlsBestPractices] in /opt/sp
lunk/etc/apps/splunk_instrumentation/default/savedsearches.conf, line 451: | append [| re
st /services/configs/conf-pythonSslClientConfig | eval sslVerifyServerCert (value: if(isn
ull(sslVerifyServerCert),"unset",sslVerifyServerCert), splunk_server=sha256(splunk_server
) | stats values(eai:acl.app) as python_configuredApp values(sslVerifyServerCert) as pyth
on_sslVerifyServerCert by splunk_server | eval python_configuredSystem=if(python_configur
edApp="system","true","false") | fields python_sslVerifyServerCert, splunk_server, python
_configuredSystem]
| append [| rest /services/configs/conf-web/settings | eval mgmtHostPort=if(isnull(mgmtHo
stPort),"unset",mgmtHostPort), splunk_server=sha256(splunk_server) | stats values(eai:acl
.app) as fwdrMgmtHostPort configuredApp values(mgmtHostPort) as fwdr_mgmtHostPort by splu
```

Command: splunk status

The splunk status command is used to check the status of the Splunk server. This command will display information about the current state of the server, including whether it is running or not, and any errors that may be occurring.

```
root@coffely:/opt/splunk/bin# ./splunk status
splunkd is running (PID: 5412).
splunk helpers are running (PIDs: 5413 5565 5615 5626 5643 5696 6028).
```

Command: splunk add oneshot

The splunk add oneshot command is used to add a single event to the Splunk index. This is useful for testing purposes or for adding individual events that may not be part of a larger data stream.

```
root@coffely:/opt/splunk/bin# ./splunk add oneshot
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslC
onfig]/cliVerifyServerName for details.
Splunk username: SplunkAdmin
Password:
Cannot perform action "POST" without a target name to act on.
```

Command: splunk search

The splunk search command is used to search for data in the Splunk index. This command can be used to search for specific events, as well as to perform more complex searches using Splunk's search language.

```
root@coffely:/opt/splunk#./bin/splunk search coffely
WARNING: Server Certificate Hostname Validation is disabled. Please s
Feb 18 21:09:04 coffley ubuntu: coffely-has-the-best-coffee-in-town
Feb 18 13:48:17 coffely ubuntu: COFFELY
Feb 18 13:48:17 coffely ubuntu: COFFELY
```

Command: splunk help

The most important command is the help command which provides all the help options.

```
root@coffely:/opt/splunk/bin# ./splunk help
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslC
onfig]/cliVerifyServerName for details.


Welcome to Splunk's Command Line Interface (CLI).

    Type these commands for more help:

        help [command]              type a command name to access its help page
        help [object]               type an object name to access its help page
        help [topic]                type a topic keyword to get help on a topic
        help commands               display a full list of CLI commands
        help clustering             commands that can be used to configure the clustering
 setup
        help shclustering           commands that can be used to configure the Search Head
 Cluster setup
        help control, controls      tools to start, stop, manage Splunk processes
        help datastore              manage Splunk's local filesystem use
        help distributed            manage distributed configurations such as
                                    data cloning, routing, and distributed search
        help forwarding             manage deployments
        help input, inputs          manage data inputs
        help licensing              manage licenses for your Splunk server
        help settings               manage settings for your Splunk server
        help simple, cheatsheet     display a list of common commands with syntax
        help tools                  tools to help your Splunk server
        help search                 help with Splunk searches

    Universal Parameters:

        The following parameters are usable by any command. For more details on each para
meter, type "help [parameter]".
```

These are just a few of the many CLI commands available in Splunk. Administrators can use the CLI to manage and configure their Splunk servers more efficiently and effectively.

****

Answer the questions below:

In Splunk, what is the command to search for the term coffely in the logs?

Answer: ./bin/splunk search coffely

Use the help command to explore different help options and their syntax.

No answer needed

Splunk: Data Ingestion

Configuring data ingestion is an important part of Splunk. This allows for the data to be indexed and searchable for the analysts. Splunk accepts data from various log sources like Operating System logs, Web Applications, Intrusion Detection logs, Osquery logs, etc. In this task, we will use Splunk Forwarder to ingest the Linux logs into our Splunk instance.

Splunk Forwarders

Splunk has two primary types of forwarders that can be used in different use cases. They are explained below:

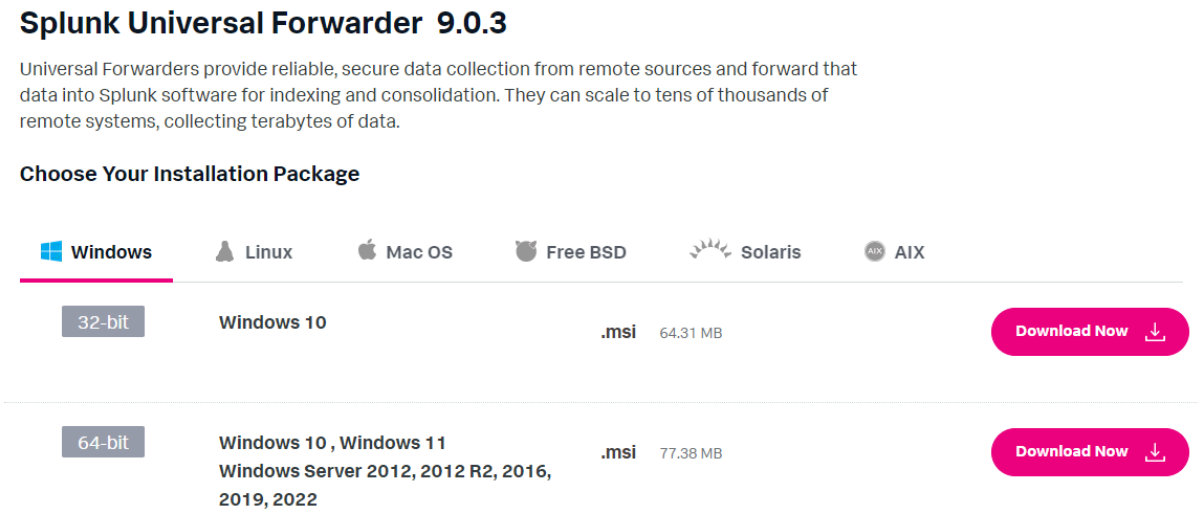
Heavy Forwarders

Heavy forwarders are used when we need to apply a filter, analyze or make changes to the logs at the source before forwarding it to the destination. In this task, we will be installing and configuring Universal forwarders.

Universal Forwarders

It is a lightweight agent that gets installed on the target host, and its main purpose is to get the logs and send them to the Splunk instance or another forwarder without applying any filters or indexing. It has to be downloaded separately and has to be enabled before use. In our case, we will use a universal forwarder to ingest logs.

Universal forwarders can be downloaded from the official Splunk website. It supports various OS, as shown below:

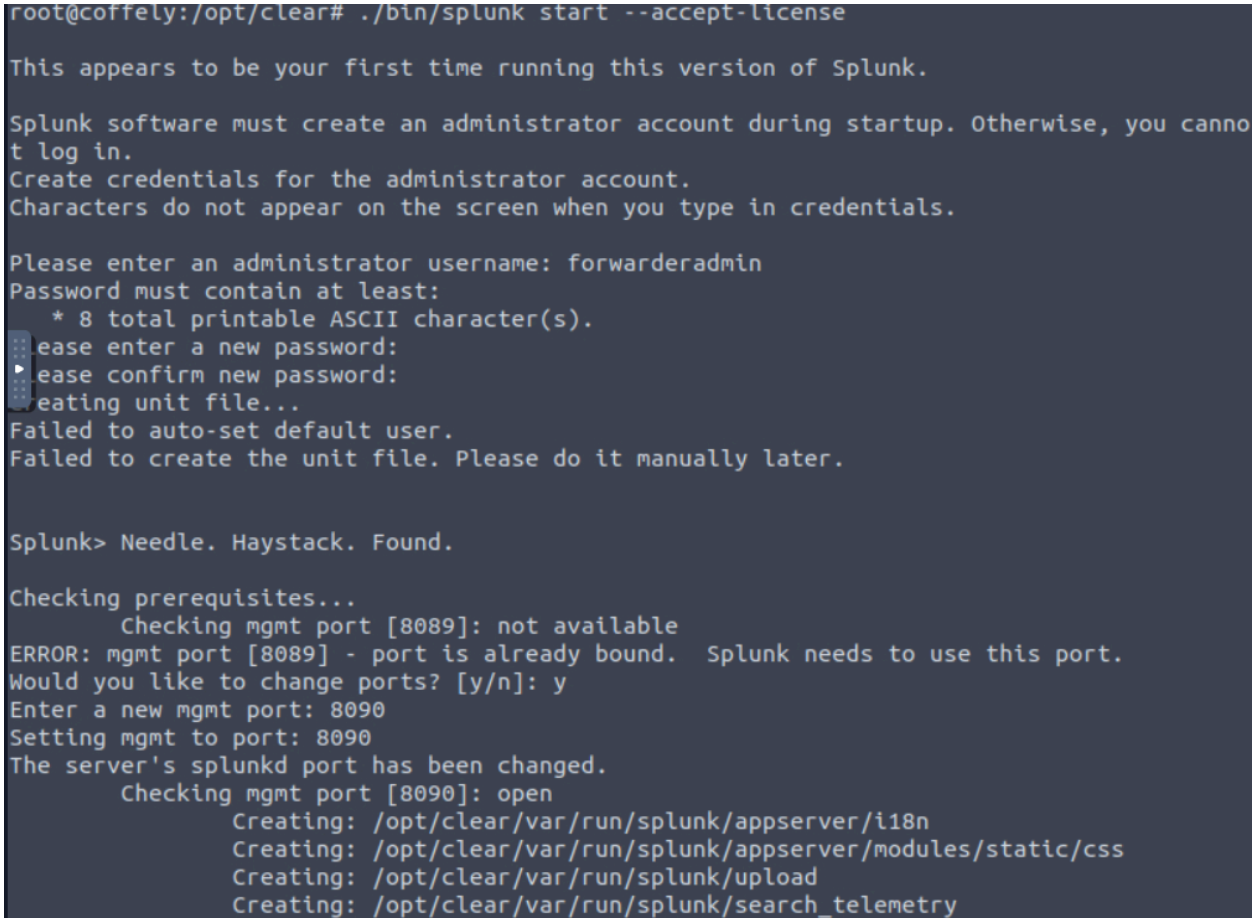


Note: As of writing this, 9.0.3 is the latest version available on the Splunk site.

For this task, the 64-bit version of Linux Forwarder is already downloaded in the folder ~/Downloads/splunk.

```
root@coffely:/home/ubuntu/Downloads/splunk# ls
splunk_installer.tgz  splunkforwarder.tgz
root@coffely:/home/ubuntu/Downloads/splunk# tar xvzf splunkforwarder.tgz
```

The above command will install all required files in the folder splunkforwarder. Next, we will move this folder to /opt/ path with the command mv splunkforwarder /opt/.
We will run the Splunk forwarder instance now and provide it with the new credentials as shown below:



By default, Splunk forwarder runs on port 8089. If the system finds the port unavailable, it will ask the user for the custom port. In this example, we are using 8090 for the forwarder.

Splunk Forwarder is up and running but does not know what data to send and where. This is what we are going to configure next.

****

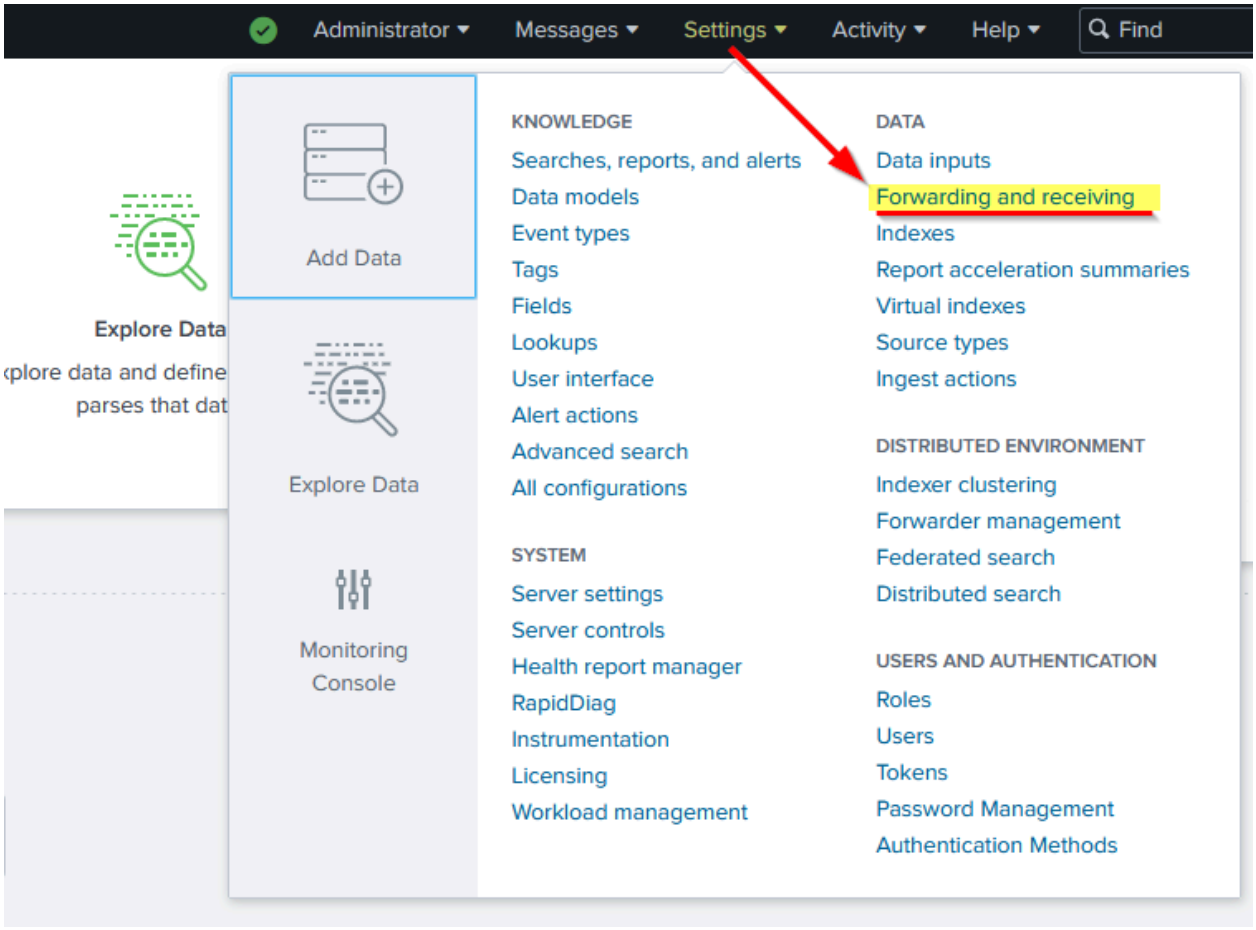
Answer the questions below:
What is the default port, on which Splunk Forwarder runs on?
Answer: 8089

Configuring Forwarder on Linux

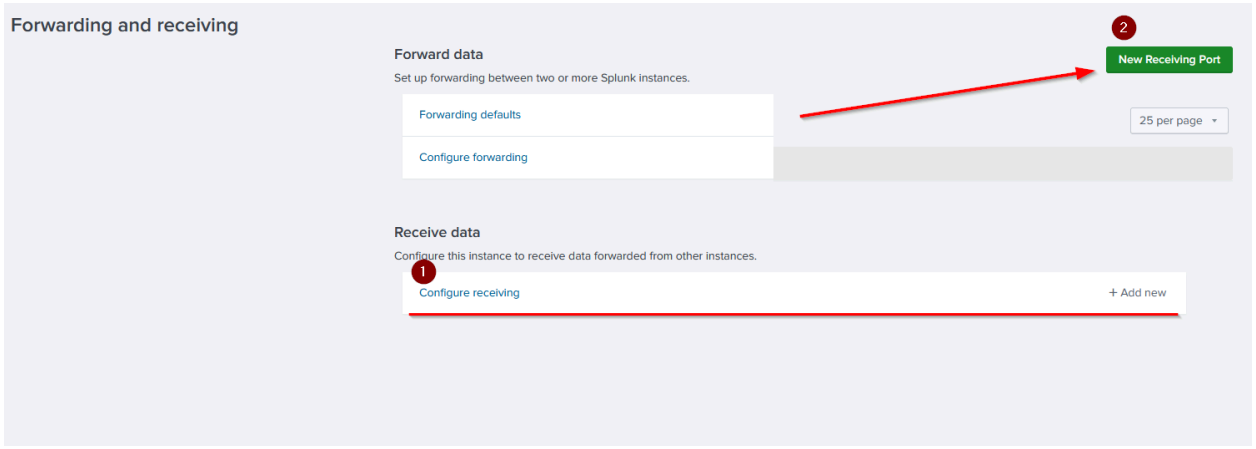
Now that we have installed the forwarder, it needs to know where to send the data. So we will configure it on the host end to send the data and configure Splunk so that it knows from where it is receiving the data.

Splunk Configuration

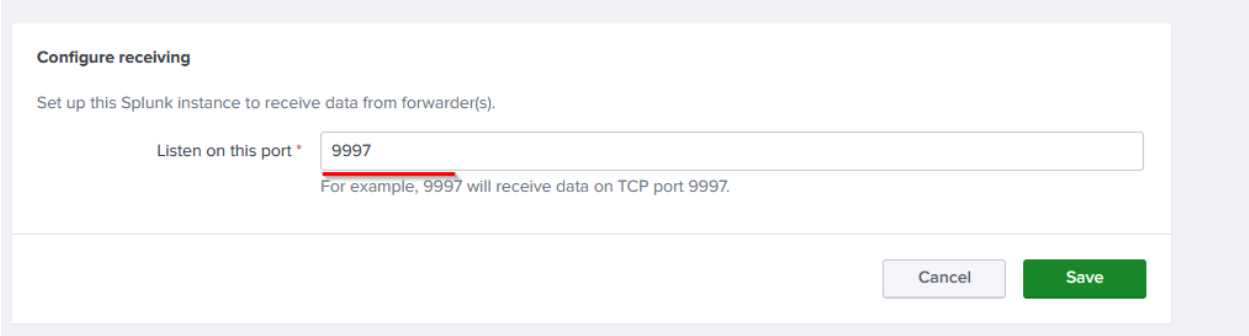
Log into Splunk and Go to Settings -> Forward and receiving tab as shown below:



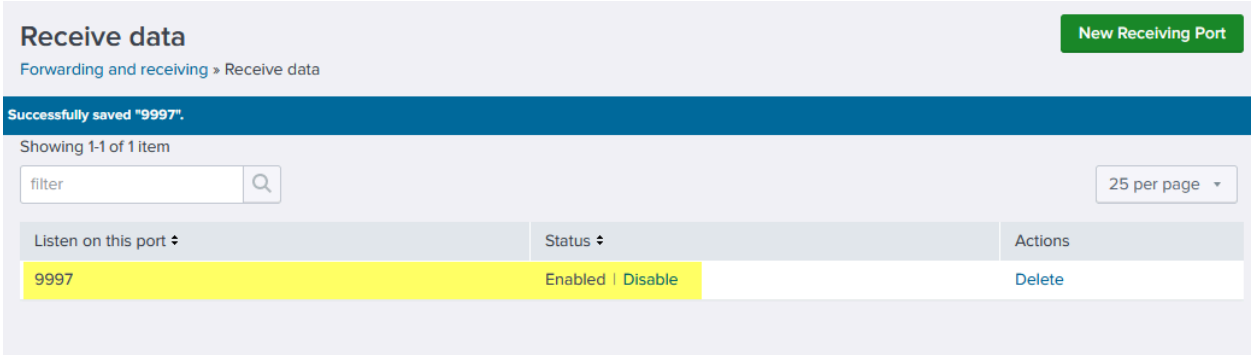
It will show multiple options to configure both forwarding and receiving. As we want to receive data from the Linux endpoint, we will click on Configure receiving and then proceed by configuring a new receiving port.



By default, the Splunk instance receives data from the forwarder on the port 9997. It's up to us to use this port or change it. For now, we will configure our Splunk to start listening on port 9997 and Save, as shown below:

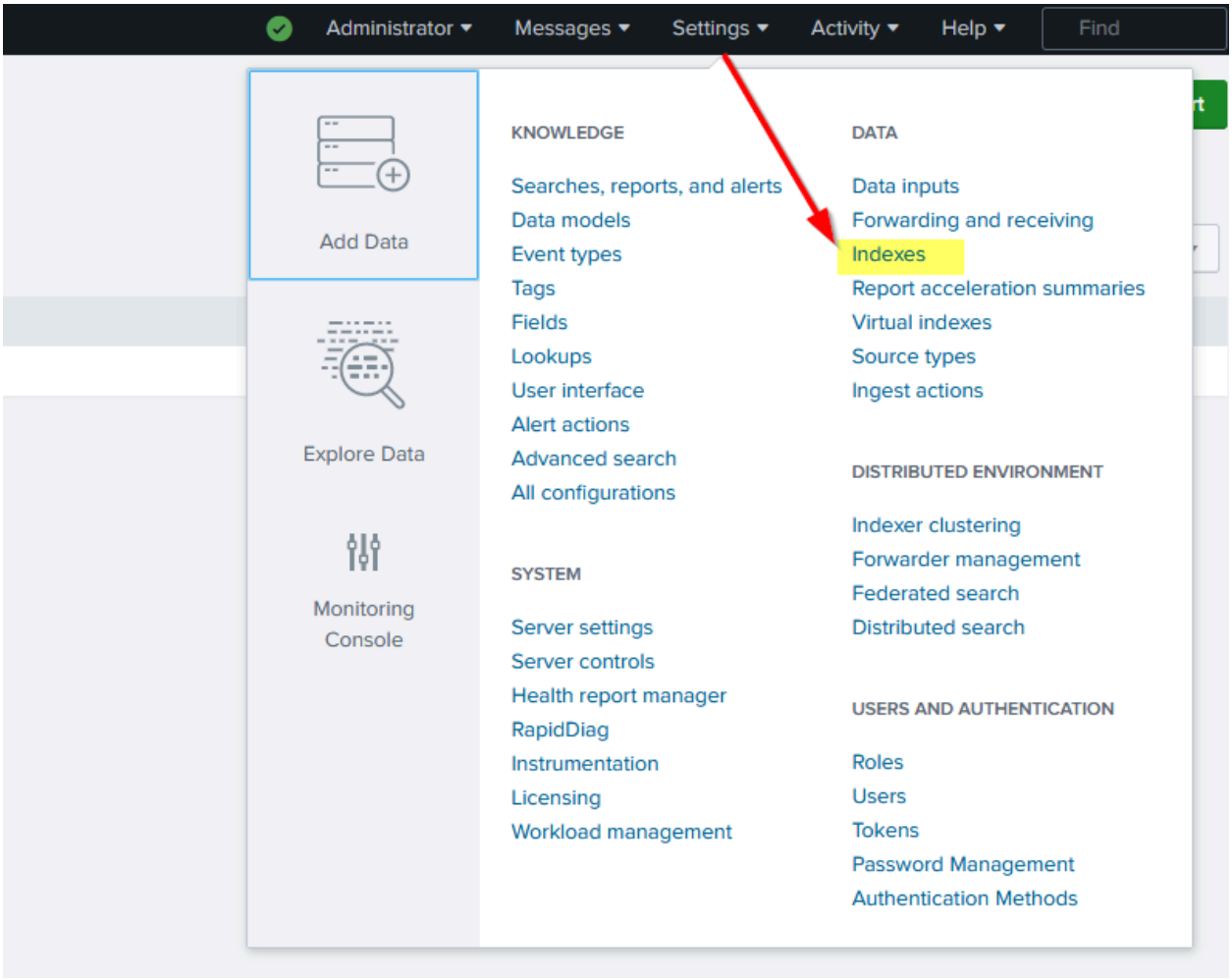


Our listening port 9997 is now enabled and waiting for the data. If we want, we can delete this entry by clicking on the Delete option under the Actions column.

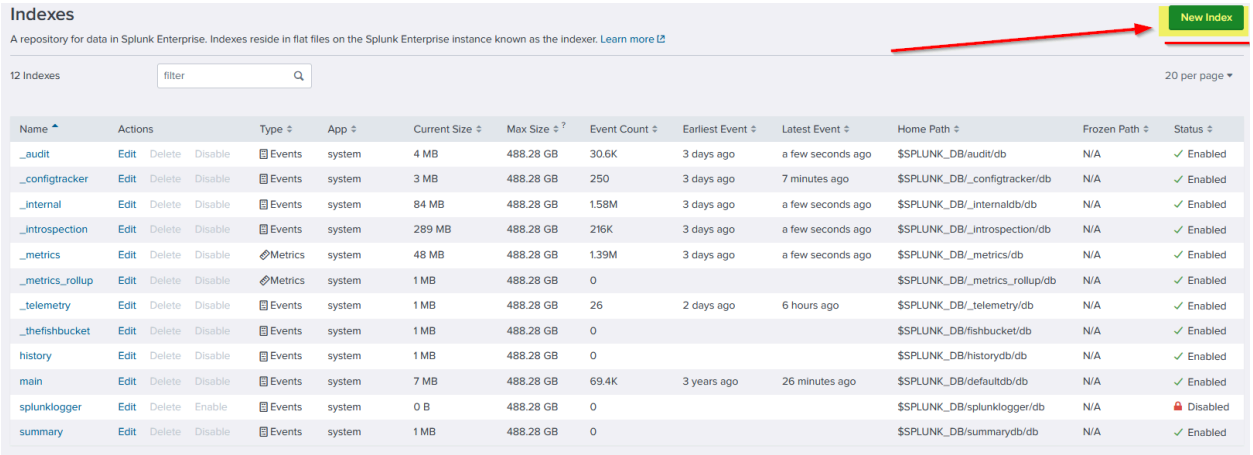


Creating Index

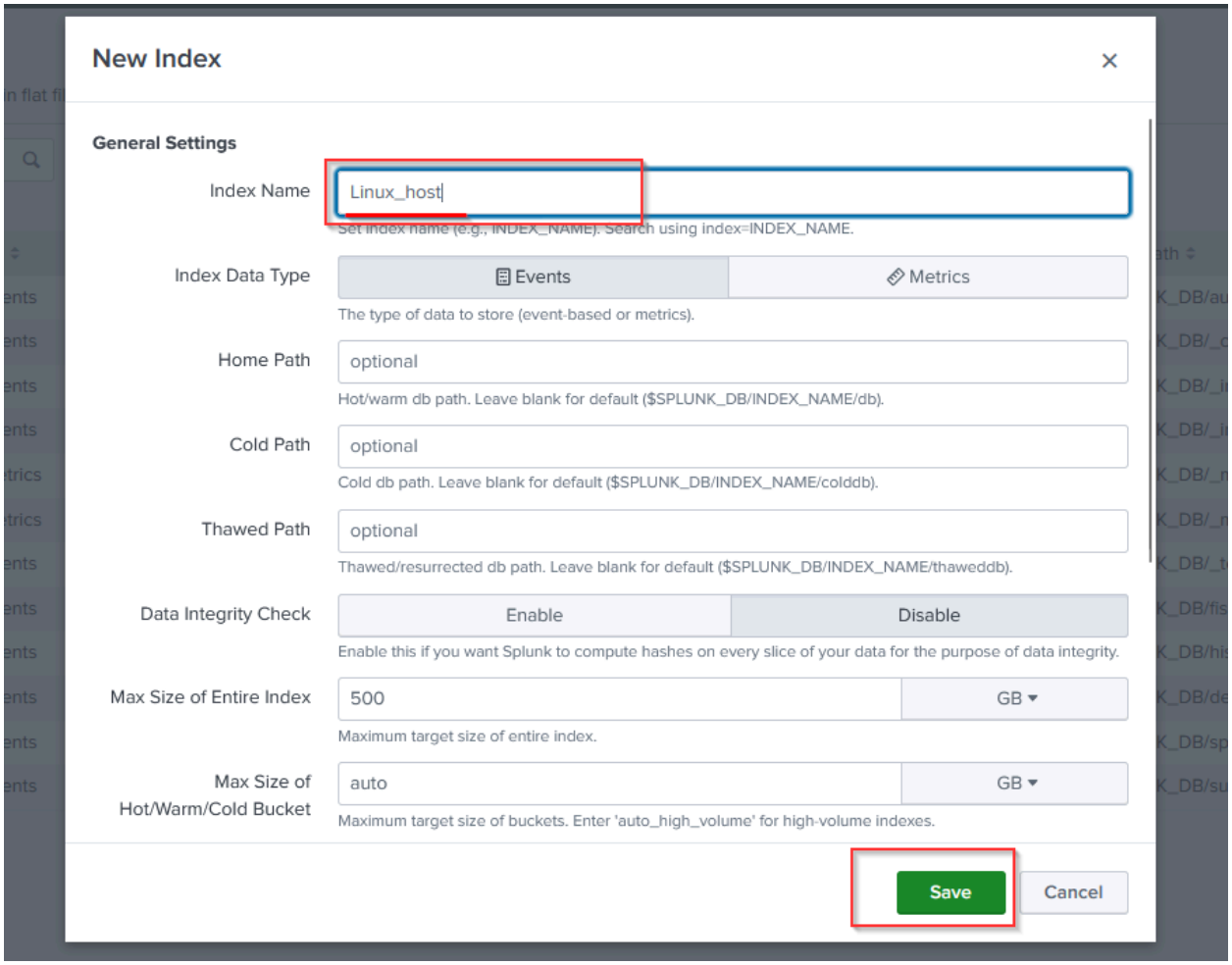
Now that we have enabled a listening port, the important next step is to create an index that will store all the receiving data. If we do not specify an index, it will start storing received data in the default index, which is called the main index.



The indexes tab contains all the indexes created by the user or by default. This shows some important metadata about the indexes like Size, Event Count, Home Path, Status, etc



Click the New Index button, fill out the form, and click Save to create the index. Here we have created an index called Linux_host as shown below:



Configuring Forwarder

It's time to configure the forwarder to ensure it sends the data to the right destination. Back in the Linux host terminal, go to the /opt/splunkforwarder/bin directory

```
root@coffely:/opt/clear/bin# ./splunk add forward-server 10.10.217.84:9997
Splunk username: forwarderadmin
Password:
Added forwarding to: 10.10.217.84:9997.
```

This command will add the forwarder server, which listens to port 9997.

Linux Log Sources

Linux stores all its important logs into the /var/log file, as shown below. In our case, we will ingest syslog into Splunk. All other logs can be ingested using the same method.

```
Xorg.0.log                dmesg.1.gz                prime-offload.log
Xorg.0.log.old            dmesg.2.gz                prime-supported.log
alternatives.log          dmesg.3.gz                private
amazon                    dmesg.4.gz                samba
apport.log                dpkg.log                  speech-dispatcher
apport.log.1              fontconfig.log            syslog
apt                       gdm3                      syslog.1
audit                     gpu-manager-switch.log    syslog.2.gz
auth.log                  gpu-manager.log           syslog.3.gz
auth.log.1                hp                        syslog.4.gz
btmp                      journal                   syslog.5.gz
cloud-init-output.log     kern.log                  syslog.6.gz
cloud-init.log            kern.log.1                syslog.7.gz
cups                      landscape                 unattended-upgrades
dist-upgrade              lastlog                   wtmp
dmesg                     lightdm
dmesg.0                   openvpn
```

Next, we will tell Splunk forwarder which logs files to monitor. Here, we tell Splunk Forwarder to monitor the /var/log/syslog file.

```
root@coffely:/opt/clear/bin# ./splunk add monitor /var/log/syslog -index Linux_host
Added monitor of '/var/log/syslog'.
```

Exploring Inputs.conf

We can also open the inputs.conf file located in /opt/splunkforwarder/etc/apps/search/local, and look at the configuration added after the commands we used above.

```
root@coffely:/opt/clear/etc/apps/search/local# ls
inputs.conf
```

We can view the content of the input.conf using the cat command.

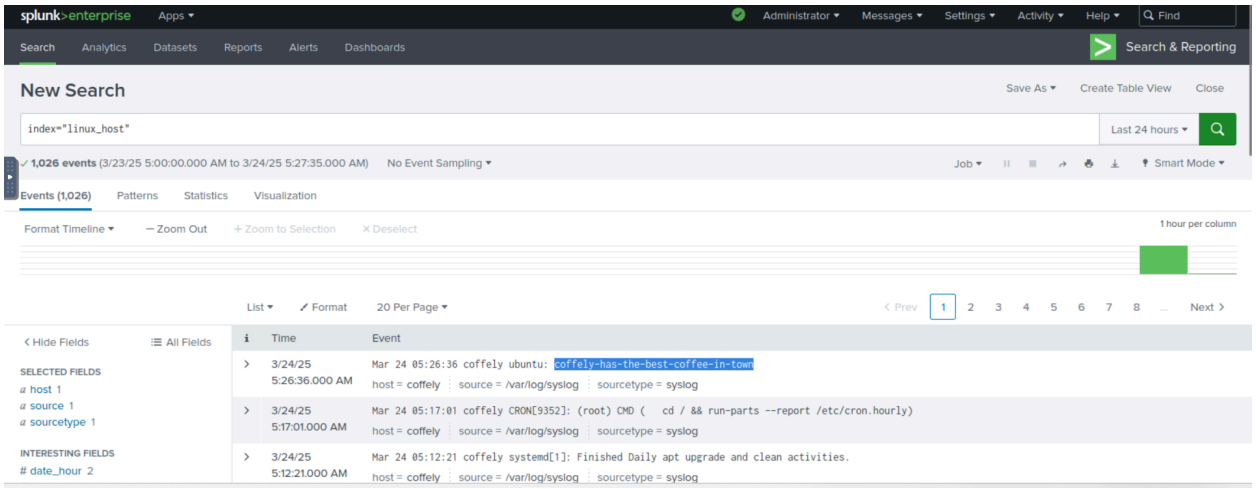
```
root@coffely:/opt/clear/etc/apps/search/local# ls
inputs.conf
root@coffely:/opt/clear/etc/apps/search/local# cat inputs.conf
[monitor:///var/log/syslog]
disabled = false
index = Linux_host
root@coffely:/opt/clear/etc/apps/search/local#
```

Utilizing Logger Utility

Logger is a built-in command line tool to create test logs added to the syslog file. As we are already monitoring the syslog file and sending all logs to Splunk, the log we

generate in the next step can be found with Splunk logs. To run the command, use the following command.

```
root@coffely:/opt/clear/bin# logger "coffely-has-the-best-coffee-in-town"
root@coffely:/opt/clear/bin#  tail -1 /var/log/syslog
Mar 24 05:26:36 coffely ubuntu: coffely-has-the-best-coffee-in-town
```



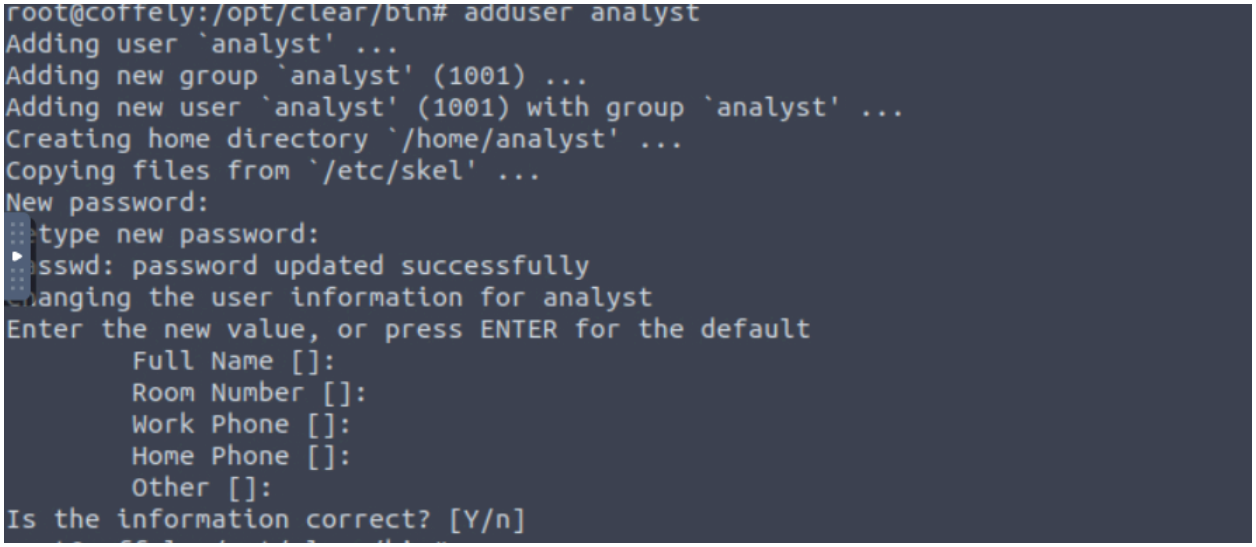
Great, We have successfully installed and configured Splunk Forwarder to get the logs from the syslog file into Splunk.

****

Answer the questions below:
Follow the same steps and ingest /var/log/auth.log file into Splunk index Linux_logs. What is the value in the sourcetype field?
Answer: syslog

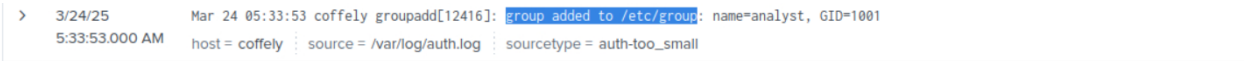
Create a new user named analyst using the command adduser analyst. Once created, look at the events generated in Splunk related to the user creation activity. How many events are returned as a result of user creation?

Answer: 6



What is the path of the group the user is added after creation?

Answer: /etc/group



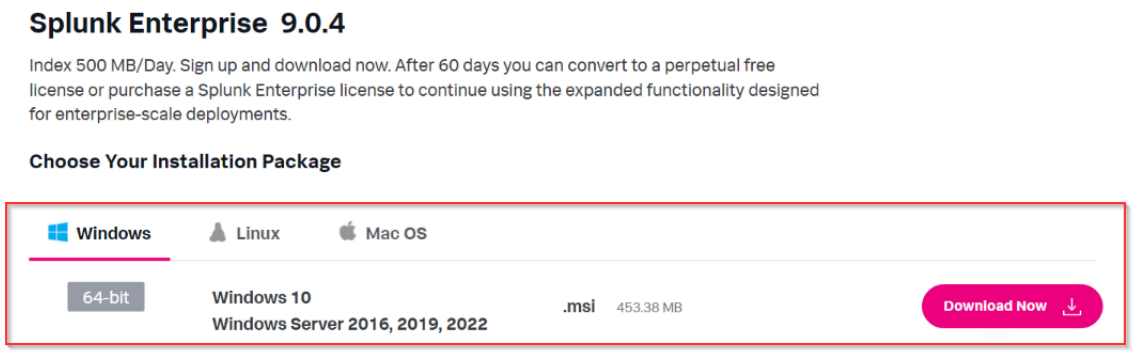
Splunk: Installing on Windows

Installing Splunk on a Windows platform is relatively simple with just running the installer. Connect with the Windows Machine by clicking the Start Machine button on the right. It will take around 3-5 minutes to boot completely and will start in Split-Screen View on the right side of the screen. In case the VM is not visible, use the blue Show Split View button at the top-right of the page.

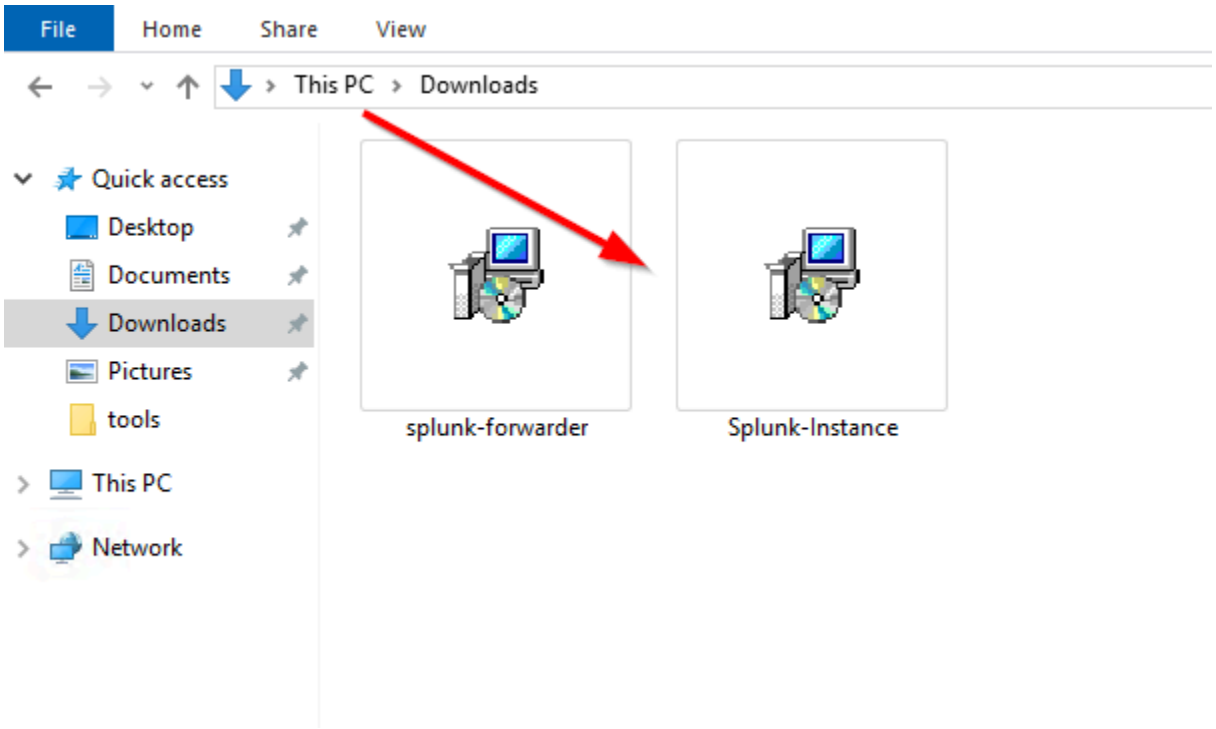
On the Windows machine, we will first install Splunk, configure a forwarder to capture Windows Event logs, and integrate Coffely weblogs to collect all requests and responses into Splunk Instance.

Downloading Splunk Enterprise

The first step would be to log in to the Splunk portal and download the Splunk Enterprise instance from the website, as shown below:

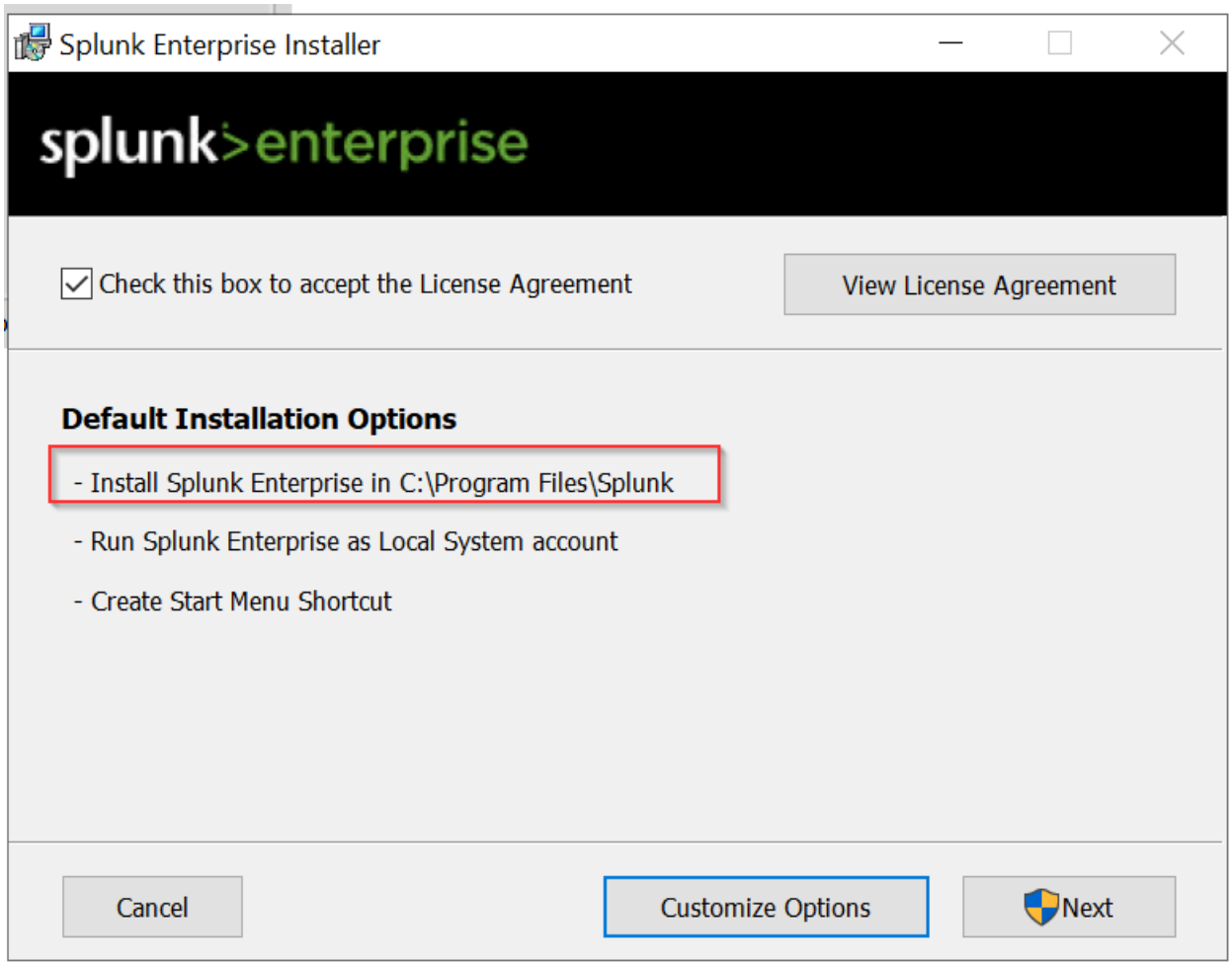


The installer Splunk-Instance is already been downloaded and placed in the Downloads folder to speed up the process.



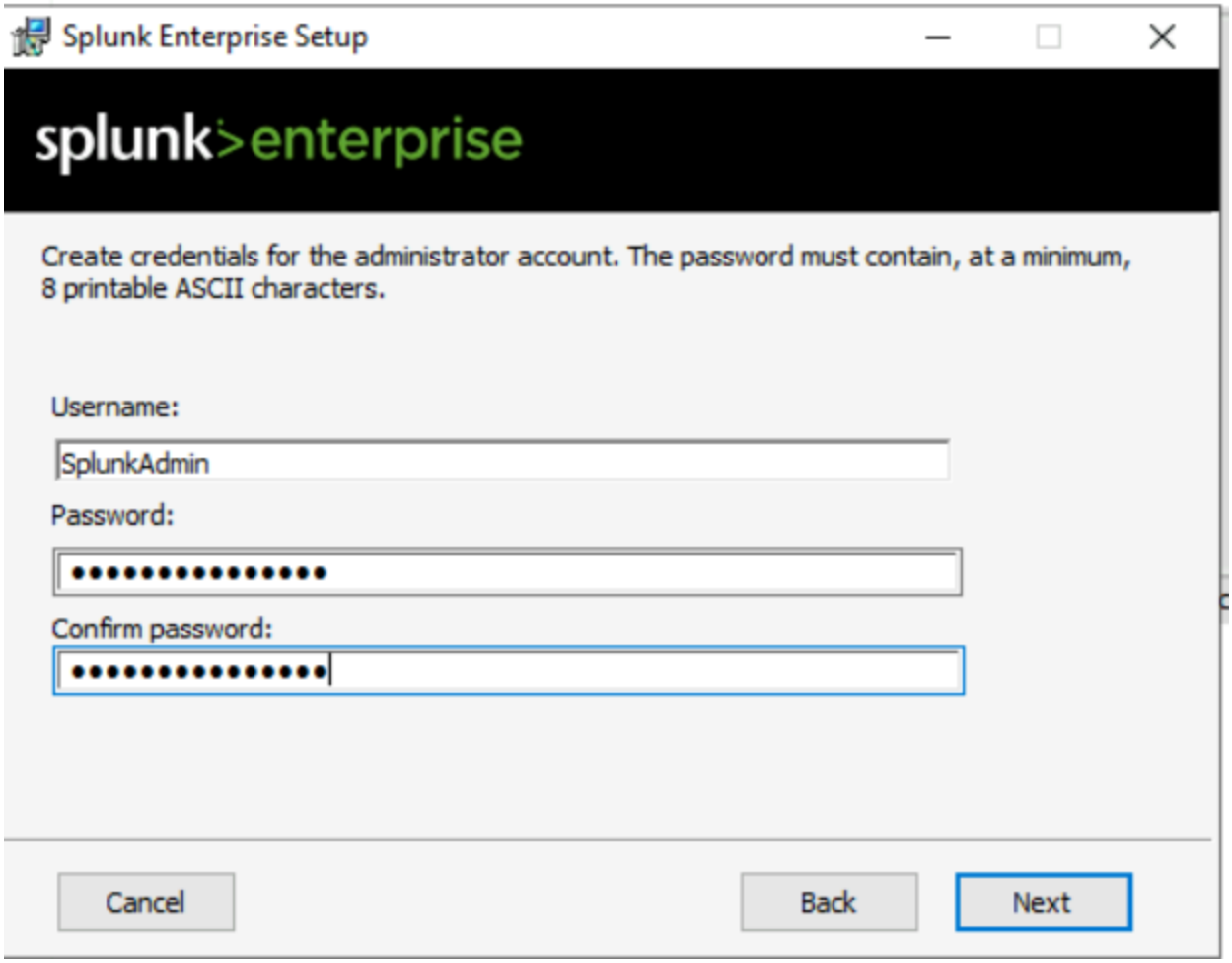
Run the Splunk-Instance installer. By default, it will install Splunk in the folder C:\Program Files\Splunk. This will check the system for dependencies and will take 5-8 minutes to install the Splunk instance.

First, click the Check this box to accept the License Agreement and click Next.

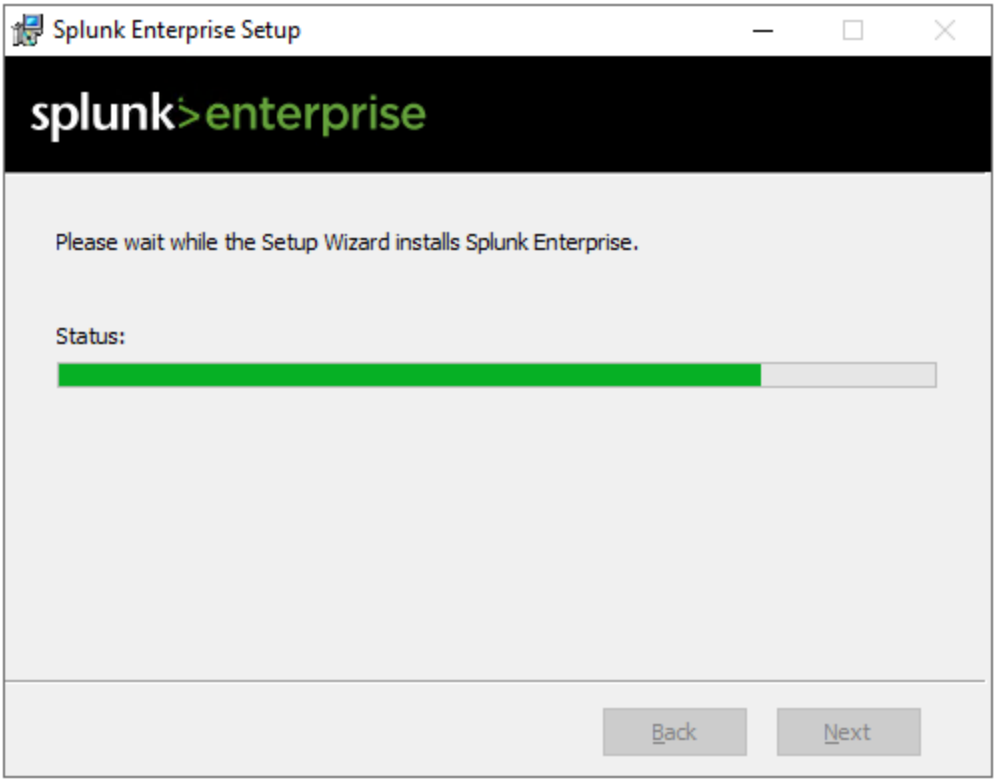


Create Administrator Account

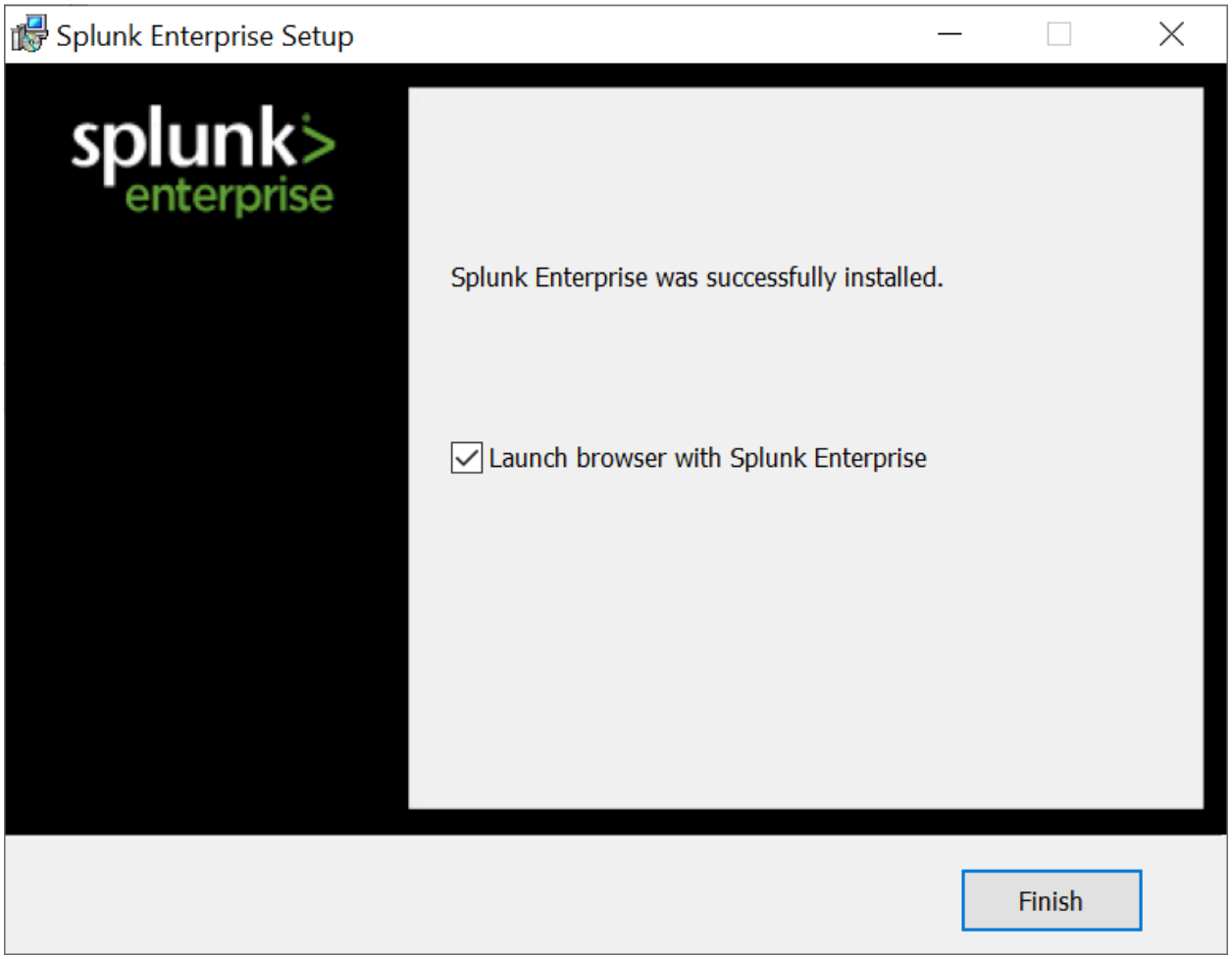
The important step during installation is creating an administrator account, as shown below. This account will have high privileges, create and manage other accounts, and control all administrative roles.



It will look for the system requirement for compatibility and other checks.



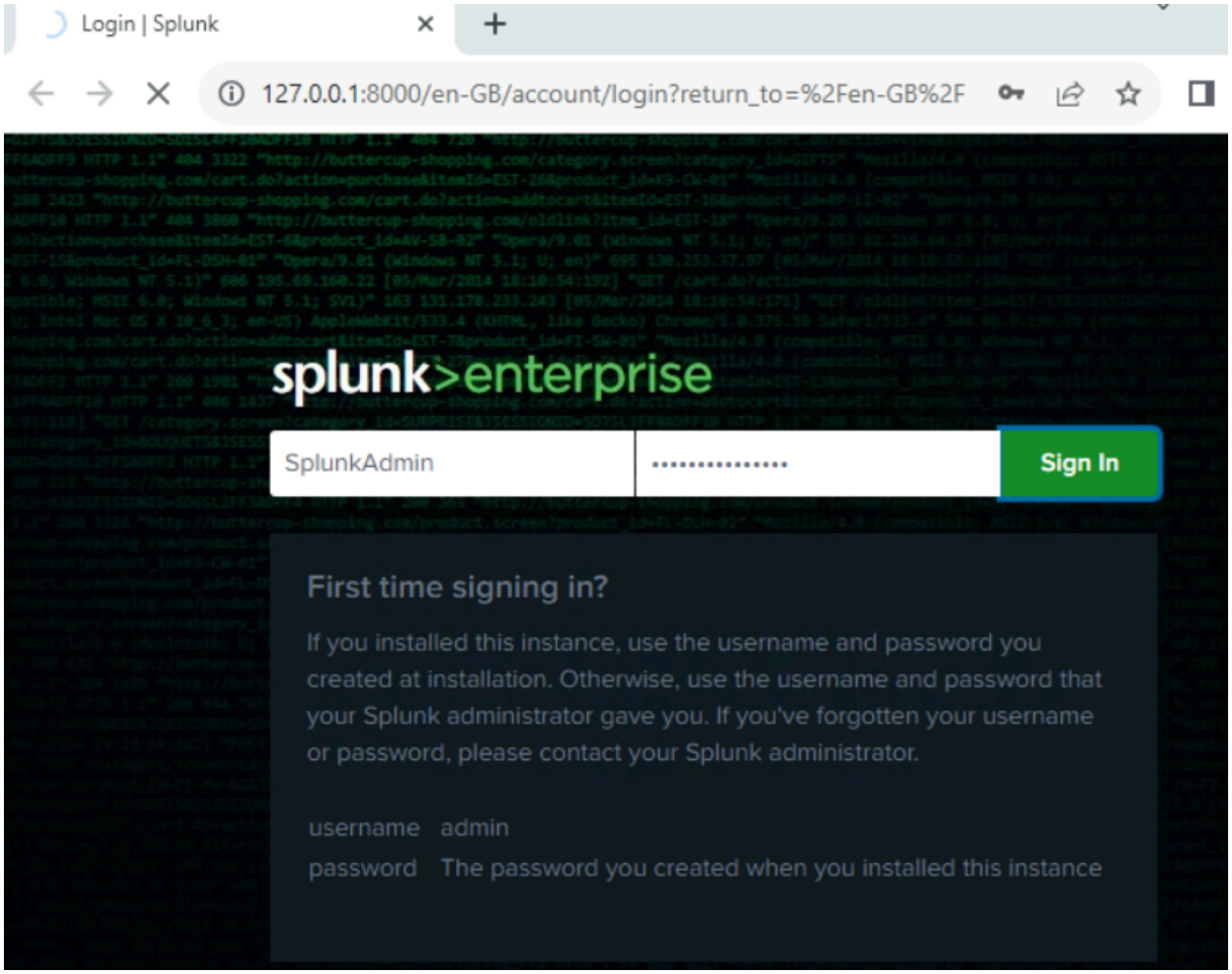
We will get the following message if all system requirements are met, and installation is complete.



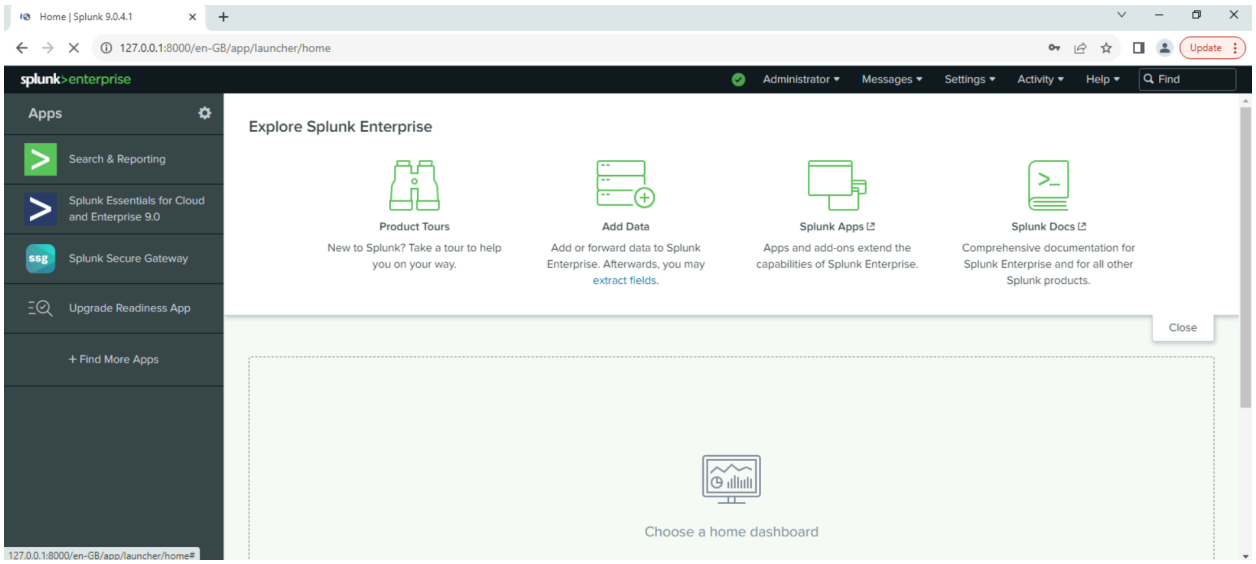
Accessing Splunk Instance

Splunk is installed on port 8000 by default. We can change the port during the installation process as well. Now open the browser in the lab and go to the URL HTTP://127.0.0.1:8000. If you are connected with the VPN, then you can also access the newly installed Splunk Instance in your browser by going to

HTTP://10.10.100.188:8000



Use the credentials created during the installation process to get the Splunk dashboard.



Great. We have successfully installed Splunk on a Windows OS. In the next task, we will follow similar steps we did during Linux Lab to install Splunk Forwarder.

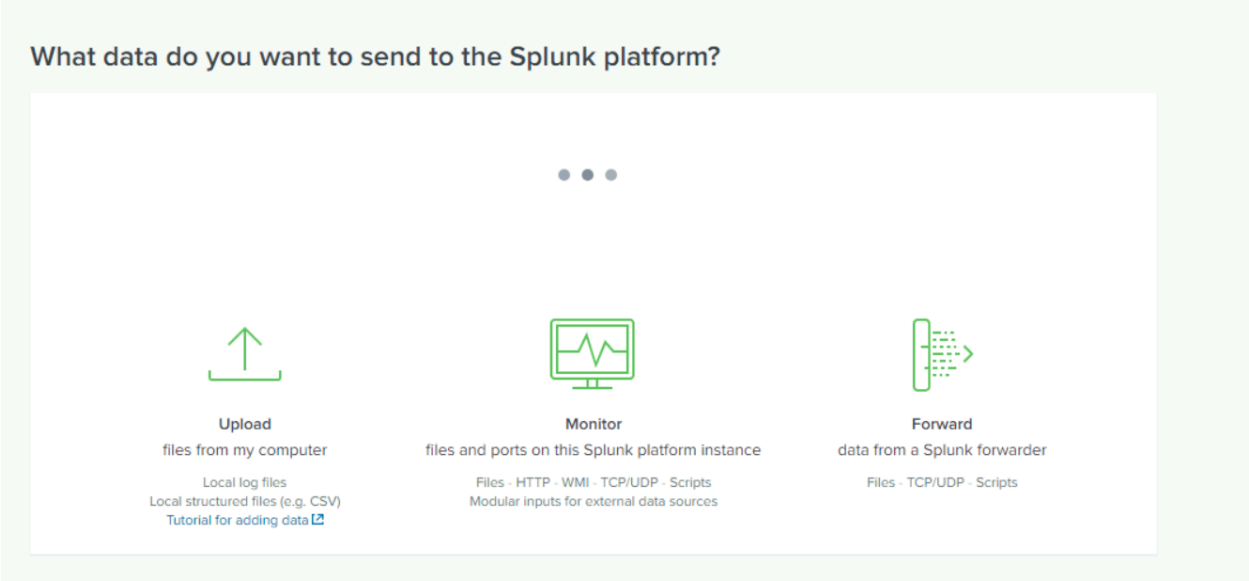
****

Answer the questions below:

What is the default port Splunk runs on?

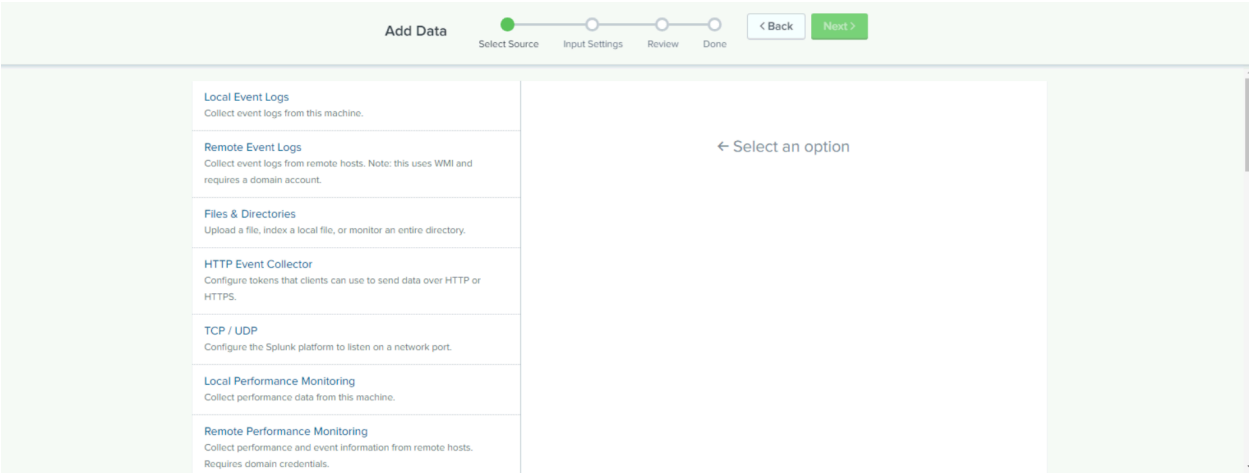
Answer: 8000

Click on the Add Data tab; how many methods are available for data ingestion?



Answer: 3

Click on the Monitor option; what is the first option shown in the monitoring list?



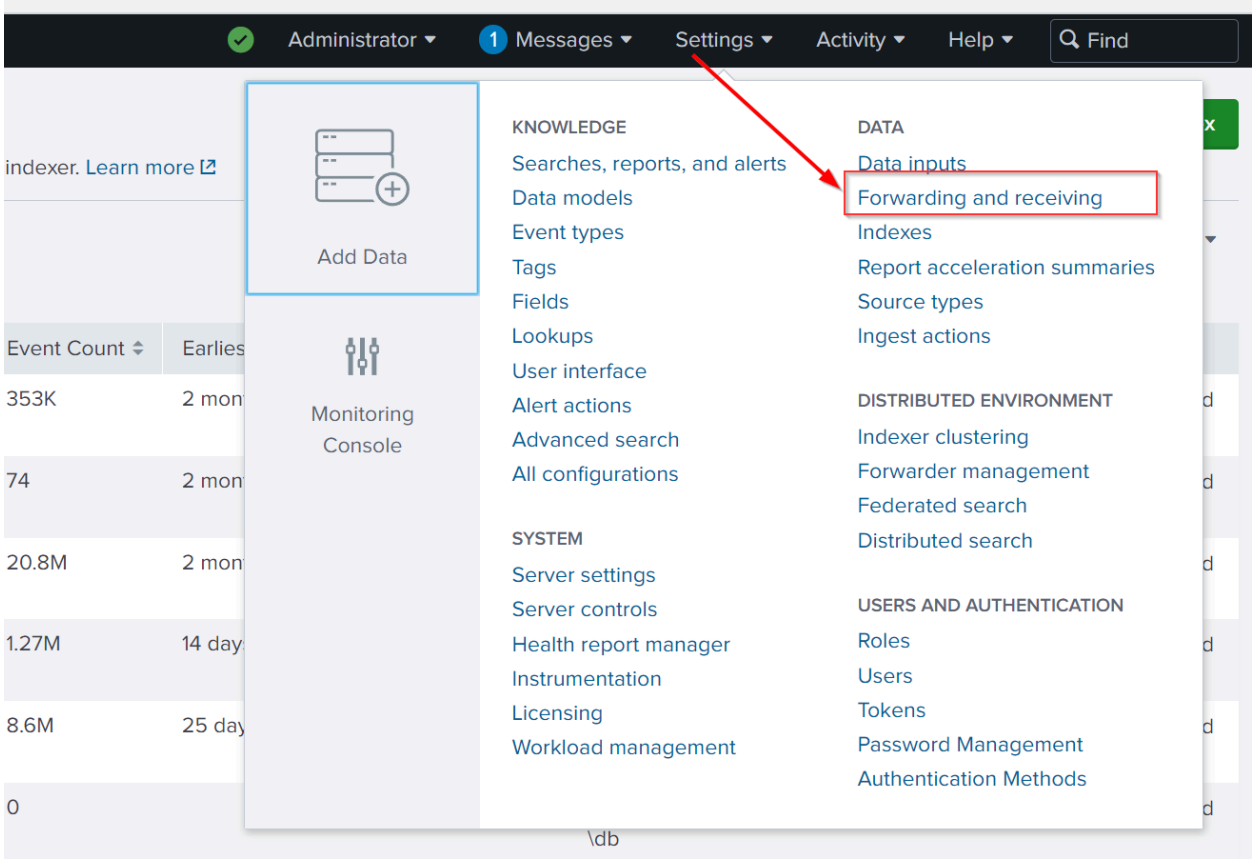
Answer: Local Event Logs

Installing and Configuring Forwarder

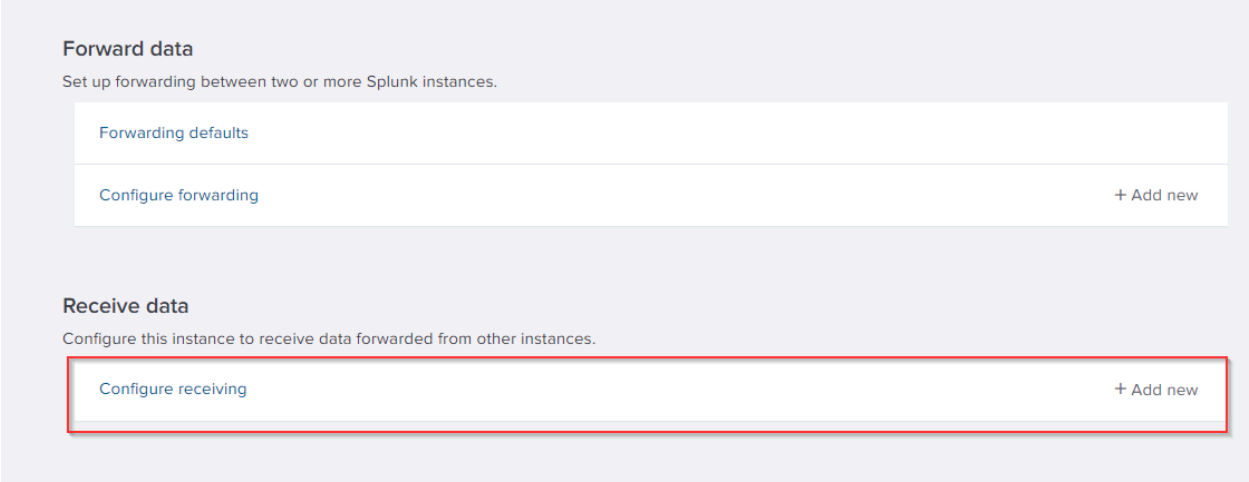
First, we will configure the receiver on Splunk so the forwarder knows where to send the data.

Configure Receiving

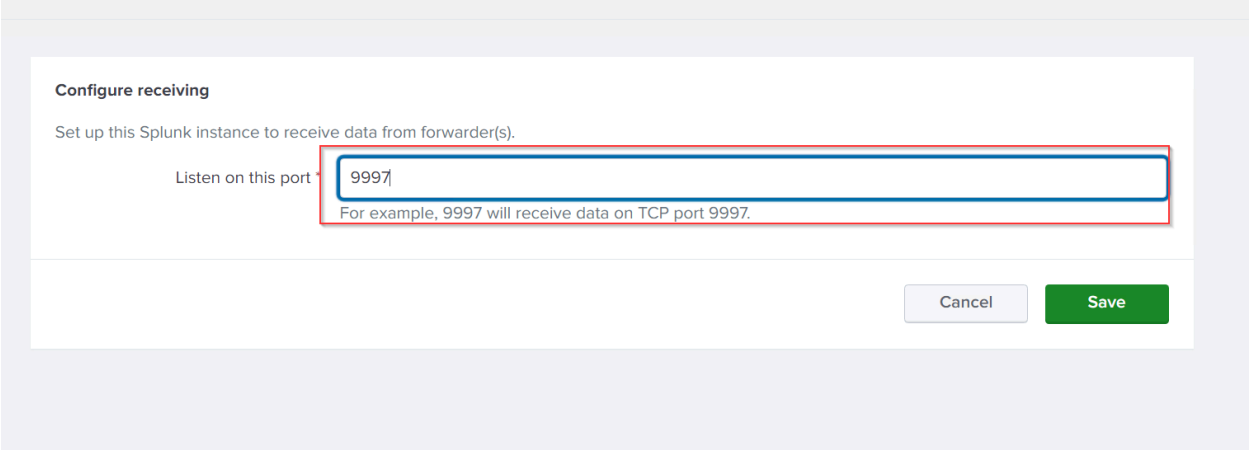
Log into Splunk and Go to Settings -> Forward and receiving tab as shown below:



It will show multiple options to configure both forwarding and receiving. As we want to receive data from the Windows Endpoint, we will click on Configure receiving and then proceed by configuring a new receiving port.

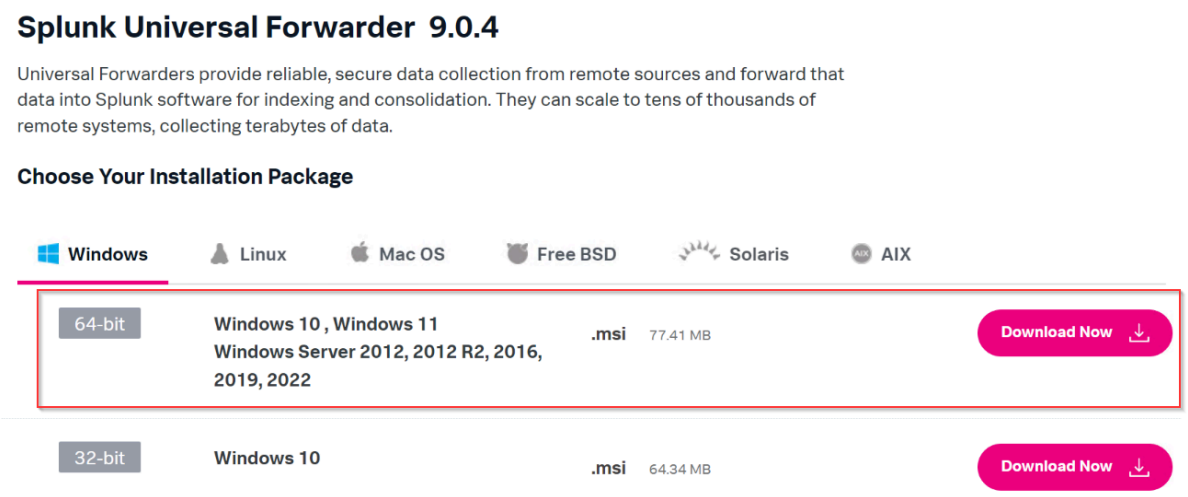


By default, the Splunk instance receives data from the forwarder on port 9997. It's up to us to use this port or change it. For now, we will configure our Splunk to start listening on port 9997 and Save, as shown below:

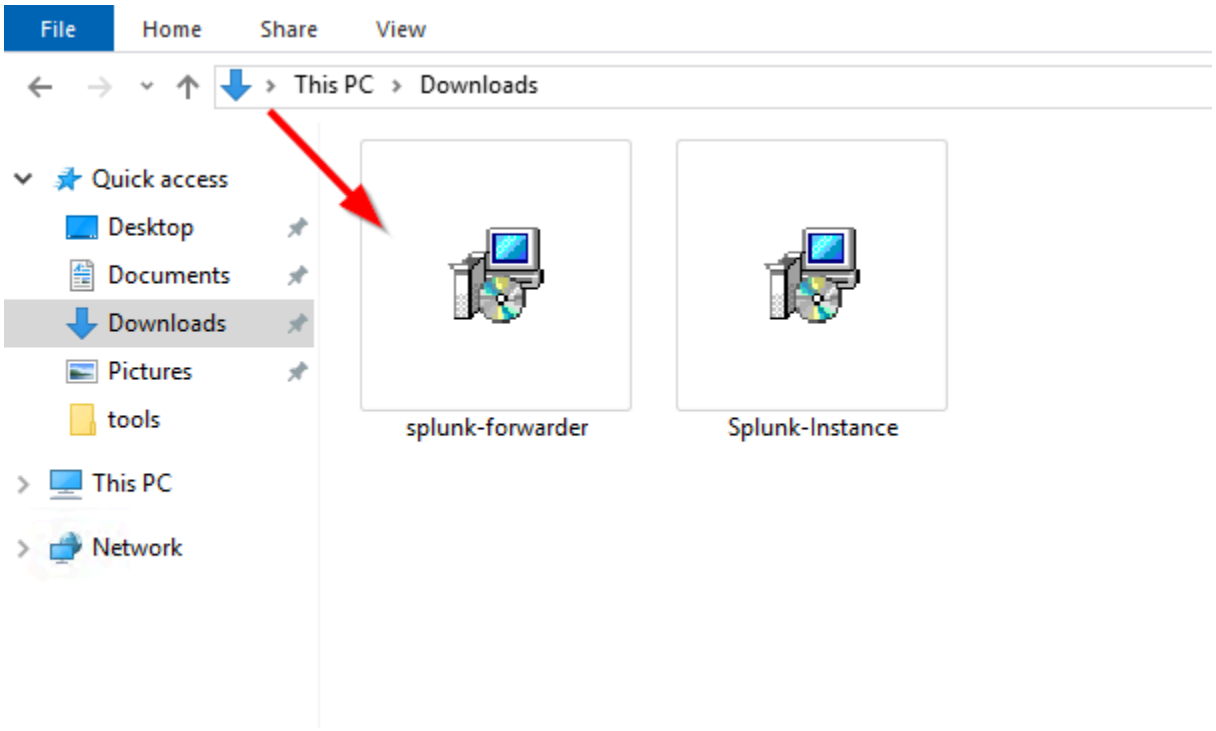


Installing Splunk Forwarder

Installing Splunk Forwarder is very straightforward. First, we will download the latest forwarder from the official website here. As of writing this, Splunk Forwarder 9.0.4 is the newest version available on the site.

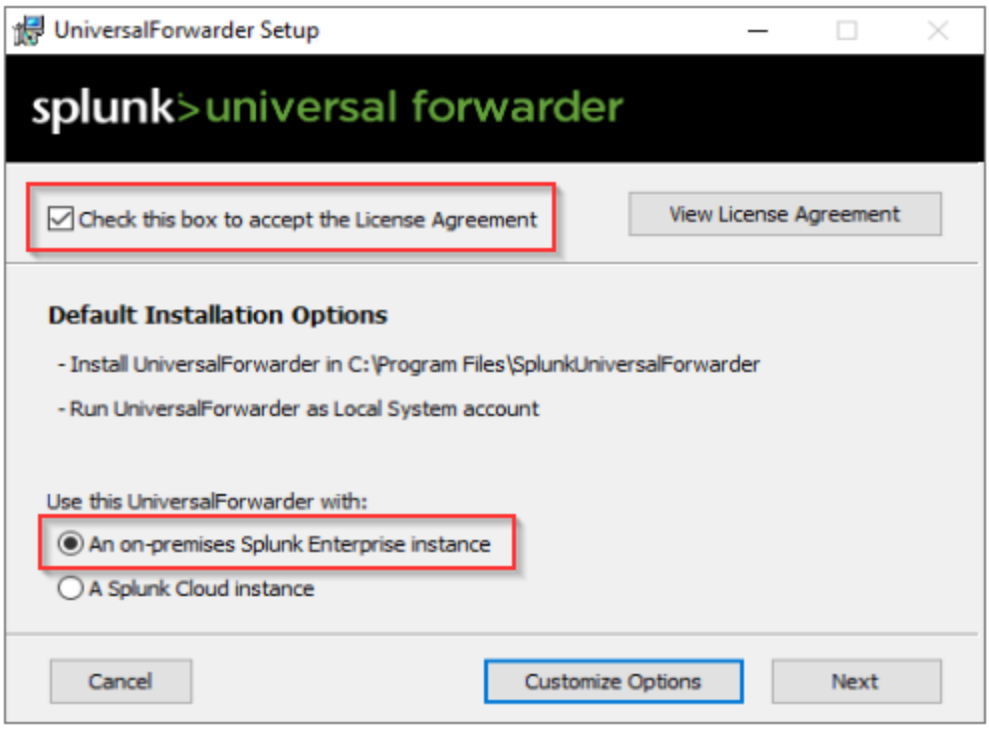


For this lab, the forwarder is already downloaded and placed in the Downloads folder, as shown below:

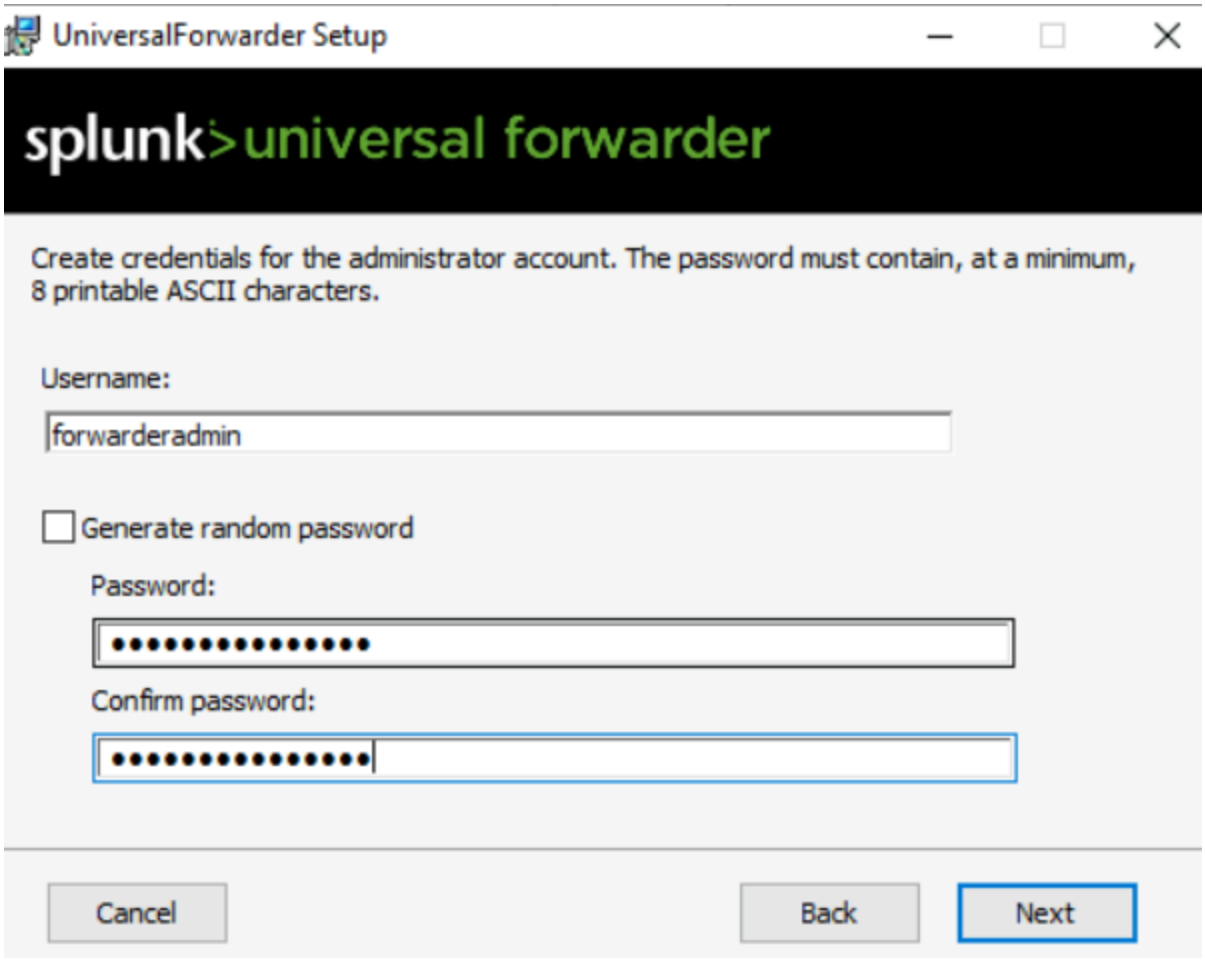


Installation Process

Click on the installer and begin installing Splunk Forwarder, as shown below. Don't forget to click the Check this box to accept the License Agreement. Select the Select the On-Premises Option as we are installing it on an on-premises appliance.

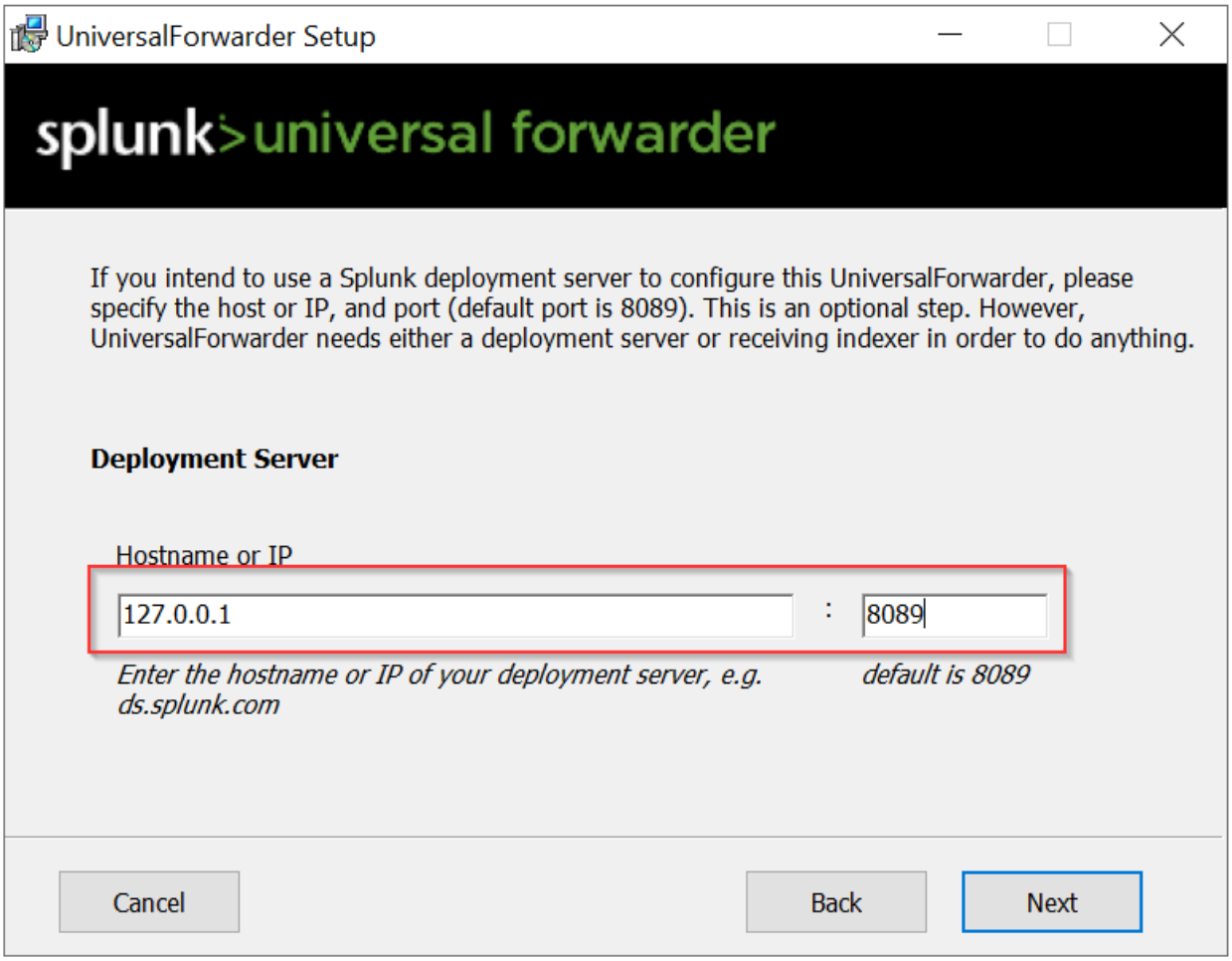


Create an account for Splunk Forwarder. This will be used when connecting the Splunk forwarder to the Splunk Indexer.



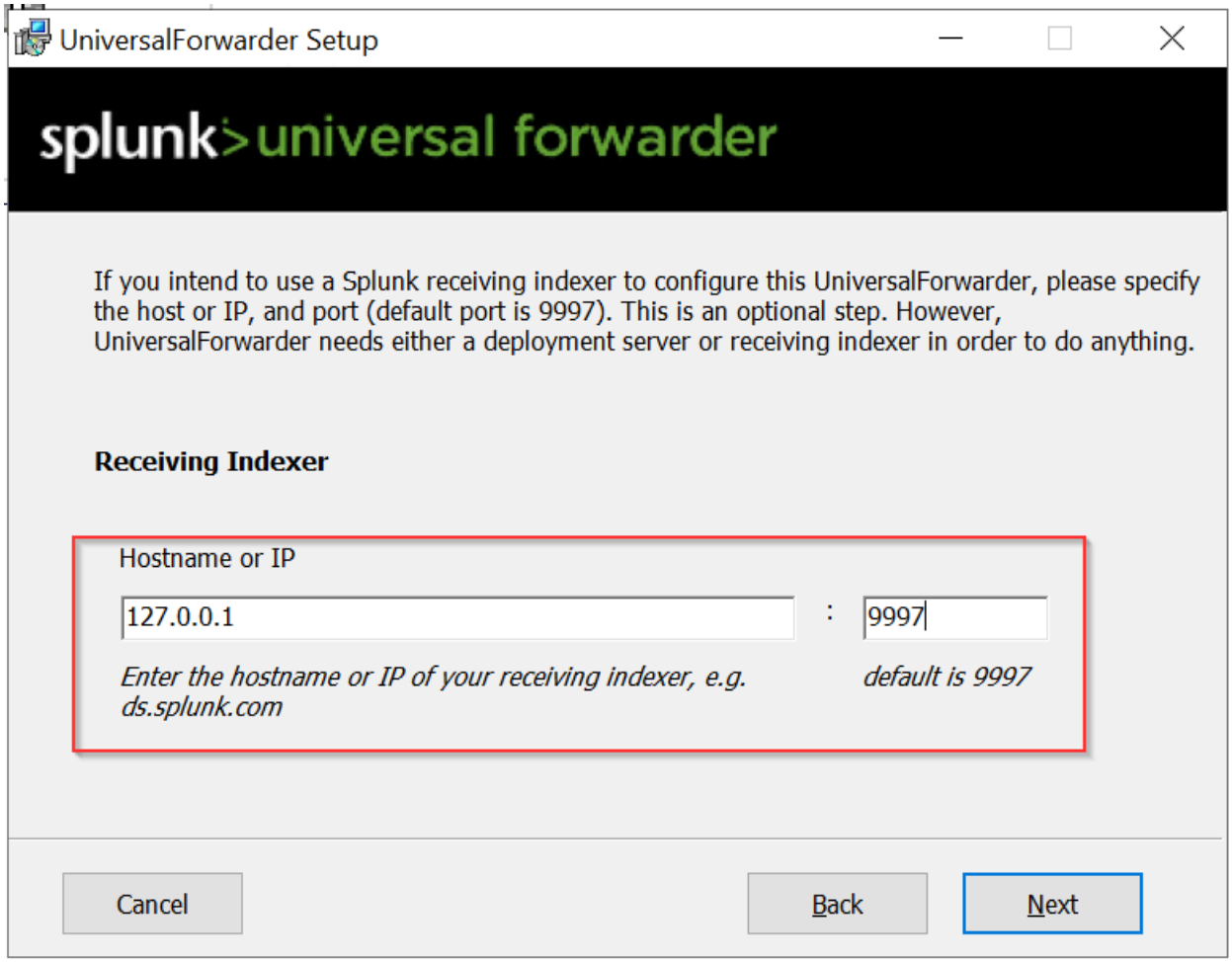
Setting up Deployment Server

This configuration is important if we install Splunk forwarder on multiple hosts. We can skip this step as this step is optional.

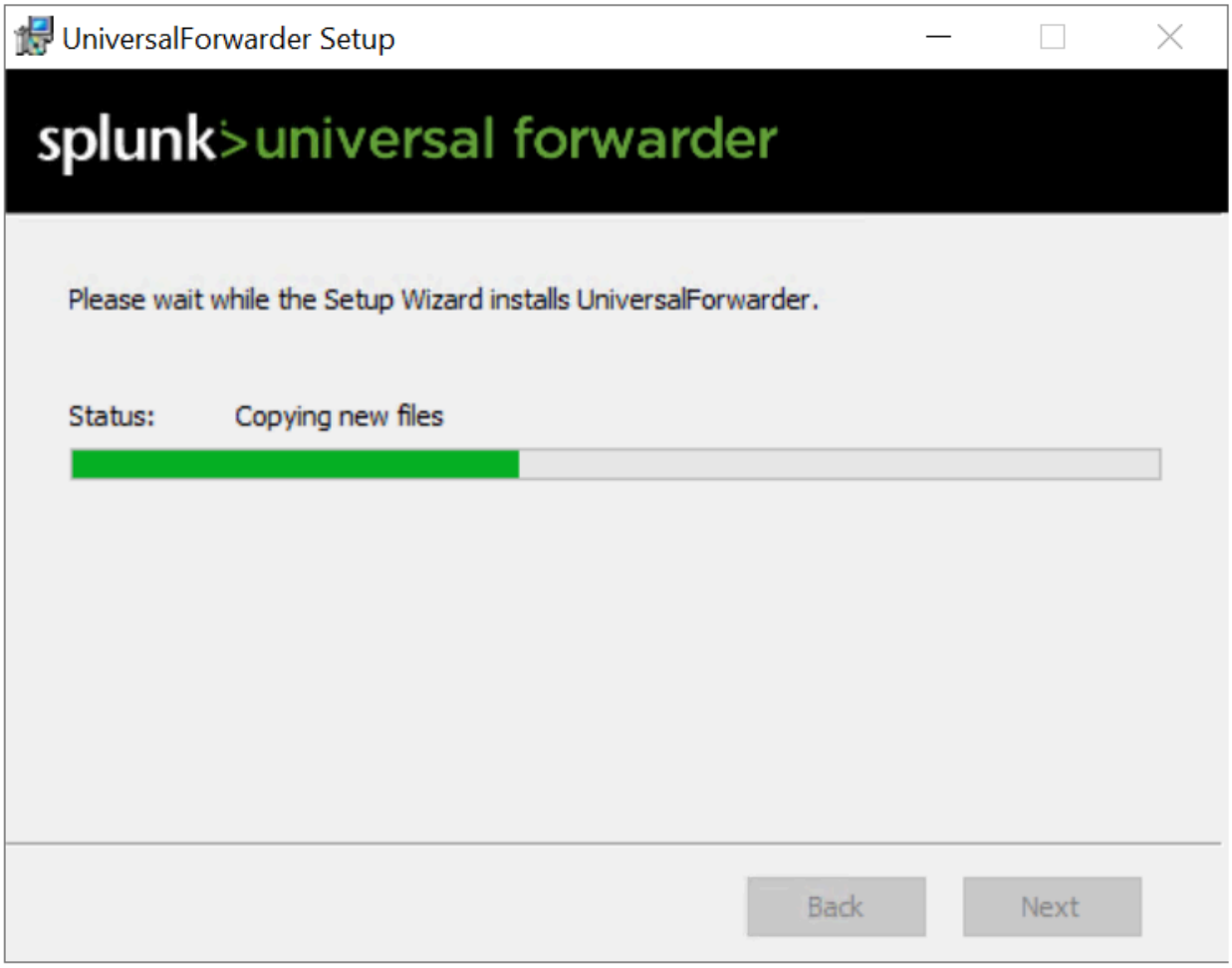


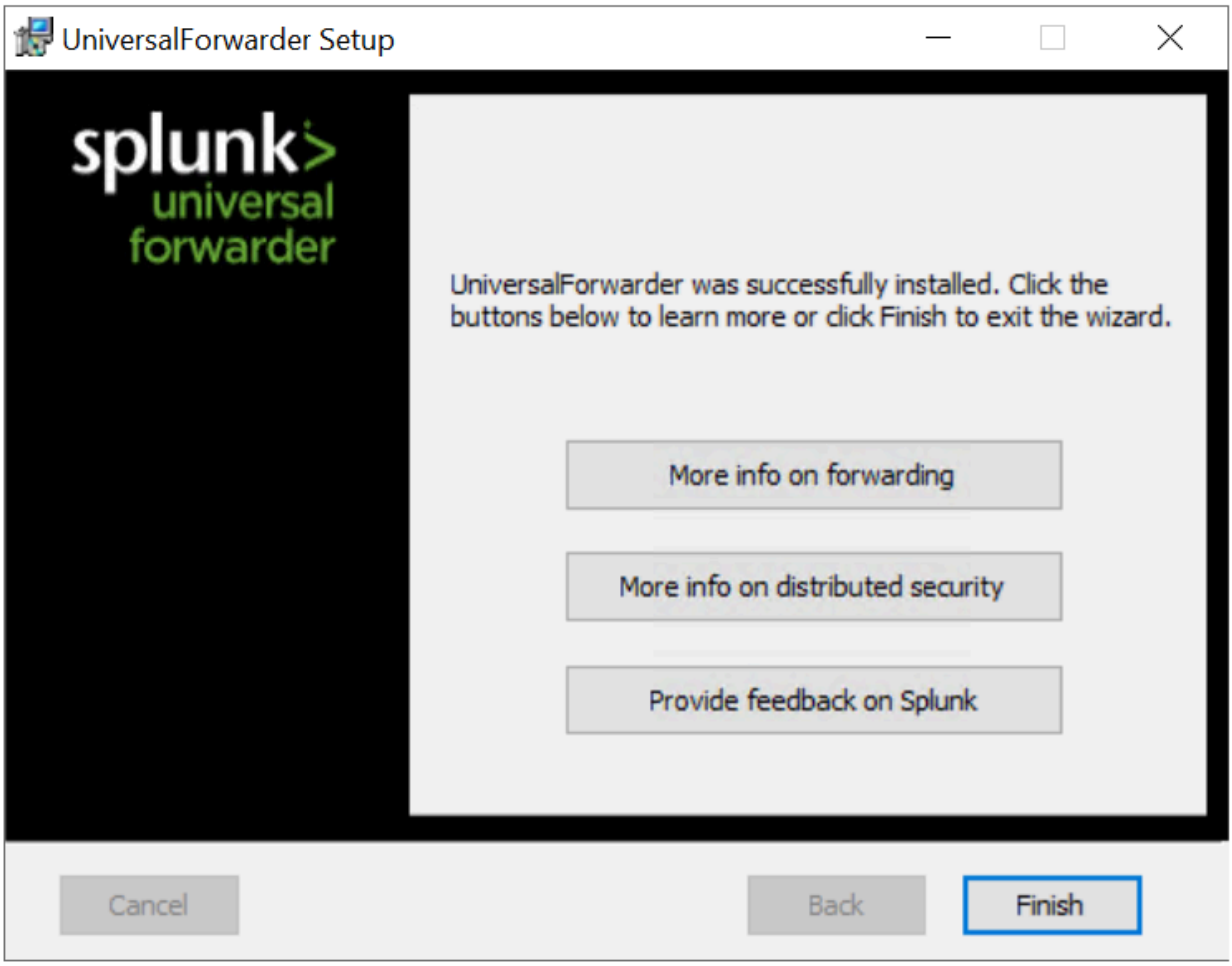
Setting up Listener

We must specify the server's IP address and port number to ensure that our Splunk instance gets the logs from this host. By default, Splunk listens on port 9997 for any incoming traffic.

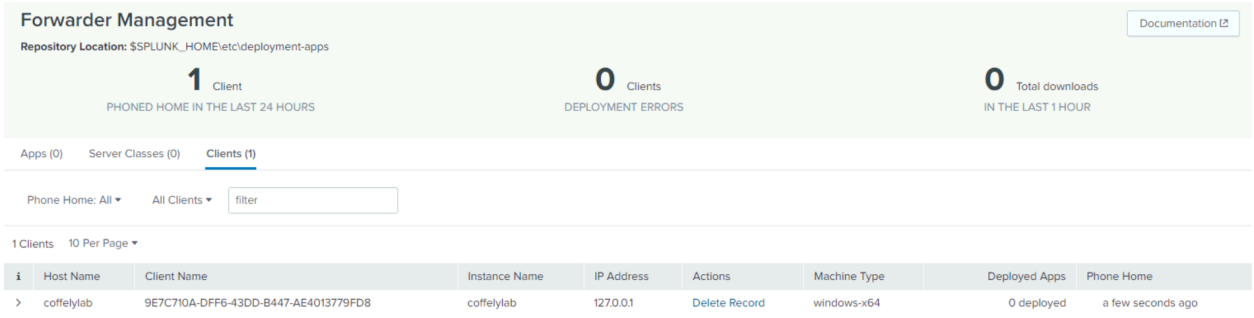


Installing the forwarder on a Windows endpoint will take 3-5 minutes.


UniversalForwarder Setup
splunk>universal forwarder
Please wait while the Setup Wizard installs UniversalForwarder.
Status: Copying new files
Back
Next



If we had provided the information about the deployment server during the installation phase, our host details would be available in the Settings -> Forwarder Management tab, as shown below:



Now that Splunk forwarder is installed, we will now configure our forwarder to send logs to our Splunk instance in the upcoming tasks.

****

Answer the questions below:

What is the full path in the C:\Program Files where Splunk forwarder is installed?

Answer: C:\Program Files\SplunkUniversalForwarder

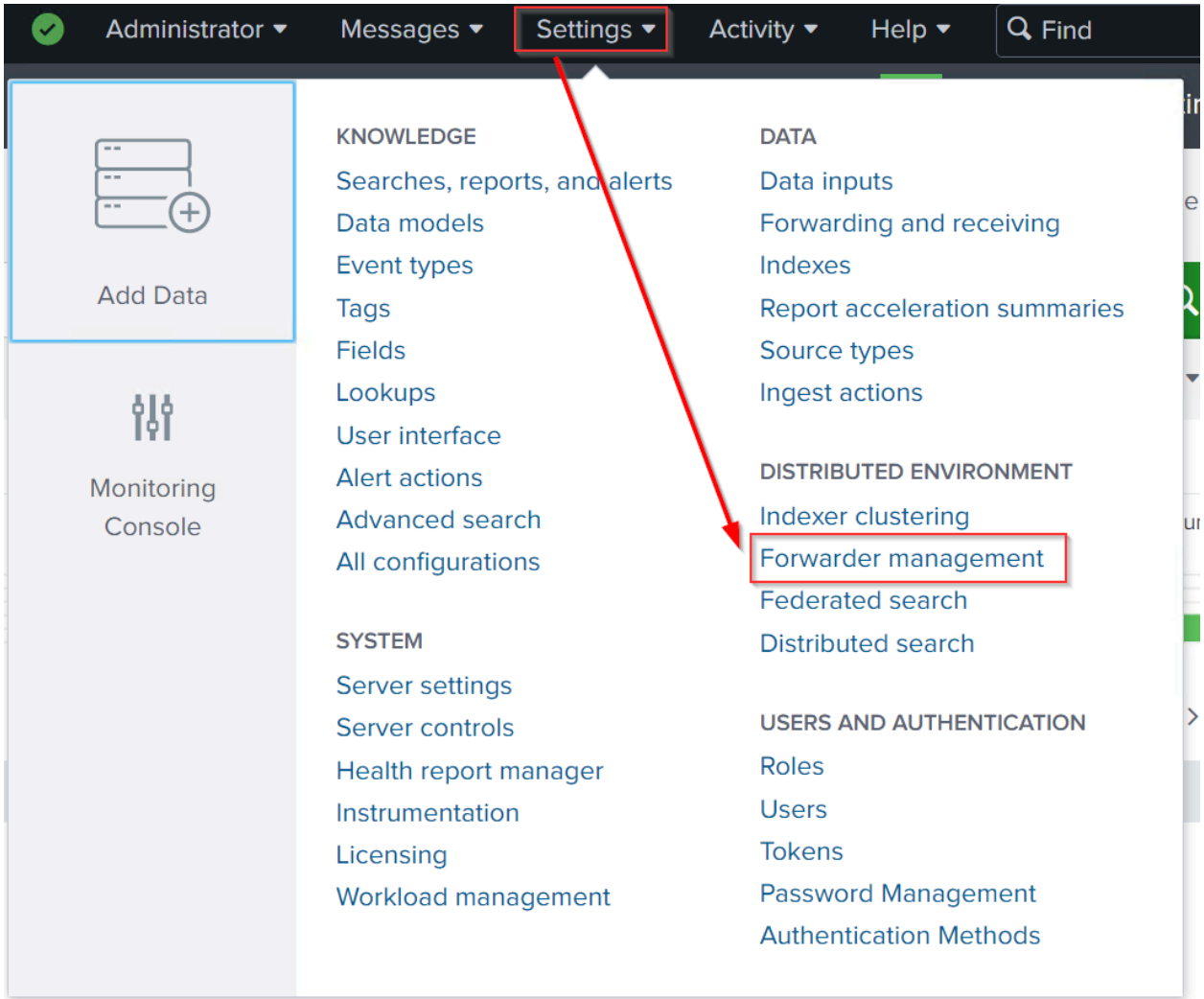
What is the default port on which Splunk configures the forwarder?
Answer: 9997

Splunk: Ingesting Windows Logs

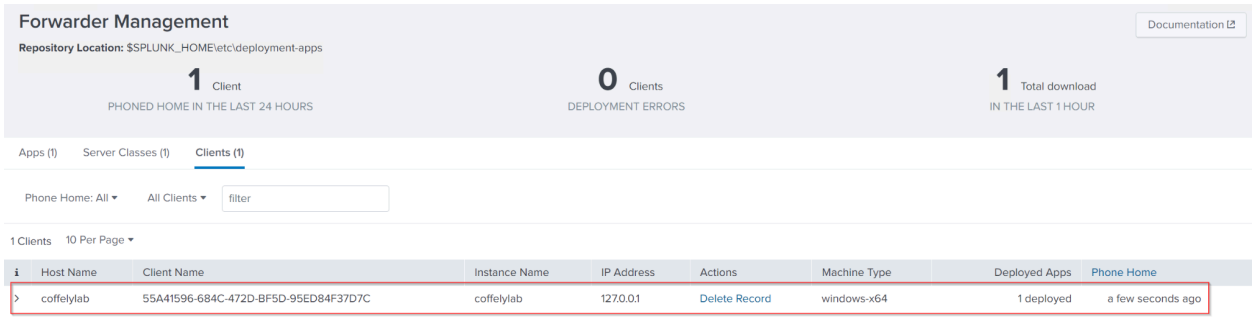
We have installed the forwarder and set up the listener on Splunk. It's time to configure Splunk to receive Event Logs from this host and configure the forwarder to collect Event Logs from the host and send them to the Splunk Indexer. Let's go through this step by step.

Check Forwarder Management

The Forwarder Management tab views and configures the deployment of servers/hosts.



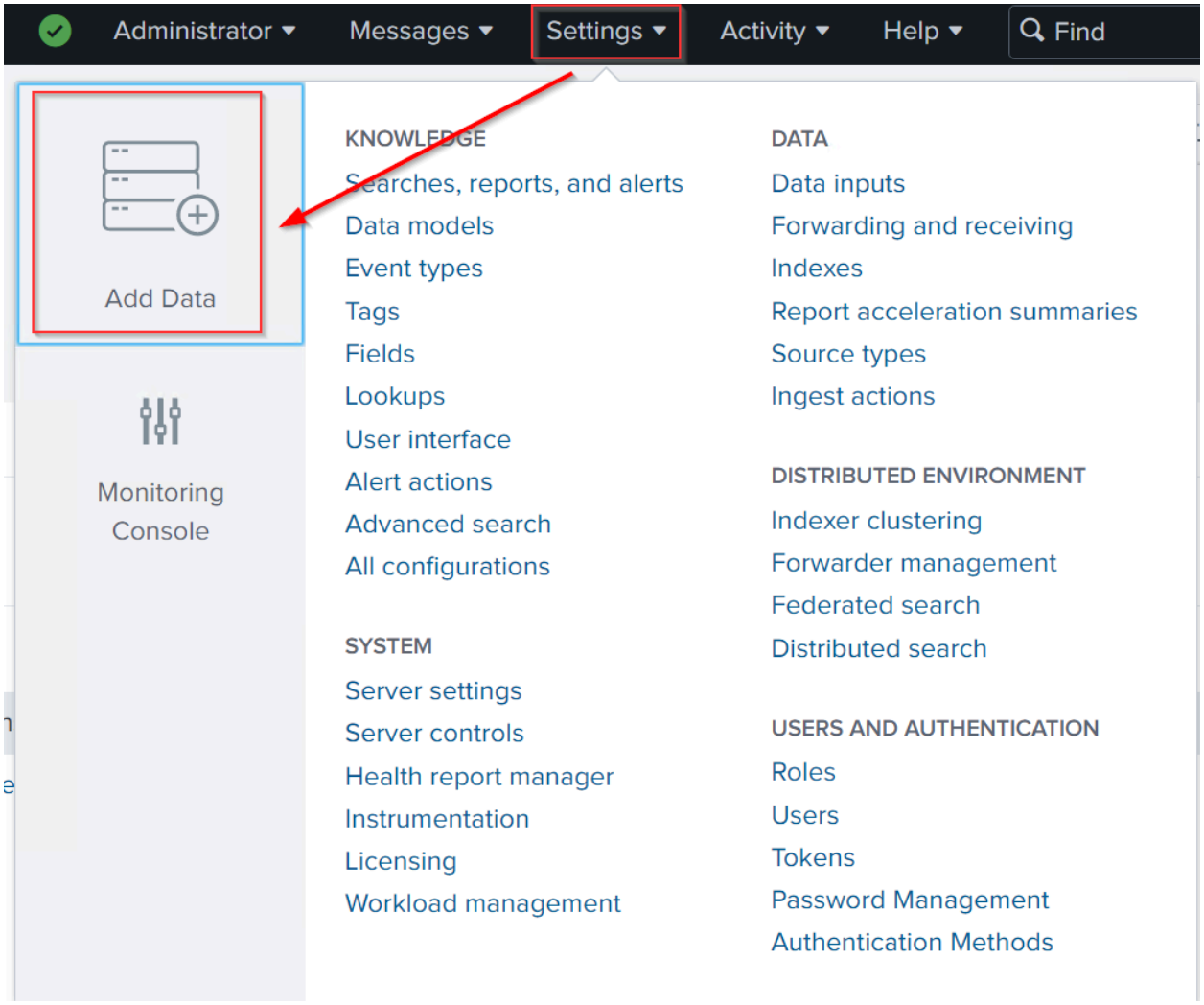
Go to settings -> Forwarder Management tab to get the details of all deployment hosts. In an actual network, this tab will be filled with all the hosts and servers configured to send logs to Splunk Indexer.



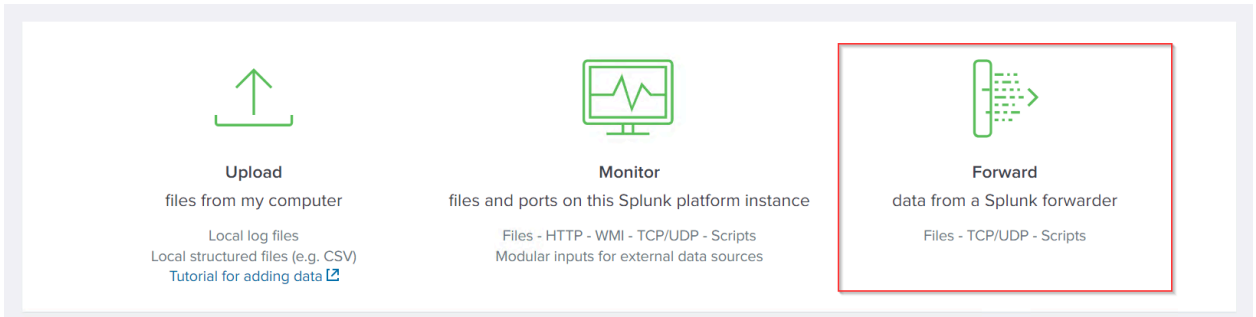
It will appear here if we have properly configured the forwarder on the host. Now it's time to configure Splunk to receive the Event Logs.

Select Forwarder

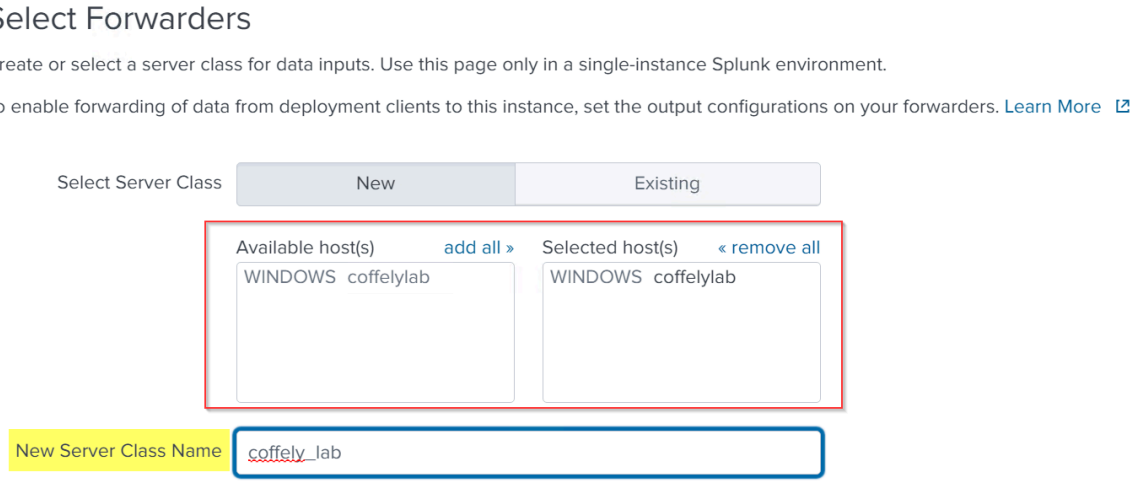
Click on Settings -> Add data. It shows all the options to add data from different sources.



It provides us with three options for selecting how to ingest our data. We will choose the Forward option to get the data from Splunk Forwarder.

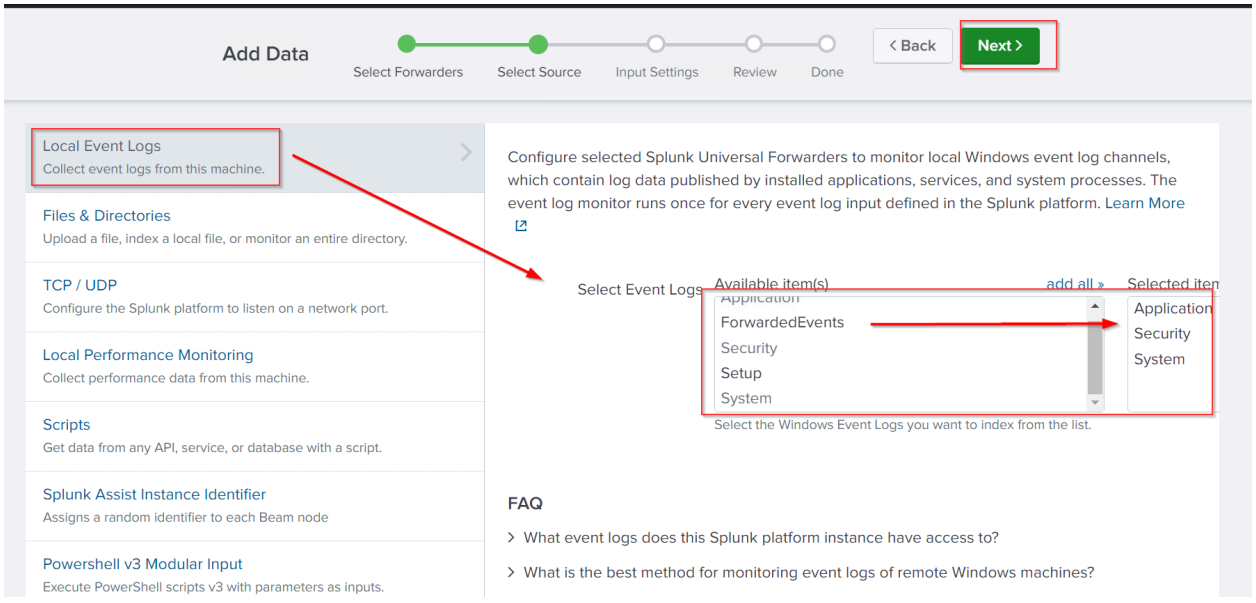


In the Select Forwarders section, Click on the host coffelylab shown in the Available host(s) tab, and it will be moved to the Selected host(s) tab. Then, click Next.



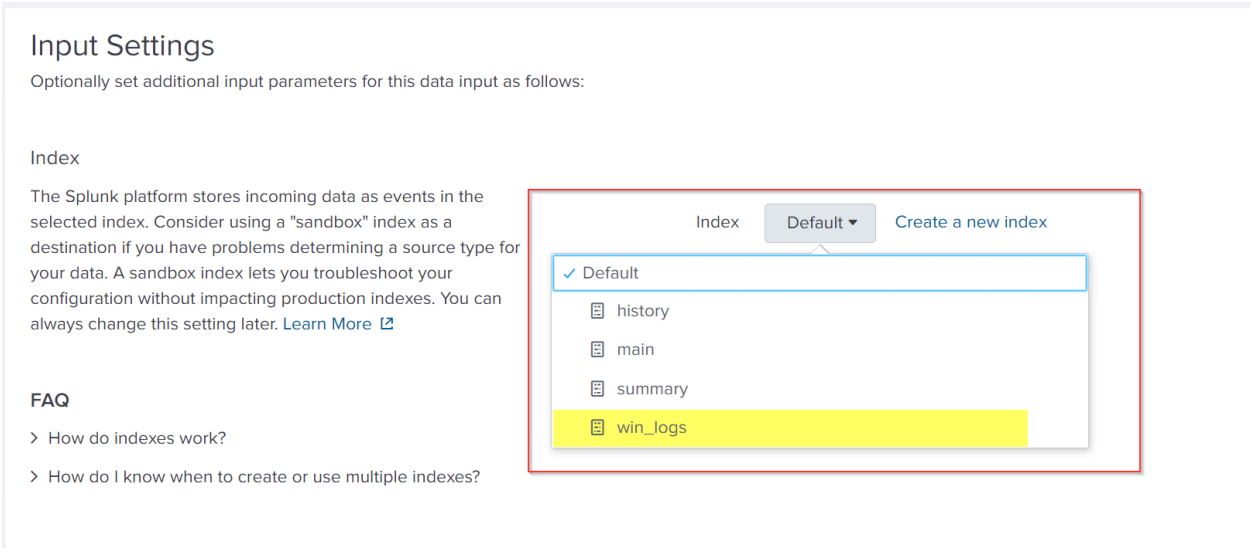
Select Source

It's time to select the log source that we need to ingest. The list shows many log sources to choose from. Click on Local Event Logs to configure receiving Event Logs from the host. Different Event Logs will appear in the list to choose from. As we know, various Event Logs are generated by default on the Windows host. More about Event Logs can be learned in this Windows Event Logs room. Let's select a few of those and move to the next step.



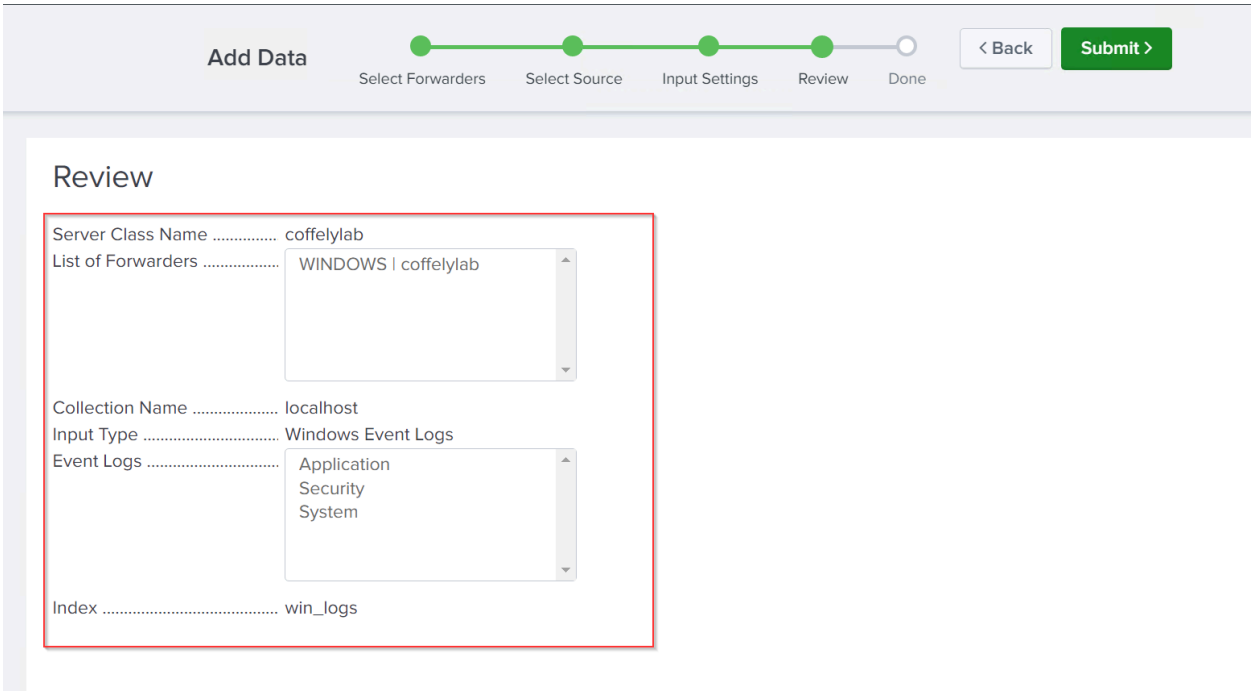
Creating Index

Create an index that will store the incoming Event logs. Once created, select the Index from the list and move to the next step.

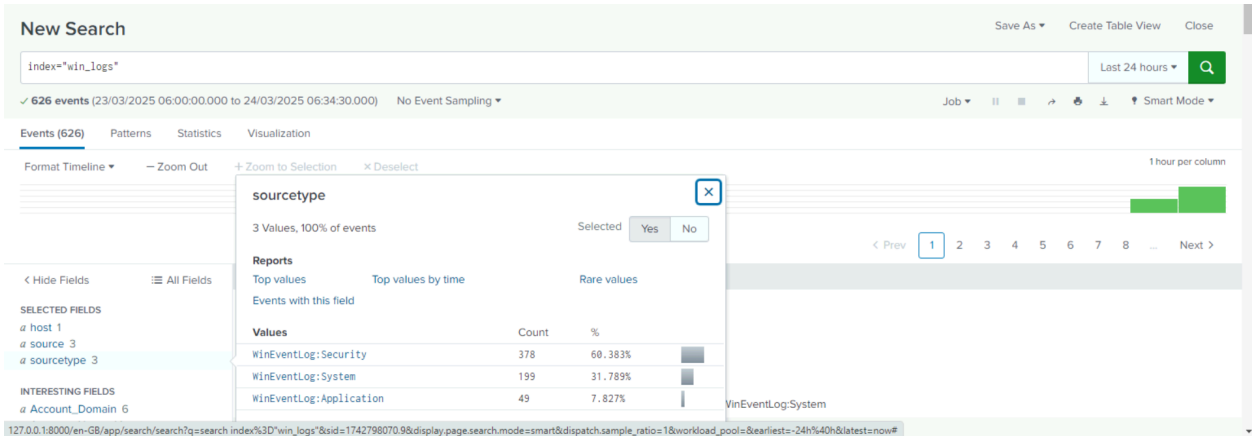


Review

The review tab summarizes the settings we just did to configure Splunk. Move to the next step.



Click on the Start Searching tab. It will take us to the Search App. If everything goes smoothly, we will receive the Event Logs immediately.



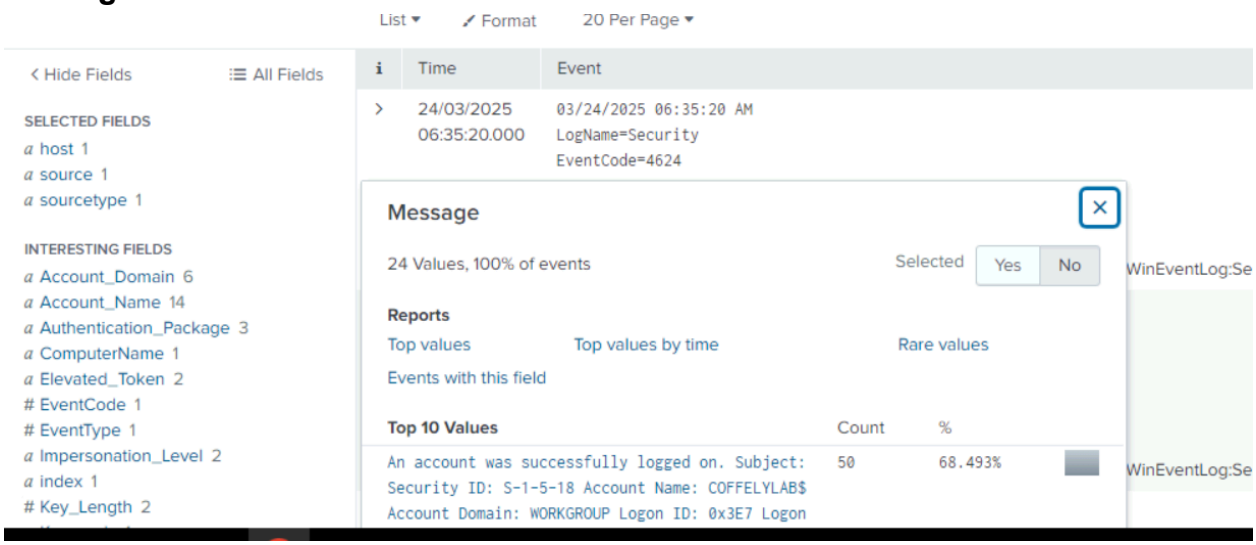
****

Answer the questions below:

While selecting Local Event Logs to monitor, how many Event Logs are available to select from the list to monitor?

Answer: 5

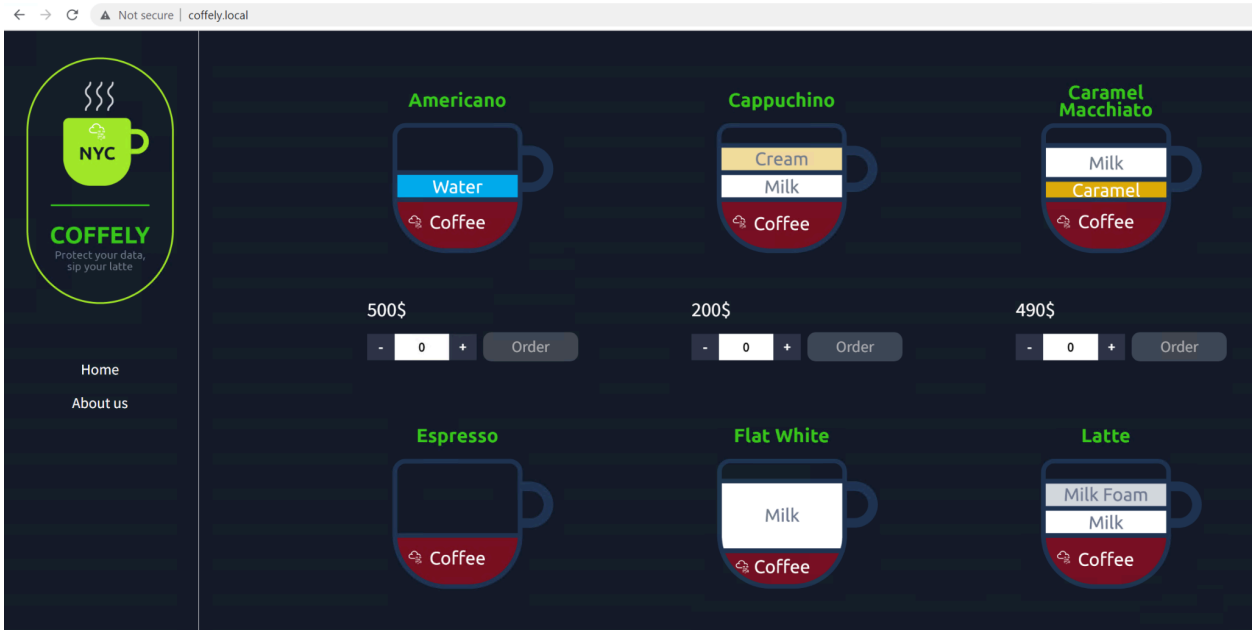
Search for the events with EventCode=4624. What is the value of the field Message?



Answer: An account was successfully logged on.

Ingesting Coffely Web Logs

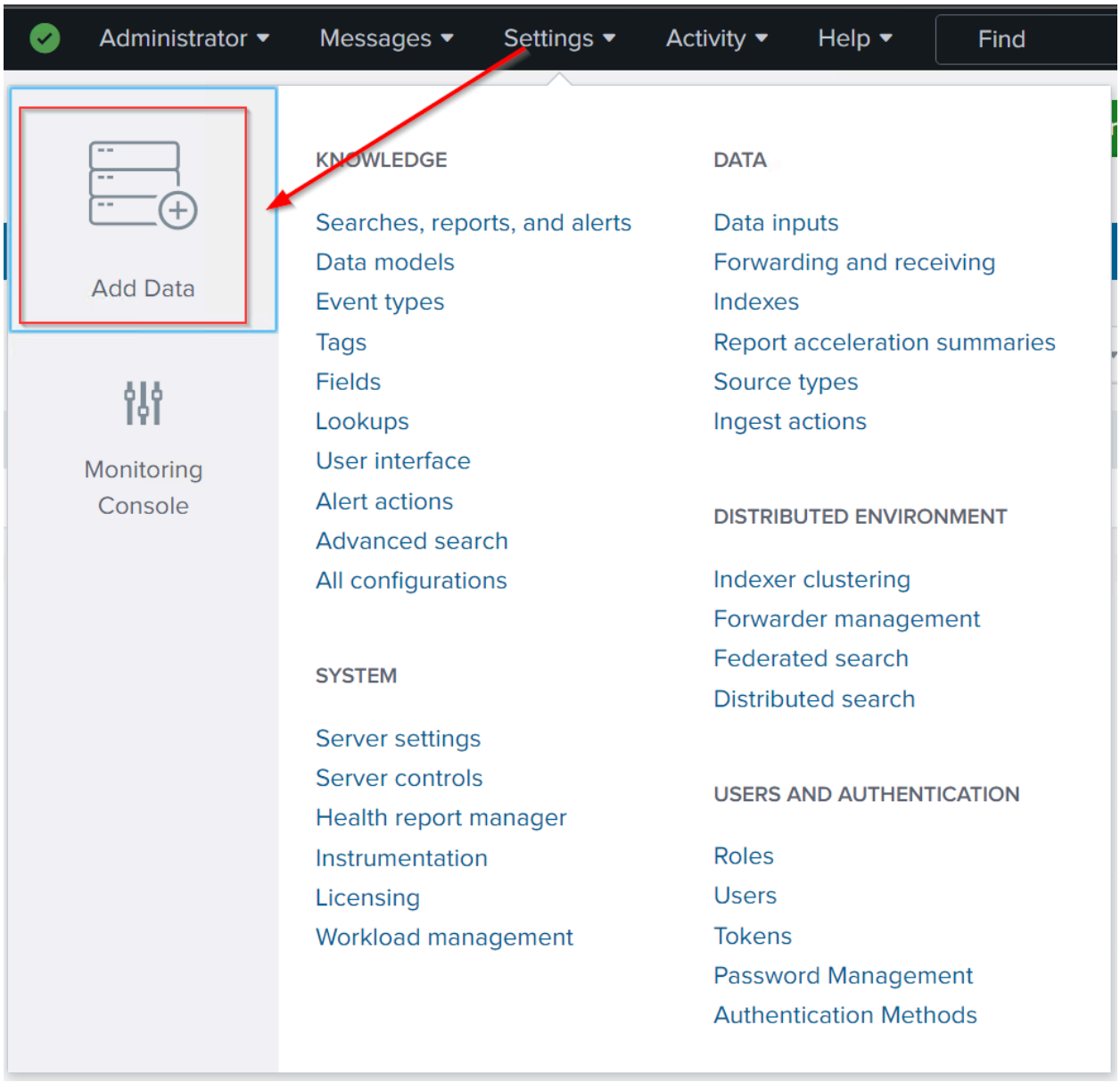
The Windows host we connected to Splunk Instance also hosts a local copy of their website, which can be accessed via http://coffely.thm from the VM and is in the development phase. You are asked to configure Splunk to receive the weblogs from this website to trace the orders and improve coffee sales.



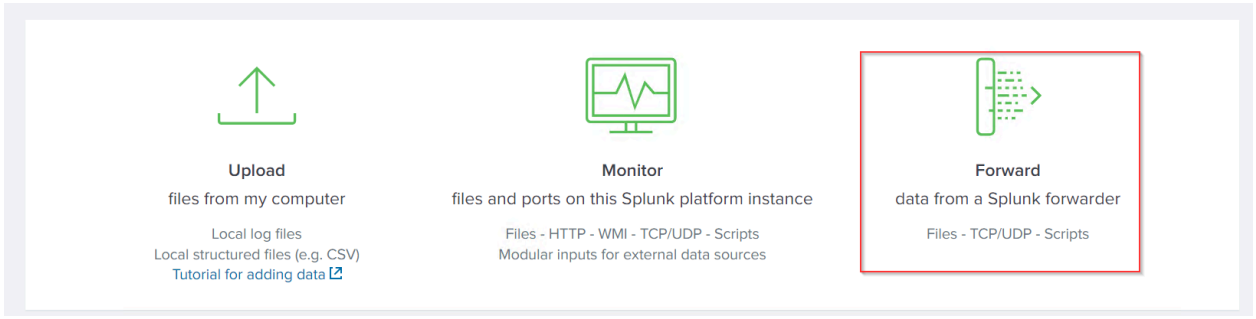
This site will allow users to order coffee online. In the backend, it will keep track of all the requests and responses and the orders placed. Now let's follow the next steps to ingest web logs into Splunk.

Add Data

Go to settings -> Add Data and select Forward from the list, as shown below:

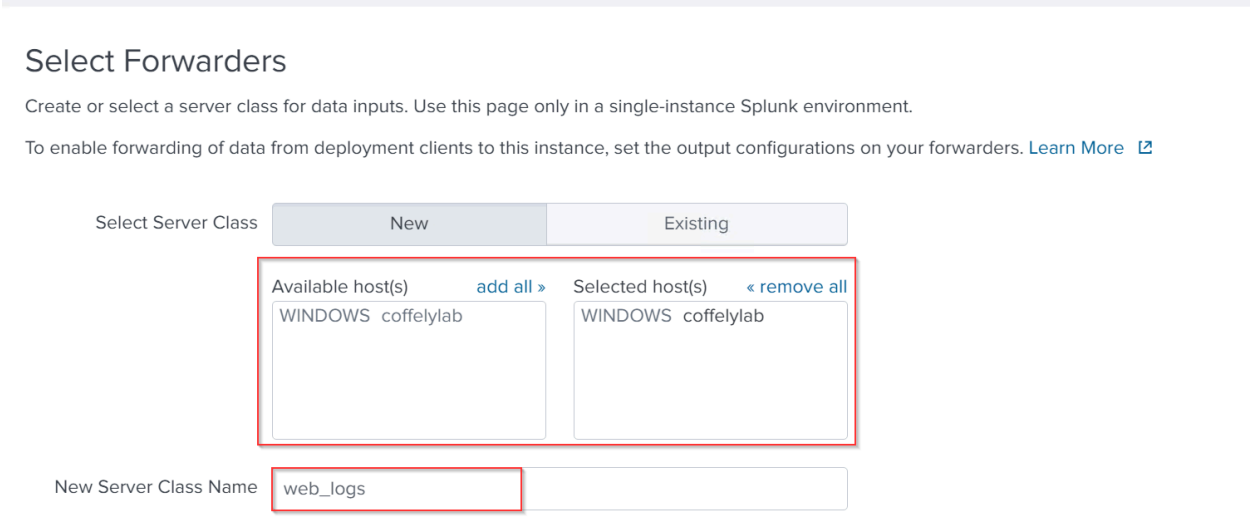


Select the Forwarder option:

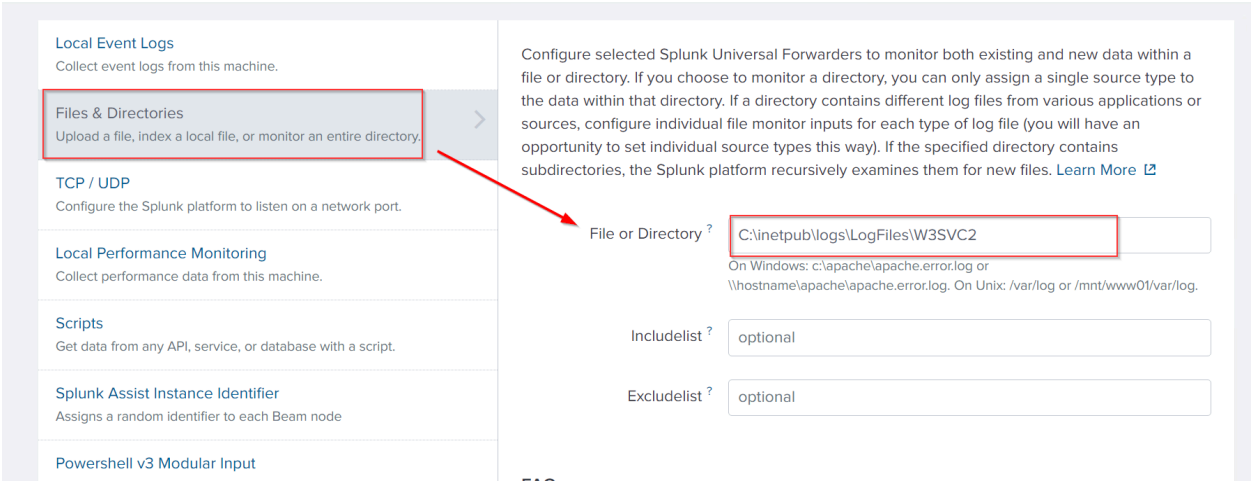


Select Forwarder

Here we will select the Web host where the website is being hosted.

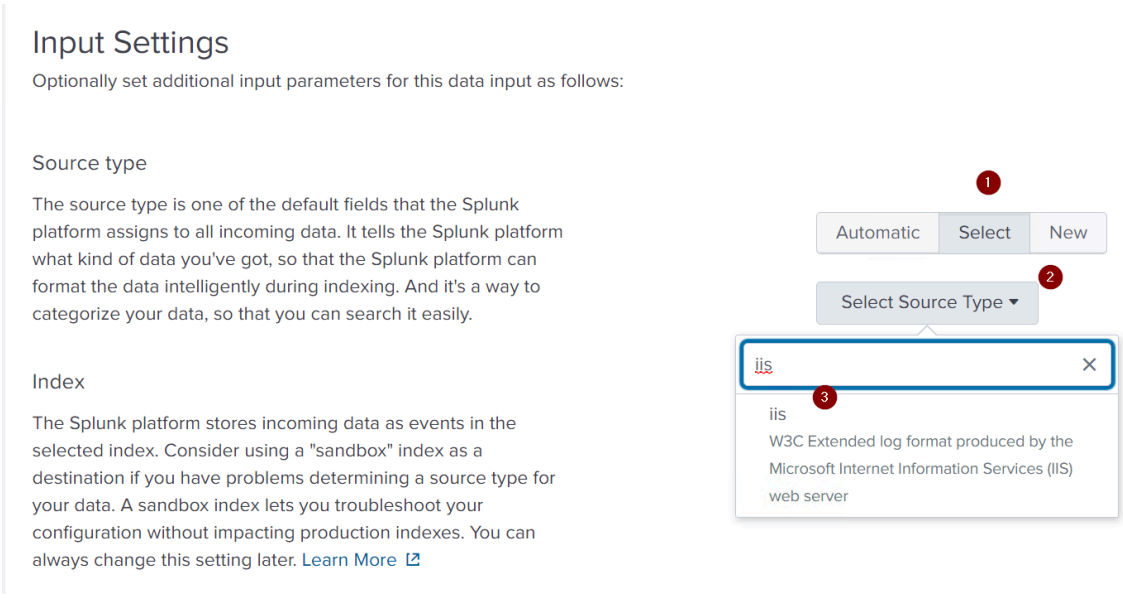


Web logs are placed in the directory C:\inetpub\logs\LogFiles\W3SVC*. The directory may contain one or more log files which will be continuously updated with the logs. We will be configuring Splunk to monitor and receive logs from this directory.

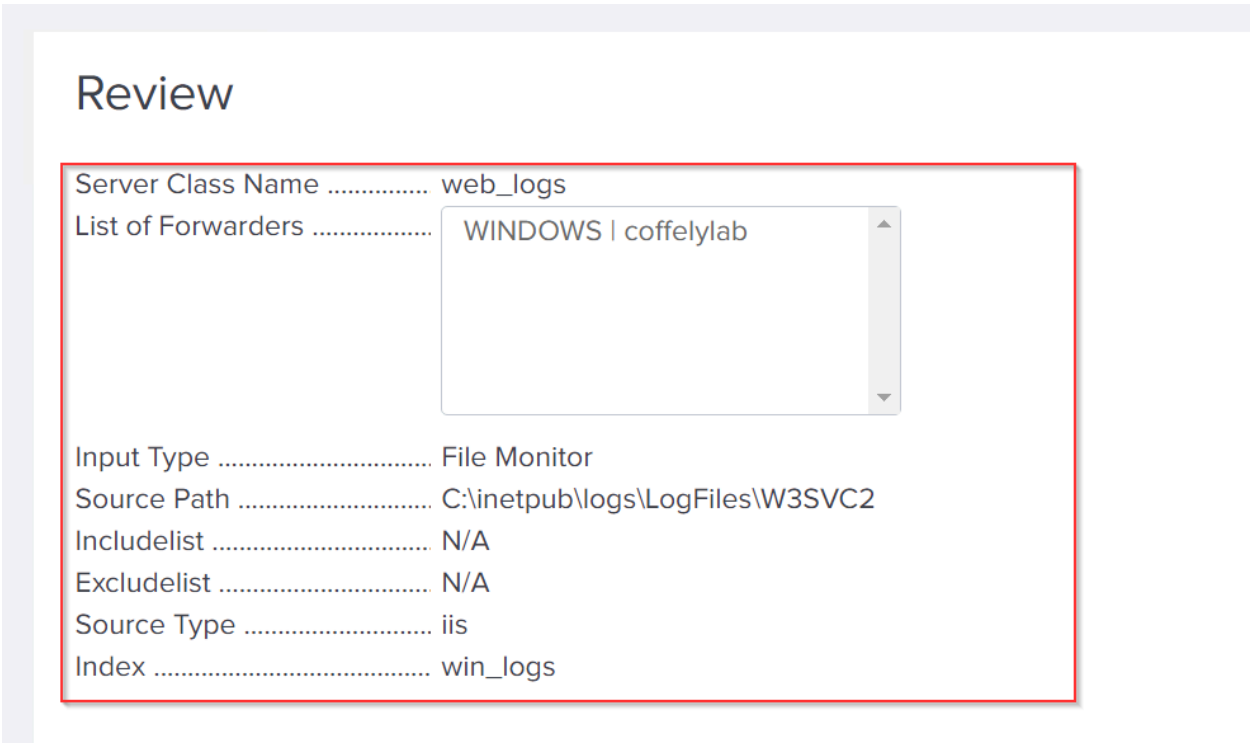


Setting up Source Type

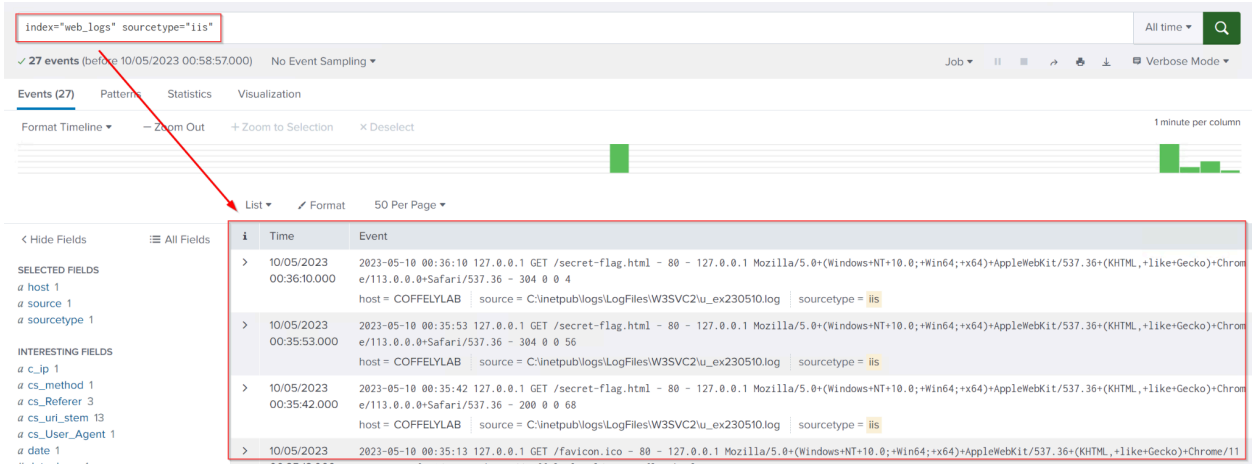
Next, we will select the source type for our logs. As our web is hosted on an IIS server, we will choose this option and create an appropriate index for these logs.



We can look at the summary to see if all settings are fine.



Now everything is done. It's time to see if we get the weblogs in our newly created index. Let's visit the website coffely.thm and generate some logs. The logs should start propagating in about 4-5 minutes in the search tab, as shown below:

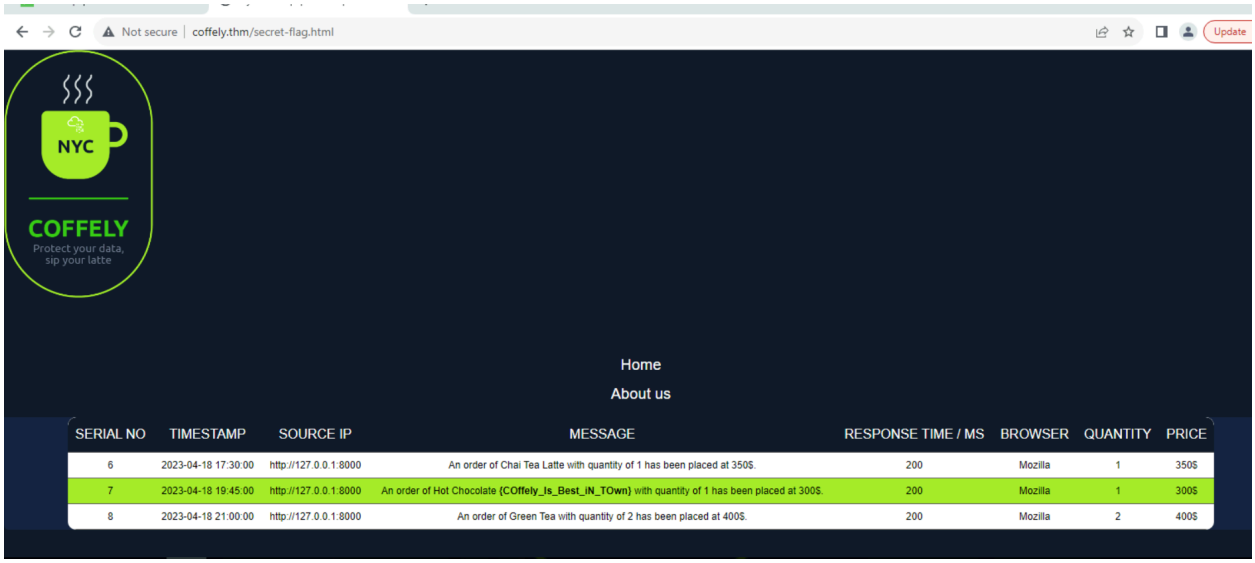


Excellent. It looks like we were successful in getting the weblogs ingested into Splunk. However, the logs may need proper parsing and normalizing, which is something to be discussed in upcoming rooms.

****

Answer the questions below:

In the lab, visit http://coffely.thm/secret-flag.html; it will display the history logs of the orders made so far. Find the flag in one of the logs.



Answer: {COffely_Is_Best_iN_TOwn}