As explained in the Splunk Basics room, Splunk is a SIEM solution that allows us to collect, analyze, and correlate logs in a centralized server in real-time. This room will cover installing Splunk on Linux/Windows and configuring different log sources from both OS into Splunk.

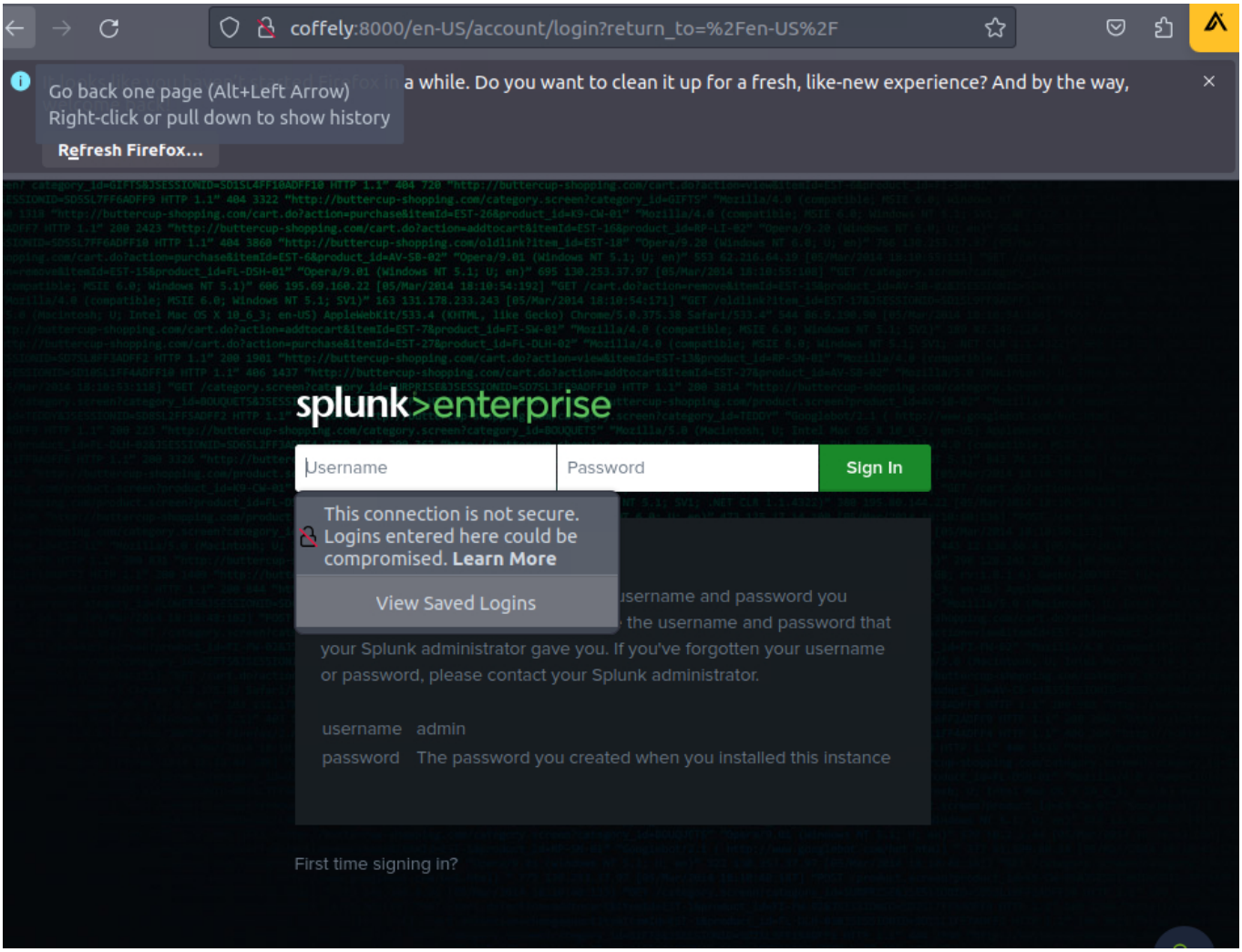
Answer the questions below

What is the default port for Splunk?

8000

✓ Correct Answer

We can see that the default port is 8000



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.

Splunkstart

```
root@coffely:/opt/splunk#./bin/splunk start
Splunk> Finding your faults, just like mom.
....
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.
....
....
The Splunk web interface is at http://coffely:8000
```

As mentioned in the output, the Splunk dashboard will be accessible within the VM 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.

Splunkstop

```
root@tryhackme:/opt/splunk#./bin/splunk stop
 ...some output ommitted ...
```

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.

splunk: restart

```
root@tryhackme:/opt/splunk#./bin/splunk restart
...some output ommitted ...
```

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.

Splunk: Start

```
root@coffely:/opt/splunk#./bin/splunk status
splunkd is running (PID: 2158).
splunk helpers are running (PIDs: 2159 2301 2351 2437).
```

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.

splunk: add oneshot

```
root@coffely:/opt/splunk#./bin/splunk add oneshot
...some output ommitted ...
```

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.

Splunk: search

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

splunk HELP Command

```
root@tryhackme:/opt/splunk#./bin/splunk help
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
        ....
        ....
```

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?

./bin/splunk search coffely

✓ Correct Answer

Hint

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

./bin/splunk search coffely ✓ Correct Answer Hint

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

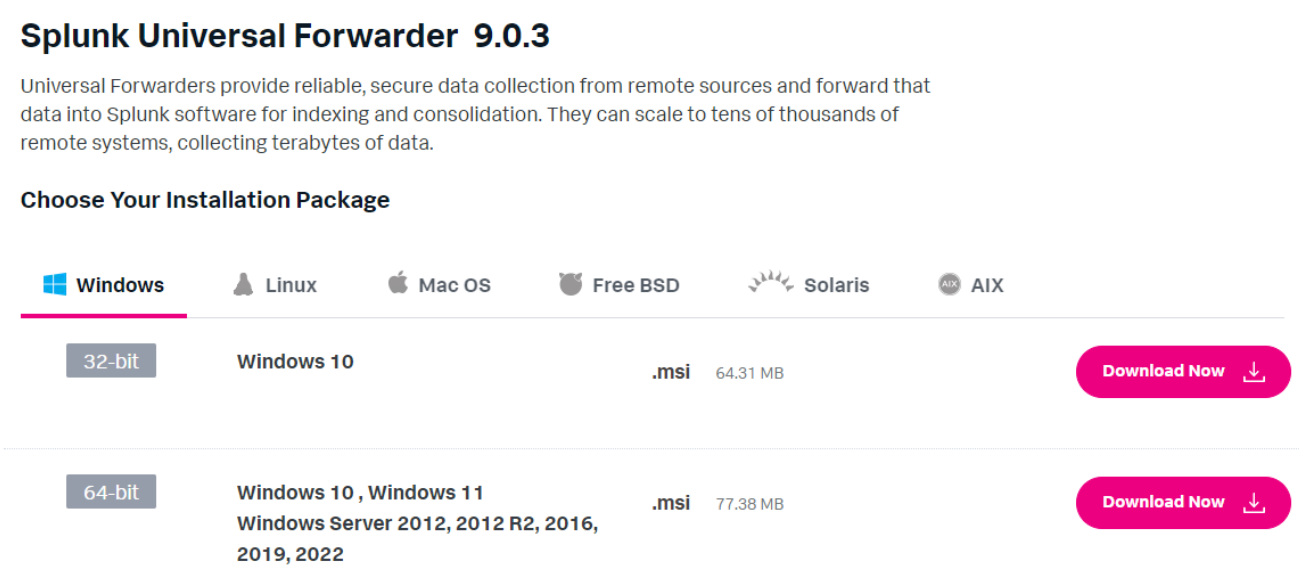
Heavy forwarders are used when we need to apply a filter, analyze or make changes to the logs at the source before forwarding it to the destination. In this task, we will be installing and configuring Universal forwarders.

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`.

splunk: Forwarder

```
ubuntu@coffely:~/Downloads/splunk# ls
splunk_installer.tgz splunkforwarder.tgz
```

Install Forwarder

Change the user to sudo, unpack, and install the forwarder with the following command.

splunk: Forwarder

```
ubuntu@coffely:~/Downloads/splunk# sudo su
root@coffely:/home/ubuntu/Downloads/splunk# tar xvzf splunkforwarder.tgz
splunkforwarder/
splunkforwarder/swidtag/
splunkforwarder/swidtag/splunk-UniversalForwarder-primary.swidtag
splunkforwarder/ftr
splunkforwarder/openssl/
...
...
splunkforwarder/etc/deployment-apps/
splunkforwarder/etc/deployment-apps/README
splunkforwarder/etc/log-debug.cfg
```

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/`.

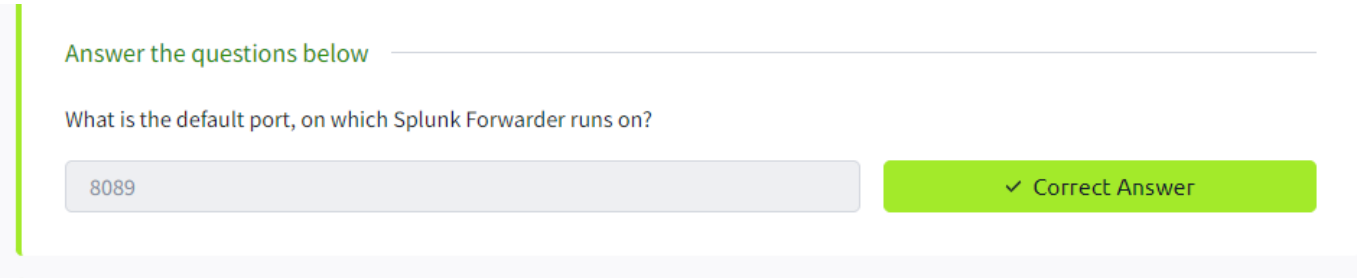
We will run the Splunk forwarder instance now and provide it with the new credentials as shown below:

SplunkInstallation

```
root@coffey:~/Downloads/splunk# mv splunkforwarder /opt/
root@coffey:~/Downloads/splunk# cd /opt/splunkforwarder
root@coffey:/opt/splunkforwarder# ./bin/splunk start --accept-license
This appears to be your first time running this version of Splunk.
...
...
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:
Creating unit file...
Failed to auto-set default user.
...
...
Checking prerequisites...
        Checking mgmt port [8089]: not available
ERROR: mgmt port [8089] - port is already bound.  Splunk needs to use this
port.
Would you like to change ports? [y/n]: y
Enter a new mgmt port: 8090
Setting mgmt to port: 8090
The server's splunkd port has been changed.
        Checking mgmt port [8090]: open
Starting splunk server daemon (splunkd)...
Done
```

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.

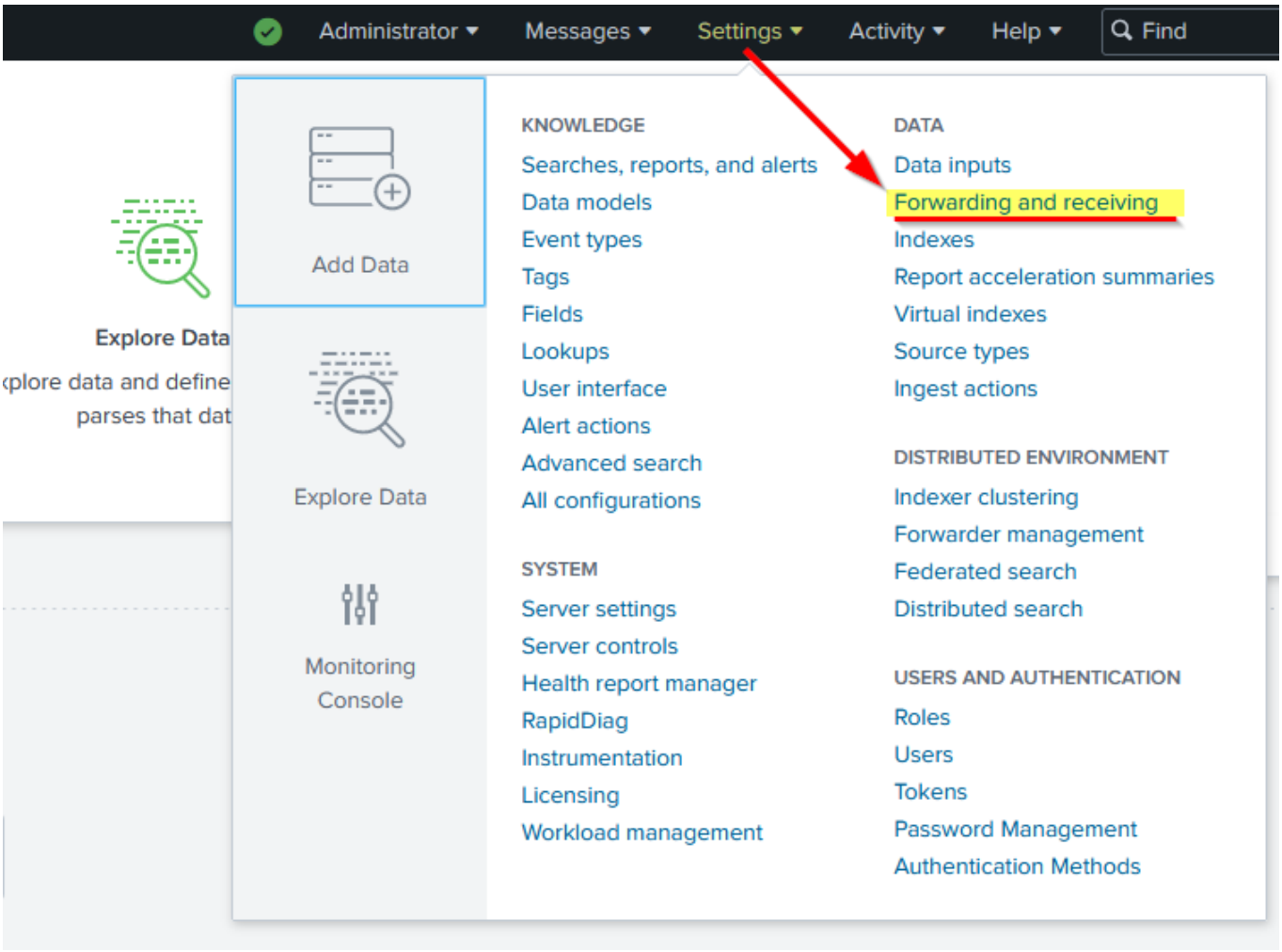
Splunk Forwarder is up and running but does not know what data to send and where. This is what we are going to configure next.



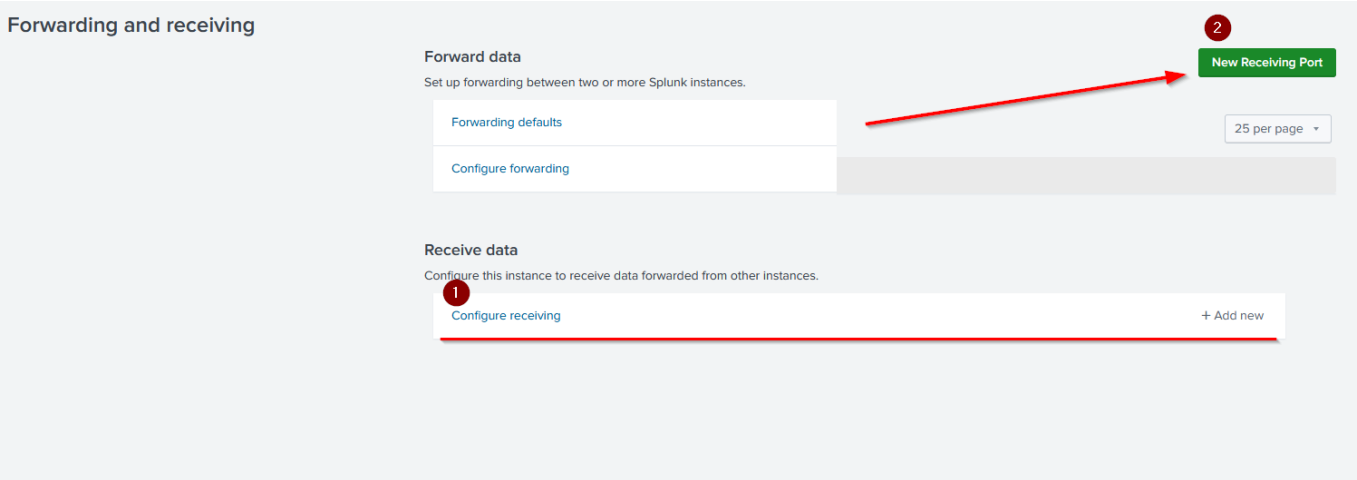
Now that we have installed the forwarder, it needs to know where to send the data. So we will configure it on the host end to send the data and configure Splunk so that it knows from where it is receiving the data.

Splunk Configuration

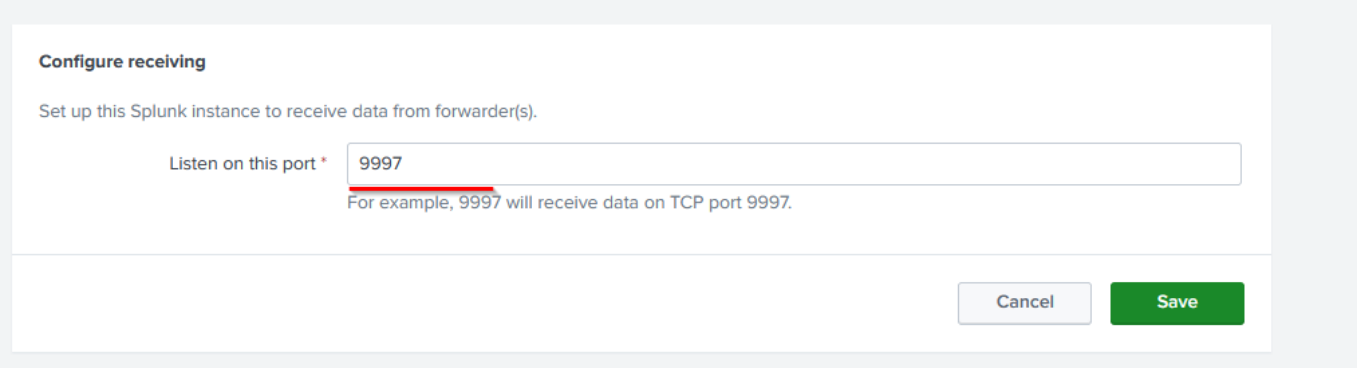
Log into Splunk and Go to Settings -> Forward and receiving tab as shown below:



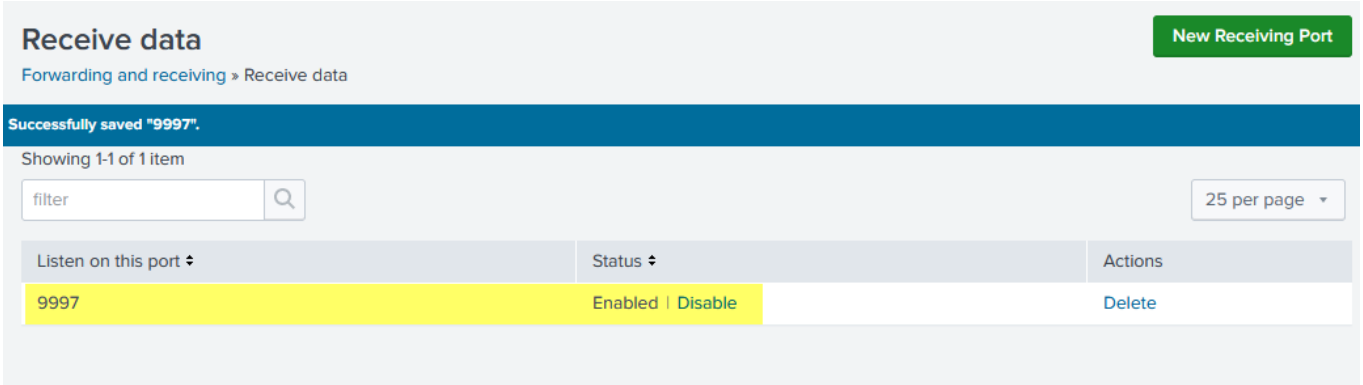
It will show multiple options to configure both forwarding and receiving. As we want to receive data from the Linux endpoint, we will click on **Configure receiving** and then proceed by configuring a new receiving port.



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:

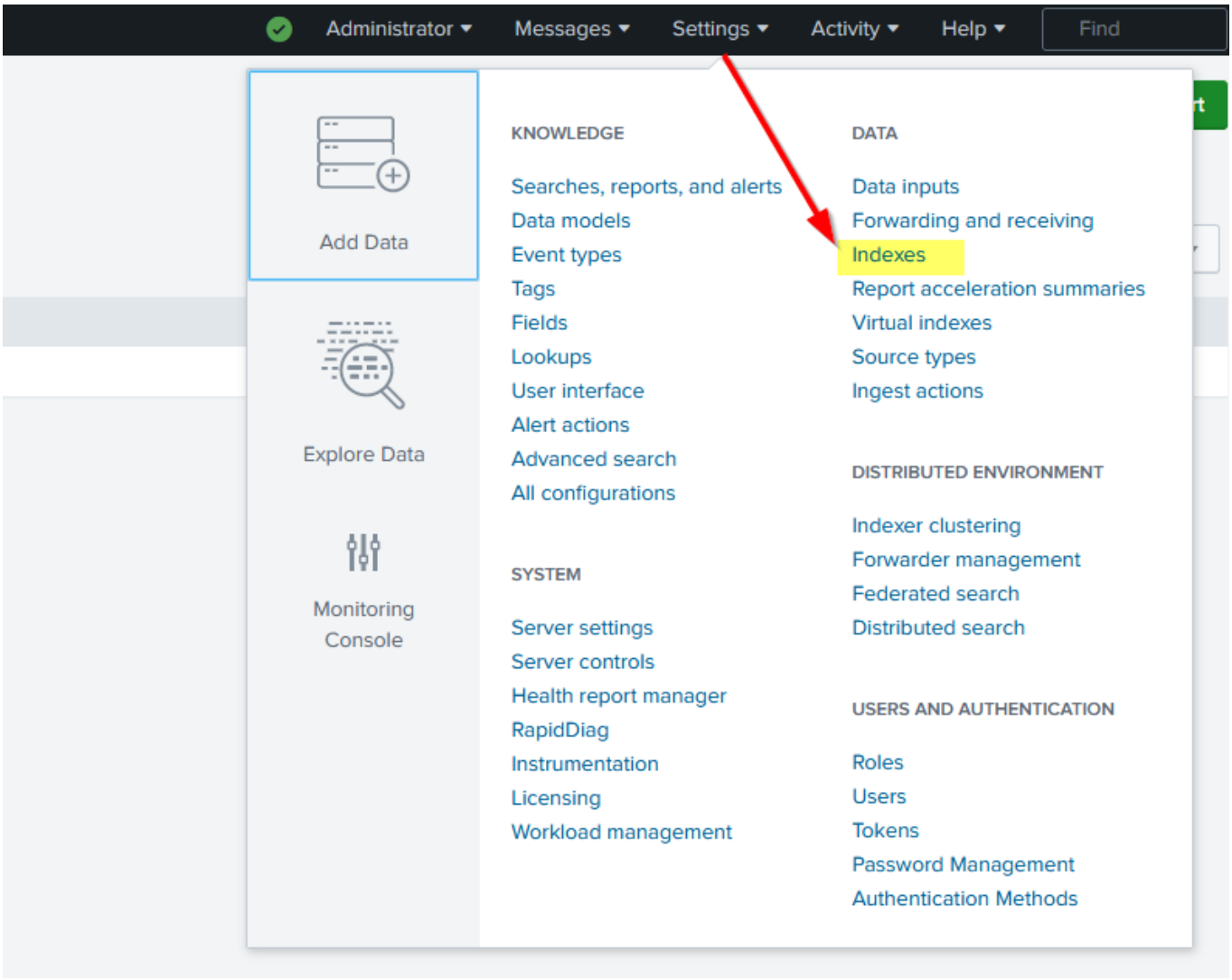


Our listening port 9997 is now enabled and waiting for the data. If we want, we can delete this entry by clicking on the `Delete` option under the `Actions` column.

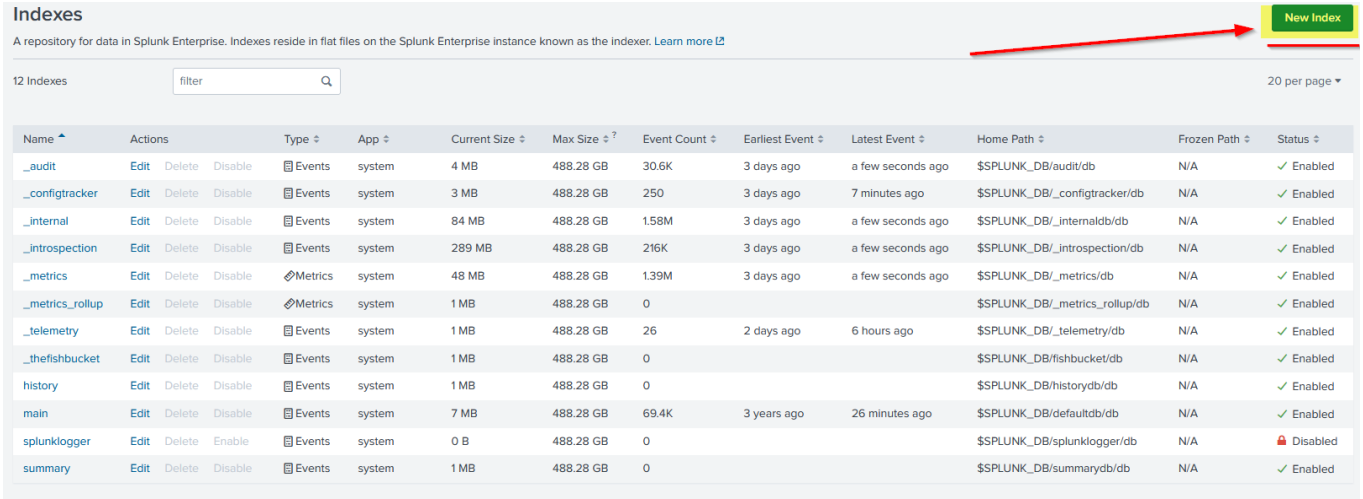


Creating Index

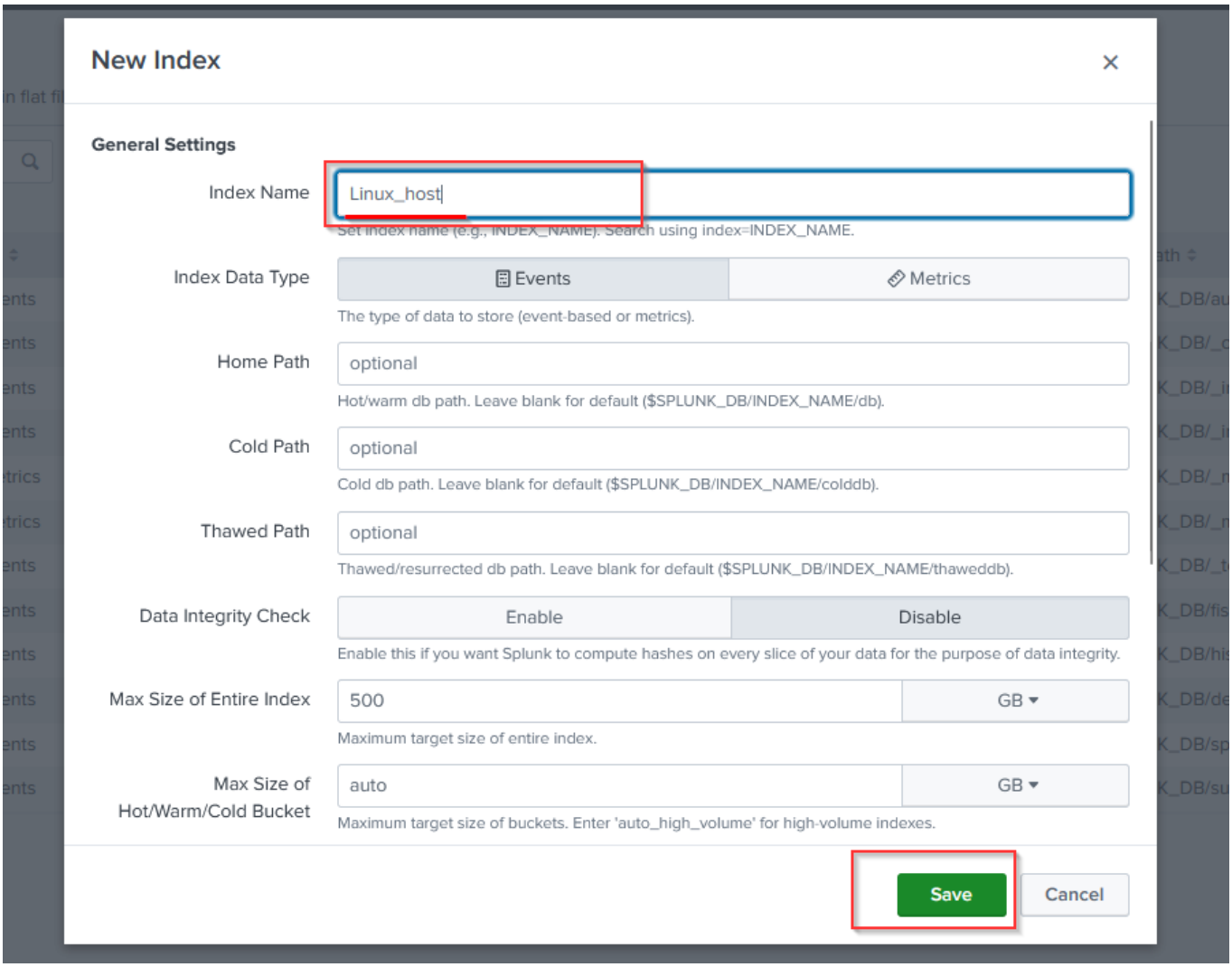
Now that we have enabled a listening port, the important next step is to create an index that will store all the receiving data. If we do not specify an index, it will start storing received data in the default index, which is called the `main` index.



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:

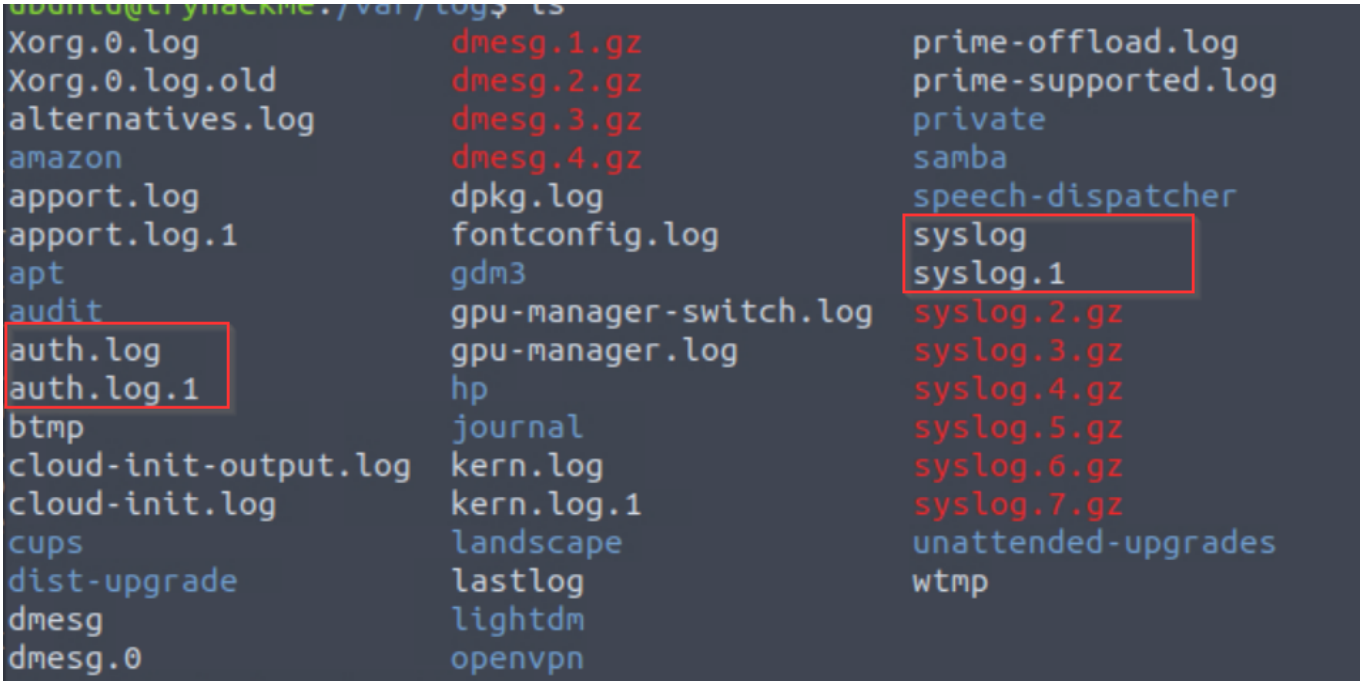
Splunk: Forwarder

```
root@coffely:/opt/splunkforwarder/bin# ./splunk add forward-server
10.10.250.40:9997
WARNING: Server Certificate Hostname Validation is disabled. Please see
server.conf/[sslConfig]/cliVerifyServerName for details.
Splunk username: splunkadmin
Password:
Added forwarding to: 10.10.250.40:9997.
```

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.



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

Ingest syslog file

```
root@coffely:/opt/splunkforwarder/bin# ./splunk add monitor /var/log/syslog -
index Linux_host
WARNING: Server Certificate Hostname Validation is disabled. Please see
server.conf/[sslConfig]/cliVerifyServerName for details.
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.

Inputs.conf

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

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

Inputs.conf

```
root@coffely:/opt/splunkforwarder/etc/apps/search/local# cat inputs.conf
[monitor:///var/log/syslog]
```

```
disabled = false
index = Linux_host
```

Utilizing Logger Utility

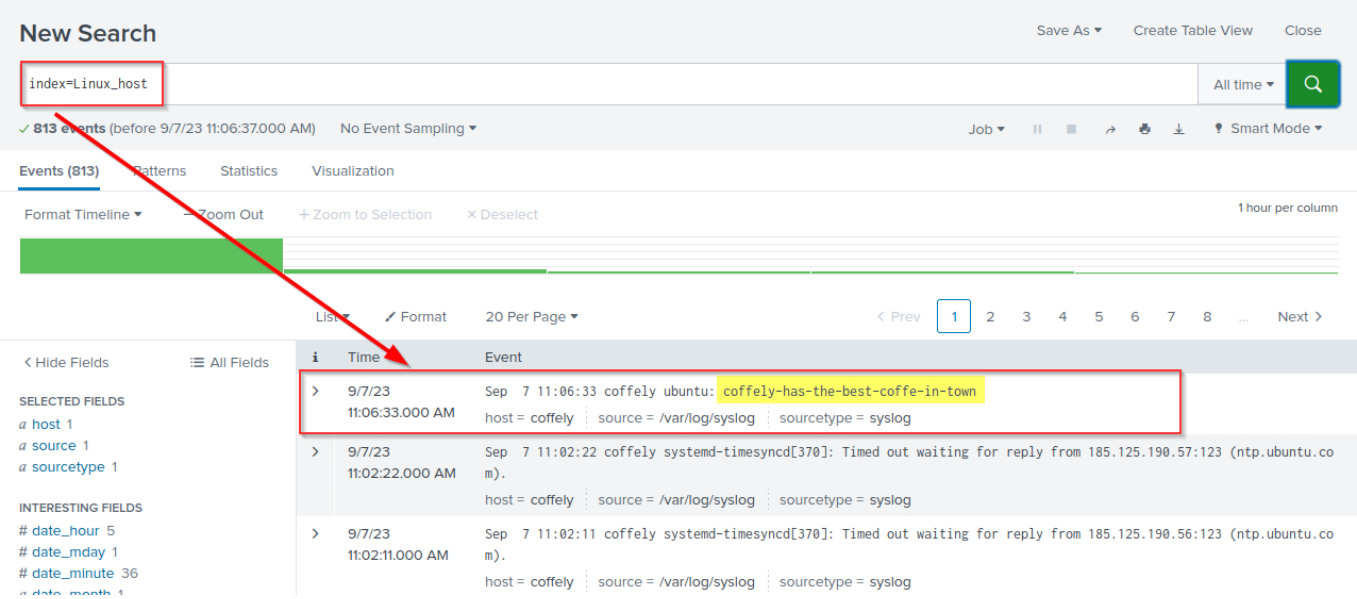
Logger is a built-in command line tool to create test logs added to the syslog file. As we are already monitoring the syslog file and sending all logs to the Splunk, the log we generate in the next step can be found with Splunk logs. To run the command, use the following command.

Logger: syslog

```
tryhackme@coffely:/opt/splunkforwarder/bin# logger "coffely-has-the-best-coffee-in-town"
```

Logger: syslog

```
tryhackme@coffely:/tryhackme@coffleylab:/opt/splunkforwarder/bin# tail -1 /var/log/syslog
```



Great, We have successfully installed and configured Splunk Forwarder to get the logs fom 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?

syslog ✓ Correct Answer

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?

6 ✓ Correct Answer

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

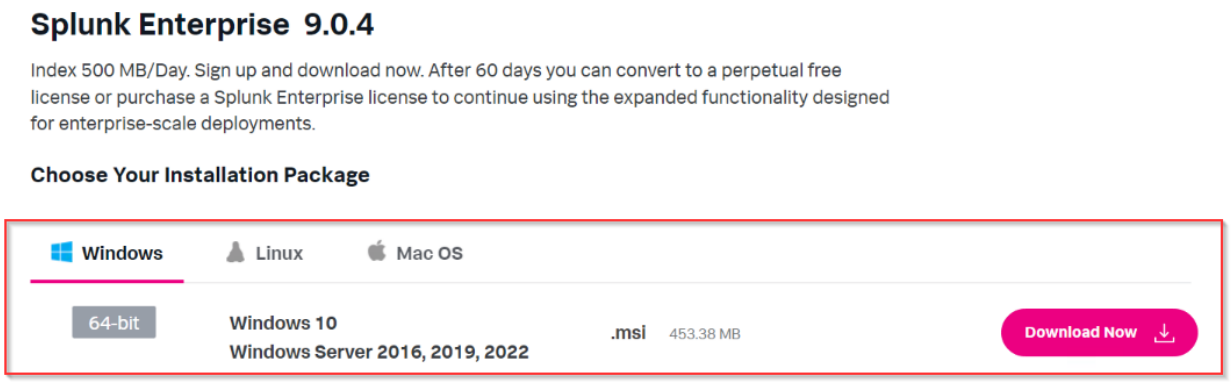
/etc/group ✓ Correct Answer

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.

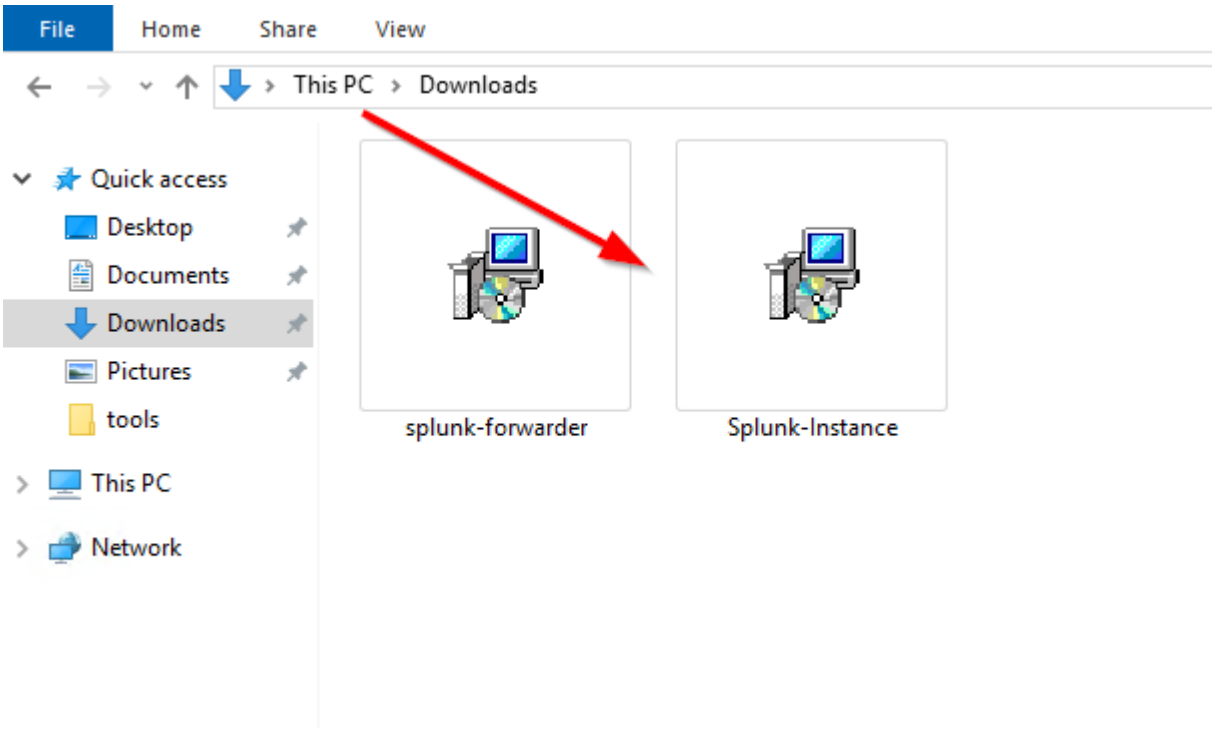
On the Windows machine, we will first install Splunk, configure a forwarder to capture Windows Event logs, and integrate `Coffely` weblogs to collect all requests and responses into Splunk Instance.

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:

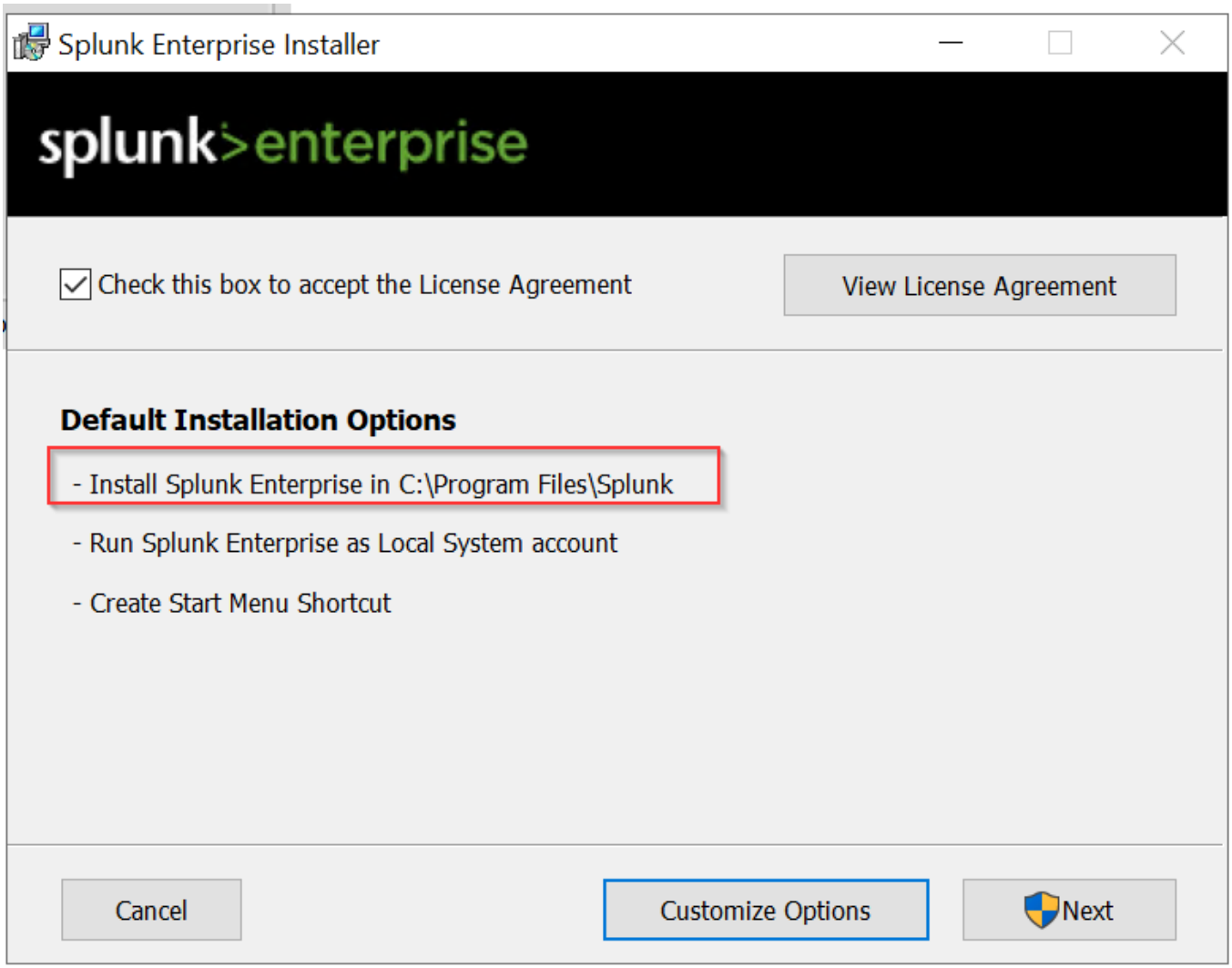


The installer Splunk-Instance is already been downloaded and placed in the `Downloads` folder to speed up the process.



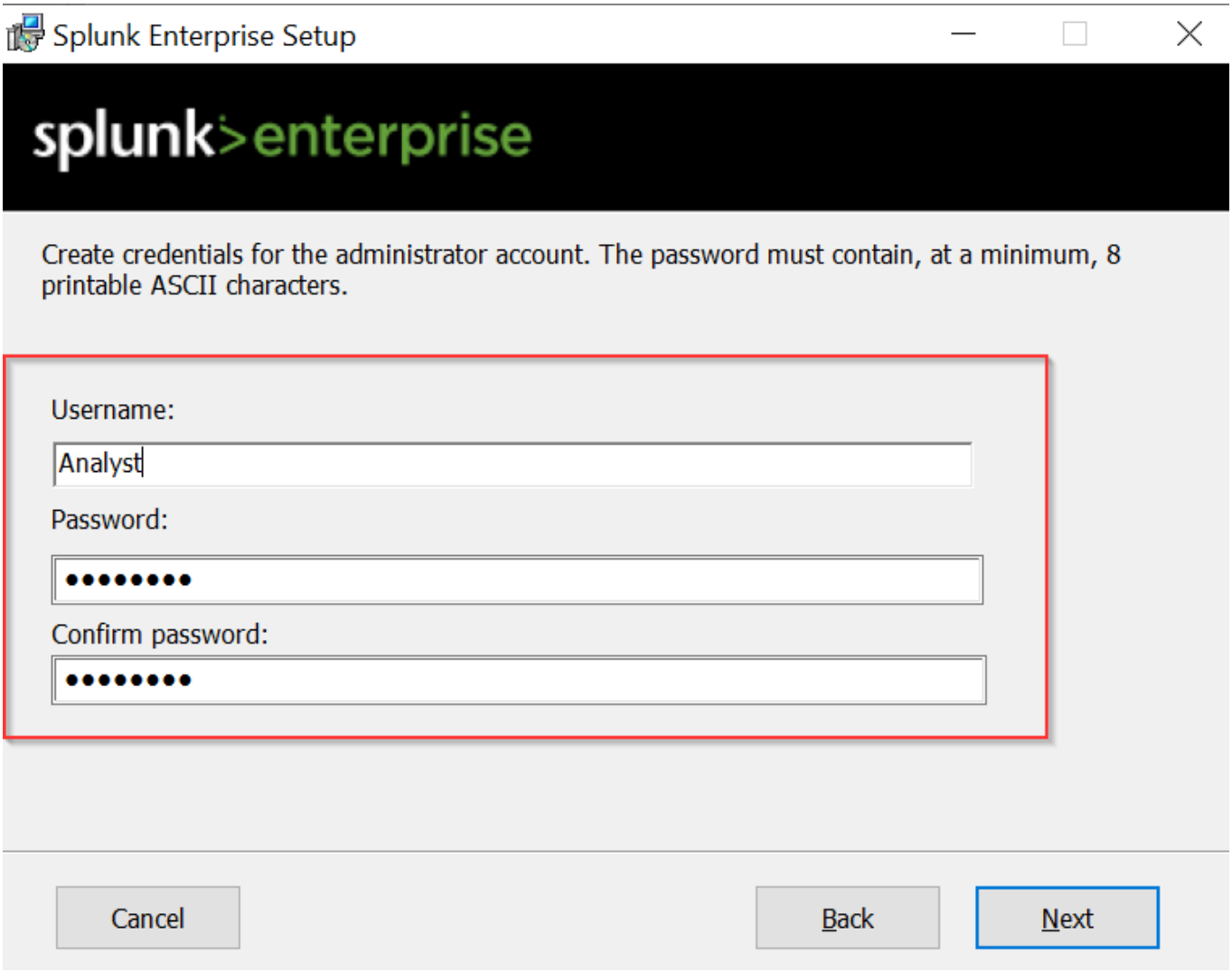
Run the `Splunk-Instance` installer. By default, it will install Splunk in the folder `C:\Program Files\Splunk`. This will check the system for dependencies and will take 5-8 minutes to install the Splunk instance.

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

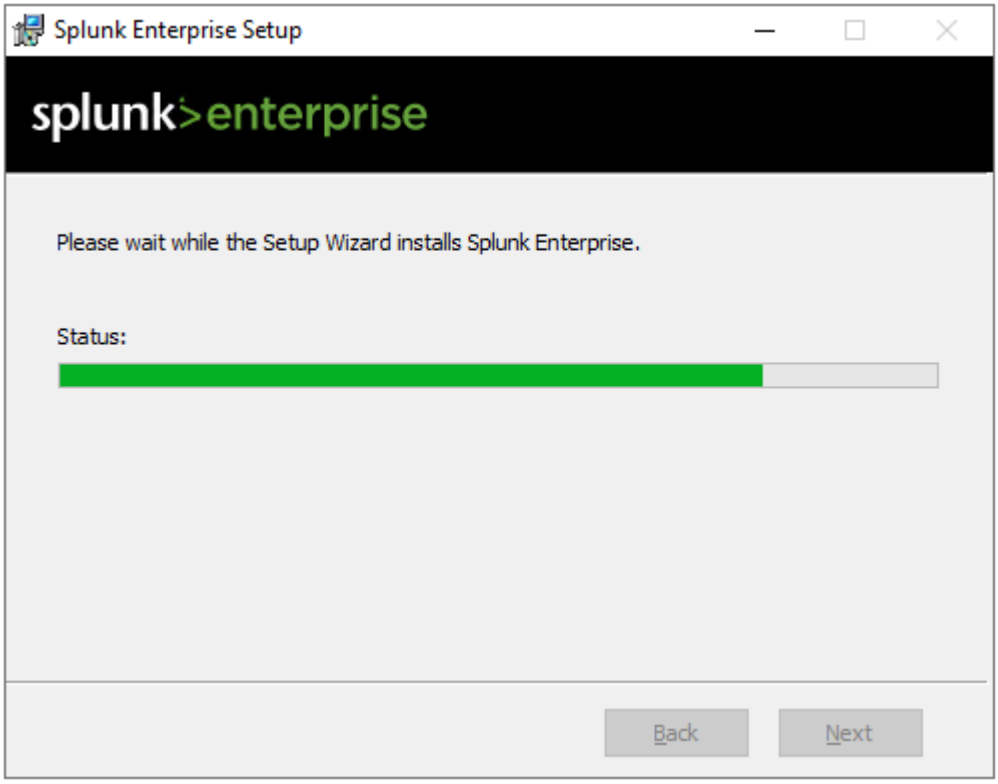


Create Administration Account

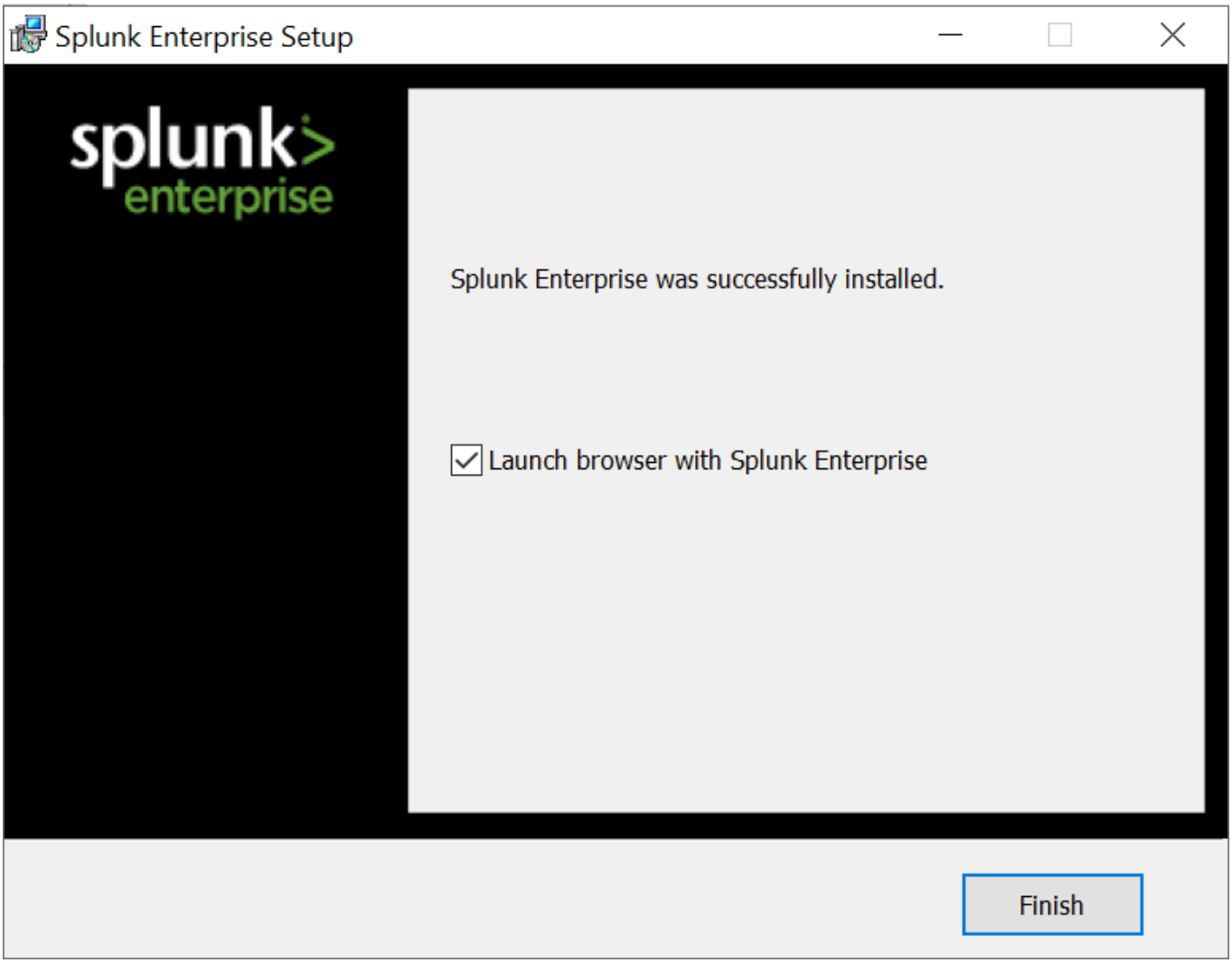
The important step during installation is creating an administrator account, as shown below. This account will have high privileges, create and manage other accounts, and control all administrative roles.



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

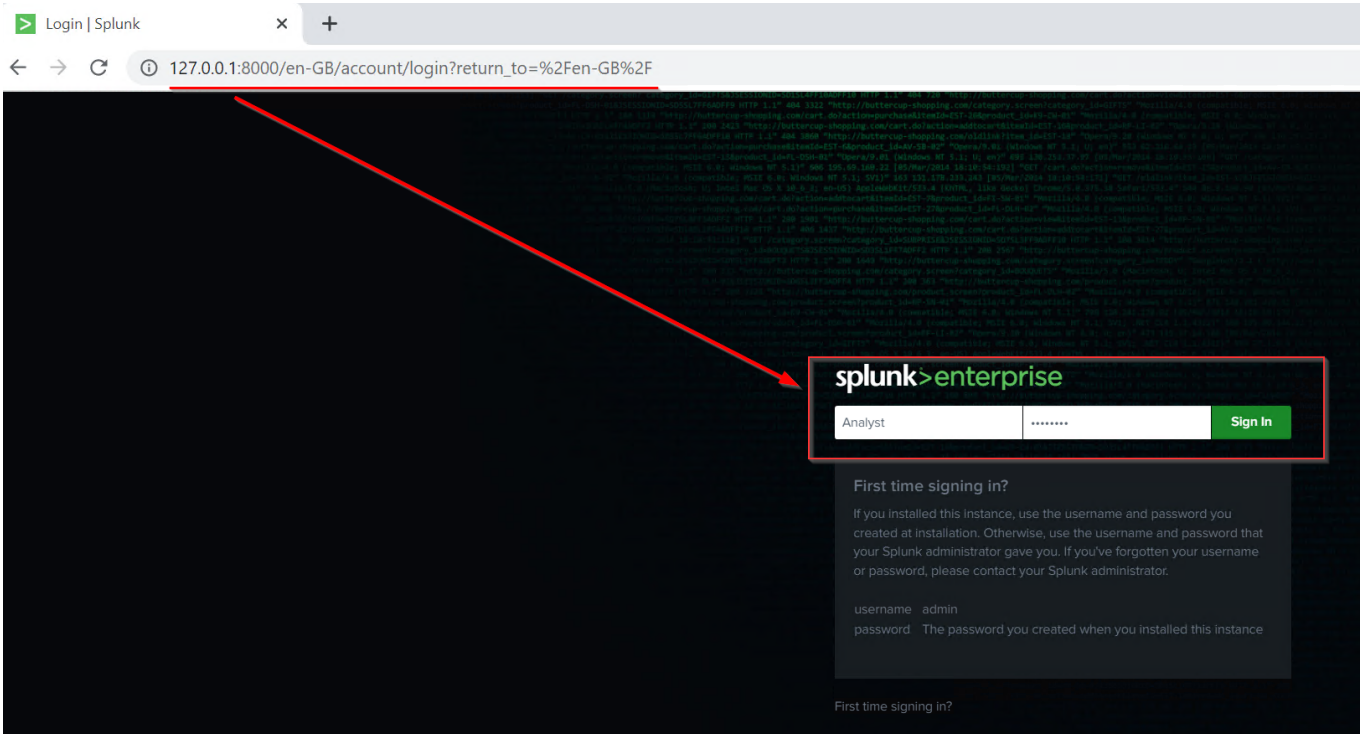


We will get the following message if all system requirements are met, and installation is complete.

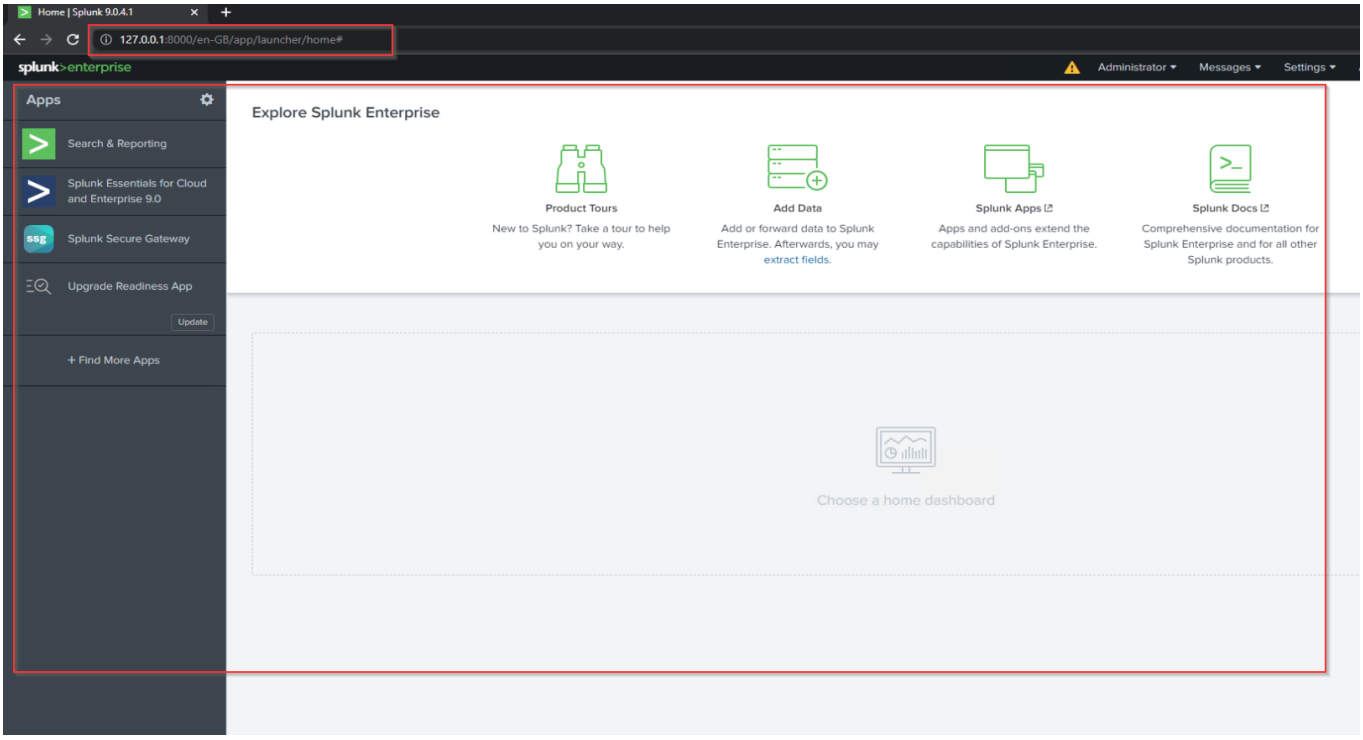


Accessing Splunk Instance

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://10.10.250.40:8000`.



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.

What is the default port Splunk runs on?

8000

✓ Correct Answer

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

3 ✓ Correct Answer

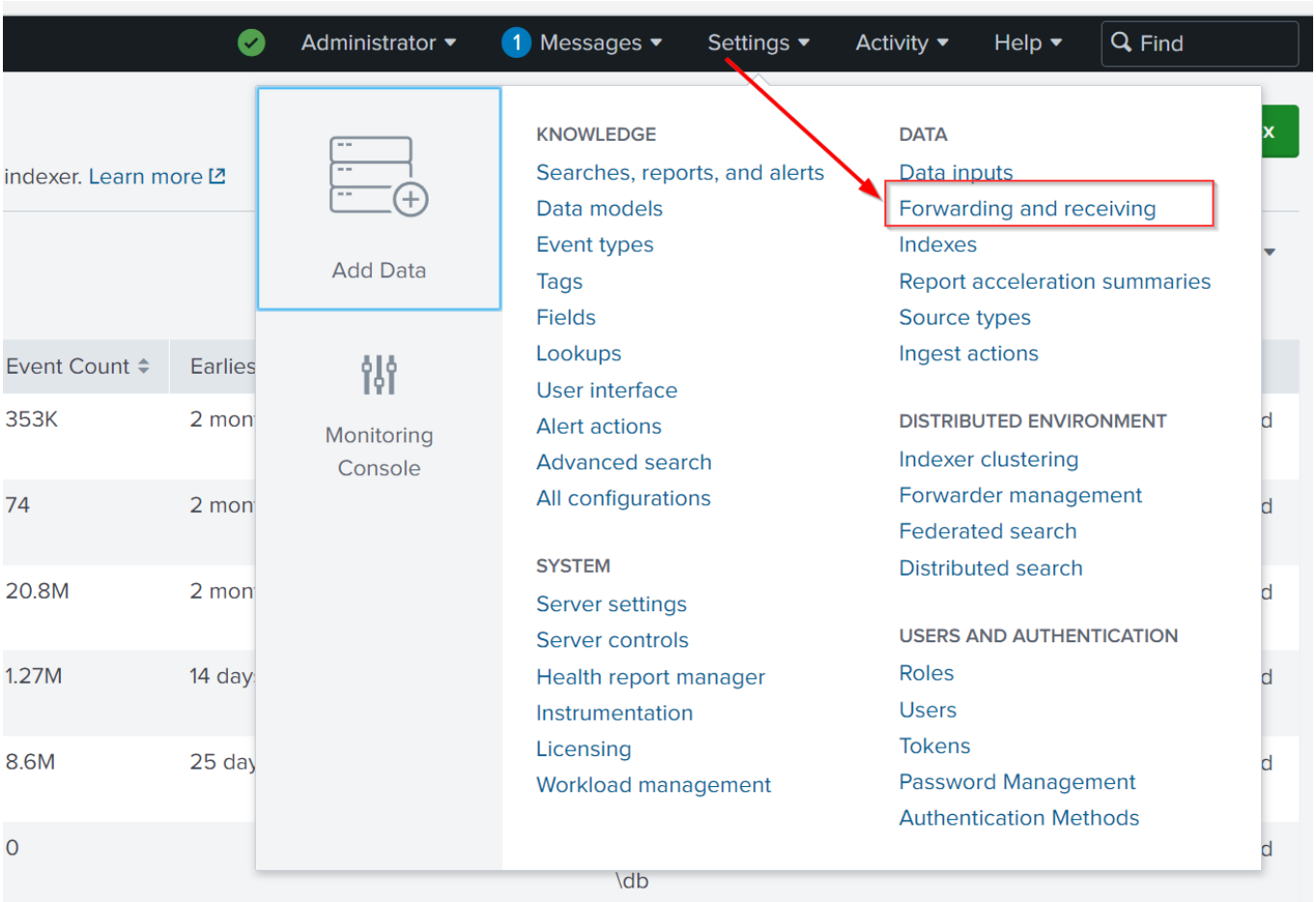
Click on the Monitor option; what is the first option shown in the monitoring list?

Local Event Logs ✓ Correct Answer

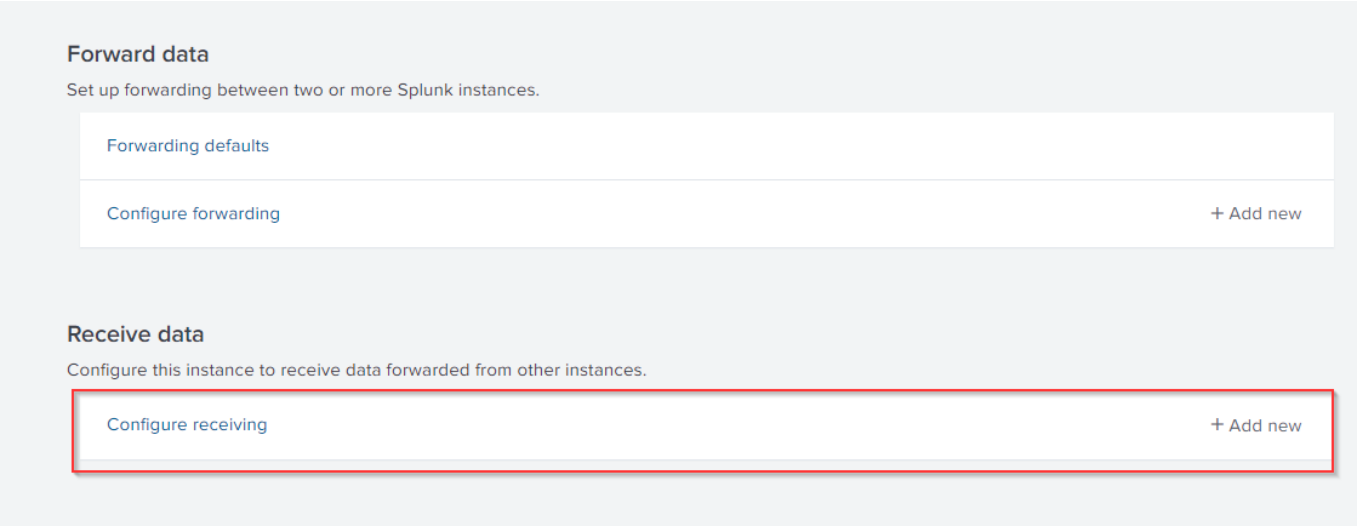
First, we will configure the receiver on Splunk so the forwarder knows where to send the data.

Configure Receiving

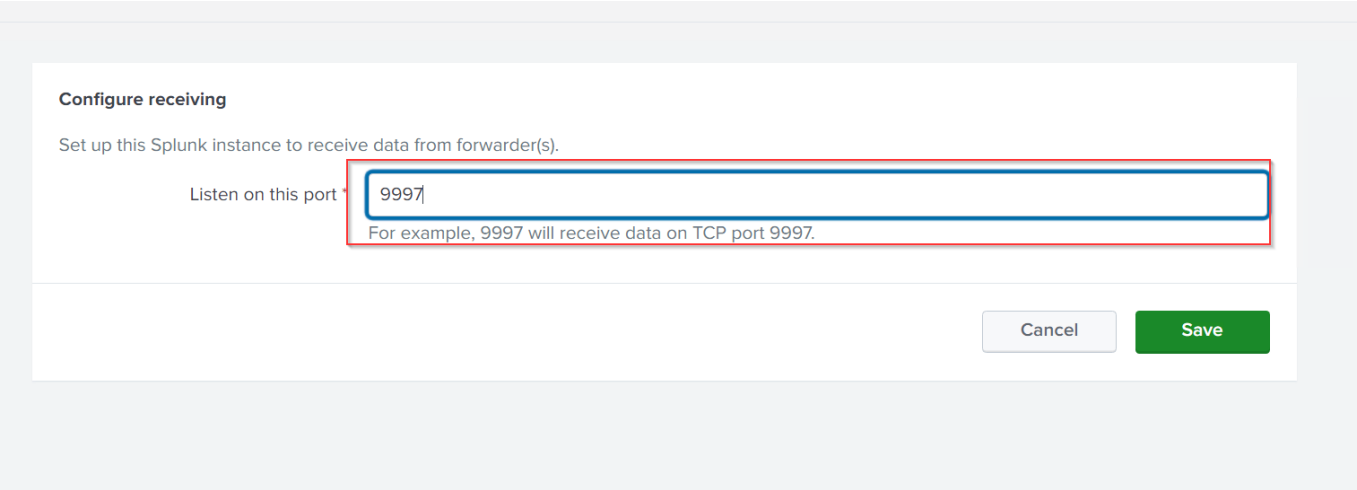
Log into Splunk and Go to Settings -> Forward and receiving tab as shown below:



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.

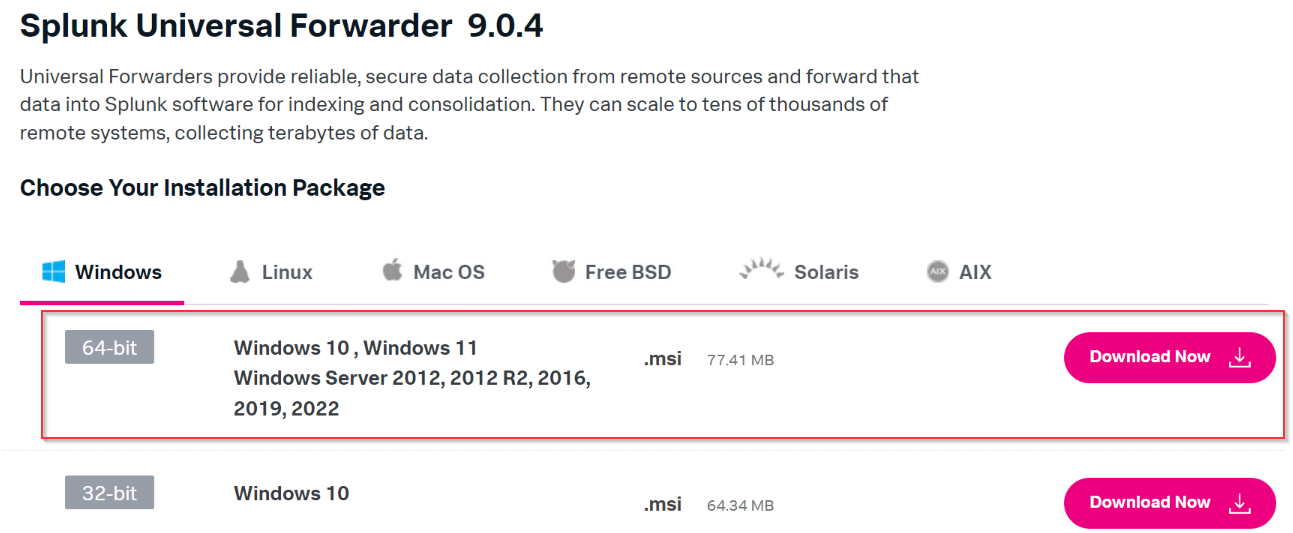


By default, the Splunk instance receives data from the forwarder on port `9997`. It's up to us to use this port or change it. For now, we will configure our Splunk to start listening on port 9997 and **Save**, as shown below:

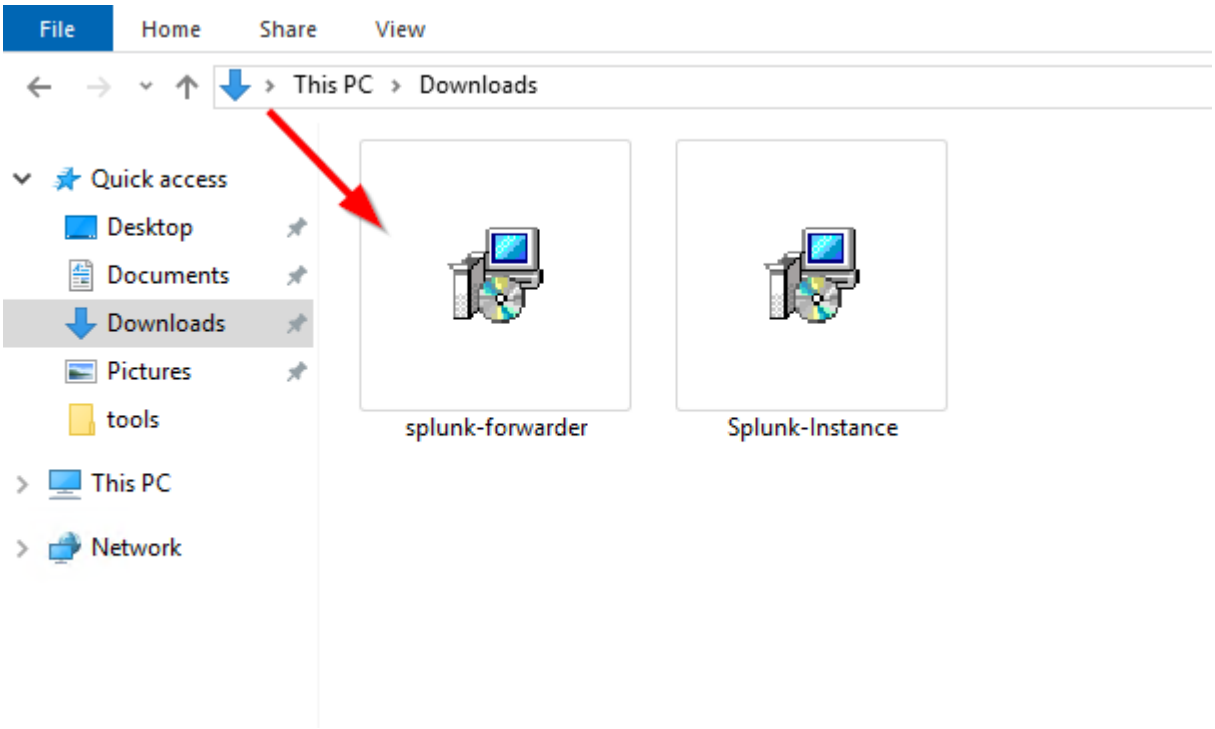


Installing Splunk Forwarder

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.

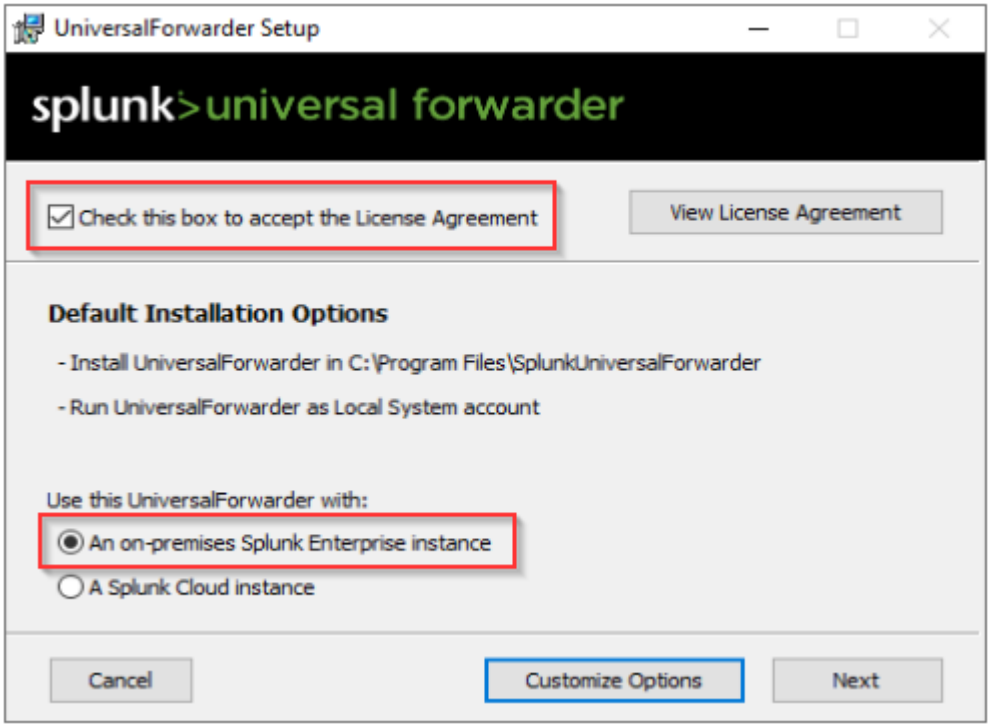


For this lab, the forwarder is already downloaded and placed in the Downloads folder, as shown below:

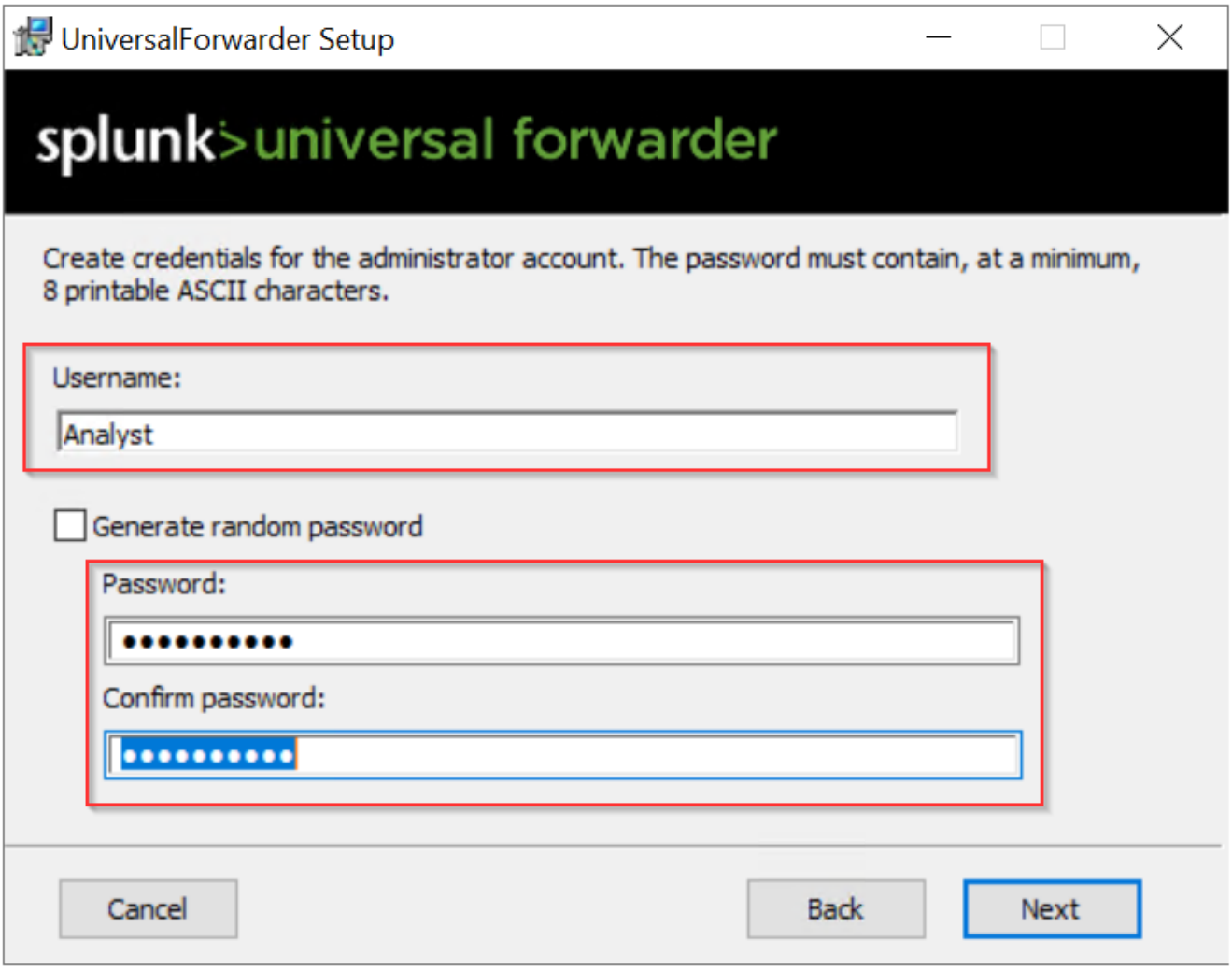


Installation Process

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.

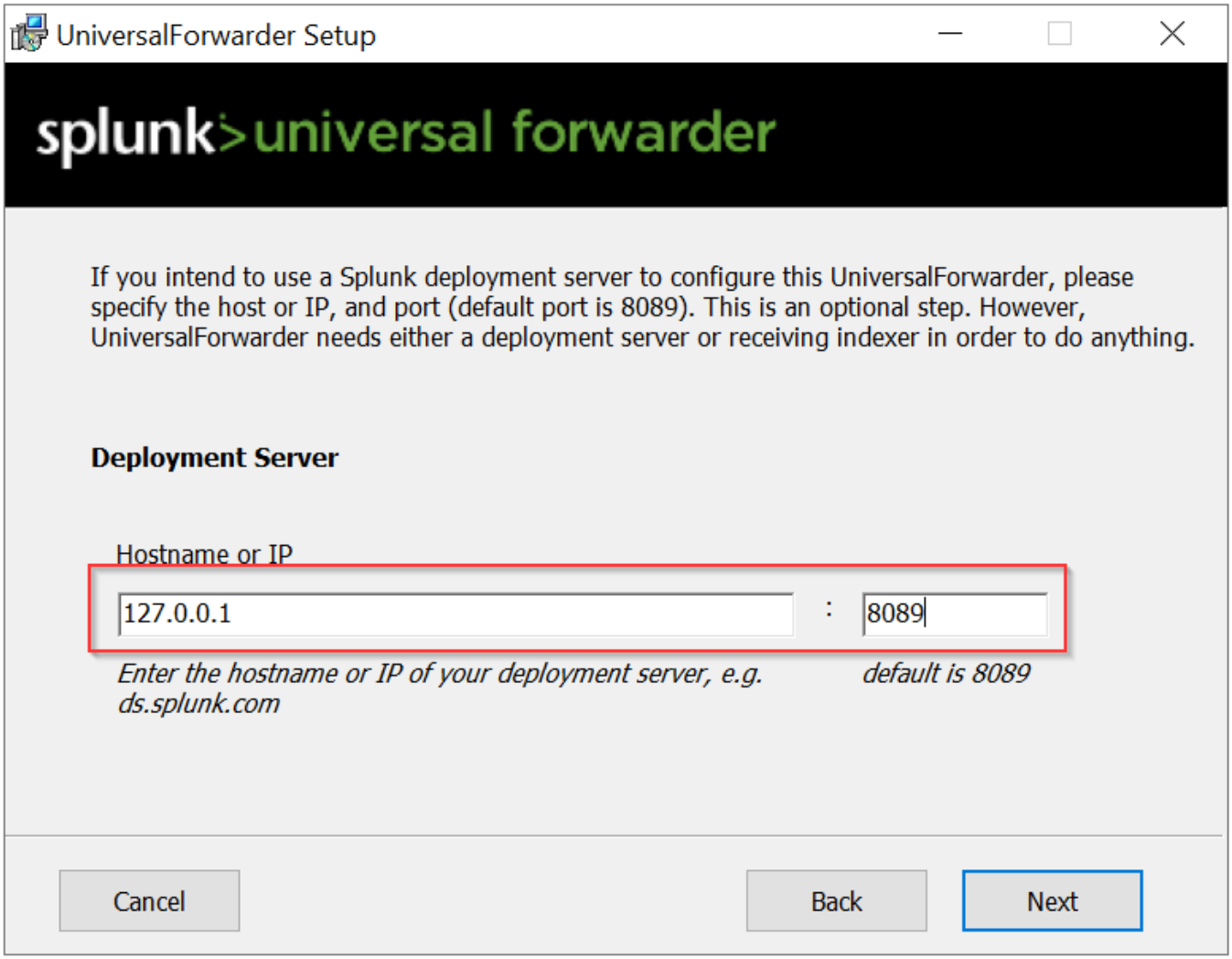


Create an account for Splunk Forwarder. This will be used when connecting the Splunk forwarder to the Splunk Indexer.



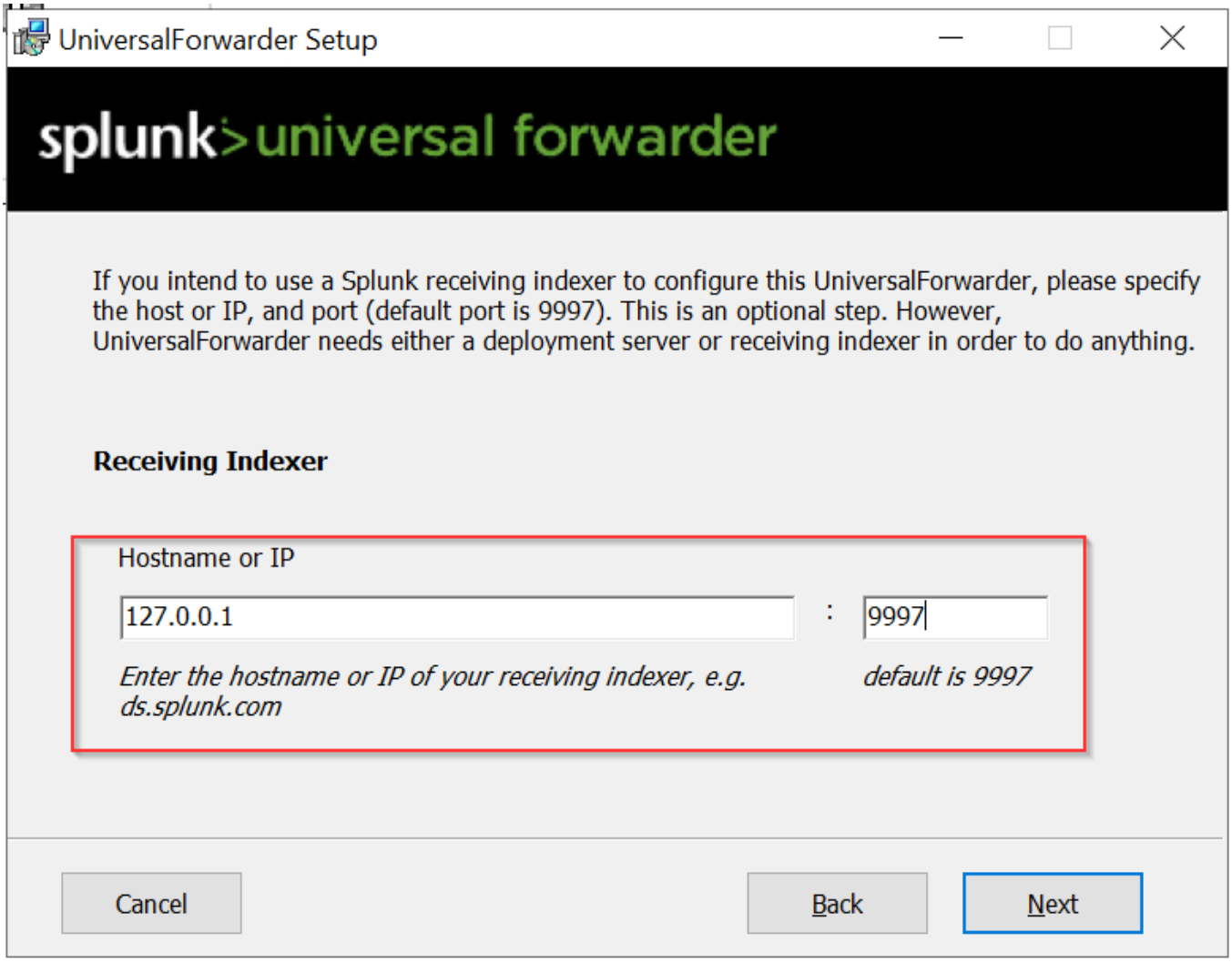
Setting up Deployment Server

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

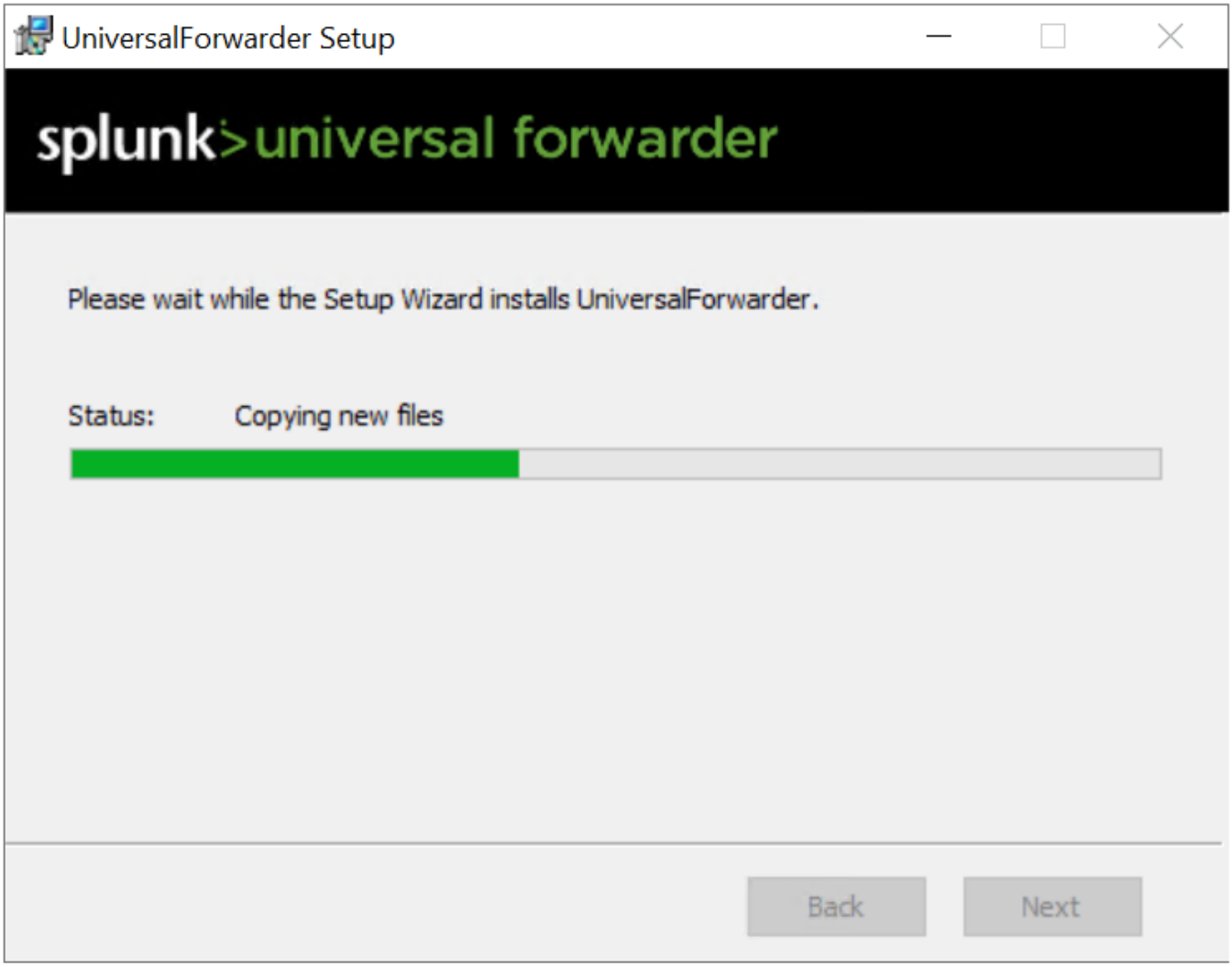


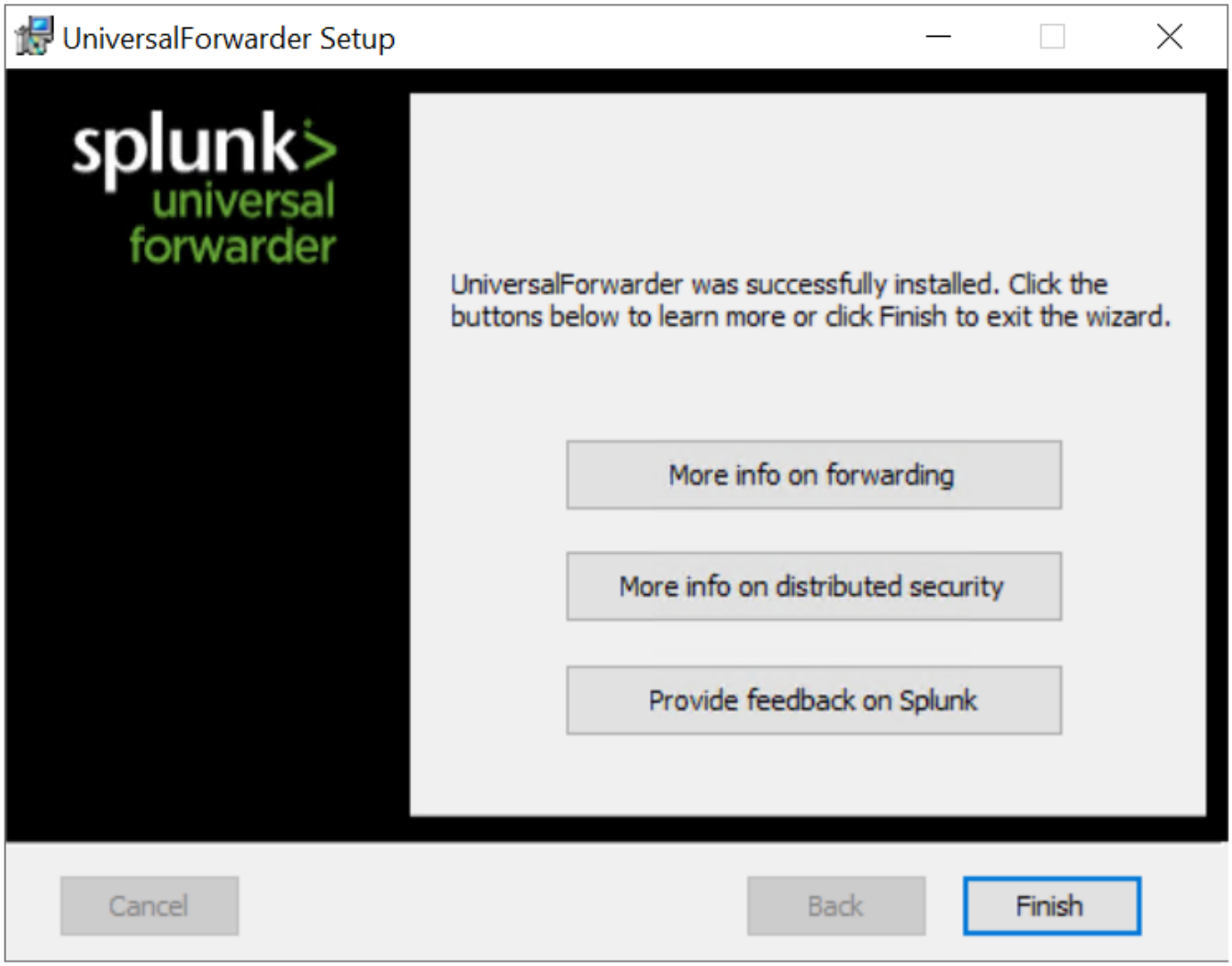
Setting Up Listener

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.

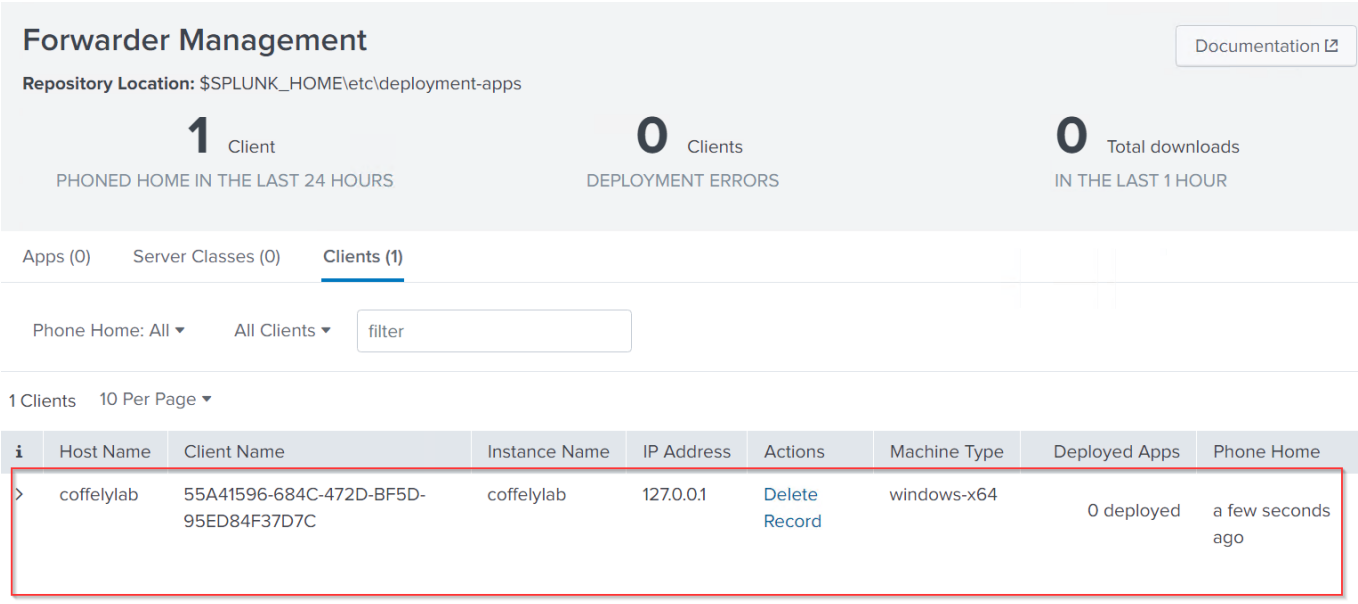


Installing the forwarder on a Windows endpoint will take 3-5 minutes.

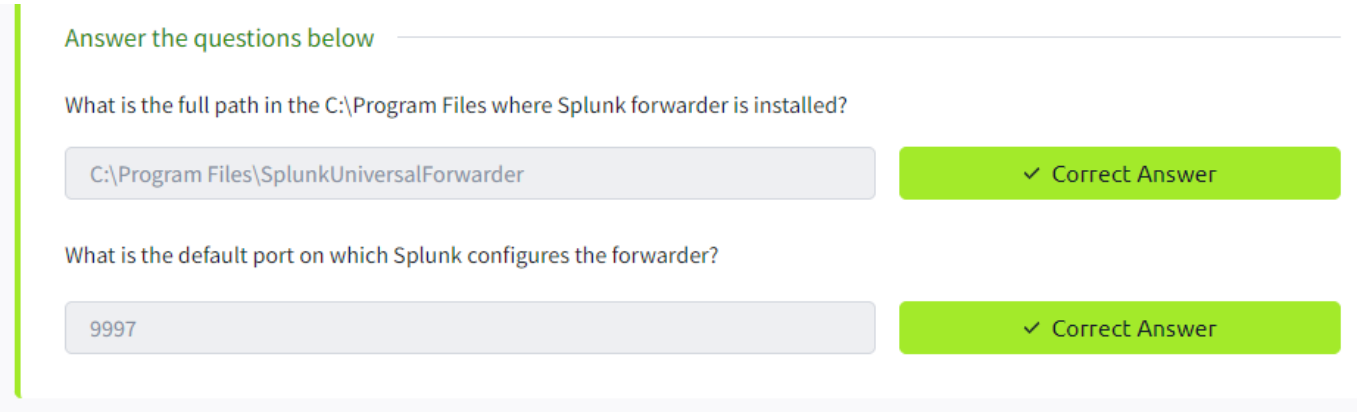

UniversalForwarder Setup
splunk>universal forwarder
Please wait while the Setup Wizard installs UniversalForwarder.
Status: Copying new files
Back
Next



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:



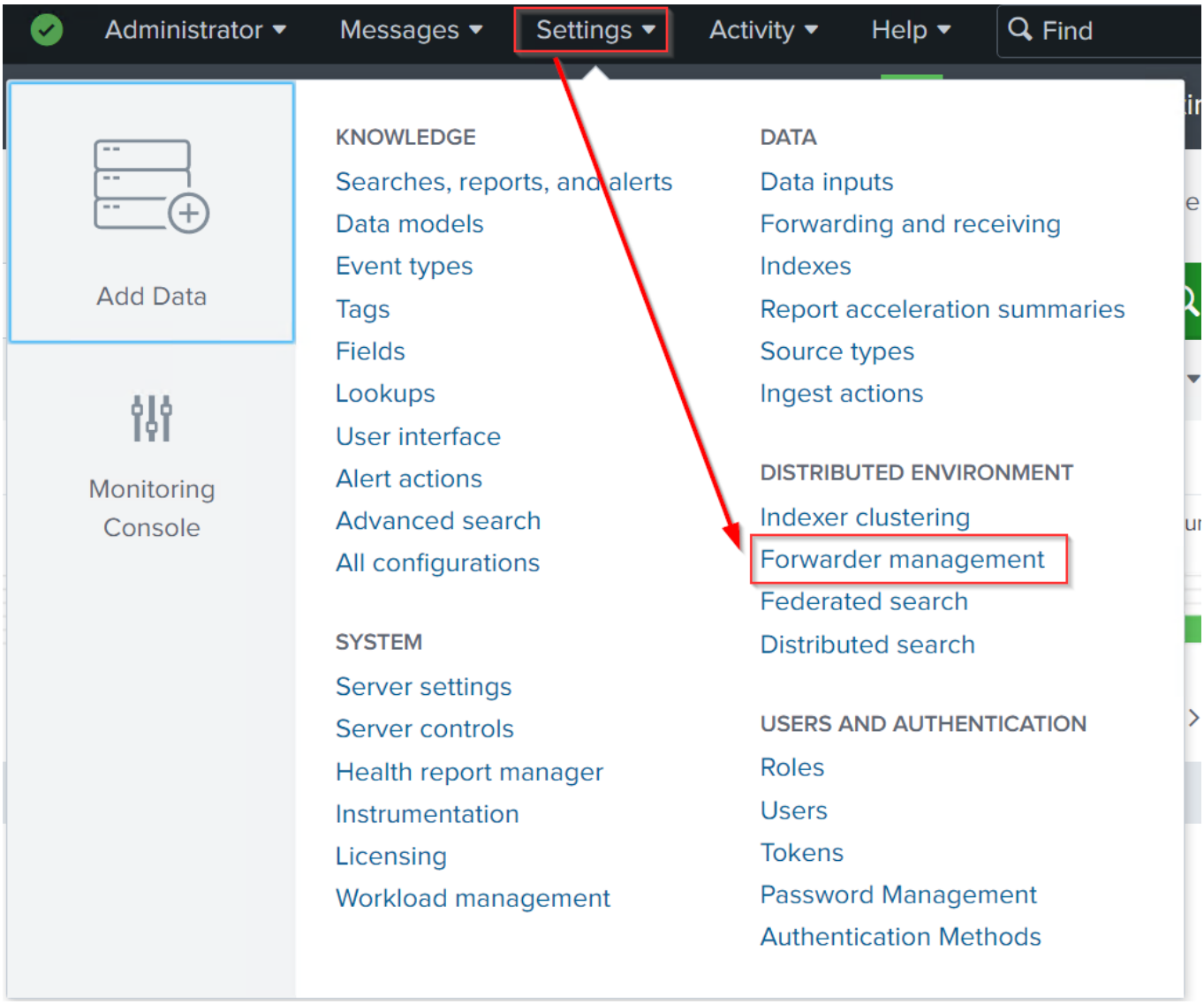
Now that Splunk forwarder is installed, we will now configure our forwarder to send logs to our Splunk instance in the upcoming tasks.



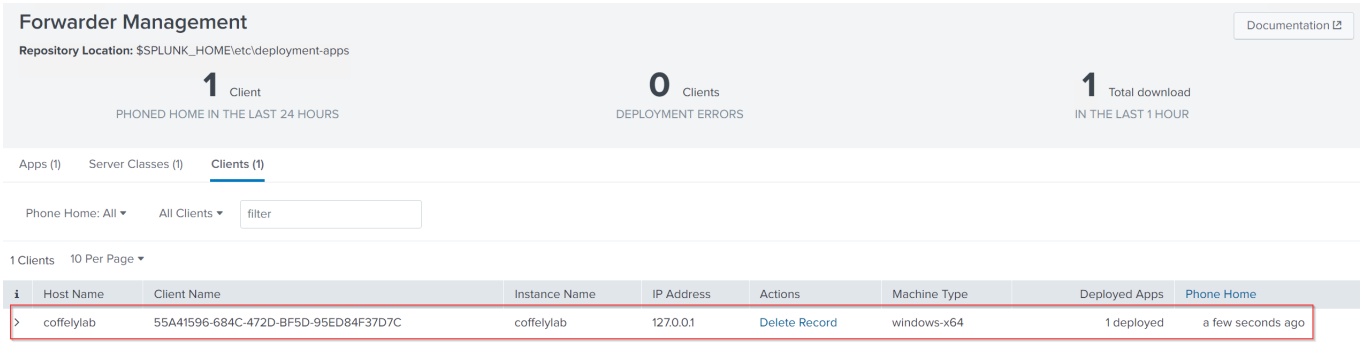
We have installed the forwarder and set up the listener on Splunk. It's time to configure Splunk to receive Event Logs from this host and configure the forwarder to collect Event Logs from the host and send them to the Splunk Indexer. Let's go through this step by step.

Check Forwarder Management

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



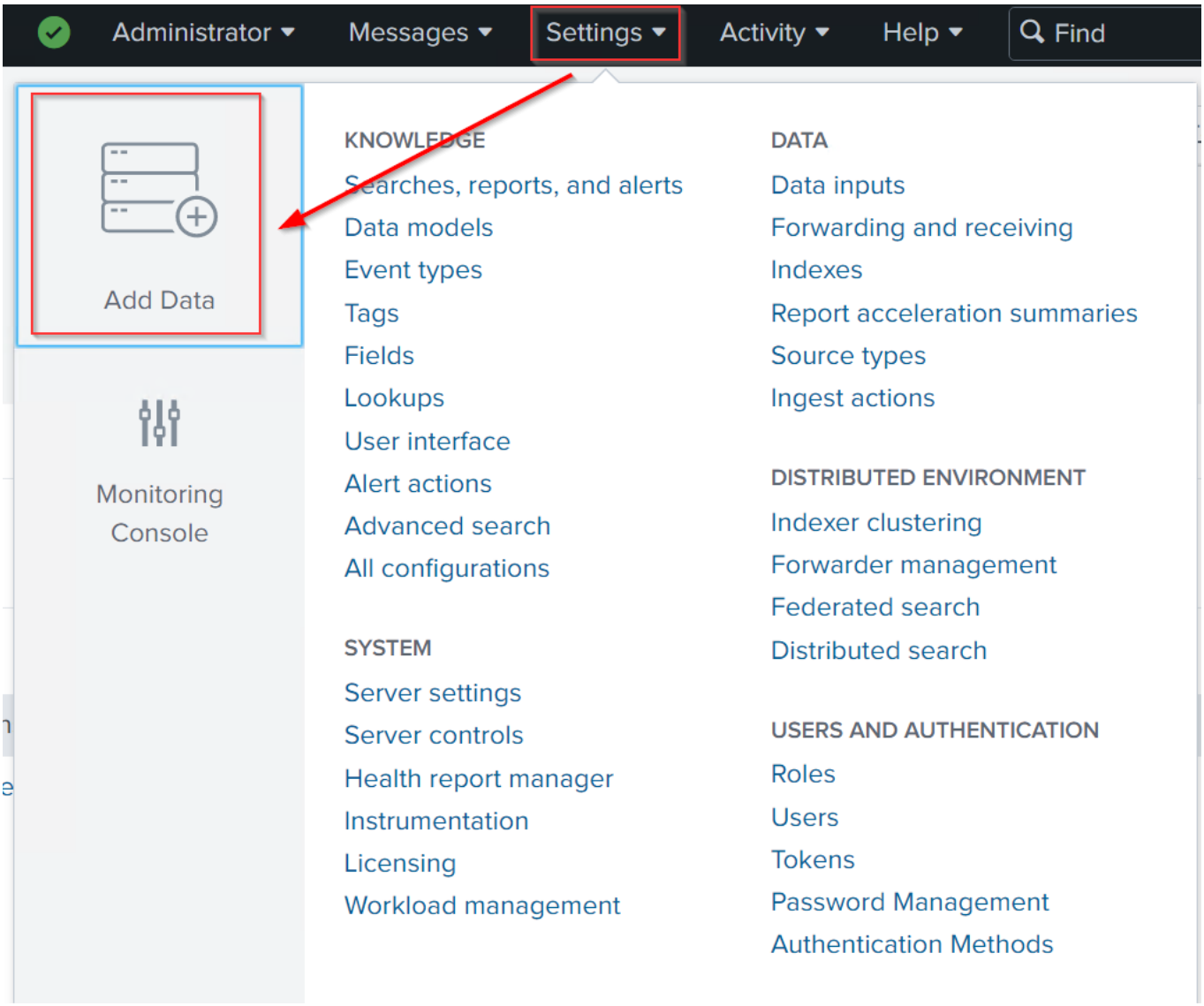
Go to settings -> Forwarder Management tab to get the details of all deployment hosts. In an actual network, this tab will be filled with all the hosts and servers configured to send logs to Splunk Indexer.



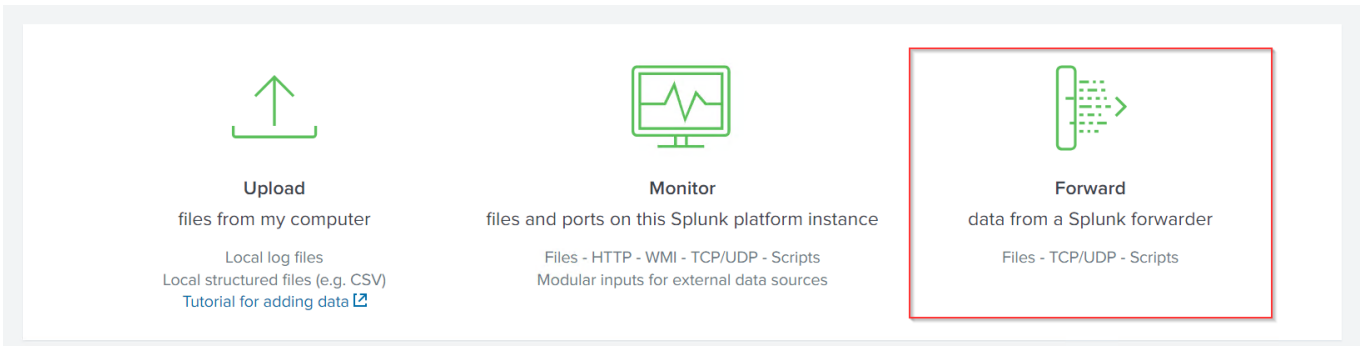
It will appear here if we have properly configured the forwarder on the host. Now it's time to configure Splunk to receive the Event Logs.

Select Forwarder

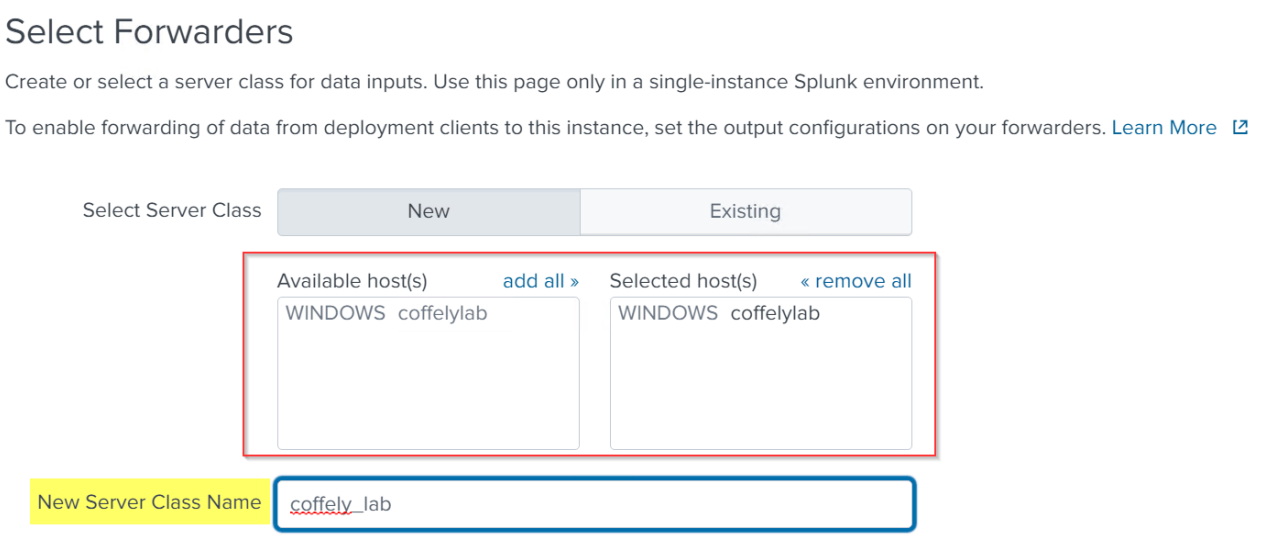
Click on Settings -> Add data. It shows all the options to add data from different sources.



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.

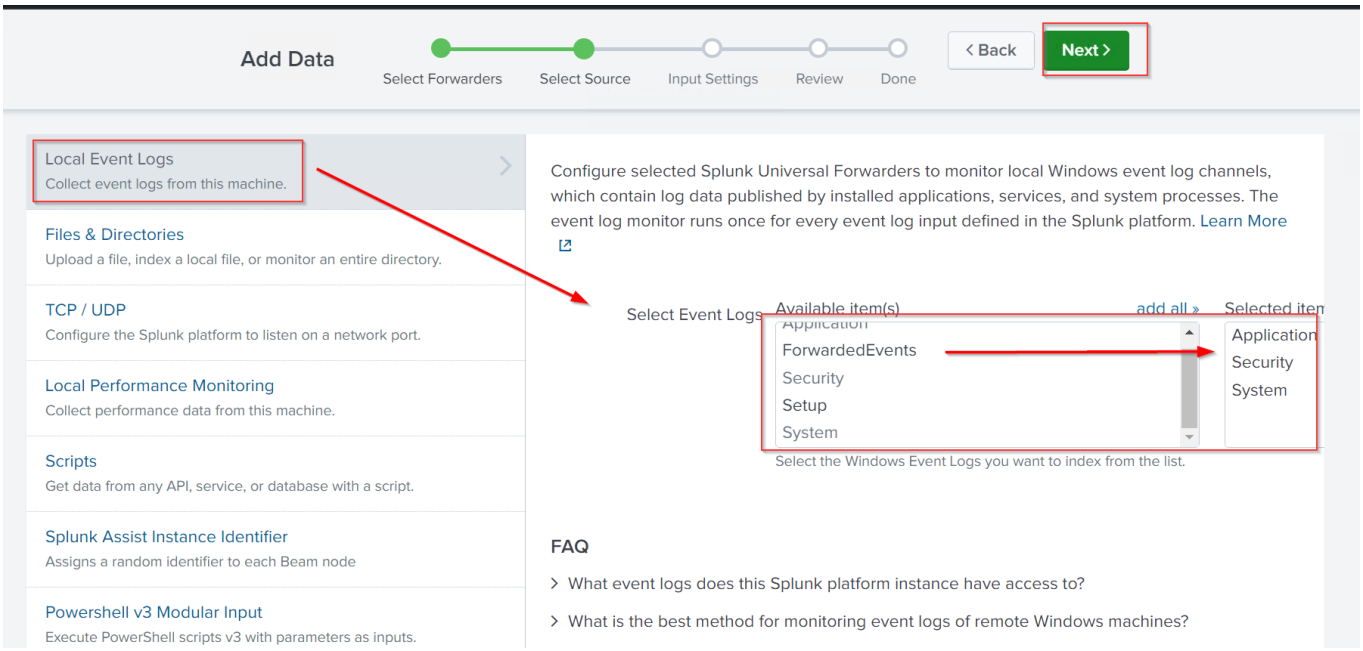


In the **Select Forwarders section,** Click on the host `coffelylab` shown in the Available host(s) tab, and it will be moved to the Selected host(s) tab. Then, click Next.



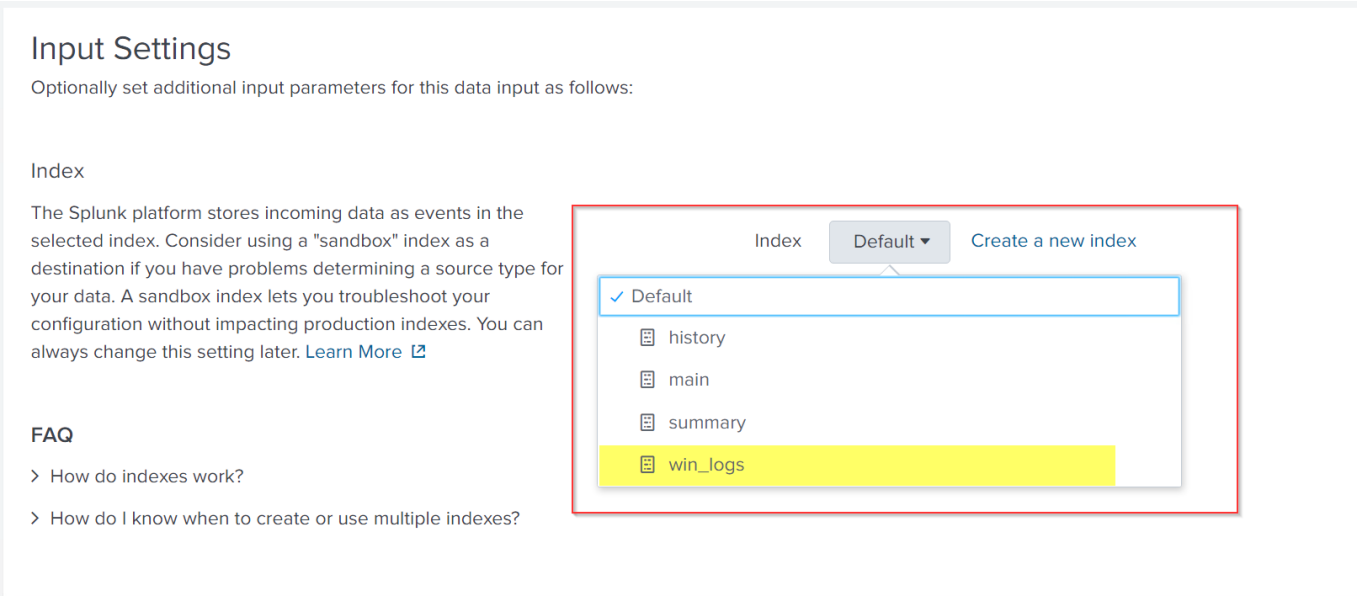
Select Source

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.



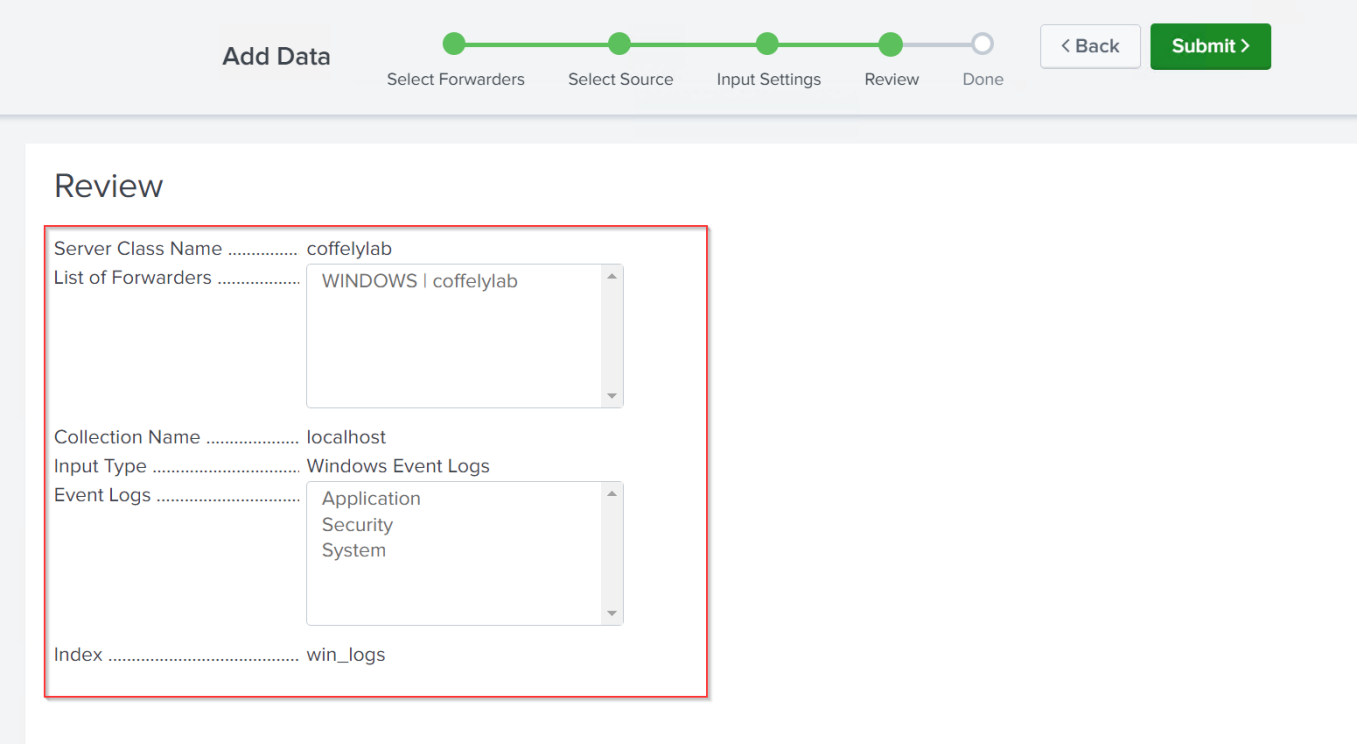
Creating Index

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

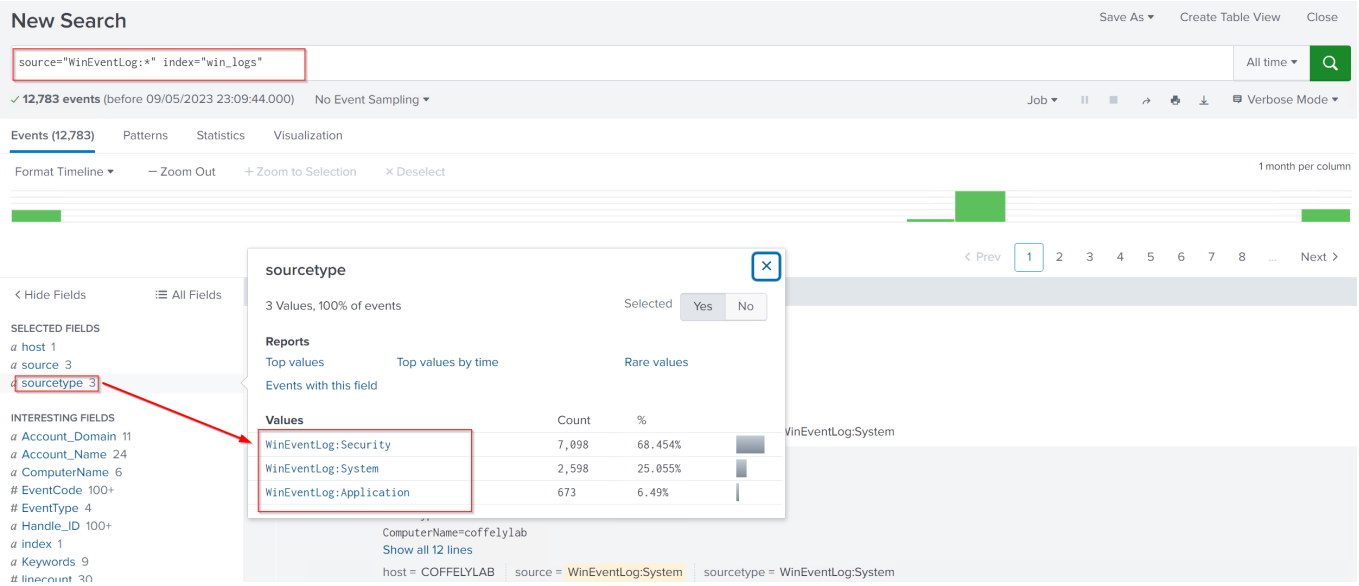


Review

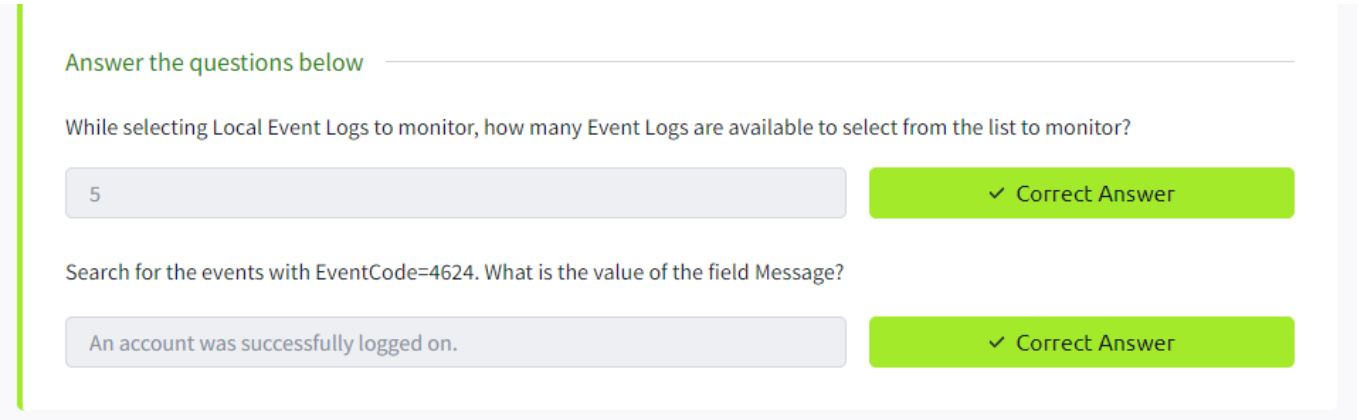
The review tab summarizes the settings we just did to configure Splunk. Move to the next step.



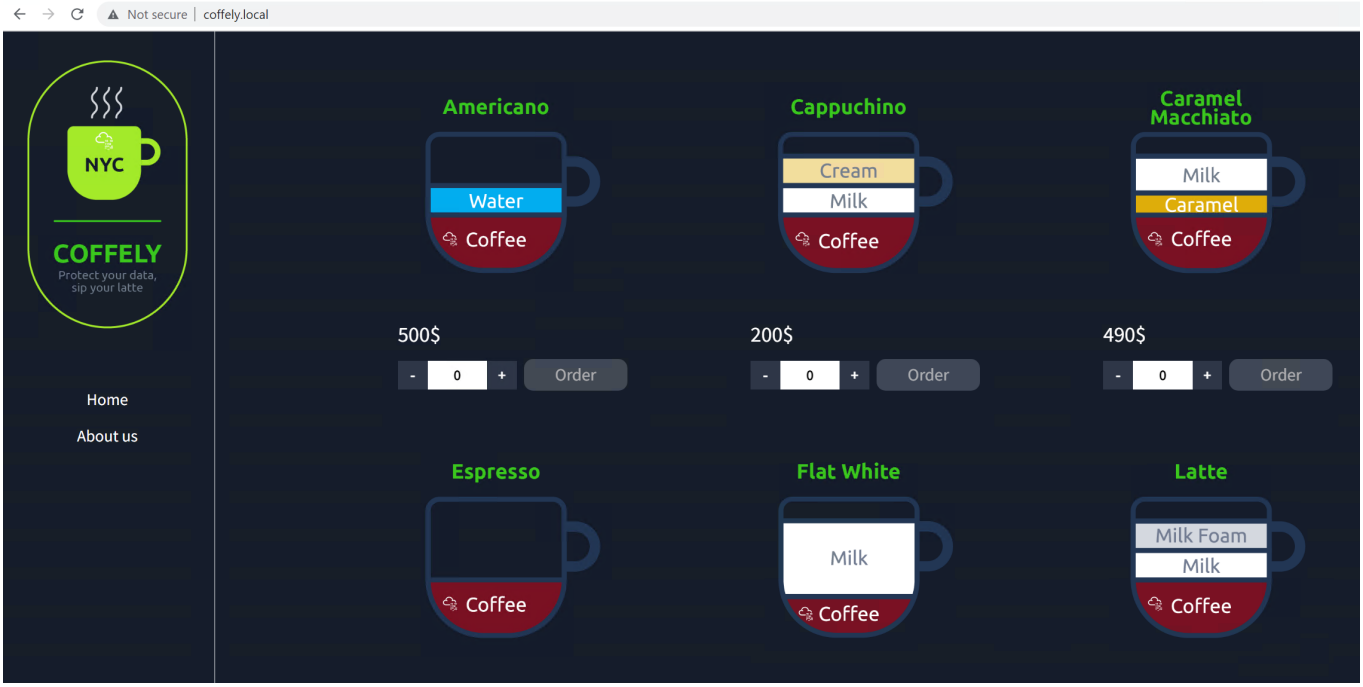
Click on the **Start Searching** tab. It will take us to the Search App. If everything goes smoothly, we will receive the Event Logs immediately.



Great. We have successfully configured Splunk to receive Event Logs from the Windows host. Let's move on to the next task, where we will look at the steps to ingest weblogs.



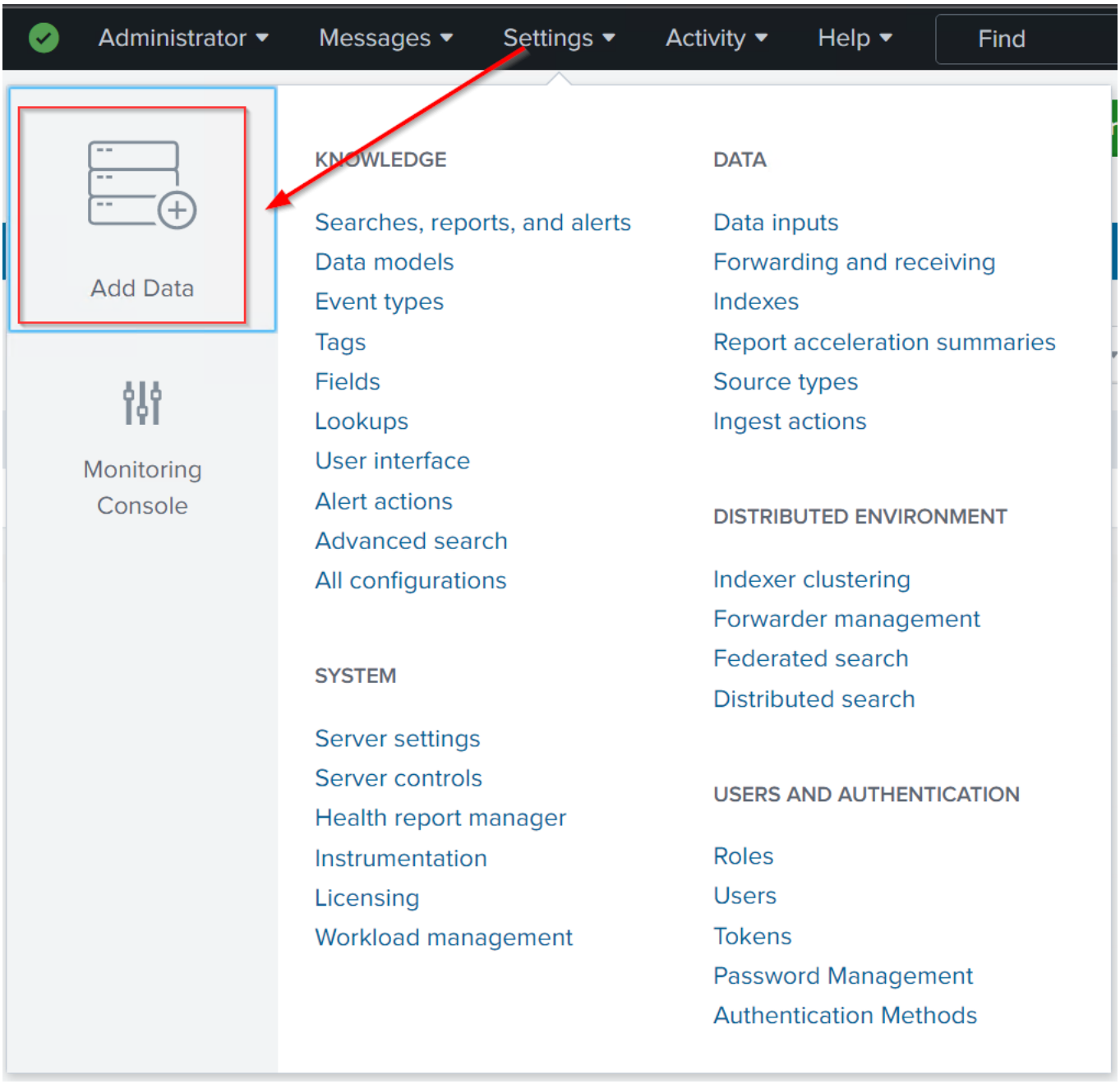
The Windows host we connected to Splunk Instance also hosts a local copy of their website, which can be accessed via `http://coffely.thm` from the VM and is in the development phase. You are asked to configure Splunk to receive the weblogs from this website to trace the orders and improve coffee sales.



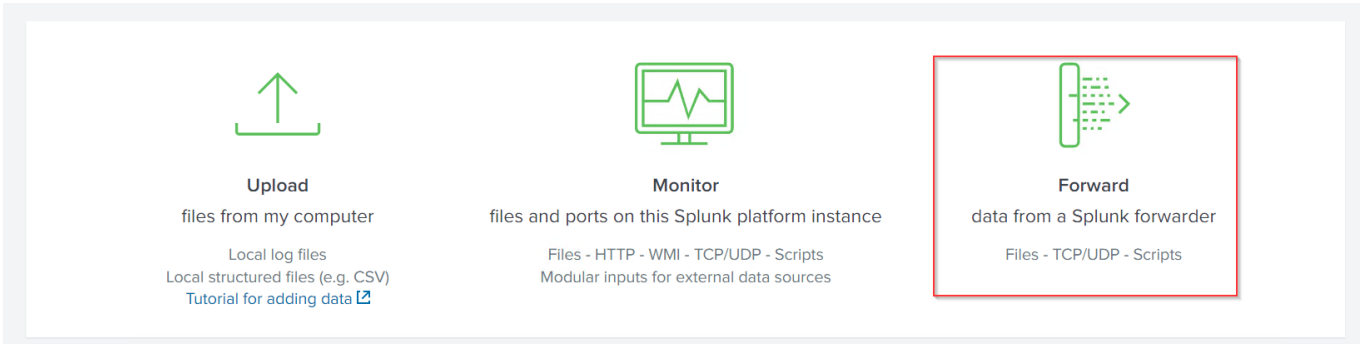
This site will allow users to order coffee online. In the backend, it will keep track of all the requests and responses and the orders placed. Now let's follow the next steps to ingest web logs into Splunk.

Add Data

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

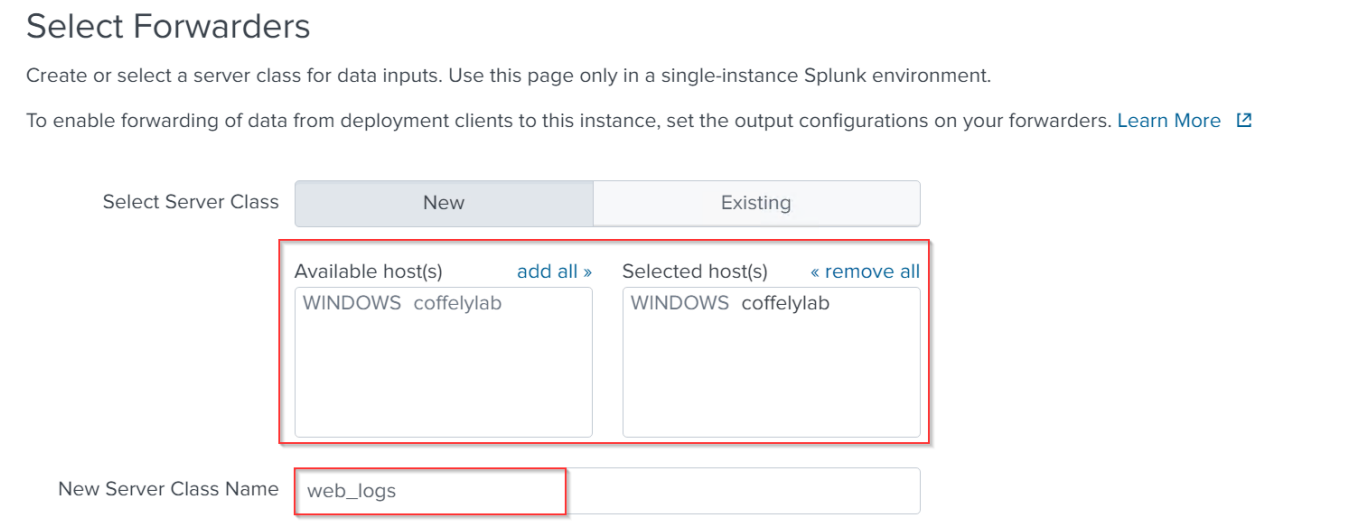


Select the Forwarder option:

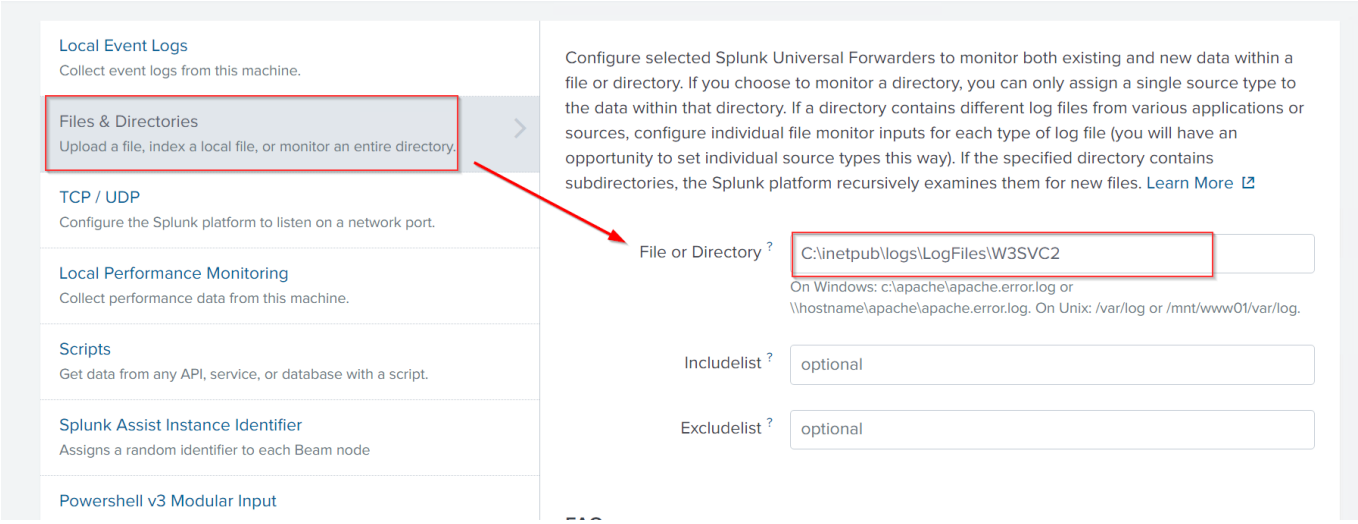


Select Forwarder

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

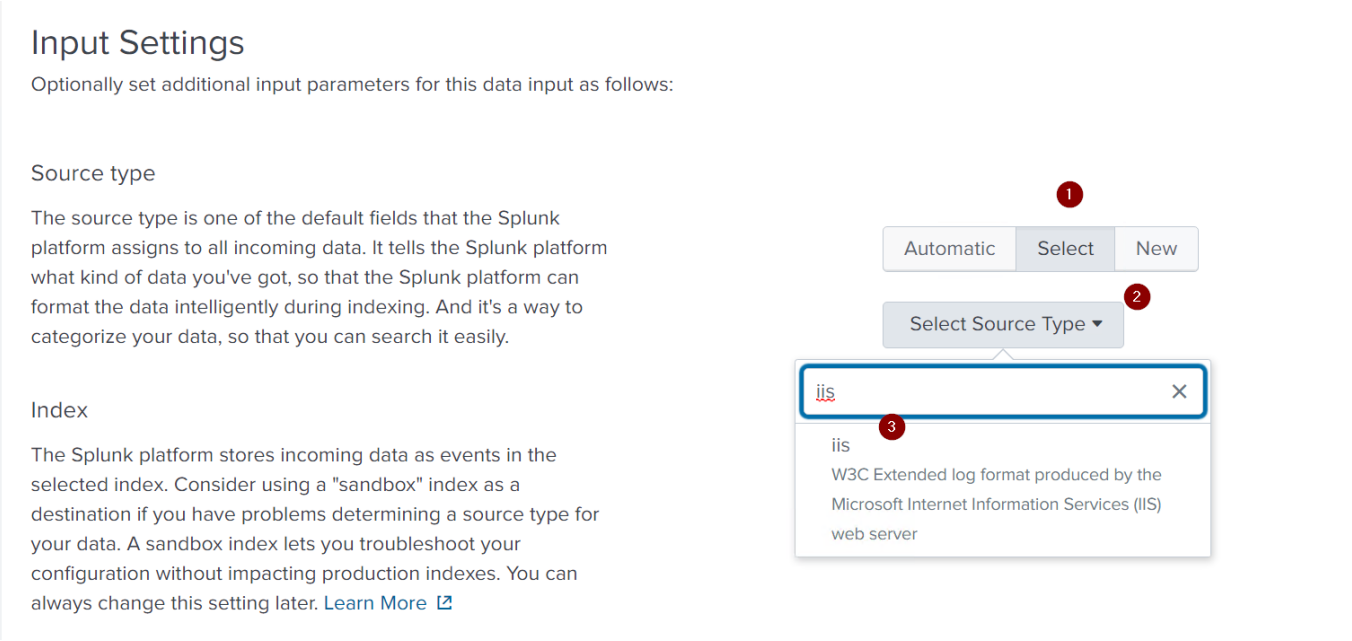


Web logs are placed in the directory `C:\inetpub\logs\LogFiles\W3SVC*`. The directory may contain one or more log files which will be continuously updated with the logs. We will be configuring Splunk to monitor and receive logs from this directory.

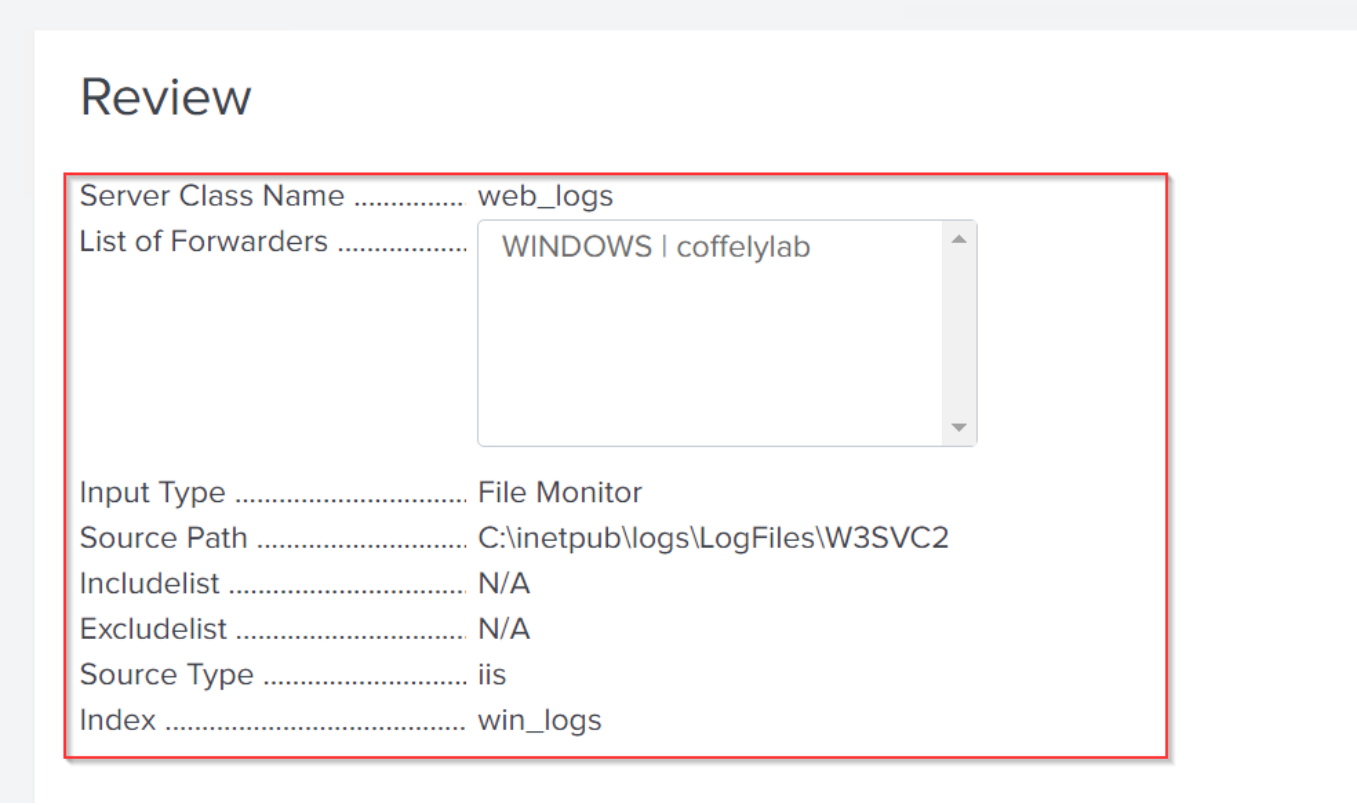


Setting up Source Type

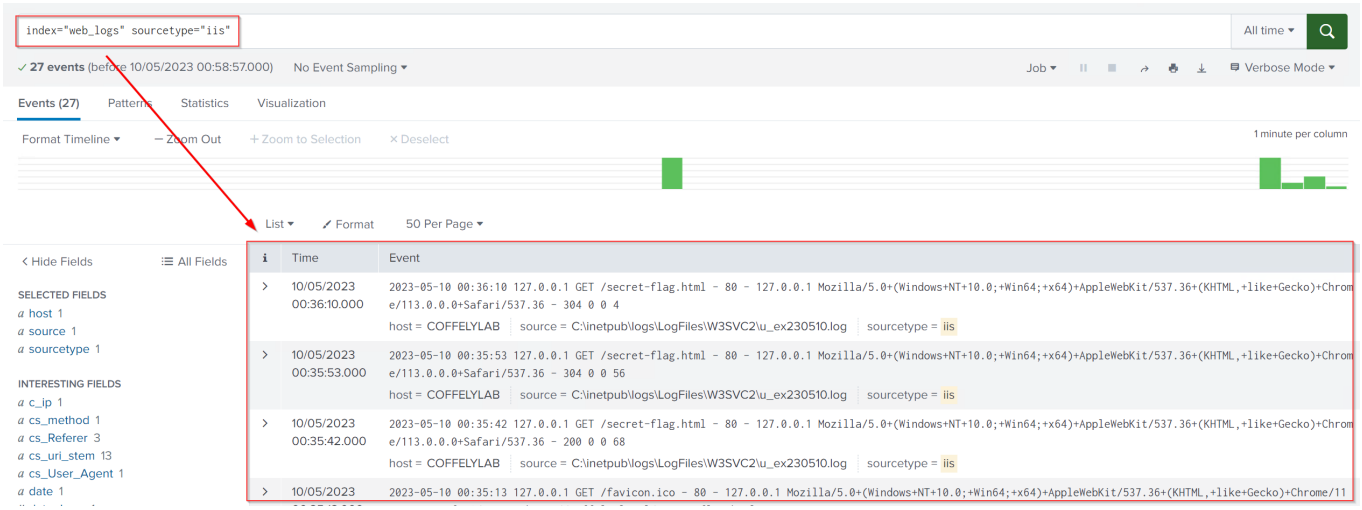
Next, we will select the source type for our logs. As our web is hosted on an IIS server, we will choose this option and create an appropriate index for these logs.



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.