

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.

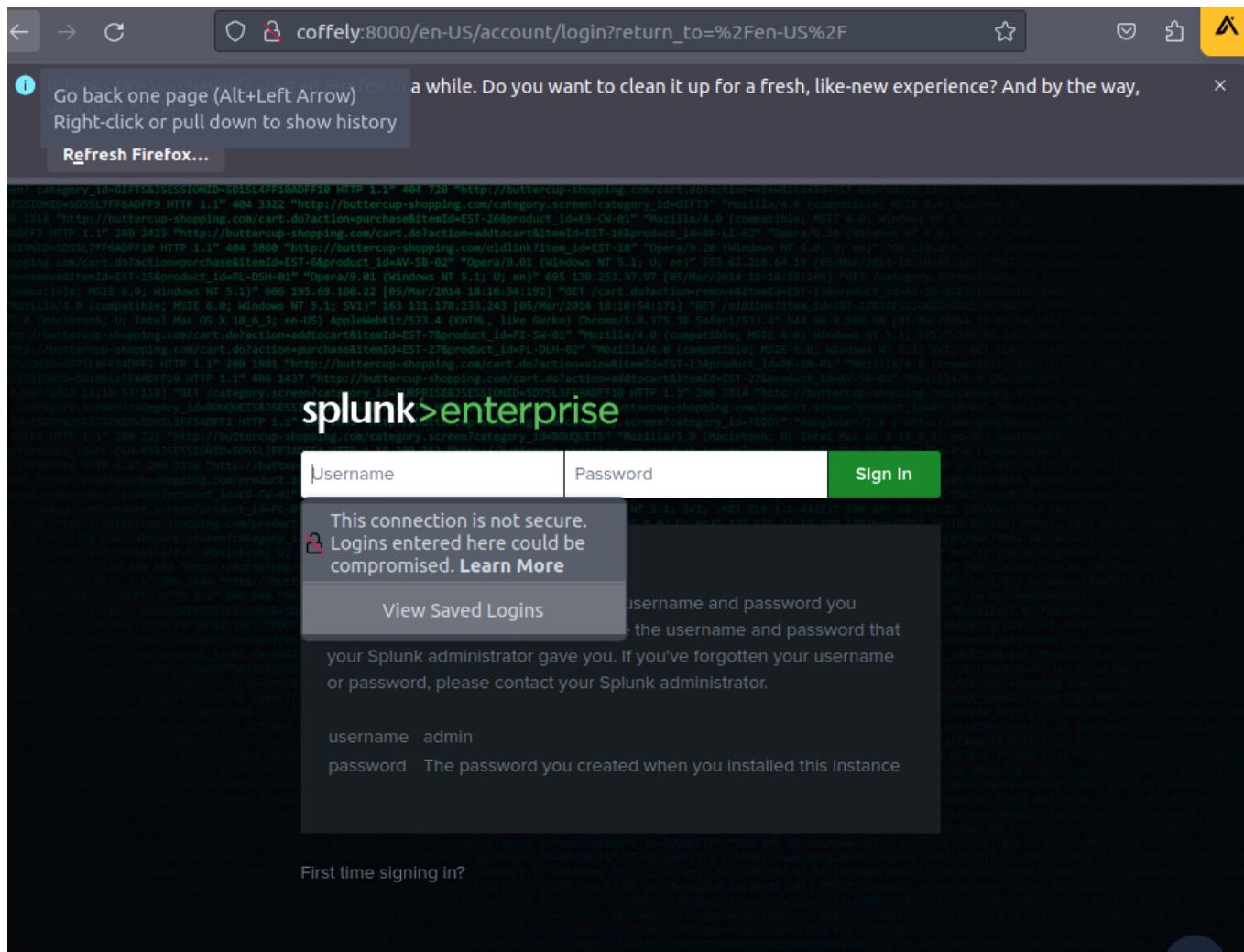
Answer the questions below

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 omitted ...
```

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 omitted ...
```

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	commands that can be used to configure the
help shclustering	Search Head Cluster setup
Search Head Cluster setup	tools to start, stop, manage Splunk
help control, controls	processes
processes	manage Splunk's local filesystem use
help datastore	manage distributed configurations such as
help distributed	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.

Splunk Universal Forwarder 9.0.3

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

The screenshot shows the download page for Splunk Universal Forwarder 9.0.3. The Windows section is highlighted with a pink bar. It lists two options: "32-bit" and "64-bit". The "64-bit" option is selected and shows details for "Windows 10 , Windows 11" and "Windows Server 2012, 2012 R2, 2016, 2019, 2022". Both options have ".msi" files with sizes of 64.31 MB and 77.38 MB respectively. Each option has a "Download Now" button with a downward arrow icon.

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.

Answer the questions below

What is the default port, on which Splunk Forwarder runs on?

8089

✓ Correct Answer

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:

The screenshot shows the Splunk web interface with the 'Settings' dropdown menu open. The 'Forwarding and receiving' option is highlighted with a yellow background and a red arrow pointing to it from the top right. The menu is organized into several sections: KNOWLEDGE, DATA, EXPLORE DATA, EXPLORE DATA (continued), SYSTEM, and USERS AND AUTHENTICATION. Each section contains various configuration options.

Section	Options
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
EXPLORE DATA	Explore Data
EXPLORE DATA (continued)	Explore Data
SYSTEM	Server settings Server controls Health report manager RapidDiag Instrumentation Licensing Workload management
USERS AND AUTHENTICATION	Roles Users Tokens Password Management Authentication Methods

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.

The screenshot shows the 'Forwarding and receiving' page. In the 'Receive data' section, there is a red box around the 'Configure receiving' link. A red arrow points from this box to a green button labeled 'New Receiving Port' at the top right of the page.

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:

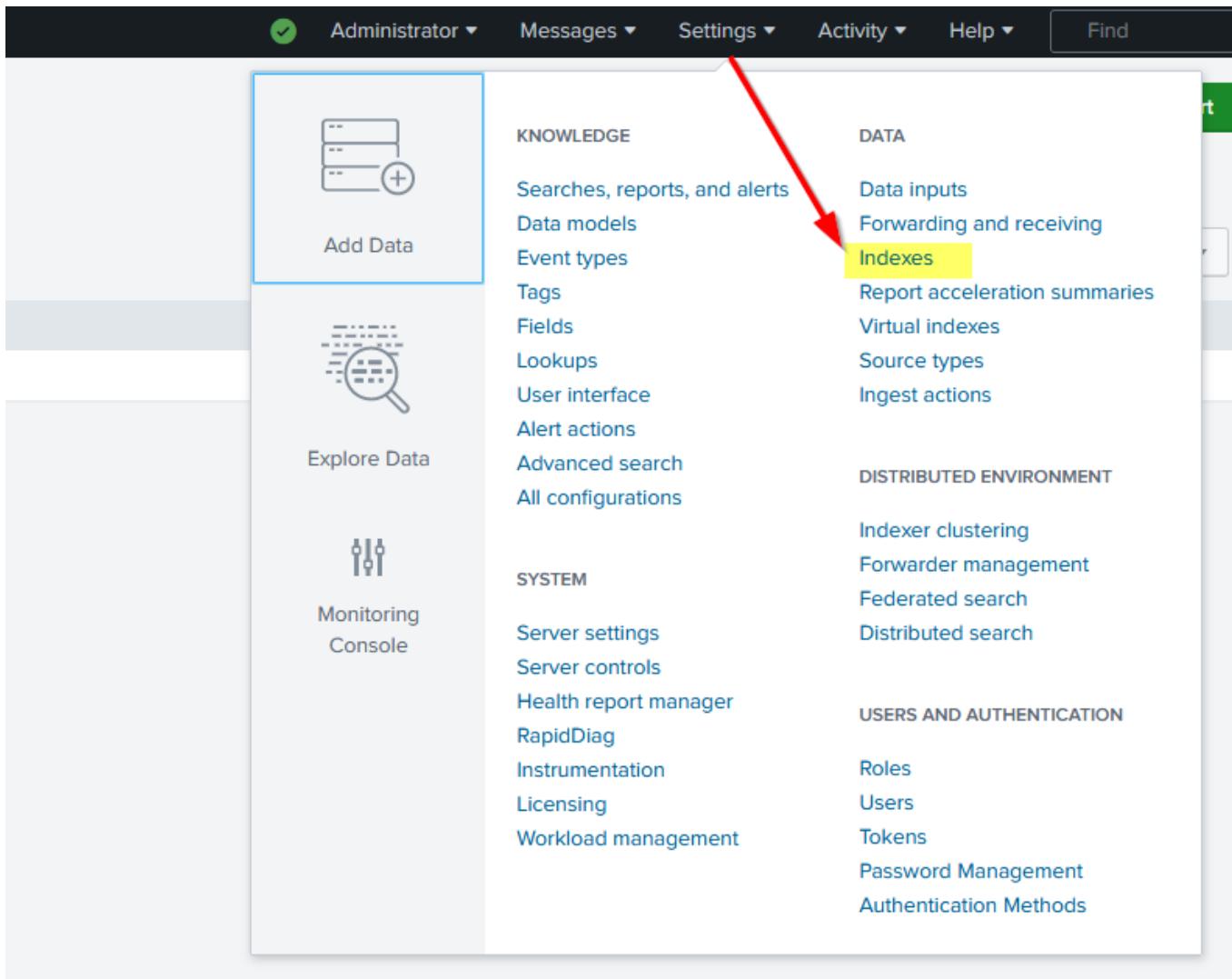
The screenshot shows the 'Configure receiving' dialog. The 'Listen on this port' field contains '9997'. A red box highlights this field. Below it, a note says 'For example, 9997 will receive data on TCP port 9997.' At the bottom are 'Cancel' and 'Save' buttons, with 'Save' being green.

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.

The screenshot shows the 'Receive data' list view. A blue banner at the top says 'Successfully saved "9997".' The table has columns for 'Listen on this port', 'Status', and 'Actions'. The row for port 9997 is highlighted with a yellow background. The 'Status' column shows 'Enabled | Disable'. The 'Actions' column shows a 'Delete' link.

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.

This screenshot shows the 'Indexes' table page. At the top, there's a header with 'Indexes' and a note: 'A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. Learn more.' Below the header, there are buttons for 'New Index' (highlighted with a yellow box and a red arrow), 'filter', and a search icon. The table itself has 12 rows and columns for Name, Actions, Type, App, Current Size, Max Size, Event Count, Earliest Event, Latest Event, Home Path, Frozen Path, and Status. The 'Actions' column includes Edit, Delete, and Disable buttons. The 'Status' column shows green checkmarks for most entries except for 'splunklogger' which is marked as 'Disabled' with a red lock icon. The table also includes a '20 per page' dropdown.

Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen Path	Status
_audit	Edit Delete Disable	Events	system	4 MB	488.28 GB	30.6K	3 days ago	a few seconds ago	\$SPLUNK_DB/audit/db	N/A	Enabled
_configtracker	Edit Delete Disable	Events	system	3 MB	488.28 GB	250	3 days ago	7 minutes ago	\$SPLUNK_DB/_configtracker/db	N/A	Enabled
_internal	Edit Delete Disable	Events	system	84 MB	488.28 GB	1.58M	3 days ago	a few seconds ago	\$SPLUNK_DB/_internal/db	N/A	Enabled
_introspection	Edit Delete Disable	Events	system	289 MB	488.28 GB	216K	3 days ago	a few seconds ago	\$SPLUNK_DB/_introspection/db	N/A	Enabled
_metrics	Edit Delete Disable	Metrics	system	48 MB	488.28 GB	1.39M	3 days ago	a few seconds ago	\$SPLUNK_DB/_metrics/db	N/A	Enabled
_metrics_rollup	Edit Delete Disable	Metrics	system	1 MB	488.28 GB	0			\$SPLUNK_DB/_metrics_rollup/db	N/A	Enabled
_telemetry	Edit Delete Disable	Events	system	1 MB	488.28 GB	26	2 days ago	6 hours ago	\$SPLUNK_DB/_telemetry/db	N/A	Enabled
_thefishbucket	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/_thefishbucket/db	N/A	Enabled
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/historydb/db	N/A	Enabled
main	Edit Delete Disable	Events	system	7 MB	488.28 GB	69.4K	3 years ago	26 minutes ago	\$SPLUNK_DB/defaultdb/db	N/A	Enabled
splunklogger	Edit Delete Enable	Events	system	0 B	488.28 GB	0			\$SPLUNK_DB/splunklogger/db	N/A	Disabled
summary	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/summarydb/db	N/A	Enabled

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:

New Index

General Settings

Index Name	Linux_host	
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.		
Max Size of Hot/Warm/Cold Bucket	auto	GB ▾
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

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.

```
root@coffely:/var/log$ ls
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
audit               gpu-manager-switch.log syslog.1
auth.log             gpu-manager.log syslog.2.gz
auth.log.1           hp             syslog.3.gz
btmp                journal        syslog.4.gz
cloud-init-output.log kern.log      syslog.5.gz
cloud-init.log       kern.log.1    syslog.6.gz
cups                landscape     syslog.7.gz
dist-upgrade        lastlog       unattended-upgrades
dmesg               lightdm       wtmp
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.

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
```

The screenshot shows the Splunk interface with a search bar containing 'index=Linux_host'. Below it, a table displays search results. A red arrow points from the search bar to the first log entry in the table, which is highlighted with a red box. The log entry is: 'Sep 7 11:06:33 coffely ubuntu: coffely-has-the-best-coffe-in-town'. The table has columns for Time and Event. The Time column shows 'Sep 7 11:06:33.000 AM' and the Event column shows the log message. The interface includes various navigation and search controls.

Time	Event
Sep 7 11:06:33.000 AM	coffely-has-the-best-coffe-in-town host = coffely source = /var/log/syslog sourcetype = syslog
Sep 7 11:02:22.000 AM	Timed out waiting for reply from 185.125.190.57:123 (ntp.ubuntu.co m). host = coffely source = /var/log/syslog sourcetype = syslog
Sep 7 11:02:11.000 AM	Timed out waiting for reply from 185.125.190.56:123 (ntp.ubuntu.co m). host = coffely source = /var/log/syslog sourcetype = syslog

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?

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.

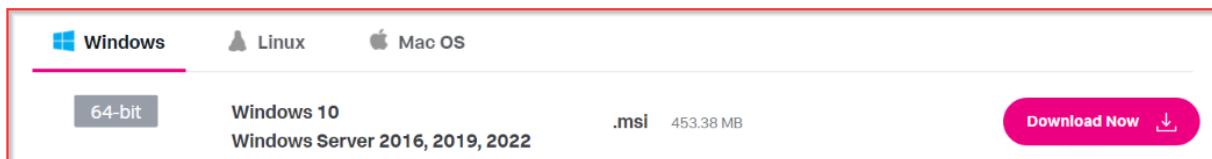
Downloading Splunk Enterprise

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

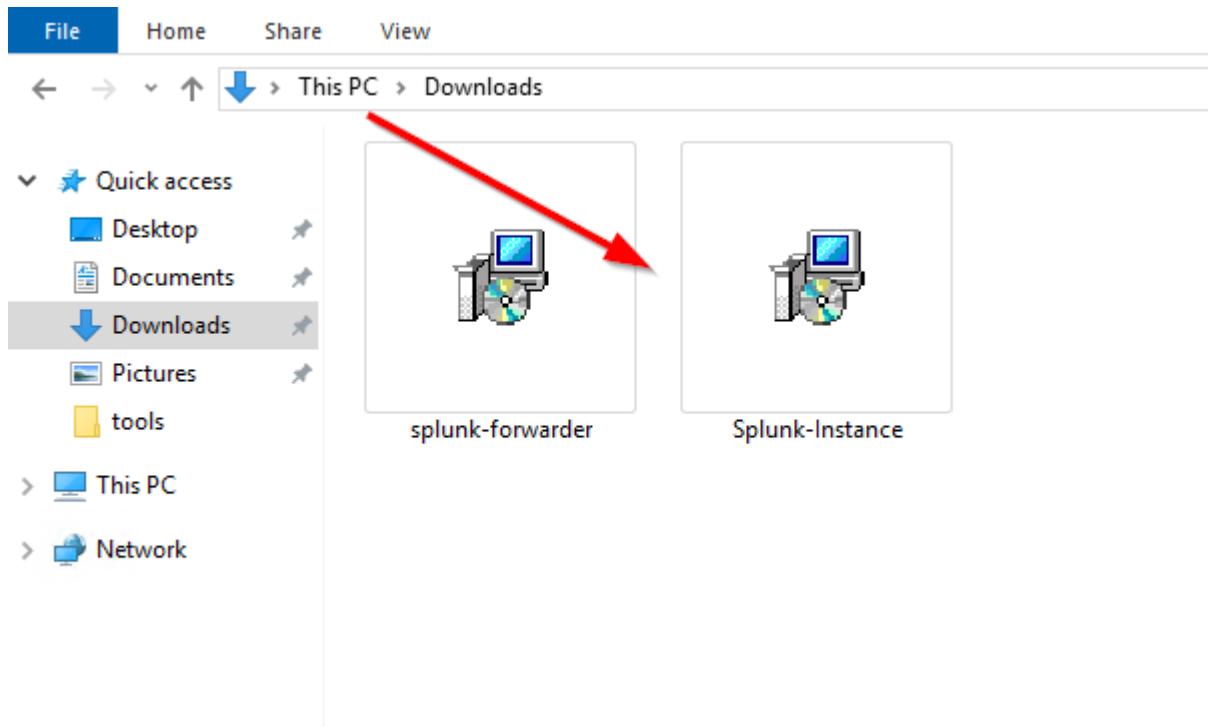
Splunk Enterprise 9.0.4

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

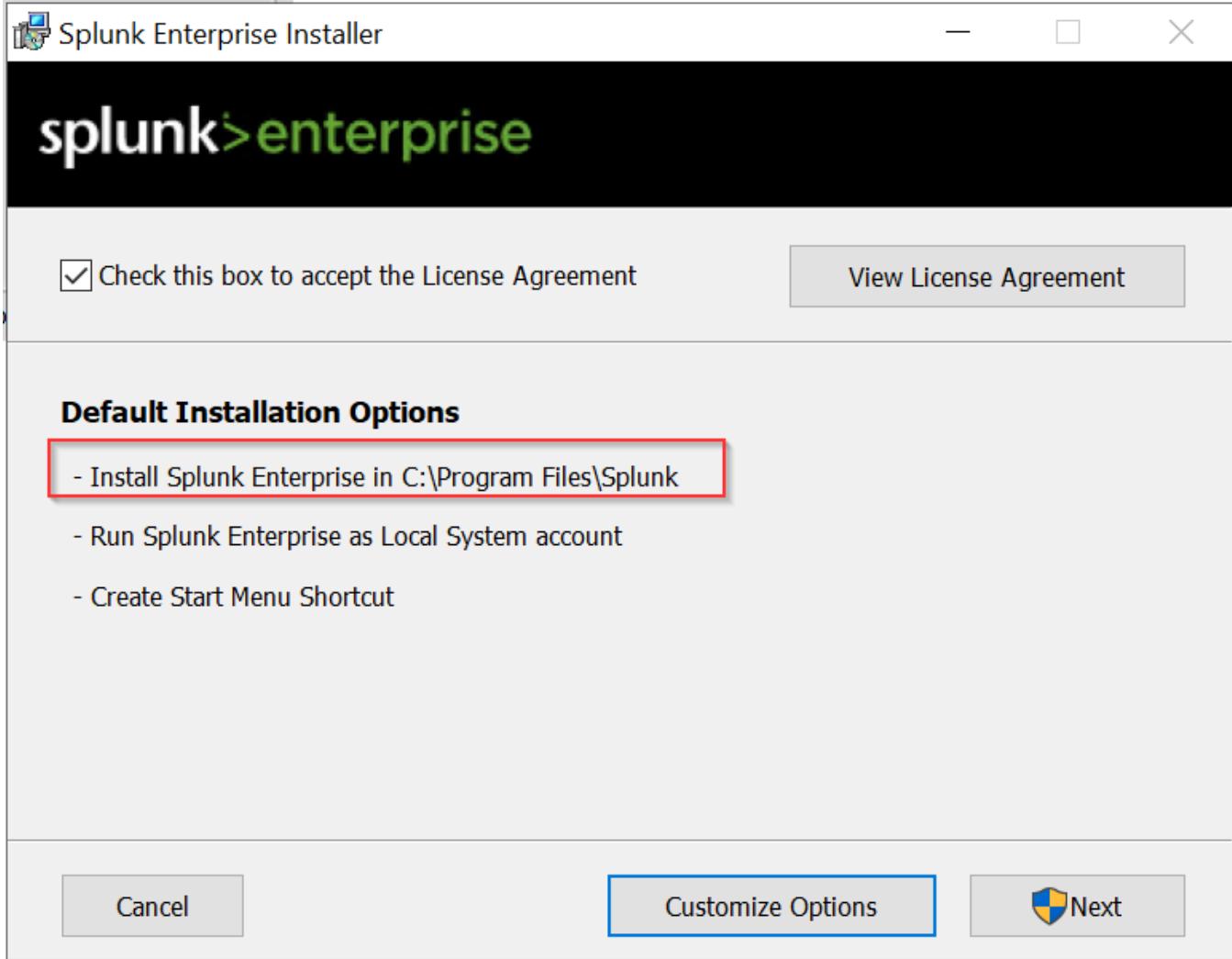


The installer Splunk-Instance is already been downloaded and placed in the `Downloads` folder to speed up the process.



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.

splunk>enterprise

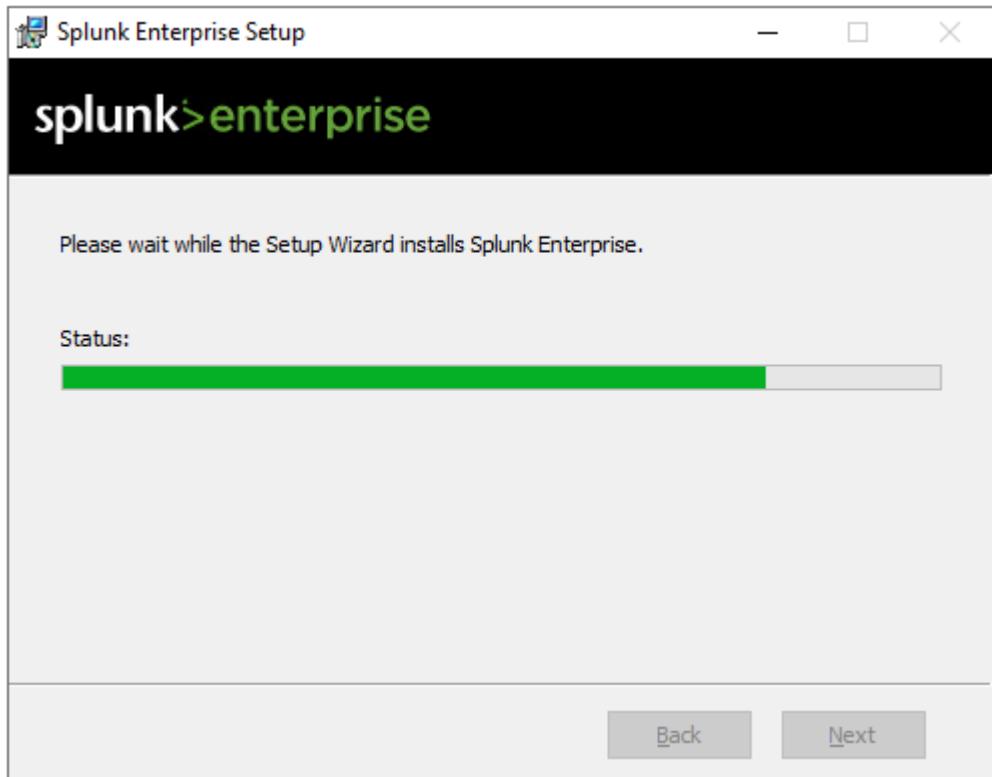
Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

Username:

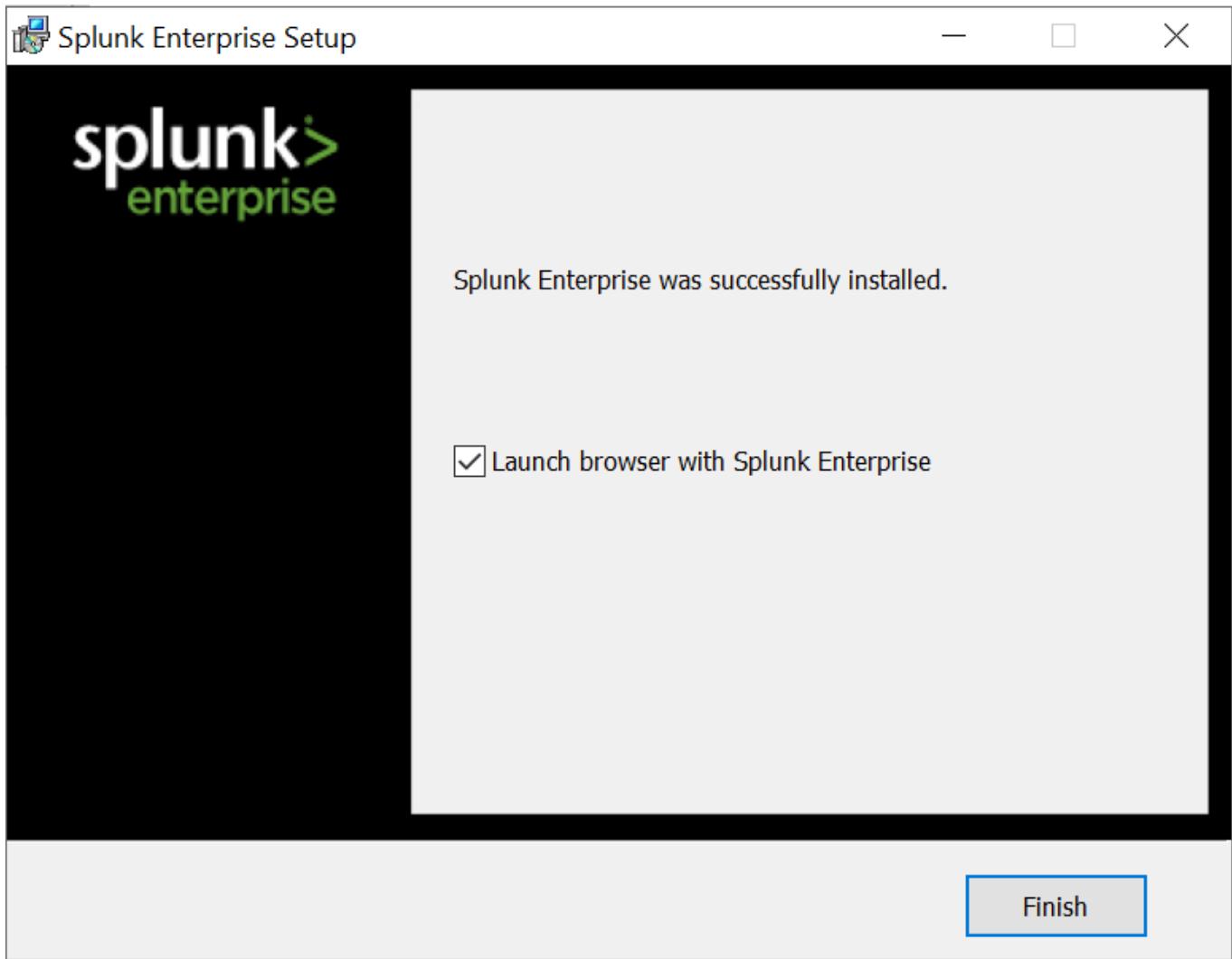
Password:

Confirm password:

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

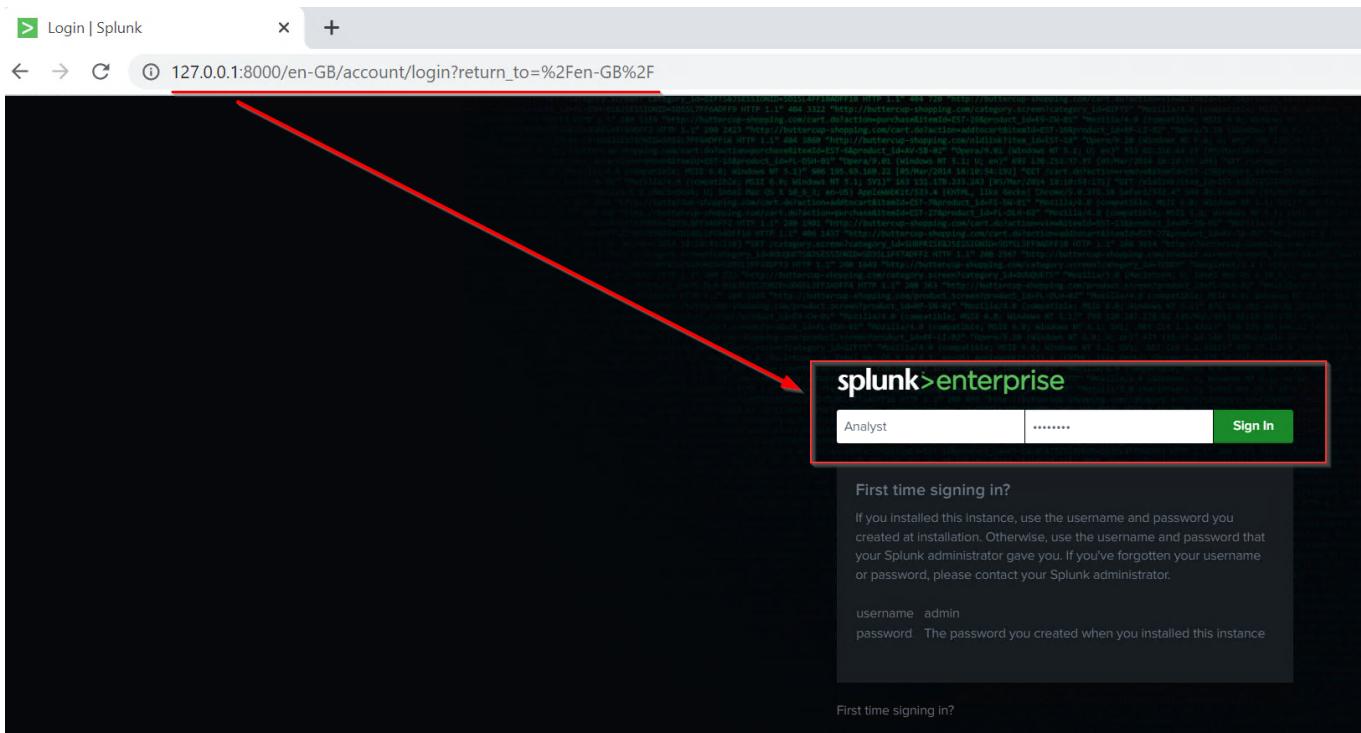


We will get the following message if all system requirements are met, and installation is complete.

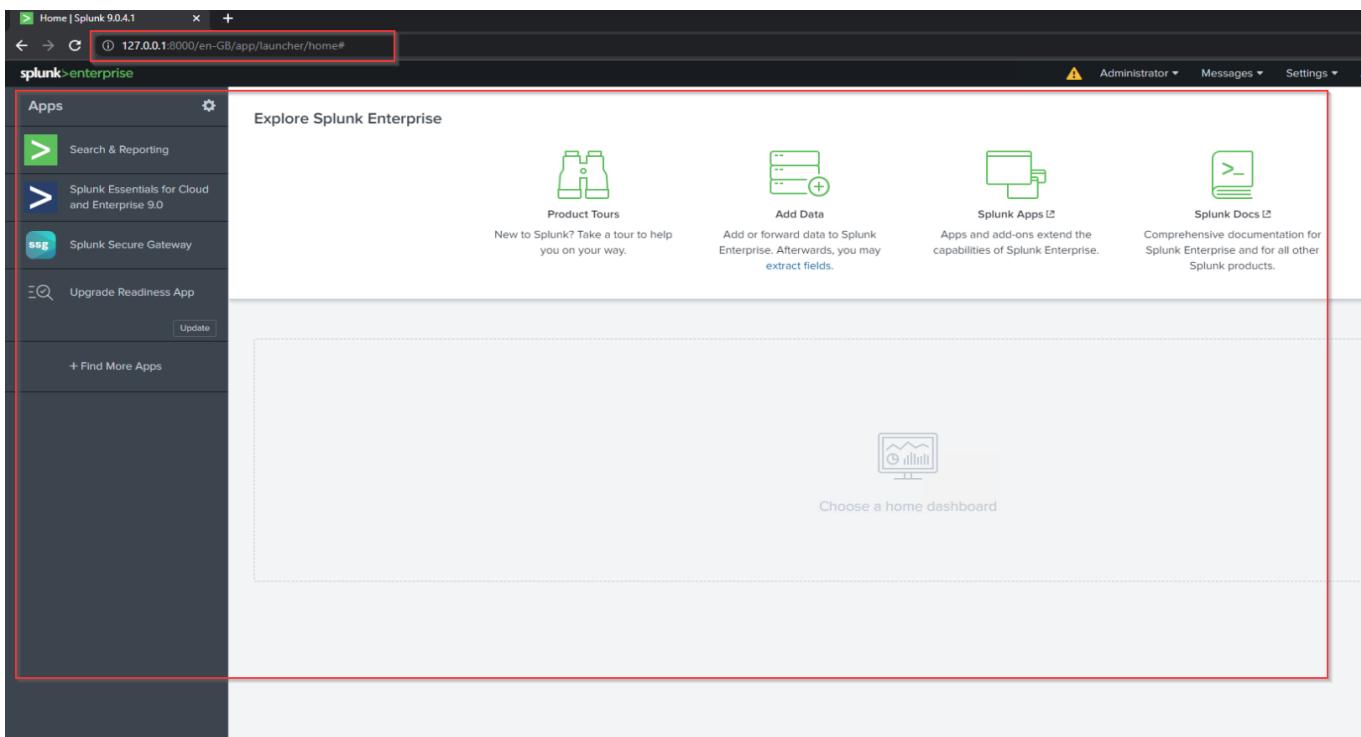


Accessing Splunk Instance

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:

The screenshot shows the Splunk Settings menu. The 'DATA' section is expanded, and the 'Forwarding and receiving' option is highlighted with a red box and a red arrow pointing to it from the top right. Other options in the DATA section include 'Data inputs', 'Indexes', 'Report acceleration summaries', 'Source types', and 'Ingest actions'. The 'Forwarding and receiving' section contains sub-options like 'Forwarder management', 'Federated search', and 'Distributed search'. The 'Monitoring Console' section shows event counts for various sources. The 'Add Data' button is also visible.

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.

Forward data

Set up forwarding between two or more Splunk instances.

[Forwarding defaults](#)

[Configure forwarding](#)

[+ Add new](#)

Receive data

Configure this instance to receive data forwarded from other instances.

[Configure receiving](#)

[+ Add new](#)

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:

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](#)

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.

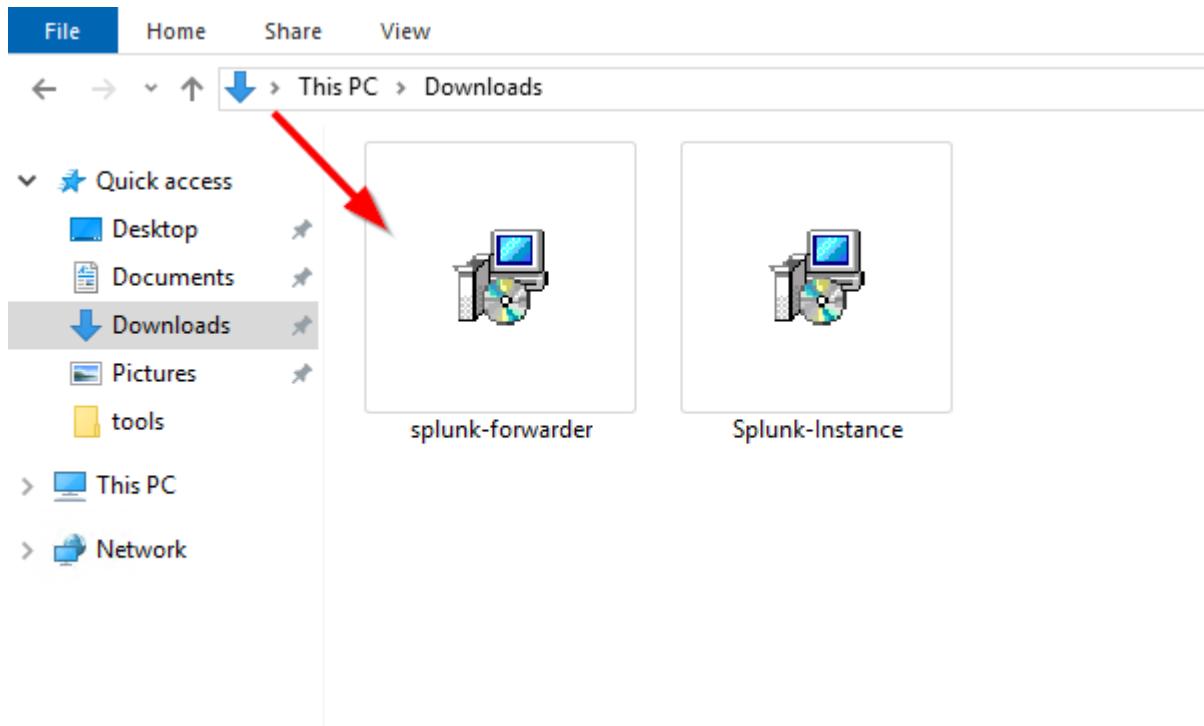
Splunk Universal Forwarder 9.0.4

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

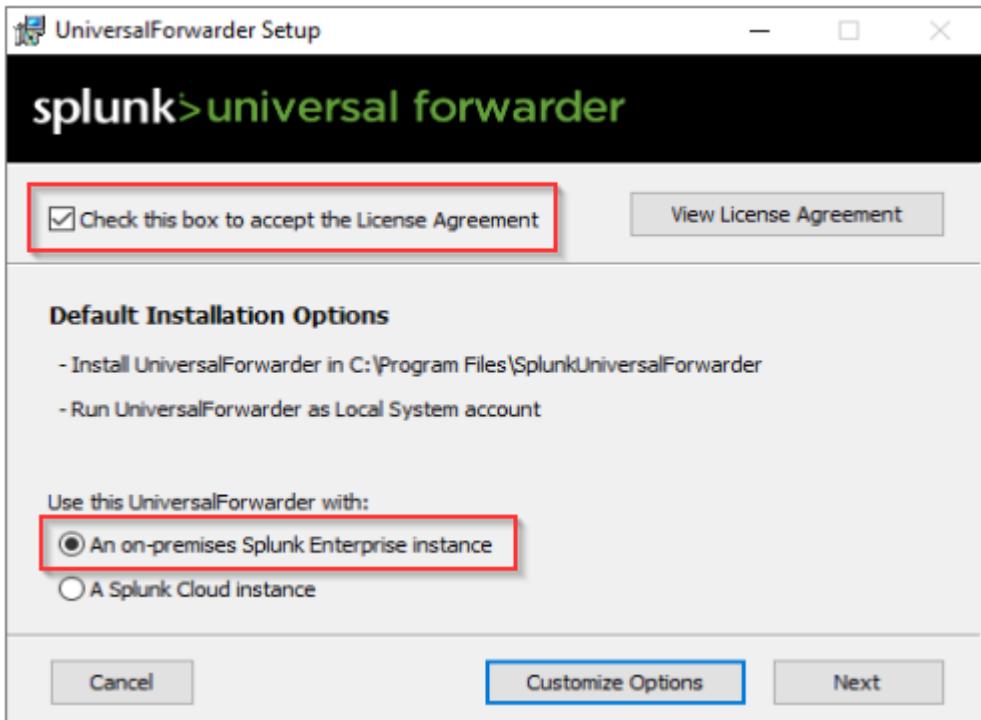
The screenshot shows the download page for Splunk Universal Forwarder 9.0.4. At the top, there are links for Windows, Linux, Mac OS, FreeBSD, Solaris, and AIX. Below these, two main sections are shown: '64-bit' and '32-bit'. The '64-bit' section contains a link for 'Windows 10 , Windows 11' with a note about compatibility with Windows Server 2012, 2012 R2, 2016, 2019, and 2022. It specifies a file size of .msi 77.41 MB. To the right is a pink 'Download Now' button with a downward arrow icon. The '32-bit' section contains a link for 'Windows 10' with a file size of .msi 64.34 MB. It also has a 'Download Now' button with a downward arrow icon.

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.



UniversalForwarder Setup



splunk>universal forwarder

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

Username:

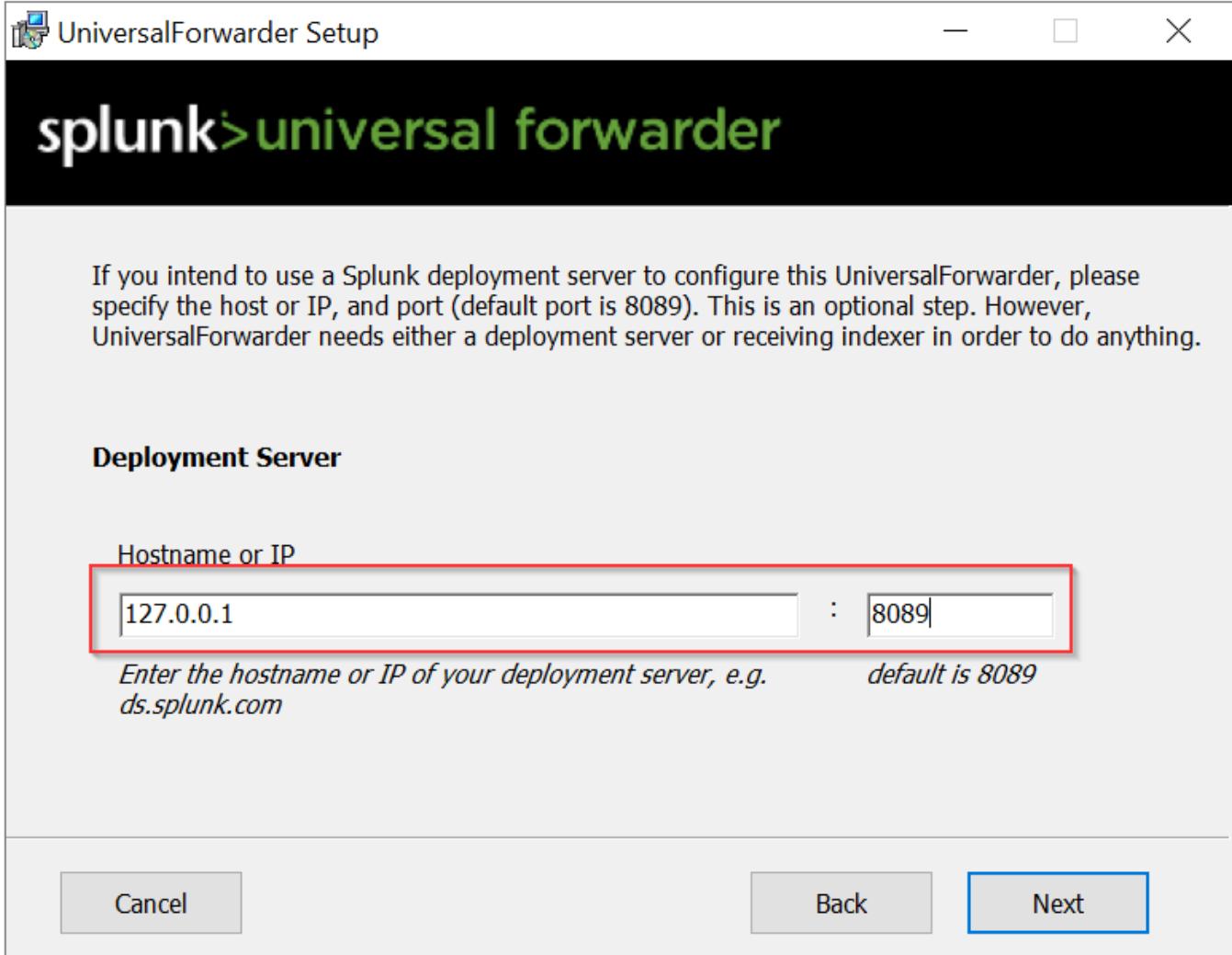
Generate random password

Password:

Confirm password:

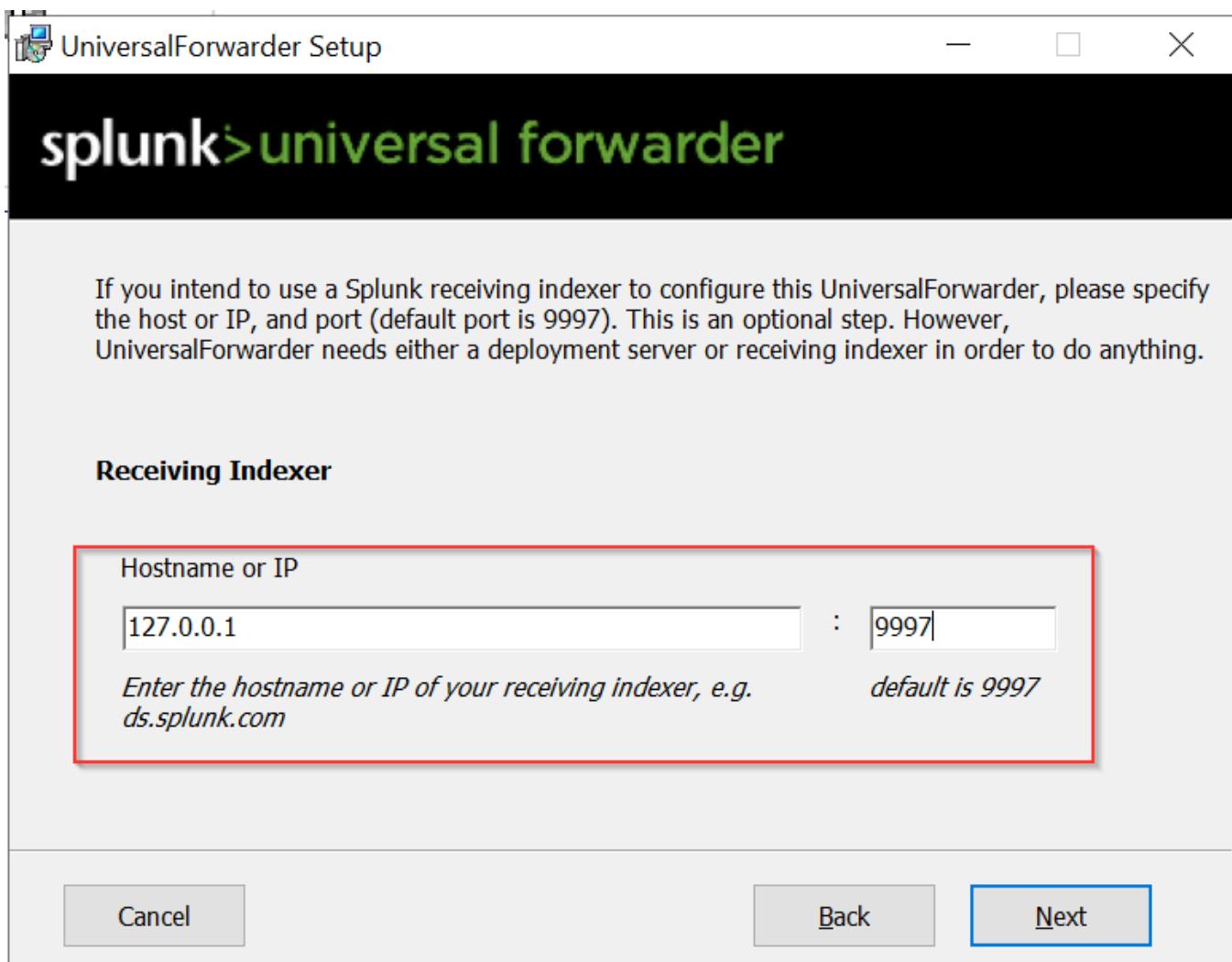
Setting up Deployment Server

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.



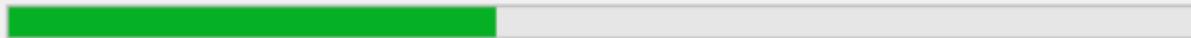
UniversalForwarder Setup



splunk>universal forwarder

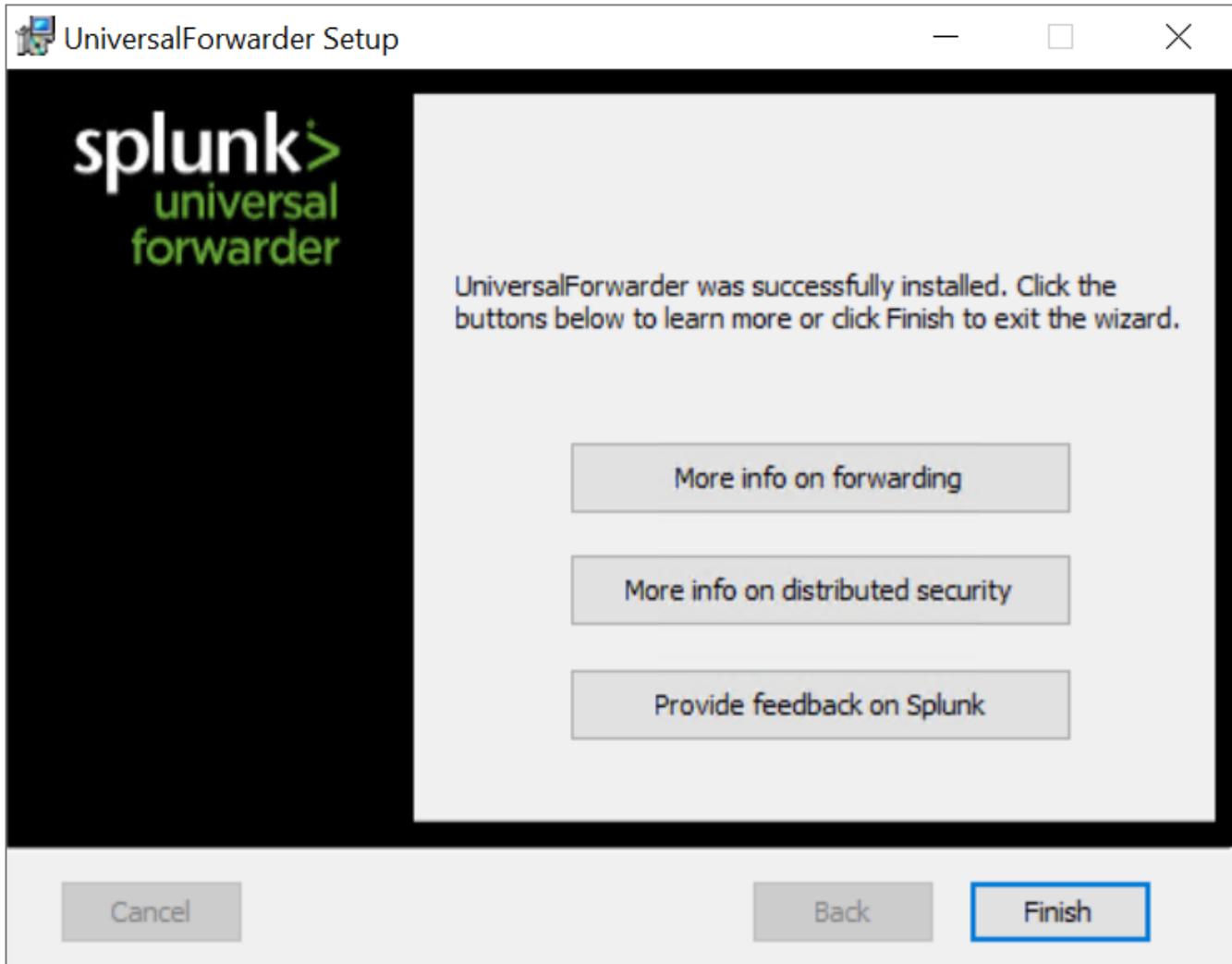
Please wait while the Setup Wizard installs UniversalForwarder.

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:

A screenshot of the Splunk Forwarder Management dashboard. It shows summary statistics: 1 Client phoned home in the last 24 hours, 0 Clients with deployment errors, and 0 Total downloads in the last 1 hour. Below this, there's a table titled "Clients (1)". The table has columns: Host Name, Client Name, Instance Name, IP Address, Actions, Machine Type, Deployed Apps, and Phone Home. A single row is listed: coffelylab, 55A41596-684C-472D-BF5D-95ED84F37D7C, coffelylab, 127.0.0.1, Delete Record, windows-x64, 0 deployed, and a few seconds ago. The "Phone Home" column for this row is highlighted with a red border.

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?

✓ Correct Answer

What is the default port on which Splunk configures the forwarder?

✓ Correct Answer

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.

The screenshot shows the Splunk web interface with the following navigation bar:

- Administrator
- Messages
- Settings (highlighted with a red box)
- Activity
- Help
- Find

The main content area is divided into several 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; Source types; Ingest actions.
- DISTRIBUTED ENVIRONMENT**: Indexer clustering; **Forwarder management** (highlighted with a red box).
- SYSTEM**: Server settings; Server controls; Health report manager; Instrumentation; Licensing; Workload management.
- USERS AND AUTHENTICATION**: Roles; Users; Tokens; Password Management; Authentication Methods.

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.

The Forwarder Management page displays the following information:

- Repository Location: \$SPLUNK_HOME/etc/deployment-apps
- Statistics:
 - 1 Client PHONED HOME IN THE LAST 24 HOURS
 - 0 Clients DEPLOYMENT ERRORS
 - 1 Total download IN THE LAST 1 HOUR
- Filtering options: Apps (1), Server Classes (1), Clients (1); Phone Home: All, All Clients; filter input field.
- Pagination: 1 Clients, 10 Per Page.
- Table of deployment hosts:

i	Host Name	Client Name	Instance Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
>	coffelylab	55A41596-684C-472D-BF5D-95ED84F37D7C	coffelylab	127.0.0.1	Delete Record	windows-x64	1 deployed	a few seconds ago

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.

The screenshot shows the Splunk web interface with the 'Settings' dropdown menu highlighted by a red box. To the left, there's a sidebar with a 'Monitoring Console' section containing a 'Monitoring' icon and a 'Console' link. A large blue box highlights the 'Add Data' section, which contains a database icon and a plus sign icon. An arrow points from the 'Add Data' section towards the 'Settings' dropdown. The main content area is organized into several 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; Source types; Ingest actions.
- DISTRIBUTED ENVIRONMENT**: Indexer clustering; Forwarder management; Federated search; Distributed search.
- SYSTEM**: Server settings; Server controls; Health report manager; Instrumentation; Licensing; Workload management.
- USERS AND AUTHENTICATION**: Roles; Users; Tokens; Password Management; Authentication Methods.

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.

The screenshot shows the 'Add Data' configuration page. It displays three options for data ingestion:

- Upload**: Represented by an upward arrow icon. Options: files from my computer (Local log files, Local structured files (e.g. CSV), Tutorial for adding data).
- Monitor**: Represented by a monitor icon showing a graph. Options: files and ports on this Splunk platform instance (Files - HTTP - WMI - TCP/UDP - Scripts, Modular inputs for external data sources).
- Forward**: Represented by a green icon showing a server with an arrow pointing right. This option is highlighted with a red box. Options: data from a Splunk forwarder (Files - TCP/UDP - Scripts).

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 Forwarders

Create or select a server class for data inputs. Use this page only in a single-instance Splunk environment.

To enable forwarding of data from deployment clients to this instance, set the output configurations on your forwarders. [Learn More](#)

Select Server Class

New Existing

Available host(s)	Selected host(s)
WINDOWS coffelylab	WINDOWS coffelylab

New Server Class Name

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.

Add Data

Select Forwarders Select Source Input Settings Review Done < Back **Next >**

Local Event Logs Collect event logs from this machine.

Files & Directories Upload a file, index a local file, or monitor an entire directory.

TCP / UDP Configure the Splunk platform to listen on a network port.

Local Performance Monitoring Collect performance data from this machine.

Scripts Get data from any API, service, or database with a script.

Splunk Assist Instance Identifier Assigns a random identifier to each Beam node

Powershell v3 Modular Input Execute PowerShell scripts v3 with parameters as inputs.

Configure selected Splunk Universal Forwarders to monitor local Windows event log channels, which contain log data published by installed applications, services, and system processes. The event log monitor runs once for every event log input defined in the Splunk platform. [Learn More](#)

Select Event Logs

Available item(s)	Selected item
Application	
ForwardedEvents	
Security	
Setup	
System	

Select the Windows Event Logs you want to index from the list.

FAQ

What event logs does this Splunk platform instance have access to?

What is the best method for monitoring event logs of remote Windows machines?

Creating Index

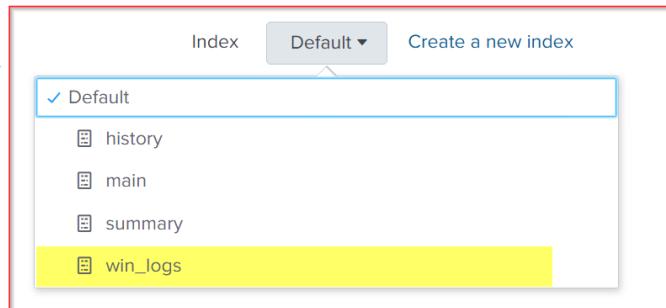
Create an index that will store the incoming Event logs. Once created, select the Index from the list and move to the next step.

Input Settings

Optionally set additional input parameters for this data input as follows:

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

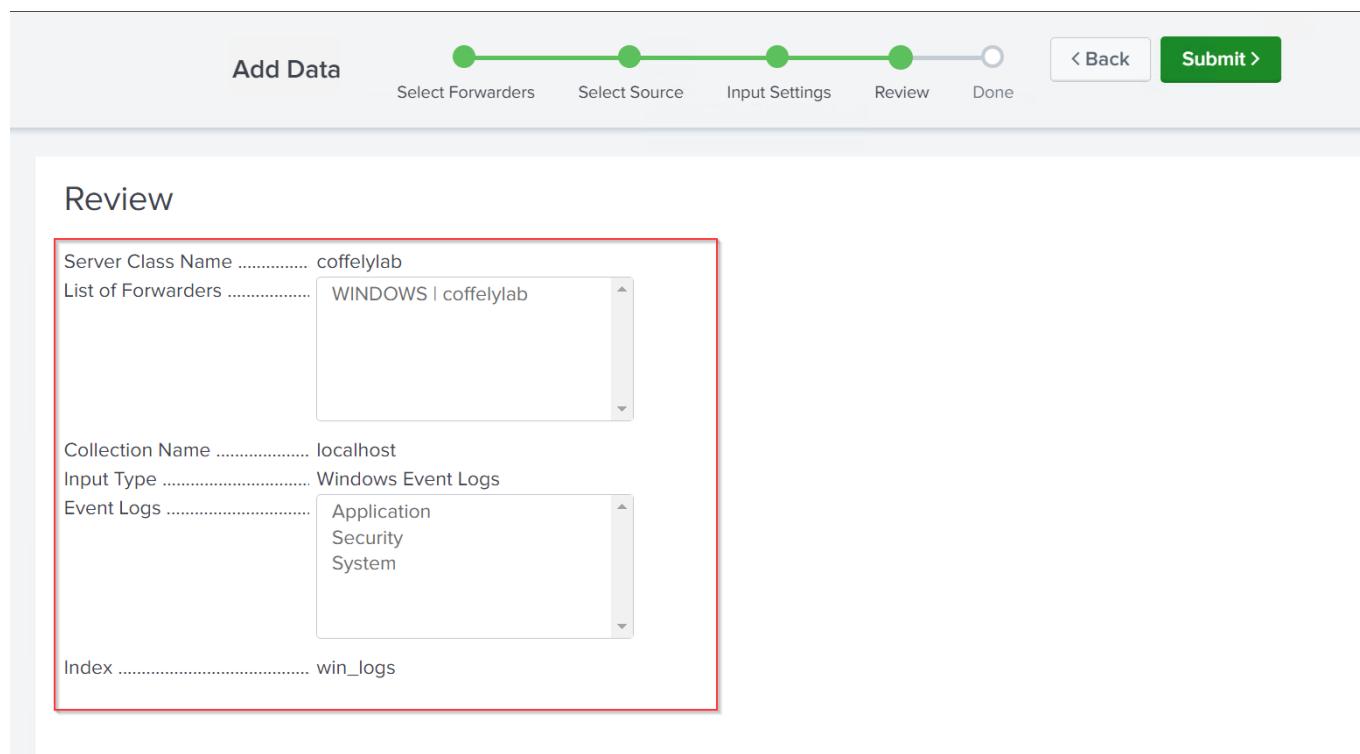


FAQ

- › How do indexes work?
- › How do I know when to create or use multiple indexes?

Review

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



Add Data

Select Forwarders Select Source Input Settings Review Done

< Back Submit >

Review

Server Class Name	coffelylab
List of Forwarders	WINDOWS coffelylab
Collection Name	localhost
Input Type	Windows Event Logs
Event Logs	Application Security System
Index	win_logs

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.

New Search

source="WinEventLog:/*" index="win_logs"

✓ 12,783 events (before 09/05/2023 23:09:44.000) No Event Sampling ▾

Events (12,783) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection × Deselect

1 month per column

sourcetype

3 Values, 100% of events Selected Yes No

Reports Top values Top values by time Rare values

Events with this field

Values	Count	%
WinEventLog:Security	7,098	68.45%
WinEventLog:System	2,598	25.05%
WinEventLog:Application	673	6.49%

ComputerName=coffelylab
Show all 12 lines
host = COFFELYLAB source = WinEventLog:System sourcetype = WinEventLog:System

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.

Answer the questions below

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

5

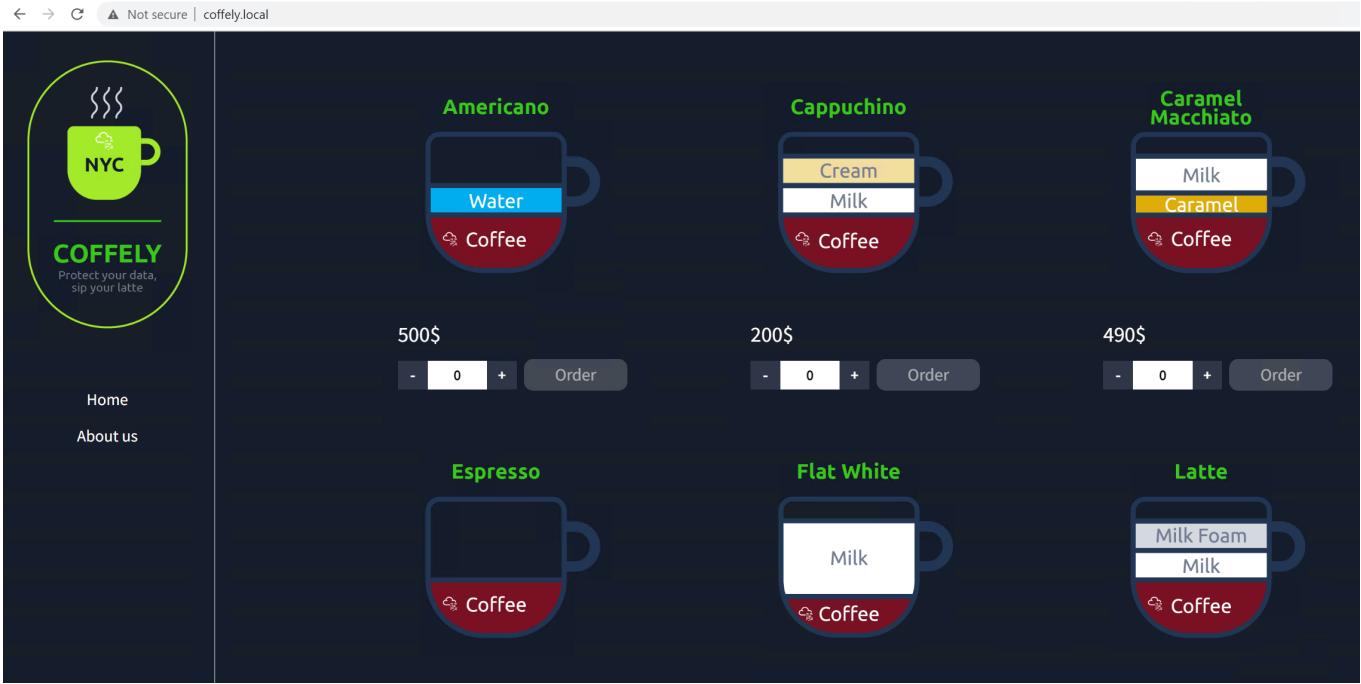
✓ Correct Answer

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

An account was successfully logged on.

✓ Correct Answer

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:

The screenshot shows the Splunk web interface with the 'Administrator' role selected. A red arrow points from the 'Add Data' button in the left sidebar to the 'Forwarding and receiving' option under the 'DATA' category in the main menu.

Left Sidebar:

- Add Data
- Monitoring Console

Main Menu Categories:

- 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
 - Source types
 - Ingest actions
- DISTRIBUTED ENVIRONMENT**
 - Indexer clustering
 - Forwarder management
 - Federated search
 - Distributed search
- SYSTEM**
 - Server settings
 - Server controls
 - Health report manager
 - Instrumentation
 - Licensing
 - Workload management
- USERS AND AUTHENTICATION**
 - Roles
 - Users
 - Tokens
 - Password Management
 - Authentication Methods

Select the Forwarder option:

The screenshot shows the 'Add Data' screen with three options:

- Upload**: Adds files from my computer. Sub-options include Local log files, Local structured files (e.g. CSV), and a Tutorial for adding data.
- Monitor**: Monitors files and ports on this Splunk platform instance. Sub-options include Files - HTTP - WMI - TCP/UDP - Scripts and Modular inputs for external data sources.
- Forward**: Adds data from a Splunk forwarder. Sub-options include Files - TCP/UDP - Scripts.

A red box highlights the 'Forward' option.

Select Forwarder

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

Select Forwarders

Create or select a server class for data inputs. Use this page only in a single-instance Splunk environment.

To enable forwarding of data from deployment clients to this instance, set the output configurations on your forwarders. [Learn More](#)

Select Server Class

New Existing

Available host(s)	Selected host(s)
WINDOWS coffelylab	WINDOWS coffelylab

New Server Class Name: web_logs

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.

Local Event Logs
Collect event logs from this machine.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Local Performance Monitoring
Collect performance data from this machine.

Scripts
Get data from any API, service, or database with a script.

Splunk Assist Instance Identifier
Assigns a random identifier to each Beam node

Powershell v3 Modular Input

Configure selected Splunk Universal Forwarders to monitor both existing and new data within a file or directory. If you choose to monitor a directory, you can only assign a single source type to the data within that directory. If a directory contains different log files from various applications or sources, configure individual file monitor inputs for each type of log file (you will have an opportunity to set individual source types this way). If the specified directory contains subdirectories, the Splunk platform recursively examines them for new files. [Learn More](#)

File or Directory ? `C:\inetpub\logs\LogFiles\W3SVC2`

Includelist ? optional

Excludelist ? optional

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.

Input Settings

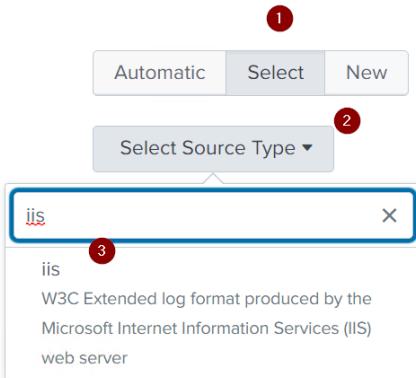
Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)



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

Review

Server Class Name	web_logs
List of Forwarders	WINDOWS coffelylab
Input Type	File Monitor
Source Path	C:\inetpub\logs\LogFiles\W3SVC2
Includelist	N/A
Excludelist	N/A
Source Type	iis
Index	win_logs

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:

The screenshot shows the Splunk interface with a search bar at the top containing the query `index="web_logs" sourcetype="iis"`. Below the search bar, it says `✓ 27 events (before 10/05/2023 00:58:57.000)` and `No Event Sampling`. There are tabs for `Events (27)`, `Patterns`, `Statistics`, and `Visualization`. The `Events (27)` tab is selected. Below the tabs are buttons for `Format Timeline`, `- Zoom Out`, `+ Zoom to Selection`, and `x Deselect`. To the right, it says `1 minute per column`. The main area displays a table of events with columns `i`, `Time`, and `Event`. The first few rows of the event list are:

i	Time	Event
>	10/05/2023 00:36:10.000	2023-05-10 00:36:10 127.0.0.1 GET /secret-flag.html - 80 - 127.0.0.1 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/113.0.0.0+Safari/537.36 - 304 0 0 4 host = COFFELYLAB source = C:\inetpub\logs\LogFiles\W3SVC2\u_ex230510.log sourcetype = iis
>	10/05/2023 00:35:53.000	2023-05-10 00:35:53 127.0.0.1 GET /secret-flag.html - 80 - 127.0.0.1 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/113.0.0.0+Safari/537.36 - 304 0 0 56 host = COFFELYLAB source = C:\inetpub\logs\LogFiles\W3SVC2\u_ex230510.log sourcetype = iis
>	10/05/2023 00:35:42.000	2023-05-10 00:35:42 127.0.0.1 GET /secret-flag.html - 80 - 127.0.0.1 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/113.0.0.0+Safari/537.36 - 200 0 0 68 host = COFFELYLAB source = C:\inetpub\logs\LogFiles\W3SVC2\u_ex230510.log sourcetype = iis
>	10/05/2023 00:35:13	2023-05-10 00:35:13 127.0.0.1 GET /favicon.ico - 80 - 127.0.0.1 Mozilla/5.0+(Windows+NT+10.0;+Win64;+x64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/113.0.0.0+Safari/537.36 - 200 0 0 68 host = COFFELYLAB source = C:\inetpub\logs\LogFiles\W3SVC2\u_ex230510.log sourcetype = iis

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.

{COffely_Is_Best_iN_TTown}

✓ Correct Answer