

# **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.

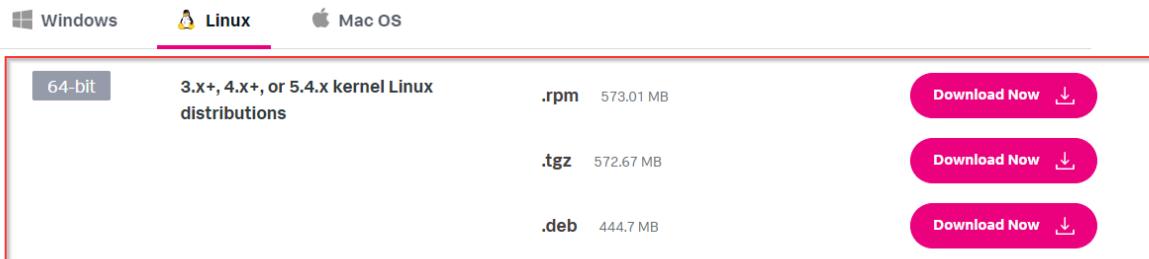
## **Learning Objectives**

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](http://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.

```
root@coffely:/home/ubuntu/Downloads/splunk
File Edit View Search Terminal Help
ubuntu@coffely:~$ cd Downloads/splunk
ubuntu@coffely:~/Downloads/splunk$ ls
splunk_installer.tgz  splunkforwarder.tgz
ubuntu@coffely:~/Downloads/splunk$ sudo su
root@coffely:/home/ubuntu/Downloads/splunk#
```

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.

```
root@coffely:/opt/splunk/bin# ./splunk start --accept-license
This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you can't log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

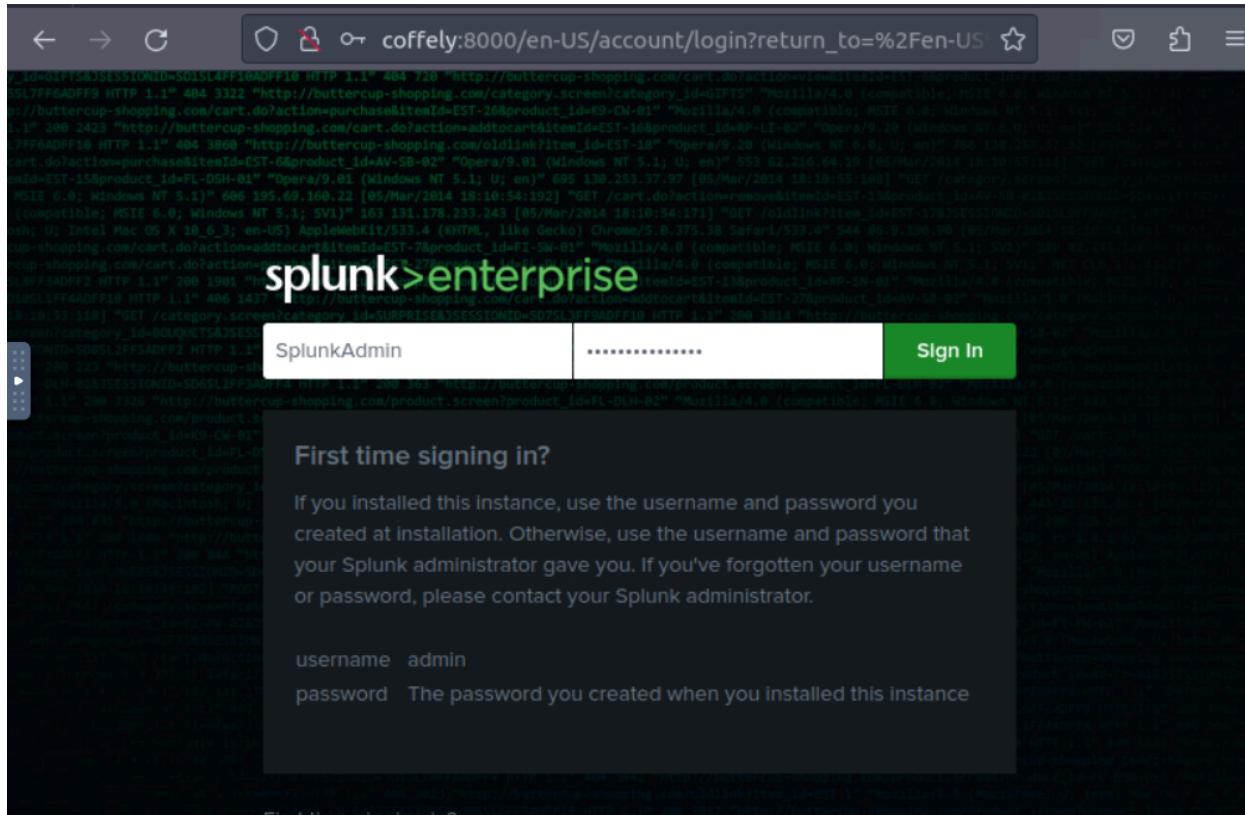
Please enter an administrator username: SplunkAdmin
Password must contain at least:
 * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Copying '/opt/splunk/etc/openldap/ldap.conf.default' to '/opt/splunk/etc/openldap/ldap.conf'.
Generating RSA private key, 2048 bit long modulus
.....+++++
e is 65537 (0x10001)
writing RSA key

Generating RSA private key, 2048 bit long modulus
...+++++
...+++++
e is 65537 (0x10001)
writing RSA key
```

## 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 _metrics_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/splunk/etc/apps/splunk_instrumentation/default/savedsearches.conf, line 451: | append [| rest /services/configs/conf-pythonSslClientConfig | eval sslVerifyServerCert (value: if(isnull($sslVerifyServerCert),"unset",$sslVerifyServerCert), splunk_server=sha256(splunk_server) | stats values(eai:acl.app) as python_configuredApp values($sslVerifyServerCert) as python_sslVerifyServerCert by splunk_server | eval python_configuredSystem=if(python_configuredApp="system","true","false") | fields python_sslVerifyServerCert, splunk_server, python_configuredSystem]
| append [| rest /services/configs/conf-web/settings | eval mgmtHostPort=if(isnull($mgmtHostPort),"unset",$mgmtHostPort), splunk_server=sha256(splunk_server) | stats values(eai:acl.app) as fwdrMgmtHostPort configuredApp values($mgmtHostPort) as fwdr_mgmtHostPort by splunk_server]

splunkd is running (PID: 5412).
splunk helpers are running (PIDs: 5413 5565 5615 5626 5643 5696 6028).
```

## 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 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.

```
root@coffely:/opt/splunk/bin# ./splunk help
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[sslConfig]/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 parameter, 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:

## 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 Splunk Universal Forwarder download page. At the top, there are tabs for Windows, Linux, Mac OS, FreeBSD, Solaris, and AIX. Below these, two sections are shown: one for 32-bit Windows 10 (.msi, 64.31 MB) and one for 64-bit Windows 10/11 and Server 2012-2022 (.msi, 77.38 MB). Each section has a 'Download Now' button with a downward arrow icon.

Architecture	Operating System	File Type	Size	Action
32-bit	Windows 10	.msi	64.31 MB	Download Now
64-bit	Windows 10, Windows 11 Windows Server 2012, 2012 R2, 2016, 2019, 2022	.msi	77.38 MB	Download Now

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:

```
root@coffely:/opt/clear# ./bin/splunk start --accept-license
This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you can't log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: forwarderadmin
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.
Failed to create the unit file. Please do it manually later.

Splunk> Needle. Haystack. Found.

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
        Creating: /opt/clear/var/run/splunk/appserver/i18n
        Creating: /opt/clear/var/run/splunk/appserver/modules/static/css
        Creating: /opt/clear/var/run/splunk/upload
        Creating: /opt/clear/var/run/splunk/search_telemetry
```

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:

The screenshot shows the Splunk navigation bar with 'Administrator' selected. Below it, the 'Settings' dropdown is open, revealing a list of configuration categories. A red arrow points from the text above to the 'Forwarding and receiving' link, which is highlighted with a yellow background.

- Administrator
- Messages
- Settings
- Activity
- Help
- Find

- Explore Data
- Add Data
- Explore Data
- Monitoring Console

- KNOWLEDGE
- Searches, reports, and alerts
- Data models
- Event types
- Tags
- Fields
- Lookups
- User interface
- Alert actions
- Advanced search
- All configurations
- SYSTEM
- Server settings
- Server controls
- Health report manager
- RapidDiag
- Instrumentation
- Licensing
- Workload management
- DATA
- Data inputs
- Forwarding and receiving**
- Indexes
- Report acceleration summaries
- Virtual indexes
- Source types
- Ingest actions
- DISTRIBUTED ENVIRONMENT
- Indexer clustering
- Forwarder management
- Federated search
- Distributed search
- 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' configuration page. It has two main sections: 'Forward data' and 'Receive data'. The 'Receive data' section is currently active, as indicated by a red circle with the number '1' next to the 'Configure receiving' button. A red arrow points from this button to the right. In the top right corner of the 'Receive data' section, there is a green button labeled 'New Receiving Port' with a red circle containing the number '2' above it. Another red arrow points from this button towards the first red arrow.

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:

**Configure receiving**

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

Listen on this port \*  9997

For example, 9997 will receive data on TCP port 9997.

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.

**Receive data** [New Receiving Port](#)

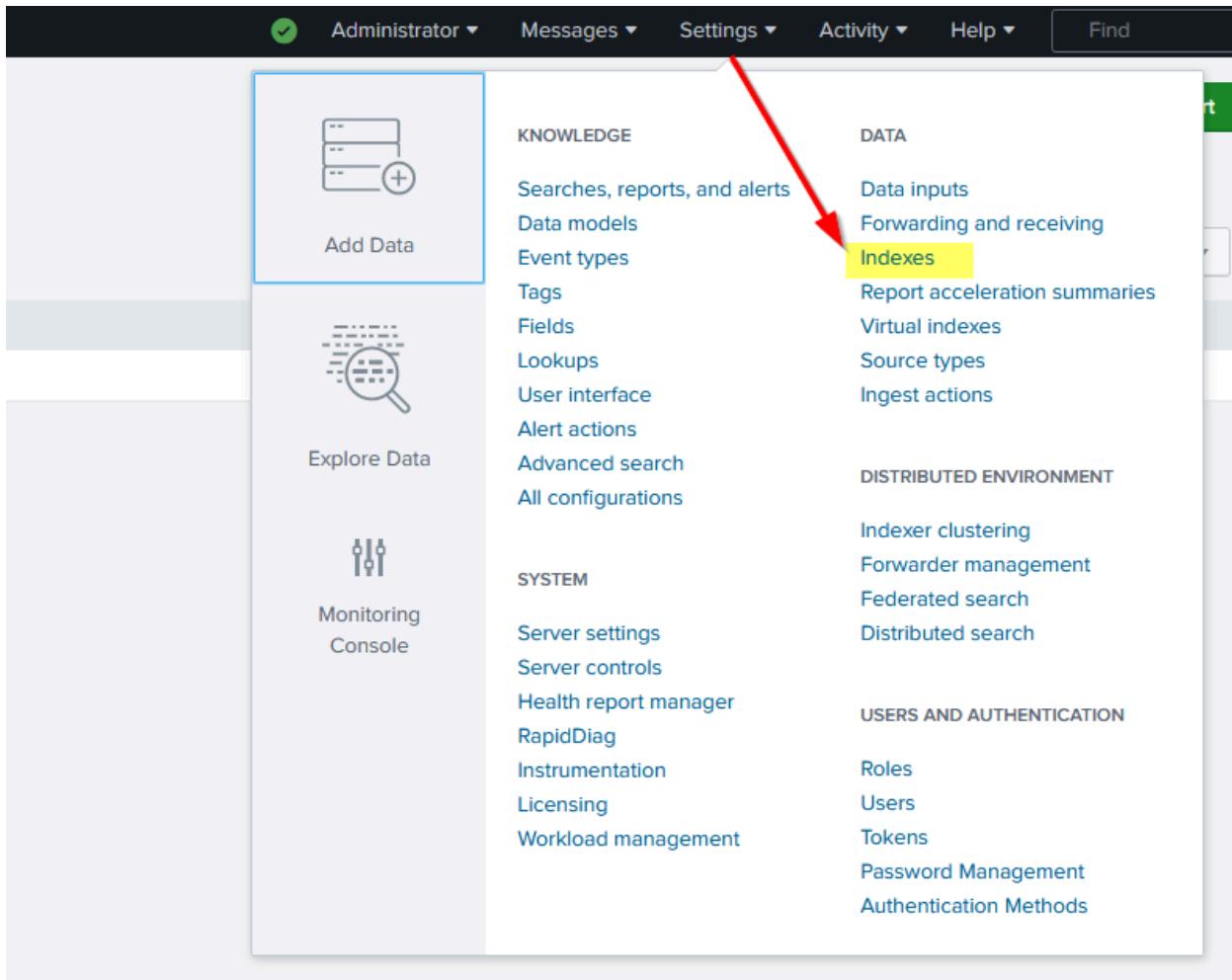
[Forwarding and receiving](#) > [Receive data](#)

**Successfully saved "9997".**

Showing 1-1 of 1 item		
filter	Actions	25 per page ▾
Listen on this port ▾	Status ▾	
9997	Enabled   Disable	<a href="#">Delete</a>

## 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

The screenshot shows the 'Indexes' table page. At the top, it says 'Indexes' and 'A repository for data in Splunk Enterprise. Indexes reside in flat files on the Splunk Enterprise instance known as the indexer. Learn more' with a 'Learn more' link. Below that is a search bar with 'filter' and a magnifying glass icon, and a 'New Index' button with a red arrow pointing to it. The table 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.

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	158M	3 days ago	a few seconds ago	\$SPLUNK_DB/_internaldb/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	139M	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/_fishbucket/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	<input type="text" value="Linux_host"/>
Index Data Type	<input checked="" type="radio"/> Events <input type="radio"/> Metrics
Home Path	optional
Cold Path	optional
Thawed Path	optional
Data Integrity Check	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Max Size of Entire Index	500 <input type="button" value="GB ▾"/>
Max Size of Hot/Warm/Cold Bucket	auto <input type="button" value="GB ▾"/>
<input style="background-color: green; color: white; border: 2px solid red; padding: 5px; width: 100px; height: 30px; margin-right: 10px;" 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

```
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.

```

doumitu@tryhackme:~/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
bttmp                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.

```

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
```

Splunk>enterprise Apps ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾

Search > Analytics Datasets Reports Alerts Dashboards

New Search

index="linux\_host"

1,026 events (3/23/25 5:00:00.000 AM to 3/24/25 5:27:35.000 AM) No Event Sampling

Events (1,026) Patterns Statistics Visualization

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

Last 24 hours ▾

1 hour per column

Time	Event
3/24/25 5:26:36.000 AM	Mar 24 05:26:36 coffely ubuntu: coffely-has-the-best-coffee-in-town host = coffely : source = /var/log/syslog : sourcetype = syslog
3/24/25 5:17:01.000 AM	Mar 24 05:17:01 coffely CRON[3552]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly) host = coffely : source = /var/log/syslog : sourcetype = syslog
3/24/25 5:12:21.000 AM	Mar 24 05:12:21 coffely systemd[1]: Finished Daily apt upgrade and clean activities. 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?**

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

```
root@coffely:/opt/clear/bin# adduser analyst
Adding user `analyst' ...
Adding new group `analyst' (1001) ...
Adding new user `analyst' (1001) with group `analyst' ...
Creating home directory `/home/analyst' ...
Copying files from `/etc/skel' ...
New password:
  type new password:
  ssd: password updated successfully
  changing the user information for analyst
Enter the new value, or press ENTER for the default
      Full Name []:
      Room Number []:
      Work Phone []:
      Home Phone []:
      Other []:
Is the information correct? [Y/n]
```

```
> 3/24/25      Mar 24 05:34:01 coffely passwd[12438]: gkr-pam: couldn't update the login keyring password: no old password was entered
5:34:01.000 AM  host = coffely | source = /var/log/auth.log | sourcetype = auth-too_small

> 3/24/25      Mar 24 05:34:01 coffely passwd[12438]: pam_unix(passwd:chauthtok): password changed for analyst
5:34:01.000 AM  host = coffely | source = /var/log/auth.log | sourcetype = auth-too_small

> 3/24/25      Mar 24 05:33:55 coffely systemd-timesyncd[380]: Timed out waiting for reply from 185.125.190.58:123 (ntp.ubuntu.com).
5:33:55.000 AM  host = coffely | source = /var/log/syslog | sourcetype = syslog

> 3/24/25      Mar 24 05:33:53 coffely useradd[12425]: new user: name=analyst, UID=1001, GID=1001, home=/home/analyst, shell=/bin/bash, from=/dev/pts/0
5:33:53.000 AM  host = coffely | source = /var/log/auth.log | sourcetype = auth-too_small

> 3/24/25      Mar 24 05:33:53 coffely groupadd[12416]: new group: name=analyst, GID=1001
5:33:53.000 AM  host = coffely | source = /var/log/auth.log | sourcetype = auth-too_small

> 3/24/25      Mar 24 05:33:53 coffely groupadd[12416]: group added to /etc/gshadow: name=analyst
5:33:53.000 AM  host = coffely | source = /var/log/auth.log | sourcetype = auth-too_small

> 3/24/25      Mar 24 05:33:53 coffely groupadd[12416]: group added to /etc/group: name=analyst, GID=1001
5:33:53.000 AM  host = coffely | source = /var/log/auth.log | sourcetype = auth-too_small
```

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

Answer: /etc/group

```
> 3/24/25      Mar 24 05:33:53 coffely groupadd[12416]: group added to /etc/group: name=analyst, GID=1001
5:33:53.000 AM  host = coffely | source = /var/log/auth.log | sourcetype = auth-too_small
```

## 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.

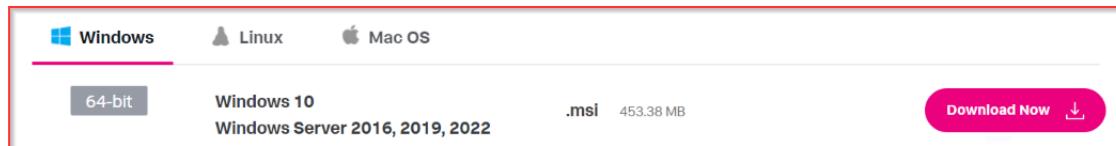
## Downloading Splunk Enterprise

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

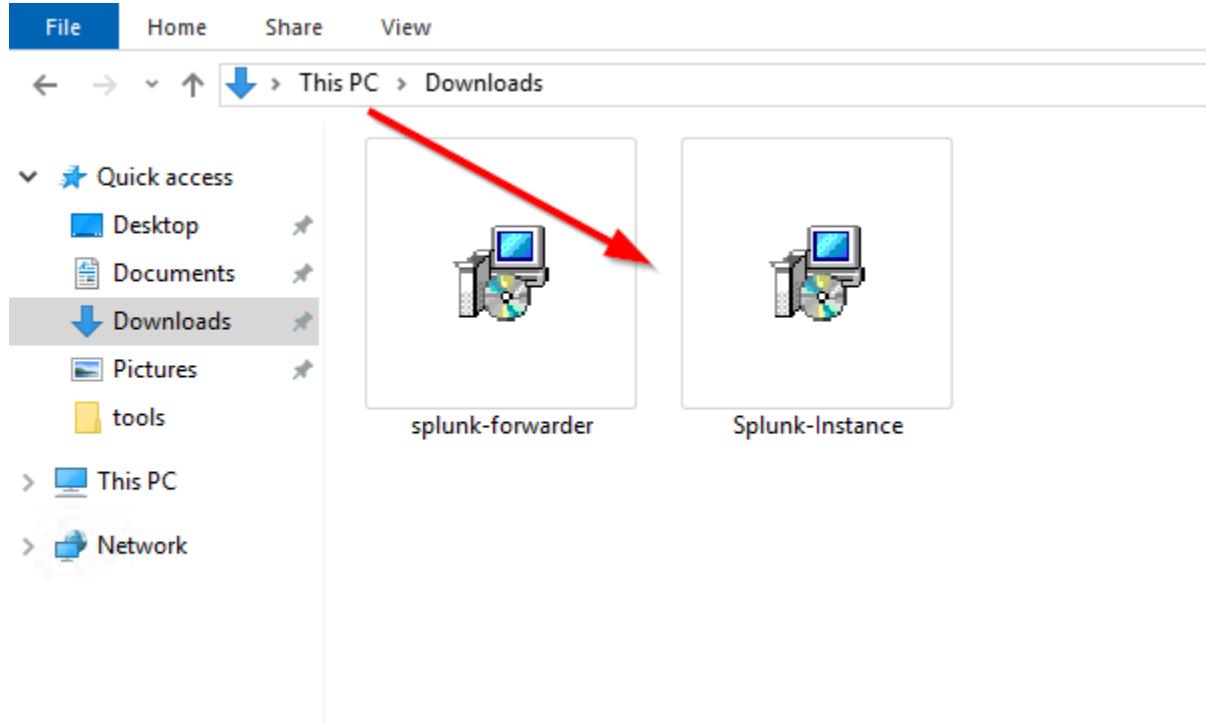
### Splunk Enterprise 9.0.4

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

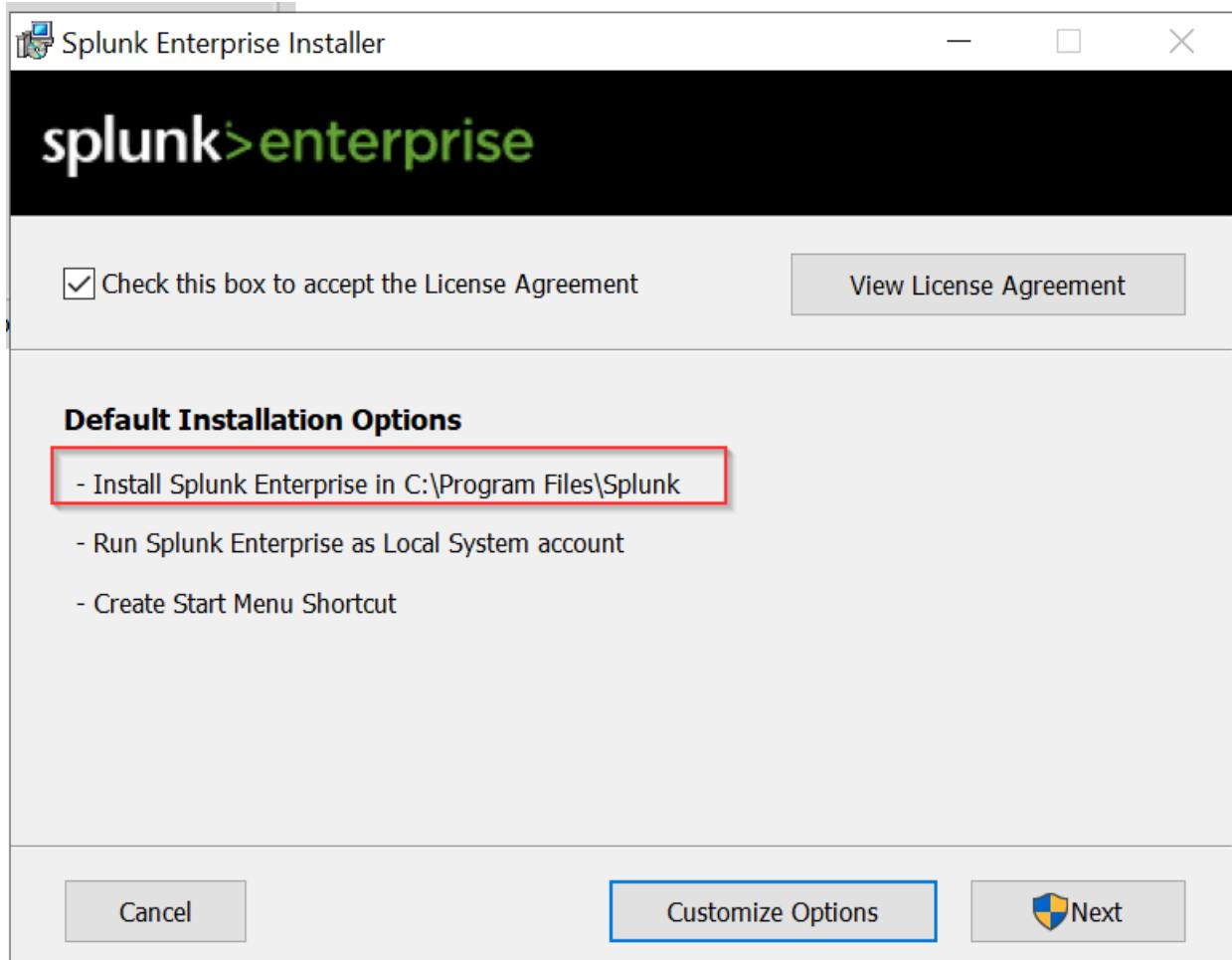


The installer Splunk-Instance is already been downloaded and placed in the Downloads folder to speed up the process.



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 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.



Splunk Enterprise Setup

— □ ×

## splunk>enterprise

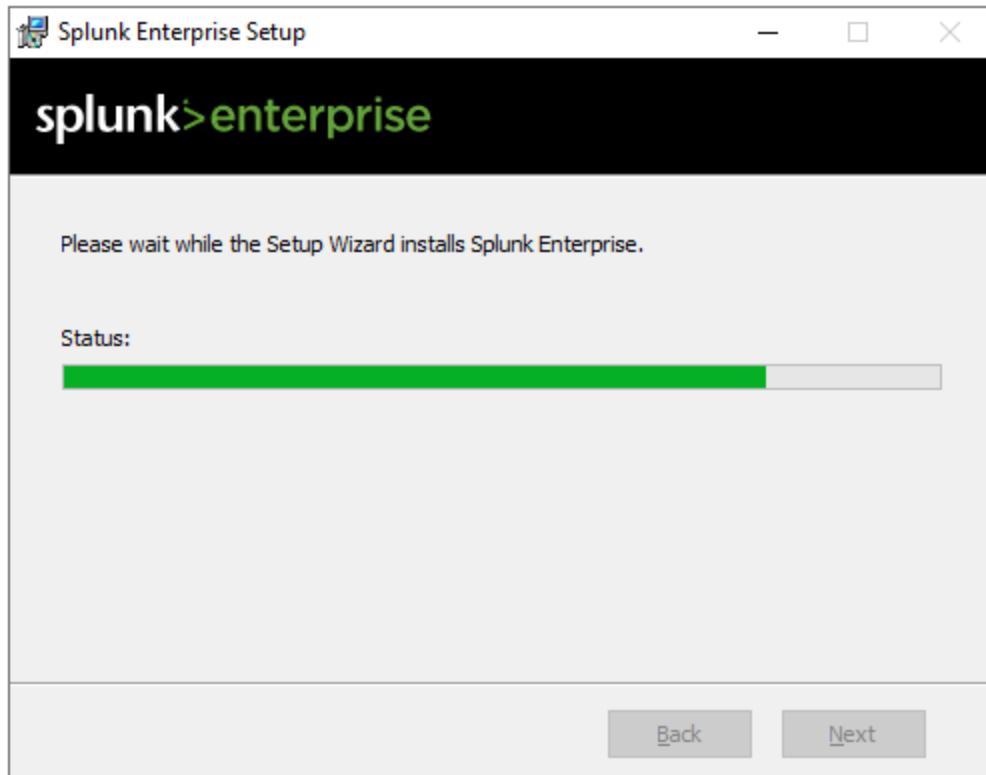
Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

Username:

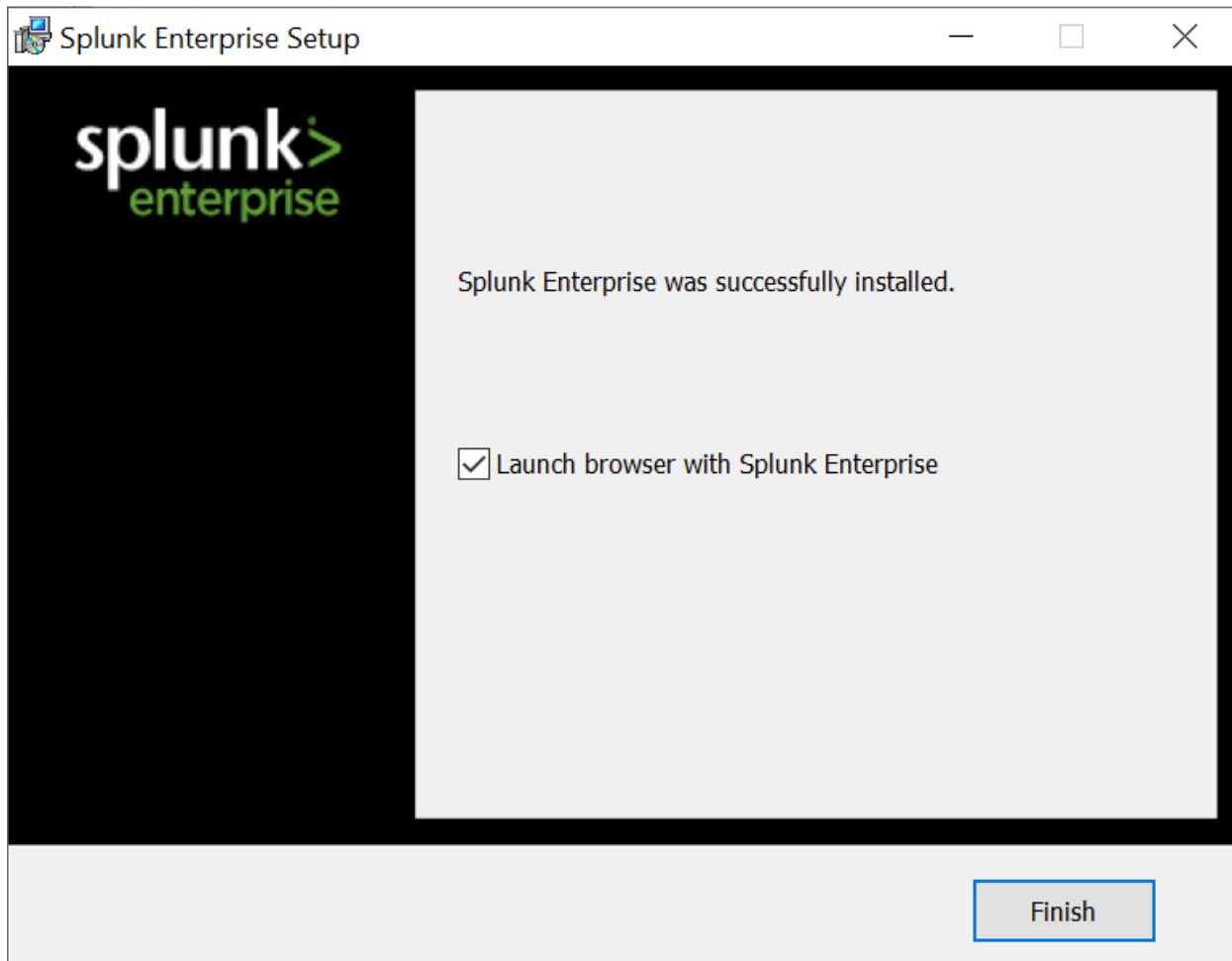
Password:

Confirm password:

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



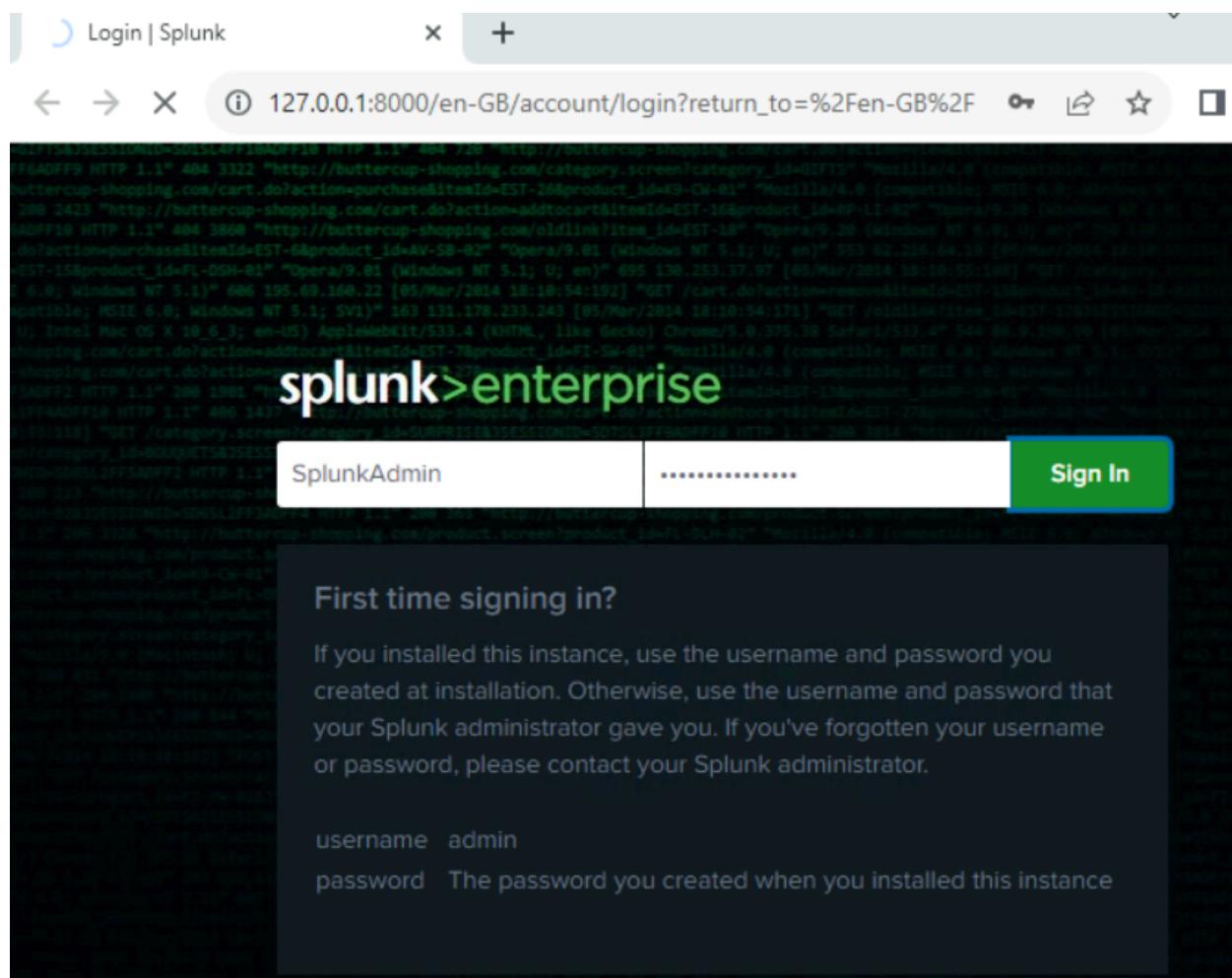
We will get the following message if all system requirements are met, and installation is complete.



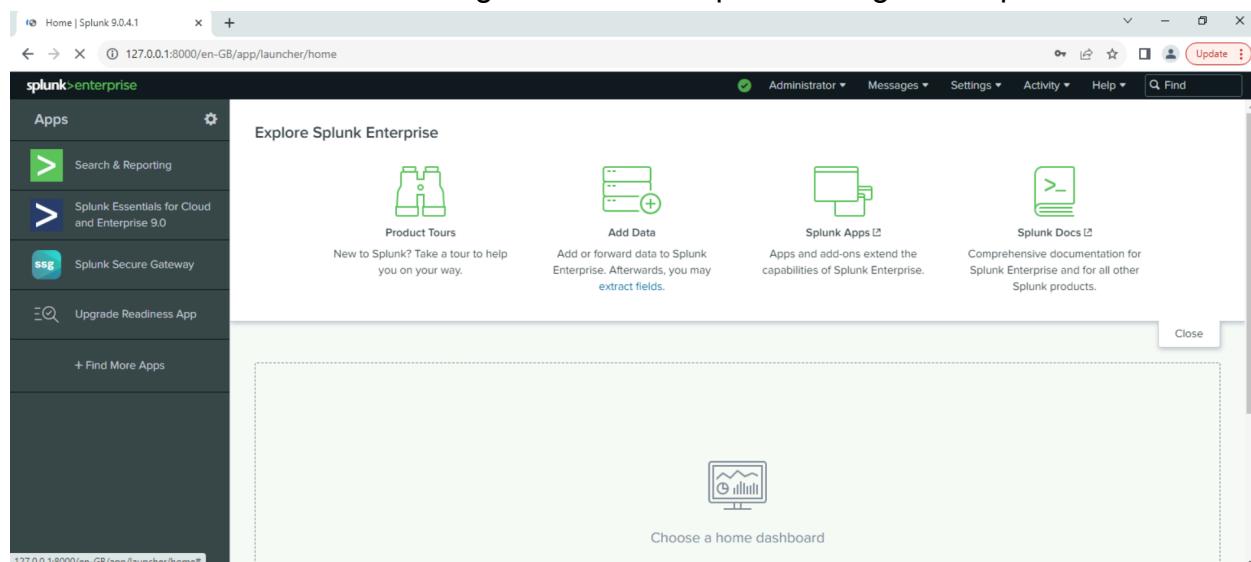
## Accessing Splunk Instance

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://10.10.100.188:8000



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?**

The screenshot shows the 'Add Data' interface. At the top, a question asks: 'What data do you want to send to the Splunk platform?'. Below this, there are three main options: 'Upload', 'Monitor', and 'Forward'. Each option has a corresponding icon and a brief description.

- Upload**: files from my computer. Icons: a green arrow pointing up. Sub-options: Local log files, Local structured files (e.g. CSV). Tutorial link: [Tutorial for adding data](#).
- Monitor**: files and ports on this Splunk platform instance. Icons: a monitor displaying a line graph. Sub-options: Files - HTTP - WMI - TCP/UDP - Scripts, Modular inputs for external data sources.
- Forward**: data from a Splunk forwarder. Icons: a green arrow pointing right. Sub-options: Files - TCP/UDP - Scripts.

Answer: **3**

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

The screenshot shows the 'Add Data' interface at the 'Select Source' step. The 'Monitor' option is selected. On the left, a list of monitoring sources is shown. On the right, a note says '← Select an option'.

- Local Event Logs**: Collect event logs from this machine.
- Remote Event Logs**: Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.
- Files & Directories**: Upload a file, index a local file, or monitor an entire directory.
- HTTP Event Collector**: Configure tokens that clients can use to send data over HTTP or HTTPS.
- TCP / UDP**: Configure the Splunk platform to listen on a network port.
- Local Performance Monitoring**: Collect performance data from this machine.
- Remote Performance Monitoring**: Collect performance and event information from remote hosts. Requires domain credentials.

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:

The screenshot shows the Splunk web interface with the 'Settings' dropdown menu open. The 'Forwarding and receiving' option is highlighted with a red box and an arrow pointing to it from the text above. The menu also lists other settings like 'Data inputs', 'Indexes', and 'Report acceleration summaries'.

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.

The screenshot shows the Splunk Forwarding interface. The 'Forward data' section is visible at the top, with a sub-section for 'Forwarding defaults'. Below it is a 'Configure forwarding' button and a '+ Add new' button. The 'Receive data' section follows, with a sub-section for 'Configure receiving'. This 'Configure receiving' section is highlighted with a red border. Below it is a 'Save' button.

**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:

The screenshot shows a 'Configure receiving' dialog box. It asks to set up the instance to receive data from forwarder(s). A field labeled 'Listen on this port' contains the value '9997', which is highlighted with a red border. Below the field is a note: 'For example, 9997 will receive data on TCP port 9997.' At the bottom are 'Cancel' and 'Save' buttons.

Configure receiving

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

Listen on this port: 9997  
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.

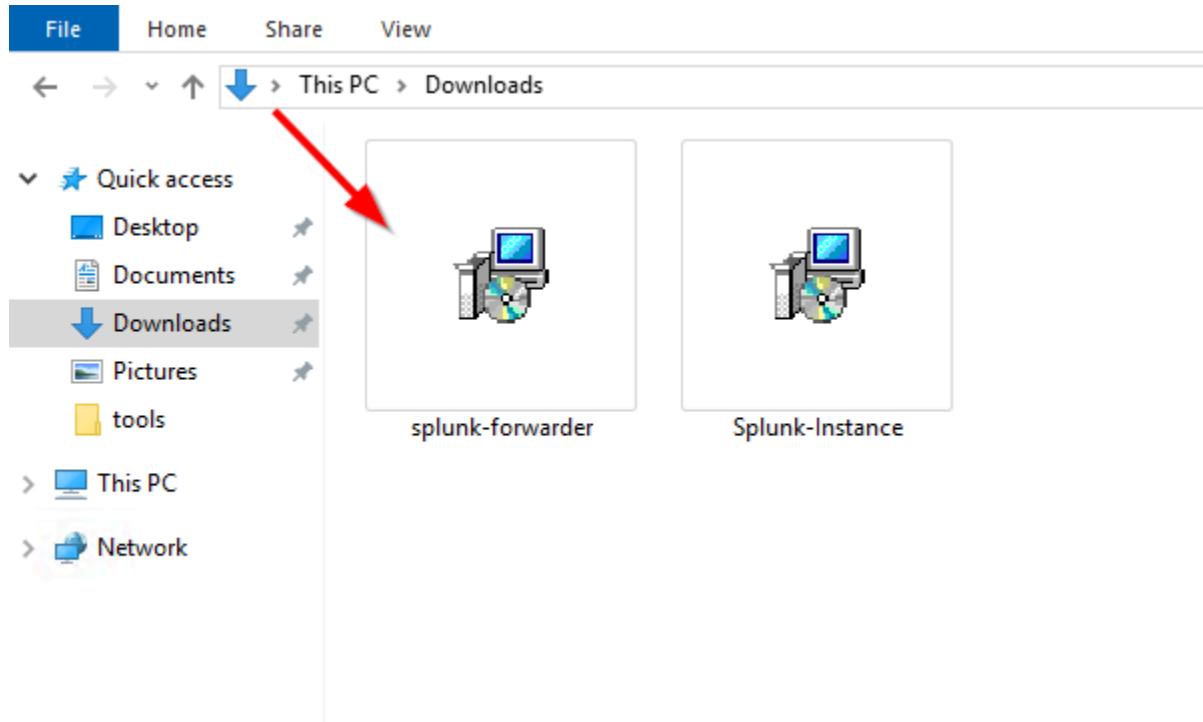
## Splunk Universal Forwarder 9.0.4

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

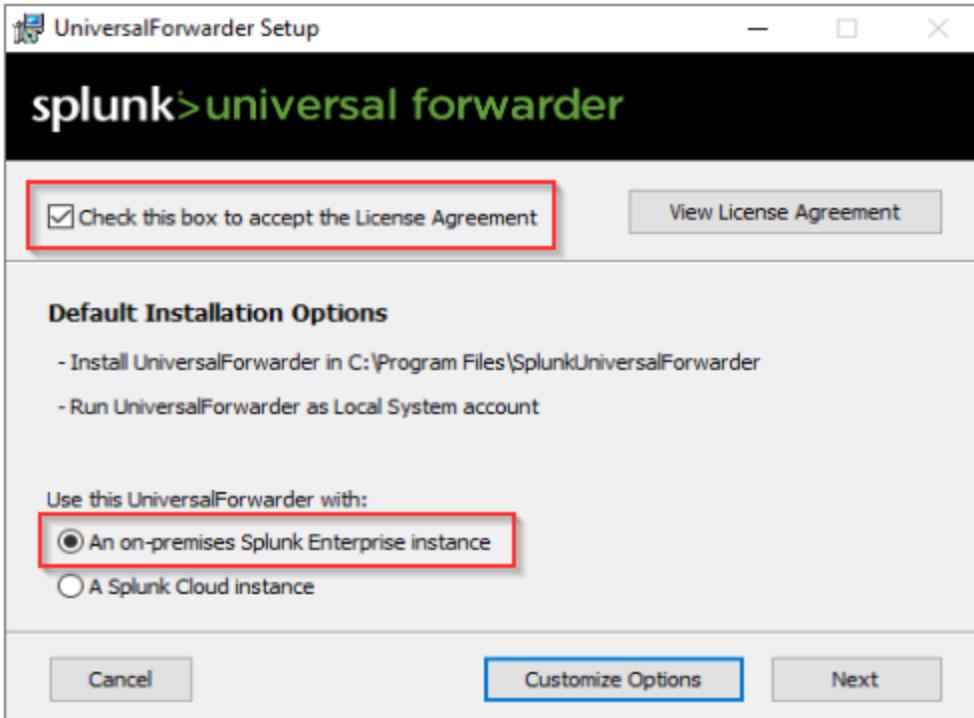
The screenshot shows the download page for Splunk Universal Forwarder 9.0.4. At the top, there are links for Windows, Linux, Mac OS, FreeBSD, Solaris, and AIX. Below these, two options are listed: '64-bit' (Windows 10, Windows 11, Windows Server 2012, 2012 R2, 2016, 2019, 2022) and '32-bit' (Windows 10). Each option includes a file size (.msi), download count (77.41 MB and 64.34 MB respectively), and a 'Download Now' button with a download 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.

## splunk>universal forwarder

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

Username:

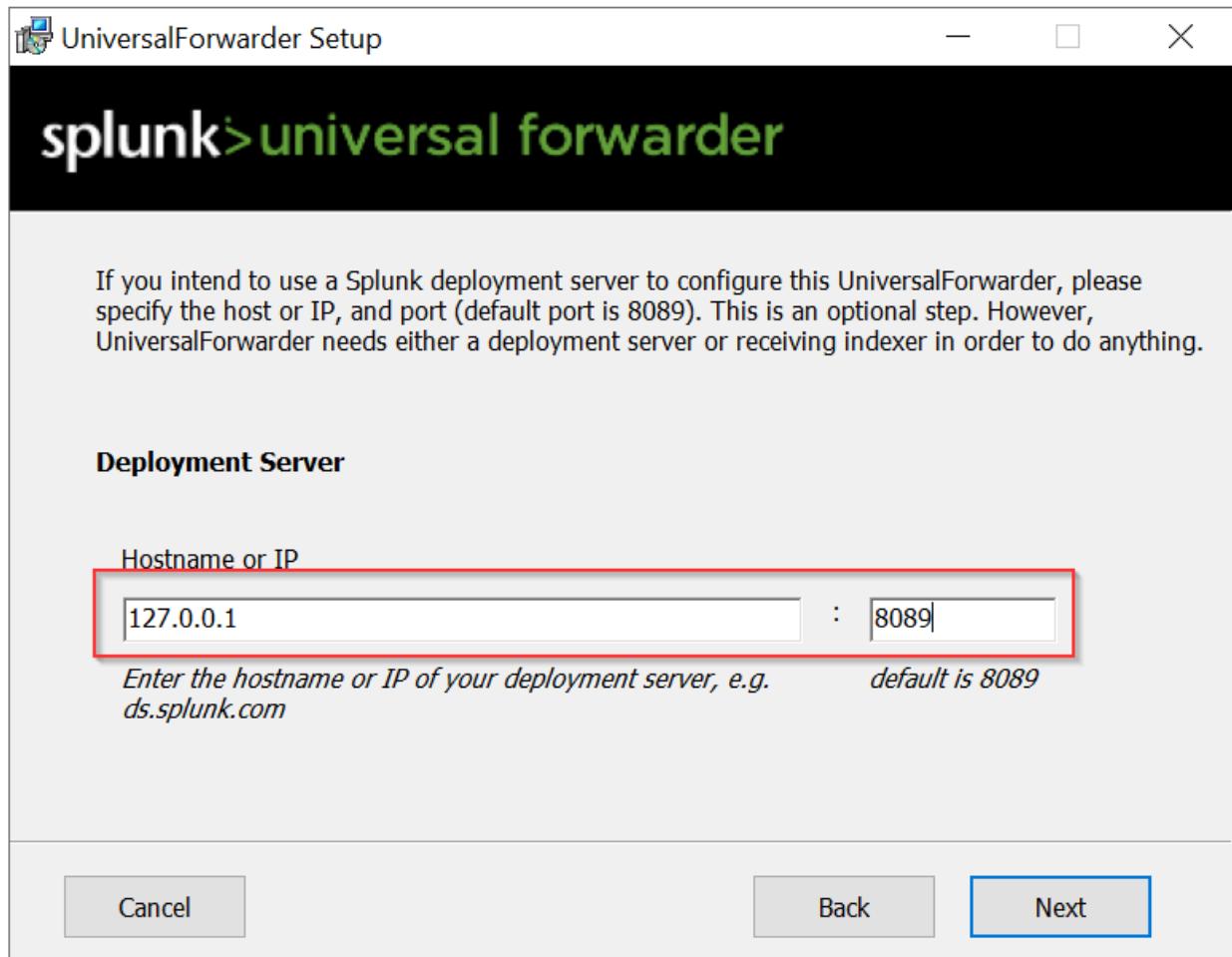
Generate random password

Password:

Confirm password:

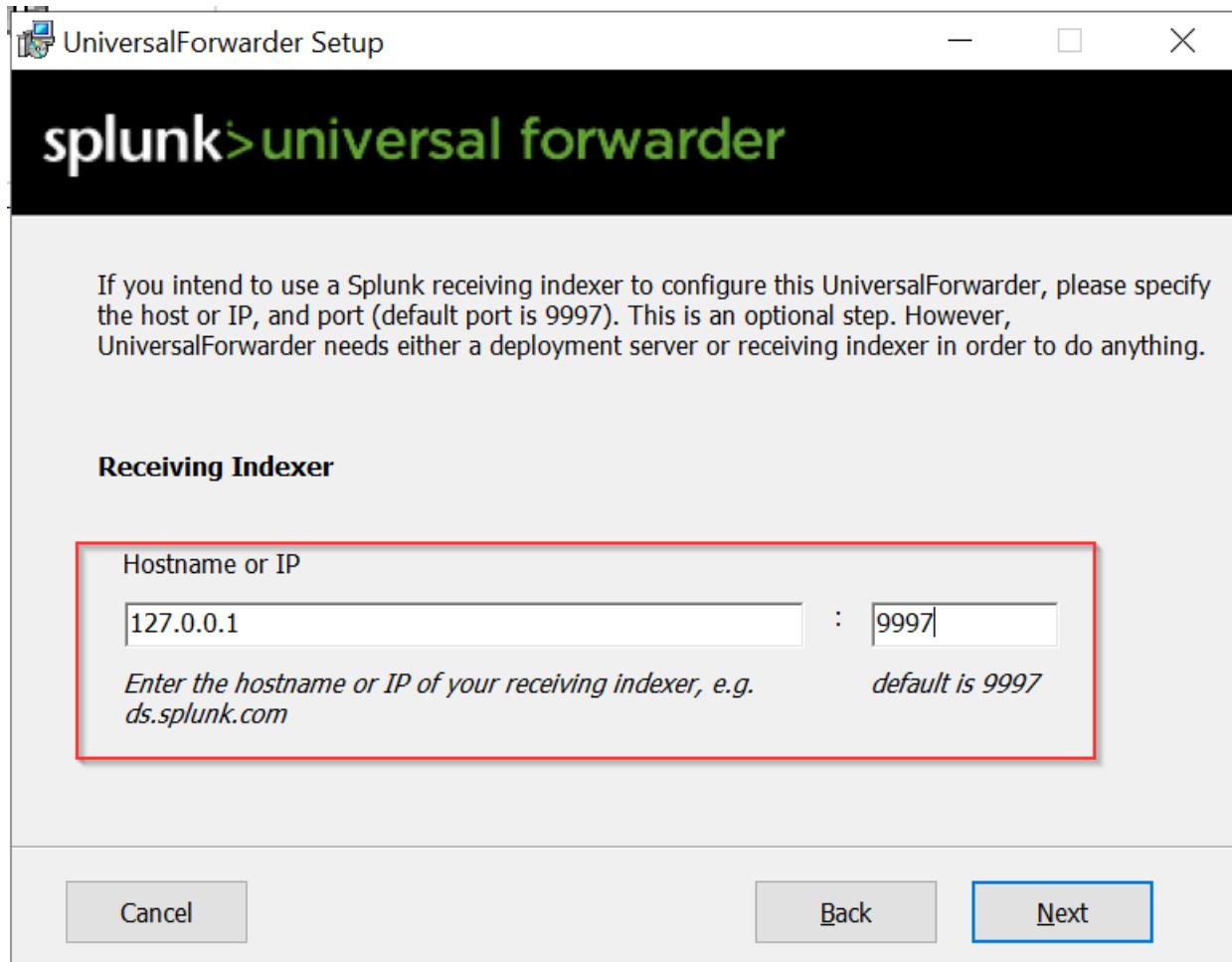
### Setting up Deployment Server

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.



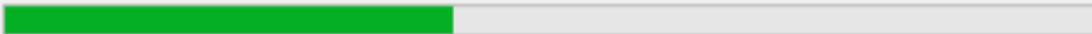
UniversalForwarder Setup



## splunk>universal forwarder

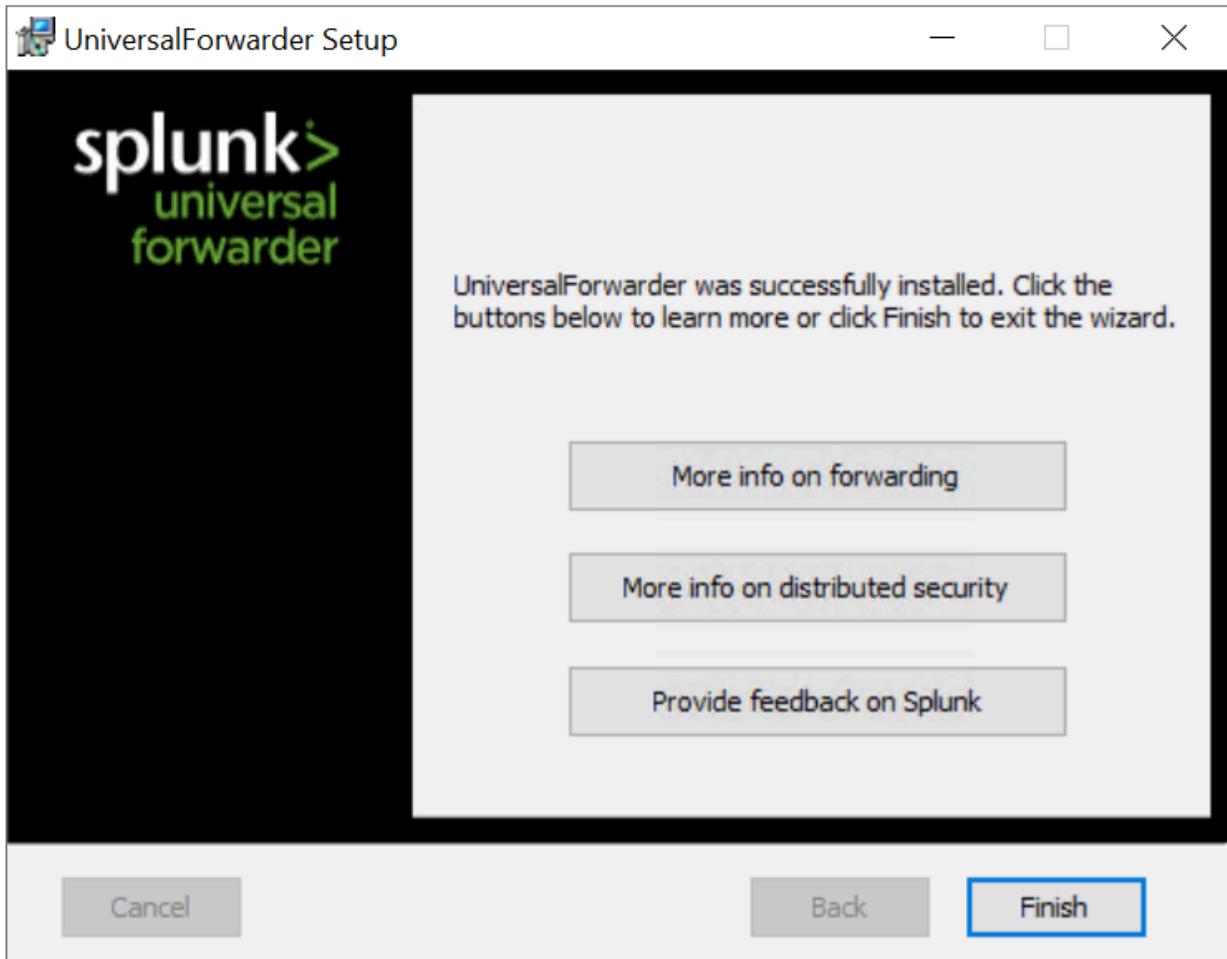
Please wait while the Setup Wizard installs UniversalForwarder.

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 interface. The top header says "Forwarder Management" and "Repository Location: \$SPLUNK\_HOME/etc/deployment-apps". It shows summary statistics: 1 Client (Phoned home in the last 24 hours), 0 Clients (Deployment Errors), and 0 Total downloads in the last 1 hour. Below this, there are tabs for "Apps (0)", "Server Classes (0)", and "Clients (1)". The "Clients" tab is selected. A sub-header says "Phone Home: All" and "All Clients". There is a "filter" input field. Below this, it says "1 Clients 10 Per Page". A table lists one client: coffeyleab (Host Name: 9E7C710A-DFF6-43DD-B447-AE4013779FD8, Client Name: 9E7C710A-DFF6-43DD-B447-AE4013779FD8, Instance Name: coffeyleab, IP Address: 127.0.0.1, Actions: Delete Record, Machine Type: windows-x64, Deployed Apps: 0 deployed, Phone Home: a few seconds ago).

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.

The screenshot shows the Splunk web interface with the 'Forwarder management' option highlighted. A red arrow points from the 'Forwarder management' link to the 'Settings' dropdown menu in the top navigation bar, indicating that this is the path to access the configuration page.

The interface includes a sidebar with 'Add Data' and 'Monitoring Console' options, and a main content area with sections for KNOWLEDGE, DATA, DISTRIBUTED ENVIRONMENT, SYSTEM, and USERS AND AUTHENTICATION. The 'Forwarder management' link is located under the 'DISTRIBUTED ENVIRONMENT' section.

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

KNOWLEDGE	DATA
Searches, reports, and alerts	Data inputs
Data models	Forwarding and receiving
Event types	Indexes
Tags	Report acceleration summaries
Fields	Source types
Lookups	Ingest actions
User interface	
Alert actions	
Advanced search	
All configurations	

DISTRIBUTED ENVIRONMENT
Indexer clustering
<b>Forwarder management</b> (highlighted with a red box)
Federated search
Distributed search

SYSTEM	USERS AND AUTHENTICATION
Server settings	Roles
Server controls	Users
Health report manager	Tokens
Instrumentation	Password Management
Licensing	Authentication Methods
Workload management	

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 screenshot shows the 'Forwarder Management' page. At the top, it displays deployment statistics: 1 Client phoned home in the last 24 hours, 0 Clients for deployment errors, and 1 Total download in the last 1 hour. Below this, there are tabs for 'Apps (1)', 'Server Classes (1)', and 'Clients (1)', with 'Clients (1)' being the active tab. A search bar allows filtering by phone home status ('All', 'All Clients', 'filter'). The main table lists one client: coffeyleab, with details: Host Name (55A41596-684C-472D-BF5D-95ED84F37D7C), Client Name (coffeyleab), Instance Name (coffeyleab), IP Address (127.0.0.1), Actions (Delete Record), Machine Type (windows-x64), Deployed Apps (1 deployed), and Phone Home (a few seconds ago). The entire table row for this client is highlighted with a red border.

i	Host Name	Client Name	Instance Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
>	coffeyleab	55A41596-684C-472D-BF5D-95ED84F37D7C	coffeyleab	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. At the top, there's a navigation bar with links for Administrator, Messages, Settings (which is highlighted with a red box), Activity, Help, and a search bar labeled 'Find'. On the left, there's a sidebar with icons for Monitoring and Console. 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; Federated search; Distributed search), SYSTEM (Server settings; Server controls; Health report manager; Instrumentation; Licensing; Workload management), and USERS AND AUTHENTICATION (Roles; Users; Tokens; Password Management; Authentication Methods). A red box highlights the 'Add Data' button in the sidebar, and a red arrow points from it to the 'Data inputs' link in the DATA section.

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 has three main options: 'Upload' (represented by an upward arrow icon), 'Monitor' (represented by a monitor icon with a graph), and 'Forward' (represented by a server icon with an arrow). Below each option are detailed descriptions and configuration links. The 'Forward' option is highlighted with a red box.

Option	Description	Configuration Links
Upload	Upload files from my computer	Local log files Local structured files (e.g. CSV) <a href="#">Tutorial for adding data</a>
Monitor	Monitor files and ports on this Splunk platform instance	Files - HTTP - WMI - TCP/UDP - Scripts Modular inputs for external data sources
Forward	Forward 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)	<a href="#">add all »</a>	Selected host(s)	<a href="#">« remove all</a>
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.

**Select Event Logs**

Available item(s)	<a href="#">add all »</a>	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

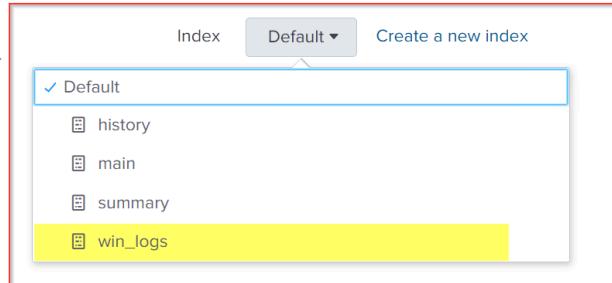
Create an index that will store the incoming Event logs. Once created, select the Index from the list and move to the next step.

## 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

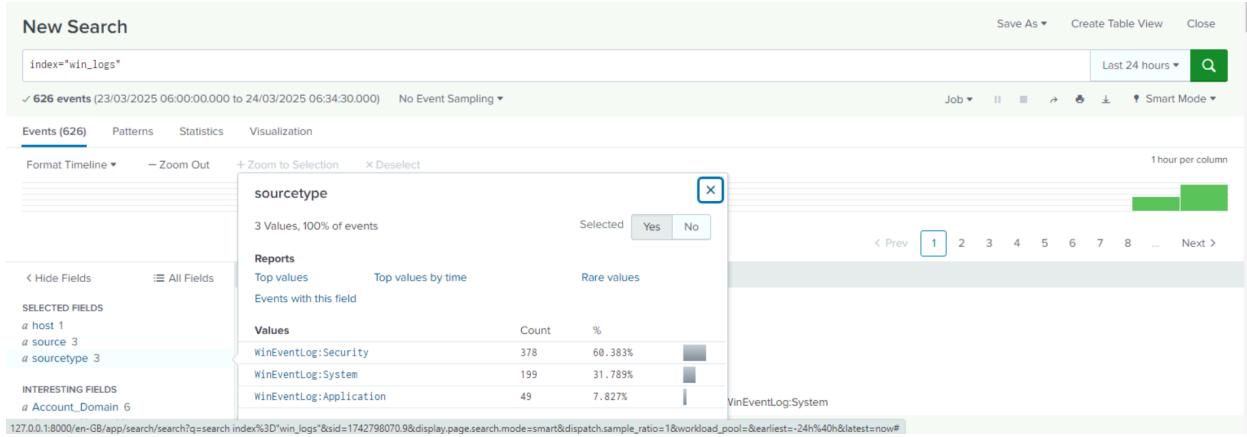
Review

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.



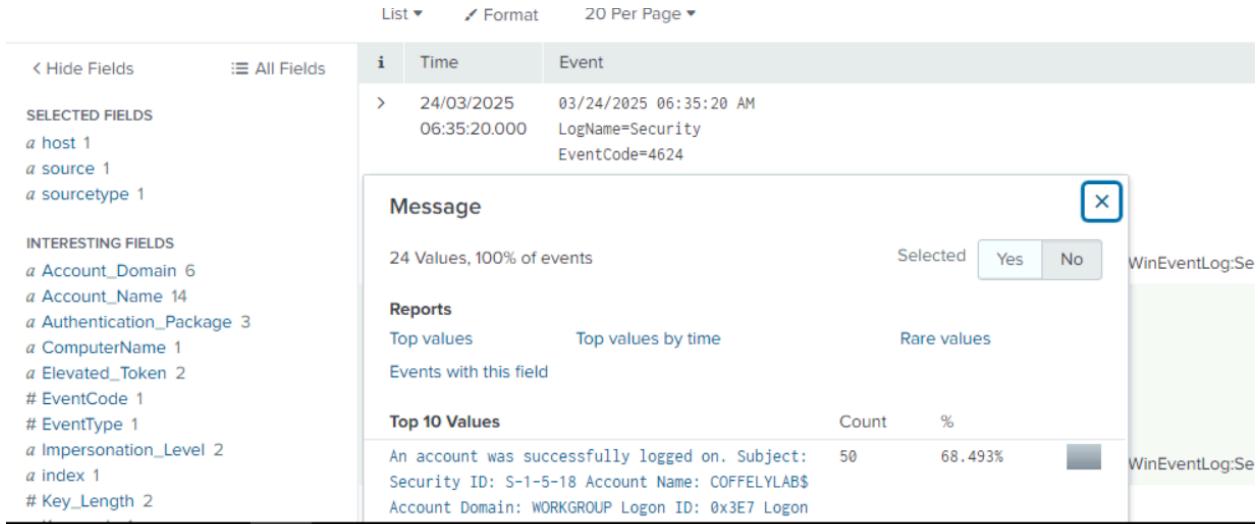
\*\*\*\*\*

### 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

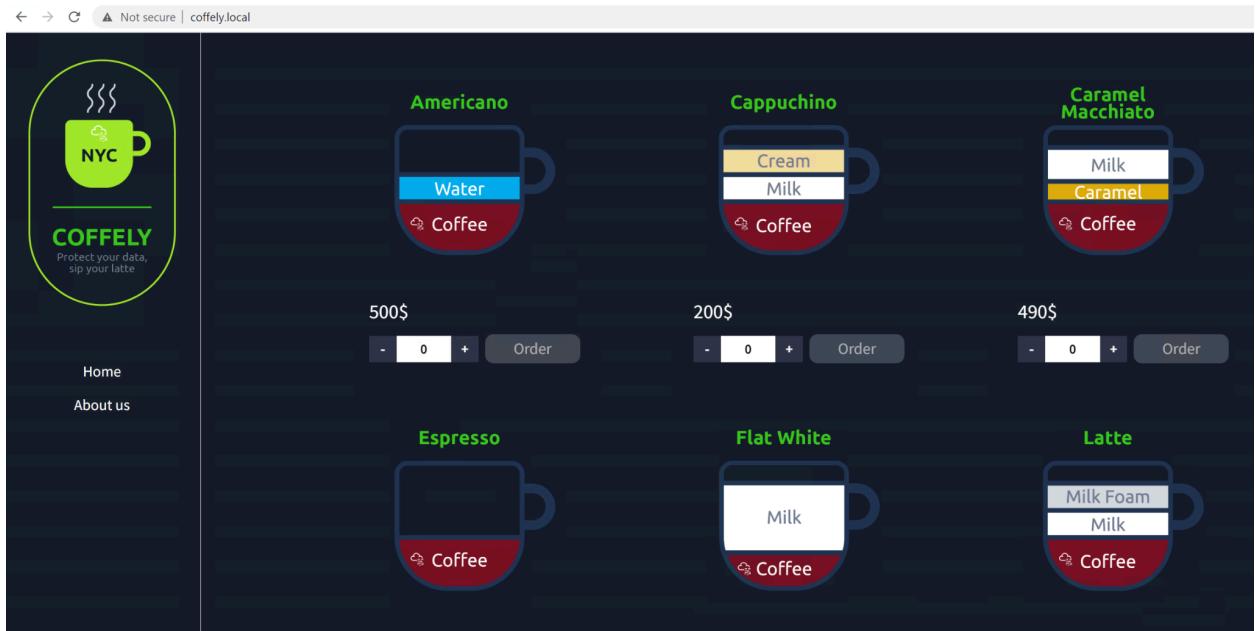
**Search for the events with EventCode=4624. What is the value of the field Message?**



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:

The screenshot shows the Splunk web interface with a red arrow pointing from the 'Forwarder' option in the 'DATA' section of the Settings menu to the 'Forwarder management' link in the main content area.

**Administrator** Messages Settings Activity Help Find

**Add Data**

**Monitoring Console**

**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 'Forwarder' configuration page in Splunk. The 'Forward' option is highlighted with a red box.

**Upload**  
files from my computer  
Local log files  
Local structured files (e.g. CSV)  
[Tutorial for adding data](#)

**Monitor**  
files and ports on this Splunk platform instance  
Files - HTTP - WMI - TCP/UDP - Scripts  
Modular inputs for external data sources

**Forward**  
data from a Splunk forwarder  
Files - TCP/UDP - Scripts

## 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)
<a href="#">add all &gt;</a> WINDOWS coffelylab	<a href="#">remove all &lt;</a> WINDOWS coffelylab

New Server Class Name

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.

The screenshot shows the 'Select Forwarders' interface with the 'Existing' tab selected. A red box highlights the 'Available host(s)' and 'Selected host(s)' sections, both containing 'WINDOWS coffelylab'. Below this, a red box highlights the 'New Server Class Name' input field containing 'web\_logs'.

On the right, the 'Source Types' configuration page is shown. A red box highlights the 'Files & Directories' section under 'Source Types'. An arrow points from this section to the 'File or Directory' input field, which contains 'C:\inetpub\logs\LogFiles\W3SVC2'. This field is also highlighted with a red box. Below it, the 'Includelist' and 'Excludelist' fields are shown as 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

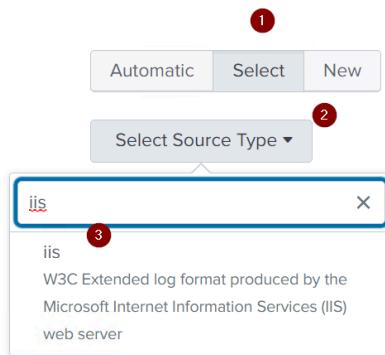
Optionally set additional input parameters for this data input as follows:

### 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](http://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 web interface. At the top, there is a search bar with the query "index='web\_logs' sourcetype='iis'". Below the search bar, it says "27 events (before 10/05/2023 00:58:57.000) No Event Sampling". On the right side of the header, there are buttons for "Job", "All time", and a search icon. Underneath the header, there are tabs for "Events (27)", "Patterns", "Statistics", and "Visualization". Below these tabs, there are buttons for "Format Timeline", "Zoom Out", "Zoom to Selection", and "Deselect". To the right of these buttons, it says "1 minute per column". The main area displays a table of events. The first four rows of the table are highlighted with a red box. The columns are labeled "Time" and "Event". The event details include timestamp, source IP, browser information, and log file path.

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\IIS_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\IIS_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\IIS_ex230510.log   sourcetype = iis
>	10/05/2023 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 11 host = COFFELYLAB source = C:\inetpub\logs\LogFiles\W3SVC2\IIS_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.

The screenshot shows a web browser displaying a website for "COFFELY". The logo features a green coffee cup with "NYC" and "COFFELY" text. Below the logo, it says "Protect your data, sip your latte". The main content area has a dark background with white text. At the top, there are links for "Home" and "About us". Below these, there is a table titled "Order History". The table has columns: SERIAL NO, TIMESTAMP, SOURCE IP, MESSAGE, RESPONSE TIME / MS, BROWSER, QUANTITY, and PRICE. There are three rows of data in the table.

SERIAL NO	TIMESTAMP	SOURCE IP	MESSAGE	RESPONSE TIME / MS	BROWSER	QUANTITY	PRICE
6	2023-04-18 17:30:00	http://127.0.0.1:8000	An order of Chai Tea Latte with quantity of 1 has been placed at 350\$.	200	Mozilla	1	350\$
7	2023-04-18 19:45:00	http://127.0.0.1:8000	An order of Hot Chocolate (COFFELY_Is_Best_IN_Town) with quantity of 1 has been placed at 300\$.	200	Mozilla	1	300\$
8	2023-04-18 21:00:00	http://127.0.0.1:8000	An order of Green Tea with quantity of 2 has been placed at 400\$.	200	Mozilla	2	400\$

Answer: {COFFELY\_Is\_Best\_IN\_Town}