Splunk: Setting up a SOC Lab

Introduction

This repository showcases my experience in setting up a Security Operations Center (SOC) Lab using Splunk. The lab involves the installation and configuration of Splunk on both Linux and Windows platforms, data ingestion from various sources, and performing specific searches to analyze data. This project demonstrates my ability to work with Splunk in a professional setting, highlighting my skills in data analysis and cybersecurity.

Tasks

In this section, I set up a Splunk environment to simulate a SOC. This includes the deployment of Splunk on a Linux server, configuring data forwarders, and ingesting various types of log data.

Deployment on Linux Server

1. Install Splunk:
    - Download and install the Splunk Enterprise package on the Linux server.
    - Follow the on-screen instructions to complete the installation.
2. Start Splunk:
    - Start the Splunk service and enable it to run at boot.
    - Create an administrative user during the setup process.
3. Configure Splunk:
    - Set up initial configuration settings, including network and security parameters.

Interacting with CLI

Using the Command Line Interface (CLI) to interact with Splunk provides greater control and automation capabilities.

1. Start and Stop Splunk:
    - Use ./splunk start and ./splunk stop commands to manage the Splunk service.
2. Check Splunk Status:
    - Use ./splunk status to check the status of the Splunk service.
3. Manage User Accounts:
    - Create and manage user accounts with specific roles and permissions.

Data Ingestion

Configuring Forwarder on Linux

1. Setup Receiving Port:
    - Configure Splunk to listen on port 9997 for incoming data from forwarders.
    - Save the configuration to start receiving data.
2. Create a New Index:
    - Define a new index in Splunk to store the incoming log data.
3. Monitor Log Files:
    - Configure the Splunk forwarder to monitor specific log files, such as /var/log/syslog.

Configuring Forwarder on Windows

1. Install Universal Forwarder:
    - Download and install the Splunk Universal Forwarder on the Windows host.
    - Accept the license agreement and choose to use it with an on-premises Splunk Enterprise instance.

2. Setup Administrator Account:
    - Create an administrative account during the installation process.
3. Configure Forwarder:
    - Set up the forwarder to send logs to the Splunk instance.

Ingesting Windows Logs

1. Select Forwarders:
    - Configure Splunk to receive data from the Windows forwarder.
2. Select Source:
    - Specify the log source, such as Local Event Logs, to be ingested.
3. Create Index:
    - Create an index to store the incoming Event logs.
4. Start Searching:
    - Verify that logs are being received and indexed correctly by Splunk.

Ingesting Web Logs

1. Select Forwarders:
    - Choose the web host from which to receive log data.
2. Select Source:
    - Specify the directory containing the web logs (e.g., C:\inetpub\logs\LogFiles\W3SVC1).
3. Input Settings:
    - Configure the source type and create an index for the web logs.
4. Start Propagation:
    - Logs should start appearing in the search tab after a few minutes.

Task 1: Introduction

Task 1 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.

Task 2: Splunk: Setting up a Lab

Task 2 Splunk: Setting up a Lab

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. Each lab covers the following topics:

Linux Lab

- Install Splunk on Ubuntu Server
- Install and integrate Universal Forwarder
- Collecting Logs from important logs sources/files like syslog, auth.log, audited, etc

Windows Lab

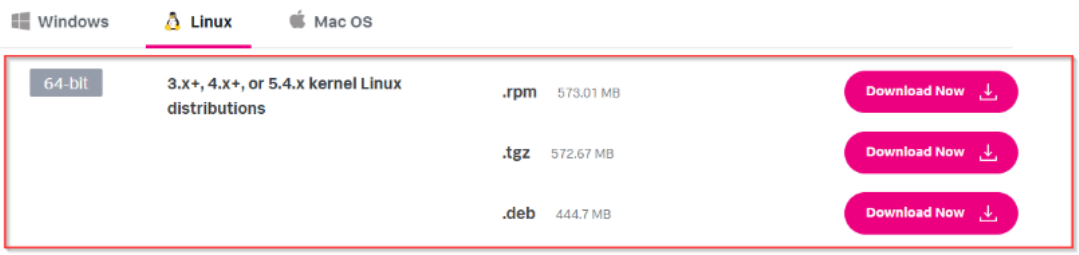
- Install Splunk on Windows Machine
- Install and Integrate the Universal Forwarder
- Integrating and monitoring Coffely.THM's weblogs
- Integrating Windows Event Logs

Task 3: Splunk: Deployment on Linux Server

Task 3 Splunk: Deployment on Linux Server

Start Machine

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



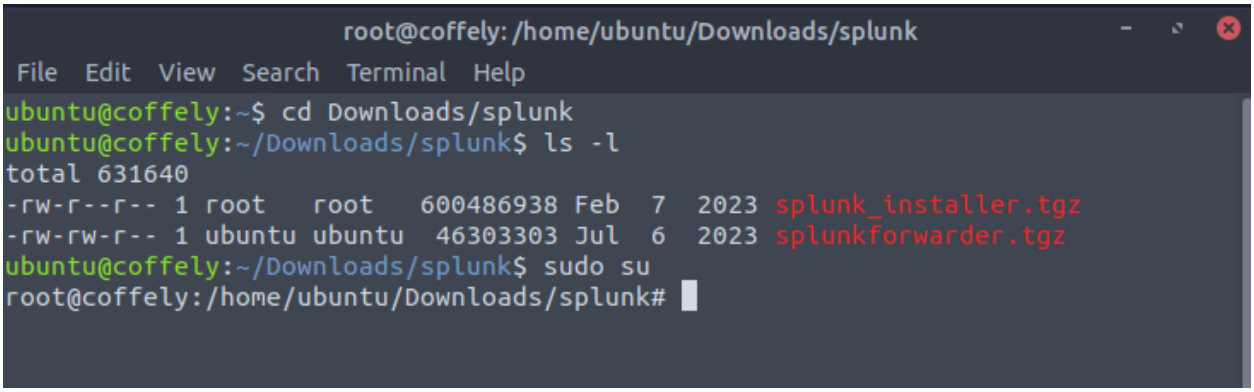
Note: Users are not expected to create an account and download the Splunk Enterprise during this activity. All required executables are already downloaded in relevant paths.

1.

Connect with the Lab

This task will explore installing and configuring Splunk on a Linux machine. Connect with the lab by pressing the **Start Machine** button at the top of this task, and it 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. It will take around 3-5 minutes to load fully.

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



2.

Splunk Installation

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
splunk/
splunk/splunk-9.0.3-dd0128b1f8cd-linux-2.6-x86_64-manifest
splunk/swidtag/
splunk/swidtag/splunk-Splunk-Enterprise-primary.swidtag
splunk/ftr
splunk/openssl/
splunk/openssl/misc/
splunk/openssl/misc/c_info
splunk/openssl/misc/tsget
splunk/openssl/misc/c_issuer
splunk/openssl/misc/CA.sh
splunk/openssl/misc/c_hash
splunk/openssl/misc/c_name
splunk/openssl/misc/CA.pl
splunk/openssl/openssl.cnf
splunk/openssl/copyright.txt
splunk/share/
```

3.

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 -l
total 631644
drwxr-xr-x 10  10777  10777      4096 Dec 13  2022 splunk
-rw-r--r--  1 root   root   600486938 Feb  7  2023 splunk_installer.tgz
-rw-rw-r--  1 ubuntu ubuntu  46303303 Jul  6  2023 splunkforwarder.tgz
root@coffely:/home/ubuntu/Downloads/splunk# mv splunk /opt/
root@coffely:/home/ubuntu/Downloads/splunk# ls -l
total 631640
-rw-r--r-- 1 root   root   600486938 Feb  7  2023 splunk_installer.tgz
-rw-rw-r-- 1 ubuntu ubuntu  46303303 Jul  6  2023 splunkforwarder.tgz
root@coffely:/home/ubuntu/Downloads/splunk# ls -l /opt/
total 4
drwxr-xr-x 10 10777 10777 4096 Dec 13  2022 splunk
root@coffely:/home/ubuntu/Downloads/splunk#
```

4.

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:/home/ubuntu/Downloads/splunk# cd /opt/splunk/bin/
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, y
ou cannot 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: Gerren
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

Moving '/opt/splunk/share/splunk/search_mrsparkle/modules.new' to '/opt/splunk/sh
are/splunk/search_mrsparkle/modules'.
```

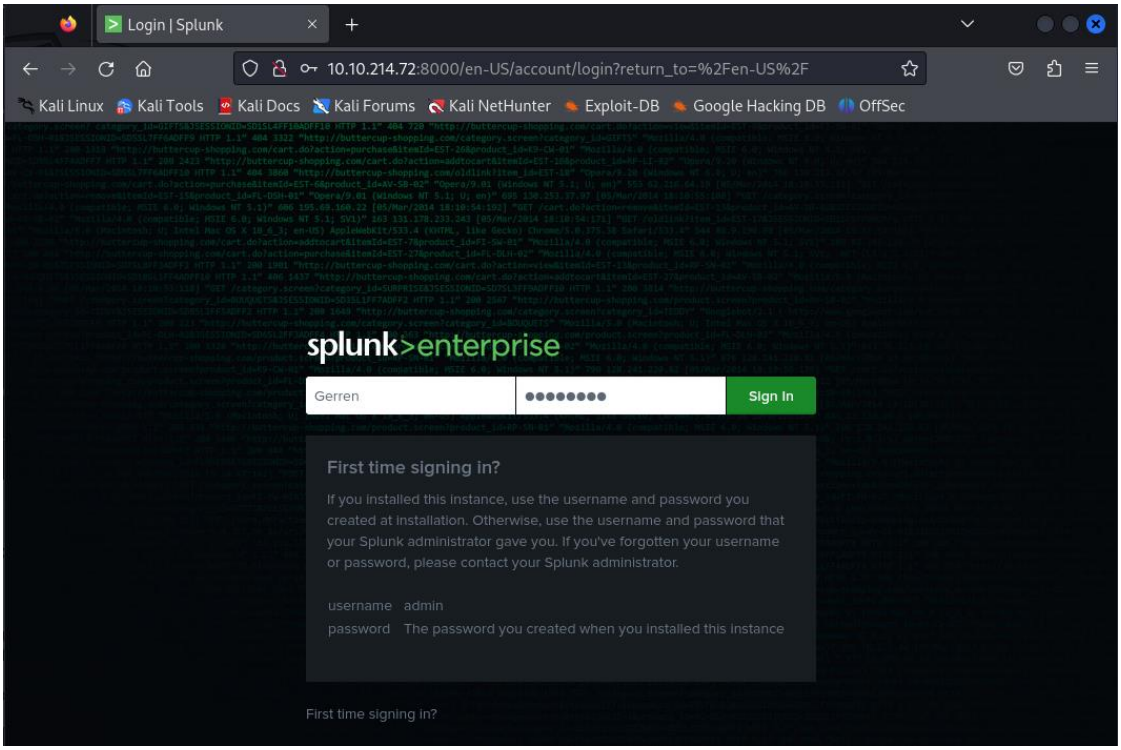
```
Waiting for web server at http://127.0.0.1:8000 to be available............... Do
ne


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

root@coffely:/opt/splunk/bin#
```

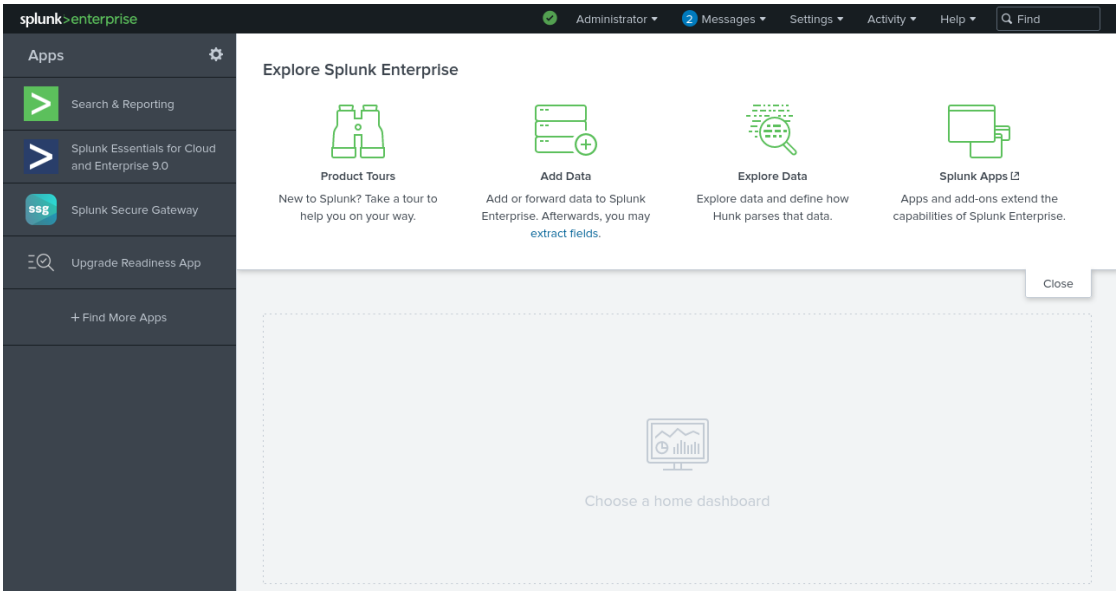
5.

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://10.10.214.72:8000`.

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





Task 4: Splunk: Interacting with CLI

Task 4 Splunk: Interacting 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:

1.

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.

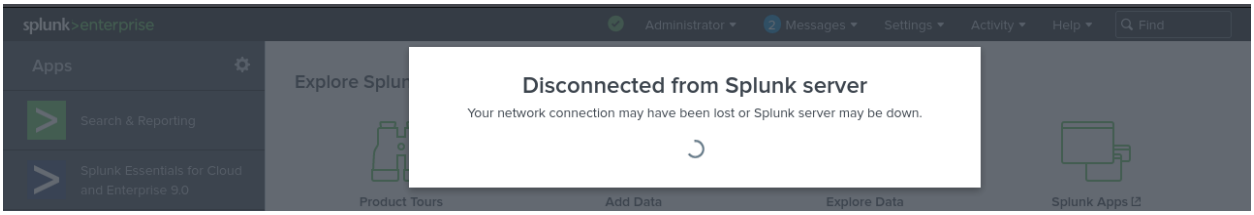
```
root@coffely:/opt/splunk/bin# cd ..
root@coffely:/opt/splunk# ./bin/splunk start
The splunk daemon (splunkd) is already running.


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

root@coffely:/opt/splunk#
```

2.

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.
root@coffely:/opt/splunk#
```



3.

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.
```

4.

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: 12600).
splunk helpers are running (PIDs: 12601 12733 12793 12802 12815 12873).
root@coffely:/opt/splunk#
```

5.

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.

6.

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

./bin/splunk search coffely

✓ Correct Answer

Hint

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

No answer needed

✓ Correct Answer

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

Task 5: Splunk: Data Ingestion

Task 5 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:

1.

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:/home/ubuntu/Downloads/splunk# mv splunkforwarder /opt/
root@coffely:/home/ubuntu/Downloads/splunk# cd /opt/splunkforwarder/
root@coffely:/opt/splunkforwarder# ./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, y
ou cannot 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: Gerren
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
```

```
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/splunkforwarder/var/run/splunk/appserver/i18n
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/s
tatic/css
                Creating: /opt/splunkforwarder/var/run/splunk/upload
                Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
                Creating: /opt/splunkforwarder/var/run/splunk/search_log
                Creating: /opt/splunkforwarder/var/spool/splunk
                Creating: /opt/splunkforwarder/var/spool/dirmoncache
                Creating: /opt/splunkforwarder/var/lib/splunk/authDb
                Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
```

2.

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

8089

✓ Correct Answer

```
Checking prerequisites...
        Checking mgmt port [8089]: not available
ERROR: mgmt port [8089] - port is already bound.  Splunk needs to use this port.
```

Task 6: Configuring Forwarder on Linux

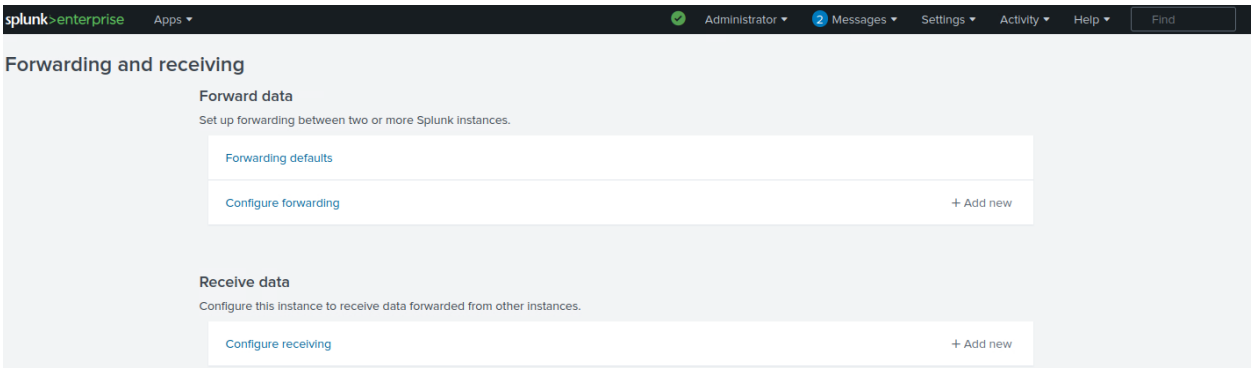
Task 6 Configuring Forwarder on Linux

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.

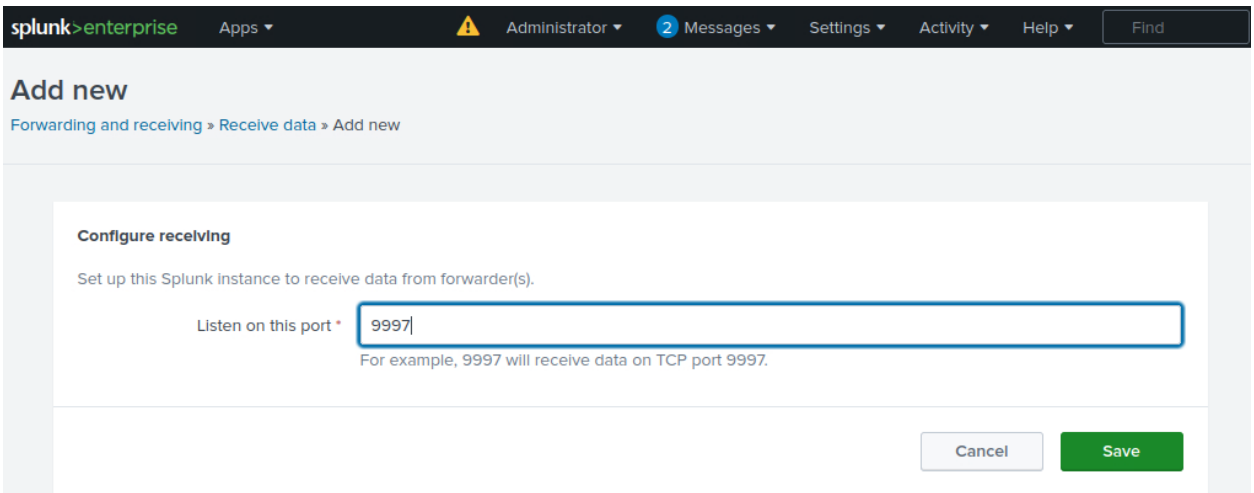
Splunk Configuration

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

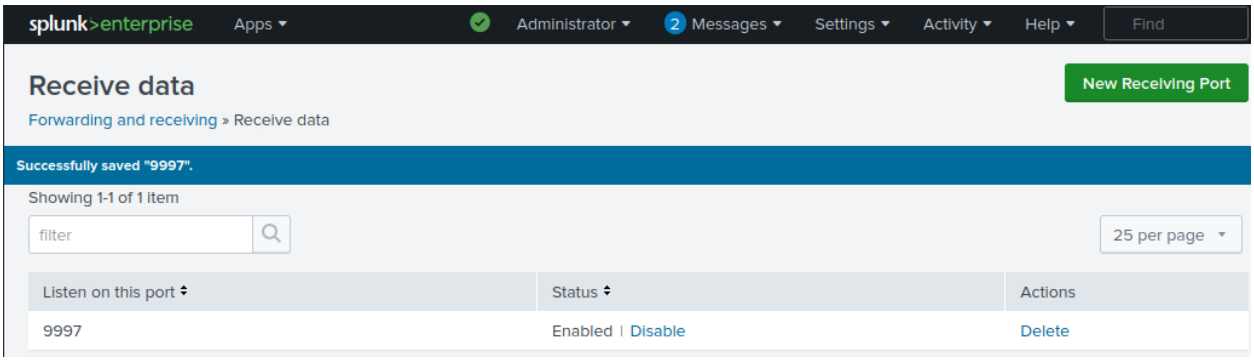
1.



In Forwarding and receiving, there are multiple options to configure both forwarding and receiving. As I want to receive data from the Linux endpoint, I clicked on Configure receiving and then proceeded by configuring a new receiving port.



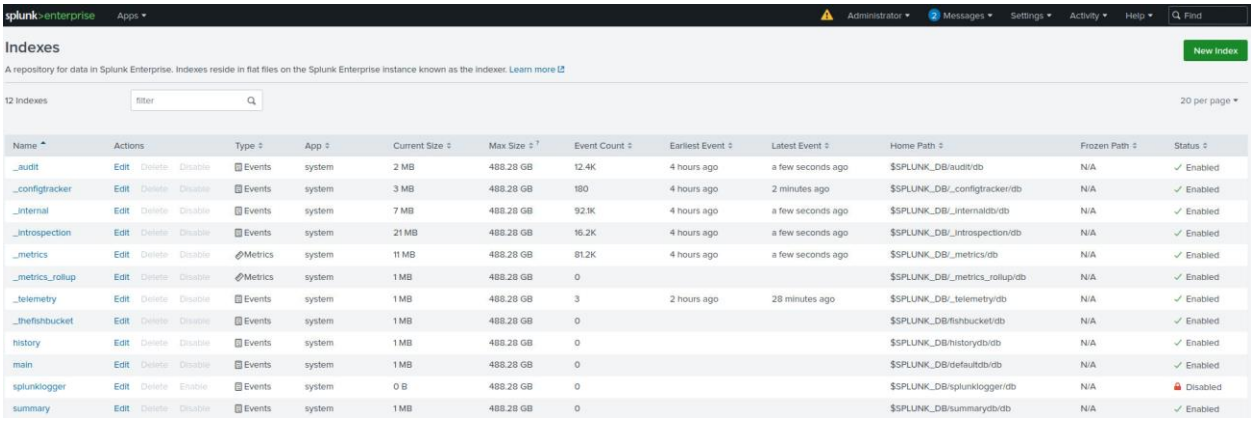
The Splunk instance receives data from the forwarder on the port 9997. I will start listening on port 9997 and Save.



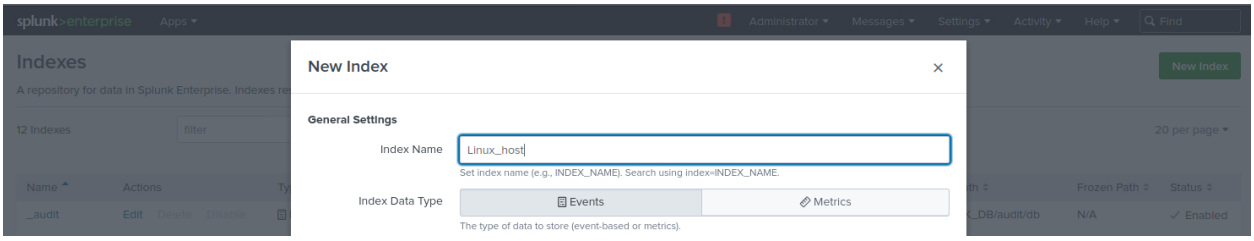
2.

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.



Click New Index and fill it out.



3.

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/splunkforwarder# cd bin
root@coffely:/opt/splunkforwarder/bin# ./splunk add forward-server 10.10.189.209
:9997
Splunk username: Gerren
Password:
Added forwarding to: 10.10.189.209:9997.
root@coffely:/opt/splunkforwarder/bin#
```

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:/opt/splunkforwarder/bin# ls /var/log
Xorg.0.log                dist-upgrade              kern.log.3.gz
Xorg.0.log.old            dmesg                     kern.log.4.gz
alternatives.log          dmesg.0                   landscape
alternatives.log.1        dmesg.1.gz                lastlog
alternatives.log.2.gz     dmesg.2.gz                lightdm
amazon                    dmesg.3.gz                openvpn
apport.log                dmesg.4.gz                prime-offload.log
apport.log.1              dpkg.log                  prime-supported.log
apt                       dpkg.log.1                private
auth.log                  dpkg.log.2.gz             samba
auth.log.1                fontconfig.log            speech-dispatcher
auth.log.2.gz             gdm3                      syslog
auth.log.3.gz             gpu-manager-switch.log    syslog.1
auth.log.4.gz             gpu-manager.log           syslog.2.gz
btmp                      hp                        syslog.3.gz
btmp.1                    journal                   syslog.4.gz
cloud-init-output.log     kern.log                  unattended-upgrades
cloud-init.log            kern.log.1                wtmp
cups                      kern.log.2.gz
root@coffely:/opt/splunkforwarder/bin#
```

Next, I will tell Splunk forwarder to monitor the /var/log/syslog file

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

4.

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/splunkforwarder/bin# cd /opt/splunkforwarder/etc/apps/search/local/
root@coffely:/opt/splunkforwarder/etc/apps/search/local# ls -l
total 4
-rw------- 1 root root 64 Jul 11 15:25 inputs.conf
root@coffely:/opt/splunkforwarder/etc/apps/search/local# cat inputs.conf
[monitor:///var/log/syslog]
disabled = false
index = Linux_host
root@coffely:/opt/splunkforwarder/etc/apps/search/local#
```

5.

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.

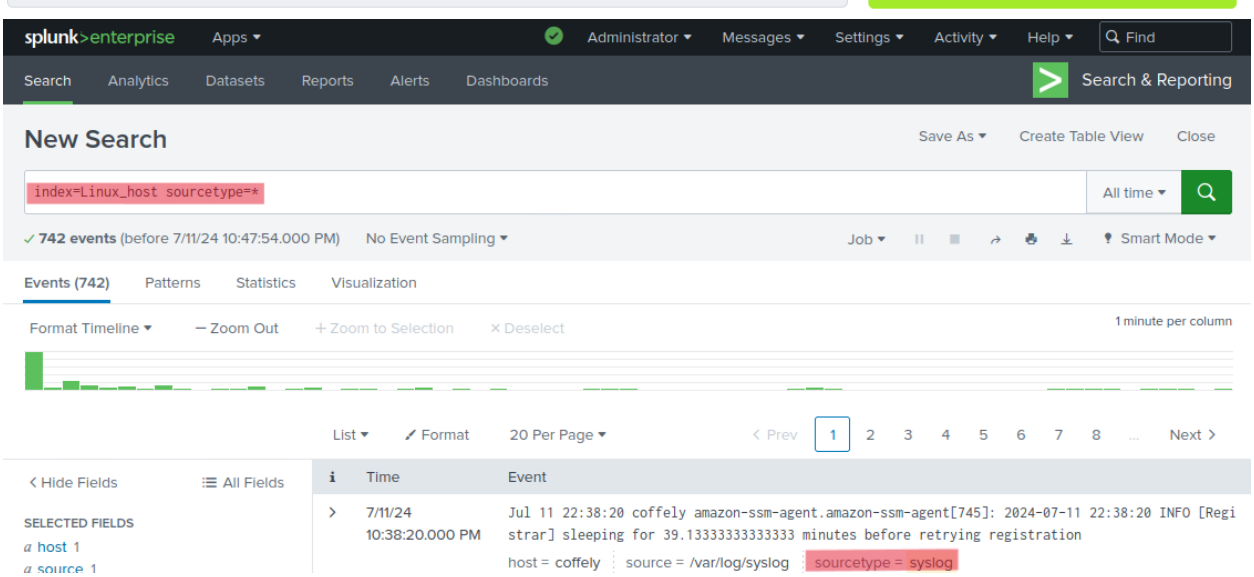
```
root@coffely:/opt/splunkforwarder/etc/apps/search/local# cd ../../../../
root@coffely:/opt/splunkforwarder# cd /opt/splunkforwarder/bin
root@coffely:/opt/splunkforwarder/bin# logger "coffely-has-the-best-coffee-in-town"
root@coffely:/opt/splunkforwarder/bin# tail -1 /var/log/syslog
Jul 11 22:32:48 coffely ubuntu: coffely-has-the-best-coffee-in-town
root@coffely:/opt/splunkforwarder/bin#
```

6.

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



7.

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

/etc/group

✓ Correct Answer

```
root@coffely:/opt/splunkforwarder/bin# sudo 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:
Retype new password:
passwd: password updated successfully
Changing the user information for analyst
Enter the new value, or press ENTER for the default
        Full Name []: Gerren
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
root@coffely:/opt/splunkforwarder/bin#
```

```
root@coffely:/opt/splunkforwarder/bin# grep 'analyst' /etc/group
analyst:x:1001:
root@coffely:/opt/splunkforwarder/bin#
```

Task 7: Splunk: Installing on Windows

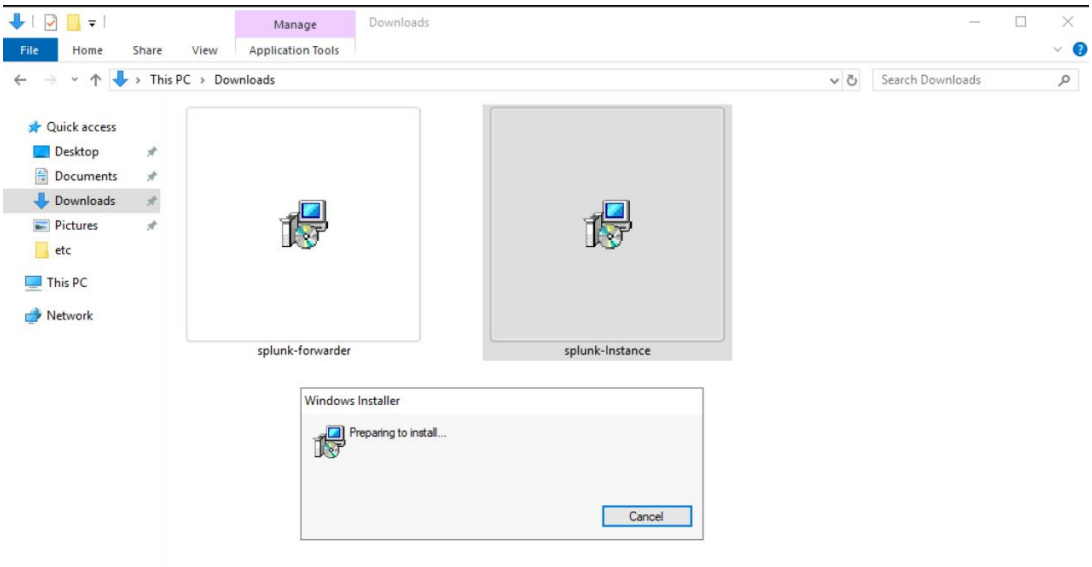
Task 7 Splunk: Installing on Windows

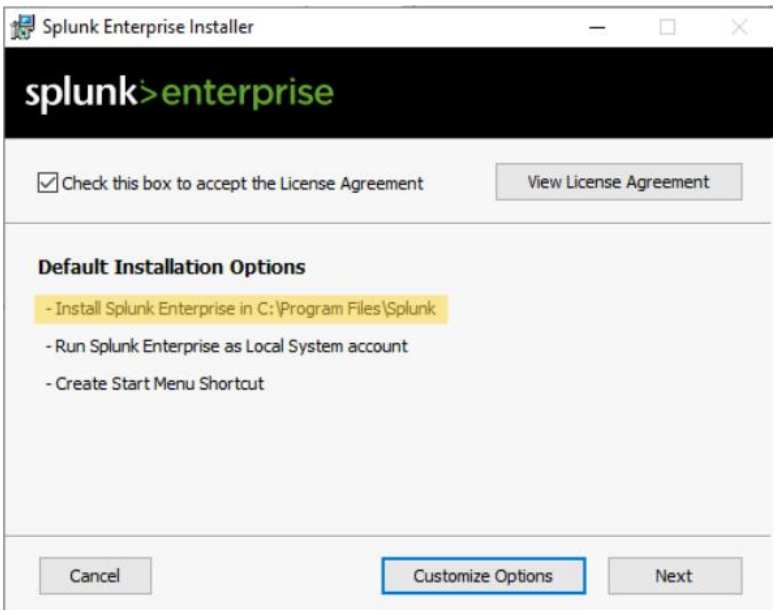
Installing Splunk on a Windows platform is relatively simple with just running the installer. Connect with the Windows Machine by clicking the `Start Machine` button on the right. It will take around 3-5 minutes to boot completely and will start in **Split-Screen View** on the right side of the screen.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

Start Machine

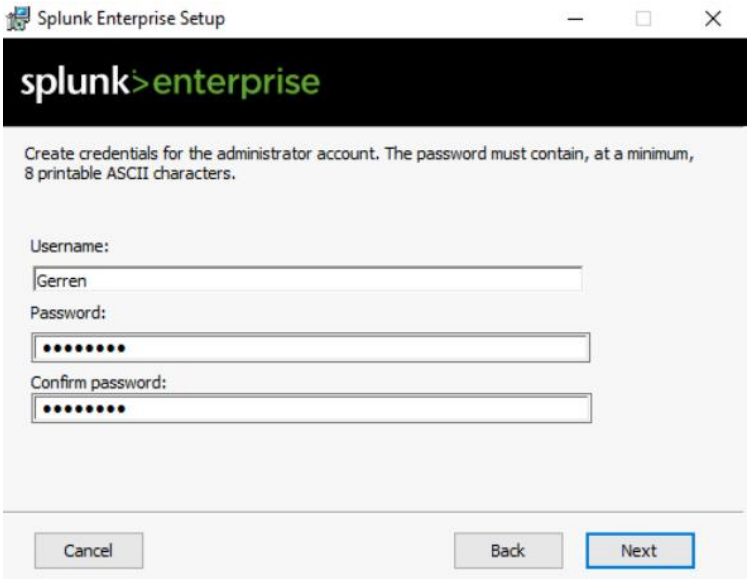
On the Windows machine, we will first install Splunk, configure a forwarder to capture Windows Event logs, and integrate `Coffely` weblogs to collect all requests and responses into Splunk Instance.

1.

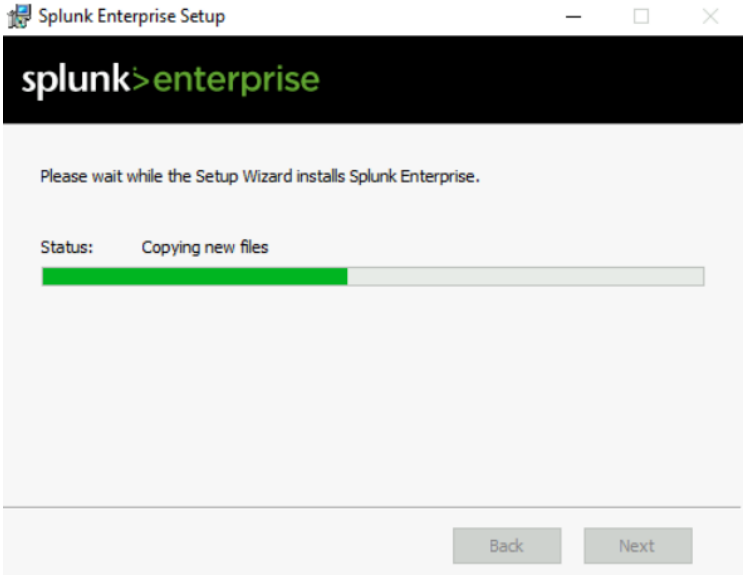




An important step during installation is creating an administrator account, as shown below. This account will have high privileges, create and manage other accounts, and control all administrative roles.

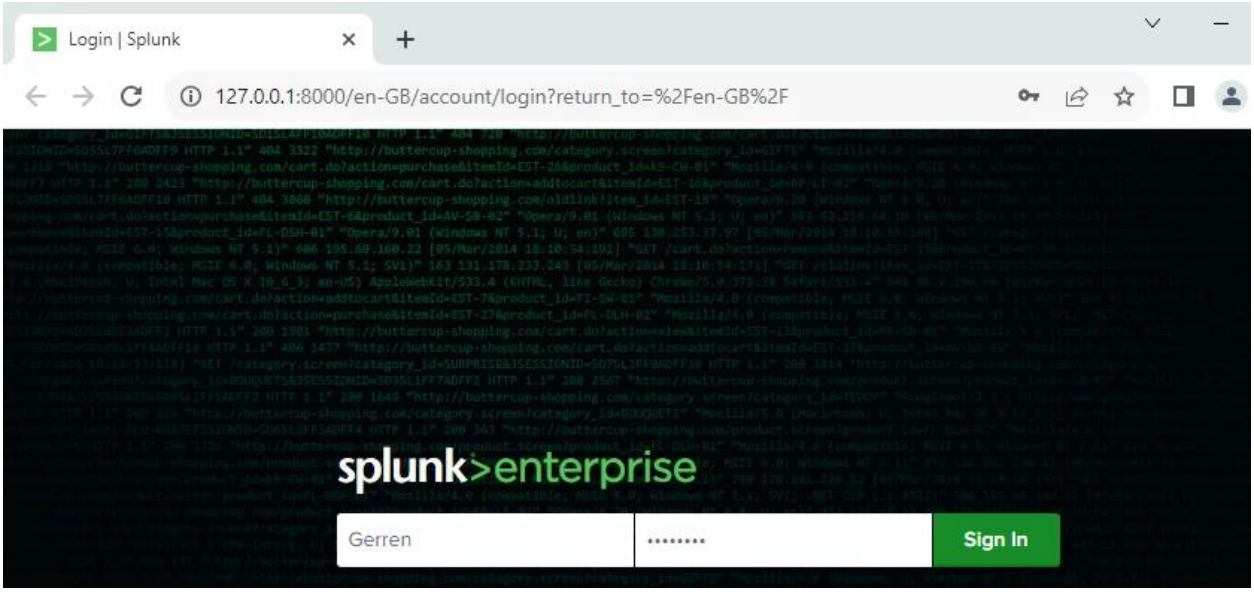


Next it will look for the system requirement for compatibility and other checks.

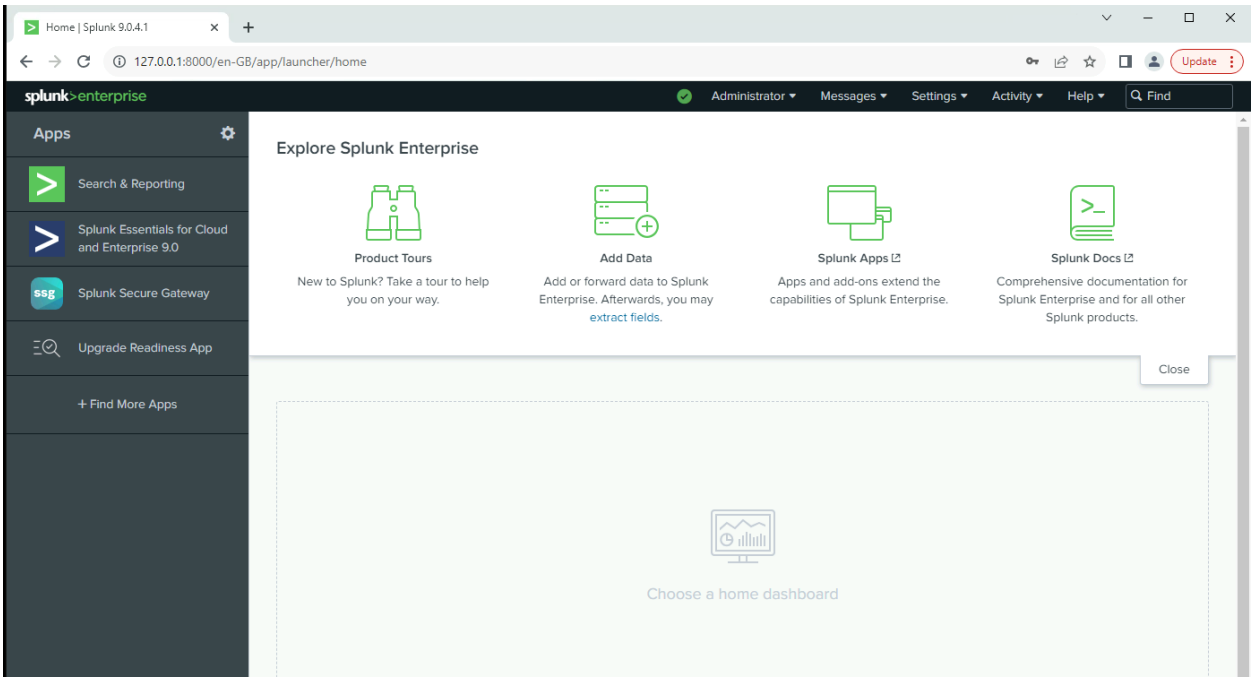


2.
Accessing Splunk Instance

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://10.10.246.105:8000`.



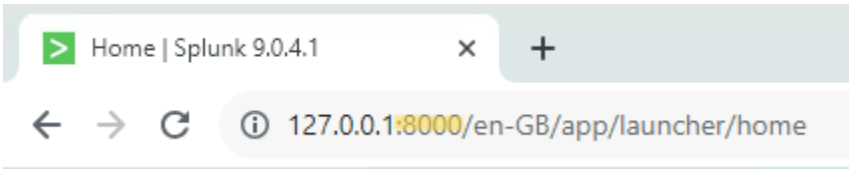
Login



3.

What is the default port Splunk runs on?

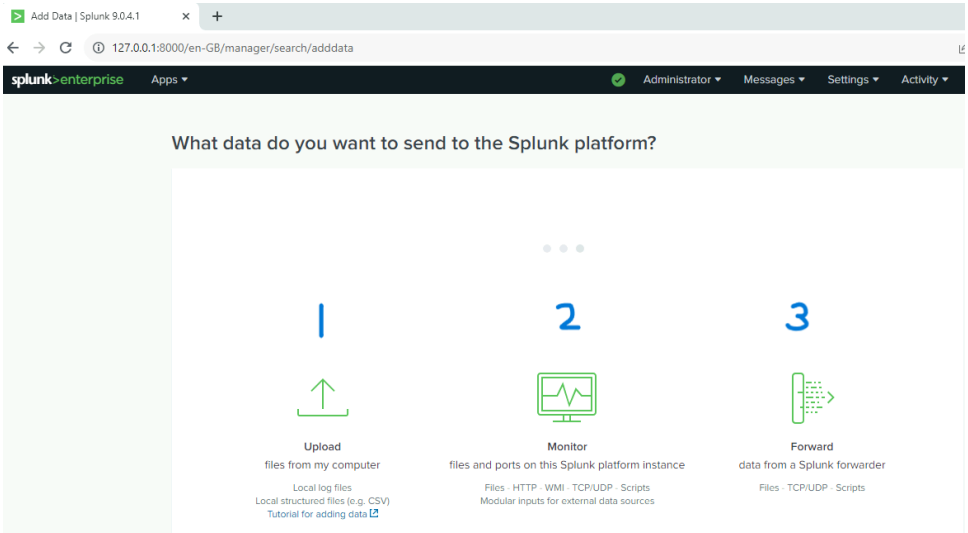
8000 ✓ Correct Answer



4.

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

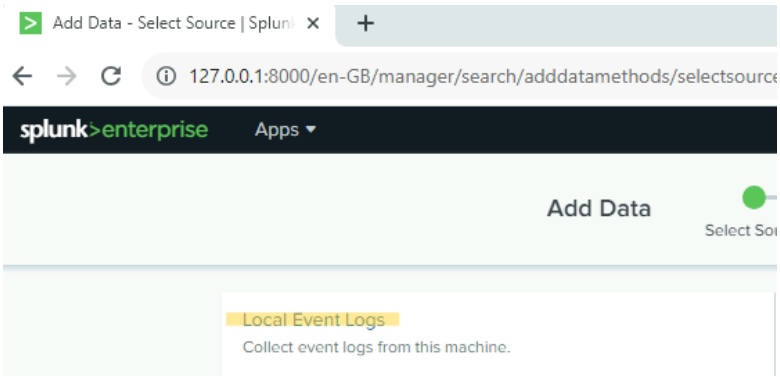
3 ✓ Correct Answer



5.

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

Local Event Logs ✓ Correct Answer



Task 8: Installing and Configuring Forwarder

Task 8 Installing and Configuring Forwarder

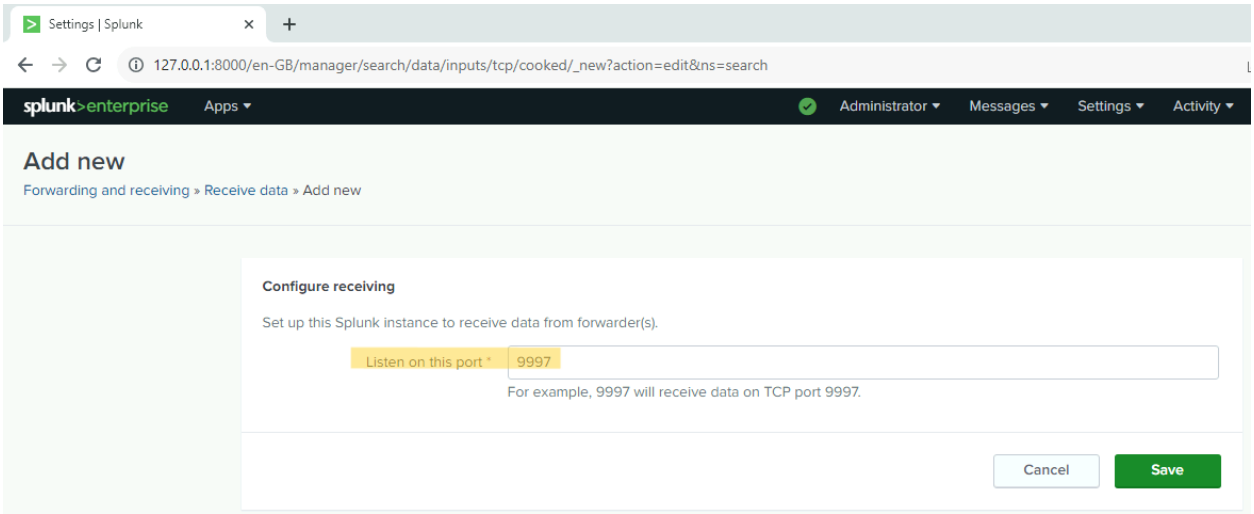
First, we will configure the receiver on Splunk so the forwarder knows where to send the data.

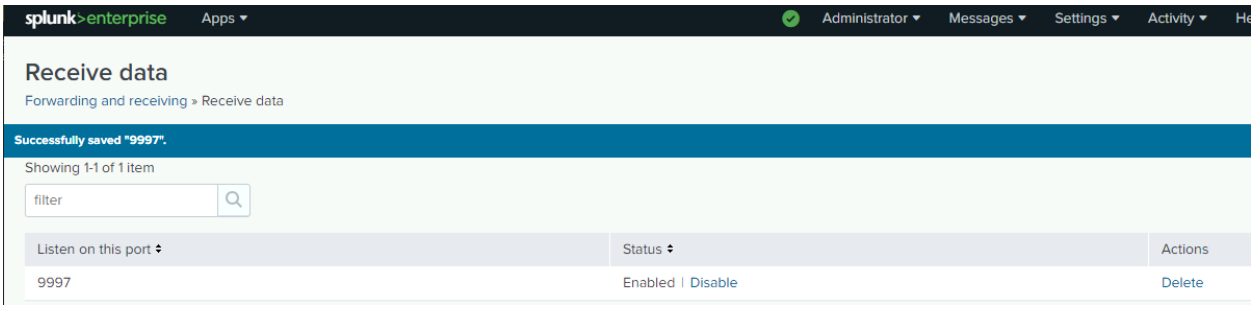
Configure Receiving

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

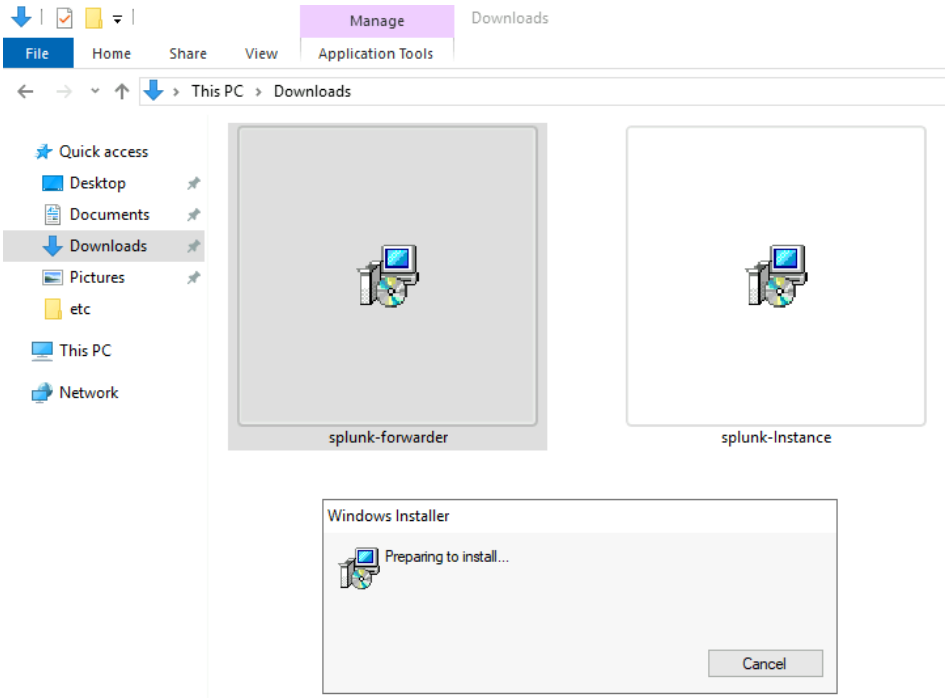
A lot of this task is a repeat of Task 6: Configuring Forwarder on Linux, only we will be doing this in Windows OS.

1.

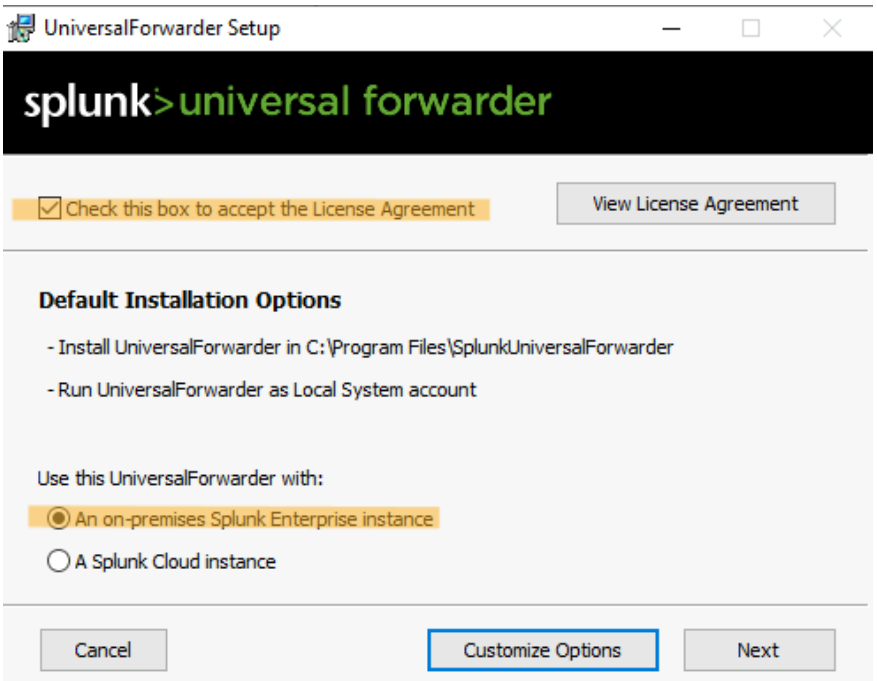




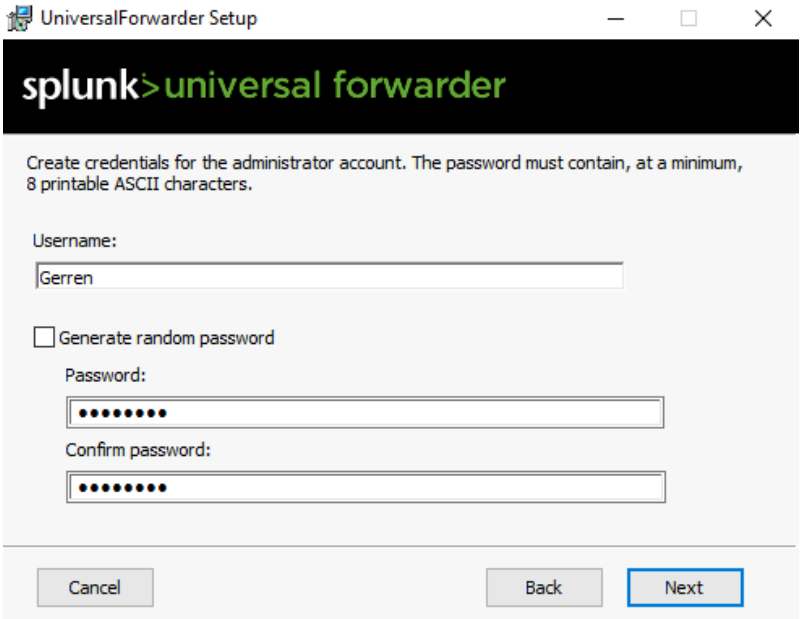
I downloaded the Splunk-forwarder



Make sure that you accept the License Agreement and click, use this UniversalForwarder with: An on-premises Splunk Enterprise instance. UniversalForwarder Setup

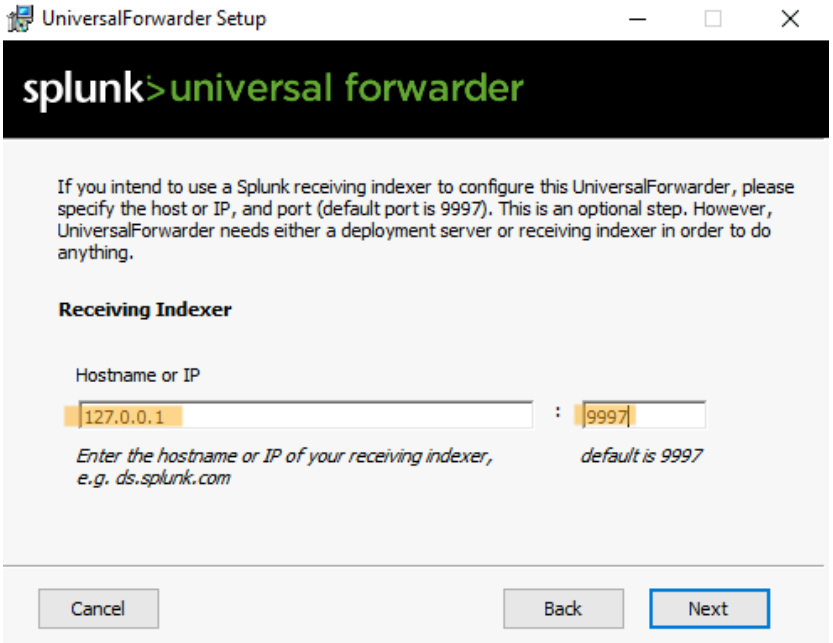


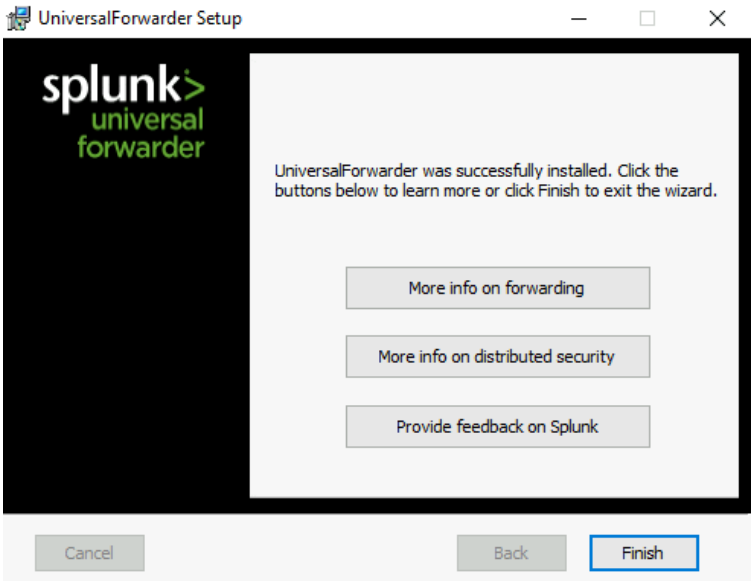
Set up an administrator account.



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.

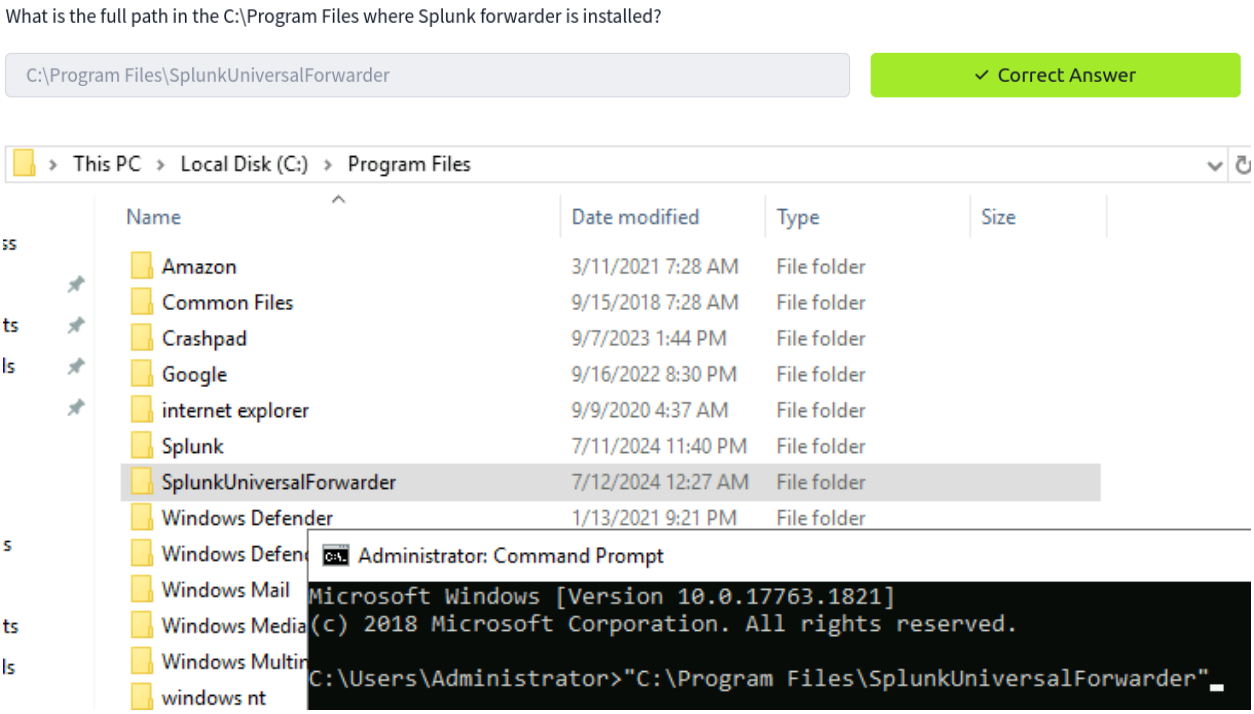




Now that Splunk forwarder is installed, I will configure our forwarder to send logs to my Splunk instance in the upcoming tasks.

2.

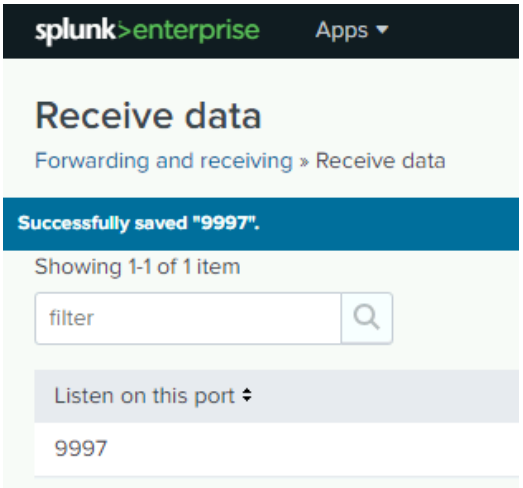
Drag and drop the SplunkUniversalForwarder into the command prompt to get the exact path location of the folder.



3.

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

9997 ✓ Correct Answer



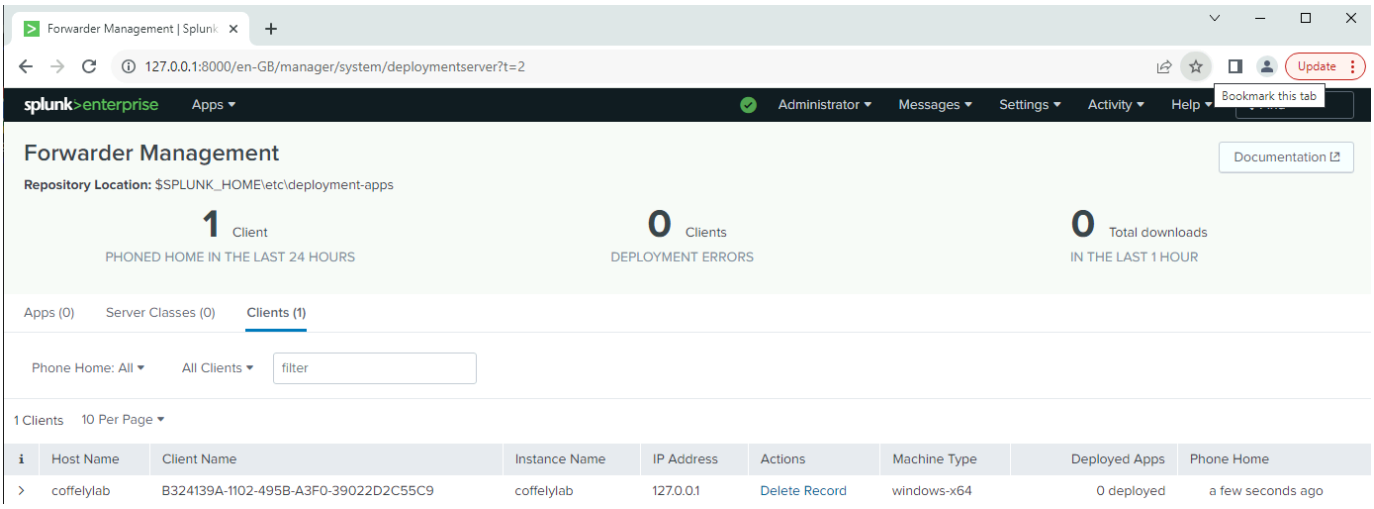
Task 9: Splunk: Ingesting Windows Logs

Task 9 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.

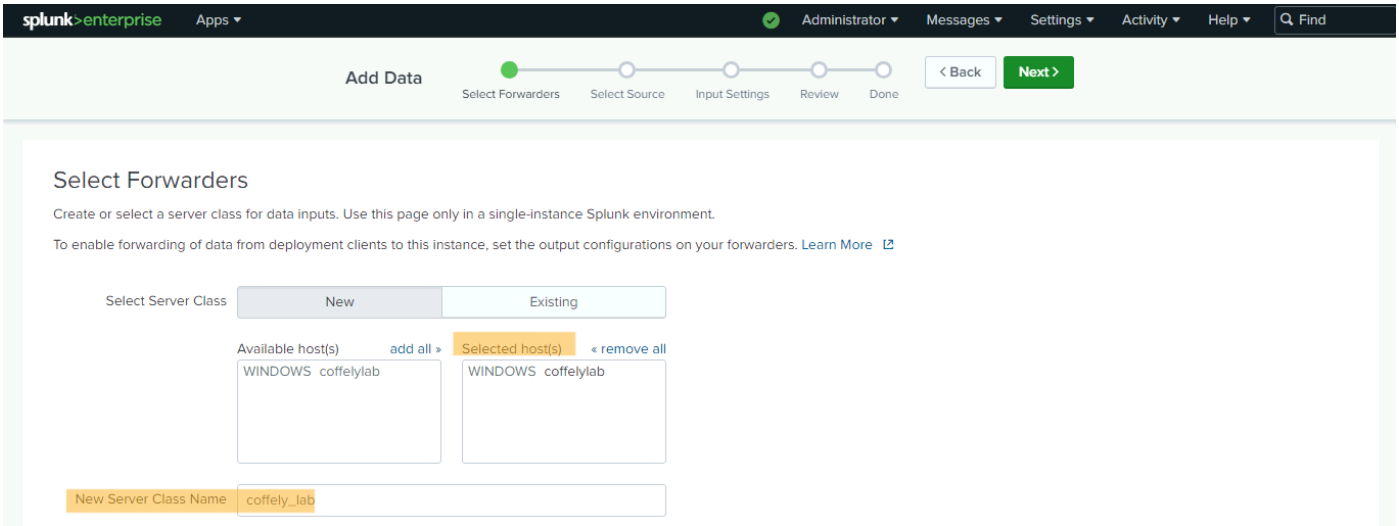
Check Forwarder Management

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



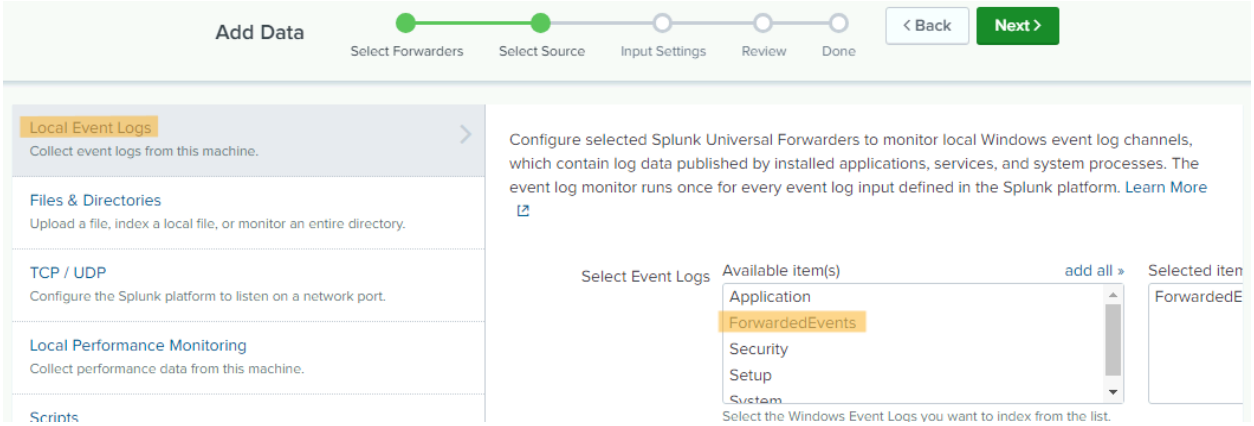
1. Select Forwarders

This shows that I have properly configured the forwarder on the host. Now I will configure Splunk to receive the Event Logs. This can be found in Settings → Add data → Forward (data from a Splunk forwarder).



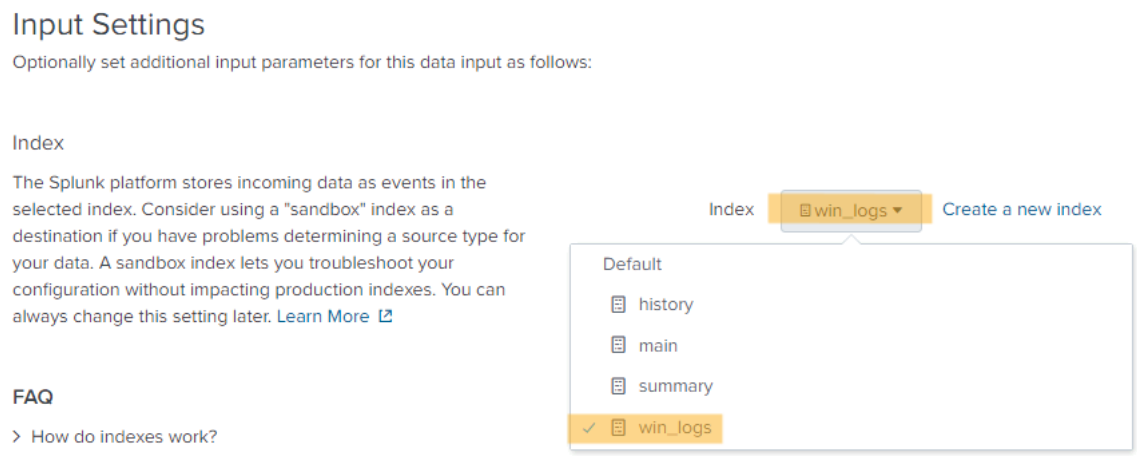
2. Select Source

Next, I am going to select the log source that we need to ingest. The list shows many log sources, but I am going to use Local Event Logs to configure receiving Event Logs from the host.

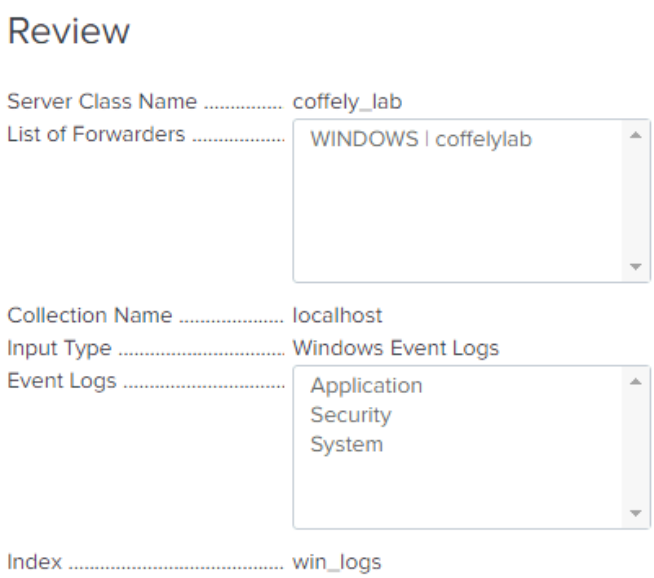


3. Creating Index

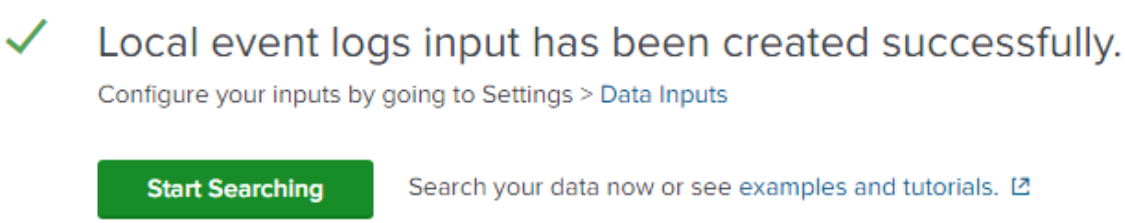
I created an index that stores the incoming Event logs.

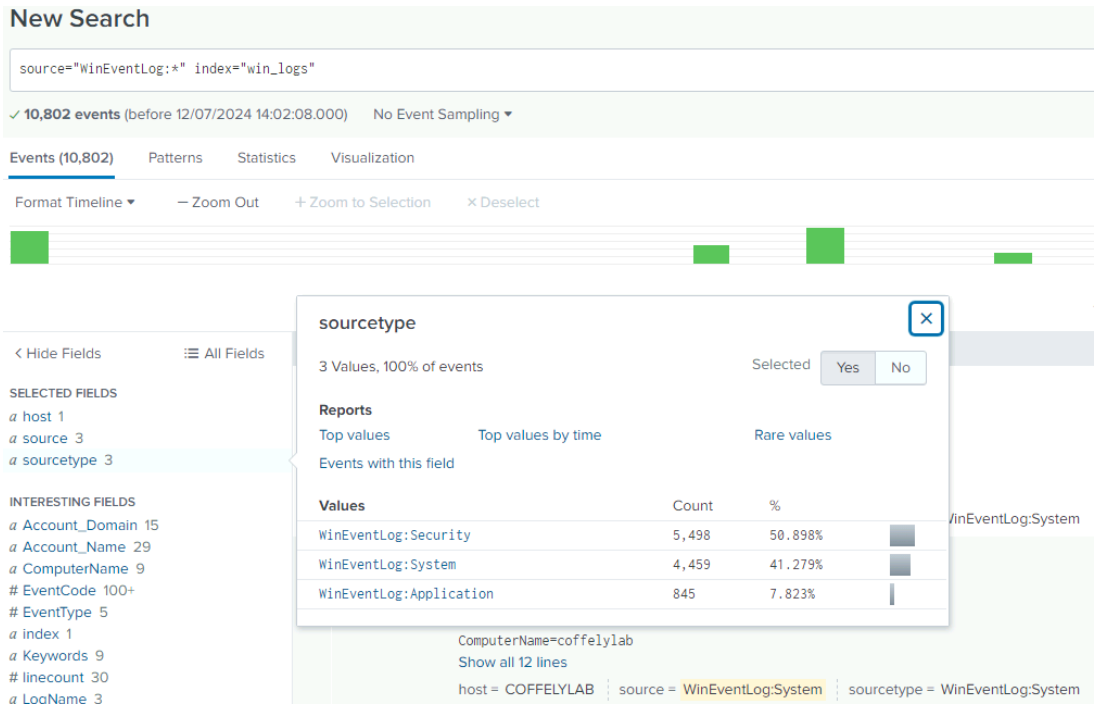


4. Review



Click on Start Searching and we should receive the Event Logs immediately.

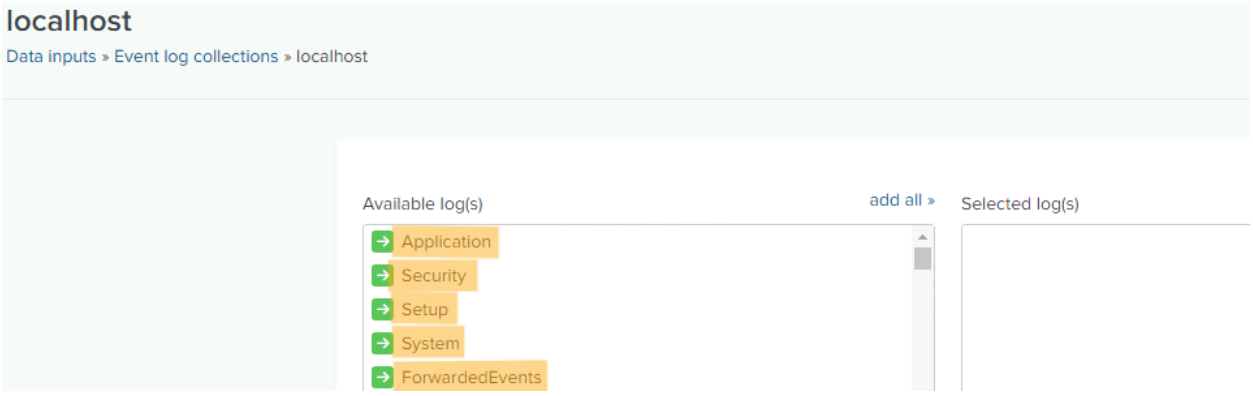




5.

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

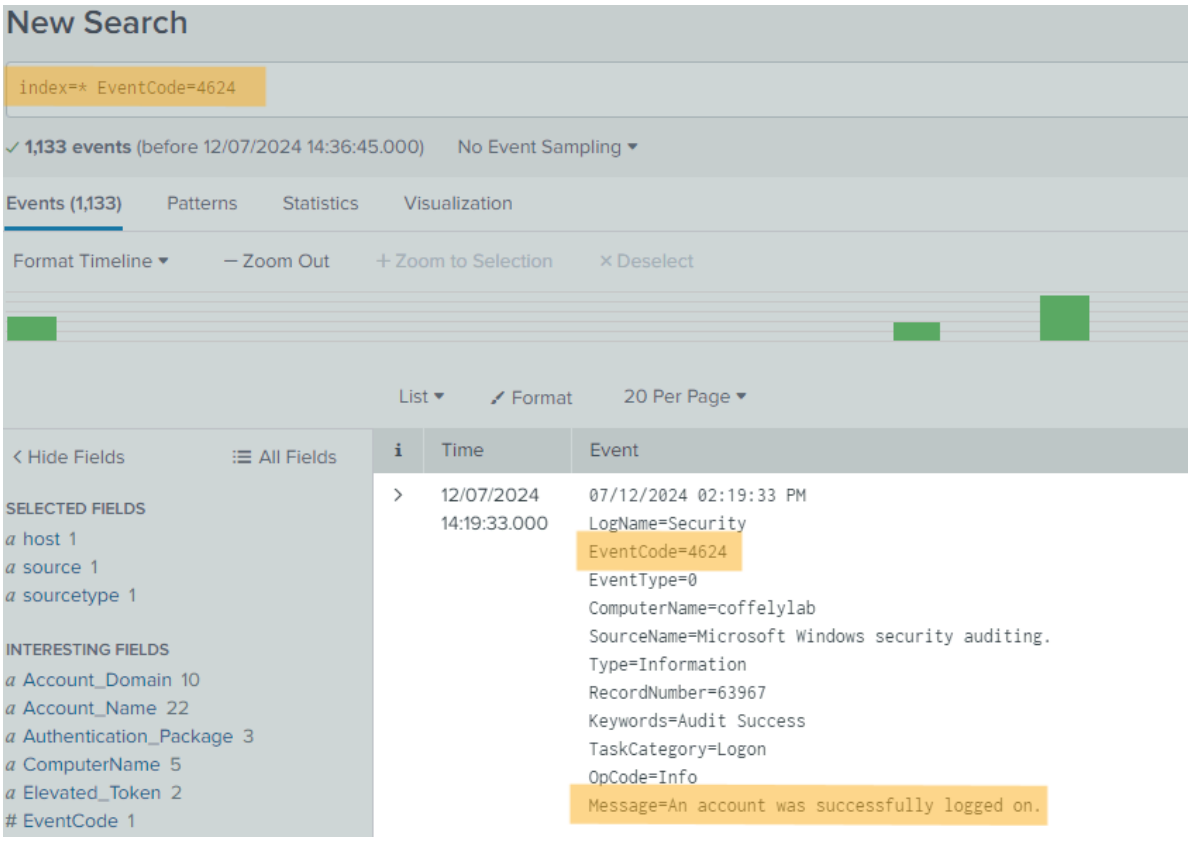
5 ✓ Correct Answer



6.

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

An account was successfully logged on. ✓ Correct Answer


New Search
index=* EventCode=4624
1,133 events (before 12/07/2024 14:36:45.000)
No Event Sampling
Events (1,133)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
List
Format
20 Per Page
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
Account_Domain 10
Account_Name 22
Authentication_Package 3
ComputerName 5
Elevated_Token 2
EventCode 1
Time
Event
12/07/2024 14:19:33.000
07/12/2024 02:19:33 PM
LogName=Security
EventCode=4624
EventType=0
ComputerName=coffelylab
SourceName=Microsoft Windows security auditing.
Type=Information
RecordNumber=63967
Keywords=Audit Success
TaskCategory=Logon
OpCode=Info
Message=An account was successfully logged on.

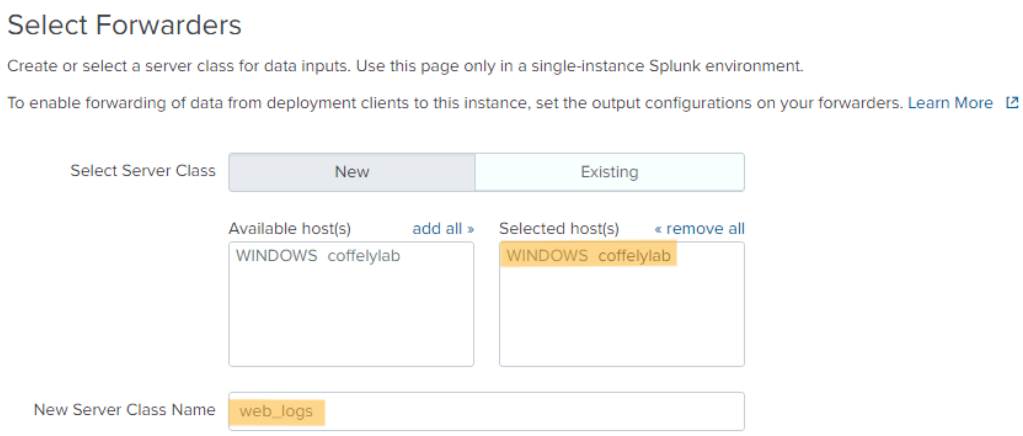
Task 10: Ingesting Coffely Web Logs

Task 10 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.

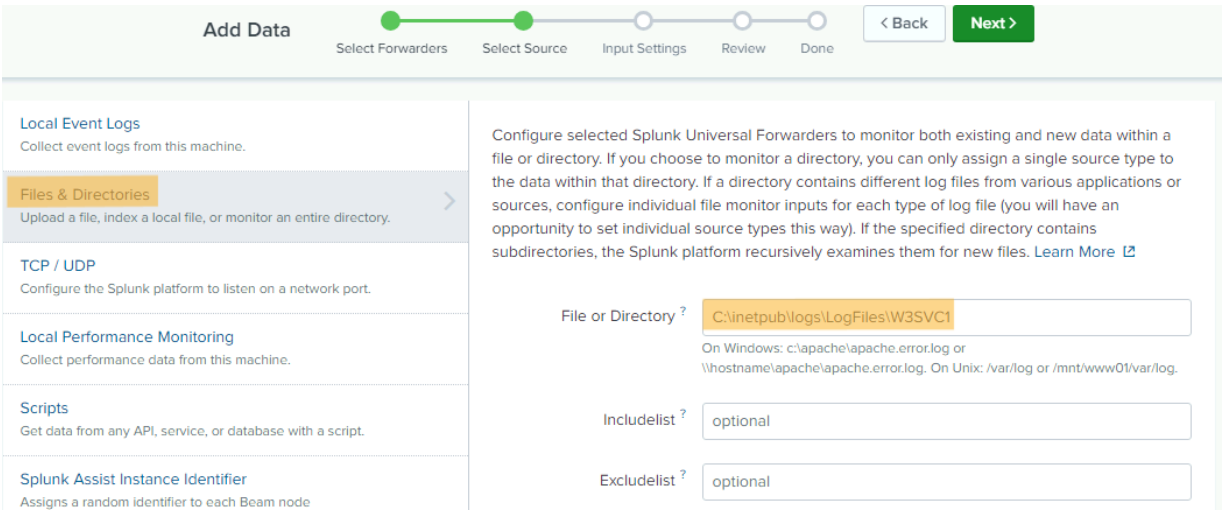
1. Select Forwarders

I am going to select the Web host where the website is being hosted.



2. Select Source

Web logs are placed in the directory C:\inetpub\logs\LogFiles\W3SVC* (* = whichever number it is, in my case it was W3SVC1). This directory usually contains one or more log files which will be continuously updated with the logs. I will be configuring Splunk to monitor and receive logs from this directory.



3. Input Settings

I am going to select the source type for our logs. As my web is hosted on an IIS server, I will choose that source type and create an index for those logs.

Input Settings

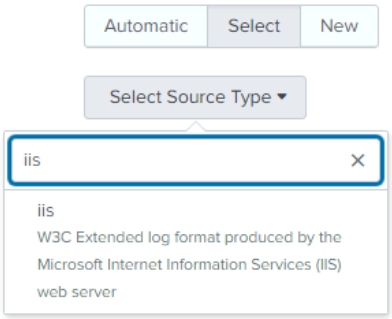
Optionally set additional input parameters for this data input as follows:

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



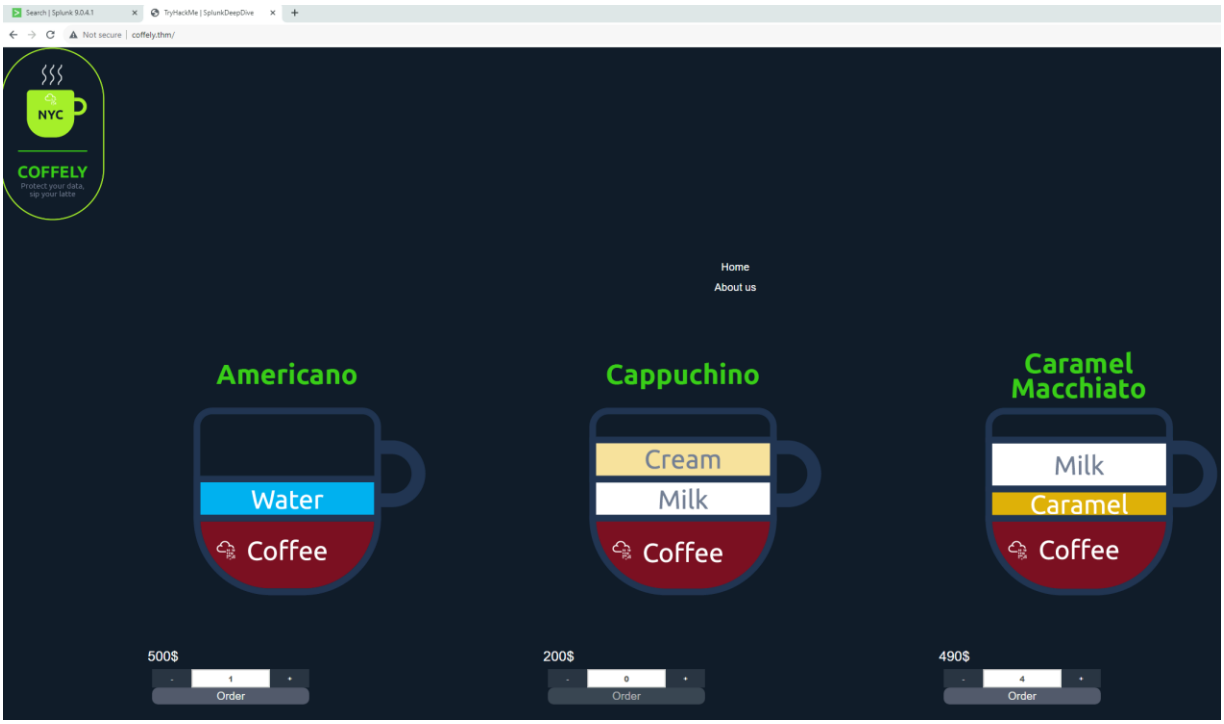
4. Review

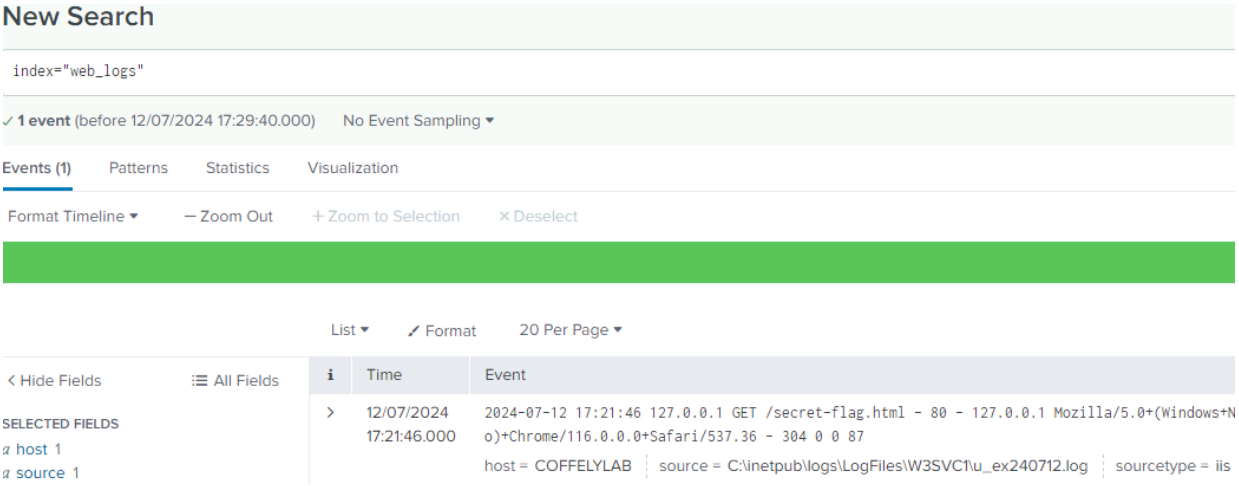
Review

Server Class Name ..... web_logs
List of Forwarders ..... WINDOWS | coffelylab

Input Type ..... File Monitor
Source Path ..... C:\inetpub\logs\LogFiles\W3SVC1
Includelist ..... N/A
Excludelist ..... N/A
Source Type ..... iis
Index ..... win_logs

Logs should start propagating in about 4-5 minutes in the search tab after making a few purchases.



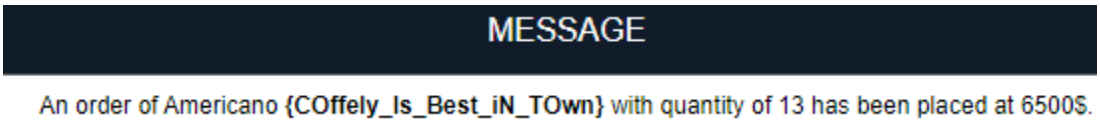


5.

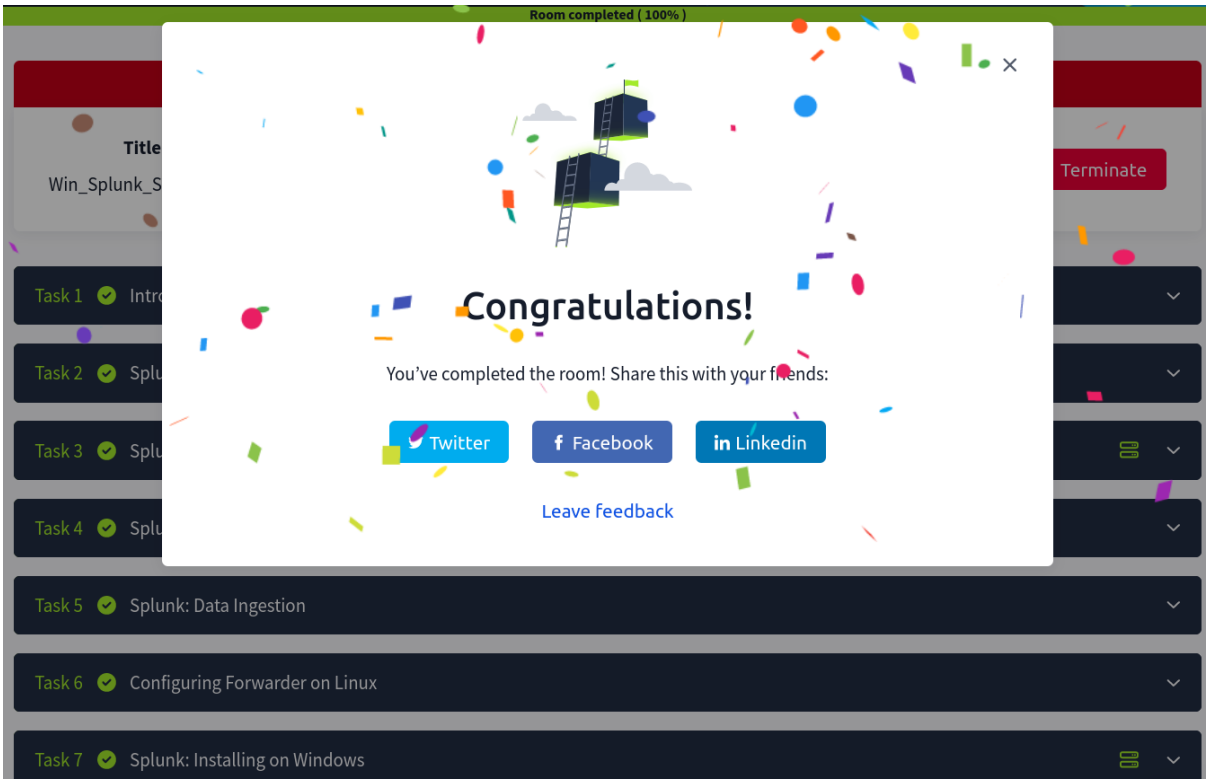
In the lab, visit http://coffely.thm/secret-flag.html; it will display the history logs of the orders made so far. Find the flag in one of the logs.

{COffely_Is_Best_iN_TOwn}

✓ Correct Answer



Inflation?



Reflection

Setting up a SOC Lab using Splunk has provided me with valuable hands-on experience in data ingestion, configuration, and analysis. This project demonstrates my proficiency in using Splunk for cybersecurity and IT operations. By leveraging Splunk's powerful search and visualization capabilities, I was able to gain insights into various data sources and enhance my understanding of data-driven security monitoring.