

Step-by-Step Search VM Installation Guide

This documentation will walk you through installing and setting up **Splunk Enterprise** on the **Index** VM.

Step 1: Downloading Splunk Enterprise

We need to first download the debian file splunk enterprise from their official website:

https://www.splunk.com/en_us/download/splunk-enterprise.html

NOTE: after downloading the .deb file. Do not ssh into the VM but have it's IP address for transfer

>> \$ _____[14 April 2025]

Step 2: copy the .deb from host to index VM

We need to copy the downloaded file from the host (**do not ssh, use the host**) to the VM and we gonna do that using or via ssh. To copy a .deb file (or any file) to your VM using scp, you need the following:

- IP address of the VM
- Username on the VM
- Path to the .deb file on your host machine

Then run the following command to copy the file:

```
scp ~/Downloads/splunk-enterprise.deb search@192.168.122.11:~
```

- Once the copy is done ssh into the VM, navigate to where you copied the file and run the following command to install splunk enterprise debian file:

```
sudo dpkg -i splunk-enterprise.deb
```

```
search@search-node [08:44:38 PM] [~]
-> % sudo dpkg -i splunk-9.4.1-e3bdab203ac8-linux-amd64.deb
[sudo] password for search:
Selecting previously unselected package splunk.
(Reading database ... 126362 files and directories currently installed.)
Preparing to unpack splunk-9.4.1-e3bdab203ac8-linux-amd64.deb ...
no need to run the pre-install check
Unpacking splunk (9.4.1) ...
```

>> \$ _____[14 April 2025]

Step 3: Configure the system to receive log files from the forward system

Before we even go feather we need to accept splunk terms and conditions (Licensing) and great an administrative username and password. Use the following command to accept the licensing agreement:

```
sudo /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 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: mk-mahwete
Password must contain at least:
  * 8 total printable ASCII character(s).
Please enter a new password: 
```

- Set a password you will remember because you gonna need it later on or when you want to login

```
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate
ust be set to "1" for increased security
Done

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

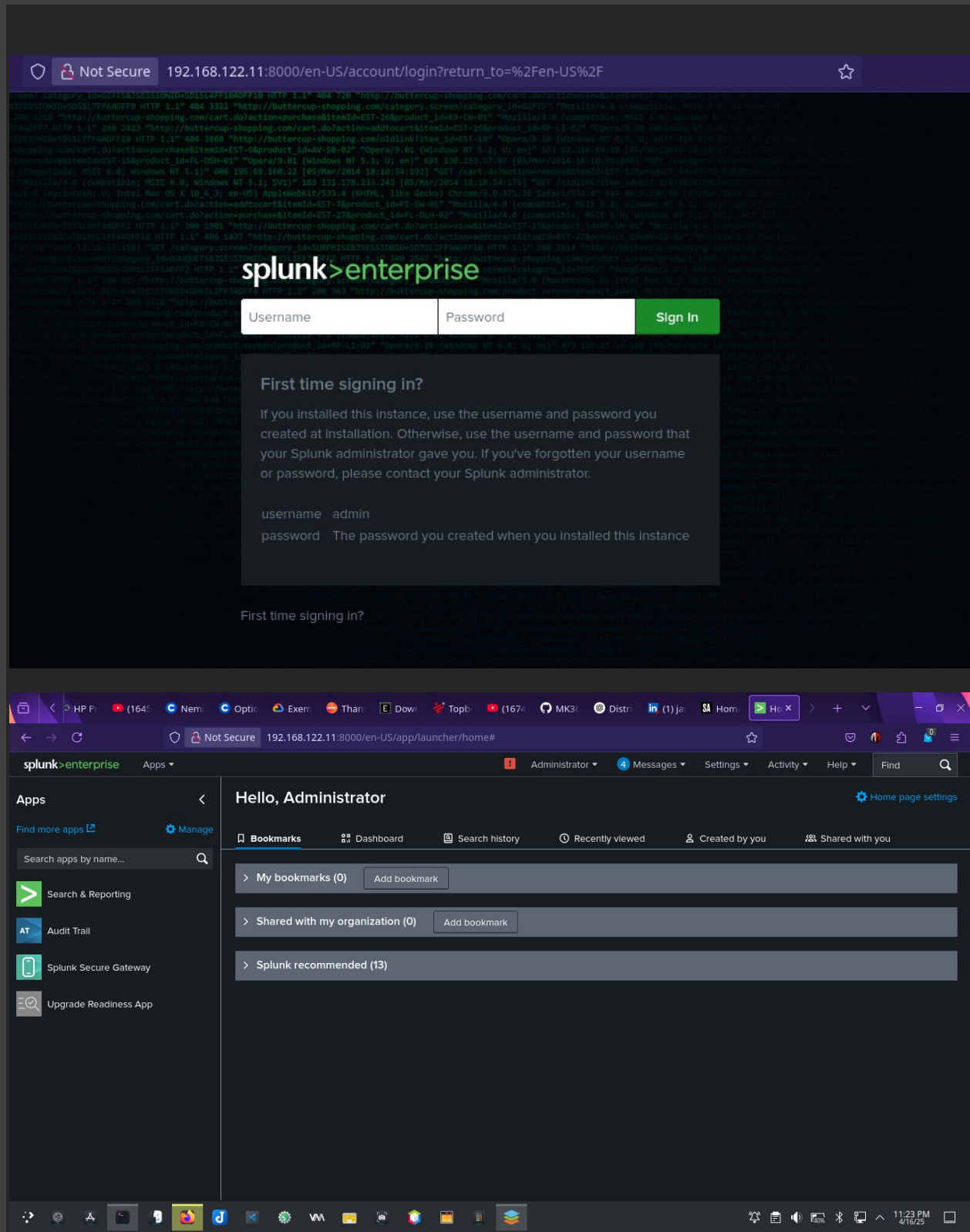
If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://search-node:8000
```

- The installation and configurations is complete and now we have a web interface at [http://search-node](http://search-node:8000)<or your VM IP address>:8000

MK Mahwete

Now get the IP address of the index VM to test if the splunk we interface works: my VM IP is **192.168.122.11:8000** (make sure that port 8000 is open)



- Enable boot start:

```
sudo /opt/splunk/bin/splunk enable boot-start
```

- Add the indexer as a search peer:

```
sudo /opt/splunk/bin/splunk add search-server 192.168.122.10:8089 \
-auth 'mk-mahwete:@LmiCh*aIMk' \
-remoteUsername mk-mahwete \
-remotePassword '@LmiCh*aIMk'

search@search-node [09:55:40 PM] [~]
-> % sudo /opt/splunk/bin/splunk add search-server 192.168.122.10:8089 \
-auth 'mk-mahwete:@LmiCh*aIMk' \
-remoteUsername mk-mahwete \
-remotePassword '@LmiCh*aIMk'

WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf
Peer added
```

NOTE: the index server needs to be online to add the search peers to it. So make sure that the index VM is running.