Step-by-Step Forward VM Installation Guide

This documentation will walk you through installing and setting up **Splunk Universal Forwarder** on the **forward** VM.

Step 1: Downloading Splunk universal forwarder
We need to first download the debian file splunk universal forwarder from their official website: https://www.splunk.com/en_us/download/universal-forwarder.html

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

>> $ [16 April 2025]

Step 2: copy the .deb from host to search 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:

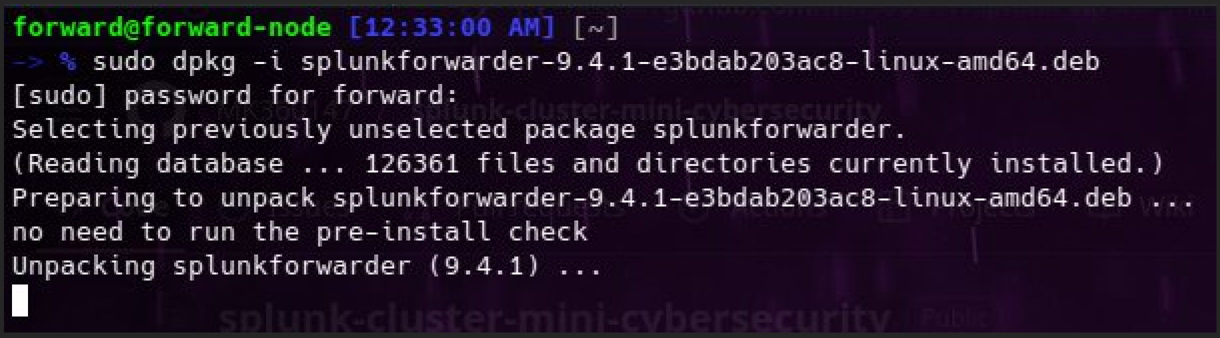
- IP address of the VM
- Username on the VM
- Path to the .deb file on your host machine

Then run the following command to copy the file:

```
scp ~/Downloads/splunk-universal-forwarder.deb search@192.168.122.12:~
```

- 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-universal-forwarder.deb
  ```



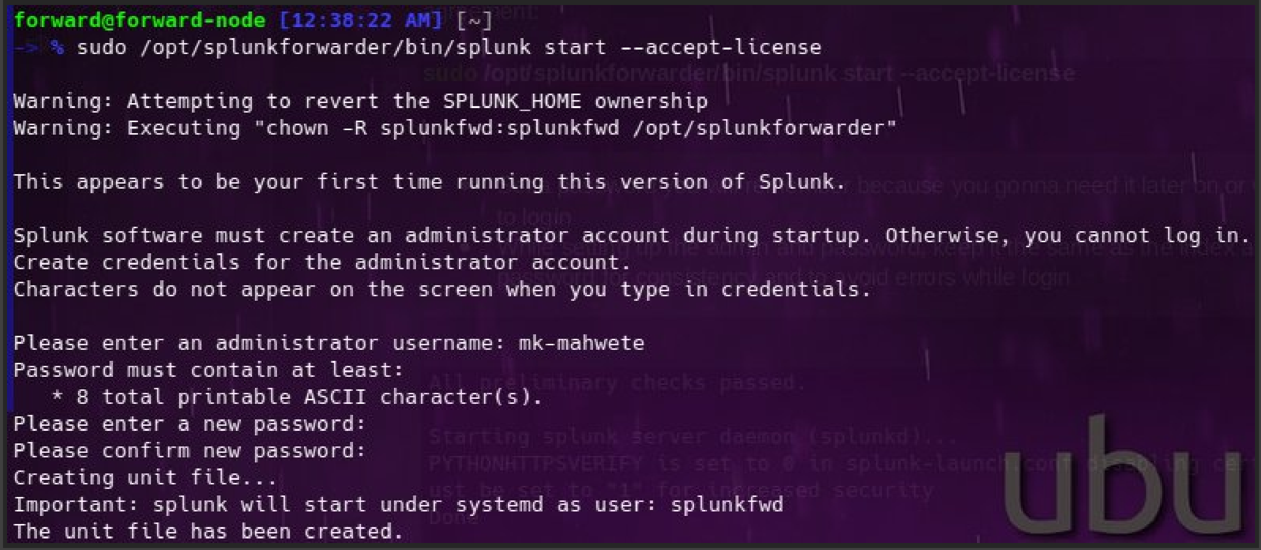
```
forward@forward-node [12:33:00 AM] [~]
-> % sudo dpkg -i splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb
[sudo] password for forward:
Selecting previously unselected package splunkforwarder.
(Reading database ... 126361 files and directories currently installed.)
Preparing to unpack splunkforwarder-9.4.1-e3bdab203ac8-linux-amd64.deb ...
no need to run the pre-install check
Unpacking splunkforwarder (9.4.1) ...
```

>> $ [16 April 2025]

Step 3: Configure the system to retrieve log file from other system (firewall logs, ssh logs $ etc)

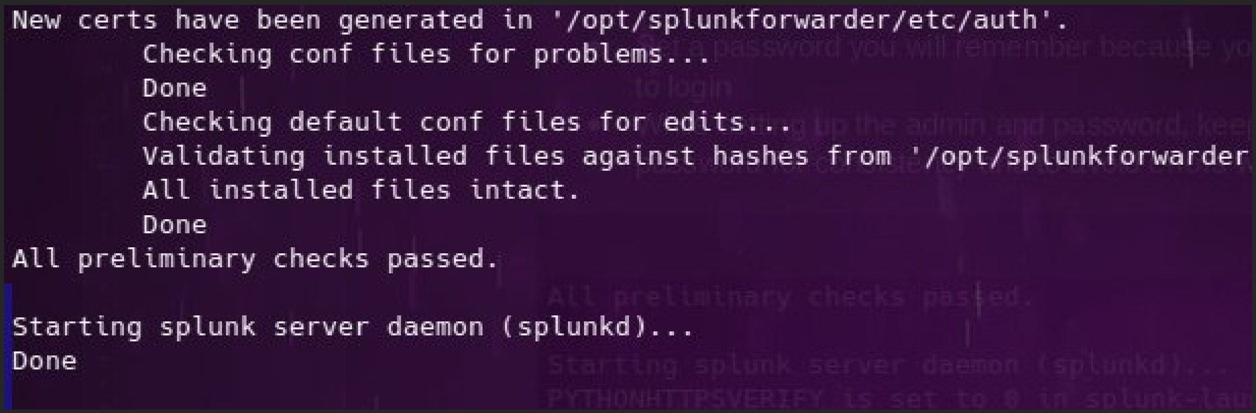
Before we even go feather we need to accept splunk terms and conditions (Licensing) and great an administrative username and password. Use the following command to accept the licensing agreement:

```
sudo /opt/splunkforwarder/bin/splunk start --accept-license
```



```
forward@forward-node [12:38:22 AM] [~]
-> % sudo /opt/splunkforwarder/bin/splunk start --accept-license

Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"

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:
Please confirm new password:
Creating unit file...
Important: splunk will start under systemd as user: splunkfwd
The unit file has been created.
```

- Set a password you will remember because you gonna need it later on or when you want to login
- While setting up the admin and password, keep it the same as the index, search admin & password for consistency and to avoid errors while login



```
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done
```

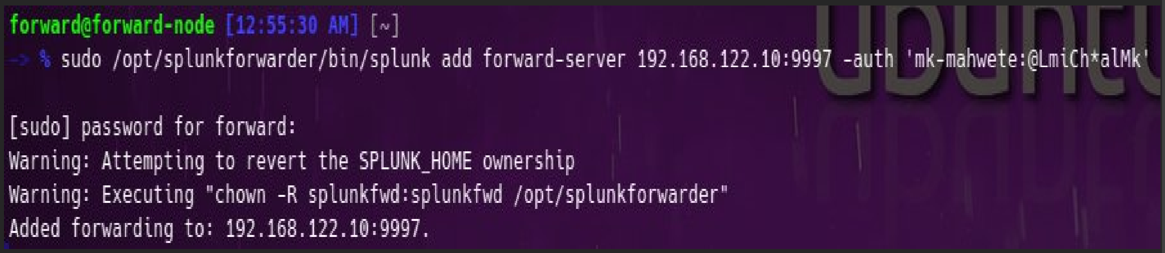
- The installation and configurations is complete and we don't need a web interface for the forwarder because it only take log from other machine and forwards them to index

- Enable boot start:

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

- Forward logs to indexer: index IP <192.168.122.10>

```
sudo /opt/splunkforwarder/bin/splunk add forward-server <indexer-ip>:9997 -auth
‘mk-mahwete:@Lmi*alMK’
```



```
forward@forward-node [12:55:30 AM] [~]
-> % sudo /opt/splunkforwarder/bin/splunk add forward-server 192.168.122.10:9997 -auth 'mk-mahwete:@LmiCh*alMk'

[sudo] password for forward:
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added forwarding to: 192.168.122.10:9997.
```

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

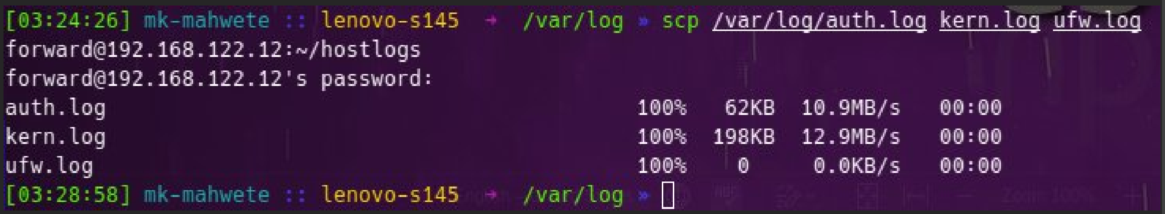
>> $——————————————————————————————————————[16 April 2025]

Step 4: using scp command to Transfer Logs

we will periodically transfer logs from my host to the forwarder and let the forwarder monitor that folder.

- Create a shared folder on your forwarder VM. From the host run:

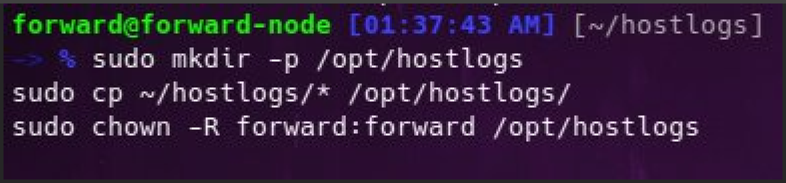
```
scp /var/log/auth.log kern.log ufw.log
forward@192.168.122.12:/home/username/hostlogs/
```



```
[03:24:26] mk-mahwete :: lenovo-s145  →  /var/log » scp /var/log/auth.log kern.log ufw.log
forward@192.168.122.12:~/hostlogs
forward@192.168.122.12's password:
auth.log                                        100%   62KB  10.9MB/s   00:00
kern.log                                        100%  198KB  12.9MB/s   00:00
ufw.log                                         100%    0     0.0KB/s   00:00
[03:28:58] mk-mahwete :: lenovo-s145  →  /var/log »
```

- Make the folder readable by Splunk user and copy log file from home/hostlogs to /opt/hostlogs:

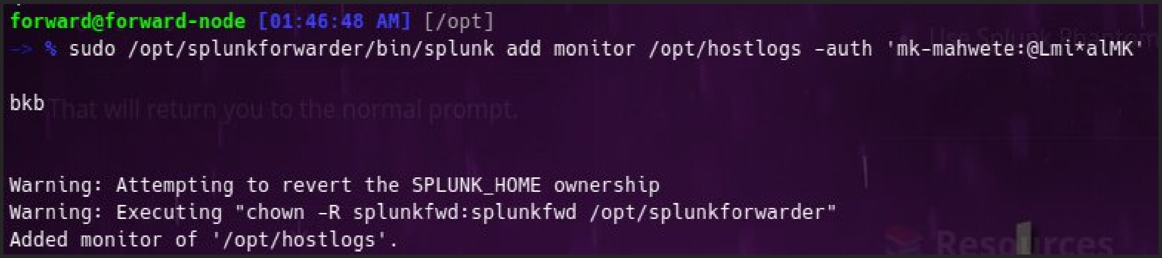
```
sudo mkdir -p /opt/hostlogs
sudo cp /home/forward/hostlogs/* /opt/hostlogs/
sudo chown -R forward:forward /opt/hostlogs
```



```
forward@forward-node [01:37:43 AM] [~/hostlogs]
-> % sudo mkdir -p /opt/hostlogs
sudo cp ~/hostlogs/* /opt/hostlogs/
sudo chown -R forward:forward /opt/hostlogs
```

- On the Forwarder VM, monitor that folder by running this command:

sudo /opt/splunkforwarder/bin/splunk add monitor /opt/hostlogs -auth ‘mk-mahwete:@Lmi*alMK’



```
forward@forward-node [01:46:48 AM] [/opt]
-> % sudo /opt/splunkforwarder/bin/splunk add monitor /opt/hostlogs -auth 'mk-mahwete:@Lmi*alMK'

bkb


Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added monitor of '/opt/hostlogs'.
```

By doing this, now i can simulate logs

NOTE: If you want real-time live collection from the host system, install the Universal Forwarder directly on your host and forward logs to your indexer.