Splunk on Linux Server Installation guide

STEP1

#########
POWER ON YOUR LINUX BOX

STEP 2

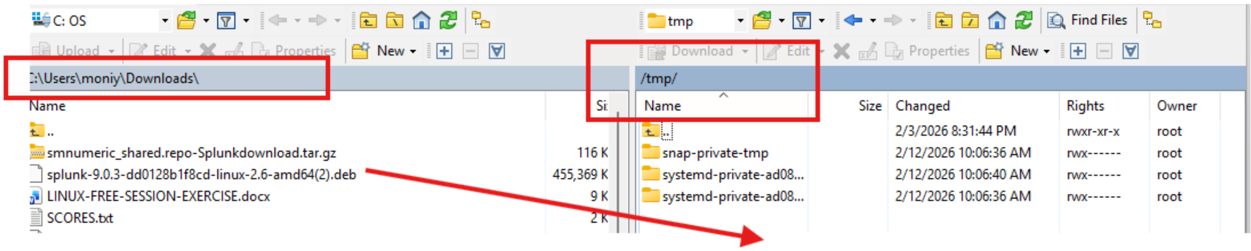
######
Login to your WINSCP

STEP 3

########

A. Edit the destination directory (as shown on the RIGHT-HAND SIDE OF THE SCREENSHOT BELOW) to point to /tmp on your server.

B. Drag and drop the Splunk installation file you downloaded a few days ago to the tmp folder as shown below



:\Users\moniy\Downloads\

Name	Si
..	
smnumeric_shared.repo-Splunkdownload.tar.gz	116 K
splunk-9.0.3-dd0128b1f8cd-linux-2.6-amd64(2).deb	455,369 K
LINUX-FREE-SESSION-EXERCISE.docx	9 K
SCORES.txt	2 K

/tmp/

Name	Size	Changed	Rights	Owner
..		2/3/2026 8:31:44 PM	rwxr-xr-x	root
snap-private-tmp		2/12/2026 10:06:36 AM	rwx------	root
systemd-private-ad08...		2/12/2026 10:06:40 AM	rwx------	root
systemd-private-ad08...		2/12/2026 10:06:36 AM	rwx------	root

STEP 4

########
Login to your linux server via Putty

STEP 5

######

Change your directory to /tmp using the following command

cd /tmp

STEP 6

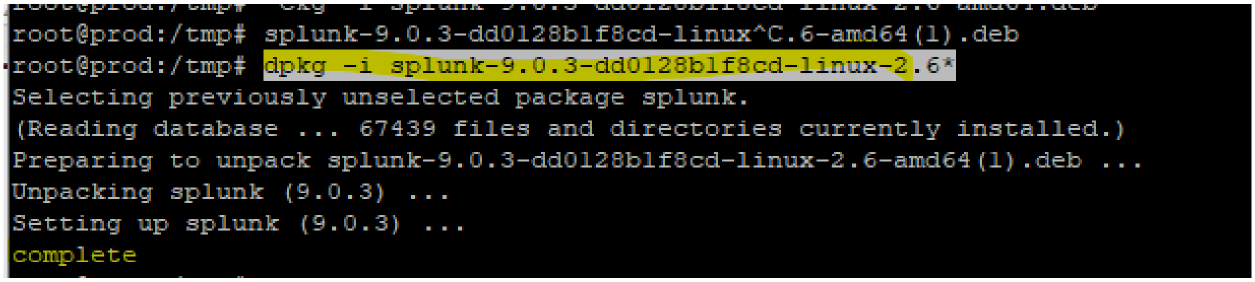
#######
Run the following commands one-after-the-other
ls -ltr (*to confirm your splunk file is already in tmp directory*)

sudo su (to become an admin user)

STEP 7

#######
Install Splunk on your linux server with the following command

dpkg -i splunk-9.0.3-dd0128b1f8cd-linux-2.6*



```
root@prod:/tmp# ckg -i splunk-9.0.3-dd0128b1f8cd-linux-2.6-amd64.deb
root@prod:/tmp# splunk-9.0.3-dd0128b1f8cd-linux^C.6-amd64(1).deb
root@prod:/tmp# dpkg -i splunk-9.0.3-dd0128b1f8cd-linux-2.6*
Selecting previously unselected package splunk.
(Reading database ... 67439 files and directories currently installed.)
Preparing to unpack splunk-9.0.3-dd0128b1f8cd-linux-2.6-amd64(1).deb ...
Unpacking splunk (9.0.3) ...
Setting up splunk (9.0.3) ...
complete
```

STEP 8

########
After it shows complete
Run the following command

whereis splunk (*to show you where the Splunk is installed to)*

STEP 9

########
Run the following command

/opt/splunk/bin/splunk status

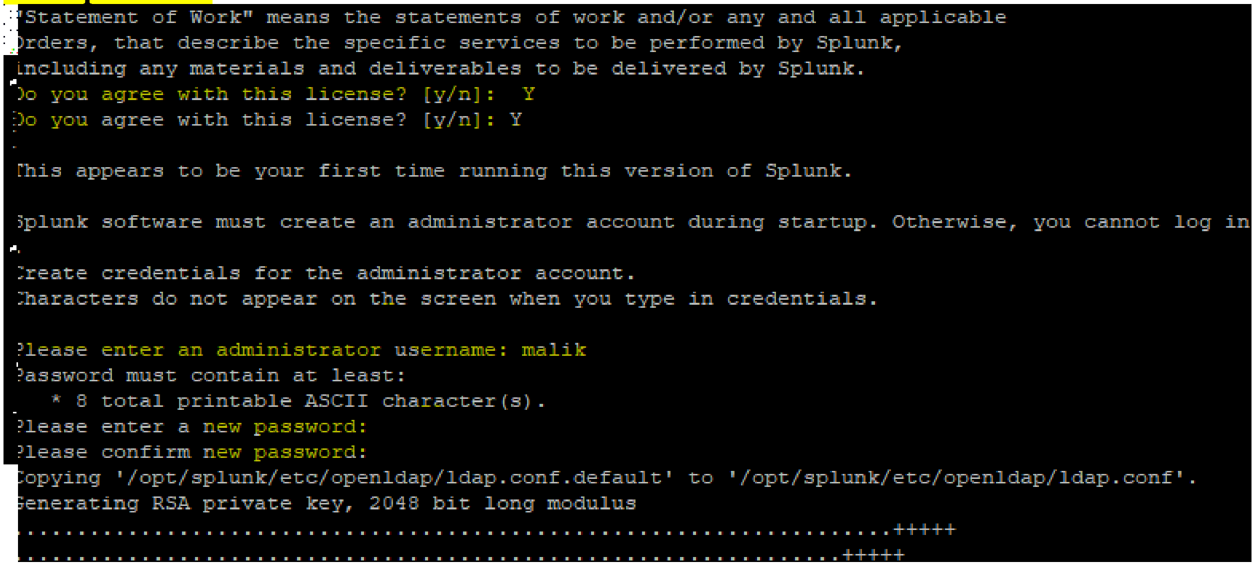
You'll be displayed more → PRESS ENTER ENTER ON YOUR KEYBOARD UNTIL YOU GET TO THE END (You can use your keyboard space bar – that'll take you to the end of the page quicker)

STEP 10

###########

Confirm the license agreement with "y"
Confirm "y" again

Then create an admin user by using any username
Then password



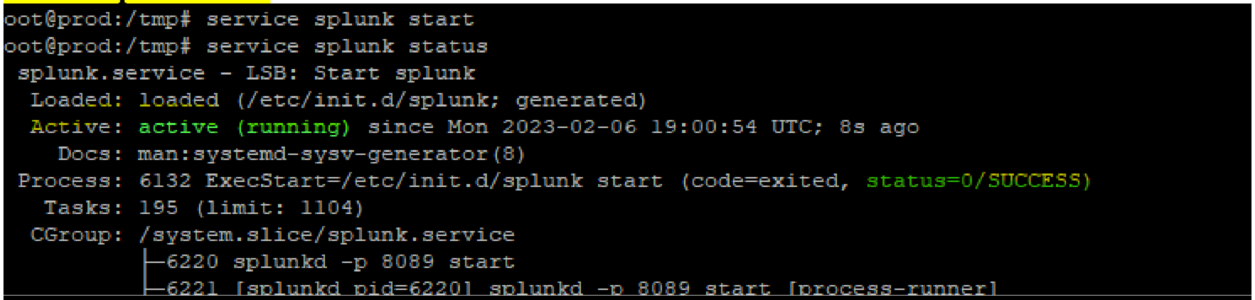
```
"Statement of Work" means the statements of work and/or any and all applicable
Orders, that describe the specific services to be performed by Splunk,
including any materials and deliverables to be delivered by Splunk.
Do you agree with this license? [y/n]:  Y
Do you agree with this license? [y/n]: Y

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: malik
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
.....................................................................+++++
.................................................................+++++
```

STEP 11

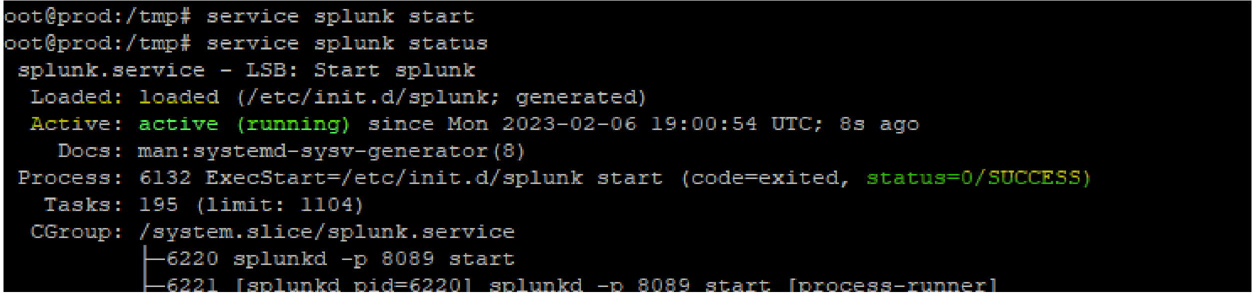
###########
Run the following two commands one-after-the-other to enable boot start and start Splunk

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

service splunk start



```
oot@prod:/tmp# service splunk start
oot@prod:/tmp# service splunk status
 splunk.service - LSB: Start splunk
  Loaded: loaded (/etc/init.d/splunk; generated)
  Active: active (running) since Mon 2023-02-06 19:00:54 UTC; 8s ago
    Docs: man:systemd-sysv-generator(8)
 Process: 6132 ExecStart=/etc/init.d/splunk start (code=exited, status=0/SUCCESS)
   Tasks: 195 (limit: 1104)
  CGroup: /system.slice/splunk.service
          ├─6220 splunkd -p 8089 start
          ├─6221 [splunkd pid=6220] splunkd -p 8089 start [process-runner]
```



```
oot@prod:/tmp# service splunk start
oot@prod:/tmp# service splunk status
 splunk.service - LSB: Start splunk
  Loaded: loaded (/etc/init.d/splunk; generated)
  Active: active (running) since Mon 2023-02-06 19:00:54 UTC; 8s ago
    Docs: man:systemd-sysv-generator(8)
 Process: 6132 ExecStart=/etc/init.d/splunk start (code=exited, status=0/SUCCESS)
   Tasks: 195 (limit: 1104)
  CGroup: /system.slice/splunk.service
          ├─6220 splunkd -p 8089 start
          ├─6221 [splunkd pid=6220] splunkd -p 8089 start [process-runner]
```

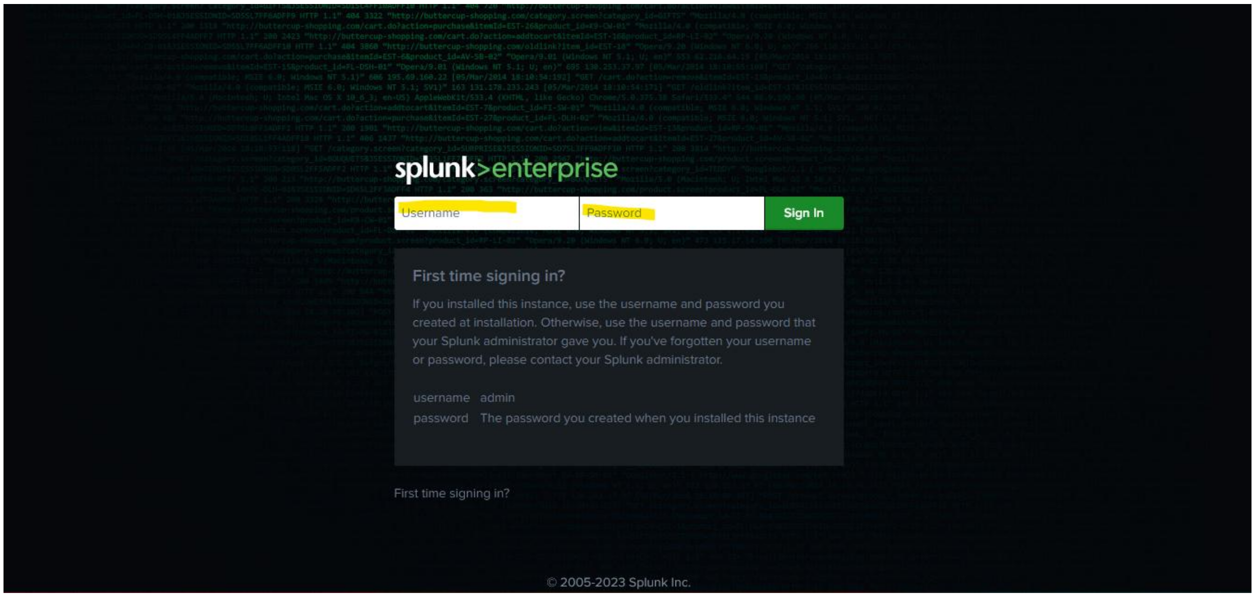
STEP 12

##########
Validate Splunk status with the following command

service splunk status

STEP 13

########
Final Step   Insert your server IP addr with port 8000 on your web browser (for example)
http://192.168.0.16:8000
Then you welcome to Splunk Dashboard (and login to splunk using the admin username and password you created on STEP 10)



First time signing in?

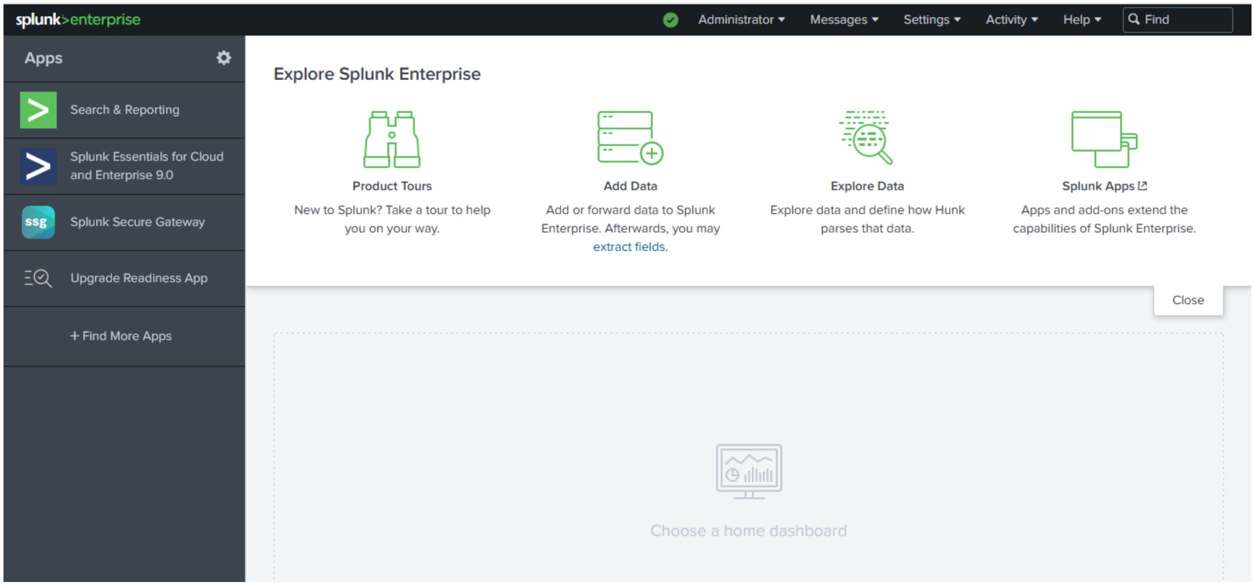
If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.

username admin
password The password you created when you installed this instance

First time signing in?

© 2005-2023 Splunk Inc.

Then login with your created admin username and password



Explore Splunk Enterprise

Product Tours
New to Splunk? Take a tour to help you on your way.

Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Explore Data
Explore data and define how Hunk parses that data.

Splunk Apps
Apps and add-ons extend the capabilities of Splunk Enterprise.