

Splunk

Installation:

Splunk Website, Download and installation page:

[Splunk Enterprise Free Trial | Splunk](https://download.splunk.com/products/splunk/releases/9.3.1/linux/splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.deb)

Ubuntu: `wget -O splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.deb`

`"https://download.splunk.com/products/splunk/releases/9.3.1/linux/splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.deb"`

```
root@ubuntu:/home/ntsapi# wget -O splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.de
b "https://download.splunk.com/products/splunk/releases/9.3.1/linux/splunk-9.3.
1-0b8d769cb912-linux-2.6-amd64.deb"
--2024-10-03 10:02:11-- https://download.splunk.com/products/splunk/releases/9
.3.1/linux/splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 18.239.208.102, 18.239.2
08.7, 18.239.208.39, ...
Connecting to download.splunk.com (download.splunk.com)|18.239.208.102|:443...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 749476896 (715M) [binary/octet-stream]
Saving to: 'splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.deb'

splunk-9.3.1-0b8d76 100%[=====] 714,76M 3,52MB/s in 4m 3s

2024-10-03 10:06:15 (2,95 MB/s) - 'splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.de
b' saved [749476896/749476896]
```

Package:

```
root@ubuntu:/home/ntsapi# dpkg -i splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 362117 files and directories currently installed.)
Preparing to unpack splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.deb ...
configuration error - unknown item 'NONEXISTENT' (notify administrator)
configuration error - unknown item 'NONEXISTENT' (notify administrator)
Unpacking splunk (9.3.1) ...
Setting up splunk (9.3.1) ...
complete
```

Splunk Configuration:

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

```
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: ntsapi
Password must contain at least:
* 8 total printable ASCII character(s).
Please enter a new password:
```

Firewall configuration:

```
root@ubuntu:/home/ntsapi# ufw allow OpenSSH
Rules updated
Rules updated (v6)
root@ubuntu:/home/ntsapi#
```

```
root@ubuntu:/home/ntsapi# sudo ufw allow 8000 # which is the default port for splunk
Rules updated
Rules updated (v6)
```

```
root@ubuntu:/home/ntsapi# ufw enable
Firewall is active and enabled on system startup
root@ubuntu:/home/ntsapi#
```

Start Splunk

```
root@ubuntu:/home/ntsapi# /opt/splunk/bin/splunk start

Splunk> Take the sh out of IT.

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.
  Creating: /opt/splunk/var/lib/splunk
  Creating: /opt/splunk/var/run/splunk
  Creating: /opt/splunk/var/run/splunk/appserver/i18n
  Creating: /opt/splunk/var/run/splunk/appserver/modules/static/css
  Creating: /opt/splunk/var/run/splunk/upload
  Creating: /opt/splunk/var/run/splunk/search_telemetry
  Creating: /opt/splunk/var/run/splunk/search_log
  Creating: /opt/splunk/var/spool/splunk
  Creating: /opt/splunk/var/spool/dirmoncache
  Creating: /opt/splunk/var/lib/splunk/authDb
  Creating: /opt/splunk/var/lib/splunk/hashDb
  Creating: /opt/splunk/var/run/splunk/sessions
New certs have been generated in '/opt/splunk/etc/auth'.
  Checking critical directories... Done
```

After starting it will indicate the port where the server is available, usually port 8000.

Next Step:

Insert you ip and the port number into the URL

← → ↻ 10.0.2.15:8000/en-US/account/login?return_to=%2F

splunk>enterprise

Username Password **Sign In**

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?

Insert your details and sign in:

