Missed capitalising the C here but it worked after that

Screenshot 1 - Terminal output:

```
splunk/etc/system/default/distsearch.conf
splunk/etc/system/default/transforms.conf
splunk/etc/system/default/global-banner.conf
splunk/etc/system/default/health.conf
splunk/etc/system/default/serverclass.conf
splunk/etc/system/default/workflow_actions.conf
splunk/etc/system/default/metric_rollups.conf
splunk/etc/system/local/
splunk/etc/system/local/README
splunk/etc/disabled-apps/
splunk/etc/disabled-apps/README
splunk/etc/deployment-apps/
splunk/etc/deployment-apps/README
splunk/etc/manager-apps/
splunk/etc/manager-apps/_cluster/
splunk/etc/manager-apps/_cluster/default/
splunk/etc/manager-apps/_cluster/default/indexes.conf
splunk/etc/manager-apps/_cluster/local/
splunk/etc/manager-apps/_cluster/local/README
sam@sam-VMware-Virtual-Platform:~/Desktop$ cd opt/splunk/bin
bash: cd: opt/splunk/bin: No such file or directory
sam@sam-VMware-Virtual-Platform:~/Desktop$ cd /opt/splunk/bin
sam@sam-VMware-Virtual-Platform:/opt/splunk/bin$ sudo ./splunk start --accept-li
cense
```


Screenshot 2 - Splunk login page:

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?

© 2005-2025 Splunk Inc.

GitHub - splunk/botsv3: S   +

github.com/splunk/botsv37tab=readme-ov-file   Sign in

README   CC0-1.0 license

Dataset	Description	Size	Format
BOTS V3 Dataset	BOTSv3 dataset.	320.1MB	Pre-indexed Splunk

d7ccca99a01cff070dff3c139cdc10eb

botsv3_data_set.tgz
21m left — 4.2 of 320 MB (287 KB/sec)

Show all downloads

Herrald

timfrazier1 Tim Frazier

Installation

1. Download the dataset file indicated above and check the MD5 hash to ensure integrity.
2. Install Splunk Enterprise and the apps/add-ons listed in the *Required Software* section below. It is important to match the specific version of each app and add-on.
3. Unzip/untar the downloaded file into $SPLUNK_HOME/etc/apps
4. Restart Splunk
5. The BOTS v3 data will be available by searching:

```
index=botsv3 earliest=0
```

6. Note that because the data is distributed in a pre-indexed format, there are no volume-based licensing limits to be concerned with.

Data Sourcetypes included

- access_combined
- alternatives
- amazon-ssm-agent

Files

Home / Downloads / botsv3_data_set

- Recent
- Starred
- Home
- Documents
- Downloads
- Music
- Pictures
- Videos
- Trash
- CDROM
- Floppy Disk
- Ubuntu 24...

bin   default   lookups   var   LICENSE   README.txt

splunk-10.0.2-
e2d18b4767e9-l...

Home

Screenshot 1 — Terminal: root@sam-VMware-Virtual-Platform: /home/sam/Desktop

```
sam@sam-VMware-Virtual-Platform:~/Desktop$ sudo su
[sudo] password for sam:
root@sam-VMware-Virtual-Platform:/home/sam/Desktop#
```

Screenshot 2 — Terminal: root@sam-VMware-Virtual-Platform: /home/sam/Downloads

```
bash: cd: /downloads: No such file or directory
root@sam-VMware-Virtual-Platform:/home/sam/Desktop# ls
splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz
root@sam-VMware-Virtual-Platform:/home/sam/Desktop# cd /Downloads
bash: cd: /Downloads: No such file or directory
root@sam-VMware-Virtual-Platform:/home/sam/Desktop# cccd-
cccd-: command not found
root@sam-VMware-Virtual-Platform:/home/sam/Desktop# cd-
Command 'cd-' not found, did you mean:
  command 'cde' from deb cde (0.1+git9-g551e54d-1.2)
  command 'cdi' from deb cdo (2.3.0-1)
  command 'cdo' from deb cdo (2.3.0-1)
  command 'cdw' from deb cdw (0.8.1-3)
  command 'cd5' from deb cd5 (0.1-4)
  command 'cdp' from deb irpas (0.10-9)
  command 'cdb' from deb tinycdb (0.81-1)
Try: apt install <deb name>
root@sam-VMware-Virtual-Platform:/home/sam/Desktop# cd -
bash: cd: OLDPWD not set
root@sam-VMware-Virtual-Platform:/home/sam/Desktop# cd
root@sam-VMware-Virtual-Platform:~# cd Downloads
bash: cd: Downloads: No such file or directory
root@sam-VMware-Virtual-Platform:~# cd /home/sam/Downloads
root@sam-VMware-Virtual-Platform:/home/sam/Downloads#
```

Dec 8 18:57

root@sam-VMware-Virtual-Platform: /home/sam/Downloads

```
splunk-10.0.2-e2d18b4767e9-linux-amd64.tgz
root@sam-VMware-Virtual-Platform:/home/sam/Desktop# cd /Downloads
bash: cd: /Downloads: No such file or directory
root@sam-VMware-Virtual-Platform:/home/sam/Desktop# cccd-
cccd-: command not found
root@sam-VMware-Virtual-Platform:/home/sam/Desktop# cd-
Command 'cd-' not found, did you mean:
  command 'cde' from deb cde (0.1+git9-g551e54d-1.2)
  command 'cdi' from deb cdo (2.3.0-1)
  command 'cdo' from deb cdo (2.3.0-1)
  command 'cdw' from deb cdw (0.8.1-3)
  command 'cd5' from deb cd5 (0.1-4)
  command 'cdp' from deb irpas (0.10-9)
  command 'cdb' from deb tinycdb (0.81-1)
Try: apt install <deb name>
root@sam-VMware-Virtual-Platform:/home/sam/Desktop# cd -
bash: cd: OLDPWD not set
root@sam-VMware-Virtual-Platform:/home/sam/Desktop# cd
root@sam-VMware-Virtual-Platform:~# cd Downloads
bash: cd: Downloads: No such file or directory
root@sam-VMware-Virtual-Platform:~# cd /home/sam/Downloads
root@sam-VMware-Virtual-Platform:/home/sam/Downloads# cp -r botsv3_data_set /opt
/splunk/etc/apps
root@sam-VMware-Virtual-Platform:/home/sam/Downloads#
```

To direct input to this VM, click inside or press Ctrl+G.

Dec 8 18:58

root@sam-VMware-Virtual-Platform: /opt/splunk/etc/apps

```
root@sam-VMware-Virtual-Platform:~# cd Downloads
bash: cd: Downloads: No such file or directory
root@sam-VMware-Virtual-Platform:~# cd /home/sam/Downloads
root@sam-VMware-Virtual-Platform:/home/sam/Downloads# cp -r botsv3_data_set /opt
/splunk/etc/apps/
root@sam-VMware-Virtual-Platform:/home/sam/Downloads# cd /opt/splunk/etc/apps
root@sam-VMware-Virtual-Platform:/opt/splunk/etc/apps# ls
alert_logevent              splunk-data-management
alert_webhook               SplunkDeploymentServerConfig
appsbrowser                 SplunkForwarder
audit_trail                 splunk_gdi
botsv3_data_set             splunk_httpinput
introspection_generator_addon  splunk_instrumentation
journald_input              splunk_internal_metrics
launcher                    SplunkLightForwarder
learned                     splunk_metrics_workspace
legacy                      splunk_monitoring_console
python_upgrade_readiness_app  splunk_pipeline_builders
sample_app                  splunk_rapid_diag
search                      splunk-rolling-upgrade
splunk_app_for_splunk_o11y_cloud  splunk_secure_gateway
splunk_archiver             splunk-visual-exporter
splunk-dashboard-studio     user-prefs
root@sam-VMware-Virtual-Platform:/opt/splunk/etc/apps#
```

To direct input to this VM, click inside or press Ctrl+G.