

Splunk Practical Implementation: Deployment, Configuration & Real-Time Log Forwarding

Introduction to Splunk

Environment Setup

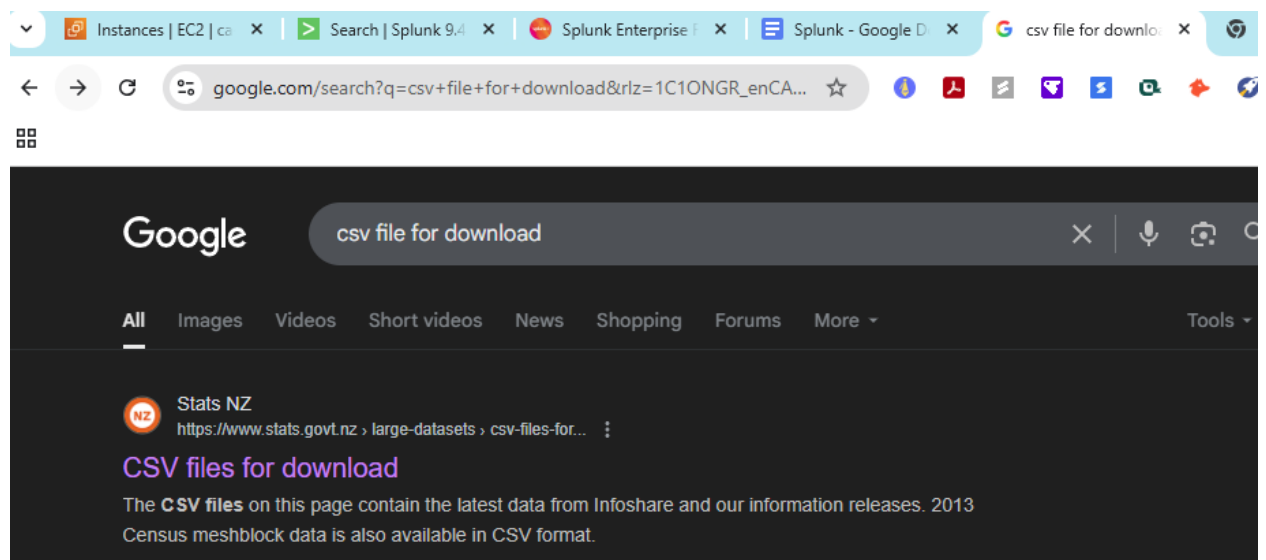
Indexes & Data Onboarding

Dataset Used:

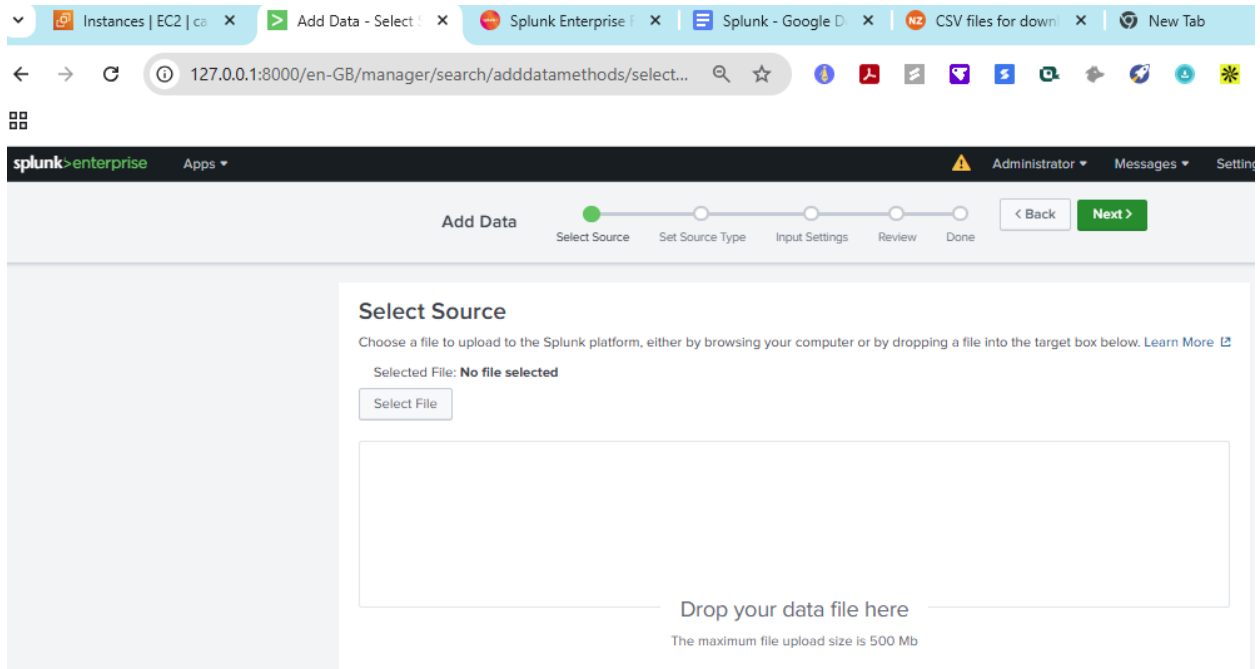
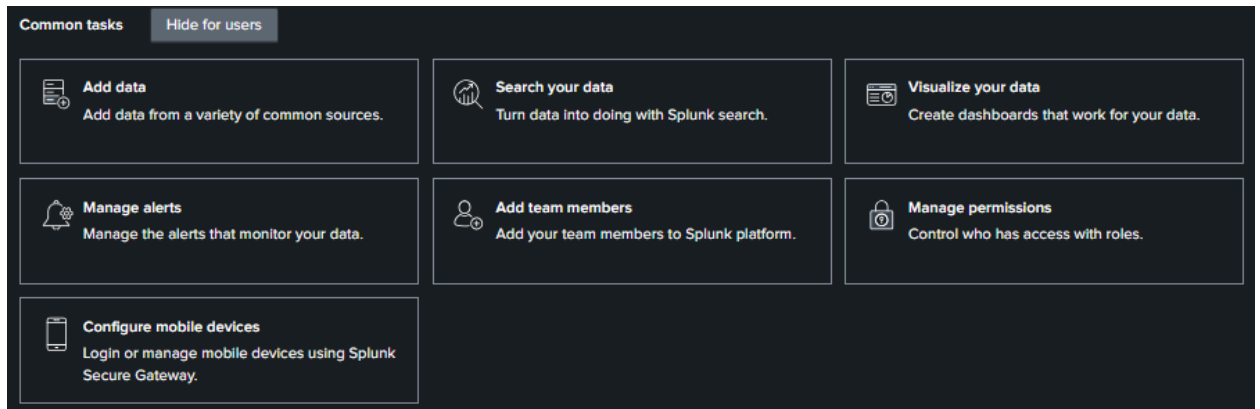
annual-enterprise-survey-2023-financial-year-provisional.csv (sample business dataset used for ingestion)

Steps:

- Access the Splunk Web interface.
- Create a new index.
- Upload and ingest the sample CSV data via GUI or CLI for parsing and indexing.



Sample data from here name: annual-enterprise-survey-2023-financial-year-provisional.csv



The screenshot shows the Splunk Enterprise Search interface. The search bar contains the query: `source="annual-enterprise-survey-2023-financial-year-provisional.csv" host="JONAM" index="pookie" sourcetype="csv"`. The search results show 50,985 events. The interface includes a sidebar with field lists (Selected, Interesting, and Extract New Fields) and a main table of search results.

Time	Event
22/06/2025 13:45:11.000	2013,Level 3,ZZ11,Food product manufacturing,Percentage,H41,Liabilities structure,Financial ratios,46,"ANZSIC06 groups C111, C112, C113, C114, C115, C116, C117, C118, and C119"
22/06/2025 13:45:11.000	2013,Level 3,ZZ11,Food product manufacturing,Percentage,H40,Return on total assets,Financial ratios,5,"ANZSIC06 groups C111, C112, C113, C114, C115, C116, C117, C118, and C119"
22/06/2025 13:45:11.000	2013,Level 3,ZZ11,Food product manufacturing,Percentage,H39,Return on equity,Financial ratios,12,"ANZSIC06 groups C111, C112, C113, C114, C115, C116, C117, C118, and C119"
22/06/2025 13:45:11.000	2013,Level 3,ZZ11,Food product manufacturing,Percentage,H38,Margin on sales of goods for resale,Financial ratios,40,"ANZSIC06 groups C111, C112, C113, C114, C115, C116, C117, C118, and C119"
22/06/2025 13:45:11.000	2013,Level 3,ZZ11,Food product manufacturing,Percentage,H37,Quick ratio,Financial ratios,52,"ANZSIC06 groups C111, C112, C113, C114, C115, C116, C117, C118, and C119"
22/06/2025 13:45:11.000	2013,Level 3,ZZ11,Food product manufacturing,Percentage,H36,Current ratio,Financial ratios,91,"ANZSIC06 groups C111, C112, C113, C114, C115, C116, C117, C118, and C119"
22/06/2025 13:45:11.000	2013,Level 3,ZZ11,Food product manufacturing,Dollars,H35,Surplus per employee count,Financial ratios,"17,780","ANZSIC06 groups C111, C112, C113, C114, C115, C116, C117, C118, and C119"

Universal Forwarder Setup (Real-Time Log Forwarding)

The screenshot shows the Splunk Enterprise Manager interface, specifically the 'Forwarding and receiving' configuration page. The page is divided into two main sections: 'Forward data' and 'Receive data'. The 'Forward data' section includes options for 'Type' (Forwarding defaults, Configure forwarding) and 'Set up forwarding between two or more Splunk instances.' The 'Receive data' section includes options for 'Type' (Configure receiving) and 'Configure this instance to receive data forwarded from other instances.'

On the right side of the page, there is a 'Search settings...' search bar and a list of settings categories:

- KNOWLEDGE**
 - Searches, reports, and alerts
 - Data models
 - Event types
 - Tags
 - Fields
 - Lookups
 - User interface
 - Alert actions
 - Advanced search
 - All configurations
- DATA**
 - Data inputs
 - Forwarding and receiving
 - Indexes
 - Report acceleration summaries
 - Source types
 - Ingest actions
- DISTRIBUTED ENVIRONMENT**
 - Forwarder management
 - Indexer clustering
 - Federation
 - Distributed search
- SYSTEM**
 - Server settings
 - Server controls
 - Health report manager
 - Instrumentation
 - Licensing
 - Workload management
 - Mobile settings
- USERS AND AUTHENTICATION**
 - Roles
 - Users
 - Tokens
 - Password management
 - Authentication methods

Home Settings | Splunk Splunk - Google Instances | EC2 EC2 Instance Conn Splunk Enterprise

127.0.0.1:8000/en-GB/manager/launcher/data/inputs/tcp/cook...

splunk enterprise Apps Administrator Messages Settings Activity Help Find

Receive data

Forwarding and receiving > Receive data

Successfully saved "9997".

Showing 1-1 of 1 item

filter 25 per page

Listen on this port	Status	Actions
9997	Enabled Disable	Delete

Home Settings | Splunk Splunk - Google Instances | EC2 EC2 Instance Conn Splunk Enterprise

ca-central-1.console.aws.amazon.com/ec2/home?region=ca-central-...

aws Search [Alt+S] Canada (Central) Manoj%20Khadka

EC2

EC2 > Instances

EC2

Dashboard
EC2 Global View
Events

Instances

Instance Types
Launch Templates

Instances (2)

Last updated less than a minute ago

Connect Instance state Actions Launch instances

Find Instance by attribute or tag (case-sensitive)

Instance state: running Clear filters

All states

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
spunky	i-09bc4848d93e0e510	Running	t2.medium	2/2 checks passed	View alarms +
agent	i-075089f8e51b32d67	Running	t2.medium	Initializing	View alarms +

Splunk Universal Forwarder 9.4.3

Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

Choose Your Installation Package

Windows Linux Mac OS Free BSD Solaris AIX

Architecture	Kernel/Platform	Package Format	Size	Download Now	Copy wget link	More
PPCLE	4.x+, or 5.x+ kernel Linux distributions	.rpm	32.47 MB	Download Now	Copy wget link	More
		.tgz	32.6 MB	Download Now	Copy wget link	More
ARM	4.14+, 5.4+ kernel Linux distributions with libc v2.21+, 6.x+ kernel, Graviton+ Servers 64-bit	.deb	52.17 MB	Download Now	Copy wget link	More
		.rpm	84.76 MB	Download Now	Copy wget link	More
		.tgz	75.01 MB	Download Now	Copy wget link	More
64-bit	4.x+, 5.x+, 6.x+ kernel Linux distributions	.rpm	97.21 MB	Download Now	Copy wget link	More
		.deb	64.56 MB	Download Now	Copy wget link	More
		.tgz	84.92 MB	Download Now	Copy wget link	More

By continuing to use our website, you acknowledge the use of cookies. [Privacy Statement](#) [Change Settings](#)

Copied the command to Clipboard. Click here to select the entire command.

```
wget -O splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb "https://download.splunk.com/products/universalforwarder/releases/9.4.3/linux/enl"
```

Now connect to your new instance agent then install universal forwarder in ubuntu

Steps on Ubuntu Instance (Forwarder):

Install Splunk Universal Forwarder: `cd /opt`

Start the forwarder: `/opt/splunkforwarder/bin/splunk start --accept-license`

Navigate to log directory: `cd /var/log`

Configure inputs.conf and outputs.conf:

inputs.conf (Add file inputs):

```
[monitor:///var/log]
```

```
disabled = false
```

outputs.conf (Forward logs to Splunk indexer):

```
[tcpout]
```

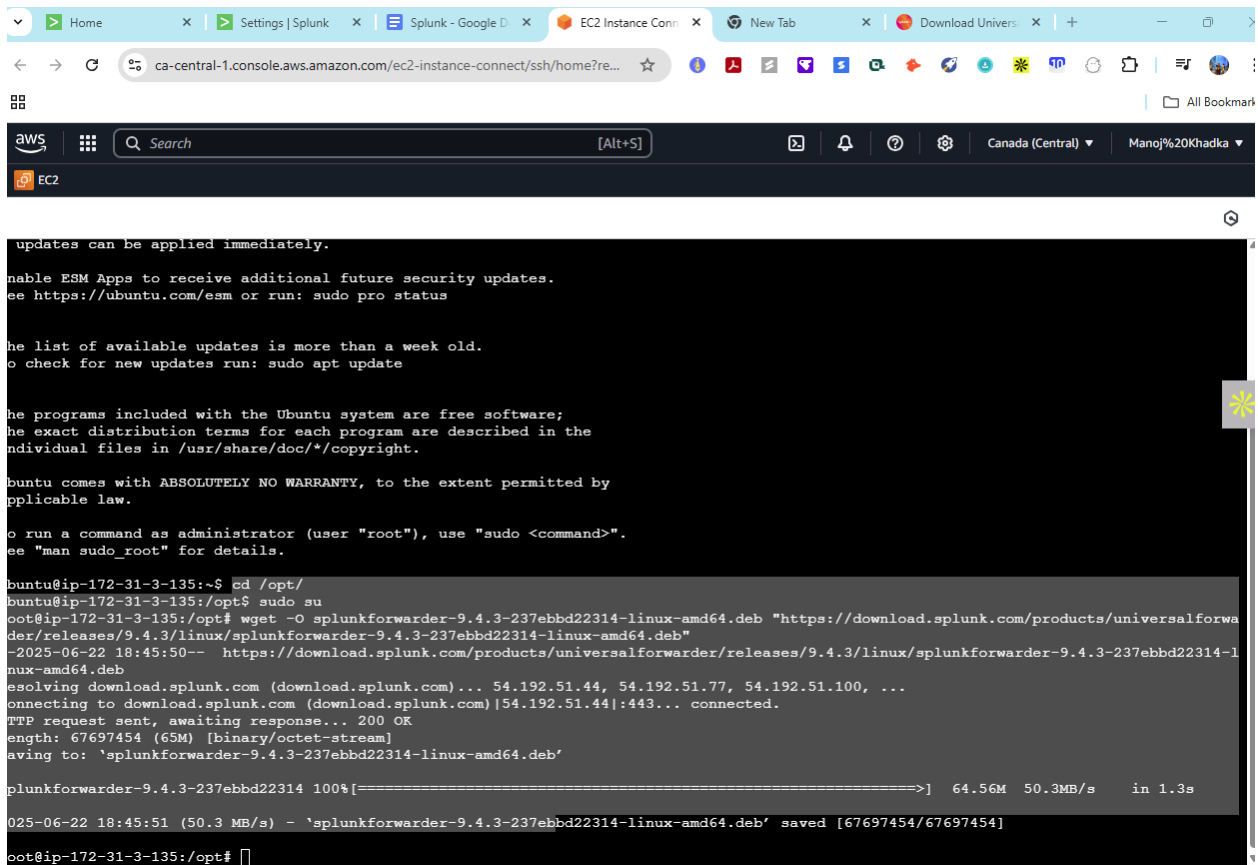
```
defaultGroup = pookie
```

[tcpout:my_indexers]
server = 35.182.180.109:9997

[tcpout-server://35.182.180.109:9997]

Save configurations:

- Press ESC, type :wq, and press Enter to save vi.



```
updates can be applied immediately.

enable ESM Apps to receive additional future security updates.
see https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
to check for new updates run: sudo apt update

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

to run a command as administrator (user "root"), use "sudo <command>".
see "man sudo_root" for details.

buntu@ip-172-31-3-135:~$ cd /opt/
buntu@ip-172-31-3-135:/opt$ sudo su
root@ip-172-31-3-135:/opt# wget -O splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb "https://download.splunk.com/products/universalforwarder/releases/9.4.3/linux/splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb"
--2025-06-22 18:45:50-- https://download.splunk.com/products/universalforwarder/releases/9.4.3/linux/splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 54.192.51.44, 54.192.51.77, 54.192.51.100, ...
Connecting to download.splunk.com (download.splunk.com)[54.192.51.44]:443... connected.
HTTP request sent, awaiting response... 200 OK
Content-Length: 67697454 (65M) [binary/octet-stream]
Saving to: 'splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb'

splunkforwarder-9.4.3-237ebbd22314 100%[=====>] 64.56M 50.3MB/s in 1.3s

2025-06-22 18:45:51 (50.3 MB/s) - 'splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb' saved [67697454/67697454]

root@ip-172-31-3-135:/opt#
```

```

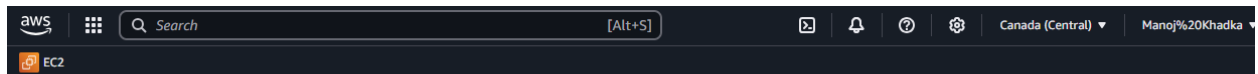
root@ip-172-31-3-135:~$ cd /opt/
root@ip-172-31-3-135:/opt$ sudo su
root@ip-172-31-3-135:/opt# wget -O splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb "https://download.splunk.com/products/universalfor
rder/releases/9.4.3/linux/splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb"
--2025-06-22 18:45:50-- https://download.splunk.com/products/universalforwarder/releases/9.4.3/linux/splunkforwarder-9.4.3-237ebbd22314-l
inux-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 54.192.51.44, 54.192.51.77, 54.192.51.100, ...
Connecting to download.splunk.com (download.splunk.com)|54.192.51.44|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 67697454 (65M) [binary/octet-stream]
Saving to: 'splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb'

splunkforwarder-9.4.3-237ebbd22314 100%[=====>] 64.56M 50.3MB/s in 1.3s

2025-06-22 18:45:51 (50.3 MB/s) - 'splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb' saved [67697454/67697454]

root@ip-172-31-3-135:/opt# ls
splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb
root@ip-172-31-3-135:/opt# dpkg -i splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb
Selecting previously unselected package splunkforwarder.
(Reading database ... 70681 files and directories currently installed.)
Preparing to unpack splunkforwarder-9.4.3-237ebbd22314-linux-amd64.deb ...
no need to run the pre-install check
Unpacking splunkforwarder (9.4.3) ...
Setting up splunkforwarder (9.4.3) ...
find: '/opt/splunkforwarder/lib/python3.7/site-packages': No such file or directory
find: '/opt/splunkforwarder/lib/python3.9/site-packages': No such file or directory
complete
root@ip-172-31-3-135:/opt# cd splunkforwarder/bin
root@ip-172-31-3-135:/opt/splunkforwarder/bin# ./splunk start --accept-licence --answer-yes

```



```

Checking default conf files for edits...
Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.4.3-237ebbd22314-linux-amd64-manifest'
All installed files intact.
Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

root@ip-172-31-3-135:/opt/splunkforwarder/bin# cd /var/log
root@ip-172-31-3-135:/var/log# ls -la
total 496
drwxrwxr-x 11 root    syslog      4096 Jun 22 18:38 .
drwxr-xr-x 13 root    root        4096 Jun 22 18:38 ..
lrwxrwxrwx 1 root    root         39 Jun 10 10:00 README -> ../../usr/share/doc/systemd/README.logs
-rw-r--r-- 1 root    root         444 Jun 10 10:03 alternatives.log
lrwx----- 3 root    root         4096 Jun 22 18:38 amazon
-rw-r----- 1 root    adm          0 Jun 22 18:38 apport.log
lrwxr-xr-x 2 root    root         4096 Jun 10 10:07 apt
-rw-r----- 1 syslog  adm         5118 Jun 22 18:47 auth.log
-rw-rw---- 1 root    utmp          0 Jun 10 10:02 btmp
lrwxr-xr-x 2 _chrony _chrony      4096 Jun 22 18:38 chrony
-rw-r----- 1 root    adm         4322 Jun 22 18:38 cloud-init-output.log
-rw-r----- 1 syslog  adm       131583 Jun 22 18:38 cloud-init.log
lrwxr-xr-x 2 root    root         4096 Jan 31 17:11 dist-upgrade
-rw-r----- 1 root    adm         47388 Jun 22 18:38 dmesg
-rw-r--r-- 1 root    root        37664 Jun 22 18:47 dpkg.log
lrwxr-sr-x+ 3 root    systemd-journal 4096 Jun 22 18:38 journal
-rw-r----- 1 syslog  adm       59588 Jun 22 18:38 kern.log
lrwxr-xr-x 2 landscape landscape 4096 Jun 22 18:43 landscape
-rw-rw-r-- 1 root    utmp       292292 Jun 22 18:43 lastlog
lrwx----- 2 root    root         4096 Jun 22 18:38 private
-rw-r----- 1 syslog  adm       141637 Jun 22 18:50 syslog
lrwxr-xr-x 2 root    root         4096 Jun 22 18:38 sysstat
lrwxr-xr-x 2 root    adm         4096 Jun 22 18:38 unattended-upgrades
-rw-rw-r-- 1 root    utmp         2688 Jun 22 18:43 wtmp
root@ip-172-31-3-135:/var/log#

```

```
root@ip-172-31-3-135:/opt/splunkforwarder/bin# cd /var/log
root@ip-172-31-3-135:/var/log# ls -la
total 496
drwxrwxr-x 11 root    syslog      4096 Jun 22 18:38 .
drwxr-xr-x 13 root    root        4096 Jun 22 18:38 ..
lrwxrwxrwx 1 root    root         39 Jun 10 10:00 README -> ../../usr/share/doc/systemd/README.logs
-rw-r--r-- 1 root    root         444 Jun 10 10:03 alternatives.log
drwx----- 3 root    root        4096 Jun 22 18:38 amazon
-rw-r----- 1 root    adm          0 Jun 22 18:38 apport.log
drwxr-xr-x 2 root    root        4096 Jun 10 10:07 apt
-rw-r----- 1 syslog  adm         5118 Jun 22 18:47 auth.log
-rw-rw---- 1 root    utmp          0 Jun 10 10:02 bttmp
drwxr-x--- 2 _chrony _chrony     4096 Jun 22 18:38 chrony
-rw-r----- 1 root    adm         4322 Jun 22 18:38 cloud-init-output.log
-rw-r----- 1 syslog  adm       131583 Jun 22 18:38 cloud-init.log
drwxr-xr-x 2 root    root        4096 Jan 31 17:11 dist-upgrade
-rw-r----- 1 root    adm         47388 Jun 22 18:38 dmesg
-rw-r--r-- 1 root    root        37664 Jun 22 18:47 dpkg.log
drwxr-xr-x+ 3 root    systemd-journal 4096 Jun 22 18:38 journal
-rw-r----- 1 syslog  adm        59588 Jun 22 18:38 kern.log
drwxr-xr-x 2 landscape landscape  4096 Jun 22 18:43 landscape
-rw-rw-r-- 1 root    utmp       292292 Jun 22 18:43 lastlog
drwx----- 2 root    root        4096 Jun 22 18:38 private
-rw-r----- 1 syslog  adm       141637 Jun 22 18:50 syslog
drwxr-xr-x 2 root    root        4096 Jun 22 18:38 sysstat
drwxr-x--- 2 root    adm         4096 Jun 22 18:38 unattended-upgrades
-rw-rw-r-- 1 root    utmp        2688 Jun 22 18:43 wtmp
root@ip-172-31-3-135:/var/log# cd /opt/splunkforwarder/etc/system/local
root@ip-172-31-3-135:/opt/splunkforwarder/etc/system/local# vi inputs.conf
```

```
monitor:///var/log/syslog]
isable = 0
index = pookie
```

wc


```
ooot@ip-172-31-3-135:/var/log# ls -la
total 496
-rwxr-xr-x 11 root    syslog      4096 Jun 22 18:38 .
-rwxr-xr-x 13 root    root        4096 Jun 22 18:38 ..
-rwxr-xr-x 1 root    root        39 Jun 10 10:00 README -> ../../usr/share/doc/systemd/README.logs
-rw-r--r-- 1 root    root        444 Jun 10 10:03 alternatives.log
-rwx----- 3 root    root        4096 Jun 22 18:38 amazon
-rw-r----- 1 root    adm         0 Jun 22 18:38 apport.log
-rwxr-xr-x 2 root    root        4096 Jun 10 10:07 apt
-rw-r----- 1 syslog  adm        5118 Jun 22 18:47 auth.log
-rw-rw---- 1 root    utmp         0 Jun 10 10:02 btmp
-rwxr-xr-x 2 _chrony  _chrony     4096 Jun 22 18:38 chrony
-rw-r----- 1 root    adm        4322 Jun 22 18:38 cloud-init-output.log
-rw-r----- 1 syslog  adm       131583 Jun 22 18:38 cloud-init.log
-rwxr-xr-x 2 root    root        4096 Jan 31 17:11 dist-upgrade
-rw-r----- 1 root    adm       47388 Jun 22 18:38 dmesg
-rw-r--r-- 1 root    root       37664 Jun 22 18:47 dpkg.log
-rwxr-sr-x+ 3 root    systemd-journal 4096 Jun 22 18:38 journal
-rw-r----- 1 syslog  adm       59588 Jun 22 18:38 kern.log
-rwxr-xr-x 2 landscape landscape 4096 Jun 22 18:43 landscape
-rw-rw-r-- 1 root    utmp       292292 Jun 22 18:43 lastlog
-rwx----- 2 root    root        4096 Jun 22 18:38 private
-rw-r----- 1 syslog  adm      141637 Jun 22 18:50 syslog
-rwxr-xr-x 2 root    root        4096 Jun 22 18:38 sysstat
-rwxr-xr-x 2 root    adm        4096 Jun 22 18:38 unattended-upgrades
-rw-rw-r-- 1 root    utmp        2688 Jun 22 18:43 wtmp
ooot@ip-172-31-3-135:/var/log# cd /opt/splunkforwarder/etc/system/local
ooot@ip-172-31-3-135:/opt/splunkforwarder/etc/system/local# vi inputs.conf
ooot@ip-172-31-3-135:/opt/splunkforwarder/etc/system/local# vi outputs.conf
ooot@ip-172-31-3-135:/opt/splunkforwarder/etc/system/local# cd /opt/splunkforwarder/bin/
ooot@ip-172-31-3-135:/opt/splunkforwarder/bin# ./splunk restart
arning: Attempting to revert the SPLUNK_HOME ownership
arning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
topping splunkd...
utting down. Please wait, as this may take a few minutes.

topping splunk helpers...

one.
plunkd.pid doesn't exist...

plunk> Winning the War on Error

hecking prerequisites...
Checking mgmt port [8089]: open
```

The screenshot displays the Splunk Enterprise web interface. At the top, there's a navigation bar with tabs for Home, Search | Splunk, and other browser tabs. The main header shows 'splunk>enterprise' and various user options like Administrator, Messages, Settings, Activity, Help, and Find. Below this, a 'New Search' section shows the search query 'Index=pookie' and a 'Search & Reporting' button. The search results indicate 50,985 events for the time range 22/06/2025 00:00:00.000 to 22/06/2025 15:21:22.000. The interface includes a sidebar with 'SELECTED FIELDS' and 'INTERESTING FIELDS', a main table of search results, and a top navigation bar.

i	Time	Event
>	22/06/2025 13:45:11.000	2013,Level 3,ZZ11,Food product manufacturing,Percentage,H41,Liabilities structure,Financial ratios,46,"ANZSIC06 groups C111, C112, C113, C114, C115, C116, C117, C118, and C119" host = JONAM source = annual-enterprise-survey-2023-financial-year-provisional.csv sourcetype = csv
>	22/06/2025 13:45:11.000	2013,Level 3,ZZ11,Food product manufacturing,Percentage,H40,Return on total assets,Financial ratios,5,"ANZSIC06 groups C111, C112, C113, C114, C115, C116, C117, C118, and C119" host = JONAM source = annual-enterprise-survey-2023-financial-year-provisional.csv sourcetype = csv
>	22/06/2025 13:45:11.000	2013,Level 3,ZZ11,Food product manufacturing,Percentage,H39,Return on equity,Financial ratios,12,"ANZSIC06 groups C111, C112, C113, C114, C115, C116, C117, C118, and C119" host = JONAM source = annual-enterprise-survey-2023-financial-year-provisional.csv sourcetype = csv
>	22/06/2025 13:45:11.000	2013,Level 3,ZZ11,Food product manufacturing,Percentage,H38,Margin on sales of goods for resale,Financial ratios,40,"ANZSIC06 groups C111, C112, C113, C114, C115, C116, C117, C118, and C119" host = JONAM source = annual-enterprise-survey-2023-financial-year-provisional.csv sourcetype = csv
>	22/06/2025 13:45:11.000	2013,Level 3,ZZ11,Food product manufacturing,Percentage,H37,Quick ratio,Financial ratios,52,"ANZSIC06 groups C111, C112, C113, C114, C115, C116, C117, C118, and C119" host = JONAM source = annual-enterprise-survey-2023-financial-year-provisional.csv sourcetype = csv
>	22/06/2025 13:45:11.000	2013,Level 3,ZZ11,Food product manufacturing,Percentage,H36,Current ratio,Financial ratios,91,"ANZSIC06 groups C111, C112, C113, C114, C115, C116, C117, C118, and C119" host = JONAM source = annual-enterprise-survey-2023-financial-year-provisional.csv sourcetype = csv
>	22/06/2025 13:45:11.000	2013,Level 3,ZZ11,Food product manufacturing,Dollars,H35,Surplus per employee count,Financial ratios,"17,780",ANZSIC06 groups C111, C112, C113, C114, C115, C116, C117, C118, and C119" host = JONAM source = annual-enterprise-survey-2023-financial-year-provisional.csv sourcetype = csv

Outcome

- Splunk Enterprise successfully installed on AWS EC2 instance.
- Sample dataset ingested and analyzed using SPL.
- Real-time Ubuntu logs forwarded to Splunk via Universal Forwarder.