

SPLUNK

Splunk is a strong tool used for analyzing data, especially in cybersecurity. It helps organizations gather, organize, and analyze log data from different sources. With its powerful features, it lets users quickly solve problems by providing complete insights and analytics.

/opt/splunk/bin/splunk start

```
root@Ubuntu:/home/vboxuser# /opt/splunk/bin/splunk start
The splunk daemon (splunkd) is already running.

A Waiting for web server at http://127.0.0.1:8000 to be available..... Done

? If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

> The Splunk web interface is at http://Ubuntu:8000

root@Ubuntu:/home/vboxuser#
```

Splunk overview and dashboard

The screenshot shows the Splunk Enterprise dashboard. At the top, there's a navigation bar with icons for Home, Apps, and various system status indicators. The main content area starts with a greeting "Hello, Administrator". Below this is a section titled "Common tasks" containing six cards:

- Add data: Add data from a variety of common sources.
- Search your data: Turn data into doing with Splunk search.
- Visualize your data: Create dashboards that work for your data.
- Add team members: Add your team members to Splunk platform.
- Manage permissions: Control who has access with roles.
- Configure mobile devices: Login or manage mobile devices using Splunk Secure Gateway.

At the bottom, there's a section titled "Learning and resources" with two cards:

- Product tours: New to Splunk? Take a tour to help you on
- Learn more with Splunk Docs: Deploy, manage, and use Splunk software

Splunk offers a robust platform for data visualization and monitoring through its dashboard features. Users can create and customize dashboards to display real-time metrics, visualizations, and alerts, enabling quick insights into system performance and security events.

Configure forwarder and receiver from settings

The screenshot shows the Splunk Settings interface with the URL <https://192.168.1.65:8000/en-US/manager/launcher/forwardreceive>. The page title is "Forwarding and receiving".

Forward data: Set up forwarding between two or more Splunk instances.

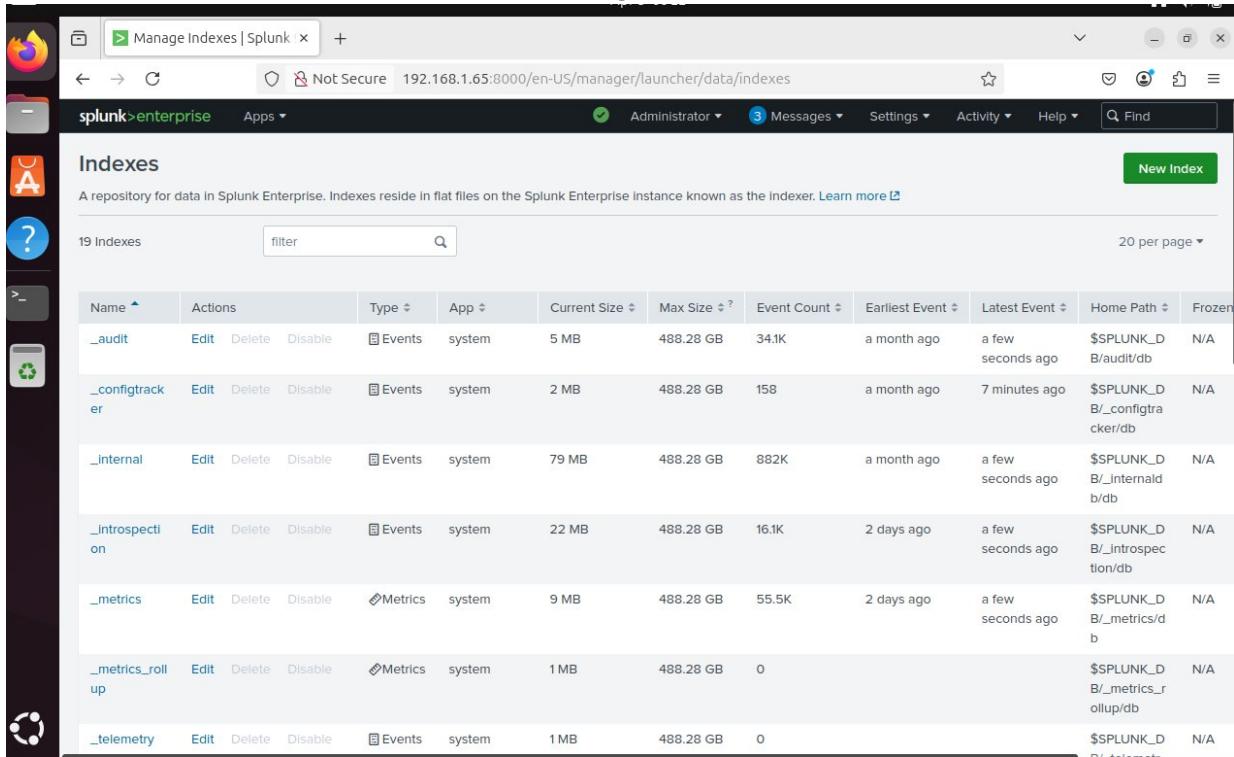
| Type | Actions |
|----------------------|-----------|
| Forwarding defaults | |
| Configure forwarding | + Add new |

Receive data: Configure this instance to receive data forwarded from other instances.

| Type | Actions |
|---------------------|-----------|
| Configure receiving | + Add new |

Configuring a Splunk Forwarder and Receiver involves setting up a Splunk Universal Forwarder (for data collection) and a Splunk instance (for data receiving and indexing). Below are the steps to configure both components.

Create Indexes as per choice from setting > indexes > new index



| Name | Actions | Type | App | Current Size | Max Size | Event Count | Earliest Event | Latest Event | Home Path | Frozen |
|-----------------|---------------------|---------|--------|--------------|-----------|-------------|----------------|-------------------|---------------------------------|--------|
| _audit | Edit Delete Disable | Events | system | 5 MB | 488.28 GB | 34.1K | a month ago | a few seconds ago | \$SPLUNK_D/B/_audit/db | N/A |
| _configtracker | Edit Delete Disable | Events | system | 2 MB | 488.28 GB | 158 | a month ago | 7 minutes ago | \$SPLUNK_D/B/_configtracker/db | N/A |
| _internal | Edit Delete Disable | Events | system | 79 MB | 488.28 GB | 882K | a month ago | a few seconds ago | \$SPLUNK_D/B/_internal/db | N/A |
| _introspection | Edit Delete Disable | Events | system | 22 MB | 488.28 GB | 16.1K | 2 days ago | a few seconds ago | \$SPLUNK_D/B/_introspection/db | N/A |
| _metrics | Edit Delete Disable | Metrics | system | 9 MB | 488.28 GB | 55.5K | 2 days ago | a few seconds ago | \$SPLUNK_D/B/_metrics/db | N/A |
| _metrics_rollup | Edit Delete Disable | Metrics | system | 1 MB | 488.28 GB | 0 | | | \$SPLUNK_D/B/_metrics_rollup/db | N/A |
| _telemetry | Edit Delete Disable | Events | system | 1 MB | 488.28 GB | 0 | | | \$SPLUNK_D/B/_telemetry | N/A |

Creating a new index in Splunk is essential for organizing and managing your data effectively. Whether you choose to use the Splunk Web interface or edit configuration files directly, both methods are valid and will allow you to set up a new index for your data.

Create source type as per choice from setting > source types > new source type

Creating a new sourcetype in Splunk is essential for ensuring that your data is indexed and interpreted correctly. Whether you choose to use the Splunk Web interface or edit configuration files directly, both methods are valid and will allow you to set up a new sourcetype for your data.

The screenshot shows the 'Source Types' page in Splunk 9.1. The URL is 192.168.1.65:8000/en-US/manager/launcher/sourcetypes. The page displays a table of 49 source types, each with a name, description, actions (Edit, Clone), category, and app. The columns are Name, Actions, Category, and App. The table includes rows for '_json', 'access_combined', 'apache_error', 'catalina', 'cisco:asa', 'collectd_http', 'csv', and 'db2_diag'. The 'db2_diag' row is currently selected.

| Name | Actions | Category | App |
|-----------------|------------|--------------------|--------|
| _json | Edit Clone | Structured | system |
| access_combined | Edit Clone | Web | system |
| apache_error | Edit Clone | Web | system |
| catalina | Edit Clone | Application | system |
| cisco:asa | Edit Clone | Network & Security | system |
| collectd_http | Edit Clone | Metrics | system |
| csv | Edit Clone | Structured | system |
| db2_diag | Edit Clone | Database | system |

Open Workstation

/opt/splunkforwarder/bin/splunk start

```
vboxuser@workstation:~$ sudo su
[sudo] password for vboxuser:
root@workstation:/home/vboxuser# /opt/splunkforwarder/bin/splunk start
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
The splunk daemon (splunkd) is already running.
root@workstation:/home/vboxuser#
```

nano /opt/splunkforwarder/etc/system/local/inputs.conf

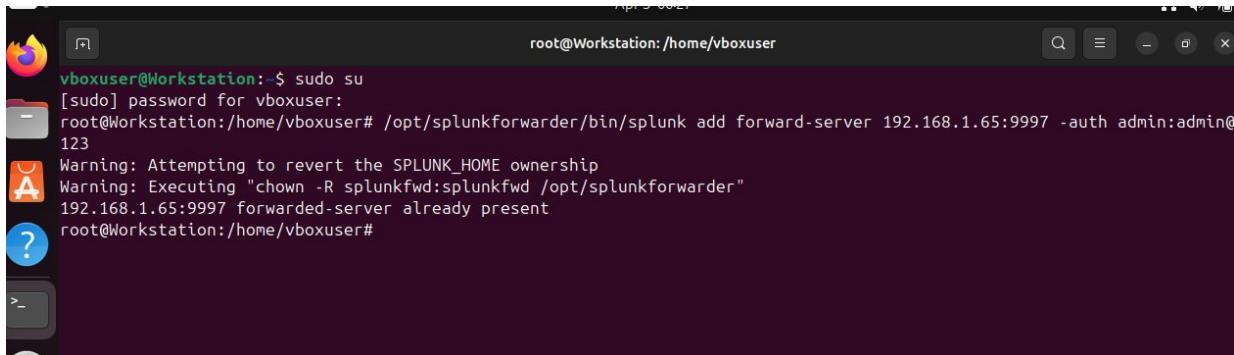
```
GNU nano 7.2
[monitor:///var/log/syslog]
disabled = false
index = linux_os
sourcetype = syslog

[monitor:///var/log/auth.log]
disabled = false
index = security
sourcetype = linux_secure
```

This configuration is likely used in a Linux environment where Splunk is collecting logs for monitoring and analysis.

The specified logs are crucial for system administration and security, providing insights into both general system events (syslog) and security-related events (auth.log).

```
/opt/splunkforwarder/bin/splunk add forwarder-server 192.168.1.65:9997 -auth admin:admin@123
```



```
vboxuser@Workstation:~$ sudo su
[sudo] password for vboxuser:
root@Workstation:/home/vboxuser# /opt/splunkforwarder/bin/splunk add forwarder-server 192.168.1.65:9997 -auth admin:admin@123
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
192.168.1.65:9997 forwarded-server already present
root@Workstation:/home/vboxuser#
```

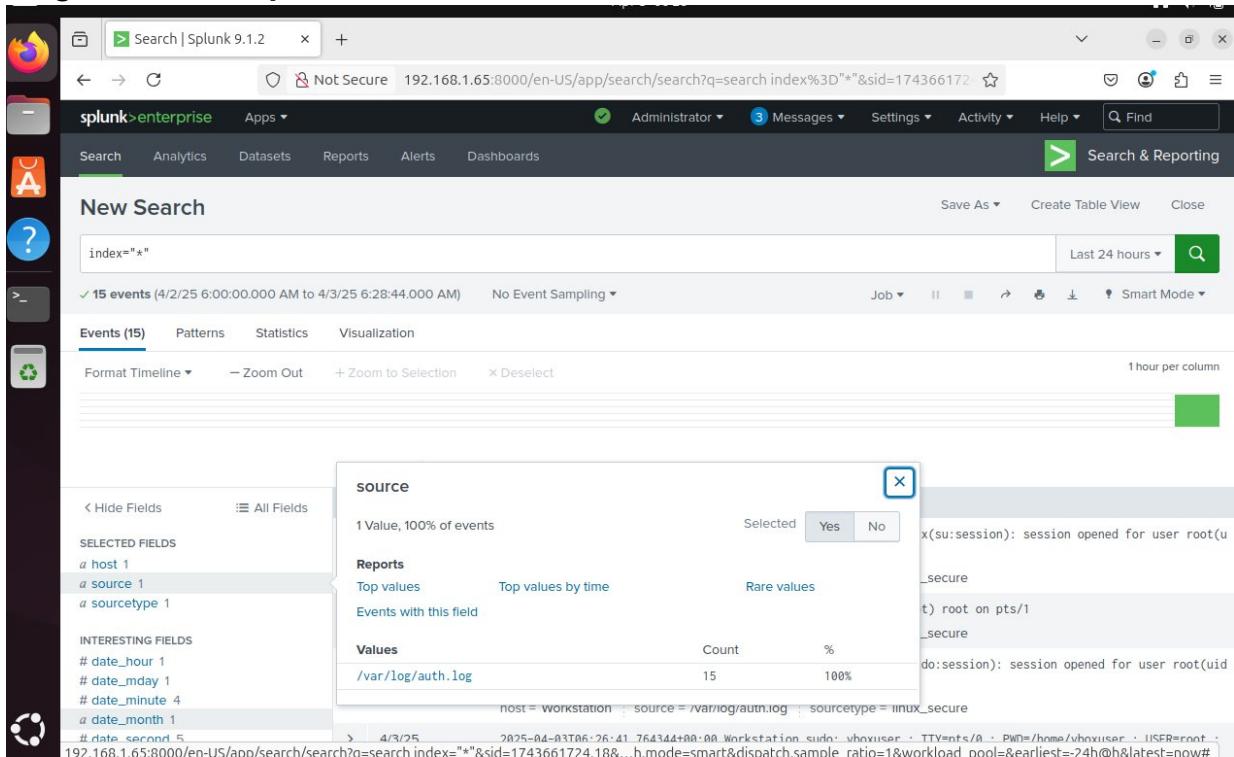
In short, this command is meant to set up the Splunk Universal Forwarder to monitor a specific data source, but the address format looks like it might be wrong for a file or folder. The command also includes login details to connect to the Splunk system. If you want to monitor a specific file or folder, you should replace 192.168.1.65:9997 with the actual file or folder path you want to track.

```
/opt/splunkforwarder/bin/splunk add monitor /var/log/auth.log
```

```
/opt/splunkforwarder/bin/splunk add monitor /var/log/syslog
```

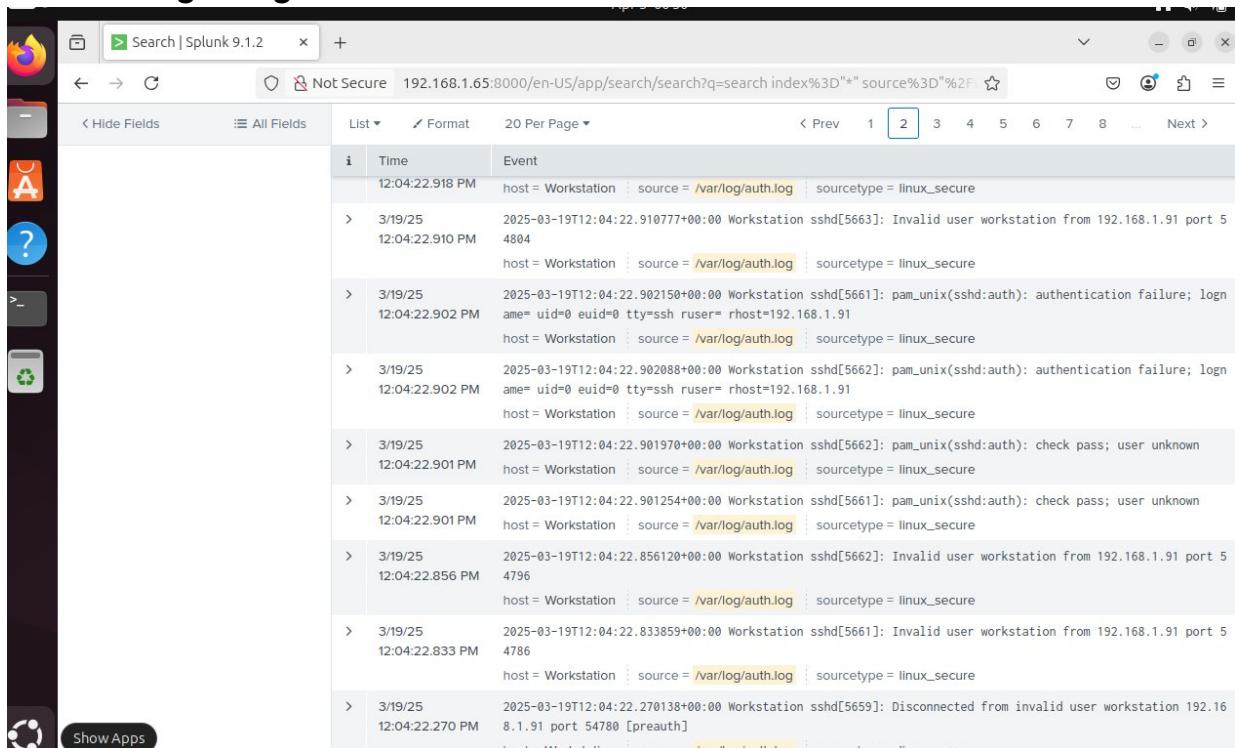
These commands configure Splunk to actively monitor two critical log files (auth.log for authentication events and syslog for system events), ensuring that important security and operational data is collected for analysis.

Logs shown on splunk server



The screenshot shows the Splunk Enterprise search interface. A search query "index='*' is entered in the search bar. The results pane displays 15 events from April 2, 2025, between 6:00:00.000 AM and 6:28:44.000 AM. The "Events (15)" tab is selected. The left sidebar shows fields like host, source, and sourcetype. A tooltip for the source field indicates it is selected (1 Value, 100% of events). The bottom right corner shows a partial log entry: "x(su:session): session opened for user root(uid".

Attacker logs are generated



The screenshot shows a Firefox browser window with the URL `192.168.1.65:8000/en-US/app/search/search?q=search index%3D"*" source%3D"%2F`. The search results table has columns for Time, host, source, and Event. The table contains 10 rows of log entries from `/var/log/auth.log` on a Linux system. The logs show multiple failed SSH login attempts from IP 192.168.1.91, with timestamps ranging from 2025-03-19T12:04:22.910 PM to 2025-03-19T12:04:22.856 PM.

| i | Time | Event |
|---|----------------------------|---|
| | 12:04:22.918 PM | host = Workstation : source = <code>/var/log/auth.log</code> : sourcetype = linux_secure |
| > | 3/19/25 12:04:22.910 PM | 2025-03-19T12:04:22.910777+00:00 Workstation sshd[5663]: Invalid user workstation from 192.168.1.91 port 54804 host = Workstation : source = <code>/var/log/auth.log</code> : sourcetype = linux_secure |
| > | 3/19/25 12:04:22.902 PM | 2025-03-19T12:04:22.902150+00:00 Workstation sshd[5661]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.91 host = Workstation : source = <code>/var/log/auth.log</code> : sourcetype = linux_secure |
| > | 3/19/25 12:04:22.902 PM | 2025-03-19T12:04:22.902088+00:00 Workstation sshd[5662]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.1.91 host = Workstation : source = <code>/var/log/auth.log</code> : sourcetype = linux_secure |
| > | 3/19/25 12:04:22.901 PM | 2025-03-19T12:04:22.901970+00:00 Workstation sshd[5662]: pam_unix(sshd:auth): check pass; user unknown host = Workstation : source = <code>/var/log/auth.log</code> : sourcetype = linux_secure |
| > | 3/19/25 12:04:22.901 PM | 2025-03-19T12:04:22.901254+00:00 Workstation sshd[5661]: pam_unix(sshd:auth): check pass; user unknown host = Workstation : source = <code>/var/log/auth.log</code> : sourcetype = linux_secure |
| > | 3/19/25 12:04:22.856 PM | 2025-03-19T12:04:22.856120+00:00 Workstation sshd[5662]: Invalid user workstation from 192.168.1.91 port 54796 host = Workstation : source = <code>/var/log/auth.log</code> : sourcetype = linux_secure |
| > | 3/19/25 12:04:22.833 PM | 2025-03-19T12:04:22.833859+00:00 Workstation sshd[5661]: Invalid user workstation from 192.168.1.91 port 54786 host = Workstation : source = <code>/var/log/auth.log</code> : sourcetype = linux_secure |
| > | 3/19/25 12:04:22.270 PM | 2025-03-19T12:04:22.270138+00:00 Workstation sshd[5659]: Disconnected from invalid user workstation 192.168.1.91 port 54780 [preauth] host = Workstation : source = <code>/var/log/auth.log</code> : sourcetype = linux_secure |

Nmap -sV 192.168.1.65

```
(root㉿kali)-[~] # nmap -sV 192.168.1.65
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-03 12:17 IST
Nmap scan report for 192.168.1.65
Host is up (0.0044s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
25/tcp    open  smtp   Postfix smtpd
8000/tcp  open  http   Splunkd httpd
8089/tcp  open  ssl/http Splunkd httpd
MAC Address: DC:97:BA:5E:02:59 (Intel Corporation)
Service Info: Host: Ubuntu

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.31 seconds
```

This command helps you learn more about what software is running on a specific device in your local network.

Hydra -L user.txt -P user.txt ssh://192.168.1.65

```
[root@kali) ~] # hydra -L user.txt -P user.txt ssh://192.168.1.65
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-03 12:22:16
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:3/p:3), -1 try per task
[DATA] attacking ssh://192.168.1.65:22/
[ERROR] could not connect to ssh://192.168.1.65:22 - Connection refused
```

This command is trying to log into the SSH service on the specified device by testing all combinations of usernames and passwords from the provided files