# splunk>enterprise

Splunk Enterprise is a platform that ingests, indexes, and searches machine-generated data (like logs from servers, firewalls, endpoints, cloud services, etc.) so you can find useful insights quickly. It turns *raw logs* into searchable data and provides dashboards, alerts, and analytics. Splunk can be used for IT ops, DevOps, and importantly cybersecurity

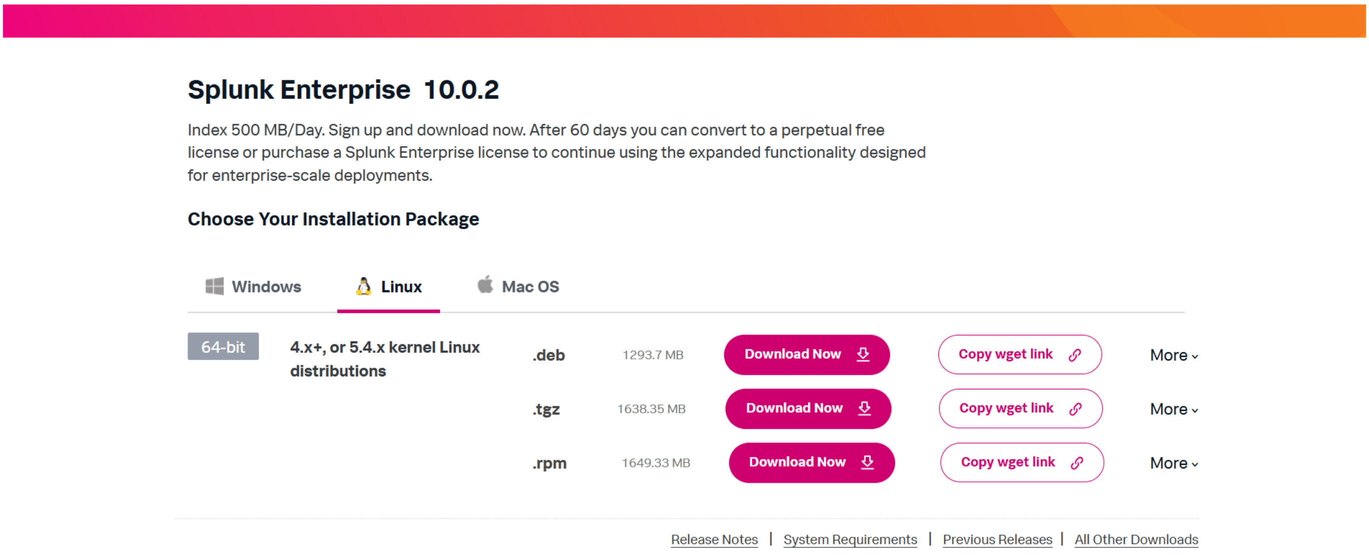
**Splunk Enterprise Security (ES) helps in cybersecurity by:**

- Detecting threats in real time through log correlation and security analytics
- Centralizing security data from endpoints, networks, servers, and cloud
- Reducing alert noise using risk-based alerting
- Enabling fast investigations with dashboards and context-rich incident views
- Identifying abnormal behavior via UEBA (insider threats, compromised accounts)
- Supporting threat hunting aligned with MITRE ATT&CK
- Automating response through SOAR integrations
- Supporting compliance with audit logs and security reporting

## Install Splunk in ubuntu:

### Download the Splunk .deb Package

First, obtain the download link for the Linux (.deb) file from the official Splunk website. If you don't have the link, you can download it via a browser.



**Splunk Enterprise 10.0.2**

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

**Choose Your Installation Package**

| | | | | | | |
|---|---|---|---|---|---|---|
| 64-bit | 4.x+, or 5.4.x kernel Linux distributions | .deb | 1293.7 MB | Download Now | Copy wget link | More |
| | | .tgz | 1638.35 MB | Download Now | Copy wget link | More |
| | | .rpm | 1649.33 MB | Download Now | Copy wget link | More |

Release Notes | System Requirements | Previous Releases | All Other Downloads

save it in your Downloads folder

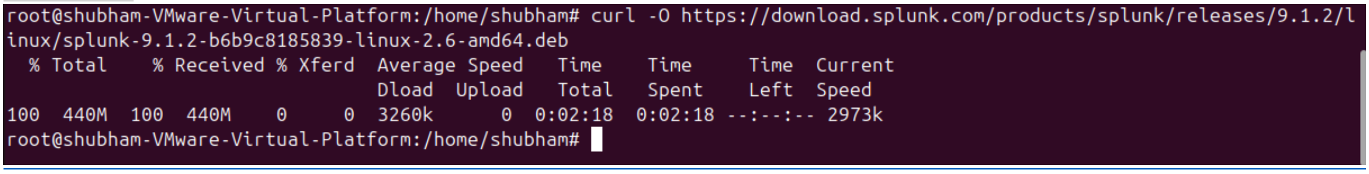
```
cd ~/Downloads
```

firstly, install curl:

```
apt install curl
```

then run following command:

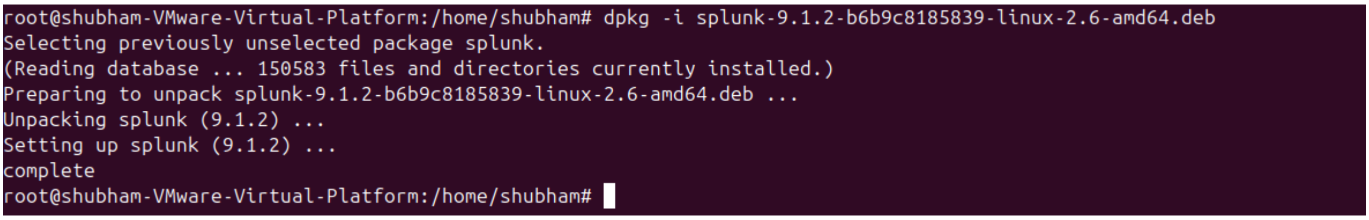
curl -O  https://download.splunk.com/products/splunk/releases/9.1.2/linux/splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb



```
root@shubham-VMware-Virtual-Platform:/home/shubham# curl -O https://download.splunk.com/products/splunk/releases/9.1.2/l
inux/splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  440M  100  440M    0     0  3260k      0  0:02:18  0:02:18 --:--:-- 2973k
root@shubham-VMware-Virtual-Platform:/home/shubham#
```

Use the dpkg package manager to start the installation:

dpkg -i splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb



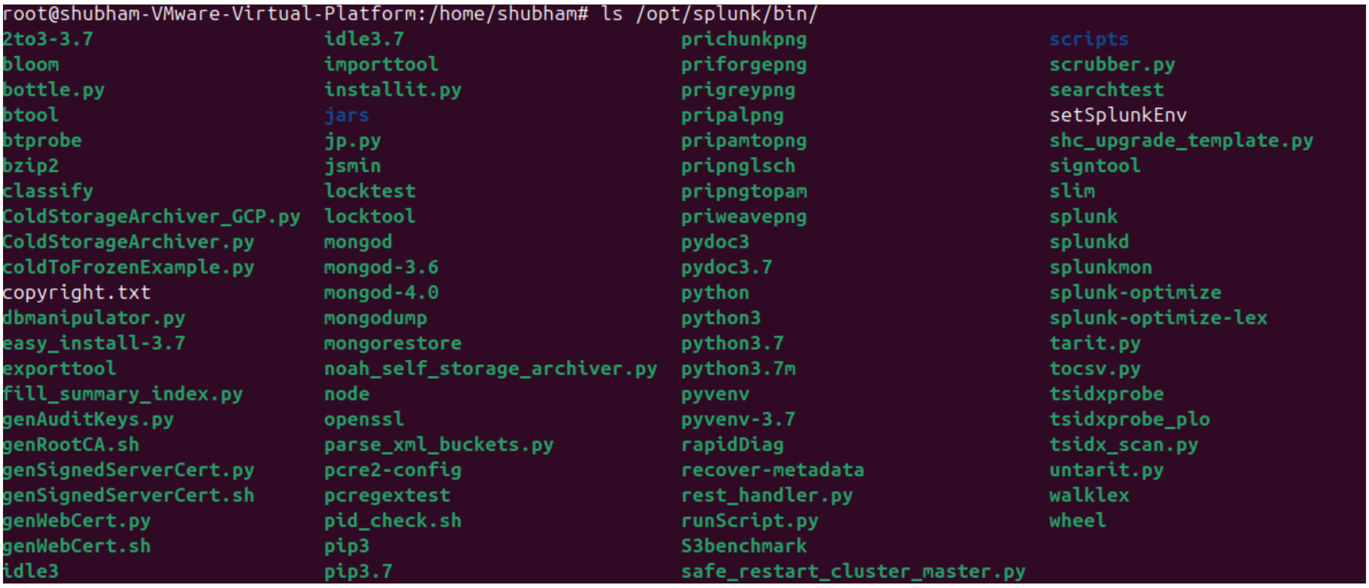
```
root@shubham-VMware-Virtual-Platform:/home/shubham# dpkg -i splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 150583 files and directories currently installed.)
Preparing to unpack splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb ...
Unpacking splunk (9.1.2) ...
Setting up splunk (9.1.2) ...
complete
root@shubham-VMware-Virtual-Platform:/home/shubham#
```

This command installs the Splunk software into the /opt/splunk directory by default.

Once installed, you must start the Splunk service. During the first run, you will be required to accept the license agreement and create an **Administrator Username and Password**.

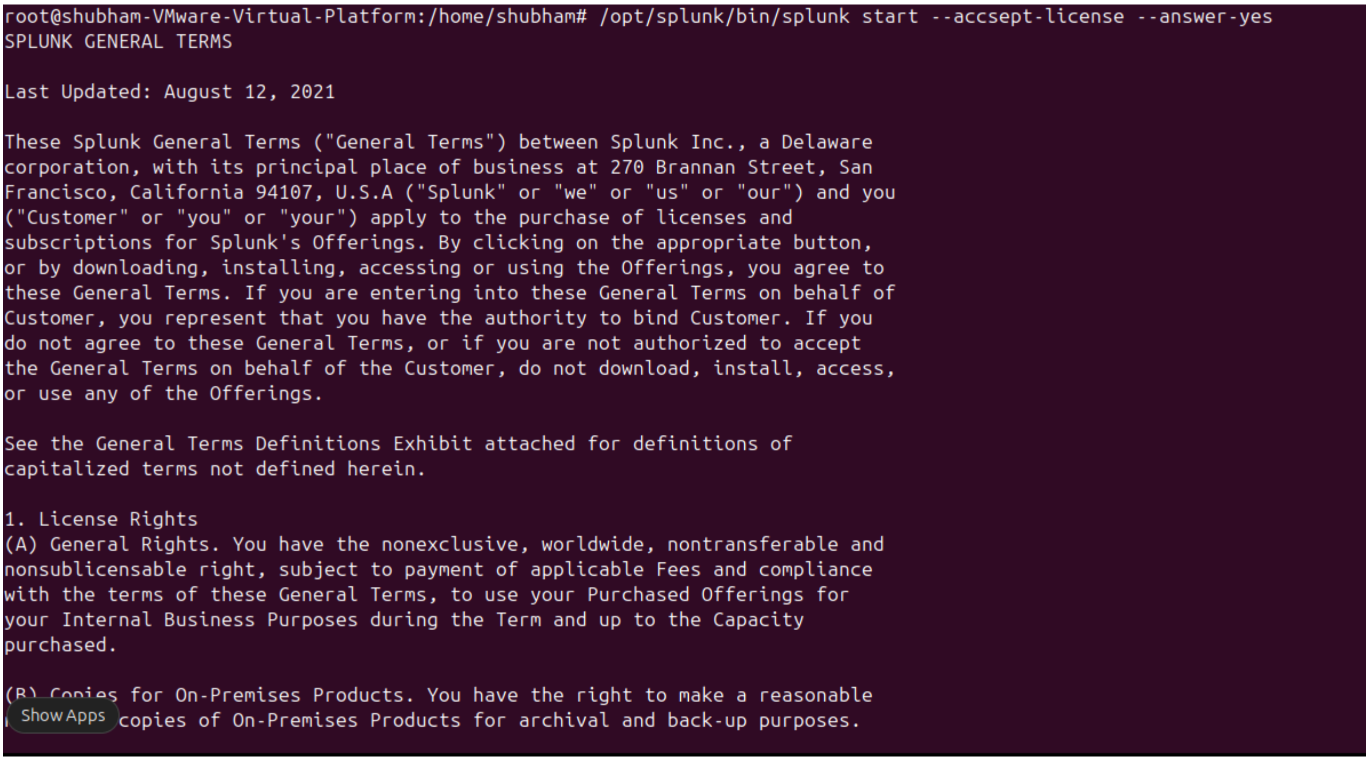
First check splunk bin file:

ls /opt/splunk/bin/



```
root@shubham-VMware-Virtual-Platform:/home/shubham# ls /opt/splunk/bin/
2to3-3.7                    idle3.7                        prichunkpng                     scripts
bloom                       importtool                     priforgepng                     scrubber.py
bottle.py                   installit.py                   prigreypng                      searchtest
btool                       jars                           pripalpng                       setSplunkEnv
btprobe                     jp.py                          pripamtopng                     shc_upgrade_template.py
bzip2                       jsmin                          pripnglsch                      signtool
classify                    locktest                       pripngtopam                     slim
ColdStorageArchiver_GCP.py  locktool                       priweavepng                     splunk
ColdStorageArchiver.py      mongod                         pydoc3                          splunkd
coldToFrozenExample.py      mongod-3.6                     pydoc3.7                        splunkmon
copyright.txt               mongod-4.0                     python                          splunk-optimize
dbmanipulator.py            mongodump                      python3                         splunk-optimize-lex
easy_install-3.7            mongorestore                   python3.7                       tarit.py
exporttool                  noah_self_storage_archiver.py  python3.7m                      tocsv.py
fill_summary_index.py       node                           pyvenv                          tsidxprobe
genAuditKeys.py             openssl                        pyvenv-3.7                      tsidxprobe_plo
genRootCA.sh                parse_xml_buckets.py           rapidDiag                       tsidx_scan.py
genSignedServerCert.py      pcre2-config                   recover-metadata                untarit.py
genSignedServerCert.sh      pcregextest                    rest_handler.py                 walklex
genWebCert.py               pid_check.sh                   runScript.py                    wheel
genWebCert.sh               pip3                           S3benchmark
idle3                       pip3.7                         safe_restart_cluster_master.py
```

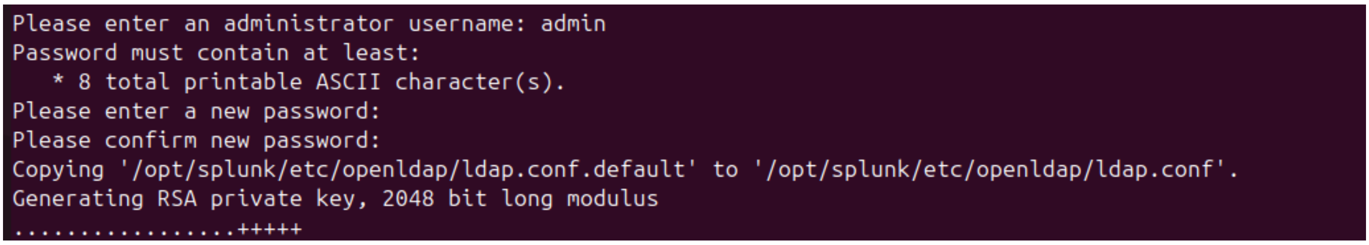
cd /opt/splunk/bin/splunk start --accept-license



```
root@shubham-VMware-Virtual-Platform:/home/shubham# /opt/splunk/bin/splunk start --accsept-license --answer-yes
SPLUNK GENERAL TERMS

Last Updated: August 12, 2021

These Splunk General Terms ("General Terms") between Splunk Inc., a Delaware
corporation, with its principal place of business at 270 Brannan Street, San
Francisco, California 94107, U.S.A ("Splunk" or "we" or "us" or "our") and you
("Customer" or "you" or "your") apply to the purchase of licenses and
subscriptions for Splunk's Offerings. By clicking on the appropriate button,
or by downloading, installing, accessing or using the Offerings, you agree to
these General Terms. If you are entering into these General Terms on behalf of
Customer, you represent that you have the authority to bind Customer. If you
do not agree to these General Terms, or if you are not authorized to accept
the General Terms on behalf of the Customer, do not download, install, access,
or use any of the Offerings.

See the General Terms Definitions Exhibit attached for definitions of
capitalized terms not defined herein.

1. License Rights
(A) General Rights. You have the nonexclusive, worldwide, nontransferable and
nonsublicensable right, subject to payment of applicable Fees and compliance
with the terms of these General Terms, to use your Purchased Offerings for
your Internal Business Purposes during the Term and up to the Capacity
purchased.

(B) Copies for On-Premises Products. You have the right to make a reasonable
         copies of On-Premises Products for archival and back-up purposes.
```

**Important:** You will be prompted: Please enter an administrator username: Type admin.

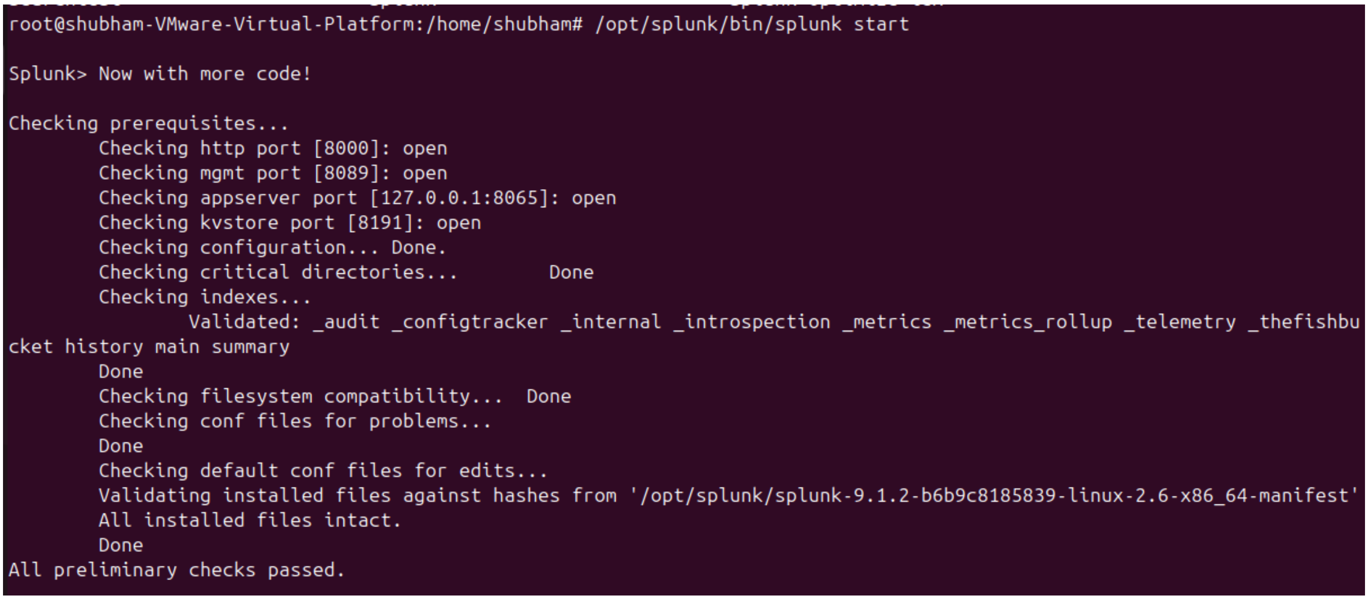
Next, enter a strong password (e.g., Admin@123).



```
Please enter an administrator username: admin
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
.................+++++
```

To ensure Splunk starts

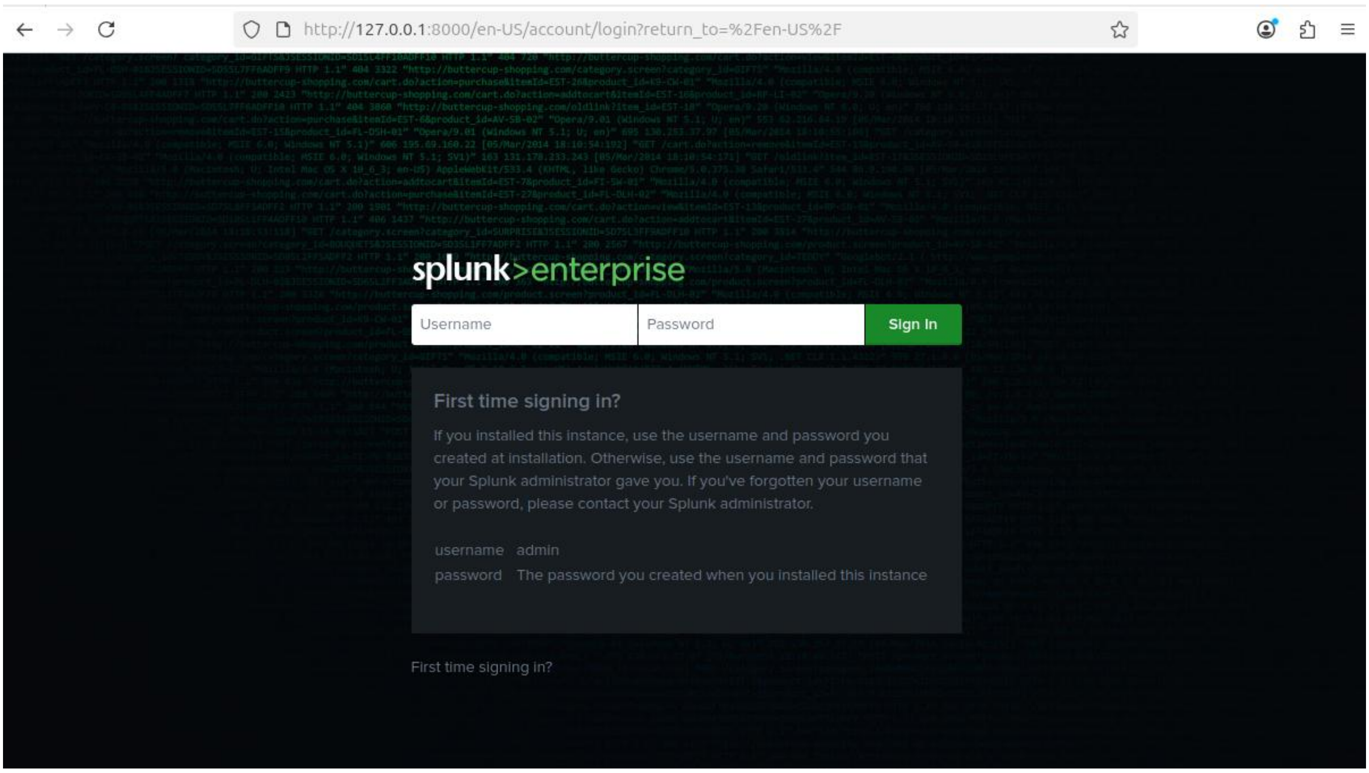
/opt/splunk/bin/splunk start



```
root@shubham-VMware-Virtual-Platform:/home/shubham# /opt/splunk/bin/splunk start

Splunk> Now with more code!

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.
        Checking critical directories...        Done
        Checking indexes...
                Validated: _audit _configtracker _internal _introspection _metrics _metrics_rollup _telemetry _thefishbu
cket history main summary
        Done
        Checking filesystem compatibility...  Done
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunk/splunk-9.1.2-b6b9c8185839-linux-2.6-x86_64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.
```

Splunk is now running as a background service. To access the dashboard, open your web browser (Chrome or Firefox) and navigate to: http://localhost:8000

Log in using the **admin** credentials you just created.



http://127.0.0.1:8000/en-US/account/login?return_to=%2Fen-US%2F

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

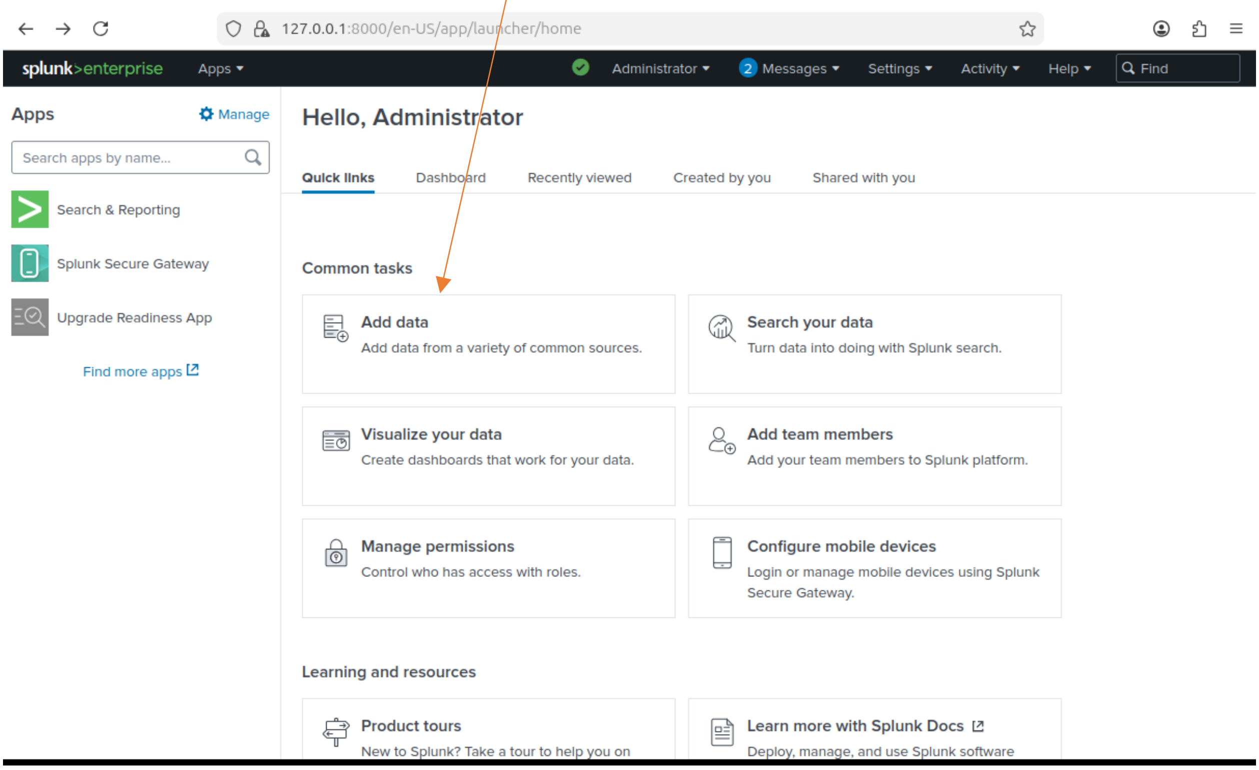
password The password you created when you installed this instance

First time signing in?

## Data Ingestion (Adding Logs)

To begin monitoring your Ubuntu system logs (e.g., authentication attempts):

1. From the Splunk home screen, click **"Add Data"**.



127.0.0.1:8000/en-US/app/launcher/home

Hello, Administrator

Common tasks

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.

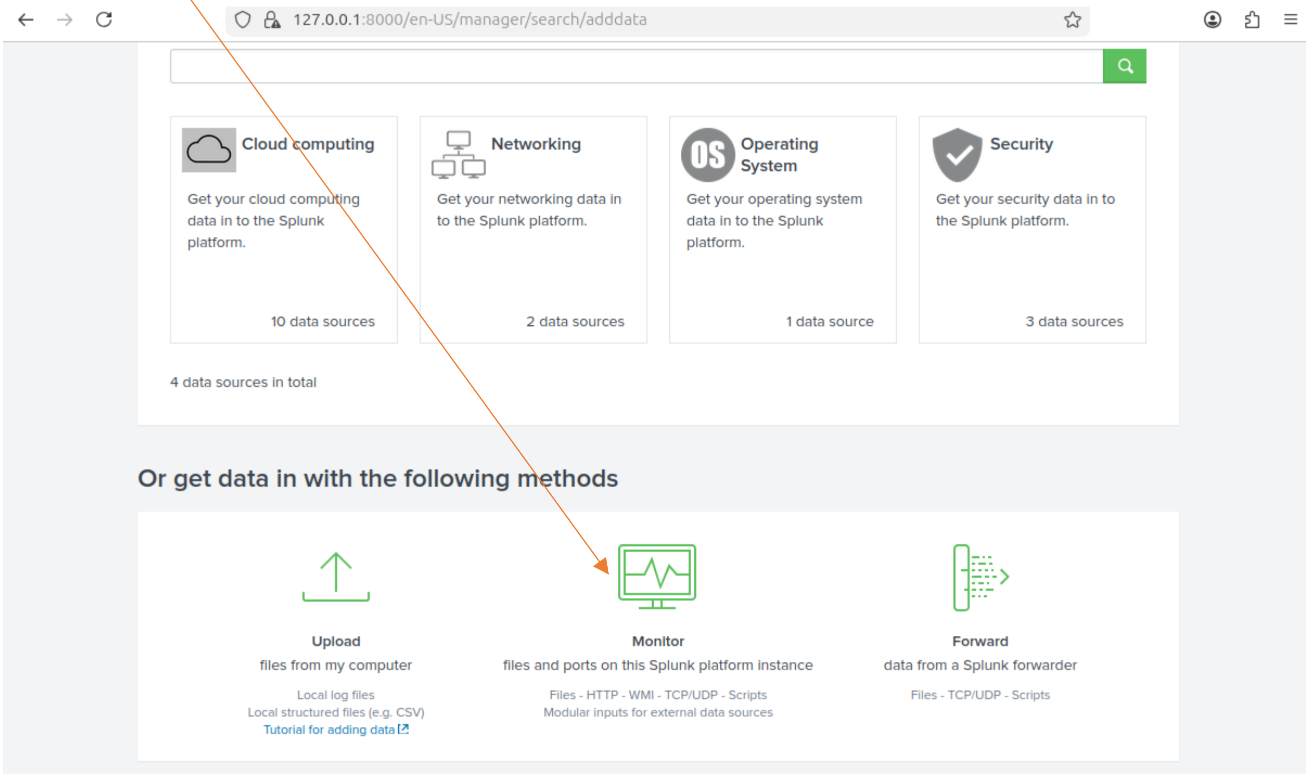
Configure mobile devices
Login or manage mobile devices using Splunk Secure Gateway.

Learning and resources

Product tours
New to Splunk? Take a tour to help you on

Learn more with Splunk Docs
Deploy, manage, and use Splunk software

2. Select the **"Monitor"** option.


127.0.0.1:8000/en-US/manager/search/adddata
Cloud computing
10 data sources
Networking
2 data sources
Operating System
1 data source
Security
3 data sources
Upload
files from my computer
Local log files
Local structured files (e.g. CSV)
Tutorial for adding data
Monitor
files and ports on this Splunk platform instance
Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources
Forward
data from a Splunk forwarder
Files - TCP/UDP - Scripts

Get your cloud computing data in to the Splunk platform.

Get your networking data in to the Splunk platform.

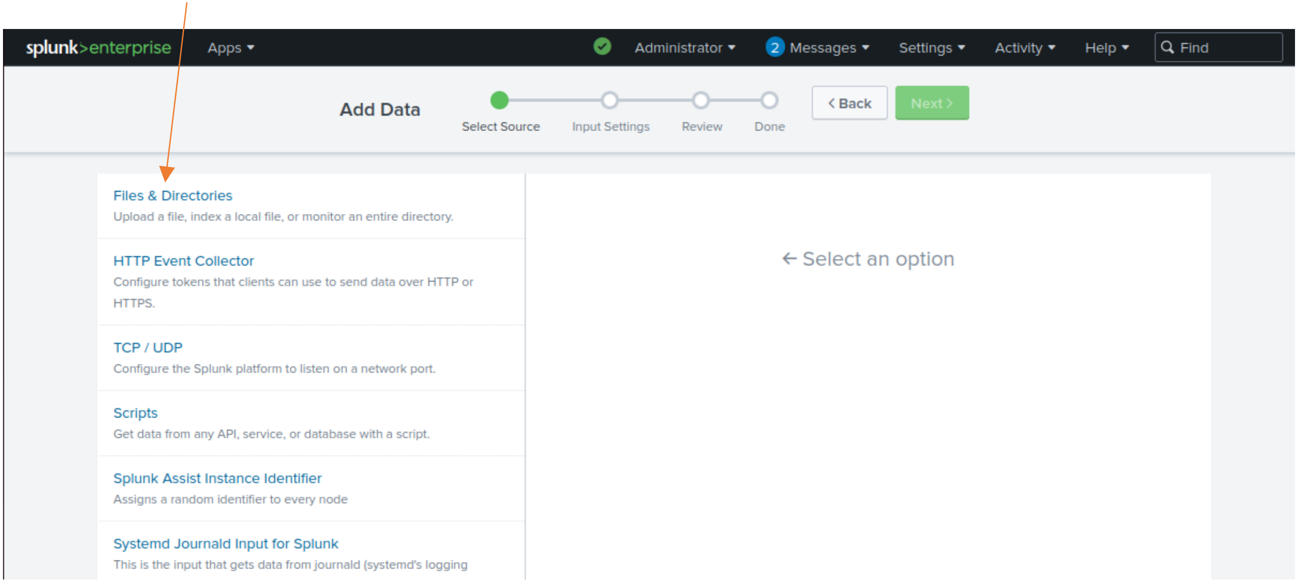
Get your operating system data in to the Splunk platform.

Get your security data in to the Splunk platform.

4 data sources in total

Or get data in with the following methods

3. Click on **"Files & Directories"**.



Files & Directories: Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector: Configure tokens that clients can use to send data over HTTP or HTTPS.

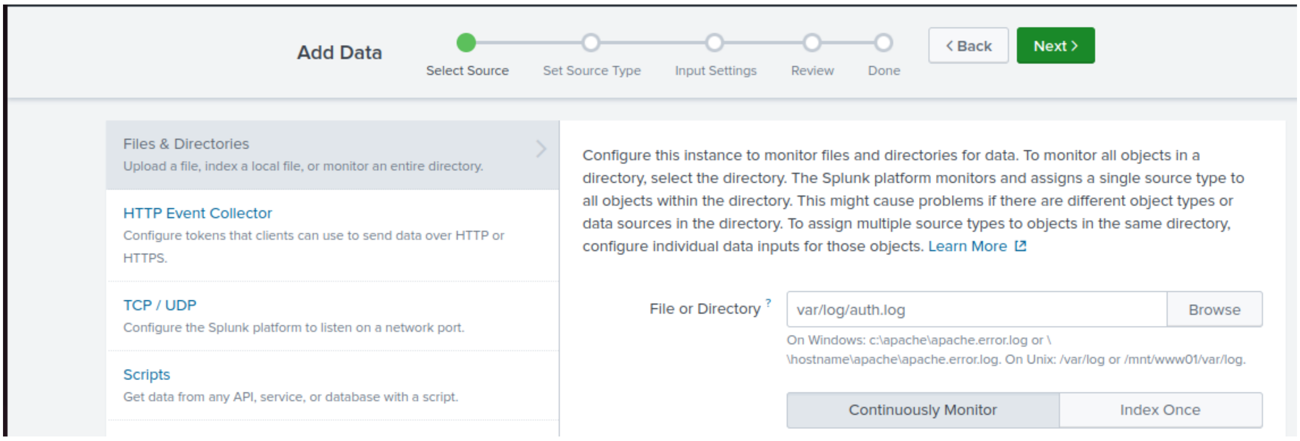
TCP / UDP: Configure the Splunk platform to listen on a network port.

Scripts: Get data from any API, service, or database with a script.

Splunk Assist Instance Identifier: Assigns a random identifier to every node

Systemd Journald Input for Splunk: This is the input that gets data from journald (systemd's logging

4. Click **Browse** and navigate to: /var/log/auth.log (this tracks login activity).



Files & Directories: Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector: Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP: Configure the Splunk platform to listen on a network port.

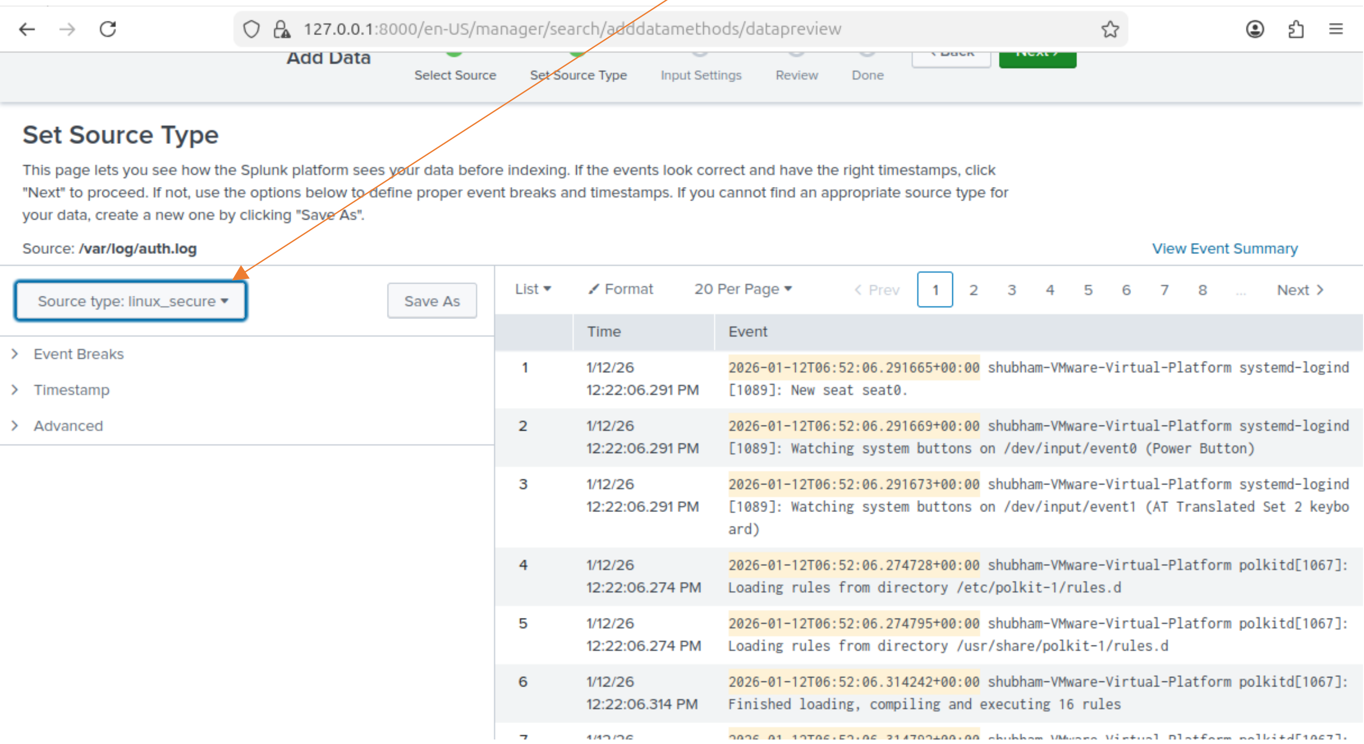
Scripts: Get data from any API, service, or database with a script.

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. Learn More

File or Directory: var/log/auth.log

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

5. Click **Next**, review the settings (ensure Sourcetype is linux_secure), and click **Submit**.



## Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **/var/log/auth.log**

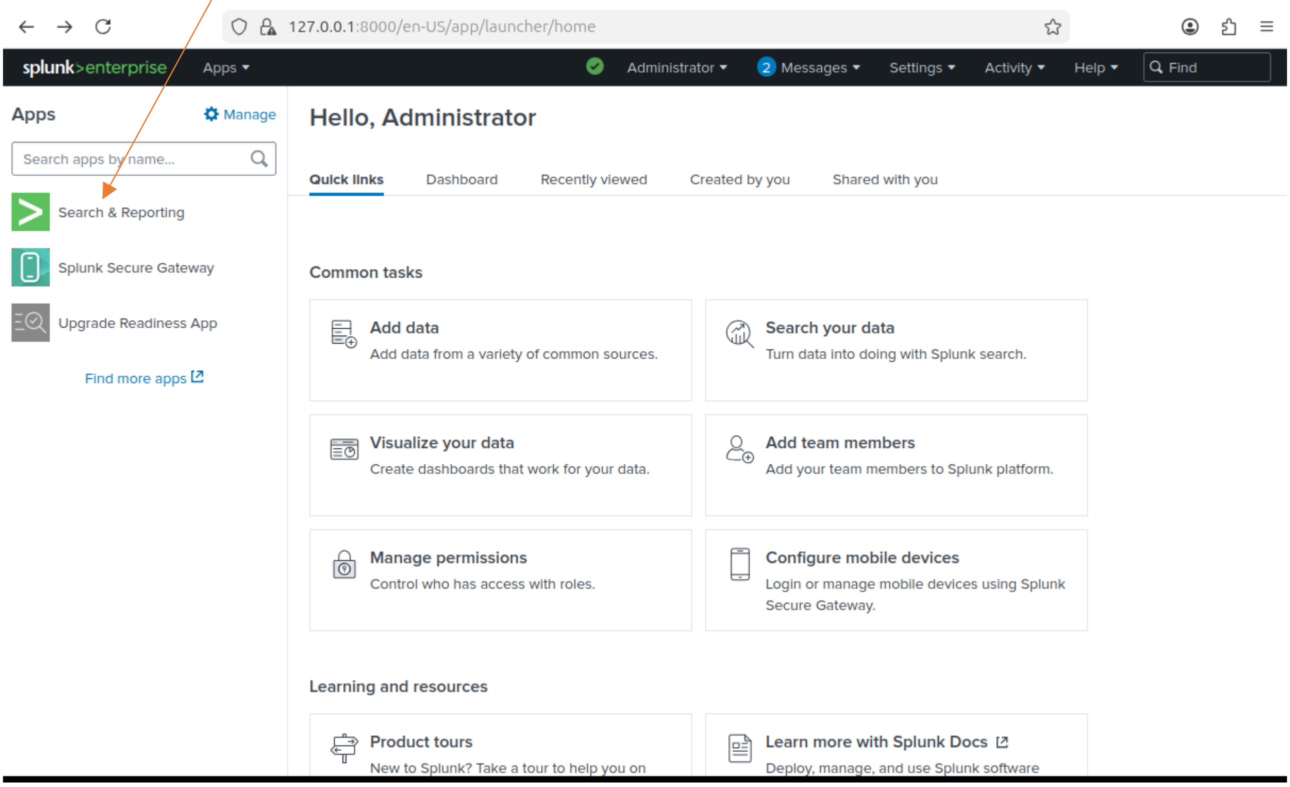
Source type: linux_secure ▾

| | Time | Event |
|---|---|---|
| 1 | 1/12/26 12:22:06.291 PM | 2026-01-12T06:52:06.291665+00:00 shubham-VMware-Virtual-Platform systemd-logind [1089]: New seat seat0. |
| 2 | 1/12/26 12:22:06.291 PM | 2026-01-12T06:52:06.291669+00:00 shubham-VMware-Virtual-Platform systemd-logind [1089]: Watching system buttons on /dev/input/event0 (Power Button) |
| 3 | 1/12/26 12:22:06.291 PM | 2026-01-12T06:52:06.291673+00:00 shubham-VMware-Virtual-Platform systemd-logind [1089]: Watching system buttons on /dev/input/event1 (AT Translated Set 2 keyboard) |
| 4 | 1/12/26 12:22:06.274 PM | 2026-01-12T06:52:06.274728+00:00 shubham-VMware-Virtual-Platform polkitd[1067]: Loading rules from directory /etc/polkit-1/rules.d |
| 5 | 1/12/26 12:22:06.274 PM | 2026-01-12T06:52:06.274795+00:00 shubham-VMware-Virtual-Platform polkitd[1067]: Loading rules from directory /usr/share/polkit-1/rules.d |
| 6 | 1/12/26 12:22:06.314 PM | 2026-01-12T06:52:06.314242+00:00 shubham-VMware-Virtual-Platform polkitd[1067]: Finished loading, compiling and executing 16 rules |

The implementation focuses on establishing a real-time security monitoring pipeline using Splunk Enterprise. By ingesting the linux_secure sourcetype, we enable automated parsing of authentication events, allowing for proactive detection of brute-force attacks and unauthorized privilege escalation.

## Searching and Analysis

Go to the **"Search & Reporting"** app



Hello, Administrator

Common tasks

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.

Learning and resources

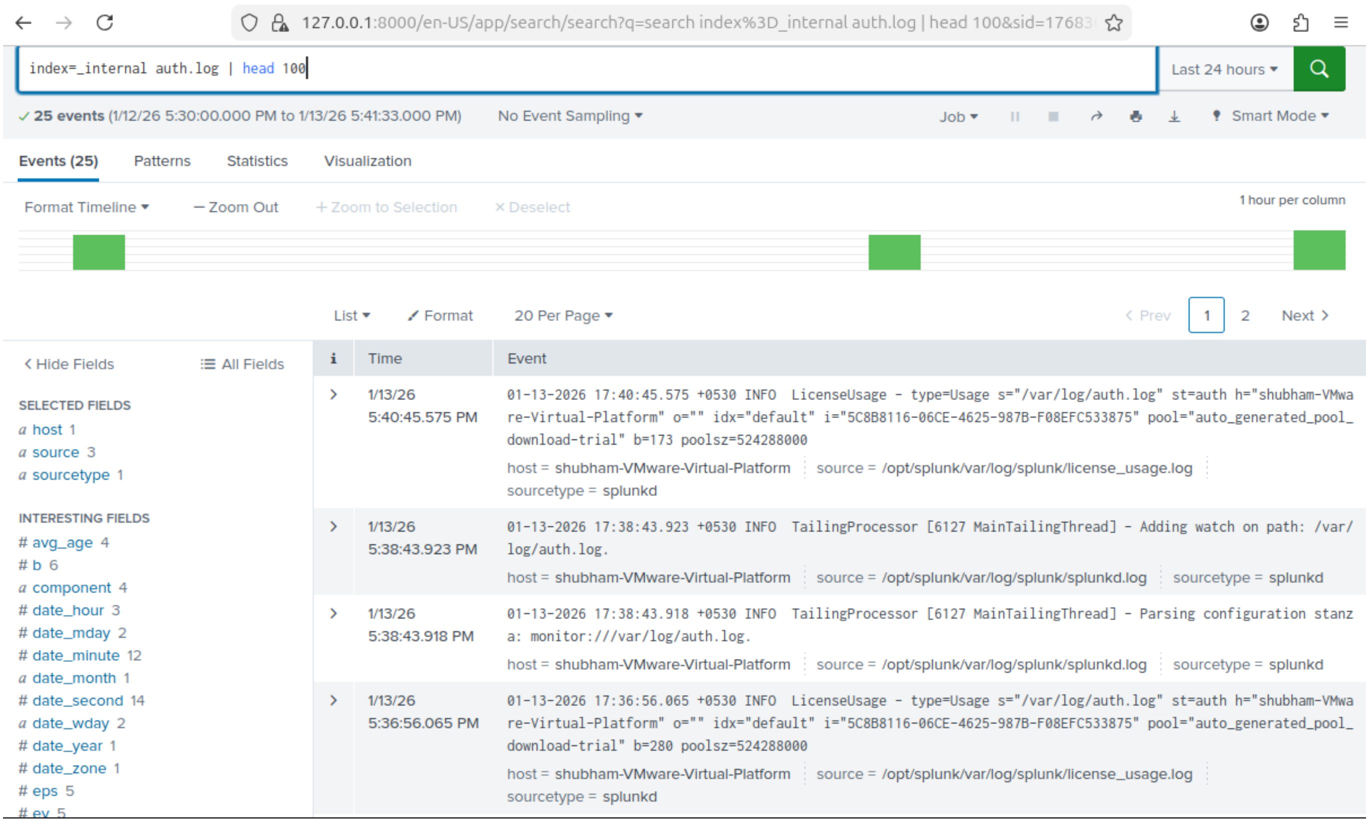
Product tours
New to Splunk? Take a tour to help you on

Learn more with Splunk Docs
Deploy, manage, and use Splunk software

enter the following query in the search bar:

index=_internal auth.log | head 100

head 100 show top recently 100 logs



```
index=_internal auth.log | head 100
```

✓ 25 events (1/12/26 5:30:00.000 PM to 1/13/26 5:41:33.000 PM)

SELECTED FIELDS
a host 1
a source 3
a sourcetype 1

INTERESTING FIELDS
# avg_age 4
# b 6
a component 4
# date_hour 3
# date_mday 2
# date_minute 12
a date_month 1
# date_second 14
a date_wday 2
# date_year 1
# date_zone 1
# eps 5
# ev 5

| i | Time | Event |
|---|---|---|
| › | 1/13/26<br>5:40:45.575 PM | 01-13-2026 17:40:45.575 +0530 INFO  LicenseUsage - type=Usage s="/var/log/auth.log" st=auth h="shubham-VMware-Virtual-Platform" o="" idx="default" i="5C8B8116-06CE-4625-987B-F08EFC533875" pool="auto_generated_pool_download-trial" b=173 poolsz=524288000<br>host = shubham-VMware-Virtual-Platform  source = /opt/splunk/var/log/splunk/license_usage.log  sourcetype = splunkd |
| › | 1/13/26<br>5:38:43.923 PM | 01-13-2026 17:38:43.923 +0530 INFO  TailingProcessor [6127 MainTailingThread] - Adding watch on path: /var/log/auth.log.<br>host = shubham-VMware-Virtual-Platform  source = /opt/splunk/var/log/splunk/splunkd.log  sourcetype = splunkd |
| › | 1/13/26<br>5:38:43.918 PM | 01-13-2026 17:38:43.918 +0530 INFO  TailingProcessor [6127 MainTailingThread] - Parsing configuration stanza: monitor:///var/log/auth.log.<br>host = shubham-VMware-Virtual-Platform  source = /opt/splunk/var/log/splunk/splunkd.log  sourcetype = splunkd |
| › | 1/13/26<br>5:36:56.065 PM | 01-13-2026 17:36:56.065 +0530 INFO  LicenseUsage - type=Usage s="/var/log/auth.log" st=auth h="shubham-VMware-Virtual-Platform" o="" idx="default" i="5C8B8116-06CE-4625-987B-F08EFC533875" pool="auto_generated_pool_download-trial" b=280 poolsz=524288000<br>host = shubham-VMware-Virtual-Platform  source = /opt/splunk/var/log/splunk/license_usage.log  sourcetype = splunkd |

This will display all login activities on your Ubuntu machine, including successful entries and failed attempts.