WEEK-4

Asad Muhammad Channar

DHC-56

Task-2:

Security Automation with SIEM

Use Security Information and Event Management (SIEM) tools to automate log analysis and alerting.

Required:

- Set up a SIEM tool like Splunk or ELK.
- Configure it to monitor logs and generate alerts for suspicious activities.
- Automate response mechanisms (e.g., isolate affected systems) based on specific alerts.

Deliverables:

- Demonstration of security alerts and automation in action, along with a report explaining the setup and alerts triggered.

Setting Up SIEM (Splunk)

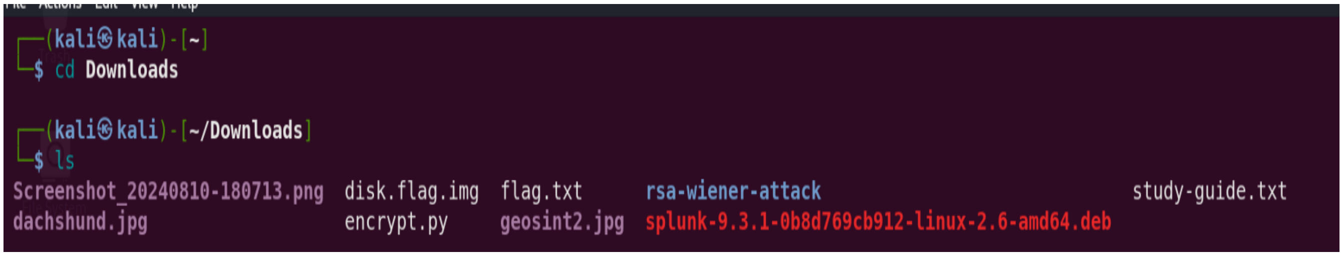
Splunk is a SIEM solution to monitor logs and generate appropriate alerts . For this task we use splunk as it is easy and user friendly to use.

Following is the complete procedure to set up splunk in linux. You can download splunk from the following link.

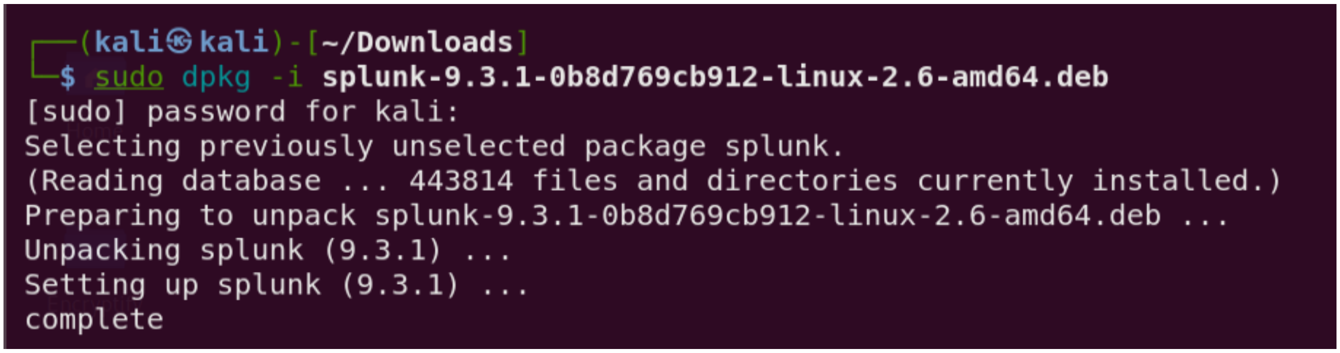
Download Splunk

Setting up Splunk:

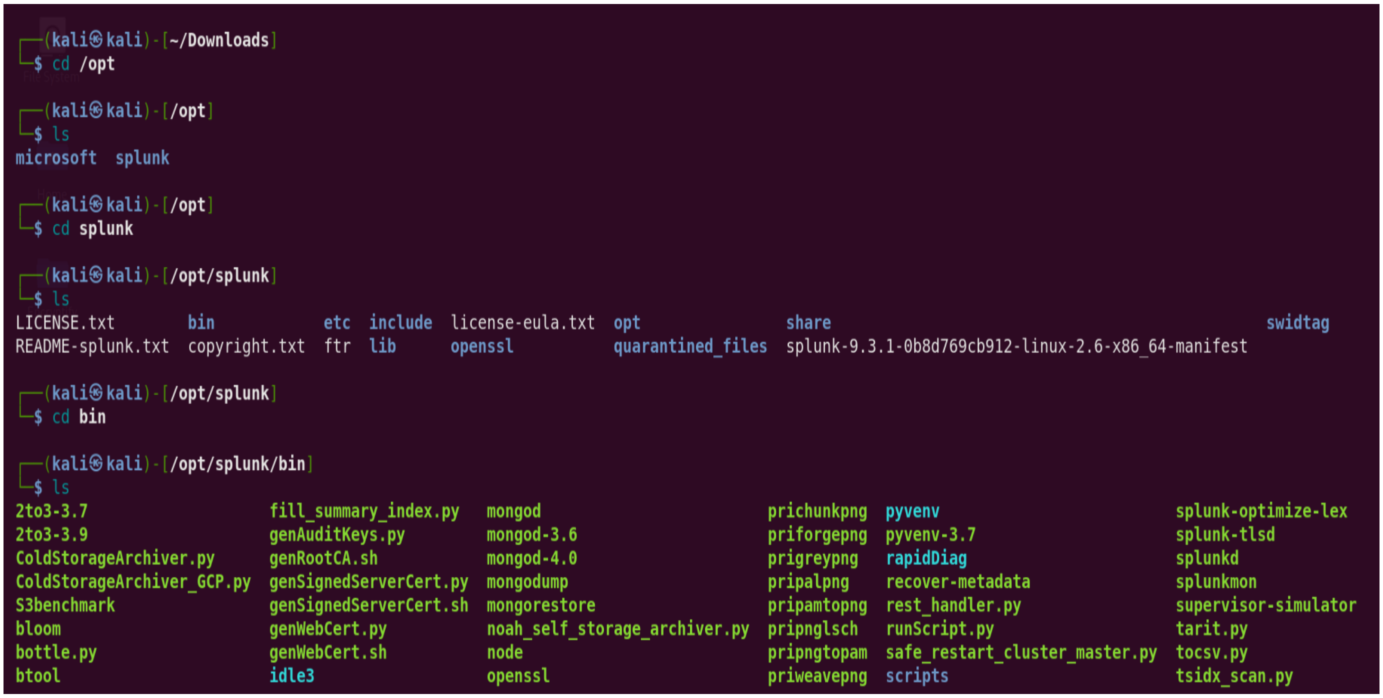
- The complete process to download splunk is shown using screenshots for better understanding .



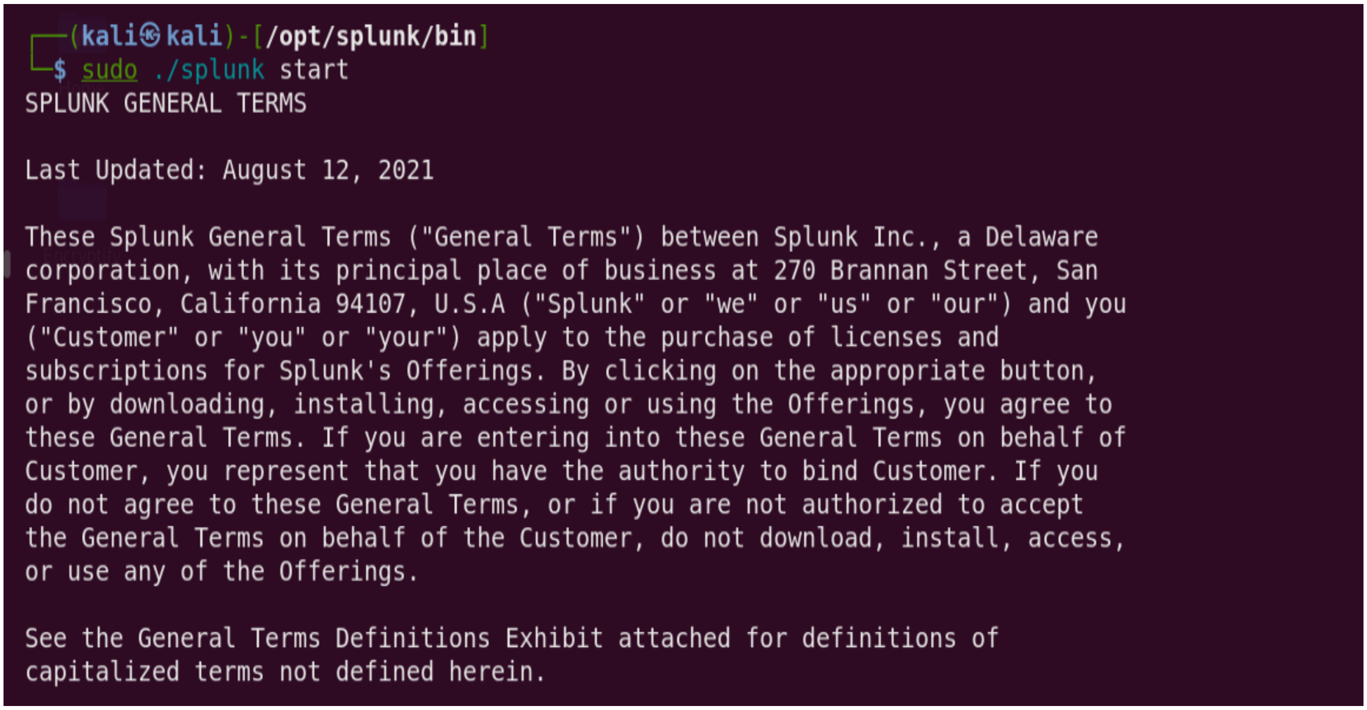
```
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
Screenshot_20240810-180713.png  disk.flag.img  flag.txt      rsa-wiener-attack                              study-guide.txt
dachshund.jpg                   encrypt.py     geosint2.jpg  splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.deb
```



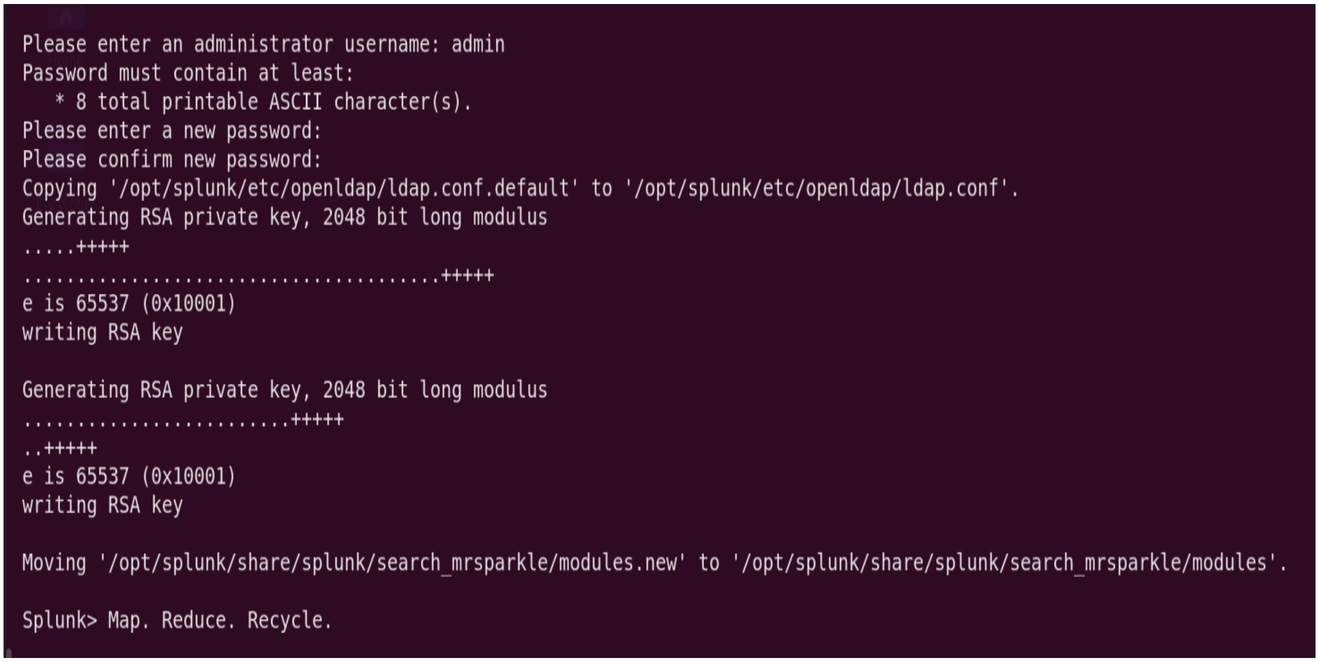
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo dpkg -i splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.deb
[sudo] password for kali:
Selecting previously unselected package splunk.
(Reading database ... 443814 files and directories currently installed.)
Preparing to unpack splunk-9.3.1-0b8d769cb912-linux-2.6-amd64.deb ...
Unpacking splunk (9.3.1) ...
Setting up splunk (9.3.1) ...
complete
```



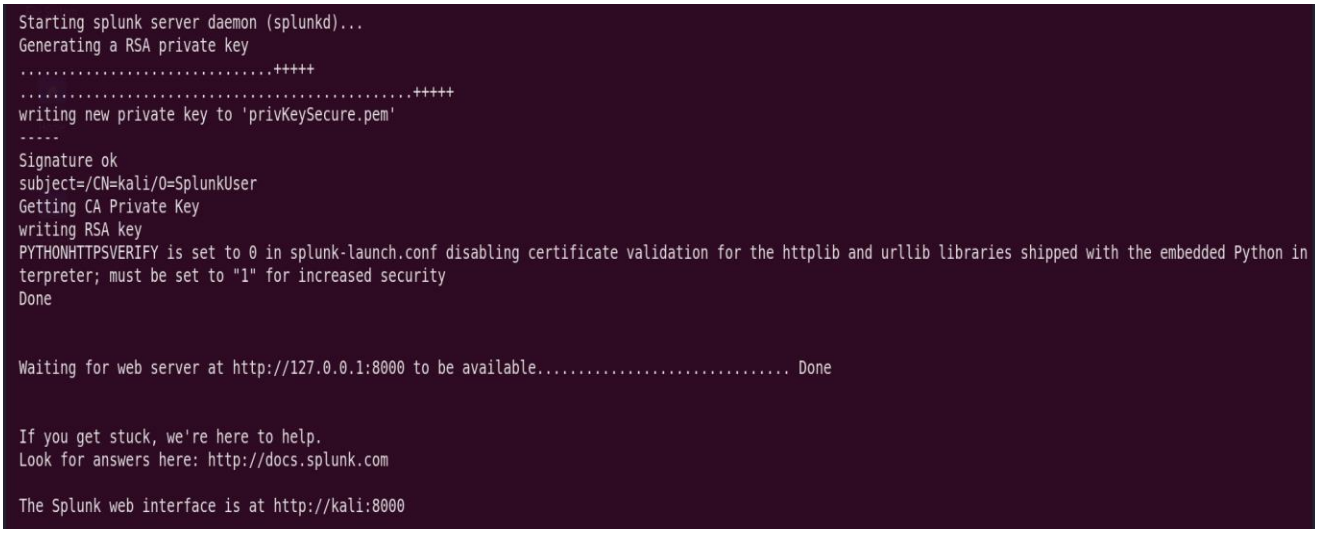
```
┌──(kali㉿kali)-[~/Downloads]
└─$ cd /opt

┌──(kali㉿kali)-[/opt]
└─$ ls
microsoft  splunk

┌──(kali㉿kali)-[/opt]
└─$ cd splunk

┌──(kali㉿kali)-[/opt/splunk]
└─$ ls
LICENSE.txt        bin            etc  include  license-eula.txt  opt                share                                                swidtag
README-splunk.txt  copyright.txt  ftr  lib      openssl           quarantined_files  splunk-9.3.1-0b8d769cb912-linux-2.6-x86_64-manifest

┌──(kali㉿kali)-[/opt/splunk]
└─$ cd bin

┌──(kali㉿kali)-[/opt/splunk/bin]
└─$ ls
2to3-3.7                    fill_summary_index.py   mongod                         prichunkpng  pyvenv                          splunk-optimize-lex
2to3-3.9                    genAuditKeys.py         mongod-3.6                     priforgepng  pyvenv-3.7                      splunk-tlsd
ColdStorageArchiver.py      genRootCA.sh            mongod-4.0                     prigreypng   rapidDiag                       splunkd
ColdStorageArchiver_GCP.py  genSignedServerCert.py  mongodump                      pripalpng    recover-metadata                splunkmon
S3benchmark                 genSignedServerCert.sh  mongorestore                   pripamtopng  rest_handler.py                 supervisor-simulator
bloom                       genWebCert.py           noah_self_storage_archiver.py  pripnglsch   runScript.py                    tarit.py
bottle.py                   genWebCert.sh           node                           pripngtopam  safe_restart_cluster_master.py  tocsv.py
btool                       idle3                   openssl                        priweavepng  scripts                         tsidx_scan.py
```



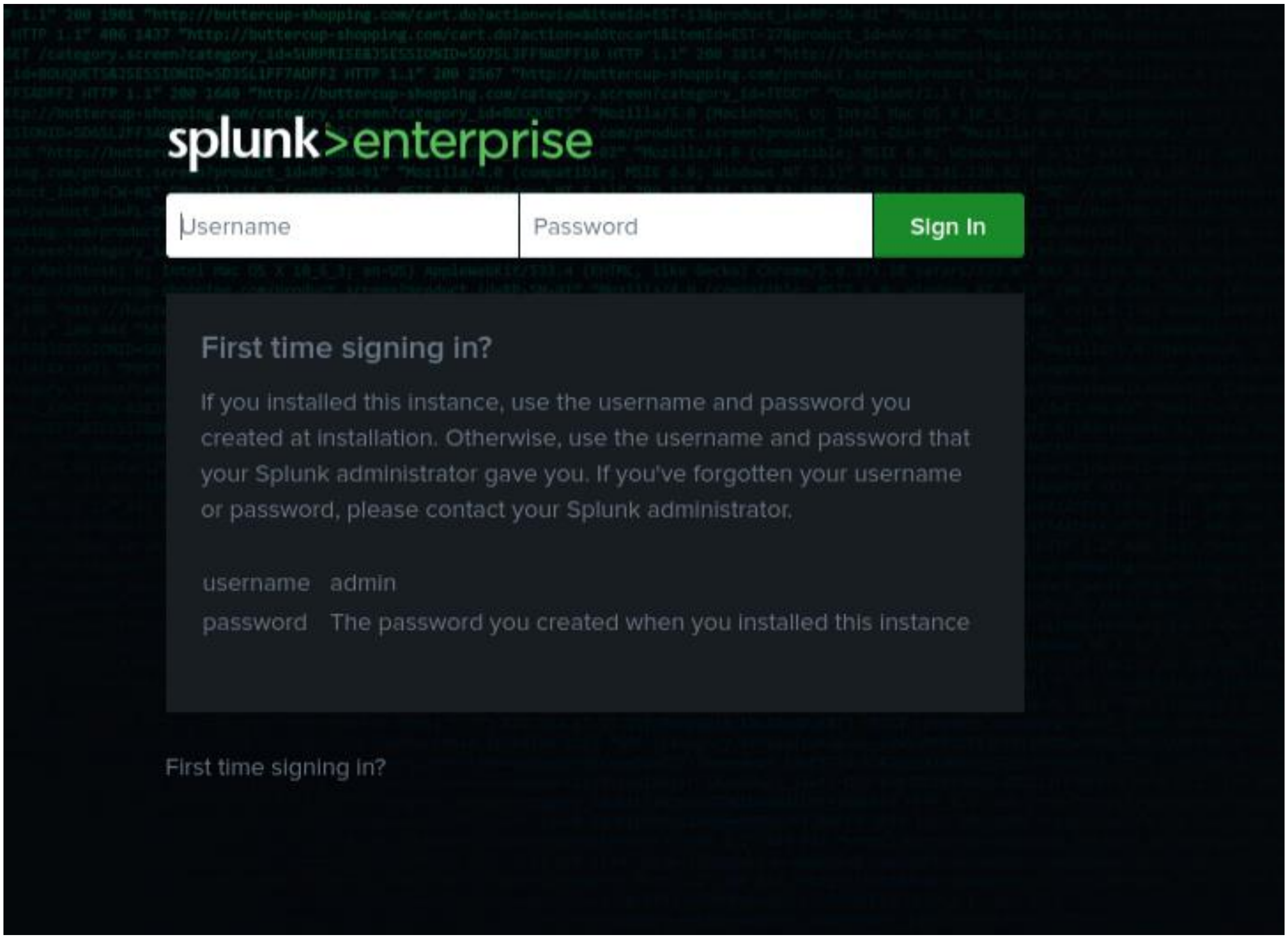
```
┌──(kali㉿kali)-[/opt/splunk/bin]
└─$ sudo ./splunk start
SPLUNK GENERAL TERMS

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.
```



```
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
.....+++++
.......................................+++++
e is 65537 (0x10001)
writing RSA key

Generating RSA private key, 2048 bit long modulus
.........................+++++
..+++++
e is 65537 (0x10001)
writing RSA key

Moving '/opt/splunk/share/splunk/search_mrsparkle/modules.new' to '/opt/splunk/share/splunk/search_mrsparkle/modules'.

Splunk> Map. Reduce. Recycle.
```



```
Starting splunk server daemon (splunkd)...
Generating a RSA private key
...............................+++++
................................................+++++
writing new private key to 'privKeySecure.pem'
-----
Signature ok
subject=/CN=kali/O=SplunkUser
Getting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python in
terpreter; must be set to "1" for increased security
Done


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://kali:8000
```



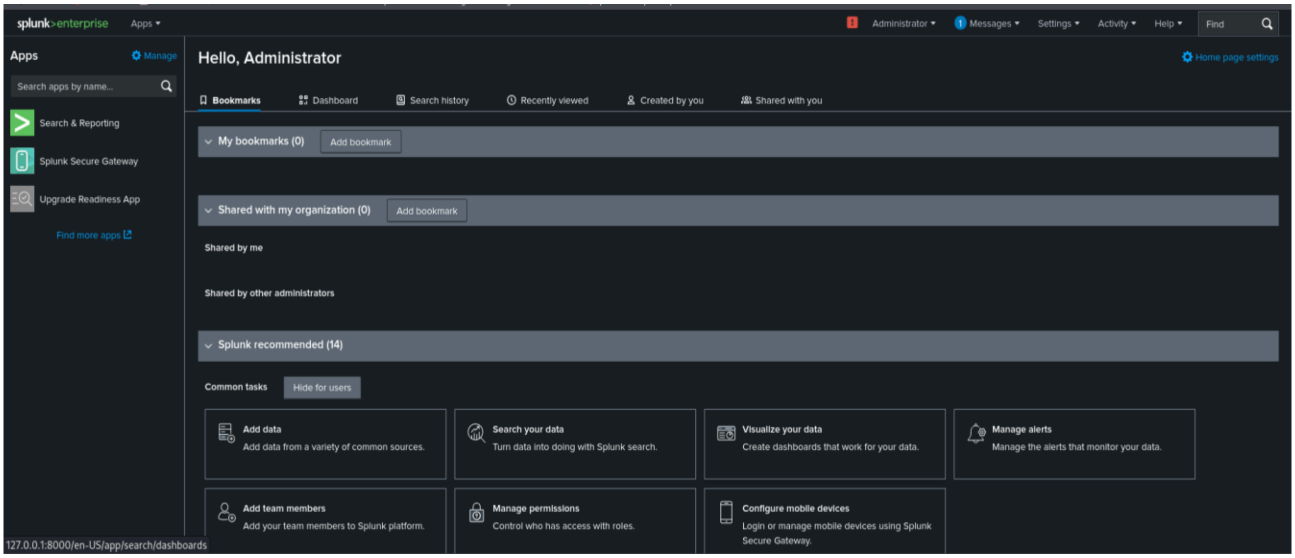
First time signing in?

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?



Hello, Administrator

My bookmarks (0)

Shared with my organization (0)

Shared by me

Shared by other administrators

Splunk recommended (14)

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.

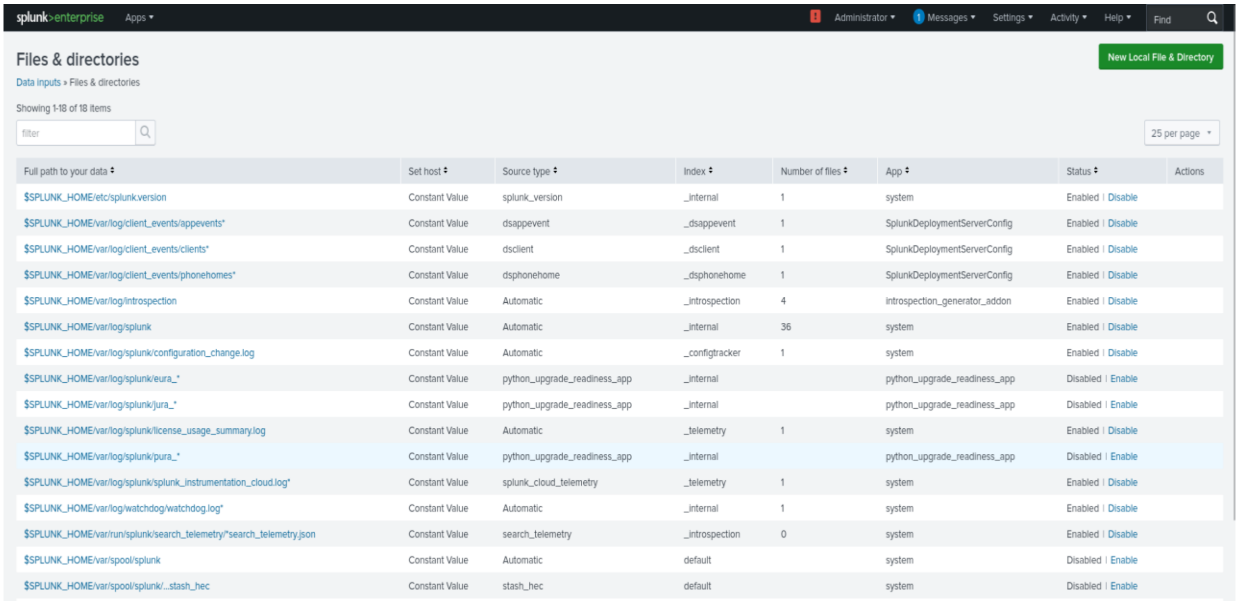
Manage alerts
Manage the alerts that monitor your data.

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.

127.0.0.1:8000/en-US/app/search/dashboards



Files & directories

Data inputs » Files & directories

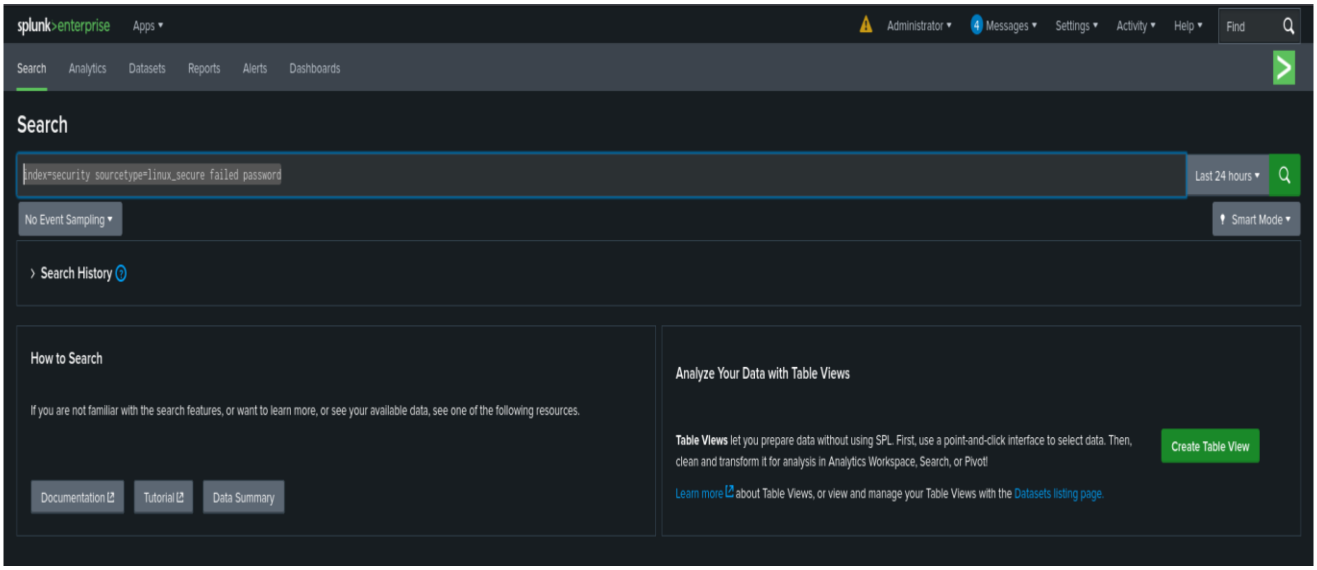
Showing 1-18 of 18 items

Full path to your data	Set host	Source type	Index	Number of files	App	Status	Actions
$SPLUNK_HOME/etc/splunk.version	Constant Value	splunk_version	_internal	1	system	Enabled | Disable	
$SPLUNK_HOME/var/log/client_events/appevents*	Constant Value	dsappevent	_dsappevent	1	SplunkDeploymentServerConfig	Enabled | Disable	
$SPLUNK_HOME/var/log/client_events/clients*	Constant Value	dsclient	_dsclient	1	SplunkDeploymentServerConfig	Enabled | Disable	
$SPLUNK_HOME/var/log/client_events/phonehomes*	Constant Value	dsphonehome	_dsphonehome	1	SplunkDeploymentServerConfig	Enabled | Disable	
$SPLUNK_HOME/var/log/introspection	Constant Value	Automatic	_introspection	4	introspection_generator_addon	Enabled | Disable	
$SPLUNK_HOME/var/log/splunk	Constant Value	Automatic	_internal	36	system	Enabled | Disable	
$SPLUNK_HOME/var/log/splunk/configuration_change.log	Constant Value	Automatic	_configtracker	1	system	Enabled | Disable	
$SPLUNK_HOME/var/log/splunk/eura_*	Constant Value	python_upgrade_readiness_app	_internal		python_upgrade_readiness_app	Disabled | Enable	
$SPLUNK_HOME/var/log/splunk/jura_*	Constant Value	python_upgrade_readiness_app	_internal		python_upgrade_readiness_app	Disabled | Enable	
$SPLUNK_HOME/var/log/splunk/license_usage_summary.log	Constant Value	Automatic	_telemetry	1	system	Enabled | Disable	
$SPLUNK_HOME/var/log/splunk/pura_*	Constant Value	python_upgrade_readiness_app	_internal		python_upgrade_readiness_app	Disabled | Enable	
$SPLUNK_HOME/var/log/splunk/splunk_instrumentation_cloud.log*	Constant Value	splunk_cloud_telemetry	_telemetry	1	system	Enabled | Disable	
$SPLUNK_HOME/var/log/watchdog/watchdog.log*	Constant Value	Automatic	_internal	1	system	Enabled | Disable	
$SPLUNK_HOME/var/run/splunk/search_telemetry/*search_telemetry.json	Constant Value	search_telemetry	_introspection	0	system	Enabled | Disable	
$SPLUNK_HOME/var/spool/splunk	Constant Value	Automatic	default		system	Disabled | Enable	
$SPLUNK_HOME/var/spool/splunk/...stash_hec	Constant Value	stash_hec	default		system	Disabled | Enable	

So, this is the complete procedure to set up splunk in your system . I tried to provide SC's for each step to completely clear any confusion if any present.

Setting up Alert Conf:

In the next section we will set up alert configuration for incorrect password attempt . We wil set the conf that if wrong password for sudo is entered multiple times alert will be generated for this.

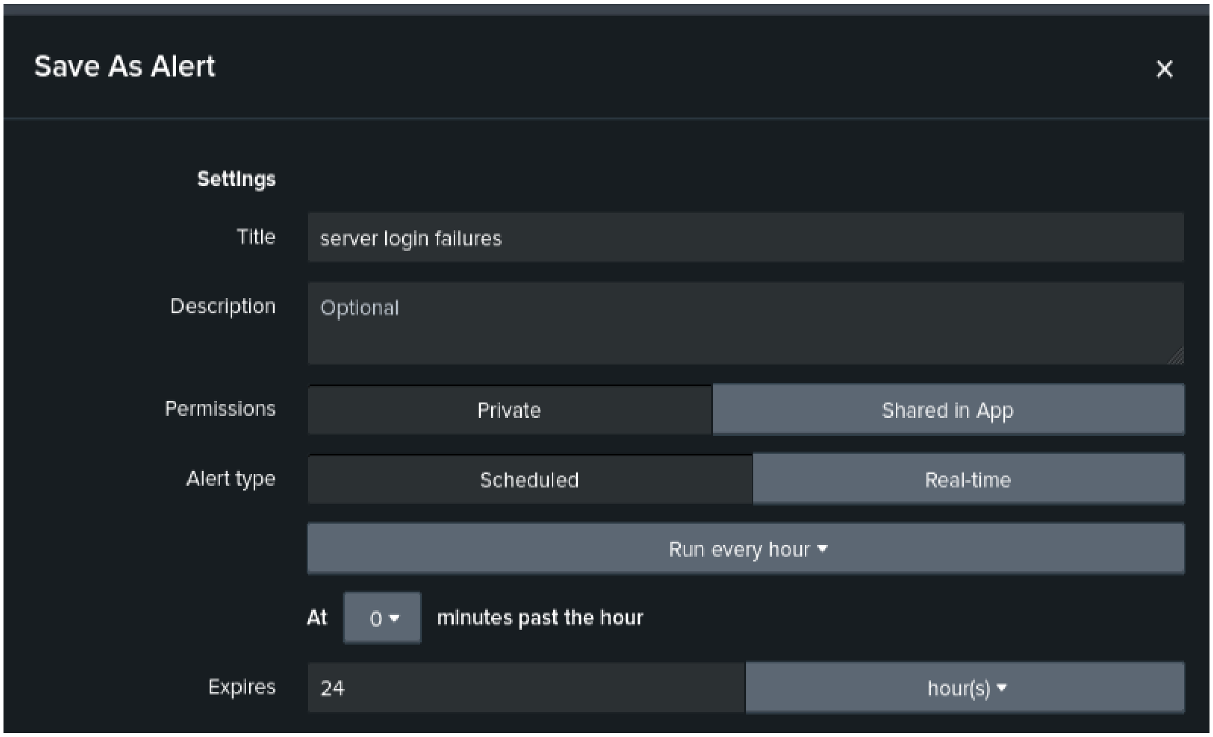


```
index=security sourcetype=linux_secure failed password
```

If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.

Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!

Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.



Save As Alert

Settings

Title: server login failures

Description: Optional

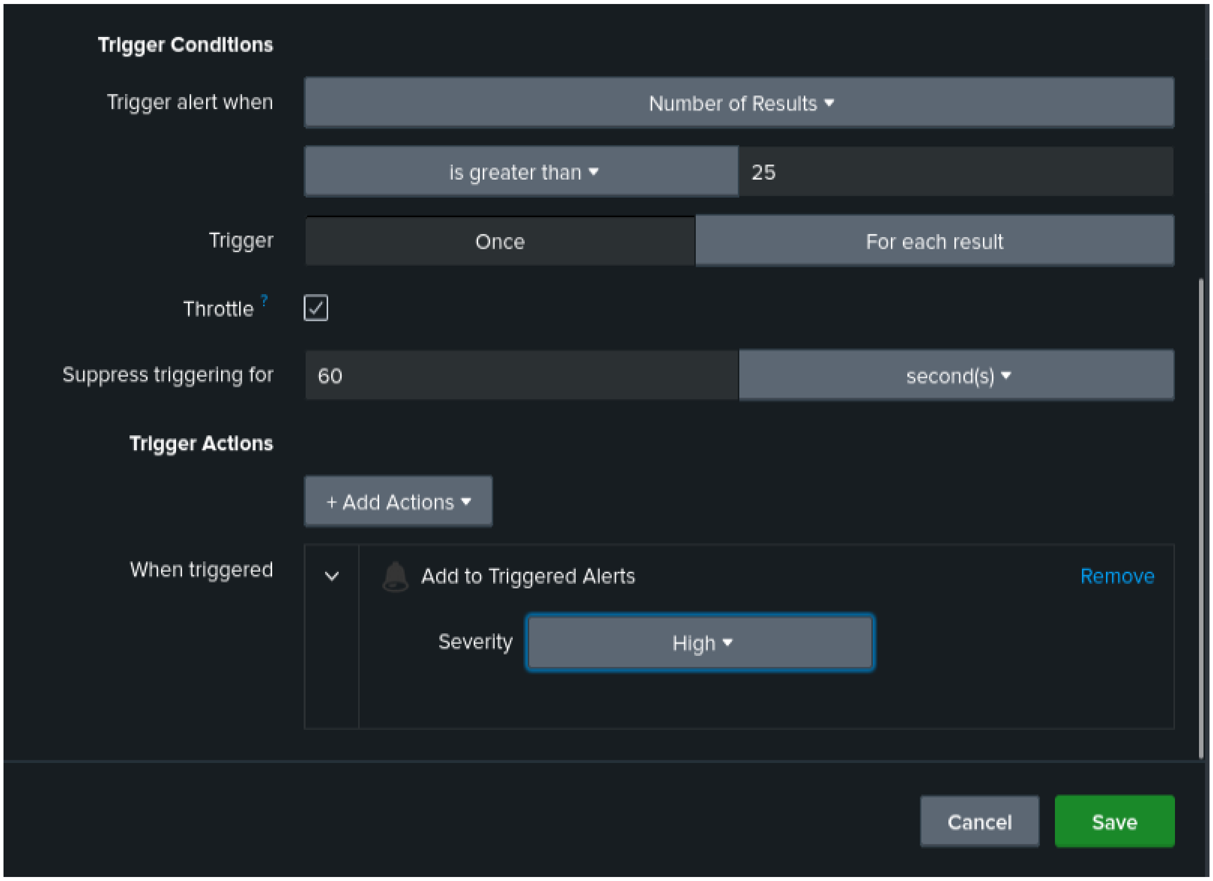
Permissions: Private | Shared in App

Alert type: Scheduled | Real-time

Run every hour ▾

At 0 ▾ minutes past the hour

Expires: 24 | hour(s) ▾



Trigger Conditions

Trigger alert when: Number of Results ▾

is greater than ▾ | 25

Trigger: Once | For each result

Throttle ? ☑

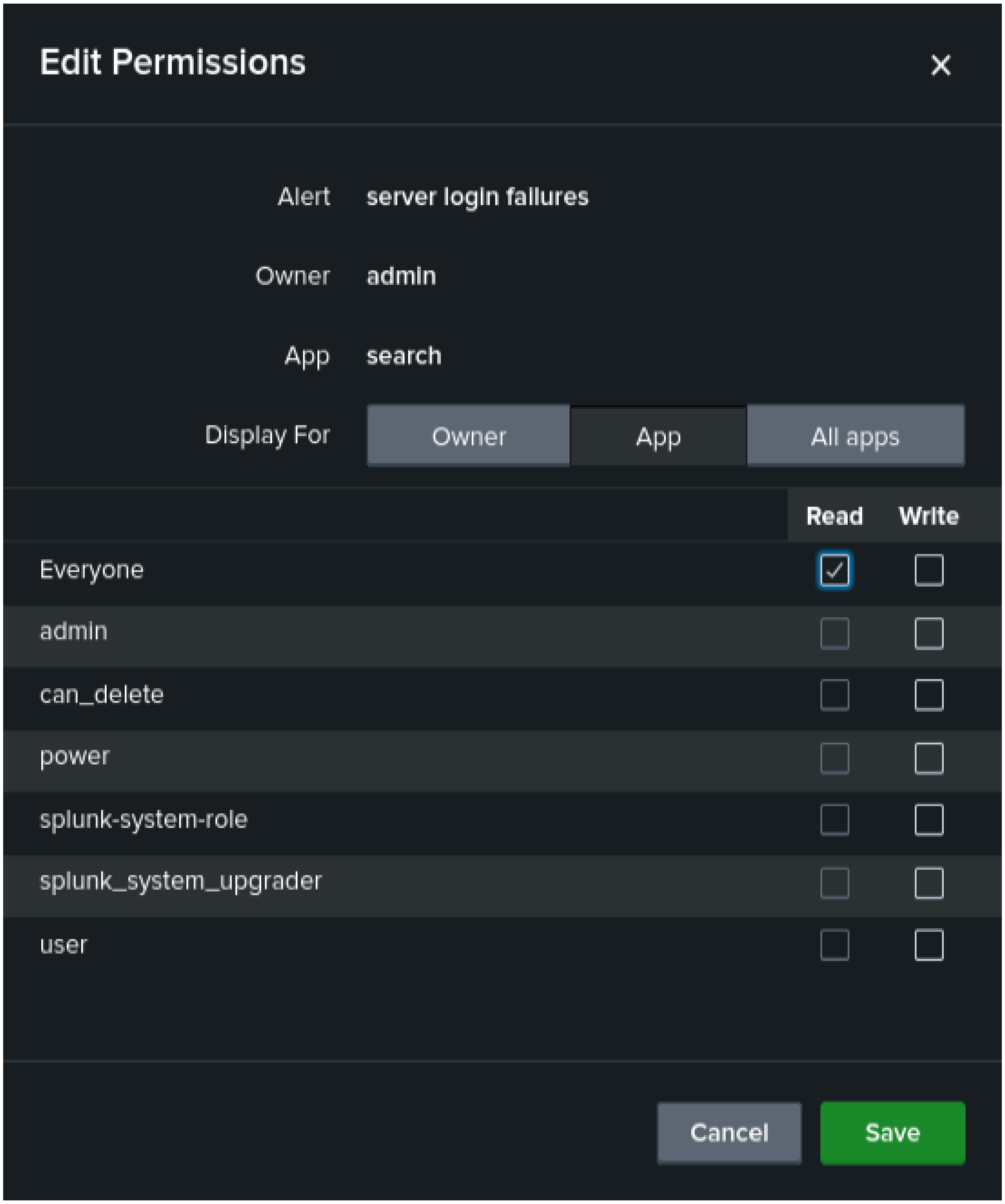
Suppress triggering for: 60 | second(s) ▾

Trigger Actions

+ Add Actions ▾

When triggered: Add to Triggered Alerts — Remove

Severity: High ▾



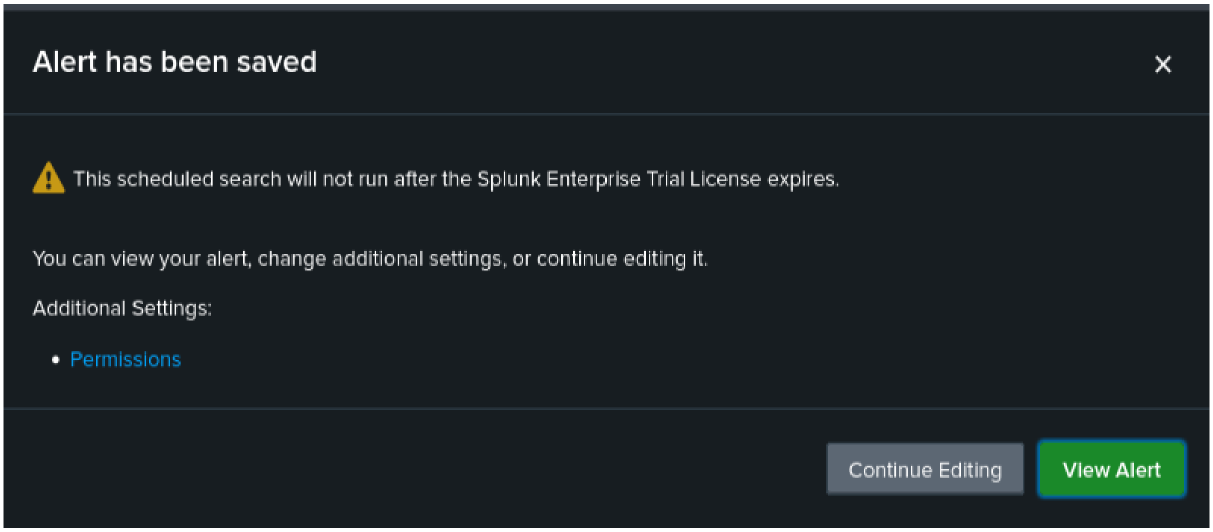
Alert server login failures

Owner admin

App search

Display For Owner App All apps

	Read	Write
Everyone	☑	☐
admin	☐	☐
can_delete	☐	☐
power	☐	☐
splunk-system-role	☐	☐
splunk_system_upgrader	☐	☐
user	☐	☐



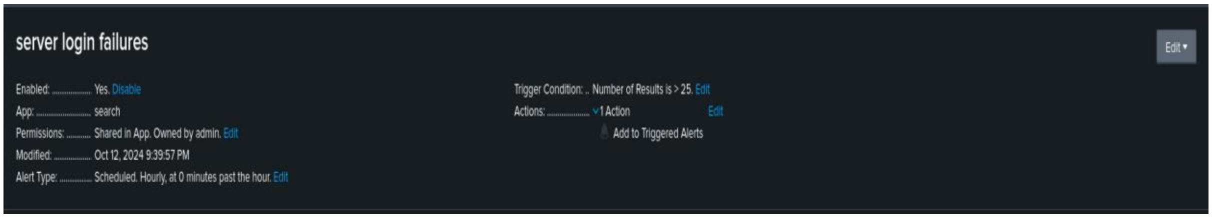
Alert has been saved

This scheduled search will not run after the Splunk Enterprise Trial License expires.

You can view your alert, change additional settings, or continue editing it.

Additional Settings:

- Permissions



server login failures

```
Enabled: ............... Yes. Disable          Trigger Condition: .. Number of Results is > 25. Edit
App: ...................... search                Actions: ................. ✓1 Action          Edit
Permissions: ........... Shared in App. Owned by admin. Edit      Add to Triggered Alerts
Modified: ................ Oct 12, 2024 9:39:57 PM
Alert Type: ............. Scheduled. Hourly, at 0 minutes past the hour. Edit
```

By following these steps , we have set an alert to incorrect password login attempts foe sudo previlages in a linux system.