

Splunk Cheatsheet

Connection

splunk login

Connect to Splunk server with credentials

splunk login --uri=https://splunk.example.com:8089

Connect to a specific Splunk instance

splunk logout

End the current session

Search Commands

search "error"

Search for events containing 'error'

**index=main sourcetype=access_combined | stats
count by status**

Search main index and count by status field

| tstats count where index=* by index

Show event counts across all indexes

earliest=-24h latest=now

Time range modifier for the last 24 hours

| timechart span=1h count

Create time-based chart with hourly buckets

Data Manipulation

| table field1 field2

Display only specified fields in table format

| sort -count

Sort results by count descending

| rename field1 as "User Friendly Name"

Rename fields for display

| dedup username

Remove duplicate events based on username field

| eval newField=field1+field2

Create calculated fields

Alerts and Dashboards

| savedsearch name="My Saved Search"

Save current search

| sendalert email to="user@example.com"

Send email alert

| addtotals fieldname=total

Add totals to numeric fields

| geom

Generate geographical visualization

Data Input

splunk add monitor /var/log

Monitor a file or directory

splunk add forward-server

splunk.example.com:9997
Add a forwarding destination

splunk add tcp 514

Listen for data on TCP port

splunk add udp 514

Listen for data on UDP port

Administration

splunk start

Start Splunk services

splunk stop

Stop Splunk services

splunk restart

Restart Splunk services

splunk status

Check Splunk service status

splunk show config

Display current configuration