SSH Log Analysis using Splunk Project

By Gaurav Ghandat

📌 Project Overview

This project focuses on analyzing **SSH authentication logs** using **Splunk** to detect suspicious activities such as brute-force attacks, failed login attempts, unauthorized connections, and successful logins from unknown sources.

The project demonstrates **real-world SOC analyst skills**, including log ingestion, searching, visualization, dashboard creation, and alert configuration.

🎯 Objective

The primary goals of this project are to analyze SSH logs to detect:

- ✅ **Successful SSH logins** (who connected and from where)
- ❌ **Failed login attempts** (possible brute-force or password spraying)
- 🚨 **Multiple failed authentication attempts** (brute-force indicators)
- 🔍 **Connections without authentication** (scanning or incomplete sessions)

By completing this project, you will learn how to:

- Ingest SSH logs into Splunk
- Write SPL queries for log analysis
- Build dashboards and visualizations
- Configure alerts for suspicious behavior

🧪 Lab Setup & Prerequisites

Prerequisites

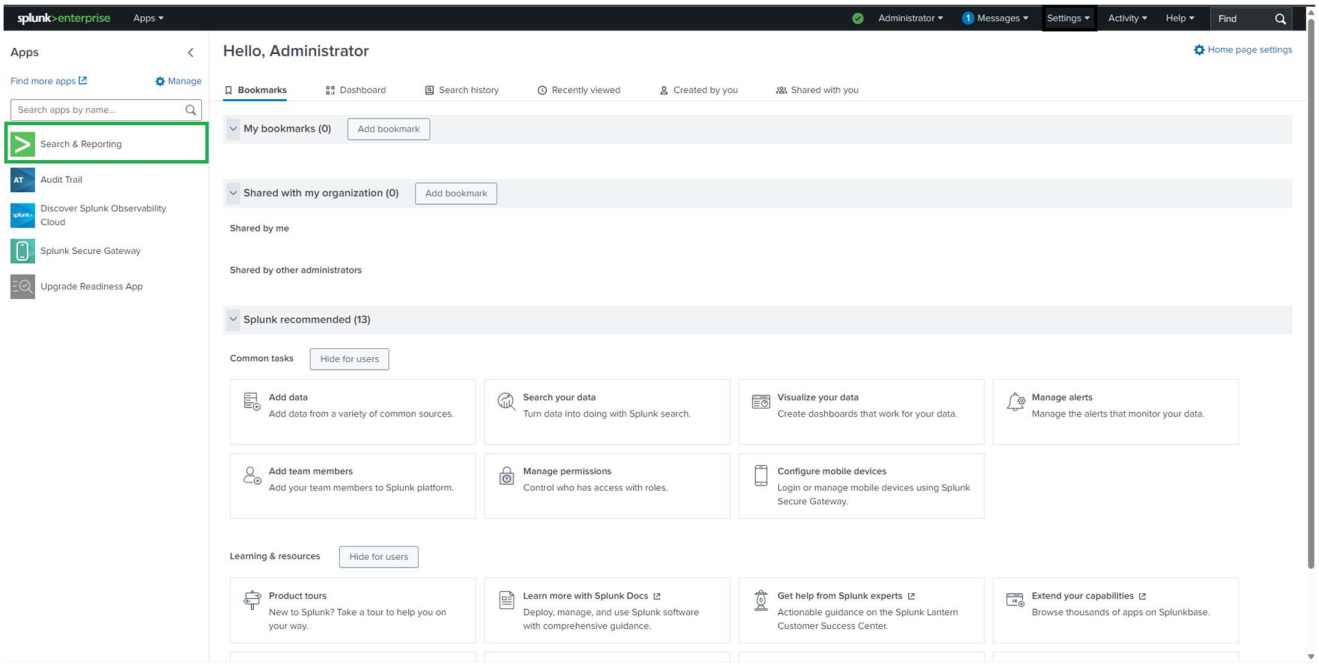
- Splunk Enterprise or Splunk Free installed
- Basic understanding of SPL (Search Processing Language)

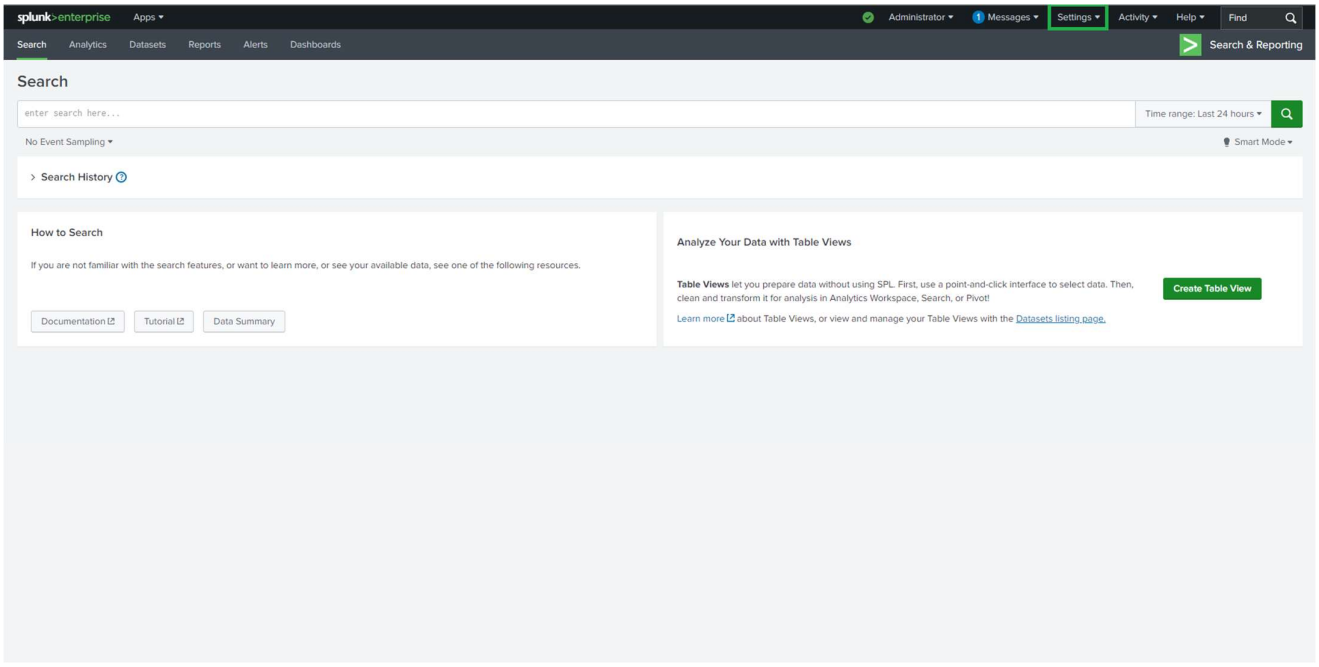
Files Required

- ssh_log.json (SSH authentication logs)

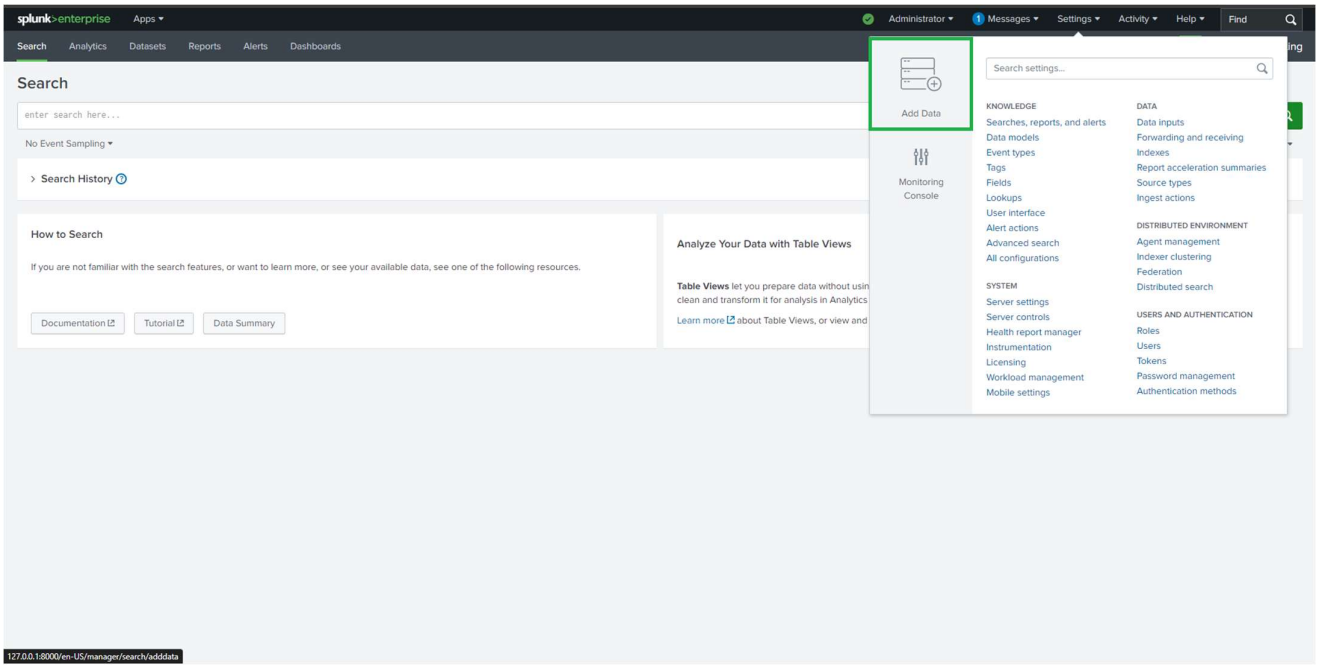
⚙️ Preparation Steps

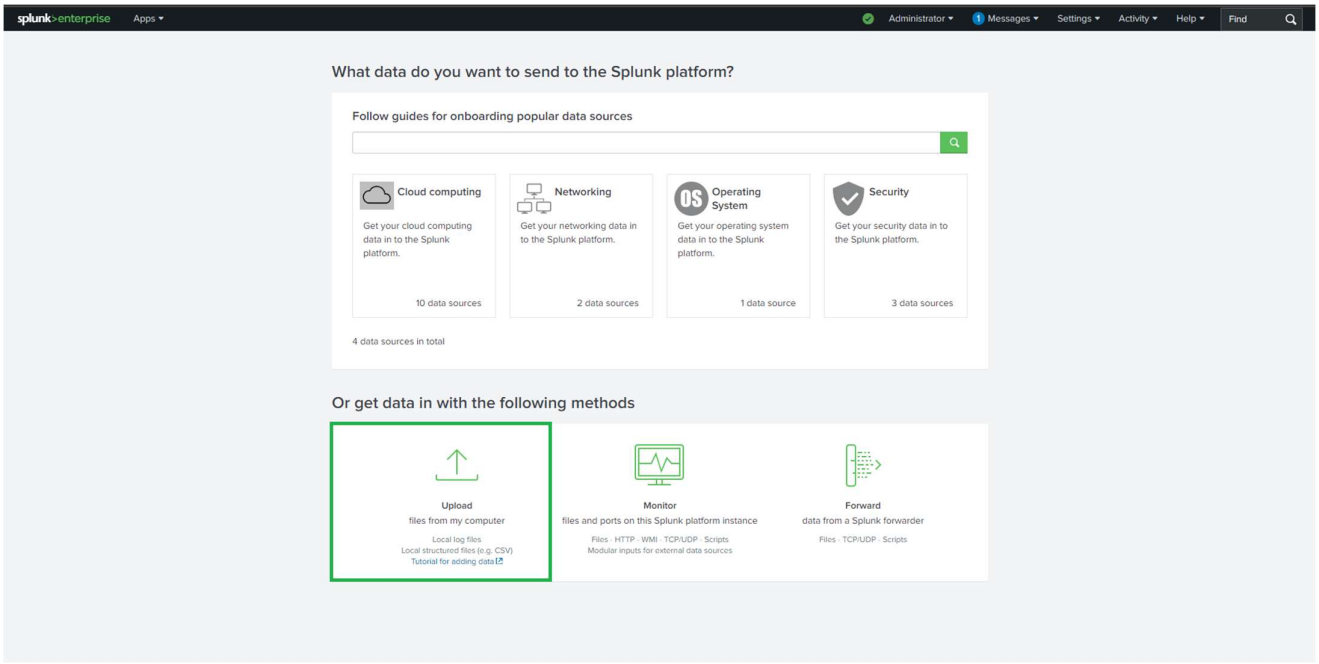
1. Log in to your **Splunk Web Interface**
2. Navigate to: Apps → Search & Reporting



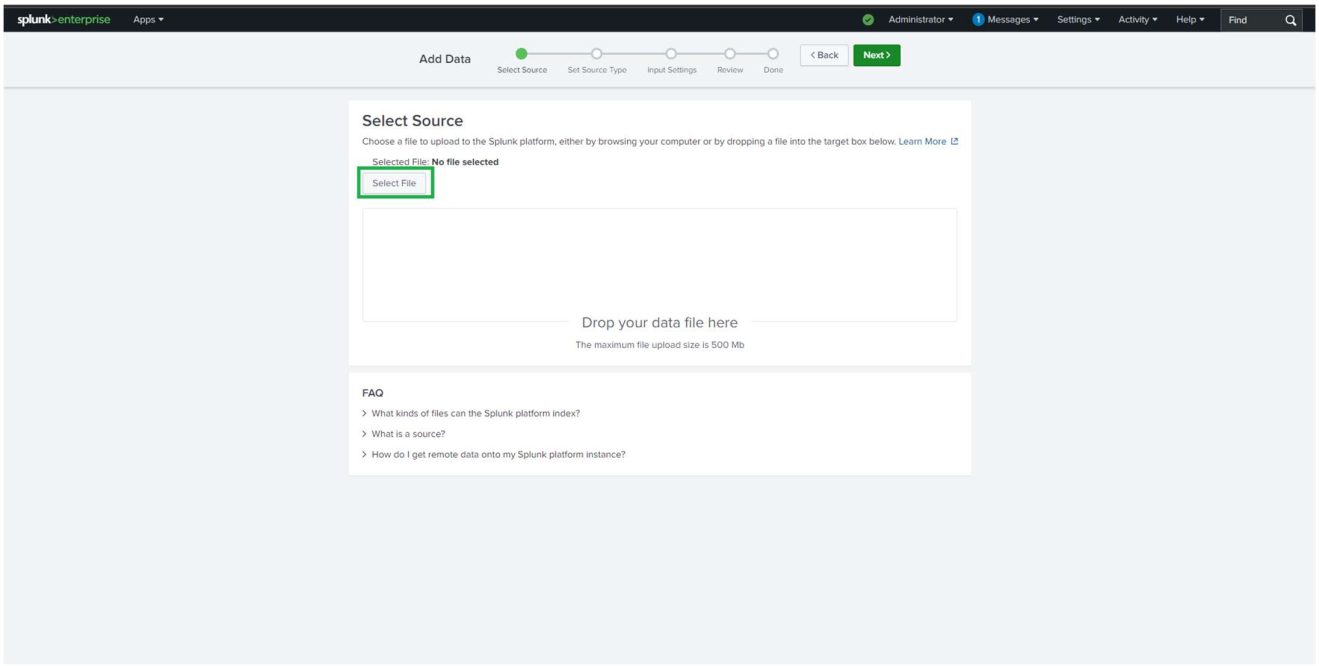


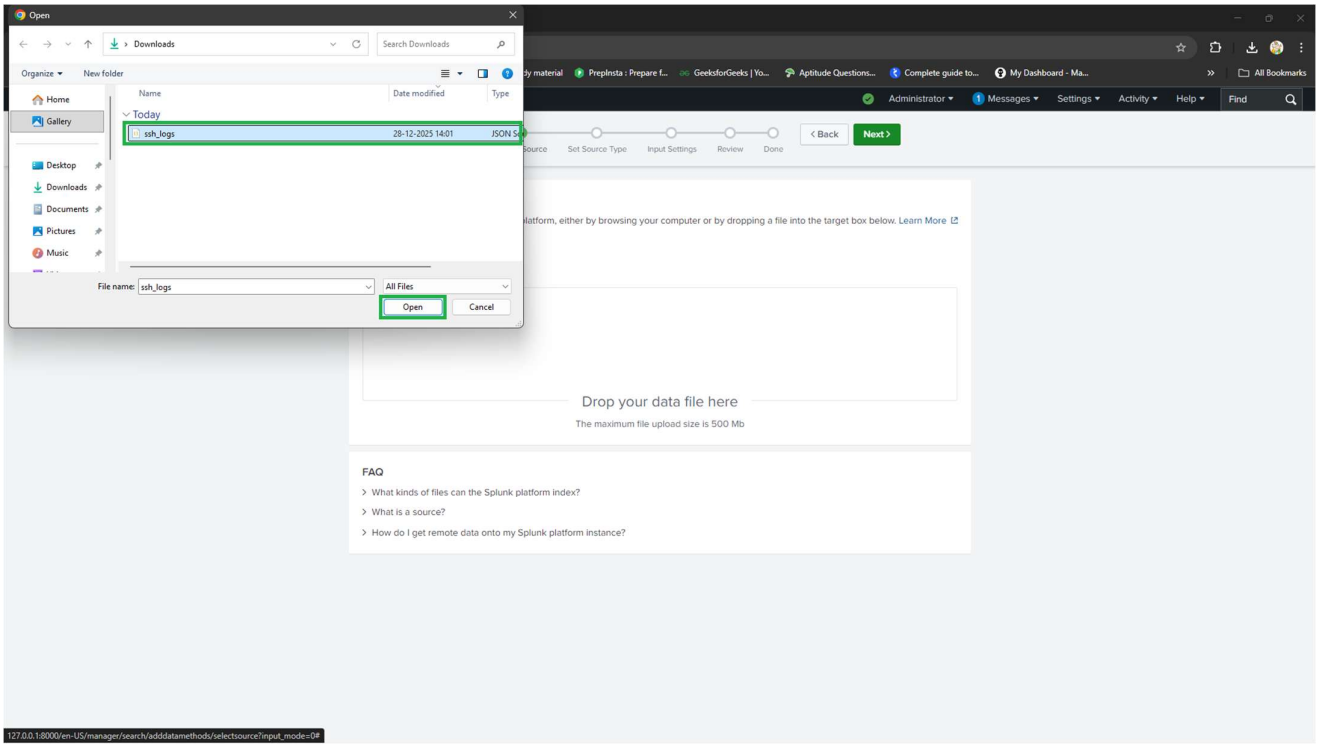
3. Click: Add Data → Upload

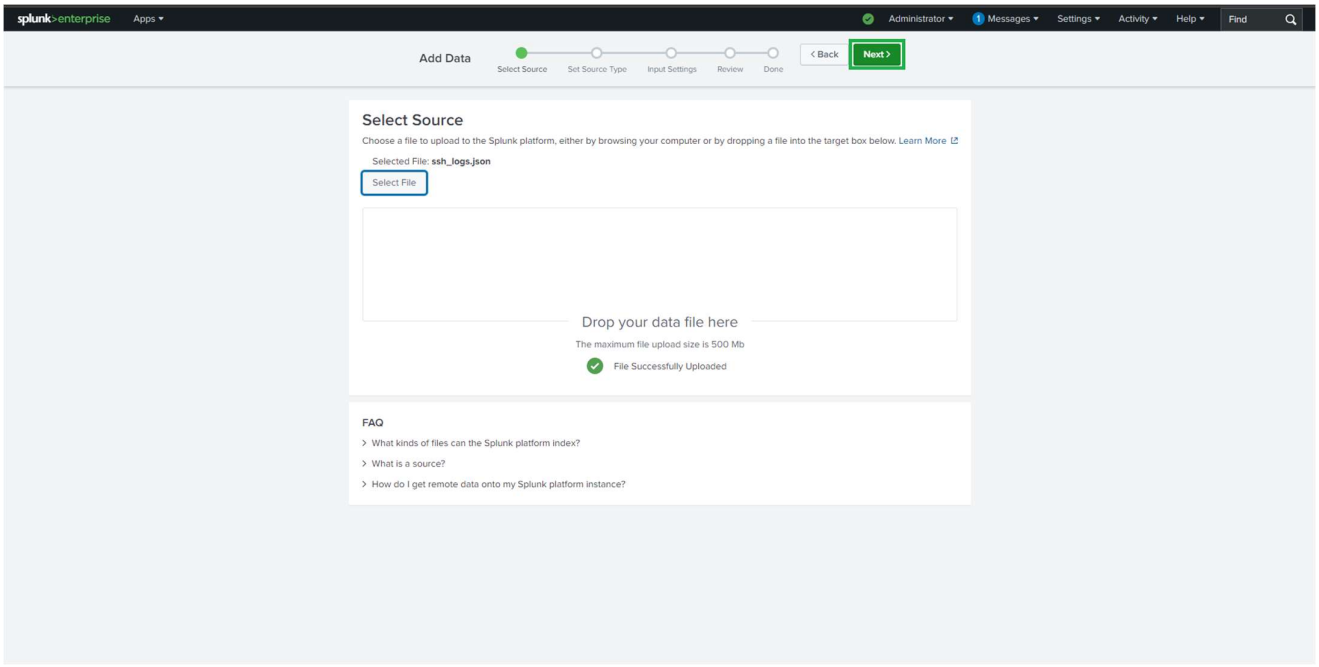




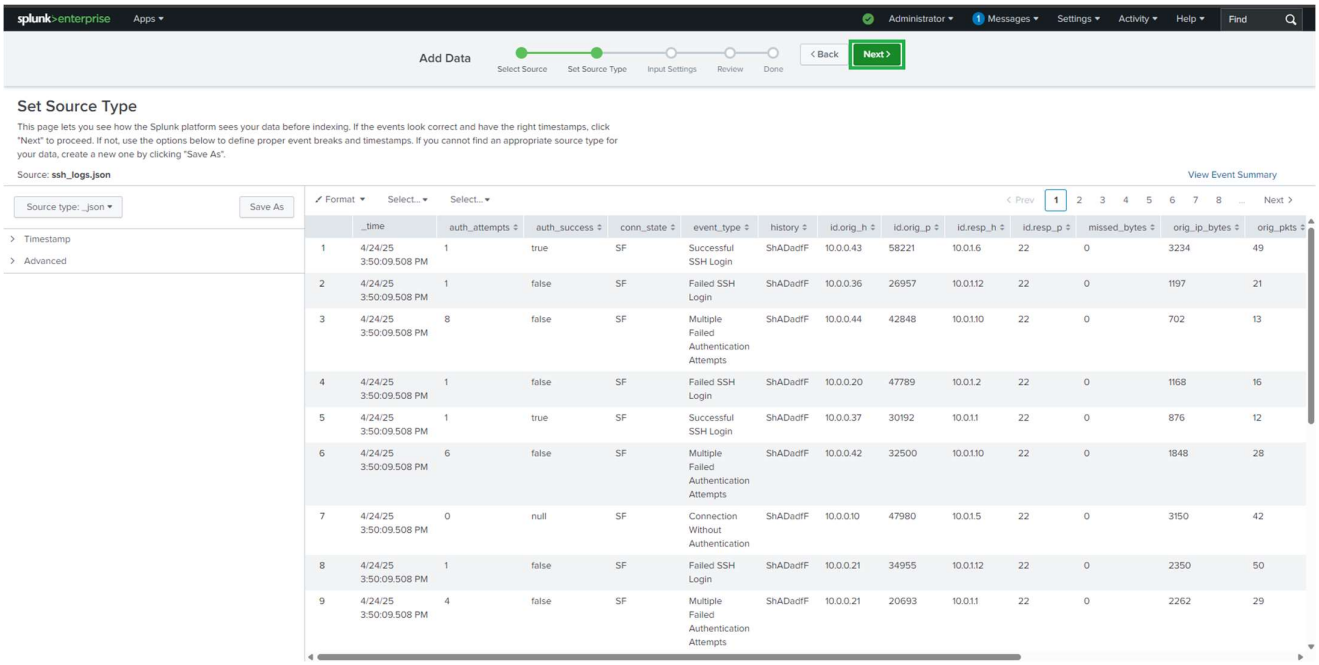
4. Upload the file: ssh_log.json

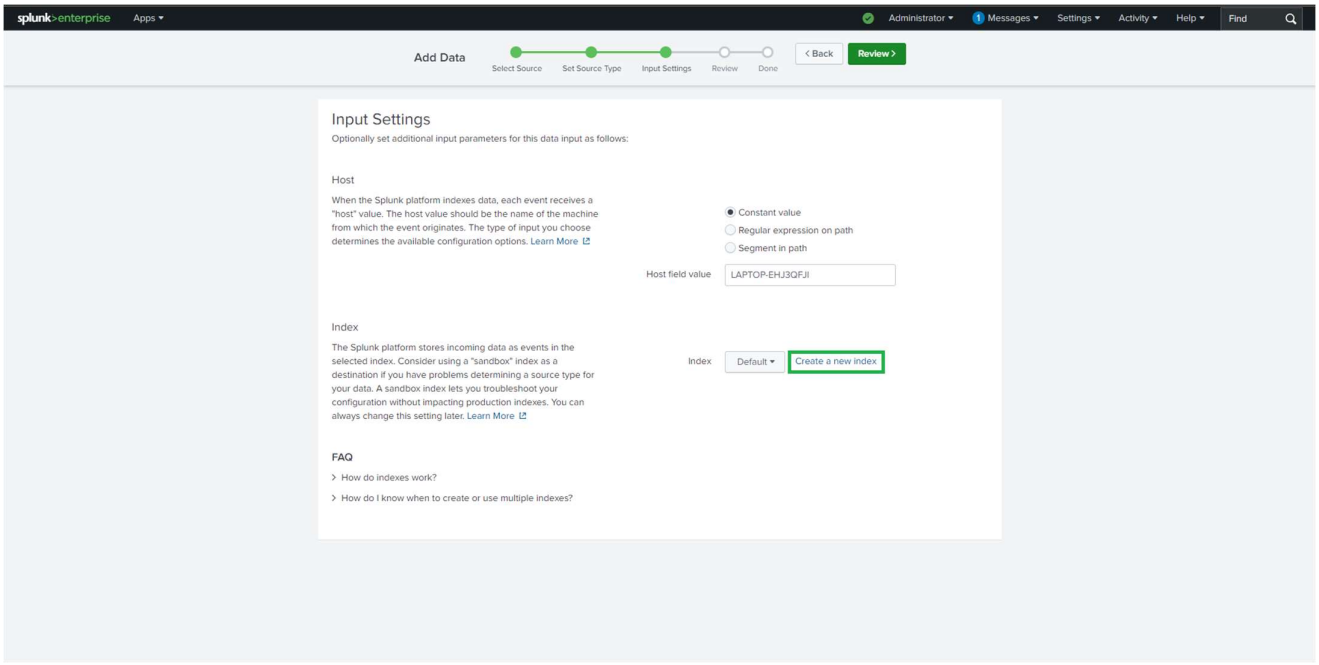


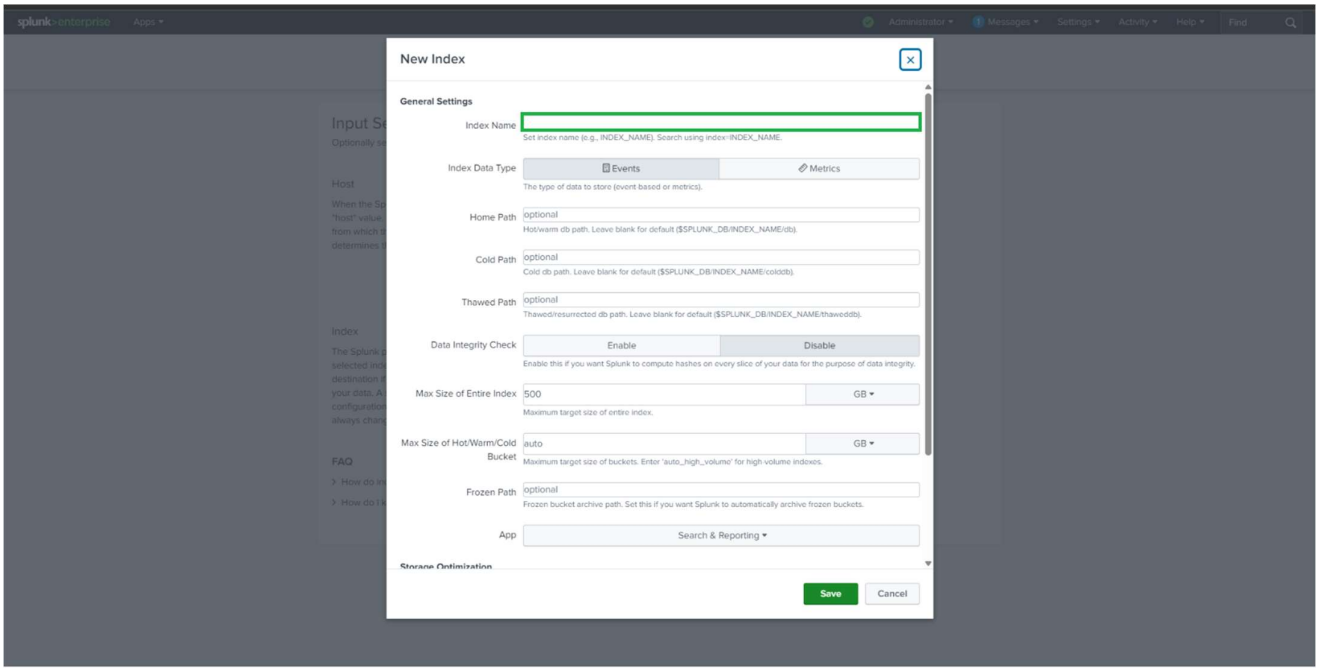


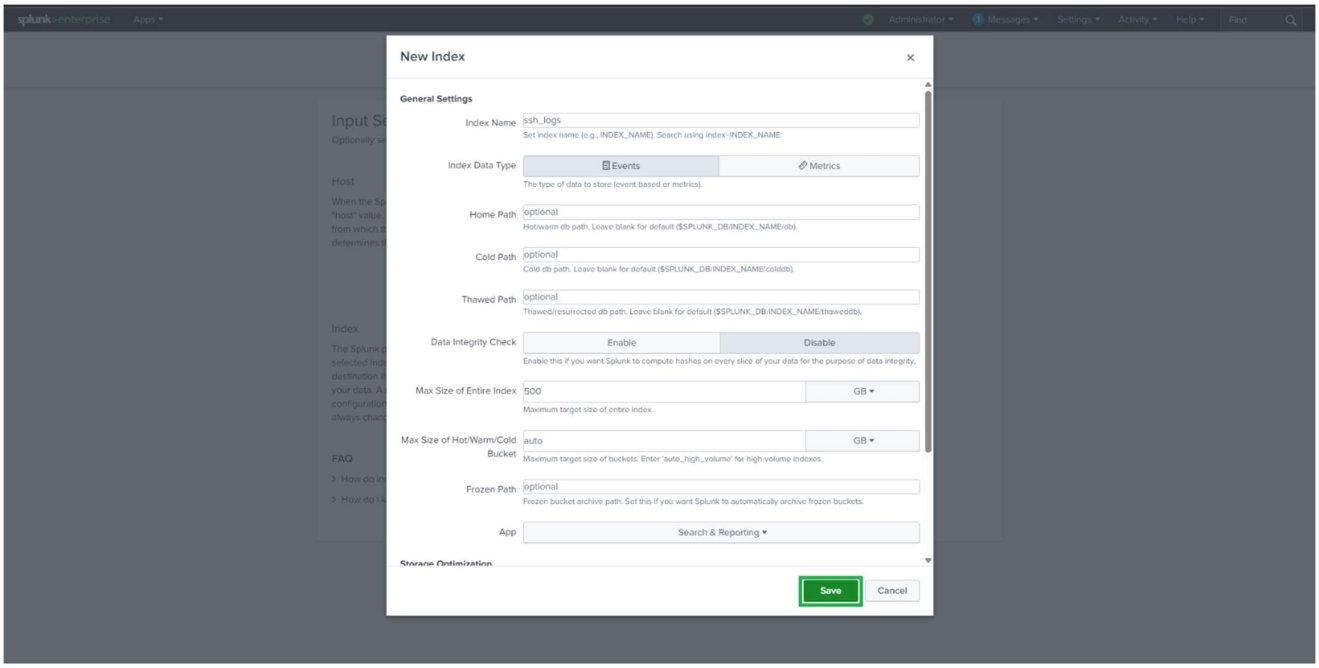


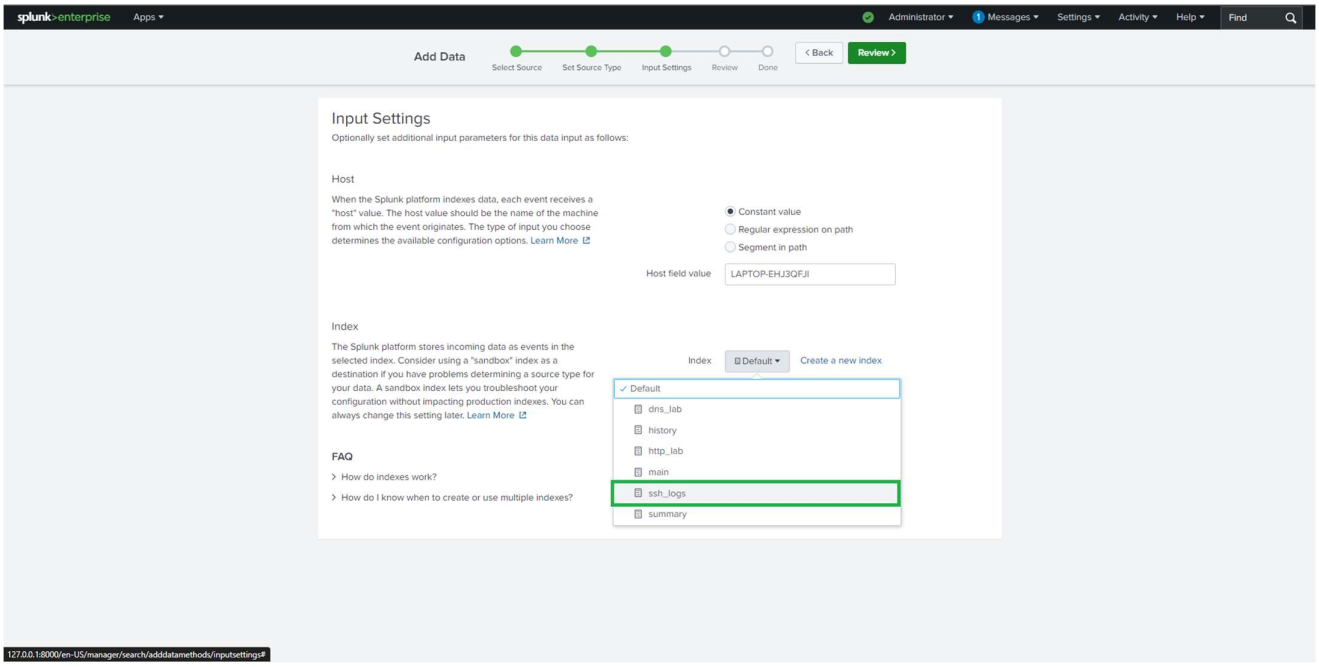
5. Set:
    - **Source type**: _json
    - **Index**: ssh_logs (create a new index)

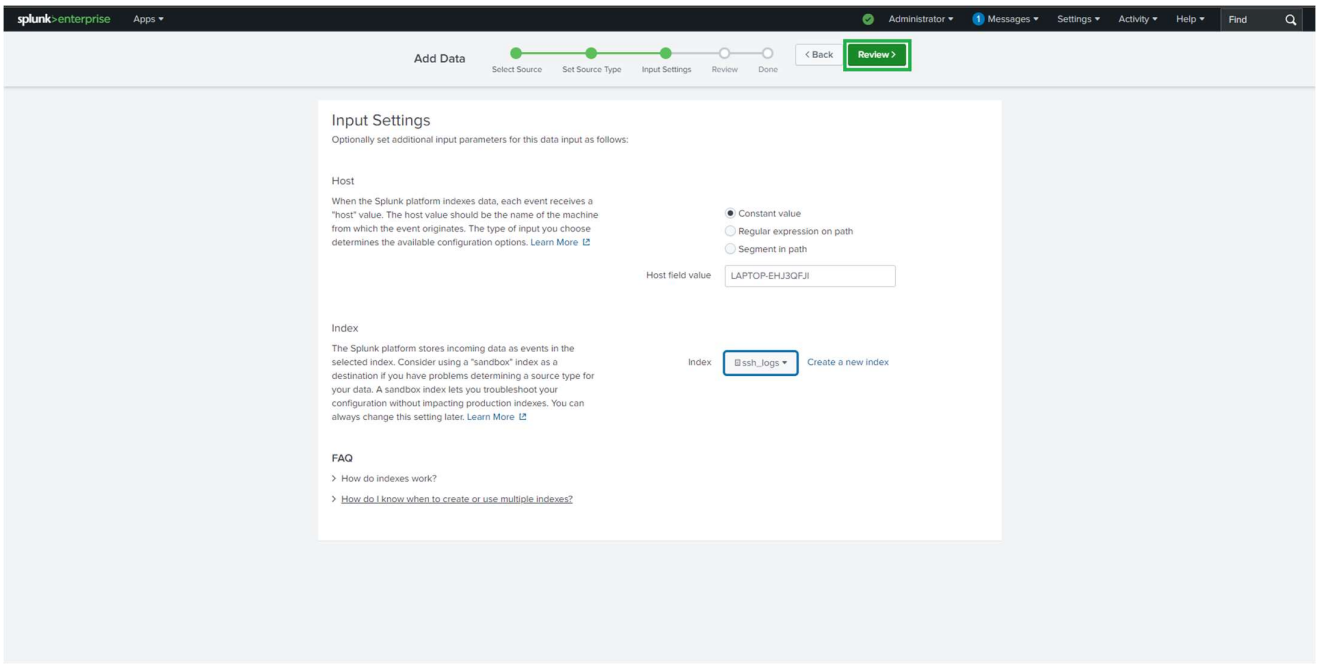


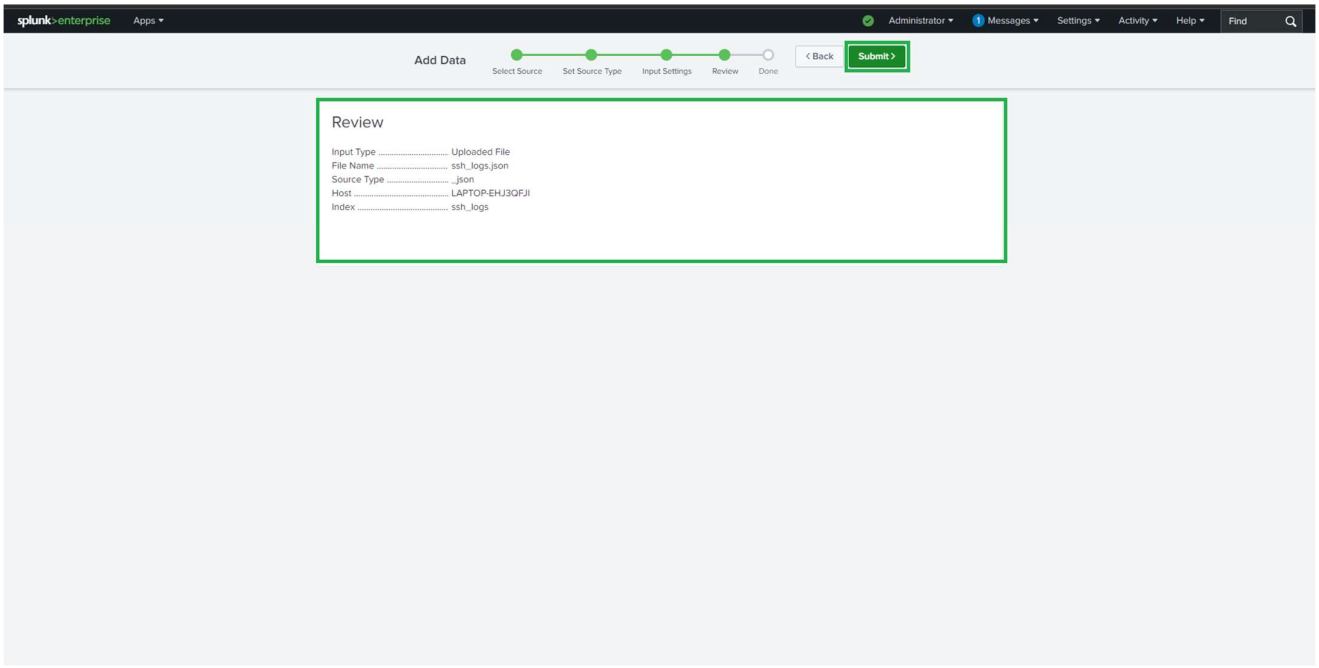

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Review >
Input Settings
Optionally set additional input parameters for this data input as follows:
Host
When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More
Constant value
Regular expression on path
Segment in path
Host field value
LAPTOP-EHJ3QFJI
Index
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More
Index
Default
Create a new index
FAQ
How do indexes work?
How do I know when to create or use multiple indexes?


New Index
General Settings
Index Name
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.
Index Data Type
Events
Metrics
The type of data to store (event based or metrics).
Home Path
optional
Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).
Cold Path
optional
Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).
Thawed Path
optional
Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).
Data Integrity Check
Enable
Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.
Max Size of Entire Index
500
GB
Maximum target size of entire index.
Max Size of Hot/Warm/Cold Bucket
auto
GB
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.
Frozen Path
optional
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.
App
Search & Reporting
Storage Optimization
Save
Cancel

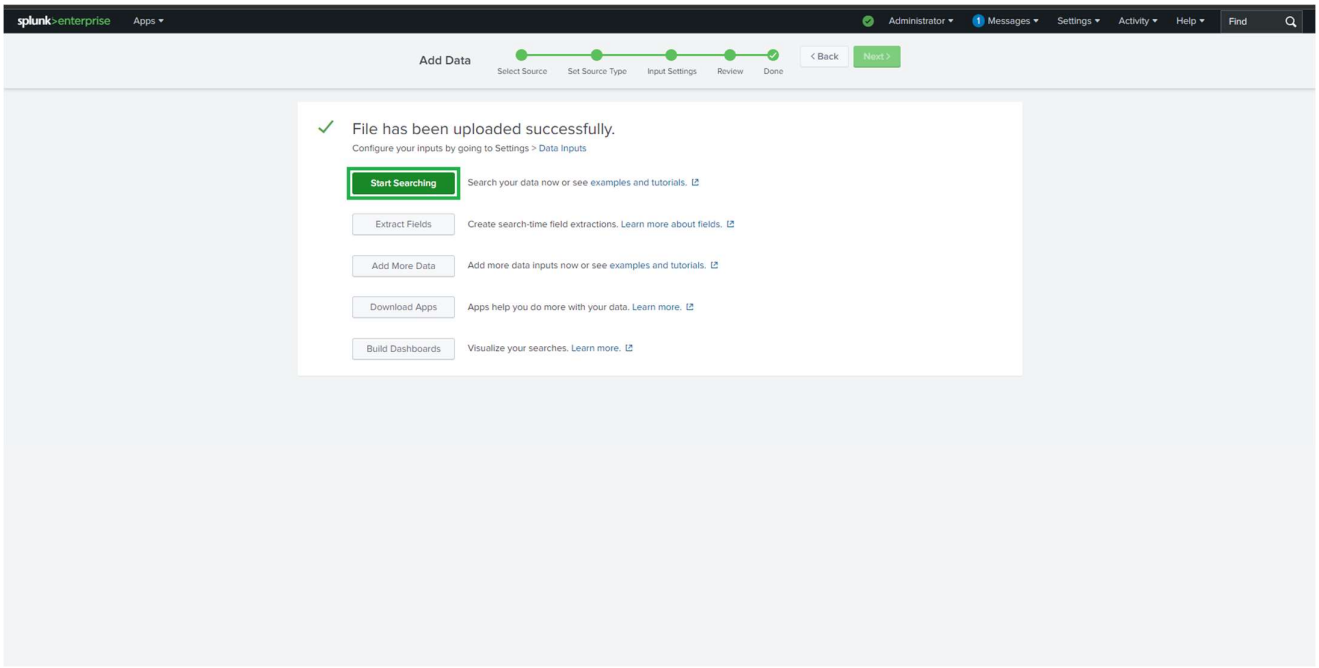

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
New Index
General Settings
Index Name
ssh_logs
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.
Index Data Type
Events
Metrics
The type of data to store (event-based or metrics).
Home Path
optional
Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).
Cold Path
optional
Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).
Thawed Path
optional
Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).
Data Integrity Check
Enable
Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.
Max Size of Entire Index
500
GB
Maximum target size of entire index.
Max Size of Hot/Warm/Cold Bucket
auto
GB
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.
Frozen Path
optional
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.
App
Search & Reporting
Storage Optimization
Save
Cancel


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Review >
Input Settings
Optionally set additional input parameters for this data input as follows:
Host
When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More
Constant value
Regular expression on path
Segment in path
Host field value
LAPTOP-EHJ3QFJI
Index
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More
Index
Default
Create a new index
Default
dns_lab
history
http_lab
main
ssh_logs
summary
FAQ
How do indexes work?
How do I know when to create or use multiple indexes?
127.0.0.1:8000/en-US/manager/search/adddatamethods/inputsettings#


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Review
Input Settings
Optionally set additional input parameters for this data input as follows:
Host
When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More
Constant value
Regular expression on path
Segment in path
Host field value
LAPTOP-EHJ3QFJI
Index
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More
Index
ssh_logs
Create a new index
FAQ
How do indexes work?
How do I know when to create or use multiple indexes?


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Submit
Review
Input Type ..... Uploaded File
File Name ..... ssh_logs.json
Source Type ..... _json
Host LAPTOP-EHJ3QFJI
Index ..... ssh_logs

6. Review settings and click **Start Searching**



🧩 Step-by-Step Implementation

🔹 Task 1: Ingest and Parse SSH Logs

Validate Field Extraction

Ensure the following fields are extracted correctly:

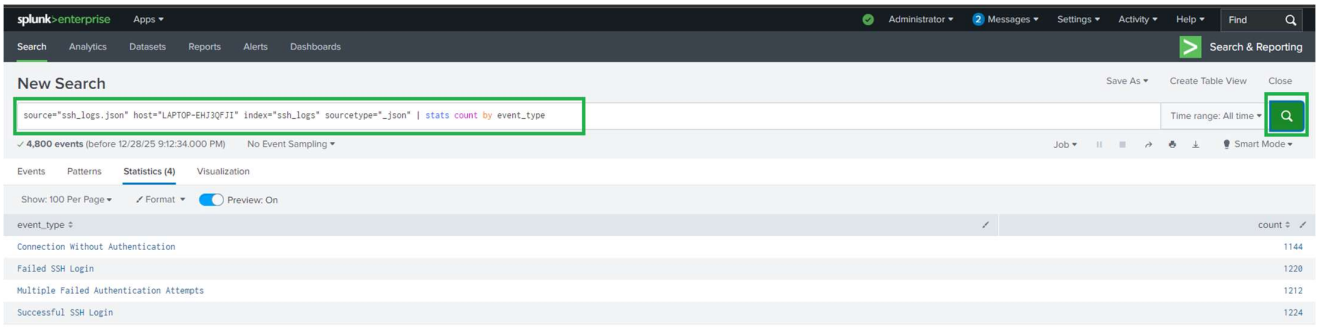
- event_type
- auth_success
- auth_attempts
- id.orig_h (Source IP)
- id.resp_h (Destination Host)

Validation Query

index=ssh_logs

| stats count by event_type

This confirms that logs are ingested and parsed successfully.



- **Task 2: Analyze Failed Login Attempts**

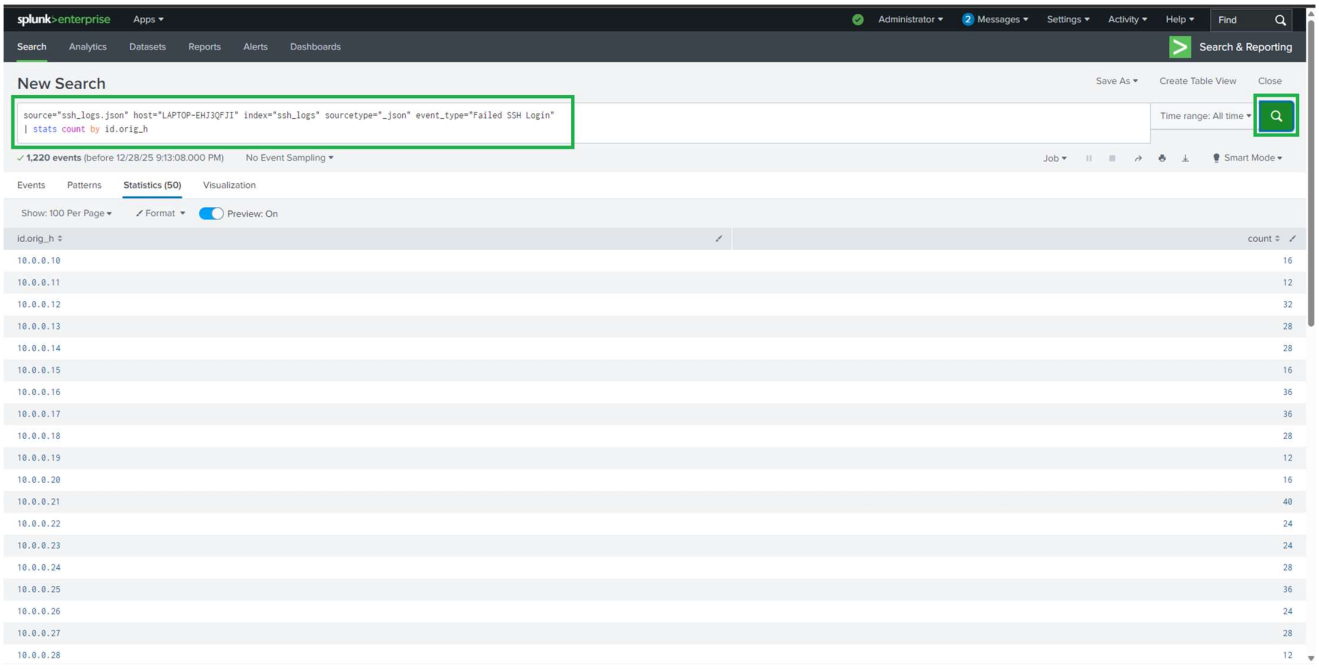
Identify Failed SSH Logins

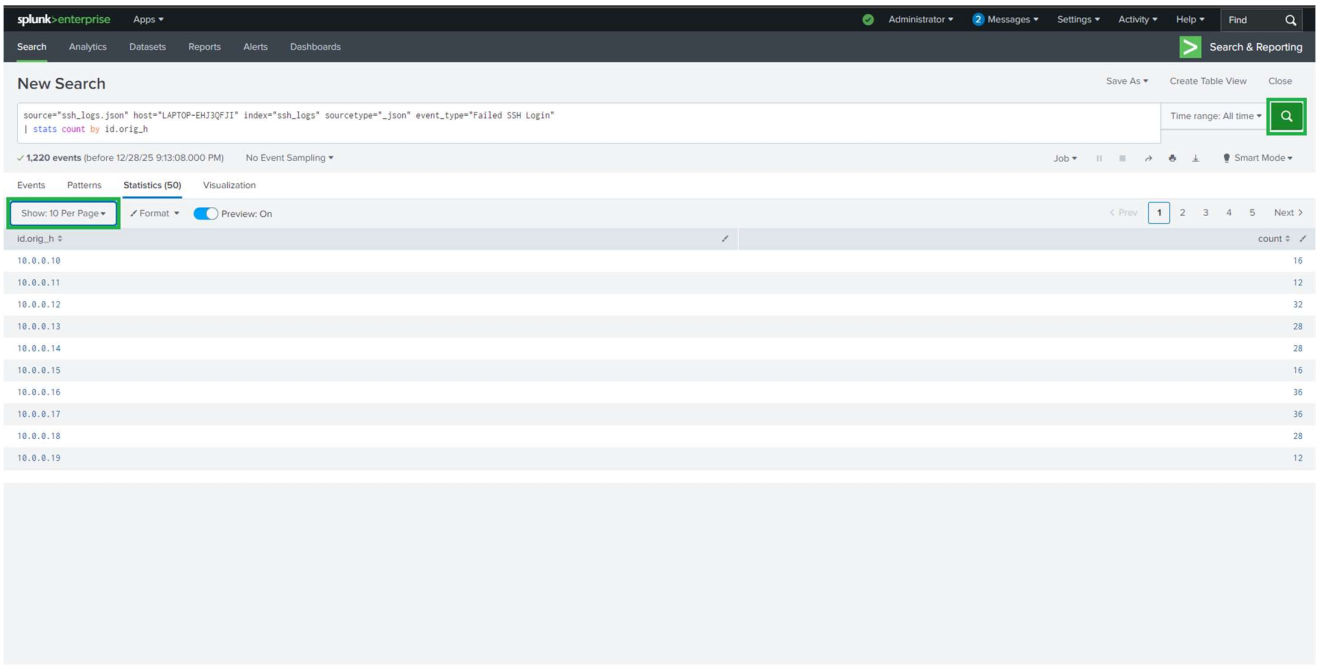
index=ssh_logs event_type="Failed SSH Login"

| stats count by id.orig_h

| sort - count

| head 10

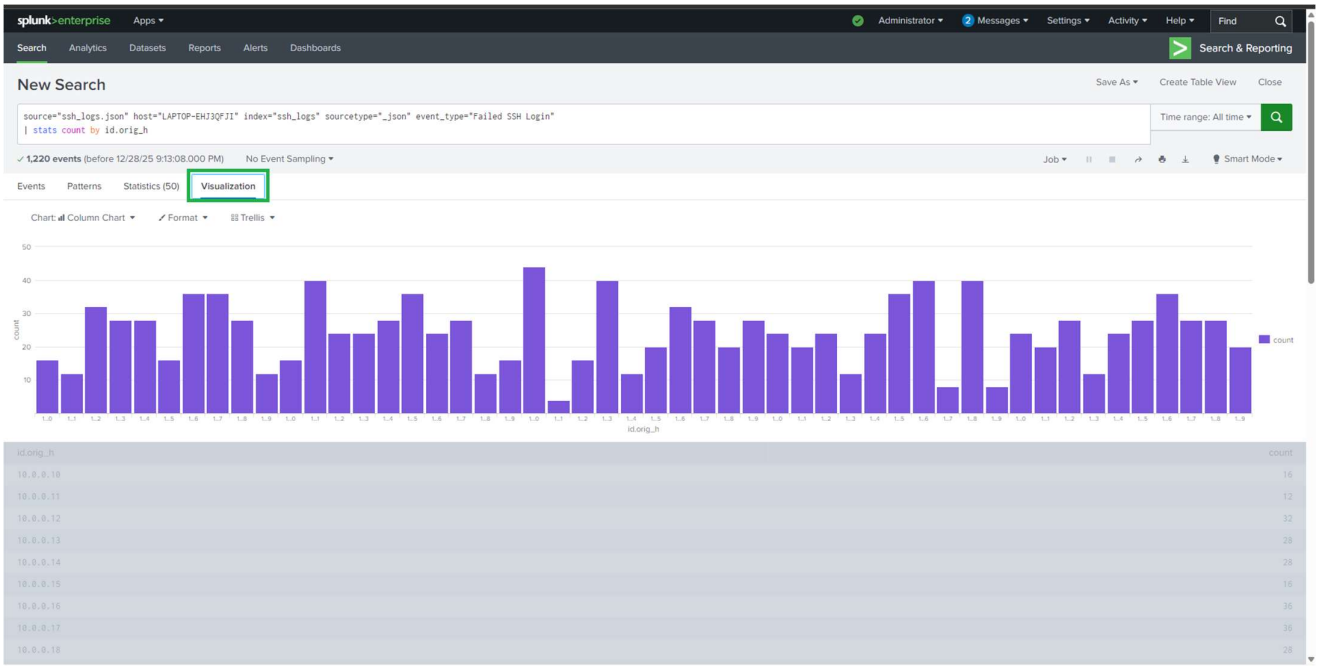


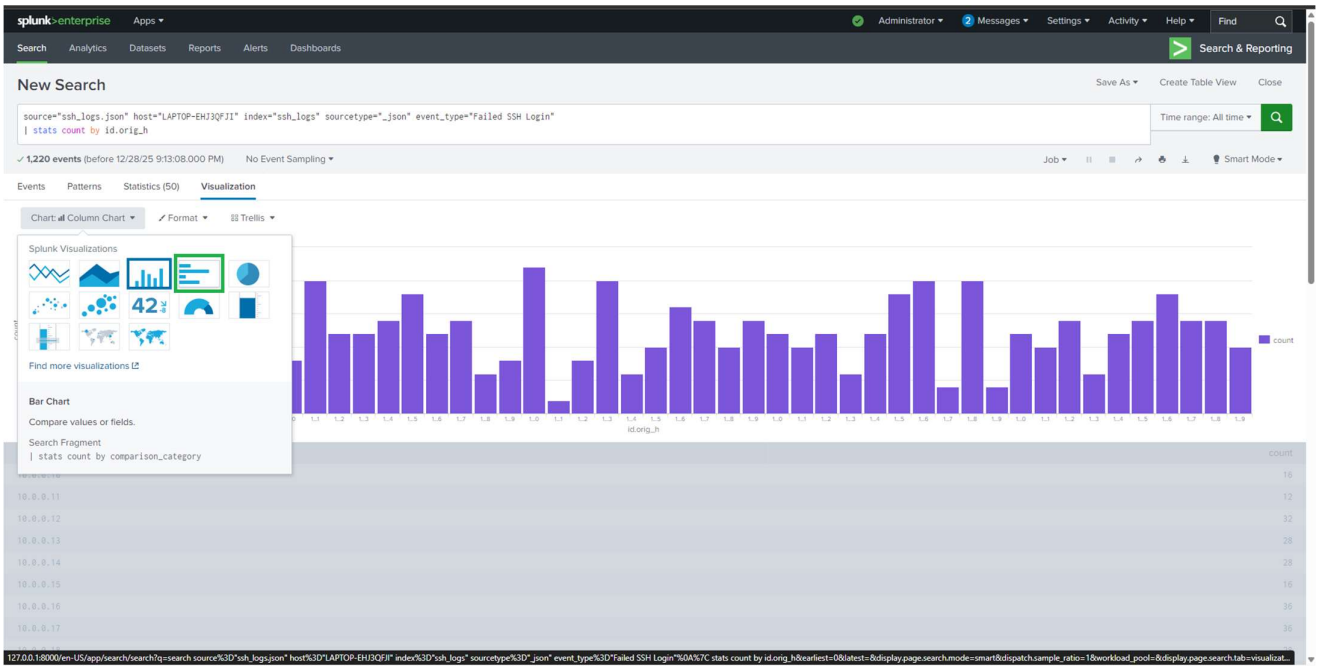


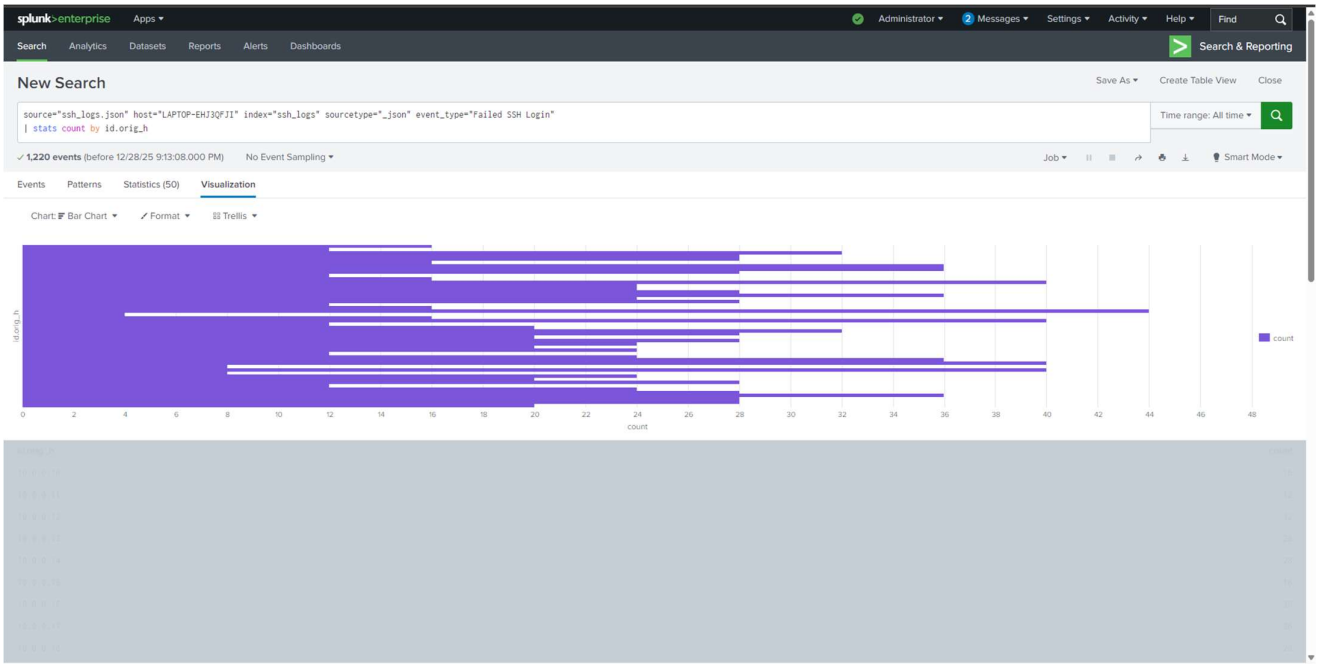
Visualization

- Create a **Bar Chart**
- X-axis: id.orig_h
- Y-axis: Count of failed logins

📌 **Purpose**: Identify IPs generating excessive failed login attempts.







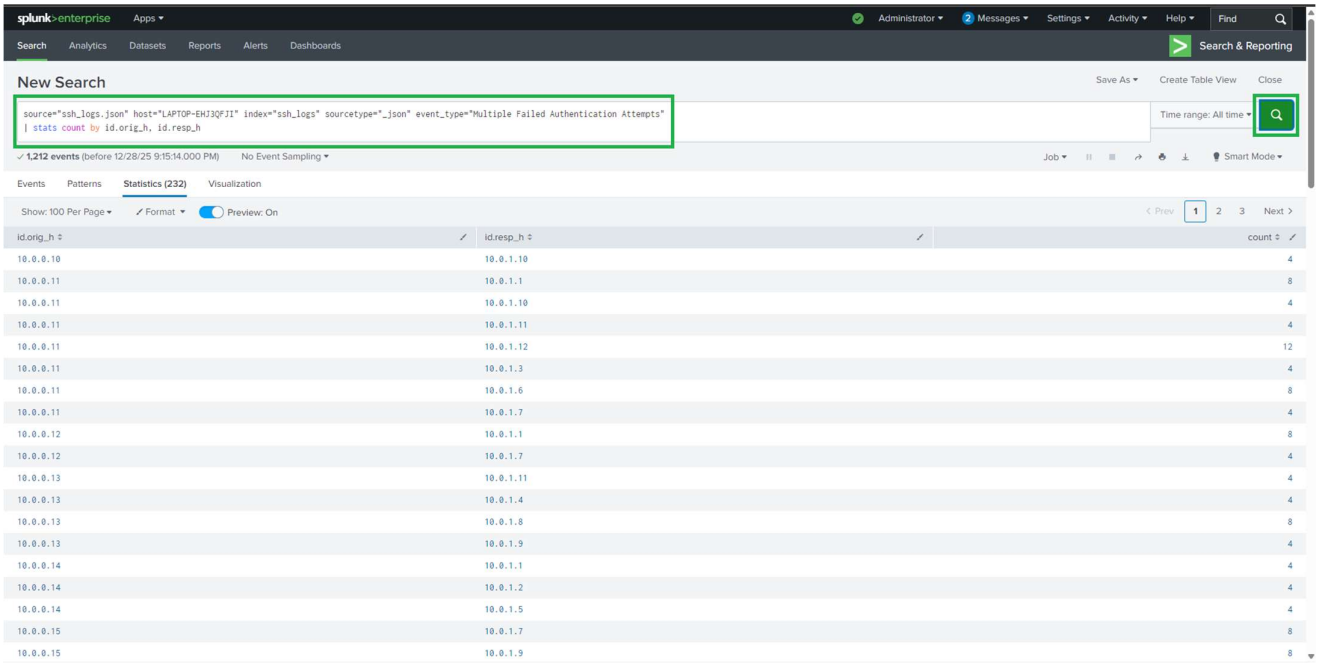
- **Task 3: Detect Multiple Failed Authentication Attempts (Brute Force)**

Search for Multiple Failed Attempts

index=ssh_logs event_type="Multiple Failed Authentication Attempts"

| stats count by id.orig_h, id.resp_h

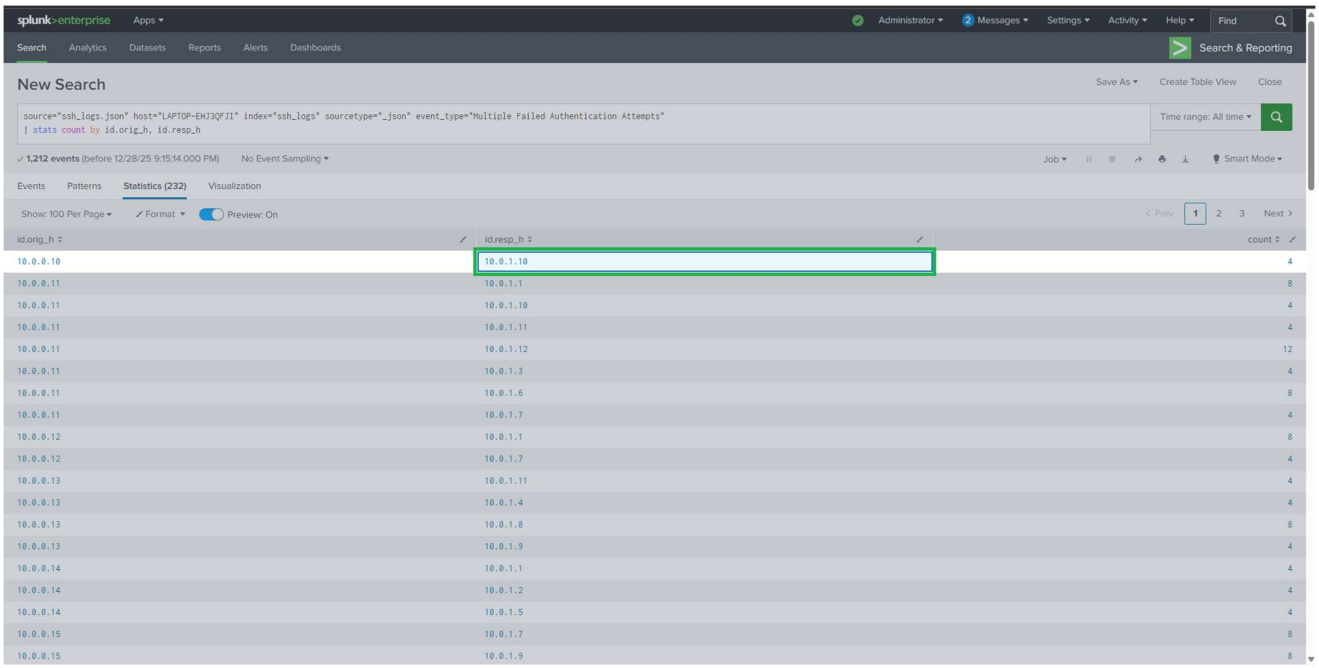
| where count > 5

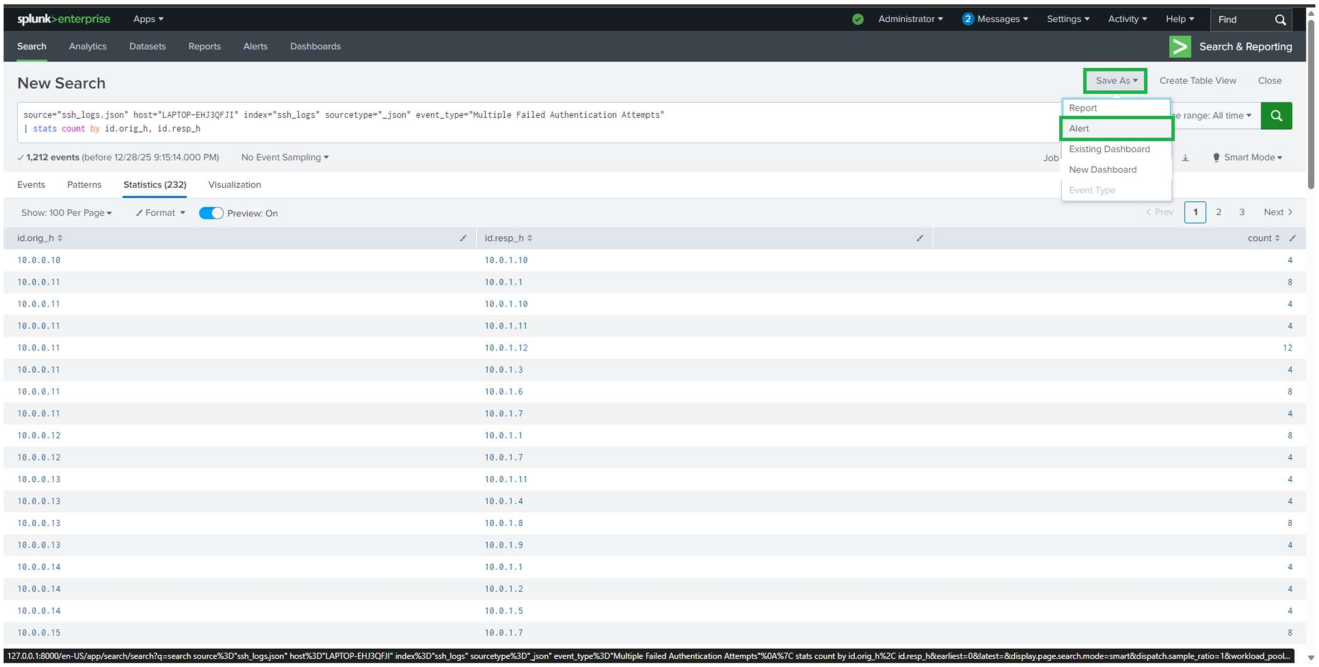


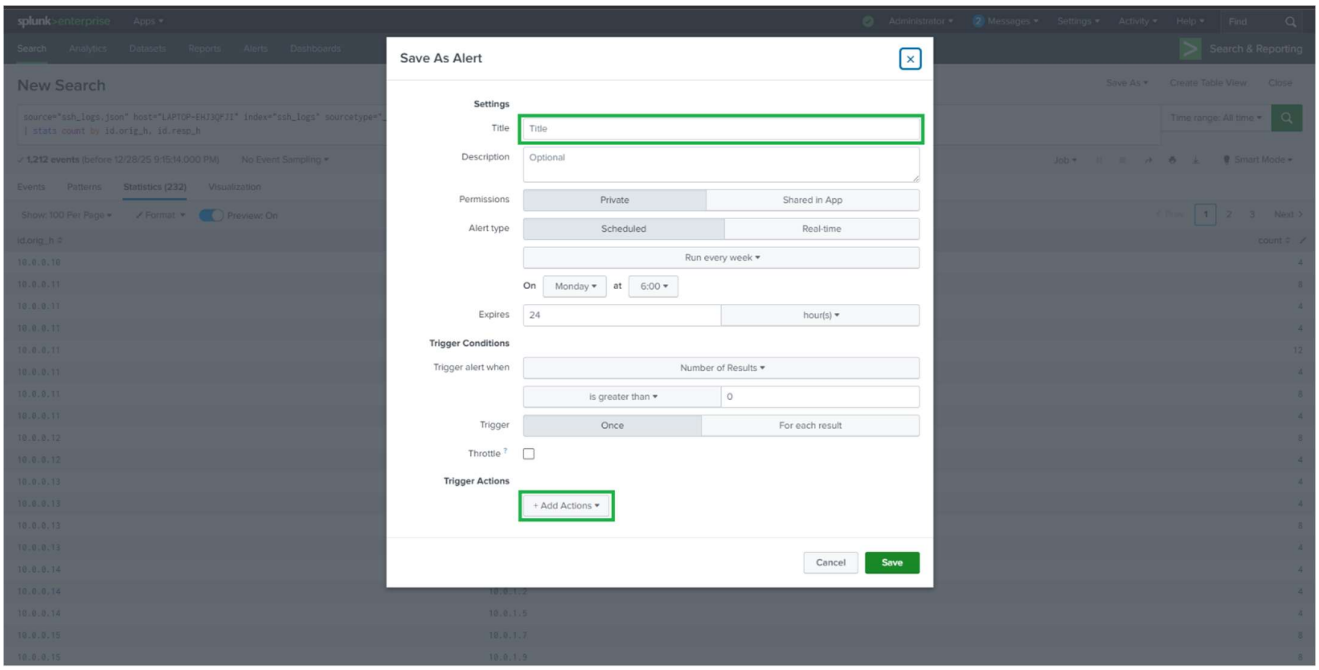
Alert Configuration

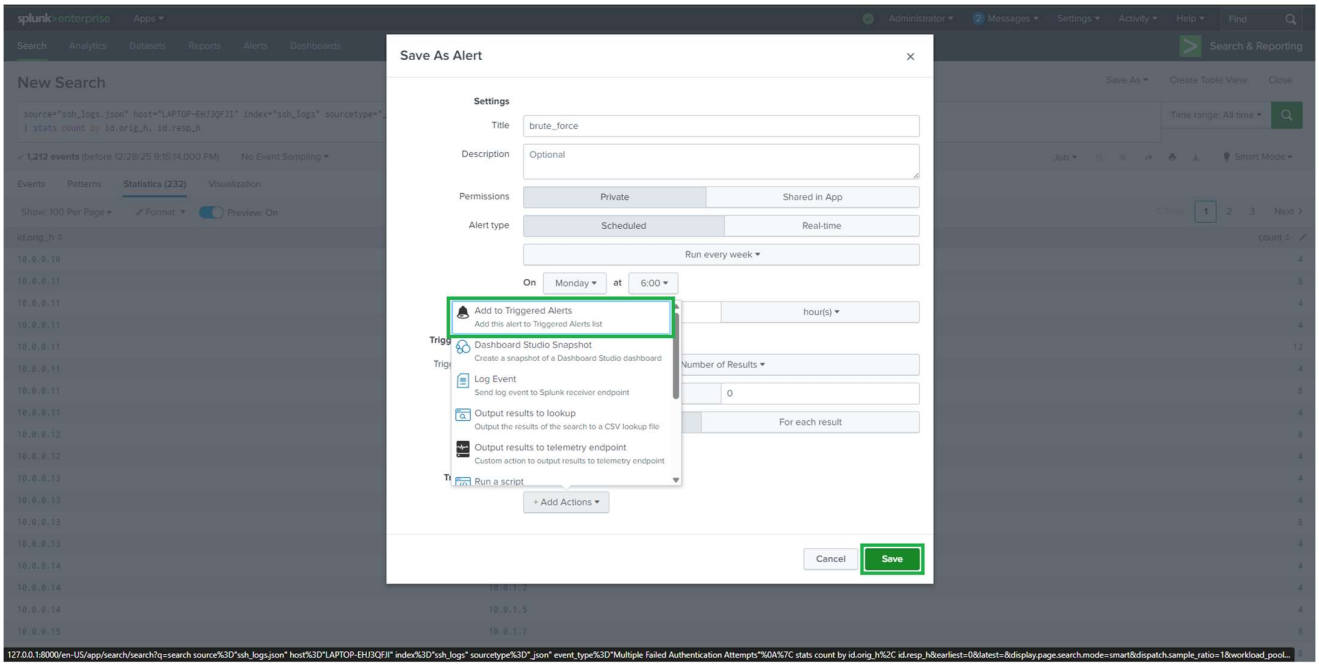
- **Trigger condition**: More than 5 failed attempts
- **Time window**: 10 minutes
- **Alert type**: Real-time or Scheduled
- **Action**: Email / SOC notification

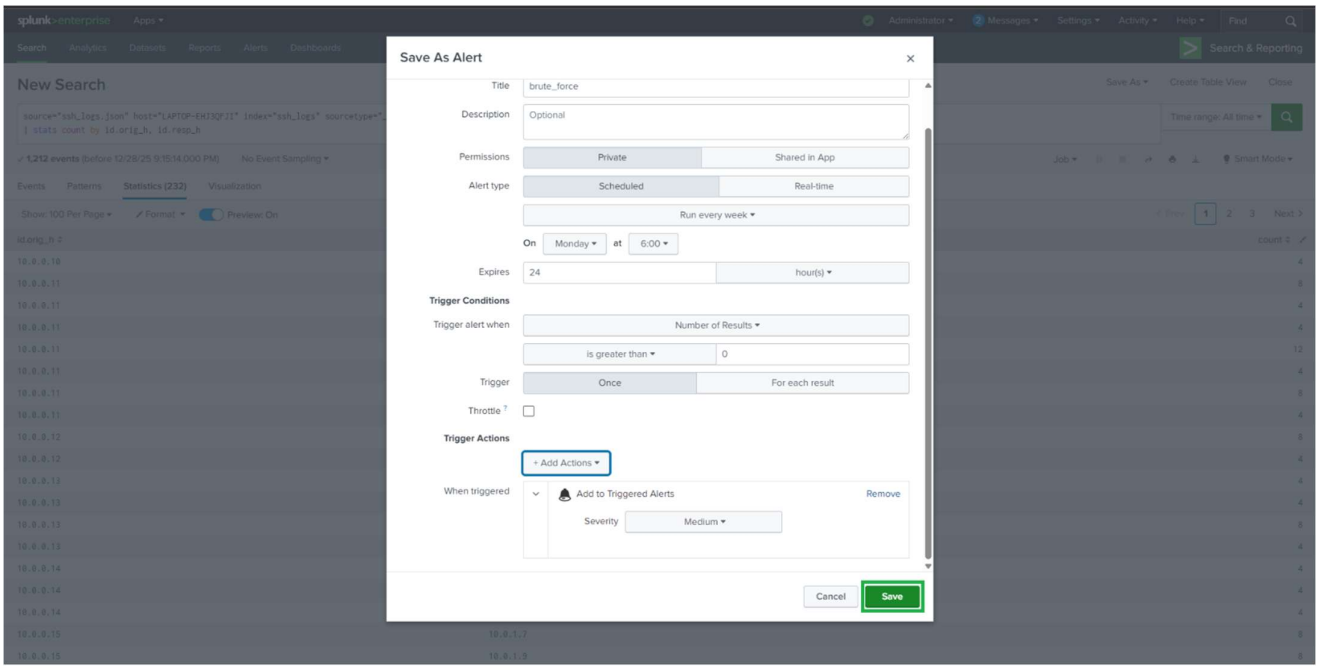
🚨 **Purpose**: Detect brute-force attacks early.

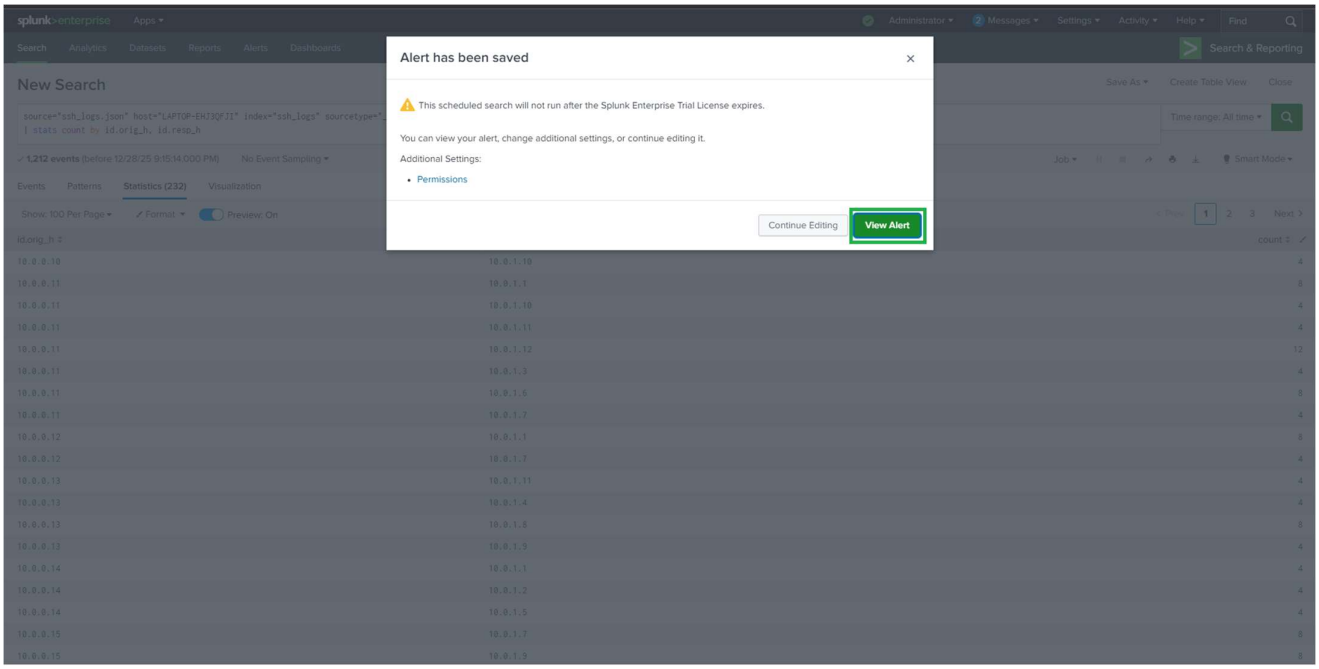


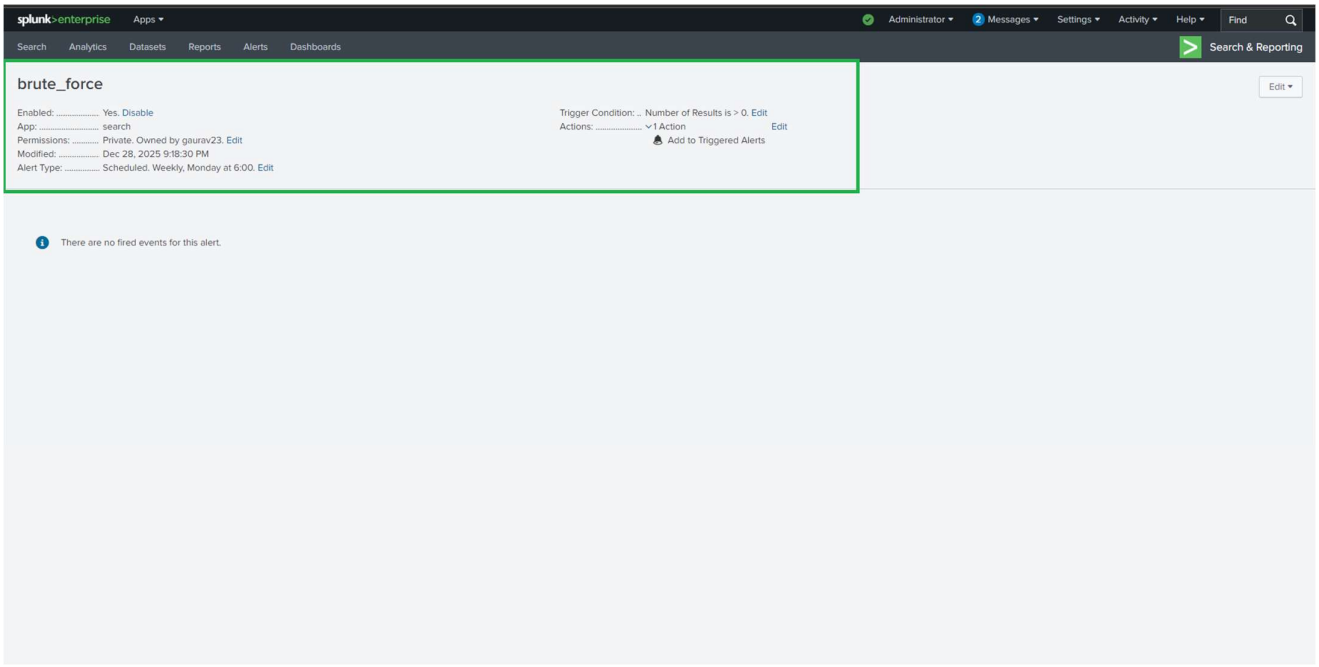







Save As Alert
Title
brute_force
Description
Optional
Permissions
Private
Shared in App
Alert type
Scheduled
Real-time
Run every week
On
Monday
at
6:00
Expires
24
hour(s)
Trigger Conditions
Trigger alert when
Number of Results
is greater than
0
Trigger
Once
For each result
Throttle
Trigger Actions
+ Add Actions
When triggered
Add to Triggered Alerts
Remove
Severity
Medium
Cancel
Save


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
Continue Editing
View Alert


splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
brute_force
Edit
Enabled: Yes. Disable
App: search
Permissions: Private. Owned by gaurav23. Edit
Modified: Dec 28, 2025 9:18:30 PM
Alert Type: Scheduled. Weekly, Monday at 6:00. Edit
Trigger Condition: Number of Results is > 0. Edit
Actions: 1 Action Edit
Add to Triggered Alerts
There are no fired events for this alert.

🔹 Task 4: Track Successful SSH Logins

Successful Login Query

index=ssh_logs event_type="Successful SSH Login"

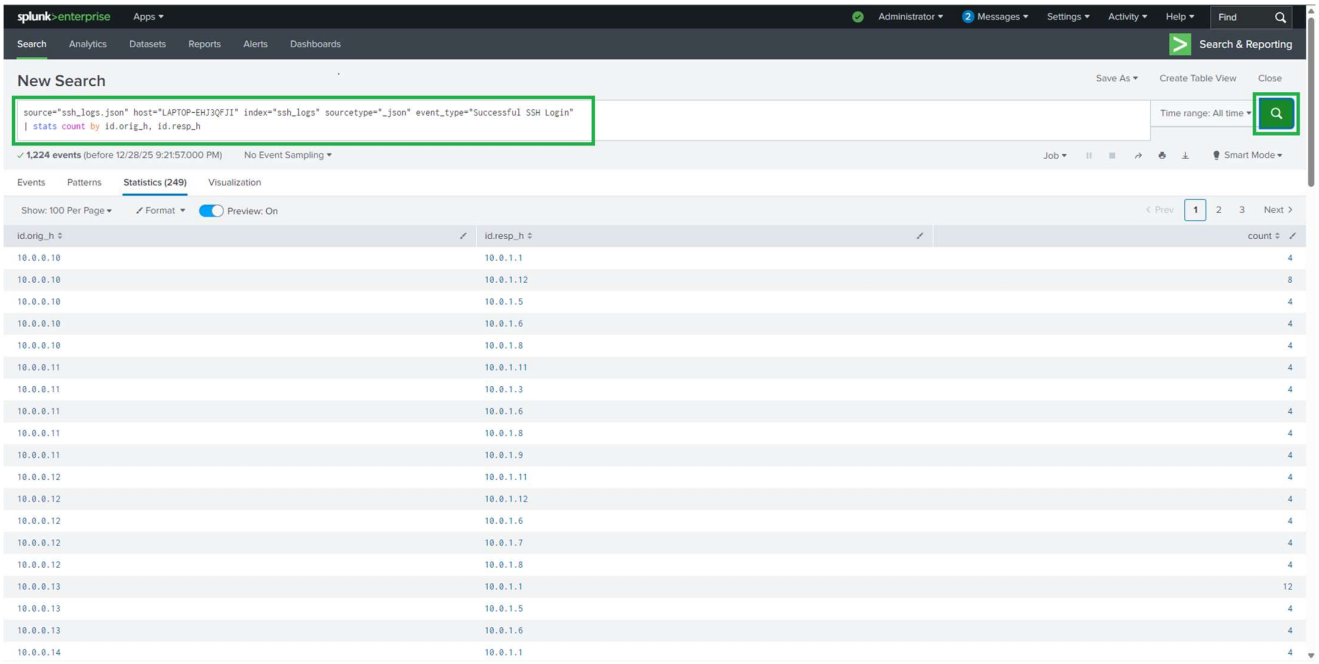
| stats count by id.orig_h, id.resp_h

Correlation Use Case

Compare:

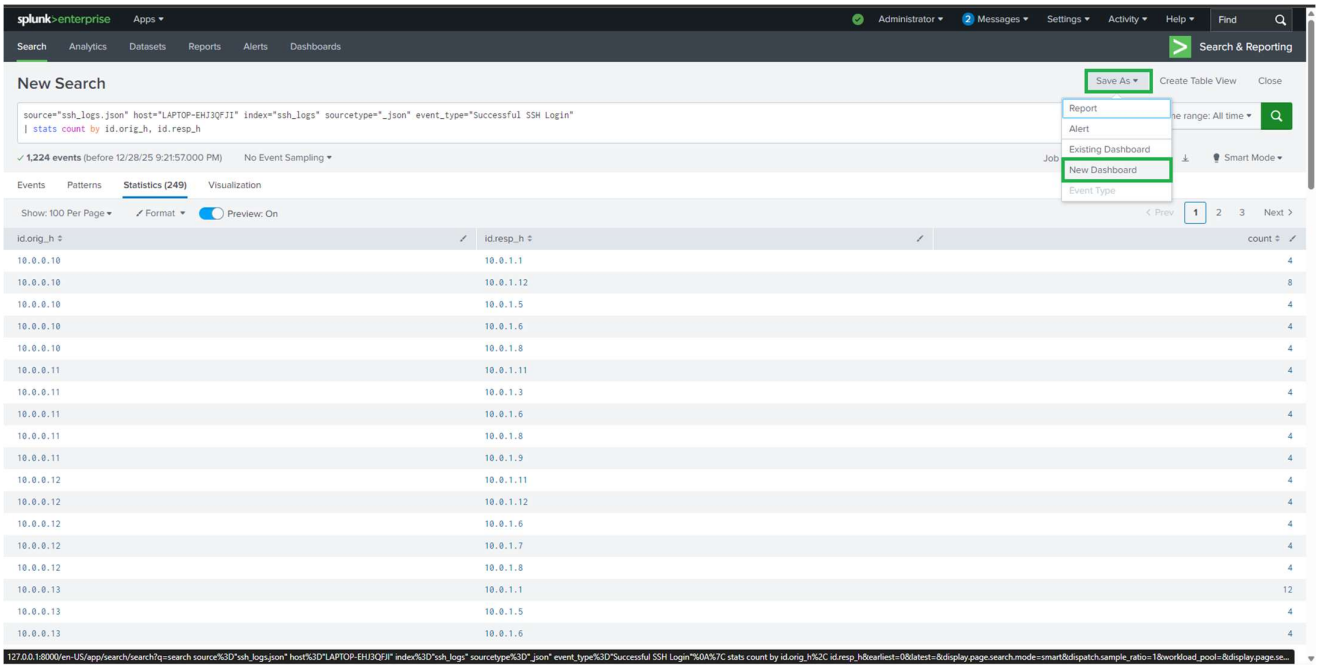
- IPs with multiple failed logins
- IPs that later successfully authenticate

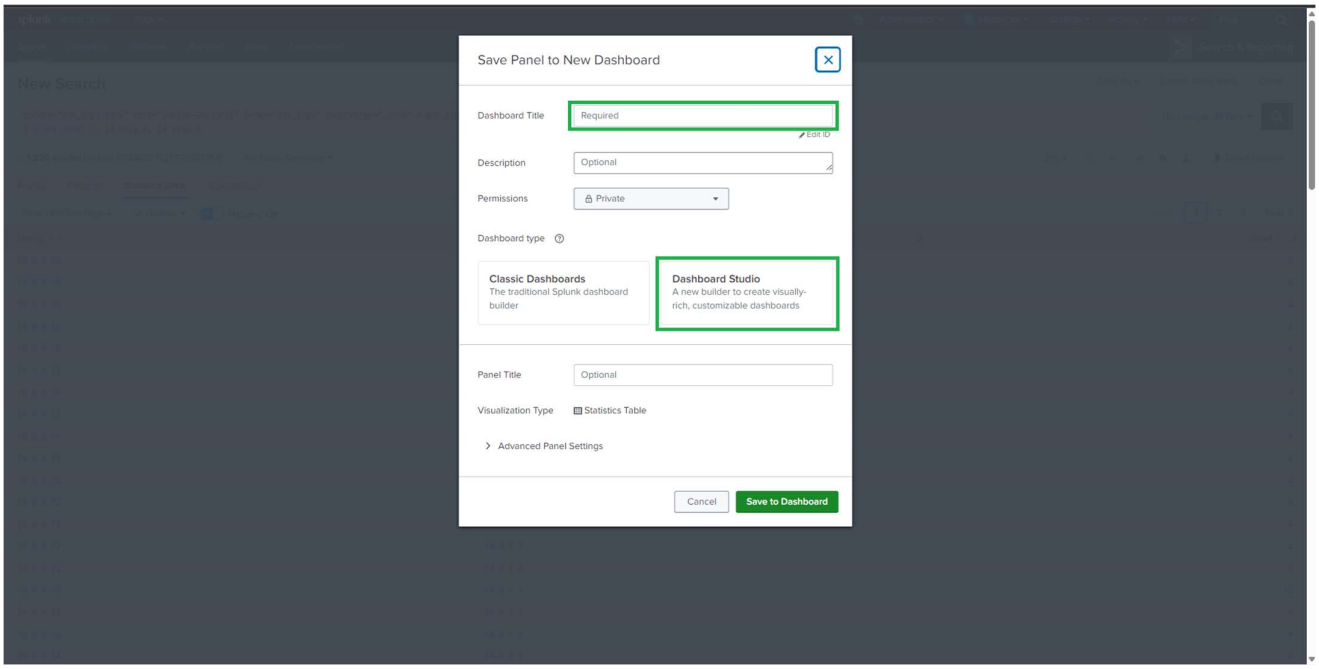
📌 **Purpose**: Detect potential compromised credentials.

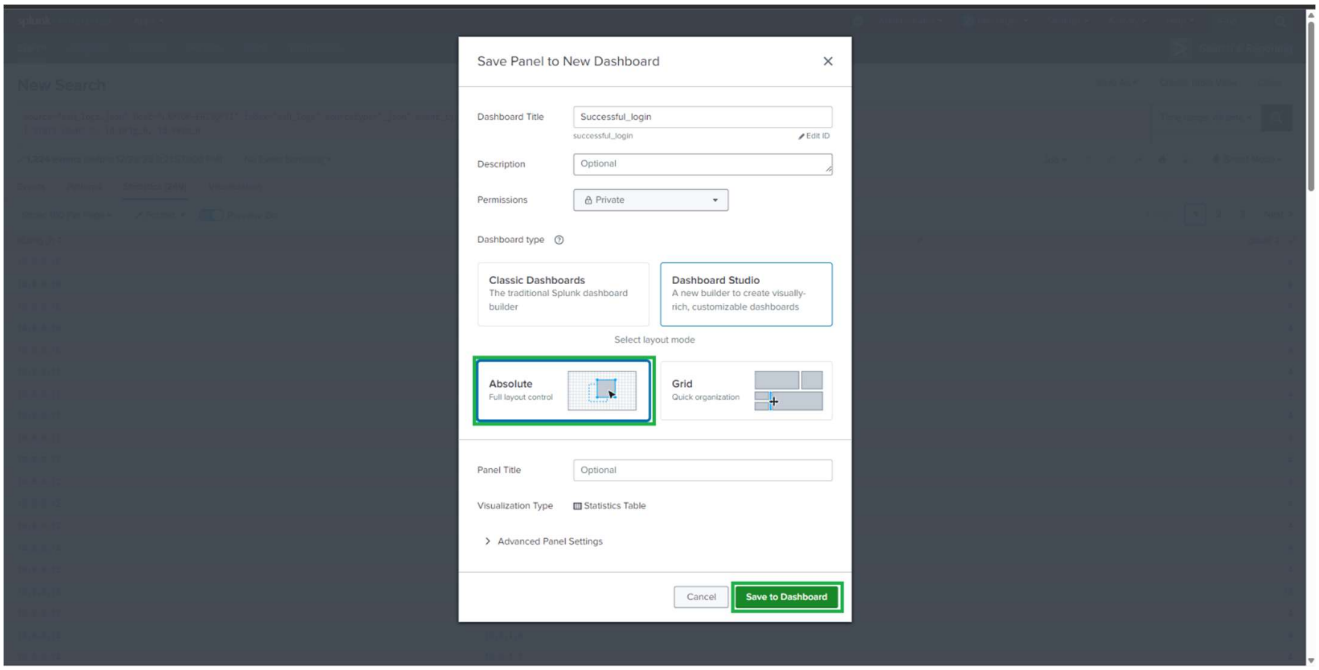


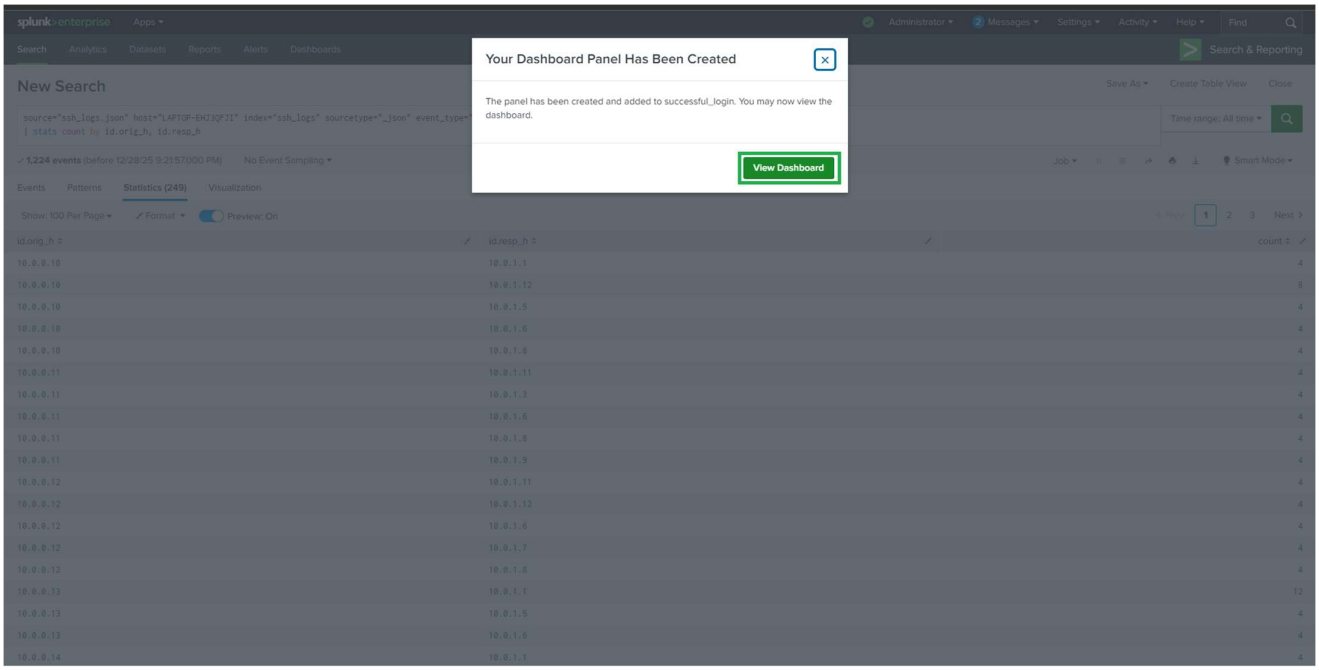
Dashboard Panel

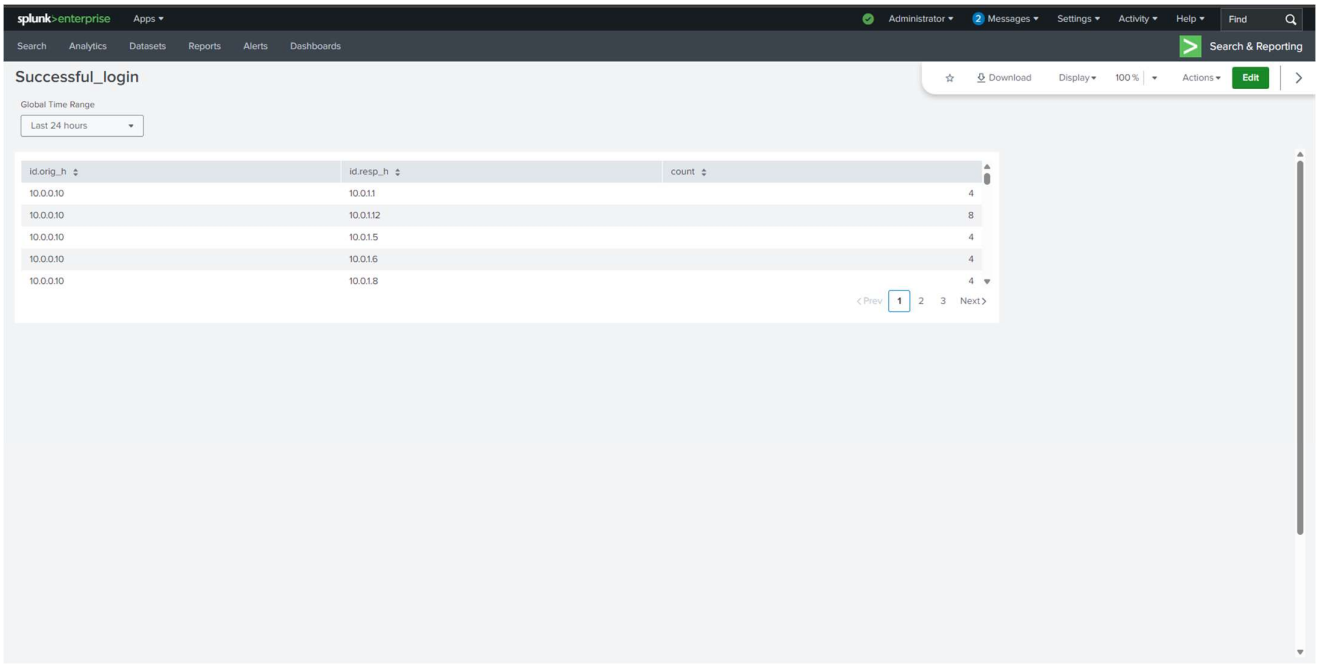
- Visualization: Bar Chart or Table
- Metric: Top source IPs with successful SSH logins






Save Panel to New Dashboard
Dashboard Title
Successful_login
successful_login
Edit ID
Description
Optional
Permissions
Private
Dashboard type
Classic Dashboards
The traditional Splunk dashboard builder
Dashboard Studio
A new builder to create visually-rich, customizable dashboards
Select layout mode
Absolute
Full layout control
Grid
Quick organization
Panel Title
Optional
Visualization Type
Statistics Table
Advanced Panel Settings
Cancel
Save to Dashboard


Your Dashboard Panel Has Been Created
The panel has been created and added to successful_login. You may now view the dashboard.
View Dashboard
New Search

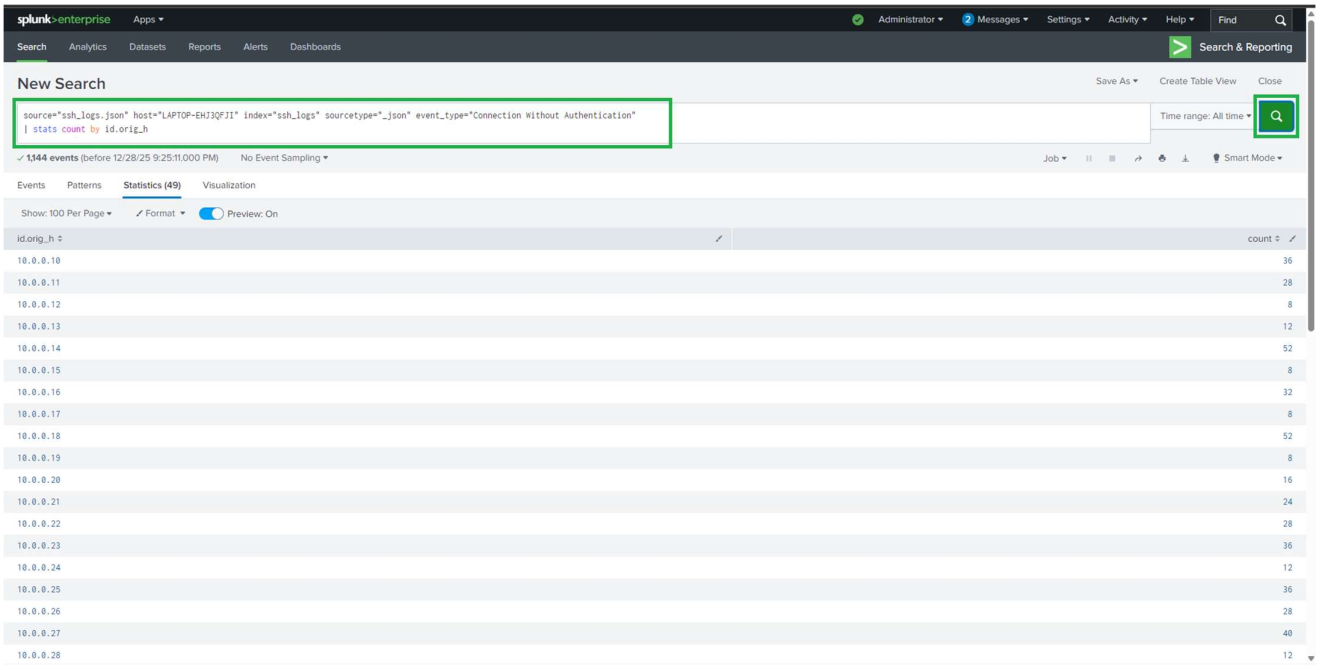


- **Task 5: Detect Connections Without Authentication**

Search Unauthenticated Connections

index=ssh_logs event_type="Connection Without Authentication"

| stats count by id.orig_h



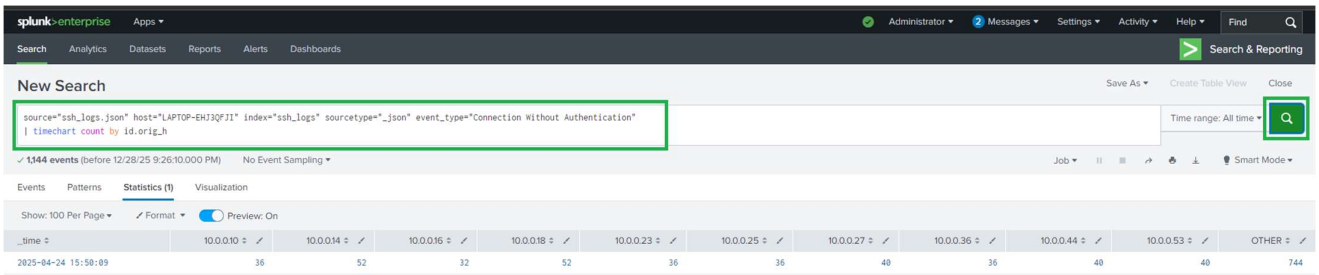
Time-Based Monitoring

index=ssh_logs event_type="Connection Without Authentication"

| timechart count by id.orig_h

📌 **Purpose:**

- Identify SSH probing
- Detect port scanning or reconnaissance activity



📊 Dashboards Created

- 🔐 SSH Successful Login Monitoring
- ❌ Failed Login Attempts per IP
- 🚨 Brute Force Detection
- 🔍 Unauthenticated SSH Connection Trends

🚨 Alerts Configured

- **Brute-force detection alert**
- Triggered on multiple failed authentication attempts
- Time-based correlation (10-minute window)

✅ Conclusion

By completing this project, you have:

✓ Ingested and parsed SSH logs in Splunk
✓ Written SPL queries for threat detection
✓ Built SOC-style dashboards
✓ Configured alerts for high-risk activity
✓ Gained hands-on **SOC Analyst–level log analysis experience**