🔐 Splunk Dashboard for SSH Logs

By Gaurav Ghandat

📌 Objective

The objective of this project is to design and implement a **Splunk dashboard** for monitoring **SSH authentication activity** on Linux servers.
The dashboard helps security analysts:

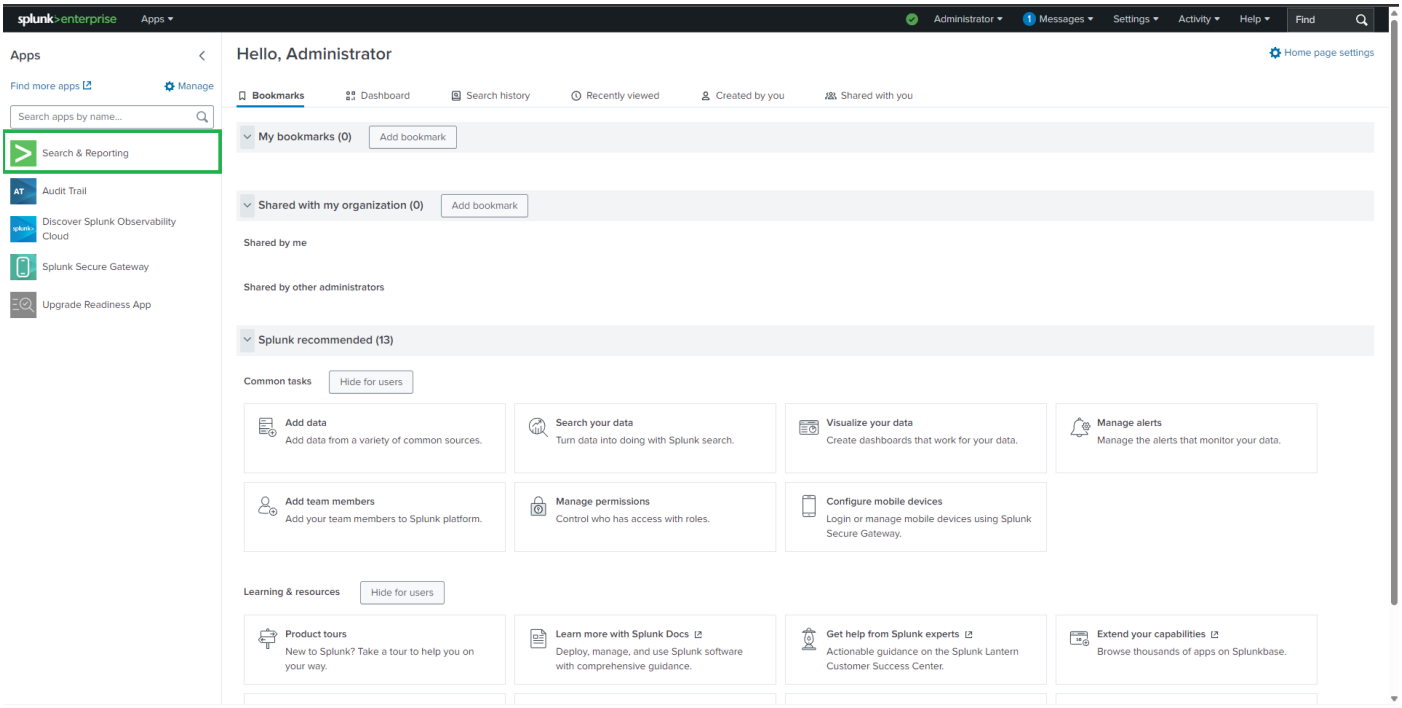
- Monitor total SSH activity
- Track successful and failed login attempts
- Detect brute-force attacks
- Visualize attack origins using geo-location data

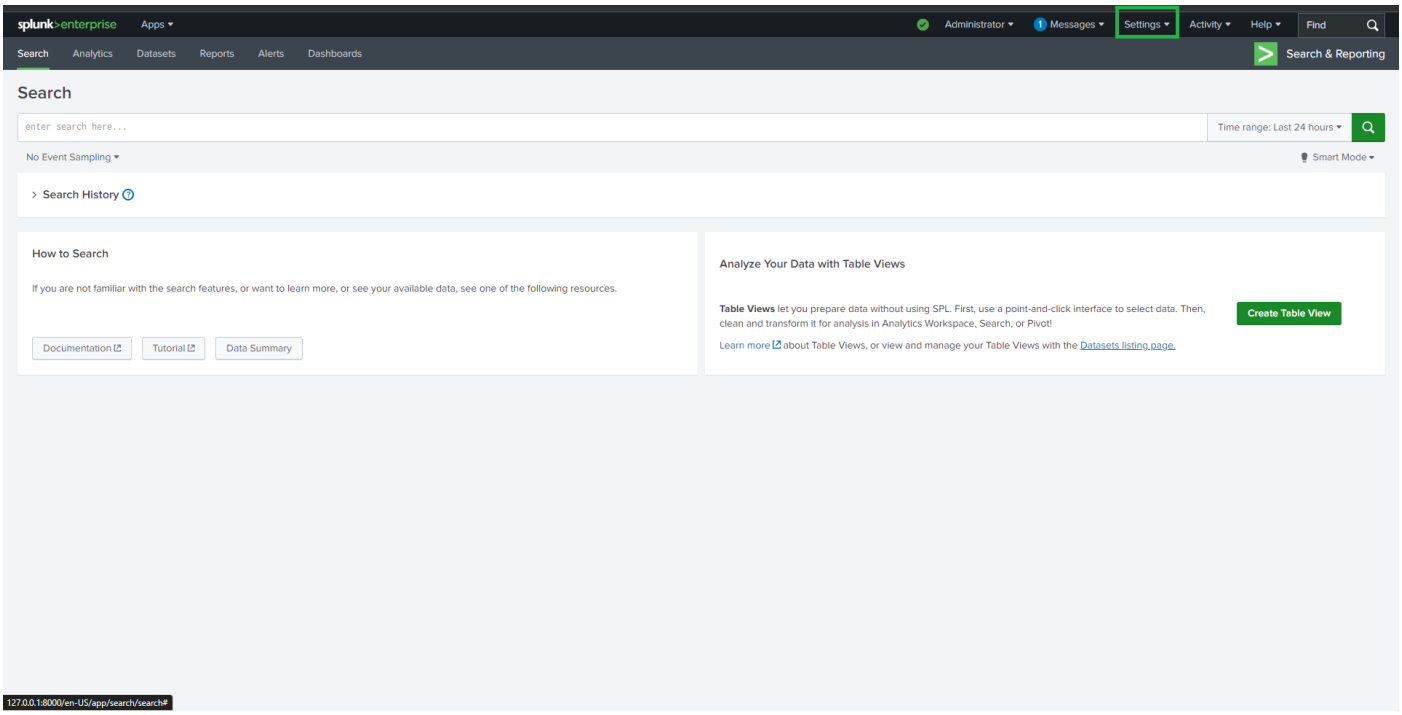
This dashboard is designed with **consistent time filtering** and **security-focused visualizations** for effective threat detection.

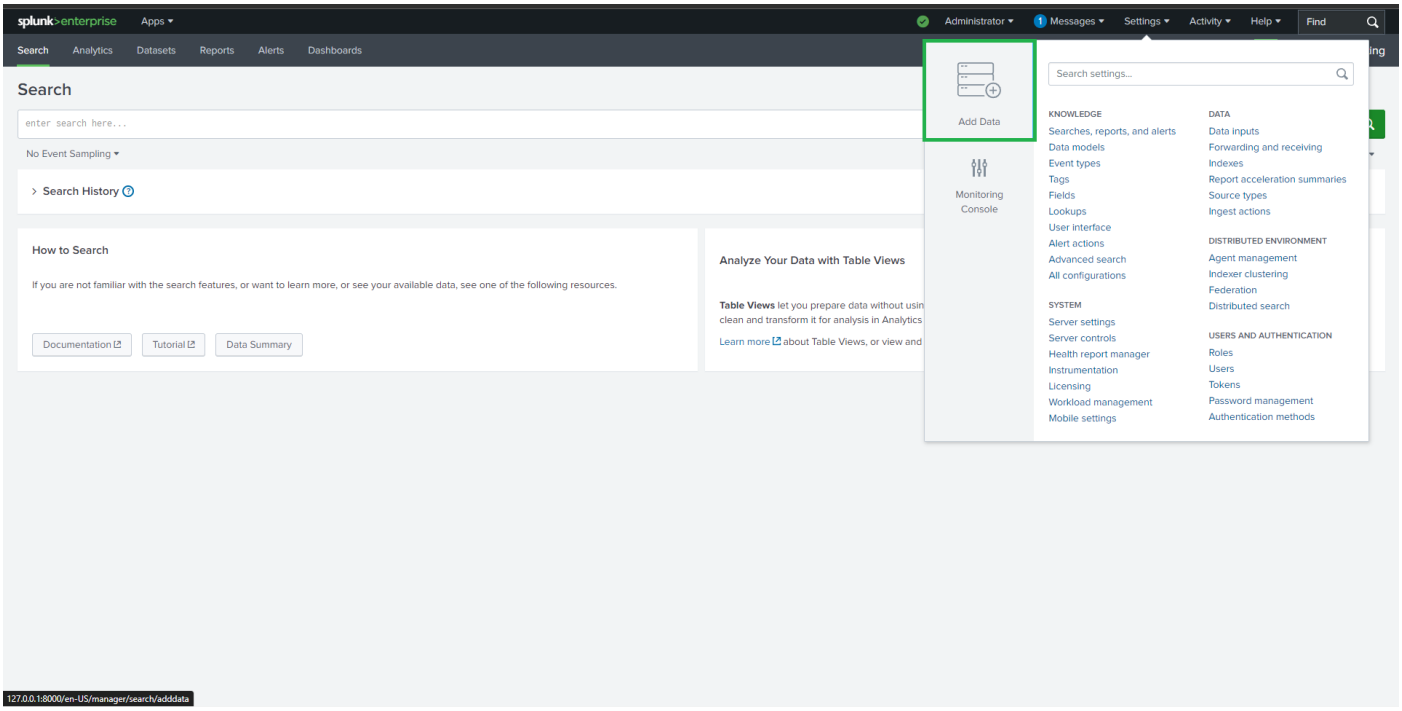
🧪 Lab Setup

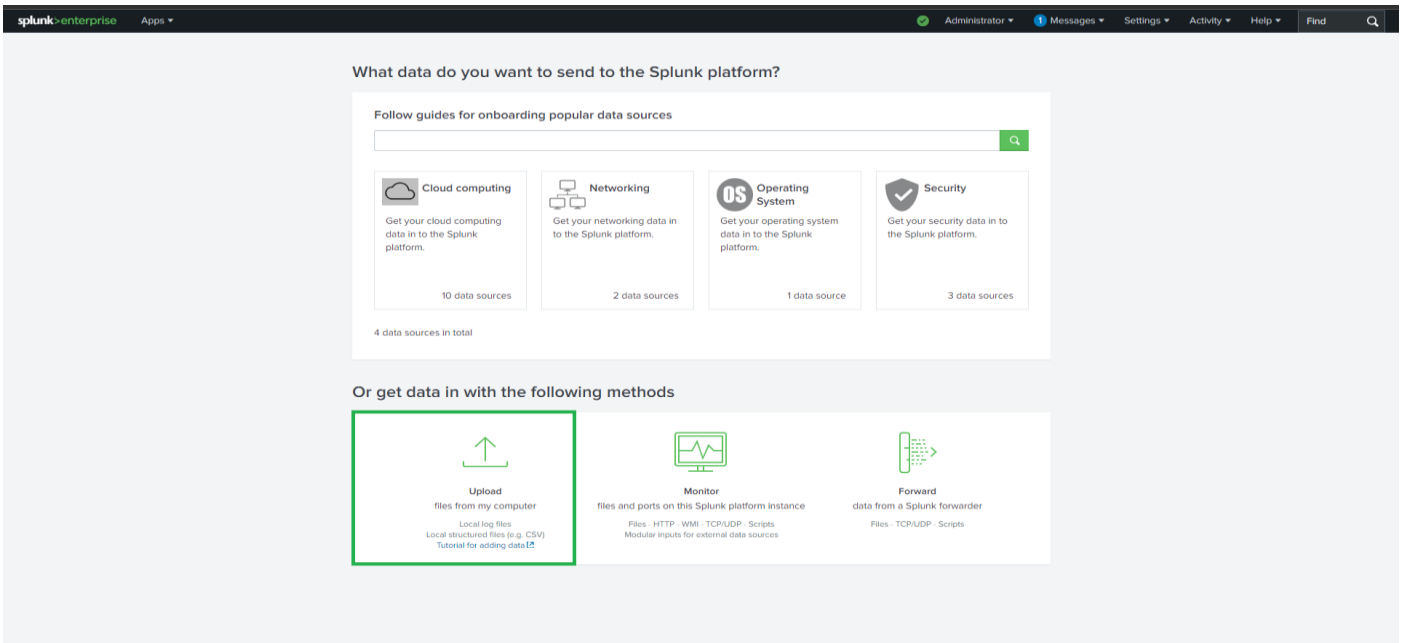
Prerequisites

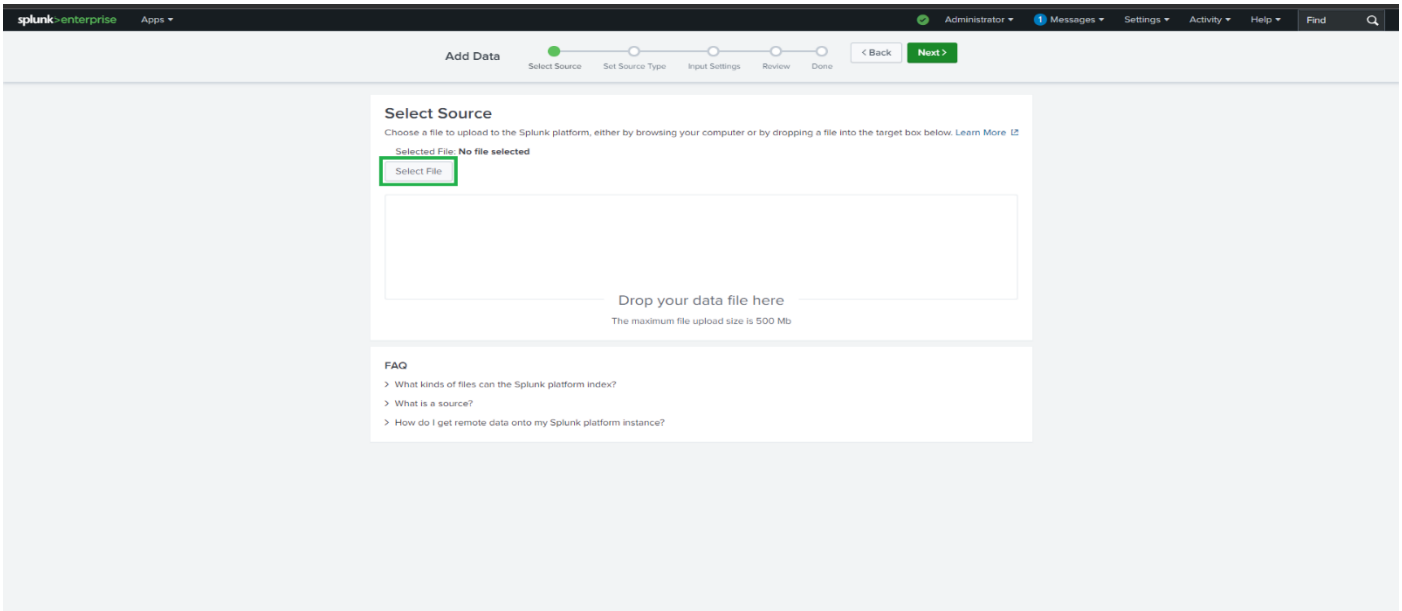
- Splunk Enterprise / Splunk Free
- SSH log data ingested in JSON format
- Indexed SSH log files:
    - ssh_logs.json
    - ssh_logs_new.json
- Linux servers:
    - LinuxServer
    - LinuxNew

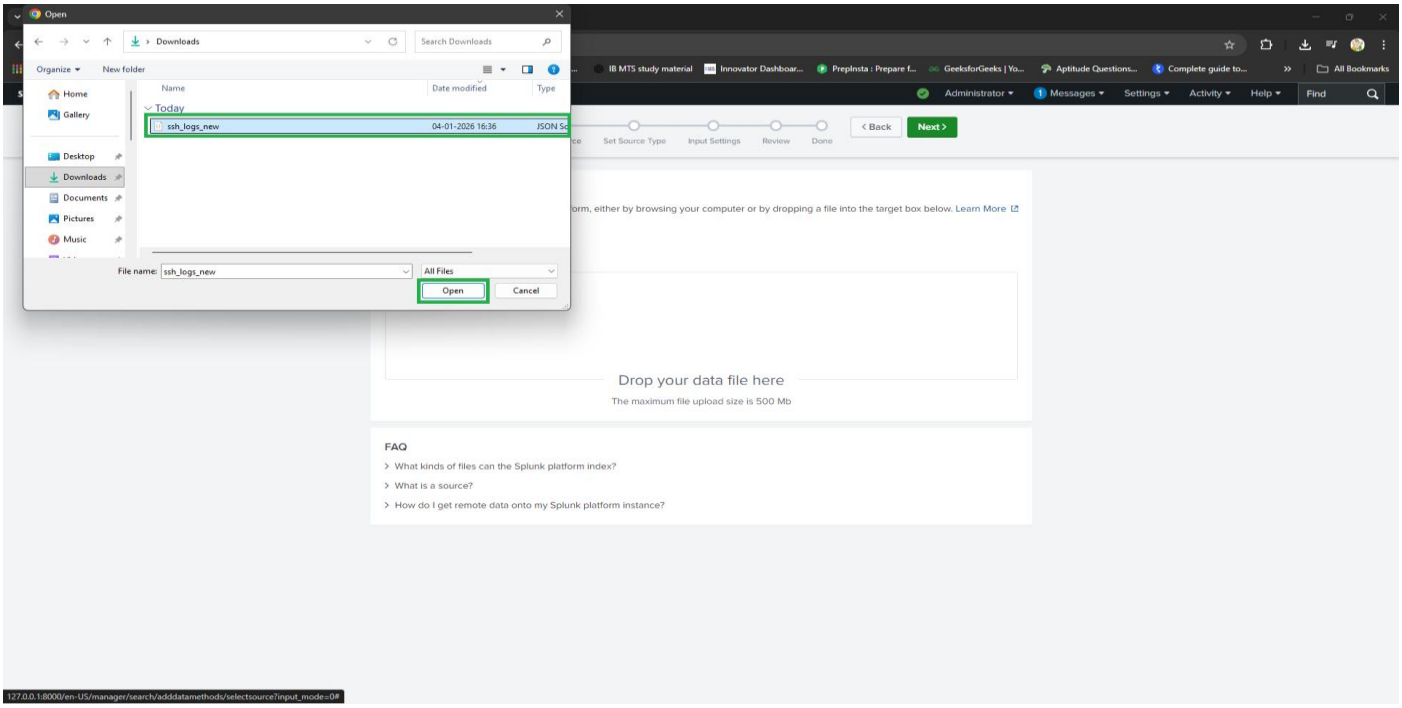

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Apps
Find more apps
Manage
Search apps by name...
Search & Reporting
Audit Trail
Discover Splunk Observability Cloud
Splunk Secure Gateway
Upgrade Readiness App
Hello, Administrator
Home page settings
Bookmarks
Dashboard
Search history
Recently viewed
Created by you
Shared with you
My bookmarks (0)
Add bookmark
Shared with my organization (0)
Add bookmark
Shared by me
Shared by other administrators
Splunk recommended (13)
Common tasks
Hide for users
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.
Learning & resources
Hide for users
Product tours
New to Splunk? Take a tour to help you on your way.
Learn more with Splunk Docs
Deploy, manage, and use Splunk software with comprehensive guidance.
Get help from Splunk experts
Actionable guidance on the Splunk Lantern Customer Success Center.
Extend your capabilities
Browse thousands of apps on Splunkbase.

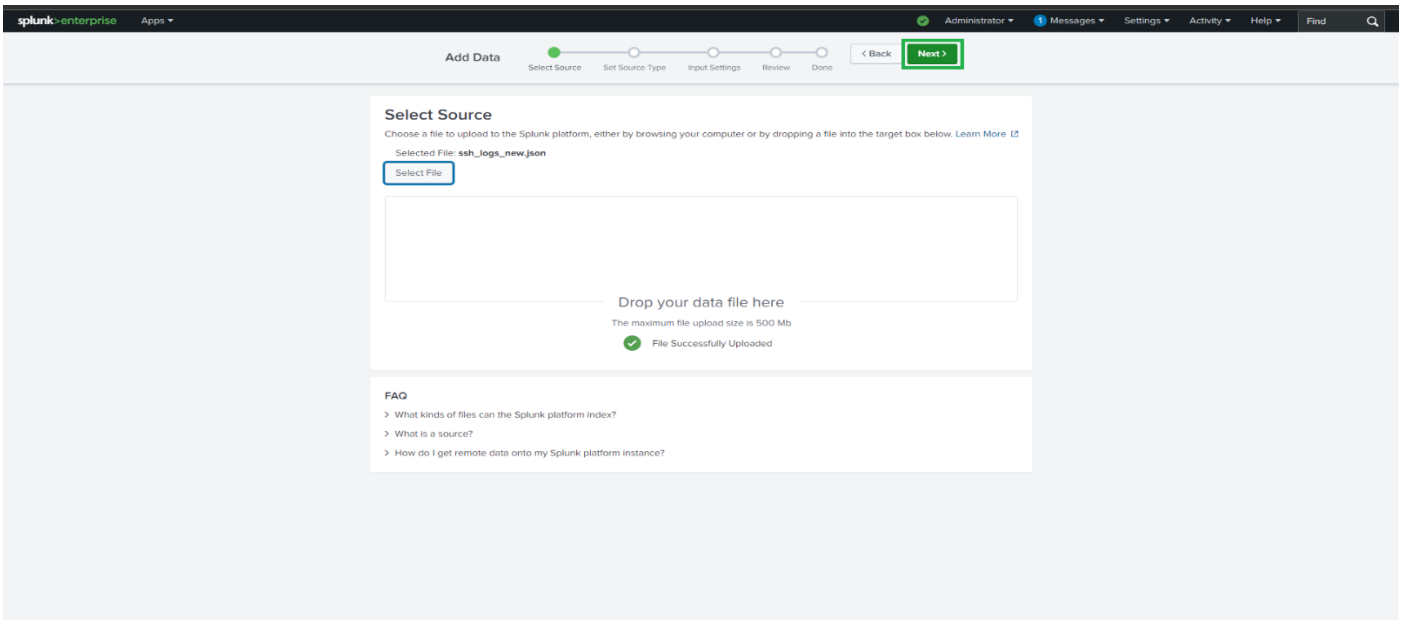

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Search
enter search here...
Time range: Last 24 hours
No Event Sampling
Smart Mode
Search History
How to Search
If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.
Documentation
Tutorial
Data Summary
Analyze Your Data with Table Views
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!
Create Table View
Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.
127.0.0.1:8000/en-US/app/search/search#

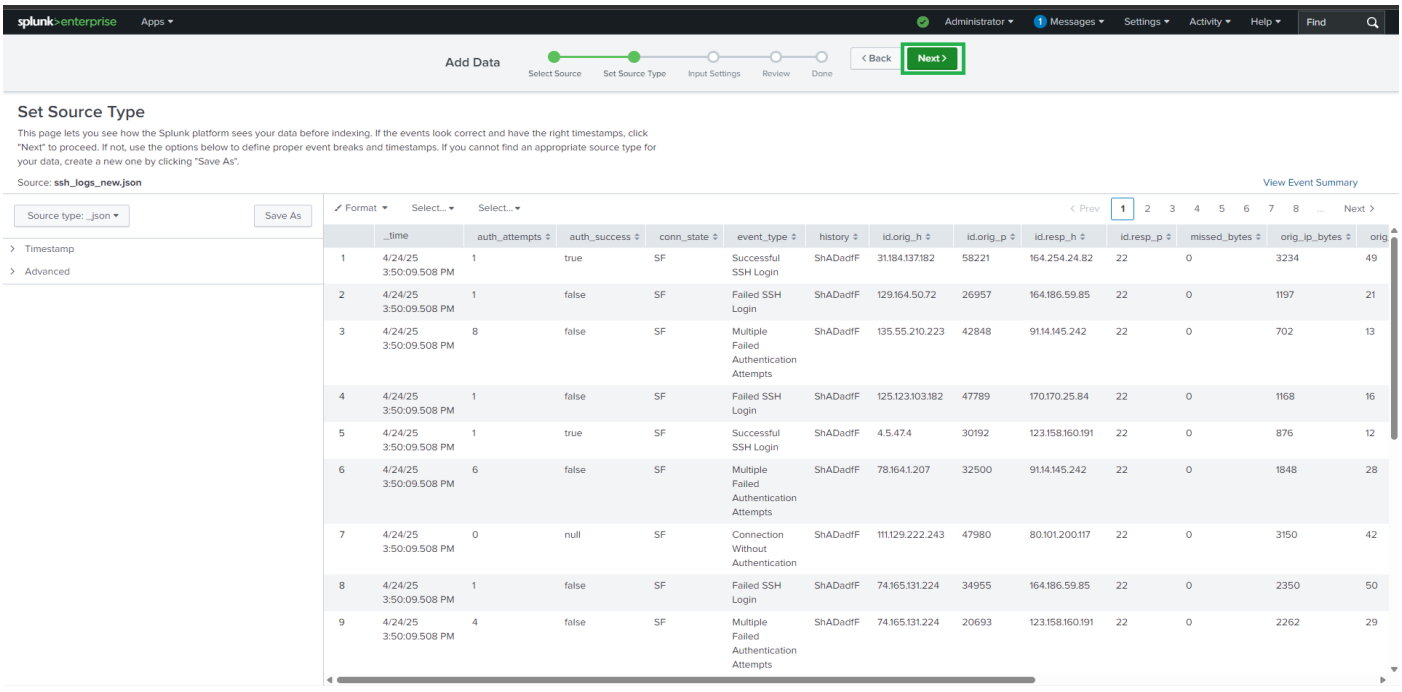

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search
enter search here...
No Event Sampling
Search History
How to Search
If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.
Documentation
Tutorial
Data Summary
Analyze Your Data with Table Views
Table Views let you prepare data without usin
clean and transform it for analysis in Analytics
Learn more about Table Views, or view and
Add Data
Monitoring Console
Search settings...
KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations
SYSTEM
Server settings
Server controls
Health report manager
Instrumentation
Licensing
Workload management
Mobile settings
DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Source types
Ingest actions
DISTRIBUTED ENVIRONMENT
Agent management
Indexer clustering
Federation
Distributed search
USERS AND AUTHENTICATION
Roles
Users
Tokens
Password management
Authentication methods
127.0.0.1:8000/en-US/manager/search/adddata


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
What data do you want to send to the Splunk platform?
Follow guides for onboarding popular data sources
Cloud computing
Get your cloud computing data in to the Splunk platform.
10 data sources
Networking
Get your networking data in to the Splunk platform.
2 data sources
Operating System
Get your operating system data in to the Splunk platform.
1 data source
Security
Get your security data in to the Splunk platform.
3 data sources
4 data sources in total
Or get data in with the following methods
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

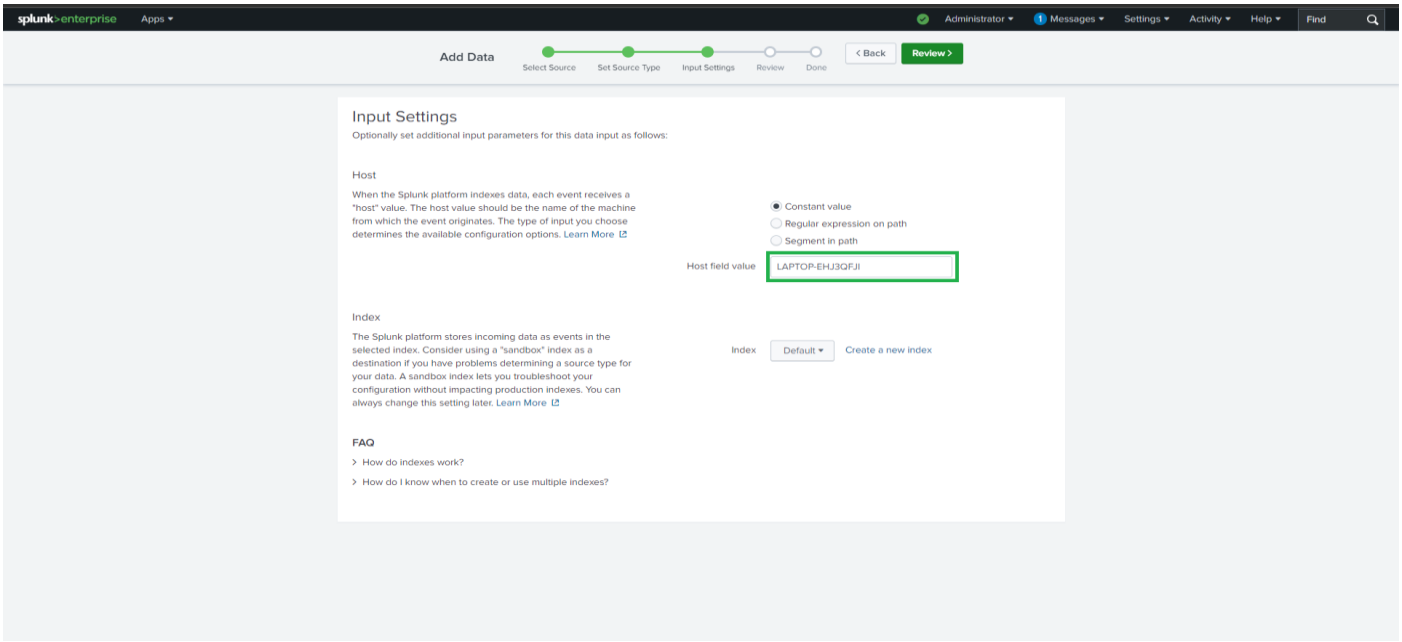

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Next >
Select Source
Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More
Selected File: No file selected
Select File
Drop your data file here
The maximum file upload size is 500 Mb
FAQ
What kinds of files can the Splunk platform index?
What is a source?
How do I get remote data onto my Splunk platform instance?

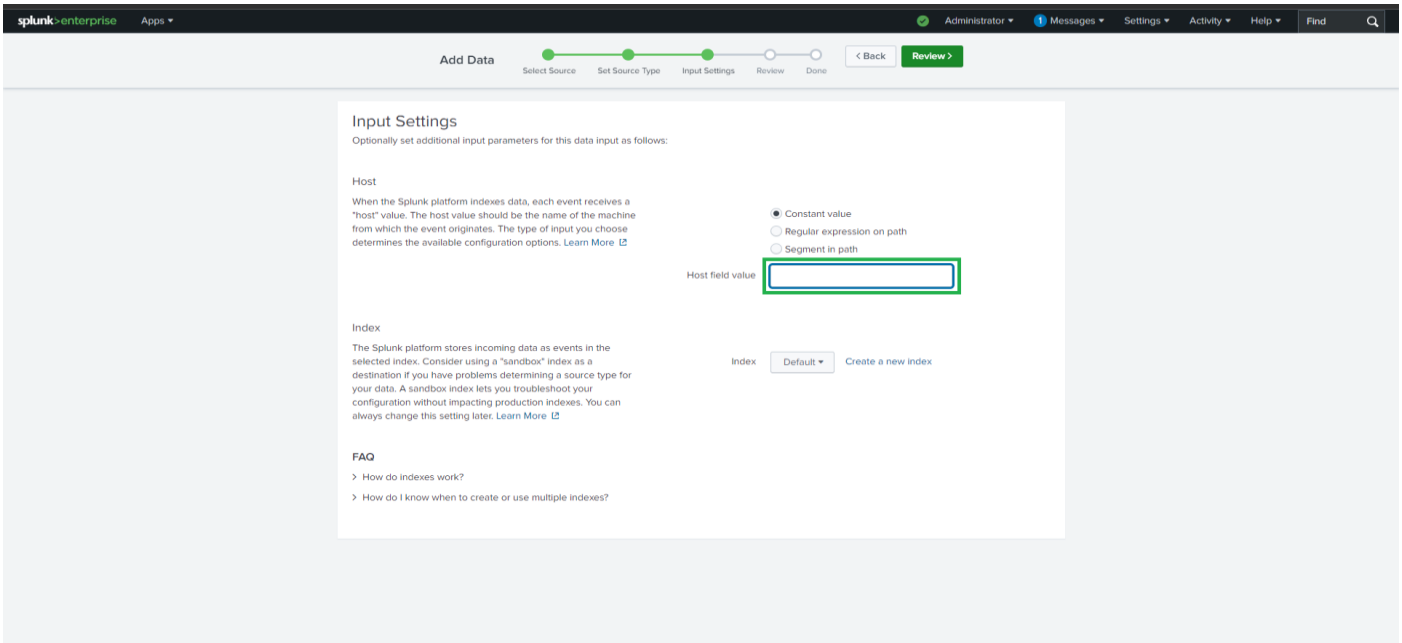


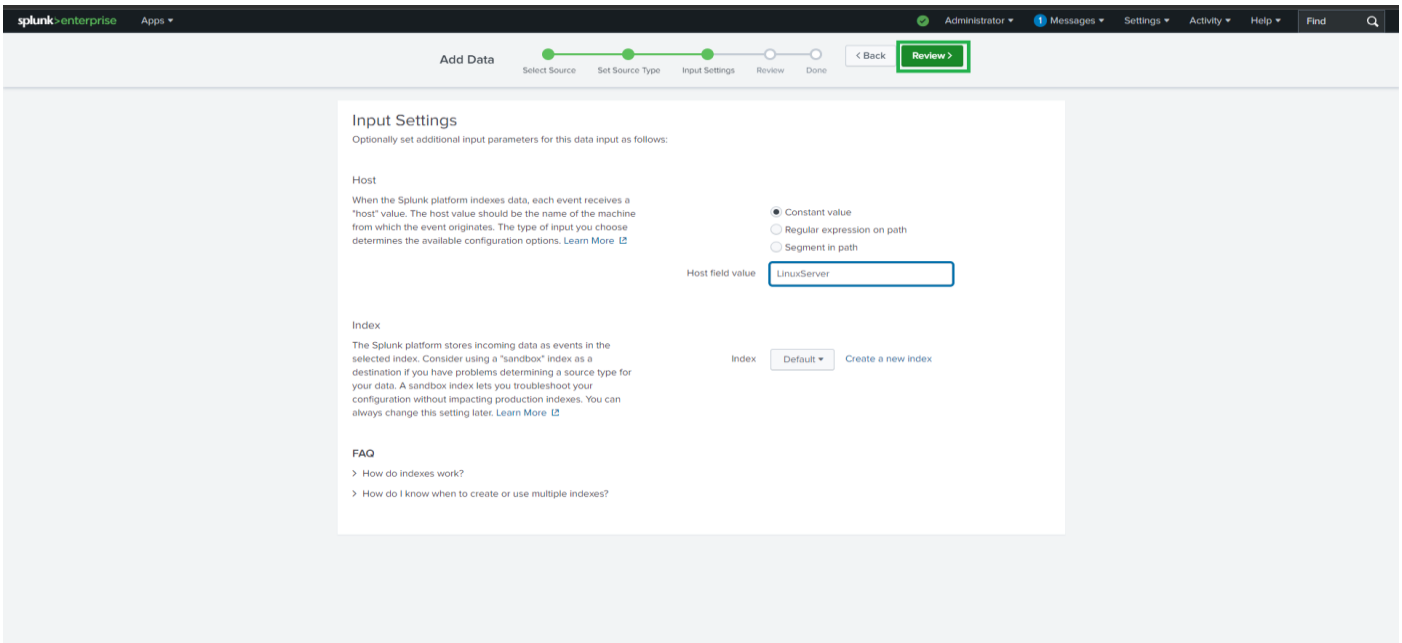


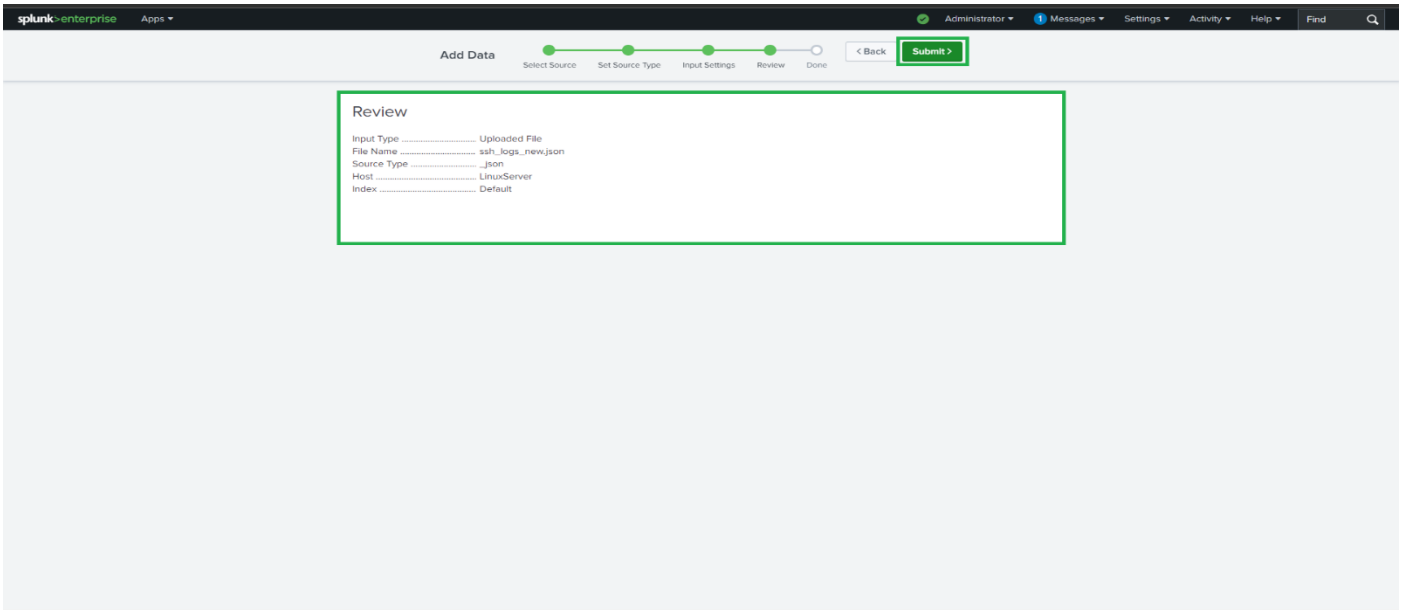


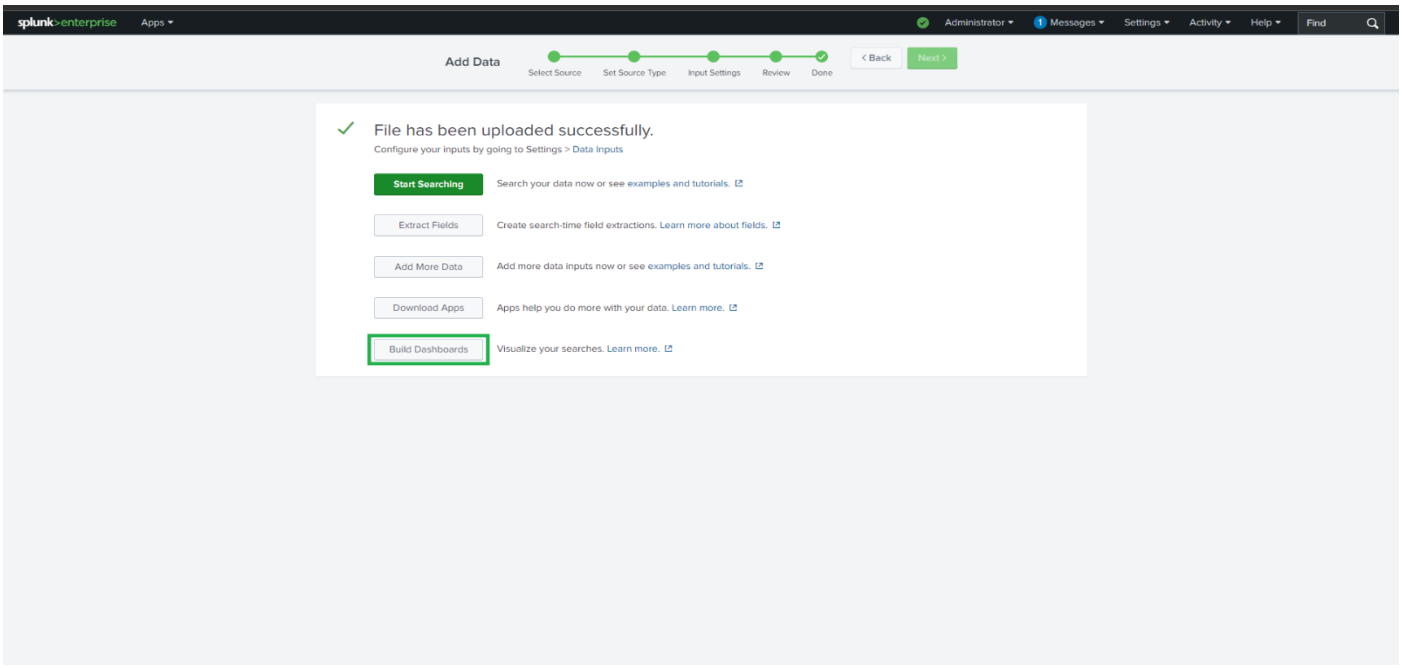
	_time	auth_attempts	auth_success	conn_state	event_type	history	id.orig_h	id.orig_p	id.resp_h	id.resp_p	missed_bytes	orig_ip_bytes	orig
1	4/24/25 3:50:09.508 PM	1	true	SF	Successful SSH Login	ShADadfF	31.184.137.182	58221	164.254.24.82	22	0	3234	49
2	4/24/25 3:50:09.508 PM	1	false	SF	Failed SSH Login	ShADadfF	129.164.50.72	26957	164.186.59.85	22	0	1197	21
3	4/24/25 3:50:09.508 PM	8	false	SF	Multiple Failed Authentication Attempts	ShADadfF	135.55.210.223	42848	91.14.145.242	22	0	702	13
4	4/24/25 3:50:09.508 PM	1	false	SF	Failed SSH Login	ShADadfF	125.123.103.182	47789	170.170.25.84	22	0	1168	16
5	4/24/25 3:50:09.508 PM	1	true	SF	Successful SSH Login	ShADadfF	4.5.47.4	30192	123.158.160.191	22	0	876	12
6	4/24/25 3:50:09.508 PM	6	false	SF	Multiple Failed Authentication Attempts	ShADadfF	78.164.1.207	32500	91.14.145.242	22	0	1848	28
7	4/24/25 3:50:09.508 PM	0	null	SF	Connection Without Authentication	ShADadfF	111.129.222.243	47980	80.101.200.117	22	0	3150	42
8	4/24/25 3:50:09.508 PM	1	false	SF	Failed SSH Login	ShADadfF	74.165.131.224	34955	164.186.59.85	22	0	2350	50
9	4/24/25 3:50:09.508 PM	4	false	SF	Multiple Failed Authentication Attempts	ShADadfF	74.165.131.224	20693	123.158.160.191	22	0	2262	29

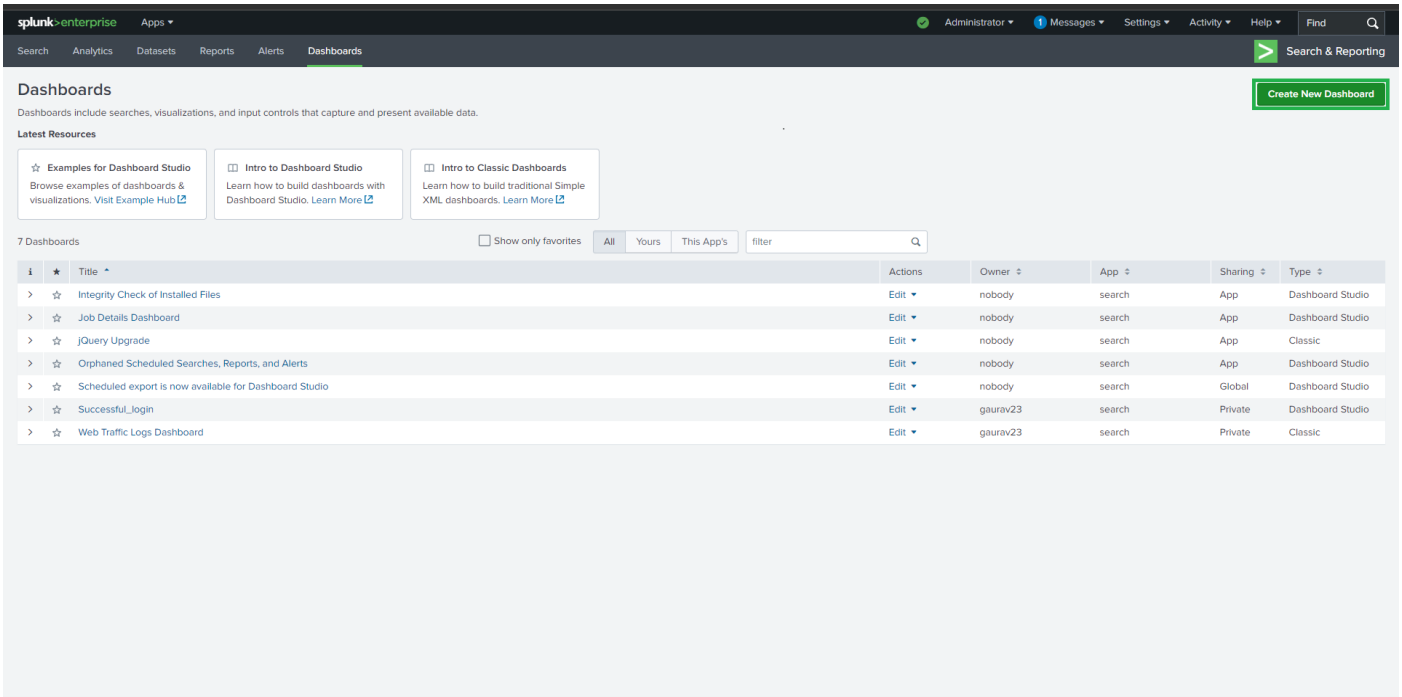

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Review >
Input Settings
Optionally set additional input parameters for this data input as follows:
Host
When the Splunk platform indexes data, each event 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?

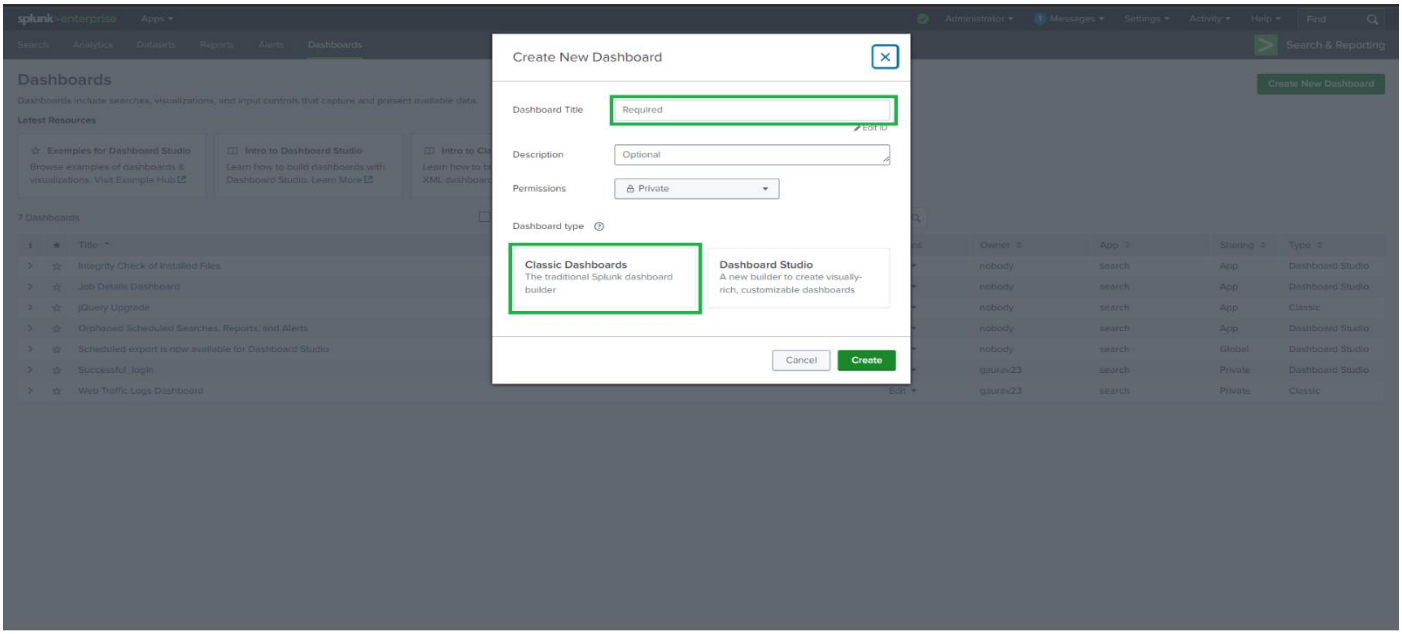

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Review >
Input Settings
Optionally set additional input parameters for this data input as follows:
Host
When the Splunk platform indexes data, each event 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
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?

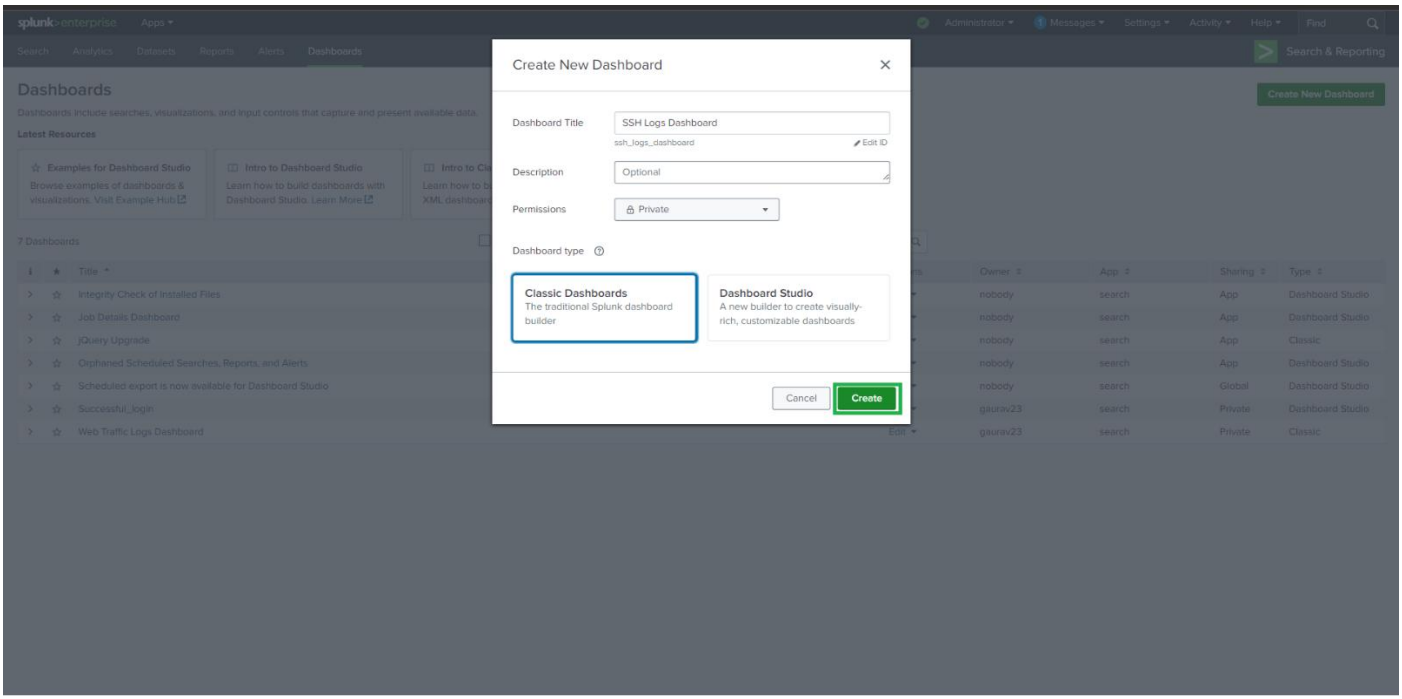

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Review >
Input Settings
Optionally set additional input parameters for this data input as follows:
Host
When the Splunk platform indexes data, each event 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
LinuxServer
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?


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_new.json
Source Type ..... _json
Host ..... LinuxServer
Index ..... Default


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Next >
File has been uploaded successfully.
Configure your inputs by going to Settings > Data Inputs
Start Searching
Search your data now or see examples and tutorials.
Extract Fields
Create search-time field extractions. Learn more about fields.
Add More Data
Add more data inputs now or see examples and tutorials.
Download Apps
Apps help you do more with your data. Learn more.
Build Dashboards
Visualize your searches. Learn more.


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Dashboards
Create New Dashboard
Dashboards include searches, visualizations, and input controls that capture and present available data.
Latest Resources
Examples for Dashboard Studio
Browse examples of dashboards & visualizations. Visit Example Hub
Intro to Dashboard Studio
Learn how to build dashboards with Dashboard Studio. Learn More
Intro to Classic Dashboards
Learn how to build traditional Simple XML dashboards. Learn More
7 Dashboards
Show only favorites
All
Yours
This App's
filter
Title
Actions
Owner
App
Sharing
Type
Integrity Check of Installed Files
Edit
nobody
search
App
Dashboard Studio
Job Details Dashboard
Edit
nobody
search
App
Dashboard Studio
jQuery Upgrade
Edit
nobody
search
App
Classic
Orphaned Scheduled Searches, Reports, and Alerts
Edit
nobody
search
App
Dashboard Studio
Scheduled export is now available for Dashboard Studio
Edit
nobody
search
Global
Dashboard Studio
Successful_login
Edit
gaurav23
search
Private
Dashboard Studio
Web Traffic Logs Dashboard
Edit
gaurav23
search
Private
Classic


Create New Dashboard
Dashboard Title
Required
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
Cancel
Create


Create New Dashboard
Dashboard Title
SSH Logs Dashboard
ssh_logs_dashboard
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
Cancel
Create

⏱️ Task 0: Setting Up Time Range

Goal

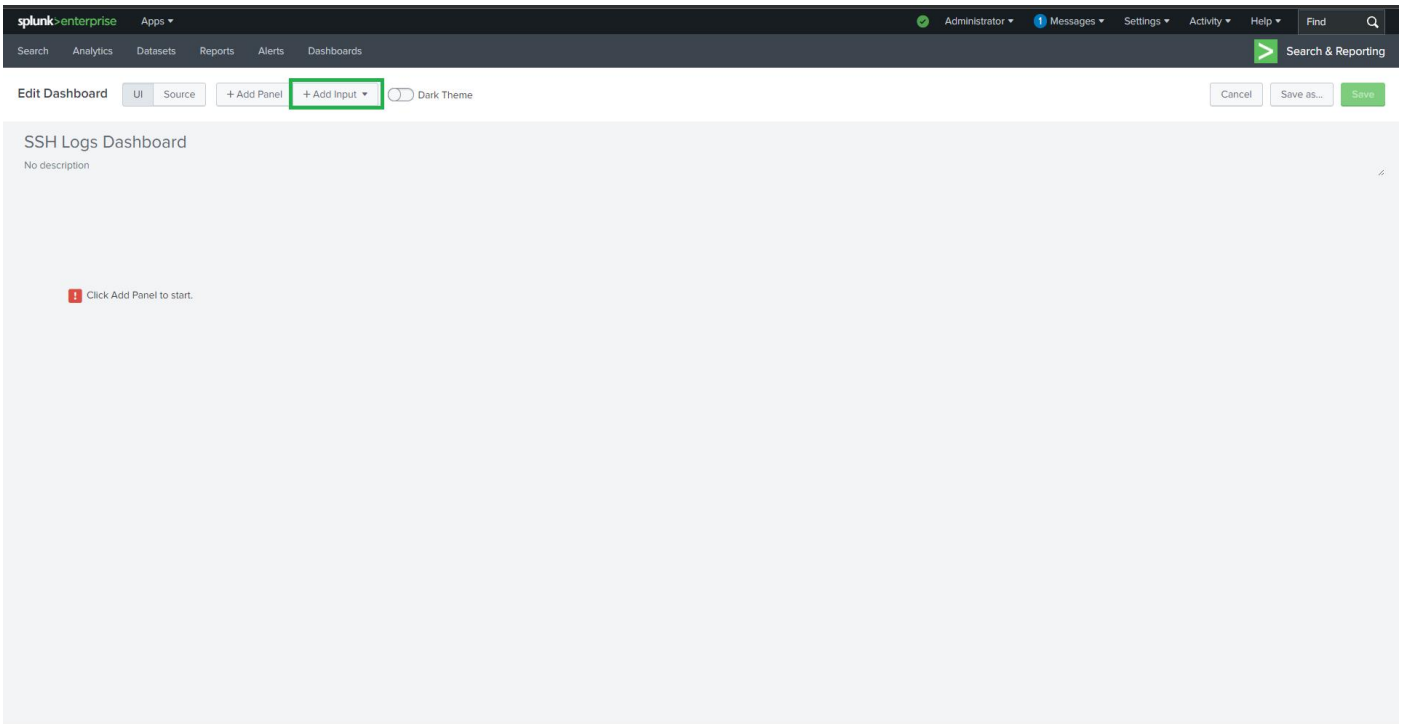
Ensure **consistent time filtering** across all dashboard panels.

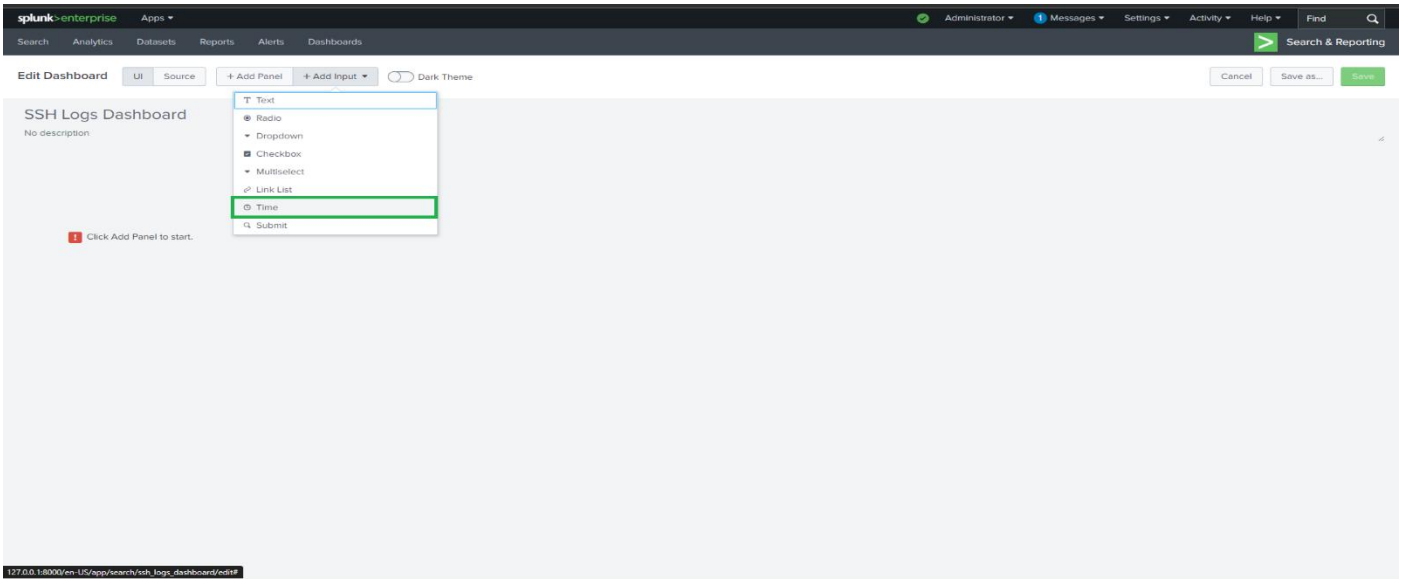
Steps

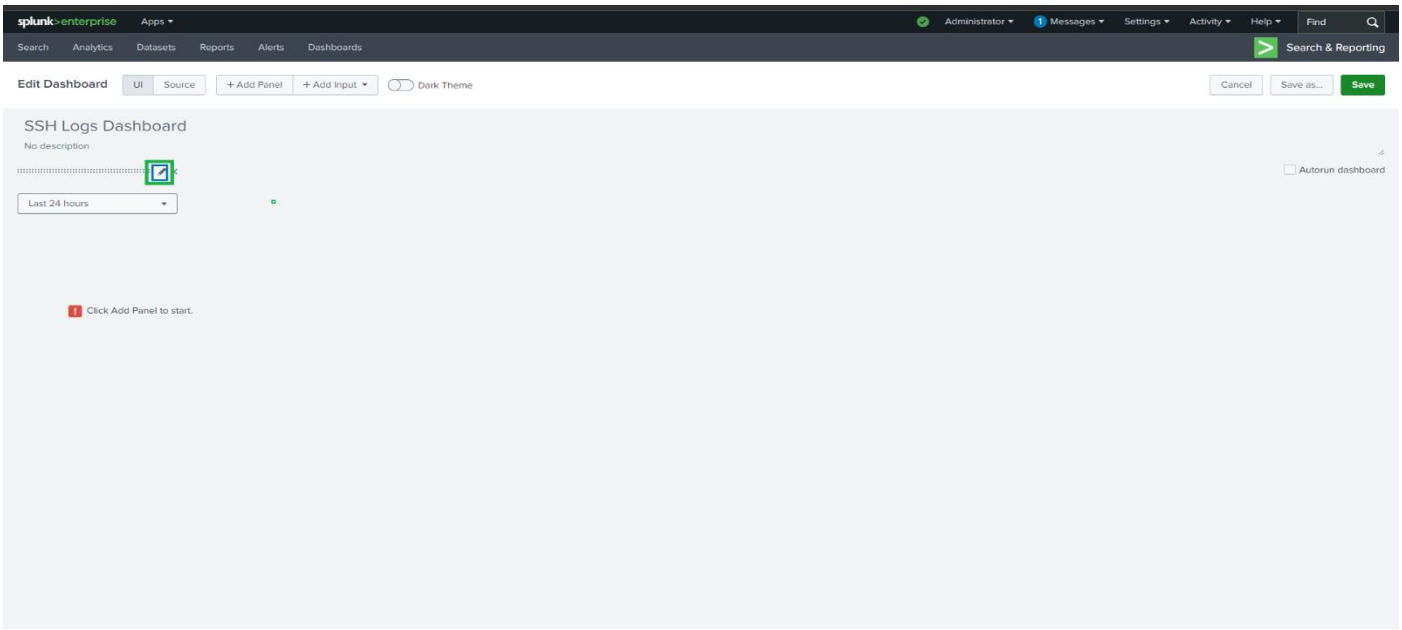
1. Click **Add Time Range Button**
2. Click **Add Input**
3. Select **Time**
4. Click the **Pencil Icon**
5. Set:
    - **Label:** Time Range
    - **Token:** time_range
6. Click **Add Input**
7. Select **Submit**

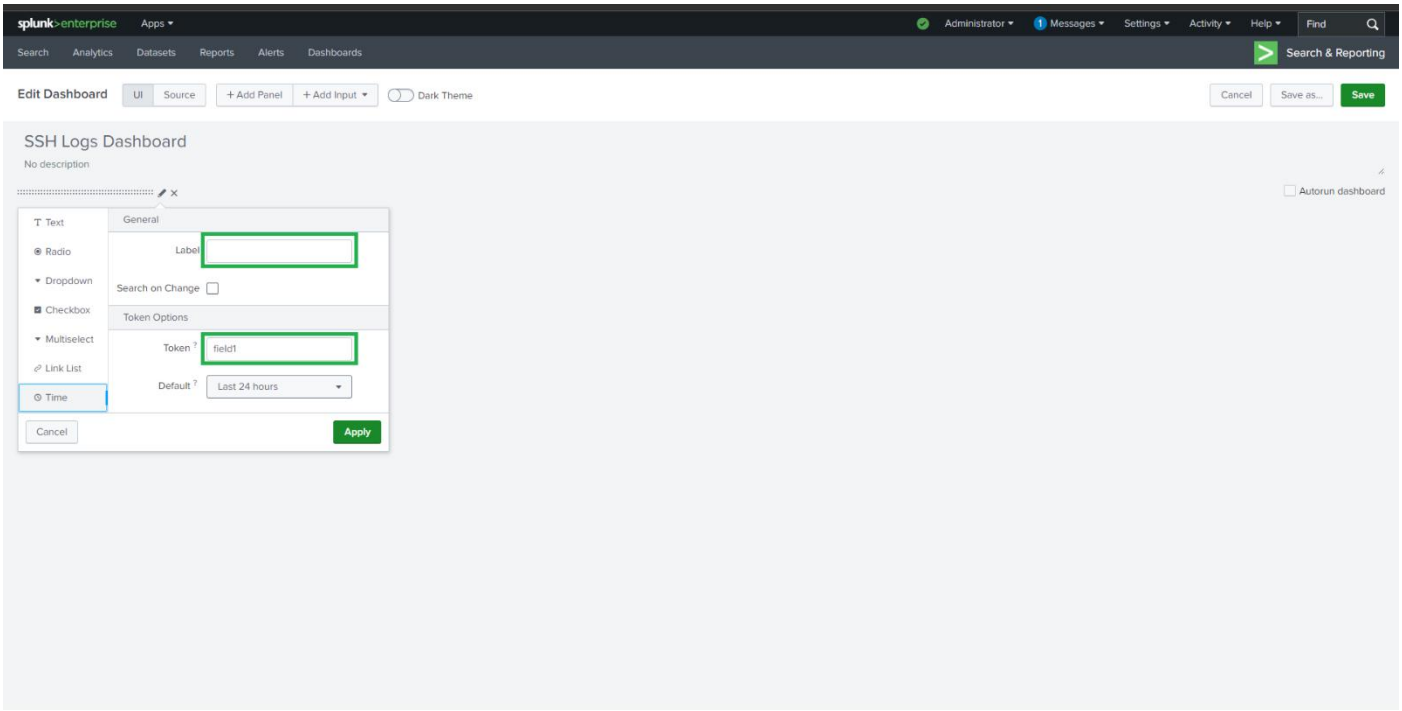
⚠️ Note:

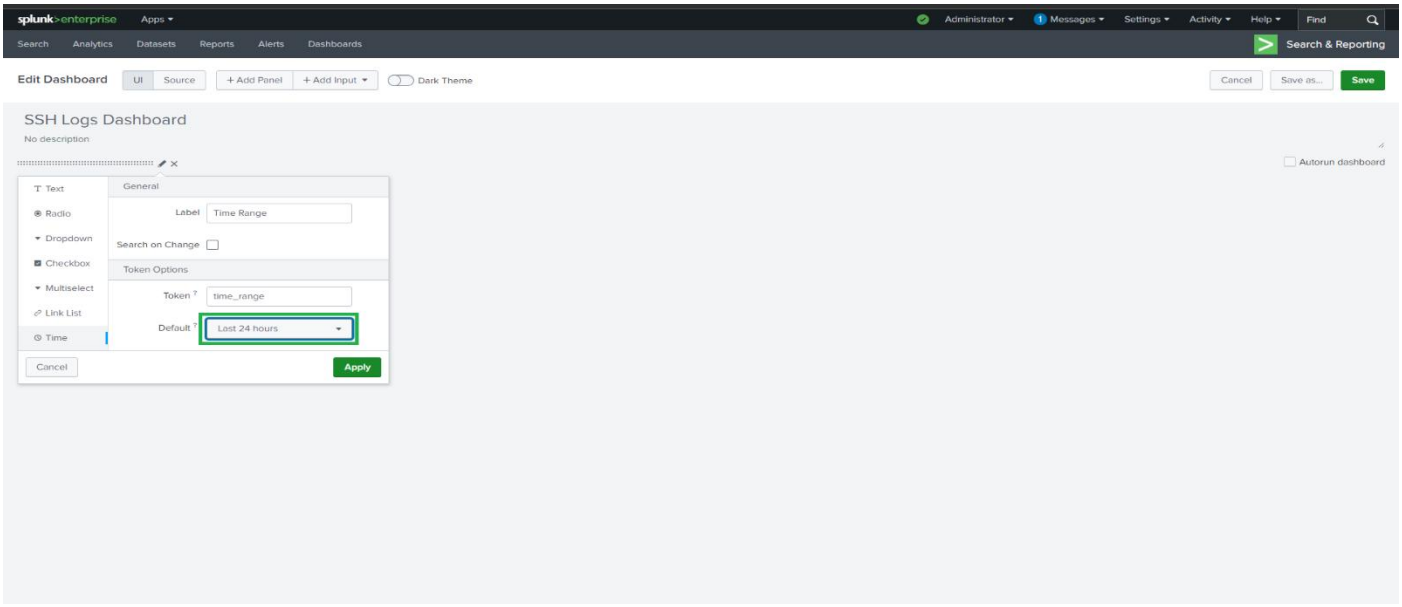
For **all future panels**, set the **Time Picker** to time_range for consistency.

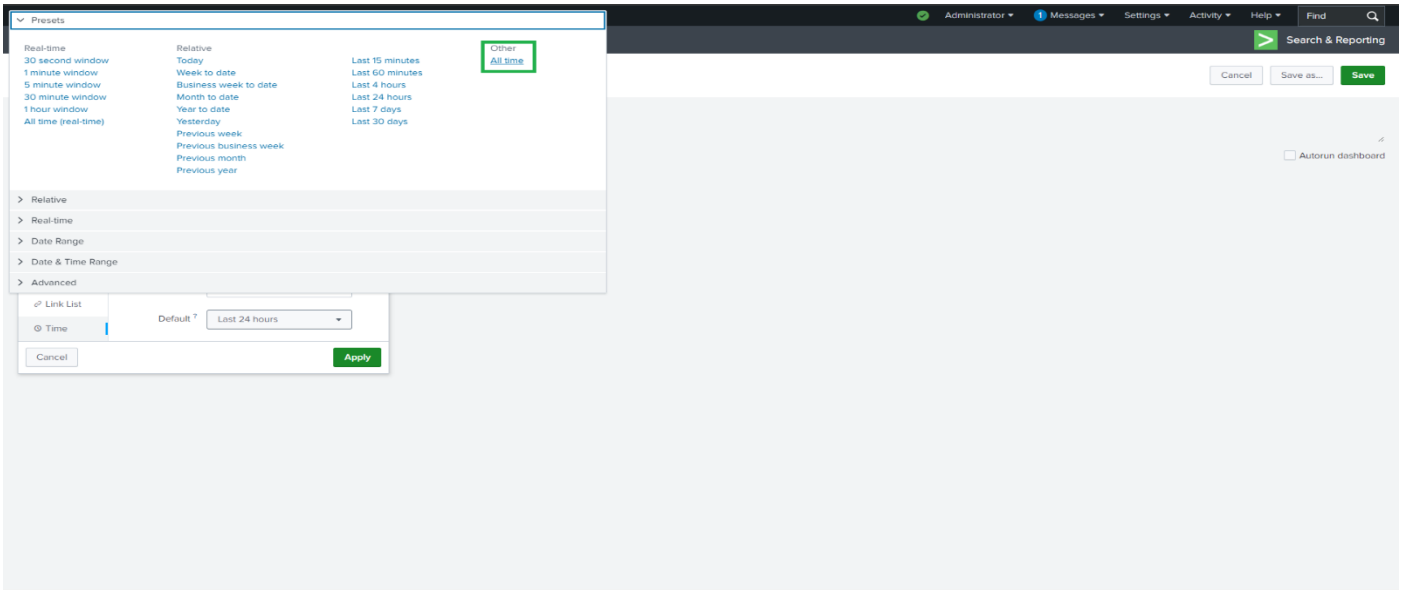


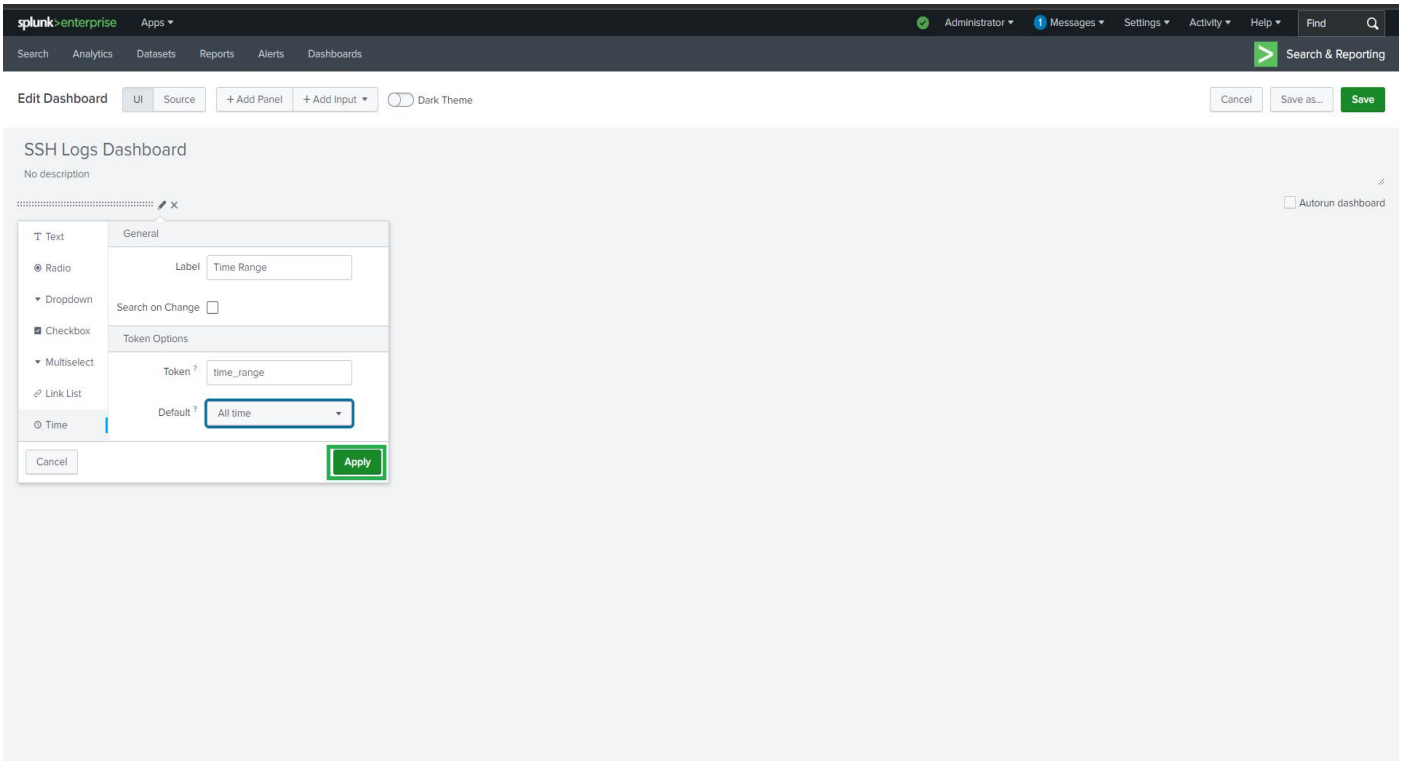

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Text
Radio
Dropdown
Checkbox
Multiselect
Link List
Time
Submit
Click Add Panel to start.
127.0.0.1:8000/en-US/app/search/ssh_logs_dashboard/edit#

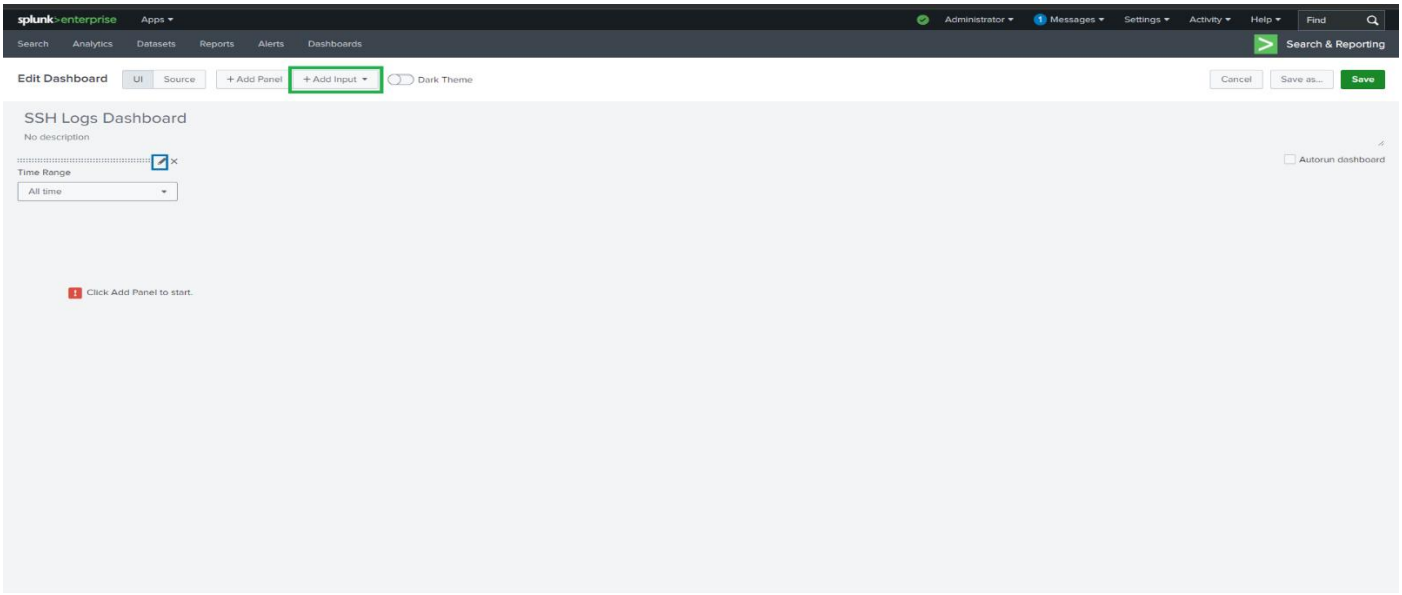

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Autorun dashboard
Last 24 hours
Click Add Panel to start.

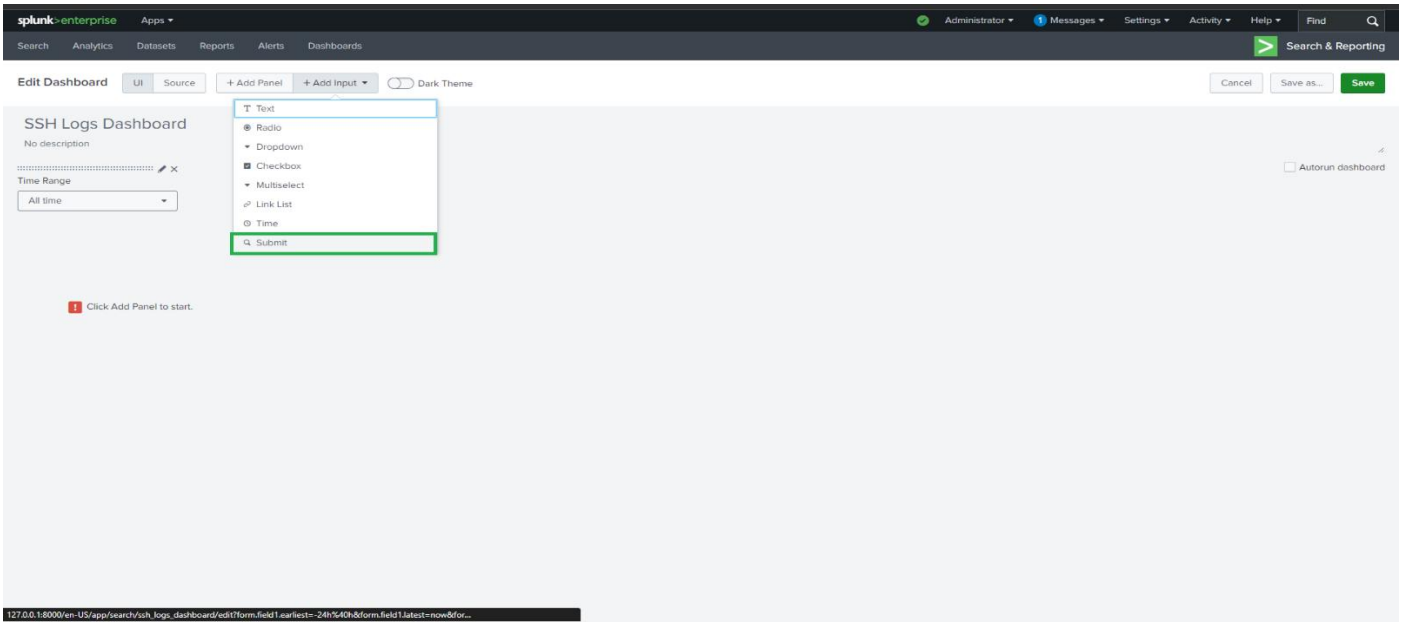

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Autorun dashboard
Text
Radio
Dropdown
Checkbox
Multiselect
Link List
Time
General
Label
Search on Change
Token Options
Token
field1
Default
Last 24 hours
Cancel
Apply

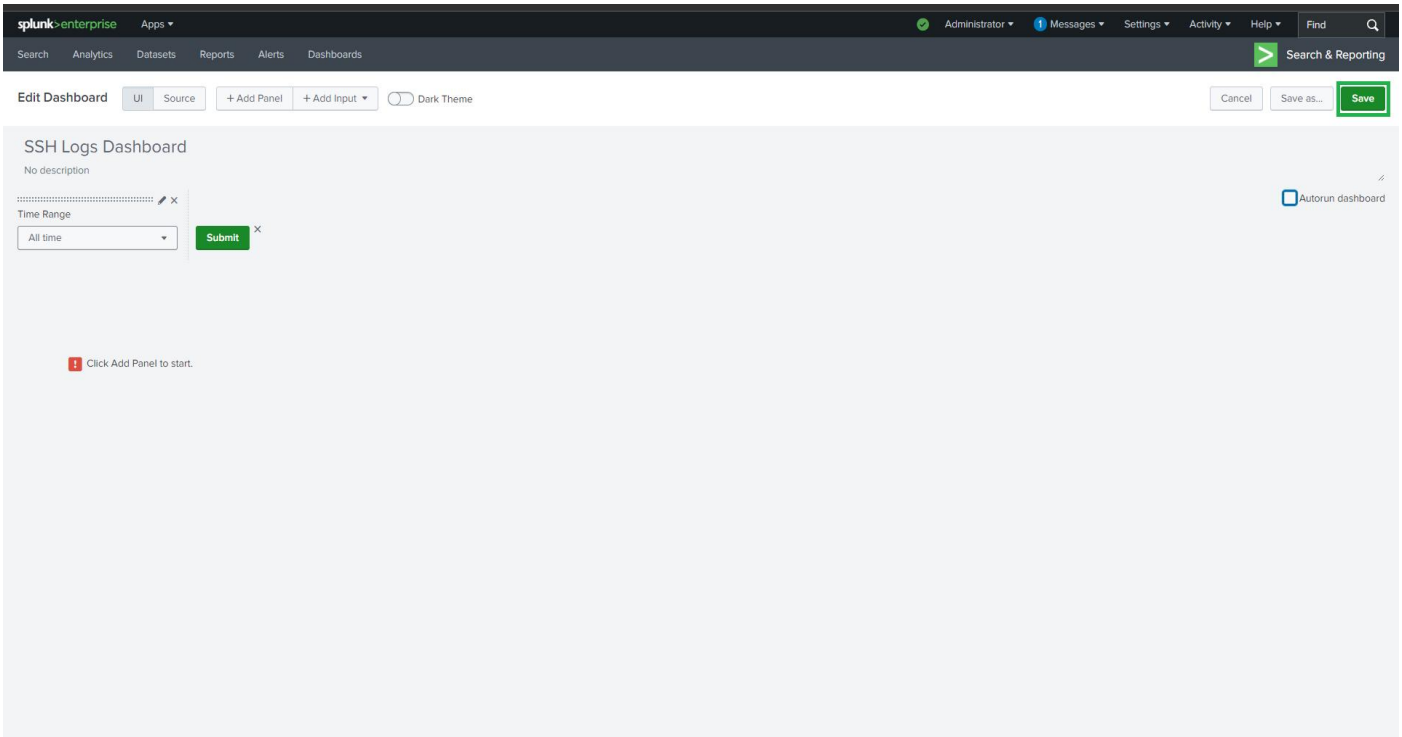

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Autorun dashboard
Text
Radio
Dropdown
Checkbox
Multiselect
Link List
Time
General
Label
Time Range
Search on Change
Token Options
Token
time_range
Default
Last 24 hours
Cancel
Apply


Presets
Real-time
30 second window
1 minute window
5 minute window
30 minute window
1 hour window
All time (real-time)
Relative
Today
Week to date
Business week to date
Month to date
Year to date
Yesterday
Previous week
Previous business week
Previous month
Previous year
Last 15 minutes
Last 60 minutes
Last 4 hours
Last 24 hours
Last 7 days
Last 30 days
Other
All time
Relative
Real-time
Date Range
Date & Time Range
Advanced
Link List
Time
Default
Last 24 hours
Cancel
Apply


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Autorun dashboard
Text
Radio
Dropdown
Checkbox
Multiselect
Link List
Time
General
Label
Time Range
Search on Change
Token Options
Token
time_range
Default
All time
Cancel
Apply


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Click Add Panel to start.


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
Text
Radio
Dropdown
Checkbox
Multiselect
Link List
Time
Submit
SSH Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Click Add Panel to start.
127.0.0.1:8000/en-US/app/search/ssh_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now&for...


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
Click Add Panel to start.

🔐 Task 1: Authentication Overview Panels

Goal

Provide a **quick overview** of SSH authentication activity.

---

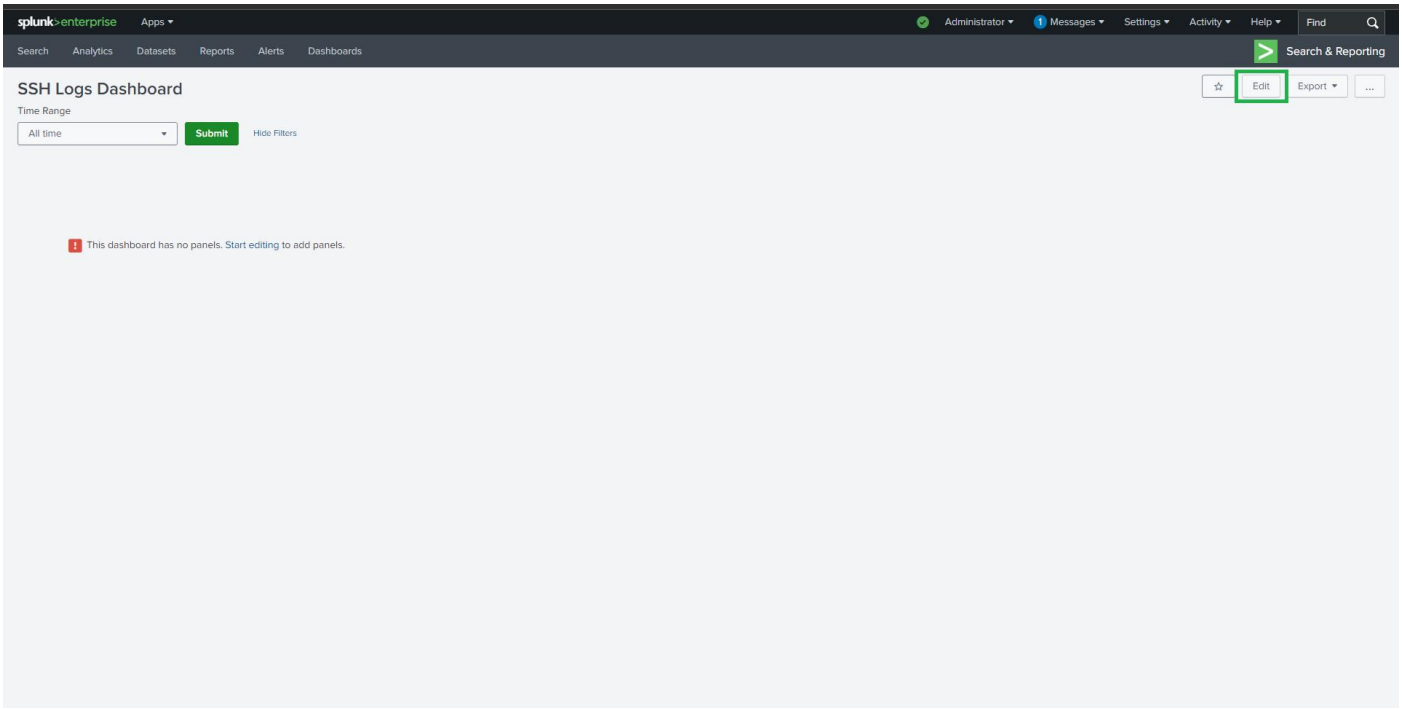
1. Total SSH Events

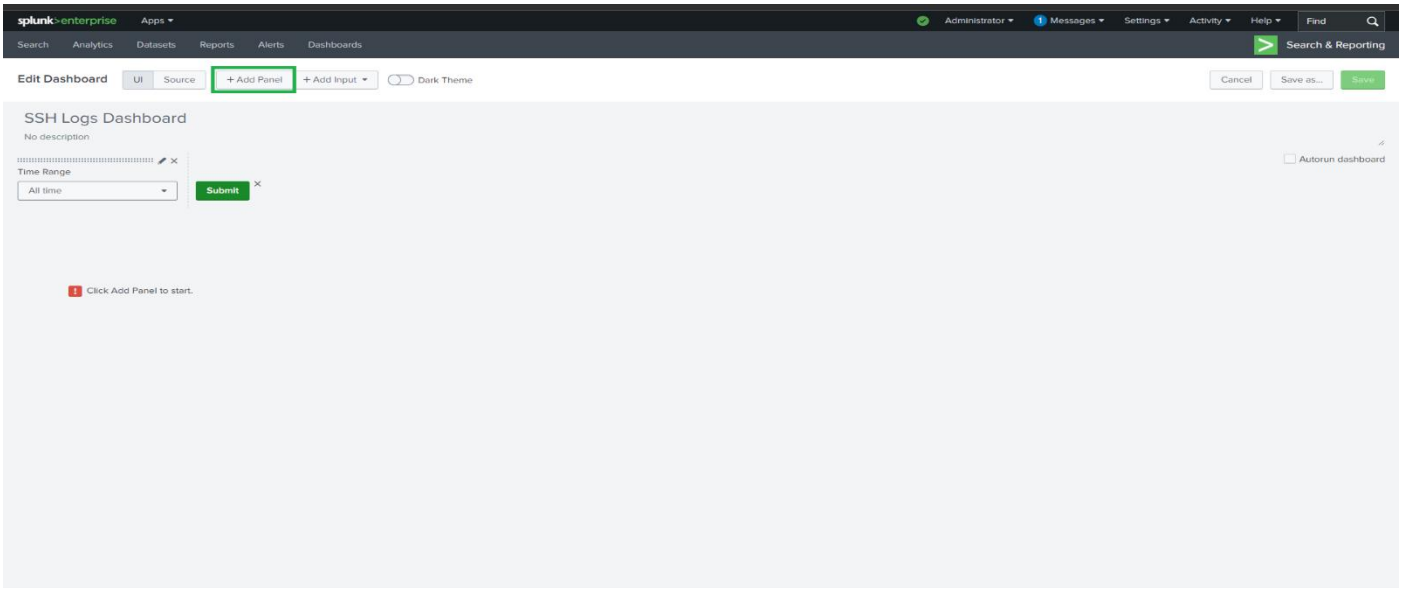
- **Panel Type:** Single Value
- **Time Picker:** time_range
- **Title:** Total SSH Events

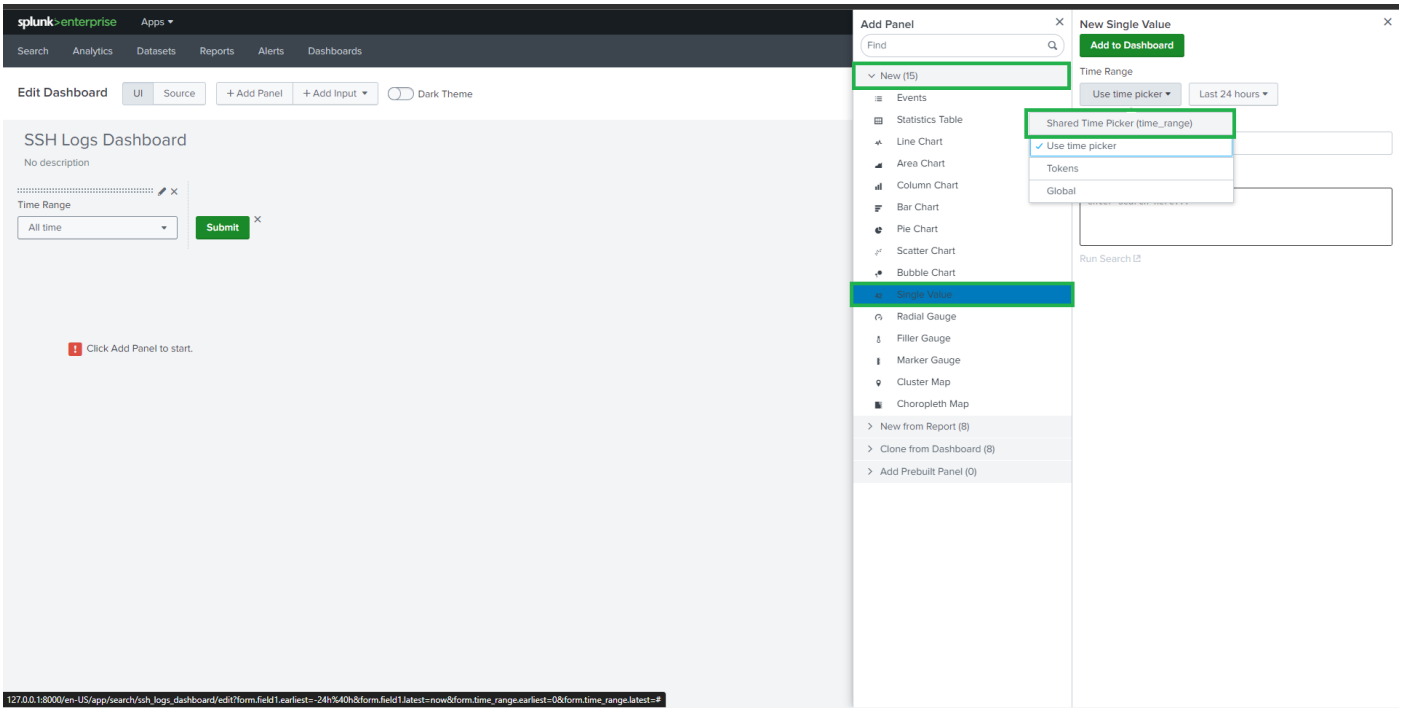
Search Query:

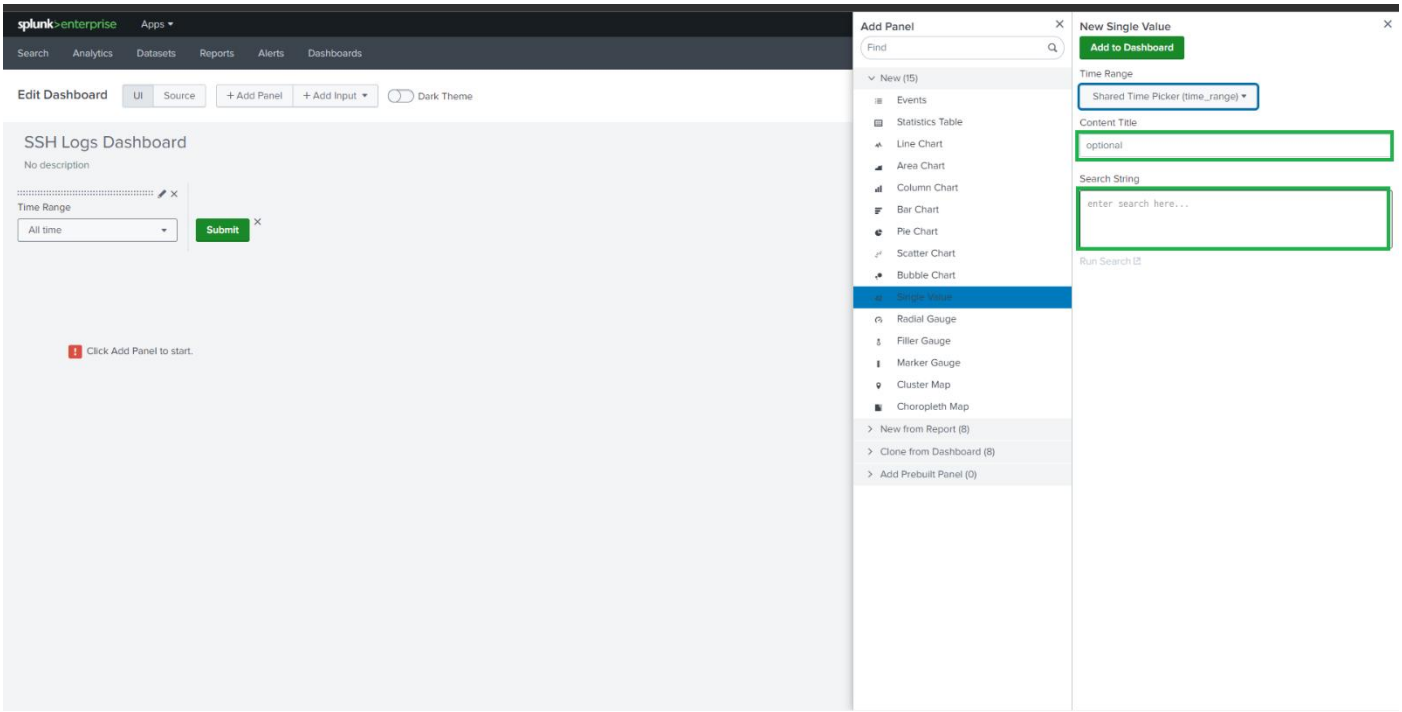
source="ssh_logs.json" host="LinuxServer" sourcetype="_json"

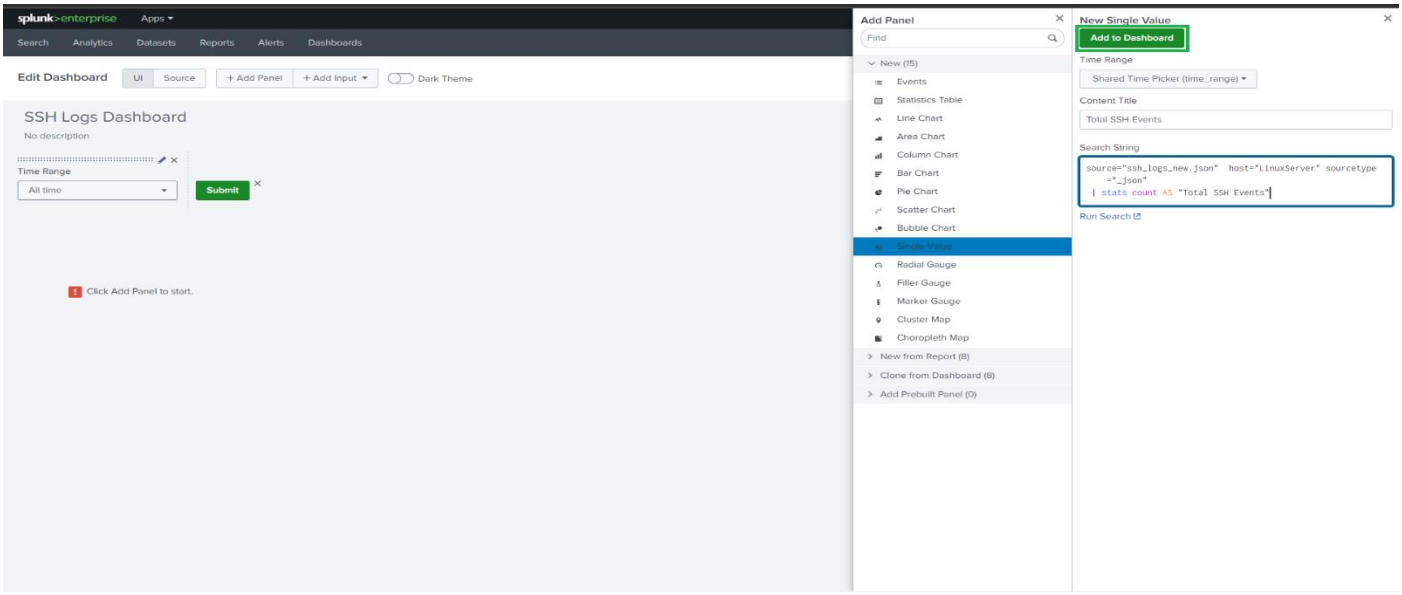
| stats count AS "Total SSH Events"

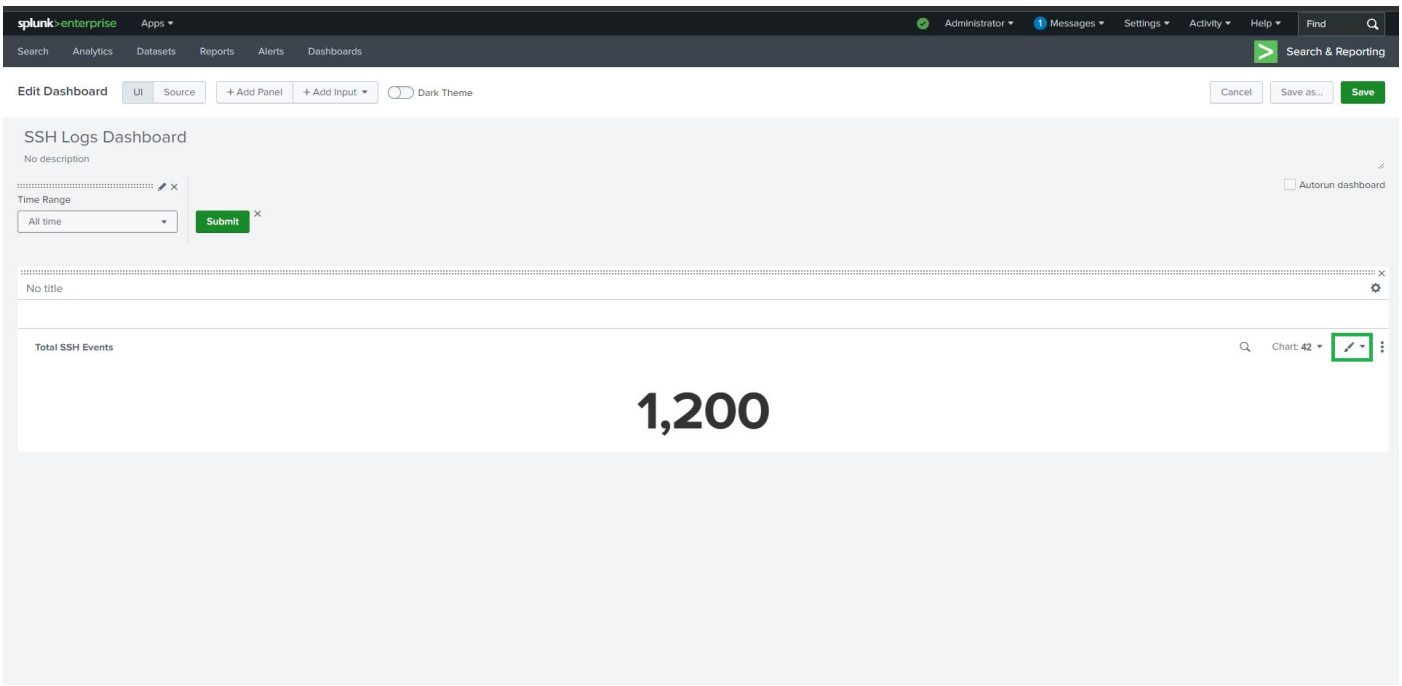


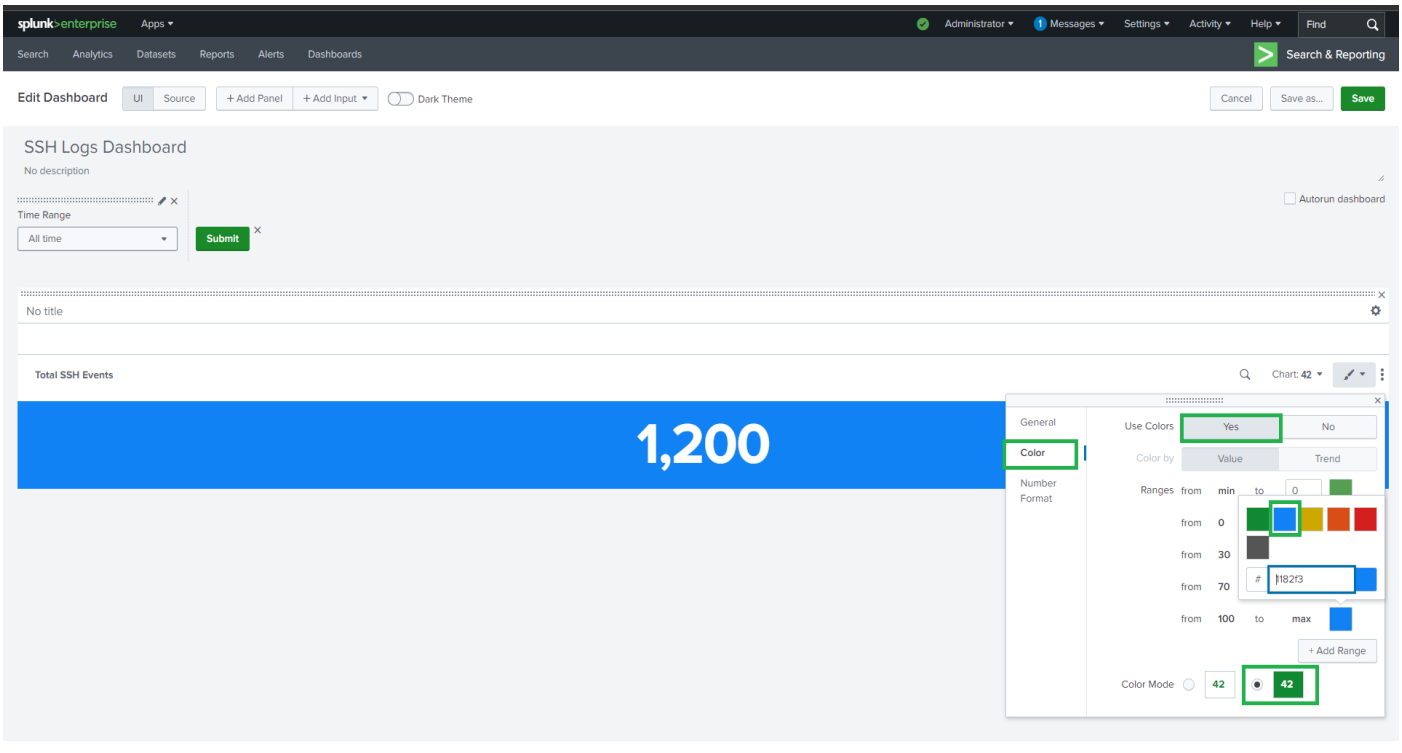

splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
Click Add Panel to start.

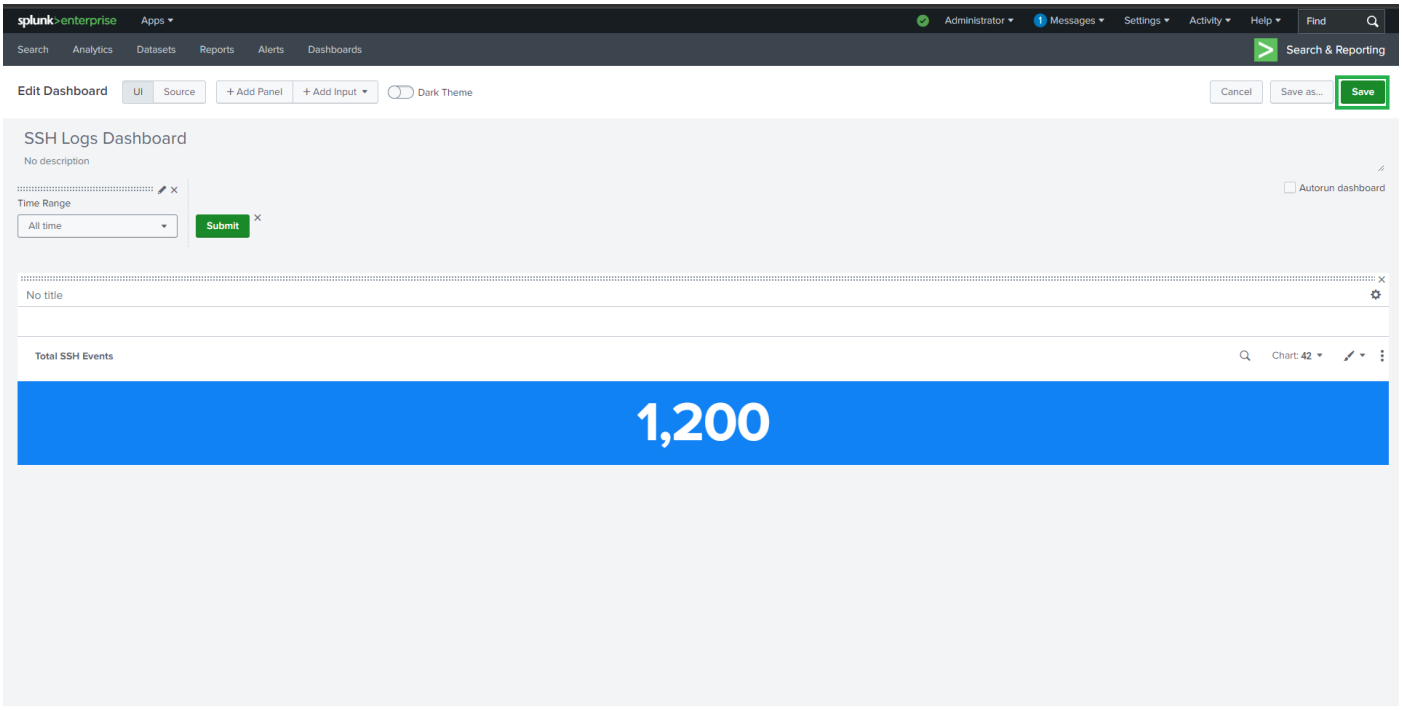

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
SSH Logs Dashboard
No description
Time Range
All time
Submit
Click Add Panel to start.
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (8)
Add Prebuilt Panel (0)
Shared Time Picker (time_range)
Use time picker
Tokens
Global
New Single Value
Add to Dashboard
Time Range
Use time picker
Last 24 hours
Run Search
127.0.0.1:8000/en-US/app/search/ssh_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now&form.time_range.earliest=0&form.time_range.latest=#


splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
SSH Logs Dashboard
No description
Time Range
All time
Submit
Click Add Panel to start.
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (8)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
optional
Search String
enter search here...
Run Search


splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
SSH Logs Dashboard
No description
Time Range
All time
Submit
Click Add Panel to start.
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (8)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
Total SSH Events
Search String
source="ssh_logs_new.json" host="LinuxServer" sourcetype
="_json"
| stats count AS "Total SSH Events"
Run Search


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total SSH Events
Chart: 42
1,200


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total SSH Events
Chart: 42
1,200
General
Color
Number Format
Use Colors
Yes
No
Color by
Value
Trend
Ranges
from min to 0
from 0
from 30
from 70
from 100 to max
#1182f3
+ Add Range
Color Mode
42
42



---

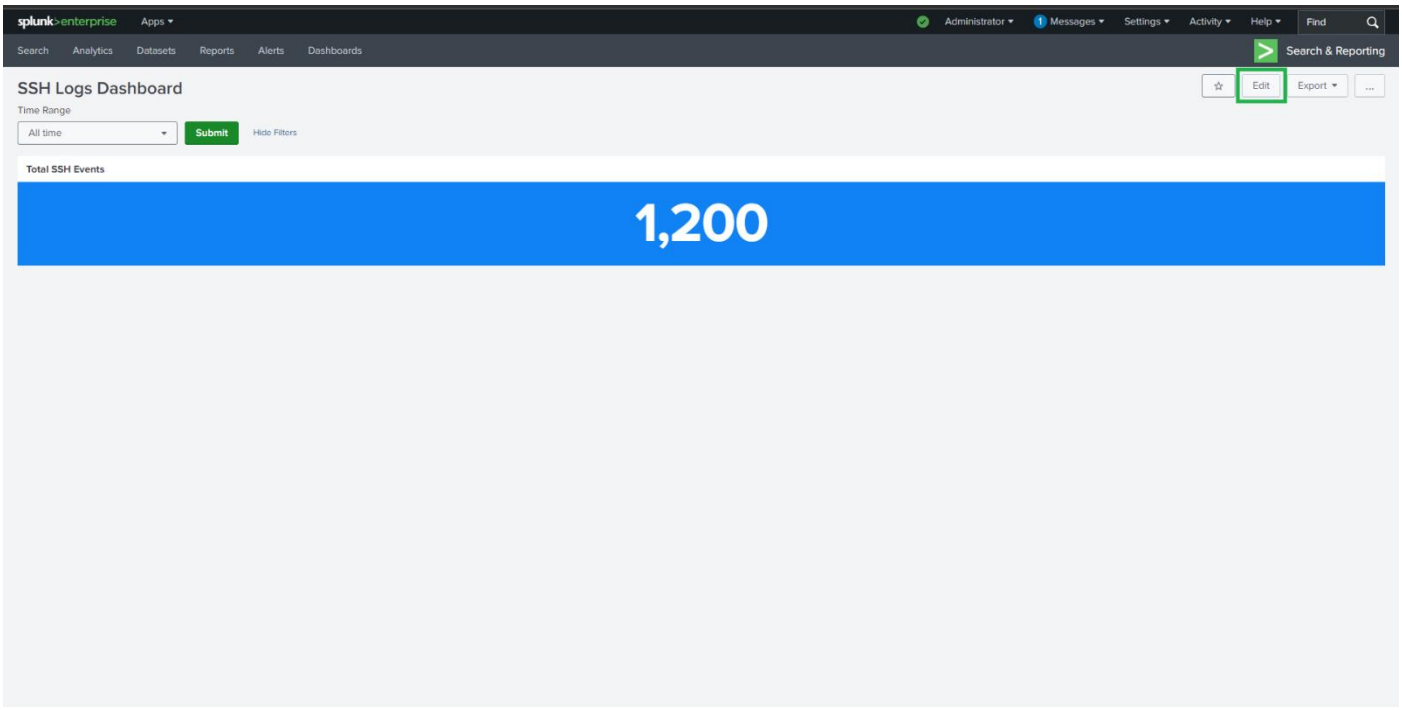
2. Successful Logins

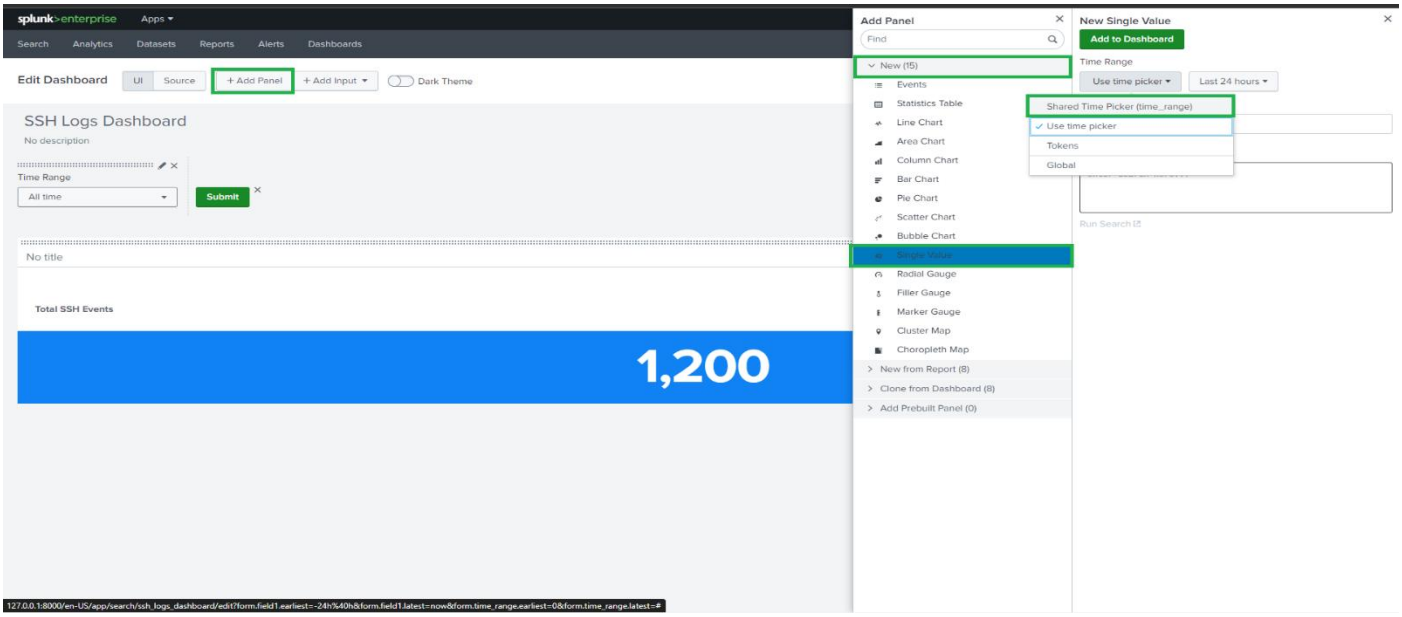
- **Panel Type:** Single Value
- **Time Picker:** time_range
- **Title:** Successful Logins

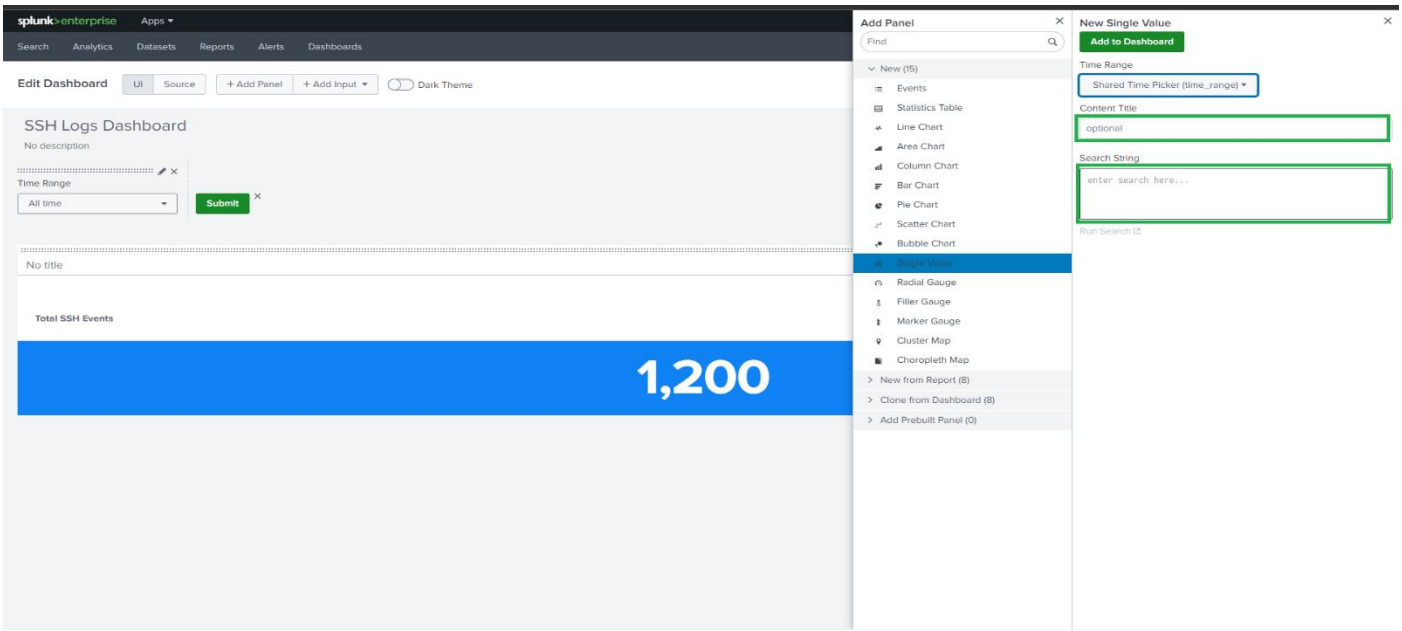
Search Query:

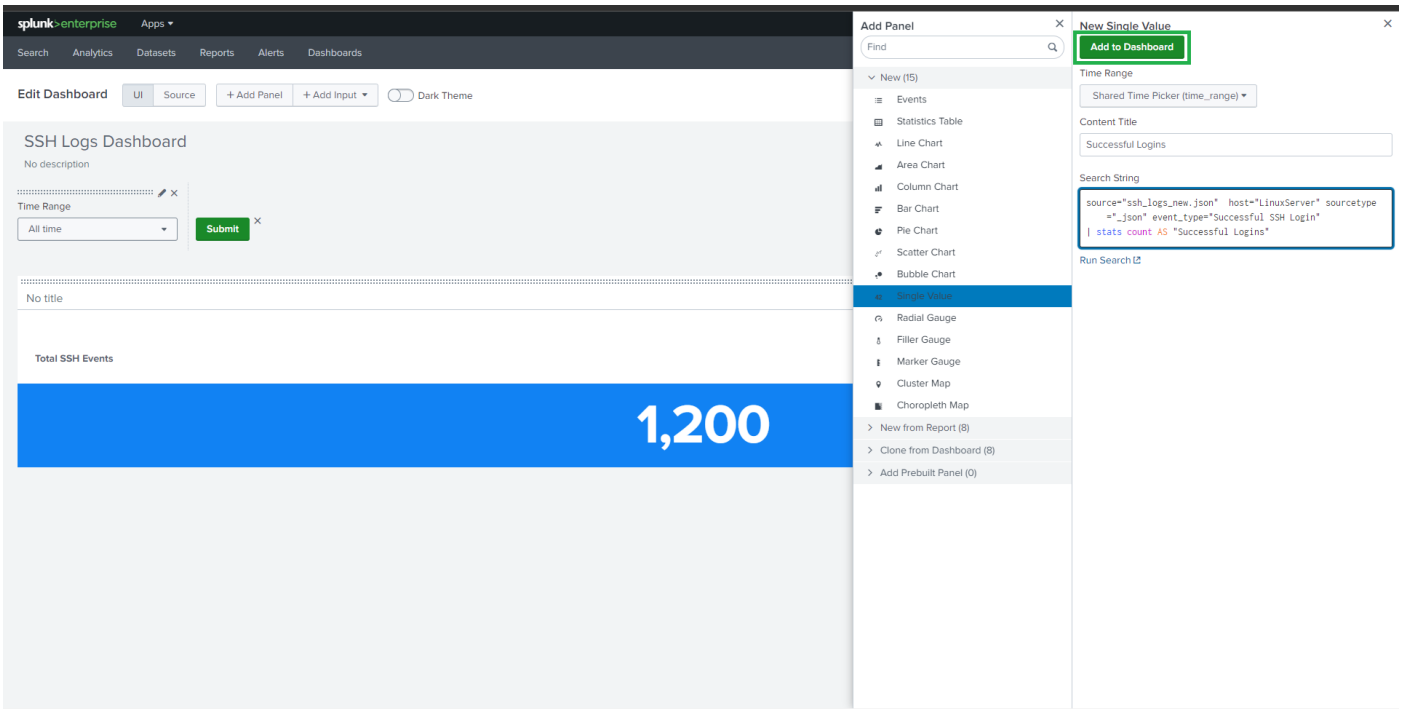
source="ssh_logs.json" host="LinuxServer" sourcetype="_json" event_type="Successful SSH Login"

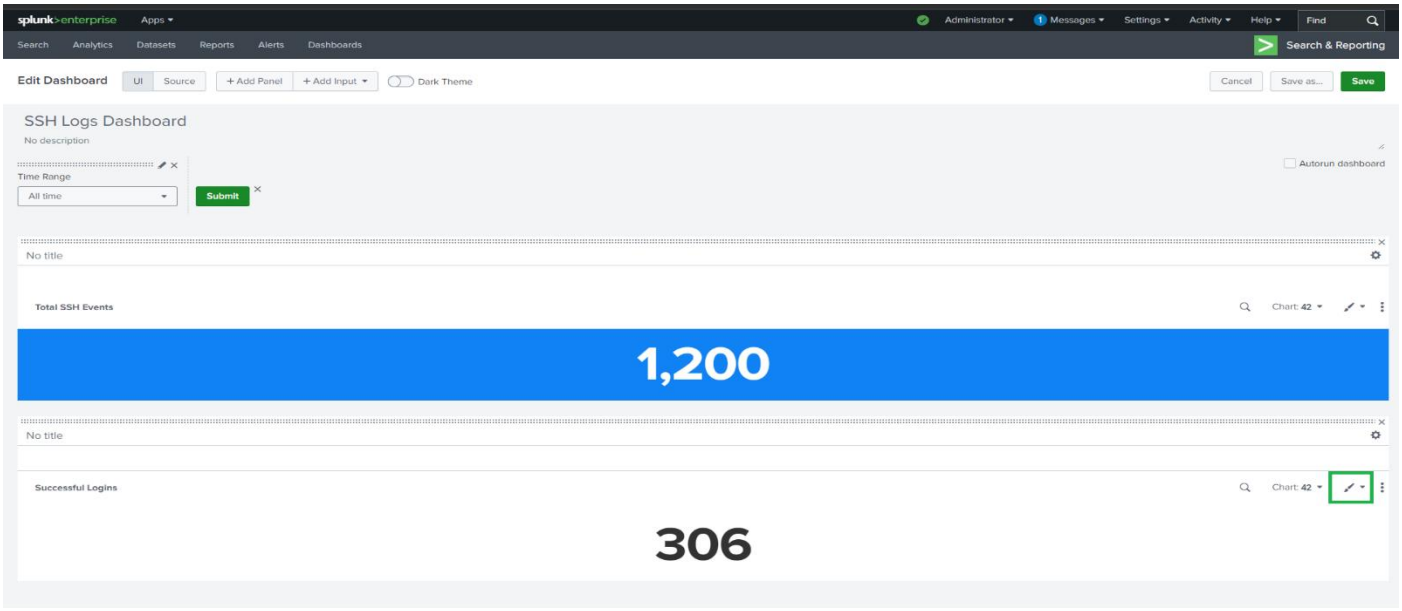
| stats count AS "Successful Logins"

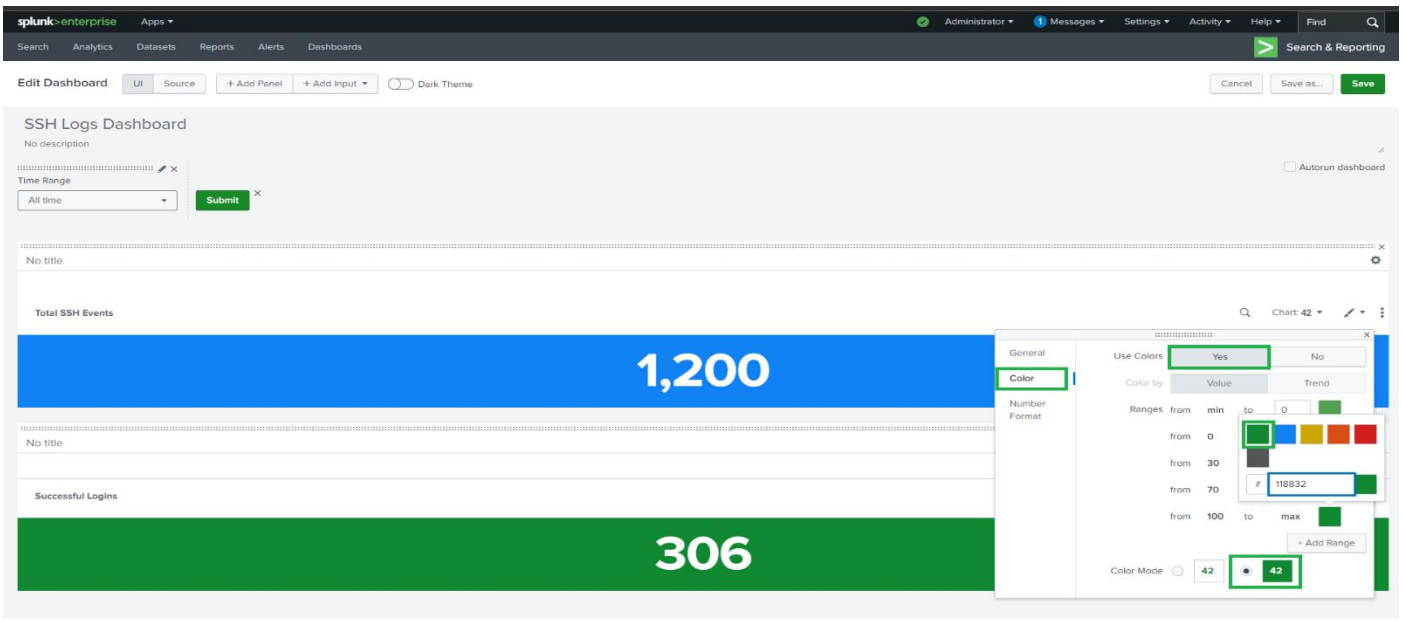


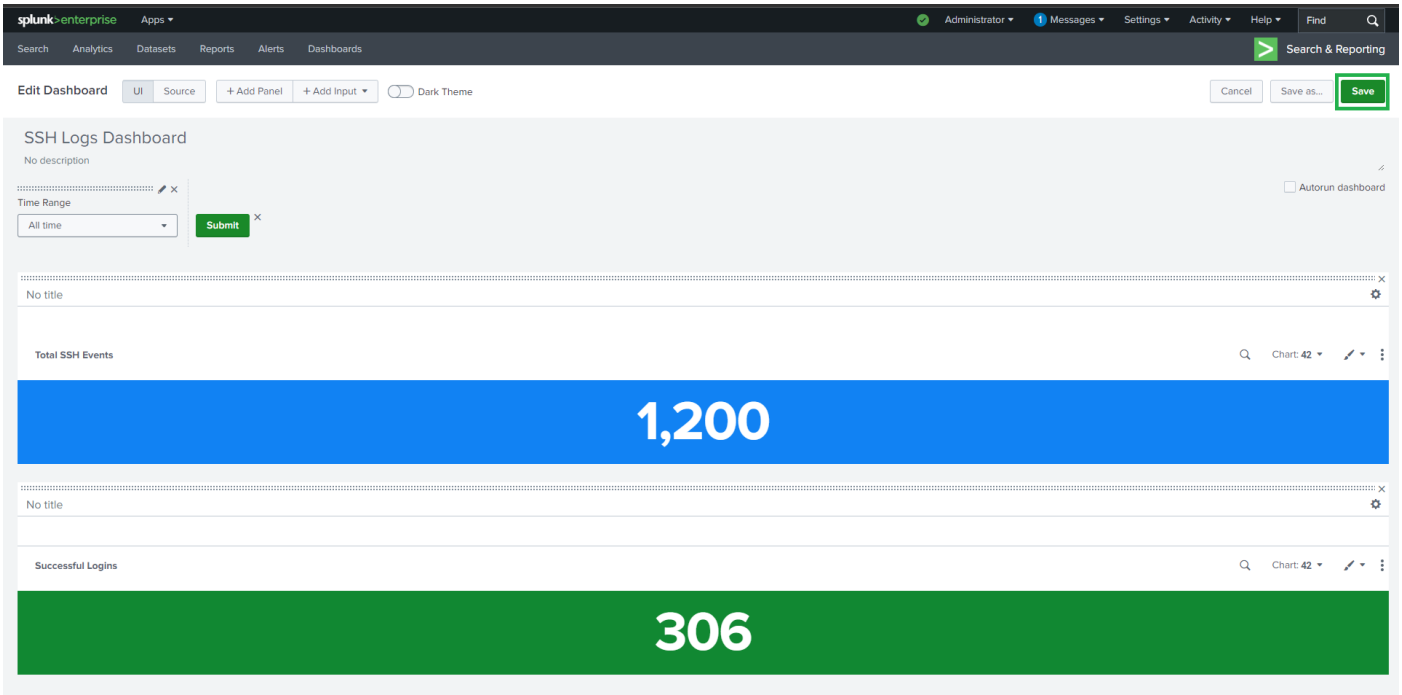

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
SSH Logs Dashboard
No description
Time Range
All time
Submit
No title
Total SSH Events
1,200
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (8)
Add Prebuilt Panel (0)
Shared Time Picker (time_range)
Use time picker
Tokens
Global
New Single Value
Add to Dashboard
Time Range
Use time picker
Last 24 hours
Run Search
127.0.0.1:8000/en-US/app/search/ssh_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now&form.time_range.earliest=0&form.time_range.latest=#


splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
SSH Logs Dashboard
No description
Time Range
All time
Submit
No title
Total SSH Events
1,200
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (8)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
optional
Search String
enter search here...
Run Search


splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
SSH Logs Dashboard
No description
Time Range
All time
Submit
No title
Total SSH Events
1,200
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (8)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
Successful Logins
Search String
source="ssh_logs_new.json" host="LinuxServer" sourcetype
="_json" event_type="Successful SSH Login"
| stats count AS "Successful Logins"
Run Search


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Time Range
All time
Submit
Autorun dashboard
No title
Total SSH Events
Chart: 42
1,200
No title
Successful Logins
Chart: 42
306


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Time Range
All time
Submit
Autorun dashboard
No title
Total SSH Events
Chart: 42
1,200
No title
Successful Logins
306
General
Color
Number Format
Use Colors
Yes
No
Color by
Value
Trend
Ranges
from min to 0
from 0
from 30
from 70
from 100 to max
118832
+ Add Range
Color Mode
42
42


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Time Range
All time
Submit
Autorun dashboard
No title
Total SSH Events
Chart: 42
1,200
No title
Successful Logins
Chart: 42
306

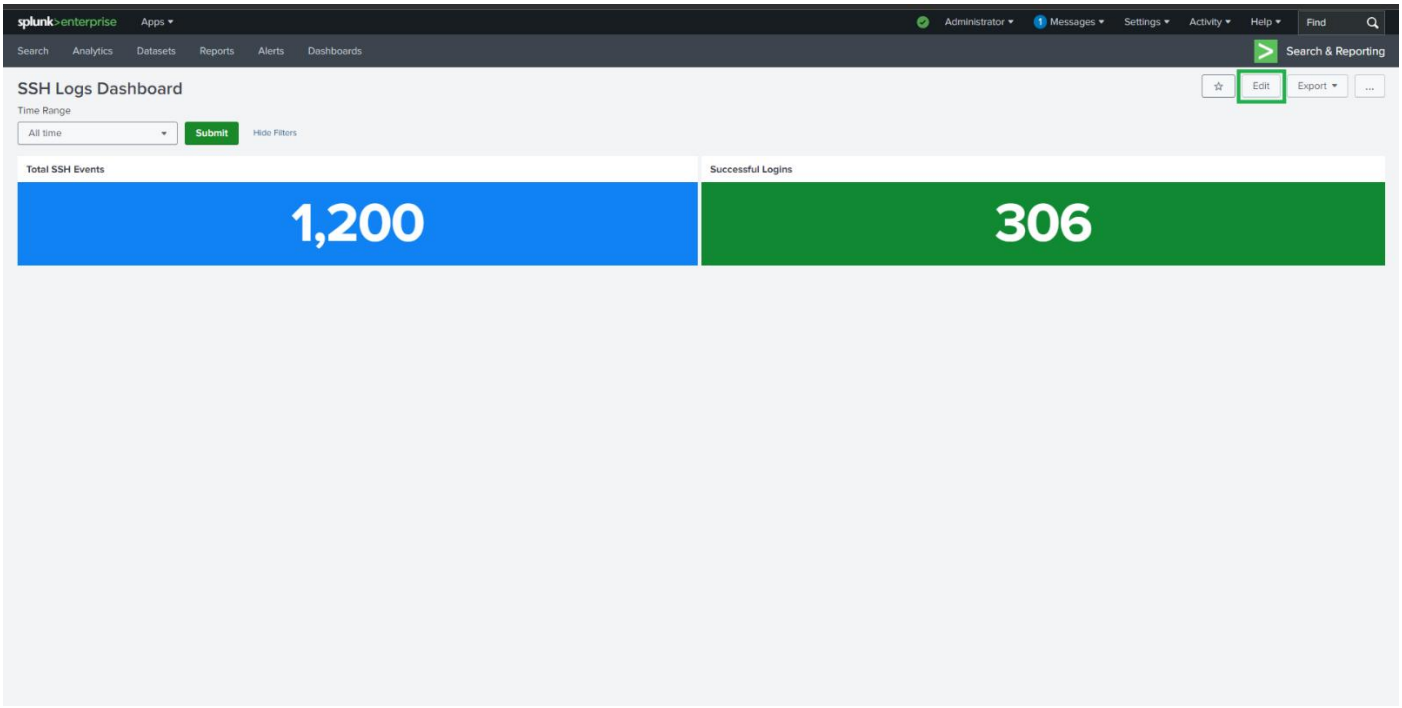
3. Failed Logins

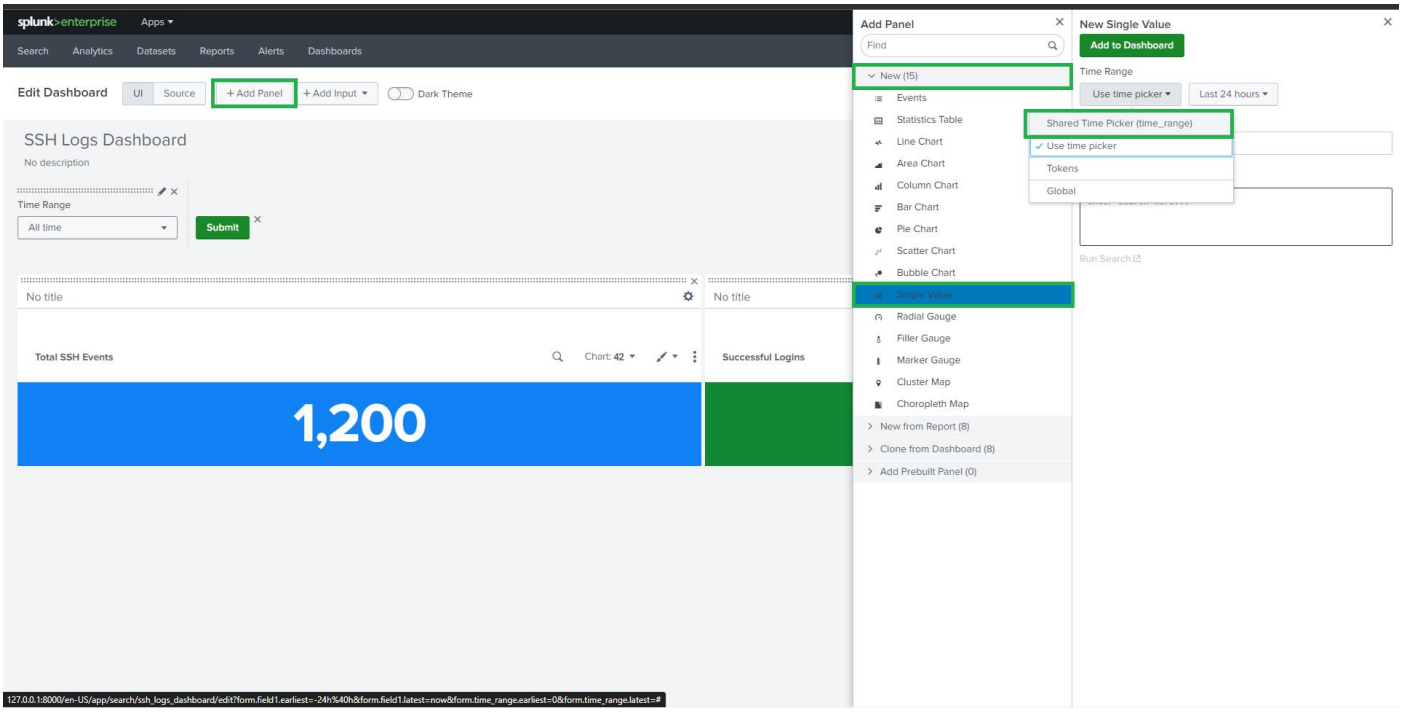
- **Panel Type:** Single Value
- **Time Picker:** time_range
- **Title:** Failed Logins

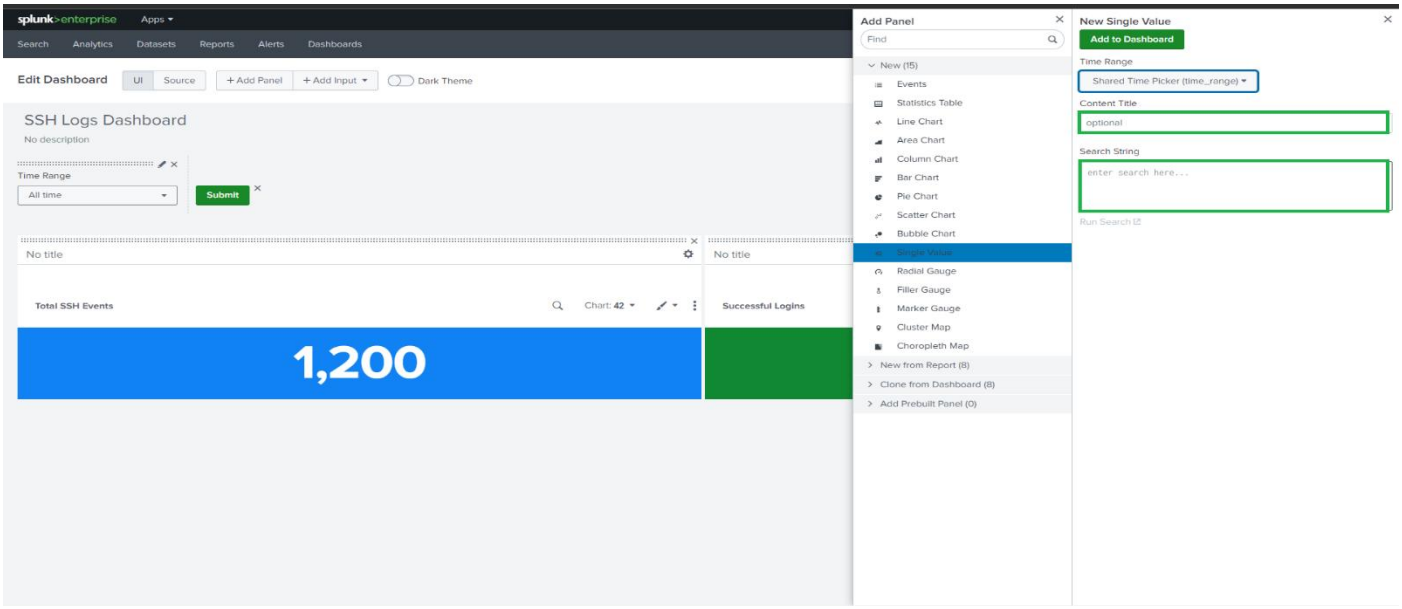
Search Query:

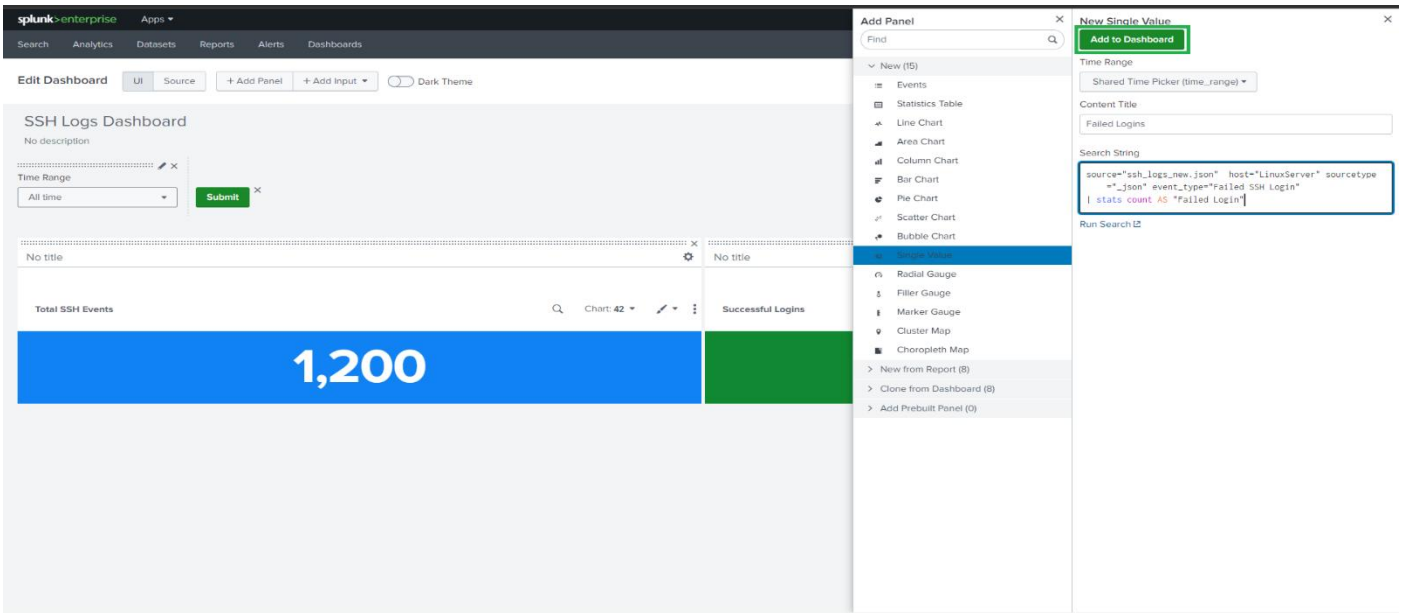
source="ssh_logs.json" host="LinuxServer" sourcetype="_json" event_type="Failed SSH Login"

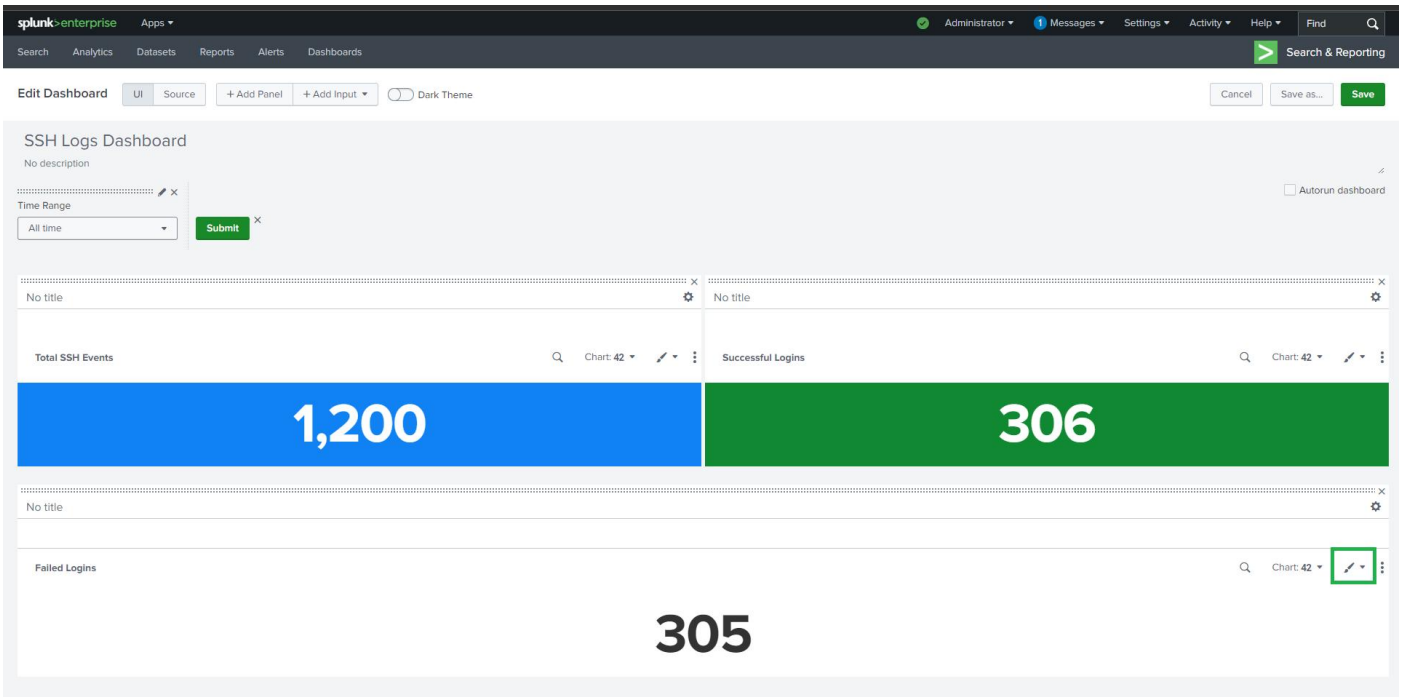
| stats count AS "Failed Login"

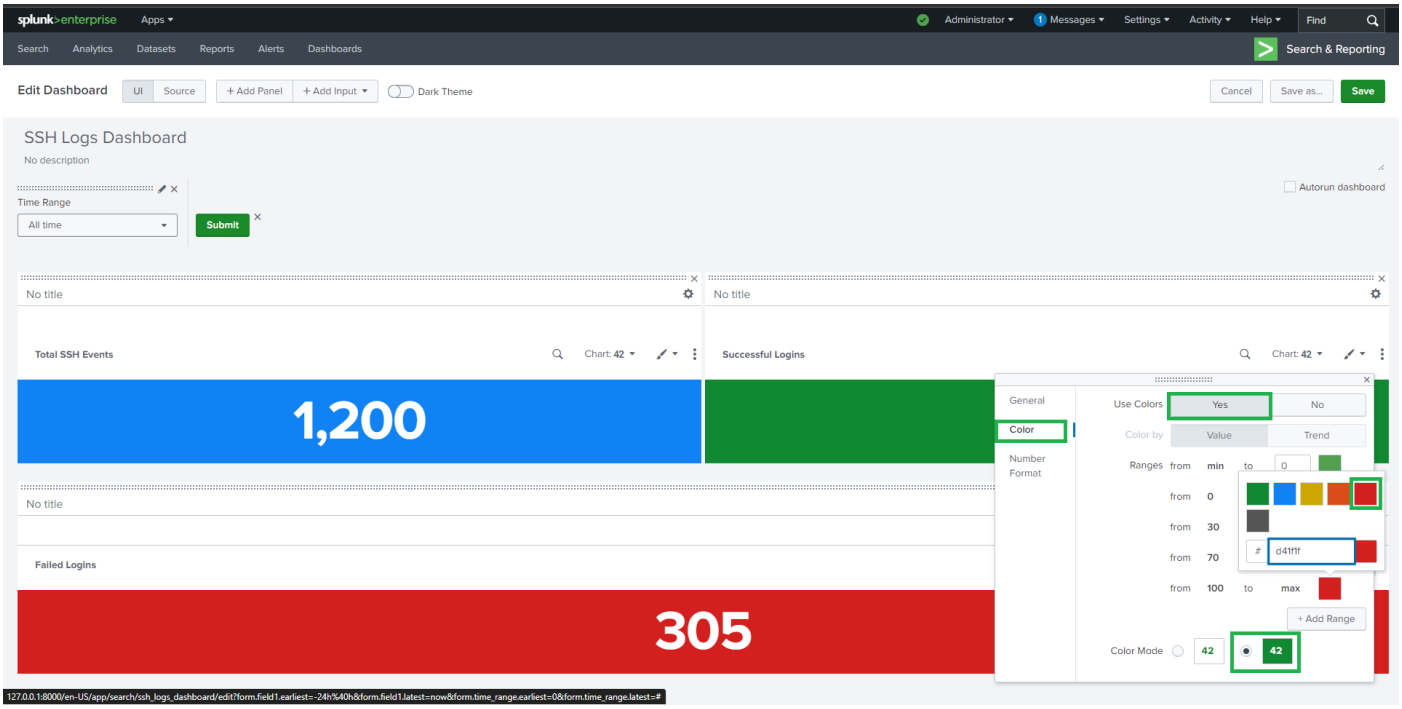


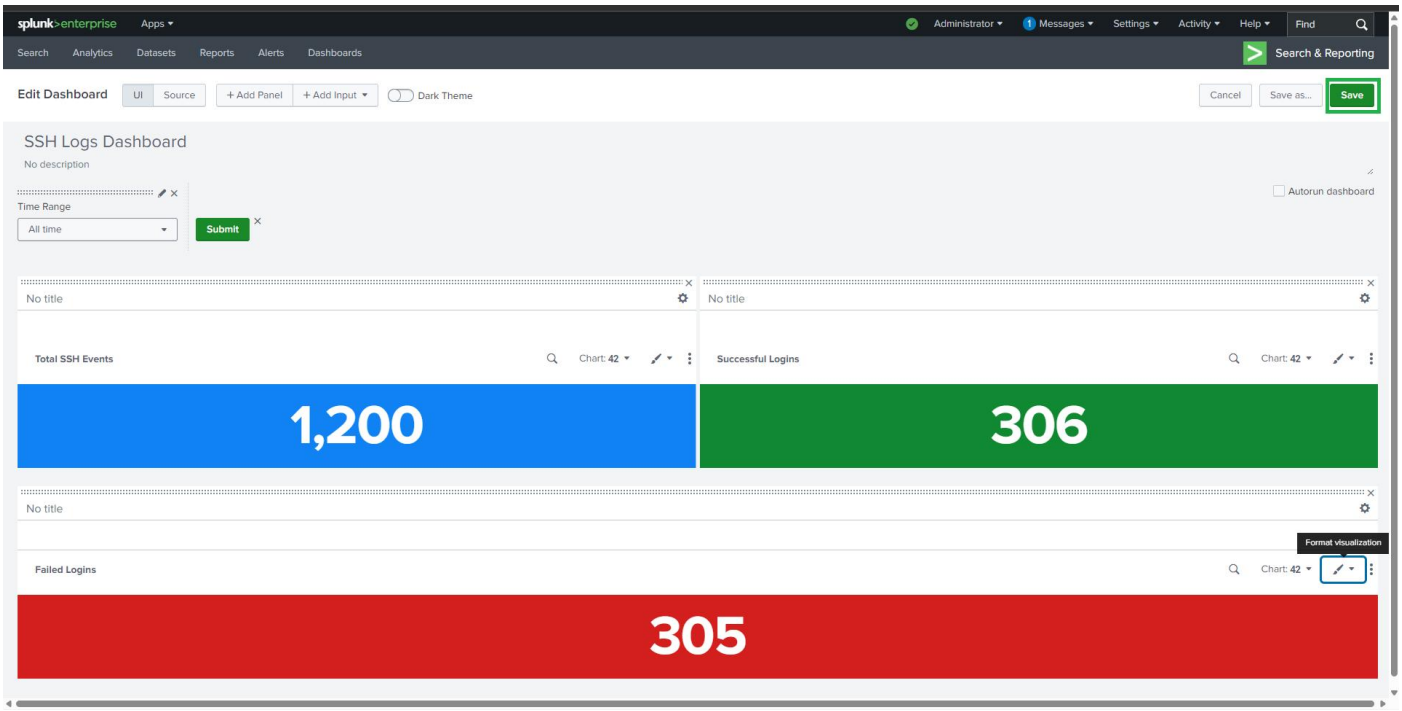



splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
SSH Logs Dashboard
No description
Time Range
All time
Submit
No title
Total SSH Events
Chart: 42
1,200
No title
Successful Logins
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (8)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
optional
Search String
enter search here...
Run Search


splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
SSH Logs Dashboard
No description
Time Range
All time
Submit
No title
Total SSH Events
Chart: 42
1,200
No title
Successful Logins
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (8)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
Failed Logins
Search String
source="ssh_logs_new.json" host="LinuxServer" sourcetype
="_json" event_type="Failed SSH Login"
| stats count AS "Failed Login"
Run Search


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total SSH Events
Chart: 42
1,200
No title
Successful Logins
Chart: 42
306
No title
Failed Logins
Chart: 42
305


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total SSH Events
Chart: 42
1,200
Successful Logins
General
Color
Number Format
Use Colors
Yes
No
Color by
Value
Trend
Ranges
from min to 0
from 0
from 30
from 70
from 100 to max
d41f1f
+ Add Range
Color Mode
42
42
Failed Logins
305
127.0.0.1:8000/en-US/app/search/ssh_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now&form.time_range.earliest=0&form.time_range.latest=#


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total SSH Events
Chart: 42
1,200
Successful Logins
306
Failed Logins
Format visualization
305

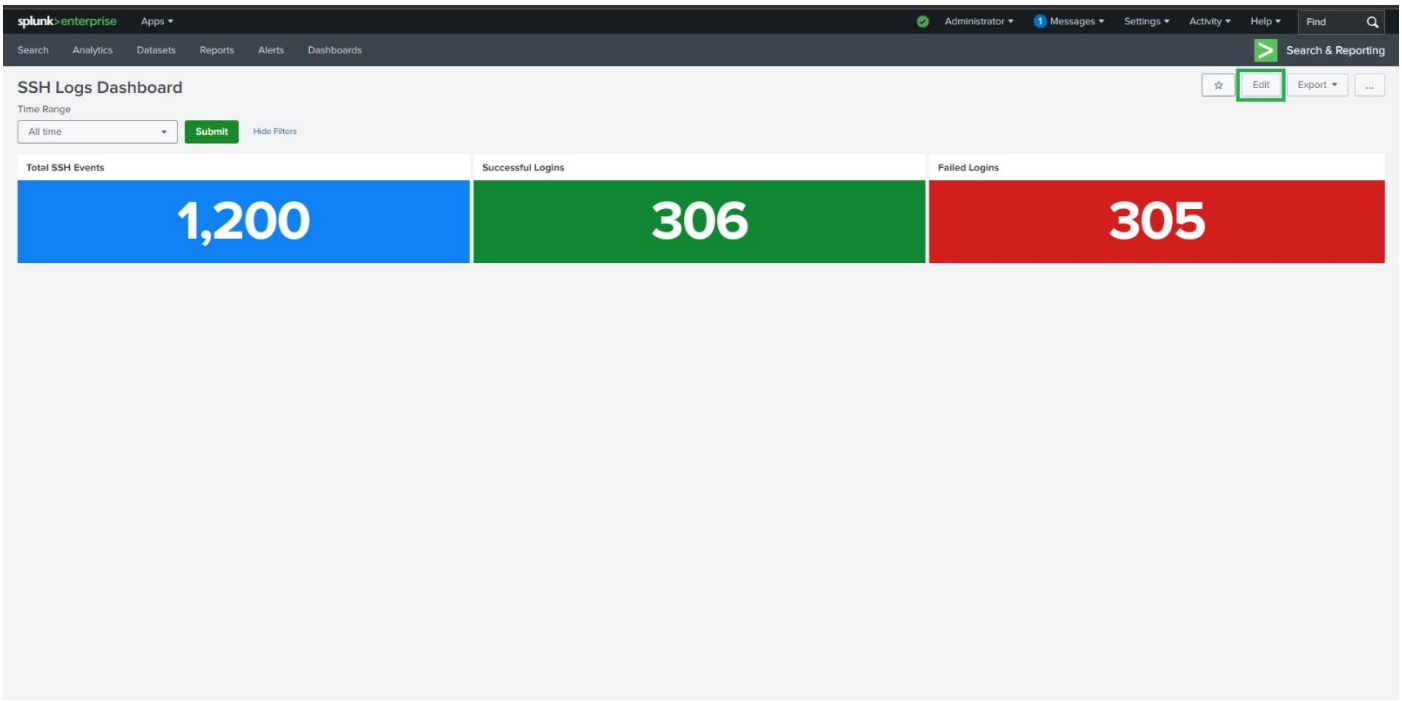
4. Connection Without Authentication (Invalid Users)

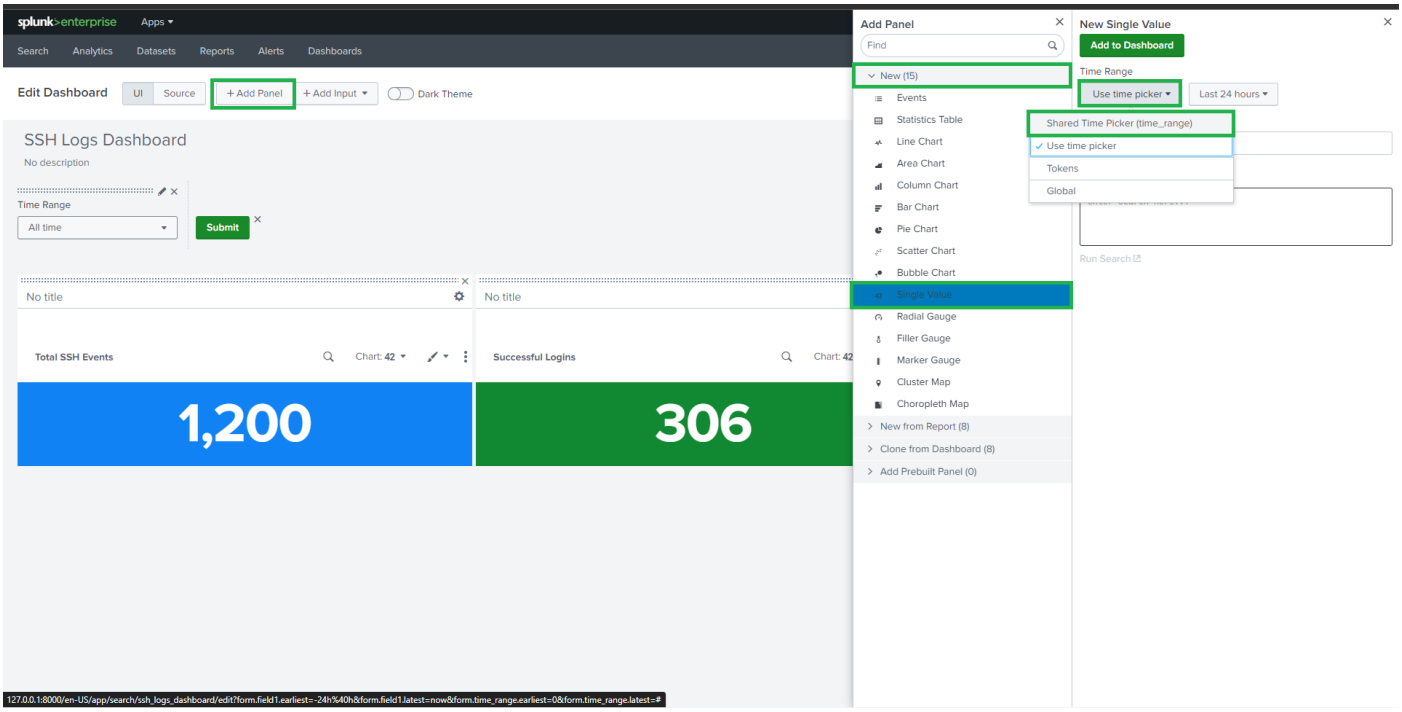
- **Panel Type:** Single Value
- **Time Picker:** time_range
- **Title:** Invalid User Attempts

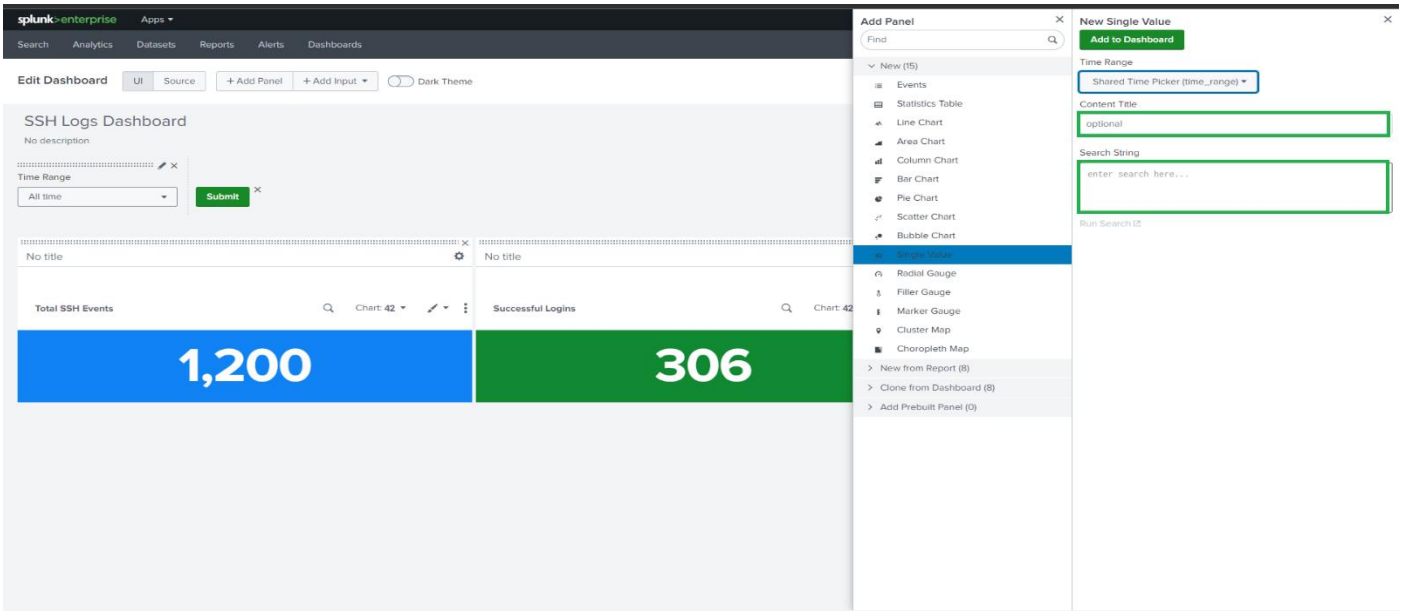
Search Query:

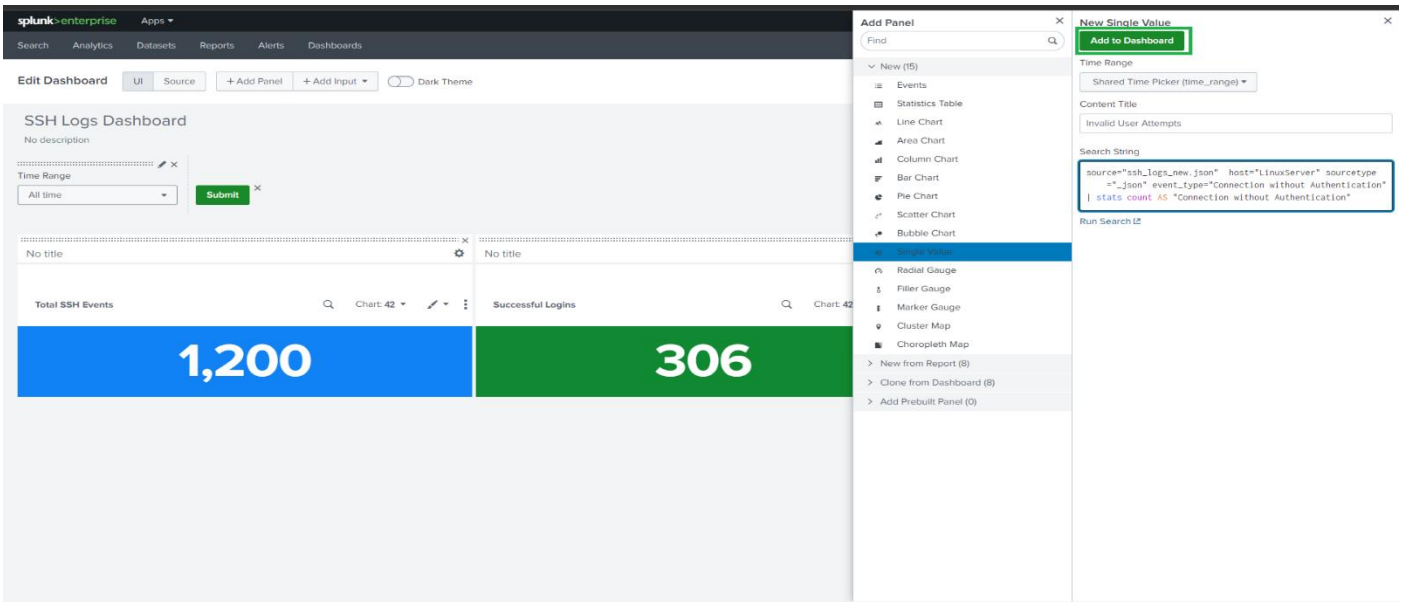
index=auth "sshd" "invalid user"

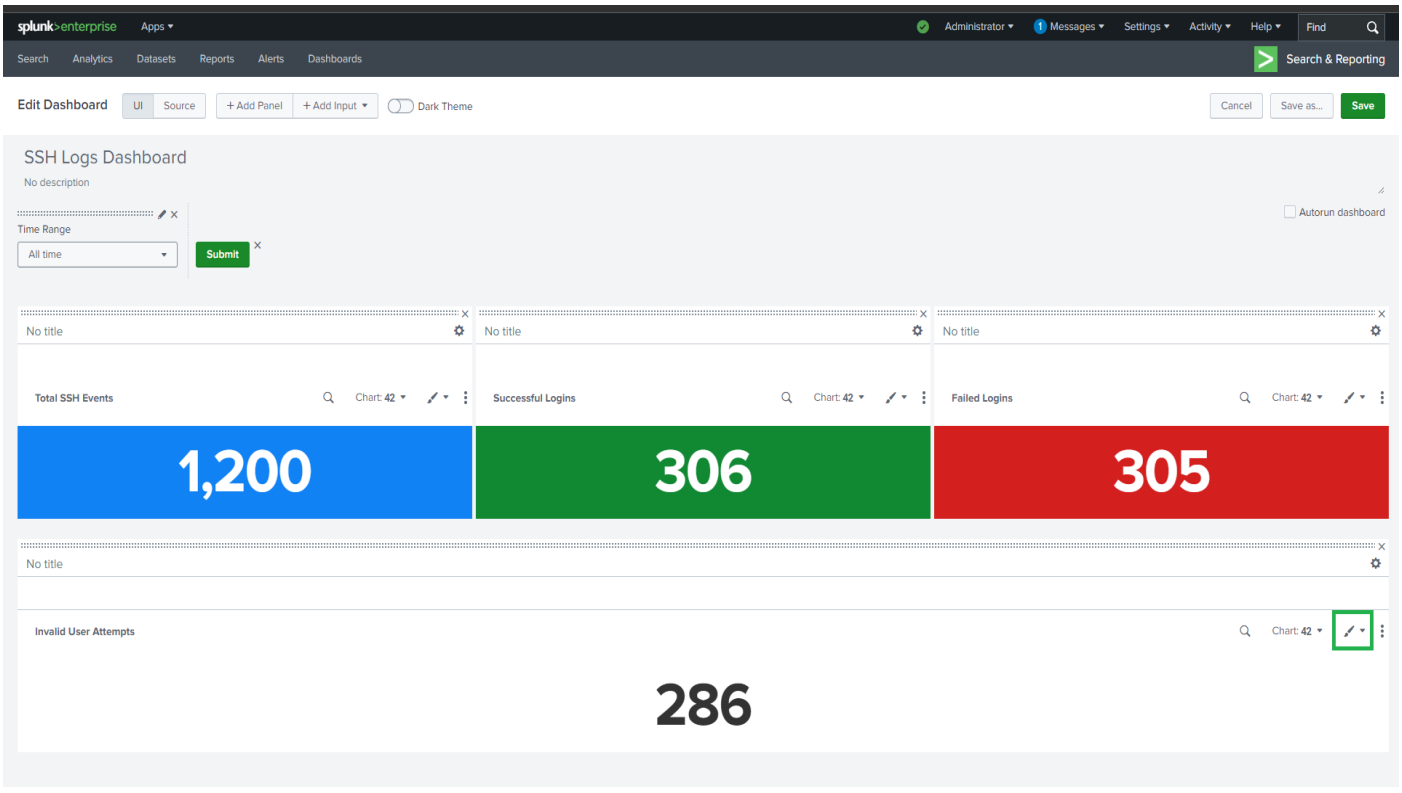
| stats count AS "Invalid User Attempts"

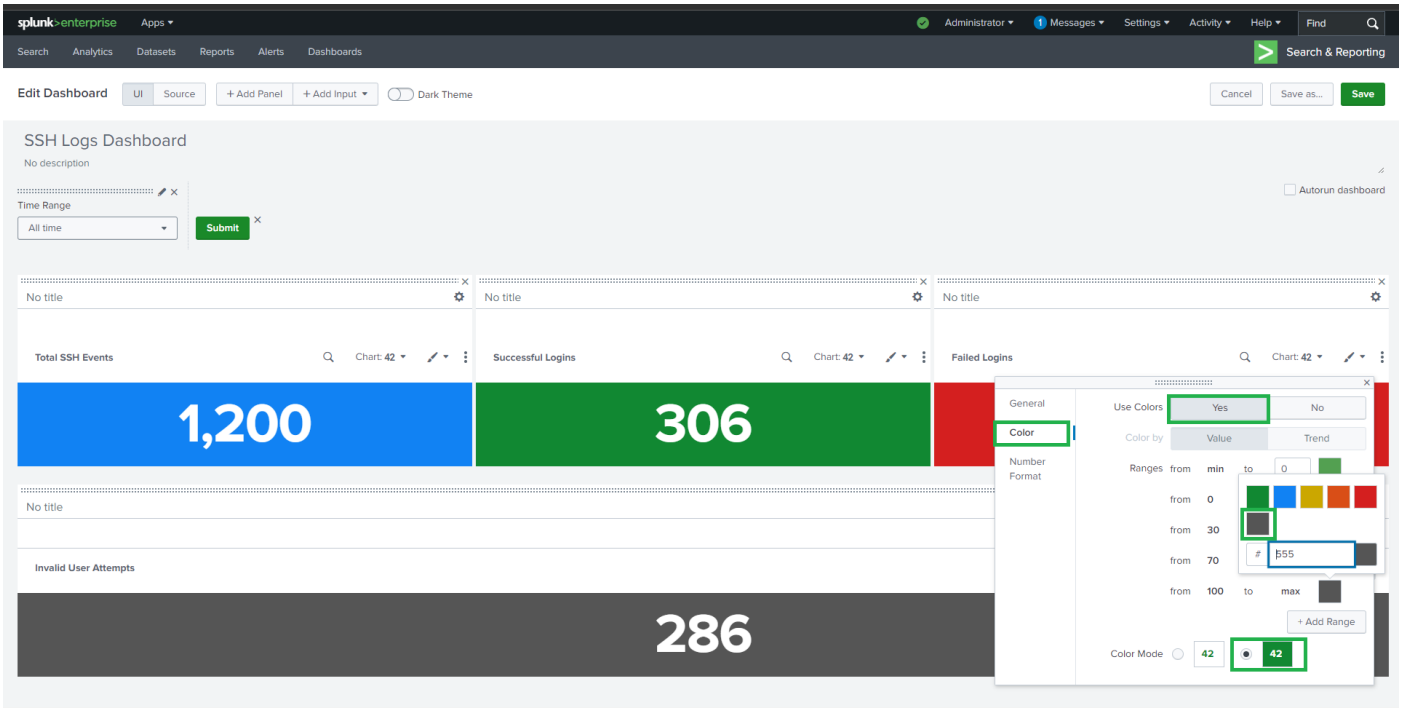


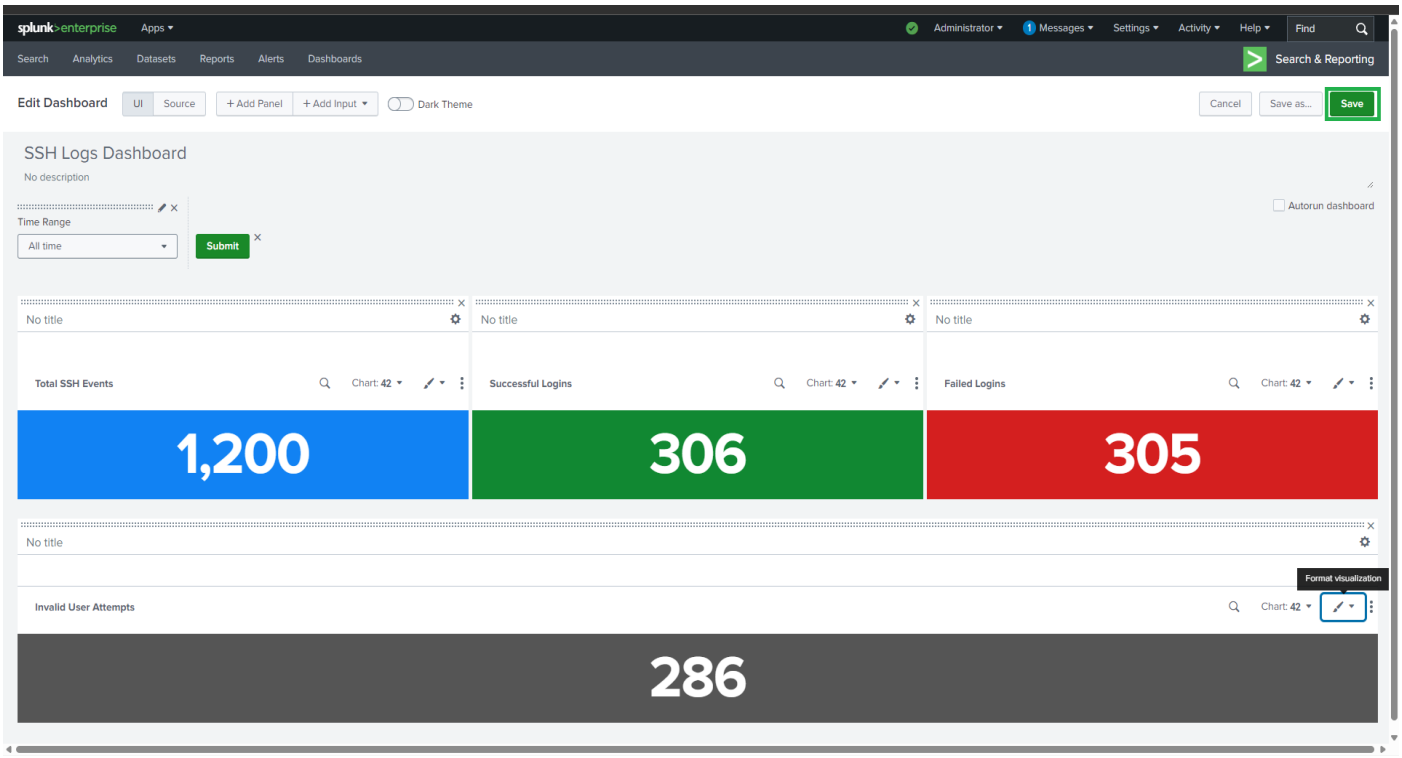



splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
SSH Logs Dashboard
No description
Time Range
All time
Submit
No title
Total SSH Events
1,200
Successful Logins
306
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (8)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
optional
Search String
enter search here...
Run Search


splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
SSH Logs Dashboard
No description
Time Range
All time
Submit
No title
Total SSH Events
1,200
Successful Logins
306
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (8)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
Invalid User Attempts
Search String
source="ssh_logs_new.json" host="linuxServer" sourcetype
="_json" event_type="Connection without Authentication"
| stats count AS "Connection without Authentication"
Run Search


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Autorun dashboard
Time Range
All time
Submit
No title
Total SSH Events
1,200
Successful Logins
306
Failed Logins
305
Invalid User Attempts
286


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Time Range
All time
Submit
Autorun dashboard
No title
Total SSH Events
Chart: 42
1,200
Successful Logins
306
Failed Logins
Invalid User Attempts
286
General
Color
Number Format
Use Colors
Yes
No
Color by
Value
Trend
Ranges
from min to 0
from 0
from 30
from 70
from 100 to max
+ Add Range
Color Mode
42


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Time Range
All time
Submit
Autorun dashboard
No title
Total SSH Events
Chart: 42
1,200
Successful Logins
306
Failed Logins
305
Invalid User Attempts
286
Format visualization

📈 Task 2: Login Activity Trends

Goal

Analyze login patterns over time and **detect anomalies or attack behavior**.

---

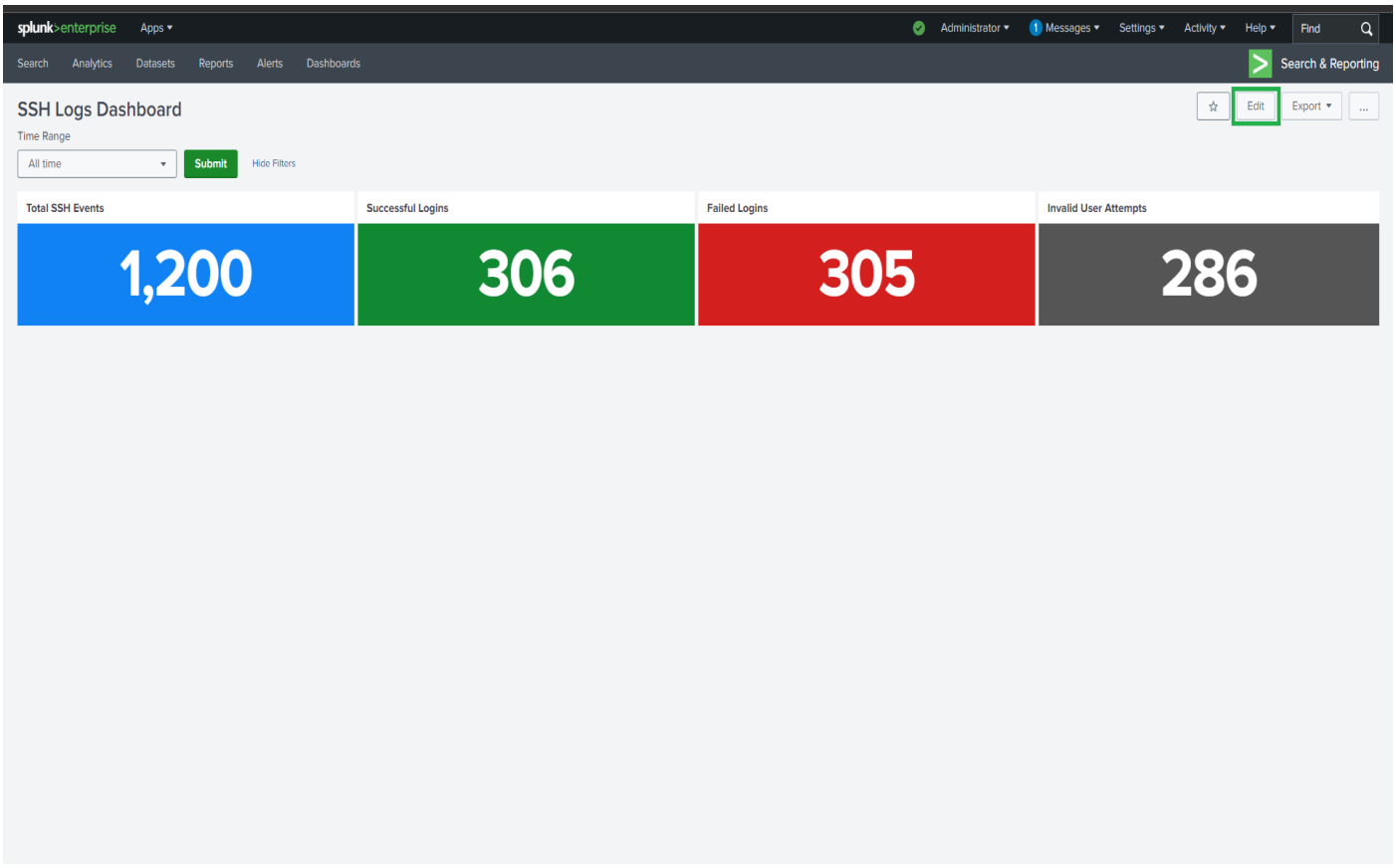
1. Failed Logins by Username

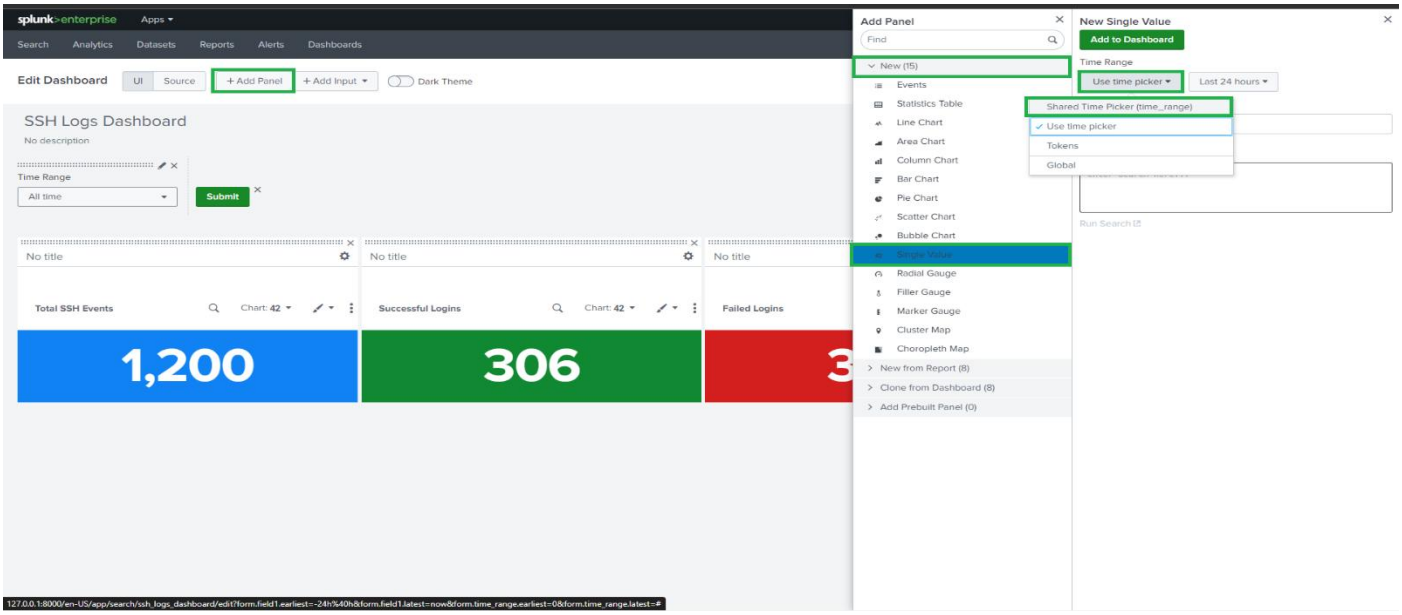
- **Panel Type:** Bar Chart
- **Time Picker:** time_range
- **Title:** Failed Logins by Username

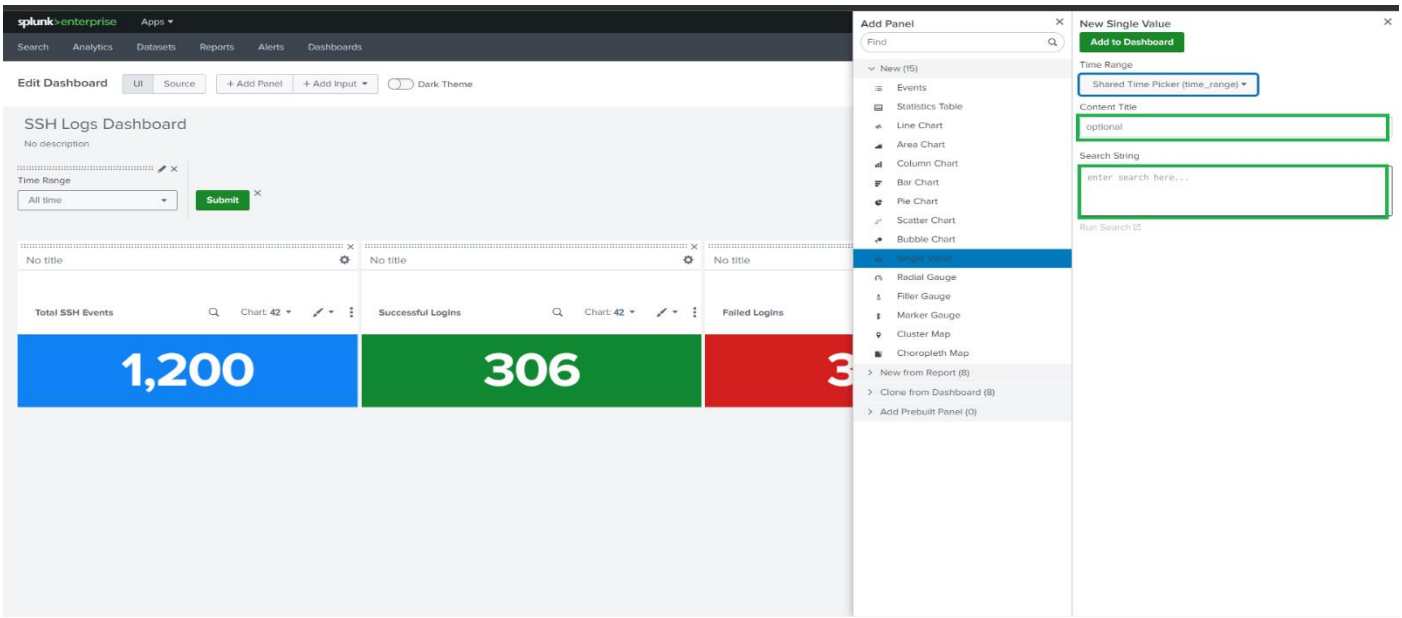
Search Query:

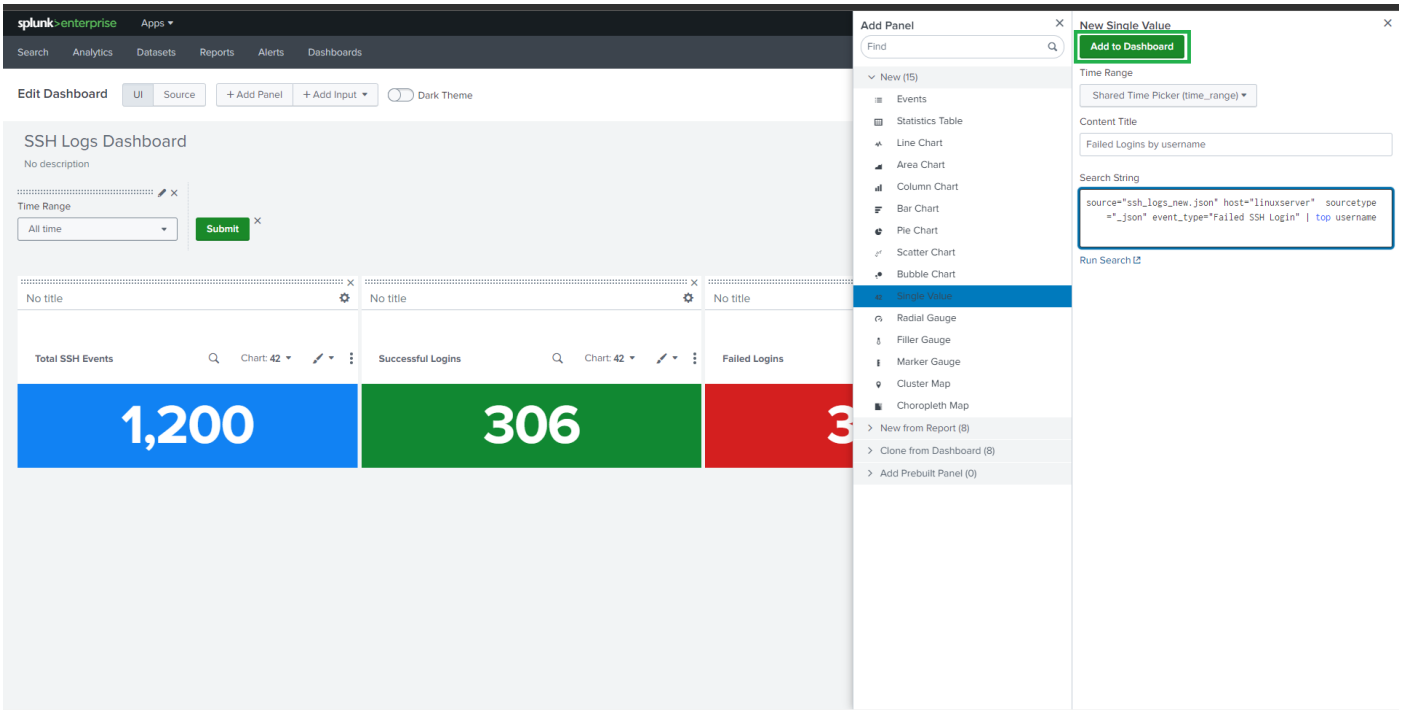
source="ssh_logs_new.json" host="LinuxNew" sourcetype="_json" event_type="Failed SSH Login"

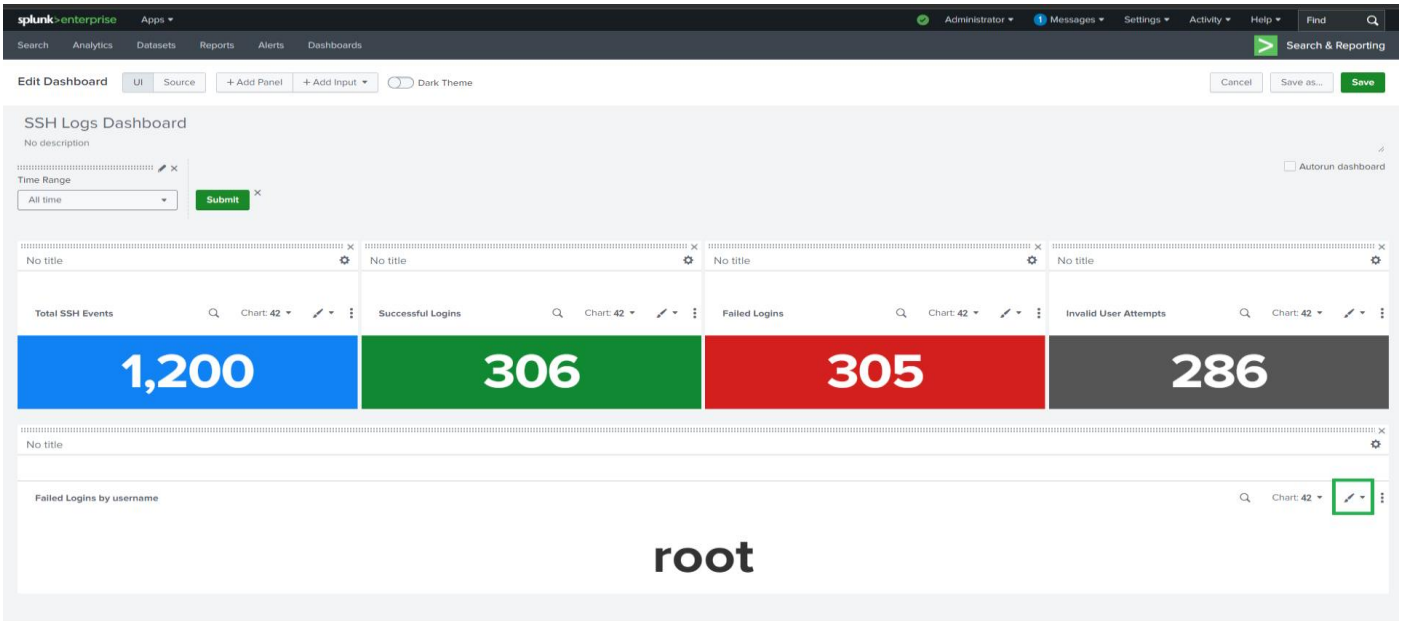
| top username

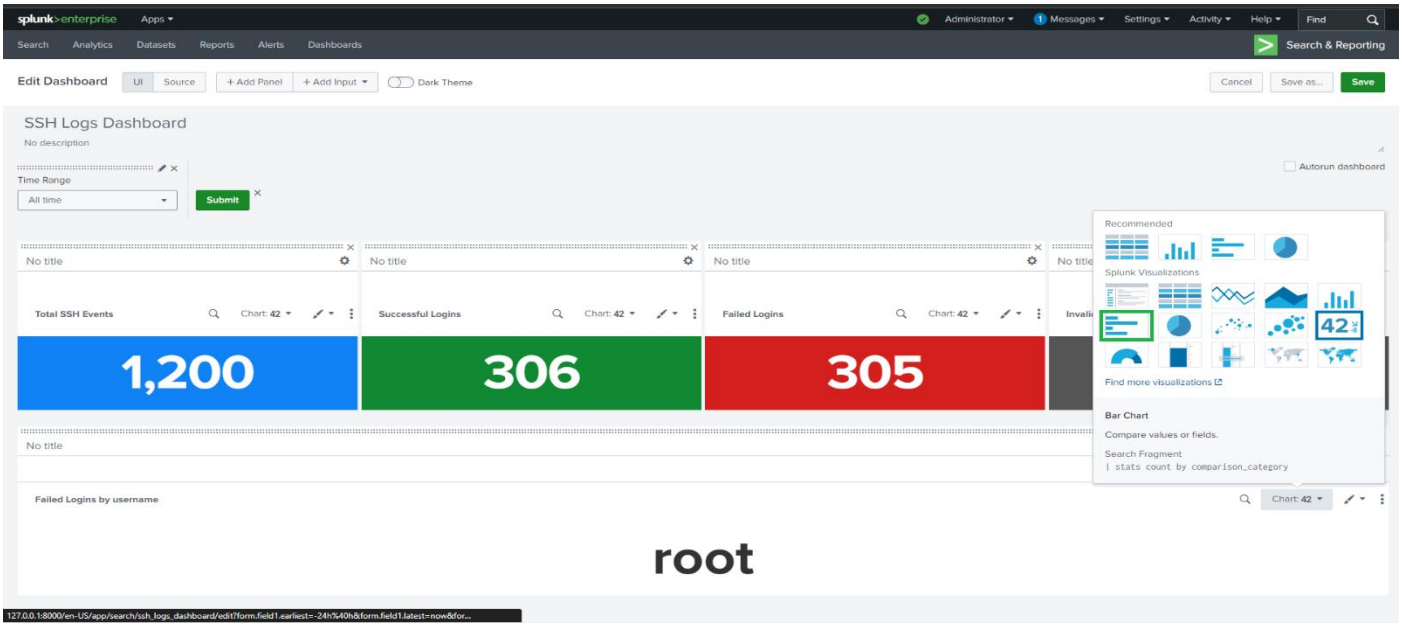


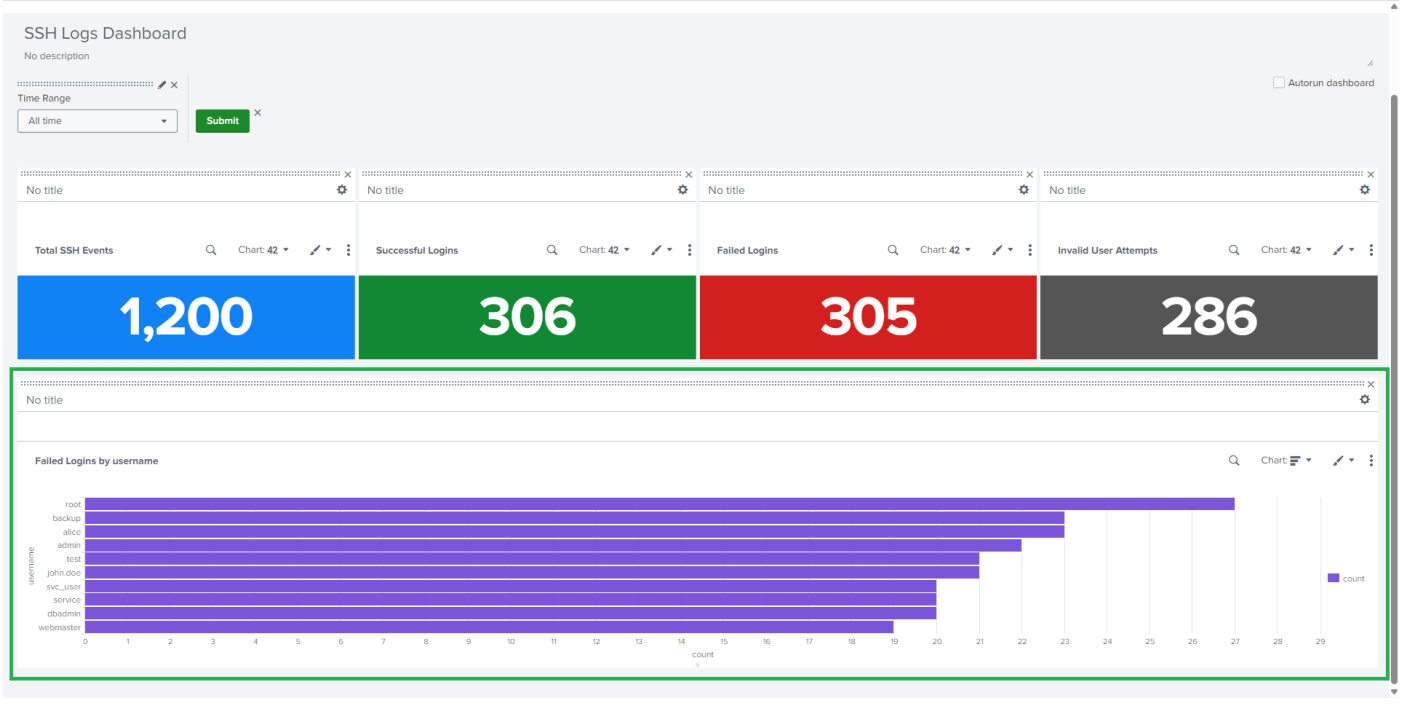

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
SSH Logs Dashboard
No description
Time Range
All time
Submit
No title
Total SSH Events
Chart: 42
1,200
Successful Logins
306
Failed Logins
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (8)
Add Prebuilt Panel (0)
Shared Time Picker (time_range)
Use time picker
Tokens
Global
New Single Value
Add to Dashboard
Time Range
Use time picker
Last 24 hours
Run Search
127.0.0.1:8000/en-US/app/search/ssh_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now&form.time_range.earliest=0&form.time_range.latest=#

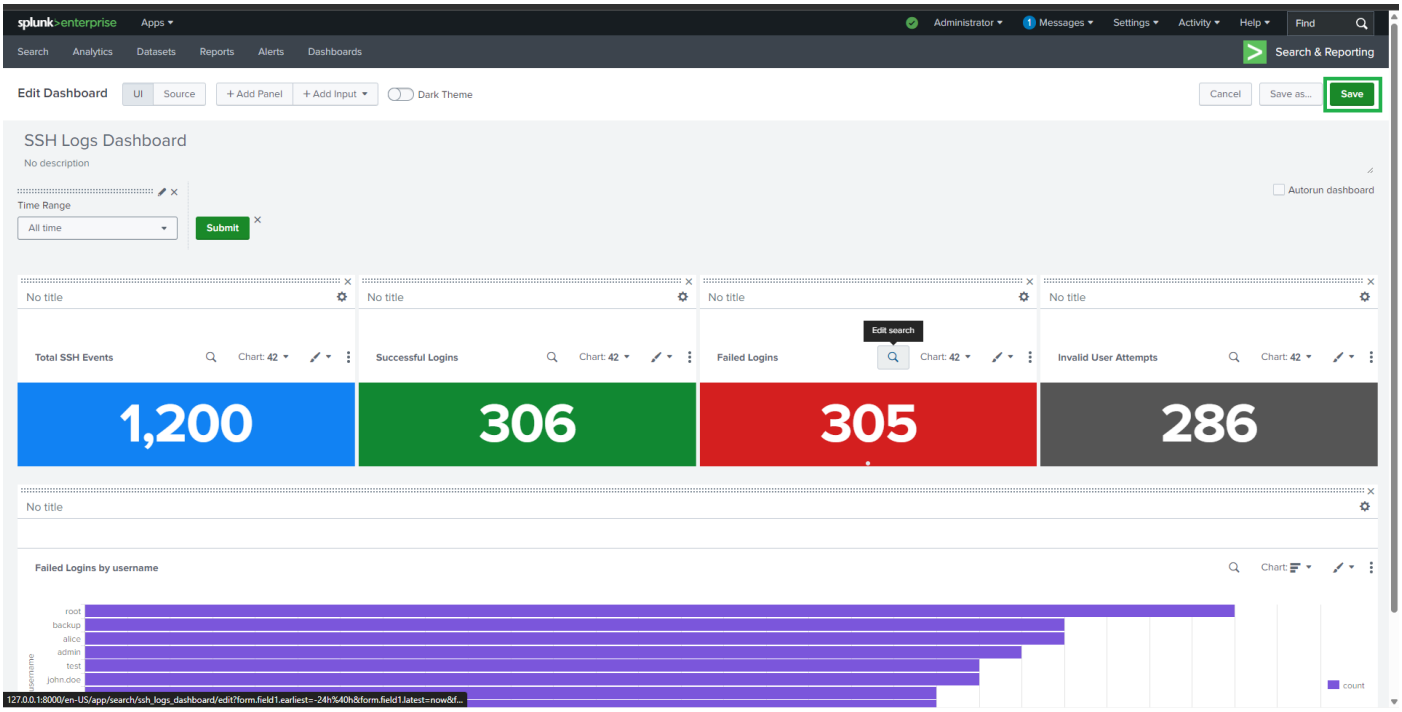

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
SSH Logs Dashboard
No description
Time Range
All time
Submit
No title
Total SSH Events
Chart: 42
1,200
Successful Logins
306
Failed Logins
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (8)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
optional
Search String
enter search here...
Run Search


splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
SSH Logs Dashboard
No description
Time Range
All time
Submit
No title
Total SSH Events
Chart: 42
1,200
Successful Logins
306
Failed Logins
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (8)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
Failed Logins by username
Search String
source="ssh_logs_new.json" host="linuxserver" sourcetype="_json" event_type="Failed SSH Login" | top username
Run Search


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Time Range
All time
Submit
Autorun dashboard
No title
Total SSH Events
Chart: 42
1,200
Successful Logins
306
Failed Logins
305
Invalid User Attempts
286
Failed Logins by username
root


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Time Range
All time
Submit
Autorun dashboard
Recommended
Splunk Visualizations
Find more visualizations
Bar Chart
Compare values or fields.
Search Fragment
| stats count by comparison_category
No title
Total SSH Events
Chart: 42
1,200
Successful Logins
306
Failed Logins
305
Failed Logins by username
root
127.0.0.1:8000/en-US/app/search/ssh_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now&for...


SSH Logs Dashboard
No description
Time Range
All time
Submit
Autorun dashboard
No title
Total SSH Events
Chart: 42
1,200
Successful Logins
306
Failed Logins
305
Invalid User Attempts
286
Failed Logins by username
root
backup
alice
admin
test
john.doe
svc_user
service
dbadmin
webmaster
username
count



---

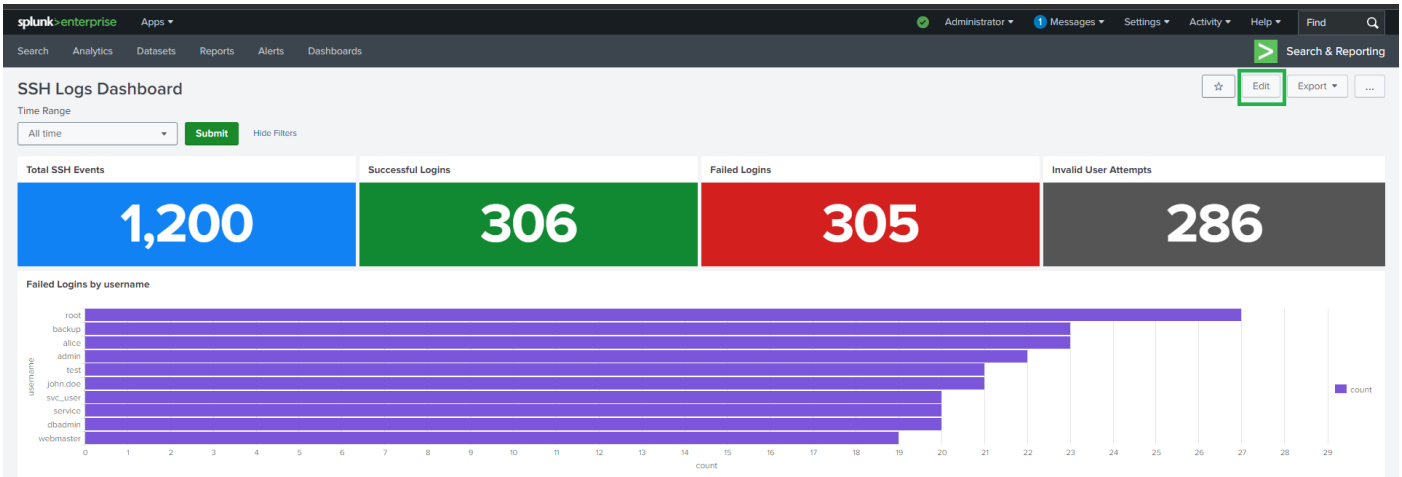
2. Possible Brute Force Attempts by IP Address

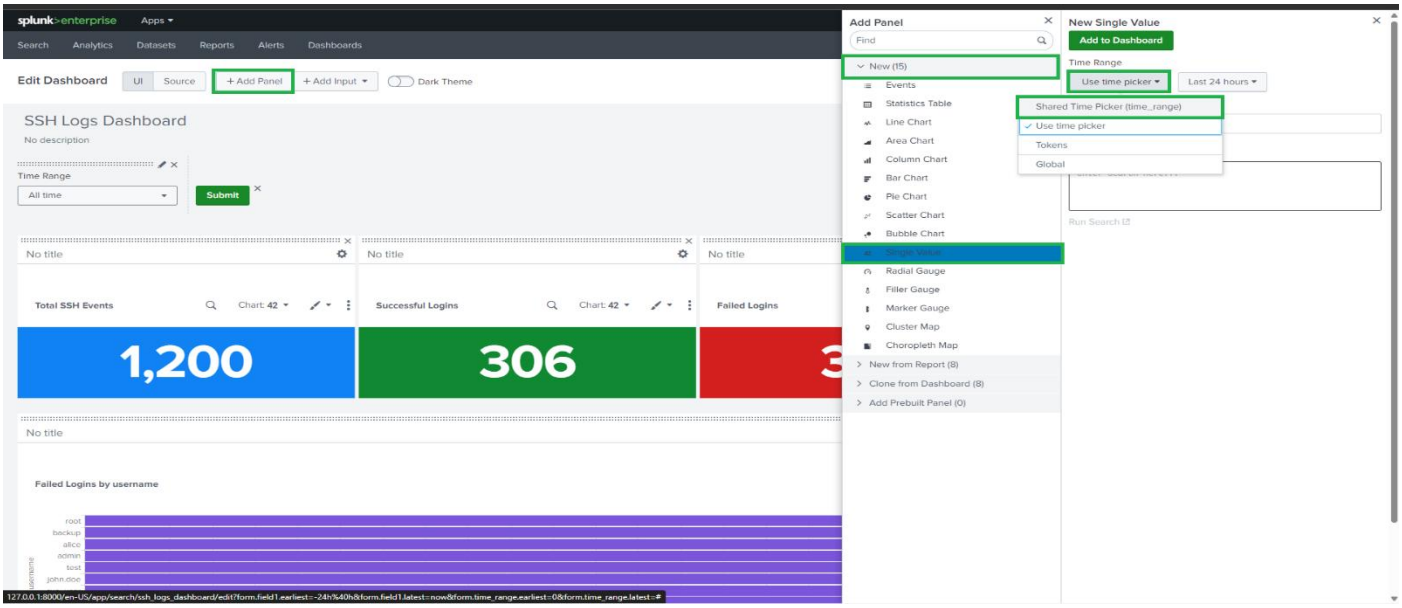
- **Panel Type:** Statistics Table
- **Time Picker:** time_range
- **Title:** Possible Brute Force by IP Address

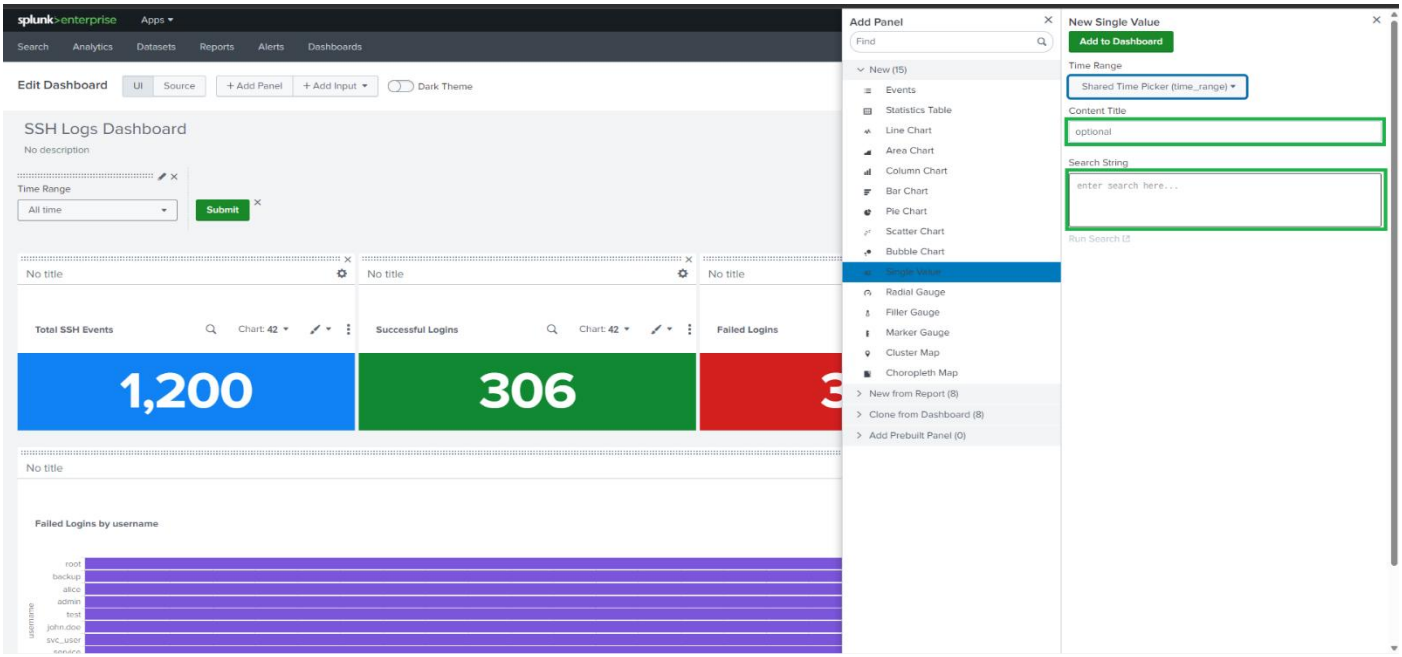
Search Query:

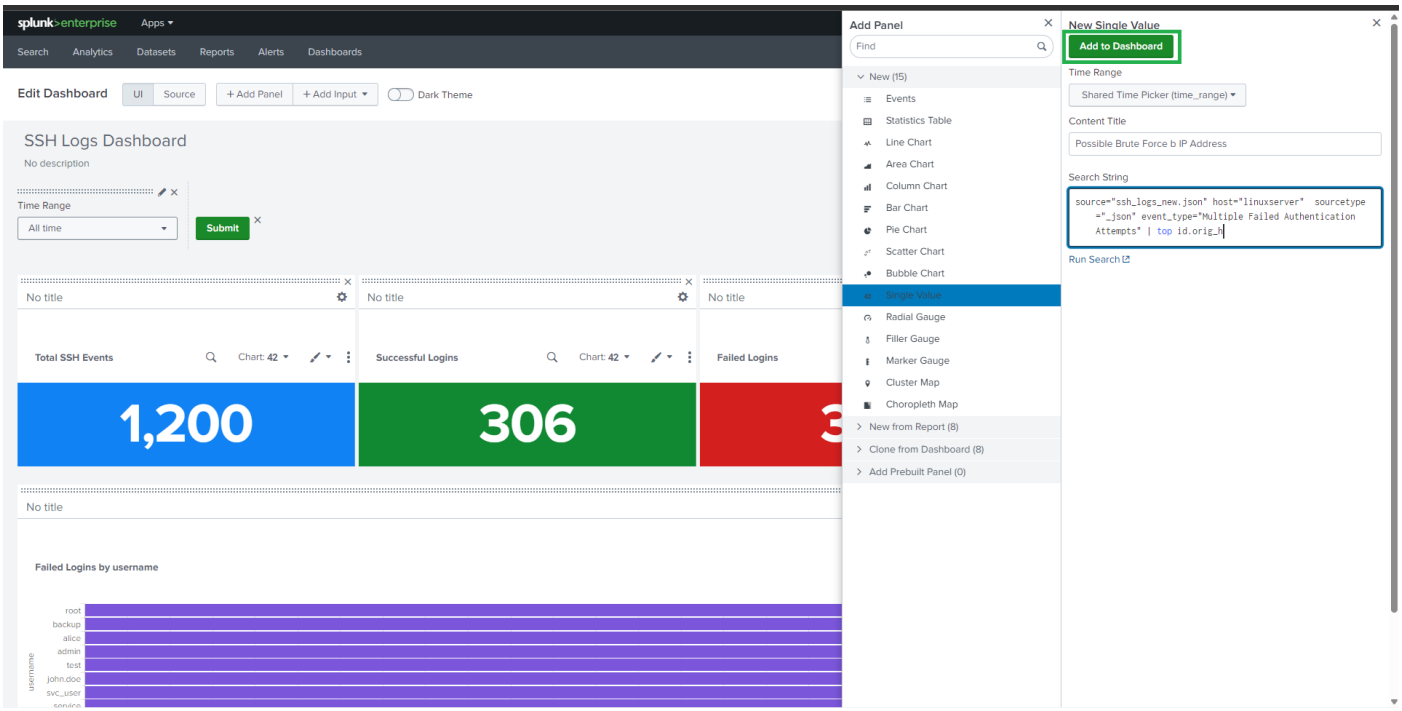
source="ssh_logs_new.json" host="LinuxNew" sourcetype="_json" event_type="Multiple Failed Authentication Attempts"

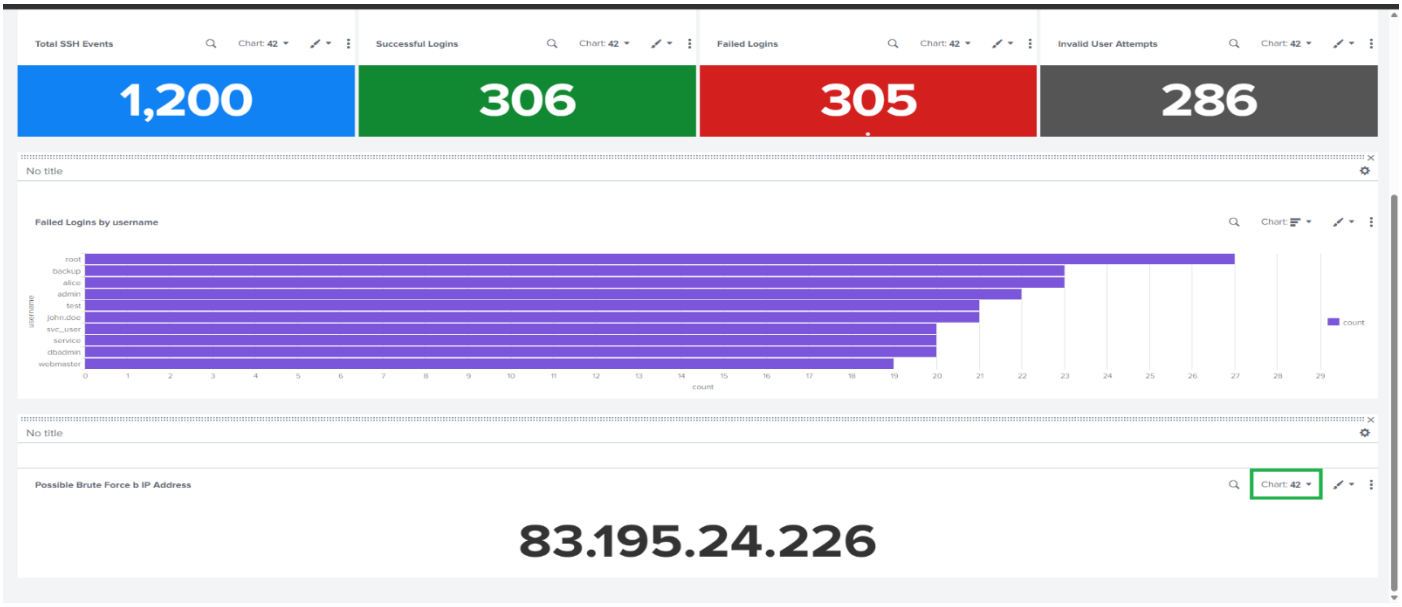
| top id.orig_h

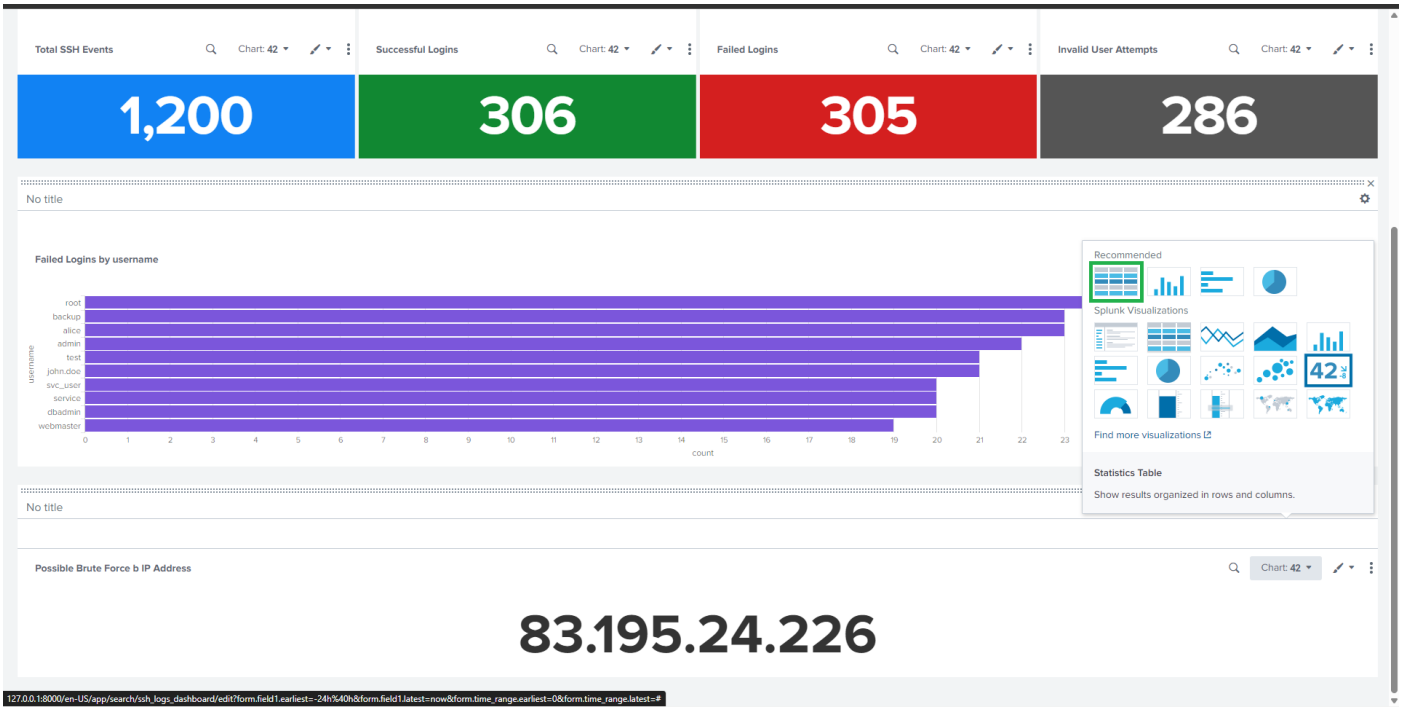



splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
SSH Logs Dashboard
No description
Time Range
All time
Submit
No title
Total SSH Events
Chart: 42
1,200
Successful Logins
306
Failed Logins
Failed Logins by username
root
backup
alice
admin
test
john.doe
username
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (8)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Use time picker
Last 24 hours
Shared Time Picker (time_range)
Use time picker
Tokens
Global
Run Search

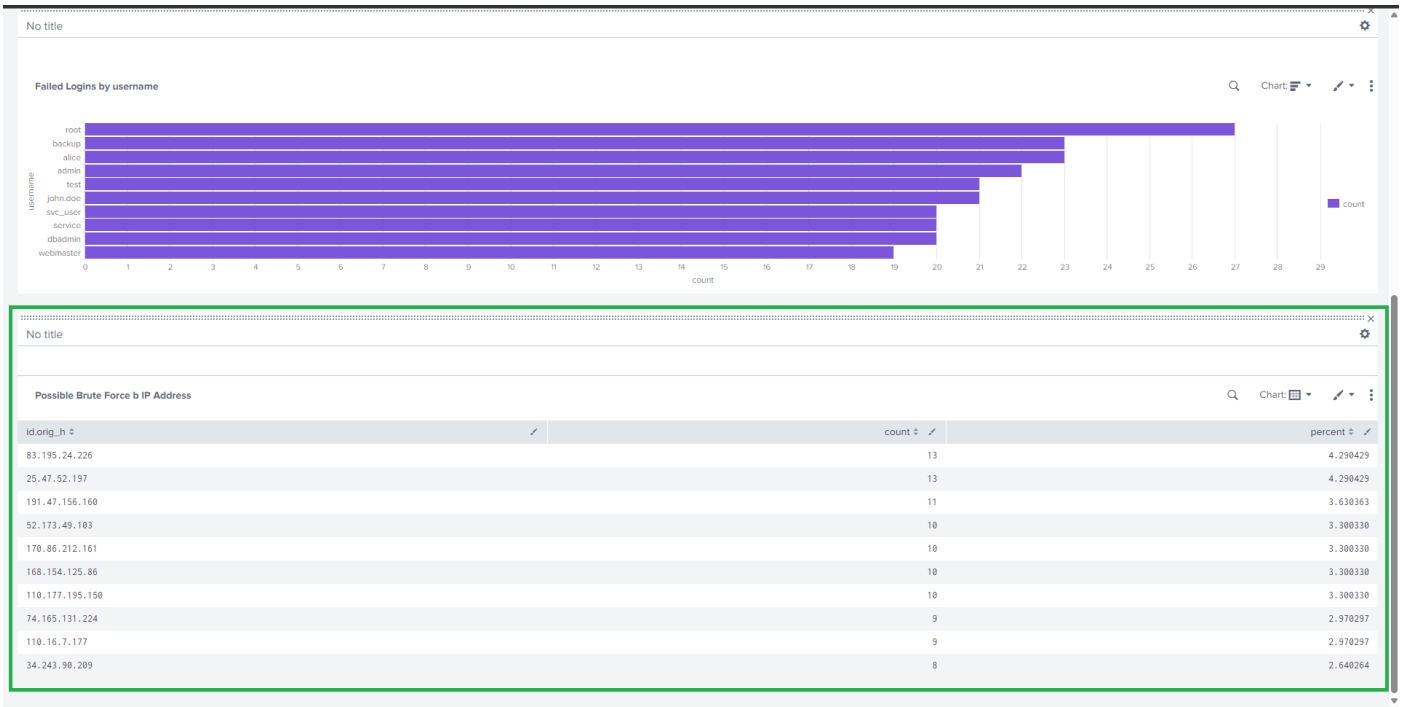

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
SSH Logs Dashboard
No description
Time Range
All time
Submit
No title
Total SSH Events
Chart: 42
1,200
Successful Logins
306
Failed Logins
Failed Logins by username
root
backup
alice
admin
test
john.doe
svc_user
username
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (8)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
optional
Search String
enter search here...
Run Search


splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
SSH Logs Dashboard
No description
Time Range
All time
Submit
No title
Total SSH Events
Chart: 42
1,200
Successful Logins
306
Failed Logins
Failed Logins by username
root
backup
alice
admin
test
john.doe
svc_user
username
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (8)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
Possible Brute Force b IP Address
Search String
source="ssh_logs_new.json" host="linuxserver" sourcetype="_json" event_type="Multiple Failed Authentication Attempts" | top id.orig_h
Run Search

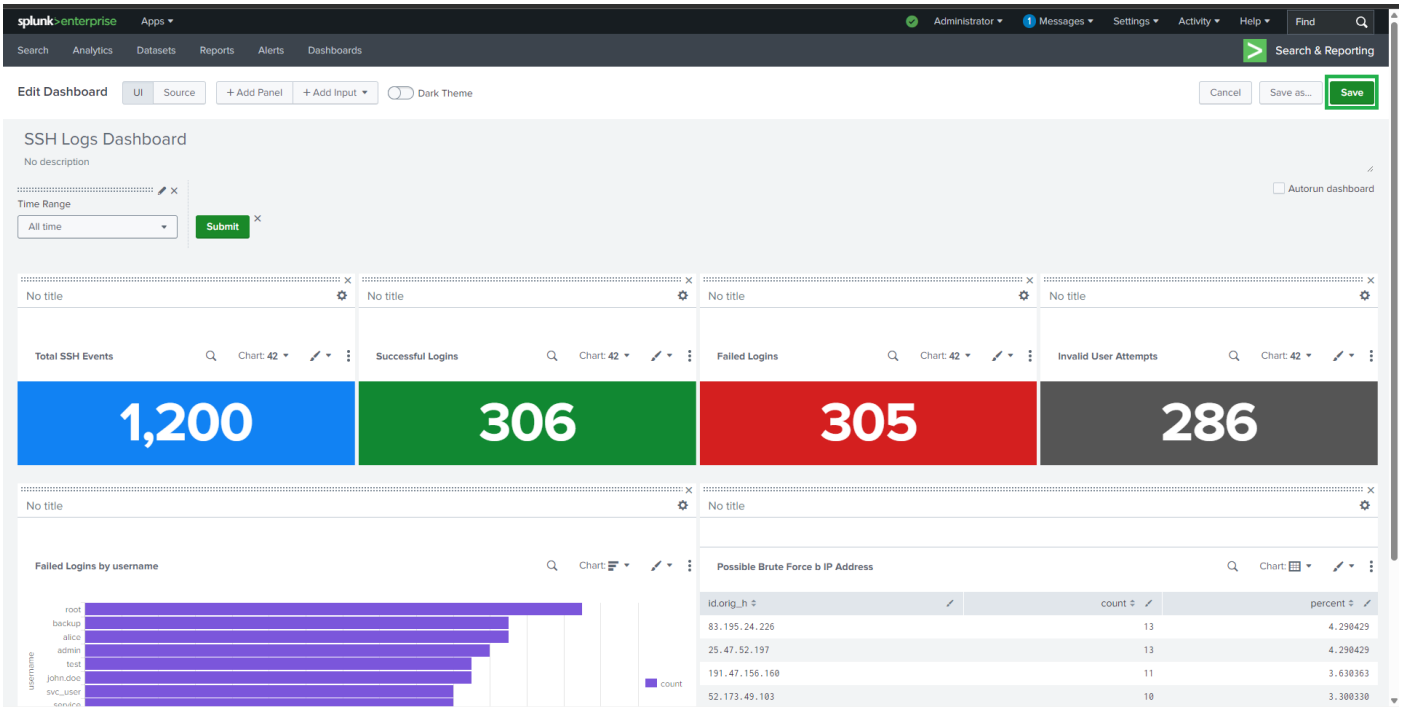




127.0.0.1:8000/en-US/app/search/ssh_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now&form.time_range.earliest=0&form.time_range.latest=#



id.orig_h	count	percent
83.195.24.226	13	4.290429
25.47.52.197	13	4.290429
191.47.156.160	11	3.630363
52.173.49.103	10	3.300330
170.86.212.161	10	3.300330
168.154.125.86	10	3.300330
110.177.195.150	10	3.300330
74.165.131.224	9	2.970297
110.16.7.177	9	2.970297
34.243.90.209	8	2.640264


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
Cancel
Save as...
Save
SSH Logs Dashboard
No description
Time Range
All time
Submit
Autorun dashboard
No title
Total SSH Events
Chart: 42
1,200
Successful Logins
306
Failed Logins
305
Invalid User Attempts
286
Failed Logins by username
root
backup
alice
admin
test
john.doe
svc_user
username
count
Possible Brute Force b IP Address
id.orig_h
count
percent
83.195.24.226
13
4.290429
25.47.52.197
13
4.290429
191.47.156.160
11
3.630363
52.173.49.103
10
3.300330

🌍 Task 3: Visualizing Brute Force Attacks Using Geo-Location

Goal

Identify **geographical sources** of brute-force SSH attacks.

---

1. Brute Force Attack with Geo-Location

- **Panel Type:** Choropleth Map
- **Time Picker:** time_range
- **Title:** Brute Force Attack with Geo-Location

Search Query:

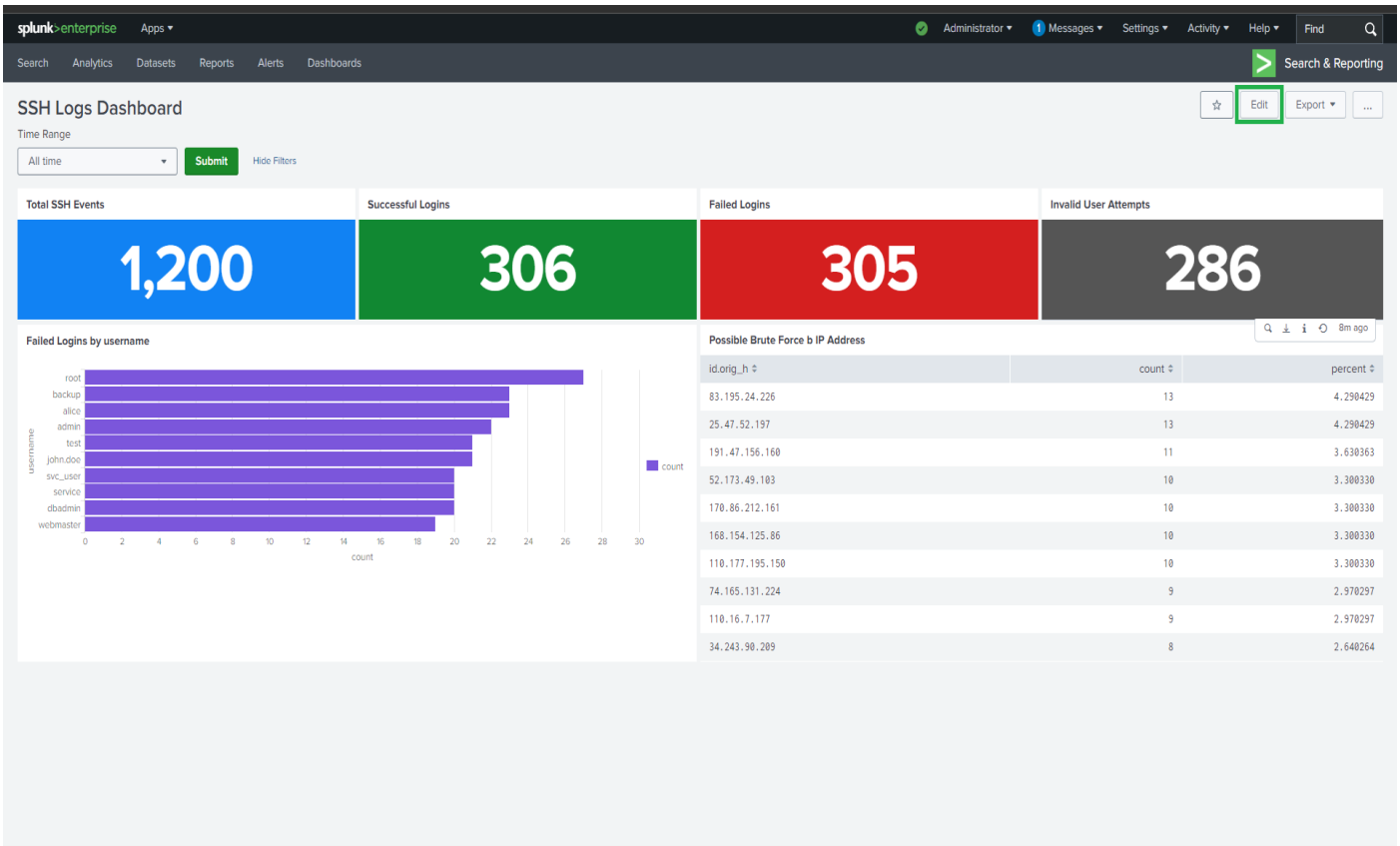
source="ssh_logs_new.json" host="LinuxNew" sourcetype="_json" event_type="Multiple Failed Authentication Attempts"

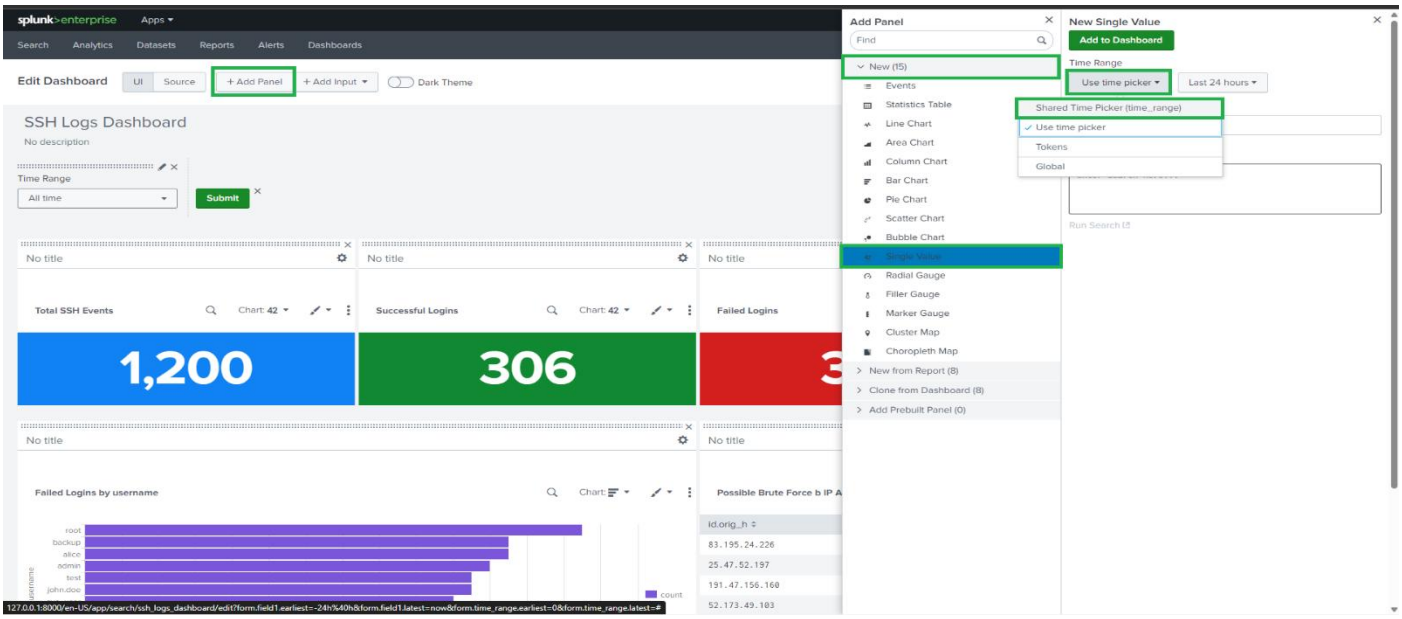
| table id.orig_h

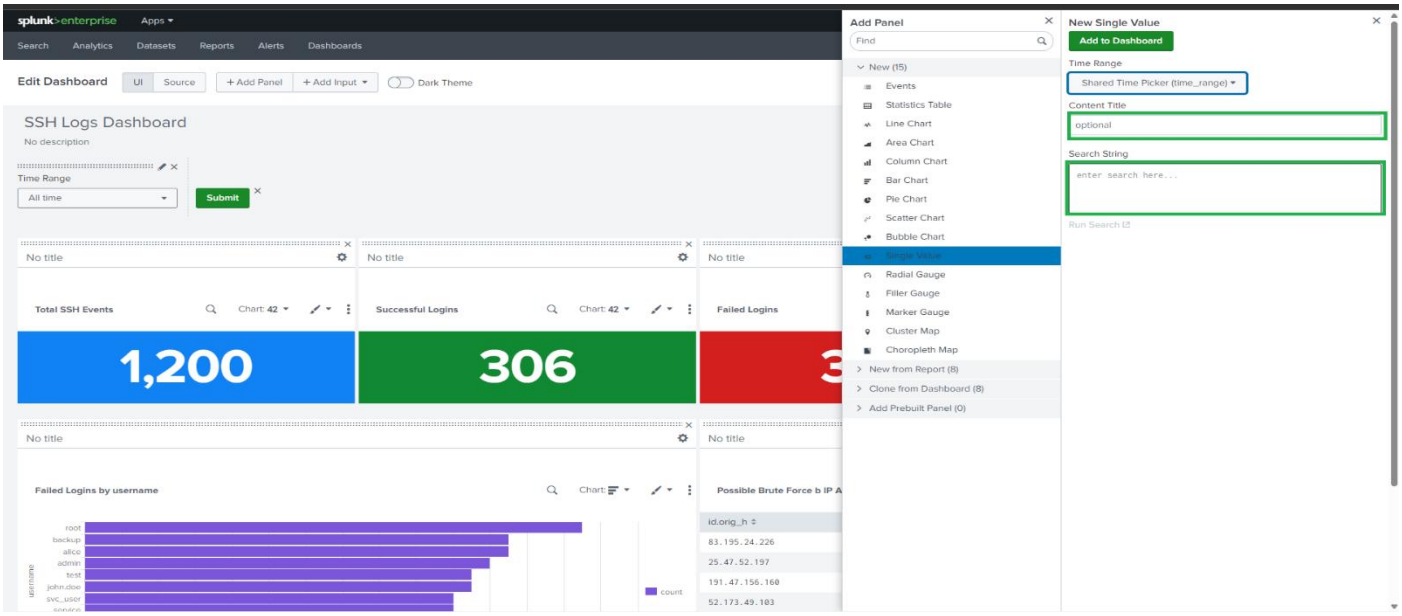
| iplocation id.orig_h

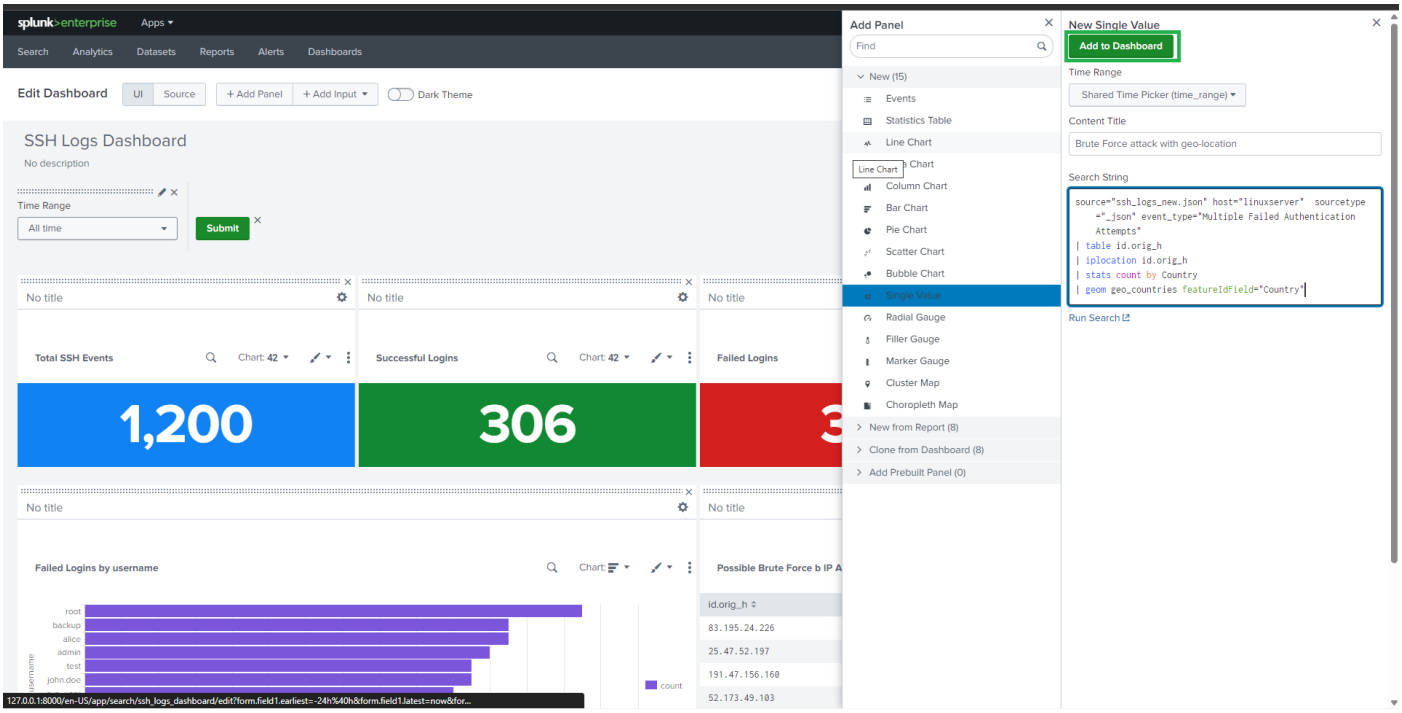
| stats count by Country

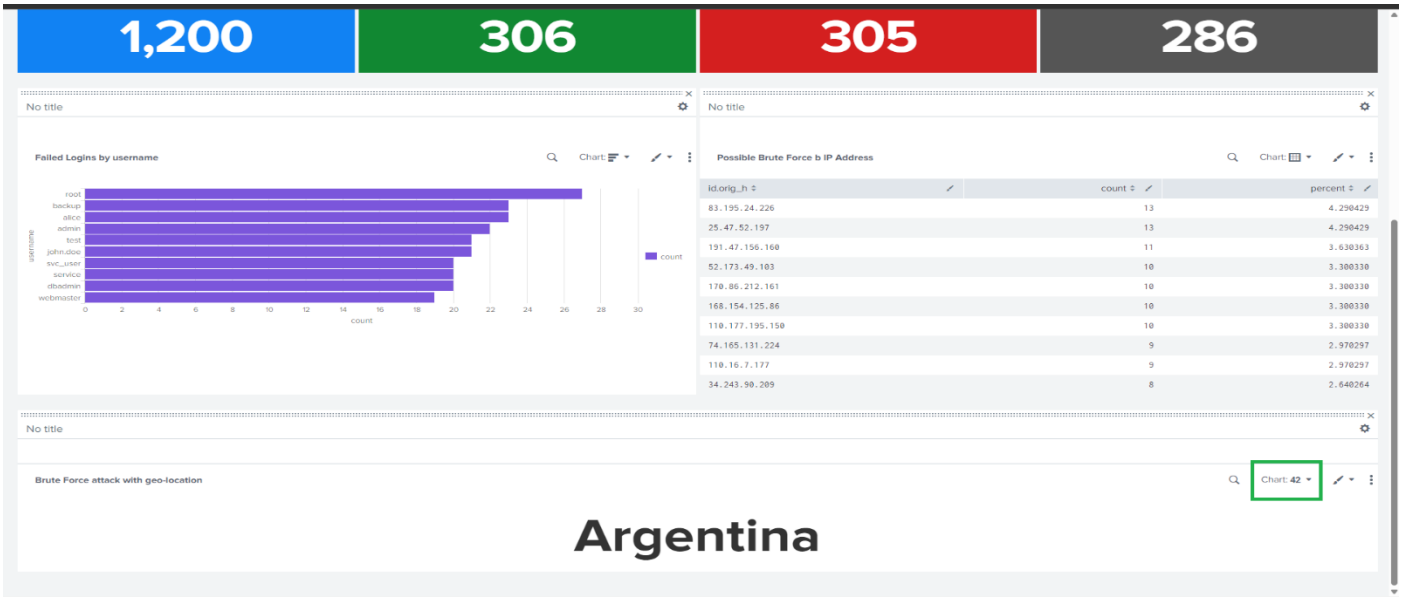
| geom geo_countries featureIdField="Country"

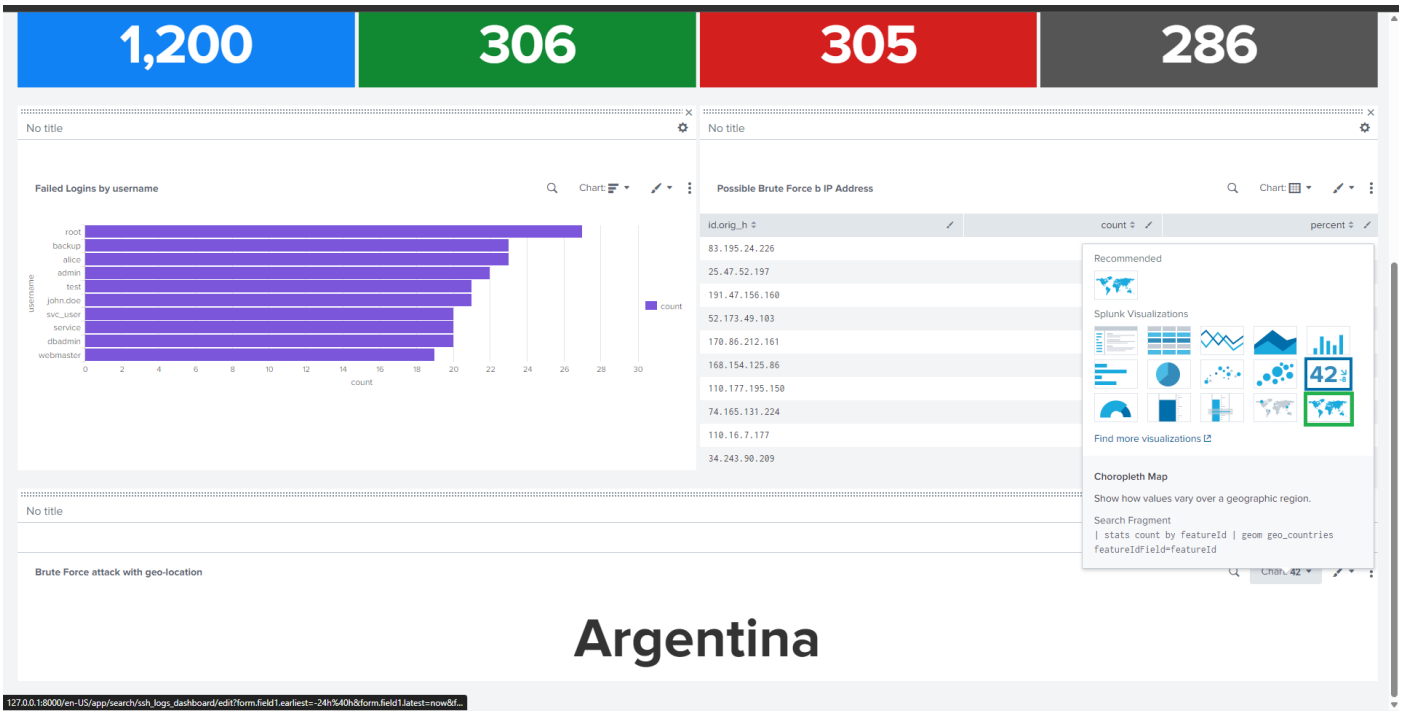


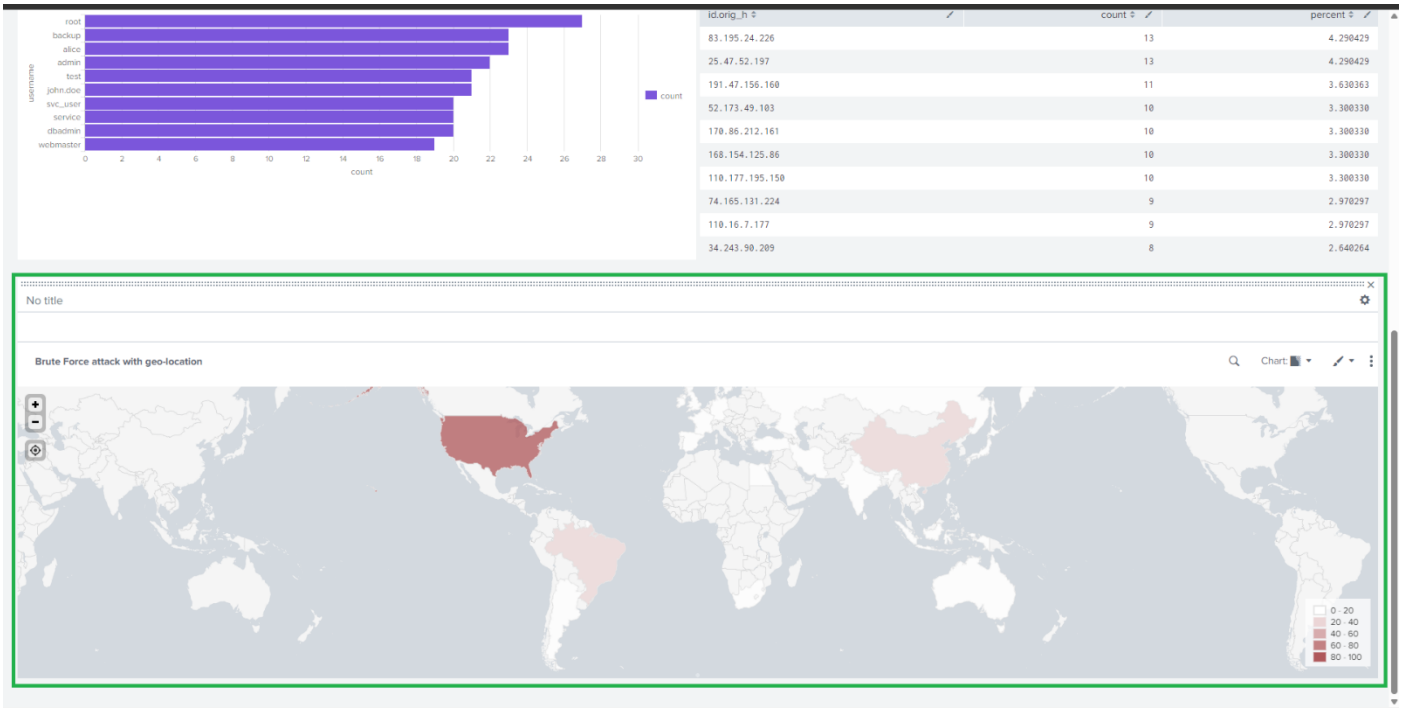

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
SSH Logs Dashboard
No description
Time Range
All time
Submit
No title
Total SSH Events
Chart: 42
1,200
Successful Logins
306
Failed Logins
Failed Logins by username
Possible Brute Force b IP A
id.orig_h
83.195.24.226
25.47.52.197
191.47.156.160
52.173.49.103
root
backup
alice
admin
test
john.doe
username
count
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (8)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Use time picker
Last 24 hours
Shared Time Picker (time_range)
Use time picker
Tokens
Global
Run Search
127.0.0.1:8000/en-US/app/search/ssh_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now&form.time_range.earliest=0&form.time_range.latest=#

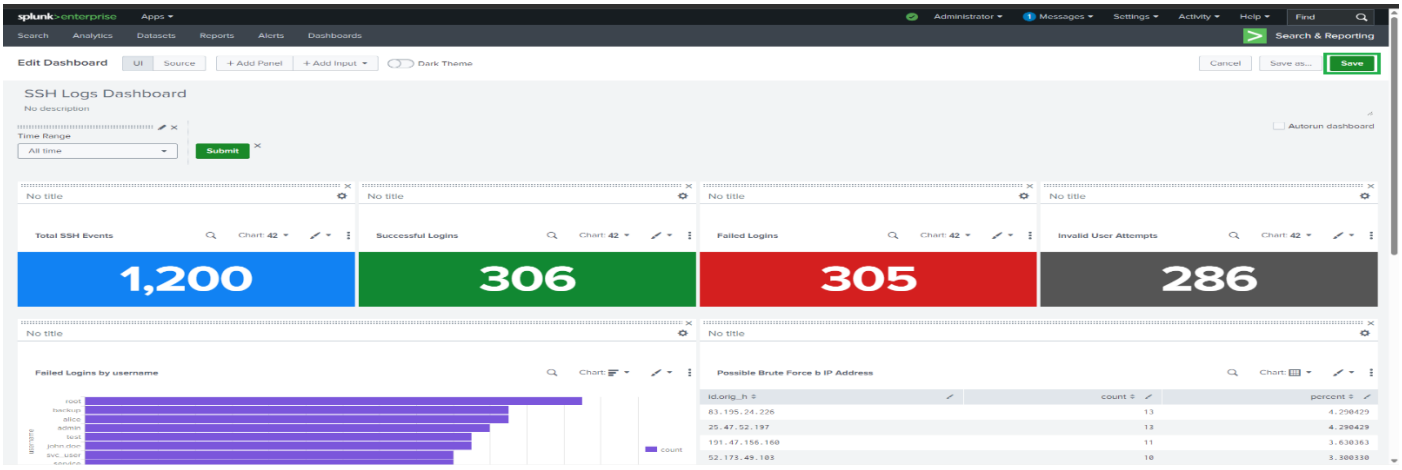

splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
SSH Logs Dashboard
No description
Time Range
All time
Submit
No title
Total SSH Events
Chart: 42
1,200
Successful Logins
306
Failed Logins
Failed Logins by username
Possible Brute Force b IP A
id.orig_h
83.195.24.226
25.47.52.197
191.47.156.160
52.173.49.103
root
backup
alice
admin
test
john.doe
svc_user
username
count
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Area Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (8)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
optional
Search String
enter search here...
Run Search


splunk>enterprise
Apps
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Edit Dashboard
UI
Source
+ Add Panel
+ Add Input
Dark Theme
SSH Logs Dashboard
No description
Time Range
All time
Submit
No title
Total SSH Events
Chart: 42
1,200
Successful Logins
306
Failed Logins
Failed Logins by username
Possible Brute Force b IP A
id.orig_h
83.195.24.226
25.47.52.197
191.47.156.160
52.173.49.103
root
backup
alice
admin
test
john.doe
username
count
Add Panel
Find
New (15)
Events
Statistics Table
Line Chart
Line Chart
Column Chart
Bar Chart
Pie Chart
Scatter Chart
Bubble Chart
Single Value
Radial Gauge
Filler Gauge
Marker Gauge
Cluster Map
Choropleth Map
New from Report (8)
Clone from Dashboard (8)
Add Prebuilt Panel (0)
New Single Value
Add to Dashboard
Time Range
Shared Time Picker (time_range)
Content Title
Brute Force attack with geo-location
Search String
source="ssh_logs_new.json" host="linuxserver" sourcetype="_json" event_type="Multiple Failed Authentication Attempts"
| table id.orig_h
| iplocation id.orig_h
| stats count by Country
| geom geo_countries featureIdField="Country"
Run Search
127.0.0.1:8000/en-US/app/search/ssh_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now&for...


1,200
306
305
286
No title
Failed Logins by username
Chart:
root
backup
alice
admin
test
john.doe
svc_user
service
dbadmin
webmaster
username
count
0 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30
count
No title
Possible Brute Force b IP Address
Chart:
id.orig_h
count
percent
83.195.24.226 13 4.290429
25.47.52.197 13 4.290429
191.47.156.160 11 3.630363
52.173.49.103 10 3.300330
170.86.212.161 10 3.300330
168.154.125.86 10 3.300330
110.177.195.150 10 3.300330
74.165.131.224 9 2.970297
110.16.7.177 9 2.970297
34.243.90.209 8 2.640264
No title
Brute Force attack with geo-location
Chart: 42
Argentina


1,200
306
305
286
No title
Failed Logins by username
Chart:
root
backup
alice
admin
test
john.doe
svc_user
service
dbadmin
webmaster
username
count
0 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30
count
No title
Possible Brute Force b IP Address
Chart:
id.orig_h
count
percent
83.195.24.226
25.47.52.197
191.47.156.160
52.173.49.103
170.86.212.161
168.154.125.86
110.177.195.150
74.165.131.224
110.16.7.177
34.243.90.209
Recommended
Splunk Visualizations
42
Find more visualizations
Choropleth Map
Show how values vary over a geographic region.
Search Fragment
| stats count by featureId | geom geo_countries featureIdField=featureId
No title
Brute Force attack with geo-location
Argentina
127.0.0.1:8000/en-US/app/search/ssh_logs_dashboard/edit?form.field1.earliest=-24h%40h&form.field1.latest=now&f...


root
backup
alice
admin
test
john.doe
svc_user
service
dbadmin
webmaster
username
count
0 2 4 6 8 10 12 14 16 18 20 22 24 26 28 30
count
id.orig_h
count
percent
83.195.24.226 13 4.290429
25.47.52.197 13 4.290429
191.47.156.160 11 3.630363
52.173.49.103 10 3.300330
170.86.212.161 10 3.300330
168.154.125.86 10 3.300330
110.177.195.150 10 3.300330
74.165.131.224 9 2.970297
110.16.7.177 9 2.970297
34.243.90.209 8 2.640264
No title
Brute Force attack with geo-location
Chart:
0 - 20
20 - 40
40 - 60
60 - 80
80 - 100



🚀 Key Outcomes

- Centralized SSH authentication monitoring
- Early detection of brute-force attacks
- Improved visibility using geo-location analysis
- Consistent time-based analysis across panels

🛡️ Security Use Case

This dashboard can be used by:

- SOC Analysts
- Blue Teams
- System Administrators
- Cybersecurity Students

to **detect unauthorized access attempts** and **respond to SSH-based attacks efficiently**.