

splunk>enterprise Apps ▾

Administrator 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Hello, Administrator

Home page settings

Apps

Find more apps Manage

Search apps by name...

Search & Reporting

Audit Trail

Discover Splunk Observability Cloud

Splunk Secure Gateway

Upgrade Readiness App

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.

The screenshot shows the Splunk Enterprise search interface. At the top, there is a dark header bar with the "splunk>enterprise" logo, a "Apps" dropdown, user status (Administrator), message count (1), and a "Settings" menu which is highlighted with a green box. To the right of the settings are "Activity", "Help", "Find", and a search icon. Below the header is a secondary navigation bar with links for "Search", "Analytics", "Datasets", "Reports", "Alerts", and "Dashboards". A "Search & Reporting" link is also present. The main content area is titled "Search" and contains a search bar with placeholder text "enter search here...". To the right of the search bar are "Time range: Last 24 hours" and a search button. Below the search bar, there is a message "No Event Sampling" and a "Smart Mode" toggle. A "Search History" link is available. The left side of the page has a "How to Search" section with a link to "Documentation", "Tutorial", and "Data Summary". The right side has a "Analyze Your Data with Table Views" section with a "Create Table View" button. A footer at the bottom left shows the URL "127.0.0.1:8000/en-US/app/search/search#".

Splunk > enterprise Apps ▾

Administrator 1 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 using complex transforms, clean and transform it for analysis in Analytics. Learn more ⓘ about Table Views, or view and edit existing Table Views.

Add Data

Monitoring Console

KNOWLEDGE

- Searches, reports, and alerts
- Data models
- Event types
- Tags
- Fields
- Lookups
- User interface
- Alert actions
- Advanced search
- All configurations

DATA

- Data inputs
- Forwarding and receiving
- Indexes
- Report acceleration summaries
- Source types
- Ingest actions

DISTRIBUTED ENVIRONMENT

- Agent management
- Indexer clustering
- Federation
- Distributed search

SYSTEM

- Server settings
- Server controls
- Health report manager
- Instrumentation
- Licensing
- Workload management
- Mobile settings

USERS AND AUTHENTICATION

- Roles
- Users
- Tokens
- Password management
- Authentication methods

Search settings... Q

127.0.0.1:8000/en-US/manager/search/adddata

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

Add Data



< 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

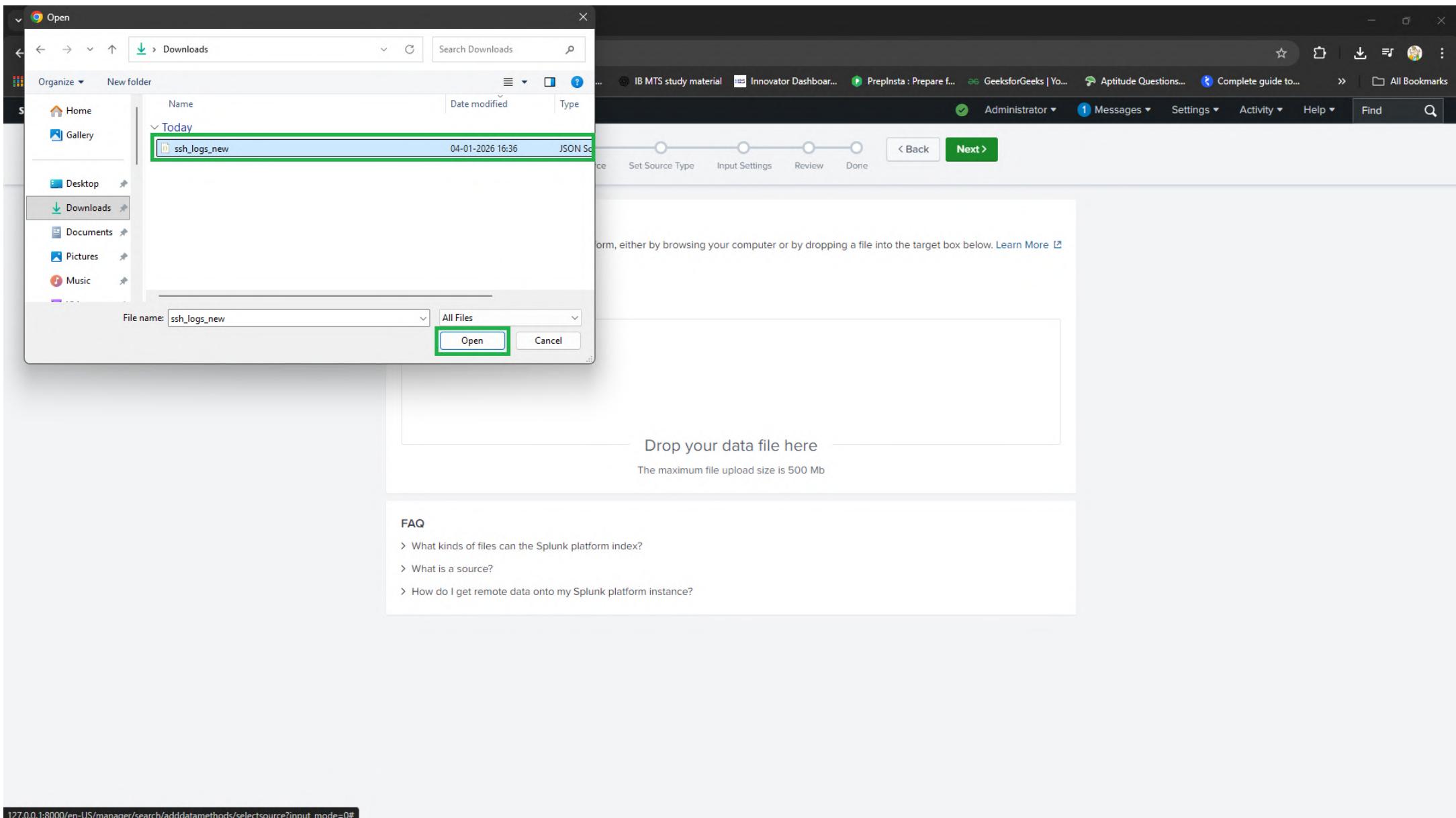
Select File

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?



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: **ssh_logs_new.json**

Select File

Drop your data file here

The maximum file upload size is 500 Mb

File Successfully Uploaded

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?

splunk>enterprise Apps ▾

Administrator 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Add Data

Select Source Set Source Type Input Settings Review Done

< Back Next >

Set Source Type

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

Source: ssh_logs_new.json

View Event Summary

Source type: _json ▾	Save As	Format ▾	Select... ▾	Select... ▾	_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	
> Timestamp					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
> Advanced					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 ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Add Data

Select Source Set Source Type Input Settings Review Done

Input Settings

Optional 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](#)

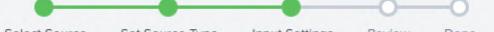
Index Default ▾ Create a new index

FAQ

› How do indexes work?
› How do I know when to create or use multiple indexes?

splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Add Data 

[Select Source](#) [Set Source Type](#) [Input Settings](#) [Review](#) [Done](#)

[Back](#) [Review >](#)

Input Settings

Optional 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 ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Add Data

Select Source Set Source Type Input Settings Review Done

Review >

Input Settings

Optionaly 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 Create a new index

FAQ

› How do indexes work?
› How do I know when to create or use multiple indexes?

splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Add Data

Select Source Set Source Type Input Settings Review Done

Submit < Back

Review

Input Type Uploaded File
File Name ssh_logs_new.json
Source Type _json
Host LinuxServer
Index Default

The screenshot shows the Splunk Add Data wizard in progress, specifically the 'Review' step. The top navigation bar includes links for 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a search icon. Below the navigation is a progress bar with five steps: 'Select Source' (green dot), 'Set Source Type' (green dot), 'Input Settings' (green dot), 'Review' (green dot), and 'Done' (light gray circle). To the right of the progress bar are buttons for '< Back' and 'Submit' (which is highlighted with a green border). The main content area is titled 'Review' and contains the following configuration details:
Input Type Uploaded File
File Name ssh_logs_new.json
Source Type _json
Host LinuxServer
Index Default

Add Data



< 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. [Learn more](#)

[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 ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

Dashboards

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 Q

i	★	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

splunk>enterprise Apps ▾

Search Analytics Datasets Reports Alerts Dashboards

Dashboards

Dashboards include searches, visualizations, and input controls that capture and present available data.

Latest Resources

- Examples for Dashboard Studio
- Intro to Dashboard Studio
- Intro to Classic XML dashboards

7 Dashboards

#	Title	Owner	App	Sharing	Type
>	Integrity Check of Installed Files	nobody	search	App	Dashboard Studio
>	Job Details Dashboard	nobody	search	App	Dashboard Studio
>	jQuery Upgrade	nobody	search	App	Classic
>	Orphaned Scheduled Searches, Reports, and Alerts	nobody	search	App	Dashboard Studio
>	Scheduled export is now available for Dashboard Studio	nobody	search	Global	Dashboard Studio
>	Successful Login	gaurav23	search	Private	Dashboard Studio
>	Web Traffic Logs Dashboard	gaurav23	search	Private	Classic

Create New Dashboard

Dashboard Title Required

Description

Permissions

Dashboard type ?

Classic Dashboards
The traditional Splunk dashboard builder

Dashboard Studio
A new builder to create visually-rich, customizable dashboards

splunk>enterprise Apps ▾

Search Analytics Datasets Reports Alerts Dashboards

Dashboards

Dashboards include searches, visualizations, and input controls that capture and present available data.

Latest Resources

- Examples for Dashboard Studio
- Intro to Dashboard Studio
- Intro to Classic Dashboards

7 Dashboards

i	Title
>	Integrity Check of Installed Files
>	Job Details Dashboard
>	jQuery Upgrade
>	Orphaned Scheduled Searches, Reports, and Alerts
>	Scheduled export is now available for Dashboard Studio
>	Successful Login
>	Web Traffic Logs Dashboard

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](#)

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search & Reporting [Create New Dashboard](#)

Owner	App	Sharing	Type
nobody	search	App	Dashboard Studio
nobody	search	App	Dashboard Studio
nobody	search	App	Classic
nobody	search	App	Dashboard Studio
nobody	search	Global	Dashboard Studio
gaurav23	search	Private	Dashboard Studio
gaurav23	search	Private	Classic

splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

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

! Click Add Panel to start.

The screenshot shows the Splunk Enterprise interface for creating a new dashboard. The top navigation bar includes links for Search, Analytics, Datasets, Reports, Alerts, and Dashboards, along with a 'Search & Reporting' button. Below the navigation is a toolbar with tabs for UI, Source, and '+ Add Panel' (which is highlighted with a green box), followed by a '+ Add Input' dropdown, a 'Dark Theme' toggle, and buttons for Cancel, Save as..., and Save. The main content area is titled 'SSH Logs Dashboard' and contains the message 'No description'. At the bottom left, there is a red exclamation mark icon with the text 'Click Add Panel to start.' The entire dashboard area is enclosed in a light gray box.

splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

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

! Click Add Panel to start.

T Text
Radio
Dropdown
Checkbox
Multiselect
Link List
Time
Submit

The screenshot shows the Splunk Enterprise interface for editing a dashboard. The top navigation bar includes links for Search, Analytics, Datasets, Reports, Alerts, and Dashboards, along with a 'Search & Reporting' button. Below the navigation is a toolbar with tabs for 'Edit Dashboard' (selected), 'UI' (highlighted in blue), 'Source', and buttons for '+ Add Panel', '+ Add Input' (with a dropdown menu open), and 'Dark Theme'. On the right side of the toolbar are 'Cancel', 'Save as...', and 'Save' buttons. The main area is titled 'SSH Logs Dashboard' with a note 'No description'. A red exclamation mark icon with the text 'Click Add Panel to start.' is present. A context menu is open over the dashboard area, listing various input component types: Text (selected), Radio, Dropdown, Checkbox, Multiselect, Link List, Time (highlighted with a green border), and Submit. The URL in the browser's address bar is 127.0.0.1:8000/en-US/app/search/ssh_logs_dashboard/edit#.

splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

Edit Dashboard UI Source + Add Panel + Add Input ▾ Dark Theme Cancel Save as... Save

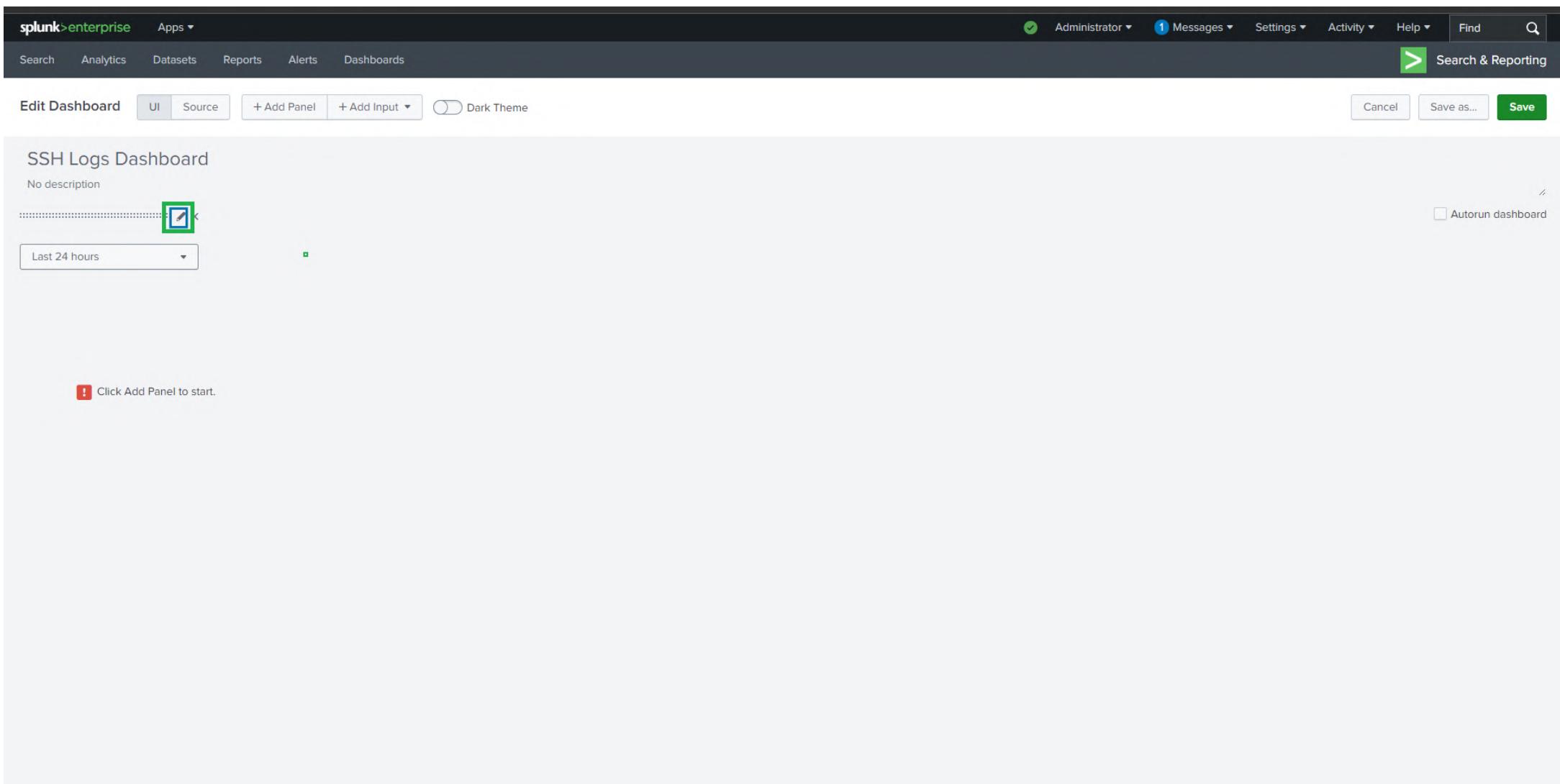
SSH Logs Dashboard

No description

Last 24 hours

Autorun dashboard

! Click Add Panel to start.

A screenshot of the Splunk Enterprise interface showing a blank dashboard titled "SSH Logs Dashboard". The dashboard has a single search bar at the top set to "Last 24 hours". There are tabs for "UI", "Source", "+ Add Panel", and "+ Add Input". A "Dark Theme" toggle is off. On the right, there are buttons for "Cancel", "Save as...", and a large green "Save" button. A message at the bottom left says "Click Add Panel to start." with a red exclamation mark icon. The top navigation bar includes links for "splunk>enterprise", "Apps", "Administrator", "Messages", "Settings", "Activity", "Help", "Find", and a search bar.

splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

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

General

Label

Search on Change

Token Options

Token?

Default?

Cancel Apply

Autorun dashboard

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with links for 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a search bar. Below the navigation is a secondary menu with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. To the right of this is a large green button labeled '> Search & Reporting'. The main area is titled 'SSH Logs Dashboard' and has a note 'No description'. A modal window is open for adding a new input field. The 'Time' input type is selected. The 'Label' field is empty, and the 'Token' field contains 'field1'. The 'Default' dropdown is set to 'Last 24 hours'. There are 'Cancel' and 'Apply' buttons at the bottom of the modal. In the top right corner of the main dashboard area, there are 'Cancel', 'Save as...', and 'Save' buttons. A checkbox for 'Autorun dashboard' is also visible.

splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

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

General

Label Time Range

Search on Change

Token Options

Token ? time_range

Default ? Last 24 hours

Cancel Apply

This screenshot shows the Splunk Enterprise interface for editing a dashboard. A modal dialog is open for configuring a search input component. The 'Time' tab is selected on the left. The 'Default?' dropdown is set to 'Last 24 hours' and is highlighted with a green border. The 'Apply' button at the bottom right of the dialog is also highlighted with a green border.

Presets

Real-time	Relative	Other
30 second window	Today	Last 15 minutes
1 minute window	Week to date	Last 60 minutes
5 minute window	Business week to date	Last 4 hours
30 minute window	Month to date	Last 24 hours
1 hour window	Year to date	Last 7 days
All time (real-time)	Yesterday	Last 30 days
	Previous week	
	Previous business week	
	Previous month	
	Previous year	

> Relative

> Real-time

> Date Range

> Date & Time Range

> Advanced

Link List

Default ? Last 24 hours

Time

Cancel Apply

Administrator 1 Messages Settings Activity Help Find

> Search & Reporting

Cancel Save as... Save

Autorun dashboard

splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

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

General

Label Time Range

Search on Change

Token Options

Token ? time_range

Default ? All time

Cancel Apply

Autorun dashboard

This screenshot shows the Splunk Enterprise interface for editing a dashboard. A modal dialog is open for configuring a search input field. The 'Time' tab is selected in the left sidebar. The 'Default' dropdown is set to 'All time'. The 'Apply' button at the bottom right of the dialog is highlighted with a green border.

splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

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

Autorun dashboard

! Click Add Panel to start.

splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

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

Autorun dashboard

Submit

! 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 ▾ 1 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

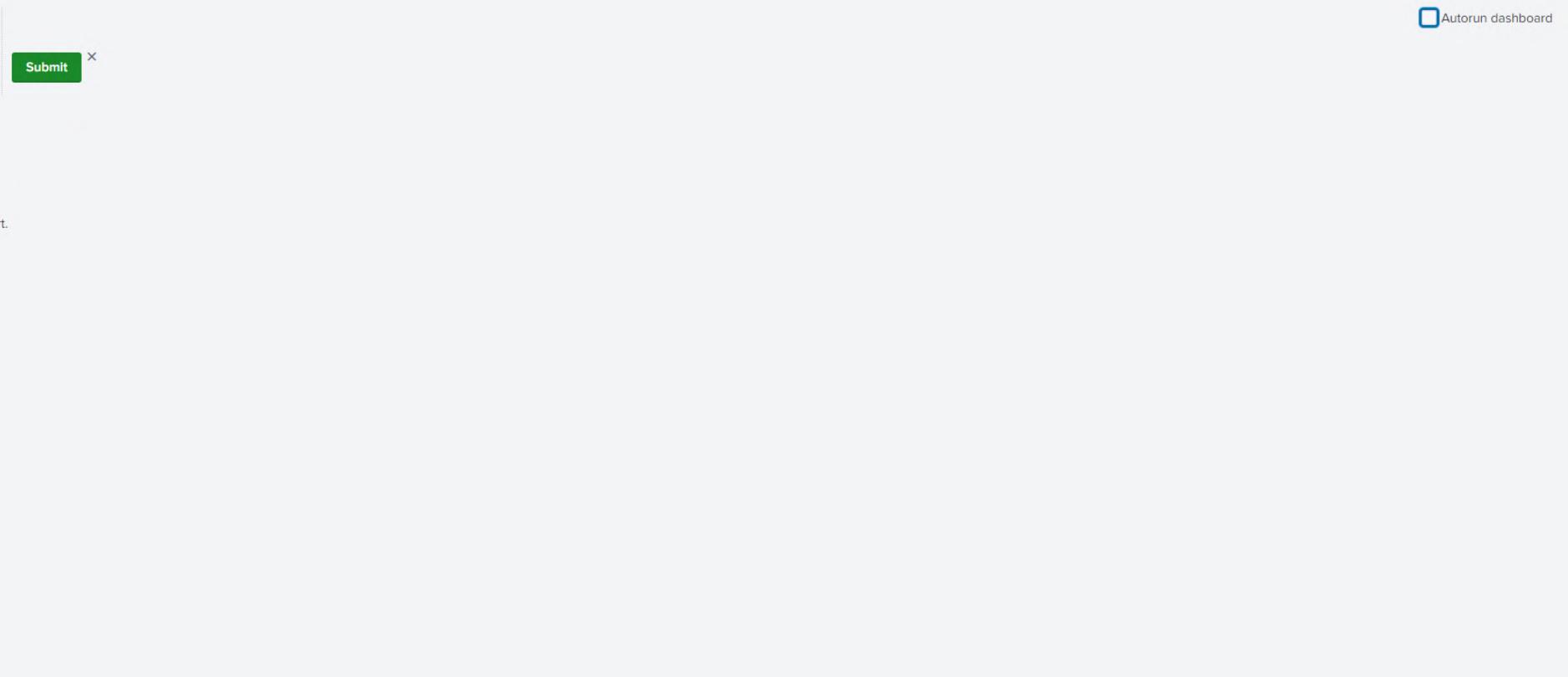
No description

Time Range

All time

Autorun dashboard

Click Add Panel to start.



splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

SSH Logs Dashboard

Time Range

All time Hide Filters

! This dashboard has no panels. Start editing to add panels.

The screenshot shows the Splunk Enterprise web interface. At the top, the navigation bar includes links for 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a search bar. Below the navigation is a secondary menu with links for 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. A green arrow icon followed by 'Search & Reporting' is also present. The main content area is titled 'SSH Logs Dashboard'. It features a 'Time Range' dropdown set to 'All time', a 'Submit' button, and a 'Hide Filters' link. A message at the bottom indicates 'This dashboard has no panels. Start editing to add panels.' with a red exclamation mark icon. On the far right, there are buttons for 'Edit' (which is highlighted with a green box), 'Export', and three dots (...). The overall interface is dark-themed.

splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

Edit Dashboard UI Source + Add Panel + Add Input ▾ Dark Theme Cancel Save as... Save

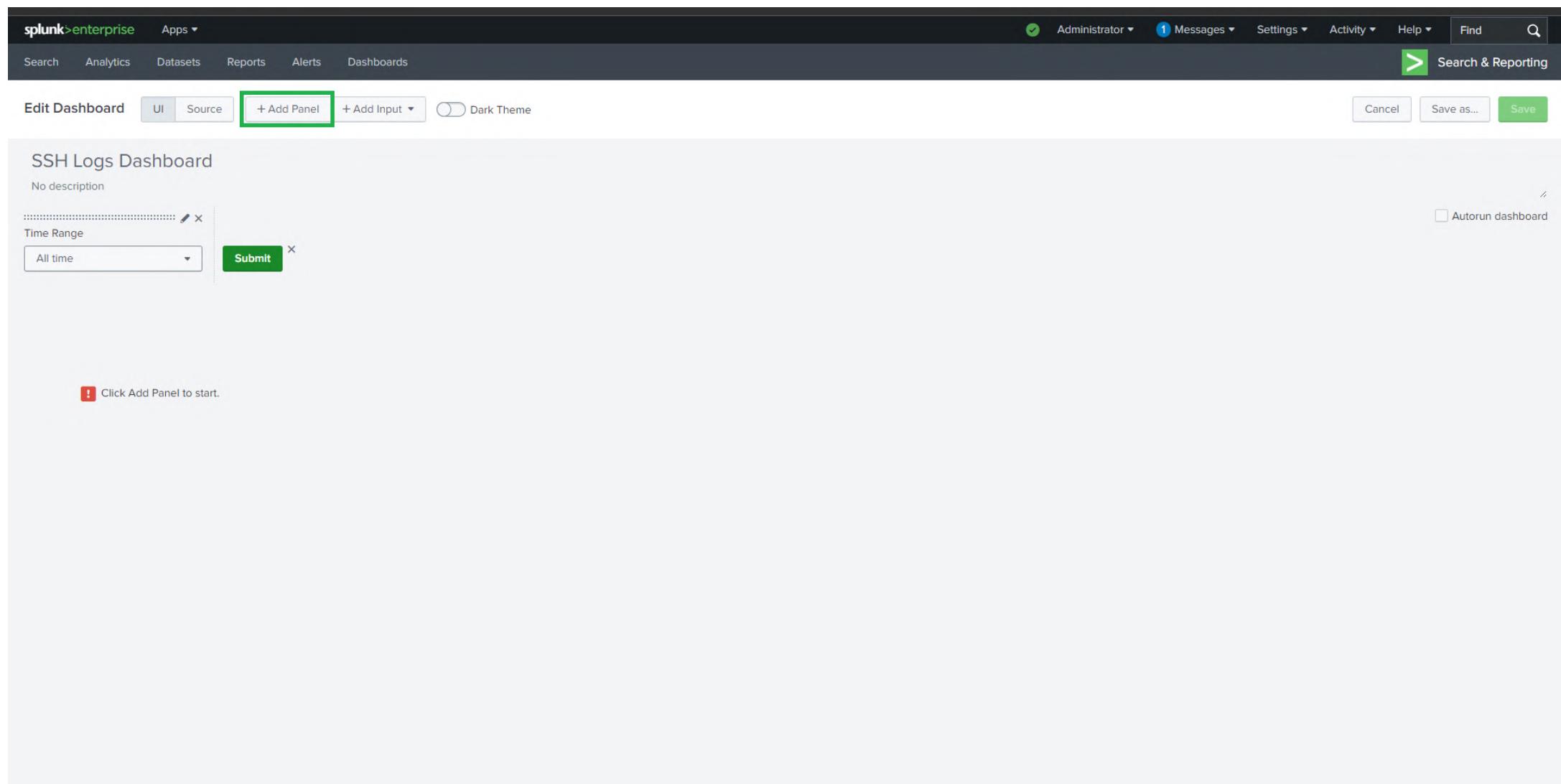
SSH Logs Dashboard

No description

Time Range

Autorun dashboard

 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

! Click Add Panel to start.

Add Panel

New Single Value

Time Range

Use time picker ▾ Last 24 hours ▾

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

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

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

! Click Add Panel to start.

Add Panel

Find

New Single Value

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

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)

splunk>enterprise Apps ▾

Administrator ▾ 1 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

No title

Total SSH Events

1,200

Splunk > enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

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 Autorun dashboard

All time

No title

Total SSH Events

Chart: 42

1,200

General Use Colors Yes No

Color by Value Trend

Color

Number Format

Ranges from min to 0

from 0 to 30

from 30 to 70

from 70 to 100

from 100 to max

#182f3

+ Add Range

Color Mode 42

42

Color

Color by Value Trend

Color Mode 42

splunk>enterprise Apps ▾

Administrator ▾ 1 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 Submit Autorun dashboard

No title

Total SSH Events Chart: 42 ▾

1,200

This screenshot shows the Splunk Enterprise interface for creating and managing dashboards. The top navigation bar includes links for 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and search functions. Below the navigation is a toolbar with buttons for 'Edit Dashboard', 'UI', 'Source', 'Add Panel', 'Add Input', 'Dark Theme', and save options ('Cancel', 'Save as...', 'Save'). The main content area is titled 'SSH Logs Dashboard' with a 'No description' note. It features a 'Time Range' filter set to 'All time' with a 'Submit' button. A large blue panel displays the count '1,200'.

splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

SSH Logs Dashboard

Time Range

All time Hide Filters

Total SSH Events

1,200

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with links for 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a search bar. Below the navigation is a secondary menu with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. A green arrow icon followed by 'Search & Reporting' is also present. The main content area is titled 'SSH Logs Dashboard'. It features a 'Time Range' dropdown set to 'All time', a 'Submit' button, and a 'Hide Filters' link. A prominent blue summary card displays the text 'Total SSH Events' and the number '1,200' in large white font. In the top right corner of this card, there are several buttons: a star icon, 'Edit' (which is highlighted with a green box), 'Export' (with a dropdown arrow), and a three-dot menu icon.

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

Total SSH Events

1,200

Add Panel X

New Single Value X

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)

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

Total SSH Events

1,200

Add Panel

New Single Value

Time Range Shared Time Picker (time_range) ▾

Content Title optional

Search String enter search here...

▼ 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)

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

Total SSH Events

1,200

Add Panel

New Single Value

Add to Dashboard

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

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 ▾ 1 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 Submit

No title

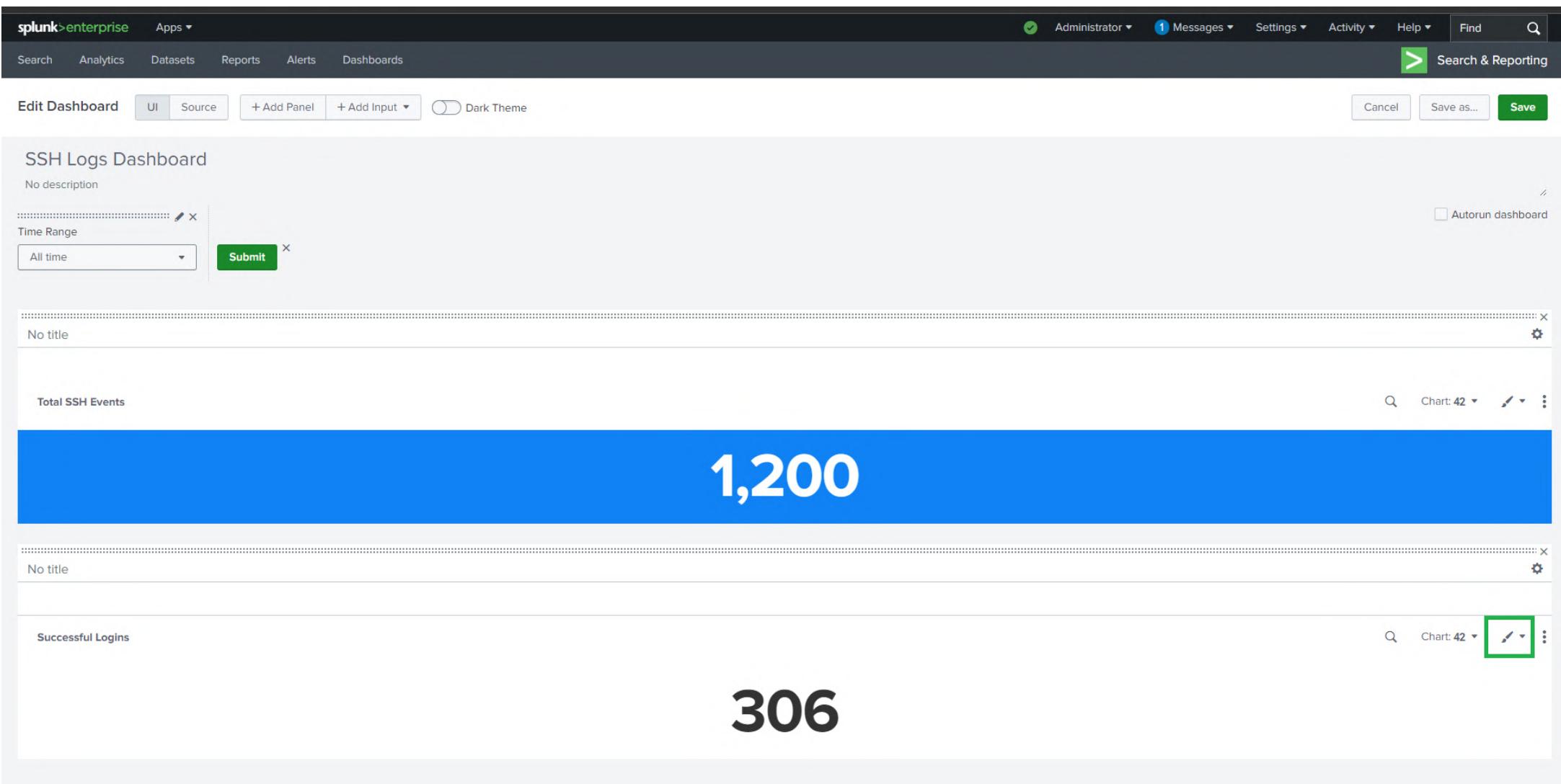
Total SSH Events Chart: 42 ▾  

1,200

No title

Successful Logins Chart: 42 ▾  

306



splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

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 Autorun dashboard

All time

No title

Total SSH Events

1,200

General Use Colors Yes No

Color by Value Trend

Number Format

Ranges from min to max

Range	Value	Color
from 0	0	Green
from 30	30	Yellow
from 70	70	Red
from 100	100	Dark Red
to max	118832	Dark Green

+ Add Range

Color Mode 42 42

No title

Successful Logins

306

splunk>enterprise Apps ▾

Administrator ▾ 1 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

Total SSH Events Chart: 42 ▾

1,200

No title

Successful Logins Chart: 42 ▾

306

splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

SSH Logs Dashboard

Time Range

All time Submit Hide Filters

Total SSH Events

Successful Logins

1,200 306

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with links for 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a search bar. Below the navigation is a secondary header with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', 'Dashboards', and a 'Search & Reporting' dropdown. The main content area is titled 'SSH Logs Dashboard'. It features two large, bold numbers in colored boxes: '1,200' in blue for 'Total SSH Events' and '306' in green for 'Successful Logins'. Above each number is its respective metric name. At the bottom left of the dashboard, there are filter options for 'Time Range' (set to 'All time'), a 'Submit' button, and a 'Hide Filters' link. On the far right of the dashboard, there are buttons for 'Edit' (which is highlighted with a green box), 'Export', and three dots for more options.

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

Total SSH Events

1,200

Successful Logins

Add Panel

New Single Value

Add to Dashboard

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)

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

Total SSH Events

1,200

Successful Logins

Add Panel

New Single Value

Time Range Shared Time Picker (time_range) ▾

Content Title optional

Search String enter search here...

Panel Options:

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

Add Panel Find New Single Value Add to Dashboard

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)

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 ↗

```
source="ssh_logs_new.json" host="LinuxServer" sourcetype ="_json" event_type="Failed SSH Login" | stats count AS "Failed Login"
```

splunk>enterprise Apps ▾

Administrator ▾ 1 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

Total SSH Events No title Failed Logins

splunk>enterprise Apps ▾

Administrator 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

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 Autorun dashboard

All time

No title

Total SSH Events

1,200

Successful Logins

Number Format

General

Use Colors Yes No

Color by Value Trend

Ranges from min to max

Range	Value	Trend
from 0	0	Green
from 30	30	Grey
from 70	70	Blue
from 100	100	Red
to max		

+ Add Range

Color Mode 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 1 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 Submit

No title

Total SSH Events Chart: 42

1,200

Successful Logins Chart: 42

306

No title

Failed Logins Chart: 42

305

splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

SSH Logs Dashboard

Time Range

All time Submit Hide Filters

Total SSH Events

Successful Logins

Failed Logins

1,200 306 305

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with links for 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a search bar. Below the navigation is a secondary header with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', 'Dashboards', and a 'Search & Reporting' dropdown. The main title 'SSH Logs Dashboard' is displayed. Underneath, there's a 'Time Range' section with a dropdown set to 'All time', a 'Submit' button, and a 'Hide Filters' link. The dashboard features three large, colored boxes: a blue box for 'Total SSH Events' containing the number '1,200', a green box for 'Successful Logins' containing '306', and a red box for 'Failed Logins' containing '305'. In the top right corner of the dashboard area, there are several small buttons: a star icon, 'Edit' (which is highlighted with a green box), 'Export', and a three-dot menu. The overall background is white with dark grey header sections.

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

Total SSH Events

1,200

Successful Logins

306

Add Panel

New Single Value

Add to Dashboard

New (15)

- Events
- Statistics Table
- Line Chart
- Area Chart
- Column Chart
- Bar Chart
- Pie Chart
- Scatter Chart
- Bubble Chart

Shared Time Picker (time_range)
Use time picker

Tokens

Global

Run Search

Single Value

- Radial Gauge
- Filler Gauge
- Marker Gauge
- Cluster Map
- Choropleth Map

New from Report (8)

Clone from Dashboard (8)

Add Prebuilt Panel (0)

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 No title

Total SSH Events Chart: 42 Successful Logins Chart: 42

1,200 306

Add Panel Find X

New Single Value Add to Dashboard

Time Range Shared Time Picker (time_range)

Content Title optional

Search String enter search here...

Run Search

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)

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

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

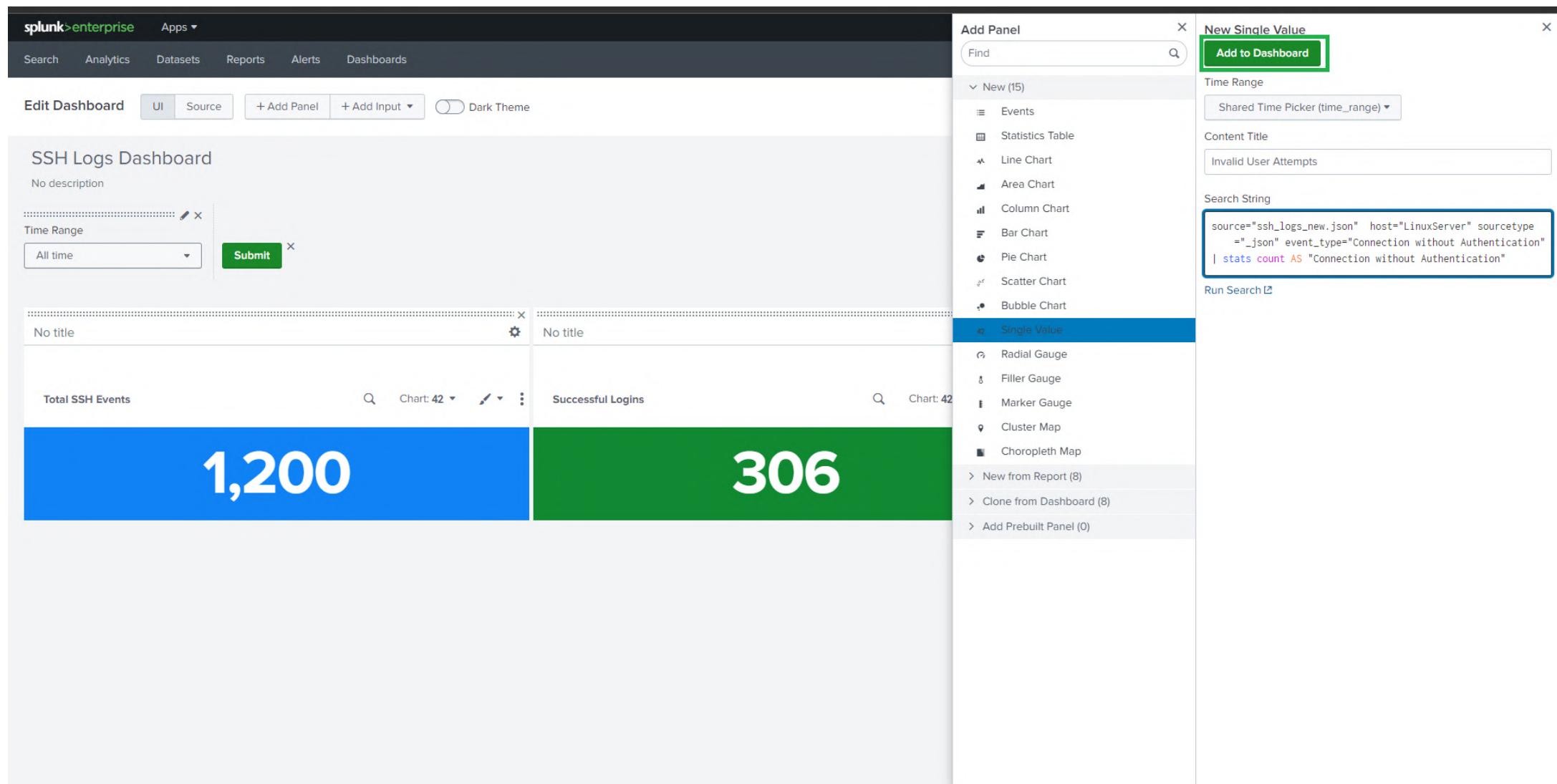
New Single Value Add to Dashboard

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 ▾ 1 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

Total SSH Events Chart: 42

1,200

Successful Logins Chart: 42

306

Failed Logins Chart: 42

305

No title

Invalid User Attempts Chart: 42

286

This screenshot shows the Splunk Enterprise interface for editing a dashboard titled 'SSH Logs Dashboard'. The dashboard has no description and includes an 'Autorun dashboard' checkbox. It features a search bar for 'Time Range' set to 'All time' with a 'Submit' button. The main area contains four data panels: 'Total SSH Events' (1,200), 'Successful Logins' (306), 'Failed Logins' (305), and 'Invalid User Attempts' (286). Each panel has search, chart, edit, and more options icons. The interface includes a top navigation bar with links for Search, Analytics, Datasets, Reports, Alerts, and Dashboards, along with a 'Find' and search bar. A bottom navigation bar offers options to 'Edit Dashboard', switch between 'UI' and 'Source' modes, add panels or inputs, enable 'Dark Theme', and save changes.

splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

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 Autorun dashboard

All time

No title No title No title

Total SSH Events Successful Logins Failed Logins

1,200 306

Invalid User Attempts

286

General Use Colors Yes No

Color by Value Trend

Number Format

Ranges from min to max

	from	to	Color
0	0	0	Green
30	30	30	Blue
70	70	70	Yellow
100	100	100	Red

+ Add Range

Color Mode 42 42

SSH Logs Dashboard

No description

Time Range Autorun dashboard

All time

No title No title No title

Total SSH Events Successful Logins Failed Logins

1,200 306

Invalid User Attempts

286

General Use Colors Yes No

Color by Value Trend

Number Format

Ranges from min to max

	from	to	Color
0	0	0	Green
30	30	30	Blue
70	70	70	Yellow
100	100	100	Red

+ Add Range

Color Mode 42 42

splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards

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

No title No title No title

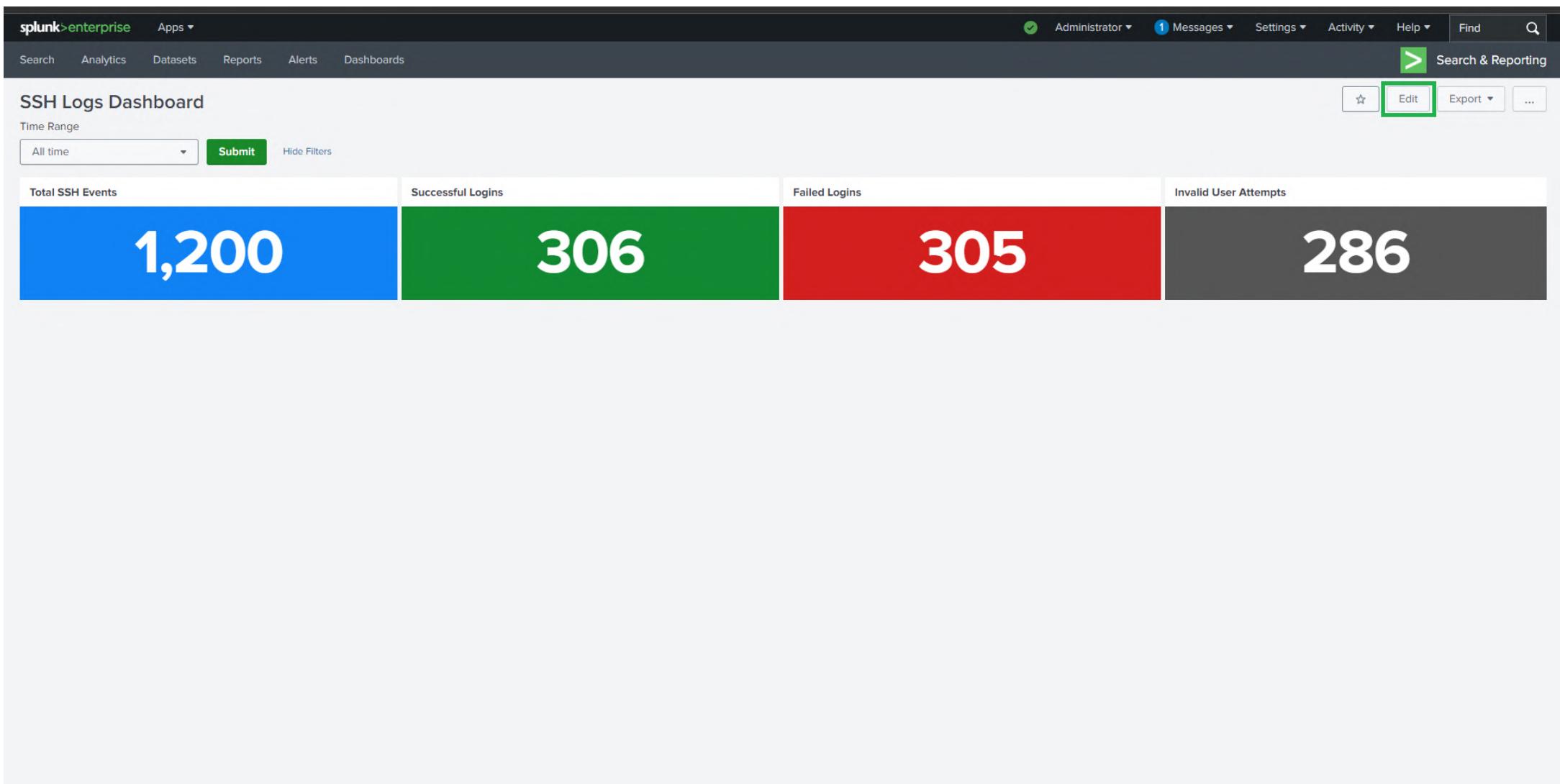
Total SSH Events Chart: 42 Successful Logins Chart: 42 Failed Logins Chart: 42

1,200 **306** **305**

No title

Invalid User Attempts Chart: 42

286



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

Total SSH Events Successful Logins Failed Logins

1,200 306 3

Add Panel

New Single Value

Add to Dashboard

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)

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

Total SSH Events No title No title No title

Successful Logins Failed Logins

1,200 306 3

Add Panel Find X

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 Single Value Add to Dashboard

Time Range Shared Time Picker (time_range) ▾

Content Title optional

Search String enter search here...

Run Search

The screenshot shows the Splunk Enterprise interface for creating a dashboard. On the left, the 'SSH Logs Dashboard' is displayed with three main data points: 'Total SSH Events' (1,200), 'Successful Logins' (306), and 'Failed Logins' (3). Each point has its own search bar and chart configuration options. On the right, a context menu is open under 'Add Panel', listing various chart types and other panel options. The 'Single Value' option is currently selected. The overall interface is clean and modern, typical of enterprise monitoring tools.

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

Total SSH Events No title No title No title

Successful Logins Failed Logins

1,200 306 3

Add Panel Find X

New (15)

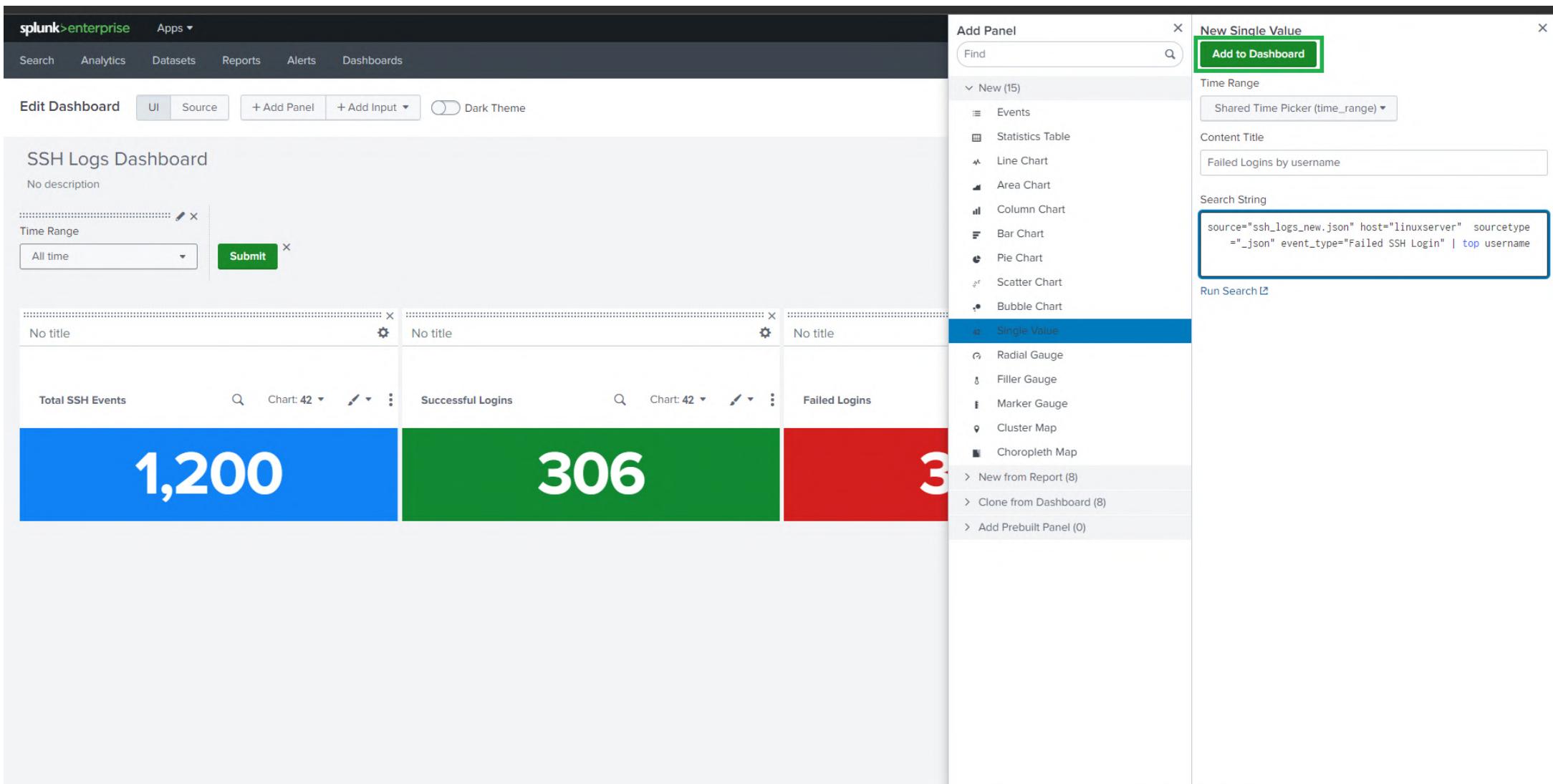
- Events
- Statistics Table
- Line Chart
- Area Chart
- Column Chart
- Bar Chart
- Pie Chart
- Scatter Chart
- Bubble Chart
- Single Value
- Radial Gauge
- Filler Gauge
- Marker Gauge
- Cluster Map
- Choropleth Map

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 ▾ 1 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	No title	No title	No title
Total SSH Events <input type="text"/> Chart: 42 <input type="button"/> <input type="button"/> <input type="button"/> <input type="button"/>	Successful Logins <input type="text"/> Chart: 42 <input type="button"/> <input type="button"/> <input type="button"/> <input type="button"/>	Failed Logins <input type="text"/> Chart: 42 <input type="button"/> <input type="button"/> <input type="button"/> <input type="button"/>	Invalid User Attempts <input type="text"/> Chart: 42 <input type="button"/> <input type="button"/> <input type="button"/> <input type="button"/>
1,200	306	305	286

No title

Failed Logins by username Chart: 42

root

The screenshot shows the Splunk Enterprise interface with the 'SSH Logs Dashboard' open. The dashboard features a top navigation bar with links for Search, Analytics, Datasets, Reports, Alerts, and Dashboards, along with a 'Find' search bar. Below the navigation is a toolbar with buttons for 'Edit Dashboard' (UI or Source), '+ Add Panel', '+ Add Input', 'Dark Theme', and save options ('Cancel', 'Save as...', 'Save'). The main content area is titled 'SSH Logs Dashboard' with a 'No description' note and an 'Autorun dashboard' checkbox. It includes a 'Time Range' section with a dropdown for 'All time' and a 'Submit' button. The dashboard is divided into four sections: 'Total SSH Events' (1,200), 'Successful Logins' (306), 'Failed Logins' (305), and 'Invalid User Attempts' (286), each with its own search and chart controls. Below these are two additional panels: 'Failed Logins by username' and a summary card for the user 'root'. A green box highlights the edit icon in the 'Failed Logins by username' panel's control menu.

Splunk>enterprise Apps ▾

Administrator 1 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 Submit

Total SSH Events Chart: 42 No title

Successful Logins Chart: 42 No title

Failed Logins Chart: 42 No title

Invalid Logins Chart: 42 No title

1,200 306 305

Failed Logins by username Chart: 42

Bar Chart

Compare values or fields.

Search Fragment | stats count by comparison_category

root

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

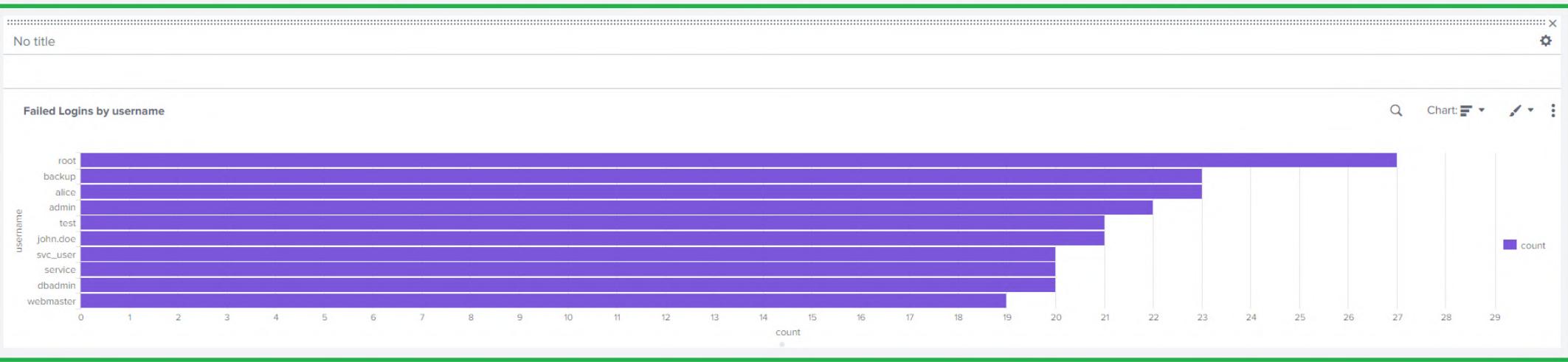
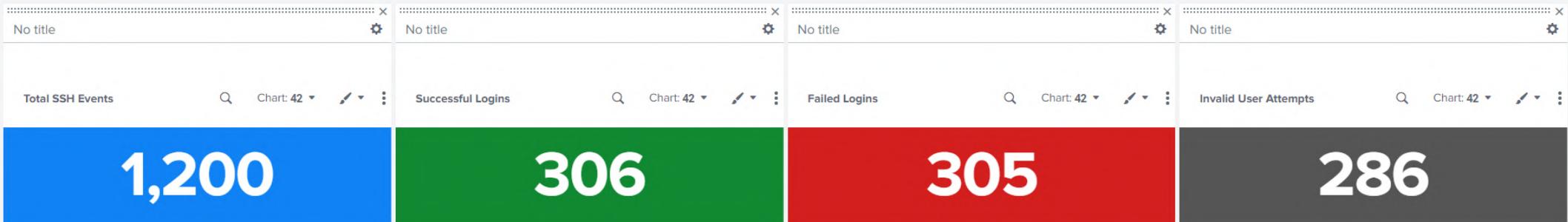
SSH Logs Dashboard

No description

Time Range

All time

Autorun dashboard



splunk>enterprise Apps ▾

Administrator 1 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

No title	No title	No title	No title
Total SSH Events Chart: 42	Successful Logins Chart: 42	Failed Logins Chart: 42	Invalid User Attempts Chart: 42
1,200	306	305	286

No title

Failed Logins by username Chart:

username	count
root	1,200
backup	306
alice	305
admin	286
test	
john.doe	

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

splunk>enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

SSH Logs Dashboard

Time Range

All time Submit Hide Filters

Total SSH Events: 1,200

Successful Logins: 306

Failed Logins: 305

Invalid User Attempts: 286

Failed Logins by username

username count

username	count
root	27
backup	23
alice	22
admin	21
test	20
john.doe	19
svc_user	19
service	19
dbadmin	19
webmaster	19

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

Total SSH Events

Successful Logins

Failed Logins

Failed Logins by username

root
backup
alice
admin
test
john.doe

Add Panel Find X

New Single Value Add to Dashboard

Time Range Use time picker Last 24 hours

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)

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=#

SSH Logs Dashboard

No description

Time Range

All time

Total SSH Events

Successful Logins

Failed Logins

Failed Logins by username

username
root
backup
alice
admin
test
john.doe
svc_user
conroo

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

Total SSH Events 1,200

Successful Logins 306

Failed Logins 3

Failed Logins by username

username
root
backup
alice
admin
test
john.doe
svc_user
service

Add Panel Find Add to Dashboard

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

Time Range Shared Time Picker (time_range)

Content Title Possible Brute Force by 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

Total SSH Events



Chart: 42



Successful Logins



Chart: 42



Failed Logins



Chart: 42



Invalid User Attempts



Chart: 42



1,200

306

305

286

No title



Chart:



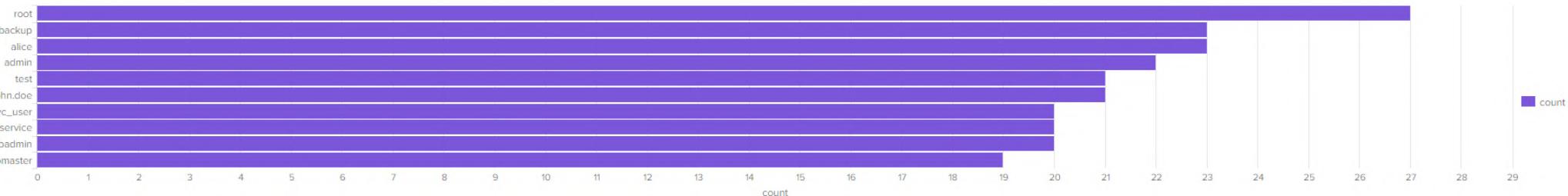
Failed Logins by username



Chart:



username



No title

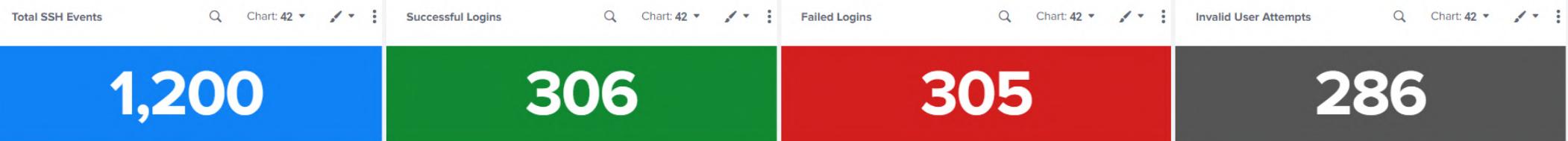


Chart: 42



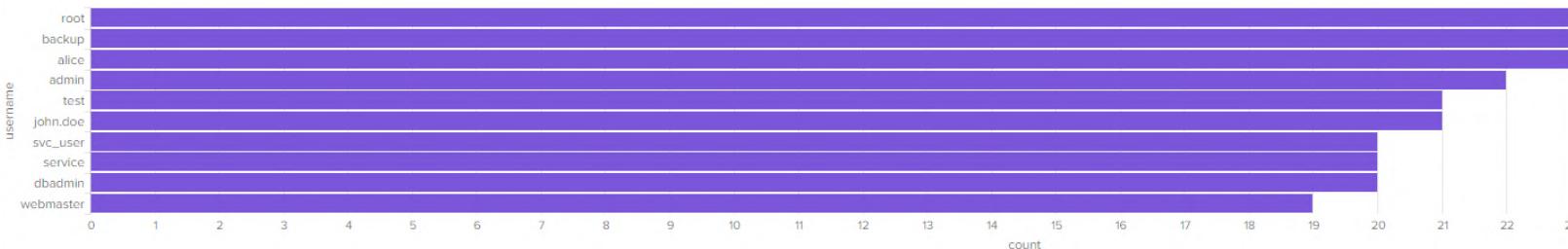
Possible Brute Force IP Address

83.195.24.226



No title

Failed Logins by username



Recommended

Splunk Visualizations

Find more visualizations [»](#)

Statistics Table

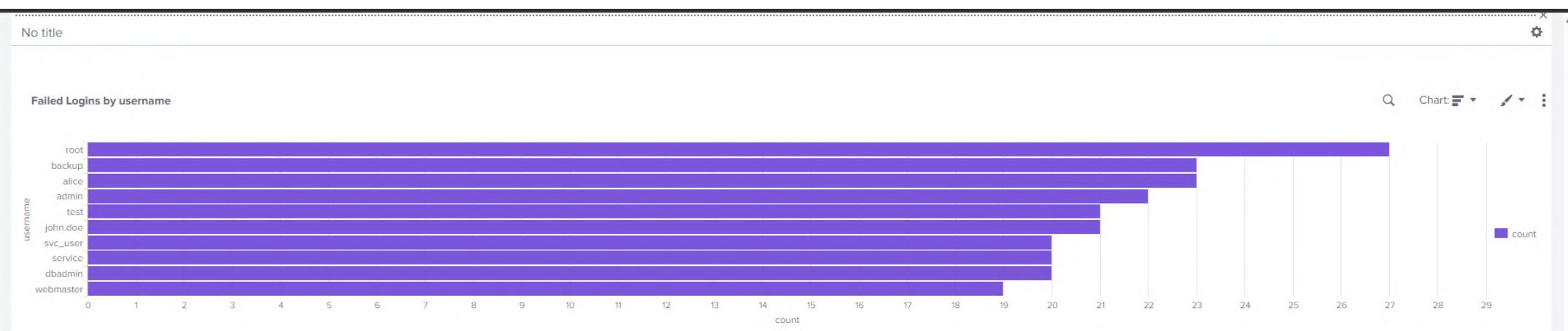
Show results organized in rows and columns.

No title

Possible Brute Force IP Address

83.195.24.226

Chart: 42



No title

Possible Brute Force by 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

splunk>enterprise Apps ▾

Administrator 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Search & Reporting

Search Analytics Datasets Reports Alerts Dashboards

Edit Dashboard UI Source + Add Panel + Add Input ▾ Dark Theme

Cancel Save as... Save

SSH Logs Dashboard

No description

Time Range Autorun dashboard

Total SSH Events: 1,200

Successful Logins: 306

Failed Logins: 305

Invalid User Attempts: 286

Failed Logins by username:

username	count
root	13
backup	13
alice	11
admin	10
test	10
john.doe	10
SVC_User	10
service	10

Possible Brute Force by 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

Splunk > enterprise Apps ▾

Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

SSH Logs Dashboard

Time Range All time Submit Hide Filters

Total SSH Events: 1,200

Successful Logins: 306

Failed Logins: 305

Invalid User Attempts: 286

Failed Logins by username

username	count
root	28
backup	24
alice	23
admin	22
test	21
john.doe	21
svc_user	20
service	20
dbadmin	20
webmaster	19

Possible Brute Force by 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
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 ▾

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 No title No title

Total SSH Events 1,200

Successful Logins 306

Failed Logins 3

No title No title

Failed Logins by username

username	count
root	1200
backup	100
alice	50
admin	80
test	70
john.doe	60

Possible Brute Force by IP Address

id.orig_h
83.195.24.226
25.47.52.197
191.47.156.160
52.173.49.103

Add Panel Find New Single Value

New (15) Add to Dashboard

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

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

Total SSH Events Successful Logins Failed Logins

1,200 306 3

Failed Logins by username

username	count
root	1200
backup	100
alice	80
admin	70
test	60
john.doe	50
svc_user	40
conrad	30

Possible Brute Force by IP Address

id.orig_h	count
83.195.24.226	1200
25.47.52.197	100
191.47.156.160	80
52.173.49.103	70

Add Panel

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 Single Value

Add to Dashboard

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 No title No title

Total SSH Events Successful Logins Failed Logins

Failed Logins by username

username	count
root	1200
backup	306
alice	3
admin	3
test	3
john.doe	3

Possible Brute Force by IP Address

id.orig_h
83.195.24.226
25.47.52.197
191.47.156.160
52.173.49.103

Add Panel

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

1,200**306****305****286**

No title

Failed Logins by username

username	count
root	27
backup	23
alice	23
admin	22
test	21
john.doe	21
svc_user	20
service	20
dbadmin	20
webmaster	19

Chart: Bar

No title

Possible Brute Force by 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
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

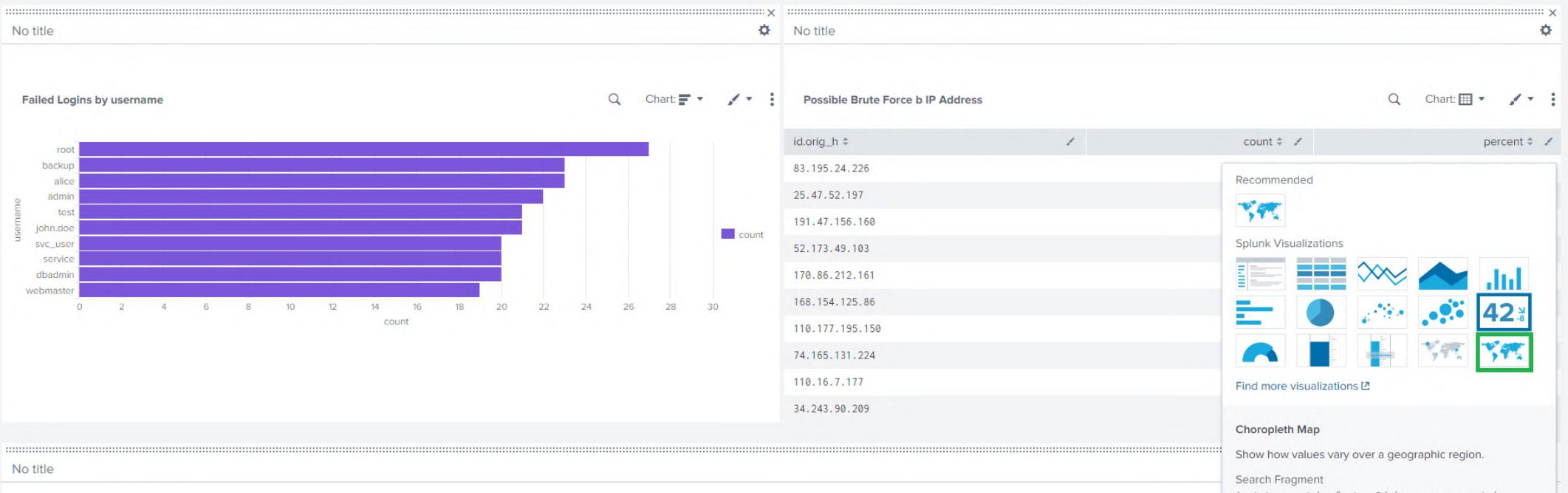
Chart: Table

No title

Brute Force attack with geo-location

Chart: 42

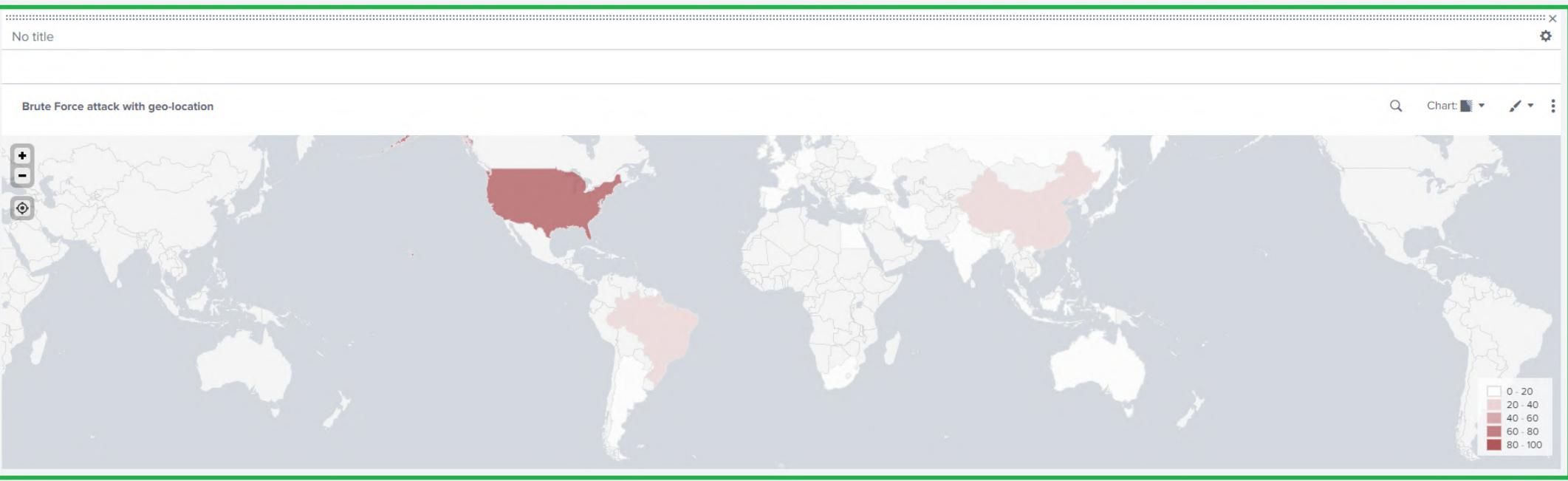
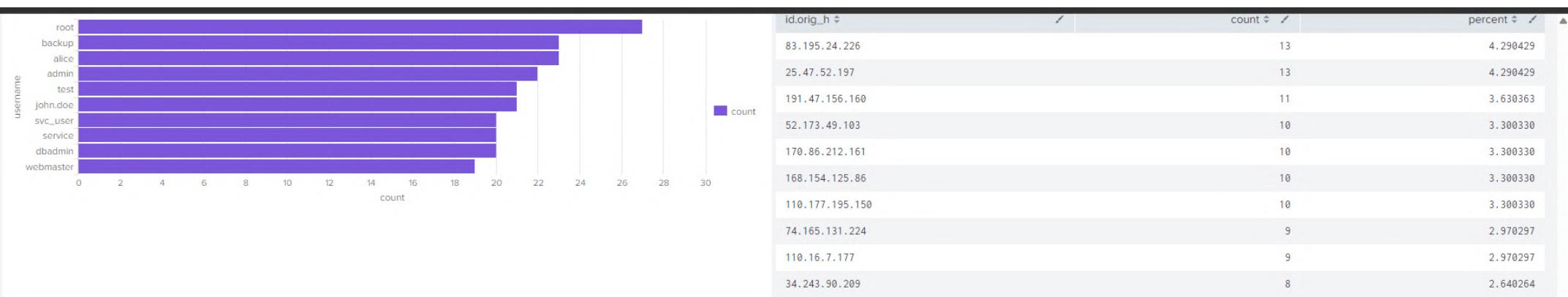
Argentina

1,200**306****305****286**

No title

Brute Force attack with geo-location

Argentina



Splunk > enterprise Apps ▾

Administrator 1 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 Autorun dashboard

All time

Total SSH Events Successful Logins Failed Logins Invalid User Attempts

1,200 306 305 286

Failed Logins by username

username	count
root	13
backup	13
alice	11
admin	10
test	10
john.doe	10
svc_user	10
coninc	10

Possible Brute Force by 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

