

STORMSHIELD



DASHBOARD & VISUALIZATION GUIDE

Version 2

Document last updated: July 4, 2024 Reference: sls-en_dashboard_visualization_gde



Table of contents

Change log	4
Getting started	5
All Dashboards	7
Creating a Dashboard	7
Nashboard Tunes	8
Dashboard Tools	۵
Adding a Widget	q
Editing a Widget	
Report	13
Change Repos	13
Auto Arrange	13
Sharing a Dashboard	13
Sharing a Dashboard from the Dashboard Page	
Sharing a Dashboard from Knowledge Base	
Using a Shared Dashboard	
Deleting a Shared Dashboard's Owner	16
Importing and Exporting Dashboards	16
Exporting Dashboards using Knowledge Base	
Importing a Dashboard using Knowledge Base	17
Customizable Drilldown from Dashboard Widgets	
Non-Empty Search from Widget	
Empty Search from Widget	22
Overview	26
System Health Dashboard	2b
SUL Uperation Dashboard	
Visualization	
Response Tupes in Visualization	29
Single Aggregation without Grouping	29
Single Aggregation with Grouping	29
Multiple Aggregation without Grouping	32
Multiple Aggregation with Grouping	34
Timechart Single Aggregation without Grouping	
Timechart Single Aggregation with Grouping	
Timechart Multiple Aggregation without Grouping	
Timechart Multiple Aggregation with Grouping	51
Features of Visualization	55
Area Chart	62
Response Types Supported	62
ATT&CK chart	64
Description	64
Grouping by Entities	64
Response Types Supported	67
Single Aggregation with Grouping	68
Bar Chart	
Response Types Supported	69
Bubble Chart	71







Rendering Parameters	74
Clustered Bar Chart	
Response Types Supported	
Clustered Column Chart	
Response Types Supported	
Clustered Line Chart	
Response Types Supported	
Column Chart	
Response Types Supported	
Dau/Hour Heatmap Chart	
Response Tupes Supported	87
Rendering Parameters	88
Displau Chart	89
Response Tupes Supported	89
Rendering Parameters	9'
Nonut Chart	q
Response Tupes Supported	Q?
Gauge Chart	Q
Response Tunes Supported	
Rendering Parameters	
Heatman Chart	
Pospopso Tupos Supported	
Line Chart	
Response Types Supported	
Parallel Coordinale Chart	
Response Types Supported	
Uperations	
Lompined Urill-down	
Radar chart	
Response Types Supported	
Sankey chart	
Response Types Supported	
Operations	
Stacked Area Chart	
Response Types Supported	
Stacked Column Chart	
Response Types Supported	
TreeMap Chart	
Response Types Supported	
Rendering Parameters	
Operations	
World Map Chart	
Response Types Supported	
Rendering Parameters	
Operations	
Drilldown from Search Visualization	
Common Features of Drill-down	
Demonstration of Customizable Drilldown from Search Visualization	
Special Drilldown Scenarios	
rther reading	





Change log

Date	Description
July 4, 2024	New document







Getting started

Welcome to the SLS version 2 Dashboard & Visualization Guide.

Dashboard is data visualization updated in real-time. SLS comes with two main, pre-configured dashboards: **All Dashboards** and **Overview**.

• All Dashboards allow you to create dynamic dashboards by adding multiple widgets. A widget can contain charts, tables, and graphs generated by a search query. A dashboard can also have diagrams, lists, and tables. If needed, you can change the widgets' height, width, and positioning.

All Dashboards start with **Quick Start**, from which you can easily access most of the features of SLS.



 Overview allows you to monitor your system operations and real-time cybersecurity incidents based on key measures, workflows, and behavioral patterns. This is a static dashboard that you cannot customize.



Page 5/146





SLS provides an array of visualization options including regular bar, line and column charts, various other statistical tools have been added. Charts are not only an aesthetically pleasing way to view search results, they also help make data analysis easier.

These options are available in:

- Search Interface
- Dashboards (Widgets)
- Search Templates

← васк fields ac	tion, log_ts, devic	e_ip, device_name			Use v	wizard All 👻 LAST 10 MINUTES 👻	SEARCH
Found 692 logs						🕄 Add Search To 🔻 🛛 🌟 More 🔻	Logs
Histogram In	terval: 20 seconds 📋	III Normal III Cumulative Sh	ow/Hide Trendline: 🗌	Container			Line 👻
35 36 37 38<							● ■ count()
L			Dec	ember 7, 2021			
				× .			_
Interesting Fields	0	action	log_ts		device_ip	device_name	
Select Fields	Add Fields 👻	reporting speed	2021/12/0	7 13:41:58	127.0.0.1	localhost	
Field	ev	reporting speed	2021/12/0	7 13:41:58	127.0.0.1	localhost	
Field	76	reporting speed	2021/12/0	7 13:41:58	127.0.0.1	localhost	Table
col_type	100	reporting speed	2021/12/0	7 13:41:58	127.0.0.1	localhost	
collected at	100	reporting speed	2021/12/0	7 13:41:58	127.0.0.1	localhost	
deutee te	100	reporting speed	2021/12/0	7 13:41:58	127.0.0.1	localhost	
device_ip	100	reporting speed	2021/12/0	7 13:41:48	127.0.0.1	localhost	
source_name	100	conacting anood	2021/12/0	7 10-41-40	127.0.0.1	lassilkast	
device name	100	« < 1 of 28 pages	> >>		Displaying 1-25 of 692 logs 👔	Display maximum: 25	 logs per page

In this document, Stormshield Log Supervisor is referred to in its short form SLS. Images used in this document are from the partner vendor's (Logpoint) software program. In your SLS, the graphics may vary but user experience is exactly the same.

Page 6/146



All Dashboards

All Dashboards allows you to design your own dashboards based on different analytics that provide an overview of SLS data. It displays data for a specified period of time and includes dashboards designed for different user roles. All Dashboards aggregates widgets from various sources so you can group different widgets as you would like to view them. All users can view All Dashboards. You don't need a SLS admin role.

The dashboard creates an overview of any data you wish to monitor regularly, enabling you to react faster to information.

Creating a Dashboard

- 11 Dashboards Ø All Dashboards Overview 0 QUICK START ø System Settings Repos Applications Α Configure the following settings: • LogPoint Name • DNS • NTP Q Import applications cont below: Create repo stored. IP Address
 SMTP
 SNMP Dashboard Package
 Label Package
 Plugins Þ on Package Normalization r
 Search Package
 Report Package It is possible to have more than one place to store Settings 5 Applications Repos ŵ Devices and Device Groups Users and Groups My Preferences 2 Configure the following for the devices: • Log Parsers • Fetchers • Device Groups Configure the following settings:
 Time zone
 Notification
 Date time display format
 Log fields to be shown on the search results Create users and groups: • Setup permissions based on permission groups • Assign permission groups to user groups • Add users to the user groups Parsers • Device Groups • Devices Permission Groups • User Groups • Users My Preferences Dashboards Reports Q Search When you import applications, they can contain dashboard packages. You can import these dashboards from the dashboard I You create your own dashboards by clicking the + tab next to the Quick Start tab Use reports templates to schedule and create ad-hoc reports in the following formats: PDF + HTML XLS + DocX Search after logs or tables in the system. The search results can be viewed in tabular form as well as in graphical charts and timecharts 0 Search • Quick Overview ¢ Reports Dashboards • Quick Overview 0 8 Ξ
- 1. Go to Dashboard from the navigation bar.

- 2. Click on All Dashboards.
- 3. Click +.





ADD DASHBOARD	
New	
My Dashboards	►
Vendor Dashboards	•
Used Dashboards	►
Shared Dashboards	►

- 4. Enter the Dashboard Name. You can also pull dashboards from the tabs on the left.
- 5. Click Ok.

Dashboard Types

All Dashboards list all the dashboards created in the SLS and display the information of the widgets in each dashboard.

At the top left, you can switch among **My Dashboards**, **Used Dashboards**, **Vendor Dashboards** and **Shared Dashboards** from the drop-down.

🗲 васк My Dashboa	rds				
MY DASHBOARD 👻 🛓 🖻	KPORT 🛓 IMPORT	MORE 🔻	0 SELECTED	Search	۲
My Dashboard	Widgets Info			Actions	
Used Dashboard Vendor Dashboard					0
Shared Dashboard					

11	6	Page 1	of 1	5	>>	C	Displaying 1 - 1 of 1 Page size:	25	+	
11		ruge 1	0.1	1	//	\sim	bibliopidying in the regeneration	23		

- My Dashboards: The ones created by you. You can **Clone**, **Share/Unshare**, **Lock/Unlock**, and **Delete** these dashboards from **Actions**.
- Used Dashboards: The ones you used.
- Shared Dashboards: The ones shared between users. Click the **Use** icon from **Actions** to use it.
- Vendor Dashboards: The ones included with SLS. Click the **Use** icon from **Actions** to use it. Click the **Clone** icon make a copy of the dashboard where you can apply changes.





Dashboard Tools

Adding a Widget

Widgets help you monitor logs in real-time. You can personally set up a widget and add it to a **Dashboard** of your choice. For example, if you want to monitor the firewall activities of devices, create a widget with the search queries related to the firewall.

- 1. Go to Dashboard from the navigation bar.
- 2. Click on All Dashboards. Select a Dashboard and click Add Widget.

QUICK START	DASHBOARD 2	+		
ADD WIDGET	🖹 REPORT 🛛 🎓 SH	ARE	CHANGE REPOS	AUTO ARRANGE

3. Enter a Name for the widget.

CREATE WIDGET - STEP 1									
Create your own custom dashboard widget.									
CREATE DASHBO	ARD WIDGET								
Name:	Widget 1								
Query:	chart count() by action						Select		
Repos:	For all repos from all LogPoint	ts 🔻	✓ Expose widget to pub	lic U	IRL?				
Description:	Newly Created Widget								
Time-range:	Day:		Hour:		Minute:				
	0	÷	1	÷	0		\$		
Cancel						Previous	Finish		

4. Enter a **Query**. Alternatively, click **Select** to choose any query from the **Advanced Query Picker**.





ADVANCED QUERY PIC	KER			8			
My Search History		My Search History	filter				
My Saved Searches	►	sent_datasize=* source_address=* chart max(sent_datasize), max(received_datasize) order by max(sent_datasize), max(received_datasize) desc limit 10	e) by source_addres	s			
Vendor Searches	•	chart count()					
	timechart count(), avg(datasize)						
Search Labels	•	chart max(sent_datasize), max(received_datasize)					
Live Searches	•	<pre>sent_datasize=* source_address=* chart max(sent_datasize), max(received_datasize) order by max(sent_datasize), max(received_datasize)</pre>	e) by source_addres	s			
		timechart count()					
		source_address=* chart count() by source_address					
		process geoip(destination_address) as country_name chart count() by country_name	ne, action, protocol				
		Selected Queries	1	Clear			
				-			
			Ok Cance				

If you choose the Advanced Query Picker, select a query from the lists.

- 5. Choose the **Repos** from where you want to generate the logs.
- 6. Select a Limit for the number of logs generate.
- 7. Select **Expose widget to public URL?** to share the widget publicly. When you share a widget with other users they don't need permission to view it.

1 NOTE

- The user the widget is shared with does not need the credentials to view the shared widget.
- If you selected **Expose widget to public URL?**, you now have the option to **Open public URL**. Click it opens the search results in a new window.



- 8. Provide a **Description** for the widget.
- 9. Select a Time Range for the logs in the repos.





🚺 NOTE

- You can set a time range in minutes, hours, or days..
- The maximum limit of the time range for the day field is 30.
- 10. Click Finish.

🚺 NOTE

If Data Privacy Module is enabled, Can Request Access users can only view encrypted data.

🕒 IMPORTANT

When configuring repos for a new dashboard, only select the relevant ones. Using a large number of repos impacts SLS performance.

Editing a Widget

At the top-right, click the Widget Options icon.



You can **Search** for the results, get **Info, Edit**, **Remove**, and open the widget in **Public URL**. You can also toggle the display of the **Legend** if there is one.

Additionally, You can create Alerts and Incidents.





You can also create and use graphs, including tables, area charts, line charts, bar charts, column charts, gauge charts, display charts, and donut charts. The type of graph you can use depends on the type of search results.

Tables

The following query:

| chart count() by action

Generates the following table:

Widget	Widget 1 - Table									
Q Search	🚺 Info 📝 Edit 🛛 Remove 🥥									
Q	udp,block-url	10								
Q	widget dimension edited	3								
Q	block-url	129								
Q	indexing speed	698								
Q	reset-server	145								
Q	reset-clinent	118								
Q	udp,reset-both	8								
Q	alert	119								
Column	Line Donut Area Bar Heatmap Radar Tr	reeMap World Map Table								

There are other graphs. Click on their link to learn more.

- Area Chart
- ATTCK chart
- Bar Chart
- Bubble Chart
- Clustered Bar Chart
- Clustered Column Chart
- Clustered Line Chart
- Column Chart
- Day/Hour Heatmap Chart
- Display Chart
- Donut Chart
- Gauge Chart
- Heatmap Chart
- Line Chart
- Parallel Coordinate chart
- Radar chart





- Sankey chart
- Stacked Area Chart
- Stacked Column Chart
- TreeMap Chart
- World Map Chart

Report

QUICK START	DASHBOARD 2	+		
ADD WIDGET	🖹 REPORT 🏓 SH	ARE	CHANGE REPOS	AUTO ARRANGE

You can use dashboards to generate reports. A report replicates the contents and data in a widget. You can't schedule or change a report's layout in a widget.

Change Repos

QUICK START	DASHBOARD 2	+		
ADD WIDGET	🖹 REPORT 🏾 🏓 SH	ARE	CHANGE REPOS	AUTO ARRANGE

You can change the **Repos** for log results of all the **Widgets** in the Dashboard.

Auto Arrange

QUICK START	DASHBOARD 2	+		
ADD WIDGET	🖹 REPORT 🛛 🏓 SH	IARE	CHANGE REPOS	AUT

You can manually change the sizes and position of widgets, you can also use Auto Arrange.

Sharing a Dashboard

You can share a dashboard from All Dashboards with different users and give them the read, edit, or full permissions. Any changes made in the dashboard are visible to all the shared users. However, auto-arranging or re-arranging a widget's size and position is reflected only on the current user's dashboard.

Sharing a Dashboard from the Dashboard Page

- 1. Go to Dashboard from the navigation bar.
- 2. Select the dashboard you want to share and click Share.

QUICK START	DASHBOARD 2	+		
ADD WIDGET	🖹 REPORT 🏓 SH	ARE	CHANGE REPOS	AUTO ARRANGE

- 3. Select a User Group. All the users in that user group are listed in the drop-down.
- 4. Select the **Read**, **Edit**, or **Full** permission for the users. Selecting the **Full** permission allows the user to read, edit, remove, and share the dashboard.





SHARE DASHBO	ARD			8
User Group:	User Account Administrator	LogPoint Admin	istrator 🙁	-
User Groups		Read	Edit	Full
🔻 🤱 User Acc	ount Administrator			
a johndo 🚨	e			
SHARE DASHBOARD User Group: User Account Administrato User Groups User Account Administrator Johndoe Janedoe LogPoint Administrator	e	v	\checkmark	
a LogPoint A	Administrator			
		Subr	nit	Cancel

5. Click Submit.

🚺 NOTE

- You can't share UEBA or vendor dashboards with other users.
- By default, a new user has the same permission as the user group they belong to.

Sharing a Dashboard from Knowledge Base

- 1. Go to Settings >> Knowledge Base from the navigation bar and click Dashboard.
- 2. Select My Dashboard from the drop-down.
- 3. Click the Share icon in the Actions column.

MY DASHBOARD * EXPORT IMPORT MORE * S.N. Name Widgets Info Image: Dashboard 1 widget_name: Widget 1 description: query: device_ip=127.0.0.1 display_type: chart repos: repos from 1 LogPoints time_range: last 1 hour public url: https://10.45.3.18/api/iframe/widget/5ff6e44a20e5e95186f45936?user=admin MORE *						
S.N. Name Widgets Info Image: 1 Dashboard 1 widget_name: Widget 1 description: query: device_ip=127.0.0.1 display_type: chart repos: repos from 1 LogPoints time_range: last 1 hour public url: https://10.45.3.18/api/iframe/widget/5ff6e44a20e5e95186/45936?user=admin	MORE	MOR	▼ 0 S	SELECTED	search	8
1 Dashboard 1 widget_name: Widget 1 description: query: device_ip=127.0.0.1 display_type: chart repos: repos from 1 LogPoints time_range: last 1 hour public url: https://10.45.3.18/api/iframe/widget/Sff6e44a20e5e95186/45936?user=admin					Actions	
widget_name: Widget 2 description: query: [chart count() by device_name display_type: chart repos: repos from 1 LogPoints time_rance_last 1 hour					2 	•

- 4. Select a User Group. All the users in that user group are listed in the drop-down.
- 5. Select the Read, Edit, or Full permission for the users.
- 6. Click Submit.





Using a Shared Dashboard

- 1. Go to Settings >> Knowledge Base from the navigation bar and click Dashboard.
- 2. Select Shared Dashboard from the drop-down.
- 3. Click the **Use** icon in the **Actions** column.

Shared Dashboards			
SHARED DASHBOARD 🔻 🛓 IMPORT		MORE 🔻 0 SELECTED	search 😒
S.N. Name	Widgets Info	User	Actions
1 Dashboard 1	widget_name: Widget 1 description: query: device_ip=127.0.0.1 display_type: chart repos: repos from 1 LogPoints time_range: last 1 hour	admin	• 2 ₪ 3

NOTE

- If a user does not have access to a repo used in a shared dashboard, the data displayed comes from repos they have access to.
- If only one repo is selected in the shared dashboard, and the user does not have access to the repo, the dashboard is empty.
- When a widget's graphs in a shared dashboard is changed by a user with the **Edit** or **Full** permission, the graphs are changed for all users. However, when a user with the Read permission changes a graph it only changes for them.

You can also use a shared dashboard from Add Dashboard.

- 1. Go to Dashboard from the navigation bar and click the + icon.
- 2. Select Shared Dashboards.
- 3. Select the dashboard you want to use and click Ok.

ADD DASHBOARD						8
New	•				Search	8
My Dashboards	•	SN	Name	Widget Cou	unt	
Vendor Dashboards	•	1	Jane_Dashboard	1		
Used Dashboards	•	2	Dashboard 3	1		
Shared Dashboards	Þ	3	Dashboard 2	1		
						Cancel

4. Choose Repos and click Ok.





Deleting a Shared Dashboard's Owner

- 1. Go to Settings >> User Accounts from the navigation bar and click Users.
- 2. De-activate the user by clicking the De-Activate User icon in the Actions column.
- 3. Click Manage De-Activated Users.
- 4. Click the Delete icon in the Actions column of the user.
- 5. Click Yes.

🚺 NOTE

You can do this using **Transfer Ownership** when you delete the user whose dashboard is being shared.

6. To transfer ownership, select a user from the drop-down and click Submit.

TRANSFER OWNERSHIP		⊗
Please re-assign or delete the foll	owing personalized items of the user(s)	
Username	Shared Item	Name
janedoe	Dashboards	Jane_Dashboard
ASSIGN TO USER		
admin		•
Delete		Submit Cancel

🚺 NOTE

The transferred dashboard is listed in My Dashboards of the new owner.

7. To delete the user and user's dashboard without transferring ownership, click Delete.

TRANSFER OWNERSHIP		8
Please re-assign or delete the following perso	onalized items of the user(s)	
Username	Shared Item	Name
janedoe	Dashboards	Jane_Dashboard
ASSIGN TO USER		
admin		-
Delete		Submit Cancel

Importing and Exporting Dashboards

In addition to importing and exporting dashboards, you can also clone, share, unshare, lock, unlock, and delete them using the icons in the Actions column or from the More drop-down at the top-right corner. Click Details for more information about the dashboard.





Exporting Dashboards using Knowledge Base

1. Go to Settings >> Knowledge Base from the navigation bar and click Dashboards.

€ ВА	ск Му	y Dashboards					
M	DASHB	oard 👻 🏦 e	XPORT 🛓 IMPORT	MORE 👻	1 SELECTED	Search	8
	S.N.	Name 👃	Widgets Info			Actions	
	1	dashboard_1	widget_name: widget1 description: query: chart count() display_type: chart repos: repos from 1 LogPoints time_range: last 1 hour public url: https://10.45.3.91/api/iframe/widget/5b504a81d8aaa42c1ad1505d?user=harry			₽ 001	ו î
	2	Quick Start					0
						0 (0 0 1	

- 2. Select the dashboards that you want to export.
- 3. Click EXPORT.
- 4. Save the .pak file as a backup or store in the computer system to use it in another SLS.

Importing a Dashboard using Knowledge Base

1. Go to Settings >> Knowledge Base from the navigation bar and click Dashboards.

€ В	аск М	y Dashboards					
М	Y DASHB	oard 👻 🏦 e	EXPORT	MORE 👻	0 SELECTED	Search	8
	S.N.	Name 👃	Widgets Info			Actions	
	1	dashboard_1	widget_name: widget1 description: query: chart count() display_type: chart repos: repos from 1 LogPoints time_range: last 1 hour public url: https://10.45.3.91/api/iframe/widget/5b504a81d8aaa42c1ad1505d?user=harry			40 0 1	f 🛅 🗊
	2	Quick Start					0
~	< P	age 1 of 1	> » B		Displaying 1 -	2 of 2 Page size:	25 💌

- 2. Click IMPORT.
- 3. Browse and upload the .pak file containing the dashboards to import.
- 4. Click Submit.



 You can drag and drop the widgets from one dashboard to another and must avoid dropping the widgets into a locked dashboard.

Page 17/146





Customizable Drilldown from Dashboard Widgets

Customizable drill-down options are available in dashboard widgets. You can get more information from your search queries. Using drill down in your dashboard widgets lets you look at specific details of query results.

For example, when viewing results that include the **destination_address**, **destination_port**, **source_address**, and **source_port** in the query you can drill down in each individual parameter.

Here are two scenario examples.

Non-Empty Search from Widget

A widget with the following search query:

```
destination address=* | timechart count() by destination port
```

Search from Widget									~				
Q	0	Ø	8	V L	egend								
Curre	nt sna	pshot	is for	2018/	/07/12 0	04:01:0	0 To 2	2018/	07/12	04:	11:00)	
destin	ation_a	addre	ss=* t	imech	art coun	t() by d	estina	tion_p	ort				
For <u>1</u>	<u>repo f</u>	rom '	<u>l Log</u> P	oint o	over the	last 10) minu	tes					
Clust	ered Line	a St	acked Co	olumn	Table								

The query results are displayed as a graph.





You can toggle between **edit** and **non-edit** mode. In edit mode, you can select the graph type, for example **Clustered Line Chart**, **Stacked Column Chart**, and **Tables**. In non-edit mode, you can drill down.







When you click on the highlighted result, you get the option to drill down one of the following specific parameters:

- Filter
- Drill down by
- Top 10 drill-down by







The Filter drilldown searches on Range, destination_port and count(). The Drilldown by and Top 10 drill-down searches for the destination_address.

The results of all three drilldown types can be opened and viewed in the same window or a new window. Enable **Range**.

Filter	Filter	
Range: 2018/07/12 05:09:00 To 2018/07/12 05:11:00	Range: 2018/07/12 05:09:00 To 2018/07/12 05:09:05	
destination_port: 80	destination_port: 80	
count(): 4	count(): 4	
View Logs	View Logs	
Drilldown by	Drilldown by	
destination_address	destination_address	
Top 10 drilldown by	Top 10 drilldown by	
destination_address	destination_address	

Enabled Time Range of 05:09:00 to 05:11:00

Disabled Time Range of 05:09:00 to 05:09:05

When drilling down on the **Range** value, the results opens on the same page.







	CK destination_address=* tim	echart count) by destination_port				SEARCH
) four	nd 30 loga			Add Search To +	± Mon ≠	Timechart
2 15 12 14	S accode		\times / \times	$\frown \land$	\bigwedge	Classes Lize S7845 rul S7845 rul S7 S7
0	508.97 AM 05.07.10 AM	MAN GOOD AM GOOD AM GOOD AM GOOD AM AN	OS 10 00 AM BS 10 10 AM	05.10.20 AM 05.10.20 AM 1	051240AM	
0	E GESTY AM CEGORIE CAM	destination post	05-1030 AM 05-102-10 AM		OS 10 KO AM	
0 -	5 05 59 АМ (55 09 10 АМ Тіттеязаттр ♥ № 2016/07/12 05:09:00	destination_port	22.1020 AM 22.12.13 AM	CE 1020AM 05:020AM 1	OS 10 AD AM	18402
0 -	COR.50 AM 05:00±0 AM Timestamp ▼ to 2018/07/12 05:09:00	SREDUM CONDUM CONTOUND CONDUM My 12, 201 destination_post	05.10.00 AM 05.10.13 AM (count)	0511020 AM 0511030 AM 1	05.15.40 AM	
0	Совозчан осол юлан Тіттевантр Ф № 2016/07/12 05:09:00	destination_port	ал 19 со 19 али (19 со 19 али (19 со 19 со 19 со 19 со (19 со)))) (19 со (19 со (19)		05.112.40 AM	
0	COLOTION COLOTION	NATION NATION AND AND AND AND AND AND AND AND AND AN	2 rount) 2 1	051020AM 8:1020AM 1	OS TED NO AM	
0	Тиневіатр Ф. 10 2016/07/12 205/96 20 10 2016/07/12 205/96 20 10 2016/07/12 205/96 10 10 2016/07/12 205/96 10	S (S)) AN (S (S)) AN (S (S + A)) (S (S)) AN Ar 17 (S) descination, gost	25 1020 AM 25 103 AM counti) 2 1	CE 11220 AM 25-10220 AM 1	CC 10-40 AM	
0	Титеваатр > 2016/07/12 05:09:00 > 2016/07/12 05:09:00 > 2016/07/12 05:09:00 > 2016/07/12 05:09:00	SERVICE SCRUDE SERVICE SCRUDE SERVICE SERVICE SERVICES SE	201030AM 251010AM 2 1 1	85 19 20 AM	CC 10-10 AM	
0	Timestamp Isosti to AA Immediate Isosti to AA	ENDINE CONTRACTOR CONTRACTOR AND CONTRACTOR Internation part 1,577	(5100144) (51001	211224 21224 I	CC 10-10 AM	
0	COST DATE COST DE LAS COST COST DE LAS COST DE LAS COST	Balan Balan Sarah Balan Balan Sarah Balan Sarah Balan Sarah Sarah Sarah Sarah Sarah Sarah Sarah Sarah Sarah Sar Anterester Jost 1577 168	00 100 MA 00 10 MM	8112544 8132344 I	CC 10 HO AM	

						SEARCH
@ Fex	and 3 logs				🔘 Add Search To 👻 🚖 More 👻	Tinschert
Interval	I: 5 seconds					Clustered Line 🗢
2						1573
1.8						
1.6						
1.4						
1.2						
		05:00:59 AM			05:09:00 AM	
			July 12, 2018			
	Timestemp	destination_port		count()		
Q	▼ 15 2018/07/12 05:09:0	00				
Q	- 🗈			2		
Q.	- 10	1,573		1		

Search Result for Enabled Time Range of 05:09:00 to 05:11:00

Search Result for Disabled Time Range of 05:09:00 to 05:09:05

When drilling down on **"destination_port"=138**, the results for the destination port opens in the same page.



When the drilling down is carried out on "count()"=3, the search results for the count open on the same page.

🗲 ВАСК	destination_address=* time	echart count() by destination_port filter "count()"=3		Use wiza	rd x /1 👻	2019/11/12 09:25:00 TO 2019/11.	/29 03:59:00 👻	SEARCH
Found	4,091 logs					🕜 Add Search To 🔻	🔺 More 🔻	Timechart
Interval: 1	3 hours							Clustered Line 🔻
3 2.5 2 1.5 1 0.5 0 Tu	ue 12 Wed 13 Thu 14	Fri 15 Sat 16 Sun 17 Mon 18 Tr.	ue 19 Wed 20 Thu 21 November 2019	Fri 22 Sat 23	Sun 24	Mon 25 Tue 26	Wed 27	 67 137 138 52808 Thu 28
			*					
	Timestamp	destination_port		count()				
Q	10	67						
Q		137		3				
Q	181	138						
Q	- 10	52,808						
Q	V b 2019/11/16 04:25:00							
Q	100	67						
Q	[10]	137						
Q	🖬	138						
Q	100	52,808						
Q	V b 2019/11/16 17:25:00							
Q	82	67						
Q	18	137						
Q	100	138						
-		50.000						





When drilling down on destination_address, the results open in the same page.

🗲 ВАСК	"destination_port"="2090"destination_address	=* chart count() by destination_address order by coun	nt() desc Use wizard	1/1 🔻	2018/07/12 05:09:00 TO 2018/07/12 05:11:00 👻	SEARCH
Found 1	logs				🚯 Add Search To 👻 🌟 More 👻	Chart
						Column 👻
						= count0
0.9						County
0.7						
0.5						
0.3						
0.1						
		10.233.1.72				
		^				
	destination_address	c	ount()			
0	10.233.1.72	1				

When drilling down on the destination_address, the results open in the same page.

🗲 ВАСК	"destination_port"="2090"destination_address	=* chart count() by destination_address order by count() o	desc Use wizard	1/1 🗢 2018/07/12 05:09:00 TO 2018/07/12 05:11:00 👻 🚺	
Found 1	logs			🕒 Add Search To 👻 🛛 🚖 More 👻 🛛 🕻	Chart
					Column 🔻
					count()
0.9					
0.7					
0.5					
0.3					
0.1					
		10.233.1.72			-
	destination_address	coun	t()		
Q	10.233.1.72	1			

Empty Search from Widget

This widget has no search query.

Page 22/146





CREATE WIDGE	T - STEP 1			•
Create your own cu	ustom dashboard widget.			
CREATE DASHBOAR	RD WIDGET			
Name:	Empty Search			
Query:				Select
Repos:	For 1 repo from 1 LogPoint 🛛 👻	Limit: 100 🗘 🗆 Exp	pose widget to public URL?	
Description:				
T:	Deve	Have	Minutes	
Time-range:	0	 nour: 1 		-
		•	•	
Cancel			Previous	Finish

A blank query looks like this.

Empty Search

2018/07/12 05:49:59
log_ts=2018/07/12 05:49:59 ~ device_ip=127.0.0.1 ~ device_name=localhost ~ col_type=syslog ~ repo_name=_logpoint ~ severity=3 ~ facility=7 ~ col_ts=2018/07/12 05:49:59 ~ collected_at=LogPoint ~ logpoint_name=LogPoint ~
<59> Jul 12 05:49:59 LP002.logpoint.net MSWinEventLog 2 Security 12994861 Wed Jul 15 12:08:26 2 015 4729 Microsoft-Windows-Security-
Auditing IMMUNE\bizsrv_Local_Administrators N/A Success Audit LP002.logpoint.net Security Group M anagement A member was removed from a security-enabled global group. Subject: Security ID: S-1-5-21- 469186442-1298088002-1541874228- 7946 Account Name: Jennifer Account Domain: IMMUNEDOMAIN Logon ID: 0xxt5r2pit Member: Security ID: S-1-5-21- 21-469186442-1298088002-1541874228- 1045 Account Name: CN=Chris Beagle,OU=Standard,OU=Users,OU=logpoint.net,DC=logpoint,DC=net Group: Security 1D: S-1-5-21-469186442-1298088002-1541874228- 12767 Group Name: bizsrv_Local_Administrators Group Domain: IMMUNEDOMAIN Additional Information: Privileges: - 12989566 12989566 12989566 12989566 12989566
2018/07/12 05:49:59

```
      log_ts=2018/07/12 05:49:59 v | device_ip=127.0.0.1 v | device_name=localhost v | col_type=syslog v | repo_name=_logpoint v

      col_ts=2018/07/12 05:49:59 v | collected_at=LogPoint v | logpoint_name=LogPoint v |

      <0>Jul 12 2018 05:49:59 %PIX|ASA-1-

      107001: RIP auth failed from IP_address: version=number, type=string, mode=string, sequence=number on interface interface __name
```

The results of a blank query are only the logs collected for the specified range of time, no graphs. You can refine the search query by clicking the on specific parts of the search results, for example key-value pair, or a raw log message. This starts a of search based on the selected parameter.

For example, if you click syslog:

Page 23/146





Empty Search

2018/07/12 05:49:59
log_ts=2018/07/12 05:49:59 \ device_ip=127.0.0.1 \ device_name=localhost \ col_type=syslog \ repo_name=_logpoint \ severity=3 \ facility=7 \ col_ts=2018/07/12 05:49:59 \ collected_at=LogPoint \ logpoint_name=LogPoint \
<59> Jul 12 05:49:59 LP002.logpoint.net MSWinEventLog 2 Security 12994861 Wed Jul 15 12:08:26 2 015 4729 Microsoft-Windows-Security-
Auditing IMMUNE\bizsrv_Local_Administrators N/A Success Audit LP002.logpoint.net Security Group M anagement A member was removed from a security-enabled global group. Subject: Security ID: S-1-5-21- 469186442-1298088002-1541874228- 7946 Account Name: Jennifer Account Domain: IMMUNEDOMAIN Logon ID: 0xxt5r2pit Member: Security ID: S-1-5- 21-469186442-1298088002-1541874228- 1045 Account Name: CN=Chris Beagle,OU=Standard,OU=Users,OU=logpoint.net,DC=logpoint,DC=net Group: Security ID: S-1-5-21-469186442-1298088002-1541874228- 12767 Group Name: bizsrv_Local_Administrators Group Domain: IMMUNEDOMAIN Additional Information: Privileges: - 12989566 12989566 12989566 12989566 12989566
2018/07/12 05:49:59
log_ts=2018/07/12 05:49:59 \ device_ip=127.0.0.1 \ device_name=localhost \ col_type=syslog \ repo_name=_logpoint \ col_ts=2018/07/12 05:49:59 \ collected_at=LogPoint \ logpoint_name=LogPoint \ l
<0>Jul 12 2018 05:49:59 %PIX ASA-1-

107001: RIP auth failed from IP_address: version=number, type=string, mode=string, sequence=number on interface interface __name

This opens the search result of the query "col_type"="syslog". The graph used depends on what you select.



Now you can drill down. When you hover a specific part of the search results, you can drill down to get more details.

Page 24/146





SLS - DASHBOARD & VISUALIZATION GUIDE - V 2 ALL DASHBOARDS

€ ВА	ck "col_type"="syslog"	Use wizard 1/1	▼ 2018/07/12 04:55:00 TO 2018/07/12 0	05:55:00 - SEARCH
🕑 Fou	nd 34,920 logs		🕜 Add Search To 👻	🚖 More 👻 Logs 📗
Histogr	am 📲 Interval: 2 minutes 🕍 Normal 📲 Cumulative Show/Hide Trendline:			Column 🔻
1.1K 900 700 500 300 100	D455 AM 05:00 AM 05:05 AM 05:10 AM 05:15 AM 05:20 AM 05:20 AM 05:20 AM 05:30 AM	07/12 05:25:00 и ам us:35 AM	05-40 AM 05-45 AM	© = count()
_				
Interesting Fields	2018/07/12 05:54:59 log_ts=2018/07/12 05:54:59 device_jp=127.0.1 \rightarrow device_name=localhost \rightarrow col_type=syslog \rightarrow repo_name=_logpoint \rightarrow sever logpoint_name=LogPoint \rightarrow <138-Jul 12 05:54:59 D014.logpoint.net MSWinEventLog 2 Security 27960415 Fri Jan 16 10:02:45 2015 Auditing IMMUNECSAMinistrator VIA Success Audit LP014.logpoint.net Security Group Management 49186442.1298088002.1541874228.13219 Account Name: James Account Domain: IMMUNEDOMAIN Logon ID: 0x17u3ep01 13054 Group Name: CSAdministrator Group Domain: IMMUNEDOMAIN Attributes: SAM Account Name: CSAdministrator SID 2018/07/12 05:54:59 log_ts=2018/07/12 05:54:59 \ device_jp=127.0.0.1 \rightarrow device_name=localhost \rightarrow col_type=syslog \rightarrow repo_name=_logpoint \rightarrow sever	ity=2 × facility=17 × cc 4754 Microsoft-Wir A security-enabled un Group: Security ID: S History: - Additional I	bl_ts=2018/07/12 05:54:59 v collected ndows-Security- iversal group was created. Subject: -1.5-21-469186442-1298088002-15411 Information: Privileges: - 279500 bl_ts=2018/07/12 05:54:59 v collected	Lat=LogPoint v Security ID: S-1-5-21- 874228- 998
	logpoint_name=LogPoint v		-	
	≪ < 1 of 38 pages > ≫	Displaying 1-25 of 939	logs () Display maximum: 25	
	Filter Range: 2018/07/12 05:25:00 To 2018/07/12 05:27:00 (0 0 7		
	count(): 1,162			
	View Logs			
	Drilldown by			
	col_type			
	Top 10 drilldown by			
	col_type			







Overview

Overview shows the same data for a specific and non-adjustable period from one place. It includes multiple dashboards for different personas, including a SOC manager, SOC analyst and SIEM engineer. It brings together widgets from various sources, aggregates their data and lets you manage how you want to view it. You need SLS admin permission to view Overview.

To view Overview:

- 1. Click Dashboard from the navigation bar.
- 2. By default, All Dashboards opens. Click Overview on the right of All Dashboards.

System Health Dashboard

The System Health dashboard monitors system components such as disk usage, memory usage, CPU usage, and messages per second events, providing administrators with a high-level system health overview. These system events can help you identify unusual patterns or activities, understand whether the system is running efficiently, and detect potential threats, malware, or malicious events early so you can take corrective actions.

The dashboard's widgets are:

Widget Name	Description
Disk Usage	The total number of gigabytes SLS is using to run programs and carry out tasks daily in the specified period. Disk usage relates to hard disk performance.
Memory Usage	The trend of memory (RAM) capacity SLS uses while running processes or tasks in the specified period. This helps admin users understand system capacity and make sure there is enough memory.
CPU Usage	The total percentage of processing power in use so an admin user can check system performance, health and speed.
Messages Per Second	SLS's scalability and capacity to handle a large volume of messages within a second. It can help admin users identify peak message rates and assess capacity.

Page 26/146







SOC Operation Dashboard

The SOC Operation dashboard is an overview of real-time cybersecurity incidents based on key measures, workflows, and behavioral patterns. The incident status/severity, cases status/severity and case response event data SLS provides is from daily activity during a specified period. You can use this dashboard to check SOC effectiveness and ensure all security operations including detections, analyses, and responses are running effectively.

Widget Description Name Incidents By Unresolved and resolved incident trend's accumulated data collected each day over a Status specified period so SOC managers can use to find the number of changed incident states. Incidents By The total number of accumulated incidents with severity (critical, high and medium) not closed daily in a specified period so a SOC manager can view risk trends associated with Severity incidents and adjust the incident threshold. Cases By The total number of accumulated cases with severity (critical, high and medium) not closed Severity daily in a specified period so SOC managers can see how case severity has changed and help them prioritize case work. Cases By The accumulated data on open and in progress cases trends for each day in a specified period. SOC managers can view the proportion of cases whose status changed and evaluate Status the current risk level. Automated The accumulated data of cases closed by playbooks (automated response) and cases Response vs closed by SOC analysts (manual response) monthly in the specified period to assess the Manual case resolution reliability of the playbook so SOC managers can track the efficiency of Response automation.

The dashboard's widgets are:



SLS - DASHBOARD & VISUALIZATION GUIDE - V 2 OVERVIEW







Page 28/146





Visualization

Response Types in Visualization

Altogether, there are eight response types for the representation of search results in the visualization. Four of them are the regular response types, and the other four response types are the same responses grouped into time buckets for a given time-range.

Single Aggregation without Grouping

The Single Aggregation without Grouping response type is used for aggregation of an individual parameter concerning a given aggregation parameter.

The general syntax for the Single Aggregation without Grouping is:

```
| chart aggregation parameter
```

This search query displays the value of the aggregation parameter over a specified range of time. The result of this response type can be represented in the form of :

Visualization Type	Sample Search Query
Display Chart	chart count()
Gauge Chart	chart count()

Single Aggregation with Grouping

The **Single Aggregation with Grouping** response type is used for aggregation of various grouping parameters concerning a given aggregation parameter. The general syntax for **Single Aggregation with Grouping** is:

```
| chart aggregation_parameter by grouping_parameter1, grouping_parameter2,
...., grouping_parametern
```

Example queries of Single Aggregation with Grouping are:

| chart count() by device name

```
| chart sum(datasize) by action, protocol
```

| chart avg(datasize) by type, protocol, device_ip

The response type displays the value of the aggregation parameter, grouped by all the grouping parameter(s) in the specified time range. The result of this query can be represented in the form of :

Visualization Type	Sample Search Query
Display Chart	chart count() by attack_category
Column Chart	severity=* chart count() by severity order by count() desc limit 5 $$
Line Chart	<pre>severity=* chart count() by severity</pre>



Visualization Type	Sample Search Query
Donut Chart	<pre>source_address=* chart count() by source_address</pre>
Area Chart	<pre>action=* source_address=* chart count() by action, source_ address</pre>
Bar Chart	<pre>severity=* chart count() by severity order by count() desc limit 5</pre>
Heatmap Chart	<pre>source_address=* action=* chart count() by source_address, action order by count() desc limit 10</pre>
Radar chart	<pre>service=* action=* chart count() by action, service</pre>
TreeMap Chart	<pre>source_address=* action=* chart count() by source_address, action order by count() desc limit 10</pre>
Parallel Coordinate Chart	<pre> process geoip(source_address) as source_country chart count() by source_country, sub_category, destination_location</pre>
Sankey chart	<pre> process geoip(source_address) as country chart count() by country, severity, category, sub_category</pre>
World Map Chart	<pre> process geoip(destination_address) as country_name chart count(), avg(datasize) by country_name, action</pre>
ATT&CK chart	chart count() by attack_id

General Operations for Single Aggregation with Grouping

This section contains the general operations applicable to all the charts belonging to the **Single Aggregation with Grouping** response type.

NOTE

Some charts might consist of operations that are relevant to the specific chart only. In that case, refer to the article of the particular chart.

Drill-down

In the Single Aggregation with Grouping response type, you can perform the drill-down specific value of the grouping or aggregation parameter.

When you hover over a component of a graph (including but not limited node, line, bar, point) a tooltip appears. The tooltip displays all the relevant information about the particular component.

Page 30/146







Click the component to open a new drill-down window. The window summarizes the information of the selected node along with the option to drill down as per your preference.

Filter	
action: allow	
protocol: udp	
count(): 22	
View Logs	
Drilldown by	
action	
protocol	
Top 10 drilldown by	
action	
protocol	

Click the corresponding **Open in a new window** icon to further drill down on any field. Additionally, you can view the search results for the selected set of data by clicking **View Logs** in the same window.

Page 31/146





♦ BACK	BACK action=* protocol=* chart count() by action, protocol search *action* = *allow* Use wizard All 👻 LAST 10 MINUTES 👻 SEARCH				
S Found	253 logs		6	Add Search To 👻 🌟 More 👻 Chart 📗	
				Column 🔻	
22				count()	
18					
14					
10					
6					
2					
		allow, udp			
	action	protocol	count()		
Q	allow	udp	22		

Multiple Aggregation without Grouping

The Multiple Aggregation without Grouping response type is used for aggregation of multiple aggregation parameters for all the available logs or the given repo and time range. An example of a search query for such response is:

| chart count(), avg(datasize)

This query displays the total count and the average of datasize of the logs collected in the specified range of time. The result of this query can be represented in the form of :

Visualization Type	Sample Search Query
Clustered Column Chart	<pre> chart max(sent_datasize), max(received_datasize)</pre>
Clustered Bar Chart	<pre> chart avg(sent_datasize), avg(received_datasize)</pre>
Display Chart	<pre> chart count(), max(datasize), avg(datasize)</pre>

General Operations for Multiple Aggregation without Grouping

Interactive Legend

In **Multiple Aggregation without Grouping**, when a chart is rendered, all selected aggregation parameters are displayed with a unique color for each aggregation parameter. However, you can choose to view the graphs concerning a specific aggregation parameter(s).

To hide an aggregation parameter, click the name of the parameter on the legend at the extreme right side of the container.







When you click a name of a parameter on the legend, the section referring to the respective parameter disappears, and a new chart is rendered consisting of all other aggregation parameters. You can unhide the parameter by clicking the legend again.



🚺 NOTE

The scale on the y-axis is auto-adjusted as per the value of the remaining aggregation parameter (s).

Drill down

Through the drill-down feature, you can choose to retrieve detailed results about a specific section of a chart. In Multiple Aggregation without Grouping response type, you can drill-down search operation over a specific value of aggregation parameter.

Hover over a component of a graph (example: node, line, bar, point) to view the tooltip. The tooltip displays all the relevant information about the particular component.

♦ BACK	chart max(sent_datasize), max(receiv	ved_datasize)		Use wizard 🛛 All 👻 LAST	10 MINUTES 👻 SEARCH
S Found	591 logs			Add Search To	🔻 🌟 More 💌 Chart 📗
					Clustered Column 👻
450 400 350 300 250 200 150 100 50				ter max(received_datasize): 429	■ max(sent_datasize) ■ max(received_datasize)
	max(sent_datasize)		~	max(received_datasize)	
0	453			429	

Click the segment to open a drill-down window. The window summarizes the related information of the selected section along with the option to drill down as per your preference.

Filter	
max(received_datasize): 449	
View Logs	C

Click the corresponding **Open in a new window** icon to further drill-down the search result from any field. Additionally, click the **View Logs** to view the search result for the selected set of data.







🚺 NOTE

The drill-down feature is not applicable for the Display format of Multiple Aggregations without Grouping response type.

Multiple Aggregation with Grouping

The Multiple Aggregation with Grouping response type is used for aggregation of grouping parameters concerning given multiple aggregation parameters.

The general syntax for Multiple Aggregation with Grouping is:

```
| chart aggregation_parameter1, aggregation_parameter2 by grouping_parameter1, grouping parameter2, ..., grouping parametern
```

Example queries of Multiple Aggregation with Grouping type are:

```
| chart count(), avg(datasize) by action
```

```
user=* | chart count(label=Fail) as Failed, count(label=Successful) as
Successful by user order by Failed desc limit 10
```

This query displays the count and average datasize of the collected logs in the specified time range grouped by the actions applied. The result of this query can be represented in the form of :

Visualization Type	Sample Search Query		
Clustered Column Chart	<pre>action=Allow or action=Deny chart count(action=allow) as AllowedConnection, count(action=deny) as DeniedConnection by source_address order by count(action=allow), count (action=deny) desc limit 10</pre>		
Clustered Bar Chart	<pre>action=Allow or action=Deny chart count(action=allow) as AllowedConnection, count(action=deny) as DeniedConnection by source_address order by count(action=allow), count (action=deny) desc limit 10</pre>		



Visualization Type	Sample Search Query
Clustered Line Chart	<pre>sent_datasize=* source_address=* chart max(sent_datasize), max(received_datasize) by source_address order by max(sent_ datasize), max(received_datasize) desc limit 10</pre>
Stacked Area Chart	<pre>sent_datasize=* source_address=* chart max(sent_datasize), max(received_datasize) by source_address order by max(sent_ datasize), max(received_datasize) desc limit 10</pre>
Radar chart	<pre>"norm_id"="WinDNSDHCP" chart count(lease_address=end), count (lease_address=start) by user</pre>
World Map Chart	<pre> process geoip(destination_address) as country_name chart count(), avg(datasize) by country_name, action</pre>
Bubble Chart	<pre> chart count(), max(sig_id) by action</pre>

General Operations for Multiple Aggregation with Grouping

This section contains the general operations that can be applied to all the charts belonging to the Multiple Aggregation with Grouping response type.

1 NOTE

Some charts might consist of operations that are relevant to the specific chart only. For such operations, refer to the section of the particular chart.

Interactive Legend

In the Multiple Aggregation with Grouping response type, when a chart is rendered, values of all the selected aggregation parameters are displayed with a unique color for each aggregation parameter. However, you can choose to view the graphs concerning specific aggregation parameter(s).

To hide an aggregation parameter, click the name of the parameter on the legend at the extreme right side of the container.

♦ BACK	action=Allow or action=Deny chart count(action=allow) as AllowedConnection, co	unt(action=deny) as DeniedConnection by source_addre	Use wizard All 👻 LAST 10 MINUTES 👻 SEARCH
S Found 7	7,604 logs		🚯 Add Search To 🔻 🛛 🚖 More 👻 🛛 Chart 📗
40 35 30 25 20 15 10 5	127.00.10 22.11.108.0 176.31.150.16 35.233.114.27 195.22.4	21 208.100.26.251 193.186.255.171 195.157.15.100	€utered Cohmertion ■ Dispection 95,140.229.147 157.122.84.205
	source_address	AllowedConnection	DeniedConnection
Q	127.0.0.10	34	40
Q	22.11.108.0	4	0
Q	176.31.150.16	3	0
Q	35.233.114.27	2	6
Q	195.22.4.21	2	1
Q	208.100.26.251	2	1
0	193.166.255.171	2	0 Displaying 1 - 10 of 10

Page 35/146





Click the name of a parameter on the legend, to hide its respective section. A new chart is rendered consisting of all other aggregation parameters. You can unhide the parameter by clicking the legend again.



🚺 NOTE

The scale on the y-axis is auto-adjusted as per value of the remaining aggregation parameter(s).

Drill-down

In the Multiple Aggregation with Grouping response type, you can drill-down search operation regarding a specific value of the grouping parameter concerning a single or multiple aggregation parameters.

Hover over a component of a graph (example: node, line, bar, point e.t.c) to view a tooltip. The tooltip displays all the relevant information about the particular component.

♦ BACK	action=Allow or action=Deny	chart count(action=allow) as Allow	edConnection, count(action=deny) as Denie	edConnection by source_addre	Use wizard	All 👻 LAST 10 MIN	UTES 🔻 SEARCH
S Found	7,604 logs				(Add Search To 👻 🤺	More 👻 Chart
40 35 30 25 20 15	li i						Clustered Column
10							
5	127.0.0.10 22.11.108.	0 176.31.150.16 35.233.11	source_address: 35.233.114.27 DeniedConnection: 6	193.166.255.171 195.157.15.100	95.140.229.147	157.122.62.205	
	source_address		AllowedConnection		DeniedConnecti	on	
Q	127.0.0.10		34		40		
Q	22.11.108.0		4		0		
Q	176.31.150.16		3		0		
Q	35.233.114.27		2		6		
Q	195.22.4.21		2		1		
Q	208.100.26.251		2		1		
0	193.166.255.171		2		0		
~ <	Page 1 of 1 > >> 2						Displaying 1 - 10 of 10

Click the segment to open a drill-down window. The window summarizes the related information of the selected section along with the option to drill down as per your preference.




Filter	
source_address: 35.233.114.27	
DeniedConnection: 6	
View Logs	
Drilldown by	
action	C
Top 10 drilldown by	
action	

Click the corresponding **Open in a new window** icon to further drill-down the search result from any field. Additionally, click the **View Logs** to view the search result for the selected set of data.

← BAC	K source_address="35.233.114.2	27" action=Allow or action=Deny chart count() by ac	tion order by count() desc	Use wizard	All 👻 LAST 10 MINUTES 👻	SEARCH
S Foun	d 8 logs			C) Add Search To 👻 🍵 📩 More 👻	Chart
						Column 🗢
						count()
5.5						
4.5						
3.5						
2.5						
1.5						
0.5						
		deny		allow		
			ă I			
	action		count()			
Q	deny		6			
0	allow		2			

Timechart Single Aggregation without Grouping

The Timechart Single Aggregation without Grouping response type is used for aggregation of processed logs to a given aggregation parameter grouped into time buckets (as a time series data) over a specified time range.

The general syntax for the Timechart Single Aggregation without Grouping is:

```
| timechart aggregation_parameter
```

Example queries of the Timechart Single Aggregation without Grouping type are:

```
| timechart count()
```

```
| timechart sum(datasize)
```

```
| timechart avg(datasize)
```

This response type displays the value of the aggregation parameter in the specified range of time. The charts that are used to visualize the queries belonging to this response type are : **Column, Line, Area, Day/Hour Heatmap**, and **Radar**





Visualization Type	Sample Search Query
Column Chart	timechart avg(datasize)
Line Chart	timechart avg(datasize)
Area Chart	timechart sum(datasize)
Radar chart	<pre>"norm_id"="WinDNSDHCP" timechart count(lease_ address=drop)</pre>
Day/Hour Heatmap Chart	timechart sum(datasize) as TotalDatasize every 1 hour

Additionally, the **Cumulative** chart option is also available along with the **Normal** chart for the **Column**, **Line**, and **Area** charts. The **Cumulative** option visualizes the results by accumulating data from the starting point to the current time-bucket for all time-buckets whereas the normal option visualizes the results as obtained from the query.

General Operations for Timechart Single Aggregation without Grouping

Drill-down

You can choose to view a detailed search for the response type regarding a specific value in two ways, i.e., from the line, or using a drag box.

Hover over a specific component/area of a chart to view a tool-tip. The tooltip displays all the information about the particular node.

♦ BACK	timechart avg(datasize)	Use wizard All 👻 LAST 10 MINUTES 👻 SEARCH
S Found	177,843 logs	🕒 Add Search To 💌 🔺 More 💌 Timechart
Interval: 1	rour Idd Normal and Cumulative Show/Hide Trendline:	Column 💌
1.2K 1K 800 600 400 200	08 AM 09 AM 10 AM 11 AM 12 PM 01 PM 02 PM 01 PM 02 PM 03 PM 04 segulatates: 646.15 July 11, 2018	
		Ä
	Timestamp	avg(datasize)
Q	2018/07/11 08:00:00	651.73
Q	2018/07/11 09:00:00	547.56
Q	2018/07/11 10:00:00	573.02
Q	2018/07/11 11:00:00	233.98
Q	2018/07/11 12:00:00	139.11
Q	2018/07/11 13:00:00	230.86
Q	2018/07/11 14:00:00	353.31
Q	2018/07/11 15:00:00	212.69
Q	2018/07/11 16:00:00	646.15
Q	2018/07/11 17:00:00	113.73
Q	2018/07/11 18:00:00	0
Q	2018/07/11 19:00:00	0.36
Q	2018/07/11 20:00:00	0

Click the component to open a drill-down window. The window summarizes the related information of the selected section along with the option to drill down as per your preference.

Page 38/146



2018/07/11 22:00:00

2018/07/11 23:00:00

Q

sls-en_dashboard_visualization_gde - 07/04/2024

1323.32

963.51



Filter	
Range: 2018/07/11 16:00:00 To 2018/07/11 17:00:00	O C
avg(datasize): 646.15	
ViewpLogs	C

Click the corresponding **Open in a new window** icon to further drill-down the search result from any field. Additionally, click the **View Logs** to view the search result for the selected set of data.



In addition to that, you can also drill down any chart of the response type using the drag box. Click and drag the mouse inside the graph, a yellow colored transparent drag box appears. You can drill-down the selected section of the chart by clicking the drill-down icon on the top-right corner of the box. You can resize or move the drag box as per your requirement.







€ BA	ск timechart	avg(datasize)							Use wizard All	 LAST 10 MINUTES 	SEARCH
🕑 Fou	nd 184 logs								Add Search T	o 👻 🄺 More 🤘	Timechart
Interval	: 10 seconds 🔤 📊	Normal _{atl} Cumulative	Show/Hide Trendlin	e:							Column 🔻
12K 10K 8K 6K 4K	I			Ð							avg(datasize)
2K											
Ĺ	03:56:00 AM	03:56:30 AM	03:57:00 AM	03:57:30 AM	03:58:00 AM	03:58:30 AM	03:59:00 AM	03:59:30 AM	04:00:00 AM	04:00:30 AM	
					July	12, 2018					
	T'										
	Timestamp							avg(datasize)			
Q	2018/07/12 0	3:56:01						0			
Q	2018/07/12 0	3:56:11						12818.97			
Q	2018/07/12 0	3:56:21						1721.94			
Q	2018/07/12 0	3:30:31						39.5			
Q	2018/07/12 0	3:30:41						0			
q	2018/07/12 0	2:57:01						0			
Q	2018/07/12 0	3-57-11						62			
9	2018/07/12 0	2.57.21						124			
Q	2018/07/12 0	3-57-31						0			
0	2018/07/12 0	3-57-41						0			
9	2018/07/12 0	3-57-51						0			
0	2018/07/12 0	3:58:01						0			
3	2018/07/12 0	3-58-11						62			
õ	2018/07/12 0	3:58:21						124			
~	20.0/0//12.0										

Cumulative chart

The Cumulative chart displays the accumulated data values throughout the given time range. To view the cumulative chart, click **Cumulative** on the left side of the container of a chart.

♦ BAC	κ timechart avg(datasize)	Use wizard All 👻 LAST 10 MINUTES 👻 SEARCH
S Foun	d 184 logs	🕼 Add Search To 💌 🌟 More 💌 🏾 Timechart
Interval:	10 seconds and Normal adjumulative Show/Hide Trendline:	Column 💌
12K		● ■ avg(datasize)
10K		
86		
OK AK		
48.		
2K		
	03:56:00 AM 03:56:30 AM 03:57:00 AM 03:57:30 AM 03:58:00 AM	03:58:30 AM 03:59:00 AM 03:59:30 AM 04:00:00 AM 04:00:30 AM
	L	uly 12, 2018
		Ä
	Timestamp	avg(datasize)
0	2018/07/12 03:56:01	0
Q	2018/07/12 03:56:11	12818.97
Q	2018/07/12 03:56:21	1721.94
Q	2018/07/12 03:56:31	39.5
Q	2018/07/12 03:56:41	0
Q	2018/07/12 03:56:51	0
Q	2018/07/12 03:57:01	0
Q	2018/07/12 03:57:11	62
Q	2018/07/12 03:57:21	124
Q	2018/07/12 03:57:31	0
Q	2018/07/12 03:57:41	0
Q	2018/07/12 03:57:51	0
Q	2018/07/12 03:58:01	0
Q	2018/07/12 03:58:11	62
Q	2018/07/12 03:58:21	124
Q	2018/07/12 03:58:31	0







Click Normal to view the regular chart.

Trendline

You can select the **Show/Hide Trendline** checkbox to identify whether the time-series data is likely to increase, decrease, or remain constant over a time period. The data on an increasing trend forms an upsloping line, whereas, on a decreasing trend, it forms a downsloping line. The **Show/Hide Trendline** checkbox is available for **Column**, **Line**, and **Area** charts of this response type only.

🚺 NOTE

The **Show/Hide Trendline** checkbox is also available for **Column**, **Line**, and **Area** charts resulted from Simple search queries and a blank search query.

♦ BACK	timechart avg(datasize)	Use wizard All 👻 LAST 10 MINUTES 👻 SEARCH
S Found	,035,450 logs	🔕 Add Search To 🔻 🛛 🚖 More 🔻 🛛 Timechart 📗
Interval: 1	ay 🔝 Normal 🔐 Cumulative Show/Hide Trendline: 🗹	Column 👻
120 100 80 60 40 20		avg(datasize)
0	4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 December 2019	25 26 27 28 29 30 31 1 2 January 2020
_		
	Timestamp	avg(datasize)
Q	2019/12/24 00:00:00	0
Q	2019/12/25 00:00:00	0
Q	2019/12/26 00:00:00	87.23
Q	2019/12/27 00:00:00	125.33
Q	2019/12/28 00:00:00	0
Q	2019/12/29 00:00:00	0
Q	2019/12/30 00:00:00	66.25
Q	2019/12/31 00:00:00	62.73
Q	2020/01/01 00:00:00	87.88
0	2020/01/02 00:00:00	0

Interactive Animation

The charts belonging to the **Timechart** response type include an interactive play button. The button allows you to slide through values of the charts concerning time buckets known as **Interval**.





Click **Play** on the right side of the container to start the animation. The graph is refreshed every four seconds, i.e., that graph shifts from one time-bucket to another time bucket every four seconds. Value of the time bucket is dependent upon the time-range specified in the **Interval**.

€ BA	ск timechart avg(datasize)	Use wizard All 👻 LAST 10 MINUTES 👻 SEA	RCH
🕑 Fou	and 184 logs	🔘 Add Search To 🔻 📋 📩 More 👻 📋 Timechart	
Interva	I: 10 seconds [dit] Normaldt] Cumulative Show/Hide Trendline: 🗌	1721 1107 ♥ TUDOVE PROVER	elumn 👻
_		Max: 12818.97	_
	Timestamp	avg(datasize)	
Q	2018/07/12 03:56:01	0	
Q	2018/07/12 03:56:11	12818.97	
Q	2018/07/12 03:56:21	1721.94	
Q	2018/07/12 03:56:31	39.5	
Q	2018/07/12 03:56:41	0	
Q	2018/07/12 03:56:51	0	
Q	2018/07/12 03:57:01	0	
Q	2018/07/12 03:57:11	62	
Q	2018/07/12 03:57:21	124	
Q	2018/07/12 03:57:31	0	
Q	2018/07/12 03:57:41	0	
Q	2018/07/12 03:57:51	0	
Q	2018/07/12 03:58:01	0	
Q	2018/07/12 03:58:11	62	
Q	2018/07/12 03:58:21	124	
-	2010/07/12 02-50-21	0	

You can also click Pause, Stop, Previous, Next, Replay as required.

🚺 NOTE

The operations Cumulative chart and Interactive Animation are not available for the Radar chart.

Timechart Single Aggregation with Grouping

The Timechart Single Aggregation with Grouping response type is used for aggregation of processed logs by an individual grouping parameter concerning given a single aggregation parameter grouped into time buckets (as a time series data) over a specified time range.

The general syntax for Timechart Single Aggregation with Grouping is:

```
| timechart aggregation_parameter by grouping_parameter1, grouping_
parameter2, ...., grouping_parametern
```

Example queries of Timechart Single Aggregation with Grouping type are:

| timechart count() by action

This query displays the count of the logs generated by the individual action, for an individual time bucket over a specified range of time. The result of this query can be represented in the form of :

Visualization Type	Sample Search Query				
Clustered Line Chart	<pre>event_category=* timechart count() by event_category</pre>				
Stacked Column Chart	<pre>source_address=* timechart count() by source_address</pre>				



General Operations for Timechart Single Aggregation with Grouping

This section contains the general operations that can be applied to all the charts belonging to the Timechart Single Aggregation with Grouping response type.

🚺 NOTE

Some charts might consist of operations that are relevant to the specific chart only. In this case, refer to the section of the particular chart.

Interactive Legend

In the Timechart Single Aggregation with Grouping response type, when a chart is rendered, all the aggregation values of the selected grouping parameter(s) are displayed with a unique color for each value of the grouping parameter(s). However, you can choose to view the graphs concerning a specific value of grouping parameter(s).

To hide the value of a grouping parameter, click the name of the parameter on the legend at the extreme right side of the container.



		· · · · · · · · · · · · · · · · · · ·	
	Timestamp	event_category	count()
Q	▼ ≥ 2018/07/12 06:05:00		
Q		TRAFFIC	339
Q		THREAT	372
Q		hrtimer	
Q	▼ 🗁 2018/07/12 06:20:00		
Q		TRAFFIC	70
Q		THREAT	63
Q		hrtimer	
Q	▼ 🗁 2018/07/12 06:35:00		
Q		TRAFFIC	
Q		THREAT	
Q		hrtimer	
Q	▼ 🗁 2018/07/12 06:50:00		
Q	- 10	TRAFFIC	248

When you click a name of a parameter on the legend, the section (line, bar) referring to the respective parameter disappears, and a new chart is rendered consisting all other values of the grouping parameter(s). Click the legend again to unhide the particular value.







06-15 AM 06-30 AM 06-45 AM 07-00 AM 07-15 AM 07-30 AM 07-35 AM 08:00 AM 08:15 AM 08:30 AM 08:45 AM 07:00 AM 07:15 AM 07:30 AM 10:15 AM 10:30 AM 10:45 AM 11:30 AM 11:

		ă I	
	Timestamp	event_category	count()
Q	▼ 🗁 2018/07/12 06:05:00		
Q	- 10	TRAFFIC	339
Q	📓	THREAT	372
Q		hrtimer	
Q	▼ ≥ 2018/07/12 06:20:00		
Q	🖬	TRAFFIC	70
Q	🖬	THREAT	63
Q		hrtimer	
Q	▼ ≥ 2018/07/12 06:35:00		
Q	🖬	TRAFFIC	
Q	- 10	THREAT	
Q		hrtimer	
Q	▼ ≥ 2018/07/12 06:50:00		
Q	- 10	TRAFFIC	248

🚺 NOTE

The scale on the y-axis is auto-adjusted as per the value of the remaining values of grouping parameter(s).

Drill-down

You can choose to view a detailed search for the response type regarding a specific value in two ways, i.e., from the line, or using a drag box.

Hover over a specific component/area of a chart to view a tool-tip. The tooltip displays all the information about the particular node.



Click the component to open a drill-down window. The window summarizes the related information of the selected section along with the option to drill down as per your preference.





Filter	
Range: 2018/07/11 20:00:00 To 2018/07/11 21:00:00	0 🛛
event_category: TRAFFIC	
count(): 340	
View Logs	
Drilldown by	
event_category	C
Top 10 drilldown by	
event_category	

Click the corresponding **Open in a new window** icon to further drill-down the search result from any field. Additionally, click the **View Logs** to view the search result for the selected set of data.

♦ BACK	timechart count("event_category" = "THREAT") as D	Dangerous, count("event_category"="TRAFFIC") as 1	Traffic	Use wizard All 👻 LAST 10 MINUTES 👻 SEARCH
S Found	340 logs			🖸 Add Search To 🔻 🔺 More 👻 Chart 📗
				Column 🗢
				■ count()
300				
250				
200				
150				
100				
50				
		TRAFFIC		
		^		
	event_category	c	count()	
Q	TRAFFIC	3	340	

In addition to that, you can also drill-down any chart of the response type using the drag box. Click and drag the mouse inside the graph, a yellow colored transparent drag box appears. You can drill-down the selected section of the chart by clicking the drill-down icon on the top-right corner of the box. You can resize or move the drag box as per your requirement.







- 18 **Interactive Animation**

Q

RPC

The charts belonging to the Timechart response type include an interactive Play button. It allows you to slide through values of the charts concerning time buckets known as Interval.

♦ BAC	<pre>event_category=* timechar</pre>	t count() by event_category		Use wizard All 👻 LAST 10 MINUTES 👻	SEARCH
S Found	17,071 logs			🕒 Add Search To 👻 🛛 🊖 More 👻 🛛 Tii	imechart
Interval: 8	l minutes				Clustered Line 👻
2018/0	77112(120:00)		*		8 • 8 •
	THRE	TAT	TRAFFIC	RPC	
			× ·		
	Timestamp	event_category	_	count()	
Q	▼ ≥ 2018/07/11 20:00:00				
Q	- 18	THREAT			
Q	- 18	TRAFFIC			
Q		RPC			
Q	▼ 🗁 2018/07/11 20:08:00				
Q	- 18	THREAT			
Q	- 18	TRAFFIC			
Q		RPC			
Q	▼ ► 2018/07/11 20:16:00				
Q	- 18	THREAT			
Q	-18	TRAFFIC			
0	- 88	RPC			

Click the **Play** on the right side of the container to start the animation. The graph is refreshed every four seconds, i.e., that graph shifts from one time-bucket to another time bucket every four seconds. Value of the time bucket is dependent upon the time-range specified in the Interval.

You can also click Pause, Stop, Previous, Next, Replay as required.

Timechart Multiple Aggregation without Grouping

The Timechart Multiple Aggregation without Grouping response type is used for aggregation of processed logs related to the given parameters. The logs are grouped into time buckets (as a





time series data) over a specified time-range.

The general syntax for Timechart Multiple Aggregation without Grouping is:

```
| timechart aggregation_parameter1, aggregation_parameter2, ....
aggregation parametern
```

Example queries of Timechart Multiple Aggregation without Grouping type are:

| timechart count(), avg(datasize)

This query displays the count of total logs generated and the average datasize of collected logs for individual time bucket over a specified range of time. The result of this query can be represented in the form of :**Clustered Column, Clustered Line, Radar**, and **Stacked Area** charts.

Visualization Type	Sample Search Query
Clustered Column Chart	<pre>norm_id=WinDNSDHCP timechart count(lease_address=drop) as Dropped, count(lease_address=start) as Started,count(lease_ address=end) as ENDED</pre>
Clustered Line Chart	<pre> timechart count("event_category" = "THREAT") as Dangerous, count("event_category" ="TRAFFIC") as Traffic</pre>
Radar chart	<pre>norm_id=WinDNSDHCP timechart count(lease_address=drop) as Dropped, count(lease_address=start) as Started, count(lease_ address=end) as ENDED</pre>
Stacked Area Chart	<pre>sent_datasize=* source_address=* chart max(sent_datasize), max(received_datasize) by source_address order by max(sent_ datasize), max(received_datasize) desc limit 10</pre>

General Operations of Timechart Multiple Aggregation without Grouping

This section contains the general operations that can be applied to all the charts belonging to the Timechart Multiple Aggregation without Grouping response type.

🚺 NOTE

Some charts might consist of operations that are relevant to the specific chart only. For such operations, refer to the section of the particular chart.

Interactive Legend

In the Timechart Multiple Aggregation without Grouping response type, when a chart is rendered, all the values of the selected aggregation parameter(s) are displayed with a unique color for each value of the aggregation parameter(s). However, you can view the graphs for specific aggregation parameter(s).

To hide an aggregation parameter, click the name of the parameter on the legend at the extreme right side of the container.

Page 47/146



sls-en_dashboard_visualization_gde - 07/04/2024



€ ВАСК	timechart co	ount("event_cate	gory" = "THRE	EAT") as Dangero	us, count("even	it_category"="TRAF	FIC") as Traffi	c		Use wiza	rd All 👻 LAST	T 10 MINUTES 👻	SEARCH
S Found 2	210,466 logs									0	Add Search To 👻	🜟 More 👻	Timechart
Interval: 15	minutes											c	lustered Column 👻
450					1.1.1.1							۲	Dangerous
400				. IL.	11								Traffic
350				16 H.	H. Le								
250		U. 18											
150							_		le		_		
50			11 B.			de la l	1 I.	de la	11 D.	te te	le le	lt le	
	05:30 AM	06:00 AM	06:30 AM	07:00 AM	07:30 AM	08:00 AM	08:30 AM	09:00 AM	09:30 AM	10:00 AM	10:30 AM	11:00 AM	1
						July 12, 20	18						_
							Â						
	Timestamp						Dangero	us		Traffic			
Q	2018/07/12 05:2	6:58					0			0			
Q	2018/07/12 05:4	1:58					0			0			
Q	2018/07/12 05:5	6:58					359			355			
Q	2018/07/12 06:1	1:58					255			258			
Q	2018/07/12 06:2	6:58					0			0			
Q	2018/07/12 06:4	1:58					81			64			
Q	2018/07/12 06:5	1,58					385			337			
0	2018/07/12 07:2	6:58					502			426			
0	2018/07/12 07:4	1:58					358			311			
õ	2018/07/12 07:5	6:58					114			85			
Q	2018/07/12 08:1	1:58					104			89			
Q	2018/07/12 08:2	6:58					102			100			
Q	2018/07/12 08:4	1:58					130			94			
Q	2018/07/12 08:5	6:58					126			87			
0	2018/07/12 09:1	1:58					111			77			

When you click a name of a parameter on the legend, the section (line, column, bar) referring to the respective parameter disappears, and a new chart is rendered consisting all other aggregation parameters (s). Click the legend again to unhide the value.



🚺 NOTE

The scale on the y-axis is auto-adjusted as per the value of the remaining aggregation parameter (s).

Drill-down

You can choose to view a detailed search for the response type regarding a specific value in two ways, i.e., from the line, or using a drag box.

Hover over a specific component/area of a chart to view a tool-tip. The tooltip displays all the information about the particular node.





♦ BACK	timechart co	unt("event_cate	gory" = "THREA	AT") as Dangerou	s, count("event_	_category"="TRAFFIC) as Traffic			Use w	izard All 👻 LAS	T 10 MINUTES 👻	SEARCH
S Found 2	210,466 logs									(🕽 Add Search To 👻	🔺 More 👻	Timechart
Interval: 15	minutes												Clustered Column 👻
450 350 250 150 50	05:30 AM	06:00 AM	06:30 AM	07:00 AM	timestan Traffic: 07:30 AM	np: 2018/07/12 07:26:58 436 08:00 AM July 12, 2018	08:30 AM	09:00 AM	09:30 AM	10:00 AM	10:30 AM	11:00 AM	Dangerous Traffic
						*							
	Timestamp						Dangero	IS		Traf	fic		
Q	2018/07/12 05:20	6:58					0			0			
Q	2018/07/12 05:4	1:58					0			0			
Q	2018/07/12 05:5	6:58					359			355			
Q	2018/07/12 06:1	1:58					255			258			
Q	2018/07/12 06:20	6:58					0			0			
Q	2018/07/12 06:4	1:58					295			04			
0	2018/07/12 07:1	1:58					497			428			
0	2018/07/12 07:20	6:58					502			436			
õ	2018/07/12 07:4	1:58					358			311			
Q	2018/07/12 07:5	6:58					114			85			
Q	2018/07/12 08:1	1:58					104			89			
Q	2018/07/12 08:20	6:58					102			100			
Q	2018/07/12 08:4	1:58					130			94			
Q	2018/07/12 08:5	6:58					126			87			
0	2019/07/12 00:1	1.69					111			77			

Click the component to open a drill-down window. The window summarizes the related information of the selected section along with the option to drill down as per your preference.

Filter	
Range: 2018/07/12 07:26:58 To 2018/07/12 07:41:58	02
Traffic: 436	
View Logs	C

Click the corresponding **Open in a new window** icon to further drill-down the search result from any field. Additionally, click the **View Logs** to view the search result for the selected set of data.







In addition to that, you can also drill-down any chart of the response type using the drag box. Click and drag the mouse inside the graph, a yellow colored transparent drag box appears. You can drill-down the selected section of the chart by clicking the drill-down icon at the top-right corner of the box. You can resize or move the drag box as per your requirement.



Interactive Animation

The charts belonging to the **Timechart** response type include an interactive play button. It allows you to slide through values of the charts concerning time buckets known as **Interval**.



Click **Play** on the right side of the container to start the animation. The graph is refreshed every four seconds, i.e., that graph shifts from one time-bucket to another time bucket every four seconds. Value of the time bucket is dependent upon the time-range specified in the **Interval**.

You can also click Pause, Stop, Previous, Next, Replay as required.





Timechart Multiple Aggregation with Grouping

The Timechart Multiple Aggregation with Grouping response type is used for aggregation of an individual grouping parameter for given multiple aggregation parameters grouped into time buckets over a specified time range.

The general syntax for Timechart Multiple Aggregation without Grouping is:

```
| timechart aggregation_parameter1, aggregation_parameter2, ....,
aggregation_parametern by grouping_parameter1, grouping_parameter2, ....,
grouping_parametern
```

An example of a search query for the response is:

```
"norm_id"="WinDNSDHCP" | timechart count("description" = "THREAT") as
Dangerous, count("description" = "TRAFFIC") as Traffic by lease address
```



The result of this query can be represented in the form of : Clustered Column and Bubble charts.

Visualization Type	Sample Search Query
Clustered Column Chart	<pre>norm_id=WinDNSDHCP timechart count(lease_address=drop) as Dropped, count(lease_address=start) as Started,count(lease_ address=end) as ENDED</pre>
Bubble Chart	<pre> timechart count(), avg(sig_id), max(datasize), distinct_ count(sig_id) by status_code</pre>

General operations for Timechart Multiple Aggregation with Grouping

Drill-down

Like in the search results of other responses, when you hover on any section (here, any count () or avg(doable_mps)), the selected section is highlighted, and the information for the selected section is as shown in the tooltip.





♦ BACK	"norm_id"="WinDNSDHCP	" timechart count("description"=	"THREAT") as Dangerous,	count("description"="TRAFFIC";) as Traffic by lease Use wiza	All 👻 LAST 10 MINUT	SEARCH
Found	295 logs					🗂 Add Search To 🔻 🛛 🛨 More	Timechart
Interval: 2	minutes						Chustered Column -
Dangero Traffic	NUS 7 6 5 4 3 2 1 07:50 AM	07:55 AM 08:00 AM 0	ROS AM OR: 10 AM	08:15 AM July 12. Traffic: 6	8/07/12 08:16:52 08:30 AM	08:35 AM 06:40 AM	College Count
				Ä			
	Timestamp	lease_address		Dangerous	Traf	fic	
Q	2018/07/12 07:48:52						
Q	16	end					
Q	16	start			2		
Q	- E	drop			2		
Q	- 10	deny			4		
Q		url					
Q							
Q		enu			2		
Q		drop			2		
30		deny			1		
0		url					
0	2018/07/12 07:52:52						
Q	- 10	end			1		

Click the component to open a drill-down window. The window summarizes the related information of the selected section along with the option to drill down as per your preference.

Filter		
Range: 2018/07/12 08:16:52 To 2018/07/12 08:18:52	\bigcirc	
lease_address: end		
Traffic: 6		
View Logs		
Drilldown by		
norm_id		
Top 10 drilldown by		
norm_id		

Click the corresponding **Open in a new window** icon to further drill-down the search result from any field. Additionally, click the **View Logs** to view the search result for the selected set of data.





sls-en_dashboard_visualization_gde - 07/04/2024



♦ BACK	"norm_id"="WinDNSDHCf	• timechart cou	Int("description	"="THREAT") a	s Dangerous,	count("description"	="TRAFFIC")	as Traffic by lease	Use wizard	All	LAST 10 MINUTES	SEARCH
S Found	13 logs									C Add Search To	v v m m m m m m m m m m m m m m m m m m	Timechart
Interval: 5	seconds											Clustered Column 👻
 Dangeroi 	us											end
 Traffic 	1.8											start drop
	1.4											deny
	0.6											
	0.2											
	08:16:30 AM	08:16:40 AM	08:16:50 AM	08:17:00 AM	08:17:10 AM	08:17:20 AM July 12, 2018	08:17:30 AM	08:17:40 AM	08:17:50 AM	08:18:00 AM	08:18:10 AM	
						, A						
	Timestamp	lease_address				Dangerous			Traffic			
Q	▼ ≥ 2018/07/12 08:16:28											
Q	10	end										
Q	18	start										
Q	- 10	drop										
Q	- 60	deny										
Q	✓											
Q	- 16	end										
0	- 60	drop										
0	- B)	denv										
0	2018/07/12 08:16:38											
Q	- 10	end										
Q	- 10	start										
Q	- 18	drop										

In addition to that, you can also drill-down any chart of the response type using the drag box. Click and drag the mouse inside the graph, a yellow colored transparent drag box appears. You can drill-down the selected section of the chart by clicking the drill-down icon on the top-right corner of the box. You can resize or move the drag box as per your requirement.



Interactive Legend

For the responses of **Timechart Multiple Aggregation with Grouping**, the legend is displayed on either side of the search graph. The aggregation parameter(s) is shown on the left-hand side whereas the grouping parameter is shown on the right-hand side.

An important thing to note here is that at an instant, the result of only one of the grouping parameters is displayed. Moreover, only the legends of the grouping parameter (on the right) are interactive. The legends of aggregation parameters (on the left) are not interactive.





♦ ВАСК	"norm_id"="WinDNSDHCP	<pre>" timechart count("description"="THR")</pre>	EAT") as Dangerous, co	unt("description"="TRAFFIC") as Traffic by I	ease Use wizard	All 👻 LAST 10 MINUTES 👻 SEARCH
S Found	145 logs					🕼 Add Search To 👻 🛛 🌟 More 👻 🗌 Timechart 🏢
Interval: 1	minute					Clustered Column 👻
- D						
 Traffic 	0.9					drop start
						deny
	0.7					69
	0.5					
	0.3					
	0.1					
	08:23 AM 08:25 AM	08:30 AM	08:35 AM	08:40 AM	08:45 AM	08:50 AM
				July 12, 2018		
				Â		
	Timestamp	lease_address	t	Dangerous	Traffic	
Q	▼ ≥ 2018/07/12 08:24:08					
Q		end				
Q		drop				
Q		start			1	
Q	- 60	url				
0	 2018/07/12 08:25:08 	63.1				
Q		end				
Q	16	drop				
Q	18	start			1	
Q	68	deny				
Q		url	1			
Q	▼ № 2018/07/12 08:26:08					
Q	- 66	end			1	

Interactive Animation

The charts belonging to the **Timechart** response type include an interactive Play button. It allows you to slide through values of the charts concerning time buckets known as **Interval**.

♦ BACK	"norm_id"="WinDNSDHCP	" timechart count("description"="THREAT	") as Dangerous, count("description"="TRAFFIC")	as Traffic by lease Use wizard	All 👻 LAST 10 MINUTES 👻 SEARCH
S Found	145 logs				😋 Add Search To 👻 🌟 More 👻 Timechart 🏢
Interval: 1	minute				Clustered Column 👻
• Dangero • Traffic	US 0.9 0.7 0.5 0.3 0.3 0.3 0.3 0.2 0.23 AM 08:25 AM	0630 AM	08:35 AM 08:40 AM July 12, 2018	0845 AM	€ end drop start deny ∎ uri 0850 AM
			*		
	Timestamp	lease_address	Dangerous	Traffic	
Q	▼ ≥ 2018/07/12 08:24:08				
Q	- 16	end			
Q	- 16	drop			
Q		start		1	
Q	- 10	deny			
Q	- 10	url			
Q	▼ ≥ 2018/07/12 08:25:08				
Q	- 16	end			
Q	- 16	drop			
Q	R	etart		1	
0		3(8)(
Q		deny			
Q		deny url	1		
α α α	Image: Second secon	deny url	1		

Click the **Play** on the right side of the container to start the animation. The graph is refreshed every four seconds, i.e., that graph shifts from one time-bucket to another time bucket every four seconds. Value of the time bucket is dependent upon the time-range specified in the **Interval**.

You can also click Pause, Stop, Previous, Next, Replay as required.





Features of Visualization

Some features of the new visualization of search graphs are provided below:

The legend for the search results is interactive in multiple ways.

You can toggle the display of the legend as **ON** and **OFF**. Click the desired legend to hide/unhide it. For example,



Click the legend of **count()** to hide its corresponding result.



Click the legend of **avg(datasize)** to hide its corresponding result.

Page 55/146



sls-en_dashboard_visualization_gde - 07/04/2024





The status of the legend (either ON or OFF) is saved for the result which is dynamically populated in the widgets in the dashboards.

All the related data can be highlighted at once by hovering over the legend. If you hover the mouse over the legend of **count()** then all the data of average is highlighted.



Q	2018/07/10 02:38:59	68
Q	2018/07/10 02:39:19	64
Q	2018/07/10 02:39:39	69
Q	2018/07/10 02:39:59	77
Q	2018/07/10 02:40:19	57
Q	2018/07/10 02:40:39	70
Q	2018/07/10 02:40:59	73
Q	2018/07/10 02:41:19	53
Q	2018/07/10 02:41:39	72
Q	2018/07/10 02:41:59	69

The Pan and Zoom feature in the axes is provided for better visibility of the results.

Pan is the ability to click and drag the cursor over the search result visualization to select the desired area. With this feature, the axes can be moved to cover a larger area of the timespan of the search result.

Consider the following search result:





0

-280

-1171

-1162

Displaying 1 - 25 of 30



Q	2018/07/07 04:00:00
Q	2018/07/07 10:00:00

« < Page 1 of 2 > > 3

2018/07/06 22:00:00

Q

Q 0

If you click and drag the y-axis, it is displayed as in the following screenshot:



0

1.03

1.32

70.25

July 4, 2018 July 5, 2018 July 6, 2018 July 7, 2018 July 3, 2018 July 8, 2018 July 9, 2018

	· · · · · · · · · · · · · · · · · · ·		
	Timestamp	average	difference
Q	2018/07/03 04:00:00	667.37	2128
Q	2018/07/03 10:00:00	2.08	2884
Q	2018/07/03 16:00:00	0	0
Q	2018/07/03 22:00:00	0.44	-272
Q	2018/07/04 04:00:00	581.18	903
Q	2018/07/04 10:00:00	24.2	2190
Q	2018/07/04 16:00:00	0	0
Q	2018/07/04 22:00:00	322.39	-214
Q	2018/07/05 04:00:00	225.56	260
Q	2018/07/05 10:00:00	172.59	618
Q	2018/07/05 16:00:00	0	0
Q	2018/07/05 22:00:00	272.44	-197
Q	2018/07/06 04:00:00	523.34	121
Q	2018/07/06 10:00:00	167.83	4112
Q	2018/07/06 16:00:00	0	0
Q	2018/07/06 22:00:00	1.03	-280
Q	2018/07/07 04:00:00	1.32	-1171
Q	2018/07/07 10:00:00	70.25	-1162
~ <	Page 1 of 2 >>> C		Displaying 1 - 25 of 30

Zoom is the ability to expand and shrink the scale of the axis. With this feature, the scale of the axes can be zoomed in and out for better visibility of the search results.





Consider the following search result:



If the you zoom over the axes individually, it is displayed as in the following screenshot:

♦ BACK	timechart count()	Use wizard All 👻 LAST 10 MINUTES 👻 SEARCH
S Found	639 logs	🔘 Add Search To 👻 🛛 🔺 More 👻 🗌 Timechart 📗
Interval: 2) seconds 🔄 📶 Normal 🔄 📶 Cumulati Show/Hide Trendline: 🗌	Line 🔻
35 30 25 20 15 10 5		
	23:58 AM 02:59 AM 04:00 AM 04:01 AM 04:02 AM 04:03 AM 04:04 AM July 10, 2018	04:05 AM 04:06 AM 04:07 AM
	Timestamp	count()
Q	2018/07/10 04:00:50	21
Q	2018/07/10 04:01:10	31
Q	2018/07/10 04:01:30	10
Q	2018/07/10 04:01:50	18
Q	2018/07/10 04:02:10	26
Q	2018/07/10 04:02:30	16
Q	2018/07/10 04:02:50	15
Q	2018/07/10 04:03:10	18
Q	2018/07/10 04:03:30	21
Q	2018/07/10 04:03:50	18
\ll $<$	Page 1 of 2 >>> C	Displaying 1 - 25 of 30

In the Timechart responses, a new feature called "Drilldown via Drag Box" has been introduced.

If you click and drag the mouse inside the container, a transparent drag box appears. This drag box is movable and resizable.

Page 58/146







The main purpose of the drag box is to further drill-down within a custom time-range which is a subset of the previous time-range. Once the desired vicinity of the drag box is set, click the drill-down icon. This displays the search results of the particular time-frame tapped by the drag box.

The axes label auto-adjusts as per the size of the container.

This feature is especially useful for dashboards with many widgets where the size of a widget is user-configurable. Whenever you resize a widget or click the **Auto-arrange** option, the labels of both the axes auto-adjust as per the space occupied by the search graph whenever applicable.

Consider the third widget (Multiple Aggregation with Grouping) of the following dashboard:



For the same dashboard, if the widget's size is increased, the labels of the axes are autoadjusted.







The legend's text auto adjusts as per the widget's dimension.

When the container's dimension is expanded or shrunk, the legend's text auto-adjusts without blocking the search result.

Consider the following dashboard:



As you customize the size of a widget in the first row, you can see that the legend of the donut chart automatically adjusts.









sls-en_dashboard_visualization_gde - 07/04/2024



Area Chart

The Area chart is used to represent quantitative data graphically. The graph is used to interpret the quantitative statistics graphically. The graph is based on a Line graph, and the area between the x-axis and lines are emphasized with colors, textures or hatchings.

Area charts are used to represent accumulated totals using numbers and percentages. It is also used to show the trends over time along with all related attributes.

The x-axis of the Area chart represents the grouping parameter(s), and the y-axis represents values of the aggregation parameter.



The following query gives the output shown above.

| timechart count()

Response Types Supported

The **Area** chart supports two aggregation response types for representation of search results in the visualization. They are:

Response Type	General Syntax
Single Aggregation with Grouping	<pre> chart aggregation_parameter by grouping_parameter1, grouping_parameter2,, grouping_parametern</pre>
Timechart Single Aggregation without Grouping	timechart aggregation_parameter

Single Aggregation with Grouping

Example:



а

	source_address=^	chart count() by ac	tion, source_address	
♦ BACK	source_address=* action=* chart count() by so	urce_address, action	Use wizard 🛛 🛪 LAST 10 MINUTI	ES - SEARCH
S Found	133 logs		🕒 Add Search To 👻 🛛 🚖	More 👻 Chart
4 3.5 3 2.5 2 1.5				Area 🕶
0.5				
0.5		··· ··· ··· ··· ··· ··· ··· ··· ··· ··		
0.5	action	source_address		
0.5 	action	source_address 128.246.120.74	count()	
0.5 	action block-url drop-all-packets	source_address 128.246.120.74 209.195.123.125	count() 1 1	
0.5 Q Q Q	action block-url drop-all-packets	Image: Control of the contro		
0.5 Q Q Q Q	action in a set of the	source_address 128.246.120.74 209.195.123.125 10.455.325 119.162.215.101		10 10
0.5 Q Q Q Q Q Q	action	Image: Control of the control of th		

You can refer to Single Aggregation with Grouping for more details.

Timechart Single Aggregation without Grouping

Example:



You can refer to Timechart Single Aggregation without Grouping for more details.

Page 63/146





ATT&CK chart

The **ATT&CK** chart is a heatmap describing the attacks carried out on a system in the form of attack tactics, techniques, and sub-techniques described by MITRE. You can select the **ATT&CK** chart from the search page only if you provide **attack_id** as a grouping parameter.

To populate the ATT&CK chart, SLS adds the following fields to the corresponding logs each time an alert is triggered:

- 1. attack_id: An ID for the attack.
- 2. attack category: The type of attack tactic used.
- 3. attack tag: The type of attack technique used.

Description

The header row of the **ATT&CK** chart contains the tactics that may be used to perform an attack. The body of the chart displays the techniques used to execute the corresponding tactics.

The ATT&CK chart also displays a drop-down icon on some cells. You can select the icon to see the sub-techniques involved in the relevant attack technique.

🚺 NOTE

The color intensity for each cell is based on the frequency of the corresponding technique and sub-technique.



The following query gives the output shown above.

```
| chart count() by attack_id
```

🚺 NOTE

You can drill down on the ATT&CK chart by clicking on each tactic on the header row and each technique and sub-technique cell on the heatmap.

Grouping by Entities

SLS also provides the option to further analyze the ATT&CK chart based on multiple entities. You can do this by grouping the results using the required entity. SLS currently supports grouping by the following entities:

- 1. user
- 2. ip_address
- 3. workstation







chart count() by attack id, user

If you group the results by an entity, the ATT&CK chart provides the following additional features:

1. The Entity icon at the top-right corner of the visualization.



Clicking the icon displays a bar chart describing the contribution of each entity to the overall results. Here, the y-axis represents the entities and the x-axis represents the count of the entities in the overall results.





2. The Info icon displayed while hovering on each cell of the ATT&CK chart.

Clicking the icon displays a bar chart describing the contribution of the entities to the corresponding attack technique or sub-technique. Here, the x-axis represents the entities and



👗 🛛 🗛







NOTE

The bar chart shows the data for the selected technique or sub-technique under all the attack tactics. To display the data for only the selected tactic, you must group the results by **attack_ category** as well.

If you have enabled SLS UEBA, you can also view the risk scores for the entities by clicking **UEBA**. This chart displays only the entities that have a risk score of more than one.

Page 66/146



sls-en_dashboard_visualization_gde - 07/04/2024





NOTE

- The entity and info icons are displayed only if you group the results by user, ip_ address, or workstation fields. Therefore, if you have a field named differently in the search results, make sure to rename the field to one of the required names using the rename command.
- If you group the results by multiple valid entities, the results are grouped only by one of the provided entities. In this case, SLS prioritizes the entities in the following order:
 - ° user
 - ip_address
 - workstation
- You can drill down on each entity's results by clicking the corresponding column of the entity bar charts. Additionally, you can drill down onto the UEBA dashboard by clicking the risk score for each entity.
- The entity icons are not displayed in the Search Templates and Dashboard.

Response Types Supported

The **ATT&CK** chart supports a single aggregation response type for the representation of search results in the visualization. It is:

Response Type	General Syntax
Single Aggregation with Grouping	<pre> chart aggregation_parameter by attack_id</pre>





Single Aggregation with Grouping

Example:

♦ ВАСК	chart co	unt() by attack_id								Use wizard All		s
Found 7	7,062 logs									🚺 Add Sea	rch To 🔻 🛛 🚖 More 🔻	С
Initial	Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	
Supply Comp	ly Chain promise	Command and Scripting Interpreter			Signed Binary Proxy Execution		File and Directory Discovery			Web Service		
Trusted Re	telationship	Native API	Valid Accounts	Valid Accounts	Valid Accounts							
Valid A	Accounts	Shared Modules	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion							
		Exploitation for Client Execution					Virtualization/Sandbox Evasion					
		Scheduled Task/Job										
		Scheduled Task/Job										_
	attack_id	Scheduled Task/Job					count()					
Q	attack_id T1059	Scheduled Task/Job					count() 111					
Q Q	attack_id T1059 T1035	Scheduled Task/Job					count() 111 45					
Q Q Q	attack_id T1059 T1035 T1075	Scheduled Task/Job					count() 111 45 35					
a a a a	attack_id T1059 T1035 T1075 T1083	Scheduled Task/Job					count() 1111 45 35 43					
Q Q Q Q Q	attack_id T1059 T1035 T1075 T1083 T1061	Scheduled Task/Job					count() 111 45 35 43 148					
Q Q Q Q Q Q	attack_idd T1059 T1035 T1075 T1083 T1061 T1085	Scheduled Task/Job					counti) 111 45 35 43 148 57					

You can refer to Single Aggregation with Grouping for more details.







Bar Chart

The Bar chart is a horizontal bar graph that visualizes categorical data in a rectangular bar with the width proportional to the value.

In a Bar Chart, the x-axis represents the aggregation parameter and the y-axis represents the grouping parameter(s). Besides this, it is similar to the Column Chart.

Widget 1 - B	ar Ch	art						~
Q Search	Info	🕜 Edit	🗴 Remove	Legend	0			
2018/07/11 09:02:44								
2018/07/11 08:56:58								
2018/07/11 09:04:05								
2018/07/11 08:40:30								
2018/07/11 08:40:40								
Column Line	Donut	Area	Bar Heatmap	Radar Tree	 Map World	Map Table	 	

The following query gives the output shown above.

| chart count() by col ts limit 5

Response Types Supported

The **Bar** chart supports a single aggregation response types for representation of search results in the visualization. It is :

Response Type	General Syntax
Single Aggregation with Grouping	<pre> chart aggregation_parameter by grouping_parameter1, grouping_parameter2,, grouping_parametern</pre>

Single Aggregation with Grouping

Example:

```
severity=* | chart count() by severity order by count() desc limit 5`
```





You can refer to Single Aggregation with Grouping for more details.





Bubble Chart

The Bubble Chart is a scatter chart that shows the relationship between variables using three dimensions: the x-axis, the y-axis, and the bubble radius. The chart can display different groups of data at once. Based on the grouping parameter, the chart groups the data into bubbles of different colors with each color representing a single group.

You can see the group names and their corresponding colors in the legend to the right of the chart.



The following query gives the output shown above.

timechart count(), avg(sig_id) by action

Response Types Supported

The **Bubble** chart supports two aggregation response types for representation of search results in the visualization. They are:

Response Type	General Syntax
Multiple Aggregation with Grouping	<pre> chart aggregation_parameter1, aggregation_parameter2 by grouping_parameter1, grouping_parameter2,,grouping_ parametern</pre>
Timechart Multiple Aggregation with Grouping	<pre> timechart aggregation_parameter1, aggregation_parameter2, , aggregation_parametern by grouping_parameter1, grouping_parameter2,, grouping_parametern</pre>

Multiple Aggregation with Grouping

Example:

```
| chart count(), max(sig_id) by action
```







♦ BACK		chart count(), max(sig_id) by action								Use wizard All	▼ LAST 10 MINUTES ▼ SEARCH
Ø	Found 2	321 logs								C Add S	earch To 🔻 📩 More 🔻 Chart 🏢
max(sig_id)	30K 25K 20K 15K 10K 5K 0 -5K		200	-		800	1000	1200	1400	1400	Bubble ▼ Ug0Fw: ©AcOGidTbHMWFhEGETgWHyEE POYNPJELXFFEALAES8 mult POXAByASLToBhY ©ACACC OAE3ByTMYEBw MgACHywX Ud0aE1MAYEBW OAE1FmkADDXABo OAE1FmkADDXABo OAE1FmkADDXABo
		U	200	400	600	count()	1000	1200	1400	1800	
							Ä				
		action					count()			max(sig_id)	
Q		Jg0IFw					4			10562	
Q		OAcOGidTbHMWFhEGETgWHyEE					1			10530	
Q		PQYNFjEaLzRFEAIAES8					111			10537	
Q		null					1579			21500	
Q		PQYAByASLTofBhY					1			10562	
Q		OAcOGic					1			10562	
Q		MA0HGiwX					23			19023	
~	< 1	Page 1 of 1 > >>	ç								Displaying 1 - 12 of 12

By default, in the search command for the Bubble Chart, the first aggregation parameter represents the x-axis while the next two parameters represent the y-axis and the bubble radius respectively.

You can also use the Bubble Chart with more than three aggregation parameters. To see the values of the other parameters, hover over a bubble in the chart. A tooltip appears, displaying all the values of the parameters associated with the bubble chart.

NOTE

The radii with negative values are represented in the red-colored text. However, the system takes the modulus of the negative value and plots it in the chart.

Example:

```
| chart count(), max(sig_id), distinct_count(action), distinct_count(sig_
id) by action
```






€ 8	BACK	chart count(), max(sig_id), distinct_count(action), distinct_count(sig_id) by action							TES 🔻 SEARCH				
🔿 F	ound 2	2,513 logs									O Adi	d Search To 🔻 🛛 🚖	More 🔻 Chart 📗
(sig_id)	30K 25K 20K 15K 10K 5K 0 -5K	0	200	400 600)	 	1000	1200	1400	1600	1800	LIGDIFW MIQLAHYWW POYNFJEIL DUNFJEIL POYABASSI DAEB271 JWDA4CACI JAODESYBL JOZZOGIC OACOGICT OACOGICT OACOGICT	zRFEALAES8 JoBbYU M2YEBW SMAGwIMBI4B SMAGwIMBI4B ODCCWeVES4B DHMWFhEGETgWHyEE JDDXABo
_						count()							
		action			count()		^	max(sig_id)		distinct_count(action)		distinct_count	:(sig_id)
Q		Jg0IFw			5			10562		1		1	
Q		MgkAHywX			122			19020		1		1	
Q		PQYNFjEaLzRFEAIAES8			111			10537		1		1	
Q		null			1763			21500		0		6	
Q		PQYAByASLTofBhY			1			10562		1		1	
Q		MA0HGiwX			23			19023		1		1	
Q		OAEaBzpTMzYEBw			5			10562		1		1	
~	< 1	Page 1 of 1 🔉 ≫	0										Displaying 1 - 13 of 13

You can refer to Multiple Aggregation with Grouping for more details.

Timechart Multiple Aggregation with Grouping

Example:

```
| timechart count(), avg(sig_id) by status_code
```



By default, in the search command for the Bubble Chart, the timechart represents the **Time** paramter in the x-axis while the next two parameters represent the y-axis and the bubble radius respectively.

You can also use the Bubble Chart with more than three aggregation parameters. To see the values of the other parameters, hover over a bubble in the chart. A tooltip appears, displaying all the values of the parameters associated with the bubble.





🚺 NOTE

The radii with negative values are represented in the red-colored text. However, the system takes the modulus of the negative value and plots it in the chart.

Example:

```
| timechart count(), avg(sig_id), max(datasize), distinct_count(sig_id) by
status_code
```



			Time			
			×			
	Timestamp	status_code	count()	avg(sig_id)	max(datasize)	distinct_count(sig_id)
Q	V 🖕 2019/03/29 09:09:09					
Q	- 10	200				
Q	- 10		47	4,611.89	NaN	4
Q	- 10	302				
Q		499				
Q	V 🖕 2019/03/29 09:09:29					
Q	- 10	200				
Q	- 10		48	4,610.48	NaN	4
Q	- 10	302				
Q		499				
Q	V 🖕 2019/03/29 09:09:49					
Q	- 10	200	1	21,500	125	1
Q	- 10		83	5,837.78	NaN	5

You can refer to Timechart Multiple Aggregation with Grouping for more details.

Rendering Parameters

Click the settings icon at the top-right corner of the Bubble Chart to open a dialog box. The dialog box allows you to configure the rendering parameters of the Bubble Chart.

BUBBLE			8
RENDERING PARAI	METERS		
Plot in Y-axis:	count()		-
Plot as Radius:	avg(sig_id)		-
		Submit	Cancel

You can select the required parameters from the **Plot in Y-axis** and **Plot in Radius** drop-down menus to represent the y-axis and the bubble radius respectively.

🚺 NOTE

Make sure you select different parameters to represent the y-axis and the bubble radius.





Clustered Bar Chart

The Clustered Bar chart is a horizontal bar graph that represents multiple categorical data in a rectangular bar with the width proportional to the value.

The only difference between a Clustered Bar chart and a **Clustered Column Chart** is the placement of parameters. In a **Clustered Column Chart**, the aggregation parameter is placed on the x-axis whereas, in a Clustered Bar chart, the parameters are placed in the y-axis.

Widget 1 - C	lustered Bar	Chart					A ~
Q Search	Info 📝 Edit	Remove	Legend				
allow indexing speed writt reset-serve reset-clinen udp,reset-bott udp,reset-bott udp,drop-all-packet udp,drop udp,drop-all-packet udp,drop block-ur nul Registered clogin - Successtu udp,reset-clinen reset-bott udp,reset-clinen reset-bott udp,reset-clinen reset-bott udp,reset-clinen reset-bott udp,reset-clinen reset-bott udp,reset-clinen reset-bott udp,reset-clinen reset-bott udp,reset-clinen reset-bott udp,reset-clinen reset-bott udp,reset-clinen reset-bott udp,aler read		Lustered Line	 Stacked Area	Radar	World Map	Table	■ avg(sig_id)

The following query gives the output shown above.

| chart count(), avg(sig_id) by action

Response Types Supported

The **Clustered Bar** chart supports two aggregation response types for representation of search results in the visualization. They are:

Response Type	General Syntax
Multiple Aggregation without Grouping	chart count(), avg(datasize)
Multiple Aggregation with Grouping	<pre> chart aggregation_parameter1, aggregation_parameter2 by grouping_parameter1, grouping_parameter2,, grouping_ parametern</pre>

Multiple Aggregation without Grouping

Example:

| chart avg(sent_datasize), avg(received_datasize)





You can refer to Multiple Aggregation without Grouping for more details.

Multiple Aggregation with Grouping

Example:

action=Allow or action=Deny | chart count(action=allow) as AllowedConnection, count(action=deny) as DeniedConnection by source_ address order by count(action=allow), count(action=deny) desc limit 10

♦ BACK	action=Allow or ac	tion=Deny chart cou	unt(action=allow) as All	lowedConnection, co	unt(action=deny) as	DeniedConnection	by source_addre	Use wizard	All 👻 LAST 10 M	IINUTES 👻	SEARCH
S Found	7,656 logs								Add Search To 🔻	🔺 More 👻	Chart
11 176.3 22. 213. 35.23 208.10 199. 193.166 95.140 8.25	27.0.010 1.150.16 45.90.63 0.26.251 0.26.251 225.171 229.147 4.218.46									■ Alloi ■ Den	Clustered Bar 🔻
		5	10	15	20	25	30	35	40		
	source_address				AllowedConnecti	ion		DeniedConne	ction		
Q	127.0.0.10				34			40			
Q	176.31.150.16				5			0			
Q	22.11.108.0				4			0			
Q	213.46.90.63				3			0			
Q	35.233.114.27				2			6			
Q	208.100.26.251				2			1			
Q	195.22.4.21				2			1			
Q	193.166.255.171				2			0			
« <	Page 1 of 1	×C								Di	splaying 1 - 10 of 10

You can refer to Multiple Aggregation with Grouping for more details.





Clustered Column Chart

The Clustered Column chart is a type of Column Chart which allows you to display multiple quantitative variables.

Unlike a standard Column Chart, where only one variable is used to mark x-axis, a Clustered Column chart uses multiple variables on the x-axis with a different color for each variable.



The following query gives the output shown above.

| timechart count(), avg(datasize)

Response Types Supported

The **Clustered Column** chart supports four aggregation response types for representation of search results in the visualization. They are:

Response Type	General Syntax
Multiple Aggregation without Grouping	chart count(), avg(datasize)
Multiple Aggregation with Grouping	<pre> chart aggregation_parameter1, aggregation_parameter2 by grouping_parameter1, grouping_parameter2,,grouping_ parametern</pre>
Timechart Multiple Aggregation without Grouping	<pre> timechart aggregation_parameter1, aggregation_parameter2, aggregation_parametern</pre>





Response Type	General Syntax
Timechart Multiple Aggregation with Grouping	<pre> timechart aggregation_parameter1, aggregation_parameter2, , aggregation_parametern by grouping_parameter1, grouping_parameter2,, grouping_parametern</pre>

Multiple Aggregation without Grouping

For the Multiple Aggregation without Grouping response type, the x-axis represents the different aggregation parameter, and y-axis contains the scale that denotes the value of the aggregation parameter.

Example:

```
| chart max(sent_datasize), max(received_datasize)
```



You can refer to Multiple Aggregation without Grouping for more details.

Multiple Aggregation with Grouping

For the Multiple Aggregation with Grouping response type, the x-axis contains the values of grouping parameter(s) with a vertical bar for each aggregation parameter. The height of the bar determines the value of the aggregation parameter for the specific value of a grouping parameter. The y-axis contains the scale that denotes the value of the aggregation parameter.

Example:

```
action=Allow or action=Deny | chart count(action=allow) as
AllowedConnection, count(action=deny) as DeniedConnection by source_
address order by count(action=allow), count(action=deny) desc limit 10
```





♦ BACK	action=Allow or action=Deny chart count(ac	ction=allow) as AllowedConnection, co	unt(action=deny) as Denie	edConnection by source_addre	Use wizard All	▼ LAST 10 MINUTES ▼ SEARCH
S Found	7,604 logs				C Add	Search To 💌 📩 More 💌 Chart 🏢
						Clustered Column 👻
						AllowedConnection
40						DeniedConnection
35						
30						
20						
15						
10						
5						
	127.0.0.10 22.11.108.0 176.31.	.150.16 35.233.114.27 195.22.4.	21 208.100.26.251	193.166.255.171 195.157.15.100	95.140.229.147 157.	122.62.205
			Ä			
	source_address		AllowedConnection		DeniedConnection	
Q	127.0.0.10		34		40	
Q	22.11.108.0		4		0	
Q	176.31.150.16		3		0	
Q	35.233.114.27		2		6	
Q	195.22.4.21		2		1	
Q	208.100.26.251		2		1	
0	193.166.255.171		2		0	
≪ <	Page 1 of 1 🔉 🚿 📿					Displaying 1 - 10 of 1

You can refer to Multiple Aggregation with Grouping for more details.

Timechart Multiple Aggregation without Grouping

For the Timechart Multiple Aggregation without Grouping response type, the x-axis represents the different time buckets within the specified time range, and the y-axis contains the scale that denotes the value of the aggregation parameter. The bars indicate the different values of the aggregation parameter at different timestamps. The vertical length of a bar signifies its value of the aggregation parameter at that particular timestamp.

Example:

norm_id=WinDNSDHCP | timechart count(lease_address=drop) as Dropped, count (lease_address=start) as Started, count(lease_address=end) as ENDED



You can refer to Timechart Multiple Aggregation without Grouping for more details.





Timechart Multiple Aggregation with Grouping

For the Timechart Multiple Aggregation with Grouping response type, the x-axis represents the different time buckets within the specified time range, and the y-axis contains the scale that denotes the value of the aggregation parameter. The bars indicate the different values of the aggregation parameter at different timestamps. The vertical length of a bar signifies its value of the aggregation parameter at that particular timestamp.

Example:

```
norm_id=WinDNSDHCP | timechart count(lease_address=drop) as Dropped, count
(lease address=start) as Started, count(lease address=end) as ENDED
```



You can refer to Timechart Multiple Aggregation with Grouping for more details.







Clustered Line Chart

The Clustered Line chart is an extension of the Line Chart in which multiple lines are used to represent values of different categories. Silimar to the Clustered Column Chart, in a Clustered Line chart the x-axis contains the values of the grouping parameters, and the y-axis contains the scale to measure the value of an aggregation parameter of the particular grouping parameter.



The following query gives the output shown above. :

| chart count(), avg(sig_id) by action

Response Types Supported

The **Clustered Line** chart supports three aggregation response types for representation of search results in the visualization. They are:

Response Type	General Syntax
Multiple Aggregation with Grouping	<pre> chart aggregation_parameter1, aggregation_parameter2 by grouping_parameter1, grouping_parameter2,,grouping_ parametern</pre>
Timechart Single Aggregation with Grouping	<pre> timechart aggregation_parameter by grouping_parameter1, grouping_parameter2,, grouping_parametern</pre>
Timechart Multiple Aggregation without Grouping	<pre> timechart aggregation_parameter1, aggregation_ parameter2, aggregation_parametern</pre>

Multiple Aggregation with Grouping

Example:





sent data data	_dat size size	tasize= e) by s e) desc	=* source source_ad c limit 1	_address=* dress orde 0	* cha er by m	rt max(sent_ ax(sent_data	datasize size), m), max(r ax(recei	received	-
	♦ ВАСК	sent_datasize=*	* source_address=* char	t max(sent_datasize), max(re	ceived_datasize) by	source_address order by max(sen	t_datasize), max(r	Use wizard	Ali 👻 LAST 10 MINUTES	SEARCH
	S Found 9	9 logs						Ado	d Search To 🔻 🛉 🃩 More	• Chart
										Clustered Line 🔻
	80K		•						■ max(s ■ max(r	ent_datasize) eceived_datasize)
	60K									
	40K							_		
	20K									
	0							•		
		2	13.46.90.63	67.87.195.179	22.11.108.0	176.31.150.16	165.129.175.60	197.126.237.40		
		source_address			n	nax(sent_datasize)		max(received_datasize	e)	
	Q	213.46.90.63			83	874		74059		
	Q	67.87.195.179			66	612		75461		
	Q	22.11.108.0			44	640		66960		
	Q	176.31.150.16			44	349		71851		
	Q	165.129.175.60			13	848		876		
	Q	197.126.237.40			72	50		49825		

You can refer to Multiple Aggregation with Grouping for more details.

Timechart Single Aggregation with Grouping

In the Timechart Single Aggregation with Grouping, the y-axis represents the aggregation value for every grouping parameter, and the x-axis displays the value of the timestamps. Similarly, the lines represent the values of the grouping parameter(s).

Example:



You can refer to Timechart Single Aggregation with Grouping for more details.





Timechart Multiple Aggregation without Grouping

Alike to the Clustered Column chart, the y-axis represents values of the aggregation parameter, and the x-axis displays the value of the timestamps. Similarly, the lines represent the values of the aggregation parameters at a particular timestamp.

Example:

| timechart count("event_category" = "THREAT") as Dangerous, count("event_ category" ="TRAFFIC") as Traffic



You can refer to Timechart Multiple Aggregation without Grouping for more details.

Page 83/146



sls-en_dashboard_visualization_gde - 07/04/2024



Column Chart

The Column Chart is a vertical bar graph that represents categorical data in rectangular bars with heights proportional to the values that they represent.

The Column Chart shows comparisons among discrete categories. It is a two-dimensional graph in which one axis of the graph shows the specific groups being compared and another one represents the measured value.



The following query gives the output shown above.

| chart count() by action limit 5

Response Types Supported

The **Column** chart supports two aggregation response types for representation of search results in the visualization. They are:

Response Type	General Syntax
Single Aggregation with Grouping	<pre> chart aggregation_parameter by grouping_parameter1, grouping_parameter2,, grouping_parametern</pre>
Timechart Single Aggregation without Grouping	timechart aggregation_parameter

Single Aggregation with Grouping

In the Single Aggregation with Grouping response type, the x-axis of a Column chart represents the values of the grouping parameter(s) whereas the y-axis represents the values of the aggregation parameter.

Example:





seve	rity	=*	chart	count()	by	severity	order	by	count()	desc	limit 5		
	♦ BACK	severity=	* chart count()	by severity order by	count() c	desc				Use w	izard All 👻 LAST 10	MINUTES 👻	SEARCH
	S Found 4	168 logs									🕒 Add Search To 👻	🔺 More 👻	Chart
													Column 🔻
				_									count()
	220												
	140												
	100												
	60											_	
	20				L. L.				and the set				
			0		nign		iow		critical		medium		
		severity					<u> </u>	count()					
	Q	6						236					
	0	high						47					
	~	low						41					
	Q Q	aniti ani						44					
	Q	critical						41					
	Q	medium						36					
	« <	Page 1	of 1 🔰 ≫	C								Dis	olaying 1 - 5 of 5

You can refer to Single Aggregation with Grouping for more details.

Timechart Single Aggregation without Grouping

In the Timechart Single Aggregation without Grouping response type, the x-axis of the Column chart represents the value of timestamps whereas the y-axis represents the values of the aggregation parameter.

Each bar represents the value of the aggregation parameter in a given **Interval**. The **Interval** is calculated automatically as per the time range selected in the **Search Bar**. The value of the **Interval** is displayed on the extreme left of the container.

Example:







You can refer to Timechart Single Aggregation without Grouping for more details.





sls-en_dashboard_visualization_gde - 07/04/2024



Day/Hour Heatmap Chart

Heatmaps are used to visualize individual values contained in a matrix and represent them using different shades of a single color.

The Day/Hour Heatmap is an extension of a regular heatmap in which results are displayed in the day/hour format. It has seven rows and 24 columns. Each row represents a day of the week and each column represents an hour of the day. Therefore, each cell represents a single hour of a particular day.

The query format for the Day/Hour Heatmap is:

| timechart aggregation parameter1 every 1 hour

Example:

```
| timechart sum(datasize) as TotalDatasize every 1 hour
```



Response Types Supported

The **Day/Hour Heatmap** chart supports a single aggregation response types for representation of search results in the visualization. It is :

Response Type	General Syntax
Timechart Single Aggregation without Grouping	timechart aggregation_parameter

Timechart Single Aggregation without Grouping

The Day/Hour Heatmap only works for the Timechart Single Aggregation with Grouping response type with **every 1 hour** suffixed to the query.

The values of the aggregation parameter are displayed in the cells as per their timestamps.

The intensity of the color is dependent upon the relative value of the aggregation parameters.





Example:

♦ BAG	.cк timechart	sum(data	size) as '	TotalDat	asize eve	ery 1 hou	ir												Use wiz	zard All	➡ LAST	10 MINUTE	s 👻 📕
S Four	and 267,324 logs																		C) Add Searc	th To 🔻	🔺 More	w Tir
Interval:	a 1 hour																						Day/H
2018	3/07/11 10:00:00 to 201 1a 2a	8/07/12 10:00: 3a	4a	5a	6a	7a	8a	9a	10a	11a	12p	1p	2p	3p	4p	5p	6p	7p	8p	9p	10p	11p	12a
We																							
Th																							
Fr																							
Sa																							
Su																							
Мо																							
Tu																							
0																							
												×.											
	Timestamp																TotalDa	tasize					
Q	2018/07/11 1	0:00:00															4082751						
Q	2018/07/11 1	1:00:00															1658212						
Q	2018/07/11 1	2:00:00															641566						
	2018/07/11 1	3:00:00															1593376						
Q	2018/07/11 1	4:00:00															3100606						
d d	2010/07/11 1	E-00-00															13/0//9						
d d d d	2018/07/11 1	5:00:00															3030170						
α α α α α α	2018/07/11 1 2018/07/11 1 2018/07/11 1	5:00:00 6:00:00 7:00:00															536112						

When the selected time range is more than a week, a slider appears on the right end of the container that allows the user to slide over the particular days.

You can refer to Timechart Single Aggregation without Grouping for more details.

Rendering Parameters

You can assign custom colors to the Day/Hour heatmap for both positive and negative values. SLS uses the selected color to represent the maximum value of the data obtained, and lesser values have the same color with linear transparency.

RENDERING PARAM	ETERS		
Positive Value:	#E78383		Ψ.
Negative Value:	#2A2424		v
Reset		Submit	Cancel







Display Chart

Widget 1 - Display Chart Q Search Info Remove Control avg(datasize) count() max(datasize) avg(datasize) 12532 442037 387.72

The Display format shows the value of the aggregation parameter in the container.

The following query gives the output shown above.

Table

| chart count(), max(datasize), avg(datasize)

To view the search results in display format, select **Display** from the drop-down at the top-right corner of the **Search Result** page.

Response Types Supported

Clustered Column Clustered Bar Display

The Display chart supports three aggregation response types for representation of search results in the visualization. They are:

Response Type	General Syntax
Single Aggregation without Grouping	chart aggregation_parameter
Single Aggregation with Grouping	<pre> chart aggregation_parameter by grouping_ parameter</pre>
Multiple Aggregation without Grouping	chart count(), avg(datasize)

Page 89/146





Single Aggregation without Grouping

€ ВАСК	chart count()	Use wizard	All 🔻	LAST 10 M		SEARCH
Found 1	510 logs	0	Add Sea	ch To 👻	🚖 More 👻	Chart
						Display 🔻
	count()					
	1610					
	count()					
Q	1610					

To view the search results in display format, select **Display** from the drop-down on the top-right corner of the **Search Result** page.

🚺 NOTE

By default, SLS renders the display format for all queries of the **Single Aggregation without Grouping** type.

You can refer to Single Aggregation without Grouping for more details.

Single Aggregation with Grouping

← BACK	attack_category=* ch	art count() by attack_ca	tegory			Use wizard All	LAST 10 MINUTES V SEARCH
S Found	1,225 logs					C Add Search	To 🔻 📩 More 💌 Chart 📗 🛄 Display 👻
R Dev	esource velopment	Privilege Escalation	Execution	Command and Control	Command and Control,Persistence,Privilege Escalation	Defense Evasion, Privilege Escalation	Reconnaissance
	189	40	60	68	2	3	236
					Ŕ		
	attack_category					count	0
Q	Resource Development					189	
0	Privilege Escalation					40	

To view the search results in display format, select **Display** from the drop-down on the top-right corner of the **Search Result** page.

🚺 NOTE

The Display chart is available in Search, Dashboards, and Search Templates.

You can refer to Single Aggregation with Grouping for more details.

Multiple Aggregation without Grouping

For Multiple Aggregation without Grouping response type, the value of the first aggregation parameter is displayed in the container.





♦ BACK	chart avg(sent_datasize), avg(received_datasize)			Use wizard All 👻 LAST 10 MINUTES 👻 SEARCH
S Found 4	184 logs			🕼 Add Search To 🔻 🛛 📩 More 💌 🛛 Chart 📗
		avg(sent_datasize)	avg(received_datasize) 1.87	Digitaj 💌
	avg(sent_datasize)		avg(received_datasize)	
Q	1.98		1.87	

To view the search results in display format, select **Display** from the drop-down on the top right corner of the Search result page.

You can refer to Multiple Aggregation without Grouping for more details.

Rendering Parameters

Click the Settings icon at the top-right corner to change the Rendering Parameters.

RENDERING PARAMETER	;
	avg(sent_datasize) avg(received_datasize)
Output format:	Avenir ᅌ B I U T* T* T =
	{{avg(sent_ <u>datasize)}}</u> {{avg(received_ <u>datasize</u>)}}
Background color:	#C64444 ~
	☑ Use default layout
	Submit Cancel

You can choose the output format, font and the background color from the rendering parameter section.







♦ ВАСК	chart avg(sent_datasize), avg(received_datasize)	Use wizard All 👻 LAST 10 MINUTES 👻 SEARCH
S Found 4	184 logs	🔕 Add Search To 🔻 🛛 🚖 More 👻 🗌 Chart 💵
		Display 💌
	avg[sent_datasize)	avg(received_datasize)
Q	1.98	1.87

Customize the output of the display by configuring the **Output format**. In this section, you can choose the fonts and color of the result. Additionally, you can use the display template similar to "jinja" to customize the search result.

RENDERING PARAMET	ERS
	count() max(datasize) avg(datasize)
Output format:	Avenir 🕒 B I 🖳 T* T* 🔳
	The count is: {{count()}}
	The maximum data size is:{{max(datasize)}}
	The average data size is : {{avg(<u>datasize</u>)}}
Background color:	#ffffff
	Use default layout
	Submit Cancel

The result of the configuration looks like:



ONOTE The **Output Format** section is disabled when you select the default layout.



Donut Chart

The Donut Chart shows the data distribution based on the length of its arc. It was introduced in SLS to replace the Pie Chart. The reason for this is that pie charts can be hard to interpret as they focus on the proportional areas of the slices. Donut charts de-emphasize the use of area and focus on the lengths of the arcs of each individual element



The following query gives the output shown above.

source_address=* | chart sum(datasize) as Datasize by source_address

Response Types Supported

The **Donut** chart supports a single aggregation response types for representation of search results in the visualization. It is :

Response Type	General Syntax
Single Aggregation with Grouping	<pre> chart aggregation_parameter by grouping_parameter1, grouping_parameter2,, grouping_parametern</pre>

Single Aggregation with Grouping

Example:

source_address=* | chart count() by source_address





♦ BACK	source_address=* action=* chart count() by source_address, action order by count() desc limit 10		Use wizard All 👻 LAST 10 MINUTES	SEARCH
S Found	273 logs		🚯 Add Search To 👻 🔺 📩 More	e 👻 Chart 📗
				Donut 🔻
				$\begin{array}{c} 127,0,0,10\\ 148,108,123,180\\ 239,219,39,109\\ 239,219,39,109\\ 239,119,39,109\\ 240,107,182,208\\ 16,200,214,3\\ 41,95,105,122\\ 203,225,92,138\\ 10,94,0,254\\ 110,155,124,242\\ 83,83,198,65\\ 1181,154,198,152\\ 1181,154,198,152\\ 1181,154,198,152\\ 10,37,78\\ 0,0,0,0\\ 235,25,47,180\\ 55,243,207,69\\ 55,243,207,69\\ 55,217,15,124\\ \end{array}$
	source_address	count()		
Q	127.0.0.10	4		
Q	168.108.121.80	1		
Q	1.29.219.8	1		
Q	239.168.239.109	1		
Q	200.107.182.208	1		
Q	16.200.214.3	1		
Q	41.95.105.122	1		
Q	203.225.92.138	1		
Q	10.94.0.254	6		
Q	110.155.124.242	1		
Q	83.83.198.65	1		
Q	181.154.198.152	1		
~ <	Page 1 of 1 >>>> 💭			Displaying 1 - 12 of 12

You can refer to Single Aggregation with Grouping for more details.





Gauge Chart

Gauge chart, also known as speedometer chart, uses a single needle to show the information as a reading on a dial. The graph is used to visualize percentage values as well as a fixed range of data.



The following query gives the output shown above.

| chart count()

The value of the aggregation parameter determines the value pointed by the needle. You can configure the maximum value of the dial from **Max value** while rendering parameters. When a value of the aggregation parameter is equal to, or greater than the **Max value**, the percentage value of the needle is displayed as 100%.

Three different colors, green, yellow, and red are used to represent the limits for the data being depicted in the gauge. By default, the green, yellow, and red colors represent the low, mid, and high range of values respectively. However, you can configure the threshold value (in percentage) to display the dial in the yellow and red colors.

Response Types Supported

The **Gauge** chart supports a single aggregation response types for representation of search results in the visualization. It is:

Response Type	General Syntax
Single Aggregation without Grouping	chart aggregation_parameter





Single Aggregation without Grouping

♦ BACK	chart count()		Use wizard All 👻 LAST 10 MINUTES 👻 SEARCH
Found 1	,610 logs		🚯 Add Search To 👻 🔺 More 👻 Chart 📗
		1610 100%	Guge 🕶
_			
	count()		
Q	1610		

To view the search results in a Gauge chart, select **Gauge** from the drop-down menu on the topright corner of **Search Result** page.

You can refer to Single Aggregation without Grouping for more details.

Rendering Parameters

Click the settings icon on the right side of the chart container to open the **Rendering Parameters** panel.

♦ BACK	chart count()			U	se wizard All 👻 LAST 10 M		SEARCH
S Found	1,610 logs				Add Search To •	🔺 More 👻	Chart
		$\left(\right)$	1610 100*				Gauge 💌
	count()		^				
Q	1610						
RE							
Ma	ix value:	5000		\$			
Re	d starts (% of max value):	90		\$			
Ye	low starts (% of max value):	70		\$			
			Submit	Cancel			

You can specify the threshold value for the red and yellow colors in the **Red Starts** and **Yellow Starts** configuration fields on the **Rendering Parameters** panel.





NOTE

The value of **Red starts** is 90% and **Yellow starts** is 70% by default.

← BACK	1,610 logs					Use wizard	All 👻 LAST 10	MINUTES 👻	SEARCH Chart
									Gauge 🔻
			(1610 32*					
	count()								
Q	1610								





sls-en_dashboard_visualization_gde - 07/04/2024



Heatmap Chart

Heatmap visualizes individual values in a matrix and represents them through different color shades based on their intensity. Use it to analyze the differences across multiple variables, reveal patterns, and detect correlations between them.



The following query gives the output shown above.

```
| chart count() by action, protocol
```

Response Types Supported

The **Heatmap** chart supports a single aggregation response types for representation of search results in the visualization. It is :

Response Type	General Syntax
Single Aggregation with Grouping	<pre> chart aggregation_parameter by grouping_parameter1, grouping_parameter2,, grouping_parametern</pre>

Single Aggregation with Grouping

Example:

```
source_address=* action=* | chart count() by source_address, action order
by count() desc limit 10
```





♦ BACK	ck source_address=* action=* chart count() by source_address, action order by count() desc limit 10 Use wizard All 👻 LAST 10 MINUTES 👻 SEARCH										
S Found	🛇 Found 153 logs 🔹 🗘 Add Search To 👻 🖈 More 👻 Chart 🔢									Chart	
											Heatmap 🔻
de	enied										6
reset-cl	linent										
udp	,drop										11
blo	ckurd										÷.
510											11
drop-all-pa	ickets										0
	0.0.0.0	10.45.3.199	10.45.3.77	10.45.3.241	10.45.3.198	10.45.3.252	232.245.161.52	37.156.73.221	70.115.81.238	31.21.32.11	
	source_address			acti	on			count()			
Q	0.0.0.0			denie	ed	6					
Q	10.45.3.199			denie	denied 2						
Q	10.45.3.77			denie	ed		2				
Q	10.45.3.241			denie	ed		2				
٥	10.45.3.198			denie	ed			2			
Q	10.45.3.252			denie	denied						
Q	232,245,161.52			reset	t-clinent			1			
Q	37.156.73.221			udp,	drop			1			
Q	70.115.81.238			block	k-url			1			
Q	31.21.32.11			drop	drop-all-packets 1						
« < I	Page 1 of 1	»								Display	ing 1 - 10 of 10

You can refer to Single Aggregation with Grouping for more details.

Rendering Parameters

Click the settings icon at the top-right corner of the heatmap chart to open a dialog box. The dialog box allows you to configure the rendering parameters of the Heatmap chart.



The Rendering Parameters such as **X-axis Group**, **Positive Value**, and **Negative Value** provide a custom settings option to view data in different formats.





By default, the first grouping parameter of the query is assigned to the X-axis of the Heatmap. For example, the grouping parameter **source_name** is assigned in the X-axis of the Heatmap for the query:

| chart count() by source name, action

However, by selecting a value from the drop-down menu of the **X-axis Group**, you can choose the grouping parameter to be placed on the X-axis of the chart. For example,

| chart count() by source name, action

The query above contains two grouping parameters: **source_name** and **action**. If you choose **action** for x-axis, **source_name** is shown on y-axis. The **count()** value is represented according to the transparency level of the chosen cell color.

🚺 NOTE

If a query contains three or more than three grouping parameters, and you choose to keep grouping parameter_1 on the x-axis, then the combination of grouping parameter_2,, grouping parameter_n is shown on the y-axis.

Furthermore, you can assign custom colors to the Heatmap for both positive and negative values. SLS uses the selected color to represent the maximum value of the data obtained, and lesser values have the same color with linear transparency.

RENDERING PARAMETERS							
X-Axis Group:	action		Ŧ				
Positive Value:	#6e4c7a		-				
Negative Value:	#c64944		Ŧ				
Reset		Submit	Cancel				

Page 100/146



sls-en_dashboard_visualization_gde - 07/04/2024



SLS - DASHBOARD & VISUALIZATION GUIDE - V 2 VISUALIZATION

♦ BACK	source_address=* action=* chart count() by	source_address, action order by count() de	sc limit 10 U	se wizard All 🔻 LAST 10 MINUTES 🖣	SEARCH
💿 Found	136 logs			🔹 Add Search To 👻 🄺 More	
					Heatmap 👻
0	000				6
10.45.	3.241				
10.45.	3.198				
10.45.	3.245				
10.45	.3.25				
10.45.	3.252				
232.245.1	61.52				
27.60.14	9.231				0
	denied	reset-clinent	deny	allow	
	source_address	action	cou	nt()	
Q	0.0.0.0	denied	6		
Q	10.45.3.241	denied	4		
Q	10.45.3.198	denied	2		
Q	10.45.3.245	denied	2		
Q	10.45.3.199	denied	2		
Q	10.45.3.25	denied	2		
Q	10.45.3.252	denied	2		
Q	232.245.161.52	reset-clinent	1		
Q	127.0.0.10	deny	1		
Q	27.60.149.231	allow	1		
~ <	Page 1 of 1 🔉 🚿 📿				Displaying 1 - 10 of 10



sls-en_dashboard_visualization_gde - 07/04/2024



Line Chart

The Line chart displays information as a series of data points called markers. The markers are connected to each other by a line.

The Line chart consists of two axes, in which x-axis contains the value of the grouping parameter(s) and the y-axis contains the values of the aggregation parameter. It is similar to a Column chart, except that, a Column chart usually displays discrete values, whereas a line chart visualizes a trend in continuous data.



The following query gives the output shown above.

source_address=* | chart sum(datasize) as Datasize by source_address

Response Types Supported

The **Line** chart supports two aggregation response types for representation of search results in the visualization. They are:

Response Type	General Syntax
Single Aggregation with Grouping	<pre> chart aggregation_parameter by grouping_parameter1, grouping_parameter2,, grouping_parametern</pre>
Timechart Single Aggregation without Grouping	timechart aggregation_parameter

Single Aggregation with Grouping

Example:

severity=* | chart count() by severity





You can refer to Single Aggregation with Grouping for more details.

Timechart Single Aggregation without Grouping

Example:

```
| timechart avg(datasize)
```

♦ BACK	timechart avg(data	asize)							Use wizard	Ali 👻 LAS	T 10 MINUTES 👻	SEARCH
S Found	397 logs								🖸 Add S	iearch To 🐨	🔺 More 👻	Timechart
Interval: 1	0 seconds	. Cumulative Show/F	Hide Trendline:									Line 👻
1.2K 1K 800 600 400 200 0						~^			-	•	• • • •	avg(datasize)
	04:47:00 AM	04:47:30 AM	04:48:00 AM	04:48:30 AM	04:49:00 AM July 12, 2018	04:49:30 AM	04:50:00 AM	04:50:30 AM	0	4:51:00 AM		
	Timestamo				^			avo(datasize)				
0	2018/07/12 04:46:50							1031.07				
0	2018/07/12 04:47:00							342.45				
0	2018/07/12 04:47:10							730.2				
0	2018/07/12 04:47:20							0				
0	2018/07/12 04:47:30							0				
0	2018/07/12 04:47:40							510.33				
0	2018/07/12 04:47:50							18.17				
0	2018/07/12 04:48:00							558.12				
0	2018/07/12 04:48:10							1139.33				
õ	2018/07/12 04:48:20							1278				
0	2018/07/12 04:48:30							133.78				
Q	2018/07/12 04:48:40							832.4				
0	2018/07/12 04:48:50							293.67				
Q	2018/07/12 04:49:00							287.82				
0	2018/07/12 04:49:10							195				
Q	2018/07/12 04:49:20							124				

You can refer to Timechart Single Aggregation without Grouping for more details.







Parallel Coordinate Chart

The Parallel Coordinate Chart is a visualization technique used to plot individual data elements across multiple dimensions. The charts are ideal for comparing many grouping parameters and analyzing the relationships between them. Each grouping parameter has its axis, and all the axes are placed in parallel to each other. Values are plotted as a series of lines that are connected across all the axes. This means that each line is a collection of points placed on each axis, which have all been linked together.

The Parallel Coordinate chart shows both the forest and the tree. You can see the big picture in the patterns of the lines. You can highlight the individual lines to see the performance of a specific value of parameters. It is useful in the situations when the behavior of particular parameters may not be of concern, but a combination of those parameters may emphasize an abnormal pattern or relationship.



The following query gives the output shown above.

```
| process geoip(source_address) as source_country | chart count() by
source_country, sub_category, destination_location
```

🚺 NOTE

- 1. Each line represents a relationship between two parameters rather than a trend or change in value.
- 2. As the number of values increase, the graph may be cluttered or may even overlap at times, which makes it difficult to perceive. In such a case, use the Brushing feature to highlight an individual or a group of values for better understanding.
- 3. You can view the value of the aggregation parameter by hovering over a relationship line.





Response Types Supported

The **Parallel Coordinate** chart supports a single aggregation response types for representation of search results in the visualization. It is :

Response Type	General Syntax
Single Aggregation with Grouping	<pre> chart aggregation_parameter by grouping_parameter1, grouping_parameter2,, grouping_parametern</pre>

Single Aggregation with Grouping

Example:

```
| process geoip(source_address) as source_country | chart count() by
source_country, sub_category, destination_ location
```



Some notable points about the Parallel Coordinate chart are as follows:

- 1. Each line represents a relationship between two parameters rather than a trend or a change in value.
- 2. As the number of values increase, the graph may be cluttered or even overlapped at times, which makes it difficult to analyze. In this case, use the Brushing feature to highlight an individual or a group of values for better understanding.
- 3. You can view the value of the aggregation parameter by hovering over a relationship line.

You can refer to Single Aggregation with Grouping for more details.

Operations

Brushing

The Brushing feature eliminates one of the primary drawbacks of the Parallel Coordinate chart, which is cluttering and overlapping of the graph. When the number of data items in a Parallel Coordinate chart gets very high, lines get cluttered and even overplotted which eventually becomes difficult to understand. Using the brushing feature, you can select an area containing one or many data points.

Page 105/146





The line(s) under the brushed area is highlighted. You can view the details of the stressed relationship by hovering over the particular line. In addition to that, you can further drill-down to its details of the relationship by clicking it.



Combined Drill-down

In addition to the regular drill down operation, you can also perform a combined drill-down using the **Brush**. Select a range of values in multiple axes using a brush and click the brushed area, to drill down.



The results of the drill-down filters down to the combination of the selected grouping parameter values.







Changing order of the parameter

By default, the first grouping parameter of the query is assigned to the first axis of the Parallel Coordinate chart, followed by the other grouping parameters.

For example, in the above query, the grouping parameter **source_address**, **sub_category** and **destination_location** are placed in first, second and third axes respectively.

You can also change the order of parameters by dragging them across the parameters with which the value is to be exchanged.







Radar chart

The Radar chart is a graphical representation of multivariate data in the form of a twodimensional graph, in which one or more quantitative variables are represented on axes starting from the same point.

Each value of grouping parameter(s) forms an individual axis which is arranged radially around a point. These axes are equiangular to each other and known as spoke or radii. Each node depicts the value of a spoke, and the lines are drawn to connect the nodes to each other.

The Radar chart is best for visualizing outliers in a dataset, especially in cases of operation related analysis such as performance metrics and quality improvement. The line between the origin points and radii can be used as the scale for data points.



The following query gives the output shown above.

```
| chart count by action()
```

Response Types Supported

The **Radar** chart supports four aggregation response types for representation of search results in the visualization. They are:

Response Type	General Syntax
Single Aggregation with Grouping	<pre> chart aggregation_parameter by grouping_parameter1, grouping_parameter2,, grouping_parametern</pre>
Multiple Aggregation with Grouping	<pre> chart aggregation_parameter1, aggregation_parameter2 by grouping_parameter1, grouping_parameter2,, grouping_ parametern</pre>


Response Type	General Syntax
Timechart Single Aggregation without Grouping	timechart aggregation_parameter
Timechart Multiple Aggregation without Grouping	<pre> timechart aggregation_parameter1, aggregation_ parameter2, aggregation_parametern</pre>

Single Aggregation with Grouping

Example:

```
service=* action=* | chart count() by action, service
```



		*		
	service	action	count()	
۹	normalizer_0	reporting speed	55	
Q	indexsearcher_default	indexing speed	16	
Q	labeling	reporting speed	2	
Q	filesystem_collector	reporting speed	57	
Q	normalizer_3	reporting speed	56	
Q	normalizer_1	reporting speed	56	
Q	syslog_collector_c	reporting speed	38	
~ <	Page 1 of 1 > >> 2		Displaying 1 - 10 of 10	

You can refer to Single Aggregation with Grouping for more details.

Multiple Aggregation with Grouping

Example:

```
"norm_id"="WinDNSDHCP"| chart count(lease_address=end), count(lease_
address=start) by user
```





SLS - DASHBOARD & VISUALIZATION GUIDE - V 2 VISUALIZATION

♦ BACK	"norm_id"="WinDNSDHCP" chart count(lease_address=end), count(lease_a	ss=start) by user	Use wizard All 👻 LAST 1	0 MINUTES 👻	SEARCH
S Found 2	278 logs		C Add Search To 👻	🔺 More 🔻	Chart
	10.207.31.46 67.87.195.179	12947108.182		Count(lesse_	Radar 💌
	user	count(lease_address=end)	count(lease_address=start)		
Q	129.49.108.182	28	0		
Q	74.119.194.18	0	29		
Q	165.129.175.60	0	18		
Q	197.126.237.40	0	13		

You can refer to Multiple Aggregation with Grouping for more details.

Timechart Single Aggregation without Grouping

The Radar chart can be used in time queries to graphically represent the change in values of the aggregation parameter over a period.

Example:

67.87.195.179

Q



Q	018/07/12 06:55:14	1
You	an refer to Timechart Single Aggregation without Grouping for m	ore details.

Timechart Multiple Aggregation without Grouping

2018/07/12 06:51:14 2018/07/12 06:53:14

The Radar chart can be used in time queries to graphically represent the change in values of aggregation over a period. For Timechart Multiple Aggregation without grouping type, each aggregation parameter is represented by a unique color.





Example:

orm_ leas	_id=WinDNSDHCP t se_address=start)	<pre>imechart count(lease_ad as Started, count(lease</pre>	dress=drop) as _address=end)	Dropped, count as ENDED	
	BACK norm_id=WinDNSDHCP timechart court	t(lease_address=drop) as Dropped, count(lease_address=start) as	Started, count(lease_address=en Us	se wizard All 👻 LAST 10 MINUTES 👻	SEARCH
	S Found 140 logs			🕲 Add Search To 👻 🌟 More 👻 🛛 Ti	imechart
	Interval: 1 minute				Radar 👻
			06-05 06-06 0.607 06-09 06-10 06-10 06-11 06-12 06-13 06-13 06-14		Dropped Started ENDED
- 1	T:	Descend	Started	ENDED	
	2018/07/12 04-02-00	Dropped	Started	ENDED	
0	2018/07/12 06:02:00	1	0	1	
0	2018/07/12 06:03:00	0	1	2	
0	2018/07/12 06:04:00	2	0	2	
0	2018/07/12 06:05:00	2	1	0	
0	2018/07/12 06:07:00	1	2	1	
0	2018/07/12 06:08:00	0	2	1	
0	2018/07/12 06:08:00	1	2	1	
0	2018/07/12 06:07:00	2	2	2	
0	2018/07/12 06:10:00	3	2	2	
0	2018/07/12 06:12:00	1	0	3	

You can refer to Timechart Multiple Aggregation without Grouping for more details.





Sankey chart

Sankey chart is a flow diagram used to depict a flow from one set of values to another. The connected values are called **nodes** and the connections are called **links**. It displays the corresponding grouping parameters on top of each node of the chart. The width of the link shows the magnitude of the flow. Colors are used to divide the diagram into different nodes or to show the transition from one state of the process to another.

Use the Sankey chart to show a **many to many** mapping between two or more nodes. The **aggregation parameter** is used to define the width of the flow between a source node and the destination node.

Example:

```
| process geoip(source_address) as country | chart count() by country,
severity, category, sub_category
```



Response Types Supported

The **Sankey** chart supports a single aggregation response types for representation of search results in the visualization. It is :

Response Type	General Syntax			
Single Aggregation with Grouping	<pre> chart aggregation_parameter by grouping_parameter1, grouping_parameter2,, grouping_parametern</pre>			

Single Aggregation with Grouping

Example:





pro	oces rity	ss geoip(sourc , category, s	ce_address) a sub_category	s country	chart coun	t() by count	try,
	♦ ВАСК	process geoip(source_address) as c	ountry chart count() by country, sev	erity, category, sub_category		Use wizard All	
	Someth	ing is wrong !!				Add Sea	arch To 🔻 🔺 More 🔻 Chart 📗
							Sankey 🔻
	Country United Belgiu	States	severity		category		sub_category
	India		6		computer-and-internet-info		end
	null		nut				
	Austra China Indone Japan Nepal Appendi	a da ag Sonoa Cog	NTO 4 1 7 0 2 5		N		nd
1				Ä			
		country	severity	category	sub	o_category	count()
	Q	Belgium	6	computer-and-internet-into	end	1	3
	Q	Japan	2	null	null		6
	Q	Indonesia	0	null	null		6
	≪ ∢	Page 1 of 2 > ≫ 😂					Displaying 1 - 25 of 40

You can refer to Single Aggregation with Grouping for more details.

Operations

Vertical Reposition

You can change the vertical position of the nodes by dragging them in the upward or the downward direction. You can either overlap the nodes or place them distinctly.

Page 113/146



sls-en_dashboard_visualization_gde - 07/04/2024



Stacked Area Chart

Stacked Area charts are fundamentally similar to a standard Area Chart, except for the use of multiple variables in the x-axis instead of a single variable.



The following query gives the output shown above.

```
| chart count(), avg(sig_id) by action
```

Response Types Supported

The **Stacked Area** chart supports two aggregation response types for representation of search results in the visualization. They are:

Response Type	General Syntax
Multiple Aggregation with Grouping	<pre> chart aggregation_parameter1, aggregation_parameter2 by grouping_parameter1, grouping_parameter2,,grouping_ parametern</pre>
Timechart Multiple Aggregation without Grouping	<pre> timechart aggregation_parameter1, aggregation_ parameter2, aggregation_parametern</pre>

Multiple Aggregation with Grouping

In the Multiple Aggregation with Grouping response type, the x-axis contains the values of the grouping parameter(s), whereas the y-axis consists the scale to measure the value of the aggregation parameters. A unique color represents each aggregation parameter.

```
sent_datasize=* source_address=* | chart max(sent_datasize), max(received_
datasize) by source_ address order by max(sent_datasize), max(received_
datasize) desc limit 10`
```





You can refer to Multiple Aggregation with Grouping for more details.

Timechart Multiple Aggregation without Grouping

Example:

```
| timechart count(), avg(datasize)
```



You can refer to Timechart Multiple Aggregation without Grouping for more details.







Stacked Column Chart

A Stacked Column chart uses bars to show the comparisons between categories of data but with an ability to break down and compare parts of a whole. Each bar in the chart represents a whole, and segments in the bar represent different parts or categories of that whole.

Similar to the **Clustered Line Chart**, the y-axis represents value of the aggregation parameter, and the x-axis displays value of the timestamps.



The following query gives the output shown above.

| timechart count() by action

You can use this chart to display the following response type:

Response Types Supported

The **Stacked Column** chart supports a single aggregation response type for representation of search results in the visualization. They are:

Response Type	General Syntax			
Timechart Single Aggregation with Grouping	<pre> timechart aggregation_parameter by grouping_ parameter1, grouping_parameter2,, grouping_ parametern</pre>			

Timechart Single Aggregation with Grouping

Example:

source_address=* | timechart count() by source_address





🚺 NOTE

If the search result contains a large number of data points (more than 50) or groups (more than 20), switching from the Clustered Line to Stacked Column consumes a large amount of CPU resources. In this case, SLS displays the following message.

♦ BACK	timechart count() by action		Use wizard All 👻 LAST 10 MINUTES 👻 SEARCH
S Found	203,901 logs		🕼 Add Search To 👻 🔺 More 👻 🛛 Timechart 📗
Interval:	l hour	Chart contains large number of data points or groups. This can make browse	Stacked Column ▼
	Timestamp	action	count()
Q	▼ ≥ 2018/07/11 09:00:00		
Q	- 2		569
Q	- 10	indexing speed	268
Q	- 1	reporting speed	1,832
Q		live search	160
Q	▼ ≥ 2018/07/11 10:00:00		
Q	- 10	denied	53
0	B		3 174

You can refer to Timechart Single Aggregation with Grouping for more details.





TreeMap Chart

The **TreeMap** chart visualizes the hierarchical structure of a tree diagram. It displays the weight of each node in the form of the area size. Each node is assigned a rectangular area with their child nodes nested inside. The space of each node inside a parent node is displayed with proportion to all other nodes within the same parent node. If the weight of a child node is zero, the node is not included in the diagram.



The following query gives the output shown above.

```
source_address=* action=* | chart count() by source_address, action order
by count() desc limit 10
```

The first grouping parameter is the parent node of a TreeMap diagram, and all its successive parameters are the child nodes.

The name of the first grouping parameter is displayed in the breadcrumb, while all its fields are displayed in the containers as individual nodes.

Response Types Supported

The **Treemap** chart supports a single aggregation response types for representation of search results in the visualization. It is :

Response Type	General Syntax
Single Aggregation with Grouping	<pre> chart aggregation_parameter by grouping_parameter1, grouping_parameter2,, grouping_parametern</pre>

Single Aggregation with Grouping

Example:



sour by co	ce_a ount	ddress=* action=* cha () desc limit 10	art count()	by source	e_address, act	ion order
	♦ BACK	source_address=* action=* chart count() by source_add	ress, action order by coun	t() desc limit 10	Use wizard All	▼ LAST 10 MINUTES ▼ SEARCH
	Found	1,209 logs	Brea	adcrumb	Adv	I Search To 👻 🗼 More 👻 Chart 📳 🛄 TreeMap 👻
	source_a	ddress				
	10.94.2.9	4				
	0.0.0.0		10.45.3.252			
			10.45.3.77	10.45.3.241		
				10,45.3.198	10.45.3.25	
					10.45.3.245	10.94.0.254
	_	source address	action	Container	count()	
	Q	0.0.0	denied	Container	58	
	Q	10.94.2.94	performed		43	
	Q	10.94.2.94	read		37	
	Q	10.45.3.252	denied		36	
	Q	10.45.3.77	denied		24	
	Q	10.45.3.241	denied		16	
	Q	10.45.3.25	denied		12	
	Q	10.45.3.198	denied		12	
	Q	10.45.3.245	denied		6	
	Q	10.94.0.254	read		3	
	« < I	Page 1 of 1 > >> C				Displaying 1 - 10 of 10

NOTE

The aggregation parameter determines the area size of each node in the container.

You can refer to Single Aggregation with Grouping for more details.

Rendering Parameters

Click the **gear** icon on the right side of the breadcrumb to select the rendering parameters for the nodes of the treemap chart.







♦ BACK	source_address=* action=* chart count() by source_ad	dress, action order by count() desc lin	nit 10	Use wizard All 👻 LAS	ST 10 MINUTES 👻	SEARCH
Found 1	,243 logs			Add Search To	👻 🌟 More 👻	Chart
						TreeMap 🔻
source_ad	idress					0
10.94.2.94						7 190
0.0.0.0						
		10.45.3.77 10.45.3.241	10.45.3.198			
				10.45.3.25	10.45.3.245	
					10.94.0.254	
		*				
	source_address	action		count()		
Q	source_address	action denied		count() 57		
م م	source_address 0.0.0.0 10.94.2.94	action denied performed		count() 57 44		
৫ ৫ ৫	source_address 0.0.00 10.94.2.94 10.45.3.252	action denied performed denied		count() 57 44 38		

You can choose one of the following type in the rendering parameters

denied

1. Single

Q

10.45.3.77

- 2. Unique
- 3. Gradient

If the **Single** type is selected, all the nodes in the container are represented by a single color. You can also select the color to represent the nodes from the **Color** picker tool.

	RE	NDERING PARAME	ETERS							
	Тур	be:	Single			-				
	Co	lor:	#d4cde1			-				
				Submit	Can	cel				
÷	BACK	source_address=* action=*	* chart count() by source_ad	ddress, action order by	count() desc limit	10	Use wizard	All 👻 LAST 10	MINUTES 👻	SEARCH
۲	Found 1	,243 logs					0	Add Search To 👻	🔺 More 👻	Chart
										TreeMap 🔻
	source_ad	idress								
	10.94.2.94									
•				10.45.3.252						
				10.45.3.77		10.45.3.241				
									10.45.3.245	
									10.94.0.254	
_					Ā					
		source_address		action			count()			
Q		0.0.0.0		denied			57			
۹		10.94.2.94		performed			44			
۹		10.45.3.252		denied			38			
Q		10.94.2.94		read			37			
0		10.45.3.77		denied			24			





sls-en_dashboard_visualization_gde - 07/04/2024



If the **Unique** type rendering parameter is selected, all the nodes in the container are represented by a unique color. The colors are chosen randomly by the SLS itself.

RENDERING PARAMETERS					
Туре:	Unique		-		
		Submit	Cancel		

If you select the **Gradient** type rendering parameter, the **Color High** represents the node with the most significant area size and **Color Low** represents the node with the least area size.

RENDERING PARAMETERS				
Туре:	Gradient		Ψ.	
Color Low:	#d4cde1		×	
Color High:	#6E4B7C		Ŧ	
		Submit	Cancel	

Each section has a defined color, and different shades of color represent all the nodes of the division. The darkest shade represents the node with the most significant area size, and the shade of the color fades as the area size of the nodes decrease.

You can select the color for the nodes of high area value and low area value from **Color High** and **Color Low** drop-down menu respectively.

♦ BACK	← BACK source_address=* action=* chart count() by source_address, action order by count() desc limit 10				O MINUTES 👻	SEARCH
S Found	1,243 logs			🚯 Add Search To 👻	🔺 More 👻	Chart
						TreeMap 🔻
1011000	nel danas					
source_a	5541939					
10.94.2.9						
0.0.0.0		10.45.3.252				
		10.45.3.77	10 45 3 241	10.45.3.198		
					10.94.0.254	
	source address	action		count()		
Q	0.0.0.0	denied		57		
Q	10.94.2.94	performed		44		
-						
Q	10.45.3.252	denied		38		
Q	10.94.2.94	read		37		
Q	10.45.3.77	denied		24		







Operations

Zoom In and Zoom Out

The Zoom In feature allows you to click any node of the container and expand the chart further.

♦ BACK	source_address=* action=* chart count() by source_ad	dress, action order by cou	nt() desc limit 10		Use wizard All 👻 LAST		SEARCH
S Found	1,243 logs				🚯 Add Search To 👻	🔺 More 👻	Chart
							TreeMap 🔻
source_a	ddress						0
10.94.2.9	4						
0.0.0.0		10.45.3.252					Θ
		10.45.3.77	10.45.3.252: 38	5.3.241	10.45.3.198		
					10.45.3.25	10.45.3.245	
						10.94.0.254	
			*				
	source_address	action	_		count()		
Q	0.0.0.0	denied			57		
Q	10.94.2.94	performed			44		
Q	10.45.3.252	denied			38		
Q	10.94.2.94	read			37		
Q	10.45.3.77	denied			24		

The expanded diagram displays the nodes of the successive grouping parameter associated with the selected parent node. The new node is shifted to the breadcrumb, and the container is updated with the fields of the node in the breadcrumb.

For example: In the diagram above, when the user clicks **source_address**10.45.3.252, it is shifted to the breadcrumb and all its related fields are displayed in the container.

♦ BACK	<pre>source_address=* action=* chart count() by source_address,</pre>	Use wizard All 👻 LAST 10 MINUTES 👻 SEARCH	
Found 1	,243 logs		🕒 Add Search To 👻 🖌 More 👻 🛛 Chart 📗
			TreeMap 🗢
10.45.3.2			
denied			
		*	
	source_address	action	count()
Q	0.0.0.0	denied	57
Q	10.94.2.94	performed	44
Q	10.45.3.252	denied	38
Q	10.94.2.94	read	37
Q	10.45.3.77	denied	24

With the Zoom Out feature, you can go back to the previous state of the diagram by clicking the breadcrumb.





World Map Chart

A World Map is a map of a country, a continent, or a region, with colors and values assigned to specific regions. Values are displayed as a color scale, and you can see the name of the country by hovering over a particular part.



The following query gives the output shown above.

```
| process geoip(destination_address) as country_name | chart count(), avg
(datasize) by country_name, action
```

Response Types Supported

The **World Map** chart supports two aggregation response types for representation of search results in the visualization. They are:

Response Type	General Syntax
Single Aggregation with Grouping	<pre> chart aggregation_parameter by grouping_parameter1, grouping_parameter2,, grouping_parametern</pre>
Multiple Aggregation with Grouping	<pre> chart aggregation_parameter1, aggregation_parameter2 by grouping_parameter1, grouping_parameter2,, grouping_ parametern</pre>

Single Aggregation with Grouping

In Single Aggregation with Grouping, the color shade on each region of a World Map displays the value of the aggregation parameter, i.e., higher the value of the aggregation parameter, darker the color.

Example:



pro	oces try_	s geoip(destination_addre name, action	ss) as country_name ch	art count() by
	€ ВАСК	process geoip(destination_address) as country_name chart co	ount() by country_name, action	Use wizard All 👻 LAST 10 MINUTES 👻 SEARCH
	Found 1	36,784 logs		🕒 Add Search To 👻 🔺 More 👻 🛛 Chart 📗
	0	5226		Wold Map •
		country_name	action	count()
	Q	null	null	42544
	Q	Brazil	null	129

Some notable points about the World Map:

- 1. Sections of a graph are only clickable if they have some value of aggregation parameter and the search query contains two or three grouping parameter meaning that you cannot click and further drill-down the chart for a query with one grouping parameter or more than three grouping parameters.
- 2. For search queries with a single aggregation parameter and two grouping parameters, you can view a Donut chart by clicking on any region of a World Map (with some value for the aggregation parameter).





3. For search queries with a Single aggregation parameter and three grouping parameters, you can view a Heatmap by clicking on any region of a World Map(with some value for the aggregation parameter).



🚺 NOTE

You can drill-down operations from these sub-charts.

You can refer to Single Aggregation with Grouping for more details.

Multiple Aggregation with Grouping

In Multiple Aggregation with Grouping, the color shade on each region of a World Map displays the value of the first aggregation parameter, i.e., higher the value of the aggregation parameter, darker the color. The values of all other successive aggregation parameters can be viewed using the sub-charts.

Example:

```
| process geoip(destination_address) as country_name | chart count(), avg
(datasize) by country_name, action
```

Page 125/146







NOTE

- 1. The value of the first grouping parameter can only be depicted in the chart if the search query contains only one grouping parameter. However, the value can be viewed from the **Search Table**.
- 2. Sections of a graph are only clickable if they have some value of aggregation parameter and the search query contains two or three grouping parameters. Thus, you cannot click and further drill-down the chart for a query with one grouping parameter or more than three grouping parameters.
- 3. For search queries with multiple aggregation parameters and two or three grouping parameters, you can view a Clustered Column chart by clicking on any region of a World Map (with some value for the aggregation parameter).







1 NOTE You can further drill down from these charts.

You can refer to Multiple Aggregation with Grouping for more details.

Rendering Parameters

Click the gear icon at the top right corner of the World Map to open the rendering parameters panel.

The Rendering Parameters such as **Country**, **Positive Value**, and **Negative Value** provide a custom settings option to view data in different formats.

Through the **Country** option, you can specify the grouping parameter containing the names of the countries. Whereas, the **Positive Value** and **Negative Value** options allow you to select the color to represent the positive values of the aggregation parameter and the negative value of the aggregation parameter respectively.

RENDERING PARAMETERS				
country:	country_name		~	
Positive Value:	#D73232		Ψ.	
Negative Value:	#282323			
Reset		Submit	Cancel	

Page 127/146



sls-en_dashboard_visualization_gde - 07/04/2024



Operations

Pan and Zoom

The **Pan and Zoom** feature allows you to zoom in and out on a specific section on the world map and shift from one section to another.



Page 128/146



sls-en_dashboard_visualization_gde - 07/04/2024



Drilldown from Search Visualization

SLS provides a number of options for search result visualization. While visualizing the search results or the content of a widget, it is possible to dive deeper into the results by clicking the graphical representation. For example, while viewing a search result which includes the fields such as **destination_address**, **destination_port**, **source_address**, and **source_port** in the search query, it is possible to drill down to the results based on these parameters. Use the keys from the original query to drill down.

Common Features of Drill-down

Depending on the original query chosen to drill down from, the contents in the drill-down context menu varies. There are 3 types of drill-down options in SLS visualization:

- 1. Filter
- 2. Drilldown by
- 3. Top 10 drilldown by

The **Filter** type drill-down searches on the **Range**, the **Field**, and the **count()**. The **Drilldown by** and the **Top 10 drilldown by** types drill down on the **fields** and the **labels** respectively.

For example:

destination address=* source port=* destination port=* source address=*

While performing drill-down from this query, the following context menu appears on the screen. It lists all three possible sections in a drill-down context menu.







1. Filter

This section contains the following components depending on the original query:

- **Range**: Displays the subset of the time-period from which you have chosen to drill-down. It is only displayed for queries containing the timechart command or logs plotted in a time series manner.
- count(): Total number of logs.
- View Logs: Lets you view the drilled-down logs. You can view them in the same or a new window by clicking View Logs in the context menu for the given time-range.

🚺 NOTE

By default, the **Drilldown on full result set** slider and **count()** are disabled (grayed out).

2. Drilldown by

This section contains the fields or labels present in the original query.

3. Top 10 Drilldown by

This section contains the fields or labels present in the original query.

Besides these, the context menu also contains some other options for the following.

Filter				
Range: 2018/07/12 06:51:23	To 2018/07	7/12 07:01:23		
count(): 2				
View Logs	Drill down on full result set (enable/disable)			
Drilldown by				
destination_address			1	
source_port		Open in new Window	\rightarrow	ß
destination_port			-	⊠ Op
source_address				
Top 10 drilldown by				
destination_address				
source_port				
destination_port				
source_address				

Drilldown on Full Result Set

It is possible to drill down on the full result. The slider icon present next to the **Range** value lets you drill down on the full result set in addition to the subset.

Open drilldown in a New Window





While performing drill-down, it executes in the same window by default. However, you can click the **Open in New Window** icon to open the results in the new window.

Demonstration of Customizable Drilldown from Search Visualization

Consider the following search query:

```
device_ip=* device_name=* col_type=* source_address = 10.94.2.94
```

This query displays the following visualization.



SLS's search result drill-down actions let you dive deeper into the details of the information presented in the visualization. If you hover over the search graph, the related information of the selected area is summarized in a tooltip.



Click the highlighted section of the result.





Filter	
Range: 2018/07/12 07:17:00 To 2018/07/12 07:18:00	O C
count(): 22	
View Logs	
Drilldown by	
device_ip	
device_name	
col_type	
source_address	
Top 10 drilldown by	
device_ip	
device_name	
col_type	
source_address	

In the context menu, enable or disable the drill-down on the **Range** value by clicking the slider icon. The corresponding search visualization for the **Range** is shown below:







Filter	
Range: 2018/07/12 07:14:00 To 2018/07/12 07:44:00	•
count(): 26	
View Logs	
Drilldown by	
device_ip	
device_name	
col_type	
source_address	
Top 10 drilldown by	
device_ip	
device_name	
col_type	
source_address	

€ BA	ck device_ip=* device_name=* col_type=* source_address = 10.94.2.94 timechart count()	Use wizard All 🗢 2018/07/12 07:14:00 TO 2018/07/12 07:44:00 👻 SEARCH
🕑 For	und 491 logs	🕼 Add Search To 👻 🛛 📩 More 👻 🛛 Timechart 📗
Interva	al: 1 minute 🔐 Normal 🔐 Cumulative Show/Hide Trendline: 🗌	Column 🔻
90		€ ∎ count()
50		
30 10		na dha an Inn a' shekara a she
	07:13 AM 07:15 AM 07:20 AM 07:25 AM 07:30 AM	07:35 AM 07:40 AM
	JUIY 14, 2016	
	Timestamp	count()
Q	2018/07/12 07:14:00	2
Q	2018/07/12 07:15:00	11
Q	2018/07/12 07:16:00	14
Q	2018/07/12 07:17:00	22
Q	2018/07/12 07:18:00	18
Q	2018/07/12 07:19:00	22
Q	2018/07/12 07:20:00	10
Q	2018/07/12 07:21:00	18
Q	2018/07/12 07:22:00	2
Q	2018/07/12 07:23:00	8







Filter	
Range: 2018/07/12 07:30:00 To 2018/07/12 07:31:00	0 6
count(): 26	
View Logs	
Drilldown by	
device_ip	
device_name	
col_type	
source_address	
Top 10 drilldown by	
device_ip	
device_name	
col_type	
source_address	

€ В∕	CK	Use wizard All - 2018/07/12 07:30:00 TO 2018/07/12 07:31:00 - SEARCH
🕑 Fo	und 26 logs	🕒 Add Search To 👻 🔺 More 👻 🛛 Logs 📗
Histog	ram III Interval: 5 seconds III Normal all Cumulative Show/Hide Trendline:	Column 👻
14 12 10 8 6 4 2		■ counti)
	07:30:00 AM 07:30:05 AM 07:30:10 AM 07:30:15 AM 07:30:20 AM 07:30:25 AM 07:30:30 AM July 12, 2018	07:30:35 AM 07:30:40 AM 07:30:45 AM 07:30:50 AM
Interesting Fields	2018/07/12 07:30:37 Access Successful log_ts=2018/07/12 07:30:37 device_ip=127.0.0.1 \ device_name=localhost \ col_type=filesystem \ source_address= repp_name=_logpoint \ status_code=200 \ col_tr=2018/07/12 07:30:37 \ collected_at=LogPointP1 \ data5ize=3703 protocol_version=2.0 \ refore=https://10.45.3.91/ \ request_method=GET \ resource=/data7_dc=1531380628113& \ 10.44.294 - [12/Jul/2818:07:30:27 +0000] "CET / data7_dc=1531380628113&requestData=%78%22search_df2%22%3A% 9e8c3cda1520%22%2C%22secn_version%22%3A0%7D&is_dashboard=false&CSRFToken=b2b8e942-b818-4b1a-91b0-258 1531378664.88&LOGGEDINUSER=William HTTP/2.0* 200 3703 "https://10.45.3.91/" "Mozilla/5.0 (Macintosh; Intel Mac O * 0.080	+10.94.2.94 v sig_id=21500 v source_name=/var/log/nginx/access.log v < duration=0.080 v logpoint_name=LogPoint91 v norm_id=WCL v protocol=HTTP v < user_agent=Mozilla/5.0 (Macintosh; Int v 22217911a=8317-4(d-b409- 490ccfc29- 5 X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36
	<pre>« < 1 of 38 pages > >></pre>	Displaying 1-25 of 939 logs 👔 Display maximum: 25 🔹 logs per page

Click **View Logs** to see the corresponding log results. The results can be viewed in the same window or in a new one.



Filter	
Range: 2018/07/12 07:30:00 To 2018/07/12 07:31:00	0 6
count(): 26	
View Logs	
Drilldown by	
device_ip	
device_name	
col_type	
source_address	
Top 10 drilldown by	
device_ip	
device_name	
col_type	
source_address	

€ В,	ACK device_ip=* device_name=* col_type=* source_address = 10.94.2.94	Use wizard All 🗢 2018/07/12 07:30:00 TO 2018/07/12 07:31:00 🗢 SEARCH
🔿 F	ound 26 logs	🕼 Add Search To 👻 🛛 🌟 More 👻 🗌 Logs 📗
Histo	gram III Interval: 5 seconds I III Normal III Cumulative Show/Hide Trendline:	Column 💌
14		(b) County
12		
10		
6		
4		
2		
	07:30:00 AM 07:30:05 AM 07:30:10 AM 07:30:15 AM 07:30:20 AM 07:30:25 AM 07:30:30 AM	07:30:35 AM 07:30:40 AM 07:30:45 AM 07:30:50 AM
	July 12, 2018	
	Ā	
Intel	2018/07/12 07:30:37 Access Successful	
resting Fiel	log_ts=2018/07/12 07:30:37 v device_ip=127.0.0.1 v device_name=localhost v col_type=filesystem v source_address= repo_name=_logpoint v status_code=200 v col_ts=2018/07/12 07:30:37 v collected_at=LogPoint91 v datasize=3703 v protocol_version=2.0 v referer=https://10.45.3.91/ v request_method=GET v resource=/data?_dc=1531380628113& v	<pre>r10.94.2.94 ∨ sig_id=21500 ∨ source_name=/var/log/nginx/access.log ∨ / duration=0.080 ∨ logpoint_name=LogPoint91 ∨ norm_id=WCL ∨ protocol=HTTP ∨ / user_agent=Mozilla/5.0 (Macintosh; Int ∨ </pre>
lds	10.94.2.94 [12/Jul/2018:07:30:27 +0000] "GET /data?_dc=1531380628113&requestData=%78%22search_id%22%3A% 9e8c3cda1b20%22%2C%22seen_version%22%3A0%7D&is_dashboard=false&CSRFToken=b2b8e942-b818-4b1a-91b0-258 1531378664.88&LOGGEDINUSER=William HTTP/2.0" 200 3703 "https://10.45.3.91/" "Mozilla/5.0 (Macintosh; Intel Mac O " 0.080	:223f79f1ae-83f7-4cl4-b409- 490ccfc29- /S X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36
	≪ K 1 of 38 pages > ≫	Displaying 1-25 of 939 logs 🚯 Display maximum: 25 💌 logs per page

Click the required **Field-values** in the **Drilldown by** section to see the corresponding search results. The results can be viewed in the same window or in a new one.





Click the **device_ip** in the **Drilldown by** section to append **chart count() by device_ip order by count() desc** in the search query. The search result can be viewed in the same window or in a new one.

```
device_ip=* device_name=* col_type=* source_address = 10.94.2.94 | chart
count() by device_ip order by count() desc
```

Click the required **labels** in the **Top 10 drilldown by** section to see the corresponding search results. These results can be viewed in the same window or in a new one.





Filter		3			
Range: 2018/07/12 07:30:00 To 2018/07/12 07:31:00	0	3			
count(): 26		3			
View Logs		3			
Drilldown by					
device_ip		3			
device_name		3			
col_type		3			
source_address		3			
Top 10 drilldown by					
device_ip		3			
device_name		3			
col_type		2			
source_address		3			
BACK [device_ip=* device_name=* col_type=* source_address = 10.94.2.94 chart count() { Found 26 logs	by device_ip order b Use wizar	d All 🗢 2018/07/	12 07:30:00 TO 2018/07/12 0	7:31:00 ▼	SEARCH
6					count()
2					
4 0					
° 2 127.0.0.1					
device_ip	count()				
127.0.0.1	26				

Click device_ip in the Top 10 Drilldown by section to append | chart count() by device_ip order by count() limit 10 desc to the search query. Choosing device_ip results in the following query.

```
device_ip=* device_name=* col_type=* source_address = 10.94.2.94 | chart
count() by device_ ip order by count() desc limit 10
```

Similarly, the search results can be drilled down on the basis of the **source_port**, **destination_ port**, and the **source_address**.

The search result can be further drilled down by clicking any part of the result set.

```
device_ip=127.0.0.1 device_name=* col_type=* source_address = 10.94.2.94 |
chart count() by device_ name order by count() desc
```



Special Drilldown Scenarios

Filter Drilldown

Example 1

For **Filter Drilldown**, if you drill down on the **Range** and open the results in the same page, the search is executed in the selected time-range. If you open the search in a new window, it is executed in the selected time-range with **| timechart count()** appended to it. The command is appended only for simple queries.



Select a bar to drill down from. The following context menu appears.

Filter	0
Range: 2018/07/12 07:11:00 To 2018/07/12 07:13:00	0 🖉
count(): 220	
View Logs	

Once you drill down, you can see results similar to the following example.









For the filter type, when the drill-down is executed on **Field**, search is executed with **| filter** <**field**> = <**value**>

Consider the following query:

action=*|chart count() by action

The following visualization appears.

♦ ВАСК	action=* chart count() by action		Use wizard	All 🔻 LAST 10 MINUTES 👻 SEARCH
S Found	795 logs		Add	Search To 👻 🌟 More 💌 Chart 📗
				block-url live search indexing speed deniad Login - Saicesful widhre-upload-skip alert reporting speed login forward deny alert reporting speed login forward deny alert read
	and a	*		
	action		county	
Q	block-url		22	
Q	live search		40	
Q	indexing speed		66	
Q	denied		13	

If you drill down on the reporting Speed, the following context menu appears.





sls-en_dashboard_visualization_gde - 07/04/2024



action: reporting speed	
count(): 576	
View Logs	
Drilldown by	
action	
Top 10 drilldown by	
action	

If you drill down on the **reporting speed**, the appended search query is:

action=* | chart count() by action | filter "action"="reporting speed"



Example 2

When the drill-down is executed on **count()** for the **Filter** type, the search is executed with | **search count()** = <**value**>. Consider the following example:

action=* | chart count() by action

The following visualization appears.





♦ BACK	action=* chart co	ount() by action								Us	e wizard	All 🔻 LAS	T 10 MINUTES 🔻	SEARCH
S Found 8	857 logs										🕒 Add	Search To 📼	🔺 More 👻	Chart
														Bar 🔻
													_	∎ count()
	_			action: reporting speed count(): 544										
	50	100	150	200	250	300	350		400	450	1	500	550	
						×								
	action							count()	†					
Q	reporting speed							544						
Q	indexing speed							65						
Q	live search							40						
Q	alert							35						

The context menu for this drilldown is:

-

Filter	8
action: reporting speed	
count(): 544	
View Logs	
Drilldown by	
action	
Top 10 drilldown by	
action	

When the drill-down is executed on **count(): 544**, the new appended query is:

```
action=*|chart count() by action | filter "count()" = 544
```





sls-en_dashboard_visualization_gde - 07/04/2024



Example 3

When the drill-down is conducted for <**empty_query**> | **chart count() by group**, the customizable drill-down options differ. Consider the following:

```
| chart count() by action
```

block-url

0

The following visualization appears.



40

Clicking drill-down for a bar opens up the following context menu. In this case, only the Filter section with **field, count()** and **View Logs** is displayed as shown.

Filter	0
action: reporting speed	C ²
count(): 554	C ²
View Logs	C

If you click "action: reporting speed", the new query becomes:

| chart count() by action | filter "action"="reporting speed"

If you click "count(): 544", the new query becomes:

| chart count() by action | filter "count()"=544

Drilldown by

For **Drilldown by**, when the drill-down is executed on **fields** or **label**, search is executed with the given query followed by | **chart count() by <field> order by count() desc**





For example:

```
action = denied
```



The following visualization appears. Hover over the required result and click to drill down.

In the Drilldown Context Menu, click action under the Drilldown by section.

Filter	
Range: 2018/07/12 13:39:26 To 2018/07/12 13:39:46	02
count(): 2	
View Logs	
Drilldown by	
action	
Top 10 drilldown by	

The search results of the drilldown appear.

Page 143/146





← BACK action=denied chart count() by action order by count() desc					Use wizard All 👻 LAST 10 MINUTES 👻 📑	SEARCH		
🔿 F	ound 2 logs				🕒 Add Search To 👻 🛛 🚖 More 👻 🛛 Cl	hart		
						Column 🔻		
						■ count0		
1.8					1	county		
14								
1.4								
1								
0.6								
0.2								
denied								
_			*					
	action			count()				
Q	denied			2				

New query:

```
action = denied| chart count() by action order by count() desc
```

Top 10 Drilldown by

For **Top 10 Drilldown by**, when you execute the drill-down on **field-values** or **label**, the search is executed with the given query followed by | **chart count() by <field> order by count() desc limit 10**.

Execute a query and click the search result visualization to dive deeper. In the context menu, click the field under the Top 10 Drilldown by section. The search result of the drill-down appears on the screen.

€ ВАСК	action=denied chart count() by action order b	Use wizard All 👻 LAST 10 MINUTES 👻 SEARCH						
Found	2 logs			🕒 Add Search To 👻 🔺 More 👻 Chart 📗 📰				
				Column 🔻				
				■ count()				
1.8								
1.4								
1								
0.6								
0.2								
denied								
		*						
	action		count()					
Q	denied		2					

New query:

```
action = denied | chart count() by action order by count() desc limit 10
```








Additional information and answers to questions you may have about SLS are available in the **Stormshield knowledge base** (authentication required).



sls-en_dashboard_visualization_gde - 07/04/2024





documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.

Copyright © Stormshield 2024. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.





sls-en_dashboard_visualization_gde - 07/04/2024