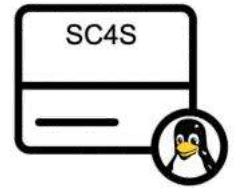


Splunk4Rookies - Splunk Connect for Syslog (SC4S)

Lab Guide



Containerized Syslog Appliance

Overview

This lab guide contains the hands-on exercises for the Splunk4Rookies - Splunk Connect for Syslog (SC4S) workshop and is a companion to the full workshop slides to assist you with configuration file contents and flow.

Before proceeding with these exercises, please ensure that you have a copy of the workshop slide deck, which will help to put into context the tasks you are carrying out.

Download the workshop slide deck: <https://splk.it/S4R-SC4S-Attendee>

Prerequisites

In order to complete these exercises, you will need your own Splunk instance. The presenter delivering your workshop will give you a unique URL for your event, which will allow you to register and create your own Splunk instance.

Please follow the steps provided by the presenter to get access to Splunk!

⚠ Troubleshooting Connectivity

If you experience connectivity issues with accessing either your workshop environment or the event page, please try the following troubleshooting steps. If you still experience issues please reach out to the team running your workshop.

- **Use Google Chrome** (if you're not already)
- If the event page (i.e. <https://show.splunk.com/event/<eventID>>) didn't load when you clicked on the link, try **refreshing the page**
- **Disconnect from VPN** (if you're using one)
- **Clear your browser cache and restart your browser** (if using Google Chrome, go to: Settings > Privacy and security > Clear browsing data)
- **Try using private browsing mode** (e.g. Incognito in Google Chrome) to rule out any cache issues
- **Try using another computer** such as your personal computer - all you need is a web browser! Cloud platforms like AWS can often be blocked on corporate laptops.

Table of Contents

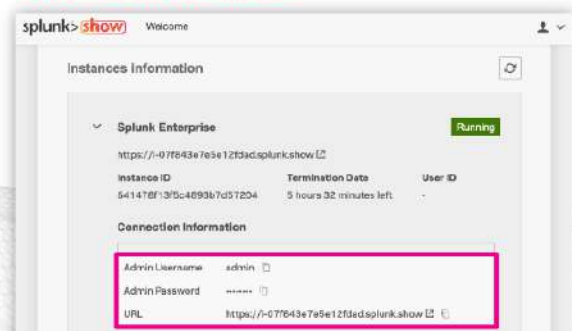
Table of Contents	2
Labs: SC4S 101	3
Lab 1: Setup Your Environment	3
Lab 2: Introduction to Search	8
Lab 3: InfoSec App for Splunk	9
Lab 4: Config Explorer	11
Lab 5: Set a Custom Index and Source	12
Splunk_metadata.csv contents:	13
Example search to check the changes have been applied:	13
Labs: SC4S 201	15
Lab 6: Set a Custom Filter	15
Lab 7: null_queue	18
Check Labs Dashboard	21

Labs: SC4S 101

Lab 1: Setup Your Environment

Login to Splunk

Locate your instance URL and credentials in the Splunk Show event
<https://show.splunk.com>



Scroll down the event page and expand the **Splunk Enterprise** section to view your login details

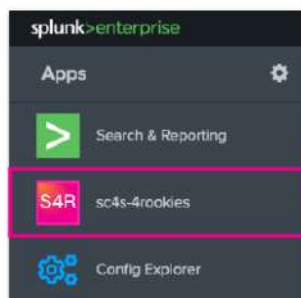
Log in to your Splunk instance



Login using the credentials from Splunk Show

splunk>

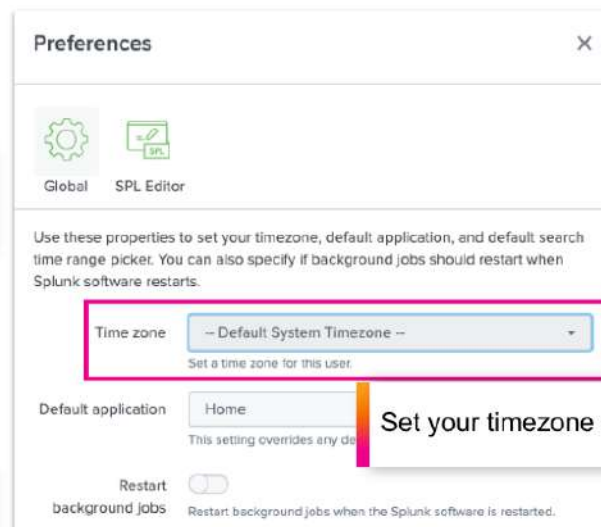
Login and Set Your Timezone



Click on the **sc4s-4rookies** app



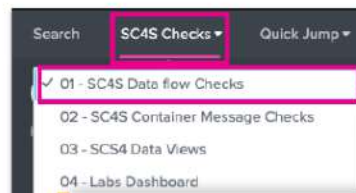
Open your user preferences



Set your timezone

splunk>

Check the Data Flow



Click on **SC4S Checks** and then on **01 - SC4S Data flow Checks**

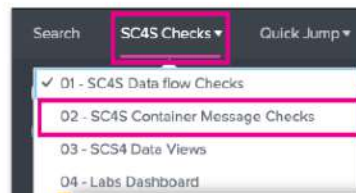
All inputs are turned off and the sc4s service is stopped after the initial image creation

You may see some historical data or blank graphs - this is normal



splunk>

Check the Data Flow



Click on **SC4S Checks** and then on **02 - SC4S Container Message Checks**

All inputs are turned off and the sc4s service is stopped after the initial image creation

You may see some historical data or blank tables - this is normal

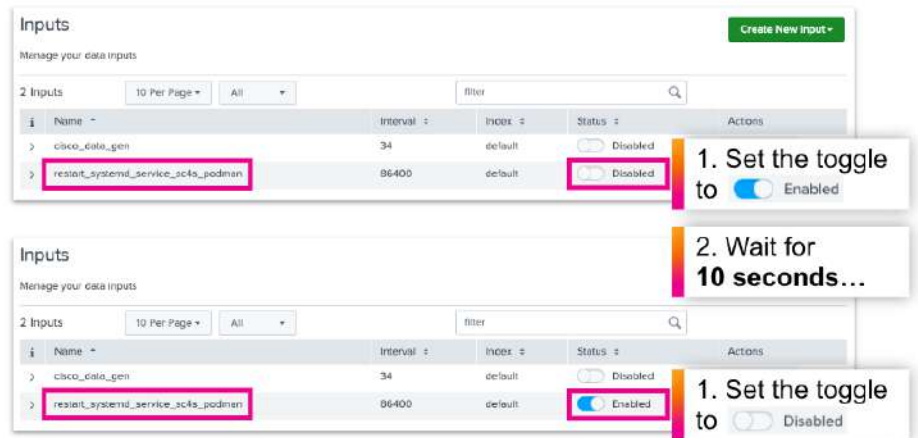
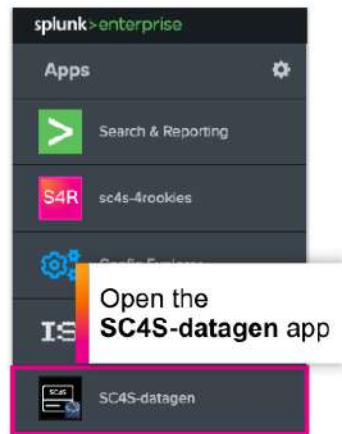
#	_time	sourcetype	_raw
1	2021-09-09T14:17:41+12:00	sc4s.events	2021-09-09T02:17:41.728+00:00 sc4s4rookies syslog-ng 104 - [meta:sequenceId="2"] syslog-ng starting up; version="3.32.1"
2	2021-09-09T14:17:36+12:00	sc4s.probe	HEC TEST EVENT
3	2021-09-09T14:17:36+12:00	sc4s.probe	HEC TEST EVENT
4	2021-09-09T14:17:30+12:00	sc4s.events	2021-09-09T02:17:30.695+00:00 sc4s4rookies syslog-ng 104 - [meta:sequenceId="276043"] syslog-ng shutting down; version="3.32.1"

splunk>



Restart the SC4S systemd Service

Restart the systemd service for podman and SC4S by enabling the input, waiting a few seconds, then disabling it again:

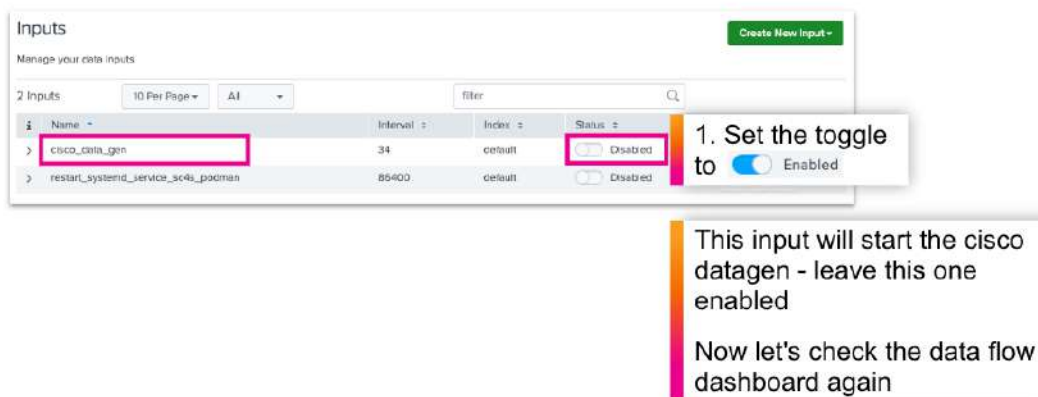


Note: In environments with CLI access you can also restart the service using the following command:

```
sudo systemctl restart sc4s
```

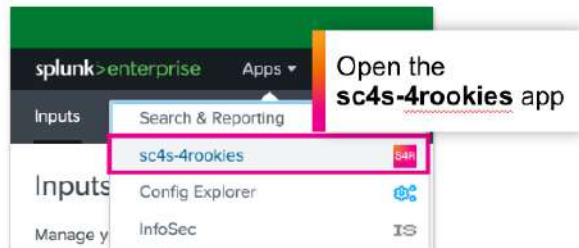
splunk>

Enable the Cisco Datagen



splunk>

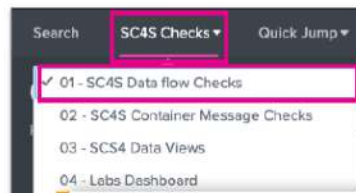
Go Back to the sc4s-4rookies App



splunk>

Check the Data Flow

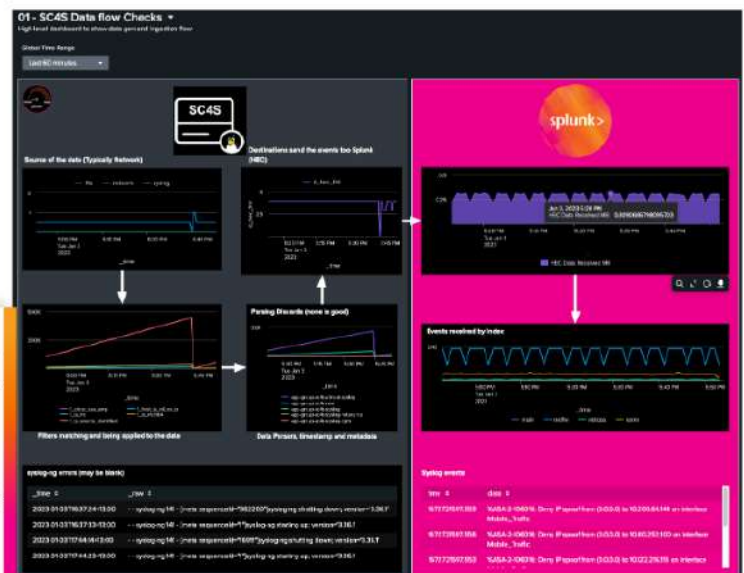
S4R sc4s-4rookies



Click on **SC4S Checks** and then on **01 - SC4S Data flow Checks**

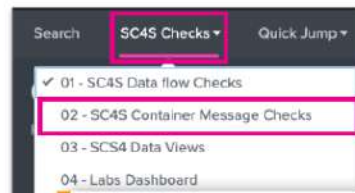
Now we have started the Cisco datagen you should see a steady flow of data start to populate your dashboard

The arrows indicate the flow of the events through your log paths and out to Splunk over HEC to the indexes



splunk>

Check the Data Flow



Click on **SC4S Checks** and then on **02 - SC4S Container Message Checks**

02 - SC4S Container Message Checks

Messages from "sc4sevents" or "sc4sgenerator"

Data-Time Range: Last 15 minutes

#	_time	_source	_type	_raw
1	2023-09-10T15:00:01.000	sc4sevents	sc4sevents	-- syslog-ng 143 - [meta sequenceid="1032670"]Server disconnected while sending HTTP request, url="https://127.0.0.1:8080/services/collector/event", error="Couldn't connect to server, worker_index="4, driver_id_hec="test", location=host generator dest_hec="5"
2	2023-09-10T15:00:01.000	sc4sevents	sc4sevents	-- syslog-ng 143 - [meta sequenceid="1032680"]Server disconnected while preparing messages for sending, trying again; driver_id_hec="test", location=host generator dest_hec="5"; worker_index="0, batch_size="10"
3	2023-09-10T15:00:01.000	sc4sevents	sc4sevents	-- syslog-ng 143 - [meta sequenceid="1032690"]Server disconnected while preparing messages for sending, trying again; driver_id_hec="test", location=host generator dest_hec="5"; batch_size="10"
4	2023-09-10T15:00:01.000	sc4sevents	sc4sevents	-- syslog-ng 143 - [meta sequenceid="1032694"]Just error sending HTTP request, url="https://127.0.0.1:8080/services/collector/event", error="Couldn't connect to server, worker_index="5, driver_id_hec="test", location=host generator dest_hec="5"
5	2023-09-10T15:00:01.000	sc4sevents	sc4sevents	-- syslog-ng 143 - [meta sequenceid="1032698"]Just error sending HTTP request, url="https://127.0.0.1:8080/services/collector/event", error="Couldn't connect to server, worker_index="7, driver_id_hec="test", location=host generator dest_hec="5"
6	2023-09-10T15:00:01.000	sc4sevents	sc4sevents	-- syslog-ng 143 - [meta sequenceid="1032699"]Server disconnected while preparing messages for sending, trying again; driver_id_hec="test", location=host generator dest_hec="5"; worker_index="2, batch_size="10, batch_size="10"
7	2023-09-10T15:00:01.000	sc4sevents	sc4sevents	-- syslog-ng 143 - [meta sequenceid="1032700"]Server disconnected while preparing messages for sending, trying again; driver_id_hec="test", location=host generator dest_hec="5"
8	2023-09-10T15:00:01.000	sc4sevents	sc4sevents	-- syslog-ng 143 - [meta sequenceid="1032701"]Just error sending HTTP request, url="https://127.0.0.1:8080/services/collector/event", error="Couldn't connect to server, worker_index="1, driver_id_hec="test", location=host generator dest_hec="5"
9	2023-09-10T15:00:01.000	sc4sevents	sc4sevents	-- syslog-ng 143 - [meta sequenceid="1032702"]Just error sending HTTP request, url="https://127.0.0.1:8080/services/collector/event", error="Couldn't connect to server, worker_index="5, driver_id_hec="test", location=host generator dest_hec="5"
10	2023-09-10T15:00:01.000	sc4sevents	sc4sevents	-- syslog-ng 143 - [meta sequenceid="1032703"]Server disconnected while preparing messages for sending, trying again; driver_id_hec="test", location=host generator dest_hec="5"; worker_index="8, batch_size="10"
11	2023-09-10T15:00:01.000	sc4sevents	sc4sevents	-- syslog-ng 143 - [meta sequenceid="1032704"]Server disconnected while preparing messages for sending, trying again; driver_id_hec="test", location=host generator dest_hec="5"; worker_index="0, batch_size="10"

Now we have restarted the sc4s service you should see some startup messages from syslog-ng from inside the container

(If not you may have disabled the sc4s restart input too quickly a few slides back - try that again!)

Lab 2: Introduction to Search

Q. How would you find DNS events that are NOT .google.com?

Possible answers:

dns NOT *.google.com


dns query!=*.google.com

NOT vs !=

For more information on the difference between NOT and != please see

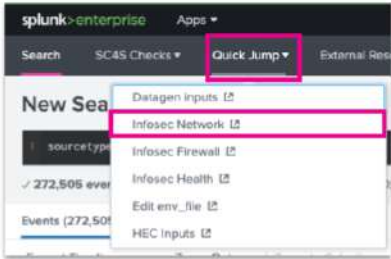
<https://docs.splunk.com/Documentation/Splunk/latest/Search/NOTexpressions>.

Lab 3: InfoSec App for Splunk



InfoSec App for Splunk: Examples

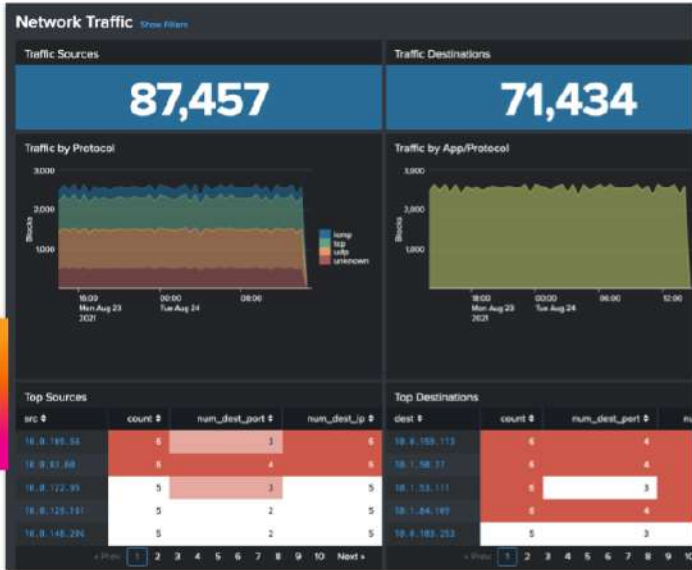
© 2023 SPLUNK INC.



The screenshot shows the Splunk interface with the 'Quick Jump' menu open. The 'Infosec Network' option is highlighted in the list.

Network Traffic


This dashboard provides visibility into your network traffic




The Network Traffic dashboard displays various metrics and charts. At the top, it shows 'Traffic Sources' with a count of 87,457 and 'Traffic Destinations' with a count of 71,434. Below these are two area charts: 'Traffic by Protocol' and 'Traffic by App/Protocol'. At the bottom, there are two tables: 'Top Sources' and 'Top Destinations'.

src #	count #	num_dest_port #	num_dest_ip #
10.0.100.54	6	3	6
10.0.101.40	5	4	6
10.0.122.95	5	3	5
10.0.123.191	5	2	5
10.0.148.226	5	2	5

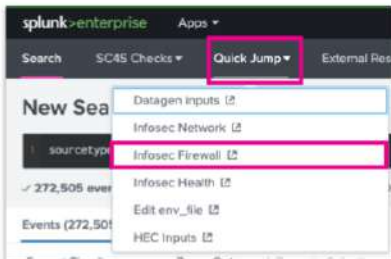
dest #	count #	num_dest_port #	num_dest_ip #
10.0.100.113	6	4	4
10.1.100.17	6	4	4
10.1.101.111	6	3	3
10.1.104.107	6	4	4
10.0.100.213	5	3	3





InfoSec App for Splunk: Examples


© 2023 SPLUNK INC.




The screenshot shows the Splunk interface with the 'Quick Jump' menu open. The 'Infosec Firewall' option is highlighted in the list.

Firewalls

Provides visibility into your firewalls, regardless of vendor or the presence of data from multiple vendors in the same environment.



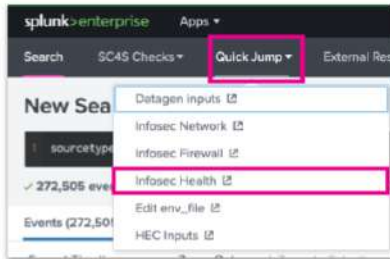
The Firewalls dashboard displays various metrics and charts. At the top, it shows 'Blocked Connections' with a count of 27,566, 'Allowed Connections' with a count of 70,168, and 'External Source IPs' with a count of 63,667. Below these are two area charts: 'Network Traffic by Action (Logarithmic Scale)' and 'Traffic by Protocol'. At the bottom, there is a world map showing 'Blocked Incoming Traffic by Destination Port'.





InfoSec App for Splunk: Examples

© 2023 SPLUNK INC.



Health


Provides visibility into your InfoSec Health.

InfoSec is built on top of Splunk's amazing CIM data models.



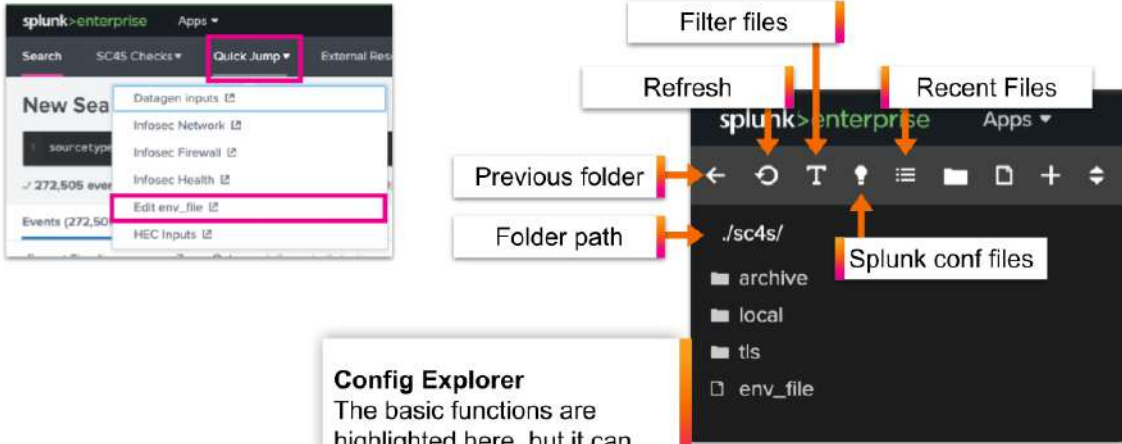
splunk>

Lab 4: Config Explorer




Config Explorer 101

© 2023 SPLUNK INC.



Config Explorer
The basic functions are highlighted here, but it can also do much more than this!

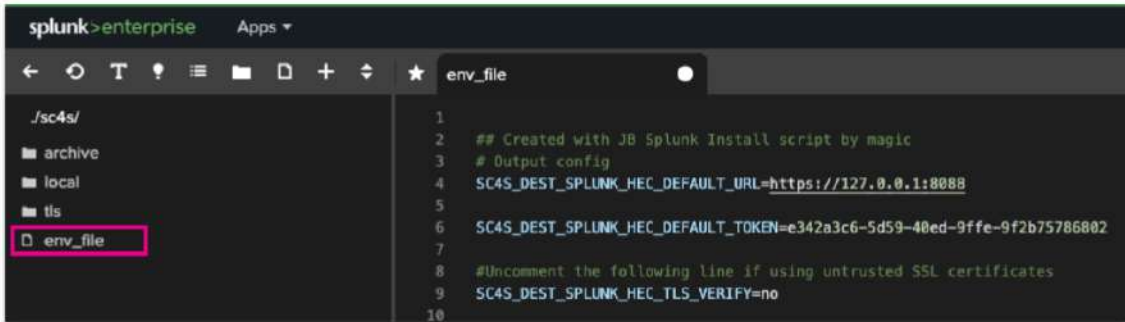
splunk>



Config Explorer 102

It's like Visual Studio Code, but in Splunk!

Click on the **env_file** to see the contents:



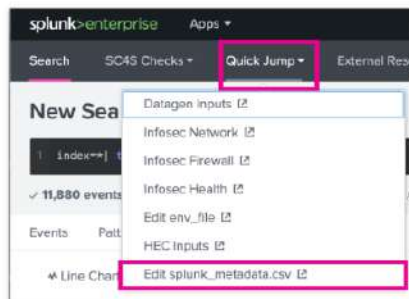
Learn more: <https://splunk.github.io/splunk-connect-for-syslog/main/configuration/#global-configuration>

splunk>

Lab 5: Set a Custom Index and Source

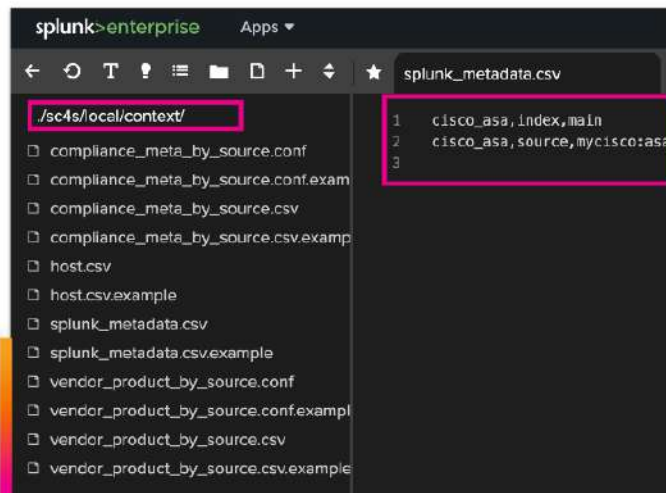
Edit splunk_metadata.csv

© 2023 SPLUNK INC.



As you can see the file is currently empty.

We are going to set some custom items, restart SC4S and enjoy the show!

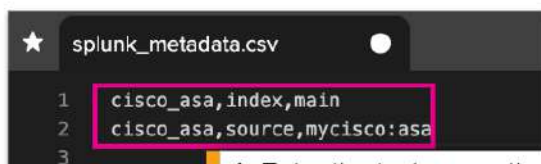


Learn more: <https://splunk.github.io/splunk-connect-for-syslog/main/configuration/#sc4s-metadata-configuration>

splunk>

Edit splunk_metadata.csv

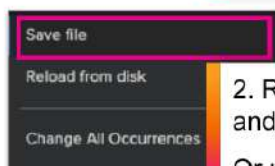
© 2023 SPLUNK INC.



1. Enter the text as per the screenshot to the left

change:

- index to main
- source to mycisco:asa



2. Right click in the window and select **Save file**

Or use **cmd+S** (Mac) or **ctrl+S** (Windows)

This configuration will take precedence over the default for the **cisco_asa** filter.

The default values of:

key = cisco_asa
metadata = index
value = **netfw**

key = cisco_asa
metadata = source
value = **cisco:asa**

will become:

key = cisco_asa
metadata = index
value = **main**

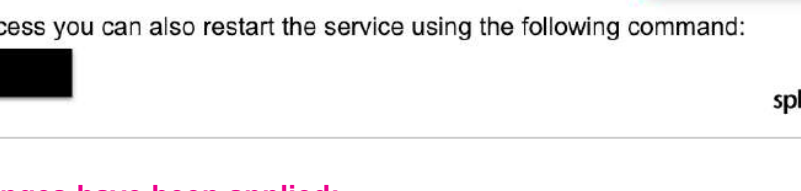


key = cisco_asa
metadata = source
value = **mycisco:asa**

Learn more: <https://splunk.github.io/splunk-connect-for-syslog/main/sources/Cisco/#product-asa-and-ftd-firepower>

splunk>

Splunk_metadata.csv contents:

```
cisco_asa,index,main
cisco_asa,source,mycisco:asa
```



Restart the SC4S systemd Service

Restart the systemd service for podman and SC4S by enabling the input, waiting a few seconds, then disabling it again:

Open the SC4S-datagen app


Note: In environments with CLI access you can also restart the service using the following command:

```
sudo systemctl restart sc4s
```

splunk>

Example search to check the changes have been applied:

```
index=main sourcetype=cisco:asa
```



Check the Changes Have Been Applied

Run the following Splunk search:

```
index=main
```

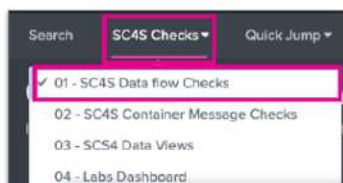
Our custom index

Our custom source

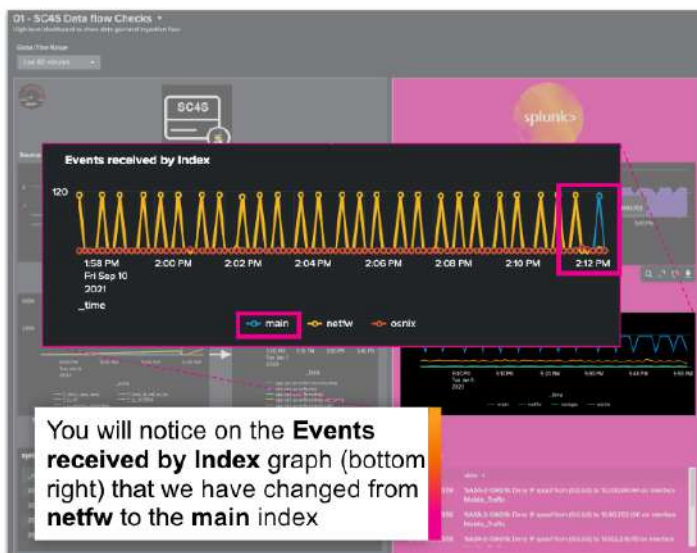
Learn more: <https://splunk.github.io/splunk-connect-for-syslog/main/configuration/#sc4s-metadata-configuration>

splunk>

Check the Index Change



Click on **SC4S Checks** and then on **01 - SC4S Data flow Checks**



You will notice on the **Events received by Index** graph (bottom right) that we have changed from **netfw** to the **main** index

splunk>

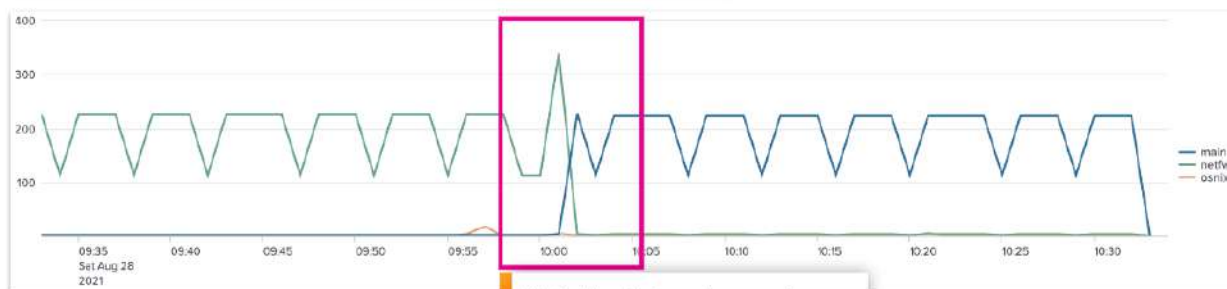
Example search to see index changeover:

`index=* | timechart count by index`

Check the Index Change

Run the following Splunk search:

```
index=* | timechart count by index
```



Note the index change here when we restarted SC4S

Learn more: <https://splunk.github.io/splunk-connect-for-syslog/main/configuration/#sc4s-metadata-configuration>

splunk>

Labs: SC4S 201

Lab 6: Set a Custom Filter

Filter and Enrich

The image shows two screenshots of the Splunk Enterprise interface. The left screenshot shows the 'Quick Jump' menu with 'Edit compliance_meta' highlighted. The right screenshot shows the 'compliance_meta_by_source.conf' file in the configuration editor, which is currently empty. A text box on the right explains that the file is empty and that custom items will be added.

As you can see the file is currently empty

We are going to set some custom items, restart SC4S and enjoy the show

Learn more:
<https://splunk.github.io/splunk-connect-for-syslog/main/configuration/#override-index-or-metadata-based-on-host-ip-or-subnet-compliance-overrides>

splunk>

Compliance_meta_by_source.conf contents:

```
filter f_sc4s {  
  host("192.168.12.*" type(glob)) or  
  netmask(192.168.12.0/24)  
};
```

Compliance_meta_by_source.csv contents:

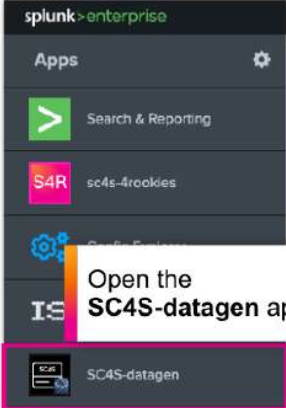
```
f_sc4s,fields.compliance,"pci"  
f_sc4s,fields.datacenter,"DC1"  
f_sc4s,fields.city,"Auckland"  
f_sc4s,fields.country,"New Zealand"  
f_sc4s,fields.lat,"-36.8509"  
f_sc4s,fields.lon,"174.7645"
```

SC4S-datagen


Restart the SC4S systemd Service

Restart the systemd service for podman and SC4S by enabling the input, waiting a few seconds, then disabling it again:


© 2023 SPLUNK INC.



Open the SC4S-datagen app



1. Set the toggle to Enabled



2. Wait for 10 seconds...

 1. Set the toggle to Disabled

Note: In environments with CLI access you can also restart the service using the following command:

```
sudo systemctl restart sc4s
```

splunk>

Example search to check events:

index=main

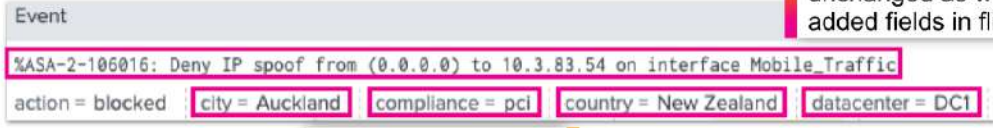
SC4S-datagen

Check the Changes Have Been Applied

© 2023 SPLUNK INC.

Run the following Splunk search:

```
index=main
```



Our custom fields

The raw event is unchanged as we have added fields in flight

Learn more:

<https://splunk.github.io/splunk-connect-for-syslog/main/configuration/#override-index-or-metadata-based-on-host-ip-or-subnet-compliance-overrides>

splunk>

Check the Changes Have Been Applied

index=main

Our custom fields

SELECTED FIELDS

a action 8
a city 1
a compliance 1
a country 1
a datacenter 1
a dest 100+
a host 1
a index 1
lat 2
lon 1

These ones look fun... what can we do with these?

city	1 Value, 100% of events		Selected	Yes	No
Reports					
Top values	Top values by time	Rare values			
Events with this field					
Values	Count	%			
Auckland	2,664	100%			

splunk>

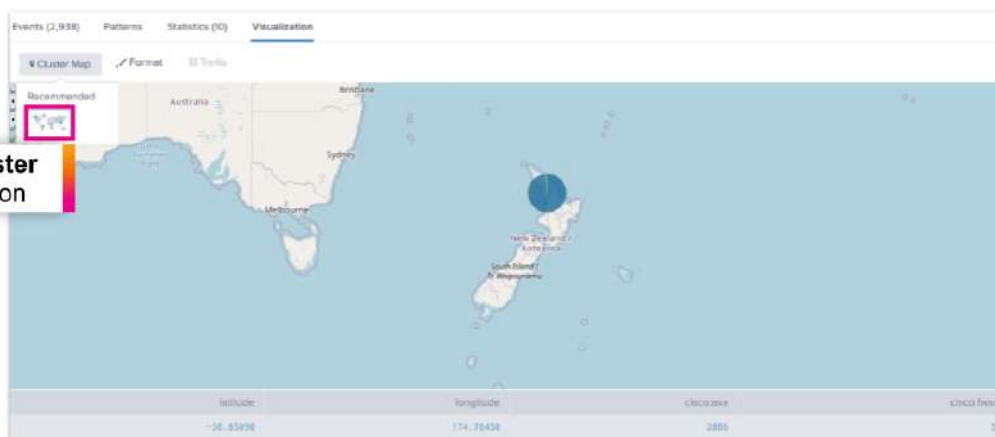
Example search to check events:

```
index=main sourcetype=*cisco*
| geostats count by sourcetype latfield=lat longfield=lon
```

Map It!

```
index=main sourcetype=*cisco*
| geostats count by sourcetype latfield=lat longfield=lon
```

Select the **Cluster Map** visualisation



Learn more:

<https://splunk.github.io/splunk-connect-for-syslog/main/configuration/#override-index-or-metadata-based-on-host-ip-or-subnet-compliance-overrides>

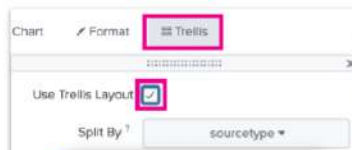
splunk>

Lab 7: null_queue

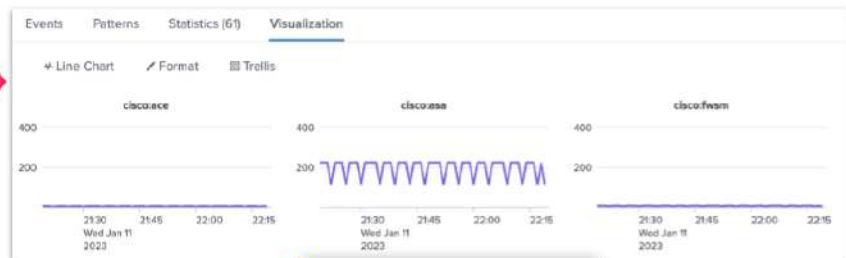
```
index=* host=192* sourcetype=*cisco*  
| timechart count by sourcetype
```

null_queue

```
index=* host=192* sourcetype=*cisco*  
| timechart count by sourcetype
```



Enable the trellis layout and split by **sourcetype**



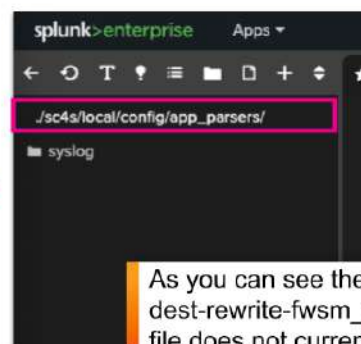
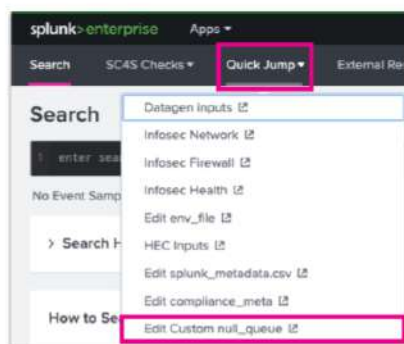
We are currently getting data from:

- ace
- asa
- fwsm

Learn more: <https://splunk.github.io/splunk-connect-for-syslog/main/configuration/#dropping-all-data-by-ip-or-subnet>

splunk>

null_queue



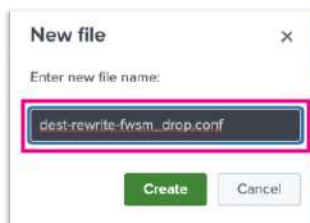
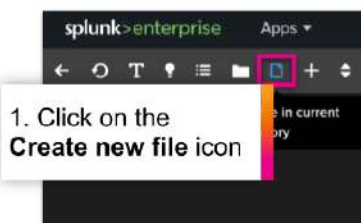
As you can see the `dest-rewrite-fwsm_drop.conf` file does not currently exist

We are going to create the file and its contents

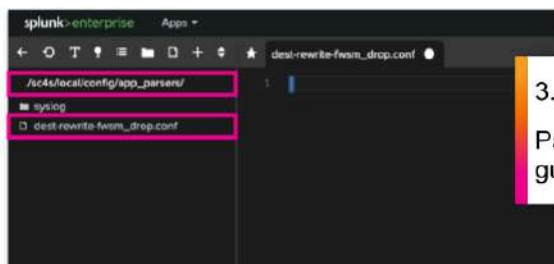
Learn more: <https://splunk.github.io/splunk-connect-for-syslog/main/configuration/#dropping-all-data-by-ip-or-subnet>

splunk>

null_queue



This file name is arbitrary but make sure it makes sense to you!



Learn more: <https://splunk.github.io/splunk-connect-for-syslog/main/sources/#filtering-events-from-output>

splunk>

dest-rewrite-fwsm_drop.conf:

```
# /opt/splunk/sc4s/local/config/app_parsers/dest-rewrite-fwsm_drop.conf

block parser fwsm_drop-postfilter() {
  channel {
    # In this case the outcome is drop the event
    rewrite(r_set_dest_splunk_null_queue);
  };
};

application fwsm_drop-postfilter[sc4s-postfilter] {
  filter {
    "${fields.sc4s_vendor}" eq "cisco" and
    "${fields.sc4s_product}" eq "fwsm"
    # Note regex reads as start from first position
    # Any atleast 1 char that is not a '-'
    # constant '-7-'
    # and message('^%[\^\\-]+-7-');
  };
  parser { fwsm_drop-postfilter(); };
};
```

Restart the SC4S systemd Service

Restart the systemd service for podman and SC4S by enabling the input, waiting a few seconds, then disabling it again:

1. Set the toggle to **Enabled**

2. Wait for **10 seconds...**

1. Set the toggle to **Disabled**

Note: In environments with CLI access you can also restart the service using the following command:

```
sudo systemctl restart sc4s
```

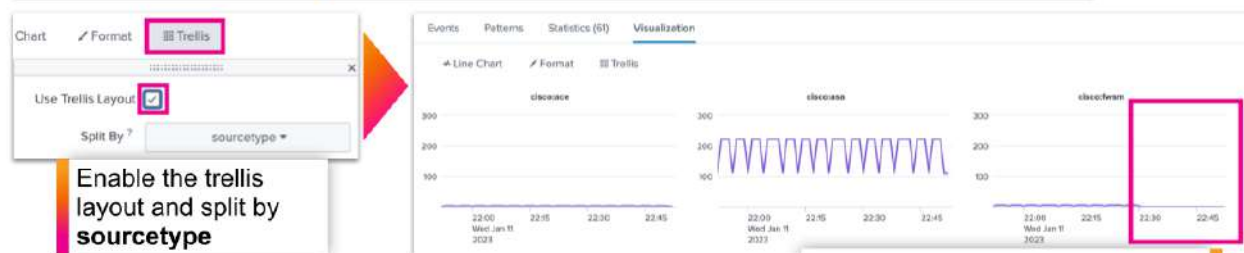
splunk>

Example search to check events:

```
index=* host=192* sourcetype=*cisco*
| timechart count by sourcetype
```

null_queue

```
index=main host=192* sourcetype=*cisco*
| timechart count by sourcetype
```



We are currently getting data from:

- ace
- asa

fws has dropped away thanks to our filter

Learn more: <https://splunk.github.io/splunk-connect-for-syslog/main/configuration/#dropping-all-data-by-ip-or-subnet>

splunk>

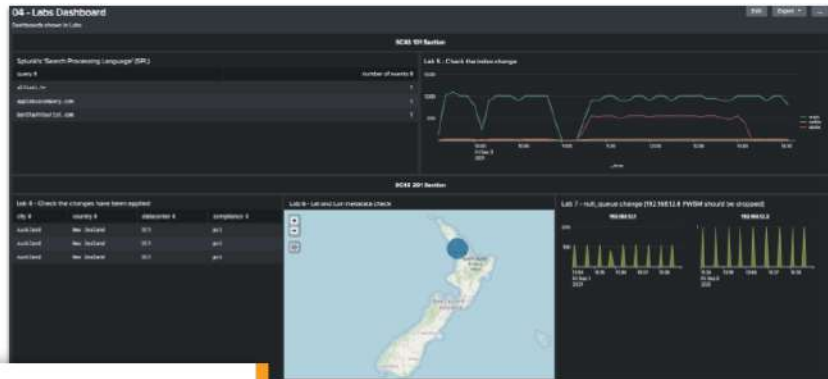
Check Labs Dashboard

Check Labs Dashboard

© 2023 SPLUNK INC.



Click on **SC4S Checks** and then on **04 - Labs Dashboard**



This Dashboard contains some of the panels from the labs.

Yours may not match exactly, but this is a good checkpoint.

```
splunk>
```