Splunk4Industry: Financial Services

Lab Guide

Overview

This lab guide contains the hands-on Labs for the **Splunk4Industry:Financial Services** workshop. Before proceeding with these Labs, please ensure that you have a copy of the Splunk4Industry slide deck, which will help to put into context the tasks you are carrying out.

Download the workshop slide deck: https://splk.it/FSI-Attendee

Prerequisites

In order to complete these Labs, you will need your own Splunk instance. Splunk's hands-on workshops are delivered via the Splunk Show portal and you will need a splunk.com account in order to access this.

If you don't already have a Splunk.com account, please create one here before proceeding with the rest of the workshop.

Registering for a **Splunk.com Account**

To help reduce any additional identity verification checks during the registration process, please use full names and full company names where possible, avoiding nicknames and abbreviations. Please see Splunk.com Registration Best Practices for more details.

⚠️ 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

Lab 1 – Access Your Lab Environment.......... 4
Description.......... 4
Steps.......... 4
Lab 2 – Create an App and Add Data to Splunk.......... 7
Description.......... 7
Steps.......... 7
Lab 3 - Start Exploring Your Data.......... 13
Description.......... 13
Steps.......... 13
Lab 4 – IT Operations team: Investigate successful vs unsuccessful web server requests over time.......... 15
Description.......... 15
Steps.......... 15
Lab 5 – DevOps team: Show the most common customer operating systems and which web browsers are experiencing the most failures.......... 19
Description.......... 19
Steps.......... 19
Extract a New Field.......... 19
Show the most common customer operating systems.......... 21
Show which web browsers are experiencing the most failures.......... 23
Lab 6 – Security/Fraud teams: Show website activity by geographic location.......... 25
Description.......... 25
Steps.......... 25
Lab 7 – Customise Your Dashboard.......... 26
Description.......... 26
Steps.......... 26
Add a Custom Background Image to Your Dashboard.......... 26
Link Your Dashboard Panels to the Global Time Picker.......... 29
Lab 8 - Financial Services: exploring additional use cases.......... 31
Description.......... 31
Steps.......... 31
Create a new app.......... 31
Create a new index.......... 31
Add data to Index.......... 32
Run Sample Searches.......... 33
Lab 9 - Business Service Insights: exploring capability.......... 35
Description.......... 35
Steps.......... 35
Switching lab environment.......... 35
Exploring a Glass Table view.......... 36
Exploring a Service Analyzer.......... 37
Exploring Deep Dive view.......... 39

Create a multi-KPI alert.... 42

Exploring Alerts & Episodes View....43

Lab 10 - Business Service Insights: building out a service view.... 46

Description....46

Steps.... 46

Build a new service....46

Add pre-existing service configurations to the new service....47

Add new VMware service.... 49

Create service using pre-built content / KPIs.... 52

Test your new configuration....53

Create service mappings to create a holistic view....54

OPTIONAL: use a CSV import to show bulk import.... 57

Build custom Glass Tables: CxO & Line of Business.... 60

Build custom Glass Tables: Infrastructure Overview.... 68

Connecting Glass Tables....69

Lab 11 - Build Your Own Service....71

Description....71

Answers: Lab 9....72

Lab 1 – Access Your Lab Environment

Description

You'll need a Splunk instance to do these hands-on Labs – time to get one!

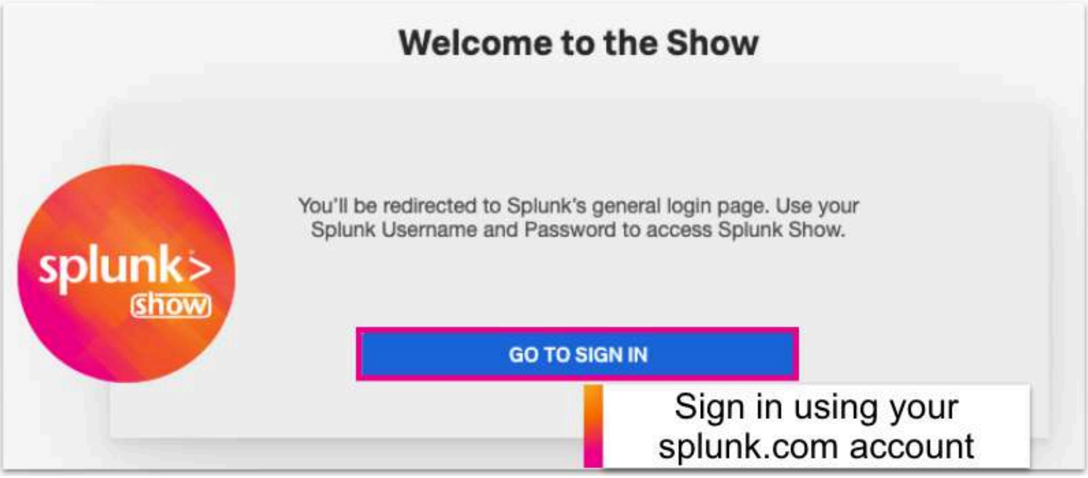
In this Lab, you will create your own Splunk Enterprise instance using our Splunk Show portal.

Already been given your Splunk instance details?

If your workshop host has already provided you with your instance URL and login details then you do not need to follow the instructions in Lab 1 of this lab guide - you can skip straight to Lab 2!

Steps

1. Browse to https://show.splunk.com and log in using your **Splunk.com account**.



Welcome to the Show

You'll be redirected to Splunk's general login page. Use your Splunk Username and Password to access Splunk Show.

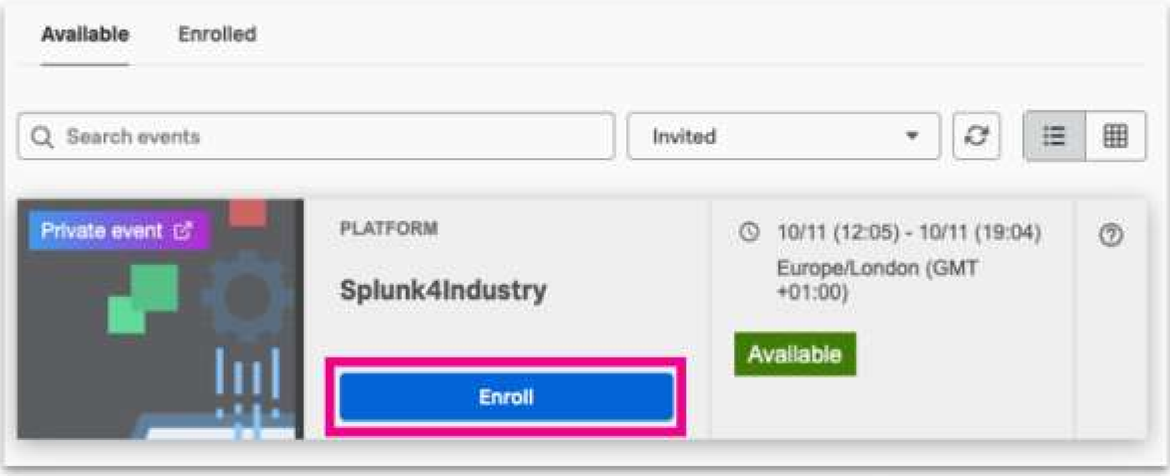
Sign in using your splunk.com account

🔑 **Don't have a Splunk.com Account?**

To access our hands-on workshop events you will need a Splunk.com account. If you don't already have a Splunk.com account, don't worry - it only takes a few minutes to create one! Please create one here.

2. Once logged in to Splunk Show you will see the event page for the event that you have been invited to. If no events are listed, try selecting '**Invited**' from the dropdown list.

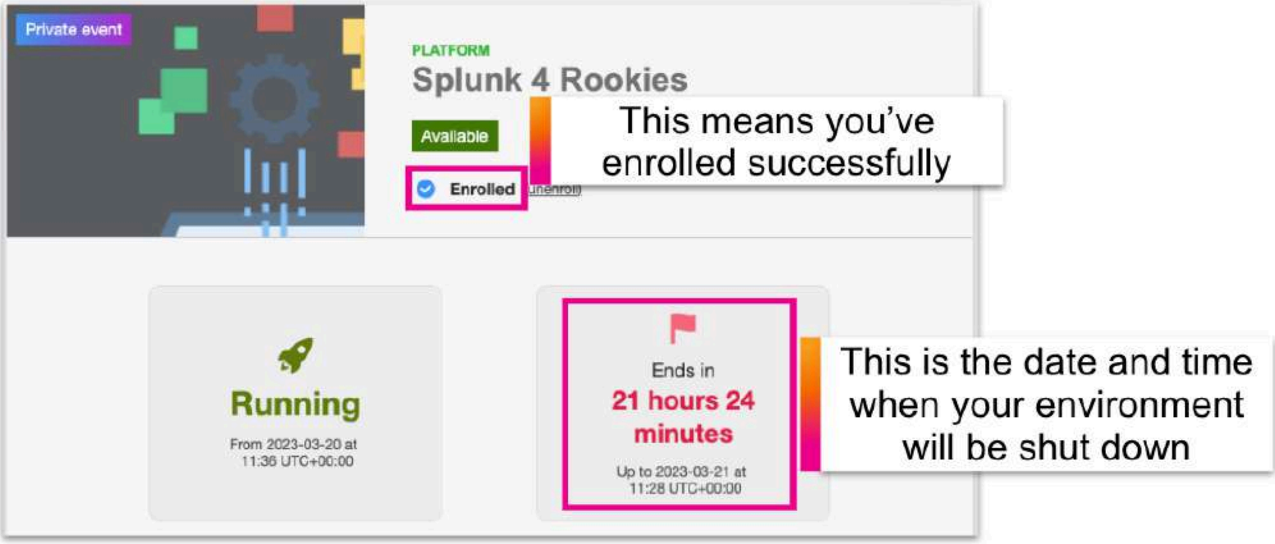
Click on **Enroll** to join the event.



The page will refresh and the event will now display ‘Enrolled’.

🕘 Lab environment expiration

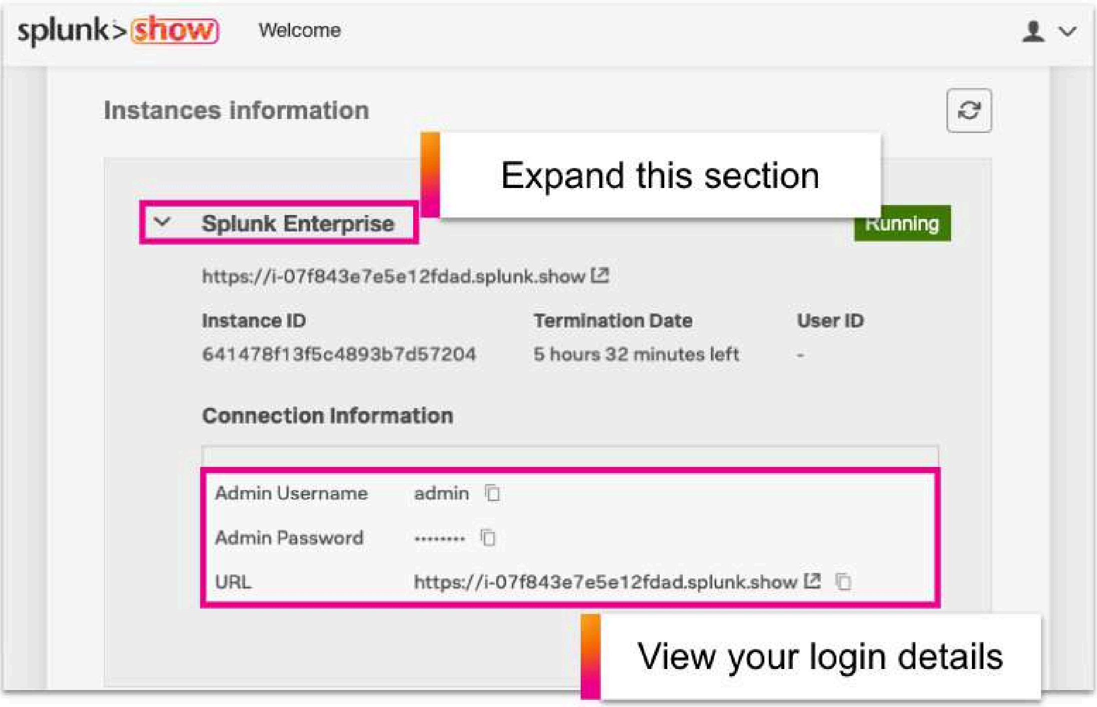
All Splunk environments that are part of this workshop event will automatically be shut down at the date and time specified on this screen so feel free to continue to play around with your lab environment until then!



This means you’ve enrolled successfully

This is the date and time when your environment will be shut down

3. Scroll down the page to the **Instances Information** section and expand out the 'Splunk Enterprise' section to locate the user credentials and link to your lab environment.



Instances information

Splunk Enterprise

Running

Expand this section

https://i-07f843e7e5e12fdad.splunk.show

Instance ID	Termination Date	User ID
641478f13f5c4893b7d57204	5 hours 32 minutes left	-

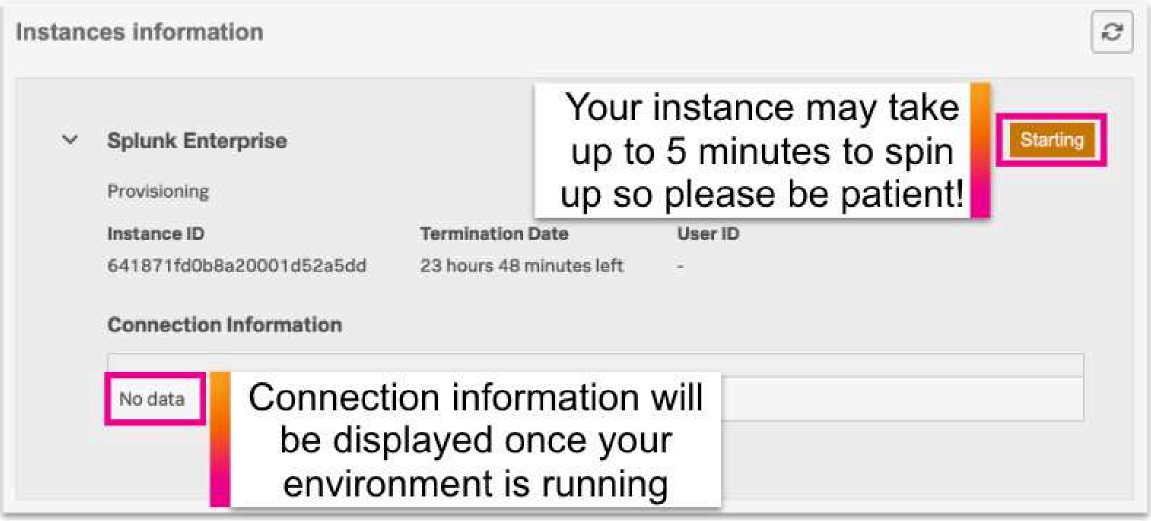
Connection Information

Admin Username	admin
Admin Password	••••••••
URL	https://i-07f843e7e5e12fdad.splunk.show

View your login details

⚠️ No connection information shown?

If you don't see any connection information displayed yet it means that your lab environment is currently starting up. Please try refreshing this view in a few minutes.



Instances information

Splunk Enterprise

Provisioning

Your instance may take up to 5 minutes to spin up so please be patient!

Starting

Instance ID	Termination Date	User ID
641871fd0b8a20001d52a5dd	23 hours 48 minutes left	-

Connection Information

No data

Connection information will be displayed once your environment is running

Lab 2 – Create an App and Add Data to Splunk

Description

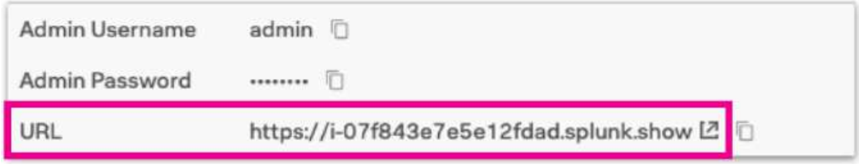
Splunk apps and add-ons provide customisable content and capabilities for a variety of technologies and use cases, accelerating the time it takes to get value from your data. They're also a great way to organise and share your content - such as reports and dashboards - to Splunk users. Anyone can build apps and add-ons, and today we're going to create our own app that contains a dashboard.

Since Splunk is a data platform, we'll also need to load some data in before we can do anything!

In this Lab, you will create a new app and then add some data to your Splunk Enterprise instance. We will configure Splunk to monitor some sample web server logs, which are currently being generated on the same server that Splunk is running on.

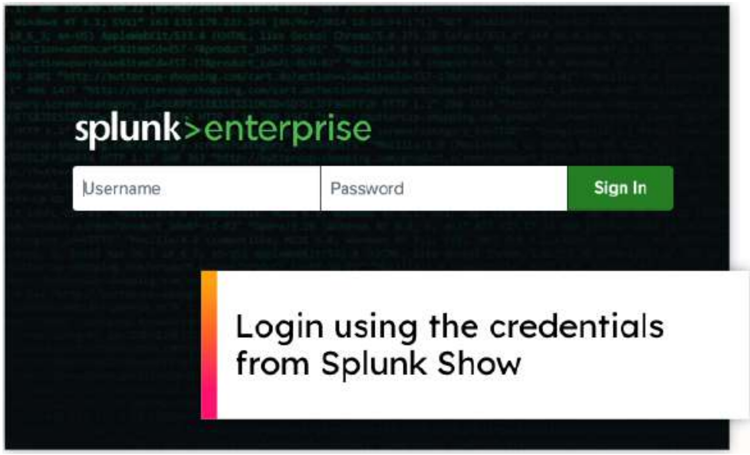
Steps

1. Browse to your Splunk instance by using the unique URL link provided in the Splunk Show event (see step 3 of Lab 1 - Access Your Lab Environment.)



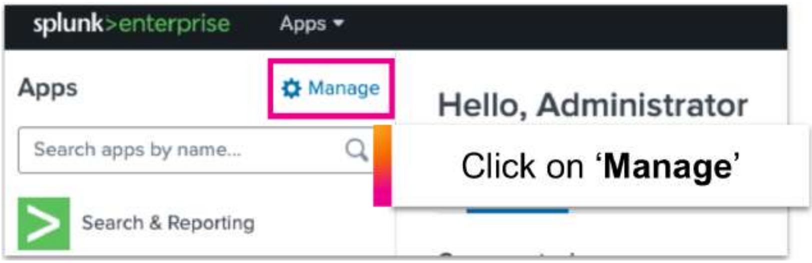
Admin Username	admin
Admin Password	••••••••
URL	https://i-07f843e7e5e12fdad.splunk.show

2. Log in using the credentials from the Splunk Show event.



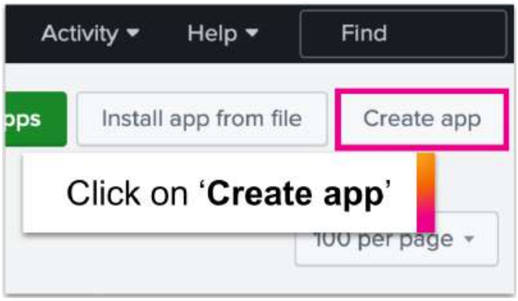
Login using the credentials from Splunk Show

3. On the left side of the page, under the **Apps** section, click on **Manage**.



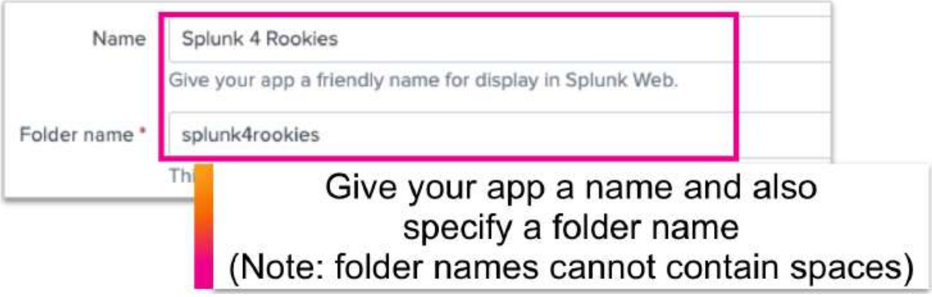
Click on ‘**Manage**’

4. On the top right corner of the screen, click on **Create app**.



Click on ‘**Create app**’

5. Give your app a name and enter a folder name. Leave all other values as they are and click on **Save**.



Name: Splunk 4 Rookies

Give your app a friendly name for display in Splunk Web.

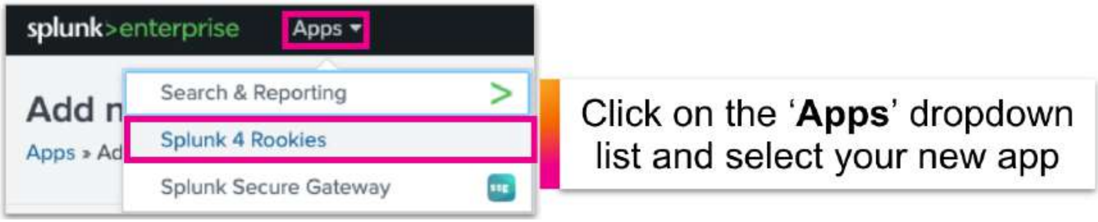
Folder name *: splunk4rookies

Th

Give your app a name and also
specify a folder name
(Note: folder names cannot contain spaces)

6. Now that our blank app has been created, we need to select the app so that everything we do from now on will be created and saved within the new app.

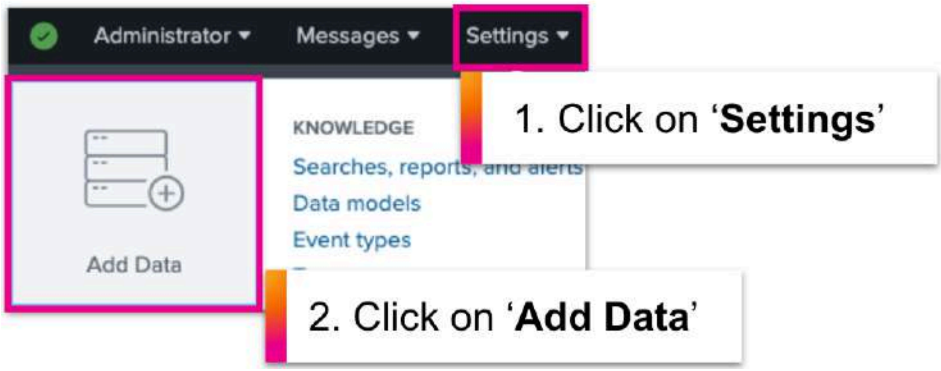
   To select your app, click on the **Apps** dropdown list at the top left of the page and select your app.



Click on the ‘**Apps**’ dropdown
list and select your new app

Now let’s add some data!

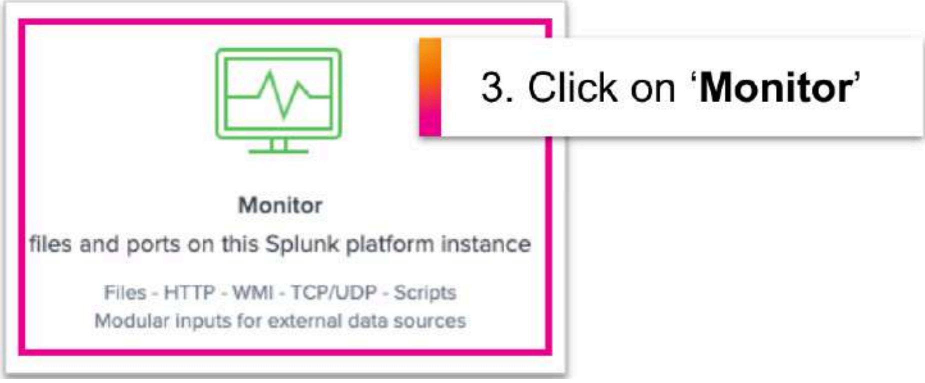
7. With our new app still selected from the dropdown list, go to **Settings** > **Add Data**.



1. Click on ‘**Settings**’

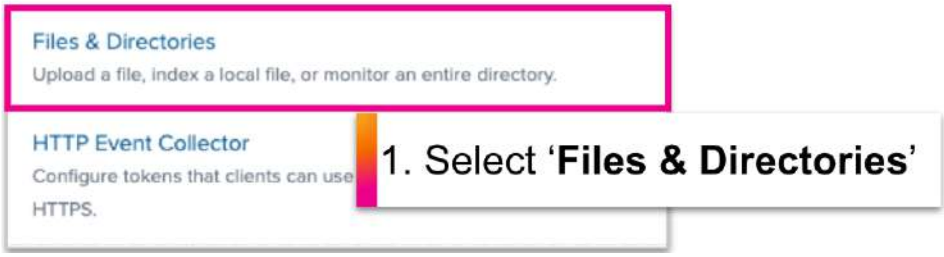
2. Click on ‘**Add Data**’

8. For this Lab we will monitor a directory, as this will allow us to pick up new data as it is generated by the web server. To do this, click on ‘**Monitor**’.


Monitor
files and ports on this Splunk platform instance
Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources

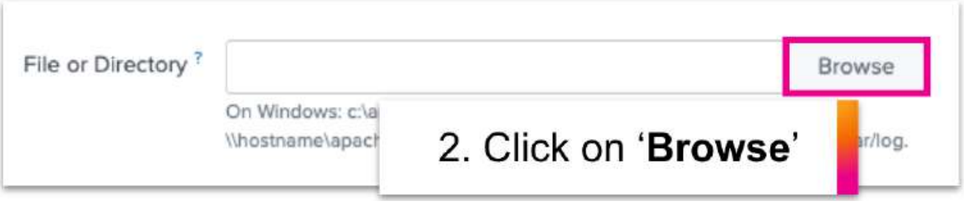
3. Click on ‘**Monitor**’

9. Select ‘**Files & Directories**’ and then click ‘**Browse**’.



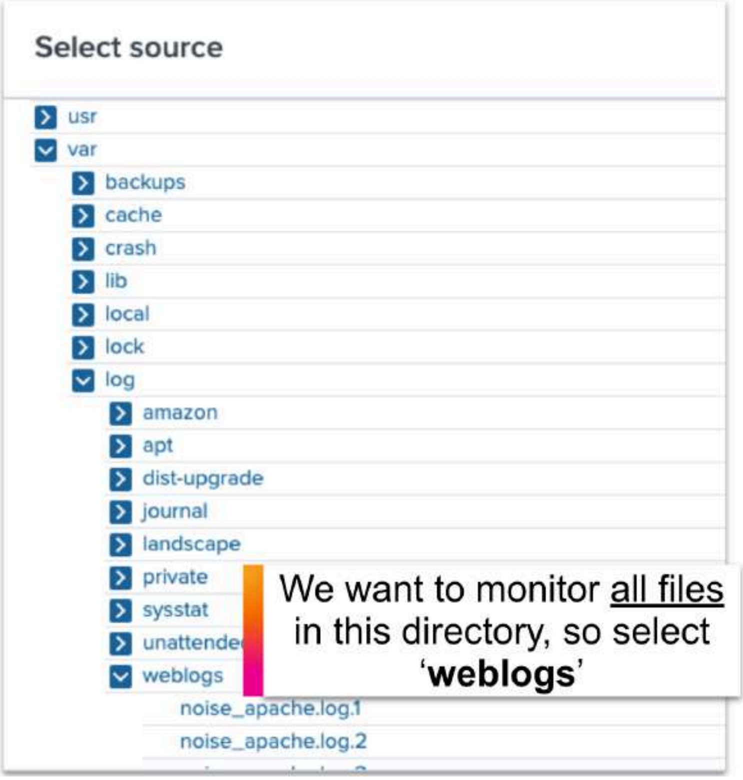
Upload a file, index a local file, or monitor an entire directory.

1. Select ‘**Files & Directories**’



2. Click on ‘**Browse**’

10. Browse to **/var/log** and select the **weblogs** directory. Click on **Select** to choose this directory.

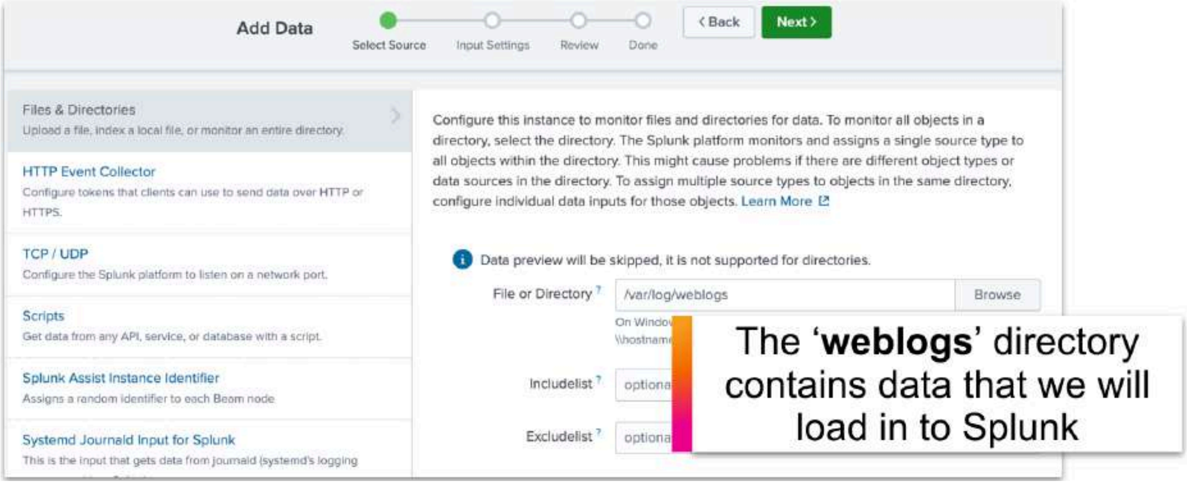


Select source

- usr
- var
  - backups
  - cache
  - crash
  - lib
  - local
  - lock
  - log
    - amazon
    - apt
    - dist-upgrade
    - journal
    - landscape
    - private
    - sysstat
    - unattende
    - weblogs
      - noise_apache.log.1
      - noise_apache.log.2

We want to monitor all files in this directory, so select '**weblogs**'

11. Check that the directory path is correct (**/var/log/weblogs**) and click on **Next**.



Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

Splunk Assist Instance Identifier
Assigns a random identifier to each Beam node

Systemd Journald Input for Splunk
This is the input that gets data from journald (systemd's logging

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. Learn More

Data preview will be skipped, it is not supported for directories.

File or Directory ? /var/log/weblogs Browse

On Windo
\\hostname

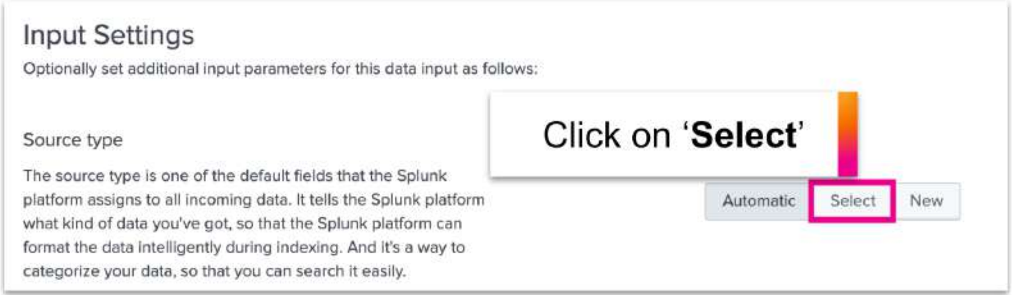
Includelist ? optiona

Excludelist ? optiona

The '**weblogs**' directory contains data that we will load in to Splunk

12. Now we need to select a source type for this data. A source type determines how Splunk formats the data during the indexing process. Splunk comes with a large set of predefined source types and can often detect the source type automatically. However, for this Lab you will specify the source type.

On the **Input Settings** screen, to the right of the **Source type** section, click on **Select**.



Input Settings

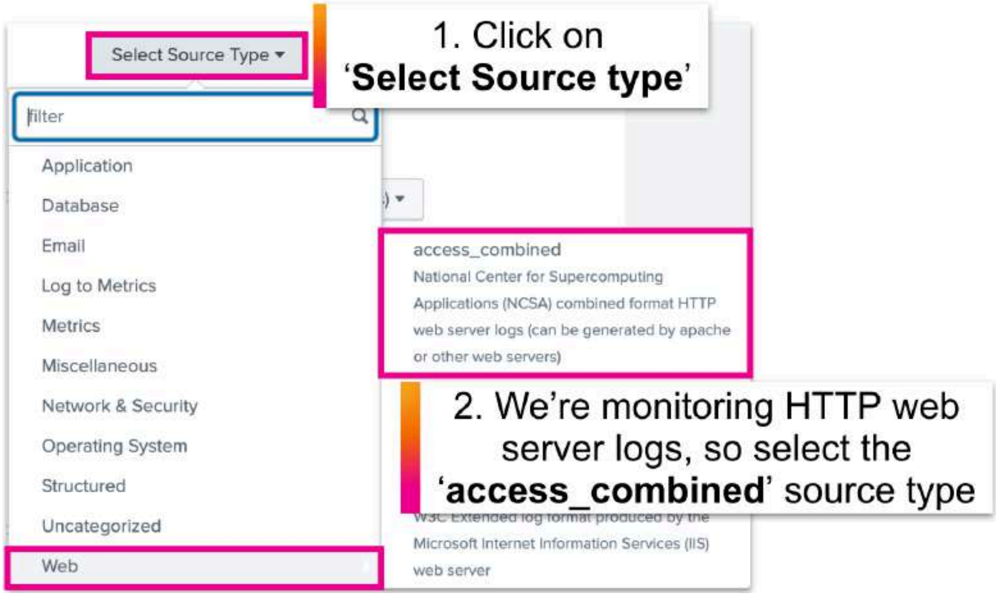
Optionally set additional input parameters for this data input as follows:

Source type

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Click on '**Select**'

13. Click on the **Select Source Type** dropdown list and browse to **Web > access_combined**. Alternatively, you can start typing 'access' in the **filter** field and the 'access_combined' source type should appear.



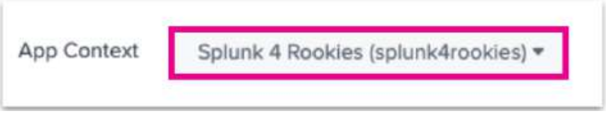
1. Click on '**Select Source type**'

access_combined
National Center for Supercomputing Applications (NCSA) combined format HTTP web server logs (can be generated by apache or other web servers)

2. We're monitoring HTTP web server logs, so select the '**access_combined**' source type

W3C Extended log format produced by the Microsoft Internet Information Services (IIS) web server

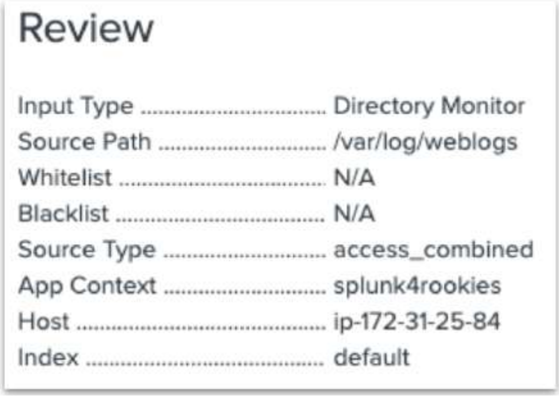
14. For the **App Context**, ensure that your new app is selected from the list.



App Context: Splunk 4 Rookies (splunk4rookies)

15. Leave all other values as default and click on **Review**.

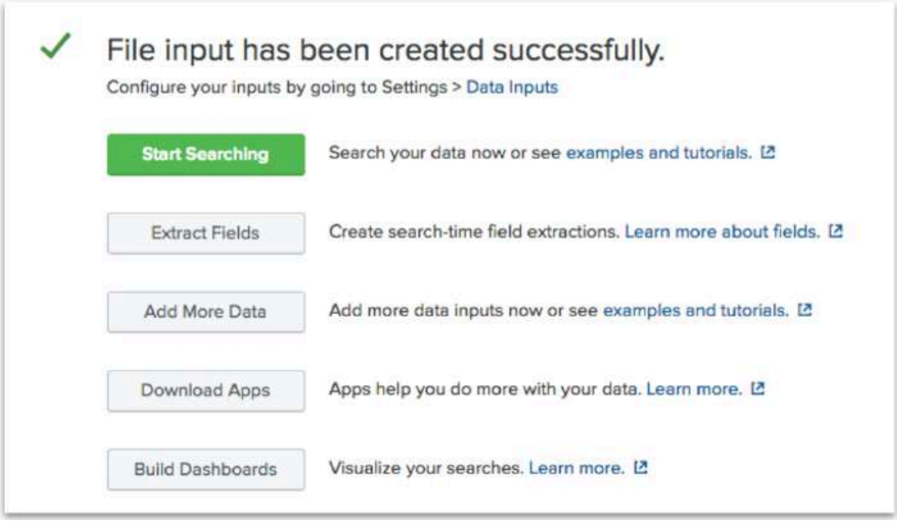
16. Review your settings and click on **Submit**.



Review

```
Input Type ............................... Directory Monitor
Source Path .............................. /var/log/weblogs
Whitelist ................................ N/A
Blacklist ................................ N/A
Source Type .............................. access_combined
App Context .............................. splunk4rookies
Host ..................................... ip-172-31-25-84
Index .................................... default
```

17. You should now receive a message stating that your ‘**File input has been created successfully**’. Click on **Start Searching** to search the data you have just added to Splunk.



File input has been created successfully.

Configure your inputs by going to Settings > Data Inputs

Search your data now or see examples and tutorials.

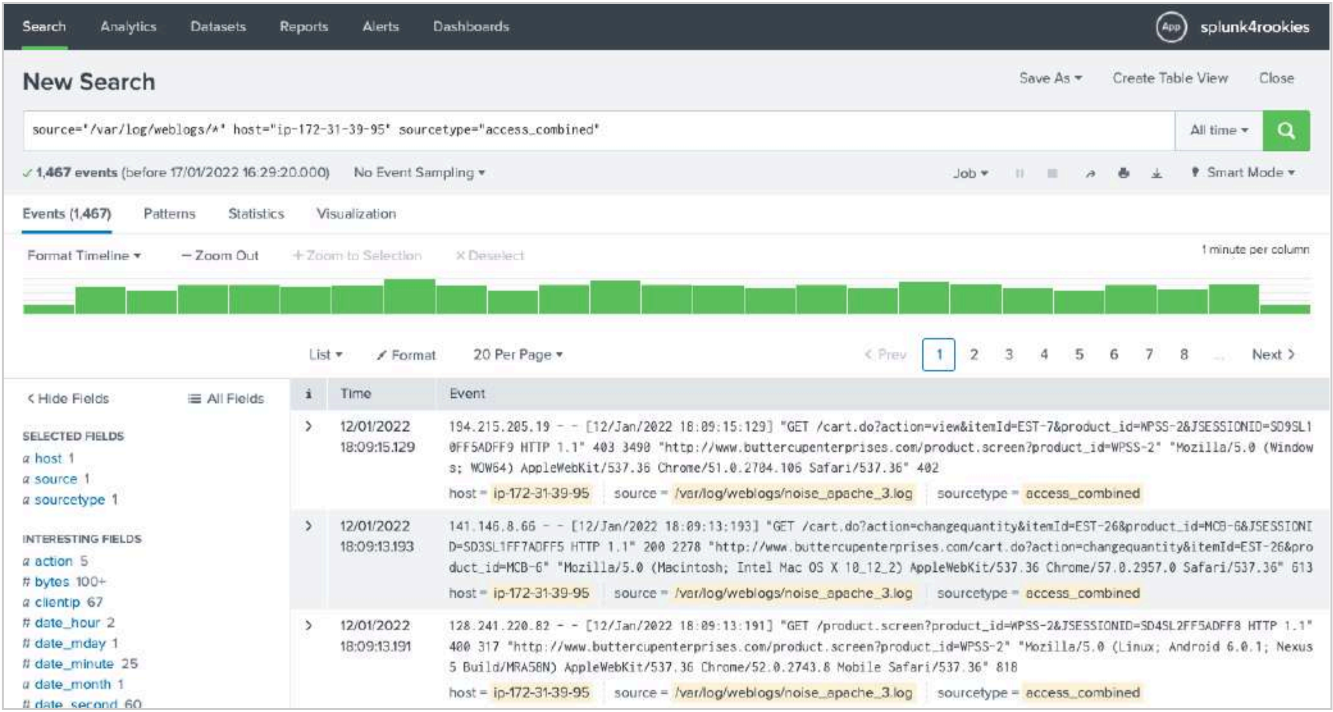
Create search-time field extractions. Learn more about fields.

Add more data inputs now or see examples and tutorials.

Apps help you do more with your data. Learn more.

Visualize your searches. Learn more.

You should now see the raw events being shown in Splunk.



```
source="/var/log/weblogs/*" host="ip-172-31-39-95" sourcetype="access_combined"
```

✓ 1,467 events (before 17/01/2022 16:29:20.000)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 5
# bytes 100+
a clientip 67
# date_hour 2
# date_mday 1
# date_minute 25
a date_month 1
# date_second 60

```
12/01/2022    194.215.205.19 - - [12/Jan/2022 18:09:15:129] "GET /cart.do?action=view&itemId=EST-7&product_id=WPSS-2&JSESSIONID=SD9SL1
18:09:15.129  0FF5ADFF9 HTTP 1.1" 403 3490 "http://www.buttercupenterprises.com/product.screen?product_id=WPSS-2" "Mozilla/5.0 (Window
              s; WOW64) AppleWebKit/537.36 Chrome/51.0.2704.106 Safari/537.36" 402
              host = ip-172-31-39-95    source = /var/log/weblogs/noise_apache_3.log    sourcetype = access_combined

12/01/2022    141.146.8.66 - - [12/Jan/2022 18:09:13:193] "GET /cart.do?action=changequantity&itemId=EST-26&product_id=MCB-6&JSESSIONI
18:09:13.193  D=SD3SL1FF7ADFF5 HTTP 1.1" 200 2278 "http://www.buttercupenterprises.com/cart.do?action=changequantity&itemId=EST-26&pro
              duct_id=MCB-6" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_2) AppleWebKit/537.36 Chrome/57.0.2957.0 Safari/537.36" 613
              host = ip-172-31-39-95    source = /var/log/weblogs/noise_apache_3.log    sourcetype = access_combined

12/01/2022    128.241.220.82 - - [12/Jan/2022 18:09:13:191] "GET /product.screen?product_id=WPSS-2&JSESSIONID=SD4SL2FF5ADFF8 HTTP 1.1"
18:09:13.191  400 317 "http://www.buttercupenterprises.com/product.screen?product_id=WPSS-2" "Mozilla/5.0 (Linux; Android 6.0.1; Nexus
              5 Build/MRA58N) AppleWebKit/537.36 Chrome/52.0.2743.8 Mobile Safari/537.36" 818
              host = ip-172-31-39-95    source = /var/log/weblogs/noise_apache_3.log    sourcetype = access_combined
```

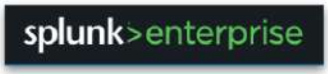
Lab 3 - Start Exploring Your Data

Description

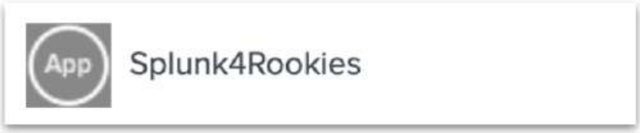
In this Lab, you will try some basic Splunk searches using the Search section of your new app.

Steps

1. Click on the Splunk logo in the top left corner of the screen to take you back to the default home screen.



2. Under the **Apps** section on the left of the page, click on the new app that you created in task 2 (Note: the name will be whatever you entered when you created it.)



3. To search, just type any word or phrase into the search bar and Splunk will search for all events that contain those words.

   So enough talking – let's try some searches!

   Firstly, set the time picker (to the right of the search bar) to **Last 60 minutes**. Your environment has an event generator running in the background, which is constantly creating sample data for you to use. This data started being generated from the moment you registered for your Splunk environment, so let's stick to the last 60 minutes of data…

   Try the following search:

```
503 purchase
```

   This will return all events from Splunk that contain the number '**503**' and the word '**purchase**'.

ℹ️ **Spaces between words in a search**

In Splunk, a space between two words is an implied Boolean 'AND', meaning that Splunk will automatically search for events containing both words – you don't need to specify it.

4. That's great, but what if there are events with the word '*purchased*', '*purchasing*', or '*purchaser*', for example? Well, we can use a wildcard asterisk (*****) to search for any events containing '**503**' and any word beginning with '**pur**':

   ```
   503 pur*
   ```

   A wildcard is useful if we want to be a bit more flexible with what we're searching for.

5. Remember the '`AND`' operator we mentioned in step 3? Well you can also use the other Boolean operators as well: `OR` and `NOT`. Note that these must be in UPPERCASE.

   Let's try using one of these operators in a search:

   ```
   503 (purchase OR addtocart)
   ```

   This search will return all events containing the number '**503**' and either the word '**purchase**' or the word '**addtocart**'.

6. So far, we've just been searching for text – those numbers could appear anywhere in our data, so how do we know that we're searching the right values? Depending on our data '**503**' could be a HTTP status code, or it could be part of a session ID or a phone number.

   Well, we know we're looking at web logs, so let's include field/value pairs in our search to be more specific with what we're looking for:

   ```
   status=503 action=purchase
   ```

   This will ensure that our results only return web server **purchase** events where the HTTP status code is '**503**'. Always specify field names where possible to ensure that your results are as accurate as possible!

ℹ️ Search Best Practices

In a production environment you will likely have much more data to search through than in today's workshop environment. As a best practice, always specify the index and sourcetype if you know them - it will make your searches MUCH faster!

Example:

```
index=main sourcetype=access_combined
```

For more information please see Write better searches in the Splunk docs.

Lab 4 – IT Operations team: Investigate successful vs unsuccessful web server requests over time

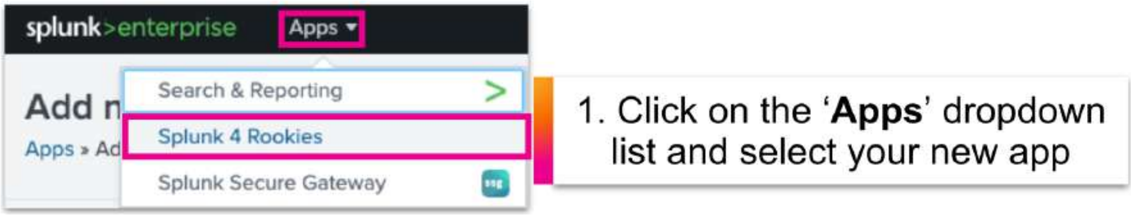
Description

The IT Operations team currently has no visibility of failures on the Buttercup Enterprises website.

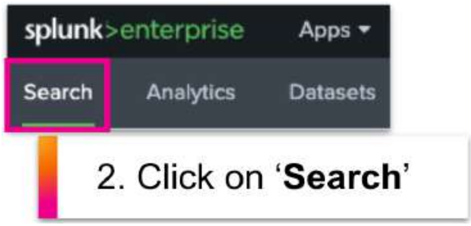
In this Lab, you will produce a dashboard panel for the IT Operations team, showing website successes vs failures over time.

Steps

1. To start a new search, first make sure your app is selected from the Apps dropdown list and then click Search on the app menu bar.



1. Click on the ‘**Apps**’ dropdown list and select your new app

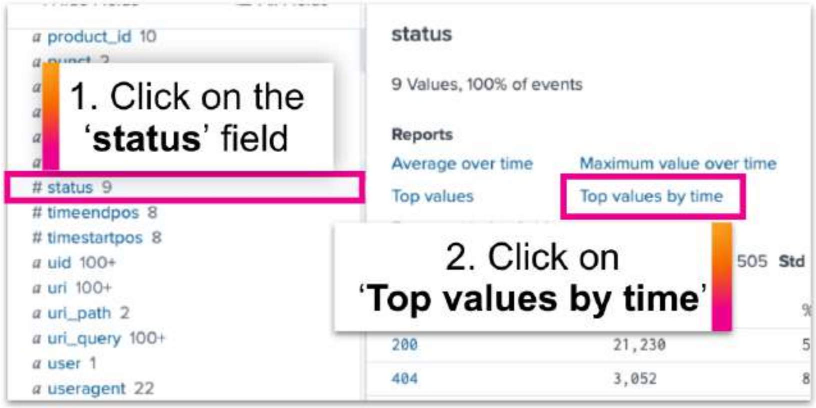


2. Click on ‘**Search**’

2. Search the **main** index (i.e. the default index) for all web server events over the **Last 60 minutes**:

```
index=main sourcetype=access_combined
```

3. Scroll down the page and find the **status** field. Click on the field name to display the field window and select **Top values by time**.



1. Click on the '**status**' field

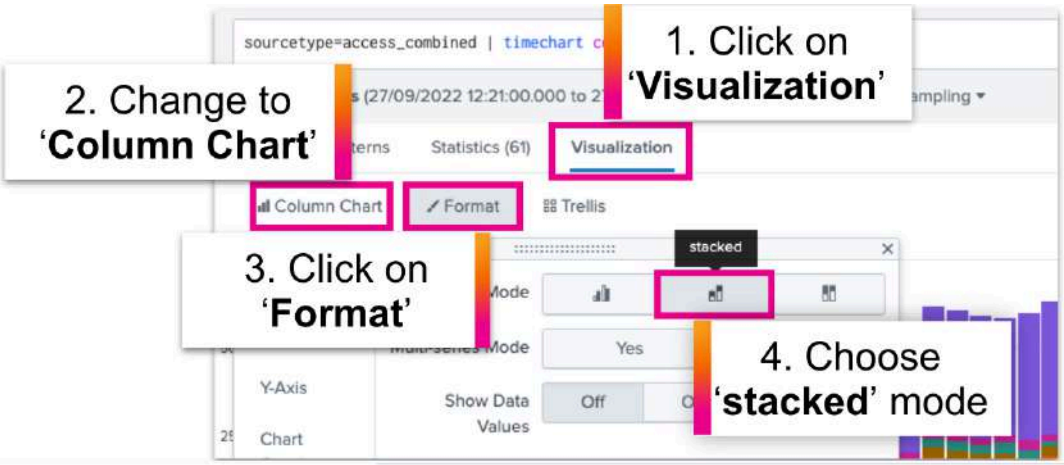
2. Click on '**Top values by time**'

Splunk will automatically populate your search as follows:

```
index=main sourcetype=access_combined | timechart count by status limit=10
```

4. A chart will display on the **Visualization** tab. Change the visualization to a **Column Chart**.

Click on **Format** and then on the **General** tab to change the **Stack Mode** to '**stacked**'. Feel free to play around with the formatting until you're happy with the visualization.



1. Click on '**Visualization**'

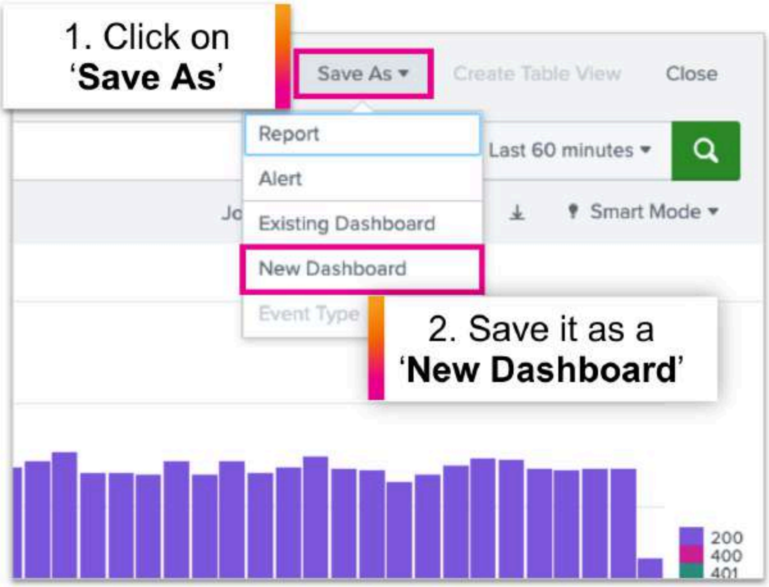
2. Change to '**Column Chart**'

3. Click on '**Format**'

4. Choose '**stacked**' mode

5. Now that we have a nice chart visualization, let's add it to a new dashboard so we can share this information with the business.

In the top right corner of the screen, go to **Save As > New Dashboard**.



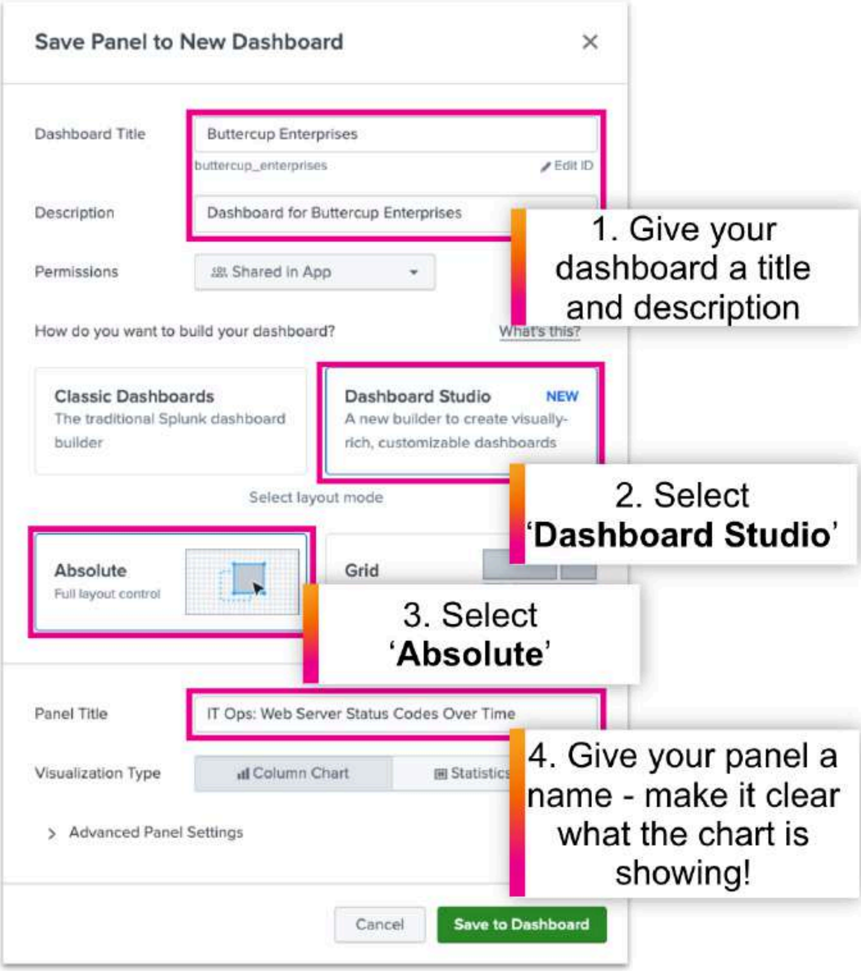
1. Click on '**Save As**'

2. Save it as a '**New Dashboard**'

6. On the **Save Panel to New Dashboard** screen, give your dashboard a suitable title and optionally a description too. If you can't think of a name for your dashboard, call it '**Buttercup Enterprises**, or something else meaningful to you.

   Choose how you want to build your dashboard. For today's workshop we will use **Dashboard Studio**. For your layout mode, select **Absolute**.

   Give your panel a title – something that describes what this chart is showing, such as '**IT Ops: Web Server Status Codes Over Time**'.


Save Panel to New Dashboard

Dashboard Title: Buttercup Enterprises
buttercup_enterprises

Description: Dashboard for Buttercup Enterprises

Permissions: Shared in App

How do you want to build your dashboard?

Select layout mode

Panel Title: IT Ops: Web Server Status Codes Over Time

Visualization Type: Column Chart

×
Edit ID
What's this?
Classic Dashboards
The traditional Splunk dashboard builder
Dashboard Studio
NEW
A new builder to create visually-rich, customizable dashboards
Absolute
Full layout control
Grid
Statistics
> Advanced Panel Settings
Cancel
Save to Dashboard

1. Give your dashboard a title and description

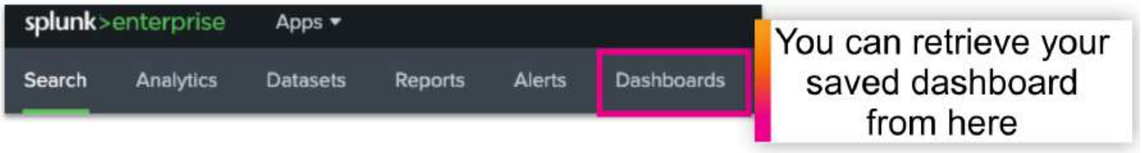
2. Select '**Dashboard Studio**'

3. Select '**Absolute**'

4. Give your panel a name - make it clear what the chart is showing!

7. Click on **Save to Dashboard** and then **View Dashboard**.

   Congratulations - you've just created a Splunk dashboard with your first panel! Anytime you want to access a dashboard, click on **Dashboards** in the menu bar and select the dashboard you wish to display. Go ahead – give it a try!



Lab 5 – DevOps team: Show the most common customer operating systems and which web browsers are experiencing the most failures

Description

In this Lab, you will need to extract a new field from your events in order to create the report we need. To accomplish this, we will use Splunk's field extractor wizard.

Custom field extractions are useful in a variety of scenarios, such as:

- When you have custom data and Splunk did not recognise/extract a particular field that you need
- When you need to extract a particular part of an event in order to be able to search/report on that value

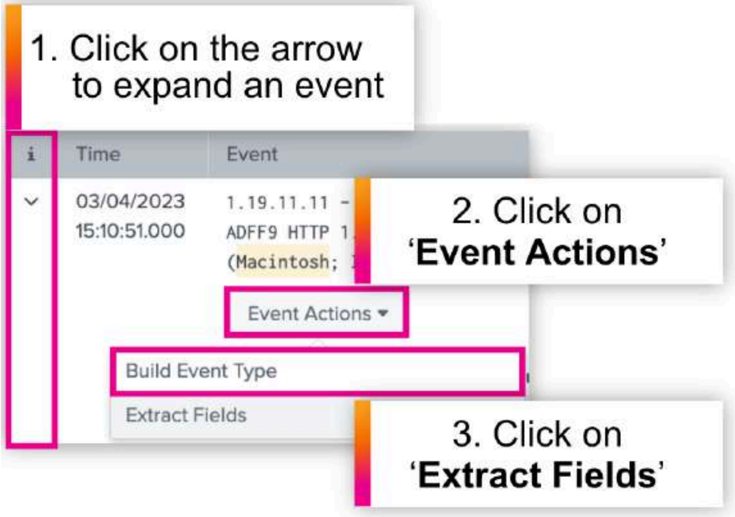
Steps

Extract a New Field

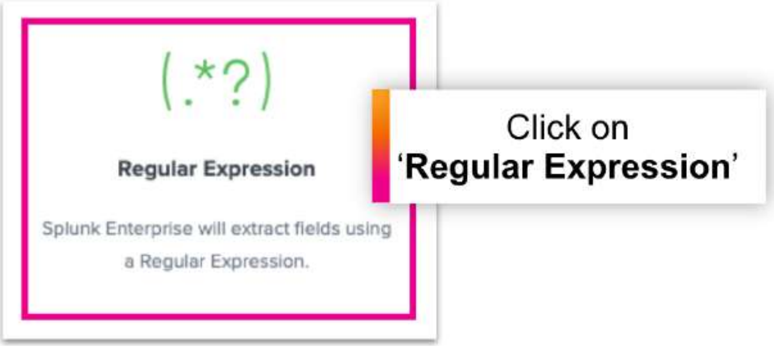
1. Click **Search** if you don't see the search bar displayed. Search for all web server events over the **Last 60 minutes**:

```
index=main sourcetype=access_combined
```

2. Expand out one of the events by clicking on the arrow (**>**) to the left of the event timestamp. Click on the **Event Actions** dropdown list and select **Extract Fields**:



3. We have two options for extracting fields: Regular Expression or Delimiters. For this Lab, we will choose Regular Expression. Click on **Regular Expression** and then click on **Next**.

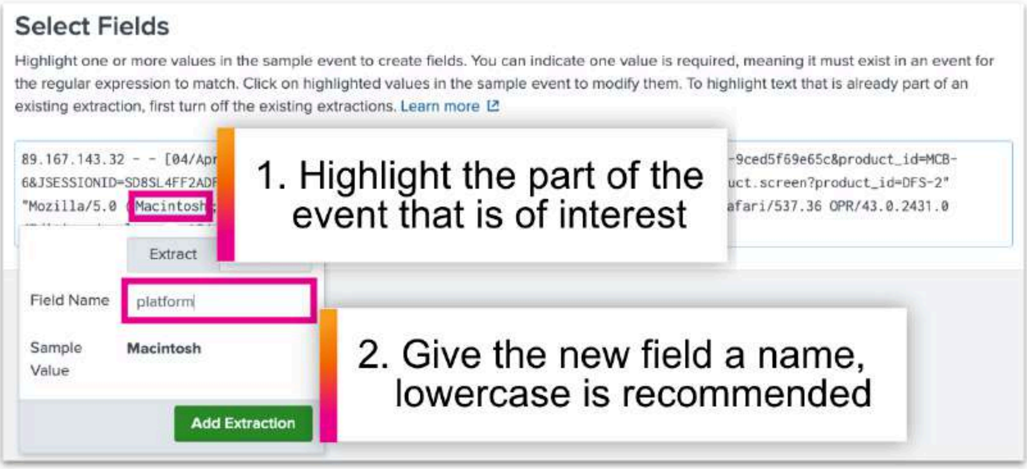


Splunk Enterprise will extract fields using a Regular Expression.

Click on ‘**Regular Expression**’

4. You will now be presented with a sample event from which to extract your field. For this Lab, we will need to extract the platform (operating system) information from each event so we can report on it. Look for the platform/operating system information in your event (e.g. Linux, Macintosh, Windows, etc.) contained in the useragent string towards the end of the event and highlight it.

   Give the new field the following name: **platform** (field names are case sensitive, so be sure to use all lowercase letters for this to make your life easier!)



Select Fields

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression to match. Click on highlighted values in the sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. Learn more

```
89.167.143.32 - - [04/Apr                -9ced5f69e65c&product_id=MCB-
6&JSESSIONID=SD8SL4FF2ADF               uct.screen?product_id=DFS-2"
"Mozilla/5.0 (Macintosh;                afari/537.36 OPR/43.0.2431.0
```

Field Name: platform

Sample Value: Macintosh

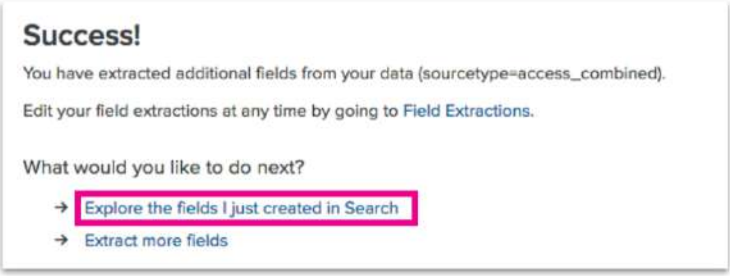
1. Highlight the part of the event that is of interest

2. Give the new field a name, lowercase is recommended

5. Click on **Add Extraction** and then click on **Next**.

6. Click on **Next** again to reach the **Save** screen. On the Save screen, click on **Finish** to save your new field extraction.

7. You should now see a **Success!** page. Click on **Explore the fields I just created in Search**.



Success!

You have extracted additional fields from your data (sourcetype=access_combined).

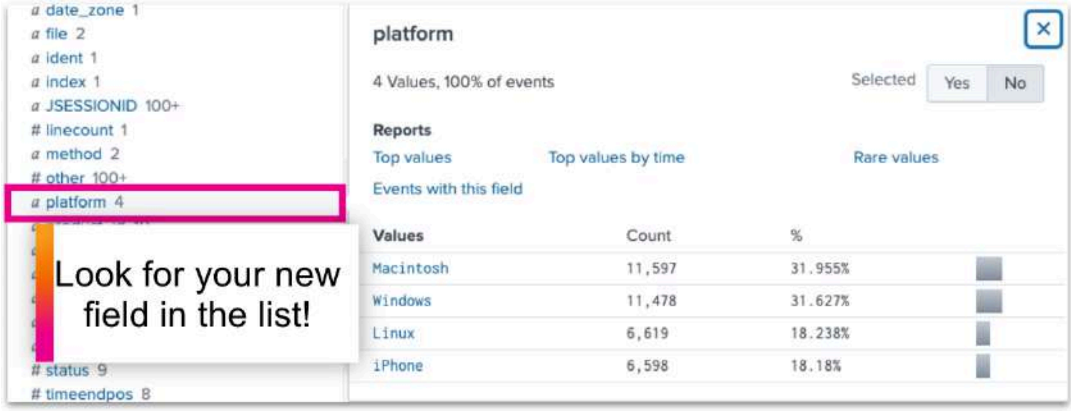
Edit your field extractions at any time by going to Field Extractions.

What would you like to do next?

→ Explore the fields I just created in Search

→ Extract more fields

8. Splunk will show you search results for all of your web server data over the last 24 hours. Scroll down the page and look for your new field listed on the left – you can now use it in your searches!



a date_zone 1
a file 2
a ident 1
a index 1
a JSESSIONID 100+
# linecount 1
a method 2
# other 100+
a platform 4
# status 9
# timeendpos 8

Look for your new field in the list!

platform

4 Values, 100% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Values	Count	%
Macintosh	11,597	31.955%
Windows	11,478	31.627%
Linux	6,619	18.238%
iPhone	6,598	18.18%

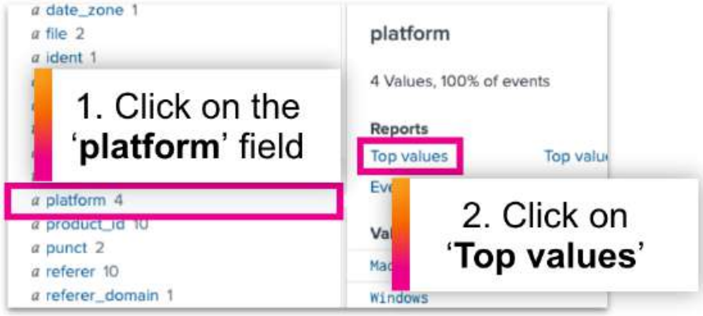
Show the most common customer operating systems

Now that we have our new field, we can use it to report for the DevOps team!

1. Search for all web server events over the **Last 60 minutes**:

```
index=main sourcetype=access_combined
```

2. Scroll down the page and find the **platform** field that you just extracted. Click on the field name to display the field window, and then select **Top values**.



a date_zone 1
a file 2
a ident 1
a platform 4
a product_id 10
a punct 2
a referer 10
a referer_domain 1

1. Click on the '**platform**' field

platform

4 Values, 100% of events

Reports

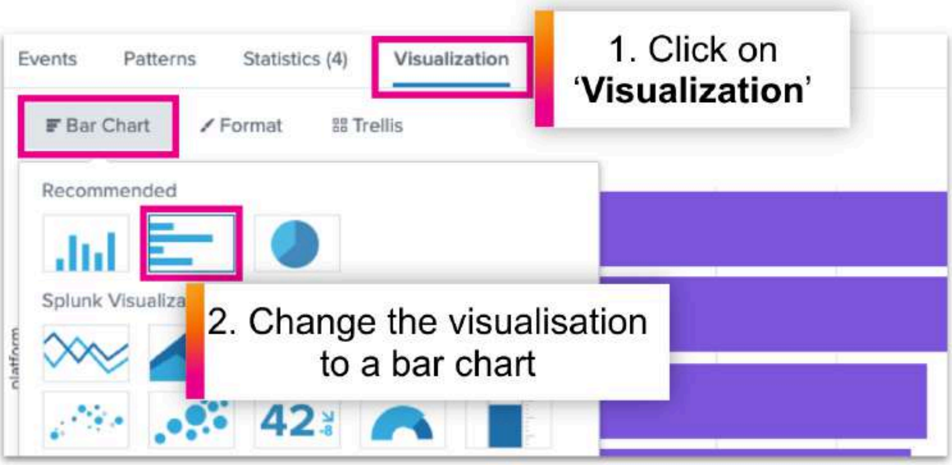
Top values Top valu

2. Click on '**Top values**'

Splunk will automatically populate your search as follows:

```
index=main sourcetype=access_combined | top limit=20 platform
```

3. Select the **Visualization** tab if not already displayed and change the visualization to a **Bar Chart**.

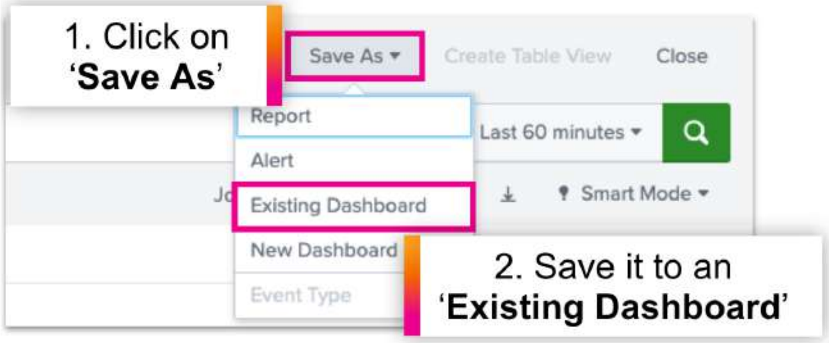


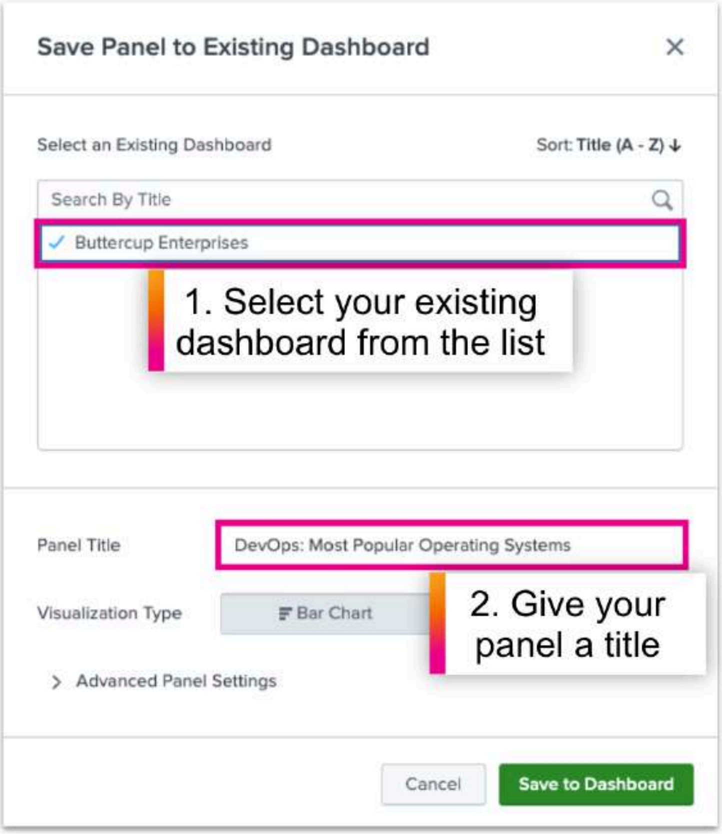
ℹ️ **Tip for cleaning up your chart**

You can optionally add `showperc=f` to the `top` command to remove the 'percent' column from the table of statistics. This will help to keep the chart nice and clean when we view it on our dashboard later.

```
index=main sourcetype=access_combined | top limit=20 platform showperc=f
```

4. When you're happy with your chart, save it to an '**Existing Dashboard**' and select the dashboard you previously created from the list. Finally, give the dashboard panel a suitable title, such as '**DevOps: Most Popular Operating Systems**' and click on **Save to Dashboard**.




Save Panel to Existing Dashboard
×
Select an Existing Dashboard
Sort: Title (A - Z) ↓
Search By Title
✓ Buttercup Enterprises
Panel Title
DevOps: Most Popular Operating Systems
Visualization Type
Bar Chart
> Advanced Panel Settings
Cancel
Save to Dashboard

1. Select your existing dashboard from the list

2. Give your panel a title

Show which web browsers are experiencing the most failures

One DevOps use case down, one more to go! We now need to report on failures by web browser.

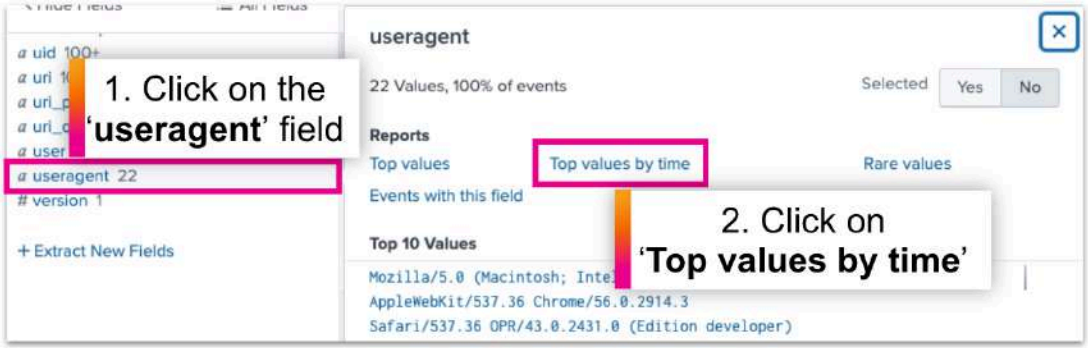
1. Search for all web server events over the **Last 60 minutes**:

```
index=main sourcetype=access_combined
```

2. Add a search filter to return only events with a status code of 400 or higher (an event with a status value of 400 or higher is considered a failure of some kind.)

```
index=main sourcetype=access_combined status>=400
```

3. Scroll down the page and find the **useragent** field (Note: ‘useragent’ is a field containing information about the web browsers that are interacting with our website.) Click on the field name to display the field window and then select **Top values by time**.



1. Click on the ‘useragent’ field

2. Click on ‘Top values by time’

Splunk will automatically populate your search as follows:

```
index=main sourcetype=access_combined status>=400
| timechart count by useragent limit=10
```

4. Select the **Visualization** tab if not already displayed and change the visualization to an **Area Chart**.

   To make your chart cleaner, limit your output to the top 5 useragents by changing the “limit” to 5 in your search.

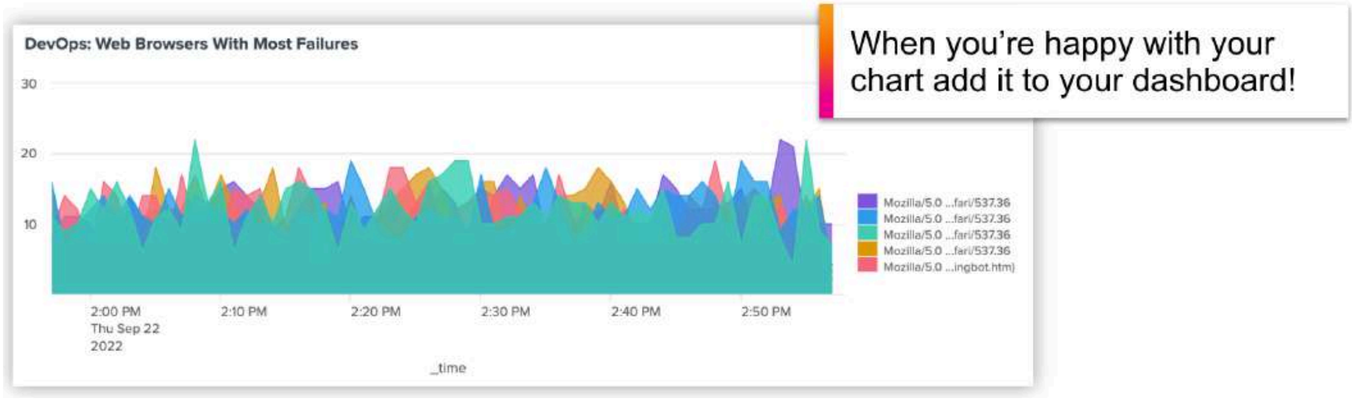
```
index=main sourcetype=access_combined status>=400
| timechart count by useragent limit=5
```

ℹ️ **Tip for cleaning up your chart**

You can optionally add `useother=f` to the `timechart` command to remove the ‘OTHER’ value from your chart.

```
index=main sourcetype=access_combined status>=400
| timechart count by useragent limit=5 useother=f
```

When you’re happy with your chart, add it to your dashboard and give the panel a title such as ‘**DevOps: Web Browsers With Most Failures**’.


DevOps: Web Browsers With Most Failures
30
20
10
2:00 PM
Thu Sep 22
2022
2:10 PM
2:20 PM
2:30 PM
2:40 PM
2:50 PM
_time
Mozilla/5.0 ...fari/537.36
Mozilla/5.0 ...fari/537.36
Mozilla/5.0 ...fari/537.36
Mozilla/5.0 ...fari/537.36
Mozilla/5.0 ...ingbot.htm)

When you’re happy with your chart add it to your dashboard!

Note: Remember to add it to your existing dashboard rather than creating a new one!

Lab 6 – Security/Fraud teams: Show website activity by geographic location

Description

Buttercup Enterprises is based in the United States, and there is a concern that there could be many potentially fraudulent transactions coming from other countries. However, they don't currently have any visibility of where website traffic is originating from.

In this Lab, we will create a **Cluster Map** visualization that shows the geographic location of anyone connecting to the company website.

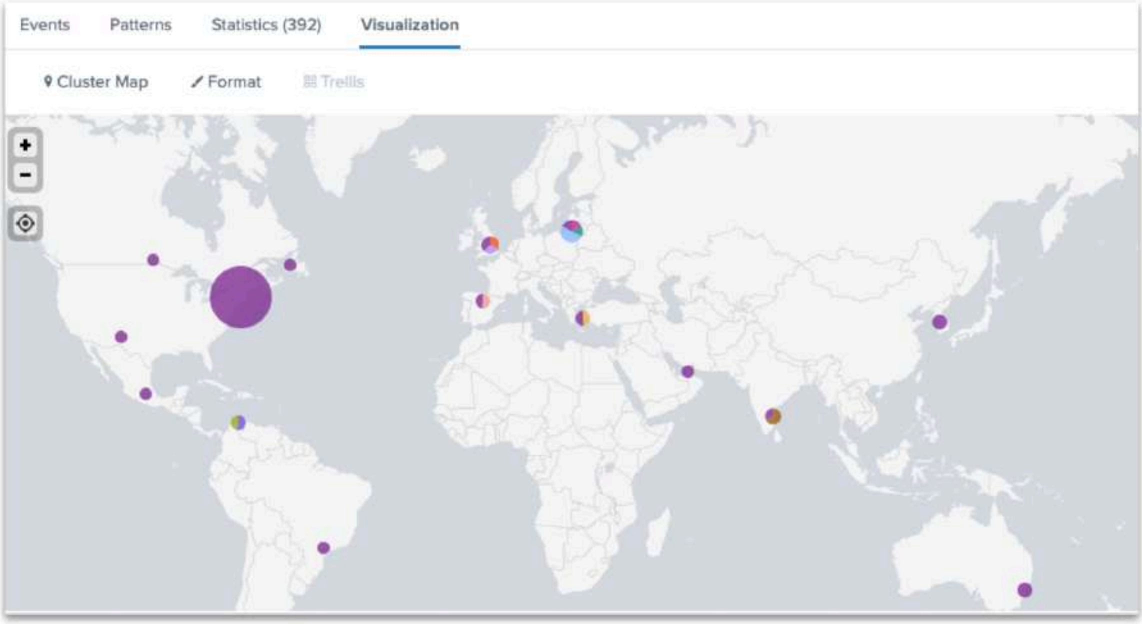
Steps

1. First, search for all web server events and use the `iplocation` and `geostats` commands to count the events by **City** (**Note:** 'City' is one of the fields in our data that's created when we use the `iplocation` command):

   ```
   index=main sourcetype=access_combined
   | iplocation clientip | geostats count by City
   ```

2. If it isn't selected already, click on the **Visualization** tab. For your visualization type, choose **Cluster Map**.

   You should now have a map showing the location of clients (i.e. customers) connecting to the company website.

   Don't forget to add the resulting map to your dashboard and give your panel a name such as '**Security/Fraud: Customer Locations**'.

Lab 7 – Customise Your Dashboard

Description

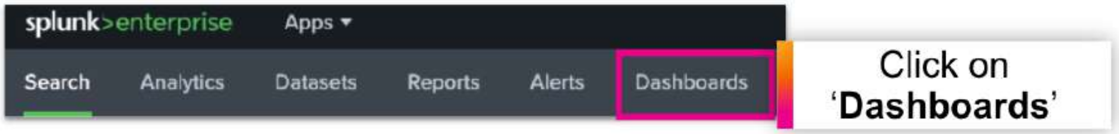
Having a dashboard with multiple panels is powerful, but the layout of your dashboard is also important to ensure that the information presented is clear and easy for users to consume.

The Buttercup Enterprises Marketing team has seen what we've built so far and have provided us with a custom background image that they would like us to use on our new dashboard. In this Lab we will upload the custom background image and rearrange our panels to work with the new background. Finally, we will configure each of our dashboard panels to use the global time picker so it's all ready to share with the business!

Steps

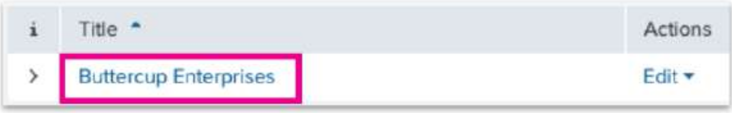
Add a Custom Background Image to Your Dashboard

1. First, open your dashboard. To do that, click on **Dashboards** in the top menu bar.

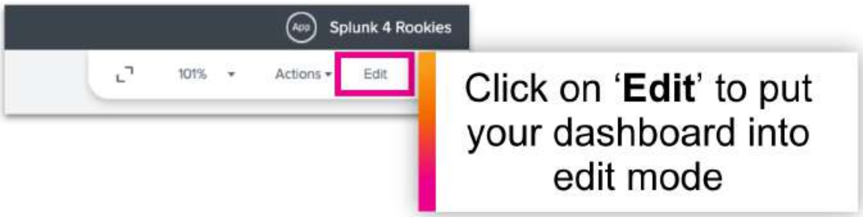


Click on 'Dashboards'

2. Click on the name of your dashboard to open it.



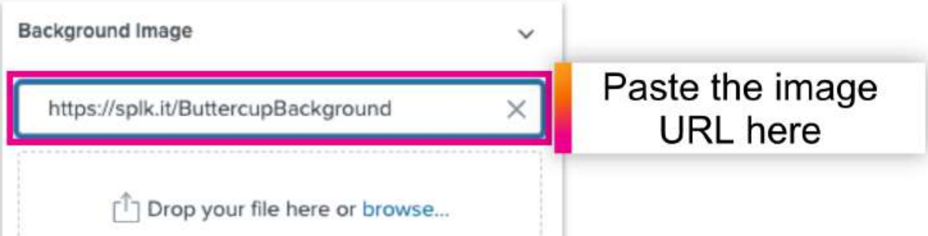
3. Click on the **Edit** button to put your dashboard into edit mode.



Click on '**Edit**' to put your dashboard into edit mode

4. Locate the **Background Image** section and copy/paste the following image URL into the '**Enter URL**' box:

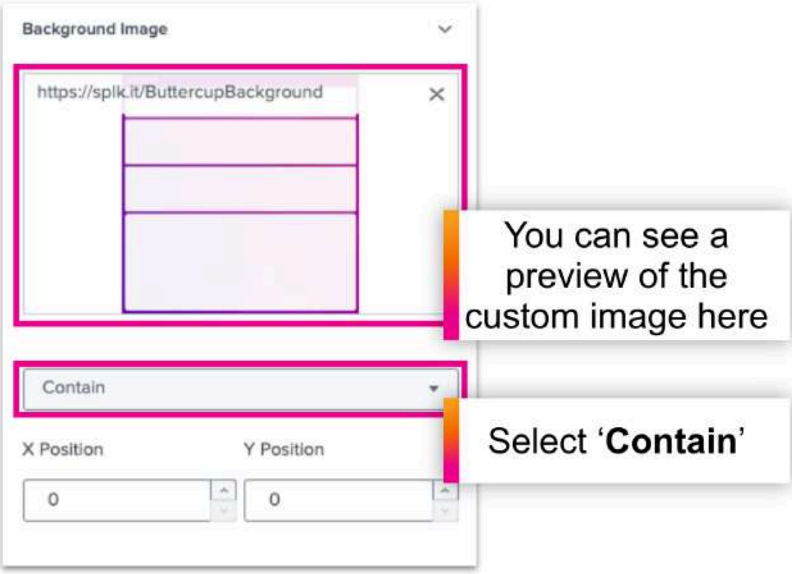
```
https://splk.it/ButtercupBackground
```


Background Image
https://splk.it/ButtercupBackground
Drop your file here or browse...

Paste the image URL here

To upload the image, either hit the Enter key on your keyboard or click anywhere on your dashboard.

To ensure that our custom image is contained within the dimensions of our dashboard, click on the dropdown list beneath the image preview and select **‘Contain**’.



Background Image

https://splk.it/ButtercupBackground

Contain

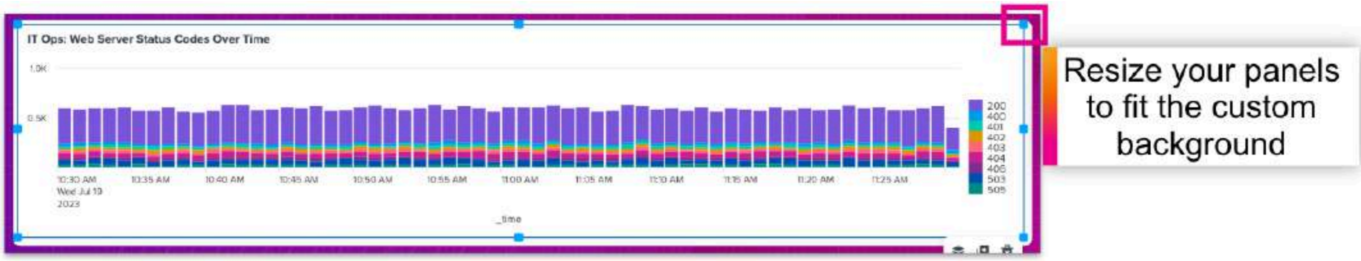
X Position: 0

Y Position: 0

You can see a preview of the custom image here

Select ‘**Contain**’

5. Now click on each dashboard panel and drag the blue squares that appear around the edges of the panels to resize them to fit within the areas on your custom background image.

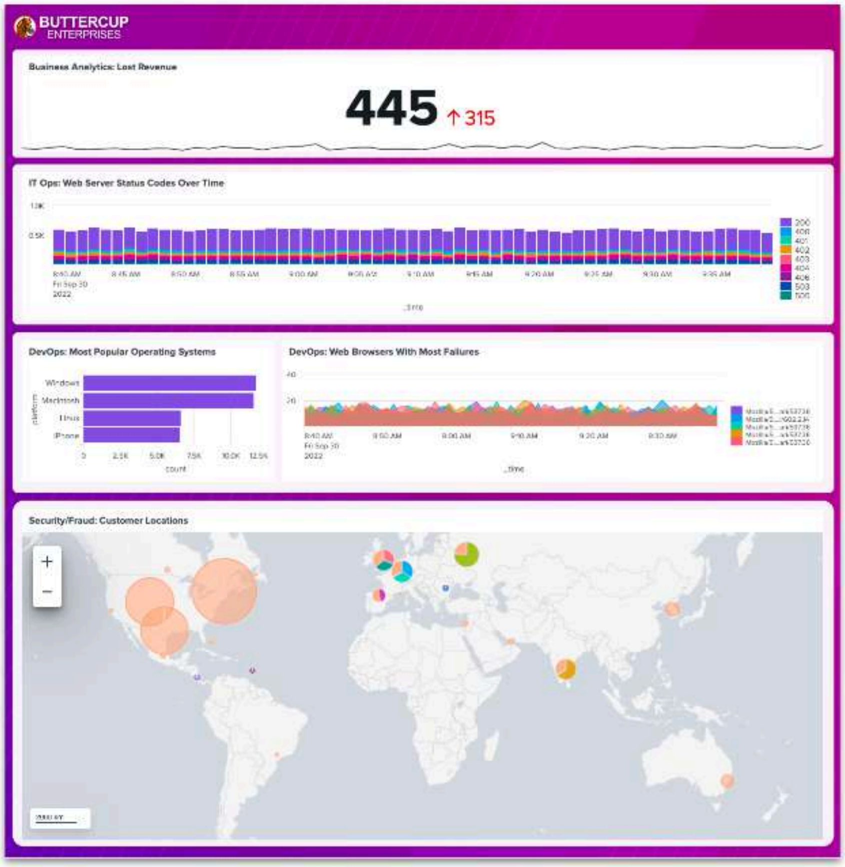


IT Ops: Web Server Status Codes Over Time

Resize your panels to fit the custom background

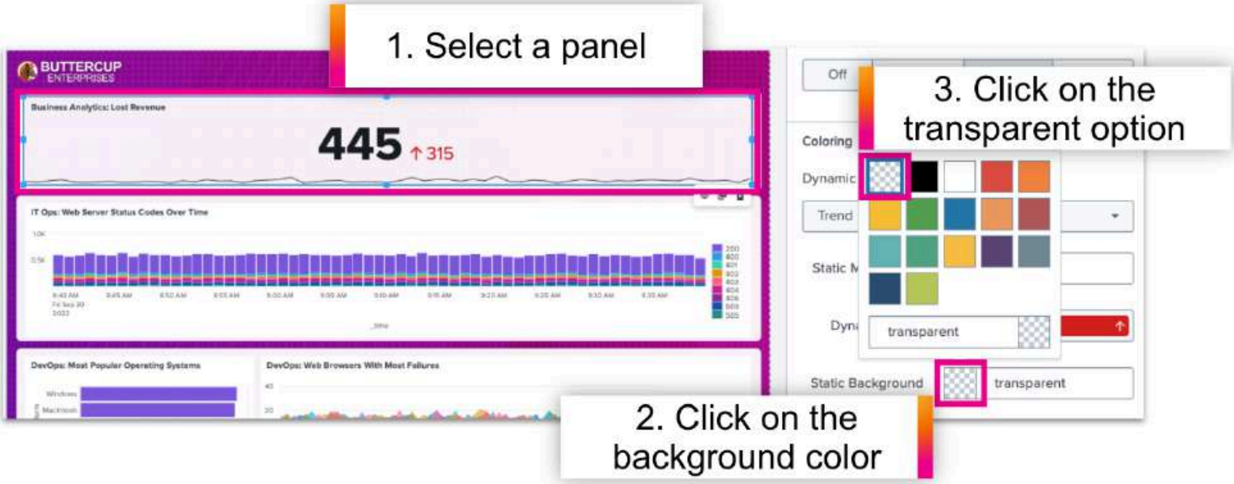
Be sure to click on **Save** when you’ve finished rearranging everything!

When you're finished, your dashboard should now look something like this:


BUTTERCUP
ENTERPRISES
Business Analytics: Lost Revenue
445 ↑315
IT Ops: Web Server Status Codes Over Time
DevOps: Most Popular Operating Systems
Windows
Macintosh
Linux
iPhone
count
DevOps: Web Browsers With Most Failures
_time
Security/Fraud: Customer Locations

6. Finally, since we have a nice colored background to show off we can set each panel to be transparent to help the color to shine through! To do this, click on a dashboard panel and in the Configuration panel on the right find the **Coloring** section.

   Find the '**Background**' or '**Static Background**' option for your panel (the name will vary from visualization to visualization) and change the background color to be transparent. Repeat this step for each dashboard panel. Note that the Cluster Map visualization has no background color option so you can ignore this panel.

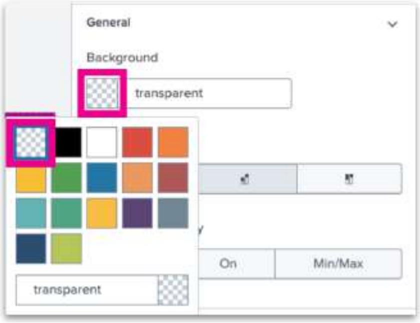

1. Select a panel

2. Click on the background color

3. Click on the transparent option

BUTTERCUP
ENTERPRISES
Business Analytics: Lost Revenue
445 ↑315
IT Ops: Web Server Status Codes Over Time
DevOps: Most Popular Operating Systems
DevOps: Web Browsers With Most Failures
Off
Coloring
Dynamic
Trend
Static
Dyn
transparent
Static Background
transparent

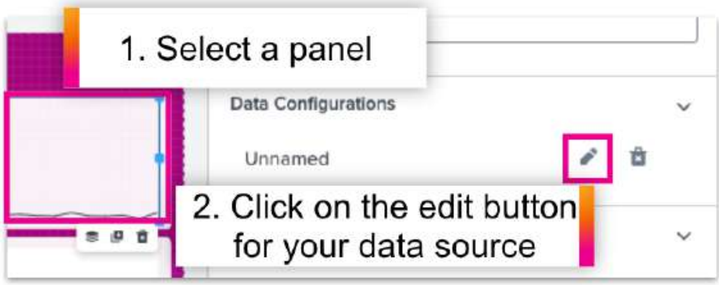
Note: Some visualizations may have a slightly different name for the background color setting, for example:



Link Your Dashboard Panels to the Global Time Picker

The global time picker is included in all new dashboards by default and allows you to control the time range of all dashboard panels from a single place. Since each of our panels was using a static time range (i.e. **Last 60 minutes**) when we added them to our dashboard we just need to switch each panel to use the global time picker instead.

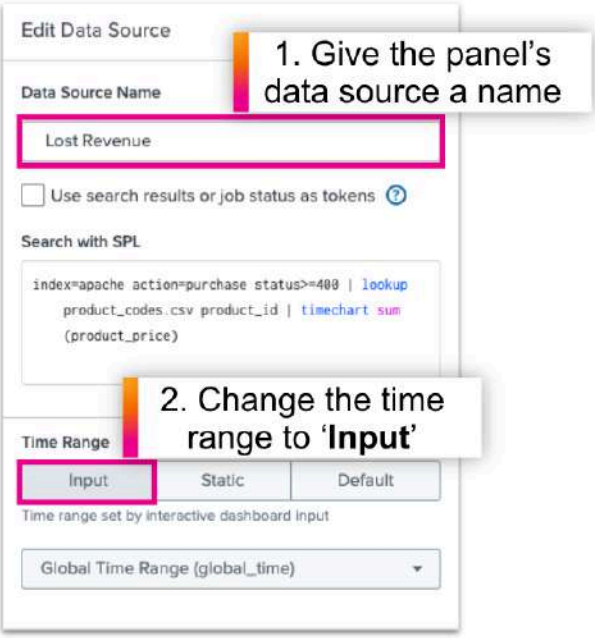
1. With your dashboard in edit mode, click a dashboard panel and in the Configuration panel on the right find the **Data Configurations** section. Click on the pencil icon to edit the '**Unnamed**' data source.



1. Select a panel

2. Click on the edit button for your data source

2. To make changes to the data source we will need to give each data source a name. For simplicity, use the name of the dashboard panel. For example, if you're working with our Single Value visualization panel, use 'Lost Revenue' as the data source name.



Edit Data Source

Data Source Name: Lost Revenue

□ Use search results or job status as tokens

Search with SPL

```
index=apache action=purchase status>=400 | lookup
    product_codes.csv product_id | timechart sum
    (product_price)
```

Time Range: [✓ Input] Static Default

Time range set by interactive dashboard input

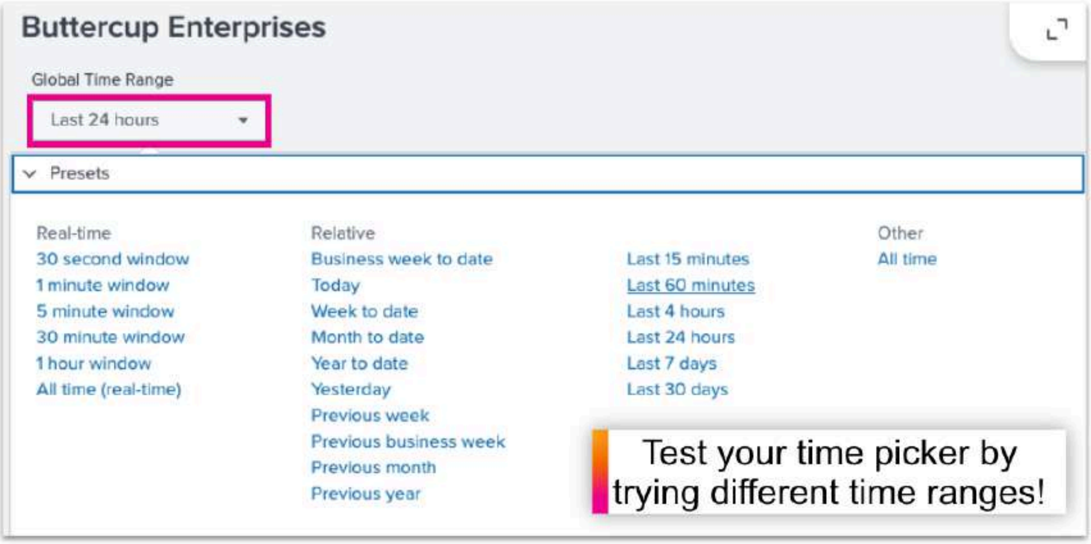
Global Time Range (global_time)

1. Give the panel's data source a name

2. Change the time range to '**Input**'

3. Click on **Apply & Close** to save your panel changes. Repeat this step for each dashboard panel and save your dashboard.

   Now that you've linked all your panels to the global time picker, click on **Save** and then click on **View** to view your updated dashboard. Try changing the search time range for your dashboard by choosing different time ranges from the dropdown list. All of your panels should update to reflect the time setting.



Test your time picker by trying different time ranges!

Lab 8 - Financial Services: exploring additional use cases

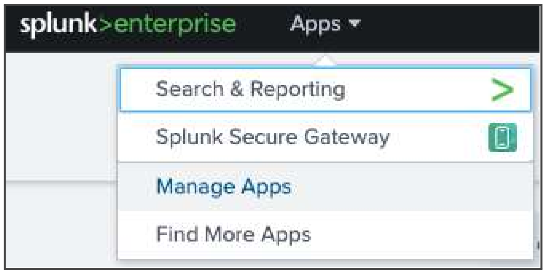
Description

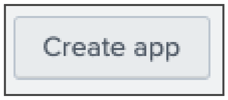
Now that we have some familiarity with using the Splunk interface, let’s have a look at a few examples of FSI specific data, and build out a dashboard that shows insights across a number of different FSI use cases.

Steps

Create a new app

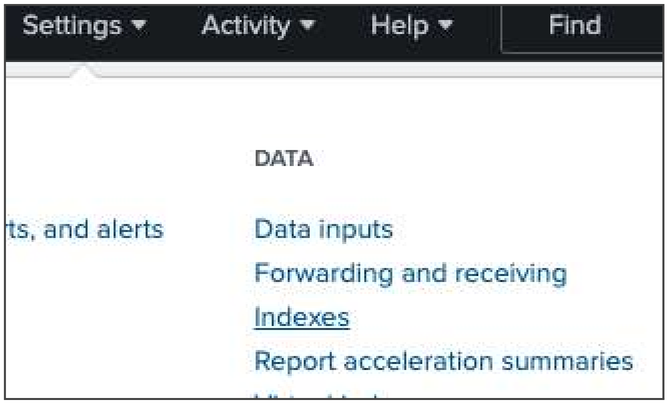
Create a new app for this part of the lab? e.g. “Financial Services Insights”



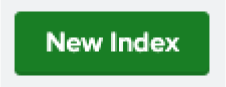


Create a new index

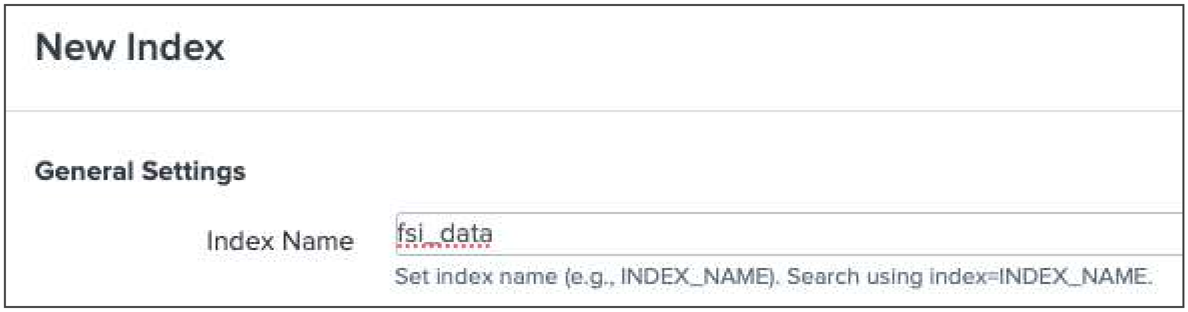
From the **Settings** menu, select **Indexes** in the **Data** section



Click the **New Index** button



Give the Index a meaningful name, to reflect the data being ingested



New Index

General Settings

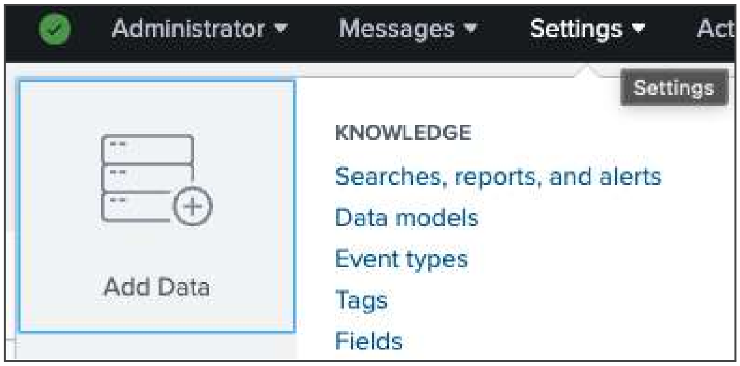
Index Name: fsi_data

Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

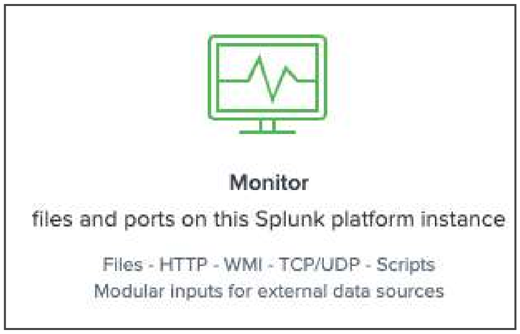
In the **App** settings, ensure you replace “Search & Reporting” with your app name “Financial Services Insights”
Click **Save** button

Add data to Index

Add data using the **Monitor** method. Select **Add Data** icon from **Settings** menu option.



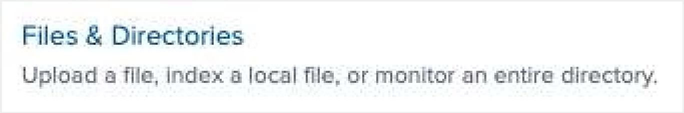
Select the **Monitor** icon



Monitor
files and ports on this Splunk platform instance

Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources

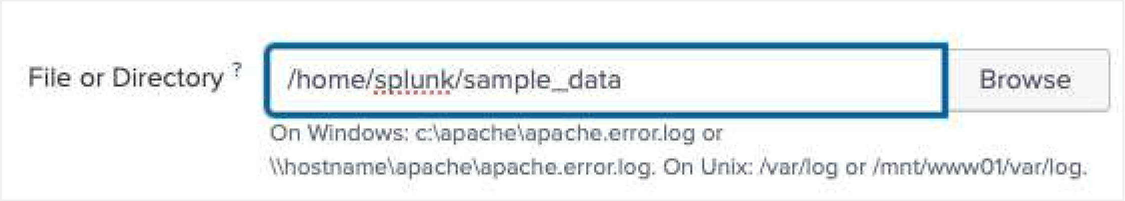
We will be monitoring a number of files in a single directory



Files & Directories

Upload a file, index a local file, or monitor an entire directory.

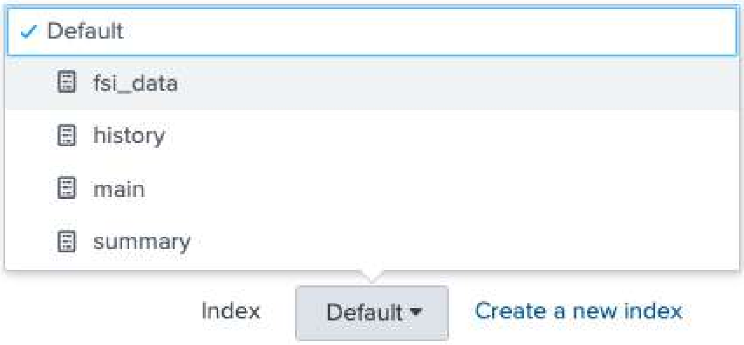
Locate the sample data in /home/splunk/sample_data



File or Directory ? /home/splunk/sample_data

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

Choose the **fsi_data** index as the target index for this data source



Confirm data is present

```
index=fsi_insights
```

You should see ~14k events over 2023

Run Sample Searches

Run these example searches and add them to a dashboard - create a new dashboard in the first instance, then add the remaining searches to the same dashboard by selecting “save to existing”

Banking Fraud: Waiving Large Fee

```
index=* source=*waive.csv | sort - _time | where fee>50 | table _time customer
employee fee waived
```

Banking Fraud: New Account Login Trellis Action Chart

This example shows a Trellis chart for different actions upon new account logins over time. Monitoring this condition is important to improve customer experience.

```
index=* source=*new_today.csv" | timechart count by action fixedrange=F
```

Set the visualisation as a **Trellis**, arrange by **action**

New Credit Limit Requested Amount Over Time

Customers have asked for a credit limit increase. This example provides a time chart that shows the average new credit limit amount requested over time to help monitor the potential available credit needed.

```
index=* source=*credit_limit_requests.csv | timechart span=10m fixedrange=F
avg(new_limit) as requested_limit
```

Payment Response Statistics: Top 10 Customers with Highest Amounts Processed

```
index=* source=*RequestResponse.csv | stats count  values(_time) as _time
values(amount) as amount by customer | where count>2 AND (count%2==0) | eval
CompletedPayments=count/2 | top CompletedPayments by customer | sort
-CompletedPayments | head 10 | fields - count, percent
```

ATM Location Fraud

Find users who have used ATMs at more than one location in under a minute.

```
index=* source=*ATM_list.csv" | search action=withdrawal | eval
amount=tostring(round(amount, 2),"commas") | streamstats time_window=1m
dc(location) as dc list(amount) as amount list(location) as location
earliest(epoch) as epoch latest(epoch) as latest_epoch by user|where dc>1 | dedup
user | eval first_time=strftime(epoch,"%m/%d/%y %H:%M:%S"),
last_time=strftime(latest_epoch,"%m/%d/%y %H:%M:%S") | table user amount action
location first_time last_time
```

Wire Transfer Fraud: Multiple Client IPs

```
index=* source=*wire_transfer.csv | eval amount=tostring(round(amount,
2),"commas")|streamstats time_window=1m count(eval(action="authorized")) as
authorized_count list(FromAccount) as FromAccount list(ToAccount) as ToAccount
list(amount) as amount list(action) as action list(c_time) as time
values(clientIP) as clientIP dc(clientIP) as clientIP_count by customer|where
clientIP_count>=2 | table FromAccount ToAccount action amount clientIP customer
time
```

Lab 9 - Business Service Insights: exploring capability

Description

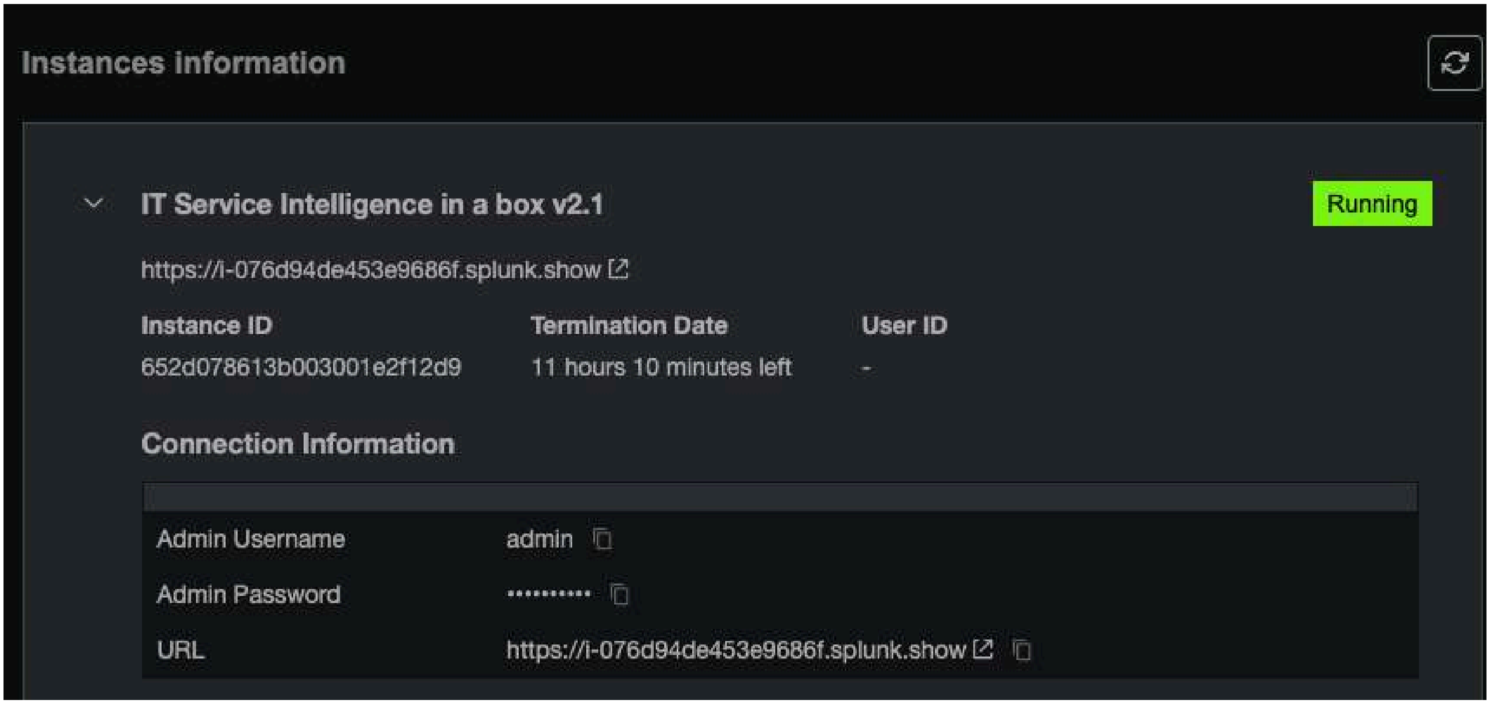
Service Insights in IT Service Intelligence (ITSI) represents the mapping and monitoring of business and technical services within your organisation. The information derived from Service Insights helps you better detect problems, simplify investigations, triage issues, and accelerate resolutions.

Within ITSI, a service is a set of interconnected applications and hosts that are configured to offer a specific service to the organisation. Services can be internal, like an organisation email system, or customer-facing, like an organisation's website. For example, creating financial reports through a web-based application requires a computer, web server, application server, databases, middleware, and network infrastructure. These applications and hosts are all configured to offer the service of financial reporting.

Steps

Switching lab environment

For the remainder of the labs, you will using the “IT Service Intelligence in box” instance



Instances information

IT Service Intelligence in a box v2.1

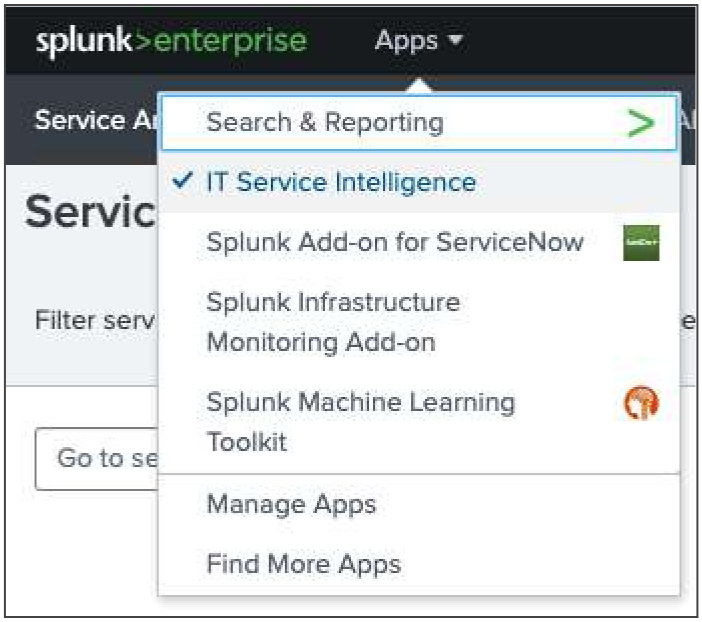
https://i-076d94de453e9686f.splunk.show

Instance ID	Termination Date	User ID
652d078613b003001e2f12d9	11 hours 10 minutes left	-

Connection Information

Admin Username	admin
Admin Password	••••••••••
URL	https://i-076d94de453e9686f.splunk.show

Navigate to the “IT Service Intelligence” app, if not already taken there after logging in

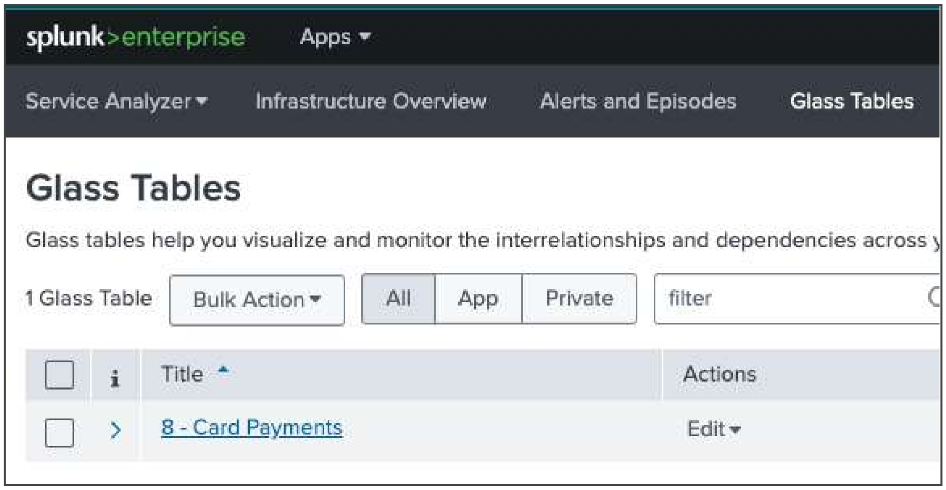

splunk>enterprise
Apps ▾
Service A
Servic
Filter serv
Go to se
Search & Reporting
✓ IT Service Intelligence
Splunk Add-on for ServiceNow
Splunk Infrastructure Monitoring Add-on
Splunk Machine Learning Toolkit
Manage Apps
Find More Apps

Exploring a Glass Table view

Glass tables allow users to visualise and monitor the interrelationships and dependencies across your IT and business services. You can use glass tables to create dynamic contextual views of your IT topology or business processes and monitor them in real time. You can add metrics like KPIs, ad hoc searches, and service health scores that update in real time against a background that you design. Glass tables show real-time data generated by KPIs and services.

Let’s explore an example Glass Table that was built to represent a “Card Payments” process that mirrors what a commercial/retail bank may need to monitor.

Locate the “Card Payments” Glass Table by selecting the Glass Tables tab from the ITSI main menu



Glass Tables

Glass tables help you visualize and monitor the interrelationships and dependencies across y

1 Glass Table

□	i	Title ▴	Actions
□	>	8 - Card Payments	Edit ▾

Select the hyperlink “8 - Card Payments” to view the Glass Table

Note that there are several other example Glass Tables which you are free to explore throughout today

Please review the following questions to help identify what we can learn about the information presented to the user. Remember that Glass Tables are completely customisable for all types of audience, so this a demonstration of the “art of the possible” - you are only limited by your imagination!

Q1: Service Health - which of the 4 services has the lowest/worst health score?

Q2: KPIs - how many Fraud alerts have occurred in the last hour?

Q3: What’s the main reason that Confirmation has a low score?

Q4: What technical components are involved in this degradation?

Exploring a Service Analyzer

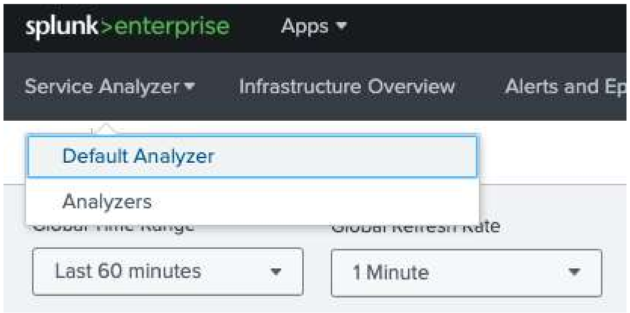
The Service Analyzer is the home page for Splunk IT Service Intelligence (ITSI) and serves as your starting point for monitoring your IT operations. The Service Analyzer enables you to see the health of your IT environment at a glance.

The Service Analyzer provides an overview of ITSI service health scores and KPI search results that are currently trending at the highest severity levels. Use the Service Analyzer to quickly view the status of IT operations and to identify services and KPIs running outside expected norms. Click on any tile in the Service Analyzer to drill down to the deep dives for further analysis and comparison of search results over time.

There are two service analyzer views: the tile view and the tree view. You can drill down to more detailed information from each view to investigate services with poor health scores.

To access the Service Analyzer, click **Service Analyzer > Default Service Analyzer** from the ITSI main menu. The tile view is the default view, but whichever view you last saved loads the next time you open the Service Analyzer.

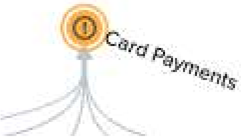
Navigate to the Default Analyzer via Service Analyzer tab



Please review the following questions to learn how the Service Analyzer can be used to determine likely root causes of issues

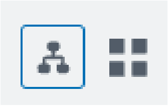
Q5: There are actually a number of services impacting Card Payments - name 2 of them. HINT: focus on the root cause.

Locate the KPIs for the Card Payment service by selecting the icon

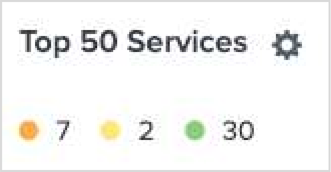


Q6: How many KPIs are there and what are their severities?

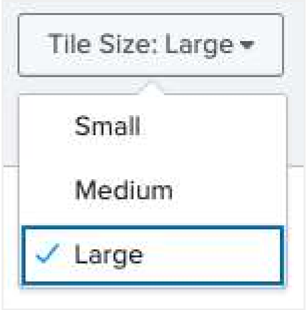
Experiment toggling between Hierarchy view and Tile view:



Using the cog icon, reduce the number of services that appear in the tile view



and experiment with different tile sizes

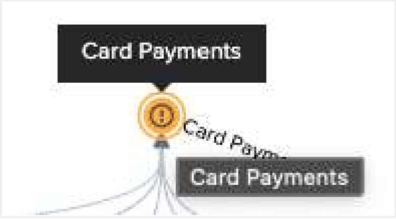


Exploring Deep Dive view

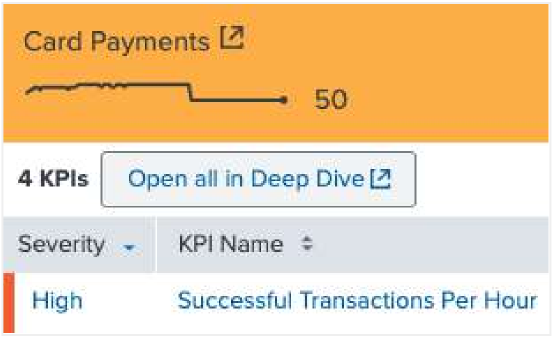
Deep dives are an investigative tool to help you identify and troubleshoot issues in your IT environment in IT Service Intelligence (ITSI). Use deep dives to view KPI search results over time, zoom-in on KPI search results, and visually correlate root cause. Stack and organise deep dive lanes to create contextual views of metrics across your services.

You can use deep dives to quickly zoom in on metric and log events, and visually correlate root cause. You can create swim lanes for both KPI and ad hoc searches, and you can customise the look of your swimlanes with unique graph types and colours to differentiate services and metrics.

In the Tree view of Service Analyzer, access Deep Dive via Card Payment service in Analyzer - ensure Card Payment icon has been selected.

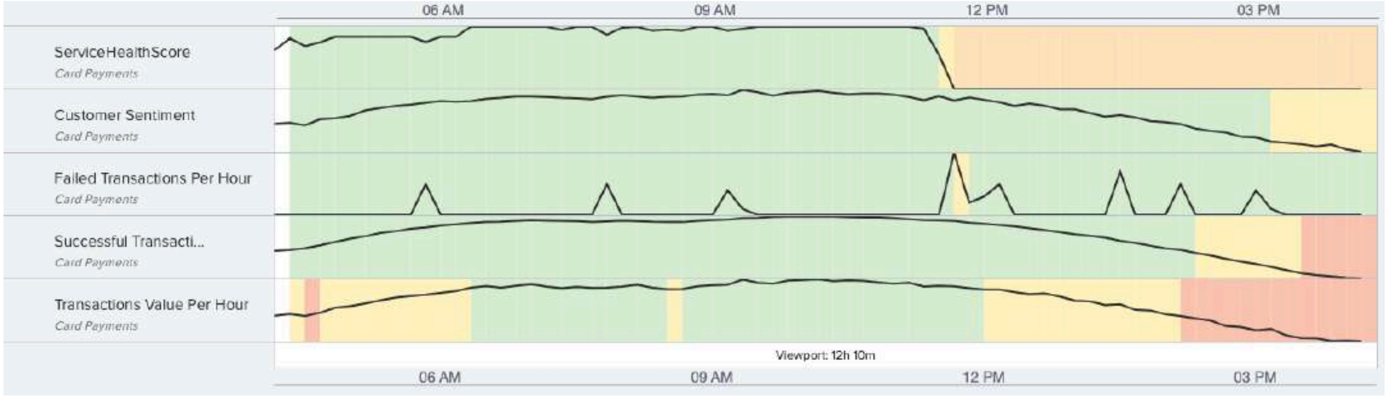


Then select “Open all in Deep Dive” link

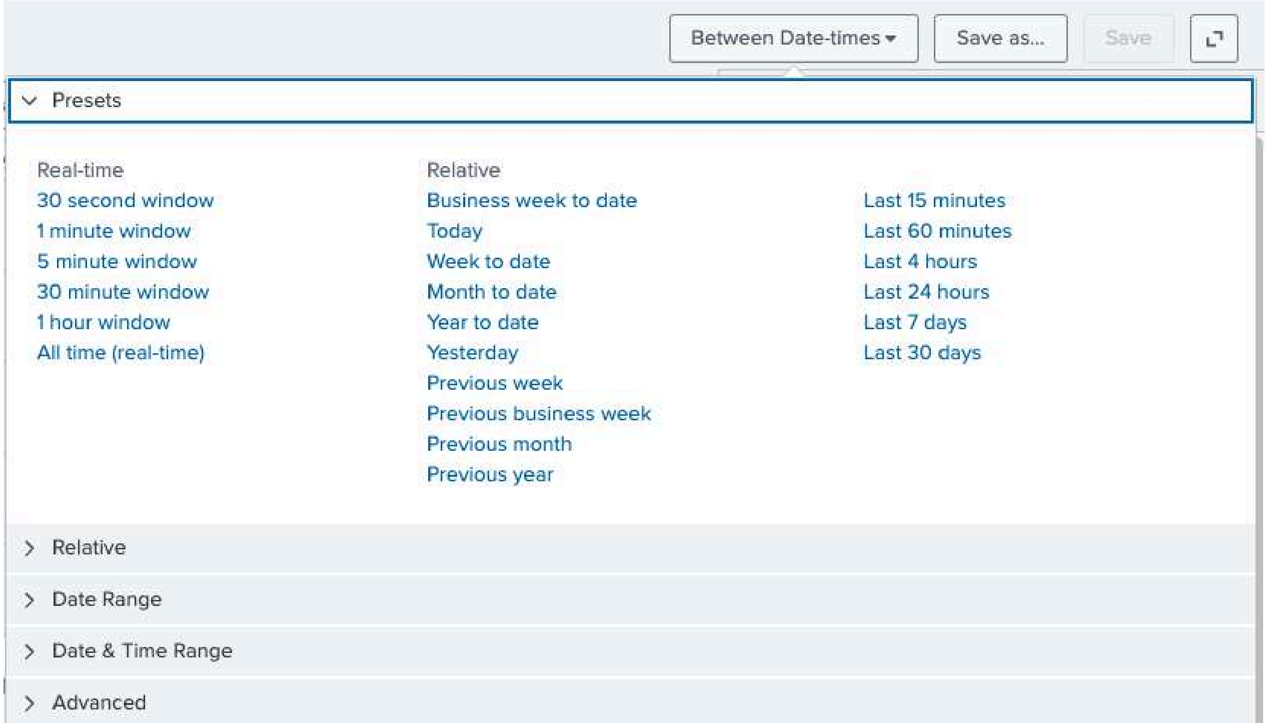


Severity	KPI Name
High	Successful Transactions Per Hour

Here we see the RAG value of KPIs over any given time range, and we can see their relationship to each other.



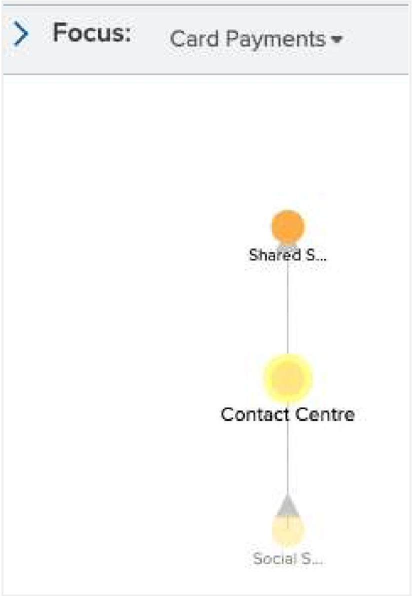
As this is Splunk, we have full control over the time range of the data displayed. Experiment with different settings.



Although we are looking at the KPIs for the Card Payment service, we can pull in any business or technical KPIs from any other service. Let’s add a KPI from the Social Sentiment service.

In the Focus view to the right of the swim-lane view, view the Contact Centre KPIs under

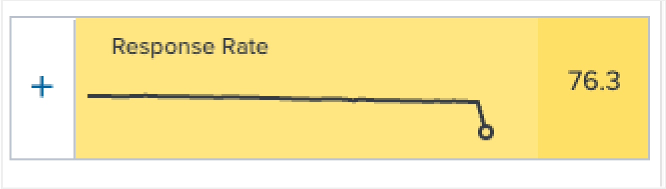
Card Payments > Shared Services > Contact Centre >Social Sentiment



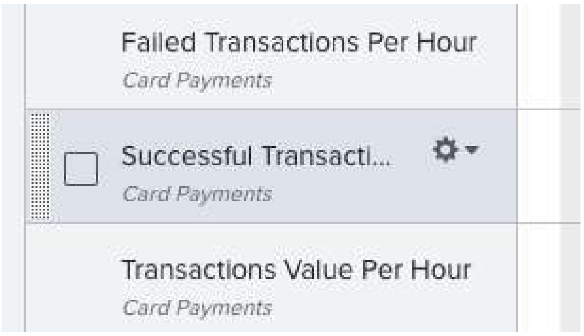
Note the various KPIs available and their individual values (red/amber/green)

Q7: Which KPIs look particularly problematic?

Add it into the deep dive view (if none stand out, pick one that is red / amber)



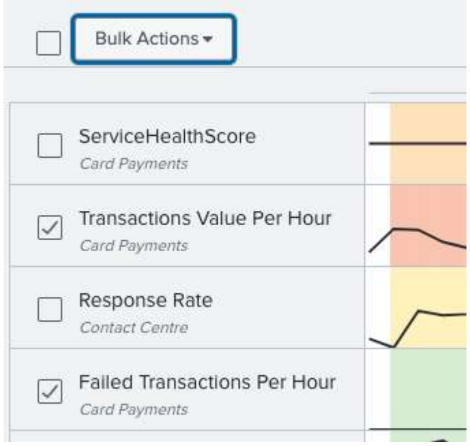
As this is a timeline view (from left to right), it would be good to be able to reorder these swimlanes, or lessen the focus on the KPIs that aren't impacting service performance. Experiment with moving the swimlanes around using the "drag" icon



Create a multi-KPI alert

Rather than being alerted when individual thresholds are breached, we want to create a “multi-KPI alert” - something where we will only be alerted if a number of thresholds are breached, using a determination of our own choosing.

Select a couple of KPIs



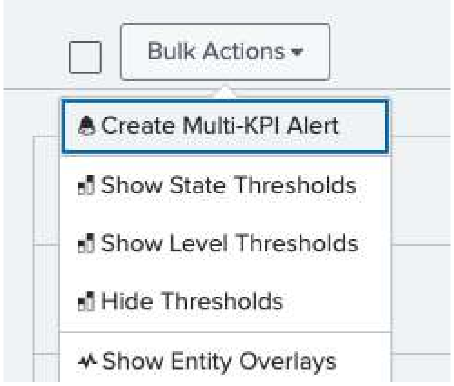
□ ServiceHealthScore
Card Payments

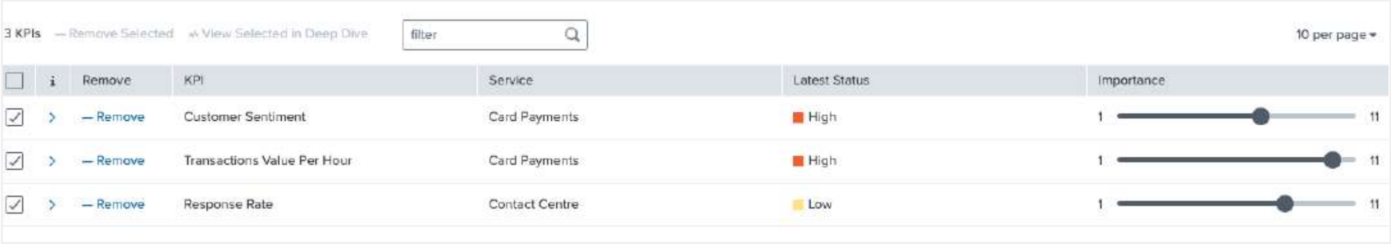
☑ Transactions Value Per Hour
Card Payments

□ Response Rate
Contact Centre

☑ Failed Transactions Per Hour
Card Payments

And then select the Bulk Action button to navigate to the alert config screen





3 KPIs — Remove Selected View Selected in Deep Dive filter 10 per page ▾

□	i	Remove	KPI	Service	Latest Status	Importance
☑	›	— Remove	Customer Sentiment	Card Payments	🟥 High	1 ——●—— 11
☑	›	— Remove	Transactions Value Per Hour	Card Payments	🟥 High	1 ——●—— 11
☑	›	— Remove	Response Rate	Contact Centre	🟨 Low	1 ——●—— 11

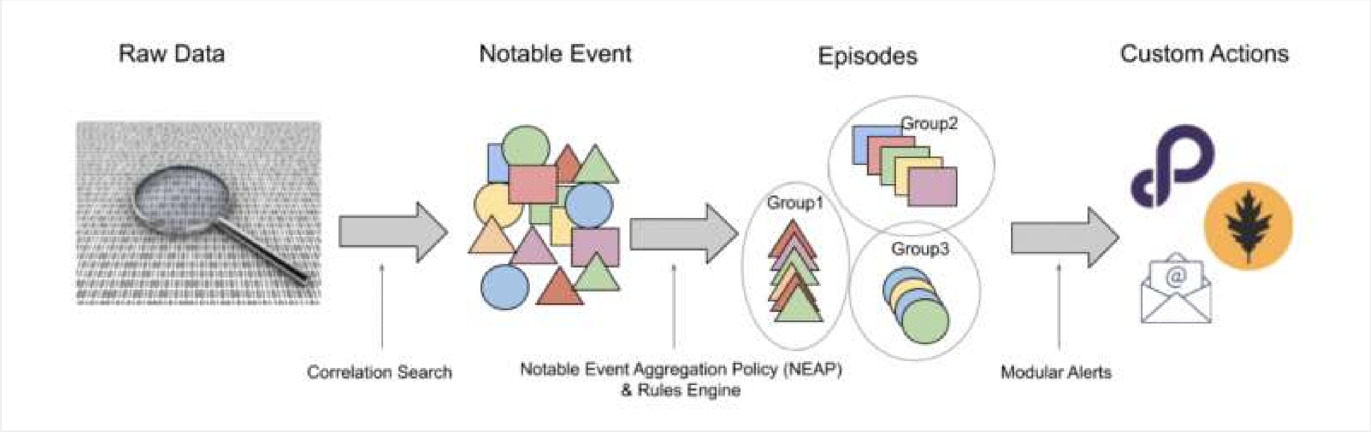
No need to save changes - there are many configurable options in this screen which we will not cover today, but are covered in our in-depth workshops.

Exploring Alerts & Episodes View

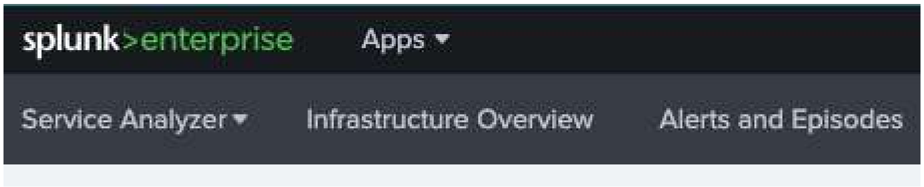
Splunk IT Service Intelligence (ITSI) Event Analytics ingests events from across your IT landscape and from other monitoring silos to provide a unified operational console of all your events and service-impacting issues. You can also integrate with incident management tools and help desk applications to accelerate incident investigation and automate remedial actions.

Event Analytics is equipped to handle huge numbers of events coming into ITSI at once. Because these events might be related to each other, they must be grouped together so you can identify the underlying problem. Event Analytics provides a way to deal with this huge volume and variety of events.

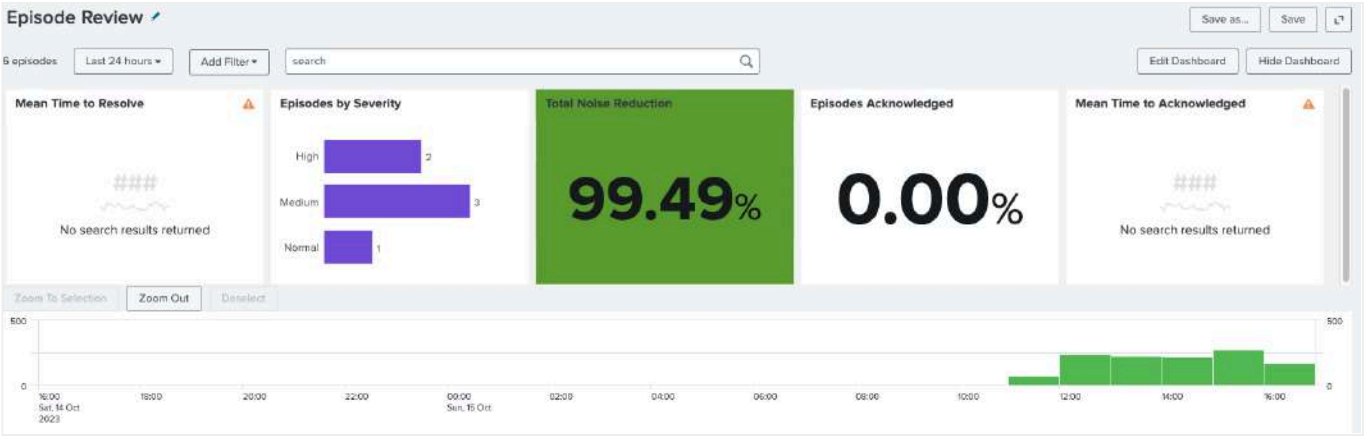
Aggregation policies reduce your event noise by grouping notable events based on their similarity and displaying them in Episode Review. An episode is a collection of notable events grouped together based on a set of predefined rules. An episode represents a group of events occurring as part of a larger sequence, or an incident or period considered in isolation. Aggregation policies let you focus on key event groups and perform actions based on certain trigger conditions, such as consolidating duplicate events, suppressing alerts, or closing episodes when a clearing event is received.



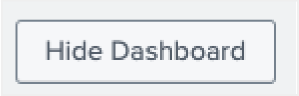
Navigate to the Alerts and Episode view via the main menu



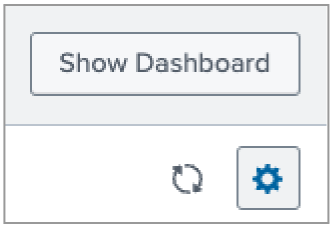
The Episode Review dashboard provides insights in high-level metrics around noise reduced through improved filtering and alerting of events



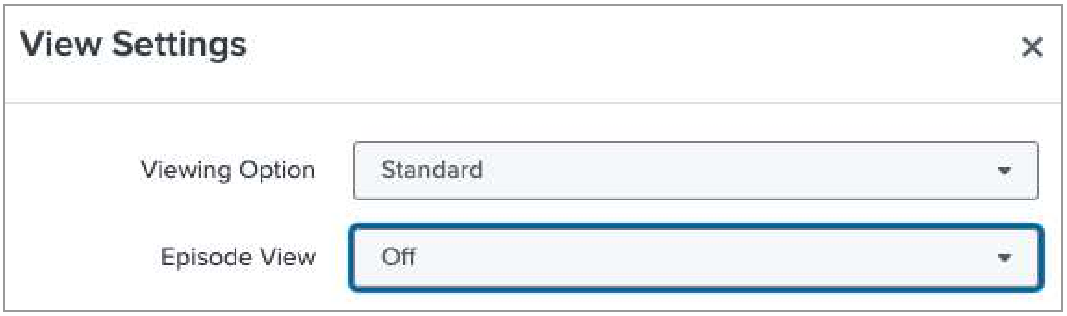
We can hide this for now



Before proceeding, ensure that “Episode View” is set to “off” via the configuration cog icon:



Toggle the “Episode View” setting as necessary:

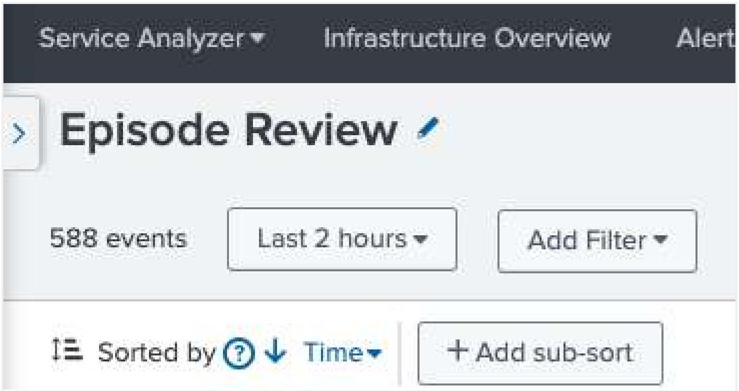


View Settings

Viewing Option: Standard

Episode View: Off

Q8: How many events have occurred in the last 2 hours (your results may differ from screenshot below)?



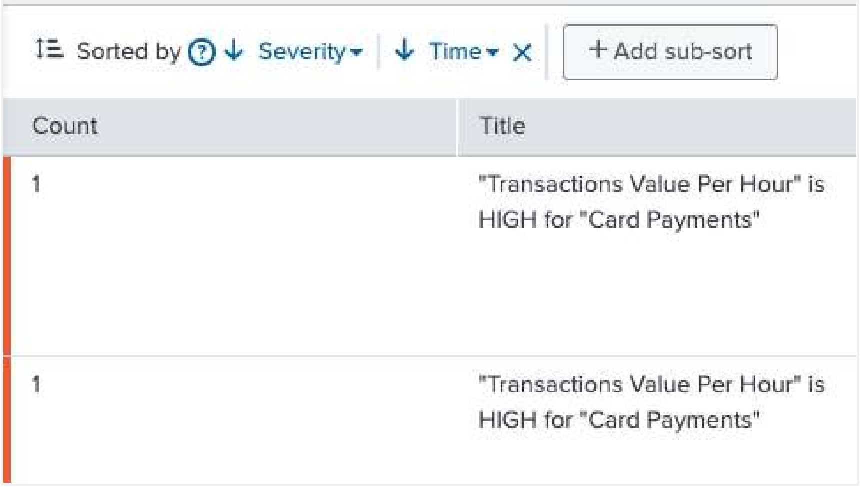
Episode Review

588 events

Last 2 hours ▾

Sorted by ↓ Time ▾

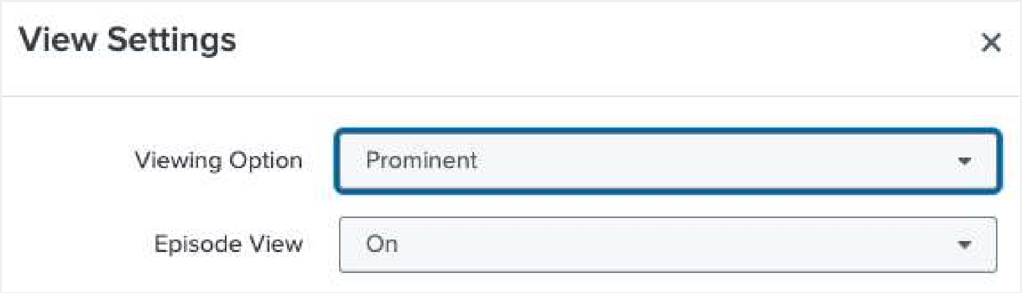
Note that you can change how events are sorted, and add additional sort settings



Sorted by ↓ Severity ▾ ↓ Time ▾

Count	Title
1	"Transactions Value Per Hour" is HIGH for "Card Payments"
1	"Transactions Value Per Hour" is HIGH for "Card Payments"

Now turn on Episode View back on and also ensure “Prominent” is selected from Viewing Option:



View Settings

Viewing Option: Prominent

Episode View: On

Q9 How many are there now? More or Less? Why do you think that is? Hint: click on one of the episodes for more information.

Congratulations - you have successfully navigated through IT Service Intelligence.

Lab 10 - Business Service Insights: building out a service view

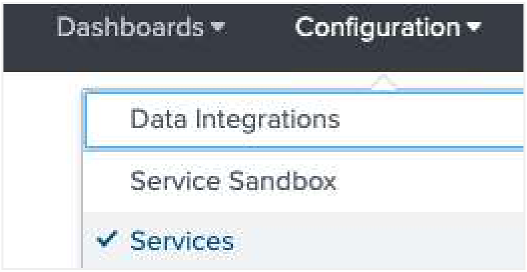
Description

Now that you have explored some of the key features of ITSI, now is the time for you to start building out a few examples yourself.

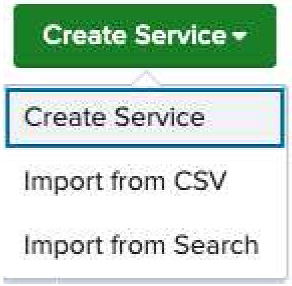
Steps

Build a new service

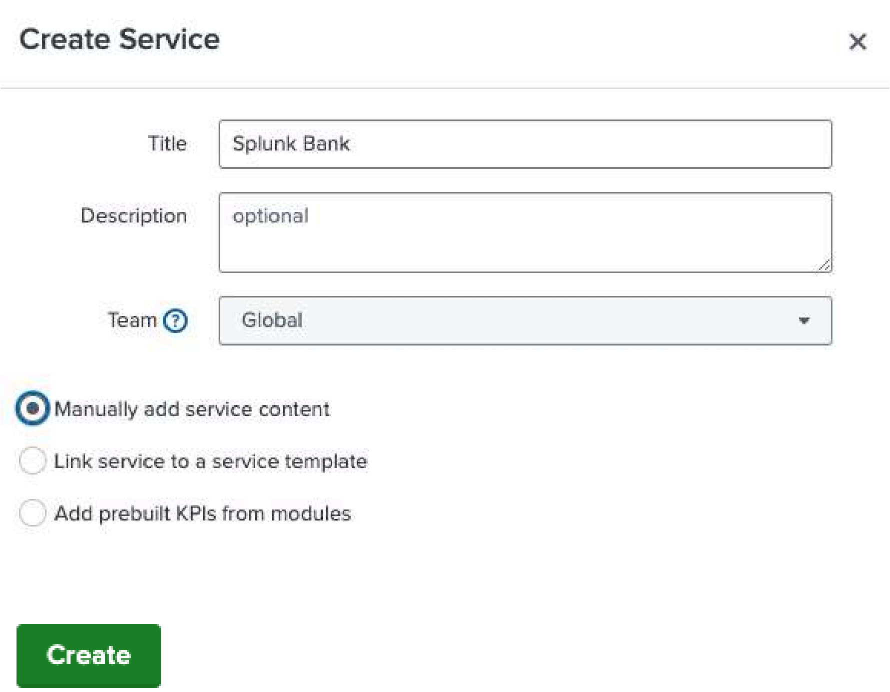
Create a new service named after your org e.g. “Splunk Bank” by selecting the **Configuration** tab from the main menu, and then selecting **Services**.



Create a new service using the first option but note that there are multiple ways to create a service hierarchy e.g. we would not expect users to manually create large/complex service trees



This will be a service that contains a number of sub-services, and we will manually add service content for now



Create Service

Title: Splunk Bank

Description: optional

Team: Global

● Manually add service content

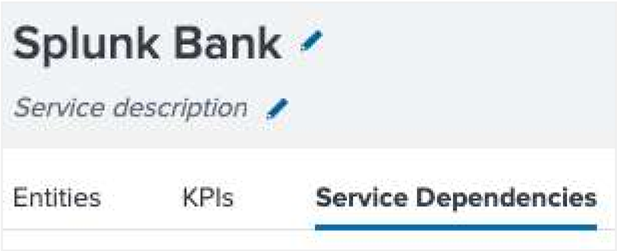
○ Link service to a service template

○ Add prebuilt KPIs from modules

Add pre-existing service configurations to the new service

Now that we have a high-level service ready for configuration, we can start to add content to it. For this step, we will reuse some pre-existing lab content, namely a set of **Shared Services**.

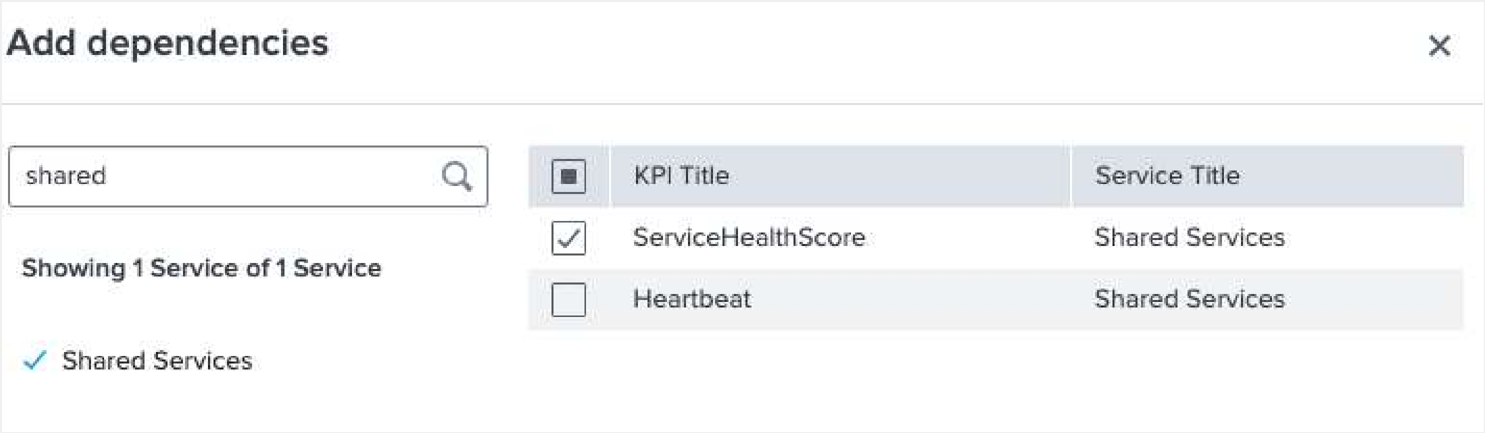
Select the **Service Dependencies** tab



And then click the **Add dependencies** button

Add service dependency of Shared Services, using the filter. We only need to pull in the ServiceHealthScore at this point.

Click **Done** button.



shared

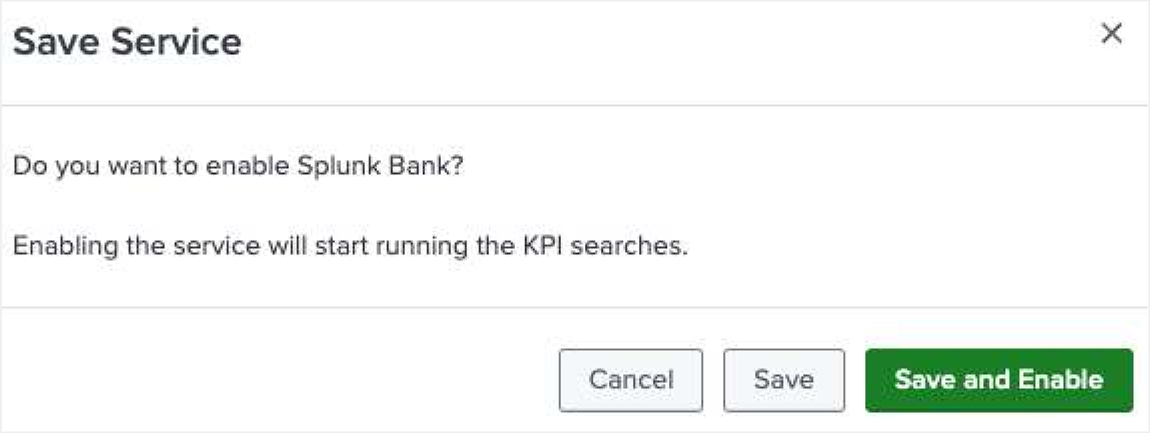
Showing 1 Service of 1 Service

✓ Shared Services

■	KPI Title	Service Title
☑	ServiceHealthScore	Shared Services
□	Heartbeat	Shared Services

Save your progress

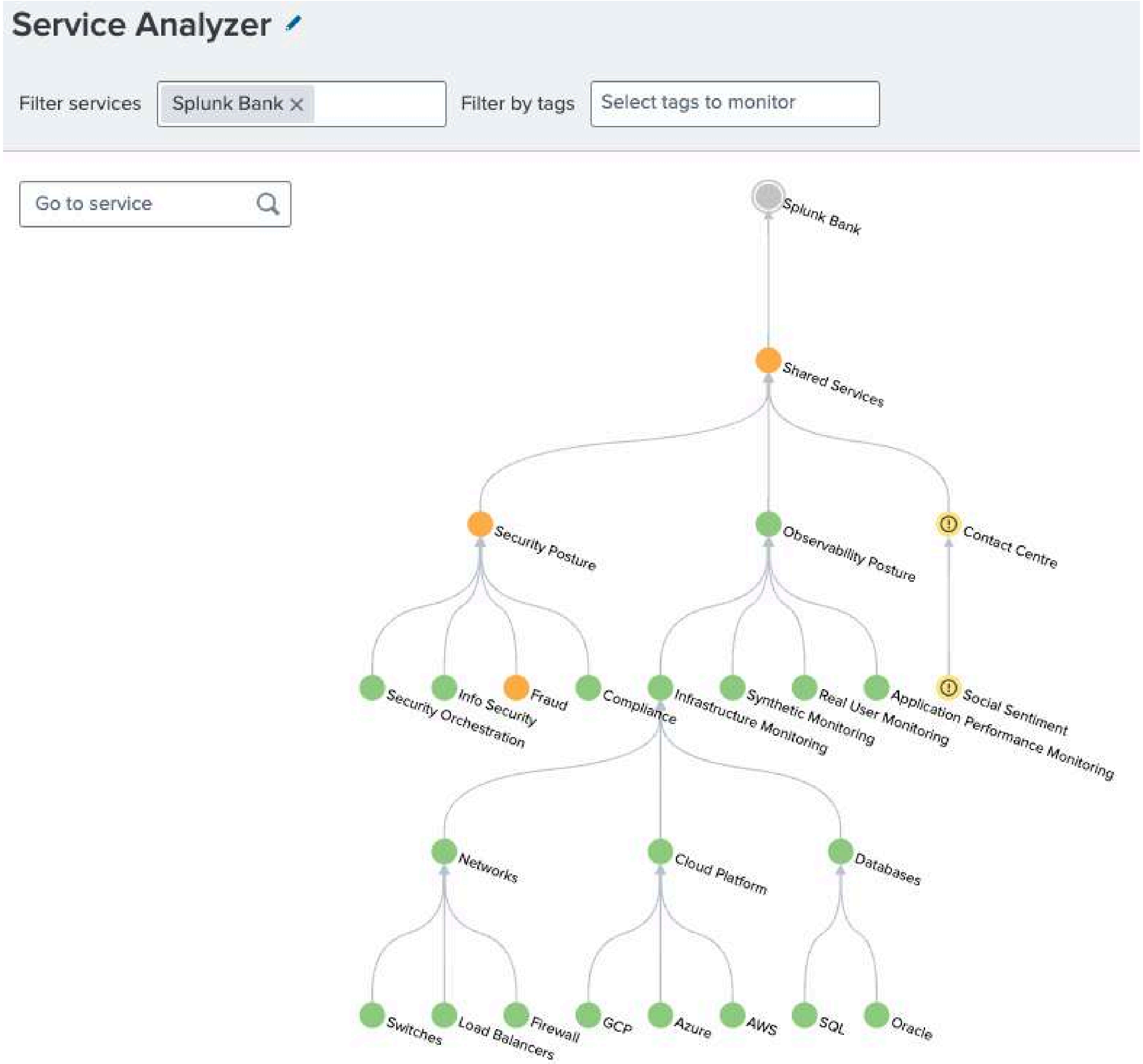
You'll need to save all changes and enable the service to start generating live KPIs



Do you want to enable Splunk Bank?

Enabling the service will start running the KPI searches.

Check your work: Go to **Service Analyzer** and hide existing Payments config by filtering on your new service name created above



Service Analyzer

Filter services: Splunk Bank ×

Filter by tags: Select tags to monitor

Go to service

Save new service analyzer. Now whenever you choose Default Service Analyzer, only your new service tree will be visible.

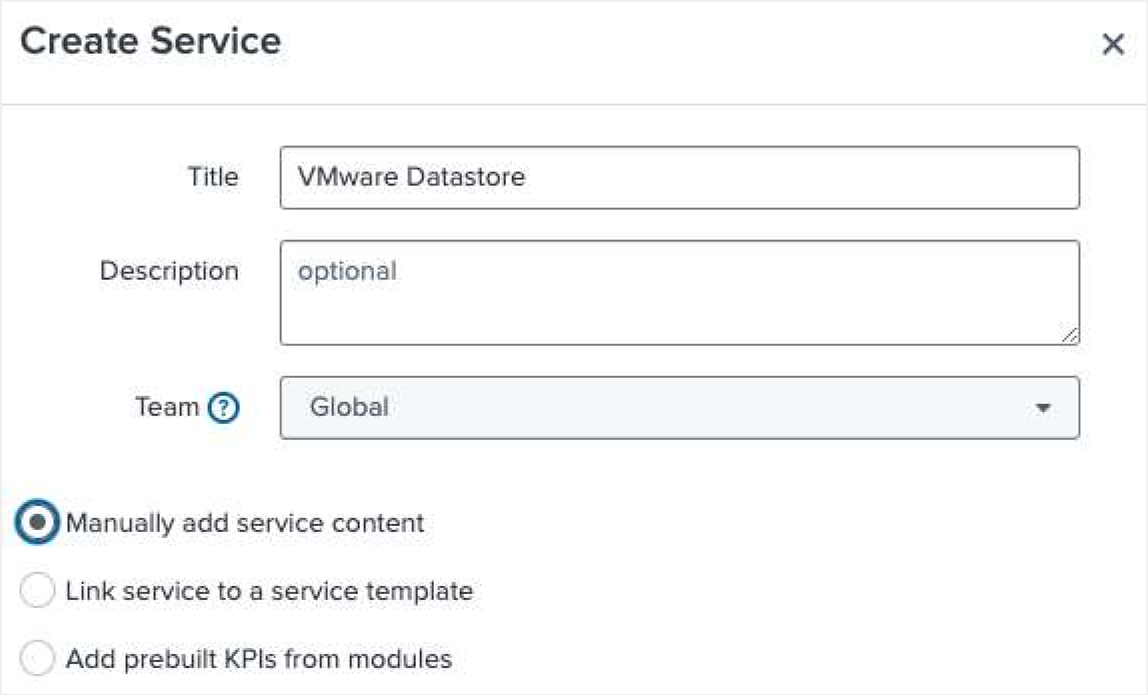
Save your work and this will become the new Default Service Analyzer:

Add new VMware service

Let’s create some new visibility into our VMware environment, by adding it as a dependent service, with a few sub-services, and associated KPIs.

Navigate to the service creation via **Configuration** tab and selecting **Services** from menu drop-down

New Service “VMware Datastore”, using the “Manually add service content” method



Create Service

Title: VMware Datastore

Description: optional

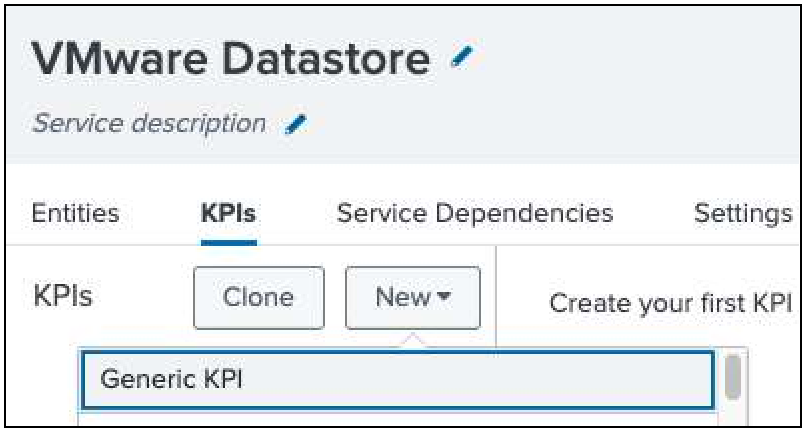
Team: Global

● Manually add service content

○ Link service to a service template

○ Add prebuilt KPIs from modules

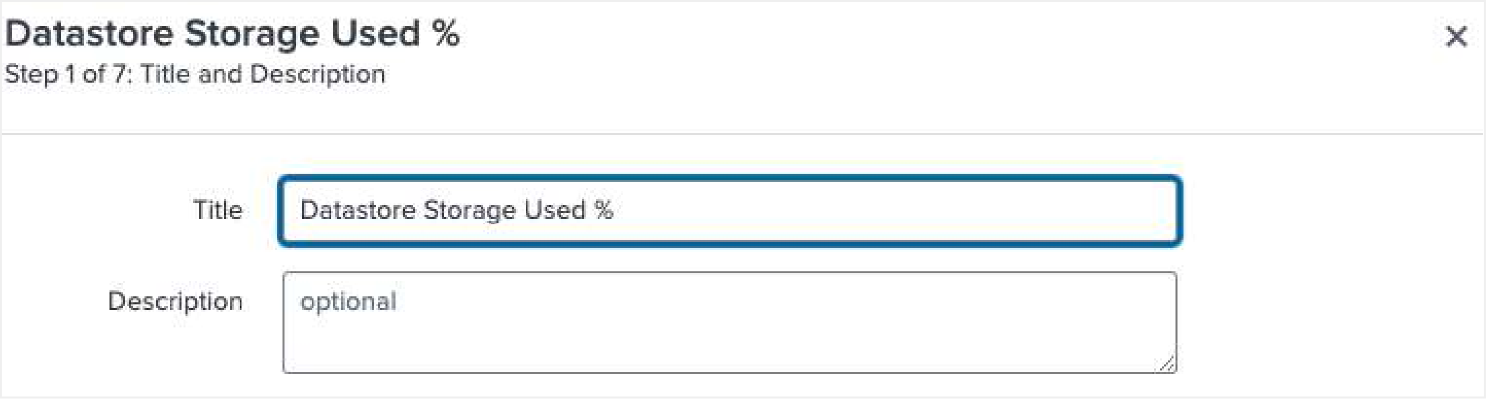
Select KPIs tab and create a new Generic KPI



VMware Datastore

Service description

Add new generic KPI titled “Datastore Storage Used %” , click Next button to proceed



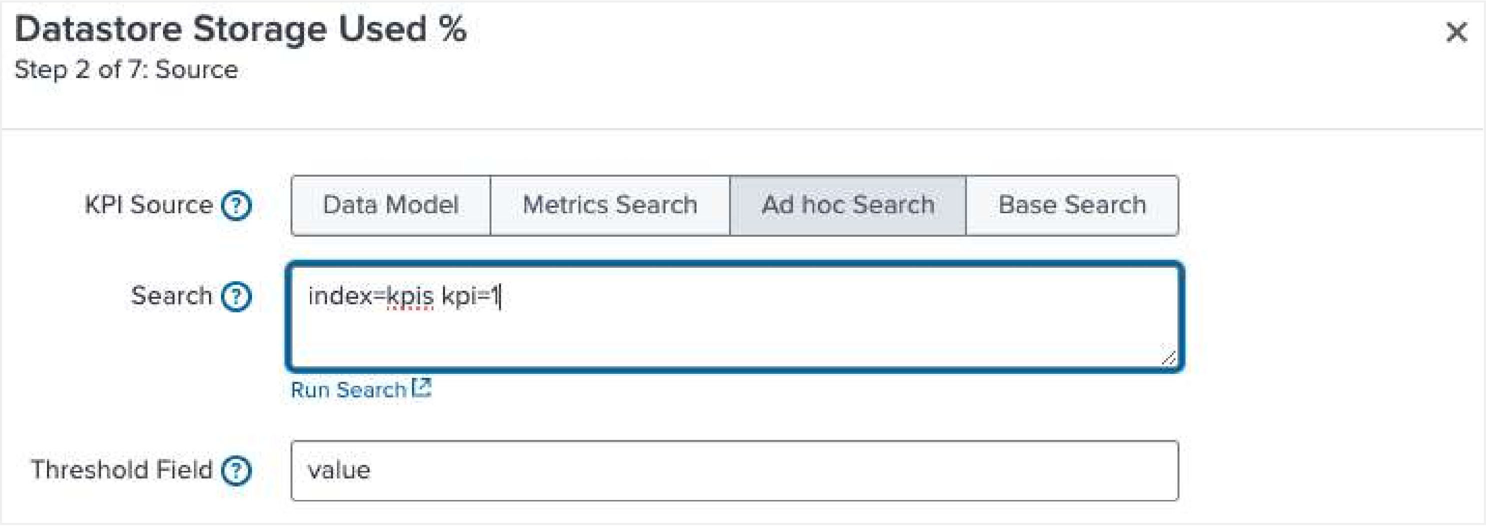
Datastore Storage Used %

Step 1 of 7: Title and Description

Title: Datastore Storage Used %

Description: optional

We are going to pull the value of the KPI from an existing set of KPI demo data



Datastore Storage Used %

Step 2 of 7: Source

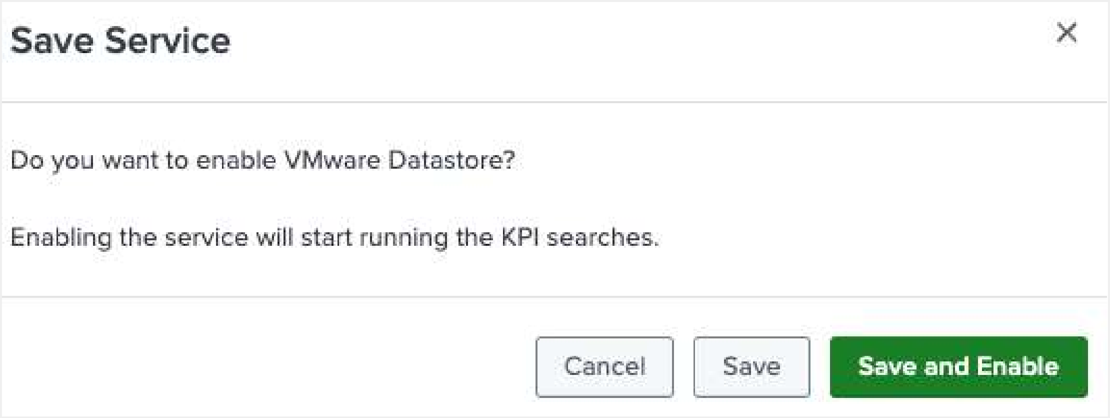
KPI Source: Data Model | Metrics Search | Ad hoc Search | Base Search

Search: index=kpis kpi=1

Threshold Field: value

We don’t need additional configuration so click **Finish** button (it will be grey)

Click **Save** button and **Save and Enable** button



Save Service

Do you want to enable VMware Datastore?

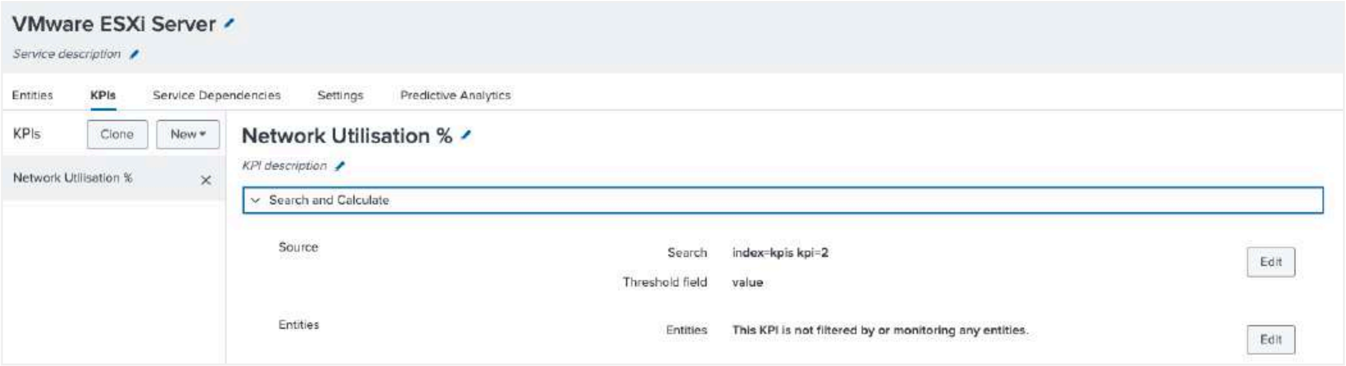
Enabling the service will start running the KPI searches.

Repeat the above steps for another service using:

- Service Names: “VMware ESXi Server”
- KPI Title: “Network Utilisation %”
- Ad-hoc search: index=kpis kpi=2

Remember to **Save** and **Save and Enable**.

Your updates should match the screenshot below



VMware ESXi Server

Service description

Network Utilisation %

KPI description

Source

Search: index=kpis kpi=2

Threshold field: value

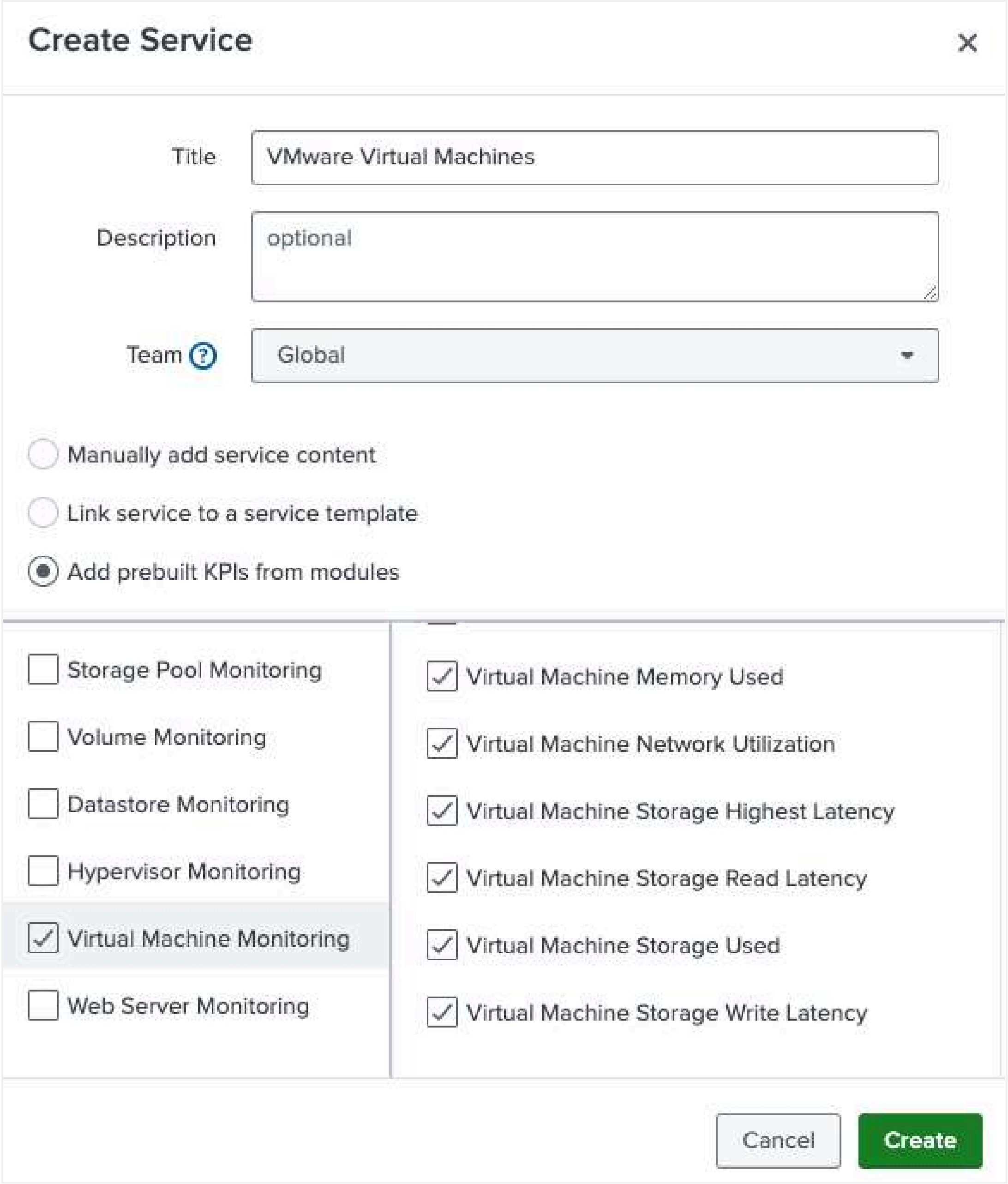
Entities

Entities: This KPI is not filtered by or monitoring any entities.

Create service using pre-built content / KPIs

Create a new service “VMware Virtual Machines”, this time selecting “Add prebuilt KPIs from modules” from the options

Select “Virtual Machine Monitoring” from the list of modules and note the 10 KPIs pre-selected (you can pick and choose)



Create Service

Title: VMware Virtual Machines

Description: optional

Team: Global

○ Manually add service content

○ Link service to a service template

● Add prebuilt KPIs from modules

□ Storage Pool Monitoring

□ Volume Monitoring

□ Datastore Monitoring

□ Hypervisor Monitoring

☑ Virtual Machine Monitoring

□ Web Server Monitoring

☑ Virtual Machine Memory Used

☑ Virtual Machine Network Utilization

☑ Virtual Machine Storage Highest Latency

☑ Virtual Machine Storage Read Latency

☑ Virtual Machine Storage Used

☑ Virtual Machine Storage Write Latency

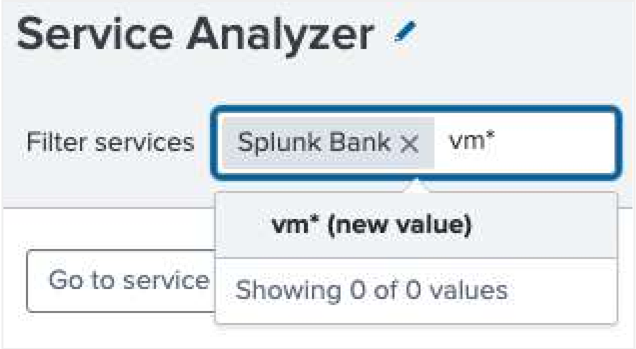
Click **Create** button

As this is a pre-build module designed specifically for VMware monitoring, it has an existing configuration for determining entities (specific hosts) within a VMware environment. We are not leveraging entities today so this can be ignored.

Test your new configuration

Now return to your Service Analyzer view and add a new filter “VM*” to see your new config.

Ensure that you click on the “vm* (new value)” item from the list



Q10: Are your new KPIs appearing and do they have values?

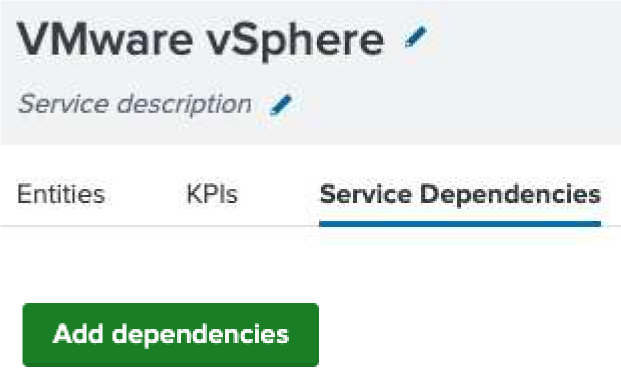
Q11: What else do you notice about the service tree?

Create service mappings to create a holistic view

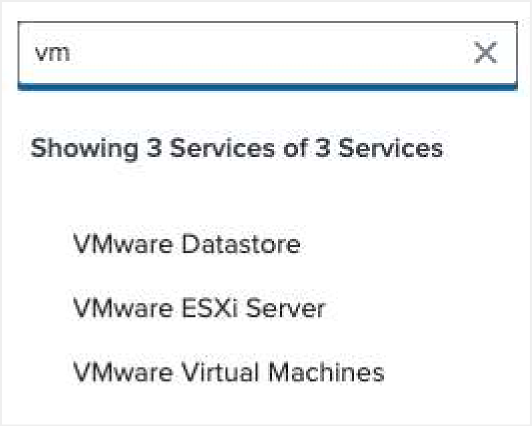
Let’s connect them up and add them to our overall business service monitoring “your Org”

Create a fourth and final service called “VMware vSphere”, using the “manually add service content” method.

From **Service Dependencies** tab, select **Add dependencies**



Filter by “vm”



vm

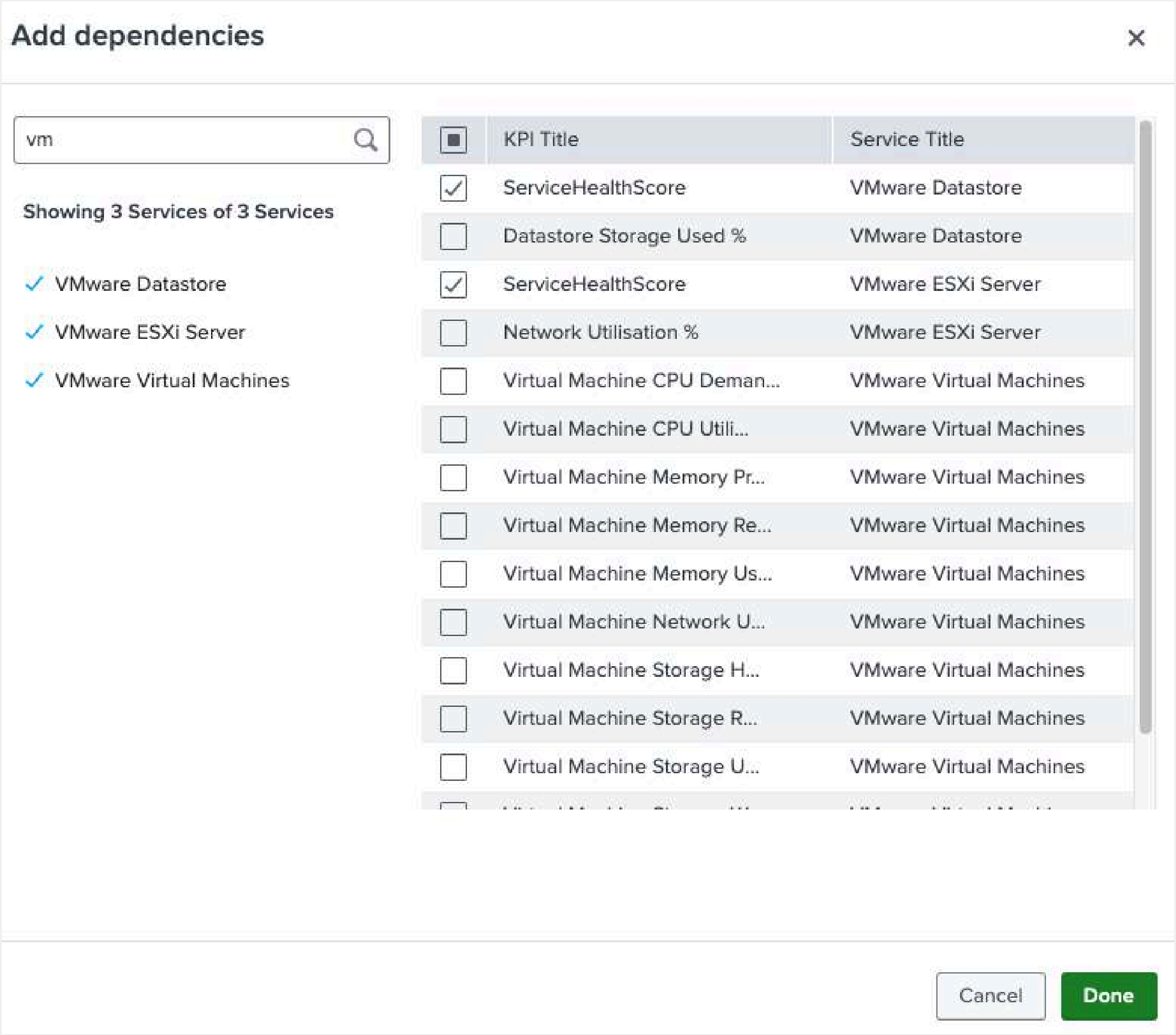
Showing 3 Services of 3 Services

VMware Datastore

VMware ESXi Server

VMware Virtual Machines

Select each of **VMware Datastore**, **VMware ESXi Server** and **VMware Virtual Machines**, and the ServiceHealthScore for each.



Add dependencies

vm

Showing 3 Services of 3 Services

✓ VMware Datastore

✓ VMware ESXi Server

✓ VMware Virtual Machines

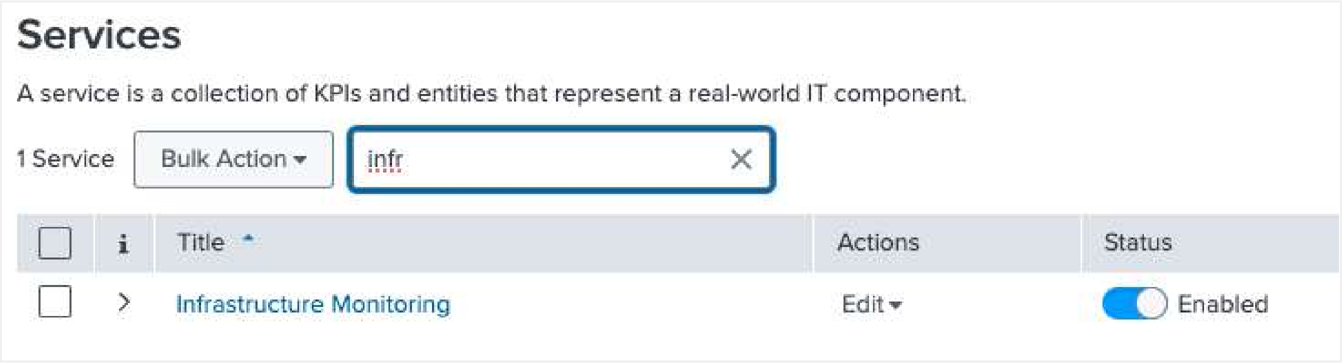
■	KPI Title	Service Title
☑	ServiceHealthScore	VMware Datastore
□	Datastore Storage Used %	VMware Datastore
☑	ServiceHealthScore	VMware ESXi Server
□	Network Utilisation %	VMware ESXi Server
□	Virtual Machine CPU Deman...	VMware Virtual Machines
□	Virtual Machine CPU Utili...	VMware Virtual Machines
□	Virtual Machine Memory Pr...	VMware Virtual Machines
□	Virtual Machine Memory Re...	VMware Virtual Machines
□	Virtual Machine Memory Us...	VMware Virtual Machines
□	Virtual Machine Network U...	VMware Virtual Machines
□	Virtual Machine Storage H...	VMware Virtual Machines
□	Virtual Machine Storage R...	VMware Virtual Machines
□	Virtual Machine Storage U...	VMware Virtual Machines

We only need the health score of each, so ensure only those three boxes are selected.

Click **Done** button.

Make sure you save the changes and also select **Save and Enable**.

Now add this new service to “your Org” - as VMware is clearly in the “technical” ranking (vs “business service”), it makes sense to add this to our existing “Infrastructure Monitoring” service



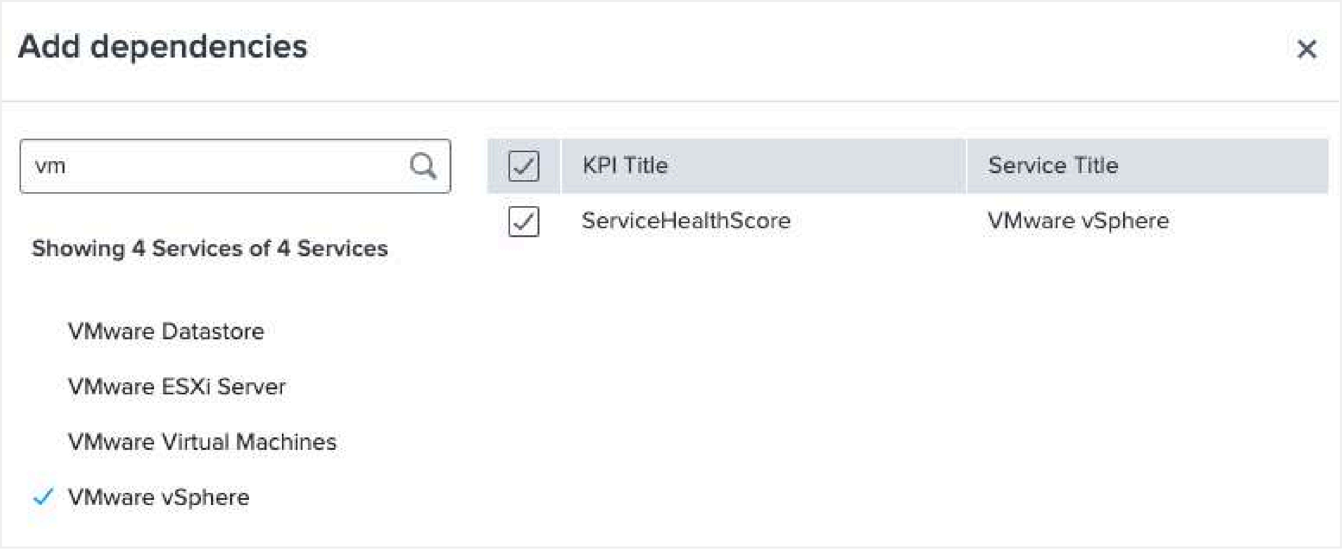
Services

A service is a collection of KPIs and entities that represent a real-world IT component.

1 Service | Bulk Action ▾ | infr ✕

□	i	Title ▴	Actions	Status
□	>	Infrastructure Monitoring	Edit ▾	Enabled

And edit that service and add “VMware vSphere” as a dependency.



Add dependencies ✕

vm

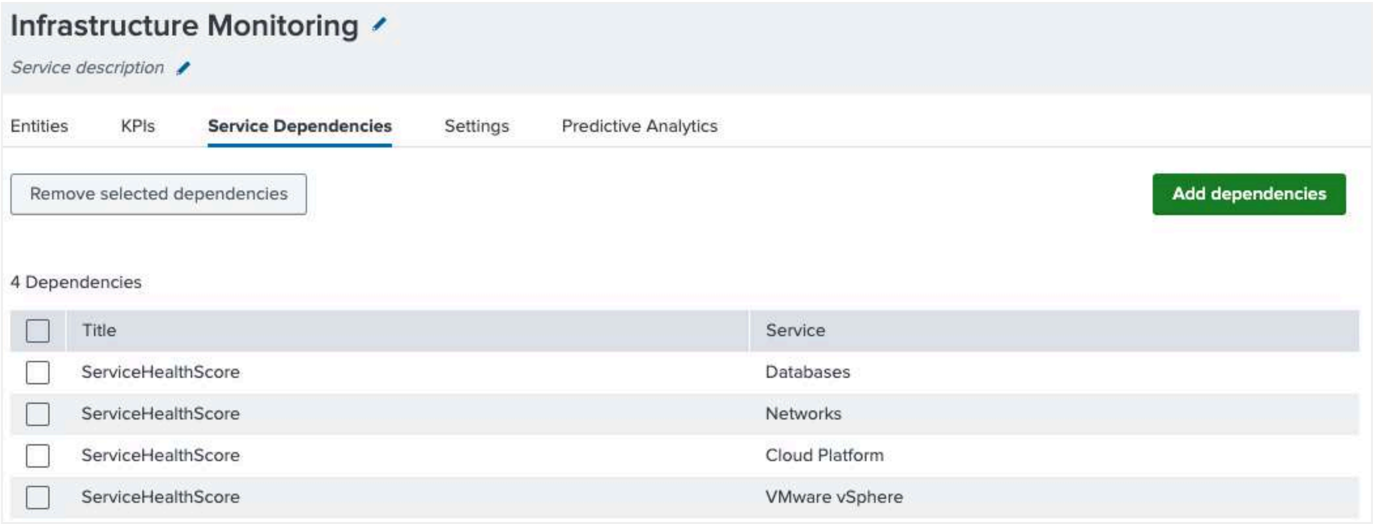
Showing 4 Services of 4 Services

VMware Datastore
VMware ESXi Server
VMware Virtual Machines
✓ VMware vSphere

☑	KPI Title	Service Title
☑	ServiceHealthScore	VMware vSphere

Click **Done** button

Check your progress:



Infrastructure Monitoring

Service description

Entities KPIs **Service Dependencies** Settings Predictive Analytics

Remove selected dependencies

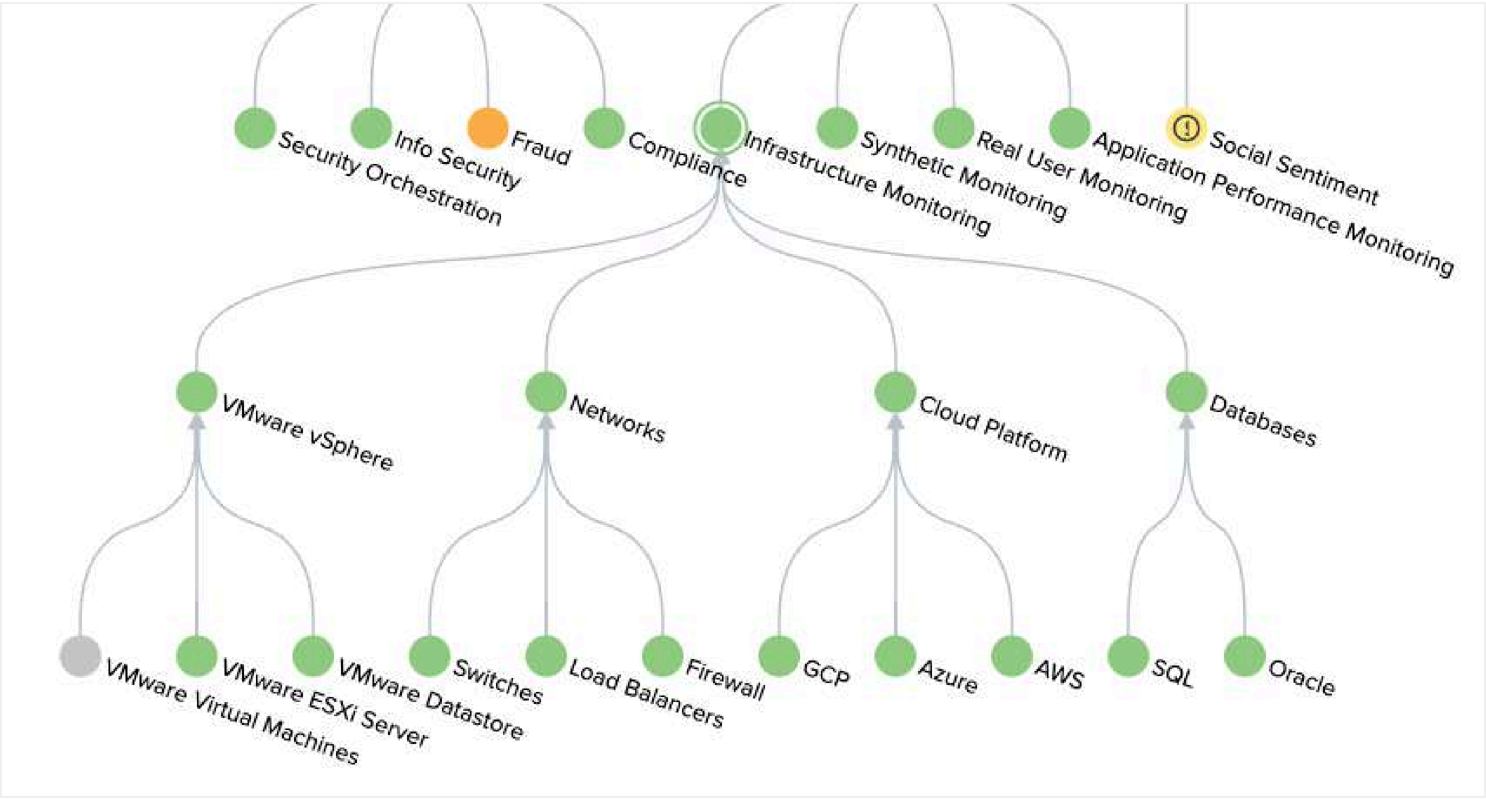
Add dependencies

4 Dependencies

□	Title	Service
□	ServiceHealthScore	Databases
□	ServiceHealthScore	Networks
□	ServiceHealthScore	Cloud Platform
□	ServiceHealthScore	VMware vSphere

Save your work.

Now view your Service Analyzer to confirm everything is set up as expected. Did you manage to get your VMware services all connected up correctly? If you did - well done! If not, please ask for help.



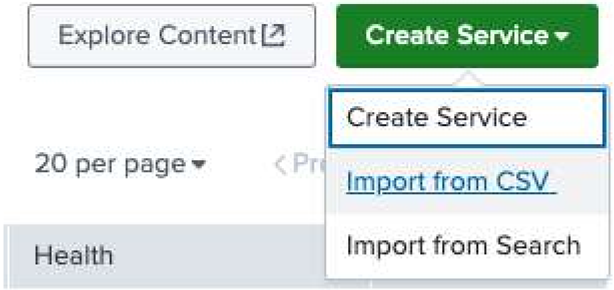
We no longer need to filter on “vm*” so we can remove that (and save)

OPTIONAL: use a CSV import to show bulk import

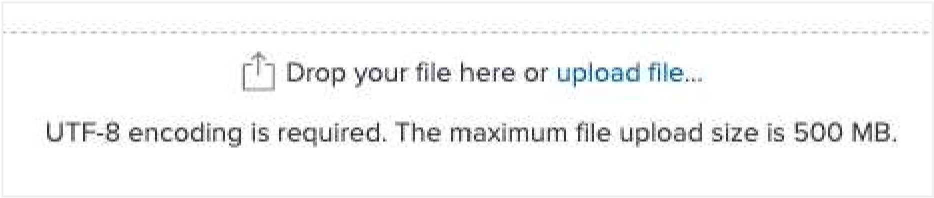
Create a text file on your own laptop and add the following text. Save as **ServiceTreeImport.csv**.

```
Service,Service Description,"Dependent Services,"
Retail Banking,,Products
Commercial Banking,,
Insurance,,"Service A, Service B, Service C"
Asset-Wealth Management,,
Lending,,
Payments,,
Capital Markets,,
Exchanges,,Trading Platform
Products,Sub-services of Retail Banking,"Transactional Accounts,Savings Accounts,Debit Cards,ATM Cards,Credit Cards,Travelers Cheques,Mortgages,Home Equity Loans,Personal Loans"
Transactional Accounts,,
Savings Accounts,,
Debit Cards,,
ATM Cards,,
Credit Cards,,
Travelers Cheques,,
Mortgages,,
Home Equity Loans,,
Personal Loans,,
Service A,Sub-services of Insurance,"Service a1, Service a2, Service a3"
Service B,,"Service b1, Service b2"
Service C,,"Service c1, Service c2, Service c3, Service c4"
```

Create a new service using the **Import from CSV** method

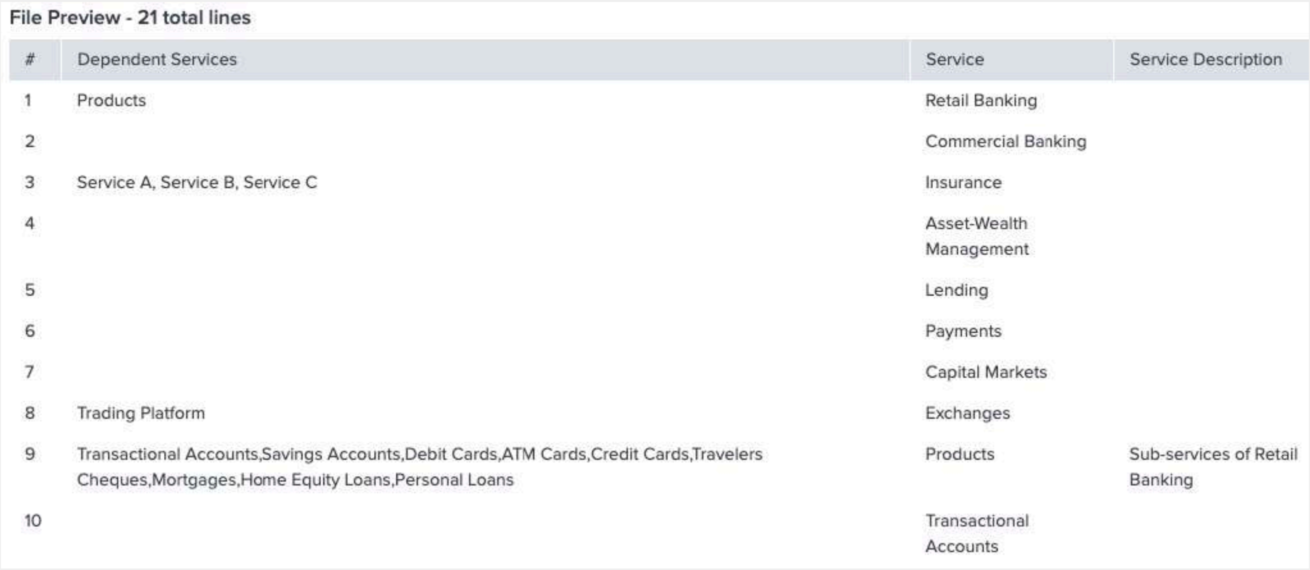


Upload your file


Drop your file here or upload file...

UTF-8 encoding is required. The maximum file upload size is 500 MB.

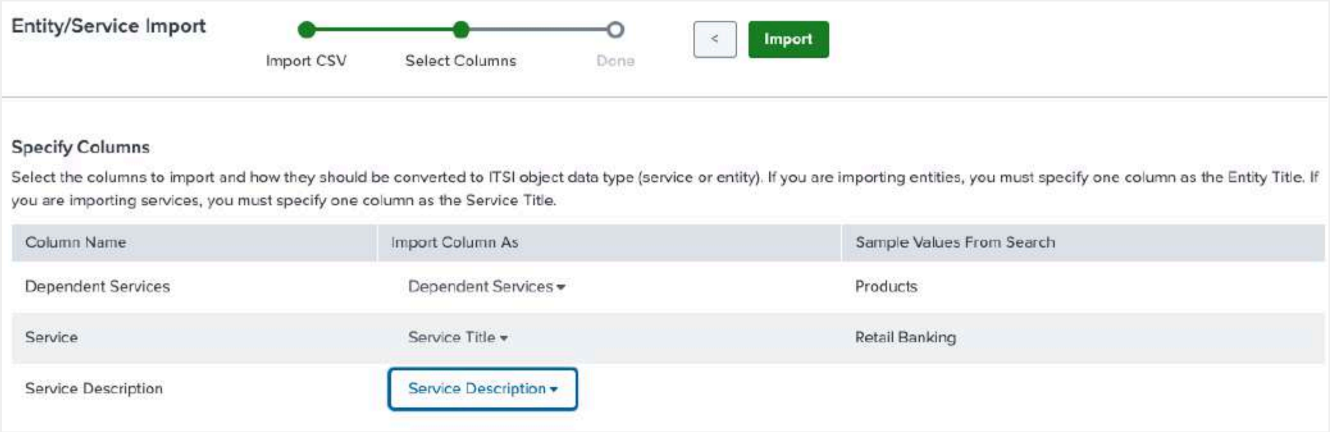
Check the preview looks ok



File Preview - 21 total lines

#	Dependent Services	Service	Service Description
1	Products	Retail Banking	
2		Commercial Banking	
3	Service A, Service B, Service C	Insurance	
4		Asset-Wealth Management	
5		Lending	
6		Payments	
7		Capital Markets	
8	Trading Platform	Exchanges	
9	Transactional Accounts,Savings Accounts,Debit Cards,ATM Cards,Credit Cards,Travelers Cheques,Mortgages,Home Equity Loans,Personal Loans	Products	Sub-services of Retail Banking
10		Transactional Accounts	

Set the appropriate **Import Column As** values



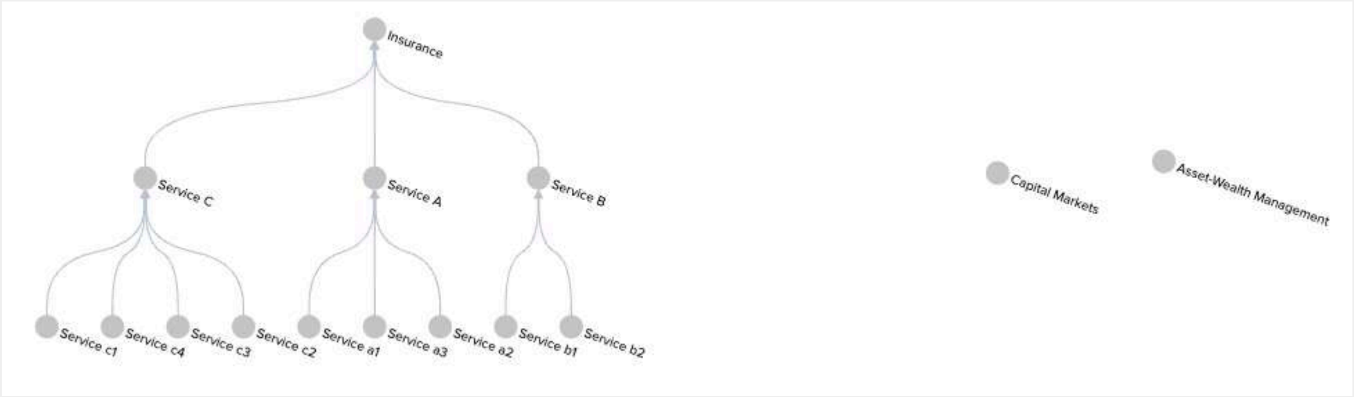
Specify Columns

Select the columns to import and how they should be converted to ITSI object data type (service or entity). If you are importing entities, you must specify one column as the Entity Title. If you are importing services, you must specify one column as the Service Title.

Column Name	Import Column As	Sample Values From Search
Dependent Services	Dependent Services ▾	Products
Service	Service Title ▾	Retail Banking
Service Description	Service Description ▾	

And click **Import** button

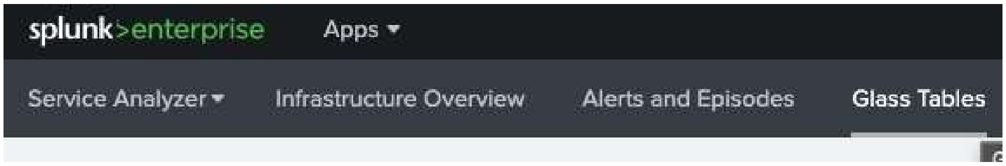
Check in your Service Analyzer that you have something similar to below. Everything will likely be grey as we have not added any KPIs or Service Health score yet.



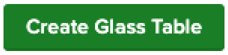
This is one example of how you can carry out a bulk-import Lab in IT Service Intelligence.

Build custom Glass Tables: CxO & Line of Business

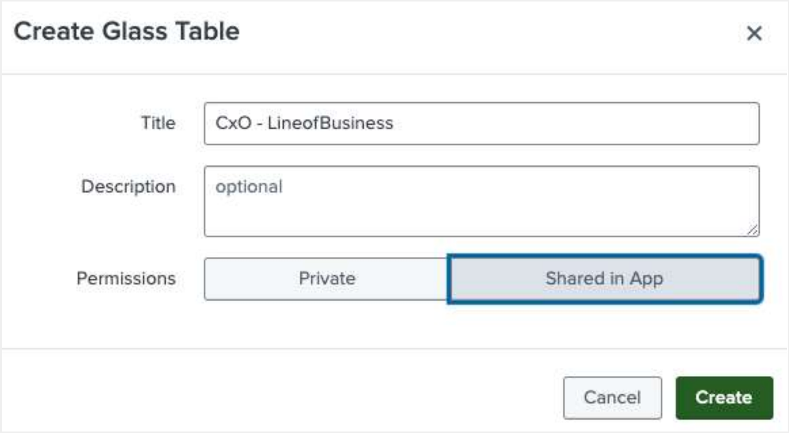
Navigate to the Glass Table UI via the main menu



Create a new Glass Table



We will target this GT at the business, so let's give a name that reflects the audience, such as "CxO - LineOfBusiness"



Create Glass Table

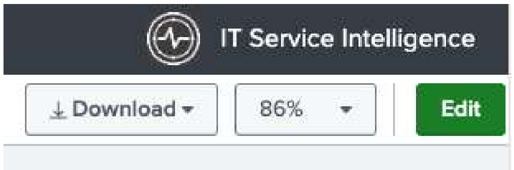
Title: CxO - LineofBusiness

Description: optional

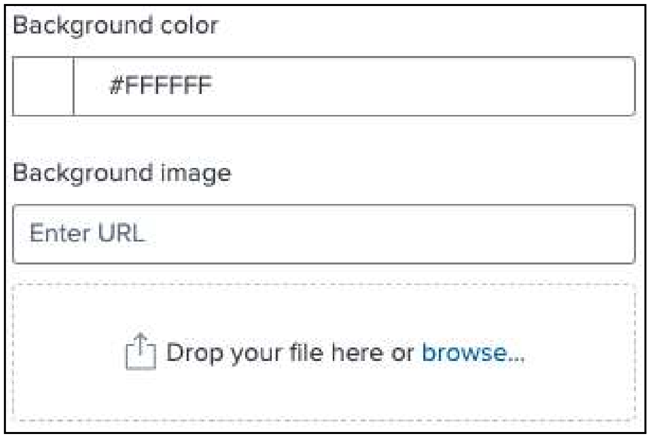
Permissions: Private | Shared in App

Click on the GT's title (hyperlink) to start editing it. You will see a blank canvas for now (as we have not created anything yet).

Select the **Edit** button to continue



[OPTIONAL] - Download a hi-res background from the Internet and save to your local device. E.g. https://unsplash.com/s/photos/technology-background


Background color

#FFFFFF

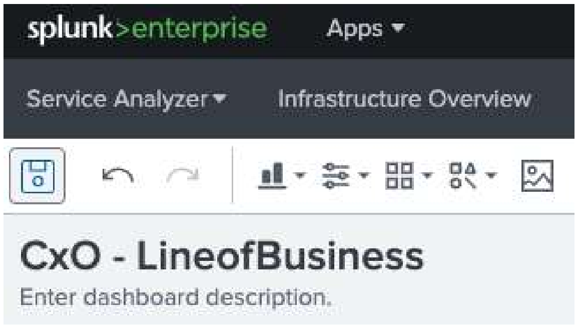
Background image

Enter URL

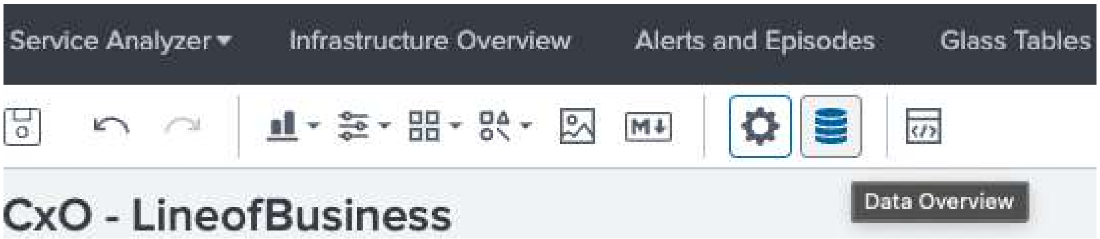
Drop your file here or browse...

Or if you prefer, you can enter a URL for an appropriate background image, or pick a background colour of your choice.

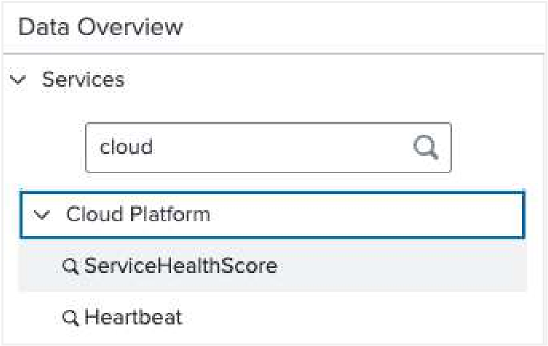
ℹ️**Note: changes are not saved unless you select the save icon** 💾 **in the Glass Table menu**



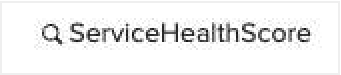
Add some Service Health scores to the dashboard using the **Data Overview** icon - this provides access to both health score and KPIs



Add ServiceHealthScore for Cloud services by filtering on “cloud” from the Services search bar,



and then selecting

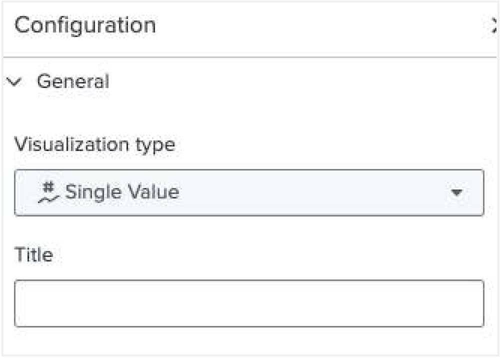


The newly added health score will now appear on the canvas. It can be moved, resized and configured.

Follow the same steps as above to also add the ServiceHealthScores from

- Compliance
- Fraud
- Observability Posture
- Add any score of your choice - this will represent “Sustainability” in the next step

For each of the service health scores, add a title.g. “Cloud Journey”, “Compliance”, “Fraud”, “Digital Experience”, “Sustainability” by selecting each health score and selecting entering a title in the Configuration options

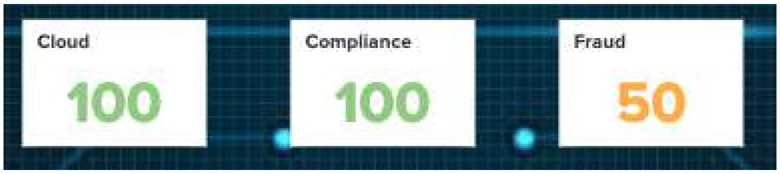


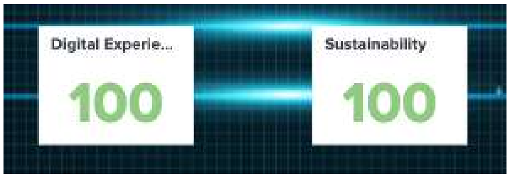
Visualization type

Single Value

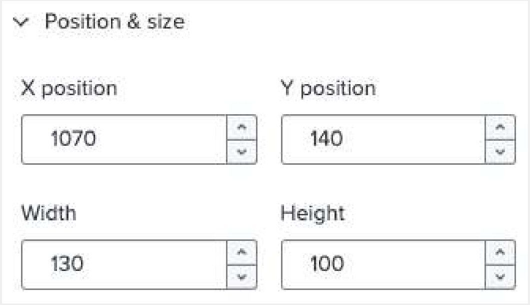
Title

So that you end up with the following:





Experiment with Width and Height options to ensure consistency



Position & size

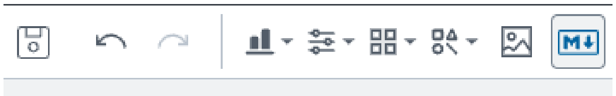
X position: 1070

Y position: 140

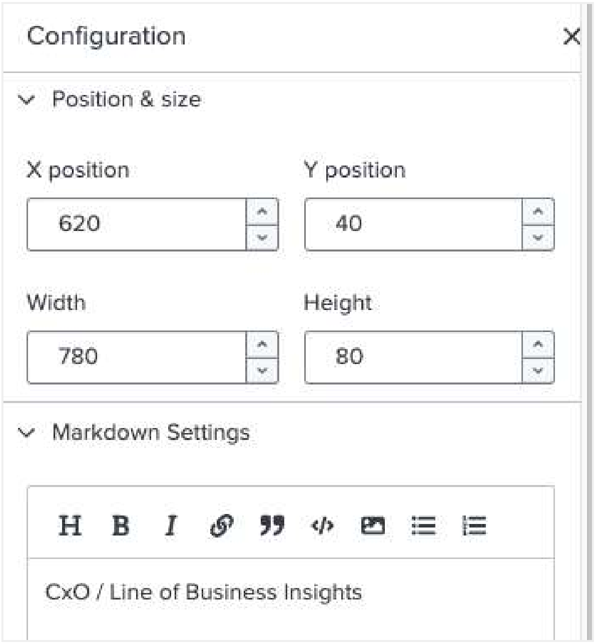
Width: 130

Height: 100

Add a title for the Glass Table by adding a markdown text component



Experiment with positioning, font colours, and size



Configuration

Position & size

X position: 620

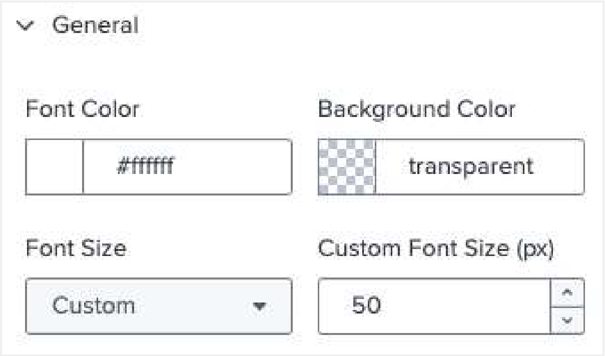
Y position: 40

Width: 780

Height: 80

Markdown Settings

CxO / Line of Business Insights



General

Font Color: #ffffff

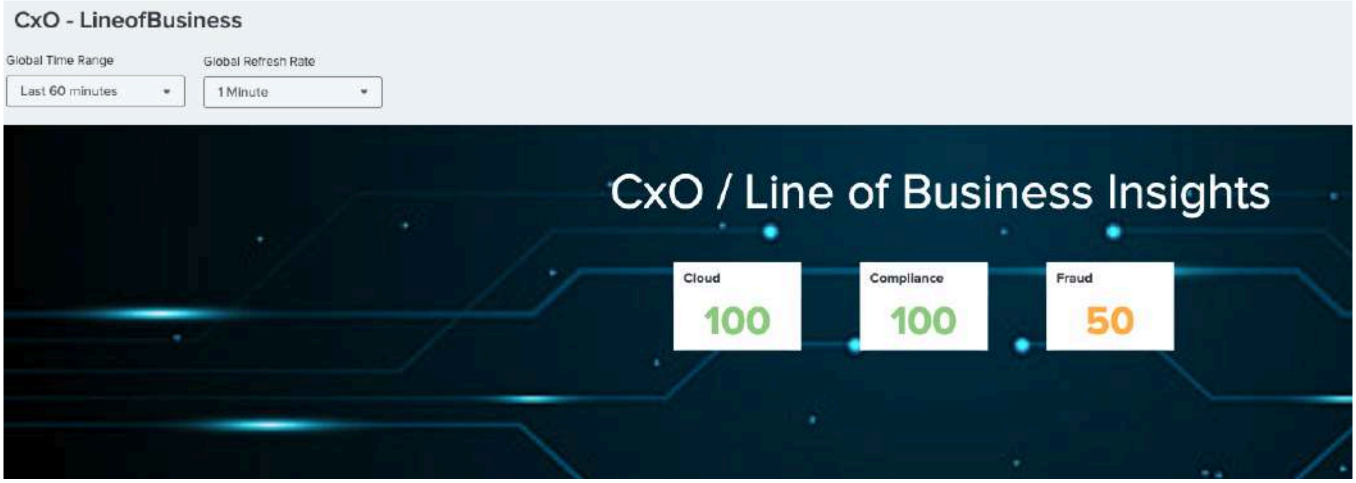
Background Color: transparent

Font Size: Custom

Custom Font Size (px): 50

Save your work and then **View** your work

View



CxO - LineofBusiness

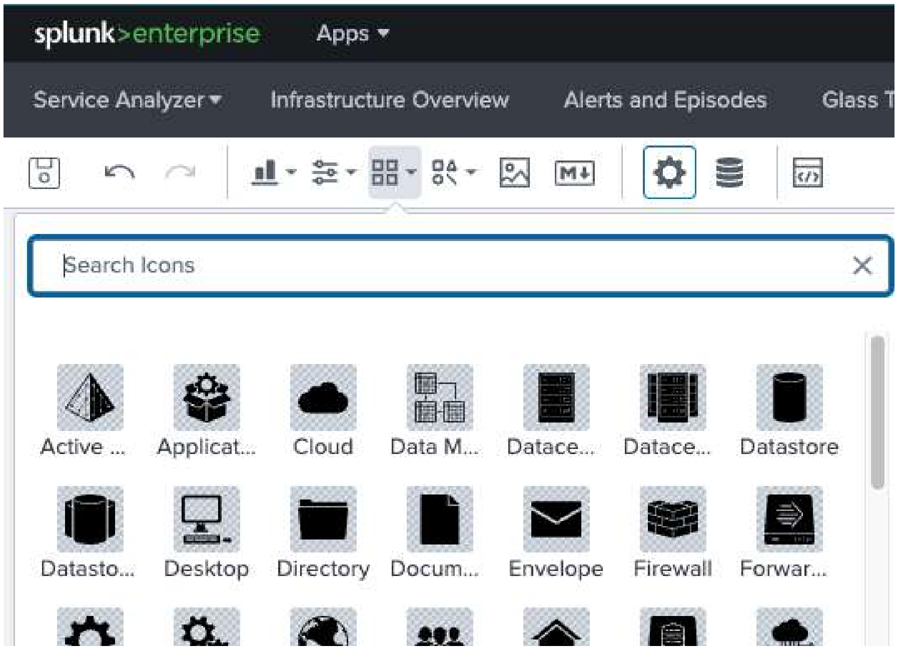
Global Time Range: Last 60 minutes

Global Refresh Rate: 1 Minute

Use this icon to view in Full Screen mode

Press “Escape” key to return and select **Edit** button to make more changes

Add some icons to the canvas, for each of the health scores, using the icons menu option

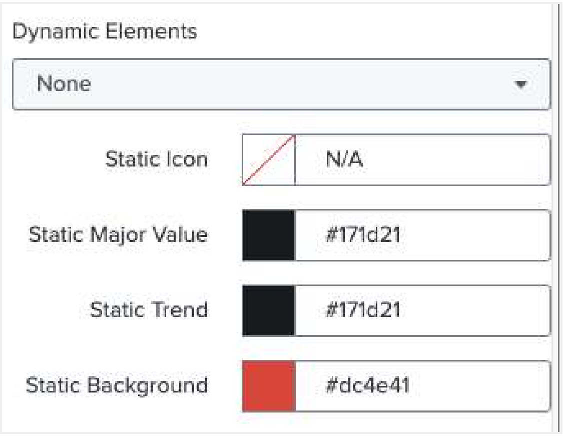


E.g.

- Cloud icon > Cloud Journey
- Group icon > Compliance
- Mag glass icon > Fraud
- iPhone icon > Digital Experience
- Globe icon > Sustainability

You might find some of your icons are of the same colour as your background. Select an icon and experiment with the colour settings

E.g. static background

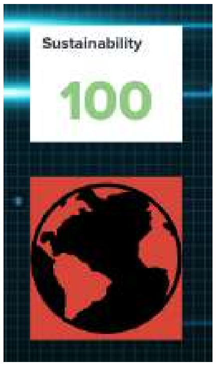


Dynamic Elements

None ▾

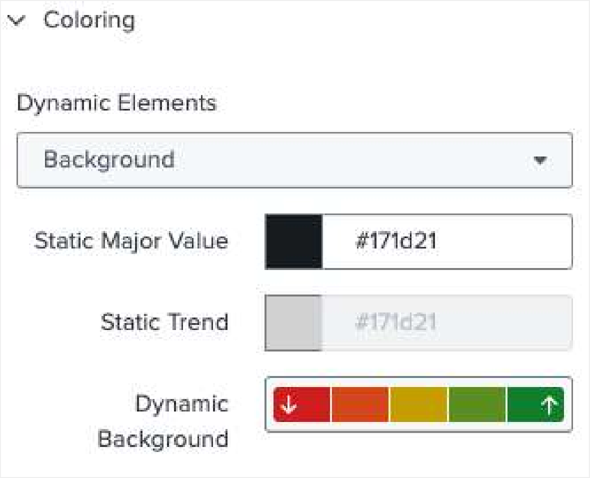
Static Icon	N/A
Static Major Value	■ #171d21
Static Trend	■ #171d21
Static Background	🟥 #dc4e41

=



It might be preferred to have the colours of the Service Health Scores update automatically (red/amber/green), depending on the score values.

For each score, set the Dynamic Element as “Background”



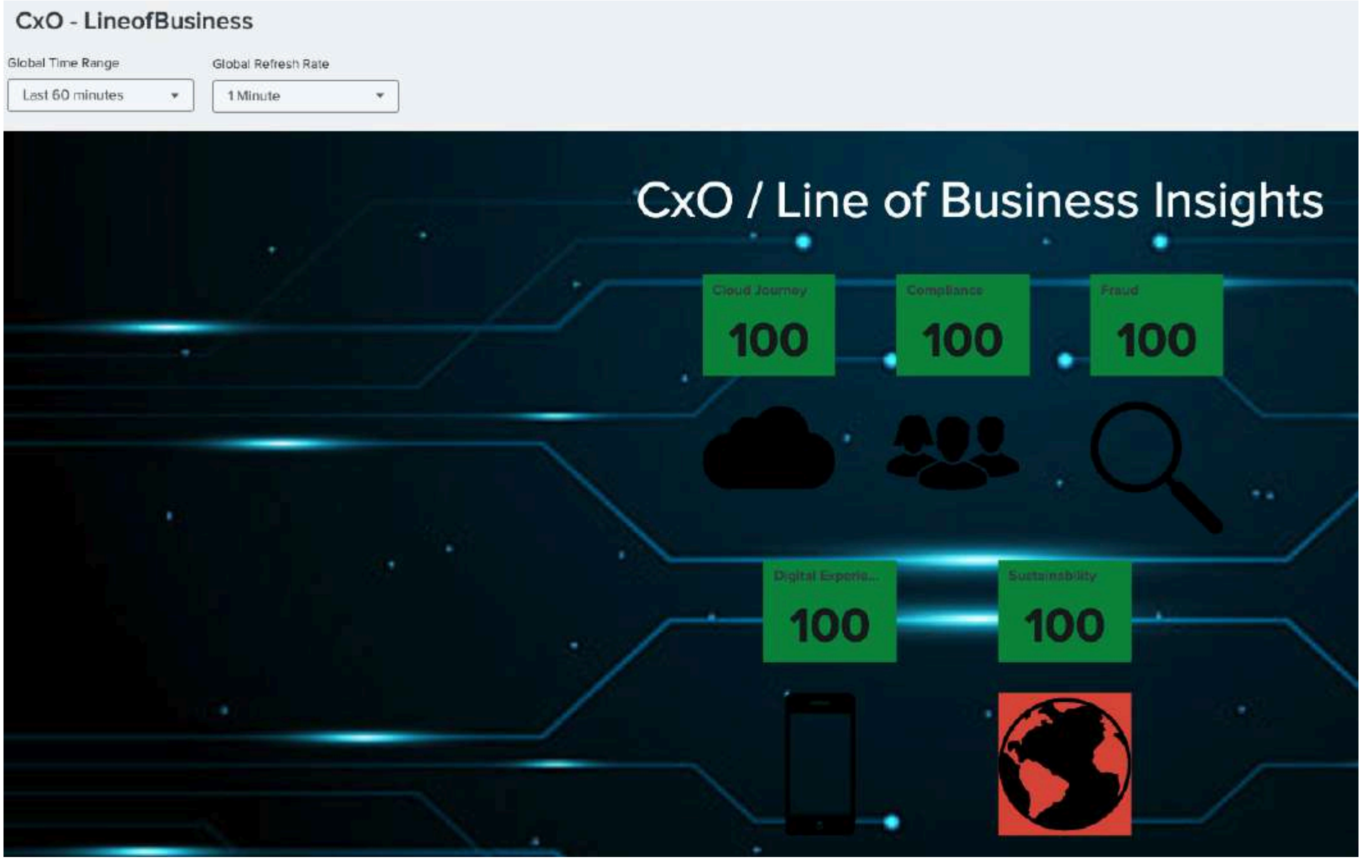
Coloring

Dynamic Elements

Background ▾

Static Major Value	■ #171d21
Static Trend	#171d21
Dynamic Background	↓ 🟥 🟧 🟨 🟩 🟩 ↑

Save and **view** your work



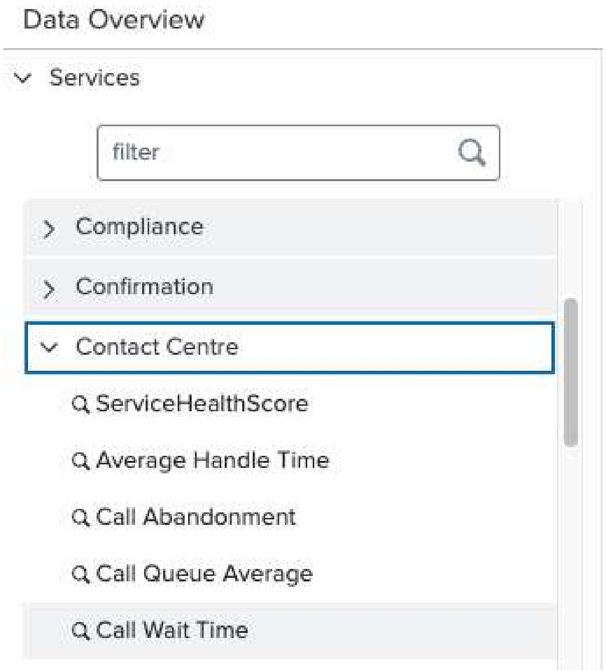
CxO - LineofBusiness

Global Time Range: Last 60 minutes

Global Refresh Rate: 1 Minute

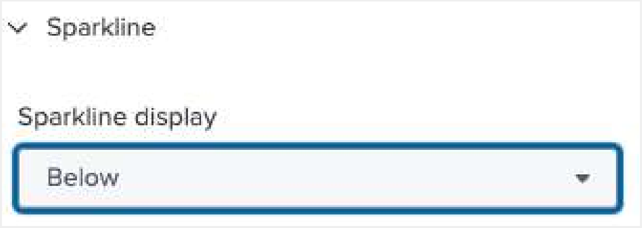
For completeness, we’ll add a KPI to the view also.

We will add “Call Wait Time” from the Contact Centre service



Give the new component a title “Call Wait Time”

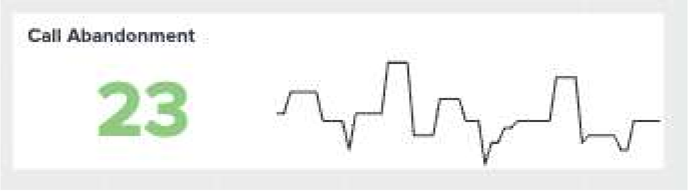
As this is a KPI, we’d also like to see a sparkline of recent values, which you can add from the **Configuration** settings



Sparkline display

Below

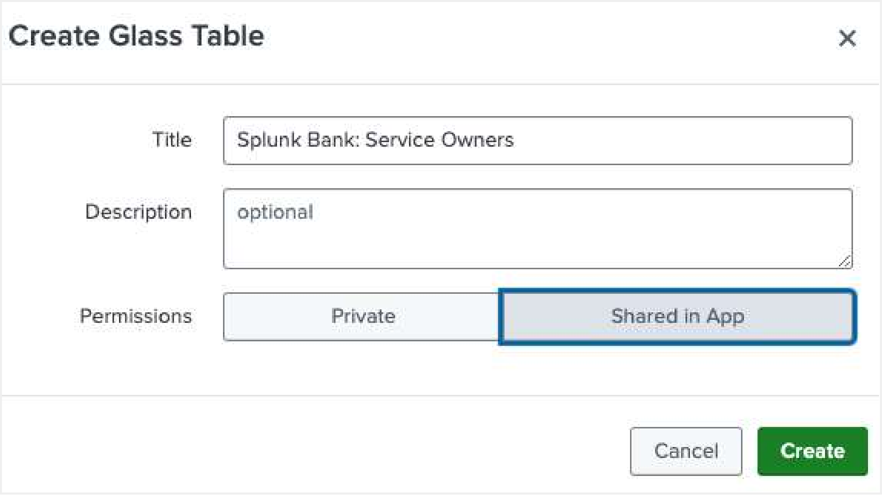
Your sparkline should be visible either before, below or after the KPI value



Finish by saving your work.

Build custom Glass Tables: Infrastructure Overview

Create a new Glass Table “my Org: Service Owners”



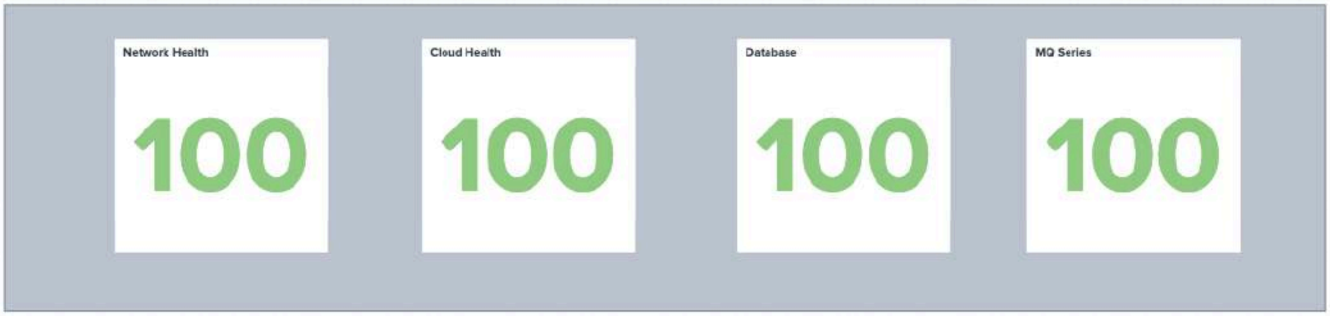
Create Glass Table

Title: Splunk Bank: Service Owners

Description: optional

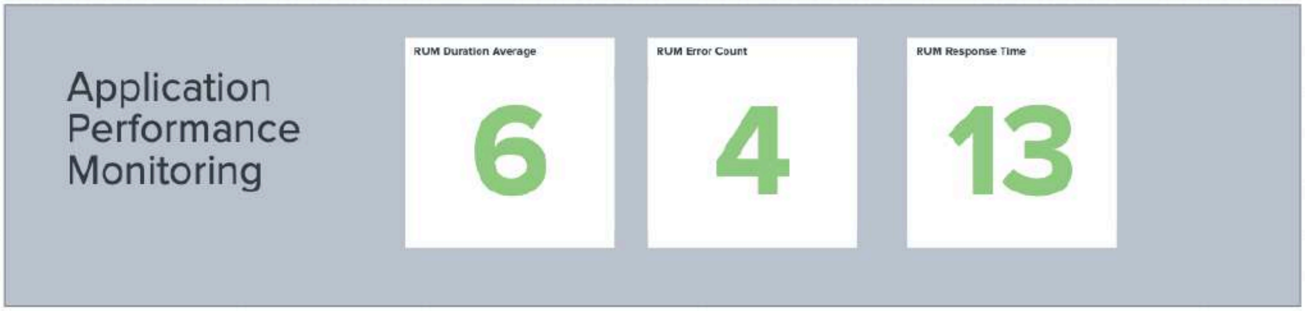
Permissions: Private | Shared in App

Add health scores for: Networks, Cloud, Database, MQ Series



Network Health	Cloud Health	Database	MQ Series
100	100	100	100

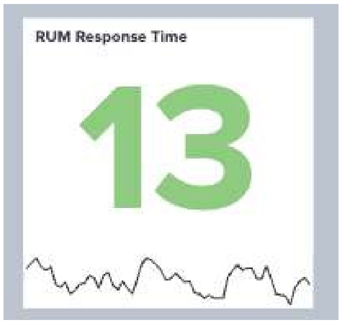
Add some KPIs by finding the RUM service and adding: APM Duration, Error Count, Response Time



Application Performance Monitoring

RUM Duration Average	RUM Error Count	RUM Response Time
6	4	13

Add a Sparkline example to one KPI

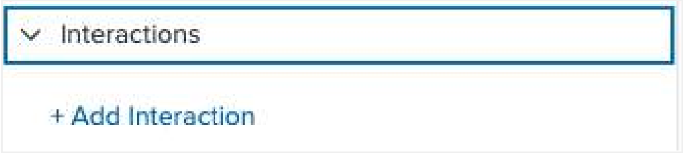


Save your work.

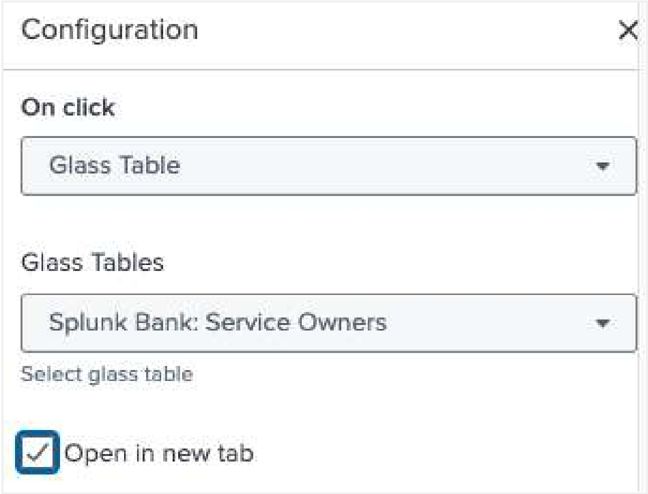
Connecting Glass Tables

Return to the first Glass Table “CxO - LineofBusiness”

Select any component e.g. Digital Experience and edit the Interactions settings



Connect this Glass Table to the one we just finished creating


Configuration

On click

Glass Table

Glass Tables

Splunk Bank: Service Owners

Select glass table

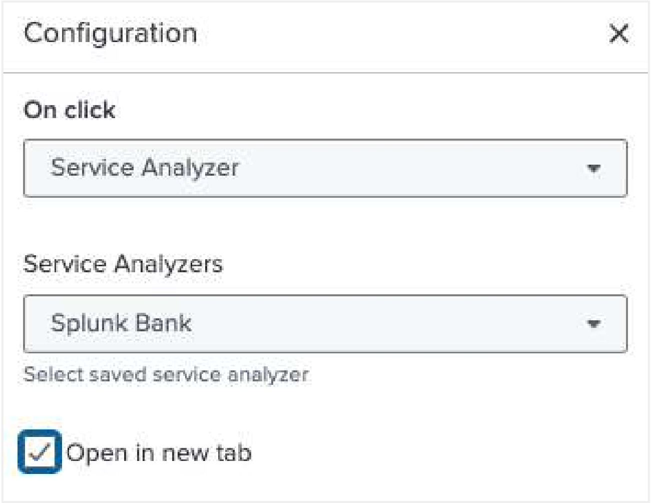
☑ Open in new tab

Ensure you click the **apply** button

Save and **View** and confirm the drill-down works.

Now edit the **Service Owner** glass table and pick a component to edit.

Add a new interaction but this time connect it to a **Service Analyzer** - you may find you need to create your own custom Service Analyzer to complete this step.



Configuration

On click

Service Analyzer

Service Analyzers

Splunk Bank

Select saved service analyzer

☑ Open in new tab

Lab 11 - Build Your Own Service

Description

Now that you have learned some of the key features within ITSI, try and build a service view that aligns to your role, team or department.

Start by picking a key service - something that Line of Business cares about, and has a relatively complex IT stack supporting it.

Focus on something that provides maximum business value. Then identify 4 or 5 key technology components that underpin that service.

Finally, for each technical component, how would you determine if it was performing well or not? I.e. what are they KPIs you'd be interested in?

See how far you can get in building that out in the remaining lab time - and ask for help!

Good luck.

Answers: Lab 9

Glass Tables

Q1: Service Health - which of the 4 services has the lowest/worst health score?

A: Confirmation / 24

Q2: KPIs - how many Fraud alerts have occurred in the last hour?

A:45

Q3: What's the main reason that Confirmation has a low score?

A: 101 Failures

Q4: What technical components are involved in this degradation?

A: Arcot 3DS + CCM

Service Analyzer

Q5: There are actually a number of services impacting Card Payments - name 2 of them. HINT: focus on the root cause.

A: Fraud, Sentiment, CCM.

Q6: How many are there and what are their severities?

A:4. Severities will change over time - it's a live view

Deep Dive

Q7: Which KPIs look particularly problematic?

A: Response Rate (but there may be others)

Q8: How many events have there been in the last 2 hours?

A: Depends on demo data and time range selected

Q9: How many are there now?

A: less than there were in the previous view!

Service Creation

Q10: Are your new KPIs appearing and do they have values?

A: Yes, you should have some values (after 5 mins at most)

Q11: What else do you notice about the service tree?

A: The new services are not connected to any other service