

Introduction to Dashboards

Before Taking This Course

- To be successful, students must have a working understanding of these courses:
 - Intro to Splunk
 - Using Fields
 - Search Optimization

Course Objectives

- Describe the dashboard framework
- Identify the dashboard definition
- Name the dashboard workflows
- Compare absolute and grid layouts
- Create event annotations
- Use mock data
- Describe troubleshooting steps
- Use base and chain searches
- Identify methods to improve performance

Course Outline

- Creating a Prototype
- Selecting a Data Source
- Improving Performance

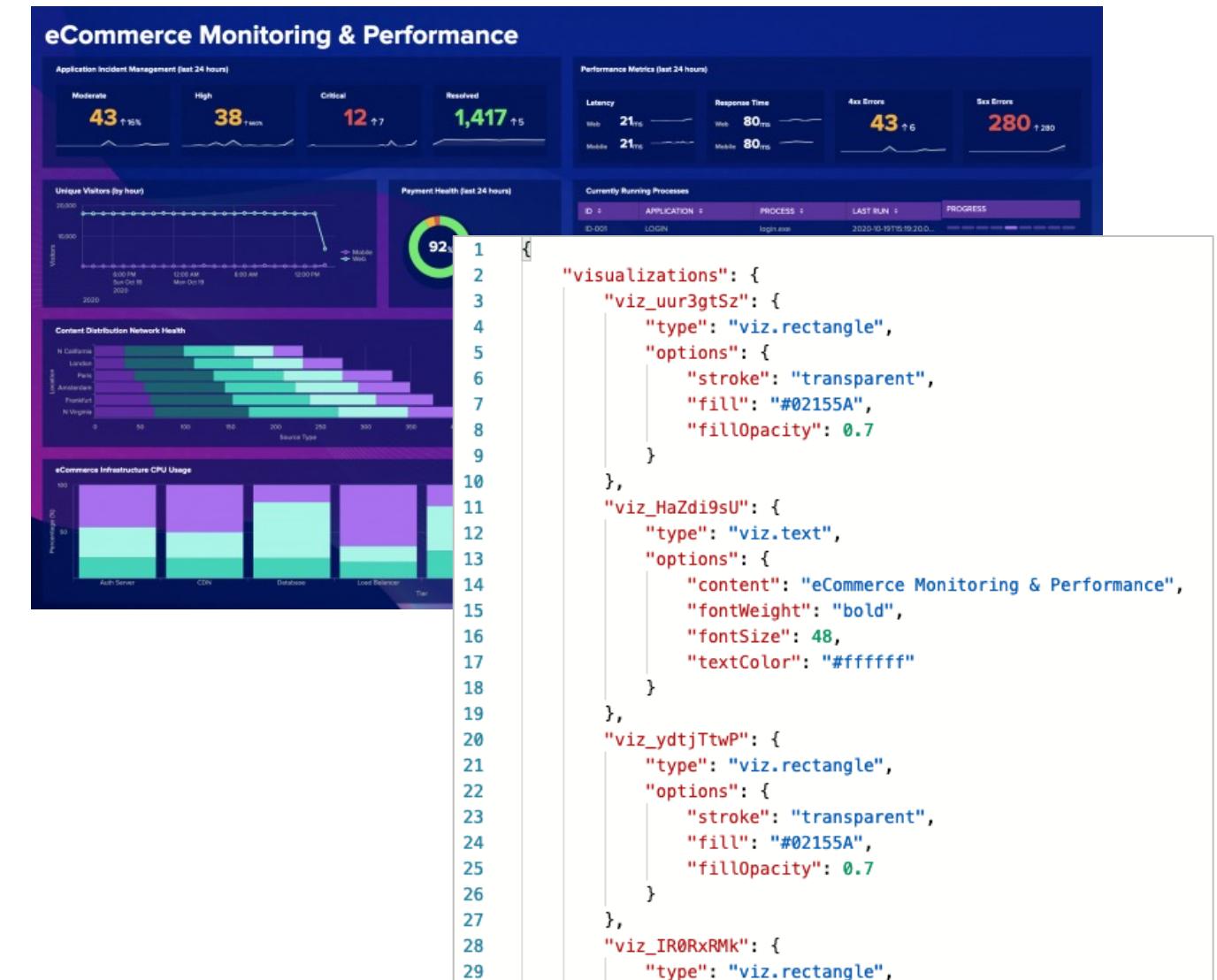
Topic 1: Create a Prototype

Topic Objectives

- Describe the dashboard framework
- Identify the dashboard definition
- Name the dashboard workflows
- Compare grid and absolute layout
- Describe troubleshooting options

Splunk Dashboard Framework

- Classic Dashboard
 - Source code: simple XML
 - Layout: row and column
- Dashboard Studio
 - Source code: JSON
 - Layouts: absolute and grid
 - Layering visualizations
 - More visualizations: images, icons, shapes, and text boxes



Dashboard Definition

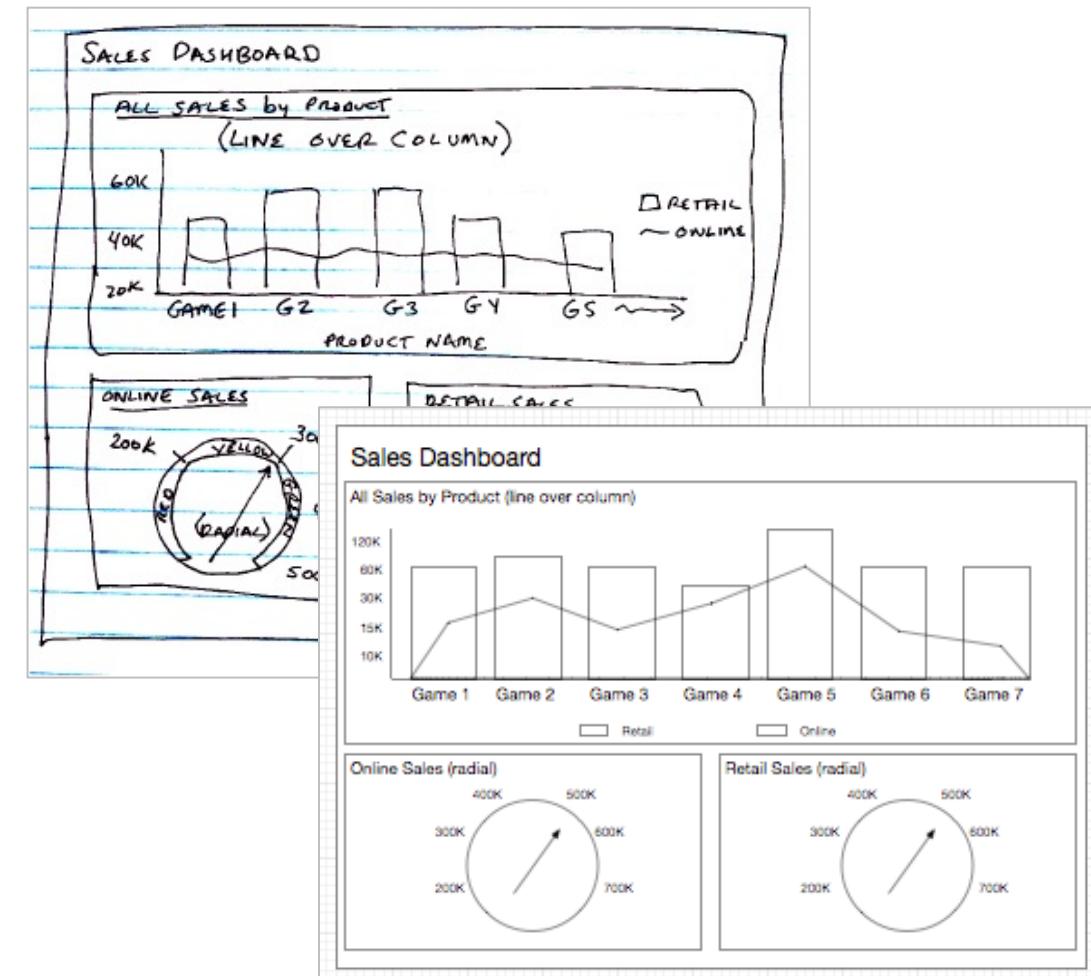
- JSON that renders the dashboard in the visual editor
- Includes five sections:
 - **visualizations**: unique ID, type, data source and their options for each
 - **dataSources**: unique ID type, query, and options for each search
 - **defaults**: global defaults
 - **inputs**: unique ID, input stanzas
 - **layout**: list of inputs, canvas size
- Every object in the dashboard definition is in the format of a JSON-formatted stanza

```
Web Sales
1 {  
2 > "visualizations": {--  
14 > },  
15 > "dataSources": {--  
30 > },  
31 > "defaults": {--  
47 > },  
48 > "inputs": {--  
57 > },  
58 > "layout": {--  
76 > },  
77 > "description": "",  
78 > "title": "Web Sales"  
79 }
```

Plan

- Who is the audience?
- What is your data story?
- Identify stakeholders
- Use wireframing
- Create a prototype

Wireframes:
hand drawn or digital drawings



Creating a Dashboard

Save a search to a new dashboard

New Search

```
index=cafegames sourcetype=access_combined_cg
| fields action, host, price, product_name, status
| search status=200 action IN (addtocart, purchase)
| chart count AS number BY product_name action useother=f
| eval abandoned = addtocart - purchase
```

576 events (8/6/23 3:00:00.000 PM to 8/7/23 3:22:21.000 PM) No Event Sampling Job

Events Patterns Statistics (11) Visualization

20 Per Page Format Preview

product_name	addtocart	purchase	abandoned
Benign Space Debris	20	40	-20
Blade Hopper	5	16	-11
Dragon Race	13	20	-7
Dream Crusher	24	31	-7
Final Sequel	9	7	2
Marshmallow Missiles	26	35	-9
Orvil the Wolverine	30	30	0
Puppies vs. Zombies	30	36	-6
Running With Scissors	38	49	-11
SIM Cubicle	8	12	-4
Zombie Chase	37	60	-23

Save Panel to New Dashboard

Dashboard Title Required [Edit ID](#)

Description Optional

Permissions

How do you want to build your dashboard? [What's this?](#)

Classic Dashboards
The traditional Splunk dashboard builder

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

Select layout mode

Absolute Full layout control

Grid Quick organization

Panel Title Optional

Visualization Type Statistics Table

> Advanced Panel Settings

Creating a Dashboard (cont.)

Click **Create a New Dashboard** on the Dashboards page

1 Click the **Dashboards** tab in the top navigation bar.

2 Click the **Create New Dashboard** button.

3 Enter a title for your dashboard in the **Dashboard Title** field.

4 Select **Dashboard Studio** as the builder type.

5 Choose the **Absolute** layout mode.

6 Click the **Create** button to create the dashboard.

Absolute Layout

The screenshot shows the Splunk Absolute Layout interface. At the top is a toolbar with various icons for charts, user inputs, icons, shapes, images, and markup. Below the toolbar is a header bar with tabs for 'Absolute Layout' and 'Enter dashboard description'. A 'Global Time Range' dropdown is set to 'Last 24 hours'. The main area is a 'Canvas' where panels can be placed anywhere, featuring a grid overlay. A callout box labeled 'Canvas' points to this area. Another callout box labeled 'Gridlines' points to a circular icon representing the grid. To the right is a 'Configuration' panel with sections for 'Display mode', 'Background', and 'Preferences'. A callout box labeled 'Settings, Data Sources, Source Code' points to the top of the configuration panel. Callout boxes for 'Display Mode', 'Background', and 'Background color' point to their respective sections in the configuration panel.

Charts, User Inputs, Icons, Shapes, Images, and Markup

Settings, Data Sources, Source Code

Canvas
Place panels anywhere

Gridlines
Assist panel placement

Display Mode

Auto: display the best zoom level for your dashboard's visibility (default)

Actual size: set custom width and height

Fit to width: automatically scales dashboard to the browser's window size

Background

Background color: set background color by selecting a color square or entering a hexadecimal code

Background image: upload or reference a custom image

Grid Layout

The screenshot shows the Splunk Dashboard Editor interface. At the top, there are two main sections: "Charts, User Inputs, Markup, Rectangle" and "Settings, Data Sources, Source Code". Below these are various dashboard controls: back/forward arrows, chart, search, and refresh icons; a gear icon for settings; and a save button. The main area is titled "Grid Layout" and contains a "Global Time Range" set to "Last 24 hours". On the right side, there's a "Configuration" panel with sections for "Preferences" (which includes a toggle for "Show title & description" and a slider for "Gutter size" set to 8) and "View Options" (which includes toggles for "Show Edit Button", "Show Open In Search Button", and "Show Export Button"). Two callout boxes highlight specific features: one for the "Canvas" section (listing panel placement in rows, snap-to row alignment, and only row height changeable) and one for "Display Mode" (describing fit-to-width scaling).

Charts, User Inputs, Markup, Rectangle

Settings, Data Sources, Source Code

Grid Layout

Enter dashboard description.

Global Time Range

Last 24 hours

Canvas

- Panel placement in rows
- Snap-to row alignment
- Only row height can be changed

Display Mode

Fit to width: automatically scales dashboard to the browser's window size

Light ▾

View

Save

Configuration

Preferences

Show title & description

Gutter size

8

View Options

Show Edit Button

Show Open In Search Button

Show Export Button

Layouts Compared

- Absolute layout: all features including pixel-perfect control
- Grid layout: when you need quick and simple
 - chart visualizations, user inputs, markup, and rectangles

Option	Absolute	Grid
Charts	✓	✓
Customizable Background Color	✓	–
Customizable Canvas size	✓	Customize row height and visualization widths only
Unlimited visualizations on a dashboard	✓	Number per row depends on the width of the visualizations –which can be modified
Shapes: rectangles, lines, and ellipses	✓	rectangles
Icons: built-in and custom	✓	–
Images	Up to 16MB	–

Dashboard Studio – Visual Editor

Absolute Layout Only

Undo / Redo

Add User Input

Add Shape

Add Markup

Config

Source Editor

Gridlines

100%

Light

View

Save

Add Chart

Add Icon

Add Shape

Add Image

Add Rectangle

Data Overview

Purchases & Lost Sales

Product Name	Purchases	Lost Sales
Benign Space Debris	~5K	~1K
Blade Hopper	~4K	~1K
Dragon Race	~3K	~1K
Dream Crusher	~5K	~1K
Final Sequel	~1K	~1K
Marshmallow Missiles	~6K	~1K
Orvil the Wolverine	~4K	~1K
Puppies vs. Zombies	~5K	~1K
Running With Scissors	~6K	~1K
SIM Cubicle	~1K	~1K
Zombie Chase	~7K	~1K

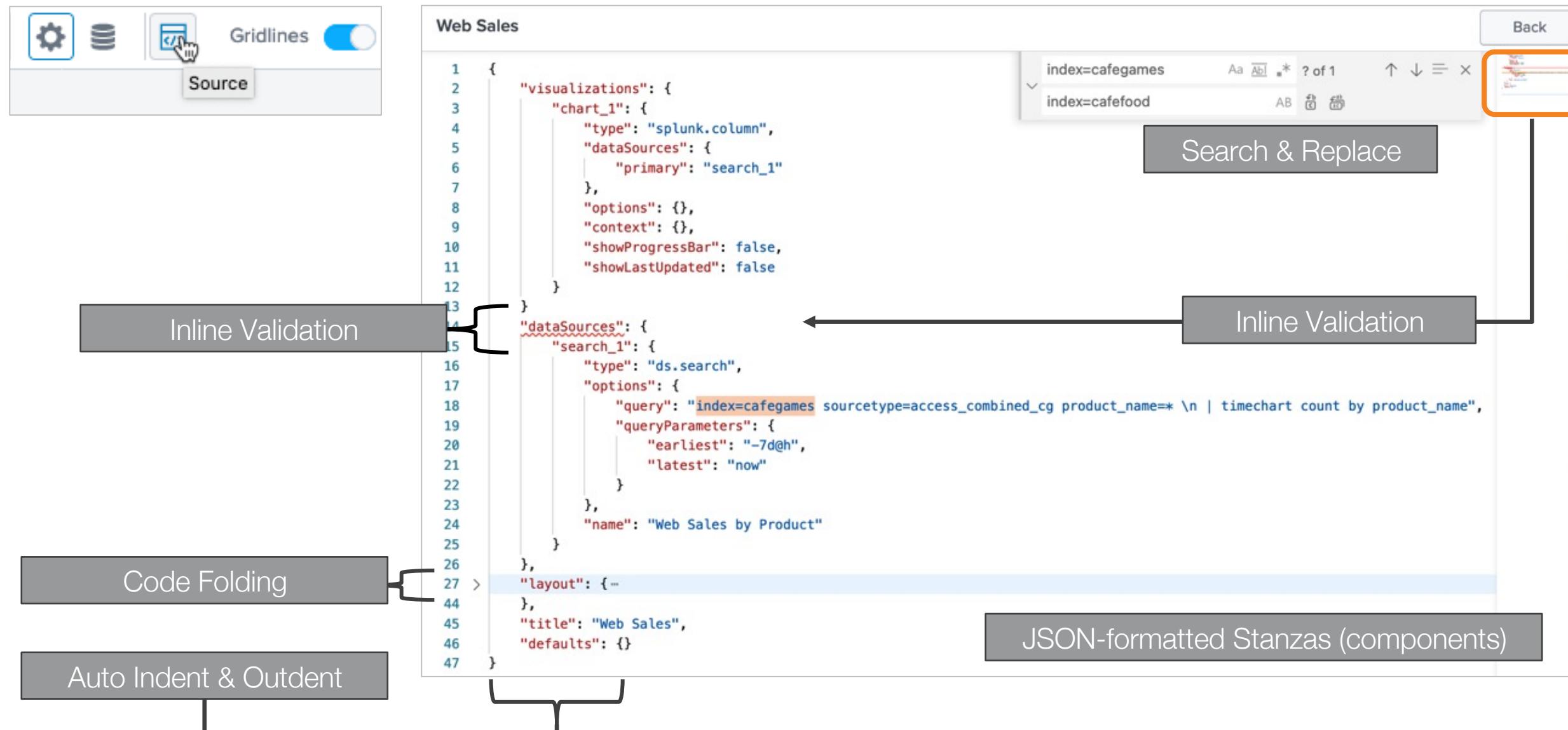
Top Server Errors

host	404	406	503
web1	1226	315	223
web2	1284	286	240
web3	1305	273	246

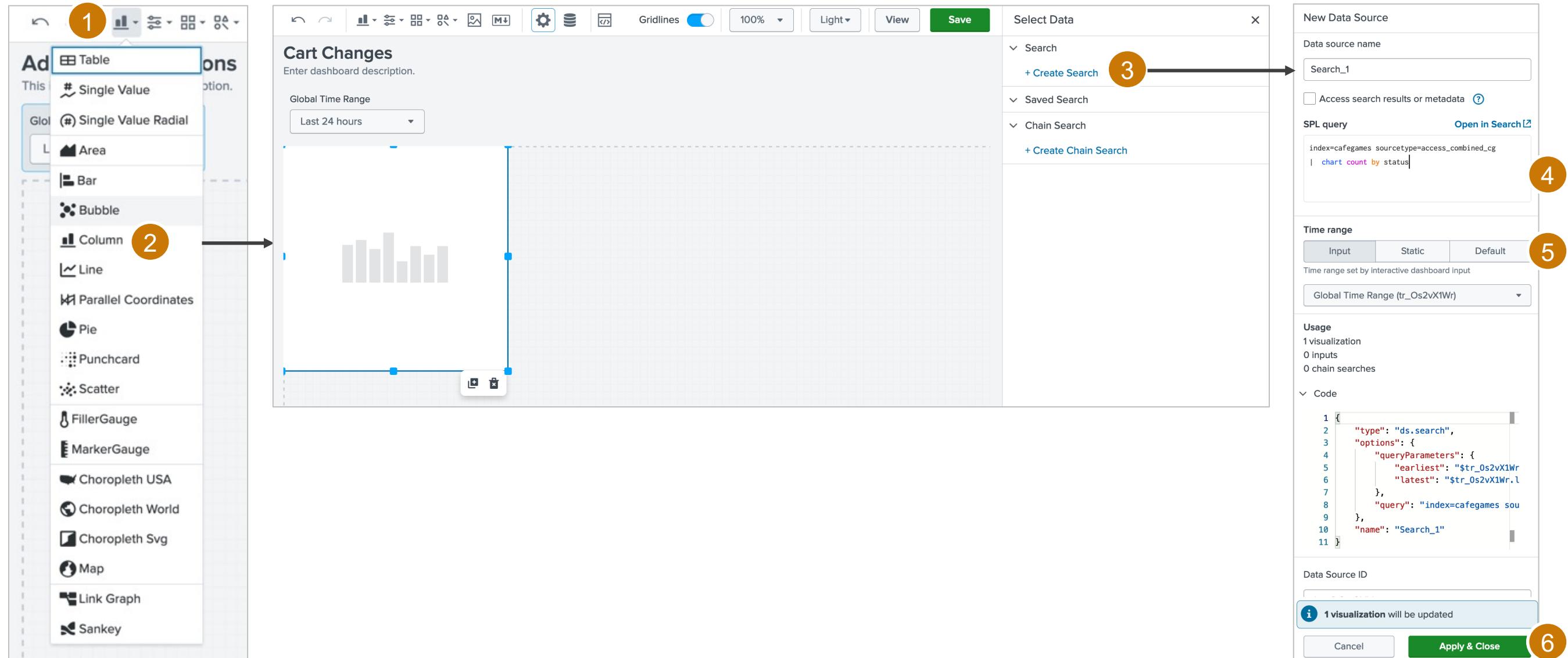
All Errors by Host

time	web1	web2	web3
Mon Jul 31	~0.4K	~0.4K	~0.4K
Tue Aug 1	~0.9K	~0.9K	~0.9K
Wed Aug 2	~0.5K	~0.5K	~0.5K
Thu Aug 3	~0.4K	~0.4K	~0.4K
Fri Aug 4	~0.4K	~0.4K	~0.4K
Sat Aug 5	~0.4K	~0.4K	~0.4K
Sun Aug 6	~0.4K	~0.4K	~0.4K
Mon Aug 7	~0.4K	~0.4K	~0.4K

Dashboard Studio – Source Editor



Adding Visualizations



Visualization Action Panel

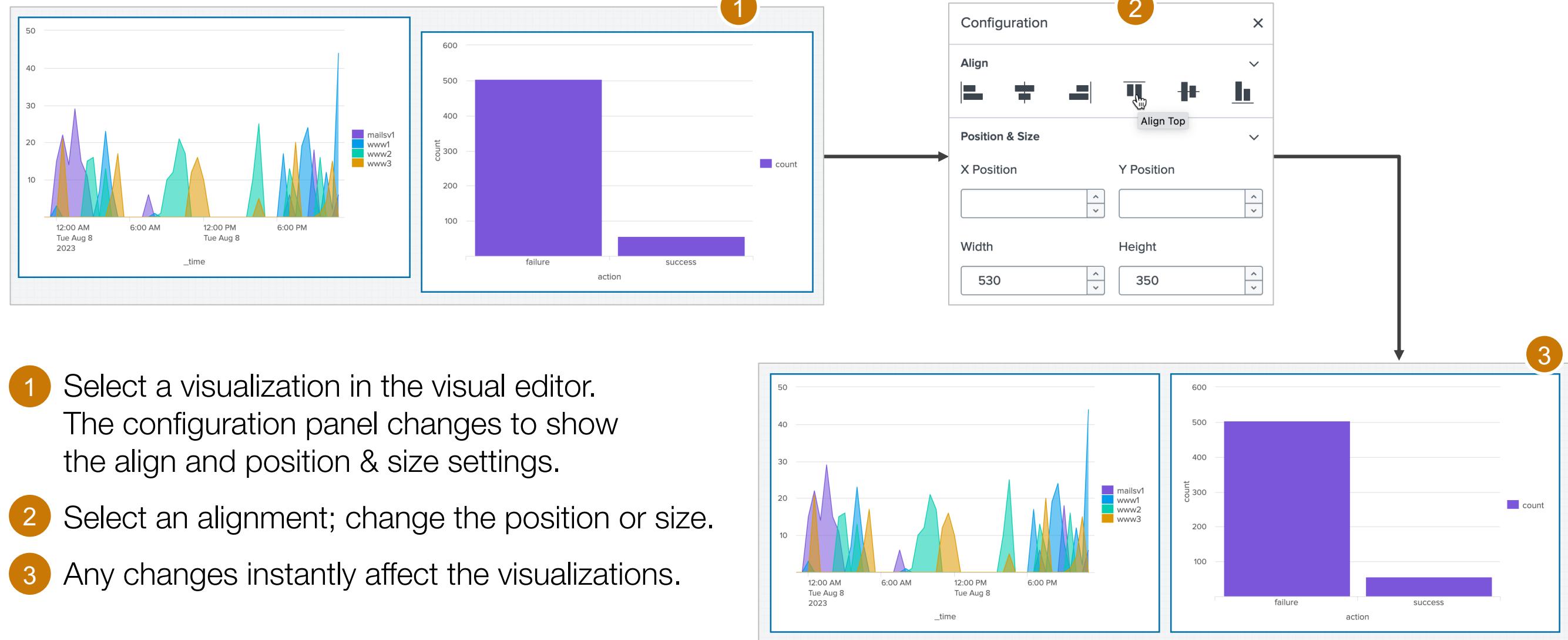
Edit Mode

Layer the visualization
Clone the visualization
Delete the visualization

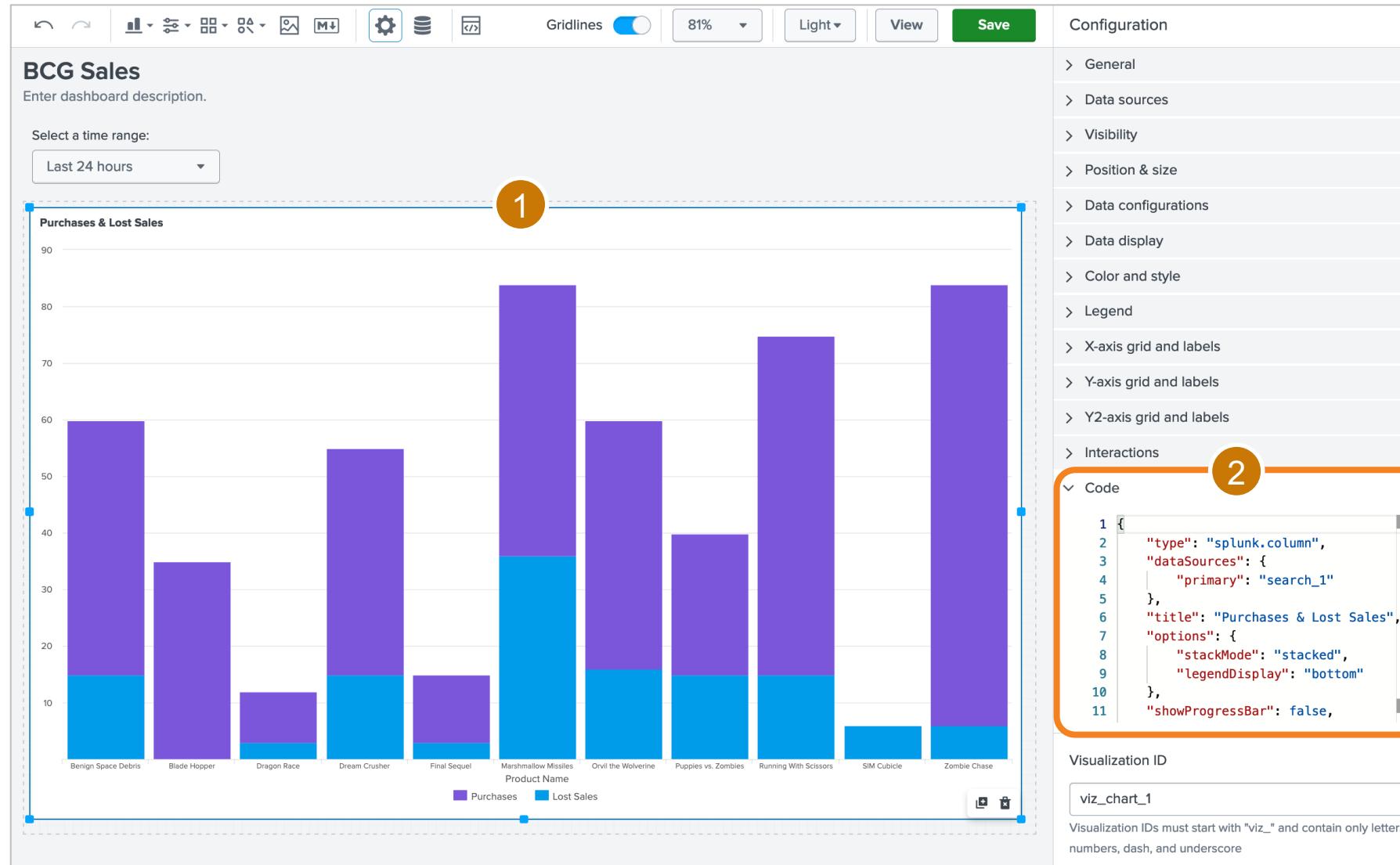
View Mode

Open in search
Inspect the search
Expand the visualization to full screen mode
Refresh the search driving the visualization
Download the visualization (PNG format)

Aligning Visualizations



Visual Editor's Code Window



1 Select a visualization or data source in the visual editor

2 Open the Code window in the configuration panel

Any changes instantly affect the visualization or data source selected

Troubleshooting

- Look for typos in source code and search queries
- Run a search manually
- Verify tokens are being set and have the expected values
- Use the Job Inspector
 - Check the impact of knowledge object processing
 - Look at debug messages in the Search Job Inspector
 - Debug messages appear after the search has completed

The screenshot shows the Splunk Jobs interface. At the top, there are navigation links: Settings, Activity, Help, and a dropdown for Jobs (which is selected) and Triggered Alerts. Below this is a search bar and a filter dropdown set to '10 Per Page'. The main area displays a table of jobs with columns: i, Owner, Application, Events, Size, Created at, Expires, Runtime, Status, and Actions. There are five entries listed:

- index=cafegames sourcetype=access_combined_cg | timechart count by product_name useother=f [before 8/8/23 5:17:35.000 PM]
- index=cafegames sourcetype=access_combined_cg | fields action, host, price, product_name, status | search status=200 action IN (ad)
- index=cafegames sourcetype=access_combined_cg | fields action, host, price, product_name, status [8/1/23 12:00:00.000 AM to 8/8/23 5:15:35.000 PM]
- index=cafegames sourcetype=access_combined_cg | timechart count by product_name useother=f [8/1/23 12:00:00.000 AM to 8/8/23 5:15:11.000 PM]

In the Actions column of the first entry, a context menu is open, with the 'Extend Job Expiration' option highlighted with an orange box. A large orange arrow points from this menu down to the 'Search job inspector' window below.

The screenshot shows the 'Search job inspector' interface. At the top, it says 'Search job inspector'. Below that, it states: 'This search has completed and has returned **9** results by scanning **13,580** events in **1.05** seconds (SID: 1691540255.39) [search.log](#) [Job Details Dashboard](#)'. There are two sections with expandable arrows:

- > Execution costs
- > Search job properties

At the bottom, it shows 'Server info: Splunk 9.1.0.2, localhost:8000, Tue Aug 08 17:22:11 2023 User: poweruser'.

Managing Views

- Scoped to your app context
- Set Sharing permissions
- Open, Clone, Move, Delete

poweruser ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾

KNOWLEDGE

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

User interface
Create and edit views, dashboards, and navigation menus.

Type	Actions
Time ranges	+ Add new
Views	+ Add new
View PDF scheduling	
Navigation menus	
Prebuilt panels	+ Add new
Bulletin messages	+ Add new

Views
User interface » Views
Showing 1-10 of 28 items

View name	Owner	App	Sharing	Status	Actions
alert	No owner	search	Global Permissions	Enabled	Open Clone
alerts	No owner	search	Global Permissions	Enabled	Open Clone
charting	No owner	search	Global Permissions	Enabled	Open Clone
dashboard_live	No owner	search	App Permissions	Enabled	Open Clone
dashboards	No owner	search	Global Permissions	Enabled	Open Clone
data_model_editor	No owner	search	Global Permissions	Enabled	Open Clone
data_model_explorer	No owner	search	Global Permissions	Enabled	Open Clone
data_model_manager	No owner	search	Global Permissions	Enabled	Open Clone
data_models	No owner	search	Global Permissions	Enabled	Open Clone
dataset	No owner	search	Global Permissions	Enabled	Open Clone

Lab 1 – Create a Prototype

Time: 20 minutes

Tasks:

- Create a dashboard
- Use the makeresults command
- Add a single value
- Add a chart
- Clone a visualization
- Add a table



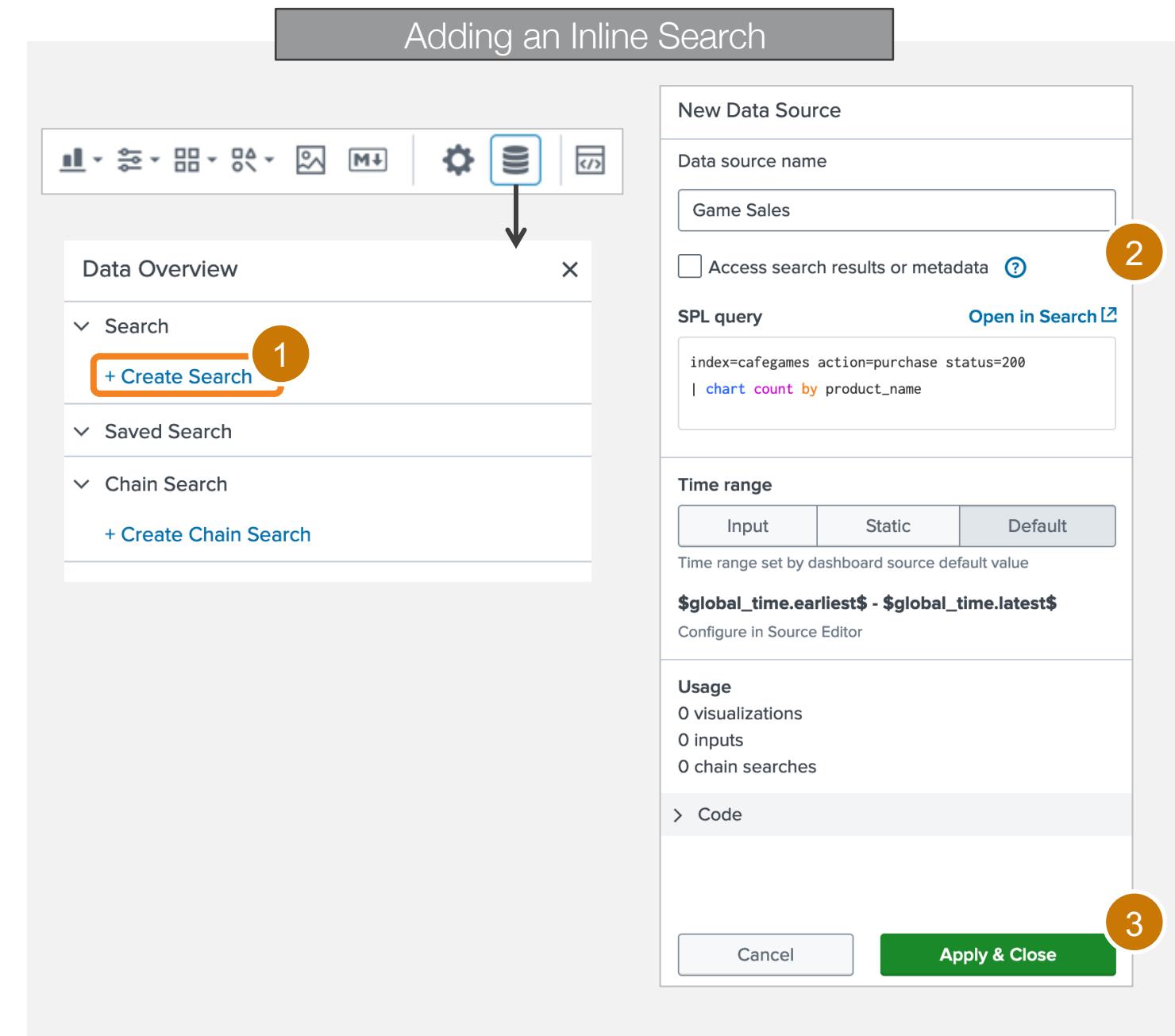
Topic 2: Selecting a Data Source

Topic Objectives

- Define the `dataSources` stanza fields
- Explain how mock data can be used
- Create event annotations

Data Sources

- Primary
 - Inline search
 - Saved search (report)
 - Chain search
 - Mock data (requires source editor)
- Secondary
 - Annotation
- Time Range
 - Input: Use time input range input
 - Static: Set time range in search
 - Default: Use the time range from the dashboard source setting
- Once added, available to other visualizations on that dashboard
- Not deleted with a visualization



Data Sources – Source Code

1 Data Source Stanza

- Adding a search to a visualization in the visual editor creates a unique stanza for it in the `dataSources` section

2 Unique ID

- Referenced twice:
 - `dataSources` section
 - `visualization` stanza
- Customizable

```
{
  "visualizations": {
    "viz_chart_1": {
      "type": "splunk.column",
      "dataSources": {
        "primary": "ds_search_1"
      },
      "options": {
        "chart.stackMode": "stacked",
        "legend.mode": "standard",
        "legend.placement": "bottom"
      },
      "title": "Game Sales"
    }
  },
  "dataSources": {
    "ds_search_1": {
      "type": "ds.search",
      "options": {
        "query": "index=cafegames sourcetype=access_combined_cg",
        "queryParameters": {
          "earliest": "-7d@d",
          "latest": "now"
        }
      },
      "name": "Game Sales by Product"
    }
  }
}
```

3 Type

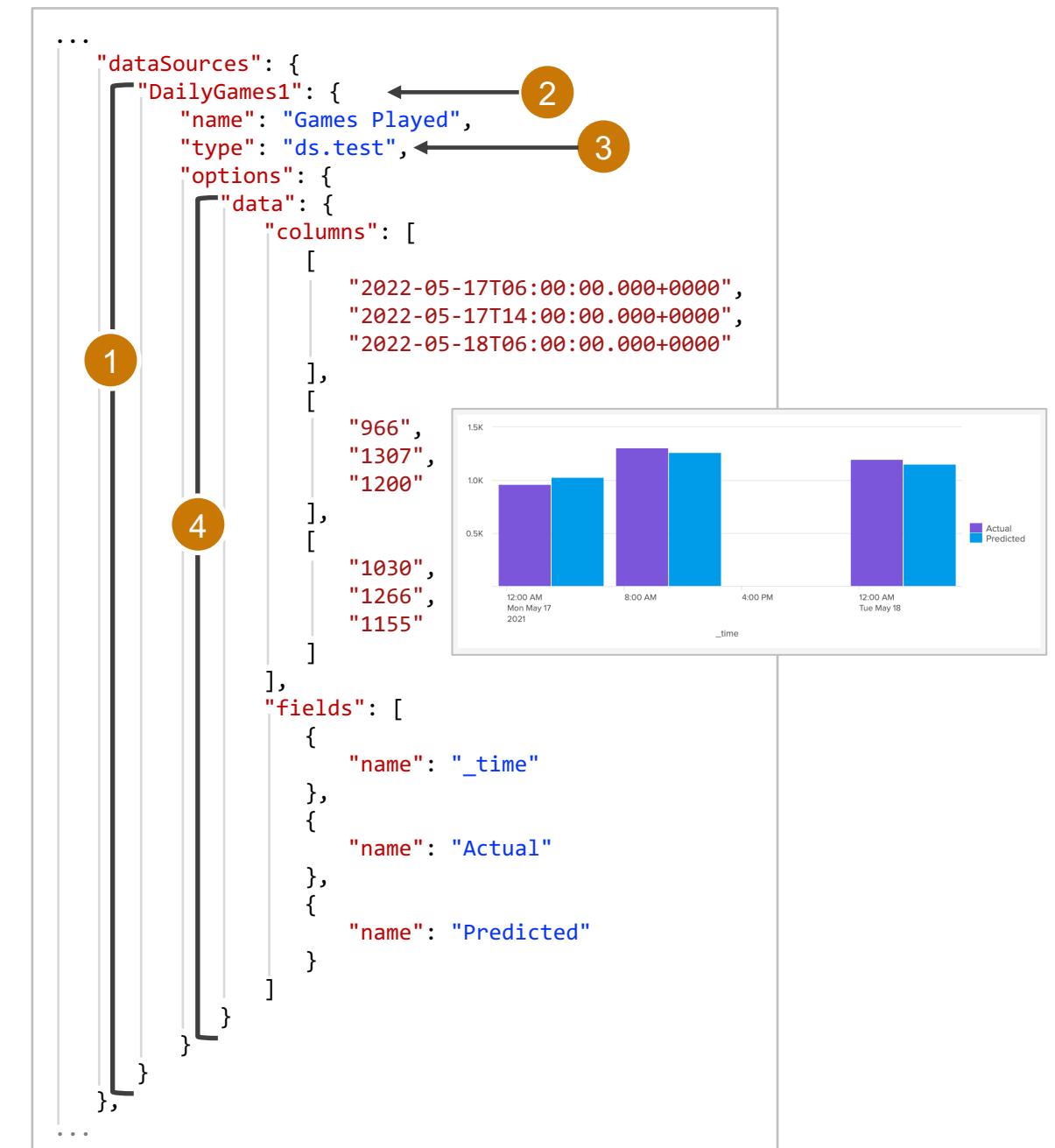
- Requires the prefix: `ds.`
- Four types:
 - Inline search: `ds.search`
 - Saved search: `ds.savedSearch`
 - Chain search: `ds.chain`
 - Mock data: `ds.test`

4 Time Range

- A time range picker is added to every dashboard by default
 - All data source time ranges are controlled by the default global time range picker, except `ds.savedSearch` and `ds.test`
 - Can be overridden
 - For example:
- ```
"earliest": "-7d@d",
"latest": "now",
```

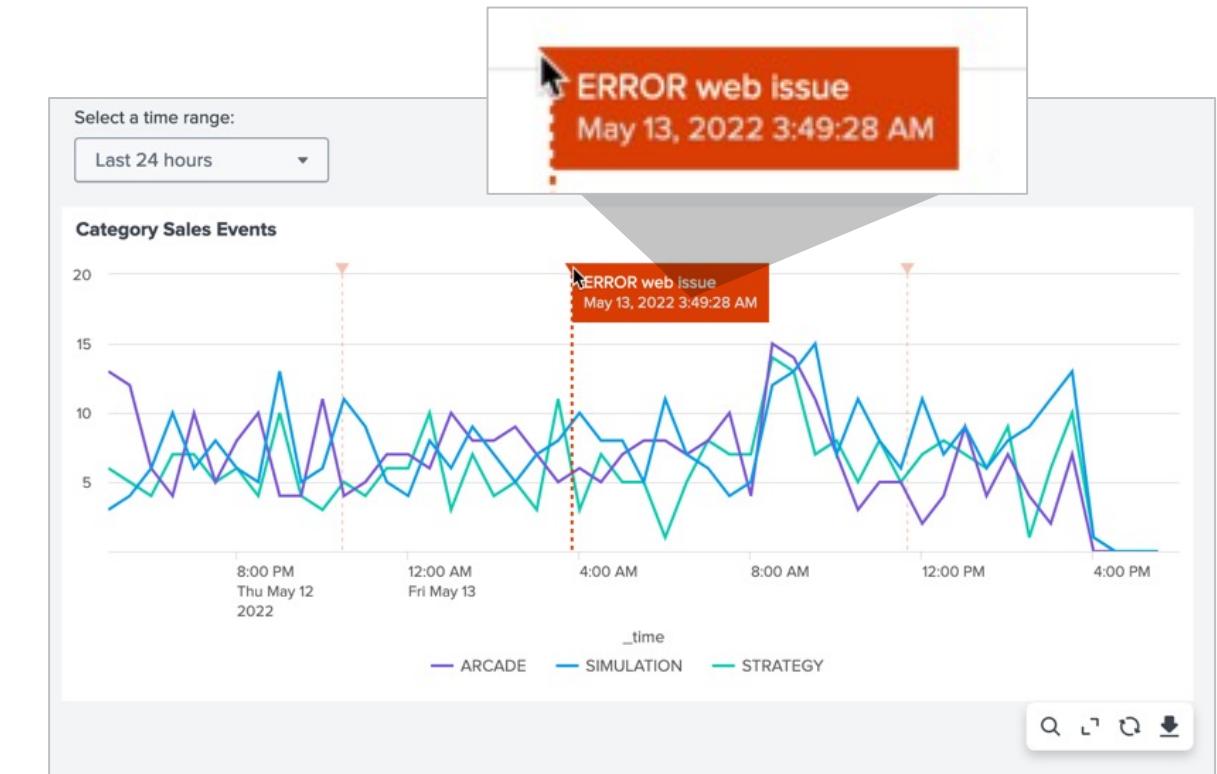
# Mock Data – ds.test

- Sample Data
- Uses type: **ds.test**
- Create in the source editor
  - 1 Data source stanza
  - 2 Unique ID
  - 3 Data source type: **ds.test**
  - 4 Columns and Fields
    - Under options in a data stanza
    - **columns**: comma-delimited values in brackets
    - **fields**: key / value pairs in curly braces



# Event Annotations

- Secondary Data Source
  - Visualizations can have both a primary and secondary, annotation data source
  - Displays as a callout
  - Can assign a color for all callouts or a unique color for each category value
  - Automatically filters for events matching the chart's time range
  - Available for line, column, area charts
  - PDF export is not available



# Event Annotations – Add a Flag

The screenshot shows a Splunk dashboard titled "Web Store Server". The main view displays a timechart titled "Web Server Status Events" for the last 7 days. The chart has multiple series represented by colored bars. Below the chart, a legend lists ten event types: Benign Space Debris, Orville the Wolverine, Blade Hopper Puppies vs. Zombies, Dragon Race Running With Scissors, Dream Crusher, Final Sequel, Marshmallow Missiles, Benign Space Debris, Blade Hopper Puppies vs. Zombies, Dragon Race Running With Scissors, Dream Crusher, Final Sequel, and Marshmallow Missiles. A blue dashed box encloses the chart area. To the right, three configuration windows are shown in sequence:

- Step 1:** Shows the "Data sources" section with "Cafe Sales" selected. An orange circle labeled "1" is over the "Cafe Sales" entry.
- Step 2:** Shows the "Annotations" section where "annotations" is added under "Data sources". An orange circle labeled "2" is over the "Select a field from data source" dropdown.
- Step 3:** Shows the final configuration with "annotations" listed under "Data sources" and "message (string)" selected for "Annotation labels".

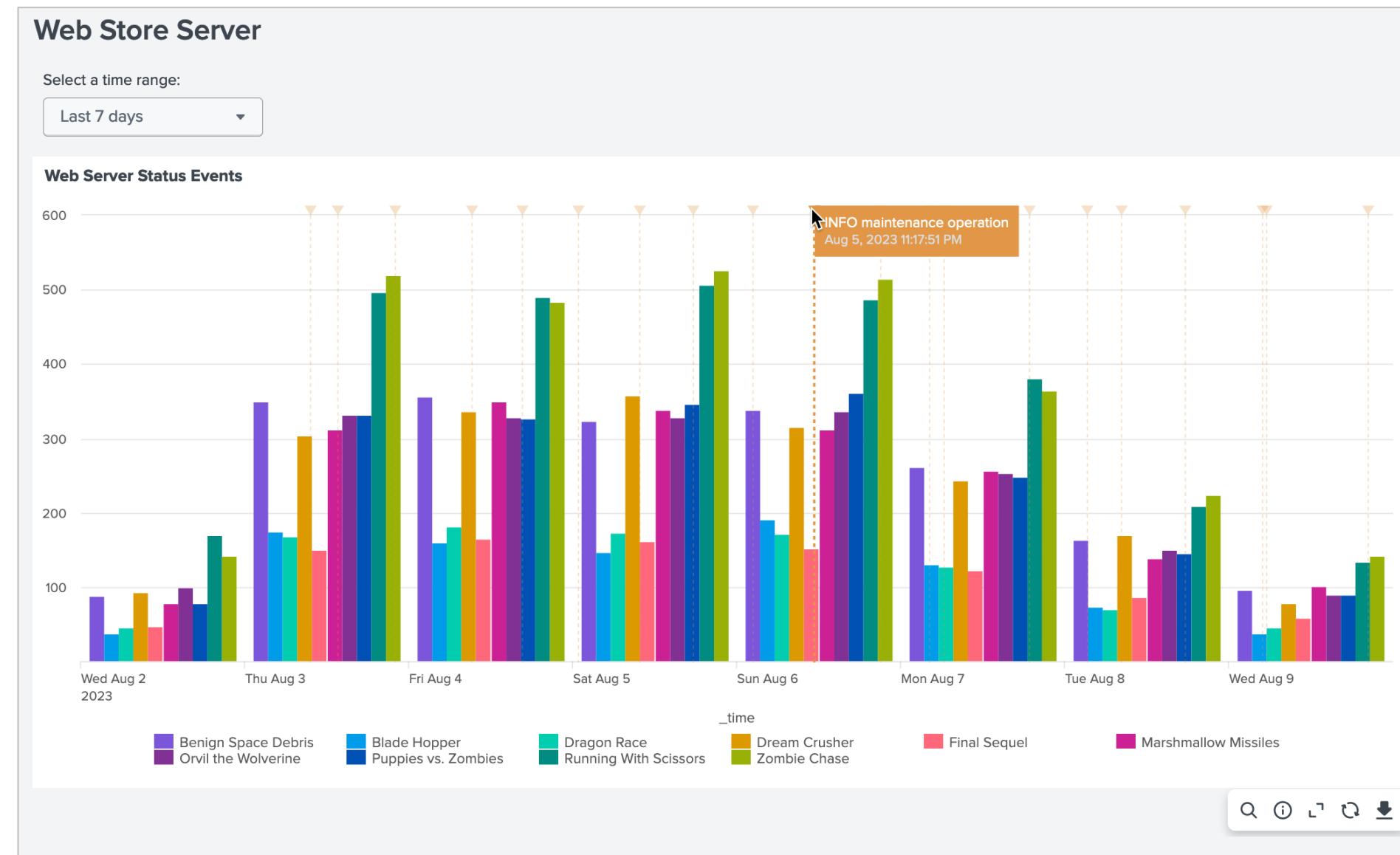
Primary Search: Cafe Sales

```
index=cafegames sourcetype=access_combined_cg
| timechart count by product_name useother=f
```

Secondary Search: annotations

```
index=webapp sourcetype=access_combined
| fields message
```

# Event Annotations – Add a Flag (cont.)



# Event Annotations – Add a Flag Color

- Use `eval` in the annotation search to create a field identifying color HEX codes
  - Allows different flag colors without editing the dashboard source code

**Single Color**

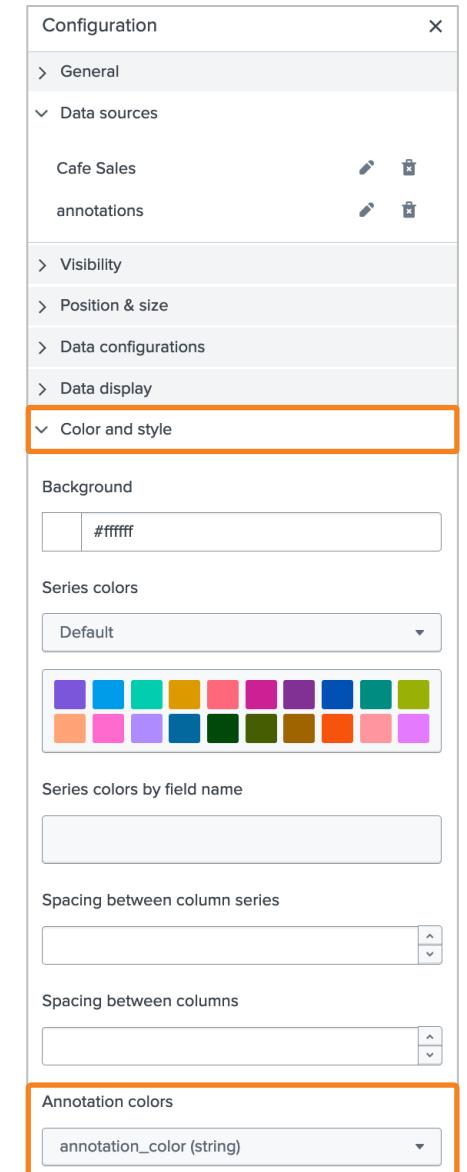
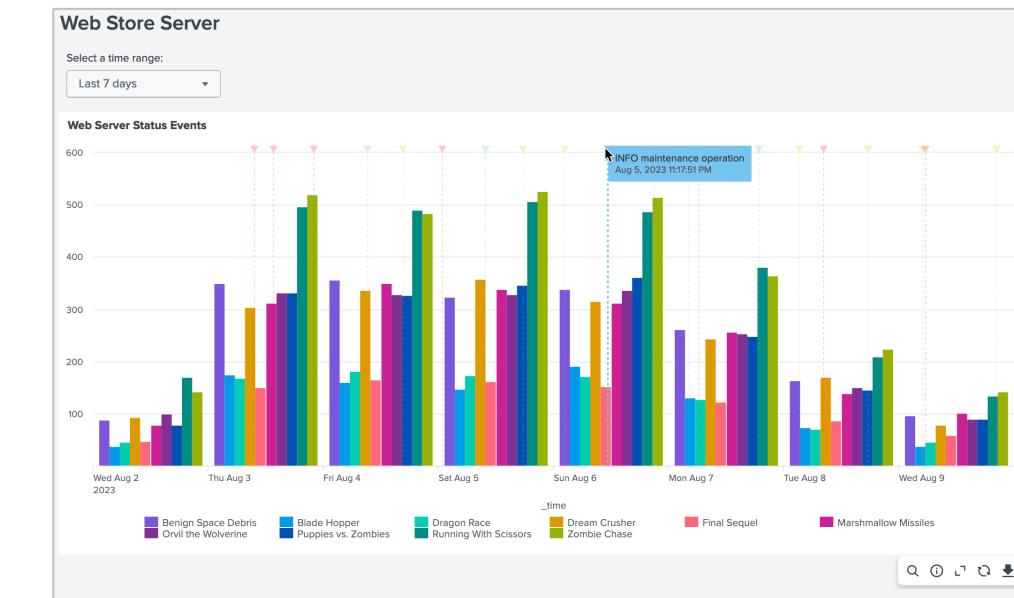
```
... | eval annotation_color = "#FF3300"
```

**Multiple Colors**

```
... | eval annotation_color = case(message="INFO maintenance operation", "#75C5F0", message="CRITICAL security issue", "#FF4747", message="WARNING network issue", "#F3CC17")
```

**Secondary Search: annotations**

```
index=webapp sourcetype=access_combined
| fields message
| eval annotation_color = case(message="INFO maintenance operation", "#75C5F0", message="CRITICAL security issue", "#FF4747", message="WARNING network issue", "#F3CC17")
```



# Lab 2 – Create an Event Annotation

Time: 25 minutes

## Tasks:

- Create a dashboard
- Add a single value visualization
- Add a column chart
- Add an annotation search



# Topic 3: Improving Performance

# Topic Objectives

- Name ways to improve dashboard performance
- Create base and chain searches
- Set dashboard defaults

# Improving Performance

- Refine searches
- Schedule reports
- Accelerate reports
- Accelerate data models
- Use the tstats command
- Use chain searches



# Use Scheduled Reports

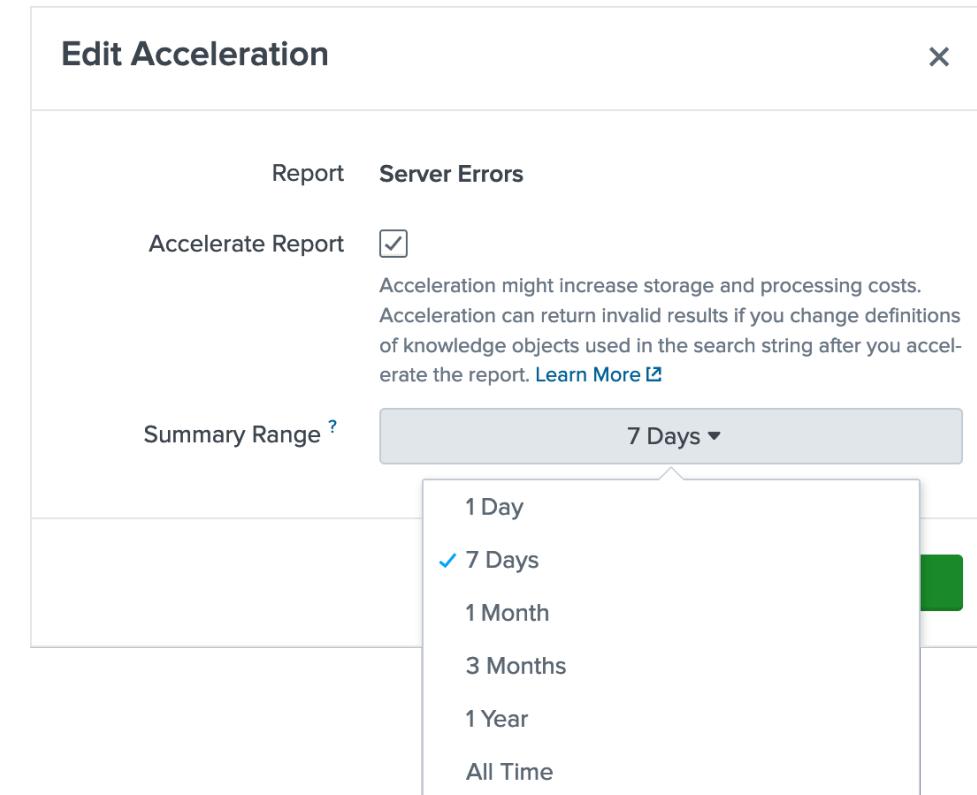
- Avoid inline searches
- Schedule to run every 5 or 10 minutes or less
- Prevent a flood of search jobs when dashboards are loaded

The image displays two side-by-side 'Edit Schedule' dialog boxes from the Splunk interface. Both dialogs have 'Report' and 'Server Errors' tabs selected, with 'Schedule Report' checked. In the left dialog, the 'Schedule' dropdown is set to 'Run on Cron Schedule', and the 'Cron Expression' field contains '0 6 \* \* 1'. In the right dialog, the 'Schedule' dropdown is set to 'Run every week', and the 'On' field is set to 'Monday' and the 'at' field is set to '6:00'.

| Cron Parameter | Schedule                                |
|----------------|-----------------------------------------|
| */5 * * * *    | Every 5 minutes                         |
| */30 * * * *   | Every 30 minutes                        |
| 0 */12 * * *   | Every 12 hours, on the hour             |
| */20 * * * 1-5 | Every 20 minutes, Monday through Friday |
| 0 9 1-7 * 1    | First Monday of each month, at 9am.     |

# Accelerated Reports

- Automatically creates summaries to speed completion times
- Periodically ages out data
- Data is stored on the indexers
- Search must meet three criteria:
  - Uses a transforming command
  - Commands before the first transforming command, must be streamable
  - Cannot use event sampling



# Accelerated Data Models

- Accelerates all fields defined in a data model
- Creates time-series index (TSIDX) files
- Updates every five minutes
- Only users with admin permissions can accelerate data models (default)
- Anyone can search using an accelerated data model

The screenshot shows the Splunk interface for managing data models. At the top, there's a header with "Data Models" and a sub-header stating "Data models enable users to easily create reports in the Pivot tool. Learn More". Below this is a table titled "Data Models" with columns for "Title", "Type", and "Actions". Several data models are listed, including "Alerts", "Application State", "Authentication", "Certificates", "Change Analysis", "CIM Validation (S.o.S.)", "Data Loss Prevention", "Databases", and "Email". The "Edit Datasets" and "Edit Acceleration" options are highlighted with blue and orange boxes respectively. A modal window titled "Edit Acceleration" is open for the "bcg\_xl" data model. It contains fields for "Data Model" (set to "bcg\_xl"), "Accelerate" (with a checked checkbox), and "Summary Range" (set to "7 Days"). There are "Cancel" and "Save" buttons at the bottom of the modal.

# Base & Chain Searches

- Base Searches

- Use a transforming search (**stats**, **chart**, **timechart**, etc.)
  - Fields are automatically available for chain searches
- If non-transforming, use the **fields** command to name fields in the chain search
  - Only the first 500,000 events are returned
  - Fields not in the base search appear null in a chain search

- Chain Searches

- Do not process events in excess of 500,000, silently ignoring them (matches the `max_count` default setting in `limits.conf`)
- Large number of results passed to a chain can cause a timeout
- Chain search complexity can cause a timeout
- Time-related tokens are only supported in base searches, not chain searches

**New Data Source**

**Data source name**: myBaseSearch

**SPL query**:

```
index=cafegames sourcetype=access_combined_cg
| stats count by action, description, host,
 product_name, status, _time
| fillnull value="NONE"
```

**Time range**: Global Time Range (global\_time)

**Usage**: 1 visualization, 0 inputs, 0 chain searches

**Code**:

```
1 [
2 "type": "ds.search",
3 "options": {
4 "query": "index=cafegames sou",
5 "queryParameters": {
6 "earliest": "$global_time",
7 "latest": "$global_time.l"
8 }
9 },
10 "name": "myBaseSearch"
11]
```

**1 visualization will be updated**

**New Data Source**

**Data source name**: myChainSearch

**SPL query**:

```
index=cafegames sourcetype=access_combined_cg
| stats count by action, description, host,
 product_name, status, _time
| fillnull value="NONE"
```

**Parent Search**: myBaseSearch

**myBaseSearch**: index=cafegames sourcetype=access\_combined\_cg
| stats count by action, description, host,
 product\_name, status, \_time
| fillnull value="NONE"

**myChainSearch**: | search status>399 host=\*
| timechart count by status useother=f

**Time range**: Currently using Global Time Range input
\$global\_time.earliest\$ - \$global\_time.latest\$

**Usage**: 0 visualizations, 0 inputs, 0 chain searches

**Code**:

```
1 [
2 "type": "ds.chain",
3 "options": {
4 "extend": "ds_xzcbkWEg",
5 "query": "| search status>39"
6 },
7 "name": "myChainSearch"
8]
```

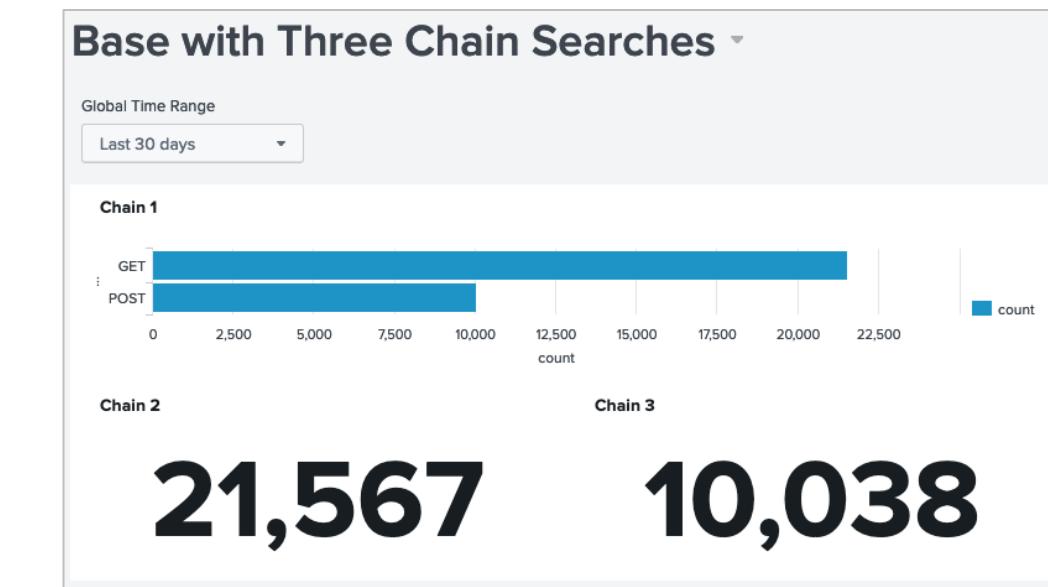
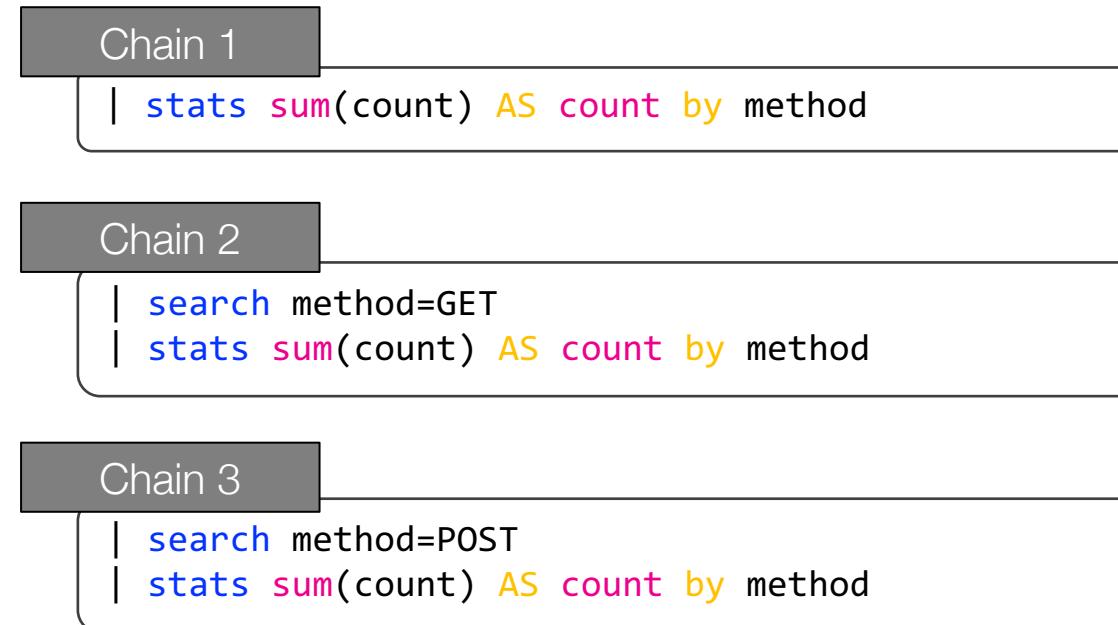
**Data Source ID**

# Data Source Types – ds.chain

- Instead of multiple searches you can use a base search with multiple chain searches
  - The base search gathers statistics for the downline processing

```
index=web sourcetype=access_combined status>399 | stats count by host, status, method
```

- The chain(s) performs further processing of results



# Data Source Types – ds.chain (cont.)

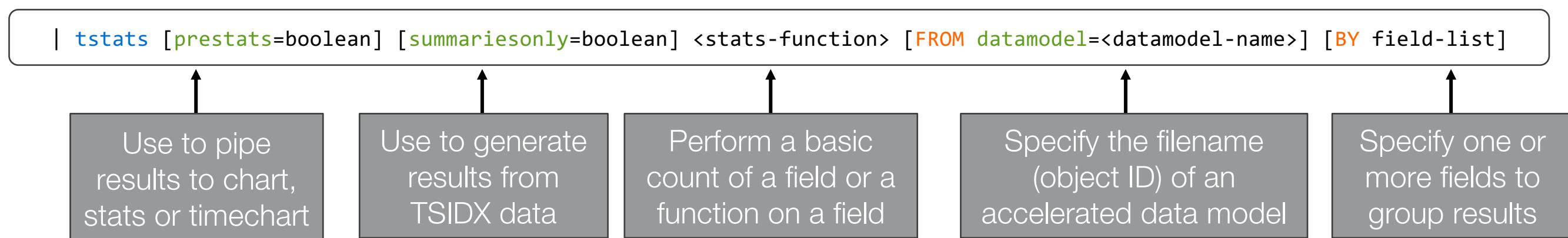
- Multiple searches with the same initial sections of SPL can use the initial section as a base search
- Extend inline searches, saved searches, or a chain search (once)
- Query parameters (refresh rate, time range) are inherited from the base search
- Chain searches use less computing power because the base search is only run one time
- Global search: a single base search with chain searches that populate all visualizations on a dashboard

What it looks like in the dashboard source

```
...
"dataSources": {
 "myBase": {
 "type": "ds.search",
 "options": {
 "query": "index=web sourcetype=access_combined status>399 | stats count by host, status, method\\n"
 },
 "name": "Base Search"
 },
 "myChain1": {
 "type": "ds.chain",
 "options": {
 "extend": "myBase",
 "query": "| stats sum(count) AS count by method"
 },
 "name": "Chain_1"
 },
 "myChain2": {
 "type": "ds.chain",
 "options": {
 "extend": "myBase",
 "query": "| search method=GET\\n| stats sum(count) AS count by method"
 },
 "name": "Chain_2"
 },
 "myChain3": {
 "type": "ds.chain",
 "options": {
 "extend": "myBase",
 "query": "| search method=POST\\n| stats sum(count) AS count by method"
 },
 "name": "Chain_3"
 },
 ...
}
```

# tstats Command

- Generating command
- Use to search data models or data model objects
- Perform statistical queries on indexed fields in tsidx files
  - Also, against indexed fields like source, host, sourcetype, and index
- Wildcard characters are not supported in field values in aggregate functions or BY clauses



# tstats Command – Arguments

- **prestats=<boolean>**
  - **true** allows you to pipe the data to chart, stats, or timechart
    - Prevents renaming the result using the AS keyword
    - Enables **append=t** where the results append to existing results instead of generating them
  - **false** is the default

```
| tstats [prestats=boolean] [summariesonly=boolean] <stats-function> [FROM datamodel=<datamodel-name>] [BY field-list]
```

# tstats Command – Arguments (cont.)

- **summariesonly=<boolean>**
  - Applies only to an accelerated data model
  - **true** generates results from summarized data (an accelerated data model's TSIDX data)
  - **false** (default) generates results from both summarized and non-summarized data
    - May cause a larger result count if: some of the data has not yet been added to the summary OR has been aged out of it

```
| tstats [prestats=boolean] [summariesonly=boolean] <stats-function> [FROM datamodel=<datamodel-name>] [BY field-list]
```

# tstats Command – Functions

- **stats-function**

- Perform a basic count or a function on a field
- Perform any number of aggregates
- Can rename the result using AS

```
| tstats [prestats=boolean] [summariesonly=boolean] <stats-function> [FROM datamodel=<datamodel-name>] [BY field-list]
```

| Type                                 | Supported functions and syntax                  |                                                          |                                               |                                                         |  |
|--------------------------------------|-------------------------------------------------|----------------------------------------------------------|-----------------------------------------------|---------------------------------------------------------|--|
| Aggregate functions                  | avg()<br>count()<br>distinct_count()<br>estdc() | exactperc<int>()<br>max()<br>median()<br>min()<br>mode() | perc<int>()<br>range()<br>stdev()<br>stdevp() | sum()<br>sumsq()<br>upperperc<int>()<br>var()<br>varp() |  |
| Event order functions                | earliest()                                      | first()                                                  | last()                                        | latest()                                                |  |
| Multivalue stats and chart functions | values(x)                                       |                                                          |                                               |                                                         |  |

# tstats Command – Clause Arguments

- **FROM datamodel=<datamodel-name>**
  - Accesses an accelerated data model's summaries
- **WHERE <search-query>**
  - Specify a search
  - Can specify a set of values with the IN operator
- **BY <field-list>**
  - You must specify a field-list
  - Use span to group the time buckets
  - Cannot use wildcards

```
| tstats [prestats=boolean] [summariesonly=boolean] <stats-function> [FROM datamodel=<datamodel-name>] [BY field-list]
```

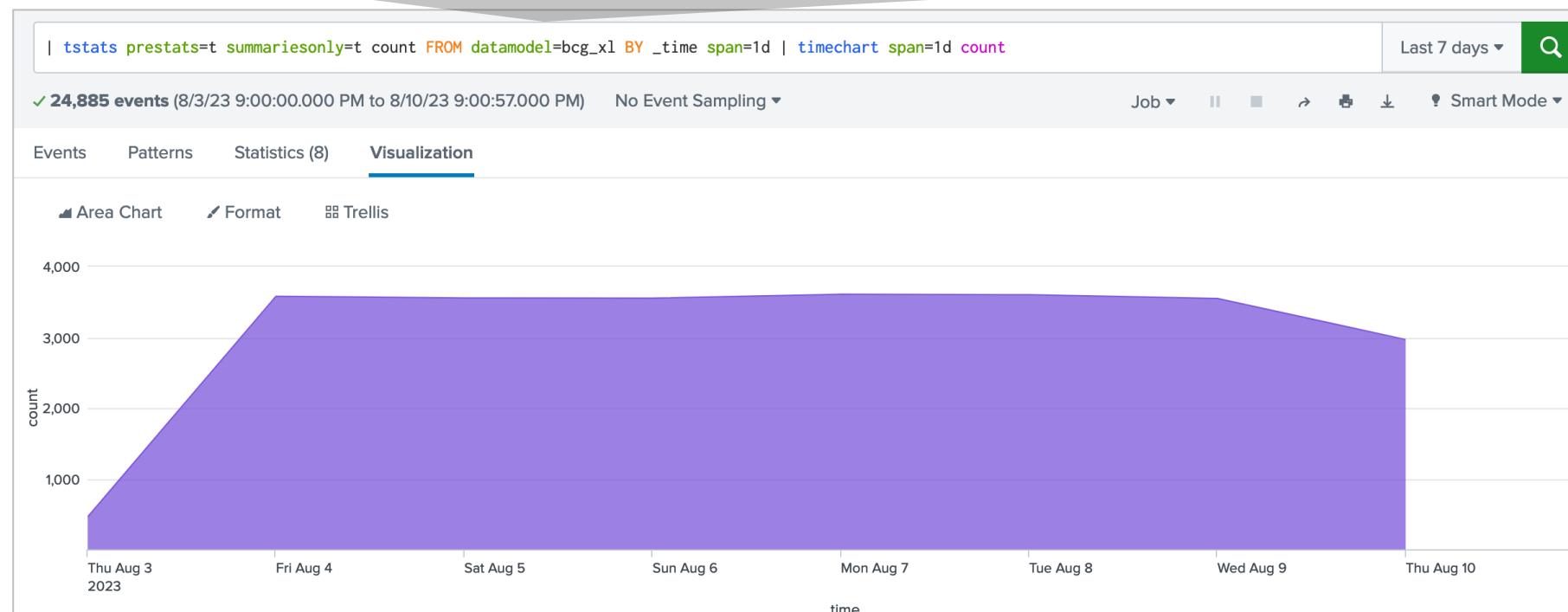
# tstats Command – Example

tstats is a transforming command

Generates results from only the accelerated data model's TSIDX data

Uses the bsg\_xl data model summaries

```
| tstats prestats=t summariesonly=t count FROM datamodel=bcg_xl BY _time span=1d | timechart span=1d count
```



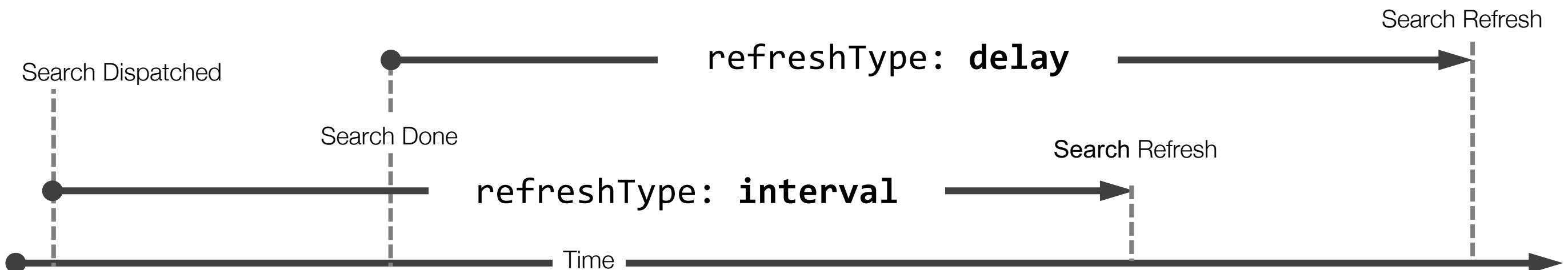
# Dashboard Definition – defaults

- Can set all data source or visualization options in one place
  - For example, query parameters, refresh, refresh type, show progress bar, and show last updated
- Exceptions
  - Settings at the component level, in the **visualization** or **dataSource** sections, override the same settings in **defaults**

```
...
 "defaults": {
 "dataSources": {
 "ds.search": {
 "options": {
 "refresh": "10m",
 "refreshType": "delay",
 "queryParameters": {
 "latest": "$global_time.latest$",
 "earliest": "$global_time.earliest$"
 }
 }
 }
 }
 }
}
```

# Setting Dashboard Defaults – Example

- Auto-Refresh
  - **refresh**: amount of time between refreshes
    - Default: do not refresh
  - **refreshType**: point from which the refresh time is counted
    - **delay**: start counting down when the search is done (default)
    - **interval**: start counting when the search is dispatched



# Setting Dashboard Defaults – Example (cont.)

- 1 All `ds.search` (inline search) stanzas refresh every 5 minutes
  - Saved searches and chain searches will not refresh every 5 minutes
- 2 Using the `refreshType` setting `interval`, the refresh time starts counting when the search is dispatched
- 3 All visualizations will not show a progress bar when updating
- 4 All visualizations will not show the time they were last updated

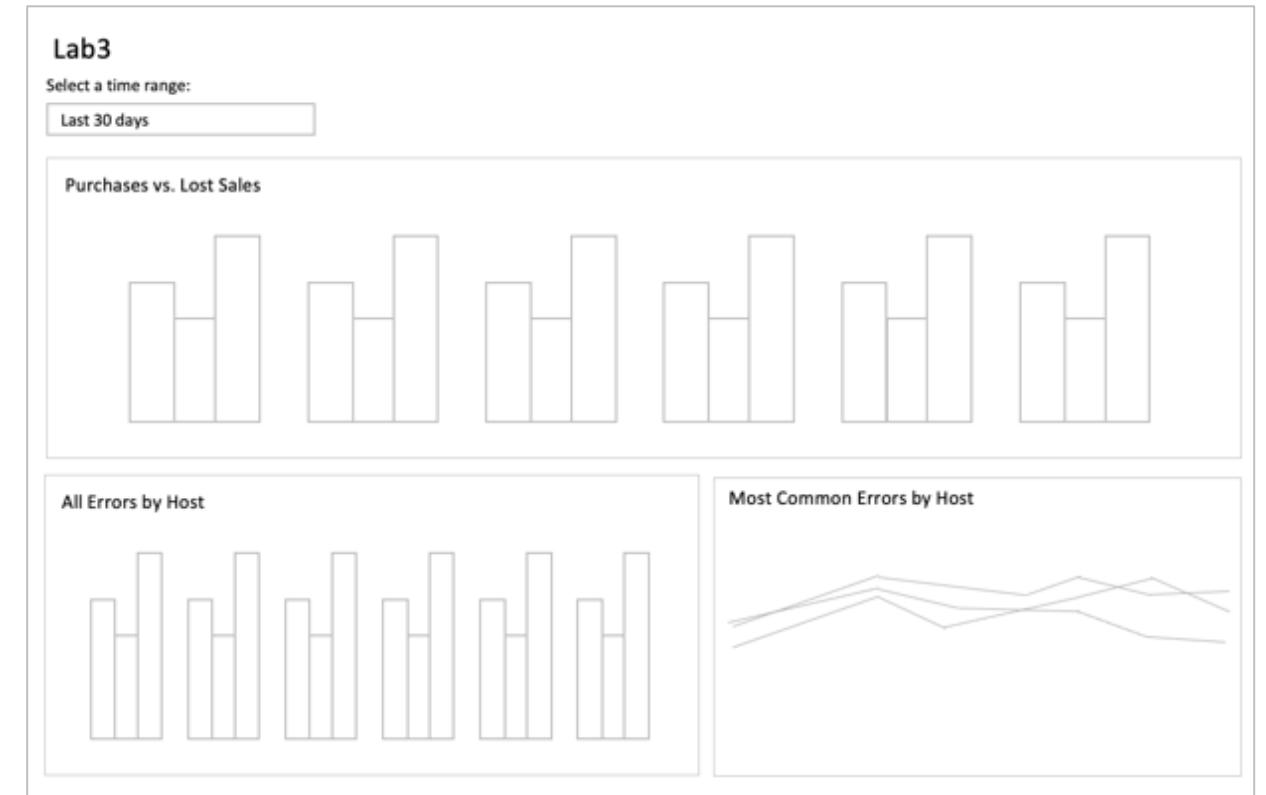
```
...
 "defaults": {
 "dataSources": {
 "ds.search": {
 "options": {
 "refresh": "5m", 1
 "refreshType": "interval", 2
 "queryParameters": {
 "latest": "$global_time.latest$"
 "earliest": "$global_time.earliest$"
 }
 }
 }
 }
 }
 "visualizations": {
 "global": {
 "showProgressBar": false, 3
 "showLastUpdated": false 4
 }
 }
}
```

# Lab 3 – Improve Performance

Time: 25 minutes

Tasks:

- Create a dashboard
- Add base and chain searches
- Add chart visualizations
- Use tstats command
- Use an accelerated data model
- Compare the search times of an ad-hoc search and a search using tstats with an accelerated data model



# Wrap Up



- You should now be able to:
  - Describe the dashboard framework
  - Identify the dashboard definition
  - Name the dashboard workflows
  - Compare absolute and grid layouts
  - Create event annotations
  - Use mock data
  - Describe troubleshooting steps
  - Use base and chain searches
  - Identify methods to improve performance



# Documentation

Search Docs

Search

## Topic 1: Create a Prototype

- [Create a dashboard in Dashboard Studio](#)
- [The source code stanza of a visualization](#)
- [Use layout options to modify your dashboard canvas with the source editor](#)

## Topic 2: Selecting a Data Source

- [Create search-based visualizations](#)
- [Use reports and saved searches](#)
- [Use mock data](#)
- [Add secondary data sources](#)

- Topic 3: Improving Performance

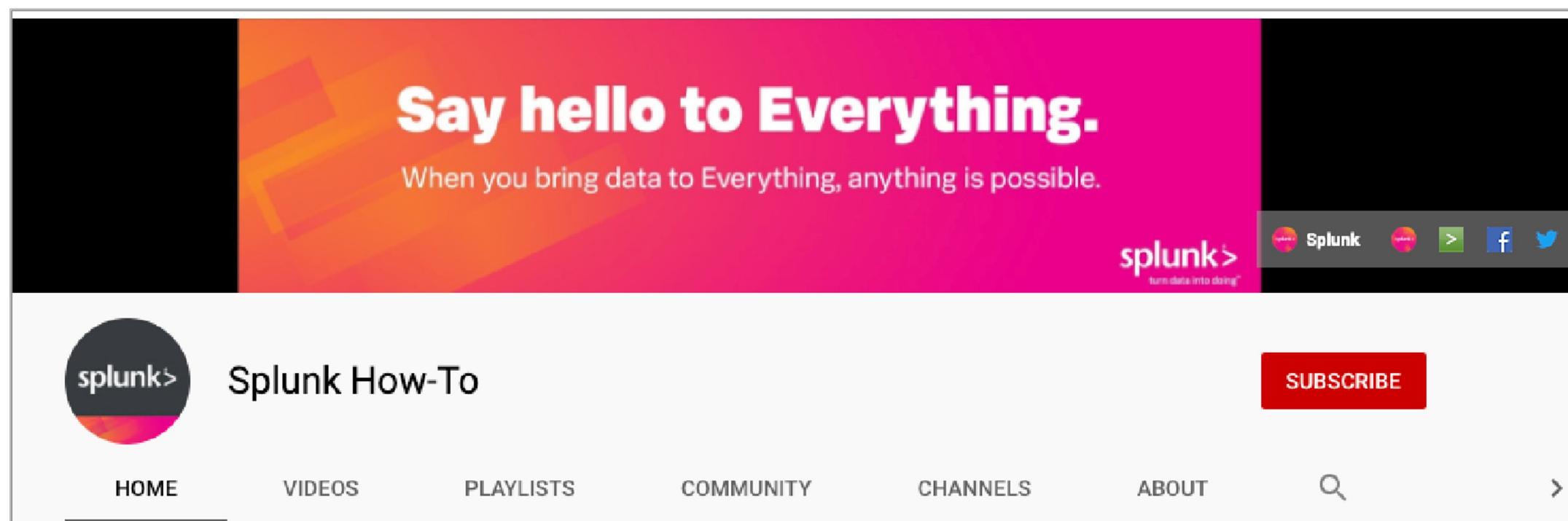
- [Set global and local defaults](#)
- [Chain searches together with a base search and chain searches](#)
- [Search Reference – tstats](#)
- [Accelerate Data Models](#)

# Community

- Splunk Community Portal  
<https://community.splunk.com/>
  - Answers
  - Discussions
  - Splunk Trust
  - User Groups
  - Ideas
- Splunk Blogs  
<https://splunk.com/blog/>
- Splunk Apps  
<https://splunkbase.com/>
- Splunk Dev Google Group  
<https://groups.google.com/forum/#!forum/splunkdev>
- Splunk Docs on Twitter  
<https://twitter.com/splunkdocs>
- Splunk Dev on Twitter  
<https://twitter.com/splunkdev>
- Splunk Live!  
<https://splunklive.splunk.com/>
- .conf  
<https://conf.splunk.com/>

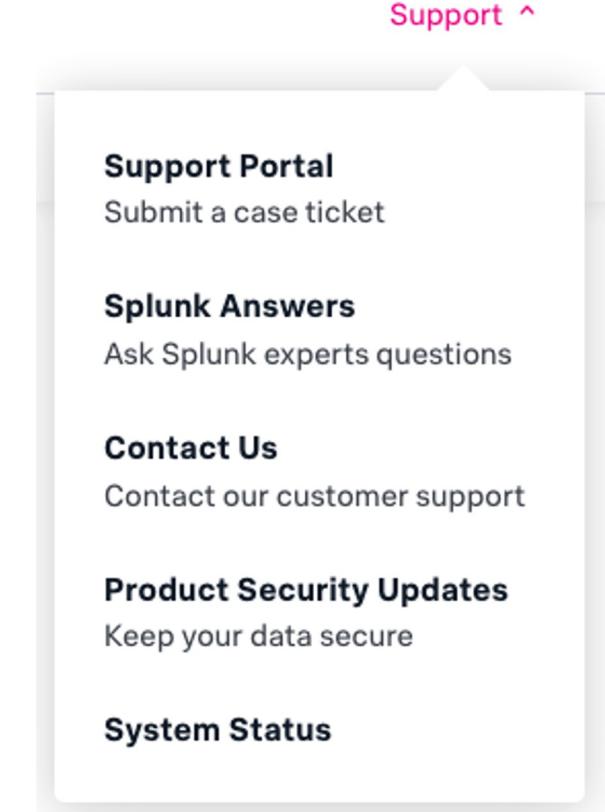
# Splunk How-To Channel

- Check out the Splunk Education How-To channel on YouTube: [splk.it/How-To](https://splk.it/How-To)
- Free, short videos on a variety of Splunk topics



# Support Programs

- Web
  - Documentation: [dev.splunk.com](https://dev.splunk.com) and [docs.splunk.com](https://docs.splunk.com)
  - Wiki: [wiki.splunk.com](https://wiki.splunk.com)
- Splunk Lantern: Guidance from Splunk experts
  - [lantern.splunk.com](https://lantern.splunk.com)
- Global Support: Support for critical issues, a dedicated resource to manage your account – 24 x 7 x 365
  - Web: [splunk.com/index.php/submit\\_issue](https://splunk.com/index.php/submit_issue)
- Enterprise, Cloud, ITSI, Security Support
  - Web: [splunk.com/en\\_us/about-splunk/contact-us.html#tabs/customersupport](https://splunk.com/en_us/about-splunk/contact-us.html#tabs/customersupport)
  - Phone: (855) SPLUNK-S or (855) 775-8657



# Learning Paths

## Search Expert - Recommended Courses

Free eLearning courses are highlighted in blue and courses with an \* are present in both learning paths.

- [Introduction to Splunk \\*](#)
- [Using Fields \\*](#)
- [Scheduling Reports and Alerts](#)
- [Visualizations](#)
- Statistical Processing
- Working with Time
- Comparing Values
- Result Modification
- Leveraging Lookups and Subsearches
- Correlation Analysis
- [Search Under the Hood](#)
- Multivalue Fields
- Search Optimization \*

# Learning Paths

## Knowledge Manager - Recommended Courses

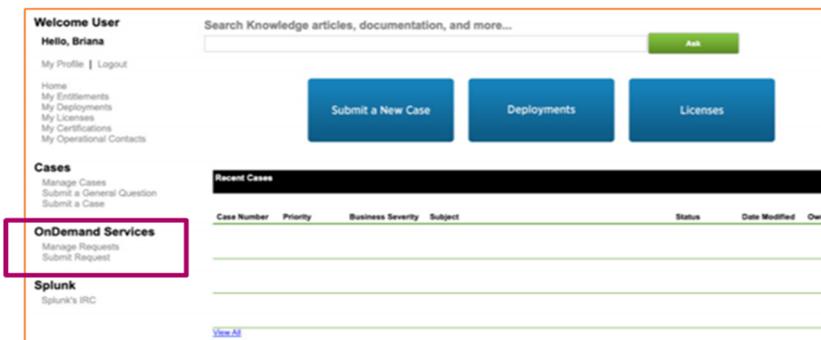
Free eLearning courses are in blue and courses with an asterisk (\*) are present in both learning paths.

- [Introduction to Splunk \\*](#)
- [Using Fields \\*](#)
- [Introduction to Knowledge Objects](#)
- Creating Knowledge Objects
- Creating Field Extractions
- Enriching Data with Lookups
- Data Models
- [Introduction to Dashboards](#)
- Dynamic Dashboards
- Creating Maps
- Search Optimization \*

# OnDemand Services for Expert Assistance

## Direct Access

- Credit-based service accessible through the Support Portal.



## Get Started

- Choose your product and desired task and get access to Splunk Experts!

## Continued Help

- Over 20 tasks available for continued growth and help:
- General consultations
- Adoption, onboarding
- ...and more!

# OnDemand Requests

- How to Open a Case
  - Most customers have [OnDemand Services](#) included as a part of their license purchase
- Use the [OnDemand Services Portal End User Guide](#)
  - Pick the product you need help with
  - Open a request under Pick Your Product > Splunk Core - Enterprise/Splunk Cloud and task Build a Simple Dashboard
- Issue Opening a Case?
  - Contact the ODS team at [OnDemand@splunk.com](mailto:OnDemand@splunk.com) OR contact your Customer Success Manager/Advocate or Account Team

# Splunk Mobile

- Free app available to all Splunk Cloud and Splunk Enterprise customers
- Analyze data and receive actionable alerts on-the-go with mobile-friendly dashboards
- iOS and Android
- See the [Product Brief](#)

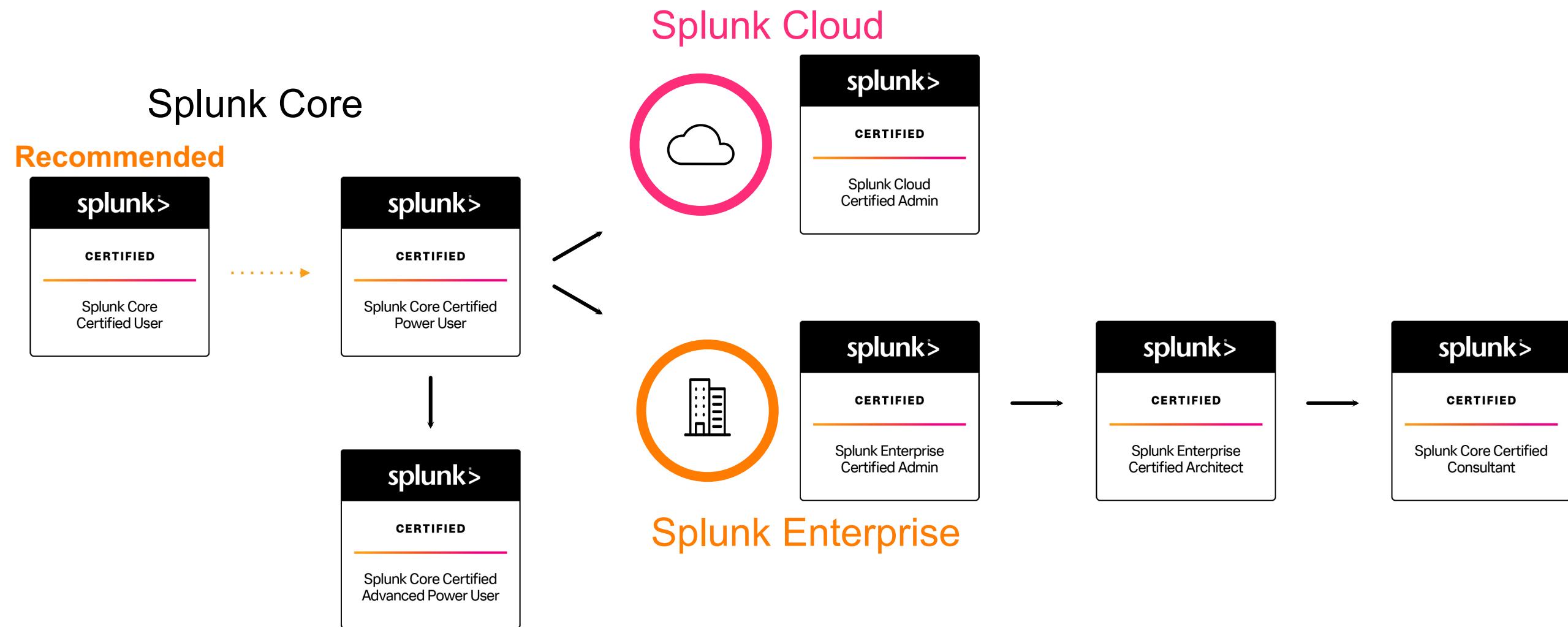


# Splunk Certification

## Offerings and Requirements

# Splunk Core and Beyond

Regardless of which Splunk product you use, it all starts with Splunk Core



# App-Specific Offerings

For Splunk Add-Ons



ES  
Administration



ITSI  
Administration



SOAR  
Automation  
Developer

# Splunk Core Certified User

This entry-level certification demonstrates an individual's basic ability to navigate and use Splunk software



## Prerequisite Certification(s):

- None

## Prerequisite Course(s):

- None

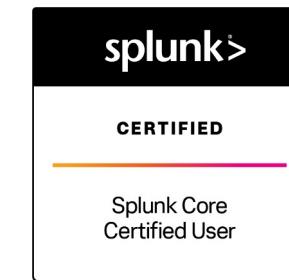
## Splunk Core Certified User Exam

Time to study! We suggest candidates looking to prepare for this exam complete Fundamentals 1 **or** the following courses:

- What is Splunk?
- Intro to Splunk
- Using Fields
- Scheduling Reports and Alerts
- Visualizations
- Statistical Processing
- Working with Time
- Leveraging Lookups and Subsearches
- Search Optimization
- Enriching Data with Lookups
- Data Models

See [here](#) for registration assistance.

## Congratulations! You are a...



## Recommended Next Step

- Splunk Core Certified Power User

# Splunk Core Certified Power User

This entry-level certification demonstrates an individual's foundational competence of Splunk's core software



## Prerequisite Certification(s):

- None

## Prerequisite Course(s):

- None

## Splunk Core Certified Power User Exam

Time to [study](#)! We suggest candidates looking to prepare for this exam complete Fundamentals 2 **or** the following courses:

- Visualizations
- Statistical Processing
- Working with Time
- Comparing Values
- Result Modification
- Correlation Analysis
- Search Under the Hood
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Data Models
- Creating Maps

See [here](#) for registration assistance.

## Congratulations! You are a...



## Recommended Next Steps

- [Splunk Core Certified Advanced Power User](#)
- [Splunk Enterprise Certified Admin](#)
- [Splunk Cloud Certified Admin](#)

# Splunk Core Certified Advanced Power User

This certification demonstrates an individual's ability to generate complex searches, reports, and dashboards with Splunk's core software to get the most out of their data



## Prerequisite Certification(s):

- [Splunk Core Certified Power User](#)

## Prerequisite Course(s):

- None

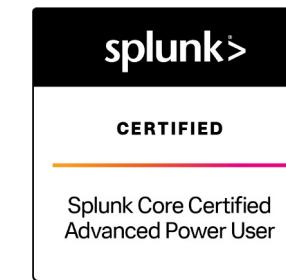
## Splunk Core Certified Advanced Power User Exam

Time to [study](#)! We suggest candidates looking to prepare for this exam complete Fundamentals 3, Creating Dashboards, and Advanced Searching & Reporting **or** the following courses:

- Using Fields
- Working with Time
- Comparing Values
- Result Modification
- Leveraging Lookups and Subsearches
- Correlation Analysis
- Search Under the Hood
- Multivalue Fields
- Search Optimization
- Creating Field Extractions
- Enriching Data with Lookups
- Data Models
- Creating Maps
- Introduction to Dashboards
- Dynamic Dashboards

See [here](#) for registration assistance.

## Congratulations! You are a...



## Recommended Next Steps

- [Splunk Enterprise Certified Admin](#)
- [Splunk Cloud Certified Admin](#)

# Splunk Cloud Certified Admin

This certification demonstrates an individual's ability to support the day-to-day administration and health of a Splunk Cloud environment



## Prerequisite Certification(s):

- [Splunk Core Certified Power User](#)

## Prerequisite Course(s):

- None

## Splunk Cloud Certified Admin Exam

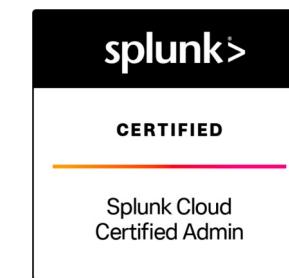
Time to [study](#)! We suggest candidates looking to prepare for this exam complete **either** the Splunk Cloud Administration **or** the Transitioning to Splunk Cloud course.

Both courses will equally prepare candidates for the exam, but are tailored to meet the needs of the individual based on prior Splunk experience.

**Splunk Cloud Administration** is designed for net-new administrators working in a Splunk Cloud environment. **Transitioning to Splunk Cloud** is for experienced Enterprise administrators looking to maximize their success in migrating to a Cloud environment.

See [here](#) for registration assistance.

## Congratulations! You are a...



# Splunk Enterprise Certified Admin

This certification demonstrates an individual's ability to support the day-to-day administration and health of a Splunk Enterprise environment



## Prerequisite Certification(s):

- [Splunk Core Certified Power User](#)

## Prerequisite Course(s):

- None

## Splunk Enterprise Certified Admin Exam

Time to [study](#)! We suggest candidates looking to prepare for this exam complete the following courses:

- Splunk System Administration
- Splunk Data Administration

See [here](#) for registration assistance.

## Congratulations! You are a...



## Recommended Next Steps

- [Splunk Enterprise Certified Architect](#)

# Splunk Certified Architect

This certification demonstrates an individual's ability to deploy, manage, and troubleshoot complex Splunk Enterprise environments



## Prerequisite Certification(s):

- [Splunk Core Certified Power User](#)
- [Splunk Enterprise Certified Admin](#)

## Prerequisite Course(s):

- Architecting Splunk Enterprise Deployments
- Troubleshooting Splunk Enterprise
- Splunk Cluster Administration
- Splunk Deployment Practical Lab

## Splunk Enterprise Certified Architect Exam

Time to [study](#)! We **require** candidates looking to register for this exam to complete the following prerequisite courses:

- Architecting Splunk Enterprise Deployments
- Troubleshooting Splunk Enterprise
- Splunk Cluster Administration
- Splunk Deployment Practical Lab

Candidates who are **Splunk Enterprise Certified Admin** and have completed all of the above courses will automatically receive an exam authorization for the Splunk Enterprise Certified Architect exam within 5-7 business days of receiving their passing lab results.

See [here](#) for registration assistance.

## Congratulations! You are a...



## Recommended Next Steps

- [Splunk Core Certified Consultant](#)

# Splunk Core Certified Consultant

This certification demonstrates an individual's ability to properly size, install, and implement Splunk environments and to advise others on how to utilize the product and maximize its value for their needs



## Prerequisite Certification(s):

- [Splunk Core Certified Power User](#)
- [Splunk Enterprise Certified Admin](#)
- [Splunk Enterprise Certified Architect](#)

## Prerequisite Course(s):

- Advanced Power User courses **or** digital badge\*
- Core Consultant Labs
  - Indexer Cluster Implementation
  - Distributed Search Migration
  - Implementation Fundamentals
  - Architect Implementation 1-3
  - Services Core Implementation

## Splunk Core Certified Consultant Exam

Time to [study](#)! We **require** candidates looking to register for this exam to complete the following prerequisite courses:

- *Fundamentals 3, Creating Dashboards, Advanced Searching & Reporting\**
- Core Consultant Labs
- Services Core Implementation

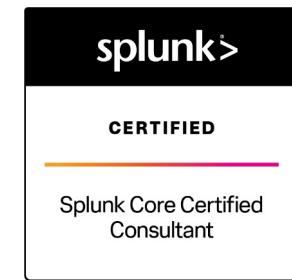
Candidates who are **Splunk Enterprise Certified Architects** and have completed all of the above courses must contact [certification@splunk.com](mailto:certification@splunk.com) to request their Core Consultant exam authorization.

See [here](#) for registration assistance.

*\*These Advanced Power User courses can be replaced with a Splunk Certified Advanced Power User badge **or** completion of the following courses:*

- |                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Using Fields</li> <li>• Creating Field Extractions</li> <li>• Enriching Data with Lookups</li> <li>• Data Models</li> <li>• Search Optimization</li> <li>• Working with Time</li> <li>• Leveraging Lookups and Subsearches</li> <li>• Comparing Values</li> </ul> | <ul style="list-style-type: none"> <li>• Correlation Analysis</li> <li>• Result Modification</li> <li>• Multivalue Fields</li> <li>• Search Under the Hood</li> <li>• Introduction to Dashboards</li> <li>• Dynamic Dashboards</li> <li>• Creating Maps</li> </ul> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Congratulations! You are a...



## Recommended Next Steps

- None

# Splunk Enterprise Security Certified Admin

This certification demonstrates an individual's ability to install, configure, and manage a Splunk Enterprise Security deployment



## Prerequisite Certification(s):

- None

## Prerequisite Course(s):

- None

## Splunk Enterprise Security Certified Admin Exam

Time to [study](#)! We suggest candidates looking to prepare for this exam complete the following course:

- Administering Splunk Enterprise Security

Please note: all candidates are expected to have working knowledge and experience as either Splunk Cloud or Splunk Enterprise Administrators.

See [here](#) for registration assistance.

## Congratulations! You are a...



## Recommended Next Steps

- Splunk Phantom Certified Admin

# Splunk IT Service Intelligence Certified Admin

This certification demonstrates an individual's ability to deploy, manage, and utilize Splunk ITSI to monitor mission-critical services



## Prerequisite Certification(s):

- None

## Prerequisite Course(s):

- None

## Splunk IT Service Intelligence Certified Admin Exam

Time to [study](#)! We suggest candidates looking to prepare for this exam complete the following course:

- Implementing Splunk IT Service Intelligence

Please note: all candidates are expected to have working knowledge and experience as either Splunk Cloud or Splunk Enterprise Administrators.

See [here](#) for registration assistance.

Congratulations! You are a...



## Recommended Next Steps

- [Courses on Observability](#)

# Splunk SOAR Certified Automation Developer

This certification demonstrates an individual's ability to install and configure a SOAR server, integrate it with Splunk, and plan, design, create, and debug playbooks



## Prerequisite Certification(s):

- None

## Prerequisite Course(s):

- None

## Splunk SOAR Certified Automation Developer Exam

Time to [study](#)! We suggest candidates looking to prepare for this exam complete the following courses:

- Administering SOAR (Phantom)
- Developing SOAR (Phantom) Playbooks
- Advanced SOAR (Phantom) Implementation

Please note: all candidates are expected to have working knowledge and experience as either Splunk Cloud or Splunk Enterprise Administrators.

See [here](#) for registration assistance.

## Congratulations! You are a...



## Recommended Next Steps

- None

# Thank You



**splunk**® turn data into doing™