Introduction to Dashboards

splunk>

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

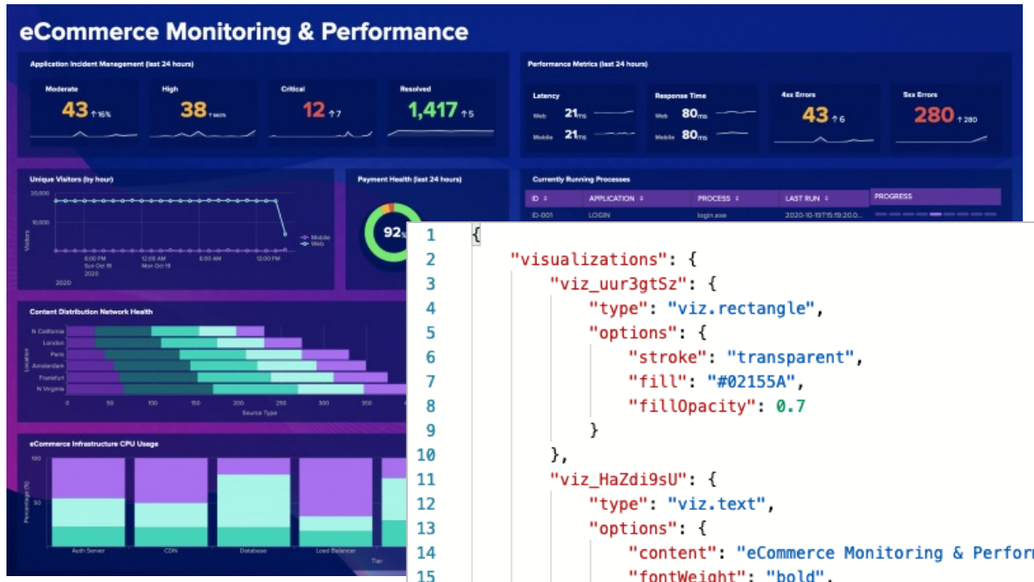
Topic 1: Create a Prototype

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




```
{
    "visualizations": {
        "viz_uur3gtSz": {
            "type": "viz.rectangle",
            "options": {
                "stroke": "transparent",
                "fill": "#02155A",
                "fillOpacity": 0.7
            }
        },
        "viz_HaZdi9sU": {
            "type": "viz.text",
            "options": {
                "content": "eCommerce Monitoring & Performance",
                "fontWeight": "bold",
                "fontSize": 48,
                "textColor": "#ffffff"
            }
        },
        "viz_ydtjTtwP": {
            "type": "viz.rectangle",
            "options": {
                "stroke": "transparent",
                "fill": "#02155A",
                "fillOpacity": 0.7
            }
        },
        "viz_IR0RxRMk": {
            "type": "viz.rectangle",
```


splunk>

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

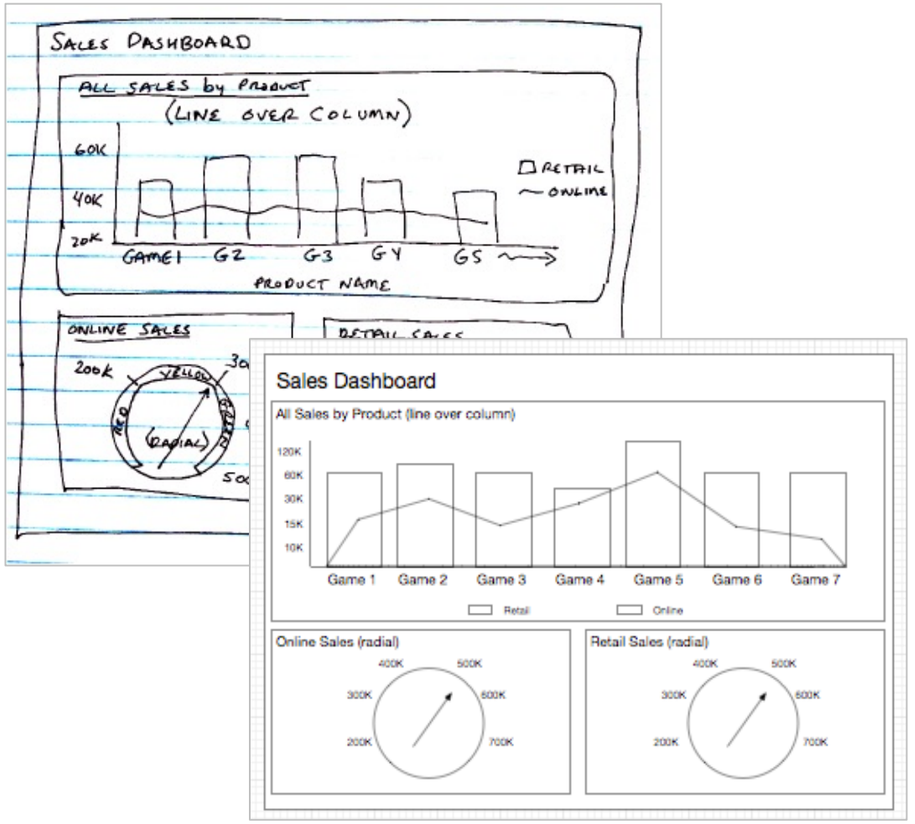
```
{
    "visualizations": {…
    },
    "dataSources": {…
    },
    "defaults": {…
    },
    "inputs": {…
    },
    "layout": {…
    },
    "description": "",
    "title": "Web Sales"
}
```


splunk>

Plan

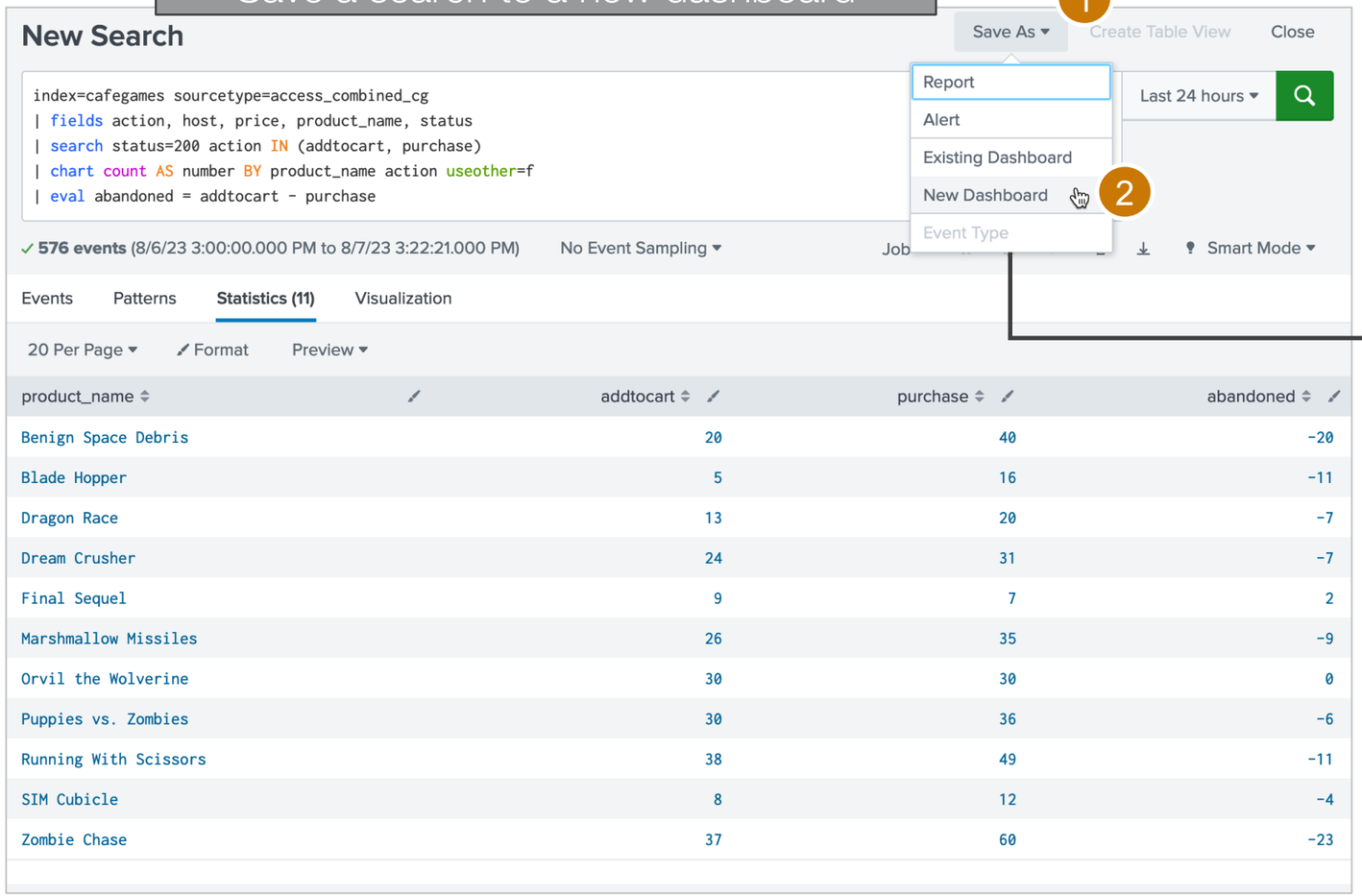
- Who is the audience?
- What is your data story?
- Identify stakeholders
- Use wireframing
- Create a prototype

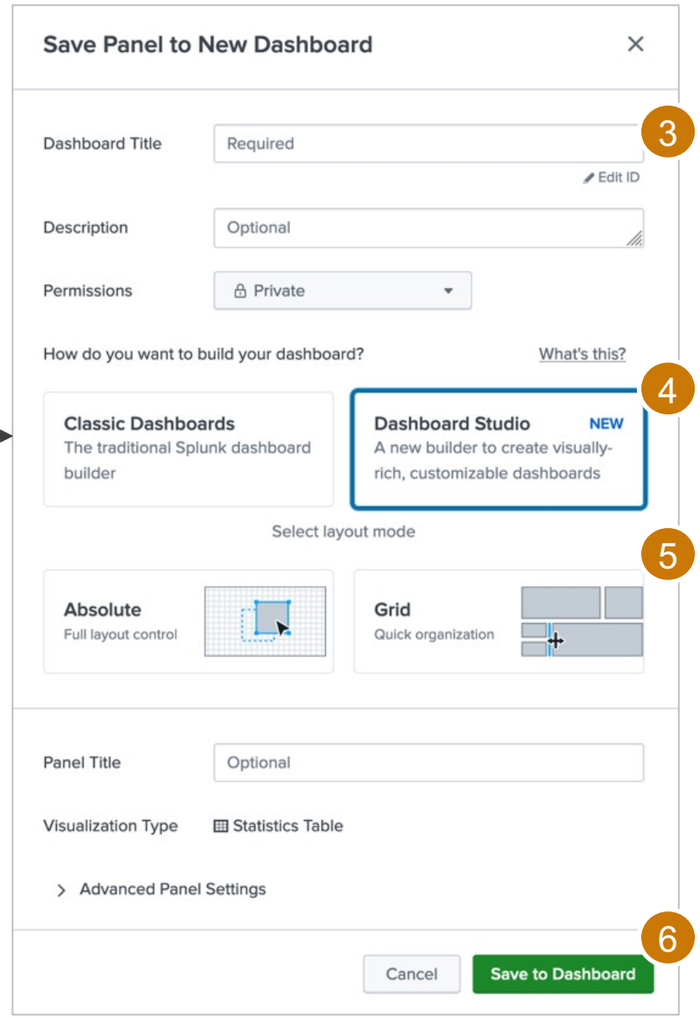
Wireframes:
hand drawn or digital drawings



Creating a Dashboard

Save a search to a new dashboard

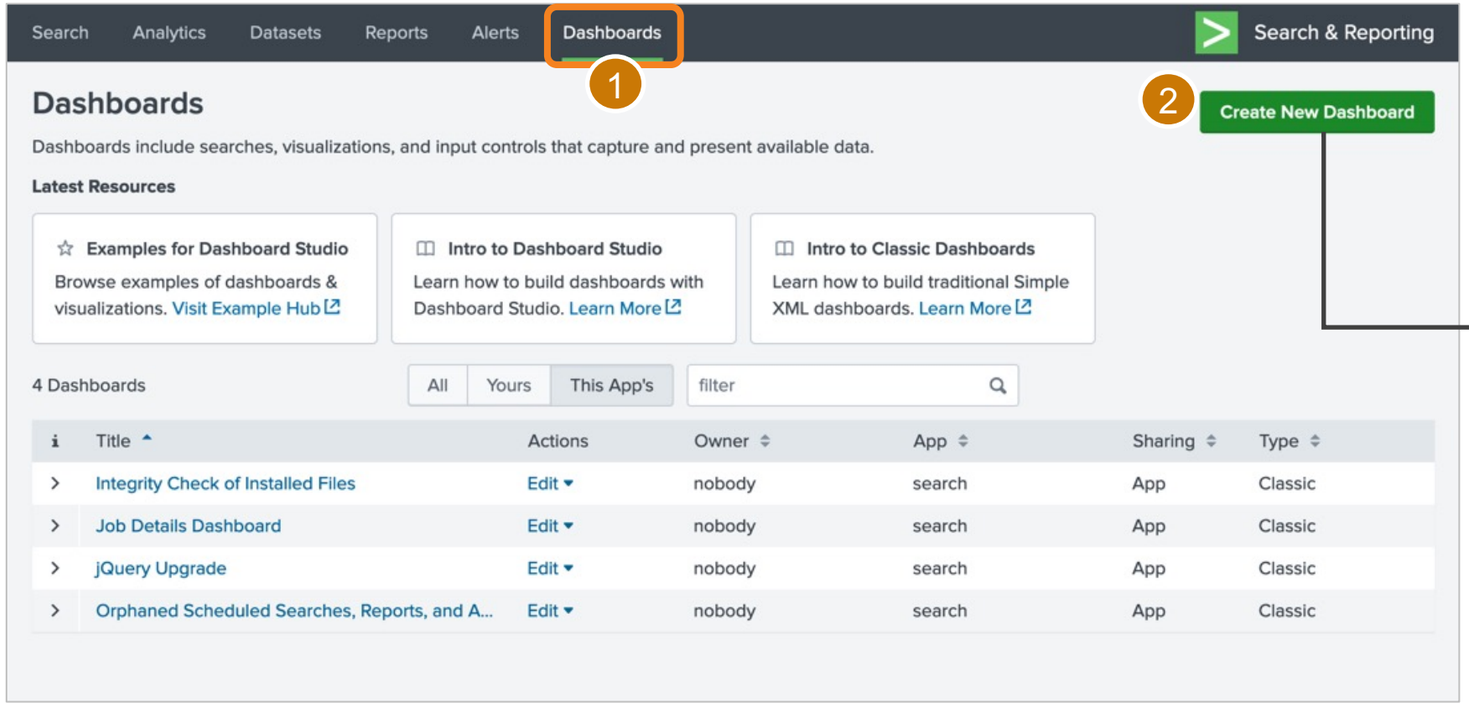


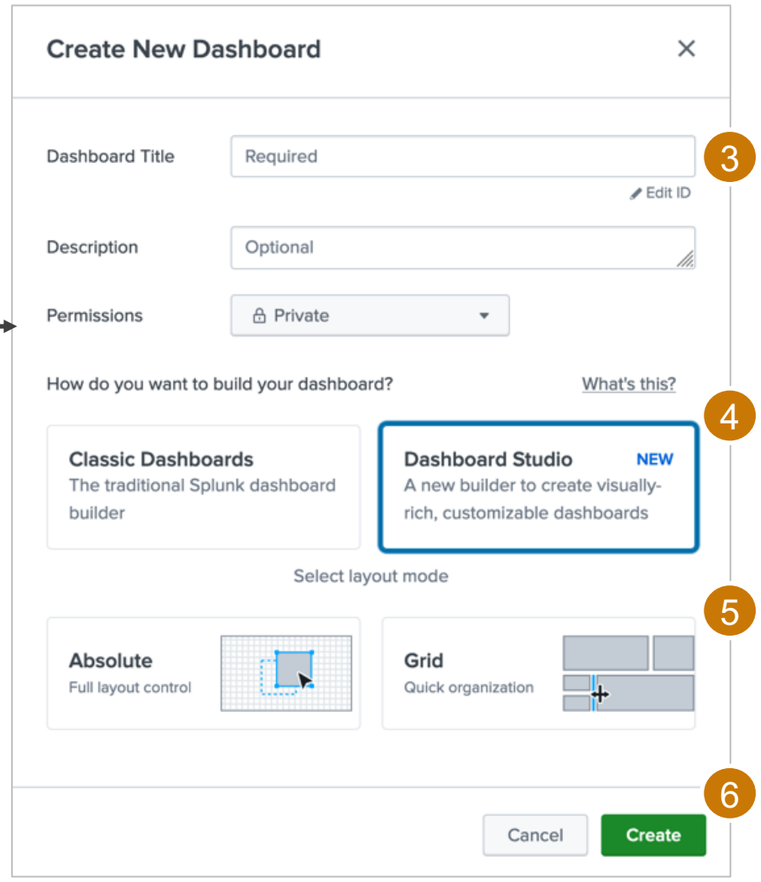


splunk>

Creating a Dashboard (cont.)

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



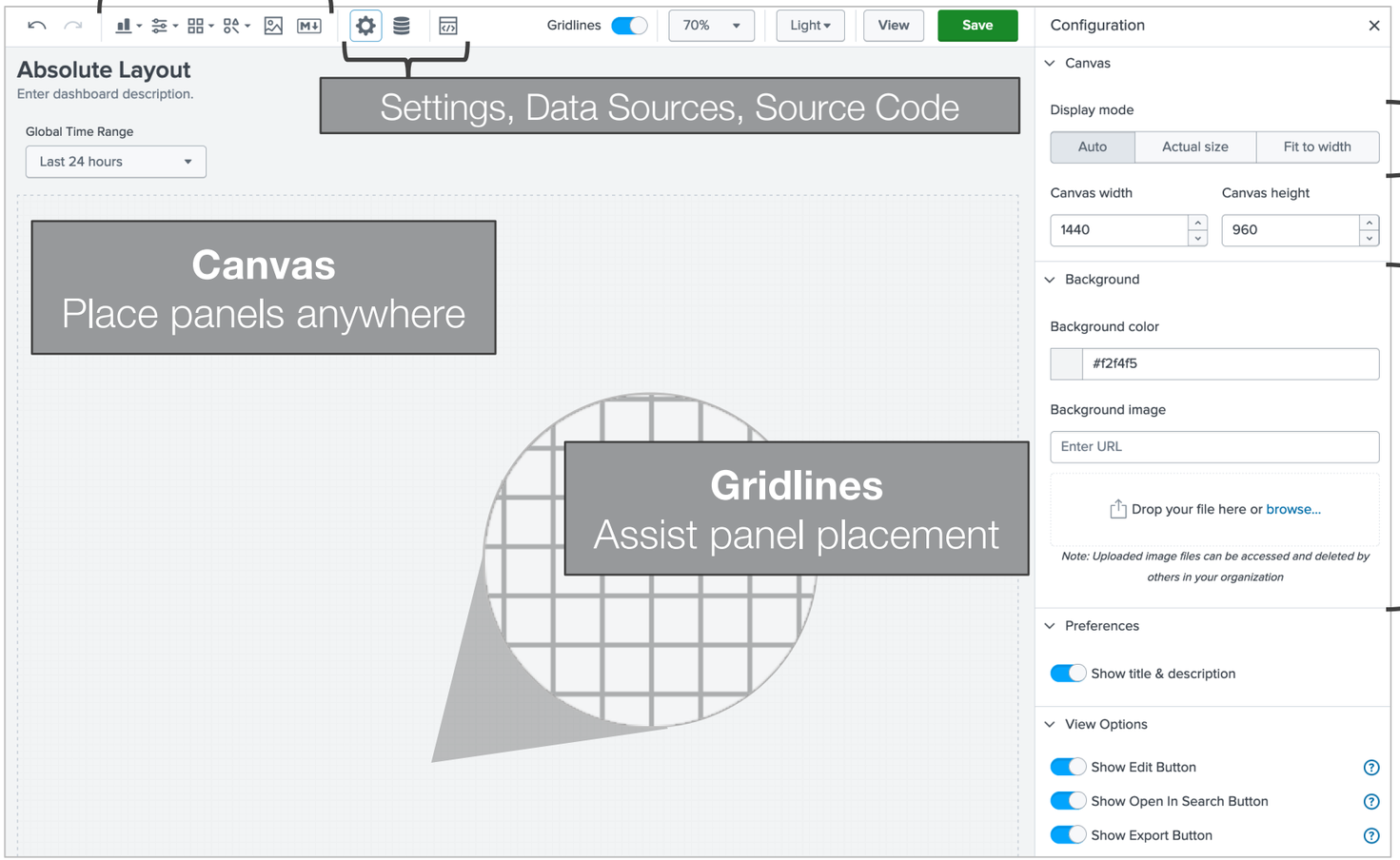


splunk>

Absolute Layout

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

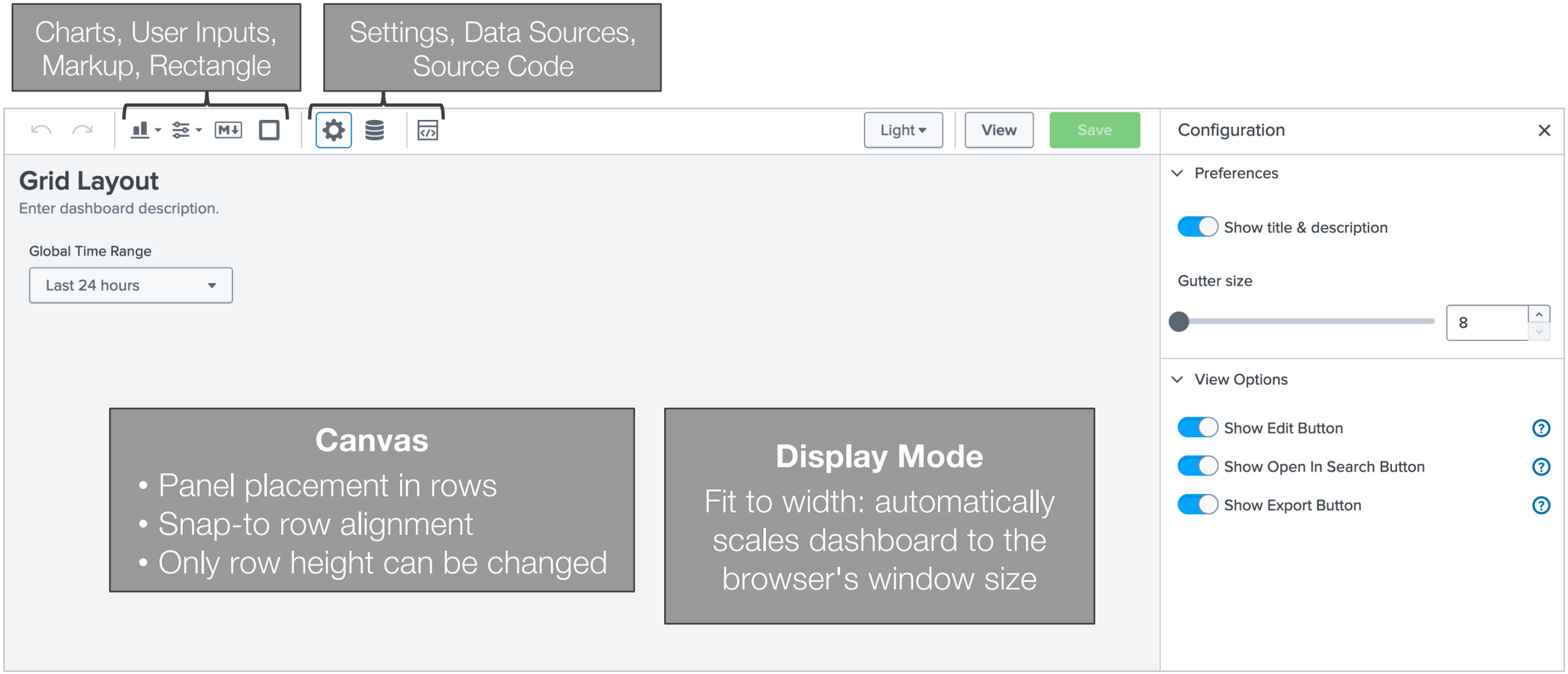
Background

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

Background image: upload or reference a custom image

splunk>

Grid Layout



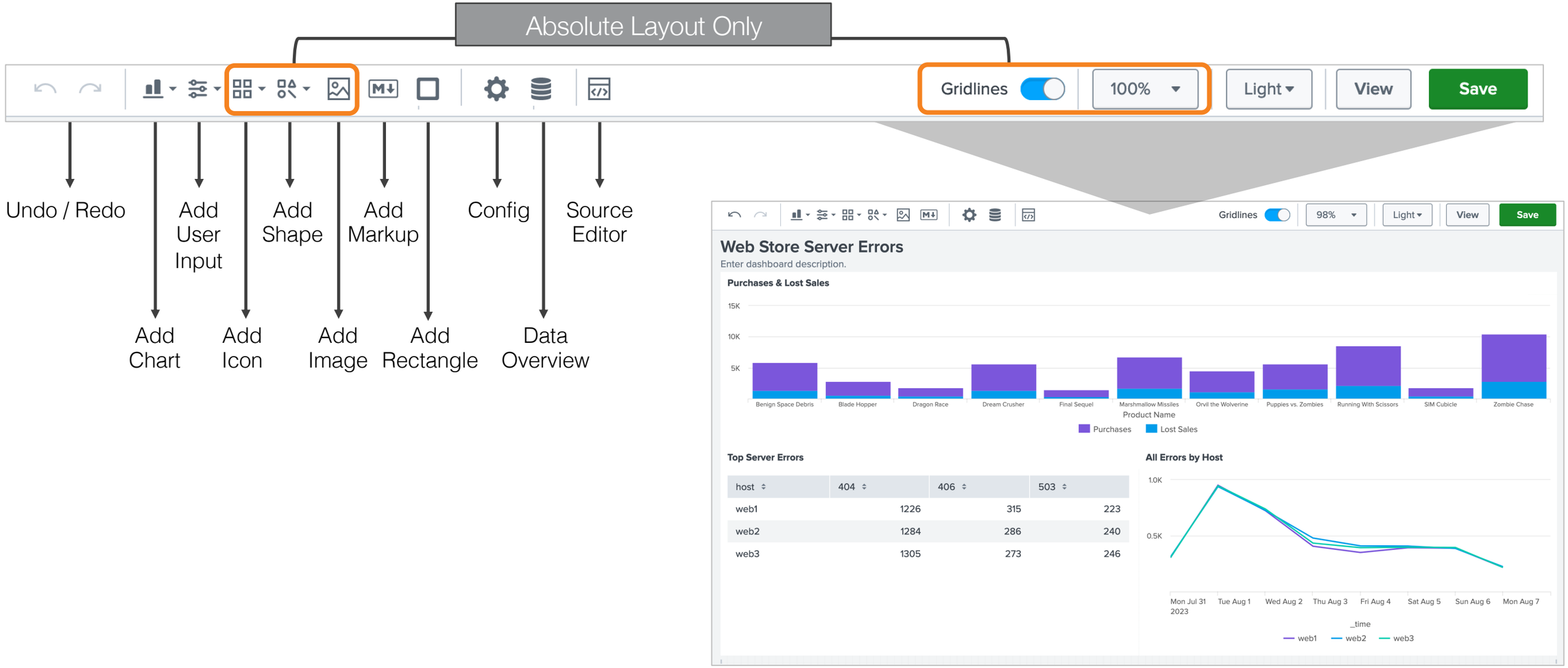
Layouts Compared

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

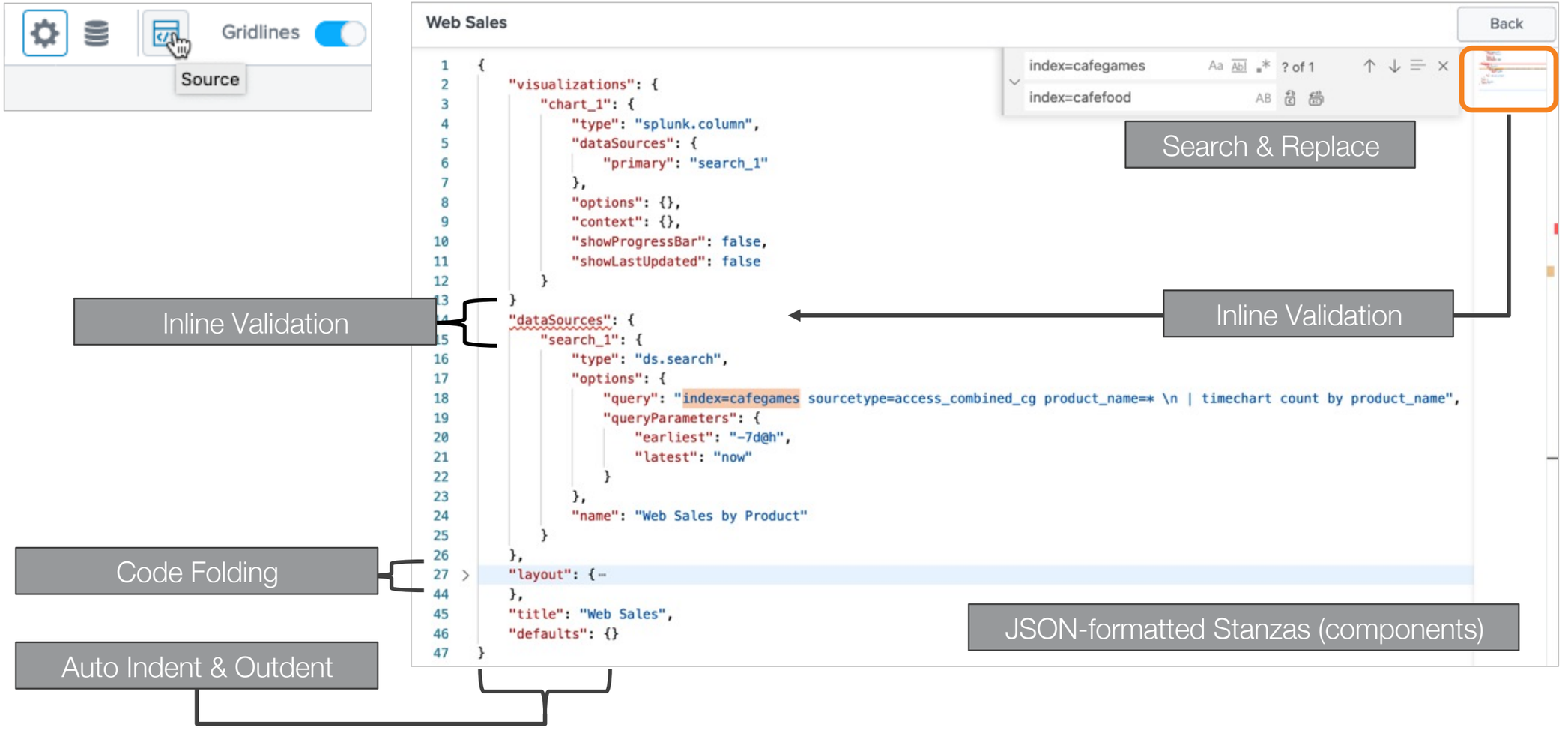
Option	Absolute	Grid
Charts	✓	✓
Customizable Background Color	✓	–
Customizable Canvas size	✓	Customize row height and visualization widths only
Unlimited visualizations on a dashboard	✓	Number per row depends on the width of the visualizations –which can be modified
Shapes: rectangles, lines, and ellipses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

splunk>

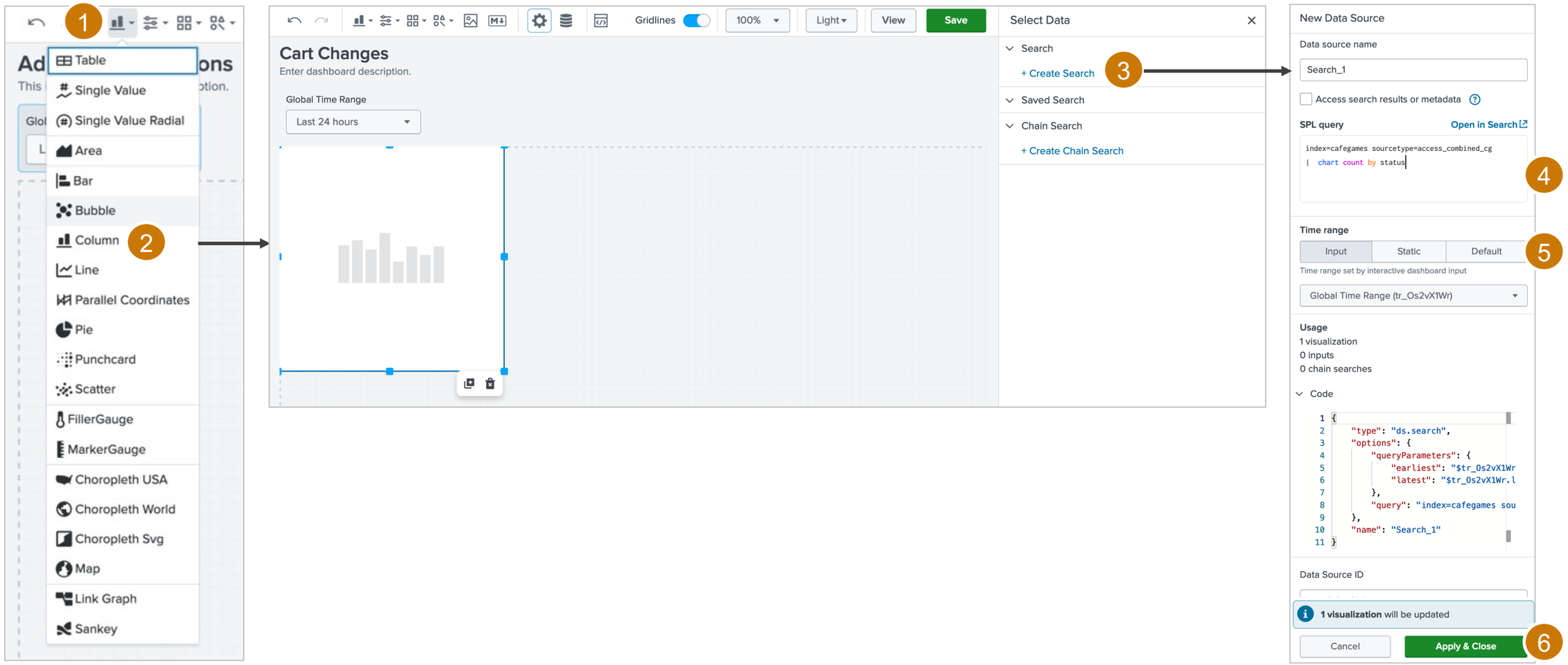
Dashboard Studio – Visual Editor



Dashboard Studio – Source Editor

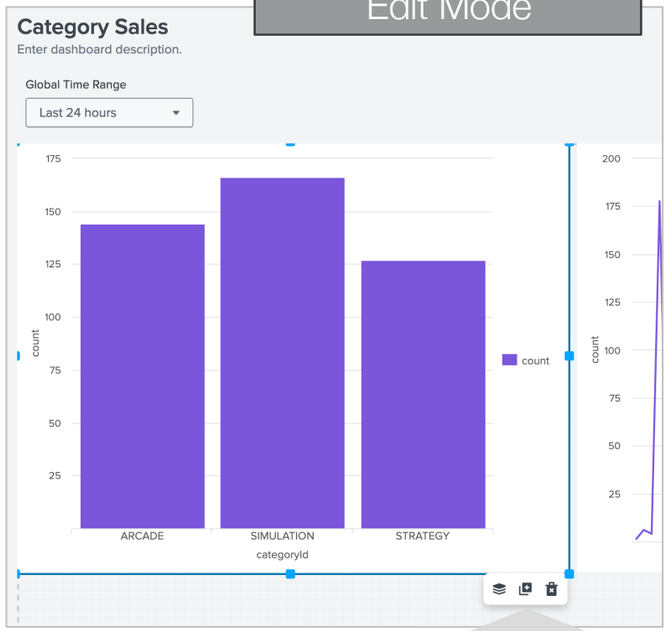


Adding Visualizations



Visualization Action Panel

Edit Mode

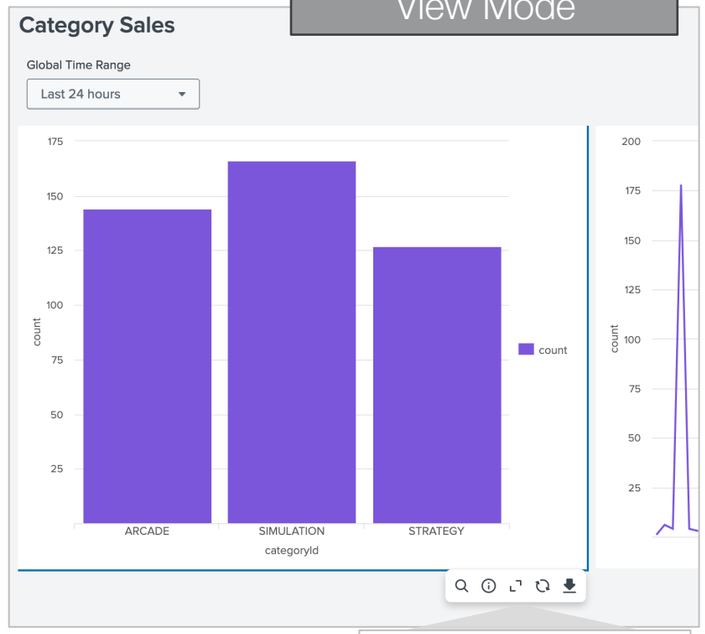


Layer the visualization

Clone the visualization

Delete the visualization

View Mode



Open in search

Inspect the search

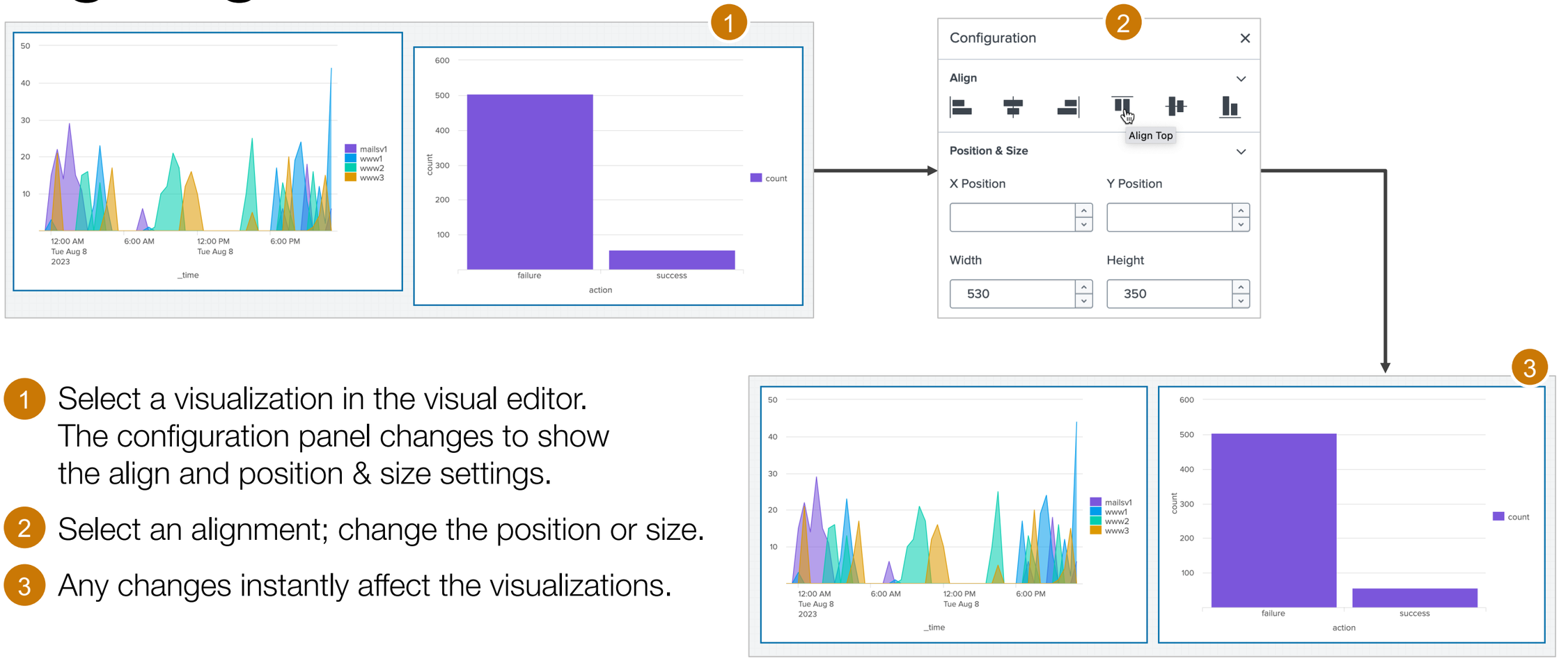
Expand the visualization to full screen mode

Refresh the search driving the visualization

Download the visualization (PNG format)

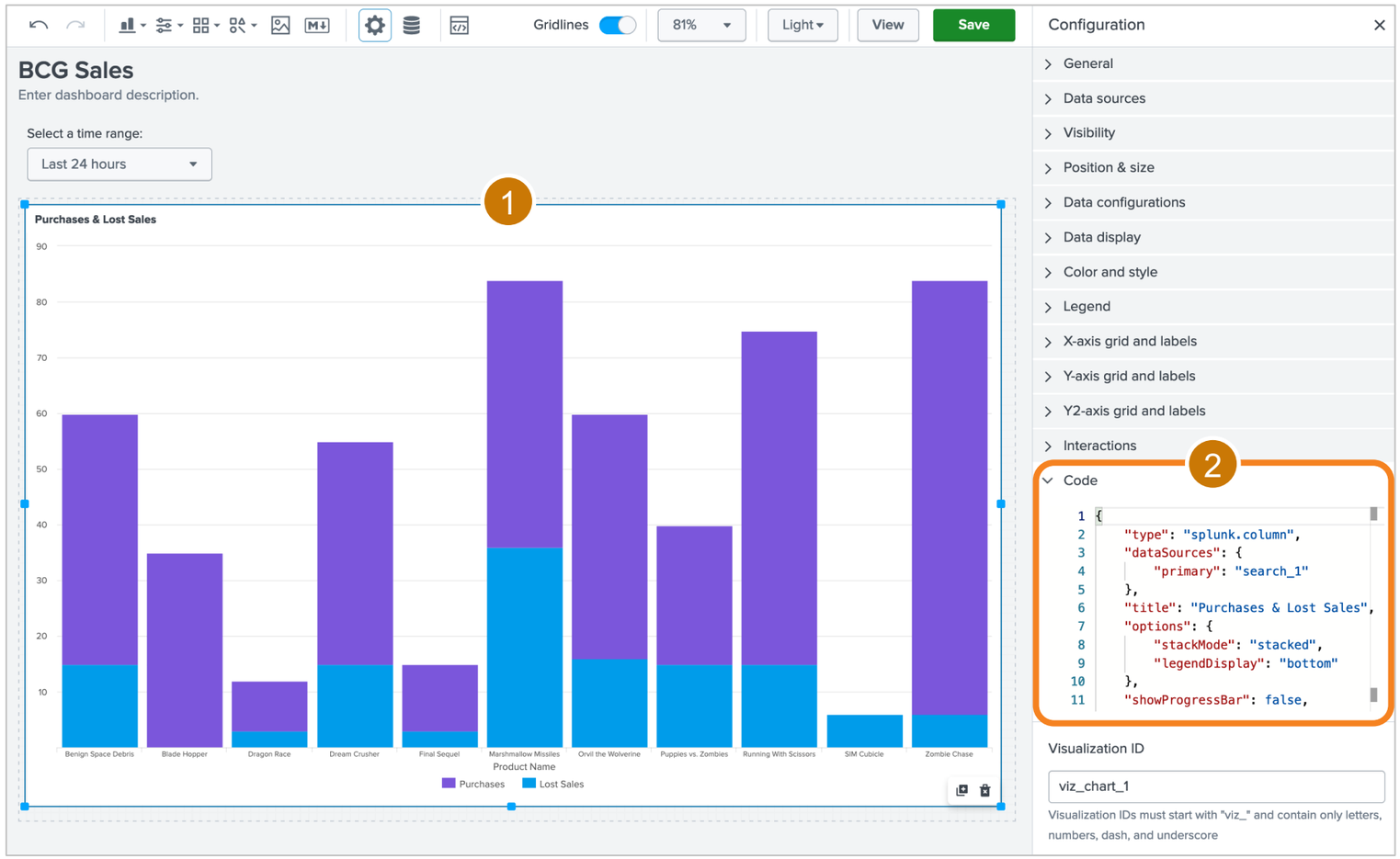
splunk>

Aligning Visualizations



1. Select a visualization in the visual editor. The configuration panel changes to show the align and position & size settings.
2. Select an alignment; change the position or size.
3. Any changes instantly affect the visualizations.

Visual Editor's Code Window

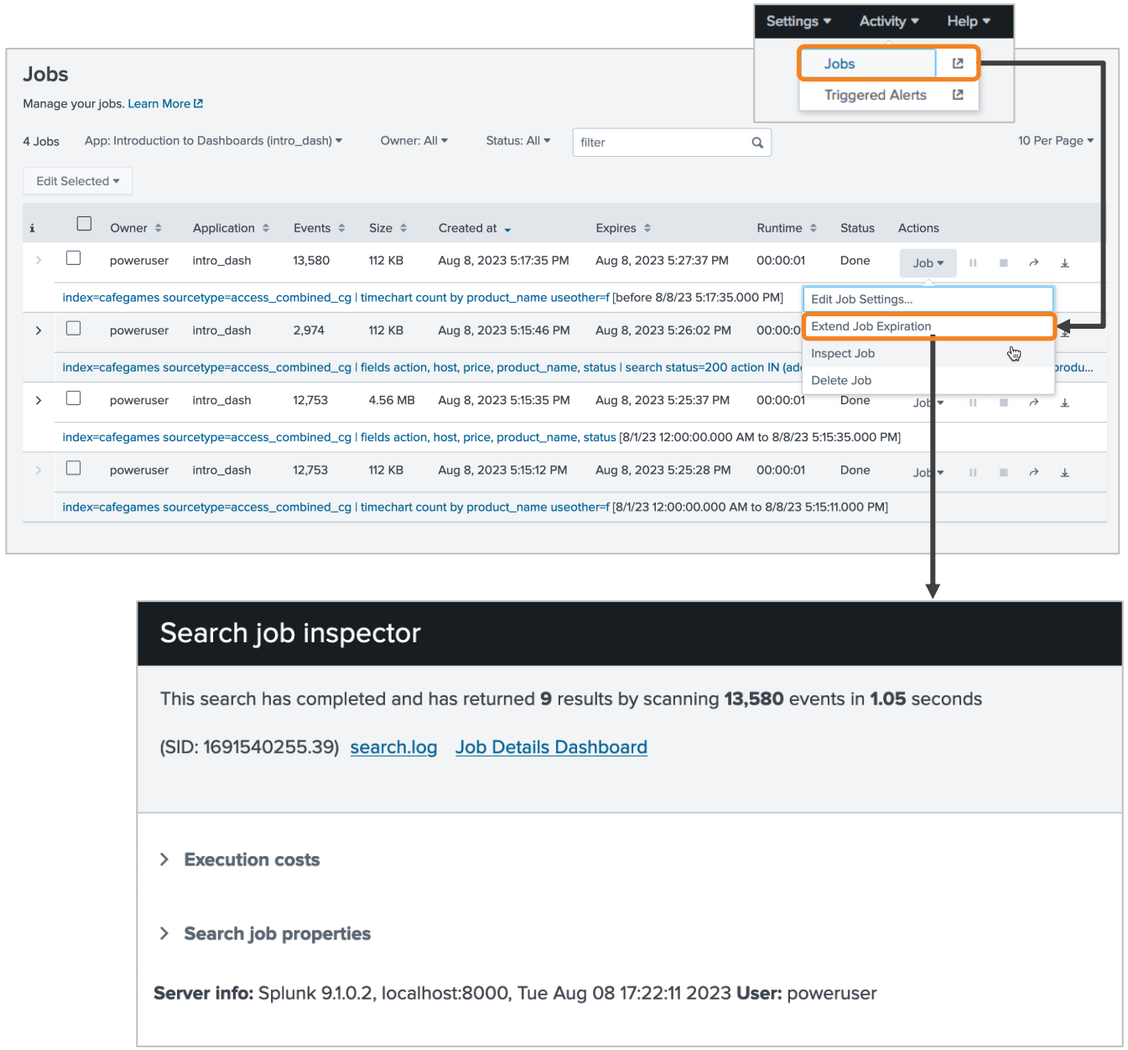


1. Select a visualization or data source in the visual editor
2. Open the Code window in the configuration panel

Any changes instantly affect the visualization or data source selected

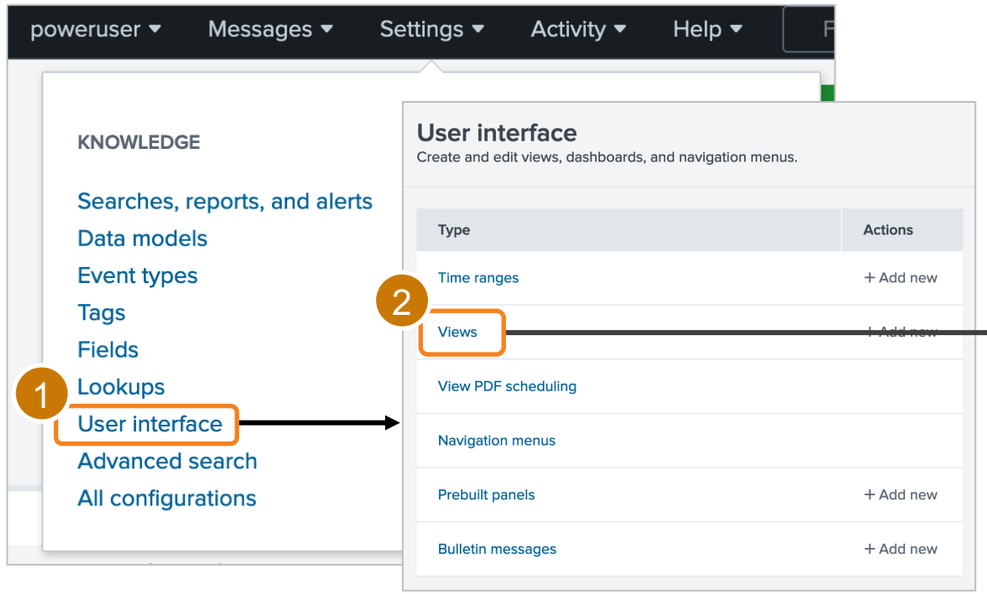
Troubleshooting

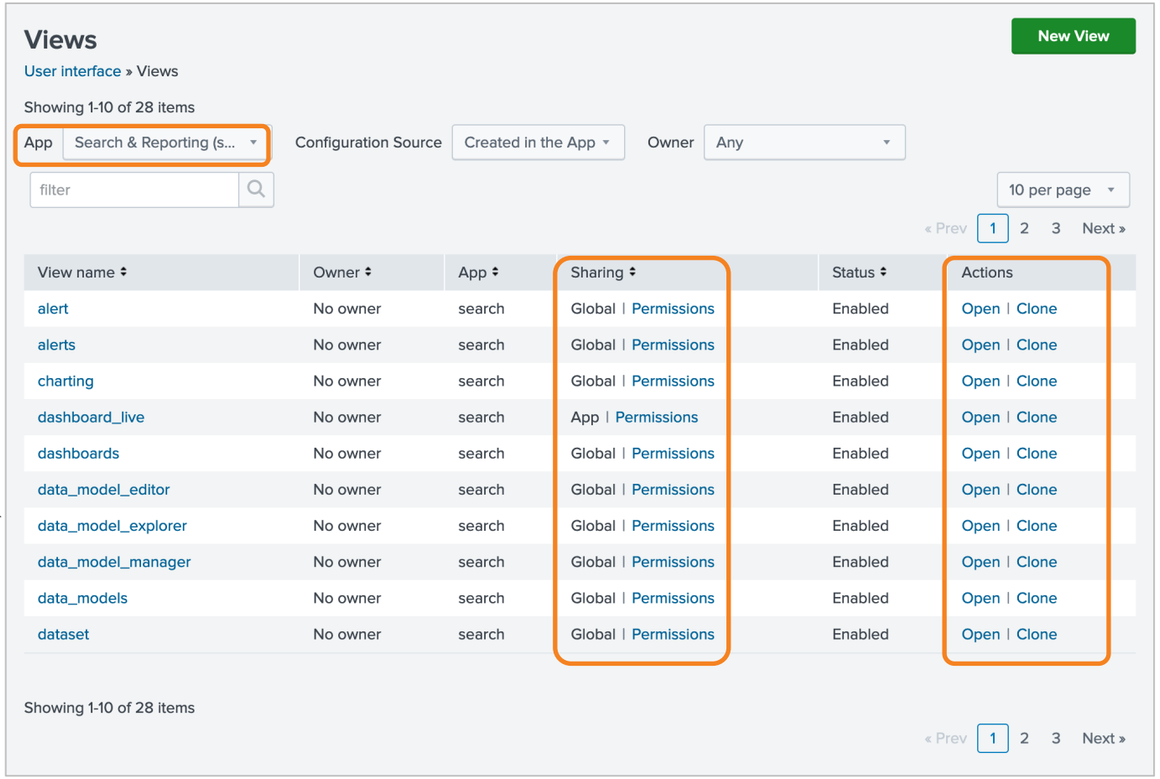
- Look for typos in source code and search queries
- Run a search manually
- Verify tokens are being set and have the expected values
- Use the Job Inspector
  - Check the impact of knowledge object processing
  - Look at debug messages in the Search Job Inspector
  - Debug messages appear after the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



Managing Views

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





splunk>

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

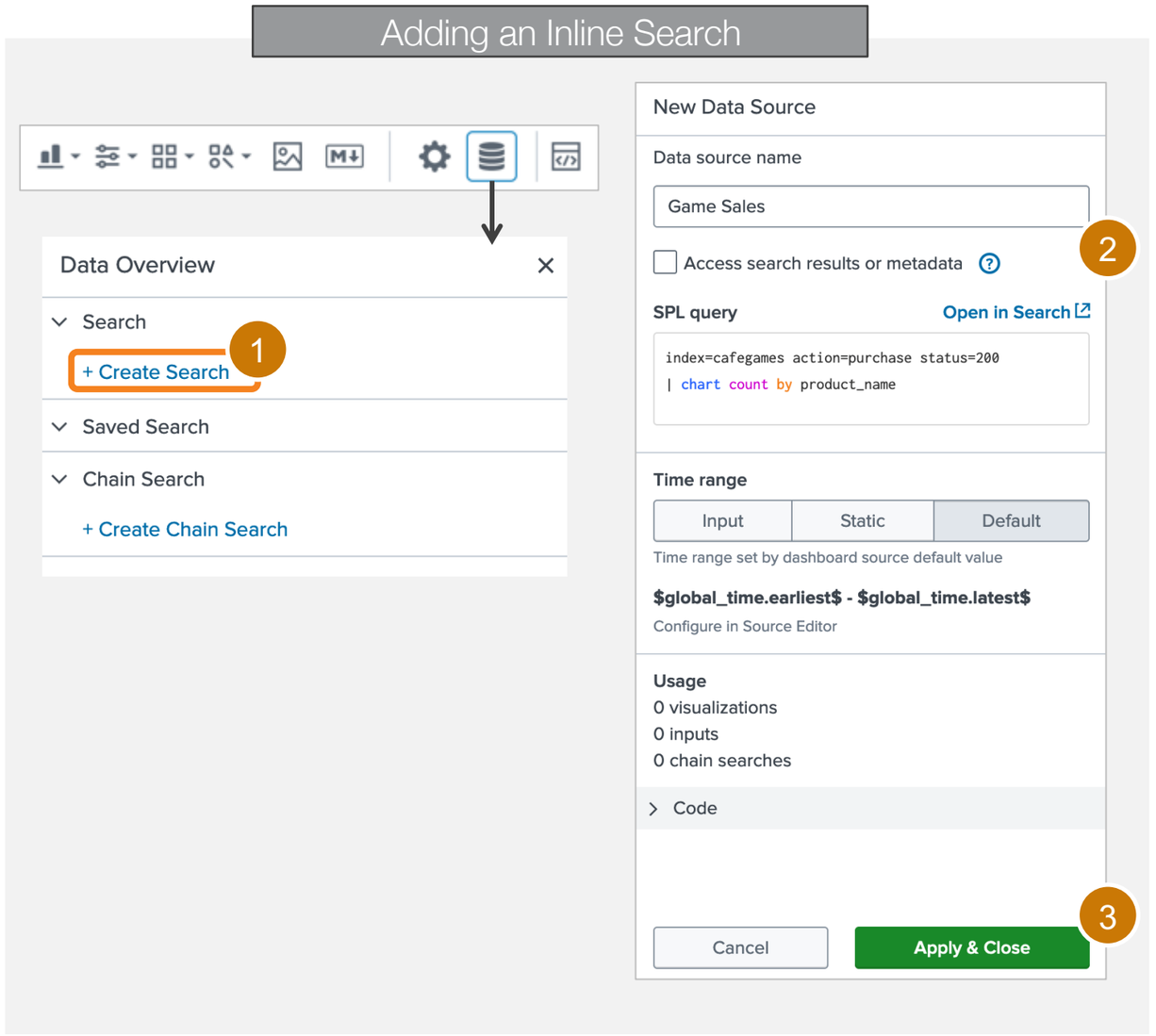
Topic 2: Selecting a Data Source

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



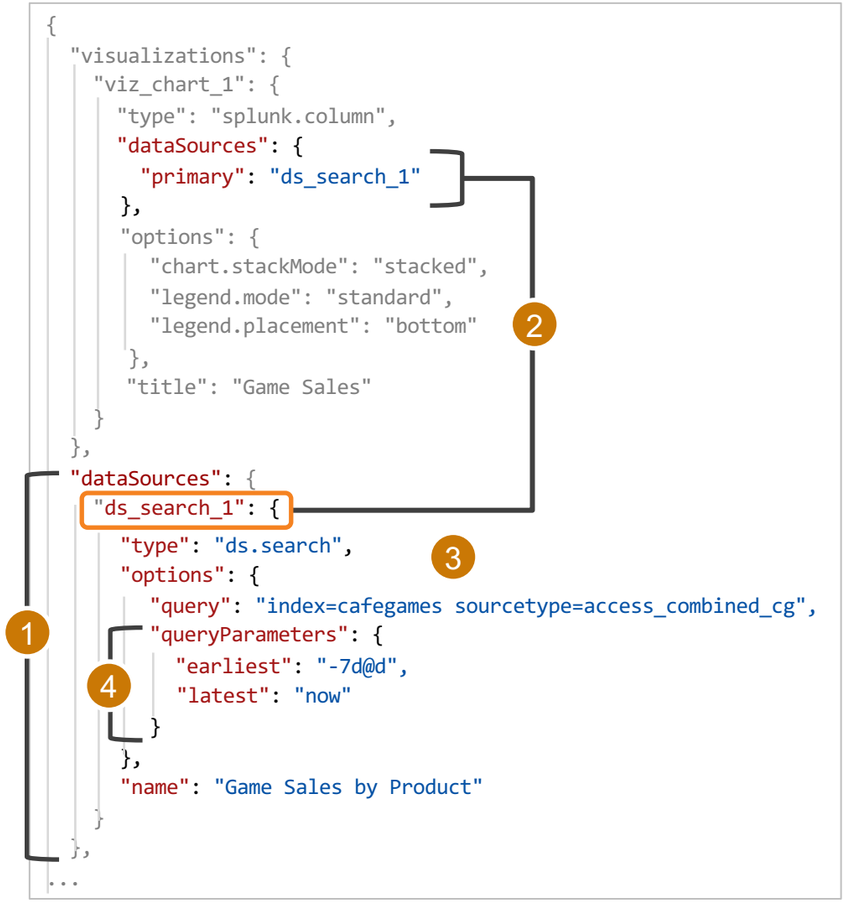
Data Sources – Source Code

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



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:

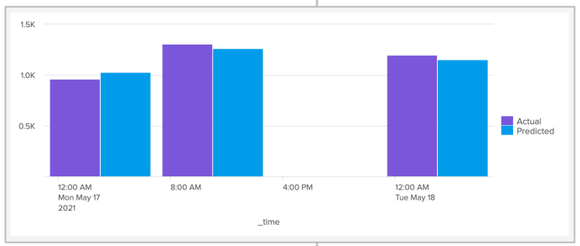
```
"earliest": "-7d@d"
"latest": "now",
```


splunk>

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

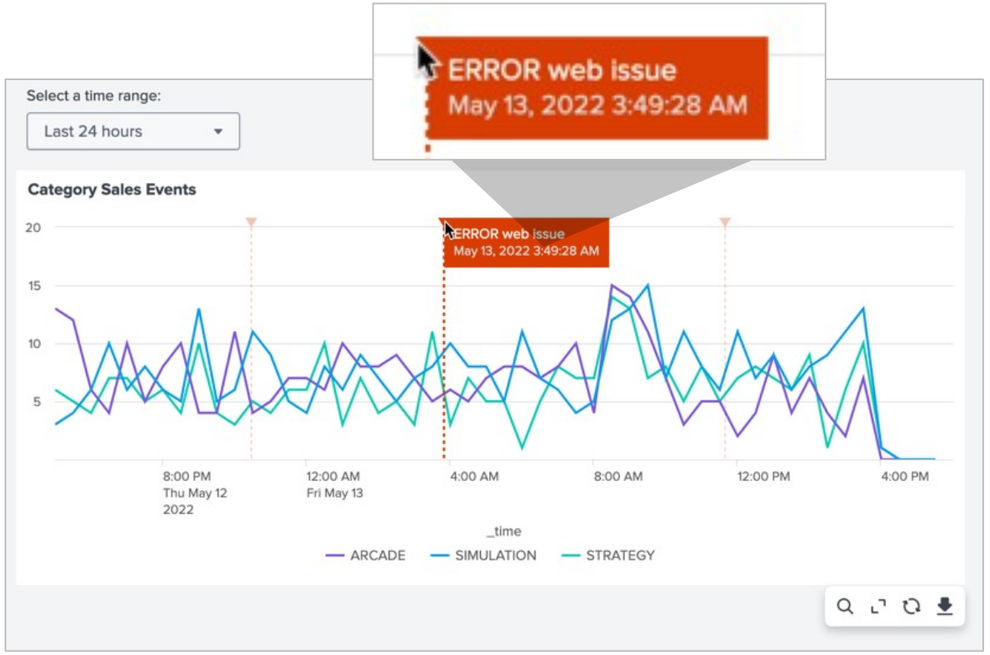
```
...
  "dataSources": {
    "DailyGames1": {                          <- 2
      "name": "Games Played",
      "type": "ds.test",                      <- 3
      "options": {
        "data": {
          "columns": [
            [
              "2022-05-17T06:00:00.000+0000",
              "2022-05-17T14:00:00.000+0000",
              "2022-05-18T06:00:00.000+0000"
            ],
            [
              "966",
              "1307",
              "1200"
            ],
            [
              "1030",
              "1266",
              "1155"
            ]
          ],
          "fields": [
            {
              "name": "_time"
            },
            {
              "name": "Actual"
            },
            {
              "name": "Predicted"
            }
          ]
        }
      }
    }
  },
...
```



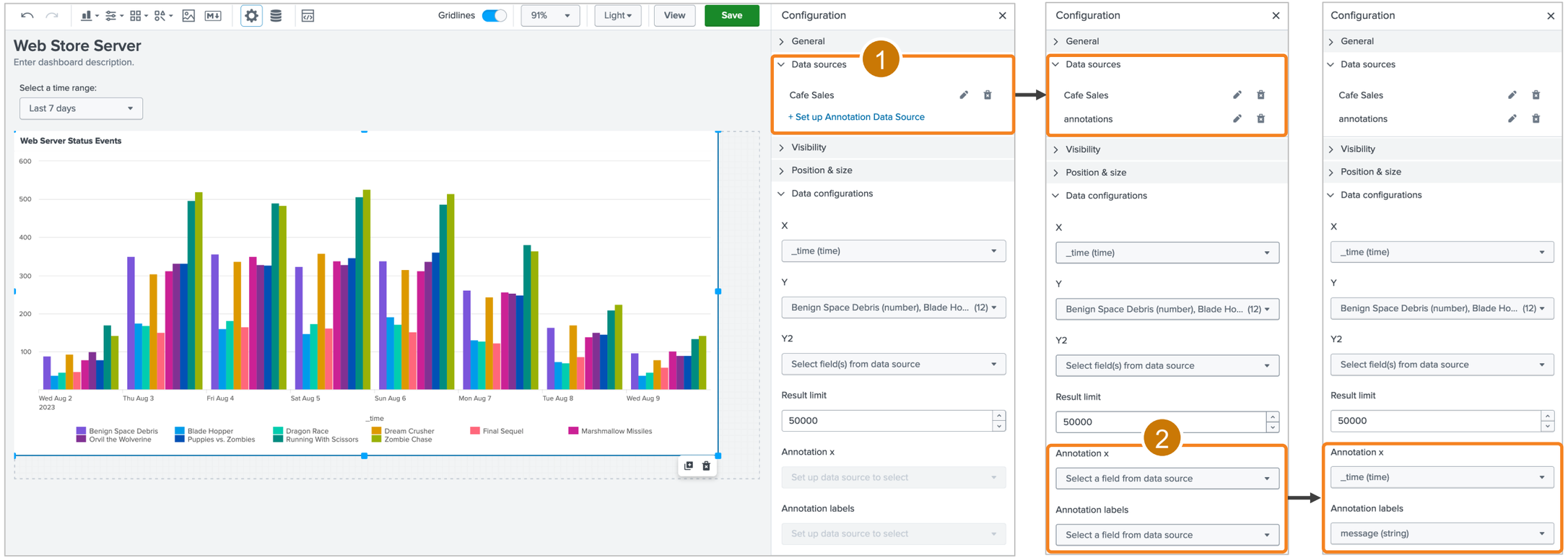
splunk>

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



Primary Search: Cafe Sales

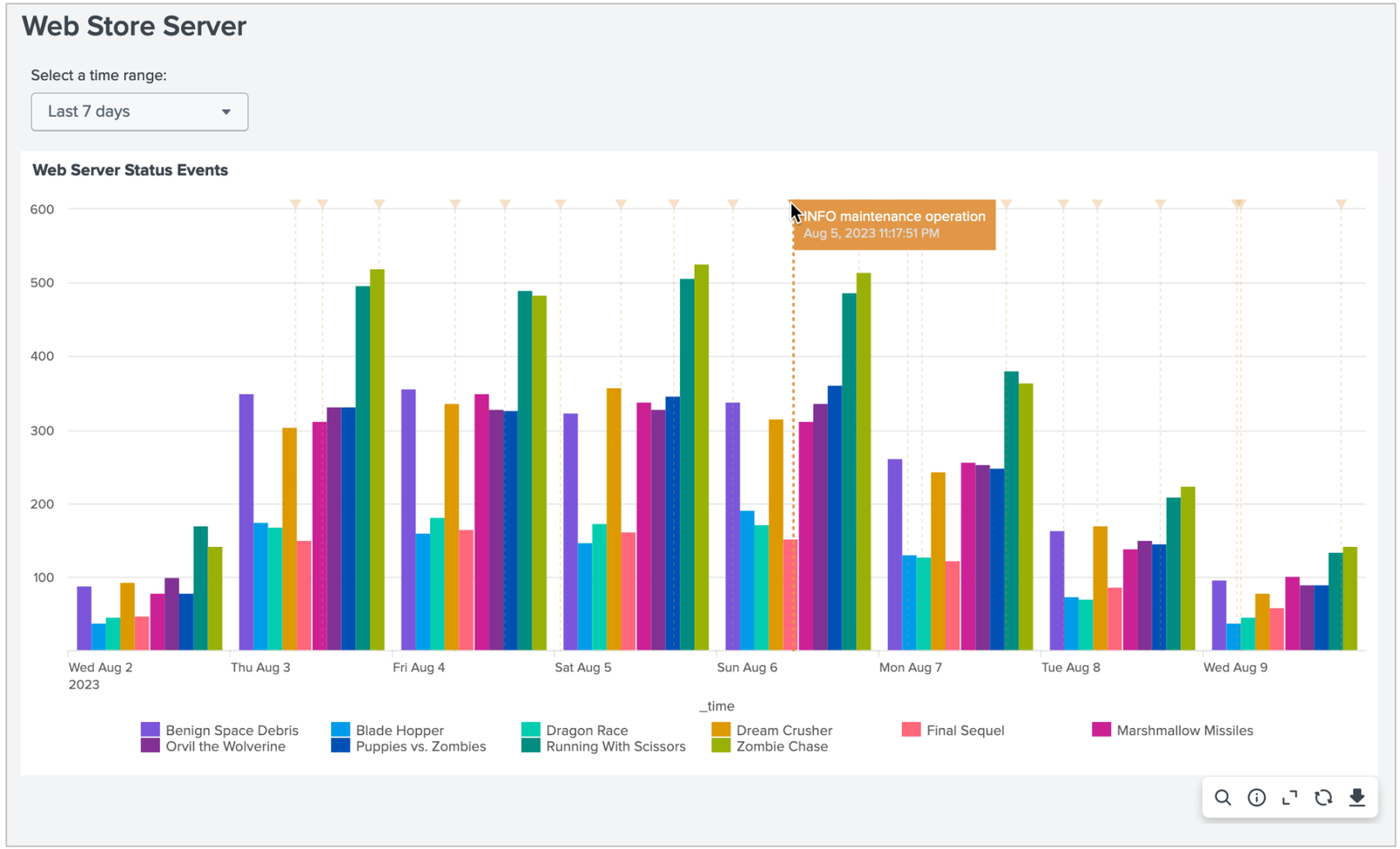
```
index=cafegames sourcetype=access_combined_cg
| timechart count by product_name useother=f
```

Secondary Search: annotations

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


splunk>

Event Annotations – Add a Flag (cont.)



splunk>

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

Secondary Search: annotations

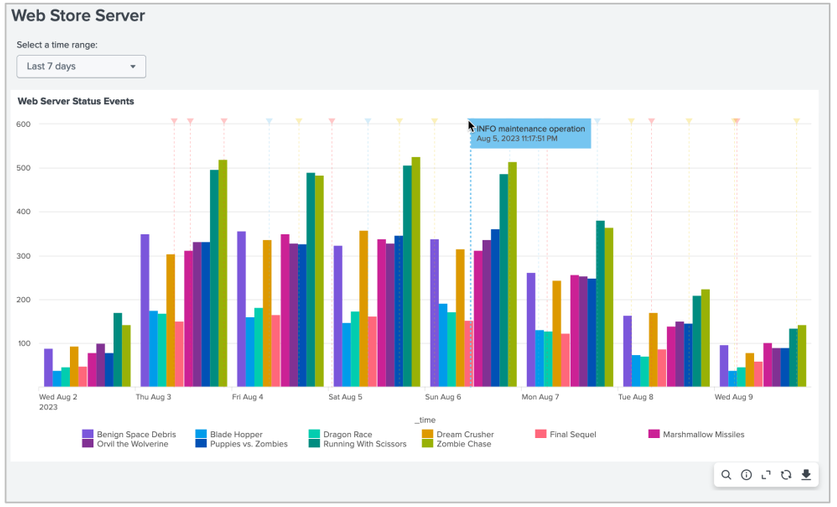
```
index=webapp sourcetype=access_combined
| fields message
| eval annotation_color = case(message="INFO
maintenance operation", "#75C5F0",
message="CRITICAL security issue", "#FF4747",
message="WARNING network issue", "#F3CC17")
```

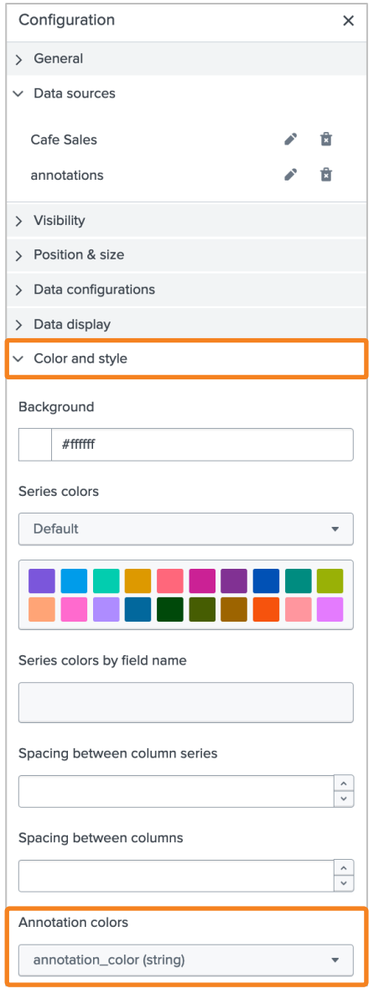
Single Color

```
...| 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")
```





splunk>

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

splunk>

Topic 3: Improving Performance

Topic Objectives

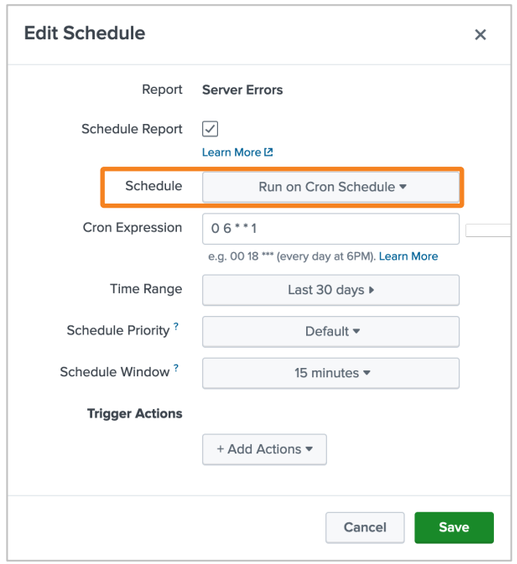
- Name ways to improve dashboard performance
- Create base and chain searches
- Set dashboard defaults

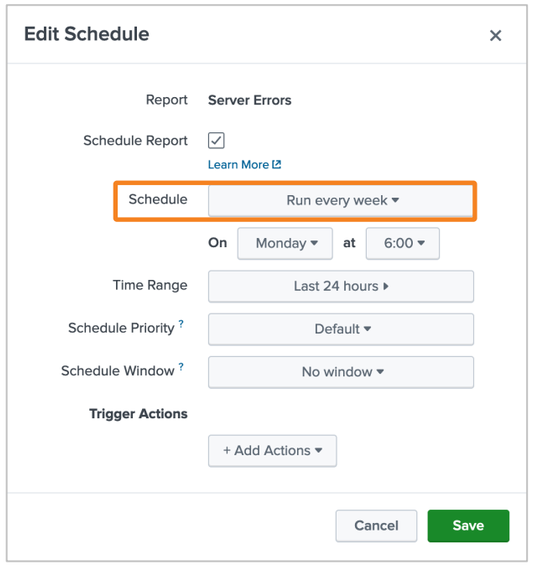
Improving Performance

- 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

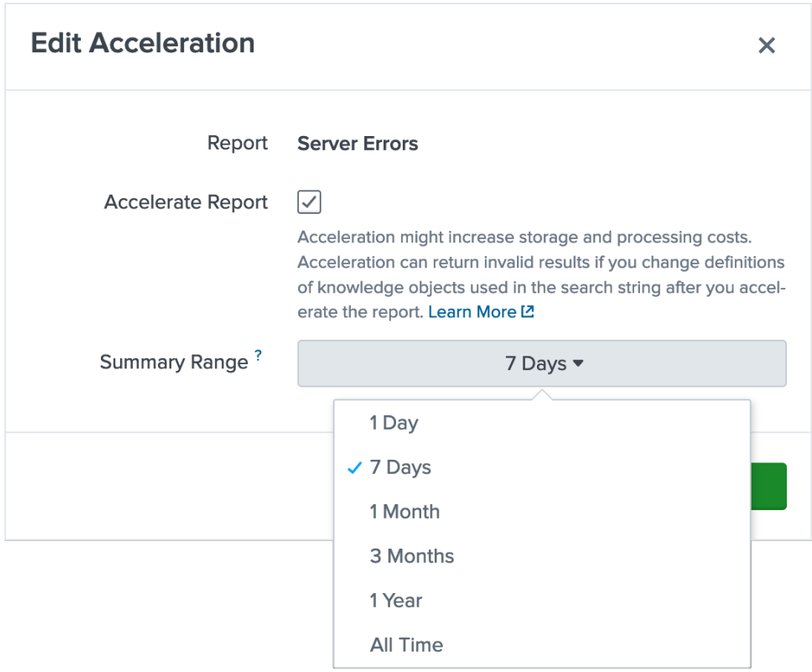




Cron Parameter	Schedule
*/5 * * * *	Every 5 minutes
*/30 * * * *	Every 30 minutes
0 */12 * * *	Every 12 hours, on the hour
*/20 * * * 1-5	Every 20 minutes, Monday through Friday
0 9 1-7 * 1	First Monday of each month, at 9am.

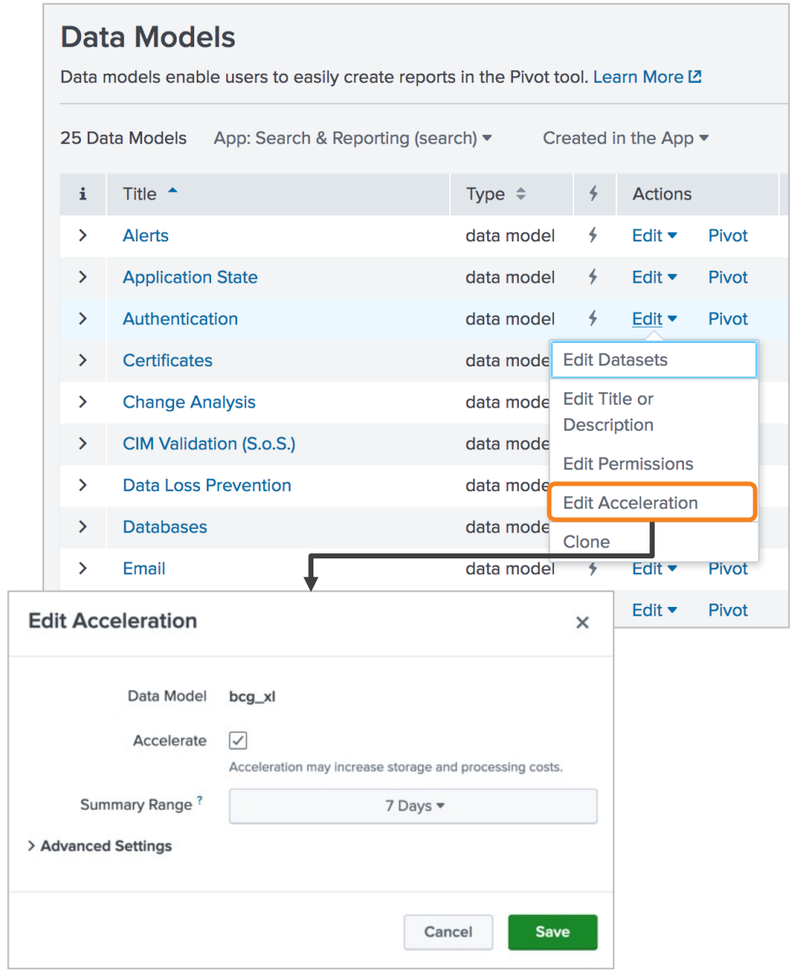
Accelerated Reports

- 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



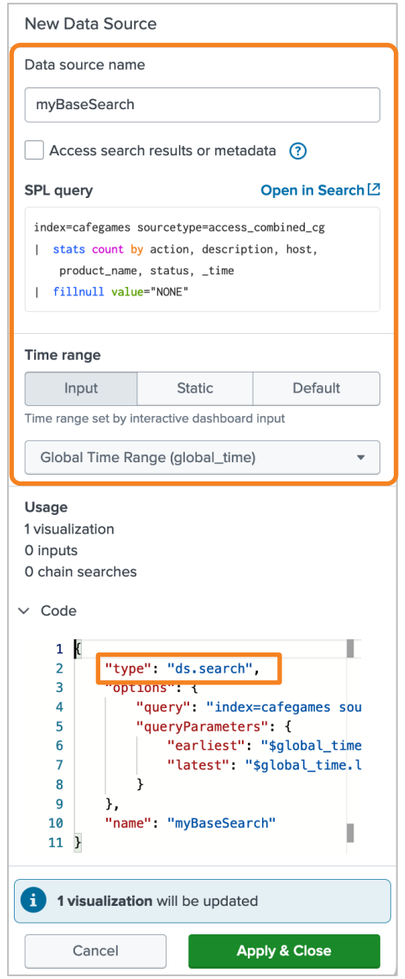
Accelerated Data Models

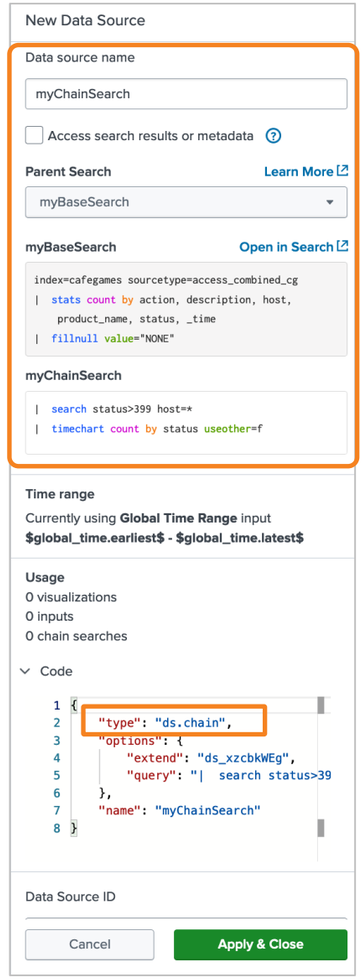
- Accelerates all fields defined in a data model
- Creates time-series index (TSIDX) files
- Updates every five minutes
- Only users with admin permissions can accelerate data models (default)
- Anyone can search using an accelerated data model



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





splunk>

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

Chain 1

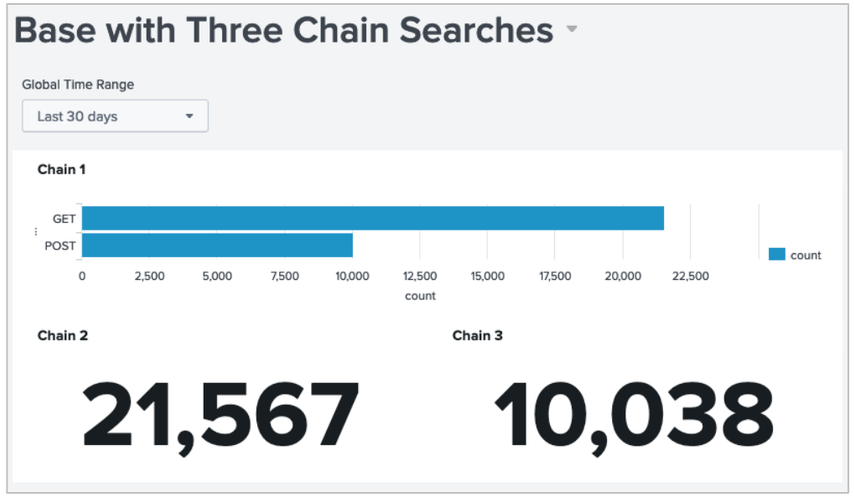
```
| stats sum(count) AS count by method
```

Chain 2

```
| search method=GET
| stats sum(count) AS count by method
```

Chain 3

```
| search method=POST
| stats sum(count) AS count by method
```



splunk>

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"
   }
},
...
```


splunk>

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

- Use to pipe results to chart, stats or timechart
- Use to generate results from TSIDX data
- Perform a basic count of a field or a function on a field
- Specify the filename (object ID) of an accelerated data model
- Specify one or more fields to group results

`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]
```


splunk>

`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() count() distinct_count() estdc()	exactperc<int>() max() median() min() mode()	perc<int>() range() stdev() stdevp()	sum() sumsq() upperperc<int>() var() varp()
Event order functions	earliest()	first()	last()	latest()
Multivalue stats and chart functions	values(x)			

splunk>

`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]
```


splunk>

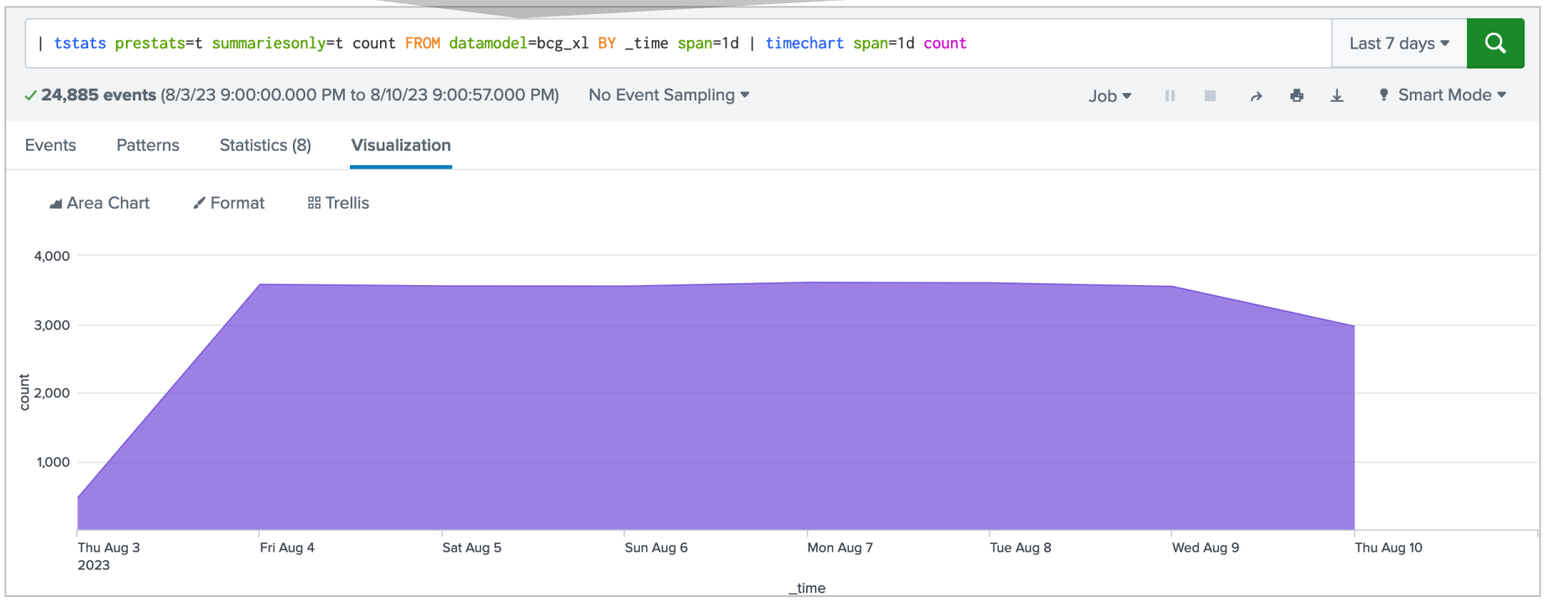
`tstats` Command – Example

`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
```



splunk>

Dashboard Definition – `defaults`

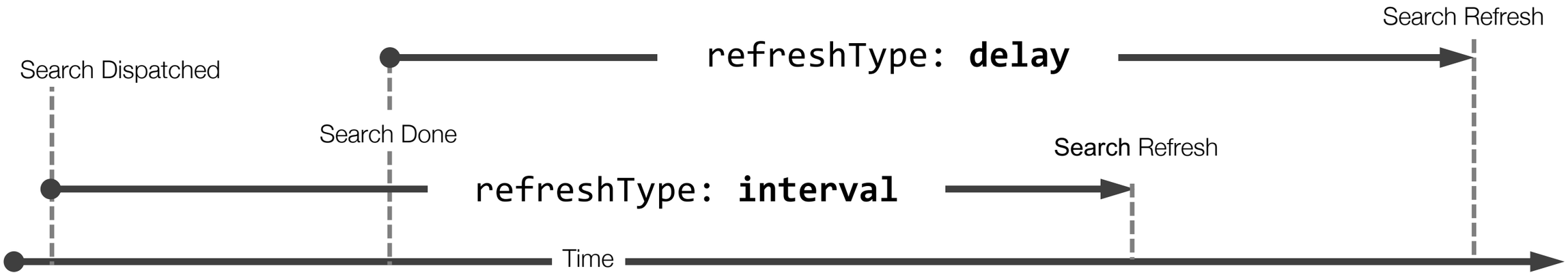
- Can set all data source or visualization options in one place
  - For example, query parameters, refresh, refresh type, show progress bar, and show last updated
- Exceptions
  - Settings at the component level, in the `visualization` or `dataSource` sections, override the same settings in `defaults`

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


splunk>

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
      }
    }
  }
}
```


splunk>

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

splunk>

Documentation

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

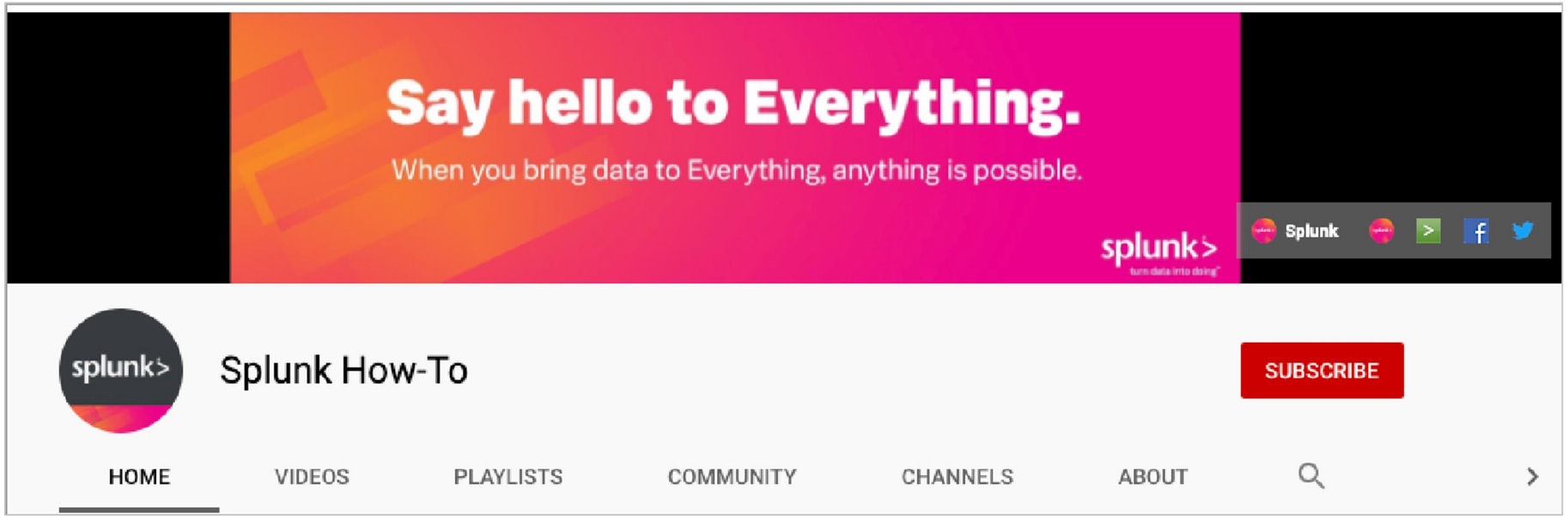
- Topic 3: Improving Performance
  - Set global and local defaults
  - Chain searches together with a base search and chain searches
  - Search Reference – tstats
  - Accelerate Data Models

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

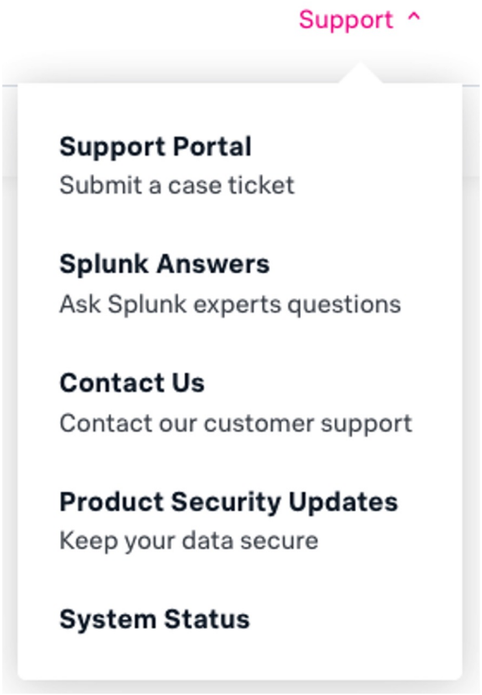
- Check out the Splunk Education How-To channel on YouTube: splk.it/How-To
- Free, short videos on a variety of Splunk topics



splunk>

Support Programs

- Web
  - Documentation: dev.splunk.com and docs.splunk.com
  - Wiki: wiki.splunk.com
- Splunk Lantern: Guidance from Splunk experts
  - 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
- Enterprise, Cloud, ITSI, Security Support
  - Web: 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 *

splunk>

Learning Paths

Knowledge Manager - Recommended Courses

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

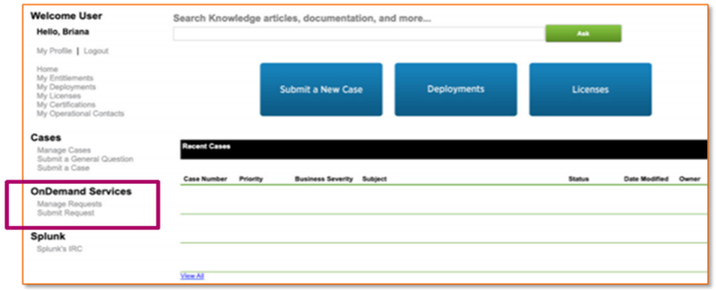
- Introduction to Splunk *
- Using Fields *
- Introduction to Knowledge Objects
- Creating Knowledge Objects
- Creating Field Extractions
- Enriching Data with Lookups
- Data Models
- Introduction to Dashboards
- Dynamic Dashboards
- Creating Maps
- Search Optimization *

splunk>

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!

splunk>

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 OR contact your Customer Success Manager/Advocate or Account Team

Splunk Mobile

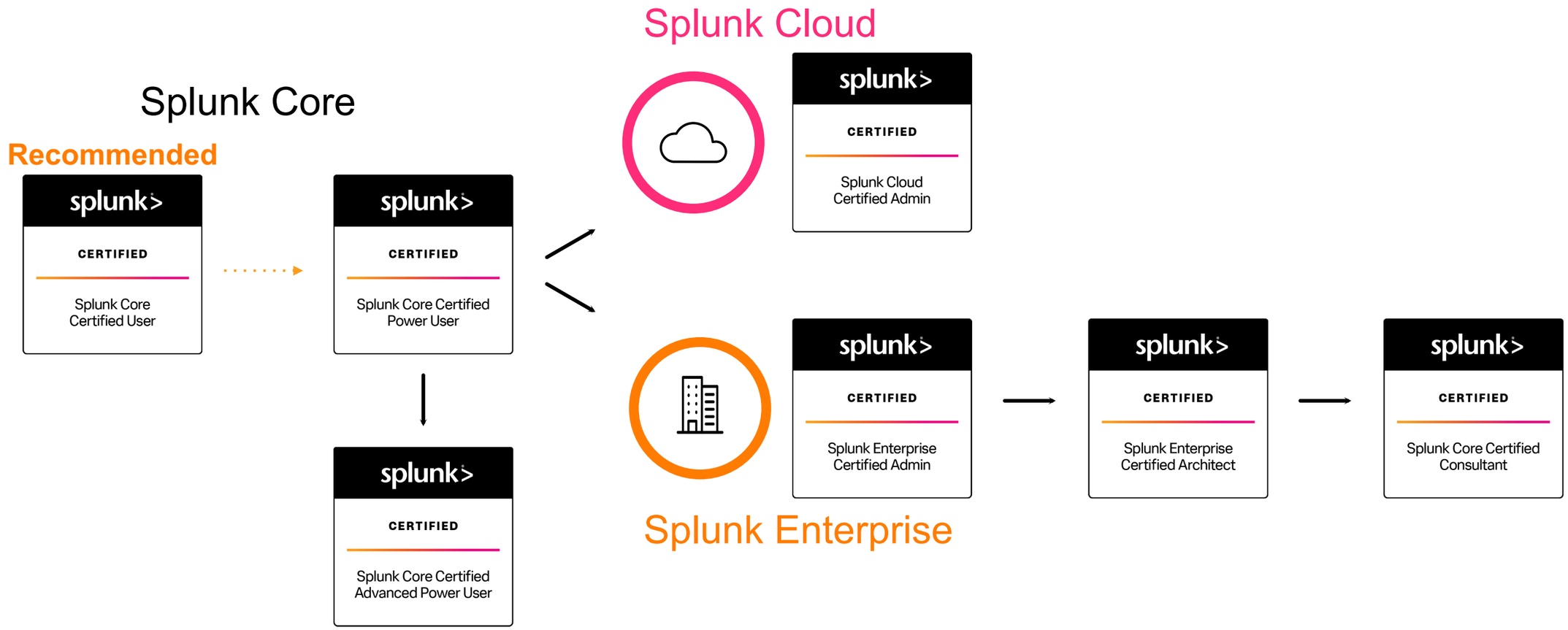
- Free app available to all Splunk Cloud and Splunk Enterprise customers
- Analyze data and receive actionable alerts on-the-go with mobile-friendly dashboards
- iOS and Android
- See the Product Brief

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>

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 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:*

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

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

splunk>

Thank You

splunk> turn data into doing™