Dynamic Dashboards

splunk>

Before Taking This Course

- To be successful, students must have a working understanding of these courses:
  - Intro to Splunk
  - Introduction to Dashboards

Course Objectives

- Define token syntax
- Create user inputs
- Create dynamic inputs
- Build cascading inputs
- Create a dynamic drilldown
- Set tokens
- Use dynamic coloring

Course Outline

- Using Tokens
- Adding Inputs
- Using Drilldowns
- Dynamic Visualizations

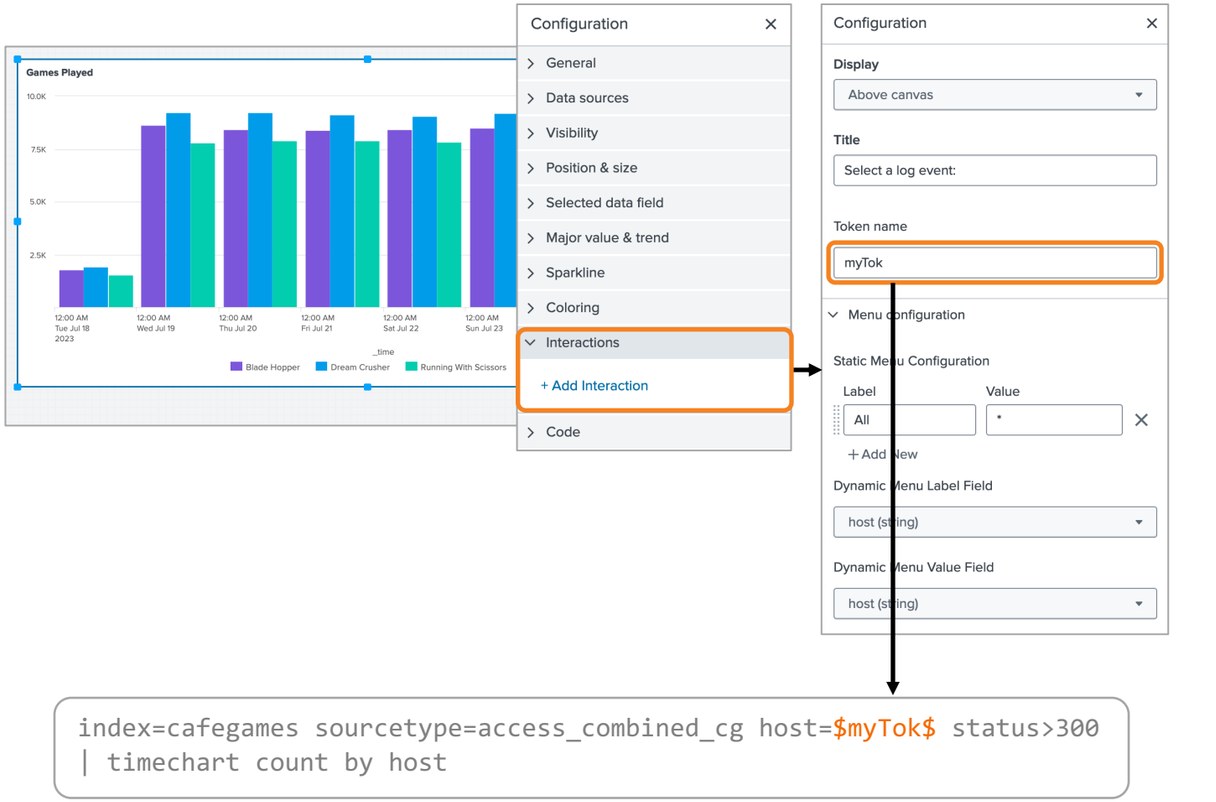
Topic 1: Using Tokens

Topic Objectives

- Define dashboard token syntax
- Describe types of predefined tokens
- Use token filters

Dashboard Tokens

- Syntax
  - Use $...$ delimiters to access the value of a token
  - Types
    - User defined
    - Predefined
      - Search, environment, inputs, drilldowns, maps, and visualizations
    - Default token



Predefined Tokens – Search

- Set tokens from search job metadata or search results
  - Embed search-related information in other searches or visualizations

Search Results	
`$search name:result.<field_name>$`	Returns the first value for the specified field name from the first result in the search.

Search Job Metadata	
`$search name:job.done$`	Is the job is done? True or false.
`$search name:job.failed$`	Did the job fail? True or false.
`$search name:job.hasResults$`	Did the search return results? True or false.
`$search name:job.inProgress$`	Is the job in progress? True or false.
`$search name:job.isRealTimeSearch$`	Does the job use a real time search? True or false.
`$search name:job.lastUpdated$`	Returns a timestamp of the last update.
`$search name:job.messages$`	List of error and debug messages.
`$search name:job.percentComplete$`	The job's percentage of completeness. Numerical value.
`$search name:job.queued$`	Is the job is queued? True or false.
`$search name:job.resultCount$`	Number of results returned. Returns an integer.
`$search name:job.sid$`	Returns the search job ID.
`$search name:job.startTime$`	Time a search job started. Returns date and time.
`$search name:job.status$`	What is the status? Done, queued, in progress, or failed.
`$search name:result.<field>$`	Returns the first result for the specified field.

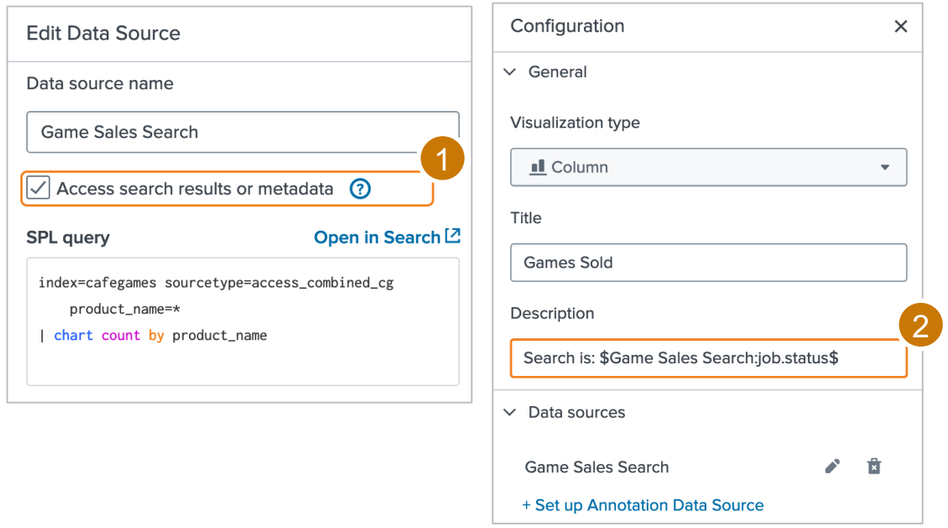
splunk>

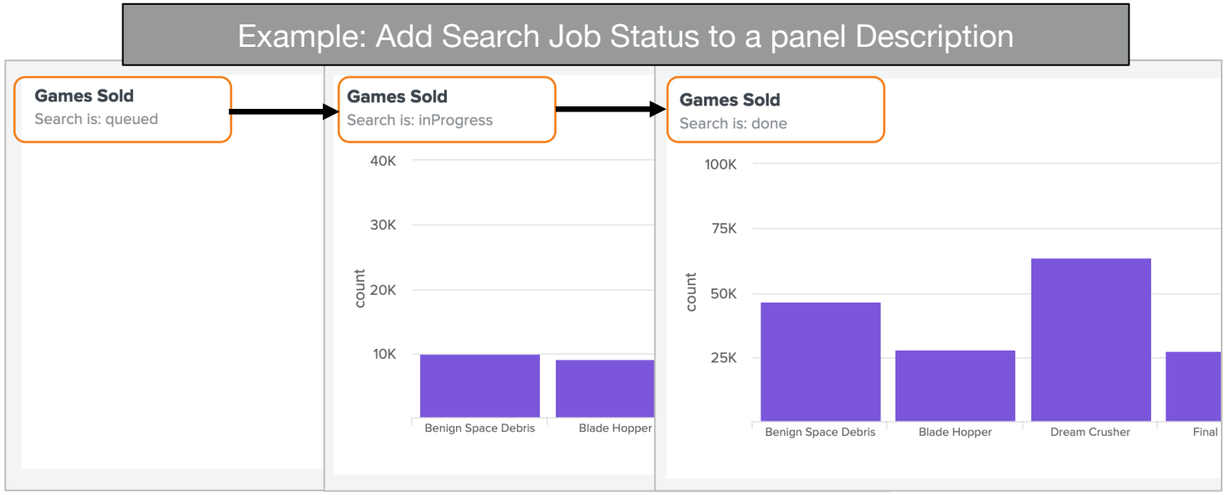
Predefined Tokens – Search Example 1

- Search job metadata
  - Search job status

    Syntax: $Search Name:job.status$

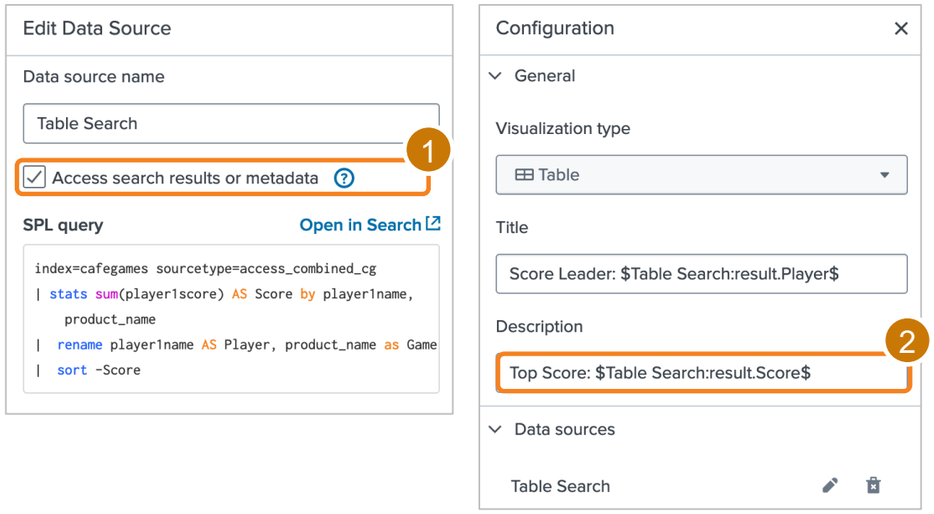
    Returns: queued, inProgress, done, or failed





Predefined Tokens – Search Example 2

- Search results
  - Syntax: `$Search Name:result.<field>$`
  - Returns: first value from the first result of the named field



Example: Add Score Leader and Top Score to Panel

Score Leader - tcrosioag
Top Score: 1980

#	Player	Game	Score
1	tcrosioag	Marshmallow Missiles	1980
2	ipassod	Benign Space Debris	1859
3	mpledgerg	Blade Hopper	1825
4	candraultpf	Orvil the Wolverine	1823
5	mnottram7x	Marshmallow Missiles	1820

< Prev 1 2 3 4 5 ... Next >

Predefined Tokens – Environment Example

- Capture user details and Splunk platform instance and embed on dashboards:
  - Titles, labels, or text
  - Search queries
- Can read environment token data but not write environment token data

1. `$env:user$`	**Current user's username:** supportuser
2. `$env:user_realname$`	**Current user's full name:** Administrator
3. `$env:user_email$`	**Current user's email address:** changeme@example.com
4. `$env:app$`	**Current app context:** dynamic_dash
5. `$env:locale$`	**Current locale:** en-US
6. `$env:page$`	**Current open page:** environment_token_example
7. `$env:product$`	**Current instance's product type:** enterprise
8. `$env:version$`	**Current instance's product version:** 9.0.0
9. `$env:is_cloud$`	**Current instance is Splunk Cloud:** $env:is_cloud$
10. `$env:is_enterprise$`	**Current instance is Splunk Enterprise:** true
11. `$env:is_lite_free$`	**Current instance is using a Splunk Light free license:** $env:is_lite_free$
12. `$env:is_free$`	**Current instance is using a Splunk Splunk Enterprise free license:** $env:is_free$

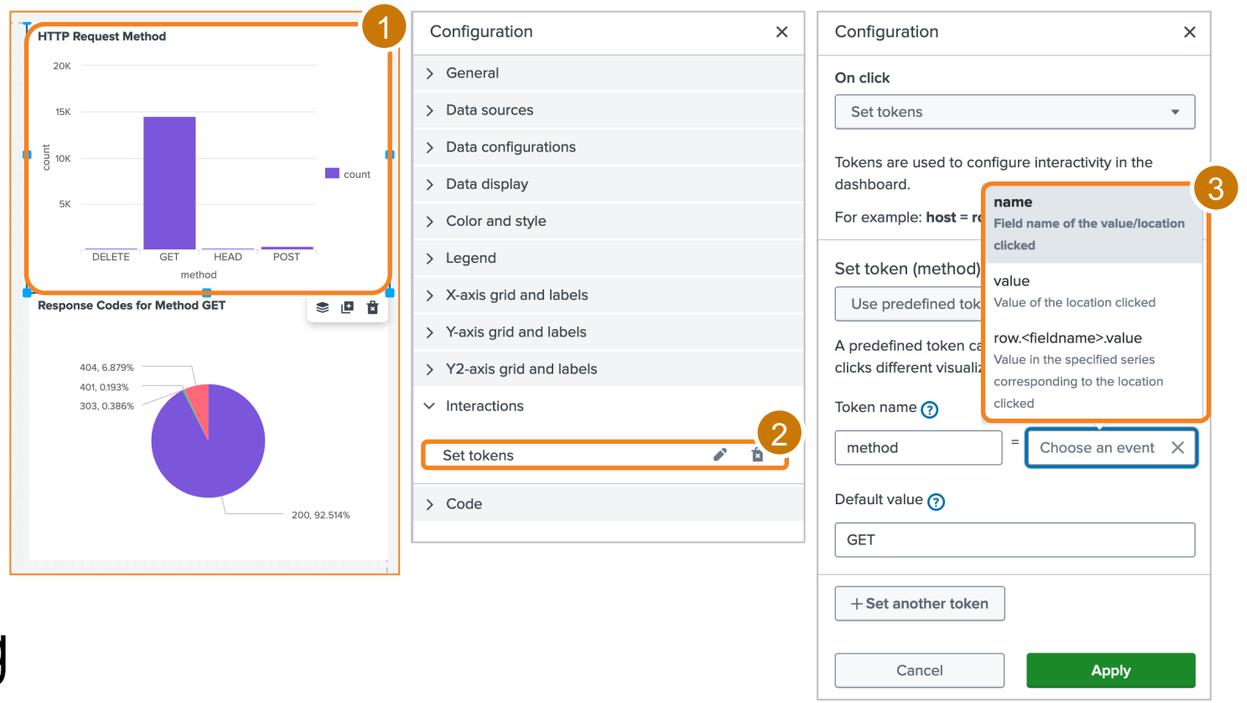
These tokens are only set only if 'true'

splunk>

Predefined Tokens – Visualizations

- Set tokens and capture values from a visualization click
- Use the token elsewhere in the dashboard
- Three predefined tokens:
  - `name`
  - `value`
  - `row.<fieldname>.value`
- Captured values vary according to visualization type

Example: Set a token to capture the HTTP Request Method



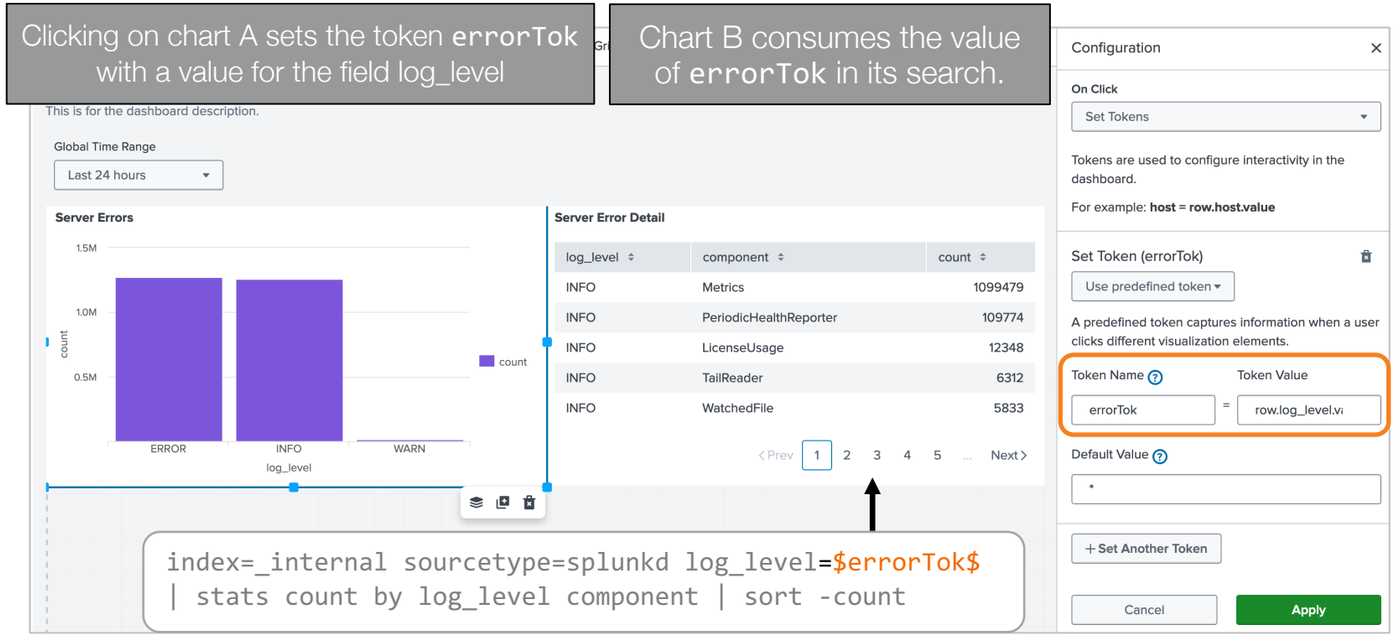
splunk>

Default Token

Used when there is no other token value

Clicking on chart A sets the token **errorTok** with a value for the field log_level

Chart B consumes the value of **errorTok** in its search.



The default value for **errorTok**, the wildcard asterisk (*), is stored as text in the dashboard source code, in the defaults section

```
...
  "defaults": {
    "dataSources": {
      "ds.search":{
        "options": {
          "queryParameters": {
            "latest": "$global_time.latest$",
            "earliest": "$global_time.earliest$"
          }
        }
      }
    },
    "tokens": {
      "defaults": {
        "errorTok": {
          "value": "*"
        }
      }
    }
  },
...
```


splunk>

Token Filters

Token filters ensure that you correctly capture a token's value

Token Filter	Description
`$token_name\|s$`	Wrap value in quotes
`$token_name\|h$`	Escape any HTML in value
`$token_name\|u$`	Encode URL values
`$token_name\|n$`	No encode
`$$token_name$$`	Escape the $ token delimiter character

splunk>

Lab Exercise 1 – Using Tokens

- **Description:** Create a dashboard, add a chart, and search token.
- **Duration:** 10 minutes
- **Tasks:**
  - Create a dashboard
  - Add markdown text
  - Add a chart
  - Add predefined tokens

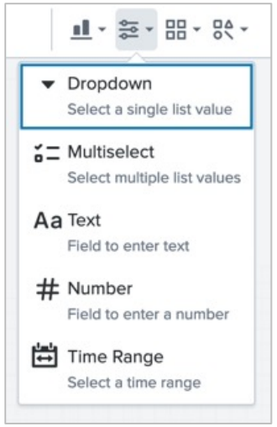
Topic 2: Adding Inputs

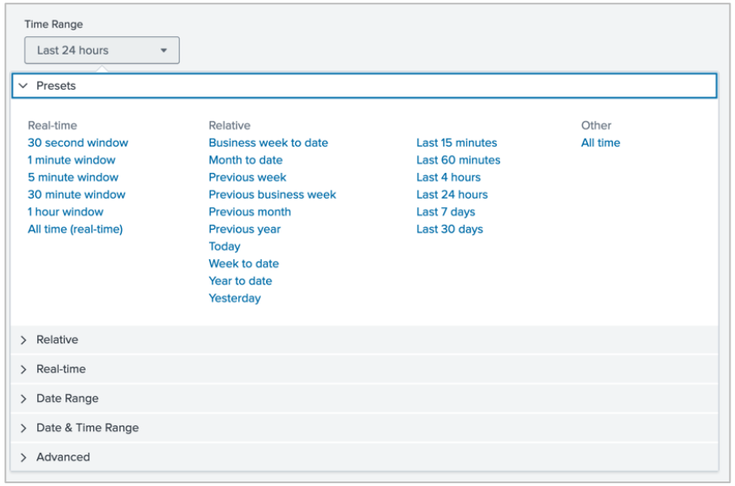
Topic Objectives

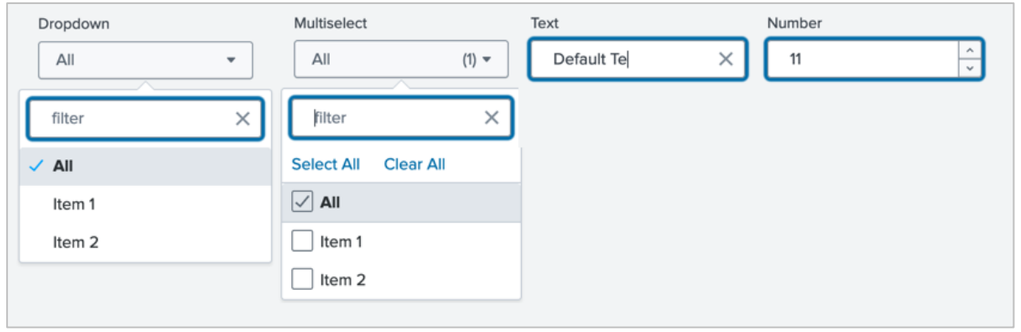
- Name the types of inputs
- Create a dynamic input
- Create cascading inputs

Inputs

- Types: dropdown, multiselect, text, number, and time range
- Input tokens
  - Automatically generated
  - Customizable
- Visualization editor
  - Customize token name
  - Add static values
  - Specify default values
  - Define the data source
- Source editor
  - Configure when input values populate: Page load, input change, Submit button clicked



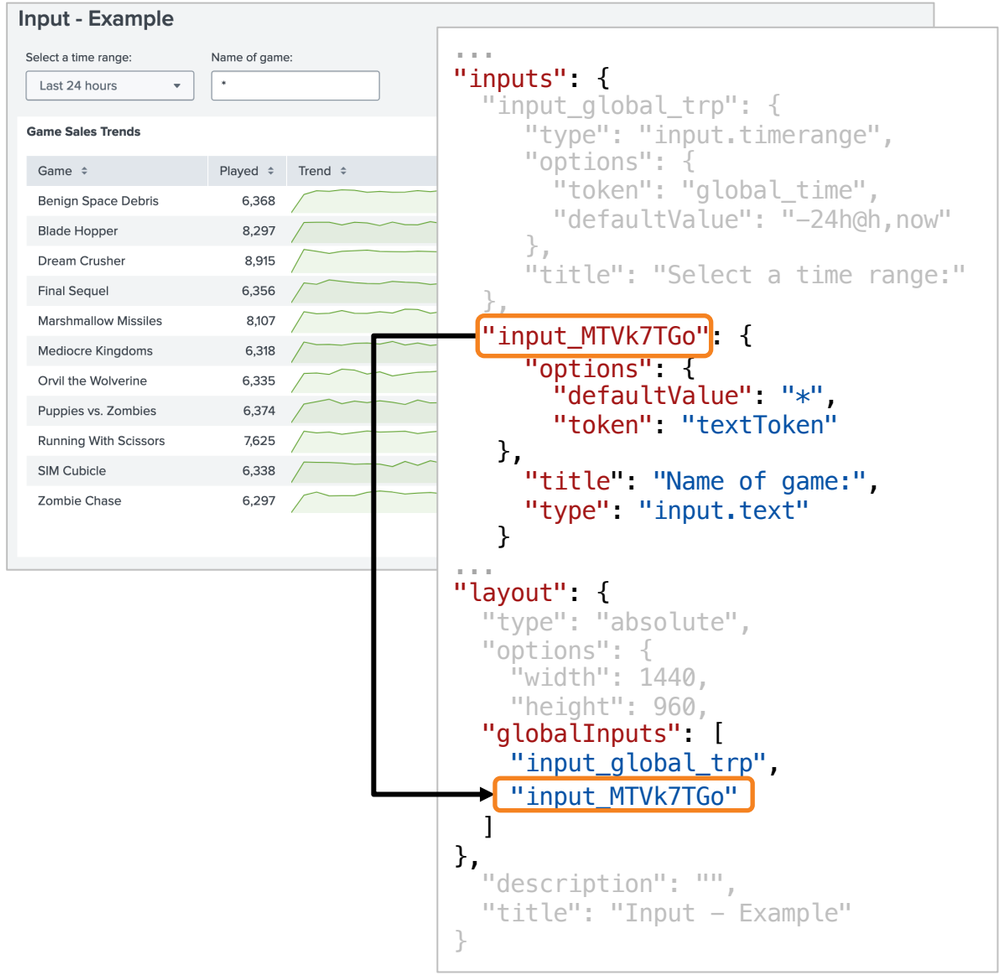




splunk>

Adding Inputs

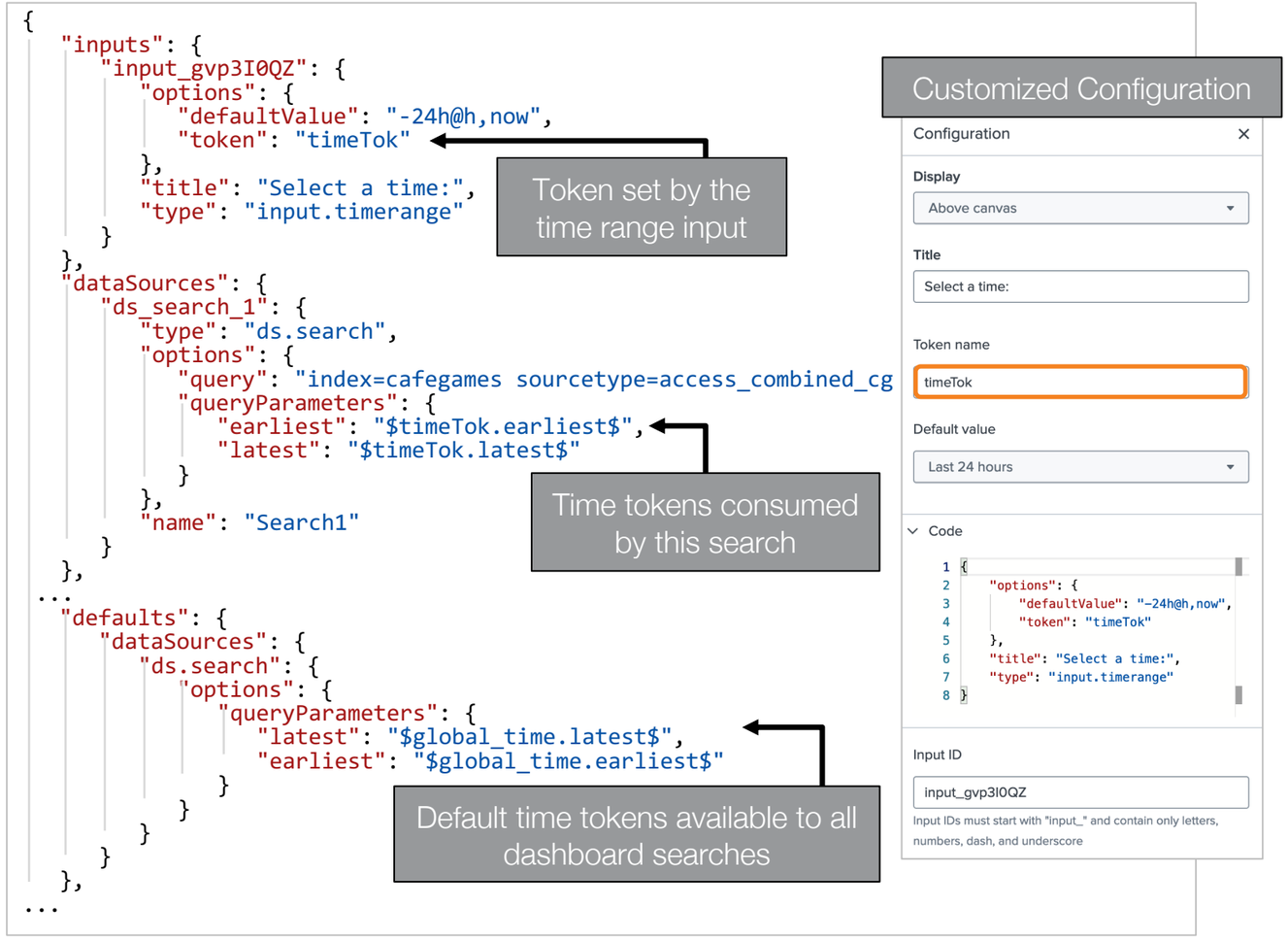
- Using the visual editor:
  - Source code automatically created
- Using the source editor:
  - Input ID must begin with **`input_`**
  - You must add it in two places in the dashboard definition
    1. Define the input stanza in the dashboard definition inputs section
    2. List the input unique ID in the globalInputs area of the layout section



splunk>

Time Range Input Example

- Automatically added to every new dashboard
- Can have more than one
- Can customize token name
- Time token is consumed as two tokens
  - `.earliest` and `.latest` are automatically appended
  - Automatically added to the defaults section
- Works with inline and base & chain searches



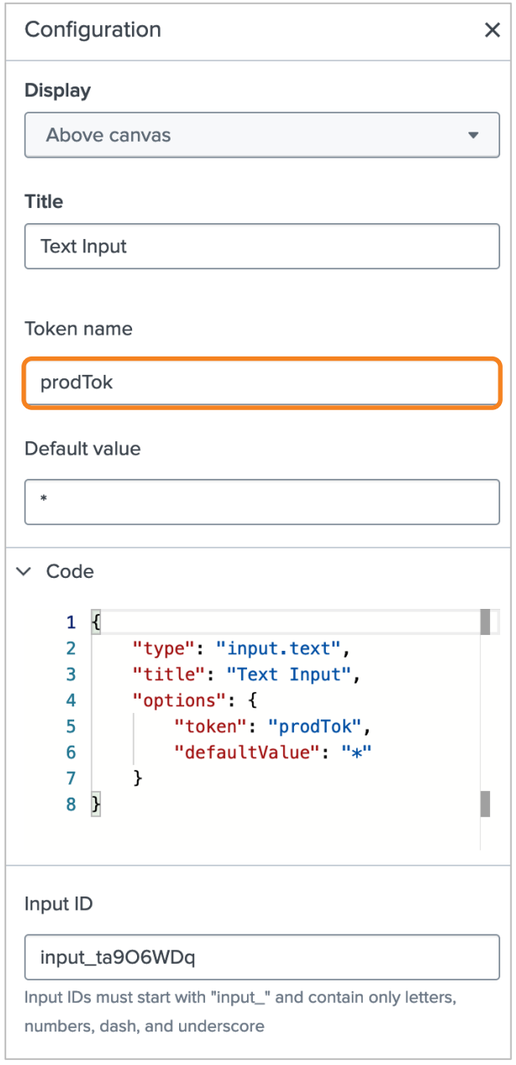
splunk>

Text Input Example

Enter any number or string to the input

```
{
 "dataSources": {
  "ds_search_1": {
   "type": "ds.search",
   "options": {
    "query": "index=\"cafegames\" product_name=$prodTok|s$ | timechart count by product_name useother=f"
    },
   "name": "Cafe Game Sales"
  }
 },
 "inputs": {
  "input_ta9O6WDq": {
   "type": "input.text",
   "title": "Enter product name:",
   "options": {
    "token": "prodTok",
    "defaultValue": "*"
   }
  }
 },
...
 "layout": {
  "globalInputs": [
   "input_global_trp",
   "input_ta9O6WDq"
  ]
 },
 "title": "Text Input Example",
...
```

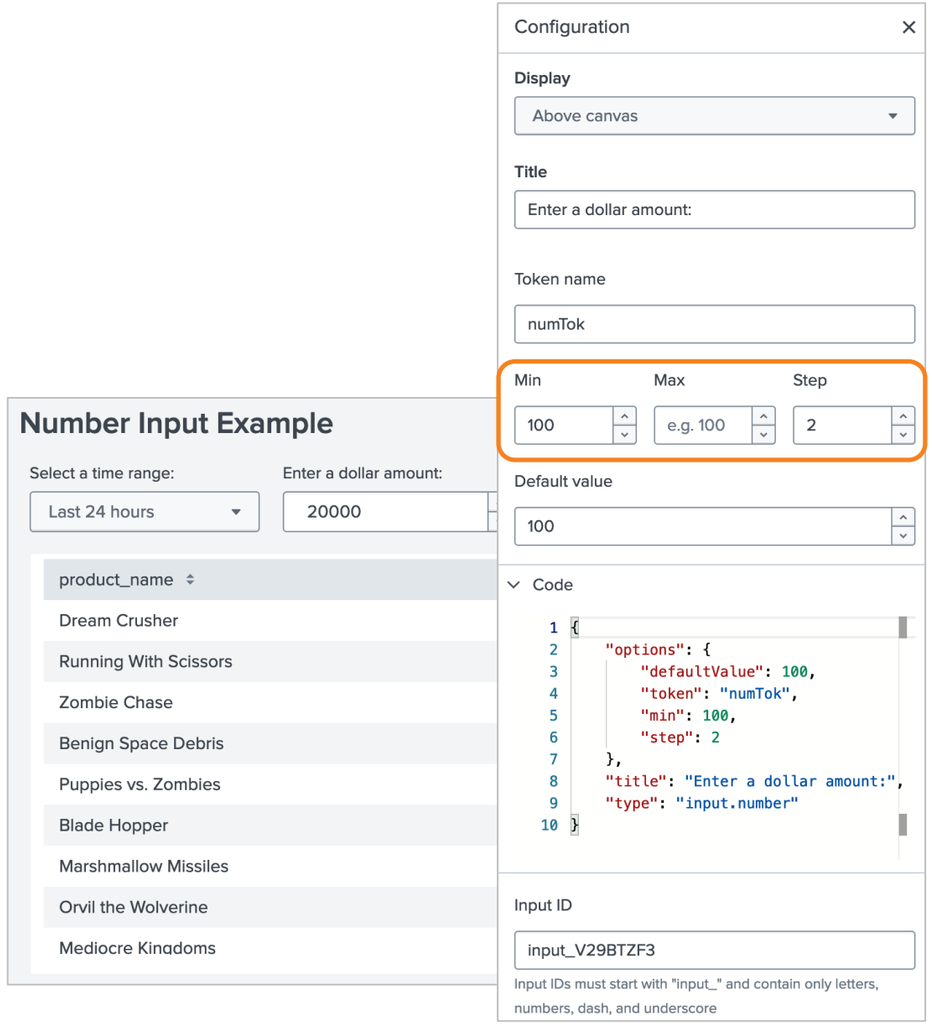
In the search, use $ as a delimiter and optionally, a token filter



splunk>

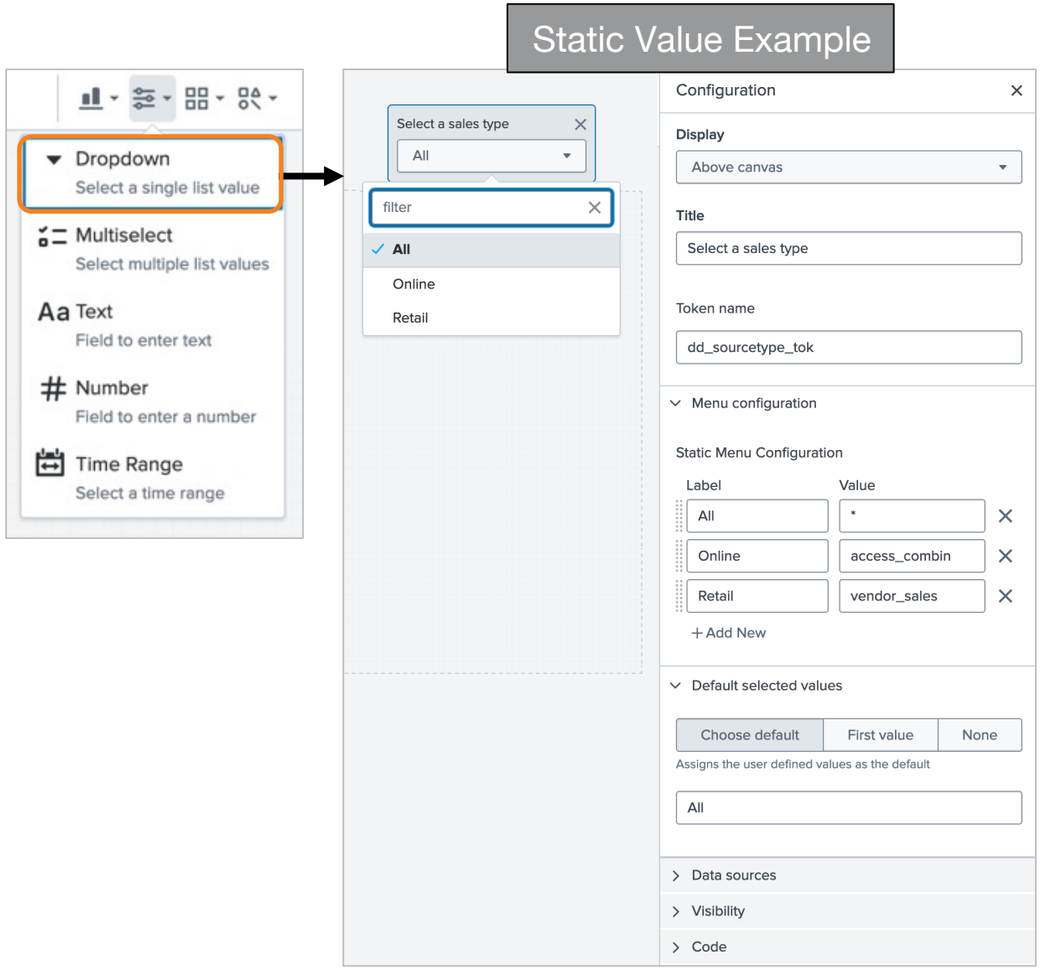
Number Input Example

- Ensures users only enter numbers
- Supports decimals and negative numbers
- Useful when passing a token to a search that requires a numerical argument
- Available options:
  - defaultValue
  - token
  - min: minimum number available
  - max: maximum number available
  - step: interval for the up / down arrow



Dropdown Menu Input

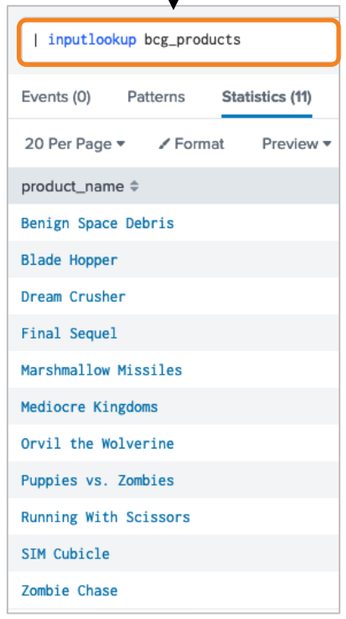
- Populate dropdown inputs using static values or dynamically with search results
  - Up to 1,000 items in the menu
- Requires defining key/value pairs
  - Label appears in the menu
  - Value is passed as the token



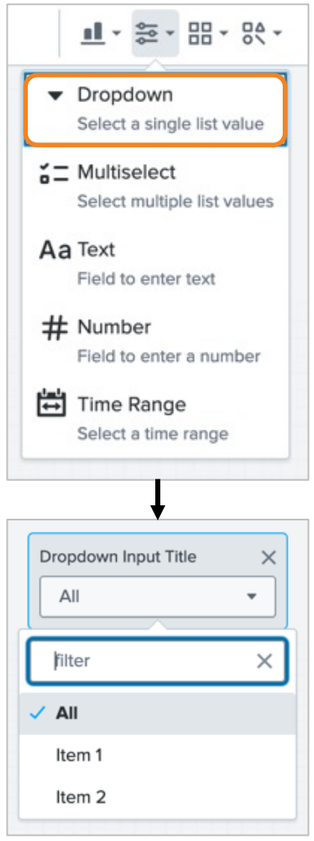
Dropdown Menu Input – Dynamic Example

1 Create a scheduled search that outputs a lookup (optional)

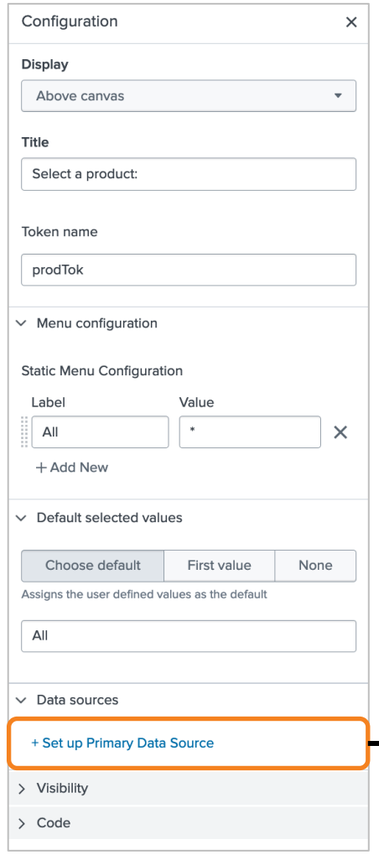
```
index=cafegames product_name="*"
| dedup product_name
| table product_name
| sort product_name
| outputlookup bcg_products
```



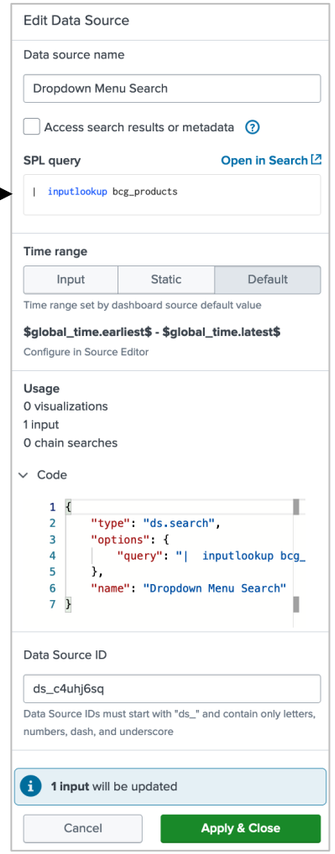
2 Add the input to the dashboard



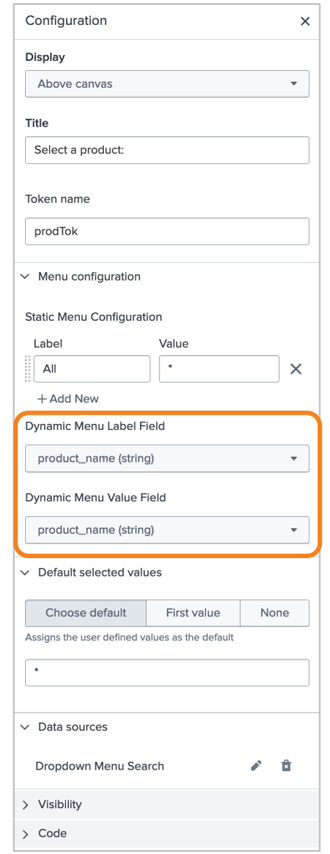
3 Customize title, token, and static options (optional)



4 Use a lookup or ad-hoc search



5 Select the label and value fields

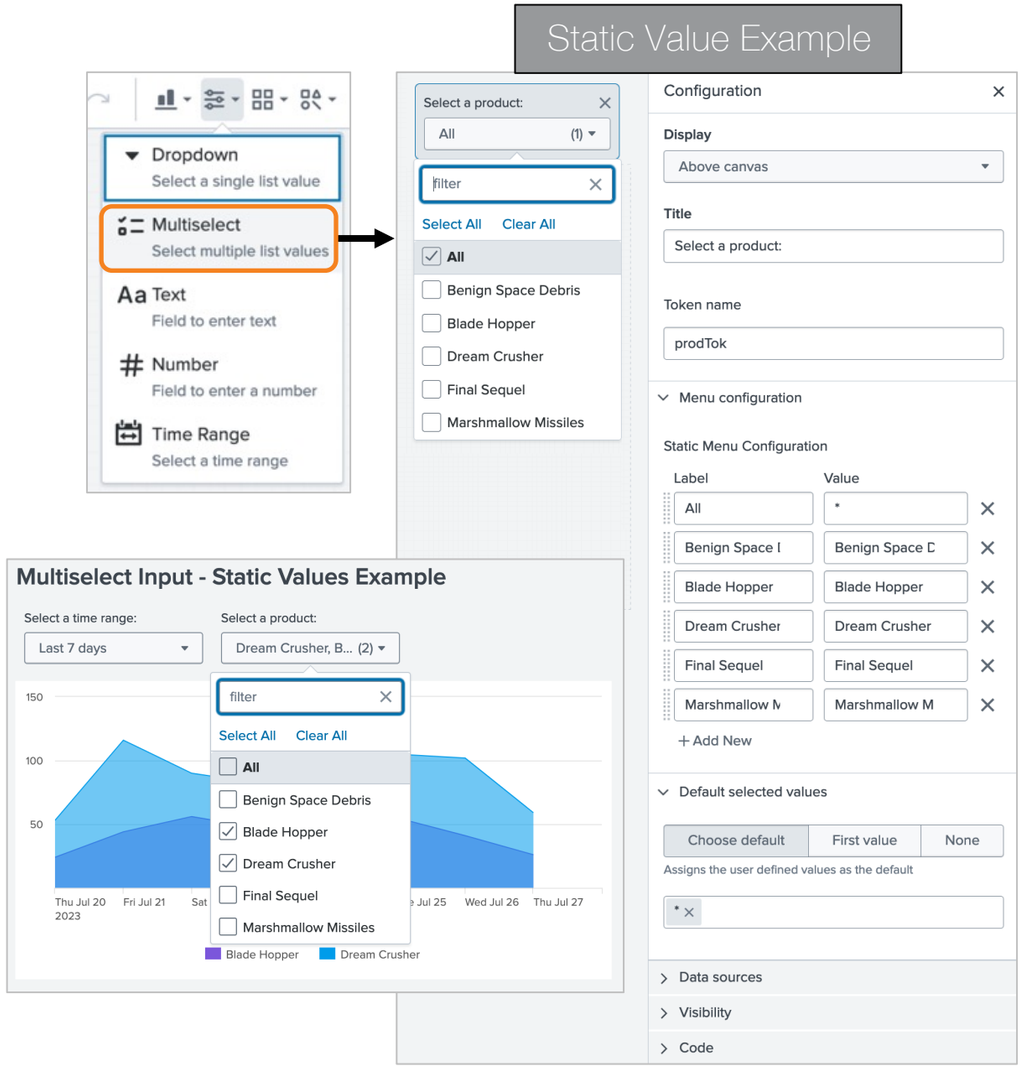


splunk>

Multiselect Input

- Select multiple options from a menu
- Populate input using static values or dynamically with search results
  - Up to 1,000 items in the menu
- Only a comma delimiter is supported
  - Use the IN operator and format your queries appropriately

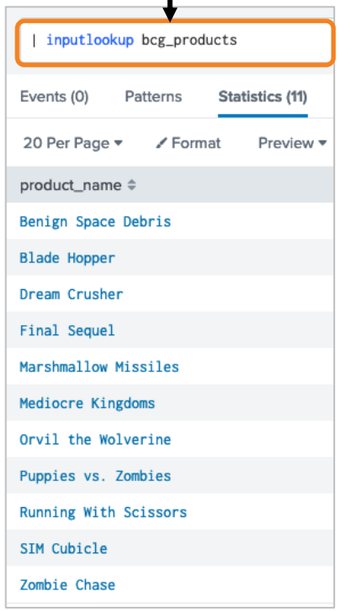
```
index=cafegames sourcetype=access_combined_cg product_name IN ($prodTok|s$)
| timechart count by product_name
```



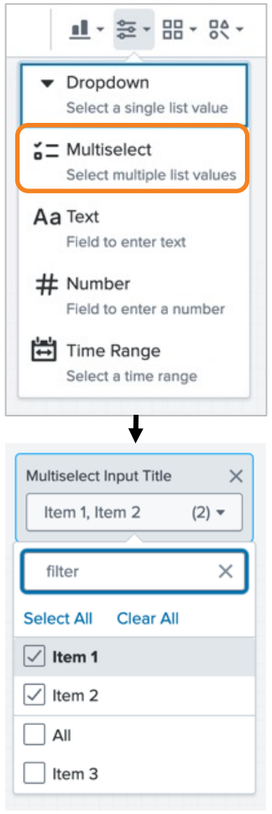
Multiselect Input – Dynamic Example

1. Create a scheduled search that outputs a lookup (optional)

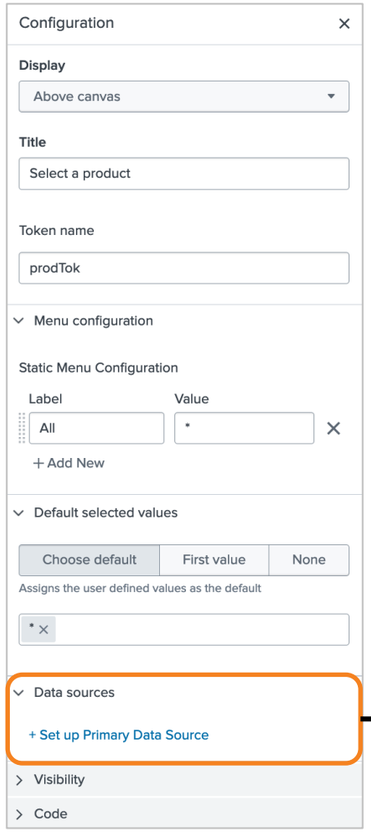
```
index=cafegames product_name="*"
| dedup product_name
| table product_name
| sort product_name
| outputlookup bcg_products
```



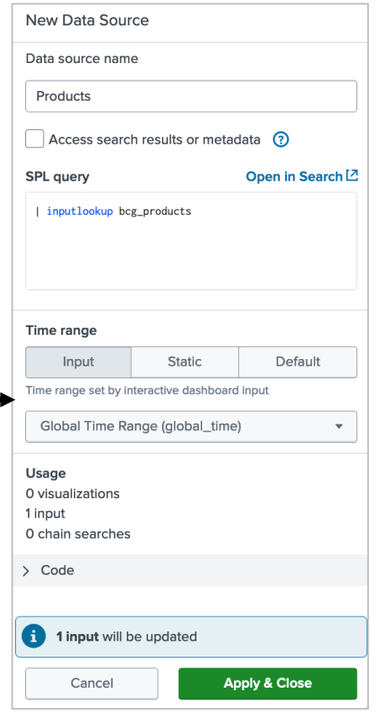
2. Add the input to the dashboard



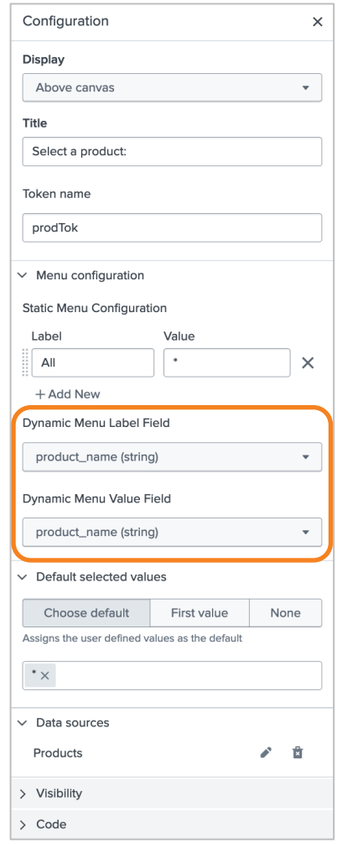
3. Customize the title and token and static options (optional)



4. Use the lookup search or an ad-hoc search



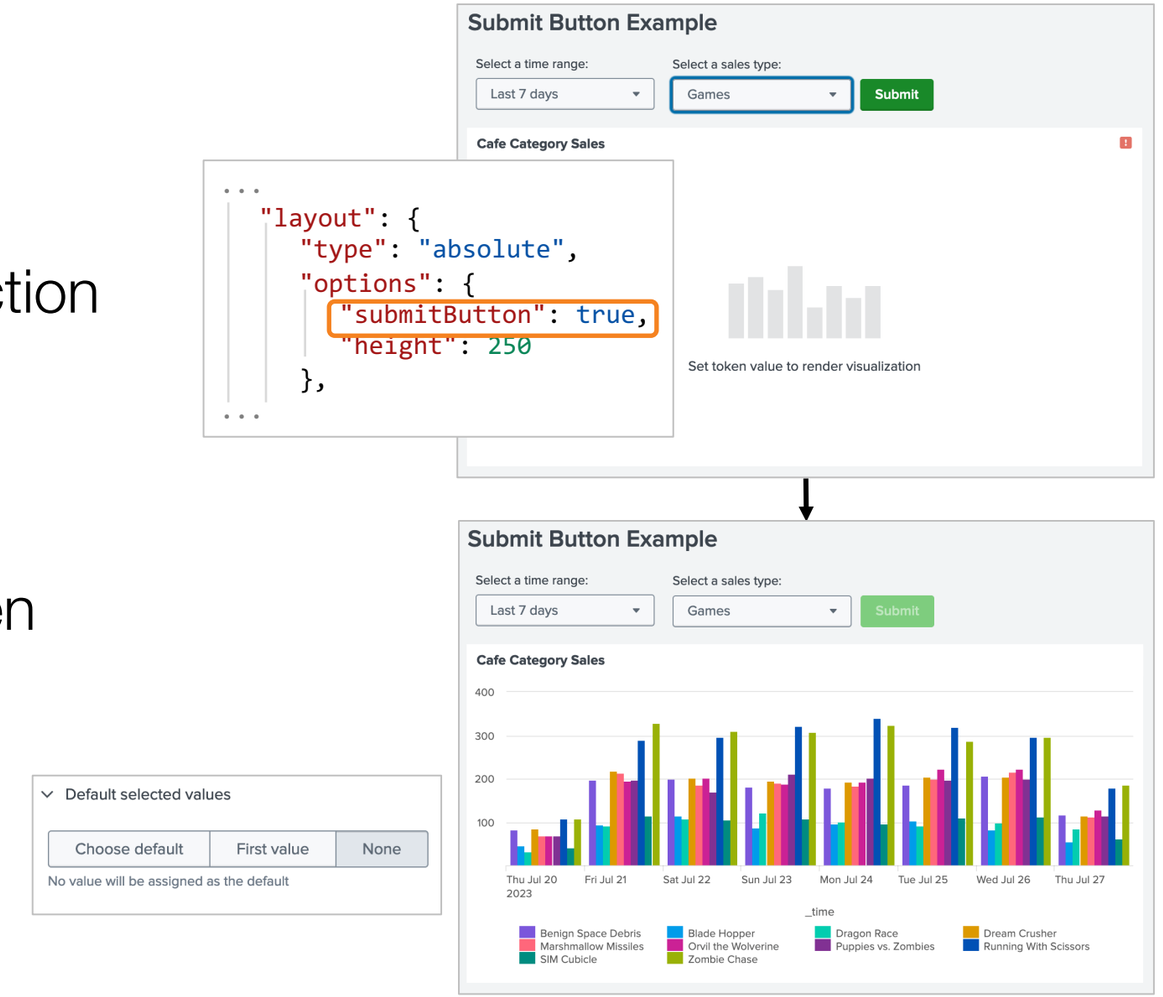
5. Select the label and value fields



splunk>

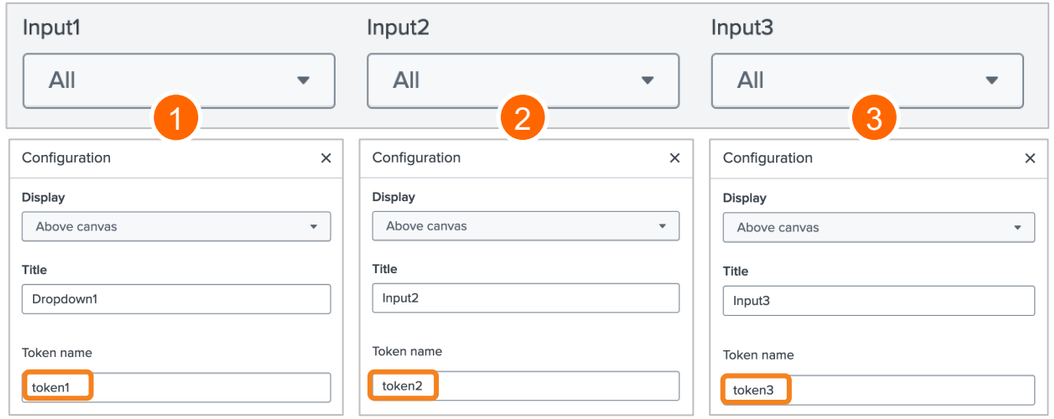
Submit Button

- Click to refresh a dashboard after making input selections
  - Requires adding the submitButton property to options in the layout section
- Boolean settings
  - true: Submit button click required for an input selection to take effect
  - false or not specified: refreshes when input selection is made
- Input default values determine whether visualization displays on initial dashboard load



Cascading Inputs

- One input sets values for another input
- To each input search, add the other input tokens
  - For example, in a three-input cascade:
    - Input1 search: add token2 and token3
    - Input2 search: add token1 and token3
    - Input3 search: add token1 and token2



Input1 Search

```
| inputlookup myLookup
| search field2=$token2$ field3=$token3$
| dedup field1 | fields field1 | sort field1
```

Input2 Search

```
| inputlookup myLookup
| search field1=$token1$ field3=$token3$
| dedup field2 | fields field2 | sort field2
```

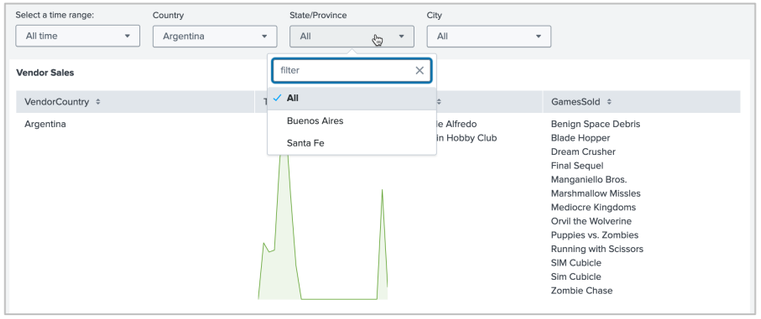
Input3 Search

```
| inputlookup myLookup
| search field1=$token1$ field2=$token2$
| dedup field3 | fields field3 | sort field3
```

Cascading Inputs – Example

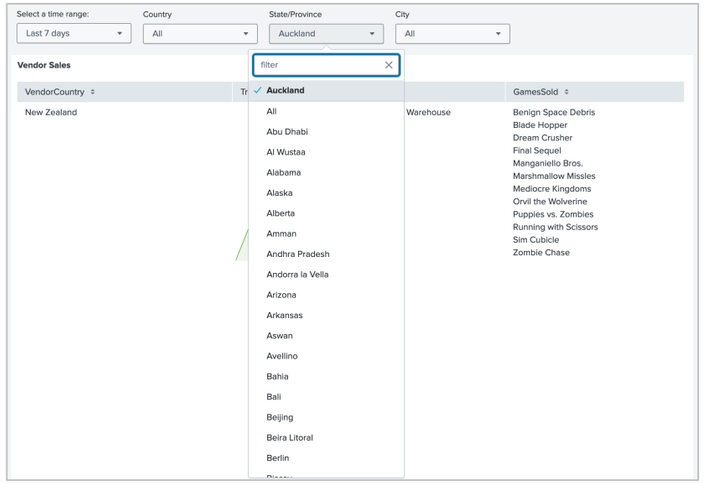
Country Input Search

```
| inputlookup bcg_vendors
| search VendorStateProvince=$vStateTok|s$ VendorCity=$vCityTok|s$
| dedup VendorCountry | fields VendorCountry | sort VendorCountry
```



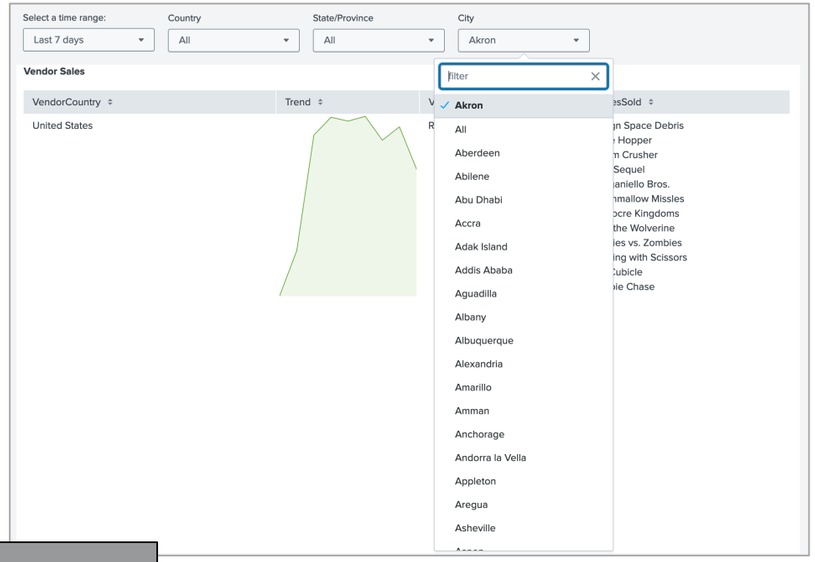
State/Province Input Search

```
| inputlookup bcg_vendors
| search VendorCountry=$vCountryTok|s$ VendorCity=$vCityTok|s$
| dedup VendorStateProvince | fields VendorStateProvince
| sort VendorStateProvince
```



City Input Search

```
| inputlookup bcg_vendors
| search VendorCountry=$vCountryTok|s$ VendorStateProvince=$vStateTok|s$
| dedup VendorCity | fields VendorCity | sort Vendor
```



The table search consumes all three tokens

```
index=sales sourcetype=vendor_sales VendorCountry=$vCountryTok$ VendorStateProvince=$vStateTok$ VendorCity=$vCityTok$
| stats sparkline(count) as Trend values(Vendor) as Vendor values(product_name) as GamesSold by VendorCountry
```


splunk>

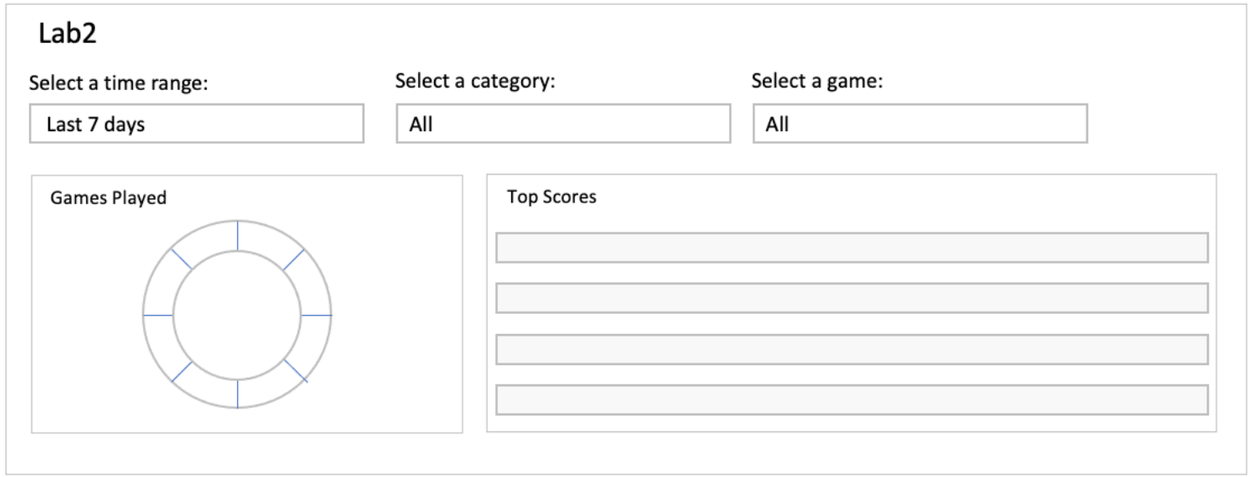
Lab Exercise 2 – Create Cascading Inputs

Description: Create a dashboard, add dropdown inputs, and make the inputs cascade.

Duration: 25 minutes

Tasks:

- Create a dashboard
- Add dropdown menu inputs
- Make inputs cascade
- Add a chart



Topic 3: Adding Drilldowns

Topic Objectives

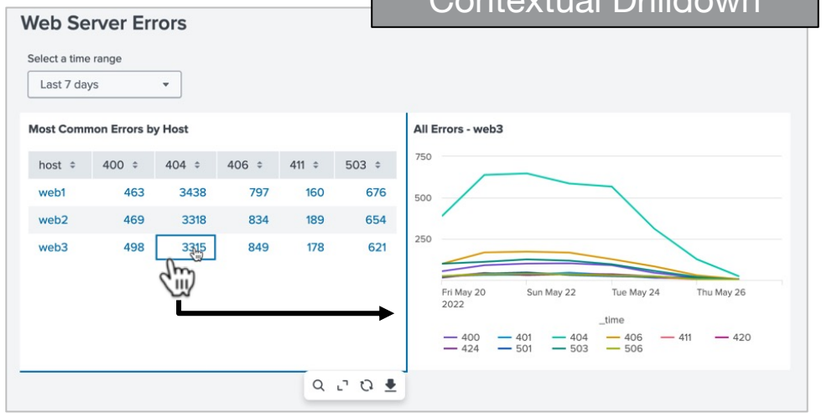
- Identify types of drilldowns
- Create a dynamic drilldown
- Create a contextual drilldown

Custom Drilldowns

- Dynamic Drilldown
  - Link to dashboard
    - Set tokens
    - Pass values as tokens from a user click to another dashboard
  - Specify a path to a URL
    - Relative path to a dashboard in another app
    - Absolute path to an external website
- Contextual Drilldown
  - Set tokens
    - Pass values as tokens from a user click to visualizations on the same dashboard

Dynamic Drilldown

Contextual Drilldown

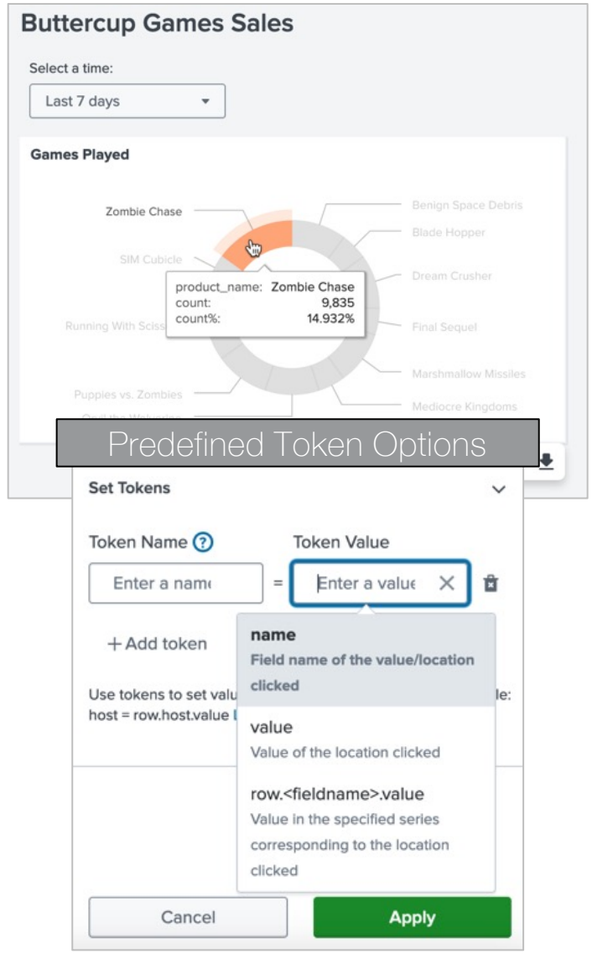


splunk>

Custom Drilldowns – Setting Tokens

- Set tokens with a visualization click
- Use predefined tokens or a static token value
  - `name` captures the field name of the value or location clicked
  - `value` captures the value of the location clicked
  - `row.<field_name>.value` captures the value in the specified series of the location clicked
- Use `$...$` delimiters in the token value to pass the value of an existing token
  - For example, pass the time range using:

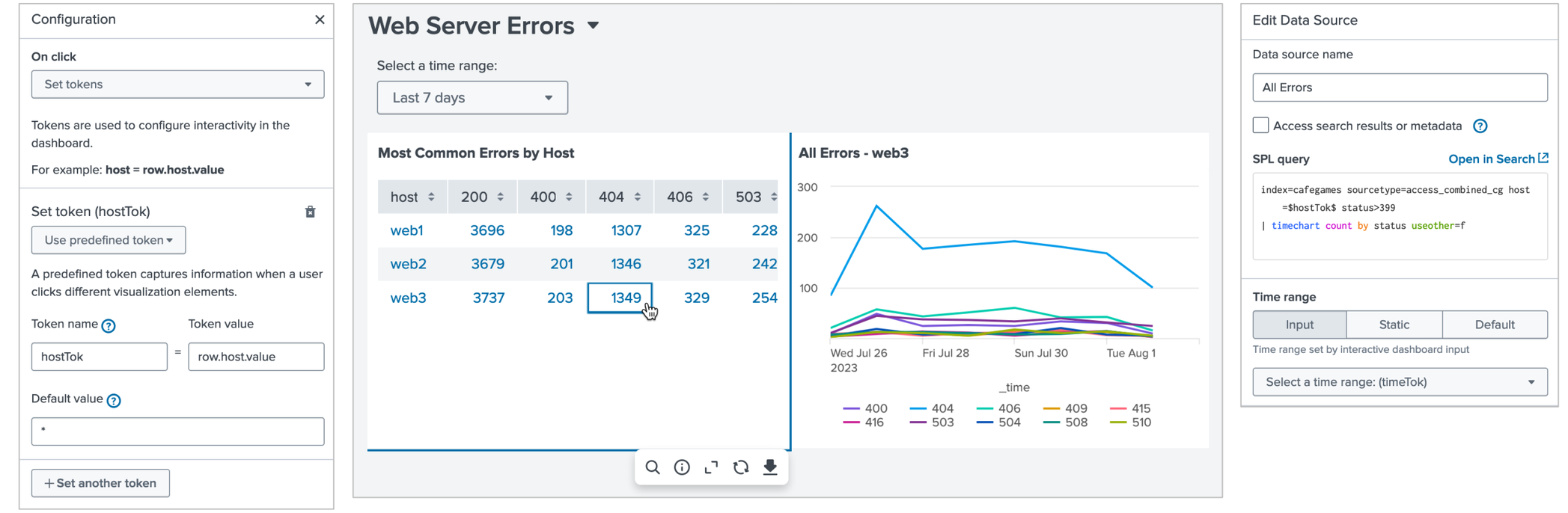
Token Name	Token Value
`<timeRangeToken>.earliest`	`$<timeRangeToken>.earliest$`
`<timeRangeToken>.latest`	`$<timeRangeToken>.latest$`



Setting Tokens – Example

Set a token with one visualization

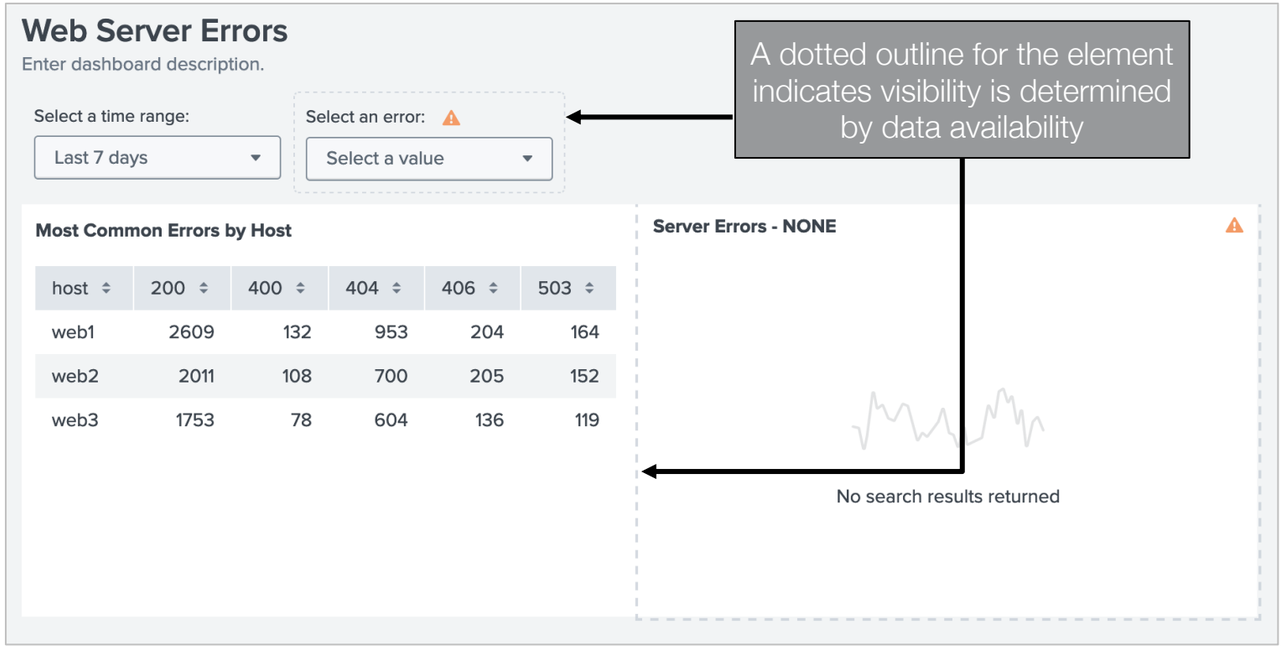
Use that token in the search used by others



splunk>

Hiding Elements

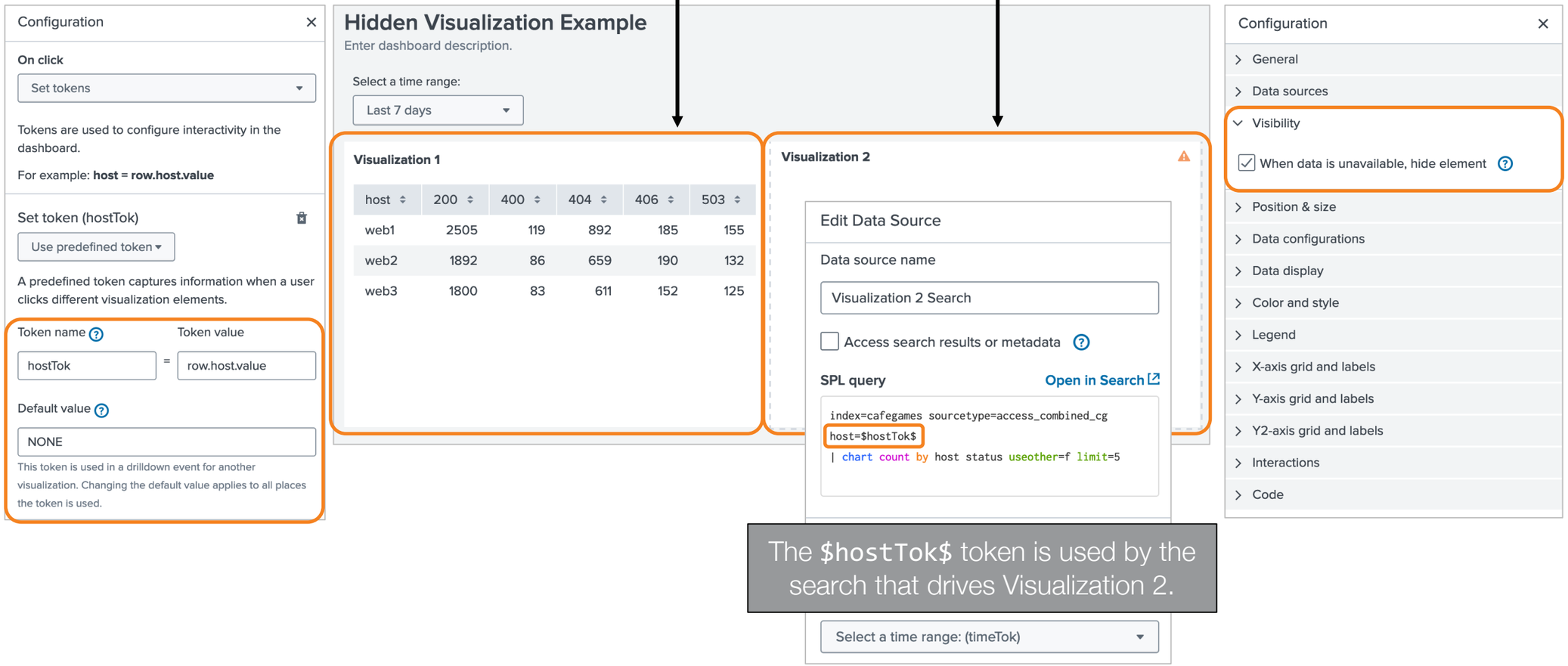
- Hide visualizations and inputs based on the existence of search results
- Requires absolute layout
- Available for the following:
  - Charts
  - Icons
  - Shapes
  - Dropdown input
  - Multiselect input



Hiding Elements – Visualization Example

A click on Visualization 1 sets the `$hostTok$` token.

Visualization 2 is hidden until the `$hostTok$` token is set.

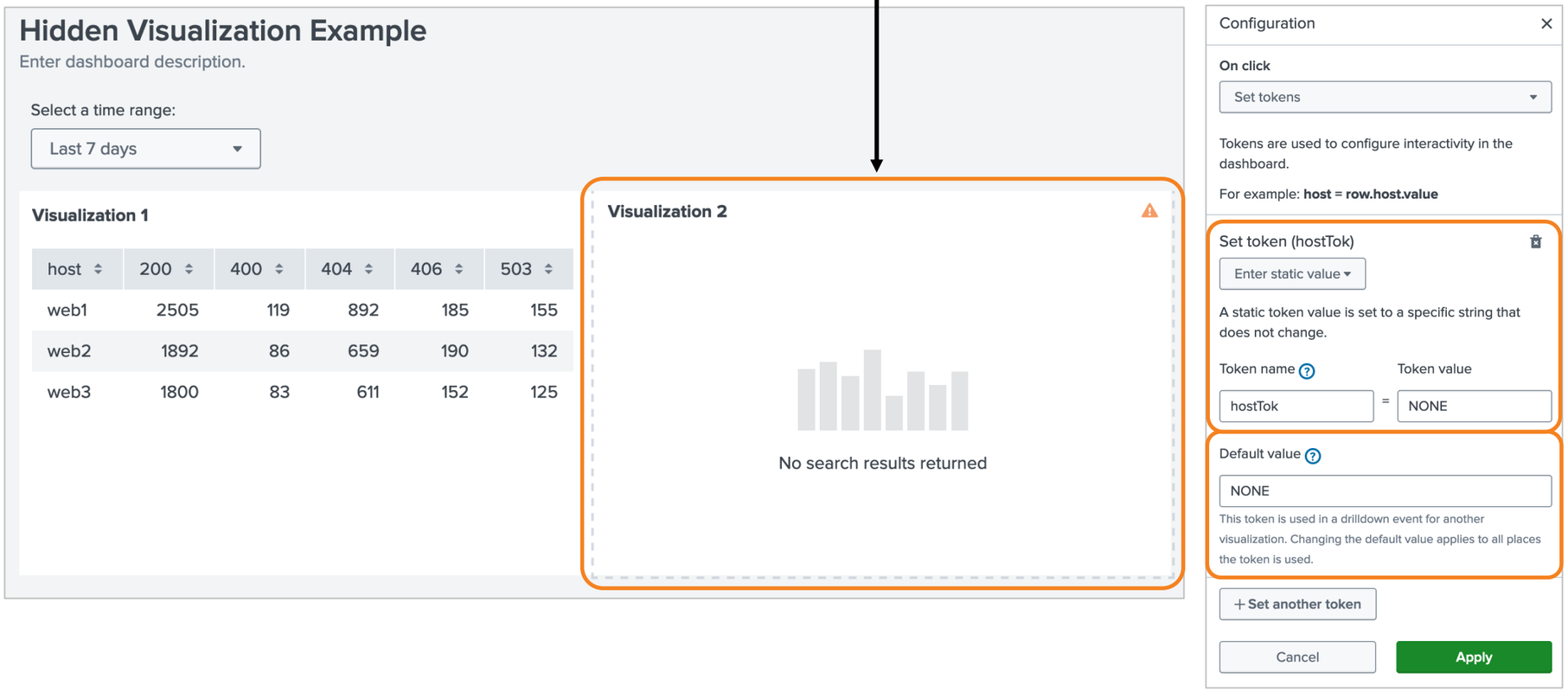


The `$hostTok$` token is used by the search that drives Visualization 2.

splunk>

Hiding Elements – Visualization Example (cont.)

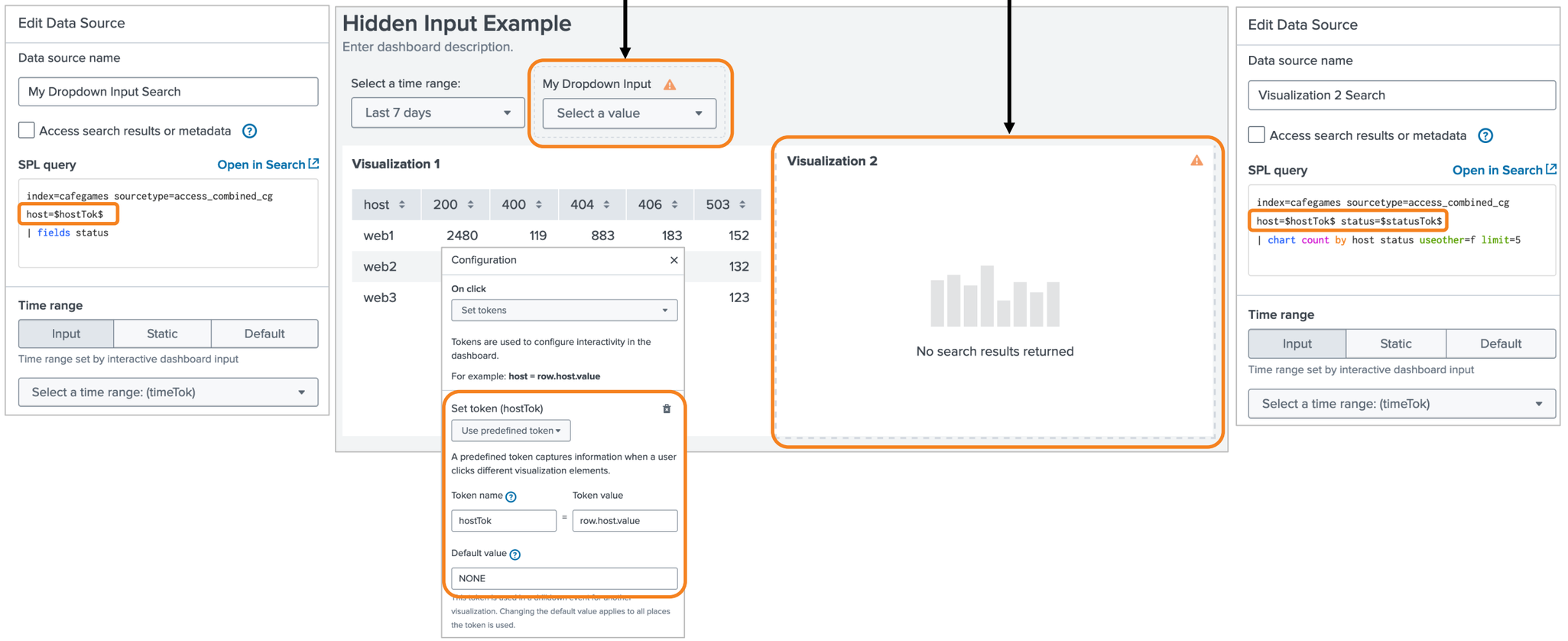
Hide visualization 2 again by having a user click reset the token to the default value



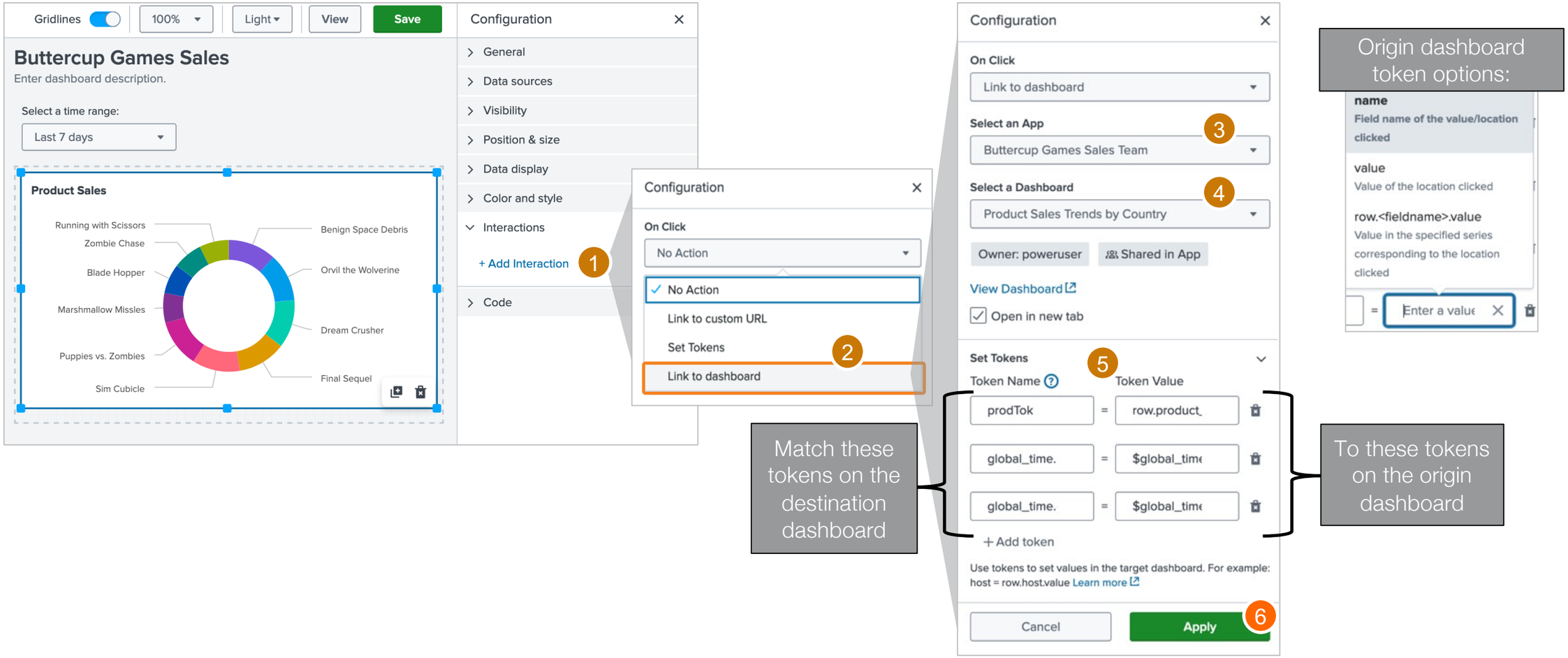
Hiding Elements – Input Example

My Dropdown Input is hidden until the `$hostTok$` token is set by a click on Visualization 1

Visualization 2 is hidden until a selection from My Dropdown Input sets the `$statusTok$` token consumed by Visualization 2.



Dynamic Drilldown – Origin Dashboard

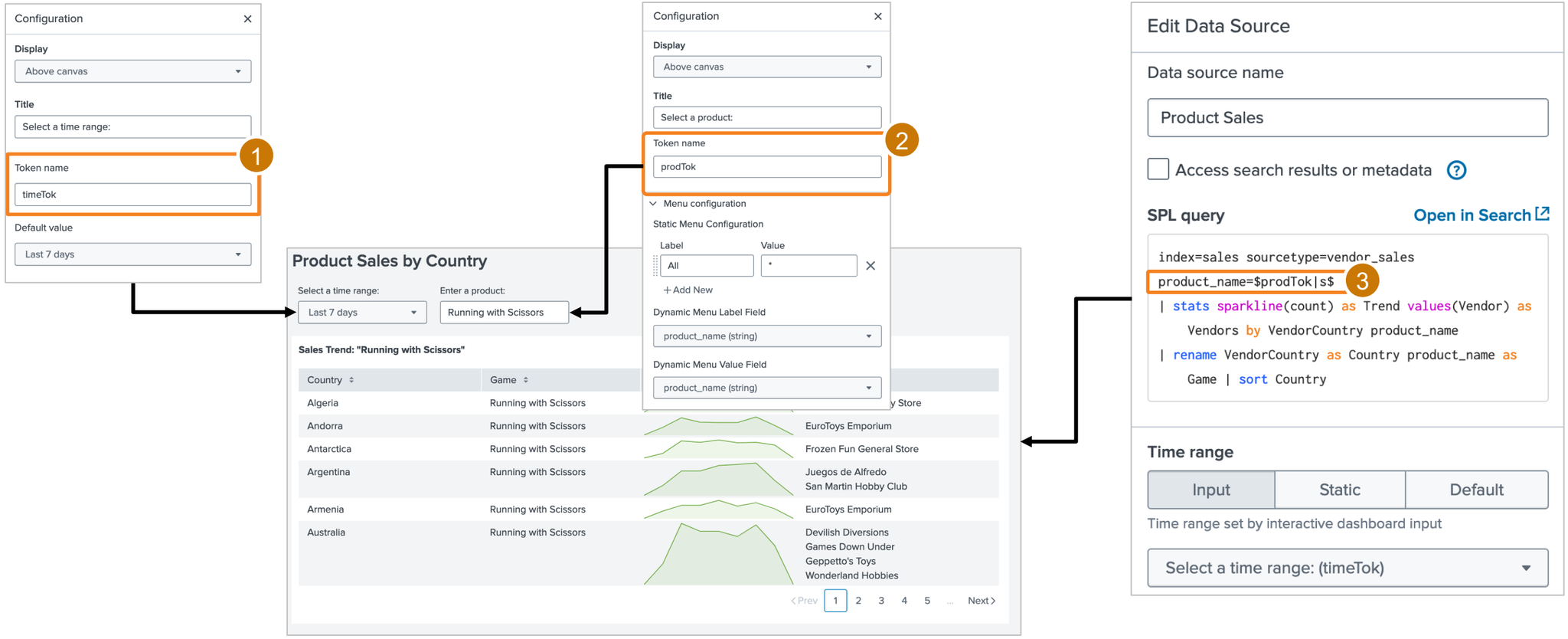


Dynamic Drilldown – Destination Dashboard

If passing a time input token match their token names on both dashboards

Can use the source token on destination inputs

Add the source token to the search used by the visualization on the destination dashboard



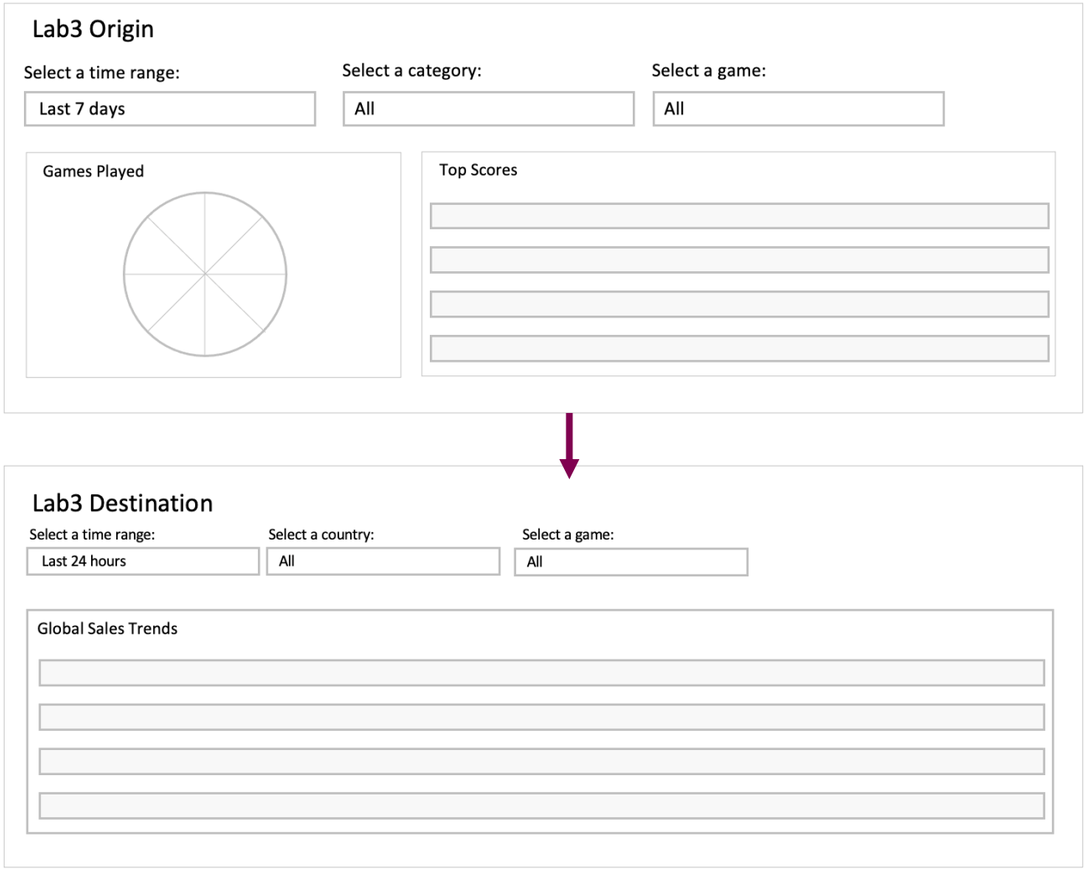
Lab Exercise 3 – Create a Dynamic Drilldown

Description: Create a dynamic drilldown from the Games Played pie chart to a new form

Duration: 25 minutes

Tasks:

- Create a destination form
- Configure the data source
- Add dropdown inputs
- Clone a dashboard
- Add a drilldown



splunk>

Topic 4: Dynamic Visualizations

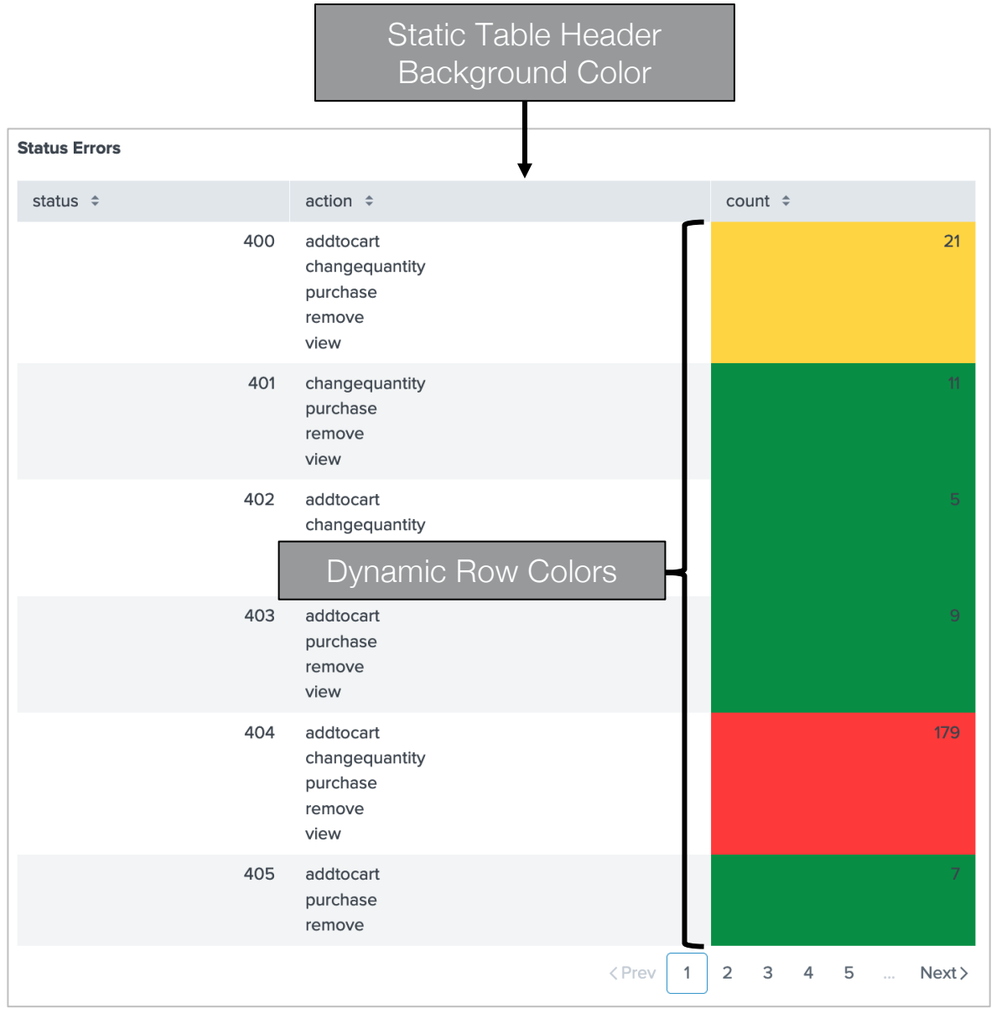
Topic Objectives

- Describe static and dynamic coloring
- Add dynamic coloring to a visualization

splunk>

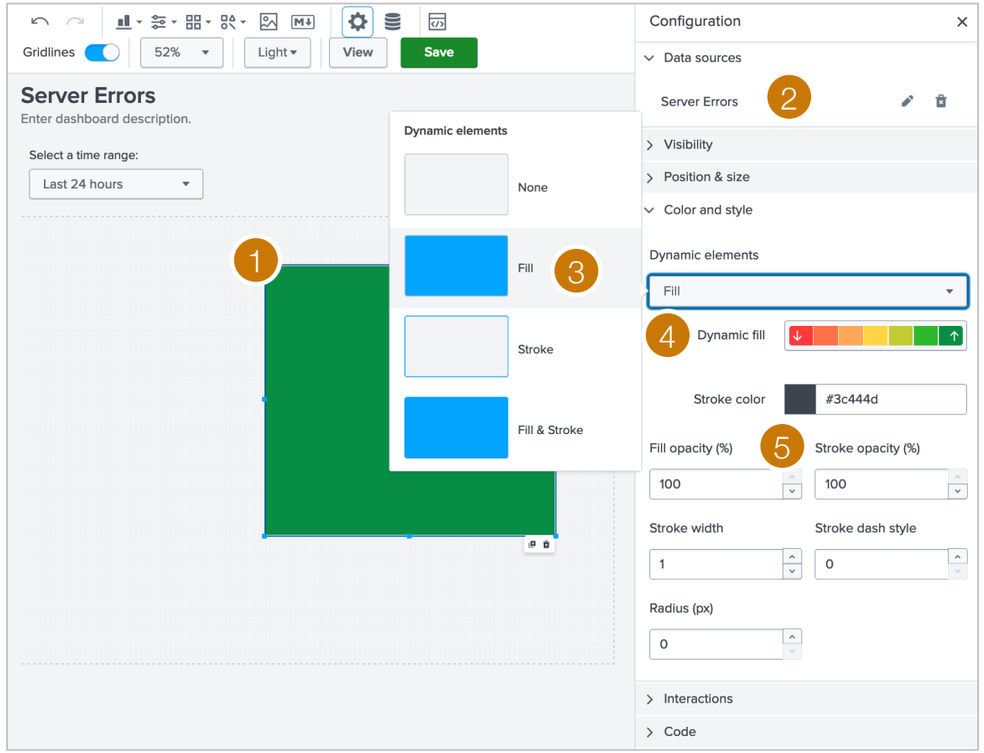
Visualization Coloring

- Static: color part of the visualization
  - Fill, lines, rows, and more
- Dynamic: use search results to dynamically color visualizations
  - Color values by trend, value, and more
  - Fill, lines, columns, rows, values, text, and more
  - Available for these visualizations:
    - Icon
    - Punchcard
    - Marker Gauge
    - Table
    - Shape
    - Single Value
    - Single Value Radial
    - Single Value Icon
    - Sankey
    - Choropleth SVG



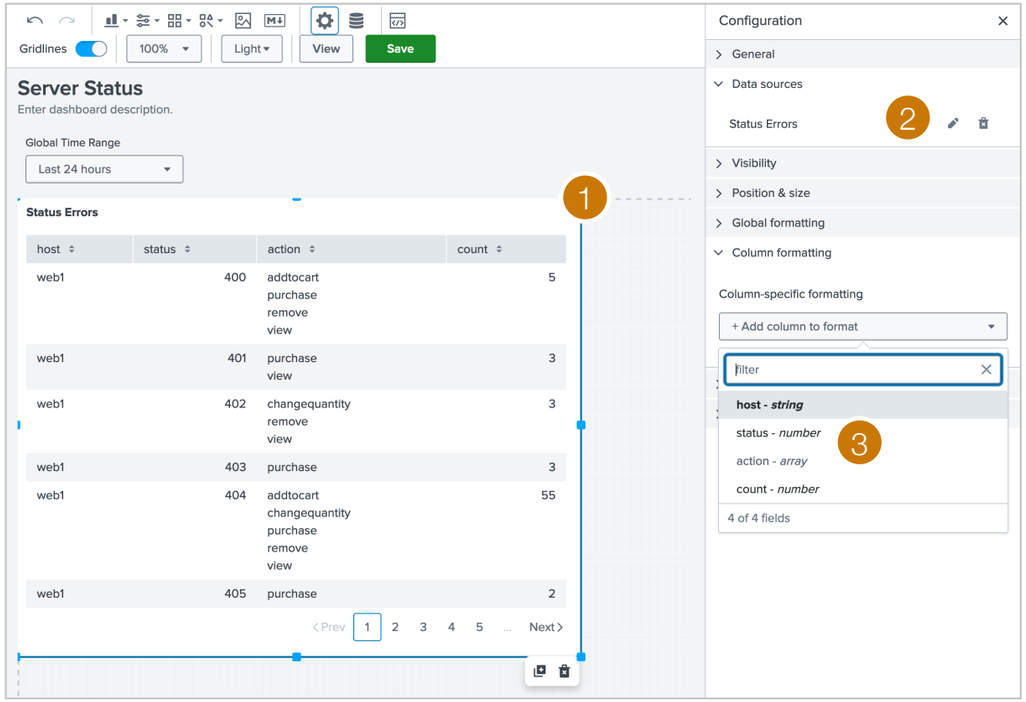
Dynamic Coloring – Shape Example

- To enable dynamic coloring:
  1. Select the shape
  2. Set up the Primary Data Source
  3. Select an option in Dynamic Elements
  4. Set threshold values and colors
  5. Set fill and stroke opacity



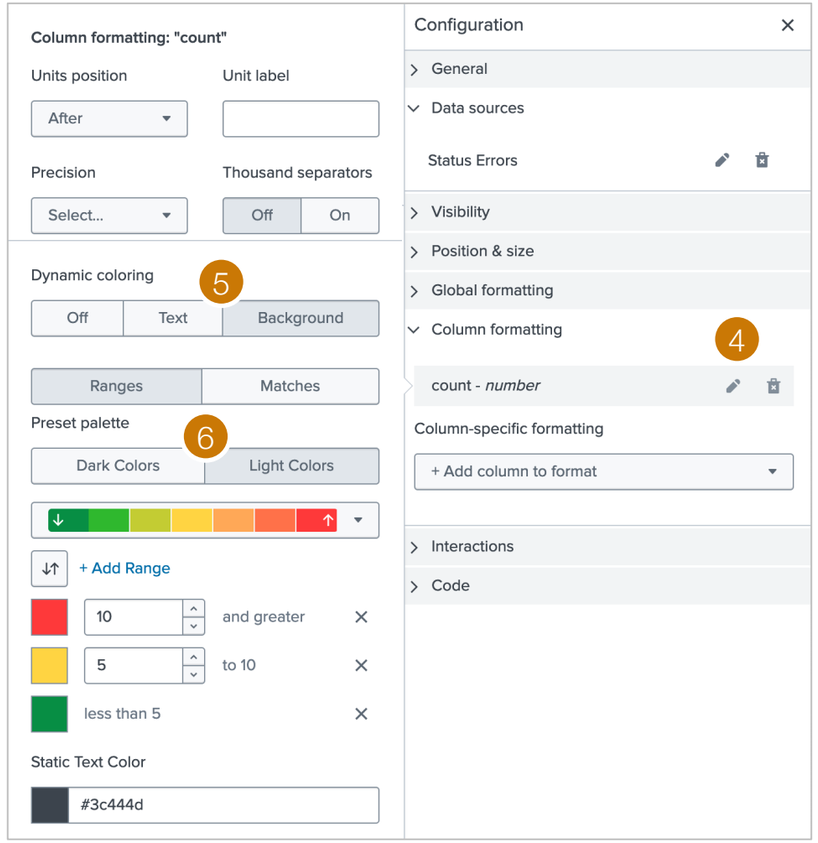
Dynamic Coloring – Table Example

- To enable dynamic coloring:
  1. Select the table
  2. Set up the Primary Data Source
  3. Select the column to be dynamically colored



Dynamic Coloring – Table Example (cont.)

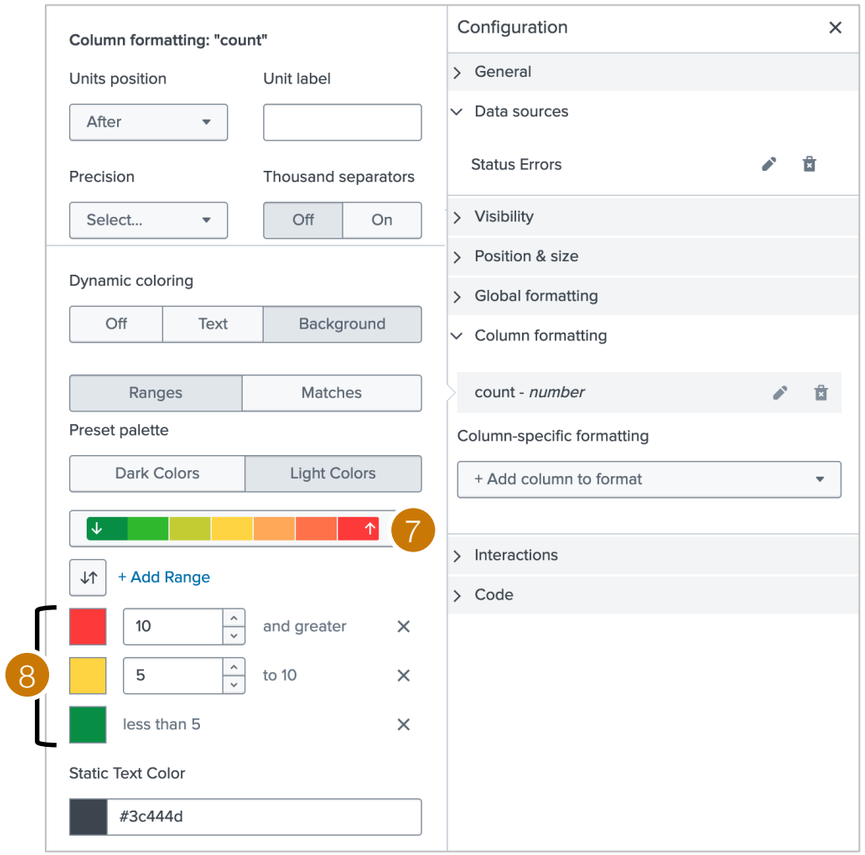
4. Click the pencil icon beside the column selected
5. Select text or background of the column to be colored
6. Choose between dark and light colors



splunk>

Dynamic Coloring – Table Example (cont.)

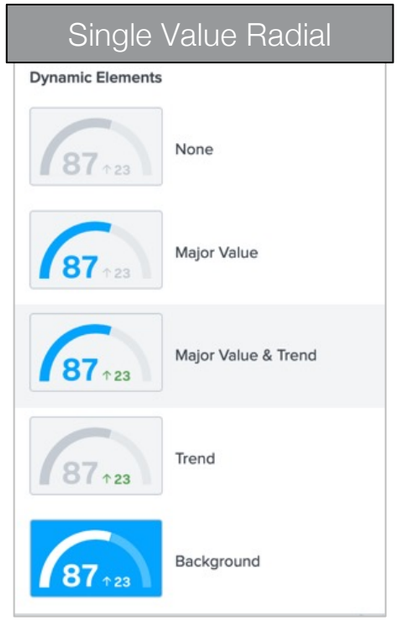
7. Select a preset palette
   - If needed, switch the range order of the colors
8. Specify the range values
   - More than seven can be added using the source editor
   - If needed, change the range colors

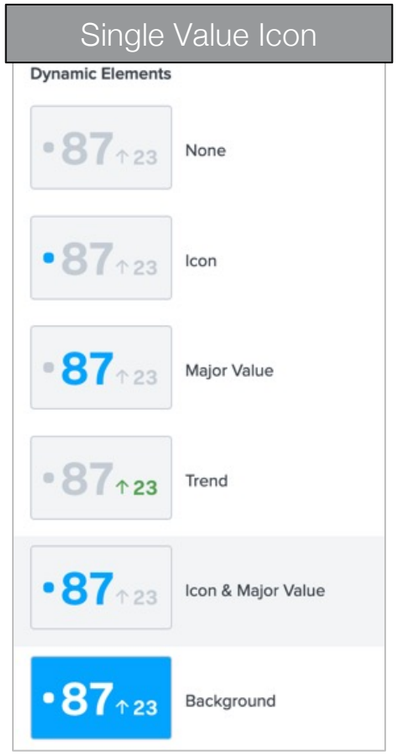


splunk>

Dynamic Coloring – Single Value

- Single Value and Single Value Radial
  - Major value, trend, and background
- Single Value Icon
  - Icon, major value, trend, and background
- Set color thresholds for different data ranges
- Single value icon visualizations start with an icon being added to a layout and then linked to a data source

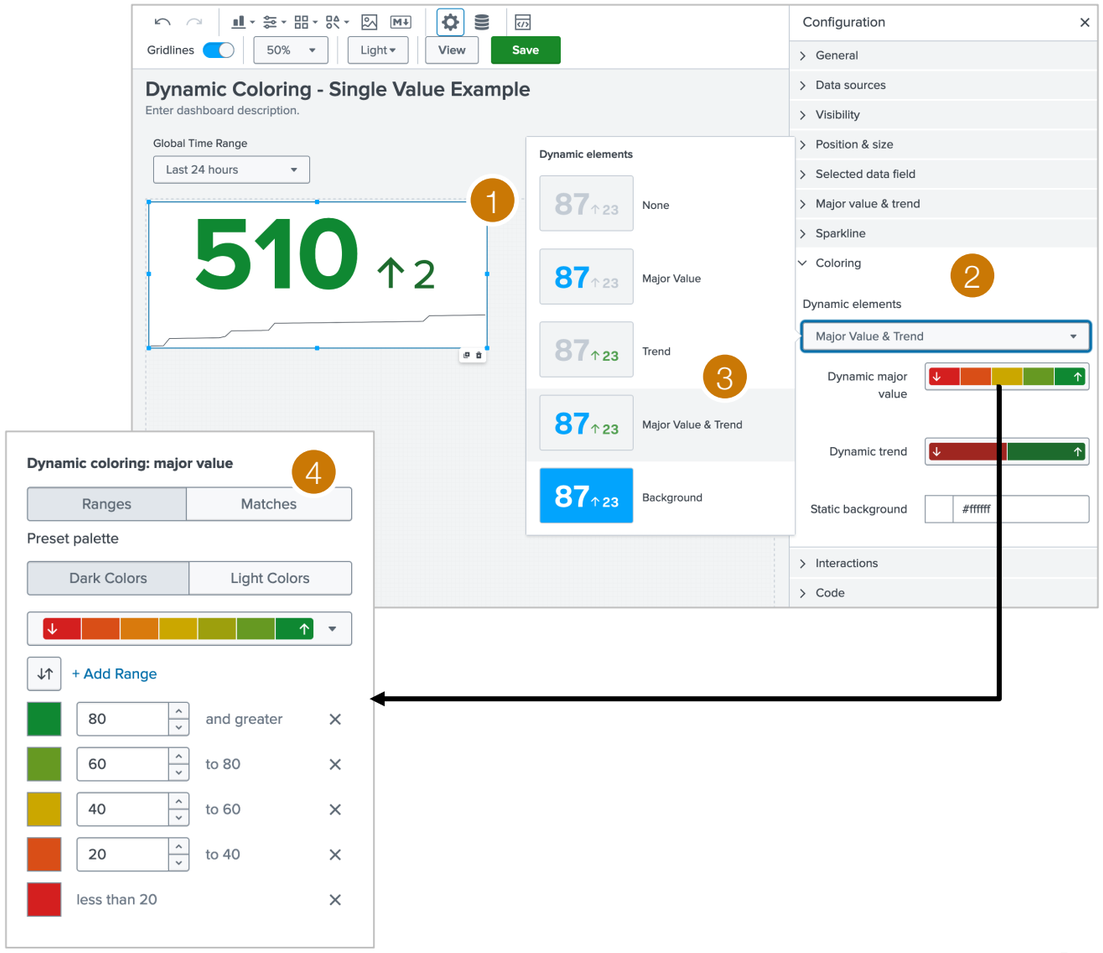




splunk>

Dynamic Coloring – Single Value Example

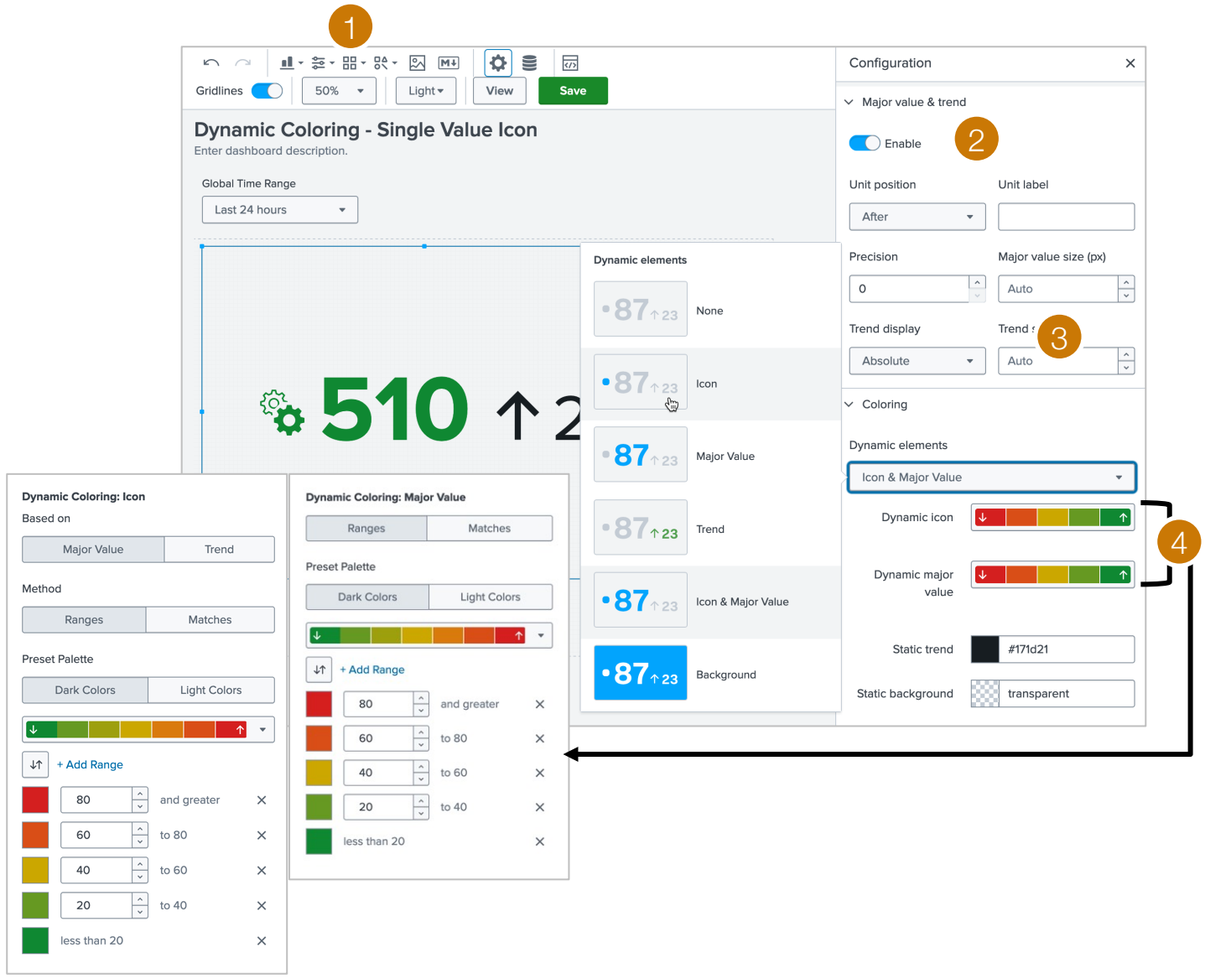
- To enable dynamic coloring:
  1. Add a single value visualization to an absolute layout
  2. Scroll to the Coloring section
  3. In the Dynamic elements menu, select which elements should be dynamically colored
  4. Adjust the color palettes and ranges or accept the defaults



splunk>

Dynamic Coloring – Single Value Icon Example

- To enable dynamic coloring:
  1. Add an icon to an absolute layout
  2. Enable Major value & trend
  3. In the Dynamic Elements menu, select which elements should be dynamically colored
  4. Adjust the color palettes and ranges or accept the defaults



Dynamic Options Example – Source Editor

```
"visualizations": {
    "viz_C8fYK7RH": {
        "type": "splunk.table",
        "options": {
            "columnFormat": {
                "count": {
                    "data": "> table | seriesByName(\"count\") | formatByType(countColumnFormatEditorConfig)",
                    "rowColors": "> table | seriesByName('count') | pick(countRowColorsEditorConfig)",
                    "rowBackgroundColors": "> table | seriesByName(\"count\") | rangeValue(countRowBackgroundColorsEditorConfig)"
                }
            }
        },
        "context": {
            "countColumnFormatEditorConfig": {
                "number": {
                    "thousandSeparated": false,
                    "unitPosition": "after"
                }
            },
            "countRowColorsEditorConfig": [
                "#3c444d"
            ],
            "countRowBackgroundColorsEditorConfig": [
                {
                "value": "#669922",
                "to": 10
                },
                {
                "value": "#CBA700",
                "from": 10,
                "to": 30
                },
                {
                "value": "#D41F1F",
                "from": 30
                }
            ]
        },
    }
...
```

Visualization Formatting

Column of query results to use

Object Properties

Colors and ranges for each color

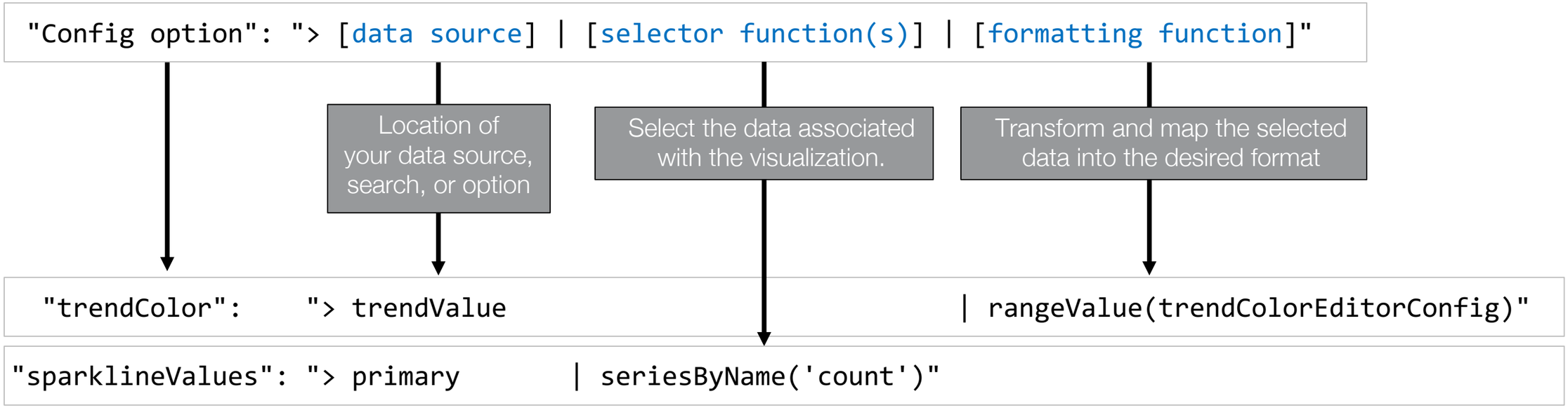
status	action	count
400	addtocart purchase remove view	28
401	changequantity purchase remove	6
402	addtocart purchase view	6
403	purchase view	6
404	addtocart changequantity purchase remove view	163
405	changequantity purchase view	7

< Prev 1 2 3 4 Next >

splunk>

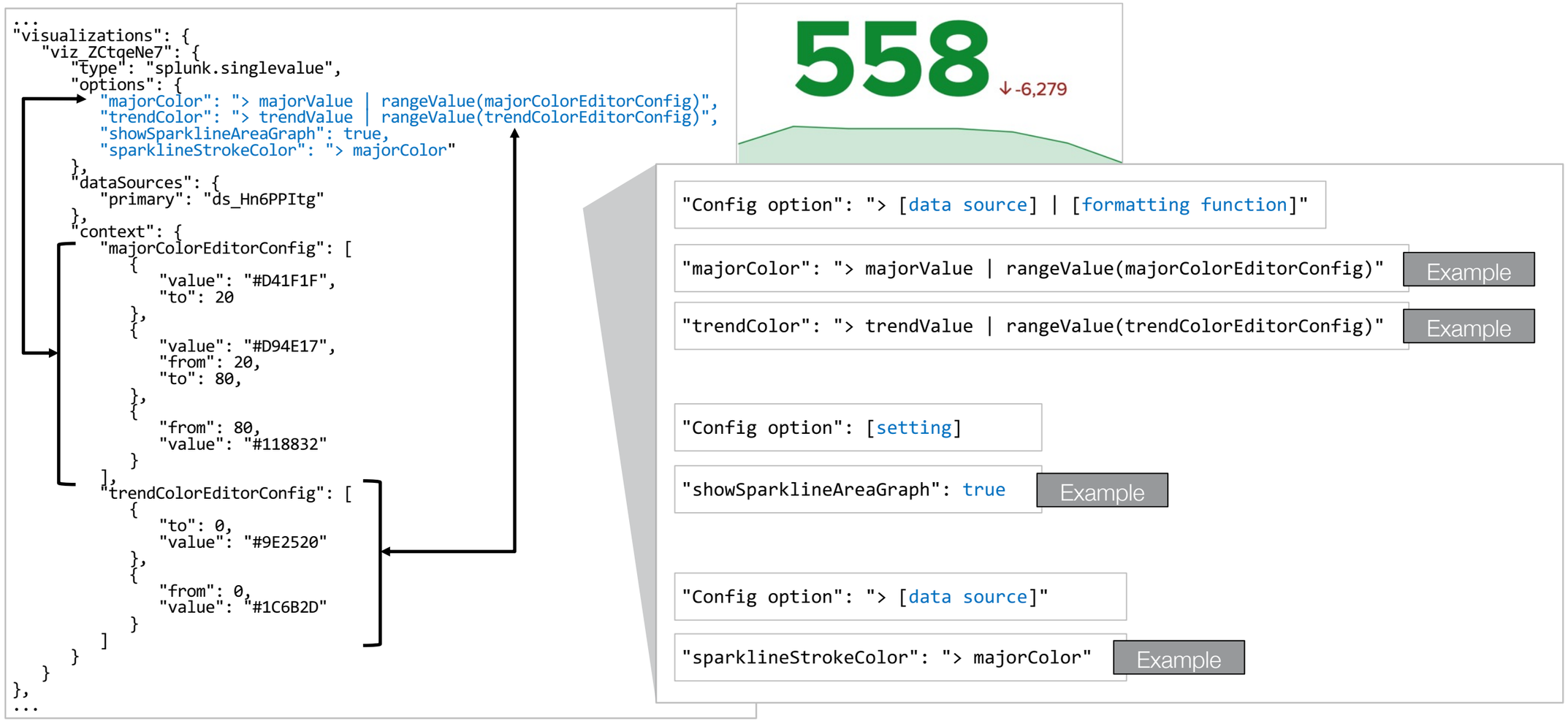
Dynamic Options – Source Editor Only

- Some options are only available by editing the source code
- Add these in the options section of your visualization
  - Items listed configure the illustrative specifics
  - Use dynamic options syntax (DOS) structure



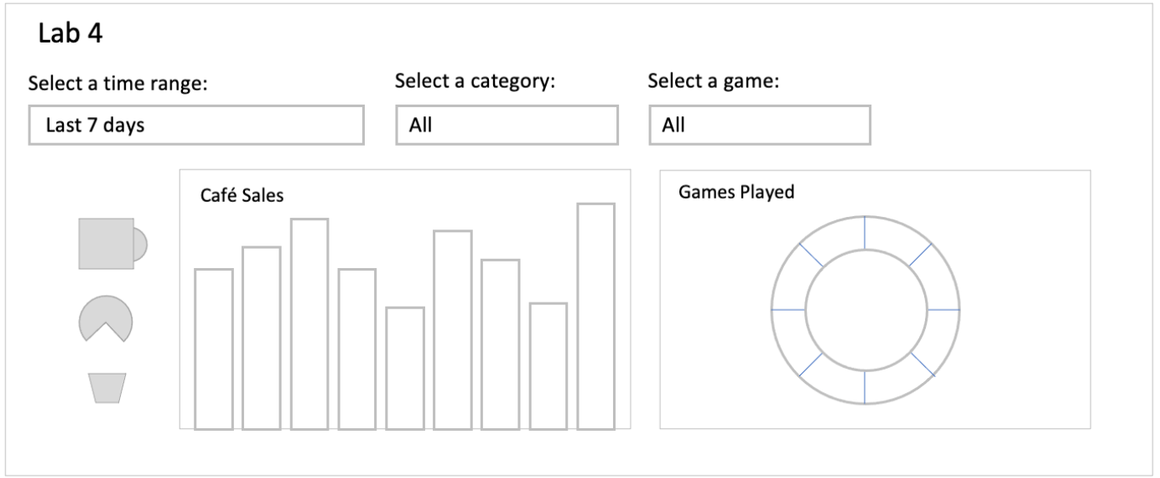
splunk>

Dynamic Options – Source Editor Only (cont.)



Lab 4 – Add Dynamic Coloring

- **Description:** Clone a dashboard, delete a visualization, customize a visualization, add icons and dynamic coloring.
- **Duration:** 25 minutes
- **Tasks:**
  - Clone a dashboard
  - Revise the data sources
  - Revise the pie chart
  - Add a single value visualization
  - Add a column chart
  - Add icons
  - Add dynamic coloring



Summary

Wrap Up

- You should now be able to:
  - Create user inputs
  - Define token syntax
  - Create dynamic inputs
  - Build cascading inputs
  - Create a dynamic drilldown
  - Set tokens
  - Use dynamic coloring

Documentation

Topic 1: Using Tokens

- Use inputs and tokens to make dashboards dynamic

Topic 2: Adding Inputs

- Use Drilldown for Dashboard Interactivity
- Link to a dashboard
- Predefined Drilldown Tokens

Topic 3: Adding Drilldowns

- Object options and defaults reference
- Advanced dynamic options syntax
- The source code stanza of a visualization

Topic 4: Dynamic Visualizations

- How the dashboard definition is structured in the source editor

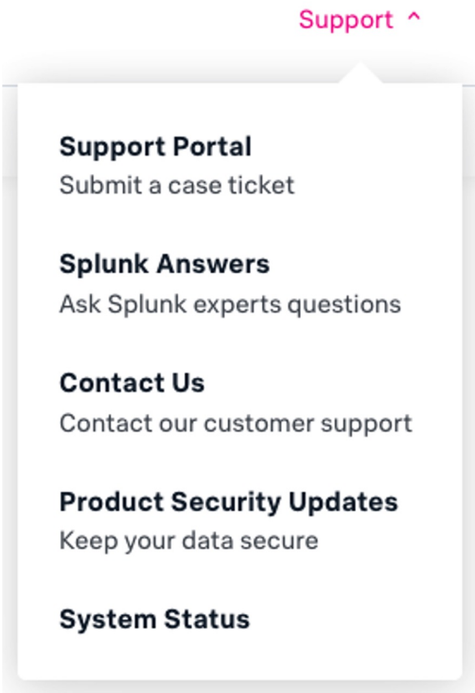
splunk>

References

- Splunk Community Portal – community.splunk.com
  - Answers
  - Discussions
  - Splunk Trust
  - User Groups
  - Ideas
- Splunk Blogs – splunk.com/blog/
- Splunk Apps – splunkbase.com
  - Apps
  - Curated Collections
- Splunk Docs on Twitter – twitter.com/splunkdocs
- Splunk Dev on Twitter – twitter.com/splunkdev
- Splunk on Slack – splk.it/slack
- .conf – conf.splunk.com

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 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 (cont.)

Knowledge Manager - Recommended Courses

Free eLearning courses are in blue and courses with an * 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>

Splunk Mobile

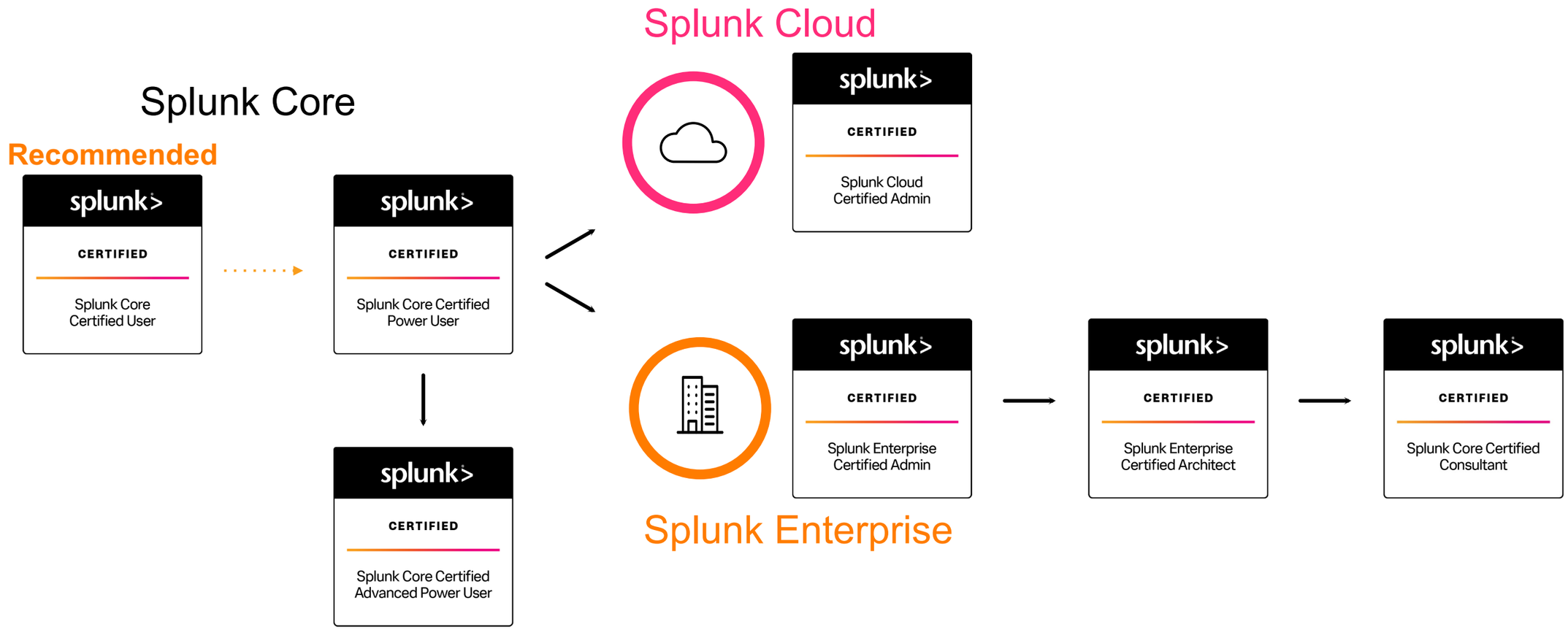
- Free app available to all Splunk Cloud and Splunk Enterprise customers
- Analyze data and receive actionable alerts on-the-go with mobile-friendly dashboards
- iOS and Android
- See the Product Brief

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 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:

- 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>

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>

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 Classic 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
- Creating Maps
- Introduction to Dashboards
- Dynamic Dashboards

Congratulations! You are a...

splunk>
CERTIFIED
Splunk Core Certified Consultant

Recommended Next Steps

- None

splunk>

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>

Splunk IT Service Intelligence Certified Admin

This certification demonstrates an individual's ability to deploy, manage, and use 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>

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™