Creating Maps

splunk>

© 2024 SPLUNK INC.

Before Taking This Course

- To be successful, students must have a working understanding of this course:
  - Intro to Splunk
  - Introduction to Dashboards
  - Dynamic Dashboards

© 2024 SPLUNK INC.

Course Objectives

- Use the `geostats`, `geom`, and `iplocation` commands
- Create and customize cluster maps
- Add interactivity to a map
- Create and customize choropleth maps
- Use choropleth SVGs on a dashboard

© 2024 SPLUNK INC.

Course Outline

- Module 1: Creating a Cluster Map
- Module 2: Adding a Choropleth Map
- Module 3: Customizing Maps
- Module 4: Using Choropleth SVG

© 2024 SPLUNK INC.

Module 1: Creating a Cluster Map

© 2024 SPLUNK INC.

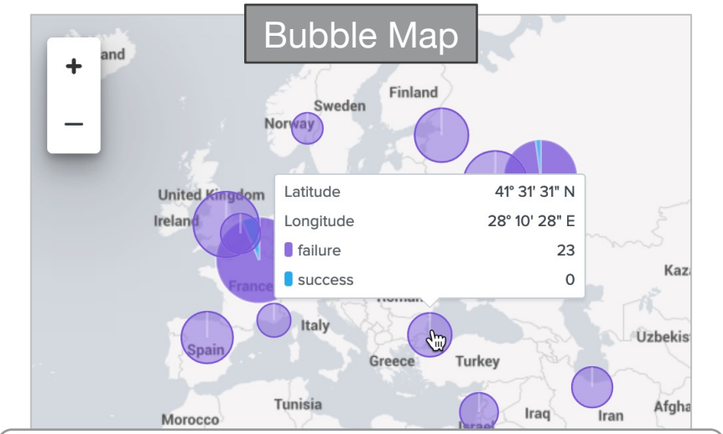
Module Objectives

- Define cluster map requirements
- Use the `geostats` and `iplocation` commands
- Create and format a cluster map

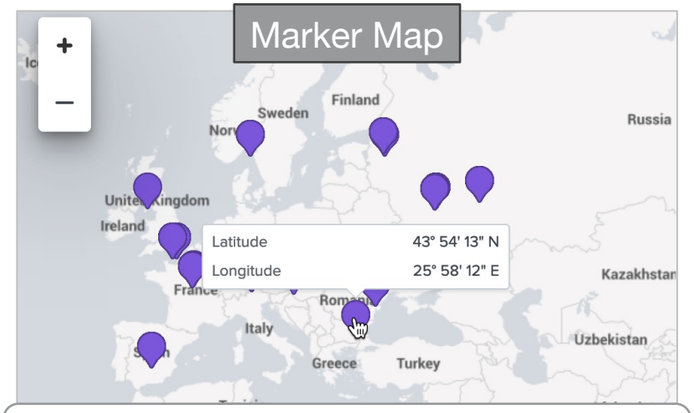
© 2024 SPLUNK INC.

Cluster Maps

- Group data based on location
- Two types: bubble and marker
  - Bubble maps visualize counts across geographic regions
  - Marker maps identify specific locations
    - Marker maps are available on dashboards only
- Requirements
  - Data with latitude and longitude values
    - If needed, use `iplocation` for these
  - Bubble maps require the `geostats` command
  - Marker maps require the `table` command




```
index=security sourcetype=linux_secure
| iplocation src_ip | geostats count by action
```




```
index=security sourcetype=linux_secure
| iplocation src_ip | table action lat lon
```

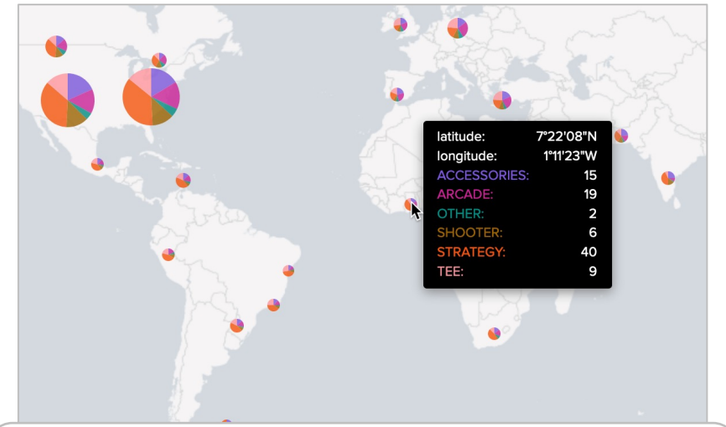

splunk>

© 2024 SPLUNK INC.

geostats Command – Bubble Maps

```
| geostats [latfield=string] [longfield=string] [globallimit=int] [binspanlat=<float> binspanlong=<float>]
[maxzoomlevel=<int>] function(<field>) [by <field>]
```

- Generates statistics clustered into geographic bins
  - Transforming command
  - Supports most `stats` aggregate numerical functions
- Requires data with latitude and longitude values
  - If needed use the `iplocation` command for these
- Arguments
  - Define the `latfield` and `longfield` only if they differ from the default `lat` and `lon` fields
  - Use `globallimit` to control the number of named categories added to each bubble. The default is 10.
  - Use `binspanlat`, `binspanlong` and `maxzoomlevel` to control the zoom level




```
index=sales sourcetype=vendor_sales
| geostats globallimit=5 latfield=VendorLatitude
longfield=VendorLongitude count by categoryId
```


splunk>

© 2024 SPLUNK INC.

iplocation Command

```
| iplocation <ip-address-fieldname> [prefix=<string>] [allfields=<bool>] [lang=<string>]
```

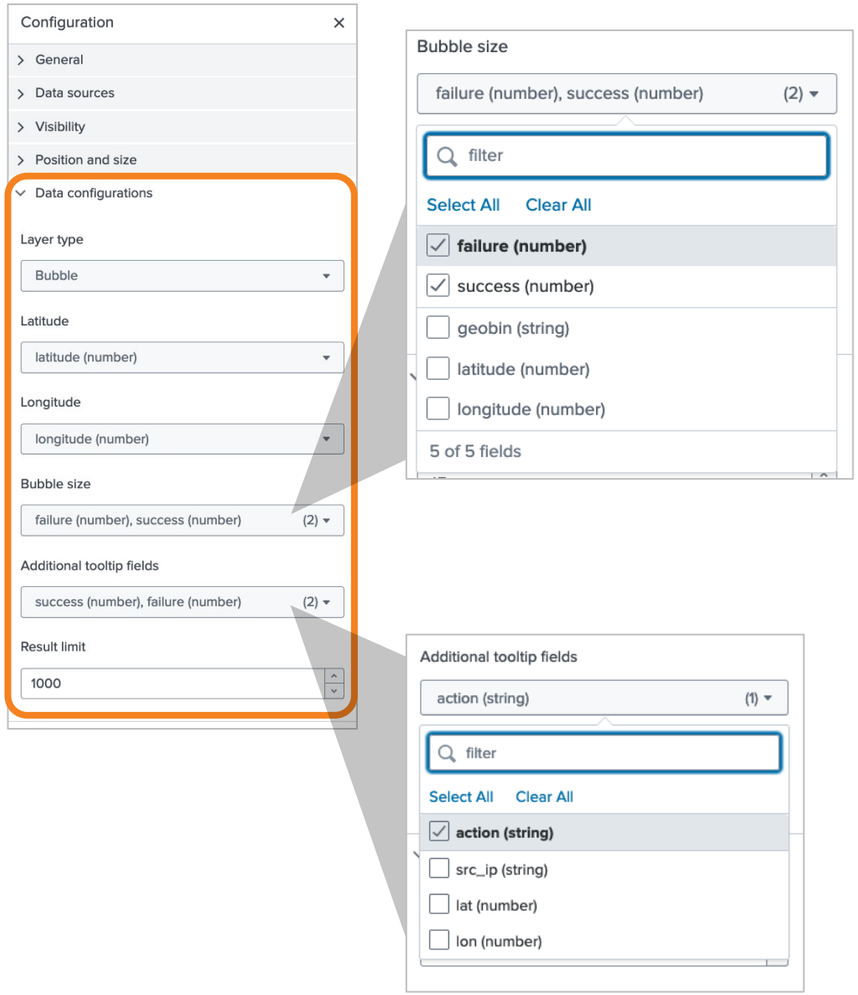
- Adds location data based on an event's IP address
  - lat and lon fields (required by the geostats command)
  - City, Country, Region fields
- Optional Arguments
  - prefix specifies a string to prefix the field name
  - allfields adds Continent, MetroCode, and Timezone fields
  - lang renders the resulting strings in different languages. For example, City, Country, and Region values
- Works with both IPv4 and IPv6
  - Geolocation using IP addresses determines approximate locations, not precise addresses


```
index=security sourcetype=linux_secure
| iplocation src_ip allfields=true
```

© 2024 SPLUNK INC.

Format a Cluster Map – Dashboard Studio

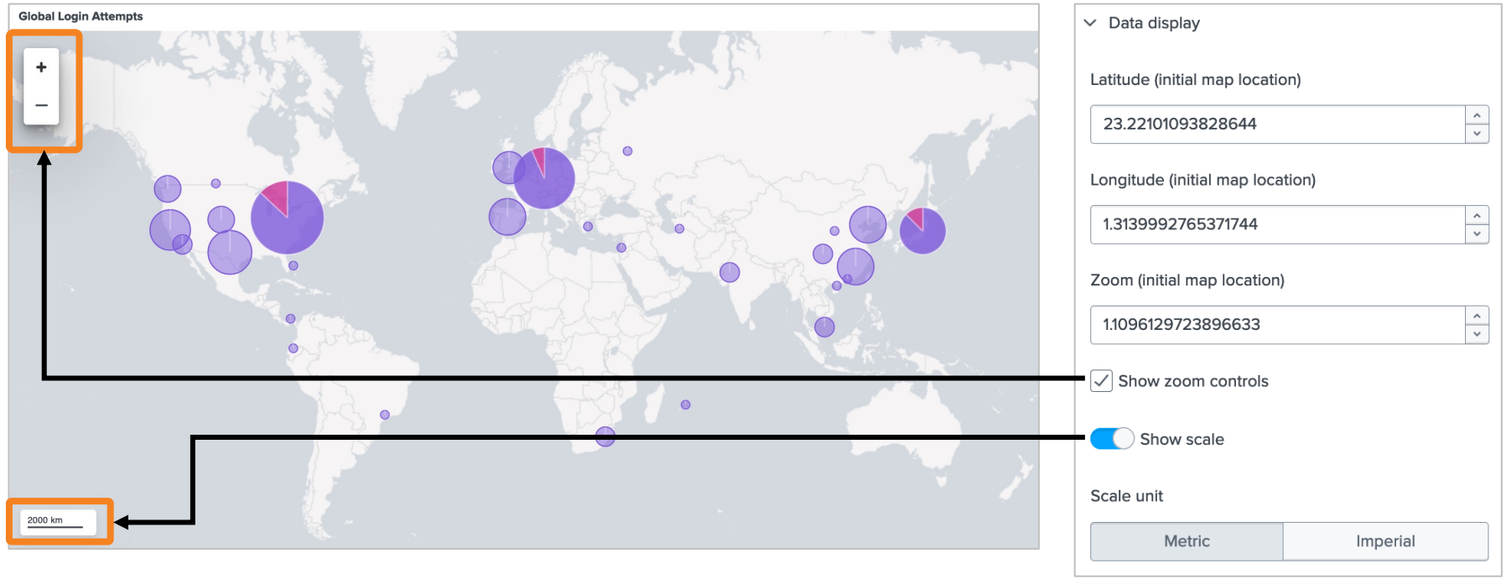
- Configuration Side Panel
  - Data Configurations
    - Layer type: marker or bubble
    - Latitude: data source for latitude values
    - Longitude: data source for longitude values
    - Bubble Size: data source for size (bubble map only)
    - Additional tooltip fields: fields from your search results



© 2024 SPLUNK INC.

Format a Cluster Map – Dashboard Studio (cont.)

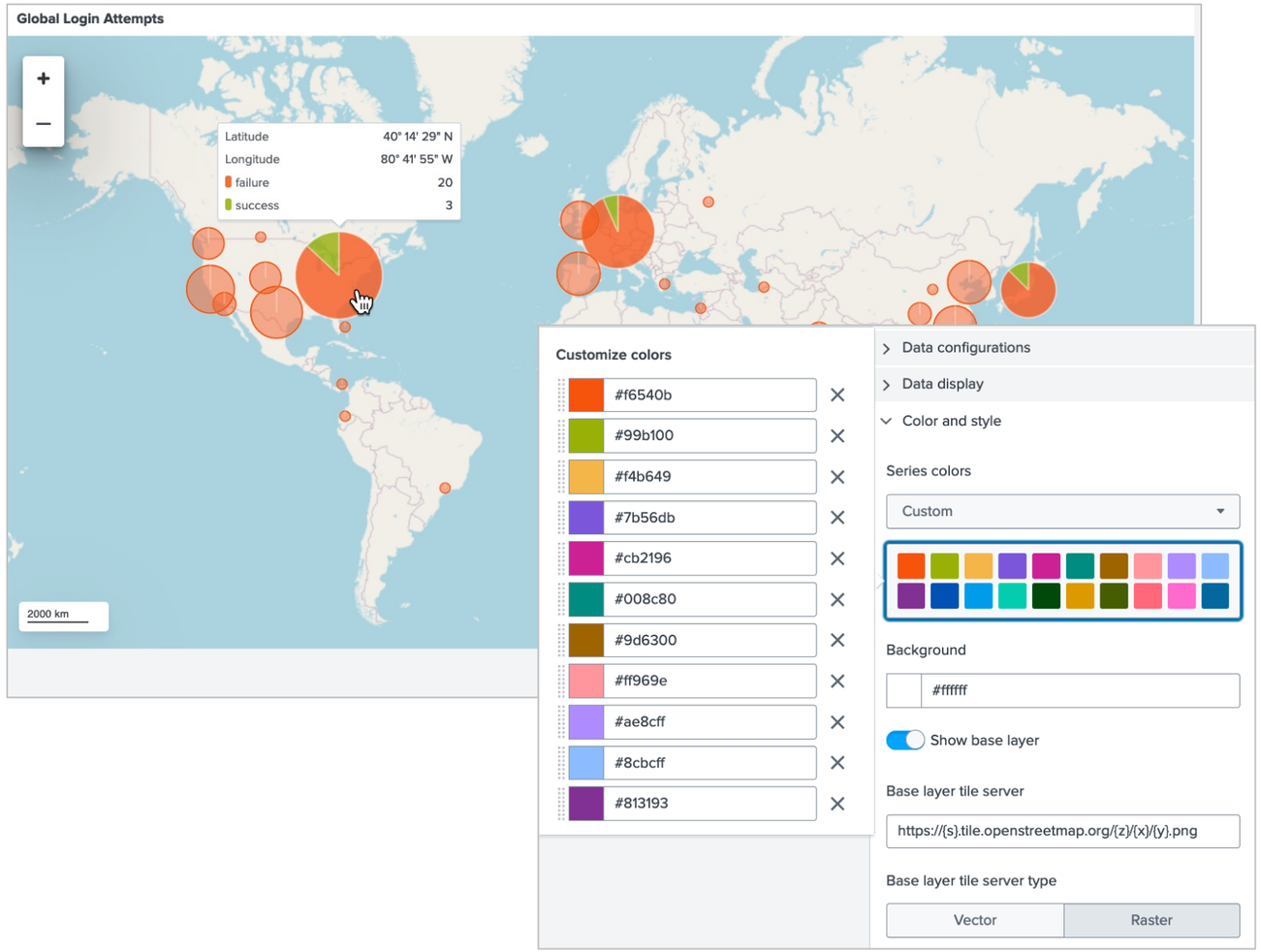
- Configuration Side Panel
  - Data Display
    - Default location
    - Zoom control visibility
    - Scale visibility



© 2024 SPLUNK INC.

Format a Cluster Map – Dashboard Studio (cont.)

- Configuration Side Panel
  - Color and Style
    - Series color
      - Re-order the default palette or add colors
    - Background
      - Set background color
      - Link to a custom map tile set



© 2024 SPLUNK INC.

`table` Command – Marker Maps

```
| table <field-list>
```

- Transforming command
- Non-streaming command
  - If a streaming command is needed, use the `fields` command
- A list of valid field names
  - Can be space-delimited or comma-delimited
  - Can use the asterisk (*) as a wildcard
- Renaming Fields
  - Only specify the fields that you want to show in your tabulated results
  - If renaming a field is needed, do it before piping the results to `table`

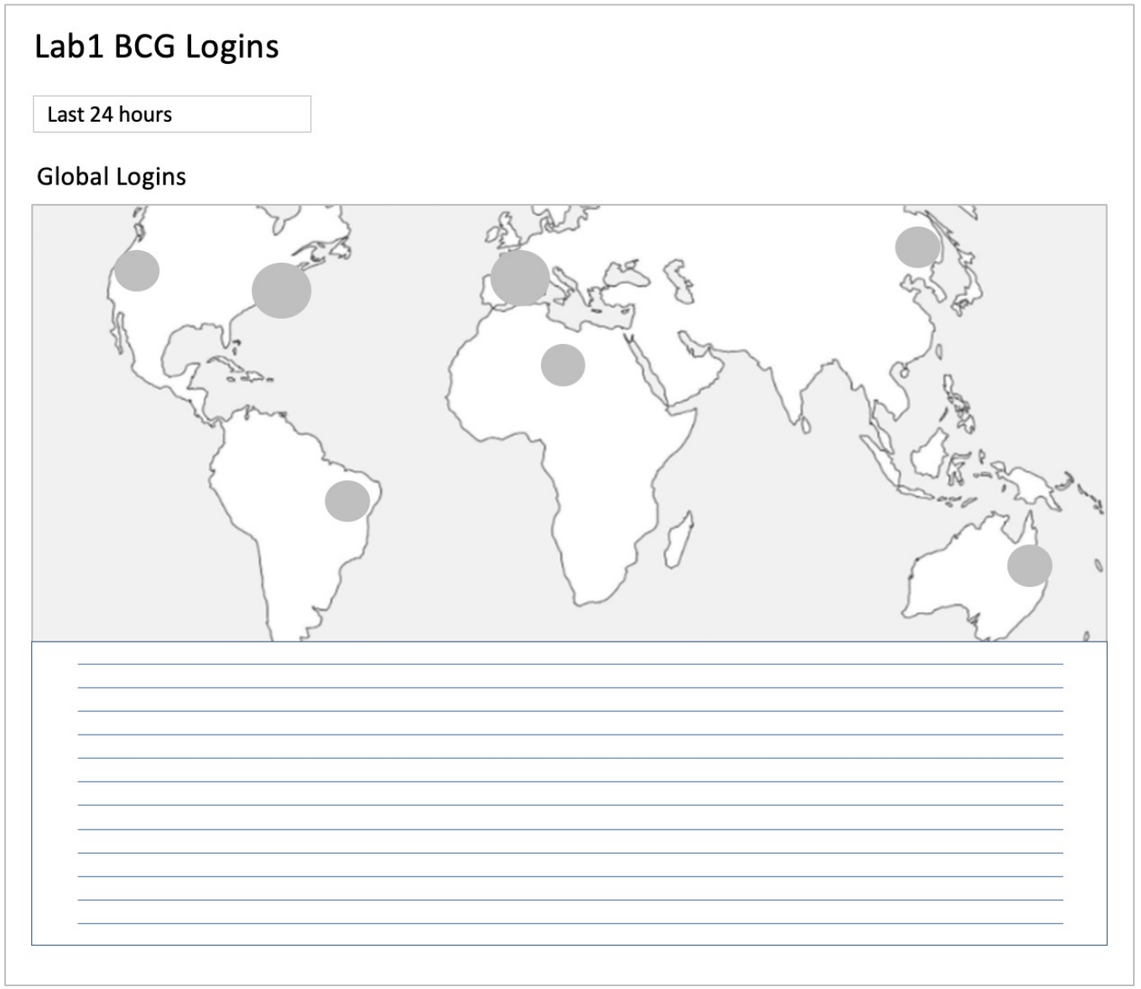

```
index=web sourcetype=access_combined
| iplocation clientip | table bytes lat lon
```


splunk>

© 2024 SPLUNK INC.

Lab Exercise 1

- Description: Create a cluster map
- Time: 15 minutes
- Tasks:
  - Create a bubble map search
  - Format a map
  - Save map to a dashboard
  - Add formatting
  - Add a table



© 2024 SPLUNK INC.

Module 2: Adding a Choropleth Map

© 2024 SPLUNK INC.

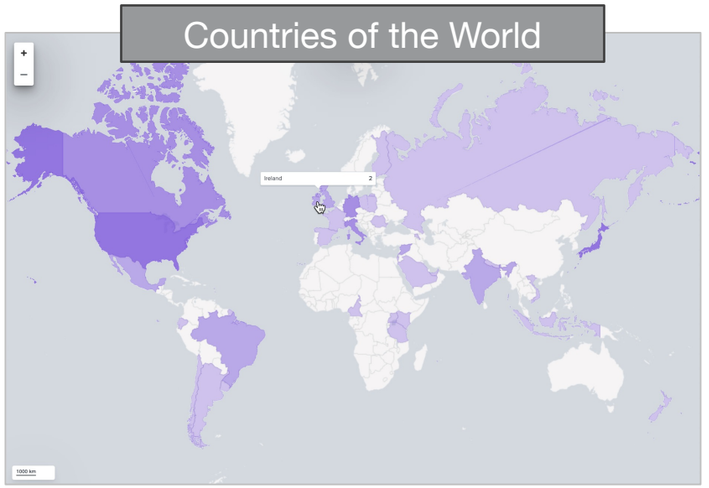
Module Objectives

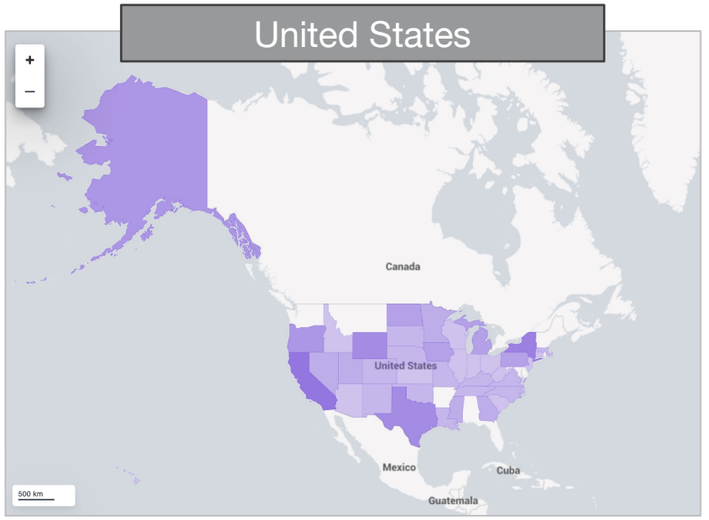
- Identify choropleth map requirements
- Define the `geom` command
- Create a choropleth map
- Format a choropleth map

© 2024 SPLUNK INC.

Choropleth Maps

- Metrics as shaded geographic regions
- Built-in maps
  - Geospatial lookups that work with the choropleth layer of the `splunk.map` visualization
    - United States
    - Countries of the world
- Import maps or create your own
  - Dashboard Studio with SVG files
    - SVG: Scalable Vector Graphic





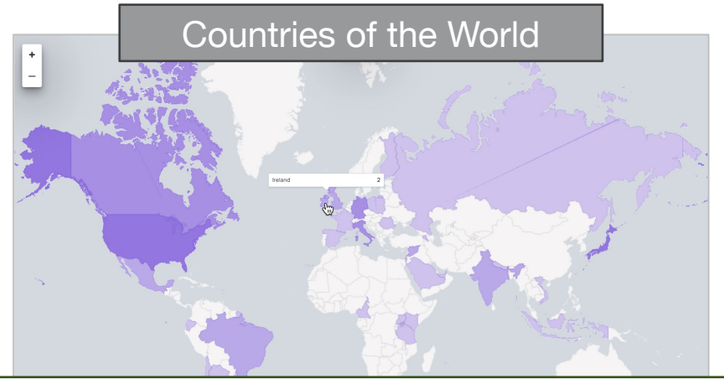
Note

Choropleth SVG is discussed in topic 4 of this course.

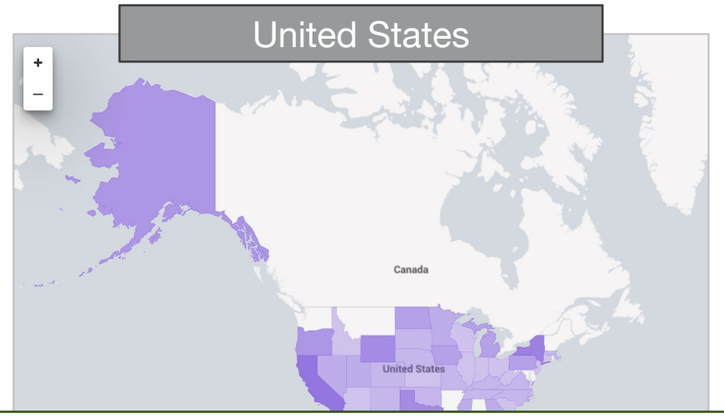
© 2024 SPLUNK INC.

Requirements

- Data with geographic information
  - Signed degree latitude and longitude coordinates
  - OR location names that match the location in a lookup
  - OR IP address field values that can generate `lat` and `lon` fields using the `iplocation` command
- Lookup Table File
  - Defines region boundaries, such as state or province
  - Built-in lookups for the United States or countries of the world
  - OR an uploaded KML or KMZ file for other places
- Geospatial Lookup
  - Matches coordinates to region definitions in the lookup
  - Built-in lookups for the United States or world countries
  - OR a custom geospatial lookup
- Transforming search
- `geom` command




```
index=sales sourcetype=vendor_sales
 | stats count by VendorCountry
 | geom geo_countries featureIdField=VendorCountry
```




```
index=sales sourcetype=vendor_sales VendorCountry="United States"
 | stats count by VendorStateProvince
 | geom geo_us_states featureIdField=VendorStateProvince
```

© 2024 SPLUNK INC.

Creating the Search

1. Use a transforming command to create a table
   - First column: geographic regions
   - Second column: numeric values

```
index=sales sourcetype=vendor_sales
| stats count by VendorCountry
```

20 Per Page ▾ | Format | Preview ▾ | < Prev | 1 | 2 | 3 | Next >

VendorCountry	count
Algeria	6
Andorra	4
Argentina	15
Armenia	5
Australia	11
Austria	3
Bahrain	3
Belarus	7
Belgium	3
Bermuda	3
Bolivia	5
Brazil	38
Burkina Faso	1
Cameroon	4
Canada	98
Chad	3
Chile	8
China	44

© 2024 SPLUNK INC.

Creating the Search – geom Command

```
...| geom [<featureCollection> [featureIdField=<string>]]
```

2. Pipe events to the geom command
   - Adds a field named geom with geographic data structure values for each event
3. Name a geospatial lookup as the featureCollection
4. Use the featureIdField argument to name a field in your events that has the featureId values

```
index=sales sourcetype=vendor_sales
| stats count by VendorCountry
| geom geo_countries featureIdField=VendorCountry
```

20 Per Page ▾ | Format | Preview ▾

VendorCountry	count	featureCollection	geom
Algeria	47	geo_countries	{"type":"MultiPolygon","coordinates":[[[[8 [8.357711791992188,36.43038558959961],[8.2 [8.236478805541992,34.64765548706055],[7.8 [8.086823463439941,33.09428787231445],[8.3 [9.286543846130371,30.117128372192383],[9. [9.721349716186523,27.2918758392334],[9.89 [10.032028198242188,24.856338500976562],[1 [7.482726097106934,20.872577667236328],[5. [3.2608134746551514,19.38832664489746],[3. [1.891387939453125,20.231788635253906],[1. [-4.516024589538574,24.803991317749023],[- [-7.1469340324401855,29.509239196777344],[

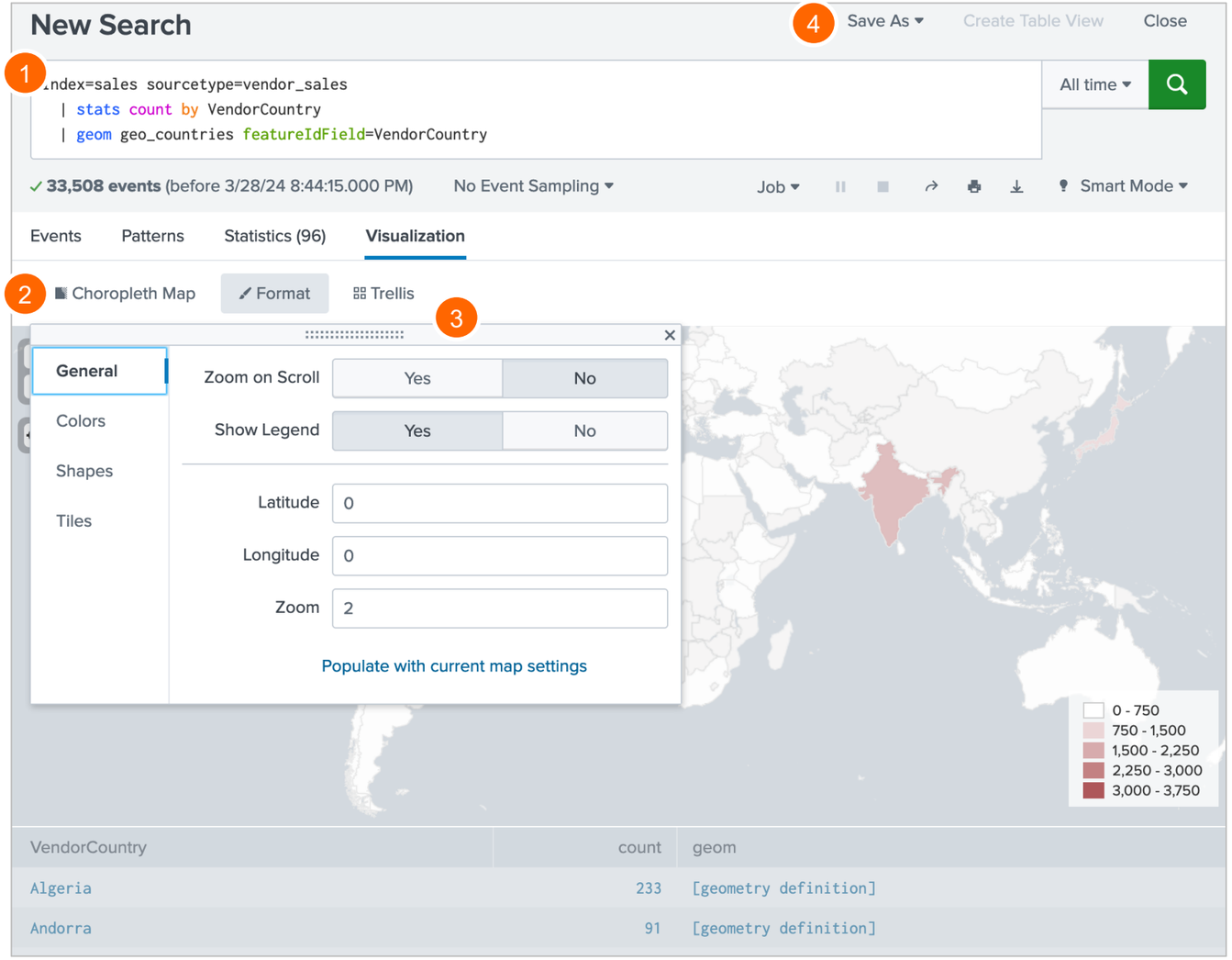
Note

Geographic data structures can be large.

splunk>

© 2024 SPLUNK INC.

Create a Choropleth Map – Search Page



1. Enter a search that includes a transforming command and uses the `geom` command to identify the `featureIdfield`
2. Select Choropleth Map from the type menu under the Visualization tab
3. Select the Format tab and make any changes to the defaults
4. Save to a report, alert, existing or new dashboard

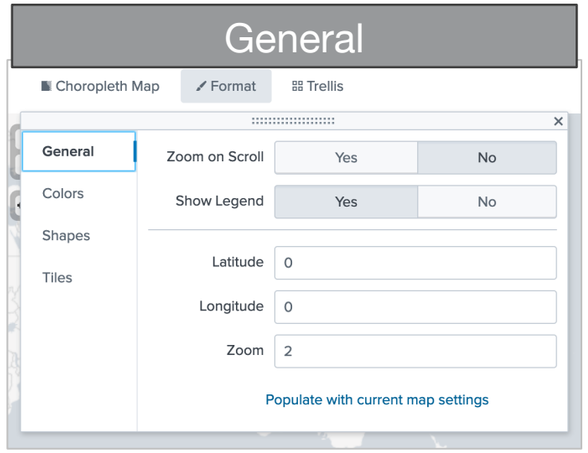
Note

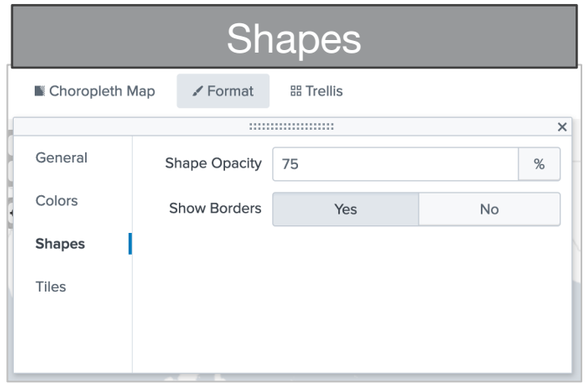
Default colors and color modes on the Search page are different than in choropleth map created in Dashboard Studio. Saving from the Search page to a dashboard retains these settings.

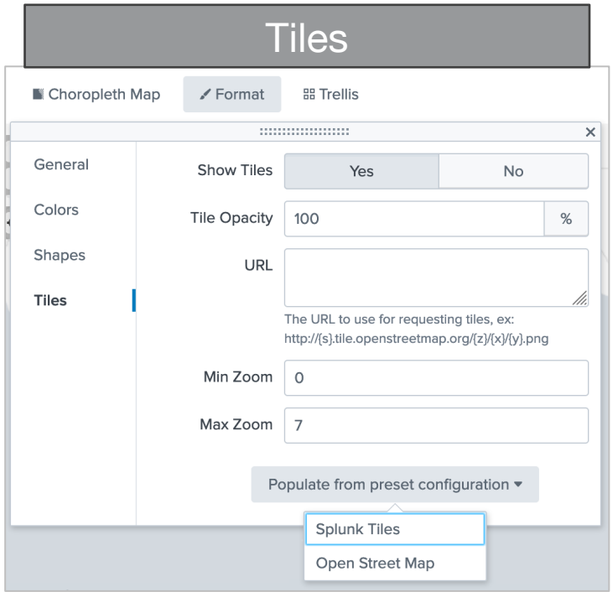
© 2024 SPLUNK INC.

Format a Choropleth Map – Search Page

- General
  - Zoom defaults
  - Show legend
- Shapes
  - Map shape opacity
  - Show borders
- Tiles
  - Show or hide map background features, such as oceans
  - Select a different tile set



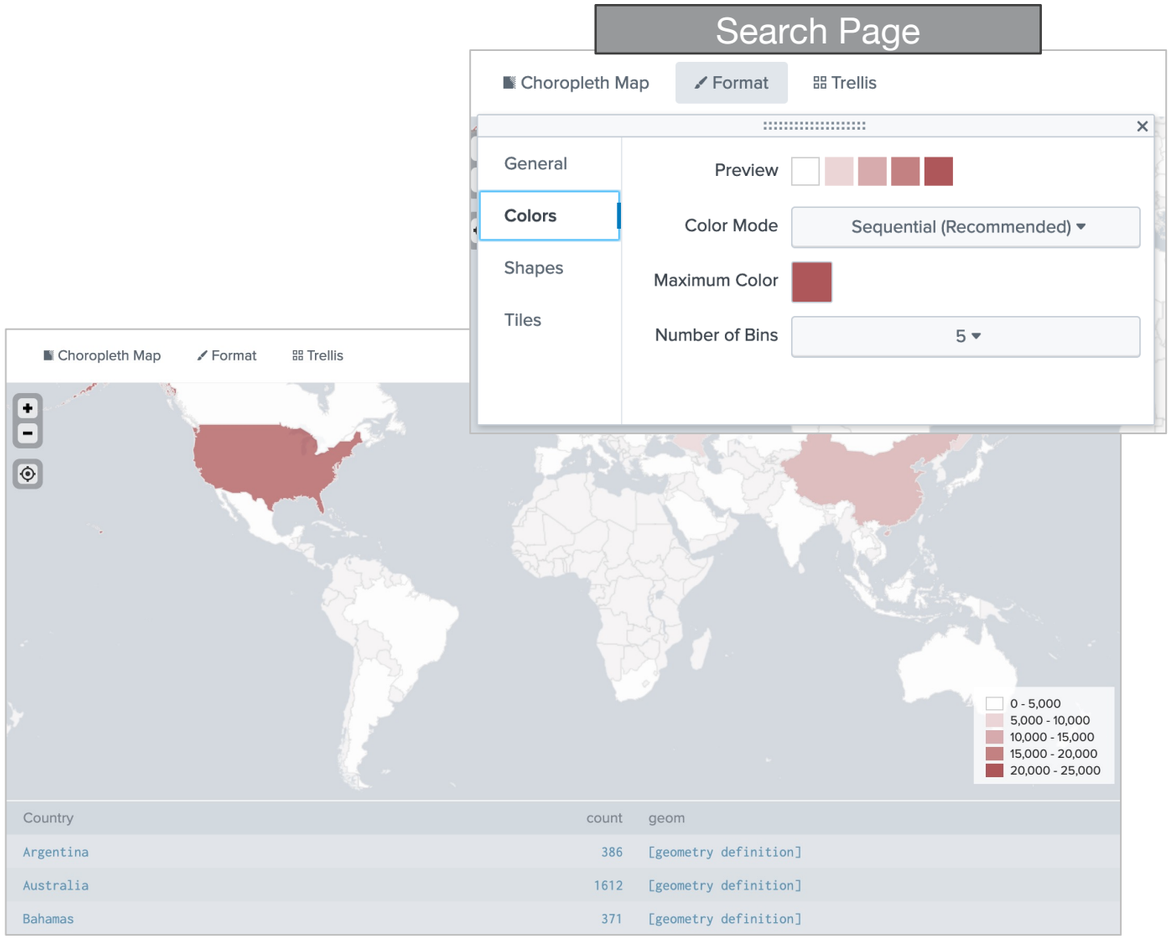




© 2024 SPLUNK INC.

Format a Choropleth Map – Search Page (cont.)

- Default Colors
  - Color: #AF575A
  - Color mode: Sequential (gradient)
    - Color by value
    - Light to dark shades of a single hue
  - A choropleth map saved from the search page to a dashboard will retain this default color

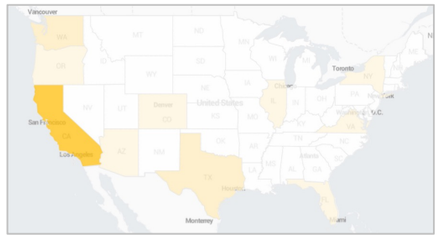


Note

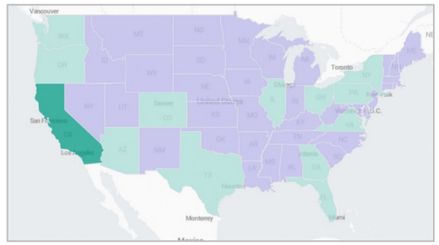
Custom colors are discussed in topic 3 of this course.

© 2024 SPLUNK INC.

Search Page Color Modes

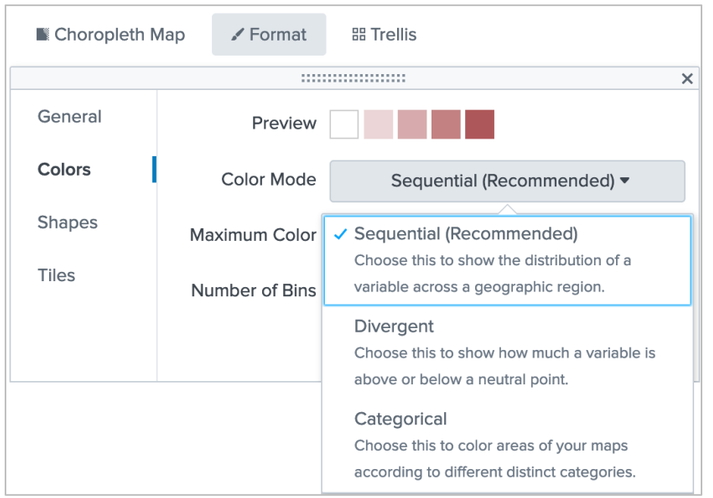


- Sequential
  - Color regions according to value with light to dark shades of a single color



- Divergent
  - Color regions according to high and low values with dark to light shades of two distinct colors
  - Color fades in the middle of the range

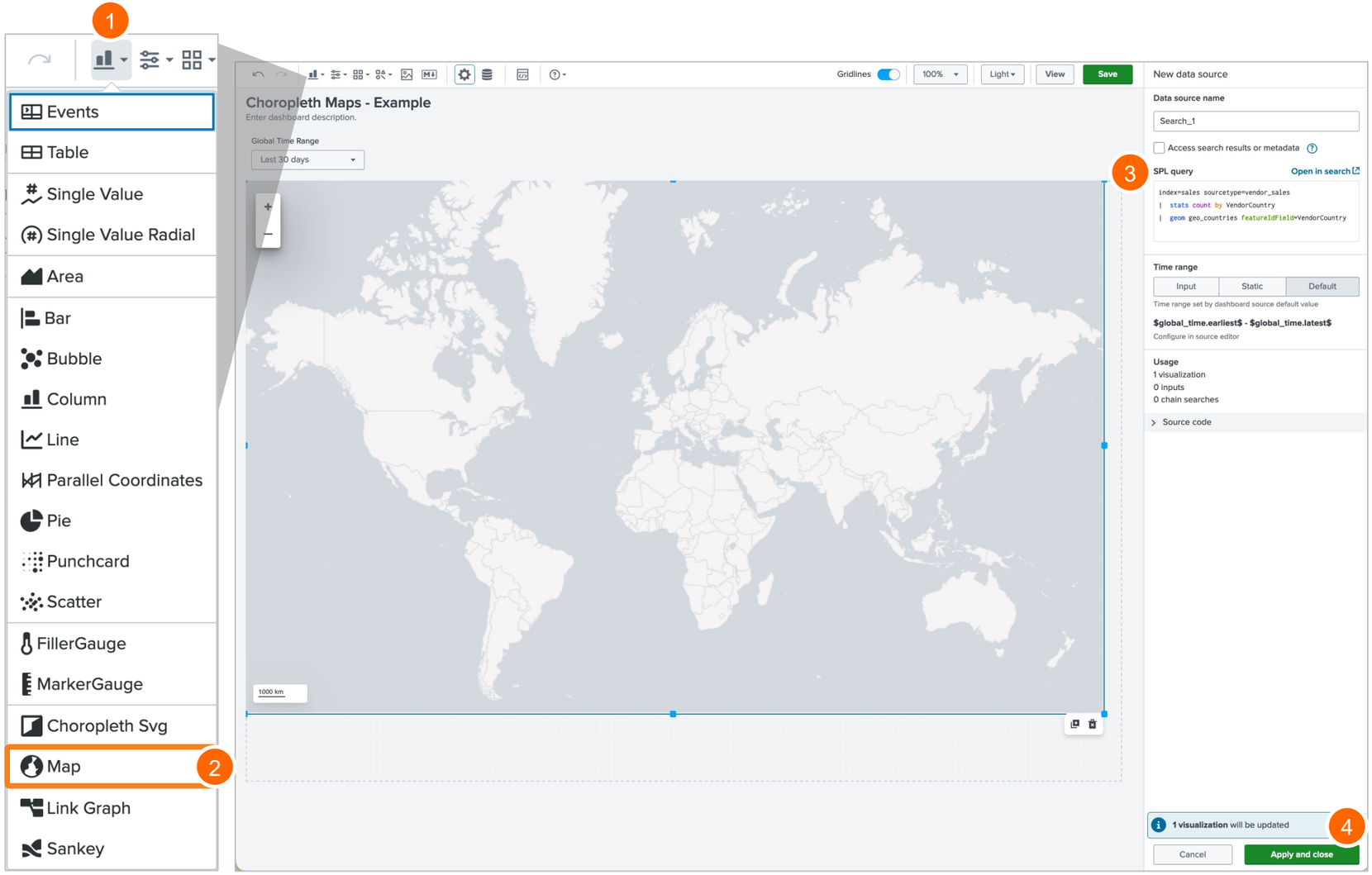
- Categorical
  - Color by category value
  - If multiple regions have the same category value, they share a color



© 2024 SPLUNK INC.

Create a Choropleth Map – Dashboard Studio

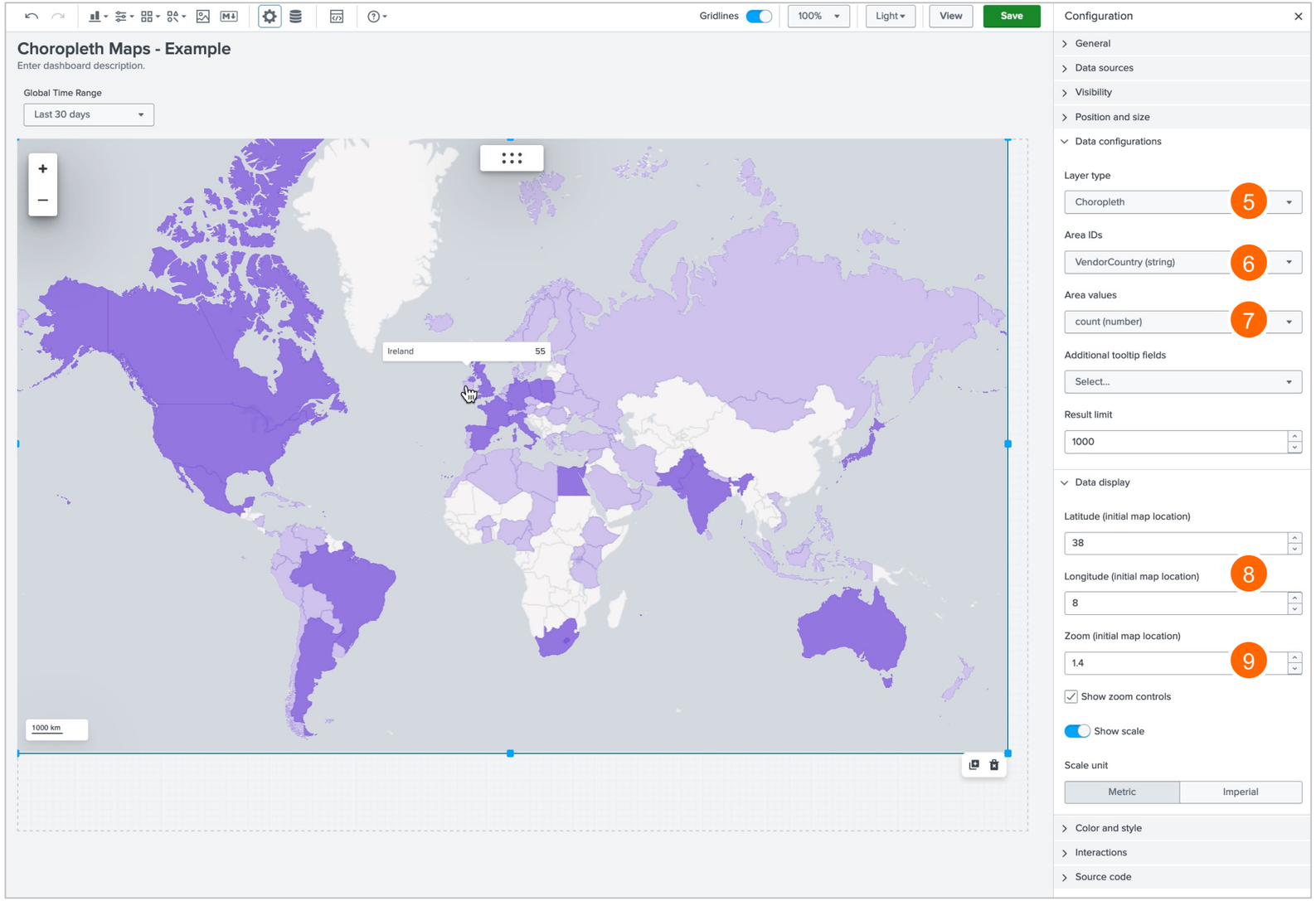
1. Click the chart button
2. Select Map
3. Enter a search that includes a transforming command and uses the `geom` command to identify the `featureIdfield`
4. Click **Apply and close**



© 2024 SPLUNK INC.

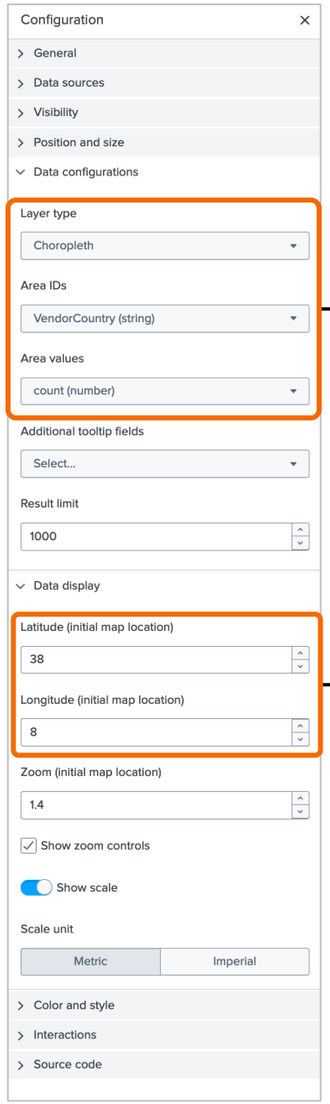
Create a Choropleth Map – Dashboard Studio

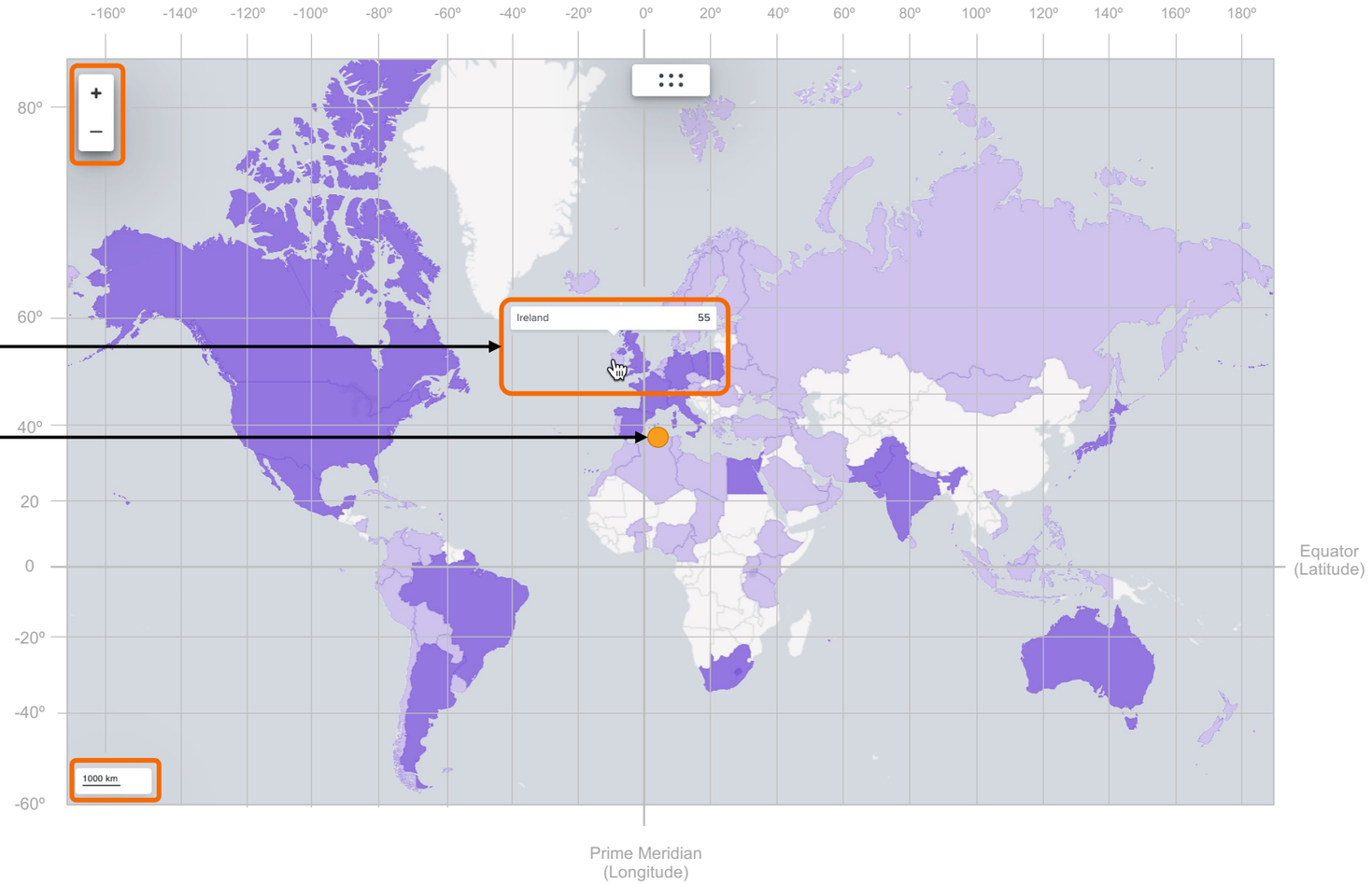
5. In the Data configurations section, select Choropleth in the Layer type menu
6. Select the field for Area IDs
7. Select the field for Area values
8. In the Data display section, set the default latitude and longitude
9. Set initial zoom level



© 2024 SPLUNK INC.

Create a Choropleth Map – Dashboard Studio

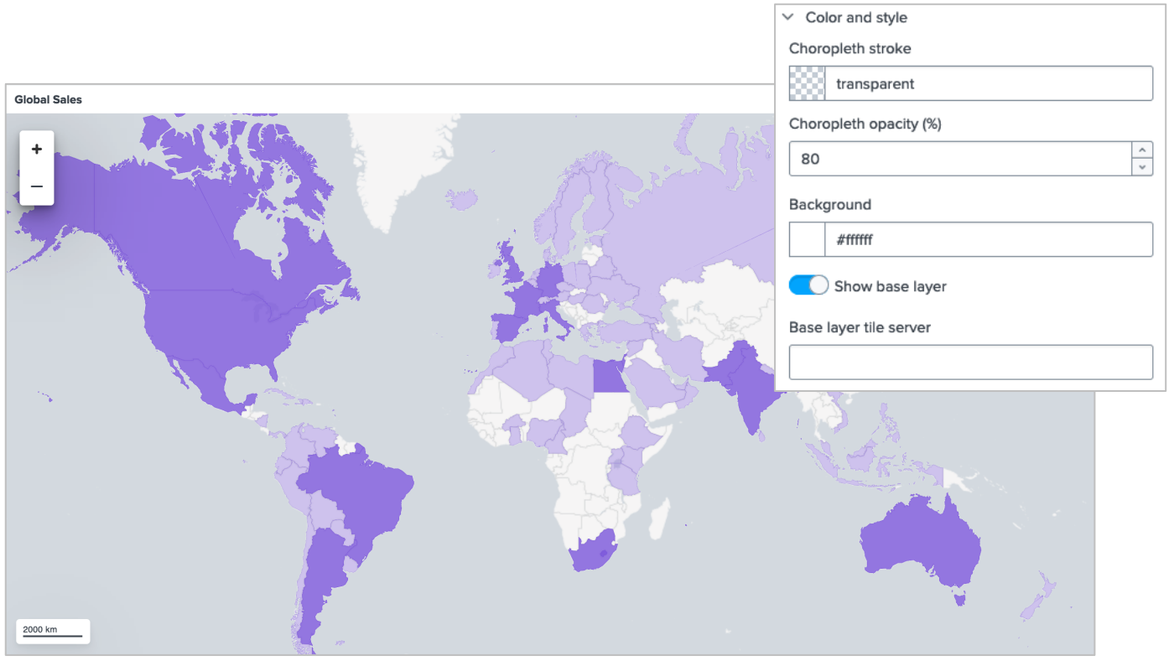




© 2024 SPLUNK INC.

Format a Choropleth Map – Dashboard Studio

- Default Colors
  - Color: #7B56DB
  - Color mode: sequential
    - Color by value
    - Light to dark shades of a single hue
- Stroke
- Opacity
- Background
- Tile Server



Note

Custom colors are discussed in topic 3 of this course.

© 2024 SPLUNK INC.

Lab Exercise 2

- Description Create a choropleth map
- Time: 15 minutes
- Tasks:
  - Create a choropleth map search
  - Save the map to a dashboard
  - Format the choropleth map

© 2024 SPLUNK INC.

Module 3: Customizing Maps

© 2024 SPLUNK INC.

Module Objectives

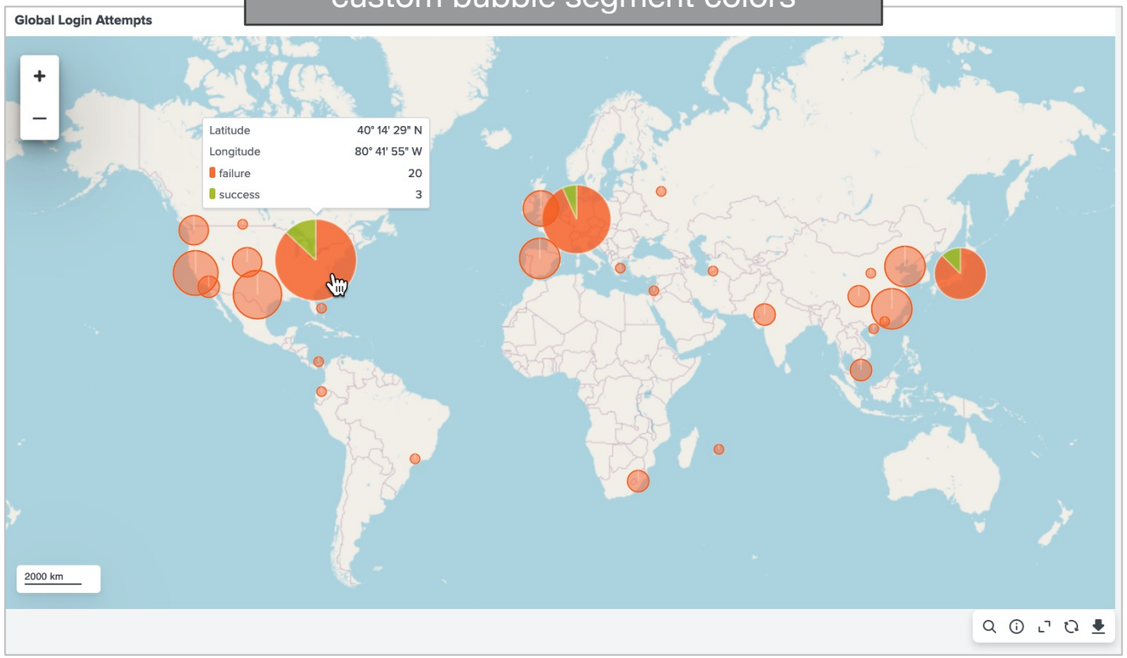
- Add custom colors to a cluster map
- Add custom colors to a choropleth map
- Use predefined map tokens with drilldowns

© 2024 SPLUNK INC.

Map Customization

- Dashboard Editor
  - Background color
  - Scale
  - Zoom level
  - Map tile set
  - Interactivity
  - Marker color
  - Bubble segment color
- Source code editor options
  - Marker and Choropleth Maps
    - Add a color that matches a value in a range
    - Add a color that matches an exact value
  - Choropleth Maps
    - Interpolation of colors based on total values

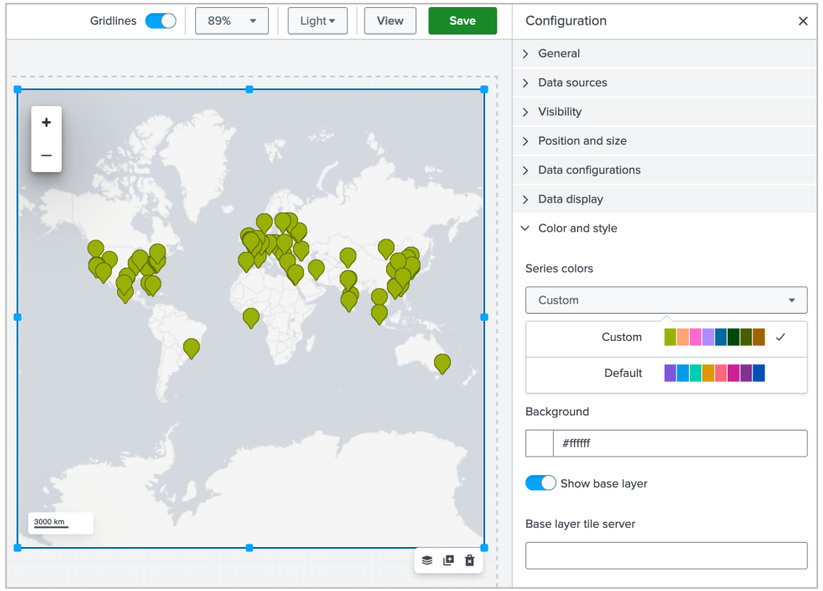
Example: Custom map tile set and custom bubble segment colors

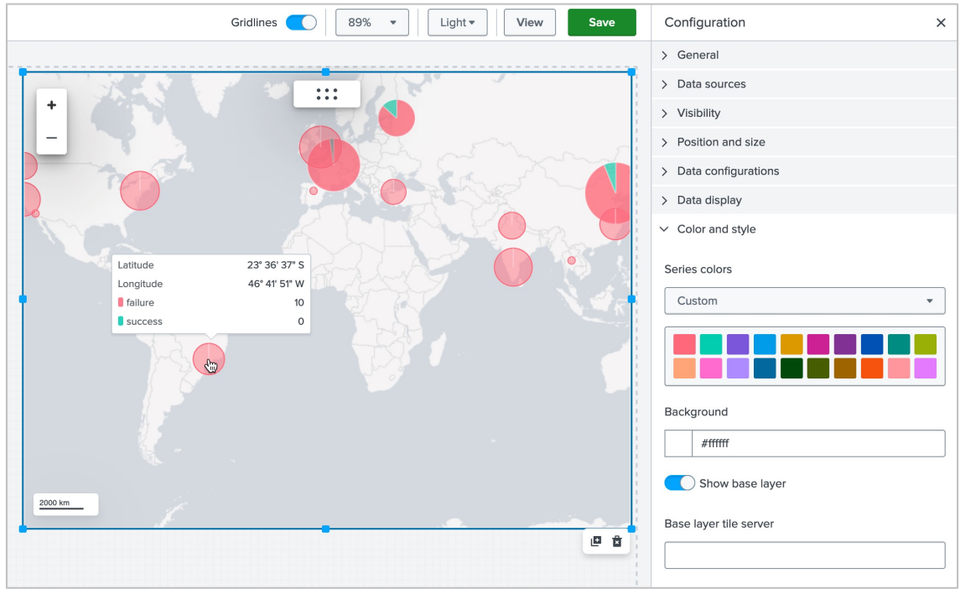


© 2024 SPLUNK INC.

Custom Map Colors – Dashboard Editor

- Use the Dashboard Editor's Color and style menu to specify colors used for data points on cluster maps
  - Custom marker color
  - Custom color for specific values

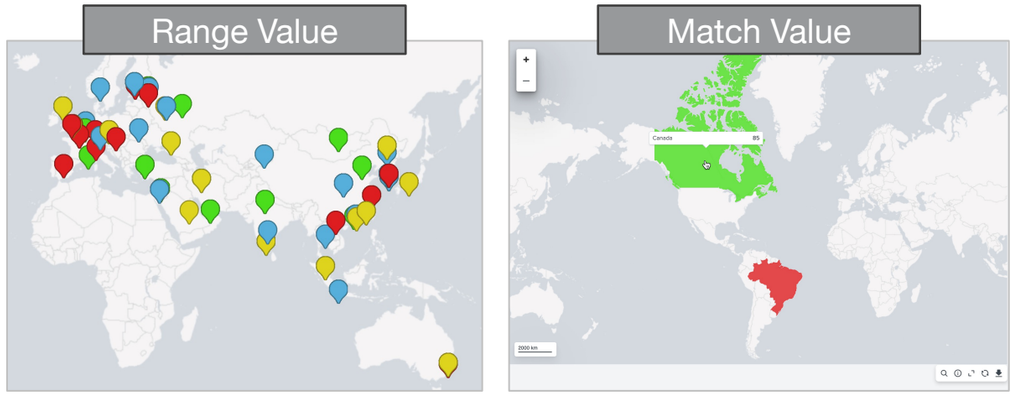


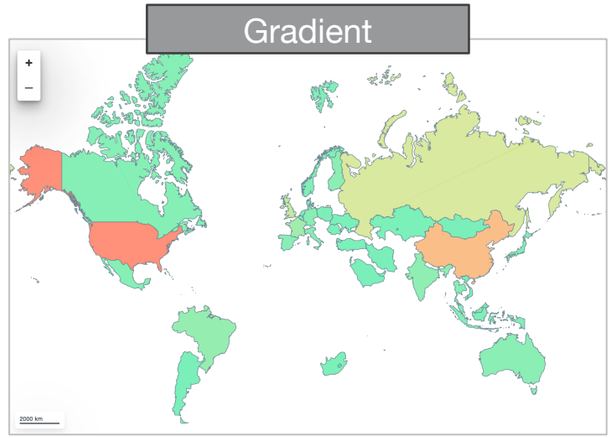


© 2024 SPLUNK INC.

Custom Map Colors – Dashboard Source Editor

- Choropleth and Marker Maps
  - `rangeValue`
    - Assigns a color to a range of values
  - `matchValue`
    - Assigns colors to an exact match of a value
- Choropleth Maps
  - `gradient`
    - Assigns the full color or a blend of colors based on the proximity of a region's value to a list of values and colors





© 2024 SPLUNK INC.

Dynamic Options Syntax (DOS)

- Syntax used in Dashboard Studio for visualization options
- The structure has four parts

```
"Option": "> [data source or viz option] | [selector function(s)] | [formatting function]"
```

DOS Part	What it does	Required?
Option name	Name of the option	Yes
Data source or visualization option	A data source, which can be a visualization data source such as a primary data source or visualization option such as areaValues.	Yes
Selector functions	Identifies the data from the data source associated with the visualization. A dynamic option can have one or multiple selector functions.	No
Formatting function	Formats the selected data.	Yes

© 2024 SPLUNK INC.

Marker Map – rangeValue

Use custom marker colors for a range of values

```
"dataColors":      "> primary    | seriesByName('bytes')            | rangeValue(myCustomColors)"
```

Add the dataColors option to the layers stanza

Identify the data source

Use the selector function seriesByName to identify the field values to use

Use the rangeValue formatting function and reference the name of the array of colors in the context stanza

```
"layers": [
  {
    "type": "marker",
    "latitude": "> primary | seriesByName('lat')",
    "longitude": "> primary | seriesByName('lon')",
    "dataColors": "> primary | seriesByName('bytes') | rangeValue(myCustomColors)"
  }
 ]
},
"context": {
  "myCustomColors": [
    {
       "from": 3001,
       "value": "#de1d20"
    },
    {
       "from": 2001,
       "to": 3000,
       "value": "#54afda"
    },
    {
       "from": 1001,
       "to": 2000,
       "value": "#ded41d"
    },
    {
       "to": 1000,
       "value": "#4ade1d"
    }
  ]
},
```

Note

Marker maps can use the dataColors or seriesColors options and default to seriesColors when nothing is defined.

splunk>

© 2024 SPLUNK INC.

Marker Map – matchValue

Use custom marker colors to match exact values

```
"dataColors":      "> primary    | seriesByName(count)          | matchValue(myCustomColors)"
```

Add the dataColors option to the layers stanza	Identify the data source	Use the selector function seriesByName to identify the field values to use	Use the matchValue formatting function and reference the name of the array of colors in the context stanza


```
"layers": [
  {
    "type": "marker",
    "latitude": "> primary | seriesByName('lat')",
    "longitude": "> primary | seriesByName('lon')",
    "dataColors": "> primary | seriesByName('count') | matchValue(myColorMatches)"
  }
 ]
},
"context": {
  "myColorMatches": [
    {
       "match": 4,
       "value": "#4ade1d"
    },
    {
       "match": 3,
       "value": "#54afda"
    },
    {
       "match": 2,
       "value": "#ded41d"
    },
    {
       "match ": 1,
       "value": "#de1d20"
    }
  ]
},
```

Note

Marker maps can use the dataColors or seriesColors options and default to seriesColors when nothing is defined.

splunk>

© 2024 SPLUNK INC.

Choropleth Map – gradient

Use custom region colors based on stops where values show the full color

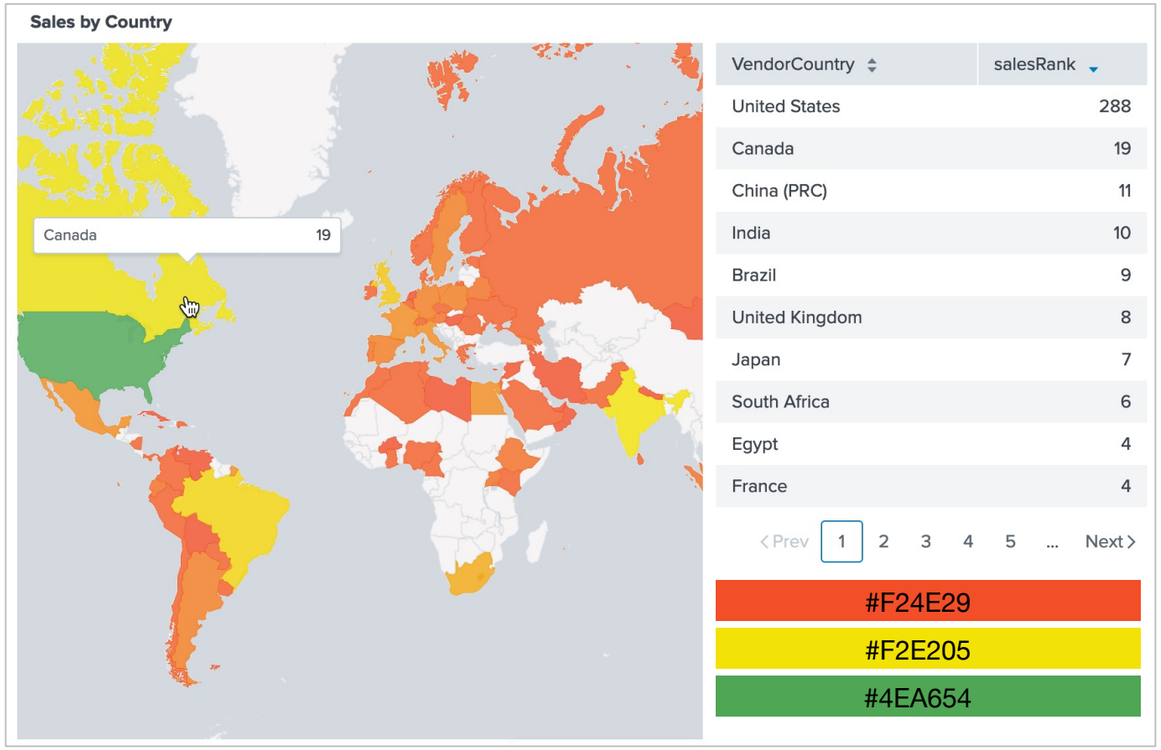
```
"dataColors":      "> primary    | seriesByIndex(1)                    | gradient(myCustomColors)"
```

Add the dataColors option to the layers stanza

Identify the data source

Use the selector function seriesByIndex to identify the column of data (index) to use

Use the gradient formatting function and reference the name of the array of colors in the context stanza




```
"viz_2o9siADk": {
  "type": "splunk.map",
  "options": {
   "layers": [
    {
      "type": "choropleth",
      "dataColors": "> primary | seriesByIndex(1) | gradient(myCustomColors)"
    }
  ]
},
"context": {
    "myCustomColors": {
      "stops": [
        0,
        10,
        250
      ],
      "colors": [
        "#F24E29",
        "#F2E205",
        "#4EA654"
      ]
    }
},
```

Note

Choropleth maps can only use the dataColors DOS option.

© 2024 SPLUNK INC.

Choropleth Map – rangeValue

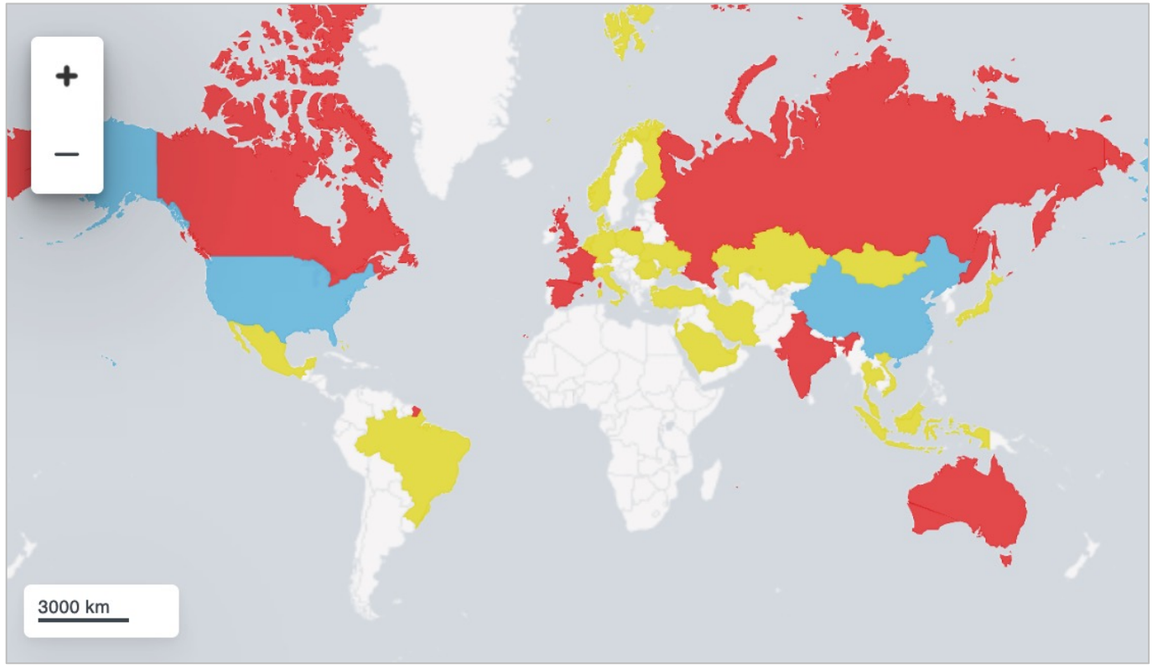
Use custom region colors for a range of values

```
"dataColors":          "> areaValues          | rangeValue(myCustomColors)"
```

Add the dataColors option to the layers stanza

Identify the visualization option

Use the rangeValue formatting function and reference the name of the array of colors in a context stanza




```
"viz_2o9siADk": {
  "type": "splunk.map",
  "options": {
    "layers": [
      {
        "type": "choropleth",
        "dataColors": "> areaValues | rangeValue(myCustomColors)"
      }
    ]
},
"context": {
    "myCustomColors": [
        {
            "from": 501,
            "value": "#54afda"
        },
        {
            "from": 101,
            "to": 500,
            "value": "#de1d20"
        },
        {
            "to": 100,
            "value": "#ded41d"
        }
    ]
},
```

Note

Choropleth maps can only use the dataColors DOS option.

splunk>

© 2024 SPLUNK INC.

Choropleth Map – matchValue

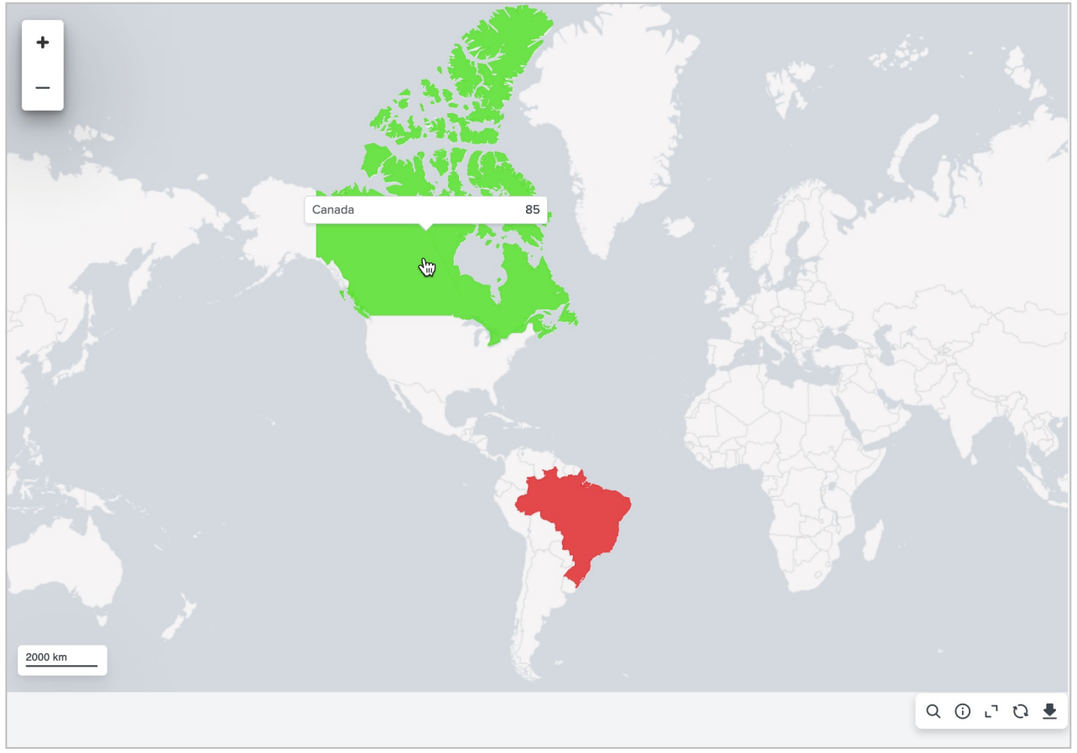
Use custom region colors to match exact values

```
"dataColors":          "> areaValues          | matchValue(myCustomColors)"
```

Add the dataColors option to the layers stanza

Identify the visualization option

Use the matchValue formatting function and reference the name of the array of colors in a context stanza




```
"viz_2o9siADk": {
  "type": "splunk.map",
  "options": {
  "layers": [
    {
      "type": "choropleth",
      "dataColors": "> areaValues | matchValue(myColorsMatches)"
    }
  ]
},
 "context": {
   "myColorsMatches": [
     {
       "match": 138,
       "value": "#de1d20"
     },
     {
       "match": 85,
       "value": "#54afda"
     }
   ]
 },
```

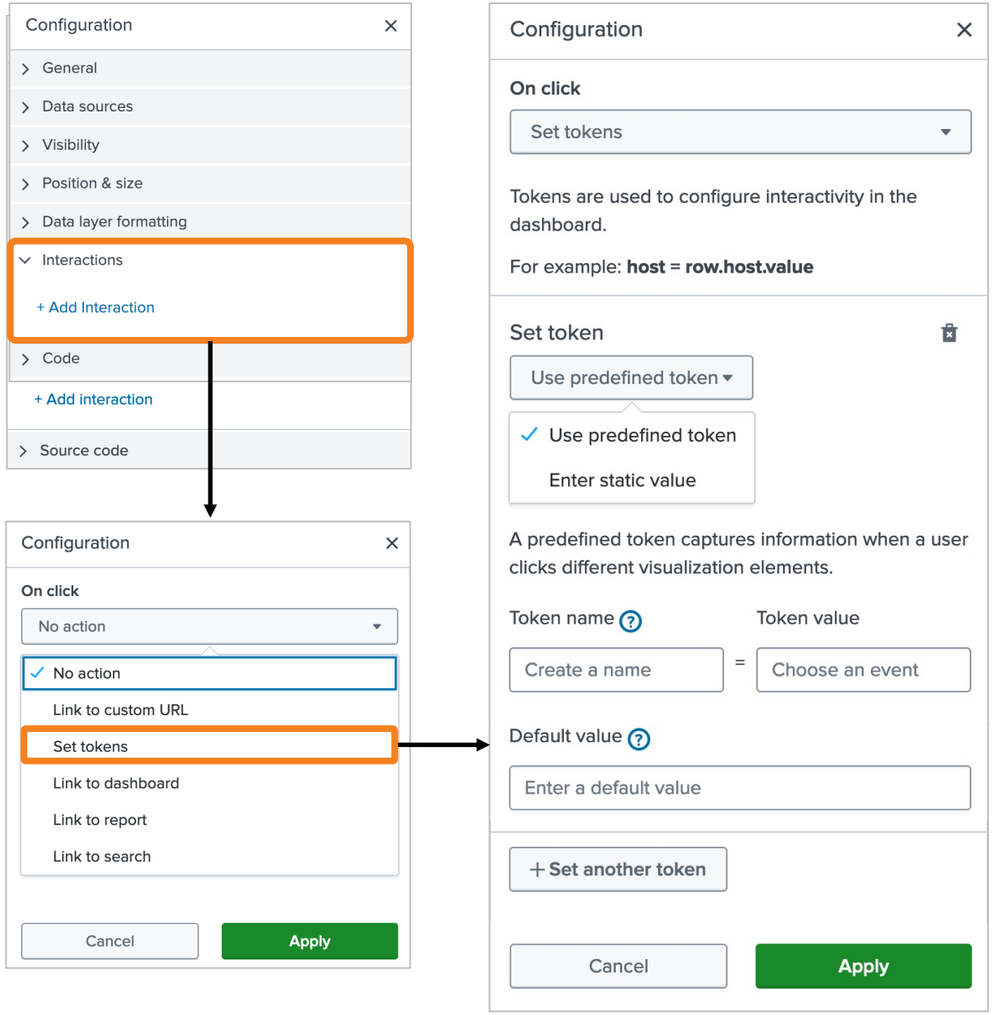
Note

Choropleth maps can only use the dataColors DOS option.

© 2024 SPLUNK INC.

Drilldowns

- Configuration Side Panel
  - Interactions
    - Link to a custom URL
    - Link to a dashboard, report, or search
    - Set tokens
      - Pass a value from a click to another visualization
      - Use predefined or static token values
      - Use $...$ delimiters to pass a token value



Note

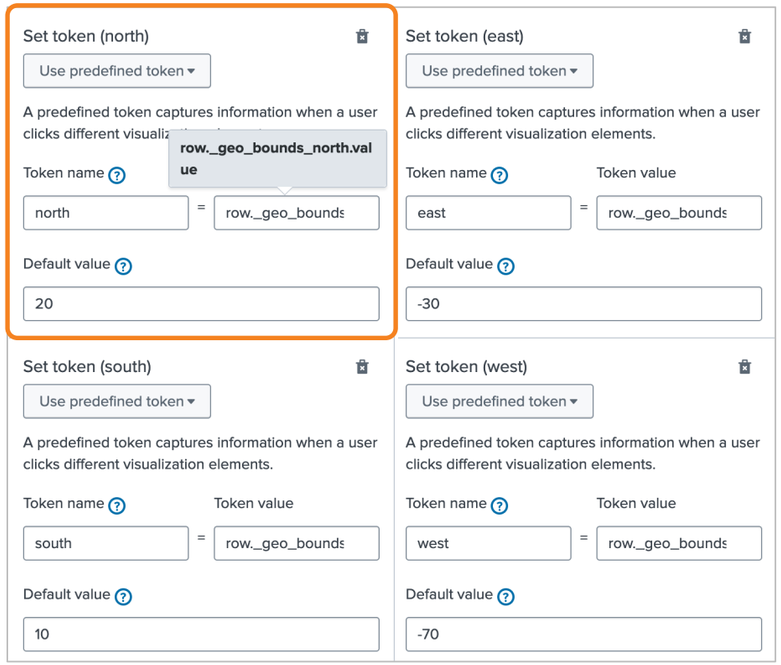
Linking to a search or report is new in Splunk 9.2.

© 2024 SPLUNK INC.

Set Map Tokens

- Predefined Bubble Map Tokens
  - Capture the outer boundaries of a location on a bubble map
  - A default value, other than a wildcard, is required

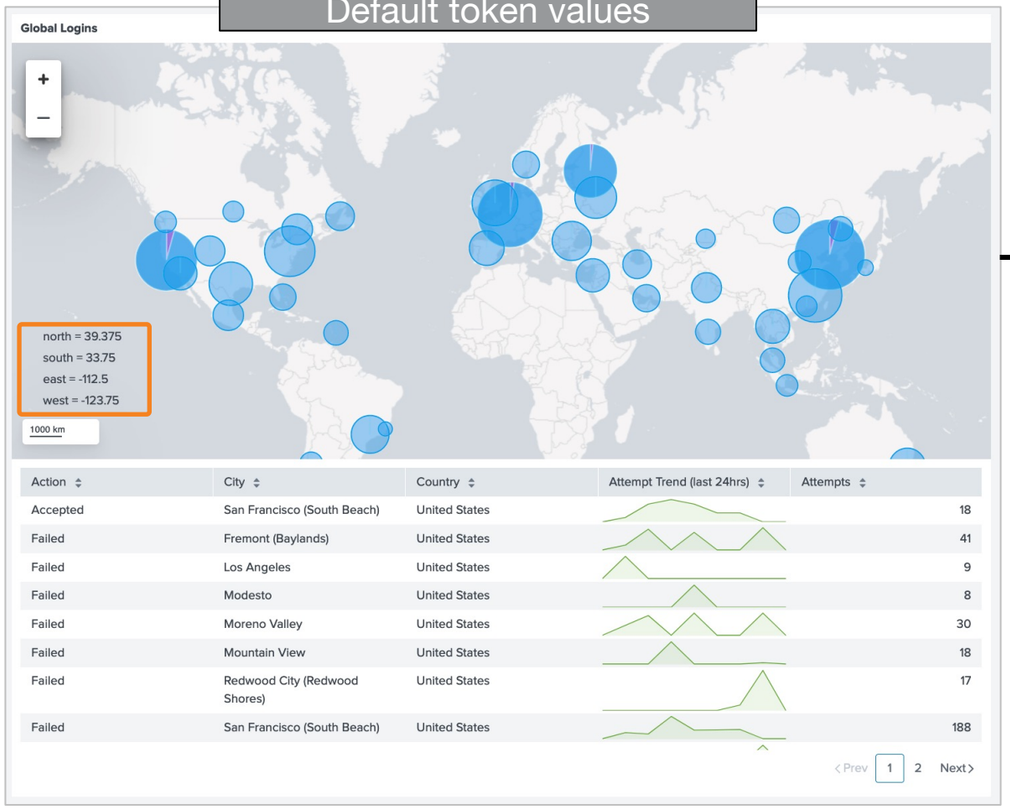
Token Names	Token Value	Default
north	row._geo_bounds_north.value	20
south	row._geo_bounds_south.value	-30
east	row._geo_bounds_east.value	10
west	row._geo_bounds_west.value	-70



© 2024 SPLUNK INC.

Set Map Tokens – Example

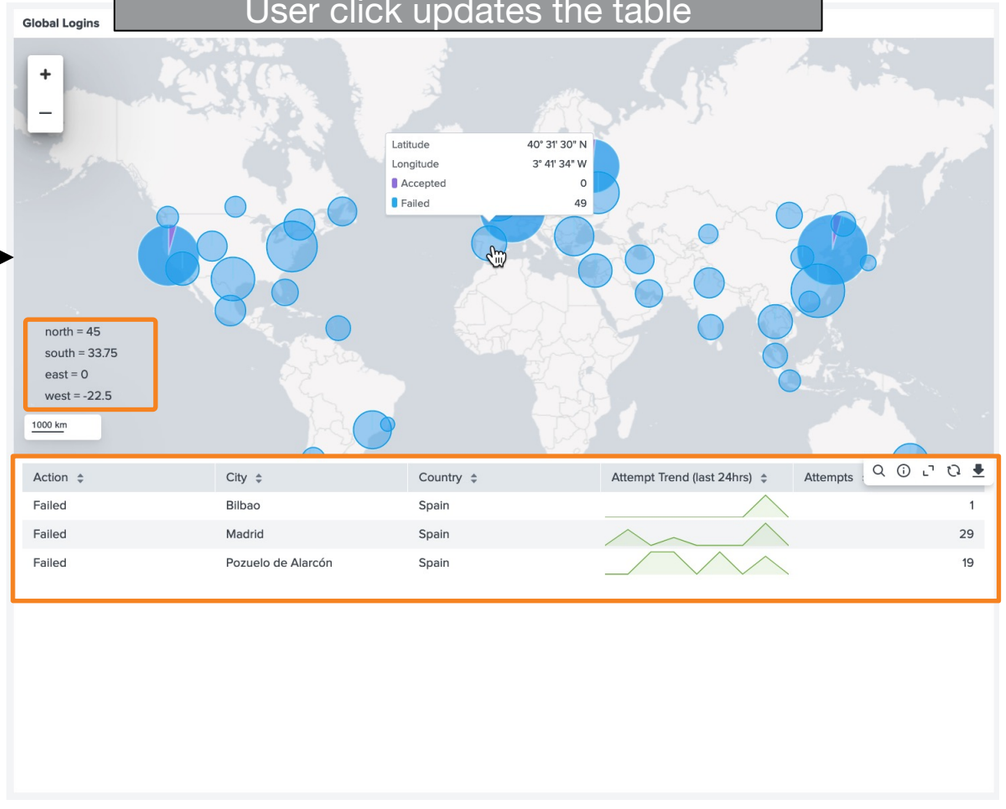
Default token values



Action	City	Country	Attempt Trend (last 24hrs)	Attempts
Accepted	San Francisco (South Beach)	United States		18
Failed	Fremont (Baylands)	United States		41
Failed	Los Angeles	United States		9
Failed	Modesto	United States		8
Failed	Moreno Valley	United States		30
Failed	Mountain View	United States		18
Failed	Redwood City (Redwood Shores)	United States		17
Failed	San Francisco (South Beach)	United States		188

Prev 1 2 Next

User click updates the table



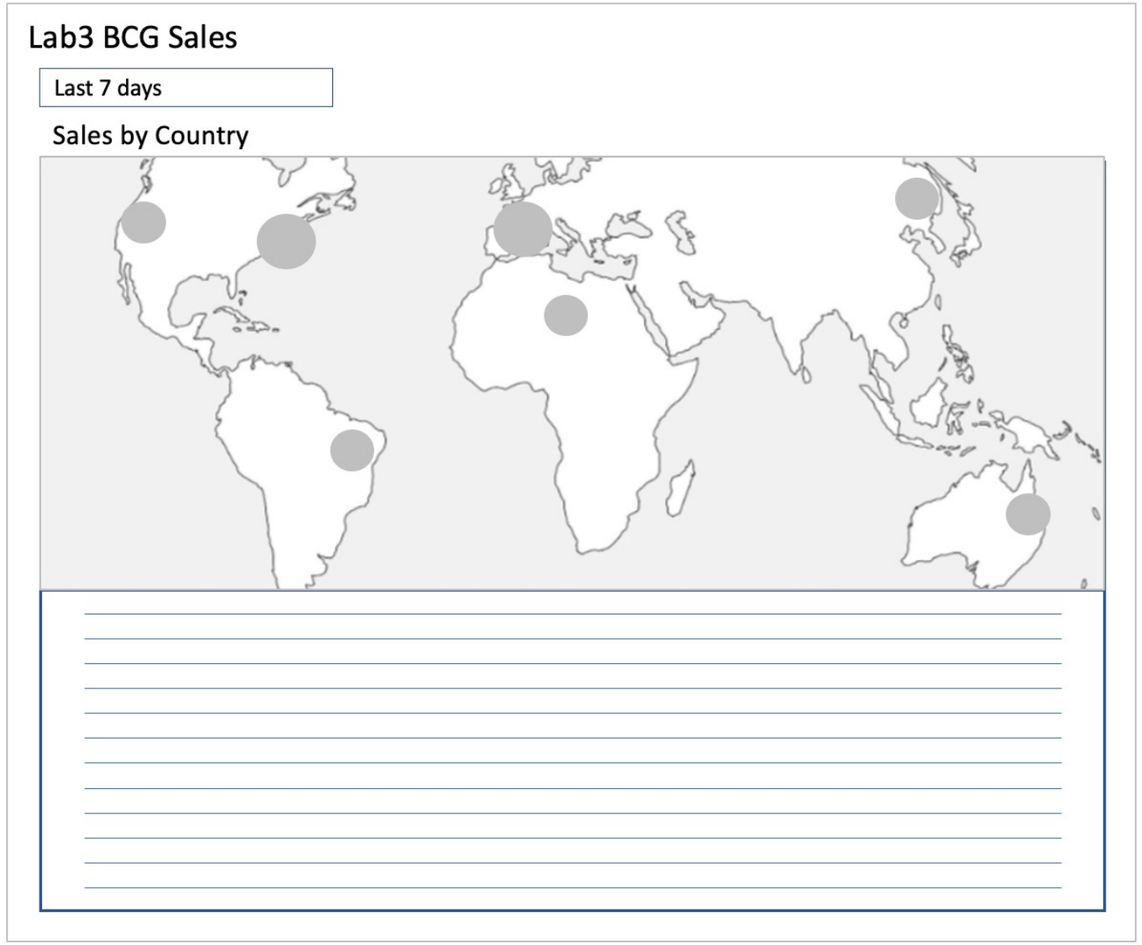
Action	City	Country	Attempt Trend (last 24hrs)	Attempts
Failed	Bilbao	Spain		1
Failed	Madrid	Spain		29
Failed	Pozuelo de Alarcón	Spain		19

```
index=security sourcetype=linux_secure
| iplocation src_ip
| search lat>=$south$ lat<$north$ lon>=$west$ lon<$east$
| stats sparkline(count(vendor_action),24h) AS "Attempt Trend (last 24hrs)" count AS Attempts by vendor_action, City, Country
| rename vendor_action AS Action
```

© 2024 SPLUNK INC.

Lab Exercise 3

- Description: Customize a bubble map
- Time: 15 minutes
- Tasks:
  - Create a bubble map
  - Add map tokens
  - Add a table



© 2024 SPLUNK INC.

Module 4: Using Choropleth SVG

© 2024 SPLUNK INC.

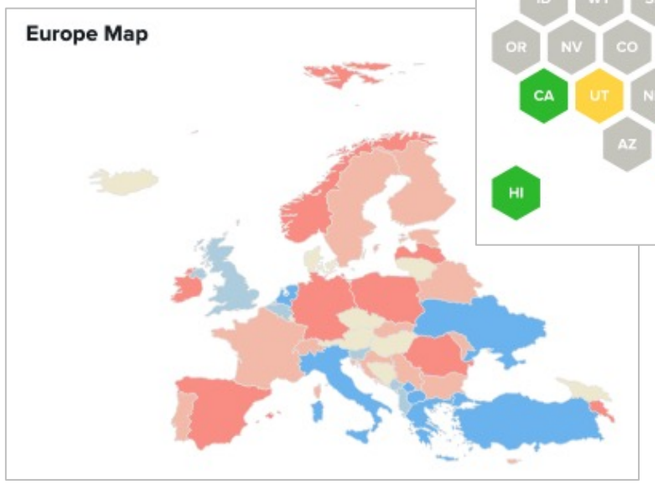
Module Objectives

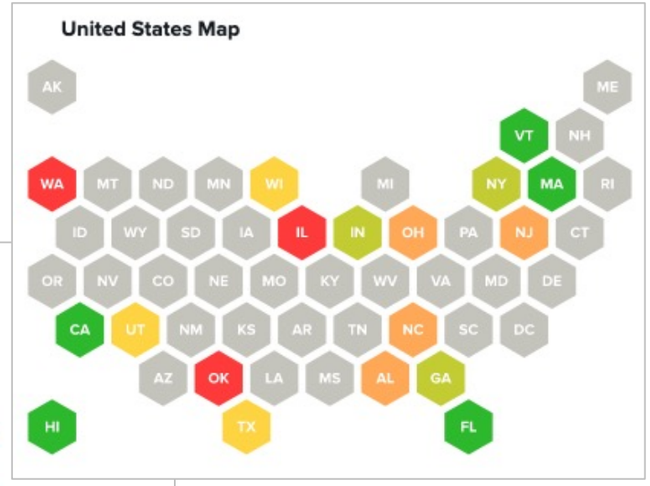
- Define choropleth SVG requirements
- Create a choropleth SVG
- Assign color ranges to a choropleth SVG

© 2024 SPLUNK INC.

Choropleth SVG

- Create custom images that are backed by a data source and dynamically colored
- SVG (Scalable Vector Graphic)
  - XML-based files used to render images
  - Contain paths that define shapes
  - For example, diagrams, icons, floor plans, and maps
- Only admins, sc_admins, and power users can upload or delete images

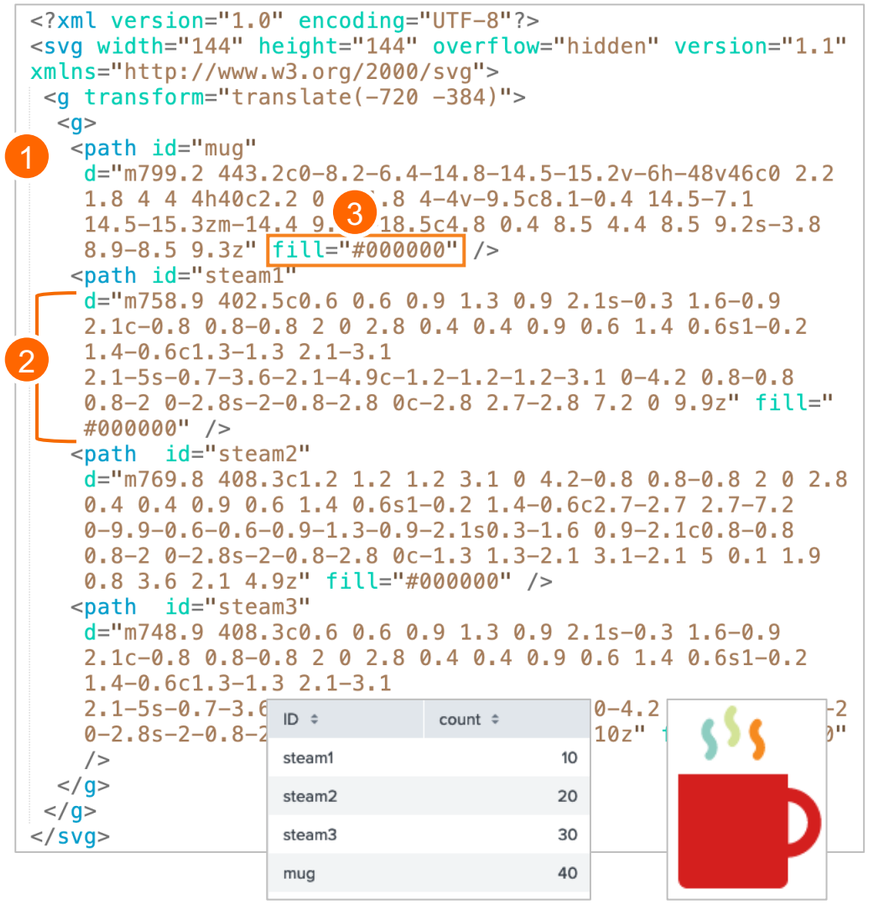




© 2024 SPLUNK INC.

Choropleth SVG File Requirements

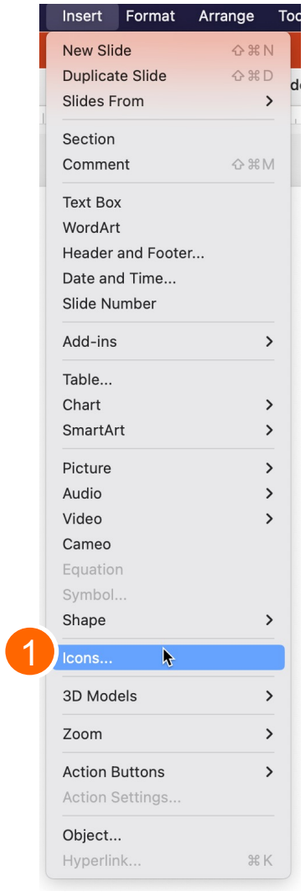
1. `path id` element: the name used here should match a field name in your data
   - This links the area defined to your data
2. `d` attribute: determines the shape of the outline using pixel positioning
3. `fill` attribute: provides a field for a color hexadecimal reference
   - When data is available this hexadecimal is replaced by those used in the Dashboard Editor Color and style settings
   - When no data is available the hexadecimal in the SVG file is used

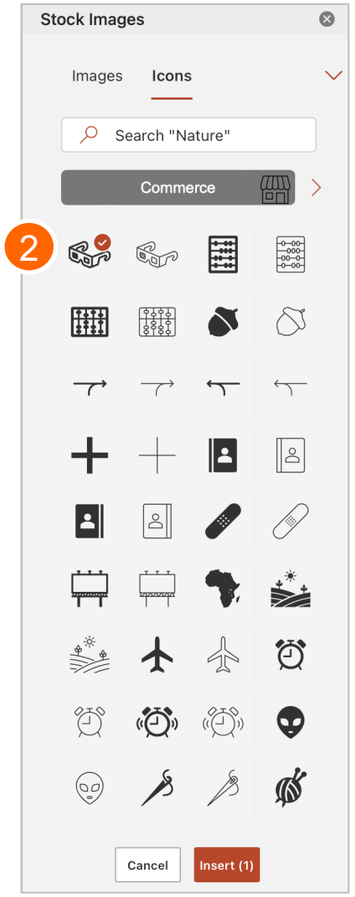


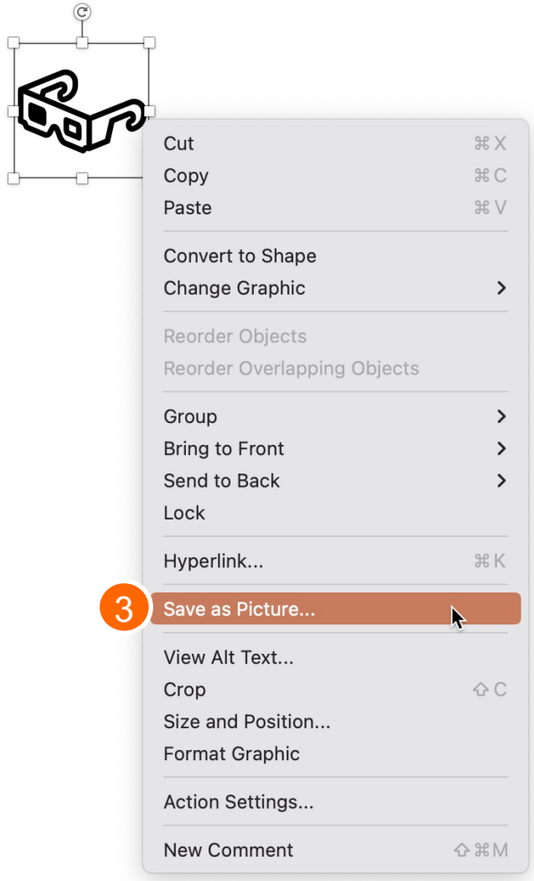
© 2024 SPLUNK INC.

Creating a Choropleth SVG – Example 1

PowerPoint

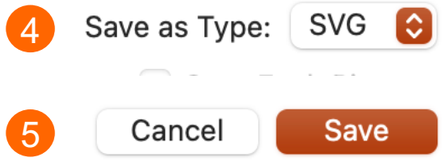






Export an icon as an SVG file from Powerpoint:

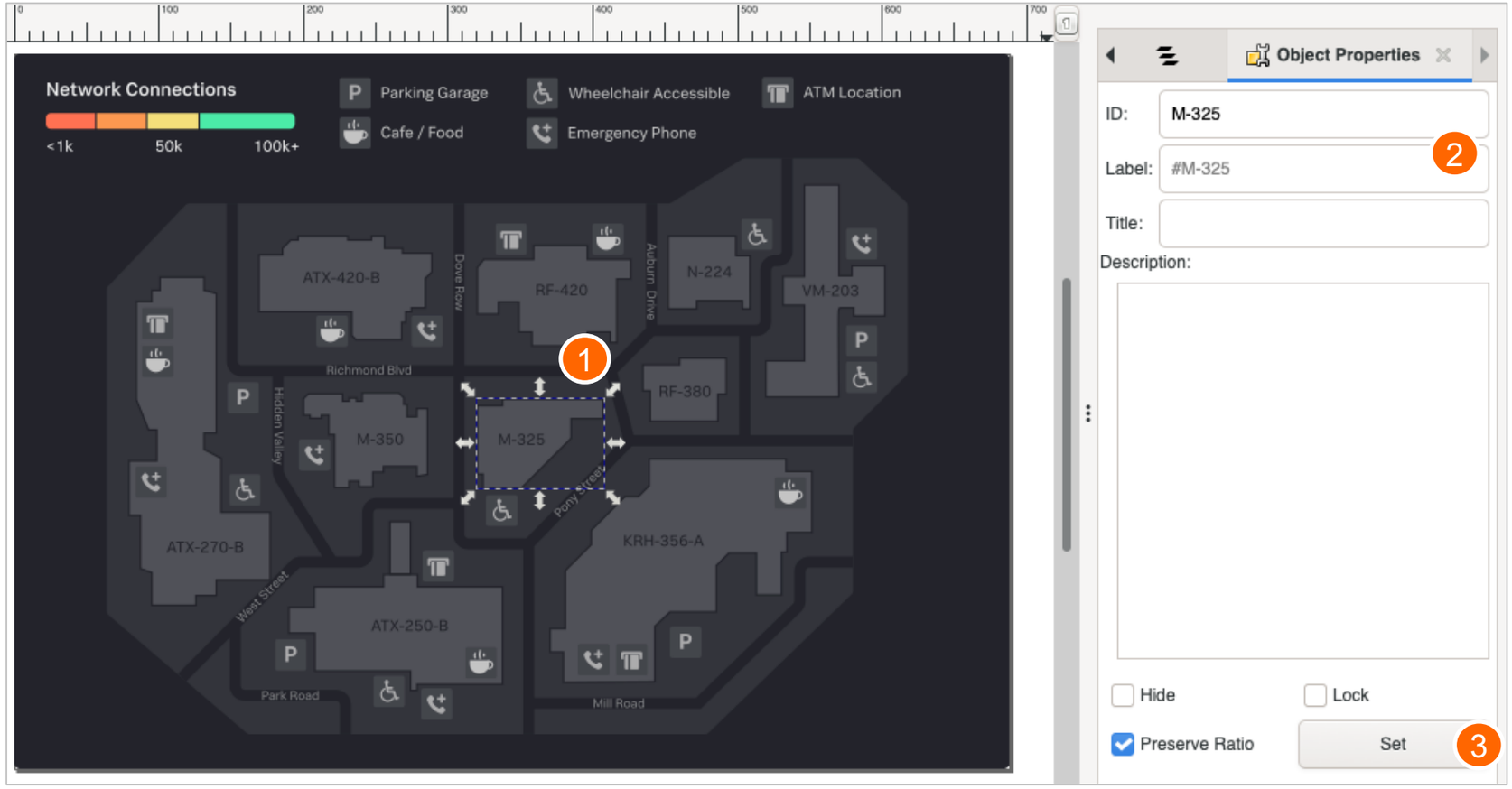
1. Select **Insert menu** > **Icons…**
2. Add an icon to a slide
3. Right-click the **icon** and select **Save as Picture…**
4. Select **Save as Type: SVG**
5. Name the file and click **Save**.



© 2024 SPLUNK INC.

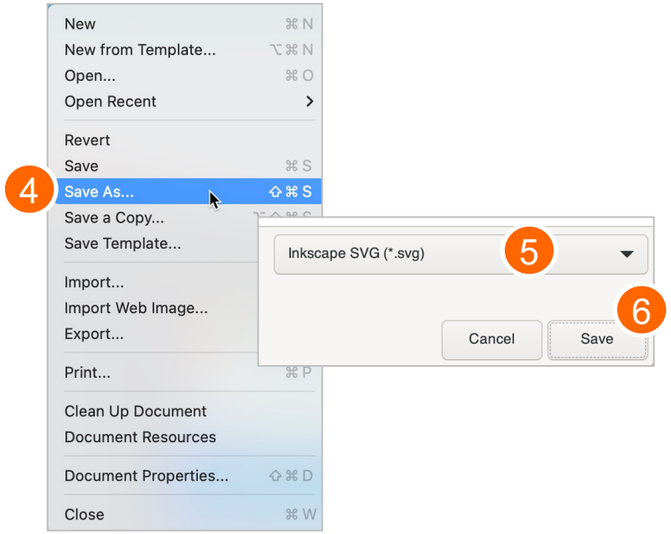
Creating a Choropleth SVG – Example 2

Inkscape



Create an SVG file in Inkscape:

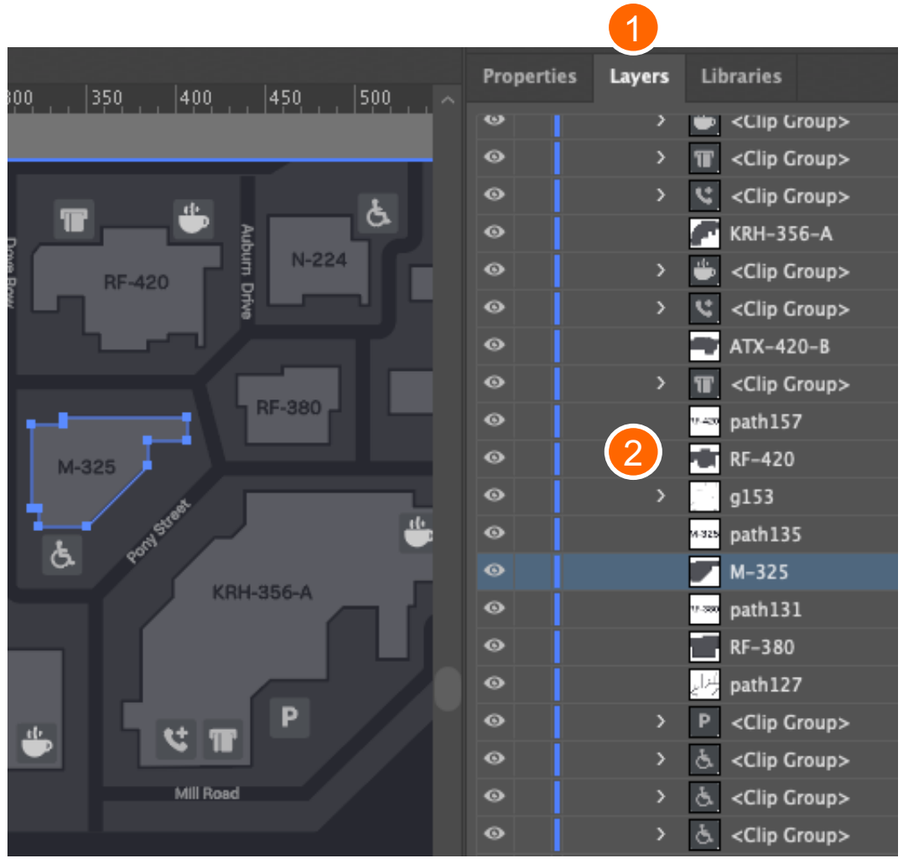
1. Select the area to assign an ID.
2. In Object Properties **enter an ID**.
3. Click **Set.**
4. Select **File** menu > **Save As…**
5. Select **Inkscape SVG**.
6. Click **Save**.



© 2024 SPLUNK INC.

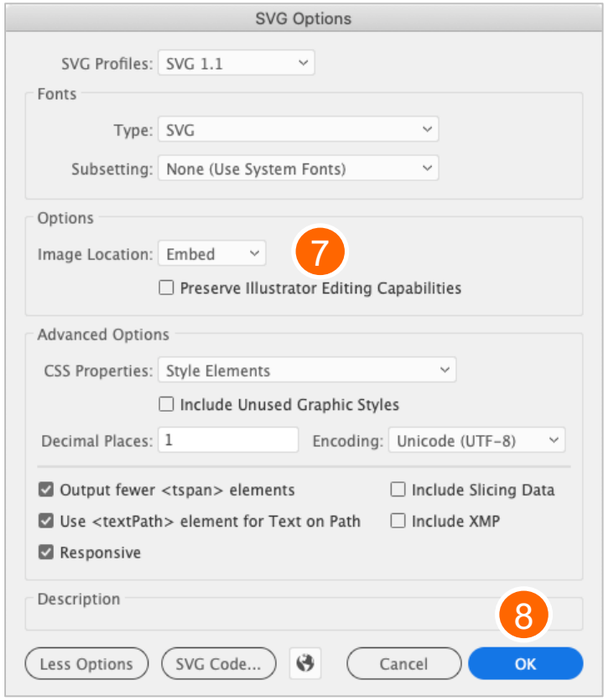
Creating a Choropleth SVG – Example 3

Adobe Illustrator



Create an SVG file in Illustrator:

1. Use layers for areas that receive color.
2. Assign the shape outline a name. This is the path ID.
3. In the File menu, select **Save As…**
4. Name the file.
5. In the Format menu select **SVG**
6. Click **Save**.
7. In the SVG Options window, from the Image Location menu, select **Embed**.
8. Click **OK**.



© 2024 SPLUNK INC.

Assign a Data Source

- Match path IDs to the first column of search results
  - Use field names as path IDs, OR
  - Rename each field using `eval` or rename commands, OR
  - Create a lookup file to match the fields to the unique path IDs
- Ensure at least one column of numbers is associated with each field in your search results
  - These are used to determine the fill color of each path ID

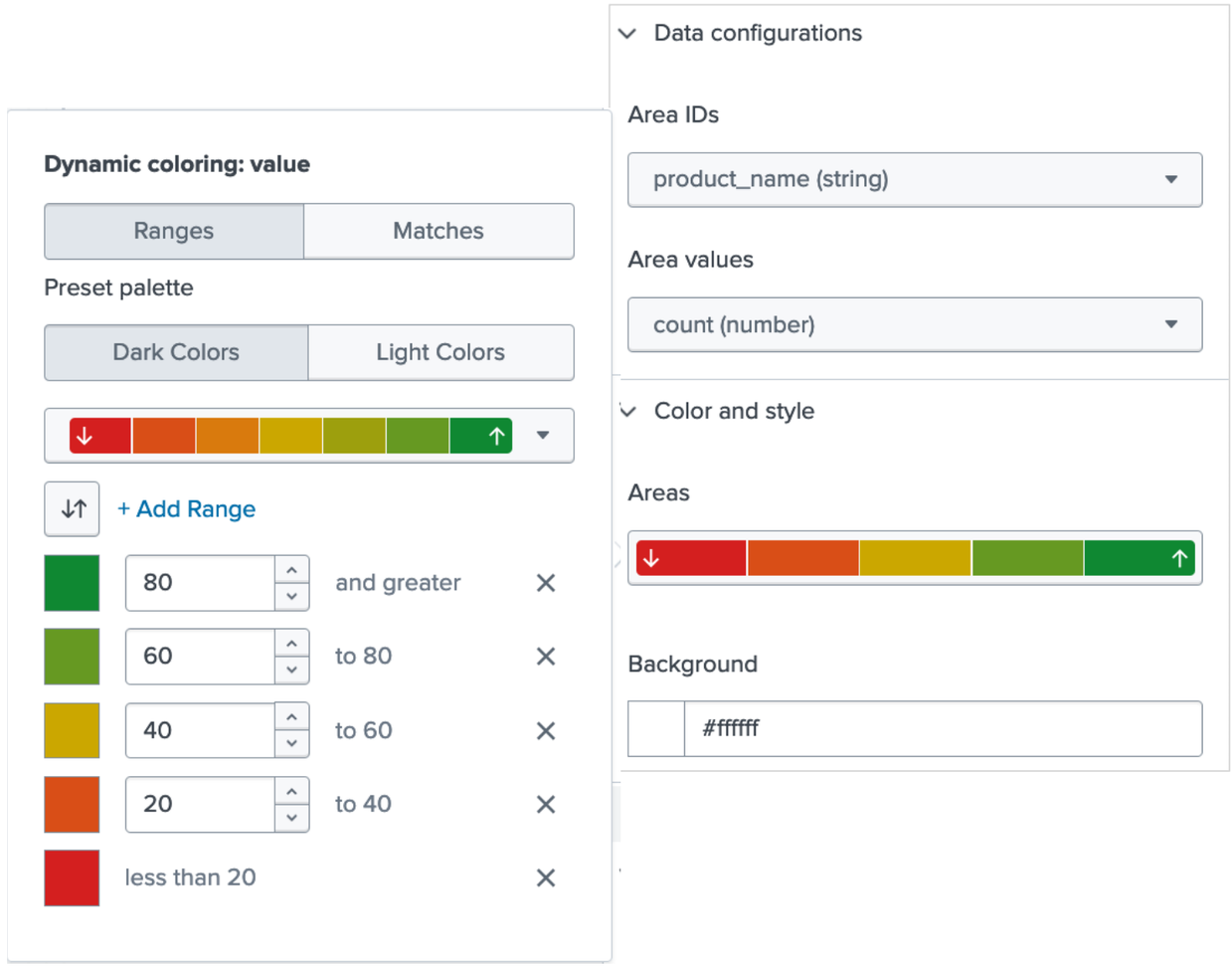
```
<path
  d="m 337.6,238.61 v 4.512 h -17.482 v 47.371 h 3.948 v 9.587
  h 26.505 l 34.401,-34.401 v -13.534 h 21.993 V 238.61 Z"
  fill="#505158"
  stroke="#23242b"
  stroke-width="1.171"
  id="M-325" />
```

Building_Name	count
ATX-270-B	10
N-224	547000
VM-203	673000
RF-380	8700
KRH-356-A	510000
M-325	43700
M-350	80800
ATX-420-B	73000
ATX-250-B	89000
RF-420	900000

© 2024 SPLUNK INC.

Assign Color Ranges

- Data configurations
  - Area IDs (path id)
  - Area values
- Color and style
  - Areas (path colors)



Note

When using dynamic coloring with a choropleth SVG, the value of zero "0" is ignored and the value defaults to white, `#ffffff`.

© 2024 SPLUNK INC.

Choropleth SVG – Example

SVG Source

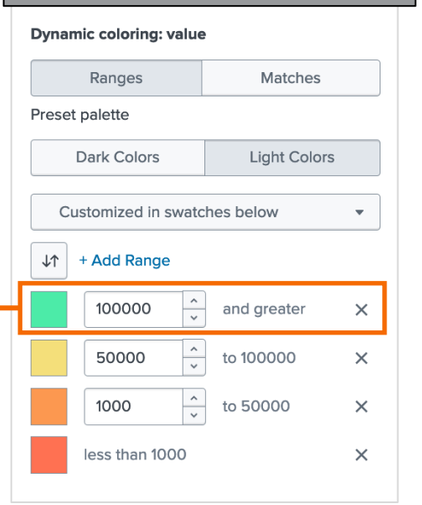
```
<path
  d="m 452.09,125.91 0.013,50.382 h 19.728 v -5.661 h 31.581 v 5.661 h 5.243
  l -0.012,-36.678 h -9.746 V 125.91 Z"
  fill="#505158"
  stroke="#23242b"
  stroke-linecap="round"
  stroke-linejoin="round"
  stroke-miterlimit="10"
  stroke-width="1.2025"
  id="N-224" />
```

Building_Name	count
ATX-270-B	10
N-224	147000
VM-203	173000
RF-380	8700

Dashboard Visualization Source

```
"context": {
  "areaColorsEditorConfig": [
    {
      "value": "#FF7152",
      "to": 1000
    },
    {
      "value": "#FC9850",
      "from": 1000,
      "to": 50000
    },
    {
      "value": "#F4DF7A",
      "from": 50000,
      "to": 100000
    },
    {
      "value": "#4BEBA8",
      "from": 100000
    }
  ]
}
```

Dashboard Studio Side Panel



splunk>

© 2024 SPLUNK INC.

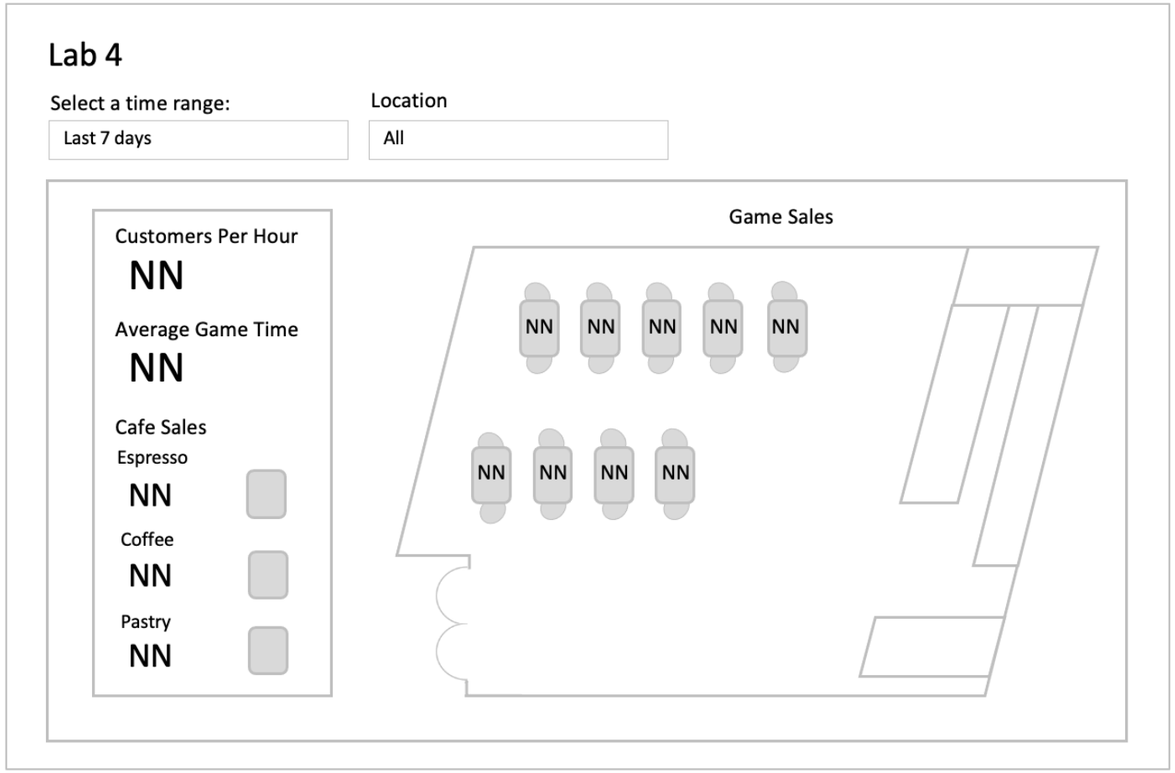
Lab Exercise 4

Time: 25 minutes

Description: Using choropleth SVG

Tasks:

- Clone a dashboard
- Add SVGs
- Assign data sources
- Set dynamic color ranges



© 2024 SPLUNK INC.

Wrap Up

- You should now be able to:
  - Use the `geostats`, `geom`, and `iplocation` commands
  - Create and customize cluster maps
  - Add interactivity to a map
  - Create and customize choropleth maps
  - Create a choropleth SVG

© 2024 SPLUNK INC.

Documentation

- Module 1: Creating a Cluster Map
  - Generate a Map
- Module 2: Adding a Choropleth Map
  - Generate a Choropleth Map
  - Use IP addresses to generate choropleth maps
  - Define a geospatial lookup in Splunk Web
- Module 3: Customizing Maps
  - Dynamic Options in Dashboard Studio
  - Setting tokens on a visualization click
  - Dynamic Options Syntax Formatting Functions
- Module 4: Adding a Choropleth SVG
  - Choropleth SVG
  - Choropleth SVG Options
  - Painting with Data: Choropleth SVG

© 2024 SPLUNK INC.

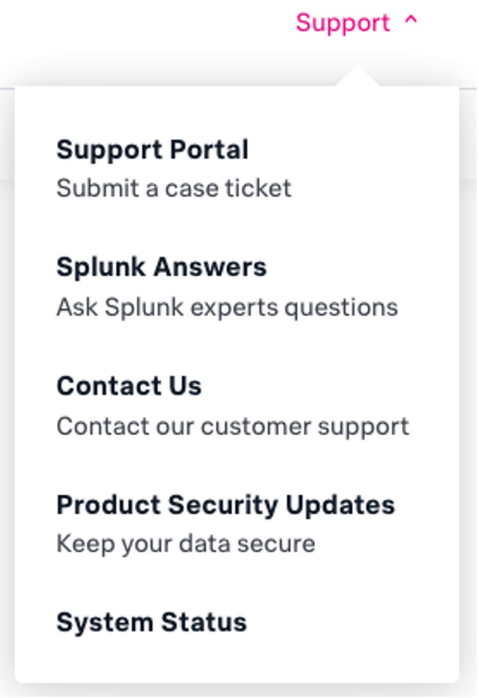
References

- 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

© 2024 SPLUNK INC.

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



© 2024 SPLUNK INC.

Learning Paths

Search Expert - Recommended Courses

Free eLearning courses are in blue.

- 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

© 2024 SPLUNK INC.

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 *

© 2024 SPLUNK INC.

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

Thank You

splunk>