

Build a Graph Over Time: Single Field Over Time

Example: sourcetype=access_combined | timechart count

1: Define report content

Search | Define report using search language

`sourcetype="access_combined" | timechart count`

Time range
Last 15 minutes

Report Data

Report type: Values over time

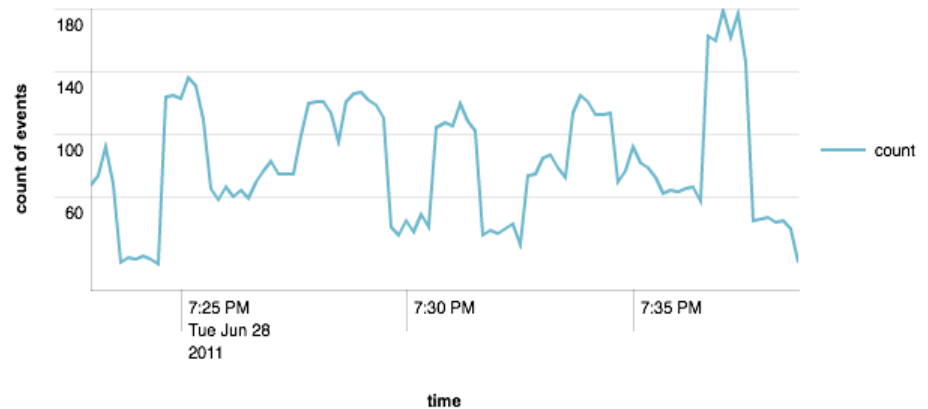
Report will display: Single field over time

Fields

Show: Number (count) of Events

Set span for time axis intervals (for example: every 10 minutes)

Next Step: Format Report



Build a Graph Over Time: Multiple Fields Over Time

Example: `sourcetype=access_combined | timechart avg(bytes) max(bytes)`

1: Define report content

Search | Define report using search language

```
sourcetype=access_combined | timechart avg(bytes) max(bytes)
```

Time range
Last 15 minutes

Report Data

Report type: Values over time

Report will display: Multiple fields over time

Fields

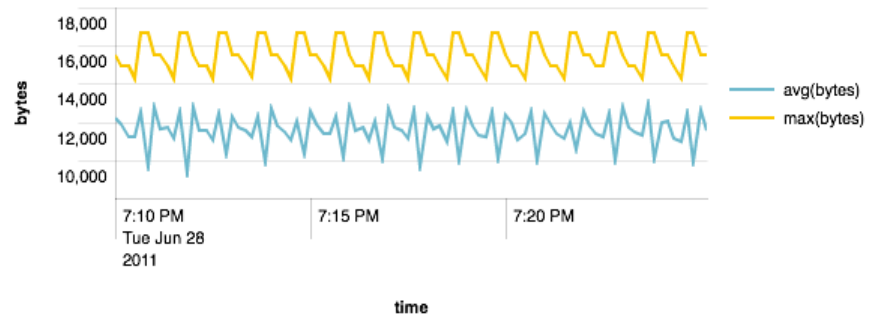
Show Average of bytes (n)

Show Maximum of bytes (n)

[add series](#)

Set span for time axis intervals (for example: every 10 minutes)

Next Step: Format Report



Build a Graph Over Time: Single Field Split by Another Field

Example: sourcetype=access_combined | timechart span=5m count by clientip

1: Define report content

Search | Define report using search language

```
sourcetype=access_combined | timechart span=5m count by clientip
```

Time range
Last 60 minutes

Report Data

Report type
Values over time

Report will display
Single field split by another field

- Single field over time
- Multiple fields over time
- Single field split by another field

Fields

Show
Number (count)

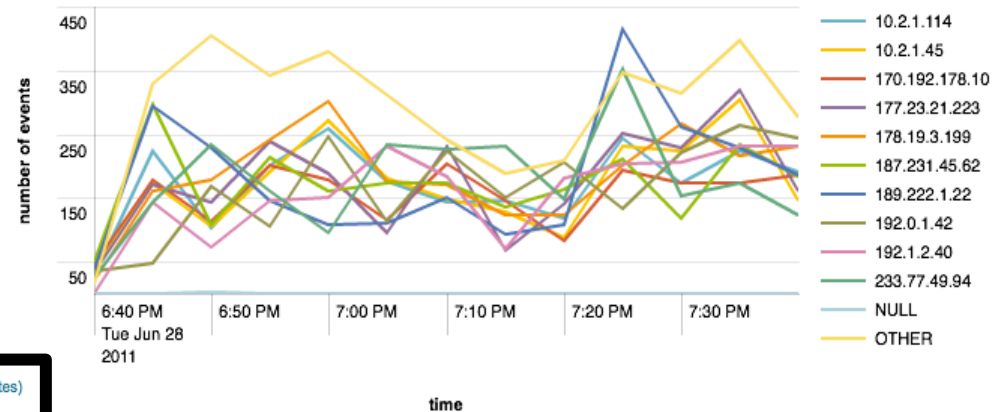
of
Events

split by
clientip

Set span for time axis intervals (for example: every 10 minutes)
Time span for each interval
 Auto
 Custom
5 Minute(s)

Next Step: Format Report

Count by Client IP Last Hour



Stack Values

1: Define report content > 2: Format report

Save Export... Print... Get

Chart

Formatting options

Chart type: column

Format: General | X-axis | Y-axis

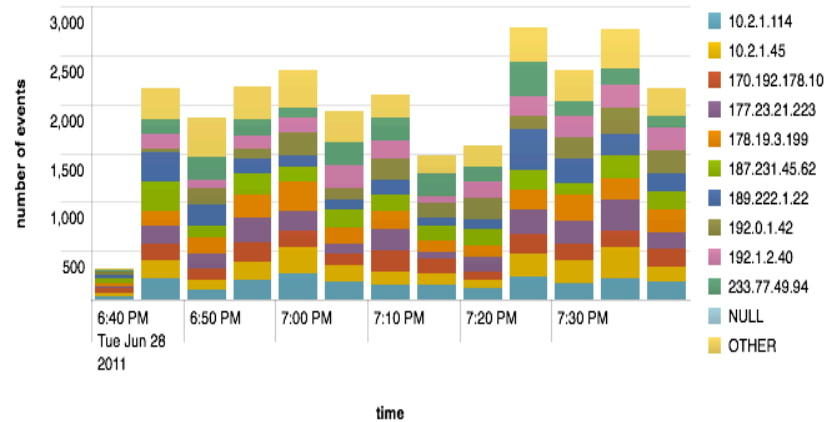
Chart title: Count by Client IP Last Hour

Stack mode: Stacked

None
Stacked
100% Stacked

Apply

Count by Client IP Last Hour



Build a Graph on Values

Example: sourcetype=access_combined | top uri_path

1: Define report content

Search | Define report using search language

```
sourcetype="access_combined" | top uri_path limit="1000"
```

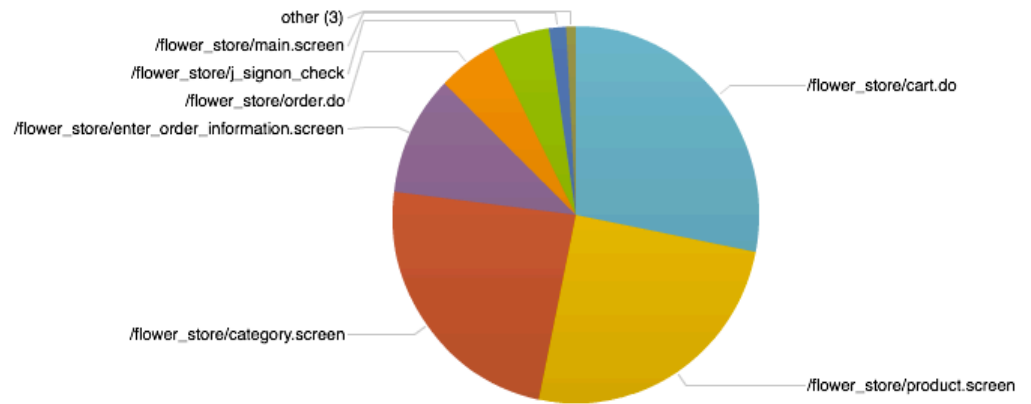
Time range
Last 24 hours

Report Data
Report type
Top values

Fields
of
uri_path

Next Step: Format Report

Top Paths Last 24 Hours

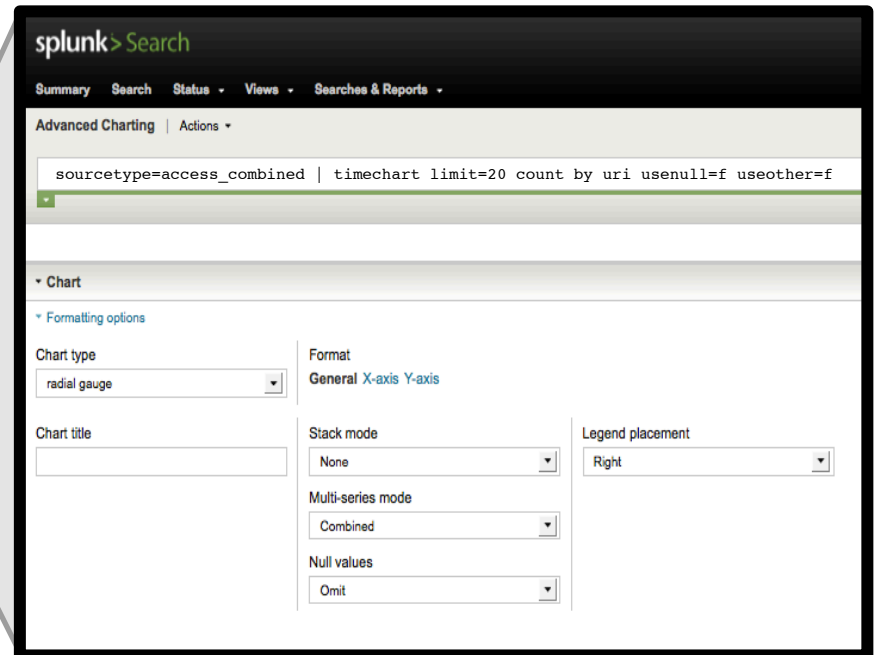
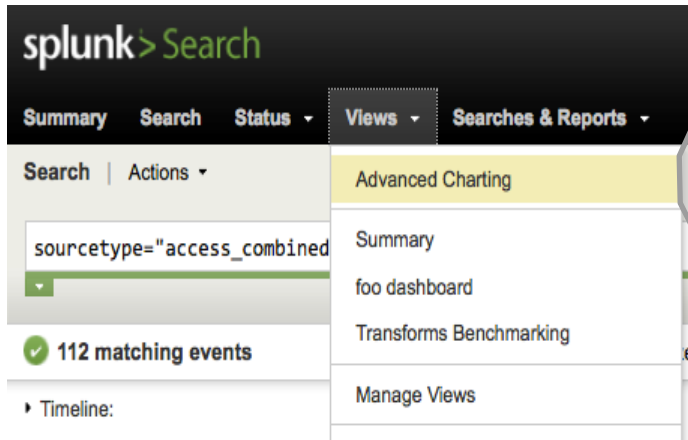


Use the Advanced Charting (AC) View

Define reports and toggle options in the search bar

Example: `sourcetype=access_combined |`

`timechart limit=20 count by uri usenull=f useother=f`



Build Gauges

Set thresholds via search + make gauge type selections in UI

Example: sourcetype=access_combined | stats count | gauge count 0 25 50 100 150

