



QuickStart Webinar

Getting Started with Sumo Logic

Agenda

- + What is Sumo Logic?
- + Key Points Regarding Data Collection
- + Searching, Parsing and Analyzing Data
- + Visualizing and Monitoring - Dashboards
- + Introduction to Library and Apps
- + Introduction to Performance Tools



What is Sumo Logic?

From Data to Decisions

DEVOPS



Streamline continuous delivery



Monitor KPI's and Metrics



Accelerate Troubleshooting

IT INFRASTRUCTURE AND OPERATIONS



Monitor all workloads



Troubleshoot and increase uptime



Simplify, Modernize, and save costs

COMPLIANCE AND SECURITY



Automate and demonstrate compliance



Audit all systems



Think beyond rules

Sumo Logic Cloud Analytics Service

The Sumo Logic Service

DEVOPS



IT INFRASTRUCTURE
AND OPERATIONS



COMPLIANCE AND
SECURITY



Collect and Centralize: Effortlessly collect terabytes of data from anywhere



Search and Analyze: Run searches and correlate events in real-time



Detect and Predict: Detect outliers and deviations to uncover the unknowns



Monitor and Visualize: Easily monitor and visualize your data in real-time



Alert and Notify: Proactively notifies you when specific events are identified

Securing your Data

Compliance and Certifications on top of AWS Security

- PCI/DSS 3.0 Service Provider Level 1 Certified
- AES 256-bit encryption at rest
- SSL encryption in transit
- U.S. – E.U. Safe Harbor attestation
- SOC 2, Type II attestation
- HIPAA compliant
- FIPS 140 compliant

Resource: <https://www.sumologic.com/resource/white-paper/securing-the-sumo-logic-service/>

Enterprise Logs are Everywhere

	Content Delivery	IaaS, PaaS	SaaS	Security
Custom App Code				
Open Source				
Middleware				
Databases				
Server / OS				
Virtual				
Network				

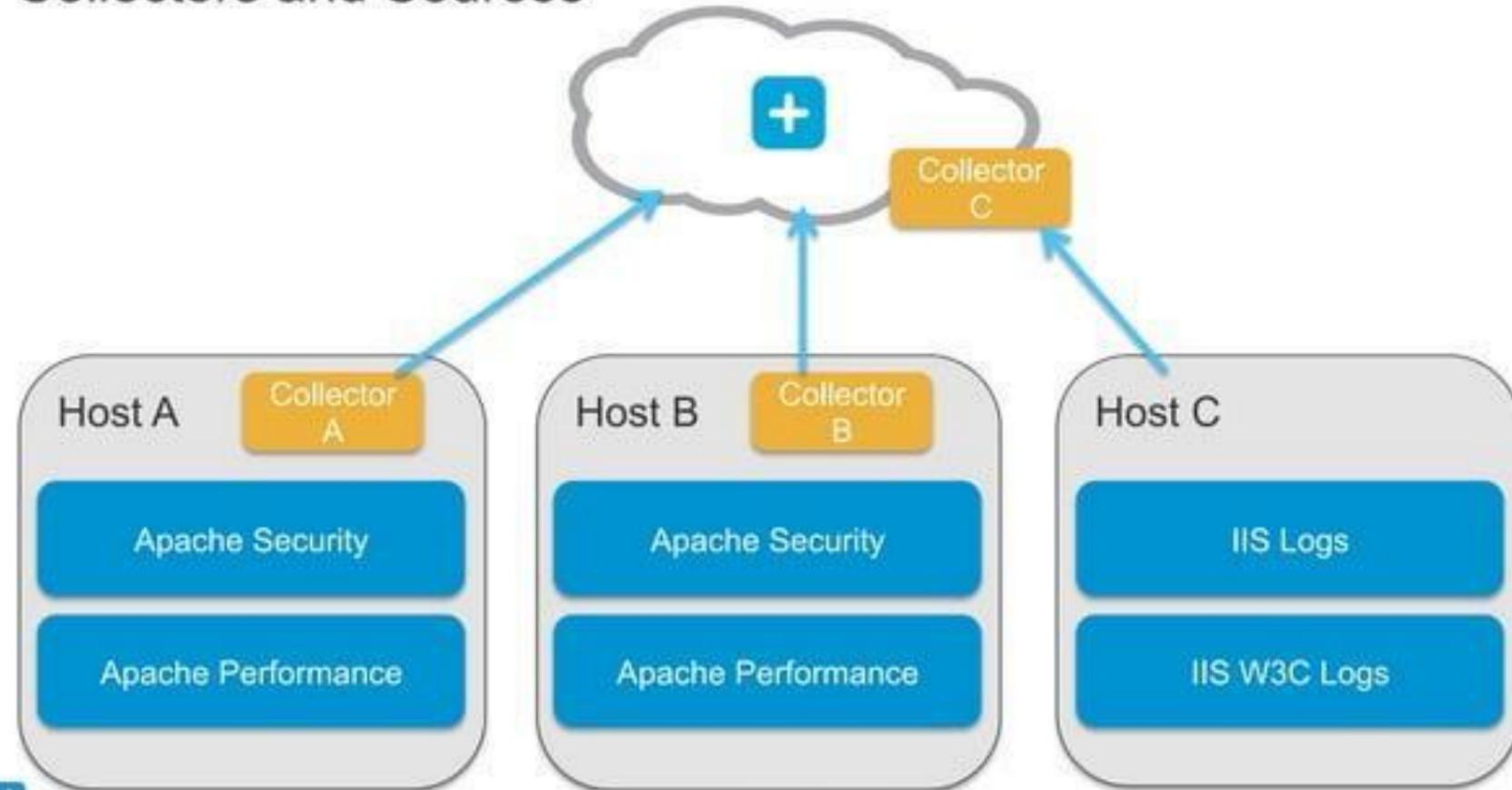
High-Level Data Flow

Sumo Logic Data Flow



Data Collection

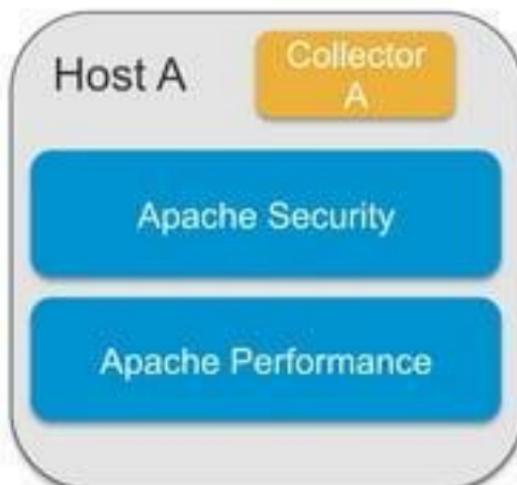
Collectors and Sources



Metadata Fields

Tags added to your messages when data is collected

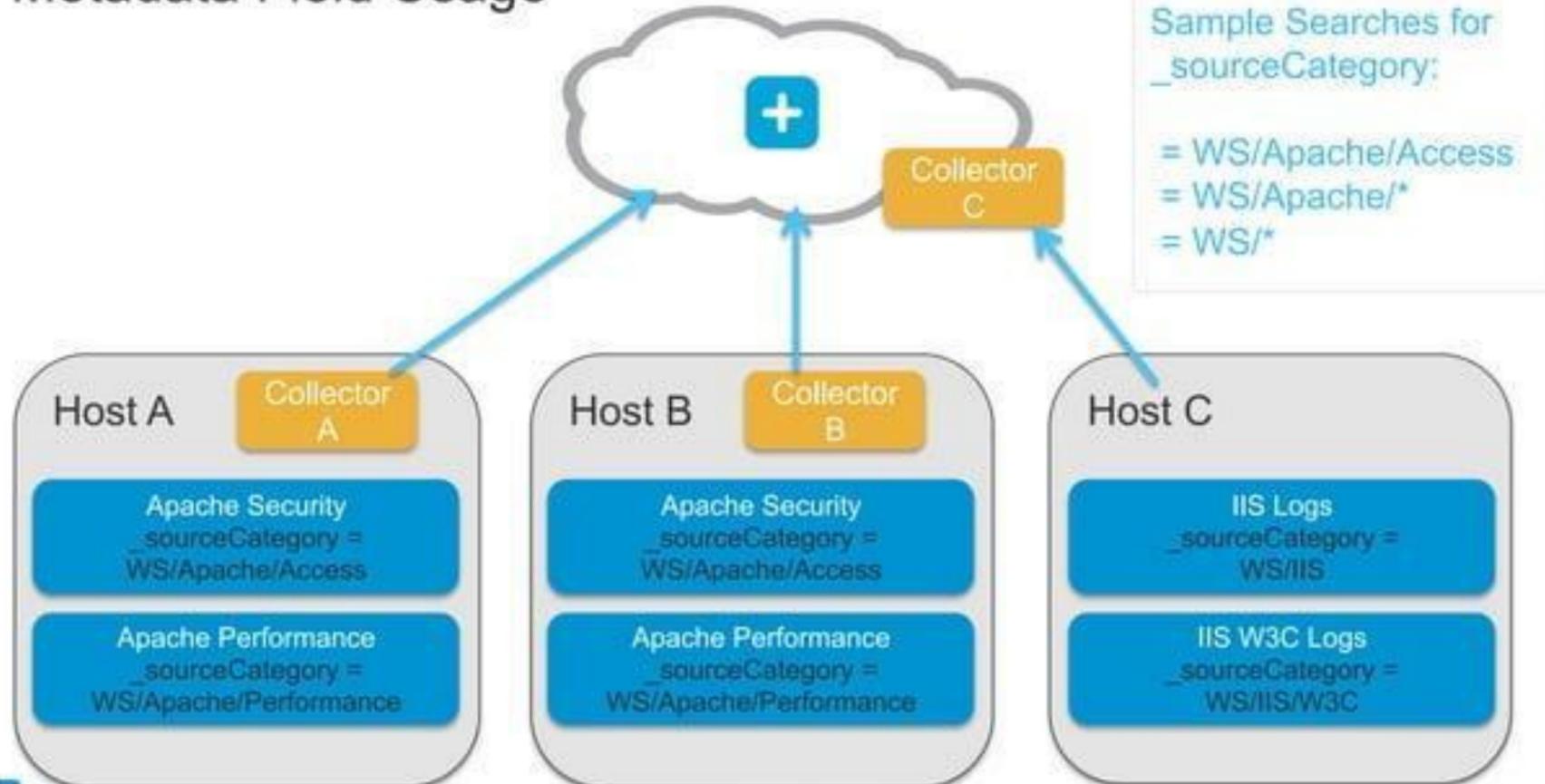
Name	Description
_collector	Name of the collector this data came from
_source	Name of the source this data came through
_sourceHost	Hostname of the server this data came from
_sourceName	Name of the log file (including path)
_sourceCategory	Category designation of source data



#	Time	Message
1	08/06/2013 18:05:55.000	169.107.162.237 - - [Wed Aug 07 01:05:55 UTC 2013] "GET /_css/master.133435683 "SAMSUNG-C5212/C5212XDIK1 NetFront/3.4 Profile/MIDP-2.0 Configuration/CLDC-1.1 Host: apache ▾ Name: /var/sumolabs/log/web51_access.log ▾ Category: Apache/Access ▾



Metadata Field Usage



Source Category Naming Convention

- + Simplifies Search Syntax and Scope Definitions
- + Used for other Sumo Logic features
 - + Role-Based Access Control (Data Provisioning)
 - + Partitioning (Search Optimization Tool)
- + Adopt a Robust Naming Convention Early
 - + Ex: Prod/Sumo/Apache/Access → Env/Customer/Device/MessageType
 - + Ex: OS/Windows/2012/Messages → Device/Vendor/Version/MessageType
 - + [Blog Post: Good SourceCategory, Bad SourceCategory](#)



Search and Analyze

Preferences

My Profile

Organization: SumoLabs
Organization ID: 0000285A74
Username: mario+sumolabs@sumologic.com
Password: Change.Password

Set your Preferences

My Access Keys



Label

Access ID

Created

Status

There are no Access Keys associated with your account. Click the Add button to generate your first key.

My Preferences

Default Timezone:

Use the browser's default time zone

Set your Session Timeout

Web session timeout: 12 Hours

* Any changes to the session timeout will take effect the next time you sign in.

Automatically run the search after selecting it from a list of saved searches.

Show confirmation dialog when closing a search tab.

Automatically open the search autocomplete dialog when editing. (Use <Esc> or <Alt> <Space> to open it manually).

Query editing:

<Enter> runs the query, <Alt> <Enter> creates a new line.

<Alt> <Enter> runs the query, <Enter> creates a new line.

Query Editing versus Running

Save

Search Basics Overview

The screenshot shows the Splunk search interface with several UI elements highlighted by yellow callout bubbles:

- Time Range**: Located at the top right, it includes a date range selector from "Yesterday" to "Start" and a checkbox for "Use Receipt Time".
- Search Bar**: The search query entered is:

```
_sourceCategory=Apache/Access GET  
| parse "GET * HTTP/1.1" * * `` as url,status_code,size,referer  
| where !(status_code = 200 and status_code=304)  
| timeslice 1m  
| count by status_code, _timeslice  
| sort by _timeslice, status_code asc  
| transpose row _timeslice column status_code
```
- Histogram**: A bar chart showing the distribution of file sizes over time. The x-axis represents time intervals from 4:25 PM to 4:40 PM, and the y-axis represents file size from 0 to 10,000. The bars are blue.
- Display Options**: A toolbar at the bottom with various icons for modifying the search results view.
- Search Results**: The main table showing the results of the search query. It includes columns for #, Time, and status codes (200, 302, 304, 401, 403, 404, 500, 503). The first three rows of data are:

#	Time	200	302	304	401	403	404	500	503
1	07/30/2015 4:25:00 PM	1,346	75	260	37	2	79	8	17
2	07/30/2015 4:26:00 PM	5,607	306	1,235	186	5	326	46	109
3	07/30/2015 4:27:00 PM	5,526	311	1,130	181	6	323	47	112

Search Syntax Flow

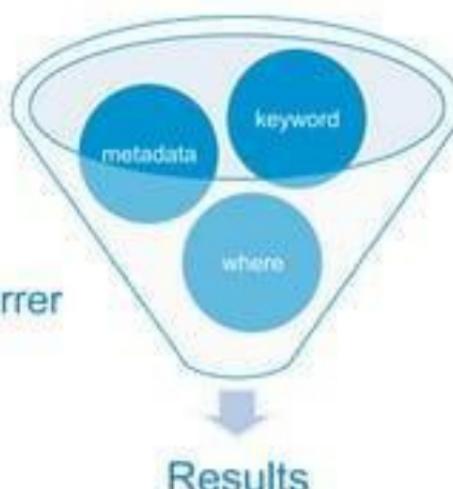
Enter keywords and operators (separated by |) that build on top of each other

Syntax:

keyword | parse | where | group by | sort | limit

Example:

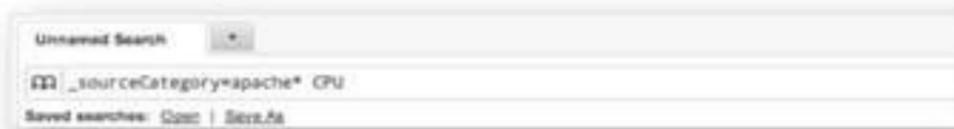
```
_sourceCategory=Apache/Access and GET  
| parse "GET * HTTP/1.1\* * *\\" as url, status_code, size, referrer  
| where !(status_code = 200 and status_code=304)  
| count by status_code  
| sort by status_code asc
```



Keyword Expression

Full-text search expressions enable you to search for multiple terms and logical expressions

- Case insensitive
- Wildcard support
- Metadata field
- Boolean logic
 - Complete (AND/OR)
 - Implicit AND



Messages		
#	Time	Message
1	09/06/2013 17:50:41.022	[05 CPU Percentages] - cpu_idle = 15.18, cpu_user = 19.87, cpu_system = 30.47, cpu_stolen = 27.45, cpu_iowait = 28.36 = 0.20, five_min_loadavg = 0.87, fifteen_min_loadavg = 0.87 Host apache - Name /var/run/limits.d/50-resources.conf - Category: Apache/Access -

Time Range

- The data available to your search request is determined by the selected time range.
 - Pre-populated
 - Last 15 min, Last 3 Hrs, Today
 - Absolute
 - 12:25 12:30
 - 8/11 12:00 8/11 13:00
 - Relative
 - 5m
 - 2h
 - 2h -1h



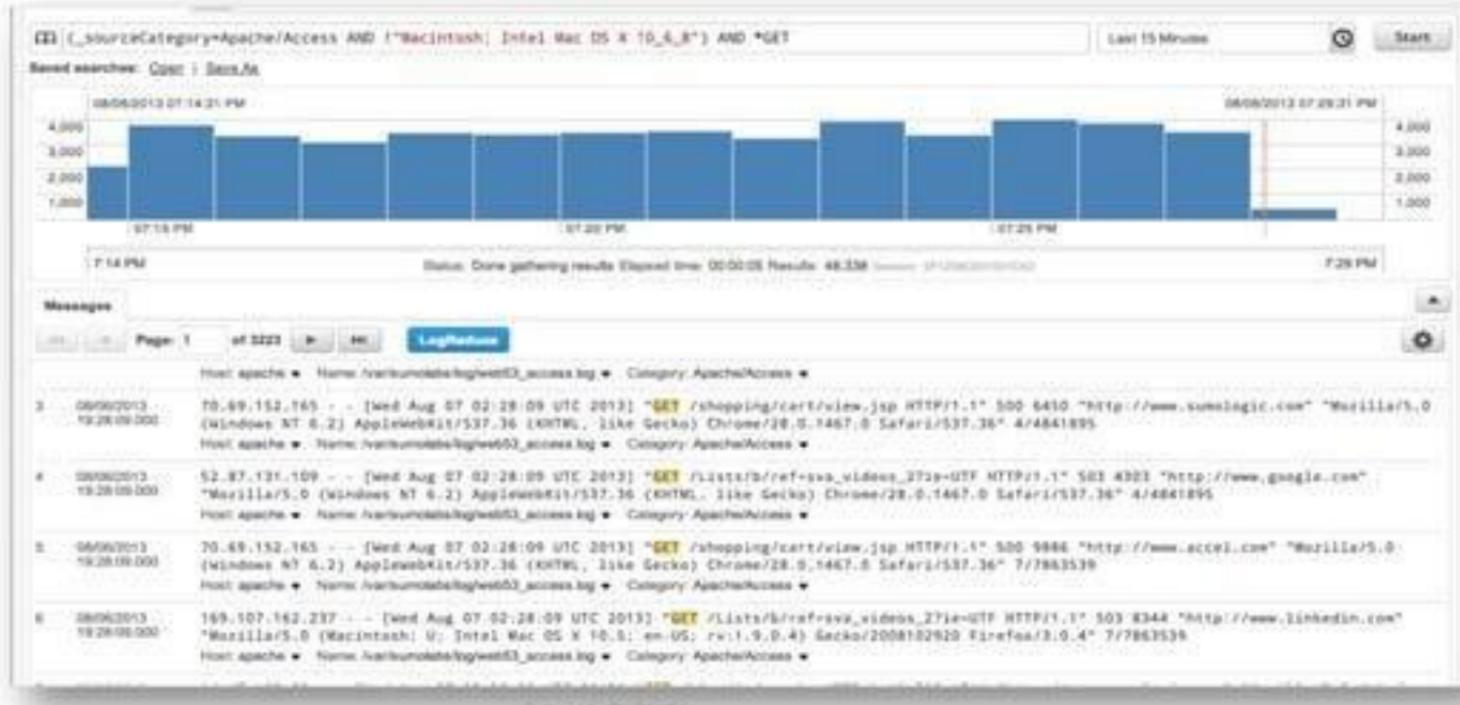
Syntax Example 1: Boolean logic, wildcards and metadata

(Error* OR fail* OR except*) AND _sourceCategory="apache"



Syntax Example 2: Exact String Matching

`(_sourceCategory=Apache/Access AND !"Macintosh; Intel Mac OS X 10_6_8") AND *GET`

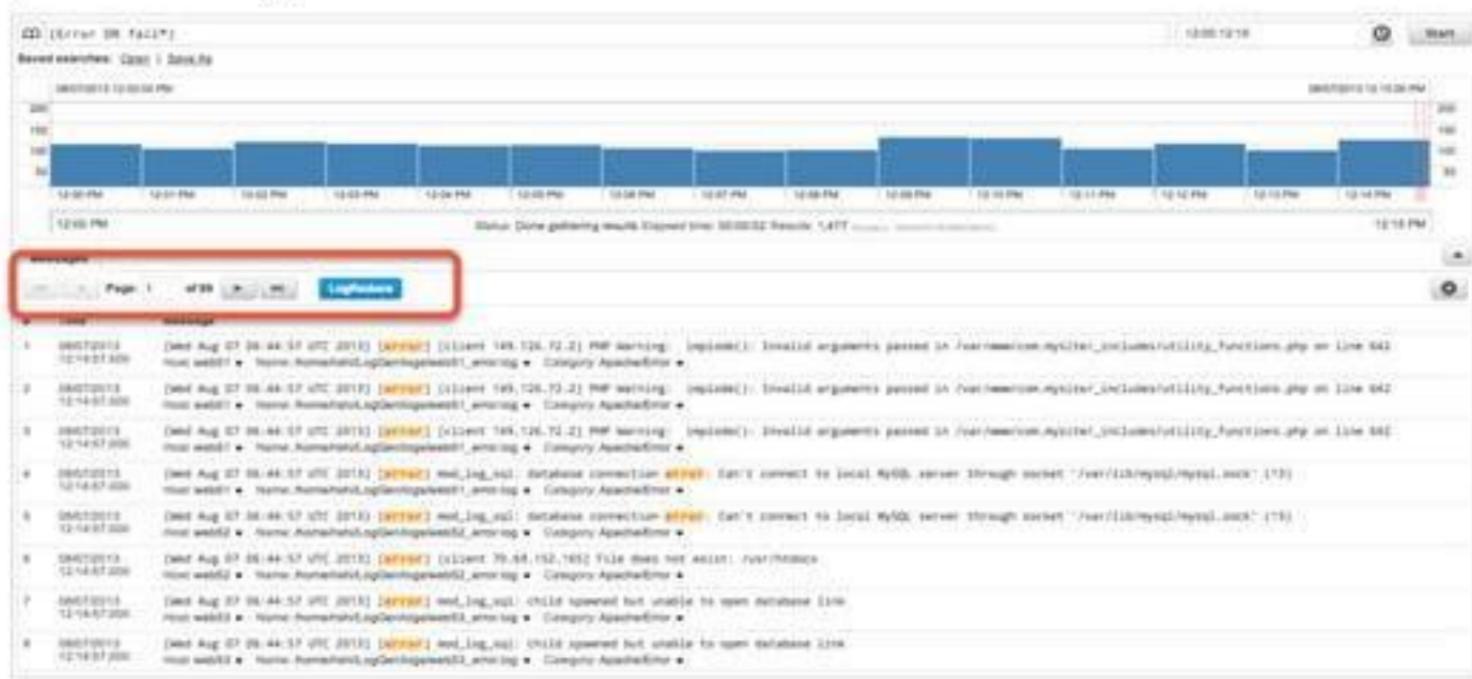


Refining Results by Surrounding Messages

Messages		
#	Time	Message
1	08/22/2013 19:20:15.000	[Aug 22 19:50:15] [ERR#] [client:149.128.72.3] PHP Warning: implode(): Invalid arguments passed in /var/www/cse.mysite/_includes/utility_functions.php on line 642 Host: apache ▾ Name: /var/sumolabs/log/web02_error.log ▾ Category: Apache/Access ▾
2	08/22/2013 19:20:15.000	[Aug 22 19:50:15] [ERR#] mod_log_sql: database connection ERR# : Can't connect to local MySQL server through socket '/var/lib/mysql/mysql.sock' (13) Host: apache ▾ Name: /var/sumolabs/log/web02_error.log ▾ Category: Apache/Access ▾
3	08/22/2013 19:20:15.000	[Aug 22 19:50:15] [ERR#] mod_log_sql: child spawned but unable to open database link Host: apache ▾ Name: /var/sumolabs/log/web01_errorlog ▾ Category: Apache/Access ▾
4	08/22/2013 19:20:15.000	[Aug 22 19:50:15] [ERR#] mod_log_sql: child spawned but unable to open database link Host: apache ▾ Name: /var/sumolabs/log/web01_errorlog ▾ Category: Apache/Access ▾
5	08/22/2013 19:20:15.000	[Aug 22 19:50:15] [ERR#] mod_log_sql: child spawned but unable to open database link Host: apache ▾ Name: /var/sumolabs/log/web01_errorlog ▾ Category: Apache/Access ▾
6	08/22/2013 19:20:15.000	[Aug 22 19:50:15] [ERR#] mod_log_sql: database connection ERR# : Can't connect to local MySQL server through socket '/var/lib/mysql/mysql.sock' (13) Host: apache ▾ Name: /var/sumolabs/log/web01_errorlog ▾ Category: Apache/Access ▾
7	08/22/2013 19:20:15.000	[Aug 22 19:50:15] [ERR#] mod_log_sql: child spawned but unable to open database link Host: apache ▾ Name: /var/sumolabs/log/web01_errorlog ▾ Category: Apache/Access ▾

Looking for the Unknown

- LogReduce uses fuzzy logic and soft matching to cluster messages providing quick investigation view into your environment.
(Error OR fail*) | summarize



Looking for the Unknown

- LogReduce uses fuzzy logic and soft matching to cluster messages providing quick investigation view into your environment.
(Error OR fail*) | summarize
- Influencing the outcome

Icon	Action
	Promote a signature to the top position of the Summarize tab.
	Demote a signature to move it to the bottom of the last page of the Summarize tab.
	Split a signature into multiple signature.
	Edit a signature.
	Undo the last action or step back through the history of changes.
	Redo the last action. Repeat to redo the history of undos.

Finding Outliers

- Identify unexpectedly high or low values ...
 - |timeslice 1m
 - |count by _timeslice
 - |outlier _count



Finding Outliers (continued)

- Timeslices are required
- Adjustable variables allow you to get the right sensitivity
 - Threshold
 - Number of rolling stddev above/below the moving average
 - Default: 3
 - Consecutive
 - Number of consecutive points above/below the threshold to trigger
 - Default: 1
 - Direction
 - Detect high values, low values or both
 - Default: Both
 - Window
 - Number of trailing timeslices used to calculate
 - Default: 10



Extracting Additional Labels/Fields

- Parsing enables a user to extract parts of a message and classify them as fields.
 - A specific key/value you want to extract
 - Enables you to perform additional operations
 - Logical/conditional – based on values
 - Mathematical – operations on value sets
- Ways of defining fields
 - Parse anchor: leverages start and stop anchors
 - Parse regex: extracts nested information via regexField extraction



Parse Anchor Using the UI

- Single field example

sourceCategory=Apache/Access - [parse "GET * HTTP/1.1" as url]

Last 15 Minutes

Start

Saved searches: Open | Save As

2013-07-09 00:00:04 PM 2013-07-09 00:14:54 PM

6,000
4,000
2,000

00:10 PM 00:15 PM 00:20 PM

5:09 PM Status: Done gathering results Request time: 00:00:05 Results: 5,201 Ingested: 5,190 Last updated: 00:14:54 PM

5:24 PM

8,000
6,000
4,000
2,000

00:10 PM 00:15 PM 00:20 PM

5:09 PM 5:24 PM

Messages

Page: 1 of 2001

LogParser

#	Time	url	Message
1	2013-07-09 00:14:54 PM	r_includesFollowFollow_js.php	17.233.159.80 - - [Aug 9 11:53:17] "GET /_includes/follow/follow_js.php HTTP/1.1" 200 8289 "http://www.google.com" "Mozilla/5.0 (Linux; U; Android; 2.3.4; en-US; SCH-R72; Build/GRJ33) AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1" Host apache • Name: /var/www/html/log/webd2_access.log • Category: ApacheAccess •
2	2013-07-09 00:14:54 PM	shoppingcartconfirm.jsp	19.174.45.8 - - [Aug 9 11:53:17] "GET /shopping/cartconfirm.jsp HTTP/1.1" 200 8997 "http://www.sunlogic.com" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.2.4) Gecko/2009102320 Firefox/3.6.4" Host apache • Name: /var/www/html/log/webd2_access.log • Category: ApacheAccess •
3	2013-07-09 00:14:54 PM	favicon.ico	34.87.4.8 - - [Aug 9 11:53:17] "GET /favicon.ico HTTP/1.1" 401 9619 "http://www.greylock.com" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:23.0) Firefox/23.0" Host apache • Name: /var/www/html/log/webd2_access.log • Category: ApacheAccess •
4	2013-07-09 00:14:54 PM	r_media/company_logo.png	Se.87.4.8 - - [Aug 9 11:53:17] "GET /r_media/company_logo.png HTTP/1.1" 200 4180 "http://www.sunlogic.com" "Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:23.0) Gecko/20131071 Firefox/23.0" Host apache • Name: /var/www/html/log/webd2_access.log • Category: ApacheAccess •
5	2013-07-09 00:14:54 PM	r_includes/ep/blogeo-contentplugins/acl1062195-random.php?ban50&id=8&random=1331983798	54.87.4.8 - - [Aug 9 11:53:17] "GET /_includes/ep/blogeo-contentplugins/acl1062195-random.php?ban50&id=8&random=1331983798 HTTP/1.1" 200 5887 "http://www.greylock.com" "Mozilla/5.0 (iPad; CPU OS 8.0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/8.0 Mobile/10A535d Safari/8536.25" Host apache • Name: /var/www/html/log/webd2_access.log • Category: ApacheAccess •

The count operator

- The count Operator enables you to group messages that match a classification
 - No Group: provides a total message count
 - Ex: * | count
 - Ex: : * | count as mycount

Messages		Aggregates	
		Page: 1 of 1	
#	_count		
1	45,805		

Messages		Aggregates	
		Page: 1 of 1	
#	mycount		
1	45,805		



Leveraging Metadata for grouping

- Dissecting your result sets using metadata fields
 - Ability to aggregate results sets and grouping them by metadata fields
 - EX: _collector=*apache* | count by _sourceCategory
 - Get a count of grouped result sets
 - Ex: (Error OR fail*)| count by _sourcecategory , _sourcehost
 - Organize Results by Count
 - Ex: _collector=*apache*| count by _sourceCategory | sort by _count



Time-based Grouping

- Timeslice operator enables you to segment your results by time buckets
 - Minute (timeslice by 5m)
 - Hour (timeslice by 1h)
 - Day (timeslice by 1d)

* Surver Page Views

```
filter _sourceCategory=*Surver* AND "HTTP" AND "GET"
| parse "GET *: * " as src_ip,URL
| timeslice by 1m
| count as page_views by _timeslice
```

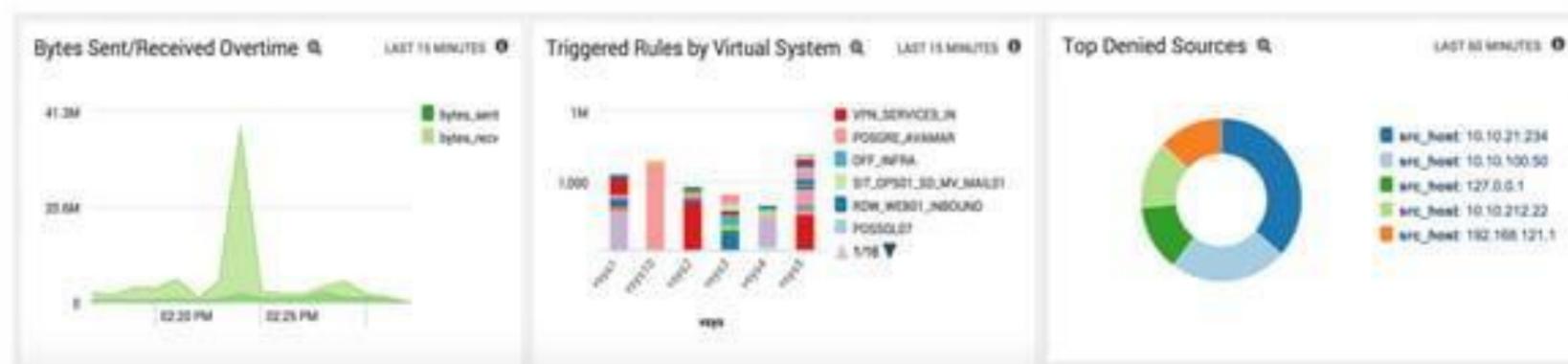
Last 15 Minutes

Saved searches: Queso | SereAn

Visualize and Monitor

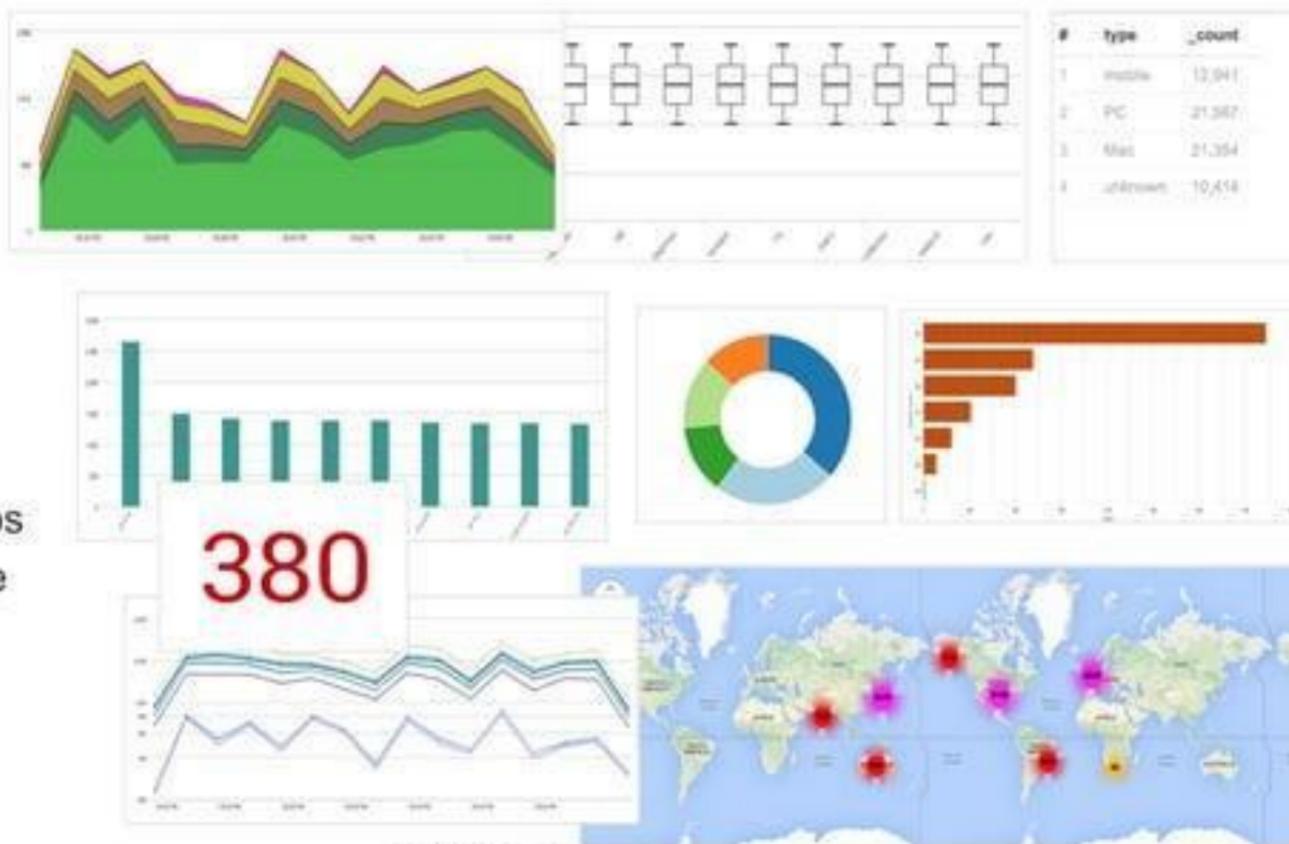
Introduction to Dashboards

- Collection of Monitors that provide graphical representation of data
 - Each Monitor processes results of a search for display
 - Drilldown for additional analysis
 - Drill to another dashboard
 - Drill into the query behind the dashboard



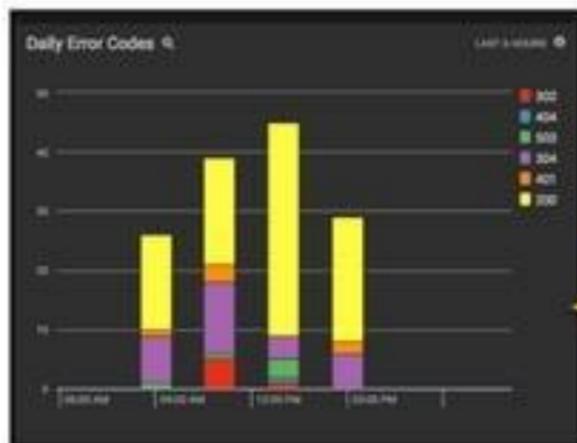
Providing Context through Visualization

- Chart Types
 - Table
 - Bar
 - Column
 - Line
 - Area
 - Pie
 - Box Plot
 - Google Maps
 - Single Value

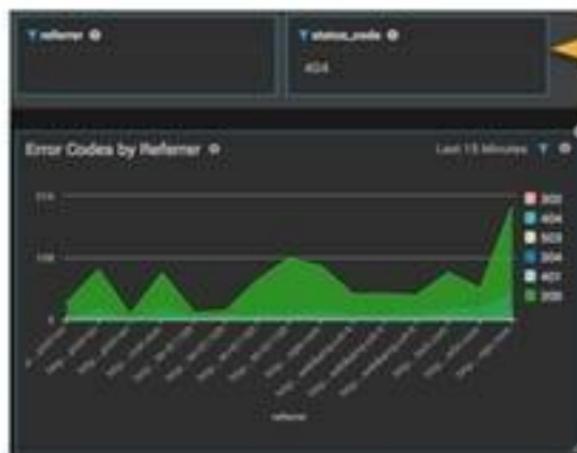


Dashboard Types

- Live Dashboards
 - Provides a live stream of data
 - No back filling of data
- Interactive Dashboards
 - Search based (On-Demand)
 - Backfilling of data
 - Support Filtering



No Interaction



Ability to use Pre-defined filters

Live Dashboards versus Interactive Dashboards

Use Case	Examples	Dashboard Type
Large Screen Displays with Streaming Updates	<ul style="list-style-type: none">• Shared Screens for NOC, Operations, Developers, etc.	Live Dashboards (Streaming/CQ)
Template for Exploring Data	<ul style="list-style-type: none">• Sumo Logic Sales Dashboards• Operational Investigations	Interactive Dashboards
Historical Reporting and Investigation	<ul style="list-style-type: none">• Search Usage• Customer Usage• Audits	Interactive Dashboards



Dashboards - Adding a Panel



Jumpstart with Apps

Installing Applications

The screenshot shows the Sumo Logic web interface. At the top, there's a navigation bar with links for Library, Search, Anomalies, Dashboards, Manage, and Help. On the far right, it shows a user profile for "Mario (SumoLabel)".

On the left, a sidebar has icons for Recent, Favorites, Personal, Org, and Apps. The "Apps" icon is highlighted with a blue background.

The main content area has a sidebar titled "Apps" with a plus sign icon. Under this, there are several collapsed categories: Active Directory, Akamai Cloud Monitor, Amazon CloudFront, Amazon S3 Audit, Apache, Apache Tomcat, Artifactory, Audit, and AWS CloudTrail.

To the right of this sidebar, a specific application page is displayed for "Apache". It features a small Apache logo icon, the word "Apache" in bold, and a descriptive text: "The Sumo Logic App for Apache uses searches and Dashboards to help you stay aware of web server operations, visitor information, and errors." Below this is a large blue "Install" button.

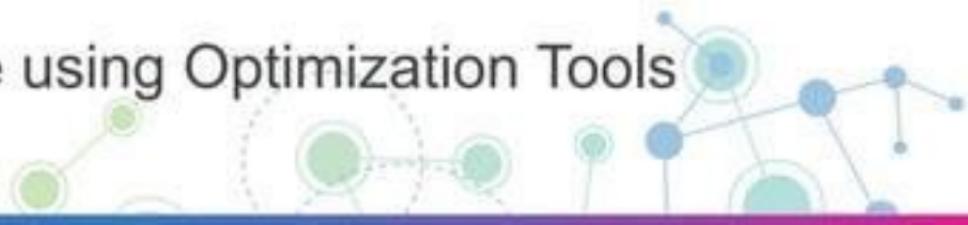
Below the "Install" button is a table with two columns: "NAME" and "DESCRIPTION". There are eight rows in the table:

NAME	DESCRIPTION
Apache - Overview	
Apache - Visitor Access Types	
Apache - Visitor Locations	
Apache - Visitor Traffic Insight	
Apache - Web Server Operations	
All HTTP Response codes with 4xx	
Client Errors (4xx response codes)	

Managing Performance

Factors in Search Performance

- + Query Structure
 - + Time range
 - + Data Selectivity (keywords, metadata, where statements)
 - + Heavy Operations (join, transaction, summarize)
- + Overall Data Volume
- + System load
- + Improve search experience using Optimization Tools

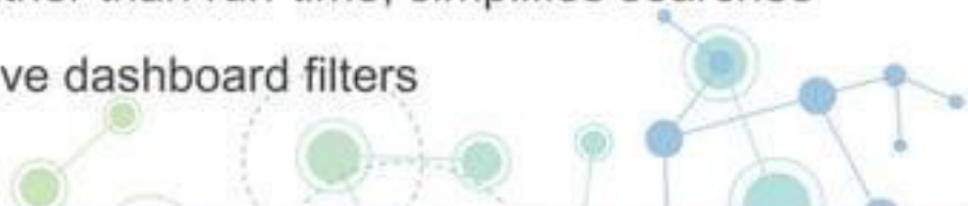


Search Optimization Tools

- + Partitions
 - + Separate index for searching over a smaller data set

- + Scheduled Views
 - + Pre-aggregating data for fast counts/sums over longer time ranges

- + Field Extraction Rules
 - + Parse the data on ingest rather than run-time; simplifies searches
 - + Take advantage of interactive dashboard filters



Questions?



Additional Resources

- ⊕ Search Online Documentation

- ⊕ Search/Post to Community Forums
 - Search, post, respond
 - Submit/vote for feature requests
 - Submit Tips & Tricks

- ⊕ Open a Support Case

- ⊕ Sumo Logic Services
 - Customer Success, Professional Services, Training

Helpful Links

Support Portal, Documentation, Community Forums, Feature Requests

<https://support.sumologic.com/home> (Help -> Support from SL Service)

Resources (Whitepapers, videos, screencasts)

<https://www.sumologic.com/resource/>

Blog Posts

<https://www.sumologic.com/blog/>

Services

customer-success@sumologic.com

Feature Spotlight Series: How TuneIn uses Outlier Detection and Predictive Analytics

Sep 22, 2015, 10am Pacific

[Register Now](#)

“How To” Webinars: Optimizing Your Search Experience

Sep 23, 2015, 10am Pacific

[Register Now](#)

Thank you!