

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

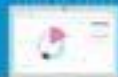


The Sumo Logic Service

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	   				

The background of the slide features a faint, abstract network diagram. It consists of numerous circular nodes of varying sizes, some in shades of blue and others in light green. These nodes are interconnected by thin, light-colored lines, creating a complex web-like structure that suggests data flow or network connectivity. The overall aesthetic is clean and modern, typical of a professional presentation.

High-Level Data Flow

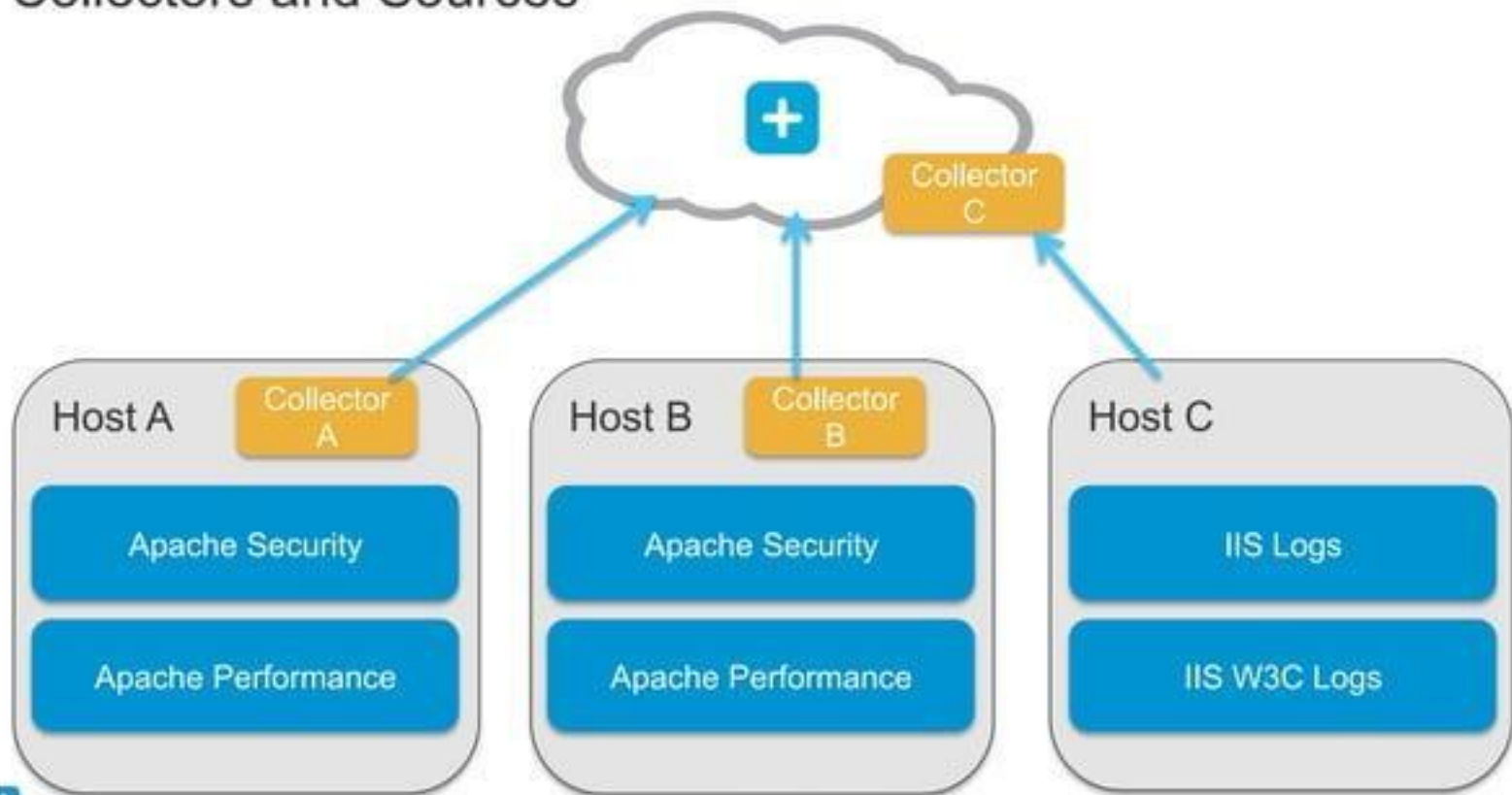
Sumo Logic Data Flow





Data Collection

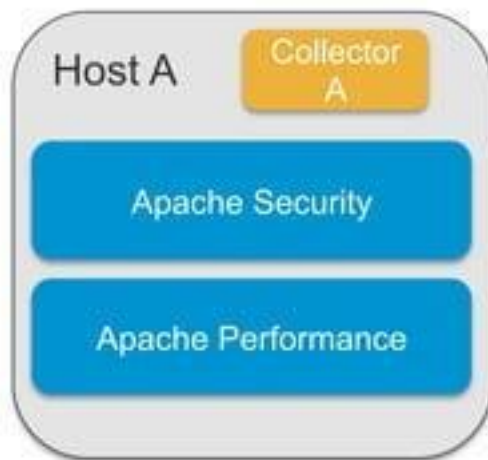
Collectors and Sources



Metadata Fields

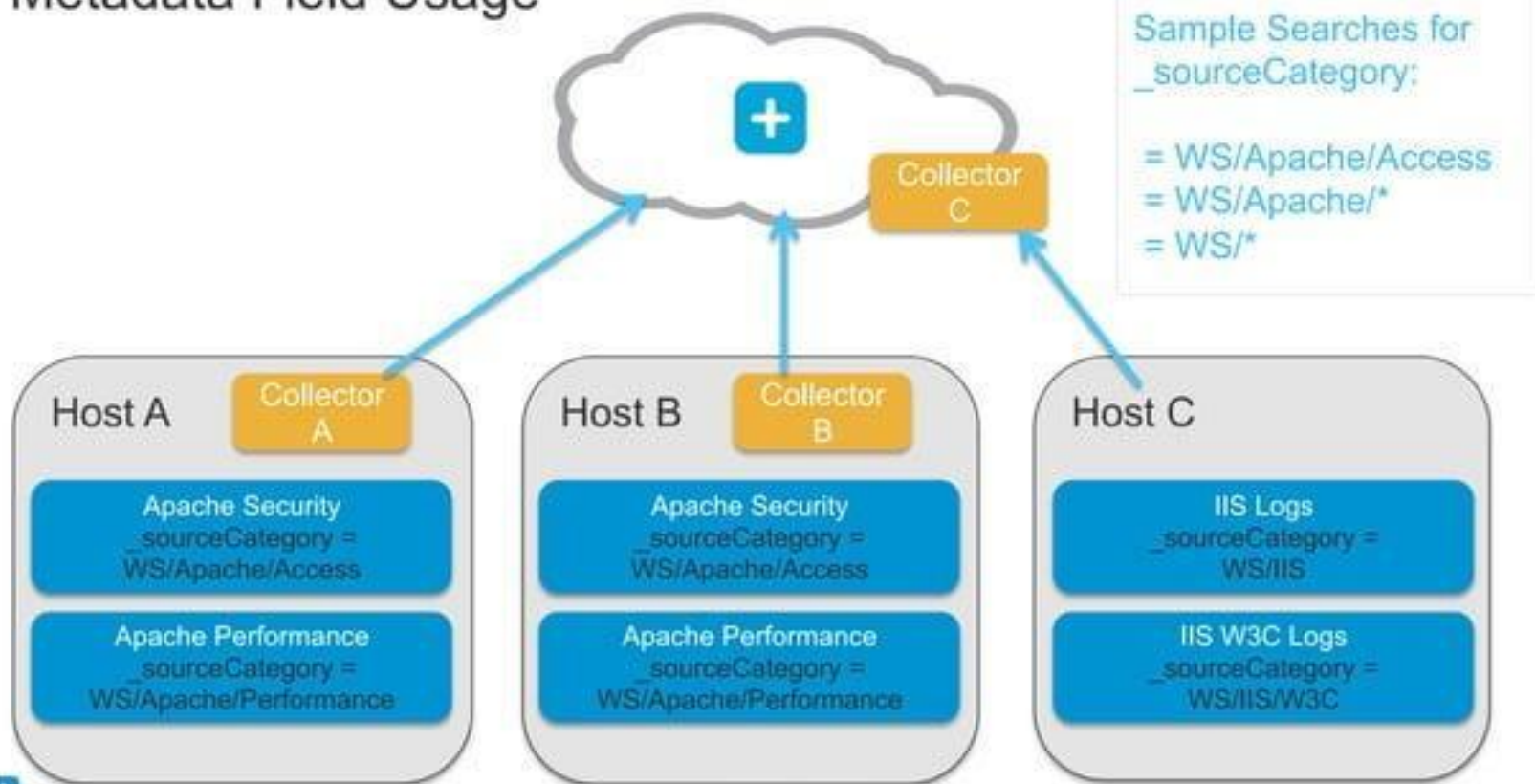
Tags added to your messages when data is collected

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



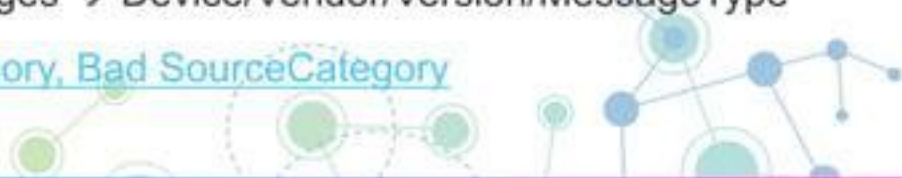
#	Time	Message
1	08/08/2013 18:05:55.000	169.107.162.237 - - [Wed Aug 07 01:05:55 UTC 2013] "GET /_css/master.133435683 "SAMSUNG-C5212/C5212XDIK1 NetFront/3.4 Profile/MIDP-2.0 Configuration/CLDC-1.1 Host: apache ▼ Name: /var/sumolabs/log/web51_access.log ▼ Category: Apache/Access ▼

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](#)



An abstract network diagram with various sized nodes in shades of blue and green, connected by thin lines, forming a complex web-like structure across the background.

Search and Analyze

Preferences

Set your
Preferences

My Profile

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

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:

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



Search Syntax Flow

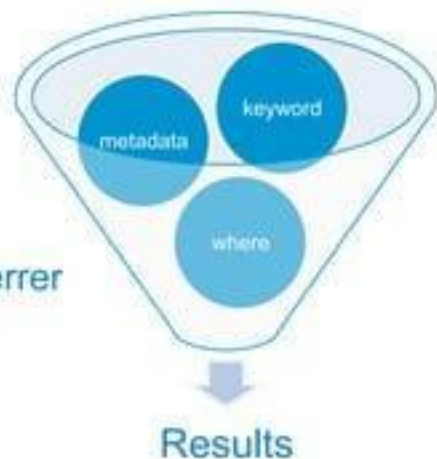
Enter keywords and operators (separated by |) that build on top of each other

Syntax:

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

Example:

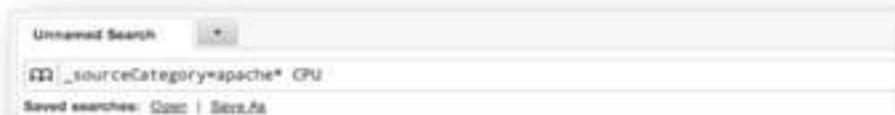
```
_sourceCategory=Apache/Access and GET  
| parse "GET * HTTP/1.1\" * * \"*\" as url, status_code, size, referrer  
| where !(status_code = 200 and status_code=304)  
| count by status_code  
| sort by status_code asc
```



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



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

Time Range Selection Interface:

Time Range	Start
Last 15 Minutes	
This Hour	
Today	
Yesterday	3:00 PM
This Month	8
Last Minute	6
Last 15 Minutes	4
Last 60 Minutes	2
Last 3 Hours	
Last 6 Hours	
Last 12 Hours	
Last 24 Hours	
Last 7 Days	
Last 14 Days	
Last 30 Days	
All Time	

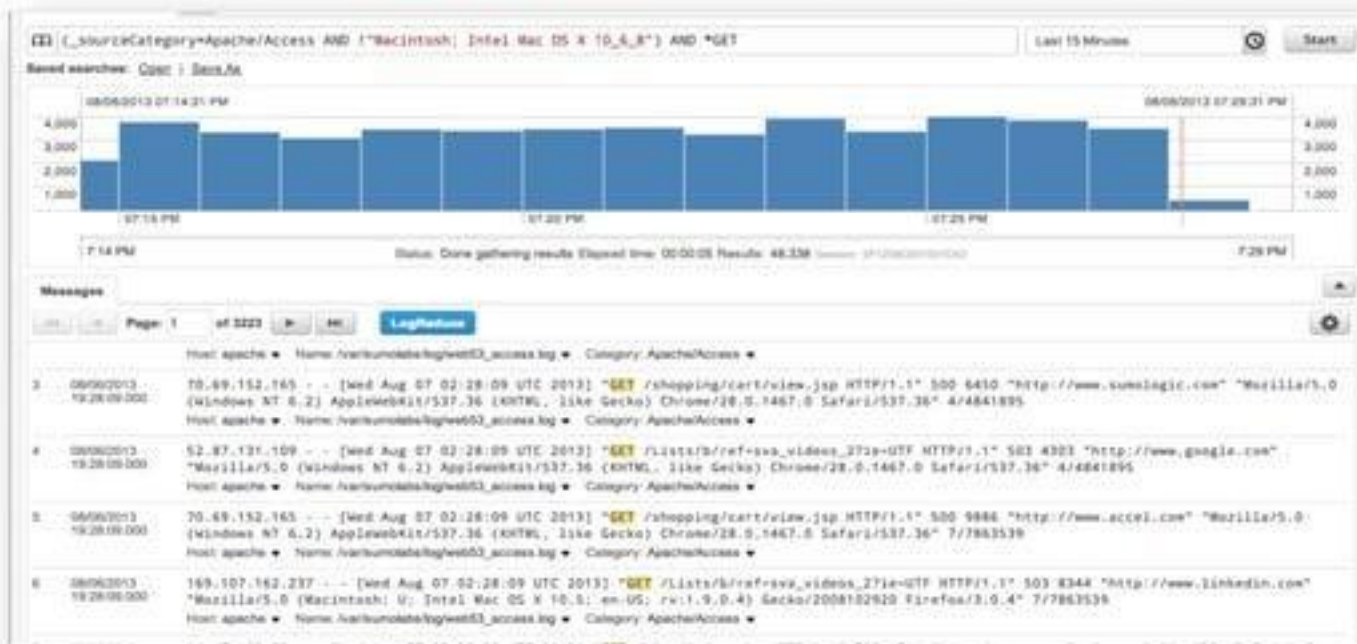
Syntax Example 1: Boolean logic, wildcards and metadata

(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

The screenshot shows a log viewer interface with a table of messages. A red box highlights a context menu for message 5, which is selected. The menu options are:

- Surrounding Messages >
- <- 1 Minute
- <- 5 Minutes
- <- 10 Minutes

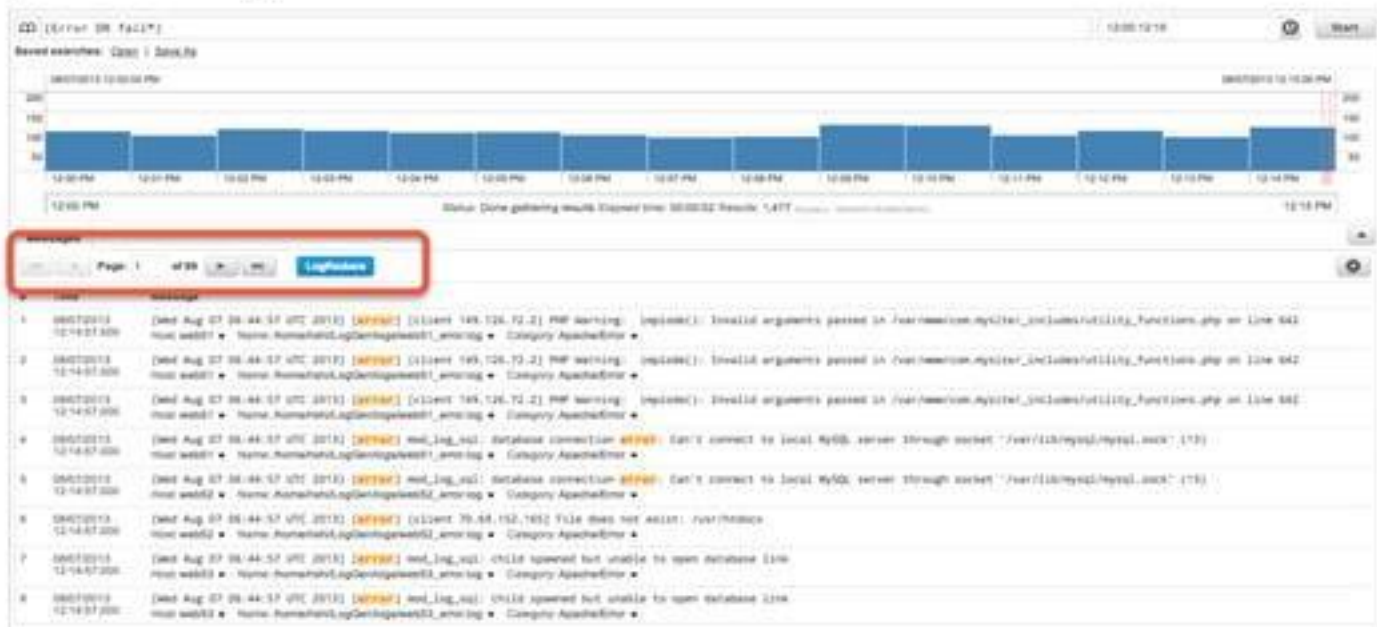
The table of messages is as follows:

#	Time	Message
1	08/22/2013 19:20:15.000	[Aug 22 13:50:15] [error] [client 149.126.72.2] PHP Warning: implode(): Invalid arguments passed in /var/www/csm.mysite/includes/utility_functions.php on line 642 Host: apache Name: /var/sunolabs/log/web02_error.log Category: Apache/Access
2	08/22/2013 19:20:15.000	[Aug 22 13:50:15] [error] mod_log_sql: database connection error: Can't connect to local MySQL server through socket '/var/lib/mysql/mysql.sock' (13) Host: apache Name: /var/sunolabs/log/web02_error.log Category: Apache/Access
3	08/22/2013 19:20:15.000	[Aug 22 13:50:15] [error] mod_log_sql: child spawned but unable to open database link Host: apache Name: /var/sunolabs/log/web01_error.log Category: Apache/Access
4	08/22/2013 19:20:15.000	[Aug 22 13:50:15] [error] mod_log_sql: child spawned but unable to open database link Host: apache Name: /var/sunolabs/log/web01_error.log Category: Apache/Access
5	08/22/2013 19:20:15.000	[Aug 22 13:50:15] [error] mod_log_sql: child spawned but unable to open database link Host: apache Name: /var/sunolabs/log/web01_error.log Category: Apache/Access
6	08/22/2013 19:20:15.000	[Aug 22 13:50:15] [error] mod_log_sql: database connection error: Can't connect to local MySQL server through socket '/var/lib/mysql/mysql.sock' (13) Host: apache Name: /var/sunolabs/log/web01_error.log Category: Apache/Access
7	08/22/2013 19:20:15.000	[Aug 22 13:50:15] [error] mod_log_sql: child spawned but unable to open database link Host: apache Name: /var/sunolabs/log/web01_error.log 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



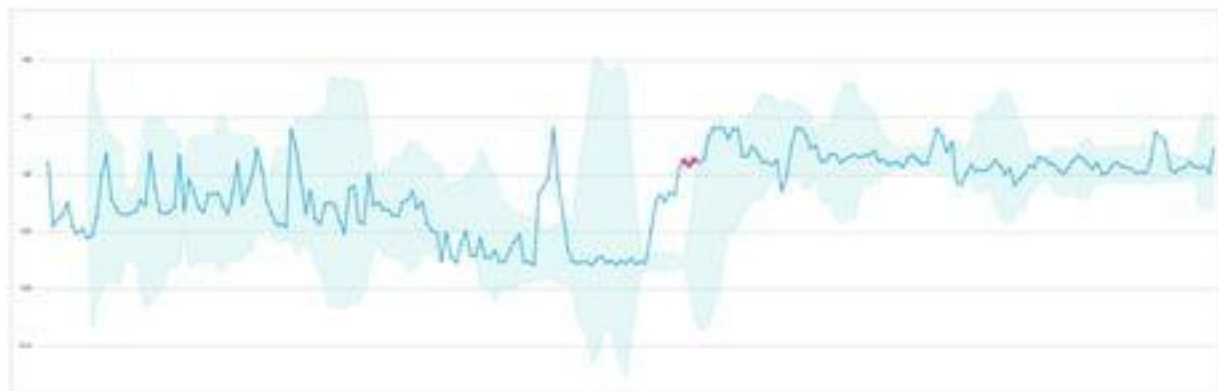
Looking for the Unknown

- 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



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)

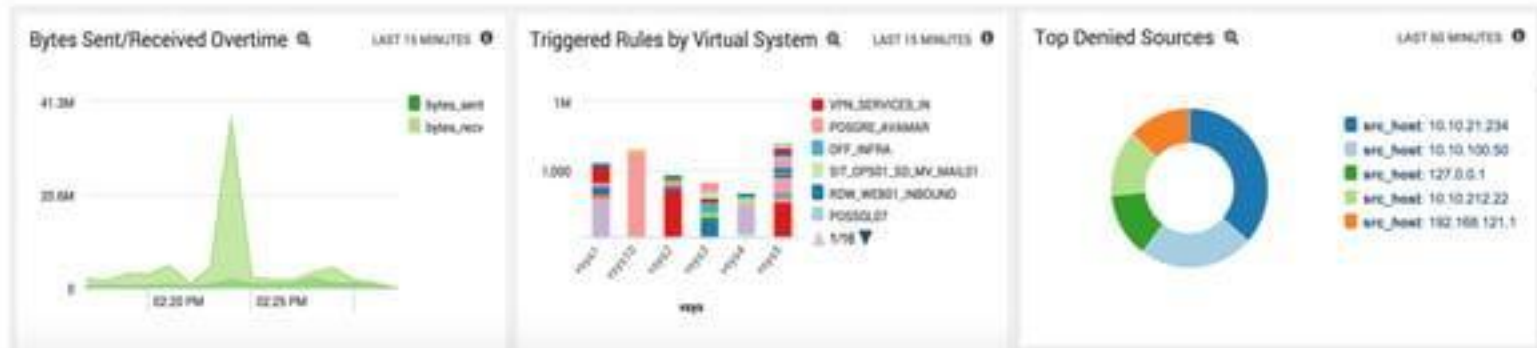


An abstract network diagram with various sized nodes (circles) in shades of blue, green, and grey, connected by thin lines. The nodes are distributed across the slide, with a higher concentration in the lower-left and middle areas.

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

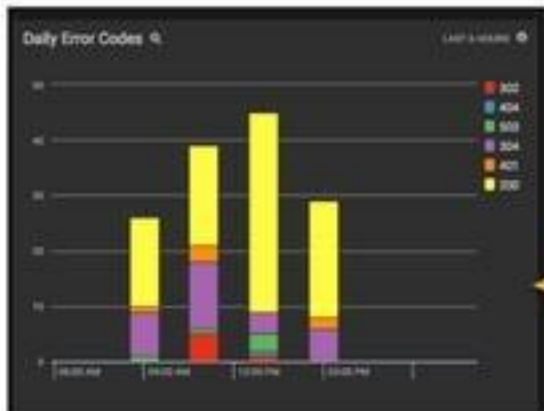
- Chart Types

- 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

 Library Search Anomalies Dashboards Manage Help Mario (SumoLabs)

Recent

Favorites

Personal

Org

Apps

Apps

Active Directory

Akamai Cloud Monitor

Amazon CloudFront

Amazon S3 Audit


Apache

Apache Tomcat

Artifactory

Audit

AWS CloudTrail



Apache

The Sumo Logic App for Apache uses searches and Dashboards to help you stay aware of web server operations, visitor information, and errors.

Install

NAME	DESCRIPTION
Apache - Overview	
Apache - Visitor Access Types	
Apache - Visitor Locations	
Apache - Visitor Traffic Insight	
Apache - Web Server Operatio...	
All HTTP Response codes wit...	
Client Errors (4xx response co...	



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!