sumologic Search Examples Cheat Sheet

For the examples below, refer to this sample Apache log message where applicable:

```
10.154.181.28 - - [24/Jan/2012:12:34:58 -0700] "GET /Courses/Topics/54.htm HTTP/1.1"
200 9951 "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.7 (KHTML, like Gecko)
Chrome/16.0.912.75 Safari/535.7"
```

Host: raw_hosted_apps Name: /usr/sumo/collector-16.1-5/logs/reporter.log Category: apache

KEYWORD EXPRESSIONS	SUMO LOGIC QUERY EXAMPLE
Look for failed attempts to su or sudo to root.	(su OR sudo) AND (fail* OR error)
Look for errors in sshd logs.	sshd AND (fail* OR error OR allowed OR identity)
Look for general authorization failures excluding router messages.	auth* AND (fail* OR error?) NOT _sourceCategory=routers
PARSE, COUNT, & SORT OPERATORS	**SUMO LOGIC QUERY EXAMPLE**
Extract "from" and "to" fields using regular expressions. For example, if a raw event contains "From: Jane To: John", then from=Jane and to=John.	* | parse "From: * To: *" as (from, to)
Extract the source IP addresses using a regex pattern for the four octects of an IP address.	*| parse regex "(?<src_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})"
Identify all URL addresses visited from users on your network from Source Category "apache", extract them as the "url" field.	_sourceCategory=apache | parse "GET * " as url
Identify traffic from Source Category "apache" and extract the source addresses, message sizes, and the URLs visited.	_sourceCategory=apache | parse "* " as src_IP | parse " 200 * " as size | parse "GET * " as url
For the Source Category "apache", calculate the total number of bytes transferred to each source IP address.	_sourceCategory=apache | parse "* " as src_IP | parse " 200 * " as size | count, sum(size) by src_IP
For the Source Category "apache", calculate the average size of all successful HTTP responses.	_sourceCategory=apache | parse " 200 * " as size | avg(size)
For the Source Category "apache", parse out src, size, and URL even if the size field is missing from the log message (nodrop).	_sourceCategory=apache | parse "* " as src_IP | parse " 200 * " as size nodrop | parse "GET * " as url
Identify the number of times a URL has been visited.	_sourceCategory=apache | parse "GET * " as url | count by url
Identify the total number of pages by source IP addresses.	_sourceCategory=apache | parse "* -" as src_ip | count by src_ip
Identify the total number of pages by source IP address sorted, re-order them by most frequently loaded pages.	_sourceCategory=apache | parse "* " as src_ip | parse "GET * " as url | count by src_ip | sort by _count
Identify the top 10 URLs.	* | parse "GET * " as url | count by url | sort by _count | limit 10
Identify the top 10 source IP addresses by bandwidth usage.	_sourceCategory=apache | parse " 200 * " as size | parse "* -" as src_ip | sum(size) as total_bytes by src_ip | sort by total_bytes | limit 10
Identify the top 100 source IP addresses by number of hits.	_sourceCategory=apache | parse "* -" as src_ip | count by src_ip | sort by _count | limit 100
WHERE OPERATOR	**SUMO LOGIC QUERY EXAMPLE**
Use the where operator to match only weekend days.	* | parse "day=*:" as day_of_week | where day_of_week in ("Saturday","Sunday")
Identify all URLs that contain the subdirectory "Courses" in the path.	*| parse "GET * " as url | where url matches "*Courses*"
Find version numbers that match numeric values 2, 3 or 6. Use the num operator to change the string into a number.	* | parse "Version=*." as number | num(number) | where number in (2,3,6)
SUMMARIZE OPERATOR	**SUMO LOGIC QUERY EXAMPLE**
Use Sumo Logic's clustering algorithm to look for patterns in error/exception incidents in your deployment.	exception* or fail* or error* or fatal* | summarize

A Note about Metadata: For any query, you can increase specificity by adding metadata fields to the keyword espression. Metadata fields include _sourceCategory, _sourceHost , and _sourceName. Edit Source metadata in the Collectors tab of the Web Application.