Cheatography

[LR] Web Console Display Name - Lucene Syntax Cheat Sheet

by DonPromillo via cheatography.com/40290/cs/12396/

Examples

To escape a special character that is part of the query syntax, use a backslash before the character. Characters that require this treatment are: + - && || ! ( ) { } [ ] ^ " ~ * ? : \

Operators: **|| OR AND && NOT !**

If you wanted to run a query for all impacted users whose account ends with Smith, you would use: **login:/.*Smith/**

If you wanted to run a query for impacted users whose names are similar to Jon, such as Ron or John, you would use: **login:Jon~**

If you wanted to run a query for all activity that falls under the Malware or Attack classifications, you would use: **classificationName:("Malware" "Attack")**

If you wanted to run a query for the host from which a log activity originated, INCLUSIVE of the first and last IP address, you would use: **originHost: [106.194.190.210 TO 106.194.190.250]**

If you wanted to run a query for the host from which a log activity originated, EXCLUSIVE of the first and last IP address, you would use: **originHost: {106.194.190.210 TO 106.194.190.250}**

Network

Domain (Impacted)	`domainImpacted`
Domain (Origin)	`domainOrigin`
NAT TCP/UDP Port (Impacted)	`impactedNatPort`
NAT TCP/UDP Port (Origin)	`originNatPort`
Network (Impacted)	`impactedNetwork`
Network (Origin)	`originNetwork`
Protocol	`protocolName`
Session	`session`
Session Type	`sessionType`
TCP/UDP Port (Origin)	`originPort`
TCP/UDP Port (Impacted)	`impactedPort`
URL	`url`
User Agent	`userAgent`

Classification

Classification	`classificationName`
Common Event	`commonEventName`
CVE	`cve`
Direction	`directionName`
MPE Rule Name	`mpeRuleName`
Policy	`policy`
Reason	`reason`
Response Code	`esponseCode`
Result	`result`
Severity	`severity`
Status	`status`
Threat Name	`threatName`
Vendor Info	`vendorInfo`
Vendor Message ID	`vendorMessageId`

Applications

Action	`action`
Amount	`amount`
Command	`command`
Duration	`duration`
Hash	`hash`
Known Appliaction	`serviceName`
Object	`object`
Object Name	`objectName`
Object Type	`objectType`
Parent Process ID	`parentProcessId`
Parent Process Path	`parentProcessPath`
Process Name	`process`
Process ID	`processId`
Quantity	`quantity`
Rate	`rate`
Size	`size`
Subject	`subject`
Thread ID	`threatid`
Version	`version`

Cheatography

[LR] Web Console Display Name - Lucene Syntax Cheat Sheet

by DonPromillo via cheatography.com/40290/cs/12396/

Host	
Host (Impacted)	impactedHost
Host (Origin)	originHost
Hostname (Impacted)	impactedName
Hostname (Origin)	originName
Interface (Impacted)	impactedInterface
Interface (Origin)	originInterface
IP Address (Impacted)	impactedIp
IP Address (Origin)	originIp
Known Host (Impacted)	impactedHostName
Known Host (Origin)	originHostName
Mac Address (Impacted)	impactedMac
Mac Address (Origin)	originMac
NAT IP Address (Impacted)	impactedNatIp
NAT IP Address (Origin)	originNatIp
Serial Number	serialNumber

Log	
First Log Date	normalMsgDate
Last Log Date	normalDateMax
Log Count	count
Log Date	normalDate
Log Message	logMessage
Log Source	logSourceName
Log Source Entity	entityName
Log Source Host	logSourceHostName
Log Source Type	logSourceTypeName
Log Sequence Number	sequenceNumber

Location	
Country (Impacted)	impactedCountry
Country (Origin)	originCountry
Entity (Impacted)	impactedEntityName
Entity (Origin)	originEntityName
Location (Impacted)	impactedLocation
Location (Origin)	originLocation

Location (cont)	
Region (Impacted)	impactedRegion
Region (Origin)	originRegion
Zone (Impacted)	impactedZoneName
Zone (Origin)	originZoneName

Traffic	
Host (Impacted) KBytes Rcvd	kBytesIn
Host (Impacted) KBytes Sent	kBytesOut
Host (Impacted) KBytes Total	impactedHostTotalKBytes
Host (Impacted) Packets Rcvd	itemsPacketsIn
Host (Impacted) Packets Sent	itemsPacketsOut
Host (Impacted) Packets Total	impactedHostTotalPackets
KBytes Inbound	kBytes
KBytes Outbound	outboundKBytes

Identity	
Group	group
Recipient	recipient
Sender	sender
User (Origin)	login
User (Impacted)	account