MICROSOFT OPERATIONS MANAGEMENT SUITE (OMS) – LOG SEARCH CHEAT SHEET

SOURCE (REQUIRED)

Syntax:
Literal strings, keywords e.g.
*, error, warning, fail, ID4323, system

by Type field use = or : / solution (not complete list):
Type=Event
Type=PerfHourly
Type=Alert

Notes:

- Use * to return all available data
- Wildcarding Type=*SQL* finds all records containing "SQL"
- Literal string "Windows Server" returns only results containing "Windows Server"
- Records on a specific point in time
  TimeGenerated:2016-10-01T12:20
  Time formats:
  - yyyy-mm-ddThh:mm:ss.dddZ
  - yyyy-mm-ddThh:mm:ss.ddd
  - yyyy-mm-ddThh:mm:ss
  - yyyy-mm-ddThh:mm:ss
  - yyyy-mm-ddThh:mm
  - yyyy-mm-dd

RegEx Syntax:
Example:
server01.domain.com
Computer=RegEx("server..@")
Computer=RegEx("server...domain.com")

@	Any string of characters
.	Any single character
a?	Zero or one occurance
a*	Zero or more occurances
a+	One or more occurances
[abc]	Match any character in brackets
[^abc]	None of the characters in brackets
[a-z]	Match any single character in the brackets
[^a-z]	None of the characters in the range
[n-m]	Match a range of numeric characters

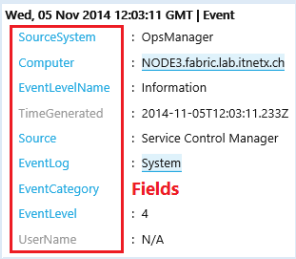
OPERATOR

Use one or more:
AND
OR
NOT

FIELD

Syntax (Case Sensitive):
Field=Value or
Field:Value
Field > Value or >=,<,<=
Field:[from..to]

Example:
EventLog:"System"



Syntax:
IN

Example:
Type=Event EventID IN {4634,1201}

TIME

Syntax:
NOW
YEAR(S)
MONTH(S)
DAY(S)
HOUR(S)
MINUTE(S)
SECOND(S)
MILLISECOND(S)

INTERVAL

Example:
NOW-3HOURS
MONTH+4DAYS
INTERVAL 1DAY

„PIPE"

Step2: Use pipe "|" symbol to separate commands to sort, aggregate or filter result

Optional Step 1: Use pipe "|"to crunch/extend and calculate

SORT

Syntax:
SORT
[ASC/DESC]

SELECT

Syntax:
TOP
LIMIT
SKIP
SELECT

AGGREGATE

Syntax:
MEASURE

Functions:
COUNT()
MAX(Field)
MIN(Field)
SUM(Field)
AVG(Field)
STDDEV(Field)

Alias:
AS
[Expression]

Group:
[by Field]

DEDUP/EXTEND

Syntax:
DEDUP
EXTEND

Example:
Type=Event | DEDUP EventID

Type=Perf CounterName="Private Bytes" | EXTEND div(CounterValue,1024) AS KBs

WHERE

Syntax:
WHERE

Example:
WHERE [Expression] >1

Time:
INTERVAL 1HOUR

FUNCTIONS

Syntax:

abs(x)	exp(x)	product(x,y,..)
acos(x)	floor(x)	recip()
and()	hypo(x,y)	rad(x)
asin(x)	if()	rint(x)
atan(x)	linear()	sin(x)
atan2(x,y)	ln(x)	sinh(x)
cbrt(x)	log(x)	scale()
ceil(x)	map()	sqrt()
cos(x)	max(x,y,..)	strdist()
cosh(x)	min(x,y,..)	sub(x,y)
def()	mod(x,y)	sum(x,y,..)
deg(x)	ms()	termfreq()
div(x,y)	not()	tan(x)
dist()	or()	tanh(x)
exists()	pow(x,y)	

MICROSOFT OPERATIONS MANAGEMENT SUITE (OMS) – LOG SEARCH CHEAT SHEET

Examples:

If you don't receive any data it could be, that you haven't installed the necessary solution. These queries should illustrate how to write simple and more complex queries.

Retrieves all Events
Type=Event

Retrieve all Type, grouped by Type
*** | MEASURE COUNT() by Type**

Retrieve Events 100 up to 3000 from Application Log
Type=Event EventLog=Application EventID:[100..3000]

Count of Events grouped by Event ID
Type=Event | MEASURE COUNT() by EventID

List all available Type
*** | MEASURE COUNT() by Type**

When did my servers initiate restart?
shutdown Type=Event EventLog=System Source=User32 EventID=1074 | SELECT TimeGenerated,Computer

Which management group sends most data
*** | MEASURE count() by ManagementGroupName**

Searches all Events for shutdown warning event
shutdown Type=Event EventLog=System Source=User32 EventLevelName=warning

On which machines and how many times have Windows Firewall Policy settings changed
Type=Event EventLog="Microsoft-Windows-Windows Firewall With Advanced Security/Firewall" EventID=2008 | MEASURE COUNT() by Computer

Computer with Available Memory more than 2GB and display it as line chart
Type=Perf ObjectName=Memory CounterName="Available MBytes" | MEASURE AVG(CounterValue) by Computer | WHERE AggregatedValue>2000 | DISPLAY lineChart

Stale Computers (data older than 24 hours)
NOT(ObjectName="Advisor Metrics" OR ObjectName=ManagedSpace) | MEASURE MAX(TimeGenerated) as LastData by Computer | TOP 500000 | WHERE LastData < NOW-24HOURS

Active Recommendations for databases
Type=SQLAssessmentRecommendation RecommendationResult=Failed | MEASURE COUNT() by DatabaseName

List all Computers whose last reported data is older than 4 hours
ObjectName!="Advisor Metrics" ObjectName!=ManagedSpace ObjectName!="Advisor Metrics" ObjectName!=ManagedSpace | MEASURE MAX(TimeGenerated) as LastData by Computer | WHERE LastData<NOW-4HOURS | SORT Computer

Computers with detected threats
Type=ProtectionStatus ThreatStatusRank > 199 ThreatStatusRank != 470 | MEASURE MAX(ThreatStatusRank) as Rank by Computer | Top 50000

Average CPU utilization by Top 5 machines
Type=Perf CounterName="% Processor Time" InstanceName="_Total" | MEASURE AVG(SampleValue) as AVGCPU by Computer | SORT AVGCPU DESC | TOP 5

Returns % CPU Usage and % Free Disk Space in the past 4 hours
Type=Perf InstanceName:_Total ((ObjectName:Processor AND CounterName:"% Processor Time") OR (ObjectName="LogicalDisk" AND CounterName="% Free Space")) AND TimeGenerated>NOW-4HOURS

List all Events that have "Ops" in their SourceSystem field
Type=Event SourceSystem=RegEx("Ops@")

List all Events that have "Bytes Sent/sec" in CounterPath
Type=Perf CounterPath=Regex("@Bytes Sent/sec@")

List all network adapters which do not contain Realtek RTL8139C
Type=Perf InstanceName=Regex("[^Realtek RTL8139C]@")

List all Heartbeat events from OS version 5, 6 and 7
Type=Heartbeat OSMajorVersion=RegEx("[5-7]")

Tips & Tricks:

- ***NOW/DAY*** rounds the current Date/Time to the midnight of the current day.
- Every item has ***TimeGenerated*** field which can be used to filter the data
- Use display LineChart, display StackedBarChart to visualize your data
- "Type" is a field name and therefore case sensitive. "TYPE" does not work!

Sources:

- Log Search Overview (Microsoft)
- Log Analytics Search Reference (Microsoft)
- OMS Blog (Microsoft)