Example of using Splunk TA for MS SQL to collect PerfMon data as metrics instead of events. Complements Windows TA (inputs) and SAI (props) to parse.

TL/DR set inputs as metrics, add \_meta to help filter/differentiate sql hosts in SAI and set sourcetype to parse as metrics as per Splunk TA Infrastructure.

1. Inputs.conf on UF

##### Monitor inputs

# ERROR Log for SQL Server

[monitor://D:\Program Files\Microsoft SQL Server\MSSQL\*\MSSQL\Log\ERRORLOG\*]

sourcetype = mssql:errorlog

disabled = 0

index = database

# Default SQL Server Agent Log for the SQL Server Agent Service of SQL Server

[monitor://D:\Program Files\Microsoft SQL Server\MSSQL\*\MSSQL\Log\SQLAGENT.OUT]

sourcetype = mssql:agentlog

disabled = 0

index = database

##### Windows performance monitoring inputs

### Performance Monitoring for System

# Reference Splunk\_TA\_windows for standard PerfMon collection

[perfmon://PhysicalDisk]

counters = % Disk Read Time;% Disk Write Time;Current Disk Queue Length;% Disk Time;% Idle Time;Avg. Disk sec/Read; Avg. Disk sec/Write;Disk Reads/sec;Disk Writes/sec;Avg. Disk sec/Transfer;Disk Read Bytes/sec;Disk Write Bytes/sec;Avg. Disk Queue Length

\_meta = os::"Microsoft Windows" entity\_type::Windows\_Host database::mssql

[perfmon://Memory]

counters = Pages/sec;Available Mbytes;Pages Input/sec;Free System Page Table Entries;Available Bytes;Commit Limit;Cache Faults/sec;Cache Bytes;System Cache Resident Bytes;% Committed Bytes In Use;Page Reads/sec;Pages Input/sec;Pages Output/sec;Committed Bytes

\_meta = os::"Microsoft Windows" entity\_type::Windows\_Host database::mssql

[perfmon://System]

counters = Processor Queue Length;System Up Time;Threads;Context Switches/sec

\_meta = os::"Microsoft Windows" entity\_type::Windows\_Host database::mssql

[perfmon://Process]

\_meta = os::"Microsoft Windows" entity\_type::Windows\_Host database::mssql

[perfmon://PagingFile]

counters = % Usage;% Usage Peak

\_meta = os::"Microsoft Windows" entity\_type::Windows\_Host database::mssql

### Performance Monitoring for SQL Server

[perfmon://sqlserver:buffer\_manager]

object = (SQLServer|MSSQL[^:]\*):Buffer Manager

counters = Page life expectancy;Buffer cache hit ratio

interval = 60

disabled = 0

mode = single

useEnglishOnly = true

\_meta = os::"Microsoft Windows" entity\_type::Windows\_Host database::mssql

sourcetype = PerfmonMetrics:MSSQL

index = em\_metrics

[perfmon://sqlserver:memory\_manager]

object = (SQLServer|MSSQL[^:]\*):Memory Manager

counters = Total Server Memory(KB);Memory Grants Pending

interval = 60

disabled = 0

mode = single

useEnglishOnly = true

\_meta = os::"Microsoft Windows" entity\_type::Windows\_Host database::mssql

sourcetype = PerfmonMetrics:MSSQL

index = em\_metrics

[perfmon://sqlserver:databases]

object = (SQLServer|MSSQL[^:]\*):Databases

counters = Active Transactions;Data File(s) Size (KB);Log File(s) Size (KB);Log File(s) Used Size (KB);Transactions/sec

instances = \*

interval = 60

disabled = 0

mode = single

useEnglishOnly = true

\_meta = os::"Microsoft Windows" entity\_type::Windows\_Host database::mssql

sourcetype = PerfmonMetrics:MSSQL

index = em\_metrics

[perfmon://sqlserver:general\_statistics]

object = (SQLServer|MSSQL[^:]\*):General Statistics

counters = User Connections;Processes blocked

interval = 60

disabled = 0

mode = single

useEnglishOnly = true

\_meta = os::"Microsoft Windows" entity\_type::Windows\_Host database::mssql

sourcetype = PerfmonMetrics:MSSQL

index = em\_metrics

[perfmon://sqlserver:sql\_statistics]

object = (SQLServer|MSSQL[^:]\*):SQL Statistics

counters = Batch Requests/sec

interval = 60

disabled = 0

mode = single

useEnglishOnly = true

\_meta = os::"Microsoft Windows" entity\_type::Windows\_Host database::mssql

sourcetype = PerfmonMetrics:MSSQL

index = em\_metrics

[perfmon://sqlserver:access\_methods]

object = (SQLServer|MSSQL[^:]\*):Access Methods

counters = Forwarded Records/sec;Full Scans/sec;Index Searches/sec;Page Splits/sec;Workfiles Created/sec;Worktables Created/sec;Worktables From Cache Ratio;Table Lock Escalations/sec

instances = \*

interval = 60

disabled = 1

mode = single

useEnglishOnly = true

[perfmon://sqlserver:latches]

object = (SQLServer|MSSQL[^:]\*):Latches

counters = Latch Waits/sec;Avg Latch Wait Time (ms);Total Latch Wait Time (ms)

interval = 60

disabled = 1

mode = single

useEnglishOnly = true

\_meta = os::"Microsoft Windows" entity\_type::Windows\_Host database::mssql

sourcetype = PerfmonMetrics:MSSQL

index = em\_metrics

[perfmon://sqlserver:sql\_errors]

object = (SQLServer|MSSQL[^:]\*):SQL Errors

counters = Errors/sec

instances = DB Offline Errors;Info Errors;Kill Connection Errors;User Errors;\_Total

interval = 60

disabled = 1

mode = single

useEnglishOnly = true

\_meta = os::"Microsoft Windows" entity\_type::Windows\_Host database::mssql

sourcetype = PerfmonMetrics:MSSQL

index = em\_metrics

[perfmon://sqlserver:locks]

object = (SQLServer|MSSQL[^:]\*):Locks

counters = Number of Deadlocks/sec;Average Wait Time (ms)

instances = \*

interval = 60

disabled = 0

mode = single

useEnglishOnly = true

\_meta = os::"Microsoft Windows" entity\_type::Windows\_Host database::mssql

sourcetype = PerfmonMetrics:MSSQL

index = em\_metrics

[perfmon://sqlserver:transactions]

object = (SQLServer|MSSQL[^:]\*):Transactions

counters = Transactions; Longest Transaction Running Time

interval = 60

disabled = 0

mode = single

useEnglishOnly = true

\_meta = os::"Microsoft Windows" entity\_type::Windows\_Host database::mssql

sourcetype = PerfmonMetrics:MSSQL

index = em\_metrics

1. props.conf on parsing/indexing layer

Appended this to Splunk\_TA\_Infrastructure/local/props.conf

[PerfmonMetrics:MSSQL]

TRANSFORMS-\_value\_for\_perfmon\_metrics\_store\_sai = value\_for\_perfmon\_metrics\_store\_sai

TRANSFORMS-metric\_name\_for\_perfmon\_metrics\_store\_sai = metric\_name\_for\_perfmon\_metrics\_store\_sai

TRANSFORMS-object\_for\_perfmon\_metrics\_store\_sai = object\_for\_perfmon\_metrics\_store\_sai

TRANSFORMS-instance\_for\_perfmon\_metrics\_store\_sai = instance\_for\_perfmon\_metrics\_store\_sai

TRANSFORMS-collection\_for\_perfmon\_metrics\_store\_sai = collection\_for\_perfmon\_metrics\_store\_sai

EVAL-metric\_type = "gauge"

SEDCMD-remove-whitespace = s/ /\_/g s/\s/ /g