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.

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

# MSSQL

[mssql:instance]

FIELDALIAS-session\_limit = MaxConnections AS session\_limit

EVAL-vendor\_product = "Microsoft SQL Server"

FIELDALIAS-character\_set = SqlCharSetName AS character\_set

FIELDALIAS-collation = Collation AS collation

EVAL-vendor = "Microsoft"

FIELDALIAS-version = ProductVersion AS version

FIELDALIAS-database\_instance = ServerName AS database\_instance

FIELDALIAS-database\_name = DatabaseName AS database\_name

EVAL-instance\_role = "database\_instance"

LOOKUP-host= sqlserver\_host\_dbserver\_lookup database\_instance OUTPUT host

LOOKUP-port= sqlserver\_host\_dbserver\_lookup database\_instance OUTPUT port

[mssql:os:dm\_os\_performance\_counters]

FIELDALIAS-database\_instance = ServerName AS database\_instance

FIELDALIAS-database\_name = DatabaseName AS database\_name

EVAL-instance\_read\_iops = case(counter\_name="Page reads/sec", cntr\_value)

EVAL-instance\_write\_iops = case(counter\_name="Page writes/sec", cntr\_value)

EVAL-transaction\_rate = case(counter\_name="Transactions/sec" AND instance\_name="\_Total", cntr\_value)

EVAL-current\_size = case(counter\_name="Data File(s) Size (KB)" AND instance\_name="\_Total", cntr\_value/1024)

EVAL-connection\_pool\_used\_percent = case(counter\_name="User Connections", cntr\_value\*100/max\_connection)

EVAL-connections = case(counter\_name="User Connections", cntr\_value)

EVAL-active\_transactions = case(counter\_name="Open Connection Count", cntr\_value)

EVAL-deadlock\_rate = case(counter\_name="Number of Deadlocks/sec" AND instance\_name="\_Total", cntr\_value)

EVAL-error\_rate = case(counter\_name="Errors/sec" AND instance\_name="\_Total", cntr\_value)

LOOKUP-host= sqlserver\_host\_dbserver\_lookup database\_instance OUTPUT host

LOOKUP-port= sqlserver\_host\_dbserver\_lookup database\_instance OUTPUT port

[mssql:table]

DATETIME\_CONFIG = NONE

FIELDALIAS-table\_name = TableName AS table\_name

FIELDALIAS-row\_count = RowCounts AS row\_count

FIELDALIAS-last\_update\_time = ModifyTime AS last\_update\_time

EVAL-size = TableSizeKB/1024

FIELDALIAS-database\_instance = ServerName AS database\_instance

FIELDALIAS-database\_name = DatabaseName AS database\_name

LOOKUP-host= sqlserver\_host\_dbserver\_lookup database\_instance OUTPUT host

LOOKUP-port= sqlserver\_host\_dbserver\_lookup database\_instance OUTPUT port

[mssql:user]

DATETIME\_CONFIG = NONE

FIELDALIAS-user\_name = name AS user\_name

FIELDALIAS-user\_id = principal\_id AS user\_id

FIELDALIAS-database\_instance = ServerName AS database\_instance

FIELDALIAS-database\_name = DatabaseName AS database\_name

LOOKUP-host= sqlserver\_host\_dbserver\_lookup database\_instance OUTPUT host

LOOKUP-port= sqlserver\_host\_dbserver\_lookup database\_instance OUTPUT port

[mssql:os:dm\_os\_sys\_info]

FIELDALIAS-session\_limit = max\_workers\_count AS session\_limit

FIELDALIAS-uptime = time\_of\_last\_restart AS uptime

EVAL-mem = case(isnotnull(physical\_memory\_kb),round(physical\_memory\_kb/1024,2),isnotnull(physical\_memory\_in\_bytes),round(physical\_memory\_in\_bytes/1024/1024,2))

EVAL-mem\_committed = case(isnotnull(committed\_target\_kb),round(committed\_target\_kb/1024,2),isnotnull(bpool\_commit\_target),round(bpool\_commit\_target/1024,2))

EVAL-vendor\_product = "Microsoft SQL Server"

FIELDALIAS-database\_instance = ServerName AS database\_instance

FIELDALIAS-database\_name = DatabaseName AS database\_name

LOOKUP-host= sqlserver\_host\_dbserver\_lookup database\_instance OUTPUT host

LOOKUP-port= sqlserver\_host\_dbserver\_lookup database\_instance OUTPUT port

[mssql:instancestats]

FIELDALIAS-instance\_reads = total\_reads AS instance\_reads

FIELDALIAS-instance\_writes = total\_writes AS instance\_writes

FIELDALIAS-number\_of\_users = total\_users AS number\_of\_users

FIELDALIAS-sessions = total\_sessions AS sessions

EVAL-vendor\_product = "Microsoft SQL Server"

FIELDALIAS-database\_instance = ServerName AS database\_instance

FIELDALIAS-database\_name = DatabaseName AS database\_name

LOOKUP-host= sqlserver\_host\_dbserver\_lookup database\_instance OUTPUT host

LOOKUP-port= sqlserver\_host\_dbserver\_lookup database\_instance OUTPUT port

[mssql:execution:dm\_exec\_sessions]

FIELDALIAS-elapsed\_time = total\_elapsed\_time AS elapsed\_time

FIELDALIAS-physical\_reads = reads AS physical\_reads

FIELDALIAS-session\_status = status AS session\_status

EVAL-cpu\_used = cpu\_time/10

FIELDALIAS-database\_instance = ServerName AS database\_instance

FIELDALIAS-database\_name = DatabaseName AS database\_name

LOOKUP-host= sqlserver\_host\_dbserver\_lookup database\_instance OUTPUT host

LOOKUP-port= sqlserver\_host\_dbserver\_lookup database\_instance OUTPUT port

[mssql:transaction:dm\_tran\_locks]

FIELDALIAS-lock\_session\_id = request\_session\_id AS lock\_session\_id

FIELDALIAS-lock\_mode = request\_mode AS lock\_mode

FIELDALIAS-serial\_num = request\_mode AS serial\_num

FIELDALIAS-os\_pid = request\_exec\_context\_id AS os\_pid

EVAL-vendor\_product = "Microsoft SQL Server"

FIELDALIAS-database\_instance = ServerName AS database\_instance

FIELDALIAS-database\_name = DatabaseName AS database\_name

LOOKUP-host= sqlserver\_host\_dbserver\_lookup database\_instance OUTPUT host

LOOKUP-port= sqlserver\_host\_dbserver\_lookup database\_instance OUTPUT port

[mssql:execution:dm\_exec\_query\_stats]

REPORT-kv = first\_level\_value\_with\_quotation

FIELDALIAS-query\_id = sql\_handle AS query\_id

FIELDALIAS-query = SQLStatement AS query

FIELDALIAS-query\_type = Command AS query\_type

FIELDALIAS-user = LoginName AS user

FIELDALIAS-response\_time = Cpu AS response\_time

FIELDALIAS-database\_instance = ServerName AS database\_instance

FIELDALIAS-database\_name = DatabaseName AS database\_name

LOOKUP-host= sqlserver\_host\_dbserver\_lookup database\_instance OUTPUT host

LOOKUP-port= sqlserver\_host\_dbserver\_lookup database\_instance OUTPUT port

[mssql:trclog]

REPORT-multi\_value\_with\_quotation = multi\_value\_with\_quotation

REPORT-multi\_value\_without\_quotation = multi\_value\_without\_quotation