Metrics Onboarding Workshop for IT Ops

Lab Sheet

This document will have the corresponding “text” and “commands” for the different activities. This should make it simpler to copy and paste into your Splunk environment.

Activity #2

Splunk_TA_windows

Inputs.conf:

```
[perfmon://CPU]
counters = % Processor Time; % User Time; % Privileged Time;
Interrupts/sec; % DPC Time; % Interrupt Time; DPCs Queued/sec; DPC
Rate; % Idle Time; % C1 Time; % C2 Time; % C3 Time; C1
Transitions/sec; C2 Transitions/sec; C3 Transitions/sec
disabled = 0
instances = *
interval = 60
mode = single
object = Processor
useEnglishOnly=true
sourcetype=PerfmonMetrics:CPU
index=itsi_im_metrics


[perfmon://LogicalDisk]
counters = % Free Space; Free Megabytes; Current Disk Queue Length; %
Disk Time; Avg. Disk Queue Length; % Disk Read Time; Avg. Disk Read
Queue Length; % Disk Write Time; Avg. Disk Write Queue Length; Avg.
Disk sec/Transfer; Avg. Disk sec/Read; Avg. Disk sec/Write; Disk
Transfers/sec; Disk Reads/sec; Disk Writes/sec; Disk Bytes/sec; Disk
Read Bytes/sec; Disk Write Bytes/sec; Avg. Disk Bytes/Transfer; Avg.
Disk Bytes/Read; Avg. Disk Bytes/Write; % Idle Time; Split IO/Sec
disabled = 0
instances = *
interval = 60
mode = single
object = LogicalDisk
```

```
useEnglishOnly=true
sourcetype=PerfmonMetrics:LogicalDisk
index=itsi_im_metrics


[perfmon://PhysicalDisk]
counters = Current Disk Queue Length; % Disk Time; Avg. Disk Queue
Length; % Disk Read Time; Avg. Disk Read Queue Length; % Disk Write
Time; Avg. Disk Write Queue Length; Avg. Disk sec/Transfer; Avg. Disk
sec/Read; Avg. Disk sec/Write; Disk Transfers/sec; Disk Reads/sec;
Disk Writes/sec; Disk Bytes/sec; Disk Read Bytes/sec; Disk Write
Bytes/sec; Avg. Disk Bytes/Transfer; Avg. Disk Bytes/Read; Avg. Disk
Bytes/Write; % Idle Time; Split IO/Sec
disabled = 0
instances = *
interval = 60
mode = single
object = PhysicalDisk
useEnglishOnly=true
sourcetype=PerfmonMetrics:PhysicalDisk
index=itsi_im_metrics


[perfmon://Memory]
counters = Page Faults/sec; Available Bytes; Committed Bytes; Commit
Limit; Write Copies/sec; Transition Faults/sec; Cache Faults/sec;
Demand Zero Faults/sec; Pages/sec; Pages Input/sec; Page Reads/sec;
Pages Output/sec; Pool Paged Bytes; Pool Nonpaged Bytes; Page
Writes/sec; Pool Paged Allocs; Pool Nonpaged Allocs; Free System Page
Table Entries; Cache Bytes; Cache Bytes Peak; Pool Paged Resident
Bytes; System Code Total Bytes; System Code Resident Bytes; System
Driver Total Bytes; System Driver Resident Bytes; System Cache
Resident Bytes; % Committed Bytes In Use; Available KBytes; Available
MBytes; Transition Pages RePurposed/sec; Free & Zero Page List Bytes;
Modified Page List Bytes; Standby Cache Reserve Bytes; Standby Cache
Normal Priority Bytes; Standby Cache Core Bytes; Long-Term Average
Standby Cache Lifetime (s)
disabled = 0
interval = 60
mode = single
object = Memory
useEnglishOnly=true
sourcetype=PerfmonMetrics:Memory
index=itsi_im_metrics
```

```
[perfmon://Network]
counters = Bytes Total/sec; Packets/sec; Packets Received/sec; Packets
Sent/sec; Current Bandwidth; Bytes Received/sec; Packets Received
Unicast/sec; Packets Received Non-Unicast/sec; Packets Received
Discarded; Packets Received Errors; Packets Received Unknown; Bytes
Sent/sec; Packets Sent Unicast/sec; Packets Sent Non-Unicast/sec;
Packets Outbound Discarded; Packets Outbound Errors; Output Queue
Length; Offloaded Connections; TCP Active RSC Connections; TCP RSC
Coalesced Packets/sec; TCP RSC Exceptions/sec; TCP RSC Average Packet
Size
disabled = 0
instances = *
interval = 60
mode = single
object = Network Interface
useEnglishOnly=true
sourcetype=PerfmonMetrics:Network
index=itsi_im_metrics

[perfmon://Process]
counters = % Processor Time; % User Time; % Privileged Time; Virtual
Bytes Peak; Virtual Bytes; Page Faults/sec; Working Set Peak; Working
Set; Page File Bytes Peak; Page File Bytes; Private Bytes; Thread
Count; Priority Base; Elapsed Time; ID Process; Creating Process ID;
Pool Paged Bytes; Pool Nonpaged Bytes; Handle Count; IO Read
Operations/sec; IO Write Operations/sec; IO Data Operations/sec; IO
Other Operations/sec; IO Read Bytes/sec; IO Write Bytes/sec; IO Data
Bytes/sec; IO Other Bytes/sec; Working Set - Private
disabled = 0
instances = *
interval = 60
mode = single
object = Process
useEnglishOnly=true
sourcetype=PerfmonMetrics:Process
index=itsi_im_metrics


[perfmon://ProcessorInformation]
counters = % Processor Time; Processor Frequency
disabled = 0
instances = *
interval = 60
mode = single
object = Processor Information
useEnglishOnly=true
```

```
sourcetype=PerfmonMetrics:ProcessorInformation
index=itsi_im_metrics


[perfmon://System]
counters = File Read Operations/sec; File Write Operations/sec; File
Control Operations/sec; File Read Bytes/sec; File Write Bytes/sec;
File Control Bytes/sec; Context
Switches/sec; System Calls/sec; File Data Operations/sec; System Up
Time; Processor Queue Length; Processes; Threads; Alignment
Fixups/sec; Exception Dispatches/sec; Floating Emulations/sec; %
Registry Quota In Use
disabled = 0
instances = *
interval = 60
mode = single
object = System
useEnglishOnly=true
sourcetype=PerfmonMetrics:System
index=itsi_im_metrics
```

Splunk_TA_nix

Inputs.conf:

```
[script://./bin/vmstat_metric.sh]
sourcetype = vmstat_metric
source = vmstat
interval = 60
disabled = 0
index=itsi_im_metrics

[script://./bin/iostat_metric.sh]
sourcetype = iostat_metric
source = iostat
interval = 60
disabled = 0
index=itsi_im_metrics

[script://./bin/ps_metric.sh]
sourcetype = ps_metric
source = ps
interval = 60
```

```
disabled = 0
index=itsi_im_metrics

[script://./bin/df_metric.sh]
sourcetype = df_metric
source = df
interval = 60
disabled = 0
index=itsi_im_metrics

[script://./bin/interfaces_metric.sh]
sourcetype = interfaces_metric
source = interfaces
interval = 60
disabled = 0
index=itsi_im_metrics

[script://./bin/cpu_metric.sh]
sourcetype = cpu_metric
source = cpu
interval = 60
disabled = 0
index=itsi_im_metrics
```

Activity #3

Deployment Server reload from browser:

https://<your Splunk server>:8089/services/deployment/server/serverclasses/_reload

Activity #4

```
index=itsi_im_metrics
```

mpreview command:

```
| mpreview index=itsi_im_metrics
```

mcatalog command:

```
| mcatalog values(metric_name) WHERE index=itsi_im_metrics
```

mstats command:

```
| mstats count where index=itsi_im_metrics metric_name=* by metric_name

| mstats avg("cpu_metric.pctIdle") WHERE index=itsi_im_metrics by host

| mstats chart=t avg("cpu_metric.pctIdle") WHERE index=itsi_im_metrics
by host span=1m

| mstats chart=t avg("df_metric.UsePct") WHERE index=itsi_im_metrics
by host span=1m

| mstats chart=t avg("Memory.Available_MBytes") WHERE
index=itsi_im_metrics by host span=1m
```