**Splunk CLI and update config steps**

1. **File load**

Splunk add oneshot to load file one at a time:

.\splunk.exe add oneshot "C:\Path\to\log\file.txt" -sourcetype vmstat\_monitor

1. **Directory monitoring**

Then you can add monitor the directory using CLI:

.\splunk.exe add monitor C:\Path\to\log\

Or can be added below entries in $SPLUNK\_HOME\etc\apps\search\local\inputs.conf config file setting to monitor the directory:

[monitor://C:\Path\to\log\]

disabled = false

1. **Source Type configuration**

For example, below vmstat output stored in a file called C:\Path\to\log\file.txt and you want to extract the filed using regular expression in the configuration file.

procs -----------memory---------- ---swap-- -----io---- --system-- -----cpu------ ---timestamp---

r b swpd free buff cache si so bi bo in cs us sy id wa st

1 0 308096 4078676 2021572 52275020 0 0 72 335 1 1 4 3 92 1 0 2018-11-06 22:10:14 GMT

0 0 308096 4047248 2021572 52274988 0 0 0 4 2781 9050 3 3 94 0 0 2018-11-06 22:10:15 GMT

0 0 308096 4034700 2021572 52275532 0 0 0 0 1571 4067 1 1 98 0 0 2018-11-06 22:10:16 GMT

0 0 308096 4034340 2021572 52275536 0 0 0 832 792 3505 0 0 99 0 0 2018-11-06 22:10:17 GMT

0 0 308096 4043140 2021572 52275544 0 0 0 84 846 3384 0 0 99 0 0 2018-11-06 22:10:18 GMT

1 0 308096 4088800 2021572 52275040 0 0 0 88 2356 7276 2 3 95 0 0 2018-11-06 22:10:19 GMT

0 0 308096 4081724 2021572 52274992 0 0 0 4 2257 7110 1 2 97 0 0 2018-11-06 22:10:20 GMT

0 0 308096 4092804 2021572 52274044 0 0 0 564 1138 1692 1 1 99 0 0 2018-11-06 22:10:21 GMT

1 0 308096 4094208 2021572 52273924 0 0 0 136 1197 1542 0 1 99 0 0 2018-11-06 22:10:22 GMT

0 0 308096 4107812 2021580 52273948 0 0 0 664 1735 2496 1 1 98 0 0 2018-11-06 22:10:23 GMT

0 0 308096 4118804 2021580 52273920 0 0 0 440 944 1482 0 0 99 0 0 2018-11-06 22:10:24 GMT

0 0 308096 4119452 2021580 52273884 0 0 0 100 670 776 0 0 100 0 0 2018-11-06 22:10:25 GMT

0 0 308096 4119700 2021580 52273888 0 0 0 0 551 565 0 0 100 0 0 2018-11-06 22:10:26 GMT

0 0 308096 4119824 2021580 52273892 0 0 0 0 573 614 0 0 99 0 0 2018-11-06 22:10:27 GMT

0 0 308096 4119824 2021580 52273896 0 0 0 344 668 1101 0 0 99 0 0 2018-11-06 22:10:28 GMT

0 0 308096 4119928 2021580 52273900 0 0 0 0 580 556 0 0 100 0 0 2018-11-06 22:10:29 GMT

0 0 308096 4121052 2021580 52273912 0 0 0 64 667 679 0 0 100 0 0 2018-11-06 22:10:30 GMT

0 0 308096 4121076 2021580 52273916 0 0 0 0 722 992 0 0 99 0 0 2018-11-06 22:10:31 GMT

Go to $SPLUNK\_HOME\etc\apps\search\local\ directory and update the below two .conf files. In props.conf file add below entries.

[vmstat\_monitor]

MAX\_TIMESTAMP\_LOOKAHEAD = 20

NO\_BINARY\_CHECK = 1

SHOULD\_LINEMERGE = FALSE

pulldown\_type = 1

REPORT-myname = vmstat\_fields

And in transforms.conf file add below entries.

[vmstat\_fields]

REGEX = \s+(?<r>[^\s]\*)\s+(?<b>[^\s]\*)\s+(?<swpd>[^\s]\*)\s+(?<free>[^\s]\*)\s+(?<buff>[^\s]\*)\s+(?<cache>[^\s]\*)\s+(?<si>[^\s]\*)\s+(?<so>[^\s]\*)\s+(?<bi>[^\s]\*)\s+(?<bo>[^\s]\*)\s+(?<in>[^\s]\*)\s+(?<cs>[^\s]\*)\s+(?<us>[^\s]\*)\s+(?<sy>[^\s]\*)\s+(?<id>[^\s]\*)\s+(?<wa>[^\s]\*)\s+(?<st>[^\s]\*)\s+(?<tm>.\*)