1·VIEW

Log Reader – Regular Expressions – Examples

monsalta
performance monitoring and tuning

1 Introduction

This document provides you with a few detailed examples of how regular expressions can be used when translating entries from a log file to information that can be used by the OneView Log Reader.

Use this document in cooperation with the document: 'OneView Log Reader – User Guide' to get details on how the log reader is used.

1.1 Regular Expression Example #1 – IIS Log

In each log line the OneView Log Reader looks for [Time stamp], [Transaction Name], [Availability] and [Response time].

The example below in red is an example of a log line from a log file:
10.104.14.10 2016-03-08 08:35:23 GET /front/administration.portal 200 34969 22.363

This log line has 15 different items – please refer to table below for all 15 items.

The OneView Log Reader should read and understand these 15 items and extract the information to be used in OneView. The information is marked in blue in the table below.

The OneView Log Reader will read each of the 15 items using a regular expression. The items that we want pass on to OneView needs to be marked with brackets (x) in the regular expression.

Item Number	Item Content	Item description	Read each item with this regular expression	Pass this on to OneView	We want to read these into OneView and forget the rest
1	10.104.14.10	IP	\S+		
2		Blank space	\s+		
3	2016-03-08	Date	(\d{4}-\d{2}-\d{2})	$1	Date - When did the user ask for this
4		Blank space	\s+		
5	08:35:23	Time stamp	(\d{2}:\d{2}:\d{2})	$2	Time - When did the user ask for this
6		Blank space	\s+		
7	GET	Text	\S+		
8		Blank space	\s+		
9	/front/administration.portal	Transaction Name	(\S+)	$3	Transaction name - What did the user ask for
10		Blank space	\s+		
11	200	HTTP Return code	(\d{3})	$4	Availability - Did the user get a useful response
12		Blank space	\s+		

13	34969	Number of bytes	\d+		
14		Blank space	\s+		
15	22.363	Response time	(\S+)	$5	Response Time – How long was the response time (In this case 22 seconds and 363 ms)

In the OneView LogReader the regular expression will look like:
\S+\s+(\d{4}-\d{2}-\d{2})\s+(\d{2}:\d{2}:\d{2})\s+\S+\s+(\S+)\s+(\d{3})\s+\d+\s+(\S+)

As already mentioned the OneView Log Reader looks for: [Time stamp], [Transaction Name], [Availability] and [Response time]. Based on the example above the OneView Log Reader now has enough information to build a new OneView LogReader definition. These are the details that should be provided:

[Time Stamp] is selection $1 $2
[Transaction Name] is selection $3
[Availability] is selection $4
[Response time] is selection $5

1.2 Regular Expression Example #2 – cBrain F2

Let us have a look at this log line from the cBrain F2 application. The information we want to extract is marked with blue.

As stated in example 1 the OneView Log Reader looks for [Time stamp], [Transaction Name], [Availability] and [Response time]. In this case we are looking for Time Stamp, Transaction Name and Response Time.

INFO 2016-03-17 09:08:00,525 14629497ms StaffId:326 LogOnUserStaffId:(null) [Elapsed: 8074ms] WebMethod : DoManagementCabinetRequest

Item Number	Item Content	Item description	Read each item with this regular expression	Pass this on to OneView	We want to read these into OneView and forget the rest
1	INFO	text	\S+		
2		Blank space	\s+		
3	2016-03-17 09:08:00,525	Date & Time	(\d{4}-\d{2}-\d{2}\s\d{2}:\d{2}:\d{2},\d{3})	$1	Date & Time - When did the user ask for this
4		Blank space	\s		
5	14629497ms StaffId:326 LogOnUserStaffId:(null) [Elapsed:	text	[^\[]+\[Elapsed:		
6		Blank space	\s*		
7	8074	Response time	(\d*)	$2	Response Time – How long was the response time (8074 ms)
8	ms]	Text	ms\]		
9	WebMethod :	Text	[^:]*:		
10		Blank space	\s		
11	DoManagementCabinetRequest	Text	(.*)	**$3**	Transaction name - What did the user ask for

In the OneView LogReader the regular expression will look like:
INFO\s+(\d{4}-\d{2}-\d{2}\s\d{2}:\d{2}:\d{2},\d{3})\s[^\[]+\[Elapsed:\s*(\d*)ms\][^:]*:\s(.*)

Based on the example above the OneView Log Reader now has enough information to build a new OneView LogReader definition. These are the details that should be provided:

[Time Stamp] is selection $1
[Transaction Name] is selection $2
[Response time] is selection $3
[Availability] There is no information about availability in this log file. If “Result string” is left blank the transaction is handled as successful.

1.3 Regular Expression Example #3 – Access Log File

Let us have a look at this log line from an access log file. The information we want to extract is marked with blue.

As stated in example 1 the OneView Log Reader looks for [Time stamp], [Transaction Name], [Availability] and [Response time]. In this case we are looking for all.

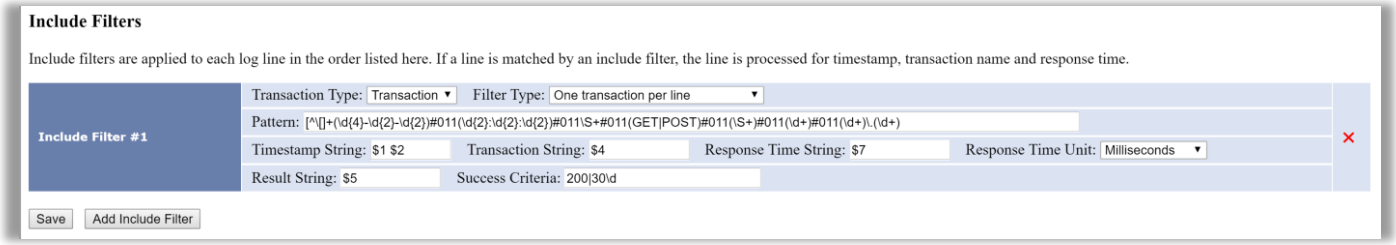
Mar 26 12:17:53 cs01por01 PorServer1_access.log: 2016-03-26#01112:17:47#011193.88.156.134#011GET#011/sanity-test-web/securitySanityTest.jsp#011200#0110.136

This log line has 15 different items – please refer to table below for all 16 items.

Item Number	Item Content	Item description	Read each item with this regular expression	Pass this on to OneView	We want to read these into OneView and forget the rest
1	Mar 26 12:17:53 cs01por01 PorServer1_access.log:	INFO	[^\[]+		
2	2016-03-26	Date	(\d{4}-\d{2}-\d{2})	$1	Timestamp – When did the transaction occur? In this case the timestamp consists of $1 and $2
3	#011	Blank space	#011		
4	12:17:47	Time	(\d{2}:\d{2}:\d{2})	$2	Timestamp – When did the transaction occur? In this case the timestamp consists of $1 and $2
5	#011	Blank space	#011		
6	193.88.156.134	Text	\S+		
7	#011	Blank space	#011		
8	GET	Text	(GET|POST)		
9	#011	Blank space	#011		
10	/sanity-test-web/securitySanityTest.jsp	Transaction Name	(\S+)	$4	Transaction Name – What did the user ask for
11	#011	Blank space	#011		
12	200	HTTP Return code	(\d+)	**$5**	Availability - Did the user get a useful response
13	#011	Blank space	#011		
14	0		(\d+)		
15	.		\.		
16	136	Response Time	(\d+)	**$7**	Response Time – How long was the response time – this time in milliseconds

In the OneView LogReader the regular expression will look like:

[^\[]+(\d{4}-\d{2}-
\d{2})#011(\d{2}:\d{2}:\d{2})#011\S+#011(GET|POST)#011(\S+)#011(\d+)#011(\d+)\.(\d+)



$1 og $2: Timestamp string - 12:17:53 2016-03-26
$4: Transaction string - sanity-test-web/ securitySanityTest.jsp
$5: Result string - 200
$7: Response time string – 136

1.4 Regular Expression Example #4 – Log Handler

Let us have a look at this log line from a log handler log file. The information we want to extract is marked with blue.

2016-04-08 06:57:41,077 INFO [default task-1] KlientPerformanceLogHandler - KlientTime: 2016-04-08 06:57:38,686 User: jaja0808 Operation: GemTilMasterPlan_Meddel Time: 2395 Size: -1

This log line has 12 different items – please refer to table below for all 12 items.

Item Number	Item Content	Item description	Read each item with this regular expression	Pass this on to OneView	We want to read these into OneView and forget the rest
1	2016-04-08 06:57:41,077	Date/Time	(\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2},\d{3})	$1	Timestamp – When did the transaction occur? In this case the timestamp consists of $1
2	INFO	INFO	\S+		
3	[default task-1] KlientPerformanceLogHandler	Text	\[\S+ \S+\] KlientPerformanceLogHandler		
4	- KlientTime:	Text	\S+ KlientTime:		
5	2016-04-08 06:57:38,686	Date/time	(\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2},\d{3})	$2	Not used in this example
6	User:	Text	User:		
7	jaja0808	Text	(\S+)	$3	Not used in this example
8	Operation:	Text	Operation:		
9	GemTilMasterPlan_Meddel	Transaction Name	(\S+)	$4	Transaction Name – What did the user ask for
10	Time:	Text	Time:		
11	2395	Response time	(\d+)	$5	Response Time – How long was the response time – this time in milliseconds
12	Size: -1	Text	.*		

$1 - Timestamp string - 2016-04-08 06:57:41,077
$4 – Transaction string - GemTilMasterPlan_Meddel
$5 – Response time string – 2395

In the OneView LogReader the regular expression will look like:
(\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2},\d{3}) \S+ \[\S+ \S+\] KlientPerformanceLogHandler \S+ KlientTime: (\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2},\d{3}) User: (\S+) Operation: (\S+) Time: (\d+) .*