



Documentation

IBM Workload Scheduler integration with Splunk



Written by :	Date :
Miguel Sanders	August 18 2017
Uniforce	





Table of Contents

1. INTRODUCTION	4
2. INSTALLING AND CONFIGURING THE PLUG-IN FOR SPLUNK	. 5
3. DEFINING A SPLUNK JOB	6
4. MONITORING A SPLUNK JOB	9







CHANGE HISTORY

Version	Date of change	Change detail
1.0	August 18 2017	Initial version by M. Sanders







1. INTRODUCTION

Splunk Enterprise and Splunk Cloud monitor and analyze machine data from any source to deliver Operational Intelligence to optimize your IT, security and business performance. With intuitive analysis features, machine learning, packaged applications and open APIs, Splunk Enterprise and Splunk Cloud are flexible platforms that scale from focused use cases to an enterprise-wide analytics backbone. Features include the following:

- Collects and indexes log and machine data from any source
- Powerful search, analysis and visualization capabilities empower users of all types
- Apps provide solutions for security, IT ops, business analysis and more
- Enables visibility across on premise, cloud and hybrid environments
- Delivers the scale, security and availability to suit any organization
- Available as software or as a cloud service

Using the IBM Workload Scheduler plug-in for Splunk, you will be able to schedule reports in Splunk Enterprise and Splunk Cloud.

splunk> Ave.1	learch & Reporting	NC.				Administrator ~ N	lessages - Detlings - Activity - H
Beach First		rts Deshboards					Search & Repor
Q New Sea	rch						Save As v O
Index-oldeno							Last 24 hours ~
- 622,634 events (4/3	/14 1:00:00.000 #	M to 4/4/14 1:45:55.000 PM				v dat.	I I A L & Webow Mod
Events (522,634)	Statistics	Veuelization					
Formal Timeline -	- Joom Out	+ Zoore to Selection + Deusland					1 hour per s
45,000							
36,000						Concession of the local distance of the loca	
15,000							
		5.00	10 PM	12:00 AM	6.00 AM		12:01 PM
		2014	14	Trides.			
		Raw v Formativ 50	50 Per Page ~			Our 1 1	3 4 5 5 7 8 9 - 5
A DECEMBER OF	a in the second	1 Event					
	12 Ho 1 House	> 10.2.1.33 27.102.0.0	0 (06/0pr/2016 13:45:56:332819) 1	1681 /category.screen?category_cd=01SPLKrPR01001	AUSESSIONID-SEDSLBFFAADFF7 HETP 1.1" 200 929 "	http://shop.splunktel.com/cat	egory.screen?category_id=0CSPLAMPR
Salected Fields		T* "Wozilla/5.0 (1PM	Phone: U: CPU sPhone 05 4_2_10 like M	lac 05 X; en-us) ApplewebKit/533.17.9 (HOTML, 11)	w Secko) Version/5.0.2 Mobile/WE600 Safari/653	03.18.5* 2169	
# Dyles 100-		3 10.2.1.35 12.130.60. T. Manufact Links.	0.5 (04/Apr/2014 13:45:54:301728)	*GET /product.screenTproduct_id=NC-SANDESK-NEO	ROSD64GB8_HEESSOCHID+SOTSLEFF3ADFF7 HTTP 1.1" 20	00 362 "http://shop.splunktel.	com/cart.do?action+addtocart&item3
a clentip 1004		11 Staproduct_20*8C-S	South St	St. 1995 core debetion-to corrigoritio/tioch	1.1 WENDERLEY 2021	CONTRACTOR OF A 1	a had and there i takes and stated a
e data,hour 34		art.dolaction+change	gequantity&itemId=EST-19&product_id=B#	#-MOPHIE-JUDGEPACKPLUS" "Mozilla/5.0 (Linum; U;	Android 3.1; de-de; GT-P7510 Bulld/VBJ37) Appl	Leweb411/534.13 (GHTML, like 6	iecko) Version/4.0 Safari/S34.13" 3
# date,minute 10		> 10.2.1.34 131.138.23 RA-H01SP0165* "Wast1	233.243 [04/Apv/2014 13:45:54:3304 111a/5.0 (Linux; U; Android 2.2; en-ur	614) "GET /product.screen/product_id=AC-SIERAR- s; Comet Build/FRF91) AppleMetMit/533.1 (HOTML,	<pre>ctSPONGAUSESSIONID-SD75LSFF3ADFF3 HTTP 1.1* 5 Like Gecko) Version/4.0 Wobile Safari/533.1* 1</pre>	503 967 "Witp://shop.splumktel 1961	.com/product.screen?product_id+AC+
# data_second 10 # data_wday 2 # data_year 1 # data_pear 1		3 214-84-84 31.04.16.6.0004 [heter-special]]upper-dates. Interestant;1377782, appression Ediformationables, 2008aug 2018 49, 30200877750 (10172), arthorizontal and anti-special anti- -special anti-special anti-					
a eventype 1		> 104/Apr/2014 13:45-5	St Widdill prosecul-1 solutional con	transaction speed-the countiledd men utiledd a	serve-bild() + ROM sessions WHRM session ide	*7135679153**	
a host A		> 104/Aur/2014 13:45:1	SENTMALL arc-musal-1 salumetel.com	transaction speed-103 cou stil-55 mes stil-43 :	were "MLECT * FROM customers while customer i	Ld-1945541*	
a ident 1		> IDE/Anr/2016 VB/45-1	(5) (\$73181) provided of solutions con	transaction speed-162 ma stilled and stilled	server'SLICT product id, sky, price. 1800 and	storts wells product (dettage	
a brecourt 1		> 104/04/14 13:45:55:5	507) 500000be Query E ros like	e ice de porteble query Query ppenQueryCorsurit	Paras Warker 1: Type = Long	and a set of the state of the	
a method 2		> 104/Apr/2014 13:45:5	-52-974034) arcement-1 soluristel.com	transaction speed=192 cpu util=16 mem util=76	serve SLICT price FROM products WHERE product	14+1882*	
a punct 100+		> 104/Apr/2014 13:45:1	S2:8737851 arc+mysol-1.solumits1.com	transaction speed+178 cou stil-44 men stil+53 s	surversities + FROM customers while customer 1	Ld+1934091*	
a registre 100+		> 104/04/14 13:45:52:4	B631 00000001 Serviethrappe : SRVE	02421: IPA web5canner1 [/wps/PA Meb5canner1 1/10	a/html/WanapelearchCollections.isph: faitializ	nation successful.	
a sourcetupe 7		> 10.2.1.35 131.138.23	233.243 [04/Apr/2014 13:45:52:329	969) "GET /category.screen?category_cavelabilitia	LISESSIONID-SOTSLAFFEADEFS HTTP 1.1" 200 806 "W	vite://shop.spluristel.com/cart	-doTection-additionart&itest#+EST-13
a splate server 1		duct_L0-0P-H1C0R0100	DINC" "Woollin'S.D (1Pad; U; CPU 05 3)	2 11ke Wac OS X; er-us) ApplemetAlt/531.21.10 (XHTML, like Gecks) Werslon/4.0.4 Bobile/78067	Safar1/531.21.10* 3500	
# status 40		3 (04/Apr/2014 13:45:15	(\$1:974283) src-mysel-1.splumktel.com	transaction_speed+120 cpu_util+60 mem_util+67 (pery+"SELECT * FROM sessions WHERE session_Ld+	*8441997043**	
at the same dama and the		> (04/Apr/2014 13:45:5	S1:972850] src=mysql-3.splumktel.com	transaction_speed=109 cpu_util=23 meh_util=55 (pery="SELECT * FROM sessions WHERE session_id=	1947519867111	
a beneficiation 11		> 10.2.1.33 89.167.143	43.32 (54/Apr/2014 13:45:51:33226) ABBA-FREEMAN* "Mec111a/5.0 (Linux: V.	7] "GET /cart.doTuction=remove&itemId=EST-13&pro t Android 2.3.4; en-us: DR0ID #D0WDC Build/5.5.1	duct_id=BT-CK-JABRA-TREEwKY%JSESSIONID=SD95L4F L_84_DBM+62_WR-11) AppleWebKit/533.1 (WHTML, 11	FF3ADFF7 HTTP 1.1" 200 358 "ht lke Gecks) Version/4.0 Mobile	tp://shop.splunktel.com/product.sc Sefer1/533.1" 2111
a timestargos 11 a unie 1		rproduct_speak -ck-sk					
al timestartpos 11 a unit 1 Interesting Fields		> Apr 64 10:45:51:0790	9917 aas1 radiund(2363):(30 959576 Los	call.info) DNPD RADOP(13) acct stop for 97783158	198splunktel.com 10.149.191.81 from 64.66.0.20	0 recorded 0K.	







2. INSTALLING AND CONFIGURING THE PLUG-IN FOR SPLUNK

The following prerequisites must be met in order to use the IBM Workload Scheduler plug-in for Splunk.

- IBM Workload Scheduler 9.1 or later
- IBM Dynamic Workload Console 9.1 or later
- Splunk 6.6 or later

To install and configure the IBM Workload Scheduler plug-in for Splunk, perform the following steps:

- Copy *com.ibm.scheduling.agent.splunk_<version>.jar* to the *<TWA_HOME>/TWS/applicationJobPlugIn* folder on either the Master Domain Manager or a Dynamic Domain Manager
- Copy *com.ibm.scheduling.agent.splunk* _<*version>.jar* to the <*TWA_HOME>/TWS/JavaExt/eclipse/plugins* folder on the Dynamic Agent that will run the Splunk jobs
- Modify *config.ini* located in *<TWA_HOME>/TWS/JavaExt/eclipse/configuration* on the Dynamic Agent that will run the Splunk jobs. At the end of the line that starts with "osgi.bundles=", add the following: *",com.ibm.scheduling.agent.splunk@4:start"*
- Restart the WebSphere Application Server of either the Master Domain Manager or the Dynamic Domain Manager.
- Restart the Dynamic Agent
- Restart the Dynamic Workload Console







3. DEFINING A SPLUNK JOB

From the Dynamic Workload Console, you can define a Splunk job as follows:

- In the Dynamic Workload Console navigation tree, expand Administration and select Manage Workload Definitions.
- Specify the name of the engine. Subsequently, the Workload Designer is displayed.
- In the Working List panel, select New -> Job Definition -> Business Analytics -> Splunk.
- On the Splunk panel, fill in the job details
 - **Hostname** : Hostname of the Splunk Enterprise Server or Splunk Cloud. For Self-service Splunk Cloud deployments, use the following URL

input-<deployment-name>.cloud.splunk.com

- **Username** : The username to log on to Splunk Enterprise or Splunk Cloud. For Splunk Cloud, submit a support case with Splunk to get non-SAML user credentials.
- **Password** : The password of the user that will log on to Splunk Enterprise or Splunk Cloud.
- **Use SSL** : Select whether SSL/TLS is used for the connection to Splunk Enterprise or Splunk Cloud. For Splunk Cloud, this is mandatory.

To validate the connection, click Test Connection.

- **Report name** : The name of the report that you want to schedule. Use the "Select..." button to get a picklist which shows all defined reports.
- **Polling interval** : The monitoring frequency determines how often the job is monitored. The default value is 10 seconds..
- **Maximum count** : Limit the maximum number of results before finalizing the search.
- **Maximum time** : Limit the maximum amount of time before finalizing the search.
- Buckets : Sets the maximum number of timeline buckets.
- **Output mode** : Select the output mode for the search result (XML, JSON or CSV).
- **Force dispatch** : Indicates whether to start a new search, even if another instance of this search is already running.
- **Spawn process** : Indicates whether the search should run in a separate spawned process. Searches against indexes must run in a separate process.
- Enable lookups : Indicates whether to enable lookups for this search.
- **Trigger actions** : Indicates whether to trigger the alert actions that are associated with the report.







SPLUNK (9.4.0.01) - DELTA#P_SPLUNK_DEMO						
Select an Action 🔻		ē 🧷	Θ	C 🖣	SAP	
General	Affinity	Recovery	Options	Splun	ik	Versions
* Hostname	indigo.uniforce.be					
* Port	8089					
* Username	admin					
* Password	•••••	•••••				
	⊠Use SSL					
	Test Connection					

Report Details

* Report name	IWS	Select
* Polling interval	10	
Maximum count		
Maximum time		
Buckets		
Output mode	XML -	
Force dispatch		
Spawn process		
🔲 Enable lookups		
✓Trigger actions		





Alternatively, the *composer* command line can be used to define the job. Example:

DELTA#P_SPLUNK_DEMO

TASK

<?xml version="1.0" encoding="UTF-8"?>

<jsdl:jobDefinition xmlns:jsdl="http://www.ibm.com/xmlns/prod/scheduling/1.0/jsdl" xmlns:jsdlsplunk="http://www.ibm.com/xmlns/prod/scheduling/1.0/jsdlsplunk" name="SPLUNK">

<jsdl:application name="splunk">

<jsdlsplunk:splunk>

<jsdlsplunk:SplunkParameters>

<jsdlsplunk:SplunkParms>

<jsdlsplunk:serverInformation>

<jsdlsplunk:hostname>indigo.uniforce.be</jsdlsplunk:hostname>

<jsdlsplunk:port>8089</jsdlsplunk:port>

<jsdlsplunk:username>admin</jsdlsplunk:username>

<jsdlsplunk:password>{aes}UG/QqqXCFjk=</jsdlsplunk:password>

<jsdlsplunk:ssl/>

</jsdlsplunk:serverInformation>

<jsdlsplunk:reportDetails>

<jsdlsplunk:reportName>IWS</jsdlsplunk:reportName>

<jsdlsplunk:pollingInterval>10</jsdlsplunk:pollingInterval>

<jsdlsplunk:maximumCount/>

<jsdlsplunk:maximumTime/>

<jsdlsplunk:buckets/>

<jsdlsplunk:outputMode>outputModeXml</jsdlsplunk:outputMode>

<jsdlsplunk:triggerActions/>

</jsdlsplunk:reportDetails>

</jsdlsplunk:SplunkParms>

</jsdlsplunk:SplunkParameters>

</jsdlsplunk:splunk>

</jsdl:application>

</jsdl:jobDefinition>

RECOVERY STOP





4. MONITORING A SPLUNK JOB

Like regular jobs, you can monitor Splunk jobs by using either the Dynamic Workload Console or the *conman* command line.

Plan Name: Current Plan

@#JOBS.@						
Job Log De	pendencies Rela	ease Dependencies	Rerun What-If Job Stream View More Actions ~	Ø•~		
Status	^ Internal Status 4	^ Job	^ Job Type	^ Workstation (Job)	^ Job Stream	^ Workstation (Job Stream)
🔲 🔽 Success	ful SUCC	P_SPLUNK_DEMO	Splunk	DELTA	JOBS	DELTA

Extended job properties can be displayed using either the Dynamic Workload Console or the conman command line using the *«;props»* option

'P_SPLUNK_DEMO' Properties

Acuon	
 Deadline 	
Length of Time	
Action	
Repeat Range	
 Extra Information 	
Disk Usage	1675264
Dispatch State	DONE
Done Progress	1.0
Drop Count	0
Event Available Count	33075
Event Count	33075
Event Field Count	6
Label	IWS
Priority	5
Result Count	33075
Run Duration	1.003
Scan Count	33075
Search Identifier	admin_admin_search_IWS_at_1503052151_910
Time to live	86400
 Splunk 	
buckets	
forceDispatch	false
hostname	indigo.uniforce.be
lookups	false
maximumCount	
maximumTime	
outputMode	outputModeXmI
password	{aes}UG/QqqXCFjmnmhthzZfXv33vAv3vXcfY9PubhegSxZk=
pollingInterval	10
port	8089
reportName	IWS
spawnProcess	false
ssl	true
triggerActions	true
username	admin

