

Loggly Plugin

We will set up the example application, using Fluentd with Loggly, for handling logs.

WARNING You will need an account at Loggly to continue.

Setting up Loggly

For testing this tutorial, if you do not already have an account, you may create a free trial at Loggly.

Once you have created your account, you must get an API token to set in the environment variable: LOGGLY_TOKEN

Go to the Loggly token endpoint for your organization:

https://{your-organization}.loggly.com/account/users/api/tokens

solarwinds 🗲 🔍 🖃 👂 🊅 📣 >_ 🦘	Subscribe Now III 上 🤉				
Overview Users API Tokens Archiving CloudTrail Subscription User Settings					
Please note: This API token is used to retrieve your logs from Loggly. The Customer Token required to send your logs to Loggly is available here.	The API token is used to				
API Tokens Add New Active (1)	retrieve your logs from Loggly programmatically. It is separate from your Source Setup Customer Tokens, which are used for sending data to Loggly.				
API Token A	Additional tokens are				
12345678-abcd-1234-efgh-098765432100	often useful to segment client authorization or to replace existing tokens in the event a token is compromised.				

Figure 1.1 - API Tokens List at Loggly.

To create a token, click the Add New button (see Figure 1.1). Once created, the token will appear in the active tokens list, such as the example above. That value will need to be set, in the next step, in a Postman environment variable: {{logglyToken}}

Install the example application and configure Fluentd"

Oak Platform (API): Install

```
{
    services": [{
    "image": "index.docker.io/oaklabs/app-example:release-1.0.1",
    "environment": {
    "TZ": "America/Phoenix"
    }
    ,
    {
         image": "index.docker.io/oaklabs/component-fluentd:loggly",
         "environment": {
            "LOGGLY_TAG": "{{logglyTag}}",
            "LOGGLY_TOKEN": "{{logglyToken}}"
```



|--|

Viewing the logs

*Default × I + New All Sources REMOTE_URL × I -1h now Image: Search * Image: Arrow and the search	🔍 🔍 🔍 🚺 Le	oggly Search	:	× +										
Doda * O ther * EMOTE_URL * O ther * Sourch * * * * Applied Filters: ag: my/loggly-tag × Cother Table Table Cother Table Table Cother Table	← → C ⓒ https://{your-organization}.loggly.com/search#terms=REMOTE_URL&from=2019-08-08T23:00:45.345Z&until=2019-08-09T00:00:45.345Z&source_group=&filter=tag;my-logg													
All Sources REMOTE URL X 0 -1h now Reach X • Applied Filters: Degree/seg X Image: regree/seg X Image: regree/seg X Image: regree/seg X Image: regree/seg X Image: regree/seg X Image: regree/seg X Image: regree/seg X Image: regree/seg X Image: regree/seg X Image: regree/seg X Image: regree/seg X Image: regree/seg X Image: regree/seg X Image: regree/seg X Image: regree/seg X Image: regree/seg X Image: reg X Image: regree/seg X Im		Q Search	🗠 Charts	Dashboard	Alerts	Derived Fields	s 🚯 Source Setup	>_ Live Tail	₩ Metrics/APM					? Help
<pre> • Applied Filters: bg:my-loggy-tag # • Applied Filters: bg:my-loggy-tag # • Field Explorer • Gother • tag • Field Actions • Field Act</pre>	*Default ×	+ New												
C Field Explorer I values 1 values 2 events 2 events <	All Sources	-	REMOTE_UR	L				x 🛿 -1h		now	Ê	• Search	**	
Aug 8, 4 - 5 PM (1 hr) Q Q I values 2 events Ny-loggly-tag 2 I values 2 events My-loggly-tag 1 (http://static.oak.host/signage/index.html*, */tag: I values 2 events 2 events I values 2 events <td>Applied Filters</td> <td>tag : r</td> <td>ny-loggly-tag 🗙</td> <td></td>	Applied Filters	tag : r	ny-loggly-tag 🗙											
Other tag X Iogtype Field Actions - tag 1 values 2 events my-loggly-tag 2 Detrome 04:00 PM	Q Field Explore	r			X Event Tim	eline ビ Chart								•
tag 1 1 1 <	금 Other		tag	×		S					Aug 8, 4	1 - 5 PM (1 hr) Q	€ 2
tag 1 values 2 events my-loggly-tag 2 letto PM letto PM letto PM letto PM <tr< td=""><td>< logtype</td><td></td><td>Field Actions</td><td>-</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Ţ</td></tr<>	< logtype		Field Actions	-										Ţ
D4:00 PM D4:20 PM D4:20 PM D4:30 PM D4:40 PM D4:40 PM D4:40 PM D4:50 PM D5:00 Event View Image: Sort: Descending ~ Expand Events More Options ~ Image: Sort: Descending ~ Expand Events More Options ~ Image: Sort: Descending ~ Expand Events More Options ~ Image: Sort: Descending ~ Expand Events Image: Sort: Descending ~ Expand Event Image: Sort: Descending Events Image: Sort: Descending Even	tag	•		_	1									1
<pre>B 2019-08-08 16:10:09.879 { json: { hostname: "54abcd123efg", service: "app-example-0_1", pid: "3420", message: "REMOTE_URL http://static.oak.host/signage/index.html" }, http: { clientHost: "11.22.123.123", contentType: "application/json" } } D 2019-08-08 16:10:09.672 % Copy link * Expand Event & Create Derived Fields & View Surrounding Events tag: my-loggly-tag logtype: json http: clientHost: 11.22.123.123 contentType: application/json json: hostname: 54abcd123efg message: REMOTE_URL: 'http://static.oak.host/signage/index.html', pid: 3420 service: "app-example-0_1 Crow message {"hostname": "54b20313b6dc", "pid": "3420", "message": "REMOTE_URL: 'http://static.oak.host/signage/index.html',", "service": "app-example-0_1"}</pre>			my-loggly-tag	2 🐠	04:00 PM		04:10 PM	04:20 PM	04:30 PM	04:40 P	M 0	4:50 PM		05:00 PM
<pre>http://static.oak.host/signage/index.html" }, http: { clientHost: "11.22.123.123", contentType: "application/json" } } 2019-08-08 16:10:09.672 % Copy link * Expand Event & Create Derived Fields & View Surrounding Events tag: my-loggly-tag logtype: json http: clientHost: 11.22.123.123 contentType: application/json json: hostname: 54abcd123efg message: REMOTE_URL: 'http://static.oak.host/signage/index.html', pid: 3420 service: app-example-0_1 row message {"hostname": "54b2d313b6dc", "pid": "3420", "message": "REMOTE_URL: 'http://static.oak.host/signage/index.html',", "service": "app-example-0_1"}</pre>					Event View	Sort: Desce	nding - Expand Events	s More Options 🔻					Ċ	•
<pre>tag: my-loggly-tag logtype: json tag: my-loggly-tag logtype: json thtp: clientHost: 11.22.123.123 contentType: application/json json: hostname: 54abcd123efg message: REMOTE_URL: 'http://static.oak.host/signage/index.html', pid: 3420 service: app-example-0_1 row message { hostname': "54b20313b6dc", "pid": "3420", "message": "REMOTE_URL: 'http://static.oak.host/signage/index.html', ", "service": "app-example-0_1"}</pre>					⊞ 2019-08-08								/json"]	+ }
<pre>http: clientHost: 11.22.123.123 contentType: application/json json: hostname: 54abcd123efg message: REMOTE_URL: "http://static.oak.host/signage/index.html', pid: 3420 service: app-example-0_1 row message {"hostname":"54b20313b6dc","pid":"3420","message":"REMOTE_URL: 'http://static.oak.host/signage/index.html',","service":"app-example-0_1"}</pre>					□ 2019-08-08	16:10:09.672			% Copy link	🖌 Expand Event	Create Derived Fields	🅫 View Surrou	nding Eve	ents I
{"hostname":"54b20313b6dc","pid":"3420","message":"REMOTE_URL: 'http://static.oak.host/signage/index.html',","service":"app-example-0_1"}					<pre>bhtp: clientHost: 11.22.123.123 contentType: application/json json: hostname: 54abcd123efg message: REMOTE_URL: 'http://static.oak.host/signage/index.html', pid: 3420</pre>									
■ A notifications (0)							c","pid":"3420","me	ssage":" <mark>REMOTE_L</mark>	<pre>IRL: 'http://static</pre>	.oak.host/signage/inde	ex.html',","service	":"app-example	e-0_1"}	
					🗈 🛦 notific	cations (0)								

The logs being sent to Loggly are the same that were sent in the Logz.io Plugin tutorial.

Figure 1.2 - Expanded log entry for **REMOTE_URL** at Loggly. This screenshot shows an expanded example log message with the **REMOTE_URL** environment variable being logged in the example application.

The search results are filtering by the example tag that was set in {{logglyTag}}: my-loggly-tag