

## Runbook Transforming Squid Message

Date of publish: 2017-11-06



# Legal Notice

© Cloudera Inc. 2019. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 ("ASLv2"), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER'S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

# Contents

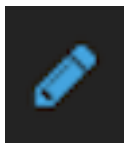
**Transform the Squid Message..... 4**

## Transform the Squid Message

You can customize your sensor data to provide more meaningful data. For example, you can choose to transform a url to provide the domain name of the outbound connection or the IP address. To do this, you need to add transformation information.

### Procedure

1.



In the Management module, click (edit button) for your sensor.

The Management module displays the schema panel.

**Squid** [Close]

NAME \*

Squid

No Matching Kafka Topic

PARSER TYPE \*

Grok

GROK STATEMENT

SCHEMA

TRANSFORMATIONS	0
ENRICHMENTS	0
THREAT INTEL	0

THREAT TRIAGE

RULES	0
-------	---

SAVE CANCEL Advanced

2.



In the Schema box, click (expand window button).

The Management module displays the Schema panel and populates it with message, field, and value information.


The Sample field, at the top of the panel, displays a parsed version of a sample message from the sensor. The Management module will test your transformations against this parsed message.

You can use the right and left arrow buttons in the Sample field to view the parsed version of each sample message available from the sensor.

You can apply transformations to an existing field or create a new field. Typically users choose to create and transform a new field, rather than transforming an existing field.

3.



To add a new transformation, either click the  next to a field or click the



(plus sign) at the bottom of the **Schema** panel.

The module displays a new dialog box for your transformations.

A dialog box titled "new" with a close button (X) in the top right corner. It contains several sections with input fields:

- INPUT FIELD**: A dark blue input field with a small up/down arrow on the right.
- NAME**: A dark blue input field containing the text "new".
- TRANSFORMATIONS**: A dark blue input field with a small up/down arrow on the right.
- ENRICHMENTS**: A dark blue input field with a small up/down arrow on the right.
- THREAT INTEL**: A dark blue input field with a small up/down arrow on the right.

At the bottom left is a button labeled "SAVE".

4. Choose the field you want to transform from the **INPUT FIELD** box, enter the name of the new field in the **NAME** field, and then choose a function with the appropriate parameters in the **TRANSFORMATIONS** box. You can apply more than transformation to the input field.

**ip\_dst\_addr\_copy**

**INPUT FIELD**

ip\_dst\_addr

**NAME**

ip\_dst\_addr\_copy

**TRANSFORMATIONS**

DOMAIN\_REMOVE\_SUBDOMAINS -

DOMAIN\_REMOVE\_TLD -

DOMAIN\_REMOVE\_TLD(DOMAIN\_REMOVE\_SUBDOMAINS(ip\_dst\_addr))

**ENRICHMENTS**

**THREAT INTEL**

**SAVE**

5. Click **SAVE** to save your additions.

The Management module populates the Transforms field with the number of transformations applied to the sensor.

If you change your mind and want to remove a transformation, click "-" next to the field.

6. Click **SAVE** in the parser panel to save the transformation information.