Cloudera Runtime 7.2.16

Securing Streams Messaging Manager

Date published: 2019-08-22
Date modified: 2023-01-11

https://docs.cloudera.com/

Legal Notice

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.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

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

Securing Streams Messaging Manager

As a cluster administrator, you can combine Kerberos authentication and Ranger authorization to secure the Streams Messaging Manager (SMM) web user interface (UI). After you secure the SMM web UI, the login page appears, which does not appear by default.

About this task

If you deploy SMM without security, the login page is not enabled on the SMM UI by default. When you enable Kerberos authentication, SMM uses SPNEGO to authenticate users and allows them to view or create topics within Kafka by administering Ranger Kafka Policies. For information on enabling browsers to use SPNEGO, see How to Configure Browsers for Kerberos Authentication.

After you secure SMM, anyone within the organization can login to SMM. However, if they do not have the correct policy configuration in Ranger, then they may not have the necessary privileges to perform their required tasks through SMM.

Before you begin

- Configure Kafka in Ranger

  For more information, see *Configure a resource-based service: Kafka*.
- Enable Kerberos authentication for Kafka

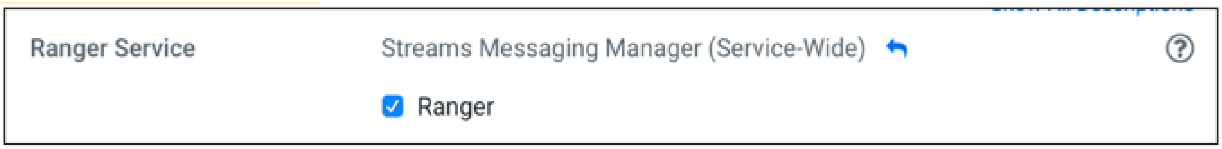
  For more information, see *Enable Kerberos authentication*.
- Add and configure SMM

  For more information, see *Creating your first Streams Messaging cluster*.

Note: For the Kafka Client security protocol, it is possible to use INFERRED, SASL_PLAINTEXT, and SASL_SSL for securing SMM. However, Cloudera recommends using SASL_SSL.

Procedure

1. Go to Cloudera Manager > SMM , and click Configuration.
2. Enable Ranger for SMM.



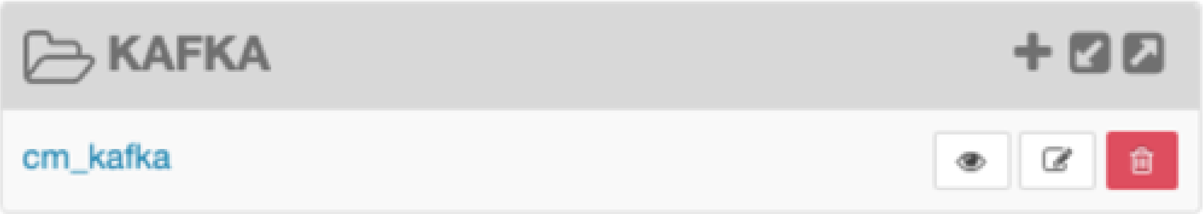
Ranger Service

Streams Messaging Manager (Service-Wide)

☑ Ranger

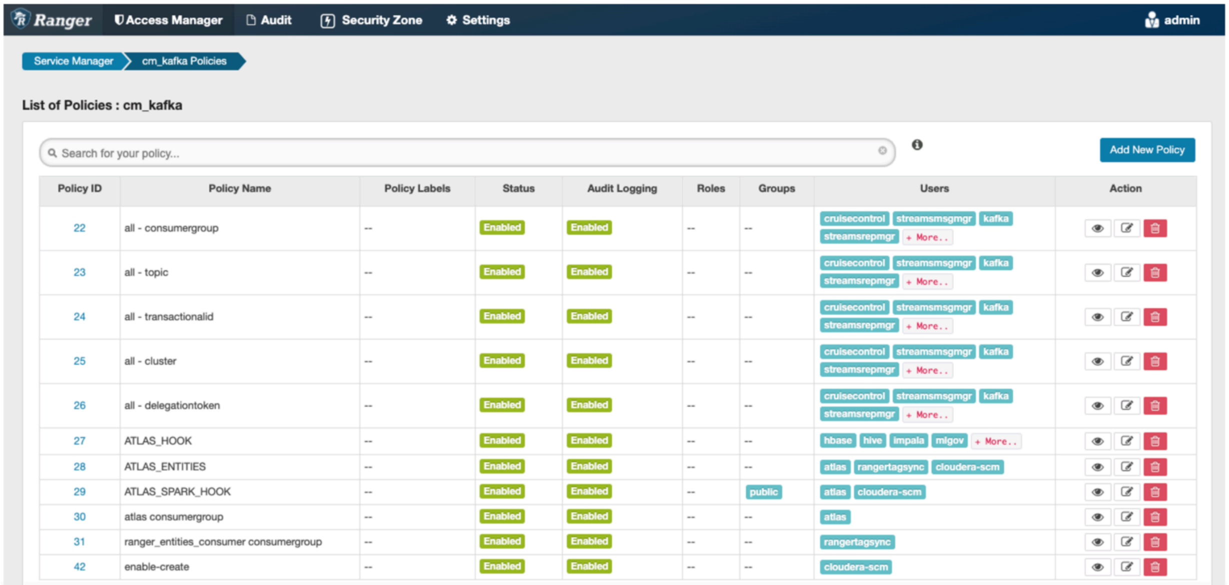
3. Go to the Ranger service UI and configure the Kafka policies.

   Note: Review your Ranger Kafka Policies. Remember to log in to Ranger with a user that has the Ranger Admin role.
4. Click cm_kafka in the Ranger service UI.



The List of Policies page appears.

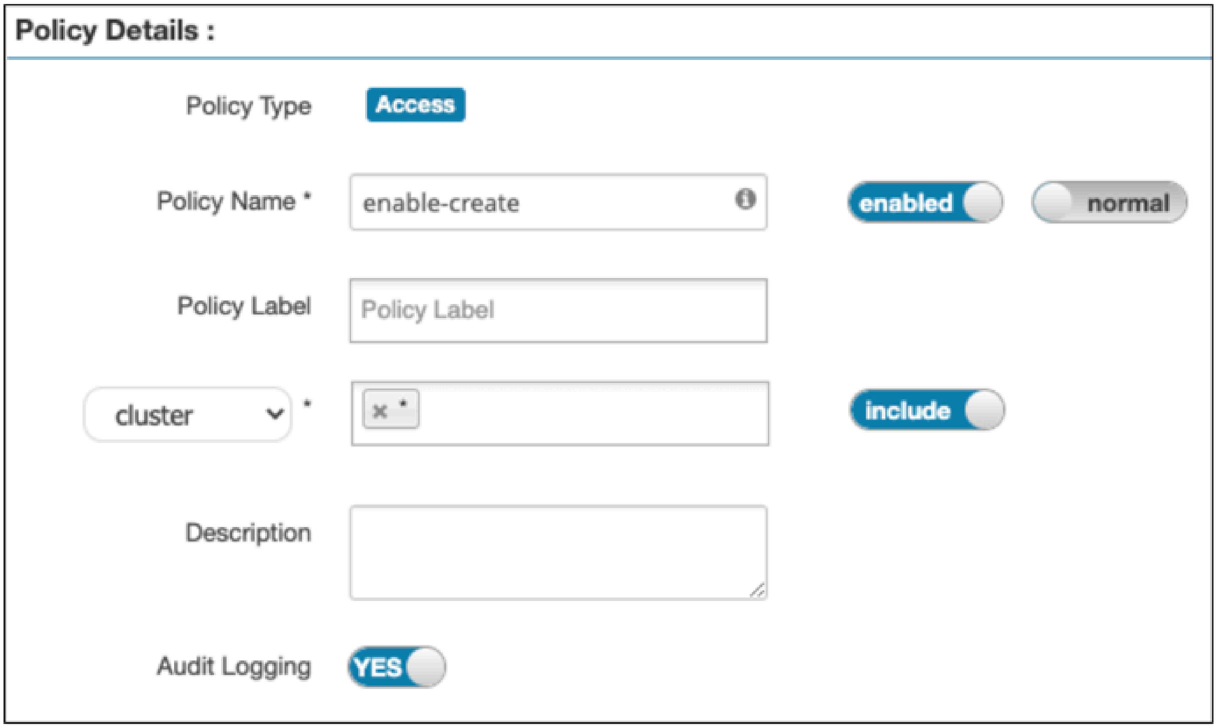
5. Click Add New Policy.



List of Policies : cm_kafka

Policy ID	Policy Name	Policy Labels	Status	Audit Logging	Roles	Groups	Users	Action
22	all - consumergroup	--	Enabled	Enabled	--	--	cruisecontrol streamsmsgmgr kafka streamsrepmgr + More..	👁 ✎ 🗑
23	all - topic	--	Enabled	Enabled	--	--	cruisecontrol streamsmsgmgr kafka streamsrepmgr + More..	👁 ✎ 🗑
24	all - transactionalid	--	Enabled	Enabled	--	--	cruisecontrol streamsmsgmgr kafka streamsrepmgr + More..	👁 ✎ 🗑
25	all - cluster	--	Enabled	Enabled	--	--	cruisecontrol streamsmsgmgr kafka streamsrepmgr + More..	👁 ✎ 🗑
26	all - delegationtoken	--	Enabled	Enabled	--	--	cruisecontrol streamsmsgmgr kafka streamsrepmgr + More..	👁 ✎ 🗑
27	ATLAS_HOOK	--	Enabled	Enabled	--	--	hbase hive impala mlgov + More..	👁 ✎ 🗑
28	ATLAS_ENTITIES	--	Enabled	Enabled	--	--	atlas rangertagsync cloudera-scm	👁 ✎ 🗑
29	ATLAS_SPARK_HOOK	--	Enabled	Enabled	--	public	atlas cloudera-scm	👁 ✎ 🗑
30	atlas consumergroup	--	Enabled	Enabled	--	--	atlas	👁 ✎ 🗑
31	ranger_entities_consumer consumergroup	--	Enabled	Enabled	--	--	rangertagsync	👁 ✎ 🗑
42	enable-create	--	Enabled	Enabled	--	--	cloudera-scm	👁 ✎ 🗑

The Policy Details page appears.



Policy Details :

Policy Type: Access

Policy Name *: enable-create

enabled normal

Policy Label: Policy Label

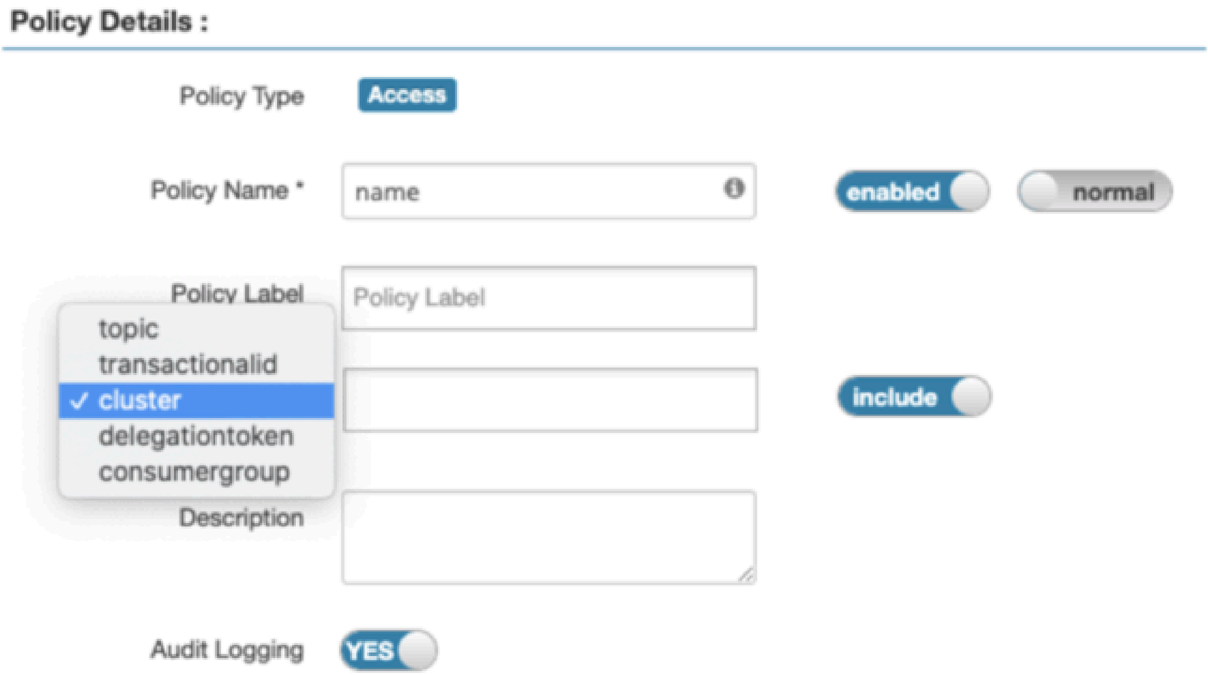
cluster *: × *

include

Description:

Audit Logging: YES

6. Add a policy name and select cluster from the dropdown.



Policy Details :

Policy Type: Access

Policy Name *: name — enabled — normal

Policy Label: Policy Label

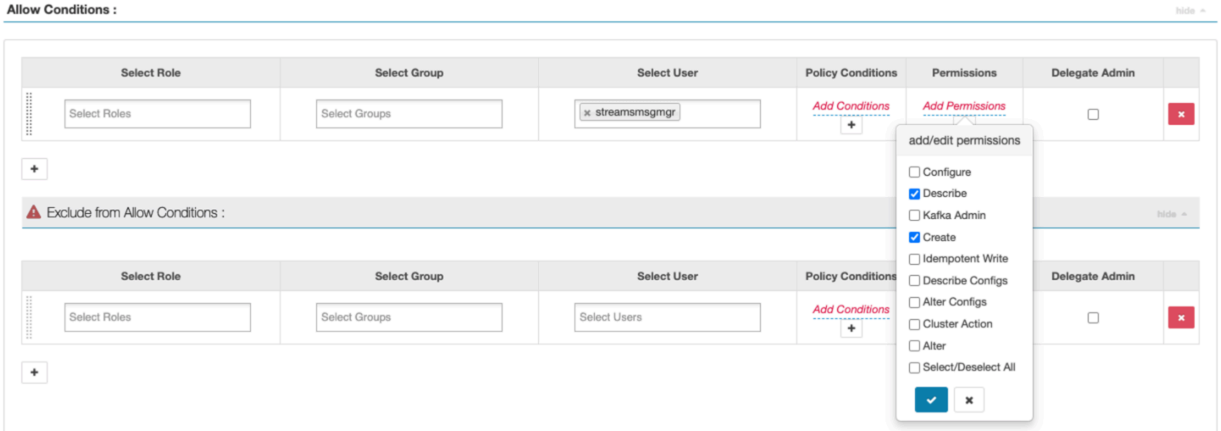
- topic
- transactionalid
- ✓ cluster
- delegationtoken
- consumergroup

include

Description

Audit Logging: YES

7. Type * in the field beside cluster, and select the * from the values that appear.
8. Go to the Allow Condition section and select the user.
9. Add permissions by clicking the + under Add Permissions.



Allow Conditions : hide

Select Role	Select Group	Select User	Policy Conditions	Permissions	Delegate Admin	
Select Roles	Select Groups	× streamsmsgmgr	Add Conditions +	Add Permissions	□	×

+

add/edit permissions

- □ Configure
- ☑ Describe
- □ Kafka Admin
- ☑ Create
- □ Idempotent Write
- □ Describe Configs
- □ Alter Configs
- □ Cluster Action
- □ Alter
- □ Select/Deselect All

✓ ×

Exclude from Allow Conditions : hide

Select Role	Select Group	Select User	Policy Conditions	Permissions	Delegate Admin	
Select Roles	Select Groups	Select Users	Add Conditions +		□	×

+

10. Select Create and Describe permissions.
11. Click Add.

Related Information

Configure a resource-based service: Kafka

Enable Kerberos Authentication

Setting up your Streams Messaging cluster

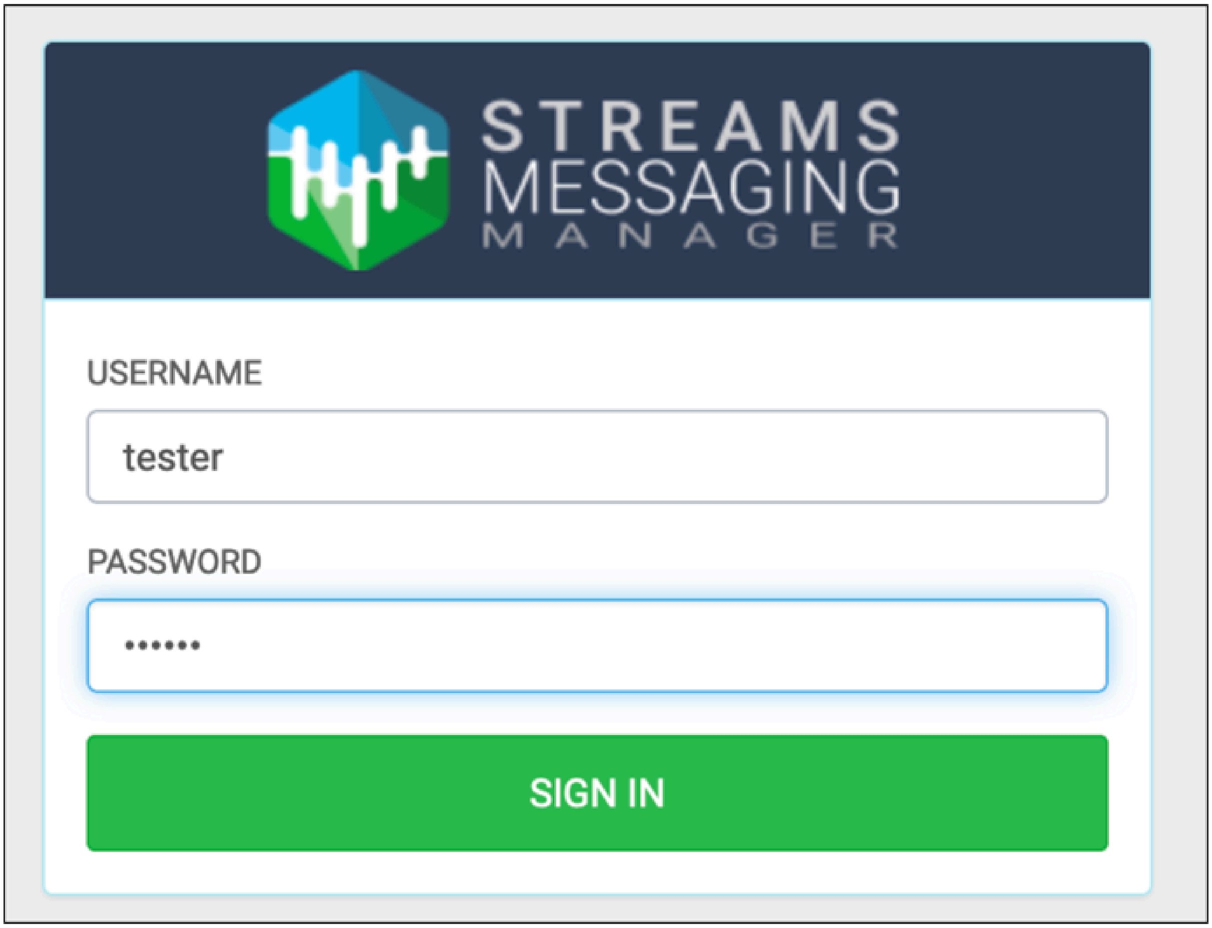
Verifying the setup

After you secure SMM, you can verify the security setup. You can login to the SMM web UI and create Kafka topics.

Procedure

1. Go to Cloudera Manager > SMM .

   The login page for SMM appears.



USERNAME

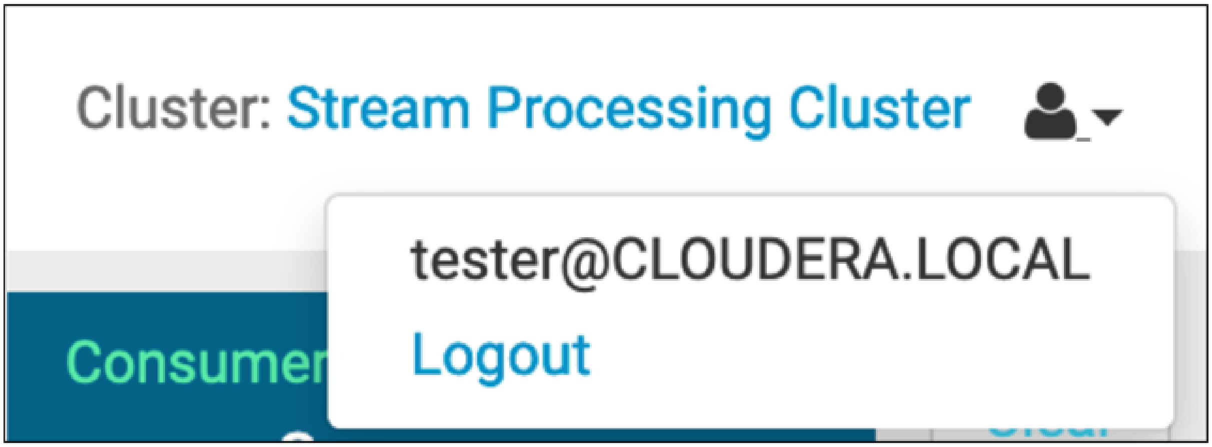
tester

PASSWORD

••••••

2. Login to the SMM UI using your regular credentials.

   After you log in, you see the user logout dropdown at the top right corner of your screen. It shows the domain associated with the user.

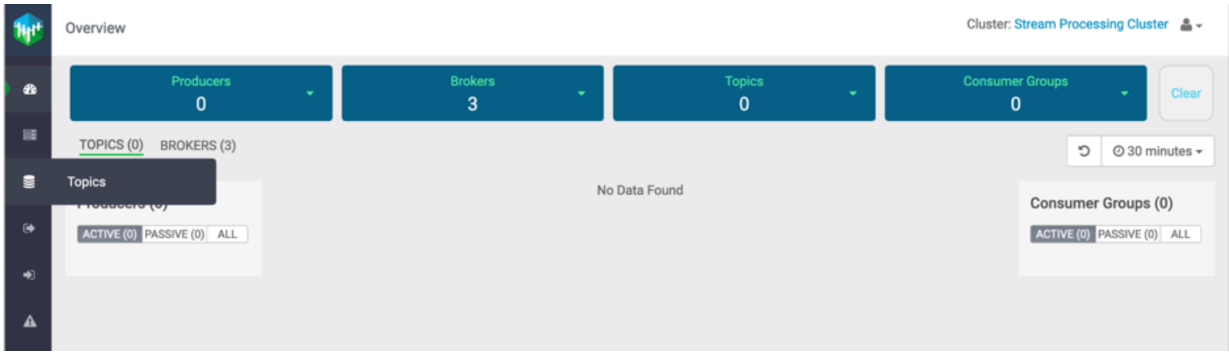


Cluster: Stream Processing Cluster

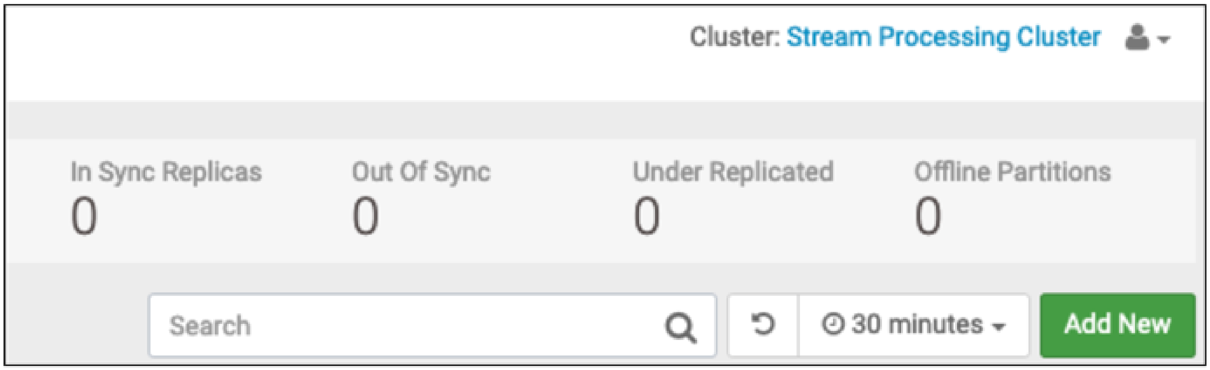
tester@CLOUDERA.LOCAL

3. Click Streams Messaging Manager Web UI.

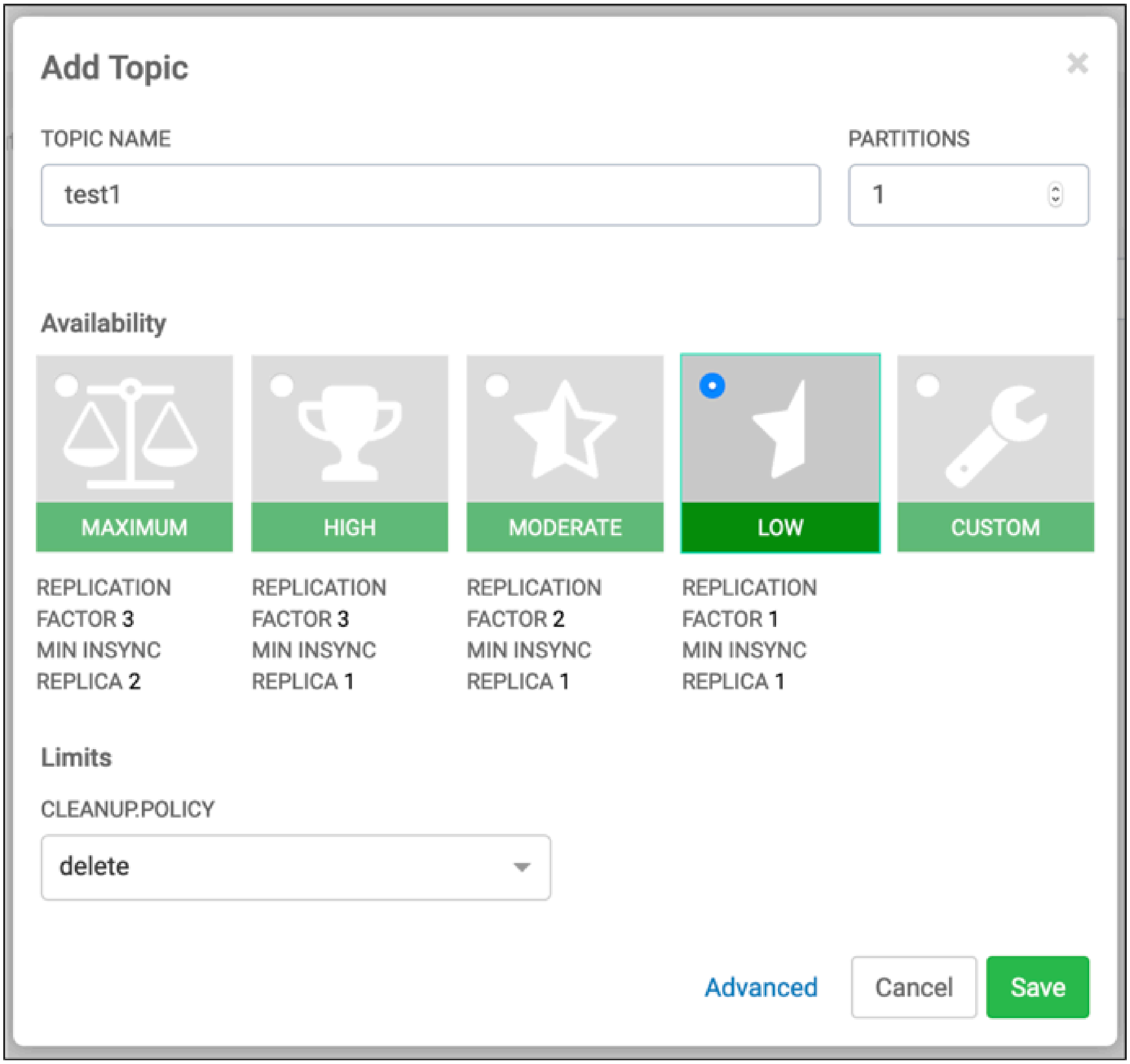
4. To add a topic, go to Topics.



5. Click Add New.



6. Add a topic name, select partitions, and cleanup policy.



Add Topic

TOPIC NAME: test1

PARTITIONS: 1

Availability

○ MAXIMUM — REPLICATION FACTOR 3 MIN INSYNC REPLICA 2

○ HIGH — REPLICATION FACTOR 3 MIN INSYNC REPLICA 1

○ MODERATE — REPLICATION FACTOR 2 MIN INSYNC REPLICA 1

● LOW — REPLICATION FACTOR 1 MIN INSYNC REPLICA 1

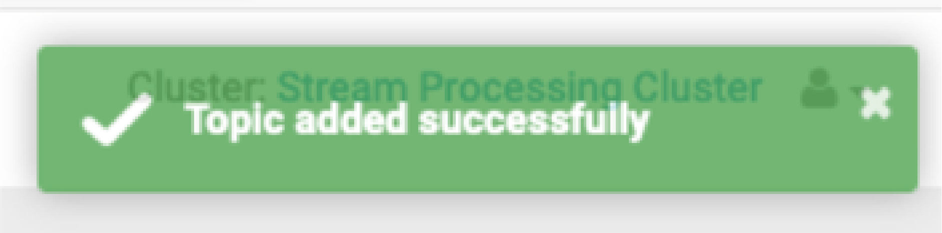
○ CUSTOM

Limits

CLEANUP.POLICY: delete

7. Click Save.

You see the following message in the top right corner of the webpage.



Cluster: Stream Processing Cluster

✓ Topic added successfully