Securing Streams Messaging Manager

Date published: 2020-05-22
Date modified: 2020-05-22

https://docs.cloudera.com/

Legal Notice

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).

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

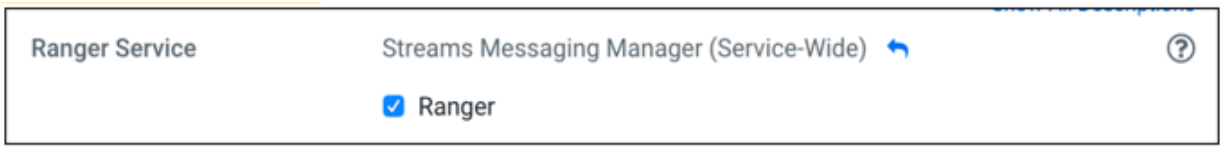
  For more information, see *Configure a resource-based service: Kafka*.
- Enable Kerberos authentication for Kafka

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

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.

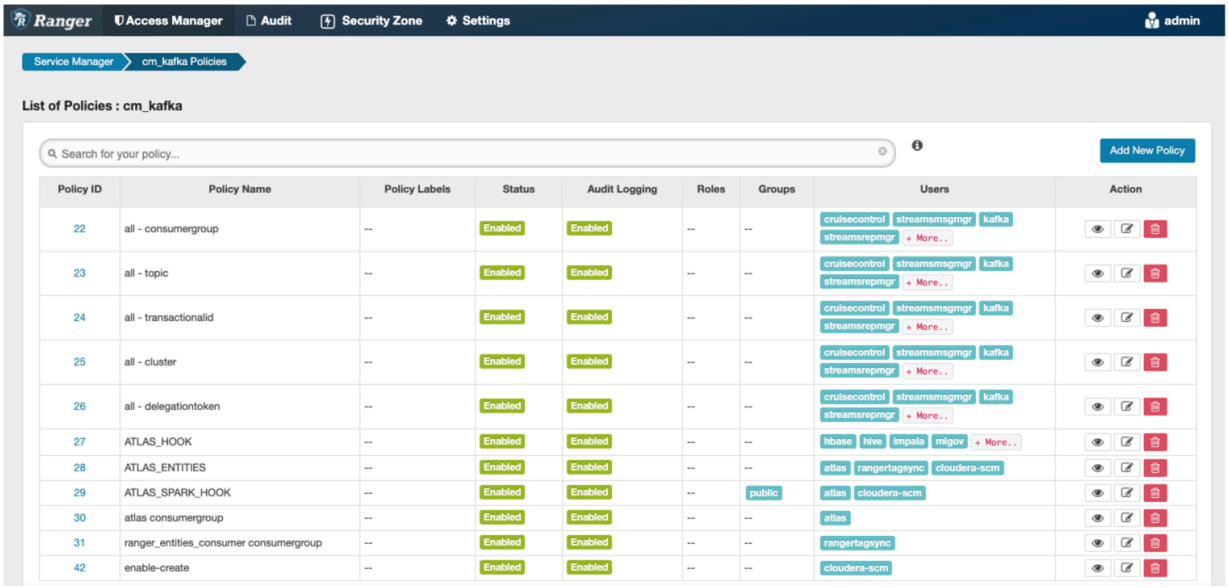


3. Go to the Ranger service UI and configure the Kafka policies.

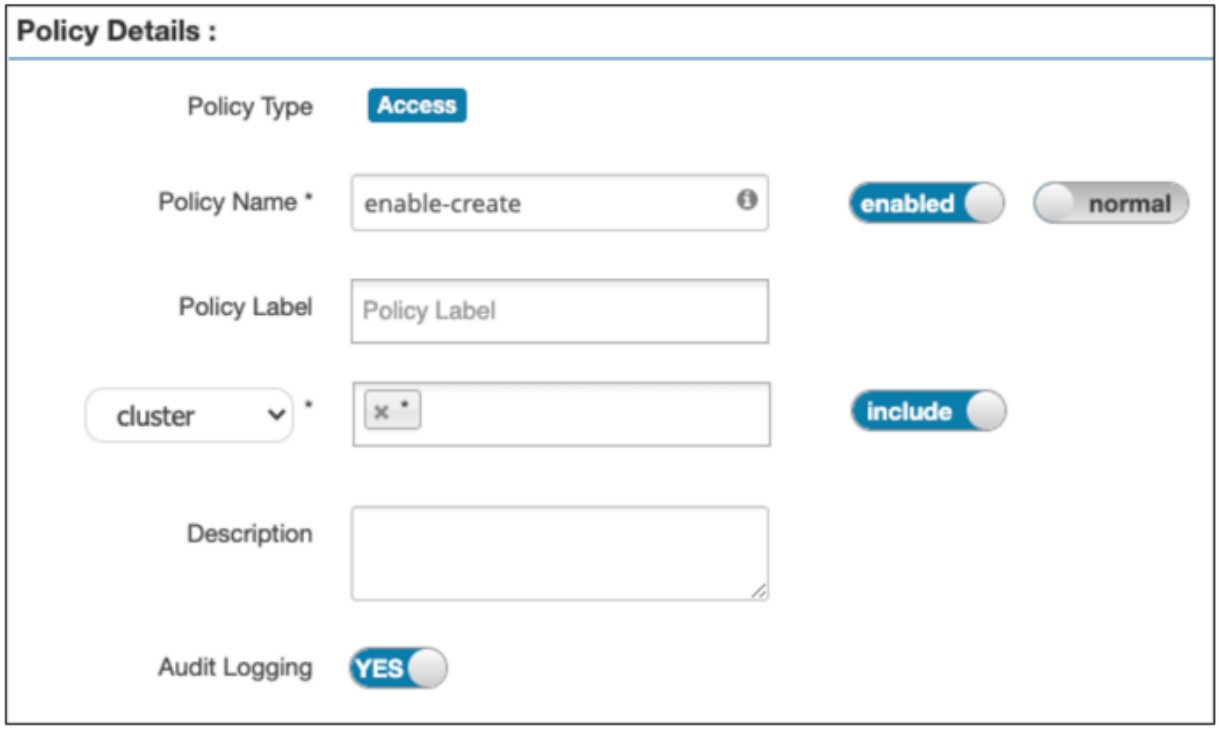
   Note: Review your Ranger Kafka Policies. Remember to log in to Ranger with a user that has the Ranger Admin role.
4. Click cm_kafka in the Ranger service UI.

   The List of Policies page appears.

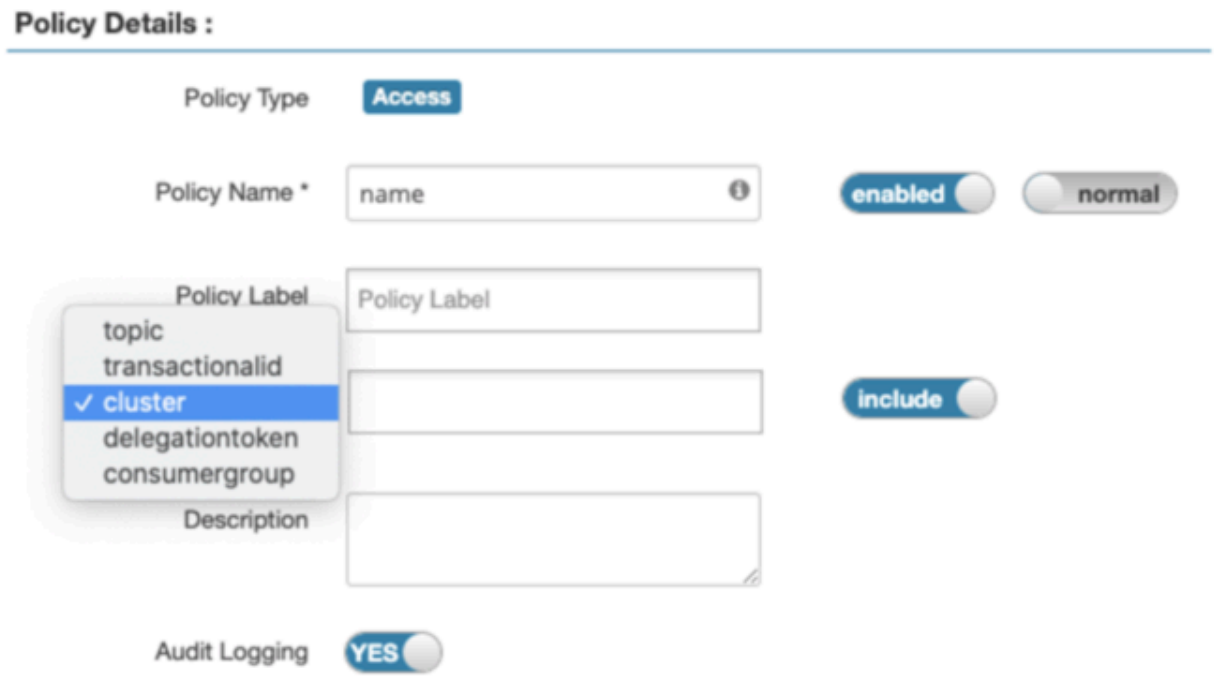
5. Click Add New Policy.



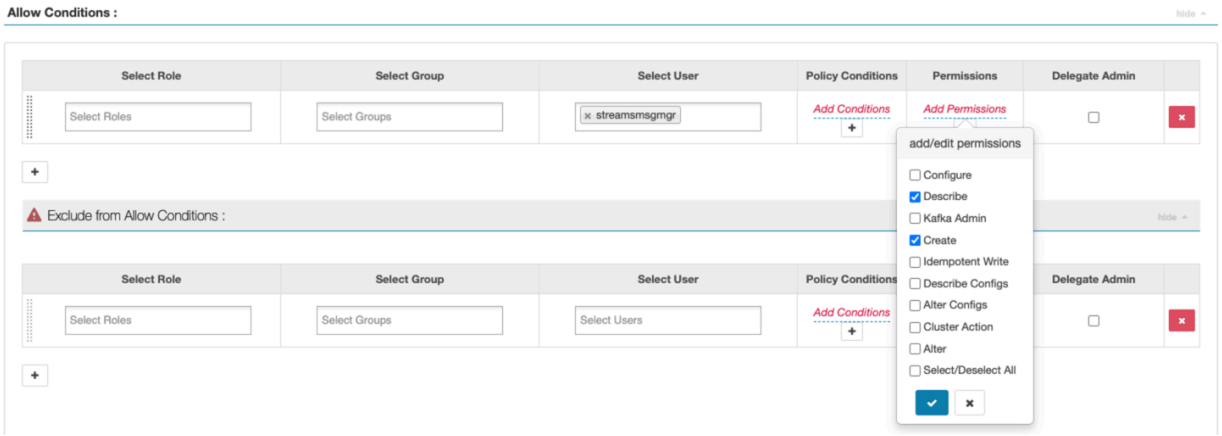
The Policy Details page appears.



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



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.



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

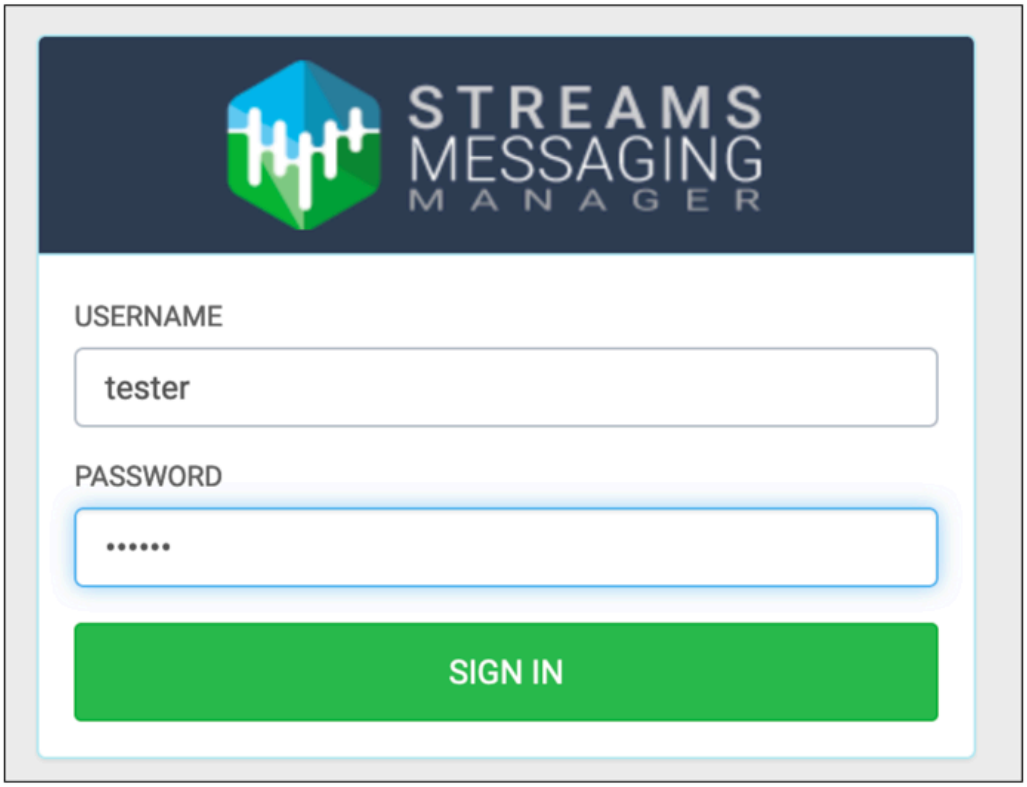
What to do next

Verifying the Setup

After you secure SMM, you can verify the security setup.

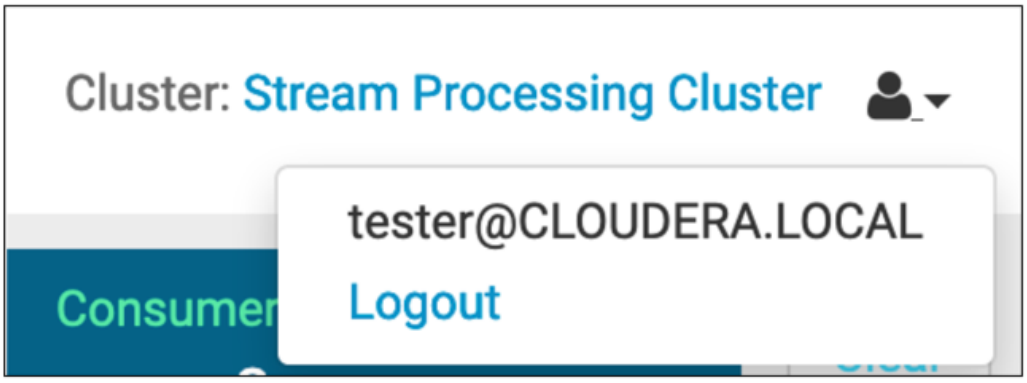
1. Go to Cloudera Manager > SMM .

   The login page for SMM appears.



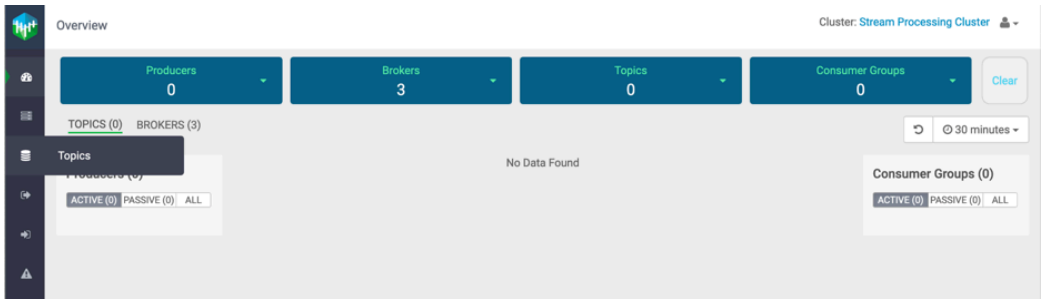
2. Login to the SMM UI using your regular credentials.

   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.

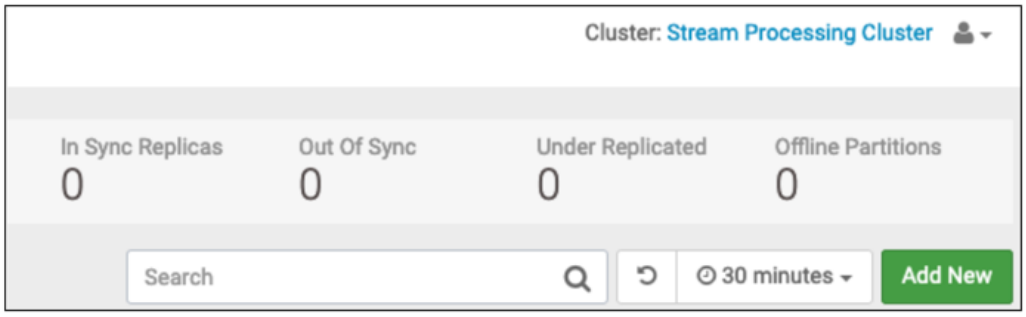


3. Click Streams Messaging Manager Web UI.

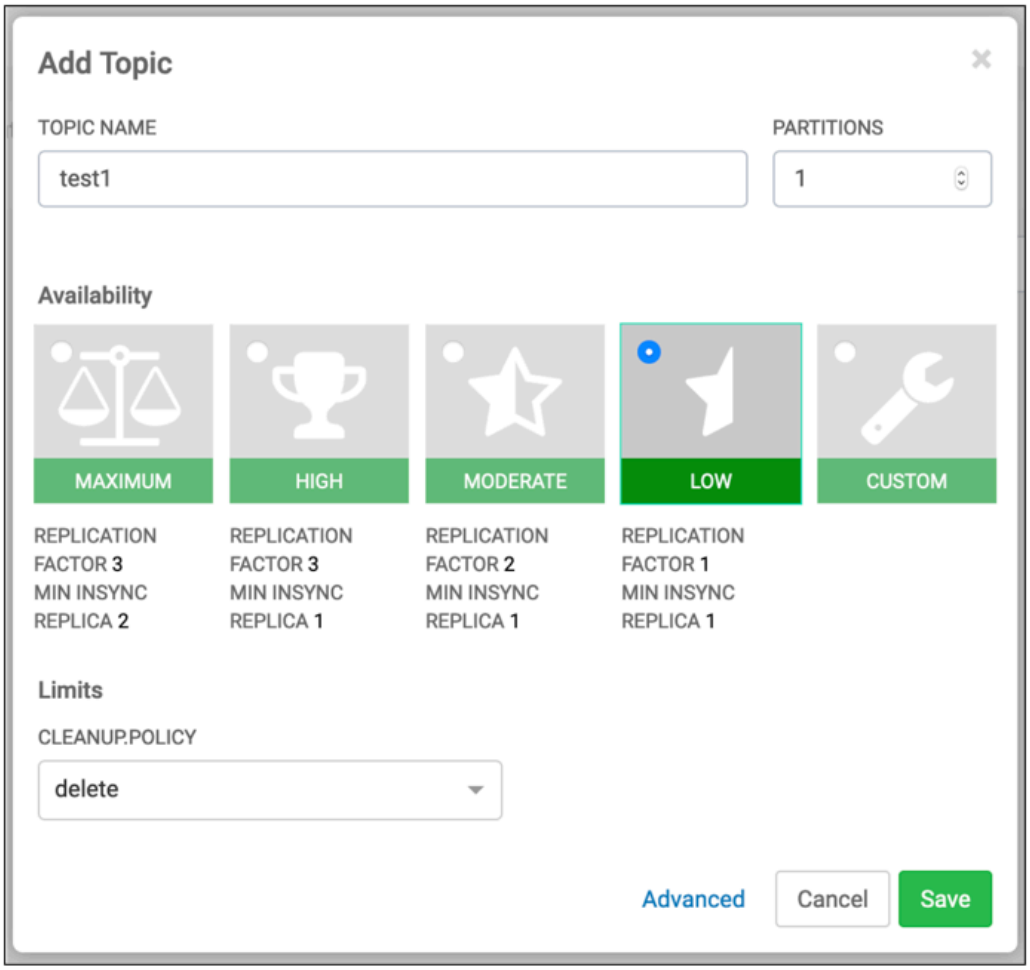
4. To add a topic, go to Topics.



5. Click Add New.

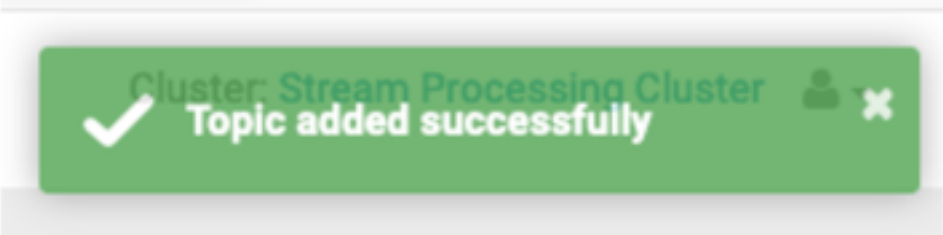


6. Add a topic name, select partitions, and cleanup policy.



7. Click Save.

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



Related Information

Configure a resource-based service: Kafka

Enable Kerberos Authentication