Securing Streams Messaging Manager

Date published: 2020-08-10
Date modified: 2021-03-19

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). 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

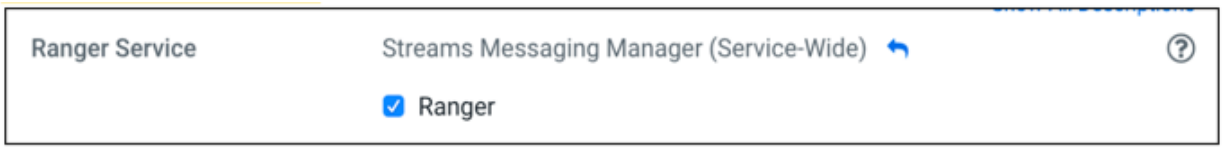
  For more information, see *Enable Kerberos authentication*.
- Add and configure SMM

  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.

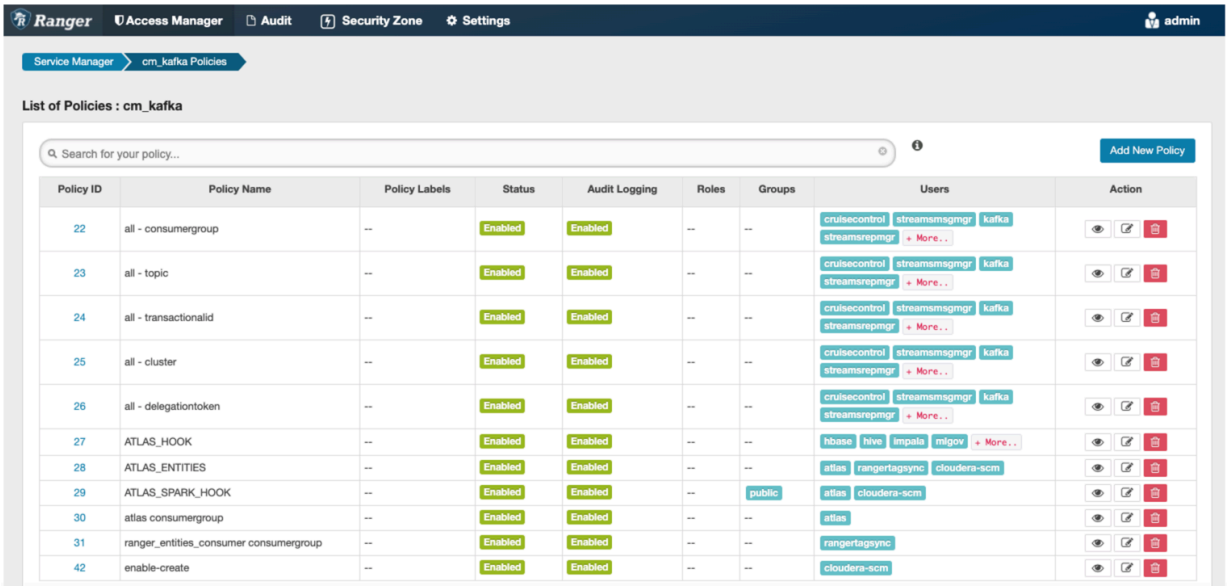


3. Go to the Ranger service UI and configure the Kafka policies.

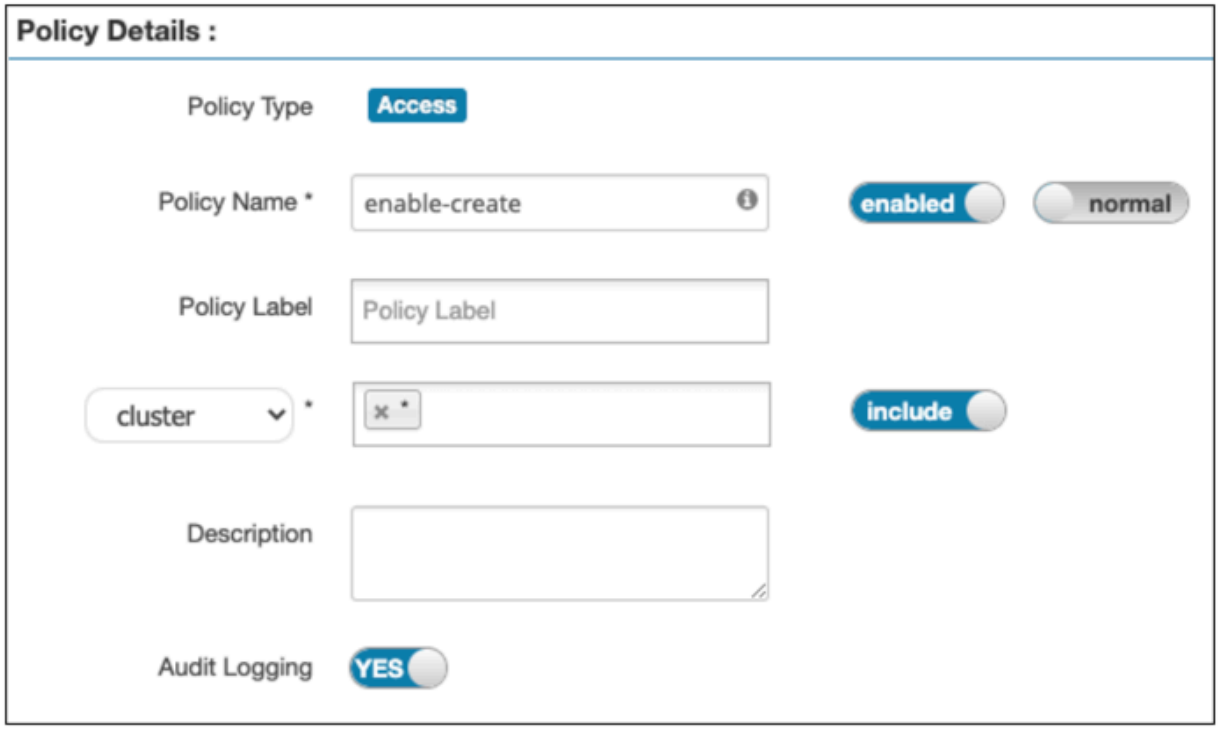
   Note: Review your Ranger Kafka Policies. Remember to log in to Ranger with a user that has the Ranger Admin role.
4. Click cm_kafka in the Ranger service UI.

   The List of Policies page appears.

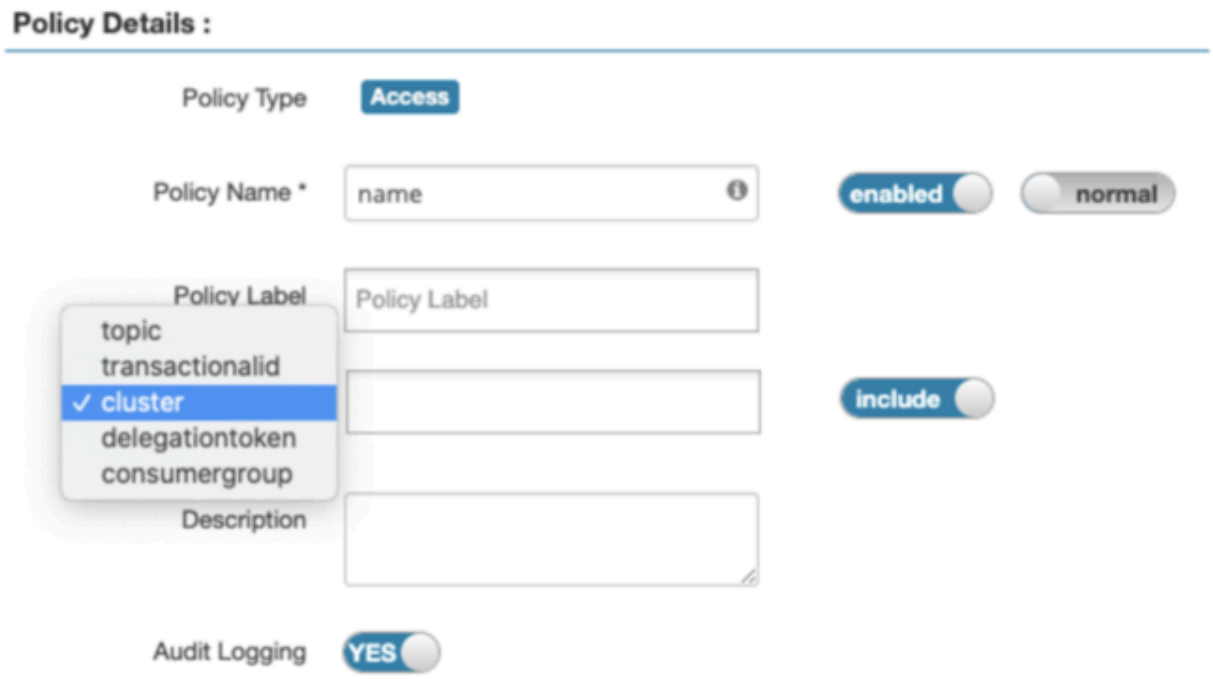
5. Click Add New Policy.



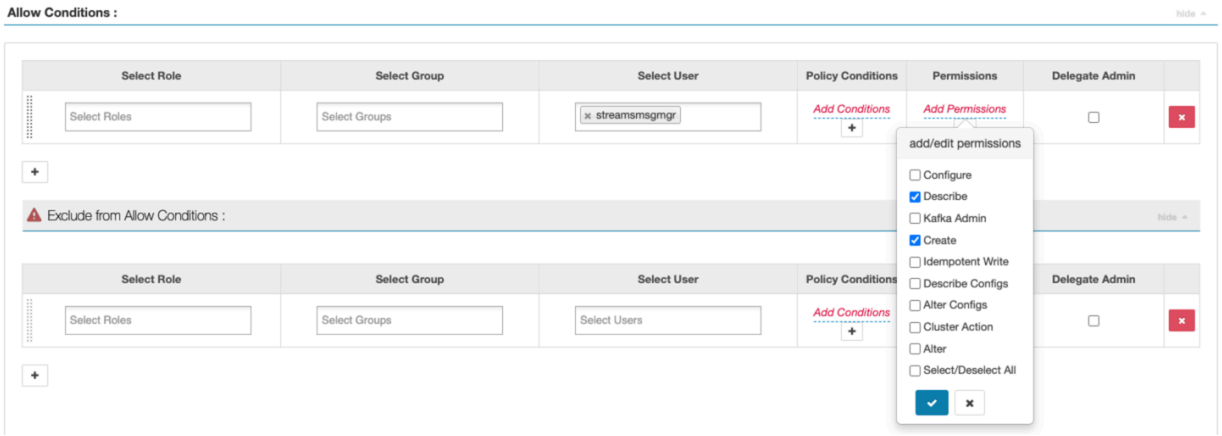
The Policy Details page appears.



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.

Related Information

Configure a resource-based service: Kafka
Enable Kerberos Authentication
Creating your first Streams Messaging cluster

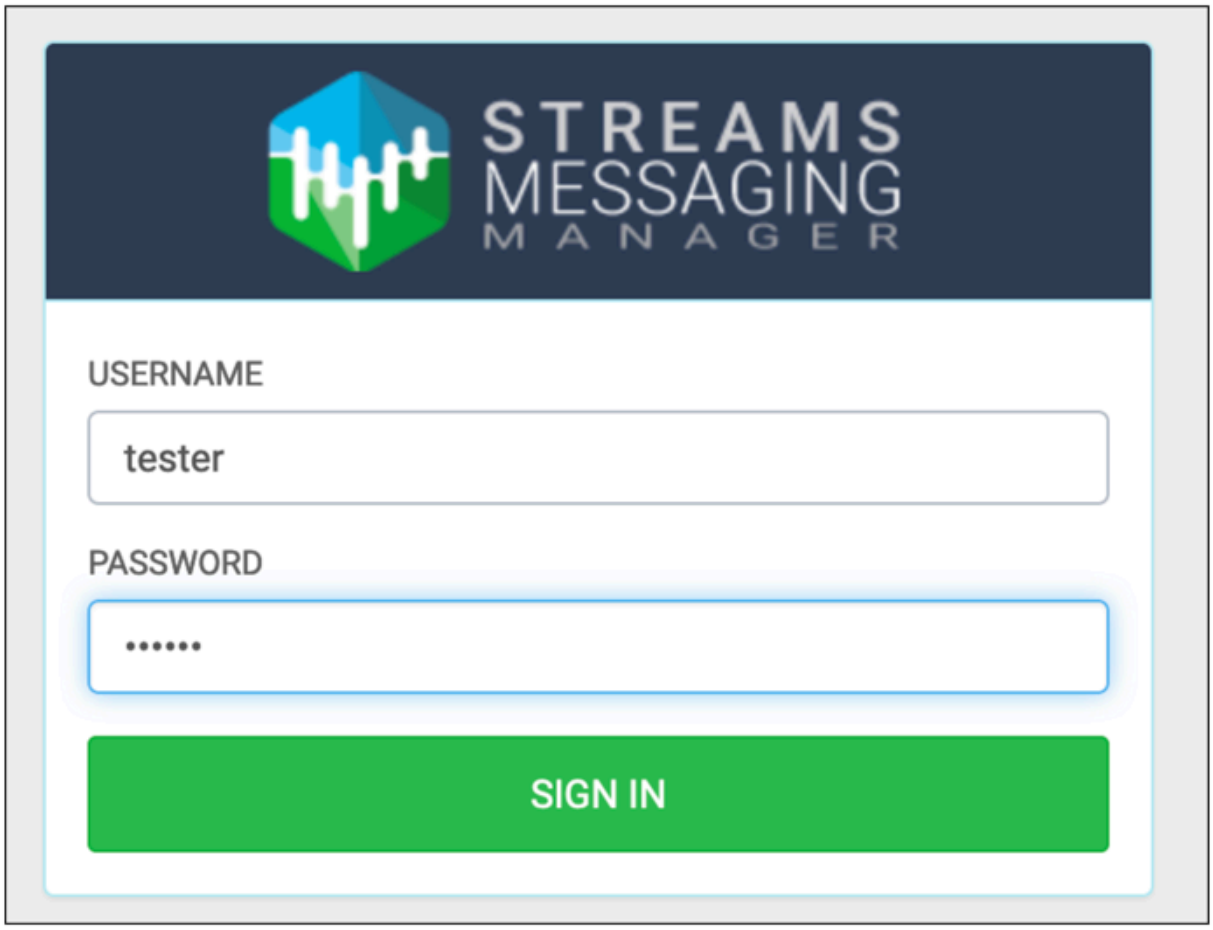
Verifying the setup

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

Procedure

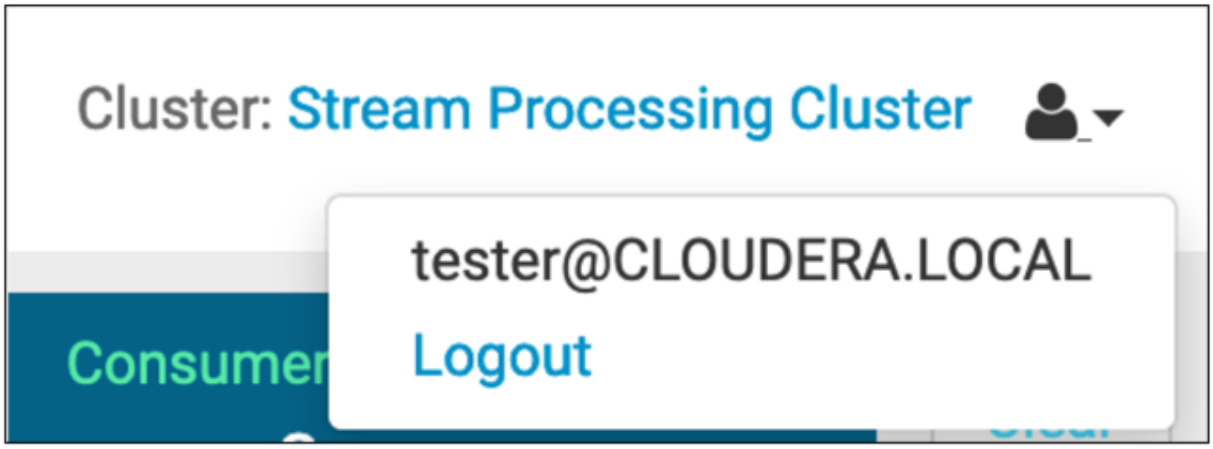
1. Go to Cloudera Manager > SMM .

   The login page for SMM appears.



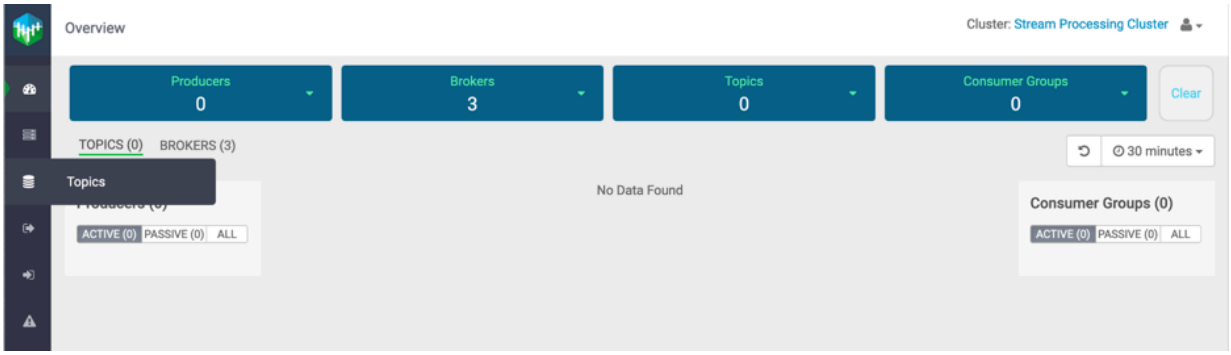
2. Login to the SMM UI using your regular credentials.

   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.

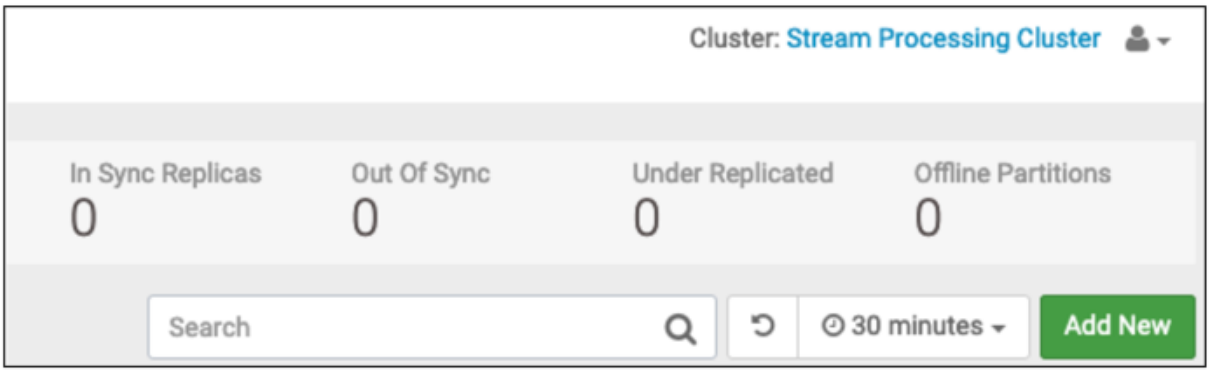


3. Click Streams Messaging Manager Web UI.

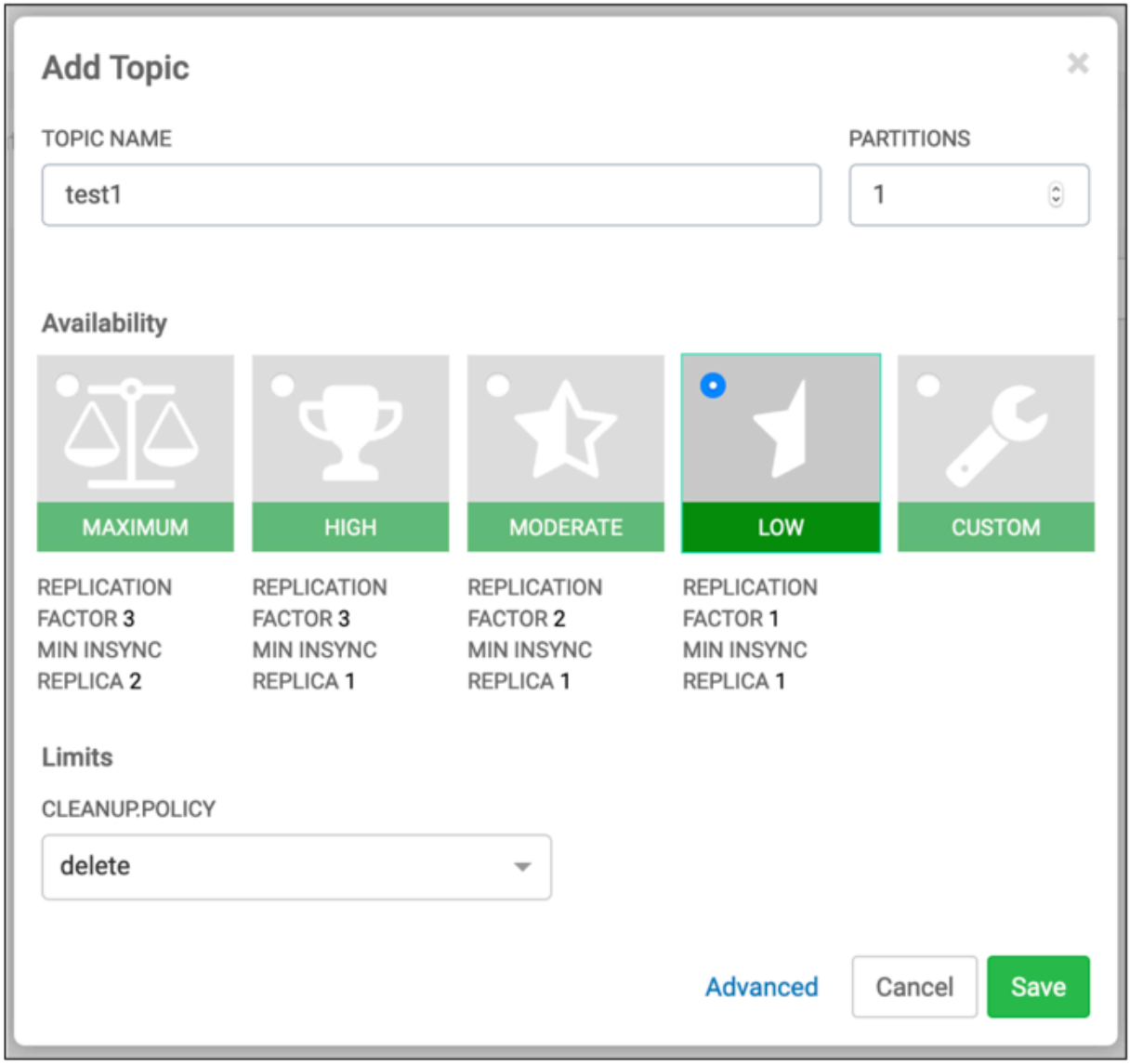
4. To add a topic, go to Topics.



5. Click Add New.

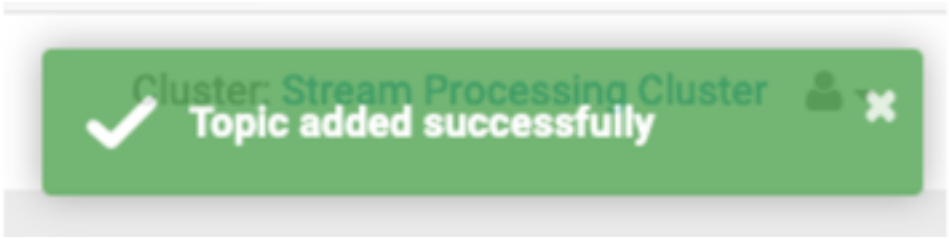


6. Add a topic name, select partitions, and cleanup policy.



7. Click Save.

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



Enabling TLS Encryption for SMM on CDP Private Cloud

Learn how to enable TLS/SSL encryption for Streams Messaging Manager (SMM) on CDP Private Cloud. You can enable the settings in Cloudera Manager according to the cluster configuration.

About this task

If Kerberos is enabled, then you must enable SSL for Streams Messaging Manager (SMM). SMM UI fails to load if Kerberos is enabled and SSL is not enabled.

Also, if Kafka has Kerberos/SSL enabled, the same should be enabled for SMM.

Procedure

1. Go to Cloudera Manager.
2. Select Streams Messaging Manager cluster.
3. Click Configuration from the menu bar.
4. In the Search field, type TLS/SSL to show the SMM TLS/SSL properties.

   The security related properties appear.
5. Edit the security properties according to the cluster configuration.
6. Click Save Changes.

TLS/SSL settings for Streams Messaging Manager

To enable TLS/SSL settings for Streams Messaging Manager (SMM), you need to configure SMM server properties, SMM UI properties, and SMM Server's Oracle TLS connection properties in Cloudera Manager according to the cluster configuration.

Table 1: TLS/SSL Settings for SMM

Properties	Description
SMM Server properties	
Enable TLS/SSL for Streams Messaging Manager Rest Admin Server ssl.enable	Encrypt communication between clients and Streams Messaging Manager Rest Admin Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).
Streams Messaging Manager port (SSL) streams.messaging.manager.ssl.port	HTTPS port Streams Messaging Manager rest server runs on when SSL is enabled.
Streams Messaging Manager Admin Port (SSL) streams.messaging.manager.ssl.adminPort	HTTPS admin port Streams Messaging Manager rest server runs on when SSL is enabled.
SSL Keystore Type streams.messaging.manager.ssl.keyStoreType	The keystore type. Required if Streams Messaging Manager rest server's SSL is enabled. e.g. PKCS12 or JKS. If it is left empty then the keystore type will come from CM settings.
SSL TrustStore Type streams.messaging.manager.ssl.trustStoreType	The truststore type. Required if streams messaging manager's ssl is enabled. e.g. PKCS12 or JKS. If it is left empty then the keystore type will come from CM settings.
Streams Messaging Manager Rest Admin Server TLS/SSL Server JKS Keystore File Location streams.messaging.manager.ssl.keyStorePath	The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Streams Messaging Manager Rest Admin Server is acting as a TLS/SSL server.
Streams Messaging Manager Rest Admin Server TLS/SSL Server JKS Keystore File Password	The password for the Streams Messaging Manager Rest Admin Server keystore file.
Streams Messaging Manager Rest Admin Server TLS/SSL Server JKS Keystore Key Password	The password that protects the private key contained in the keystore used when Streams Messaging Manager Rest Admin Server is acting as a TLS/SSL server.

Properties	Description
Streams Messaging Manager Rest Admin Server TLS/SSL Client Trust Store File streams.messaging.manager.ssl.trustStorePath	The location on disk of the trust store used to confirm the authenticity of TLS/SSL servers that Streams Messaging Manager Rest Admin Server might connect to. This is used when Streams Messaging Manager Rest Admin Server is the client in a TLS/SSL connection. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.
Streams Messaging Manager Rest Admin Server TLS/SSL Client Trust Store Password	The password for the Streams Messaging Manager Rest Admin Server TLS/SSL Certificate Trust Store File. This password is not required to access the trust store; this field can be left blank. This password provides optional integrity checking of the file. The contents of trust stores are certificates, and certificates are public information.
Cloudera Manager Metrics TrustStore Type cm.metrics.truststore.type	Cloudera Manager's truststore type. If it is left empty then the keystore type will come from CM settings. If it is left empty then the keystore type will come from CM settings.
SSL ValidateCerts streams.messaging.manager.ssl.validateCerts	Whether or not to validate TLS certificates before starting. If enabled, it will refuse to start with expired or otherwise invalid certificates.
SSL validatePeers streams.messaging.manager.ssl.validatePeers	Whether or not to validate TLS peer certificates.
SMM UI properties	
Enable TLS/SSL for Streams Messaging Manager UI Server streams.messaging.manager.ui.ssl.enable	Encrypt communication between clients and Streams Messaging Manager UI Server using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).
Streams Messaging Manager UI Server TLS/SSL Server Private Key File (PEM Format) streams.messaging.manager.ui.ssl.private.key.location	The path to the TLS/SSL file containing the private key used for TLS/SSL. Used when Streams Messaging Manager UI Server is acting as a TLS/SSL server. The certificate file must be in PEM format.
Streams Messaging Manager UI Server TLS/SSL Server Certificate File (PEM Format) streams.messaging.manager.ui.ssl.cert.location	The path to the TLS/SSL file containing the server certificate key used for TLS/SSL. Used when Streams Messaging Manager UI Server is acting as a TLS/SSL server. The certificate file must be in PEM format.
Streams Messaging Manager UI Server TLS/SSL Server CA Certificate (PEM Format) streams.messaging.manager.ui.ssl.ca.cert.location	The path to the TLS/SSL file containing the certificate of the certificate authority (CA) and any intermediate certificates used to sign the server certificate. Used when Streams Messaging Manager UI Server is acting as a TLS/SSL server. The certificate file must be in PEM format, and is usually created by concatenating all of the appropriate root and intermediate certificates.
Streams Messaging Manager UI Server TLS/SSL Private Key Password	The password for the private key in the Streams Messaging Manager UI Server TLS/SSL Server Certificate and Private Key file. If left blank, the private key is not protected by a password.
Streams Messaging Manager UI Server TLS/SSL Certificate Trust Store File streams.messaging.manager.ui.ssl.trust.store.location	The location on disk of the trust store, in .pem format, used to confirm the authenticity of TLS/SSL servers that Streams Messaging Manager UI Server might connect to. This is used when Streams Messaging Manager UI Server is the client in a TLS/SSL connection. This trust store must contain the certificate(s) used to sign the service(s) connected to. If this parameter is not provided, the default list of well-known certificate authorities is used instead.
SMM Server’s Oracle TLS connection properties	
Enable TLS with Oracle DB streams.messaging.manager.enable.TLS.Oracle	Enable TLS with Oracle as DB for Schema Registry.
Oracle.net.ssl_version streams.messaging.manager.oracle.net.ssl_version	Oracle net ssl version.
Oracle TLS javax.net.ssl.keyStore streams.messaging.manager.javax.net.ssl.keyStore	Path to keystore file if enabling TLS using Oracle DB.

Properties	Description
Oracle TLS javax.net.ssl.keyStoreType streams.messaging.manager.javax.net.ssl.keyStoreType	KeyStoreType type if enabling TLS using Oracle DB.
Oracle TLS javax.net.ssl.keyStorePassword streams.messaging.manager.javax.net.ssl.keyStorePassword	KeyStorePassword if enabling TLS using Oracle DB.
Oracle TLS javax.net.ssl.trustStore streams.messaging.manager.javax.net.ssl.trustStore	Required Path to truststore file if enabling TLS using Oracle DB.
Oracle TLS javax.net.ssl.trustStoreType streams.messaging.manager.javax.net.ssl.trustStoreType	Required Truststore type if enabling TLS using Oracle DB.
Oracle TLS javax.net.ssl.trustStorePassword streams.messaging.manager.javax.net.ssl.trustStorePassword	TrustStorePassword type if enabling TLS using Oracle DB.
Oracle TLS oracle.net.ssl_cipher_suites streams.messaging.manager.oracle.net.ssl_cipher_suites	net ssl cipher suites if enabling TLS using Oracle DB e.g. SSL_DH_DSS_WITH_DES_CBC_SHA.
Oracle TLS oracle.net.ssl_server_dn_match streams.messaging.manager.oracle.net.ssl_server_dn_match	ssl server domain name match if enabling TLS using Oracle DB.
Oracle TLS oracle.net.authentication_services streams.messaging.manager.oracle.net.authentication_services	Oracle net authentication service if enabling TLS using Oracle DB.