Cloudera Runtime 7.1.3

Securing Cruise Control

Date published: 2020-05-04
Date modified: 2020-06-16

CLOUDƎRA

https://docs.cloudera.com/

Legal Notice

Contents

Enable security for Cruise Control

You can use SSL/TLS security protocols for securing Cruise Control. The security protocol should be the same as it is for Kafka. You can also choose between Spengo and Trusted Proxy as authentication method, and can assign admin, user and viewer roles to users to achieve further authorization over Cruise Control tasks.

You can find the security settings for Cruise Control at Cloudera Manager > Configuration > Security .

You must to set the SSL/TLS security protocol in Cruise Control just as it is set for Kafka. You can set the following security protocols:

• PLAINTEXT
• SSL
• SASL_PLAINTEXT
• SASL_SSL

Keytabs are generated when using Kerberos. You need to provide the trust store file location and the trust store password.

You can enable TLS/SSL for the Cruise Control web server using the webserver.ssl.enable property. You must provide the TLS/SSL configuration settings of the Kafka broker to the keystore. For more information about the security settings for Kafka, see the Kafka documentation.

There are two authentication methods for Cruise Control Spengo and Trusted Proxy. Spengo uses Kerberos over HTTP. Trusted Proxy uses Knox through a gateway mechanism where Knox authenticates with Cruise Control over Spengo and forwards the real user ID.

You can specify users in the following user groups:

• Admin role: has access to all endpoints
• User role: has access to all the GET endpoints except bootstrap and train
• Viewer role: has access to the most lightweight kafka_cluster_state, user_tasks and review_board endpoints