Cloudera Runtime 7.3.1

Securing Cruise Control

Date published: 2019-08-22
Date modified: 2024-12-10

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

Enable security for Cruise Control

When AutoTLS is disabled, you need to configure the security properties in Cloudera Manager to use Cruise Control in a secure environment. You can also choose between SPENGO and Trusted Proxy as an authentication method, and can assign admin, user and viewer roles to users to achieve further authorization over Cruise Control tasks.

About this task

You can use TLS/SSL security protocols for securing Cruise Control. You must set the TLS/SSL security protocol in Cruise Control just as it is set for Kafka. When TLS/SSL security is enabled, the secure connection is automatically set for Zookeeper as well for secure communication and the non-secure ports are cannot be used.

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.

Before you begin

Ensure that you have set up TLS for Cloudera Manager:

- Generate TLS certificates
- Configure TLS for Admin Console and Agents
- Enable server certificate verification on Agents
- Configure agent certificate authentication

Procedure

1. Access Cloudera Manager for the Cruise Control configurations.
   a) Go to your cluster in Cloudera Manager.
   b) Select Cruise Control from the list of Services.
   c) Click on Configuration tab.
2. Select Category > Main.
3. Edit the authorization and Kafka security properties according to the cluster configuration.

   You need the following authorization and security properties from the Main category.

Security property		Description
Kafka Client Security Protocol	security.protocol	Protocol to be used for communicating with Kafka. Select the same protocol as you use for Kafka.
Authentication Method	auth_method	Authentication method that Cruise Control uses to authenticate clients.
Trusted Proxy Authentication Service	trusted_auth_service_user	The username part of the trusted proxy authentication service's principal. The default service is Knox for Cruise Control.
ADMIN Level Users	auth_admins	The list of ADMIN level users to have access to all endpoints.
USER Level Users	auth_users	The list of USER level users to have access to all the GET endpoints except bootstrap and train.
VIEWER Level Users	auth_viewers	The list of VIEWER level users to have access to the most lightweight kafka_cluster_state, user_tasks and review_board endpoints.

4. Click Save Changes.

5. Click Clear next to the Category Filter.
6. Select Category > Security.
   All the security related properties are displayed.
7. Edit the security properties according to the cluster configuration.

Security property		Description
Enable TLS/SSL for Cruise Control Server	webserver.ssl.enable	Encrypting communication between clients and Cruise Control Server using TLS.
Cruise Control Server TLS/SSL Server Keystore File Location	webserver.ssl.keystore.location	The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Cruise Control Server is acting as a TLS/SSL server.
Cruise Control Server TLS/SSL Server Keystore File Password	webserver.ssl.keystore.password	The password for the Cruise Control Server keystore file.
Cruise Control Server TLS/SSL Server Keystore Key Password	webserver.ssl.key.password	The password that protects the private key contained in the keystore used when Cruise Control Server is acting as a TLS/SSL server.
HTTP Strict Transport Security Enabled	webserver.ssl.sts.enabled	Enables the Strict Transport Security header in the web server responses. By default the configuration is enabled.
Cruise Control Server TLS/SSL Client Trust Store File	ssl.truststore.location	The location on disk of the trust store, used to confirm the authenticity of TLS/SSL servers that Cruise Control Server might connect to. This is used when Cruise Control 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.
Cruise Control Server TLS/SSL Client Trust Store Password	ssl.truststore.password	The password for the Cruise Control Server TLS/SSL Certificate Trust Store File. This password is not required to access the trust store, the 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.

8. Click Save Changes.
9. Click Clear next to the Category Filter.
10. Type ssl.properties to the Search field.

    The Cruise Control Server Advanced Configuration Snippet (Safety Valve) for ssl.properties field is displayed. You can define additional confiuration parameters for Cruise Control in the Safety Valve field. You also need to add properties that are inherited from Kafka clients, if needed for the secured communication. The values for the inherited properties should match with the values defined in Kafka.

a) Add the webserver keystore type, if needed, by adding the following property and its value to the Advanced Configuration Snippetfield.

Security property	Description
webserver.ssl.keystore.type	The file format of the key store file. This configuration is optional. If the keystore type for the webserver is not set, it falls back to Jetty's default behavior.

b) Add the following additional security properties to the Advanced Configuration Snippet.

Security property	Description
ssl.provider	The name of the security provider used for SSL connections. Default value is the default security provider of the JVM.
ssl.cipher.suites	A cipher suite is a named combination of authentication, encryption, MAC, and a key exchange algorithm used to negotiate the security settings for a network connection using TLS or SSL network protocol.
ssl.enabled.protocols	This property should list at least one of the protocols (TLSv1.2, TLSv1.1,TLSv1) configured on the broker side.
ssl.truststore.type	The file format of the trust store file.
ssl.keystore.type	The file format of the key store file.

11. Adding the following properties to the Advanced Configuration Snippet helps customizing the default TLS configurations defined for the Cruise Control web server:

Security property	Description
webserver.ssl.include.ciphers	Sets the included ciphers for the webserver.
webserver.ssl.exclude.ciphers	Sets the excluded ciphers for the webserver.
webserver.ssl.include.protocols	Sets the included protocols for the webserver.
webserver.ssl.exclude.protocols	Sets the excluded protocols for the webserver.

12. Click Save Changes.

Configuring custom Kerberos principal for Cruise Control

The Kerberos principal for Cruise Control is configured by default to use the same service principal as the default process user. To change the default setting:

Procedure

1. Go to your Cluster in Cloudera Manager.
2. Select Cruise Control from the list of services.
3. Go to the Configuration tab.
4. Search for the Kerberos principal by entering "kerberos" in the search field.
5. Provide a custom name to the Kerberos Principal property.
6. Click Save Changes.
7. Click on Actions > Restart next to the Cruise Control service name to restart the service.

What to do next

If you use Ranger for authorization, update all resource-based services and policies that use the old principal and add the new principal. For more information on updating resource-based services and policies, see *Using Ranger to Provide Authorization in CDP*.

Related Information

Using Ranger to Provide Authorization in CDP