Cloudera Runtime 7.0.2

Configuring Advanced Security Options for Apache Ranger

Date published: 2019-11-01
Date modified:

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

Configure Kerberos authentication for Apache Ranger

How to configure Kerberos Authentication for Apache Ranger

About this task

Kerberos authentication for Apache Ranger is automatically configured when HDFS Kerberos authentication is configured in Cloudera Manager (typically using the Cloudera Manager Kerberos Wizard).

Specifically, Ranger depends on the HDFS hadoop.security.authentication property to enable or disable Kerberos authentication. When the hadoop.security.authentication property is updated, the Ranger service gets a restart indicator for the core-site.xml file that resides inside the Ranger service conf directory generated by Cloudera Manager.

Ranger Kerberos authentication is automatically enabled when HDFS Kerberos authentication is enabled.

Related Information

Enabling Kerberos Authentication for CDP

Configure TLS/SSL for Apache Ranger

How to configure TLS/SSL for Apache Ranger

About this task

Procedure

1. In Cloudera Manager, select Ranger, then click the Configuration tab.
2. Under Category, select Security.
3. Set the following properties.

Table 1: Apache Ranger TLS/SSL Settings

Configuration Property	Description
Enable TLS/SSL for Ranger Admin ranger.service.https.attrib.ssl.enabled	Select this check box to encrypt communication between clients and Ranger Admin using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).
Ranger Admin TLS/SSL Server JKS Keystore File Location ranger.https.attrib.keystore.file	The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Ranger Admin is acting as a TLS/SSL server. The keystore must be in JKS format.
Ranger Admin TLS/SSL Server JKS Keystore File Password ranger.service.https.attrib.keystore.pass	The password for the Ranger Admin JKS keystore file.
Ranger Admin TLS/SSL Client Trust Store File ranger.truststore.file	The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Ranger Admin might connect to. This is used when Ranger Admin is the client in a TLS/SSL connection. This trust store must contain the certificate(s) used to sign the connected service(s). If this parameter is not provided, the default list of well known certificate authorities is used.

Configuration Property	Description
Ranger Admin TLS/SSL Client Trust Store Password ranger.truststore.password	The password for the Ranger Admin 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.
Enable TLS/SSL for Ranger Tagsync	Select this check box to encrypt communication between clients and Ranger Tagsync using Transport Layer Security (TLS) (formerly known as Secure Socket Layer (SSL)).
Ranger Tagsync TLS/SSL Server JKS Keystore File Location xasecure.policymgr.clientssl.keystore	The path to the TLS/SSL keystore file containing the server certificate and private key used for TLS/SSL. Used when Ranger Tagsync is acting as a TLS/SSL server. The keystore must be in JKS format.
Ranger Tagsync TLS/SSL Server JKS Keystore File Password xasecure.policymgr.clientssl.keystore.password	The password for the Ranger Tagsync JKS keystore file.
Ranger Tagsync TLS/SSL Client Trust Store Password xasecure.policymgr.clientssl.truststore.password	The password for the Ranger Tagsync 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.
Ranger Usersync TLS/SSL Client Trust Store File ranger.usersync.truststore.file	The location on disk of the trust store, in .jks format, used to confirm the authenticity of TLS/SSL servers that Ranger Usersync might connect to. This is used when Ranger Usersync is the client in a TLS/SSL connection. This trust store must contain the certificate(s) used to sign the connected service(s). If this parameter is not provided, the default list of well known certificate authorities is used.
Ranger Usersync TLS/SSL Client Trust Store Password ranger.usersync.truststore.password	The password for the Ranger Usersync 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.

4. Click Save Changes.