Cloudera Runtime 7.2.18

Configuring Infra Solr

Date published: 2015-05-05
Date modified: 2024-04-03



https://docs.cloudera.com/

Legal Notice

© Cloudera Inc. 2026. All rights reserved.

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 Ranger authorization on the Solr service used by Ranger for auditing.....4

Configuring custom Kerberos principals for Solr..... 4

Enable Ranger authorization on the Solr service used by Ranger for auditing

Add a Ranger service to enable access control on the Solr service that is used by Ranger to index and store audit logs (Infra Solr).

Before you begin

- Ranger authorization requires that Kerberos authentication is enabled in Solr.

Procedure

1. In Cloudera Manager select the Infra Solr service that is used by Ranger to index and store audit logs.
2. Select Configuration and find the Enable Ranger Authorization for the Infrastructure Solr Service property.
3. Select Enable Ranger Authorization for the Infrastructure Solr Service.
4. Click Save Changes.
5. Restart the Solr service.

Results

Ranger authorization is enabled. The Solr service depends on the selected Ranger service for authorization.

Note: If you want Service Monitor (SMON) user to access Ranger policies for monitoring, add hue to the Ranger policies in Solr.

1. Go to Cloudera Manager Ranger Web UI Ranger Admin Web UI .
2. On the **Service Manager** page, click cm_solr under SOLR.
3. Click Edit button under Actions for all - schema and all - collection policies.
4. Select the hue user (if not already added) under Allow Conditions and save changes.

Related Information

Configure a resource-based service: Solr

Configuring custom Kerberos principals for Solr

In a Kerberos enabled cluster, the Solr service uses the solr principal by default. Changing the default principal and using custom principals is supported. Principals can be configured on a service-wide level in Cloudera Manager with the Kerberos Principal property.

Before you begin

- Ensure that you have the following privileges:
  - SSH access to the cluster where you want to enable the custom principal
  - administrative privileges in Cloudera Manager
  - HDFS super user access
- If the SunJCE cryptographic provider is removed to run the zkcli.sh utility, you must set the JDK_JAVA_OPTIONS environment variable. For example,

```
export FIPS_JAVA_ARGS
=
"-Dcom.safelogic.cryptocomply.fips.approved_only=true  --add-modules=com
.safelogic.cryptocomply.fips.core  --add-modules=bctls  --add-exports=ja
```

```
va.base/sun.security.provider=com.safelogic.cryptocomply.fips.core  --add-
exports=java.base/sun.security.provider=bctls  --module-path=/cdep/extra_j
ars  -Djdk.tls.trustNameService=true  -Dsun.security.krb5.disableReferra
ls=true  -Djdk.tls.ephemeralDHKeySize=2048  -Dcom.sun.management.jmxremo
te.ssl.enabled.protocols=TLSv1.2,TLSv1.3 --add-opens=java.base/java.lang
=ALL-UNNAMED --add-opens=java.base/java.util=ALL-UNNAMED --add-opens=jav
a.base/java.util.zip=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED
 --add-opens=java.base/java.lang.reflect=ALL-UNNAMED --add-opens=java.base
/java.net=ALL-UNNAMED --add-exports=java.base/sun.net.www.protocol.jar=A
LL-UNNAMED --add-opens=java.base/sun.net.www.protocol.jar=ALL-UNNAMED --
add-opens=java.base/sun.net.www.protocol.file=ALL-UNNAMED --add-exports=
java.base/sun.net.www=ALL-UNNAMED --add-opens=java.base/sun.net.www=ALL-
UNNAMED"


export JDK_JAVA_OPTIONS
=
"${JDK_JAVA_OPTIONS} ${FIPS_JAVA_ARGS}"
```

Procedure

1. Stop the Solr service.
2. Disable ZooKeeper ACL checking temporarily.
   a) In Cloudera Manager, navigate to ZooKeeper Configuration .
   b) Find the Java Configuration Options for ZooKeeper Server property.
   c) Add the following value:

      ```
      -Dzookeeper.skipACL=yes
      ```

   d) Click Save Changes.
   e) Restart the ZooKeeper service.
3. In Cloudera Manager, navigate to Clusters Solr service Configuration and find the Kerberos Principal property.
4. Provide the custom Kerberos principal.
5. Click Save Changes.
6. If the Solr system user (service user) does not match the custom Kerberos principal, configure the solr.security.proxyuser properties for the system user:
   a) In Cloudera Manager, navigate to Clusters Solr service Configuration and find the Solr Service Environment Advanced Configuration Snippet (Safety Valve) property.
   b) Locate the SOLR_SECURITY_PROXY_JAVA_OPTS key and append its value with the following:

      ```
      -Dsolr.security.proxyuser.[***SYSTEM_USER***].groups=* -Dsolr.securit
      y.proxyuser.[***SYSTEM_USER***].hosts=*
      ```

      Replace *[***SYSTEM_USER***]* with the service user name you want to associate with the custom Kerberos principal.
   c) Click Save Changes.
7. Create a jaas.conf file containing the following:

```
Client {
          com.sun.security.auth.module.Krb5LoginModule required
          useKeyTab=false
          useTicketCache=true
          principal
="[***CUSTOM_SOLR_KERBEROS_PRINCIPAL@KERBEROS_REALM_NAME***]";
          };
```

Replace *[***CUSTOM_SOLR_KERBEROS_PRINCIPAL@KERBEROS_REALM_NAME***]* with your Kerberos principal and realm name.

8. Set the *LOG4J_PROPS* environment variable to a log4j.properties file:

```
export LOG4J_PROPS=/etc/zookeeper/conf/log4j.properties
```

9. Set the ZKCLI_JVM_FLAGS environment variable:

```
export ZKCLI_JVM_FLAGS="-Djava.security.auth.login.config=/path/to/jaas.
conf \
-DzkACLProvider=org.apache.solr.common.cloud.SaslZkACLProvider \
-Droot.logger=INFO,console \
-Dsolr.authorization.superuser=[***CUSTOM_SOLR_KERBEROS_PRINCIPAL***]"
```



Note: If Solr ZooKeeper TLS is enabled, append the JVM options documented in Using Search ZooKeeper CLI tools with TLS-enabled ZooKeeper to this export.

10. Authenticate as the *[***CUSTOM_SOLR_KERBEROS_PRINCIPAL***]*:

```
kinit [***CUSTOM_SOLR_KERBEROS_PRINCIPAL@KERBEROS_REALM_NAME***]
```

Replace *[***CUSTOM_SOLR_KERBEROS_PRINCIPAL@KERBEROS_REALM_NAME***]* with your Kerberos principal and realm name.

11. Run the zkcli.sh script as follows:

```
/opt/cloudera/parcels/CDH/lib/solr/bin/zkcli.sh -zkh
ost [***ZOOKEEPER_SERVER_HOSTNAME***]:[***ZOOKEEPER_SERVER_PORT***] -cmd
 updateacls /solr
```

Replace *[***ZOOKEEPER_SERVER_HOSTNAME***]* and *[***ZOOKEEPER_SERVER_PORT***]* with the hostname and port of a ZooKeeper server.



Note: If Solr ZooKeeper TLS is enabled, set ZKCLI_JVM_FLAGS as described in Using Search ZooKeeper CLI tools with TLS-enabled ZooKeeper before you run this command.

For example:

```
/opt/cloudera/parcels/CDH/lib/solr/bin/zkcli.sh -zkhost zk01.example.com
:2181 -cmd updateacls /solr
```

12. Check ACLs in Zookeeper:

```
zookeeper-client -server ${HOSTNAME}:2181 getAcl /solr
```

13. Change ownership of Solr's HDFS Data Directory. Check the value in Cloudera Manager under Solr Configuration HDFS Data Directory .
14. Execute the following command as the HDFS superuser:

```
hdfs dfs -chown -R [***CUSTOM_SOLR_KERBEROS_PRINCIPAL***] [***HDFS_DATA_
DIRECTORY***]
```

15. Re-enable ZooKeeper ACL check.
    a) In Cloudera Manager, navigate to ZooKeeper Configuration .
    b) Find the Java Configuration Options for ZooKeeper Server property.
    c) Remove the following value:

```
-Dzookeeper.skipACL=yes
```

d) Click Save Changes.
e) Restart the ZooKeeper service.