How to configure Solr Cloud with Kerberos for Ranger 0.5

Overview

Apache Ranger supports Apache Solr 5.2 in SolrCloud mode. For enabling Ranger authorization, the following need to be done:

1. Install Apache Solr 5.2
2. Install and configure Kerberos
3. Configure SolrCloud

Install Apache Solr 5.2

Download Apache Solr 5.2 from http://archive.apache.org/dist/lucene/solr. Extract the package on all the servers.

Install and configure Kerberos

Follow the below instructions. You might want to replace everything that is in **bold** with your custom values.

- Install and configure MIT Kerberos. If you have ActiveDirectory in your environment, then you can use ActiveDirectory as your Kerberos KDC.
- Create principal "solr" in your KDC. You can make it host specific or headless
    - For MIT KDC, login as root on to server which has KDC and create the keytabs for user solr and HTTP

```
kadmin.local
Authenticating as principal root/admin@EXAMPLE.COM with password.
kadmin.local:  addprinc -randkey solr@EXAMPLE.COM
WARNING: no policy specified for solr@EXAMPLE.COM; defaulting to no policy
Principal "solr@EXAMPLE.COM" created.
kadmin.local:  xst -k solr.keytab solr@EXAMPLE.COM
Entry for principal solr@EXAMPLE.COM with kvno 2, encryption type aes256-cts-hmac-sha1-96 added to
keytab WRFILE:solr.keytab.
Entry for principal solr@EXAMPLE.COM with kvno 2, encryption type aes128-cts-hmac-sha1-96 added to
keytab WRFILE:solr.keytab.
Entry for principal solr@EXAMPLE.COM with kvno 2, encryption type des3-cbc-sha1 added to keytab
WRFILE:solr.keytab.
Entry for principal solr@EXAMPLE.COM with kvno 2, encryption type arcfour-hmac added to keytab
WRFILE:solr.keytab.
Entry for principal solr@EXAMPLE.COM with kvno 2, encryption type des-hmac-sha1 added to keytab
WRFILE:solr.keytab.
Entry for principal solr@EXAMPLE.COM with kvno 2, encryption type des-cbc-md5 added to keytab
WRFILE:solr.keytab.
kadmin.local:  quit
```

    - The above example creates headless keytab for service user "solr". It is recommend to create keytab per host. If you wish to do that, then for each host where Solr is going to run, create a principal like above, except use the principal name with the host, e.g. addprinc -randkey solr/***${HOST1}***@EXAMPLE.COM. Replace ***${HOST1}*** with the actual host names
    - You will also need another keytab for SPNEGO. This is used by Solr for authenticating HTTP request. Follow the above process, but replace solr with HTTP. E.g.

```
kadmin.local
kadmin.local:  addprinc -randkey HTTP@EXAMPLE.COM
kadmin.local:  xst -k HTTP.keytab HTTP@EXAMPLE.COM
kadmin.local:  quit
```

- After the keytabs is created you need to copy them to all the hosts running Solr. And chown to solr and chmod to 400.

```
mkdir -p /etc/solr/conf
#scp both the keytab files to the above folder
chown solr:solr /etc/solr/conf/solr.keytab
chmod 400 /etc/solr/conf/solr.keytab
chown solr:solr /etc/solr/conf/HTTP.keytab
chmod 400 /etc/solr/conf/HTTP.keytab
```

Configuring SolrCloud

Follow the below instructions. You might want to replace everything that is in **bold** with your custom values.

- Install ZooKeeper and setup the ensemble. If you are using Hadoop, it is very likely you might already have Zookeeper installed and configured. Else, follow the instruction from Solr site for configuring ZooKeeper.
- Create path in zookeeper for storing the Solr configs and other parameters.
  - ***$SOLR_INSTALL_HOME***/server/scripts/cloud-scripts/zkcli.sh -zkhost ***$ZK_HOST***:281 -cmd makepath **solr**
- Upload your collection config to zookeeper. Below is an example to upload a default config packaged in Solr
  - ***$SOLR_INSTALL_HOME***/server/scripts/cloud-scripts/zkcli.sh -cmd upconfig -zkhost ***$ZK_HOST***:2181/**solr** -confname **basic_configs** -confdir **$SOLR_INSTALL_HOME/server/solr/configsets/basic_configs/conf**
- Create a new JAAS file at the path /etc/solr/conf and replace the REALM name **@EXAMPLE.COM** with your REALM name.

```
vi /etc/solr/conf/solr_jaas.conf
Client {
       com.sun.security.auth.module.Krb5LoginModule required
       useKeyTab=true
       keyTab="/etc/solr/conf/solr.keytab"
       storeKey=true
       useTicketCache=true
       debug=true
       principal="solr@EXAMPLE.COM";
};
```

- Copy the solr_jaas.conf to all the host which are running Solr
- Update solr.in.sh in $SOLR_INSTALL_HOME/bin/solr.in.sh

  vi $SOLR_INSTALL_HOME/bin/solr.in.sh and add the below lines at the end

  SOLR_JAAS_FILE=/etc/solr/conf/solr_jaas.conf
  SOLR_HOST=`hostname -f`
  ZK_HOST="***$ZK_HOST1***:2181,***$ZK_HOST2***:2181,***$ZK_HOST3***:2181/solr"
  KERBEROS_REALM="***EXAMPLE.COM***"
  SOLR_KEYTAB=/etc/solr/conf/solr.keytab
  SOLR_KERB_PRINCIPAL=HTTP@${KERBEROS_REALM}
  SOLR_KERB_KEYTAB=/etc/solr/conf/HTTP.keytab
  SOLR_AUTHENTICATION_CLIENT_CONFIGURER="org.apache.solr.client.solrj.impl.Krb5HttpClientConfigurer"
  SOLR_AUTHENTICATION_OPTS=" -DauthenticationPlugin=org.apache.solr.security.KerberosPlugin -Djava.security.auth.login.config=$SOLR_JAAS_FILE -Dsolr.kerberos.principal=${SOLR_KERB_PRINCIPAL} -Dsolr.kerberos.keytab=${SOLR_KERB_KEYTAB} -Dsolr.kerberos.cookie.domain=${SOLR_HOST} -Dhost=${SOLR_HOST} -Dsolr.kerberos.name.rules=DEFAULT"

- Copy solr.in.sh to all the host which will be running Solr
- Enable Kerberos as the authentication scheme by updating security.json in zookeeper

```
$SOLR_INSTALL_HOME/server/scripts/cloud-scripts/zkcli.sh -zkhost  $ZK_HOST:2181 -cmd put /solr/security.
json '{"authentication":{"class": "org.apache.solr.security.KerberosPlugin"}}'
```

- Now restart Solr on all hosts. With this setting only access via Kerberos authentication is enabled. For configuring authorization, you can now use Ranger for Solr, refer to Apache Ranger 0.5.0 Installation#EnablingRangerSolrPlugin

Connecting to Kerberos enabled Solr from your local machine.

- On Linux and Mac, copy /etc/krb5.conf from the Solr host to your local /etc/krb5.conf. If you already have a local /etc/krb5.conf, then you could merge both
- Create an user on the KDC.
    - Go to the KDC and login as root

      ```
      # kadmin.local
      addprinc $USERNAME@EXAMPLE.COM
      ```
- On your local machine
    - kinit **$USERNAME@EXAMPLE.COM**
- Use Safari and FireFox to connect to your Solr URL

Trouble Shooting

Kerberos not working

There could be multiple issues, the common ones are:

- Make sure the user "solr" has permissions to read the keytab files and jaas config file.
- Make sure the solr.in.sh is updated properly