Configuring TLS/SSL for HDFS, YARN and MapReduce (#xd_583c10bfdbd326ba--6eed2fb8-14349d04bee--76bb)

Required Role: Configurator (cm_sg_user_roles.html#concept_wfh_tvy_qp__configurator), Cluster Administrator (cm_sg_user_roles.html#concept_wfh_tvy_qp__cluster_admin), or Full Administrator (cm_sg_user_roles.html#concept_wfh_tvy_qp__fulladministrator)

TLS/SSL for the core Hadoop services—HDFS, MapReduce, and YARN—must be enabled as a group. Because most clusters run either MapReduce or YARN, not both, you will typically enable HDFS and YARN, or HDFS and MapReduce. Enabling TLS/SSL on HDFS is required before it can be enabled on either MapReduce or YARN.

Note: If you enable TLS/SSL for HDFS, you must also enable it for MapReduce or YARN.

The steps below include enabling Kerberos authentication for HTTP Web-Consoles. Enabling TLS/SSL for the core Hadoop services on a cluster without enabling authentication displays a warning.

Before You Begin (#xd_583c10bfdbd326ba--6eed2fb8-14349d04bee--76bb__section_ijw_lgy_5q)

- Before enabling TLS/SSL, keystores containing certificates bound to the appropriate domain names will need to be accessible on all hosts on which at least one HDFS, MapReduce, or YARN daemon role is running.
- Since HDFS, MapReduce, and YARN daemons act as TLS/SSL clients as well as TLS/SSL servers, they must have access to truststores. In many cases, the most practical approach is to deploy truststores to all hosts in the cluster, as it may not be desirable to determine in advance the set of hosts on which clients will run.
- Keystores for HDFS, MapReduce and YARN must be owned by the `hadoop` group, and have permissions `0440` (that is, readable by owner and group). Truststores must have permissions `0444` (that is, readable by all)
- Cloudera Manager supports TLS/SSL co… d YARN at the service level. For each of th… paths to the keystore and truststore files. Thes… ae roles of the service in question run. Ther… li all hosts.

An implication of this is that the keystore file names for a given service must be the same on all hosts. If, for example, you have obtained separate certificates for HDFS daemons on hosts `node1.example.com` and `node2.example.com`, you might have chosen to store these certificates in files called `hdfs-node1.keystore` and `hdfs-node2.keystore` (respectively). When deploying these keystores, you must give them both the same name on the target host — for example, `hdfs.keystore`.

- Multiple daemons running on a host can share a certificate. For example, in case there is a DataNode and an Oozie server running on the same host, they can use the same certificate.

Configuring TLS/SSL for HDFS (#xd_583c10bfdbd326ba--6eed2fb8-14349d04bee--76bb__section_wcb_ngy_5q)

1. Go to the **HDFS** service.
2. Click the Configuration tab.
3. Select Scope > HDFS (Service-Wide).
4. Select Category > Security.
5. In the Search field, type **TLS/SSL** to show the TLS/SSL properties (found under the **Service-Wide** > **Security** category).
6. Edit the following properties according to your cluster configuration:

Property	Description
Hadoop TLS/SSL Server Keystore File Location	Path to the keystore file containing the server certificate and private key.
Hadoop TLS/SSL Server Keystore File Password	Password for the server keystore file.
Hadoop TLS/SSL Server Keystore Key Password	Password that protects the private key contained in the server keystore.

7. If you are not using the default truststore, configure TLS/SSL client truststore properties:
   Important: The HDFS properties below define a cluster-wide default truststore that can be overridden by YARN and MapReduce (see the **Configuring TLS/SSL for YARN and MapReduce** section below).

Property	Description
Cluster-Wide Default TLS/SSL Client Truststore Location	Path to the cli… certificates of … trusted to ider…

Property	Description
Cluster-Wide Default TLS/SSL Client Truststore Password	Password for the client truststore file.

8. **(Optional)** Cloudera recommends you enable web UI authentication for the HDFS service. Web UI authentication uses SPNEGO. After enabling this, you cannot access the Hadoop web consoles without a valid Kerberos ticket and proper client-side configuration. For more information, see **How to Configure Browsers for Kerberos Authentication (cdh_sg_browser_access_kerberos_protected_url.html)** .

   To enable web UI authentication, enter **web consoles** in the Search field to bring up the **Enable Authentication for HTTP Web-Consoles** property (found under the **Service-Wide**>**Security** category). Check the property to enable web UI authentication.

Enable Authentication for HTTP Web-Consoles	Enables authentication for Hadoop HTTP web-consoles for all roles of this service. Note: This is effective only if security is enabled for the HDFS service.

9. Click **Save Changes**.
10. Follow the procedure described in the following **Configuring TLS/SSL for YARN and MapReduce** section, at the end of which you will be instructed to restart all the affected services (HDFS, MapReduce and YARN).

Configuring TLS/SSL for YARN or MapReduce (#xd_583c10bfdbd326ba--6eed2fb8-14349d04bee--76bb__section_kpb_4gy_5q)

Perform the following steps to configure TLS/SSL for the YARN or MapReduce services:

1. Go to the **YARN** or **MapReduce** service.
2. Click the Configuration tab.
3. Select Scope > *service name* (Service-Wide).
4. Select Category > Security.
5. Locate the <property name> property o Search box.
6. In the Search field, type **TLS/SSL** to sh le **Service-Wide** > **Security** category).
7. Edit the following properties according to your cluster configuration:

Property	Description
Hadoop TLS/SSL Server Keystore File Location	Path to the keystore file containing the server certificate and private key.
Hadoop TLS/SSL Server Keystore File Password	Password for the server keystore file.
Hadoop TLS/SSL Server Keystore Key Password	Password that protects the private key contained in the server keystore.

8. Configure the following TLS/SSL client truststore properties for MRv1 or YARN only if you want to override the cluster-wide defaults set by the HDFS properties configured above.

Property	Description
TLS/SSL Client Truststore File Location	Path to the client truststore file. This truststore contains certificates of trusted servers, or of Certificate Authorities trusted to identify servers.
TLS/SSL Client Truststore File Password	Password for the client truststore file.

9. Cloudera recommends you enable Web UI authentication for the service in question.

   Enter **web consoles** in the Search field to bring up the **Enable Authentication for HTTP Web-Consoles** property (found under the **Service-Wide**>**Security** category). Check the property to enable web UI authentication.

Enable Authentication for HTTP Web-Consoles	Enables authentication for Hadoop HTTP web-consoles for all roles of this service. Note: This is effective only if security is enabled for the HDFS service.

10. Enter a Reason for change, and then click Save Changes to commit the changes.
11. Go to the **HDFS** service
12. Click the Configuration tab.
13. Type Hadoop SSL Enabled in the Search
14. Select the Hadoop SSL Enabled propert FS MapReduce, and YARN.

Property	Description

Property	Description
Hadoop TLS/SSL Enabled	Enable TLS/SSL encryption for HDFS, MapReduce, and YARN web UIs, as well as encrypted shuffle for MapReduce and YARN.

15. Enter a Reason for change, and then click Save Changes to commit the changes.
16. Restart all affected services (HDFS, MapReduce and YARN), as well as their dependent services.

Configuring HSTS for HDFS (#xd_583c10bfdbd326ba--6eed2fb8-14349d04bee--76bb__section_lpn_sty_flb)

Configuring the HTTP Strict Transport Security (HSTS) for HDFS ensures that a web browser does not load the service information using HTTP. Additionally, all attempts to load the information using HTTP will automatically be converted to HTTPS.

Perform the following steps to configure HSTS for HDFS:

1. Go to the **HDFS** service.
2. Click the Configuration tab.
3. Set the HSTS credentials in Cluster-wide Advanced Configuration Snippet (Safety Valve) for core-site.xml.

```
<property>
<name>hadoop.http.header.Strict_Transport_Security</name>
<value>max-age=63072000;includeSubDomains;preload</value>
</property>
```

4. If required, configure additional headers by using the safety value specified in the previous step for the `hadoop.http.header.http-header` property.
5. Enter a Reason for change, and then click Save Changes to commit the changes.
6. Restart the HDFS service.

Categories: Configuring (../categories/hub_configuring.html) | HDFS (../categories/hub_hdfs.html) | MapReduce (../categories/hub_mapreduce.html) | SSL (../categories/hub_ssl.html) | Security (../categories/hub_security.html) | TLS (../categories/hub_tls.html) | YARN (../categories/hub_yarn.html) | All Categories (../categories/hub.html)

- About Cloudera (https://www.cloud
- Resources (https://www.cloudera.c
- Contact (https://www.cloudera.com/contact-us.html)
- Careers (https://www.cloudera.com/about-cloudera/careers.html)

- Press (https://www.cloudera.com/about-cloudera/press-center.html)
- Documentation (https://www.cloudera.com/documentation.html)

United States: +1 888 789 1488
Outside the US: +1 650 362 0488

- (https://www.linkedin.com/company/cloudera)
- (https://www.facebook.com/cloudera)
- (https://twitter.com/cloudera)
- (https://www.cloudera.com/contact-us.html)

Page generated April 26, 2020.