

## mod18\_ex03: Verify Kerberos and SASL

The purpose of this exercise is to review Kerberos properties and to verify Simple Authentication and Security Layer (SASL). SASL is a security protocol for Java. It manages the level of security between JRE's. The Cloudera Manager's Kerberos wizard automatically configures SASL.

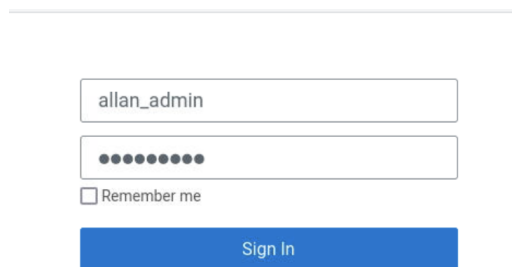
### Reference Information

The following documents provide information related to this exercise.

- [Encrypting](#)

1. Login to Cloudera Manager as the administrative user, allan\_admin.

1.1 Login into Cloudera Manager as the administrative user, allan\_admin, with password <password>.



allan\_admin

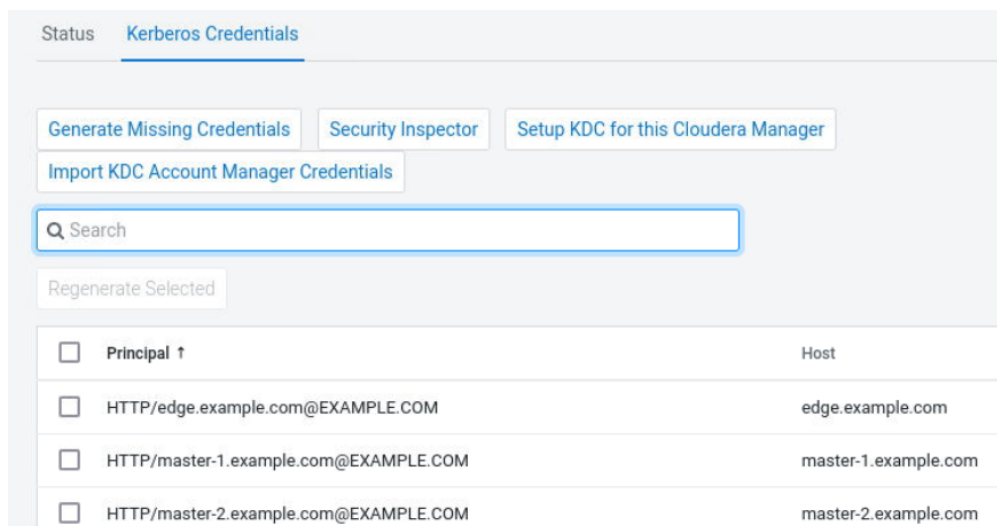
••••••••

☐ Remember me

Sign In

2. Review Kerberos properties.

2.1 On Cloudera Manager Home select Administration select Security. Select Kerberos Credentials.



Status **Kerberos Credentials**

Generate Missing Credentials Security Inspector Setup KDC for this Cloudera Manager

Import KDC Account Manager Credentials

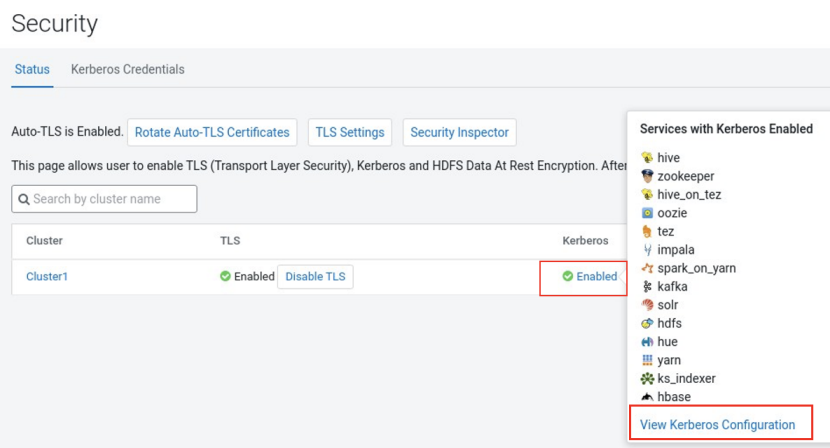
Q Search

Regenerate Selected

<input type="checkbox"/> Principal ↑	Host
<input type="checkbox"/> HTTP/edge.example.com@EXAMPLE.COM	edge.example.com
<input type="checkbox"/> HTTP/master-1.example.com@EXAMPLE.COM	master-1.example.com
<input type="checkbox"/> HTTP/master-2.example.com@EXAMPLE.COM	master-2.example.com

This page is used to managed Kerberos credentials. You can generate missing credentials, i.e. keytabs, or even regenerate current credentials.

2.2 Select the Status tab. Select Enabled to list Kerberos enabled components.



Security

Status **Kerberos Credentials**

Auto-TLS is Enabled. Rotate Auto-TLS Certificates TLS Settings Security Inspector

This page allows user to enable TLS (Transport Layer Security), Kerberos and HDFS Data At Rest Encryption. After

Q Search by cluster name

Cluster	TLS	Kerberos
Cluster1	Enabled Disable TLS	Enabled

Services with Kerberos Enabled

- hive
- zookeeper
- hive\_on\_tez
- oozie
- tez
- impala
- spark\_on\_yarn
- kafka
- solr
- hdfs
- hue
- yarn
- ks\_indexer
- hbase

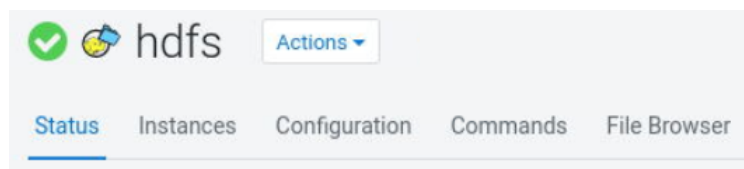
View Kerberos Configuration

## 2.3 Click View Kerberos Configuration. Review Kerberos properties.

Kerberos Configuration for Cluster1

<b>HBase Secure Authentication</b> hbase.security.authentication <a href="#">hbase_security_authentication</a>	hbase (Service-Wide) <a href="#">↗</a> <input type="radio"/> simple <input checked="" type="radio"/> kerberos
<b>HBase Secure Authorization</b> hbase.security.authorization <a href="#">hbase_security_authorization</a>	<input checked="" type="checkbox"/> hbase (Service-Wide) <a href="#">↗</a>
<b>HBase Thrift Authentication</b> hbase.thrift.security.qop <a href="#">hbase_thriftserver_security_authentication</a>	hbase (Service-Wide) <a href="#">↗</a> <input type="radio"/> none <input type="radio"/> auth <input type="radio"/> auth-int <input checked="" type="radio"/> auth-conf
DataNode Transceiver Port	DataNode Default Group

## 2.4 On Cloudera Manager Home select hdfs. Select Configuration.



## 2.5 Search data transfer. This will list the algorithm and key strength settings. Scroll to find Data Transfer Encryption Algorithm. The Kerberos wizard automatically configured these properties.

<b>Data Transfer Encryption Algorithm</b> dfs.encrypt.data.transfer.algorithm <a href="#">dfs_encrypt_data_transfer_algorithm</a>	hdfs (Service-Wide) <a href="#">↗</a> <input type="radio"/> 3des <input type="radio"/> rc4 <input checked="" type="radio"/> AES/CTR/NoPadding	<a href="#">ⓘ</a>
<b>Data Transfer Cipher Suite Key Strength</b> dfs.encrypt.data.transfer.cipher.key.bitlength <a href="#">dfs_encrypt_data_transfer_cipher_keybits</a>	hdfs (Service-Wide) <input type="radio"/> 128 <input type="radio"/> 192 <input checked="" type="radio"/> 256	<a href="#">ⓘ</a>

2.6 The recommended practice is to NOT change port numbers. However, this may be a source of error. In Filters select DataNode. Search ports. Find the the value of the DataNode Transceiver Port (dfs.datanode.address) property and the DataNode HTTP Web UI Port (dfs.datanode.http.address) property.

Filters (2) Clear All

SCOPE Clear

- hdfs (Service-Wide) 1
- Balancer 0
- DataNode** 6
- Gateway 0
- HttpFS 2
- JournalNode 4
- NFS Gateway 5
- NameNode 5
- SecondaryNameNode 3
- Fallover Controller 0

CATEGORY Clear

- Advanced 15
- Checkpointing 0
- Cloudera Navigator 0
- Erasure Coding 3
- High Availability 0
- Logs 4
- Main 3
- Monitoring 30
- Performance 11
- Ports and Addresses** 6
- Proxy 0
- Replication 0
- Resource Management 7
- Security 1
- Stacks Collection 5

Bind DataNode to Wildcard Address ☐ DataNode Default Group [Show All Descriptions](#)

[dfs.datanode\\_bind\\_wildcard](#)

Use DataNode Hostname ☐ DataNode Default Group

[dfs.datanode\\_use\\_datanode\\_hostname](#)

[dfs.datanode\\_use\\_datanode\\_hostname](#)

DataNode Protocol Port DataNode Default Group

[dfs.datanode\\_ipc\\_address](#) 9867

[dfs.datanode\\_ipc\\_port](#)

DataNode Transceiver Port DataNode Default Group

[dfs.datanode\\_address](#) 9866

[dfs.datanode\\_port](#)

DataNode HTTP Web UI Port DataNode Default Group

[dfs.datanode\\_http\\_address](#) 9864

[dfs.datanode\\_http\\_port](#)

Secure DataNode Web UI Port (TLS/SSL) DataNode Default Group

[dfs.datanode\\_https\\_address](#) 9865

[dfs.datanode\\_https\\_port](#)

1 - 6 of 6

### 3. Verify SASL configurations.

3.1 In Filters click clear all. Search for 'protection'. Review the properties for DataNode Data Transfer and for Hadoop RPC. Both SASL properties are automatically configured by the Kerberos wizard.

hdfs [Actions](#) Jul 12, 10:31 AM PDT

Status Instances **Configuration** Commands File Browser Charts Library Cache Statistics Audits Web UI Quick Links

Q protection [Filters](#) [Role Groups](#) [History & Rollback](#)

Filters

SCOPE Clear

- hdfs (Service-Wide) 3
- Balancer 0
- DataNode 0
- Gateway 0
- HttpFS 0
- JournalNode 0
- NFS Gateway 0
- NameNode 0
- SecondaryNameNode 0
- Fallover Controller 0

CATEGORY Clear

- Advanced 0
- Checkpointing 0
- Cloudera Navigator 0
- Erasure Coding 0
- High Availability 0
- Logs 0
- Main 0
- Monitoring 0
- Performance 0
- Ports and Addresses 0
- Proxy 0
- Replication 0
- Resource Management 0
- Security** 3
- Stacks Collection 0

STATUS

- Error 0
- Warning 0

DataNode Data Transfer Protection hdfs (Service-Wide) [Show All Descriptions](#)

☐ Authentication

☐ Integrity

☒ Privacy

SASL protection mode for secured connections to the DataNodes when reading or writing data. Value is the type of SASL protection to be used for secured connections to the DataNode when reading or writing block data. Possible values are 'authentication', 'integrity' and 'privacy'. **authentication** means authentication only and no integrity or privacy; **integrity** implies that only authentication and integrity are enabled; and **privacy** implies all of authentication, integrity and privacy are enabled. If 'Enable Data Transfer Encryption' is set to true, then it supersedes the setting for this parameter and enforces that all connections must use a specialized encrypted SASL handshake. This property is ignored for connections to a DataNode listening on a privileged port. In this case, it is assumed that the use of a privileged port establishes sufficient trust.

Hadoop RPC Protection hdfs (Service-Wide) [Show All Descriptions](#)

☐ authentication

☐ integrity

☒ privacy

Quality of protection for secured RPC connections between NameNode and HDFS clients. For effective RPC protection, enable Kerberos authentication.

Enable Data Transfer Encryption ☒ hdfs (Service-Wide) [Show All Descriptions](#)

[dfs.encrypt\\_data\\_transfer](#)

[dfs\\_encrypt\\_data\\_transfer](#)

Enable encryption of data transfer between DataNodes and clients, and among DataNodes. When enabled, block data that is read/written from/to HDFS will be encrypted on the wire. For effective data transfer protection, enable Kerberos authentication and pick privacy for "Hadoop RPC Protection".

SASL defines three levels of security as Quality of Protection (QoP). The three levels are Authentication, Integrity, and Privacy. Privacy is the highest level of QoP.

4. Return to Cloudera Manager Home.