

|  |  |
| --- | --- |
| **Doc Title:** | **DATA LAKE Minimum Security Verification Checklist** |
| **Doc ID:** |  |
| **Version:** | **1.0** |
| **Process Category:** | **Information Security Management** |

Table of Contents

[1 Security Verification Checklist 3](#_Toc513195820)

[1.1 Purpose: 3](#_Toc513195821)

[1.2 Scope: 3](#_Toc513195822)

[1.3 Pre-requisites: 3](#_Toc513195823)

[2 Prerequisites 3](#_Toc513195824)

[3 Minimum Security Verification Checklist 4](#_Toc513195825)

[4 Document History 14](#_Toc513195826)

[4.1 Superseded Document(s) 14](#_Toc513195827)

[4.2 Revision History 14](#_Toc513195828)

# Security Verification Checklist

## Purpose:

The purpose of this checklist is to ensure that the minimum Data Lake Security Configurations are implemented and verified on all the Data Lake environments.

## **Scope:**

The scope of this checklist is to provide instruction for the Johnson and Johnson Technology (JJT) EDL Administrators whose responsibility is to verify and document the minimum Data Lake security configurations across all JJT, managed Data Lake systems.

## Pre-requisites:

The JJT EDL Administrator who is responsible for executing this checklist must have the following accesses on the JJT managed Data Lake environments:

* Cloudera Manager UI access for the JJT managed Data Lake environments
* Linux server access on the JJT managed Data Lake Linux servers.

# Prerequisites

|  |  |  |
| --- | --- | --- |
| **Step** | **Tasks** | **Completed** |
|  | Identify the target Data Lake Environment.  DEV |  |
|  | Executor has access on the Cloudera Manager UI. |  |
|  | Executor has access to the Data Lake Linux servers.  (Note that all the Linux commands must be executed on all the Data Lake Nodes) |  |

|  |
| --- |
| **Steps 1 to 3 Completed**  Comments: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Completed by (initials):\_\_\_\_\_ABM\_\_\_\_\_ Date: 17- April – 2019 (dd-mmm-yyyy) |

# Minimum Security Verification Checklist

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Step** | **Service** | **Step Instructions** | **Expected Results** | **Pass/ Fail** | **Initials/Date** |
|
| 1 | Cloudera Manager | 1.Logon to the Cloudera Manager with username & password | External Authentication Type should be **LDAP** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Cloudera Management Services->Configuration->Type **'External Authentication Type'** in search box |
| 2 | Cloudera Manager | 1.Logon to the Cloudera Manager with username & password | LDAP URL used should be (**ldaps://jnj.com:3269**). | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Cloudera Management Services->Configuration->Type **'LDAP URL**' in search box |
| 3 | Cloudera Manager | 1.Logon to the Cloudera Manager with username & password | LDAP Bind User Distinguished Name should be [**Respective Service Account**] | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Cloudera Management Services->Configuration->Type **'LDAP Bind User Distinguished Name**' in search box |
| 4 | Cloudera Manager | 1.Logon to the Cloudera Manager with username & password | Encryption for Admin Console is **enabled**. | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Administration->Settings->Search for **'TLS Encryption for Admin Console** ' in search box |
| 5 | Cloudera Manager | 1.Logon to the Cloudera Manager with username & password | TLS Encryption for Agents is **enabled**. | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Administration->Settings->Search for **'TLS Encryption for Agents** ' in search box |
| 6 | Cloudera Manager | 1.Logon to the Cloudera Manager with username & password | TLS Authentication of Agents to Server is **enabled**. | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Administration->Settings->Search for **'TLS Authentication of Agents to Server** ' in search box |
| 7 | Cloudera Manager | 1.Logon to the Cloudera Manager with username & password | Path to TLS Keystore File should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Administration->Settings->Search for '**Cloudera Manager TLS/SSL Server JKS Keystore File Location** ' in search box | **/opt/cloudera/security/jks/server\_chrome01.keystore**  **or**  **/opt/cloudera/security/jks/server.keystore** |  |  |
| 8 | Cloudera Manager | 1.Logon to the Cloudera Manager with username & password | Path to TLS Keystore File should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Administration->Settings->Search for **'Cloudera Manager TLS/SSL Certificate Trust Store File**' in search box | **/opt/cloudera/security/jks/truststore.jks** |  |  |
| 9 | Cloudera Manager | 1.Login to the Linux server on which Cloudera Manager is hosted, using username & password  2.Run the following command  **ls -lrt /opt/cloudera/security/jks/server\_chrome01.keystore**  **or**  **ls -lrt**  **/opt/cloudera/security/jks/server.keystore** | File should be present with read access to all or more restricted | Pass  Fail  N/A | ABM\_04/17/2019 |
| **/opt/cloudera/security/jks/server\_chrome01.keystore**  **Or**  **/opt/cloudera/security/jks/server.keystore** |  |  |
|  |  |  |
|  |  |  |
| 10 | Cloudera Manager | 1.Login to the Linux server on which Cloudera Manager is hosted, using username & password  2.Run the following command  **ls -lrt /opt/cloudera/security/jks/truststore.jks** | The file should be | Pass  Fail  N/A |  |
| **/opt/cloudera/security/jks/truststore.jks** present with read access for all or more restricted |  |  |
|  |  | ABM\_04/17/2019 |
|  |  |  |
| 11 | HBase | 1.Logon to the Cloudera Manager with username & password | Web UI SSL Encryption Enabled should be **enabled** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->HBASE->Configuration->Search for **'hbase.ssl.enabled'** in search box |
| 12 | HBase | 1.Logon to the Cloudera Manager with username & password | Path to HBase TLS/SSL Server JKS Keystore File should be | Pass  Fail  N/A |  |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->HBASE->Configuration->Search for **'ssl.server.keystore.location'** in search box | **/opt/cloudera/security/jks/hbase.keystore** |  | ABM\_04/17/2019 |
| 13 | HBase | 1.Login to all the Linux server on which Hbase is hosted, using username & password  2.Run the following command  **ls -lrt /opt/cloudera/security/jks/hbase.keystore** | The file should be |  |  |
| **/opt/cloudera/security/jks/hbase.keystore** present with read access for all or more restricted | Pass  Fail  N/A | ABM\_04/17/2019 |
|  |  |  |
|  |  |  |
| 14 | HDFS | 1.Logon to the Cloudera Manager with username & password | Hadoop SSL should be **enabled** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->HDFS->Configuration->Search for **'hadoop.ssl.enabled'** in search box |
| 15 | HDFS | 1.Logon to the Cloudera Manager with username & password | Path to Hadoop TLS/SSL Server Keystore File should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->HDFS->Configuration->Search for **'ssl.server.keystore.location'** in search box | **/opt/cloudera/security/jks/hdfs.keystore** |  |  |
| 16 | HDFS | 1.Logon to the Cloudera Manager with username & password | Path to Cluster-Wide Default TLS/SSL Client Truststore Location should be | Pass  Fail  N/A |  |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->HDFS->Configuration->Search for **'ssl.client.truststore.location'** in search box | **/opt/cloudera/security/jks/truststore.jks** |  | ABM\_04/17/2019 |
| 17 | HDFS | 1.Logon to the Cloudera Manager with username & password | Path to HttpFS TLS/SSL Server JKS Keystore File should be | Pass  Fail  N/A |  |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->HDFS->Configuration->Search for **'HttpFS TLS/SSL Server JKS Keystore File Location'** in search box | **/opt/cloudera/security/jks/httpfs.keystore** |  | ABM\_04/17/2019 |
| 18 | HDFS | 1.Login to all the Linux server on which HDFS is hosted, using username & password  2.Run the following command  **ls -lrt /opt/cloudera/security/jks/hdfs.keystore** | The file should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| **/opt/cloudera/security/jks/hdfs.keystore** present with **read access for all or more restricted** |  |  |
|  |  |  |
|  |  |  |
| 19 | HDFS | 1.Login to all the Linux server on which HDFS is hosted, using username & password  2.Run the following command  **ls -lrt /opt/cloudera/security/jks/httpfs.keystore** | The file should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| **/opt/cloudera/security/jks/httpfs.keystore** present with read access for all or more restricted |  |  |
|  |  |  |
|  |  |  |
| 20 | Hive | 1.Logon to the Cloudera Manager with username & password | Enable LDAP Authentication should be **set** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Hive->Configuration->Search for **'Enable LDAP Authentication'** in search box |
| 21 | Hive | 1.Logon to the Cloudera Manager with username & password | LDAP URL used should be **(ldaps://jnj.com:3269).** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Hive->Configuration->Search for **'LDAP URL'** in search box |
| 22 | Hue | 1.Logon to the Cloudera Manager with username & password | Enable TLS/SSL for Hue property should be **set** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->HUE->Configuration->Search for **'Enable TLS/SSL** ' in search box |
| 23 | Hue | 1.Logon to the Cloudera Manager with username & password | Path to Hue TLS/SSL Server Certificate file should be | Pass  Fail  N/A |  |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->HUE->Configuration->Search for **'ssl\_certificate'** in search box | **/opt/cloudera/security/x509/hueserver\_chrome01.cert**  **OR**  **/opt/cloudera/security/x509/hueserver.cert** |  | ABM\_04/17/2019 |
| 24 | Hue | 1.Logon to the Cloudera Manager with username & password | Path to Hue TLS/SSL Server Private Key File should be | Pass  Fail  N/A |  |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->HUE->Configuration->Search for **'ssl\_private\_key '** in search box | **/opt/cloudera/security/x509/hueserver\_chrome01.key**  **OR**  **/opt/cloudera/security/x509/hueserver.key** |  | ABM\_04/17/2019 |
| 25 | Hue | 1.Logon to the Cloudera Manager with username & password | Path to Hue TLS/SSL Server CA Certificate should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters-> JnJ\_EDL\_NewDEVCluster HUE->Configuration->Search for **'ssl\_cacerts'** in search box | **/opt/cloudera/security/CAcerts/combinedtrust\_chrome01.pem**  **OR** |  |  |
|  | **/opt/cloudera/security/CAcerts/combinedtrust.pem**  **OR**  **/opt/cloudera/security/CAcerts/combinedtrust\_chrome.pem** |  |  |
| 26 | Hue | 1.Logon to the Cloudera Manager with username & password | Path to Hue Load Balancer TLS/SSL Server Certificate File should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->HUE->Configuration->Search for **'SSLCertificateFile'** in search box | **/opt/cloudera/security/x509/hueloadbalancer\_chrome01.cert**  **OR**  **/opt/cloudera/security/x509/hueloadbalancer.cert** |  |  |
| 27 | Hue | 1.Logon to the Cloudera Manager with username & password | Path to Hue Load Balancer TLS/SSL Server Private Key File should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->HUE->Configuration->Search for '**SSLCertificateKeyFile**' in search box | **/opt/cloudera/security/x509/hueloadbalancer\_chrome01.key**  **OR**  **/opt/cloudera/security/x509/hueloadbalancer.key** |  |  |
| 28 | Hue | 1.Logon to the Cloudera Manager with username & password  2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->HUE->Configuration->Search for **'Hue Service Advanced Configuration Snippet (Safety Valve) for hue\_safety\_valve.ini**' in search box | Its value should be:  [desktop]  [[ldap]]  ignore\_username\_case=true  force\_username\_lowercase=true  [impala]  close\_queries=true  [beeswax]  close\_queries=true  auth\_username=\*\*\*\*\*\*\*  auth\_password=\*\*\*\*  Note: The auth\_username and password will be as per the environment. | Pass  Fail  N/A | ABM\_04/17/2019 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |  |
| 29 | Hue | 1.Logon to the Cloudera Manager with username & password | Its value should be set to **desktop.auth.backend.LdapBackend** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->HUE->Configuration->Search for **'Authentication Backend'** in search box |
| 30 | Hue | 1.Logon to the Cloudera Manager with username & password | LDAP URL should be **ldap://jnj.com:3268** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->HUE->Configuration->Search for **'ldap\_url'** in search box |
| 31 | Hue | 1.Logon to the Cloudera Manager with username & password | Use Search Bind Authentication should be **enabled** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->HUE->Configuration->Search for **'Use Search Bind Authentication** ' in search box |
| 32 | Hue | 1.Logon to the Cloudera Manager with username & password | Use StartTLS should be **set** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->HUE->Configuration->Search for **'Use StartTLS '** in search box |
| 33 | Hue | 1.Logon to the Cloudera Manager with username & password | LDAP Search Base should be |  |  |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->HUE->Configuration->Search for **'base\_dn'** in search box | **dc=JNJ,dc=COM** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 34 | Hue | 1.Logon to the Cloudera Manager with username & password | LDAP Bind User should be **[Service Account]** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->HUE->Configuration->Search for **'LDAP Bind User Distinguished Name**' in search box |
| 35 | Hue | 1.Login to all the Linux server on which HUE is hosted, using username & password  2.Run the following command  **ls -lrt /opt/cloudera/security/x509/hueserver\_chrome01.cert**  **OR**  **ls -lrt**  **/opt/cloudera/security/x509/hueserver.cert** | The file should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| **/opt/cloudera/security/x509/hueserver\_chrome01.cert**  or  **/opt/cloudera/security/x509/hueserver.cert**  should be present with **read access for all or more restricted** |  |  |
|  |  |  |
|  |  |  |
| 36 | Hue | 1.Login to all the Linux server on which HUE is hosted, using username & password  2.Run the following command  **ls -lrt /opt/cloudera/security/x509/hueserver\_chrome01.key**  **OR**  **ls -lrt /opt/cloudera/security/x509/hueserver.key** | The file should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| **/opt/cloudera/security/x509/hueserver\_chrome01.key**  or **/opt/cloudera/security/x509/hueserver.key**  should be present with **read access for all or more restricted** |  |  |
|  |  |  |
|  |  |  |
| 37 | Hue | 1.Login to all the Linux server on which HUE is hosted, using username & password  2.Run the following command  **ls -lrt /opt/cloudera/security/CAcerts/combinedtrust\_chrome01.pem**  **OR**  **ls -lrt /opt/cloudera/security/CAcerts/combinedtrust.pem**  **OR**  **ls -lrt /opt/cloudera/security/CAcerts/combinedtrust\_chrome.pem** | The file should be | Pass  Fail  N/A |  |
| **/opt/cloudera/security/CAcerts/combinedtrust\_chrome01.pem**  **OR**  **/opt/cloudera/security/CAcerts/combinedtrust.pem**  OR  **/opt/cloudera/security/CAcerts/combinedtrust\_chrome.pem**  Should be present with read access for all or more restricted |  | ABM\_04/17/2019 |
|  |  |  |
|  |  |  |
| 38 |  | 1.Login to Hue load balancer linux server  2.Run the following command  **ls -lrt /opt/cloudera/security/x509/hueloadbalancer\_chrome01.cert**  **OR**  **ls -lrt /opt/cloudera/security/x509/hueloadbalancer.cert** | The file should be | Pass  Fail  N/A |  |
| **/opt/cloudera/security/x509/hueloadbalancer\_chrome01.cert**  OR  **/opt/cloudera/security/x509/hueloadbalancer.cert**  Should be present with **read access for all or more restricted** |  | ABM\_04/17/2019 |
|  |  |  |
|  |  |  |
| 39 | Hue | 1.Login to all the Linux server where HUE loadbalancer is hosted, using username & password  2.Run the following command  **ls -lrt /opt/cloudera/security/x509/hueloadbalancer\_chrome01.key**  **OR**  **/opt/cloudera/security/x509/hueloadbalancer.key** | The file should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| **/opt/cloudera/security/x509/hueloadbalancer\_chrome01.key**  OR  **/opt/cloudera/security/x509/hueloadbalancer.key**  Should be present with **read access for all or more restricted** |  |  |
|  |  |  |
|  |  |  |
| 40 | Impala | 1.Logon to the Cloudera Manager with username & password | Enable LDAP Authentication should be **set**. | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Impala->Configuration->Search for **'Enable LDAP Authentication'** in search box |
| 41 | Impala | 1.Logon to the Cloudera Manager with username & password | **ldap://jnj.com:3268** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Impala->Configuration->Search for **'LDAP URL'** in search box |
| 42 | Impala | 1.Logon to the Cloudera Manager with username & password | Enable LDAP TLS should be **set** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Impala->Configuration->Search for **'ldap\_tls'** in search box |
| 43 | Impala | 1.Logon to the Cloudera Manager with username & password | SSL/TLS should have been **enabled** for Impala | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Impala->Configuration->Search for '**Enable TLS/SSL for Impala'** in search box |
| 44 | Impala | 1.Logon to the Cloudera Manager with username & password | Path to Impala TLS/SSL Server Certificate File should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Impala->Configuration->Search for **'ssl\_server\_certificate'** in search box | **/opt/cloudera/security/x509/impala.cert** |  |  |
| 45 | Impala | 1.Logon to the Cloudera Manager with username & password | Path to Impala TLS/SSL Server Private Key File should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Impala->Configuration->Search for **'ssl\_private\_key'** in search box | **/opt/cloudera/security/x509/impala.key** |  |  |
| 46 | Impala | 1.Logon to the Cloudera Manager with username & password | It should be set to **ITSUSRAJNJDC56.jnj.com** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Impala->Configuration->Search for **'ldap\_domain'** in search box |
| 47 | Impala | 1.Logon to the Cloudera Manager with username & password | Path to Impala Daemon Webserver TLS/SSL Server Certificate File should be | Pass  Fail  N/A |  |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Impala->Configuration->Search for **'Impala Daemon Webserver TLS/SSL Server Certificate File'** in search box | **/opt/cloudera/security/x509/impalacombined.cert** |  | ABM\_04/17/2019 |
| 48 | Impala | 1.Login to all the Linux server where Impala is hosted, using username & password    2.Run the following command  **ls -lrt /opt/cloudera/security/x509/impala.cert** | The file should be | Pass  Fail  N/A |  |
| **/opt/cloudera/security/x509/impala.cert** present with read access for all or more restricted |  |  |
|  |  | ABM\_04/17/2019 |
|  |  |  |
|  |  |  |
| 49 | Impala | 1.Login to all the Linux server where Impala is hosted, using username & password  2.Run the following command  **ls -lrt /opt/cloudera/security/x509/impala.key** | The file should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| **/opt/cloudera/security/x509/impala.key** present with **read access for all or more restricted** |  |  |
|  |  |  |
|  |  |  |
| 50 | Impala | 1.Login to all the Linux server where Impala is hosted, using username & password  2.Run the following command  **ls -lrt /opt/cloudera/security/x509/impalacombined.cert** | The file should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| **/opt/cloudera/security/x509/impalacombined.cert** present with read access for all or more restricted |  |  |
|  |  |  |
|  |  |  |
| 51 | Impala | 1.Login to all the Linux server where Impala is hosted, using username & password  2.Run the following command  **ls -lrt /opt/cloudera/security/jks/truststore.jks** | The file should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| **/opt/cloudera/security/jks/truststore.jks** present with read access for all or more restricted |  |  |
|  |  |  |
|  |  |  |
| 52 | Kafka | 1.Logon to the Cloudera Manager with username & password | Enable TLS/SSL for Kafka Broker should be **set to ‘true’.** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Kafka->Configuration->Search for **'Enable TLS/SSL for Kafka Broker'** in search box |
| 53 | Kafka | 1.Logon to the Cloudera Manager with username & password | Path to Kafka Broker TLS/SSL Certificate Trust Store File should be **/opt/cloudera/security/jks/server.keystore** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Kafka->Configuration->Search for **'Kafka Broker TLS/SSL Server JKS Keystore File Location '** in search box |
| 54 | Kafka | 1.Logon to the Cloudera Manager with username & password | SSL Client Authentication should be set to **‘required’**. | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Kafka->Configuration->Search for **'SSL Client Authentication'** in search box |
| 55 | Kafka | 1.Logon to the Cloudera Manager with username & password | Inter Broker Protocol should be set to **‘SASL\_SSL’.** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Kafka->Configuration->Search for **'Inter Broker Protocol '** in search box |
| 56 | Kafka | 1.Logon to the Cloudera Manager with username & password | Destination Kafka Cluster's Security Protocol should be set to **‘SASL\_SSL’.** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Kafka->Configuration->Search for **'Destination Kafka Cluster's Security Protocol'** in search box |
| 57 | Kafka | 1.Logon to the Cloudera Manager with username & password | Source Kafka Cluster's Client Auth should be **set to ‘true’.** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Kafka->Configuration->Search for **'Source Kafka Cluster's Client Auth '** in search box |
| 58 | Kafka | 1.Logon to the Cloudera Manager with username & password | Destination Kafka Cluster's Client Auth should be **set to ‘true’.** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Kafka->Configuration->Search for **'Destination Kafka Cluster's Client Auth'** in search box |
| 59 | Kafka | 1.Login to all the Linux server where Kafka is hosted, using username & password  2.Run the following command  **ls -lrt /opt/cloudera/security/jks/truststore.jks** | The file should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| **/opt/cloudera/security/jks/truststore.jks** present with read access for all or more restricted |  |  |
|  |  |  |
|  |  |  |
| 60 | KMS | 1.Logon to the Cloudera Manager with username & password | Minimum TLS support should be set to **TLSv1.** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDev\_KeyTrustee->Key Trustee Server->Configuration->Search for **'Minimum TLS Support '** in search box |
| 61 | KMS | 1.Logon to the Cloudera Manager with username & password | Active Key Trustee Server TLS/SSL Server Private Key File should be **/opt/cloudera/security/x509/server.key**. | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_ NewDev\_KeyTrustee->Key Trustee Server->Configuration->Search for **'Active Key Trustee Server TLS/SSL Server Private Key File'** in search box |
| 62 | KMS | 1.Logon to the Cloudera Manager with username & password | Active Key Trustee Server TLS/SSL Server Certificate File should be **/opt/cloudera/security/x509/server.pem**. | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_ NewDev \_KeyTrustee->Key Trustee Server->Configuration->Search for **'Active Key Trustee Server TLS/SSL Server Certificate File'** in search box |
|  |
| 63 | KMS | 1.Login to all the Linux server where KMS is hosted, using username & password  2.Run the following command  **ls -lrt /opt/cloudera/security/x509/server.key** | The file should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| **/opt/cloudera/security/x509/server.key** present with read access for all or more restricted |  |  |
|  |  |  |
|  |  |  |
| 64 | KMS | 1.Login to all the Linux server where KMS is hosted, using username & password  2.Run the following command  **ls -lrt /opt/cloudera/security/x509/server.pem** | The file should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| **/opt/cloudera/security/x509/server.pem** present with read access for all or more restricted |  |  |
|  |  |  |
|  |  |  |
| 65 | Kudu | 1.Logon to the Cloudera Manager with username & password | Enable Secure Authentication And Encryption should be **set to 'true'.** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Kudu->Configuration->Search for **'Enable Secure Authentication And Encryption'** in search box |
| 66 | Kudu | 1.Logon to the Cloudera Manager with username & password | Kerberos Principal should be **set to 'kudu' to enable Kerberos**. | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Kudu->Configuration->Search for **'Kerberos Principal '** in search box |
| 67 | Kudu | 1.Logon to the Cloudera Manager with username & password | Enable TLS/SSL for Master should be **set to 'true'.** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Kudu->Configuration->Search for **'Enable TLS/SSL for Master '** in search box |
| 68 | Kudu | 1.Logon to the Cloudera Manager with username & password | Master TLS/SSL Server Private Key File should be **/opt/cloudera/security/x509/kudu.key**. | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Kudu->Configuration->Search for **'Master TLS/SSL Server Private Key File '** in search box |
| 69 | Kudu | 1.Logon to the Cloudera Manager with username & password | Master TLS/SSL Server Certificate File should be **/opt/cloudera/security/x509/kudu.cert.** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Kudu->Configuration->Search for **'Master TLS/SSL Server Certificate File '** in search box |
| 70 | Kudu | 1.Logon to the Cloudera Manager with username & password | Master TLS/SSL Server CA Certificate should be **/opt/cloudera/security/CAcerts/combinedtrust.pem**. | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Kudu->Configuration->Search for **'Master TLS/SSL Server CA Certificate '** in search box |
| 71 | Kudu | 1.Logon to the Cloudera Manager with username & password | Tablet Server TLS/SSL Server Private Key File should be **/opt/cloudera/security/x509/kudu.key**. | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Kudu->Configuration->Search for **'Tablet Server TLS/SSL Server Private Key '** in search box |
| 72 | Kudu | 1.Logon to the Cloudera Manager with username & password | Tablet Server TLS/SSL Server Certificate File should be **/opt/cloudera/security/x509/kudu.cert**. | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Kudu->Configuration->Search for **'Tablet Server TLS/SSL Server Certificate File '** in search box |
| 73 | Kudu | 1.Logon to the Cloudera Manager with username & password | Tablet Server TLS/SSL Server CA Certificate should be **/opt/cloudera/security/CAcerts/combinedtrust.pem.** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->Kudu->Configuration->Search for **'Tablet Server TLS/SSL Server CA Certificate '** in search box |
| 74 | Kudu | 1.Login to all the Linux server where Kudu (Master & Tablet) is hosted, using username & password  2.Run the following command  **ls -lrt /opt/cloudera/security/x509/kudu.key** | The file should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| **/opt/cloudera/security/x509/kudu.key** present with read access for all or more restricted |  |  |
|  |  |  |
|  |  |  |
| 75 | Kudu | 1.Login to all the Linux server where Kudu (Master & Tablet) is hosted, using username & password | The file should be | Pass  Fail  N/A | ABM\_04/17/2019 |
|  | **/opt/cloudera/security/x509/kudu.cert** present with read access for all or more restricted |  |  |
| 2.Run the following command |  |  |  |
| **ls -lrt /opt/cloudera/security/x509/kudu.cert** |  |  |  |
| 76 | Kudu | 1.Login to all the Linux server where Kudu (Master & Tablet) is hosted, using username & password | The file should be | Pass  Fail  N/A |  |
|  | **/opt/cloudera/security/CAcerts/combinedtrust.pem** present with read access for all or more restricted |  | ABM\_04/17/2019 |
| 2.Run the following command |  |  |  |
| **ls -lrt /opt/cloudera/security/CAcerts/combinedtrust.pem** |  |  |  |
| 77 | Navigator | 1.Logon to the Cloudera Manager with username & password | External Authentication Type should be **LDAP** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Cloudera Management Services->Instances->Navigator Metadata Server->Configuration->Search for **'External Authentication Type '** in search box |
| 78 | Navigator | 1.Logon to the Cloudera Manager with username & password | Enable TLS/SSL for Navigator Metadata Server **should be set** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Cloudera Management Services->Instances->Navigator Metadata Server->Configuration->Search for **'Enable TLS/SSL for Navigator Metadata Server**' in search box |
| 79 | Navigator | 1.Logon to the Cloudera Manager with username & password | LDAP URL should be **ldaps://jnj.com:3269** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Cloudera Management Services->Instances->Navigator Metadata Server->Configuration->Search for **'LDAP URL'** in search box |
| 80 | Navigator | 1.Logon to the Cloudera Manager with username & password | LDAP Bind User Distinguished Name should be **[Respective Service Account]** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Cloudera Management Services->Instances->Navigator Metadata Server->Configuration->Search for **'LDAP Bind User Distinguished Name** ' in search box |
| 81 | Navigator | 1.Logon to the Cloudera Manager with username & password | SSL should be **enabled** | Pass  Fail  N/A | ABM\_04/17/2019 |
| 2.Navigate to Cloudera Management Services->Instances->Navigator Metadata Server->Configuration->Search for **'nav.http.enable\_ssl** ' in search box |
| 82 | Navigator | 1.Logon to the Cloudera Manager with username & password | Path to TLS/SSL Keystore File should be | Pass  Fail  N/A |  |
| 2.Navigate to Cloudera Management Services->Instances->Navigator Metadata Server->Configuration->Search for **'TLS/SSL Keystore File Location'** in search box | **/opt/cloudera/security/jks/server\_chrome01.keystore**  **OR**  **/opt/cloudera/security/jks/server.keystore** |  | ABM\_04/17/2019 |
| 83 | Navigator | 1.Login to all the Linux server where Navigator Metadata server is hosted, using username & password | The file should be | Pass  Fail  N/A | ABM\_04/17/2019 |
|  | **/opt/cloudera/security/jks/server.keystore** present with read access for all or more restricted |  |  |
| 2.Run the following command |  |  |  |
| **ls -lrt /opt/cloudera/security/jks/server.keystore** |  |  |  |
| 84 | Yarn | 1.Logon to the Cloudera Manager with username & password | Path to Hadoop TLS/SSL Server Keystore File should be | Pass  Fail  N/A |  |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->YARN->Configuration->Search for **'ssl.server.keystore.location'** in search box | **/opt/cloudera/security/jks/hdfs\_chrome01.keystore**  **OR**  **/opt/cloudera/security/jks/hdfs.keystore** |  | ABM\_04/17/2019 |
| 85 | Yarn | 1.Logon to the Cloudera Manager with username & password | Path to TLS/SSL Client Truststore File should be | Pass  Fail  N/A |  |
| 2.Navigate to Clusters->JnJ\_EDL\_NewDEVCluster->YARN->Configuration->Search for **'ssl.client.truststore.location'** in search box | **/opt/cloudera/security/jks/truststore.jks** |  | ABM\_04/17/2019 |
| 86 | Yarn | 1.Login to all the Linux server where Yarn is hosted, using username & password  2.Run the following command  **ls -lrt /opt/cloudera/security/jks/hdfs\_chrome01.keystore**  **OR**  **ls -lrt /opt/cloudera/security/jks/hdfs.keystore** | The file should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| **/opt/cloudera/security/jks/hdfs\_chrome01.keystore**  Or  **/opt/cloudera/security/jks/hdfs.keystore**  Should be present with **read access for all or more restricted** |  |  |
|  |  |  |
|  |  |  |
| 87 | Yarn | 1.Login to all the Linux server where Yarn is hosted, using username & password  2.Run the following command  **ls -lrt /opt/cloudera/security/jks/truststore.jks** | The file should be | Pass  Fail  N/A | ABM\_04/17/2019 |
| **/opt/cloudera/security/jks/truststore.jks** present with **read access for all or more restricted** |  |  |
|  |  |  |
|  |  |  |

# Document History

## Superseded Document(s)

* **Doc ID:** – [Doc ID] **Title:** – [Title] **Effective Date:** – [DD-Mmm-YYYY]

## Revision History

| **Version** | **Date** | **Originator/ Author** | **Pages** | **Change Summary** |
| --- | --- | --- | --- | --- |
| 1.0 | 17 April 2019 | Abdul Baseer Mohammed | All | Initial Version |