**sudoTest Coverage :**

1. **Tests the Big data steps in a secure cluster**
2. **To run the job HDP cluster has to be setup**

**O/S coverage**

**Ubuntu**

**Windows**

**Set up Steps:**

1. Create a VM (or use an existing one)
2. Copy down 9.0.0.0 test assets from 172.16.10.71 using scp or tool of your choice from your VM to /home/devuser on Ubuntu and C: on Windows
   1. scp -r devuser@172.16.10.71:/home/devuser/integration /home/devuser
3. Download the Pentaho build from build.pentaho.net/hosted
4. Copy the contents of /home/devuser/integrationsudo/resources/.kettle/kettle-ubuntu.properties or .kettle-windows.properties to the end of the kettle.properties file
5. Using an editor of your choice, edit kettle.properties file and validate the paths to the following variables.

NOTE: you will not need to change the paths if you’ve downloaded test asset library to the recommended location.

ora\_sqlldr\_path (this should be the Oracle Home path)

regression\_baseline\_path (this should be the path 9.0.0.0/baselines)

regression\_output\_path (this should be the path 9.0.0.0/output)

regression\_data\_path (this should be the path 9.0.0.0/data)

regression\_hadoop\_input (this should be path for home/Mandalorian/wordcount/input)

regression\_hadoop\_output (the path for home/Mandalorian/output/result\_output)

1. **Kerberos connection on UBUNTU for HDP31secure**

<http://iwiki.pentaho.com/display/QA/Big+Data+Test+Cluster+Connection+Info>

1. Set up your machine to use Kerberos commands on Ubuntu
   1. sudo apt install -y krb5-user libpam-krb5 libpam-ccreds auth-client-config
   2. sudo dpkg-reconfigure krb5-config
   3. Note: This step should prompt you about a KDC.
      1. Any references to a "realm" should be set to "PENTAHO.NET"
      2. Any references to a "hostname or KDC" should be "[hdp31secn1.pentaho.net](http://hdp31secn1.pentaho.net:8080)"( or latest working one)
      3. Administrative server for your Kerberos realm [devuser@PENTAHO.NET](mailto:devuser@PENTAHO.NET)
2. Open a terminal and navigate to the /etc folder and execute the following command : sudo scp [devuser@10.177.178.159:/etc/krb5.conf ./krb5.conf](mailto:devuser@10.177.177.122:/etc/krb5.conf%20./krb5.conf)
3. Enter the password for the VM eg:password
4. Enter the password for the HDP31 system we are connecting (to password is password) [devuser@10.177.178.159](mailto:devuser@10.177.178.159) password:
5. You will get the following message on the terminal  
   krb5.conf 100% 683 448.4KB/s 00:00
6. On the same terminal enter the following command  
   kinit [devuser@PENTAHO.NET](mailto:devuser@PENTAHO.NET)  
   Password for [devuser@PENTAHO](mailto:devuser@PENTAHO).NET: (password)
7. On the same terminal enter the following command /etc$ klist cp

On the console following message displays :

Ticket cache: FILE:/tmp/krb5cc\_1000

Default principal: devuser@PENTAHO.NET

Valid starting Expires Service principal

03/23/2020 15:16:06 03/24/2020 15:16:06 krbtgt/PENTAHO.NET@PENTAHO.NET

1. copy the krb5.conf to Pentaho/java/lib/security folder eg: $ cp krb5.conf /home/devuser/Pentaho/java/lib/security/
2. Restart spoon

**Kerberos connection on UBUNTU for CDH62secure**

<http://iwiki.pentaho.com/display/QA/Big+Data+Test+Cluster+Connection+Info>

1. Set up your machine to use Kerberos commands on Ubuntu
   1. sudo apt install -y krb5-user libpam-krb5 libpam-ccreds auth-client-config
   2. sudo dpkg-reconfigure krb5-config
   3. Note: This step should prompt you about a KDC.
      1. Any references to a "realm" should be set to "PENTAHO.NET"
      2. Any references to a "hostname or KDC" should be [cdh62secn1.pentaho.net](https://svqxobcdh61secn1.pentaho.net:7183/cmf/login) (or latest working one)
      3. Administrative server for your Kerberos realm [devuser@PENTAHO.NET](mailto:devuser@PENTAHO.NET)
2. Open a terminal and navigate to the /etc folder and execute the following command : sudo scp [devuser@172.16.10.11:/etc/krb5.conf ./krb5.conf](mailto:devuser@172.16.10.11:/etc/krb5.conf%20./krb5.conf)
3. Enter the password for the VM eg : password
4. Enter the password for the cdh62 system we are connecting (to password is password) [devuser@172.16.10.11](mailto:devuser@172.16.10.11) password:
5. You will get the following message on the terminal  
   krb5.conf 100% 683 448.4KB/s 00:00
6. On the same terminal enter the following command  
   kinit [devuser@PENTAHO.NET](mailto:devuser@PENTAHO.NET)  
   Password for [devuser@PENTAHO](mailto:devuser@PENTAHO).NET: (password)
7. On the same terminal enter the following command /etc$ klist

On the console following message displays :

Ticket cache: FILE:/tmp/krb5cc\_1000

Default principal: devuser@PENTAHO.NET

Valid starting Expires Service principal

03/23/2020 15:16:06 03/24/2020 15:16:06 krbtgt/PENTAHO.NET@PENTAHO.NET

1. copy the krb5.conf to Pentaho/java/lib/security folder eg: $ cp krb5.conf /home/devuser/Pentaho/java/lib/security/
2. Restart spoon

**MongoDB SSL connection Setup On WINDOWS**

1. Download pscp <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>
2. From your command prompt run the below command (this will copy the certificate file to your local system in the current folder):  
   **pscp devuser@10.177.177.125:/etc/ssl/mongodb-cert.crt .**   
   If prompted for password, enter pentaho06 or verify the test database link for the correct password.
3. Edit the C:\Windows\System32\drivers\etc\hosts file and include the mapping of ip address to host names. (this may vary depending upon the MongoDB version you are testing)   
   eg: #MongoSSL   
   **10.177.177.125 svqxbdcn6mongodb32ssln1.pentahoqa.com svqxbdcn6mongodb32ssln1**
4. Install java on the your machine or JAVA gets installed if your ran the installer on your machine, navigate to Pentaho/java/bin folder - and make sure the keytool app is present
5. Launch command prompt with administrator privileges and goto to /Pentaho/java/bin and run the following command
6. Run the following command :  
   keytool -import -trustcacerts -alias mongodb-cert -file <The path where you saved your mongodb-cert.crt file mongodb-cert.crt /home/devuser/mongodb-cert.crt> -keystore <Path to save the key /home/devuser/Pentaho/java/lib/security/cacerts>  
   eg:  
   **keytool -import -trustcacerts -alias mongodb-cert -file /home/devuser/mongodb-cert.crt -keystore /home/devuser/Pentaho/java/lib/security/cacerts**
7. When the above command runs it will ask for a password enter the following  
   Enter password = changeit

You will get a message Trust this certificate? [no]: enter yes

You will get the following message : Ceritificate was added to keystore

( if you have already the mongodb-cert installed on this machine if u enter the following command then you will get the keytool error message  
./keytool -import -trustcacerts -alias mongodb-cert -file /home/devuser/mongodb-cert.crt -keystore /home/devuser/Pentaho/java/lib/security/cacerts  
Enter keystore password:  
keytool error: java.lang.Exception: Certificate not imported, alias <mongodb-cert> already exists

**MongoDb kerberos connection on Windows**

1. Download and Install MIT Kerberos for Windows/64bit 4.0.1 from link: <http://web.mit.edu/kerberos/dist/kfw/4.0/kfw-4.0.1-amd64.msi>
2. Just leave the default settings and complete installation
3. Download pscp or any other program to get the configuration file from the server
4. Open a command prompt and enter the below command. The IP name will change depending on what server you are connecting to: **pscp devuser@10.177.177.122:/etc/krb5.conf .**
5. Copy the file krb5.conf to krb5.ini.
6. Move krb5.ini to C:\ProgramData\MIT\Kerberos5. This is a hidden folder. If you don't see it in Window Explorer, go to "View" menu and check on the hidden items and the folder will be displayed
7. Create a folder C:\temp. To setup environment variable, create a system variable KRB5CCNAME with value C:\temp\krb5cache. krb5cache file will be generated eventually and saved to this folder
8. Restart VM after adding the environment variable
9. Go to a command prompt and run the command:  
   **kinit** [**devuser@PENTAHOQA.COM**](mailto:devuser@PENTAHOQA.COM)
10. You will be prompted for password. Enter password as password
11. You will see that a ticket is generated for Kerberos and the krb5cache file is added to C:\temp directory
12. Copy "krb5.conf" file to C:\Pentaho\java\lib\security folder. PDI uses this file to reach to the KDC server