Cloudera Runtime 7.0.3

# Hue Troubleshooting

**Date published: 2020-07-28**
**Date modified: 2020-08-10**

## CLOUDERA

**https://docs.cloudera.com/**

# Legal Notice

# Contents

# The Hue load balancer not distributing users evenly across various Hue servers

The Hue load balancer redirects the new users to the newly added Hue servers and the existing users to the existing Hue servers on your cluster. Even though you add more Hue servers to meet the growing user base, the resources might not be utilized effectively.

### About this task

The Hue load balancer is tasked to evenly distribute users across the available Hue servers for effective resource utilization. However, due to session persistence, it does not distribute users evenly. To overcome this issue, you can refresh the cookies from Cloudera Manager.

The load balancer uses the cookie ROUTEID with a random string from your browser and is stored in the hue.conf file. This random string is used to redirect a user to the Hue server. To refresh the cookie and set a new random string every time you add a new Hue server, do the following:

### Procedure

1. Go to Cloudera Manager Clusters Hue Configuration .
2. Click Scope Load balancer and select the Hue Load Balancer Cookie Refresh checkbox.

   This refreshes the cookie value in the hue.conf file to rebalance the Hue backend connections.
3. In the Instances tab, select all the Hue services and roles, and click Action for Services Restart .

   This creates a new random string for the cookie which the load balancer can now use to evenly distribute users.

### Results

Whenever you restart the Hue server, the load balancer will redistribute users evenly based on the server load.

# Unable to authenticate users in Hue using SAML

If you have configured SAML to authenticate users, but your users are unable to log into Hue using Single Sign On (SSO), then it is possible that the RSA key format is not supported. To resolve this issue, you can use an unprotected private key and then specify the private key filename in the safety valve.

### Procedure

1. Convert the .key file to an unprotected private key file by using the following command:

```
openssl rsa -in /opt/cloudera/security/<file name>.key -out /opt/cloudera/
security/<file name_unprotected>.key
```

```
openssl rsa -in /opt/cloudera/security/hadoop-cpi-prod.key -out /opt/cloud
era/security/hadoop-cpi-prod_unprotected.key
```

2. Update the advanced configuration snippet as shown in the following example:

```
[libsaml]
xmlsec_binary=/usr/bin/xmlsec1
metadata_file=/opt/cloudera/security/saml/idp-openam-metadata.xml
key_file=/opt/cloudera/security/hadoop-cpi-prod_unprotected.key
cert_file=/opt/cloudera/security/hadoop-cpi-prod.pem
```