Managed Service - Incident Resolution

Azure

1. Lost Root Access to Azure Instance:

If you lose root access to an Azure instance, you can use the CustomScript Extension to push a Linux VM Customization Task, essentially running any bash/python code against that instance as root. This CustomScript Extension runs as the Azure Linux Agent (waagent).

As an example, to delete a corrupt sudoers file to fix sudo access:
Create delete-cdh_admin_full.sh on local desktop:

```
#!/bin/bash
rm -f /etc/sudoers.d/cdh_admin_full
ls /etc/sudoers.d/cdh_admin_full
```

In Azure portal:
Azure VM
Settings
Extensions
Add
Custom Script for Linux
Create
Upload script: delete-cdh_admin_full.sh
Commands: sh delete-cdh_admin_full.sh
OK

Click on the notification to see status.

Should only take a minute or two (has to load the custom script extension)

Reference:
https://azure.microsoft.com/en-us/blog/automate-linux-vm-customization-tasks-using-customscript-extension/
https://docs.microsoft.com/en-us/azure/virtual-machines/linux/agent-user-guide

AWS

1. Restarting AWS Worker

Host not pingable:
"--- drona-worker13.cargill.com ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 1999ms

1. Stopped roles on host
2. Put host in Maintenance Mode
3. Tried rebooting host from AWS UI
4. Check if host came back up with all it's disk mounted. Start all the Roles and remove the host from Maintenance Mode

Now these Host are AWS instance so we need AWS account to be able to get these host rebooted.

These host should be rebooted not Stopped and Started since Stop/Start causes host to start with new disk and they need to be formated then.

Cloudera

1. In HDFS HA environment both Namenode are in standby mode.

We need to get rid of following tree in Zookeeper

/hadoop-ha/nameservice1/ActiveStandbyElectorLock

Capture the data from ActiveStandbyElectorLock

zkCli $ get /hadoop-ha/touk-cluster-dev/ActiveStandbyElectorLock

Option 1:

(On Kerberos System)

-> kinit -kt zookeeper.keytab zookeeper/stlprdhdoopnn01.rgare.net@RGARE.NET

-> ./zkCli.sh -server stlprdhdoopnn01

In case we have a authorization failure when trying to perform following operation
-> [zk: stlprdhdoopnn01(CONNECTED) 1] ls /hadoop-ha/nameservice1/ActiveStandbyElectorLock
Authentication is not valid : /hadoop-ha/nameservice1/ActiveStandbyElectorLock

disable ACLs (if you decide to go that route): `**Java Configuration Options for Zookeeper Server**`: `**-Dzookeeper.skipACL=yes**`. Then restart zookeeper. Once you're done, re-enable ACLs and restart again.

Option 2:

(Non kerberos system)

- Disable ACLs (if you decide to go that route): `Java Configuration Options for Zookeeper Server`: `-Dzookeeper.skipACL=yes`. Then restart zookeeper.

Or

Follow this link to create a superuser https://community.hortonworks.com/articles/29900/zookeeper-using-super digest-to-gain-full-access-to.html

Then go to CM UI, “All service” -> “hdfs1″ -> “Instances” -> “Failovercontroller (xx1)” -> “Actions” -> “Initialize Automatic Failover “. This will create a new ZNode with correct lock(of Fail over controller). Then restart the HDFS service.

2. Too many open files in system

Exception Message: j*ava.util.concurrent.ExecutionException: java.io.IOException: Cannot run program “bash”: error=23, Too many open files in system*

Command to identify Open File: *sudo lsof | awk '$4 ~ /[0-9]+[rwu -].*/{p[$1"t"$2"t"$3]=p[$1"t"$2"t"$3]+1}END{for (i in p) print p[i],i}' | sort -n | tail*

Or

for p in /proc/[0-9] ; do echo $(ls $p/fd | wc -l) $(cat $p/cmdline) ; done | sort -n | tail*

Solution proposed increase the File Handles size "*/proc/sys/fs/file-max*"

https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/5/html/Tuning_and_Optimizing_Red_Hat_Enterprise_Linux_for_Oracle_9i_and_10g_Databases/chap-Oracle_9i_and_10g_Tuning_Guide-Setting_File_Handles.html

Changes will be performed in ansible common roles default value set will be 1M if memory is less and 2M if memory is decent or good.

3. 20511 Monitor-GenericMonitor urllib2_kerberos CRITICAL GSSAPI Error: Unspecified GSS failure. Minor code may provide more information/Server not found in Kerberos database

Issue: Duplicate 'http' principals for the hosts (*This is what we suspect to be happening*)

After we had migrated JHS to Gateway Node we found Cloudera Manager Agent is not able to communicate with JHS web server. Text highlighted in red below is the error message logged in /hadooplogs/log/cloudera-scm-agent/cloudera-scm-agent.log which indicates agent is not able to monitor the web roles

Solution proposed:
1. Stop the JHS roles
2. Windows AD Administrator deletes the duplicate entries.
3. Start the JHS roles once the duplicate http principals are removed

Comments From Partner: As long as we use Centrify on our Linux servers, this will continue to happen. Centrify creates http SPNs (among others) for a host when it's deployed. Anytime you use Cloudera Manager to set up SPNs for services on a newly deployed server in AD, we'll need to delete the SPN created by centrify before you run the SPN creation in Cloudera Manager. Is Cloudera Manager not able to look for (and remove) potential duplicate SPNs when creating a new one?

4. Replication: java.lang.IllegalStateException: Cannot find host for replication job in service hive.

1) Please check the hosts on the source cluster to see if any roles are in maintenance mode. This can cause this issue.

Solution:

If any services or roles are in maintenance mode please check with the below documentation to know how to exit the maintenance mode:

https://www.cloudera.com/documentation/enterprise/latest/topics/cm_mc_maint_mode.html

2 Please also check the HOST_WHITELIST for Hive Replication Environment Advanced Configuration Snippet (Safety Valve) for the source Cluster and verify if the Meta server and the Hiveserver2 instance are part of White list.

Solution:

If not then please add the following:

Add the metaserver and the hive server2 host to the HOST_WHITELIST in the "Hive Replication Environment Advanced Configuration Snippet (Safety Valve) for the source Cluster" configuration for Hive.

CM > Hive > configuration> "Hive Replication Environment Advanced Configuration Snippet (Safety Valve) for the source Cluster"

5. Datanode Volume failure.

Issue : The DataNode has X volume failure(s)" for the node

Solution Proposed:

1. Check the replication factor in CM and Identify the missing blocks on the node(hdfs fsck -list-corruptfileblocks)
2. Check with customer for the maintenance window in order to restart the node.
3. Set the Datanode Balancing Bandwidth to value somewhere between 200MB to 300MB
    a. Check the network speed
    ethtool eth0 | egrep 'Speed|Duplex'
4. During the window, Stop roles,Decommission the data node.
5. Restart the datanode via AWS.
6. Check if all Filesystems are mounted and formatted correctly. If not, issue stop and start.
7. Kudu Tablet is present
    a. Decommission Tablet Server so that data can be replicated to other node. Check the health by following the below steps.

    b. In case of Kerberos kinit as Kudu
    c. Run following command
        i. kudu cluster ksck <MASTER_NODE>:7051
8. Stop all services on the Node where we are planning to replace or fix the disk
9. STOP/START in case of AWS or Replace the failed disk.
10. Run ansible role cluster-disk on the impacted node
11. You may need to get the node rebooted again to see the partitions using *lsblk*
12. Recommission the DataNode role instance.
13. Recommission server and roles on the nodes
14. Rebalance the cluster in HDFS
15. hdfs fsck / -delete to clear of the missing blocks if HDFS still reports missing block.
16. Verify and remove from MM

6. Hive on Spark Error: Timed out waiting for client connection (1)

Identifying the Issue:

Create HoS job:

```
beeline -u
"jdbc:hive2://edh.irco.com:10000/default;principal=hive/_HOST@C
ORP.IRCO.COM;ssl=true" -e "set hive.execution.engine=spark;
analyze table p_user_ccdqwo.employees compute statistics;"
```

Sporadically occurring errors like:

```
ERROR : Failed to execute spark task, with exception
'org.apache.hadoop.hive.ql.metadata.HiveException(Failed to
create spark
client.)'org.apache.hadoop.hive.ql.metadata.HiveException:
Failed to create spark client.
FAILED: Execution Error, return code 1 from
org.apache.hadoop.hive.ql.exec.spark.SparkTask
(state=08S01,code=1)
Closing: 0:
jdbc:hive2://edh.irco.com:10000/default;principal=hive/_HOST@CO
RP.IRCO.COM;ssl=true
Caused by: java.lang.RuntimeException:
```

```
java.util.concurrent.ExecutionException:
java.util.concurrent.TimeoutException: Timed out waiting for
client connection.
```

Note: running a similar MR job does not have the same issue.

Background:

Hive on Spark uses the YARN scheduler. When under high load, containers are not allocated to jobs immediately. When the container for the job is not allocated before a certain timeout, the HoS job fails. Looking in the YARN application log, you'll see something like:

```
2017-09-26 09:05:13,093 INFO
org.apache.hadoop.yarn.server.resourcemanager.rmcontainer.RMCon
tainerImpl: container_e36_1504280718239_23450_01_000001
Container Transitioned from NEW to RESERVED
```

And then, several minutes later, YARN allocates the container to the job, but the HoS job has already timed out.

```
2017-09-26 09:09:01,629 INFO
org.apache.hadoop.yarn.server.resourcemanager.rmcontainer.RMCon
tainerImpl: container_e36_1504280718239_23450_01_216135
Container Transitioned from NEW to ALLOCATED
...
2017-09-26 09:09:17,746 INFO
org.apache.hadoop.yarn.server.resourcemanager.rmapp.attempt.RMA
ppAttemptImpl: appattempt_1504280718239_23450_000001 State
change
 from FINAL_SAVING to FAILED
```

Ticket with Cloudera:
https://cloudera-portal.force.com/supportcase?id=5003400000yGx4sAAC

Resolution:

Add the following to the Hive Service Advanced Configuration Values configured in CM for hive-site.xml:

```
<property>
   <name>hive.spark.client.connect.timeout</name>
   <value>30000ms</value>
</property>
<property>
```

```
    <name>hive.spark.client.server.connect.timeout</name>
    <value>300000ms</value>
</property>
```

This configuration has been added to the Best Practices Template: https://docs.google.com/document/d/1J3hAC-r3jmx3Qf55zfYYZrvtJwgND4WrO3u1yl7UBh8/edit#

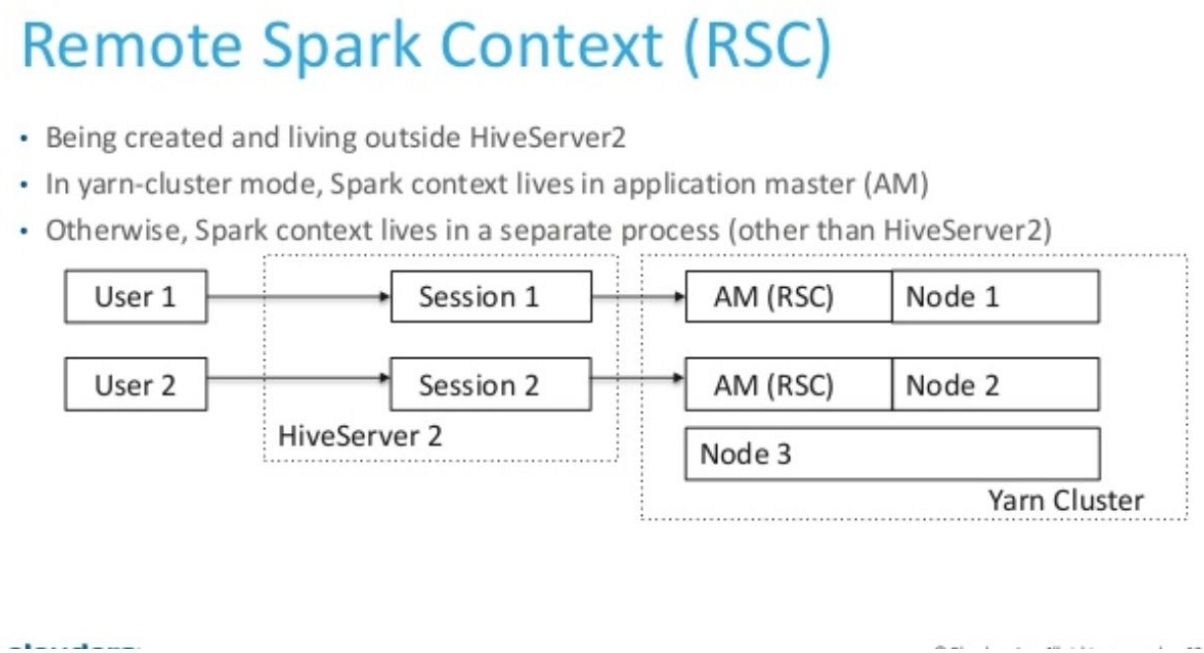
If you are still having these issues, consider bumping up the timeout.

Cloudera KB: https://cloudera-portal.force.com/articles/KB_Article/Hive-on-Spark-Jobs-Failed-With-Error-Client-closed-before-SASL-negotiation-finished?caseId=5003400000yGx4s&isCaseCreation=1&popup=true

7. Hive on Spark Error: Timed out waiting for client connection (2)

The logs you sent over are much better now that we have INFO enabled. Before debugging let's align on the architecture. Hive-on-Spark (HOS) has a few components:

* HiveServer2 (HS2) - the service which submits hive either MR, Spark, or Tez jobs
* Spark Context (SC) - effectively the "job tracker" for spark. You can only have one of these per JVM and HOS runs one per user session, thus HOS's strategy is to run the SparkContext inside the cluster, known as yarn-cluster mode. However HS2 needs some way to communicate with the SC thus there is the library discussed directly below.
* Remote Spark Context (RSC) - the library which allows HS2 to control a Spark Job running in yarn-cluster mode.
* RSC Client - runs inside the Spark Driver which due to yarn-cluster mode runs inside the YARN Application Master (AM)
* RSC Server - runs inside the HS2 daemon. The RSC Client connects from the cluster to this server so that the HS2 can start spark jobs via the RSC.



Source

Ok, now let's discuss the flow of a HOS job:

1. HS2 calls spark-submit to submit job to cluster
2. HS2 starts the RSC Server waiting for the RSC Client inside the App Master to connect back
3. Spark job inside YARN starts, starts the RSC Client, and connects back to the RSC Server inside the HS2
4. HS2 sends commands via the RSC to the Spark Context and the job starts.

So with that context in mind, here is what I see in the logs.

1. (HS2) The job **application_1530773453671_8634** was submitted by the HS2 about **2018-07-23 9:25:22** on and hive.spark.client.server.connect.timeout was 1800000ms or 30 minutes. The hive.spark.client.server.connect.timeout parameter controls how long the RSC Server will wait for a RSC Client to connect back before it assume it's died for some reason.

2018-07-23 09:25:22,958 INFO org.apache.hive.spark.client.SparkClientImpl: [HiveServer2-Handler-Pool: Thread-111572]: Running client driver with argv: /opt/cloudera /parcels/CDH-5.10.2-1.cdh5.10.2.p0.5/lib/spark/bin/spark-submit --executor-cores 3 --executor-memory 48318382080 --principal hive/email@redacted.host --keytab hive.k eytab --properties-file /tmp/spark-submit.6747162167538075860.properties --class org.apache.hive.spark.client.RemoteDriver /opt/cloudera/parcels/CDH-5.10.2-1.cdh5.10 .2.p0.5/jars/hive-exec-1.1.0-cdh5.10.2.jar --remote-host usaepapp023r1.acloud.experian.corp --remote-port 11655 --conf hive.spark.client.connect.timeout=1000 --conf **hive.spark.client.server.connect.timeout=1800000** --conf hive.spark.client.channel.log.level=null --conf hive.spark.client.rpc.max.size=52428800 --conf hive.spark.cli ent.rpc.threads=8 --conf hive.spark.client.secret.bits=256 --conf hive.spark.client.rpc.server.address=null

2. (HS2) Thirty minutes later the RSC Server HS2 times out saying the Spark application inside yarn never started and connected back to the HS2.

2018-07-23 09:55:22,963 ERROR org.apache.hive.spark.client.SparkClientImpl: [HiveServer2-Handler-Pool: Thread-111572]: Timed out waiting for client to connect.
Possible reasons include network issues, errors in remote driver or the cluster has no available resources, etc.
Please check YARN or Spark driver's logs for further information.
java.util.concurrent.ExecutionException: java.util.concurrent.TimeoutException: Timed out waiting for client connection.
...
Caused by: java.util.concurrent.TimeoutException: Timed out waiting for client connection.
at org.apache.**hive.spark.client**.rpc.**RpcServer**$2.run(RpcServer.java:141)

3. (RSC Client/Spark Driver/AM) Interestingly a few seconds later, the YARN job actually started. You can see it's trying to connect a random port on the HS2 daemon as well where the RSC Server is listening.

18/07/23 09:55:29 INFO client.RemoteDriver: Connecting to: **usaepapp023r1.acloud.experian.corp:11655**
18/07/23 09:55:30 WARN rpc.Rpc: Invalid log level null, reverting to default.
18/07/23 09:55:30 ERROR yarn.ApplicationMaster: User class threw exception:
java.util.concurrent.ExecutionException: javax.security.sasl.SaslException: Client closed
before SASL negotiation finished.
java.util.concurrent.ExecutionException: javax.security.sasl.SaslException: Client closed before SASL negotiation finished.
at io.netty.util.concurrent.AbstractFuture.get(AbstractFuture.java:37)
at org.apache.hive.spark.client.RemoteDriver.<init>(RemoteDriver.java:156)
at org.apache.hive.spark.client.RemoteDriver.main(RemoteDriver.java:556)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
at org.apache.spark.deploy.yarn.ApplicationMaster$$anon$2.run(ApplicationMaster.scala:553)
Caused by: javax.security.sasl.SaslException: Client closed before SASL negotiation finished.
at org.apache.**hive.spark.client**.rpc.Rpc$Sasl**Client**Handler.dispose(Rpc.java:454)

4. (HS2) Back inside the HS2, we can see the RSC Server complain that it doesn't know about this RSC client, because the back in step 2, the query failed.

2018-07-23 09:55:30,398 INFO org.apache.hive.spark.client.rpc.RpcServer$SaslServerHandler: [RPC-Handler-4]: Exception in SASL negotiation.
java.lang.IllegalArgumentException: Unexpected client ID '877d813e-41d0-4314-af3a-e7865897cdc9' in SASL handshake.
at com.google.common.base.Preconditions.checkArgument(Preconditions.java:115)
at org.apache.**hive.spark.client**.rpc.**RpcServer**$SaslServerHandler.update(RpcServer.java:253)

This is indicative of a cluster which has hit one of the three scenarios:

- cluster is fully utilized
- maxAMShare (or queueMaxAMShareDefault) or maxRunningApps (or queueMaxAppsDefault) on the queue has been exeeceded so no new AM's are allowed to start
- userMaxAppsDefault has been exceeded

One of the major behavior differences between Hive on MR vs HOS is that Hive on MR will wait forever for a job to be submitted while HOS cannot detect the difference between a busy cluster and a job which failed to launch.

8. Sqoop fails with java.lang.NoClassDefFoundError: org/json/JSONObject

Packages install had been deleted left around the directory /usr/lib/hive-hcatalog. Which led to the wrong home for HCAT being found:

https://github.com/cloudera/sqoop/blob/cdh5-1.4.6_5.14.4/bin/configure-sqoop#L87

Which leads to hive-exec not being in the classpath and the following error occuring.

```
Exception in thread "main" java.lang.NoClassDefFoundError: org/json/JSONObject
        at
org.apache.sqoop.util.SqoopJsonUtil.getJsonStringforMap(SqoopJsonUtil.java:42)
        at org.apache.sqoop.SqoopOptions.writeProperties(SqoopOptions.java:742)
        at
org.apache.sqoop.mapreduce.JobBase.putSqoopOptionsToConfiguration(JobBase.j
ava:369)
        at org.apache.sqoop.mapreduce.JobBase.createJob(JobBase.java:355)
        at
org.apache.sqoop.mapreduce.ImportJobBase.runImport(ImportJobBase.java:249)
        at org.apache.sqoop.manager.SqlManager.importQuery(SqlManager.java:748)
        at org.apache.sqoop.tool.ImportTool.importTable(ImportTool.java:499)
        at org.apache.sqoop.tool.ImportTool.run(ImportTool.java:605)
        at org.apache.sqoop.Sqoop.run(Sqoop.java:143)
        at org.apache.hadoop.util.ToolRunner.run(ToolRunner.java:70)
        at org.apache.sqoop.Sqoop.runSqoop(Sqoop.java:179)
        at org.apache.sqoop.Sqoop.runTool(Sqoop.java:218)
        at org.apache.sqoop.Sqoop.runTool(Sqoop.java:227)
        at org.apache.sqoop.Sqoop.main(Sqoop.java:236)
Caused by: java.lang.ClassNotFoundException: org.json.JSONObject
        at java.net.URLClassLoader$1.run(URLClassLoader.java:366)
        at java.net.URLClassLoader$1.run(URLClassLoader.java:355)
        at java.security.AccessController.doPrivileged(Native Method)
        at java.net.URLClassLoader.findClass(URLClassLoader.java:354)
        at java.lang.ClassLoader.loadClass(ClassLoader.java:425)
        at sun.misc.Launcher$AppClassLoader.loadClass(Launcher.java:308)
        at java.lang.ClassLoader.loadClass(ClassLoader.java:358)
        ... 14 more
```

9. Small File issue

Commands to identify small files:
Ensure "dfs.cluster.administrators" is configured with the proper group with a Safety Valve override: "NameNode Advanced Configuration Snippet (Safety Valve) for hdfs-site.xml"

```
hdfs dfsadmin -fetchImage fsimg
env HADOOP_OPTS="-Xmx4G $HADOOP_OPTS" hdfs oiv -i fsimg -o
fsout -p Delimited
cat fsout |cut -f1|cut -f1,2,3,4 -d'/'|sort |uniq -c|sort
-n|tail -n20
```

10. BDR/Replication setup

Be sure to restart CM after any configuration changes. Only way for them to be picked up

11. Sentry Not working

After checking all the usual suspects. If you're on 5.13.1 and it is a new build then this is a known issue with this release. Please upgrade. Applicable to BDAs too. At the same time, to confirm if issue is indeed SENTRY-2046, can you please check if AUTHZ_PATHS_SNAPSHOT_ID table in Sentry backend DB is empty? You can find more information on this bug in this KB article[KB]. Also, per same KB article, there is no workaround for this issue and to fix this issue, please upgrade to either CDH 5.13.2 or CDH 5.14.

Please let me know if you have any questions.

Thanks,
Karan

[1] https://issues.apache.org/jira/browse/SENTRY-2046
[KB]
https://cloudera-portal.force.com/articles/KB_Article/Enabling-Sentry-HDFS-ACL-synchronization-following-CDH-5-13-upgrade

12. This role's process failed to start (YARN NodeManager)

This error occured after starting the services of a recommissioned worker node. The following error message appeared in the NodeManager role log file:

Exit code from container executor initialization is : 24
ExitCodeException exitCode=24: File /opt/cloudera must be owned by root, but is owned by 995

This error message is misleading. We do not need to change the owner of /opt/cloudera.
This error is indicative of a symlink / alternatives issue:

[libby@worker5 ~]$ find /var/lib/alternatives/ -size 0 # check for 0 byte alternatives
[libby@worker5 ~]$ sudo find /var/lib/alternatives/ -size 0 -delete # delete for 0 byte alternatives
[libby@worker5 ~]$ sudo service cloudera-scm-agent restart # restart the agent
[libby@worker5 ~]$ ls -al /var/lib/alternatives/ # check that the alternatives are fixed

After these steps, we can deploy client configurations in Cloudera Manager. Then, we should be able to start the roles.

13. Command was terminated due to timeout(10000ms). See templeton.exec.timeout property, exitcode=143)

The 'templeton.exec.timeout' property can be increased by defining a safety valve in the Hive configuration. The safety valve that needs to be added to webhcat-site.xml in "WebHCat Server Advanced Configuration Snippet (Safety Valve) for webhcat-site.xml" and then restart WebHCat service.
For example:
Name: templeton.exec.timeout
Value: 20000

14. Enable LDAP Authentication on Hive caused HUE to not load a databases

If you have also configured Kerberos on your cluster, and want Hue to use kerberos authentication to Hive.

From Cloudera Manager, go to HUE configuration.
Search the "Hue Server Advanced Configuration Snippet (Safety Valve) for hive-site.xml" and add the following property.
Name: hive.server2.authentication
Value: kerberos

15. **Failed to start namenode. java.io.IOException: File is not under construction: /user/hive/.sparkStaging/application_1534639482711_40710/credentials-8d2ee118-aa03-4feb-b49d-bcefa31f72a3-3.tmp**

Generally happens due to active namenode server crash and there were some yarn application job running where edit log write was interrupted during the namenode shutdown.
Mitigation Steps
CM => HDFS => Instances => Click on active Namenode => Actions
1) Enter safemode
2) Run Savenamespace from the active NN in CM which dumps the current snapshot of the filesystem from the heap to a new fsimage.
3) Copy the generated new fsimage and supporting files from the active NN over to the stopped standby NN.

As root on igredhnwh02node02:

```
cd /opt/hadoop/dfs/nn
mkdir corrupt_20180924
mv current/* corrupt_20180924/
cd current/
scp ccdumg@igredhnwh02node01:/opt/hadoop/dfs/nn/current/* ./
chown hdfs.hadoop *
```

4) Start the standby NN.
5) Leave safemode

16. WebHcat - When you get HTTP 413 response - Below is the fix .

create a file with the below contents in a secure location and name it webhcat.xml (On the host that is running webhcat)

```
<?xml version="1.0"?>
<!DOCTYPE Configure PUBLIC "-//Jetty//Configure//EN"
"http://www.eclipse.org/jetty/configure.dtd">
<Configure id="FileServer" class="org.eclipse.jetty.server.Server">
<Call name="addConnector">
<Arg>
<New class="org.eclipse.jetty.server.nio.SelectChannelConnector">
<Set name="port">50111</Set>
<Set name="requestHeaderSize">65535</Set>      <<<<<<<<<      SET THIS TO A HIGHER SIZE IN THIS EXAMPLE ITS SET TO 65K
</New>
</Arg>
</Call>
</Configure>
```

Go to CM: CM -> Hive -> Configuration -> Search (WebHCat Server Advanced Configuration Snippet (Safety Valve) for webhcat-site.xml)

Name : templeton.jetty.configuration

Value : <<PATH TO webhcat.xml FILE ON THE SERVER>>

Description : Comment

17. Impala | IMPALAD_QUERY_MONITORING_STATUS has become bad

https://community.cloudera.com/t5/Customer/Impala-IMPALAD-QUERY-MONITORING-STATUS-has-become-bad/ta-p/75434

18. Impala | IMPALA_ASSIGNMENT_LOCALITY has become bad

Error: *The health test result for IMPALA_ASSIGNMENT_LOCALITY has become bad: 2.94% of assignments operating on local data over the past 15 minute(s). 1 local assignments. 34 total assignments. Critical threshold: 5.00%.*

Link:
https://www.cloudera.com/documentation/enterprise/5-5-x/topics/cm_ht_impala.html

FIX : New worker nodes were added a few days back and the cluster was rebalanced . Therefore , we ran Impala Invalidate Metadata Command .

CentOS/RHEL

1. An explanation of “yum remove”:

“Yum was developed to handle dependencies. This works great for installation and not so great for removal. If you need to remove packages with precision, you can use `rpm -e <package_name>` Keep in mind, you may still run into issues if the package is needed by something else. When unsure spin up an AWS micro and test there.

On the flip side, you can then use `rpm -i <package_name>` to install outside of Yum. These procedures should only be used when you fully understand what needs to be done.”

- ## How To Recover from Yum Remove OpenLDAP

Several packages depend on OpenLDAP, including YUM, SSH, and curl. If you run a “yum remove openldap” (only on a box with Centrify installed?), those apps will not work. Don’t ever do that. Below is a method to recover:

Identifying the Issue:

You can’t ssh to the box.
$ dzdo yum install openldap
There was a problem importing one of the Python modules
required to run yum. The error leading to this problem was:

liblber-2.4.so.2: cannot open shared object file: No such file or directory

Please install a package which provides this module, or
verify that the module is installed correctly.

It's possible that the above module doesn't match the

current version of Python, which is:
2.7.5 (default, Nov 6 2016, 00:28:07)
[GCC 4.8.5 20150623 (Red Hat 4.8.5-11)]

If you cannot solve this problem yourself, please go to
the yum faq at:
  http://yum.baseurl.org/wiki/Faq

$ which sshd
/usr/sbin/sshd
$ ldd /usr/sbin/sshd
	linux-vdso.so.1 => (0x00007fff453ec000)
	….
	libdl.so.2 => /lib64/libdl.so.2 (0x00007f89a4442000)
	libldap-2.4.so.2 => not found
	liblber-2.4.so.2 => not found
	libutil.so.1 => /lib64/libutil.so.1 (0x00007f89a423e000)
	…..

$ curl www.google.com
curl: error while loading shared libraries: liblber-2.4.so.2: cannot open shared object file:
No such file or directory

Pull Down the Package & Host It

On a node that is not broken.

$ yum provides libldap-2.4.so.2
…
openldap-2.4.44-5.el7.i686 : LDAP support libraries
Repo   : base
Matched from:
Provides   : libldap-2.4.so.2

…
$ yum install yum-utils
$ yumdownloader openldap
$ dzdo cp openldap-2.4.44-5.el7.* /var/www/html/
$ dzdo systemctl start httpd
$ curl -I "http://$HOSTNAME/openldap-2.4.44-5.el7.i686.rpm"
HTTP/1.1 200 OK

Date: Thu, 12 Oct 2017 03:42:32 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
Last-Modified: Thu, 12 Oct 2017 03:41:29 GMT
ETag: "57ae4-55b5150ca5e64"
Accept-Ranges: bytes
Content-Length: 359140
Content-Type: application/x-rpm

$ echo curl -I "http://$HOSTNAME/openldap-2.4.44-5.el7.x86_64.rpm"
curl -I http://aws1bdudev-clustermaster1.qg.com/openldap-2.4.44-5.el7.x86_64.rpm

Fix It

Back on the broken node:
$ wget http://aws1bdudev-clustermaster1.qg.com/openldap-2.4.44-5.el7.x86_64.rpm
$ rpm -i openldap-2.4.44-5.el7.x86_64.rpm
$ ldd /usr/sbin/sshd
    linux-vdso.so.1 => (0x00007ffd399e2000)
    ….
    libdl.so.2 => /lib64/libdl.so.2 (0x00007fb27483c000)
    libldap-2.4.so.2 => /lib64/libldap-2.4.so.2 (0x00007fb2745e8000)
    liblber-2.4.so.2 => /lib64/liblber-2.4.so.2 (0x00007fb2743d9000)
    libutil.so.1 => /lib64/libutil.so.1 (0x00007fb2741d5000)
    ….

Verify

SSH to the box
Verify Cloudera-SCM-Agent can restart:
$ systemctl restart cloudera-scm-agent
$ systemctl status cloudera-scm-agent
Verify yum works:
$ yum provides openldap

Issues and Identified Solutions during CDH or Cloudera Manager Upgrade

1. Redhat subscription has expired?

Disable RedHat related repo
#mv /etc/yum.repos.d/redhat.repo /etc/yum.repos.d/redhat.repo.bak

2. Cloudera Parcel not able to auto detect latest version?

Download the parcel using wget into the parcel repo directory(default: /opt/cloudera/parcel-repo)

https://www.cloudera.com/documentation/enterprise/latest/topics/cm_ig_create_local_parcel_repo.html#concept_cdc_kbk_mz

3. Parcel downloaded on local path but hash fails?

Create the hash-file based on parcel and make sure the owner is cloudera-scm

$ *sha1sum /opt/cloudera/parcel-repo/CDH-parcel-file.parcel | cut -d ' ' -f 1 > /opt/cloudera/parce-repo/CDH-parcel-file.parcel.sha*
$ chown cloudera-scm:cloudera-scm /opt/cloudera/parcel-repo/CDH-parcel-file.parcel /opt/cloudera/parcel-repo/CDH-parcel-file.parcel.sha

4. Change the Parcel Directory on the cluster nodes.

- It doesn't say this, but best to shut down the services first. They need to be restarted with the updated parcel path anyway. Avoid a holiday light display.
- You may need to do what I learned today is a 'hard' restart of the agent rather than a restart of the agent. `sudo service cloudera-scm-agent hard_restart_confirmed`. This apparently will stop everything that it has started. Or something like that.
- Make sure when you move the parcel directory, you verify *ALL SERVERS* have space available. I verified some and got bitten by one.
- Convince your client to hire experts to do this rather than an architect.

5. java.lang.RuntimeException: java.lang.ClassNotFoundException: Class com.sas.lasr.hadoop.DataNodeService not found

`sas.lasr.hadoop.jar`, `sas.lasr.jar` Jars are present in /opt/cloudera/parcels/CDH-5.11.1-1.cdh5.11.1.p0.4/lib/hadoop/lib and missing in

/opt/cloudera/parcels/CDH-5.13.1-1.cdh5.13.1.p0.2/lib/hadoop/lib... Just copying might resolve the issue temporarily

In Ansible there is a role named post-upgrade that should do what you need. Please test and verify.

6. Event Server after Cloudera Manager fails to start with exception java.io.FileNotFoundException: /var/lib/cloudera-scm-eventserver/v3/_desl.fdt (No such file or directory)

Backup Event Server Index Directory:
cp -ra /var/lib/cloudera-scm-eventserver
/var/lib/cloudera-scm-eventserver_backup

Remove all Event Server Index Directory Content:
rm -fr /var/lib/cloudera-scm-eventserver/*

Restart Event Server Role
It should work.

7. Missing Hive Metastore Tables

During the Validation of Hive Metastore Schema an error is produced stating tables are missing. The best description of the issue is found in the following location based on database.

less /opt/cloudera/parcels/CDH/lib/hive/scripts/metastore/upgrade/[derby/ mssql/ mysql/ oracle/ postgres/]README

Before beginning the upgrade, create or verify there is a current backup of the Hive Metastore.

Section #4 in the README states

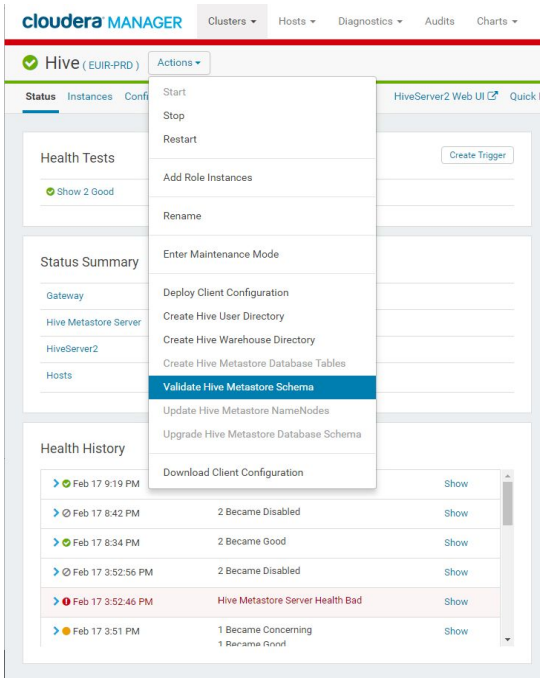
* Missing Tables: Hive's default configuration causes the MetaStore
to create schema elements only when they are needed. Some tables
may be missing from your MetaStore schema if you have not created
the corresponding Hive catalog objects, e.g. the PARTITIONS table
will probably not exist if you have not created any table
partitions in your MetaStore. You MUST create these missing tables

before running the upgrade scripts. The easiest way to do this is by executing the official schema DDL script against your schema. Each of the CREATE TABLE statements in the schema script include an IF NOT EXISTS clause, so tables which already exist in your schema will be ignored, and those which don't exist will get created.

The exact “official schema DDL” script will depend on the version of Hive. As an example, with CDH 5.11.1, Hive is version 1.1. To create missing tables, execute the following script based on the database.

/opt/cloudera/parcels/CDH/lib/hive/scripts/metastore/upgrade/[derby/ mssql/ mysql/ oracle/ postgres/]hive-schema-1.1.0.[database].sql

After completion, use the drop down menu in CM to run the validation of Hive Metastore Schema



Cleanup NodeManager user cache after Enabling Kerberos

8. Yarn “usercache” permissions errors after enabling Kerberos

Can't create directory /data1/yarn/nm/usercache/phounidmpprodmcoeing/appcache/application_1529596262942_0035 - Permission denied

Usercache directories created with simple/basic authentication are no longer accessible after enabling Kerberos. The recommended cleanup is to purge these directories. They will likely be spanned across several data volumes. This snippet should assist in safely purging them, continue to use appropriate caution.

```
# generate
find /data*/yarn/nm/usercache -type d -mindepth 1 -maxdepth 1 -exec echo rm -Rf {} \; >
/tmp/cleanup.sh

# review
less /tmp/cleanup.sh

# execute
chmod +x /tmp/cleanup.sh
/tmp/cleanup.sh
```

Kudu

1. org.apache.kudu.client.NonRecoverableException: Server requires Kerberos, but this client is not authenticated (kinit)

   https://issues.apache.org/jira/browse/KUDU-2264

   To do this navigate to CM -> Kudu -> Configuration, and under 'Kudu Service Advanced Configuration Snippet (Safety Valve) for gflagfile', append the following:
   --unlock_experimental_flags

   --authn_token_validity_seconds=31536000

   Where 31536000 is the number of seconds in a 365 days (1 year).

2. Check failed: _s.ok() Bad status: Corruption: Failed to load FS layout: Could not process records in container /data6/kudu/data/data/038f82aa516942178dc900b17a0c8c0e: Data length checksum does not match: Incorrect checksum in file /data6/kudu/data/data/038f82aa516942178dc900b17a0c8c0e.metadata at offset 2646054: Checksum does not match. Expected: 0. Actual: 1214729159

   https://docs.google.com/document/d/1lfMT_czoVjBVd1RMQQk6wHVkMGj11U2dmrs5W9j6q1U/edit

SOLR

Issue: ERROR (http-8985-1)-----o.a.s.s.SolrDispatchFilter: null:org.apache.solr.common.SolrException: SolrCore 'prod_rauptime_unharmonized_index_shard1_replica1' is not available due to init failure: Index locked for write for core prod_rauptime_unharmonized_index_shard1_replica at org.apache.solr.core.CoreContainer.getCore(CoreContainer.java:925)

Solution:
1. Stop the solr server, delete the write.lock files in hdfs path.

Ex: ***hadoop fs -ls /solr/prod_rauptime_unharmonized_index/core_node1/data/index***
Found 95 items
-rw-r----- 3 solr solr 0 2018-10-23 04:16 /solr/prod_rauptime_unharmonized_index/core_node1/data/index/HdfsDirectory

@e4290eec
lockFactory=org.apache.solr.store.hdfs.HdfsLockFactory@4b2ab60b-write.lock
-rw-r----- 3 solr solr 0 2018-10-01 12:55
/solr/prod_rauptime_unharmonized_index/core_node1/data/index/HdfsDirectory
@e4290eec
lockFactory=org.apache.solr.store.hdfs.HdfsLockFactory@66e6f9be-write.lock
-rw-r----- 3 solr solr 0 2018-10-01 16:26
/solr/prod_rauptime_unharmonized_index/core_node1/data/index/HdfsDirectory
@e4290eec
lockFactory=org.apache.solr.store.hdfs.HdfsLockFactory@71603ff3-write.lock

2. Ensure all the write.lock files are deleted in all the nodes and no solr processes are running.

3. Start the solr server and ensure new write.lock files are created.

4. Check the clusterstate.json file in zookeeper to ensure all the shards are active and also in solr web UI.

RCA: After restart of Zookeeper performed, Solr did not recover gracefully.Solr should have been able to completely recover after re-connecting to Zookeeper.

Kafka

1. ERROR admin.TopicCommand$: kafka.admin.AdminOperationException: replication factor: 1 larger than available brokers: 0

   While creating a topic if you encounter this error - you had either missed the zookeeper along with port number or forgot to mention the chroot directory
   kafka-topics --create --zookeeper blabla.host.com:2181/kafka --topic testing --partitions 3

   in the above command “/kafka ” is the chroot directory

   How to find the chroot directory in your environment ?

   cluster - > kafka - >configuration -> Search zookeeper.chroot

2. kafka.server.ReplicaFetcherThread: [ReplicaFetcherThread-0-235], Exiting because log truncation is not allowed for partition [npc_admin_topic,1], Current leader 235's latest offset 23439 is less than replica 234's latest offset 23442

   With this exception Kafka service will fail to start

   - kafka-configs.sh --zookeeper <SERVER NAME:PORT> --entity-type topics --entity-name npc_admin_topic --alter --add-config unclean.leader.election.enable=true
   - Restart the kafka service
   - Once the Kakfa service comes up test if you're able to produce and consume message from this broker.
   - kafka-configs.sh --zookeeper <SERVER NAME:PORT> --entity-type topics --entity-name npc_admin_topic --alter --add-config unclean.leader.election.enable=false
   - kafka-configs.sh --zookeeper <SERVER NAME:PORT> --entity-type topics --entity-name npc_admin_topic --alter --delete-config unclean.leader.election.enable

3. org.I0Itec.zkclient.exception.ZkException: org.apache.zookeeper.KeeperException$NoAuthException: KeeperErrorCode = NoAuth for /brokers/topics/Deepa-new-2/partitions

   The above errors are displayed while creating or deleting topic from an ordinary user. This is because only the process owner of Kafka service such as root, can write to Zookeeper znodes (/configs/topics). Create the topic as kafka user or root.

   2 . The below error will pop up if you try to create a topic without mentioning the root directory of kafka . (The bolded one in the command is the rootdirectory for me)

ERROR admin.TopicCommand$: kafka.admin.AdminOperationException: replication factor: 1 larger than available brokers: 0
at kafka.admin.AdminUtils$.assignReplicasToBrokers(AdminUtils.scala:117)
at kafka.admin.AdminUtils$.createTopic(AdminUtils.scala:403)
at kafka.admin.TopicCommand$.createTopic(TopicCommand.scala:110)
at kafka.admin.TopicCommand$.main(TopicCommand.scala:61)
at kafka.admin.TopicCommand.main(TopicCommand.scala)

bash-4.1# kafka-topics --create --zookeeper mapls352.bsci.bossci.com:2181/**kafka** --topic testing --partitions 3 --replication-factor 1
SLF4J: Class path contains multiple SLF4J bindings.
SLF4J: Found binding in [jar:file:/cloudera/opt/cloudera/parcels/KAFKA-2.1.1-1.2.1.1.p0.18/lib/kafka/libs/slf4j-log4j12-1.7.21.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: Found binding in [jar:file:/cloudera/opt/cloudera/parcels/KAFKA-2.1.1-1.2.1.1.p0.18/lib/kafka/libs/slf4j-log4j12-1.7.5.jar!/org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: See http://www.slf4j.org/codes.html#multiple_bindings for an explanation.
SLF4J: Actual binding is of type [org.slf4j.impl.Log4jLoggerFactory]
Created topic "testing".

Rack assignment issue after commissioning new node to CM

- **Issue:** After commissioning first new worker host it was identified that it is still considering to be in the default rack from HDFS Rebalancer logs by which it had large number of blocks on it when compared to other node blocks.
    - The first node was commissioned without any rack assignment so it took default rack and later after all roles started on host, the rack was assigned to it. This rack assignment made a stale config on few services and refreshable config's on hdfs and yarn services.
    - For refreshable configurations we just did cluster refresh which did refresh the configurations on hdfs and yarn but hdfs rebalancer

was still considering it with default rack moving all data blocks to this one particular new worker node.
    - Interestingly, the topology.py in the namenode process directory has the updated rack info. but still load balancer is considering it with default rack. We assumed this is because the topology probably cached in memory.
    - We tried redeploying configurations and starting the load balancer it did not work in this case.
- **Solution:**
    - We assumed that load balancer talks RPC to the namenode to pull the rack locations and just restarted namenode and this fixed the issue.
    - After the namenode restart, the hdfs reblanacer was able to pick appropriate rack for the new worker node and balanced hdfs blocks accordingly.

Sample hdfs load balancer log with new worker node considering it with default rack:

2018-09-21 20:13:22,937 INFO [main] balancer.Balancer (Balancer.java:getLong(227)) - dfs.balancer.max-size-to-move = 10737418240 (default=10737418240)

2018-09-21 20:13:22,959 INFO [main] net.NetworkTopology (NetworkTopology.java:add(425)) - Adding a new node: /maplegrove/weaverlake3/9P/10.44.128.92:1004

2018-09-21 20:13:22,961 INFO [main] net.NetworkTopology (NetworkTopology.java:add(425)) - Adding a new node: /maplegrove/weaverlake3/9R/10.44.129.128:1004

2018-09-21 20:13:22,961 INFO [main] net.NetworkTopology (NetworkTopology.java:add(425)) - Adding a new node: /default/default/default/10.44.129.119:1004

2018-09-21 20:13:22,966 INFO [main] balancer.Balancer (Balancer.java:logUtilizationCollection(408)) - 0 over-utilized: []

2018-09-21 20:13:22,966 INFO [main] balancer.Balancer (Balancer.java:logUtilizationCollection(408)) - 0 underutilized: []

The cluster is balanced. Exiting...

Sep 21, 2018 8:13:22 PM 0 0 B 0 B -1 B

Sep 21, 2018 8:13:22 PM Balancing took 1.677 seconds

Exit code: 0

Bad disk issue with Navencrypt

- **Issue:** One of the encrypted disk did not show up with its partition (sdc) after server reboot. After reboot the services on it started creating the directories as below. With corrupted disk the kudu tablet server will fail to start.

```
sdb                 8:16   0  200G  0 disk
└─sdb1              8:17   0  200G  0 part
  └─01 (dm-11)    253:11   0  200G  0 crypt /cloudera/data/01
sdc                 8:32   0    1T  0 disk
sdf                 8:80   0    1T  0 disk
└─sdf1              8:81   0 1024G  0 part
  └─11 (dm-7)     253:7    0 1024G  0 crypt /cloudera/data/11
```

```
root@mapls197# ls -al /cloudera/data/02/dfs/
total 12
drwxr-xr-x 3 root root   4096 Sep 26 05:46 .
drwxr-xr-x 5 root root   4096 Sep 26 05:46 ..
drwx------ 3 hdfs hadoop 4096 Sep 26 10:08 dn
```

  - When checked for mount status of disks with navencrypt, sdc disk appears to be unmounted or it was unable to mount.
    - $ sudo navencrypt-collect > navencrypt.info basically pulls out navencrypt complete status information.
    - From navencrypt log info, we notice that the disk was unable to mount.
      - 2018-09-26 15:39:07,816 +0000 level=WARNING app=navencrypt-mount action=configure Unable to mount /dev/disk/by-uuid/5afd3709-a3b6-407f-8ab8-4101a5fd8b55. Execute 'dmsetup table', 'cryptsetup status <device>'and 'cryptsetup luksClose <device>' to list and close a device if needed.
  - When we try to mount using navencrypt-mount command it will fail in this scenario
- **Solution:**
  - We had to stop all roles on the server, delete all the dirs in disk/format the corrupted disk and prepare the disk sdc for navencrypt again which is basically creating the disk partition and encrypting it which solved the bad disk problem.
  - Kudu being at 1.5 version is not capable of handling this kind of disk failures and in order to get kudu backup and running we had to delete all the kudu related data dir's including wal files from all disks on server and start all the roles back which are stopped. With this kudu should be able to start back again.

        - Kudu 1.6 version is more capable of handling this kind of failures.
    - Hdfs blocks and kudu tablets will be replicating to this server after all roles are up and started on this server. We won't expect any data loss in this situation provided the data in hdfs and kudu are adhere to replication factor 3.

CDSW

1. Unable to connect to the server :x509:cannot validate certificate for

Issue: When we ran the *cdsw_protect_stop_restart.sh* as part of CDSW v1.4.2 upgrade we got below error.

Error: Unable to connect to the server :x509:cannot validate certificate for 10.243.140.184 because it dosen't contain any IP SANs

Fix: Replaced the IP with FQDN of Master AON node in */etc/kubernetes/admin.conf and /etc/kubernetes/kubelet.conf*

and re ran the *cdsw_protect_stop_restart.sh* to resolve the issue.

HDFS File Browser Error

Issue:

- Server Error when accessing file browser

Root Cause:

- In the Reports Manager logs you'll see the following error as you try to access the file browser:
  ORA-00942: table or view does not exist

Solution:

- The Reports manager database is missing a table. To figure out which table is missing turn the logs up to 'trace' this will give you the SQL query the app is trying to run and tell you the missing table.
- Create the table in the DB or if you don't have access have the DBA create it for you.

Navigator Audit pipeline failure

Issue:

- The Navigator audit pipeline failure for impala

Root Cause:

- The Navigator audit pipelines for impala are getting failed due to incorrect string value like sql.SQLException: Incorrect string value: '\xF0\x9F\x98\x8A ...' for column 'OPERATION_TEXT' at row 1.

Solution:
Temporary Fix:

- As Workaround we can move the impala audit files that contains the emoji out from the audit directory and restart the agent.

- Moving the audit files that contains the emoji to an appropriate location on each host affected:

  1. Execute the following command to identify the audit log file(s) containing the problematic character data:
  # perl -nle '/\xF0\x9F/ && print $ARGV' /var/log/impalad/audit/* | uniq

  2. For each file name returned, execute the following command, substituting the file name for <affected_filename>.
  # perl -i.bak -nlE 'print unless /\xF0\x9F/'
  <foreach_affected_filename_result_from_point -1->

  3. The previous step will produce a backup file for each audit log file on which it was executed. Move all the .bak files somewhere appropriate (different directory).

  4. Restart the Cloudera Manager agent with the following command:
  # service cloudera-scm-agent restart

Permanent fix:

- The databases characterset and collation should be converted to utf8mb4 format or upgrade CDH to 6.1

{1} Below you can find the steps to alter the schema of the navigator db, it will require a downtime as we recommend to stop all the services.

[prerequisite: mysql version >= 5.5.3]

1./ Stop all the CDH and CM services
2./ Backed up all the databases with mysqldump.

3./ Changed the encoding and collation on the database and the first table:
ALTER DATABASE <Navigator DB Name> CHARACTER SET = utf8mb4 COLLATE = utf8mb4_unicode_ci;
USE <Navigator DB Name>;
ALTER TABLE IMPALA_AUDIT_EVENTS CONVERT TO CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;

4./ Changed the encoding of each text column in the IMPALA_AUDIT_EVENTS table, for example:

ALTER TABLE IMPALA_AUDIT_EVENTS CHANGE `SESSION_ID` `SESSION_ID` VARCHAR(255) CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
ALTER TABLE IMPALA_AUDIT_EVENTS CHANGE `STATUS` `STATUS` longtext CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;

We generally left the length of VARCHAR columns unchanged, except for the PRIVILEGE column to VARCHAR(191) to avoid exceeding a size limit on InnoDB index columns.

I'll attach a file containing all the ALTER TABLE statements as example "file:alter-impala_audit_events-utf8mb4.sql".

5. Repeated the table changes from IMPALA_AUDIT_EVENTS above on the tables called IMPALA_AUDIT_EVENTS_YYYY_MM_DD.

6. Edit /etc/my.cnf, changing the two following lines
collation-server = utf8mb4_unicode_ci
character-set-server = utf8mb4

7. Restarted mariadb/mysqldb.
systemctl restart mariadb.service
OR
service mysqld restart

8. Restarted all the CDH and CM services (in retrospect, it would've been safer to shut them down before modifying the DB).

Impala:

Issue: R program failing with error rawoToChar error.

Rootcause: query failed due the special character \0 in some of the impala tables.

Solution : Remove the special special characters from the table.

Steps to find : execute the below queries in the impala to find out the special characters.

- Ex: i*mpala-shell -k --ssl -i cloudera-eap.aonnet.aon.net -q "SHOW COLUMN STATS <<TABLE_NAME>>;"* **>** *<<COLOUMN>>.cols*

- *cat <<COLOUMN>>..cols |grep STRING |awk '{print "impala-shell -k --ssl -i cloudera-eap.aonnet.aon.net -q \"SELECT COUNT("$2") FROM <<TABLE_NAME>> WHERE ascii("$2") = 0;\""}' > <<COLOUMN>>.queries*

- *bash <<COLOUMN>>.queries > <<COLOUMN>>.results*