

CCP Preparing for Upgrade 2.0.1

Preparing to Upgrade CCP

Date of publish: 2017-11-06

CLOUDERA

<https://docs.cloudera.com/>

Legal Notice

© Cloudera Inc. 2019. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 ("ASLv2"), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER'S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

- Preparing to Upgrade.....4**
 - Stop All Metron Services.....4
 - Back up Your Configuration.....6
 - Remove Metron Installation.....7

Preparing to Upgrade

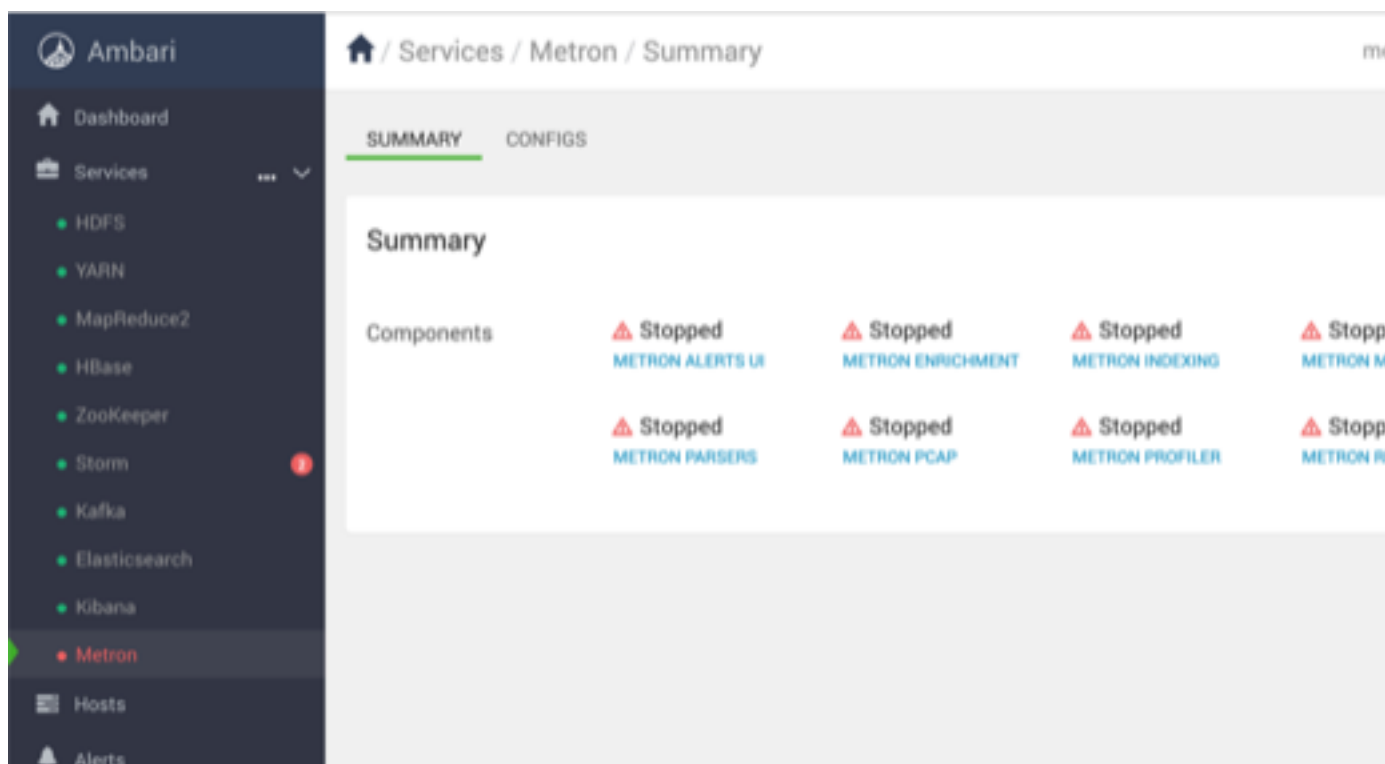
Cloudera Cybersecurity Platform (CCP) upgrades are not officially supported. However you can use the guidelines provided in the Upgrade Guide if you want to attempt an upgrade. Prior to upgrading CCP, you must back up your configuration and stop all Metron services.

Stop All Metron Services

You need to stop all Metron services prior to uninstalling Metron.

Procedure

1. Stop any inputs into Metron.
For example, stop any NiFi feeds.
2. In Ambari, stop all Metron services in the following order:
 - Metron Alerts UI
 - Metron Management UI
 - Metron REST



3. Stop Storm.
 - a) From the Storm node, list all of the Storm topologies that are currently running:

```
storm list
```

If any topologies are running, your output should look similar to the following:

```
Running: /usr/jdk64/jdk1.8.0_112/bin/java -Ddaemon.name= -  
Dstorm.options=
```

```
-Dstorm.home=/usr/hdp/3.1.4.1050-37/storm -Dstorm.log.dir=/var/log/
storm
-Djava.library.path=/usr/local/lib:/opt/local/lib:/usr/lib:/usr/hdp/
current/storm-client/lib
-Dstorm.conf.file= -cp /usr/hdp/3.1.4.1050-37/storm/lib/ring-
cors-0.1.5.jar:/usr/hdp/3.1.4.1050-37
/storm/lib/storm-core-1.1.0.3.1.4.1050-37.jar:/usr/hdp/3.1.4.1050-37/
storm/lib/disruptor-3.3.2.jar:
/usr/hdp/3.1.4.1050-37/storm/lib/asm-5.0.3.jar:/usr/hdp/3.1.4.1050-37/
storm/lib/reflectasm-1.10.1.jar:
/usr/hdp/3.1.4.1050-37/storm/lib/slf4j-api-1.7.21.jar:/usr/
hdp/3.1.4.1050-37
/storm/lib/servlet-api-2.5.jar:/usr/hdp/3.1.4.1050-37/storm/lib/log4j-
over-slf4j-1.6.6.jar:
/usr/hdp/3.1.4.1050-37/storm/lib/kryo-3.0.3.jar:/usr/hdp/3.1.4.1050-37/
storm/lib/minlog-1.3.0.jar:
/usr/hdp/3.1.4.1050-37/storm/lib/log4j-core-2.8.2.jar:/usr/
hdp/3.1.4.1050-37/storm
/lib/zookeeper.jar:/usr/hdp/3.1.4.1050-37/storm/lib/log4j-
api-2.8.2.jar:/usr/hdp/3.1.4.1050-37
/storm/lib/storm-rename-hack-1.1.0.3.1.4.1050-37.jar:/usr/
hdp/3.1.4.1050-37/storm/lib
/log4j-slf4j-impl-2.8.2.jar:/usr/hdp/3.1.4.1050-37/storm/lib/
clojure-1.7.0.jar:/usr/hdp
/3.1.4.1050-37/storm/lib/objenesis-2.1.jar:/usr/hdp/3.1.4.1050-37/storm/
extlib-daemon
/ranger-plugin-classloader-0.7.0.3.1.4.1050-37.jar:/usr/
hdp/3.1.4.1050-37/storm/extlib-daemon
/ranger-storm-plugin-shim-0.7.0.3.1.4.1050-37.jar:/usr/
hdp/3.1.4.1050-37/storm/extlib-daemon
/ojdbc6.jar:/usr/hdp/current/storm-supervisor/conf:/usr/
hdp/3.1.4.1050-37/storm/bin org.apache.storm.command.list
2670 [main] INFO o.a.s.u.NimbusClient - Found leader nimbus :
node1:6627
Topology_name      Status      Num_tasks  Num_workers  Uptime_secs
-----
enrichment         ACTIVE      8           1             49253
bro__snort__yaf    ACTIVE      7           1             48749
batch_indexing     ACTIVE      5           1             48613
pcap               ACTIVE      3           1             49140
profiler           ACTIVE      7           1             49001
random_access_indexing ACTIVE      5           1             48493
```

b) Kill each of the running Storm topologies in the following order:

- all parsers such as bro and snort
- enrichment
- indexing
- profiler

```
storm kill bro
```

c) Return to the Storm UI and verify that all topologies are killed.

d) In Ambari, stop Storm by selecting Storm and clicking **Stop All** in the **Actions** menu.

4. Ensure that the UIs are shut down.

If the Metron Alerts Ui or Metron Management Ui status in Ambari is "running," shut down the UIs by entering the following:

```
service metron-alerts-ui status
service metron-alerts-ui stop

service metron-management-ui status
```

```
service metron-management-ui stop
```

Back up Your Configuration

The Cloudera Cybersecurity Platform (CCP) upgrade uses the default configuration for the new Metron version. If you made any changes to the Metron configuration in the previous version, you must back up your old configuration so you can incorporate those changes into the new Metron configuration. A convenience script has been provided to automatically extract and insert your Metron Ambari configuration.

About this task

You do not need to back up the CCP data residing in HBase, Hive, Elasticsearch, and Solr. Existing HCP processed data residing in HBase, HDFS, Hive, Elasticsearch, and Solr remains untouched during the cluster upgrade and is reconnected with CCP after you add back your configuration parameters.

Procedure

1. Login to the node on which Ambari is installed.
2. Create an upgrade directory:

```
mkdir /<HCP200_UPGRADE>
```

3. Navigate to the upgrade directory:

```
cd /<HCP200_UPGRADE>
```

4. Create a folder for your Metron configuration in the upgrade directory:

```
mkdir metron-config
```

5. Copy your Metron configuration from the host on which Metron was installed into the Metron configuration directory you created in the previous step:

```
scp -rp <INSTALLED_METRON_HOSTNAME>:/usr/hcp/current/metron/config/  
<file_name> metron-config/
```

Be sure to copy the following property files:

- elasticsearch.properties
- enrichment.properties
- pcap.properties

6. Copy the Metron defaults script from the host on which Metron was installed to the /etc/defaults folder:
Make sure the account you are logged into has access to run ssh.

```
scp <INSTALLED_METRON_HOSTNAME>:/etc/default/metron .  
source etc/default/metron  
scp <INSTALLED_METRON_HOSTNAME>:$METRON_HOME/bin/upgrade_helper.sh  
mkdir -p $METRON_HOME/bin  
scp <INSTALLED_METRON_HOSTNAME>:$METRON_HOME/bin/zk_load_configs.sh  
$METRON_HOME/bin
```

7. Take note of the installed cluster name displayed by Ambari.
8. Run the upgrade_helper.sh script from the HCP200-Update folder to back up your Ambari configurations related to Metron and your Metron ZooKeeper configuration files and put them into a local directory called metron-backup.

```
$METRON_HOME/bin/upgrade_helper.sh backup <ambari address> <ambari admin  
username> <ambari admin password> <cluster_name>
```

If the credentials or cluster is not correct, you will see the following error message:

```
Unable to get cluster detail from Ambari. Check your username, password,
and cluster name. Skipping.
```

9. Ensure that the metron-backup folder contains your Metron and ZooKeeper configuration:

```
ls -l
```

You should see at least the following:

```
metron-configs
zk-configs
```

10. If you created custom components in Metron, copy the contents of /usr/hcp/current/metron/parser_contrib to the metron-backup folder:

```
scp -rp <INSTALLED_METRON_HOSTNAME>:/usr/hcp/current/metron/
parser_contrib/ parser_contrib
```

11. Confirm that the parser_contrib information was copied correctly:

```
ls -l parser_contrib/
```

You should see a list of your custom jars.

Remove Metron Installation

After you have backed up your configuration and stopped all Metron services, you need to uninstall Metron.

Procedure

1. Verify Metron is stopped:

```
storm list
```

Examine the output and verify no Metron topologies are active.

2. In Ambari, select **Metron > Services Actions menu > Delete Service**.
3. At the bottom of the **Delete Service** window, click **Delete**.
4. When prompted, enter **delete**, then click the **Delete** button to confirm deleting the service.
5. Uninstall Metron Mpack:

```
ambari-server uninstall-mpack --mpack-name=metron-ambari.mpack --verbose
```

6. Restart Ambari:

```
ambari-server restart
```

7. Uninstall ElasticSearch mpack if installed:

```
ambari-server uninstall-mpack --mpack-name=elasticsearch-ambari.mpack --
verbose
```

8. Restart Ambari:

```
ambari-server restart
```

9. From the Ambari node, enter the following to list all of the Metron packages:

```
srpm -qa | grep metron
```

You should see output similar to the following:

```
metron-metron-management-0.7.1-201904012257.noarch
metron-enrichment-0.7.1-201904012257.noarch
metron-indexing-0.7.1-201904012257.noarch
metron-rest-0.7.1-201904012257.noarch
metron-alerts-0.7.1-201904012257.noarch
metron-data-management-0.7.1-201904012257.noarch
metron-parsers-common-0.7.1-201904012257.noarch
metron-parsing-storm-0.7.1-201904012257.noarch
metron-profiler-storm-0.7.1-201904012257.noarch
metron-profiler-repl-0.7.1-201904012257.noarch
metron-elasticsearch-0.7.1-201904012257.noarch
metron-pcap-0.7.1-201904012257.noarch
metron-config-0.7.1-201904012257.noarch
metron-maas-service-0.7.1-201904012257.noarch
metron-common-0.7.1-201904012257.noarch
metron-parsers-0.7.1-201904012257.noarch
metron-profiler-spark-0.7.1-201904012257.noarch
metron-solr-0.7.1-201904012257.noarch
metron-performance-0.7.1-201904012257.noarch
```

10. Using the metron-config information you received from the input in the previous step, enter the following to remove all of the Metron packages:

```
sudo rpm -q --scripts metron-config-0.7.1-201904012257.noarch
```

You should see output similar to the following:

```
chkconfig --add metron-management-ui
chkconfig --add metron-alerts-ui
preuninstall scriptlet (using /bin/sh):
chkconfig --del metron-management-ui
chkconfig --del metron-alerts-ui
```

11. List all metron packages by running the following on each host:

```
rpm -qa | grep metron
```

12. Remove all traces of old Metron packages on each host:

```
yum remove <metron package names>
yum clean all
```

13. Ensure that no Metron packages remain by running the following on each host:

```
rpm -qa | grep metron
```

The command should return no packages.