

CCP Upgrading 2.0.0

Upgrading Metron

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

Upgrade Metron..... 4

Upgrade Metron

After you shut down Metron and all of its services, you must uninstall Metron and then reinstall the newest version of Metron.

Before you begin

You must upgrade to HDP 3.1.4 prior to upgrading Metron. For more information about upgrading to HDP 3.1.4, see the HDP 3.1.4 Upgrade documentation.

About this task

Although the product has been rebranded to Cloudera Cybersecurity Platform (CCP), the repository, mpack, and directory names currently remain hcp.

Procedure

1. Back up your Metron configuration:

a) Create an upgrade folder:

```
mkdir HCP200-Upgrade
cd HCP200-Upgrade/
```

b) Copy your Metron configuration into the upgrade folder:

```
cp -rp /usr/hcp/current/metron/config metron-config
```

c) Download the ZooKeeper configuration into the upgrade folder:

```
source /etc/default/metron
/usr/hcp/current/metron/bin/zk_load_configs.sh -z $ZOOKEEPER -m PULL -o
zk-config
```

d) Ensure that the upgrade folder contains your Metron and ZooKeeper configurations:

```
ls -l
```

You should see something similar to the following:

```
metron-config
zk-config
```

e) If you have created custom components in Metron, copy the contents of /usr/hcp/current/metron/parser_contrib to the upgrade folder:

```
cp -rp /usr/hcp/current/metron/parser_contrib/ parser_contrib
```

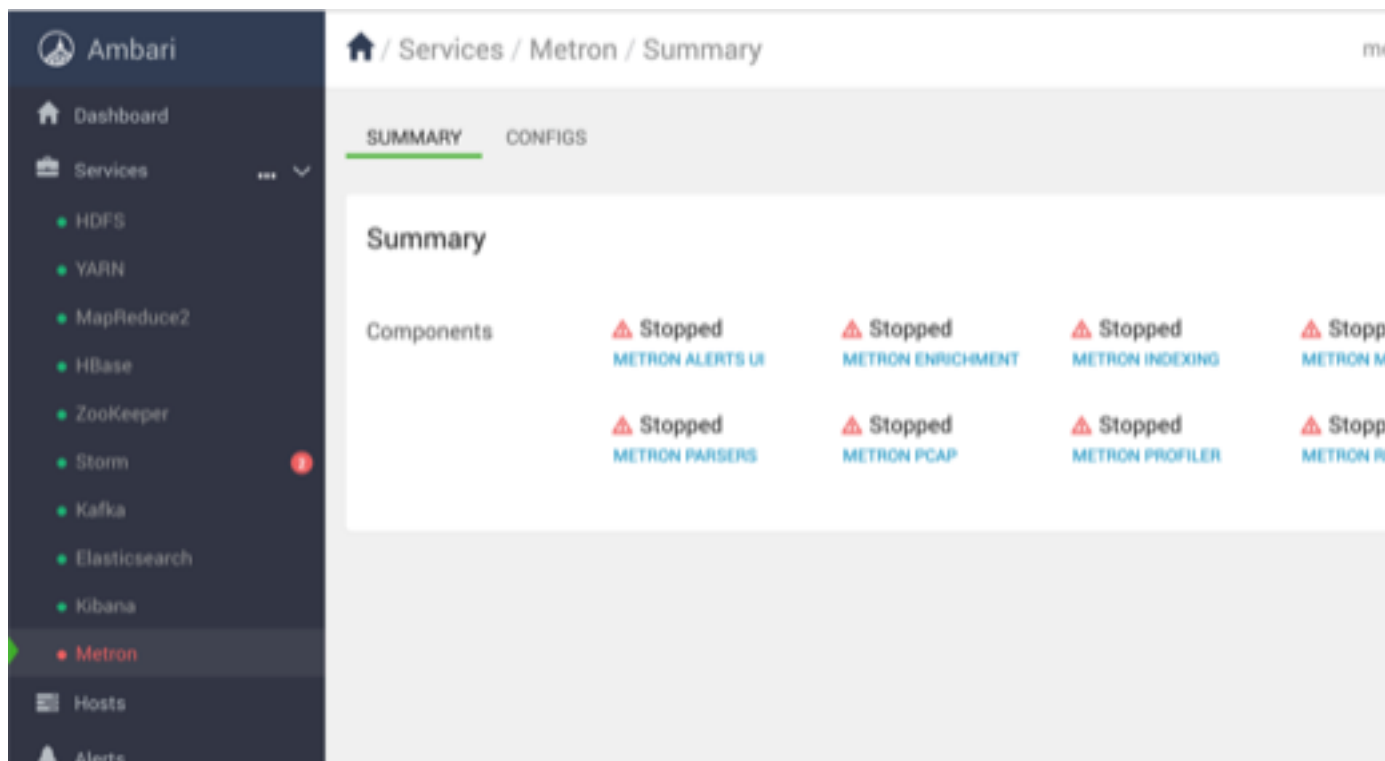
f) Confirm that the parser_contrib information was copied correctly:

```
ls -l parser_contrib/
```

You should see something similar to the following:

```
first_parser.jar
second_parser.jar
third_parser.jar
fourth_parser.jar
```

2. In Ambari, stop all Metron Services.



3. Stop all Storm Metron topologies and confirm all are stopped.

a) List all topologies in Storm.

```
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) Stop all of the Metron Storm topologies:

```
storm kill <TOPOLOGY_NAME>
```

- c) Confirm that all of the Metron Storm topologies are stopped:

```
storm list
```

You should see No topologies running.

4. Uninstall Metron.

- In Ambari, select **Metron**, then under the **Service Actions** menu, click **Delete Service**.
 - At the bottom of the **Delete Service** window, click **Delete**.
 - When prompted, enter "delete" then click the **Delete** button to confirm deleting the service.
- Ambari displays a confirmation window stating "Service Metron was successfully deleted."

5. Remove all of the rpms from the old Metron version.

CentOS

- a) From the Ambari node, enter the following to list all of the Metron packages:

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

You should see input 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
```

- b) 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
```

6. Remove older Metron rpms on other nodes.

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

7. In Ambari, update the Repo version.

To navigate to the Repositories page, from the **admin** menu, choose **Manage Ambari**, click **Versions**, then click **REGISTER VERSION**.

Repositories

Provide Base URLs for the Operating Systems you are configuring.

OS	Name	Base URL
redhat7	ES-Curator-5.x	<input type="text" value="http://shd01-rep01.shd01.ops.omss/repo/Elasticsean"/>
	HCP-1.4.2.0	<input type="text" value="shd01.ops.omss/repo/HortonWorks/HCP-1.8.0.0-58/"/>
	HDP-2.6	<input type="text" value="http://shd01-rep01.shd01.ops.omss/repo/HortonWorl"/>
	HDP-UTILS-1.1.0.21	<input type="text" value="http://shd01-rep01.shd01.ops.omss/repo/HortonWorl"/>
	elasticsearch-5.x	<input type="text" value="http://shd01-rep01.shd01.ops.omss/repo/Elasticsean"/>
	kibana-5.x	<input type="text" value="http://shd01-rep01.shd01.ops.omss/repo/Elasticsean"/>

☐ Skip Repository Base URL validation (Advanced)
 ☐ Use RedHat Satellite/Spacewalk

Cancel

- Uninstall the old HCP mpack version:

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

- Install the current HCP mpack repo from [Release Notes](#).

```
wget http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.9.1.0/tars/metron/ccp-ambari-mpack-1.9.1.0-6.tar.gz
ambari-server install-mpack --force --mpack=/${MPACK_DOWNLOAD_DIRECTORY}/ccp-ambari-mpack-1.9.1.0-6.tar.gz --verbose
```

- Restart the Ambari server.

```
ambari-server restart
```


11.Re-open Ambari and add the updated Metron version.

From the **Actions** menu, click **Add Service**, then click Metron from the **Choose Services** page. Ensure Metron is the updated version.

Ambari lists each service on which Metron is dependent.

12.Click yes to add each dependency.

13.In Ambari, add back your Metron configuration information in the **Property** fields.

Do not copy and paste into the Metron property fields. You can inadvertently add a special character.

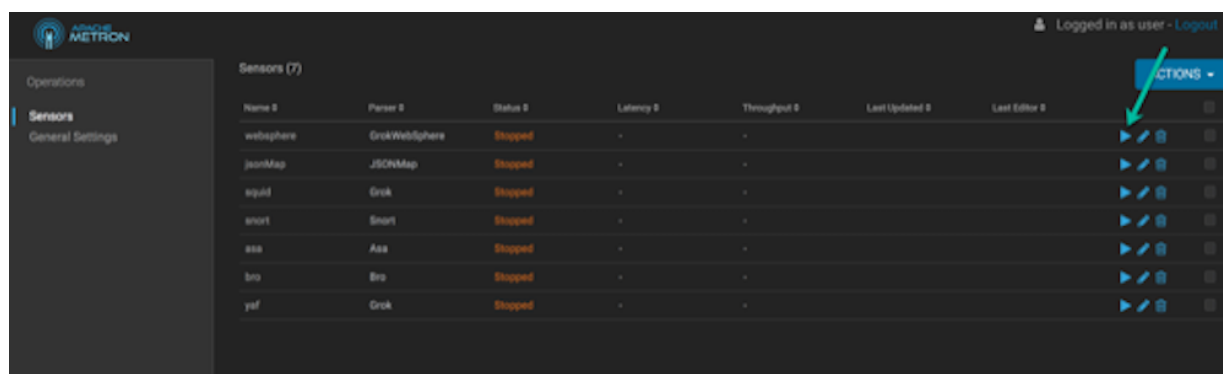
14.Click **Deploy** to start the Metron set up.

The process to install, start, and test Metron will take a while.

15.Restart the Metron services:

- Metron REST
- Metron Management UI
- Metron Alerts UI
- Indexing

16.In the Management UI, restart the Metron Parsers including Enrichment, Bro, Snort, Yaf, and any other parsers you added previously.



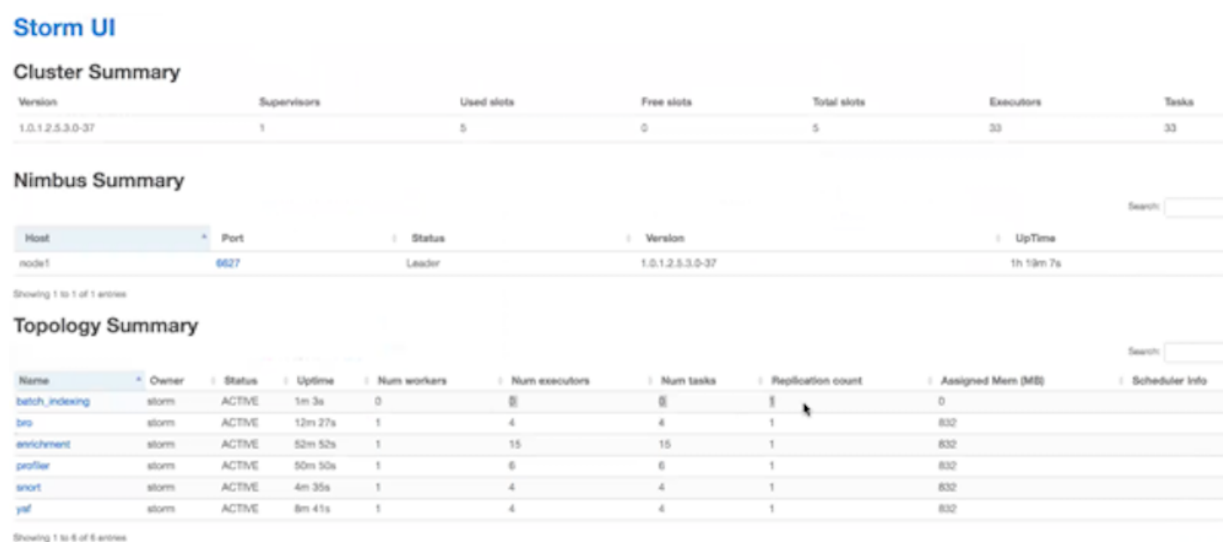
The screenshot shows the Metron Management UI. On the left is a sidebar with 'Operations' and 'Sensors' (selected). The main area displays a table of 7 sensors. A red arrow points to the 'ACTIONS' button in the top right corner of the table.

Name	Parser	Status	Latency	Throughput	Last Updated	Last Editor	ACTIONS
webSphere	GrokWebSphere	Stopped	-	-	-	-	[Start] [Stop] [Refresh] [Delete]
jsonMap	JSONMap	Stopped	-	-	-	-	[Start] [Stop] [Refresh] [Delete]
sqoop	Grok	Stopped	-	-	-	-	[Start] [Stop] [Refresh] [Delete]
snort	Snort	Stopped	-	-	-	-	[Start] [Stop] [Refresh] [Delete]
asa	Asa	Stopped	-	-	-	-	[Start] [Stop] [Refresh] [Delete]
bro	Bro	Stopped	-	-	-	-	[Start] [Stop] [Refresh] [Delete]
yaf	Grok	Stopped	-	-	-	-	[Start] [Stop] [Refresh] [Delete]



Note: Starting the Metron parsers might take a while.

17.Check the status of the parsers in the Storm UI.



The screenshot shows the Storm UI. It includes sections for Cluster Summary, Nimbus Summary, and Topology Summary.

Cluster Summary

Version	Supervisors	Used slots	Free slots	Total slots	Executors	Tasks
1.0.1.2.5.3.0-37	1	5	0	5	33	33

Nimbus Summary

Host	Port	Status	Version	UpTime
node1	6627	Leader	1.0.1.2.5.3.0-37	1h 19m 7s

Topology Summary

Name	Owner	Status	Uptime	Num workers	Num executors	Num tasks	Replication count	Assigned Mem (MB)	Scheduler Info
batch_indexing	storm	ACTIVE	1m 3s	0	0	0	1	0	
bro	storm	ACTIVE	12m 27s	1	4	4	1	832	
enrichment	storm	ACTIVE	52m 52s	1	15	15	1	832	
profiler	storm	ACTIVE	50m 50s	1	6	6	1	832	
snort	storm	ACTIVE	4m 35s	1	4	4	1	832	
yaf	storm	ACTIVE	8m 41s	1	4	4	1	832	