

CCP Upgrading 2.0.1

## 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 and uninstall Metron, you can reinstall the newest version of Metron.

## Before you begin

- Stop all Metron services
- Back up your Metron configuration
- Remove the Metron installation

## About this task

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

## Procedure

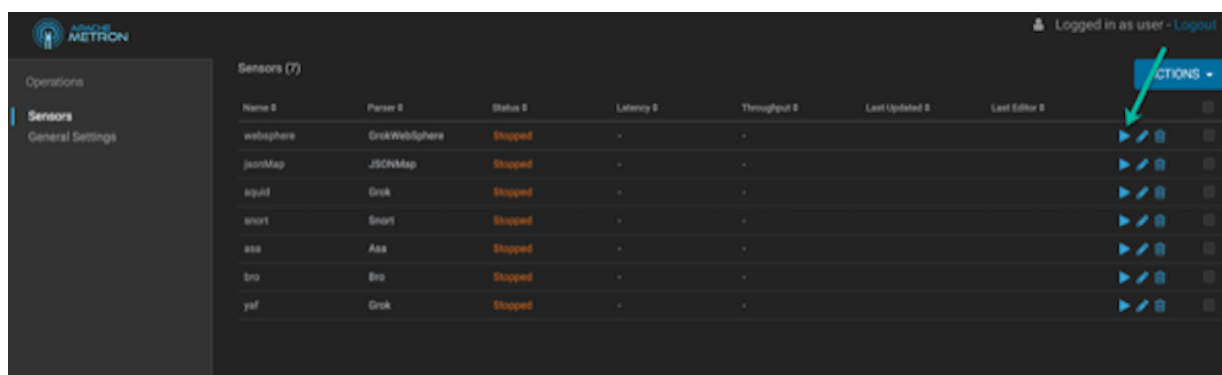
1. If you have SOLR or Elasticsearch installation, follow the relevant instructions to update the index to HDP 3.1.4
2. Update Ambari.  
For more information on updating Ambari, see the upgrade documentation for Ambari.
3. Update to HDP 3.1.4.  
For more information about upgrading to HDP 3.1.4, see the HDP 3.1.4 Upgrade documentation.
4. Install the current HCP mpack repo from [Release Notes](#).

```
wget http://public-repo-1.hortonworks.com/HCP/centos7/2.x/updates/2.0.0.0/tars/metron/hcp-ambari-mpack-2.0.0.0-4.tar.gz
ambari-server install-mpack --force --mpack=${MPACK_DOWNLOAD_DIRECTORY}/hcp-ambari-mpack-2.0.0.0-4.tar.gz --verbose
```

5. Restart the Ambari server.

```
ambari-server restart
```

6. 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.
7. Click yes to add each dependency.
8. Click **Deploy** to start the Metron set up.  
The process to install, start, and test Metron will take a while.
9. Restart the Metron services:
  - Metron REST
  - Metron Management UI
  - Metron Alerts UI
  - Indexing
10. In the Management UI, restart the Metron Parsers including Enrichment, Bro, Snort, Yaf, and any other parsers you added previously.



**Note:** Starting the Metron parsers might take a while.

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

### Storm UI

#### 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

Showing 1 to 1 of 1 entries

#### 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	0	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	

Showing 1 to 6 of 6 entries

12. Stop all Metron services again.

See Stop All Metron Services for more information.

13. Retrieve the New Metron Ambari configs.

a) On the host on which Ambari is installed, create the HCP200-New directory and navigate to that directory:

```
mkdir HCP200-New
cd HCP200-New/
```

Take note of the installed cluster name displayed by Ambari.

b) Run the upgrade\_helper.sh from the HCP200-Update folder:

```
$METRON_HOME/bin/upgrade_helper.sh restore <ambari address> <ambari
admin username> <ambari admin password> <cluster_name> <full path of
HCP200-New>
```

14. Perform a diff between the old and new Metron Ambari state files:

```
diff -bur <folder container old Ambari state files> <folder containing new
Ambari state files>
```

**15.** Merge the json files together by hand and place the result in the HCP-200-upgrade folder (not the HCP200-new folder).

**16.** Push the saved configuration to the new Metron installation.

From the host on which Ambari is installed, enter:

```
cd HCP200-Upgrade
$METRON_HOME/bin/upgrade_helper.sh restore localhost:8080 <ambari admin
  username> <ambari admin password> <cluster_name>

scp -rp parser_contrib/* <INSTALLED_METRON_HOSTNAME>:$METRON_HOME/
  parser_contrib/

scp -rp metron-config/* <INSTALLED_METRON_HOSTNAME>:$METRON_HOME/config/
```

**17.** In Ambari, start Metron.

**18.** Push some data through Metron and monitor the indexed output to ensure correct operation.

**19.** Enable production feeds and monitor the indexed output to ensure correct operation.