

CCP Preparing for Upgrade 2.0.0

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
 Back up Your Configuration.....4
 Stop All Metron Services.....4

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.

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. You will also need to re-enter values for the Metron properties in Ambari.

Procedure

1. Create a backup directory.

```
mkdir /$HCP_BACKUP_DIRECTORY
```

2. Back up your configuration information in ZooKeeper to your backup directory:

```
${METRON_HOME}/bin/zk_load_configs.sh -m DUMP -z $ZOOKEEPER >  
/$HCP_BACKUP_DIRECTORY/$BACKUP_CONFIG.txt
```

3. Back up the following property files in the \$METRON_HOME/config directory to your backup directory:

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

For example:

```
cp elasticsearch.properties /$HCP_BACKUP_DIRECTORY/  
elasticsearch.properties
```

4. Copy the zookeeper directory to your backup directory:

```
cp -R zookeeper/ /$HCP_BACKUP_DIRECTORY/zookeeper
```

5. Back up your Metron configuration.

The easiest way to do this is to take a screenshot of each of the Metron configuration pages that you modified in Ambari. At a minimum, take a screen shot of the following configuration pages:

- Index Settings
- Parsers
- REST

Stop All Metron Services

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

Procedure

1. Stop all Metron services in Ambari.

Stop each Metron service in the following order:

- Metron Alerts UI
- Metron Management UI
- Metron REST

2. Stop Storm:

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

```
storm list
```

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.

3. 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 from \$METRON_HOME/var/log/metron/metron:

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

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