CCP Upgrading 2.0.1

Upgrading Metron

Date of publish: 2017-11-06

https://docs.cloudera.com/

Legal Notice

Contents

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.

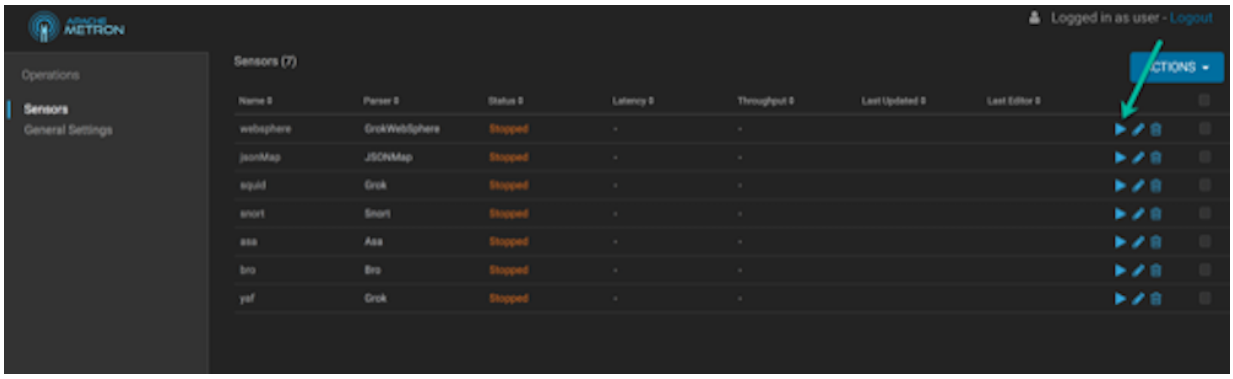
   ```
   ambari-server restart
   ```
6. Re-open Ambari and add the updated Metron version.

   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.

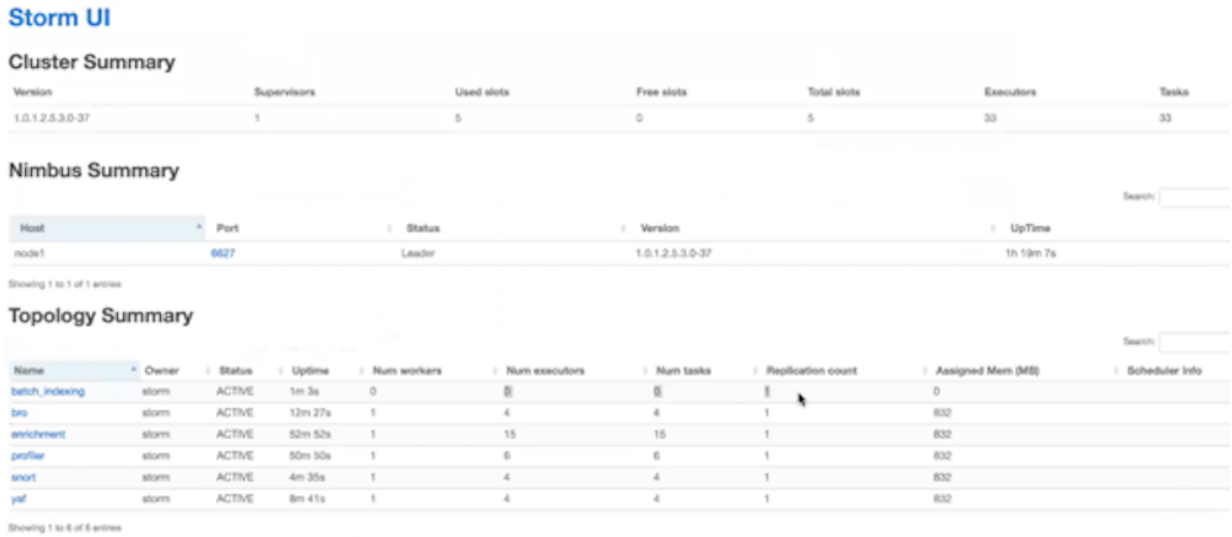
   The process to install, start, and test Metron will take a while.
9. Restart the Metron services:

   - 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.



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.