Upgrading Metron

Date of Publish: 2019-3-18

Contents

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

- Back up your Metron configuration.
- Stop all Metron services

Procedure

1. Uninstall Metron.

   In Ambari, select **Metron**, then under the **Service Actions** menu, click **Delete Service**.

   When prompted, enter "delete" to confirm deleting the service.

2. 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) Incorporate the input you received in the previous step into the following to list 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
   ```

c) Remove each of the packages:

```
rmp -e $PACKAGE_NAME
```

For example:

```
sudo chkconfig --del metron-management-ui
```

Ubuntu

From the Ambari node, enter the following to delete all of the Metron packages:

```
sudo aptitude purge $PACKAGE_NAME
```

3. Modify the /etc/yum.repos.d/HCP.repo file with the updated repo version:

```
vi /etc/yum.repos.d/HCP.repo
```

4. Update the HCP.repo file.
CentOS

```
yum update
```

Ubuntu

```
apt-get update
```

5. Install the current HCP mpack repo from Release Notes.

```
wget http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.9.0.0/
tars/metron/hcp-ambari-mpack-1.9.0.0-9.tar.gz
ambari-server install-mpack --force --mpack=/${MPACK_DOWNLOAD_DIRECTORY}/
hcp-ambari-mpack-1.9.0.0-9.tar.gz --verbose
```

6. Restart the Ambari server.

```
ambari-server restart
```

7. Re-open Ambari and add back 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.

8. Click yes to add each dependency.

9. 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.

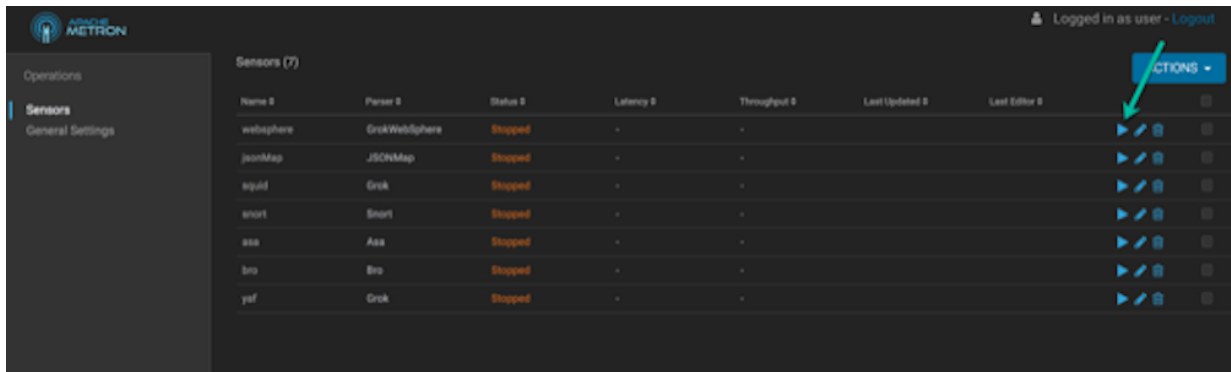**10.** Click **Deploy** to start the Metron set up.

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

11. Restart the Metron services:

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

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

Management UI

Note: Starting the Metron parsers might take a while.

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

Storm UI