Preparing to Upgrade HCP

Date of Publish: 2018-10-15

http://docs.hortonworks.com

Contents

Preparing to Upgrade

Hortonworks Cybersecurity Platform (HCP) 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 Hortonworks Cybersecurity Platform (HCP), you must back up your configuration and stop all Metron services.

Back up Your Configuration

The Hortonworks Cybersecurity Platform (HCP) 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/elasticsearch.properties
```

4. Copy the zookeeper directory to your backup directory:

```
cp -R zookeeper/ /$HCP_BACKUP/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 modifed 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 verifiy 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
   ```