Hortonworks Cybersecurity Platform

Upgrade Guide

(April 24, 2018)

docs.cloudera.com

Hortonworks Cybersecurity Platform: Upgrade Guide

Copyright © 2012-2018 Hortonworks, Inc. Some rights reserved.

Hortonworks Cybersecurity Platform (HCP) is a modern data application based on Apache Metron, powered by Apache Hadoop, Apache Storm, and related technologies.

HCP provides a framework and tools to enable greater efficiency in Security Operation Centers (SOCs) along with better and faster threat detection in real-time at massive scale. It provides ingestion, parsing and normalization of fully enriched, contextualized data, threat intelligence feeds, triage and machine learning based detection. It also provides end user near real-time dashboarding.

Based on a strong foundation in the Hortonworks Data Platform (HDP) and Hortonworks DataFlow (HDF) stacks, HCP provides an integrated advanced platform for security analytics.

Please visit the Hortonworks Data Platform page for more information on Hortonworks technology. For more information on Hortonworks services, please visit either the Support or Training page. Feel free to Contact Us directly to discuss your specific needs.



Except where otherwise noted, this document is licensed under Creative Commons Attribution ShareAlike 4.0 License. http://creativecommons.org/licenses/by-sa/4.0/legalcode

Table of Contents

1. Preparing to Upgrade	1
1.1. Backing up Your Configuration	1
1.2. Stopping All Metron Services	2
2. Upgrading Metron	3
3. Mandatory Post-Upgrade Tasks	6
3.1. Upgrading Your Configuration	6
3.2. Changes to STELLAR Language	6
4. Troubleshooting	7
4.1. Checking the Status of the Parsers	7

List of Figures

2.1.	Management UI	5
2.2.	Storm UI	5
4.1.	Ambari Summary Tab	7
4.2.	Ambari Background Operation Page	8
4.3.	Metron Parsers Start Page	9

1. Preparing to Upgrade

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

1.1. Backing up Your Configuration

The 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 need to 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.

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
 - profiler 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 modified in Ambari. At a minimum, take a screen shot of the following configuration pages:

- Index Settings
- Parsers
- REST

1.2. Stopping All Metron Services

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

1. Stop all Metron services in Ambari.

Stop each Metron service in the following order:

- Metron Alerts UI
- Metron Management UI
- Metron REST
- Storm

To stop Storm, complete the following steps:

a. Kill each Storm topology.

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

For example:

storm kill bro

c. Return to the Storm UI.

Verify that all topologies are killed.

- d. In Ambari, stop Storm by selecting Storm and clicking Stop All in the Actions menu.
- 2. 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 <code>\$METRON_HOME/var/log/metron/metron</code>:

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

2. Upgrading Metron

After you shut down Metron and all of its services, you must uninstall Metron and then reinstall the newest version of Metron.

Prerequisite

• Back up your Metron configuration.

See Backing up Your Configuration for more information.

• Stop all Metron services

See Stopping All Metron Services for more information.

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

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

rpm -e \$(rpm -qa | grep metron)

Remove each of the packages:

rmp remove \$PACKAGE_NAME

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.

For example:

```
wget http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.4.2.0/
tars/metron/hcp-ambari-mpack-1.4.2.0-18.tar.gz
ambari-server install-mpack --force --mpack=/${MPACK_DOWNLOAD_DIRECTORY}/
hcp-ambari-mpack-1.4.2.0-18.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.



Important

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.

Figure 2.1. Management UI

	METRON						🛔 Logge		
		Sensors (7)						спо	NS -
	Sensors				Throughput 0	Last Updated #		1	
1			GrokWebSphere					F18	
		jeonMap	JSONMap					►Z8	
								► Z 8	
								F 2 B	
								F 2 8	
								- F Z B	
			Grok					►ZB	



Note

Starting the Metron parsers might take a while.

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

Figure 2.2. Storm UI

Storm UI

Cluster Summary

Version	Supervisors	Used slots	Free slots	Total slots	Executors	Taska
1.0.1.2.5.3.0-37	1	5	0	5	53	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	i Status	Uptime	Num workers	Num executors	Num tasks	Replication count	Assigned Mem (MB)	Scheduler Info
betch_indexing	storm	ACTIVE	1m 3a	0	0	01	1	0	
bro	storm	ACTIVE	12m 27a	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	
trone	storm	ACTIVE	4m 35s	1	4	4	1	832	
yead	storm	ACTIVE	8m-41s	1	4	4	1	832	

Showing 1 to 6 of 6 entries

3. Mandatory Post-Upgrade Tasks

After you finish updating the Ambari M-Pack, depending on your configuration, you need to update the following features in your cluster:

- Upgrading Your Configuration [6]
- Changes to STELLAR Language [6]

3.1. Upgrading Your Configuration

The upgrade uses the default configuration for the new Metron version. If you made any changes to the Metron configuration in the previous version, incorporate those changes into the new Metron configuration by changing one or more of the following:

- Metron properties in Ambari
- ZooKeeper

Incorporate changes from the ZooKeeper file you backed up earlier.

• Flux files

Incorporate changes from the Flux files you backed up earlier.

3.2. Changes to STELLAR Language

HCP adds additional Stellar keywords to each new HCP version. These new keywords might cause compatablity issues where these reserved words and symbols are used in existing scripts. Be sure to check the Stellar Language Quick Reference for new and changed Stellar keywords.

HCP 1.4.2 adds match to the Stellar lanaguage which introduces the following new reserved keywords and symbols:

```
match, default, \{, \}, `=>'
```

You must modify any Stellar expressions that use these keywords not in quotes.

4. Troubleshooting

If you run into issues with your upgrade use the following troubleshooting tips to identify and resolve those issues.

4.1. Checking the Status of the Parsers

If your parsers do not restart, you can check the status of the parsers by completing the following steps:

1. Click the operation status tab at the top of the Ambari window.

Figure 4.1. Ambari Summary Tab

🔬 Ambari metro	n_ciu (1ee Ediets	Dashboard ¹⁰	Services	Hosts	Alerts	Admin		≜ admin •
HDFS YVAN MapReduce2 Tez	Summary Cgotos	Quick Links +					1	Service Actions • Restart •
 Hive Hibase Pig ZooKeeper Btorm Kafka Bpark Zoppein 	Summary Meton Alerta LI © Started Meton Enclohment © Started Meton Enclohment © Started Meton Indexing & Started Meton Nanoement LI © Started Meton Profiler © Started Meton Profiler © Started Meton Profiler © Started Meton Clant 1 Meton C	Na sianta Na sianta Na sianta Na sianta Na sianta Na sianta Na sianta						
Notebook Easticsearch Kibana Metron Silder Actions •								

Ambari displays the Operations Running Status window.

Figure 4.2. Ambari Background Operation Page

Operations	Start Time	Duration	Show: A	1(10)
0 Start Metron Parsers	Today 14:37	145.37 secs		15%
Start Metron Management UI	Today 14:35	£.73 secs		00%
Start Metron Alerts UI	Today 14:34	20.48 secs		100%
Start Metron REST	Today 14:33	8.60 secs		00%
Restart Metron REST	Today 14:32	19.48 secs		00%
Start Metron REST	Today 14:24	30.85 secs		00%
Start Added Services	Today 13:56	299.24 anca		00%
V Install Services	Today 13:48	465.22 secs		00%
Restart all components for MapReduce2	Today 13:34	33.18 secs		00%
Restart all components for HBase	Today 13:34	8.30 secs		00%
	Show	more		

2. Click Start Metron Parsers.

Ambari displays the **Start Metron Parsers** window.

3. Click the parser node you want to check, then click Metron Parsers Start.

Ambari displays information on the status of the parser.



← Tasks	O Metron Parsers Start	Copy C Open
stderr: /var/lib/ambari-agent/data/errors-302.b1		
stdout: /vav/lib/ambari-agent/data/output-302.bd		
2051 [main-EventThread] ISFO o.s.c.f.s.Connect 2692 [main] ESFO o.s.s.StormNubmitter - General 2925 [main] ESFO o.s.s.s.s.s.s.kuthUtils - Gos Aut 3100 [main] ESFO o.s.s.s.s.s.s.kuthUtils - Gos Aut 3100 [main] ESFO o.s.s.StormNubmitter - Upload (detai/Addoor/storm/inhus/inhus/stormJu-bl320 7831 [main] ESFO o.s.s.StormNubmitter - Succes her-s.4510.haad-blad1571HBsA2, jar 7437 [main] ESFO o.s.s.StormNubmitter - Submit ("storm.zookeeper.topology.suth.scheme's'storm 4556 [main] ESFO o.s.s.StormNubmitter - Finlas 2018-02-12 21:199:25,738 - Starting yaf 2018-02-12 21:199:25,748 - Execute '/usr/hcp/1.4 -s model:2181 'metron', 'try_sleep': 5] Running: /usr/jdk64/jdk1.s.0_77/bin/java -serv Djsvs.Iberary.math-/usr/icol.71/bb/ring-cors- 5.5.jar/usr/hdp/2.5.3.0-37/storm/11b/ring-cors 5.5.jar/usr/hdp/2.5.3.0-37/storm/11b/ring-cors 5.5.jar/usr/hdp/2.5.3.0-37/storm/11b/ring-cors 5.5.jar/usr/hdp/2.5.3.0-37/storm/11b/ring-cors 7/storm/11b/scokeeper.jar/usr/hdp/2.5.3.0-37/ 57/storm/11b/scokeeper.jar/usr/hdp/2.5.3.0-37/ 57/storm/11b/scokeeper.jar/usr/hdp/2.5.3.0-37/ 57/storm/11b/scokeeper.jar/usr/hdp/2.5.3.0-37/	<pre>tionBtateManager - State change: CONNECTED sted BooKeeper secret payload for MDS-digest: -5405670104303 occreents [] ding topology jar /tmp/ff193742103011e0Ebaf0800279b7065.jar 0744-be70-4570-baa6-bbed157dfaa2.jar esfully uploaded topology jar to assigned location: /data1/h tting topology hero is distributed mode with conf t; "storm.sockeeper.topology.auth.payload': "-540567010430311 bed submitting topology hero 4.1.0-18/metron/bin/start_parser_topology.sh -s yafksp FLAINTEX er -Ddaemon.name -Dstorm.home-/wsr/hdp/2.5 1bi/usr/hdp/2.5.3.0-37/storm.home-/wsr/hdp/2.5 5.3.0-37/storm/lib/disryb-3.0.3/str/wsr/hdp/2.5.3.0-37/storm/ -7/storm/lib/log9-core-2.1.jsr/wsr/hdp/2.5.3.0-37/storm/ /ar/storm/lib/log9-core-2.1.jsr/wsr/hdp/2.5.3.0-37/storm/ /ar/storm/lib/log9-core-2.1.jsr/wsr/hdp/2.5.3.0-37/storm/ /ar/storm/lib/log9-core-2.1.jsr/wsr/hdp/2.5.3.0-37/storm/ /ar/storm/lib/log9-core-2.1.jsr/wsr/hdp/2.5.3.0-37/storm/ /ar/storm/lib/log9-core-2.1.jsr/wsr/hdp/2.5.3.0-37/storm/ /ar/storm/lib/log9-core-2.1.jsr/wsr/hdp/2.5.3.0-37/storm/ /ar/storm/lib/log9-core-2.1.jsr/wsr/hdp/2.5.3.0-37/storm/ /ar/storm/lib/log9-core-2.1.jsr/wsr/hdp/2.5.3.0-37/storm/ /ar/storm/lib/log9-core-2.1.jsr/wsr/hdp/2.5.3.0-37/storm/ /ar/storm/lib/log9-core-2.1.jsr/wsr/hdp/2.5.3.0-37/storm/ /ar/storm/lib/log9-core-2.1.jsr/wsr/hdp/2.5.3.0-37/storm/ /ar/storm/lib/log9-core-2.1.jsr/wsr/hdp/2.5.3.0-37/storm/lib/ /dsr/ms/lib/log9-core-2.1.jsr/wsr/hdp/2.5.3.0-37/storm/lib/ /dsr/ms/lib/log9-core-2.1.jsr/wsr/hdp/2.5.3.0-37/storm/lib/ /dsr/ms/lib/log9-core-2.1.jsr/wsr/hdp/2.5.3.0-37/storm/lib/ /dsr/ms/lib/log9-core-2.1.jsr/wsr/hdp/2.5.3.0-37/storm/lib/ /dsr/ms/lib/log9-core-2.1.jsr/wsr/hdp/2.5.3.0-37/storm/lib/ /dsr/ms/ms/lib/log9-core-2.1.jsr/wsr/ms/lib/log9-core-2.1.4.1.0-18/ /msr/ms/lib/log9-core-2.1.jsr/wsr/hdp/2.5.3.0-37/storm/lib/ /dsr/ms/msr/msr/msr/msr/msr/msr/msr/msr/ms</pre>	<pre>115508:-7241442855444134715 to assigned location: adoop/storm/nisbus/isbox/stormjar-b192074f- 5508:-7241442855444134715')</pre>

4. Review the information in this window to determine the status of your parsers.