Release Notes 1

# Hortonworks Cybersecurity Platform

**Date of Publish:** 2018-07-30

**http://docs.hortonworks.com**

# Contents

# Hortonworks Cybersecurity Platform 1.6.0 Release Notes

This document provides you with the latest information about the Hortonworks Cybersecurity Platform (HCP) powered by Apache Metron release 1.6.0 and its product documentation.

## Apache Component Support

Hortonworks Cybersecurity Platform (HCP) 1.6.0 is built on HDP 2.6.4 and HDF 3.0.1.1 and later.

The official Apache versions of all HCP 1.6.0 components are:

- Apache Metron 0.5.0
- HDP supported component versions

All components listed are official Apache releases of the most recent stable versions available.

The Hortonworks approach is to provide patches only when necessary, to ensure the interoperability of components. Unless you are explicitly directed by Hortonworks Support to take a patch update, each of the HCP components should remain at the following package version levels, to ensure a certified and supported copy of HCP 1.6.0.

**Note:**

For information on open source software licensing and notices, refer to the Licenses and Notices files included with the software install package.

## New Features

HCP is a cybersecurity application framework that provides the ability to parse diverse security data feeds, enrich, triage, and store the data at scale, and detect cybersecurity anomalies.

HCP 1.6.0 provides the following new features:

- PCAP search panel

  Provides a graphical user interface to expand or refine your query by searching the PCAP data stored in HDFS.

## Support Matrix

HCP 1.6.0 supports a select set of operating system, database, browser, and JDK versions.

You can find the most current information about HCP's interoperability for this release on the Support Matrix. The Support Matrix tool provides information about:

- Operating Systems
- Databases
- Browsers
- JDKs

**Note:** HCP does not support Internet Explorer.

To access the tool, go to: https://supportmatrix.hortonworks.com"

## Unsupported Features

Although some features exist with HCP 1.6.0, Hortonworks does not support some community features and technical preview features.

### Community Features

Some community features are developed and tested by the Hortonworks community but are not officially supported by Hortonworks. These features are excluded for a variety of reasons, including insufficient reliability or incomplete test case coverage, declaration of non-production readiness by the community at large, and feature deviation from Hortonworks best practices. Do not use these features in your production environments.

#### Table 1: Community Features

| Feature | Description |
|---|---|
| Vagrant-based deployment | A single-node quick deployment option intended solely for development of Metron. |
| Docker-based deployment | A Docker-container based deployment intended solely for development of Metron. |
| Ansible installs | A multi-node deployment option via Ansible. |

### Technical Preview Features

Some features included in the HCP 1.6.0 release are not yet officially supported by Hortonworks. These technical preview features are still under development and are not recommended for a production environment.

#### Table 2: Technical Preview Features

| Feature | Description |
|---|---|
| Meta Alerts UI | The Meta Alerts UI feature with Solr is technical preview in this release. We do not yet recommend this for production use, but please let us know about any bugs you might find. We appreciate your feedback. |
| Stellar in Zeppelin | The ability to run Stellar commands in Zeppelin notebook |
| Event time profiling | Changes the behavioral profiling window to use the event time instead of system time. This better reflects the actual timing of the event and increases the accuracy of the profiles. |

## HCP 1.6.0 Repositories

You can download HCP 1.6.0 from HCP repository locations specific to the operating system you use.

Use the following table to identify the HCP 1.6.0 repo location for your operating system and operational objectives:

**Note:**

When installing Elasticsearch with the management pack on Ubuntu, you must manually install the Elasticsearch repositories. The management pack does not do this, like it does on CentOS.

#### Table 3: HCP Repo Locations

| OS | Format | Download Location |
|---|---|---|
| RedHat Enterprise Linux / CentOS 6 (64-bit) | Repo | http://public-repo-1.hortonworks.com/HCP/centos6/1.x/updates/1.6.0.0/hcp.repo |
| | HCP Management Pack | http://public-repo-1.hortonworks.com/HCP/centos6/1.x/updates/1.6.0.0/tars/metron/hcp-ambari-mpack-1.6.0.0-7.tar.gz |
| | Elasticsearch Management Pack | http://public-repo-1.hortonworks.com/HCP/centos6/1.x/updates/1.6.0.0/tars/metron/elasticsearch_mpack-1.6.0.0-7.tar.gz |
| RedHat Enterprise Linux / CentOS 7 (64-bit) | Repo | http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.6.0.0/hcp.repo |
| | HCP Management Pack | http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.6.0.0/tars/metron/hcp-ambari-mpack-1.6.0.0-7.tar.gz |

| OS | Format | Download Location |
|---|---|---|
| | Elasticsearch Management Pack | http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.6.0.0/tars/metron/elasticsearch_mpack-1.6.0.0-7.tar.gz |
| Ubuntu 14.04 | Repo | http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.6.0.0/hcp.list |
| | HCP Management Pack | http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.6.0.0/tars/metron/hcp-ambari-mpack-1.6.0.0-7.tar.gz |
| | Elasticsearch Management Pack | http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.6.0.0/tars/metron/elasticsearch_mpack-1.6.0.0-7.tar.gz |

## Upgrading to HCP 1.6.0

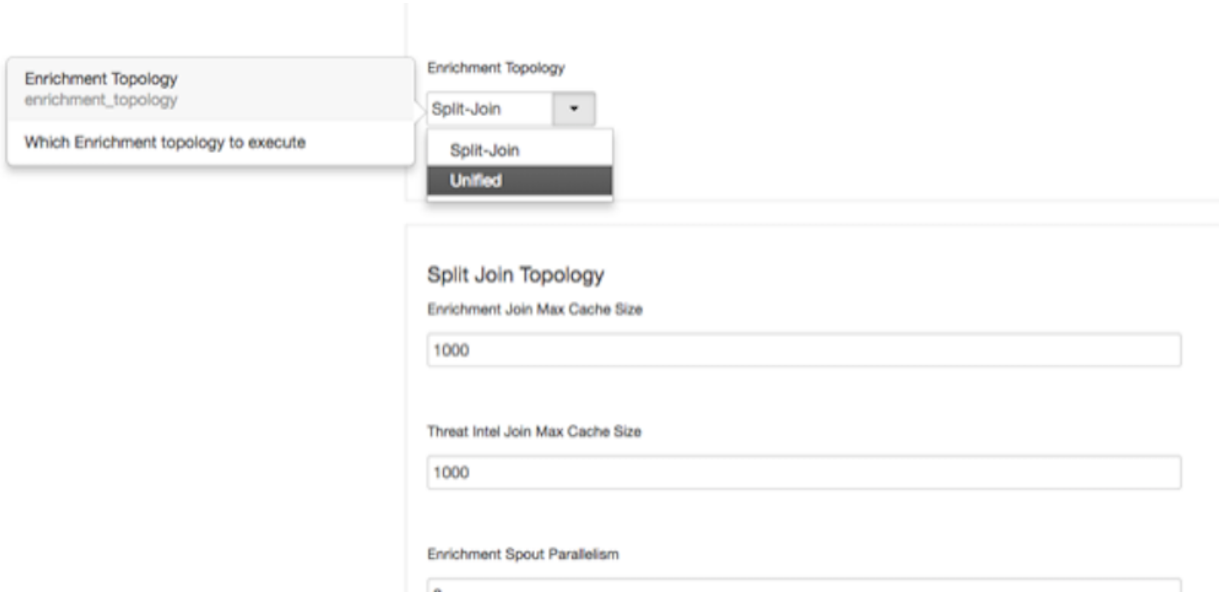
For information on how to upgrade to HCP 1.6.0 from a previous release, see Hortonworks Cybersecurity Platform Upgrade Guide.

## Switching to Unified Enrichment Topology (Technical Preview)

Switching from the current split-join enrichment topology to the new unified enrichment topology can reduce the latency of enrichment messages and avoid overloading the enrichment cache during times of heavy traffic.

### Procedure

1. Stop the Metron enrichment topology in Ambari.
   a) Click **Metron Enrichment** in the **Summary** list.
   b) Choose **Stop** from the menu next to **Metron Enrichment / Metron**.
2. In the **Enrichment** tab, choose **Unified** from the **Enrichment Topology** menu.




   Where appropriate, the unified topology reuses the same settings from the split-join topology.
3. Verify that the unified topology settings are appropriate for your system.
4. Restart the enrichment topology in Ambari.

## Third-Party Licenses

HCP deploys numerous third-party licenses and dependencies, all of which are compatible with the Apache software license. For complete third-party license information, see the licenses and notice files contained within the distribution.

**Related Information**

Apache 2.0

## Known Issues

The HCP 1.6.0 release has the following known issue:

- During HCP installation, some versions of Zeppelin might fail to install. If the Zeppelin notebooks are not installed, import the Apache Zeppelin Notebook manually.
- The Kerberization process might lock solr directories. If this occurs you will see the following message in the logs: is locked (lockType=hdfs). Throwing exception. and you will not see Solr alerts in the Alerts UI. If this issue occurs, remove the write.lock file located at /solr/bro/core_node1/data-index/write.lock or, in Ambari, navigate to **Solr > config > Advanced solr-hdfs** and check the **Delete write.lock files on HDFS** checkbox. After you have deleted the write.lock file, restart Solr.

**Related Information**

Importing the Apache Zeppelin Notebook Manually

### Known Differences Between HCP 1.6.0 and HCP 1.5.1

The following bugs identify known differences between HCP 1.6.0 and HCP 1.5.1.

**Table 4: Known Differences Between HCP 1.6.0 and HCP 1.5.1**

| Feature | Description |
|---|---|
| METRON-1236 | Add start/stop/restart commands that execute successfully, when ambari agents run as non-root user |
| METRON-1607 | Add a 'wrap' to incoming messages in the metron json parser |
| METRON-1619 | Stellar empty collections should be considered false in boolean expressions |
| METRON-1620 | Fixes for forensic clustering use case example |
| METRON-1621 | Sorting alerts table by score |
| METRON-1631 | Alerts UI: Dash score does not show if only filtering by one group |
| METRON-1635 | Alerts UI status update doesn't immediately show up |
| METRON-1636 | Fix broken unit test setup in metron-alerts |
| METRON-1642 | KafkaWriter should be able choose the topic from a field in addition to topology construction time |
| METRON-1643 | Create a REGEX_ROUTING field transformation |
| METRON-1644 | Support parser chaining |
| METRON-1645 | Check wether the Solr management pack is installed before configuring the solr principal name |
| METRON-1646 | Sensor Stubs should work when kerberized |
| METRON-1647 | Fix logging level score |
| METRON-1649 | Intermittent Test Failure ProfileBuilderBoltTest#testFlushExpiredProfiles |

| Feature | Description |
|---|---|
| METRON-1651 | Parser aggregation in storm |
| METRON-1652 | Document X-Pack Common Problem |
| METRON-1655 | Make REGEXP_MATCH take multiple regexs in the 2nd arg |
| METRON-1656 | Create KAKFA_SEEK function |
| METRON-1657 | Parser aggregation in storm |
| METRON-1658 | Upgrade bro to 2.5.4 |
| METRON-1659 | The platform-info.sh should check for the vagrant hostmanager plugin |
| METRON-1660 | On Solr, sorting by threat score fails |
| METRON-1670 | Stellar WEEK_OF_YEAR test is locale sensitive |
| METRON-1672 | Add metron-alerts's UI unit tests to travis build process |
| METRON-1673 | Fix Javadoc errors |
| METRON-1684 | Fix Markdown problems in 3rdPartyParser.md |

## Known Differences Between HCP 1.6.0 and Apache Metron 0.5.0

The following bugs identify known differences between HCP 1.6.0 and Apache 0.5.0.

### Table 5: Known Differences Between HCP 1.6.0 and Apache 0.5.0

| Feature | Description |
|---|---|
| METRON-1555 | Update REST to run YARN and MR jobs |
| METRON-1560 | Update MPack to support Pcap panel |
| METRON-1562 | Enable Kerberos in REST for YARN and MR jobs |
| METRON-1606 | Add a 'wrap' to incoming messages in the metron json parser |
| METRON-1614 | Create job status abstraction |
| METRON-1641 | Enable Pcap jobs to be submitted asynchronousl |
| METRON-1638 | Retrieve Pcap results in pdml format |
| METRON-1649 | Intermittent Test Failure ProfileBuilderBoltTest#testFlushExpiredProfiles |
| METRON-1651 | Parser aggregation in storm |
| METRON-1652 | Document X-Pack Common Problem |
| METRON-1655 | Make REGEXP_MATCH take multiple regexs in the 2nd arg |
| METRON-1656 | Create KAKFA_SEEK function |
| METRON-1661 | Create Pcap Query Filter endpoint |
| METRON-1672 | Add metron-alerts's UI unit tests to travis build process |
| METRON-1674 | Create REST endpoint for job status abstraction |
| METRON-1685 | Retrieve Pcap results in raw binary format |
| METRON-1686 | Create stop job endpoint for Pcap queries |
| METRON-1690 | Add more context to PcapJob JobStatus |
| METRON-1691 | REST should limit the number of Pcap jobs a user can submit |
| METRON-1693 | Fix Pcap CLI local FS finalizer |