HCP 1.8.0 Release Notes

Date of Publish: 2018-12-21

https://docs.hortonworks.com/

Contents

HCP Release Notes Introduction

This document provides you with the latest information about the Hortonworks Cybersecurity Platform (HCP) powered by Apache Metron release 1.8.0 and its product documentation.

Apache Component Support

Hortonworks Cybersecurity Platform (HCP) 1.8.0 is built on HDP 2.6.5 and HDF 3.0.1.1 and later.

The official Apache versions of all HCP 1.8.0 components are:

- Apache Metron 0.7.0
- 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 1.8.0.

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 1.8.0 provides the following new features:

- Support for Knox SSO
- LDAP authentication
- Performance improvements for Elasticsearch ingest: native Elasticsearch document IDs
- Support for generic REGEX parser
- Stellar shell-based parser debugging

Support Matrix

HCP 1.8.0 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”

Support for Elasticsearch (Optional)

- HCP 1.8.0 supports Elasicsearch version 5.6.2

JDK Support Matrix

HCP 1.8.0 supports a select set of Java Development Kits (JDK) versions.

Unless otherwise noted, the following Java Development Kits (JDKs) are validated and supported for HDP 2.6.5:

Table 1: HDP 2.6.5 JDK Support Matrix

JDK	Version
Open Source	JDK8†
Oracle	JDK 8

†Not validated, but supported.

Deprecation Notices

This section points out any technology from previous releases that have been deprecated, moved, or removed from this release. Use this section as a guide for your implementation plans.

Terminology

Items in this section are designated as follows:

Items in this section are designated as follows:

Deprecated	Technology that Hortonworks is removing in a future HCP release. Marking an item as deprecated gives you time to plan for removal in a future HCP release.
Moving	Technology that Hortonworks is moving from a future HCP release and is making available through an alternative Hortonworks offering or subscription. Marking an item as moving gives you time to plan for removal in a future HCP release and plan for the alternative Hortonworks offering or subscription for the technology.
Removed	Technology that Hortonworks has removed from HCP and is no longer available or supported as of this release. Take note of technology marked as removed since it can potentially affect your upgrade plans.

Deprecation Notices

The following component is deprecated in this HCP release.

Support for split-join topology	Support for the split-join topology is deprecated as of the HCP 1.7.1 release and will be removed in HCP 1.9.0. The unified enrichment topology is now the default.

Unsupported Features

Although some features exist with HCP 1.8.0, 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 2: 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 1.8.0 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 3: Technical Preview Features

Feature	Description
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 1.8.0 Repositories

You can download HCP 1.8.0 from HCP repository locations specific to the operating system you use.

Use the following table to identify the HCP 1.8.0 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 4: 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/1.8.0.0/hcp.repo
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/centos6/1.x/updates/1.8.0.0/tars/metron/hcp-ambari-mpack-1.8.0.0-58.tar.gz
	Elasticsearch Management Pack	http://public-repo-1.hortonworks.com/HCP/centos6/1.x/updates/1.8.0.0/tars/metron/elasticsearch_mpack-1.8.0.0-58.tar.gz
	Solr Management Pack	http://public-repo-1.hortonworks.com/HDP-SOLR/hdp-solr-ambari-mp/solr-service-mpack-3.0.0.tar.gz
RedHat Enterprise Linux / CentOS 7 (64-bit)	Repo	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.8.0.0/hcp.repo
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.8.0.0/tars/metron/hcp-ambari-mpack-1.8.0.0-58.tar.gz
	Elasticsearch Management Pack	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.8.0.0/tars/metron/elasticsearch_mpack-1.8.0.0-58.tar.gz
	Solr Management Pack	http://public-repo-1.hortonworks.com/HDP-SOLR/hdp-solr-ambari-mp/solr-service-mpack-3.0.0.tar.gz
Ubuntu 14.04	Repo	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.8.0.0/hcp.list
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.8.0.0/tars/metron/hcp-ambari-mpack-1.8.0.0-58.tar.gz
	Elasticsearch Management Pack	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.8.0.0/tars/metron/elasticsearch_mpack-1.8.0.0-58.tar.gz
	Solr Management Pack	http://public-repo-1.hortonworks.com/HDP-SOLR/hdp-solr-ambari-mp/solr-service-mpack-3.0.0.tar.gz

Upgrading to HCP 1.8.0

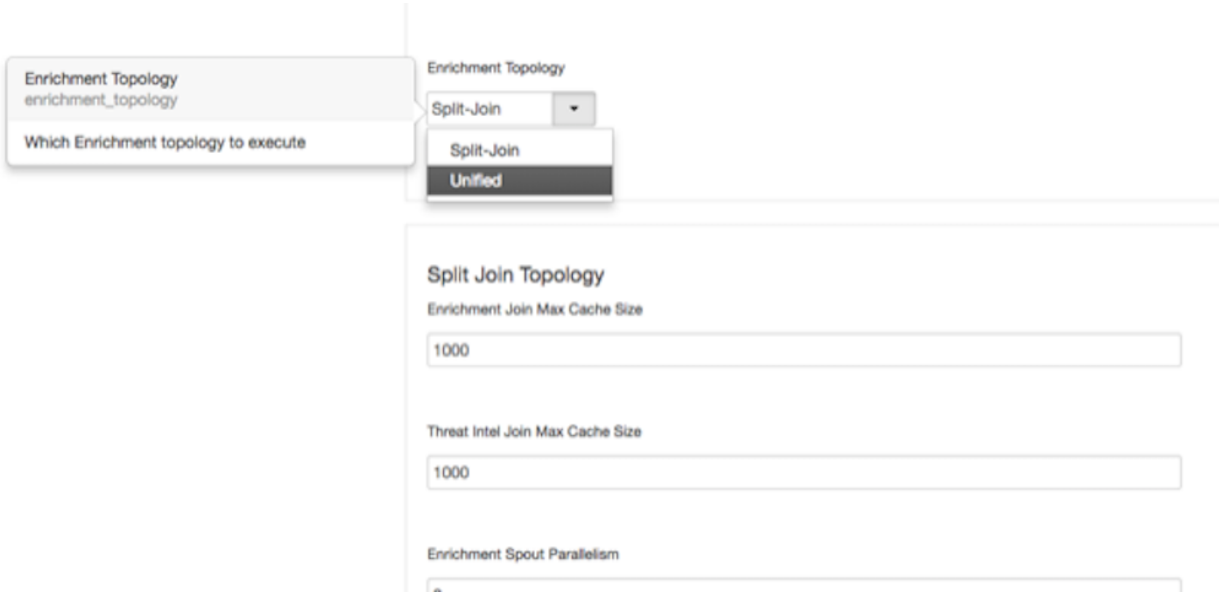
For information on how to upgrade to HCP 1.8.0 from a previous release, see Hortonworks Cybersecurity Platform Upgrade Guide.

Switching to Unified Enrichment Topology

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.

Unified Topology Output

The timestamp output from the unified topology differs from the timestamp output from the split-join topology because the unified toplogy does not have split and join bolts.
The timestamp output from the unified topology will be similar to the following:

```
Adapter timestamps
```

```
"adapter:geoadapter:begin:ts": "1542882553866",
  "adapter:geoadapter:end:ts": "1542882553866",
  "adapter:threatinteladapter:begin:ts": "1542882553869",
  "adapter:threatinteladapter:end:ts": "1542882553870",
  "adapter:hostfromjsonlistadapter:begin:ts": "1542882553866",
  "adapter:hostfromjsonlistadapter:end:ts": "1542882553866"
```

```
Enrichment bolt timestamps
```

```
"parallelenricher:enrich:begin:ts": "1542882553869",
  "parallelenricher:enrich:end:ts": "1542882553870",
  "parallelenricher:splitter:begin:ts": "1542882553869",
  "parallelenricher:splitter:end:ts": "1542882553869"
```

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 1.8.0 release has the following known issues:

- 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.
- When running a large sized PCAP query, the REST API can die silently if the result set exceeds the memory available to the REST server.
- On Kerberized clusters Storm rebalances can fail to correctly distribute tickets. This can be resolved by running storm upload-credentials against each topology.

Known Differences Between HCP 1.8.0 and HCP 1.7.1

The following bugs identify known differences between HCP 1.7.0 and HCP 1.7.1.

Table 5: Known Differences Between HCP 1.8.0 and HCP 1.7.1

Feature	Description
METRON-1936	Cypress fails when trying to parse double quotes
METRON-1815	Separate metron-parsers into metron-parsers-common and metron-parsers-storm
METRON-1932	Update ES and Kibana to 5.6.14
METRON-1938	Add Parser Debugger to READMEs
METRON-1925	Support Column Oriented Input with Batch Profiler
METRON-1795	General Purpose Regex Parser
METRON-1892	Parser Debugger Should Load Config From Zookeeper
METRON-1937	Update public web site to point at 0.7.0 new release
METRON-1879	Allow Elasticsearch to Auto-Generate the Document ID
METRON-1930	Update webpack-dev-server in Alerts UI
METRON-1849	Elasticsearch Index Write Functionality Should be Shared
METRON-1938	Bump Metron version to 0.7.0 for release
METRON-1931	Update dev utilities to support new repo location
METRON-1922	Escaping incorrectly handled in current aesh version
METRON-1867	Remove `/api/v1/update/replace` endpoint
METRON-1810	Storm Profiler Intermittent Test Failure
METRON-1909	Remove http filter from release utils changelog generation
METRON-1869	Unable to Sort an Escalated Meta Alert
METRON-1889	Add any missing timestamp fields to unified enrichment topology

Feature	Description
METRON-1913	Build broken by missing transitive dependency
METRON-1845	Correct Test Data Load in Elasticsearch Integration Tests
METRON-1888	Default Topology Settings in MPack Cause Profiler to Stall
METRON-1887	Add logging to the ClasspathFunctionResolver
METRON-1873	Update Bootstrap version in Management UI
METRON-1825	Upgrade bro to 2.5.5
METRON-1890	Metron Vagrant should disable audio
METRON-1874	Create a Parser Debugger
METRON-1880	Use Caffeine for Profiler Caching
METRON-1877	Nested IF ELSE statements can cause parse errors in Stellar
METRON-1872	Move rat plugin away from snapshot version
METRON-1875	Expose configurable global settings in the Alerts UI
METRON-1834	Migrate Elasticsearch from TransportClient to new Java REST API
METRON-1749	Update Angular to latest release in Management UI
METRON-1870	Intermittent Stellar REST test failures
METRON-1868	metron-committer-common incorrectly checking REPO_NAME
METRON-1740	Improve Palo Alto parser to handle CONFIG and SYSTEM syslog messages

Known Differences Between HCP 1.8.0 and Apache Metron 0.7.0

There are no known differences between HCP 1.8.0 and Apache Metron 0.7.0.

Table 6: Known Differences Between HCP 1.8.0 and Apache Metron 0.7.0

Feature	Description
METRON-1936	Cypress fails when trying to parse double quotes
METRON-1815	Separate metron-parsers into metron-parsers-common and metron-parsers-storm
METRON-1932	Update ES and Kibana to 5.6.14
METRON-1938	Add Parser Debugger to READMEs
METRON-1925	Provide Verbose View of Profile Results in REPL
METRON-1795	General Purpose Regex Parser
METRON-1892	Parser Debugger Should Load Config From Zookeeper
METRON-1937	Update public web site to point at 0.7.0 new release
METRON-1879	Allow Elasticsearch to Auto-Generate the Document ID
METRON-1930	Update webpack-dev-server in Alerts UI
METRON-1849	Elasticsearch Index Write Functionality Should be Shared