Release Notes

Date of Publish: 2018-10-15

http://docs.hortonworks.com

Contents

Hortonworks Cybersecurity Platform 1.7.0 Release Notes

This document provides you with the latest information about the Hortonworks Cybersecurity Platform (HCP) powered by Apache Metron release 1.7.0 and its product documentation.

Apache Component Support

Hortonworks Cybersecurity Platform (HCP) 1.7.0 is built on HDP 2.6.4 and HDF 3.0.1.1 and later.

The official Apache versions of all HCP 1.7.0 components are:

- Apache Metron 0.6.0
- 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 1.7.0.

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 1.7.0 provides the following new features:

- Batch profiling - Running profiler against historical data to prewarming and restating baselines
- Configure PCAP in Ambari during installation

Support Matrix

HCP 1.7.0 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”

JDK Support Matrix

HCP 1.5.0 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 2.6.4:

Table 1: HDP 2.6.4 JDK Support Matrix

JDK	Version
Open Source	JDK8†
Oracle	JDK 8

†Not validated, but supported.

Unsupported Features

Although some features exist with HCP 1.7.0, 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 1.7.0 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
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 1.7.0 Repositories

You can download HCP 1.7.0 from HCP repository locations specific to the operating system you use.

Use the following table to identify the HCP 1.7.0 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/1.7.0.0/hcp.repo
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/centos6/1.x/updates/1.7.0.0/tars/metron/hcp-ambari-mpack-1.7.0.0-38.tar.gz
	Elasticsearch Management Pack	http://public-repo-1.hortonworks.com/HCP/centos6/1.x/updates/1.7.0.0/tars/metron/elasticsearch_mpack-1.7.0.0-38.tar.gz
RedHat Enterprise Linux / CentOS 7 (64-bit)	Repo	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.7.0.0/hcp.repo
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.7.0.0/tars/metron/hcp-ambari-mpack-1.7.0.0-38.tar.gz
	Elasticsearch Management Pack	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.7.0.0/tars/metron/elasticsearch_mpack-1.7.0.0-38.tar.gz
Ubuntu 14.04	Repo	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.7.0.0/hcp.list
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.7.0.0/tars/metron/hcp-ambari-mpack-1.7.0.0-38.tar.gz
	Elasticsearch Management Pack	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.7.0.0/tars/metron/elasticsearch_mpack-1.7.0.0-38.tar.gz

Upgrading to HCP 1.7.0

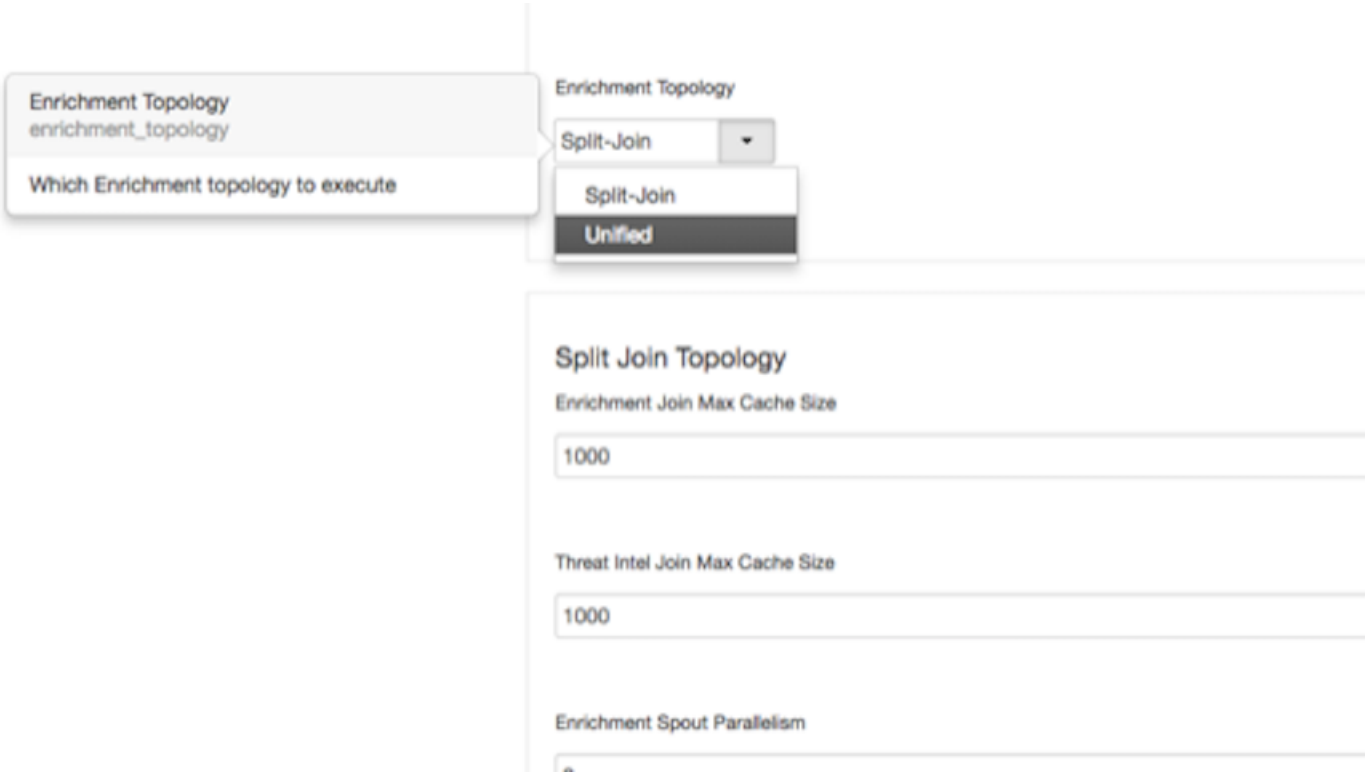
For information on how to upgrade to HCP 1.7.0 from a previous release, see Hortonworks Cybersecurity Platform Upgrade Guide.

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 1.7.0 release has the following known issues:

- To avoid out of memory errors in the indexing topology, set the Ambari Metron Indexing properties **Indexing Max Pending for Random Access** and **Indexing Max Pending for HDFS** to 300.
- 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.

Known Differences Between HCP 1.7.0 and HCP 1.6.1

The following bugs identify known differences between HCP 1.7.0 and HCP 1.6.1.

Table 5: Known Differences Between HCP 1.7.0 and HCP 1.6.1

Feature	Description
METRON-1761	Allow a grok statement to be applied to each line in a file.
METRON-1813	Stellar REPL Not Initialized with Client JAAS
METRON-1812	Fix dependencies_with_url.csv
METRON-1811	Alert Search Fails When Sorting by Alert Status
METRON-1809	Support Column Oriented Input with Batch Profiler
METRON-1806	Upgrade Maven Shade Plugin version
METRON-1792	Simplify Profile Definitions in Integration Tests
METRON-1807	Auto populate the recommended values to some of the metron config parameters
METRON-1808	Add Ansible created pyc to gitignore
METRON-1695	Expose pcap properties through Ambari
METRON-1771	Update REST endpoints to support eventually consistent UI updates
METRON-1791	Add GUID to Messages Produced by Profiler
METRON-1804	Update version to 0.6.1
METRON-1798	Add mpack support for parser aggregation
METRON-1750	Create Parser for Syslog RFC 5424 Messages
METRON-1794	Include User Details When Escalating Alerts
METRON-1782	Add Kafka Partition and Offset to Profiler Debug Logs
METRON-1758	Add support for Ansible 2.6 in dev
METRON-1699	Create Batch Profiler
METRON-1787	Input Time Constraints for Batch Profiler
METRON-1508	In Ubuntu14 Dev Indexing Fails to Write to Elasticsearch
METRON-1786	Pcap Topology Status Incorrect
METRON-1709	Add controls to start / stop the PCAP topology from Ambari.
METRON-1759	PCAP UI: Removing wrong Input annotations from pcap panel component
METRON-1772	Support alternative input formats in the Batch Profiler
METRON-1770	Add Docs for Running the Profiler with Spark on YARN
METRON-1774	Allow user to configure JAAS client in Ambari
METRON-1760	Kill PCAP job should prompt for confirmation
METRON-1777	Fix Elasticsearch X-Pack sample pom in documentation
METRON-1699	create-batch-profiler
METRON-1780	Fix broken website images
METRON-1476	Update to Angular 6.1.3
METRON-1776	Update public web site to point at 0.6.0 new release
METRON-1775	Transient exception could prevent expired profiles from being flushed
METRON-1717	Relocate Storm Profiler Code
METRON-1748	Improve Storm Profiler Integration Test
METRON-1764	Update version to 0.6.0

Feature	Description
METRON-1741	Move REPL Port of Profiler to Separate Project
METRON-1757	Storm Profiler Serialization Exception
METRON-1743	CEF testPaloAltoCEF test using a confusing variable name
METRON-1715	Create DEB Packaging for Batch Profiler
METRON-1736	Enhance Batch Profiler Integration Test
METRON-1714	Create RPM Packaging for the Batch Profiler
METRON-1752	Prevent package.lock from changing during build
METRON-1708	Run the Batch Profiler in Spark
METRON-1724	Date/time validation missing in PCAP query
METRON-1707	Port Profiler to Spark
METRON-1705	Create ProfilePeriod Using Period ID
METRON-1706	HbaseClient.mutate should return the number of mutations
METRON-1704	Message Timestamp Logic Should be Shared
METRON-1703	Make Core Profiler Components Serializable

Known Differences Between HCP 1.7.0 and Apache Metron 0.6.0

There are no known differences between HCP 1.7.0 and Apache Metron 0.6.0.

Table 6: Known Differences Between HCP 1.7.0 and Apache Metron 0.6.0

Feature	Description
METRON-1769	Script creation of a release candidate.
METRON-1761	Allow a grok statement to be applied to each line in a file.
METRON-1813	Stellar REPL Not Initialized with Client JAAS
METRON-1812	Fix dependencies_with_url.csv
METRON-1811	Alert Search Fails When Sorting by Alert Status
METRON-1809	Support Column Oriented Input with Batch Profiler
METRON-1806	Upgrade Maven Shade Plugin version
METRON-1792	Simplify Profile Definitions in Integration Tests
METRON-1807	Auto populate the recommended values to some of the metron config parameters
METRON-1808	Add Ansible created pyc to gitignore
METRON-1695	Expose pcap properties through Ambari
METRON-1771	Update REST endpoints to support eventually consistent UI updates
METRON-1791	Add GUID to Messages Produced by Profiler
METRON-1804	Update version to 0.6.1
METRON-1798	Add mpack support for parser aggregation
METRON-1750	Create Parser for Syslog RFC 5424 Messages
METRON-1794	Include User Details When Escalating Alerts
METRON-1782	Add Kafka Partition and Offset to Profiler Debug Logs
METRON-1758	Add support for Ansible 2.6 in dev

Feature	Description
METRON-1699	Create Batch Profiler
METRON-1784	Re-allow remote ssh and scp in Centos full dev
METRON-1787	Input Time Constraints for Batch Profiler
METRON-1508	In Ubuntu14 Dev Indexing Fails to Write to Elasticsearch
METRON-1786	Pcap Topology Status Incorrect
METRON-1709	Add controls to start / stop the PCAP topology from Ambari.
METRON-1759	PCAP UI: Removing wrong Input annotations from pcap panel component
METRON-1772	Support alternative input formats in the Batch Profiler
METRON-1770	Add Docs for Running the Profiler with Spark on YARN
METRON-1774	Allow user to configure JAAS client in Ambari
METRON-1760	Kill PCAP job should prompt for confirmation
METRON-1777	Fix Elasticsearch X-Pack sample pom in documentation
METRON-1781	Fix RPM Spec File
METRON-1780	Fix broken website images
METRON-1476	Update to Angular 6.1.3
METRON-1776	Update public web site to point at 0.6.0 new release
METRON-1775	Transient exception could prevent expired profiles from being flushed
METRON-1717	Relocate Storm Profiler Code
METRON-1748	Improve Storm Profiler Integration Test