Release Notes

Date of Publish: 2018-11-15

http://docs.hortonworks.com

Contents

Hortonworks Cybersecurity Platform 1.7.1 Release Notes

This document provides you with the latest information about the Hortonworks Cybersecurity Platform (HCP) powered by Apache Metron release 1.7.1 and its product documentation.

Apache Component Support

Hortonworks Cybersecurity Platform (HCP) 1.7.1 is built on HDP 2.6.4 through 2.6.5 and HDF 3.0.1.1 and later.

The official Apache versions of all HCP 1.7.1 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 1.7.1.

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 1.7.1 provides the following new features:

- Supports LDAP integration for authentication of user interfaces and REST API
- Integration for HTTP-based enrichments via Stellar HTTP client
- Batch profiling - Running profiler against historical data to prewarming and restating baselines
- Configure PCAP in Ambari during installation

Support Matrix

HCP 1.7.1 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 1.7.1 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.

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 enrichment topology is deprecated as of the HCP 1.7.1 release. The unified enrichment topology is now the default which is recommended for all users.

Unsupported Features

Although some features exist with HCP 1.7.1, 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 1.7.1 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

HCP 1.7.1 Repositories

You can download HCP 1.7.1 from HCP repository locations specific to the operating system you use.

Use the following table to identify the HCP 1.7.1 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/1.7.1.0/hcp.repo
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/centos6/1.x/updates/1.7.1.0/tars/metron/hcp-ambari-mpack-1.7.1.0-24.tar.gz
	Elasticsearch Management Pack	http://public-repo-1.hortonworks.com/HCP/centos6/1.x/updates/1.7.1.0/tars/metron/elasticsearch_mpack-1.7.1.0-24.tar.gz

OS	Format	Download Location
	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/1.7.1.0/hcp.repo
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.7.1.0/tars/metron/hcp-ambari-mpack-1.7.1.0-24.tar.gz
	Elasticsearch Management Pack	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.7.1.0/tars/metron/elasticsearch_mpack-1.7.1.0-24.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/1.7.1.0/hcp.list
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.7.1.0/tars/metron/hcp-ambari-mpack-1.7.1.0-24.tar.gz
	Elasticsearch Management Pack	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.7.1.0/tars/metron/elasticsearch_mpack-1.7.1.0-24.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 1.7.1

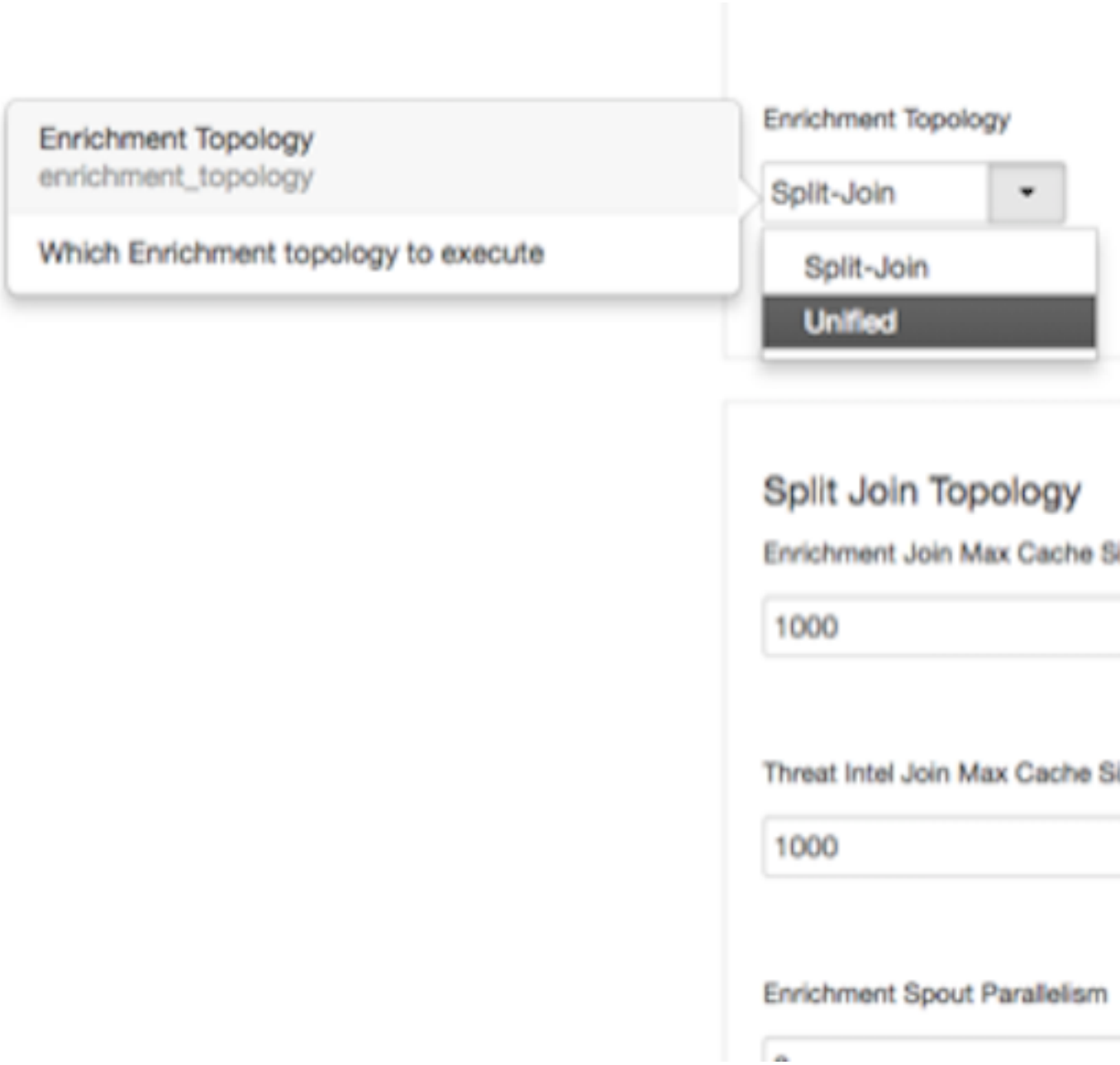
For information on how to upgrade to HCP 1.7.1 from a previous release, see Hortonworks Cybersecurity Platform Upgrade Guide.

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.

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 1.7.1 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 1.7.1 and HCP 1.7.0

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

Table 5: Known Differences Between HCP 1.7.1 and HCP 1.7.0

Feature	Description
METRON-1847	Create reusable script with functions from prepare-commit
METRON-1850	Stellar REST function
METRON-1858	BasicFireEyeParser check style cleanup and optimization
METRON-1864	Stellar date format test fails after daylight saving
METRON-1861	REST fails to start when LDAP enabled and 'Active Spring profiles' config is empty
METRON-1853	Add shutdown hook to Stellar BaseFunctionResolver
METRON-1857	Fix Metaalert Nested Alert Field Name in Index Template
METRON-1855	Make unified enrichment topology the default and deprecate split-join
METRON-1790	Unsubscribe from every observable in the pcap panel UI component
METRON-1803	Integrate Cypress with Travis
METRON-1844	Allow for LDAP to be used for authentication and roles
METRON-1830	Re-implement Alerts dialog box without jQuery
METRON-1801	Allow Customization of Elasticsearch Document ID
METRON-1826	Update librdkafka and devtoolset
METRON-1839	Install Elasticsearch MPack Step in Ansible Not Idempotent
METRON-1833	Management UI incorrectly displaying sensor topology latency units as seconds instead of millis
METRON-1829	Large Error Message Causes Slow Search Performance
METRON-1831	Project Version Substitution Not Working
METRON-1816	Date format Stellar function
METRON-1681	Decouple the ParserBolt from the Parse execution logic
METRON-1820	Update to new Simple-Syslog-5424 version to support error handling
METRON-1805	Provide a default value for the Storm topology.max.spout.pending setting
METRON-1821	Align prepare-release-candidate with documentation

Feature	Description
METRON-1801	Allow Customization of Elasticsearch Document ID
METRON-1799	Remove outdated bylaws from site.

Known Differences Between HCP 1.7.1 and Apache Metron 0.6.0

There are no known differences between HCP 1.7.1 and Apache Metron 0.6.0.

Table 6: Known Differences Between HCP 1.7.1 and Apache Metron 0.6.0

Feature	Description
METRON-1847	Create reusable script with functions from prepare-commit
METRON-1850	Stellar REST function
METRON-1858	BasicFireEyeParser check style cleanup and optimization
METRON-1864	Stellar date format test fails after daylight saving
METRON-1861	Add shutdown hook to Stellar BaseFunctionResolver
METRON-1857	Fix Metaalert Nested Alert Field Name in Index Template
METRON-1855	Make unified enrichment topology the default and deprecate split-join
METRON-1790	Unsubscribe from every observable in the pcap panel UI component
METRON-1803	Integrate Cypress with Travis
METRON-1844	Allow for LDAP to be used for authentication and roles
METRON-1830	Re-implement Alerts dialog box without jQuery
METRON-1801	Allow Customization of Elasticsearch Document ID
METRON-1826	Update librdkafka and devtoolset
METRON-1839	Install Elasticsearch MPack Step in Ansible Not Idempotent
METRON-1833	Management UI incorrectly displaying sensor topology latency units as seconds instead of millis
METRON-1829	Large Error Message Causes Slow Search Performance
METRON-1831	Project Version Substitution Not Working
METRON-1816	Date format Stellar function
METRON-1681	Decouple the ParserBolt from the Parse execution logic
METRON-1820	Update to new Simple-Syslog-5424 version to support error handling
METRON-1805	Provide a default value for the Storm topology.max.spout.pending setting
METRON-1821	Align prepare-release-candidate with documentation
METRON-1801	Allow Customization of Elasticsearch Document ID
METRON-1799	Remove outdated bylaws from site.