Release Notes 1

Hortonworks Cybersecurity Platform

Date of Publish: 2018-08-23

http://docs.hortonworks.com

Contents

Hortonworks Cybersecurity Platform 1.6.1 Release Notes

This document provides you with the latest information about the Hortonworks Cybersecurity Platform (HCP) powered by Apache Metron release 1.6.1 and its product documentation.

Apache Component Support

Hortonworks Cybersecurity Platform (HCP) 1.6.1 is built on HDP 2.6.4 and HDF 3.0.1.1 and later.

The official Apache versions of all HCP 1.6.1 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 1.6.1.

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 1.6.1 provides the following new features:

- PCAP search panel

Support Matrix

HCP 1.6.1 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”

Unsupported Features

Although some features exist with HCP 1.6.1, 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 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 1.5.0 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 1.6.1 Repositories

You can download HCP 1.6.1 from HCP repository locations specific to the operating system you use.

Use the following table to identify the HCP 1.6.1 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 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/1.6.1.0/hcp.repo
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/centos6/1.x/updates/1.6.1.0/tars/metron/hcp-ambari-mpack-1.6.1.0-23.tar.gz
	Elasticsearch Management Pack	http://public-repo-1.hortonworks.com/HCP/centos6/1.x/updates/1.6.1.0/tars/metron/elasticsearch_mpack-1.6.1.0-23.tar.gz
RedHat Enterprise Linux / CentOS 7 (64-bit)	Repo	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.6.1.0/hcp.repo
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.6.1.0/tars/metron/hcp-ambari-mpack-1.6.1.0-23.tar.gz

OS	Format	Download Location
	Elasticsearch Management Pack	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.6.1.0/tars/metron/elasticsearch_mpack-1.6.1.0-23.tar.gz
Ubuntu 14.04	Repo	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.6.1.0/hcp.list
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.6.1.0/tars/metron/hcp-ambari-mpack-1.6.1.0-23.tar.gz
	Elasticsearch Management Pack	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.6.1.0/tars/metron/elasticsearch_mpack-1.6.1.0-23.tar.gz

Upgrading to HCP 1.6.1

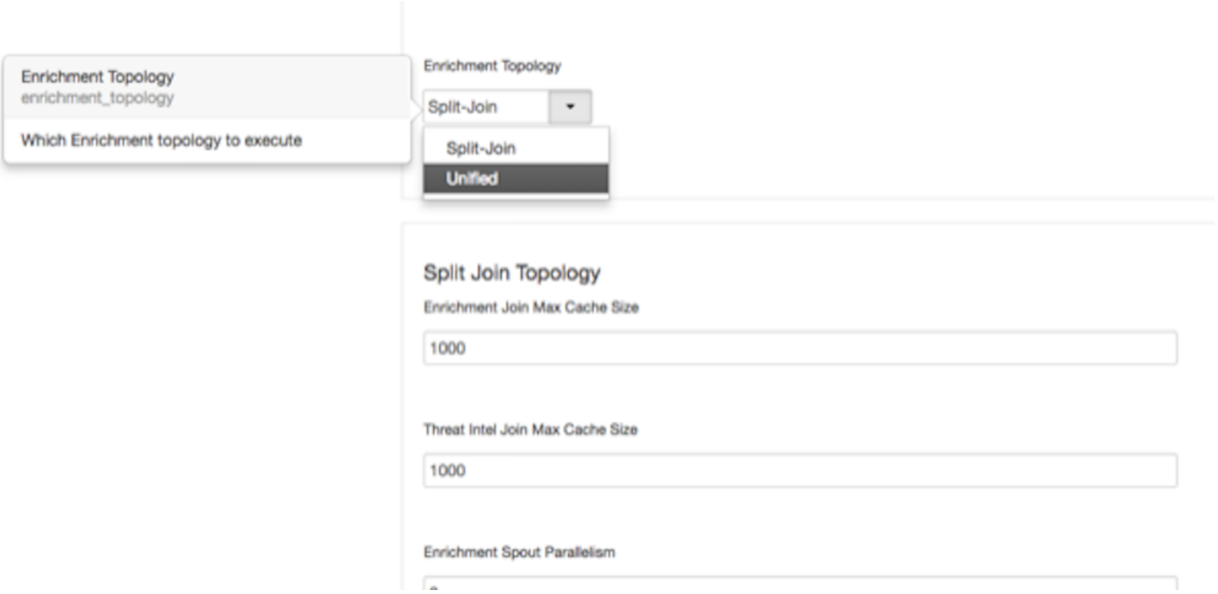
For information on how to upgrade to HCP 1.6.1 from a previous release, see Hortonworks Cybersecurity Platform Upgrade Guide.

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.



Enrichment Topology
enrichment_topology
Which Enrichment topology to execute

Enrichment Topology: Split-Join

Split Join Topology

Enrichment Join Max Cache Size: 1000

Threat Intel Join Max Cache Size: 1000

Enrichment Spout Parallelism

   Where appropriate, the unified topology reuses the same settings from the split-join topology.
3. Restart the enrichment topology in Ambari.

Note: Switching to the unified enrichment topology will require some tuning changes for your system.

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 1.6.1 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.

Related Information

Importing the Apache Zeppelin Notebook Manually

Known Differences Between HCP 1.6.1 and HCP 1.6.0

The following bugs identify known differences between HCP 1.6.1 and HCP 1.6.0.

Table 4: Known Differences Between HCP 1.6.1 and HCP 1.6.0

Feature	Description
METRON-1725	Add ability to specify YARN queue for pcap jobs
METRON-1731	Escape colons in output dir names
METRON-1702	Reload a running job in the UI
METRON-1722	PcapCLI should print progress to stdout
METRON-1730	Update steps to run pycapa on Centos 6
METRON-1713	PCAP UI - Add a way to kill a pcap job
METRON-1723	PCAP UI - Unable to select/copy from packets details in PCAP query panel
METRON-1712	PCAP UI - Input validation
METRON-1720	Better error messages when there are no results or wireshark is not installed
METRON-1726	Refactor PcapTopologyIntegrationTest
METRON-1683	PCAP UI - Fix the download progress bar
METRON-1675	PCAP UI - Introduce the paging capability
METRON-1721	New default input path is wrong in pcap CLI
METRON-1662	PCAP UI - Downloading PCAP page files
METRON-1700	Create REST endpoint to get job configuration
METRON-1671	Create PCAP UI

Feature	Description
METRON-1701	Update General notes on the installation of Pycapa on Kerberized cluster
METRON-1650	Packaging docker containers are too large
METRON-1640	Add RHEL 7 power pc to OS family for the HCP management pack repo info
METRON-1694	Clean up Metron REST docs