Hortonworks Cybersecurity Package

Release Notes

(August 18, 2017)

docs.cloudera.com

Hortonworks Cybersecurity Package: Release Notes

Hortonworks Cybersecurity Package (HCP) is a modern data application based on Apache Metron, powered by Apache Hadoop, Apache Storm, and related technologies.

HCP provides a framework and tools to enable greater efficiency in Security Operation Centers (SOCs) along with better and faster threat detection in real-time at massive scale. It provides ingestion, parsing and normalization of fully enriched, contextualized data, threat intelligence feeds, triage and machine learning based detection. It also provides end user near real-time dashboards.

Based on a strong foundation in the Hortonworks Data Platform (HDP) and Hortonworks DataFlow (HDF) stacks, HCP provides an integrated advanced platform for security analytics.

Please visit the Hortonworks Data Platform page for more information on Hortonworks technology. For more information on Hortonworks services, please visit either the Support or Training page. Feel free to Contact Us directly to discuss your specific needs.

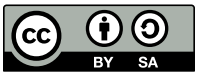

Table of Contents

List of Tables

1. Hortonworks Cybersecurity Suite 1.2.2 Release Notes

This document provides you with the latest information about the Hortonworks Cybersecurity Package (HCP) powered by Apache Metron release 1.2.2 and its product documentation.

1.1. Apache Component Support

Component Versions

HCP is built on HDP 2.5.3 and HDF 2.1.2 . HCP supports HDP 2.5.x and 2.6.x. The official Apache versions of all HCP 1.2.2 components are:

- Apache Metron 0.4.0
- 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 1.2.2.

Note

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

1.2. 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 1.2.2 provides the following new features:

- Support for Fastcapa both in a regular and Kerberized environment

- Alerts user interface
  - Displaying alerts
  - Searching alerts
  - Saving searches
  - Viewing your recent and saved searches
  - Configuring Alerts table
- New Tuning Guide
- Significant performance improvement for parsing
- M-pack support for Management Module
- Additional Zeppelin dashboards
  - Bro Data
  - IP Investigation
  - PC Query Interface
- PCAP filtering options
  - Binary regular expression (regex) searches
  - PCAP querying by Stellar expression

1.3. Platform Support Matrices

This section outlines the platform support matrices for HCP 1.2.2.

1.3.1. Operating System Support Matrix

Unless otherwise noted, the following operating systems are validated and supported for HDP 2.5.3: (HCP supports HDP 2.5.x and HDP 2.6.x.)

Table 1.1. HDP 2.5.3 Operating System Support Matrix

Operating System	Version
CentOS (64-bit)	CentOS 6.x and CentOS 7.x
Red Hat (64-bit)	RHEL 7.0†
Ubuntu	Ubuntu 14.04

†Not validated, but supported.

1.3.2. JDK Support Matrix

Unless otherwise noted, the following Java Development Kits (JDKs) are validated and supported for HDP 2.5.3:

Table 1.2. HDP 2.5.3 JDK Support Matrix

JDK	Version
Open Source	JDK8[† ‡]
Oracle	JDK 8

[†]Not validated, but supported.

1.4. Unsupported Features

Although the following features exist within HCP 1.2.2, Hortonworks does not currently support these specific capabilities:

- Technical Preview Features [3]
- Community Features [3]

1.4.1. Technical Preview Features

The following features are available within HCP 1.2.2 but are not ready for production deployment. Hortonworks encourages you to explore these technical preview features in non-production environments and provide feedback on your experiences through the Hortonworks Community Forums.

Table 1.3. Technical Previews

Feature	Description
Stellar REPL	A REPL (Read Eval Print Loop) for the Stellar language helps in debugging, troubleshooting, and learning Stellar. Stellar transforms streaming data within Apache Storm. This REPL is intended to help facilitate creation of configurations and transformations by allowing a user to replicate data and transformations encountered in production, with rapid feedback.
Alerts user interface	A standalone user interface that connects to Elasticsearch to display alerts. You can use this UI to search alerts, save your searches, and modify the Alerts table to display Alerts in a helpful format.

1.4.2. Community Features

The following 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 1.4. Community Features

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

1.5. HCP 1.2.2 Repositories

Use the following table to identify the HCP 1.2.2 repo location for your operating system and operational objectives:

Table 1.5. 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/1.2.2.0/hcp.repo
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/centos6/1.x/updates/1.2.2.0/tars/metron/hcp-ambari-mpack-1.2.2.0-2.tar.gz
RedHat Enterprise Linux / CentOS 7 (64-bit)	Repo	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.2.2.0/hcp.repo
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.2.2.0/tars/metron/hcp-ambari-mpack-1.2.2.0-2.tar.gz
Ubuntu 14.04	Repo	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.2.2.0/hcp.list
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.2.2.0/tars/metron/hcp-ambari-mpack-1.2.2.0-2.tar.gz

1.6. Upgrading to HCP 1.2.2

Upgrade instructions to HCP 1.2.2 are not currently documented. For informationon about upgrading HCP, contact Hortonworks Professional Services.

For a list of configuration changes that are non-backwards compatible, see Apache Metron Upgrading.

1.7. Third-Party Licenses

Global: Apache 2.0

Apache Component	Subcomponents	License
Storm	Logback	EPL

1.8. Known Issues

The HCP 1.2.2 release has the following known issues:

Alerts UI	ACTIONS menu - The status buttons are non-functional.
Alert Status	The alert-status column displays **New** as the status for all alerts, even if the alert status is not New.
After installing the Management Module user interface, some directory permissions are incorrect.	To fix this issue, complete the following tasks: 1. Run the following on the management UI host: `find /usr/hcp/current/metron/web/ -type d -exec chmod a+x {} \;` 2. Restart the Management Module UI.

1.8.1. Known Differences Between HCP 1.2.2 and Apache Metron 0.4.0

The following Apache bugs identify known differences between HCP 1.2.2 and Apache Metron 0.4.0.

- METRON-988 UI for viewing alerts generated by Metron
- METRON-1001 Allow metron to ingest parser metadata along with data
- METRON-1011 Enforce submission of 4 params Stellar ENRICHMENT functions #628
- METRON-986 Enhance Fastcapa to improve interoperability with the Intel X520 NIC
- METRON-1012 Update Metron public web site for 0.4.0 release
- METRON-1014 StellarShell class name typo
- METRON-990 Clean up and organize flux properties
- METRON-508 Expand Elasticsearch templates to support the stand bro logs
- METRON-1007 Ship the metron-management jar as part of the mpack install
- METRON-877 Extract core implementation and UDF support, create metron-stellar module
- METRON-1004 Travis CI - Job exceeded maximum time limit
- METRON-999 Add virtualization support checks to platform-info.sh

1.9. Documentation Errata

There are no late additions or corrections to the product documentation for this release.