Hortonworks Cybersecurity Package

Release Notes

(April 13, 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.

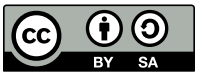

Table of Contents

List of Tables

1. Hortonworks Cybersecurity Suite 1.1.0 Release Notes

This document provides you with the latest information about the Hortonworks Cybersecurity Package (HCP) powered by Apache Metron release 1.1.0 and its product documentation.

1.1. Apache Component Support

Component Versions

HCP is built on HDP 2.5.3 and HDF 2.1.2 . The official Apache versions of all HCP 1.1.0 components are:

- Apache Metron 0.3.1
- 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 1.1.0.

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 1.1.0 provides the following new features:

- Support for running HCP in a Kerberos environment
- Significant improvements to Management module
  - Threat triage configuration
  - Enrichment configuration
- Support for full numeric types in Stellar .
- Support for Common Event Format (CEF) parser.
- HyperLogLogPlus (HLLP) sketches for Stellar and profiler for cardinality estimations.

  Now you can answer questions like "# of distinct IPs did this user connect to?" in triage rules.
- Geo enrichment no longer relies on MySQL.
- Removed all dependencies on MySQL simplifying licensing and installation.
- Performance improvements for enrichment loading.
- Stellar transformations are now enabled in enrichment loading.
- Stability and robustness improvements to the profiler and core Stellar functions.
- Indexes can be turned on and off at the sensor granularity (for example, you can write to HDFS without writing to Elasticsearch).
- Support for Zeppelin notebooks.

1.3. Platform Support Matrices

This section outlines the platform support matrices for HCP 1.1.0.

1.3.1. Operating System Support Matrix

Unless otherwise noted, the following operating systems are validated and supported for HDP 2.5.3:

Table 1.1. HDP 2.5.3 Operating System Support Matrix

Operating System	Version
CentOS (64-bit)	CentOS 6.0 and CentOS 7.0
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 1.1.0, 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 1.1.0 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.

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 1.1.0 Repositories

Use the following table to identify the HCP 1.1.0 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/1.1.0.0/hcp.repo
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/centos6/1.x/updates/1.1.0.0/tars/metron/hcp-ambari-mpack-1.1.0.0-71.tar.gz
RedHat Enterprise Linux / CentOS 7 (64-bit)	Repo	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.1.0.0/hcp.repo
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.1.0.0/tars/metron/hcp-ambari-mpack-1.1.0.0-71.tar.gz
Ubuntu 14.04	Repo	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.1.0.0/hcp.list
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.1.0.0/tars/metron/hcp-ambari-mpack-1.1.0.0-71.tar.gz

1.6. Upgrading to HCP 1.1.0

For information on how to upgrade to HCP 1.1.0 from a previous release, see http://metron.apache.org/current-book/Upgrading.html.

1.7. Third-Party Licenses

Global: Apache 2.0

Apache Component	Subcomponents	License
Storm	Logback	EPL

1.8. Known Differences Between HCP 1.1.0 and Apache Metron 0.3.1

The following Apache bugs identify known differences between HCP 1.1.0 and Apache Metron 0.3.1.

- METRON-839 RPM build should happen after archives are built (merrimanr) closes apache/incubator-metron#522
- METRON-829 Use Fastcapa with Kerberos (nickwallen) closes apache/incubator-metron#514
- METRON-831 Add lambda expressions and rudimentary functional programming primitives to Stellar. This closes apache/incubator-metron#517
- METRON-817 Customise output file path patterns for HDFS indexing (justinleet) closes apache/incubator-metron#505
- METRON-826 Ambari MPack should utilize service specific repos closes apache/incubator-metron#515
- METRON-827 Fix full dev build dependency multi-threading issue with maven (mmiklavc) closes apache/incubator-metron#513
- METRON-822 Improve Fastcapa Performance (nickwallen) closes apache/incubator-metron#509

- METRON-823 bro-plugin-kafka/README.md has Markdown usages not compatible with site-book closes apache/incubator-metron#511
- METRON-820 StellarProcessor should have a static expression cache. This closes apache/incubator-metron#508
- METRON-808 Amazon EC2 deployment fails at Expanding Volume Step (KunalAggarwal via mmiklavc) closes apache/incubator-metron#496
- METRON-196 Deployment Fails Without Ansible 2.0.0.2 closes apache/incubator-metron#499
- METRON-814 minor tweaks in document format of Kerberos-setup.md (mattf-horton) closes apache/incubator-metron#502
- METRON-642 Correct path to ES gc log file (DimDroll via mattf-horton) closes apache/incubator-metron#406
- METRON-815 sensor-stubs sometimes send malformed bro timestamps (JonZeolla via jonzeolla) closes apache/incubator-metron#503
- METRON-818 Ambari elasticsearch.properties template is missing topology.worker.childopts (justinleet) closes apache/incubator-metron#506
- METRON-812 Make the bro-kafka plugin work with kerberos this closes apache/incubator-metron#501
- METRON-810 Add Jon Zeolla to the Metron website community and project status pages (JonZeolla via jonzeolla) closes apache/incubator-metron#498
- METRON-816 Add jmeyer to Contributor List (jjmeyer0) closes apache/incubator-metron#504
- METRON-804 Create a document to describe kerberizing vagrant (mmiklavc) closes apache/incubator-metron#497
- METRON-796 Mpack uses wrong group for owning HDFS directories (justinleet) closes apache/incubator-metron#488
- METRON-773 Intermittent unit test errors in the KafkaControllerIntegrationTest this closes apache/incubator-metron#491
- METRON-797: Pass security.protocol and enable auto-renew for the storm topologies closes apache/incubator-metron#495
- METRON-797 Pass security.protocol and enable auto-renew for the storm topologies
- METRON-797 Pass security.protocol and enable auto-renew for the storm topologies
- METRON-793 Migrate to storm-kafka-client kafka spout from storm-kafka closes apache/incubator-metron#486
- METRON-700 Add hadoop container to metron-docker (kylerichardson) closes apache/incubator-metron#472

- METRON-806 Posix for long file names is required on all assembly plugin configurations - metron-rest edition (ottobackwards) closes apache/incubator-metron#494
- METRON-807 Changed resources to use non-relative path (simonellistonball via merrimanr) closes apache/incubator-metron#493
- Add mattf to committer list on site (mattf-horton) closes apache/incubator-metron#492
- METRON-765 Add GUID to messages (iraghumitra via cestella) closes apache/incubator-metron#483
- METRON-770 Unable to Launch Fastcapa Test Environment (nickwallen via cestella) closes apache/incubator-metron#480
- METRON-771 Stellar INDEXING_SET_BATCH incorrectly defaults batchSize to 5 closes apache/incubator-metron#485
- METRON-792 Quick Dev should remove/replace RPM packages closes apache/incubator-metron#487
- METRON-791 Add links to website and downloads to top level POM (justinleet) closes apache/incubator-metron#482
- METRON-769 Cisco ASA parser doesn't include syslog wrapper fields (simonellistonball via kylerichardson) closes apache/incubator-metron#479
- METRON-767 Clean up license (cestella via justinleet) closes apache/incubator-metron#478
- METRON-766 Release 0.3.1 closes apache/incubator-metron#477
- METRON-764 DST bug in metron-profiler-client Unit Tests (mattf-horton) closes apache/incubator-metron#476
- METRON-671 Refactor existing Ansible deployment to use Ambari MPack (dlyle via justinleet) closes apache/incubator-metron#436
- METRON-641 Fix Kibana install file (DimDroll via ottobackwards) closes apache/incubator-metron#405
- METRON-755 Update GitHub PR Template closes apache/incubator-metron#471
- METRON-752 Fix documentation typos and MD issues closes apache/incubator-metron#470
- METRON-745 Create Error Dashboards (justinleet via cestella) closes apache/incubator-metron#475
- METRON-712 Separate evaluation from parsing in Stellar this closes apache/incubator-metron#473
- METRON-758 HdfsServiceImplTest should sort files for list test (merrimanr via ottobackwards) closes apache/incubator-metron#474
- METRON-694 Index Errors from Topologies (merrimanr) closes apache/incubator-metron#453

- METRON-744 Allow Stellar functions to be loaded from HDFS this closes apache/incubator-metron#468
- METRON-701 Triage Metrics Produced by the Profiler (nickwallen) closes apache/incubator-metron#449
- METRON-503 Metron REST API this closes apache/incubator-metron#316
- METRON-503 Metron REST API this closes apache/incubator-metron#316
- METRON-503 Metron REST API this closes apache/incubator-metron#316
- METRON-743 Sort the files when reading results from Pcap closes apache/incubator-metron#467
- METRON-646 Add index templates to metron-docker (kylerichardson) closes apache/incubator-metron#441
- Revert "METRON-646 Add index templates to metron-docker (kylerichardson via merrimanr) closes apache/incubator-metron#441"
- METRON-686 Record Rule Set that Fired During Threat Triage (nickwallen) closes apache/incubator-metron#438
- METRON-646 Add index templates to metron-docker (kylerichardson via merrimanr) closes apache/incubator-metron#441
- METRON-742 Generated code for profile window selector DSL did not get committed as part of METRON-690 closes apache/incubator-metron#466
- METRON-741: Stellar Field Transformations should execute all of the transformations, not just the output closes apache/incubator-metron#465
- METRON-740 Normalizing and adding log4j properties override where possible. closes apache/incubator-metron#464
- METRON-728 ReaderSpliteratorTest fails randomly and extremely rarely closes apache/incubator-metron#463
- METRON-733 Remove Geo database from ParserBolt (justinleet via cestella) closes apache/incubator-metron#461
- METRON-690 Create a DSL-based timestamp lookup for profiler to enable sparse windows closes apache/incubator-metron#450
- METRON-734 Builds failing because of MaxMind DB transitive dependency (justinleet via cestella) closes apache/incubator-metron#462
- METRON-636 Capture memory and cpu details as a part of platform-info script (anandsubbu via nickwallen) closes apache/incubator-metron#400
- METRON-157 Create CEF Parser (simonellistonball via kylerichardson) closes apache/incubator-metron#451
- METRON-725 Javadoc is broken by the use of apiNote (justinleet) closes apache/incubator-metron#458

- METRON-715: Removed MySQL from Enrichment Diagram closes apache/incubator-metron#452
- METRON-720 modify generate-md.sh to re-throw errors from within 'find' closes apache/incubator-metron#455
- METRON-730 Fix links to mailings list on landing Apache Metron homepage (anandsubbu via cestella) closes apache/incubator-metron#460
- METRON-705 Parallelize the build in travis to the extent that is obvious closes apache/incubator-metron#444
- METRON-724 Account for `in` grammar in Stellar Documentation and Unit Tests (ottobackwards) closes apache/incubator-metron#457
- METRON-721 Add Github pull request template to help submitters and reviewers (ottobackwards) closes apache/incubator-metron#456
- METRON-716 Add README.md to site-book (ottobackwards) closes apache/incubator-metron#454
- METRON-708 Update metron documentation closes apache/incubator-metron#447
- METRON-710 Rev MPack Version to 0.3.1.0 (justinleet) closes apache/incubator-metron#448
- METRON-707 Correct ansible to execute threat intel bulk loading via the flat file script closes apache/incubator-metron#446
- METRON-706 Add Stellar transformations and filters to enrichment and threat intel loaders (mmiklavc via cestella) closes apache/incubator-metron#445

1.9. Documentation Errata

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