Hortonworks Cybersecurity Package

Release Notes

(November 22, 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.

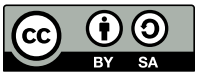

Table of Contents

List of Tables

1. Hortonworks Cybersecurity Suite 1.3.2 Release Notes

This document provides you with the latest information about the Hortonworks Cybersecurity Package (HCP) powered by Apache Metron release 1.3.2 and its product documentation.

1.1. Apache Component Support

Component Versions

HCP is built on HDP 2.6.0 and HDF 3.0.1.1 and later. The official Apache versions of all HCP 1.3.2 components are:

- Apache Metron 0.4.1
- 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 1.3.2.

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 1.3.2 provides the following new features:

- Alerts user interface
  - Displaying alerts

- Searching alerts
- Saving searches
- Viewing your recent and saved searches
- Configuring Alerts table
- The ability to group alerts into meta-alerts
- Adding comments
- Alert status based workflow
- Ability to escalate alerts to external ticketing systems

- Significant performance improvement for parsing
- M-pack based installation and configuration for Profiling
- Performance improvement for Indexing
- Additional geospatial and hash functions in Stellar
- Short circuit evaluation and multi-line Stellar statements

1.3. Platform Support Matrices

This section outlines the platform support matrices for HCP 1.3.2.

- Section 1.3.1, "Operating System Support Matrix" [2]
- Section 1.3.2, "JDK Support Matrix" [2]

1.3.1. Operating System Support Matrix

Unless otherwise noted, the following operating systems are validated and supported for HDP 2.6.2:

Table 1.1. HDP 2.6.2 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 14.0

[†]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 2.6.0:

Table 1.2. HDP 2.6.0 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 1.3.2, Hortonworks does not currently support these specific capabilities:

- Community Features [3]

1.4.1. 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 1.3. 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.

1.5. HCP 1.3.2 Repositories

Use the following table to identify the HCP 1.3.2 repo location for your operating system and operational objectives:

Table 1.4. 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/1.3.2.0/hcp.repo
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/centos6/1.x/updates/1.3.2.0/tars/hcp_ambari_mp/hcp-ambari-mpack-1.3.2.0-3.tar.gz
RedHat Enterprise Linux / CentOS 7 (64-bit)	Repo	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.3.2.0/hcp.repo
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.3.2.0/tars/hcp_ambari_mp/hcp-ambari-mpack-1.3.2.0-3.tar.gz
Ubuntu 14	Repo	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.3.2.0/hcp.list
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.3.2.0/tars/metron/hcp-ambari-mpack-1.3.2.0-3.tar.gz

1.6. Upgrading to HCP 1.3.2

For Elasticsearch 2.x, the existing indexes and templates need to upgraded. For more information, see:

- Updating Elasticsearch Templates
- Updating Existing Indexes

For information on how to upgrade to HCP 1.3.2 from a previous release, 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 1.3.2 release has no known issues.

For a list of known differences between HCP 1.3.2 and Apache Metron 0.4.1, see the following Section 1.8.1, “Known Differences Between HCP 1.3.2 and Apache Metron 0.4.1” [4].

1.8.1. Known Differences Between HCP 1.3.2 and Apache Metron 0.4.1

The following Apache bugs identify known differences between HCP 1.3.2 and Apache Metron 0.4.1.

Table 1.5. Known Differences Between HCP 1.3.2 and Apache Metron 0.4.1

Feature	Description
METRON-632	Added validation of "shew.enrichmentType" and "shew.keyColumns" closes apache/incubator-metron#732
METRON-938	"service metron-rest start <password>" does not work on CentOS 7. (justinleet) closes apache/metron#757
METRON-1052	Add forensic similarity hash functions to Stellar closes apache/incubator-metron#781
METRON-1055	Metron 0.4.0 manual installation guide for CentOS 6 updates (lvets via ottobackwards) closes apache/metron#661
METRON-1059	Address checkstyle warning AvoidStarImport in metron-stellar (dbist via ottobackwards) closes apache/metron#664
METRON-1063	Address javadoc warnings in metron-stellar (dbist via ottobackwards) closes apache/metron#668
METRON-1079	STELLAR NaN should be a keyword (ottobackwards) closes apache/metron#681

Feature	Description
METRON-1080	Fix Alerts and Ops UI Notices file (james-sirota) closes apache/metron#682
METRON-1081	Fix Alerts and Ops UI Notices file (james-sirota) closes apache/metron#682
METRON-1083	Add filters using faceted search capabilities of metron-rest-api (iraghumitra via james-sirota) closes apache/metron#710
METRON-1085	Add REST endpoint to save a user profile for the Alerts UI (merrimanr) closes apache/metron#694
METRON-1114	Add group by capabilities to search REST endpoint (merrimanr) closes apache/metron#702
METRON-1123	Add group by option using faceted search capabilities of metron-rest-api (iraghumitra via james-sirota) closes apache/metron#768
METRON-1146	Add ability to parse JSON string into JSONObject for stellar closes apache/incubator-metron#727
METRON-1153	HDFS HdfsWriter never recovers from exceptions closes apache/incubator-metron#741
METRON-1156	Simulate Triage Rules in the Stellar REPL (nickwallen) closes apache/metron#733
METRON-1158	Build backend for grouping alerts into meta alerts (justinleet) closes apache/metron#734
METRON-1161	Add ability to edit parser command line options in the management UI (merrimanr) closes apache/metron#737
METRON-1163	RAT failures for metron-interface/metron-alerts closes apache/incubator-metron#743
METRON-1167	Define Session Specific Global Configuration Values in the REPL (nickwallen) closes apache/metron#740
METRON-1168	Add SUBSTRING method to stellar this closes apache/incubator-metron#742
METRON-1169	Dependency checker has not been running in travis closes apache/incubator-metron#744
METRON-1171	Better validation for the SUBSTRING stellar function closes apache/incubator-metron#745
METRON-1173	Fix pointers to old stellar docs closes apache/incubator-metron#746
METRON-1176	REST: HDFS Service should support setting permissions on files when writing (ottobackwards) closes apache/metron#749
METRON-1177	Stale running topologies seen post-kerberization and cause exceptions (nickwallen) closes apache/metron#748
METRON-1179	Make STATS_ADD to take a list closes apache/incubator-metron#750
METRON-1180	Make Stellar Shell accept zookeeper quorum as a CSV list and not require a port closes apache/incubator-metron#751
METRON-1182	Refactor Code in alert list to accommodate new view types (iraghumitra via merrimanr) closes apache/metron#756
METRON-1183	Improve KDC Setup Instructions (nickwallen) closes apache/metron#753
METRON-1185	Stellar REPL does not work on a kerberized cluster when calling functions interacting with HBase closes apache/incubator-metron#755

Feature	Description
METRON-1186	Profiler Functions use classutils from shaded storm closes apache/incubator-metron#758
METRON-1187	Indexing/Profiler Kafka ACL Groups Not Setup Correctly (nickwallen) closes apache/metron#759
METRON-1188	Ambari global configuration management (mmiklavc) closes apache/metron#760
METRON-1189	Add alert escalation to the Alerts UI (merrimanr) closes apache/metron#762
METRON-1190	Fix Meta Alert Type handling in calculation of scores (justinleet) closes apache/metron#763
METRON-1191	Update public web site to point at 0.4.1 new release (mattf-horton) closes apache/metron#764
METRON-1194	Add Profiler Debug Functions to Profiler README (nickwallen via ottobackwards) closes apache/metron#765
METRON-1195	Meta alerts improperly handle updates to non-alert fields (justinleet) closes apache/metron#766
METRON-1196	Increment master version number to 0.4.2 for on-going development (mattf-horton) closes apache/metron#767
METRON-1198	Pycapa - No such configuration property 'sasl.kerberos.principal' (nickwallen) closes apache/metron#769
METRON-1202	ElasticsearchDao Has extraneous sleep call (justinleet) closes apache/metron#770
METRON-1204	UI does not time out after being idle, but stops functioning (merrimanr) closes apache/metron#771
METRON-1206	Make alerts UI conform to ops UI for install (merrimanr) closes apache/metron#773
METRON-1207	Make RPMs for Alerts UI (merrimanr) closes apache/metron#777
METRON-1208	MPack for Alerts UI (merrimanr) closes apache/metron#778
METRON-1209	Make stellar repl take logging properties, like other CLI apps in metron closes apache/incubator-metron#772
METRON-1215	Fix link to RPMs chapter (DimDroll via justinleet) closes apache/metron#776
METRON-1218	Metron REST should return better error messages (merrimanr) closes apache/metron#779
METRON-1220	Create documentation around alert nested field (justinleet) closes apache/metron#780
METRON-1222	Fix warning for The expression ${parent.version} is deprecated. Please use ${project.parent.version} instead. (dbist via mmiklavc) closes apache/metron#782
METRON-1223	Add support to add comments for alerts (iraghumitra via james-sirota) closes apache/metron#788
METRON-1224	Add time range selection to search control (iraghumitra via james-sirota) closes apache/metron#796
METRON-1226	Searching Can Errantly Query the Wrong Indices (nickwallen) closes apache/metron#793
METRON-1228	Configuration Management PUSH immediately does DUMP after (mmiklavc via mmiklavc) closes apache/metron#783
METRON-1229	Management UI type is part of the declarations of 2 modules (merrimanr) closes apache/metron#784

Feature	Description
METRON-1232	Alert status changes are not reflected in list view (iraghumitra via merrimanr) closes apache/metron#787
METRON-1234	Fix for WARNING 'dependencies.dependency. (groupId:artifactId:type:classifier)' must be unique: org.apache.hadoop:hadoop-yarn-api:jar (dbist via mmiklavc) closes apache/metron#790
METRON-1235	Document the properties pulled from the global configuration closes apache/incubator-metron#791
METRON-1237	Address javadoc warnings in metron-maas-common (dbist via james-sirota) closes apache/metron#792
METRON-1240	Address javadoc warnings in metron-platform and metron-analytics (dbist via james-sirota) closes apache/metron#794
METRON-1241	Enable the REST API to use a cache for the zookeeper config similar to the Bolts closes apache/incubator-metron#795
METRON-1243	Add a REST endpoint which allows us to get a list of all indice closes apache/incubator-metron#797
METRON-1247	REST search and findOne endpoints return unexpected or incorrect results for guids (justinleet) closes apache/metron#798
METRON-1249	Improve Metron MPack Service Checks (nickwallen) closes apache/metron#799
METRON-1251	Typo and formatting fixes for metron-rest README closes apache/incubator-metron#800
METRON-1252	Bug fixes
METRON-1254	Conditionals as map keys do not function in Stellar closes apache/incubator-metron#801
METRON-1255	MetaAlert search is not filtering on status (merrimanr) closes apache/metron#802
METRON-1260	Include Alerts UI in Ambari Service Check (nickwallen) closes apache/metron#804
METRON-1261	Apply Bro security patch (JonZeolla via ottobackwards) closes apache/metron#805
METRON-1262	Unable to add comment for a alert in a meta-alert (merrimanr) closes apache/metron#806
METRON-1263	Start Alerts UI service after Metron REST (anandsubbu via nickwallen) closes apache/metron#807
METRON-1266	Profiler - SASL Authentication Failed (nickwallen) closes apache/metron#809
METRON-1267	Alerts UI returns a 404 when refreshing the alerts-list page (merrimanr) closes apache/metron#808
METRON-1270	Fix for warnings missing @return tag argument in metron-analytics/metron-profiler-common and metron-profiler-client closes apache/incubator-metron#810
METRON-1272	Hide child alerts from searches and grouping if they belong to meta alerts (justinleet) closes apache/metron#811
METRON-1274	Master has failure in StormControllerIntegrationTest (merrimanr) closes apache/metron#813
METRON-1275	Fix Metron Documentation closes apache/incubator-metron#833
METRON-1278	Strip "Build Status" widget from root README.md in site-book build (mattf-horton) closes apache/metron#815

Feature	Description
METRON-1280	0.4.1 -> 0.4.2 missed a couple of projects (cestella via justinleet) closes apache/metron#816
METRON-1282	Remove hard-coded indices from the Alerts UI (merrimanr) closes apache/metron#821
METRON-1283	Install Elasticsearch template as a part of the mpack startup scripts (anandsubbu via nickwallen) closes apache/metron#817
METRON-1284	Remove extraneous dead query in ElasticsearchDao (justinleet) closes apache/metron#818
METRON-1287	Full Dev Fails When Installing EPEL Repository (nickwallen) closes apache/metron#820
METRON-1289	Alert fields are lost when a MetaAlert is created (merrimanr) closes apache/metron#824
METRON-1290	Only first 10 alerts are update when a MetaAlert status is changed to inactive (justinleet) closes apache/metron#842
METRON-1291	Kafka produce REST endpoint does not work in a Kerberized cluster (merrimanr) closes apache/metron#826
METRON-1294	IP addresses are not formatted correctly in facet and group results (merrimanr) closes apache/metron#827
METRON-1295	Unable to Configure Logging for REST API (nickwallen) closes apache/metron#828
METRON-1296	Full Dev Fails to Deploy Index Templates (nickwallen via cestella) closes apache/incubator-metron#829
METRON-1301	Alerts UI - Sorting on Triage Score Unexpectedly Filters Some Records (nickwallen) closes apache/metron#832
METRON-1307	Orce install of java8 since java9 does not appear to work with the scripts (brianhurley via ottobackwards) closes apache/metron#835
METRON-1309	Change metron-deployment to pull the plugin from apache/metron-bro-plugin-kafka (JonZeolla) closes apache/metron#837
METRON-1310	Template Delete Action Deletes Search Indices (nickwallen) closes apache/metron#838
METRON-1311	Service Check Should Check Elasticsearch Index Templates (nickwallen) closes apache/metron#839
METRON-1319	Column Metadata REST service should use default indices on empty input (merrimanr) closes apache/metron#843
METRON-1321	Metaalert Threat Score Type Does Not Match Sensor Indices (nickwallen) closes apache/metron#845