HCP 1.9.0 Release Notes

Date of Publish: 2019-3-18

Hortonworks

https://docs.hortonworks.com

Contents

Release Notes Introduction

This document provides you with the latest information about the Hortonworks Cybersecurity Platform (HCP) powered by Apache Metron release 1.9.0 and its product documentation.

Apache Component Support

Hortonworks Cybersecurity Platform (HCP) 1.9.0 is built on HDP 2.6.5 and HDF 3.0.1.1 and later.

The official Apache versions of all HCP 1.9.0 components are:

- Apache Metron 0.7.0
- 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 1.9.0.

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 1.9.0 contains a number of updates focused on performance improvements, stability, and bug fixes.

HCP 1.9.0 includes the following new features:

- Numerous improvements around process and real-time batches
- Enrichment with the ASN (autonomous system number) database
- Multiple bug fixes and performance tweaks

Support Matrix

HCP 1.9.0 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”

Support for Elasticsearch (Optional)

- HCP 1.9.0 supports Elasicsearch version 5.6.14

JDK Support Matrix

HCP 1.9.0 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 2.6.5:

Table 1: HDP 2.6.5 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 topology is deprecated as of the HCP 1.7.1 release and will be removed in this release. The unified enrichment topology is now the default.

Unsupported Features

Although some features exist with HCP 1.9.0, 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 1.9.0 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 3: Technical Preview Features

Feature	Description
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 1.9.0 Repositories

You can download HCP 1.9.0 from HCP repository locations specific to the operating system you use.

Use the following table to identify the HCP 1.9.0 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/1.9.0.0/hcp.repo
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/centos6/1.x/updates/1.9.0.0/tars/metron/hcp-ambari-mpack-1.9.0.0-9.tar.gz
	Elasticsearch Management Pack	http://public-repo-1.hortonworks.com/HCP/centos6/1.x/updates/1.9.0.0/tars/metron/elasticsearch_mpack-1.9.0.0-9.tar.gz
RedHat Enterprise Linux / CentOS 7 (64-bit)	Repo	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.9.0.0/hcp.repo
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.9.0.0/tars/metron/hcp-ambari-mpack-1.9.0.0-9.tar.gz
	Elasticsearch Management Pack	http://public-repo-1.hortonworks.com/HCP/centos7/1.x/updates/1.9.0.0/tars/metron/elasticsearch_mpack-1.9.0.0-9.tar.gz
Ubuntu 14.04	Repo	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.9.0.0/hcp.list
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.9.0.0/tars/metron/hcp-ambari-mpack-1.9.0.0-9.tar.gz
	Elasticsearch Management Pack	http://public-repo-1.hortonworks.com/HCP/ubuntu14/1.x/updates/1.9.0.0/tars/metron/elasticsearch_mpack-1.9.0.0-9.tar.gz

Upgrading to HCP 1.9.0

For information on how to upgrade to HCP 1.9.0 from a previous release, see Hortonworks Cybersecurity Platform Upgrade Guide.

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 1.9.0 release has the following known issues:

- 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.
- When running a large sized PCAP query, the REST API can die silently if the result set exceeds the memory available to the REST server.
- On Kerberized clusters Storm rebalances can fail to correctly distribute tickets. This can be resolved by running storm upload-credentials against each topology.

Known Differences Between HCP 1.9.0 and HCP 1.8.0

The following bugs identify known differences between HCP 1.9.0 and HCP 1.8.0.

Table 5: Known Differences Between HCP 1.9.0 and HCP 1.8.0

Feature	Description
METRON-2030	SensorParserGroupControllerIntegrationTest intermittent errors
METRON-2031	Turning off initial search request and polling by default on Alerts UI
METRON-2012	Unable to Execute Stellar Functions Against HBase in the REPL
METRON-1971	Short timeout value in Cypress may cause build failures
METRON-1940	Check if not and install Elastic search templates / Solr collections when indexing server is restarted
METRON-2019	Improve Metron REST Logging
METRON-2016	Parser aggregate groups should be persisted and available through REST
METRON-1987	Upgrade Alert UI to stable Bootstrap 4
METRON-1968	Messages are lost when a parser produces multiple messages and batch size is greater than 1
METRON-1778	Out-of-order timestamps may delay flush in Storm Profiler
METRON-1996	Solr search throws NPE for group search if the group parameter is null or empty
METRON-1944	Unable to Delete a Comment in Alerts UI
METRON-2010	Unable to Build Metron Due to Inaccessible Repository
METRON-1998	Only one sensor is flushed by tick tuple
METRON-2009	Address Javadoc checkstyle issues in metron-common
METRON-2005	Batch Writer writes 0-byte files to HDFS on rotation
METRON-2007	Management UI not loading grok statements correctly
METRON-1986	Batch Profiler Fails to Resolve Stats Stellar Functions
METRON-1993	Stellar REST_GET should handle responses when content length is less than zero
METRON-1999	Adding validation against special characters to parser name field
METRON-1985	Improve Error Handling When Cannot Connect to HBase
METRON-1974	Batch Profiler Should Handle Errant Profiles Better
METRON-1970	Add Metadata to Error Messages Generated During Parsing
METRON-1995	Arrow icon in date range selector moved to a wrong position
METRON-1973	Upgrade Alert UI's webpack-dev-server to 3.1.14
METRON-1948	Dropped messages from REGEX_SELECT parser field transformation are not acked in Storm
METRON-1969	Adding Cypress documentation to Alert UI's README.md
METRON-1933	mprove build-utils helper scripts
METRON-1962	Make entering JDBC details in REST config to be optionaln
METRON-1929	Build GET_ASN Stellar function
METRON-1956	prepare-commit does not run all the tests it should

Known Differences Between HCP 1.9.0 and Apache Metron 0.6.0

There are no known differences between HCP 1.9.0 and Apache Metron 0.6.0.

Table 6: Known Differences Between HCP 1.9.0 and Apache Metron 0.6.0

Feature	Description
METRON-1748	Improve Storm Profiler Integration Test
METRON-1936	Cypress fails when trying to parse double quotes
METRON-1815	Separate metron-parsers into metron-parsers-common and metron-parsers-storm
METRON-1932	Update ES and Kibana to 5.6.14
METRON-1938	Add Parser Debugger to READMEs
METRON-1925	Provide Verbose View of Profile Results in REPL
METRON-1795	General Purpose Regex Parser
METRON-1892	Parser Debugger Should Load Config From Zookeeper
METRON-1937	Update public web site to point at 0.7.0 new release
METRON-1879	Allow Elasticsearch to Auto-Generate the Document ID
METRON-1930	Update webpack-dev-server in Alerts UI
METRON-1849	Elasticsearch Index Write Functionality Should be Shared
METRON-1928	Bump Metron version to 0.7.0 for release.
METRON-1931	Update dev utilities to support new repo location
METRON-1922	Escaping incorrectly handled in current aesh version
METRON-1867	Remove `/api/v1/update/replace` endpoint
METRON-1810	Storm Profiler Intermittent Test Failure
METRON-1909	Remove http filter from release utils changelog generation
METRON-1869	Unable to Sort an Escalated Meta Alert
METRON-1889	Add any missing timestamp fields to unified enrichment topology
METRON-1913	metron-alert UI - Build broken by missing transitive dependency
METRON-1845	Correct Test Data Load in Elasticsearch Integration Tests
METRON-1888	Default Topology Settings in MPack Cause Profiler to Stall
METRON-1887	Add logging to the ClasspathFunctionResolver
METRON-1873	Update Bootstrap version in Management UI
METRON-1825	Upgrade bro to 2.5.5
METRON-1890	Metron Vagrant should disable audio
METRON-1874	Create a Parser Debugger
METRON-1880	Use Caffeine for Profiler Caching
METRON-1877	Nested IF ELSE statements can cause parse errors in Stellar
METRON-1872	Move rat plugin away from snapshot version
METRON-1875	Expose configurable global settings in the Alerts UI
METRON-1834	Migrate Elasticsearch from TransportClient to new Java REST API
METRON-1834	Migrate Elasticsearch from TransportClient to new Java REST API

Feature	Description
METRON-1834	Migrate Elasticsearch from TransportClient to new Java REST API
METRON-1749	Update Angular to latest release in Management UI
METRON-1870	Intermittent Stellar REST test failures
METRON-1868	metron-committer-common incorrectly checking REPO_NAME
METRON-1740	Improve Palo Alto parser to handle CONFIG and SYSTEM syslog messages
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	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-1844	Allow for LDAP to be used for authentication and roles
METRON-1830	Re-implement Alerts dialog box without jQuery
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.
METRON-1769	Script creation of a release candidate
METRON-1761	Allow a grok statement to be applied to each line in a file.
METRON-1813	Stellar REPL Not Initialized with Client JAAS
METRON-1812	Fix dependencies_with_url.csv
METRON-1811	Alert Search Fails When Sorting by Alert Status
METRON-1809	Support Column Oriented Input with Batch Profiler
METRON-1806	Upgrade Maven Shade Plugin version

Feature	Description
METRON-1792	Simplify Profile Definitions in Integration Tests
METRON-1807	Auto populate the recommended values to some of the metron config parameters
METRON-1808	Add Ansible created pyc to gitignore
METRON-1695	Expose pcap properties through Ambari
METRON-1771	Update REST endpoints to support eventually consistent UI updates
METRON-1791	Add GUID to Messages Produced by Profiler
METRON-1804	Update version to 0.6.1
METRON-1798	Add mpack support for parser aggregation
METRON-1750	Create Parser for Syslog RFC 5424 Messages
METRON-1794	Include User Details When Escalating Alerts
METRON-1782	Add Kafka Partition and Offset to Profiler Debug Logs
METRON-1758	Add support for Ansible 2.6 in dev
METRON-1699	Create Batch Profiler
METRON-1784	Re-allow remote ssh and scp in Centos full dev
METRON-1787	Input Time Constraints for Batch Profiler
METRON-1508	In Ubuntu14 Dev Indexing Fails to Write to Elasticsearch
METRON-1786	Pcap Topology Status Incorrect
METRON-1709	Add controls to start / stop the PCAP topology from Ambari.
METRON-1759	PCAP UI: Removing wrong Input annotations from pcap panel component
METRON-1772	Support alternative input formats in the Batch Profiler
METRON-1770	Add Docs for Running the Profiler with Spark on YARN
METRON-1774	Allow user to configure JAAS client in Ambari
METRON-1760	Kill PCAP job should prompt for confirmation
METRON-1777	Fix Elasticsearch X-Pack sample pom in documentation
METRON-1781	Fix RPM Spec File
METRON-1780	Fix broken website images
METRON-1476	Update to Angular 6.1.3
METRON-1776	Update public web site to point at 0.6.0 new release
METRON-1775	Transient exception could prevent expired profiles from being flushed
METRON-1717	Relocate Storm Profiler Code
METRON-1748	Improve Storm Profiler Integration Test
METRON-1741	Move REPL Port of Profiler to Separate Project
METRON-1715	Create DEB Packaging for Batch Profiler
METRON-1736	Enhance Batch Profiler Integration Test
METRON-1714	Create RPM Packaging for the Batch Profiler
METRON-1708	Run the Batch Profiler in Spark
METRON-1707	Port Profiler to Spark
METRON-1705	Create ProfilePeriod Using Period ID

Feature	Description
METRON-1706	HbaseClient.mutate should return the number of mutations
METRON-1704	Message Timestamp Logic Should be Shared
METRON-1703	Make Core Profiler Components Serializable