CCP 2.0.0 Release Notes

Date of publish: 2017-11-06

https://docs.cloudera.com/

Legal Notice

© Cloudera Inc. 2019. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 (“ASLv2”), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

Release Notes Introduction

This document provides you with the latest information about the Cloudera Cybersecurity Platform (CCP) powered by Apache Metron release 0.7.0 and its product documentation.

Apache Component Support

Cloudera Cybersecurity Platform (CCP) 2.0.0 is built on HDP 3.1.4 and HDF 3.3.1 and later.

The official Apache versions of all CCP 2.0.0 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 CCP components should remain at the package version levels listed in the Support Matrix to ensure a certified and supported copy of CCP 2.0.0.

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

CCP 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.

CCP 2.0.0 provides the following new features:

- Support for HDP 3.1.4 and Ambari 2.7.3
- Enhancements to Alerts user interface, including the ability to:
  - Modify the alert data refresh rate and filter alerts
  - Hide resolved or dismissed alerts
  - Set local timestamp
  - Integrate third-party portals

Support Matrix

CCP 2.0.0 supports a select set of operating system, database, browser, and JDK versions.

You can find the most current information about CCP's interoperability for this release on the Support Matrix. The Support Matrix tool provides information about:

- Operating Systems
- Databases
- Browsers
- JDKs

Note: CCP does not support Internet Explorer.

To access the tool, go to: https://supportmatrix.hortonworks.com

Support for Elasticsearch (Optional)

- CCP 2.0.0 supports Elasicsearch version 5.6.14.

JDK Support Matrix

CCP 2.0.0 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 3.1.4:

Table 1: HDP 3.1.4 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 CCP release. Marking an item as deprecated gives you time to plan for removal in a future CCP release.
Moving	Technology that Hortonworks is moving from a future CCP 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 CCP release and plan for the alternative Hortonworks offering or subscription for the technology.
Removed	Technology that Hortonworks has removed from CCP 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 CCP release.
There are no feature deprecations in this release, but some support has been removed as a consequence of platform upgrades:

- Support for CentOS 6
- Support for HDP 2.6.5

Unsupported Features

Although some features exist with CCP 2.0.0, Hortonworks does not support some community features and technical preview features.

Community Features

Some Apache 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: Apache 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 CCP 2.0.0 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
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.

CCP 2.0.0 Repositories

You can download CCP 2.0.0 from HCP repository locations specific to the operating system you use.

Use the following table to identify the HCP 2.0.0 repo location for your operating system and operational objectives:

Note: Although HCP has been rebranded to CCP, the product management pack is still named HCP and it is still located in the hortonworks repository in the HCP directory.

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 7 (64-bit)	Repo	http://public-repo-1.hortonworks.com/HCP/centos7/2.x/updates/2.0.0.0/hcp.repo
	RPM tarball	http://public-repo-1.hortonworks.com/HCP/centos7/2.x/updates/2.0.0.0/HCP-2.0.0.0-centos7-rpm.tar.gz
	HCP Management Pack	http://public-repo-1.hortonworks.com/HCP/centos7/2.x/updates/2.0.0.0/tars/metron/hcp-ambari-mpack-2.0.0.0-4.tar.gz
	Elasticsearch Management Pack	http://public-repo-1.hortonworks.com/HCP/centos7/2.x/updates/2.0.0.0/tars/metron/elasticsearch_mpack-2.0.0.0-4.tar.gz

Upgrading to CCP 2.0.0

For information on how to upgrade to CCP 2.0.0 from a previous release, see Cloudera Cybersecurity Platform Upgrade Guide. Upgrading the platform to HDP 3.1.4 is also required for this release.

Third-Party Licenses

CCP 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 CCP 2.0.0 release has the following known issues:

Installing Spark 2 fails	Workaround: Before attempting to install Spark2 with Ambari, install the MySQL Connector manually and ensure Ambari can find it. This needs to be run on the node hosting Ambari. `yum -y install mysql-connector-java`

```
ln -s /usr/share/java/mysql-
connector-java.jar /var/lib/ambari-
server/resources/mysql-connector-
java.jar
cd /var/lib/ambari-server/resources/
ln -s /usr/share/java/mysql-
connector-java.jar mysql-connector-
java.jar
```

Kerberos authentication against HDFS from Metron's Storm topologies can fail.	If this issue occurs, the Storm worker is unable to present a valid Kerberos ticket to authenticate against HDFS. This impacts the Enrichment and Batch Indexing topologies, each of which interact with HDFS. To mitigate this problem, before starting the Metron topologies in a secured cluster using Kerberos authentication, perform the following additional installation steps: **1.** Schedule a periodic job to obtain and cache a Kerberos ticket. **2.** Schedule the job on each node hosting a Storm Supervisor. **3.** Run the job as user metron. **4.** Ensure the job performs kinit using the Metron keytab which is often located at /etc/security/keytabs/metron.headless.keytab. **5.** Schedule the job to run at least as frequently as the ticket lifetime to ensure that a ticket is always cached and available for the topologies.
During CCP 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 CCP 2.0.0 and HCP 1.9.1

The following bugs identify known differences between CCP 2.0.0 and CCP 1.9.1.

Table 5: Known Differences Between CCP 2.0.0 and CCP 1.9.1

Feature	Description
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
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-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-1699	create-batch-profiler
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

Feature	Description
METRON-1764	Update version to 0.6.0
METRON-1741	Move REPL Port of Profiler to Separate Project
METRON-1757	Storm Profiler Serialization Exception
METRON-1743	CEF testPaloAltoCEF test using a confusing variable name
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-1752	Prevent package.lock from changing during build
METRON-1708	Run the Batch Profiler in Spark
METRON-1724	Date/time validation missing in PCAP query
METRON-1707	Port Profiler to Spark
METRON-1705	Create ProfilePeriod Using Period ID
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
METRON-2274	Flatfile loader and summarizer mapreduce mode broken
METRON-2272	[UI] Performance: Switching manual filtering on and off multiple times leads slow typing
METRON-2190	[UI] Alerts UI: Indicating loading and preventing parallel requests
METRON-2275	Solr Indexing Topology Fails to Start on Secure Cluster with HDP 3.1
METRON-2265	Update Kerberos settings
METRON-2271	Reorganize Travis Build
METRON-2232	Added missing dependencies to dependencies_with_url.csv
METRON-2266	REST debug instructions
METRON-2264	Upgrade metron-hbase-client to HBase 2.0.2
METRON-2235	Increase server startup timeout
METRON-2261	Isolate Curator Dependencies
METRON-2257	Metron-Alerts GUI testing failing on MacOS builds
METRON-2250	Missing services in HDP 3.1 metron mpack and installer stuck
METRON-2247	rpm-docker: Provide an option to bypass running rpmlint
METRON-2254	Intermittent Test Failure in RestFunctionsIntegrationTest
METRON-2188	Upgrade to HBase 2.0.2
METRON-2252	PcapTopologyIntegrationTest Intermittent Failures
METRON-2211	[UI] Alerts UI should optionally render timestamp in local time
METRON-2248	Merge Master into Feature Branch
METRON-2217	Migrate current HBase client from HTableInterface to Table
METRON-2231	Revert METRON-2175, METRON-2176, METRON-2177 in HDP 3.1 upgrade feature branch

Feature	Description
METRON-2241	Profiler Integration Test Fails After Storm 1.2.1 Upgrade
METRON-2201	The description for the IS_IP method default behavior needs to corrected as per implementation
METRON-2227	Increase Kafka test harness timeout
METRON-2221	Notebook import fails through Zeppelin REST API
METRON-2243	[UI] Update npm dependencies to resolve audit warnings
METRON-2199	[UI] Add ability to turn off query building in Alerts UI search input
METRON-2238	Streaming enrichments regression
METRON-2225	Upgrade to Solr 7.4.0
METRON-2169	Upgrade to Kafka 2.0.0 and Storm 1.2.1
METRON-2149	Shaded jar classifier is not consistent
METRON-2224	Upgrade to Zeppelin 0.8.0
METRON-2179	[UI] Make navigation in both UIs consistent
METRON-2212	Add debugging developer docs to hbase-server README
METRON-2076	Fixed up flakey stellar timezone test
METRON-614	Eliminate use of the default Charset
METRON-614	Eliminate use of the default Charset
METRON-2205	Cease querying on filter or time-range change
METRON-2177	Upgrade Profiler for HBase 2.0.2
METRON-2195	Add defensive log level checks when constructing logs is expensive
METRON-2202	Add parameter validation for the stellar field validation functions
METRON-2197	Add debugging info output for Solr queries
METRON-2189	Optimize imports in mpack python scripts
METRON-2194	Update Ambari tooltip to specify single quotes for parser names with hyphens
METRON-2192	[UI] "All time" time range is broken on Alerts UI
METRON-2191	[UI] Checkbox selector on Alerts UI is broken
METRON-2130	[UI] Numeric steppers on the Management UI seems broken
METRON-2129	[UI] Clearing the search bar resets alert filter range to 'All Time'
METRON-2140	[UI] Implement logic behind show/hide RESOLVE and DISMISS items in Alerts UI
METRON-2176	Upgrade REST for HBase 2.0.2
METRON-2172	Solr Updates Not Tested in Integration Test
METRON-2185	Update Simple-Syslog dependency to fix error in Structured Data
METRON-2079	Fix documentation for installing Ansible for fulldev Centos 6
METRON-2175	Introduce HBase Connection Abstractions for HBase 2.0.2
METRON-2174	[UI] Grouped alerts total can differ from search alerts total
METRON-2161	[UI] CSS positioning bugs in Alerts and MGMT UI
METRON-2183	Update to Angular v7

Feature	Description
METRON-2148	Stellar REST POST function
METRON-2150	[UI] User not able to filter by multiple values of the same field on Alerts UI
METRON-2168	Elasticsearch Updates Not Tested in Integration Test
METRON-2084	Add documentation notice for MacOS Mojave users for new security permissions
METRON-2061	Solr documents with date fields cannot be updated with Dao classes
METRON-2164	Remove the Split-Join Enrichment Topology
METRON-2166	FileFilterUtilTest.test_getPaths_leftEdge:116 expected:1 but was:2
METRON-2161	Ambari client exception occurred: No JSON object could be decoded
METRON-2155	Cache Maven in Travis CI Builds
METRON-2156	Remove Storm dependency from metron-hbase
METRON-2142	Install solar schema as metron user
METRON-1253	Manual pasting of timestamps into the timestamp picker
METRON-2073	Create in-memory use case for enrichment with map type and flatfile summarizer
METRON-2092	[UI] Config UI does not require you to set a grok timestamp field by default
METRON-2141	Cache REST API status update calls to the Storm UI
METRON-2102	[UI] Adding click-through navigation to Alerts table
METRON-2153	ParserIntegrationTest should print failed messages
METRON-2127	Update Maven repositories to https
METRON-2145	Clarify RPM build documentation
METRON-2083	Fix broken links in root metron README
METRON-2152	Add debug logging for when sensor batchTimeout exceeds the calculated maximum
METRON-2112	Normalize parser original_string handling
METRON-2087	Remove Storm dependency from metron-indexing
METRON-2128	LEEF config file is missing in RPM spec file
METRON-2143	Travis Build Fails to Download Maven
METRON-2123	Expand Stellar JOIN to work on all Iterables
METRON-2109	Add option to use Metron GUID as the id in Elasticsearch
METRON-2113	Update version to 0.7.2
METRON-1788	Batch profiler pull profile information from zookeeper
METRON-2118	Added a LEEF parser
METRON-2085	[UI] Alerts UI Details Pane: naming meta alerts is broken
METRON-2058	UI: Actions -> Add to Alert can still be selected from dropdown when no alerts are selected.
METRON-2107	Add architecture diagram item to PR checklist
METRON-1997	Replace Threat Triage Score Field Slider with Text Box

Feature	Description
METRON-2111	Update public web site to point at 0.7.1 new release
METRON-2089	[UI] Adding loading state to Alerts details view
METRON-1989	Tooltip for ES mpack path_data is incorrect
METRON-2075	Site book build support for MacOS that has GNU sed installed
METRON-2106	Escalation topic setting in Ambari has no effect
METRON-2097	Install Metron MPack in Ambari 2.7.3.0
METRON-2100	Update developer documentation for full dev management UI parser aggregation feature gap
METRON-2018	Update prepare-commit to add Bro plugin tests
METRON-2093	Metron RC check script is outdated
METRON-2094	Create CentOS 7 Development Environment
METRON-2094	Create CentOS 7 Development Environment
METRON-2090	Full dev is failing with missing org.mortbay.jetty:jetty-util:jar:6.1.26.hwx dependency
METRON-2091	SimpleHBaseEnrichmentWriterTest should be included in tests
METRON-2078	Remove Storm dependency from metron-writer
METRON-2065	Setting Parser Output Topic in Sensor Config is broken
METRON-2067	Maven pom file duplicate dependency fixes
METRON-2074	Script to handle TGT renewal with Storm and Kerberos enabled
METRON-2082	Update the README document steps to run Batch Profiler
METRON-2006	Reenable JacoCo code coverage
METRON-2071	Add MAP_PUT and MAP_MERGE to Stellar
METRON-2014	Add architectural documentation for metron-writer
METRON-2026	Remove Storm dependency from metron-common
METRON-2062	Metron Alerts: Accidentally commited 'fdescribe' in unit tests
METRON-2050	Automatically populate a list of enrichments from HBase
METRON-2060	Improving Alerts table config pane
METRON-2064	Metron REST API overwriting global.json values
METRON-2066	Documentation and logging corrections
METRON-1654	findOne request after an alert patch returns with the original state of the alert item

Known Differences Between CCP 2.0.0 and Apache Metron 0.7.0

The following bugs identify the known differences between CCP 2.0.0 and Apache Metron 0.7.0.

Table 6: Known Differences Between CCP 2.0.0 and Apache Metron 0.7.0

Feature	Description
METRON-2274	Flatfile loader and summarizer mapreduce mode broken
METRON-2272	[UI] Performance: Switching manual filtering on and off multiple times leads slow typing
METRON-2190	[UI] Alerts UI: Indicating loading and preventing parallel requests

Feature	Description
METRON-2275	Solr Indexing Topology Fails to Start on Secure Cluster with HDP 3.1
METRON-2265	Update Kerberos settings
METRON-2271	Reorganize Travis Build
METRON-2232	Added missing dependencies to dependencies_with_url.csv
METRON-2266	REST debug instructions
METRON-2264	Upgrade metron-hbase-client to HBase 2.0.2
METRON-2235	Increase server startup timeout
METRON-2261	Isolate Curator Dependencies
METRON-2257	="html" scope="external">METRON-Alerts GUI testing failing on MacOS builds
METRON-2250	Missing services in HDP 3.1 metron mpack and installer stuck
METRON-2247	rpm-docker: Provide an option to bypass running rpmlint
METRON-2254	Intermittent Test Failure in RestFunctionsIntegrationTest
METRON-2188	Upgrade to HBase 2.0.2
METRON-2252	PcapTopologyIntegrationTest Intermittent Failures
METRON-2211	[UI] Alerts UI should optionally render timestamp in local time
METRON-2248	Merge Master into Feature Branch
METRON-2217	Migrate current HBase client from HTableInterface to Table
METRON-2231	Revert METRON-2175, METRON-2176, METRON-2177 in HDP 3.1 upgrade feature branch
METRON-2241	Profiler Integration Test Fails After Storm 1.2.1 Upgrade
METRON-2201	The description for the IS_IP method default behavior needs to corrected as per implementation
METRON-2227	Increase Kafka test harness timeout
METRON-2221	Notebook import fails through Zeppelin REST API
METRON-2243	[UI] Update npm dependencies to resolve audit warnings
METRON-2199	[UI] Add ability to turn off query building in Alerts UI search input
METRON-2238	Streaming enrichments regression
METRON-2225	Upgrade to Solr 7.4.0
METRON-2169	Upgrade to Kafka 2.0.0 and Storm 1.2.1
METRON-2149	Shaded jar classifier is not consistent
METRON-2224	Upgrade to Zeppelin 0.8.0
METRON-2179	[UI] Make navigation in both UIs consistent
METRON-2212	Add debugging developer docs to hbase-server README
METRON-2076	Fixed up flakey stellar timezone test
METRON-614	Eliminate use of the default Charset
METRON-614	Eliminate use of the default Charset
METRON-2205	Cease querying on filter or time-range change
METRON-2177	Upgrade Profiler for HBase 2.0.2

Feature	Description
METRON-2195	Add defensive log level checks when constructing logs is expensive
METRON-2202	Add parameter validation for the stellar field validation functions
METRON-2197	Add debugging info output for Solr queries
METRON-2189	Optimize imports in mpack python scripts
METRON-2194	Update Ambari tooltip to specify single quotes for parser names with hyphens
METRON-2192	[UI] "All time" time range is broken on Alerts UI
METRON-2191	[UI] Checkbox selector on Alerts UI is broken
METRON-2130	[UI] Numeric steppers on the Management UI seems broken
METRON-2129	[UI] Clearing the search bar resets alert filter range to 'All Time'
METRON-2140	[UI] Implement logic behind show/hide RESOLVE and DISMISS items in Alerts UI
METRON-2176	Upgrade REST for HBase 2.0.2
METRON-2172	Solr Updates Not Tested in Integration Test
METRON-2185	Update Simple-Syslog dependency to fix error in Structured Data
METRON-2079	Fix documentation for installing Ansible for fulldev Centos 6
METRON-2175	Introduce HBase Connection Abstractions for HBase 2.0.2
METRON-2174	[UI] Grouped alerts total can differ from search alerts total
METRON-2161	[UI] CSS positioning bugs in Alerts and MGMT UI
METRON-2183	Update to Angular v7
METRON-2148	Stellar REST POST function
METRON-2150	[UI] User not able to filter by multiple values of the same field on Alerts UI
METRON-2168	Elasticsearch Updates Not Tested in Integration Test
METRON-2084	Add documentation notice for MacOS Mojave users for new security permissions
METRON-2061	Solr documents with date fields cannot be updated with Dao classes
METRON-2164	Remove the Split-Join Enrichment Topology
METRON-2166	FileFilterUtilTest.test_getPaths_leftEdge:116 expected:1 but was:2
METRON-2161	Ambari client exception occurred: No JSON object could be decoded
METRON-2155	Cache Maven in Travis CI Builds
METRON-2156	Remove Storm dependency from metron-hbase
METRON-2142	Install solar schema as metron user
METRON-1253	Manual pasting of timestamps into the timestamp picker
METRON-2073	Create in-memory use case for enrichment with map type and flatfile summarizer
METRON-2092	[UI] Config UI does not require you to set a grok timestamp field by default
METRON-2141	Cache REST API status update calls to the Storm UI

Feature	Description
METRON-2102	[UI] Adding click-through navigation to Alerts table
METRON-2153	ParserIntegrationTest should print failed messages
METRON-2127	Update Maven repositories to https
METRON-2145	Clarify RPM build documentation
METRON-2083	Fix broken links in root metron README
METRON-2152	Add debug logging for when sensor batchTimeout exceeds the calculated maximum
METRON-2112	Normalize parser original_string handling
METRON-2087	Remove Storm dependency from metron-indexing
METRON-2128	LEEF config file is missing in RPM spec file
METRON-2143	Travis Build Fails to Download Maven
METRON-2123	Expand Stellar JOIN to work on all Iterables
METRON-2109	Add option to use Metron GUID as the id in Elasticsearch
METRON-2113	Update version to 0.7.2
METRON-1788	Batch profiler pull profile information from zookeeper
METRON-2118	Added a LEEF parser
METRON-2085	[UI] Alerts UI Details Pane: naming meta alerts is broken
METRON-2058	UI: Actions -> Add to Alert can still be selected from dropdown when no alerts are selected.
METRON-2107	Add architecture diagram item to PR checklist
METRON-1997	Replace Threat Triage Score Field Slider with Text Box
METRON-2111	Update public web site to point at 0.7.1 new release
METRON-2089	[UI] Adding loading state to Alerts details view
METRON-1989	Tooltip for ES mpack path_data is incorrect
METRON-2075	Site book build support for MacOS that has GNU sed installed
METRON-2106	Escalation topic setting in Ambari has no effect
METRON-2097	Install Metron MPack in Ambari 2.7.3.0
METRON-2100	Update developer documentation for full dev management UI parser aggregation feature gap
METRON-2018	Update prepare-commit to add Bro plugin tests
METRON-2093	METRON RC check script is outdated
METRON-2094	Create CentOS 7 Development Environment
METRON-2094	Create CentOS 7 Development Environment
METRON-2090	Full dev is failing with missing org.mortbay.jetty:jetty-util:jar:6.1.26.hwx dependency
METRON-2091	SimpleHBaseEnrichmentWriterTest should be included in tests
METRON-2078	Remove Storm dependency from metron-writer
METRON-2065	Setting Parser Output Topic in Sensor Config is broken
METRON-2067	Maven pom file duplicate dependency fixes
METRON-2074	Script to handle TGT renewal with Storm and Kerberos enabled
METRON-2082	Update the README document steps to run Batch Profiler

Feature	Description
METRON-2006	Reenable JacoCo code coverage
METRON-2071	Add MAP_PUT and MAP_MERGE to Stellar
METRON-2014	Add architectural documentation for metron-writer
METRON-2026	Remove Storm dependency from metron-common
METRON-2062	METRON Alerts: Accidentally commited 'fdescribe' in unit tests
METRON-2050	Automatically populate a list of enrichments from HBase
METRON-2060	Improving Alerts table config pane
METRON-2064	METRON REST API overwriting global.json values
METRON-2066	Documentation and logging corrections
METRON-1654	findOne request after an alert patch returns with the original state of the alert item
METRON-2053	Refactor metron-enrichment to decouple Storm dependencies
METRON-2022	METRON rest creates large number of connections to ZK which causes subsequent connection to zk fail
METRON-2056	Support LDAP Bind Authentication
METRON-2039	Time range queries do not work with Solr
METRON-2052	[UI] Changing default query time range to 15 minutes
METRON-2051	Improve stellar-zeppelin documentation
METRON-2023	[UI] Covering Grok Parser Creation with Cypress tests
METRON-2046	IS_EMPTY stellar functions fails on empty map
METRON-2029	Configure Table should have filter
METRON-2032	Create summary table having list of stellar functions in README
METRON-2038	Enrichment Loader Fails When Run as MR Job
METRON-2035	Allow User to Configure Role Names for Access Control
METRON-2041	RegularExpressionsParser in wrong source folder
METRON-2036	Maven builds fail locally in HDFSWriterTest
METRON-2030	SensorParserGroupControllerIntegrationTest intermittent errors
METRON-2031	[UI] 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

Feature	Description
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	Improve build-utils helper scripts
METRON-1962	Make entering JDBC details in REST config to be optional
METRON-1929	Build GET_ASN Stellar function
METRON-1956	prepare-commit does not run all the tests it should
METRON-1965	Knox should work on a multi-node installation
METRON-1939	Update version to 0.7.1
METRON-685	Scores in Threat Triage should be a Stellar Statement
METRON-1963	Remove left over integration test from before refactoring
METRON-1945	METRON MPack support for Knox SSO setup
METRON-1878	Add Metron as a Knox service
METRON-1958	Optimize Cypress to use best practices
METRON-1957	5424 and 3164 parser configurations are packaged in wrong place
METRON-1955	Update metron SPEC file to include syslog 3164 parser
METRON-1893	Create a syslog 3164 parser
METRON-1954	Commit Script Fails to Extract Usernames with Numerals
METRON-1953	Stellar REPL Fails on Start
METRON-1941	Alert Escalation Not Consistent in Alerts UI
METRON-1951	Add site-book generation to Travis build
METRON-1934	Stellar should built without error prone messages
METRON-1950	Site-book generation broken in master
METRON-1936	Cypress fails when trying to parse double quotes

Feature	Description
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