Server Changelog

CB v4.2.7.150629.0500

July 10, 2015

Contents

Future Carbon Black Enterprise Server releases (June 10 2015)

- **For release 4.2.7 and later, please refer to the Release Notes Document for that version**

Carbon Black Enterprise Server 4.2.5 (March 8 2015)

Changelog

- **E-4110 - Backport E-4109 fix to 4.2.5 "cbsyslog fails ungracefully when there are no matches"**
  - fix for cbsyslog producing a traceback when there are no query matches
- **E-4108 - Backport E-4107 fix to 4.2.5 "cbsyslog does not submit the query string correctly"**
  - fix for cbsyslog queries that were not getting submitted properly, producing invalid results.
- **E-4156 - cbsyslog tool doesn't return fields identical to watchlist searcher for syslog notifications**
  - fix for cbsyslog tool not firing syslog notifications with fields matching the normal system operation.
- **E-4063 - Binaries are deleted if hash reporting enabled, but uploads disabled**
  - fix for unable to download binaries from the UI when binary uploads to alliance is disabled.
- **E-4095 - E-mail notifications from watchlist will not recover from error**
  - fix for failure to send e-mail notification throwing an exception and required system restart.

Carbon Black Enterprise Server 4.2.4 (January 23 2015)

Changelog

- **E-3970 - cbcheck for iptables "doesn't work"**
  - fix an issue with cbcheck in regards to iptable rules in a clustered environment
- **E-3901 - Dashboard shows red alliance comms error after 1 week of good health**
  - fix error with sql purge when alliance comms status has not changed for one week
- **E-3893 - New cbrotate command line tool to help with stdout rotation when doing long-term data collection**
  - added cb log rotate utility to help when standard output is logged to a file
- **E-3889 - FROM TT 42026: Exporting events to CSV fails**
  - fix an error with process analysis event table CSV export
- **E-3883 - Datastore needs additional debugging around SQL calls to help us troubleshoot ingress perf**
  - increased verbosity for certain cbfs storage model sql store calls
- **E-3880 - Our use of 'cache' throttle pressure needs to be reviewed as it may cause low ingress rate cap even when server is not being loaded**
  - Introduced two new cb.conf settings to customize sensor throttle pressure Low and High watermarks. Please talk with Bit9/Carbon Black support
- **E-3838 - We need to add LVM information dump to cbdiag**
  - added pvdisplay, lvdisplay and vgdisplay to cbdiag collection

Carbon Black Enterprise Server 4.2.3 (November 20 2014)

Highlights

- **ENT-3789 - Remove use of unique_id and segment_id in grouped and sorted queries so that they do not go into the field cache**
  - This update reduces the memory footprint and requirements of solr in order to improve performance
- **ENT-3761 - Make datastore event ingress queue configurable via cb.conf**
  - Configurable options added to cb.conf to limit datastore event ingress queue to help tune server perf
  - DatastoreEventWriteQLen=1024 changed from 8192 docs
  - DatastoreStorageWriteQLen=30 unchanged
- **E-3738 - Increase watchlist_searcher cron job to 10 minutes**
  - Updated cron.d/cb watchlist searcher to run every 10 minutes
- **E-3737 - Reduce SOLR's internal cache usage**
  - Change SOLR config to reduce Document and Query/Filter Cache to help improve server perf
- **E-3736 - Update cbsolr to process migrate quicker**
  - cbsolr updated to support multithreaded operation
- **E-3733 - Increase the Redis stats connection timeout in order to prevent 'all-stop'**
  - Increased default Redis stats connection timeout from 2 seconds to 20
- **E-3703 - Datastore HTTP solr client thread count not configurable**
  - Enable the configuration of datastore HTTP solr client threads via cb.conf "DatastoreEventCoreClient-Threads="
  - Reduce default threads from 24 to 1/2 number of CPU cores
- **E-3702 - Difficult to troubleshoot Solr garbage collection**
  - Enabled GC stats in Solr

Changelog

- **E-3784 - Sensor sync causes invalid cbstats DatastoreCache.num.bytes_in_cache metric**

Fixed double decrement of DatastoreCache.num.bytes_in_cache byte count

- **E-3769 - Multiple minions writing to moduleinfo_events end up deadlocking each other**

Update how minions write transactions to postgres

- **E-3768 - cb-datastore creates high number of SQL connections and doesn't recover when limit is reached**

Fix cb-datastore sql connection gc

- **E-3759 - cb-enterprise service may fail to start a cluster during race condition**

Fix to remove race situation where minion fails to populate cbstats metric

- **E-3749 - SELINUX upgrade had default rules that disable nginx**

Fix for cb-nginx so that it has the correct selinux permissions

- **E-3729 - FeedTagger task does not tag VT hits**

Fix issue with FeedTagger and VT hits

- **E-3685 - POODLE: SSLv3 vulnerability (CVE-2014-3566)**

Update nginx configuration to not allow fallback to SSLv3 protocol for GUI and sensors

- **E-3594 - Bugfix Alliance stats fail on cluster with multiple minions**

Fix of cluster failing to upload Alliance stats when master has 0 shards

Carbon Black Enterprise Server 4.2.2 (October 2 2014)

Highlights

- **E-3633 - Feed report title is now available in feed syslog notifications**
  - Feed report title can be specified in syslog template with title='{{doc['report_title']}}'
- **E-3595 - Make syslog notifications and general CB log message length configurable**
  - CB notifications are controlled by cb.conf entry 'MaxSyslogSenderMessageSize = xxxx' (default value is 1024)
  - CB logs are controlled by cb.conf entry 'MaxCbLoggingMessageSize = xxxx' (default value is 2048)

Changelog

- **E-3656 - update cbevent limits in cb.conf on new installs**

Update defaults for collection of cbevents to 30 days or 60 million events on NEW installs. Upgrades keep original values.

- **E-3654 - Tokenization changes in 4.2.1 broke watchlist path queries**

Change tokenization to index all path prefixes so that wildcard queries are not needed for unknown path queries

- **E-3637 - Linux installer package downloaded from server didn't have execute permissions**

Fix so that Linux installer package installer script has execute permissions

- **E-3632 - Negation and wildcard queries do not work together**

Fix so that negation of wildcard queries return correct results because we have full path tokenization

- **E-3561 - Alliance stats uploads fail if an HTTP error is returned from solr**

Fix so that a failure in HTTP request of solr doesn't stop that upload of stats to the Alliance

- **CBUI-832 - Fix typo in mouseover text in process analyze facets**

Carbon Black Enterprise Server 4.2.1 (September 2 2014)

Highlights

- **E-3525 - Add link to OSX and Linux sensor install packages if available on the server**
  - Allows downloading of OSX and Linux sensor packages via the cb web gui
- **E-3471 - Addition of IOC hit attributes to feed event syslog**
  - Feed hit json output enhanced to include IOC attributes, ioc_type, ioc_value
  - Netconn directionality
- **E-3453 - Process host OS type can now be queried**
  - Allows searching of process by OS type
- **E-3435 - Process PID added to process documents**
  - Process and Parent PID fields added to process doc but not indexed
- **E-3114 - API updated to expose osx/linux sensor download**
  - Prep work for osx/linux sensor package downloads
- **E-3037 - Postgres tables added to cbdiag collection**
  - Added collection of select sanitized postgres tables

Changelog

- **E-3540 - Storage Statistics not showing up in specific clustered configuration**

Fix for Dashboard storage statistics not showing up in shardless master configuration.

- **E-3467 - Analyze page does not show feed hits when report names have spaces**

Fix to allow for proper query of feed reports with spaces in the report ID

- **E-3463 - 4.2 index improvements broke various queries for full paths**

Fix to bring back full search ability without putting full tokenization back in

- **E-3418 - “Pending” process info now called “unknown”**

Instead of “pending” for incomplete process data the word “unknown” will be used

- **E-3417 - Tomcat xml file not getting updated during Datastore move**

Fix to update solr.xml file with datastore location from cb.conf

- **E-3416 - Time “Between” filter not handling ‘years’ properly**

Implemented check for ‘years’ when determine before/after date ranges

- **E-3380, 3468 - API watchlist and feed hits not consistent with other API citizens**

Fields returned with feed and watchlist hits are now more consistent

- **E-3355 - VT scores are missing after upgrade to 4.2**

VT tags are now reapplied during cbupgrade

- **E-3354 - 'ago' on second line in process analyze page**

Process, hostname, user and time of process on one line now
Implemented check for 'years' when determine before/after date ranges

- **E-3345 - Binary search by publisher resulted in query that had missing quotes**

Fix to include quotes around publisher search terms

- **E-3272 - API allows more simultaneous connections than DB pool size allows**

Workarund until CB v5.0 fix is implemented is to lower "CoreServicesWorkerConnections=5" in /etc/cb/cb.conf

- **E-3235 - Sensor report not using sensor_timestamp for comm failures**

Fix to use sensor_timestamp value in sensor report

- **E-2708 - Removal of Sensor page multi-facet filtering not working correctly**

Fix for multi-facet filtering on sensor page

- **E-1342 - Binary files not getting cleaned up**

Fix to cleanup binaries from Enterprise server after upload to Alliance

- **E-1085 - cb-multihome.conf example out of date**

4.2 changes (websockets) was not updated in multihome example file

Carbon Black Enterprise Server 4.2.0 (June 1 2014)

Highlights

- **Bit9 Platform Server Integration**
  - Standardize Process ID across Bit9 and CarbonBlack
  - Carbonblack watchlist hits published to Bit9 Platform Server
- **New Pub/Sub Architecture makes the following available**
  - Watchlist hits
  - Feed hits
  - Binary store events
- **New Alerts using Websockets**

```
- Alerts are available via Pub/Sub architecture and Websockets
- Watchlist and Feed hits will be presented at the upper right of the UI,
  most recent events at the bottom
```

- **New Sensor Throttling**

  - Sensor throttling based on internal performance statistics

- **Improved VDI support**
  - Updated registration logic for VDI machines to allow for non-duplication of sensor machines
  - Updated group registration logic
  - Enhanced API to support VDI status

- **Enhanced Server Performance, monitoring and metric collection**
  - New database schema implimented in order to improve query times
  - Improved sensor check-in efficiency
  - Ability to configure max solr file system usage

- **Alliance Feeds Improvements**
  - Process and Binary feed search from Alliance view
  - Quick add watchlist from feed search
  - Add process search via Alliance feeds view
  - Added Bit9 SRS (Trust) and TIS (Threat) feeds
  - Added ThreatConnect feed
  - Improved feed validation logic and error reporting

- **Improved Alliance Statistics Collection**
  - Fixed upload of CB server diagnostics in a clustered environment

- **Sensor Improvements**
  - Requires 4.2.0 or higher sensor – Ability to track filewrites at a high level in order to track filewrite requests
  - Reduced CPU and memory usage in high volume environments
  - Enhanced diagnostics logging of host machine statistics, module processing and
  - Requires 4.2.1 or higher sensor
  - Reduced Disk IO to decrease remote disk usage in VDI environments
  - Increased robustness around unexpected data from the OS

Changelog

- **E-3240 - 3rd Party bugfix**

Updated openssl library requirement for server install to address CVE-2014-0224

Carbon Black Enterprise Server 4.1.6 (May 02 2014)

- **E-3118 - Bugfix**

Fix for issue while exploring process tree when server is in a sharded configuration.

- **E-3055 - Bugfix**

Fix for process names not being rendered properly with new Chrome browser version.

Carbon Black Enterprise Server 4.1.5 (April 10 2014)

- **E-3033, E-3024 - Improvement**

Server and Web Console - Delivery and documentation of feature to add watchlist during cbinit

- **E-3031, E-3030, E-3029, E-3023 - Improvement**

Server and Web Console - Ability to create a watchlist as read-only introduced.

- **E-3026 - Improvement**

Documentation - clean up server_ssl doc

- **E-3025 - Improvement**

Documentation - Clean up cb.conf documentation per feedback from field

- **E-3022 - 3rd party patch**

Server Backend - Address openssl vulnerability (CVE-2014-0160) in alliance client

- **E-3020 - 3rd party patch**

Server Backend - Address openssl vulverability (CVE-2014-0160) in server

- **E-3017 - Bugfix**

Server Backend - Enabling sensor eventlog archiving causes ingress of event logs to fail.

- **E-2997 - Bugfix**

Server Backend - Sensor upgrade throttle task may fail on startup due to a race condition in redis stats

Carbon Black Enterprise Server 4.1.4

- **E-2978 - Bugfix**

Server Backend - Fix for alliance statistics upload in clustered environment

- **E-2976 - Documentation**

Documentation - binary template example correction

- **E-2974, 2962 - Improvement**

Server Backend - Enable adding feed via API

- **E-2967, 2966 - Improvement**

Server Backend - API example and documentation updates

- **E-2962 - Improvement**

Server Backend - Deliver sensor package download via API

- **E-2961 - Improvement**

Server Backend - default API to use auth token

- **E-2950 - Improvement**

Installation - Deliver specific OpenSSL version with CB

- **E-2949 - Improvement**

Documentation - fix wrong yum baseurl link

Carbon Black Enterprise Server 4.1.3

- **E-2883 - Improvement**

Server Backend - hardening of Alliance client performance statistics

- **E-2879, 2801 - Improvement**

Server Backend - added hardware diagnostic toolkit to cbdiag functionality

- **E-2868 - Bugfix**

Web Console - fix for process preview md5 modload link

- **E-2860 - Improvement**

Web Console - update spinner at login page

- **E-2858 - Improvement**

Server Backend - cbsensorinstallergen utility default settings changed to reflect current cb.conf

- **E-2857, 2856, 2855, 2854, 2853, 2852 - Improvement**

Server Backend - add endpoint hostname and group to binary documents and watchlist syslog/emails

- **E-2851 - Bugfix**

Web Console - Splash page text incorrectly referred to sensorsettings.bin

- **E-2846 - Bugfix**

Server Backend - exception sending email via non-CB alliance SMTP server was fixed

- **E-2845 - Bugfix**

Server backend - Fix for Analyze page childproc row dropdown

- **E-2841 - Bugfix**

Server Backend - changing password for newly created user fixed

- **E-2837 - Bugfix**

Server Backend - fix for infinite sync status of sensor when it was instructed to perform a sync

- **E-2749 - Improvement**

Licensing - update license text

Carbon Black Enterprise Server 4.1.2

- **E-2810 - Improvement**

Server Backend - include sensor registration “callback” script for sensor id mapping to computer name

- **E-2809 - Improvement**

Server Backend - Reduce overall suggestor dictionary size

- **E-2793 - Improvement**

Server Backend - add feedback text during solr startup to indicate long-running suggestor buildup

- **E-2773 - Bugfix**

Server Backend - fix to a handle corrupted sensor event logs

- **E-2763 - Improvement**

Server Backend - Operational VDI support

- **E-2756 - Improvement**

Sensor - provide sensor upgrade support for osx sensor

- **E-2755 - Improvement**

Sensor - Add OSX-specific sensor checkin handler logic

Carbon Black Enterprise Server 4.1.1

- **E-2799 - Improvement**

Documentation - Updated syslog_template doc to reflect correct key values.

- **E-2796 - Improvement**

Web Console - Process Analyze page now highlights matching search terms when linked from the watchlists page. The highlighting allows for easy recognition and filtering on matching terms.

- **E-2795 - Bugfix**

Web Console - Floating investigation pane is now hidden on logoff.

- **E-2781 - New Feature**

Web Console - Feed synchronization (both full and incrementatal) can now be triggered in the web console via the feeds page.

- **E-2776, E-2777 - Improvement**

Web Console - Process names in watchlist page (for process watchlists) now link to the analyze page rather than the search results page. This is consistent with the process search page behavior.

- **E-2771 - Bugfix**

Server Backend - Certain classes of internal cb-datastore diagnostic data is now pushed to the minion redis instance. This only applies to cluster configurations.

- **E-2766 - Bugfix**

Web Console - Binary search page 'autocomplete' functionality now works when used with 'terms' component functionality.

- **E-2757 - Improvement**

Web Console - When changing active investigation in floating investigation pane, navigating to the investigation pane now shows the currently selected investigation by default.

- **E-2751 - Improvement**

Web Console - When tagging events in the analyze page with the floating investigation pane open, the tagged event lists in the floating investigation pane is now updated dynamically.

- **C-668 - Bugfix**

Web Console - Event tagging on the analyze page fails if the select process was changed using the process tree graph control.

- **C-667 - Bugfix**

Web Console - Analyze page event expansion for netconns now avoids 'infinite spinner' in certain circumstances. In particular, if the network connection event included exactly one of an IPv4 address and a DNS name, network connection data was not displayed and the 'spinner' icon was displayed.

- **C-665 - Improvement**

Web Console - When an investigation is removed on the investigations pane, the floating investigation pane is now updated to reflect the deleted investigation.

- **C-662 - Bugfix**

Web Console - 'Actions' dropdown on host detail page now correctly performs an action after a previous action had been cancelled.

Carbon Black Enterprise Server 4.1.0

Highlights

- **Process Analyze Page Improvements**
  - Timeline
  - Inclusion of digital signature publisher and status for all module loads
  - Inclusion of file types for certain filemod events
  - Inclusion of Alliance feed matches
  - Inclusion of 'highlighting' based on search term
- **Investigations pane moved to be a 'top-level' UI element**
  - Provides at-a-glance access to current investigation
- **"True" network endpoint detection**
  - Add support for logging the destination of HTTP and FTP requests made via web proxies
  - Requires 4.1 sensor
- **Server Security Hardening**
  - Includes improved CSRF defense
  - Includes improved XSS defense
- **Watchlist Notification E-Mail Improvements**
  - Process Watchlists now include 'highlighting' to help identify why a process matched a watchlist
  - Watchlist Notification E-Mails now include HTML support for an easer-to-read experience
- **Data File Tracking by MD5**
  - Support for tracking the MD5s of certain classes of data files
  - Collection of data file tracking is configurable on a per-group basis
  - Requires 4.1 sensor
- **Improved Highlighting Support**
  - Search results include improved 'highlighting' on matching terms, including DNS names
- **Improved Sensor Management when Sensor Ids are Reused**
  - Better support for automatic sensor re-registration when a sensor ID is re-used.
  - In particular, supports scenarios where an already-registered sensor installation is cloned
- **High-Performance, Low-Latency Feed Tagging**
  - Process and Binary documents are now tagged as event data arrives from the sensor
  - Higher-performance and much lower latency
- **Improved Frequency Calculation Performance**
  - Module Load (MD5), FileMod, and RegMod frequency improved, sometimes by an order-of-magnitude or more
  - Process username (security context) support
  - Username (including domain) included as a searchable and retrievable field in all process documents
  - Collection of username is configurable on a per-group basis
  - Requires 4.1 sensor
- **Improved Support for Special Characters in Search**
  - In particular, support for quotes ("") and backslashes () improved

- **Improved Support for Sensor Installation Scenarios**
  - MSI can be used to upgrade or reinstall
  - Avoid two entries in the endpoint Add/Remove Programs database when installed via MSI
  - Update Add/Remove Programs database when sensor is upgraded via Enterprise Server
  - Requires 4.1 sensor
  - Sensor uninstallation removes all registry entries
- **Add Support for EICAR test file**
  - To be used in troubleshooting and end-to-end verification testing
  - Requires 4.1 sensor
- **Adds Support for Server-Sensor Clock Delta Tracking**
  - Clock Delta between CB server and sensor is reported in the Host Detail Page of the UI
- **Sensor Compresses Eventlogs for Transmission to Server**
  - Reduces bandwidth requirements 50-90 percent
  - Requires 4.1 sensor
- **Add Support for 'Rolling' Sensor Upgrades**
  - Server can be configured to 'trickle' out sensor upgrades
  - Allows time to abort an in-progress deployment of upgraded sensor version as needed
- **Finalized Support for FireFox, Safari, and IE 10+**
  - IE10+ compatibility mode NOT supported
- **Numerous Host Detail Page Improvements**
  - Improved Timestamp Accuracy
  - Improved Flagging of 'Warning' Behavior (high resource usage, etc.)
  - Decreased verbosity of component status logging
- **Add support for 'Bulk' Search in the UI**
  - Supports both binary and process searches
  - Allows pasting multiple indicators (search terms)
  - For high volumes of indicators, a feed is recommended for performance reasons
- **Improve legibility of 'Add Criteria' Selections in Search**
  - Significant expansion of space dedicated to choosing criteria to search on
- **Improved Feed Retrieval Support**
  - Support via Proxy
  - Per-Feed configuration of server SSL certificate verification
  - Support for using SSL client certificates for authentication
- **Improved Autocomplete Performance**
  - leveraged database 'suggester'
- **Increased Configurablity of Search Results**
  - Number of process and/or binary search results displayed per-page is configurable
  - Default sort order of process and/or binary search results is configurable
- **Sensor Checkin Performance Improvements**
  - improve use of redis caching for sensor checkin

- **API Expansion**
  - Watchlists Management is now part of documented API
  - Feed Management is now part of documented API
  - License Management is now part of documented API
  - Binary search now includes POST support for larger queries
- **Binary Detail Page Performance Improvements**
  - API improvements used by Binary Detail page
- **Additional fields added to query parser**
  - Sensor Id
  - Host Type (Workstation, Server, Domain Controller)
  - Binary Architecture (32bit/x86, 64bit/x64)
  - Binary Type (Standalone Executable, Library (DLL, SYS))
  - Server Added Timestamp
- **Watchlist Page Performance Improvements**
  - API improvements used by Watchlist page
- **Enhanced Backend Toolset**
  - cbpasswd now allows for adding a CB user
  - cbdiag now includes support for web proxies, reports sensor/server clock deltas and has a hardcoded uploaded file size limit of 1Gig.
  - cbstats now includes detailed performance monitoring and instrumentation
  - cbcheck tool used to help with troubleshooting log files and iptables rules
  - cblicense tool used to retrieve and update CB license file data
  - cbssl now has new command ‘sso’ to create SAML2.0 Service Provider metadata
  - cbsyslog tool used to view current and test new CB syslog and watchlist output templates (see syslog_templates and syslog_cef pdf files)
- **Add Support for SAML Third-Party Authentication**
  - added new sso/ directory under /etc/cb configuration
- **Add Support for Automating Analysis of Network Edge Device Alerts**
  - CheckPoint, Fidelis, FireEye, Palo Alto Networks
  - Requires a separate RPM; contact support for details

Carbon Black Enterprise Server 4.0.3

Changelog

- **E-2533 - New Feature**

The syslog output on watchlist match is now controllable, both in terms of format and order of fields. For more information, see the separate usage guide for custom watchlist formatting.

- **E-2536 - Bugfix**

The UI license feature allows for the application of a new Carbon Black license. This feature has been improved to be more accepting of various formats of data.

- **E-2539 - Improvement**

The “Carbon Black Alliance Status” pane in the Server Dashboard now provides clearer output when the Alliance Client has never attempted to reach the Alliance Server, or when all errors in reaching the Alliance Server were at the TCP layer or below.

- **E-2535 - Improvement**

Additional debug logging has been put in place to assist with identifying the source of malformed binary file data from sensors.

- **E-2538 - Improvement**

Update copyright date from 2013 to 2014

Carbon Black Enterprise Server 4.0.2

- **E-2355 - Improvement**

The logging for the feed_searcher cron job now includes additional verbosity to troubleshoot feed issues.

- **E-2353 - Bugfix**

The warning log output in the feed_searcher cron job is now correct for a feed report with no indicators (IOCs)

- **E-2352 - Improvement**

The feed_searcher cron job may be run with the “–terms” switch. In certain cases, particularly during feed development, this may improve performance. The “–terms” switch results in querying the SOLR terms component for all terms (such as IPs, domain names, etc.). This query may take a long time to complete. As a result, the timeout on the query was increased to allow for usage of “–terms” on bigger SOLR indexes.

- **E-2348 - Improvement**

Feeds automatically added to the Enterprise Server via the Alliance Server are now removed when they are removed from the Alliance Server.

- **E-2347 - Bugfix**

Alliance Server-provided feeds are now added in a case-insensitive manner.

- **E-2319 - Bugfix**

The web UI link to the VirusTotal web page was incorrect for binaries that had a ‘0’ VirusTotal score. This was because VirusTotal changed the format of their link. The 4.0.2 Enterprise Server adjust the format of the link to match the new VirusTotal link format.

- **E-2315 - Improvement**

The feed_searcher cron job now allows execution against a particular feed, specified on the feed_searcher command line. This can assist feed development.

- **E-2313 - Bugfix**

Postgres logs are now rotated properly.

- **E-2312 - Bugfix**

Datetime and timestamps are now correct on the host detail page in the web UI.

- **E-2311 - Improvement**

Alliance Server feeds can now be added, via the web UI, by URL rather than manually. This is useful when doing feed development.

- **E-2310 - Bugfix**

The error log output from the feed_searcher cron job is now correct if the HTTP response code from the feed server is not 200.

- **E-2307, E-2306 - Bugfix**

Certain classes of potential cross-site scripting (XSS) vulnerabilities in the web UI were identified and addressed.

Carbon Black Enterprise Server 4.0.1

Changelog

- **E-2254 - Bugfix**

The Alliance status on the server dashboard failed to properly display in certain cases. In particular, when the Alliance client was not properly connected with the Alliance Server, date parsing was not properly performed.

Enterprise Server 4.0.1 addresses this issue by properly parsing and displaying the date in all situations.

- **E-2255 - Bugfix**

The process search results page includes a 'magnifying glass' icon for each search result to allow for a 'process preview' of the search result. Clicking on this icon failed for certain classes of data. In particular, data generated by 3.0.0 servers, as well as some pre-release 3.1.0 servers, was not preview-able. An error in the JavaScript console occurred when clicking on the process preview magnifying glass icon.

Enterprise Server 4.0.1 addresses this issue by properly handling the data. All search results, including those backed by data gathered on 3.0.0 servers, are now previewable.

- **E-2264 - Bugfix**

Enterprise Server 4.0.1 now properly calculates an internal identifier for communications with Alliance Server properly in both clustered and non-clustered situations. There is no customer-facing impact from this change.

- **E-2267 - Bugfix**

Enterprise Server 4.0.1 now restricts the changing of the username via the 'Users & Teams' UI page. The first name, last name, email, password, and api token are still changeable. The reason is due to how Enterprise Server uses a secure mechanism of digest authentication - changing the username also requires knowing the plaintext password. In the interests of security, the plaintext password is never stored on the Enterprise Server.

- **E-2272 - Bugfix**

Enterprise Server 4.0.1 now ensures that the URLs used by the sensor to push data to the Enterprise Server never include repeated / characters. The only ramification of this bug was a repeated / in the nginx access logs. There was no direct customer-facing issue as a result of the bug. Note that this is a server change only; no sensor modifications have been made.

- **E-2274 - Bugfix**

Enterprise Server 4.0.1 now allows authentication via the Carbon Black API token for the /api/v1/binary//summary REST endpoint. This bug did not affect the server UI, but it did interfere with the ability to consume this endpoint via CB API scripts.

- **E-2275 - Bugfix**

Enterprise Server 4.0.1 now allows binary downloads via both the CB API and the UI for binaries collected prior to 4.0.0 installation. Due to the way clustering was implemented, binaries collected on server versions 3.2.2 and below could not be found by the 4.0.0 server.

- **E-2279 - Bugfix**

Enterprise Server 4.0.1 improves the 'module sync' cron job. This job runs once daily to synchronize the list of known binary files between the Postgres SQL database and the filesystem.

- **E-2280 - Improvement**

Enterprise Server 4.0.1 adds the end-user-controllable selection of new 'fuzzy' faceting. Fuzzy faceting uses statistical sampling to more quickly provide facet calculations. The use of this option is controllable via two new cb.conf options. See cb.conf documentation for details.

- **E-2281 - Improvement**

Enterprise Server 4.0.1 increases an internal timeout used to query SOLR statistics when reporting performance statistics to the Alliance Server. This improvement has no customer-facing impact.

- **E-2282 - Improvement**

Enterprise Server 4.0.1 adds two new fields to the 'sensor vitals' section of the host detail page in the UI. These fields provide the size of queued eventlogs and binary files on a particular sensor, as of the last sensor checkin.

- **E-2283 - Bugfix**

Enterprise Server 4.0.1 now supports API token authentication access to the binary search REST endpoint.

- **E-2285 - Bugfix**

Enterprise Server 4.0.1 now successfully completes sensor checkins even when the detailed sensor diagnostic data cannot be properly processed.

- **E-2288 - Bugfix**

The reset search terms button on the process and binary search pages now works properly when facets are disabled.

- **E-2293 - Bugfix**

The reset search terms button on the process search page works properly when cb.conf has been modified to timebox process search results.

- **E-2294 - Bugfix**

The reset search terms button on the binary search page works properly when cb.conf has been modified to timebox process search results.

Carbon Black Enterprise Server 4.0.0

Changelog

- **E-2131 - Bugfix**

Deleting users via the web UI sometimes appeared to fail, as an error 'toaster' UI indicator appeared in the top-right corner of the UI. In most cases, the deletion had actually succeeded, with the error appearing erroneously.

Enterprise Server 4.0.0 addresses this issue by more robustly deleting the user and properly reporting the result to the UI.

- **E-2129 - New Feature**

The Enterprise Server API is now authenticated with either a username and password, as with Enterprise Server 3.x, or with a new API token or key. The key is visible from the 'User Profile' page in the web UI.

- **E-2117 - Improvement**

The Enterprise Server REST API included trailing slashes inconsistently, from endpoint to endpoint, in Enterprise Server 3.x. In 4.0, trailing slashes are not used and that is consistent across the API.

- **E-2113 - Improvement**

Enterprise Server 4.0 allows an optional cb.conf parameter, CoreServicesProcessSearchIntervalSeconds. When set, this parameter sets a default search criteria to all process searches. This can reduce the number of results for searches to only 'recent' results, and can improve performance on large data sets. The default value can be overridden in the UI at any time.

- **E-2086 - Improvement**

Enterprise Server 4.0 adds a new process search query syntax parameter, last_server_update. This allows searching processes based on the last time the process document was updated on the server. More information is available in the query parser documentation.

- **E-2075 - Improvement**

The 'computers' page in the web UI has been updated to avoid auto-refreshing every sixty seconds. This makes it easier to use the page, as the contents do not change or scroll automatically. An update can be accomplished by refreshing the page.

- **E-2053 - Improvement**

The process search time for process start time has been updated to provide more consistent results when searching on time ranges.

- **E-2042 - Improvement**

The 3.x Enterprise Server sometimes functioned sporadically if localhost was included in /etc/hosts with an ipv6 address. The 4.0 Enterprise Server addresses this issue by using 127.0.0.1, and not localhost, thereby avoiding any dependency on /etc/hosts.

- **E-2031 - Improvement**

The process search REST API endpoint (/api/v1/process) has been updated to allow the HTTP verb POST, in addition to GET. This allows providing significantly longer query strings.

- **E-2021 - Bugfix**

Enterprise Server 3.x could be configured, via Alliance Community Participation settings, in such a way as binaries were uploaded to the Carbon Black Alliance server, but could not be downloaded via the "binary detail" UI page. Enterprise Server 4.0 addresses this issue and always allows downloading if the file had been uploaded previously.

- **E-2015 - Bugfix**

The host detail page previously displayed the wrong month, although the right day of the month and the right time, for all sensor diagnostic data. Enterprise Server 4.0 displays the correct date on the host detail page.

- **E-2012 - Improvement**

The Alliance Client now supports NTLM authentication. Furthermore, the proxy password can be optionally encrypted in cb.conf for further protection.

- **E-1942 - Improvement**

Enteprise Server 4.0 now includes the source endpoint hostname, the Carbon Black server name, and a directly link to the analyze page, in watchlist notification e-mails.

- **E-1947 - Improvement**

The server dashboard now includes a summary of outstanding data, in terms of size of event logs and binary files, that are outstanding on sensors. This provides a good global indication of how 'current' the server is relative to incoming sensor data.

- **E-1931 - New Feature**

The Carbon Black Enterprise Server can now subscribe to threat intelligence feeds, consisting of IOCs such as MD5s, domain names, and IPs. These feeds can be provided by the Carbon Black Alliance Server, an on-premise device, or via custom lists of indicators.

In 4.0, the index is automatically searched for feed data and, when matches are found, documents are tagged to reflect.

- **E-1910 - New Feature**

The Enterprise Server API can now be used to find sensors based on the host endpoint IP address.

- **E-1902, E-1894 - New Feature**

It is now possible to do a process search based on the parent process MD5 using 'parent_md5'. See the query parser documentation for additional information.

- **E-1900 - Improvement**

The host list page 'export to CSV' capability now exports the all of the same data visible in the UI.

- **E-1893 - Improvement**

Postgres connection logging is now disabled to reduce the verbosity of debug logging. It can be enabled via config file as needed. For existing deployments, this setting must be changed manually.

- **E-1892 - Improvement**

Server performance and consistency is now improved when handling high volumes of concurrent sensor checkins.

- **E-1880 - Improvement**

The cbdiag tool now produces better and more accurate results with respect to sensor report data.

- **E-1849 - Improvement**

The computers page, which lists installed sensors, now includes a last-known power state. This includes states such as “powering off”, “rebooting”, and “suspending”. This can provide insight as to why a particular sensor is marked as offline.

- **E-1827 - Improvement**

A binary preview dialog has been added to the web UI, providing a quick at-a-glance summary of a binary without requiring navigation away from the current page.

- **E-1820 - Bugfix**

The “frequency data” pane sometimes showed the wrong data for child processes in event pane. This was obvious when it happened, as the name in the frequency pane did not match the name in the event table. In 4.0, the frequency pane now consistently matches the expected value.

- **E-1813 - Improvement**

First and last name for Enterprise Server user accounts can now include certain non-ASCII characters, particularly the umlaut and other diacritics used with the Latin alphabet.

- **E-1770 - Improvement**

Maximum Sensor Checkin Interval is now exposed as a cb.conf configuration option.

- **E-1735 - Improvement**

The Alliance Client can now be configured to avoid use of a SSL client certificate. This option requires coordination with Carbon Black support. It is intended to be used in environments where perimeter network devices do not support the user of SSL client certificates.

- **E-1710 - Improvement**

Configured feeds are not persisted to Postgres SQL. Previous feed configuration files in /etc/cb/feeds are no longer supported.

- **E-1643 - Improvement**

Internal communication between Enterprise Server components via HTTP is now more robust against deadlock and hangs through the use of considered timeout values.

- **E-1619 - Bugfix**

Event tagging is made more robust in cases where events are tagged in multiple segments of the same process.

- **E-1434 - Improvement**

The computers page no longer supports the idea of “hiding” or “unhiding” a sensor installation. Instead, all sensors that are both:

(a) not uninstalled
(b) not marked as pending uninstallation

are visible by default. The ‘Show Uninstalled Sensors’ on the computers page allows these sensors to be shown.

- **E-1430 - Improvement**

Sensor diagnostic data verbosity is reduced on sensor checkin. This results in lower write requirements in Postgres.

- **E-1344 - New Feature**

A Sensor may not be restarted via either the computers page, or the host detail page.

- **E-1327 - Bugfix**

Additional references to the anachronistic ‘modules’ term have been removed from the UI. They have been replaced with ‘binary’.

- **E-1309 - Improvement**

It is no longer possible to delete the current (active) user via the web UI. This sidesteps issues that resulted from having a UI session with no active user context.

- **E-1295 - Improvement**

User password changing via the web UI has been made more robust.

- **E-1211 - Improvement**

Search autocomplete now works with spaces.

- **E-1062 - New Feature**

Enterprise Server now supports “horizontal scaling”. This means that data can be distributed across two or more nodes of a cluster. Shards can be configured at setup time, or configured at any time after installation. In the case that the sharding strategy changes after installation, downtime may be required to transfer data and re-shard as necessary.

All existing functionality, including watchlists, search query, feeds, Alliance communications, licensing, and sensors, work as before.

Please contact Carbon Black support to determine best practices for a cluster environment.

- **E-512 - Improvement**

SOLR log verbosity has been reduced.

Carbon Black Enterprise Server 3.2.1

Changelog

- **E-2024 - Performance Improvement**

Limit process watchlist results to the last seven days of results in the watchlist page. This includes limiting the results themselves, updating the “last hit” histogram to account only for the last seven days, updating the displayed text to reference the seven day window. These changes improve the performance of the watchlist page by limiting the amount of data which needs to be processed.

- **E-2026 - Performance Improvement**

Default process search page to limit search results to the last 24 hours by default. This includes limiting the results themselves, in the UI with an adjustment of the “last modified” facet on the process search results page

- **E-2025 - Performance Improvement**

Allow individual facets to be removed from calculations both the process and binary search pages. This capability is triggered by adding the following two configuration options to cb.conf:

```
CoreServicesDisabledProcessFacets
CoreServicesDisabledBinaryFacets
```

Neither option is required. The value for the option is a comma-delimited list of one or more facets to avoid calculating. For larger data sets, it is recommended to avoid calculating two process facets: path_full and process_md5.

- **E-2023 - Performance Improvement**

Avoid performing search result highlighting on the watchlist page. Highlighting results are not displayed on the watchlist page and are therefore unnecessary.

- **E-1985 - Bugfix**

Server 3.2.0 release did not properly rotate logs in some cases. In particular, logs for nginx and SOLR were not properly logged. 3.2.1 addresses this issue by updating logger configuration to properly rotate logs.

- **E-1983 - Bugfix**

Enterprise server 3.2.0 did not properly execute a maintenance job, events_purge. The purposes of events_purge is to purge old event data from the process store. Because it was not execute properly, data was not deleted as aggressively as it should have been. 3.2.1 addresses this issue by updating the crond configuration to properly execute the events_purge job.

- **P-27 - Bugfix**

The /etc/cb directory may be owned by root in certain upgrade scenarios. This prevents certain licensing-related features from working properly. 3.2.1 addresses this issue by removing directory permission requirements.

Carbon Black Enterprise Server 3.2.0

Highlights

- **Simplified Licensing**

  Enterprise Server 3.2.0 completely replaces the licensing scheme from Enterprise Server versions 3.0.x and 3.1.x. The 'credit' model has been replaced with a single 'concurrent use with expiration' model. A single human-readable license file, /etc/cb/server.lic, provides a maximum count of simultaneous licenses sensors and a license end-date. Please contact your Carbon Black point-of-contact or support@carbonblack.com prior to upgrading to 3.2.0.

- **Improved Query Performance**

  Search performance, particularly on the process search and watchlist pages, has been improved through increased parallelization on the search backend.

- **Joined Search**

  Binary search characteristics, such as file version and digital signature information, is now searchable from the process search page. This makes it possible to perform a new set of queries not possible on 3.1.x.

- **User Logon Activity Monitoring**

  The history of UI user logon activity, including remote IP, is now available via the "Users and Teams" UI pages.

- **Enhanced Computer & Sensor Management UI**

  The "host detail" and "host list" pages, which track sensors, sensor groups, and computers, now include additional information for exploration and troubleshooting purposes.

- **Improved Bandwidth Throttling**

  The bandwidth throttling UI, available from the 'sites' section of the administration page, is improved in that a throttle may extend to multiple hours and can be extended via dragging.

- **Alliance Client Communications Enhancements**

  The Alliance Client, in the form of the cb-allianceclient service, can now communicate via web proxy, including web proxies with basic authentication.

- **Improved Data Purging**

  The background data purging logic, which helps keep disk usage at a consistent and reasonable level, is now improved.

- **Child Process Tagging**

  Child process creation and terminations are now tracked in the process analyze page, and can be tagged to an investigation. Support for child processes, including child process name and MD5, and count of child processes, are now supported in queries.

- **Alternate Browser Support**

  The UI is now usable in Internet Explorer 10, Safari 6, and Firefox 23. There are a small number of minor artifacts remaining - none affect core functionality. When the artifacts are removed, the banner indicating that the browser is unsupported will be removed.

Changelog

- U-382 - Improvement - Web UI

  Add criteria dialogs for digital signature status now include checkbox options rather open-ended text box. This makes options discoverable.

- U-425 - Improvement - Web UI

  Process analyze page events table now renders larger numbers of events at one time while scrolling down. This makes it easier and faster to see all events.

- U-443 - Bugfix - Web UI, Enterprise Server Backend

  Downloading sensor installers and binaries from the binary detail page is now done in a more straightforward manner, avoiding rare issues where the entire file was not downloaded.

- U-449 - Bugfix - Web UI

  Watchlist page now works properly with no watchlists.

- U-470, E-1081, E-1208 - New Feature - Web UI

  A new feature, the 'process preview' dialog, was added to the process analyze, process search, and watchlists page. It allows for the high-level summary of a process to be previewed via a dialog rather than requiring transitioning pages.

- U-473 - New Feature - Web UI

  Bandwidth throttle configuration can now be done on a multi-hour basis via mouse dragging. This compares favorably to the 3.1.0 bandwidth throttle configuration, which could only be done on an hour-by-hour basis.

- U-478 - New Feature - Web UI

  Bandwidth throttle configuration page now supports both local and GMT times to assist in setting appropriate time intervals for bandwidth throttles.

- E-342 - New Feature - Enterprise Server

  Enterprise Server components can now be run in a user-configurable user context. This compares with 3.1.0, which required that all Enterprise Server components run as the 'cb' user. User context can be specified in cb.conf.

- E-418, E-1040, E-1041 - Improvement - Enterprise Server

  Enterprise Servers now bind to the same interfaces for both ipv4 and ipv6 connectivity.

- E-1044 - Bugfix - Query Parser

  Negation queries with domain names now work as expected.

- E-1053 - Improvement - Enterprise Server

  Included nginx version is now upgraded from 1.2.6 to 1.4.1. The upgrade of nginx is performed automatically by the cb-enterprise installer on upgrade of the Enterprise Server.

- E-1054 - Improvement - Alliance Client, Web UI

  The Alliance client now supports connect via web proxies. Both un-authenticated and basic authentication are supported.

- E-1064 - New Feature - Enterprise Server, Web UI

  Joined binary and process searches are now supported. This means that any criteria supported in binary searches are now availble in the process search, and vice versa. In practical terms, this means a process search may now include binary details such as digital signature status, Virus Total hit count, and version number.

- E-1066 - Web UI - Improvement

  The web UI now provides proactive notification of licensing issues, including warning prior to license expiration.

- E-1155 - Enterprise Server, Web UI - New Feature

  Child processes are not presented as events in the process analyze page. This includes child process creation and termination. Child process events can also be 'tagged' to an investigation.

  Child process events are only shown from processes captured via a version 3.2.0 or greater sensor.

- E-1162 - Web UI - Improvement

  Sensor uptime is now tracked via the host detail page.

  Sensor uptime is only available for versions 3.1.0 and higher of the sensor.

- E-1204 - Web UI - Improvement

  Web UI's logon page now includes better indication of login status.

- E-1213 - Enterprise server - Bugfix

  cb-coreservices RPM now includes proper metadata, including associated e-mail address.

- E-1238 - Enterprise Server - Improvement

  Debug logging for cron jobs now includes appropriate prefix such that the cron job name is included in the log output.

- E-1241 - Enterprise Server - Improvement

  Sensor event logs are no longer written to disk temporarily during upload from sensor. This reduces disk load.

  This requires 3.2.0 or better sensors. Previous sensor versions continue to function, although event logs are temporarily written to disk as before.

- E-1245 - Enterprise server - Improvement

  Watchlist searcher cron job avoids holding open Postgres transactions while performing queries. This reduces number of open Postgres transactions.

- E-1252 - Web UI - New Feature

  Web UI login activity, to include username, timestamp, and remote IP, is now available via the web UI from the Users and Teams page.

- E-1267 - Enterprise Server - Improvement

  Watchlist notification e-mails now include the Carbon Black server name.

- E-1268 - Enterprise Server - New Feature

  Carbon Black now includes integration support for NVD. This allows for identifying binaries that are known-vulnerable based on the National Vulnerability Database.

- E-1300 - Enterprise Server - Improvement

  Licensing model has been overhauled and dramatically simplified.

- E-1316, E-1317 - Enterprise Server, Web UI - Improvement

  Host detail page now includes a listing of all communications failures with the Enterprise Server, including HTTP layer failures uploading event logs and binary files. The HTTP failure code is included in the logs.

- E-1318 - Web UI - Improvement

  The host detail page now includes a link to the process search page pre-filtered by that host.

- E-1326 - Web UI - Improvement

  Host detail page now includes dramatically more information and a new layout to improve sensor troubleshooting and information gathering.

- E-1369 - Enterprise Server - Improvement

  Accounts are now locked out after 10 successive failed authentication attempts. Accounts can be unlocked via the ‘cbpasswd’ script in /usr/share/cb. The number of successive logins before lock is configurable via cb.conf

- E-1411 - Web UI - Bugfix

  Binary detail page now avoids displaying duplicate filenames.

- E-1443 - Enterprise Server - Improvement

  Performance statistics are uploaded to api.cloud.carbonblack.com hourly rather than every twelve hours. This only occurs if ‘Community Participation’ is explicitly enabled in the Web UI’s setting page.

- E-1472 - Web UI - Bugfix

  Deleting the topmost (first) watchlist on the web UI’s watchlist page now works as expected.

- E-1475 - Web UI - Bugfix

  Cancelling the ‘Add Site’ dialog on the bandwidth throttle page now avoids redireting to the root page.

- E-1540 - Enterprise Server - Bugfix

  cb.conf is now restricted to the root user, for both read and write.

- E-1620 - Web UI - Improvement

  The 'reset search terms' button on both the binary and process search pages now resets all aspects of the search, including facets.

- E-1621 - Enterprise Server, Web UI - Bugfix

  Host detail page is now restricted to users that have view or greater access to the host's group.

- E-1622 - Web UI - Bugfix

  Search results page UI elements are now displayed consistently when no search results are returned.

- E-1639 - Enterprise Server - Improvement

  The data 'purge' cron job, which purges old process data to keep disk usage at operational levels, is now improved. In particular, it better handles cases where timestamps of process documents were incorrect due to sensors with incorrect clocks.

- E-1644 - Alliance Client - Behavior Change

  Alliance client changed to never upload customer-built watchlists to api.alliance.carbonblack.com.

- E-1651 - Web UI - Bugfix

  IP address 'Add Criteria' dialog box on web UI now works as expected.

- E-1729 - Enterprise Server - Bugfix

  Addresses issue that could occur when migrating 3.0.0 sensors from one group to another and simultaneously upgrading the sensor version. In this scenario, the sensor would no longer be able to communicate with the server.

- E-1730 - Web UI - Improvement

  E-mail subscription to a watchlist can now occur at the time of watchlist creation.

- E-1732 - Alliance Client - New Feature

  Alliance Client can now communicate without the use of SSL client certificates. This provides support for certain network environments that do not support passing SSL client certificates.

- E-1750 - Enterprise Server - Improvement

  Facet calculation is now performed in parallel rather than in series. This improves query performance on both the process and binary search pages.

- E-1520 - Enterprise Server - Improvement

  Provide additional control over sensor registration behavior when the computer SID cannot be determined.

- E-1781 - Web UI - Bugfix

  Investigations page event table can sometimes inappropriately wrap long text.

- E-1782 - Web UI - Improvement

  Timestamps are now properly rendered in Internet Explorer, Firefox, and Chrome

- E-1788 - Web UI - Bugfix

  In the process or binary search results, attempting to page forward to the second (or subsequent) page of results while a facet is selected results in an infinite spinner.