Carbon Black Version 5.0.0 Patch 3

Release Notes

Carbon Black v 5.0.0.150528.1341
28 May 2015

Bit9, Inc.
1100 Winter Street, Waltham, MA 02451 USA
Tel: 617.393.7400 Fax: 617.393.7499
E-mail: support@bit9.com
Web: http://www.bit9.com

Introduction

The *Carbon Black Version 5.0.0 Patch 3 Release Notes* document provides information for users upgrading from previous versions as well as users new to the product. It consists of the following major sections:

- **Before you begin**: This section describes preparations you should make before beginning the installation process for Carbon Black Server.
- **Carbon Black 5.0.0 Patch 3 new and modified features**: This section provides a quick reference to changes in Carbon Black since version 5.0.0 Patch 2.
- **Corrective content:** This section describes issues resolved by this release as well as more general improvements in performance or behavior.
- **Known issues and limitations:** This section describes known issues or anomalies in Carbon Black v5.0.0 Patch 3 that you should be aware of.
- **Contacting Bit9 support:** This section describes ways to contact Bit9 Technical Support and the information to have prepared to troubleshoot a problem.

This document is a supplement to the main Carbon Black Product documentation.

Important information

We recommend that you review these release notes carefully, especially the *New and modified features* and *Known issues and limitations* sections.

Purpose of this release

This release contains the following changes:

- Security and other bug fixes
- Performance improvements

No major new functionality was introduced in this version.

Documentation

The standard user documentation for Carbon Black includes:

- **Carbon Black User Guide:** Describes Carbon Black feature functionality in detail.

- **Carbon Black - Enterprise Server Sizing Guide:** Provides details on infrastructure sizing for Carbon Black.

Before you begin

This section describes preparations you should make before beginning the installation process for the Carbon Black server. These include actions you should take before installing the Carbon Black server, preparations you should make for configuring the server after installation, and general information you should know about the server and sensor. It contains information that applies to upgrades and new installations.

YUM URL:

Please use caution when pointing to the YUM repository. Different versions of the product are available on different branches as shown below:

The current 5.0.0 Patch 3 version is available on Carbon Black YUM, pointed to by the following base URL:

baseurl=https://yum.carbonblack.com/enterprise/stable/x86_64/

The current v4.2.x version is available on Carbon Black YUM, pointed to by the following base URL:

baseurl=https://yum.carbonblack.com/enterprise/release/x86_64/

System requirements

The document *Carbon Black - Enterprise Server Sizing Guide describes* the hardware and software platform requirements for the Carbon Black Server and provides the current requirements for systems running the sensor. Both are available in the customer support portal area of the Bit9 web site.

Both upgrade and new customers should be sure to meet the requirements specified in these documents before proceeding.

Carbon Black Server Installations and Upgrades

Carbon Black server upgrades are supported from the following Carbon Black server versions to this v5.0.0 Patch 3 version

- Version 4.1.5
- All 4.2.x versions
- All 5.0 versions, including earlier patch releases

For more detailed instructions for installing or upgrading the server, please refer to the *Carbon Black User Guide*. It is available in the support area of the Bit9 web site.

Support for the upgrade process

Carbon Black Server and sensor upgrade support is covered under the Customer Maintenance Agreement. Bit9 recommends contacting Technical Support prior to performing the upgrade, for further details on the upgrade process and the latest information that supplements the information contained in this document. Technical Support is available to assist with the upgrade process to ensure a smooth and efficient upgrade installation.

Server Upgrade Steps

If you are UPGRADING the server, please follow the steps in this section. These steps require SSH or console access to the server with root privileges.

- **Standalone Server**
    1. On the server, stop the Carbon Black services: service cb-enterprise stop
    2. Update the Carbon Black services: yum update cb-enterprise
    3. Restart the Carbon Black services: service cb-enterprise start

- **Clustered Server**

    1. On the Master server, navigate to the cb install directory (defaults to /usr/share/cb) and stop the Carbon Black services: ./cbcluster stop
    2. Update the Carbon Black services on all nodes: yum update cb-enterprise
    3. Restart the Carbon Black services: ./cbcluster start

Improvements of Carbon Black will occasionally require a utility called ‘cbupgrade’ to be used after *yum install cb-enterprise* to migrate the database schema or alliance feed data. Upgrading from previous stable version of Carbon Black (5.0.0 Patch 2) to current release is not expected to require this step. However, running the utility is required when there are local

changes to configuration files that have to be manually consolidated with the newer versions distributed by the release. The operator will be notified of this requirement when attempting to start the cb-enterprise services. In a clustered Server configuration, this utility will need to be run on all nodes before restarting the cluster. When running this utility in a clustered environment, be sure to answer ‘NO’ when asked to start the CB services, the administrator will need to use ‘cbcluster’ to start the clustered server.

Corrective Content

The following section provides the corrective content changes made for each patch release

Carbon Black v5.0.0 Patch 3:

Console and Server

1) Fixed the default disk usage threshold setting in cb.conf and config.py (E-4343)

2) Reworked API endpoint used by Administration | Sensors page so that it doesn't take too long to load with large number of sensors (E-4318)

3) Fixed the time format discrepancy in feed.storage.hit alerts (E-4321)

4) Fixed an issue with parsing of queries with multiple terms that have to be joined across binary and process data (E-4341)

5) Enabled ingress feed hits based on process execution with given md5 (E-4379)

Carbon Black v5.0.0 Patch 2:

Console and Server

1) Fixed an issue with deduplication of endpoint values in binary info documents that caused those documents to grow large in memory (E-4327)

2) Added support for reverse proxy setup with F5 proxy (E-4324)

Carbon Black v5.0.0 Patch 1:

Console and Server

1) Fixed an issue with rendering of process analyze page when process has too many srstrust hits (E-4218)

2) Fixed an issue with regmod tokenization for long paths (E-4207)

3) Fixed an issue with some Detect Dashboard graphs not rendering and throwing red toaster (E-4194)

4) Fixed an issue with use of site throttles available for throttling algorithm (E-4193)

5) Fixed an issue with check-in interval computation breaking data throttle and hammering on SQL (E-4184)

6) Fixed an issue with executable versus module detection in process search (E-4177)

7) Fixed an issue with data validation in sensor site throttle value (non-numeric) that allows null value in postgres table row that shouldn't allow nulls (E-4163)

8) Fixed an issue with fields that cbsyslog utility returns not matching what server returns under normal operation (E-4156)

9) Fixed an issue with cbsyslog utility failing ungracefully when there is no query to match (E-4109)

10) Fixed an issue with cbsyslog utility not submitting the query string correctly (E-4107)

11) Fixed an issue with watchlist_searcher tagging all documents due to erroneous queries (E-4102)

12) Fixed an issue with e-mail notifications from watchlist not recovering from error and requiring restart of cluster (E-4095)

13) Fixed an issue with alert severity and criticality not correctly reported for Binary feed hit (E-4079)

14) Fixed an issue with binaryinfo.group and binaryinfo.host events not being published on the bus; cb-notifications-binaryinfo.log file is not generated (E-4062)

15) Fixed an issue with navigating to the "last" process event during a default process query on a machine that has millions of process docs, causing solr problems (E-4061)

16) Fixed an selinux issue with /var/cb/nginx/props/nginx.runtime.cblr_api.client_body_temp_path.prop permissions (E-4035)

17) Fixed an issue with dashboard_stats job failing on clustered servers (E-4013)

18) Fixed an issue with minion nodes failing on DashboardStatisticsUpdate enterprise task.. (E-3964)

19) Fixed an issue with cbstats utility producing traceback with new solr.select_reqs.cpu.pct metric (E-3911)

20) Fixed an issue with 'cache' throttle pressure that may cause low ingress rate cap even when server is not being loaded (E-3880)

21) Fixed an issue with changing feed rating score not triggering recalculation of alert severity (E-3864)

22) Fixed an issue with process search / day of week facet missing processes started on saturday (E-3861)

23) Fixed an issue with query parsing when searching for multiple alliance_score_<feed> in (E-3832)

24) Fixed an issue with graceful handling of API access with an invalid sensor ID in coreservices (E-3778)

25) Fixed an issue with connect failed errors in nginx log (E-3766)

26) Fixed an issue with sensor report producing an error that reports data is out of range (E-3728)

27) Fixed an issue with license application does not working properly in a clustered environment (E-3922)

28) Fixed an issue with creating watchlists from Alliance feeds defaulting to wrong sort option for process watchlists (CBUI-1249)

29) Fixed an issue with selecting "all" option for Alliance Feed add criteria (CBUI-1239)

30) Fixed an issue with date range alert searches on Firefox creating "endless" loop (CBUI-1233)

31) Fixed an issue with using third party mail vendor for Mail Server configuration (CBUI-1217)

32) Fixed an issue with count and IP address range queries not working with Firefox (CBUI-1208)

33) Fixed an issue with searching for IP information crashing the CB UI (CBUI-1125)

34) Fixed an issue with Sensor group filter not filtering on "Sensor Version" (CBUI-982)

Windows Sensor (5.0.1.150401)

1) Fixed an issue with parent process being set incorrectly for existing processes (WIN-215)

2) Fixed an issue with missing md5 and process path metadata in the event header of majority of netconn events (WIN-213)

3) Fixed an issue with incorrect reference count increment on process context (WIN-208)

4) Fixed an issue with incorrect, but easily performed, driver unload order (WIN-206)

5) Fixed an issue with cross-process events appearing to cause memory of cb.exe to grow (WIN-188)

6) Fixed an issue with Windows7+ upgrades causing carbonblackk.sys file to be updated or removed (WIN-159)

7) Fixed an issue with MD5 of all zeros being reported in few cases (WIN-146)

8) Improved handling of cross-process events for lsass process (WIN-116)

9) Fixed an issue with reporting of destination port with inbound connections (WIN-268)

OS X Sensor (4.2.6.150323)

1) Fixed an issue with obtaining certificate info that caused memory leak in sensor (OSX-170)

2) Fixed an issue with certain network responses with nested indirect names causing sensor to go into infinite loop (OSX-168)

3) Fixed an issue with binary signature status being reported by sensor as "undefined" (OSX-172)

Linux Sensor (4.2.6.150413)

1) Fixed access permissions of sensitive files for the sensor (LNX-128)

2) Fixed an issue with incorrect time stamps on events (LNX-126)

3) Fixed an issue with handling of file rename (delete and create) (LNX-120)

4) Fixed an issue with reporting of network connection domain name URL (LNX-119)

5) Fixed an issue with modload classification (LNX-118)

6) Fixed an issue with sensor not sending hostname with netconns (LNX-117)

7) Fixed an issue with the amount of data send to the server by earlier version of sensor (LNX-108)

Carbon Black v5.0.0:

The following is additional corrective content in this version, along with some security vulnerabilities which have been addressed:

1) 1) Fixed feed synchronization issue by including the default value during startup. (ENT-3898)

2) Included other IOC hit attributes (in addition to ioc_value and ioc_type) as a JSON field in feed events. (ENT-3471)

3) Modifying DatastoreRootDir in cb.conf now updates solr.xml during startup. (ENT-3417)

4) Investigation Times are now sorted correctly - When investigations are sorted by time, they used to be "string ordered" based on day of week instead of day of the month and time. (ENT-3543)

5) For customers installing on RedHat, cb-enterprise install required a wxBase package, which was not part of the CarbonBlack yum repo. The wxBase package is now part of CarbonBlack yum repo. (ENT-3563)

6) Fixed issue where "cbcluster add-node" command could fail on start with cb-rabbitmq timeout message - The issue is related to cbcluster add-node command attempting to start cb-rabbitmq cluster on the head node before it does anything else. According to RabbitMQ Clustering guide when the entire cluster is brought down, the last node to be shutdown must be the first node to come back up. (ENT-3635)

7) Improved internal API calls to collect server statistics. (ENT-3693)

8) Fixed Nginx startup issue after CentOS/RedHat SELinux policy updates. (ENT-3749)

9) Fixed internal Datastore JVM memory pressure. (ENT-3761)

10) Sensor throttle stops all eventlog ingest due to an error in accounting of total number of bytes committed to SOLR index. (ENT-3733)

11) Fixed an issue with combined search queries that include ‘alliance_score_<feed>’. (ENT-3832)

12) Fixed issue where links from investigations pane for analyze returned 404 error. (CBUI-941)

13) On process analyze page, Reg Action and Sig facet fields now jump into the right position. (CBUI-942)

14) Addressed bug whereby two subsequent network connections via different domain names but the same underlying IP were both reported using the first of the two domain names. (WIN-152)

15) Fixed issue wherein CB sensor causing BSOD - Machines are also part of an AV-Container of Kaspersky that have the encryption modules present. ONLY the machines with both the encryption modules AND CB installed ended up with Blue screen. (WIN-181)

Carbon Black v5.0.0 Patch 3: OS Support

Server / Console:

- CentOS 6.4-6.6, (64-bit)
- Red Hat Enterprise Linux (RHEL) 6.4-6.6 (64-bit)

Installation and testing is done on default installs using the 'minimal' distribution and the distribution’s official package repositories. Customized Linux installations must be individually evaluated.

Sensor OSes (endpoints + servers)

- **Windows**: XP SP3 - 8.1 / Server 2003 - 2012R2, x86 and x64
  - Windows embedded OSes are individually evaluated
- **Mac**: OS X 10.6 through 10.10, x64 on Intel

- **Linux:** RHEL & CentOS 6.4-6.6, 7.0 x64 – standard kernel versions (2.6.32-358.el6, 2.6.32-431.el6, 2.6.32-504.el6, 3.10.0.el7.x86_64) and the standard minor/ maintenance releases. Non RHEL/CentOS distributions or Modified RHEL/CentOS environments (those built on the RHEL platform) are not supported.
  Note: Major releases of 6.7 and 7.1 will require moving to the next patch of the sensor.

The Linux sensor now supports Redhat/CentOS 6.4,6.5,6.6, and 7.0 without the need for a patch. The release of a major revision, such as 6.7 or 7.1 will require the release of a patch.

Known Issues and Limitations

1. If sensor clock is wrong and in the future, UI does not interpret process start time correctly. (CBUI-1102)
2. The state of the sensor changes to "Uninstall Pending Uninstalled" when uninstalling from the UI. (ENT-3698)
3. When a sensor is moved out of a group with a user on a team with only "Viewer" access to that particular group, results for that group are still searchable for the time period it was in that group, but the process details page links get 405 errors. If the sensor is put back into the group, the 405 errors for those processes go away. (ENT-3788)
4. Reshard tool can fail with “File Not Found” exception in turn causing a corrupt index. If a re-shard is necessary please contact support for a potential work around. (ENT-3493)
5. Power state of a Linux sensor is not displayed correctly on the host detail page - When Linux Sensor is powered off, icon next to Computer Name does not change to correct state. (LNX-53)
6. On Win7 64-bit and Win8.1 systems that also have the Bit9 Agent installed, uninstalling the sensor fails with an “insufficient permissions” error unless Bit9 tamper protection is disabled. Please contact Bit9 Support if you need assistance disabling tamper protection. (WIN-204)
7. The sensor is sending duplicate module info events (WIN-276)

8. Mac OS X sensor does not correctly handle relative paths (OSX-179)
9. Lost filemod data on Mac OS X sensor (OSX-178)

Contacting Bit9 Support

For your convenience, Bit9 Technical Support offers several channels for resolving support questions:

Technical Support Contact Options
Web: www.bit9.com
E-mail: support@bit9.com
Phone: 877.248.9098 (877.**BIT9**.098)
Fax: 617.393.7499
Hours: 8 a.m. to 8 p.m. EST

Reporting Problems

When you call or e-mail Bit9 Technical Support, please provide the following information to the support representative:

Required Information	Description
Contact	Your name, company name, telephone number, and e-mail address
Product version	Product name (Carbon Black Server and Carbon Black Sensor version)
Hardware configuration	Hardware configuration of the Carbon Black Server or computer (processor, memory, and RAM)
Document version	For documentation issues, specify the version of the manual you are using. The date and version of the document appear after the copyright section of each manual.

Problem	Action causing the problem, error message returned, and event log output (as appropriate)
Problem severity	Critical, serious, minor, or enhancement