Carbon Black
Version 4.2.7
Release Notes

Carbon Black v4.2.7.150629.0500

10 July 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 4.2.7 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 4.2.7 new and modified features**: This section provides a quick reference to changes in Carbon Black since version 4.2.5.
- **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 v4.2.7 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 *major new feature functionality* as well as quality and performance improvements.

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 v5.1.0 is available on Carbon Black YUM, pointed to by the following base URL:

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

The current v4.2.7 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 v4.2.7 version

- v4.1.5
- All 4.2.x versions

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.

Before running the server upgrade

Carbon Black v4.2.7 comes with updated sensor versions. Before you run the Carbon Black Server upgrade program, you should determine if you would like to upgrade to the new sensor version. Servers and Sensors can be upgraded independently, and sensors can be upgraded by sensor groups, rather than all at once.

Decide if you would like to the new sensor to be deployed immediately to existing sensor installations, or if you want to install only the server updates first. Bit9 recommends a gradual upgrade of sensors to avoid any unacceptable impact on network and server performance.

Note: There is no expected degradation to sensor performance with Carbon Black 4.2.7

Deployment of sensors can be configured via the web UI in the following manner:

1. Log in to the web UI, navigate to the ‘Sensors’ page, and edit the group settings for each active group:

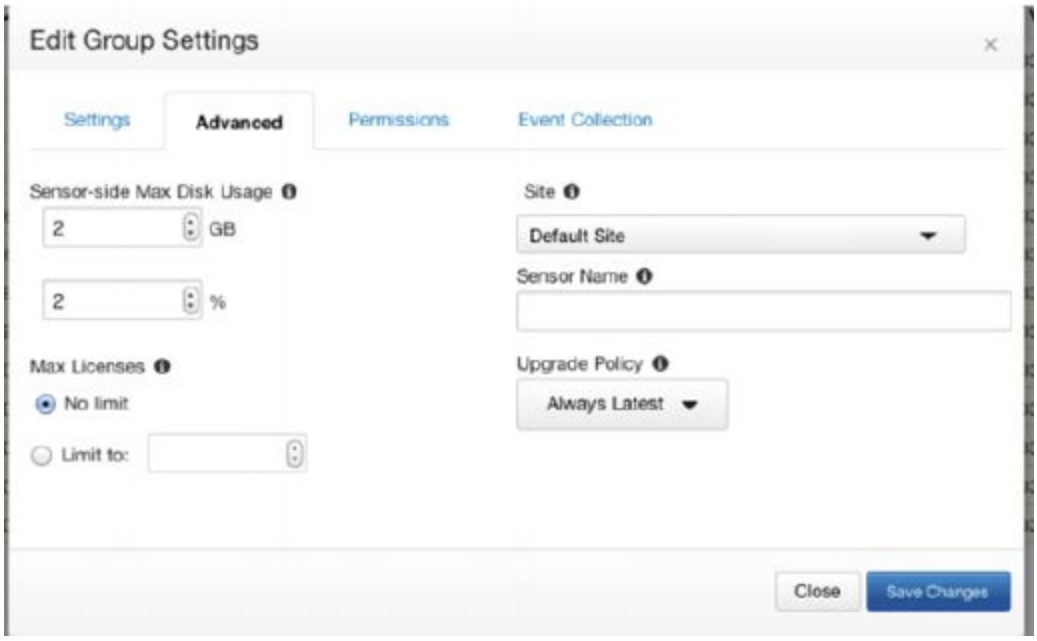

Figure Group settings dialog

2. Under the ‘Advanced’ tab, find the “Upgrade Policy” setting. If this is set to “Always Latest”, the server will automatically sensors to the latest sensor version. If you want to keep the sensors at a specific version, select that version number from the dropdown prior to upgrade. If you want to continue using whatever sensor versions are already installed, regardless of version, select ‘Manual’.

Note: These settings apply to Windows sensors only . To change OS X and Linux sensor settings please see the Installing and Managing Sensors chapter of the Carbon Black User Guide .

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 and minions 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) 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 release

Carbon Black 4.2.7

Console and Server (4.2.7.150629.0500)

1) cbsyslog fails with some event types (E-4197)
2) Analyze preview throws toaster for process with unknown path and name (CBUI-1471)
3) Security fixes

Windows Sensor (4.2.7.150625.0326)

1) None

OS X Sensor (4.2.7.50624)

1) A race condition in the daemon would occasionally cause it to crash. This has been corrected. (OSX-209)

Linux Sensor (4.2.7.50624)

1) The Linux sensor now gracefully handles DNS timeouts. (LNX-98)
2) An issue was fixed involving RPM name collision of the Linux sensor installer package installed on the cb-enterprise server. (LNX-137)
3) Support for Redhat/Centos 7.1 has been added. (LNX-144)
4) The Linux sensor will now ignore its own operations. (LNX-152)
5) The subsystem start/shutdown sequence was adjusted to avoid a potential race condition. (LNX-154)

Carbon Black 4.2.5

Console and Server (4.2.5)

4) Fixed an issue with cbsyslog utility that caused it to fail ungracefully when there are no matches to a submitted query (E4110)
5) Fixed an issue with cbsyslog utility that caused it to submit the query string incorrectly (E4108)
6) Fixed an issue with cbsyslog utility that caused it to send syslog notifications with missing fields (E4156)
7) Fixed an issue that caused binary downloads to fail from the UI when hash reporting is enabled, but binary uploads to Alliance server is disabled (E4063)
8) Fix email notifications from watchlist not recovering from an error (E4095)

Windows Sensor (4.2.5.50223)

2) Fix for Sensor Group Netconn event collection not working properly when disabled and reenabled (WIN233)
3) Fixed an issue with downgrades of sensor from 5.0.0 to 4.2.x resulting in mix of driver versions (WIN229)
4) Fix for an issue that caused upgrades from 4.2.x to 4.2.4 fail in some cases (WIN224)
5) Fix for a name resolution issue that for certain network responses with nested indirect names causing sensor to go into an infinite loop (WIN223)
6) Performance enhancement to move discarding of modload events to kernel module
7) (WIN209,WIN153)
8) Fixed an issue that caused sensor to occasionally report corrupted MD5 in mod info message (WIN151)

OS X Sensor (4.2.5.50217)

2) Fix for a memory leak in sensor while obtaining certificate information (OSX170)
3) Fix for a name resolution issue that for certain network responses with nested indirect names causing sensor to go into an infinite loop (WIN168)

Linux Sensor (4.2.5.50305)

6) Fix for sensor not correctly honoring the bytestopush value set by throttling algorithm (LNX113)
7) Upgrade OpenSSL to version 1.0.1k (LNX112)
8) Performance enhancement for CBonCB case by filtering UID of the CB server (LNX110)
9) Fix a memory leak in sensor on CentOS 2.6.32.358 kernels (LNX109)
10) Fix for a name resolution issue that for certain network responses with nested indirect names causing sensor to go into an infinite loop (LNX106)

Carbon Black v4.2.7: OS Support

Server / Console:

- CentOS 6.46.6, (64bit)
- Red Hat Enterprise Linux (RHEL) 6.46.6 (64bit)

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 6.46.6, 7.0 , 7.1 x64 – standard kernel versions (2.6.32358.el6, 2.6.32431. el6, 2.6.32504. el6, 3.10.0.el7.x86_64, 3.10.0-129.el7.x86_64, 7.1 - 3.10.0-229.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. Licensing application does not work properly in a clustered environment. When licenses are applied via the UI, they are applied against the master only. The minions do not get an updated license. When the minion license expires, there is no indication of that in the UI. The minion does, however start rejecting data push to the server from sensors via the 402 HTTP error code. (ENT-3922)

2. If sensor clock is wrong and in the future, UI does not interpret process start time correctly. (CBUI1102)

3. The state of the sensor changes to "Uninstall Pending Uninstalled" when uninstalling from the UI. (ENT3698)

4. 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. (ENT3788)

5. Reshard tool can fail with “File Not Found” exception in turn causing a corrupt index. If a reshard is necessary please contact support for a potential work around. (ENT3493)

6. 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. (LNX53)

7. Count and IP address range queries do not work correctly using Firefox v.30+. (CBUI1208)

8. On Win7 64bit 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. (WIN204)

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