Release Notes: Server v6.2.4

November 2018

Summary

New! We've updated our Release Notes format to be clearer. Cloud and On-Prem release notes have been combined into a single document, we've trimmed out old content, updated the format to match other Carbon Black products. Let us know what you think!

Cb Response 6.2.4 is a maintenance release of the Cb Response server and console. The 6.2.4 release contains the first set of changes for Enhanced Permissions and bug fixes and improvements throughout the console. The goal of enhanced permissions is to give users greater granularity in user permissions through consistent application of the Principle of Least Privilege, and moving the ability to use core product functionality from Global Admin to Analyst.

For a broad look at Enhanced Permissions, please refer to the post about Enhanced Permissions on UeX.

Enhanced Permissions Changes

- Results consistently limited to team assignments. (CB-21281)
- Sharing/Settings Page is only visible for Global Admins. (CB-21289)
- Users Page is only visible to Global Admins. (CB-21299)
- Server Dashboard is only visible to Global Admin. (CB-21300)
- Cb Live Response permission is now usable by user if that user's team has Analyst access to the sensor group. A user must have Analyst access for at least one sensor group to see the Go-Live page. (CB-21298)

Postgres SQL Upgrade (CB-21420)

1. Postgresql93 should be installed during first service startup after 6.2.4 upgrade. By default yum will not remove postgresql. If the yum configuration option `clean_requirements_on_remove` is enabled it may try to remove the packages. To migrate server data, ensure postgresql93 packages are not removed until the services have been started at least once.
2. The postgresql.conf file will be re-initialized to default settings during the upgrade. If manual changes were made, review and update the file accordingly. Old postgresql.conf file will be copied into pgsql data directory to postgresql.conf.old file.
3. All previous 9.3 data will remain in a folder named "pgsql.93" in the cb data directory. The folder can be safely deleted after the migration is complete.

Erlang Package Upgrade (CB-22166)

- Due to a bug in the previous Erlang package, the Erlang dependency of RabbitMQ may not automatically update to the version required for Cb Response 6.2.4 to function correctly.
- If the correct version is not installed when starting the Cb Response server services, it will warn that an incorrect version of Erlang was detected and fail to start.

- If the Erlang package does not update to 20.3.8.9 automatically as part of the server upgrade, please run `yum update erlang` while pointing to the Cb Response 6.2.4 yum repository.

This release includes the following components:

- Server version 6.2.4.181101.1217
  Release Notes: (this document)
- Windows Sensor version 6.1.9.181012.1229
  Release Notes:
  https://community.carbonblack.com/t5/Documentation-Downloads/Cb-Response-Windows-Sensor-6-1-9-Release-Notes/ta-p/60306
- macOS Sensor version 6.2.2.180803
  Release Notes:
  https://community.carbonblack.com/t5/Cb-Response-Knowledge/Cb-Response-MacOS-Sensor-6-2-2-Release-Notes/ta-p/33038
- Linux Sensor version 6.1.8.10098
  Release Notes:
  https://community.carbonblack.com/t5/Documentation-Downloads/Cb-Response-Linux-Sensor-v6-1-8-Release-Notes/ta-p/59568
- Linux Sensor Version 5.2.17.
  Release Notes:
  https://community.carbonblack.com/t5/Documentation-Downloads/Cb-Response-Linux-Sensor-v5-2-17-Release-Notes-pdf/ta-p/50106

Each release of Cb Response software is cumulative and includes changes and fixes from all previous releases.

Document contents

This document provides information for users upgrading to Cb Response Server version 6.2.3 from previous versions as well as users new to Cb Response. The key information specific to this release is provided in the following major sections:

- **Preparing for Server Installation or Upgrade** – Describes requirements to meet and key information needed before beginning the installation process for the Cb Response server.
- **New features** – Provides a quick reference to the new and modified features introduced with this version.
- **Corrective content** – Describes issues resolved by this release as well as more general improvements in performance or behavior.
- **Known issues and limitations** – Describes known issues or anomalies in this version that you should be aware of.

Additional documentation

This document supplements other Carbon Black documentation. Click here to search the full library of Cb Response user documentation on the Carbon Black User eXchange.

Technical support

Cb Response server and sensor update releases are covered under the Customer Maintenance Agreement. Technical Support is available to assist with any issues that might develop during the installation or upgrade process. Our Professional Services organization is also available to assist to ensure a smooth and efficient upgrade or installation.

Note: Before performing an upgrade, Carbon Black recommends reviewing content on the User eXchange for the latest information that supplements the information contained in this document.

[On-Prem Only] Preparing for Server Installation or Upgrade

This section describes requirements to meet and key information needed before beginning the installation process for the Cb Response server. All on-premises users, whether upgrading or installing a new server should review this section before proceeding. Next, see the appropriate section of the *Cb Response Server/Cluster Management Guide* for version 6.2.4 for specific installation instructions for your situation:

- **To install a new Cb Response server**, see “Installing the Cb Response Server”.
- **To upgrade an existing Cb Response server**, see “Upgrading the Cb Response Server”.

Yum URLs

Cb Response Server software packages are maintained at the Carbon Black yum repository (yum.distro.carbonblack.io). **The links will not work until the on-premises Cb Response Server is released.**

Our yum links for the Cb Response server have changed. The links below make use of variables to ensure that you install the correct version of Cb Response based on your machine's OS version and architecture.

Use caution when pointing to the yum repository; different versions of the product are available on different branches as follows:

- **Specific version:** The 6.2.4 version described here is available from the Carbon Black yum repository specified in the following base URL:

  baseurl=https://yum.distro.carbonblack.io/enterprise/6.2.4-1/$releasever/$basearch

  This link will remain available as long as this specific release is available. It can be used to get to this release even after later versions have been released, and so can be useful if you want to add servers to your environment while maintaining the same version you already have installed.

- **Latest version:** The latest supported version of the Cb Response server is available from the Carbon Black yum repository specified in the following base URL:

  baseurl= https://yum.distro.carbonblack.io/enterprise/stable/$releasever/$basearch/

  This will point to version 6.2.4-1 until a newer release becomes available, at which point it will automatically point to the newer release.

Note: Communication with this repository is over HTTPS and requires the presence of appropriate SSL keys and certificates. During the Cb Response server install or upgrade process, other core CentOS packages may be installed to meet various dependencies. The standard mode of operation for the yum package manager in CentOS is to first retrieve a list of available mirror servers from http://mirror.centos.org:80 and then select one of those mirrors to download the actual dependency packages. If your Cb Response server is installed behind a firewall that blocks access to the outside, it is up to the local network and system administrators to ensure that the host machine is able to communicate with standard CentOS yum repositories.

[On-Prem Only] System Requirements

Operating system support for the server is listed here for your convenience. The document *Cb Response Operating Environment Requirements* document describes the full hardware and software platform requirements for the Cb Response server. This document is available on the Carbon Black User eXchange.

Both upgrade and new customers should be sure to meet all of the requirements specified here and in the Operating Environment Requirements before proceeding.

Server / Console Operating Systems

Note: For best performance, Carbon Black recommends running the latest supported software versions.

- CentOS 6.7-6.10 (64-bit)
- CentOS 7.3-7.5 (64-bit)
- Red Hat Enterprise Linux (RHEL) 6.7-6.10 (64-bit)
- Red Hat Enterprise Linux (RHEL) 7.3-7.5 (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 Operating Systems (for Endpoints and Servers)

For the most up-to-date list of supported operating systems for Cb Response sensors (and all Cb endpoint products), refer to the following page in the Carbon Black User eXchange:

https://community.carbonblack.com/docs/DOC-7991

Note: Non RHEL/CentOS distributions or modified RHEL/CentOS environments (those built on the RHEL platform) are not supported.

Configure Sensor Updates Before Upgrading Server

Cb Response 6.2.4 comes with updated sensor versions. 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 the new sensor to be deployed immediately to existing sensor installations, or if you want to install only the server updates first. Carbon Black recommends a gradual upgrade of sensors to avoid any unacceptable impact on network and server performance and strongly recommends reviewing your Sensor group Upgrade Policies before upgrading your server to avoid inadvertently upgrading all of the sensors across your

environment at once. For detailed information on Sensor Group Upgrade Policy, please refer to the “Sensor Groups” chapter of the *Cb Response User Guide* for version 6.2.4.

To configure deployment of new sensors via the Cb Response web UI, follow the instructions found in the “Installing Sensors” chapter of the *Cb Response User Guide*.

New features

- We’ve updated several package dependencies to latest versions throughout the Cb Response Server. List of packages we’ve upgraded to:
    - **[CentOS/RHEL 6-series only]** Python 2.7.15 (CB-21305)
    - Openresty-1.13.6.2 (CB-21304)
    - Erlang 20.3.8.9
- The 6.2.4 version of the server adds CentOS / RHEL 7.4 and 7.5 qualifications (CB-21246)
- The sensor communications failure table has been removed and the sensor communications failures are now written to a log file at /var/log/cb/sensor_comm_failures/sensor_comm_failures.log (CB-19707)
- In Process Search, we’ve created a new menu called “Counts” that contains the “Count” Criteria previously found in several other menus. (CB-18415) The Counts Criteria found under this new menu are:
    - Count of modified files
    - Count of binary mod loads
    - Count of child procs
    - Count of netconns
    - Count of regmods
- We’ve added new Sensor Group Facet on the Triage Alerts page, allowing users to filter Triage Alerts to only those groups they need to see. (CB-21651)

Corrective Content

- Query blocking functionality now correctly applies when changing the time-frame. (CB-20346)
- Fixed an issue that could result in positives in some cases. (CB-18300)
- Resolve an issue where some characters were stripped from searches when running a saved search from the HUD. (CB-16899)
- Fixed an issue where cbssl sensor_certs would fail. (CB-17069)
- Fixed an issue where customers with large numbers of sensor groups, users and/or teams would experience long load times on the Triage Alerts page. (CB-16862)
- Fixed an issue where creating a watchlist from a Threat Intel field resulted in an incorrect query. (CB-20781)

Known Issues

6.2.4

- Creating a new team will grant “Analyst Access” to all sensor groups on creation. (CB-22702)
- Clicking the “Reset Search” button on the Process Search page does not reset the page view. (CB-22492)
- When doing a net-new installation, the “Administrators” Team created during the setup process will not have access to the Default Sensor group on creation. The Administrators team will need to be given access to the Default sensor group manually. (CB-22645)

Earlier Versions

1. If the browser timezone is different from the server timezone, you might notice discrepancy in the last check-in time shown for Sensors. (CB-20076)
2. CSV export of user activity audit is malformed in certain cases. (CB-18936)
3. CSV Export of ‘Recently Observed Hosts’ has no header row. (CB-18927)
4. When using a custom email server, you are unable to enable or disable Alliance Sharing. The workaround for this is to disable the custom email server, make the change, then re-enable customer email server. (CB-20565).
5. In order for sensor upgrades to work properly, McAfee EPO may need to be configured to exclude c:\windows\carbonblack\cb.exe from its "Prevent creation of new executable files in the Windows folder" option. [CB-7061]

Contacting Support

Use one of the following channels to request support or ask support questions:

- **Web:** User eXchange
- **Email:** support@carbonblack.com
- **Phone:** 877.248.9098
- **Fax:** 617.393.7499

Reporting Problems

When contacting Carbon Black Technical Support, be sure to provide the following required information about your question or issue:

- **Contact:** Your name, company name, telephone number, and email address
- **Product version**: Product name (Cb Response server and sensor version)
- **Hardware configuration:** Hardware configuration of the Cb Response server (processor, memory, and RAM)

- **Document version:** For documentation issues, specify the version and/or date of the manual or document you are using
- **Problem:** Action causing the problem, error message returned, and event log output (as appropriate)
- **Problem severity:** Critical, serious, minor, or enhancement request