Release Notes: Server v6.2.3

August 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 6.2.3 is a maintenance release of the Cb Response server and console. The 6.2.3 release contains support for CentOS 7, enhancements to watchlists, bug fixes and performance improvements.

This release includes the following components:

- Server version 6.2.3.180809.1703
  Release Notes: (this document)
- Windows Sensor version 6.1.7.180722
  Release Notes: https://community.carbonblack.com/docs/DOC-15837
- macOS Sensor version 6.2.2.180803
  Release Notes: https://community.carbonblack.com/docs/DOC-16232
- Linux Sensor version 6.1.7.10053
  Release Notes: https://community.carbonblack.com/docs/DOC-15613
- Linux Sensor Version 5.2.17.
  Release Notes: https://community.carbonblack.com/docs/DOC-15614

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 6.2.3 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-prem GA date**.

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 6.2.3 version described here is available from the Carbon Black yum repository specified in the following base URL:

  baseurl=https://yum.distro.carbonblack.io/enterprise/6.2.3-1/$releasever/$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 6.2.3-1 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 and sensors 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 and provides the current requirements for systems running the sensor. 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 6.2.3 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 Group section of the *Cb Response User Guide* for version 6.2.3.

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

New features

- CentOS7 and RHEL7 support is now available for new on-prem server installations. For more information, please refer to the CentOS 7 / RHEL7 Release Announcement on UeX
- Cb Response now supports CentOS 6.10
- CbR Global Admin can now block interactive process searches containing leading wildcards or binary metadata in the console. These settings are enabled by default. Global Admins can control this behavior in the console under “Settings > Advanced Settings.” Additionally, the settings may be set in cb.conf. If set in cb.conf, the UI settings are forced to a specific value, grayed out and are not configurable.
    - Note: This feature only applies to interactive searches in the console. Searches executed via the API, existing watchlists or feeds will not be impacted by these settings.
- This release includes several enhancements to watchlist capabilities.
    - The **Watchlists list view** now shows the status of the watchlist, including the following:
        - Queued – Watchlist is still in the queue, waiting to be run.
        - Expired – Watchlist has not had any hits in the specified time period.
        - Timeout – Watchlist has timed out.
        - Error – Watchlist has errored out.
    - Watchlists can now be **sorted by duration** in the List view. When sorting by duration, the list will show any errored- or timed-out Watchlists first, followed by the slowest- or longest-running Watchlists.
    - The **Watchlist details view** now shows the following new data:
        - Timeout – Watchlist execution has timed out. The next attempt will be tried with a recent timestamp. If this persists, investigate the performance of the query or consider deleting the Watchlist.
        - Error – Watchlist execution failed due to an error. If this error persists, please consult Carbon Black Technical Support.
        - Execution time and duration – (Example) Last successful Watchlist execution was 4 minutes ago, duration was 0.04 s.
- In certain cases, advanced users might want to ignore .rpmnew files when upgrading. We’ve added a command line argument to allow users to ignore these files when upgrading. *Note - ignoring .rpmnew files can cause significant issues with your CbR installation if used improperly. You should only use this option if directed by support.* (CB-19564)

- Added *hostname* to the CbLR Audit logs so customers don't need to manually convert IPs to hostnames. (CB-18140)
- Added new facet to search for Username on the Process Search page. If the user has a domain, that will be part of the user name. (CB-20297)
    - You may need to add the Facet on the Process Search page after the upgrade. Do this by clicking on the gear icon next to the Filters menu in the Facet list, and select "Username."
- Added an API to allow users to see recent solr queries. The API takes two forms: "/api/v1/query/stats" and "/api/v1/query/stats/collate"; the former returns the entries as-is (sorted by duration, longest first), and the latter groups the entries based on query and query source (so that you can more easily see aggregate statistics for repeated queries). Both forms accept the optional arguments "?limit=N" (sets the number of results to return) and "?query_source=XXX" (to filter by query source, e.g. "?query_source=ui") (CB-18106)

Corrective Content

This release provides the following corrective content change:

- Fixed an issue where the console had problems communicating with Alliance over a proxy connection. (CB-19556)
- Fixed an issue with in-app notifications introduced in 6.2.2. (CB-19770)
- Resolved a bug where sensor throttle upgrade would lose throttle configurations in some situations. (CB-16160)
- Fixed an issue where using Sensor LastCheckIn Time filters didn't always return expected results. (CB-17114)
- Fixed an issue where the UI wasn't timing out as expected. (CB-19182)
- Fixed the formatting of DNS IOCs in IPv4 format. (CB-19376)
- Fixed an issue where adding EAP Threat Intel feed URLs manually would fail. (CB-20350)
- Increased performance on the site throttle page when working with a large number of sites. (CB-19355)
- Updated the start-up sequence to ensure that sshd starts before any Cb Response services. (CB-19487)
- Increased performance in Investigations with a large number of tagged events. (CB-14001)
- Fixed an issue where the Cb Protection Settings checkboxes were always checked, even when unchecking. (CB-14931)

Known Issues

Invalid query when creating a watchlist from a Threat Feed

When creating a watchlist from Threat Feed, Cb Response incorrectly creates the query and the watchlist will not run, and error. To see if you watchlist created from a threat feed has errored, please check the Watchlist page for the status. As a workaround, the Cb Response Team suggests clicking on the *Search Binaries* or *Search Process* hyperlinks on the threat feed and then *Add/Create Watchlist* action from the search page.

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