CB RESPONSE

Release Notes: Server v7.2.0

July 2020

Summary

CB Response 7.2.0 is a feature release of the CB Response server and console (now known as VMware Carbon Black EDR). The CB Response 7.2.0 server includes two new beta features – Live Query and Anti-Malware Scanning Interface (AMSI) Support together with bug fixes. This version of the server release also has CentOS/RHEL 7.8 Support. See the New Features section for details.

These release notes include the following:

This release includes the following components:

- Server version 7.2.0.200713

Release Notes: (this document)

- Windows Sensor version 7.0.1.16744
  Release Notes
- MacOS Sensor version 6.3.0.16031
  Release Notes
- Linux Sensor version 6.3.2.10003
  Release Notes

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 who are upgrading to CB Response Server version 7.2 from previous versions, and for users who are 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 information needed before beginning the installation process for the CB Response server.
- **New features** – Provides a quick reference to new and modified features that are introduced in this version.

- **Corrective content** – Describes issues that are resolved by this release, and general improvements in performance or behavior.
- **Known issues and limitations** – Describes known issues or anomalies in this version.

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.

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

This section describes the requirements and key information that is needed before installing a CB Response server. All on-premises users, whether upgrading or installing a new server, should review this section before proceeding. See the appropriate section of the *CB Response 7.2 Server/Cluster Management Guide* 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.

The following links use variables to make sure that you install the correct version of CB Response, based on your machine's operating system 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 7.2.0 version is available from the Carbon Black yum repository that is specified in the following base URL:

baseurl=https://yum.distro.carbonblack.io/enterprise/7.2.0-1/$releasever/$basearch

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

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

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

This URL will point to version 7.2.0-1 until a newer release becomes available, at which time it will automatically point to the newer release.

Note: Communication with this repository is over HTTPS and requires appropriate SSL keys and certificates. During the CB Response server install or upgrade process, other core CentOS packages can 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 a mirror from which to download the dependency packages. If a CB Response server is installed behind a firewall, local network and system administrators must make sure that the host machine can 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 *CB Response 7.2 Operating Environment Requirements* document describes the full hardware and software platform requirements for the CB Response server and provides the current requirements and recommendations for systems that are running the sensor. This document is available on the Carbon Black User Exchange.

Both upgrading and new customers must meet all of the requirements specified here and in the *CB Response 7.2 Operating Environment Requirements* document before proceeding.

Server / Console Operating Systems

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

- CentOS 6.7-6.10 (64-bit)
- CentOS 7.3-7.8 (64-bit)
- CentOS 8.1 (64-bit)
- Red Hat Enterprise Linux (RHEL) 6.7-6.10 (64-bit)
- Red Hat Enterprise Linux (RHEL) 7.3-7.8 (64-bit)
- Red Hat Enterprise Linux (RHEL) 8.1 (64-bit)

Installation and testing are performed on default install 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 current list of supported operating systems for CB Response sensors, see 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 Update Settings Before Upgrading Server

CB Response 7.2.0 comes with updated sensor versions. Servers and sensors can be upgraded independently, and sensors can be upgraded by sensor groups.

Decide whether you want the new sensor to be deployed immediately to existing sensor installations or install only the server updates first. Carbon Black recommends a gradual upgrade of sensors to avoid network and server performance impact. We strongly recommend that you review your sensor group upgrade policies before upgrading your server, to avoid inadvertently upgrading all sensors at the same time. For detailed information on Sensor Group Upgrade Policy, see the Sensor Group section of the *CB Response 7.2 User Guide*.

To configure the deployment of new sensors via the CB Response web console, follow the instructions in the *CB Response 7.2 User Guide*.

New Features

Live Query (beta)

Live Query is an implementation of the osquery tool on the CB Response Server. osquery is an open source project that uses an SQLite interface. Live Query can expose an operating system as a high-performance relational database. Users can write SQL-based queries that explore operating system data to analyze security vulnerabilities. This release includes recommended queries from our Threat Intelligence team.

Live Query is released as a beta feature in this server version. Please see the *CB Response 7.2. User Guide* for more information. Live Query beta requires the Windows 7.1.0 sensor. VMware Carbon Black welcomes all customer feedback on this feature as we continue to develop it for general availability.

Anti-Malware Scanning Interface (AMSI) Support (beta)

CB Response now provides Anti-Malware Scanning Interface (AMSI) support for endpoints running Windows 10 RS2 or higher. The Windows sensor records these events as “fileless scriptload” events. This event represents each instance the sensor detects AMSI-decoded script content that was executed by a process on the endpoint. The collection of AMSI events can be toggled in the VMware Carbon Black EDR Console, through sensor group settings. Collection of the data is disabled by default. AMSI events can be forwarded through the Event Forwarder in JSON and LEEF.

AMSI support is available as a beta feature in CB Response 7.2.0 server release, 3.7.0 Event Forwarder release, and later releases with the Windows 7.1.0 sensor. Please see the *CB Response 7.2 Integration Guide* for more information. VMware Carbon Black welcomes all customer feedback on this feature as we continue to develop it for general availability.

Event Forwarder Configuration via UI for Cloud Customers

Cloud customers can configure the CB Response Event Forwarder from the server console. This feature allows Cloud customers to self-serve Event Forwarder configuration without any assistance from Carbon Black support.

See the *CB Response 7.2 User Guide* “Configuring the Event Forwarder” chapter for more information.

Please note: This feature was already available for on-prem customers with the 7.1 server release.

Corrective Content

1. The ban hashes screen will no longer display any errors if a ban is requested for the same hash more than once. [CB-28662]
2. Ability to change read time out for Solr based stats collection, which was initially hard coded to 5 seconds. With larger timeout configuration option, the stats collection may not report constant timeouts on heavy system attempting to collect Solr stats via cbstats. [CB-30037]
3. Properly applies the value configured on CbFileDescriptorLimit for EL7 [CB-27866]
4. Server certificates must not contain exactly two SAN DNS entries. EDR will not accept a server certificate where one SAN DNS entry is an FQDN and the other entry is a bare hostname that matches the FQDN. For example, the below setup will not be permitted. DNS.1=myserver.example.com and DNS.2=myserver. [CB-29295]
5. Configuring bundle_send_max parameter while setting up an AWS S3 bucket or other outputs via Event Forwarder configuration API will not throw a 400 error. [CB-31102]
6. When a watchlist is created from a process search, neither "q=" or the URL will be displayed. Pre-filled search query will only include the query component. [CB-30014]
7. When viewing, editing, or creating a watchlist the query will be displayed without any URL components such as “q=”. Queries may be written in these modals just as they are written on the process or binary search pages. Queries pasted in URL format will work as expected. [CB-30019]
8. If a request is made to the EDR server using an HTTP address instead of HTTPS, the user is redirected to the HTTPS version of the request URL, for proper security. Carbon Black EDR server is configured to restrict host header redirections to avoid attacks. [CB-30454]
9. Usernames and directories that include special characters such as an apostrophe are now displayed correctly in the Process Analysis page. [CB-18698]
10. Fixed an issue where notifications stopped happening on systems with no smtp server password [CB-31488]
11. Following a new, successful login, the Activity Audit page will not show a 403 entry related to that login. [CB-27159]
12. Error wherein user cannot reset a threat feed rating back to the default value is fixed [CB-31315]
13. There was a bug in the /api/v1/feed/<feed_id> endpoint such that it was possible to submit undesired values for the local_rating property of a feed. With this fix, any submitted value that is lower than the minimum value (1) will be coerced to 1; any submitted value that exceeds the maximum value (5) will be coerced to 5. Note that this was only possible if the API was called directly – the EDR console already constrains the value of this property. [CB-31316]

14. RabbitMQ presented expected behavior. The error indication has been corrected and promoted to the DEBUG log level, so it no longer fills the user logs with unusable service exception information. [CB-31317]

Known Issues

1. After an upgrade of server and sensor, older files did not get SHA-256 values. When an older file is executed, it creates a process event that contains SHA-256. When a user clicks the link, the binary store shows no SHA-256. [CB-24519]
2. When creating a watchlist from a Threat Feed, CB Response incorrectly creates the query and the watchlist does not run – it creates an error. To see if your watchlist formed an error, check the status on the Watchlist page. As a workaround, the CB Response team suggests clicking the **Search Binaries** or **Search Process** hyperlinks on the Threat Feed, and then using the **Add/Create Watchlist** action from the Search page.
3. The CSV export of the user activity audit is malformed in certain cases. [CB-18936]
4. The CSV export of **Recently Observed Hosts** has no header row. [CB-18927]
5. When using a custom email server, you cannot enable or disable Alliance Sharing. The workaround is to disable the custom email server, make the change, and re-enable the custom email server. [CB-20565]
6. Process searches using *_md5, md5, *_SHA256, SHA256 are case-sensitive in SOLR 6.x. These searches were case-insensitive in SOLR 5.x. [CB-14311]
7. A bug in SOLR 6 (https://issues.apache.org/jira/browse/SOLR-9882.) is causing incomplete results when partialResults=True. The Pagination bar, together with a large number, will appear on the Process Search page as a result of a search. However, only a few or even zero actual documents are displayed. [CB-30074]
8. LiveQuery [BETA] feature does not respect SensorInactiveLookupDays in Total sensor count. [CB-31136]

Contacting Support

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

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, provide the following required information:

- **Contact:** Your name, company name, telephone number, and email address
- **Product version**: Product name (CB Response server and sensor versions)
- **Hardware configuration:** Hardware configuration of the CB Response server (processor, memory, and RAM)
- **Document version:** For documentation issues, specify the date of the manual or document you are using
- **Problem:** Action causing the problem, the error message returned, and event log output (as appropriate)
- **Problem Severity:** Critical, serious, minor, or enhancement request

Note: Before performing an upgrade, Carbon Black recommends that you review the content on the User Exchange.