CB RESPONSE

Release Notes: Server v7.0.1

February 2020

Summary

CB Response 7.0.1 is a platform release of the CB Response server and console. The CB Response 7.0.1 server includes upgrades of two major third party applications - Python 3 and SOLR 6, both of which are used by CB Response Server.

These release notes include the following:

- Document Contents
- [On-Prem Only] Preparing for Server Installation or Upgrade
- Configure Sensor Update Settings Before Upgrading Server
- New Features
- Corrective Content
- Known Issues
- Contacting Support

This release includes the following components:

- Server version 7.0.1.200205

  Release Notes: (this document)

- Windows Sensor version 6.2.5.91203
  Release Notes

- MacOS Sensor version 6.2.7.15949
  Release Notes

- Linux Sensor version 6.2.2.10003
  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 7.0 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 the new and modified features that are introduced with 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 Server Cluster Management Guide* 7.0 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 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 7.0.1 version is available from the Carbon Black yum repository that is specified in the following base URL:

  baseurl=https://yum.distro.carbonblack.io/enterprise/7.0.1-1/$releasever/$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 7.0.1-1 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 the presence of 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 Operating Environment Requirements* document describes the full hardware and software platform requirements for the CB Response server and provides the current requirements 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 Operating Environment Requirements* document 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 7.3-7.7 (64-bit)
- Red Hat Enterprise Linux (RHEL) 6.7-6.10 (64-bit)
- Red Hat Enterprise Linux (RHEL) 7.3-7.7 (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 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 Update Settings Before Upgrading Server

CB Response 7.0.1 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 User Guide*.

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

New Features

Technical Currency

Third-party software that the CB Response server uses will be updated to maintain software currency and a better security posture.

Upgrade to Python 3

Python 2 will be at the End of Life status in early 2020. CB Response Server will be on Python 3 from 7.x series onwards. All existing features will work as expected after the upgrade. Python 3 provides improved Unicode support.

Upgrade to SOLR 6

Cb Response will upgrade from SOLR 5 to SOLR 6. No action is required from customers for the upgrade.

New and Improved Sensor Detail Page

Cb Response 7.0.x server has a new and improved Sensor Detail page. The new design highlights the most important stats and actions. The new page design has a cleaner and more accessible interface.

The sensor details page shows sensor check-ins and registrations for the last 30 minutes.[CB-28551]

Live Response Enhancements

CB Live Response can configure throttling and chunk size on the server interface. Users can improve their quality of service according to their site bandwidth and stability limitations.

- All memdumps are compressed by default from 6.2.5 Windows sensor onwards. [CB-13082]
- The current progress of data transfer in the Live Response terminal is displayed. Users can track the progress or identify whether it is a stale request [CB-27084]

Additional File Types Supported

The CB Response Server will support .lnk and .swf file types starting with 7.x series. [CB-28707] Please note: These file types are supported on 6.2.5 Windows sensor onwards. This option is available on the Windows sensor only.

Display Threat Report Name

The Report name is displayed instead of or together with the Report ID. This feature is controlled by the `FeedHitLoadReportTitles` setting in `cb.conf`. This setting is set to **False** by default (feature is turned off). To turn on the feature, set `FeedHitLoadReportTitles` to **True** and restart the cb-enterprise services.

Note: Please use this feature with caution. Additional memory will be used, proportional to the number of reports on your server.

The length of the Report Title can be controlled through the `FeedHitMaxReportTitleLength` setting. The default value is set to 80, which is also the maximum length. The value for this setting should be between 0 and 80.

With these settings enabled:

1. Threat Report names (titles) are populated in the Triage Alerts hit records without being truncated.
2. The addition of the "report_title" field with the truncated value of the feed report name is populated in event bus events.
3. The "report_title" field with the truncated value of the feed report name is populated in syslog notifications.
4. The "report_title" field with the truncated value of the feed report name is populated in email notifications.
5. Both Report ID and Report name is displayed in the email. If the feature is turned off, the Report Name is displayed as *Unknown*.

Corrective Content

1. Error handling is added to the api/info endpoint so that it will not return a 500 error when invalid data is passed. [CB-29117]
2. All Crossprocs, ProcessOpen or ThreadOpen were shown in the Events table of the Process Analysis page as "ThreadOpen" types. This fix correctly shows different Crossproc types. [CB-25512]
3. In prior versions, Unicode text (for example, filenames) within alert records was improperly stored and was not rendered properly in the console. This is fixed in version 7.0.x. [CB-27405]
4. The **Export Alerts to CSV** link on the Alerts page works as expected. [CB-28665]
5. The parser in the server recognizes the new line in the query syntax from Process Analysis Page and does not throw a 400 error. [CB-27636]
6. The diagnostics data collection script, cbdiag, has been corrected by removing the attempted collection of the watchlist_action_settings table that no longer exists. This was producing an error (ERROR: relation "watchlist_action_settings" does not exist) in the `/var/log/cb/pgsql/postgresql.log` every time the cbdiag collection was run. [CB-28400]
7. 7.0.x-svr will support rabbitmq 3.7.19 or above which has the fix for the `cbrabbitmqctl` report command. [CB-29371]
8. Sensors were not being properly displayed when the browser was in a different timezone than the sensor. With this fix, the time zone differences should not impact server/browser communication with relation to sensors check-ins. [CB-20076]
9. If a sensor group is created without the server URL (sensorbackend_server), sensors that are moved to this group cannot submit data. The fix prevents new sensor groups from being created without the server URL. [CB-28742]
10. Long CBLR command prompts used to be handled with a scrollbar. This fix allows the command prompts to be word wrapped; commands typed at a long command prompt shows each character as they are being typed.[CB-29219]
11. The /api/communication_settings GET previously allowed analysts to retrieve communication settings. Global admin permissions are now required for this API to reflect the POST for the endpoint. [CB-28684]

12. The diagnostics data collection script, cbdiag, has been corrected by removing the attempted collection of the watchlist_action_settings table (which no longer exists in the product), which was producing an error (ERROR: relation "watchlist_action_settings" does not exist) in the `/var/log/cb/pgsql/postgresql.log` every time the cbdiag collection was run. [CB-28400]

13. The error condition in which the Unified View (UV) portal failed to display Process Analysis results correctly is resolved. The servers now agree on Content Security Policy and the icons from the cluster appear correctly on the UV portal presentation. [CB-27709]

14. Updates to feed reports require the report timestamp to be updated in order for the server to recognize that a feed report change has occurred. Please refer to this page for additional details. This code change allows an updated or modified feed report to take effect on the CB Response server even if the feed report timestamp has not been updated. This requires a special `cb.conf` flag and setting; contact VMware Carbon Black Technical Support to enable this capability. [CB-29575]

15. 500 error is not returned when the `_xsrf_token` cookie is not sent in the request. Instead, the `X-XSRFToken` header is checked as a fallback so the ADFS SSO redirect does not fail.[CB-29409]

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 on the link, the binary store shows no SHA-256.[CB-24519]

2. Invalid query when creating a watchlist from a Threat Feed. When creating a watchlist from a Threat Feed, CB Response incorrectly creates the query and the watchlist does not run and it creates an error. To see if your watchlist that was created from a threat feed that 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, then re-enable the custom email server. [CB-20565]

6. The current version of `logback.qos.ch` used in CB Response server is leaving large sizes .tmp files. The next server release will have a newer version of the same library with a fix for this issue. [CB-14090]

7. Process searches using *_md5,md5, *_SHA256, SHA256 are case-sensitive in SOLR 6.x, This was case-insensitive in SOLR 5.x. [CB-14311]
8. A bug in SOLR 6 ([https://issues.apache.org/jira/browse/SOLR-9882.](https://issues.apache.org/jira/browse/SOLR-9882)) is causing incomplete results when `partialResults=True`. The Pagination bar together with a large number appears on the Process Search page as a result of a search. However, only a few or even zero actual documents are displayed.

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 VMWare 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 version and/or 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.