CB RESPONSE

Release Notes: Server v7.1.0

April 2020

Summary

CB Response 7.1.0 is a feature release of the CB Response server and console (now known as VMware Carbon Black EDR). The CB Response 7.1.0 server includes new Enterprise Linux version support, console features, and TLS fingerprinting support together with bug fixes. See the New Features section for details.

These release notes include the following:

This release includes the following components:

- Server version 7.1.0.200327

  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 6.3.0.10191
  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 7.1 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 7.1 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 7.1.0 version is available from the Carbon Black yum repository that is specified in the following base URL:

  baseurl=https://yum.distro.carbonblack.io/enterprise/7.1.0-1/$releasever/$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 7.1.0-1 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 7.1 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 7.1 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 7.3-7.7 (64-bit)
- CentOS 8.1 (64-bit)
- Red Hat Enterprise Linux (RHEL) 6.7-6.10 (64-bit)
- Red Hat Enterprise Linux (RHEL) 7.3-7.7 (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 7.1.0 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 7.1 User Guide*.

To configure the deployment of new sensors via the CB Response web console, follow the instructions in the *CB Response 7.1 User Guide*.

New Features

Enterprise Linux(EL) 8 Installation

VMware Carbon Black EDR server supports CentOS/RHEL 8.1. During installation of EL8 servers, run the following commands:

```
$ sudo yum module disable postgresql redis
```

```
$ sudo yum install cb-enterprise
```

Postgresql and Redis must be disabled to successfully install CB EDR Server on EL8.

Note: CB Response Server upgrades from EL6 or EL7 to EL8 are not supported at this time – only fresh installs on EL8 are supported.

Adding temp directory for cbdiag

The feature is for servers that have limited space in `/tmp`. Currently, `--tmpdir=/desired/location` must be passed on each cbdiag execution to make sure that `/tmp` is not used, and another mount with less space constraint is used instead. You can now permanently configure the `\tmp` location for generated staging and temp files.

To set this feature on `cb.conf`:

1. Edit `/etc/cb/cb.conf`
2. Add token `CbDiagTmpDir=/desired/location` (`example: /var/cb/data`). We recommend that this is done on all nodes.

After it is set, staging/temp files are generated at the `CbDiagTmpDir` location instead of `/tmp`.

Logon Type in Process Summary

Logon Type information from Windows Process Executions is available under **Process Summary** on the Process Analysis Page. You can use this data for querying, investigation, and analysis in the CB Response Server console (for Windows 6.2.5 and higher sensors only). Users can search with `logon_type` Queryparser token. See the *CB Response 7.1 User Guide* for more information.

TLS Fingerprinting

Transport Layer Security (TLS) fingerprinting is a platform-independent method for creating TLS fingerprints that can easily be shared for improved threat intelligence. TLS fingerprints are properties of a netconn event for TCP connectivity only.

TLS fingerprinting is available with the 7.1 release of CB Response Server (for Windows 7.0.0 and higher sensors only). It provides additional endpoint telemetry that can be delivered to the CB Response server, and can be used for narrowing investigations of known malware by identifying known TLS fingerprints.TLS fingerprints can be specified as IOCs in custom threat feeds. See the *CB Response 7.1 User Guide "*Netconn Metadata*"* chapter for more information.

Configure the Event Forwarder from the CB Response Server Console

With this release, you can configure the CB Response Event Forwarder from the server console. Cloud customers can self-serve Event Forwarder configuration without any assistance from Carbon Black support. Customers must install *CB Response Eventforwarder 3.6.2 or higher* (available here) to use this feature.

On prem customers can enable this feature by adding `EventForwarderEnabled=true` in `cb.conf` and restarting services.

This feature is currently not available for Cloud customers. It will be turned on by the end of April 2020. The supporting version of Eventforwarder will automatically be available for all Cloud customers.

See the *CB Response 7.1 User Guide* "Configuring the Event Forwarder" chapter for more information.

Configure Ingress Filter from the CB Response Server Console

With previous server versions, you could set up ingress filtering via API only. Starting with 7.1, global admins can view, edit, modify ingress filters in the CB Response Server console. See the *CB Response 7.1 User Guide* "Ingress Filtering" chapter for more information.

Corrective Content

1. When creating a new watchlist, a new option is available to avoid performance overload. You can choose the interval at which to query the existing data. This value is set to **Last day** by default. [CB-29549]

2. cbdiag uses the `netstat` command to collect a list of listening and connected ports. However, this is a deprecated command on RHEL 7.x and is not installed on those systems by default. cbdiags that run on a RHEL 7.x system are missing that data. [CB-27382]

3. `Cb.conf` value `DatastoreJvmMax` is obsolete and will be removed from existing `cb.conf` files during a `cbupgrade` operation. [CB-29579]

4. The `logback.qos.ch` that the CB Response server uses is not leaving large `.tmp` files. [CB-14090]

5. Clicking the **Reset search** button now correctly changes the label of the timeframe dropdown to **Last 3 days**. Clicking the **Reset search** button now correctly enables fetching filters for future searches. If there are search results, Carbon Black now always requests filters. [CB-22492]

6. Remote attackers with an analyst role level cannot change major features for sensors by sending restricted data via PUT request into API Endpoint. With this fix, the restricted data is blocked from modifying the sensor. [CB-28683]

7. Carbon Black is now using a more performant API on the HUD Alerts widget; this saves bandwidth. [CB-29056]

8. In previous versions, a filter would show a **0.0%** ratio if it was .04% or fewer. Now, we display **<0.1%** for filters that have that low a ratio on the Process search, Triage Alerts, Binary Search, and Threat Report Search pages. [CB-29325], [CB-29730]

9. The Unified View instance health check call was failing with invalid credentials even though the correct authorization token was used in the configuration. This was caused by a race condition with the auth token in use while the UV server was iterating through configured instances. This fix alleviates this race condition. [CB-30137]

10. A corrupt MD5 field in `cbmodule` docs could result in an infinite loop in the `modulestore` purge job. The server now checks that docs being queued for deletion by this job have a valid MD5 before they are added to the list of docs to be removed. [CB-29322]

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]

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 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.