Release Notes: Server v7.4.0

January 2021

Summary

VMware Carbon Black EDR 7.4.0 is a feature release of the VMware Carbon Black EDR (formerly CB Response) server and console. This release contains Tamper Protection, bug fixes, and other small-scale enhancements. This release also introduces RHEL/CentOS 7.9 support. See the New Features section for more details.

This release includes the following components:

- Server version 7.4.0.201215
  Release Notes (this document)
- Windows Sensor version 7.2.0.17354
  Release Notes
- MacOS Sensor version 7.0.1.16317
  Release Notes
- Linux Sensor version 7.0.1.14543
  Release Notes

Each release of VMware Carbon Black EDR software is cumulative and includes changes and fixes from all previous releases.

Document Contents

This document provides information for users who are upgrading to VMware Carbon Black EDR Server version 7.4.0 from previous versions, and for users who are new to VMware Carbon Black EDR and are installing it for the first time.

The key information specific to this release is provided in the following major sections:

- **[On-Prem Only] Preparing for Server Installation or Upgrade** – Describes requirements to meet and information needed before beginning the installation process for the VMware Carbon Black EDR 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** – 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 VMware Carbon Black EDR 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 VMware Carbon Black EDR server. All on-premises users, whether upgrading or installing a new server, should review this section before proceeding. See the appropriate section of the *VMware Carbon Black EDR 7.4 Server/Cluster Management Guide* for specific installation instructions for your situation:

- **To install a new VMware Carbon Black EDR server**, see "Installing the VMware Carbon Black EDR Server".
- **To upgrade an existing VMware Carbon Black EDR server**, see "Upgrading the VMware Carbon Black EDR Server".

Yum URLs

VMware Carbon Black EDR Server software packages are maintained at the Carbon Black yum repository (yum.distro.carbonblack.io). The links will not work until the on-prem General Availability (GA) date.

The following links use variables to make sure you install the correct version of VMware Carbon Black EDR, 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 7.4.0 version is available from the Carbon Black yum repository, that is specified in the following base URL:

  baseurl= https://yum.distro.carbonblack.io/enterprise/7.4.0-1/$releasever/$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 VMware Carbon Black EDR 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 7.4.0-1 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 VMware Carbon Black EDR 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 VMware Carbon Black EDR 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 *VMware Carbon Black EDR 7.4 Operating Environment Requirements* document describes the full hardware and software platform requirements for the VMware Carbon Black EDR server and provides the current requirements and recommendations for systems that are running the sensor.

Both upgrading and new customers must meet all of the requirements specified here and in the *VMware Carbon Black EDR 7.4 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 - 7.9 (64-bit)
- CentOS 8.1 - 8.2 (64-bit)
- Red Hat Enterprise Linux (RHEL) 6.7 - 6.10 (64-bit)
- Red Hat Enterprise Linux (RHEL) 7.3 - 7.9 (64-bit)
- Red Hat Enterprise Linux (RHEL) 8.1 - 8.2 (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.

However, if the customers are pinning dependencies to a specific OS version, the product only supports the following software versions for the Carbon Black EDR Server and Unified View:

- CentOS 6.7 - 6.10 (64-bit)
- CentOS 7.5 - 7.9 (64-bit)
- CentOS 8.2 (64-bit)
- Red Hat Enterprise Linux (RHEL) 6.7 - 6.10 (64-bit)
- Red Hat Enterprise Linux (RHEL) 7.5 - 7.9 (64-bit)
- Red Hat Enterprise Linux (RHEL) 8.2 (64-bit)

Note: Versions 7.3, 7.4, and 8.1 (64-bit) of CentOS/RHEL are not supported if customers are pinning dependencies.

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 VMware Carbon Black EDR 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

VMware Carbon Black EDR 7.4.0 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 *VMware Carbon Black EDR 7.4 User Guide*.

To configure the deployment of new sensors via the VMware Carbon Black EDR web console, follow the instructions in the *VMware Carbon Black EDR 7.4 User Guide*.

New Features

Tamper Protection MVP

Tamper Protection provides more security to the EDR Windows sensor by blocking local admin attempts to inject, remove, modify, or delete the sensor by protecting the sensor service, drivers, files, folders, registry settings and other sensor components. Please see the *VMware Carbon Black EDR 7.4 User Guide* for more information. Tamper Protection requires minimum versions of both EDR Server 7.4.0 and Windows Sensor 7.2.0.

Corrective Content

1. Removed the checkbox for turning on/off the sensor-group level sharing options for Hosted EDR (Cloud) instances. [CB-21791]

2. When BinarySharingKillSwitch is set to True on cb.conf, it will no longer interfere with the cb-supervisord service start up status. This will allow the cb-enterprise services to restart properly. [CB-29282]

3. Watchlists created from Threat Intel Feeds now use correct search query syntax and execute as expected. [CB-29925]

4. IPADDR range queries related to treatment of IPv4 addresses as signed integers when the range query crosses from positive to negative values now work as intended. [CB-30742]

5. Crossproc event descriptions in the Process Analysis page events list are now displayed in the correct direction (Process A launched Process B). [CB-31139]

6. The value of the "local_rating" is now properly validated, and if the value is incorrect, it will result in a 400 response with an explanatory payload. [CB-31324]

7. EDR now tracks the configured run state of Event Forwarder, so that on reboot of the server, or restart of cb-enterprise (EDR), the Event Forwarder Connector returns to the state (running or stopped) for which it was configured at the time the reboot or restart command was initiated. [CB-32558]

8. Improved error logging for failures to add partitions in the solr_client. [CB-31750]

9. If any of these conditions (report id is null, report id is numeric instead of string, and report name is null) are detected, an error message will now be printed on the

   /var/log/cb/enterprise/enterprise.log and the report feed will not be allowed to be added to the cbfeeds. [CB-32019]

10. Throttle APIs will now return consistent data if invoked repeatedly in rapid succession. [CB-32674]

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, VMware Carbon Black EDR 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 VMware Carbon Black EDR 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. For Server versions 6.x.x - 7.1.0, based on Solr 6.x, Process Searches using `*_md5,md5, *_SHA256, SHA256` are case-sensitive. These searches were case-insensitive in pre-6-series Server versions, based on SOLR 5.x. [CB-14311] This issue is resolved in Server 7.1.1 +.

7. For Server versions 6.x.x - 7.2.0 (all versions based on SOLR 6.x), a bug in SOLR 6 (https://issues.apache.org/jira/browse/SOLR-9882.) causes 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] The fix for this issue has not yet been validated in Server 7.3.0 +, based on Solr 8.

8. cb-enterprise fails to install on RHEL/CentOS 8 with FIPS 140-2 enabled. The workaround is to use RHEL/CentOS 7 if you'll enable FIPS 140-2. This issue is due to a

change on Red Hat 8 that affected Paramiko (https://bugzilla.redhat.com/show_bug.cgi?id=1778939). This issue is being addressed on RHEL/CentOS 8.4. [CB-33352]

Contacting Support

VMware Carbon Black EDR 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 (VMware Carbon Black EDR server and sensor versions)
- **Hardware configuration:** Hardware configuration of the VMware Carbon Black EDR 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 you review the related content on the User Exchange.