VMware Carbon Black EDR

Release Notes: Windows Sensor v7.1.0

July 2020

Summary

VMware Carbon Black EDR Windows Sensor v7.1.0 is intended to provide support for two new beta features - Live Query and Antimalware Scan Interface (AMSI) support in addition to bug fixes and other improvements. This sensor release also includes all changes and fixes from previous releases.

This document provides information for users upgrading to VMware Carbon Black EDR Windows Sensor v7.1.0 from previous versions as well as users new to VMware Carbon Black EDR. The key information specific to this release is provided in the following major sections:

- **Installation Instructions** - Provides instructions for VMware Carbon Black EDR Windows sensor installation.
- **New features** – Describes new features introduced in this release.
- **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.

Server compatibility

VMware Carbon Black EDR sensors included with server releases are compatible with all server releases going forward. It is always recommended to use the latest server release with our latest sensors to utilize the full feature capabilities of our product, however, using earlier server versions with the latest sensor should not impact core product functionality.

Sensor operating systems

VMware Carbon Black EDR sensors interoperate with multiple operating systems. For the most up-to-date list of supported operating systems for VMware Carbon Black EDR sensors (and all VMware Carbon Black products), refer to the following location in the VMware Carbon Black User eXchange: https://community.carbonblack.com/docs/DOC-7991

Documentation

This document supplements other VMware Carbon Black documentation. Click here to search the full library of VMware Carbon Black EDR user documentation on the VMware Carbon Black User eXchange.

Technical support

VMware Carbon Black EDR 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, VMware Carbon Black recommends reviewing content on the User eXchange for the latest information that supplements the information contained in this document.

Installation Instructions

To install the sensors on to your server, run through the following instructions:

1. Ensure your VMW CB EDR YUM repo is set appropriately:
    a. The VMW CB EDR repository file to modify is */etc/yum.repos.d/CarbonBlack.repo*
    b. Baseurl = https://yum.distro.carbonblack.io/enterprise/stable/$releasever/$basearch/
2. On the VMW CB EDR server, clear the YUM cache by running the following command:
    a. yum clean all
3. After the YUM cache has been cleared, download the sensor install package by running the following command:
    a. Run *yum install --downloadonly --downloaddir=<package local download directory> <package>*
        i. **Note:** The *<package local download directory>* is a directory of your choice
        ii. **Note:** *<package>* is replaced by *cb-sensor-7.1.0.16951-win*
4. Install the new sensor package on the VMW CB EDR server by running the command:
    a. rpm -i --force <package>
5. Make the new installation package available in the server console UI by running the command:
    a. */usr/share/cb/cbcheck sensor-builds --update*
        i. **Note:** If your groups have *Automatic Update* enabled, the sensors in that group will start to automatically update.

Your new sensor versions should now be available via the console. For any issues, please contact VMware Carbon Black Technical Support.

Important Note: It is always encouraged to conduct a reboot of the endpoint after installation (or restart) of our sensor to ensure the sensor properly captures the full historical data of all running processes and associated information.

New Features

This release provides the following new beta feature content:

- **Live Query**: Live Query is an implementation of the osquery tool on the CB EDR Server/Windows sensor. 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. Please see the CB Response 7.2. User Guide for more information. Live Query beta requires both the Windows 7.1.0 sensor and 7.2.0 EDR Server. [CB-27939]
- **Antimalware Scan Interface (AMSI) Support**: 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. [CB-29872]

Corrective Content

This release provides the following corrective content changes:

- Improved sensordiag.exe to allow users to configure file output location when generating sensor diagnostics. [CB-30135]
- Fixed a bug where "Events Dropped in IQE->CBE" appeared twice in the DriverStats.log [CB-30802]
- Fixed a bug that could cause duplicate process start events under certain conditions. [CB-30877]
- Fixed a bug with throttling IPv6 network connections. [CB-31140]
- Fixed a bug with tracking PID value for UDP network connections under certain conditions. [CB-31199]

- Fixed a bug with TCP network connections causing high cpu spikes under certain conditions. [CB-31200]
- Fixed a bug that could cause the Windows EDR service to crash. [CB-31282]
- Improved capturing of DNS data. [CB-31323]
- Fixed a bug with parsing and copying hosts file. [CB-31663]
- Fixed a bug that caused BSOD under certain conditions. [CB-31734]
- Fixed a bug with encoding hash values of network events. [CB-31756]
- Fixed a bug with missing parent_name information for process events. [CB-31821]
- Fixed a bug with collecting modinfo events with long path names. [CB-31891]
- Added logging improvements around process bans and terminations. [CB-31938]
- Fixed bug with sensor overwriting banned hash list. [CB-31942]
- Fixed bug with certain null exceptions causing BSOD conditions. [CB-32041]
- Fixed bug with deleting executables from a network drive. [CB-32117]

Known Issues and Limitations

Known issues associated with this version of the sensor are included below:

- **Enabling Collection of Binary Info on Running Sensors Does Not Immediately Report Previously Observed Binary Info:** Sensors which enable collection of binary information (post sensor installation) will not see binary information for binaries already observed while collection of binary info was disabled. This can be worked around through an uninstall and reinstall of the sensor. [CB-30893]
- **Disabling DNS Name Resolution For NetConn Events:** Customers have observed that the Windows sensor can report high CPU utilization by the Carbon Black service (‘cb.exe’) on machines with a continually large number of network connections (e.g. DHCP/DNS servers, Domain Controllers, etc.). To help alleviate the high CPU utilization, without having to disable collection of network connection events, the windows sensor can be configured to disable DNS name resolution in data collection for network connection events by configuring the windows registry key [CB-17552]:

  [HKEY_LOCAL_MACHINE\SOFTWARE\CarbonBlack\config]

  "DisableNetConnNameResolution"=dword:00000001

- **Obfuscated Windows Sensors Will Not Start After First Reboot:** Windows sensors installed from an obfuscated sensor group will not start after first reboot. A second reboot will start the sensor service. [CB-28062]

- **CB Entries Remaining in Add/Remove Programs:** Customers uninstalling their CB EDR Windows sensor through uninst.exe will notice remaining CB entries in the Add/Remove Programs window. [CB-28059]
- **CB Branding Is Different Between MSI and EXE Installers:** Customers using the Add/Remove Program window to manage their CB EDR Windows sensor installation should be aware that the CB branding between the MSI and EXE installers is different. [CB-28063]

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