Release Notes: Windows Sensor v7.2.1

June 2021

Summary

VMware Carbon Black EDR Windows Sensor v7.2.1 is intended to provide two new *service control codes* to help with VDI administrators doing VM cloning, 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 v7.2.1 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.
- **Contacting Technical Support** – Describes ways to contact Carbon Black Technical Support and what information to have ready.

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 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-7.2.1.17664-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 feature content:

- Added 2 new *service control codes*: “209” and “210”. [CB-33441]

  `sc control carbonblack 209` -- Configures and shuts down the sensor in preparation for a VDI "golden image" snapshot being taken on the machine.

  `sc control carbonblack 210` -- Resets the sensor such that it believes it is a new install. The use case here is that if an admin clones a running sensor, we can run this command on the cloned machine to re-register without shutting down the services.

Corrective Content

This release provides the following corrective content changes:

- Fixed a bug where uninstalling the sensor through the server could fail. [CB-26045]
- Fixed a bug with removing stale sensor artifacts left behind after sensor upgrades. [CB-26046]
- Removed auto-uploading of sensor diagnostics from C:\Windows\CarbonBlack\Diags\ directory. [CB-30811]
- Fixed a bug with the sensor reporting an “unknown” parent process when using the “Live Query” feature. [CB-32128]
- Improved sensor collection of user-mode crash dumps. [CB-32462]
- Fixed a bug causing excessive “process not found” log entries in Sensor.log file. [CB-32753]
- Fixed a bug causing a decreased sensor health score on Windows 10 May 2020 versions related to “Excessive (or Very High) Event Loss” on startup due to an uptick of regmod events observed by the sensor during boot up for this particular OS version. [CB-32896]
- Updated osqueryi.exe version to 4.6.0. [CB-33165]
- Updated functionality for reporting “Tamper Detection” events. [CB-33341]
- Improved Tamper Hardening through added mitigation policies of our calling process. [CB-33416]
- Improved detection of process Doppelgänging techniques. [CB-33417]
- Improved detection of process Hollowing techniques. [CB-33418]
- Improved detection of process Herpaderping techniques. [CB-33419]

- Fixed a bug with sensor shutdowns reporting erroneous Tamper Events. [CB-33492]
- Fixed a bug causing delayed logons and spikes in network usage with sensors running on certain Citrix VDI environments. [CB-33578]
- Added a new Tamper Alert for “event underflow” conditions to alert users to the possibility the sensor is no longer reporting EDR events. [CB-33658]
- Added support for a new registry entry to disable hashing in the “post create” file lifecycle process for improved sensor performance: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CarbonblackK] "DisablePostCreateHashing"=dword:00000001 [CB-33922]
- Fixed a bug reducing sensor health score when OS is suspended or shutdown. [CB-33939]
- Fixed a bug relating to process terminations. [CB-34300]
- Improved sensor performance of hashing files in “post create”. [CB-34354]
- Improved performance with sensor check-ins. [CB-34393]
- Fixed a bug regarding reverse TCP connections. [CB-34462]
- Fixed a bug with EDR Windows sensor entry in Add/Remove programs for sensors upgraded through the console that were originally installed using GPO. [CB-34517]
- Improved netconn event reporting to capture socket connections for all connections lasting 3 seconds or more. [CB-34731]
- 7.2.1+ EDR Windows sensor installers will not install on unsupported Windows operating systems. Please see our User Exchange post for more information on our supported operating systems. [CB-35571]

Known Issues and Limitations

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

- **Sensor Upgrades from 7.2.0-win with Tamper Protection Enabled May Fail:** Sensor upgrades from 7.2.0-win → 7.2.1-win (with Tamper Protection enabled) may fail to fully upgrade the sensor to the 7.2.1-win version. Users should temporarily disable the Tamper Protection enforcement, per the sensor group, ahead of scheduling any sensor upgrades to 7.2.1-win. Tamper Protection can be reapplied after sensor upgrades are successfully completed. If EDR server communication with an endpoint in Tamper Protection enforcement is lost, the endpoint will have to be booted into “Safe Mode” in order to locally disable Tamper Protection functionality and restore EDR sensor-server communications.
- **Disabling DNS Name Resolution For NetConn Events:** Versions of the sensor prior to 7.1.1 (and 6.1.12 for XP/Server2003) were susceptible to high CPU utilization in the IP

Address-to-Hostname resolution functionality of the sensor. This issue has been addressed, however, this registry key will still disable IP address name resolution for customers who wish to do so. [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 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]
- **Carbon Black App Control "Tamper Protection" Rapid Config Update Recommended:** For users running Carbon Black App Control (formerly "CB Protection") to tamper protect the Carbon Black EDR Windows Sensor (and do not opt-in to CDC) it is recommended to update the tamper rule settings for Carbon Black App Control to the latest "Carbon Black EDR Tamper Protection" Rapid Config to avoid possible conflict with applying Tamper Protection enforcement on both EDR and App Control. Please note, enabling Tamper Protection on both App Control and EDR does not provide extra protection and it is recommended to disable App Control enforcement of Tamper Protection once EDR enforcement is confirmed to be in place. When running EDR in "Tamper Detection" mode, "Tamper Protection" through App Control is still recommended. Tamper Protection (for EDR) requires a minimum Operating System version of Windows 10 v1703 (Desktop) or Windows Server v1709. In addition,Tamper Protection (for EDR) requires minimum versions of both the Windows 7.2.0 sensor and 7.4.0 EDR Server. Please contact technical support to obtain the latest Rapid Config for CB App Control if needed. [EP-11934]

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 EDR server and sensor version)
- **Hardware configuration:** Hardware configuration of the CB 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, error message returned, and event log output (as appropriate)
- **Problem severity:** Critical, serious, minor, or enhancement request