8.6.0 LINUX AGENT RELEASE NOTES

Build: 8.6.0.217
Document Revision 2.0, February 5, 2021

Introduction

This document provides change information regarding VMware Carbon Black App Control v8.6.0.217 Linux agents and instructions for installation.

Installation

As of the 8.1.4 server release, the Linux Agent no longer comes bundled with the Carbon Black App Control Server, nor does it require manual (command line) steps to add it to the server. You can upgrade Carbon Black App Control Linux Agents without having to upgrade their Carbon Black App Control Server. Please visit the latest *Carbon Black App Control User Guide* for more information.

For information regarding which Linux operating systems are supported in this release, please review the Carbon Black EDR sensors & Carbon Black App Control agents document on the Carbon Black User Exchange.

Purpose of This Release

The Carbon Black App Control v8.6.0.217 Linux Agent provides improved security, reliability, and improved performance.

For more detailed information, please review the specific sections carefully:

- New Features and Product Enhancements
- Corrective Content
- Known Issues and Limitations

Carbon Black App Control

New Features and Product Enhancements

Product security is our top priority for Carbon Black App Control. In this release, we have included several new enhancements to ensure that our product is prepared to keep you and your endpoints secure. These changes include:

- Added support for RHEL 8.3
- Improved system performance and eliminated most instances of "b9daemon failed to allocate pages" in syslog by improved kernel module communications.
- Added ability for customers to upgrade App Control Linux agents with *GPG checking* enabled.

Corrective Content

This section lists defects fixed in this release, Carbon Black App Control 8.6.0.217 Linux Agent.

Item #	Description
EP-11961	Fixed an issue to ensure that the installer is extracted in a secure path when the installation is run.
EP-11098	Fixed an issue where the Linux agent failed the health check if restarted more than once.

Carbon Black App Control

Known Issues and Limitations

The following table lists the known issues and limitations present in the Carbon Black App Control 8.6.0.217 Linux Agent.

Item #	Description
NA	Prelinking must be disabled on Red Hat and CentOS computers before installing agents. When prelinking is enabled, executable file content will be changed whenever prelinking runs, which will bloat server inventory and result in many more files that need to be approved. This makes it difficult to ascertain whether an executable file was maliciously modified since each instance can have a unique hash.
NA	If you have an existing Carbon Black EDR Sensor running on your system and you wish to install the Carbon Black App Control Agent, a reboot will be required after the installation is completed.
NA	There is a new Carbon Black EDR Updater available for Linux systems that are running both Carbon Black App Control Agents and Carbon Black EDR Sensors. This updater can be enabled from the Carbon Black App Control console on the **Rules > Software Rules > Updaters** tab. Be sure to also enable the updater for Redhat Software Update.
NA	Reboot of an endpoint containing both Carbon Black App Control Agent v7.4.2 and Carbon Black EDR Sensor may take several minutes.
EP-201	If a file is renamed with symlink, the event that reports this action shows an empty filename (quotation marks with nothing between them).
EP-344	On some Linux systems, the Carbon Black App Control Agent notifier might not start automatically after installation or upgrade. There are several ways to remedy this: • The notifier can be started manually with root privileges. From the location /opt/bit9/bin, run the command: ./b9notifier & **There is no such file.** • You can reboot the endpoint and the Carbon Black App Control Agent notifier should start automatically. • You can log out and log back in. However, this will not work with an SSH session running with the -X or -Y option. In that case, if you want to use the notifier, start it using one of the previous methods.

Item #	Description
EP-850	If a system is stressed, it is possible for the OOM Killer to kill the b9daemon process. It is recommended that you exempt the b9daemon process from the OOM Killer as it cannot currently be blocked via tamper protection. The exemption can be created running the following command as the root user: **echo -1000 > /proc/`pgrep b9daemon`/oom_score** This command could be run as a chron job on a regular basis (e.g., once an hour). To verify if OOM has killed the b9daemon, the syslog can be checked as follows: **grep -i kill /var/log/messages** If the OOM Killer terminated a process, the command would show results similar to this: **host kernel: Out of Memory: Killed process 1402 (b9daemon)** **Note:** While oom_adj can be used, this has been deprecated in RH6/7; the current recommendation for RH6/7 is to use oom_score file.
EP-2817	Incorrect logic could intermittently allow the agent to misclassify a mount as a local drive if the mount point is ever lost or disconnected. This issue can be worked around by unmounting and remounting.
EP-3392	Starting the Linux Protection agent through CLI using the /Applications/Bit9/bin/b9cli -startup fails to start the b9notifier. **Workaround**: Run the following: `/opt/bit9/bin/b9notifier &`
EP-7786	A Debug Level error, *Error (1)*…,displays on the Linux agent after you send the debug level from the server to that agent.
EP-7903	Despite creating a custom rule for a trusted path that would allow and promote the files within that folder, the file state does not change after execution from that trusted folder.
EP-8203	Running a Baseline Drift Report produces no results for Linux agents.
EP-8349	Linux Agent upgrade fails if Linux Agent is running.
EP-8834	On the server events page, names associated with rules created for Linux triggering an execution block event may not display in the “Rule Name” Column.
EP-8845	Custom Rules using the macro, <OnlyIf>, do not work. For example, the macro, <OnlyIf:ConnectedToServer:No>, behaves the same regardless of connection status.

Item #	Description
EP-8885	ELF files are not recognized as installer files.
EP-8912	On the server “Computer Details” page, the Debug Level may display the incorrect set level for Linux agents.
EP-8923	On the server events page, Tamper Protection warning events do not include “From” Locations on Linux agents.
EP-8932	The time in which a Policy Override code expires may not be communicated correctly depending on the Client/Server time zone. **NOTE**: This issue was resolved with Carbon Black App Control Server 8.1.8; however, if you have not upgraded to 8.1.8, the issue persists.
EP-8950	Custom rules using a process pattern including a prepended wildcard, such as “**folder*” do not block files as expected.
EP-9022	After modifying the “Notifier Text” when editing the enforcement policy advanced settings for blocking scripts, the resulting error that occurs when triggering the notifier does not display in the log.
EP-9030	After restoring server from backup, an Alert erroneously displays regarding the Linux agent: “Host Package Not Found”.
EP-9434	Repeated, unclean, shutdowns can result in a cache that grows exponentially and thus negatively impacts agent and device performance.
EP-9556	When upgrading from 7.4.2 to 7.4.4 on Oracle Linux 8.0, the upgrade may fail. In order to workaround this issue you must use a special set of commands that can be found in this KB article
EP-9567	After installing the Linux agent, the agent can take 2-3 hours to fully synchronize.
EP-10262	When upgrading a Linux agent specifically from version 7.4.2.112 to 7.4.4, an error may display on the console indicating that the process has stopped. **Note**: This error has been resolved when upgrading from 7.4.4 to 7.4.6.
EP-10414	On a device with low memory, the agent does not start after rebooting.
EP-10508	Occasionally, when copying one interesting file over another interesting file, the latter is no longer found by dascli/b9cli command.
EP-10768	Linux Agent Does Not Report Application Data to File Catalog in App Control Server.

Item #	Description
EP-11005	In some cases, the agent installation log files contain a warning “RPMDB altered outside of yum.” after a successful installation.
EP-11067	In some cases, pushing code to an agent can cause NMI watchdog soft lockup errors that can cause the code deployment to fail.
EP-11147	The Linux agent displays as “Not Validated” on the server System Configuration page for Linux Users and Groups.
EP-11464	The Linux agent does not support Mini Dumps.
44496	The process command line field in Carbon Black App Control events will list only the name of the executable that ran, not the arguments that were used to invoke that executable.
46389	You cannot add a custom notifier icon for Linux agents in this release.
49579	Some virtual machines running on VMWare Fusion may hang on reboot. Removing “rhgb quiet” from the kernel menu entry appears to work around this issue.

Carbon Black App Control

Contacting VMWare Carbon Black Support

Please view our Customer Support Guide on the User Exchange for more information about Technical Support:

https://community.carbonblack.com/t5/Support-Zone/Guide-to-Carbon-Black-Customer-Support/ta-p/34324

For your convenience, support for Carbon Black App Control is available through several channels:

Technical Support Contact Options
Web: User eXchange
E-mail: support@carbonblack.com
Phone: 877.248.9098

Reporting Problems

When you call or email technical support, please provide the following information to the support representative:

Required Information	Description
Contact	Your name, company name, telephone number, and e-mail address
Product version	Product name (for example, Carbon Black App Control Server or Agent) and version number
Hardware configuration	Hardware configuration of the server or endpoint having the issue (processor, memory, and RAM)
Problem	Action causing the problem, error message returned, and event log output (as appropriate)
Problem severity	Critical, Major, Minor, Request