VMware Carbon Black App Control Linux Agent 8.7.12 Release Notes

VMware Carbon Black App Control 8.7.12

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

1 Introduction 4

2 What's New 5

3 Installation Instructions 6

4 Resolved Issues 7

5 Known Issues 8

Introduction

1

VMware Carbon Black App Control 8.7.12 | 24 January 2023 | Build 8.7.12.5.524

Check for additions and updates to these release notes.

What's New

2

This document provides change information and installation instructions for VMware Carbon Black App Control v8.7.12 Linux Agents.

Important **2 February, 2023 Update:**

An OS compatibility issue has been discovered in the App Control 8.7.12 Linux Agent. This issue may prevent users from deploying the Agent successfully on RHEL 8.7 (4.18.0-425.3.1+).

We are working on a resolution to this issue and will update this post when we have more information available.

The Carbon Black App Control v8.7.12 Linux Agent is a maintenance release.

New changes include:

- **RHEL 9.1 and RHEL 8.7 Support**

  The App Control 8.7.12 Linux agent now supports RHEL 9.1 (5.14.0-162.6.1) and RHEL 8.7 (4.18.0-425.3.1).

  Note **We do not support CentOS Stream**

- **Reduced CPU Consumption**

  The Linux App Control 8.7.12 agent resolves abnormally high CPU consumption issues found in the previous 8.7.10 Linux App Control release.

Installation Instructions

3

Important Before you install the Carbon Black App Control agent on the Red Hat Enterprise Linux 9.0 Endpoint:

- Install the initscripts RPM manually or connect the host to Red Hat network.
- Upgrade the Carbon Black App Control server to version 8.9.0 or later.
- If you are using a Carbon Black App Control server deployed on Windows Server 2012, please update the DH modulus to 2048 bytes as described in https://learn.microsoft.com/en-us/security-updates/SecurityAdvisories/2016/3174644.

For more details, see Install Linux Agents on Endpoints in the Agent Installation Guide.

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 VMware Carbon Black App Control Agent Installation Guide for more information.

For information regarding which Linux operating systems are supported in this release, please review the Supported Operating Systems and Agents in the Linux OER on VMware Docs.

Carbon Black EDR Updater for Linux systems

There is a Carbon Black EDR Updater for Linux systems that run both Carbon Black App Control Agents and Carbon Black EDR Sensors. You can enable this updater from the Carbon Black App Control console on the **Rules** > **Software Rules** > **Updaters** tab.

Tip: Be sure to also enable the updater for Redhat Software Update.

Resolved Issues

4

The following issues were resolved in this release:

- **EP-17210: Fixed an issue where users may experience high CPU usage due to the b9daemon.**

Known Issues

5

- **Reboot of an endpoint can take several minutes**

  Reboot of an endpoint, containing both Carbon Black App Control Agent v7.4.2 and Carbon Black EDR Sensor, can take several minutes.

- **EP-16852: Inadvertently unloading the App Control proxy module may cause a system panic if the hooks were changed.**

  This may happen when installing App Control after installing EDR.

- **EP-16731: The configuration property "ABExclusion" are currently not supported on the Linux agent.**

- **EP-9030: Restoring server from backup displays an alert**

  After restoring server from backup, an alert erroneously displays regarding the Linux agent: `Host Package Not Found`.

- **EP-9434: Exponential growth of a cache can negatively impact agent and device performance**

  Repeated, unclean, shutdowns can result in a cache that grows exponentially and thus, negatively impacting agent and device performance.

- **EP-9556: Upgrade from 7.4.2 to 7.4.4 on Oracle Linux 8.0 can result with failure**

  When upgrading from Linux agent 7.4.2 to 7.4.4 on Oracle Linux 8.0, the upgrade may fail.

  See KB 88833

- **EP-9567: Linux agent can take up to 3 hours to fully synchronize**

  After installing the Linux agent, the agent can take 2-3 hours to fully synchronize.

- **EP-10262: Linux agent upgrade from version 7.4.2.112 to 7.4.4 can result with an error**

  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.

  Upgrade Linux agent to version 7.4.6.

- **EP-10414: Unable to start agent an a device with low memory**

  On a device with low memory, the agent does not start after rebooting.

- **EP-10508: When copying one interesting file over another, the latter is no longer found by the `dascli/b9cli` command**

  Occasionally, when copying one interesting file over another interesting file, the latter is no longer found by the `dascli/b9cli` command.

- **EP-9022: Error does not display in the log when modifying the "*Notifier Text*" for enforcement policy advanced settings**

  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-10768: Linux agent does not report application data to File Catalog in App Control Server**

  Currently, the App Control Server does not collect application data on Linux endpoints. If visiting the File Catalog and look for this data, it is not present. The missing fields are **Publisher**, **Product Name**, and **Product Version**. This data is needed to support Common Platform Enumeration (CPE).

- **EP-11067: Pushing code to an agent may cause NMI watchdog lockup errors**

  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 a message when adding an user for Linux User/Group to Manage Agents**

  When adding an user by navigating to the server **System Configurations**>**General**tab> **Edit**>**Agent Management** section>**Linux User/Group to Manage Agents** page, selecting **User**, and clicking the **Update** button causes the display of the `Not Validated` message.

- **EP-11431: Local Approval mode does not work on a Linux agent**

  Temporary Local Approval mode does not work on a Linux agent when FIPS is enabled on the agent.

- **EP-12731: On RHEL 8 platform, pressing random keyboard keys results with an error**

  When using the RHEL 8 platform, an error occurs if the user presses random keyboard keys while on the **unapproved script** notifier dialog.

  - Do not use keys while on the **unapproved script** dialog.
  - If the **assertion failed** dialog appears, click **continue**, and go back to the previous screen.

- **44496: The process command line field in Carbon Black App Control events lists only the executable name**

  The process command line field in Carbon Black App Control events lists only the name of the executable that ran, not the arguments that were used to invoke that executable.

- **46389: No custom notifier icon for Linux agents**

  You cannot add a custom notifier icon for Linux agents in this release.

- **49579: Virtual machines may hang on reboot**

  Some virtual machines running on VMWare Fusion may hang on reboot.

  Remove the **rhgb quiet** from the kernel menu entry.

- **EP-11005: Agent installation log files may contain a warning**

  In some cases, the agent installation log files contain a warning `RPMDB altered outside of yum.` after a successful installation.

- **EP-8950: Custom rules using *\folder do not block files as expected**

  Custom rules using a process pattern including a prepended wildcard, such as “*\folder” do not block files as expected.

- **EP-8932: Communicating the Policy Override code expiration depends on the Client/Server time zone**

  The time in which a Policy Override code expires may not be communicated correctly depending on the Client/Server time zone.

  Upgrade to Carbon Black App Control Server 8.1.8

- **EP-8923: Tamper Protection warning events do not include "from location"**

  On the server events page, Tamper Protection warning events do not include “From” locations on Linux agents.

- **Carbon Black App Control Agent installation requires a reboot**

  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 completes.

- **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.

- **EP-201: Renaming files with symlink reports empty filename**

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: Carbon Black App Control Agent notifier might not start automatically after automatic upgrade**

  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:

  - Start the notifier manually with root privileges. From the location */opt/bit9/bin*, run the command: `./b9notifier &` **`There is no such file.`**
  - Reboot the endpoint and the Carbon Black App Control Agent notifier should start automatically.
  - 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.

- **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. You can run it as a chron job on a regular basis (e.g., once an hour).

  ```
  echo -1000 > /proc/`pgrep b9daemon`/oom_score
  ```

  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 can misclassify a mount**

  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.

  Unmount and remount.

- **EP-3392: Starting the Linux Protection agent through CLI fails to start b9notifier**

Starting the Linux Protection agent through CLI using the */Applications/Bit9/bin/b9cli* -startup fails to start the b9notifier.

Run the following command:

```
/opt/bit9/bin/b9notifier &
```

- **EP-7786: A Debug Level error displays on the Linux agent**

  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: Creating trusted folder does not change file state**

  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: Baseline Drift Report does nor work for Linux agents**

  Running a Baseline Drift Report returns no results for Linux agents. The following message appears: *There are no items to display.*

- **EP-8349: Linux Agent upgrade fails**

  Linux Agent upgrade fails if Linux Agent is running.

- **EP-8834: Rules names do not match with the created rules in the events page**

  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: The macro `<OnlyIf>` does not work with custom rules**

  Custom rules using the macro `<OnlyIf>` do not work. For example, the macro `<OnlyIf:ConnectedToServer:No>` behaves the same regardless of connection status.

- **EP-8885: ELF files are not recognized as installer files**

  ELF files are not recognized as installer files.

- **EP-8912: Debug Level can display incorrect set level for agents**

  On the server **Computer Details** page, the Debug Level may display the incorrect set level for Linux agents.

- **EP-14575: When an unapproved file is executed and user clicks “block” on “unapproved file” pop-up, two events are generated and sent to console**

  The process name is missing on one of those two events. The other event displays the process name and all respective information correctly.

- **EP-14659: Agent starts synchronization every time there is a change in enforcement level and a user creates a script rule for a file type that already has a script rule associated with it.**

  For example, the issue may occur if a user creates custom rules for certain file extensions that already have a script rule in place.

- **EP-14764: With agent in medium/high enforcement level, upgrading RHEL version to 8.x using “software upgrade GUI Interface” results in “unapproved file” pop-up coming up for some files**

  This is for the files that get added to the system as a part of RHEL upgrade.

  Workarounds:

  a A manual “local approval” of the files being flagged resolves the issue. This can be done on the console.

  b The problem can be avoided by upgrading RHEL using command line option rather than GUI option.

  c Change the enforcement mode to “Low”. Upgrade the OS using GUI option. Then change the agent mode back to “medium/high”, as per the need. This sequence makes sure that the files get locally approved and "unapproved file" pop-up does not appear.