CB PROTECTION

Release Notes: Linux Agent 7.2.4 Patch 7

November 2018

Introduction

This document provides information for users installing Cb Protection v7.2.4.2301 (Patch 7) Linux agents.

This v7.2.4 Linux agent release requires manual installation of new files on the Cb Protection Server. Once these files are installed, they may be used to deploy agents on Linux systems. Please review the *Supported Operating Systems* document on the Carbon Black User Exchange to determine the Linux operating systems that are supported in this release.

System Requirements

To use the v7.2.4 Linux agent, you must have **Cb Protection Server 7.2.3 or later (including version 8.x.x)** installed. Previous server versions will recognize the drivers for this agent, but this agent is not supported on them.

Important: If you are running versions earlier than 7.2.4.1150 of the Linux agent, the old agents must be uninstalled and unloaded from their hosts, and the hosts must be rebooted before the new agent is installed. Instructions below identify the specific preparations needed for different releases.

Purpose of This Release

This release contains corrective content that resolves reported issues. Please review the "Corrective Content" and the "Known Issues and Limitations" sections carefully.

This release also adds support for the following:

- Red Hat (RHEL), Oracle (RHCK) and CentOS Linux version 7.6

Note: This Linux agent *does not* support the Oracle unbreakable kernel versions.
As of this Patch 7 Release CentOS 7.6 *has not* yet been released.

Installation Instructions

To complete deployment of the Linux agents, you must:

- Add the v7.2.4 Linux Agent files to your Cb Protection Server. See the section *Adding the v7.2.4 Linux Agent Files on the Cb Protection Server* on page 3.
- For each system with an existing agent whose version is *earlier than* v7.2.4.1150, remove the agent from the system.
- Complete the agent installation procedure(s) specific to your upgrade or new installation environment. See the section *Installing or Upgrading the Agent on Endpoints* on page 3.
- *Supported Operating Systems*

Included Files

The following files are included with this release:

- Agent installation files, which you will copy to the Cb Protection Server:
  - **Bit9Redhat7Install.bsx**: Agent installation program for Red Hat Linux v7.0 through v7.6.
  - **Bit9Redhat6Install.bsx**: Agent installation program for Red Hat Linux v6.2 through v6.10
  - **b9notifierRedhat7.rpm**: Notifier program for Red Hat Linux v7.0 through v7.6.
  - **b9notifierRedhat6.rpm**: Notifier program for Red Hat Linux v6.2 through v6.10.
  - **b9agentRedhat7.rpm**: Agent application program for Red Hat Linux v7.0 through v7.6.
  - **b9agentRedhat6.rpm**: Agent application program for Red Hat Linux v6.2 through v6.10.

- Additional files to copy to the server to allow approval and deployment of the agent files, and to enable automatic upgrades:
  - **GeneratedFilesToApprove.sql**: A SQL script to approve the Linux agent files on the Cb Protection Server.
  - **EnableGenerateRedhatInstaller.sql**: A SQL script to automatically enable the Cb Protection server to generate Linux Agent package files for each policy
  - **Linux-Upgrade.xml**: Contents to add to **upgrade.xml** so that agents work with the Cb Protection Server automatic upgrade capability.
  - **LinuxSelfProtectionUpdater.b9u:** A file for adding the latest version of the Linux Self Protection Updater to the server so that agents can protect their own files.
  - **b9install.sh** and **bit9cs.asc**: Installation files needed by the Cb Protection Server to allow deployment of the agent files to the endpoint.

- Documentation files:
  - **Cb Protection Linux Agent v7.2.4 Patch 7 Release Notes.pdf**: This document (the one you are currently reading) provides the release notes associated with this release. It includes the defects fixed in this release, as well as the current known issues.

Adding the v7.2.4 Linux Agent Files on the Cb Protection Server

Follow these steps to add the Linux agent files to the Cb Protection Server so that agents can be deployed from the Download Agent Install Packages page of the Cb Protection console:

1. Be sure you are running **Cb Protection Server version 7.2.3 or later (including 8.x.x)**. Previous versions of the server are not compatible with this agent release.
2. Stop the Cb Protection Server by running the following command:

   net stop ParityServer

3. The file **GeneratedFilesToApprove.sql** is included with this distribution. This will approve all Linux content. Run this SQL script.
4. Copy the BSX and RPM files listed in the Included Files section on page 2 to the hostpkg folder on your Cb Protection Server. If you used the default installation directory, this folder is in one of the following locations:
   - **c:\Program Files (x86)\Bit9\Parity Server\hostpkg** (for 64-bit server OS)
   - **c:\Program Files\Bit9\Parity Server\hostpkg** (for 32-bit server OS)
5. Replace or add the following files in the **hostpkg\Assets\Linux** folder on your server:
   - **b9install.sh**
   - **bit9cs.asc**
6. Restart the ParityService service by running the following command:

   net start ParityServer

7. Do either one of the following procedures:
   a. Execute the **EnableGenerateRedhatInstaller.sql** script included on your server database.
      -or-
   b. Complete the following manual steps
      i. Log in to the Cb Protection Console as an Administrator, and navigate to: **https://**<*myservername.mydomainname*>**/shepherd_config.php**
      ii. On the Defined Properties menu, choose **GenerateRedhatInstaller** and enter **true** in the Property value field.
      iii. Click the **Change** button and confirm your changes.
8. Navigate to the Support page on the console:

   https://<*myservername.mydomainname*>**/support.php**

9. On the Support page, click on the **Advanced Configuration** tab, and in the right panel Actions menu, click on **Regenerate install files**.

Installing or Upgrading the Agent on Endpoints

Once you update the Cb Protection Server with the new v7.2.4 Linux agent, your next tasks depend upon whether an agent already exists on your systems, and if so, what version:

- **Existing agent *prior to* v7.2.4.1150 on the system** – For systems with existing agents *earlier than* version 7.2.4.1150, you must uninstall the agent and manually remove certain files. This is described in Removing pre-v7.2.4.1150 agents on page 4. You can then use one of the procedures in the section Manual agent installations and upgrades on page 5 to install the agent. The installation procedure you use depends upon whether you preserved the database of your older agents.
- **Existing agent v7.2.4.1150 or later on the system** – For systems with a current agent at version 7.2.4.1150 or later, you can either let the server do an automatic upgrade as described in Server-managed upgrades from v7.2.4.1150 or later on page 4 or use one of the methods in section Manual agent installations and upgrades on page 5.

- **No previous agent or agent database on the system** – If you are installing the v7.2.4 agent on a system that does not currently have an agent installed and does not have an agent database from a previous installation, go directly to the section Manual agent installations and upgrades on page 5.

Removing pre-v7.2.4.1150 agents

If your systems currently have a Linux agent version that is earlier than v7.2.4.1150, you must uninstall the agent, reboot the system, and then install the new agent.

1. Uninstall the agent:
   a. From the Cb Protection Console, move the computer into an agent disabled policy.
   b. On the client computer, login as an administrator or an account that can run *sudo*.
   c. In a shell window, change to the Cb Protection Agent application directory:
      cd /opt/bit9/bin
   d. Run the uninstall script:
      i. To remove the agent and all of its data:
         sudo sh ./b9uninstall.sh
      ii. To remove the agent but preserve Cb Protection Agent data in /srv/bit9:
         sudo sh ./b9uninstall.sh –d

Note: If you preserve the database with the –d option, you cannot use b9install.sh to install the new agent. You must use the RPM files as described in Installing an agent on a system with an agent database but no current agent on page 5.

   e. Prior to the v7.2.4 agent, the uninstall script would leave some files and directories behind. Do the following on any endpoints where this occurred:
      i. Remove the directories **/opt/bit9** and **/srv/bit9**
      ii. Remove the **b9kernel** file under **/lib/modules/$(uname -r)/kernel/lib**
      iii. Remove the **b9kernel** file under **/dev**
      iv. Remove **b9daemon** under **/etc/init.d**
      v. Remove the **b9daemon service** using command:
         chkconfig --del b9daemon
      vi. Run the command **depmod** to reset module dependencies.
   f. Delete the listing for this computer from the Computers page in the Cb Protection Console. This indicates to the Cb Protection Server that the computer is no longer in service (rather than temporarily disconnected from the network).
2. Reboot the system the agent was running on.
3. Choose the appropriate option for installing the agent in the section Manual agent installations and upgrades on page 5.

Server-managed upgrades from v7.2.4.1150 or later

If your systems currently have existing Linux agents at v7.2.4.1150 or later, you can use the automatic agent upgrade features of the Cb Protection Server. The following steps enable automatic upgrades:

1. Stop the Cb Protection Server by running the following command:

   net stop ParityServer

2. Locate the **upgrade.xml** file. If you used the default installation directory, it is located in one of these upgrade folders:

   - **c:\Program Files (x86)\Bit9\Parity Server\upgrade** (for 64-bit server OS)
   - **c:\Program Files\Bit9\Parity Server\upgrade** (for 32-bit server OS**)**

3. Modify the file **upgrade.xml** by replacing the current ‘Redhat’ and ‘Centos’ 6 and 7 upgrade sections with the content of the **Linux-Upgrade.xml** file provided with the

v7.2.4 distribution. The contents of Linux-Upgrade.xml should be pasted into the <upgradelist> section of the **upgrade.xml** file.

4. Restart the Cb Protection Server by running the following command:
   net start ParityServer
5. If not already configured, enable Automatic Agent Upgrades from the console on the **Administration > System Configuration > Advanced Options** tab.
6. On the **Assets > Computers** page, select all computers you want to upgrade, and from the Action menu select **Upgrade Computers**.
   Note: Computers in Policies set to 'Allow Upgrades' do not require this step since they will be scheduled to upgrade automatically after completing the previous step.
7. Wait for each of the machines to upgrade. You may see the status 'Disconnected' display on the console Computers page during the upgrade process – when upgrade is complete, this changes to ‘Up to date’.
8. Although not necessary, a reboot of the upgraded agent machine is recommended.

Manual agent installations and upgrades

The following procedures covers three manual installation and upgrade cases.

Manually upgrading a Cb Protection Agent connected to the server

1. Log in to the Cb Protection Console as an administrator, navigate to the **Assets > Computers** page, and click on the computer name or View Details link for the computer you intend to manually upgrade.
2. On the Computer Details page, click **Disable Tamper Protection**, located on the far right under the Advanced section. It may take a few minutes before tamper protection is disabled on the agent.
3. On the agent machine, copy the appropriate BSX file included with this release package:
   - Bit9Redhat6Install.bsx – used for 6.x versions of RHEL, CentOS or Oracle RHCK
   - Bit9Redhat7Install.bsx – used for 7.x versions of RHEL, CentOS or Oracle RHCK
4. Execute the following command with the appropriate version of the BSX file:

```
sudo bash Bit9Redhat{6,7}Install.bsx
```

Installing an agent on a system with an agent database but no current agent

This procedure should be used for systems that once had a previous Cb Protection Agent and then had the agent removed, but still have an agent database. This would occur when the –d option was used during agent uninstall.

1. Copy the appropriate RPM files from the release package to the agent computer:
   - **b9agentRedhat6.rpm** and **b9notifierRedhat6.rpm –** used for 6.x versions of RHEL, CentOS or Oracle RHCK
   - **b9agentRedhat7.rpm** and **b9notifierRedhat7.rpm –** used for 7.x versions of RHEL, CentOS or Oracle RHCK
2. If you run a GUI on your Linux server, install the notifier RPM. The notifier RPM must be installed before the Agent RPM:

```
rpm -ivh b9notifierRedhat7.rpm
```

3. Install the agent RPM:

```
rpm -ivh b9agentRedhat7.rpm
```

Installing an agent on a system with no agent and no agent database

Important: This procedure (and any installation involving b9install.sh) should be used **only** on completely new systems and systems that had a previous agent but have completely removed the agent *and its database*.

1. Log in to the Cb Protection Console as an administrator, navigate to the **Rules > Policies** page, and click on the link for downloading agent software.
2. On the Download Agent Install Packages page, choose the agent installer corresponding to the policy and operating system version you want to install. A TGZ file specific to the operating system and policy you chose will be downloaded.
3. On the agent system, extract the downloaded tar file:

   tar -xvzf <*policyname*>**-Red Hat.tgz**

   Note: If the policy name contains characters not accepted in command arguments, such as spaces or parentheses, escape each character with a backslash.
4. Change to the directory matching the download tarball name:

   cd <*policyname*>**-Red Hat**
5. In whatever shell you choose, use sudo to run the agent installation, adding the -n option if you do not want the blocked file notifier installed. For example:
   - To use the Bourne shell to install an agent with a notifier:
     sudo sh ./b9install.sh
   - To install the agent **without** the notifier (usually used on headless servers):
     sudo sh ./b9install.sh –n

Configuring Antivirus Software

If you run antivirus software, exclude the Cb Protection installation directory from antivirus scanning. For enhanced security, Cb Protection protects its own application directory. To avoid performance problems, use whatever mechanism is provided by your antivirus software vendor to specify that the following directories or files are not scanned:

- **/opt/bit9/bin** – the Cb Protection Agent application and uninstall script
- **/srv/bit9/data** – the Cb Protection Agent database and diagnostics logs
- **/lib/modules/**<*kernelversion*>**/kernel/lib/b9k_* –** the Cb Protection Agent kernel
- **/lib/modules/**<*kernelversion*>**/kernel/lib/cbproxy_* –** the Cb Protection Agent kernel proxy
- **/etc/rc*/*b9daemon and /etc/init.d/b9daemon** – the Cb Protection Agent startup script
- **/etc/X11/xinit/xinitrc.d/90b9notifier.sh –** the Cb Protection blocked file notifier

Firewalls may recognize Cb Protection software as a new application and block access to the network. Instruct users running the agent to permanently allow it access.

Upgrading the Operating System while the Agent is Installed

Since the Cb Protection Linux agent is very kernel specific, we strongly recommend following these steps to allow safe upgrade of your operating system:

1. Move the agent to a disabled enforcement policy
2. Follow the steps for upgrading the operating system
3. Move the agent back into the original enforcement policy. Re-enabling the agent will cause it to re-initialize.

Installing the Linux Self-Protection Updater

A Cb Protection *Updater* is available to protect the agent from tampering. If your server is configured to accept updaters from the cloud and it is connected to the internet, you should have received the latest Linux Self-Protection Updater automatically.

If you are not receiving automatic updates to Cb Protection Updaters, follow these steps to add the latest self-protection Updater:

1. Copy the updater file **LinuxSelfProtectionUpdater.b9u** to a location accessible from the Cb Protection server.
2. If you are running v8.X.X server: In order to make the Add Updater button visible you need to make a change on the Support.php page:
    a. Enter **https://***<servername>***/Support.php** and select the **Advanced Configuration** tab.
    b. Near the bottom of the page, check the Show Import Buttons box and then click the **Update** button at the bottom of the page.
3. Choose **Rules > Software Rules** on the console menu and select the **Updaters** tab.
4. Click the **Add Updater** button.
5. In the Add Updater dialog, select the **LinuxSelfProtectionUpdater.b9u** updater file, enter the password **bit9** and click the **Save** button. This imports the new version (version 2) of the Linux Self Protection updater to the server. The updated version will automatically be pushed to Linux agents associated with the server.

Corrective Content

Corrective Content in Cb Protection 7.2.4 Patch 7 Linux Agent (Build 2301)

- Fixed an issue where the agent would add duplicate process entries in the disk-resident SQLite DB. Over time, this would cause a large cache DB and potentially impact agent performance. [EP-4934]
- Previously, the Cb Protection agent monitored the LSM callback for every file write. This was found to be performance prohibitive and now file modifications are determined with write-intent at open. While a file may be opened with write intent and closed with no modifications, the agent will determine this result on analysis. This will increase false-positive occurrence on report-write rules which can be mitigated by adding exclusions for the processes that are expected to open the target file with write-intent. [EP-6237]
- To help reduce potential CPU spikes of the b9daemon, this release reduces the default frequency of the cache maintenance task from every 15 minutes to every 75 minutes. [EP-6096]
- Contention for an internal lock was reduced by using an improved algorithm that has a shorter lockout duration increasing performance on larger Linux systems. [EP-6759]

Corrective Content in Cb Protection 7.2.4 Patch 6 Linux Agent (Build 2252)

- As a safeguard, this release includes a new health check warning when the /srv/bit9/data/cache.db increases its size more than 50% over the course of a 24-hour period. The growth is measured proportionally on an hourly basis and a warning is determined based on the growth of the cache.db over the number of hours that have passed from either the last health check that was run, or cache consistency check scan for new files. [EP-4934]
- Fixed an issue where running a Cache Consistency Check (CC3) in local approval mode caused existing unapproved files to be locally approved. [EP-5276]

Corrective Content in Cb Protection 7.2.4 Patch 5 Linux Agent (Build 2245)

- In previous releases, Performance Optimization rules did not work correctly if the system had multiple partitions mounted on top of one another. This has been corrected. [EP-5557]

Corrective Content in Cb Protection 7.2.4 Patch 4 Linux Agent (Build 1611)

- Previous Cb Protection Agents tracked processes even when set to Disabled mode. This added significant overhead to the machine when the expectation was that a disabled agent would have little to no impact. This has been corrected in this release. [EP-4802]
- In certain cases, when the Cb Protection daemon was killed, it was not being restarted correctly and the agent would not reconnect to the server. The daemon restart logic has been changed to ensure proper operation. [EP-4737]
- When traversing unlocked or possibly stale data structures, previous agents could get trapped in a recursive algorithm and eventually run out of kernel stack, causing a crash. This has been corrected. [EP-4678]
- Certain low memory conditions could result in system crashes. The specific low memory conditions are now detected and handled without a crash. [EP-4998]

- Under certain circumstances the Cb Protection daemon would not restart after an unexpected shutdown. This issue has been corrected ensuring the daemon restarts automatically in these cases. [EP-4600]
- This release corrects a problem that would cause the Linux system to crash when looking up certain short-lived processes. [EP-4508]
- Installing the Cb Protection agent on a busy machine with very low available memory would occasionally result in kernel panics. In this release, the agent launching process has been modified so that installation fails cleanly, without kernel panics, on machines with insufficient memory resources. [EP-4456]
- On the new RedHat kernels (kernel-2.6.32-696.23.1 and kernel-3.10.0-693.21.1) released to mitigate Spectre/Meltdown vulnerabilities, previous agents will not load correctly, leaving the agent in the 'unprotected' state. This release provides proper interoperability and protection on the latest RedHat patches. [EP-5147]
- Certain agent conditions that could cause CentOS 7.1 to hang on rare occasions have been remedied. [46771]

Corrective Content in Cb Protection 7.2.4 Patch 3 Linux Agent (Build 1527)

- Addressed a race condition that existed on b9daemon shutdown. This condition could cause the system to hang during driver disconnect, leading to a system panic on systems with kernel.hung_task_panic configured. [EP-3059]
- Eliminated a problem where certain commands issued by the b9daemon to collect configuration or diagnostic information could require allocations that failed, potentially crashing the system under low-memory scenarios. [EP-2691]
- Adding additional termination handlers to correct a problem in which not all process terminations were seen by the agent, leading to growth in both the in-memory and persisted process tracking tables. [EP-2434]
- Corrected a race condition in mount traversal that could lead to a tight-spin in the kernel that caused intermittent hangs in some file operations. [EP-2368]

Corrective Content in Cb Protection 7.2.4 GA Linux Agent (Build 1501)

- Eliminated a kernel panic during file path resolution caused by a race condition while traversing mount paths. [EP-1044]
- Eliminated a kernel panic on AMD Opteron processors caused by initialization code that was Intel processor specific. [EP-1054]

Corrective Content in Cb Protection 7.2.4 CD3 Linux Agent (Build 1398)

- Due to a race condition, the Cb Protection kernel module could leak kernel memory under high-volume, short-lived process activity. The kernel memory recovery does not occur even when the kernel module is unloaded. In this release, the race condition has been eliminated, which in turn addressed the memory leak as well. Note that, this issue exists in all prior versions of the Cb Protection for Linux agent. [EP-1044]
- Process-specific mounts that occur in namespaces or Docker on Red Hat or CentOS 7.x could cause incorrect mount traversals when resolving file paths, leading to kernel panics, particularly in Docker environments. The logic has been addressed in this release. This issue exists in all prior versions of the Cb Protection for Linux agent. [EP-948]
- During shutdown of the agent, a race condition could cause a deadlock in the kernel, preventing the kernel module from unloading and therefore preventing upgrades from working properly. [EP-898]

Corrective Content in Cb Protection 7.2.4 CD2 Linux Agent (Build 1384)

- The agent now correctly tracks operations when file system root is modified (chroot). [44389]
- On Red Hat Linux v7.1, a File Creation Control rule correctly prevents empty files from being created. This issue does not happen in Red Hat Linux v6.x. [EP-254]
- Interoperability issues with Docker container (e.g., Gitlab generating a 502 error) were corrected through the use of file op exclusions. [EP-264]
- If the b9daemon crashes, it is now automatically relaunched. [46175]
- Resolved agent initialization performance issue. [EP-302]
- Addressed an issue where the Linux agent installer would stop if the /srv/bit9 or /srv/bit9/data directories are present and not empty. [EP-296]
- Resolved a server crash of a puppet server during the agent initialization [EP=69]
- Resolved memory leak due to numerous kernel threads being created and not releasing the memory. [EP-364]
- Addressed a daemon hang condition during agent shutdown that could cause upgrade failures. [49320, EP-67]
- Corrected a condition in which a network domain change caused the agent to disconnect and stay offline. [EP-70]
- Addressed a problem in which an agent encountering a blank entry during certain file system operations could cause frequent system panics. [49790, EP-76]
- Modified the behavior of the ‘b9cli –shutdown’ command so that it no longer unloads the kernel. [49903, EP-91]

- The evaluation rank of file monitoring rules has been changed so that these rules are now evaluated before file creation rules, assuring that changes to matching files are always tracked. [39885, EP-97]
- Fixed a communication failure caused by the agent not handling overlapping connect requests. [50115, EP-126]
- Fixed an agent crash that occurred when an agent processed files on a remote share and the share was stopped during processing. [47621, EP-151]
- Reduced the kernel memory footprint of the agent, which should improve performance and could help avoid crashes on systems with pre-existing memory constraints. [47944]
- Eliminated a problem with agents hanging while waiting for a server connection by limiting the time the agent will wait before retrying the connection to 15 seconds. [48365]
- Improved the agent's network connection recovery mechanism so that the agent can reconnect to the server after a network operation failure. [49362]

Corrective Content in Cb Protection 7.2.4 CD1 Linux Agent (Build 1150)

- After this release of the Linux agent is installed, you will no longer be required to reboot after future agent upgrades. [EP-300]
- Resolved an agent initialization performance issue. [EP-302]
- Addressed an issue where the Linux agent installer would stop if the /srv/bit9 or /srv/bit9/data directories were present and not empty. [EP-296]
- Resolved a crash on Puppet servers that occurred during agent initialization. [EP-69]
- Resolved a memory leak that occurred when numerous kernel threads were created and their memory was not released. [EP-364]

Corrective Content in Cb Protection 7.2.4 EAP 4 Linux Agent (Build 1084)

- Addressed a daemon hang condition during agent shutdown that could cause upgrade failures. [49320, EP-67]
- Corrected a condition in which a network domain change caused the agent to disconnect and stay offline. [EP-70]
- Addressed a problem in which an agent encountering a blank entry during certain file system operations could cause frequent system panics. [49790, EP-76]
- Modified the behavior of the 'b9cli –shutdown' command so that it no longer unloads the kernel. [49903, EP-91]
- Fixed a communication failure caused by the agent not handling overlapping connect requests. [50115, EP-126]
- Fixed an agent crash that occurred when an agent processed files on a remote share and the share was stopped during processing. [47621, EP-151]
- Reduced the kernel memory footprint of the agent, which should improve performance and could help avoid crashes on systems with pre-existing memory constraints. [47944]
- Eliminated a problem with agents hanging while waiting for a server connection by limiting the time the agent will wait before retrying the connection to 15 seconds. [48365]
- Improved the agent's network connection recovery mechanism so that the agent can reconnect to the server after a network operation failure. [49362]

Corrective Content in Cb Protection 7.2.2 EAP 3 (Build 3048)

In this release, numerous defects were addressed, including security fixes. The list below is a high-importance subset of those fixes.

- Unloading the Cb Protection kernel when the agent is uninstalled can cause crashes [27179]
  - Details: The install script will no longer unload the running kernel. This to allow other applications that refer to the memory allocation not to crash.
  - Applies to: Agent [Linux]
- Linux agent installed with disconnected network adapter fails to connect to server after adapter is reconnected [47309]
  - Details: On a system where Network Manager controls IP access, disconnecting the network adapter or dropping the link on the Ethernet interface results in the Network Manager removing the name server addresses, as they are assumed to be stale. With the previous agent, the resolver library looks for name server information upon startup of the agent. Due to this behavior the agent will never connect to the Cb Protection Server when network connectivity is restored, as it does not have any name servers to query.
In this version, this behavior has been corrected. After the failure of three consecutive name queries, the agent will force the resolver library to look for name server information. This activity is driven by the polling timeout sent by the server and equates to three poll attempts.
  - Applies to: Agent [Linux]
- Periodic health checks are not being run [48115]
  - Details: Periodic Health Checks would not start until the health-check interval was set to something other than the default value. This issue has been addressed in this release.
  - Applies to: Agent [Linux]
- During file operations the agent causes a kernel panic [48778]
  - Details: Overlapping file operations on a set of files where there were multiple handles open on the same file caused a double free. This resulted in a NULL pointer being returned to the agent for a file operation, and there was no check for this condition. In this version, there is a check in place to avoid using the NULL pointer.
  - Applies to: Agent [Linux]
- When the network adapter is disconnected and then reconnected, the agent will not connect [48793, 47318]
  - Details: When the agent was started without proper nameserver information in the /etc/resolv.conf file, it would never connect to the server, even after the nameserver information was updated. This was due to the resolver library being initialized only at startup. In this version, the agent will re-initialize the resolver library after three consecutive failures.
  - Applies to: Agent [Linux]
- Linux agent causing the system to crash [49312]
  - Details: The system was unable to handle failed memory allocation. Now the agent will try different method when memory allocation fails.
  - Applies to: Agent [Linux]

- Change macro for Carbon Black server ignore rule to use <OnlyIf:FileExistsOnDisk:/var/cb> [48384] [EP-106]
    - Applies to: Agent [Linux]

Corrective Content in Cb Protection 7.2.2 EAP 1 (Build 799)

In this release, numerous defects were addressed, including security fixes. The list below is a high-importance subset of those fixes.

- If the Symantec agent is present, Cb Protection causes agent to crash [47534]
    - Details: If the Symantec agent is present on a system, the Cb Protection agent kernel should not be unloaded, as this may cause the Symantec agent to panic the system. Previously, this required that agent upgrades be run manually. In this release, automatic upgrades may be run without encountering this problem.
    - Applies to: Agent [Linux]
- Parity (Cb Protection) Service script should not unload the Cb Protection kernel [48041]
    - Details: Previously, uninstalling or automatically upgrading the agent would run a script that also unloaded the Cb Protection kernel. If another security regime is running, unloading the Bit9 kernel may cause the security regime to panic. To allow users to upgrade and uninstall the agent without encountering this problem, the shutdown script used during these operations no longer unloads the Cb Protection kernel.
    - Applies to: Agent [Linux]

Corrective Content in Cb Protection 7.2.2 (Build 715)

Significant effort has been put into this release to address the quality of the Linux agent. The release includes fixes for memory management issues, where the agent would crash due to the inability to process memory effectively. Additional changes include improvements in operating system interaction, which the previous agent was not managing properly.

Known Issues and Limitations

This section lists known issues and limitations of this Linux agent release. See also the *Known Issues and Limitation*s section in the separate Release Notes for your Cb Protection Server version for issues that might be relevant to this v7.2.4 Linux agent release.

- 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.
- If you have an existing Cb Response Sensor running on your system and you wish to install the Cb Protection Agent, a reboot will be required after the installation is completed.
- If the b9daemon is stopped via b9cli -shutdown and then restarted via b9cli -startup, the notifier is not automatically started.
  To manually start the notifier run the shell script **daemonize_notifier.sh** located under /opt/bit9/bin. [EP-3392]
- 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-2817]

- If the /srv/bit9 directory is a separate mount point (not the root file system), you may see the following spurious warning when uninstalling the agent:
  Warning: directory /srv/bit9: remove failed: Device or resource busy.
  The agent will correctly be uninstalled, leaving the /srv/bit9 mount point intact. [EP-2577]
- If you wish to install the Cb Response sensor on a system running the Cb Protection Agent at High, Medium, or Low Enforcement, put the Cb Protection Agent into Local Approval to successfully complete the installation of the Cb Response sensor. Be sure to restore the endpoint to its previous Enforcement Level after sensor installation is complete. [EP-313]
- Reboot of an endpoint containing both Cb Protection agent v7.2.4 and Cb Response sensor may take several minutes.
- There is a new Cb Response Updater available for Linux systems that are running both Cb Protection and Cb Response agents. This updater can be enabled from the Cb Protection console on the **Rules > Software Rules > Updaters** tab. Be sure to also enable the updater for Redhat Software Update.
- 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-850]
- On some Linux systems, the Cb Protection Agent notifier might not start automatically after installation or upgrade. [EP-344, EP-359]

  There are several ways to remedy this:

  1. The notifier can be started manually with root privileges. From the location **/opt/bit9/bin** run the command:

     ```
     ./daemonize_notifier.sh
     ```

  2. You can reboot the endpoint and the Cb Protection Agent notifier should start automatically.
  3. 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.

- When a system has synchronous and asynchronous write file operations, the Linux agent could miss some file writes. This is related to EXT4 but may extend to other file systems. [EP-131]
- If a file is renamed with symlink, the event that reports this action shows an empty filename (quotation marks with nothing between them). [EP-201]
- 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. [49579]
- Because of the version difference between this agent and the server it runs with, Bit9 Platform content in the Cb Protection installation directory (b9cli, b9daemon, b9notifier, etc) is not getting globally approved. For this release, you must approve these files manually to ensure proper functioning of your endpoints. This is addressed by the GenerateFilesToApprove.sql script described in the procedure under Adding the v7.2.4 Linux Agent Files on the Cb Protection Server on page 3. [45875]
- The process command line field in Cb Protection events will list only the name of the executable that ran, not the arguments that were used to invoke that executable. [44496]
- You cannot add a custom notifier icon for Linux agents in this release. [46389]
- When performing an upgrade from a previous version of the CB Protection Agent, you may experience decreased server performance and increased CPU utilization during installation. [EP-6000]
- When pushing updates automatically from the Cb Protection console, its use of BSX files will remove the record of a Cb Protection agent install from the RPM catalog. [EP-6021]

Contacting Carbon Black Support

For your convenience, support for Cb Protection is available through several channels:

- **Web:** User Exchange
- **Email:** support@carbonblack.com
- **Phone:** 877.248.9098
- **Fax:** 617.393.7499

Reporting Problems

When you call or e-mail technical support, please provide the following information to the support representative:

- **Contact:** Your name, company name, telephone number, and email address
- **Product version**: Product name (Cb Protection server and agent version)
- **Hardware configuration:** Hardware configuration of the Cb Protection 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