Qualys Cloud Agent Linux 6.2 (x64)

January 2024

We're excited to tell you about new features, improvements, platform coverage changes, and fixes in this Cloud Agent release. These updates are specific to the agent binary. Platform updates for new features and fixes of management, syncing, tagging, and reporting capabilities of Cloud Agents are documented in the Cloud Platform and Cloud Suite release notes.

New Features

- User and process-based inclusion and exclusion filters in File Integrity Monitoring (FIM) configuration profiles: With this new feature, you can define rules to monitor actions performed by specific users or processes on the specified file or directory and exclude the activities performed by users and processes from generating events.

  This feature helps reduce the number of events generated by valid actions performed by authorized users, thereby reducing the load on the Qualys Cloud Platform.

  Required Application Version: File Integrity Monitoring 3.9.0

Enhancements

- Reduced Activity Period: You can only control network activity with the existing reduced activity period configuration.

  With the enhanced feature, you can control the application and network activity for specific applications. You can configure a reduced activity period for an application and define whether you want to prevent data transmission, network transmission, or both in the specified time interval.

  For example, when you configure a reduced activity period and define prevention of data transmission for VM, activities such as data collection and VM scanning are not performed.

  Only network activity is controlled for assets with Agent versions earlier than 6.2. If anyone runs an on-demand scan for the module during the reduced activity period, the on-demand scan will be delayed.

  For the required application version, contact your Qualys representative.
- Enhancement in Software Composition Analysis (SwCA): The following enhancements are
  - Added support for on-demand SwCA scan
  - Added support for the languages— Ruby, Rust, PHP

Language	File	Package Managers
Ruby	Gemfile.lock	bundler
Rust	Cargo.lock	cargo
PHP	composer.lock	composer

  - Updated SwCA scan for Java language packages— By default, SwCA scan uses a `.jar`, `.war`, and `.ear` files for detection instead of a `pom.xml` file.

Language	File	Package Managers
Java	jar/war/ear	jar

  - Added support for downloading SwCA binary through HTTPS TLS proxy.

- Extended support on the following platforms:
  - CentOS 6, 7 and 8
  - SUSE Linux Enterprise Server (SLES) 12 and 15
  - Debian 7, 8, 9, 10, 11, and 12

  Required application version: Qualys Cloud Platform 3.17.1.0
- Added exclusion for the following common network filesystems:
  - afs
  - cifs
  - fuse.sshfs
  - gfs
  - gfs2
  - nfs
  - nfs4
  - nfsd
  - safenetfs
  - secfs
  - smb2
  - smbfs
  - vxfs
  - vxodmfs

  These filesystems are excluded from SwCA scan. This helps in optimizing CPU consumption.

- Enhancements in QualysProxy connection:
  - If the connection using the proxy server fails, the Cloud Agent will failover to the next configured proxy in case of http failures.
  - If the connections using all the configured proxies fail, the Cloud Agent attempts a direct connection to the Qualys Cloud Platform.

    Prerequisites: To activate this feature on the newly-installed Agent, the `ProxyFailOpen` parameter must be set to 1.
  - If the proxy is configured, all manifest commands use the proxy configured in https_proxy and http_proxy variables when agent is installed as root user.

  Note: If you update the proxy settings, Cloud Agent must be restarted.
- With the enhancement in Cloud Agent for Linux, the Cloud Agent expedites the first scan after provisioning or reprovisioning, which helps minimize the delay. All the subsequent scans are performed as per the defined schedule. This applies to all the scheduled or interval scans.

Behavior Changes

There are no behavior changes in this release.

End of Support for Platforms (Operating Systems)

With this release, Qualys Cloud Agent for Linux discontinues the support for the following platforms:

- CentOS versions earlier to CentOS 6
- Red Hat Enterprise Linux (RHEL) versions earlier than RHEL 6
- Oracle Enterprise Linux (OEL) versions earlier than OEL 6
- SUSE Linux Enterprise Server (SLES) 11

The Cloud Agent for Linux support is discontinued as these platforms do not support third-party libraries.

Note: The Cloud Agent versions on the assets with these operating systems cannot be upgraded to Cloud Agent for Linux 6.2.

Fixed Defects

The following reported and notable issues have been fixed in this release.

ID	Description
CRM-109876	Fixed an issue where Cloud Agent created core files utilizing large disk space.
CRM-110365 CRM-114087	Fixed issues where create and delete file events were not reflected in the File Integrity Monitoring (FIM), although the events were available in the audit record file.
CRM-112517	Fixed an issue where the Endpoint Detection and Response (EDR) process did not start when Cloud Agent was installed with a relocated usr/local directory and SELinux was in an enforcing state.
CRM-114791	Fixed an issue where Cloud Agent provisioning failed due to hostid and Agent UUID validation issues.
CRM-116077 CRM-115846	Cloud Agent for Linux 6.1 used the curl library version earlier than 8.4. The issue is resolved as the Cloud Agent for Linux 6.2 uses the curl version 8.4.0.
CRM-109876	Fixed an issue where the FIM events were not recorded, as the Cloud Agent could not retrieve the FIM manifest.
CRM-111952	Fixed an issue where the FileContentCheck control of UDC did not provide the expected value as the last character of the value was getting trimmed. This issue occurred when the contents of the file did not have the ending newline.

Known Limitations and Workarounds

- When a non-root user tries to perform a create or rename operation on a file or directory, and the operation is not successful, this event is not reported in FIM.
- For using the Proxy Auto-Configuration (PAC) file: Before using the automatic proxy with the PAC file, you must check the connection between the PAC server and the host asset. If the connection fails, the Agent cannot fetch the proxy configuration defined in the PAC file.
- If an on-demand scan request is triggered when the SwCA package download event is in the queue, other events in the scheduler, such as scan for other manifest types, self-patch download, agent health status, are not executed till either one of the following conditions is fulfilled:
    - all retry attempts to download the SwCA package are exhausted.
    - SwCA package is downloaded.