Qualys Cloud Agent Linux 6.1 (x64)

August 2023 (Updated in October 2023)

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

- Software Composition Analysis (SwCA): With the software composition analysis (SwCA) feature, Cloud Agent can identify vulnerable dependencies or software components used by first-party (custom application packages) and third-party (open-source application) packages.

  This enables customers to detect, manage, and proactively address the potential risk of software supply chain vulnerabilities in the production environment.

  Supported languages:

Language	File	Package Managers
Python	Pipfile.lock	Pipenv
	poetry.lock	poetry
	requirements.txt	Pip
Go	go.mod	Go
Java	pom.xml	Apache Maven
DotNet	packages.lock.json	Nuget
NodeJs	package-lock.json	npm
	yarn.lock	yarn

  SwCA scan is supported on the following operating systems:

  - Red Hat Enterprise Linux (RHEL) 6, 7 through 7.9, 8 through 8.9, and 9
  - Ubuntu 12.04, 14.04, 16.04, 18.04, 20.04, and 22.04

  Note: The SwCA scan runs only in offline mode and can only be activated if VM is activated for the agent.

  Required Application Version: Qualys Cloud Platform 3.16.0.0

Enhancements

- File Integrity Monitoring
  - File Access Monitoring – With this enhancement, an event is generated upon accessing a file, even when no modification is done in the file. The event is generated in the following scenarios:
    - The sensitive file is read.
    - The file is copied to another location.

  Required application version: File Integrity Monitoring 3.7.0.0
- Support for AWS tags: The Cloud Agent is enhanced to fetch AWS instance tags in the AWS instance metadata that the agent collects.
- Binaries download changes—Updated the RequestTimeOut parameter value in the `qualys-cloud-agent.conf` file to 1800.

- Added support for the Cloud Agent binary to detect whether Expanded Security Maintenance (ESM) is enabled on Ubuntu.

Behavior Changes

On Linux-based systems, use the following command to uninstall the agent:

```
nohup /usr/local/qualys/cloud-agent/bin/qagent_uninstall.sh &
```

The current ssh connection will be terminated because of a network issue while uninstalling EPP, which can be reconnected again.

Note: This is applicable for Cloud Agent for Linux version 6.1 and later

Platform Coverage Support (Operating Systems)

Added support for the following platforms:

- VMware Photon 3, 4 for Inventory and PC application
- Scientific Linux 7.x for Inventory and PC application
- Kali Linux

Fixed Defects

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

ID	Description
CRM-107315	Fixed an issue where FIM events were generated from a sub-directory even if the directory was added in the Exclude filter.

Known Limitations and Workarounds

- For fetching AWS tags data, you must provide a valid JSON file to be parsed. If an invalid JSON file is provided, the JSON file does not get parsed. As a result, the Cloud Agent application does not display AWS tags in the **EC2 Information** tab in asset details.
- If you have a Cloud Agent for Linux version earlier to 6.1, the File Access Monitoring feature will not work even if the required File Integrity Monitoring (FIM) version is available.

  Workaround: Upgrade the Cloud Agent for Linux to version 6.1.

Known Issues for File Access Monitoring (FAM)

- For some specific kernel versions, the procTitle field is not populated in the audit logs for any event. For example, CentOS 7 and Kernel versions earlier than or equal to 3.10.0-229.el7.x86_64. In this case, the Cloud Agent does not send the procTitle information.
- For the .mp3 and .mp4 files, when the user performs the read event once, multiple read events are logged incorrectly in the audit logs. As the Cloud Agent sends the events based on the audit logs, it sends multiple read events to the File Integrity Monitoring application.
- The Cloud Agent uploads the FIM events based on the defined **Payload threshold time** value. However, as the buffering and uploading activities are performed independently, the event upload can be delayed. You can modify the **Payload threshold time** value in the Cloud Agent Configuration Profile.
- Even if you do not select file creation and select file events in the scope of file monitoring, the file creation event is generated.

- For some kernel versions earlier than 5.14.0-70.49.1.el9_0.x86_64, two read events are logged incorrectly for file access when the less command is used to read a file.
- When the content change tracking is enabled for a kernel version earlier than or equal to 3.10.0-1160.88.1.el7.x86_64, the file rename events are not generated.