![Qualys logo]

Qualys Cloud Agent Unix 4.20.1

January 2024 (Updated in February 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

There are no new features in this release.

Enhancements

Added support for Agent Health Status (AHS) that provides detailed monitoring of agent status. This includes information on installation, deployment, and the status of Cloud Agent activities like manifest download, scanning, uploading results, errors encountered, and communication with the Qualys Cloud Platform.

Behavior Changes

With this release, the following change is observed in the FIM behavior on AIX assets:

The events detected in the first scan after the new FIM manifest download are not sent to FIM. The events are stored as baseline events. All the events detected in the subsequent scans are sent to FIM.

Fixed Defects

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

ID	Description
CRM-113960	Fixed an issue where multiple create and rename events were reported incorrectly. Now, when the Cloud Agent for AIX performs the first scan of the directories and files, it does not send the scan data to FIM. In the subsequent scans, changes in the directories and files are reported.
CRM-114104	Fixed an issue where the CAR job could not get completed as Cloud Agent failed to execute the remediation tool. Now, the remediation script is updated with the necessary changes.

Known Limitations and Workarounds

- In a scenario where the Cloud Agent for AIX self-patches from version 3.10.0-17 to 4.20.1-12, even if self-patch is successful using the sudo user, the FIM manifest download fails due to permissions or ownership of the `/opt/qualys/cloud-agent/fim` directory.
  Workaround: Use the agent provision script again or use the agent configuration script to change LogLevel parameter as presented in the following example:
  `sudo /opt/qualys/cloud-agent/bin/qualys-cloud-agent.sh LogLevel=3`
- For all agent health status codes, Cloud Agent for AIX does not send additional fields, such as manifest type, scan start time, and scan type in scan status.

- Cloud Agent for AIX does not support hard links of files on AIX assets, as multiple rename events are generated while scanning hard links of the files.
- For the file delete event, Cloud Agent does not provide any time stamp to FIM. When the scan is performed after the file deletion, the time stamp of the scan is recorded as the time stamp of the delete event.
- Cloud Agent for AIX does not support user and process-based inclusion and exclusion filters in File Integrity Monitoring (FIM).
- Cloud Agent on AIX does not support FIM status codes.