Qualys Cloud Agent Windows 5.3

August 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

- 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—Go, Python, .Net, Java, NodeJS, Rust, Ruby, and PHP.

  Required Application Version: Qualys Cloud Platform 3.16.0.0

Enhancements

- Enhancements for Patch Management:
  - With the addition of the System Reboot action as a part of Pre-Actions in a patch job, you configure the system to be restarted explicitly before the patch job starts.

    Required Application Version: Patch Management 2.5.0.0
  - You can install software as a pre-or-post action in a patch job only by providing an installer path in the **URL** field. To enable this, a new Install Method is added in the Pre-Actions and Post-Actions for Install Software action in the patch job.

    With this enhancement, the install software action is simplified, as you can install software without providing the installation Powershell script.

    Required Application Version: Patch Management 2.5.0.0
- With the enhancements in QualysProxy, you can now configure whether the agent should failover to the next proxy URL or attempt a direct connection to the Qualys Cloud Platform if the connection using the first proxy server fails.
- Support for AWS tags: The Cloud Agent is enhanced to fetch AWS instance tags in the AWS instance metadata that the agent collects.
- Enhancements for Qualys Endpoint Detection and Response (EDR): The following enhancements will help IT security teams to perform attack investigations with reduced turnaround time, irrespective of the location of the asset.
  - Support for remote Powershell commands: Using this feature, you can connect to the remote host using a Remote shell interface. You can execute some pre-defined Powershell commands on the remote system to retrieve detailed information about the

system and perform required actions if the system is suspected to be under malware attack.

Currently, the following commands are supported using remote shell:

- cd
- ps
- restart
- scriptrun
- ls
- run
- env
- kill
- delete
- netstat
- users
- shares
- reg
- regquery
- copy
- ipconfig
- drivers
- mkdir
- shutdown
- hash

The IT security team can use this feature to access the asset irrespective of the location of the asset, which is helpful in the investigation of incidents at the endpoint system.

Required Application Version: Endpoint Detection and Response 2.5.0.0

- Forensic data collection: With this feature, you can collect the system information, such as registry settings, network information, processes, logs, and so on, by executing pre-defined Powershell scripts on the endpoint system.

  This feature helps in retrieving accurate forensic data required for incident response. The required data can be retrieved on demand in a single action and save manual efforts for data collection.

  Required Application Version: Endpoint Detection and Response 2.5.0.0

- Support for Policy Compliance is enhanced to detect user accounts with empty passwords and user accounts with passwords that are the same as the username.

  Note: This feature is supported on all Windows versions prior to Windows 10 v1607.

Behavior Changes

There are no behavior changes in this release.

Platform Coverage Support (Operating Systems)

There is no new platform coverage added in this release.

Fixed Defects

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

CRM-27814	Added support for the following Data Point IDs in the Policy Compliance scan: • 802857: Check if, the password is empty for the user accounts. • 802858: Check if, the password is equal to user name for the user accounts.
CRM-105431	Fixed an issue where the Windows Cloud Agent service went into Not Responding mode with error 1001.
CRM-106688	Fixed an issue where Qualys Cloud Agent was collecting incorrect data for Policy Compliance CID 100317.
CRM-107938	Fixed an issue where the *Deployment in-progress* notification continued to remain on the screen even after the successful deployment of the patch. Now, the *Deployment in-progress* notification is closed after deployment completion, and the patch job proceeds as per the settings.
CRM-108517	Fixed an issue where the reboot countdown was initiated intermittently even when the user clicked the Defer option in the Patch Management notification window.
CRM-108054	Fixed an issue where an on-demand scan could result in upgrade failure and prevent Cloud Agent from upgrading to a newer version.
CRM-107466	Fixed an issue where Cloud Agent installation failed with the following error: `Failed to create event log channel: (win32 code: 13), "The data is invalid."`
CRM-107454	Fixed an issue where FIM exclusions did not work if the exclusion path contained non-English language characters.

Known Limitations and Workarounds

- Windows System Restore does not work if the self-protection feature is enabled for the host. For details on the workaround, refer to https://success.qualys.com/support/s/article/000007303.