Qualys Cloud Agent Windows 5.2

June 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

- Troubleshooting options in the Cloud Agent application interface: Earlier, the administrator user needed to access the asset and perform multiple steps for performing common troubleshooting actions, such as restarting the agent service.

  With this feature, you can perform common troubleshooting actions easily using the Cloud Agent application interface.

  - Enable or disable the trace log level
  - Disable self-protection
  - Restart agent service

  Note: These options are available only to the Administrator user.

  Required application version: Qualys Cloud Platform 3.15.1.0

- File integrity check: As a part of security enhancements, a check is performed on all the files that are downloaded from Qualys to verify that the files are not tampered with.

  If the file integrity checks fail for the file, the file is deleted and downloaded again from Qualys.

- Support for setting default proxy configuration during agent installation: With this feature, you can add the initial proxy configuration as an argument when the agent is being installed.

  You can also pass multiple proxies, separated by semi-colon, as an argument during agent installation.

  Note: This is applicable only for the new installation of Cloud Agent for Windows.

Enhancements

- Enhancements for Patch Management
  - You can select the patches to be installed from a shared drive in the network. You can download the installer or patches, save it to the local drive, and install patches from the shared drive in the network. To enable this, a new option is added to the Protocol list in Pre-Actions and Post-Actions in the deployment job.

    With this enhancement, there is no dependency on internet connectivity to download the patches while installing.

    Note: The share must be a public share and should not need credentials for access.

    Required Application Version: Patch Management 2.3.0.0

Copyright 2023 by Qualys, Inc. All Rights Reserved.

- You can change the patch download link and direct it to your local repository. Once you set the path to your local HTTP or HTTPS repository, the agent uses the patch from the local repository instead of accessing the vendor website.

  With this feature, you can add patches, where patch URLs need user credentials for access, to be added as a part of the deployment job.

  Note: You must download the patches from the official vendor website.

  Required Application Version: Patch Management 2.3.0.0

- Enhanced the agent logs to remove an error that was incorrectly logged upon agent service restart when the Patch management application is enabled.

- Custom Assessment and Remediation (CAR):
  - Added support for executing single Powershell command on host assets using CAR. Powershell commands can be used irrespective of the Powershell execution policy set on the host asset. Achieve faster remediation by executing individual Powershell commands.
  - You can select Powershell Commands under 'Script Details' when creating a new script.

    Required Application Version: Custom Assessment and Remediation 1.6.1.0

- File Integrity Monitoring (FIM):
  - The following enhancements are done in reporting of events tracked on the assets by the content change tracking feature:
    - Additional write events, such as, create and delete performed on an application (Notepad++, WordPad) are not tracked. For example, create and delete events that occurred in succession with the same timestamp are dropped by the content change tracking feature.
    - For an existing monitored file, a write event, where no content is added or no content status is generated, is not tracked by content change tracking.

    Required Application Version: File Integrity Monitoring 3.6.0.0

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-94716	Fixed an issue where the Cloud Agent did not get installed, as old traces were available on the system. The issue was observed with Cloud Agent for Windows version 4.9.0.16, 4.8.0.31, and 4.7.0.30. Now, for fresh installation, Cloud Agent identifies whether traces of the previous, current, or later version installation are available on the system.

Copyright 2023 by Qualys, Inc. All Rights Reserved.

CRM-89630	Fixed an issue where the Cloud Agent main thread execution is getting blocked while attempting to upgrade the patch catalog file.
CRM-95313	Internal changes made to the agent to ensure that the agent accesses the registry only with required access rights while performing the scans. Earlier, Cloud Agent was accessing registry keys with Write Access even though Cloud Agent does not perform any write operation on Registry key/value (*except the agent registry keys)*. Now, the Cloud Agent accesses registry keys only with Read access.
CRM-105152	Fixed an issue where the user generated the key to disable self protection for a specific agent host when self-protection was not enabled on the agent host. In this case, the agent did not check the existing status of self-protection on the agent host. Now, when the self-protection is not enabled on the agent host and if the user tries to disable self-protection, a message is displayed that states that the self-protection is already disabled.
CRM-104466	Fixed an issue where the Agent was upgraded to the latest version on Azure VM even when auto-upgrade option was disabled in the configuration profile.

Known Limitations and Workarounds

There are no reported and notable issues open in this release.

Copyright 2023 by Qualys, Inc. All Rights Reserved.