Qualys Cloud Agent Windows 3.0

March 2019

We're excited to tell you about new features, improvements, platform coverage changes, and fixes in this Cloud Agent Windows 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 Platform release notes.

New Features

This release has the following new features:

- Client-side initiated "ScanOnDemand" function
  - This feature is used to trigger the agent to initiate an on-demand collection of the asset's metadata for supported activated modules: Vulnerability Management, Policy Compliance, and Inventory.
  - Refer to the Cloud Agent Windows Install Guide for description of this feature
- Client-side configured "ScanOnStartup" function
  - This feature is used to trigger the action to initiate an on-demand collection of the asset's metadata for supported activated modules on a system startup: Vulnerability Management, Policy Compliance, and Inventory.
  - Refer to the Cloud Agent Windows Install Guide for description of this feature
- Support for Qualys Patch Management 1.0 release
  - This agent version is required to activate the agent for Patch Management.
  - A new companion utility (stdeploy.exe) and associated utilities is downloaded from the Qualys Platform when Patch Management is activated on a supported agent
  - All programs under ProgramData\Qualys directories must be whitelisted by anti-virus and other endpoint protection programs.
  - When activated for Patch Management and assigned an Assessment Profile, Cloud Agent will execute a patch assessment scan on the defined interval (4 hours default).
    - On average, the patch assessment scan takes 30-120 seconds and may consume more memory during the assessment
- Support for new Agent Health and Status function
  - This agent version sends periodic, real-time health and status message to the platform to support the new Patch Management application and future customer-facing monitoring and troubleshooting use cases
  - The agent will send on average 6 status messages per day for a daily total of 3 KB compressed upload based on the default Configuration Profile scan intervals
- Support to collect IBM Cloud provider metadata
  - A new release of Qualys Cloud Platform is required for fully utilize this feature end-to-end

Enhancements

This release has the following enhancements:

- Policy Compliance User Defined Controls (UDC) now support “match limit” and “time limit” configurations for execution on agent
- Support for Indication of Compromise 2.0 release
    - This agent version is required to utilize the IOC 2.0 platform features and updates
- Indication of Compromise streamlines event collection using new techniques that optimizes performance without a trade-off in detection or use cases:
    - Does not collect File event metadata for Microsoft-signed portable executable (PE) files in %SYSTEMROOT% and Program Files
        - Process events for Microsoft-signed portable executables (PE) are still collected
    - Does not collect File event metadata for MUI types (as they are non-executable)
- Updates to libraries utilized by the Cloud Agent as follows:
    - LMZA bundled library version
    - RapidJSON bundled library version
    - SQLite bundled library version

Behavior Changes

This release has the following behavior changes:

- A new program is installed along with this release, QualysAgentUI.exe. This program is used to display user notifications for Patch Management. It is not possible to remove/uninstall this program.
- Agent selects the network interface with the default route (or the interface with lowest IP address for bonded adapters with default route) as the primary interface. This fixes the issue where APIPA interfaces occasionally are marked as the primary interface in vulnerability reporting.

Platform Coverage Support (Operating Systems)

This release has the following platform coverage support:

- Support for Windows 10 version 1809
- Support for Policy Compliance controls on Windows Server 2019

Fixed Defects

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

ID	Description
CRM-44047	External IP (connected from address) is incorrectly used as the IP address of the asset on a system with multiple interfaces

CRM-44823 CRM-45161	Agent unable to collect the primary IP address on a system with multiple interfaces
CRM-32527 CRM-46038	Improved performance on systems that have dozens/hundreds of local user profiles, including terminal servers and Citrix servers
CRM-36066 CRM-36331 CRM-37499 CRM-37615 CRM-40227 CRM-41088 CRM-43429 CRM-49233	Fixed an issue where agent was not selecting the valid network interface adapter as the primary adapter. Agent selects the network interface with the default route (or the interface with lowest IP address for bonded adapters) as the primary interface. This fixes the issue where APIPA interfaces occasionally are marked as the primary interface.
CRM-44871	Fixed a case where agent could not finish collection if there are “path is too long” warnings
CRM-47241 CRM-48369 CRM-48916	Fixed rare edge cases where agent was consuming more memory than expected
CRM-35204 CRM-36784 CRM-40781 CRM-42449 CRM-43417	Fixed a case where agent may have a race condition with locked ntuser.dat user profiles on Server 2008 causing performance load on the system
CRM-44452	Fixed a rare case where scans were failing if the Cloud Provider table was not fully populated when running in Google Compute Platform (GCP)
CRM-28631	Agent occasionally keeps open handle for certain ASP.NET temporary files

Known Limitations and Workarounds

The following reported and notable issues are open in this release.

ID	Description
QAG-5346	Patch UI dialog box cuts off description for certain monitor sizes when running remote desktop software
QAG-2636	FIM kernel driver fails to install in certain cases
QAG-2709	Agent resets backoff multiple to 1 if HTTP 204 is received
QAG-2954	Setup fails to uninstall FIM driver and driver is left running
QAG-3002	Self patch fails if disk is full or available disk is space is less than required leaving the agent partially uninstalled and non-functional
QAG-3115	Changing configuration profile fragment size during upload will corrupt upload [platform automatically detects and fixes corrupt uploads]
QAG-3136	Vulnerability scan should abort after detection of malformed snapshot [platform automatically detects and fixes malformed snapshots]
QAG-3333	Pausing the agent does not pause the agent