Qualys Cloud Agent Windows 3.1

June 2019

We're excited to tell you about any 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:

- Baseline support for Agent Version Control feature.
    - (Requires platform update in a following release to use the feature.)
- Baseline support for re-assigning agent from one Activation Key to another key.
    - (Requires platform update in a following release to use the feature.)

Enhancements

This release has the following enhancements:

- Qualys Policy Compliance support for CID 13329.
- Qualys Patch Management app has the following enhancements:
    - Agent downloads patch files from vendor sites or Cloud Agent Gateway cache, when available and enabled.
        - Customer environments must allow Cloud Agent to connect to any arbitrary Internet resource to download patch files from vendor patch sites if Qualys Patch Management app is activated for the agent.
    - Agent downloads patch catalog information and agent-only content from Qualys Platform ("qagpublic" host).
    - Agent performs "opportunistic download" of patch files defined in a deployment jobs from the vendors' patch sites.
        - Once a deployment job has been assigned to an agent, even if the deployment window hasn't started, the agent will trickle download the patch files to cache locally (or cache by Cloud Agent Gateway, if deployed and configured) for when the deployment window is active.
        - Added retry logic for failed or timed-out downloads of patch files.
    - Added intelligent restart logic of active deployment jobs for when agent resumes after power off, sleep, hibernate, and service pause/continue states.
    - Added retry and exponential backoff logic to patch deployment job status messages sent to the Qualys platform.

Copyright 2019 by Qualys, Inc. All Rights Reserved.

    - Improved download performance of patch files for low-resourced assets.
    - Immediate deployment jobs take effect immediately without regards to the time zone offset of the asset.
    - Agent logs summary results into the agent log file after each Patch deployment job, stating the number of total patches, success, failed, already installed, superseded, and not applicable patches.
    - Patch UI displays for non-Administrator users, including support for Defer and Reboot actions.
    - Deployment Job Complete user notification window can be set to auto-dismiss.
    - Patch scheduler managed by CPU Limit configuration profile performance setting.
- Added multiple proxy/failover support using QualysProxy tool and PAC file.
    - If multiple proxy servers are defined, the agent will try the first proxy in order, if it can't connect, the agent will try the subsequent proxy server(s) until all proxy servers have been attempted. Cloud Agent Windows will fail open to a Direct Connection as a last resort.
    - This approach can be used to create High-Availability and Geographic Failover logic for proxy servers and Cloud Agent Gateway proxy appliances.
- Added support to disable WPAD proxy configuration.
    - Usage: QualysProxy.exe /w on | off
    - WPAD is disabled by default and must be explicitly enabled.
    - Previously, it was not possible to disable WPAD. For agents running on networks where WPAD was enabled, the agent used the WPAD proxy settings sometimes causing agent communications to fail if the WPAD proxy could not connect to the Qualys Platform.
- Cloud Agent protocol sequence numbers now also stored in the registry.
    - This supports a use case where an administrator uninstalls and re-installs the agent on the same machine. Previously, the re-installed agent will have a new sequence number causing the platform to trigger clone detection logic. Now, the re-installed agent will utilize the sequence number in the registry, so it will not trigger a clone detection.
- Updates to libraries utilized by the Cloud Agent as follows:
  SQLite bundled library version

Behavior Changes

This release has the following behavior changes:

- Patch deployment using Qualys Patch Management will now trigger a Vulnerability Management scan outside of the configured scan interval on the agent to verify that vulnerabilities have been remediated by the patch installation.
- IOC collection no longer collects at-rest file hashes for non-executable MUI files.
- IOC agents, on upgrade to the Windows 3.1 agent version, will have the installer delete any local IOC snapshots to prepare the system for the new data model used in IOC 2.0 backend.
- Removed forced TLS 1.0 negotiation on those Windows XP operating systems that support TLS 1.2, such as POSReady 2009 (baseline Windows XP does not support TLS 1.2 used by Cloud Agent).
    - Previously on these operating systems, the agent only attempted TLS 1.0 negotiation even if the system supported TLS 1.2.
    - Now the agent will use TLS 1.2 if supported on the operating system.

Copyright 2019 by Qualys, Inc. All Rights Reserved.

- Changed Add/Remove Program registry key location for 64-bit operating systems
    - New: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\QualysAgent
    - Previous: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Microsoft\Windows\CurrentVersion\Uninstall\QualysAgent
- ScanOnDemand registry key now deleted when agent is uninstalled
- Uninstall of agent from the Cloud Agent user interface now will terminate any active scans.
    - Previously, the agent completed any active scans before uninstalling, causing an unnecessary delay in the uninstall process.
- Health and Status log messages changed to Debug log level, so they don't fill up the log file. There are no customer-facing log messages for this function.

Platform Coverage Support (Operating Systems)

This release has the following platform coverage support:

- Windows 10, version 1903

Fixed Defects

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

ID	Description
CRM-42820 CRM-25794	Fixed an issue where VM scan may cause TrustedInstaller.exe to consume additional memory
CRM-25794	Updates to fix an issue of profile corruption on Server 2008R2-based Citrix servers
CRM-48175	Fixed a case where agent service doesn't start up on low-resourced virtual machines due to time-out calling SCM
CRM-51899	Fixed a patch failure case when the local patch file cache size is exceeded before all patch files are downloaded
CRM-42820 CRM-48369	Fixed reproduceable memory utilization cases when running Patch Management

Known Limitations and Workarounds

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

ID	Description
CRM-42820 CRM-48369	Engineering is still working with reported cases to reproduce isolated memory utilization cases when running Patch Management. Some issues have been fixed as documented above.

Copyright 2019 by Qualys, Inc. All Rights Reserved.