Qualys Cloud Agent Windows 2.1.1

October 2018

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:

- [2.1.1] Cloud Agent reports the network adapter with Default Gateway as the primary adaptor for the system. This eliminates cases where APIPA addresses were reported.
- Support for Policy Compliance User Defined Controls (UDCs).
- Support for Google Cloud Platform (GCP) instance identity metadata, adding to existing support for AWS and Microsoft Azure.
- Cloud Agent compresses downloads and uploads of resources to/from the Qualys Platform.
    - Downloads include manifests, configuration profiles, and agent upgrade installers.
    - Uploads include Inventory, Vulnerability, and Compliance snapshots and deltas.
    - This is an always-on feature and is not user-configurable.
    - Cloud Agent deployments can expect to see up to 5x reduction in data size uploaded from agent to the Qualys Platform reducing the bandwidth usage of enterprise networks.
    - For example, a 1 MB delta upload can be reduced to 250 KB at full compression. Actual data size may vary depending on network connectivity, delays, dropped packets, and other environmental variables.
    - Compression utilization is managed by the "CPU Limit" value in the Configuration Profile.

Enhancements

This release has the following enhancements:

- [2.1.1] Removed use of SAMR and UserAccount WMI to eliminate network calls to Primary Domain Controllers
- [2.1.1] Improved FIM kernel driver stability
- [2.1.1] Logging added when Policy Compliance UDCs with match limit are reached
- [2.1.1] Improved metadata collection efficiency resulting in less Disk I/O
- [2.1.1] New installations will not download and self-patch to its same version
- Indication of Compromise event collection is performed in parallel to other product modules.

Copyright 2018 by Qualys, Inc. All Rights Reserved.

- File certificate information is collected for catalog-signed process images.

Behavior Changes

This release has the following behavior changes:

- [2.1.1] Permissions changed for ProgramData\Qualys and Program Files\Qualys folders and files
    - Users not in Administrators group cannot access these folders through any means
    - Administrators cannot access these folders using Windows Explorer for operating systems 2008 and later, but can access using Administrator command prompt or remote network share or other tools running as SYSTEM
- [2.1.1] Service is set to automatically restart on crash or failure up to three times per day.
- Auto-upgrade does not error/terminate if the system cannot check the certificate revocation list for the signer of the agent installer. The previous behavior of terminating the self-patch prevented customer systems from upgrading if the system did not have direct Internet access to check the CRL.
- Cloud Agent options in Programs and Features now only have Uninstall as an option, removing Change as an option.
- Fixed a case where duplicate clone detection was triggered if the agent is not able to write to its configuration database commonly due to a disk full condition or locked database. In these cases, the agent will not communicate to the platform until the system's issues are remediated.
- Uninstaller is digitally signed.

Platform Coverage Support (Operating Systems)

This release has the following platform coverage support:

- Support for Windows 10 version 1803 ("Redstone").

Fixed Defects

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

ID	Description
CRM-37159 CRM-37641 CRM-41863	[2.1.1] Removed use of SAMR and UserAccount WMI to eliminate network calls to Primary Domain Controllers
CRM-32081	[2.1.1] Improved metadata collection efficiency resulting in less Disk I/O
CRM-37269	[2.1.1] Cloud Agent reports the network adapter with Default Gateway as the primary adaptor for the system. This eliminates cases where APIPA addresses were reported.
CRM-27548	Agent-side support for CID 8279, 8364, 8365, 8366, 8367, 8368
CRM-27814	Agent-side support for CID 2421, 2422, 3657
CRM-28983	Fixed a case where agent has file locks on files in Temporary ASP.NET folder
CRM-29099	Agent-side support for Windows 2003 support of CID 2185, 2186, 2192, 2195, 2384, 2386, 2387, 2392, 2393, 2395, 2396, 2399, 2400, 2402

Copyright 2018 by Qualys, Inc. All Rights Reserved.

CRM-29397 CRM-32128 CRM-34762 CRM-35173 CRM-35578	Fixed an issue where VM cannot collect metadata from directories that have a very long path name
CRM-30107 CRM-34801	Agent-side support Windows Server 2012 support of QID 91229
CRM-30710	Fixed an issue where agent stops communicating after manifest download
CRM-30710 CRM-42161	Fixed a case where agent was throttling non-agent threads using the CPU Limit setting
CRM-32085 CRM-32461	Fixed a case where agent did not process server revoke message as agent was in provisioning state
CRM-32128 CRM-34762 CRM-35578	Fixed a case where agent could not process a file path that was too long
CRM-32638	Fixed an issue where the CPU Limit is reset to default after initial scan
CRM-33347 CRM-32957	Fixed a case where a locked agent configuration database caused the agent to provision with a new/different agent UUID [Behavior Change]
CRM-33651	Agent-side support for CID 9288 and QID 807891
CRM-33916	Agent-side support for QID 91426
CRM-33971	FN QID 87313 for Windows OS (Oracle WebLogic Server Multiple Vulnerabilities)
CRM-35339	Agent-side support for CID 4151, 7520, 11561
CRM-35693	Agent-side support for CID 11565
CRM-35927	Fixed a case where agent was closing/re-opening QIDs between assessments
CRM-36986	Fixed a case where Agent UUID is zero'd out when gold image instances are provisioned in public cloud providers
CRM-37626	Agent-side support for CID 4469, 9297, 9301, 9302, 9303, 9304, 9305
CRM-39053	Fixed a case where Google Chrome was not reported in inventory scans
CRM-41123	Fixed a case where FIM driver was loading on agents not activated for FIM
CRM-42317	Changed agent self-patch behavior to not error/terminate if system cannot check the public CRL

Known Limitations and Workarounds

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

ID	Description
CRM-28631	Agent occasionally keeps open handle for certain ASP.NET temporary files
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

Copyright 2018 by Qualys, Inc. All Rights Reserved.

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

Copyright 2018 by Qualys, Inc. All Rights Reserved.