Qualys Cloud Agent Windows 5.1

March 2023 (Updated July 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

- Added support for new Cloud Provider: Alibaba Cloud. The Alibaba instance metadata information can be viewed on the Cloud Agent User Interface.
- On-Demand Scan: The on-demand scan feature helps you with the flexibility to initiate a scan without waiting for the next scheduled scan. You can initiate the on-demand scan using the Cloud Agent User Interface. Using this feature, you can initiate VM, PC, Inventory, UDC, and SCA scans.

  Currently, you can initiate 1000 on-demand scans for each subscription in a single action and send a maximum of 15000 on-demand scan requests per day for each subscription.

  Required application version: Qualys Cloud Platform 3.13.1.0
- Scan on startup: With the scan on startup feature, you can configure the agent the run a vulnerability scan when the agent service starts. This helps in verifying whether the newly-installed patches have remediated the associated vulnerabilities on the asset.

  You can configure the scan on startup option using the Configuration Profile in Cloud Agent User Interface. Users can Enable/Disable Scan on Startup in the Configuration Profile on the portal.

  Note: This feature is not available by default. To enable the feature, contact your Qualys representative.

  Required Application version: Qualys Cloud Platform 3.14.0.0

Enhancements

- Revamped Patch Management
  - Improvements in the patch management functionality are made to ensure that the user responses to the patch user interface prompts are executed correctly.
  - User interface has been revamped without changing the user experience.

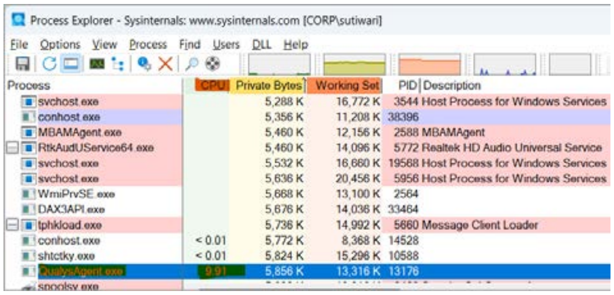
  Required application version: Patch Management 2.1.0.0
- Endpoint Detection and Response (EDR): Enhanced to reduce the memory consumption by the Qualys Agent with EDR.
- With the enhancement, the agent starts the agent ID service under the local service account C:\ProgramData\Qualys\SandboxRO\agentid-service.exe to limit security risks.

  Earlier, the agent ID service used to start from C:\ProgramData\Qualys\QualysAgent\Correlation\Resources\agentid-service.exe

The agent ID service binary is copied to a specially-crafted sandbox folder that will run as LocalService account.

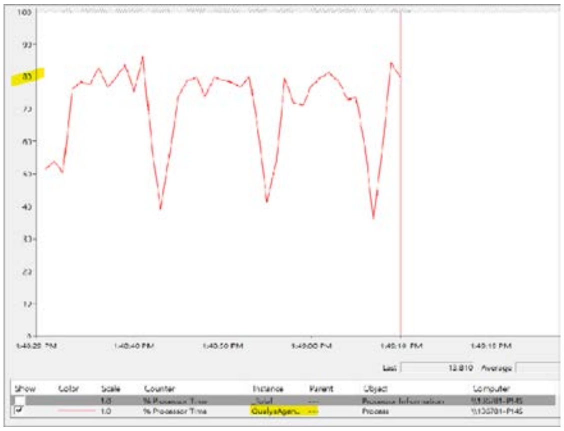
- Improvements to the CPU Limit functionality to correctly handle multiple cores/processors during CPU utilization: The Agent will be utilizing all cores for the CPU time calculation, that is, <percent value> of utilization on all cores, and hence the performance would go up by multiple of the number of cores.

  The CPU usage monitored by different performance monitoring tools can display different results. For example, when CPU usage is set to 10% by an administrator, the CPU usage shown in two performance monitoring tools:

  
  Process Explorer - Sysinternals: www.sysinternals.com [CORP\sutiwari]
File Options View Process Find Users DLL Help

Process	CPU	Private Bytes	Working Set	PID	Description
svchost.exe		5,288 K	16,772 K	3544	Host Process for Windows Services
conhost.exe		5,356 K	11,208 K	38396	
MBAMAgent.exe		5,460 K	12,156 K	2588	MBAMAgent
RtkAudUService64.exe		5,460 K	14,096 K	5772	Realtek HD Audio Universal Service
svchost.exe		5,532 K	16,660 K	19568	Host Process for Windows Services
svchost.exe		5,636 K	20,456 K	5956	Host Process for Windows Services
WmiPrvSE.exe		5,668 K	13,100 K	2564	
DAX3API.exe		5,676 K	14,036 K	33464	
tphkload.exe		5,736 K	14,992 K	5660	Message Client Loader
conhost.exe	< 0.01	5,772 K	8,368 K	14528	
shtctky.exe	< 0.01	5,824 K	15,296 K	10588	
QualysAgent.exe	9.91	5,856 K	13,316 K	13176	
spoolsv.exe					

  - The Process Explorer displays that the CPU usage is around the administrator's target usage, ~10% or less.
  - The Performance Monitor (Perfmon) displays around 80% usage on an 8-core system, as Perfmon represents one core with a 1.0 scale.

Show	Color	Scale	Counter	Instance	Parent	Object	Computer
□		1.0	% Processor Time	_Total	---	Processor Information	[illegible]
☑		1.0	% Processor Time	QualysAgen...	---	Process	\\130701-P145

- Logging improvement
  - You can enable debug-level logging for Agent by setting the registry value
    In the Registry Key - HKEY_LOCAL_MACHINE\SOFTWARE\Qualys\QualysAgent\Logs, create an entry with the following values:
    - Value name - TraceLevel
    - Value data – 6

    Restart the Cloud Agent service to enable the Agent to start printing the debug messages in all the log files.
    Note: The value set in the registry key takes precedence over the value in the config.db file.

  - For each module and functional area, the Agent creates a separate log inside the C:\Program Files\Qualys\QualysAgent\Logs directory. This helps support and engineering teams analyze faster by focusing on feature-specific logs.

Behavior Changes

There are no behavior changes in this release.

Platform Coverage Support (Operating Systems)

There are no new platform coverage in this release.

Fixed Defects

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

CRM-101424	Additional data integrity checks are added to the deltas sent by the Cloud Agent to produce an accurate report. Earlier, in some scenarios, we were seeing flip-flop of QIDs as they were incorrectly updated in the backend.
CRM-88716 [Fixed in 5.0.1 limited release]	Fixed the following issues with the revamped Patch Management functionality in the Qualys Agent: • The Patch Management prompt was unresponsive, whitened or blackened. • User actions were not getting executed or not getting executed on time. • Incorrect timer getting displayed on the Patch Management prompt.
CRM-100743 [Fixed in 5.0.1 limited release]	Fixed an issue where the Qualys Agent did not collect the complete Amazon Web Services (AWS) VM information using the instance metadata Service v2.
CRM-96506 [Fixed in 5.0.1 limited release]	Fixed the following issues with the changes made to handle race conditions and improve thread synchronization: • Scans were getting stuck for a long duration, or scans were not getting completed. • Scans were not getting initiated at the configured scan interval. • Increased CPU utilization by Agent Service.
CRM-98354 [Fixed in 5.0.1 limited release]	Fixed an issue with the agent installer that resulted in installation failure when the user attempted to install the agent using Microsoft SCCM or Endpoint Configuration Management. For details on deploying Windows Agent using Configuration manager, refer to https://success.qualys.com/support/s/article/000007035.
CRM-101879	Fixed an issue where incorrect status was displayed for CID 4469 - 'Network Security: Force logoff when logon hours expire'. For detail; refer to https://success.qualys.com/support/s/article/000007174.

Known Limitations and Workarounds

Patch UI Prompt may not be displayed correctly on Windows Server Core operating systems i.e. No GUI System. This problem is currently limited to Windows Cloud Agent 5.1.

Workaround:

- To deploy the patches successfully on Windows Server Core operating system, a patch job can be created without configuring user interface options in the job configuration. In this case, the patch deployment will take place withoutdisplaying any prompt. And hence, the problem with the prompt can be avoided.
- For more information, refer to https://success.qualys.com/support/s/article/000007156.