Qualys Custom Assessment and Remediation

Release Notes

Version 1.5
October 11, 2022

Here's what's new in Qualys Custom Assessment and Remediation 1.5!

Enhanced Control on Executing PowerShell Scripts
Encryption for Exported Scripts
Additional Details Included for Asset Jobs

Custom Assessment and Remediation 1.5 brings you some improvements and updates! Learn more

New Features

Enhanced Control on Executing PowerShell Scripts

With this release, CAR introduces an option to bypass the PowerShell execution policy set on the host, which enables you to have complete control on executing PowerShell scripts on the hosts via Qualys CAR.

When you switch the **Bypass PowerShell Execution Policy** to **Yes**, scripts are executed irrespective of the PowerShell execution policy set on the host.

Note: The **Bypass PowerShell Execution Policy** option does not change the PowerShell execution policy on a host; it only bypasses the policy for script execution.

Important:

The option to bypass the PowerShell execution policy is available only if you have Qualys Cloud Agent 5.0 for Windows installed. However, this option is not applicable if the 'Machine Policy' scope for PowerShell execution policy is set as 'Restricted'. Moreover, if the Machine Policy requires the script to be signed, bypass does not work for unsigned scripts.
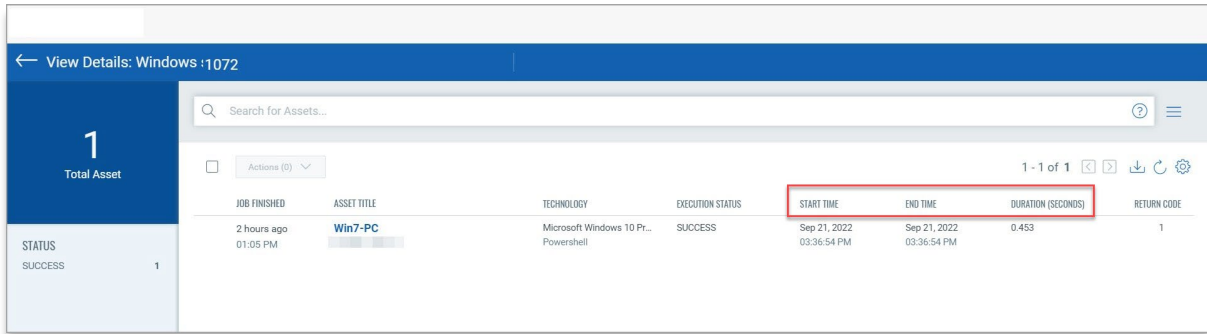
Encryption for Exported Scripts

Starting this release, scripts are exported in an encrypted format so that users cannot modify the script content or their metadata. This ensures that the confidentiality and integrity of the scripts are kept intact.

Additional Details Included for Asset Jobs

Qualys CAR displays details such as Asset Title, Technology, and Execution Status for asset jobs.

With this release, along with the existing details, you can now view the start time, end time, and duration for each asset job. You can view these details on the **Jobs Details** page displayed when you click a job listed on the **Jobs** tab.

With this enhancement, you know the exact time required to execute scripts on hosts, which improves visibility and helps you optimize the scripts, if required.

You can also search for asset jobs based on these new attributes using these newly added QQL tokens:

QQL Token	Description
durationInMillis	Helps you find jobs that are completed within the specified time or time range. For example, - To search for jobs that are completed within 10 to 40 seconds: **durationInMillis**:[10000 .. 40000] - To search for jobs that are completed in less than 1200 seconds: **durationInMillis**:<1200000
executionStartTime	Helps you find jobs that were executed at the specified date and time. You must provide the date in the 'YYYY-MM-DDTHH:mm:ss.sss' format. You can use quotes for an exact match. This QQL also supports the following operators: >=, >, <, and <=. For example, - To search for jobs that were executed on September 21st at 3:30 am: **executionStartTime**:"2022-09-21T03:30:00.000" - To search for jobs that were executed on September 21st at or after 3:30 am: **executionStartTime**:" >= 2022-09-21T03:30:00.000"

Other Improvements

- Previously, the maximum script size for Windows and Linux platforms was 75 KB and 500 KB, respectively. This release makes the script size uniform and the size limit for Windows as well as Linux platforms is now 500 KB.
  With this improvement, you can now create or import larger scripts without being blocked due to size constraints.

- During script creation, you can specify the threshold time to indicate how long a script must be in execution before it is timed out. Previously, the threshold time for Windows and Linux platforms was 5 minutes and 60 minutes, respectively.
  This release makes the value uniform for both the platforms and the threshold time

for Windows and Linux is now 60 minutes.
This enables you to execute scripts that typically take longer to execute, such as scripts to scan file systems or a script to find log4j traces in every running process.

- Previously, the recommended size of script output data was less than 20 KB. This release increases the script output size to 1 MB to accommodate larger outputs. However, the API Gateway service version must be 2.4.0-7 or later to support 1 MB script output.

- **Restart-Service** has been added to the list of blacklisted commands for PowerShell scripts in Qualys CAR 1.5. If your script includes this command, it will be highlighted in the **Blacklisted Commands** section of the **Script Summary** page.
With this improvement, you are more assured and confident of the commands you include in the CAR scripts.

Issue Addressed

No asset jobs were created in specific scenarios even after a successful script execution job. This issue has been fixed and asset jobs are now correctly listed on the **Job Details** page when a script is executed.