Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.21

December 15, 2022

This new version of the Qualys Cloud Platform (VM, PC) includes improvements to the Qualys API. You'll find all the details in our user guides, available at the time of release. Just log in to your Qualys account and go to Help > Resources.

What's New

Qualys API Server URL

The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click here to identify your Qualys platform and get the API URL

This documentation uses the API server URL for Qualys US Platform 1 (https://qualysapi.qualys.com) in sample API requests. If you're on another platform, please replace this URL with the appropriate server URL for your account.

VM Scan Summary API: Filter by Failed Slice and Exceeded Scan Duration Categories

APIs affected	/api/2.0/fo/scan/vm/summary/
New or Updated API	Updated
DTD or XSD changes	No

The VM Scan Summary API has been updated to include 2 new possible values for the include_hosts_summary_categories input parameter: failed_slice and exceeded_scan_duration.

The include_hosts_summary_categories input parameter is used to filter the categories that appear in the output. Note that the output already included the Failed Slice Hosts and Exceeded Scan Duration categories, but this release gives you the ability to filter the output based on these categories. When include_hosts_summary_categories is not specified, all categories are included in the XML output.

Permissions

Manager role is required.

Input Parameters

Use the following input parameter to filter the list of categories included in the API output. Refer to the Qualys API (VM,PC) User Guide for details on all available input parameters.

Parameter	Description
include_hosts_summary_categories={value}	(Optional) When unspecified, all categories are included in the XML output. To filter the categories, provide a comma-separated list of the categories to include in the output. Possible values are: scanned, excluded, cancelled, unresolved, duplicate, not_vulnerable, dead, aborted, blocked, failed_slice, exceeded_scan_duration. Each category appears a block inside <SCAN_RESULTS> <HOSTS>. If a category is filtered out, the respective category block does not appear in the output.

API Samples

Sample 1 - Filter list of categories in output by Failed Slice

In this sample, only the Failed Slice Hosts category is included.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/scan/vm/summary/?action=list&out
put_format=xml&scan_reference=scan/1234567890.12345&include_hosts_summary
_categories=failed_slice"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCAN_SUMMARY_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/vm/summary/output.dtd">
<SCAN_SUMMARY_OUTPUT>
    <RESPONSE>
        <DATETIME>2022-08-28T18:36:16Z</DATETIME>
        <SCAN_SUMMARY_LIST>
            <SCAN_SUMMARY>
                <SCAN_REFERENCE>scan/1234567890.12345</SCAN_REFERENCE>
                <SCAN_INPUT>
                    <TITLE>My-Scan-1</TITLE>
                    <USER>
                        <USERNAME>qualys_joe</USERNAME>
                    </USER>
                    <SCHEDULED>0</SCHEDULED>
                    <SCAN_DATETIME>2022-02-18T12:06:07Z</SCAN_DATETIME>
                    <NETWORK>
                        <ID>0</ID>
                        <NAME>Global Default Network</NAME>
                    </NETWORK>
                    <OPTION_PROFILE>
                        <ID>5642842</ID>
                        <NAME>Initial-Options</NAME>
                    </OPTION_PROFILE>
                    <TARGETS>
                        <IP_LIST>
                            <COUNT>106</COUNT>
                            <IP_DATA>
                                <RANGES>
                                  <RANGE>10.10.10.150-10.10.10.255</RANGE>
                                </RANGES>
                            </IP_DATA>
                        </IP_LIST>
                        <ASSET_GROUP_LIST>
                            <COUNT>1</COUNT>
```

```
                                <ASSET_GROUP_DATA>
                                    <ASSET_GROUP>
                                        <ID>5509050</ID>
                                        <NAME>My-Asset-Group</NAME>
                                    </ASSET_GROUP>
                                </ASSET_GROUP_DATA>
                            </ASSET_GROUP_LIST>
                        </TARGETS>
                    </SCAN_INPUT>
                    <SCAN_DETAILS>
                        <STATUS>ERROR</STATUS>
                      <LAUNCH_DATETIME>2022-02-18T12:06:07Z</LAUNCH_DATETIME>
                        <DURATION>53</DURATION>
                    </SCAN_DETAILS>
                    <SCAN_RESULTS>
                        <HOSTS>
                            <COUNT>106</COUNT>
                            <HOSTS_DATA>
                                <FAILED_SLICE_HOSTS>
                                    <IP_LIST>
                                        <COUNT>53</COUNT>
                                        <IP_DATA>
                                            <RANGES>
                                                <RANGE>10.10.10.150-
10.10.10.202</RANGE>
                                            </RANGES>
                                        </IP_DATA>
                                    </IP_LIST>
                                </FAILED_SLICE_HOSTS>
                            </HOSTS_DATA>
                        </HOSTS>
                        <DETECTIONS>
                            <IG>
                                <TOTAL_COUNT>0</TOTAL_COUNT>
                                <COUNT_BY_SEVERITY>
                                    <SEVERITY_1>0</SEVERITY_1>
                                    <SEVERITY_2>0</SEVERITY_2>
                                    <SEVERITY_3>0</SEVERITY_3>
                                    <SEVERITY_4>0</SEVERITY_4>
                                    <SEVERITY_5>0</SEVERITY_5>
                                </COUNT_BY_SEVERITY>
                            </IG>
                            <VULN>
                                <CONFIRMED>
                                    <TOTAL_COUNT>0</TOTAL_COUNT>
                                    <COUNT_BY_SEVERITY>
                                        <SEVERITY_1>0</SEVERITY_1>
                                        <SEVERITY_2>0</SEVERITY_2>
                                        <SEVERITY_3>0</SEVERITY_3>
```

```
                                    <SEVERITY_4>0</SEVERITY_4>
                                    <SEVERITY_5>0</SEVERITY_5>
                                </COUNT_BY_SEVERITY>
                            </CONFIRMED>
                            <POTENTIAL>
                                <TOTAL_COUNT>0</TOTAL_COUNT>
                                <COUNT_BY_SEVERITY>
                                    <SEVERITY_1>0</SEVERITY_1>
                                    <SEVERITY_2>0</SEVERITY_2>
                                    <SEVERITY_3>0</SEVERITY_3>
                                    <SEVERITY_4>0</SEVERITY_4>
                                    <SEVERITY_5>0</SEVERITY_5>
                                </COUNT_BY_SEVERITY>
                            </POTENTIAL>
                        </VULN>
                    </DETECTIONS>
                </SCAN_RESULTS>
            </SCAN_SUMMARY>
        </SCAN_SUMMARY_LIST>
    </RESPONSE>
```

Sample 2 - Filter list of categories in output by Exceeded Scan Duration

In this sample, only the Exceeded Scan Duration category is included.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/scan/vm/summary/?action=list&out
put_format=xml&scan_reference=scan/1234567890.24680&include_hosts_summary
_categories=exceeded_scan_duration"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCAN_SUMMARY_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/vm/summary/output.dtd">
<SCAN_SUMMARY_OUTPUT>
    <RESPONSE>
        <DATETIME>2022-08-28T18:28:03Z</DATETIME>
        <SCAN_SUMMARY_LIST>
            <SCAN_SUMMARY>
                <SCAN_REFERENCE>scan/1234567890.24680</SCAN_REFERENCE>
                <SCAN_INPUT>
                    <TITLE>My-Scan-2</TITLE>
                    <USER>
                        <USERNAME>qualys_joe</USERNAME>
                    </USER>
                    <SCHEDULED>0</SCHEDULED>
```

```
                        <SCAN_DATETIME>2022-07-13T11:19:57Z</SCAN_DATETIME>
                        <NETWORK>
                            <ID>0</ID>
                            <NAME>Global Default Network</NAME>
                        </NETWORK>
                        <OPTION_PROFILE>
                            <ID>6701026</ID>
                            <NAME>My-Option-Profile</NAME>
                        </OPTION_PROFILE>
                        <TARGETS>
                            <IP_LIST>
                                <COUNT>106</COUNT>
                                <IP_DATA>
                                    <RANGES>
                                      <RANGE>10.10.10.150-10.10.10.255</RANGE>
                                    </RANGES>
                                </IP_DATA>
                            </IP_LIST>
                            <ASSET_GROUP_LIST>
                                <COUNT>1</COUNT>
                                <ASSET_GROUP_DATA>
                                    <ASSET_GROUP>
                                        <ID>5509050</ID>
                                        <NAME>My-Asset-Group</NAME>
                                    </ASSET_GROUP>
                                </ASSET_GROUP_DATA>
                            </ASSET_GROUP_LIST>
                        </TARGETS>
                    </SCAN_INPUT>
                    <SCAN_DETAILS>
                        <STATUS>FINISHED</STATUS>
                       <LAUNCH_DATETIME>2022-07-13T11:19:57Z</LAUNCH_DATETIME>
                        <DURATION>2048</DURATION>
                    </SCAN_DETAILS>
                    <SCAN_RESULTS>
                        <HOSTS>
                            <COUNT>113</COUNT>
                            <HOSTS_DATA>
                                <EXCEEDED_SCAN_DURATION>
                                    <IPV4_LIST>
                                        <COUNT>7</COUNT>
                                        <IPV4_DATA>

<IPV4_CSV>10.10.10.150,10.10.10.175,10.10.10.155-
10.10.10.158,10.10.10.153,10.10.10.156-10.10.10.157</IPV4_CSV>
                                        </IPV4_DATA>
                                    </IPV4_LIST>
                                </EXCEEDED_SCAN_DURATION>
                            </HOSTS_DATA>
```

```
                        </HOSTS>
                        <DETECTIONS>
                            <IG>
                                <TOTAL_COUNT>629</TOTAL_COUNT>
                                <COUNT_BY_SEVERITY>
                                    <SEVERITY_1>498</SEVERITY_1>
                                    <SEVERITY_2>102</SEVERITY_2>
                                    <SEVERITY_3>29</SEVERITY_3>
                                    <SEVERITY_4>0</SEVERITY_4>
                                    <SEVERITY_5>0</SEVERITY_5>
                                </COUNT_BY_SEVERITY>
                            </IG>
                            <VULN>
                                <CONFIRMED>
                                    <TOTAL_COUNT>2608</TOTAL_COUNT>
                                    <COUNT_BY_SEVERITY>
                                        <SEVERITY_1>2</SEVERITY_1>
                                        <SEVERITY_2>81</SEVERITY_2>
                                        <SEVERITY_3>1176</SEVERITY_3>
                                        <SEVERITY_4>972</SEVERITY_4>
                                        <SEVERITY_5>377</SEVERITY_5>
                                    </COUNT_BY_SEVERITY>
                                </CONFIRMED>
                                <POTENTIAL>
                                    <TOTAL_COUNT>60</TOTAL_COUNT>
                                    <COUNT_BY_SEVERITY>
                                        <SEVERITY_1>7</SEVERITY_1>
                                        <SEVERITY_2>8</SEVERITY_2>
                                        <SEVERITY_3>39</SEVERITY_3>
                                        <SEVERITY_4>6</SEVERITY_4>
                                        <SEVERITY_5>0</SEVERITY_5>
                                    </COUNT_BY_SEVERITY>
                                </POTENTIAL>
                            </VULN>
                        </DETECTIONS>
                    </SCAN_RESULTS>
                </SCAN_SUMMARY>
            </SCAN_SUMMARY_LIST>
        </RESPONSE>
    </SCAN_SUMMARY_OUTPUT>
```

Improved Error Text When Adding DNS Names to Asset Group with Invalid FQDN

APIs affected	/api/2.0/fo/asset/group
New or Updated API	Updated
DTD or XSD changes	No

We improved the error text that appears in the response when adding a list of DNS names to an asset group and at least one of the DNS values is invalid. Now the response will show you the invalid entry so you can more easily revise the list and try again. This is especially useful when you're adding a very long list of DNS names and it's difficult to find the invalid entry.

In the following example, an IP address (10.10.10.10) is included in the list of DNS names being added to the asset group using the add_dns_names input parameter. Since the IP is not a valid DNS name, you'll see it in the error text.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d "action=edit&id=123456789&add_dns_names=abc.sample.qualys.com,
xyz.sample.qualys.com, 123.sample.qualys.com, 456.sample.qualys.com,
abc.demo.qualys.com, xyz.demo.qualys.com, 10.10.10.10,
123.demo.qualys.com, 456.demo.qualys.com"
"https://qualysapi.qualys.com/api/2.0/fo/asset/group/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2022-08-24T10:06:54Z</DATETIME>
    <CODE>1905</CODE>
    <TEXT> (Add DNS Hostnames - The provided DNS list has invalid FQDNs.
Please revise the list (10.10.10.10).)</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

PC API: Get Posture Based on Last Status Change

APIs affected	/api/2.0/fo/report/?action=fetch
New or Updated API	Updated
DTD or XSD changes	No

The Get Posture API has been updated to include a new optional parameter that helps you get compliance information for hosts whose posture has changed since the specified date or time.

Input Parameters

Use the following input parameter to filter the list of hosts for which you want to get the current compliance posture as compared to their last posture. Refer to the Qualys API (VM,PC) User Guide for details on all available input parameters.

Parameter	Description
StatusChangedSince	(Optional) Compliance posture information records when the posture is changed in policy since the specified date. You may also specify the time. The format for date and time is: YYYY-MM-DD or YYYY-MM-DDTHH:MM:SSZ (UTC/GMT)

API Sample

Sample - Get Posture Info without evidence, without compression, with StatusChangedSince

In this sample, only the hosts whose compliance status has changed since the specified date are included.

API request:

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=0&compressionRe
quired=0&statusChangedSince=2021-12-23" -H "accept: */*" -H
"Authorization: Bearer <token>" -H "Content-Type:
application/json" -d
"[{\"policyId\":\"<POLICYID>\",\"subscriptionId\":\"<SUBSCRIPTIONI
D>\",\"hostIds\":[\"<HOST ID1>\",\"<HOST ID2>\"]}]"
```

Response:

```
[
    {
```

```
  "id": 24442645,
  "instance": "os",
  "policyId": 5266764,
  "policyTitle": "CIS Reference Policies",
  "netBios": null,
  "controlId": 7420,
  "controlStatement": "Status of the 'default Group ID (GID)'
setting for the root account",
  "rationale": "Setting the root account to GID 0 prevents
unauthorized users from accessing files and directories owned by
the root user.  As this check reveals the Group ID (GID) for the
root user as found in '/etc/passwd', run this check periodically
according to the needs of the business.",
  "remediation": "Run the following command to set the user default
group to GID  according to the business needs and organization's
security policies.\n$sudo usermod -g <GID> <root>  \n\n#
Example\n$sudo usermod -g 0 root",
  "controlReference": null,
  "technologyId": 94,
  "status": "Failed",
  "previousStatus": "Passed",
  "firstFailDate": "2022-11-21T10:43:37Z",
  "lastFailDate": "2022-11-21T10:43:37Z",
  "firstPassDate": "2022-09-29T19:19:18Z",
  "lastPassDate": "2022-09-30T05:29:47Z",
  "postureModifiedDate": "2022-11-21T10:43:36Z",
  "lastEvaluatedDate": "2022-11-21T10:43:36Z",
  "created": "2022-11-30T14:19:55Z",
  "hostId": 8650051,
  "cloudResourceId": null,
  "ip": "10.11.70.79",
  "trackingMethod": "IP",
  "os": null,
  "osCpe": "cpe:/o:suse:linux_enterprise_server:12_sp1:::",
  "domainName": "comdevpsql92.comp.rdlab.qualys.com",
  "dns": "comdevpsql92.comp.rdlab.qualys.com",
  "qgHostid": null,
  "networkId": 0,
  "networkName": "Global Default Network",
  "complianceLastScanDate": "2022-09-30T05:08:44Z",
  "customerUuid": "f1495d3b-c169-fdd6-82cd-9ca83f5e8f8b",
  "customerId": "1743081",
  "assetId": 21450940,
  "technology": {
    "id": 94,
    "name": "SUSE Linux Enterprise 12.x"
  },
```

```
  "criticality": {
    "label": "IMPORTANT",
    "value": 5
  },
  "evidence": {
    "expectedValues": "\nSetting not found\n------------ OR ------
------\nmatch all equal to\n0",
    "currentValues": [
      "root 0"
    ],
    "actualValues": null,
    "directoryFimUdc": null
  },
  "causeOfFailure": {
    "missing": {
      "logic": null,
      "value": [
        "0",
        "------------ OR ------------",
        "Setting not found"
      ]
    },
    "unexpected": {
      "value": [
        "root 0"
      ]
    }
  },
  "currentBatch": 4,
  "totalBatches": 9
}
```

Issues Addressed

- When updating authentication records using the API, a valid error message will now appear when an IP is being added to a record and the same IP already exists in another record of the same type for the same network (when Network Support feature is enabled).
- We have fixed the issue where users could update the authentication record of a type (Windows, for example) using the API of another type (Unix, for example). The users now receive an error message when they attempt to do so.
- When a VMware ESXi authentication record with the settings Login Credentials: Use vCenter (login_type=vcenter) and Disconnected ESXi enabled (is_disconnect=1) was updated using the API (for example to add IPs to the record), the Disconnected ESXi option was being disabled when it shouldn't have been. Now this setting will not change as the result of other updates to the authentication record via the API.
- We fixed an issue where the Update action for Unix authentication record using the API returned an error when multiple record IDs were specified in the API request.
- We have fixed an issue where customers with AGMS-enabled accounts couldn't run the 'Update Schedule Scan API' due to an internal ORA error.
- We fixed the behavior of PosturStreamingAPI output when the user changes the criticality label name from policy setup. Users are now able to see the correct criticality label names in JSON and XML reports.