Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.22.3

June 07, 2023

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

Renamed a Parameter in Get Posture Info API

Enhanced Validation in VMware ESXi Authentication Record

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.

Renamed a Parameter in Get Posture Info API

APIs affected	/pcrs/1.0/posture/postureInfo
Operator	POST
New or Updated API	Updated
DTD or XSD changes	No

The “cloudResourceId” parameter in the API response is now renamed “CLOUD_RESOURCE_ID”.

API Sample

Sample

Get Posture Info without lastEvaluationDate, without evidence, with compression, with lastScanDate

API Request:

```
curl-X POST
"<qualys_base_url>/pcrs/1.0/posture/postureInfo?evidenceRequired=0&compre
ssionRequired=1&lastEvaluationDate=202
1-12-17T18:48:16Z&lastScanDate=2021-12-17T18:48:16Z"
-H "accept: */*"
-H "Content-Type: application/json"
-d "[{\"policyId\":\"<POLICY ID>\",\"subscriptionId\":\"<SUBCRIPTION
ID>\",\"hostIds\":[\"<HOST ID>\"]}]"
```

Response:

```
[
    {
        "id": "<HOST INSTANCE ID>",
        "instance": "os",
        "policyId": "<POLICY ID>",
        "controlId": "<CONTROL ID>",
        "controlStatement": "Status of the 'Minimum Password Length'
setting",
        "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
'minimum password length' requirement. Each character that is added to the
password length squares the difficulty of breaking the password via 'brute
force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password. While
no 'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along with
requiring other password security factors, such as increasing the size of
the symbol set-space by requiring mixed-cases, along with other forms of
password variability creation, increases the difficulty of breaking any
password by brute-force attack.",
        "remediation": "To specify password length requirements for new
accounts, edit the file \"/etc/login.defs\" and add or correct the
following lines: \n\nPASS_MIN_LEN <required
value>\n\nexample:\n\nPASS_MIN_LEN 14\n\n\nNote:\nThe DoD requirement is
\"14\". If a program consults \"/etc/login.defs\" and also another PAM
module (such as \"pam_cracklib\") during a password change operation, then
the most restrictive must be satisfied.",
        "controlReference": null,
        "technologyId": "<TECHNOLOGY ID>",
        "status": "Passed",
        "previousStatus": "Passed",
        "firstFailDate": "",
        "lastFailDate": "",
        "firstPassDate": "2021-12-23T08:20:23Z",
        "lastPassDate": "2022-02-02T11:54:20Z",
        "postureModifiedDate": "2021-12-23T08:20:22Z",
        "lastEvaluatedDate": "2022-02-02T11:54:20Z",
        "created": "2022-07-11T11:53:46Z",
        "hostId": "<HOST ID>",
        "CLOUD_RESOURCE_ID": "<CLOUD RESOURCE ID>",
        "ip": "xx.xx.xx.xxx",
        "trackingMethod": "EC2",
        "os": "Red Hat Enterprise Linux 8.3",
        "osCpe": null,
        "dns": "ip-xx-xx-xx-xxx.af-south-1.compute.internal",
        "qgHostid": null,
        "networkId": 0,
        "networkName": "Global Default Network",
        "complianceLastScanDate": "2021-12-23T12:59:04Z",
        "customerUuid": "<CUSTOMER UUID>",
        "customerId": "<CUSTOMER ID>",
        "assetId": "<ASSET ID>",
        "technology": {
            "id": 217,
            "name": "Red Hat Enterprise Linux 8.x"
        },
        "criticality": {
            "label": "CRITICAL",
            "value": 4
        },
        "evidence": null,
        "causeOfFailure": null,
        "currentBatch": 8,
        "totalBatches": 12
    },
]
```

Enhanced Validation in VMware ESXi Authentication Record

APIs affected	/api/2.0/fo/auth/vmware/
Operator	POST
New or Updated API	Updated
DTD or XSD changes	No

Starting this release, while creating or updating a VMware ESXi authentication record with login type vCenter, if you set “is_disconnect=1” and add IPs that are already associated with a Unix record, the VMware ESXi record is not created or updated. Instead, an error is returned in the response. Remove the IPs from the non-applicable record to resolve the error.

Sample

Try creating VMware ESXi record with “is_disconnect=1” and IPs that are already associated with a Unix record

API Request:

```
curl -k -s -S -u "aws_ak:test"
-H 'X-Requested-With:curl demo2'
-d
"action=create&ips=10.11.70.187&is_disconnect=1&title=preTestVMWaresxiAPI
&login_type=vcenter" "<qualys_base_url>/api/2.0/fo/auth/vmware/"
```

Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
   <RESPONSE>
       <DATETIME>
          2023-05-29T05:45:32Z
        </DATETIME>
        <CODE>
          1920
        </CODE>
       <TEXT>
          Unable to save the record. The Disconnected ESXi check box is
selected and a Unix record already contains the following IPs:
'10.11.70.187'. The specified IPs cannot be part of both Unix and VMware
ESXi records.
        </TEXT>
    </RESPONSE>
```

```
        </SIMPLE_RETURN>
```