Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.20

June 30, 2022 (Updated July 22, 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.

Display CVSS Version 3.1 in API Output and Reports

APIs affected	/api/2.0/fo/knowledge_base/vuln/?action=list /api/2.0/fo/qid/search_list/dynamic/?action=list /api/2.0/fo/report/?action=fetch
New or Updated API	Updated
DTD or XSD changes	Yes
APIs affected	/api/2.0/fo/report/template/scan/?action=export /api/2.0/fo/report/template/patch/?action=export /api/2.0/fo/report/template/pciscan/?action=export
New or Updated API	Updated
DTD or XSD changes	No

We calculate CVSS3 scores for vulnerabilities based on CVSS version 3.1. However, the labels that appear in the UI, API and Reports where we display CVSS3 scores do not currently reflect the 3.1 version number. Now you will see CVSS version 3.1 wherever CVSS3 values are referenced.

Note: As in previous releases, the CVSS Scoring feature must be enabled for the subscription to display CVSS scores for vulnerabilities. Managers enable CVSS Scoring for the subscription on the **CVSS Setup** page at **Reports** > **Setup** > **CVSS**.

API Output Changes

We updated the XML output for the KnowledgeBase List API and the Dynamic Search List API to include the new tag <CVSS3_VERSION>3.1</CVSS3_VERSION> which identifies the current CVSS3 version.

When you export report templates (Scan Template, Patch Template, PCI Scan Template) using the API, the value for the “cvss” INFO Key will now appear as “cvss3.1” when the cvss template setting is cvss3 (from API) or CVSSv3.1 (from UI).

Report Changes

When CVSS Scoring is enabled for the subscription, you can choose to display CVSS scores in Scan Reports, Patch Reports and PCI Scan Reports. In the report template, you’ll select whether to display CVSS version 2, CVSS version 3.1, or both. You can download reports from the UI or fetch reports using the API.

XML Reports

When CVSS scores are displayed in an XML report, the output will include the new tag <CVSS3_VERSION>3.1</CVSS3_VERSION>.

CSV Reports

We renamed CVSS3 column headings in CSV reports.

- The column “CVSS3” changed to “CVSS3.1”.
- The column “CVSS3 Base” changed to “CVSS3.1 Base”.
- The column “CVSS3 Temporal” changed to “CVSS3.1 Temporal”.

Samples

Sample KnowledgeBase List API

This sample shows the output for KnowledgeBase API where CVSS scores are included. You’ll see the new <CVSS3_VERSION> tag in the output. Also, the CVSS3 value for <VECTOR_STRING> also correctly reflects the 3.1 version.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"https://qualysapi.qualys.com/api/2.0/fo/knowledge_base/vuln/?action=list
&ids=197137,277714"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE KNOWLEDGE_BASE_VULN_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/knowledge_base/vuln/knowledge_ba
se_vuln_list_output.dtd">
<KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
    <RESPONSE>
```

```
        <DATETIME>2022-06-24T04:31:31Z</DATETIME>
        <VULN_LIST>
            <VULN>
                <QID>197137</QID>
                <VULN_TYPE>Vulnerability</VULN_TYPE>
                <SEVERITY_LEVEL>3</SEVERITY_LEVEL>
                <TITLE>
                    <![CDATA[Ubuntu Security Notification for Qemu
Vulnerabilities (USN-3649-1)]]>
                </TITLE>
                <CATEGORY>Ubuntu</CATEGORY>
                <LAST_SERVICE_MODIFICATION_DATETIME>2018-05-
17T10:49:46Z</LAST_SERVICE_MODIFICATION_DATETIME>
                <PUBLISHED_DATETIME>2018-05-
17T10:49:46Z</PUBLISHED_DATETIME>

...

                <CVSS>
                    <BASE>3.3</BASE>
                    <TEMPORAL>2.4</TEMPORAL>

<VECTOR_STRING>CVSS:2.0/AV:L/AC:M/Au:N/C:P/I:P/A:N/E:U/RL:OF/RC:C</VECTOR
_STRING>
                </CVSS>
                <CVSS_V3>
                    <BASE>4.2</BASE>
                    <TEMPORAL>3.7</TEMPORAL>

<VECTOR_STRING>CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N/E:U/RL:O/RC:
C</VECTOR_STRING>
                    <CVSS3_VERSION>3.1</CVSS3_VERSION>
                </CVSS_V3>
                <PCI_FLAG>0</PCI_FLAG>
                <DISCOVERY>
                    <REMOTE>0</REMOTE>
                    <AUTH_TYPE_LIST>
                        <AUTH_TYPE>Unix</AUTH_TYPE>
                    </AUTH_TYPE_LIST>
                    <ADDITIONAL_INFO>Patch Available</ADDITIONAL_INFO>
                </DISCOVERY>
            </VULN>
        </VULN_LIST>
    </RESPONSE>
</KNOWLEDGE_BASE_VULN_LIST_OUTPUT>
```

DTD update:

We updated the DTD for KnowledgeBase List Output to include new elements (in bold).

DTD: <platform>/api/2.0/fo/knowledge_base/vuln/knowledge_base_vuln_list_output.dtd

```
<!-- QUALYS KNOWLEDGE_BASE_VULN_LIST_OUTPUT DTD -->
<!-- $Revision: TBD $ -->
<!ELEMENT KNOWLEDGE_BASE_VULN_LIST_OUTPUT (REQUEST?,RESPONSE)>

...
        <!ELEMENT CVSS (BASE?, TEMPORAL?, VECTOR_STRING?, ACCESS?,
IMPACT?, AUTHENTICATION?, EXPLOITABILITY?, REMEDIATION_LEVEL?,
REPORT_CONFIDENCE?)>
          <!ELEMENT BASE (#PCDATA)>
            <!ATTLIST BASE source CDATA #IMPLIED>
          <!ELEMENT TEMPORAL (#PCDATA)>
          <!ELEMENT VECTOR_STRING (#PCDATA)>
          <!ELEMENT CVSS3_VERSION (#PCDATA)>
          <!ELEMENT ACCESS (VECTOR?, COMPLEXITY?)>
            <!ELEMENT VECTOR (#PCDATA)>
            <!ELEMENT COMPLEXITY (#PCDATA)>
          <!ELEMENT IMPACT (CONFIDENTIALITY?, INTEGRITY?, AVAILABILITY?)>
            <!ELEMENT CONFIDENTIALITY (#PCDATA)>
            <!ELEMENT INTEGRITY (#PCDATA)>
            <!ELEMENT AVAILABILITY (#PCDATA)>
          <!ELEMENT AUTHENTICATION (#PCDATA)>
          <!ELEMENT EXPLOITABILITY (#PCDATA)>
          <!ELEMENT REMEDIATION_LEVEL (#PCDATA)>
          <!ELEMENT REPORT_CONFIDENCE (#PCDATA)>
        <!ELEMENT CVSS_V3 (BASE?, TEMPORAL?, VECTOR_STRING?,
CVSS3_VERSION?, ATTACK?, IMPACT?, PRIVILEGES_REQUIRED?,
USER_INTERACTION?, SCOPE?, EXPLOIT_CODE_MATURITY?, REMEDIATION_LEVEL?,
REPORT_CONFIDENCE?)>
        <!ELEMENT ATTACK (VECTOR?, COMPLEXITY?)>
        <!ELEMENT PRIVILEGES_REQUIRED (#PCDATA)>
...
```

Sample Dynamic Search List API

This sample shows the output for list action for dynamic search list where CVSS3 scores are included. You'll see the new <CVSS3_VERSION> tag in the output.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/qid/search_list/dynamic/?action=
list&ids=4791898"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE DYNAMIC_SEARCH_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/qid/search_list/dynamic/dynamic_
list_output.dtd">
<DYNAMIC_SEARCH_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2022-06-21T05:37:18Z</DATETIME>
        <DYNAMIC_LISTS>
            <DYNAMIC_LIST>
                <ID>4791898</ID>
                <TITLE>
                    <![CDATA[My_Dynamic_List]]>
                </TITLE>
                <GLOBAL>No</GLOBAL>
                <OWNER>
                    <![CDATA[Joe User (joe_user)]]>
                </OWNER>
                <CREATED>2022-06-21T05:36:55Z</CREATED>
                <MODIFIED_BY>
                    <![CDATA[Joe User (joe_user)]]>
                </MODIFIED_BY>
                <MODIFIED>2022-06-21T05:36:55Z</MODIFIED>
                <CRITERIA>
                    <DISCOVERY_METHOD>
                        <![CDATA[All]]>
                    </DISCOVERY_METHOD>
                    <CVSS_BASE_SCORE>
                        <![CDATA[3]]>
                    </CVSS_BASE_SCORE>
                    <CVSS_TEMPORAL_SCORE>
                        <![CDATA[2]]>
                    </CVSS_TEMPORAL_SCORE>
                    <CVSS3_BASE_SCORE>
                        <![CDATA[2]]>
                    </CVSS3_BASE_SCORE>
                    <CVSS3_TEMPORAL_SCORE>
                        <![CDATA[2]]>
```

```
                        </CVSS3_TEMPORAL_SCORE>
                        <CVSS_BASE_SCORE_OPERAND>
                            <![CDATA[&gt;=]]>
                        </CVSS_BASE_SCORE_OPERAND>
                        <CVSS_TEMPORAL_SCORE_OPERAND>
                            <![CDATA[&lt;]]>
                        </CVSS_TEMPORAL_SCORE_OPERAND>
                        <CVSS3_BASE_SCORE_OPERAND>
                            <![CDATA[&gt;=]]>
                        </CVSS3_BASE_SCORE_OPERAND>
                        <CVSS3_TEMPORAL_SCORE_OPERAND>
                            <![CDATA[&lt;]]>
                        </CVSS3_TEMPORAL_SCORE_OPERAND>
                        <CVSS3_VERSION>3.1</CVSS3_VERSION>
                    </CRITERIA>
                </DYNAMIC_LIST>
            </DYNAMIC_LISTS>
        </RESPONSE>
</DYNAMIC_SEARCH_LIST_OUTPUT>
```

DTD update:

We updated the DTD for Dynamic Search List Output to include new elements (in bold).

DTD: <platform>/api/2.0/fo/qid/search_list/dynamic/dynamic_list_output.dtd

```
<!-- QUALYS DYNAMIC_SEARCH_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT DYNAMIC_SEARCH_LIST_OUTPUT (REQUEST?,RESPONSE)>

<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, DYNAMIC_LISTS?)>
<!ELEMENT DYNAMIC_LISTS (DYNAMIC_LIST+)>
<!ELEMENT DYNAMIC_LIST (ID, TITLE, GLOBAL, OWNER, CREATED?, MODIFIED_BY?,
MODIFIED?, QIDS?, CRITERIA, OPTION_PROFILES?, REPORT_TEMPLATES?,
REMEDIATION_POLICIES?, DISTRIBUTION_GROUPS?, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT GLOBAL (#PCDATA)>
```

```
<!ELEMENT OWNER (#PCDATA)>
<!ELEMENT CREATED (#PCDATA)>
<!ELEMENT MODIFIED_BY (#PCDATA)>
<!ELEMENT MODIFIED (#PCDATA)>
<!ELEMENT QIDS (QID+)>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT CRITERIA (VULNERABILITY_TITLE?, DISCOVERY_METHOD?,
AUTHENTICATION_TYPE?, USER_CONFIGURATION?, CATEGORY?,
CONFIRMED_SEVERITY?, POTENTIAL_SEVERITY?, INFORMATION_SEVERITY?, VENDOR?,
PRODUCT?, CVSS_BASE_SCORE?, CVSS_TEMPORAL_SCORE?, CVSS3_BASE_SCORE?,
CVSS3_TEMPORAL_SCORE?, CVSS_ACCESS_VECTOR?, PATCH_AVAILABLE?,
VIRTUAL_PATCH_AVAILABLE?, CVE_ID?, EXPLOITABILITY?, ASSOCIATED_MALWARE?,
VENDOR_REFERENCE?, BUGTRAQ_ID?, VULNERABILITY_DETAILS?,
SUPPORTED_MODULES?, COMPLIANCE_DETAILS?, COMPLIANCE_TYPE?,
QUALYS_TOP_20?, OTHER?, NETWORK_ACCESS?, PROVIDER?,
CVSS_BASE_SCORE_OPERAND?, CVSS_TEMPORAL_SCORE_OPERAND?,
CVSS3_BASE_SCORE_OPERAND?, CVSS3_TEMPORAL_SCORE_OPERAND?, CVSS3_VERSION?,
USER_MODIFIED?, PUBLISHED?, SERVICE_MODIFIED?, CPE?)>
...
<!ELEMENT CVSS_BASE_SCORE_OPERAND (#PCDATA)>
<!ELEMENT CVSS_TEMPORAL_SCORE_OPERAND (#PCDATA)>
<!ELEMENT CVSS3_BASE_SCORE (#PCDATA)>
<!ELEMENT CVSS3_TEMPORAL_SCORE (#PCDATA)>
<!ELEMENT CVSS3_BASE_SCORE_OPERAND (#PCDATA)>
<!ELEMENT CVSS3_TEMPORAL_SCORE_OPERAND (#PCDATA)>
<!ELEMENT CVSS3_VERSION (#PCDATA)>
<!ELEMENT OPTION_PROFILES (OPTION_PROFILE+)>
<!ELEMENT OPTION_PROFILE (ID, TITLE)>
<!ELEMENT REPORT_TEMPLATES (REPORT_TEMPLATE+)>
<!ELEMENT REPORT_TEMPLATE (ID, TITLE)>
<!ELEMENT REMEDIATION_POLICIES (REMEDIATION_POLICY+)>
<!ELEMENT REMEDIATION_POLICY (ID, TITLE)>
<!ELEMENT DISTRIBUTION_GROUPS (DISTRIBUTION_GROUP+)>
<!ELEMENT DISTRIBUTION_GROUP (NAME)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT COMMENTS (#PCDATA)>
<!ELEMENT USER_MODIFIED (#PCDATA)>
<!ELEMENT PUBLISHED (#PCDATA)>
<!ELEMENT SERVICE_MODIFIED (#PCDATA)>
<!ELEMENT CPE (#PCDATA)>
<!-- EOF -->
```

Sample Export Scan Template

In this sample, the Scan Template being exported has CVSSv3.1 selected. The same change applies to Patch Templates and PCI Scan Templates.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
"https://qualysapi.qualys.com/api/2.0/fo/report/template/scan/?action=exp
ort&template_id=89470&report_format=xml"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORTTEMPLATE SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/report/template/scan/scanreportt
emplate_info.dtd">
<REPORTTEMPLATE>
  <SCANTEMPLATE>
    <TITLE>
      <INFO key="title"><![CDATA[My-Scan-Report]]></INFO>
      <INFO key="owner"><![CDATA[1086]]></INFO>
    </TITLE>
...
    <DISPLAY>
      <INFO key="graph_business_risk"><![CDATA[1]]></INFO>
      <INFO key="graph_vuln_over_time"><![CDATA[1]]></INFO>
      <INFO key="display_text_summary"><![CDATA[1]]></INFO>
      <INFO key="graph_status"><![CDATA[1]]></INFO>
      <INFO key="graph_potential_status"><![CDATA[1]]></INFO>
      <INFO key="graph_severity"><![CDATA[1]]></INFO>
      <INFO key="graph_potential_severity"><![CDATA[1]]></INFO>
      <INFO key="graph_ig_severity"><![CDATA[1]]></INFO>
      <INFO key="graph_top_categories"><![CDATA[1]]></INFO>
      <INFO key="graph_top_vulns"><![CDATA[1]]></INFO>
      <INFO key="graph_os"><![CDATA[1]]></INFO>
      <INFO key="graph_services"><![CDATA[1]]></INFO>
      <INFO key="graph_top_ports"><![CDATA[1]]></INFO>
      <INFO key="display_custom_footer"><![CDATA[1]]></INFO>
      <INFO key="display_custom_footer_text"><![CDATA[Test@123]]></INFO>
      <INFO key="sort_by"><![CDATA[host]]></INFO>
      <INFO key="cvss"><![CDATA[cvss3.1]]></INFO>
      <INFO key="host_details"><![CDATA[0]]></INFO>
      <INFO key="qualys_system_ids"><![CDATA[1]]></INFO>
...
```

Sample Scan-Based Scan Report in XML Format

This sample shows a Scan Report with Scan-Based Findings in XML format. You'll see the new <CVSS3_VERSION> tag in the output.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=fetch&id=1234567&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>

<!DOCTYPE SCAN SYSTEM "https://qualysapi.qualys.com/scan-1.dtd">
<SCAN value="scan/1234567890.12345">

...
    <CAT value="General remote services" port="22" protocol="tcp">
      <VULN number="38739" severity="3">
        <TITLE><![CDATA[Deprecated SSH Cryptographic Settings]]></TITLE>
        <LAST_UPDATE><![CDATA[2021-05-26T11:40:40Z]]></LAST_UPDATE>
        <CVSS_BASE source="service">6.4</CVSS_BASE>
        <CVSS_TEMPORAL>4.7</CVSS_TEMPORAL>
        <CVSS3_BASE>6.5</CVSS3_BASE>
        <CVSS3_TEMPORAL>5.3</CVSS3_TEMPORAL>
        <CVSS3_VERSION>3.1</CVSS3_VERSION>
        <PCI_FLAG>1</PCI_FLAG>
       <DIAGNOSIS><![CDATA[The SSH protocol (Secure Shell) is a method for
secure remote login from one computer to another. <P>
The target is using deprecated SSH cryptographic settings to
communicate.]]></DIAGNOSIS>
        <CONSEQUENCE><![CDATA[A man-in-the-middle attacker may be able to
exploit this vulnerability to record the communication to decrypt the
session key and even the messages.<P>]]></CONSEQUENCE>
...
```

DTD update:

We updated the Scan DTD to include new elements (in bold).

DTD: <platform>/scan-1.dtd

```
<!-- QUALYS SCAN DTD -->
<!-- $Revision$ -->
<!ELEMENT SCAN ((HEADER | ERROR | IP | IPV6)+)>
<!ATTLIST SCAN
    value CDATA #REQUIRED
>
...
```

```
<!-- VULNERABILITIES -->
<!ELEMENT VULNS (CAT)+>
<!ELEMENT VULN (TITLE, LAST_UPDATE?, CVSS_BASE?, CVSS_TEMPORAL?,
CVSS3_BASE?, CVSS3_TEMPORAL?, CVSS3_VERSION?, PCI_FLAG, INSTANCE?,
VENDOR_REFERENCE_LIST?, CVE_ID_LIST?, BUGTRAQ_ID_LIST?,
DIAGNOSIS?, DIAGNOSIS_COMMENT?, CONSEQUENCE?, CONSEQUENCE_COMMENT?,
SOLUTION?, SOLUTION_COMMENT?, COMPLIANCE?, CORRELATION?,
RESULT?, RESULT_ERRORS?, RESULT_DEBUG?)>
<!-- number is Qualys numeric ID -->
<!-- cveid is the CVE identification code (if any) -->
<!-- severity is Qualys severity level 1 to 5 (possibly customized)  -->
<!-- standard-severity is the original Qualys severity level 1 to 5 if it
has been customized by the user -->
<!ATTLIST VULN
    number CDATA #REQUIRED
    cveid CDATA #IMPLIED
    severity CDATA #REQUIRED
    standard-severity CDATA #IMPLIED
>

<!-- Required Element -->

<!ELEMENT TITLE (#PCDATA)>

<!-- Optional Elements -->

<!ELEMENT LAST_UPDATE (#PCDATA)>

<!ELEMENT CVSS_BASE (#PCDATA)>
<!ATTLIST CVSS_BASE
    source CDATA #IMPLIED
>

<!ELEMENT CVSS_TEMPORAL (#PCDATA)>
<!ELEMENT CVSS3_BASE (#PCDATA)>
<!ELEMENT CVSS3_TEMPORAL (#PCDATA)>
<!ELEMENT CVSS3_VERSION (#PCDATA)>
<!ELEMENT PCI_FLAG (#PCDATA)>
...
```

Sample Scan-Based Scan Report in CSV Format

This sample shows a Scan Report with Scan-Based Findings in CSV format. Note the renamed column headings with CVSS3.1.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=fetch&id=1234567&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

CSV output:

```
"ScanBased","06/22/2022 at 12:56:13 (GMT+0530)"
"Qualys, Inc.","919 E Hillsdale Blvd, 4th floor",,"Foster
City","California","United States of America","94404"
"Joe User","joe_user","Manager"

"Launch Date","Active Hosts","Total
Hosts","Type","Status","Reference","Scanner Appliance","Duration","Scan
Title","Asset Groups","IPs","Excluded IPs","Option Profile","Network"
"06/09/2022 at 00:01:03 (GMT+0530)","5","5","Scheduled (default option
profile)","Finished","scan/1654713064.38255","10.115.51.101 (Scanner
12.10.24-1, Vulnerability Signatures 2.5.474-
6)","00:22:12","testUI",,"10.20.30.40-10.20.30.40",,"Initial
Options","network1"

"IP","DNS","NetBIOS","OS","IP
Status","QID","Title","Type","Severity","Port","Protocol","FQDN","SSL","C
VE ID","Vendor Reference","Bugtraq ID","CVSS Base","CVSS
Temporal","CVSS3.1 Base","CVSS3.1
Temporal","Threat","Impact","Solution","Exploitability","Associated
Malware","Results","PCI Vuln","Instance","Category"
"10.20.30.40","No registered hostname",,,"host scanned, found
vuln","38739","Deprecated SSH Cryptographic
Settings","Vuln","3","22","tcp",,,,,,"6.4
(AV:N/AC:L/Au:N/C:P/I:P/A:N)","4.7 (E:U/RL:W/RC:UC)","6.5
(AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)","5.3 (E:U/RL:W/RC:U)","The SSH
protocol (Secure Shell) is a method for secure remote login from one
computer to another...
...
```

Sample Host-Based Scan Report in XML Format

This sample shows a Scan Report with Host-Based Findings in XML format. You'll see the new <CVSS3_VERSION> tag in the output.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=fetch&id=1234567&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>

<!DOCTYPE ASSET_DATA_REPORT SYSTEM
"https://qualysapi.qualys.com/asset_data_report.dtd">
<ASSET_DATA_REPORT>
  <HEADER>
    <COMPANY><![CDATA[Qualys,Inc.]]></COMPANY>
    <USERNAME>joe_user</USERNAME>
    <GENERATION_DATETIME>2022-06-22T03:44:37Z</GENERATION_DATETIME>
    <TEMPLATE><![CDATA[MyScanReport]]></TEMPLATE>

...

        <VULN_INFO>
          <QID id="qid_34000">34000</QID>
          <TYPE>Vuln</TYPE>
          <SSL>false</SSL>
          <RESULT><![CDATA[The host responded 4 times to 4 TCP SYN probes
sent to destination port 20 using source port 53. However, it did not
respond at all to 4 TCP SYN probes sent to the same destination port using
a random source port.]]></RESULT>
          <FIRST_FOUND>2022-05-31T10:32:03Z</FIRST_FOUND>
          <LAST_FOUND>2022-06-07T04:45:26Z</LAST_FOUND>
          <TIMES_FOUND>9</TIMES_FOUND>
          <VULN_STATUS>Active</VULN_STATUS>
          <CVSS_FINAL>3.6</CVSS_FINAL>
          <CVSS3_FINAL>-</CVSS3_FINAL>
          <CVSS3_VERSION>3.1</CVSS3_VERSION>
        </VULN_INFO>
...

  <GLOSSARY>
    <VULN_DETAILS_LIST>
      <VULN_DETAILS id="qid_34000">
        <QID id="qid_34000">34000</QID>
        <TITLE><![CDATA[TCP Source Port Pass Firewall]]></TITLE>
        <SEVERITY>3</SEVERITY>
```

```
        <CATEGORY>Firewall</CATEGORY>
       <THREAT><![CDATA[Your firewall policy seems to let TCP packets with
a specific source port pass through.]]></THREAT>
        <IMPACT><![CDATA[Some types of requests can pass through the
firewall. The port number listed in the results section of this
vulnerability report is the source port that unauthorized users can use to
bypass your firewall.]]></IMPACT>
        <SOLUTION><![CDATA[Make sure that all your filtering rules are
correct and strict enough. If the firewall intends to deny TCP connections
to a specific port, it should be configured to block all TCP SYN packets
going to this port, regardless of the source port.]]></SOLUTION>
        <PCI_FLAG>1</PCI_FLAG>
        <LAST_UPDATE>2017-07-10T17:52:41Z</LAST_UPDATE>
        <CVSS_SCORE>
          <CVSS_BASE source="service">5.0
(AV:N/AC:L/Au:N/C:P/I:N/A:N)</CVSS_BASE>
          <CVSS_TEMPORAL>3.6 (E:U/RL:W/RC:UC)</CVSS_TEMPORAL>
        </CVSS_SCORE>
        <CVSS3_SCORE>
          <CVSS3_BASE>-</CVSS3_BASE>
          <CVSS3_TEMPORAL>-</CVSS3_TEMPORAL>
          <CVSS3_VERSION>3.1</CVSS3_VERSION>
        </CVSS3_SCORE>
      </VULN_DETAILS>
...
```

DTD update:

We updated the Asset Data Report DTD to include new elements (in bold).

DTD: <platform>/asset_data_report.dtd

```
<!-- QUALYS ASSET DATA REPORT DTD -->
<!-- $Revision$ -->

<!ELEMENT ASSET_DATA_REPORT (ERROR | (HEADER, RISK_SCORE_PER_HOST?,
HOST_LIST?, GLOSSARY?, NON_RUNNING_KERNELS?, APPENDICES?))>

...

<!ELEMENT VULN_INFO_LIST (VULN_INFO+)>

<!ELEMENT VULN_INFO (QID, TYPE, PORT?, SERVICE?, FQDN?, PROTOCOL?, SSL?,
INSTANCE?, RESULT?, FIRST_FOUND?, LAST_FOUND?, TIMES_FOUND?,
VULN_STATUS?, LAST_FIXED?, FIRST_REOPENED?, LAST_REOPENED?,
TIMES_REOPENED?, CVSS_FINAL?, CVSS3_FINAL?, CVSS3_VERSION?,
TICKET_NUMBER?, TICKET_STATE?, ASSET_CVE?, QDS?)>

...
```

```
<!-- GLOSSARY -->

<!ELEMENT GLOSSARY (VULN_DETAILS_LIST)>

<!ELEMENT VULN_DETAILS_LIST (VULN_DETAILS+)>

<!ELEMENT VULN_DETAILS (QID, TITLE, SEVERITY, CATEGORY,
CUSTOMIZED?, THREAT, THREAT_COMMENT?, IMPACT, IMPACT_COMMENT?,
SOLUTION, SOLUTION_COMMENT?, COMPLIANCE?, CORRELATION?, PCI_FLAG,
LAST_UPDATE?, CVSS_SCORE?, CVSS3_SCORE?, VENDOR_REFERENCE_LIST?,
CVE_ID_LIST?, BUGTRAQ_ID_LIST?)>

...

<!ELEMENT CVSS_SCORE (CVSS_BASE?, CVSS_TEMPORAL?)>
<!ELEMENT CVSS_BASE (#PCDATA)>
<!ATTLIST CVSS_BASE
    source CDATA #IMPLIED
>
<!ELEMENT CVSS_TEMPORAL (#PCDATA)>
<!ELEMENT CVSS3_SCORE (CVSS3_BASE?, CVSS3_TEMPORAL?, CVSS3_VERSION?)>
<!ELEMENT CVSS3_BASE (#PCDATA)>
<!ELEMENT CVSS3_TEMPORAL (#PCDATA)>
<!ELEMENT CVSS3_VERSION (#PCDATA)>
...
```

Sample Host-Based Scan Report in CSV Format

This sample shows a Scan Report with Host-Based Findings in CSV format. Note the renamed column headings with CVSS3.1.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=fetch&id=1234567&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

CSV output:

```
"MyScanReport","06/22/2022 at 09:11:40 (GMT+0530)"
"Qualys,Inc.","919 E Hillsdale Blvd, 4th floor",,"Foster
City","California","United States of America","94404"
"Joe User","joe_user","Scanner"

...

"IP","Network","DNS","NetBIOS","QG Host ID","IP Interfaces","Tracking
Method","OS","IP Status","QID","Title","Vuln
Status","Type","Severity","Port","Protocol","FQDN","SSL","First
```

```
Detected","Last Detected","Times Detected","Date Last Fixed","First
Reopened","Last Reopened","Times Reopened","CVE ID","Vendor
Reference","Bugtraq ID","CVSS","CVSS Base","CVSS Temporal","CVSS
Environment","CVSS3.1","CVSS3.1 Base","CVSS3.1
Temporal","Threat","Impact","Solution","Exploitability","Associated
Malware","Results","PCI Vuln","Ticket
State","Instance","Category","Associated AGs","Non-running Kernel","Cloud
Provider","Cloud Provider Service","Cloud Service","Cloud Resource
ID","Cloud Resource Type","Cloud Account","Cloud Image ID","Cloud Resource
Metadata","EC2 Instance ID","Public Hostname","Image ID","VPC
ID","Instance State","Private Hostname","Instance Type","Account
ID","Region Code","Subnet ID","Host ID","Asset ID"

"10.20.30.40","network_Scanner",,,,,"IP",,"host scanned, found
vuln","86728","Web Server Uses Plain-Text Form Based
Authentication","Active","Vuln","3","8080","tcp",,,"06/04/2022
14:17:42","06/07/2022 10:58:02","3",,,,,,,,"3.9","4.3
(AV:N/AC:M/Au:N/C:P/I:N/A:N)","3.9 (E:F/RL:W/RC:C)","Asset Group: -,
Collateral Damage Potential:  -, Target Distribution: -, Confidentiality
Requirement: -, Integrity Requirement: -, Availability Requirement: -
","5","5.3 (AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N)","5.0
(E:F/RL:W/RC:C)","The Web server uses plain-text form based
authentication...
...
```

Sample Patch Report in XML Format

This sample shows a Patch Report in XML format. You'll see the new <CVSS3_VERSION> tag in the output.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=fetch&id=1234567&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE PATCH_REPORT SYSTEM
"https://qualysapi.qualys.com/patch_report.dtd">
<PATCH_REPORT>
  <HEADER>
    <NAME><![CDATA[Patch_Report_CVSSv3.1]]></NAME>
    <GENERATION_DATETIME>2022-06-22T07:11:31Z</GENERATION_DATETIME>
    <COMPANY_INFO>
      <NAME><![CDATA[Qualys, Inc.]]></NAME>
      <ADDRESS><![CDATA[919 E Hillsdale Blvd, 4th floor]]></ADDRESS>
      <CITY><![CDATA[Foster City]]></CITY>
      <STATE><![CDATA[California]]></STATE>
```

```
      <COUNTRY><![CDATA[United States of America]]></COUNTRY>
      <ZIP_CODE><![CDATA[94404]]></ZIP_CODE>
    </COMPANY_INFO>
    <USER_INFO>
      <NAME><![CDATA[Joe User]]></NAME>
      <USERNAME>joe_user</USERNAME>
      <ROLE>Manager</ROLE>
    </USER_INFO>
  </HEADER>
  <SUMMARY>
    <REPORT_SUMMARY>
      <TITLE><![CDATA[Patch_Report_CVSSv3.1]]></TITLE>
      <ASSET_GROUPS><![CDATA[All]]></ASSET_GROUPS>
      <IPS>N/A</IPS>
      <ASSET_TAGS><![CDATA[N/A]]></ASSET_TAGS>
      <GROUP_BY><![CDATA[Host]]></GROUP_BY>
      <CREATED_ON>06/22/2022</CREATED_ON>
      <HOST_SCANNED_SINCE>05/23/2022</HOST_SCANNED_SINCE>
      <NETWORK><![CDATA[All]]></NETWORK>
    </REPORT_SUMMARY>
    <PATCH_SUMMARY>
      <TOTAL_PATCHES>140</TOTAL_PATCHES>
      <HOST_REQUIRING_PATCHES>18</HOST_REQUIRING_PATCHES>
      <VULN_ADDRESSED><![CDATA[141]]></VULN_ADDRESSED>
    </PATCH_SUMMARY>
  </SUMMARY>
  <PATCH_LIST_BY_HOST>
    <HOST_LIST>
      <HOST>
        <IP>10.20.30.40</IP>
        <DNS><![CDATA[]]></DNS>
        <NETBIOS><![CDATA[]]></NETBIOS>
        <OS><![CDATA[]]></OS>
        <PATCH_COUNT><![CDATA[12]]></PATCH_COUNT>
        <NETWORK><![CDATA[network1]]></NETWORK>
        <PATCH_LIST>
          <PATCH_INFO>
            <PATCH_QID>42382</PATCH_QID>
            <VENDOR_ID>OpenSSH Forced Command Information
Disclosure</VENDOR_ID>
            <SEVERITY>3</SEVERITY>
           <PATCH_TITLE><![CDATA[OpenSSH Commands Information Disclosure
Vulnerability]]></PATCH_TITLE>
            <VULN_COUNT>1</VULN_COUNT>
            <PATCH_PUBLISHED>01/26/2012 05:30:00</PATCH_PUBLISHED>
            <CVSS3_BASE_SCORE>0</CVSS3_BASE_SCORE>
            <CVSS3_VERSION>3.1</CVSS3_VERSION>
          </PATCH_INFO>
...
```

DTD update:

We updated the Patch Report DTD to include new elements (in bold).

DTD: <platform>/patch_report.dtd

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- QUALYS PATCH REPORT DTD -->
<!-- $Revision$ -->

<!ELEMENT PATCH_REPORT (ERROR | (HEADER, (SUMMARY | (REPORT_SUMMARY,
PATCH_SUMMARY)), PATCH_LIST_BY_HOST?, PATCH_LIST_BY_AG?,
PATCH_LIST_BY_OS?, PATCH_LIST_BY_QID?, NON_RUNNING_KERNELS?))>
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR number CDATA #IMPLIED>

...

<!ELEMENT PATCH_INFO (PATCH_QID?, VENDOR_ID?, SEVERITY?, PATCH_TITLE?,
VULN_COUNT?,  HOST_COUNT?, PATCH_PUBLISHED?,  CVSS_BASE_SCORE?,
CVSS3_BASE_SCORE?, CVSS3_VERSION?, NETWORK?, DETECTION_INFO?,
HOST_LIST?)>
    <!ELEMENT PATCH_QID (#PCDATA)>
    <!ELEMENT VENDOR_ID (#PCDATA)>
    <!ELEMENT SEVERITY (#PCDATA)>
    <!ELEMENT PATCH_TITLE (#PCDATA)>
    <!ELEMENT VULN_COUNT (#PCDATA)>
    <!ELEMENT HOST_COUNT (#PCDATA)>
    <!ELEMENT PATCH_PUBLISHED (#PCDATA)>
    <!ELEMENT CVSS_BASE_SCORE (#PCDATA)>
    <!ELEMENT CVSS3_BASE_SCORE (#PCDATA)>
    <!ELEMENT CVSS3_VERSION (#PCDATA)>
    <!ELEMENT DETECTION_INFO (DETECTION*)>

        <!ELEMENT DETECTION (VULN_QID?, VULN_SEVERITY?, VULN_TYPE?,
VULN_TITLE?, DETECTION_INSTANCE?, DETECTION_NORMALIZED_INSTANCE?,
DETECTION_DATE_LAST_FOUND?,CVSS_BASE_SCORE?, CVSS3_BASE_SCORE?,
CVSS3_VERSION?)>
            <!ELEMENT VULN_QID (#PCDATA)>
            <!ELEMENT VULN_SEVERITY (#PCDATA)>
            <!ELEMENT VULN_TYPE (#PCDATA)>
            <!ELEMENT VULN_TITLE (#PCDATA)>
            <!ELEMENT DETECTION_INSTANCE (#PCDATA)>
            <!ELEMENT DETECTION_NORMALIZED_INSTANCE (#PCDATA)>
            <!ELEMENT DETECTION_DATE_LAST_FOUND (#PCDATA)>

...
```

Sample Patch Report in CSV Format

This sample shows a Patch Report in CSV format. Note the renamed column heading CVSS3.1 Base score.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=fetch&id=1234567&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

CSV output:

```
"Patch_Report_CVSSv3.1","06/23/2022 at 09:15:18 (GMT+0530)"
"Qualys, Inc.","919 E Hillsdale Blvd, 4th floor",,"Foster
City","California","United States of America","94404"
"Joe User","joe_user","Manager"

Report Summary
Title, Asset Groups, IPs, Asset Tags, Group By, Created on, Includes hosts
scanned since, Network
"Patch_Report_CVSSv3.1","All",,,"Host","06/23/2022","05/24/2022","All"

Patch Summary
Total Patches, Hosts Requiring Patches, Total Vulnerabilities Addressed
"140","18","141"

...

Patches by Host
IP, QID, Vendor ID, Severity, Title, Vulnerability Count, Published,
CVSS3.1 Base score, Network
10.20.30.40,"13692","Jenkins Security Advisory 2020-01-29","3","Jenkins
Inbound TCP Agent Protocol/3 Authentication Bypass
Vulnerability","1","01/29/2020 05:30:00","8.6",network_UM
...
```

New API for VM Scan Summary

APIs affected	/api/2.0/fo/scan/vm/summary/
New or Updated API	New
DTD or XSD changes	New

This release introduces a new API endpoint for VM Scan Summary. This API can be used as an alternative to the previous VM Scan Summary API. It's easier to use, has more filter options and enhanced output content.

New API: /api/2.0/fo/scan/vm/summary/

Old API: /api/2.0/fo/scan/summary/

The VM Scan Summary API helps you to identify hosts that were scanned or not scanned and why. You can choose to get a scan summary for a particular scan by specifying the scan reference ID or for all scans launched since a certain date/time or within a date range.

This API will return details for all scans. Note, however, that the output will not include the <SCAN_RESULTS> block if the scan did not return results for some reason.

Permissions

Manager role is required.

Input Parameters

The following input parameters are supported.

Parameter	Description
action=list	(Required) The list action.
output_format=xml	(Optional) The only supported output format at this time is XML.
scan_reference={value}	(Optional) Specifies a unique scan reference ID. Use this option to include scan summary information for a single scan only. For VM scans, the scan reference has the format scan/987654321.98765.
	One of these parameters must be specified in the request: scan_datetime_since or scan_reference. You cannot specify scan_reference in the same request as scan_datetime_since and scan_datetime_until.

Parameter	Description
scan_datetime_since={value}	(Optional) Include scans started since a certain date. The date must be less than or equal to today's date. Specify the date in GMT timezone in RFC 3339 format: yyyy-mm-ddThh-mm-ssZ. Example: 2020-10-01T09:30:48Z
	One of these parameters must be specified in the request: scan_datetime_since or scan_reference. You cannot specify scan_datetime_since in the same request as scan_reference.
scan_datetime_until={value}	(Optional) Include scans started up to a certain date. The date must be more than or equal to scan_datetime_since, and less than or equal to today's date. Specify the date in GMT timezone in RFC 3339 format: yyyy-mm-ddThh-mm-ssZ. Example: 2020-10-01T09:30:48Z
	The parameter scan_datetime_until can only be specified when scan_datetime_since is also specified. You cannot specify scan_datetime_until in the same request as scan_reference.
include_scan_input={0|1}	(Optional) By default, scan input information is included in the XML output in the <SCAN_INPUT> block. Specify include_scan_input=0 if you don't want this entire block to appear in the output. Scan input information includes the scan title, user login (for user who launched the scan), whether or not the scan was scheduled, scan target, network, option profile, etc.
include_scan_details={0|1}	(Optional) By default, scan details are included in the XML output in the <SCAN_DETAILS> block. Specify include_scan_details=0 if you don't want this entire block to appear in the output. Scan details include the scan status, launch date/time, and scan duration.
include_hosts_summary={0|1}	(Optional) By default, hosts summary information is included in the XML output in the <HOSTS> block under <SCAN_RESULTS>. Specify include_hosts_summary=0 if you don't want the <HOSTS> block to appear in the output. The hosts summary shows the total number of hosts scanned, and lists the IP addresses, DNS hostnames and NetBIOS hostnames in the scan.

Parameter	Description
include_detections_summary={0|1}	(Optional) By default, detections summary information is included in the XML output in the <DETECTIONS> block under <SCAN_RESULTS>. Specify include_detections_summary=0 if you don't want the <DETECTIONS> block to appear in the output. The detections summary includes the total number of detections, and the number of detections by severity for confirmed, potential and information gathered.
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. See Host Summary Categories below for more information on each category. 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.

Host Summary Categories

The following host summary categories may be included in the scan summary output:

Scanned - The hosts were scanned successfully.

Excluded - The hosts were excluded. Hosts may be excluded on a per scan basis (by the user launching or scheduling the scan) or globally for all scans. Managers and Unit Managers have privileges to edit the global excluded hosts list for the subscription.

Cancelled - Hosts were not scanned because the scan was cancelled. Scans may be cancelled by a user, by an administrator or automatically by the service as specified in scheduled scan settings.

Unresolved - Hosts were scanned but they could not be reported because the NetBIOS or DNS hostname, whichever tracking method is specified for each host, could not be resolved.

Duplicate - The hosts were duplicated within a single segment/slice of the scan job. For example, two different hostnames resolving to the same IP with tracking by IP.

Not Vulnerable - Hosts were found to be not vulnerable during host discovery without having to run a full scan. This could happen for example if the list of QIDs to be scanned are limited to certain ports and those ports are found to be closed.

Dead - The hosts were not "alive" at the time of the scan, meaning that they did not respond to probes sent by the scanning engine, and the option to Scan Dead Hosts was not enabled.

Aborted - The scan was abruptly discontinued. This is a rare occurrence that may be caused for different reasons. For example, it's possible that a connection timed out or there were connection errors on a particular port or the scan time elapsed.

Blocked - Hosts were blocked from scanning for some reason. For example, user provided blacklisted IPs to scan and after the scan was launched it was blocked due to improper configuration.

Failed Slice Hosts - The scan failed for these hosts.

Exceeded Scan Duration - Applicable when the Maximum Scan Duration per Asset feature is enabled and a maximum scan duration is specified in the option profile used for the scan. This setting determines how long a scan can run on a single asset. The scan on these hosts exceeded the scan duration allowed so the scan on these hosts was aborted.

API Samples

Sample 1 - Get scan summary by scan reference

In this sample, the scan reference ID is included as part of the request.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"http://qualysapi.qualys.com/api/2.0/fo/scan/vm/summary/?action=list&incl
ude_scan_input=1&include_hosts_summary=1&output_format=xml&include_detect
ions_summary=1&scan_reference=scan/9876543210.12345"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCAN_SUMMARY_OUTPUT SYSTEM
"http://qualysapi.qualys.com/api/2.0/fo/scan/vm/summary/output.dtd">
<SCAN_SUMMARY_OUTPUT>
    <RESPONSE>
        <DATETIME>2020-09-15T09:09:36Z</DATETIME>
        <SCAN_SUMMARY_LIST>
            <SCAN_SUMMARY>
                <SCAN_REFERENCE>scan/9876543210.12345</SCAN_REFERENCE>
                <SCAN_INPUT>
                    <TITLE>CustomAgScan</TITLE>
                    <USER>
                        <USERNAME>qualys_joe</USERNAME>
                    </USER>
                    <SCHEDULED>0</SCHEDULED>
                    <SCAN_DATETIME>2020-04-01 06:55:55</SCAN_DATETIME>
                    <NETWORK>
```

```
                            <ID>63010</ID>
                            <NAME>Custom Network</NAME>
                        </NETWORK>
                        <OPTION_PROFILE>
                            <ID>86395</ID>
                            <NAME>Initial Options</NAME>
                        </OPTION_PROFILE>
                        <TARGETS>
                            <IP_LIST>
                                <COUNT>256</COUNT>
                                <IP_DATA>
                                    <RANGES>
                                        <RANGE>11.1.1.0-11.1.1.255</RANGE>
                                    </RANGES>
                                </IP_DATA>
                            </IP_LIST>
                            <DNS_LIST>
                                <COUNT>3</COUNT>
                                <DNS_DATA>

<DNS_CSV>sample2.com,sample3.com,sample1.com</DNS_CSV>
                                </DNS_DATA>
                            </DNS_LIST>
                            <NETBIOS_LIST>
                                <COUNT>3</COUNT>
                                <NETBIOS_DATA>

<NETBIOS_CSV>NB1.COM,NB3.COM,NB2.COM</NETBIOS_CSV>
                                </NETBIOS_DATA>
                            </NETBIOS_LIST>
                            <ASSET_GROUP_LIST>
                                <COUNT>1</COUNT>
                                <ASSET_GROUP_DATA>
                                    <ASSET_GROUP>
                                        <ID>206216</ID>
                                       <NAME>Custom Network Asset Group</NAME>
                                    </ASSET_GROUP>
                                </ASSET_GROUP_DATA>
                            </ASSET_GROUP_LIST>
                        </TARGETS>
                    </SCAN_INPUT>
                    <SCAN_DETAILS>
                        <STATUS>ERROR</STATUS>
                       <LAUNCH_DATETIME>2020-04-01 06:55:55</LAUNCH_DATETIME>
                        <DURATION>1261</DURATION>
                    </SCAN_DETAILS>
                    <SCAN_RESULTS>
                        <HOSTS>
                            <COUNT>262</COUNT>
```

```
                        <HOSTS_DATA>
                            <SCANNED>
                                 <IP_LIST>
                                    <COUNT>9</COUNT>
                                    <IP_DATA>
                                        <RANGES>
                                            <RANGE>43.56.78.111-
43.56.78.119</RANGE>
                                        </RANGES>
                                    </IP_DATA>
                                </IP_LIST>
                            </SCANNED>
                            <FAILED_SLICE_HOSTS>
                                <IPV4_LIST>
                                    <COUNT>8</COUNT>
                                    <IPV4_DATA>
                                        <IPV4_CSV>10.10.10.1,10.20.10.10-
10.20.10.13,10.10.10.3,10.20.10.7,10.10.10.8,10.20.10.11</IPV4_CSV>
                                    </IPV4_DATA>
                                </IPV4_LIST>
                                <IPV6_LIST>
                                    <COUNT>2</COUNT>
                                    <IPV6_DATA>

<IPV6_CSV>::ff01,::ff02,::ff02</IPV6_CSV>
                                    </IPV6_DATA>
                                </IPV6_LIST>
                                <DNS_LIST>
                                    <COUNT>4</COUNT>
                                    <DNS_DATA>
                                       <DNS_CSV>sample4.com, sample5.com,
sample6.com, sample7.com</DNS_CSV>
                                    </DNS_DATA>
                                </DNS_LIST>
                                <NETBIOS_LIST>
                                    <COUNT>4</COUNT>
                                    <NETBIOS_DATA>
                                        <NETBIOS_CSV>WIN2KB,
SATEELITE,WIN4KB, KRWSDG</NETBIOS_CSV>
                                    </NETBIOS_DATA>
                                </NETBIOS_LIST>
                            </FAILED_SLICE_HOSTS>
</HOSTS_DATA>
                    </HOSTS>
                    <DETECTIONS>
                        <IG>
                            <TOTAL_COUNT>7216</TOTAL_COUNT>
                            <COUNT_BY_SEVERITY>
                                <SEVERITY_1>4467</SEVERITY_1>
```

```
                                <SEVERITY_2>2232</SEVERITY_2>
                                <SEVERITY_3>517</SEVERITY_3>
                                <SEVERITY_4>0</SEVERITY_4>
                                <SEVERITY_5>0</SEVERITY_5>
                            </COUNT_BY_SEVERITY>
                        </IG>
                        <VULN>
                            <CONFIRMED>
                                <TOTAL_COUNT>8054</TOTAL_COUNT>
                                <COUNT_BY_SEVERITY>
                                    <SEVERITY_1>238</SEVERITY_1>
                                    <SEVERITY_2>985</SEVERITY_2>
                                    <SEVERITY_3>2124</SEVERITY_3>
                                    <SEVERITY_4>2546</SEVERITY_4>
                                    <SEVERITY_5>2161</SEVERITY_5>
                                </COUNT_BY_SEVERITY>
                            </CONFIRMED>
                            <POTENTIAL>
                                <TOTAL_COUNT>1497</TOTAL_COUNT>
                                <COUNT_BY_SEVERITY>
                                    <SEVERITY_1>17</SEVERITY_1>
                                    <SEVERITY_2>420</SEVERITY_2>
                                    <SEVERITY_3>579</SEVERITY_3>
                                    <SEVERITY_4>304</SEVERITY_4>
                                    <SEVERITY_5>177</SEVERITY_5>
                                </COUNT_BY_SEVERITY>
                            </POTENTIAL>
                        </VULN>
                    </DETECTIONS>
                </SCAN_RESULTS>
            </SCAN_SUMMARY>
        </SCAN_SUMMARY_LIST>
    </RESPONSE>
</SCAN_SUMMARY_OUTPUT>
```

Sample 2 - Get scan summary by scan date

In this sample, all scans within the date range will be returned.

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_datetime_since=2020-04-
06T02:30:00Z&scan_datetime_until=2020-04-06T02:30:00Z"
```

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>2020-09-22T05:02:40Z</DATETIME>
    <SCAN_SUMMARY_LIST>
      <SCAN_SUMMARY>
        <SCAN_REFERENCE>scan/1234567890.12345</SCAN_REFERENCE>
        <SCAN_INPUT>
          <TITLE>My-Scan</TITLE>
          <USER>
            <USERNAME>qualys_joe</USERNAME>
          </USER>
          <SCHEDULED>0</SCHEDULED>
          <SCAN_DATETIME>2020-04-06 07:17:45</SCAN_DATETIME>
          <NETWORK>
            <ID>0</ID>
            <NAME>Global Default Network</NAME>
          </NETWORK>
          <OPTION_PROFILE>
            <ID>2171</ID>
            <NAME>Initial Options</NAME>
          </OPTION_PROFILE>
          <TARGETS>
            <IP_LIST>
              <COUNT>3</COUNT>
              <IP_DATA>
                <RANGES>
                  <RANGE>10.10.30.10-10.10.30.12</RANGE>
                </RANGES>
              </IP_DATA>
            </IP_LIST>
          </TARGETS>
        </SCAN_INPUT>
        <SCAN_DETAILS>
          <STATUS>FINISHED</STATUS>
          <LAUNCH_DATETIME>2020-04-06 07:17:45</LAUNCH_DATETIME>
          <DURATION>21656</DURATION>
        </SCAN_DETAILS>
        <SCAN_RESULTS>
          <HOSTS>
            <COUNT>3</COUNT>
            <HOSTS_DATA>
              <SCANNED>
                <IP_LIST>
                  <COUNT>2</COUNT>
                  <IP_DATA>
                    <RANGES>
```

```
                        <RANGE>10.10.30.10-10.10.30.11</RANGE>
                      </RANGES>
                    </IP_DATA>
                  </IP_LIST>
                </SCANNED>
                <DEAD>
                  <IP_LIST>
                    <COUNT>1</COUNT>
                    <IP_DATA>
                      <IP_CSV>10.10.30.12</IP_CSV>
                    </IP_DATA>
                  </IP_LIST>
                </DEAD>
                <FAILED_SLICE_HOSTS>
                 <IPV4_LIST>
                   <COUNT>8</COUNT>
                   <IPV4_DATA>
                     <IPV4_CSV>10.10.10.1,10.20.10.10-
10.20.10.13,10.10.10.3,10.20.10.7,10.10.10.8,10.20.10.11</IPV4_CSV>
                   </IPV4_DATA>
                </IPV4_LIST>
                <IPV6_LIST>
                  <COUNT>2</COUNT>
                  <IPV6_DATA>
                  <IPV6_CSV>::ff01,::ff02,::ff02</IPV6_CSV>
                </IPV6_DATA>
                </IPV6_LIST>
                <DNS_LIST>
                  <COUNT>4</COUNT>
                <DNS_DATA>
                   <DNS_CSV>sample1.com, sample2.com, sample3.com,
sample4.com</DNS_CSV>
                </DNS_DATA>
                </DNS_LIST>
                <NETBIOS_LIST>
                  <COUNT>4</COUNT>
                <NETBIOS_DATA>
               <NETBIOS_CSV>SAMPLE1, SAMPLE2, SAMPLE3, SAMPLE4</NETBIOS_CSV>
                 </NETBIOS_DATA>
                 </NETBIOS_LIST>
                </FAILED_SLICE_HOSTS>
              </HOSTS_DATA>
            </HOSTS>
            <DETECTIONS>
              <IG>
                <TOTAL_COUNT>77</TOTAL_COUNT>
                <COUNT_BY_SEVERITY>
                  <SEVERITY_1>52</SEVERITY_1>
                  <SEVERITY_2>12</SEVERITY_2>
```

```
            <SEVERITY_3>5</SEVERITY_3>
            <SEVERITY_4>2</SEVERITY_4>
            <SEVERITY_5>6</SEVERITY_5>
          </COUNT_BY_SEVERITY>
        </IG>
        <VULN>
          <CONFIRMED>
            <TOTAL_COUNT>17</TOTAL_COUNT>
            <COUNT_BY_SEVERITY>
              <SEVERITY_1>0</SEVERITY_1>
              <SEVERITY_2>3</SEVERITY_2>
              <SEVERITY_3>10</SEVERITY_3>
              <SEVERITY_4>0</SEVERITY_4>
              <SEVERITY_5>4</SEVERITY_5>
            </COUNT_BY_SEVERITY>
          </CONFIRMED>
          <POTENTIAL>
            <TOTAL_COUNT>18</TOTAL_COUNT>
            <COUNT_BY_SEVERITY>
              <SEVERITY_1>2</SEVERITY_1>
              <SEVERITY_2>4</SEVERITY_2>
              <SEVERITY_3>10</SEVERITY_3>
              <SEVERITY_4>1</SEVERITY_4>
              <SEVERITY_5>1</SEVERITY_5>
            </COUNT_BY_SEVERITY>
          </POTENTIAL>
        </VULN>
      </DETECTIONS>
    </SCAN_RESULTS>
  </SCAN_SUMMARY>
...
```

Sample 3 - Filter list of categories in output

In this sample, only the Cancelled 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=cancelled"
```

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>2020-09-22T05:07:05Z</DATETIME>
  <SCAN_SUMMARY_LIST>
    <SCAN_SUMMARY>
      <SCAN_REFERENCE>scan/1234567890.12345</SCAN_REFERENCE>
      <SCAN_INPUT>
        <TITLE>My-Scan-2</TITLE>
        <USER>
          <USERNAME>qualys_joe</USERNAME>
        </USER>
        <SCHEDULED>0</SCHEDULED>
        <SCAN_DATETIME>2020-08-06 03:52:30</SCAN_DATETIME>
        <NETWORK>
          <ID>1000</ID>
          <NAME>My-Custom-Network</NAME>
        </NETWORK>
        <OPTION_PROFILE>
          <ID>2134</ID>
          <NAME>Initial Options</NAME>
        </OPTION_PROFILE>
        <TARGETS>
        </TARGETS>
      </SCAN_INPUT>
      <SCAN_DETAILS>
        <STATUS>CANCELED</STATUS>
        <LAUNCH_DATETIME>2020-08-06 03:52:30</LAUNCH_DATETIME>
        <DURATION>10</DURATION>
      </SCAN_DETAILS>
      <SCAN_RESULTS>
        <HOSTS>
          <COUNT>4</COUNT>
          <HOSTS_DATA>
            <CANCELLED>
              <IP_LIST>
                <COUNT>2</COUNT>
                <IP_DATA>
                  <IP_CSV>10.10.25.232, 10.10.25.240</IP_CSV>
                </IP_DATA>
              </IP_LIST>
              <DNS_LIST>
                <COUNT>2</COUNT>
                <DNS_DATA>
                  <DNS_CSV>dns1.qualys.com,dns2.qualys.com</DNS_CSV>
                </DNS_DATA>
              </DNS_LIST>
            </CANCELLED>
          </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>
</SCAN_SUMMARY_OUTPUT>
```

New DTD

The new VM Scan Summary API uses the following DTD.

DTD: <platform API server>/api/2.0/fo/scan/vm/summary/output.dtd

```
<!-- QUALYS VM SCAN_SUMMARY_OUTPUT.DTD -->
<!-- $Revision$ -->
<!ELEMENT SCAN_SUMMARY_OUTPUT (REQUEST?,RESPONSE)>

<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, SCAN_SUMMARY_LIST?)>
<!ELEMENT SCAN_SUMMARY_LIST (SCAN_SUMMARY+)>
<!ELEMENT SCAN_SUMMARY (SCAN_REFERENCE,
SCAN_INPUT?,SCAN_DETAILS?,SCAN_RESULTS? )>
<!ELEMENT SCAN_REFERENCE (#PCDATA)>
<!ELEMENT SCAN_INPUT
(TITLE?,USER?,SCHEDULED?,SCAN_DATETIME?,SCAN_TYPE?,NETWORK?,OPTION_PROFIL
E?,TARGETS?)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USER (USERNAME)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT SCHEDULED (#PCDATA)>
<!ELEMENT SCAN_DATETIME (#PCDATA)>
<!ELEMENT SCAN_TYPE (#PCDATA)>
<!ELEMENT NETWORK (ID,NAME)>
<!ELEMENT OPTION_PROFILE (ID,NAME)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT TARGETS (IP_LIST?, DNS_LIST?, NETBIOS_LIST?, INSTANCE_ID_LIST?,
ASSET_GROUP_LIST?, ASSET_TAG_LIST?, EXCLUDED_IP_LIST?)>
<!ELEMENT IP_LIST (COUNT, IP_DATA?)>
<!ELEMENT EXCLUDED_IP_LIST (COUNT, IP_DATA?)>
<!ELEMENT IP_DATA (RANGES?, IP_CSV?)>
<!ELEMENT COUNT (#PCDATA)>
<!ELEMENT RANGES (RANGE+)>
<!ELEMENT RANGE (#PCDATA)>
<!ELEMENT IP_CSV (#PCDATA)>
<!ELEMENT DNS_LIST (COUNT, DNS_DATA)>
```

```
<!ELEMENT DNS_DATA (DNS_CSV)>
<!ELEMENT DNS_CSV (#PCDATA)>
<!ELEMENT NETBIOS_LIST (COUNT, NETBIOS_DATA)>
<!ELEMENT NETBIOS_DATA (NETBIOS_CSV)>
<!ELEMENT NETBIOS_CSV (#PCDATA)>
<!ELEMENT INSTANCE_ID_LIST (COUNT, INSTANCE_ID_DATA)>
<!ELEMENT INSTANCE_ID_DATA (INSTANCE_ID_CSV)>
<!ELEMENT INSTANCE_ID_CSV (#PCDATA)>
<!ELEMENT ASSET_GROUP_LIST (COUNT, ASSET_GROUP_DATA)>
<!ELEMENT ASSET_GROUP_DATA (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP (ID, NAME)>
<!ELEMENT ASSET_TAG_LIST (INCLUDE_TAG_LIST?, EXCLUDE_TAG_LIST?)>
<!ELEMENT INCLUDE_TAG_LIST (COUNT, INCLUDE_TAG_DATA)>
<!ELEMENT INCLUDE_TAG_DATA (ASSET_TAG+)>
<!ELEMENT ASSET_TAG (ID, NAME)>
<!ELEMENT EXCLUDE_TAG_LIST (COUNT, EXCLUDE_TAG_DATA)>
<!ELEMENT EXCLUDE_TAG_DATA (ASSET_TAG+)>
<!ELEMENT SCAN_DETAILS (STATUS,LAUNCH_DATETIME,DURATION?)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT LAUNCH_DATETIME (#PCDATA)>
<!ELEMENT DURATION (#PCDATA)>
<!ELEMENT SCAN_RESULTS (HOSTS?,DETECTIONS?)>
<!ELEMENT HOSTS (COUNT?,HOSTS_DATA)>
<!ELEMENT HOSTS_DATA
(SCANNED?,NOT_VULNERABLE?,CANCELLED?,DEAD?,EXCLUDED?,UNRESOLVED?,DUPLICAT
E?,BLOCKED?,ABORTED?, FAILED_SLICE_HOSTS?, EXCEEDED_SCAN_DURATION?)>
<!ELEMENT SCANNED (IP_LIST?, DNS_LIST?, NETBIOS_LIST?,INSTANCE_ID_LIST?)>
<!ELEMENT NOT_VULNERABLE (IP_LIST?, DNS_LIST?,
NETBIOS_LIST?,INSTANCE_ID_LIST?)>
<!ELEMENT CANCELLED (IP_LIST?, DNS_LIST?,
NETBIOS_LIST?,INSTANCE_ID_LIST?)>
<!ELEMENT DEAD (IP_LIST?, DNS_LIST?, NETBIOS_LIST?,INSTANCE_ID_LIST?)>
<!ELEMENT EXCLUDED (IP_LIST?, DNS_LIST?,
NETBIOS_LIST?,INSTANCE_ID_LIST?)>
<!ELEMENT UNRESOLVED (IP_LIST?, DNS_LIST?,
NETBIOS_LIST?,INSTANCE_ID_LIST?)>
<!ELEMENT DUPLICATE (IP_LIST?, DNS_LIST?,
NETBIOS_LIST?,INSTANCE_ID_LIST?)>
<!ELEMENT BLOCKED (IP_LIST?, DNS_LIST?, NETBIOS_LIST?,INSTANCE_ID_LIST?)>
<!ELEMENT ABORTED (IP_LIST?, DNS_LIST?, NETBIOS_LIST?,INSTANCE_ID_LIST?)>
<!ELEMENT FAILED_SLICE_HOSTS (IPV4_LIST?, IPV6_LIST?, DNS_LIST?,
NETBIOS_LIST?, INSTANCE_ID_LIST?)>
<!ELEMENT EXCEEDED_SCAN_DURATION (IPV4_LIST?, IPV6_LIST?, DNS_LIST?,
NETBIOS_LIST?, INSTANCE_ID_LIST?)>
<!ELEMENT IPV4_LIST (COUNT, IPV4_DATA)>
<!ELEMENT IPV4_DATA (IPV4_CSV)>
<!ELEMENT IPV4_CSV (#PCDATA)>
<!ELEMENT IPV6_LIST (COUNT, IPV6_DATA)>
<!ELEMENT IPV6_DATA (IPV6_CSV)>
```

```
<!ELEMENT IPV6_CSV (#PCDATA)>
<!ELEMENT DETECTIONS (IG?,VULN?)>
<!ELEMENT IG (TOTAL_COUNT,COUNT_BY_SEVERITY)>
<!ELEMENT VULN (CONFIRMED,POTENTIAL)>
<!ELEMENT CONFIRMED (TOTAL_COUNT,COUNT_BY_SEVERITY)>
<!ELEMENT POTENTIAL (TOTAL_COUNT,COUNT_BY_SEVERITY)>
<!ELEMENT TOTAL_COUNT (#PCDATA)>
<!ELEMENT COUNT_BY_SEVERITY
(SEVERITY_1,SEVERITY_2,SEVERITY_3,SEVERITY_4,SEVERITY_5)>
<!ELEMENT SEVERITY_1 (#PCDATA)>
<!ELEMENT SEVERITY_2 (#PCDATA)>
<!ELEMENT SEVERITY_3 (#PCDATA)>
<!ELEMENT SEVERITY_4 (#PCDATA)>
<!ELEMENT SEVERITY_5 (#PCDATA)>
<!-- EOF -->
```

MongoDB Authentication: Certificates/Private Keys Now Supported With Basic and Vault Login

APIs affected	/api/2.0/fo/auth/mongodb
New or Updated API	Updated
DTD or XSD changes	Yes

Until now, MongoDB authentication record only supported one of the 3 authentication/login types:

- Basic - This username/password based.
- Vault - Username and Vault integration used for storing login credentials.
- Private Key/Cert based.

With this new implementation, customer can now use Private Keys/Certificates along with Basic & Vault based login. A new "Require Cert",tag is added for Basic and Vault based login. This option by default will be set to "0". If set to "1", user will be able to add certs/pks as well with login type Basic | vault.

"Require Cert" is shown for both Local & LDAP credential type, for both Basic and Vault based login types.The current login type = PK/Cert works as before. Both VM and PC scans will support of "Require Cert" for Basic and Vault based login in MongoDB auth record.

Input Parameters

Use the following input parameter to show require certificate information in the API output. Refer to the Qualys API (VM,PC) User Guide for details on all input parameters.

Parameter	Description
require_cert={**0**|1}	(Optional) Specify 1 to login with certificates/private keys along with login type Basic | vault. By default value will be 0 When require_cert=1, certificate is also required in the same API request.

Sample mongoDB auth List API

This sample shows the output for MongoDB auth List API. You will see the new <REQUIRE_CERT> tag in the output.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=list&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/" > file.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MONGODB_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/auth_mongodb_list_o
utput.dtd">
<AUTH_MONGODB_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2022-06-24T09:34:29Z</DATETIME>
        <AUTH_MONGODB_LIST>
            <AUTH_MONGODB>
                <ID>6297787</ID>
                <TITLE>
                    <![CDATA[Mongo_Cert]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[joe_user]]>
                </USERNAME>
                <CREDENTIAL_TYPE>
                    <![CDATA[local]]>
                </CREDENTIAL_TYPE>
                <DATABASE>
                    <![CDATA[admin]]>
                </DATABASE>
                <PORT>27017</PORT>
                <UNIX_CONFIGURATION_FILE>
                    <![CDATA[/etc/mongod2.conf]]>
                </UNIX_CONFIGURATION_FILE>
                <SSL_VERIFY>
                    <![CDATA[1]]>
                </SSL_VERIFY>
                <HOSTS>
                    <HOST>
                        <![CDATA[mlcent76mdb34.s2012r2.qualys.com]]>
                    </HOST>
                </HOSTS>
                <IP_SET>
                    <IP>10.20.30.40</IP>
                </IP_SET>
```

```
                <LOGIN_TYPE>
                    <![CDATA[basic]]>
                </LOGIN_TYPE>
                <REQUIRE_CERT>
                    <![CDATA[1]]>
                </REQUIRE_CERT>
                <PRIVATE_KEY_CERTIFICATE_LIST>
                    <PRIVATE_KEY_CERTIFICATE>
                        <ID>3326771</ID>
                        <PRIVATE_KEY_INFO type="basic">
                            <PRIVATE_KEY />
                        </PRIVATE_KEY_INFO>
                        <PASSPHRASE_INFO type="basic" />
                    </PRIVATE_KEY_CERTIFICATE>
                </PRIVATE_KEY_CERTIFICATE_LIST>
                <NETWORK_ID>0</NETWORK_ID>
                <CREATED>
                    <DATETIME>2022-06-23T05:15:45Z</DATETIME>
                    <BY>scan_at</BY>
                </CREATED>
                <LAST_MODIFIED>
                    <DATETIME>2022-06-24T09:34:19Z</DATETIME>
                </LAST_MODIFIED>
            </AUTH_MONGODB>
        </AUTH_MONGODB_LIST>
        ...
```

DTD update:

We updated the DTD for List API Output to include new element (in bold).

```
<!-- QUALYS AUTH_MONGODB_LIST_OUTPUT DTD -->
<!ELEMENT AUTH_MONGODB_LIST_OUTPUT (REQUEST?, RESPONSE)>
<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!ELEMENT POST_DATA (#PCDATA)>
<!ELEMENT RESPONSE (DATETIME, (AUTH_MONGODB_LIST|ID_SET)?, WARNING_LIST?,
GLOSSARY?)>
<!ELEMENT AUTH_MONGODB_LIST (AUTH_MONGODB+)>
<!ELEMENT AUTH_MONGODB (ID, TITLE, USERNAME?, CREDENTIAL_TYPE?,
CLEARTEXT?, DATABASE, PORT, UNIX_CONFIGURATION_FILE, SSL_VERIFY?, HOSTS?,
IP_SET?, LOGIN_TYPE?, DIGITAL_VAULT?, REQUIRE_CERT?,
```

```
PRIVATE_KEY_CERTIFICATE_LIST?, NETWORK_ID?, CREATED, LAST_MODIFIED,
COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT CREDENTIAL_TYPE (#PCDATA)>
<!ELEMENT CLEARTEXT (#PCDATA)>

<!ELEMENT REQUIRE_CERT (#PCDATA)>

<!ELEMENT PRIVATE_KEY_CERTIFICATE_LIST (PRIVATE_KEY_CERTIFICATE)*>

<!ELEMENT PRIVATE_KEY_CERTIFICATE (ID, PRIVATE_KEY_INFO, PASSPHRASE_INFO,
CERTIFICATE?)+>
<!ELEMENT PRIVATE_KEY_INFO (PRIVATE_KEY|DIGITAL_VAULT)>
<!ATTLIST PRIVATE_KEY_INFO type (basic|vault) "basic">

<!-- Private key contents will never be rendered -->
<!ELEMENT PRIVATE_KEY EMPTY>
<!ELEMENT PASSPHRASE_INFO (DIGITAL_VAULT?)>
<!ATTLIST PASSPHRASE_INFO type (basic|vault) "basic">
<!-- Certificate contents will never be rendered -->
<!ELEMENT CERTIFICATE EMPTY>
...
```

Sample mongoDB auth Create API with Basic login type

This sample shows the output for MongoDB auth Create API with Basic login type and required cert set to 1(True).

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=create&title=mongo_auth_basic_cert&username=joe_user&password=abc
123&login_type=basic&ips=10.20.30.40&database_name=admin&port=27019&requi
re_cert=1&unix_conf_path=/etc/mongod2.conf&ssl_verify=1&hosts=mlcent76mdb
34.s2012r2.qualys.com'
--header 'X-Requested-With: qweb' \
--header 'Authorization: Basic YXdzX2FrOlF3ZWJANDYzMA==' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'certificate=-----BEGIN CERTIFICATE-----
MIIErDCCApSgAwIBAgIBIDANBgkqhkiG9w0BAQUFADCBljEbMBkGA1UEAwwSU2Nh
bm5lciBRQSBSb290IENBMRMwEQYDVQQIDApDYWxpZm9ybmlhMQswCQYDVQQGEwJV
UzEeMBwGCSqGSIb3DQEJARYPbWxxYUBxdWFseXMuY29tMRswGQYDVQQKDBJRdWFs
eXMgRW5naW5lZXJpbmcxGDAWBgNVBAsMD1NjYW5uZXIgUUEgVGVhbTAeFw0yMTA2
MTQyMTEwMDBaFw0yNDA2MTMyMTEwMDBaMIGMMR4wHAYDVQQDDBVtbGNlbnQ3Nm1k
YjM0X2NsaWVudDExEzARBgNVBAgMCkNhbGlmb3JuaWExCzAJBgNVBAYTAlVTMR4w
HAYJKoZIhvcNAQkBFg9tbHFhQHF1YWx5cy5jb20xFDASBgNVBAoMC1F1YWx5cyBJ
bmMuMRIwEAYDVQQLDAlNTFFBIFRlYW0wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
```

```
ggEKAoIBAQCxPNX+jExoBJqbftSbOeMYdWgCP8o8YR+aqjS6ZqroX9i8dfFCsVc3
5ePxBDOUr5p/DivhvMWsBZsZp2qpSOAjj2vKQV4M7VNvR7h9mjQRpruLOPrCFFup
WWy+zSCzRskiYWhRGd8V5XWvaJhNytneBLsUX6l+1SAwFC+eD/M2oA4VhipAK612
sKTn7yUjYBTODjox+dumKpFTdoPfjaCO923K2fcMNrLUVYQNbibxygsQK6qFJnVl
XJ1LCSVyTBJLuOWrgBATrvcMh9Wv5U0XFRp1u6t2pqnUqkzRsa5jtGR3GBfR3lUu
1JUyo4Kx1QrDw2I3vkYFA/dVv2dTEUgBAgMBAAGjDTALMAkGA1UdEwQCMAAwDQYJ
KoZIhvcNAQEFBQADggIBAL5MYQ8XinuSInZYQgywYFWlhZJJOSEqD4B4DqDfset4
v/7OjDCDWYH8DeObWcHuJgHh1vADpHIYDjfJCPnAPBKgIquVz9QaLUgtV+u1fJDe
Hpxr6IACaizlV0IId6JmoSR+MR2LPig0mi7Du4r07vqUWBB8za4ZxDVtQNkcPI/k
8/Sgj+kyr8hF4up8kniTMEaD/7eZ7MNmYR1BFygcZ/ieYRfdWVMlOvYDxVT20tCK
V7OzI12wXy/J37xdm8BaIkkoJyKPBwP396c4BlIrC5bDvBGRH89VhNscWryhPz9l
CrNvhegnqC0sxi7b4KOEMH3NtbETRZT8IhLkzHZTF+SqxUNkqjD1jdnM3cq0Ab3d
TdB5Ul7B3IjwgtnNES6pxHaX//ycRvGo9v2rzJO8TCtsd0o21uaLXwJmqJ5qhFPz
iX92jYZqEWm3wSD2XMI8kolr4txNfzH9zwAcEGdtBqUlTJcrdOU8IUn3pqISqZkr
wWpiBeS5eU/YbnkhSz2l6bX1x0qaQWv8h16YusvBMjfb2jBWHkED/osRFA7F5f11
XBNipcTrie1iIDY758iDbFrwWaza/9cg0awluyOa560rkyhZTWxwoZkvUz/rnVE7
2UaXkwPxhWAHx3jzfcQca8GTIEVbzuDkg+jcwCoaRNI3IG3339PQE/eF50yiE1YM
-----END CERTIFICATE-----' \
--data-urlencode 'private_key=-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAsTzV/oxMaASam37UmznjGHVoAj/KPGEfmqo0umaq6F/YvHXx
QrFXN+Xj8QQzlK+afw4r4bzFrAWbGadqqUjgI49rykFeDO1Tb0e4fZo0Eaa7izj6
whRbqVlsvs0gs0bJImFoURnfFeV1r2iYTcrZ3gS7FF+pftUgMBQvng/zNqAOFYYq
QCutdrCk5+8lI2AUzg46MfnbpiqRU3aD342gjvdtytn3DDay1FWEDW4m8coLECuq
hSZ1ZVydSwklckwSS7jlq4AQE673DIfVr+VNFxUadburdqap1KpM0bGuY7RkdxgX
0d5VLtSVMqOCsdUKw8NiN75GBQP3Vb9nUxFIAQIDAQABAoIBAQCKiPzTnKJUY9Td
WgOg2Vxyz8Jej7HqBBiJ8iSI1pscS17D4ISWFrwPyzeiOiB/RctDKLaQGdeAoFkd
ckjizT21TfN5AiMbg53Fy4+fTZsJeQP6zKzkarlC480mTnwS5W9t2imJyuke2l5k
nyL9G2O0MIpyYFvB8aDZM84MhHcc6CuRme3+VS9kFaIC7wNoEzUrGZt8CE1QDZh9
zKQsVLT5y7Hk+yiDLZ7BkgecFJ52J4xcYzIQhfrfIQp0UmCcKPslHrX3Xzens1GO
AyCkRIRfaI+NIwygrzVtwPTdKNOz+E4K5bmwwNUCdBjZi4DGPxZvobktD6FI7pjA
pHcWZL2BAoGBAOxAvhc5H/66MexOdBhtNRkueMHVWgeAnHYlcGvTjumRqbhipJIc
oVQHFcnFEXrP762dSo7QA2yg0SrhBD+U0iCkDKnzNQnDsXYftDSMNrhhEIznMUvX
JWn17yrXtROsq4oFpvSdJ33fZQHEy8K6aCOGRbAsWjAjAfb98acQHxe5AoGBAMAN
TisS8ZZShhEfKussVbcJYuIHqyVvA2TV3OetMt8tMiToNVOsRukV6Hnf9DFXOdBh
ddxFbGFJiaFDduzjjig8m53FCmmOtqnOxL5lxckx2ajxxGKfdKpSOG0OzDbxEKjF
uGX9VviOlpbt2JPuHF7qc850xf54z9QRu7OX+UaJAoGARKxFFScLv9WLsW7UnE0S
RDGX9G/57XhbApS7avxh7E7lEK3LvJUJ6AzvLmlUPWi3+LVh+MVKWYcdheNGgtzV
f5tv+u6xGheCPB3XGfcv6MR+NRb24160h2pvjPqKrh9g9YvTDgOoeRQ4nh0ARag9
oSXkl+MsjBWA+rSyS6eKAjECgYEAiRR2KPSaj8tTekEe50F75OvEMsV6eXulloG3
7X2IhBfEZOeBuLmM264Rg3xA1j8GOyB1ecXrt/0/SWXYKvm5bCrmgFQ2PGXrJ4U4
lRYbeKImVBpNLH/YTAHn2J/pT4X9eBm4psOPIlbUUeJu5hfdFDqQclqTQDGHVj1a
FrRw7tECgYBEuc85ghJunoV7hENuolP19+ppaiyH98q4Mc6vpkoEItuoKjWfH1Yr
98QtS58boBphSCNU4qL51dqnEAzCd0udYINxLawaosI3aaUOEGIUUa7IO7e7qUl8
Y4pb3owl0zwdpnyEgdSpuCW8N1Gnsiiur2fJ1NeAaHCF4cG3Se7bfw==
-----END RSA PRIVATE KEY-----'"
\"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/" > file.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2022-06-23T11:15:21Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>6298437</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample mongoDB auth Create API with Vault login type

This sample shows the output for MongoDB auth Create API with Vault login type and required cert set to 1(True).

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
“action=create&title=mongo_auth_test&username=joe_user&login_type=vault&i
ps=10.20.30.40&database_name=admin&port=27019&require_cert=1&unix_conf_pa
th=/etc/mongod2.conf&ssl_verify=1&hosts=mlcent76mdb34.s2012r2.qualys.com&
vault_type=Thycotic Secret Server&vault_id=4367212&secret_name=test' \
--header 'X-Requested-With: qweb' \
--header 'Authorization: Basic c2Nhbl9hdDpRYXRlbXAxMjMj' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'certificate=-----BEGIN CERTIFICATE-----
MIIErDCCApSgAwIBAgIBIDANBgkqhkiG9w0BAQUFADCBljEbMBkGA1UEAwwSU2Nh
bm5lciBRQSBSb290IENBMRMwEQYDVQQIDApDYWxpZm9ybmlhMQswCQYDVQQGEwJV
UzEeMBwGCSqGSIb3DQEJARYPbWxxYUBxdWFseXMuY29tMRswGQYDVQQKDBJRdWFs
eXMgRW5naW5lZXJpbmcxGDAWBgNVBAsMD1NjYW5uZXIgUUEgVGVhbTAeFw0yMTA2
MTQyMTEwMDBaFw0yNDA2MTMyMTEwMDBaMIGMMR4wHAYDVQQDDBVtbGNlbnQ3Nm1k
YjM0X2NsaWVudDExEzARBgNVBAgMCkNhbGlmb3JuaWExCzAJBgNVBAYTAlVTMR4w
HAYJKoZIhvcNAQkBFg9tbHFhQHF1YWx5cy5jb20xFDASBgNVBAoMC1F1YWx5cyBJ
bmMuMRIwEAYDVQQLDAlNTFFBIFRlYW0wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQCxPNX+jExoBJqbftSbOeMYdWgCP8o8YR+aqjS6ZqroX9i8dfFCsVc3
5ePxBDOUr5p/DivhvMWsBZsZp2qpSOAjj2vKQV4M7VNvR7h9mjQRpruLOPrCFFup
WWy+zSCzRskiYWhRGd8V5XWvaJhNytneBLsUX6l+1SAwFC+eD/M2oA4VhipAK612
sKTn7yUjYBTODjox+dumKpFTdoPfjaCO923K2fcMNrLUVYQNbibxygsQK6qFJnVl
XJ1LCSVyTBJLuOWrgBATrvcMh9Wv5U0XFRp1u6t2pqnUqkzRsa5jtGR3GBfR3lUu
1JUyo4Kx1QrDw2I3vkYFA/dVv2dTEUgBAgMBAAGjDTALMAkGA1UdEwQCMAAwDQYJ
KoZIhvcNAQEFBQADggIBAL5MYQ8XinuSInZYQgywYFWlhZJJOSEqD4B4DqDfset4
```

```
v/7OjDCDWYH8DeObWcHuJgHh1vADpHIYDjfJCPnAPBKgIquVz9QaLUgtV+u1fJDe
Hpxr6IACaizlV0IId6JmoSR+MR2LPig0mi7Du4r07vqUWBB8za4ZxDVtQNkcPI/k
8/Sgj+kyr8hF4up8kniTMEaD/7eZ7MNmYR1BFygcZ/ieYRfdWVMlOvYDxVT20tCK
V7OzI12wXy/J37xdm8BaIkkoJyKPBwP396c4BlIrC5bDvBGRH89VhNscWryhPz9l
CrNvhegnqC0sxi7b4KOEMH3NtbETRZT8IhLkzHZTF+SqxUNkqjD1jdnM3cq0Ab3d
TdB5Ul7B3IjwgtnNES6pxHaX//ycRvGo9v2rzJO8TCtsd0o21uaLXwJmqJ5qhFPz
iX92jYZqEWm3wSD2XMI8kolr4txNfzH9zwAcEGdtBqUlTJcrdOU8IUn3pqISqZkr
wWpiBeS5eU/YbnkhSz2l6bX1x0qaQWv8h16YusvBMjfb2jBWHkED/osRFA7F5f11
XBNipcTrie1iIDY758iDbFrwWaza/9cg0awluyOa560rkyhZTWxwoZkvUz/rnVE7
2UaXkwPxhWAHx3jzfcQca8GTIEVbzuDkg+jcwCoaRNI3IG3339PQE/eF50yiE1YM
-----END CERTIFICATE-----' \
--data-urlencode 'private_key=-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAsTzV/oxMaASam37UmznjGHVoAj/KPGEfmqo0umaq6F/YvHXx
QrFXN+Xj8QQzlK+afw4r4bzFrAWbGadqqUjgI49rykFeDO1Tb0e4fZo0Eaa7izj6
whRbqVlsvs0gs0bJImFoURnfFeV1r2iYTcrZ3gS7FF+pftUgMBQvng/zNqAOFYYq
QCutdrCk5+8lI2AUzg46MfnbpiqRU3aD342gjvdtytn3DDay1FWEDW4m8coLECuq
hSZ1ZVydSwklckwSS7jlq4AQE673DIfVr+VNFxUadburdqap1KpM0bGuY7RkdxgX
0d5VLtSVMqOCsdUKw8NiN75GBQP3Vb9nUxFIAQIDAQABAoIBAQCKiPzTnKJUY9Td
WgOg2Vxyz8Jej7HqBBiJ8iSI1pscS17D4ISWFrwPyzeiOiB/RctDKLaQGdeAoFkd
ckjizT21TfN5AiMbg53Fy4+fTZsJeQP6zKzkarlC480mTnwS5W9t2imJyuke2l5k
nyL9G2O0MIpyYFvB8aDZM84MhHcc6CuRme3+VS9kFaIC7wNoEzUrGZt8CE1QDZh9
zKQsVLT5y7Hk+yiDLZ7BkgecFJ52J4xcYzIQhfrfIQp0UmCcKPslHrX3Xzens1GO
AyCkRIRfaI+NIwygrzVtwPTdKNOz+E4K5bmwwNUCdBjZi4DGPxZvobktD6FI7pjA
pHcWZL2BAoGBAOxAvhc5H/66MexOdBhtNRkueMHVWgeAnHYlcGvTjumRqbhipJIc
oVQHFcnFEXrP762dSo7QA2yg0SrhBD+U0iCkDKnzNQnDsXYftDSMNrhhEIznMUvX
JWn17yrXtROsq4oFpvSdJ33fZQHEy8K6aCOGRbAsWjAjAfb98acQHxe5AoGBAMAN
TisS8ZZShhEfKussVbcJYuIHqyVvA2TV3OetMt8tMiToNVOsRukV6Hnf9DFXOdBh
ddxFbGFJiaFDduzjjig8m53FCmmOtqnOxL5lxckx2ajxxGKfdKpSOG0OzDbxEKjF
uGX9VviOlpbt2JPuHF7qc850xf54z9QRu7OX+UaJAoGARKxFFScLv9WLsW7UnE0S
RDGX9G/57XhbApS7avxh7E7lEK3LvJUJ6AzvLmlUPWi3+LVh+MVKWYcdheNGgtzV
f5tv+u6xGheCPB3XGfcv6MR+NRb24160h2pvjPqKrh9g9YvTDgOoeRQ4nh0ARag9
oSXkl+MsjBWA+rSyS6eKAjECgYEAiRR2KPSaj8tTekEe50F75OvEMsV6eXulloG3
7X2IhBfEZOeBuLmM264Rg3xA1j8GOyB1ecXrt/0/SWXYKvm5bCrmgFQ2PGXrJ4U4
lRYbeKImVBpNLH/YTAHn2J/pT4X9eBm4psOPIlbUUeJu5hfdFDqQclqTQDGHVj1a
FrRw7tECgYBEuc85ghJunoV7hENuolP19+ppaiyH98q4Mc6vpkoEItuoKjWfH1Yr
98QtS58boBphSCNU4qL51dqnEAzCd0udYINxLawaosI3aaUOEGIUUa7IO7e7qUl8
Y4pb3owl0zwdpnyEgdSpuCW8N1Gnsiiur2fJ1NeAaHCF4cG3Se7bfw==
-----END RSA PRIVATE KEY-----'"
\"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/" > file.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
<RESPONSE>
<DATETIME>2022-06-24T09:45:36Z</DATETIME>
<BATCH_LIST>
```

```
<BATCH>
<TEXT>Successfully Created</TEXT>
<ID_SET>
<ID>6303169</ID>
</ID_SET>
</BATCH>
</BATCH_LIST>
</RESPONSE>
</BATCH_RETURN>
```

Sample mongoDB auth Update API with Vault login type

This sample shows the output for MongoDB auth Update API with Vault login type and required cert set to 1(True).

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=update&ids=6297980&username=joe_user&login_type=vault&require_cer
t=1&vault_type=Quest Vault&vault_id=47017&system_name=abc' \
--header 'X-Requested-With: qweb' \
--header 'Authorization: Basic c2Nhbl9hdDpRYXRlbXAxMjMj' \
--form 'certificate="-----BEGIN CERTIFICATE-----
MIIByjCCAXSgAwIBAgIQBjdsAKoAZIoRz7jUqlw19DANBgkqhkiG9w0BAQQFADAW
MRQwEgYDVQQDEwtSb290IEFnZW5jeTAeFw05NjA1MjgyMjAyNTlaFw0zOTEyMzEy
MzU5NTlaMBYxFDASBgNVBAMTC1Jvb3QgQWdlbmN5MFswDQYJKoZIhvcNAQEBBQAD
SgAwRwJAgVUiuYqkb+3W59lmD1W8183VvE5AAiGisfeHMIVe0vJEudybdbb7Rl9C
tp0jNgveVA/NvR+ZKhBYEctAy7WnQQIDAQABo4GeMIGbMFAGA1UEAwRJE0dGb3Ig
VGVzdGluZyBQdXJwb3NlcyBPbmx5IFNhbXBsZSBTb2Z0d2FyZSBQdWJsaXNoaW5n
IENyZWRlbnRpYWxzIEFnZW5jeTBHBgNVHQEEQDA+gBAS5AktBh0dTwCNYSHcFmRj
oRgwFjEUMBIGA1UEAxMLUm9vdCBBZ2VuY3mCEAY3bACqAGSKEc+41KpcNfQwDQYJ
KoZIhvcNAQEEBQADQQAtLj57iUKJP6ghF/rw9cOV22JpW8ncwbP68MRvb2Savecb
JWhyg2e9VrCNAb0q98xLvYeluocgTEIRQa0QFzuM
-----END CERTIFICATE-----"' \
--form 'private_key="-----BEGIN RSA PRIVATE KEY-----
MIICWgIBAAKBgGqDhjebTQt8qJhoNRrrd7Ll9miq/4o2+BhiL6Bta/682TH336kL
JXc0G1vDN3tCCP71IOlSdh//MV3SvIkQKERUm2jGECHfbr+NV05YSUx0deidEe/d
JghQFOHczRT9o8pAACw6tAItVw5hmI5rYttzS1IT5bZGFaC/pwmLjElvAgMBAAEC
gYAME1k2GK9FbB6ZGMdcg/GQIK4s86YA/3ZlHUyU/ZLO0I43MgjzW0YmG4w2fQ1f
Nf9bGGNg0G5/9iicoHWrfF90Kkjj0jg6R0Z0v9ugTF7wldGj4k8EnXaNybqAaWiX
ZvL2OF50wo7bI2mxx+S32bm2ZBtoICEfltnQ9Bexcac78QJBAKfkwBSx4e42wT9X
4UisQlodohxQHSgOE97tsNkveasTIEw2+juHCtSdyet3APfYjYq2a0XkhZoowLch
anUVnhMCQQCiaNsqX0QpsxDC/mMRtPy1ULSfZBLqLsowyAWsRbgBPSx9lQ+BxeM3
NG/jiuyrX0zzM2Lbvlt3KS2PWzBfRyK1AkB/fw7+qDbSF3KZD7tc3LNmi6pXpd7+
U/JzED2EMLFMYLHeLsHIAr0OyORVk4GAtUqHVBASe3+Zmej/KLkXQNtRAkAYlej/
nBZUfa/+5MWYi55p0ELXki2u19Bx3AXH03IMdfdDN4p2ab+AvuZlOsWjF7UtZ80C
WOm9uzUTa4mCEuG1AkAN/UEobJ0BQSTuiqIEj46wwNOa9zTt3s80as4xPlEiiteL
YvYA515ZegEw2xSBxI2RoRSWg0nWaNanRo+ugLkL
-----END RSA PRIVATE KEY-----"'
```

```
\"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/" > file.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2022-06-24T09:40:07Z</DATETIME>

        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>6297787</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Authentication Support for new technology: Infoblox devices

API affected	/api/2.0/fo/auth/infoblox
New or Updated API	New
DTD or XSD changes	New

With this new technology support, customer can now create Infoblox authentication records.

Infoblox authentication records are available for the PC/SCA module.

Input Parameters

Use the following input parameter to create Infoblox authentication records in the API output. Refer to the Qualys API (VM,PC) User Guide for details on all input parameters.

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
ids={value}	(Required to edit or delete record) Record IDs to edit/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
ips={value}	(Required to create record) The IP address(es) for the Infoblox devices you want to authenticate to. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed.
api_version{value}	(Required) API version required on Infoblox devices.
ssl_verify={**0**|1}	(Required) By default set to 0. When set to 1 our service will verify the certificate of the web server. When set to 0, our service will not verify the certificate of the web server.
Login credentials	
login_type={**basic**|vault}	(Optional) The login type is basic by default. You can choose vault (for vault based authentication).
username={value}	(Required to create record, optional to update record) The username to be used for authentication to Infoblox server.
password={value}	(Required to create record, optional to update record) The password to be used for authentication to Infoblox server.

Parameter	Description
Vault	
vault_type={value}	(Required to create record when login_type=vault) The vault type to be used for authentication.
vault_id={value}	(Required to create record when login_type=vault and you want to retrieve private key from vault) The vault ID where you want to retrieve the private key from. Certain vaults support this capability.
{vault parameters}	(Required to create record when login_type=vault) Vault specific parameters required depend on the vault type you've selected.

Sample Infoblox record List API

This sample shows the output for Infoblox record List API.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=list"
"https://qualysapi.qualys.com/api/2.0/fo/auth/infoblox/" > file.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_INFOBLOX_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/infoblox/auth_infoblox_list
_output.dtd">
<AUTH_INFOBLOX_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2022-06-29T11:13:21Z</DATETIME>
    <AUTH_INFOBLOX_LIST>
      <AUTH_INFOBLOX>
        <ID>6317683</ID>
        <TITLE><![CDATA[Infoblox_Auth_update]]></TITLE>
        <USERNAME><![joe_user]></USERNAME>
        <SSL_VERIFY><![CDATA[true]]></SSL_VERIFY>
        <IP_SET>
          <IP>1.1.1.1</IP>
          <IP>10.20.30.40</IP>
        </IP_SET>
        <API_VERSION><![CDATA[1v2.0124]]></API_VERSION>
        <SSL_VERIFY><![CDATA[true]]></SSL_VERIFY>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2022-06-29T10:50:19Z</DATETIME>
```

```
          <BY>scan_at</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2022-06-29T11:10:12Z</DATETIME>
        </LAST_MODIFIED>
        <COMMENTS><![CDATA[added]]></COMMENTS>
      </AUTH_INFOBLOX>
    </AUTH_INFOBLOX_LIST>
  </RESPONSE>
</AUTH_INFOBLOX_LIST_OUTPUT>
```

DTD update:

```
We updated the DTD for List API Output.
<!-- QUALYS AUTH_INFOBLOX_LIST_OUTPUT DTD -->
<!ELEMENT AUTH_INFOBLOX_LIST_OUTPUT (REQUEST?, RESPONSE)>

<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, (AUTH_INFOBLOX_LIST|ID_SET)?,
WARNING_LIST?, GLOSSARY?)>
<!ELEMENT AUTH_INFOBLOX_LIST (AUTH_INFOBLOX+)>

<!ELEMENT AUTH_INFOBLOX (ID,
TITLE,USERNAME,SSL_VERIFY?,IP_SET?,API_VERSION?,LOGIN_TYPE?,DIGITAL_VAULT
?,NETWORK_ID?,CREATED,LAST_MODIFIED,COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT SSL_VERIFY (#PCDATA)>
<!ELEMENT IP_SET (IP|IP_RANGE)+>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ELEMENT API_VERSION (#PCDATA)>
<!ELEMENT LOGIN_TYPE (#PCDATA)>
<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_USERNAME?, VAULT_FOLDER?, VAULT_FILE?,
VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_NS_TYPE?, VAULT_NS_NAME?,
```

```
VAULT_SECRET_KV_PATH?, VAULT_SECRET_KV_NAME?, VAULT_SECRET_KV_KEY?,
VAULT_SERVICE_TYPE?)>
<!ELEMENT DIGITAL_VAULT_ID (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TYPE (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TITLE (#PCDATA)>
<!ELEMENT VAULT_USERNAME (#PCDATA)>
<!ELEMENT VAULT_FOLDER (#PCDATA)>
<!ELEMENT VAULT_FILE (#PCDATA)>
<!ELEMENT VAULT_SECRET_NAME (#PCDATA)>
<!ELEMENT VAULT_SYSTEM_NAME (#PCDATA)>
<!ELEMENT VAULT_NS_TYPE (#PCDATA)>
<!ELEMENT VAULT_NS_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_PATH (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_KEY (#PCDATA)>
<!ELEMENT VAULT_SERVICE_TYPE (#PCDATA)>

<!ELEMENT NETWORK_ID (#PCDATA)>

<!ELEMENT CREATED (DATETIME, BY)>
<!ELEMENT BY (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME)>
<!ELEMENT COMMENTS (#PCDATA)>

<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?, ID_SET?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID_RANGE (#PCDATA)>

<!ELEMENT GLOSSARY (USER_LIST?)>
<!ELEMENT USER_LIST (USER+)>
<!ELEMENT USER (USER_LOGIN, FIRST_NAME, LAST_NAME)>
<!ELEMENT FIRST_NAME (#PCDATA)>
<!ELEMENT LAST_NAME (#PCDATA)>

<!-- EOF -->
```

Sample Infoblox record Create API with basic login type

This sample shows the output for Infoblox record Create API with Basic login type.

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=create&ips=10.20.30.40&title=Infoblox_Auth11&api_version=1v2.0123
&ssl_verify=false&username=joe_user&password=abc123"
```

```
"https://qualysapi.qualys.com/api/2.0/fo/auth/infoblox/" > file.xml
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2022-06-29T10:50:19Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>6317683</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample Infoblox record Update API with basic login type

This sample shows the output for Infoblox record Update API with Basic login type.

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=update&add_ips=10.20.30.40&title=Infoblox_Auth_update&api_version
=1v2.0124&ssl_verify=true&comments=added&ids=6317685"
"https://qualysapi.qualys.com/api/2.0/fo/auth/infoblox/" > file.xml
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2022-06-29T11:10:12Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>6317683</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
```

```
</BATCH_RETURN>
```

Sample Infoblox record Delete API

This sample shows the output for Infoblox record Delete API with Basic login type.

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
 "action=delete&ids=6317685"
"https://qualysapi.qualys.com/api/2.0/fo/auth/infoblox/" > file.xml
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2022-06-29T11:18:52Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Deleted</TEXT>
        <ID_SET>
          <ID>6317683</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample Infoblox record Create API with Vault login type

This sample shows the output for Infoblox record Create API with Vault login type.

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=create&ips=10.20.30.40&title=Infoblox_Auth_With_Vault&login_type=
vault&api_version=1v2.0123&username=joe_user&vault_type=HashiCorp&
vault_id=1062779&secret_kv_name=admin&secret_kv_key=Infoblox_vault_secret
&ssl_verify=0" "https://qualysapi.qualys.com/api/2.0/fo/auth/infoblox/" >
file.xml
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
```

```
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2022-07-14T07:46:29Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>1898844</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample Infoblox record Update API with Vault login type

This sample shows the output for Infoblox record Update API with vault login type.

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d
"action=update&add_ips=10.20.30.40&title=Infoblox_Auth_update&api_version
=1v2.0125&ssl_verify=1&
comments=added&ids=1898844"
"https://qualysapi.qualys.com/api/2.0/fo/auth/infoblox/" > file.xml
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2022-07-14T07:46:29Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>1898844</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Maximum Scan Duration for Asset

APIs affected	/api/2.0/fo/subscription/option_profile/vm/
New or Updated API	Updated
DTD or XSD changes	Yes

This release introduces ability to cancel or skip IP/DNS/NetBIOS if it takes more than predetermined time during scanning.

During scanning process, if a slice spends more than required time on a particular target, then it is skipped, and scan continues for the remaining assets. The maximum time on a target is determined by the user through option profile setting and the skipped targets are displayed in scan summary.

Permissions

Manager role is required.

List of Call and API

Sample Create VM Option Profile

Sample Update VM Option Profile

Sample List VM Option Profile

Sample Import Option Profile

Sample VM Scan Summary API

Sample Create VM Option Profile

There are two new parameters added to support scan time limit for assets. When maximum scan duration per asset setup is enabled for the subscription, then option profile displays option to enable maximum time duration for asset. The minimum duration for scan is 1800 (30 minutes) and maximum duration for scan is 172800 (48 hours).

Input Parameters

The following new input parameters are incorporated.

Parameter	Description
`enable_max_scan_duration_per_asset=1`	If flag value is 1 than the scan duration is enabled, else it is disabled.
`max_scan_duration_per_asset_minutes=maximum`	Maximum duration in minutes for scan to be performed on each asset.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=create&title=New Option
Proflie&scan_tcp_ports=none&scan_udp_ports=none&authoritative_option=1&ba
sic_information_gathering=none&vulnerability_detection=complete&map_overa
ll_performance=custom&map_external_scanners=16&map_scanner_appliances=16&
map_netblock_size=8192
IPs&map_packet_delay=maximum&enable_max_scan_duration_per_asset=1&max_sca
n_duration_per_asset_minutes=98"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/vm/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"http://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
 <RESPONSE>
   <DATETIME>2018-04-26T06:40:03Z</DATETIME>
   <TEXT>Option profile successfully added.</TEXT>
   <ITEM_LIST>
     <ITEM>
       <KEY>ID</KEY>
       <VALUE>32112</VALUE>
      </ITEM>
    </ITEM_LIST>
 </RESPONSE>
</SIMPLE_RETURN>
```

Sample Update VM Option Profile

There are two new parameters added to support scan time limit for assets. When maximum scan duration per asset setup is enabled for the subscription, then option profile displays option to enable maximum time duration for asset. The minimum duration for scan is 1800 (30 minutes) and maximum duration for scan is 172800 (48 hours).

Input Parameters

The following new input parameters are incorporated.

Parameter	Description
`enable_max_scan_duration_per_asset=1`	If flag value is 1 than the scan duration is enabled, else it is disabled.
`max_scan_duration_per_asset_minutes=maximum`	Maximum duration in minutes for scan to be performed on each asset.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=update&id=141948"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/vm/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"http://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2018-04-26T09:51:15Z</DATETIME>
    <TEXT>Option profile successfully updated.</TEXT>
    <ITEM_LIST>
      <ITEM>
       <KEY>ID</KEY>
      <VALUE>25121</VALUE>
     </ITEM>
   </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample List VM Option Profile

Option profile list support max_scan_duration_per_asset API parameter which specifies scan time limit configured in option profile.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=list"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/vm/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/opti
on_profile_info.dtd">
<OPTION_PROFILES>
             ...

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>
            </DISSOLVABLE_AGENT>
            <MAX_SCAN_DURATION_PER_ASSET>30</MAX_SCAN_DURATION_PER_ASSET>
             ...
```

```
<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
            </PACKET_OPTIONS>
        </ADDITIONAL>
    </OPTION_PROFILE>
</OPTION_PROFILES>
```

DTD Update

We updated the DTD for List Option Profile to include new elements (in bold).

DTD:/api/2.0/fo/subscription/option_profile/option_profile_info.dtd

```
<!ELEMENT OPTION_PROFILES (OPTION_PROFILE)*>

<!ELEMENT OPTION_PROFILE (BASIC_INFO, SCAN, MAP?, ADDITIONAL,
INSTANCE_DATA_COLLECTION?,OS_BASED_INSTANCE_DISC_COLLECTION?)>
...
 FILE_INTEGRITY_MONITORING?, CONTROL_TYPES?, DO_NOT_OVERWRITE_OS?,
TEST_AUTHENTICATION?, MAX_SCAN_DURATION_PER_ASSET?)>

...

<!ELEMENT OS_BASED_INSTANCE_DISC_COLLECTION (TECHNOLOGIES?)>
<!ELEMENT TECHNOLOGIES (TECHNOLOGY+)>
<!ELEMENT TECHNOLOGY  (#PCDATA)>
```

Sample Import Option Profile

Option profile import supports max_scan_duration_per_asset API parameter which specifies scan time limit to be configured in option profile. The maximum scan duration per asset setup on the subscription should remain enabled while importing, or else it will get ignored by the import API call.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=import"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/vm/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/optio
n_profile_info.dtd">
<OPTION_PROFILES>
    ...
```

```
<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>
            </DISSOLVABLE_AGENT>
            <MAX_SCAN_DURATION_PER_ASSET>78</MAX_SCAN_DURATION_PER_ASSET>
                  <MAP_OPTIONS>
   ...
<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
            </PACKET_OPTIONS>
        </ADDITIONAL>
    </OPTION_PROFILE>
</OPTION_PROFILES>
```

Sample VM Scan Summary API

VM scan summary API displays list of targets that were skipped for scanning because the defined time limit was reached before scan completion on those targets.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=list"  "http://qualysapi.qualys.com/api/2.0/fo/scan/vm/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCAN_SUMMARY_OUTPUT SYSTEM
"http://qualysapi.qualys.com/api/2.0/fo/scan/vm/summary/output.dtd">
<SCAN_SUMMARY_OUTPUT>
    <RESPONSE>
        ...
            <DURATION>1861</DURATION>
                </SCAN_DETAILS>
                <SCAN_RESULTS>
                    <HOSTS>
                        <COUNT>3</COUNT>
                        <HOSTS_DATA>
                            <ABORTED />
                            <EXCEEDED_SCAN_DURATION>
                                <IPV4_LIST>
                                    <COUNT>1</COUNT>
                                    <IPV4_DATA>
                                        <IPV4_CSV>10.20.30.40</IPV4_CSV>
                                    </IPV4_DATA>
                                </IPV4_LIST>
                                <IPV6_LIST>
                                    <COUNT>1</COUNT>
                                    <IPV6_DATA>

<IPV6_CSV>2001:df1:f600:247c::a73:7c87</IPV6_CSV>
                                    </IPV6_DATA>
```

```
                                    </IPV6_LIST>
                                    <DNS_LIST>
                                        <COUNT>5</COUNT>
                                        <DNS_DATA>

<DNS_CSV>ghi.com,qur.com,mno.com,ghi.com,abc.com</DNS_CSV>
                                        </DNS_DATA>
                                    </DNS_LIST>
                                    <NETBIOS_LIST>
                                        <COUNT>5</COUNT>
                                        <NETBIOS_DATA>

<NETBIOS_CSV>YXZ.COM,JKL.COM,NOQ.COM,SVW.COM,pqr.com</NETBIOS_CSV>
                                        </NETBIOS_DATA>
                                    </NETBIOS_LIST>
                                </EXCEEDED_SCAN_DURATION>
                            </HOSTS_DATA>
                        </HOSTS>
                        <DETECTIONS>
                            <IG>
                                ...
        </SCAN_SUMMARY_LIST>
    </RESPONSE>
</SCAN_SUMMARY_OUTPUT>
```

DTD Update:

We updated the DTD for Scan Summary to include modified elements (in bold).

DTD:/api/2.0/fo/scan/vm/summary/output.dtd

```
<!-- QUALYS VM SCAN_SUMMARY_OUTPUT.DTD -->
<!-- $Revision$ -->
<!ELEMENT SCAN_SUMMARY_OUTPUT (REQUEST?,RESPONSE)>
...
E?,BLOCKED?,ABORTED?, FAILED_SLICE_HOSTS?, EXCEEDED_SCAN_DURATION?)>
<!ELEMENT SCANNED (IP_LIST?, DNS_LIST?, NETBIOS_LIST?,INSTANCE_ID_LIST?)>
<!ELEMENT NOT_VULNERABLE (IP_LIST?, DNS_LIST?,
NETBIOS_LIST?,INSTANCE_ID_LIST?)>
<!ELEMENT CANCELLED (IP_LIST?, DNS_LIST?,
NETBIOS_LIST?,INSTANCE_ID_LIST?)>
<!ELEMENT DEAD (IP_LIST?, DNS_LIST?, NETBIOS_LIST?,INSTANCE_ID_LIST?)>
<!ELEMENT EXCLUDED (IP_LIST?, DNS_LIST?,
NETBIOS_LIST?,INSTANCE_ID_LIST?)>
<!ELEMENT UNRESOLVED (IP_LIST?, DNS_LIST?,
NETBIOS_LIST?,INSTANCE_ID_LIST?)>
<!ELEMENT DUPLICATE (IP_LIST?, DNS_LIST?,
NETBIOS_LIST?,INSTANCE_ID_LIST?)>
```

```
<!ELEMENT BLOCKED (IP_LIST?, DNS_LIST?, NETBIOS_LIST?,INSTANCE_ID_LIST?)>
<!ELEMENT ABORTED (IP_LIST?, DNS_LIST?, NETBIOS_LIST?,INSTANCE_ID_LIST?)>
<!ELEMENT FAILED_SLICE_HOSTS (IPV4_LIST?, IPV6_LIST?, DNS_LIST?,
NETBIOS_LIST?, INSTANCE_ID_LIST?)>
<!ELEMENT EXCEEDED_SCAN_DURATION (IPV4_LIST?, IPV6_LIST?, DNS_LIST?, >
...
<!ELEMENT SEVERITY_3 (#PCDATA)>
<!ELEMENT SEVERITY_4 (#PCDATA)>
<!ELEMENT SEVERITY_5 (#PCDATA)>
<!-- EOF -->
```

New Parameter Added to Get Posture Info API in PCRS

APIs affected	/pcrs/1.0/posture/postureInfo
New or Updated API	Updated
DTD or XSD changes	Not applicable as the output is in JSON

With this release, Qualys Policy Compliance Reporting Service (PCRS) has added `lastScanDate` as an optional request parameter to the Get Posture Info API. This parameter fetches postures based on the date on which an asset was last scanned.

You can provide the date in the following format:

- `lastScanDate=2021-12-17`

- `lastScanDate=2021-12-17T18:48:16Z`

Additionally, `cloudResourceId` has been introduced as a new response field in the response JSON to get cloud instance information when you fetch postures using the Get Posture Info API.

API request:

```
Curl-X POST
"https://gateway.xxx.eng.xxx.qualys.com/pcrs/1.0/posture/postureInfo?evid
enceRequired=0&compressionRequired=1&lastEvaluationDate=2021-12-
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>\"]}]"
```

JSON output:

```
[
    {
        "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>,
        "cloudResourceId": "<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
```

```
        },
    ]
```

Issues Addressed

- We fixed an issue where unexpected characters appeared in the API output of scanner appliance list when include_cloud_info=1 was included in the API request.
- 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.
- The Ignore Vulnerability API failed to ignore vulnerabilities if the vulnerability was detected on multiple ports. We have now fixed this issue so that vulnerability is ignored despite being detected on multiple ports.