Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.19

May 24, 2022 (Updated June 10, 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

Posture Info API - Show Extended Evidence in Output

Fixed Typo In Output and DTD for IBM WebSphere Records List

API Changes to Support Asset Risk Scoring (these changes will be visible when Qualys Cloud Platform 3.12 is available)

Issues Addressed

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.

Posture Info API - Show Extended Evidence in Output

APIs affected	/api/2.0/fo/compliance/posture/info/
New or Updated API	Updated
DTD or XSD changes	Yes

Now you can show extended evidence information in the Posture Info API output (XML and CSV formats). Specify the new input parameter "show_extended_evidence=1" in the API request to include extended evidence information in the output.

The Evidence for a control includes the Expected and Actual values for the control on the host. The Extended Evidence includes any additional findings/information collected during the control evaluation on the host to support the actual result.

Extended Evidence Statistics will show information found during the control evaluation irrespective of whether the control Passed or Failed. For example, in the case of a Directory Search control, we'll show statistics like the number of matched directories and files found and the number of directories and files searched in the search duration. In case of an error, the error message is visible under Extended Statistics Error.

XML format

When "show_extended_evidence=1" is specified for XML output, you'll see 3 new tags in the XML: <EXTENDED_EVIDENCE>, <STATISTICS>, <EXTENDED_STATISTICS_ERROR>.

CSV format

When "show_extended_evidence=1" is specified for CSV output, you'll see a new "Extended Evidence" column header in the CSV.

In the new column, you'll see "======Extended Evidence======:" followed by the extended evidence information collected for the control. If there was an error, you'll see "======Extended Evidence Statistics======:" depending upon the configuration, followed by different parameters. For example:

Search duration: 63 seconds
Match limit reached
Number of matched directories: 23
Number of matched files: 27
Number of matched directories and files: 50
Number of searched directories: 23
Number of searched files: 28
Number of searched directories and files: 51

Input Parameters

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

Parameter	Description
show_extended_evidence ={**0**|1}	(Optional when details=All or details=Light) Set to 1 to show extended evidence information in the output. When set to 0 or when unspecified, extended evidence information is not shown in the output. Note: You cannot specify show_extended_evidence=1 in the same request as hide_evidence=1. This will result in an Error. Extended evidence is a part of the evidence data and it's shown only when evidence data is shown.

Sample 1 - Posture Info in XML Format

This sample includes 2 INFO records. One record has data for Extended Evidence, and the other record has data for Statistics and Extended Statistics Error.

API request:

```
curl -H "X-Requested-With:curl" -u "USERNAME:PASSWORD" -d
"action=list&policy_id=1055704&details=All&output_format=xml&show_extende
d_evidence=1"
"http://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POSTURE_INFO_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/posture_
info_list_output.dtd">
<POSTURE_INFO_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2022-04-28T11:08:05Z</DATETIME>
    <POLICY>
<ID>1055704</ID>    <DATETIME>2022-04-28T11:08:05Z</DATETIME>
    <INFO_LIST>
      <INFO>
        <ID>10461454</ID>
        <HOST_ID>2573671</HOST_ID>
        <CONTROL_ID>1071</CONTROL_ID>
        <TECHNOLOGY_ID>80</TECHNOLOGY_ID>
        <INSTANCE><![CDATA[os]]></INSTANCE>
        <STATUS>Failed</STATUS>
        <POSTURE_MODIFIED_DATE>2022-04-
27T08:57:38Z</POSTURE_MODIFIED_DATE>
        <EVALUATION_DATE>2022-05-02T06:21:45Z</EVALUATION_DATE>
        <PREVIOUS_STATUS>Failed</PREVIOUS_STATUS>
```

```
        <FIRST_FAIL_DATE>2022-04-27T08:57:38Z</FIRST_FAIL_DATE>
        <LAST_FAIL_DATE>2022-05-02T06:21:45Z</LAST_FAIL_DATE>
        <FIRST_PASS_DATE>2022-04-21T12:05:56Z</FIRST_PASS_DATE>
        <LAST_PASS_DATE>2022-04-21T12:05:56Z</LAST_PASS_DATE>
        <EVIDENCE>
          <BOOLEAN_EXPR><![CDATA[(:dp_2 in #fv_2 or :dp_2 < $tp_1
)]]></BOOLEAN_EXPR>
          <DPV_LIST>
            <DPV lastUpdated="2022-04-28T10:03:33Z">
              <LABEL>:dp_2</LABEL>
              <V><![CDATA[5]]></V>
            </DPV>
          </DPV_LIST>
          <EXTENDED_EVIDENCE><![CDATA[Row 1:File name,Setting,Value
Row 2:/etc/login.defs,PASS_MIN_LEN,5
]]></EXTENDED_EVIDENCE>
          <STATISTICS><![CDATA[]]></STATISTICS>

<EXTENDED_STATISTICS_ERROR><![CDATA[]]></EXTENDED_STATISTICS_ERROR>
        </EVIDENCE>
      </INFO>
      <INFO>
        <ID>10479751</ID>
        <HOST_ID>2573673</HOST_ID>
        <CONTROL_ID>100002</CONTROL_ID>
        <TECHNOLOGY_ID>81</TECHNOLOGY_ID>
        <INSTANCE><![CDATA[os]]></INSTANCE>
        <STATUS>Passed</STATUS>
        <POSTURE_MODIFIED_DATE>2022-04-
28T10:09:39Z</POSTURE_MODIFIED_DATE>
        <EVALUATION_DATE>2022-05-02T06:21:45Z</EVALUATION_DATE>
        <PREVIOUS_STATUS>Passed</PREVIOUS_STATUS>
        <FIRST_FAIL_DATE>N/A</FIRST_FAIL_DATE>
        <LAST_FAIL_DATE>N/A</LAST_FAIL_DATE>
        <FIRST_PASS_DATE>2022-04-28T10:09:39Z</FIRST_PASS_DATE>
        <LAST_PASS_DATE>2022-05-02T06:21:45Z</LAST_PASS_DATE>
        <EVIDENCE>
          <BOOLEAN_EXPR><![CDATA[:dp_8 matches $tp_5]]></BOOLEAN_EXPR>
          <DPV_LIST>
            <DPV lastUpdated="2022-04-28T10:03:26Z">
              <LABEL>:dp_8</LABEL>
              <V><![CDATA[No data found]]></V>
            </DPV>
          </DPV_LIST>
          <EXTENDED_EVIDENCE><![CDATA[]]></EXTENDED_EVIDENCE>
          <STATISTICS><![CDATA[Search duration: 63 seconds
]]></STATISTICS>
          <EXTENDED_STATISTICS_ERROR><![CDATA[Error Code 28:Base directory
not foundcan't lstat target of '/usr/lib/debug/usr/.dwz ->
```

```
/usr/lib/debug/.dwz' (No such file or directory),can't lstat target of
'/usr/lib/systemd/system/dbus-org.freedesktop.network1.service ->
/usr/lib/systemd/system/systemd-networkd.service' (No such file or
directory),can't lstat target of '/usr/lib/modules/3.10.0-
327.el7.x86_64/build -> /usr/src/kernels/3.10.0-327.el7.x86_64' (No such
file or directory),can't lstat target of '/usr/lib/modules/3.10.0-
327.el7.x86_64/source -> /usr/src/kernels/3.10.0-327.el7.x86_64' (No such
file or directory),can't lstat target of '/usr/share/gdb/auto-load/bin ->
/usr/share/gdb/auto-load/usr/bin' (No such file or directory),can't lstat
target of '/usr/share/gdb/auto-load/lib -> /usr/share/gdb/auto-
load/usr/lib' (No such file or directory),can't lstat target of
'/usr/share/gdb/auto-load/sbin -> /usr/share/gdb/auto-load/usr/sbin' (No
such file or directory),can't lstat target of
'/usr/share/PackageKit/icons -> /usr/share/pixmaps/comps' (No such file
or directory)
]]></EXTENDED_STATISTICS_ERROR>
        </EVIDENCE>
      </INFO>
...
```

Sample 2 - Error In XML Output

This sample shows the error you'll get in the XML output if you specify "hide_evidence=1" and "show_extended_evidence=1" in the same request. Extended evidence is a part of the Evidence data and it's shown only when Evidence data is shown.

API request:

```
curl -H "X-Requested-With:curl" -u "USERNAME:PASSWORD" -d
"action=list&policy_ids=31480&details=All&output_format=xml&hide_evidence
=1&show_extended_evidence=1"
"http://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/"
```

XML output:

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
https://qualysapi.qualys.com/api/2.0/simple_return.dtd>
<SIMPLE_RETURN>
<RESPONSE>
<DATETIME>2022-04-28T07:32:55Z</DATETIME>
<CODE>1907</CODE>
<TEXT>The following combination of key=value pairs is not supported:
hide_evidence=1, show_extended_evidence=1 (The Extended Evidence is a
part of the evidence data, hence it is shown only when evidence data is
shown. If hide_evidence = 1 parameter is sent, then evidence data is not
sent in the response, that also means extended evidence is not sent
either.)</TEXT>
</RESPONSE>
</SIMPLE_RETURN>
```

DTD update:

We updated the DTD for Posture Info Output to include new elements (in bold).

DTD: <platform>/api/2.0/fo/compliance/posture/info/posture_info_list_output.dtd

```
<!-- QUALYS POSTURE_INFO_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT POSTURE_INFO_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, ((INFO_LIST?, SUMMARY?, WARNING_LIST?,
GLOSSARY?) | POLICY+))>

<!ELEMENT POLICY (ID, DATETIME, INFO_LIST?, SUMMARY?, WARNING_LIST?,
GLOSSARY?)>

<!ELEMENT INFO_LIST (INFO+)>
<!ELEMENT INFO (ID, HOST_ID, CONTROL_ID, TECHNOLOGY_ID, INSTANCE?, STATUS,
REMEDIATION?, POSTURE_MODIFIED_DATE?, EVALUATION_DATE?, PREVIOUS_STATUS?,
FIRST_FAIL_DATE?, LAST_FAIL_DATE?, FIRST_PASS_DATE?, LAST_PASS_DATE?,
EXCEPTION?, EVIDENCE?, CAUSE_OF_FAILURE?)>

...

<!ELEMENT EVIDENCE (BOOLEAN_EXPR, DPV_LIST?, EXTENDED_EVIDENCE?,
STATISTICS?, EXTENDED_STATISTICS_ERROR? )>
<!ELEMENT BOOLEAN_EXPR (#PCDATA)>
<!ELEMENT DPV_LIST (DPV+)>
<!ELEMENT DPV (LABEL, (ERROR|V)+, TM_REF?)>
<!ATTLIST DPV lastUpdated CDATA #IMPLIED>
<!ELEMENT V (#PCDATA|H|R)*>
<!ATTLIST V fileName CDATA #IMPLIED>
<!ELEMENT H (C+)>
<!ELEMENT R (C+)>
<!ELEMENT EXTENDED_EVIDENCE (#PCDATA)>
<!ELEMENT STATISTICS (#PCDATA)>
<!ELEMENT EXTENDED_STATISTICS_ERROR (#PCDATA)>
...
```

Sample 3 - Posture Info in CSV Format

This sample shows Extended Evidence information in CSV format.

API request:

```
curl -H "X-Requested-With:curl" -u "USERNAME:PASSWORD" -d
"action=list&policy_id=1055704&details=All&output_format=csv&show_extende
d_evidence=1"
"http://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/"
```

CSV output:

```
----BEGIN_RESPONSE_BODY_CSV
"POLICY ID","DATETIME"
"1055704","04/28/2022 11:04:48"
"ID","IP","OS","DNS Name","NetBios","Tracking Method","Control
ID","Control Statement","Criticality Label","Criticality
Value","Technology ID","Technology Name","Posture","Previous
Status","First Fail Date","Last Fail Date","First Pass Date","Last Pass
Date","Evaluation Date","Qualys Host ID","Posture
Evidence","Reference","Host ID","Instance","Asset ID","Posture Modified
Date","Last Compliance Scan Date","Last vuln Scan Date","Extended
Evidence"
"10461454","10.11.12.13","Windows Server 2008 R2 Enterprise 64 bit
Edition",,"SYS_10_11_12_13","IP","8445","Status of Application Identity
Service","MEDIUM","2","21","Windows 2008
Server","Passed","Passed","N/A","N/A","01/28/2021 09:14:34","01/28/2021
09:14:34","01/28/2021 09:14:24",,"This Integer value <B>X</B> indicates
the status of the service <B>Application Identity</B> using registry key
path <B>HKLM\SYSTEM\CurrentControlSet\services\AppIDSvc</B>. A value of
<B>2</B> indicates the service is set to <B>Automatic</B>; a value of
<B>3</B> indicates the service is set to <B>Manual</B>; a value of
<B>4</B> indicates the service is set to <B>Disabled</B>; a value of
<B>21</B> indicates the service is set to <B>Automatic (Delayed
start)</B>.

======Expected Value(s)======

Manual (3)

======Current Value(s) - Last updated: 01/15/2021 at 05:56:34 (GMT)======
Manual (3)","V-3487","678901","os","890123","01/28/2021
09:14:24","01/15/2021 05:56:34","N/A","
======Extended Evidence======:
Row 1:Service Name,Registry Key,Start Value,Delayed Start
Row 2:AppIDSvc,HKLM\SYSTEM\CurrentControlSet\Services\AppIDSvc,3,0"
"10479751","10.20.30.40","Red Hat Enterprise Linux Server
7.2",,,"IP","100002","STMT","UNDEFINED","0","81","Red Hat Enterprise
```

```
Linux 7.x","Passed","Passed","N/A","N/A","04/28/2022
10:09:39","05/02/2022 06:21:45","05/02/2022 06:21:45",,"Description of
New control UDC

======Expected Value(s)======
regular expression match
6e6c359418b7364bdd9838f0063670f0603f400f86ad21f73735863c4fcf09ed$

======Current Value(s) - Last updated: 04/28/2022 at 10:03:26 (GMT)======
Error Code 28:Base directory not found

======Statistics======
Error: Error Code 28:Base directory not found

======Actual Value List======

======Added Files/Directories======

======Removed Files/Directories======

======Permission Modified Files/Directories======

======Content Modified
Files/Directories======","N/A","2573673","os","13805915","04/28/2022
10:09:39","04/28/2022 10:03:33","N/A","
======Extended Evidence Statistics======:
Search duration: 63 seconds

Error:
Error Code 28:Base directory not found,can't lstat target of
'/usr/lib/debug/usr/.dwz -> /usr/lib/debug/.dwz' (No such file or
directory),can't lstat target of '/usr/lib/systemd/system/dbus-
org.freedesktop.network1.service -> /usr/lib/systemd/system/systemd-
networkd.service' (No such file or directory),can't lstat target of
'/usr/lib/modules/3.10.0-327.el7.x86_64/build -> /usr/src/kernels/3.10.0-
327.el7.x86_64' (No such file or directory),can't lstat target of
'/usr/lib/modules/3.10.0-327.el7.x86_64/source ->
/usr/src/kernels/3.10.0-327.el7.x86_64' (No such file or directory),can't
lstat target of '/usr/share/gdb/auto-load/bin -> /usr/share/gdb/auto-
load/usr/bin' (No such file or directory),can't lstat target of
'/usr/share/gdb/auto-load/lib -> /usr/share/gdb/auto-load/usr/lib' (No
such file or directory),can't lstat target of '/usr/share/gdb/auto-
load/sbin -> /usr/share/gdb/auto-load/usr/sbin' (No such file or
directory),can't lstat target of '/usr/share/PackageKit/icons ->
/usr/share/pixmaps/comps' (No such file or directory)"
...

----END_RESPONSE_BODY_CSV
```

Fixed Typo In Output and DTD for IBM WebSphere Records List

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

We fixed a typo in the XML output and DTD for List IBM WebSphere Authentication Records API. We changed "INSTLLATION" to "INSTALLATION" in the tags shown below.

We changed these tags:

<UNIX_INSTLLATION_DIRECTORY> changed to
<UNIX_INSTALLATION_DIRECTORY>

<WINDOWS_INSTLLATION_DIRECTORY> changed to
<WINDOWS_INSTALLATION_DIRECTORY>

Sample List IBM WebSphere Records

This sample shows the corrected tag names in the output.

API request:

```
curl -H "X-Requested-With:curl" -u "USERNAME:PASSWORD" -d
"action=list"
"https://qualysapi.qualys.com/api/2.0/fo/auth/ibm_websphere/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_IBM_WEBSPHERE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/ibm_websphere/auth_ibm_webs
phere_list_output.dtd">
<AUTH_IBM_WEBSPHERE_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2022-03-16T16:27:50Z</DATETIME>
    <AUTH_IBM_WEBSPHERE_LIST>
      <AUTH_IBM_WEBSPHERE>
        <ID>6002413</ID>
        <TITLE><![CDATA[My IBM WAS Record]]></TITLE>
        <IP_SET>
          <IP>10.11.12.13</IP>
        </IP_SET>

<UNIX_INSTALLATION_DIRECTORY><![CDATA[/opt/IBM/WebSphere/AppServer]]></U
NIX_INSTALLATION_DIRECTORY>
```

```
        <UNIX_DIR_MODE>server_dir</UNIX_DIR_MODE>

<WINDOWS_INSTALLATION_DIRECTORY><![CDATA[C:\IBM\WebSphere\AppServerUpdat
e]]></WINDOWS_INSTALLATION_DIRECTORY>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2022-03-10T10:49:32Z</DATETIME>
          <BY>joe_user</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2022-03-15T11:35:38Z</DATETIME>
        </LAST_MODIFIED>
        <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
        <IS_ACTIVE>1</IS_ACTIVE>
      </AUTH_IBM_WEBSPHERE>
...
```

DTD update:

We updated the DTD for IBM WebSphere List output to fix the tag names (in bold).

DTD: <platform>/api/2.0/fo/auth/ibm_websphere/auth_ibm_websphere_list_output.dtd

```
<!-- QUALYS AUTH_IBM_WEBSPHERE_LIST_OUTPUT DTD -->
<!-- $Revision: $ -->
<!ELEMENT AUTH_IBM_WEBSPHERE_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_IBM_WEBSPHERE_LIST|ID_SET)?,
WARNING_LIST?, GLOSSARY?)>
<!ELEMENT AUTH_IBM_WEBSPHERE_LIST (AUTH_IBM_WEBSPHERE+)>

<!ELEMENT AUTH_IBM_WEBSPHERE (ID, TITLE, IP_SET,
UNIX_INSTALLATION_DIRECTORY?,UNIX_DIR_MODE?,
WINDOWS_INSTALLATION_DIRECTORY?, NETWORK_ID?, CREATED, LAST_MODIFIED,
IS_SYSTEM_CREATED?, IS_ACTIVE?, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT UNIX_INSTALLATION_DIRECTORY (#PCDATA)>
```

```
<!ELEMENT UNIX_DIR_MODE (#PCDATA)>
<!ELEMENT WINDOWS_INSTALLATION_DIRECTORY (#PCDATA)>
<!ELEMENT IP_SET (IP|IP_RANGE)+>
...
```

API Changes to Support Asset Risk Scoring

Risk-based vulnerability management requires intelligence-driven vulnerability severity scoring and a complete understanding of assets where the vulnerabilities are detected, including their business and operational criticality, association with business-critical applications, context about the asset's exposure to attack, and so on.

Asset Risk Scoring helps users prioritize their vulnerabilities based on the risk to their assets and not just the technical severity. The Asset Risk Scoring feature will be GA with Qualys Cloud Platform 3.12.

We made changes to the Qualys APIs listed below to support new risk scores, including Asset Risk Score (ARS) for assets, Qualys Detection Score (QDS) for vulnerabilities, and Qualys Vulnerability Score (QVS) for CVEs. **Note: These API changes will only be visible when Qualys Cloud Platform 3.12 is available.**

Host List

Host List VM Detection

KnowledgeBase QVS Download in JSON Format (New)

Updates to Host Based Scan Reports

Host List

APIs affected	/api/2.0/fo/asset/host/action=list
New or Updated API	Updated
DTD or XSD changes	Yes

The Host List API has been updated to show the Asset Risk Score (ARS) for each asset record in the API output and allows users to filter the output based on the ARS.

The Asset Risk Score (ARS) is the overall risk score assigned to the asset based on multiple contributing factors, including Asset Criticality Score (ACS), Risk (QID) scores for each severity level, and an auto assigned weighting factor (w) for each criticality level of QIDs.

ARS has a range from 0 to 1000:

- Critical (850-1000)
- High (700-849)
- Medium (500-699)
- Low (0-499)

Input Parameters

Use the following new input parameters to show the Asset Risk Score (ARS) for each asset record in the API output and to filter the output based on the score. Refer to the Qualys API (VM,PC) User Guide for details on all available input parameters.

Parameter	Description
show_ars={0|1}	(Optional) Specify 1 to show the ARS value in the output. Specify 0 if you do not want to show the ARS value.
ars_min={value}	(Optional) Show only asset records with an ARS value greater than or equal to the ARS min value specified. ars_min can only be specified when show_ars=1. When ars_min and ars_max are specified in the same request, the ars_min value must be less than the ars_max value.
ars_max={value}	(Optional) Show only detection records with an ARS value less than or equal to the ARS max value specified. ars_max can only be specified when show_ars=1. When ars_min and ars_max are specified in the same request, the ars_min value must be less than the ars_max value.
show_ars_factors={0|1}	(Optional) Specify 1 to show ARS contributing factors associated with each asset record in the output. Specify 0 if you do not want to show ARS contributing factors.

Sample Host List API

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/action=list&ips=10.20
.30.40,10.11.12.13&show_ars=1&ars_min=0&ars_max=1000&show_ars_factors=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/dtd/list/output.dtd">
<HOST_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2022-01-31T12:06:31Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>2242029</ID>
                <IP>10.11.12.13</IP>
                <ASSET_RISK_SCORE>371</ASSET_RISK_SCORE>
                <ASSET_CRITICALITY_SCORE>2</ASSET_CRITICALITY_SCORE>
                <ARS_FACTORS>
                   <ARS_FORMULA>2 * {( 1.0 * 97 ) + ( 0.7 * 82 ) + ( 0.4
* 63 ) + ( 0.25 * 23 )}</ARS_FORMULA>
                    <VULN_COUNT qds_severity="1">0</VULN_COUNT>
                    <VULN_COUNT qds_severity="2">6</VULN_COUNT>
                    <VULN_COUNT qds_severity="3">11</VULN_COUNT>
                    <VULN_COUNT qds_severity="4">18</VULN_COUNT>
                    <VULN_COUNT qds_severity="5">4</VULN_COUNT>
                </ARS_FACTORS>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <DNS>
                    <![CDATA[abc.sample.qualys.com]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[abc]]>
                    </HOSTNAME>
                    <DOMAIN>
                        <![CDATA[sample.qualys.com]]>
                    </DOMAIN>
                    <FQDN>
                        <![CDATA[abc.sample.qualys.com]]>
                    </FQDN>
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[SYS_10_11_12_13]]>
                </NETBIOS>
                <OS>
```

```
                    <![CDATA[Red Hat Linux 7.3]]>
                </OS>
            </HOST>
            <HOST>
                <ID>2256697</ID>
                <IP>10.20.30.40</IP>
                <ASSET_RISK_SCORE>174</ASSET_RISK_SCORE>
                <ASSET_CRITICALITY_SCORE>2</ASSET_CRITICALITY_SCORE>
                <ARS_FACTORS>
                    <ARS_FORMULA></ARS_FORMULA>
                    <VULN_COUNT qds_severity="1">0</VULN_COUNT>
                    <VULN_COUNT qds_severity="2">1</VULN_COUNT>
                    <VULN_COUNT qds_severity="3">0</VULN_COUNT>
                    <VULN_COUNT qds_severity="4">1</VULN_COUNT>
                    <VULN_COUNT qds_severity="5">0</VULN_COUNT>
                </ARS_FACTORS>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <DNS>
                    <![CDATA[10-20-30-40.bogus.tld]]>
                </DNS>
                <DNS_DATA>
                    <HOSTNAME>
                        <![CDATA[10-20-30-40]]>
                    </HOSTNAME>
                    <DOMAIN>
                        <![CDATA[bogus.tld]]>
                    </DOMAIN>
                    <FQDN>
                        <![CDATA[10-20-30-40.bogus.tld]]>
                    </FQDN>
                </DNS_DATA>
                <NETBIOS>
                    <![CDATA[SYS_10_20_30_40]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows Server 2003 64 bit Edition Service
Pack 1]]>
                </OS>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_OUTPUT>
```

DTD update:

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

DTD: <platform>/api/2.0/fo/asset/host/dtd/list/output.dtd

```
<!-- QUALYS HOST_OUTPUT DTD FOR LIST ACTION-->
<!-- $Revision$ -->
<!ELEMENT HOST_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, (HOST_LIST|ID_SET)?, WARNING?, GLOSSARY?)>
<!ELEMENT HOST_LIST (HOST+)>
<!ELEMENT HOST (ID, ASSET_ID?, IP?, IPV6?, ASSET_RISK_SCORE?,
ASSET_CRITICALITY_SCORE?, ARS_FACTORS?, TRACKING_METHOD?, NETWORK_ID?,
DNS?, DNS_DATA?, CLOUD_PROVIDER?, CLOUD_SERVICE?, CLOUD_RESOURCE_ID?,
EC2_INSTANCE_ID?, NETBIOS?, OS?, QG_HOSTID?, TAGS?, METADATA?,
CLOUD_PROVIDER_TAGS?, LAST_VULN_SCAN_DATETIME?, LAST_VM_SCANNED_DATE?,
LAST_VM_SCANNED_DURATION?,
LAST_VM_AUTH_SCANNED_DATE?, LAST_VM_AUTH_SCANNED_DURATION?,
LAST_COMPLIANCE_SCAN_DATETIME?, LAST_SCAP_SCAN_DATETIME?, OWNER?,
COMMENTS?, USER_DEF?, ASSET_GROUP_IDS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT ASSET_ID (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IPV6 (#PCDATA)>
<!ELEMENT ASSET_RISK_SCORE (#PCDATA)>
<!ELEMENT ASSET_CRITICALITY_SCORE (#PCDATA)>
<!ELEMENT ARS_FACTORS (ARS_FORMULA, VULN_COUNT*)>
<!ELEMENT ARS_FORMULA (#PCDATA)>
<!ELEMENT VULN_COUNT (#PCDATA)>
<!ATTLIST VULN_COUNT qds_severity CDATA #REQUIRED>
<!ELEMENT TRACKING_METHOD (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
...
```

Host List VM Detection

APIs affected	/api/2.0/fo/asset/host/vm/detection/?action=list
New or Updated API	Updated
DTD or XSD changes	Yes

The Host List VM Detection API has been updated to show the Qualys Detection Score (QDS) for each detection record in the API output and allows users to filter the output based on the QDS.

The Qualys Detection Score (QDS) is assigned to vulnerabilities detected by Qualys. QDS is derived from multiple contributing factors, including vulnerability technical details (e.g. CVSS score), vulnerability temporal details (e.g. external threat intelligence like exploit code maturity), and remediation controls applied to mitigate the risk from the vulnerability.

QDS has a range from 1 to 100 with these severity levels:

- Critical (90-100)
- High (70-89)
- Medium (40-69)
- Low (1-39)

Input Parameters

Use the following new input parameters to show the Qualys Detection Score (QDS) for each detection record in the API output and filter the output based on the QDS score. Refer to the Qualys API (VM,PC) User Guide for details on all available input parameters.

Parameter	Description
show_qds={0|1}	(Optional) Specify 1 to show the QDS value in the output for each detection record. Specify 0 if you do not want to show the QDS value.
qds_min={value}	(Optional) Show only detection records with a QDS value greater than or equal to the QDS min value specified. qds_min can only be specified when show_qds=1. When qds_min and qds_max are specified in the same request, the qds_min value must be less than the qds_max value.
qds_max={value}	(Optional) Show only detection records with a QDS value less than or equal to the QDS max value specified. qds_max can only be specified when show_qds=1. When qds_min and qds_max are specified in the same request, the qds_min value must be less than the qds_max value.
show_qds_factors ={0|1}	(Optional) Specify 1 to show QDS contributing factors associated with each detection record in the output. Specify 0 if you do not want to show QDS contributing factors.

Sample Host List VM Detection

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?action=
list&ips=10.20.30.40,10.11.12.13&show_qds=1&qds_min=1&qds_max=20&show_
qds_factors=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/dtd/outp
ut.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2022-01-31T12:10:01Z</DATETIME>
    <HOST_LIST>       <HOST> ...
          <DETECTION>
            <QID>38170</QID>
            <TYPE>Confirmed</TYPE>
            <SEVERITY>2</SEVERITY>
            <PORT>443</PORT>
            <PROTOCOL>TCP</PROTOCOL
            <SSL>1</SSL>
            <RESULTS>
               <![CDATA[CCertificate #0
CN=IPMI,OU=Software,O=Super_Micro_Computer,ST=California,C=US (IPMI)
doesn&apos;t resolve]]>
            </RESULTS>
            <STATUS>ACTIVE</STATUS>
            <FIRST_FOUND_DATETIME>2021-12-
29T14:09:58Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2022-01-
11T13:11:20Z</LAST_FOUND_DATETIME>
            <QDS severity="LOW">5</QDS>
            <QDS_FACTORS>
                <QDS_FACTOR name="RTI">
                    <![CDATA[[No_Patch]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="TEMPORAL_SCORE">
                    <![CDATA[2.1]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="BASE_SCORE">
                    <![CDATA[2.6]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="SEVERITY">
                    <![CDATA[2]]>
                <QDS_FACTOR name="EXPLOIT_MATURITY">
```

```
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="EXPLOIT_AVAILABLE">
                    <![CDATA[[poc]]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="TRENDING">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="MITIGATION_CONTROLS">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="MALWARE_NAME">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="MALWARE_HASH">
                    <![CDATA[null]]>
                </QDS_FACTOR>
                <QDS_FACTOR name="RTI">
                    <![CDATA[null]]>
                </QDS_FACTOR>
            </QDS_FACTORS>
            <TIMES_FOUND>1</TIMES_FOUND>
            <LAST_TEST_DATETIME>2021-06-03T11:18:57Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2021-06-
05T03:12:47Z</LAST_UPDATE_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <LAST_PROCESSED_DATETIME>2021-06-
05T03:12:47Z</LAST_PROCESSED_DATETIME>          </DETECTION>
...
        </DETECTION_LIST>
      </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

DTD update:

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

DTD: <platform>/api/2.0/fo/asset/host/vm/detection/dtd/output.dtd

```
<!-- QUALYS HOST_LIST_VM_DETECTION_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT HOST_LIST_VM_DETECTION_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, HOST_LIST?, WARNING?)>
<!ELEMENT HOST_LIST (HOST+)>
<!ELEMENT HOST (ID, ASSET_ID?, IP?, IPV6?, TRACKING_METHOD?, NETWORK_ID?,
OS?, OS_CPE?, DNS?, DNS_DATA?, CLOUD_PROVIDER?, CLOUD_SERVICE?,
CLOUD_RESOURCE_ID?, EC2_INSTANCE_ID?, NETBIOS?, QG_HOSTID?,
LAST_SCAN_DATETIME?, LAST_VM_SCANNED_DATE?,
LAST_VM_SCANNED_DURATION?, LAST_VM_AUTH_SCANNED_DATE?,
LAST_VM_AUTH_SCANNED_DURATION?, LAST_PC_SCANNED_DATE?, TAGS?, METADATA?,
CLOUD_PROVIDER_TAGS?, DETECTION_LIST)>

...

<!ELEMENT DETECTION_LIST (DETECTION+)>
<!ELEMENT DETECTION (QID, TYPE, SEVERITY?, PORT?, PROTOCOL?, FQDN?, SSL?,
INSTANCE?,RESULTS?, STATUS?,FIRST_FOUND_DATETIME?, LAST_FOUND_DATETIME?,
QDS?, QDS_FACTORS?, TIMES_FOUND?, LAST_TEST_DATETIME?,
LAST_UPDATE_DATETIME?,LAST_FIXED_DATETIME?, FIRST_REOPENED_DATETIME?,
LAST_REOPENED_DATETIME?,TIMES_REOPENED?,SERVICE?, IS_IGNORED?,
IS_DISABLED?, AFFECT_RUNNING_KERNEL?, AFFECT_RUNNING_SERVICE?,
AFFECT_EXPLOITABLE_CONFIG?, LAST_PROCESSED_DATETIME?, ASSET_CVE?)>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT TYPE (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT PROTOCOL (#PCDATA)>
<!ELEMENT SSL (#PCDATA)>
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT RESULTS (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT SEVERITY (#PCDATA)>
<!ELEMENT QDS (#PCDATA)>
<!ATTLIST QDS severity CDATA #REQUIRED>
<!ELEMENT QDS_FACTORS (QDS_FACTOR)*>
<!ELEMENT QDS_FACTOR (#PCDATA)>
<!ATTLIST QDS_FACTOR name CDATA #REQUIRED>
<!ELEMENT FIRST_FOUND_DATETIME (#PCDATA)>
<!ELEMENT LAST_FOUND_DATETIME (#PCDATA)>
<!ELEMENT TIMES_FOUND (#PCDATA)>
...
```

KnowledgeBase QVS Download in JSON Format (New)

APIs affected	/api/2.0/fo/knowledge_base/qvs/?action=list
New or Updated API	New
DTD or XSD changes	n/a

Use this new API endpoint to download Qualys Vulnerability Score (QVS) information from the Vulnerability KnowledgeBase for one or more CVE IDs based on certain criteria. The API output is in JSON format.

The Qualys Vulnerability Score (QVS) is a Qualys-assigned score to a vulnerability based on multiple factors associated with the CVE, such as CVSS and external threat indicators like active exploitation, exploit code maturity and much more.

Input Parameters

Use the following input parameters.

Parameter	Description
action=list	(Required) You must specify the list action.
details={Basic|All}	(Required) Specify details=Basic to show the base QVS in the output. Specify details=All to show the base QVS and contributing factors in the output.
CVEs={value}	(Required) Filter the JSON output to only show vulnerabilities associated with the CVE IDs that you specify.
qvs_last_modified _before={date}	(Optional) Show only CVE IDs with a QVS score that was last modified before a certain date and time. Valid date format is: YYYY-MMDD[THH:MM:SSZ] format (UTC/GMT), like “2021-12-01” or “2021-1201T23:12:00Z”.
qvs_last_modified _after={date}	(Optional) Show only CVE IDs with a QVS score that was last modified after a certain date and time. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2021-12-01” or “2021-12-01T23:12:00Z”.
qvs_min={value}	(Optional) Show only CVEs with a QVS value greater than or equal to the QVS min value specified. (QVS Prime will not be considered.) When qvs_min and qvs_max are specified in the same request, the qvs_min value must be less than the qvs_max value.
qvs_max={value}	(Optional) Show only CVEs with a QVS value less than or equal to the QVS max value specified. (QVS Prime will not be considered.) When qvs_min and qvs_max are specified in the same request, the qvs_min value must be less than the qvs_max value.

Parameter	Description
nvd_published_before={date}	(Optional) Show only CVE IDs with a QVS score that was published before a certain date and time. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2021-12-01” or “2021-12-01T23:12:00Z”.
nvd_published_after={date}	(Optional) Show only CVE IDs with a QVS score that was published after a certain date and time. Valid date format is: YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2021-12-01” or “2021-12-01T23:12:00Z”.

Sample KnowledgeBase QVS Download

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
"https://qualysapi.qualys.com/api/2.0/fo/knowledge_base/qvs/?action=list&
cve=CVE-2021-36765,CVE-2021-
36798&qvs_min=1&qvs_max=100&qvs_last_modified_after=2016-12-
16T05:00:17Z&qvs_last_modified_before=2022-01-
20T05:00:17Z&nvd_published_after=2016-12-
16T05:00:17Z&nvd_published_before=2022-12-16T05:00:17Z&details=All"
```

JSON output:


```
{
"CVE-2021-36765": {
"base": {
"id": "CVE-2021-36765",
"idType": "CVE",
"qvs": "28",
"qvsLastChangedDate": 1642032000,
"nvdPublishedDate": 1628086500
},
"contributingFactors": {
"cvss": "5",
"cvssVersion": "v2"
}
},
"CVE-2021-36798": {
"base": {
"id": "CVE-2021-36798",
"idType": "CVE",
"qvs": "78",
"qvsLastChangedDate": 1642550400,
"nvdPublishedDate": 1628514900
},
"contributingFactors": {
"cvss": "5",
"cvssVersion": "v2",
```

```
"exploitMaturity": [
"poc"
]
}
}
}
```

Updates to Host Based Scan Reports

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

We added new risk scores to Host Based Scan Reports, including Asset Risk Score (ARS), Asset Criticality Score (ACS) and Qualys Detection Score (QDS). These values appear in all report formats, including XML and CSV. You can download reports from the UI or fetch reports using the API.

Download Host Based Scan Report in CSV Format

In this sample, we're downloading a Host Based Scan Report in CSV format. You'll see the new column headers "QDS", "ARS" and "ACS".

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"https://qualysapi.qualys.com/api/2.0/fo/report/?action=fetch&id=123457"
```

CSV output:

```
"Sample Report","05/24/2022 at 18:17:24 (GMT-0800)"
"Qualys","919 E Hillsdale Blvd",,"Foster City","California","United
States of America","94404"
"Joe User","joe_user","Manager"

...

"IP","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","Threat","Impact","Solution","Exploitability","Associated
Malware","Results","PCI Vuln","Ticket State","Instance","OS
CPE","Category","Associated Ags","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","QDS","ARS","ACS"
"10.20.30.40","10-20-30-40.bogus.tld",,,,"DNS",,"host scanned, found
vuln","100021","Microsoft Internet Explorer TABLE Status Bar URI
Obfuscation Weakness","New","Vuln","2",,,,,"05/24/2022
```

```
10:07:23","05/24/2022 10:07:23","1",,,,,"CVE-2005-
4679",,"11561","Microsoft Internet Explorer is reported prone to a URI
obfuscation weakness. The issue presents itself when a HREF tag contains
an additional HREF tag contained within a TABLE tag. It is reported that
hovering over the link of the second HREF tag will display the hostname
address of the first HREF tag in the status bar of Internet Explorer.

This weakness is reported to affect Internet Explorer 6, but other
versions may also be affected. Windows XP Service Pack 2 is not reported
to be vulnerable.","This issue may be leveraged by an attacker to display
false information in the status bar of an unsuspecting user, allowing an
attacker to present Web pages to users that seem to originate from a
trusted location. This may facilitate phishing style attacks. Other
attacks may also be possible.","This vulnerability is not exploitable with
Windows XP Service Pack 2. There are no solutions available at this time
for Windows 2000 or Windows XP Service Pack 1.",,,,"yes",,,,"Internet
Explorer",,,,,,,,,"[]",,,,,,,,,,,"2685870","14617851","28","104","4"

...
```

Download Host Based Scan Report in XML Format

In this sample, we're downloading a Host Based Scan Report in XML format. You'll see <ARS> and <ACS> as part of Host details, and you'll see <QDS> as part of Vuln Info.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"https://qualysapi.qualys.com/api/2.0/fo/report/?action=fetch&id=123456"
```

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 ]]>
    </COMPANY>
    <USERNAME>joe_user</USERNAME>
    <GENERATION_DATETIME>2022-05-24T15:30:56Z</GENERATION_DATETIME>
    <TEMPLATE>
      <![CDATA[ ARS_Report ]]>
    </TEMPLATE>
    <TARGET>
      <USER_IP_LIST>
        <RANGE>
          <START>10.20.30.40</START>
          <END>10.20.30.40</END>
```

```
          </RANGE>
        </USER_IP_LIST>
        <COMBINED_IP_LIST>
          <RANGE>
            <START>10.20.30.40</START>
            <END>10.20.30.40</END>
          </RANGE>
        </COMBINED_IP_LIST>
      </TARGET>
      <RISK_SCORE_SUMMARY>
        <TOTAL_VULNERABILITIES>5</TOTAL_VULNERABILITIES>
        <AVG_SECURITY_RISK>2.2</AVG_SECURITY_RISK>
        <BUSINESS_RISK>10/100</BUSINESS_RISK>
      </RISK_SCORE_SUMMARY>
    </HEADER>
    <RISK_SCORE_PER_HOST>
      <HOSTS>
        <IP_ADDRESS>10.20.30.40</IP_ADDRESS>
        <TOTAL_VULNERABILITIES>5</TOTAL_VULNERABILITIES>
        <SECURITY_RISK>2.2</SECURITY_RISK>
      </HOSTS>
    </RISK_SCORE_PER_HOST>
    <HOST_LIST>
      <HOST>
        <IP>10.20.30.40</IP>
        <TRACKING_METHOD>DNS</TRACKING_METHOD>
        <HOST_ID>2685870</HOST_ID>
        <ASSET_ID>14617851</ASSET_ID>
        <DNS>
          <![CDATA[ 10-20-30-40.bogus.tld ]]>
        </DNS>
        <ARS>104</ARS>
        <ACS>4</ACS>
        <VULN_INFO_LIST>
          <VULN_INFO>
            <QID id="qid_100027">100027</QID>
            <TYPE>Practice</TYPE>
            <SSL>false</SSL>
            <FIRST_FOUND>2022-05-24T04:37:23Z</FIRST_FOUND>
            <LAST_FOUND>2022-05-24T04:37:23Z</LAST_FOUND>
            <TIMES_FOUND>1</TIMES_FOUND>
            <VULN_STATUS>New</VULN_STATUS>
            <QDS>
              <![CDATA[ 32 ]]>
            </QDS>
          </VULN_INFO>
...
```

DTD update:

We updated the DTD for Host Based Scan Reports 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?))>

...

<!-- HOST_LIST -->

<!ELEMENT HOST_LIST (HOST+)>

<!ELEMENT HOST (ERROR | (IP?,IPV6?, TRACKING_METHOD, ASSET_TAGS?, HOST_ID,
ASSET_ID?, DNS?, NETBIOS?, QG_HOSTID?, CLOUD_PROVIDER?,
CLOUD_PROVIDER_SERVICE?, CLOUD_SERVICE?, CLOUD_RESOURCE_TYPE?,
CLOUD_RESOURCE_ID?, CLOUD_ACCOUNT?, EC2_INSTANCE_ID?, CLOUD_IMAGE_ID?,
IP_INTERFACES?,EC2_INFO?, CLOUD_RESOURCE_METADATA?, AZURE_VM_INFO?,
OPERATING_SYSTEM?, OS_CPE?, ARS?, ACS?, ASSET_GROUPS?, VULN_INFO_LIST?))>

<!ELEMENT IP (#PCDATA)>
<!ELEMENT IPV6 (#PCDATA)>
<!ATTLIST IP
  network_id  CDATA  #IMPLIED
  v6  CDATA  #IMPLIED
>
<!ATTLIST IPV6
network_id  CDATA  #IMPLIED
v6  CDATA  #IMPLIED
>
<!ELEMENT TRACKING_METHOD (#PCDATA)>
<!ELEMENT ASSET_TAGS (ASSET_TAG+)>
<!ELEMENT ASSET_TAG (#PCDATA)>

<!ELEMENT HOST_ID (#PCDATA)>
<!ELEMENT ASSET_ID (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT QG_HOSTID (#PCDATA)>
<!ELEMENT CLOUD_PROVIDER (#PCDATA)>
<!ELEMENT CLOUD_PROVIDER_SERVICE (#PCDATA)>
<!ELEMENT CLOUD_SERVICE (#PCDATA)>
<!ELEMENT CLOUD_RESOURCE_TYPE (#PCDATA)>
<!ELEMENT CLOUD_RESOURCE_ID (#PCDATA)>
```

```
<!ELEMENT CLOUD_ACCOUNT (#PCDATA)>
<!ELEMENT EC2_INSTANCE_ID (#PCDATA)>
<!ELEMENT CLOUD_IMAGE_ID (#PCDATA)>
<!ELEMENT IP_INTERFACES (IP*)>
<!ELEMENT EC2_INFO
(PUBLIC_DNS_NAME?,IMAGE_ID?,VPC_ID?,INSTANCE_STATE?,PRIVATE_DNS_NAME?,INS
TANCE_TYPE?, ACCOUNT_ID?, REGION_CODE?, SUBNET_ID?)>
<!ELEMENT CLOUD_RESOURCE_METADATA (INSTANCE_ID?, PUBLIC_DNS_NAME?,
VM_ID?, VM_NAME?, PLATFORM?, HOST_NAME?, MACHINE_TYPE?,
MACHINE_STATE?, PROJECT_ID?, PUBLIC_IP_ADDRESS?, VPC_NETWORK?, ZONE?,
IMAGE_OFFER?, IMAGE_PUBLISHER?,
IMAGE_VERSION?, SUBNET?, VM_STATE?, PRIVATE_IP_ADDRESS?, IMAGE_ID?,
SPOT_INSTANCE?, AVAILABILITY_ZONE?, VPC_ID?, GROUP_ID?, GROUP_NAME?,
LOCAL_HOSTNAME?, INSTANCE_STATE?, PRIVATE_DNS_NAME?, INSTANCE_TYPE?,
ACCOUNT_ID?, REGION_CODE?, SUBNET_ID?, RESERVATION_ID?,
SIZE?, SUBSCRIPTION_ID?, LOCATION?, RESOURCE_GROUP_NAME?, MAC_ADDRESS?)>
<!ELEMENT AZURE_VM_INFO
(PUBLIC_IP_ADDRESS?,IMAGE_OFFER?,IMAGE_VERSION?,SUBNET?,VM_STATE?,PRIVATE
_IP_ADDRESS?,SIZE?, SUBSCRIPTION_ID?, LOCATION?, RESOURCE_GROUP_NAME?)>
<!ELEMENT INSTANCE_ID (#PCDATA)>
<!ELEMENT PUBLIC_DNS_NAME (#PCDATA)>
<!ELEMENT IMAGE_ID (#PCDATA)>
<!ELEMENT SPOT_INSTANCE (#PCDATA)>
<!ELEMENT AVAILABILITY_ZONE (#PCDATA)>
<!ELEMENT VPC_ID (#PCDATA)>
<!ELEMENT GROUP_ID (#PCDATA)>
<!ELEMENT GROUP_NAME (#PCDATA)>
<!ELEMENT INSTANCE_STATE (#PCDATA)>
<!ELEMENT LOCAL_HOSTNAME (#PCDATA)>
<!ELEMENT PRIVATE_DNS_NAME (#PCDATA)>
<!ELEMENT INSTANCE_TYPE (#PCDATA)>
<!ELEMENT ACCOUNT_ID (#PCDATA)>
<!ELEMENT REGION_CODE (#PCDATA)>
<!ELEMENT SUBNET_ID (#PCDATA)>
<!ELEMENT RESERVATION_ID (#PCDATA)>
<!ELEMENT MAC_ADDRESS (#PCDATA)>
<!ELEMENT OPERATING_SYSTEM (#PCDATA)>
<!ELEMENT VM_ID (#PCDATA)>
<!ELEMENT VM_NAME (#PCDATA)>
<!ELEMENT PLATFORM (#PCDATA)>
<!ELEMENT HOST_NAME (#PCDATA)>
<!ELEMENT MACHINE_TYPE (#PCDATA)>
<!ELEMENT MACHINE_STATE (#PCDATA)>
<!ELEMENT PROJECT_ID (#PCDATA)>
<!ELEMENT PUBLIC_IP_ADDRESS (#PCDATA)>
<!ELEMENT VPC_NETWORK (#PCDATA)>
<!ELEMENT ZONE (#PCDATA)>
<!ELEMENT IMAGE_OFFER (#PCDATA)>
<!ELEMENT IMAGE_PUBLISHER (#PCDATA)>
```

```
<!ELEMENT IMAGE_VERSION (#PCDATA)>
<!ELEMENT SUBNET (#PCDATA)>
<!ELEMENT VM_STATE (#PCDATA)>
<!ELEMENT PRIVATE_IP_ADDRESS (#PCDATA)>
<!ELEMENT SIZE (#PCDATA)>
<!ELEMENT SUBSCRIPTION_ID (#PCDATA)>
<!ELEMENT LOCATION (#PCDATA)>
<!ELEMENT RESOURCE_GROUP_NAME (#PCDATA)>
<!ELEMENT OS_CPE (#PCDATA)>
<!ELEMENT ARS (#PCDATA)>
<!ELEMENT ACS (#PCDATA)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP_TITLE+)>
<!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?, TICKET_NUMBER?,
TICKET_STATE?, ASSET_CVE?, QDS?)>

<!ELEMENT QID (#PCDATA)>
<!ATTLIST QID id CDATA #REQUIRED>

<!ELEMENT TYPE (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT SERVICE (#PCDATA)>
<!ELEMENT FQDN (#PCDATA)>
<!ELEMENT PROTOCOL (#PCDATA)>
<!ELEMENT SSL (#PCDATA)>

<!ELEMENT RESULT (#PCDATA)>
<!ATTLIST RESULT format CDATA #IMPLIED>

<!ELEMENT FIRST_FOUND (#PCDATA)>
<!ELEMENT LAST_FOUND (#PCDATA)>
<!ELEMENT TIMES_FOUND (#PCDATA)>
<!-- Note: VULN_STATUS is N/A for IGs -->
<!ELEMENT VULN_STATUS (#PCDATA)>
<!ELEMENT ASSET_CVE (#PCDATA)>
<!ELEMENT LAST_FIXED (#PCDATA)>
<!ELEMENT FIRST_REOPENED (#PCDATA)>
<!ELEMENT LAST_REOPENED (#PCDATA)>
<!ELEMENT TIMES_REOPENED (#PCDATA)>
<!ELEMENT CVSS_FINAL (#PCDATA)>
<!ELEMENT CVSS3_FINAL (#PCDATA)>
<!ELEMENT TICKET_NUMBER (#PCDATA)>
<!ELEMENT TICKET_STATE (#PCDATA)>
<!ELEMENT QDS (#PCDATA)>
...
```

Issues Addressed

- We increased the number of characters allowed for the “password” input parameter for several authentication record types when creating authentication records using the API, making it consistent with the number of characters allowed when creating records from the UI.
- We improved performance for scans launched using the Scan Launch API.