Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.16

November 10, 2021 (Updated December 13, 2021)

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.

STIG ID added to STIG Based Report (CSV Format)

APIs affected	/api/2.0/fo/report/?action=fetch
New or Updated API	No (affects CSV report output only)
DTD or XSD changes	No

Now when you run the Compliance STIG Based Report from the UI, you'll see STIG IDs in the CSV report output. This allows you to sort STIG requirements by STIG ID. There is a one-to-one mapping between a STIG ID and a STIG Rule/Rule ID. This advanced notification is intended to inform you of new CSV columns in the report, so you can make any changes necessary to correctly parse the report data.

In the CSV report, you'll see a new STIG ID column in the following sections:

- STIG ID appears as the first column in the RULE STATISTICS section

- STIG ID appears before Rule ID in the RESULTS section

- STIG ID appears before Rule in the APPENDIX section (part of STIG Framework details)

Download STIG Based Report

You can download a STIG Based Report from the UI or fetch a saved report using the API. Specify action=fetch and provide the ID for the saved report you want to download.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"https://qualysapi.qualys.com/api/2.0/fo/report/?action=fetch&id=941401"
```

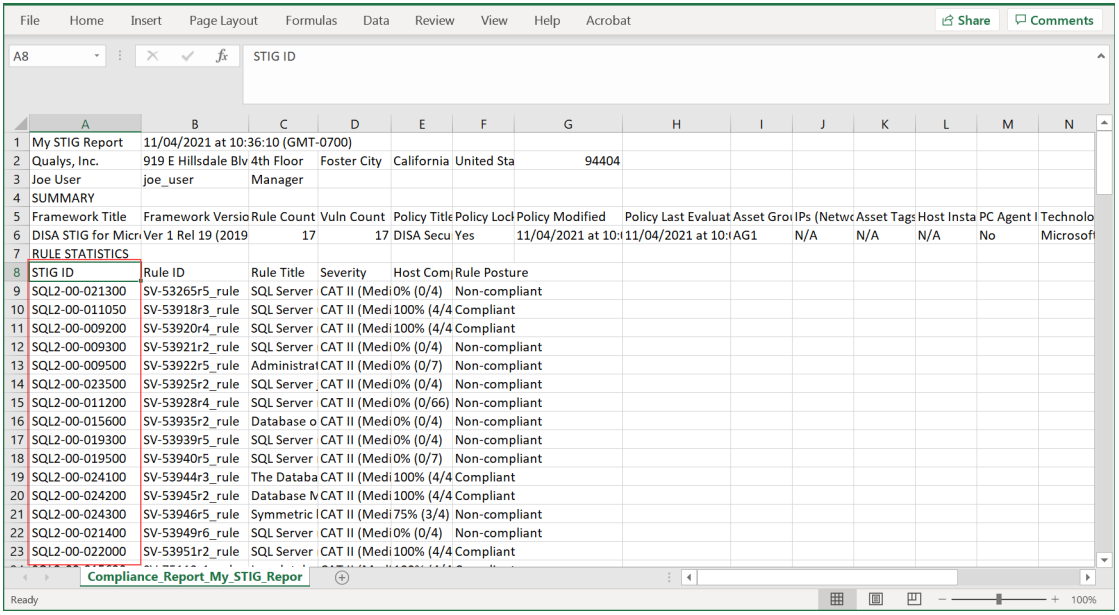
CSV output:

See the sample report below.

Sample STIG Based Report

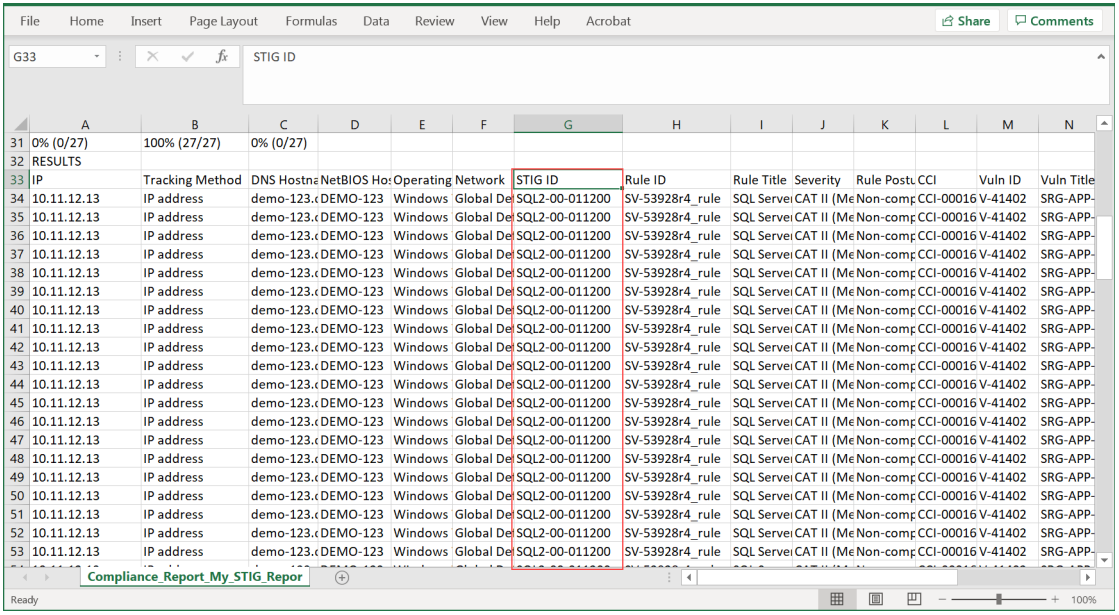
Here are clips from a sample STIG Based Report in CSV format, showing the new STIG ID columns. Run your own report to see all the columns in the CSV report output.

RULE STATISTICS section



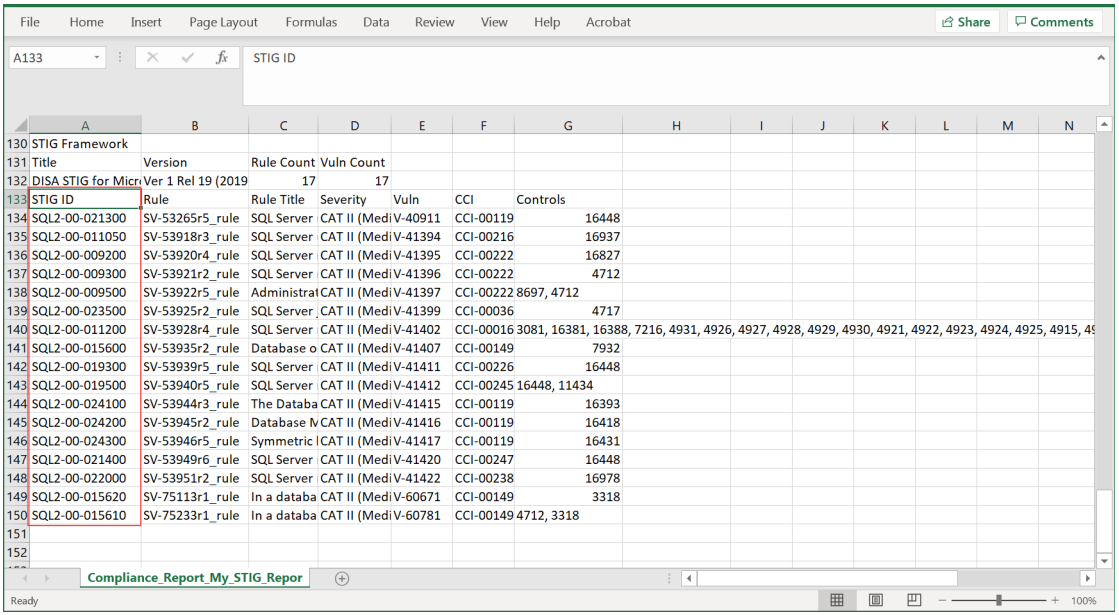
	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	My STIG Report	11/04/2021 at 10:36:10 (GMT-0700)												
2	Qualys, Inc.	919 E Hillsdale Blv	4th Floor	Foster City	California	United Sta	94404							
3	Joe User	joe_user	Manager											
4	SUMMARY													
5	Framework Title	Framework Versio	Rule Count	Vuln Count	Policy Title	Policy Loc	Policy Modified	Policy Last Evaluat	Asset Gro	IPs (Netwo	Asset Tags	Host Insta	PC Agent I	Technolo
6	DISA STIG for Micr	Ver 1 Rel 19 (2019	17	17	DISA Secu	Yes	11/04/2021 at 10:	11/04/2021 at 10:	AG1	N/A	N/A	N/A	No	Microsof
7	RULE STATISTICS													
8	STIG ID	Rule ID	Rule Title	Severity	Host Com	Rule Posture								
9	SQL2-00-021300	SV-53265r5_rule	SQL Server	CAT II (Medi	0% (0/4)	Non-compliant								
10	SQL2-00-011050	SV-53918r3_rule	SQL Server	CAT II (Medi	100% (4/4	Compliant								
11	SQL2-00-009200	SV-53920r4_rule	SQL Server	CAT II (Medi	100% (4/4	Compliant								
12	SQL2-00-009300	SV-53921r2_rule	SQL Server	CAT II (Medi	0% (0/4)	Non-compliant								
13	SQL2-00-009500	SV-53922r5_rule	Administrat	CAT II (Medi	0% (0/7)	Non-compliant								
14	SQL2-00-023500	SV-53925r2_rule	SQL Server	CAT II (Medi	0% (0/4)	Non-compliant								
15	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Medi	0% (0/66)	Non-compliant								
16	SQL2-00-015600	SV-53935r2_rule	Database o	CAT II (Medi	0% (0/4)	Non-compliant								
17	SQL2-00-019300	SV-53939r5_rule	SQL Server	CAT II (Medi	0% (0/4)	Non-compliant								
18	SQL2-00-019500	SV-53940r5_rule	SQL Server	CAT II (Medi	0% (0/7)	Non-compliant								
19	SQL2-00-024100	SV-53944r3_rule	The Databa	CAT II (Medi	100% (4/4	Compliant								
20	SQL2-00-024200	SV-53945r2_rule	Database M	CAT II (Medi	100% (4/4	Compliant								
21	SQL2-00-024300	SV-53946r5_rule	Symmetric	CAT II (Medi	75% (3/4)	Non-compliant								
22	SQL2-00-021400	SV-53949r6_rule	SQL Server	CAT II (Medi	0% (0/4)	Non-compliant								
23	SQL2-00-022000	SV-53951r2_rule	SQL Server	CAT II (Medi	100% (4/4	Compliant								

RESULTS section



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
31	0% (0/27)	100% (27/27)	0% (0/27)											
32	RESULTS													
33	IP	Tracking Method	DNS Hostna	NetBIOS Hos	Operating	Network	STIG ID	Rule ID	Rule Title	Severity	Rule Postu	CCI	Vuln ID	Vuln Title
34	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
35	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
36	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
37	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
38	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
39	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
40	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
41	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
42	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
43	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
44	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
45	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
46	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
47	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
48	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
49	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
50	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
51	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
52	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-
53	10.11.12.13	IP address	demo-123.(	DEMO-123	Windows	Global De	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Me	Non-comp	CCI-00016	V-41402	SRG-APP-

APPENDIX section



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
130	STIG Framework													
131	Title	Version	Rule Count	Vuln Count										
132	DISA STIG for Micr	Ver 1 Rel 19 (2019	17	17										
133	STIG ID	Rule	Rule Title	Severity	Vuln	CCI	Controls							
134	SQL2-00-021300	SV-53265r5_rule	SQL Server	CAT II (Medi	V-40911	CCI-00119	16448							
135	SQL2-00-011050	SV-53918r3_rule	SQL Server	CAT II (Medi	V-41394	CCI-00216	16937							
136	SQL2-00-009200	SV-53920r4_rule	SQL Server	CAT II (Medi	V-41395	CCI-00222	16827							
137	SQL2-00-009300	SV-53921r2_rule	SQL Server	CAT II (Medi	V-41396	CCI-00222	4712							
138	SQL2-00-009500	SV-53922r5_rule	Administrat	CAT II (Medi	V-41397	CCI-00222	8697, 4712							
139	SQL2-00-023500	SV-53925r2_rule	SQL Server	CAT II (Medi	V-41399	CCI-00036	4717							
140	SQL2-00-011200	SV-53928r4_rule	SQL Server	CAT II (Medi	V-41402	CCI-00016	3081, 16381, 16388, 7216, 4931, 4926, 4927, 4928, 4929, 4930, 4921, 4922, 4923, 4924, 4925, 4915, 4							
141	SQL2-00-015600	SV-53935r2_rule	Database o	CAT II (Medi	V-41407	CCI-00149	7932							
142	SQL2-00-019300	SV-53939r5_rule	SQL Server	CAT II (Medi	V-41411	CCI-00226	16448							
143	SQL2-00-019500	SV-53940r5_rule	SQL Server	CAT II (Medi	V-41412	CCI-00245	16448, 11434							
144	SQL2-00-024100	SV-53944r3_rule	The Databa	CAT II (Medi	V-41415	CCI-00119	16393							
145	SQL2-00-024200	SV-53945r2_rule	Database M	CAT II (Medi	V-41416	CCI-00119	16418							
146	SQL2-00-024300	SV-53946r5_rule	Symmetric I	CAT II (Medi	V-41417	CCI-00119	16431							
147	SQL2-00-021400	SV-53949r6_rule	SQL Server	CAT II (Medi	V-41420	CCI-00247	16448							
148	SQL2-00-022000	SV-53951r2_rule	SQL Server	CAT II (Medi	V-41422	CCI-00238	16978							
149	SQL2-00-015620	SV-75113r1_rule	In a databa	CAT II (Medi	V-60671	CCI-00149	3318							
150	SQL2-00-015610	SV-75233r1_rule	In a databa	CAT II (Medi	V-60781	CCI-00149	4712, 3318							
151														
152														

API Vault Support added for IBM DB2 Authentication Records

APIs affected	/api/2.0/fo/auth/ibm_db2/
New or Updated API	Updated
DTD or XSD changes	Yes

We already support vaults for IBM DB2 authentication records from the UI. Starting in this release, we'll also support vaults for IBM DB2 authentication records from the API. This means that you can specify a vault when creating/updating a IBM DB2 authentication record using the API and you'll see vault information when listing records using the API.

Create/Update IBM DB2 Authentication Record

Use vault input parameters when creating/updating IBM DB2 authentication records. Refer to the Qualys API (VM,PC) User Guide for details on all available input parameters.

Parameter	Description
login_type={basic|vault}	(Optional) The login type is basic by default. Specify login_type=vault to use a third party vault to retrieve the password for authentication. Vault parameters need to be provided in the record.
vault_id={value}	(Required only when action=create and login_type=vault) The ID of the vault you want to use to retrieve the password for login.
vault_type={value}	(Required only when action=create and login_type=vault) The third party vault to be used to retrieve the password for login. Certain vaults support this capability. See "Vault Support Matrix" in the API User Guide. The following vault types are supported for IBM DB2 at this time: ARCON PAM, CA Access Control, CyberArk AIM, CyberArk PIM Suite, HashiCorp, Lieberman ERPM, Quest Vault, Thycotic Secret Server
{vault parameters}	(Required only when action=create and login_type=vault) Vault specific parameters required depend on the vault type you've selected. See "Vault Definition" in the API User Guide to know which parameters are required for each vault type.

Sample Create IBM DB2 Record with Vault

In this sample, we're creating a new record and specifying a CyberArk AIM vault.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=create&title=MyDB2Record&username=joe_user&login_type=vault&vault
_id=45014&vault_type=CyberArk
AIM&folder=Root\Windows7&file=rd.txt&database=db2&port=1234&ips=10.11.12.
13" "https://qualysapi.qualys.com/api/2.0/fo/auth/ibm_db2/"
```

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>2021-10-11T11:48:03Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>112491</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample Update IBM DB2 Record with Vault

In this sample, we're updating an existing record and specifying a CyberArk AIM vault.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=update&ids=112491&title=MyDB2Record&username=joe_user&login_type=
vault&vault_id=45014&vault_type=CyberArk
AIM&folder=Root\Windows7&file=rd.txt&database=db2&port=1234&ips=10.11.12.
13" "https://qualysapi.qualys.com/api/2.0/fo/auth/ibm_db2/"
```

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>2021-11-02T06:25:35Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>112491</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

List IBM DB2 Authentication Records

When you list IBM DB2 records, you'll see vault details in the output, when applicable.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=list&ids=112491"
"https://qualysapi.qualys.com/api/2.0/fo/auth/ibm_db2/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_IBM_DB2_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/ibm_db2/auth_ibm_db2_list_o
utput.dtd">
<AUTH_IBM_DB2_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-10-11T11:49:11Z</DATETIME>
    <AUTH_IBM_DB2_LIST>
      <AUTH_IBM_DB2>
        <ID>112491</ID>
        <TITLE><![CDATA[MyDB2Record]]></TITLE>
        <USERNAME><![CDATA[joe_user]]></USERNAME>
        <DATABASE><![CDATA[db2]]></DATABASE>
        <PORT>1234</PORT>
        <IP_SET>
          <IP>10.11.12.13</IP>
        </IP_SET>
        <LOGIN_TYPE><![CDATA[vault]]></LOGIN_TYPE>
        <DIGITAL_VAULT>
          <DIGITAL_VAULT_ID><![CDATA[45014]]></DIGITAL_VAULT_ID>
          <DIGITAL_VAULT_TYPE><![CDATA[CyberArk
AIM]]></DIGITAL_VAULT_TYPE>
          <DIGITAL_VAULT_TITLE><![CDATA[MyVault]]></DIGITAL_VAULT_TITLE>
          <VAULT_FOLDER><![CDATA[Root\Windows7]]></VAULT_FOLDER>
          <VAULT_FILE><![CDATA[rd.txt]]></VAULT_FILE>
        </DIGITAL_VAULT>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2021-10-11T11:48:03Z</DATETIME>
          <BY>joe_user</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2021-10-11T11:48:03Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_IBM_DB2>
    </AUTH_IBM_DB2_LIST>
  </RESPONSE>
</AUTH_IBM_DB2_LIST_OUTPUT>
```

DTD update:

We updated the DTD for IBM DB2 List Output to include new elements (in bold).

DTD: <platform>/api/2.0/fo/auth/ibm_db2/auth_ibm_db2_list_output.dtd

```
<!-- QUALYS AUTH_DB2_LIST_OUTPUT DTD -->
<!-- $Revision: $ -->
<!ELEMENT AUTH_IBM_DB2_LIST_OUTPUT (REQUEST?, RESPONSE)>

...

<!ELEMENT AUTH_IBM_DB2 (ID, TITLE, USERNAME, DATABASE, PORT, IP_SET?,
PC_ONLY?, LOGIN_TYPE?, DIGITAL_VAULT?, NETWORK_ID?, CREATED,
LAST_MODIFIED, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT DATABASE (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT LOGIN_TYPE (#PCDATA)>
<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_FOLDER?, VAULT_FILE?, VAULT_SECRET_NAME?,
VAULT_SYSTEM_NAME?, VAULT_EP_NAME?, VAULT_EP_TYPE?, VAULT_EP_CONT?,
VAULT_NS_TYPE?, VAULT_NS_NAME?, VAULT_ACCOUNT_NAME?)>
<!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_EP_NAME (#PCDATA)>
<!ELEMENT VAULT_EP_TYPE (#PCDATA)>
<!ELEMENT VAULT_EP_CONT (#PCDATA)>
<!ELEMENT VAULT_NS_TYPE (#PCDATA)>
<!ELEMENT VAULT_NS_NAME (#PCDATA)>
<!ELEMENT VAULT_ACCOUNT_NAME (#PCDATA)>

 ...
```

Updates to Cloud Asset Metadata Fields in Host Based Scan Reports

APIs affected	/api/2.0/fo/report/
New or Updated API	Updated
DTD or XSD changes	Yes
APIs affected	/api/2.0/fo/report/template/scan/
New or Updated API	Updated
DTD or XSD changes	No

We made several updates related to cloud asset metadata shown in Host Based Scan Reports. Please note the following changes:

- We will now show cloud asset metadata for GCP (Google Cloud Platform).

- The cloud asset metadata fields have been split into 2 categories: Legacy EC2/Azure Fields and Cloud Provider Metadata Fields. The Legacy EC2/Azure Fields include cloud provider specific metadata fields originally introduced for AWS and Azure. The Cloud Provider Metadata Fields include general fields that apply to all cloud providers, including AWS, Azure, GCP and future support. You can choose whether to display Legacy EC2/Azure Fields, Cloud Provider Metadata Fields, or both sets of fields in Host Based Scan Reports. From the UI, edit the scan report template and make your selection on the Display tab. When creating/updating the scan report templates using the API, specify the new input parameter “cloud_provider_metadata=1” to display Cloud Provider Metadata fields in your report. Use the existing input “metadata_ec2_instance=1” to display Legacy EC2/Azure fields in your report.

- We’ll automatically update your existing scan report templates to use the new options. If you had the “Cloud Related Information” template option selected prior to this release, then we’ll select the “Legacy EC2/Azure Fields” option. If your subscription had the “Cloud Perimeter Azure VM Scan” feature enabled, then we will also select the “Cloud Provider Metadata Fields” option. Edit your scan report template to change these settings.

- For XML reports, we added a new tag CLOUD_RESOURCE_METADATA for all cloud providers. For AWS/Azure, this will include the same content as EC2_INFO and AZURE_VM_INFO, plus more metadata added in this release. For CSV reports, additional metadata will appear in the existing Cloud Resource Metadata column. This field (for XML and CSV) only appears when Cloud Provider Metadata Fields is selected in the template.

- We added the new field Cloud Provider Service. This will appear when Cloud Provider Metadata Fields is selected in the template. It will also appear in XML reports for AWS and Azure assets when Legacy EC2/Azure Fields is selected. The Cloud Provider Service field will replace the existing Cloud Service field in a future release. For AWS, you’ll see “EC2”

for Cloud Provider Service/Cloud Service. For Azure, you'll see "VM" for Cloud Provider Service/Cloud Service. For GCP, you'll see "Compute Engine" for Cloud Provider Service and "VM Instance" for Cloud Service.

- We added the fields Cloud Resource Type and Cloud Image ID. These fields will only appear when Cloud Provider Metadata Fields is selected in the template.

- In CSV output, we changed the order of the columns. When all fields are included in the report, the Cloud Resource Metadata column is no longer the last column in the report. It appears before the Legacy EC2/Azure fields.

- We dropped certain requirements for displaying cloud related information in reports. Users no longer need the "EC2 Scanning" feature enabled for their subscription in order to include cloud related information in Host Based Scan Reports. Also, users no longer need the "Cloud Perimeter Azure VM Scan" feature enabled for their subscription in order to display the general cloud provider metadata fields in the CSV format of the report.

Cloud Asset Metadata Fields in CSV Format

See the table below to know which cloud asset metadata columns will appear in your CSV reports based on your report template settings. Columns will appear in the order shown.

Legacy EC2/Azure Fields	Cloud Provider Metadata Fields	All Fields
EC2 Instance ID	Cloud Provider	Cloud Provider
Public Hostname	Cloud Provider Service	Cloud Provider Service
Image ID	Cloud Service	Cloud Service
VPC ID	Cloud Resource ID	Cloud Resource ID
Instance State	Cloud Resource Type	Cloud Resource Type
Private Hostname	Cloud Account	Cloud Account
Instance Type	Cloud Image ID	Cloud Image ID
Account ID	Cloud Resource Metadata	Cloud Resource Metadata
Region Code		EC2 Instance ID
Subnet ID		Public Hostname
		Image ID
		VPC ID
		Instance State
		Private Hostname
		Instance Type
		Account ID
		Region Code
		Subnet ID

Important note about the Legacy EC2/Azure Fields in CSV

These fields were originally introduced for AWS cloud assets and will be populated with metadata for your AWS EC2 assets.

For Azure and GCP assets, all Legacy EC2/Azure columns will appear blank in the CSV report, except for the EC2 Instance ID column. We will continue to populate the EC2 Instance ID column for all cloud assets (AWS, Azure, GCP). The EC2 Instance ID column is replaced by Cloud Resource ID, and will be deprecated in a future release.

Cloud Asset Metadata Fields in XML Format

See the table below to know which cloud asset metadata tags will appear in your XML reports based on your report template settings.

Cloud Provider	Legacy EC2/Azure Fields	Cloud Provider Metadata Fields	All Fields
AWS	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID EC2_INFO	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE, CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE, CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID CLOUD_IMAGE_ID EC2_INFO CLOUD_RESOURCE_METADATA
Azure	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID AZURE_VM_INFO	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE, CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID CLOUD_IMAGE_ID AZURE_VM_INFO CLOUD_RESOURCE_METADATA
GCP	CLOUD_RESOURCE_ID EC2_INSTANCE_ID	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA	CLOUD_PROVIDER CLOUD_PROVIDER_SERVICE CLOUD_SERVICE CLOUD_RESOURCE_TYPE CLOUD_RESOURCE_ID CLOUD_ACCOUNT EC2_INSTANCE_ID CLOUD_IMAGE_ID CLOUD_RESOURCE_METADATA

EC2_INFO includes: PUBLIC_DNS_NAME, IMAGE_ID, VPC_ID, INSTANCE_STATE, PRIVATE_DNS_NAME, INSTANCE_TYPE, ACCOUNT_ID, REGION_CODE, SUBNET_ID

AZURE_VM_INFO includes: PUBLIC_IP_ADDRESS, IMAGE_OFFER, IMAGE_VERSION, SUBNET, VM_STATE, PRIVATE_IP_ADDRESS, SIZE, SUBSCRIPTON_ID, LOCATION, RESOURCE_GROUP_NAME

CLOUD_RESOURCE_METADATA for AWS includes: INSTANCE_ID, PUBLIC_DNS_NAME, PUBLIC_IP_ADDRESS, 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, MAC_ADDRESS

CLOUD_RESOURCE_METADATA for Azure includes: VM_ID, VM_NAME, PLATFORM, PUBLIC_IP_ADDRESS, IMAGE_OFFER, IMAGE_PUBLISHER, IMAGE_VERSION, SUBNET, VM_STATE, PRIVATE_IP_ADDRESS, SIZE, SUBSCRIPTION_ID, LOCATION, RESOURCE_GROUP_NAME, MAC_ADDRESS

CLOUD_RESOURCE_METADATA for GCP includes: INSTANCE_ID, HOST_NAME, MACHINE_TYPE, MACHINE_STATE, PROJECT_ID, PUBLIC_IP_ADDRESS, VPC_NETWORK, ZONE, PRIVATE_IP_ADDRESS, MAC_ADDRESS

Create/Update Scan Report Template

Use the new template setting "cloud_provider_metadata" for including Cloud Provider Metadata fields in your reports. Use the existing setting "metadata_ec2_instances" to include Legacy EC2/Azure fields in your report. Refer to the Qualys API (VM,PC) User Guide for details on all available template options.

Parameter	Description
metadata_ec2_instances={**0**|1}	Specify 1 to display "Legacy EC2/Azure Fields" for each EC2 asset. See Cloud Asset Metadata Fields in XML Format to know which fields are included with this option.
cloud_provider_metadata={**0**|1}	Specify 1 to display "Cloud Provider Metadata Fields" for each cloud asset. See Cloud Asset Metadata Fields in XML Format to know which fields are included with this option.

Sample Create Scan Template

In this sample, we are creating a new scan report template and including both Legacy EC2/Azure fields and Cloud Provider Metadata fields.

API request:

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

XML payload (template settings):

```
<?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[Cloud_details_enabled_sample1]]></INFO>
      <INFO key="owner"><![CDATA[117600]]></INFO>
    </TITLE>
    <TARGET>
      <INFO key="scan_selection"><![CDATA[HostBased]]></INFO>
      <INFO key="include_trending"><![CDATA[0]]></INFO>
      <INFO key="asset_groups"><![CDATA[]]></INFO>
      <INFO key="tag_set_by"><![CDATA[id]]></INFO>
      <INFO
```

```
key="tag_set_include"><![CDATA[14649606,16944379,14649605]]></INFO>
      <INFO key="tag_set_exclude"><![CDATA[]]></INFO>
      <INFO key="tag_include_selector"><![CDATA[ANY]]></INFO>
      <INFO key="tag_exclude_selector"><![CDATA[ANY]]></INFO>
      <INFO key="network"><![CDATA[0]]></INFO>
      <INFO key="ips"><![CDATA[]]></INFO>
      <INFO key="host_with_cloud_agents"><![CDATA[]]></INFO>
    </TARGET>
    <DISPLAY>
      <INFO key="graph_business_risk"><![CDATA[0]]></INFO>
      <INFO key="graph_vuln_over_time"><![CDATA[0]]></INFO>
      <INFO key="display_text_summary"><![CDATA[1]]></INFO>
      <INFO key="graph_status"><![CDATA[0]]></INFO>
      <INFO key="graph_potential_status"><![CDATA[0]]></INFO>
      <INFO key="graph_severity"><![CDATA[0]]></INFO>
      <INFO key="graph_potential_severity"><![CDATA[0]]></INFO>
      <INFO key="graph_ig_severity"><![CDATA[0]]></INFO>
      <INFO key="graph_top_categories"><![CDATA[0]]></INFO>
      <INFO key="graph_top_vulns"><![CDATA[0]]></INFO>
      <INFO key="graph_os"><![CDATA[0]]></INFO>
      <INFO key="graph_services"><![CDATA[0]]></INFO>
      <INFO key="graph_top_ports"><![CDATA[0]]></INFO>
      <INFO key="display_custom_footer"><![CDATA[0]]></INFO>
      <INFO key="display_custom_footer_text"><![CDATA[]]></INFO>
      <INFO key="sort_by"><![CDATA[host]]></INFO>
      <INFO key="cvss"><![CDATA[all]]></INFO>
      <INFO key="host_details"><![CDATA[0]]></INFO>
      <INFO key="host_ag_details"><![CDATA[1]]></INFO>
      <INFO key="qualys_system_ids"><![CDATA[1]]></INFO>
      <INFO key="include_text_summary"><![CDATA[1]]></INFO>
      <INFO key="include_vuln_details"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_threat"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_impact"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_solution"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_vpatch"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_compliance"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_exploit"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_malware"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_results"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_appendix"><![CDATA[0]]></INFO>
      <INFO key="exclude_account_id"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_reopened"><![CDATA[0]]></INFO>
      <INFO key="metadata_ec2_instances"><![CDATA[1]]></INFO>
      <INFO key="cloud_provider_metadata"><![CDATA[1]]></INFO>
    </DISPLAY>
...
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2021-11-09T17:07:33Z</DATETIME>
        <TEXT>Scan Report Template(s) Successfully Created.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>1279265</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample Update Scan Template

In this sample, we are updating an existing scan report template.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
"https://qualysapi.qualys.com/api/2.0/fo/report/template/scan/?action=upd
ate&report_format=xml&template_id=1279266"
```

XML payload (template settings):

```
<?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[Cloud_details_enabled_sample100]]></INFO>
       <INFO key="owner"><![CDATA[117600]]></INFO>
    </TITLE>
    <TARGET>
      <INFO key="scan_selection"><![CDATA[HostBased]]></INFO>
      <INFO key="include_trending"><![CDATA[0]]></INFO>
      <INFO key="asset_groups"><![CDATA[]]></INFO>
      <INFO key="tag_set_by"><![CDATA[id]]></INFO>
      <INFO
key="tag_set_include"><![CDATA[14649606,16944379,14649605]]></INFO>
      <INFO key="tag_set_exclude"><![CDATA[]]></INFO>
      <INFO key="tag_include_selector"><![CDATA[ANY]]></INFO>
      <INFO key="tag_exclude_selector"><![CDATA[ANY]]></INFO>
```

```
      <INFO key="network"><![CDATA[0]]></INFO>
      <INFO key="ips"><![CDATA[]]></INFO>
      <INFO key="host_with_cloud_agents"><![CDATA[]]></INFO>
    </TARGET>
    <DISPLAY>
      <INFO key="graph_business_risk"><![CDATA[0]]></INFO>
      <INFO key="graph_vuln_over_time"><![CDATA[0]]></INFO>
      <INFO key="display_text_summary"><![CDATA[1]]></INFO>
      <INFO key="graph_status"><![CDATA[0]]></INFO>
      <INFO key="graph_potential_status"><![CDATA[0]]></INFO>
      <INFO key="graph_severity"><![CDATA[0]]></INFO>
      <INFO key="graph_potential_severity"><![CDATA[0]]></INFO>
      <INFO key="graph_ig_severity"><![CDATA[0]]></INFO>
      <INFO key="graph_top_categories"><![CDATA[0]]></INFO>
      <INFO key="graph_top_vulns"><![CDATA[0]]></INFO>
      <INFO key="graph_os"><![CDATA[0]]></INFO>
      <INFO key="graph_services"><![CDATA[0]]></INFO>
      <INFO key="graph_top_ports"><![CDATA[0]]></INFO>
      <INFO key="display_custom_footer"><![CDATA[0]]></INFO>
      <INFO key="display_custom_footer_text"><![CDATA[]]></INFO>
      <INFO key="sort_by"><![CDATA[host]]></INFO>
      <INFO key="cvss"><![CDATA[all]]></INFO>
      <INFO key="host_details"><![CDATA[0]]></INFO>
      <INFO key="host_ag_details"><![CDATA[1]]></INFO>
      <INFO key="qualys_system_ids"><![CDATA[1]]></INFO>
      <INFO key="include_text_summary"><![CDATA[1]]></INFO>
      <INFO key="include_vuln_details"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_threat"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_impact"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_solution"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_vpatch"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_compliance"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_exploit"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_malware"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_results"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_appendix"><![CDATA[0]]></INFO>
      <INFO key="exclude_account_id"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_reopened"><![CDATA[0]]></INFO>
      <INFO key="metadata_ec2_instances"><![CDATA[1]]></INFO>
      <INFO key="cloud_provider_metadata"><![CDATA[1]]></INFO>
    </DISPLAY>
...
```

XML output:

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

```
    <RESPONSE>
        <DATETIME>2021-11-09T17:21:54Z</DATETIME>
        <TEXT>Scan Report Template Successfully Updated.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>1279266</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Export Scan Template

When you export a scan report template, you'll see the new INFO key "cloud_provider_metadata" with a value of 0 or 1 to indicate whether the Cloud Provider Metadata Fields option is enabled in the template. You'll also see the "metadata_ec2_instances" INFO key to indicate whether the Legacy EC2/Azure Fields option is enabled in the template.

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&report_format=xml&template_id=1279256"
```

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="template_id"><![CDATA[1279256]]></INFO>
      <INFO key="title"><![CDATA[Cloud_details_enabled]]></INFO>
      <INFO key="owner"><![CDATA[117600]]></INFO>
    </TITLE>
    <TARGET>
      <INFO key="scan_selection"><![CDATA[HostBased]]></INFO>
      <INFO key="include_trending"><![CDATA[0]]></INFO>
      <INFO key="asset_groups"><![CDATA[]]></INFO>
      <INFO key="tag_set_by"><![CDATA[id]]></INFO>
      <INFO
key="tag_set_include"><![CDATA[14649606,16944379,14649605]]></INFO>
      <INFO key="tag_set_exclude"><![CDATA[]]></INFO>
      <INFO key="tag_include_selector"><![CDATA[ANY]]></INFO>
```

```
      <INFO key="tag_exclude_selector"><![CDATA[ANY]]></INFO>
      <INFO key="network"><![CDATA[0]]></INFO>
      <INFO key="ips"><![CDATA[]]></INFO>
      <INFO key="host_with_cloud_agents"><![CDATA[]]></INFO>
    </TARGET>
    <DISPLAY>
      <INFO key="graph_business_risk"><![CDATA[0]]></INFO>
      <INFO key="graph_vuln_over_time"><![CDATA[0]]></INFO>
      <INFO key="display_text_summary"><![CDATA[1]]></INFO>
      <INFO key="graph_status"><![CDATA[0]]></INFO>
      <INFO key="graph_potential_status"><![CDATA[0]]></INFO>
      <INFO key="graph_severity"><![CDATA[0]]></INFO>
      <INFO key="graph_potential_severity"><![CDATA[0]]></INFO>
      <INFO key="graph_ig_severity"><![CDATA[0]]></INFO>
      <INFO key="graph_top_categories"><![CDATA[0]]></INFO>
      <INFO key="graph_top_vulns"><![CDATA[0]]></INFO>
      <INFO key="graph_os"><![CDATA[0]]></INFO>
      <INFO key="graph_services"><![CDATA[0]]></INFO>
      <INFO key="graph_top_ports"><![CDATA[0]]></INFO>
      <INFO key="display_custom_footer"><![CDATA[0]]></INFO>
      <INFO key="display_custom_footer_text"><![CDATA[]]></INFO>
      <INFO key="sort_by"><![CDATA[host]]></INFO>
      <INFO key="cvss"><![CDATA[all]]></INFO>
      <INFO key="host_details"><![CDATA[0]]></INFO>
      <INFO key="host_ag_details"><![CDATA[1]]></INFO>
      <INFO key="qualys_system_ids"><![CDATA[1]]></INFO>
      <INFO key="include_text_summary"><![CDATA[1]]></INFO>
      <INFO key="include_vuln_details"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_threat"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_impact"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_solution"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_vpatch"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_compliance"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_exploit"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_malware"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_results"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_appendix"><![CDATA[0]]></INFO>
      <INFO key="exclude_account_id"><![CDATA[0]]></INFO>
      <INFO key="include_vuln_details_reopened"><![CDATA[0]]></INFO>
      <INFO key="metadata_ec2_instances"><![CDATA[1]]></INFO>
      <INFO key="cloud_provider_metadata"><![CDATA[1]]></INFO>
    </DISPLAY>
...
```

Download Host Based Scan Report in CSV Format

In this sample, we're downloading a Host Based Scan Report in CSV format. The report includes Legacy EC2/Azure fields and Cloud Provider Metadata fields. This sample has an AWS asset, Azure asset and GCP asset.

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","11/09/2021 at 09:45:52 (GMT-0800)"
"Qualys","919 E Hillsdale Blvd",,"Foster City","California","United
States of America","94404"
"Joe User","joe_user","Manager"

"Asset Groups","IPs","Active Hosts","Hosts Matching Filters","Trend
Analysis","Date Range","Network"
"NONE","10.4.5.6,10.11.12.13,10.90.100.110","3","3","Latest vulnerability
data","12/31/1998 - 11/09/2021","All"

"Total Vulnerabilities","Avg Security Risk","Business Risk"
"104","3.7","18/100"

"IP","Network","Total Vulnerabilities","Security Risk"
"10.11.12.13","test network","70","3.1"
"10.90.100.110","test network","6","5.0"
"10.4.5.6","test network","28","3.0"


"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","Threat","Impact","Solution","Exploitability","Associated
Malware","Results","PCI Vuln","Ticket State","Instance","Category",
"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"
"10.90.100.110","test network","ec2-12-345-67-89.compute-
1.amazonaws.com",,"ce123a4d-56b7-8901-23e4-56c7f8901fd2",,"QAGENT",,"host
scanned, found vuln","34000","TCP Source Port Pass
Firewall","Active","Vuln","5",,,,,"06/30/2020 15:07:36","07/13/2020
12:44:23","5",,"07/10/2020 13:29:38","07/10/2020 13:29:38","1",,,,"Your
```

firewall policy seems to let TCP packets with a specific source port pass through.","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.","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.",,,"The host responded 4 times to 4 TCP SYN probes sent to destination port 443 using source port 25. However, it did not respond at all to 4 TCP SYN probes sent to the same destination port using a random source port.#","yes",,,"Firewall","**AWS**","**EC2**","**EC2**","**i-012afe3fa456789e0**","**Instance**","**123456789012**","**ami-01d23fab4fff5678c**","""{""""**Instance Id**"""":""""**i-012afe3fa456789e0**"""",""""**VPC ID**"""":""""**vpc-1e23cd45**"""",""""**Image ID**"""":""""**ami-01d23fab4fff5678c**"""",""""**Instance Type**"""":""""**t2.micro**"""",""""**Instance State**"""":""""**RUNNING**"""",""""**Public Hostname**"""":""""**ec2-12-345-67-89.compute-1.amazonaws.com**"""",""""**Private Hostname**"""":""""**ip-10-90-100-110.ec2.internal**"""",""""**Account ID**"""":""""**123456789012**"""",""""**Region Code**"""":""""**us-east-1**"""",""""**Subnet ID**"""":""""**subnet-1a234567**"""",""""**Availability Zone**"""":""""**us-east-1e**"""",""""**Group ID**"""":""""**sg-12a34f5d**"""",""""**Group Name**"""":""""**launch-wizard-123**"""",""""**Private IP Address**"""":""""**10.90.100.110**"""",""""**Public IP Address**"""":""""**3.45.67.89**"""",""""**Reservation Id**"""":""""**r-0123bc456a78c9be0**"""",""""**Spot Instance**"""":""""**No**"""",""""**Local Hostname**"""":""""**ip-10-90-100-110.ec2.internal**"""",""""**MAC Address**"""":""""**12:e3:f4:d5:6f:7b**""""}""","**i-012afe3fa456789e0**","**ec2-12-345-67-89.compute-1.amazonaws.com**","**ami-01d23fab4fff5678c**","**vpc-1e23cd45**","**RUNNING**","**ip-10-90-100-110.ec2.internal**","**t2.micro**","**123456789012**","**us-east-1**","**subnet-1a234567**"
"10.11.12.13","test network","nsvpx11.qualys.com",,"f0b12ee3-4567-8901-2dfe-345f6d7d89a0",,"QAGENT","NetScaler","host scanned, found vuln","34000","TCP Source Port Pass Firewall","New","Vuln","5",,,,,"07/15/2020 09:50:58","07/15/2020 09:50:58","1",,,,,,,,"Your firewall policy seems to let TCP packets with a specific source port pass through.","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.","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.",,,"The host responded 4 times to 4 TCP SYN probes sent to destination port 20 using source port 20. However, it did not respond at all to 4 TCP SYN probes sent to the same destination port using a random source port.#","yes",,,"Firewall","**GCP**","**Compute Engine**","**VM Instance**","**8012345678901234567**","**VM Instance**","**qvsa-**

demo",,"""{""""Instance Id"""":""""8012345678901234567"""",""""Project Id"""":""""qvsa-demo"""",""""Hostname"""":""""centos-agent.c.qvsa-demo.internal"""",""""VPC Network"""":""""default"""",""""Machine Type"""":""""n1-standard-1"""",""""Machine State"""":""""RUNNING"""",""""Zone"""":""""us-west1-c"""",""""Private IP Address"""":""""10.123.4.56"""",""""Public IP Address"""":""""35.123.456.78"""",""""MAC Address"""":""""40:12:3a:f4:56:7c""""}""","8012345678901234567",,,,,,,,,
"10.4.5.6","test network",,,,,"AZURE VM","EulerOS / Ubuntu / Fedora / Tiny Core Linux / Linux 3.x / IBM","host scanned, found vuln","82045","Degree of Randomness of TCP Initial Sequence Numbers",,"Ig","1",,,,,"05/17/2020 13:35:47","12/07/2020 10:04:44","33",,,,,,,,"TCP Initial Sequence Numbers (ISNs) obtained in the SYNACK replies from the host are analyzed to determine how random they are. The average change between subsequent ISNs and the standard deviation from the average are displayed in the RESULT section. Also included is the degree of difficulty for exploitation of the TCP ISN generation scheme used by the host.","N/A","N/A",,,"Average change between subsequent TCP initial sequence numbers is 1079852538 with a standard deviation of 566787209. These TCP initial sequence numbers were triggered by TCP SYN probes sent to the host at an average rate of 1/(5102 microseconds). The degree of difficulty to exploit the TCP initial sequence number generation scheme is:
hard.#","no",,,"TCP/IP",**"Azure","VM","VM","345af6dc-c78a-9c01-23a4-c5ed6e789012","Virtual Machine","9de0e1a2-3f45-6789-012d-3456789012e3","Windows-10","""{""""VM Id"""":""""345af6dc-c78a-9c01-23a4-c5ed6e789012"""",""""VM Name"""":""""demo-vm"""",""""Public IP Address"""":""""10.20.30.40"""",""""Image Offer"""":""""Windows-10"""",""""Image Version"""":""""latest"""",""""Subnet"""":""""default"""",""""VM State"""":""""RUNNING"""",""""Private IP Address"""":""""10.4.5.6"""",""""Size"""":""""Standard_D2"""",""""Subscription Id"""":""""9de0e1a2-3f45-6789-012d-3456789012e3"""",""""Location"""":""""centralus"""",""""Resource Group Name"""":""""demo-resource-group"""",""""Platform"""":""""Windows"""",""""Image Publisher"""":""""MicrosoftWindowsDesktop"""",""""MAC Address"""":""""00-1D-2A-3F-45-D6""""}""","345af6dc-c78a-9c01-23a4-c5ed6e789012",,,,,,,,,**
...

Download Host Based Scan Report in XML Format

In this sample, we're downloading a Host Based Scan Report in XML format. The report includes Legacy EC2/Azure fields and Cloud Provider Metadata fields. This sample has an AWS asset, Azure asset and GCP asset.

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>2021-11-09T17:44:54Z</GENERATION_DATETIME>
    <TEMPLATE><![CDATA[cloud host based template]]></TEMPLATE>
    <TARGET>
      <USER_IP_LIST>
        <RANGE network_id="0">
          <START>10.4.5.6</START>
          <END>10.4.5.6</END>
        </RANGE>
        <RANGE network_id="0">
          <START>10.11.12.13</START>
          <END>10.11.12.13</END>
        </RANGE>
        <RANGE network_id="0">
          <START>10.90.100.110</START>
          <END>10.90.100.110</END>
        </RANGE>
      </USER_IP_LIST>
      <COMBINED_IP_LIST>
        <RANGE network_id="0">
          <START>10.4.5.6</START>
          <END>10.4.5.6</END>
        </RANGE>
        <RANGE network_id="0">
          <START>10.11.12.13</START>
          <END>10.11.12.13</END>
        </RANGE>
        <RANGE network_id="0">
          <START>10.90.100.110</START>
          <END>10.90.100.110</END>
        </RANGE>
```

```
      </COMBINED_IP_LIST>
    </TARGET>
    <RISK_SCORE_SUMMARY>
      <TOTAL_VULNERABILITIES>104</TOTAL_VULNERABILITIES>
      <AVG_SECURITY_RISK>3.7</AVG_SECURITY_RISK>
      <BUSINESS_RISK>18/100</BUSINESS_RISK>
    </RISK_SCORE_SUMMARY>
  </HEADER>
  <RISK_SCORE_PER_HOST>
    <HOSTS>
      <IP_ADDRESS network_id="0">10.11.12.13</IP_ADDRESS>
      <TOTAL_VULNERABILITIES>70</TOTAL_VULNERABILITIES>
      <SECURITY_RISK>3.1</SECURITY_RISK>
    </HOSTS>
    <HOSTS>
      <IP_ADDRESS network_id="0">10.90.100.110</IP_ADDRESS>
      <TOTAL_VULNERABILITIES>6</TOTAL_VULNERABILITIES>
      <SECURITY_RISK>5.0</SECURITY_RISK>
    </HOSTS>
    <HOSTS>
      <IP_ADDRESS network_id="0">10.4.5.6</IP_ADDRESS>
      <TOTAL_VULNERABILITIES>28</TOTAL_VULNERABILITIES>
      <SECURITY_RISK>3.0</SECURITY_RISK>
    </HOSTS>
  </RISK_SCORE_PER_HOST>
  <HOST_LIST>
    <HOST>
      <IP network_id="0">10.4.5.6</IP>
      <TRACKING_METHOD>AZURE VM</TRACKING_METHOD>
      <HOST_ID><![CDATA[1007]]></HOST_ID>
      <CLOUD_PROVIDER><![CDATA[Azure]]></CLOUD_PROVIDER>
      <CLOUD_PROVIDER_SERVICE><![CDATA[VM]]></CLOUD_PROVIDER_SERVICE>
<!-- <CLOUD_SERVICE> tag has been deprecated. Please refer to
<CLOUD_PROVIDER_SERVICE> tag for the same information //-->
      <CLOUD_SERVICE><![CDATA[VM]]></CLOUD_SERVICE>
      <CLOUD_RESOURCE_TYPE><![CDATA[Virtual
Machine]]></CLOUD_RESOURCE_TYPE>
      <CLOUD_RESOURCE_ID><![CDATA[345af6dc-c78a-9c01-23a4-
c5ed6e789012]]></CLOUD_RESOURCE_ID>
      <CLOUD_ACCOUNT><![CDATA[9de0e1a2-3f45-6789-012d-
3456789012e3]]></CLOUD_ACCOUNT>
<!-- <EC2_INSTANCE_ID> tag has been deprecated. Please refer to
<CLOUD_RESOURCE_ID> tag for the same information //-->
      <EC2_INSTANCE_ID><![CDATA[345af6dc-c78a-9c01-23a4-
c5ed6e789012]]></EC2_INSTANCE_ID>
      <CLOUD_IMAGE_ID><![CDATA[Windows-10]]></CLOUD_IMAGE_ID>
      <AZURE_VM_INFO>
        <PUBLIC_IP_ADDRESS><![CDATA[10.20.30.40]]></PUBLIC_IP_ADDRESS>
        <IMAGE_OFFER><![CDATA[Windows-10]]></IMAGE_OFFER>
```

```
        <IMAGE_VERSION><![CDATA[latest]]></IMAGE_VERSION>
        <SUBNET><![CDATA[default]]></SUBNET>
        <VM_STATE><![CDATA[RUNNING]]></VM_STATE>
        <PRIVATE_IP_ADDRESS><![CDATA[10.4.5.6]]></PRIVATE_IP_ADDRESS>
        <SIZE><![CDATA[Standard_D2]]></SIZE>
        <SUBSCRIPTION_ID><![CDATA[9de0e1a2-3f45-6789-012d-
3456789012e3]]></SUBSCRIPTION_ID>
        <LOCATION><![CDATA[centralus]]></LOCATION>
        <RESOURCE_GROUP_NAME><![CDATA[demo-resource-
group]]></RESOURCE_GROUP_NAME>
      </AZURE_VM_INFO>
      <CLOUD_RESOURCE_METADATA>
        <VM_ID><![CDATA[345af6dc-c78a-9c01-23a4-c5ed6e789012]]></VM_ID>
        <VM_NAME><![CDATA[demo-vm]]></VM_NAME>
        <PLATFORM><![CDATA[Windows]]></PLATFORM>
        <PUBLIC_IP_ADDRESS><![CDATA[10.20.30.40]]></PUBLIC_IP_ADDRESS>
        <IMAGE_OFFER><![CDATA[Windows-10]]></IMAGE_OFFER>

<IMAGE_PUBLISHER><![CDATA[MicrosoftWindowsDesktop]]></IMAGE_PUBLISHER>
        <IMAGE_VERSION><![CDATA[latest]]></IMAGE_VERSION>
        <SUBNET><![CDATA[default]]></SUBNET>
        <VM_STATE><![CDATA[RUNNING]]></VM_STATE>
        <PRIVATE_IP_ADDRESS><![CDATA[10.4.5.6]]></PRIVATE_IP_ADDRESS>
        <SIZE><![CDATA[Standard_D2]]></SIZE>
        <SUBSCRIPTION_ID><![CDATA[9de0e1a2-3f45-6789-012d-
3456789012e3]]></SUBSCRIPTION_ID>
        <LOCATION><![CDATA[centralus]]></LOCATION>
        <RESOURCE_GROUP_NAME><![CDATA[demo-resource-
group]]></RESOURCE_GROUP_NAME>
        <MAC_ADDRESS><![CDATA[00-1D-2A-3F-45-D6]]></MAC_ADDRESS>
      </CLOUD_RESOURCE_METADATA>
...

    <HOST>
      <IP network_id="0">10.90.100.110</IP>
      <TRACKING_METHOD>QAGENT</TRACKING_METHOD>
      <HOST_ID><![CDATA[2001]]></HOST_ID>
      <DNS><![CDATA[ec2-12-345-67-89.compute-1.amazonaws.com]]></DNS>
      <QG_HOSTID><![CDATA[ce123a4d-56b7-8901-23e4-
56c7f8901fd2]]></QG_HOSTID>
      <CLOUD_PROVIDER><![CDATA[AWS]]></CLOUD_PROVIDER>
      <CLOUD_PROVIDER_SERVICE><![CDATA[EC2]]></CLOUD_PROVIDER_SERVICE>
<!-- <CLOUD_SERVICE> tag has been deprecated. Please refer to
<CLOUD_PROVIDER_SERVICE> tag for the same information //-->
      <CLOUD_SERVICE><![CDATA[EC2]]></CLOUD_SERVICE>
      <CLOUD_RESOURCE_TYPE><![CDATA[Instance]]></CLOUD_RESOURCE_TYPE>
      <CLOUD_RESOURCE_ID><![CDATA[i-
012afe3fa456789e0]]></CLOUD_RESOURCE_ID>
      <CLOUD_ACCOUNT><![CDATA[123456789012]]></CLOUD_ACCOUNT>
```

```
<!-- <EC2_INSTANCE_ID> tag has been deprecated. Please refer to
<CLOUD_RESOURCE_ID> tag for the same information //-->
      <EC2_INSTANCE_ID><![CDATA[i-012afe3fa456789e0]]></EC2_INSTANCE_ID>
      <CLOUD_IMAGE_ID><![CDATA[ami-01d23fab4fff5678c]]></CLOUD_IMAGE_ID>
      <EC2_INFO>
        <PUBLIC_DNS_NAME><![CDATA[ec2-12-345-67-89.compute-
1.amazonaws.com]]></PUBLIC_DNS_NAME>
        <IMAGE_ID><![CDATA[ami-01d23fab4fff5678c]]></IMAGE_ID>
        <VPC_ID><![CDATA[vpc-1e23cd45]]></VPC_ID>
        <INSTANCE_STATE><![CDATA[RUNNING]]></INSTANCE_STATE>
        <PRIVATE_DNS_NAME><![CDATA[ip-10-90-100-
110.ec2.internal]]></PRIVATE_DNS_NAME>
        <INSTANCE_TYPE><![CDATA[t2.micro]]></INSTANCE_TYPE>
        <ACCOUNT_ID><![CDATA[123456789012]]></ACCOUNT_ID>
        <REGION_CODE><![CDATA[us-east-1]]></REGION_CODE>
        <SUBNET_ID><![CDATA[subnet-1a234567]]></SUBNET_ID>
      </EC2_INFO>
      <CLOUD_RESOURCE_METADATA>
        <INSTANCE_ID><![CDATA[i-012afe3fa456789e0]]></INSTANCE_ID>
        <PUBLIC_DNS_NAME><![CDATA[ec2-12-345-67-89.compute-
1.amazonaws.com]]></PUBLIC_DNS_NAME>
        <PUBLIC_IP_ADDRESS><![CDATA[3.45.67.89]]></PUBLIC_IP_ADDRESS>

<PRIVATE_IP_ADDRESS><![CDATA[10.90.100.110]]></PRIVATE_IP_ADDRESS>
        <IMAGE_ID><![CDATA[ami-01d23fab4fff5678c]]></IMAGE_ID>
        <SPOT_INSTANCE><![CDATA[No]]></SPOT_INSTANCE>
        <AVAILABILITY_ZONE><![CDATA[us-east-1e]]></AVAILABILITY_ZONE>
        <VPC_ID><![CDATA[vpc-1e23cd45]]></VPC_ID>
        <GROUP_ID><![CDATA[sg-12a34f5d]]></GROUP_ID>
        <GROUP_NAME><![CDATA[launch-wizard-123]]></GROUP_NAME>
        <LOCAL_HOSTNAME><![CDATA[ip-10-90-100-
110.ec2.internal]]></LOCAL_HOSTNAME>
        <INSTANCE_STATE><![CDATA[RUNNING]]></INSTANCE_STATE>
        <PRIVATE_DNS_NAME><![CDATA[ip-10-90-100-
110.ec2.internal]]></PRIVATE_DNS_NAME>
        <INSTANCE_TYPE><![CDATA[t2.micro]]></INSTANCE_TYPE>
        <ACCOUNT_ID><![CDATA[123456789012]]></ACCOUNT_ID>
        <REGION_CODE><![CDATA[us-east-1]]></REGION_CODE>
        <SUBNET_ID><![CDATA[subnet-1a234567]]></SUBNET_ID>
        <RESERVATION_ID><![CDATA[r-0123bc456a78c9be0]]></RESERVATION_ID>
        <MAC_ADDRESS><![CDATA[12:e3:f4:d5:6f:7b]]></MAC_ADDRESS>
      </CLOUD_RESOURCE_METADATA>
...

    <HOST>
      <IP network_id="0">10.11.12.13</IP>
      <TRACKING_METHOD>QAGENT</TRACKING_METHOD>
      <HOST_ID><![CDATA[123456]]></HOST_ID>
      <DNS><![CDATA[nsvpx11.qualys.com]]></DNS>
```

```
      <QG_HOSTID><![CDATA[f0b12ee3-4567-8901-2dfe-
345f6d7d89a0]]></QG_HOSTID>
      <CLOUD_PROVIDER><![CDATA[GCP]]></CLOUD_PROVIDER>
      <CLOUD_PROVIDER_SERVICE><![CDATA[Compute
Engine]]></CLOUD_PROVIDER_SERVICE>
<!-- <CLOUD_SERVICE> tag has been deprecated. Please refer to
<CLOUD_PROVIDER_SERVICE> tag for the same information //-->
      <CLOUD_SERVICE><![CDATA[VM Instance]]></CLOUD_SERVICE>
      <CLOUD_RESOURCE_TYPE><![CDATA[VM Instance]]></CLOUD_RESOURCE_TYPE>

<CLOUD_RESOURCE_ID><![CDATA[8012345678901234567]]></CLOUD_RESOURCE_ID>
      <CLOUD_ACCOUNT><![CDATA[qvsa-demo]]></CLOUD_ACCOUNT>
<!-- <EC2_INSTANCE_ID> tag has been deprecated. Please refer to
<CLOUD_RESOURCE_ID> tag for the same information //-->
      <EC2_INSTANCE_ID><![CDATA[8012345678901234567]]></EC2_INSTANCE_ID>
      <CLOUD_IMAGE_ID><![CDATA[]]></CLOUD_IMAGE_ID>
      <CLOUD_RESOURCE_METADATA>
        <INSTANCE_ID><![CDATA[8012345678901234567]]></INSTANCE_ID>
        <HOST_NAME><![CDATA[centos-agent.c.qvsa-
demo.internal]]></HOST_NAME>
        <MACHINE_TYPE><![CDATA[n1-standard-1]]></MACHINE_TYPE>
        <MACHINE_STATE><![CDATA[RUNNING]]></MACHINE_STATE>
        <PROJECT_ID><![CDATA[qvsa-demo]]></PROJECT_ID>
        <PUBLIC_IP_ADDRESS><![CDATA[35.123.456.78]]></PUBLIC_IP_ADDRESS>
        <VPC_NETWORK><![CDATA[default]]></VPC_NETWORK>
        <ZONE><![CDATA[us-west1-c]]></ZONE>
        <PRIVATE_IP_ADDRESS><![CDATA[10.123.4.56]]></PRIVATE_IP_ADDRESS>
        <MAC_ADDRESS><![CDATA[40:12:3a:f4:56:7c]]></MAC_ADDRESS>
      </CLOUD_RESOURCE_METADATA>
...
```

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?))>

...

<!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?, ASSET_GROUPS?, VULN_INFO_LIST?))>

...

<!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)>
...
```

New Option to Scan Disconnected ESXi Hosts via vCenter

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

Now users can scan ESXi hosts without sending any scan traffic directly to the ESXi hosts. To achieve this, we added a new option to the VMware ESXi authentication record that allows users to specify that hosts are disconnected (is_disconnect=1). This option is only supported when you scan the ESXi hosts through vCenter (login_type=vcenter) and is only supported for compliance scans.

Create/Update VMware Authentication Records

We added the new input "is_disconnect" which is supported when scanning ESXi hosts using vCenter. Refer to the Qualys API (VM,PC) User Guide for details on all parameters.

Parameter	Description
login_type={**basic**|vault|vcenter}	(Optional) Specify "basic" (the default) to use basic authentication. You'll need to specify a password using the "password" parameter. Set to "vault" if a third party vault will be used to retrieve the password. Vault parameters need to be specified in the record. Set to "vcenter" to scan ESXi hosts through vCenter. The VMware record will include your ESXi IP addresses. You also need a vCenter authentication record with the vCenter IP addresses that map to your ESXi hosts.
is_disconnect={**0**|1}	(Optional) Specify 0 (the default) if the ESXi hosts are not disconnected. Specify 1 if the ESXi hosts are disconnected and you don't want to send any traffic to the ESXi hosts. Note: is_disconnected=1 is only valid when login_type=vcenter

Sample Create VMware Authentication Record

In this sample, we are creating a new VMware authentication record and specifying that ESXi hosts are disconnected.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=create&title=NewVMwareRecordWithAPI&login_type=vcenter&ips=10.11.
12.13&is_disconnect=1"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vmware/"
```

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>2021-11-03T12:09:53Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>1344231</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample Update VMware Authentication Record

In this sample, we are updating an existing VMware authentication record to specify that ESXi hosts are disconnected.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=update&ids=1344232&is_disconnect=1"
"https://qualysapi.qualys.com/api/2.0/fo/auth/vmware/"
```

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>2021-11-03T12:19:41Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>1344232</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

List VMware Authentication Records

When you list all VMware authentication records, the XML output will indicate whether the Disconnected option is enabled (value of 1) or disabled (value of 0) in each VMware record where LOGIN_TYPE is vcenter. You will not see it for other login types.

API request:

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

XML output:

```
<?xml version=""1.0"" encoding=""UTF-8"" ?>
<!DOCTYPE AUTH_VMWARE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/vmware/auth_vmware_list_out
put.dtd">
<AUTH_VMWARE_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-11-22T07:32:21Z</DATETIME>
    <AUTH_VMWARE_LIST>
      <AUTH_VMWARE>
        <ID>409187</ID>
        <TITLE><![CDATA[VMware_Basic]]></TITLE>
        <USERNAME><![CDATA[root]]></USERNAME>
        <PORT>443</PORT>
        <SSL_VERIFY><![CDATA[skip]]></SSL_VERIFY>
        <IP_SET>
          <IP>10.20.30.40</IP>
        </IP_SET>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2020-01-23T07:55:13Z</DATETIME>
          <BY>joe_user</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2020-01-23T07:55:13Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_VMWARE>
      <AUTH_VMWARE>
        <ID>1344231</ID>
        <TITLE><![CDATA[VMware_Disconnected_Disabled]]></TITLE>
        <PORT>443</PORT>
        <IP_SET>
          <IP>10.11.12.13</IP>
        </IP_SET>
        <LOGIN_TYPE><![CDATA[vcenter]]></LOGIN_TYPE>
        <DISCONNECTED_ESXI>0</DISCONNECTED_ESXI>
```

```
            <NETWORK_ID>0</NETWORK_ID>
            <CREATED>
              <DATETIME>2021-11-03T12:09:53Z</DATETIME>
              <BY>joe_user</BY>
            </CREATED>
            <LAST_MODIFIED>
              <DATETIME>2021-11-10T13:11:23Z</DATETIME>
            </LAST_MODIFIED>
          </AUTH_VMWARE>
          <AUTH_VMWARE>
            <ID>1344232</ID>
            <TITLE><![CDATA[VMware_Disconnected_Enabled]]></TITLE>
            <PORT>443</PORT>
            <IP_SET>
              <IP>8.9.10.11</IP>
            </IP_SET>
            <LOGIN_TYPE><![CDATA[vcenter]]></LOGIN_TYPE>
            <DISCONNECTED_ESXI>1</DISCONNECTED_ESXI>
            <NETWORK_ID>0</NETWORK_ID>
            <CREATED>
              <DATETIME>2021-11-03T12:16:36Z</DATETIME>
              <BY>joe_user</BY>
            </CREATED>
            <LAST_MODIFIED>
              <DATETIME>2021-11-10T13:10:17Z</DATETIME>
            </LAST_MODIFIED>
          </AUTH_VMWARE>
        </AUTH_VMWARE_LIST>
        <GLOSSARY>
          <USER_LIST>
            <USER>
              <USER_LOGIN>joe_user</USER_LOGIN>
              <FIRST_NAME>Joe</FIRST_NAME>
              <LAST_NAME>User</LAST_NAME>
            </USER>
          </USER_LIST>
        </GLOSSARY>
      </RESPONSE>
    </AUTH_VMWARE_LIST_OUTPUT>
```

DTD update:

We updated the DTD for VMware Records List to include a new element (in bold).

DTD: <platform>/api/2.0/fo/auth/vmware/auth_vmware_list_output.dtd

```
<!-- QUALYS AUTH_VMWARE_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT AUTH_VMWARE_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_VMWARE_LIST|ID_SET)?, WARNING_LIST?,
GLOSSARY?)>
<!ELEMENT AUTH_VMWARE_LIST (AUTH_VMWARE+)>

<!ELEMENT AUTH_VMWARE (ID, TITLE, USERNAME?, PORT, SSL_VERIFY?, HOSTS?,
IP_SET, LOGIN_TYPE?, DIGITAL_VAULT?, DISCONNECTED_ESXI?, NETWORK_ID?,
CREATED, LAST_MODIFIED, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>

<!ELEMENT HOSTS (HOST)+>
<!ELEMENT HOST (#PCDATA)>

<!ELEMENT SSL_VERIFY (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>

<!ELEMENT IP_SET (IP|IP_RANGE)+>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ELEMENT LOGIN_TYPE (#PCDATA)>
<!ELEMENT DISCONNECTED_ESXI (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT CREATED (DATETIME, BY)>
<!ELEMENT BY (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME)>
<!ELEMENT COMMENTS (#PCDATA)>

<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_FOLDER?, VAULT_FILE?, VAULT_SECRET_NAME?,
VAULT_SYSTEM_NAME?, VAULT_EP_NAME?, VAULT_EP_TYPE?, VAULT_EP_CONT?,
VAULT_NS_TYPE?, VAULT_NS_NAME?, VAULT_ACCOUNT_NAME?)>
<!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_EP_NAME (#PCDATA)>
<!ELEMENT VAULT_EP_TYPE (#PCDATA)>
<!ELEMENT VAULT_EP_CONT (#PCDATA)>
<!ELEMENT VAULT_NS_TYPE (#PCDATA)>
<!ELEMENT VAULT_NS_NAME (#PCDATA)>
<!ELEMENT VAULT_ACCOUNT_NAME (#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 -->
```

Invalid EC2 Instance IDs Skipped at Scan Launch

APIs affected	/api/2.0/fo/scan/ (action=launch)
New or Updated API	Updated
DTD or XSD changes	New

Now when you launch an EC2 scan and specify EC2 instance IDs as part of the scan target, we will identify and skip any invalid instances and continue the scan on the valid instances. Previously, the entire scan would have been blocked if an instance ID specified as part of the scan target was considered invalid.

A notification will appear in the XML output listing the invalid instance IDs and the reasons they are considered invalid. Notifications appear in a new <NOTIFICATION> tag in the API response when there is at least one valid instance and one invalid instance, and in the <TEXT> tag when there are no valid targets found. Refer to the notification message to understand why an instance was not scanned.

Note: These changes only apply when the scan target includes specific EC2 instance IDs. Using the API, you specify EC2 instance IDs for a scan using ec2_instance_ids={value}.

When all instances are valid

When all of the specified EC2 instances are valid, the scan will launch successfully and you won't see a notification in the API response.

When some instances are invalid

When the specified EC2 instance IDs provided for the scan include at least one valid instance and at least one invalid instance, the scan will continue for the valid instances and the invalid instances will be skipped. You'll see the <NOTIFICATION> tag in the API response listing the invalid instance IDs and the reasons they are invalid.

A specified EC2 instance ID could be considered invalid for these reasons:

- The instance does not belong to the EC2 environment being scanned.

- The instance does not match EC2 hosts resolved from asset tags specified as part of the scan target. Applicable only when asset tags are also specified for the scan.

- The instance has not been activated for the current module (VM, PC/SCA, CertView). For example, you're launching a vulnerability scan but the EC2 host is not activated for VM.

- The Unit Manager launching the scan does not have permission to scan the EC2 host.

When no valid scan targets are found

When all of the specified EC2 instance IDs are invalid, the scan won't be launched and we will return an error code and error text. The <TEXT> element in the output will list the invalid instance IDs and the reasons they were invalid.

API Samples

See the samples below for a look at the different types of API responses you could get based on whether EC2 instance IDs specified for the scan are valid or invalid. You'll see samples with and without asset tags specified. All samples are based on a Manager user launching the scan except where Unit Manager is mentioned. In some cases the scan is not launched because there are no valid scan targets and in other cases there is at least one valid scan target so the scan is launched and invalid instance IDs are skipped.

Note - This feature applies to VM, PC/SCA and EC2 Certview scans. You'll see a mix of samples below for different scan types.

Sample 1 - All valid instances (scan launched)

This sample is for a compliance scan where a single EC2 instance ID is specified and it is valid so the scan is launched successfully.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=launch&scan_title=Sample1&connector_name=EC2
Connector&ec2_endpoint=us-east-1&option_title=Initial PC
Options&iscanner_name=EC2_Scanner&ec2_instance_ids=i-01db234bb5c67fa8f"
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/dtd/launch_output.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2021-11-22T06:27:52Z</DATETIME>
    <TEXT>New compliance scan launched</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1143983</VALUE>
      </ITEM>
      <ITEM>
        <KEY>REFERENCE</KEY>
        <VALUE>compliance/1637562471.43983</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample 2 - Mix of valid and invalid instances (scan launched)

This sample is for a vulnerability scan with a mix of valid and invalid instance IDs. The scan is launched on the valid instance IDs and the invalid instance IDs are listed in the output with the reasons they were considered invalid. Some did not belong to the EC2 environment and some were not activated for VM.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=launch&scan_title=Sample2&connector_name=EC2
Connector&ec2_endpoint=us-east-1&option_title=Initial
Options&iscanner_name=EC2_Scanner&ec2_instance_ids=i-01f234ce567ae890f,i-
0be12cb3da4567e8a,i-0d1f23d4ba5c67e8b,i-0123e456f7890f123,i-
012f3ceb4a5d6789d,i-0c123e4f567890123,i-012345a67bba89012,i-
01ba23a45cba678af,i-012345678dfc90efe,i-0ab12e3456baadeb7"
"https://qualysapi.qualys.com/api/2.0/fo/scan/"
```

XML output:

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/dtd/launch_output.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2021-11-19T09:13:21Z</DATETIME>
    <TEXT>New vm scan launched</TEXT>
   <NOTIFICATION>The following instances were skipped because they do not
belong to the selected EC2 environment: i-012f3ceb4a5d6789d, i-
0c123e4f567890123, i-012345a67bba89012. The following instances were
skipped because they are not activated for VM: i-01ba23a45cba678af, i-
012345678dfc90efe, i-0ab12e3456baadeb7.</NOTIFICATION>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1140800</VALUE>
      </ITEM>
      <ITEM>
        <KEY>REFERENCE</KEY>
        <VALUE>scan/1637313199.40800</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample 3 - Unit Manager launched scan, mix of valid and invalid instances with valid asset tags specified (scan launched)

This is a sample EC2 CertView scan launched by a Unit Manager with a mix of valid and invalid instance IDs and asset tags specified. The scan is launched on the valid instance IDs and the invalid instance IDs are listed in the output. Some instance IDs are invalid because they do not belong to the EC2 environment and some are invalid because they are not activated for CertView, they don't match the asset tags or the Unit Manager does not have permission to scan them.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=launch&scan_title=Sample3&connector_name=EC2
Connector&ec2_endpoint=us-east-1&option_title=Initial
Options&iscanner_name=EC2_Scanner&scan_type=ec2certview&ec2_instance_ids=
i-01f234ce567ae890f,i-0be12cb3da4567e8a,i-0d1f23d4ba5c67e8b,i-
0123e456f7890f123,i-012f3ceb4a5d6789d,i-0c123e4f567890123,i-
012345a67bba89012,i-01ba23a45cba678af,i-012345678dfc90efe,i-
0ab12e3456baadeb7&target_from=tags&tag_set_by=name&tag_include_selector=a
ny&tag_set_include=EC2 NEW"
"https://qualysapi.qualys.com/api/2.0/fo/scan/"
```

XML output:

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/dtd/launch_output.dtd">
 <SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2021-11-19T11:16:27Z</DATETIME>
    <TEXT>New ec2certview scan launched</TEXT>
   <NOTIFICATION>The following instances were skipped because they do not
belong to the selected EC2 environment: i-012f3ceb4a5d6789d, i-
0c123e4f567890123, i-012345a67bba89012. The following instances were
skipped because they are not activated for CertView, they do not match the
specified tags, or you do not have permission to scan them: i-
01f234ce567ae890f, i-0be12cb3da4567e8a, i-01ba23a45cba678af, i-
012345678dfc90efe, i-0ab12e3456baadeb7.</NOTIFICATION>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1140902</VALUE>
      </ITEM>
      <ITEM>
        <KEY>REFERENCE</KEY>
        <VALUE>scan/1637320585.40902</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample 4 - All invalid, instances do not belong to EC2 environment (scan not launched)

This sample is for a vulnerability scan with multiple EC2 instance IDs. All of the instance IDs are invalid because they do not belong to the EC2 environment.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=launch&scan_title=Sample4&connector_name=EC2
Connector&ec2_endpoint=us-east-1&option_title=Initial
Options&iscanner_name=EC2_Scanner&ec2_instance_ids=i-012f3ceb4a5d6789d,i-
0c123e4f567890123,i-012345a67bba89012"
"https://qualysapi.qualys.com/api/2.0/fo/scan/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2021-11-19T09:11:54Z</DATETIME>
    <CODE>999</CODE>
    <TEXT>No valid scan targets found. The following instances do not
belong to the selected EC2 environment: i-012f3ceb4a5d6789d,i-
0c123e4f567890123,i-012345a67bba89012</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample 5 - All invalid, instances not activated for module (scan not launched)

This sample is for a compliance scan where the instance ID specified for the scan is not activated for PC/SCA. There are no valid scan targets.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=launch&scan_title=Sample5&connector_name=EC2
Connector&ec2_endpoint=us-east-1&option_title=Initial PC
Options&iscanner_name=EC2_Scanner&ec2_instance_ids=i-0123a4c5678e9b0d1"
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2021-11-22T06:53:19Z</DATETIME>
```

```
    <CODE>999</CODE>
    <TEXT>No valid scan targets found. The following instances are not
activated for PC/SCA: i-0123a4c5678e9b0d1</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample 6 - Valid instance with invalid asset tag specified (scan not launched)

This sample is for a compliance scan where the instance ID is valid, but the asset tags specified as part of the scan request are not valid so there is no scan target found.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=launch&scan_title=Sample6&connector_name=EC2
Connector&ec2_endpoint=us-east-1&option_title=Initial PC
Options&iscanner_name=EC2_Scanner&ec2_instance_ids=i-
01db234bb5c67fa8f&tag_set_by=name&tag_include_selector=any&tag_set_includ
e=NULL&target_from=tags"
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2021-11-22T06:29:43Z</DATETIME>
    <CODE>999</CODE>
    <TEXT>No scan target found for the selected EC2 environment and
tags</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample 7 - Invalid instance with valid asset tag specified (scan not launched)

This sample is for a compliance scan with asset tags specified. The instance ID is not valid because it does not belong to the selected EC2 environment.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=launch&scan_title=Sample7&connector_name=EC2
Connector&ec2_endpoint=us-east-1&option_title=Initial PC
Options&iscanner_name=EC2_Scanner&ec2_instance_ids=i-
01db234bb5c67fa8fss&tag_set_by=name&tag_include_selector=any&tag_set_incl
ude=EC2 NEW&target_from=tags"
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2021-11-22T06:31:09Z</DATETIME>
    <CODE>999</CODE>
    <TEXT>No valid scan targets found. The following instances do not
belong to the selected EC2 environment: i-01db234bb5c67fa8fss. </TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample 8 - Invalid instance with invalid asset tag specified (scan not launched)

This is a sample compliance scan where the instance ID is invalid and the asset tags specified are also invalid.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=launch&scan_title=Sample8&connector_name=EC2
Connector&ec2_endpoint=us-east-1&option_title=Initial PC
Options&iscanner_name=EC2_Scanner&ec2_instance_ids=i-01db234bb5c67fa8f,i-
123456789&tag_set_by=name&tag_include_selector=any&tag_set_include=NULL&t
arget_from=tags"
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2021-11-22T06:51:32Z</DATETIME>
    <CODE>999</CODE>
    <TEXT>No scan target found for the selected EC2 environment and
tags</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample 9 - Unit Manager launched scan, all invalid instances without asset tags specified (scan not launched)

This is a sample compliance scan launched by a Unit Manager where all the instance IDs are invalid. No asset tags were included in the scan request. Some instances do not belong to the EC2 environment and some instances are not activated for PC/SCA or the Unit Manager does not have permission to scan them.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=launch&scan_title=Sample9&connector_name=EC2
Connector&ec2_endpoint=us-east-1&option_title=Initial PC
Options&iscanner_name=EC2_Scanner&ec2_instance_ids=i-1234567890098rdf, i-
0123a4c5678e9b0d1"
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/"
```

XML output:

```
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2021-11-22T07:02:01Z</DATETIME>
    <CODE>999</CODE>
    <TEXT>No valid scan targets found. The following instances do not
belong to the selected EC2 environment: i-1234567890098rdf. The following
instances are not activated for PC/SCA or you do not have permission to
scan them: i-0123a4c5678e9b0d1</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample 10 - Unit Manager launched scan, all invalid instances with asset tags specified (scan not launched)

This is a sample compliance scan launched by a Unit Manager where all the instance IDs are invalid. Asset tags were also included in this scan request. Some instances do not belong to the EC2 environment. Some instances are not activated for PC/SCA, they do not match the tags specified or the Unit Manager does not have permission to scan them.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=launch&scan_title=Sample10&connector_name=EC2
Connector&ec2_endpoint=us-east-1&option_title=Initial PC
Options&iscanner_name=EC2_Scanner&ec2_instance_ids=i-012e345f678cc1234,i-
1234567890098rdf,i-
0123a4c5678e9b0d1&tag_set_by=name&tag_include_selector=any&tag_set_includ
e=EC2 NEW&target_from=tags"
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2021-11-22T07:03:17Z</DATETIME>
    <CODE>999</CODE>
    <TEXT>No valid scan targets found. The following instances do not
belong to the selected EC2 environment: i-012e345f678cc1234, i-
1234567890098rdf. The following instances are not activated for PC/SCA,
they do not match the specified tags, or you do not have permission to
scan them: i-0123a4c5678e9b0d1</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

New DTD

We added a new DTD for the Scan Launch output.

DTD: <platform>/api/2.0/fo/scan/dtd/launch_output.dtd

```
<!ELEMENT SIMPLE_RETURN (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 specified, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>
<!ELEMENT RESPONSE (DATETIME, CODE?, TEXT, NOTIFICATION?, ITEM_LIST?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT NOTIFICATION (#PCDATA)>
<!ELEMENT ITEM_LIST (ITEM+)>
<!ELEMENT ITEM (KEY, VALUE*)>
<!-- EOF -->
```

Issues Addressed

- We made a fix to improve performance when collecting evidence information in the Compliance Posture Information API request.
- We fixed an issue so Scanner users can now create Patch Report Templates using the API with asset_group ALL.
- For Host List Detection API, we fixed the list of supported values for output_format to include "CSV_NO_METADATA_MS_EXCEL" and "CSV_MS_EXCEL" and fixed the API documentation.