Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.13

June 21, 2021 (Updated August 19, 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.

Control Comments added to CSV, XML Formats of Policy Reports

APIs affected	/api/2.0/fo/report/?action=fetch
New or Updated API	Updated
DTD or XSD changes	Yes

When creating Policy Compliance Reports, users have the option to include control comments in the report output. The control comments already appear in HTML and PDF formats of the report. Starting in this release, control comments will also appear in CSV and XML formats of the report.

Good to Know

- To include control comments in the report output you must select it in the Compliance Policy Report Template. On the Layout tab in the template, choose Group By: Controls and then make sure Comments is selected under Sections > Controls.

- You can download saved reports in different formats from the UI (go to PC > Reports) or fetch saved reports using the API by specifying the report ID. Control comments will appear in the report output when downloaded from the UI or API.

Sample Report in XML Format

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=fetch&id=4541882&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE COMPLIANCE_POLICY_REPORT SYSTEM
"https://qualysapi.qualys.com/compliance_policy_report.dtd">
<COMPLIANCE_POLICY_REPORT>
  <HEADER>
    <NAME><![CDATA[Sample Policy Report XML]]></NAME>
    <GENERATION_DATETIME>2021-06-09T17:04:39Z</GENERATION_DATETIME>
    <COMPANY_INFO>
      <NAME><![CDATA[Qualys, Inc.]]></NAME>
      <ADDRESS><![CDATA[919 E. Hillsdale Blvd.]]></ADDRESS>
      <CITY><![CDATA[Foster City]]></CITY>
      <STATE><![CDATA[California]]></STATE>
      <COUNTRY><![CDATA[United States of America]]></COUNTRY>
      <ZIP_CODE><![CDATA[94404]]></ZIP_CODE>
    </COMPANY_INFO>
```

```
    <USER_INFO>
      <NAME><![CDATA[Joe User]]></NAME>
      <USERNAME>joe_user</USERNAME>
      <ROLE>Manager</ROLE>
    </USER_INFO>
...
  <RESULTS>
    <HOST_LIST>
      <HOST>
        <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
        <QG_HOSTID><![CDATA[]]></QG_HOSTID>
        <IP><![CDATA[10.10.10.10]]></IP>
        <OPERATING_SYSTEM><![CDATA[EulerOS / SuSE Linux / Scientific
Linux]]></OPERATING_SYSTEM>
        <LAST_SCAN_DATE>2021-06-02T15:11:02Z</LAST_SCAN_DATE>
        <TOTAL_PASSED>1</TOTAL_PASSED>
        <TOTAL_FAILED>2</TOTAL_FAILED>
        <TOTAL_ERROR>0</TOTAL_ERROR>
        <TOTAL_EXCEPTIONS>0</TOTAL_EXCEPTIONS>
        <ASSET_TAGS>
          <ASSET_TAG><![CDATA[Unit1]]></ASSET_TAG>
        </ASSET_TAGS>
        <CONTROL_LIST>
          <CONTROL>
            <CID>18999</CID>
            <STATEMENT><![CDATA[Current list of the users having role
'admin']]></STATEMENT>
            <CRITICALITY>
              <LABEL><![CDATA[CRITICAL]]></LABEL>
              <VALUE>4</VALUE>
            </CRITICALITY>
            <CONTROL_REFERENCES><![CDATA[]]></CONTROL_REFERENCES>
            <RATIONALE><![CDATA[The role 'admin' has Read/write access to
the data graph. It also has Set/delete access to indexes along with any
other future schema constructs. It can View/terminate queries. If specific
roles and privileges are no longer required to the user then they should
be revoked. Thus, configure this setting as per the business requirements
or the organization's security policy.]]></RATIONALE>
            <INSTANCE><![CDATA[Neo4j 3.x:7687]]></INSTANCE>
            <STATUS><![CDATA[Failed]]></STATUS>
            <REMEDIATION>#Review, verify and assign roles to users as per
the business requirements or the organization's security
policy.</REMEDIATION>
            <CAUSE_OF_FAILURE>
              <CRITERIA>
                <UNEXPECTED>
                  <V><![CDATA[root]]></V>
                  <V><![CDATA[test&amp;$1]]></V>
                  <V><![CDATA[joe]]></V>
```

```
                    </UNEXPECTED>
                    <MISSING logic="OR" />
                  </CRITERIA>
                </CAUSE_OF_FAILURE>
                <TECHNOLOGY>
                  <ID><![CDATA[269]]></ID>
                  <NAME>Neo4j 3.x</NAME>
                </TECHNOLOGY>
                <EVALUATION_DATE>2021-05-07T03:29:27Z</EVALUATION_DATE>
                <EVIDENCE><![CDATA[CHECK1]]></EVIDENCE>
                <CONTROL_COMMENTS><![CDATA[This is a sample control
comment]]></CONTROL_COMMENTS>
              </CONTROL>
...
```

DTD update:

DTD: <platform>/compliance_policy_report.dtd

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

<!ELEMENT COMPLIANCE_POLICY_REPORT (ERROR | (HEADER, (SUMMARY),
(RESULTS)))>
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR number CDATA #IMPLIED>

...

<!ELEMENT CONTROL_LIST (CONTROL*)>
<!ELEMENT CONTROL (CID, STATEMENT, CRITICALITY?, CONTROL_REFERENCES?,
DEPRECATED?, RATIONALE?, INSTANCE?, STATUS, REMEDIATION?,
CAUSE_OF_FAILURE?, TECHNOLOGY, EVALUATION_DATE?, PREVIOUS_STATUS?,
FIRST_FAIL_DATE?, LAST_FAIL_DATE?, FIRST_PASS_DATE?, LAST_PASS_DATE?,
EVIDENCE?, EXCEPTION?,CONTROL_COMMENTS?)>
<!ELEMENT CID (#PCDATA)>
<!ELEMENT STATEMENT (#PCDATA)>
<!ELEMENT CONTROL_REFERENCES (#PCDATA)>
<!ELEMENT RATIONALE (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT REMEDIATION (#PCDATA)>
<!ELEMENT CAUSE_OF_FAILURE ((UNEXPECTED?, MISSING?)|(CRITERIA*))>
<!ELEMENT UNEXPECTED (V*)>
<!ELEMENT MISSING (V*)>
<!ATTLIST MISSING logic CDATA #FIXED "OR">
<!ELEMENT TECHNOLOGY (ID, NAME)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT EVALUATION_DATE (#PCDATA)>
```

```
<!ELEMENT PREVIOUS_STATUS (#PCDATA)>
<!ELEMENT FIRST_FAIL_DATE (#PCDATA)>
<!ELEMENT LAST_FAIL_DATE (#PCDATA)>
<!ELEMENT FIRST_PASS_DATE (#PCDATA)>
<!ELEMENT LAST_PASS_DATE (#PCDATA)>
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT EVIDENCE (#PCDATA)>
<!ELEMENT EXCEPTION (ASSIGNEE, STATUS, END_DATE, CREATED_BY, CREATED_DATE,
MODIFIED_BY, MODIFIED_DATE, COMMENT_LIST?)>
<!ELEMENT ASSIGNEE (#PCDATA)>
<!ELEMENT END_DATE (#PCDATA)>
<!ELEMENT CREATED_BY (#PCDATA)>
<!ELEMENT CREATED_DATE (#PCDATA)>
<!ELEMENT MODIFIED_BY (#PCDATA)>
<!ELEMENT MODIFIED_DATE (#PCDATA)>
<!ELEMENT COLUMN_NAME (#PCDATA)>
<!ELEMENT CONTROL_COMMENTS (#PCDATA)>
...
```

Sample Report in CSV Format

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=fetch&id=4541883&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

CSV output:

```
"Sample Policy Report","06/07/2021 at 14:43:49 (GMT+0530)"
"Qualys, Inc.","919 E. Hillsdale Blvd, 4th Floor",,"Foster
City","California","United States of America","94404"
"Joe User","joe_user","Manager"

...

RESULTS,,,,,,,,,,,,,,,,,,,,,,
Host IP,DNS Hostname,NetBIOS Hostname,Tracking Method,Operating
System,Last Scan Date,Evaluation Date,Control ID,Control
References,Technology,Control,Criticality Label,Criticality
Value,Instance,Rationale,Status,Remediation,Deprecated,Evidence,Cause of
Failure,Qualys Host ID,Control Comments
10.10.10.10,'-,'-,IP,EulerOS / SuSE Linux / Scientific Linux,06/02/2021 at
20:41:02 (GMT+0530),05/07/2021 at 08:59:27 (GMT+0530),18999,'-,Neo4j
3.x,Current list of the users having role 'admin',CRITICAL,4,Neo4j
3.x:7687,"The role 'admin' has Read/write access to the data graph. It
also has Set/delete access to indexes along with any other future schema
constructs. It can View/terminate queries. If specific roles and
privileges are no longer required to the user then they should be revoked.
```

```
Thus, configure this setting as per the business requirements or the
organization's security policy.",Failed,"#Review, verify and assign roles
to users as per the business requirements or the organization's security
policy.",0,"The following List String value(s) <B>X</B> indicates the
current list of the <B>users having role admin</B> using <B>CALL
dbms.security.listRole()</B> procedure.

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

Setting not found
------------ OR ------------
matches regular expression list
neo4j.*

======Current Value(s) - Last updated: 05/06/2021 at 20:31:02
(GMT+0530)======
neo4j
root
test&$1
joe

======Extended Evidence======:
Row 1:role,user
Row 2:admin,neo4j
Row 3:admin,root
Row 4:admin,test&$1
Row 5:admin,joe","======Unexpected values======
root
test&amp;$1
joe

======Missing values======

------------ OR ------------
Setting not found",'-,This is a sample control comment
...
```

Cloud Provider Metadata for AWS added to Patch Reports

APIs affected	/api/2.0/fo/report/template/patch/?action=create /api/2.0/fo/report/template/patch/?action=update /api/2.0/fo/report/template/patch/?action=export /api/2.0/fo/report/?action=fetch
New or Updated API	Updated
DTD or XSD changes	Yes

We've added a new patch report template option that lets you include cloud provider metadata in patch reports (all supported report formats). Simply use the new parameter include_cloud_metadata=1 when creating or updating a patch report template. When you download or fetch a saved patch report where this option was used, you'll see cloud metadata for each AWS cloud asset in the report.

Good to Know

- Only cloud provider metadata for AWS is supported in the patch report at this time. We will add support for other cloud providers in a future release.

- You can only include cloud metadata when detailed results are grouped by HOST.

- You can download saved patch reports in different formats from the UI or fetch saved reports using the API by specifying the report ID.

Note the following when updating a patch report template using the API

- If include_cloud_metadata is set to 0 in the template, then you can change the group_by option to any supported value (HOST, PATCH, OS, AG).

- If include_cloud_metadata is set to 1 in the template and you change the group_by option to a value other than HOST during an update request, then we will automatically disable the cloud metadata option and we'll show a notification in the response, letting you know that the option was disabled as a result of the change. The notification will appear in a new <NOTIFICATION> tag.

- If group_by is set to a value other than HOST in the template and you specify include_cloud_metadata=1 during an update request, then an error will occur because include_cloud_metadata can only have a value of 1 when group_by is set to HOST.

- The DTD for update patch report template was changed and renamed to: <platform>/api/2.0/fo/report/template/patch/dtd/update/output.dtd

Create/Update Patch Template

New and updated template settings are listed below. Refer to the Qualys API (VM,PC) User Guide for details on all the patch template settings.

Parameter	Description
include_cloud_metadata={**0**|1}	(Optional) Specify 1 to include cloud metadata for your cloud assets. Only cloud metadata for AWS is supported at this time. When not specified during a create request, a value of 0 is used. When not specified during an update request, the previous value saved in the template is kept.
group_by={HOST|PATCH|OS|AG}	Sort and group the results of the report by any of the following: Host = HOST Patch = PATCH Operating System = OS Asset Group = AG When include_cloud_metadata=1 is specified, then only group_by=HOST is supported.

Sample Create Patch Template

In this sample, we are creating a new patch report template with cloud metadata.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X POST -H
Content-Type:text/xml --data-binary
"@/home/sample/cloudmetadata_api/patch_create.xml"
"https://qualysapi.qualys.com/api/2.0/fo/report/template/patch/?action=cr
eate&report_format=xml"
```

Where patch_create.xml is an XML file that contains the patch template settings:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORTTEMPLATE SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/report/template/patch/patchrepor
ttemplate_info.dtd">
<REPORTTEMPLATE>
<PATCHTEMPLATE>
<TITLE>
<INFO key="title"><![CDATA[My Patch Report]]></INFO>
<INFO key="owner"><![CDATA[225889]]></INFO>
</TITLE>
<TARGET>
<INFO key="patch_evaluation"><![CDATA[qidbased]]></INFO>
<INFO key="asset_groups"><![CDATA[AG1, AG2, AG3]]></INFO>
<INFO key="ips"><![CDATA[]]></INFO>
```

```
</TARGET>
<DISPLAY>
<INFO key="group_by"><![CDATA[HOST]]></INFO>
<INFO key="include_table_of_qids_fixed"><![CDATA[0]]></INFO>
<INFO key="include_patch_links"><![CDATA[0]]></INFO>
<INFO key="include_patches_from_unspecified_vendors"><![CDATA[0]]></INFO>
<INFO key="patch_severity_by"><![CDATA[assigned]]></INFO>
<INFO key="patch_cvss_score_by"><![CDATA[none]]></INFO>
<INFO key="cvss"><![CDATA[all]]></INFO>
<INFO key="display_custom_footer"><![CDATA[0]]></INFO>
<INFO key="display_custom_footer_text"><![CDATA[]]></INFO>
<INFO key="exclude_account_id"><![CDATA[0]]></INFO>
<INFO key="include_cloud_metadata"><![CDATA[1]]></INFO>
</DISPLAY>
<FILTER>
<INFO key="selective_vulns"><![CDATA[complete]]></INFO>
<INFO key="exclude_qid_option"><![CDATA[0]]></INFO>
<INFO key="display_non_running_kernels"><![CDATA[0]]></INFO>
<INFO key="exclude_non_running_kernel"><![CDATA[0]]></INFO>
<INFO key="exclude_non_running_services"><![CDATA[0]]></INFO>
<INFO
key="exclude_qids_not_exploitable_due_to_configuration"><![CDATA[0]]></IN
FO>
<INFO key="selective_patches"><![CDATA[complete]]></INFO>
<INFO key="exclude_patch_qid_option"><![CDATA[0]]></INFO>
<INFO key="found_since_days"><![CDATA[30]]></INFO>
</FILTER>
<USERACCESS>
<INFO key="report_access_users"><![CDATA[]]></INFO>
<INFO key="global"><![CDATA[1]]></INFO>
</USERACCESS>
</PATCHTEMPLATE>
</REPORTTEMPLATE>
```

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>2021-06-18T08:06:07Z</DATETIME>
    <TEXT>Patch Report Template(s) Successfully Created.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>5084140</VALUE>
      </ITEM>
    </ITEM_LIST>
```

```
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample Update Patch Template

In this sample, we are updating a patch report template.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -H Content-
Type:text/xml --data-binary
"@/home/sample/cloudmetadata_api/patch_update.xml"
"https://qualysapi.qualys.com/api/2.0/fo/report/template/patch/?action=up
date&template_id=5062219&report_format=xml"
```

Where patch_update.xml is an XML file that contains the patch template settings. See Sample Create Patch Template for a look at the template settings.

XML output (Success):

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/report/template/patch/dtd/update
/output.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2021-06-18T10:39:12Z</DATETIME>
    <TEXT>Patch Report Template Successfully Updated</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>5062219</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

XML output (Success with Notification):

You'll see the tag <NOTIFICATION> in the response if Include Cloud Metadata is enabled in the template and the Group By option is changed to a value other than HOST during an update request. In this sample, the Group By value was changed to OS.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/report/template/patch/dtd/update
/output.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2021-06-18T10:39:12Z</DATETIME>
```

```
    <TEXT>Patch Report Template Successfully Updated</TEXT>
    <NOTIFICATION>Cloud provider Metadata setting has been turned off for
this template as group by is changed to OS</NOTIFICATION>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>5062219</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

XML output (with Error):

You'll get an error if the Group By option is set to a value other than HOST and include_cloud_metadata=1 is sent during an update request.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/report/template/patch/dtd/update
/output.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2021-06-18T10:39:12Z</DATETIME>
    <CODE>1905</CODE>
    <TEXT>parameter include_cloud_metadata has invalid value: 1
(include_cloud_metadata can only be
set when group_by is set to HOST)</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

DTD update:

We updated the DTD to add the NOTIFICATION element. Please also note that the DTD filename has changed.

DTD: <platform>/api/2.0/fo/report/template/patch/dtd/update/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 -->
```

Export Patch Template

When you export patch report templates, you'll see the new Info key "include_cloud_metadata" with a value of 0 or 1 in the response.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/report/template/patch/?action=ex
port&report_format=xml&template_id=5084139"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORTTEMPLATE SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/report/template/patch/patchrepor
ttemplate_info.dtd">
<REPORTTEMPLATE>
  <PATCHTEMPLATE>
    <TITLE>
      <INFO key="template_id"><![CDATA[5084139]]></INFO>
      <INFO key="title"><![CDATA[My Patch Report]]></INFO>
      <INFO key="owner"><![CDATA[225889]]></INFO>
    </TITLE>
    ...
    <DISPLAY>
      <INFO key="group_by"><![CDATA[HOST]]></INFO>
      <INFO key="include_table_of_qids_fixed"><![CDATA[0]]></INFO>
      <INFO key="include_patch_links"><![CDATA[0]]></INFO>
      <INFO
key="include_patches_from_unspecified_vendors"><![CDATA[0]]></INFO>
      <INFO key="patch_severity_by"><![CDATA[assigned]]></INFO>
      <INFO key="patch_cvss_score_by"><![CDATA[none]]></INFO>
      <INFO key="cvss"><![CDATA[all]]></INFO>
      <INFO key="display_custom_footer"><![CDATA[0]]></INFO>
      <INFO key="display_custom_footer_text"><![CDATA[]]></INFO>
      <INFO key="exclude_account_id"><![CDATA[0]]></INFO>
      <INFO key="include_cloud_metadata"><![CDATA[1]]></INFO>
    </DISPLAY>
   ...
  </PATCHTEMPLATE>
</REPORTTEMPLATE>
```

Fetch Patch Report in XML Format

When cloud metadata is included in the XML patch report, you'll see the tag <CLOUD_RESOURCE_METADATA> with the metadata details for each AWS cloud asset.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=fetch&id=4541882&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE PATCH_REPORT SYSTEM
"https://qualysapi.qualys.com/patch_report.dtd" >
<PATCH_REPORT>
    <HEADER>
        <NAME>My Patch Report</NAME>
        <GENERATION_DATETIME>06/18/2021 at 14:49:08
(GMT+0530)</GENERATION_DATETIME>

...
        <HOST_LIST>
            <HOST>
                <IP>10.20.30.40</IP>
                <DNS>ec2-18-19-20-21.compute-1.amazonaws.com</DNS>
                <NETBIOS/>
                <OS>Tandberg Device / CentOS</OS>
                <OS_CPE/>
                <PATCH_COUNT>2</PATCH_COUNT>
                <NETWORK>Global Default Network</NETWORK>
                <CLOUD_PROVIDER>AWS</CLOUD_PROVIDER>
                <CLOUD_PROVIDER_SERVICE>EC2</CLOUD_PROVIDER_SERVICE>
                <CLOUD_RESOURCE_TYPE>Instance</CLOUD_RESOURCE_TYPE>
               <CLOUD_RESOURCE_ID>i-01c23af4a5678f910</CLOUD_RESOURCE_ID>
                <CLOUD_ACCOUNT>123456789123</CLOUD_ACCOUNT>
                <CLOUD_IMAGE_ID>ami-01b2e34b5678fa9d1</CLOUD_IMAGE_ID>
                <CLOUD_RESOURCE_METADATA>
                    <INSTANCE_ID>i-01c23af4a5678f910</INSTANCE_ID>
                    <PUBLIC_DNS_NAME>ec2-18-19-20-21.compute-
1.amazonaws.com</PUBLIC_DNS_NAME>
                    <PUBLIC_IP_ADDRESS>18.19.20.21</PUBLIC_IP_ADDRESS>
                    <PRIVATE_IP_ADDRESS>10.20.30.40</PRIVATE_IP_ADDRESS>
                    <IMAGE_ID>ami-01b2e34b5678fa9d1</IMAGE_ID>
                    <SPOT_INSTANCE>No</SPOT_INSTANCE>
                    <AVAILABILITY_ZONE>us-east-1e</AVAILABILITY_ZONE>
                    <VPC_ID>vpc-1e23cd45</VPC_ID>
                    <GROUP_ID>sg-12a3b4e5</GROUP_ID>
                    <GROUP_NAME>default</GROUP_NAME>
```

```
                    <LOCAL_HOSTNAME>ip-10-20-30-
40.ec2.internal</LOCAL_HOSTNAME>
                    <INSTANCE_STATE>RUNNING</INSTANCE_STATE>
                    <PRIVATE_DNS_NAME>ip-10-20-30-
40.ec2.internal</PRIVATE_DNS_NAME>
                    <INSTANCE_TYPE>t2.medium</INSTANCE_TYPE>
                    <ACCOUNT_ID>123456789123</ACCOUNT_ID>
                    <REGION_CODE>us-east-1</REGION_CODE>
                    <SUBNET_ID>subnet-1d234567</SUBNET_ID>
                    <RESERVATION_ID>r-01ca2c34567d891b2</RESERVATION_ID>
                    <MAC_ADDRESS></MAC_ADDRESS>
                </CLOUD_RESOURCE_METADATA>
                <PATCH_LIST>
...
```

DTD update:

We updated the DTD to add CLOUD_RESOURCE_METADATA elements.

DTD: <platform>/patch_report.dtd

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

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

...
<!ELEMENT HOST_LIST (HOST*)>


<!ELEMENT HOST (IP?,  DNS?, NETBIOS?, OS?, OS_CPE?, PATCH_COUNT?,
VULN_COUNT?, NETWORK?, CLOUD_PROVIDER?, CLOUD_PROVIDER_SERVICE?,
        CLOUD_RESOURCE_TYPE?, CLOUD_RESOURCE_ID?, CLOUD_ACCOUNT?,
CLOUD_IMAGE_ID?, CLOUD_RESOURCE_METADATA?, PATCH_LIST?, DETECTION_INFO?
)>
    <!ELEMENT IP (#PCDATA)>
    <!ELEMENT DNS (#PCDATA)>
    <!ELEMENT NETBIOS (#PCDATA)>
    <!ELEMENT OS (#PCDATA)>
    <!ELEMENT OS_CPE (#PCDATA)>
    <!ELEMENT PATCH_COUNT (#PCDATA)>
    <!ELEMENT NETWORK (#PCDATA)>
    <!ELEMENT CLOUD_PROVIDER (#PCDATA)>
    <!ELEMENT CLOUD_PROVIDER_SERVICE (#PCDATA)>
    <!ELEMENT CLOUD_RESOURCE_TYPE (#PCDATA)>
```

```
    <!ELEMENT CLOUD_RESOURCE_ID (#PCDATA)>
    <!ELEMENT CLOUD_ACCOUNT (#PCDATA)>
    <!ELEMENT CLOUD_IMAGE_ID (#PCDATA)>

<!ELEMENT CLOUD_RESOURCE_METADATA (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?)>
    <!ELEMENT INSTANCE_ID (#PCDATA)>
    <!ELEMENT PUBLIC_DNS_NAME (#PCDATA)>
    <!ELEMENT PUBLIC_IP_ADDRESS (#PCDATA)>
    <!ELEMENT PRIVATE_IP_ADDRESS (#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 LOCAL_HOSTNAME (#PCDATA)>
    <!ELEMENT INSTANCE_STATE (#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)>
...
```

Fetch Patch Report in CSV Format

When cloud metadata is included in a CSV patch report, you'll see the column called "Cloud Resource Metadata" with the metadata details for each AWS cloud asset.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=fetch&id=4541883&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

CSV output:

```
My Patch Report,06/18/2021 at 14:50:27 (GMT+0530),,,,,,,,,,,,
Qualys,Inc.,919 E Hillsdale Blvd,4th Floor,Foster City,California,United
States of America,94404,,,,,,
Joe User,joe_user,Manager,,,,,,,,,,
,,,,,,,,,,,,
Report Summary,,,,,,,,,,,,
```

```
Title,Asset Groups,IPs,Asset Tags,Group By,Created on,Network,,,,,,,
My Patch Report,,,"Included(any): Tag1, Tag2, Tag3;
Excluded(any);",Host,6/18/2021,Global Default Network,,,,,,,
,,,,,,,,,,,,,
Patch Summary,,,,,,,,,,,,,
Total Patches,Hosts Requiring Patches,Total Vulnerabilities
Addressed,,,,,,,,,,
25,10,90,,,,,,,,,,
,,,,,,,,,,,,,
Host List,,,,,,,,,,,,
IP,DNS,NetBIOS,OS,OS CPE,Patch Count,Network,Cloud Provider,Cloud
Provider Service,Cloud Resource Type,Cloud Resource ID,Cloud Account,Cloud
Image Id,Cloud Resource Metadata
10.20.30.40,ec2-18-19-20-21.compute-1.amazonaws.com,,Tandberg Device /
CentOS,,2,Global Default Network,AWS,EC2,Instance,i-
01c23af4a5678f910,123456789123,ami-01b2e34b5678fa9d1,"""{""""Instance
Id"""":""""i-01c23af4a5678f910"""","""""VPC ID"""":""""vpc-
1e23cd45"""","""""Image ID"""":""""ami-01b2e34b5678fa9d1"""","""""Instance
Type"""":""""t2.medium"""","""""Instance
State"""":""""RUNNING"""","""""Public DNS Name"""":""""ec2-18-19-20-
21.compute-1.amazonaws.com"""","""""Private DNS Name"""":""""ip-10-20-30-
40.ec2.internal"""","""""Account ID"""":""""123456789123"""","""""Region
Code"""":""""us-east-1"""","""""Subnet ID"""":""""subnet-
1d234567"""","""""Availability Zone"""":""""us-east-1e"""","""""Group
ID"""":""""sg-12a3b4e5"""","""""Group Name"""":""""default"""","""""Private
IP Address"""":""""10.20.30.40"""","""""Public IP
Address"""":""""18.19.20.21"""","""""Reservation Id"""":""""r-
01ca2c34567d891b2"""","""""Spot Instance"""":""""No"""","""""Local
Hostname"""":""""ip-10-20-30-40.ec2.internal"""","""""MAC
Address"""":""""""""}"""
...
```

Send Email Notifications for Deactivated, Delayed, or Skipped Scheduled Scans

APIs affected	/api/2.0/fo/schedule/scan/ /api/2.0/fo/schedule/scan/compliance/
New or Updated API	Updated
DTD or XSD changes	Yes

We've added 3 new notification options for scheduled scans. Enable these options to have email notifications sent when a scheduled scan is deactivated by the service, delayed or skipped for any reason. You can also add a custom message to be included in the body of the email for each notification type. These notifications are supported for vulnerability and compliance scan types.

To support this feature, we added 6 new input parameters, delay_notify, delay_notify_message, skipped_notify, skipped_notify_message, deactivate_notify, and deactivate_notify_message to allow you to set your notification preferences and send a custom notification message if a scheduled scan is deactivated, delayed, or skipped.

For all existing scheduled scans, the skipped and deactivated notification flags will be enabled by default.

Create/Update Scheduled Scans

New notification options are listed below. These can be used for vulnerability and compliance scheduled scans. Refer to the Qualys API (VM,PC) User Guide for details on all the schedule scan settings.

Parameter	Description
delay_notify={**0**|1}	(Optional) Specify to send a notification if a scheduled scan is delayed.
delay_notify_message={value}	(Optional) Specify a message to send notification for a delayed scheduled scan. If a message is not specified or if the delay_notify=1, the following default message is shown: "The Qualys scan launch has been delayed and will be tried again."
skipped_notify={**0**|1}	(Optional) Specify to send a notification if a scheduled scan is skipped.
skipped_notify_message={value}	(Optional) Specify a message to send notification for a skipped scheduled scan. If a message is not specified or if the skipped_notify=1, the following default message is shown: "The Qualys scan launch has been skipped."

Parameter	Description
deactivate_notify={**0**|1}	(Optional) Specify to send a notification if a scheduled scan is deactivated.
deactivate_notify_message={value}	(Optional) Specify a message to send notification for a deactivated scheduled scan. If a message is not specified or if the deactivate_notify=1, the following default message is shown: "The Qualys scan has been deactivated by the service."

Sample Create Scheduled Scan

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&scan_title=My_Schedule&ip=10.10.10.23&active=1&occurrence=
daily&recurrence=3&start_date=05/25/2021&start_hour=15&start_minute=01&en
d_after=1&time_zone_code=IN&option_title=Initial
Options&frequency_days=1&observe_dst=no&delay_notify=1&skipped_notify=1&d
eactivate_notify=1"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/schedule_scan_list_output.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2021-06-21T07:18:53Z</DATETIME>
        <TEXT>New scan scheduled successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>4307728</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample Update Scheduled Scan

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=update&id=4307728&skipped_notify_message=scan
delayed&deactivate_notify_message=scan deactivated
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/schedule_scan_list_output.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2021-06-21T07:23:58Z</DATETIME>
        <TEXT>Edit scheduled scan Completed successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>4307728</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN
```

Sample Create Compliance Scheduled Scan

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&scan_title=Daily_Scan&asset_groups=AG1&active=1&occurrence
=daily&start_hour=17&start_minute=00&time_zone_code=IN&option_title=Initi
al PC
Options&frequency_days=1&iscanner_name=External&delay_notify=1&delay_noti
fy_message=This schedule has been
delayed.&deactivate_notify=1&deactivate_notify_message=This schedule has
been deactivated&skipped_notify=1&skipped_notify_message=skipped
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/compliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/schedule_scan_list_output.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2021-06-21T10:42:21Z</DATETIME>
        <TEXT>New compliance scan scheduled successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>4319737</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample Update Compliance Scheduled Scan

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=update&id=4319737&deactivate_notify_message=This schedule has
been deactivated&skipped_notify=1&skipped_notify_message=skipped
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/compliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/schedule_scan_list_output.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2021-06-21T10:51:26Z</DATETIME>
        <TEXT>Edit scheduled compliance scan Completed successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>4319737</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

List Scheduled Scans

When you list scheduled scans and specify show_notifications=1, you'll see the notification settings for each schedule in the output.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=list&show_notifications=1&id=87450
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/schedule_scan_list_output.dtd">
<SCHEDULE_SCAN_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2021-06-17T08:59:17Z</DATETIME>
        <SCHEDULE_SCAN_LIST>
            <SCAN>
                <ID>87449</ID>
                <ACTIVE>1</ACTIVE>
```

```
                    <TITLE>
                        <![CDATA[My Scheduled Scan]]>
                    </TITLE>
                    <USER_LOGIN>joe_user</USER_LOGIN>
                    <TARGET>
                        <![CDATA[10.10.10.23]]>
                    </TARGET>
                    <NETWORK_ID>
                        <![CDATA[0]]>
                    </NETWORK_ID>
                    <ISCANNER_NAME>
                        <![CDATA[External Scanner]]>
                    </ISCANNER_NAME>
                    <USER_ENTERED_IPS>
                        <RANGE>
                            <START>10.10.10.23</START>
                            <END>10.10.10.23</END>
                        </RANGE>
                    </USER_ENTERED_IPS>
                    <OPTION_PROFILE>
                        <TITLE>
                            <![CDATA[Initial Options]]>
                        </TITLE>
                        <DEFAULT_FLAG>0</DEFAULT_FLAG>
                    </OPTION_PROFILE>
                   <PROCESSING_PRIORITY>0 - No Priority</PROCESSING_PRIORITY>
                    <SCHEDULE>
                        <DAILY frequency_days="1" />
                        <START_DATE_UTC>2021-05-25T09:31:00Z</START_DATE_UTC>
                        <START_HOUR>15</START_HOUR>
                        <START_MINUTE>1</START_MINUTE>
                        <END_AFTER_HOURS>1</END_AFTER_HOURS>
                        <END_AFTER_MINUTES>0</END_AFTER_MINUTES>
                        <NEXTLAUNCH_UTC>2021-06-17T09:31:00</NEXTLAUNCH_UTC>
                        <TIME_ZONE>
                            <TIME_ZONE_CODE>IN</TIME_ZONE_CODE>
                            <TIME_ZONE_DETAILS>(GMT+0530) India:
Asia/Calcutta</TIME_ZONE_DETAILS>
                        </TIME_ZONE>
                        <DST_SELECTED>0</DST_SELECTED>
                        <MAX_OCCURRENCE>3</MAX_OCCURRENCE>
                    </SCHEDULE>
                    <NOTIFICATIONS>
                        <BEFORE_LAUNCH>
                            <TIME>6</TIME>
                            <UNIT>
                                <![CDATA[minutes]]>
                            </UNIT>
                            <MESSAGE>
```

```
                                <![CDATA[A Qualys Scan is scheduled to start
soon.]]>
                            </MESSAGE>
                        </BEFORE_LAUNCH>
                        <AFTER_COMPLETE>
                            <MESSAGE>
                                <![CDATA[A Qualys scan is finished.]]>
                            </MESSAGE>
                        </AFTER_COMPLETE>
                        <LAUNCH_DELAY>
                            <MESSAGE>
                             <![CDATA[The Qualys scan launch has been delayed
and will be tried again]]>
                            </MESSAGE>
                        </LAUNCH_DELAY>
                        <LAUNCH_SKIP>
                            <MESSAGE>
                                <![CDATA[The Qualys scan launch has been
skipped.]]>
                            </MESSAGE>
                        </LAUNCH_SKIP>
                        <DEACTIVATE_SCHEDULE>
                            <MESSAGE>
                               <![CDATA[The Qualys scan has been deactivated
by the service.]]>
                            </MESSAGE>
                        </DEACTIVATE_SCHEDULE>
                        <DISTRIBUTION_GROUPS>
                            <DISTRIBUTION_GROUP>
                                <ID>27002</ID>
                                <TITLE>
                                    <![CDATA[My Distribution Group]]>
                                </TITLE>
                            </DISTRIBUTION_GROUP>
                        </DISTRIBUTION_GROUPS>
                    </NOTIFICATIONS>
                </SCAN>
            </SCHEDULE_SCAN_LIST>
        </RESPONSE>
</SCHEDULE_SCAN_LIST_OUTPUT>
```

DTD update:

DTD: <platform>/schedule_scan_list_output.dtd

```
<!-- QUALYS SCHEDULE_SCAN_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT SCHEDULE_SCAN_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)>

...

<!-- notifications -->
<!ELEMENT NOTIFICATIONS (BEFORE_LAUNCH?, AFTER_COMPLETE?,LAUNCH_DELAY?,
LAUNCH_SKIP?, DEACTIVATE_SCHEDULE?, DISTRIBUTION_GROUPS?)>
<!ELEMENT BEFORE_LAUNCH (TIME, UNIT, MESSAGE)>
<!ELEMENT TIME (#PCDATA)>
<!ELEMENT UNIT (#PCDATA)>
<!ELEMENT MESSAGE (#PCDATA)>

<!ELEMENT AFTER_COMPLETE (MESSAGE)>
<!ELEMENT LAUNCH_DELAY (MESSAGE)>
<!ELEMENT LAUNCH_SKIP (MESSAGE)>
<!ELEMENT DEACTIVATE_SCHEDULE (MESSAGE)>
<!ELEMENT DISTRIBUTION_GROUPS (DISTRIBUTION_GROUP+)>
<!ELEMENT DISTRIBUTION_GROUP (ID, TITLE)>

<!-- EOF -->
```

List Compliance Scheduled Scans

When you list compliance scheduled scans and specify show_notifications=1, you'll see the notification settings for each schedule in the output.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=list&show_notifications=1&id=4319737
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/compliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/compliance_schedule_scan_list_output.dtd">
<COMPLIANCE_SCHEDULE_SCAN_LIST_OUTPUT>
    <RESPONSE>
```

```
            <DATETIME>2021-06-21T10:56:42Z</DATETIME>
            <COMPLIANCE_SCHEDULE_SCAN_LIST>
                <SCAN>
                    <ID>4319737</ID>
                    <ACTIVE>1</ACTIVE>
                    <TITLE>
                        <![CDATA[Daily_Scan]]>
                    </TITLE>
                    <USER_LOGIN>joe_user</USER_LOGIN>
                    <TARGET>
                        <![CDATA[10.11.12.13-10.11.12.14,10.11.12.16]>
                    </TARGET>
                    <NETWORK_ID>
                        <![CDATA[0]]>
                    </NETWORK_ID>
                    <ISCANNER_NAME>
                        <![CDATA[External Scanner]]>
                    </ISCANNER_NAME>
                    <ASSET_GROUP_TITLE_LIST>
                        <ASSET_GROUP_TITLE>
                            <![CDATA[AG1]]>
                        </ASSET_GROUP_TITLE>
                    </ASSET_GROUP_TITLE_LIST>
                    <OPTION_PROFILE>
                        <TITLE>
                            <![CDATA[Initial PC Options]]>
                        </TITLE>
                        <DEFAULT_FLAG>0</DEFAULT_FLAG>
                    </OPTION_PROFILE>
                    <SCHEDULE>
                        <DAILY frequency_days="1" />
                        <START_DATE_UTC>2021-06-21T11:30:00Z</START_DATE_UTC>
                        <START_HOUR>17</START_HOUR>
                        <START_MINUTE>0</START_MINUTE>
                        <NEXTLAUNCH_UTC>2021-06-21T11:30:00</NEXTLAUNCH_UTC>
                        <TIME_ZONE>
                            <TIME_ZONE_CODE>IN</TIME_ZONE_CODE>
                            <TIME_ZONE_DETAILS>(GMT+0530) India:
Asia/Calcutta</TIME_ZONE_DETAILS>
                        </TIME_ZONE>
                        <DST_SELECTED>0</DST_SELECTED>
                    </SCHEDULE>
                    <NOTIFICATIONS>
                        <LAUNCH_DELAY>
                            <MESSAGE>
                                <![CDATA[This schedule has been delayed.]]>
                            </MESSAGE>
                        </LAUNCH_DELAY>
                        <LAUNCH_SKIP>
```

```
                        <MESSAGE>
                            <![CDATA[skipped]]>
                        </MESSAGE>
                    </LAUNCH_SKIP>
                    <DEACTIVATE_SCHEDULE>
                        <MESSAGE>
                            <![CDATA[This schedule has been deactivated]]>
                        </MESSAGE>
                    </DEACTIVATE_SCHEDULE>
                </NOTIFICATIONS>
            </SCAN>
        </COMPLIANCE_SCHEDULE_SCAN_LIST>
    </RESPONSE>
</COMPLIANCE_SCHEDULE_SCAN_LIST_OUTPUT>
```

DTD update:

DTD: <platform>/compliance_schedule_scan_list_output.dtd

```
<!-- QUALYS COMPLIANCE_SCHEDULE_SCAN_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT COMPLIANCE_SCHEDULE_SCAN_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)>

...

<!-- notifications -->
<!ELEMENT NOTIFICATIONS (BEFORE_LAUNCH?, AFTER_COMPLETE?, LAUNCH_DELAY?,
LAUNCH_SKIP?, DEACTIVATE_SCHEDULE?, DISTRIBUTION_GROUPS?)>
<!ELEMENT BEFORE_LAUNCH (TIME, UNIT, MESSAGE)>
<!ELEMENT TIME (#PCDATA)>
<!ELEMENT UNIT (#PCDATA)>
<!ELEMENT MESSAGE (#PCDATA)>

<!ELEMENT AFTER_COMPLETE (MESSAGE)>
<!ELEMENT LAUNCH_DELAY (MESSAGE)>
<!ELEMENT LAUNCH_SKIP (MESSAGE)>
<!ELEMENT DEACTIVATE_SCHEDULE (MESSAGE)>
```

```
<!ELEMENT DISTRIBUTION_GROUPS (DISTRIBUTION_GROUP+)>
<!ELEMENT DISTRIBUTION_GROUP (ID, TITLE)>

<!-- EOF -->
```

Option to disable the case-sensitive search in the Unix agent UDCs

APIs affected	/api/2.0/fo/compliance/control/ /api/2.0/fo/compliance/policy/
New or Updated API	Updated
DTD or XSD changes	Yes

We added an option to disable the case-sensitive search in Unix agent UDCs (Directory Search and Directory Integrity). Once the <DISABLE_CASE_SENSITIVE_SEARCH> parameter is enabled (true), the search result lists all possible combinations in the upper and/or lower case file name. By default, this option is disabled (false) which lists result with case-sensitive file name. You can export policies with this option enabled or disabled.

Sample: List DS UDCs when case sensitive search is disabled

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -d
"action=list&ids=102154&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/"
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE CONTROL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/control_list_
output.dtd">
<CONTROL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-07-21T12:14:26Z</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <ID>102154</ID>
        <UPDATE_DATE>2021-07-21T07:02:43Z</UPDATE_DATE>
        <CREATED_DATE>2021-07-07T06:38:30Z</CREATED_DATE>
        <CATEGORY>Access Control Requirements</CATEGORY>
        <SUB_CATEGORY><![CDATA[Account Creation/User
Management]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[DS UDC case sensitive with new
option]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[MINIMAL]]></LABEL>
          <VALUE>1</VALUE>
        </CRITICALITY>
        <CHECK_TYPE><![CDATA[Unix Directory Search Check]]></CHECK_TYPE>
        <COMMENT><![CDATA[DI UDC case sensitive disabled]]></COMMENT>
```

```
            <USE_AGENT_ONLY>1</USE_AGENT_ONLY>
            <IGNORE_ERROR>0</IGNORE_ERROR>
            <SCAN_PARAMETERS>
                <BASE_DIR><![CDATA[/home/qa]]></BASE_DIR>
                <SHOULD_DESCEND><![CDATA[true]]></SHOULD_DESCEND>
                <DEPTH_LIMIT><![CDATA[10]]></DEPTH_LIMIT>
                <FOLLOW_SYMLINK><![CDATA[true]]></FOLLOW_SYMLINK>
                <FILE_NAME_MATCH><![CDATA[*]]></FILE_NAME_MATCH>
                <FILE_NAME_SKIP><![CDATA[]]></FILE_NAME_SKIP>
                <DIR_NAME_MATCH><![CDATA[*]]></DIR_NAME_MATCH>
                <DIR_NAME_SKIP><![CDATA[]]></DIR_NAME_SKIP>
                <PERMISSIONS>
                    <SPECIAL>
                        <USER>any</USER>
                        <GROUP>any</GROUP>
                        <DELETION>any</DELETION>
                    </SPECIAL>
                    <USER>
                        <READ>any</READ>
                        <WRITE>any</WRITE>
                        <EXECUTE>any</EXECUTE>
                    </USER>
                    <GROUP>
                        <READ>any</READ>
                        <WRITE>any</WRITE>
                        <EXECUTE>any</EXECUTE>
                    </GROUP>
                    <OTHER>
                        <READ>any</READ>
                        <WRITE>any</WRITE>
                        <EXECUTE>any</EXECUTE>
                    </OTHER>
                </PERMISSIONS>
                <PERM_COND><![CDATA[all]]></PERM_COND>
                <TYPE_MATCH><![CDATA[d,f,l,p,b,c,s,D]]></TYPE_MATCH>
                <USER_OWNER><![CDATA[Any User]]></USER_OWNER>
                <GROUP_OWNER><![CDATA[Any Group]]></GROUP_OWNER>
                <TIME_LIMIT><![CDATA[300]]></TIME_LIMIT>
                <MATCH_LIMIT><![CDATA[50]]></MATCH_LIMIT>

<DISABLE_CASE_SENSITIVE_SEARCH><![CDATA[true]]></DISABLE_CASE_SENSITIVE_
SEARCH>
                <DATA_TYPE>String List</DATA_TYPE>
                <DESCRIPTION><![CDATA[/home/qa desc]]></DESCRIPTION>
            </SCAN_PARAMETERS>
            ...
        </CONTROL_LIST>
    </RESPONSE>
</CONTROL_LIST_OUTPUT>
```

Sample: List DI UDCs when case sensitive search is enabled

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -d
"action=list&ids=102177&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/"
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE CONTROL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/control_list_
output.dtd">
<CONTROL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-07-21T12:33:43Z</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <ID>102177</ID>
        <UPDATE_DATE>2021-07-21T07:32:20Z</UPDATE_DATE>
        <CREATED_DATE>2021-07-21T07:32:20Z</CREATED_DATE>
        <CATEGORY>Database Settings</CATEGORY>
        <SUB_CATEGORY><![CDATA[DB Access Controls]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[DI /home check qa and QA dir wo new
option]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[SERIOUS]]></LABEL>
          <VALUE>3</VALUE>
        </CRITICALITY>
        <CHECK_TYPE><![CDATA[Unix Directory Integrity
Check]]></CHECK_TYPE>
        <COMMENT><![CDATA[DI /home check qa and QA dir wo new
option]]></COMMENT>
        <USE_AGENT_ONLY>1</USE_AGENT_ONLY>
        <AUTO_UPDATE>1</AUTO_UPDATE>
        <IGNORE_ERROR>1</IGNORE_ERROR>
        <SCAN_PARAMETERS>
            <BASE_DIR><![CDATA[/home]]></BASE_DIR>
            <SHOULD_DESCEND><![CDATA[true]]></SHOULD_DESCEND>

<INTEGRITY_CHECK_DEPTH_LIMIT><![CDATA[10]]></INTEGRITY_CHECK_DEPTH_LIMIT>
            <FOLLOW_SYMLINK><![CDATA[true]]></FOLLOW_SYMLINK>
            <FILE_NAME_MATCH><![CDATA[*]]></FILE_NAME_MATCH>
            <FILE_NAME_SKIP><![CDATA[]]></FILE_NAME_SKIP>
            <DIR_NAME_MATCH><![CDATA[qa]]></DIR_NAME_MATCH>
            <DIR_NAME_SKIP><![CDATA[]]></DIR_NAME_SKIP>
            <TYPE_MATCH><![CDATA[d,f,l,p,b,c,s,D]]></TYPE_MATCH>
```

```
            <USER_OWNER><![CDATA[Any User]]></USER_OWNER>
            <GROUP_OWNER><![CDATA[Any Group]]></GROUP_OWNER>

<INTEGRITY_CHECK_TIME_LIMIT><![CDATA[600]]></INTEGRITY_CHECK_TIME_LIMIT>

<INTEGRITY_CHECK_MATCH_LIMIT><![CDATA[512]]></INTEGRITY_CHECK_MATCH_LIMIT
>

<DISABLE_CASE_SENSITIVE_SEARCH><![CDATA[false]]></DISABLE_CASE_SENSITIVE
_SEARCH>
            <DIGEST_HASH><![CDATA[MD5]]></DIGEST_HASH>
            <DATA_TYPE>String</DATA_TYPE>
            <DESCRIPTION><![CDATA[desc]]></DESCRIPTION>
        </SCAN_PARAMETERS>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>10</ID>
          ...
          </TECHNOLOGY>
        </TECHNOLOGY_LIST>
      </CONTROL>
    </CONTROL_LIST>
  </RESPONSE>
</CONTROL_LIST_OUTPUT>
```

DTD update:

The newly added option in the Control List Output (control_list_output.dtd) is highlighted in bold for your reference.

DTD: <platform>/api/2.0/fo/compliance/control/control_list_output.dtd

```
<!-- QUALYS CONTROL_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT CONTROL_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, (CONTROL_LIST|ID_SET)?, WARNING?)>
<!ELEMENT CONTROL_LIST (CONTROL+)>
```

```
...
<!ELEMENT SCAN_PARAMETERS (PATH_TYPE?, REG_HIVE?, REG_KEY?,
REG_VALUE_NAME?, FILE_PATH?, FILE_QUERY?, HASH_TYPE?, WMI_NS?,
WMI_QUERY?, SHARE_USER?, PATH_USER?, GROUP_NAME?, GROUP_NAME_LIMIT?,
BASE_DIR?, SHOULD_DESCEND?, DEPTH_LIMIT?, INTEGRITY_CHECK_DEPTH_LIMIT?,
FOLLOW_SYMLINK?, FILE_NAME_MATCH?, FILE_NAME_SKIP?, DIR_NAME_MATCH?,
DIR_NAME_SKIP?, WIN_FILE_SYS_OBJECT_TYPES?,
MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN?, WIN_PERMISSION_USERS?,
WIN_PERMISSION_MATCH?, WIN_PERMISSIONS?, PERMISSIONS?, PERM_COND?,
TYPE_MATCH?, USER_OWNER?, GROUP_OWNER?,
        TIME_LIMIT?, MATCH_LIMIT?, INTEGRITY_CHECK_TIME_LIMIT?,
INTEGRITY_CHECK_MATCH_LIMIT?, INTEGRITY_CHECK_OBJECT_TYPES?,
DISABLE_CASE_SENSITIVE_SEARCH?, DIGEST_HASH?, PERMISSION_MONITOR?,
DATA_TYPE, EVALUATE_AS_STRING?, DESCRIPTION)>
<!ELEMENT PATH_TYPE (#PCDATA)>
...
<!ELEMENT DIGEST_HASH (#PCDATA)>
<!ELEMENT PERMISSION_MONITOR (#PCDATA)>
<!ELEMENT DISABLE_CASE_SENSITIVE_SEARCH (#PCDATA)>

<!ELEMENT DATA_TYPE (#PCDATA)>
<!ELEMENT EVALUATE_AS_STRING (#PCDATA)>
<!ELEMENT DESCRIPTION (#PCDATA)>
<!ELEMENT TECHNOLOGY_LIST (TECHNOLOGY+)>
<!ELEMENT TECHNOLOGY (ID, NAME, RATIONALE, DATAPOINT?, USE_SCAN_VALUE?,
DB_QUERY?, DESCRIPTION?)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT RATIONALE (#PCDATA)>
<!ELEMENT DATAPOINT (CARDINALITY, OPERATOR, DEFAULT_VALUES)>
...
<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID_RANGE (#PCDATA)>

<!ELEMENT WARNING (CODE?, TEXT, URL?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!-- EOF -->
```

Sample: Export Policy

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -d
"action=export&id=4034697&show_user_controls=1"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/"
```

XML Output:

```
 <?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_EXPORT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/policy_export_
output.dtd">
<POLICY_EXPORT_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-07-22T08:33:50Z</DATETIME>
<POLICY>
    <TITLE><![CDATA[Suse 11 DI and DS check]]></TITLE>
    <EXPORTED><![CDATA[2021-07-22T08:33:48Z]]></EXPORTED>
    <COVER_PAGE><![CDATA[]]></COVER_PAGE>
    <STATUS><![CDATA[active]]></STATUS>
    <TECHNOLOGIES total="2">
        <TECHNOLOGY>
            <ID>38</ID>
            <NAME>SUSE Linux Enterprise 11.x</NAME>
        </TECHNOLOGY>
...
                <USER_DEFINED_CONTROL>
                    <ID>100550</ID>
                    <UDC_ID>74d487e1-6c1c-5de7-8063-a878edc046d7</UDC_ID>
                    <CHECK_TYPE>Unix Directory Search Check</CHECK_TYPE>
                   <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                    <CATEGORY>
                        <ID>3</ID>
                      <NAME><![CDATA[Access Control Requirements]]></NAME>
                    </CATEGORY>
                    <SUB_CATEGORY>
                        <ID>1010</ID>
                        <NAME><![CDATA[Account Creation/User
Management]]></NAME>
                    </SUB_CATEGORY>
                    <STATEMENT><![CDATA[Basic Directory Search Check-
UNIX_edited]]></STATEMENT>
                    <CRITICALITY>
                        <LABEL><![CDATA[MEDIUM]]></LABEL>
                        <VALUE>2</VALUE>
                    </CRITICALITY>
                    <COMMENT><![CDATA[Directory Search Check]]></COMMENT>
                    <IGNORE_ERROR>0</IGNORE_ERROR>
```

```
                    <SCAN_PARAMETERS>

<BASE_DIR><![CDATA[/etc/123/yyy/eeee/lll]]></BASE_DIR>
                        <SHOULD_DESCEND><![CDATA[false]]></SHOULD_DESCEND>
...
                         <GROUP_OWNER><![CDATA[Any Group]]></GROUP_OWNER>
                         <TIME_LIMIT><![CDATA[300]]></TIME_LIMIT>
                         <MATCH_LIMIT><![CDATA[50]]></MATCH_LIMIT>

<DISABLE_CASE_SENSITIVE_SEARCH><![CDATA[false]]></DISABLE_CASE_SENSITIVE
_SEARCH>
                         <DATA_TYPE>String List</DATA_TYPE>
                         <DESCRIPTION><![CDATA[Directory Search
Check]]></DESCRIPTION>
                    </SCAN_PARAMETERS>
                    ...
                         </TECHNOLOGY>
                    </TECHNOLOGIES>
                    <REFERENCE_LIST/>
                </USER_DEFINED_CONTROL>
            </CONTROLS>
        </SECTION>
    </SECTIONS>
</POLICY>
  </RESPONSE>
</POLICY_EXPORT_OUTPUT>
```

DTD update:

The newly added option in the Policy Export Output (policy_export_output.dtd) is highlighted in bold for your reference.

DTD: <platform>/api/2.0/fo/compliance/policy/policy_export_output.dtd

```
<!-- QUALYS POLICY_EXPORT_OUTPUT DTD -->
<!-- $Revision: 62328 $ -->
<!ELEMENT POLICY_EXPORT_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 USE_SCAN_VALUE (#PCDATA)>

<!ELEMENT USER_DEFINED_CONTROL (ID, UDC_ID, CHECK_TYPE,
IS_CONTROL_DISABLE?, CATEGORY, SUB_CATEGORY, STATEMENT, CRITICALITY?,
COMMENT?, USE_AGENT_ONLY?, AUTO_UPDATE?, IGNORE_ERROR,
```

```
(IGNORE_ITEM_NOT_FOUND|ERROR_SET_STATUS)?, SCAN_PARAMETERS?,
REFERENCE_TEXT?, TECHNOLOGIES, REFERENCE_LIST)>
<!ELEMENT UDC_ID (#PCDATA)>
<!ELEMENT CHECK_TYPE (#PCDATA)>
...
<!ELEMENT SCAN_PARAMETERS (PATH_TYPE?, REG_HIVE?, REG_KEY?,
REG_VALUE_NAME?, FILE_PATH?, FILE_QUERY?, HASH_TYPE?, WMI_NS?,
WMI_QUERY?, SHARE_USER?,
PATH_USER?, BASE_DIR?, SHOULD_DESCEND?, DEPTH_LIMIT?,
INTEGRITY_CHECK_DEPTH_LIMIT?, FOLLOW_SYMLINK?, FILE_NAME_MATCH?,
FILE_NAME_SKIP?, DIR_NAME_MATCH?,
DIR_NAME_SKIP?, PERMISSIONS?, PERM_COND?, TYPE_MATCH?, USER_OWNER?,
GROUP_OWNER?, TIME_LIMIT?, MATCH_LIMIT?, INTEGRITY_CHECK_TIME_LIMIT?,
INTEGRITY_CHECK_MATCH_LIMIT?, DISABLE_CASE_SENSITIVE_SEARCH?,
INTEGRITY_CHECK_OBJECT_TYPES?, WIN_FILE_SYS_OBJECT_TYPES?,
MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN?, WIN_PERMISSION_USERS?,
WIN_PERMISSION_MATCH?, WIN_PERMISSIONS?, GROUP_NAME?,
GROUP_NAME_LIMIT?, DIGEST_HASH?, PERMISSION_MONITOR?, DATA_TYPE,
EVALUATE_AS_STRING?, DESCRIPTION)>
<!ELEMENT PATH_TYPE (#PCDATA)>
...
<!ELEMENT MATCH_LIMIT (#PCDATA)>
<!ELEMENT DISABLE_CASE_SENSITIVE_SEARCH (#PCDATA)>
<!ELEMENT INTEGRITY_CHECK_TIME_LIMIT (#PCDATA)>
<!ELEMENT INTEGRITY_CHECK_MATCH_LIMIT (#PCDATA)>
<!ELEMENT INTEGRITY_CHECK_OBJECT_TYPES (#PCDATA)>
...
<!ATTLIST K id CDATA #IMPLIED>
<!ATTLIST FV id CDATA #IMPLIED>

<!-- EOF -->
```

Database UDC Support for IBM DB2

APIs affected	/api/2.0/fo/compliance/posture/info/?action=list /api/2.0/fo/compliance/control/?action=list /api/2.0/fo/compliance/policy/?action=export /api/2.0/fo/subscription/option_profile/pc
New or Updated API	Updated
DTD or XSD changes	Yes

With this release, we are adding the Database UDC support for IBM DB2. For this new database control type, we've added new settings in the compliance option profile. You'll see API changes for create, update, list, and export option profiles. We've also added new elements to the XML output and DTDs for Control List Output, Policy Export Output, Posture Info List Output, Option Profiles, and the ImportableControl.xsd schema.

You'll see these changes:

- We've added the following new input parameters to help you set a limit on the number of rows returned per scan for an IBM DB2 UDC.

Parameter	Description
db2_db_udc_restriction= {**0**|1}	(Optional) Set value to 1 if you want to specify a limit on the number of rows to be returned per scan for custom IBM DB2 Database checks.
db2_db_udc_limit= {value}	(Optional) The default value is 256 and maximum allowed limit is 5000 rows.

- We've added a new CHECK_TYPE element to the XML output for Control List API: IBM DB2 Database Check.

- We've added support for IBM DB2 technologies (IBM DB2 9.x, IBM DB2 10.x, and IBM DB2 11.x) for the UDC, and you'll see these technologies in Posture API and Policy Export API.

- We've updated the ImportableControl.xsd schema to include a new enumeration value for the CHECK_TYPE element: DB2 Database Check.

Sample - Option Profile API: Create

In this sample, you'll create an option profile and specify the new parameters for IBM DB2: db2_db_udc_restriction and db2_db_udc_limit.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=create&title=API_DB2_udc_2&db2_db_udc_restriction=1&db2_db_udc_li
mit=300&scan_ports=standard"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/pc/"
```

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>2021-06-22T09:55:15Z</DATETIME>
    <TEXT>Compliance Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>5040089</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Option Profile API: Update

In this sample, you'll update an option profile and specify the new parameters for IBM DB2: db2_db_udc_restriction and db2_db_udc_limit.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=update&id=5040089&db2_db_udc_restriction=1&db2_db_udc_limit=350&t
itle=Updated_API_db2_udc_op_2"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/pc/"
```

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>2021-06-22T10:07:37Z</DATETIME>
    <TEXT>Compliance Option profile successfully updated.</TEXT>
```

```
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>5040089</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Option Profile API: List

When you list option profiles, you'll see the database preference keys and their corresponding values for IBM DB2.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=list&id=5040089"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/opti
on_profile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>5040089</ID>
...
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
...
      <DATABASE_PREFERENCE_KEY>
        <DB2>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>300</DB_UDC_LIMIT>
        </DB2>
      </DATABASE_PREFERENCE_KEY>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
      <CONTROL_TYPES>
        <FIM_CONTROLS_ENABLED>0</FIM_CONTROLS_ENABLED>
        <CUSTOM_WMI_QUERY_CHECKS>0</CUSTOM_WMI_QUERY_CHECKS>
      </CONTROL_TYPES>
    </SCAN>
```

```
    <ADDITIONAL>
...
    </ADDITIONAL>
    <INSTANCE_DATA_COLLECTION />
    <OS_BASED_INSTANCE_DISC_COLLECTION />
  </OPTION_PROFILE>
</OPTION_PROFILES>
```

Sample - Options Profile API: Export

When you export an option profile, you'll see the database preference keys and their corresponding values for IBM DB2 in the output.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/?act
ion=export&option_profile_id=5040089&output_format=xml"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/opti
on_profile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
...
      <DATABASE_PREFERENCE_KEY>
        <DB2>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>350</DB_UDC_LIMIT>
        </DB2>
      </DATABASE_PREFERENCE_KEY>
      <FILE_INTEGRITY_MONITORING>
...
</OPTION_PROFILES>
```

DTD update:

We updated the option_profile_info.dtd to include IBM DB2 in Database Preference Key and corresponding elements.

DTD: <platform>/api/2.0/fo/subscription/option_profile/option_profile_info.dtd

```
<!ELEMENT OPTION_PROFILES (OPTION_PROFILE)*>
 <!ELEMENT OPTION_PROFILE (BASIC_INFO, SCAN, MAP?, ADDITIONAL,
INSTANCE_DATA_COLLECTION?,OS_BASED_INSTANCE_DISC_COLLECTION?)>
...
```

```
<!ELEMENT SCAN (PORTS?, SCAN_DEAD_HOSTS?, CLOSE_VULNERABILITIES?,
PURGE_OLD_HOST_OS_CHANGED?, PERFORMANCE?, LOAD_BALANCER_DETECTION?,
PASSWORD_BRUTE_FORCING?, VULNERABILITY_DETECTION?, AUTHENTICATION?,
        ADDL_CERT_DETECTION?, DISSOLVABLE_AGENT?, LITE_OS_SCAN?,
ETHERNET_IP_PROBING?, CUSTOM_HTTP_HEADER?, HOST_ALIVE_TESTING?,
SCAN_RESTRICTION?, DATABASE_PREFERENCE_KEY?, SYSTEM_AUTH_RECORD?,
FILE_INTEGRITY_MONITORING?, CONTROL_TYPES?, DO_NOT_OVERWRITE_OS?,
TEST_AUTHENTICATION?)>
...

<!ELEMENT DATABASE_PREFERENCE_KEY (MSSQL?, ORACLE?, SYBASE?, POSTGRESQL?,
SAPIQ?, DB2?)>
<!ELEMENT MSSQL (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT ORACLE (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT SYBASE (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT POSTGRESQL (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT SAPIQ (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT DB2 (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT DB_UDC_RESTRICTION (#PCDATA)>
<!ELEMENT DB_UDC_LIMIT (#PCDATA)>
...
```

Schema update (option_profiles.xsd):

The option_profiles.xsd schema is used when importing and exporting option profiles. We added new elements for the IBM DB2 database control type.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified"
elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <xs:element name="OPTION_PROFILES" type="OPTION_PROFILESType"/>
...
   <xs:complexType name="DATABASE_PREFERENCE_KEYType">
        <xs:sequence>
            <xs:element type="MSSQLType" name="MSSQL" minOccurs="0"/>
            <xs:element type="ORACLEType" name="ORACLE" minOccurs="0"/>
            <xs:element type="SYBASEType" name="SYBASE" minOccurs="0"/>
            <xs:element type="POSTGRESQLType" name="POSTGRESQL"
minOccurs="0"/>
            <xs:element type="SAPIQType" name="SAPIQ" minOccurs="0"/>
            <xs:element type="DB2Type" name="DB2" minOccurs="0"/>
</xs:sequence>
    </xs:complexType>
...
    <xs:complexType name="DB2Type">
        <xs:sequence>
            <xs:element name="DB_UDC_RESTRICTION">
                <xs:simpleType>
```

```
                    <xs:restriction base="xs:integer">
                        <xs:enumeration value="1"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
            <xs:element name="DB_UDC_LIMIT">
                <xs:simpleType>
                    <xs:restriction base="xs:integer">
                        <xs:minInclusive value="1"/>
                        <xs:maxInclusive value="10000"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
...
```

Sample - Control List API for IBM DB2

We have added new CHECK_TYPE element to the XML output for Control List API:

DB2 Database Check.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=list&ids=100010"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE CONTROL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/control_list_
output.dtd">
<CONTROL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-06-22T11:14:08Z</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <ID>100010</ID>
        <UPDATE_DATE>2021-06-22T08:24:27Z</UPDATE_DATE>
        <CREATED_DATE>2021-06-22T08:24:27Z</CREATED_DATE>
        <CATEGORY>Database Settings</CATEGORY>
        <SUB_CATEGORY><![CDATA[DB Access Controls]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[db2 statement]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[SERIOUS]]></LABEL>
          <VALUE>3</VALUE>
```

```
        </CRITICALITY>
        <CHECK_TYPE><![CDATA[DB2 Database Check]]></CHECK_TYPE>
        <COMMENT><![CDATA[comment for db2 udc]]></COMMENT>
        <IGNORE_ERROR>1</IGNORE_ERROR>
        <ERROR_SET_STATUS>FAIL</ERROR_SET_STATUS>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>40</ID>
            <NAME>IBM DB2 9.x</NAME>
            <RATIONALE><![CDATA[db2 udc rationale]]></RATIONALE>
            <DB_QUERY><![CDATA[select * from sysadmin]]></DB_QUERY>
            <DESCRIPTION><![CDATA[test db2 udc
descprition]]></DESCRIPTION>

          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>93</ID>
            <NAME>IBM DB2 10.x</NAME>
            <RATIONALE><![CDATA[db2 udc rationale]]></RATIONALE>
            <DB_QUERY><![CDATA[select * from sysadmin]]></DB_QUERY>
            <DESCRIPTION><![CDATA[test db2 udc
descprition]]></DESCRIPTION>

          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>142</ID>
            <NAME>IBM DB2 11.x</NAME>
            <RATIONALE><![CDATA[db2 udc rationale]]></RATIONALE>
            <DB_QUERY><![CDATA[select * from sysadmin]]></DB_QUERY>
            <DESCRIPTION><![CDATA[test db2 udc
descprition]]></DESCRIPTION>

          </TECHNOLOGY>
        </TECHNOLOGY_LIST>
      </CONTROL>
    </CONTROL_LIST>
  </RESPONSE>
</CONTROL_LIST_OUTPUT>
```

Sample - Posture API

We've added support for IBM DB2 technologies (IBM DB2 9.x, IBM DB2 10.x, and IBM DB2 11.x) for the UDC, and you'll see the posture details of the IBM DB2 technology instances in the Posture API output.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=list&policy_id=4023779&details=Basic"
"https://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>2021-07-14T05:46:59Z</DATETIME>
    <INFO_LIST>
      <INFO>
        <ID>17018700</ID>
        <HOST_ID>7433950</HOST_ID>
        <CONTROL_ID>100010</CONTROL_ID>
        <TECHNOLOGY_ID>93</TECHNOLOGY_ID>
        <INSTANCE>DB2v10:1:50000:Admin</INSTANCE>
        <STATUS>Failed</STATUS>
        <POSTURE_MODIFIED_DATE>2021-06-
23T08:46:28Z</POSTURE_MODIFIED_DATE>
        <EVALUATION_DATE>2021-07-07T10:38:41Z</EVALUATION_DATE>
        <PREVIOUS_STATUS>Failed</PREVIOUS_STATUS>
        <FIRST_FAIL_DATE>2021-06-23T08:46:29Z</FIRST_FAIL_DATE>
        <LAST_FAIL_DATE>2021-07-07T10:38:41Z</LAST_FAIL_DATE>
        <FIRST_PASS_DATE>N/A</FIRST_PASS_DATE>
        <LAST_PASS_DATE>N/A</LAST_PASS_DATE>
      </INFO>
      <INFO>
        <ID>17019700</ID>
        <HOST_ID>7434183</HOST_ID>
        <CONTROL_ID>100010</CONTROL_ID>
        <TECHNOLOGY_ID>142</TECHNOLOGY_ID>
        <INSTANCE>DB2v11:1:50004:Admin</INSTANCE>
        <STATUS>Failed</STATUS>
        <POSTURE_MODIFIED_DATE>2021-06-
23T09:37:16Z</POSTURE_MODIFIED_DATE>
        <EVALUATION_DATE>2021-07-07T10:36:26Z</EVALUATION_DATE>
        <PREVIOUS_STATUS>Failed</PREVIOUS_STATUS>
        <FIRST_FAIL_DATE>2021-06-23T09:37:17Z</FIRST_FAIL_DATE>
```

```
        <LAST_FAIL_DATE>2021-07-07T10:36:26Z</LAST_FAIL_DATE>
        <FIRST_PASS_DATE>N/A</FIRST_PASS_DATE>
        <LAST_PASS_DATE>N/A</LAST_PASS_DATE>
      </INFO>
...
    </INFO_LIST>

...

    <GLOSSARY>
      <HOST_LIST>
        <HOST>
          <ID>7433950</ID>
          <IP>10.20.32.224</IP>
          <TRACKING_METHOD>IP</TRACKING_METHOD>
          <OS><![CDATA[Ubuntu Linux 12.04]]></OS>
          <ASSET_ID>20221576</ASSET_ID>
          <PERCENTAGE><![CDATA[40.00% (2 of 5)]]></PERCENTAGE>
        </HOST>
        <HOST>
          <ID>7434183</ID>
          <IP>10.20.32.184</IP>
          <TRACKING_METHOD>IP</TRACKING_METHOD>
          <DNS><![CDATA[mdw2016db2v11]]></DNS>
          <DNS_DATA>
            <HOSTNAME><![CDATA[mdw2016db2v11]]></HOSTNAME>
            <DOMAIN />
            <FQDN />
          </DNS_DATA>
          <NETBIOS><![CDATA[MDW2016DB2V11]]></NETBIOS>
          <OS><![CDATA[Windows Server 2016 Datacenter 64 bit
Edition]]></OS>
          <ASSET_ID>20221593</ASSET_ID>
          <PERCENTAGE><![CDATA[20.00% (1 of 5)]]></PERCENTAGE>
        </HOST>
      </HOST_LIST>
      <CONTROL_LIST>
        <CONTROL>
          <ID>100010</ID>
          <STATEMENT><![CDATA[db2 udc example statement 1]]></STATEMENT>
          <CRITICALITY>
            <LABEL><![CDATA[SERIOUS]]></LABEL>
            <VALUE>3</VALUE>
          </CRITICALITY>
          <REFERENCE><![CDATA[]]></REFERENCE>
        </CONTROL>
        <CONTROL>
          <ID>100012</ID>
          <STATEMENT><![CDATA[db2 udc example statement 2]]></STATEMENT>
```

```
            <CRITICALITY>
              <LABEL><![CDATA[CRITICAL]]></LABEL>
              <VALUE>4</VALUE>
            </CRITICALITY>
            <REFERENCE><![CDATA[]]></REFERENCE>
          </CONTROL>
          <CONTROL>
            <ID>100011</ID>
            <STATEMENT><![CDATA[db2 udc example statement 3]]></STATEMENT>
            <CRITICALITY>
              <LABEL><![CDATA[SERIOUS]]></LABEL>
              <VALUE>3</VALUE>
            </CRITICALITY>
            <REFERENCE><![CDATA[]]></REFERENCE>
          </CONTROL>
          <CONTROL>
            <ID>100013</ID>
            <STATEMENT><![CDATA[db2 udc example statement 4]]></STATEMENT>
            <CRITICALITY>
              <LABEL><![CDATA[CRITICAL]]></LABEL>
              <VALUE>4</VALUE>
            </CRITICALITY>
            <REFERENCE><![CDATA[]]></REFERENCE>
          </CONTROL>
          <CONTROL>
            <ID>100014</ID>
            <STATEMENT><![CDATA[db2 udc example statement 5]]></STATEMENT>
            <CRITICALITY>
              <LABEL><![CDATA[URGENT]]></LABEL>
              <VALUE>5</VALUE>
            </CRITICALITY>
            <REFERENCE><![CDATA[]]></REFERENCE>
          </CONTROL>
        </CONTROL_LIST>
      </GLOSSARY>
    </RESPONSE>
  </POSTURE_INFO_LIST_OUTPUT>
```

Sample - Policy Export API

We've added support for IBM DB2 technologies (IBM DB2 9.x, IBM DB2 10.x, and IBM DB2 11.x) for the UDC, and you'll see these technologies in the Policy Export API, when applicable.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"action=export&id=4023779&show_user_controls=1&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_EXPORT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/policy_export_
output.dtd">
<POLICY_EXPORT_OUTPUT>
  <REQUEST>
    <DATETIME>2021-06-22T13:20:24Z</DATETIME>
    <USER_LOGIN>up_at</USER_LOGIN>

<RESOURCE>https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/</RES
OURCE>
    <PARAM_LIST>
      <PARAM>
        <KEY>action</KEY>
        <VALUE>export</VALUE>
      </PARAM>
      <PARAM>
        <KEY>id</KEY>
        <VALUE>4023779</VALUE>
      </PARAM>
      <PARAM>
        <KEY>show_user_controls</KEY>
        <VALUE>1</VALUE>
      </PARAM>
      <PARAM>
        <KEY>echo_request</KEY>
        <VALUE>1</VALUE>
      </PARAM>
    </PARAM_LIST>
  </REQUEST>
  <RESPONSE>
    <DATETIME>2021-06-22T13:20:28Z</DATETIME>
<POLICY>
    <TITLE><![CDATA[DB2 UDC Policy]]></TITLE>
    <EXPORTED><![CDATA[2021-06-22T13:20:28Z]]></EXPORTED>
    <COVER_PAGE><![CDATA[]]></COVER_PAGE>
    <STATUS><![CDATA[active]]></STATUS>
    <TECHNOLOGIES total="3">
        <TECHNOLOGY>
            <ID>40</ID>
            <NAME>IBM DB2 9.x</NAME>
        </TECHNOLOGY>
        <TECHNOLOGY>
            <ID>93</ID>
            <NAME>IBM DB2 10.x</NAME>
        </TECHNOLOGY>
        <TECHNOLOGY>
```

```
            <ID>142</ID>
            <NAME>IBM DB2 11.x</NAME>
        </TECHNOLOGY>
    </TECHNOLOGIES>
    <SECTIONS total="1">
        <SECTION>
            <NUMBER>1</NUMBER>
            <HEADING><![CDATA[Untitled]]></HEADING>
            <CONTROLS total="1">
                <USER_DEFINED_CONTROL>
                    <ID>100010</ID>
                    <UDC_ID>1912154e-2329-5031-81db-b528a2fb7d7d</UDC_ID>
                    <CHECK_TYPE>DB2 Database Check</CHECK_TYPE>
                   <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                    <CATEGORY>
                        <ID>8</ID>
                        <NAME><![CDATA[Database Settings]]></NAME>
                    </CATEGORY>
                    <SUB_CATEGORY>
                        <ID>1044</ID>
                        <NAME><![CDATA[DB Access Controls]]></NAME>
                    </SUB_CATEGORY>
                    <STATEMENT><![CDATA[db2 statement]]></STATEMENT>
                    <CRITICALITY>
                        <LABEL><![CDATA[SERIOUS]]></LABEL>
                        <VALUE>3</VALUE>
                    </CRITICALITY>
                    <COMMENT><![CDATA[comment for db2 udc]]></COMMENT>
                    <IGNORE_ERROR>1</IGNORE_ERROR>
                    <ERROR_SET_STATUS>FAIL</ERROR_SET_STATUS>
                    <TECHNOLOGIES total="3">
                        <TECHNOLOGY>
                            <ID>40</ID>
                            <NAME>IBM DB2 9.x</NAME>

<EVALUATE><CTRL><AND><OR><DP><K>custom.db2_query.3128436</K><V><![CDATA[.
*]]></V><DBCOL><![CDATA[]]></DBCOL><DT>5</DT><OP>xre</OP><CD>matches</CD>
<FV set="1">No data found</FV></DP></OR></AND></CTRL></EVALUATE>
                            <RATIONALE><![CDATA[db2 udc
rationale]]></RATIONALE>
                            <REMEDIATION><![CDATA[remediation for db2
udc]]></REMEDIATION>
                            <DB_QUERY><![CDATA[select * from
sysadmin]]></DB_QUERY>
                            <DESCRIPTION><![CDATA[test db2 udc
descprition]]></DESCRIPTION>
                        </TECHNOLOGY>
                        <TECHNOLOGY>
                            <ID>93</ID>
```

```
                                <NAME>IBM DB2 10.x</NAME>

<EVALUATE><CTRL><AND><OR><DP><K>custom.db2_query.3128436</K><V><![CDATA[.
*]]></V><DBCOL><![CDATA[]]></DBCOL><DT>5</DT><OP>xre</OP><CD>matches</CD>
<FV set="1">No data found</FV></DP></OR></AND></CTRL></EVALUATE>
                                <RATIONALE><![CDATA[db2 udc
rationale]]></RATIONALE>
                                <REMEDIATION><![CDATA[remediation for db2
udc]]></REMEDIATION>
                                <DB_QUERY><![CDATA[select * from
sysadmin]]></DB_QUERY>
                                <DESCRIPTION><![CDATA[test db2 udc
descprition]]></DESCRIPTION>
                            </TECHNOLOGY>
                            <TECHNOLOGY>
                                <ID>142</ID>
                                <NAME>IBM DB2 11.x</NAME>

<EVALUATE><CTRL><AND><OR><DP><K>custom.db2_query.3128436</K><V><![CDATA[.
*]]></V><DBCOL><![CDATA[]]></DBCOL><DT>5</DT><OP>xre</OP><CD>matches</CD>
<FV set="1">No data found</FV></DP></OR></AND></CTRL></EVALUATE>
                                <RATIONALE><![CDATA[db2 udc
rationale]]></RATIONALE>
                                <REMEDIATION><![CDATA[remediation for db2
udc]]></REMEDIATION>
                                <DB_QUERY><![CDATA[select * from
sysadmin]]></DB_QUERY>
                                <DESCRIPTION><![CDATA[test db2 udc
descprition]]></DESCRIPTION>
                            </TECHNOLOGY>
                        </TECHNOLOGIES>
                        <REFERENCE_LIST/>
                    </USER_DEFINED_CONTROL>
                </CONTROLS>
            </SECTION>
        </SECTIONS>
</POLICY>
  </RESPONSE>
</POLICY_EXPORT_OUTPUT>
```

Schema update (ImportableControl.xsd):

The ImportableControl.xsd schema is used when importing and exporting controls. We added the enumeration value DB2 Database Check to the schema.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified">
...
    <xs:element name="CHECK_TYPE">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="Registry Key Existence" />
                <xs:enumeration value="Registry Value Existence" />
                <xs:enumeration value="Registry Value Content Check" />
                <xs:enumeration value="Registry Permission" />
               <xs:enumeration value="Window File/Directory Existence" />
              <xs:enumeration value="Window File/Directory Permission" />
               <xs:enumeration value="Unix File/Directory Permission" />
               <xs:enumeration value="Unix File Content Check" />
               <xs:enumeration value="Unix File/Directory Existence" />
               <xs:enumeration value="Window File Integrity Check" />
               <xs:enumeration value="Unix File Integrity Check" />
               <xs:enumeration value="WMI Query Check" />
               <xs:enumeration value="Share Access Check" />
               <xs:enumeration value="Unix Directory Search Check" />
               <xs:enumeration value="Windows Directory Search Check" />
               <xs:enumeration value="Windows Group Membership Check" />
               <xs:enumeration value="Windows Directory Integrity Check"
/>
               <xs:enumeration value="Unix Directory Integrity Check" />
               <xs:enumeration value="MS SQL Database Check" />
               <xs:enumeration value="Oracle Database Check" />
               <xs:enumeration value="Sybase Database Check" />
               <xs:enumeration value="PostgreSQL Database Check" />
               <xs:enumeration value="SAP IQ Database Check" />
               <xs:enumeration value="Windows File Content Check" />
               <xs:enumeration value="DB2 Database Check" />
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
...
```

Issues Addressed

- We fixed an issue in the API response for Export Scan Template to XML format where the Info key “host_with_cloud_agents” appeared blank instead of showing the correct template setting.