Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.4

September 21, 2020 (Updated September 29, 2020)

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.

New API to Ignore Vulnerabilities

APIs affected	/api/2.0/fo/ignore_vuln/index.php
New or Updated API	New
DTD or XSD changes	New

With this release, we're introducing a new V2 API for Ignoring Vulnerabilities which will replace the old V1 API for Ignoring Vulnerabilities.

New API: /api/2.0/fo/ignore_vuln/index.php

Old API: /msp/ignore_vuln.php

The new Ignore Vulnerabilities API has all the same functionality as the old API plus some additional functionality. Now you can specify hosts using tag related parameters (tag_set_include, tag_set_exclude, tag_set_by, tag_include_selector, tag_exclude_selector, use_ip_nt_range_tags_include, and use_ip_nt_range_tags_exclude), which was not available before. A vulnerability can be ignored for an instance, in other words a host/vulnerability/port.

When you ignore a vulnerability instance:

- You won't see these vulnerabilities throughout the UI (host information, asset search results, your dashboard, etc).

- These vulnerabilities will no longer appear in template based scan reports with host based findings.

- We'll close any remediation tickets for these vulnerabilities automatically.

Input Parameters

The following table shows the input parameters for ignoring/restoring vulnerabilities

Parameter	Description
action=ignore|restore	A flag indicating an ignore or restore request. When unspecified, the action is set to "ignore". Specify "restore" to restore (un-ignore) vulnerabilities.
qids={qid,qid,...}	(Required) Specifies the QIDs (Qualys IDs) to ignore/restore. A maximum of 10 QIDs may be specified. Multiple QIDs are comma separated.
comments={value}	(Required) Specify comments for the action. The comments may include a maximum of 255 characters. Comments are stored with ignored vulnerabilities, and are visible to users in the Qualys user interface.

Parameter	Description
reopen_ignored_days={value}	(Optional) Set to reopen ignored vulnerabilities that are detected after a number of days (1-730). If the ignored vulnerability is reopened by the service, the corresponding ticket's state/status is changed from Closed/Ignored to Open/Reopened.
reopen_ignored_date={date}	(Optional) Set to reopen ignored vulnerabilities that are detected after a specified date. If the ignored vulnerability is reopened by the service, the corresponding ticket's state/status is changed from Closed/Ignored to Open/Reopened.
asset_groups={ag1,ag2,...}	(Optional) Selects hosts by asset group. The hosts included in the one or more asset groups provided are selected. A maximum of 5 asset group titles may be specified. The asset group title "All" as defined in the Qualys user interface may be specified. Multiple asset groups are comma separated. This parameter or another host selection parameter is required.
ips={nnn, nnn-nnn,...}	(Optional) Selects hosts by IP address. Enter one or more IP addresses and/or ranges. Multiple entries are comma separated. The parameter value may include a maximum of 512 characters (ascii).This parameter or another host selection parameter is required.
tag_set_include={value}	(Optional) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_exclude={value}	(Optional) Specify a tag set to exclude. Hosts that match these tags will be excluded. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
tag_set_by={id|name}	(Optional) Specify "id" (the default) to select a tag set by providing tag IDs. Specify "name" to select a tag set by providing tag names.
tag_include_selector={all|any}	(Optional) Select "any" (the default) to include hosts that match at least one of the selected tags. Select "all" to include hosts that match all of the selected tags.
tag_exclude_selector={all|any}	(Optional) Select "any" (the default) to exclude hosts that match at least one of the selected tags. Select "all" to exclude hosts that match all of the selected tags.
use_ip_nt_range_tags_include={0|1}	(Optional) Specify "0" (the default) to select from all tags (tags with any tag rule). Specify "1" to scan all IP addresses defined in tag selection. When this is specified, only tags with the dynamic IP address rule called "IP address in Network Range(s)" can be selected.

Parameter	Description
use_ip_nt_range_tags_exclude ={0|1}	(Optional) Specify "0" (the default) to select from all tags (tags with any tag rule). Specify "1" to exclude all IP addresses defined in tag selection. When this is specified, only tags with the dynamic IP address rule called "IP address in Network Range(s)" can be selected.
network_id={value}	(Optional) Only valid when the networks feature is enabled. The network ID for the record. This parameter or another host selection parameter is required.
dns_contains={value}	(Optional) Selects hosts by DNS host name. Specify a text string contained in one or more DNS host names. The text string may include a maximum of 100 characters (ascii). This parameter or another host selection parameter is required.
netbios_contains={value}	(Optional) Selects hosts by NetBIOS host name. Specify a text string contained in one or more NetBIOS host names. The text string may include a maximum of 100 characters (ascii).This parameter or another host selection parameter is required.

Sample Ignore Vulnerabilities

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=ignore&qids=38304&comments=ignore vuln on
tags&tag_set_include=ignore_vuln_tags&tag_set_exclude=ignore_vuln_tags&ta
g_set_by=name&tag_include_selector=any&tag_exclude_selector=any&use_ip_nt
_range_tags_include=0&use_ip_nt_range_tags_exclude=0"
"https://qualysapi.qualys.com/api/2.0/fo/ignore_vuln/index.php"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE IGNORE_VULN_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/ignore_vuln/output.dtd">
<IGNORE_VULN_OUTPUT>
    <RESPONSE status="SUCCESS" number="1">
        <MESSAGE>The operation was successfully completed</MESSAGE>
        <IGNORED_LIST>
            <IGNORED>
                <TICKET_NUMBER>16</TICKET_NUMBER>
                <QID>38304</QID>
                <IP network_id="0">0.0.0.4</IP>
                <DNS>
                    <![CDATA[0-0-0-4.bogus.tld]]>
                </DNS>
            </IGNORED>
        </IGNORED_LIST>
```

```
    </RESPONSE>
</IGNORE_VULN_OUTPUT>
```

Sample Restore Vulnerabilities

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=restore&qids=38304&comments=ignore vuln on
tags&tag_set_include=ignore_vuln_tags&tag_set_exclude=ignore_vuln_tags&ta
g_set_by=name&tag_include_selector=any&tag_exclude_selector=any&use_ip_nt
_range_tags_include=0&use_ip_nt_range_tags_exclude=0"
"https://qualysapi.qualys.com/api/2.0/fo/ignore_vuln/index.php"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE IGNORE_VULN_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/ignore_vuln/output.dtd">
<IGNORE_VULN_OUTPUT>
    <RESPONSE status="SUCCESS" number="1">
        <MESSAGE>The operation was successfully completed</MESSAGE>
        <RESTORED_LIST>
            <RESTORED>
                <TICKET_NUMBER>16</TICKET_NUMBER>
                <QID>38304</QID>
                <IP network_id="0">0.0.0.4</IP>
                <DNS>
                    <![CDATA[0-0-0-4.bogus.tld]]>
                </DNS>
            </RESTORED>
        </RESTORED_LIST>
    </RESPONSE>
</IGNORE_VULN_OUTPUT>
```

New DTD:

DTD: <platform API server>/api/2.0/fo/ignore_vuln/output.dtd

```
<!-- QUALYS IGNORE VULNERABILITY OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT IGNORE_VULN_OUTPUT (REQUEST?,RESPONSE)>

<!-- "name" is the name of API -->
<!-- "at" attribute is the current platform date and time -->
<!ELEMENT REQUEST (#PCDATA)>
<!ATTLIST REQUEST
        name CDATA #REQUIRED
        username CDATA #REQUIRED
        at CDATA #REQUIRED>
```

```
<!-- the PCDATA contains an explanation of the status -->
<!ELEMENT RESPONSE (MESSAGE, IGNORED_LIST?, RESTORED_LIST?)>
<!ATTLIST RESPONSE
        status (FAILED|SUCCESS|WARNING) #REQUIRED
        number CDATA #IMPLIED>
<!ELEMENT MESSAGE (#PCDATA)*>

<!ELEMENT IGNORED_LIST (IGNORED+)>
<!ELEMENT IGNORED (TICKET_NUMBER, QID, IP, DNS?, NETBIOS?)>
<!ELEMENT TICKET_NUMBER (#PCDATA)>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT DNS (#PCDATA)*>
<!ELEMENT NETBIOS (#PCDATA)*>

<!ATTLIST IP network_id CDATA #IMPLIED>

<!ELEMENT RESTORED_LIST (RESTORED+)>
<!ELEMENT RESTORED (TICKET_NUMBER, QID, IP, DNS?, NETBIOS?)>
```

LDAP Authentication Support for MongoDB Record

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

With this release, you can list, create and update MongoDB records for LDAP authentication. We have introduced two new parameters - crendential_type (to provide separate options for local authentication and external LDAP authentication) and cleartext (enables to send cleartext password over unencrypted channel). Local authentication was already supported.

To authenticate a MongoDB server using an LDAP account, the password must be sent in the cleartext over the unencrypted channel. This cleartext password is then used by the MongoDB server to send a separate authentication request to the configured LDAP server.

New Input Parameters

The following table shows new input parameters for list, create or update MongoDB records.

Parameter	Description
credential_type=**local**|external	(Optional) The credential type is local by default which means login credential type is local authentication. You need to set credential type to external for LDAP authentication option.
cleartext=**0**|1	(Optional) You must set credential_type to external to use cleartext parameter. The default value for cleartext is 0. You must set this parameter to 1 for successful MongoDB authentication for LDAP.

Sample - List MongoDB Record for LDAP Authentication

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=list&ids=3053011&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MONGODB_LIST_OUTPUT SYSTEM
"https://qualysapi.p04.eng.sjc01.qualys.com/api/2.0/fo/auth/mongodb/auth_
mongodb_list_output.dtd">
<AUTH_MONGODB_LIST_OUTPUT>
  <RESPONSE>
```

```
      <DATETIME>2020-09-09T06:26:20Z</DATETIME>
      <AUTH_MONGODB_LIST>
        <AUTH_MONGODB>
          <ID>3053011</ID>
          <TITLE><![CDATA[mdb]]></TITLE>
          <USERNAME><![CDATA[dd]]></USERNAME>
          <CREDENTIAL_TYPE><![CDATA[external]]></CREDENTIAL_TYPE>
          <CLEARTEXT><![CDATA[No]]></CLEARTEXT>
          <DATABASE><![CDATA[admindada]]></DATABASE>
          <PORT>27017</PORT>
          <UNIX_CONFIGURATION_FILE><![CDATA[]]></UNIX_CONFIGURATION_FILE>
          <SSL_VERIFY><![CDATA[0]]></SSL_VERIFY>
          <IP_SET>
            <IP>10.10.0.10</IP>
          </IP_SET>
          <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
          <NETWORK_ID>0</NETWORK_ID>
          <CREATED>
            <DATETIME>2020-09-09T06:24:55Z</DATETIME>
            <BY>quays_an</BY>
          </CREATED>
          <LAST_MODIFIED>
            <DATETIME>2020-09-09T06:26:16Z</DATETIME>
          </LAST_MODIFIED>
        </AUTH_MONGODB>
      </AUTH_MONGODB_LIST>
      <GLOSSARY>
        <USER_LIST>
          <USER>
            <USER_LOGIN>quays_jdoe</USER_LOGIN>
            <FIRST_NAME>John</FIRST_NAME>
            <LAST_NAME>Doe</LAST_NAME>
          </USER>
        </USER_LIST>
      </GLOSSARY>
    </RESPONSE>
  </AUTH_MONGODB_LIST_OUTPUT>
```

Updated DTD:

DTD: <platform API server>/api/2.0/fo/auth/mongodb/auth_mongodb_list_output.dtd

We have added new elements in the DTD. The new elements are shown in bold.

```
<!-- QUALYS AUTH_MONGODB_LIST_OUTPUT DTD -->
<!ELEMENT AUTH_MONGODB_LIST_OUTPUT (REQUEST?, RESPONSE)>
<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
...
```

```
<!ELEMENT AUTH_MONGODB_LIST (AUTH_MONGODB+)>
<!ELEMENT AUTH_MONGODB (ID, TITLE, USERNAME?, CREDENTIAL_TYPE?,
CLEARTEXT?, DATABASE, PORT, UNIX_CONFIGURATION_FILE, SSL_VERIFY?, HOSTS?,
IP_SET?, LOGIN_TYPE?, DIGITAL_VAULT?, PRIVATE_KEY_CERTIFICATE_LIST?,
NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT CREDENTIAL_TYPE (#PCDATA)>
<!ELEMENT CLEARTEXT (#PCDATA)>

<!ELEMENT PRIVATE_KEY_CERTIFICATE_LIST (PRIVATE_KEY_CERTIFICATE)*>
...
<!ELEMENT VAULT_ACCOUNT_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_PATH (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_KEY (#PCDATA)>
<!ELEMENT VAULT_SERVICE_TYPE (#PCDATA)>
<!-- EOF -->
```

Sample - Create MongoDB Record for LDAP Authentication

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=create&title=Sample1&username=mlqa&password=12345abc&ips=10.20.32
.107&comments=Creating through API
v2.0&unix_conf_path=/etc/mongod3111.conf&port=28021&ssl_verify=0&database
_name=admin&credential_type=external&cleartext=1"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb"
```

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>2020-09-08T06:15:39Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>3052106</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Existing MongoDB Record from Local Authentication to LDAP Authentication

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=update&ids=3052107&username=mlqaUpdated&password=12345abcUpdated&
comments=Updated through API
v2.0&echo_request=1&echo_request=1&port=5858&credential_type=external&cle
artext=1" "https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb"
```

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>
  <REQUEST>
    <DATETIME>2020-09-08T06:21:16Z</DATETIME>
    <USER_LOGIN>quays_jdoe</USER_LOGIN>

<RESOURCE>https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/</RESOURCE
>
    <PARAM_LIST>
      <PARAM>
        <KEY>action</KEY>
        <VALUE>update</VALUE>
      </PARAM>
      <PARAM>
        <KEY>ids</KEY>
        <VALUE>3052107</VALUE>
      </PARAM>
      <PARAM>
        <KEY>username</KEY>
        <VALUE>mlqaUpdated</VALUE>
      </PARAM>
      <PARAM>
        <KEY>password</KEY>
        <VALUE>12345abcUpdated</VALUE>
      </PARAM>
      <PARAM>
        <KEY>comments</KEY>
        <VALUE>Updated through API v2.0</VALUE>
      </PARAM>
      <PARAM>
        <KEY>echo_request</KEY>
        <VALUE>1</VALUE>
      </PARAM>
      <PARAM>
        <KEY>port</KEY>
```

```
        <VALUE>5858</VALUE>
      </PARAM>
      <PARAM>
        <KEY>credential_type</KEY>
        <VALUE>external</VALUE>
      </PARAM>
      <PARAM>
        <KEY>cleartext</KEY>
        <VALUE>1</VALUE>
      </PARAM>
    </PARAM_LIST>
  </REQUEST>
  <RESPONSE>
    <DATETIME>2020-09-08T06:21:17Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>3052107</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Existing MongoDB Record from LDAP Authentication to Local Authentication

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=update&ids=3052107&username=mlqaUpdated&password=12345abcUpdated&
comments=Updated through API
v2.0&echo_request=1&echo_request=1&port=5858&credential_type=local"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb"
```

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>
  <REQUEST>
    <DATETIME>2020-09-08T06:50:15Z</DATETIME>
    <USER_LOGIN>quays_jdoe</USER_LOGIN>

<RESOURCE>https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/</RESOURCE
>
    <PARAM_LIST>
```

```
        <PARAM>
          <KEY>action</KEY>
          <VALUE>update</VALUE>
        </PARAM>
        <PARAM>
          <KEY>ids</KEY>
          <VALUE>3052107</VALUE>
        </PARAM>
        <PARAM>
          <KEY>username</KEY>
          <VALUE>mlqaUpdated</VALUE>
        </PARAM>
        <PARAM>
          <KEY>password</KEY>
          <VALUE>12345abcUpdated</VALUE>
        </PARAM>
        <PARAM>
          <KEY>comments</KEY>
          <VALUE>Updated through API v2.0</VALUE>
        </PARAM>
        <PARAM>
          <KEY>echo_request</KEY>
          <VALUE>1</VALUE>
        </PARAM>
        <PARAM>
          <KEY>port</KEY>
          <VALUE>5858</VALUE>
        </PARAM>
        <PARAM>
          <KEY>credential_type</KEY>
          <VALUE>local</VALUE>
        </PARAM>
      </PARAM_LIST>
    </REQUEST>
    <RESPONSE>
      <DATETIME>2020-09-08T06:50:15Z</DATETIME>
      <BATCH_LIST>
        <BATCH>
          <TEXT>Successfully Updated</TEXT>
          <ID_SET>
            <ID>3052107</ID>
          </ID_SET>
        </BATCH>
      </BATCH_LIST>
    </RESPONSE>
  </BATCH_RETURN>
```

Launch/Schedule Compliance Scans on FQDNs

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

With this release you can launch and schedule compliance scans on Fully Qualified Domain Names (FQDNs). Specify the input parameter "fqdn" during the scan request.

Good to Know

- DNS Tracking must be enabled for the subscription. A Manager user can enable this feature in the Qualys UI by going to Scans > Setup > DNS Tracking and checking the "Enable DNS Tracking for hosts" option.

- You can specify FQDNs in combination with IPs and asset groups but not with asset tags.

- The scanned FQDN must resolve to an IP address in your PC account and IP address that is resolved from the DNS name must be in an authentication record to successfully scan it and view the results.

- When you launch scans only on FQDNs, you must specify one or more scanner appliances or specify iscanner_name=External for the External scanner. If iscanner_name is not specified in the request then the Default scanner is used and you will get the error, "The Scanner Appliance setting is not allowed." Other scans that use target_from=assets also default to Default scanner when a scanner is not specified. Scans that use target_from=tags default to External scanner when a scanner is not specified.

- When updating a scheduled scan, you must specify target_from=assets when fqdn is specified in the same request.

- When sub-users launch scans only on FQDNs the scans are listed on the Scans list in the UI and in the output for Scans list in the API (action=list).

Launch and Schedule Compliance Scans

Use the following input parameter to specify the FQDNs you want to scan. Refer to the Qualys API (VM,PC) User Guide for full details on Launch/Schedule Scan APIs.

Parameter	Description
fqdn={value}	(Optional) The target FQDN for a compliance scan. You must specify at least one target i.e. IPs, asset groups or FQDNs. Multiple values are comma separated.

Launch Scan Samples

API request (FQDN only):

```
curl -H "X-Requested-With: Curl" -u "USERNAME:PASSWORD" -X "POST" -d
"action=launch&scan_title=API_Scan_fdqn&fqdn=domain.qualys.com&option_tit
le=Initial+PC+Options&iscanner_name=SV_VScanner2"
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/"
```

API request (FQDN and asset group):

```
curl -H "X-Requested-With: Curl" -u "USERNAME:PASSWORD" -X "POST" -d
"action=launch&scan_title=API_Scan_fdqn&fqdn=domain.qualys.com&option_tit
le=Initial+PC+Options&iscanner_name=SV_VScanner2&asset_groups=CEnt7"
"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>2020-09-08T11:03:17Z</DATETIME>
    <TEXT>New compliance scan launched</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>11480673</VALUE>
      </ITEM>
      <ITEM>
        <KEY>REFERENCE</KEY>
        <VALUE>compliance/1599562995.80673</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Create Scheduled Scan Samples

API request (FQDN only):

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=create&scan_title=2API_Schedule_Scan_FQDN&active=1&occurrence=dai
ly&recurrence=1&start_date=09/8/2020&start_hour=05&start_minute=03&end_af
ter=1&time_zone_code=US-
CA&option_title=Initial+PC+Options&frequency_days=1&observe_dst=yes&fqdn=
domain.qualys.com"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/compliance/"
```

API request (FQDN and asset group):

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=create&scan_title=2API_Schedule_Scan_FQDN&active=1&occurrence=dai
ly&recurrence=1&start_date=09/8/2020&start_hour=05&start_minute=03&end_af
ter=1&time_zone_code=US-
CA&option_title=Initial+PC+Options&frequency_days=1&observe_dst=yes&fqdn=
domain.qualys.com&asset_groups=CEnt7"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/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>2020-09-08T11:52:17Z</DATETIME>
    <TEXT>New compliance scan scheduled successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>2983668</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Update Scheduled Scan Samples

During an update request you must specify target_from=assets when fqdn is specified in the same request.

When fqdn is not specified during an update request for a scheduled scan that already has fqdn defined, we will keep the existing value.

API request (update FQDN):

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=update&id=2983669&target_from=assets&fqdn=domain.qualys.com"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/compliance/"
```

API request (remove FQDN and keep asset group):

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=update&id=2983669&target_from=assets&fqdn=&asset_groups=CEnt7"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/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>2020-09-08T12:18:03Z</DATETIME>
    <TEXT>Edit scheduled compliance scan Completed successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>2983669</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

List Scans and Schedules

When you list scans and schedules you'll see any FQDNs that were specified as part of the scan target in the <TARGET> section of the output.

List Compliance Scans

API request:

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCAN_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/scan_list_output.dtd">
<SCAN_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-09-08T12:28:00Z</DATETIME>
    <SCAN_LIST>
      <SCAN>
        <ID>11480818</ID>
        <REF>compliance/1599565156.80818</REF>
        <TYPE>On-Demand</TYPE>
        <TITLE><![CDATA[FQDN Scantake 2 UI]]></TITLE>
        <USER_LOGIN>quays_jdoe</USER_LOGIN>
        <LAUNCH_DATETIME>2020-09-08T11:39:16Z</LAUNCH_DATETIME>
        <DURATION>00:06:53</DURATION>
        <PROCESSED>1</PROCESSED>
        <STATUS>
```

```
            <STATE>Finished</STATE>
          </STATUS>
          <TARGET><![CDATA[domain.qualys.com]]></TARGET>
        </SCAN>
        <SCAN>
          <ID>11480673</ID>
          <REF>compliance/1599562995.80673</REF>
          <TYPE>API</TYPE>
          <TITLE><![CDATA[API_Scan_fdqn]]></TITLE>
          <USER_LOGIN>quays_jdoe</USER_LOGIN>
          <LAUNCH_DATETIME>2020-09-08T11:03:15Z</LAUNCH_DATETIME>
          <DURATION>00:06:12</DURATION>
          <PROCESSED>1</PROCESSED>
          <STATUS>
            <STATE>Finished</STATE>
          </STATUS>
          <TARGET><![CDATA[domain.qualys.com]]></TARGET>
        </SCAN>
      </SCAN_LIST>
    </RESPONSE>
</SCAN_LIST_OUTPUT>
```

List Scheduled Scans

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" "action=list"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/compliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE COMPLIANCE_SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/compliance/complia
nce_schedule_scan_list_output.dtd">
<COMPLIANCE_SCHEDULE_SCAN_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-09-09T12:04:21Z</DATETIME>
    <COMPLIANCE_SCHEDULE_SCAN_LIST>
      <SCAN>
        <ID>2983979</ID>
        <ACTIVE>0</ACTIVE>
        <TITLE><![CDATA[take1API_Schedule_Scan_FQDN]]></TITLE>
        <USER_LOGIN>quays_jdoe</USER_LOGIN>
        <TARGET><![CDATA[domain.qualys.com]]></TARGET>
        <ISCANNER_NAME><![CDATA[External Scanner]]></ISCANNER_NAME>
        <OPTION_PROFILE>
          <TITLE><![CDATA[Initial PC Options]]></TITLE>
          <DEFAULT_FLAG>0</DEFAULT_FLAG>
```

```
          </OPTION_PROFILE>
          <SCHEDULE>
            <DAILY frequency_days="1" />
            <START_DATE_UTC>2020-09-08T13:03:00Z</START_DATE_UTC>
            <START_HOUR>5</START_HOUR>
            <START_MINUTE>3</START_MINUTE>
            <END_AFTER_HOURS>1</END_AFTER_HOURS>
            <TIME_ZONE>
              <TIME_ZONE_CODE>US-CA</TIME_ZONE_CODE>
              <TIME_ZONE_DETAILS>(GMT-0800) United States:
America/Los_Angeles</TIME_ZONE_DETAILS>
            </TIME_ZONE>
            <DST_SELECTED>1</DST_SELECTED>
            <MAX_OCCURRENCE>1</MAX_OCCURRENCE>
          </SCHEDULE>
        </SCAN>
        <SCAN>
          <ID>2983669</ID>
          <ACTIVE>1</ACTIVE>
          <TITLE><![CDATA[API_PC_SCAN_AG]]></TITLE>
          <USER_LOGIN>quays_jdoe</USER_LOGIN>
          <TARGET><![CDATA[10.11.72.56]]></TARGET>
          <ISCANNER_NAME><![CDATA[External Scanner]]></ISCANNER_NAME>
          <ASSET_GROUP_TITLE_LIST>
            <ASSET_GROUP_TITLE><![CDATA[CEnt7]]></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>2020-09-08T13:18:00Z</START_DATE_UTC>
            <START_HOUR>5</START_HOUR>
            <START_MINUTE>18</START_MINUTE>
            <NEXTLAUNCH_UTC>2020-09-09T13:18:00</NEXTLAUNCH_UTC>
            <TIME_ZONE>
              <TIME_ZONE_CODE>US-CA</TIME_ZONE_CODE>
              <TIME_ZONE_DETAILS>(GMT-0800) United States:
America/Los_Angeles</TIME_ZONE_DETAILS>
            </TIME_ZONE>
            <DST_SELECTED>0</DST_SELECTED>
          </SCHEDULE>
        </SCAN>
    </COMPLIANCE_SCHEDULE_SCAN_LIST>
    </RESPONSE>
</COMPLIANCE_SCHEDULE_SCAN_LIST_OUTPUT>
```

Fetch Compliance Scan

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=fetch&scan_ref=compliance/1600333077.13214"
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/"
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE COMPLIANCE_SCAN_RESULT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/compliance_scan_
result_output.dtd">
<COMPLIANCE_SCAN_RESULT_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-09-17T09:48:48Z</DATETIME>
    <COMPLIANCE_SCAN>
      <HEADER>
        <NAME><![CDATA[Compliance Scan Results]]></NAME>
        <GENERATION_DATETIME>2020-09-17T09:48:48Z</GENERATION_DATETIME>
        <COMPANY_INFO>
          <NAME><![CDATA[Qualys]]></NAME>
          <ADDRESS><![CDATA[1600 Bridge Parkway]]></ADDRESS>
          <CITY><![CDATA[Redwood Shores]]></CITY>
          <STATE><![CDATA[California]]></STATE>
          <COUNTRY><![CDATA[United States of America]]></COUNTRY>
          <ZIP_CODE><![CDATA[94065]]></ZIP_CODE>
        </COMPANY_INFO>
        <USER_INFO>
          <NAME><![CDATA[quays_jdoe]]></NAME>
          <USERNAME>jdoe</USERNAME>
          <ROLE>Manager</ROLE>
        </USER_INFO>
        <KEY value="USERNAME">jdoe</KEY>
        <KEY value="COMPANY"><![CDATA[Qualys]]></KEY>
        <KEY value="DATE">2020-09-17T08:59:59Z</KEY>
        <KEY value="TITLE"><![CDATA[Scan by DNS With FQDN only on cust
NW]]></KEY>
        <KEY value="TARGET">domain1.qualys.com, domain2.qualys.com</KEY>
        <KEY value="EXCLUDED_TARGET"><![CDATA[N/A]]></KEY>
        <KEY value="NETWORK_ID"><![CDATA[164091]]></KEY>
        <KEY value="NETWORK_TITLE"><![CDATA[Swati - Network 1]]></KEY>
        <KEY value="DURATION">00:03:47</KEY>
        <KEY value="SCAN_HOST">SV_VScanner1 (Scanner 12.0.35-1,
Vulnerability Signatures 2.4.976-2)</KEY>
        <KEY value="NBHOST_ALIVE">2</KEY>
        <KEY value="NBHOST_TOTAL">2</KEY>
        <KEY value="REPORT_TYPE">On-demand</KEY>
        <KEY value="OPTIONS">Scanned Ports: Targeted Scan, Hosts to Scan
```

```
in Parallel - External Scanners: 15, Hosts to Scan in Parallel - Scanner
Appliances: 30, Total Processes to Run in Parallel: 10, HTTP Processes to
Run in Parallel: 10, Packet (Burst) Delay: Medium, Intensity: Normal,
Overall Performance: Normal, ICMP Host Discovery, Ignore RST packets: Off,
Ignore firewall-generated SYN-ACK packets: Off, Do not send ACK or SYN-ACK
packets during host discovery: Off</KEY>
        <KEY value="STATUS">FINISHED</KEY>
        <FQDNS>
          <FQDN><![CDATA[domain1.qualys.com]]></FQDN>
          <FQDN><![CDATA[domain2.qualys.com]]></FQDN>
        </FQDNS>
        <OPTION_PROFILE>
          <OPTION_PROFILE_TITLE
option_profile_default="0"><![CDATA[Initial PC
Options]]></OPTION_PROFILE_TITLE>
        </OPTION_PROFILE>
      </HEADER>
      <APPENDIX>
        <TARGET_HOSTS />
        <TARGET_DISTRIBUTION>
          <SCANNER>
            <NAME><![CDATA[SV_VScanner1]]></NAME>
            <HOSTS>domain1.qualys.com, domain2.qualys.com</HOSTS>
          </SCANNER>
        </TARGET_DISTRIBUTION>
        <OS_AUTH_BASED_TECHNOLOGY_LIST />
      </APPENDIX>
    </COMPLIANCE_SCAN>
  </RESPONSE>
</COMPLIANCE_SCAN_RESULT_OUTPUT>
```

Updated DTD:

DTD: <platform API server>/api/2.0/fo/scan/compliance/compliance_scan_result_output.dtd

We have added new elements in the DTD. The new elements are shown in bold.

```
<!ELEMENT COMPLIANCE_SCAN_RESULT_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)>
...
<!-- INFORMATION ABOUT THE SCAN -->
```

```
<!ELEMENT HEADER (NAME, GENERATION_DATETIME, COMPANY_INFO, USER_INFO,
KEY+, ASSET_GROUPS?, FQDNS?, OPTION_PROFILE?)>
<!ELEMENT NAME (#PCDATA)*>
<!ELEMENT GENERATION_DATETIME (#PCDATA)*>

<!ELEMENT COMPANY_INFO (NAME, ADDRESS, CITY, STATE, COUNTRY, ZIP_CODE)>
<!ELEMENT ADDRESS (#PCDATA)>
<!ELEMENT CITY (#PCDATA)>
<!ELEMENT STATE (#PCDATA)>
<!ELEMENT COUNTRY (#PCDATA)>
<!ELEMENT ZIP_CODE (#PCDATA)>

<!ELEMENT USER_INFO (NAME, USERNAME?, ROLE)>
<!ELEMENT USERNAME (#PCDATA)*>
<!ELEMENT ROLE (#PCDATA)*>

<!ELEMENT FQDNS (FQDN+)>
<!ELEMENT FQDN (#PCDATA)>
<!-- NAME of the asset group with the TYPE attribute with possible values
of (DEFAULT | EXTERNAL | ISCANNER) -->
<!ELEMENT ASSET_GROUP (ASSET_GROUP_TITLE)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>
...
<!ATTLIST INSTANCE_INFO key CDATA #IMPLIED>

<!ELEMENT AUTH_DISCOVERY_INSTANCE_LIST (AUTH_DISCOVERY_INSTANCE*)>
<!ELEMENT AUTH_DISCOVERY_INSTANCE (AUTH_TYPE, AUTH_PARAM_LIST?, IP)>

<!ELEMENT AUTH_DISCOVERY_INSTANCE_NOT_FOUND_LIST
(AUTH_DISCOVERY_INSTANCE_NOT_FOUND*)>
<!ELEMENT AUTH_DISCOVERY_INSTANCE_NOT_FOUND (AUTH_TYPE, IP)>

<!ELEMENT AUTH_DISCOVERY_INSTANCE_NOT_COLLECTED (AUTH_TYPE_LIST*)>
<!ELEMENT AUTH_TYPE_LIST (AUTH_TYPE*)>

<!ELEMENT AUTH_PARAM_LIST (AUTH_PARAM+)>
<!ELEMENT AUTH_TYPE (#PCDATA)>
<!ELEMENT AUTH_PARAM (#PCDATA)>
<!ATTLIST AUTH_PARAM name CDATA #IMPLIED>

<!ELEMENT FAILED (IP,INSTANCE?)>
<!ELEMENT SUCCESS (IP,INSTANCE?)>
<!ELEMENT INSUFFICIENT (IP,INSTANCE?)>
<!ELEMENT CONFIG_ISSUE (IP, INSTANCE)>
<!-- EOF -->
```

Host List and Host List Detection API Outputs to Show Asset ID and Cloud Provider Tags

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

View Asset IDs

We added a new "ASSET ID" tag to the Host List and Host List Detection API outputs to show you the asset IDs of the scanned hosts. A new parameter "show_asset_id" is added to the Host List and Host List Detection APIs. This parameter accepts value 0 or 1. When you set this parameter to 1 in the API request, we will show you the asset IDs of the scanned hosts in the API outputs in the new ASSET ID tag. The “show_asset_id” parameter is set to 0 when not specified. When set to 0, we do not show the asset id information for the scanned hosts in the Host list report.

View Cloud Provider Tags

We also added a new tag “Cloud Provider Tags” to the Host List and Host List Detection API outputs to show you the cloud tags and their values for the assets. For a host, the “Cloud Provider Tags” tag will show the cloud tag’s name, value, last success date for each cloud tag.

We added two new parameters “show_cloud_tags” and “cloud_tag_fields” to the Host List and Host List Detection APIs that you need to configure to view the cloud tags in “Cloud Provider Tags” for the hosts listed in the API output.

The “show_cloud_tags” parameter accepts 0 or 1. This parameter must be set to 1 in the API request for the Host List and Host List Detection APIs to show the Cloud Provider Tags.

The “cloud_tag_fields” parameter accepts comma-separated values as “key” and "key and value" combinations. When specified in the request, we will list the hosts in the output that have cloud tags with the specified “key” and “key and value” combinations and show information of only these cloud tags. The cloud_tag_fields parameter can only set when show_cloud_tags is set.

If the “cloud_tag_fields” parameter is not specified and the “show_cloud_tags” parameter is set, then we will show all the cloud tags and their values for each host in the API outputs. In the Host list Detection reports, we will now show the cloud tags information in the Cloud Providers Tags.

Reports

We now support CSV_MS_EXCEL and CSV_MS_EXCEL_NO_METADATA formats for outputs. When selected, we use the same CSV format to download the output only that the maximum length of the string allowed in a column will be 31500 characters. Data will be truncated if the length of the string exceeds 31500 characters.

Input Parameters

We have added these input parameters to the Host List and Host List Detection APIs.Refer to the Qualys API (VM,PC) User Guide for full details on the Host List and Host List Detection APIs.

Parameter	Description
action=list	(Required)
show_asset_id={**0**|1}	(Optional) When specified in the Host List and Host List Detection API requests, we show the asset ID of the scanned hosts in the output. The default value of this parameter is set to 0. When set to 0, we do not show the asset id information for the scanned hosts.
show_cloud_tags={**0**|1}	(Optional) When specified in the Host List and Host List Detection API requests, we show the "Cloud Provider Tags" tag for each host in the API outputs. The "Cloud Provider Tags" tag will show the cloud tag's name, value, last success date for each cloud tag. The default value of this parameter is set to 0.
cloud_tag_fields	(Optional) The cloud_tag_fields parameter accepts comma-separated values of "key" and "key and value" combinations for cloud tags that you want to view. When specified in the request, we will list the hosts in the API output that have cloud tags with the specified "keys" or "keys and values". For each cloud tag, we show the cloud tag's name, value, last success date. The cloud_tag_fields parameter can only be set when the show_cloud_tags parameter is set to 1. If the cloud_tag_fields parameter is not specified and show_cloud_tags is set, then we will show all the cloud tags and their values in the "Cloud Provider Tags" tag for each host in the API outputs.

Parameter	Description
output_format={XML|CSV|CSV_NO_METADATA|MS_EXCEL|CSV_MS_EXCEL|CSV_MS_EXCEL_NO_METADATA	(Optional) Specifies the format of the host detection list output. When not specified, the output format is XML. A valid value is XML, CSV, or CSV_NO_METADATA. XML (default), CSV_MS_EXCEL or CSV_MS_EXCEL_NO_METADATA. Specifies XML format for the output. CSV. Specifies CSV format for the output. The output is structured in these sections: HEADER_CSV (lists input parameters specified during the list request if echo_request=1 is also specified), BODY_CSV (lists host records matching filters) and FOOTER_CSV (lists status messages and truncation details, if applicable). CSV_NO_METADATA. Specifies CSV format for the output with no metadata. In this case, the output will not be structured with header, body and footer sections, and will not indicate whether the list is truncated. For CSV_MS_EXCEL and CSV_MS_EXCEL_NO_METADATA, we use the same CSV format to download the output only that the maximum length of the string allowed in a column will be 31500 characters. Data will be truncated if the length of the string exceeds 31500 characters.

Sample - List host asset IDs in the Host List Output

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=list&show_asset_id=1"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/"
```

XML output:

```
...
<HOST_LIST_OUTPUT>
<HOST_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2018-10-10T10:13:47Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>136049</ID>
                <ASSET_ID>
                <![CDATA[156847]]>
                </ASSET_ID>
                <IP>10.10.10.2</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>20011401</NETWORK_ID>
                <DNS>
```

```
                    <![CDATA[10-10-10-2.bogus.tld]]>
                </DNS>
                <OS>
                    <![CDATA[Red Hat Enterprise Linux ES 3]]>
                </OS>
                <TAGS>
                    <TAG>
                        <TAG_ID>
                            <![CDATA[7508434]]>
                        </TAG_ID>
                        <NAME>
                            <![CDATA[BU1]]>
                        </NAME>
                    </TAG>
                </TAGS>
            </HOST>
</HOST_LIST_OUTPUT>
```

Sample - List host asset IDs in the Host List Detection Output

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=list&show_asset_id=1"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/"
```

XML output:

```
...
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
        <DATETIME>2020-09-08T11:05:17Z</DATETIME>
        <!-- keep-alive for HOST_LIST_VM_DETECTION_OUTPUT  -->
        <HOST_LIST>
            <HOST>
                <ID>136049</ID>
                <ASSET_ID><![CDATA[156847]]>
                </ASSET_ID>
                <IP>10.10.10.2</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>20011401</NETWORK_ID>
                <OS>
                    <![CDATA[Red Hat Enterprise Linux ES 3]]>
                </OS>
                <DNS>
                    <![CDATA[10-10-10-2.bogus.tld]]>
                </DNS>
                <LAST_SCAN_DATETIME>2020-09-05T10:33:59Z
                </LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2020-09-05T10:32:32Z
                </LAST_VM_SCANNED_DATE>
```

```
                <LAST_VM_SCANNED_DURATION>13</LAST_VM_SCANNED_DURATION>
                <LAST_VM_AUTH_SCANNED_DATE>2020-09-05T10:32:32Z
                </LAST_VM_AUTH_SCANNED_DATE>
          <LAST_VM_AUTH_SCANNED_DURATION>13</LAST_VM_AUTH_SCANNED_DURATION>
                <DETECTION_LIST>
                    <DETECTION>
                        <QID>11</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>4</SEVERITY>
                        <SSL>0</SSL>
                        <RESULTS>
                        <![CDATA[Name
                          Program Version Protocol Port
                          portmap/rpcbind 100000  2   tcp 111
                          portmap/rpcbind 100000  2   udp 111]]>
                        </RESULTS>
                        <STATUS>New</STATUS>
                        <FIRST_FOUND_DATETIME>2020-09-05T10:31:10Z
                        </FIRST_FOUND_DATETIME>
                        <LAST_FOUND_DATETIME>2020-09-05T10:31:10Z
                        </LAST_FOUND_DATETIME>
                        <TIMES_FOUND>1</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2020-09-05T10:31:10Z
                        </LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2020-09-05T10:34:39Z
                        </LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                    </DETECTION_LIST>
            </HOST>
         </HOST_LIST>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Sample - Host List Detection CSV report showing Asset ID column

The sample CSV report shows a new column Asset ID at the end.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=list&show_asset_id=1&output_format=CSV"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/"
```

CSV Report

Host ID	Asset ID	IP Address	Tracking N	Network II	Operating
7930704	733950	10.115.110.144	IP	0	Windows
7930704	733950	10.115.110.144	IP	0	Windows
7930704	733950	10.115.110.144	IP	0	Windows

Sample - List hosts with Cloud Provider Tags in the Host List Output

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=list&show_cloud_tags=1&ids=7929700&cloud_tag_fields=Name13,Name11
,SomeTag6:AY_ec2_tag_duplicate,SomeTag7:AY_ec2_tag"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/"
```

XML output:

```
...
<HOST_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2020-09-12T13:34:46Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>7913991</ID>
                <IP>10.0.0.112</IP>
                <TRACKING_METHOD>EC2</TRACKING_METHOD>
                <NETWORK_ID>6001</NETWORK_ID>
                <DNS>
                    <![CDATA[aws]]>
                </DNS>
                <CLOUD_PROVIDER>
                    <![CDATA[AWS]]>
                </CLOUD_PROVIDER>
                <CLOUD_SERVICE>
                    <![CDATA[EC2]]>
                </CLOUD_SERVICE>
                <CLOUD_RESOURCE_ID>
                    <![CDATA[i-940587e123dd]]>
                </CLOUD_RESOURCE_ID>
                <!-- <EC2_INSTANCE_ID> tag has been deprecated. Please
refer to <CLOUD_RESOURCE_ID> tag for the same information //-->
                <EC2_INSTANCE_ID>
                    <![CDATA[i-940587e123dd]]>
                </EC2_INSTANCE_ID>
                <NETBIOS>
                    <![CDATA[SOMEEC2NAME]]>
```

```
                </NETBIOS>
                <CLOUD_PROVIDER_TAGS>
                    <CLOUD_TAG>
                        <NAME>
                            <![CDATA[Name13]]>
                        </NAME>
                        <VALUE>
                            <![CDATA[13AWS_instance_service_tag]]>
                        </VALUE>
                        <LAST_SUCCESS_DATE>2020-09-
12T00:00:00Z</LAST_SUCCESS_DATE>
                    </CLOUD_TAG>
                </CLOUD_PROVIDER_TAGS>
            </HOST>
            <HOST>
                <ID>7929700</ID>
                <IP>10.10.27.0</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <DNS>
                    <![CDATA[10-10-27-0.bogus.tld]]>
                </DNS>
                <NETBIOS>
                    <![CDATA[SYS_10_10_27_0]]>
                </NETBIOS>
                <OS>
                    <![CDATA[Windows Server 2003 Service Pack 1]]>
                </OS>
                <CLOUD_PROVIDER_TAGS>
                    <CLOUD_TAG>
                        <NAME>
                            <![CDATA[SomeTag6]]>
                        </NAME>
                        <VALUE>
                            <![CDATA[AY_ec2_tag_duplicate]]>
                        </VALUE>
                        <LAST_SUCCESS_DATE>2020-09-
12T00:00:00Z</LAST_SUCCESS_DATE>
                    </CLOUD_TAG>
                    <CLOUD_TAG>
                        <NAME>
                            <![CDATA[Name11]]>
                        </NAME>
                        <VALUE>
                            <![CDATA[11AWS_instance_service_tag]]>
                        </VALUE>
                        <LAST_SUCCESS_DATE>2020-09-
12T00:00:00Z</LAST_SUCCESS_DATE>
                    </CLOUD_TAG>
```

```
                </CLOUD_PROVIDER_TAGS>
            </HOST>
        </HOST_LIST>
    </RESPONSE>
</HOST_LIST_OUTPUT>
```

Sample - List hosts with Cloud Provider Tags in the Host List Detection Output

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=list&show_cloud_tags=1&ids=7929700&cloud_tag_fields=Name13,Name11
,SomeTag6:AY_ec2_tag_duplicate,SomeTag7:AY_ec2_tag"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/"
```

XML output:

```
...
"https://qualysapi.qualys.com//api/2.0/fo/asset/host/vm/detection/host_li
st_vm_detection_output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
    <RESPONSE>
        <DATETIME>2020-09-09T13:36:35Z</DATETIME>
        <HOST_LIST>
            <HOST>
                <ID>7929700</ID>
                <IP>10.10.27.0</IP>
                <TRACKING_METHOD>IP</TRACKING_METHOD>
                <NETWORK_ID>0</NETWORK_ID>
                <OS>
                    <![CDATA[Windows Server 2003 Service Pack 1]]>
                </OS>
                <DNS>
                    <![CDATA[10-10-27-0.bogus.tld]]>
                </DNS>
                <NETBIOS>
                    <![CDATA[SYS_10_10_27_0]]>
                </NETBIOS>
                <LAST_SCAN_DATETIME>2020-07-
24T09:47:05Z</LAST_SCAN_DATETIME>
                <LAST_VM_SCANNED_DATE>2020-09-
09T10:18:08Z</LAST_VM_SCANNED_DATE>
                <LAST_VM_SCANNED_DURATION>26</LAST_VM_SCANNED_DURATION>
                <LAST_VM_AUTH_SCANNED_DATE>2020-07-
20T10:18:08Z</LAST_VM_AUTH_SCANNED_DATE>
        <LAST_VM_AUTH_SCANNED_DURATION>26</LAST_VM_AUTH_SCANNED_DURATION>
                <CLOUD_PROVIDER_TAGS>
                    <CLOUD_TAG>
                        <NAME>
                            <![CDATA[Name11]]>
```

```
                        </NAME>
                        <VALUE>
                            <![CDATA[11AWS_instance_service_tag]]>
                        </VALUE>
                        <LAST_SUCCESS_DATE>2020-09-
09T00:00:00Z</LAST_SUCCESS_DATE>
                    </CLOUD_TAG>
                    <CLOUD_TAG>
                        <NAME>
                            <![CDATA[SomeTag6]]>
                        </NAME>
                        <VALUE>
                            <![CDATA[AY_ec2_tag_duplicate]]>
                        </VALUE>
                        <LAST_SUCCESS_DATE>2020-02-
03T00:00:00Z</LAST_SUCCESS_DATE>
                    </CLOUD_TAG>
                    <CLOUD_TAG>
                        <NAME>
                            <![CDATA[SomeTag7]]>
                        </NAME>
                        <VALUE>
                            <![CDATA[AY_ec2_tag]]>
                        </VALUE>
                        <LAST_SUCCESS_DATE>2020-02-
03T00:00:00Z</LAST_SUCCESS_DATE>
                    </CLOUD_TAG>
                </CLOUD_PROVIDER_TAGS>
                <DETECTION_LIST>
                    <DETECTION>
                        <QID>10592</QID>
                        <TYPE>Confirmed</TYPE>
                        <SEVERITY>2</SEVERITY>
                        <PORT>9570</PORT>
                        <PROTOCOL>tcp</PROTOCOL>
                        <FQDN>
                            <![CDATA[10-10-27-
0.bogus.tld.vuln.qa.qualys.com]]>
                        </FQDN>
                        <SSL>0</SSL>
                        <RESULTS>
                            <![CDATA[GET /examples/servlet/SnoopServlet
HTTP/1.0
Host: %s ==&gt; javax.servlet.context.tempdir =
C:\tivoli\itsanm\agent\servlet\work\localhost\examples]]>
                        </RESULTS>
                        <STATUS>Active</STATUS>
                        <FIRST_FOUND_DATETIME>2020-07-
20T04:41:21Z</FIRST_FOUND_DATETIME>
```

```
                        <LAST_FOUND_DATETIME>2020-07-
20T10:18:08Z</LAST_FOUND_DATETIME>
                        <TIMES_FOUND>2</TIMES_FOUND>
                        <LAST_TEST_DATETIME>2020-07-
20T10:18:08Z</LAST_TEST_DATETIME>
                        <LAST_UPDATE_DATETIME>2020-07-
20T10:15:06Z</LAST_UPDATE_DATETIME>
                        <IS_IGNORED>0</IS_IGNORED>
                        <IS_DISABLED>0</IS_DISABLED>
                        <LAST_PROCESSED_DATETIME>2020-07-
20T10:15:06Z</LAST_PROCESSED_DATETIME>
                    </DETECTION>
```

Sample - Host List Detection CSV report showing Cloud Provider Tags column

The sample CSV report shows a new column Cloud Provider Tags at the end.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=list&show_cloud_tags=1&ids=7929700&cloud_tag_fields=Name13,Name11
,SomeTag6:AY_ec2_tag_duplicate,SomeTag7:AY_ec2_tag&output_format=CSV"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/"
```

CSV Report

Disabled	Times Fou	Service	Last Proce	Cloud Provider Tags
0	2		2020-07-2	Company:Qualys Tech Services,Name:AWS_instance_service_ta
0	2		2020-07-2	Company:Qualys Tech Services,Name:AWS_instance_service_ta
0	2		2020-07-2	Company:Qualys Tech Services,Name:AWS_instance_service_ta
0	2		2020-07-2	Company:Qualys Tech Services,Name:AWS_instance_service_ta
0	2		2020-07-2	Company:Qualys Tech Services,Name:AWS_instance_service_ta
0	2		2020-07-2	Company:Qualys Tech Services,Name:AWS_instance_service_ta
0	2		2020-07-2	Company:Qualys Tech Services,Name:AWS_instance_service_ta
0	2		2020-07-2	Company:Qualys Tech Services,Name:AWS_instance_service_ta
0	2		2020-07-2	Company:Qualys Tech Services,Name:AWS_instance_service_ta
0	2		2020-07-2	Company:Qualys Tech Services,Name:AWS_instance_service_ta
0	2		2020-07-2	Company:Qualys Tech Services,Name:AWS_instance_service_ta
0	2		2020-07-2	Company:Qualys Tech Services,Name:AWS_instance_service_ta
0	2		2020-07-2	Company:Qualys Tech Services,Name:AWS_instance_service_ta

Updated DTD:

DTD: <platform API server>/api/2.0/fo/asset/host/host_list_output.dtd

We added new elements in the DTD.

ASSET_ID - We show the asset ID information in the Host List API output when the show_asset_id parameter is set to 1 in the API request,

CLOUD_PROVIDER_TAGS - We show in the API output the cloud provider tag information for each host when show_cloud_tag is set 1 in the request. We have also added these elements under CLOUD_PROVIDER_TAGS: CLOUD_TAG and in CLOUD_TAG these are elements: NAME, VALUE, LAST_SUCCESS_DATE. The new elements are shown in bold.

```
<!-- QUALYS HOST_OUTPUT DTD -->
<!ELEMENT HOST_LIST_OUTPUT (REQUEST?,RESPONSE)>

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

<!ELEMENT RESPONSE (DATETIME, (HOST_LIST|ID_SET)?, WARNING?, GLOSSARY?)>
<!ELEMENT HOST_LIST (HOST+)>
<!ELEMENT HOST (ID, ASSET_ID?, IP?, TRACKING_METHOD?, NETWORK_ID?,
                DNS?, CLOUD_PROVIDER?, CLOUD_SERVICE?,
                CLOUD_RESOURCE_ID?, EC2_INSTANCE_ID?, NETBIOS?, OS?,
                QG_HOSTID?, TAGS?, METADATA?, LAST_VULN_SCAN_DATETIME?,
                LAST_VM_SCANNED_DATE?, LAST_VM_SCANNED_DURATION?,
                LAST_VM_AUTH_SCANNED_DATE?,
                LAST_VM_AUTH_SCANNED_DURATION?,
                LAST_COMPLIANCE_SCAN_DATETIME?,
                LAST_SCAP_SCAN_DATETIME?, OWNER?, COMMENTS?, USER_DEF?,
                ASSET_G ROUP_IDS?, CLOUD_PROVIDER_TAGS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT ASSET_ID (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT TRACKING_METHOD (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT EC2_INSTANCE_ID (#PCDATA)>
<!ELEMENT CLOUD_PROVIDER (#PCDATA)>
<!ELEMENT CLOUD_SERVICE (#PCDATA)>
```

```
<!ELEMENT CLOUD_RESOURCE_ID (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT OS (#PCDATA)>
<!ELEMENT QG_HOSTID (#PCDATA)>
<!ELEMENT TAGS (TAG*)>
<!ELEMENT TAG (TAG_ID?, NAME?)>
<!ELEMENT TAG_ID (#PCDATA)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT LAST_VULN_SCAN_DATETIME (#PCDATA)>
<!ELEMENT LAST_VM_SCANNED_DATE (#PCDATA)>
<!ELEMENT LAST_VM_SCANNED_DURATION (#PCDATA)>
<!ELEMENT LAST_VM_AUTH_SCANNED_DATE (#PCDATA)>
<!ELEMENT LAST_VM_AUTH_SCANNED_DURATION (#PCDATA)>
<!ELEMENT LAST_COMPLIANCE_SCAN_DATETIME (#PCDATA)>
<!ELEMENT LAST_SCAP_SCAN_DATETIME (#PCDATA)>
<!ELEMENT OWNER (#PCDATA)>
<!ELEMENT COMMENTS (#PCDATA)>
<!ELEMENT USER_DEF (LABEL_1?, LABEL_2?, LABEL_3?, VALUE_1?, VALUE_2?,
VALUE_3?)>
<!ELEMENT LABEL_1 (#PCDATA)>
<!ELEMENT LABEL_2 (#PCDATA)>
<!ELEMENT LABEL_3 (#PCDATA)>
<!ELEMENT VALUE_1 (#PCDATA)>
<!ELEMENT VALUE_2 (#PCDATA)>
<!ELEMENT VALUE_3 (#PCDATA)>

<!ELEMENT METADATA (EC2|GOOGLE|AZURE)+>
<!ELEMENT EC2 (ATTRIBUTE*)>
<!ELEMENT GOOGLE (ATTRIBUTE*)>
<!ELEMENT AZURE (ATTRIBUTE*)>
<!ELEMENT ATTRIBUTE
(NAME,LAST_STATUS,VALUE,LAST_SUCCESS_DATE?,LAST_ERROR_DATE?,LAST_ERROR?)>
<!ELEMENT LAST_STATUS (#PCDATA)>
<!ELEMENT LAST_SUCCESS_DATE (#PCDATA)>
<!ELEMENT LAST_ERROR_DATE (#PCDATA)>
<!ELEMENT LAST_ERROR (#PCDATA)>

<!ELEMENT CLOUD_PROVIDER_TAGS (CLOUD_TAG*)>
<!ELEMENT CLOUD_TAG (NAME, VALUE, LAST_SUCCESS_DATE)>

<!ELEMENT ASSET_GROUP_IDS (#PCDATA)>

<!ELEMENT ID_SET ((ID|ID_RANGE)+)>
<!ELEMENT ID_RANGE (#PCDATA)>

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

```
<!ELEMENT GLOSSARY (USER_DEF?, USER_LIST?, ASSET_GROUP_LIST?)>

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

<!ELEMENT ASSET_GROUP_LIST (ASSET_GROUP+)>
<!ELEMENT ASSET_GROUP (ID, TITLE)>
<!ELEMENT TITLE (#PCDATA)>
<!-- EOF -->
```

DTD: <platform API server>/api/2.0/fo/asset/host/vm/detection/host_list_vm_detection_output.dtd

We added new elements in the DTD.

ASSET_ID - We show the asset ID information in the Host List API output when the show_asset_id parameter is set to 1 in the API request,

CLOUD_PROVIDER_TAGS - We show in the API output the cloud provider tag information for each host when show_cloud_tag is set 1 in the request. We have also added these elements under CLOUD_PROVIDER_TAGS: CLOUD_TAG and in CLOUD_TAG these are elements: NAME, VALUE, LAST_SUCCESS_DATE. The new elements are shown in bold.

```
<!-- QUALYS HOST_LIST_VM_DETECTION_OUTPUT DTD -->
<!ELEMENT HOST_LIST_VM_DETECTION_OUTPUT (REQUEST?,RESPONSE)>

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

<!ELEMENT RESPONSE (DATETIME, HOST_LIST?, WARNING?)>
<!ELEMENT HOST_LIST (HOST+)>
<!ELEMENT HOST (ID, IP?, ASSET_ID?, IPV6?, TRACKING_METHOD?, NETWORK_ID?,
                OS?, OS_CPE?, DNS?, CLOUD_PROVIDER?, CLOUD_SERVICE?,
                CLOUD_RESOURCE_ID?, EC2_INSTANCE_ID?, NETBIOS?,
                QG_HOSTID?, LAST_SCAN_DATETIME?, LAST_VM_SCANNED_DATE?,
                LAST_VM_SCANNED_DURATION?, LAST_VM_AUTH_SCANNED_DATE?,
                LAST_VM_AUTH_SCANNED_DURATION?, LAST_PC_SCANNED_DATE?,
                TAGS?, METADATA?, CLOUD_PROVIDER_TAGS?, DETECTION_LIST)>
```

```
<!ELEMENT ID (#PCDATA)>
<!ELEMENT ASSET_ID (#PCDATA)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IPV6 (#PCDATA)>
<!ELEMENT TRACKING_METHOD (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT OS (#PCDATA)>
<!ELEMENT OS_CPE (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT CLOUD_PROVIDER (#PCDATA)>
<!ELEMENT CLOUD_SERVICE (#PCDATA)>
<!ELEMENT CLOUD_RESOURCE_ID (#PCDATA)>
<!ELEMENT EC2_INSTANCE_ID (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT QG_HOSTID (#PCDATA)>
<!ELEMENT LAST_SCAN_DATETIME (#PCDATA)>
<!ELEMENT LAST_VM_SCANNED_DATE (#PCDATA)>
<!ELEMENT LAST_VM_SCANNED_DURATION (#PCDATA)>
<!ELEMENT LAST_VM_AUTH_SCANNED_DATE (#PCDATA)>
<!ELEMENT LAST_VM_AUTH_SCANNED_DURATION (#PCDATA)>
<!ELEMENT LAST_PC_SCANNED_DATE (#PCDATA)>
<!ELEMENT TAGS (TAG+)>
<!ELEMENT TAG (TAG_ID?, NAME, COLOR?, BACKGROUND_COLOR?)>
<!ELEMENT TAG_ID (#PCDATA)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT COLOR (#PCDATA)>
<!ELEMENT BACKGROUND_COLOR (#PCDATA)>
<!ELEMENT METADATA (EC2|GOOGLE|AZURE)+>
<!ELEMENT EC2 (ATTRIBUTE*)>
<!ELEMENT GOOGLE (ATTRIBUTE*)>
<!ELEMENT AZURE (ATTRIBUTE*)>
<!ELEMENT ATTRIBUTE
(NAME,LAST_STATUS,VALUE,LAST_SUCCESS_DATE?,LAST_ERROR_DATE?,LAST_ERROR?)>
<!ELEMENT LAST_STATUS (#PCDATA)>
<!ELEMENT LAST_SUCCESS_DATE (#PCDATA)>
<!ELEMENT LAST_ERROR_DATE (#PCDATA)>
<!ELEMENT LAST_ERROR (#PCDATA)>
<!ELEMENT CLOUD_PROVIDER_TAGS (CLOUD_TAG*)>
<!ELEMENT CLOUD_TAG (NAME, VALUE, LAST_SUCCESS_DATE)>
<!ELEMENT DETECTION_LIST (DETECTION+)>
<!ELEMENT DETECTION (QID, TYPE, SEVERITY?, PORT?, PROTOCOL?, FQDN?, SSL?,
                     INSTANCE?, RESULTS?, STATUS?,
                     FIRST_FOUND_DATETIME?, LAST_FOUND_DATETIME?,
                     TIMES_FOUND?,
                     LAST_TEST_DATETIME?,
                     LAST_UPDATE_DATETIME?,
                     LAST_FIXED_DATETIME?,
                     FIRST_REOPENED_DATETIME?, LAST_REOPENED_DATETIME?,
                     TIMES_REOPENED?,
```

```
                        SERVICE?, IS_IGNORED?, IS_DISABLED?,
                        AFFECT_RUNNING_KERNEL?, AFFECT_RUNNING_SERVICE?,
                        AFFECT_EXPLOITABLE_CONFIG?,
                        LAST_PROCESSED_DATETIME? )>

<!ELEMENT QID (#PCDATA)>
<!ELEMENT TYPE (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT PROTOCOL (#PCDATA)>
<!ELEMENT FQDN (#PCDATA)>
<!ELEMENT SSL (#PCDATA)>
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT RESULTS (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT SEVERITY (#PCDATA)>
<!ELEMENT FIRST_FOUND_DATETIME (#PCDATA)>
<!ELEMENT LAST_FOUND_DATETIME (#PCDATA)>
<!ELEMENT TIMES_FOUND (#PCDATA)>
<!ELEMENT LAST_TEST_DATETIME (#PCDATA)>
<!ELEMENT LAST_UPDATE_DATETIME (#PCDATA)>
<!ELEMENT LAST_FIXED_DATETIME (#PCDATA)>
<!ELEMENT FIRST_REOPENED_DATETIME (#PCDATA)>
<!ELEMENT LAST_REOPENED_DATETIME (#PCDATA)>
<!ELEMENT TIMES_REOPENED (#PCDATA)>
<!ELEMENT SERVICE (#PCDATA)>
<!ELEMENT IS_IGNORED (#PCDATA)>
<!ELEMENT IS_DISABLED (#PCDATA)>
<!ELEMENT AFFECT_RUNNING_KERNEL (#PCDATA)>
<!ELEMENT AFFECT_RUNNING_SERVICE (#PCDATA)>
<!ELEMENT AFFECT_EXPLOITABLE_CONFIG (#PCDATA)>
<!ELEMENT LAST_PROCESSED_DATETIME (#PCDATA)>
<!ELEMENT WARNING (CODE?, TEXT, URL?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!-- EOF -->
```

API Support for Kubernetes Authentication Record

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

We have added API support for creating an authentication record for Kubernetes 1.x application installed on a UNIX host. Now you can create, update, list, and delete data related to Kubernetes 1.x authentication records. User permissions for this API are the same as other authentication record APIs.

Note: For now, the support for Kubernetes 1.x authentication records is available for Security Configuration Assessment and Policy Compliance only. It is not available for Vulnerability Management.

Requirement: For successful authentication scans for Kubernetes 1.x, you must also configure authentication credentials on the UNIX target hosts on which Kubernetes is installed.

A new API endpoint /api/2.0/fo/auth/Kubernetes/ is added.

The following DTD files are updated/added to support creation and management of authentication records for a Kubernetes instance running on a UNIX machine.

- auth_records.dtd

- auth_kubernetes_list_output.dtd

List all record types

Use the Authentication Record List API (/api/2.0/fo/auth/ with action=list) to list authentication records for all types. You'll see <AUTH_KUBERNETES_IDS> in the output when you have Kubernetes records in your account.

API request:

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_RECORDS_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/auth_records.dtd">
<AUTH_RECORDS_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-09-08T06:08:19Z</DATETIME>
    <AUTH_RECORDS>
      <AUTH_UNIX_IDS>
        <ID_SET>
          <ID>3047458</ID>
          <ID>3052056</ID>
        </ID_SET>
      </AUTH_UNIX_IDS>
      <AUTH_KUBERNETES_IDS>
        <ID_SET>
          <ID>3052020</ID>
          <ID>3052057</ID>
          <ID>3052067</ID>
        </ID_SET>
      </AUTH_KUBERNETES_IDS>
    </AUTH_RECORDS>
  </RESPONSE>
</AUTH_RECORDS_OUTPUT>
```

Updated DTD:

<base_url>/api/2.0/fo/auth/auth_records.dtd

The element AUTH_KUBERNETES_IDS has been added to identify Kubernetes record IDs.

```
<!-- QUALYS AUTH_RECORDS_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT AUTH_RECORDS_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_RECORDS?, WARNING_LIST?)>
```

```
<!ELEMENT AUTH_RECORDS (AUTH_UNIX_IDS?, AUTH_WINDOWS_IDS?,
AUTH_ORACLE_IDS?, AUTH_ORACLE_LISTENER_IDS?, AUTH_SNMP_IDS?,
AUTH_MS_SQL_IDS?, AUTH_IBM_DB2_IDS?, AUTH_VMWARE_IDS?, AUTH_MS_IIS_IDS?,
AUTH_APACHE_IDS?, AUTH_IBM_WEBSPHERE_IDS?, AUTH_HTTP_IDS?,
AUTH_SYBASE_IDS?, AUTH_MYSQL_IDS?, AUTH_TOMCAT_IDS?,
AUTH_ORACLE_WEBLOGIC_IDS?, AUTH_DOCKER_IDS?, AUTH_POSTGRESQL_IDS?,
AUTH_MONGODB_IDS?, AUTH_PALO_ALTO_FIREWALL_IDS?, AUTH_VCENTER_IDS?,
AUTH_JBOSS_IDS?, AUTH_MARIADB_IDS?, AUTH_INFORMIXDB_IDS?,
AUTH_MS_EXCHANGE_IDS?, AUTH_ORACLE_HTTP_SERVER_IDS?, AUTH_GREENPLUM_IDS?,
AUTH_MICROSOFT_SHAREPOINT_IDS?, AUTH_KUBERNETES_IDS? )>
...
<!ELEMENT AUTH_MARIADB_IDS (ID_SET)>
<!ELEMENT AUTH_INFORMIXDB_IDS (ID_SET)>
<!ELEMENT AUTH_MS_EXCHANGE_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_HTTP_SERVER_IDS (ID_SET)>
<!ELEMENT AUTH_GREENPLUM_IDS (ID_SET)>
<!ELEMENT AUTH_MICROSOFT_SHAREPOINT_IDS (ID_SET)>
<!ELEMENT AUTH_KUBERNETES_IDS (ID_SET)>
...
<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT ID_RANGE (#PCDATA)>
<!-- EOF -->
```

List Kubernetes authentication records

Use these parameters to list Kubernetes authentication records.

Parameter	Description
action={action}	(Required) Specify list (using GET or POST) to list records.
details={Basic}	(Optional) Default value is Basic. You can choose from None, Basic and All.
title={value}	(Optional) The title for the record. The title must be unique and may include a maximum of 255 characters (ascii).
ids={value}	(Required) Kubernetes authentication record IDs to list. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma-separated.

Sample - List Kubernetes Authentication Records with Basic Details

API request:

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_KUBERNETES_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/kubernetes/auth_kubernetes_
list_output.dtd">
<AUTH_KUBERNETES_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2020-08-30T12:33:17Z</DATETIME>
        <AUTH_KUBERNETES_LIST>
            <AUTH_KUBERNETES>
                <ID>89173</ID>
                <TITLE>
                    <![CDATA[kubernetes auth]]>
                </TITLE>
                <IP_SET>
                    <IP>10.10.2.160</IP>
                </IP_SET>
                <UNIX>
                    <UNIX_BIN_PATH>
                        <![CDATA[]]>
                    </UNIX_BIN_PATH>
                    <UNIX_CONF_PATH>
                        <![CDATA[]]>
                    </UNIX_CONF_PATH>
                </UNIX>
                <NETWORK_ID>0</NETWORK_ID>
                <CREATED>
                    <DATETIME>2020-07-05T06:03:58Z</DATETIME>
                    <BY>joe_user</BY>
                </CREATED>
                <LAST_MODIFIED>
                    <DATETIME>2020-07-05T08:08:32Z</DATETIME>
                </LAST_MODIFIED>
            </AUTH_KUBERNETES>
            <AUTH_KUBERNETES>
                <ID>94170</ID>
                <TITLE>
                    <![CDATA[kubernetes auth record]]>
                </TITLE>
                <IP_SET>
                    <IP>10.10.10.10</IP>
```

```
                    </IP_SET>
                    <UNIX>
                        <UNIX_BIN_PATH>
                            <![CDATA[/usr/bin/kubectl]]>
                        </UNIX_BIN_PATH>
                        <UNIX_CONF_PATH>
                            <![CDATA[/root/kube/config]]>
                        </UNIX_CONF_PATH>
                    </UNIX>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CREATED>
                        <DATETIME>2020-08-30T11:35:38Z</DATETIME>
                        <BY>joe_user</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2020-08-30T12:30:58Z</DATETIME>
                    </LAST_MODIFIED>
                    <COMMENTS>
                        <![CDATA[new comment]]>
                    </COMMENTS>
                </AUTH_KUBERNETES>
            </AUTH_KUBERNETES_LIST>
        </RESPONSE>
    </AUTH_KUBERNETES_LIST_OUTPUT>
```

Sample - List Kubernetes Authentication Records with All Details

API request:

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_KUBERNETES_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/kubernetes/auth_kubernetes_
list_output.dtd">
<AUTH_KUBERNETES_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-09-07T09:52:31Z</DATETIME>
    <AUTH_KUBERNETES_LIST>
      <AUTH_KUBERNETES>
        <ID>3052026</ID>
        <TITLE><![CDATA[API_K8s_5]]></TITLE>
        <IP_SET>
          <IP>10.20.32.136</IP>
        </IP_SET>
```

```
            <UNIX>
              <UNIX_BIN_PATH><![CDATA[/usr/bin/kubectrl]]></UNIX_BIN_PATH>

<UNIX_CONF_PATH><![CDATA[/usr/.kube/configuration]]></UNIX_CONF_PATH>
            </UNIX>
            <NETWORK_ID>0</NETWORK_ID>
            <CREATED>
              <DATETIME>2020-09-07T08:47:38Z</DATETIME>
              <BY>pc_at</BY>
            </CREATED>
            <LAST_MODIFIED>
              <DATETIME>2020-09-07T08:47:38Z</DATETIME>
            </LAST_MODIFIED>
          </AUTH_KUBERNETES>
        </AUTH_KUBERNETES_LIST>
        <GLOSSARY>
          <USER_LIST>
            <USER>
              <USER_LOGIN>pc_at</USER_LOGIN>
              <FIRST_NAME>a</FIRST_NAME>
              <LAST_NAME>t</LAST_NAME>
            </USER>
          </USER_LIST>
        </GLOSSARY>
      </RESPONSE>
</AUTH_KUBERNETES_LIST_OUTPUT>
```

New DTD:

<base_url>//api/2.0/fo/auth/kubernetes/auth_kubernetes_list_output.dtd

```
<!-- QUALYS AUTH_KUBERNETES_LIST_OUTPUT DTD -->
<!ELEMENT AUTH_KUBERNETES_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_KUBERNETES_LIST|ID_SET)?,
WARNING_LIST?, GLOSSARY?)>
<!ELEMENT AUTH_KUBERNETES_LIST (AUTH_KUBERNETES+)>
<!ELEMENT AUTH_KUBERNETES (ID, TITLE, IP_SET, UNIX?, NETWORK_ID?, CREATED,
```

```
LAST_MODIFIED, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT UNIX (UNIX_BIN_PATH?, UNIX_CONF_PATH?)>
<!ELEMENT UNIX_BIN_PATH (#PCDATA)>
<!ELEMENT UNIX_CONF_PATH (#PCDATA)>
<!ELEMENT IP_SET (IP|IP_RANGE)+>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT CREATED (DATETIME, BY)>
<!ELEMENT BY (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME)>
<!ELEMENT COMMENTS (#PCDATA)>

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

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

<!-- EOF -->
```

Sample - Create Kubernetes Authentication Record

Use these parameters to create Kubernetes authentication records.

Parameter	Description
action={action}	(Required) Specify create (using POST) to create authentication records.
title={value}	(Required to create record) The title for the record. The title must be unique and may include a maximum of 255 characters (ascii).
echo_request={0|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default, these are not included.

Parameter	Description
ips={value}	(Required) The IP address(es) for the Kubernetes targets you want to authenticate to. Multiple entries are comma separated. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
ids={value}	(Optional) Kubernetes authentication record IDs to list. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma-separated.
comments={value}	(Optional) User-defined notes about the record. Maximum of 1999 characters (ascii).
unix_bin_path={value}	(Optional) Absolute path of the 'kubectl' command.
unix_conf_path	(Optional) Absolute path of the Kubernetes configuration file.
network_id={value}	(Optional, and valid when the Networks feature is enabled) The network ID for the record.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&title=kubernetes auth
record&unix_bin_path=/usr/bin/kubectl&unix_conf_path=/root/kube/config
&ips=10.10.10.10&comments=kube auth record"
"https://qualysapi.qualys.com/api/2.0/fo/auth/kubernetes/"
```

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>2020-08-30T11:30:58Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>94170</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Delete Kubernetes Authentication Record

Use these parameters to delete one or more Kubernetes authentication records.

Parameter	Description
action={action}	(Required) Specify delete (using POST) to delete one or more authentication records.
ids={value}	(Required) Kubernetes authentication record IDs to list. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma-separated.

API request to delete single record:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=delete&ids=10000"
"https://qualysapi.qualys.com/api/2.0/fo/auth/kubernetes/"
```

API request to delete multiple records:

```
curl -u "USERNAME:PASASWORD" -H "X-Requested-With: curl" -d
"action=list&ids=10000,10001"
"https://qualysapi.qualys.com/api/2.0/fo/auth/kubernetes/"
```

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>2020-08-30T12:35:29Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Deleted</TEXT>
                <ID_SET>
                    <ID>94170</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Kubernetes Authentication Record

Use these parameters to update Kubernetes authentication records.

Parameter	Description
action={action}	(Required) Specify update (using POST) to update authentication records.
title={value}	(Required) The title for the record. The title must be unique and may include a maximum of 255 characters (ascii).
echo_request={0|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default, these are not included.
ids={value}	(Required) Kubernetes authentication record IDs to update. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma-separated.
ips={value}	(Optional) Add IP addresses of the hosts you want to scan using this record. Overwrites (replaces) the IP address(es) in the IP list for an existing authentication record. The IPs you specify are added, and any existing IPs are removed. You may enter a combination of IPs and IP ranges.
add_ips= {value}	(Optional) Add IP address(es) to the IP list for an existing authentication record. You may enter a combination of IPs and IP ranges.
remove_ips={value}	(Optional) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma-separated.
comments={value}	(Optional) User-defined notes about the record. Maximum of 1999 characters (ascii).
unix_bin_path={value}	(Optional) Absolute path of the 'kubectl' command.
unix_conf_path	(Optional) Absolute path of the Kubernetes configuration file.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=update&ids=10001&title=kubernetes auth
record&unix_bin_path=/usr/bin/kubectl&unix_conf_path=/root/kube/config"
"https://qualysapi.qualys.com/api/2.0/fo/auth/kubernetes/"
```

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>2020-08-30T12:30:58Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>94170</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Compliance Option Profile - New Option to Auto Discover IBM WebSphere App Server instances from Server Directory

API affected	/api/2.0/fo/subscription/option_profile/pc/
New or Updated API	Updated
DTD or XSD changes	No
API affected	/api/2.0/fo/subscription/option_profile/pc/?action=list
New or Updated API	Updated
DTD or XSD changes	Yes

Now when you enable auto discovery and system record creation for IBM WebSphere App Server in a compliance option profile, you can choose to discover instances from the Installation Directory (the default and current behavior) or from the Server Directory. Specify the new input parameter ibm_was_discovery_mode with a value of “server_dir” to discover instances from the server directory or “installation_dir” to discover instances from the installation directory. We also made changes to the compliance option profile list response and DTD to include the new discovery mode.

Create/Update Compliance Option Profile

You’ll use the new input parameter “ibm_was_discovery_mode” with existing parameters “enable_auth_instance_discovery=1” and “auto_auth_types=IBM WebSphere App Server”.

Input Parameters

Please refer to the Qualys API (VM, PC) User Guide for a complete list of input parameters for Compliance Option Profiles.

Parameter	Description
enable_auth_instance_discovery={0|1}	(Optional to create or update option profile record) Specify enable_auth_instance_discovery=1 to enable auto discover instances and system record creation for the chosen auth types. When unspecified (enable_auth_instance_discovery=0), we will not scan to auto discover instances.
auto_auth_types={value}	(Optional to create or update option profile record) Specify the technologies for which you want to enable auto discover instances and system record creation. Valid values are: Apache Web Server, IBM WebSphere App Server, Jboss Server, Tomcat Server and Oracle. Multiple technologies are specified as comma separated values. This parameter can only be specified if enable_auth_instance_discovery=1.

Parameter	Description
ibm_was_discovery_mode={value}	(Optional to create or update option profile record) Specify ibm_was_discovery_mode=server_dir to auto discover instances at the server directory level. Specify ibm_was_discovery_mode=installation_dir to auto discover instances at the installation directory level. When unspecified and auto_auth_types=IBM WebSphere App Server, we will auto discover instances at the installation directory level. This parameter can only be specified if auto_auth_types includes IBM WebSphere App Server.

Sample create compliance option profile

In this sample we are creating a new profile to auto discover IBM WebSphere App Server from the server directory.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -d
"action=create&title=Profile-Auth-IBM-WAS-server-
dir&enable_auth_instance_discovery=1&auto_auth_types=IBM+WebSphere+App+Se
rver&ibm_was_discovery_mode=server_dir&scan_ports=targeted"
"http://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>2020-09-24T19:16:41Z</DATETIME>
    <TEXT>Compliance Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1710286</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample update compliance option profile

In this sample we are updating an existing profile to auto discover IBM WebSphere App Server from the server directory.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -d
"action=update&id=100973&title=Profile-Auth-IBM-WAS-server-
dir&enable_auth_instance_discovery=1&auto_auth_types=IBM+WebSphere+App+Se
rver&ibm_was_discovery_mode=server_dir"
"http://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>2020-09-24T06:45:00Z</DATETIME>
    <TEXT>Compliance Option profile successfully updated.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>100973</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

List Compliance Option Profiles

Now when you list compliance option profiles and the list includes a profile with IBM WebShere App Server auto discovery enabled, you'll also see the discovery mode selected in the profile - either "installation_dir" or "server_dir".

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X GET
"action=list"
"http://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>3521499</ID>
      <GROUP_NAME><![CDATA[My-Profile]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[Patrick Slimmer (qualys_ps)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>264237</SUBSCRIPTION_ID>
      <IS_GLOBAL>0</IS_GLOBAL>
      <UPDATE_DATE>2020-09-29T17:36:48Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TARGETED_SCAN>1</TARGETED_SCAN>
      </PORTS>
      <PERFORMANCE>
        <PARALLEL_SCALING>0</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
          <HTTP_PROCESSES>10</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
      </PERFORMANCE>
      <DISSOLVABLE_AGENT>
        <DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>
        <PASSWORD_AUDITING_ENABLE>
          <HAS_PASSWORD_AUDITING_ENABLE>0</HAS_PASSWORD_AUDITING_ENABLE>
        </PASSWORD_AUDITING_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>

<WINDOWS_DIRECTORY_SEARCH_ENABLE>0</WINDOWS_DIRECTORY_SEARCH_ENABLE>
      </DISSOLVABLE_AGENT>
      <SYSTEM_AUTH_RECORD>
        <ALLOW_AUTH_CREATION>
          <AUTHENTICATION_TYPE_LIST>
            <AUTHENTICATION_TYPE>Apache Web Server</AUTHENTICATION_TYPE>
            <AUTHENTICATION_TYPE>IBM WebSphere App
Server</AUTHENTICATION_TYPE>
            <AUTHENTICATION_TYPE>Jboss Server</AUTHENTICATION_TYPE>
            <AUTHENTICATION_TYPE>Tomcat Server</AUTHENTICATION_TYPE>
```

```
            <AUTHENTICATION_TYPE>Oracle</AUTHENTICATION_TYPE>
          </AUTHENTICATION_TYPE_LIST>

<IBM_WAS_DISCOVERY_MODE>installation_dir</IBM_WAS_DISCOVERY_MODE>
          <ORACLE_AUTHENTICATION_TEMPLATE>
            <ID>2625511</ID>
            <TITLE>OracleRecordTemplate</TITLE>
          </ORACLE_AUTHENTICATION_TEMPLATE>
        </ALLOW_AUTH_CREATION>
      </SYSTEM_AUTH_RECORD>
...
```

DTD update:

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

We added a new element in the DTD. The new element is shown in bold.

```
<?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">

<!ELEMENT OPTION_PROFILES (OPTION_PROFILE)*>

<!ELEMENT OPTION_PROFILE (BASIC_INFO, SCAN, MAP?, ADDITIONAL)>

...

<!ELEMENT SYSTEM_AUTH_RECORD (ALLOW_AUTH_CREATION|INCLUDE_SYSTEM_AUTH)>
<!ELEMENT ALLOW_AUTH_CREATION (AUTHENTICATION_TYPE_LIST,
IBM_WAS_DISCOVERY_MODE?, ORACLE_AUTHENTICATION_TEMPLATE?)>
<!ELEMENT INCLUDE_SYSTEM_AUTH
(ON_DUPLICATE_USE_USER_AUTH|ON_DUPLICATE_USE_SYSTEM_AUTH)>

<!ELEMENT AUTHENTICATION_TYPE_LIST  (AUTHENTICATION_TYPE+)>
<!ELEMENT AUTHENTICATION_TYPE (#PCDATA)>
<!ELEMENT IBM_WAS_DISCOVERY_MODE  (#PCDATA)>
<!ELEMENT ORACLE_AUTHENTICATION_TEMPLATE  (ID, TITLE)>
<!ELEMENT ON_DUPLICATE_USE_USER_AUTH (#PCDATA)>
<!ELEMENT ON_DUPLICATE_USE_SYSTEM_AUTH (#PCDATA)>

...
```