Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.3

July 30, 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

Scan Virtual Machines in Azure Cloud using Cloud Perimeter Scanning

Added Windows Support for the Apache HTTP and IBM HTTP servers

Added Windows Support for the IBM WebSphere Application Server

Separate Options for Use IP Network Range Tags for Include and Exclude

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.

Scan Virtual Machines in Azure Cloud using Cloud Perimeter Scanning

API affected	/api/2.0/fo/scan/cloud/perimeter/job/
New or Updated API	Updated
DTD or XSD changes	No
API affected	/api/2.0/fo/scan/
New or Updated API	Updated
DTD or XSD changes	No
API affected	/api/2.0/fo/schedule/scan/?action=list
New or Updated API	Updated
DTD or XSD changes	Yes
API affected	/api/2.0/fo/schedule/scan/compliance/?action=list
New or Updated API	Updated
DTD or XSD changes	Yes
API affected	/api/2.0/fo/asset/host/vm/detection/
New or Updated API	Updated
DTD or XSD changes	Yes
API affected	/api/2.0/fo/asset/host/
New or Updated API	Updated
DTD or XSD changes	Yes
API affected	/api/2.0/fo/report/asset/?action=search
New or Updated API	Updated
DTD or XSD changes	Yes
API affected	/api/2.0/fo/report/
New or Updated API	Updated
DTD or XSD changes	Yes

This release introduces the ability to scan public facing virtual machines in your Azure cloud environment using Cloud Perimeter Scanning. We've also introduced a new tracking method "Azure VM" (Azure Virtual Machine) for connector based Azure VM assets, and made changes to how we report cloud asset data in different API outputs and reports. There are many API changes as outlined in the sections that follow.

Updated APIs

Create/Update Cloud Perimeter Scan Job

Fetch Scan Results API

VM Schedule Scan List API

PC Schedule Scan List API

VM Host List Detection API

Host List API

Asset Search Report API

Host Based Scan Reports

Create/Update Cloud Perimeter Scan Job

To create a cloud perimeter scan job for Azure cloud, you'll specify cloud_provider=azure and cloud_service=vm (for Azure virtual machine). For AWS EC2 scans, you'll continue to specify cloud_provider=aws and cloud_service=ec2. Note that you cannot change the cloud_provider or cloud_service values during an update request.

Good to Know

- The "Cloud Perimeter Azure VM Scan" feature must be enabled for your subscription. You'll also need these features enabled: Cloud Perimeter Scanning, EC2 Scanning and Scan by Hostname.

- Cloud perimeter scans are available for VM and PC modules. Only Managers and Unit Managers have permission to configure cloud perimeter scans.

- We allow you to create/update a cloud perimeter scan job through Cloud Perimeter Scan API even if no scan targets are resolved from the provided details. At the time of scan, if no scan targets are resolved from the provided details, the scan will not be launched, and we add the error in the Activity log and Run history of the schedule scan job.

Input Parameters

The following parameters changed. Please refer to the Qualys API (VM, PC) User Guide for a complete list of input parameters for Cloud Perimeter Scans.

Parameter	Description
cloud_provider={value}	(Optional) Specify "azure" for an Azure scan. Specify "aws" for an AWS EC2 scan. The cloud_provider value cannot be changed during an update request. When cloud_provider=azure, the following parameters cannot be specified in the same request: platform_type, region_code, vpc_id, include_micro_nano_instances, include_lb_from_connector. These parameters only apply when cloud_provider=aws is specified.
cloud_service={value}	(Optional) Specify "vm" (Azure virtual machine) for an Azure scan. Specify "ec2" for an AWS EC2 scan. The cloud_service value cannot be changed during an update request.

Sample create Azure cloud perimeter scan

Samples to create new Azure cloud perimeter scan jobs for VM and PC.

API request for VM scan:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&module=vm&active=1&schedule=now&connector_name=cv360-
engg&option_title=Initial+Options&scan_title=cloud+perimeter+az&cloud_pro
vider=azure&cloud_service=vm&iscanner_name=scanner_us&elb_dns=abc.qualys.
com"
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/index.p
hp"
```

API request for PC scan:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&module=pc&active=1&schedule=now&connector_name=cv360-
engg&option_title=Initial+PC+Options&scan_title=cloud+perimeter+az-
pc&cloud_provider=azure&cloud_service=vm&iscanner_name=scanner_us&elb_dns
=abc.qualys.com"
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/index.p
hp"
```

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>2020-06-16T21:22:20Z</DATETIME>
    <TEXT>Scan has been created successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>25348</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample update Azure cloud perimeter scan

Sample to update an Azure cloud perimeter scan job to change the connector name.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=update&id=25348&connector_name=Azure-Connector"
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/"
```

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>2020-06-16T21:24:20Z</DATETIME>
    <TEXT>Scan has been updated successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>25348</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Fetch Scan Results API

When fetching scan results using the API, you'll see the field "Scan Type" in the output when output_format=csv_extended or json_extended. For an Azure cloud perimeter scan, this field will have the value "Cloud Perimeter - Azure VM" (for Azure virtual machine).

Sample fetch scan in CSV Extended format

This sample shows the Scan Type value in the CSV output.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/scan/index.php?action=fetch&scan
_ref=scan/1589687598.05043&output_format=csv_extended"
```

CSV output:

```
"Scan Results","06/16/2020 18:37:53"
"Qualys","919 E Hillsdale Blvd",,"Foster City","California","United
States of America","94404"
"Patrick Slimmer","quays_ps","Manager"

"Launch Date","Active Hosts","Total Hosts","Type","Scan
Type","Status","Reference","Scanner Appliance","Duration","Scan
Title","Asset Groups","DNS","Excluded IPs","Option Profile","Network"
"05/17/2020 07:18:00","4",,"Scheduled","Cloud Perimeter - Azure
VM","Finished","scan/1589687598.05043","scanner_us (Scanner 11.8.29-1,
Vulnerability Signatures 2.4.893-3)","00:18:36","Cloud Scan Azure -
05/16",,"10.11.41.109, 10.20.32.216, 10.20.32.237",,"Initial
Options","Global Default Network"
...
```

Sample fetch scan in JSON Extended format

This sample shows the Scan Type value in the JSON output.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/scan/index.php?action=fetch&scan
_ref=scan/1589687598.05043&output_format=json_extended"
```

JSON output:

```
[{"scan_report_template_title":"Scan Results","result_date":"06\/16\/2020
18:36:33","company":"Qualys","add1":"919 E Hillsdale
Blvd","add2":null,"city":"Foster
City","state":"California","country":"United States of
America","zip":"94404","name":"Patrick
Slimmer","username":"quays_ps","role":"Manager"},
```

```
{"launch_date":"05\/17\/2020
07:18:00","active_hosts":"4","total_hosts":null,"type":"Scheduled","scan_
type":"Cloud Perimeter - Azure
VM","status":"Finished","reference":"scan\/1589687598.05043","scanner_app
liance":"scanner_us (Scanner 11.8.29-1, Vulnerability Signatures 2.4.893-
3)","duration":"00:18:36","scan_title":"Cloud Scan Azure -
05\/16","asset_groups":null,"dns":"10.11.41.109, 10.20.32.216,
10.20.32.237","excluded_ips":"","option_profile":"Initial
Options","network":"Global Default Network"},
...
```

VM Schedule Scan List API

When "show_cloud_details=1" is specified in the API request for a schedule scan list, you'll see Azure cloud information in the XML output under CLOUD_DETAILS for Azure cloud perimeter scans.

Sample schedule scan list

This sample shows a schedule scan list for vulnerability scans.

API request:

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/schedule_scan_list
_output.dtd">
<SCHEDULE_SCAN_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-06-22T18:00:21Z</DATETIME>
    <SCHEDULE_SCAN_LIST>
      <SCAN>
        <ID>26337</ID>
        <ACTIVE>0</ACTIVE>
        <TITLE><![CDATA[cloud perimeter azure]]></TITLE>
        <USER_LOGIN>quays_us11</USER_LOGIN>
        <TARGET><![CDATA[]]></TARGET>
        <NETWORK_ID><![CDATA[0]]></NETWORK_ID>
        <ISCANNER_NAME><![CDATA[scanner_us]]></ISCANNER_NAME>
        <CLOUD_DETAILS>
          <PROVIDER>AZURE</PROVIDER>
          <CONNECTOR>
            <ID>521404</ID>
```

```
            <UUID>c0fb4361-d7a1-4b5e-8768-bee7ab0298f1</UUID>
            <NAME><![CDATA[cv360-engg]]></NAME>
          </CONNECTOR>
          <SCAN_TYPE>Cloud Perimeter</SCAN_TYPE>
        </CLOUD_DETAILS>
...
```

DTD update:

DTD: /api/2.0/fo/schedule/scan/schedule_scan_list_output.dtd

The element CLOUD_TARGET under CLOUD_DETAILS is now optional as it only applies to AWS EC2 scans and does not apply to Azure scans.

```
<!-- QUALYS SCHEDULE_SCAN_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT SCHEDULE_SCAN_LIST_OUTPUT (REQUEST?,RESPONSE)>
...
<!ELEMENT CLOUD_DETAILS (PROVIDER, CONNECTOR, SCAN_TYPE, CLOUD_TARGET?)>
<!ELEMENT PROVIDER (#PCDATA)>
<!ELEMENT CONNECTOR (ID?, UUID, NAME)>
<!ELEMENT UUID (#PCDATA)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT SCAN_TYPE (#PCDATA)>
<!ELEMENT CLOUD_TARGET (PLATFORM, REGION?, VPC_SCOPE, VPC_LIST?)>
<!ELEMENT PLATFORM (#PCDATA)>
<!ELEMENT REGION (UUID, CODE?, NAME?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT VPC_SCOPE (#PCDATA)>
<!ELEMENT VPC_LIST (VPC+)>
<!ELEMENT VPC (UUID)>
...
```

PC Schedule Scan List API

When “show_cloud_details=1” is specified in the API request for a schedule scan list, you’ll see Azure cloud information in the XML output under CLOUD_DETAILS for Azure cloud perimeter scans.

Sample schedule scan list

This sample shows a schedule scan list for compliance scans.

API request:

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

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>2020-06-22T18:01:27Z</DATETIME>
    <COMPLIANCE_SCHEDULE_SCAN_LIST>
      <SCAN>
        <ID>25347</ID>
        <ACTIVE>0</ACTIVE>
        <TITLE><![CDATA[cloud perimeter azure compliance]]></TITLE>
        <USER_LOGIN>quays_ps</USER_LOGIN>
        <TARGET><![CDATA[]]></TARGET>
        <NETWORK_ID><![CDATA[0]]></NETWORK_ID>
        <ISCANNER_NAME><![CDATA[scanner_us]]></ISCANNER_NAME>
        <CLOUD_DETAILS>
          <PROVIDER>AZURE</PROVIDER>
          <CONNECTOR>
            <ID>521404</ID>
            <UUID>c0fb4361-d7a1-4b5e-8768-bee7ab0298f1</UUID>
            <NAME><![CDATA[cv360-engg]]></NAME>
          </CONNECTOR>
          <SCAN_TYPE>Cloud Perimeter</SCAN_TYPE>
        </CLOUD_DETAILS>
...
```

DTD update:

DTD: /api/2.0/fo/schedule/scan/compliance/compliance_schedule_scan_list_output.dtd

The element CLOUD_TARGET under CLOUD_DETAILS is now optional as it only applies to AWS EC2 scans and does not apply to Azure scans.

```
<!-- QUALYS COMPLIANCE_SCHEDULE_SCAN_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT COMPLIANCE_SCHEDULE_SCAN_LIST_OUTPUT (REQUEST?,RESPONSE)>
...
<!ELEMENT CLOUD_DETAILS (PROVIDER, CONNECTOR, SCAN_TYPE, CLOUD_TARGET?)>
<!ELEMENT PROVIDER (#PCDATA)>
<!ELEMENT CONNECTOR (ID?, UUID, NAME)>
<!ELEMENT UUID (#PCDATA)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT SCAN_TYPE (#PCDATA)>
<!ELEMENT CLOUD_TARGET (PLATFORM, REGION?, VPC_SCOPE, VPC_LIST?)>
<!ELEMENT PLATFORM (#PCDATA)>
<!ELEMENT REGION (UUID, CODE?, NAME?)>
<!ELEMENT CODE (#PCDATA)>
```

```
<!ELEMENT VPC_SCOPE (#PCDATA)>
<!ELEMENT VPC_LIST (VPC+)>
<!ELEMENT VPC (UUID)>
...
```

VM Host List Detection API

We made the following changes to the VM Host List Detection API:

- The host_metadata input accepts these values: azure, google, ec2. Use in combination with the host_metadata_fields input to only return certain metadata attributes in the output for azure, google or ec2.

- You'll see tracking method "Azure VM" in the output for connector based Azure VM assets along with Azure attributes for these assets. Agent based assets will continue to show "AGENT" as the tracking method.

- In XML output, you'll see these new tags: CLOUD_PROVIDER, CLOUD_SERVICE, CLOUD_RESOURCE_ID. These will be populated for all cloud assets (Azure, EC2, Google). New tags will only appear in the output when host_metadata is specified in the API request. Please note that the tag CLOUD_RESOURCE_ID will replace EC2_INSTANCE_ID in a future release, and EC2_INSTANCE_ID will be deprecated.

- In CSV output, you'll see these new columns: Cloud Provider, Cloud Service, Cloud Resource ID, Cloud Resource Metadata. New columns will only appear in subscriptions with the "Cloud Perimeter Azure VM Scan" feature enabled. The new column Cloud Resource Metadata will hold all metadata details in JSON format, including name, last status, value, success date, error date, last error. This column is populated for all cloud assets (Azure, EC2, Google). Please note that Cloud Resource ID will replace EC2 Instance ID in a future release, and EC2 Instance ID will be deprecated.

- In CSV output, the EC2 specific columns will continue to be populated with data for EC2, Azure and Google. These columns include EC2 Name, EC2 Last Status, EC2 Value, EC2 Success Date, EC2 Error Date, EC2 Last Error. These columns (along with EC2 Instance ID) will be deprecated in a future release.

Sample VM detection list in XML output with Azure VM asset

This sample will return the host detection list in XML output.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?action=
list&host_metadata=azure&output_format=XML"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/host_lis
t_vm_detection_output.dtd">

<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-06-22T19:00:13Z</DATETIME>
      <HOST>
        <ID>1007</ID>
        <IP>10.4.8.4</IP>
        <TRACKING_METHOD>Azure VM</TRACKING_METHOD>
        <NETWORK_ID>6000</NETWORK_ID>
        <OS><![CDATA[EulerOS / Ubuntu / Fedora / Tiny Core Linux / Linux
3.x]]></OS>
        <CLOUD_PROVIDER><![CDATA[Azure]]></CLOUD_PROVIDER>
        <CLOUD_SERVICE><![CDATA[VM]]></CLOUD_SERVICE>
        <CLOUD_RESOURCE_ID><![CDATA[399af5dc-c32a-4c40-95a5-
c6ed0e786430]]></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[399af5dc-c32a-4c40-95a5-
c6ed0e786430]]></EC2_INSTANCE_ID>
        <LAST_SCAN_DATETIME>2020-06-16T18:56:01Z</LAST_SCAN_DATETIME>
        <LAST_VM_SCANNED_DATE>2020-06-15T23:02:28Z</LAST_VM_SCANNED_DATE>
        <LAST_VM_SCANNED_DURATION>606</LAST_VM_SCANNED_DURATION>
        <LAST_VM_AUTH_SCANNED_DATE>2019-07-
24T00:00:00Z</LAST_VM_AUTH_SCANNED_DATE>
        <METADATA>
          <AZURE>
            <ATTRIBUTE>
              <NAME><![CDATA[ipv6]]></NAME>
              <LAST_STATUS>Success</LAST_STATUS>
              <VALUE><![CDATA[]]></VALUE>
              <LAST_SUCCESS_DATE>2019-07-24T00:00:00Z</LAST_SUCCESS_DATE>
              <LAST_ERROR_DATE></LAST_ERROR_DATE>
              <LAST_ERROR><![CDATA[]]></LAST_ERROR>
            </ATTRIBUTE>
            <ATTRIBUTE>
              <NAME><![CDATA[vmSize]]></NAME>
              <LAST_STATUS>Success</LAST_STATUS>
              <VALUE><![CDATA[Standard_D2s_v3]]></VALUE>
              <LAST_SUCCESS_DATE>2019-07-24T00:00:00Z</LAST_SUCCESS_DATE>
              <LAST_ERROR_DATE></LAST_ERROR_DATE>
              <LAST_ERROR><![CDATA[]]></LAST_ERROR>
            </ATTRIBUTE>
...
```

```
            </AZURE>
          </METADATA>
          <DETECTION_LIST>
            <DETECTION>
              <QID>15107</QID>
              <TYPE>Potential</TYPE>
              <SEVERITY>3</SEVERITY>
              <PORT>53</PORT>
              <PROTOCOL>tcp</PROTOCOL>
              <SSL>0</SSL>
              <RESULTS><![CDATA[Vulnerable ISC BIND - 9.9.4-RedHat-9.9.4-
38.el7_3.1 detected on port 53 over TCP.]]></RESULTS>
              <STATUS>Active</STATUS>
              <FIRST_FOUND_DATETIME>2020-05-
17T21:35:47Z</FIRST_FOUND_DATETIME>
              <LAST_FOUND_DATETIME>2020-06-
15T23:02:28Z</LAST_FOUND_DATETIME>
              <TIMES_FOUND>14</TIMES_FOUND>
              <LAST_TEST_DATETIME>2020-06-15T23:02:28Z</LAST_TEST_DATETIME>
              <LAST_UPDATE_DATETIME>2020-06-
16T18:56:01Z</LAST_UPDATE_DATETIME>
              <IS_IGNORED>0</IS_IGNORED>
              <IS_DISABLED>0</IS_DISABLED>
              <LAST_PROCESSED_DATETIME>2020-06-
16T18:56:01Z</LAST_PROCESSED_DATETIME>
            </DETECTION>
...
          </DETECTION_LIST>
        </HOST>
    </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

DTD update:

DTD: /api/2.0/fo/asset/host/vm/detection/host_list_vm_detection_output.dtd

These elements were added to the DTD: CLOUD_PROVIDER, CLOUD_SERVICE, CLOUD_RESOURCE_ID.

```
<!-- QUALYS HOST_LIST_VM_DETECTION_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT HOST_LIST_VM_DETECTION_OUTPUT (REQUEST?,RESPONSE)>
<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE,
PARAM_LIST?,POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
```

```
<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, HOST_LIST?, WARNING?)>
<!ELEMENT HOST_LIST (HOST+)>
<!ELEMENT HOST (ID, IP?, 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?, DETECTION_LIST)>
<!ELEMENT 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)>
...
```

Sample VM detection list in CSV output with Azure VM asset

This sample will return the host detection list in CSV output. New columns will only appear in the CSV output for subscriptions with the "Cloud Perimeter Azure VM Scan" feature enabled.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?action=
list&host_metadata=azure&output_format=CSV"
```

CSV output:

```
...
Host ID,IP Address,Tracking Method,Network ID,Operating System,DNS
Name,Netbios Name,Last Scan Datetime,OS CPE,Last VM Scanned Date,Last VM
Scanned Duration,Last VM Auth Scanned Date,Last VM Auth Scanned
Duration,Last PC Scanned Date,Cloud Provider,Cloud Service,Cloud Resource
ID,EC2 Instance ID,EC2 Name,EC2 Last Status,EC2 Value,EC2 Success Date,EC2
Error Date,EC2 Last Error,Cloud Resource
Metadata,QID,Type,Port,Protocol,FQDN,SSL,Instance,Status,Severity,First
Found Datetime,Last Found Datetime,Last Test Datetime,Last Update
```

```
Datetime,Last Fixed Datetime,Results,Ignored,Disabled,Times
Found,Service,Last Processed Datetime
...
1007,10.4.8.4,Azure VM,6000,EulerOS / Ubuntu / Fedora / Tiny Core Linux /
Linux 3.x,,,2020-06-16T18:56:01Z,,2020-06-15T23:02:28Z,606,2019-07-
24T00:00:00Z,,,Azure,VM,399af5dc-c32a-4c40-95a5-c6ed0e786430,399af5dc-
c32a-4c40-95a5-c6ed0e786430,ipv6,Success,,7/24/19
0:00,,,"""[{""""Name"""":""""ipv6"""",""""Last
Status"""":""""1"""",""""Value"""":null,""""Success Date"""":""""2019-07-
24 00:00:00"""",""""Error Date"""":null,""""Last
Error"""":null},{""""Name"""":""""latest\/dynamic\/instance-
identity\/document\/privateIp"""",""""Last
Status"""":""""1"""",""""Value"""":""""10.4.8.4"""",""""Success
Date"""":""""2019-07-24 00:00:00"""",""""Error Date"""":null,""""Last
Error"""":null},
...
```

Host List API

We made the following changes to the Host List API:

- The host_metadata input accepts these values: azure, google, ec2. Use in combination with the host_metadata_fields input to only return certain metadata attributes in the output for azure, google or ec2.

- You'll see tracking method "Azure VM" in the output for connector based Azure VM assets along with Azure attributes for these assets. Agent based assets will continue to show "Cloud Agent" as the tracking method.

- In XML output, you'll see these new tags: CLOUD_PROVIDER, CLOUD_SERVICE, CLOUD_RESOURCE_ID. These will be populated for all cloud assets (Azure, EC2, Google). New tags will only appear in the output when host_metadata is specified in the API request. Please note that the tag CLOUD_RESOURCE_ID will replace EC2_INSTANCE_ID in a future release, and EC2_INSTANCE_ID will be deprecated.

Sample host list with Azure metadata

This sample will return the host list with azure metadata.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/?action=list&host_met
adata=azure"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
```

```
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/host_list_output.dtd"
>
<HOST_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-06-22T18:31:51Z</DATETIME>
    <HOST_LIST>
      <HOST>
        <ID>1003</ID>
        <IP>10.95.0.69</IP>
        <TRACKING_METHOD>Cloud Agent</TRACKING_METHOD>
        <NETWORK_ID>6000</NETWORK_ID>
        <DNS><![CDATA[abc.qualys.com]]></DNS>
        <CLOUD_PROVIDER><![CDATA[Azure]]></CLOUD_PROVIDER>
        <CLOUD_SERVICE><![CDATA[VM]]></CLOUD_SERVICE>
        <CLOUD_RESOURCE_ID><![CDATA[2b21e19a-01b6-45f4-b54d-
1c4e0c5b6564]]></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[2b21e19a-01b6-45f4-b54d-
1c4e0c5b6564]]></EC2_INSTANCE_ID>
        <OS><![CDATA[NetScaler]]></OS>
        <METADATA>
          <AZURE>
            <ATTRIBUTE>
              <NAME><![CDATA[ipv6]]></NAME>
              <LAST_STATUS>Success</LAST_STATUS>
              <VALUE><![CDATA[]]></VALUE>
              <LAST_SUCCESS_DATE>2019-07-24T00:00:00Z</LAST_SUCCESS_DATE>
              <LAST_ERROR_DATE></LAST_ERROR_DATE>
              <LAST_ERROR><![CDATA[]]></LAST_ERROR>
            </ATTRIBUTE>
            <ATTRIBUTE>
              <NAME><![CDATA[latest/dynamic/instance-
identity/document/privateIp]]></NAME>
              <LAST_STATUS>Success</LAST_STATUS>
              <VALUE><![CDATA[10.95.0.69]]></VALUE>
              <LAST_SUCCESS_DATE>2019-07-24T00:00:00Z</LAST_SUCCESS_DATE>
              <LAST_ERROR_DATE></LAST_ERROR_DATE>
              <LAST_ERROR><![CDATA[]]></LAST_ERROR>
            </ATTRIBUTE>
...
          </AZURE>
        </METADATA>
      </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_OUTPUT>
```

Asset Search Report API

We made the following changes to the Asset Search Report API:

- New filter parameters include azure_vm_state, azure_vm_id, azure_vm_id_modifier. Azure filters cannot be specified in the same request as EC2 filters.

- The input parameter tracking_method will now accept the value “Azure VM” to only show assets tracked by Azure VM. You’ll also see this tracking method in the output. The input parameter azure_vm_state can only be specified when tracking_method is Azure VM or AGENT. Similarly, the parameter ec2_instance_status can only be specified when tracking_method is EC2 or AGENT.

- In XML output, you’ll see these new tags: FILTER_AZURE_VM_ID, FILTER_AZURE_VM_STATE with Azure filter values. You’ll also see CLOUD_PROVIDER, CLOUD_SERVICE, CLOUD_RESOURCE_ID. These will be populated for all cloud assets (Azure, EC2, Google). Please note that the tag CLOUD_RESOURCE_ID will replace EC2_INSTANCE_ID in a future release, and EC2_INSTANCE_ID will be deprecated.

- In CSV output, you’ll see these new columns: AzureVMID and AzureVMState which will display Azure filter values in the header section. You’ll also see new columns for CloudProvider, CloudService and CloudResourceID. These will be populated for all supported cloud assets (Azure, EC2, Google). New columns will only appear in CSV output in subscriptions with the “Cloud Perimeter Azure VM Scan” feature enabled.

- In CSV output, we will continue to populate the EC2InstanceID column for all cloud assets (Azure, EC2, Google). The EC2InstanceID column will be deprecated in a future release.

Input Parameters

The following input parameters are new or changed. Please refer to the Qualys API (VM, PC) User Guide for a complete list of input parameters for Asset Search Report API.

Parameter	Description
tracking_method={value}	(Optional) Show only IP addresses/ranges which have a certain tracking method. Valid values: IP, DNS, NETBIOS, AZURE VM, EC2, AGENT
ec2_instance_status={value}	(Optional) Specify the EC2 instance status to be searched. Possible values: RUNNING,TERMINATED, PENDING, STOPPING, SHUTTING_DOWN, STOPPED. Values are case-sensitive. ec2_instance_status is valid only when tracking_method=EC2 or tracking_method=AGENT is specified

Parameter	Description
azure_vm_state={value}	(Optional) Specify the Azure virtual machine state to be searched. Possible values are: STARTING, RUNNING, STOPPING, STOPPED, DEALLOCATING, DEALLOCATED, UNKNOWN. Values are case-sensitive. azure_vm_state is valid only when tracking_method=AZURE VM or tracking_method=AGENT is specified
azure_vm_id={value}	(Optional) Specify the Azure virtual machine ID to be searched. azure_vm_id is valid only when azure_vm_id_modifier is specified
azure_vm_id_modifier={value}	(Optional) Show only assets with azure_vm_id that is either: beginning with, containing, matching, ending with, not empty azure_vm_id_modifier is valid only when azure_vm_id is specified

Sample Asset Search Report in XML output

This sample will return the asset search report in XML format.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/report/asset/?action=search&asse
t_groups=All&azure_vm_id=399af5dc-c32a-4c40-95a5-
c6ed0e786430&azure_vm_id_modifier=beginning+with&tracking_method=AZURE+VM
&azure_vm_state=RUNNING&output_format=xml"
```

XML output:

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

<!DOCTYPE ASSET_SEARCH_REPORT SYSTEM
"https://qualysapi.qualys.com/asset_search_report_v2.dtd">

<ASSET_SEARCH_REPORT>
<HEADER>
  <COMPANY><![CDATA[Qualys]]></COMPANY>
  <USERNAME>Patrick Slimmer</USERNAME>
  <GENERATION_DATETIME>2020-06-22T23:24:25Z</GENERATION_DATETIME>
  <TOTAL>1</TOTAL>
  <FILTERS>
    <ASSET_GROUPS>
      <ASSET_GROUP_TITLE><![CDATA[All]]></ASSET_GROUP_TITLE>
    </ASSET_GROUPS>
    <FILTER_AZURE_VM_ID><![CDATA[Beginning With 399af5dc-c32a-4c40-95a5-
```

```
c6ed0e786430]]></FILTER_AZURE_VM_ID>
    <TRACKING_METHOD><![CDATA[Azure VM]]></TRACKING_METHOD>
    <FILTER_AZURE_VM_STATE><![CDATA[RUNNING]]></FILTER_AZURE_VM_STATE>
  </FILTERS>
</HEADER>
<HOST_LIST>
  <HOST>
    <IP><![CDATA[10.4.8.4]]></IP>
    <TRACKING_METHOD>Azure VM</TRACKING_METHOD>
    <CLOUD_PROVIDER>Azure</CLOUD_PROVIDER>
    <CLOUD_SERVICE>VM</CLOUD_SERVICE>
    <CLOUD_RESOURCE_ID><![CDATA[399af5dc-c32a-4c40-95a5-
c6ed0e786430]]></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[399af5dc-c32a-4c40-95a5-
c6ed0e786430]]></EC2_INSTANCE_ID>
...
```

DTD update:

DTD: /asset_search_report_v2.dtd

These elements were added to the DTD: FILTER_AZURE_VM_ID, FILTER_AZURE_VM_STATE, CLOUD_PROVIDER, CLOUD_SERVICE, CLOUD_RESOURCE_ID.

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

<!ELEMENT ASSET_SEARCH_REPORT (ERROR | (HEADER, HOST_LIST?))>

<!ELEMENT ERROR (#PCDATA)*>
<!ATTLIST ERROR number CDATA #IMPLIED>


<!-- HEADER -->

<!ELEMENT HEADER (REQUEST?, COMPANY, USERNAME, GENERATION_DATETIME,
TOTAL?, FILTERS)>

<!-- REQUEST Header -->
<!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 COMPANY (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT GENERATION_DATETIME (#PCDATA)>
<!ELEMENT FILTERS
((IP_LIST|ASSET_GROUPS|ASSET_TAGS|FILTER_DNS|FILTER_NETBIOS|FILTER_AZURE_
VM_ID|TRACKING_METHOD|

FILTER_OPERATING_SYSTEM|FILTER_OS_CPE|FILTER_PORT|FILTER_SERVICE|

FILTER_QID|FILTER_RESULT|FILTER_LAST_SCAN_DATE|FILTER_FIRST_FOUND_DATE|NE
TWORK|FILTER_DISPLAY_AG_TITLES|FILTER_QID_WITH_TEXT|FILTER_LAST_COMPLIANC
E_SCAN_DATE|FILTER_LAST_SCAP_SCAN_DATE|FILTER_AZURE_VM_STATE)+)>

<!ELEMENT IP_LIST (RANGE*)>
<!ELEMENT RANGE (START, END)>
...

<!ELEMENT FILTER_NETBIOS (#PCDATA)>
<!ATTLIST FILTER_NETBIOS criterion CDATA #IMPLIED>
<!ELEMENT FILTER_AZURE_VM_ID (#PCDATA)>
<!ELEMENT TRACKING_METHOD (#PCDATA)>

...

<!ELEMENT FILTER_QID_WITH_TEXT (#PCDATA)>
<!ELEMENT FILTER_AZURE_VM_STATE (#PCDATA)>
<!ELEMENT TOTAL (#PCDATA)>
<!-- HOST_LIST -->

<!ELEMENT HOST_LIST ((HOST|WARNING)*)>

<!ELEMENT HOST (ERROR | (IP, HOST_TAGS?,TRACKING_METHOD,
                         DNS?, CLOUD_PROVIDER?, CLOUD_SERVICE?,
CLOUD_RESOURCE_ID?, EC2_INSTANCE_ID?, NETBIOS?, OPERATING_SYSTEM?,
OS_CPE?, QID_LIST?, PORT_SERVICE_LIST?,
                         ASSET_GROUPS?, NETWORK?, LAST_SCAN_DATE?,
LAST_COMPLIANCE_SCAN_DATE?, LAST_SCAP_SCAN_DATE?, FIRST_FOUND_DATE?))>

<!ELEMENT IP (#PCDATA)>
<!ATTLIST IP network_id CDATA #IMPLIED>
<!ELEMENT HOST_TAGS (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT CLOUD_PROVIDER (#PCDATA)>
<!ELEMENT CLOUD_SERVICE (#PCDATA)>
<!ELEMENT CLOUD_RESOURCE_ID (#PCDATA)>
...
```

Sample Asset Search Report in CSV output

This sample will return the asset search report in CSV format. New columns will only appear in the CSV output for subscriptions with the "Cloud Perimeter Azure VM Scan" feature enabled.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/report/asset/?action=search&outp
ut_format=csv&asset_groups=All&tracking_method=AZURE%20VM&azure_vm_state=
RUNNING&azure_vm_id=399af5dc-c32a-4c40-95a5-
c6ed0e786430&azure_vm_id_modifier=beginning%20with"
```

CSV output:

```
"Company","UserName","ReportDate","AssetGroups","IPAddresses","DNSHostnam
e","EC2InstanceID","AzureVMID","NetBIOSHostname","TargetTrackingMethod","
EC2InstanceStatus","AzureVMState","TargetOperatingSystem","TargetService"
,"TargetPort","TargetQID","QIDTitle","TargetLastScanDate","TargetFirstFou
ndDate","Tags","Network","TargetComplianceLastScanDate","Total"
"Qualys","Patrick Slimmer","2020-06-22T23:28:20Z","All",,,,"Beginning
With 399af5dc-c32a-4c40-95a5-c6ed0e786430",,"Azure
VM",,"RUNNING",,,,,,,,,,"1"
"IP","DNSHostname","NetBIOSHostname","OperatingSystem","OSCPE","Port/Serv
ice/Default
Service","TrackingMethod","Network","LastScanDate","LastComplianceScanDat
e","First
Found","Tags","CloudProvider","CloudService","CloudResourceID","EC2Instan
ceID"
"10.4.8.4",,,"EulerOS / Ubuntu / Fedora / Tiny Core Linux / Linux
3.x",,,"Azure VM","test network","2020-06-15T23:02:28Z",,"2020-05-
17T22:47:03Z",,"Azure","VM","399af5dc-c32a-4c40-95a5-
c6ed0e786430","399af5dc-c32a-4c40-95a5-c6ed0e786430"
```

Host Based Scan Reports

When you run host based scan reports you have the option (in the report template) to include cloud details. When selected, you'll see Azure VM information for your Azure assets. You can launch host based scan reports from the API and download from the UI.

- In XML output, we added these tags: CLOUD_PROVIDER, CLOUD_SERVICE, CLOUD_RESOURCE_ID, CLOUD_ACCOUNT, AZURE_VM_INFO. AZURE_VM_INFO includes the following: PUBLIC_IP_ADDRESS, IMAGE_OFFER, IMAGE_VERSION, SUBNET, VM_STATE, PRIVATE_IP_ADDRESS, SIZE, SUBSCRIPTION_ID, LOCATION, RESOURCE_GROUP_NAME

- In CSV output, we added the following new columns: Cloud Provider, Cloud Service, Cloud Resource ID, Cloud Account, Cloud Resource Metadata (JSON string that will hold the key-value pairs of metadata). Cloud resource metadata for Azure VM includes: Public

IP address, Image Offer, Image Version, Subnet, VM State, Private IP Address, Size, Subscription Id, Location, Resource Group Name. New columns will only appear in CSV output in subscriptions with the "Cloud Perimeter Azure VM Scan" feature enabled.

- In CSV output, we will continue to populate the EC2 Instance ID column for all cloud assets (Azure, EC2, Google). The EC2 Instance ID column is replaced by Cloud Resource ID. EC2 Instance ID will be deprecated in a future release.

Sample Host Based Scan Report in XML output

This sample will return a scan report in XML format.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=launch&output_format=xml&report_type=Scan&template_id=123121&repo
rt_title=scan report host based - xml"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

XML output:

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

<!DOCTYPE ASSET_DATA_REPORT SYSTEM
"https://qualysapi.qualys.com/asset_data_report.dtd">
<ASSET_DATA_REPORT>

...

  <HOST_LIST>
    <HOST>
      <IP network_id="6000">10.4.8.4</IP>
      <TRACKING_METHOD></TRACKING_METHOD>
      <CLOUD_PROVIDER><![CDATA[Azure]]></CLOUD_PROVIDER>
      <CLOUD_SERVICE><![CDATA[VM]]></CLOUD_SERVICE>
      <CLOUD_RESOURCE_ID><![CDATA[399af5dc-c32a-4c40-95a5-
c6ed0e786430]]></CLOUD_RESOURCE_ID>
      <CLOUD_ACCOUNT><![CDATA[9de9e0a7-4f67-4812-917d-
2246853844e1]]></CLOUD_ACCOUNT>
      <!-- <EC2_INSTANCE_ID> tag has been deprecated. Please refer to
<CLOUD_RESOURCE_ID> tag for the same information //-->
      <EC2_INSTANCE_ID><![CDATA[399af5dc-c32a-4c40-95a5-
c6ed0e786430]]></EC2_INSTANCE_ID>
      <AZURE_VM_INFO>
        <PUBLIC_IP_ADDRESS><![CDATA[10.20.32.237]]></PUBLIC_IP_ADDRESS>
        <IMAGE_OFFER><![CDATA[Windows-10]]></IMAGE_OFFER>
        <IMAGE_VERSION><![CDATA[latest]]></IMAGE_VERSION>
        <SUBNET><![CDATA[default]]></SUBNET>
        <VM_STATE><![CDATA[RUNNING]]></VM_STATE>
        <PRIVATE_IP_ADDRESS><![CDATA[10.4.8.4]]></PRIVATE_IP_ADDRESS>
```

```
        <SIZE><![CDATA[Standard_D2]]></SIZE>
        <SUBSCRIPTION_ID><![CDATA[9de9e0a7-4f67-4812-917d-
2246853844e1]]></SUBSCRIPTION_ID>
        <LOCATION><![CDATA[centralus]]></LOCATION>

<RESOURCE_GROUP_NAME><![CDATA[assertion_USPOD02]]></RESOURCE_GROUP_NAME>
      </AZURE_VM_INFO>
...
```

DTD update:

DTD: /asset_data_report.dtd

New elements are shown in bold.

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

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

...

<!-- HOST_LIST -->

<!ELEMENT HOST_LIST (HOST+)>

<!ELEMENT HOST (ERROR | (IP, TRACKING_METHOD, ASSET_TAGS?,
                         DNS?, NETBIOS?, QG_HOSTID?, CLOUD_PROVIDER?,
CLOUD_SERVICE?, CLOUD_RESOURCE_ID?, CLOUD_ACCOUNT?,
EC2_INSTANCE_ID?,IP_INTERFACES?,EC2_INFO?, AZURE_VM_INFO?
OPERATING_SYSTEM?, OS_CPE?, ASSET_GROUPS?, VULN_INFO_LIST?))>

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

<!ELEMENT DNS (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT QG_HOSTID (#PCDATA)>
<!ELEMENT CLOUD_PROVIDER (#PCDATA)>
<!ELEMENT CLOUD_SERVICE (#PCDATA)>
<!ELEMENT CLOUD_RESOURCE_ID (#PCDATA)>
<!ELEMENT CLOUD_ACCOUNT (#PCDATA)>
<!ELEMENT EC2_INSTANCE_ID (#PCDATA)>
```

```
<!ELEMENT IP_INTERFACES (IP*)>
<!ELEMENT EC2_INFO
(PUBLIC_DNS_NAME?,IMAGE_ID?,VPC_ID?,INSTANCE_STATE?,PRIVATE_DNS_NAME?,INS
TANCE_TYPE?, ACCOUNT_ID?, REGION_CODE?, SUBNET_ID?)>
<!ELEMENT AZURE_VM_INFO
(PUBLIC_IP_ADDRESS?,IMAGE_OFFER?,IMAGE_VERSION?,SUBNET?,VM_STATE?,PRIVAT
E_IP_ADDRESS?,SIZE?, SUBSCRIPTION_ID?, LOCATION?, RESOURCE_GROUP_NAME?)>
<!ELEMENT PUBLIC_DNS_NAME (#PCDATA)>
<!ELEMENT IMAGE_ID (#PCDATA)>
<!ELEMENT VPC_ID (#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 OPERATING_SYSTEM (#PCDATA)>
<!ELEMENT PUBLIC_IP_ADDRESS (#PCDATA)>
<!ELEMENT IMAGE_OFFER (#PCDATA)>
<!ELEMENT IMAGE_VERSION (#PCDATA)>
<!ELEMENT SUBNET (#PCDATA)>
<!ELEMENT VM_STATE (#PCDATA)>
<!ELEMENT PRIVATE_IP_ADDRESS (#PCDATA)>
<!ELEMENT SIZE (#PCDATA)>
<!ELEMENT SUBSCRIPTION_ID (#PCDATA)>
<!ELEMENT LOCATION (#PCDATA)>
<!ELEMENT RESOURCE_GROUP_NAME (#PCDATA)>
<!ELEMENT OS_CPE (#PCDATA)>
<!ELEMENT ASSET_GROUPS (ASSET_GROUP_TITLE+)>
<!ELEMENT VULN_INFO_LIST (VULN_INFO+)>
...
```

Sample Host Based Scan Report in CSV output

This sample will return the scan report in CSV format. New columns only appear in the CSV output for subscriptions with the "Cloud Perimeter Azure VM Scan" feature enabled.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=launch&output_format=csv&report_type=Scan&template_id=123121&repo
rt_title=scan report host based - csv"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

CSV output:

```
...
"IP","Network","DNS","NetBIOS","Tracking Method","OS","IP
Status","QID","Title","Vuln
```

```
Status","Type","Severity","Port","Protocol","FQDN","SSL","First
Detected","Last Detected","Times Detected","Date Last Fixed","First
Reopened","Last Reopened","Times Reopened","CVE ID","Vendor
Reference","Bugtraq
ID","Threat","Impact","Solution","Exploitability","Associated
Malware","Results","PCI Vuln","Ticket State","Instance","Category","Cloud
Provider","Cloud Service","Cloud Resource ID","Cloud Account","EC2
Instance ID","Public Hostname","Image ID","VPC ID","Instance
State","Private Hostname","Instance Type","Account ID","Region
Code","Subnet ID","Cloud Resource Metadata"
"172.16.3.4","test network",,,"AZURE VM",
...
"Azure","VM","ea4d205f-5f2f-4579-9db1-bbd3381aef35","9de9e0a7-4f67-4812-
917d-2246853844e1","ea4d205f-5f2f-4579-9db1-
bbd3381aef35",,,,,,,,,,"""{""""Public IP
Address""""":""""10.20.32.216""""",""""Image
Offer""""":""""RHEL""""",""""Subnet""""":""""default""""",""""VM
State""""":""""RUNNING""""",""""Private IP
Address""""":""""172.16.3.4""""",""""Size""""":""""Standard_D2s_v3""""",""""
Subscription Id""""":""""9de9e0a7-4f67-4812-917d-
2246853844e1""""",""""Location""""":""""centralus""""",""""Resource Group
Name""""":""""mtestrg01""""}"""
...
```

Added Windows Support for the Apache HTTP and IBM HTTP servers

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

You can now create and update Apache Web Server record for Apache HTTP and IBM HTTP servers in order to authenticate to Apache HTTP and IBM HTTP servers running on a Windows host, and scan it for compliance. Windows authentication is required so you'll also need a Windows record for the host running the web server.

We added two new input parameters to support authenticated scans for these servers running on Windows host. These parameters are: 1) windows_apache_config_file and 2) windows_apache_control_command.

Create/Update Apache Server Records

The following table shows new input parameters for creating/updating Apache Web Server record for Apache HTTP and IBM HTTP servers running on Windows host.

Parameter	Description
windows_apache_config_file= {value}	(Required to create Apache HTTP and IBM HTTP server records; valid only for this record). The Windows path to the Apache HTTP and IBM HTTP server configuration file.
windows_apache_control_command= {value}	(Required to create Apache HTTP and IBM HTTP server records; valid only for this record) The Windows path to the Apache HTTP and IBM HTTP server control command. For IBM HTTP Server, enter the path to the IBM HTTP Server “bin” directory or the specific location of “apachectl”.

Sample create Apache Server record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=create&title=Apache+Record&windows_apache_config_file=C:\apache24
\conf\httpd.conf&windows_apache_control_command=C:\apache24\bin&ips=10.10
.25.25"
"https://qualysapi.qualys.com/api/2.0/fo/auth/apache/"
```

XML output:

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

```
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-07-15T05:22:25Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>88174</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample update Apache Server record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=update&ids=88174&windows_apache_config_file=C:\apache24_2\conf\ht
tpd.conf&windows_apache_control_command=C:\apache24_2\bin&ips=10.10.25.25
"
"https://qualysapi.qualys.com/api/2.0/fo/auth/apache/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"http://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-07-15T05:22:25Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>88174</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample list Apache Server record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=list&ids=88174"
"https://qualysapi.qualys.com/api/2.0/fo/auth/apache/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_APACHE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/apache/auth_apache_list_out
put.dtd">
<AUTH_APACHE_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-07-15T04:58:31Z</DATETIME>
    <AUTH_APACHE_LIST>
      <AUTH_APACHE>
        <ID>88174</ID>
        <TITLE><![CDATA[ApacheRD]]></TITLE>
        <IP_SET>
          <IP>10.10.10.55</IP>
        </IP_SET>

<WINDOWS_CONFIGURATION_FILE><![CDATA[C:\Apache24\conf\httpd.conf]]></WIN
DOWS_CONFIGURATION_FILE>

<WINDOWS_CONTROL_COMMAND><![CDATA[C:\Apache24\bin\httpd.exe]]></WINDOWS_
CONTROL_COMMAND>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2020-07-12T05:22:25Z</DATETIME>
          <BY>quays_rd4</BY>
        </CREATED>
        <OWNER>
          <USER_NAME>quays_rd4</USER_NAME>
          <USER_ROLE>Manager</USER_ROLE>
        </OWNER>
        <LAST_MODIFIED>
          <DATETIME>2020-07-14T12:09:01Z</DATETIME>
        </LAST_MODIFIED>
        <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
        <IS_ACTIVE>1</IS_ACTIVE>
      </AUTH_APACHE>
    </AUTH_APACHE_LIST>
  </RESPONSE>
</AUTH_APACHE_LIST_OUTPUT>
```

DTD update:

The following elements were added in the Apache Authentication Record List Output DTD: WINDOWS_CONFIGURATION_FILE and WINDOWS_CONTROL_COMMAND.

DTD: <platform API server>/api/2.0/fo/auth/apache/auth_apache_list_output.dtd

```
....
<!ELEMENT AUTH_APACHE (ID, TITLE, IP_SET, UNIX_CONFIGURATION_FILE?,
UNIX_CONTROL_COMMAND?, WINDOWS_CONFIGURATION_FILE?,
WINDOWS_CONTROL_COMMAND?, NETWORK_ID?, CREATED, OWNER?, LAST_MODIFIED,
IS_SYSTEM_CREATED?, IS_ACTIVE?, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT UNIX_CONFIGURATION_FILE (#PCDATA)>
<!ELEMENT UNIX_CONTROL_COMMAND (#PCDATA)>
<!ELEMENT WINDOWS_CONFIGURATION_FILE (#PCDATA)>
<!ELEMENT WINDOWS_CONTROL_COMMAND (#PCDATA)>
...
```

Added Windows Support for the IBM WebSphere Application Server

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

You can now create and update IBM WebSphere Application Server record to authenticate to a WebSphere Application Server running on a Windows host, and scan it for compliance. Windows authentication is required so you'll also need a Windows record for the host running the web server.

We added a new input parameter windows_installation_dir to support authenticated scans for these servers running on Windows servers.

Create/Update IBM WebSphere Application server record

The following table shows new input parameter for creating/updating IBM WebSphere Application server running on Windows host.

Parameter	Description
windows_installation_dir={value}	(Required to create an IBM WebSphere App Server record; valid only for this record) The Windows directory where the WebSphere application is installed.

Sample create IBM WebSphere Application server record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d
"action=create&title=IBM+Record&windows_installation_dir=
C:\IBM\WebSphere\AppServer&ips=10.10.25.25"
"https://qualysapi.qualys.com/api/2.0/fo/auth/ibm_websphere/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"http://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-07-15T05:35:54Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
```

```
        <ID_SET>
          <ID>88175</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample update IBM WebSphere Application server record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d
"action=update&ids=88175&windows_installation_dir=
C:\IBM\WebSphere_upadte\AppServer&ips=10.10.25.25"
"https://qualysapi.qualys.com/api/2.0/fo/auth/ibm_websphere/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"http://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-07-15T05:38:50Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>88175</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample list IBM WebSphere Application server record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST"
-d
"action=list&ids=88175"
"https://qualysapi.qualys.com/api/2.0/fo/auth/ibm_websphere/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_IBM_WEBSPHERE_LIST_OUTPUT SYSTEM
```

```
"https://qualysapi.qualys.com/api/2.0/fo/auth/ibm_websphere/auth_ibm_webs
phere_list_output.dtd">
<AUTH_IBM_WEBSPHERE_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-07-15T05:11:45Z</DATETIME>
    <AUTH_IBM_WEBSPHERE_LIST>
      <AUTH_IBM_WEBSPHERE>
        <ID>88175</ID>
        <TITLE><![CDATA[IBMRD]]></TITLE>
        <IP_SET>
          <IP>10.10.10.55</IP>
        </IP_SET>
        <WINDOWS_INSTLLATION_DIRECTORY><![CDATA[C:\Program Files
(x86)\IBM\WebSphere\AppServer]]></WINDOWS_INSTLLATION_DIRECTORY>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2020-07-12T05:35:53Z</DATETIME>
          <BY>quays_rd4</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2020-07-15T05:11:33Z</DATETIME>
        </LAST_MODIFIED>
        <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
        <IS_ACTIVE>1</IS_ACTIVE>
      </AUTH_IBM_WEBSPHERE>
    </AUTH_IBM_WEBSPHERE_LIST>
  </RESPONSE>
</AUTH_IBM_WEBSPHERE_LIST_OUTPUT>
```

DTD update:

The following element was added in the IBM WebSphere Authentication Record List Output DTD: WINDOWS_INSTLLATION_DIRECTORY.

DTD:

<platform API server>/api/2.0/fo/auth/ibm_websphere/auth_ibm_websphere_list_output.dtd

```
....
<!ELEMENT AUTH_IBM_WEBSPHERE (ID, TITLE, IP_SET,
UNIX_INSTLLATION_DIRECTORY?, WINDOWS_INSTLLATION_DIRECTORY?, NETWORK_ID?,
CREATED, LAST_MODIFIED, IS_SYSTEM_CREATED?, IS_ACTIVE?, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT UNIX_INSTLLATION_DIRECTORY (#PCDATA)>
<!ELEMENT WINDOWS_INSTLLATION_DIRECTORY (#PCDATA)>
...
```

Separate Options for Use IP Network Range Tags for Include and Exclude

APIs affected	/api/2.0/fo/scan/compliance/?action=launch /api/2.0/fo/schedule/scan/compliance/?action=create /api/2.0/fo/schedule/scan/compliance/?action=list /api/2.0/fo/scan/?action=launch /api/2.0/fo/schedule/scan/?action=create /api/2.0/fo/schedule/scan/?action=list
New or Updated API	No
DTD or XSD changes	Yes

With this release we are providing separate options for the Use IP Network Range Tags option for include and exclude tags. These new options are available when specifying the scan target using tags when you launch and schedule scans. We also updated the schedule scan list output and DTD to include the new options.

The two new input parameters - use_ip_nt_range_tags_include and use_ip_nt_range_tags_exclude - provide separate options for tag selection when using IP network range tags. The new parameters can be used in place of the old input parameter use_ip_nt_range_tags, which is also still supported.

New Parameters

The following table shows new parameters used for launch and schedule new Vulnerability and Compliance scans.

Parameter	Description
use_ip_nt_range_tags_include={**0**|1}	(Optional) Specify "0" (the default) to select from include tags. 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. use_ip_nt_range_tags_include is valid only when target_from=tags is specified.
use_ip_nt_range_tags_exclude ={**0**|1}	(Optional) Specify "0" (the default) to select from exclude tags. 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. use_ip_nt_range_tags_exclude is valid only when target_from=tags is specified.

Sample - Launch a Compliance Scan

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With:curl demo2' -d
"action=launch&scan_title=API_V2_AG_Scan_1596018365&target_from=tags&tag_
set_by=name&tag_include_selector=all&tag_exclude_selector=any&tag_set_inc
lude=Inc_1&tag_set_exclude=Exc_1&option_title=Initial+PC+Options&runtime_
http_header=HTTP_123_aABbCc&scanners_in_network=1&use_ip_nt_range_tags_in
clude=1&use_ip_nt_range_tags_exclude=1"
"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>2020-07-30T06:55:26Z</DATETIME>
    <TEXT>New compliance scan launched</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>10999557</VALUE>
      </ITEM>
      <ITEM>
        <KEY>REFERENCE</KEY>
        <VALUE>compliance/1596092124.99557</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Create a Compliance Scan Schedule

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With:curl demo2' -d
"action=create&scan_title=sch scan
pc&target_from=tags&tag_set_by=name&tag_include_selector=any&tag_set_incl
ude=SA_IN_TAG_INC_GN_1&tag_exclude_selector=any&tag_set_exclude=SA_IN_TAG
_EXC_GN_1&active=0&occurrence=daily&start_date=07/29/2020&start_hour=11&s
tart_minute=30&time_zone_code=IN&option_title=Initial+PC+Options&frequenc
y_days=364&end_after=1&observe_dst=no&scanners_in_tagset=1&use_ip_nt_rang
e_tags_include=1&use_ip_nt_range_tags_exclude=1"
"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>2020-07-30T07:05:10Z</DATETIME>
    <TEXT>New compliance scan scheduled successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>2326987</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - List a Compliance Scan Schedule

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With:curl demo2'
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/compliance/?action
=list&id=2326987"
```

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>2020-07-30T07:05:42Z</DATETIME>
    <COMPLIANCE_SCHEDULE_SCAN_LIST>
      <SCAN>
        <ID>2326987</ID>
        <ACTIVE>0</ACTIVE>
        <TITLE><![CDATA[sch scan pc]]></TITLE>
        <USER_LOGIN>ap_mm</USER_LOGIN>
        <TARGET><![CDATA[Asset Tags Included]]></TARGET>
        <NETWORK_ID><![CDATA[0]]></NETWORK_ID>
        <ISCANNER_NAME><![CDATA[All Scanners in TagSet]]></ISCANNER_NAME>
        <ASSET_TAGS>
          <TAG_INCLUDE_SELECTOR>any</TAG_INCLUDE_SELECTOR>
 <TAG_SET_INCLUDE><![CDATA[SA_IN_TAG_INC_GN_1]]></TAG_SET_INCLUDE>
          <TAG_EXCLUDE_SELECTOR>any</TAG_EXCLUDE_SELECTOR>
```

```
<TAG_SET_EXCLUDE><![CDATA[SA_IN_TAG_EXC_GN_1]]></TAG_SET_EXCLUDE>
          <USE_IP_NT_RANGE_TAGS></USE_IP_NT_RANGE_TAGS>
          <USE_IP_NT_RANGE_TAGS_INCLUDE>1</USE_IP_NT_RANGE_TAGS_INCLUDE>
          <USE_IP_NT_RANGE_TAGS_EXCLUDE>0</USE_IP_NT_RANGE_TAGS_EXCLUDE>
        </ASSET_TAGS>
        <OPTION_PROFILE>
          <TITLE><![CDATA[Initial PC Options]]></TITLE>
          <DEFAULT_FLAG>0</DEFAULT_FLAG>
        </OPTION_PROFILE>
        <SCHEDULE>
          <DAILY frequency_days="364" />
          <START_DATE_UTC>2020-07-29T06:00:00Z</START_DATE_UTC>
          <START_HOUR>11</START_HOUR>
          <START_MINUTE>30</START_MINUTE>
          <END_AFTER_HOURS>1</END_AFTER_HOURS>
          <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>
      </SCAN>
    </COMPLIANCE_SCHEDULE_SCAN_LIST>
  </RESPONSE>
</COMPLIANCE_SCHEDULE_SCAN_LIST_OUTPUT>
```

Updated DTD:

New tags appear in bold.

<platform API server>/api/2.0/fo/schedule/scan/compliance/compliance_schedule_scan_list_output.dtd

```
<!-- QUALYS COMPLIANCE_SCHEDULE_SCAN_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT COMPLIANCE_SCHEDULE_SCAN_LIST_OUTPUT (REQUEST?,RESPONSE)>
...
<!ELEMENT RESPONSE (DATETIME, COMPLIANCE_SCHEDULE_SCAN_LIST?)>
<!ELEMENT COMPLIANCE_SCHEDULE_SCAN_LIST (SCAN+)>
<!ELEMENT SCAN (ID, SCAN_TYPE?, ACTIVE, TITLE?, CLIENT?, USER_LOGIN,
TARGET, NETWORK_ID?, ISCANNER_NAME?, EC2_INSTANCE?, CLOUD_DETAILS?,
ASSET_GROUP_TITLE_LIST?, ASSET_TAGS?, EXCLUDE_IP_PER_SCAN?,
USER_ENTERED_IPS?, ELB_DNS?, OPTION_PROFILE?, SCHEDULE, NOTIFICATIONS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT ACTIVE (#PCDATA)>
...
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>
<!ELEMENT ASSET_TAGS (TAG_INCLUDE_SELECTOR, TAG_SET_INCLUDE,
TAG_EXCLUDE_SELECTOR?, TAG_SET_EXCLUDE?, USE_IP_NT_RANGE_TAGS?,
```

```
USE_IP_NT_RANGE_TAGS_INCLUDE, USE_IP_NT_RANGE_TAGS_EXCLUDE?)>
<!ELEMENT TAG_INCLUDE_SELECTOR (#PCDATA)>
<!ELEMENT TAG_SET_INCLUDE (#PCDATA)>
<!ELEMENT TAG_EXCLUDE_SELECTOR (#PCDATA)>
<!ELEMENT TAG_SET_EXCLUDE (#PCDATA)>
<!ELEMENT USE_IP_NT_RANGE_TAGS (#PCDATA)>
<!ELEMENT USE_IP_NT_RANGE_TAGS_INCLUDE (#PCDATA)>
<!ELEMENT USE_IP_NT_RANGE_TAGS_EXCLUDE (#PCDATA)>
<!ELEMENT EXCLUDE_IP_PER_SCAN (#PCDATA)>
<!ELEMENT USER_ENTERED_IPS (RANGE+)>
<!ELEMENT ELB_DNS (DNS+)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT RANGE (START, END)>
<!ELEMENT START (#PCDATA)>
<!ELEMENT END (#PCDATA)>
<!ELEMENT OPTION_PROFILE (TITLE, DEFAULT_FLAG?)>
<!ELEMENT DEFAULT_FLAG (#PCDATA)>
...
<!-- notifications -->
<!ELEMENT NOTIFICATIONS (BEFORE_LAUNCH?, AFTER_COMPLETE?,
DISTRIBUTION_GROUPS?)>
<!ELEMENT BEFORE_LAUNCH (TIME, UNIT, MESSAGE)>
<!ELEMENT TIME (#PCDATA)>
<!ELEMENT UNIT (#PCDATA)>
<!ELEMENT MESSAGE (#PCDATA)>

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

<!-- EOF -->
```

Sample - Launch a VM Scan

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With:curl demo2' -d
"action=launch&scan_title=vm
scan&target_from=tags&tag_set_by=name&tag_include_selector=all&tag_exclud
e_selector=any&tag_set_include=Inc_1&tag_set_exclude=Exc_1&option_title=I
nitial+Options&runtime_http_header=HTTP_123_aABbCc&scanners_in_tagset=1&u
se_ip_nt_range_tags_include=1&use_ip_nt_range_tags_exclude=1"
"https://qualysapi.qualys.com/api/2.0/fo/scan/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
```

```
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2020-07-30T06:47:20Z</DATETIME>
    <TEXT>New vm scan launched</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>10999554</VALUE>
      </ITEM>
      <ITEM>
        <KEY>REFERENCE</KEY>
        <VALUE>scan/1596091637.99554</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Create a VM Scan Schedule

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With:curl demo2' -d
"action=create&scan_title=sch scan
1&target_from=tags&tag_set_by=name&tag_include_selector=any&tag_set_inclu
de=SA_IN_TAG_INC_GN_1&tag_exclude_selector=any&tag_set_exclude=SA_IN_TAG_
EXC_GN_1&active=0&occurrence=daily&start_date=07/29/2020&start_hour=11&st
art_minute=30&time_zone_code=IN&option_title=Initial
Options&frequency_days=364&end_after=1&observe_dst=no&scanners_in_tagset=
1&use_ip_nt_range_tags_include=1&use_ip_nt_range_tags_exclude=1"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2020-07-30T06:41:44Z</DATETIME>
    <TEXT>New scan scheduled successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>2326984</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - List Scan Schedule

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With:curl demo2'
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/?action=list&id=23
26984"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SCHEDULE_SCAN_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/schedule_scan_list
_output.dtd">
<SCHEDULE_SCAN_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-07-30T06:42:25Z</DATETIME>
    <SCHEDULE_SCAN_LIST>
      <SCAN>
        <ID>2326984</ID>
        <ACTIVE>0</ACTIVE>
        <TITLE><![CDATA[sch scan 1]]></TITLE>
        <USER_LOGIN>ap_mm</USER_LOGIN>
        <TARGET><![CDATA[Asset Tags Included]]></TARGET>
        <NETWORK_ID><![CDATA[0]]></NETWORK_ID>
        <ISCANNER_NAME><![CDATA[All Scanners in TagSet]]></ISCANNER_NAME>
        <ASSET_TAGS>
          <TAG_INCLUDE_SELECTOR>any</TAG_INCLUDE_SELECTOR>
 <TAG_SET_INCLUDE><![CDATA[SA_IN_TAG_INC_GN_1]]></TAG_SET_INCLUDE>
          <TAG_EXCLUDE_SELECTOR>any</TAG_EXCLUDE_SELECTOR>
 <TAG_SET_EXCLUDE><![CDATA[SA_IN_TAG_EXC_GN_1]]></TAG_SET_EXCLUDE>
          <USE_IP_NT_RANGE_TAGS></USE_IP_NT_RANGE_TAGS>
          <USE_IP_NT_RANGE_TAGS_INCLUDE>1</USE_IP_NT_RANGE_TAGS_INCLUDE>
          <USE_IP_NT_RANGE_TAGS_EXCLUDE>0</USE_IP_NT_RANGE_TAGS_EXCLUDE>
        </ASSET_TAGS>
        <OPTION_PROFILE>
          <TITLE><![CDATA[Initial Options]]></TITLE>
          <DEFAULT_FLAG>1</DEFAULT_FLAG>
        </OPTION_PROFILE>
        <PROCESSING_PRIORITY>0 - No Priority</PROCESSING_PRIORITY>
        <SCHEDULE>
          <DAILY frequency_days="364" />
          <START_DATE_UTC>2020-07-29T06:00:00Z</START_DATE_UTC>
          <START_HOUR>11</START_HOUR>
          <START_MINUTE>30</START_MINUTE>
          <END_AFTER_HOURS>1</END_AFTER_HOURS>
          <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>
        </SCAN>
      </SCHEDULE_SCAN_LIST>
    </RESPONSE>
</SCHEDULE_SCAN_LIST_OUTPUT>
```

Updated DTD:

New tags appear in bold.

<platform API server>/api/2.0/fo/schedule/scan/schedule_scan_list_output.dtd

```
<!-- QUALYS SCHEDULE_SCAN_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT SCHEDULE_SCAN_LIST_OUTPUT (REQUEST?,RESPONSE)>
...
<!ELEMENT SCAN (ID, SCAN_TYPE?, ACTIVE, TITLE?, CLIENT?, USER_LOGIN,
TARGET, NETWORK_ID?, ISCANNER_NAME?, EC2_INSTANCE?, CLOUD_DETAILS?,
ASSET_GROUP_TITLE_LIST?, ASSET_TAGS?, EXCLUDE_IP_PER_SCAN?,
USER_ENTERED_IPS?, ELB_DNS?, OPTION_PROFILE?, PROCESSING_PRIORITY?,
SCHEDULE, NOTIFICATIONS?)>
...
<!ELEMENT ASSET_GROUP_TITLE_LIST (ASSET_GROUP_TITLE+)>
<!ELEMENT ASSET_GROUP_TITLE (#PCDATA)>
<!ELEMENT ASSET_TAGS (TAG_INCLUDE_SELECTOR, TAG_SET_INCLUDE,
TAG_EXCLUDE_SELECTOR?, TAG_SET_EXCLUDE?, USE_IP_NT_RANGE_TAGS?,
USE_IP_NT_RANGE_TAGS_INCLUDE, USE_IP_NT_RANGE_TAGS_EXCLUDE?)>
<!ELEMENT TAG_INCLUDE_SELECTOR (#PCDATA)>
<!ELEMENT TAG_SET_INCLUDE (#PCDATA)>
<!ELEMENT TAG_EXCLUDE_SELECTOR (#PCDATA)>
<!ELEMENT TAG_SET_EXCLUDE (#PCDATA)>
<!ELEMENT USE_IP_NT_RANGE_TAGS (#PCDATA)>
<!ELEMENT USE_IP_NT_RANGE_TAGS_INCLUDE (#PCDATA)>
<!ELEMENT USE_IP_NT_RANGE_TAGS_EXCLUDE (#PCDATA)>
<!ELEMENT EXCLUDE_IP_PER_SCAN (#PCDATA)>
<!ELEMENT USER_ENTERED_IPS (RANGE+)>
<!ELEMENT ELB_DNS (DNS+)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT RANGE (START, END)>
...
<!ELEMENT AFTER_COMPLETE (MESSAGE)>
<!ELEMENT DISTRIBUTION_GROUPS (DISTRIBUTION_GROUP+)>
<!ELEMENT DISTRIBUTION_GROUP (ID, TITLE)>

<!-- EOF -->
```