Qualys Cloud Platform (VM, PC) v8.x

API Release Notes

Version 8.13.1

April 20, 2018

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

Support for Cloud Perimeter Scans (coming soon!)

URL to the Qualys API Server

Qualys maintains multiple Qualys platforms. The Qualys API server URL that you should use for API requests depends on the platform where your account is located.

Account Location	API Server URL
Qualys US Platform 1	https://qualysapi.qualys.com
Qualys US Platform 2	https://qualysapi.qg2.apps.qualys.com
Qualys US Platform 3	https://qualysapi.qg3.apps.qualys.com
Qualys EU Platform 1	https://qualysapi.qualys.eu
Qualys EU Platform 2	https://qualysapi.qg2.apps.qualys.eu
Qualys India Platform 1	https://qualysapi.qg1.apps.qualys.in
Qualys Private Cloud Platform	https://qualysapi.<customer_base_url>

The Qualys API documentation and sample code use the API server URL for the Qualys US Platform 1. If your account is located on another platform, please replace this URL with the appropriate server URL for your account.

Support for Cloud Perimeter Scans (coming soon!)

We've made updates to support Cloud Perimeter Scans in a future release (keep in mind Cloud Perimeter Scans are not supported at this time).

API updates: Schedule Scan List | Scan Results (fetch from API) | Scan Results (download from UI)

Schedule Scan List

API affected	/api/2.0/fo/schedule/scan/?action=list
New or Updated API	Updated
DTD or XSD changes	Yes

Users can now filter the schedule scan list to only show cloud perimeter scan jobs. Also, when you include cloud details in the output, we'll show scan type "Cloud Perimeter".

Input Parameters

Updated parameters are listed.

Parameter	Description
scan_type=perimeter	(Optional) List cloud perimeter scans only. **This option will be supported for Cloud Perimeter Scans in future release.**
show_cloud_details={**0**|1}	(Optional) Set to 1 to display cloud details in the XML output. The cloud details will show scan type "Cloud Perimeter" for cloud perimeter scans.

Example

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/?action=list&id=13
40788&scan_type=perimeter&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>2018-04-12T12:57:03Z</DATETIME>
   <SCHEDULE_SCAN_LIST>
```

```
    <SCAN>
      <ID>1340788</ID>
      <ACTIVE></ACTIVE>
      <TITLE><![CDATA[My_External_Scan]]></TITLE>
      <USER_LOGIN>utwrx_mp</USER_LOGIN>
      <TARGET><![CDATA[Asset Tags Included]]></TARGET>
      <ISCANNER_NAME><![CDATA[External Scanner]]></ISCANNER_NAME>
      <EC2_INSTANCE>
        <CONNECTOR_UUID><![CDATA[8047abce-c3ac-42e0-ad49-
be4181d22c84]]></CONNECTOR_UUID>
        <EC2_ENDPOINT><![CDATA[1507b6c1-07a7-4d88-acf2-
8c6b63e749c4]]></EC2_ENDPOINT>
        <EC2_ONLY_CLASSIC><![CDATA[1]]></EC2_ONLY_CLASSIC>
      </EC2_INSTANCE>
      <CLOUD_DETAILS>
        <PROVIDER>AWS</PROVIDER>
        <CONNECTOR>
          <ID>37361</ID>
          <UUID>8047abce-c3ac-42e0-ad49-be4181d22c84</UUID>
          <NAME><![CDATA[EC2 Connector]]></NAME>
        </CONNECTOR>
        <SCAN_TYPE>Cloud Perimeter</SCAN_TYPE>
        <CLOUD_TARGET>
          <PLATFORM>Classic</PLATFORM>
          <REGION>
            <UUID>1507b6c1-07a7-4d88-acf2-8c6b63e749c4</UUID>
            <CODE>us-east-1</CODE>
            <NAME><![CDATA[US East (N. Virginia)]]></NAME>
          </REGION>
          <VPC_SCOPE>None</VPC_SCOPE>
        </CLOUD_TARGET>
      </CLOUD_DETAILS>
      <ASSET_TAGS>
        <TAG_INCLUDE_SELECTOR>any</TAG_INCLUDE_SELECTOR>
        <TAG_SET_INCLUDE><![CDATA[EC2_Targets]]></TAG_SET_INCLUDE>
        <TAG_EXCLUDE_SELECTOR>any</TAG_EXCLUDE_SELECTOR>
        <TAG_SET_EXCLUDE><![CDATA[EC2_Test]]></TAG_SET_EXCLUDE>
        <USE_IP_NT_RANGE_TAGS>0</USE_IP_NT_RANGE_TAGS>
      </ASSET_TAGS>
      <ELB_DNS>
        <DNS><![CDATA[abc.com]]></DNS>
        <DNS><![CDATA[abc123.com]]></DNS>
      </ELB_DNS>
      <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>2018-04-02T05:00:00Z</START_DATE_UTC>
          <START_HOUR>10</START_HOUR>
          <START_MINUTE>30</START_MINUTE>
          <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>
```

DTD Update

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

We've added the new ELB_DNS tag that appears for Cloud Perimeter Scans only.

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

...

<!ELEMENT RESPONSE (DATETIME, SCHEDULE_SCAN_LIST?)>
<!ELEMENT SCHEDULE_SCAN_LIST (SCAN+)>
<!ELEMENT SCAN (ID, SCAN_TYPE?, ACTIVE, TITLE?, 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 ELB_DNS (DNS+)>
<!ELEMENT DNS (#PCDATA)>

...
```

Scan Results (fetch from API)

API affected	/api/2.0/fo/scan/?action=fetch
New or Updated API	Neither (output change only)
DTD or XSD changes	No

Example - CSV Extended Format

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=fetch&scan_ref=scan/1523603293.69652&mode=extended&output_format=
csv_extended" "https://qualysapi.qualys.com/api/2.0/fo/scan/"
```

Sample CSV output:

In the CSV Header we added "Scan Type" and we changed "IPs" to "DNS". These changes only apply to Cloud Perimeter Scans.

```
"Scan Results","04/12/2018 at 14:59:47 (GMT-0700)"
"Qualys, Inc.","919 E Hillsdale Blvd, Floor 4",,"Foster
City","California","United States of America","94404"
"Patrick Slimmer","Manager"

"Launch Date","Active Hosts","Total Hosts","Type","Scan
Type","Status","Reference","Scanner Appliance","Duration","Scan
Title","Asset Groups","DNS","Excluded IPs","Option Profile","Tags"
"04/17/2018 12:41:17","2","2","Scheduled","Cloud Perimeter - AWS
EC2","Finished","scan/1523968877.72179","10.1.0.23 (Scanner 10.0.14-1,
Vulnerability Signatures 2.4.290-2)","00:18:50","API-Launch-DNS-
May_work",,"ec2-184-73-79-113.compute-1.amazonaws.com,ec2-52-87-163-
204.compute-1.amazonaws.com",,"Initial Options","Included(any): tag-new;
Excluded(any);"

"IP","DNS","NetBIOS","OS","IP
Status","QID","Title","Type","Severity","Port","Protocol","FQDN","SSL","C
VE ID","Vendor Reference","Bugtraq
ID","Threat","Impact","Solution","Exploitability","Associated
Malware","Results","PCI Vuln","Instance","Category"
```

Example - JSON Extended Format

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=fetch&scan_ref=scan/1523968877.72179&mode=extended&output_format=
json_extended" "https://qualysapi.qualys.com/api/2.0/fo/scan/"
```

Sample JSON extended output:

We added "scan_type" and we changed "ips" to "dns". These changes only apply to Cloud Perimeter Scans.

```
[{"scan_report_template_title":"Scan Results","result_date":"04\/18\/2018
12:25:14","company":"Qualys","add1":"919 E Hillsdale Blvd, Floor
4","add2":null,"city":"Foster
City","state":"California","country":"United States of
America","zip":"94404","name":"Patrick
Slimmer","username":"quays_pslimmer","role":"Manager"},
{"launch_date":"04\/17\/2018
12:41:17","active_hosts":"2","total_hosts":"2","type":"Scheduled",
"scan_type":"Cloud Perimeter - AWS
EC2","status":"Finished","reference":"scan\/1523968877.72179","scanner_ap
pliance":"10.1.0.23 (Scanner 10.0.14-1, Vulnerability Signatures 2.4.290-
2)","duration":"00:18:50","scan_title":"My-
Scan","asset_groups":null,"dns":"ec2-184-73-79-113.compute-
1.amazonaws.com,ec2-52-87-163-204.compute-
1.amazonaws.com","excluded_ips":"","option_profile":"Initial
Options","tags":"Included(any): tag-new;\nExcluded(any);\n"}]
```

Scan Results (download from UI)

API affected	N/A (affects end report)
New or Updated API	Neither (output change only)
DTD or XSD changes	No

Scan Results in XML format

We added these new Key values to the Header section of the XML output for Cloud Perimeter Scans:

```
<KEY value="CLOUD_PROVIDER">AWS</KEY>
<KEY value="CLOUD_SERVICE">EC2</KEY>
<KEY value="SCAN_TYPE">Cloud Perimeter</KEY>
```

Scan Results in CSV format

In the CSV Header we added "Scan Type" and we changed "IPs" to "DNS". These changes only apply to Cloud Perimeter Scans.

Sample CSV output:

```
"Scan Results","04/12/2018 at 14:59:47 (GMT-0700)"
"Qualys, Inc.","919 E Hillsdale Blvd, Floor 4",,"Foster
City","California","United States of America","94404"
```

```
"Patrick Slimmer","Manager"

"Launch Date","Active Hosts","Total Hosts","Type",
"Scan Type","Status","Reference","Scanner Appliance","Duration",
"Scan Title","Asset Groups","DNS","Excluded IPs","Option Profile"
"04/12/2018 at 14:26:16 (GMT-0700)","1","1","Scheduled (default option
profile)","Cloud Perimeter - AWS EC2","Finished","scan/1523568376.69585",
"10.1.0.23 (Scanner 10.0.14-1, Vulnerability Signatures 2.4.290-
2)","00:18:33","AWS EC2 Perimeter Scan 20180412 - Now",,"ec2-184-73-79-
113.compute-1.amazonaws.com",,"Initial Options","Included(any): tag-new;
Excluded(any);"

...
```