Qualys API Release Notes

Version 8.10

Qualys 8.10 includes improvements to the Qualys API, giving you more ways to integrate your programs and API calls with Qualys Vulnerability Management (VM) and Qualys Policy Compliance (PC). Looking for our API user guides? Just log in to your Qualys account and go to Help > Resources.

What’s New

- Change API Rate Limit to 300 per hour
- New Support for BeyondTrust PBPS Vaults
- New API Support for Option Profiles
- Scanner Appliance List - added Cloud Information
- EC2 Assets - Improved Reporting of private DNS host name and Instance ID
- Manage assets using EC2 metadata
- IP Update - New DTD for Duplicate Hosts Error
- Export user activity log for a subscription
- Action Log API V1 - added User Details in Output
- Asset Search APIs - Search by EC2 Instance Status, ID
- VM - New API Support for Report Templates
- VM - Show Reopened Info in Scan Reports
- VM - Show Reopened Info in Vulnerability Detection API
- VM - Detection API - Identify vulnerabilities related to running and non-running kernels
- VM - Filter Detections Updated Before a Specific Date and Time
- VM - Editing vulnerabilities
- VM - EC2 asset information in scan report
- VM - Scan Report in XML Format - Ability to Exclude Glossary data
- VM - Hide target information from scan list
- VM - New tag added to KnowledgeBase API

Copyright 2017 by Qualys, Inc. All Rights Reserved.
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.

<table>
<thead>
<tr>
<th>Account Location</th>
<th>API Server URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualys US Platform 1</td>
<td><a href="https://qualysapi.qualys.com">https://qualysapi.qualys.com</a></td>
</tr>
<tr>
<td>Qualys US Platform 2</td>
<td><a href="https://qualysapi.qg2.apps.qualys.com">https://qualysapi.qg2.apps.qualys.com</a></td>
</tr>
<tr>
<td>Qualys US Platform 3</td>
<td><a href="https://qualysapi.qg3.apps.qualys.com">https://qualysapi.qg3.apps.qualys.com</a></td>
</tr>
<tr>
<td>Qualys EU Platform 1</td>
<td><a href="https://qualysapi.qualys.eu">https://qualysapi.qualys.eu</a></td>
</tr>
<tr>
<td>Qualys EU Platform 2</td>
<td><a href="https://qualysapi.qg2.apps.qualys.eu">https://qualysapi.qg2.apps.qualys.eu</a></td>
</tr>
<tr>
<td>Qualys India Platform 1</td>
<td><a href="https://qualysapi.qg1.apps.qualys.in">https://qualysapi.qg1.apps.qualys.in</a></td>
</tr>
<tr>
<td>Qualys Private Cloud Platform</td>
<td><a href="https://qualysapi">https://qualysapi</a>.&lt;customer_base_url&gt;</td>
</tr>
</tbody>
</table>

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.
Change API Rate Limit to 300 per hour

The Qualys API enforces limits on the API calls a customer can make based on their subscription settings. With this release we’ve updated the default API Rate Limit to 300 API calls per hour. The Rate Limit Period per Subscription control has been updated in all subscriptions that have the default set.

Tell me about API Rate Limits

Rate Limit per Subscription (per API): The maximum number of API calls allowed within the subscription per day (or a customized period, in seconds) for each API. The rate limit is calculated based on the settings for rate limit count and period.

- Rate Limit Count per Subscription (per API): The maximum number of API calls allowed within the subscription during the configured rate limit period. Default is 300.

- Rate Limit Period per Subscription (per API): The period of time, in seconds, that defines a window when API calls are counted within the subscription for each API. The window starts from the moment each API call is received by the service and extends backwards 24 hours (or some customized period, in seconds). New default is 3600 seconds, i.e. 1 hour (previously this default was 86400 seconds, i.e. 24 hours).

Concurrency Limit per Subscription (per API): The maximum number of concurrent API call instances allowed within the subscription for each API. Default is 2.
New Support for BeyondTrust PBPS Vaults

This new vault type can be used to retrieve authentication credentials from a BeyondTrust PowerBroker Password Safe (PBPS). We updated the authentication vault API (create, update, list, view) and the authentication record API (create, update, list) to support the new vault type. There are new input parameters for create/update vault, and a DTD change for view vault output. We also updated the DTDs for listing Windows and Unix authentication records.

Authentication Vault API

You can now create, update, list and view BeyondTrust PBPS authentication vaults.

Create BeyondTrust PBPS Authentication Vault

Use the parameter “action=create” to create a new vault in your account.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action=create</td>
<td>(Required)</td>
</tr>
<tr>
<td>title={value}</td>
<td>(Required) The vault title.</td>
</tr>
<tr>
<td>type={value}</td>
<td>(Required) Specify type=BeyondTrust PBPS.</td>
</tr>
<tr>
<td>comments={value}</td>
<td>(Optional) User defined comments.</td>
</tr>
<tr>
<td>appkey={value}</td>
<td>(Required) The application key (alpha-numeric string) for the BeyondTrust PBPS web services API. The maximum length is 128 bytes. A leading and/or trailing space or periods in the input value will be removed.</td>
</tr>
<tr>
<td>url={value}</td>
<td>(Required) The HTTP or HTTPS URL to access the BeyondTrust PBPS web services API.</td>
</tr>
<tr>
<td>ssl_verify={1</td>
<td>0}</td>
</tr>
<tr>
<td>username={value}</td>
<td>(Required) The user account that can call the BeyondTrust PBPS web services API. The maximum length is 64 characters. This special character cannot be included: @</td>
</tr>
<tr>
<td>password={value}</td>
<td>(Optional) Specify a user password when required by the Application API Key configuration in BeyondTrust.</td>
</tr>
</tbody>
</table>
New Support for BeyondTrust PBPS Vaults

**API request:**
```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d "action=create&type=BeyondTrust
PBPS&appkey=181979e5c72b7f5f91906cfe7c92745a3c9b865a9786bbaf4868a8dc01987
f69c3d13d66ab01381b175c3a724b3267ebbb81d64d9cd5b29d512ceefc6d5f01&usern
ame=joe_user&url=https://host.domain/eEye.RetinaCS.Server/api/public/v3&p
assword=bt12345&ssl_verify=0&title=My-BeyondTrust-Vault"
"https://qualysapi.qualys.com/api/2.0/fo/vault/index.php"
```

**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>2017-02-21T20:41:12Z</DATETIME>
    <TEXT>Success</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>105356922</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cert={value}</td>
<td>(Optional) Provide an X.509 client certificate with your private key when required by the Application API Key configuration in BeyondTrust. The certificate must be trusted by the PBPS web server. Enter the certificate block after the key block and be sure to include the first and last line (-----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----). For a create/update request, if the cert parameter is specified, then the private_key parameter must also be specified.</td>
</tr>
<tr>
<td>private_key={value}</td>
<td>(Optional) Specify the private key for authentication. Copy the contents of private key file (id_rsa) and be sure to include the first and last line (-----BEGIN PRIVATE KEY----- and -----END PRIVATE KEY-----). For a create/update request, if the private_key parameter is specified, then the cert parameter must also be specified.</td>
</tr>
<tr>
<td>private_key_pwd={value}</td>
<td>(Optional) Specify a password for your private key if it’s encrypted.</td>
</tr>
</tbody>
</table>

Qualys API Release Notes
Update BeyondTrust PBPS Authentication Vault

Use the parameter “action=update” to update a BeyondTrust PBPS authentication vault in your account. You’ll need to include the ID for the vault you’re updating.

API request:


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>2017-02-22T00:08:09Z</DATETIME>
    <TEXT>Success</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>105356922</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>

List Authentication Vaults

Use the parameter “action=list” to list the vault defined in your account. To view a specific BeyondTrust PBPS vault, specify the ID or title of the vault.

API request (Windows):


XML output (Windows):

<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_VAULT_LIST_OUTPUT SYSTEM "https://qualysapi.qualys.com/api/2.0/fo/vault/vault_output.dtd">
<AUTH_VAULT_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-02-22T00:52:00Z</DATETIME>
  </RESPONSE>
</AUTH_VAULT_LIST_OUTPUT>
New Support for BeyondTrust PBPS Vaults

<STATUS>Success</STATUS>
<COUNT>1</COUNT>
<AUTH_VAULTS>
  <AUTH_VAULT>
    <TITLE><![CDATA[My-BeyondTrust-Vault]]></TITLE>
    <VAULT_TYPE><![CDATA[BeyondTrust PBPS]]></VAULT_TYPE>
    <LAST_MODIFIED>
      <DATETIME>2017-02-22T00:08:09Z</DATETIME>
      <BY>joe_user</BY>
    </LAST_MODIFIED>
    <ID>105356922</ID>
  </AUTH_VAULT>
</AUTH_VAULTS>
</RESPONSE>
</AUTH_VAULT_LIST_OUTPUT>

View BeyondTrust PBPS Authentication Vault

Use the parameter “action=view” and specify the ID of the BeyondTrust authentication vault to view its details.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d "action=view&id=105356922"
"https://qualysapi.qualys.com/api/2.0/fo/vault/index.php"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE VAULT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/vault/vault_view.dtd">
<VAULT_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-02-22T01:24:40Z</DATETIME>
    <VAULT_QUEST>
      <TITLE><![CDATA[My-BeyondTrust-Vault]]></TITLE>
      <COMMENTS><![CDATA[ ]]>)
      <VAULT_TYPE><![CDATA[BeyondTrust PBPS]]></VAULT_TYPE>
      <CREATED_ON>2017-02-21T20:41:12Z</CREATED_ON>
      <OWNER>joe_user</OWNER>
      <LAST_MODIFIED>
        <DATETIME>2017-02-22T00:08:09Z</DATETIME>
        <BY>joe_user</BY>
      </LAST_MODIFIED>
      <APPKEY><![CDATA[181979e5c72b7f5f91906cfe7c92745a3c9b865a9786bbaf4868a8dc01987f69c3db13d66ab013811b175c3a724b3267ebbb81d64d9cd5b29d512ceefc6d5f01]]></APPKEY>
      <USERNAME><![CDATA[joe_user]]></USERNAME>
      <SSL_VERIFY><![CDATA[0]]></SSL_VERIFY>
  </VAULT_QUEST>
</RESPONSE>
</VAULT_OUTPUT>
```

Qualys API Release Notes
New Support for BeyondTrust PBPS Vaults

<URL><![CDATA[https://host.domain/eEye.RetinaCS.Server/api/public/v3]]></URL>
  <ID>105356922</ID>
</VAULT_QUEST>
</RESPONSE>
</VAULT_OUTPUT>

DTD update:
We added APPKEY to the Vault View DTD (vault_view.dtd).

<!-- QUALYS VAULT_VIEW DTD -->
...  
<!ELEMENT UUID (#PCDATA)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT COMMENTS (#PCDATA)>
<!ELEMENT VAULT_TYPE (#PCDATA)>
<!ELEMENT CREATED_ON (#PCDATA)>
<!ELEMENT OWNER (#PCDATA)>
<!ELEMENT APPID (#PCDATA)>
<!ELEMENT APPKEY (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!ELEMENT SSL_VERIFY (#PCDATA)>
<!ELEMENT DOMAIN (#PCDATA)>
<!ELEMENT API_USERNAME (#PCDATA)>
<!ELEMENT WEB_USERNAME (#PCDATA)>
<!ELEMENT SERVER_ADDRESS (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT SAFE (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME, BY?)>
<!ELEMENT BY (#PCDATA)>
<!-- EOF -->
New Support for BeyondTrust PBPS Vaults

Authentication Record API

You can now create, update, list authentication records with BeyondTrust PBPS vaults.

Create Authentication Record

Use these input parameters when creating/updating an authentication record and getting credentials from your BeyondTrust PBPS vault.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action=create/update</td>
<td>(Required)</td>
</tr>
<tr>
<td>login_type=[value]</td>
<td>(Required to create/update vault information) Specify login_type=vault to add vault information. By default, the parameter is set to basic.</td>
</tr>
<tr>
<td>vault_id=[value]</td>
<td>(Required when action=create and login_type=vault) A vault ID.</td>
</tr>
<tr>
<td>vault_type=[value]</td>
<td>(Required when action=create and login_type=vault) Specify vault_type=BeyondTrust PBPS.</td>
</tr>
<tr>
<td>system_name=[value]</td>
<td>(Optional) The managed system name (also known as asset name). When not specified, we'll attempt to auto-discover the system name for you at scan time.</td>
</tr>
<tr>
<td>account_name=[value]</td>
<td>(Optional) The account name. When not specified, we'll try the username specified in the authentication record.</td>
</tr>
</tbody>
</table>

**API request (Windows):**

curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d "action=create&title=WINDOWS_AUTH_BT_PBPS&username=joe_user&ips=10.10.25.2&login_type=vault&vault_id=105306922&vault_type=BeyondTrust PBPS&system_name=my_bt_system&account_name=bt_account" "https://qualysapi.qualys.com/api/2.0/fo/auth/windows/"

**XML output (Windows):**

```xml
<?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>2017-02-22T02:11:54Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>2696966922</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```
New Support for BeyondTrust PBPS Vaults

Update Authentication Record

API request (Windows):

curl -u "USERNAME:PASSWORD" -H "X-Requested-Within: curl" -d 
"action=update&ids=2727086922&login_type=vault&vault_id=125286922&vault_type=BeyondTrust 
PBPS&system_name=my_bt_system&account_name=bt_account&title=My-Windows- 
Record&username=admin&ips=10.10.10.28" 
"https://qualysapi.qualys.com/api/2.0/fo/auth/windows/"

XML output (Windows):

<?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>2017-03-09T23:56:12Z</DATETIME> 
<BATCH_LIST> 
<BATCH> 
<TEXT>Successfully Updated</TEXT> 
<ID_SET> 
<ID>2727086922</ID> 
</ID_SET> 
</BATCH> 
</BATCH_LIST> 
</RESPONSE> 
</BATCH_RETURN>

List Authentication Records

API request (Windows):

curl -u "USERNAME:PASSWORD" -H "X-Requested-Within: curl" -d 
"action=list&details=All&ids=2727086922" 
"https://qualysapi.qualys.com/api/2.0/fo/auth/windows/"

XML output (Windows):

<?xml version="1.0" encoding="UTF-8" ?>  
<!DOCTYPE AUTH_WINDOWS_LIST_OUTPUT SYSTEM 
"https://qualysapi.qualys.com/api/2.0/fo/auth/windows/auth_windows_list_output.dtd"> 
<AUTH_WINDOWS_LIST_OUTPUT> 
<RESPONSE> 
</RESPONSE> 
</AUTH_WINDOWS_LIST_OUTPUT>
New Support for BeyondTrust PBPS Vaults

<DATE>2017-03-10T00:04:12Z</DATE>
<AUTH_WINDOW_LIST>
<AUTH_WINDOW>
<ID>2727086922</ID>
<TITLE><![CDATA[My-Windows-Record]]></TITLE>
<USERNAME><![CDATA[joe_user]]></USERNAME>
<NTLM_V2>1</NTLM_V2>
<IP_SET>
<IP>10.10.10.28</IP>
</IP_SET>
<LOGIN_TYPE><![CDATA[vault]]></LOGIN_TYPE>
<DIGITAL_VAULT>
<DIGITAL_VAULT_ID><![CDATA[125286922]]></DIGITAL_VAULT_ID>
<DIGITAL_VAULT_TYPE><![CDATA[BeyondTrust PBPS]]></DIGITAL_VAULT_TYPE>
<DIGITAL_VAULT_TITLE><![CDATA[My-BeyondTrust-Vault]]></DIGITAL_VAULT_TITLE>
<VAULT_SYSTEM_NAME><![CDATA[my_bt_system]]></VAULT_SYSTEM_NAME>
<VAULT_ACCOUNT_NAME><![CDATA[bt_account]]></VAULT_ACCOUNT_NAME>
</DIGITAL_VAULT>
<CREATED>
<DATE>2017-02-21T20:41:12Z</DATE>
<BY>joe_user</BY>
</CREATED>
<LAST_MODIFIED>
<DATE>2017-02-22T00:08:09Z</DATE>
</LAST_MODIFIED>
<COMMENTS><![CDATA[]]></COMMENTS>
</AUTH_WINDOW>
</AUTH_WINDOW_LIST>
</RESPONSE>

Qualys API Release Notes 11
New Support for BeyondTrust PBPS Vaults

**DTD updates:**

We added `VAULT_ACCOUNT_NAME` to both the Windows and Unix Authentication Record List Output DTDs.

**Windows Authentication Records List Output DTD**

```
<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_FOLDER?, VAULT_FILE?, VAULT_SECRET_NAME?,
VAULT_NS_TYPE?, VAULT_NS_NAME?, VAULT_ACCOUNT_NAME?)>
```

**Unix Authentication Records List Output DTD**

```
<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_USERNAME?, VAULT_FOLDER?, VAULT_FILE?,
VAULT_EP_CONT?, VAULT_NS_TYPE?, VAULT_NS_NAME?, VAULT_ACCOUNT_NAME?)>
```
New API Support for Option Profiles

The new Option Profile API allows customers to import/export option profiles from one subscription to another in XML format. The API user must have the Manager role.

Export Option Profile API

The Export Option Profile API (/api/2.0/fo/subscription/option_profile/?action=export) allows the user to export one option profile or all option profiles in the subscription to an XML file. The output of an Export Option Profile API call is proving as POST Raw Data.

Parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action=export</td>
<td>(Required) The GET or POST method may be used.</td>
</tr>
<tr>
<td>output_format={XML}</td>
<td>(Optional) XML format is supported. When unspecified, output format is XML.</td>
</tr>
<tr>
<td>option_profile_id={value}</td>
<td>(Optional) By default all option profiles will be exported. Specify an option profile ID and we’ll export the option profile matching this ID only.</td>
</tr>
<tr>
<td>option_profile_title={value}</td>
<td>(Optional) By default all option profiles will be exported. Specify a title and we’ll export the option profile matching this title only - exact match is required.</td>
</tr>
<tr>
<td>option_profile_type={value}</td>
<td>(Optional) Option profile group name/type, e.g. user (for user defined), compliance (for compliance profile), pci (for PCI vulnerabilities profile). Note: “option_profile_type” parameter can be specified with “option_profile_id” or “option_profile_title”.</td>
</tr>
</tbody>
</table>

Example 1: Export Option Profile

API request:

curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
-X GET "action=export"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile"

All the option profiles in the user’s account get exported in XML format.

XML Response:

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM "https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/option_profile_info.dtd">```
New API Support for Option Profiles

```xml
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>111186</ID>
            <GROUP_NAME><![CDATA[OP-SCAN]]></GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID><![CDATA[John Doe(john_doe)]]></USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>44</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>1</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>N/A</UPDATE_DATE>
        </BASIC_INFO>
        <SCAN>
            <PORTS>
                <TCP_PORTS_TYPE>full</TCP_PORTS_TYPE>
                <THREE_WAY_HANDSHAKE>1</THREE_WAY_HANDSHAKE>
            </TCP_PORTS>
            <UDP_PORTS>
                <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
                <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
                <ADDITIONAL_PORTS>1-1024,8080,8181</ADDITIONAL_PORTS>
            </UDP_PORTS>
            <AUTHORITATIVE_OPTION>1</AUTHORITATIVE_OPTION>
        </PORTS>
        <SCAN_DEAD_HOSTS>1</SCAN_DEAD_HOSTS>
        <CLOSE_VULNERABILITIES>
            <HAS_CLOSE_VULNERABILITIES>1</HAS_CLOSE_VULNERABILITIES>
            <HOST_NOT_FOUND_ALIVE>7</HOST_NOT_FOUND_ALIVE>
        </CLOSE_VULNERABILITIES>
        <PURGE_OLD_HOST_OS_CHANGED>1</PURGE_OLD_HOST_OS_CHANGED>
        <PERFORMANCE>
            <PARALLEL_SCALING>1</PARALLEL_SCALING>
            <OVERALL_PERFORMANCE>Custom</OVERALL_PERFORMANCE>
            <HOSTS_TO_SCAN>
                <EXTERNAL_SCANNERS>30</EXTERNAL_SCANNERS>
                <SCANNER_APPLIANCES>48</SCANNER_APPLIANCES>
            </HOSTS_TO_SCAN>
            <PROCESSES_TO_RUN>
                <TOTAL_PROCESSES>18</TOTAL_PROCESSES>
                <HTTP_PROCESSES>18</HTTP_PROCESSES>
            </PROCESSES_TO_RUN>
            <PACKET_DELAY>Minimum</PACKET_DELAY>
            <PORTSCANNING_AND_HOST_DISCOVERY>Minimum</PORTSCANNING_AND_HOST_DISCOVERY>
        </PERFORMANCE>
    </OPTION_PROFILE>
</OPTION_PROFILES>
```
New API Support for Option Profiles

RY>

</PERFORMANCE>
<LOAD_BALANCER_DETECTION>1</LOAD_BALANCER_DETECTION>
PASSWORD_BRUTE_FORCING>

SYSTEM>
HAS_SYSTEM>1</HAS_SYSTEM>
SYSTEM_LEVEL>Standard</SYSTEM_LEVEL>
</SYSTEM>
CUSTOM_LIST>
CUSTOM>
-ID>3001</ID>
-TITLE><![CDATA[123]]></TITLE>
-TYPE>FTP</TYPE>

LOGIN_PASSWORD><![CDATA[L:temp,P:123123123]]></LOGIN_PASSWORD>
</CUSTOM>
</CUSTOM_LIST>
</PASSWORD_BRUTE_FORCING>
VULNERABILITY_DETECTION>
CUSTOM_LIST>
CUSTOM>
-ID>2094</ID>
-TITLE><![CDATA[Option Profile: Qualys Top 20 Options]]></TITLE>
</CUSTOM>
CUSTOM>
-ID>2095</ID>
-TITLE><![CDATA[Option Profile: 2008 SANS20 Options]]></TITLE>
</CUSTOM>
CUSTOM>
-ID>2096</ID>
-TITLE><![CDATA[Scan Report Template: High Severity Report]]></TITLE>
</CUSTOM>
CUSTOM>
-ID>5230</ID>
-TITLE><![CDATA[118960]]></TITLE>
</CUSTOM>
CUSTOM>
-ID>87936</ID>
-TITLE><![CDATA[Bash Shellshock Detection]]></TITLE>
</CUSTOM>
CUSTOM>
-ID>87937</ID>
-TITLE><![CDATA[Heartbleed Detection]]></TITLE>
</CUSTOM>
CUSTOM>
-ID>87938</ID>
-TITLE><![CDATA[Windows Authentication Results v.1]]></TITLE>
</CUSTOM>

Qualys API Release Notes
New API Support for Option Profiles

</CUSTOM>
</CUSTOM>
</ID>87939</ID>
<TITLE><![CDATA[Unix Authentication Results v.1]]></TITLE>
</CUSTOM>
</CUSTOM>
</ID>87940</ID>
<TITLE><![CDATA[Inventory Results v.1]]></TITLE>
</CUSTOM>
</CUSTOM>
</ID>87941</ID>
<TITLE><![CDATA[SSL Certificates]]></TITLE>
</CUSTOM>
</CUSTOM_LIST>
</DETECTION_INCLUDE>
</BASIC_HOST_INFO_CHECKS>1</BASIC_HOST_INFO_CHECKS>
</OVAL_CHECKS>
</DETECTION_INCLUDE>
</DETECTION_EXCLUDE>
</CUSTOM_LIST>
</DETECTION_EXCLUDE>
</VULNERABILITY_DETECTION>
</AUTHENTICATION><![CDATA[Windows, Unix, Oracle, Oracle Listener, SNMP, VMware, DB2, HTTP, MySQL]]></AUTHENTICATION>
</ADDL_CERT_DETECTION>1</ADDL_CERT_DETECTION>
</DISSOLVABLE_AGENT>
</DISSOLVABLE_AGENT_ENABLE>1</DISSOLVABLE_AGENT_ENABLE>
</WINDOWS_SHARE_ENUMERATION_ENABLE>1</WINDOWS_SHARE_ENUMERATION_ENABLE>
</DISSOLVABLE_AGENT>
</LITE_OS.Scan>1</LITE_OS.Scan>
</CUSTOM_HTTP_HEADER>
</SCAN>
</MAP>
</BASIC_INFO_GATHERING_ON>netblockonly</BASIC_INFO_GATHERING_ON>
</TCP_PORTS>
</TCP_PORTS_STANDARD_SCAN>1</TCP_PORTS_STANDARD_SCAN>
</TCP_PORTS_ADDITIONAL>
</HAS_ADDITIONAL>1</HAS_ADDITIONAL>
</ADDITIONAL_PORTS>1,2,3,80</ADDITIONAL_PORTS>
</TCP_PORTS_ADDITIONAL>
</TCP_PORTS>
<UDP_PORTS>
  <UDP_PORTS_STANDARD_SCAN>1</UDP_PORTS_STANDARD_SCAN>
  <UDP_PORTS_ADDITIONAL>
    <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
    <ADDITIONAL_PORTS>4,5,6,8181</ADDITIONAL_PORTS>
  </UDP_PORTS_ADDITIONAL>
</UDP_PORTS>

<MAP_OPTIONS>
  <PERFORM_LIVE_HOST_Sweep>1</PERFORM_LIVE_HOST_Sweep>
  <DISABLE_DNS_TRAFFIC>1</DISABLE_DNS_TRAFFIC>
</MAP_OPTIONS>

<MAP_PERFORMANCE>
  <OVERALL_PERFORMANCE>Custom</OVERALL_PERFORMANCE>
  <MAP_PARALLEL>
    <EXTERNAL_SCANNERS>16</EXTERNAL_SCANNERS>
    <SCANNER_APPLIANCES>14</SCANNER_APPLIANCES>
    <NETBLOCK_SIZE>64</NETBLOCK_SIZE>
  </MAP_PARALLEL>
  <PACKET_DELAY>Maximum</PACKET_DELAY>
</MAP_PERFORMANCE>

<MAP_AUTHENTICATION>VMware</MAP_AUTHENTICATION>

<ADDITIONAL>
  <HOST_DISCOVERY>
    <TCP_PORTS>
      <STANDARD_SCAN>1</STANDARD_SCAN>
      <TCP_ADDITIONAL>
        <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
        <ADDITIONAL_PORTS>1-6,1024</ADDITIONAL_PORTS>
      </TCP_ADDITIONAL>
    </TCP_PORTS>
    <UDP_PORTS>
      <STANDARD_SCAN>1</STANDARD_SCAN>
    </UDP_PORTS>
    <ICMP>1</ICMP>
  </HOST_DISCOVERY>
  <BLOCK_RESOURCES>
    <WATCHGUARD_DEFAULT_BLOCKED_PORTS>1</WATCHGUARD_DEFAULT_BLOCKED_PORTS>
    <ALL_REGISTERED_IPS>1</ALL_REGISTERED_IPS>
  </BLOCK_RESOURCES>
  <PACKET_OPTIONS>
    <IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TCP_RST>
    <IGNORE_ALL_TCP_RST>1</IGNORE_ALL_TCP_RST>
  </PACKET_OPTIONS>
</ADDITIONAL>

Qualys API Release Notes
New API Support for Option Profiles

Example 2: Export Option Profile with specific title and ID

API request:

curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"  
-X GET "action=export&option_profile_title=OP-COMP&option_profile_id=111235"  
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile"

The option profile with the specified id and title in the user’s account get exported in XML format.

XML Response:

<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM  
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/option_profile_info.dtd">  
<OPTION_PROFILES>  
<OPTION_PROFILE>  
<BASIC_INFO>  
<ID>111235</ID>  
<GROUP_NAME><![CDATA[OP-COMP]]></GROUP_NAME>  
<GROUP_TYPE>compliance</GROUP_TYPE>  
<User_ID><![CDATA[John Doe (john_doe)]></USER_ID>  
<Unit_ID>0</UNIT_ID>  
<Subscription_ID>44</Subscription_ID>  
<IS_GLOBAL>0</ISGLOBAL>  
<UPDATE_DATE>N/A</UPDATE_DATE>  
</BASIC_INFO>  
<SCAN>  
<TARGETED_SCAN>1</TARGETED_SCAN>  
</PORTS>  
<PERFORMANCE>  
<PARALLEL_SCALING>0</PARALLEL_SCALING>  
<OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>  
<HOSTS_TO_SCAN>  
<EXTERNAL_SCANNERS>5</EXTERNAL_SCANNERS>  
<SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>  
</HOSTS_TO_SCAN>  
<PROCESSES_TO_RUN>
New API Support for Option Profiles

<TOTAL_PROCESSES>10</TOTAL_PROCESSES>
<HTTP_PROCESSES>10</HTTP_PROCESSES>
</PROCESSES_TO_RUN>
<PACKET_DELAY>Short</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Minimum</PORT_SCANNING_AND_HOST_DISCOVERY>
</PERFORMANCE>
<DISSOLVABLE_AGENT>
<DISSOLVABLE_AGENT_ENABLE>1</DISSOLVABLE_AGENT_ENABLE>
</DISSOLVABLE_AGENT>

<PASSWORD_AUDITING_ENABLE>
<HAS_PASSWORD_AUDITING_ENABLE>1</HAS_PASSWORD_AUDITING_ENABLE>
<CUSTOM_PASSWORD_DICTIONARY>asdf</CUSTOM_PASSWORD_DICTIONARY>
</PASSWORD_AUDITING_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>1</WINDOWS_SHARE_ENUMERATION_ENABLE>

<WINDOWS_DIRECTORY_SEARCH_ENABLE>1</WINDOWS_DIRECTORY_SEARCH_ENABLE>
</DISSOLVABLE_AGENT>
</CONTROL_TYPES>
</SCAN>
</ADDITIONAL>

<HOST_DISCOVERY>
<TCP_PORTS>
<STANDARD_SCAN>1</STANDARD_SCAN>
</TCP_PORTS>
<UDP_PORTS>
<STANDARD_SCAN>1</STANDARD_SCAN>
</UDP_PORTS>
<ICMP>1</ICMP>
</HOST_DISCOVERY>
</BLOCK_RESOURCES>

<WATCHGUARD_DEFAULT_BLOCKED_PORTS>1</WATCHGUARD_DEFAULT_BLOCKED_PORTS>
<ALL_REGISTERED_IPS>1</ALL_REGISTERED_IPS>
</BLOCK_RESOURCES>
</PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>1</NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
</PACKET_OPTIONS>
New API Support for Option Profiles

Example 3: Export Option Profile of type PCI

**API request (export with option profile type):**

curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X GET "action=export&option_profile_type=pci" "https://qualysapi.qualys.com/api/2.0/fo/subscription(option_profile"}

The option profile with PCI type in the user's account get exported in XML format.

**XML Response:**

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM "https://qualysapi.qualys.com/api/2.0/fo/subscription(option_profile_info.dtd">
<OPTION_PROFILES>
<OPTION_PROFILE>
<BASIC_INFO>
<IID>111223</IID>
<GROUP_NAME><![CDATA[PCI-Example]]></GROUP_NAME>
<GROUP_TYPE>pci</GROUP_TYPE>
USER_ID><![CDATA[John Doe (john_doe)]></USER_ID>
<UNIT_ID>0</UNIT_ID>
<SUBSCRIPTION_ID>44</SUBSCRIPTION_ID>
<IS_GLOBAL>1</IS_GLOBAL>
<IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
<UPDATE_DATE>N/A</UPDATE_DATE>
</BASIC_INFO>
<SCAN>
<SCAN_DEAD_HOSTS>1</SCAN_DEAD_HOSTS>
<CLOSE_VULNERABILITIES>
<HAS_CLOSE_VULNERABILITIES>1</HAS_CLOSE_VULNERABILITIES>
<HOST_NOT_FOUND_ALIVE>4</HOST_NOT_FOUND_ALIVE>
</CLOSE_VULNERABILITIES>
<PURGE_OLD_HOST_OS_CHANGED>1</PURGE_OLD_HOST_OS_CHANGED>
<PERFORMANCE>
<PARALLEL_SCALING>1</PARALLEL_SCALING>
<OVERALL_PERFORMANCE>Low</OVERALL_PERFORMANCE>
<HOSTS_TO_SCAN>
<EXTERNAL_SCANNERS>5</EXTERNAL_SCANNERS>
<Scanner_APPLIANCES>10</Scanner_APPLIANCES>
</HOSTS_TO_SCAN>
<PROCESSES_TO_RUN>
<TOTAL_PROCESSES>4</TOTAL_PROCESSES>
</PERFORMANCE>
</SCAN>
```
New API Support for Option Profiles

<HTTP_PROCESSES>2</HTTP_PROCESSES>
</PROCESSES_TO_RUN>
<PACKET_DELAY>Long</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Minimum</PORT_SCANNING_AND_HOST_DISCOVERY>
</PERFORMANCE>
</SCAN>
<ADDITIONAL>
<HOST_DISCOVERY>
<TCP_PORTS>
<STANDARD_SCAN>1</STANDARD_SCAN>
<TCP_ADDITIONAL>
<HAS_ADDITIONAL>1</HAS_ADDITIONAL>
<ADDITIONAL_PORTS>1-6,1024</ADDITIONAL_PORTS>
</TCP_ADDITIONAL>
</TCP_PORTS>
</HOST_DISCOVERY>
</ADDITIONAL>
</OPTION_PROFILE>
</OPTION_PROFILES>

Import Option Profile API

The Import Option Profile API (/api/2.0/fo/subscription/option_profile/?action=import) allows the user to import all option profiles defined in input XML file.

When calling the Import Option Profile API the user needs to pass the proper XML with Content-Type XML. This will create option profiles in that user’s subscription. All validations are applied as in the Qualys portal UI while creating option profiles using the Import Option Profile API.

Validations and Constraints:

1) The Option Profile DTD file is used to validate a generated/exported Option Profile XML file.

2) An XSD file is used to validate a proper format and required elements of the option profile XML file when importing this file.

3) While importing, any Search Lists defined for Vulnerability Detection, Custom and/or Excluded Lists, must be created in the user’s subscription before making an Import Option Profile call. At import time we try to match the Search List “title” to a search list title in the user’s subscription. If a match is found the search list is used, otherwise “Complete” Vulnerability Detection is assigned.

4) Password Brute Force Lists are not imported and will always be empty assigned, regardless of Option Profile XML content.
New API Support for Option Profiles

5) Policies defined for the PC Scan Restriction feature are not imported and will be empty assigned, regardless of Option Profile XML content.

Parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action=import</td>
<td>(Required) The POST method must be used.</td>
</tr>
</tbody>
</table>

Example: Import option profiles in the input file into the user’s account.

API request:

curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @Export_OP.xml
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile"

Note: “Export_OP.xml” contains the request POST data.

Request POST data:

```xml
<?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>11123</ID>
      <GROUP_NAME><![CDATA[OP-SCAN]]></GROUP_NAME>
      <GROUP_TYPE>user</GROUP_TYPE>
      <USER_ID><![CDATA[John Doe (john_doe)]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>76084</SUBSCRIPTION_ID>
      <IS_DEFAULT>0</IS_DEFAULT>
      <IS_GLOBAL>1</IS_GLOBAL>
      <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
      <UPDATE_DATE>N/A</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <TCP_PORTS>
        <TCP_PORTS_TYPE>full</TCP_PORTS_TYPE>
        <THREE_WAY_HANDSHAKE>1</THREE_WAY_HANDSHAKE>
      </TCP_PORTS>
      <UDP_PORTS>
        <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
      </UDP_PORTS>
    </SCAN>
  </OPTION_PROFILE>
</OPTION_PROFILES>
```
New API Support for Option Profiles

</UDP_PORTS_ADDITIONAL>
</UDP_PORTS>
<AUTHORITATIVE_OPTION>1</AUTHORITATIVE_OPTION>
</PORTS>
<SCAN_DEAD_HOSTS>1</SCAN_DEAD_HOSTS>
<CLOSE_VULNERABILITIES>
  <HAS_CLOSE_VULNERABILITIES>1</HAS_CLOSE_VULNERABILITIES>
  <HOST_NOT_FOUND_ALIVE>7</HOST_NOT_FOUND_ALIVE>
</CLOSE_VULNERABILITIES>
<PURGE_OLD_HOST_OS_CHANGED>1</PURGE_OLD_HOST_OS_CHANGED>
</PERFORMANCE>
<PARALLEL_SCALING>1</PARALLEL_SCALING>
<OVERALL_PERFORMANCE>Custom</OVERALL_PERFORMANCE>
<HOSTS_TO_SCAN>
  <EXTERNAL_SCANNERS>30</EXTERNAL_SCANNERS>
  <SCANNER_APPLIANCES>48</SCANNER_APPLIANCES>
</HOSTS_TO_SCAN>
<PROCESSES_TO_RUN>
  <TOTAL_PROCESSES>18</TOTAL_PROCESSES>
  <HTTP_PROCESSES>18</HTTP_PROCESSES>
</PROCESSES_TO_RUN>
<PACKET_DELAY>Maximum</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Minimum</PORT_SCANNING_AND_HOST_DISCOVERY>
</PERFORMANCE>
<LOAD_BALANCER_DETECTION>1</LOAD_BALANCER_DETECTION>

<VULNERABILITY_DETECTION>
<CUSTOM_LIST>
  <CUSTOM>
    <ID>3001</ID>
    <TITLE><![CDATA[123]]></TITLE>
    <TYPE>FTP</TYPE>
    <LOGIN_PASSWORD><![CDATA[L:temp,P:123123123]]></LOGIN_PASSWORD>
  </CUSTOM>
</CUSTOM_LIST>
</VULNERABILITY_DETECTION>
</CUSTOM_LIST>
</PASSWORD_BRUTE_FORCING>
</CUSTOM_LIST>
</SYSTEM>
</CUSTOM>
</CUSTOM_LIST>
</PASSWORD_BRUTE_FORCING>
</CUSTOM_LIST>
</VULNERABILITY_DETECTION>
</CUSTOM_LIST>
</CUSTOM>
</CUSTOM_LIST>
</VULNERABILITY_DETECTION>
</CUSTOM_LIST>
</CUSTOM>
</CUSTOM_LIST>
</VULNERABILITY_DETECTION>
</CUSTOM_LIST>
</CUSTOM>
</CUSTOM_LIST>
</VULNERABILITY_DETECTION>
</CUSTOM_LIST>
</CUSTOM>
</CUSTOM_LIST>
</VULNERABILITY_DETECTION>
</CUSTOM_LIST>
</CUSTOM>
</CUSTOM_LIST>
</VULNERABILITY_DETECTION>
</CUSTOM_LIST>
</CUSTOM>
</CUSTOM_LIST>
</VULNERABILITY_DETECTION>
</CUSTOM_LIST>
</CUSTOM>
</CUSTOM_LIST>
</VULNERABILITY_DETECTION>
</CUSTOM_LIST>
</CUSTOM>
</CUSTOM_LIST>
</VULNERABILITY_DETECTION>
</CUSTOM_LIST>
</CUSTOM>
</CUSTOM_LIST>
</VULNERABILITY_DETECTION>
</CUSTOM_LIST>
</CUSTOM>
</CUSTOM_LIST>
</VULNERABILITY_DETECTION>
New API Support for Option Profiles

<CUSTOM>
  <ID>2095</ID>
  <TITLE><![CDATA[Option Profile: 2008 SANS20 Options]]></TITLE>
</CUSTOM>

<CUSTOM>
  <ID>2096</ID>
  <TITLE><![CDATA[Scan Report Template: High Severity Report]]></TITLE>
</CUSTOM>

<CUSTOM>
  <ID>5230</ID>
  <TITLE><![CDATA[118960]]></TITLE>
</CUSTOM>

<CUSTOM>
  <ID>87936</ID>
  <TITLE><![CDATA[Bash Shellshock Detection]]></TITLE>
</CUSTOM>

<CUSTOM>
  <ID>87937</ID>
  <TITLE><![CDATA[Heartbleed Detection]]></TITLE>
</CUSTOM>

<CUSTOM>
  <ID>87938</ID>
  <TITLE><![CDATA[Windows Authentication Results v.1]]></TITLE>
</CUSTOM>

<CUSTOM>
  <ID>87939</ID>
  <TITLE><![CDATA[Unix Authentication Results v.1]]></TITLE>
</CUSTOM>

<CUSTOM>
  <ID>87940</ID>
  <TITLE><![CDATA[Inventory Results v.1]]></TITLE>
</CUSTOM>

<CUSTOM>
  <ID>87941</ID>
  <TITLE><![CDATA[SSL Certificates]]></TITLE>
</CUSTOM>

<DETECTION_INCLUDE>
  <BASIC_HOST_INFO_CHECKS>1</BASIC_HOST_INFO_CHECKS>
  <OVAL_CHECKS>1</OVAL_CHECKS>
</DETECTION_INCLUDE>

<DETECTION_EXCLUDE>
  <CUSTOM_LIST>
    <CUSTOM>
      <ID>2099</ID>
      <TITLE><![CDATA[DL]]></TITLE>
    </CUSTOM>
  </CUSTOM_LIST>
</DETECTION_EXCLUDE>
New API Support for Option Profiles

</DETECTION_EXCLUDE>
</VULNERABILITY_DETECTION>
<AUTHENTICATION><![CDATA[Windows,Unix,Oracle,Oracle Listener,SNMP,VMware,DB2,HTTP,MySQL]]></AUTHENTICATION>
</ADDL_CERT_DETECTION>
</DISSOLVABLE_AGENT>
</DISSOLVABLE_AGENT_ENABLE>
</WINDOWS_SHARE_ENUMERATION_ENABLE>
</LITE_OS_SCAN>
</CUSTOM_HTTP_HEADER>
</SCAN>
</MAP>
</BASIC_INFO_GATHERING_ON>
</TCP_PORTS>
</UDP_PORTS>
</MAP_OPTIONS>
</PERFORM_LIVE_HOST_Sweep>
</DISABLE_DNS_TRAFFIC>
</MAP_OPTIONS>
</MAP_PERFORMANCE>
</OVERALL_PERFORMANCE>Custom</OVERALL_PERFORMANCE>
</MAP_PARALLEL>
</EXTERNAL_SCANNERS>16</EXTERNAL_SCANNERS>
</SCANNER_APPLIANCES>14</SCANNER_APPLIANCES>
</NETBLOCK_SIZE>64</NETBLOCK_SIZE>
</MAP_PARALLEL>
</PACKET_DELAY>Medium</PACKET_DELAY>
</MAP_PERFORMANCE>
</MAP_AUTHENTICATION>VMware</MAP_AUTHENTICATION>
</MAP>
</ADDITIONAL>
</TCP_PORTS>
New API Support for Option Profiles

```xml
<STANDARD_SCAN>1</STANDARD_SCAN>
<TCP_ADDITIONAL>
  <HAS_ADDITIONAL>1</HAS_ADDITIONAL>
  <ADDITIONAL_PORTS>1-6,1024</ADDITIONAL_PORTS>
</TCP_ADDITIONAL>
</TCP_PORTS>
<UDP_PORTS>
  <STANDARD_SCAN>1</STANDARD_SCAN>
</UDP_PORTS>
</UDP_PORTS>
</TCP_ADDITIONAL>
</TCP_PORTS>
<UDP_PORTS>
  <STANDARD_SCAN>1</STANDARD_SCAN>
</UDP_PORTS>
</UDP_PORTS>
</TCP_PORTS>
</TCP_ADDITIONAL>
</TCP_ADDITIONAL>
</TCP_PORTS>
<UDP_PORTS>
  <STANDARD_SCAN>1</STANDARD_SCAN>
</UDP_PORTS>
</UDP_PORTS>
</TCP_ADDITIONAL>
</TCP_ADDITIONAL>
</TCP_PORTS>
<ICMP>1</ICMP>
</HOST_DISCOVERY>
<BLOCK_RESOURCES>
  <WATCHGUARD_DEFAULT_BLOCKED_PORTS>1</WATCHGUARD_DEFAULT_BLOCKED_PORTS>
    <ALL_REGISTERED_IPS>1</ALL_REGISTERED_IPS>
  </WATCHGUARD_DEFAULT_BLOCKED_PORTS>
  <ALL_REGISTERED_IPS>1</ALL_REGISTERED_IPS>
</BLOCK_RESOURCES>
</BLOCK_RESOURCES>
</PACKET_OPTIONS>
<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TCP_RST>
  <IGNORE_ALL_TCP_RST>1</IGNORE_ALL_TCP_RST>
</IGNORE_FIREWALL_GENERATED_TCP_RST>
</PACKET_OPTIONS>
<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>
</IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>
<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>1</NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
  </PACKET_OPTIONS>
</PACKET_OPTIONS>
</OPTION_PROFILE>
</OPTION_PROFILES>

XML Response:

```xml
<?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>2017-04-03T11:17:43Z</DATETIME>
    <TEXT>Successfully imported Option profile for the subscription Id 76084</TEXT>
  </RESPONSE>
  <ITEM_LIST>
    <ITEM>
      <KEY>111234</KEY>
      <VALUE>PCI-John</VALUE>
    </ITEM>
  </ITEM_LIST>
</SIMPLE_RETURN>
```
New API Support for Option Profiles

Option Profile DTD

```
<base_url>/fo/api/2.0/subscription/option_profile/option_profile_info.dtd

<!ELEMENT OPTION_PROFILES (OPTION_PROFILE)*>

<!ELEMENT OPTION_PROFILE (BASIC_INFO, SCAN, MAP?, ADDITIONAL)>
<!ELEMENT BASIC_INFO (ID, GROUP_NAME, GROUP_TYPE, USER_ID, UNIT_ID, SUBSCRIPTION_ID, IS_DEFAULT?, IS_GLOBAL?, IS_OFFLINE_SYNCABLE?, UPDATE_DATE?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT GROUP_NAME (#PCDATA)>
<!ELEMENT GROUP_TYPE (#PCDATA)>
<!ELEMENT USER_ID (#PCDATA)>
<!ELEMENT UNIT_ID (#PCDATA)>
<!ELEMENT SUBSCRIPTION_ID (#PCDATA)>
<!ELEMENT IS_DEFAULT (#PCDATA)>
<!ELEMENT IS_GLOBAL (#PCDATA)>
<!ELEMENT IS_OFFLINE_SYNCABLE (#PCDATA)>
<!ELEMENT UPDATE_DATE (#PCDATA)>


<!ELEMENT PORTS (TCP_PORTS?, UDP_PORTS?, AUTHORITATIVE_OPTION?, (STANDARD_SCAN|TARGETED_SCAN)?)>
<!ELEMENT TCP_PORTS (TCP_PORTS_TYPE?, TCP_PORTS_STANDARD_SCAN?, TCP_PORTS_ADDITIONAL?, THREE_WAY_HANDSHAKE?, STANDARD_SCAN?, TCP_ADDITIONAL?)>
<!ELEMENT TCP_PORTS_TYPE (#PCDATA)>
<!ELEMENT TCP_PORTS_ADDITIONAL (HAS_ADDITIONAL?, ADDITIONAL_PORTS?)>
<!ELEMENT HAS_ADDITIONAL (#PCDATA)>
<!ELEMENT ADDITIONAL_PORTS (#PCDATA)>
<!ELEMENT THREE_WAY_HANDSHAKE (#PCDATA)>

<!ELEMENT UDP_PORTS (UDP_PORTS_TYPE?, UDP_PORTS_STANDARD_SCAN?, UDP_PORTS_ADDITIONAL?, (STANDARD_SCAN|CUSTOM_PORT)?)>
<!ELEMENT UDP_PORTS_TYPE (#PCDATA)>
<!ELEMENT UDP_PORTS_ADDITIONAL (HAS_ADDITIONAL?, ADDITIONAL_PORTS?)>

<!ELEMENT AUTHORITATIVE_OPTION (#PCDATA)>
<!ELEMENT STANDARD_SCAN (#PCDATA)>
<!ELEMENT TARGETED_SCAN (#PCDATA)>
```
New API Support for Option Profiles

<!ELEMENT SCAN_DEAD_HOSTS (#PCDATA)>  
<!ELEMENT CLOSE_VULNERABILITIES (HAS_CLOSE_VULNERABILITIES?, HOST_NOTFOUND_ALIVE?)>  
<!ELEMENT HAS_CLOSE_VULNERABILITIES (#PCDATA)>  
<!ELEMENT HOST_NOTFOUND_ALIVE (#PCDATA)>  
<!ELEMENT PURGE_OLD_HOST_OS_CHANGED (#PCDATA)>  

<!ELEMENT PERFORMANCE (PARALLEL_SCALING?, OVERALL_PERFORMANCE, HOSTS_TO_SCAN, PROCESSES_TO_RUN, PACKET_DELAY, PORT_SCANNING_AND_HOST_DISCOVERY)>  
<!ELEMENT PARALLEL_SCALING (#PCDATA)>  
<!ELEMENT OVERALL_PERFORMANCE (#PCDATA)>  
<!ELEMENT HOSTS_TO_SCAN (EXTERNAL_SCANNERS, SCANNER_APPLIANCES)>  
<!ELEMENT EXTERNAL_SCANNERS (#PCDATA)>  
<!ELEMENT SCANNER_APPLIANCES (#PCDATA)>  
<!ELEMENT PROCESSES_TO_RUN (TOTAL_PROCESSES, HTTP_PROCESSES)>  
<!ELEMENT TOTAL_PROCESSES (#PCDATA)>  
<!ELEMENT HTTP_PROCESSES (#PCDATA)>  
<!ELEMENT PACKET_DELAY (#PCDATA)>  
<!ELEMENT PORT_SCANNING_AND_HOST_DISCOVERY (#PCDATA)>  

<!ELEMENT LOAD_BALANCER_DETECTION (#PCDATA)>  
<!ELEMENT PASSWORD_BRUTE_FORCING (SYSTEM?, CUSTOM_LIST?)>  
<!ELEMENT SYSTEM (HAS_SYSTEM?, SYSTEM_LEVEL?)>  
<!ELEMENT HAS_SYSTEM (#PCDATA)>  
<!ELEMENT SYSTEM_LEVEL (#PCDATA)>  
<!ELEMENT CUSTOM_LIST (CUSTOM+)>  
<!ELEMENT CUSTOM (ID, TITLE, TYPE?, LOGIN_PASSWORD?)+>  
<!ELEMENT TITLE (#PCDATA)>  
<!ELEMENT TYPE (#PCDATA)>  
<!ELEMENT LOGIN_PASSWORD (#PCDATA)>  

<!ELEMENT VULNERABILITY_DETECTION ((COMPLETE|CUSTOM_LIST|RUNTIME), DETECTION_INCLUDE?, DETECTION_EXCLUDE?)>  
<!ELEMENT COMPLETE (#PCDATA)>  
<!ELEMENT RUNTIME (#PCDATA)>  
<!ELEMENT DETECTION_INCLUDE (BASIC_HOST_INFO_CHECKS, OVAL_CHECKS)>  
<!ELEMENT BASIC_HOST_INFO_CHECKS (#PCDATA)>  
<!ELEMENT OVAL_CHECKS (#PCDATA)>  
<!ELEMENT DETECTION_EXCLUDE (CUSTOM_LIST+)>  
<!ELEMENT AUTHENTICATION (#PCDATA)>  
<!ELEMENT ADDL_CERT_DETECTION (#PCDATA)>
New API Support for Option Profiles

<?xml version="1.0" encoding="UTF-8"?>
<!ELEMENT DISSOLVABLE_AGENT (DISSOLVABLE_AGENT_ENABLE, PASSWORD_AUDITING_ENABLE?, WINDOWS_SHARE_ENUMERATION_ENABLE, WINDOWS_DIRECTORY_SEARCH_ENABLE?)>
<!ELEMENT DISSOLVABLE_AGENT_ENABLE (#PCDATA)>
<!ELEMENT PASSWORD_AUDITING_ENABLE (HAS_PASSWORD_AUDITING_ENABLE?, CUSTOM_PASSWORD_DICTIONARY?)>
<!ELEMENT HAS_PASSWORD_AUDITING_ENABLE (#PCDATA)>
<!ELEMENT CUSTOM_PASSWORD_DICTIONARY (#PCDATA)>
<!ELEMENT WINDOWS_SHARE_ENUMERATION_ENABLE (#PCDATA)>
<!ELEMENT WINDOWS_DIRECTORY_SEARCH_ENABLE (#PCDATA)>

<!ELEMENT LITE_OS_SCAN (#PCDATA)>
<!ELEMENT CUSTOM_HTTP_HEADER (VALUE?, DEFINITION_KEY?, DEFINITION_VALUE?)>
<!ELEMENT VALUE (#PCDATA)>
<!ELEMENT DEFINITION_KEY (#PCDATA)>
<!ELEMENT DEFINITION_VALUE (#PCDATA)>

<!ELEMENT HOST_ALIVE_TESTING (#PCDATA)>

<!ELEMENT SCAN_RESTRICTION (SCAN_BY_POLICY?)>
<!ELEMENT SCAN_BY_POLICY (POLICY+)>
<!ELEMENT POLICY (ID, TITLE)>

<!ELEMENT CONTROL_TYPES (FIM_CONTROLS_ENABLED?, CUSTOM_WMI_QUERY_CHECKS?)>
<!ELEMENT FIM_CONTROLS_ENABLED (#PCDATA)>
<!ELEMENT CUSTOM_WMI_QUERY_CHECKS (#PCDATA)>

<!ELEMENT MAP (BASIC_INFO_GATHERING_ON, TCP_PORTS?, UDP_PORTS?, MAP_OPTIONS?, MAP_PERFORMANCE?, MAP_AUTHENTICATION?)>
<!ELEMENT BASIC_INFO_GATHERING_ON (#PCDATA)>
<!ELEMENT TCP_PORTS_STANDARD_SCAN (#PCDATA)>
<!ELEMENT UDP_PORTS_STANDARD_SCAN (#PCDATA)>

<!ELEMENT MAP_OPTIONS (PERFORM_LIVE_HOST_Sweep?, DISABLE_DNS_TRAFFIC?)>
<!ELEMENT PERFORM_LIVE_HOST_Sweep (#PCDATA)>
<!ELEMENT DISABLE_DNS_TRAFFIC (#PCDATA)>

<!ELEMENT MAP_PERFORMANCE (OVERALL_PERFORMANCE, MAP_PARALLEL?, PACKET_DELAY)>
<!ELEMENT MAP_PARALLEL (EXTERNAL_SCANNERS, SCANNER_APPLIANCES, NETBLOCK_SIZE)>
<!ELEMENT NETBLOCK_SIZE (#PCDATA)>
<!ELEMENT MAP_AUTHENTICATION (#PCDATA)>

Qualys API Release Notes
New API Support for Option Profiles

<!ELEMENT ADDITIONAL (HOST_DISCOVERY, BLOCK_RESOURCES?, PACKET_OPTIONS?)>
<!ELEMENT HOST_DISCOVERY (TCP_PORTS?, UDP_PORTS?, ICMP?)>
<!ELEMENT TCP_ADDITIONAL (HAS_ADDITIONAL?, ADDITIONAL_PORTS?)>
<!ELEMENT CUSTOM_PORT (#PCDATA)>
<!ELEMENT ICMP (#PCDATA)>
<!ELEMENT BLOCK_RESOURCES ((WATCHGUARD_DEFAULT_BLOCKED_PORTS|CUSTOM_PORT_LIST), (ALL_REGISTERED_IPS|CUSTOM_IP_LIST))>
<!ELEMENT WATCHGUARD_DEFAULT_BLOCKED_PORTS (#PCDATA)>
<!ELEMENT CUSTOM_PORT_LIST (#PCDATA)>
<!ELEMENT ALL_REGISTERED_IPS (#PCDATA)>
<!ELEMENT CUSTOM_IP_LIST (#PCDATA)>
<!ELEMENT PACKET_OPTIONS (IGNORE_FIREWALL_GENERATED_TCP_RST?, IGNORE_ALL_TCP_RST?, IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK?, NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY?)>
<!ELEMENT IGNORE_FIREWALL_GENERATED_TCP_RST (#PCDATA)>
<!ELEMENT IGNORE_ALL_TCP_RST (#PCDATA)>
<!ELEMENT IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK (#PCDATA)>
<!ELEMENT NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY (#PCDATA)>
Scanner Appliance List - added Cloud Information

The Scanner Appliance List API v2 (/api/2.0/fo/appliance/ with action=list) is used to list scanner appliances in your account with their configurations. You can now include cloud information in the output for virtual scanner appliances deployed on cloud platforms - Amazon EC2, Microsoft Azure Cloud Platform and Google Cloud Platform.

To see cloud information, your API request must include the new input parameter include_cloud_info=1 and output_mode=full.

API request:
```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d "action=list&include_cloud_info=1&output_mode=full"
"https://qualysapi.qualys.com/api/2.0/fo/appliance/
```

XML output:
Sample 1 - Cloud Info for Amazon EC2
```
...<IS_CLOUD_DEPLOYED>1</IS_CLOUD_DEPLOYED>
<Cloud_Info>
  <Platform_Provider>ec2</Platform_Provider>
  <Ec2_Info>
    <Instance_ID>i-02441120f4e14e32c</Instance_ID>
    <Instance_Type>m3.medium</Instance_Type>
    <Ami_ID>ami-2d4ed53a</Ami_ID>
    <Account_ID>205767712438</Account_ID>
    <Instance_Region>US East (N. Virginia)</Instance_Region>
    <Instance_Availability_Zone>us-east-1c</Instance_Availability_Zone>
    <Instance_Zone_Type>Classic</Instance_Zone_Type>
    <Ip_Address_Private>10.181.43.219</Ip_Address_Private>
    <Hostname_Private>ip-10-181-43-219.ec2.internal</Hostname_Private>
  </Ec2_Info>
</Cloud_Info>
...
Sample 2 - Cloud Info for Microsoft Azure Cloud Platform

...<IS_CLOUD_DEPLOYED>1</IS_CLOUD_DEPLOYED>
<CLOUD_INFO>
<PLATFORM_PROVIDER>azure</PLATFORM_PROVIDER>
<AZURE_INFO>
<INSTANCE_ID>fa74c883-6877-4381-81f4-893bd444deb</INSTANCE_ID>
<User_NAME>u15449542569729</User_NAME>
<INSTANCE_LOCATION>eastus</INSTANCE_LOCATION>
<DEPLOYMENT_MODE>ARM</DEPLOYMENT_MODE>
<IP_ADDRESS_PRIVATE>10.94.1.8</IP_ADDRESS_PRIVATE>
<HOSTNAME_PRIVATE>sada-14876-azure</HOSTNAME_PRIVATE>
</AZURE_INFO>
</CLOUD_INFO>
...

Sample 3 - Cloud Info for Google Cloud Platform

...<IS_CLOUD_DEPLOYED>1</IS_CLOUD_DEPLOYED>
<CLOUD_INFO>
<PLATFORM_PROVIDER>gce</PLATFORM_PROVIDER>
<GCE_INFO>
<INSTANCE_ID>5361537763822761158</INSTANCE_ID>
<MACHINE_TYPE>n1-standard-2</MACHINE_TYPE>
<PROJECT_ID>1035365309337</PROJECT_ID>
<PROJECT_NAME>qvsa-test</PROJECT_NAME>
<PREEMPTIBLE>FALSE</PREEMPTIBLE>
<INSTANCE_ZONE>asia-east1-c</INSTANCE_ZONE>
<IP_ADDRESS_PRIVATE>10.240.0.28</IP_ADDRESS_PRIVATE>
<HOSTNAME_PRIVATE>sada-14837.c.qvsa-test.internal</HOSTNAME_PRIVATE>
<IP_ADDRESS_PUBLIC>35.185.143.253</IP_ADDRESS_PUBLIC>
<INSTANCE_NETWORK>default</INSTANCE_NETWORK>
<GCE_INSTANCE_TAGS>
<TAG_ID>sada-tag-2</TAG_ID>
<TAG_ID>sada-tag-3</TAG_ID>
<TAG_ID>sada-tag-4</TAG_ID>
</GCE_INSTANCE_TAGS>
</GCE_INFO>
</CLOUD_INFO>
...
**DTD update:**

We updated the Appliance List Output DTD (appliance_list_output.dtd) to include new elements for cloud information (in bold).

```xml
<!-- QUALYS APPLIANCE_LIST_OUTPUT DTD -->

<!ELEMENT APPLIANCE_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, APPLIANCE_LIST?, LICENSE_INFO?)>
  <!ELEMENT APPLIANCE_LIST (APPLIANCE+)>
      <!ELEMENT ID (#PCDATA)>
      <!ELEMENT UUID (#PCDATA)>
      <!ELEMENT NAME (#PCDATA)>
      <!ELEMENT NETWORK_ID (#PCDATA)>
      <!ELEMENT SOFTWARE_VERSION (#PCDATA)>
      <!ELEMENT RUNNING_SLICES_COUNT (#PCDATA)>
      <!ELEMENT RUNNING_SCAN_COUNT (#PCDATA)>
      <!ELEMENT STATUS (#PCDATA)>
      <!ELEMENT CMD_ONLY_START (#PCDATA)>
      <!ELEMENT MODEL_NUMBER (#PCDATA)>
      <!ELEMENT SERIAL_NUMBER (#PCDATA)>
      <!ELEMENT ACTIVATION_CODE (#PCDATA)>
      <!ELEMENT INTERFACE_SETTINGS (SETTING?, INTERFACE, IP_ADDRESS, NETMASK, GATEWAY, LEASE, IPV6_ADDRESS?, SPEED, DUPLEX, DNS)>
        <!ELEMENT SETTING (#PCDATA)>
        <!ELEMENT INTERFACE (#PCDATA)>
        <!ELEMENT IP_ADDRESS (#PCDATA)>
```
IP_ADDRESS_PRIVATE?, HOSTNAME_PRIVATE?,
IP_ADDRESS_PUBLIC?,
INSTANCE_NETWORK,
GCE_INSTANCE_TAGS
)

<!ELEMENT MACHINE_TYPE (#PCDATA)>
<!ELEMENT PROJECT_ID (#PCDATA)>
<!ELEMENT PROJECT_NAME (#PCDATA)>
<!ELEMENT INSTANCE_ZONE (#PCDATA)>
<!ELEMENT GCE_INSTANCE_TAGS (GCE_INSTANCE_TAG*)>
  <!ELEMENT GCE_INSTANCE_TAG (TAG_ID)>
  <!ELEMENT TAG_ID (#PCDATA)>
<!ELEMENT IP_ADDRESS_PUBLIC (#PCDATA)>
<!ELEMENT INSTANCE_NETWORK (#PCDATA)>

<!ELEMENT AZURE_INFO (INSTANCE_ID, USER_NAME,
  INSTANCE_LOCATION, DEPLOYMENT_MODE,
  IP_ADDRESS_PRIVATE?, HOSTNAME_PRIVATE?)>
<!ELEMENT USER_NAME (#PCDATA)>
<!ELEMENT INSTANCE_LOCATION (#PCDATA)>
<!ELEMENT DEPLOYMENT_MODE (#PCDATA)>

...
EC2 Assets - Improved Reporting of private DNS host name and Instance ID

For EC2 assets we’ll now show actual private DNS names for DNS hostname in the UI and API instead of EC2 Instance ID. These APIs have been updated: Host List API, Host Info API v1, VM Detection API, and Asset Search API. A new <EC2_INSTANCE_ID> tag has been added to related DTDs and the XML output will include this tag for EC2 assets when EC2 Scanning is enabled for the subscription.

UI Changes

Host List page: For EC2 assets, the DNS column now shows the EC2 asset’s private DNS name.

Host Info page: For EC2 assets, the private DNS name is shown for Hostname and EC2 Instance ID is shown separately.
EC2 Assets - Improved Reporting of private DNS host name and Instance ID

Asset Search: We’ve added new option to search by EC2 Instance ID, and the DNS Hostname attribute searches across private EC2 host names.

DTD Changes (API and Reports)

Scan Report (template based) changes

Updates to multiple report formats: XML, CSV, HTML, PDF and DOCX.

URL: <base_url>/api/2.0/fo/report/?action=launch
DTD: <base_url>/asset_data_report.dtd

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=launch&report_title=EC2Rep1&template_id=90111&output_format=xml"
"https://qualysapi.qualys.com/api/2.0/fo/report/
```

XML output: New <EC2_INSTANCE_ID> tag as well as new <EC2_INFO> tag. These tags will only appear in subscriptions with EC2 Scanning enabled and only when the “EC2 Related Information” option is selected in the report template.

```
<?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>10.90.2.30</IP>
```
EC2 Assets - Improved Reporting of private DNS host name and Instance ID

<TRACKING_METHOD>EC2</TRACKING_METHOD>
<ASSET_TAGS>
<ASSET_TAG><![CDATA[EC2]]></ASSET_TAG>
<ASSET_TAG><![CDATA[TG1]]></ASSET_TAG>
<ASSET_TAG><![CDATA[Virginiia]]></ASSET_TAG>
<ASSET_TAG><![CDATA[agec2]]></ASSET_TAG>
</ASSET_TAGS>
<DNS><![CDATA[ip-10-90-2-30.ec2.internal]]></DNS>
<EC2_INSTANCE_ID><![CDATA[i-0b11abd19771f17ed]]></EC2_INSTANCE_ID>
<EC2_INFO>
<PUBLIC_DNS_NAME><![CDATA[ec2-184-73-79-113.compute-1.amazonaws.com]]></PUBLIC_DNS_NAME>
<IMAGE_ID><![CDATA[ami-2d4ed53a]]></IMAGE_ID>
<VPC_ID><![CDATA[vpc-1e37cd76]]></VPC_ID>
<INSTANCE_STATE><![CDATA[RUNNING]]></INSTANCE_STATE>
<PRIVATE_DNS_NAME><![CDATA[ip-10-90-2-30.ec2.internal]]></PRIVATE_DNS_NAME>
<INSTANCE_TYPE><![CDATA[t2.medium]]></INSTANCE_TYPE>
</EC2_INFO>

DTD update:
https://<base_url>/asset_data_report.dtd

<!-- HOST_LIST -->
<!ELEMENT HOST_LIST (HOST+)>  

<!ELEMENT EC2_INSTANCE_ID (#PCDATA)>  
<!ELEMENT IP_INTERFACES (IP*)>  
<!ELEMENT EC2_INFO (PUBLIC_DNS_NAME?, IMAGE_ID?, VPC_ID?, INSTANCE_STATE?, PRIVATE_DNS_NAME?, INSTANCE_TYPE?)>  
<!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 OPERATING_SYSTEM (#PCDATA)>  
<!ELEMENT OS_CPE (#PCDATA)>  
<!ELEMENT ASSET_GROUPS (ASSET_GROUP_TITLE+)>  
<!ELEMENT VULN_INFO_LIST (VULN_INFO+)>

Qualys API Release Notes 38
EC2 Assets - Improved Reporting of private DNS host name and Instance ID

CSV format:
The EC2 Instance ID column will only appear in subscriptions with EC2 Scanning enabled and only when the “EC2 Related Information” option is selected in the report template. The columns for EC2 Instance ID and metadata information appear at the end.

"IP","Network","DNS","NetBIOS","QG Host ID","IP Interfaces","Tracking Method","OS","IP Status","QID","Title","Vuln Status","Type","Severity","Port","Protocol","FQDN","SSL","First Detected","Last Detected","Times Detected","Date Last Fixed","CVE ID","Vendor Reference","Bugtraq ID","Results","PCI Vuln","Ticket State","Instance","Category","Associated Tags","EC2 Instance ID","Public Hostname","Image ID","VFC ID","Instance State","Private Hostname","Instance Type"
"10.97.13.235","EC2-us-east-1-vpc90","i-0372d653f57cd04ae","","EC2","Amazon Linux","host scanned, found vuln","82054","TCP Sequence Number Approximation Based Denial of Service","Active","Vuln","2","05/11/2017 11:41:03","05/11/2017 13:47:22","4","CVE-2004-0230","Tested on port 80 with an injected SYN/RST offset by 16 bytes.#","no","TCP/IP","QCon1, agec2","i-0372d653f57cd04ae","ami-9be6f38c","vpc-2da7154b","RUNNING","t2.medium"

HTML, PDF and DOCX format: Previously on the host level, only ip, ec2 instance id & NetBIOS was shown, now we will include both private dns name too

Host List API v2 changes
New <EC2_INSTANCE_ID> tag is now shown right after DNS name. DNS name is the private DNS name for the EC2 asset. This tag only appears when EC2 Scanning is enabled for the subscription.

URL: <base_url>/api/2.0/fo/asset/host/?action=list
DTD: <base_url>/api/2.0/fo/asset/host/host_list_output.dtd
EC2 Assets - Improved Reporting of private DNS host name and Instance ID

**API Request:**

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

**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>2017-04-13T04:47:41Z</DATETIME>
    <HOST_LIST>
      <ID>132340</ID>
      <IP>10.90.2.175</IP>
      <TRACKING_METHOD>EC2</TRACKING_METHOD>
      <DNS><![CDATA[i-0b121b9211d7e25cb]]></DNS>
      <EC2_INSTANCE_ID><![CDATA[i-0b121b9211d7e25cb]]></EC2_INSTANCE_ID>
    </HOST>
    <HOST>
      <ID>132482</ID>
      <IP>10.90.2.202</IP>
      <TRACKING_METHOD>EC2</TRACKING_METHOD>
      <DNS><![CDATA[i-0ba79104d7023d4df]]></DNS>
      <EC2_INSTANCE_ID><![CDATA[i-0ba79104d7023d4df]]></EC2_INSTANCE_ID>
    </HOST>
  </HOST_LIST>
</RESPONSE>
</HOST_LIST_OUTPUT>

**DTD:**

```xml
<!ELEMENT HOST_LIST (HOST+)>  
<!ELEMENT HOST (ID, IP?, TRACKING_METHOD?, NETWORK_ID?,  
  DNS?, EC2_INSTANCE_ID?, NETBIOS?, OS?, QQ_HOSTID?, TAGS?,  
  METADATA?, LAST_VULN_SCAN_DATE?,  
  LAST_VM_BINARIES_SCAN_DATE?, LAST_VM_BINARIES_SCAN_DURATION?,  
  LAST_VM_AUTH_SCAN_DATE?,  
  LAST_VM_AUTH_SCAN_DURATION?,  
  LAST_COMPLIANCE_SCAN_DATE?, OWNER?, COMMENTS?,  
  USER_DEF?, ASSET_GROUP_IDS?)>

<!ELEMENT ID (#PCDATA)>  
<!ELEMENT IP (#PCDATA)>  
<!ELEMENT TRACKING_METHOD (#PCDATA)>  
<!ELEMENT NETWORK_ID (#PCDATA)>  
<!ELEMENT DNS (#PCDATA)>```
EC2 Assets - Improved Reporting of private DNS host name and Instance ID

<!ELEMENT EC2_INSTANCE_ID (#PCDATA)>

... 

Host Info API v1 changes

New <EC2_INSTANCE_ID> tag is now shown right after DNS name. DNS name is the private DNS name for the EC2 asset. This tag only appears when EC2 Scanning is enabled for the subscription.

URL: <base_url>/msp/get_host_info.php
DTD: <base_url>/get_host_info.dtd

API Request:

curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
"https://qualysapi.qualys.com/msp/get_host_info.php?host_ip=10.91.78.235&general_info=1&vuln_details=1"

XML output:

<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST SYSTEM "https://qualysapi.qualys.com/get_host_info.dtd">
<HOST>
  <TRACKING_METHOD>EC2</TRACKING_METHOD>
  <SECURITY_RISK>0</SECURITY_RISK>
  <IP>10.91.78.235</IP>
  <DNS><![CDATA[i-0299276e783120b15]]></DNS>
  <EC2_INSTANCE_ID><![CDATA[i-0299276e783120b15]]></EC2_INSTANCE_ID>
  <OPERATING_SYSTEM><![CDATA[]]></OPERATING_SYSTEM>
  <ASSET_GROUP_LIST>
    <ASSET_GROUP>
      <ASSET_GROUP_TITLE><![CDATA[agec2]]></ASSET_GROUP_TITLE>
      <CVSS_ENVIRONMENT>
        <CVSS_COLLATERAL_DAMAGE_POTENTIAL>Not</CVSS_COLLATERAL_DAMAGE_POTENTIAL>
      ... 
    </CVSS_ENVIRONMENT>
    </ASSET_GROUP>
  </ASSET_GROUP_LIST>
  ... 
</HOST>

DTD update:

<!-- QUALYS HOST INFO DTD -->
<!-- $Revision$ -->

VM Detection API changes

New <EC2_INSTANCE_ID> tag is now shown right after DNS name. DNS name is the private DNS name for the EC2 asset. This tag only appears when EC2 Scanning is enabled for the subscription and the “host_metadata=ec2” parameter is specified.

URL: <base_url>/api/2.0/fo/asset/host/vm/detection/?action=list
DTD: <base_url>/api/2.0/fo/asset/host/vm/detection/host_list_vm_detection_output.dtd

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&output_format=XML&truncation_limit=0&ips=10.97.5.247&show_results=0&host_metadata=ec2"

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_list_vm_detection_output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2016-11-14T11:21:02Z</DATETIME>
    <HOST_LIST>
      <HOST>
        <ID>135151</ID>
        <IP>10.97.5.247</IP>
        <TRACKING_METHOD>EC2</TRACKING_METHOD>
        <OS><![CDATA[Amazon Linux 2016.09]]></OS>
        <DNS><![CDATA[i-0bb87c3281243cfd]]></DNS>
        <EC2_INSTANCE_ID><![CDATA[i-0bb87c3281243cfd]]></EC2_INSTANCE_ID>
        <LAST_SCAN_DATETIME>2017-03-21T13:41:20Z</LAST_SCAN_DATETIME>
      </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
EC2 Assets - Improved Reporting of private DNS host name and Instance ID

<LAST_VM_SCANNED_DURATION>229</LAST_VM_SCANNED_DURATION>
<LAST_VM_AUTH_SCANNED_DATE>2017-03-21T13:39:38Z</LAST_VM_AUTH_SCANNED_DATE>
<LAST_VM_AUTH_SCANNED_DURATION>229</LAST_VM_AUTH_SCANNED_DURATION>
<LAST_PC_SCANNED_DATE>2017-03-21T13:21:51Z</LAST_PC_SCANNED_DATE>
<METADATA>
<EC2>
<ATTRIBUTE>
<NAME><![CDATA[latest/dynamic/instance-identity/document/region]]></NAME>
<LAST_STATUS>Success</LAST_STATUS>
<VALUE><![CDATA[us-east-1]]></VALUE>
<LAST_SUCCESS_DATE>2017-03-21T13:39:38Z</LAST_SUCCESS_DATE>
<LAST_ERROR_DATE></LAST_ERROR_DATE>
<LAST_ERROR><![CDATA[]]></LAST_ERROR>
</ATTRIBUTE>
</EC2>
</METADATA>
</HOST>
</HOST_LIST>
</RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>

DTD:
...
<!ELEMENT HOST_LIST (HOST+)>
<!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 EC2_INSTANCE_ID (#PCDATA)>
...
CSV format: The EC2InstanceID column only appears when EC2 Scanning is enabled for your subscription and the “host_metadata=ec2” parameter is specified in the API request. This new column appears after DNS Name.


Asset Search API v1 changes

New input parameter for EC2 Instance ID attribute. New <EC2_INSTANCE_ID> tag is now shown right after DNS name. DNS name is the private DNS name for the EC2 asset. This tag only appears when EC2 Scanning is enabled for the subscription.

URL: <base_url>/msp/asset_search.php
DTD: <base_url>/asset_search_report.dtd

API Request:
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"

XML output:
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ASSET_SEARCH_REPORT SYSTEM "https://qualysapi.qualys.com/asset_search_report.dtd">
...
EC2 Assets - Improved Reporting of private DNS host name and Instance ID

</HOST>
</HOST>

<IP>172.31.17.104</IP>

<TRACKING_METHOD>EC2</TRACKING_METHOD>

<DNS><![CDATA[ip-172-31-17-104.eu-central-1.compute.internal]]></DNS>

<EC2_INSTANCE_ID><![CDATA[i-33f1498e]]></EC2_INSTANCE_ID>

<OPERATING_SYSTEM><![CDATA[]]></OPERATING_SYSTEM>

<ASSET_GROUPS>
  <ASSET_GROUP_TITLE><![CDATA[All]]></ASSET_GROUP_TITLE>
</ASSET_GROUPS>

</HOST>
</HOST_LIST>
</ASSET_SEARCH_REPORT>

DTD update:

<!-- QUALYS ASSET SEARCH REPORT DTD -->

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

<!-- HOST_LIST -->

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

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

<!ELEMENT IP (#PCDATA)>
<!ATTLIST IP network_id CDATA #IMPLIED>
<!ELEMENT HOST_TAGS (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>

<!ELEMENT EC2_INSTANCE_ID (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT OPERATING_SYSTEM (#PCDATA)>
<!ELEMENT OS_CPE (#PCDATA)>
<!ELEMENT QID_LIST (QID+)>
<!ELEMENT QID (ID, RESULT?)>
<!ELEMENT ID (#PCDATA)>
### Asset Search API v2 changes

New input parameter for EC2 Instance ID attribute. New `<EC2_INSTANCE_ID>` tag is now shown right after DNS name. DNS name is the private DNS name for the EC2 asset. This tag only appears when EC2 Scanning is enabled for the subscription.

URL: `<base_url>/api/2.0/fo/report/asset`

DTD: `<base_url>/asset_search_report_v2.dtd`

### API Request:

```bash
```

### XML output:

```xml
<?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-test]]></COMPANY>
<USERNAME>sada-customer customer</USERNAME>
<GENERATION_DATETIME>2017-04-07T10:27:21Z</GENERATION_DATETIME>
...
<HOST_LIST>
<HOST>
<IP><![CDATA[172.31.17.104]]></IP>
<TRACKING_METHOD>EC2</TRACKING_METHOD>
<DNS><![CDATA[ip-172-31-17-104.eu-central-1.compute.internal]]></DNS>
<EC2_INSTANCE_ID><![CDATA[i-33f1498e]]></EC2_INSTANCE_ID>
<LAST_SCAN_DATE />
<FIRST_FOUND_DATE />
</HOST>
<HOST>
<IP><![CDATA[172.31.47.228]]></IP>
<TRACKING_METHOD>EC2</TRACKING_METHOD>
<DNS><![CDATA[ip-172-31-47-228.us-east-2.compute.internal]]></DNS>
<EC2_INSTANCE_ID><![CDATA[i-0eda274d4c0bef4fa]]></EC2_INSTANCE_ID>
<LAST_SCAN_DATE />
<FIRST_FOUND_DATE />
</HOST>
</HOST_LIST>
</ASSET_SEARCH_REPORT>
```
EC2 Assets - Improved Reporting of private DNS host name and Instance ID

**DTD update:**

```xml
<!-- QUALYS ASSET SEARCH REPORT DTD -->

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

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

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

<!ELEMENT IP (#PCDATA)>
<!ATTLIST IP network_id CDATA #IMPLIED>
<!ELEMENT HOST_TAGS (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT EC2_INSTANCE_ID (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT OPERATING_SYSTEM (#PCDATA)>
<!ELEMENT OS_CPE (#PCDATA)>
<!ELEMENT QID_LIST (QID+)>
<!ELEMENT QID (ID, RESULT?)>
<!ELEMENT ID (#PCDATA)>

**CSV format:** The EC2InstanceID column only appears when EC2 Scanning is enabled for your subscription. This new column appears at the end.

"IP", "DNSHostname", "NetBIOSHostname", "OperatingSystem", "OSCPE", "Port/Service/Default Service", "TrackingMethod", "LastScanDate", "LastComplianceScanDate", "First Found", "Tags", "EC2InstanceID"

"172.31.17.104", "ip-172-31-17-104.eu-central-1.compute.internal", ",,", "EC2", 

"172.31.47.228", "ip-172-31-47-228.us-east-2.compute.internal", "i-0eda274d4c0bef4fa", ",,", "EC2", 
"i-33f1498e"
Manage assets using EC2 metadata

Search and return EC2 metadata

The following APIs can now fetch EC2 metadata. You can then search for (manage) assets using the EC2 metadata.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host_metadata={value}</td>
<td>Specify the name of the cloud provider, i.e., EC2.</td>
</tr>
<tr>
<td>host_metadata_fields={value1, value2}</td>
<td>Specify the EC2 instance fields to fetch the data for. Data can be fetched for any of the following fields:</td>
</tr>
<tr>
<td></td>
<td>- accountId</td>
</tr>
<tr>
<td></td>
<td>- region</td>
</tr>
<tr>
<td></td>
<td>- availabilityZone</td>
</tr>
<tr>
<td></td>
<td>- instanceId</td>
</tr>
<tr>
<td></td>
<td>- instanceType</td>
</tr>
<tr>
<td></td>
<td>- imageId</td>
</tr>
<tr>
<td></td>
<td>- kernelId</td>
</tr>
<tr>
<td></td>
<td>Multiple field names are comma separated.</td>
</tr>
</tbody>
</table>

Host List API example: fetch region, accountId, and instanceId info for EC2 assets

API request:

curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=list&details=All&host_metadata=ec2&host_metadata_fields=region,accountId,instanceId" "https://qualysapi.qualys.com/api/2.0/fo/asset/host/"

XML output:

```xml
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM "https://qualysapi.qualys.com/api/2.0/fo/asset/host/host_list_output.dtd" >

<HOST_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2016-11-15T09:50:46Z</DATETIME>
    <HOST_LIST>
      <HOST>
        <ID>135151</ID>
      </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_OUTPUT>
```
Manage assets using EC2 metadata

<IP>10.97.5.247</IP>
<TRACKING_METHOD>EC2</TRACKING_METHOD>
<DNS><![CDATA[i-0bb87c3281243cfd]]></DNS>
<EC2_INSTANCE_ID><![CDATA[i-0bb87c3281243cfd]]></EC2_INSTANCE_ID>
<OS> <![CDATA[Amazon Linux 2016.09]]></OS>
<METADATA>
<EC2>
<ATTRIBUTE>
  <NAME><![CDATA[latest/dynamic/instance-identity/document/region]]></NAME>
  <LAST_STATUS>Success</LAST_STATUS>
  <VALUE><![CDATA[us-east-1]]></VALUE>
  <LAST_SUCCESS_DATE>2017-03-21T13:39:38Z</LAST_SUCCESS_DATE>
  <LAST_ERROR_DATE></LAST_ERROR_DATE>
  <LAST_ERROR><![CDATA[[]]]></LAST_ERROR>
</ATTRIBUTE>
<ATTRIBUTE>
  <NAME><![CDATA[latest/dynamic/instance-identity/document/instanceId]]></NAME>
  <LAST_STATUS>Success</LAST_STATUS>
  <VALUE><![CDATA[i-0bb87c3281243cfd]]></VALUE>
  <LAST_SUCCESS_DATE>2017-03-21T13:39:38Z</LAST_SUCCESS_DATE>
  <LAST_ERROR_DATE></LAST_ERROR_DATE>
  <LAST_ERROR><![CDATA[[]]]></LAST_ERROR>
</ATTRIBUTE>
<ATTRIBUTE>
  <NAME><![CDATA[latest/dynamic/instance-identity/document/accountId]]></NAME>
  <LAST_STATUS>Success</LAST_STATUS>
  <VALUE><![CDATA[205767712438]]></VALUE>
  <LAST_SUCCESS_DATE>2017-03-21T13:39:38Z</LAST_SUCCESS_DATE>
  <LAST_ERROR_DATE></LAST_ERROR_DATE>
  <LAST_ERROR><![CDATA[[]]]></LAST_ERROR>
</ATTRIBUTE>
</EC2>
</METADATA>
<LAST_VULN_SCAN_DATETIME>2017-03-21T13:39:38Z</LAST_VULN_SCAN_DATETIME>
<LAST_VM_SCANNED_DATE>2017-03-21T13:39:38Z</LAST_VM_SCANNED_DATE>
<LAST_VM_SCANNED_DURATION>229</LAST_VM_SCANNED_DURATION>
<LAST_VM_AUTH_SCANNED_DATE>2017-03-21T13:39:38Z</LAST_VM_AUTH_SCANNED_DATE>
<LAST_VM_AUTH_SCANNED_DURATION>229</LAST_VM_AUTH_SCANNED_DURATION>
<LAST_COMPLIANCE_SCAN_DATETIME>2017-03-21T13:21:51Z</LAST_COMPLIANCE_SCAN_DATETIME>
</HOST>
</HOST_LIST>
</RESPONSE>
Manage assets using EC2 metadata

**DTD update:**

https://<base_url>/api/2.0/fo/asset/host/host_list_output.dtd

```
<!ELEMENT HOST (ID, IP?, TRACKING_METHOD?, NETWORK_ID?,
  DNS?, 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?, OWNER?, COMMENTS?,
  USER_DEF?, ASSET_GROUP_IDS?)>
```

```
<!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 ASSET_GROUP_IDS (#PCDATA)>
```

**Host List Detection API example: fetch region info for EC2 assets**

**API request:**

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/?action=list&host_metadata=ec2&host_metadata_fields=region"
```

**XML output:**

```
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/host_list_vm_detection_output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2016-11-14T11:21:02Z</DATETIME>
    <HOST_LIST>
      <HOST>
```
Manage assets using EC2 metadata

```xml
<ID>135151</ID>
<IP>10.97.5.247</IP>
<TRACKING_METHOD>EC2</TRACKING_METHOD>
<OS><![CDATA[Amazon Linux 2016.09]]></OS>
<DNS><![CDATA[i-0bb87c3281243cdff]]></DNS>
<EC2_INSTANCE_ID><![CDATA[i-0bb87c3281243cdff]]></EC2_INSTANCE_ID>
<LAST_SCAN_DATETIME>2017-03-21T13:41:20Z</LAST_SCAN_DATETIME>
<LAST_VM_SCANNED_DATE>2017-03-21T13:39:38Z</LAST_VM_SCANNED_DATE>
<LAST_VM_SCANNED_DURATION>229</LAST_VM_SCANNED_DURATION>
<LAST_VM_AUTH_SCANNED_DATE>2017-03-21T13:39:38Z</LAST_VM_AUTH_SCANNED_DATE>
<LAST_VM_AUTH_SCANNED_DURATION>229</LAST_VM_AUTH_SCANNED_DURATION>
<LAST_PC_SCANNED_DATE>2017-03-21T13:21:51Z</LAST_PC_SCANNED_DATE>
<METADATA>
</EC2>
</HOST>
</HOST_LIST>
</RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>

DTD:

https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/host_list_vm_detection_output.dtd

...
Manage assets using EC2 metadata

<!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 DETECTION_LIST (DETECTION+)>
...

Now when you perform an IP update that results in a Warning about duplicate hosts, we’ll use the new Duplicate Hosts Error Output DTD (duplicate_hosts_error_output.dtd) instead of the Command List Output DTD (command_list_output.dtd).

**API request:**
```
```

**XML output:**
```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE DUPLICATE_HOSTS_ERROR_OUTPUT SYSTEM "https://qualysapi.qualys.com/api/2.0/fo/asset/ip/duplicate_hosts_error.dtd">
<DUPLICATE_HOSTS_ERROR_OUTPUT>
  <RESPONSE>
    <CODE>1982</CODE>
    <DATETIME>2017-03-16T04:54:15Z</DATETIME>
    <WARNING>
      <TEXT>You cannot change the tracking method for the following host using the API since there are multiple scan data entries. This can happen when the host is resolved to different hostnames in different scan tasks. You'll need to change the tracking method using the UI. Use the URL to log into your account, edit the host and select another tracking method. At the prompt click Apply to save the most recent scan data and purge the other scan data.</TEXT>
      <DUPLICATE_HOSTS>
        <DUPLICATE_HOST>
          <IP>10.10.25.224</IP>
          <DNS_HOSTNAME>ora10105-win-25-224.qualys.com</DNS_HOSTNAME>
          <NETBIOS_HOSTNAME>ORA10105-WIN-25</NETBIOS_HOSTNAME>
          <LAST_SCANDATE>09/09/2016 at 13:35:29 (GMT)</LAST_SCANDATE>
          <TRACKING>DNS</TRACKING>
        </DUPLICATE_HOST>
      </DUPLICATE_HOSTS>
      <URL><![CDATA[https://qualysguard.qualys.com/fo/tools/ip_assets.php]]></URL>
    </WARNING>
  </RESPONSE>
</DUPLICATE_HOSTS_ERROR_OUTPUT>
```
New DTD:

<!-- QUALYS DUPLICATE_HOSTS_ERROR_OUTPUT DTD -->

<!ELEMENT DUPLICATE_HOSTS_ERROR_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)>
<!ELEMENT POST_DATA (#PCDATA)>

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

<!ELEMENT RESPONSE (CODE?, DATETIME, WARNING?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT WARNING (TEXT, DUPLICATE_HOSTS, URL)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!ELEMENT DUPLICATE_HOSTS (DUPLICATE_HOST*)>

<!ELEMENT DUPLICATE_HOST (IP, DNS_HOSTNAME, NETBIOS_HOSTNAME, LAST_SCANDATE, TRACKING)>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT DNS_HOSTNAME (#PCDATA)>
<!ELEMENT NETBIOS_HOSTNAME (#PCDATA)>
<!ELEMENT LAST_SCANDATE (#PCDATA)>
<!ELEMENT TRACKING (#PCDATA)>

<!-- EOF -->

Updated DTD:

We removed CODE and WARNING from the RESPONSE element in the Command List Output DTD (command_list_output.dtd).

<!-- QUALYS COMMAND_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT COMMAND_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)>
<!ELEMENT POST_DATA (#PCDATA)>
<!ELEMENT COMMAND_LIST_OUTPUT (REQUEST?, RESPONSE)>
IP Update - New DTD for Duplicate Hosts Error

<!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, COMMAND_LIST?)>  
<!ELEMENT COMMAND_LIST (COMMAND+, COMMAND_OUTPUT+)>

<!ELEMENT COMMAND (ID, STATUS, OPERATION, FRIENDLY_NAME, LAUNCH_DATE, LAST_UPDATED_DATE)>  
<!ELEMENT ID (#PCDATA)>  
<!ELEMENT STATUS (#PCDATA)>  
<!ELEMENT OPERATION (DESCRIPTION, STATUS)>  
<!ELEMENT FRIENDLY_NAME (#PCDATA)>  
<!ELEMENT LAUNCH_DATE (#PCDATA)>  
<!ELEMENT LAST_UPDATED_DATE (#PCDATA)>  
<!ELEMENT DESCRIPTION (#PCDATA)>  

<!ELEMENT COMMAND_OUTPUT (ID, STDIN?, STDOUT?, STDERR?)>  
<!ELEMENT STDIN (#PCDATA)>  
<!ELEMENT STDOUT (#PCDATA)>  
<!ELEMENT STDERR (#PCDATA)>  

<!-- EOF -->
Export user activity log for a subscription

A new API /api/2.0/fo/activity_log/ is introduced to export the user activity log for a subscription to CSV format.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action=list</td>
<td>(Required) The action required for the API request: list. The POST or GET method can be used.</td>
</tr>
<tr>
<td>user_action=[value]</td>
<td>(Optional) The actions included in the output depends on your user role. For example, user login or logout. Managers see all actions taken by all users. Unit Managers see actions taken by users in their business unit. Scanners and Readers see their own actions only.</td>
</tr>
<tr>
<td>action_details=[value]</td>
<td>(Optional) User action details for example, user_logged in or user_logged out.</td>
</tr>
<tr>
<td>username=[value]</td>
<td>(Optional) The name of the user who performed the action. Usernames are included only if you are a Manager or a Unit Manager. A Unit Manager can see usernames only for users in the Unit Manager’s hierarchy.</td>
</tr>
<tr>
<td>user_role=[value]</td>
<td>(Optional) The role of the user who performed the action. Logs are exported for any of the following user roles: - Manager - Unit Manager - Auditor - Scanner - Reader - KnowledgeBase Only - Remediation User - Contact User roles are included only if you are a Manager or a Unit Manager. A Unit Manager can see user roles only for users in the Unit Manager’s hierarchy.</td>
</tr>
<tr>
<td>since_datetime=[value]</td>
<td>(Optional) Specify the date to include the activity log starting from that point in time. Date must be in the format YYYY-MM-DD HH:mm:ss, and must be less than or equal to today’s date.</td>
</tr>
<tr>
<td>until_datetime=[value]</td>
<td>(Optional) Specify the date to include the activity log until a specific point in time. Date must be in the format YYYY-MM-DD HH:mm:ss, and must be more than or equal to since_datetime, and less than or equal to today’s date.</td>
</tr>
</tbody>
</table>
Export user activity log for a subscription

API request:

```
curl -u "username:password" -k -H "X-Requested-With:curl"
"https://qualysapi.qualys.com/api/2.0/fo/activity_log/?action=list"
```

The activity log gets exported in CSV format.

Sample CSV output:

```
"Date","Action","Module","Details","User Name","User Role","User IP"
"2017-02-03T04:35:38Z","login","auth","user_logged in","saand_rn","Manager","10.113.195.136"
"2017-02-02T13:58:16Z","login","auth","user_logged in","saand_rn","Manager","10.113.195.136"
"2017-02-02T13:48:07Z","request","auth","API:/api/2.0/fo/activity_log/index.php","saand_rn","Manager","10.113.195.136"
"2017-02-02T13:31:19Z","set","host_attribute","comment=[vvv] for 11.11.11.4","saand_rn","Manager","10.113.195.136"
```

Parameter | Description
---|---
output_format=CSV | (Optional) CSV (default)
truncation_limit=[value] | (Optional) Limit the number of log records to include in the CSV output.
Action Log API V1 - added User Details in Output

We're providing more user details in the output of the Action Log API V1 (/msp/action_log_report.php). For create user, update user and change primary contact actions, the details will now include the user role and user login for the user account that changed. There are no DTD updates.

User details appear in this format:

firstname lastname (user role: user login)

Example

API request:

```bash
curl -u "USERNAME:PASSWORD" -k -H "X-Requested-With: Curl"
```

XML output:

This example shows details for the following actions: new account created, account updated, and primary contact changed.

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ACTION_LOG_REPORT SYSTEM "https://qualysapi.qualys.com/action_log_report.dtd">
<ACTION_LOG_REPORT>
  <DATE_FROM>2017-04-03T00:00:00Z</DATE_FROM>
  <DATE_TO>2017-04-04T08:34:11Z</DATE_TO>
  <ACTION_LOG_LIST>
    <ACTION_LOG>
      <DATE>2017-04-04T08:09:53Z</DATE>
      <MODULE><![CDATA[auth]]></MODULE>
      <ACTION>login</ACTION>
      <DETAILS><![CDATA[user_logged in]]></DETAILS>
      <USER>
        <USER_LOGIN>qualys_sv19</USER_LOGIN>
        <FIRSTNAME><![CDATA[Suzy]]></FIRSTNAME>
        <LASTNAME><![CDATA[Van Pelt]]></LASTNAME>
        <ROLE>Manager</ROLE>
      </USER>
      <IP>10.10.193.20</IP>
    </ACTION_LOG>
    <ACTION_LOG>
      <DATE>2017-04-04T08:24:21Z</DATE>
      <MODULE><![CDATA[account]]></MODULE>
      <ACTION>create</ACTION>
    </ACTION_LOG>
  </ACTION_LOG_LIST>
</ACTION_LOG_REPORT>
```
<DETAILS><![CDATA[User Patrick Slimmer (Manager: qualys_ps21) created by Suzy Van Pelt (Manager: qualys_sv19)]></DETAILS>

<User>
  <USER_LOGIN>qualys_sv19</USER_LOGIN>
  <FIRSTNAME><![CDATA[Suzy]]></FIRSTNAME>
  <LASTNAME><![CDATA[Van Pelt]]></LASTNAME>
  <ROLE>Manager</ROLE>
</User>

<IP>10.10.193.10</IP>

</ACTION_LOG>

<ACTION_LOG>
  <DATE>2017-04-04T08:45Z</DATE>
  <MODULE><![CDATA[account]]></MODULE>
  <ACTION>update</ACTION>
  <DETAILS><![CDATA[user Daniel Fedasz (Reader: qualys_df20) updated by Suzy Van Pelt (Manager: qualys_sv19): user_role set from 'Scanner' to 'Reader', Create option profiles disabled, Transfer Asset Groups enabled, Transfer personal configurations enabled, Asset groups set from 'none' to 'none']></DETAILS>

<User>
  <USER_LOGIN>qualys_sv19</USER_LOGIN>
  <FIRSTNAME><![CDATA[Suzy]]></FIRSTNAME>
  <LASTNAME><![CDATA[Van Pelt]]></LASTNAME>
  <ROLE>Manager</ROLE>
</User>

<IP>10.10.193.10</IP>

</ACTION_LOG>

<ACTION_LOG>
  <DATE>2017-04-04T08:26:01Z</DATE>
  <MODULE><![CDATA[primary_contact]]></MODULE>
  <ACTION>save</ACTION>
  <DETAILS><![CDATA[Primary contact for the subscription is changed from Suzy Van Pelt (Manager: qualys_sv19) to Patrick Slimmer (Manager: qualys_ps21)]></DETAILS>

<User>
  <USER_LOGIN>qualys_sv19</USER_LOGIN>
  <FIRSTNAME><![CDATA[Suzy]]></FIRSTNAME>
  <LASTNAME><![CDATA[Van Pelt]]></LASTNAME>
  <ROLE>Manager</ROLE>
</User>

<IP>10.10.193.9</IP>

</ACTION_LOG>

</ACTION_LOG_LIST>

</ACTION_LOG_REPORT>
Asset Search APIs - Search by EC2 Instance Status, ID

We’ve added new input parameters to the Asset Search APIs to allow users to easily find their Amazon EC2 assets with a particular instance status (running, terminated, stopped, etc) or instance ID. For example, you can find EC2 instances that are terminated in order to purge or remove them from your account.

These APIs were updated:
Asset Search API v1 (/msp/asset_search.php)
Asset Search API v2 (/api/2.0/fo/report/asset/)

Asset Search API v1

New Input Parameters

Use these new parameters to search for assets based on EC2 instance status or ID.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ec2_instance_status={value}</td>
<td>(Optional) Specify the EC2 instance status to be searched. Possible values: RUNNING, TERMINATED, PENDING, STOPPING, SHUTTING_DOWN, STOPPED. Values are case-sensitive.</td>
</tr>
<tr>
<td>ec2_instance_id={value}</td>
<td>(Optional) Specify the EC2 instance ID to be searched. Enter the value in this format: MODIFIER:ID where MODIFIER is one of these values: begin, match, contain, end. For example: ec2_instance_id=contain:i-0299276e783120b15</td>
</tr>
</tbody>
</table>

Examples

Sample 1 - Search EC2 hosts with EC2 instance ID i-0299276e783120b15

API request:

curl -u "USERNAME:PASSWORD" -k -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/msp/asset_search.php?target_asset_groups=ag ec2&ec2_instance_id=contain:i-0299276e783120b15"

XML output:

<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ASSET_SEARCH_REPORT SYSTEM "https://qualysapi.qualys.com/asset_search_report.dtd">
<ASSET_SEARCH_REPORT>
Asset Search APIs - Search by EC2 Instance Status, ID

Sample 2 - Search all EC2 hosts which are currently in RUNNING state and having instance ID i-0299276e783120b15

API request:

curl -u "USERNAME:PASSWORD" -k -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/msp/asset_search.php?target_asset_groups=agec2&ec2_instance_status=RUNNING&ec2_instance_id=contain:i-0299276e783120b15"

XML output:

<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ASSET_SEARCH_REPORT SYSTEM
"https://qualysapi.qualys.com/asset_search_report.dtd">

<ASSET_SEARCH_REPORT>

<HEADER>

<COMPANY><![CDATA[qualys-test]]></COMPANY>
<USERNAME>quays_sc2</USERNAME>
<GENERATION_DATETIME>2017-04-11T10:08:53Z</GENERATION_DATETIME>

<FILTERS>

<ASSET_GROUPS>

<ASSET_GROUP_TITLE><![CDATA[agec2]]></ASSET_GROUP_TITLE>
</ASSET_GROUPS>

<FILTER_EC2_INSTANCE_ID criterion="contain"><![CDATA[i-0299276e783120b15]]></FILTER_EC2_INSTANCE_ID>

<EC2_INSTANCE_STATUS>RUNNING</EC2_INSTANCE_STATUS>
</FILTERS>
</HEADER>

<!-- 1.0% done - Searching Database... -->

<HOST_LIST>

<HOST>

<IP>10.91.78.235</IP>

<TRACKING_METHOD>EC2</TRACKING_METHOD>

<DNS><![CDATA[i-0299276e783120b15]]></DNS>

<EC2_INSTANCE_ID><![CDATA[i-0299276e783120b15]]></EC2_INSTANCE_ID>

<OPERATING_SYSTEM><![CDATA[]]></OPERATING_SYSTEM>

<ASSET_GROUPS>

<ASSET_GROUP_TITLE><![CDATA[All]]></ASSET_GROUP_TITLE>

<ASSET_GROUP_TITLE><![CDATA[agec2]]></ASSET_GROUP_TITLE>
</ASSET_GROUPS>

</HOST>

</HOST_LIST>

</ASSET_SEARCH_REPORT>
Asset Search API v2

New Input Parameters

Use these new parameters to search for assets based on EC2 instance status or ID.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ec2_instance_status=</td>
<td>(Optional) Specify the EC2 instance status to be searched. Possible values:</td>
</tr>
<tr>
<td>[value]</td>
<td>RUNNING, TERMINATED, PENDING, STOPPING, SHUTTING_DOWN, STOPPED. Values are</td>
</tr>
<tr>
<td></td>
<td>case-sensitive.</td>
</tr>
<tr>
<td>ec2_instance_id=</td>
<td>(Optional) Specify the EC2 instance ID to be searched.</td>
</tr>
<tr>
<td>[value]</td>
<td></td>
</tr>
<tr>
<td>ec2_instance_id_mod</td>
<td>(Optional) Show only hosts with ec2_instance_id that is either: beginning</td>
</tr>
<tr>
<td>ifier=[value]</td>
<td>with, containing, matching, ending with, not empty.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ec2_instance_id is valid only when ec2_instance_id_modifier is specified</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ec2_instance_id_modifier is valid only when ec2_instance_id is specified</td>
</tr>
</tbody>
</table>
Examples

Sample 1 - Search EC2 host with EC2 instance ID i-0fb7086f985856fa4

API request:

curl -u "USERNAME:PASSWORD" -k -H "X-Requested-With: Curl" -d "action=search&output_format=xml&tracking_method=EC2&use_tags=1&tag_set_by=name&tag_set_include=useasttag&ec2_instance_id=i-0fb7086f985856fa4&ec2_instance_id_modifier=containing" "https://qualysapi.qualys.com/api/2.0/fo/report/asset/

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-test]]></COMPANY>
    <USERNAME>qualys_ps</USERNAME>
    <GENERATION_DATETIME>2017-04-11T10:17:32Z</GENERATION_DATETIME>
    <TOTAL>1</TOTAL>
    <FILTERS>
      <ASSET_TAGS>
        <INCLUDED_TAGS scope="any">
          <ASSET_TAG><![CDATA[useasttag]]></ASSET_TAG>
        </INCLUDED_TAGS>
      </ASSET_TAGS>
      <TRACKING_METHOD><![CDATA[EC2]]></TRACKING_METHOD>
    </FILTERS>
  </HEADER>

  <HOST_LIST>
    <HOST>
      <IP>![CDATA[10.73.188.6]]></IP>
      <HOST_TAGS>![CDATA[EC2, Virginia, agec2, sada-0117-targets, sada-new-0308, useasttag;]]></HOST_TAGS>
      <TRACKING_METHOD>EC2</TRACKING_METHOD>
      <DNS>![CDATA[ip-10-73-188-6.ec2.internal]]></DNS>
      <EC2_INSTANCE_ID>![CDATA[i-0fb7086f985856fa4]]></EC2_INSTANCE_ID>
    </HOST>

  </HOST_LIST>
Sample 2 - Search all EC2 hosts which are currently in TERMINATED state and having instance ID i-0b121b9211d7e25cb

**API request:**

curl -u "USERNAME:PASSWORD" -k -H "X-Requested-With: Curl" -d "action=search&output_format=xml&tracking_method=EC2&use_tags=1&tag_set_by=name&tag_set_include=useasttag&ec2_instance_status=TERMINATED&ec2_instance_id=i-0b121b9211d7e25cb&ec2_instance_id_modifier=containing" "https://qualysapi.qualys.com/api/2.0/fo/report/asset/"

**XML output:**

```xml
<?xml version='1.0' encoding='UTF-8' ?>
<ASSET_SEARCH_REPORT SYSTEM "https://qualysapi.qualys.com/asset_search_report_v2.dtd">
<HEADER>
  <COMPANY>![CDATA[qualys-test]]></COMPANY>
  <USERNAME>sada-customer customer</USERNAME>
  <GENERATION_DATETIME>2017-04-11T10:49:05Z</GENERATION_DATETIME>
  <TOTAL>1</TOTAL>
  <FILTERS>
    <ASSET_TAGS>
      <INCLUDED_TAGS scope="any"/>
      <ASSET_TAG>![CDATA[useasttag]]></ASSET_TAG>
    </INCLUDED_TAGS>
    <ASSET_TAGS>
    </ASSET_TAGS>
    <TRACKING_METHOD>![CDATA[EC2]]></TRACKING_METHOD>
  </FILTERS>
</HEADER>

<HOST_LIST>
  <HOST>
    <IP>![CDATA[10.90.2.175]]></IP>
    <HOST_TAGS>![CDATA[EC2, Vriginia, por-6586, sada-0117-targets, sada-new-0308, useasttag;]]></HOST_TAGS>
    <TRACKING_METHOD>EC2</TRACKING_METHOD>
    <DNS>![CDATA[i-0b121b9211d7e25cb]]></DNS>
    <EC2_INSTANCE_ID>![CDATA[i-0b121b9211d7e25cb]]></EC2_INSTANCE_ID>
    <LAST_SCAN_DATE />
    <FIRST_FOUND_DATE />
  </HOST>
</HOST_LIST>
```
VM - New API Support for Report Templates

You can now use APIs to create custom reports with views on your scan results and the current vulnerabilities on your hosts. Use various report templates provided by Qualys as a starting point.

APIs are now available to perform various actions on templates for the following report types: Scan Template, PCI Scan Template, Patch Template, Map Template

The Report Template API allows users to perform the following actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Supported Access Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create</td>
<td>POST</td>
<td>Create a report template. A unique template ID is generated for the new template.</td>
</tr>
<tr>
<td>Update</td>
<td>PUT</td>
<td>Update an existing report template.</td>
</tr>
<tr>
<td>Delete</td>
<td>POST</td>
<td>Delete an existing report template.</td>
</tr>
<tr>
<td>Export</td>
<td>GET</td>
<td>Export a specific report template based on the template ID, or all templates for the report type.</td>
</tr>
</tbody>
</table>

Once you have your template the way you want you can run reports using the templates using the Report API /api/2.0/fo/report. For details and examples, see Qualys API V2 User Guide.

Scan Template API

The API /api/2.0/fo/report/template/scan/ allows you to perform actions such as create, update, delete and export on the Scan Template.

Scan Template Request

A summary of API Endpoint URLs is provided below.

<table>
<thead>
<tr>
<th>Action</th>
<th>API Endpoint /required parameters</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Scan Template</td>
<td>&lt;base_url&gt;/api/2.0/fo/report/template/scan/</td>
<td>POST</td>
</tr>
<tr>
<td></td>
<td>Required parameters:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>action=create</td>
<td></td>
</tr>
<tr>
<td></td>
<td>report_format=xml</td>
<td></td>
</tr>
<tr>
<td>Update Scan Template</td>
<td>&lt;base_url&gt;/api/2.0/fo/report/template/scan/</td>
<td>PUT</td>
</tr>
<tr>
<td></td>
<td>Required parameters:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>template_id=[value]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>action=update</td>
<td></td>
</tr>
<tr>
<td></td>
<td>report_format=xml</td>
<td></td>
</tr>
</tbody>
</table>
Scan Template settings

These parameters (all are optional) are used for a create or update request to define scan
template settings. When creating a new template the default value is shown in bold
where applicable.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Title</strong></td>
<td>The template title and owner.</td>
</tr>
<tr>
<td>title={value}</td>
<td>A string value for the title. Length is maximum 64 characters.</td>
</tr>
<tr>
<td>owner={value}</td>
<td>Username of the owner of this template.</td>
</tr>
<tr>
<td></td>
<td>Validity of the owner to create reports is based on the user role</td>
</tr>
<tr>
<td></td>
<td>or business unit.</td>
</tr>
<tr>
<td></td>
<td>See About template owner.</td>
</tr>
<tr>
<td><strong>Target</strong></td>
<td>What target assets to include in the report.</td>
</tr>
<tr>
<td>scan_selection={HostBased</td>
<td>ScanBased</td>
</tr>
<tr>
<td>include_trending={0</td>
<td>1 }</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>limit_timeframe=0</td>
<td>1]</td>
</tr>
<tr>
<td>selection_type=[day</td>
<td>month</td>
</tr>
<tr>
<td>selection_range=[value]</td>
<td>Specify the range for the selection type. Specify a number of units (1</td>
</tr>
<tr>
<td>asset_groups=[value]</td>
<td>Specify the name of the asset group(s) to report on. Multiple asset groups are comma separated. We'll report on all the IPs in the asset groups. This parameter is required only if scan_selection=HostBased.</td>
</tr>
<tr>
<td>asset_group_ids=[value]</td>
<td>Specify the ID of the asset group(s) to report on. Multiple asset group IDs are comma separated. We'll report on all the IPs in the asset groups. This parameter is required only if scan_selection=HostBased.</td>
</tr>
<tr>
<td>network=[value]</td>
<td>(Valid only when the Networks feature is enabled for your account.) A network name containing the IPs to include. For a new template the default network is Global Default Network.</td>
</tr>
<tr>
<td>ips=[value]xml</td>
<td>Specify the IPs or IP ranges to report on. Multiple IPs or IP ranges are comma separated. This parameter is required only if scan_selection=HostBased.</td>
</tr>
<tr>
<td>tag_set_by=[name</td>
<td>id]</td>
</tr>
<tr>
<td>tag_include_selector= [ALL</td>
<td>ANY]</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>tag_set_include={value}</td>
<td>Specify asset tags for the hosts you want to report on. We’ll find the hosts in your account that match your tag selection and include them in the report. Multiple tags can be provided using comma separated values. This parameter is required only if scan_selection=HostBased.</td>
</tr>
<tr>
<td>tag_exclude_selector={ALL</td>
<td>ANY}</td>
</tr>
<tr>
<td>tag_set_exclude={value}</td>
<td>Specify asset tags for the hosts you do not want to report on. We’ll find the hosts in your account that match your tag selection and exclude them from the report. Multiple tags can be provided using comma separated values. This parameter is required only if scan_selection=HostBased.</td>
</tr>
<tr>
<td>host_with_cloud_agents={all</td>
<td>scan</td>
</tr>
<tr>
<td>display_text_summary={0</td>
<td>1}</td>
</tr>
<tr>
<td>graph_business_risk={0</td>
<td>1}</td>
</tr>
<tr>
<td>graph_vuln_over_time={0</td>
<td>1}</td>
</tr>
<tr>
<td>graph_status={0</td>
<td>1}</td>
</tr>
<tr>
<td>graph_potential_status={0</td>
<td>1}</td>
</tr>
<tr>
<td>graph_severity={0</td>
<td>1}</td>
</tr>
<tr>
<td>Display</td>
<td>Display options such as graphs amount of detail.</td>
</tr>
<tr>
<td>graph_potential_severity={0</td>
<td>1}</td>
</tr>
<tr>
<td>graph_ig_severity={0</td>
<td>1}</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>graph_top_categories=[0</td>
<td>1]</td>
</tr>
<tr>
<td>graph_top_vulns=[0</td>
<td>1]</td>
</tr>
<tr>
<td>graph_os=[0</td>
<td>1]</td>
</tr>
<tr>
<td>graph_services=[0</td>
<td>1]</td>
</tr>
<tr>
<td>graph_top_ports=[0</td>
<td>1]</td>
</tr>
<tr>
<td>display_custom_footer=[0</td>
<td>1]</td>
</tr>
<tr>
<td>display_custom_footer_text={value}</td>
<td>Specify custom text like a disclosure statement or data classification (e.g. Public, Confidential). The text you enter will appear in all reports generated from this template, except reports in XML and CSV formats. Length is maximum 4000 characters.</td>
</tr>
<tr>
<td>sort_by=</td>
<td>host</td>
</tr>
<tr>
<td>cvss=[all</td>
<td>cvssv2</td>
</tr>
<tr>
<td>host_details=[0</td>
<td>1]</td>
</tr>
<tr>
<td>metadata_ec2_instances=[0</td>
<td>1]</td>
</tr>
<tr>
<td>include_text_summary=[0</td>
<td>1]</td>
</tr>
<tr>
<td>include_vuln_details=[0</td>
<td>1]</td>
</tr>
<tr>
<td>include_vuln_details_threat=[0</td>
<td>1]</td>
</tr>
<tr>
<td>include_vuln_details_impact=[0</td>
<td>1]</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>include_vuln_details_solution</td>
<td>Specify 1 to include a verified solution to remedy the issue, such as a link to the vendor’s patch, Web site, or a workaround.</td>
</tr>
<tr>
<td>include_vuln_details_vpatch</td>
<td>Specify 1 to include virtual patch information correlated with the vulnerability, obtained from Trend Micro real-time feeds.</td>
</tr>
<tr>
<td>include_vuln_details_compliance</td>
<td>Specify 1 to include compliance information correlated with the vulnerability.</td>
</tr>
<tr>
<td>include_vuln_details_exploit</td>
<td>Specify 1 to include exploitability information correlated with the vulnerability, includes references to known exploits and related security resources.</td>
</tr>
<tr>
<td>include_vuln_details_malware</td>
<td>Specify 1 to include malware information correlated with the vulnerability, obtained from the Trend Micro Threat Encyclopedia.</td>
</tr>
<tr>
<td>include_vuln_details_results</td>
<td>Specify 1 to include specific scan test results for each host, when available. We’ll also show the date the vulnerability was first detected, last detected and the number of times it was detected.</td>
</tr>
<tr>
<td>include_vuln_details_reopened</td>
<td>Specify 1 to include information related to reopened vulnerabilities.</td>
</tr>
<tr>
<td>include_vuln_details_appendix</td>
<td>Specify 1 to include more information like IPs in your report target that don’t have any scan results, and IPs that were scanned but results are not shown (no vulnerabilities were detected or all vulnerabilities were filtered out).</td>
</tr>
<tr>
<td>exclude_account_id</td>
<td>Specify 1 to exclude the account login ID in the filename of downloaded reports. Use this option to remove the login ID from the filename.</td>
</tr>
<tr>
<td>Filters</td>
<td>Filter options such as vulnerability status, categories, QIDs, OS.</td>
</tr>
<tr>
<td>selective_vulns</td>
<td>Specify complete to show results for any and all vulnerabilities found. Specify custom to filter your reports to specific QIDs (add static search lists) or to QIDs that match certain criteria (add dynamic search lists). For example, maybe you only want to report on vulnerabilities with severity 4 or 5. Tip - Exclude QIDs that you don’t want in the report.</td>
</tr>
<tr>
<td>search_list_ids</td>
<td>Specify search list ID or QID. Multiple search list IDs or QIDs can be provided using values separated by a comma. This parameter is required only if selective_vulns=custom.</td>
</tr>
<tr>
<td>exclude_qid_option</td>
<td>Specify 1 to exclude QIDs from the report.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>exclude_search_list_ids= [value]</td>
<td>Specify QID to be excluded from the report. Multiple QIDs can be provided using values separated by a comma. This parameter is required only if exclude_qid_option=1.</td>
</tr>
<tr>
<td>included_os={value}</td>
<td>Specify the operating system name to filter hosts. For example, to only report on Linux hosts make sure you provide the operating system name for Linux. Multiple operating system names can be provided using values separated by a comma. Specify ALL to include all operating systems. See Identified OS.</td>
</tr>
<tr>
<td>status_new={0</td>
<td>1}</td>
</tr>
<tr>
<td>status_active={0</td>
<td>1}</td>
</tr>
<tr>
<td>status_reopen={0</td>
<td>1}</td>
</tr>
<tr>
<td>status_fixed={0</td>
<td>1}</td>
</tr>
<tr>
<td>vuln_active={0</td>
<td>1}</td>
</tr>
<tr>
<td>vuln_disabled={0</td>
<td>1}</td>
</tr>
<tr>
<td>vuln_ignored={0</td>
<td>1}</td>
</tr>
<tr>
<td>potential_active={0</td>
<td>1}</td>
</tr>
<tr>
<td>potential_disabled={0</td>
<td>1}</td>
</tr>
<tr>
<td>potential_ignored={0</td>
<td>1}</td>
</tr>
<tr>
<td>ig_active={0</td>
<td>1}</td>
</tr>
<tr>
<td>ig_disabled={0</td>
<td>1}</td>
</tr>
<tr>
<td>ig_ignored={0</td>
<td>1}</td>
</tr>
<tr>
<td>display_non_running_kernels =0</td>
<td>1]</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>exclude_non_running_kernel= [0</td>
<td>1]</td>
</tr>
<tr>
<td>exclude_non_running_services = [0</td>
<td>1]</td>
</tr>
<tr>
<td>exclude_qids_not_exploitable_due_to_configuration=[0</td>
<td>1]</td>
</tr>
<tr>
<td>exclude_superceded_patches=[0</td>
<td>1]</td>
</tr>
<tr>
<td>categories_list=[value]</td>
<td>Specify the category name to filter hosts in your report based on various categories. For example, if you’re only interested in Windows vulnerabilities make sure you provide the category name for Windows. Multiple category names can be provided using values separated by a comma. Specify ALL to include all categories. See Categories.</td>
</tr>
<tr>
<td>Services and Ports</td>
<td>Services and ports to include in report.</td>
</tr>
<tr>
<td>required_services=[value]</td>
<td>Specify the name of a required service. Multiple service names can be provided using values separated by a comma. We’ll report QID: 38228 (when a required service is NOT detected). See Identified Services.</td>
</tr>
<tr>
<td>unauthorized_services=[value]</td>
<td>Specify the name of an unauthorized service. Multiple service names can be provided using values separated by a comma. We’ll report QID: 38175 (when an unauthorized service is detected). See Identified Services.</td>
</tr>
<tr>
<td>required_ports=[value]</td>
<td>Specify required ports. Multiple ports can be provided using values separated by a comma. We’ll report QID: 82051 (when a required port is NOT detected).</td>
</tr>
<tr>
<td>unauthorized_ports=[value]</td>
<td>Specify unauthorized ports. Multiple ports can be provided using values separated by a comma. We’ll report QID: 82043 (when an unauthorized port is detected).</td>
</tr>
</tbody>
</table>
Scan Template examples

Example: Create Scan template

API request:


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>2017-04-06T05:41:32Z</DATETIME>
    <CODE>Scan Report Template(s) Created Successfully [89876]</CODE>
    <TEXT></TEXT>
  </RESPONSE>
</SIMPLE_RETURN>

Example: Update Scan template

API request:

VM - New API Support for Report Templates

**XML output:**

```xml
<?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>2017-04-04T10:52:34Z</DATETIME>
    <CODE>Scan Report Template Updated Successfully [8209]</CODE>
    <TEXT></TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

**Example: Delete Scan template**

**API request:**

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
  "action=delete&template_id=8209"
  "https://qualysapi.qualys.com/api/2.0/fo/report/template/scan/"
```

**XML output:**

```xml
<?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>2017-04-04T10:54:37Z</DATETIME>
    <CODE>Scan Report Template(s) Deleted Successfully [8209]</CODE>
    <TEXT></TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```

**Example: Export Scan template**

**API request:**

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl"
  "https://qualysapi.qualys.com/api/2.0/fo/report/template/scan/?action=exp
ort&template_id=89470&report_format=xml"
```

Exports the report template based on the template ID. When the template ID is not
specified, exports all templates for the report type.

**XML output:**

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORTTEMPLATE SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/report/template/scan/scanreporttemplate_info.dtd">
<REPORTTEMPLATE>
```
VM - New API Support for Report Templates

<SCANTEMPLATE>
<TITLE>
/INFO key="title"><![CDATA[Scan-Report-To-Create-Do not Change]]></INFO>
/INFO key="owner"><![CDATA[1086]]></INFO>
</TITLE>
<TARGET>
/INFO key="scan_selection"><![CDATA[HostBased]]></INFO>
/INFO key="include_trending"><![CDATA[1]]></INFO>
/INFO key="selection_type"><![CDATA[days]]></INFO>
/INFO key="selection_range"><![CDATA[5]]></INFO>
/INFO key="limit_timeframe"><![CDATA[1]]></INFO>
/INFO key="asset_groups"><![CDATA[PBPS-Targets]]></INFO>
/INFO key="tag_set_by"><![CDATA[id]]></INFO>
/INFO key="tag_set_include"><![CDATA[8644659]]></INFO>
/INFO key="tag_set_exclude"><![CDATA[8262228]]></INFO>
/INFO key="tag_include_selector"><![CDATA[ALL]]></INFO>
/INFO key="tag_exclude_selector"><![CDATA[ALL]]></INFO>
/INFO key="network"><![CDATA[-100]]></INFO>
/INFO key="ips"><![CDATA[10.10.0.1,10.10.0.5]]></INFO>
/INFO key="host_with_cloud_agents"><![CDATA[all]]></INFO>
</TARGET>
<DISPLAY>
/INFO key="graph_business_risk"><![CDATA[1]]></INFO>
/INFO key="graph_vuln_over_time"><![CDATA[1]]></INFO>
/INFO key="display_text_summary"><![CDATA[1]]></INFO>
/INFO key="graph_status"><![CDATA[1]]></INFO>
/INFO key="graph_potential_status"><![CDATA[1]]></INFO>
/INFO key="graph_severity"><![CDATA[1]]></INFO>
/INFO key="graph_potential_severity"><![CDATA[1]]></INFO>
/INFO key="graph_ig_severity"><![CDATA[1]]></INFO>
/INFO key="graph_top_categories"><![CDATA[1]]></INFO>
/INFO key="graph_top_vulns"><![CDATA[1]]></INFO>
/INFO key="graph_os"><![CDATA[1]]></INFO>
/INFO key="graph_services"><![CDATA[1]]></INFO>
/INFO key="graph_top_ports"><![CDATA[1]]></INFO>
/INFO key="display_custom_footer_text"><![CDATA[Test@123]]></INFO>
/INFO key="sort_by"><![CDATA[host]]></INFO>
/INFO key="cvss"><![CDATA[all]]></INFO>
/INFO key="host_details"><![CDATA[0]]></INFO>
/INFO key="include_text_summary"><![CDATA[1]]></INFO>
/INFO key="include_vuln_details"><![CDATA[1]]></INFO>
/INFO key="include_vuln_details threat"><![CDATA[1]]></INFO>
/INFO key="include_vuln_details_impact"><![CDATA[1]]></INFO>
/INFO key="include_vuln_details_solution"><![CDATA[1]]></INFO>
/INFO key="include_vuln_details_vpatch"><![CDATA[1]]></INFO>
/INFO key="include_vuln_details_compliance"><![CDATA[1]]></INFO>
/INFO key="include_vuln_details_exploit"><![CDATA[1]]></INFO>
</DISPLAY>
VM - New API Support for Report Templates

<INFO key="include_vuln_details_malware"><![CDATA[1]]></INFO>
<INFO key="include_vuln_details_results"><![CDATA[1]]></INFO>
<INFO key="include_vuln_details_appendix"><![CDATA[1]]></INFO>
<INFO key="exclude_account_id"><![CDATA[1]]></INFO>
<INFO key="include_vuln_details_reopened"><![CDATA[1]]></INFO>
<INFO key="metadata_ec2_instances"><![CDATA[0]]></INFO>
</DISPLAY>
<FILTER>
<INFO key="selective_vulns"><![CDATA[complete]]></INFO>
<INFO key="search_list_ids"><![CDATA[]]></INFO>
<INFO key="exclude_qid_option"><![CDATA[1]]></INFO>
<INFO key="exclude_search_list_ids"><![CDATA[]]></INFO>
<INFO key="included_os"><![CDATA[ALL]]></INFO>
<INFO key="status_new"><![CDATA[1]]></INFO>
<INFO key="status_active"><![CDATA[1]]></INFO>
<INFO key="status_reopen"><![CDATA[1]]></INFO>
<INFO key="status_fixed"><![CDATA[1]]></INFO>
<INFO key="vuln_active"><![CDATA[1]]></INFO>
<INFO key="vuln_disabled"><![CDATA[1]]></INFO>
<INFO key="vuln_ignored"><![CDATA[1]]></INFO>
<INFO key="potential_active"><![CDATA[1]]></INFO>
<INFO key="potential_disabled"><![CDATA[1]]></INFO>
<INFO key="potential_ignored"><![CDATA[1]]></INFO>
<INFO key="ig_active"><![CDATA[1]]></INFO>
<INFO key="ig_disabled"><![CDATA[1]]></INFO>
<INFO key="ig_ignored"><![CDATA[0]]></INFO>
<INFO key="display_non_running_kernels"><![CDATA[1]]></INFO>
<INFO key="exclude_non_running_services"><![CDATA[1]]></INFO>
<INFO key="exclude_superceded_patches"><![CDATA[1]]></INFO>
<INFO key="exclude_qids_not_exploitable_due_to_configuration"><![CDATA[1]]></INFO>
<INFO key="categories_list"><![CDATA[ALL]]></INFO>
</FILTER>
<SERVICESPORTS>
<INFO key="required_services"><![CDATA[ActiveSync,akak trojan,Apple Airport Management,Applix TM1 Server]]></INFO>
<INFO key="unauthorized_services"><![CDATA[aml,Arkeiad Network Backup,auth]]></INFO>
<INFO key="services_info"><![CDATA[aml,Arkeiad Network Backup,auth]]></INFO>
<INFO key="required_ports"><![CDATA[12]]></INFO>
<INFO key="unauthorized_ports"><![CDATA[21]]></INFO>
</SERVICESPORTS>
<USERACCESS>
<INFO key="report_access_users"><![CDATA[start_rm2,start_su]]></INFO>
<INFO key="global"><![CDATA[1]]></INFO>
</USERACCESS>
Scan template DTD

https://<base_url>/api/2.0/fo/report/template/scan(scanreporttemplate_info.dtd

<!-- QUALYS REPORT_SCAN_TEMPLATE_OUTPUT DTD -->
<!ELEMENT REPORTTEMPLATE (SCANTEMPLATE)*>(
<!ELEMENT SCANTEMPLATE
(TITLE|TARGET|DISPLAY|FILTER|SERVICESPORTS|USERACCESS)*>(
<!ELEMENT TITLE (INFO)*>(
<!ELEMENT INFO (#PCDATA)>(
<!ATTLIST INFO
key CDATA #REQUIRED>
<!ELEMENT TARGET (INFO)*>(
<!ELEMENT DISPLAY (INFO)*>(
<!ELEMENT FILTER (INFO)*>(
<!ELEMENT SERVICESPORTS (INFO)*>(
<!ELEMENT USERACCESS (INFO)*>(
<!-- EOF -->

PCI Scan Template API

The API /api/2.0/fo/report/template/pciscan/ allows you to perform actions such as
create, update, delete and export on the PCI Scan Template.

PCI Scan Template Request

A summary of API Endpoint URLs is provided below.

<table>
<thead>
<tr>
<th>Action</th>
<th>API Endpoint /required parameters</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create PCI Scan Template</td>
<td>&lt;base_url&gt;/api/2.0/fo/report/template/pciscan/</td>
<td>POST</td>
</tr>
</tbody>
</table>
|                         | Required parameters:
|                         | action=create
|                         | report_format=xml                                                      |        |
| Update PCI Scan Template| <base_url>/api/2.0/fo/report/template/pciscan/                          | PUT    |
|                         | Required parameters:
|                         | template_id={value}
|                         | action=update
|                         | report_format=xml                                                      |        |
VM - New API Support for Report Templates

<table>
<thead>
<tr>
<th>Action</th>
<th>API Endpoint /required parameters</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete PCI Scan Template</td>
<td>&lt;base_url&gt;/api/2.0/fo/report/template/pciscan/</td>
<td>POST</td>
</tr>
<tr>
<td></td>
<td>Required parameters:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>template_id={value}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>action=delete</td>
<td></td>
</tr>
<tr>
<td>Export PCI Scan Template</td>
<td>&lt;base_url&gt;/api/2.0/fo/report/template/pciscan/</td>
<td>GET</td>
</tr>
<tr>
<td></td>
<td>Required parameters:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>action=export</td>
<td></td>
</tr>
<tr>
<td></td>
<td>report_format=xml</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Optional parameter:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>template_id={value}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When unspecified all templates for the report type get exported.</td>
<td></td>
</tr>
</tbody>
</table>

PCI Scan Template settings

Go to Scan Template settings. The same parameters used to define PCI Scan Template settings. All parameters (all are optional).

In addition the following parameters are used.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI Risk Ranking</td>
<td>Configure PCI Risk Ranking.</td>
</tr>
<tr>
<td>custom_pci_ranking={0</td>
<td>1}</td>
</tr>
<tr>
<td>customized_ranking_medium_from={0</td>
<td>1</td>
</tr>
<tr>
<td>customized_ranking_high_from={0</td>
<td>1</td>
</tr>
<tr>
<td>customized_ranking_comments={value}</td>
<td>When custom PCI risk ranking is enabled, a comment on the custom ranking is required. Enter any string up to 400 characters.</td>
</tr>
</tbody>
</table>
Examples

Refer to Scan template examples for create, update, delete and export sample requests. Requests and outputs for PCI Scan template are similar.

PCI Scan template DTD

https://<base_url>/api/2.0/fo/report/template/pciscan/
pciscanreporttemplate_info.dtd

<!ELEMENT REPORTTEMPLATE (PCISCANTEMPLATE)*>  
<!ELEMENT PCISCANTEMPLATE
(TITLE|TARGET|DISPLAY|FILTER|SERVICESPORTS|USERACCESS|PCIRISKRANKING)*>  
<!ELEMENT TITLE (INFO)*>  
<!ELEMENT INFO (#PCDATA)>  
<!ATTLIST INFO
  key CDATA #REQUIRED>  
<!ELEMENT TARGET (INFO)>  
<!ELEMENT DISPLAY (INFO)>  
<!ELEMENT FILTER (INFO)>  
<!ELEMENT SERVICESPORTS (INFO)>  
<!ELEMENT USERACCESS (INFO)>  
<!ELEMENT PCIRISKRANKING (INFO)>
Patch Template API

The API /api/2.0/fo/report/template/patch/ allows you to perform actions such as create, update, delete and export on the Patch Template.

**Patch Template Request**

A summary of API Endpoint URLs is provided below.

<table>
<thead>
<tr>
<th>Action</th>
<th>API Endpoint /required parameters</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Patch Template</td>
<td><code>&lt;base_url&gt;/api/2.0/fo/report/template/patch/</code></td>
<td>POST</td>
</tr>
<tr>
<td></td>
<td>Required parameters:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>action=create</td>
<td></td>
</tr>
<tr>
<td></td>
<td>report_format=xml</td>
<td></td>
</tr>
<tr>
<td>Update Patch Template</td>
<td><code>&lt;base_url&gt;/api/2.0/fo/report/template/patch/</code></td>
<td>PUT</td>
</tr>
<tr>
<td></td>
<td>Required parameters:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>template_id={value}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>action=update</td>
<td></td>
</tr>
<tr>
<td></td>
<td>report_format=xml</td>
<td></td>
</tr>
<tr>
<td>Delete Patch Template</td>
<td><code>&lt;base_url&gt;/api/2.0/fo/report/template/patch/</code></td>
<td>POST</td>
</tr>
<tr>
<td></td>
<td>Required parameters:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>template_id={value}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>action=delete</td>
<td></td>
</tr>
<tr>
<td>Export Patch Template</td>
<td><code>&lt;base_url&gt;/api/2.0/fo/report/template/patch/</code></td>
<td>GET</td>
</tr>
<tr>
<td></td>
<td>Required parameters:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>action=export</td>
<td></td>
</tr>
<tr>
<td></td>
<td>report_format=xml</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Optional parameter:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>template_id={value}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When unspecified all templates for the report type get exported.</td>
<td></td>
</tr>
</tbody>
</table>

**Patch Template settings**

These parameters (all are optional) are used for a create or update request to define Patch template settings. When creating a new template the default value is shown in bold where applicable.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>title</td>
<td>The template title and owner.</td>
</tr>
<tr>
<td>title={value}</td>
<td>A string value for the title. Length is maximum 64 characters.</td>
</tr>
</tbody>
</table>
## VM - New API Support for Report Templates

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>owner={value}</td>
<td>Username of the owner of this template. Validity of the owner to create reports is based on the user role or business unit. See About template owner.</td>
</tr>
<tr>
<td><strong>Target</strong></td>
<td>What target assets to include in the report.</td>
</tr>
<tr>
<td>patch_evaluation=</td>
<td>Specify classic to choose Classic patch evaluation or specify qidbased to choose QID based patch evaluation.</td>
</tr>
<tr>
<td>qidbased</td>
<td>classic</td>
</tr>
<tr>
<td>asset_groups</td>
<td>Asset groups to include in the report. Multiple asset groups are comma separated.</td>
</tr>
<tr>
<td>asset_group_ids={value}</td>
<td>Specify the ID of the asset group(s) to report on. Multiple asset group IDs are comma separated. We'll report on all the IPs in the asset groups.</td>
</tr>
<tr>
<td>tag_set_by={name</td>
<td>id}</td>
</tr>
<tr>
<td>tag_include_selector=</td>
<td>Specify ALL to match all the asset tags for the hosts you want to report on (This is an AND operation). Specifying ANY will match any of the assets tags (This is an OR operation).</td>
</tr>
<tr>
<td>ALL</td>
<td>ANY</td>
</tr>
<tr>
<td>tag_set_include={value}</td>
<td>Specify asset tags for the hosts you want to report on. We'll find the hosts in your account that match your tag selection and include them in the report. Multiple tags can be provided using comma separated values.</td>
</tr>
<tr>
<td>tag_exclude_selector=</td>
<td>Specify ALL to match all the asset tags for the hosts you want do not want to report on (This is an AND operation). Specifying ANY will match any of the assets tags (This is an OR operation).</td>
</tr>
<tr>
<td>ALL</td>
<td>ANY</td>
</tr>
<tr>
<td>tag_set_exclude={value}</td>
<td>Specify asset tags for the hosts you do not want to report on. We'll find the hosts in your account that match your tag selection and exclude them from the report. Multiple tags can be provided using comma separated values.</td>
</tr>
<tr>
<td>network={value}</td>
<td>(Valid only when the Networks feature is enabled for your account.) A network name containing the IPs to include. For a new template the default network is Global Default Network.</td>
</tr>
<tr>
<td>ips={value}</td>
<td>IP addresses to include in the report. Multiple IPs are comma separated.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Display</td>
<td>Display options to include in the report.</td>
</tr>
<tr>
<td>group_by=[HOST</td>
<td>PATCH</td>
</tr>
<tr>
<td>include_table_of_qids_fixed= {0</td>
<td>1}</td>
</tr>
<tr>
<td>include_patch_links={0</td>
<td>1}</td>
</tr>
<tr>
<td>include_patches_from_unspecified_vendors={0</td>
<td>1}</td>
</tr>
<tr>
<td>patch_severity_by={assigned</td>
<td>highest}</td>
</tr>
<tr>
<td>patch_cvss_score_by={assigned</td>
<td>highest</td>
</tr>
<tr>
<td>cvss=[all</td>
<td>cvssv2</td>
</tr>
<tr>
<td>display_custom_footer={0</td>
<td>1}</td>
</tr>
<tr>
<td>display_custom_footer_text={value}</td>
<td>Specify custom text like a disclosure statement or data classification (e.g. Public, Confidential). The text you enter will appear in all reports generated from this template, except reports in XML and CSV formats. Length is maximum 4000 characters.</td>
</tr>
<tr>
<td>exclude_account_id={0</td>
<td>1}</td>
</tr>
</tbody>
</table>
### VM - New API Support for Report Templates

**Parameter** | **Description**
---|---
Filters | Filter options such as vulnerabilities, QIDs, patches.
selective_vulns={complete | custom} | Specify complete to show results for any and all vulnerabilities found. Specify custom to filter your reports to specific QIDs (add static search lists) or to QIDs that match certain criteria (add dynamic search lists). For example, maybe you only want to report on vulnerabilities with severity 4 or 5. Tip - Exclude QIDs that you don't want in the report.
search_list_ids={value} | Specify QID to be included in the report. Multiple QIDs can be provided using values separated by a comma. This parameter is required only if selective_vulns=custom.
exclude_qid_option={0 | 1} | Specify 1 to exclude QIDs from the report.
exclude_search_list_ids={value} | Specify QID to be excluded from the report. Multiple QIDs can be provided using values separated by a comma. This parameter is required only if exclude_qid_option=1.
display_non_running_kernels={0 | 1} | Specify 1 to include a list of all vulnerabilities found on non-running kernels.
exclude_non_running_kernel={0 | 1} | Specify 1 to exclude vulnerabilities found on non-running kernels. Use only one parameter at a time: highlight_arf_kernel or arf_kernel.
exclude_non_running_services={0 | 1} | Specify 1 to only include vulnerabilities found where the port/service is running.
exclude_qids_not_exploitable_due_to_configuration={0 | 1} | Specify 1 to exclude vulnerabilities that are not exploitable because there’s a specific configuration present on the host.
selective_patches={complete | custom} | Specify complete to show results for any and all patches found. Specify custom to filter your reports to specific QIDs (add static search lists) or to QIDs that match certain criteria (add dynamic search lists). For example, maybe you only want to report on vulnerabilities with severity 4 or 5. Tip - Exclude QIDs that you don't want in the report.
exclude_patch_qid_option={0 | 1} | Specify 1 to exclude patch QIDs from the report.
patch_search_list_ids={value} | Specify patch QID to be included in the report. Multiple patch QIDs can be provided using values separated by a comma. This parameter is required only if selective_patches=custom.
### Examples

Refer to [Scan template examples](#) for create, update, delete and export sample requests. Requests and outputs for Patch template are similar.

### Patch template DTD

```xml
https://<base_url>/api/2.0/fo/report/template/patch/patchreporttemplate_info.dtd
```

```xml
<!ELEMENT REPORTTEMPLATE (PATCHTEMPLATE)>
<!ELEMENT PATCHTEMPLATE (TITLE|TARGET|DISPLAY|FILTER|USERACCESS)>
<!ELEMENT TITLE (INFO)>
<!ELEMENT INFO (#PCDATA)>
<!ATTLIST INFO
  key CDATA #REQUIRED>
<!ELEMENT TARGET (INFO)>
<!ELEMENT DISPLAY (INFO)>
<!ELEMENT FILTER (INFO)>
<!ELEMENT USERACCESS (INFO)>
```
Map Template API

The API /api/2.0/fo/report/template/map/ allows you to perform actions such as create, update, delete and export on the Map Template.

Map Template Request

A summary of API Endpoint URLs is provided below.

<table>
<thead>
<tr>
<th>Action</th>
<th>API Endpoint /required parameters</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Map Template</td>
<td>&lt;base_url&gt;/api/2.0/fo/report/template/map/</td>
<td>POST</td>
</tr>
<tr>
<td></td>
<td><strong>Required parameters:</strong> action=create</td>
<td></td>
</tr>
<tr>
<td></td>
<td>report_format=xml</td>
<td></td>
</tr>
<tr>
<td>Update Map Template</td>
<td>&lt;base_url&gt;/api/2.0/fo/report/template/map/</td>
<td>PUT</td>
</tr>
<tr>
<td></td>
<td><strong>Required parameters:</strong> template_id={value}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>action=update</td>
<td></td>
</tr>
<tr>
<td></td>
<td>report_format=xml</td>
<td></td>
</tr>
<tr>
<td>Delete Map Template</td>
<td>&lt;base_url&gt;/api/2.0/fo/report/template/map/</td>
<td>POST</td>
</tr>
<tr>
<td></td>
<td><strong>Required parameters:</strong> template_id={value}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>action=delete</td>
<td></td>
</tr>
<tr>
<td>Export Map Template</td>
<td>&lt;base_url&gt;/api/2.0/fo/report/template/map/</td>
<td>GET</td>
</tr>
<tr>
<td></td>
<td><strong>Required parameters:</strong> action=export</td>
<td></td>
</tr>
<tr>
<td></td>
<td>report_format=xml</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Optional parameter:</strong> template_id={value}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When unspecified all templates for the report type get exported.</td>
<td></td>
</tr>
</tbody>
</table>

Map Template settings

These parameters (all are optional) are used for a create or update request to define Map template settings. When creating a new template the default value is shown in bold where applicable..

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>The template title and owner.</td>
</tr>
<tr>
<td>title={value}</td>
<td>A string value for the title. Length is maximum 64 characters.</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>owner={value}</td>
<td>Username of the owner of this template. Validity of the owner to create reports is based on the user role or business unit. See <a href="#">About template owner</a>.</td>
</tr>
<tr>
<td>global={0</td>
<td>1}</td>
</tr>
</tbody>
</table>

#### Display

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>map_sort_by={ipaddress</td>
<td>dns</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>map_related_info_lastscandate={0</td>
<td>1}</td>
</tr>
<tr>
<td>map_related_info_assetgroups={0</td>
<td>1}</td>
</tr>
<tr>
<td>map_related_info_authenticationrecords={0</td>
<td>1}</td>
</tr>
<tr>
<td>map_related_info_discoverymethod={0</td>
<td>1}</td>
</tr>
<tr>
<td>display_custom_footer={0</td>
<td>1}</td>
</tr>
<tr>
<td>display_custom_footer_text={value}</td>
<td>Specify custom text like a disclosure statement or data classification (e.g. Public, Confidential). The text you enter will appear in all reports generated from this template, except reports in XML and CSV formats. Length is maximum 4000 characters.</td>
</tr>
<tr>
<td>map_exclude_account_id={0</td>
<td>1}</td>
</tr>
</tbody>
</table>

#### Filters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>map_included_hosttypes_innetblock={0</td>
<td>1}</td>
</tr>
<tr>
<td>map_included_hosttypes_scannable={0</td>
<td>1}</td>
</tr>
<tr>
<td>map_included_hosttypes_live={0</td>
<td>1}</td>
</tr>
</tbody>
</table>
### VM - New API Support for Report Templates

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>map_included_hosttypes_approved=0</td>
<td>1 Specify 1 to filter the report by host types - Approved.</td>
</tr>
<tr>
<td>map_included_hosttypes_outofnetblock=0</td>
<td>1 Specify 1 to filter the report by host types - Not In Netblock.</td>
</tr>
<tr>
<td>map_included_hosttypes_notcannable=0</td>
<td>1 Specify 1 to filter the report by host types - Not Scannable.</td>
</tr>
<tr>
<td>map_included_hosttypes_notlive=0</td>
<td>1 Specify 1 to filter the report by host types - Not Live.</td>
</tr>
<tr>
<td>map_included_hosttypes_rogue=0</td>
<td>1 Specify 1 to filter the report by host types - Rouge.</td>
</tr>
<tr>
<td>Included Discovery Methods</td>
<td>Specify at least one.</td>
</tr>
<tr>
<td>map_idm_tcp=0</td>
<td>1 Specify 1 to filter the report by discovery methods - TCP.</td>
</tr>
<tr>
<td>map_idm_udp=0</td>
<td>1 Specify 1 to filter the report by discovery methods - UDP.</td>
</tr>
<tr>
<td>map_idm_traceroute=0</td>
<td>1 Specify 1 to filter the report by discovery methods - TraceRoute.</td>
</tr>
<tr>
<td>map_idm_other=0</td>
<td>1 Specify 1 to filter the report by discovery methods - Other.</td>
</tr>
<tr>
<td>map_idm_dns=0</td>
<td>1 Specify 1 to filter the report by discovery methods - DNS.</td>
</tr>
<tr>
<td>map_idm_icmp=0</td>
<td>1 Specify 1 to filter the report by discovery methods - ICMP.</td>
</tr>
<tr>
<td>map_idm_auth=0</td>
<td>1 Specify 1 to filter the report by discovery methods - AUTH.</td>
</tr>
<tr>
<td>Included Status Levels</td>
<td>Only applicable for differential map reports.</td>
</tr>
<tr>
<td>map_included_statuses_added=0</td>
<td>1 Specify 1 to filter the report by statuses - Added.</td>
</tr>
<tr>
<td>map_included_statuses_removed=0</td>
<td>1 Specify 1 to filter the report by statuses - Removed.</td>
</tr>
<tr>
<td>map_included_statuses_active=0</td>
<td>1 Specify 1 to filter the report by statuses - Active.</td>
</tr>
<tr>
<td>dns_exclusions={none</td>
<td>DNS</td>
</tr>
<tr>
<td>included_os={value}</td>
<td>Specify the operating system name to filter hosts. For example, to only report on Linux hosts make sure you provide the operating system name for Linux. Multiple operating system names can be provided using values separated by a comma. Specify ALL to include all operating systems. See Identified OS.</td>
</tr>
</tbody>
</table>
Examples

Refer to Scan template examples for create, update, delete and export sample requests. Requests and outputs for Map template are similar.

Map template DTD

https://<base_url>/api/2.0/fo/report/template/map/mapreporttemplate_info.dtd

```xml
<!ELEMENT REPORTTEMPLATE (MAPTEMPLATE)*>  
<!ELEMENT MAPTEMPLATE (TITLE|DISPLAY|FILTER|OPERATINGSYSTEM)*>  
<!ELEMENT TITLE (INFO)>  
<!ELEMENT INFO (#PCDATA)>  
<!ATTLIST INFO  
  key CDATA #REQUIRED>  
<!ELEMENT DISPLAY (INFO)>  
<!ELEMENT FILTER (INFO)>  
<!ELEMENT OPERATINGSYSTEM (INFO)>  
```

About template owner

The user who created the report template is the owner by default. Managers and Unit Managers have the option to specify/change the owner while creating a report template the first time or by updating an existing report template. Use the parameter "owner" to assign a template owner.

Global report templates may be owned by Managers and Unit Managers. Non-global report templates may be owned by Managers, Unit Managers, Scanners and Readers.

Managers / Unit Managers can assign only those users as template owners who are part of their hierarchy and are added in their subscription.


Identified OS

Operating Systems identified by our service as of March 2017 are listed below.

Looking for a more current listing? Sure thing, just log in to your Qualys account and go to Help > About.

Tip - In API requests replace spaces in OS names with underscores. For example, Apple IOS must be specified as Apple_IOS

3Com
3Com HomeConnect
3Com NBX
3Com OfficeConnect
3Com SuperStack
3Com Switch
3Com Wireless Access Point
AB
AB ControlLogix
Adic
Adic Scalar
Adic Storage
ADIC Storage
Adtran
Adtran Device
Adtran NetVanta
Adtran TSUIQ
ADTX
ADTX ArrayMasStor
AIX
AIX 4.2-4.3
AIX 4.3
AIX 4.3.2.0-4.3.3.0
AIX 4.33
AIX 4.3-5.1
AIX 4.x
AIX 4.x-5.x
AIX 5.1
AIX 5.1-5.2
AIX 5.1-5.3
AIX 5.2
AIX 5.3
AIX 5.3.0.4
AIX 5.x
AIX 6.x
Aricia
Alcatel Omnistack
Alcatel OmniSwitch
Allied
Allied Telesyn Switch
Alteon
Alteon ACE Switch
Alteon Switch
Altium
Altium Wireless Device
Amazon Linux
AMX
AMX Modero
APC
APC InfraStruXure
APC MasterSwitch
APC Network
APC Network Management Card AOS
APC Smart-UPS
AppCelera
AppCelera ICX
Apple
Apple Airport Wireless Access Point
Apple iOS
Apple Wireless Access Point
Arescom
Arescom Device
Arescom NetDSL
Ascend
Ascend Router
Ascent
Ascent Router
ASUS
ASUS Wireless
ASUS Wireless Access Point
Aten
Aten KVM Switch
ATT NetGate
ATTO Device
AudioCodes
AudioCodes VOIP
Avaya
Avaya Device
Avaya G350
Avaya IP Phone
Avaya Wireless Access Point
Avocent
Avocent CCM Appliance
Axis
Axis CCM Appliance
Axis Network Camera
VM - New API Support for Report Templates

Axis Printer
Axis Storpoint CD
Axis Video Server
Axis Wireless Access Point
Axonix SuperCD
Bay Networks
Bay Networks Router
Bay Networks Switch
Belkin
Belkin Wireless Access Point
BeOS 5
BlueCoat Security Gateway
BlueSocket Embedded Linux 2.4-2.6
BorderWare Firewall
Brocade Device
Brother Printer
BSD
BSD Unix
BSDI BSD
BT Voyager
Buffalo Wireless Access Point
Cabletron
Cabletron SmartSTACK
Cabletron Switch
Caldera
Caldera Open Linux
Caldera Open UNIX 7
Caldera Open UNIX 8
Canon
Canon Network Printer
Canon Print Server
Canon Printer
Cayman3000
CEKAB Device
CentOS
CentOS
CheckPoint
CheckPoint FW1
CheckPoint FW1 NG
CheckPoint FW1 on Solaris
CheckPoint SecurePlatform
Cintech Switch
Cirronet Wireless Access Point
Cisco
Cisco Analog Phone Gateway
Cisco Analog Telephone Adaptor
Cisco Arrowpoint WebNS
Cisco ASA
Cisco Catalyst
Cisco Content Engine
Cisco Content Services Switch
Cisco Content Switching Solution
Cisco Content/File Engine
Cisco Controller
Cisco File Engine
Cisco Firewall Services Module
Cisco IOS
Cisco IP Phone
Cisco IP/TV Program Manager
Cisco Local Director
Cisco PIX
Cisco VPN
Cisco WGB350
Cisco Wireless Access Point
ClearPath MCP
CNT UltraNet Edge
Cognitive Printer
CometLabs Switch
Compaq
Compaq Insight Manager
Compaq Switch
Computone Device
Connect2Air Wireless Access Point
ControlLogix ENET
Crossroads Storage Router
Custom Micro Device
CyberGuard Firewall
CyberGuard Firewall
Datamax I-Class
Datamax Printer
Dawning SNI
Debian
Dell
Dell Laser
Dell PowerConnect
Dell PowerVault
Dell Remote Access Controller
Digi
Digi One PortServer
Digi One SP
Digi Port Server
Divar Video Camera
D-Link
D-Link DSL Modem
D-Link Print Server
D-Link Router
D-Link Switch
D-Link Wireless Access Point
<table>
<thead>
<tr>
<th>VM - New API Support for Report Templates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draytek Router</td>
</tr>
<tr>
<td>DVD Server</td>
</tr>
<tr>
<td>Efficient Router</td>
</tr>
<tr>
<td>EFI Printer</td>
</tr>
<tr>
<td>EMC's Network-Attached Storage Device</td>
</tr>
<tr>
<td>Enterasys</td>
</tr>
<tr>
<td>Entry-Master Card Access Control System</td>
</tr>
<tr>
<td>Epson Printer</td>
</tr>
<tr>
<td>ExtendedNet Print Server</td>
</tr>
<tr>
<td>Extreme</td>
</tr>
<tr>
<td>Extreme Alpine</td>
</tr>
<tr>
<td>Extreme Networks Device</td>
</tr>
<tr>
<td>Extreme Networks ExtremeWare</td>
</tr>
<tr>
<td>Extreme Networks Switch</td>
</tr>
<tr>
<td>F5 Networks Big-IP</td>
</tr>
<tr>
<td>Fabric OS</td>
</tr>
<tr>
<td>FaxPress</td>
</tr>
<tr>
<td>Fiery Printer</td>
</tr>
<tr>
<td>File Engine</td>
</tr>
<tr>
<td>Fortigate</td>
</tr>
<tr>
<td>Foundry Networks</td>
</tr>
<tr>
<td>FreeBSD</td>
</tr>
<tr>
<td>Fujitsu</td>
</tr>
<tr>
<td>Fujitsu Blade</td>
</tr>
<tr>
<td>Gestetner</td>
</tr>
<tr>
<td>Gestetner Printer</td>
</tr>
<tr>
<td>Gigafast</td>
</tr>
<tr>
<td>Gigafast Wireless Access Point</td>
</tr>
<tr>
<td>Gigafast Wireless Access Point</td>
</tr>
<tr>
<td>Google Appliance</td>
</tr>
<tr>
<td>Hawking Wireless Access Point</td>
</tr>
<tr>
<td>Honeyd HoneyPot</td>
</tr>
<tr>
<td>HP</td>
</tr>
<tr>
<td>HP 3000 MPE</td>
</tr>
<tr>
<td>HP AdvanceStack Switch</td>
</tr>
<tr>
<td>HP Deskjet Printer</td>
</tr>
<tr>
<td>HP Fabric OS</td>
</tr>
<tr>
<td>HP Guardian Service Processor</td>
</tr>
<tr>
<td>HP iLO</td>
</tr>
<tr>
<td>HP Inkjet Printer</td>
</tr>
<tr>
<td>HP JetDirect</td>
</tr>
<tr>
<td>HP LaserJet</td>
</tr>
<tr>
<td>HP OpenVMS</td>
</tr>
<tr>
<td>HP ProCurve</td>
</tr>
<tr>
<td>HP RILO</td>
</tr>
<tr>
<td>HP Surestore Library</td>
</tr>
<tr>
<td>HP Switch</td>
</tr>
<tr>
<td>VM - New API Support for Report Templates</td>
</tr>
<tr>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Juniper Networks</td>
</tr>
<tr>
<td>Juniper Networks Application</td>
</tr>
<tr>
<td>Acceleration Platform DX</td>
</tr>
<tr>
<td>Juniper Networks JUNOS</td>
</tr>
<tr>
<td>Kentrox</td>
</tr>
<tr>
<td>Kentrox Q2200 Router</td>
</tr>
<tr>
<td>Konica</td>
</tr>
<tr>
<td>Konica Minolta</td>
</tr>
<tr>
<td>Konica Printer</td>
</tr>
<tr>
<td>Kyocera</td>
</tr>
<tr>
<td>Kyocera Mita</td>
</tr>
<tr>
<td>Kyocera Printer</td>
</tr>
<tr>
<td>Lancast</td>
</tr>
<tr>
<td>Lancast Media Converter</td>
</tr>
<tr>
<td>Lanier</td>
</tr>
<tr>
<td>Lanier Printer</td>
</tr>
<tr>
<td>Lantronix</td>
</tr>
<tr>
<td>Lantronix CoBox</td>
</tr>
<tr>
<td>Lantronix ETS32PR</td>
</tr>
<tr>
<td>Lantronix MSS100</td>
</tr>
<tr>
<td>Lantronix Printer</td>
</tr>
<tr>
<td>Leitch</td>
</tr>
<tr>
<td>Lexmark</td>
</tr>
<tr>
<td>Lexmark Optra</td>
</tr>
<tr>
<td>Lexmark Print Server</td>
</tr>
<tr>
<td>Lexmark Printer</td>
</tr>
<tr>
<td>LinkCom</td>
</tr>
<tr>
<td>LinkCom Xpress Print Server</td>
</tr>
<tr>
<td>Linksys</td>
</tr>
<tr>
<td>Linksys Router</td>
</tr>
<tr>
<td>Linksys Wireless</td>
</tr>
<tr>
<td>Linux</td>
</tr>
<tr>
<td>Linux 1.2.8-1.2.13</td>
</tr>
<tr>
<td>Linux 2.0</td>
</tr>
<tr>
<td>Linux 2.0.29</td>
</tr>
<tr>
<td>Linux 2.0.30+</td>
</tr>
<tr>
<td>Linux 2.0.34-38</td>
</tr>
<tr>
<td>Linux 2.1.19-2.2.20</td>
</tr>
<tr>
<td>Linux 2.2</td>
</tr>
<tr>
<td>Linux 2.2.20</td>
</tr>
<tr>
<td>Linux 2.4</td>
</tr>
<tr>
<td>Linux 2.4.0-2.5.20</td>
</tr>
<tr>
<td>Linux 2.4.20-2.4.25</td>
</tr>
<tr>
<td>Linux 2.4.20-3</td>
</tr>
<tr>
<td>Linux 2.4.22</td>
</tr>
<tr>
<td>Linux 2.4.7</td>
</tr>
<tr>
<td>Linux 2.4.x</td>
</tr>
<tr>
<td>Linux 2.4-2.6</td>
</tr>
<tr>
<td>Linux 2.6</td>
</tr>
<tr>
<td>Linux 2.x</td>
</tr>
<tr>
<td>Linux 3.0</td>
</tr>
<tr>
<td>Linux Based MRV LX Series Server</td>
</tr>
<tr>
<td>Linux behind</td>
</tr>
<tr>
<td>Lucent</td>
</tr>
<tr>
<td>Lucent Cajun</td>
</tr>
<tr>
<td>Lucent MAX</td>
</tr>
<tr>
<td>Lucent Orinoco</td>
</tr>
<tr>
<td>Lucent PBX</td>
</tr>
<tr>
<td>Lucent Router</td>
</tr>
<tr>
<td>Lucent WAP</td>
</tr>
<tr>
<td>LynxOS</td>
</tr>
<tr>
<td>MacOS</td>
</tr>
<tr>
<td>MacOS 10.0.x-10.1.x</td>
</tr>
<tr>
<td>MacOS 10.10</td>
</tr>
<tr>
<td>MacOS 10.11</td>
</tr>
<tr>
<td>MacOS 10.12</td>
</tr>
<tr>
<td>MacOS 10.3-10.4</td>
</tr>
<tr>
<td>MacOS 8</td>
</tr>
<tr>
<td>MacOS 9</td>
</tr>
<tr>
<td>MacOS X</td>
</tr>
<tr>
<td>magicolor</td>
</tr>
<tr>
<td>magicolor 2300 Printer</td>
</tr>
<tr>
<td>magicolor 3300 Printer</td>
</tr>
<tr>
<td>magicolor Printer</td>
</tr>
<tr>
<td>MarkNet Pro Printer</td>
</tr>
<tr>
<td>Meditech MAGIC</td>
</tr>
<tr>
<td>MGE Uninterruptible Power Supply Systems</td>
</tr>
<tr>
<td>MiLAN</td>
</tr>
<tr>
<td>MiLAN Print Server</td>
</tr>
<tr>
<td>MiLAN Switch</td>
</tr>
<tr>
<td>Microtest DiscZerver</td>
</tr>
<tr>
<td>MiLAN Systems</td>
</tr>
<tr>
<td>Moxa Async Server</td>
</tr>
<tr>
<td>Moxa NPort Serial Server</td>
</tr>
<tr>
<td>Multi-Tech</td>
</tr>
<tr>
<td>Multi-Tech CommPlete</td>
</tr>
<tr>
<td>Multi-Tech MultiVOIP</td>
</tr>
<tr>
<td>Muratec MFX Printer</td>
</tr>
<tr>
<td>NCR Unix</td>
</tr>
<tr>
<td>NEC Projector</td>
</tr>
<tr>
<td>Neoteris Instant Virtual Extranet</td>
</tr>
<tr>
<td>NetApp</td>
</tr>
<tr>
<td>NetApp behind FW1</td>
</tr>
<tr>
<td>NetBlazer</td>
</tr>
<tr>
<td>Network Device</td>
</tr>
<tr>
<td>------------------------------------</td>
</tr>
<tr>
<td>NetBSD</td>
</tr>
<tr>
<td>NETBuilder Bridge</td>
</tr>
<tr>
<td>Netgear</td>
</tr>
<tr>
<td>Netgear GSM</td>
</tr>
<tr>
<td>Netgear Print Server</td>
</tr>
<tr>
<td>Netgear Printer</td>
</tr>
<tr>
<td>Netgear Router</td>
</tr>
<tr>
<td>Netgear Smart Switch</td>
</tr>
<tr>
<td>Netgear Switch</td>
</tr>
<tr>
<td>Netgear Wireless Access Point</td>
</tr>
<tr>
<td>Netopia</td>
</tr>
<tr>
<td>Netopia Router</td>
</tr>
<tr>
<td>Netphone</td>
</tr>
<tr>
<td>Netphone IP Phone</td>
</tr>
<tr>
<td>NetScaler</td>
</tr>
<tr>
<td>NetScaler VPN Device</td>
</tr>
<tr>
<td>NetScreen</td>
</tr>
<tr>
<td>NetScreen 100</td>
</tr>
<tr>
<td>NetScreen 50</td>
</tr>
<tr>
<td>NetScreen 5XF</td>
</tr>
<tr>
<td>NetSilicon Device</td>
</tr>
<tr>
<td>Netsilicon Device</td>
</tr>
<tr>
<td>NetWare</td>
</tr>
<tr>
<td>NetWare 4.11-5.0 SP5</td>
</tr>
<tr>
<td>NetWare 5</td>
</tr>
<tr>
<td>NetWare 5.0</td>
</tr>
<tr>
<td>NetWare 5.1</td>
</tr>
<tr>
<td>NetWare 6</td>
</tr>
<tr>
<td>NetWare 6.5</td>
</tr>
<tr>
<td>NetWare Print Server</td>
</tr>
<tr>
<td>Network Camera</td>
</tr>
<tr>
<td>Network Print Server</td>
</tr>
<tr>
<td>Network Printer</td>
</tr>
<tr>
<td>Network Scanner</td>
</tr>
<tr>
<td>NGS 500 Router</td>
</tr>
<tr>
<td>NIB Network Printer</td>
</tr>
<tr>
<td>Nokia</td>
</tr>
<tr>
<td>Nokia IPSO</td>
</tr>
<tr>
<td>Nokia Wireless Access Point</td>
</tr>
<tr>
<td>Nortel</td>
</tr>
<tr>
<td>Nortel Device</td>
</tr>
<tr>
<td>Nortel Networks BayStack</td>
</tr>
<tr>
<td>Nortel Passport</td>
</tr>
<tr>
<td>Nortel Router</td>
</tr>
<tr>
<td>Nortel Switch</td>
</tr>
<tr>
<td>NRG</td>
</tr>
<tr>
<td>NRG Network</td>
</tr>
<tr>
<td>NRG Printer</td>
</tr>
<tr>
<td>Okidata Printer</td>
</tr>
</tbody>
</table>
**VM - New API Support for Report Templates**

<table>
<thead>
<tr>
<th>Rockwell</th>
<th>Solaris 8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rockwell Automation</td>
<td>Solaris 8-10</td>
</tr>
<tr>
<td>Savin Printer</td>
<td>Solaris 9</td>
</tr>
<tr>
<td>Scannex NetBuffer</td>
<td>Solaris 9-10</td>
</tr>
<tr>
<td>Schneider Electric Controller</td>
<td>Solaris behind</td>
</tr>
<tr>
<td>SCO</td>
<td>Spectrum24 Wireless Access Point</td>
</tr>
<tr>
<td>SCO OpenServer</td>
<td>Stallion EasyServer</td>
</tr>
<tr>
<td>SCO Unix</td>
<td>StarDot NetCam</td>
</tr>
<tr>
<td>SCO UnixWare</td>
<td>Summit Switch</td>
</tr>
<tr>
<td>SCO UnixWare Firewall</td>
<td>Sun Cobalt Linux</td>
</tr>
<tr>
<td>SensaTronics Environmental Monitor</td>
<td>Sun Lights Out</td>
</tr>
<tr>
<td>Sentry Remote Power Manager</td>
<td>SUN StorEdge RAID</td>
</tr>
<tr>
<td>Shark supercomputer</td>
<td>SuperScript Printer</td>
</tr>
<tr>
<td>Sharp Printer</td>
<td>SuSE</td>
</tr>
<tr>
<td>Shore Microsystems Link Protector</td>
<td>SuSE Linux 10</td>
</tr>
<tr>
<td>Sidewinder G2</td>
<td>SuSE Linux 11</td>
</tr>
<tr>
<td>Siemens</td>
<td>SuSE Linux 7</td>
</tr>
<tr>
<td>Siemens 5940 Router</td>
<td>SuSE Linux 8</td>
</tr>
<tr>
<td>Siemens HiPath 3000</td>
<td>SuSE Linux 9</td>
</tr>
<tr>
<td>Siemens I-Gate</td>
<td>Sveasoft Firmware</td>
</tr>
<tr>
<td>Siemens IP Phone</td>
<td>Symantec Raptor Firewall</td>
</tr>
<tr>
<td>Siemens Wireless Access Point</td>
<td>Symbol Wireless Access Point</td>
</tr>
<tr>
<td>Signature System</td>
<td>Symon NetLite</td>
</tr>
<tr>
<td>Silex Pricom Print Server</td>
<td>SYSTEC CAN-Ethernet Gateway</td>
</tr>
<tr>
<td>SIMATIC NET CP</td>
<td>Tandberg</td>
</tr>
<tr>
<td>SMC</td>
<td>Tandberg Device</td>
</tr>
<tr>
<td>SMC Networks SMC8624T</td>
<td>Tandem</td>
</tr>
<tr>
<td>SMC Router</td>
<td>Tandem NSK</td>
</tr>
<tr>
<td>SMC Wireless Access Point</td>
<td>Tektronix Phaser Printer</td>
</tr>
<tr>
<td>SMC2671 Wireless Access Point</td>
<td>Telindus Router</td>
</tr>
<tr>
<td>SNAP Ethernet Brain</td>
<td>Tenor Switch</td>
</tr>
<tr>
<td>Snap Server</td>
<td>TINI</td>
</tr>
<tr>
<td>Solaris</td>
<td>TiVo</td>
</tr>
<tr>
<td>Solaris 10</td>
<td>TiVo Series</td>
</tr>
<tr>
<td>Solaris 11</td>
<td>TopLayer Appsafe</td>
</tr>
<tr>
<td>Solaris 2</td>
<td>Toshiba NWcamera</td>
</tr>
<tr>
<td>Solaris 2.5.1</td>
<td>Transition Networks Device</td>
</tr>
<tr>
<td>Solaris 2.5-2.5.1</td>
<td>Trendnet Print Server</td>
</tr>
<tr>
<td>Solaris 2.6</td>
<td>Trendware Print Server</td>
</tr>
<tr>
<td>Solaris 2.6-10</td>
<td>Tru64</td>
</tr>
<tr>
<td>Solaris 2.6-7</td>
<td>Tru64 Unix 4.0d</td>
</tr>
<tr>
<td>Solaris 2.6-8</td>
<td>Tru64 Unix 5.x</td>
</tr>
<tr>
<td>Solaris 2.7</td>
<td>Tut Modem</td>
</tr>
<tr>
<td>Solaris 5</td>
<td>TV Program Manager</td>
</tr>
<tr>
<td>Solaris 5.8</td>
<td>U.S. Robotics</td>
</tr>
<tr>
<td>Solaris 6-8</td>
<td>U.S. Robotics Access point</td>
</tr>
<tr>
<td>Solaris 7</td>
<td>U.S. Robotics ADSL Wireless Gateway</td>
</tr>
<tr>
<td>Solaris 7-10</td>
<td>U.S. Robotics Broadband Router</td>
</tr>
</tbody>
</table>
VM - New API Support for Report Templates

U.S. Robotics Wireless Access Point
Ubuntu
Ubuntu Linux 10
Ubuntu Linux 11
Ubuntu Linux 7
Ubuntu Linux 8
Ubuntu Linux 9
Ubuntu Linux LTS
Uninterruptible Power Supply Device
UNIX System V
UNIX System V Release 4.2
UNIX System UNIX System V 4
Uptime Devices Monitoring System
Uptime Devices Sensorprobe
VAX
VAX VMS 6.1
VAX VMS 6.1 behind Sidewinder G2
VAX VMS 6.2
VAX VMS 7.1
VAX VMS 7.1 behind Sidewinder G2
Verilink WANsuite Router
Vertical Horizon Stack
VirtualAccess LinxpeedPro
VMware
VMWare ESX 3.5
VMWare ESX 4.0
VMWare ESX 4.1
VMware ESX4 Server
VMWare ESXi 4.0
VMWare ESXi 4.1
VMWare ESXi 5.0
VMWare ESXi 5.0
VxWorks Based Device
WatchGuard Firewall
Web Smart Switch
WebNet uServer
Windows
Windows 10
Windows 2000
Windows 2003
Windows 2008
Windows 2012
Windows 7
Windows 8
Windows 95
Windows 98
Windows 9x
Windows CE
Windows Longhorn
Windows ME
Windows NT
Windows NT4
Windows RT
Windows Vista
Windows XP
WKTI RDS Encoder
Xerox
Xerox Device
Xerox DocuColor Printer
Xerox Document Centre
Xerox DocuPrint Printer
Xerox Phaser Printer
Xerox Plotter
Xerox Printer
Xerox WorkCentre
Xerox WorkCentre Printer
XES Printer
XJet Print Server
ZebraNet Print Server
ZOT Print Server

Identified Services

Services identified by our service as of March 2017 are listed below.

Looking for a more current listing? Just log in to your Qualys account and go to Help > About.

Tip - In API requests replace spaces in service names with underscores. For example, **Blackberry Attachment** must be specified as **Blackberry_Attachment**

    ActiveSync
    ADDP
    afpovertcp
    akak_trojan
    amandaidx
    aml
    Apple_Airport_Management
    Applix
    Applix_axnet
    Applix_TML_Admin_Server
    Applix_TML_Server
    Arkeiad_Network_Backup
VM - New API Support for Report Templates

ARUGIZER_BACKDOOR
auth
Berlios_Global_Positioning_System_Daemon
BIGFIX_ENTERPRISE_SERVER
BIGFIX ENTERPRISE_SERVER
BITCOIN
bitkeeper
Blackberry_Attachment
BMC_Patrol
BO2K_backdoor
bofra_worm
bpcd
bpjava_msvc
cabrightststor
CA_License_Management_Agent
CA_Unicenter_Services
CENTUM_CS_3000 chargen
chargen_udp
CHECKPOINT_FW-1_CLIENT_AUTH_SERVER
chindi
cisco_cnr
CISCO_CNR_AICSERVAGT
Cisco_Secure_ACS
cisco_ta
citadel
Citrix_CMC
Citrix_ICA
Codesys
Cognos_Powerplay_Enterprise_Server
Computer_Associates_License_Manager
COREid Access_Server
crystal_info
Crystal_Reports_App_Server
Crystal_Reports_CMS
cvpscerv
daap
dameware
darxite
daytime
daytime_udp
directory
DC Directory Server
dcerpc
dchub
DHCP_or_Bootp_Server
DNS_Server
dtscpd
echo
echo_udp
VM - New API Support for Report Templates

LANDESK_MANAGEMENT_AGENT
LANDESK_MANAGEMENT_AGENT
ldap
ldap_over_ssl
limewire
linuxconf
lpd
managesoft
McAfee_ePolicy_Orchestrator
melange_chat
MERCUR_Control-Service
Micromuse_Netcool_Object_Server
microsoft-ds
Microsoft_Message_Queue_Server
minisql
modbus
MODBUS_UDP
mqseries
msdc
MSMQ_Ping
msrpc
msrpc-over-http
msrpc_udp
mssql
mssql_monitor
MYDESKTOP
mysql
named_udp
ncp
nessus
netbios_ns
netbios_ssn
netbus
nettop
netstat
Netviewer_PC_Duo
nfs
nt
ntp
ocsp
ocssd
Omniquad_Server
open_vpn
openvpn
oracle
Oracle_Express_Server
Oracle_Express_Server_xsagent
Oracle_Express_Server-xsdaemon
oracle_intelligent_agent
ORACLE_RMI
pcanywhere
pen
Polycom_MGC_Management
pop2
pop3
PostgreSQL
pptp
Polycom_MGC_Management
proxy_http
proxy_telnet
psmond
pvserver
Quote_of_the_Day
quote_of_the_day_udp
radius
radius_tcp
radius
radmin
rccmd
RealMedia_EncoderServer
Red_Carpet_Daemon
RELIABLE_DATAGRAM_SOCKETS_OVER_TCP
Resonate_CD_Agent
resource_monitor_api
Resource_Monitoring_and_Control
rip
rlogin
RMIRegistry
rpc
rpc_udp
RSA_Auth_Mgr
rsh/rexec
rsyncd
rtsp
SAP_MAXDB
SAP_Protocol
SAPgui
SGI_Performance_Copilot
shell
SHOUTcast
skinny
skype
slapper
SMS
smtp
smux
snmp
snmp2
socks4

Qualys API Release Notes 97
VM - New API Support for Report Templates

socks5
SPLASHTOP_REMOTE_DESKTOP
spychat
Spytech_SpyAnywhere
ssdp
ssh
ssh_over_ssl
swagentd
swat
sybase_adaptive_server
Symantec EMS client server
Symantec_AntiVirus
Symantec_AntiVirus_Rtvscan
Symantec_AntiVirus_Rtvscan_UDP
SysGalUR
systat
talk
telnet
telnet_over_ssl
tftp
time
time_udp
timestamp_over_http
trendmicro_officescan
trojan_fireby
unknown
unknown_over_ssl
UPNP
ut_game_queryport
uucp
VMware_Authentication_Daemon
vnc
vnetd
voip_sip
Volume_Manager_Storage_Administrator
VXWORKS_WDBRPC_UDP
watchguard_admin
webshield
win_remote_desktop
wimx
WINS_Replication
Wonderware_InTouch
wsmserver
WSUS_SERVER
x11
X11_Font_Service
xdmcp
xinetd
Xitami
xpilot
XYZFind
Yahoo_Instant_Messenger
yeemp
ZLink

Categories

Vulnerability Categories as defined by our service as of March 2017 are listed below.

Want a current listing? No problem. Just log in to your Qualys account, go to the KnowledgeBase, click the Search button, and open the Category menu.

Looking for category descriptions? We’ve got you covered. Log in to your Qualys account, go to Help > Online Help and search for Categories and you’ll see the article on Vulnerability Categories with all the details.

Tip - In API requests replace spaces in category names with underscores. For example, Amazon Linux must be specified as Amazon_LINUX.
Information gathering
Internet Explorer
Local
Mail services
Malware
News Server
NFS
OEL
Office Application
Proxy
RedHat
RPC
Security Policy
SNMP
Solaris
SMB / NETBIOS
SUSE
TCP/IP
Ubuntu
VMware
Web Application
Web Application Firewall
Web server
Windows
X-Window
VM - Show Reopened Info in Scan Reports

When you download a scan report (with host based findings) from your account your report may now include these vulnerability details: date/time the vulnerability was first reopened, date/time the vulnerability was last reopened, number of times the vulnerability was reopened.

Good to Know

You must edit your scan report template to see reopened details in the report. In the template, go to the Display tab and choose Reopened under Vulnerability Details.

You can download scan reports using any of these methods: download the report from the UI, use the Report API v2 (/api/2.0/fo/report/?action=fetch), or use the Asset Data Report API v1 (/msp/asset_data_report.php). The Asset Data Report DTD (asset_data_report.dtd) was updated.

Sample XML Report

```xml
<!DOCTYPE ASSET_DATA_REPORT SYSTEM "https://qualysapi.qualys.com/asset_data_report.dtd">
<ASSET_DATA_REPORT>
    <HEADER>
        <COMPANY><![CDATA[Qualys, Inc.]]></COMPANY>
        <USERNAME>qualys_ps</USERNAME>
        <GENERATION_DATETIME>2017-04-11T19:05:14Z</GENERATION_DATETIME>
        <TEMPLATE><![CDATA[Vuln Details + Reopened]]></TEMPLATE>
    </HEADER>
    ...
    <VULN_INFO_LIST>
        <VULN_INFO>
            <QID id="qid_38169">38169</QID>
            <TYPE>Vuln</TYPE>
            <PORT>443</PORT>
            <PROTOCOL>tcp</PROTOCOL>
            <SSL>true</SSL>
            <FIRST_FOUND>2016-09-12T20:06:03Z</FIRST_FOUND>
            <LAST_FOUND>2016-11-10T00:22:25Z</LAST_FOUND>
            <TIMES_FOUND>17</TIMES_FOUND>
            <VULN_STATUS>Re-Opened</VULN_STATUS>
            <LAST_FIXED>2016-11-07T23:57:21Z</LAST_FIXED>
            <FIRST_REOPENED>2016-09-24T01:42:10Z</FIRST_REOPENED>
            <LAST_REOPENED>2016-11-10T00:22:25Z</LAST_REOPENED>
            <TIMES_REOPENED>2</TIMES_REOPENED>
        </VULN_INFO>
    ...
</VULN_INFO>
```

Qualys API Release Notes 100
DTD update

We added new elements (in bold) to the Asset Data Report DTD (asset_data_report.dtd).

... 
FIRST_REOPENED?, LAST_REOPENED?, TIMES_REOPENED?, CVSS_FINAL?, CVSS3_FINAL?, TICKET_NUMBER?, TICKET_STATE?)> 
...

<!ELEMENT FIRST_REOPENED (#PCDATA)> 
<!ELEMENT LAST_REOPENED (#PCDATA)> 
<!ELEMENT TIMES_REOPENED (#PCDATA)> 
...

Sample CSV Report

In the CSV report output we added First Reopened, Last Reopened and Times Reopened. We also moved the Date Last Fixed column to appear after Times Detected.

"Vuln Details + Reopened","04/12/2017 at 11:13:04 (GMT-0700)"
"Qualys, Inc.","1600 Bridge parkway","Redwood City","California","United States of America","94065"
"Patrick Slimmer","qualys_ps","Manager"

"IP","DNS","EC2 Instance ID","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","PCI Vuln","Ticket State","Instance","Non-running Kernel"
VM - Show Reopened Info in Vulnerability Detection API

The output for the Host List VM Detection API (/api/2.0/fo/asset/host/vm/detection) includes more information for vulnerabilities that have been reopened on a host:

FIRST_REOPENED_DATETIME is the date/time the vulnerability was first reopened.

LAST_REOPENED_DATETIME is the date/time the vulnerability was last reopened.

TIMES_REOPENED is the number of times the vulnerability has been reopened.

To see reopened information in the output, your API request must include the new input parameter show_reopened_info=1. Reopened information only appears for vulnerabilities that have been reopened. Not applicable to Information Gathered QIDs.

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&ips=10.10.10.11&show_reopened_info=1"

XML output:

In this example you’ll see reopened information for QID 38170.

```xml
...
<DETECTION_LIST>
  <DETECTION>
    <QID>38170</QID>
    <TYPE>Confirmed</TYPE>
    <SEVERITY>2</SEVERITY>
    <PORT>3389</PORT>
    <PROTOCOL>tcp</PROTOCOL>
    <SSL>1</SSL>
    <RESULTS><![CDATA[Certificate #0 CN=2k8r2-u-10-11 (2k8r2-u-10-11) doesn't resolve]]></RESULTS>
    <STATUS>Active</STATUS>
    <FIRST_FOUND_DATETIME>2016-08-01T07:31:48Z</FIRST_FOUND_DATETIME>
    <LAST_FOUND_DATETIME>2017-04-11T15:59:42Z</LAST_FOUND_DATETIME>
    <TIMESFOUND>199</TIMESFOUND>
    <LAST_TEST_DATETIME>2017-04-11T15:59:42Z</LAST_TEST_DATETIME>
    <LAST_UPDATE_DATETIME>2017-04-11T16:01:51Z</LAST_UPDATE_DATETIME>
    <LAST_FIXED_DATETIME>2017-03-27T16:32:08Z</LAST_FIXED_DATETIME>
  </DETECTION>
```

Qualys API Release Notes
VM - Show Reopened Info in Vulnerability Detection API

<FIRST_REOPENED_DATETIME>2016-11-25T16:22:31Z</FIRST_REOPENED_DATETIME>
<LAST_REOPENED_DATETIME>2017-03-28T15:38:57Z</LAST_REOPENED_DATETIME>
<TIMES_REOPENED>8</TIMES_REOPENED>
<IS_IGNORED>0</IS_IGNORED>
<IS_DISABLED>0</IS_DISABLED>
</DETECTION>

DTD update:
We added new reopened elements (in bold) to the Host List VM Detection Output DTD (host_list_vm_detection_output.dtd).
<!-- QUALYS HOST_LIST_VM_DETECTION_OUTPUT DTD -->
...
<!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?)>
...
<!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 WARNING (CODE?, TEXT, URL?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!-- EOF -->
VM - Detection API - Identify vulnerabilities related to running and non-running kernels

The existing parameter “active_kernels_only” helps you identify detections related to running and non-running Linux kernels. We’ve added a new `<AFFECT_RUNNING KERNEL>` tag to the output when “active_kernels_only” is set to 0, 1 or 2.

**active_kernels_only Parameter**

The behavior of the input parameter is described below.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[unspecified]</td>
<td>When unspecified, vulnerabilities are not filtered based on kernel activity. <code>&lt;AFFECT_RUNNING KERNEL&gt;</code> does not appear in the output for kernel related vulnerabilities.</td>
</tr>
<tr>
<td>active_kernels_only=0</td>
<td>Vulnerabilities are not filtered based on kernel activity. <code>&lt;AFFECT_RUNNING KERNEL&gt;</code> appears in the output for kernel related vulnerabilities.</td>
</tr>
<tr>
<td>active_kernels_only=1</td>
<td>Exclude vulnerabilities found on non-running Linux kernels. <code>&lt;AFFECT_RUNNING KERNEL&gt;</code> appears in the output for kernel related vulnerabilities.</td>
</tr>
<tr>
<td>active_kernels_only=2</td>
<td>Only include vulnerabilities found on non-running Linux kernels. <code>&lt;AFFECT_RUNNING KERNEL&gt;</code> appears in the output for kernel related vulnerabilities.</td>
</tr>
</tbody>
</table>

**<AFFECT_RUNNING KERNEL> values**

The value for `<AFFECT_RUNNING KERNEL>` will be:

1 if QID applies to a Running Kernel, or
0 if QID applies to a Non-Running Kernel

Sample API call with XML output

This sample shows `<AFFECT_RUNNING KERNEL>` tag for kernel related vulnerabilities. Value is 0 for 1st detection, 1 for 2nd, and blank (not shown) for 3rd.

**API request:**
curl -u "username:password" -H "X-Requested-With:curl demo2" -d "action=list&truncation_limit=50&ips=10.10.26.88&active_kernels_only=0" "https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/"
VM - Detection API - Identify vulnerabilities related to running and non-running kernels

**XML output:**

```xml
<DETECTION>
  <QID>119310</QID>
  <TYPE>Confirmed</TYPE>
  <SEVERITY>4</SEVERITY>
  <SSL>0</SSL>
  <RESULTS>
    <![CDATA[Package Installed Version Required Version
    kernel 2.6.32-71.29.1.el6.x86_64  2.6.32-131.2.1.el6
    kernel 2.6.32-131.0.15.el6.x86_64  2.6.32-131.2.1.el6
    kernel-devel 2.6.32-131.0.15.el6.x86_64  2.6.32-131.2.1.el6]]></RESULTS>
  <STATUS>Active</STATUS>
  <FIRST_FOUND_DATETIME>2016-02-25T20:09:55Z</FIRST_FOUND_DATETIME>
  <LAST_FOUND_DATETIME>2016-05-17T22:00:37Z</LAST_FOUND_DATETIME>
  <TIMES_FOUND>3</TIMES_FOUND>
  <LAST_TEST_DATETIME>2016-05-17T22:00:37Z</LAST_TEST_DATETIME>
  <LAST_UPDATE_DATETIME>2016-05-17T22:07:37Z</LAST_UPDATE_DATETIME>
  <IS_IGNORED>0</IS_IGNORED>
  <IS_DISABLED>0</IS_DISABLED>
  <AFFECT_RUNNING_KERNEL>0</AFFECT_RUNNING_KERNEL>
</DETECTION>

<DETECTION>
  <QID>122069</QID>
  <TYPE>Confirmed</TYPE>
  <SEVERITY>4</SEVERITY>
  <SSL>0</SSL>
  <RESULTS>
    <![CDATA[Package Installed Version Required Version
    kernel 2.6.32-71.29.1.el6.x86_64       2.6.32-431.17.1.el6
    kernel 2.6.32-279.el6.x86_64   2.6.32-431.17.1.el6
    kernel 2.6.32-131.0.15.el6.x86_64      2.6.32-431.17.1.el6
    kernel-devel    2.6.32-131.0.15.el6.x86_64      2.6.32-431.17.1.el6
    kernel-devel    2.6.32-279.el6.x86_64   2.6.32-431.17.1.el6
    kernel-firmware 2.6.32-279.el6.noarch   2.6.32-431.17.1.el6
    kernel-headers 2.6.32-279.el6.x86_64   2.6.32-431.17.1.el6]]></RESULTS>
  <STATUS>Active</STATUS>
  <FIRST_FOUND_DATETIME>2016-02-25T20:09:55Z</FIRST_FOUND_DATETIME>
  <LAST_FOUND_DATETIME>2016-05-17T22:00:37Z</LAST_FOUND_DATETIME>
  <TIMES_FOUND>3</TIMES_FOUND>
  <LAST_TEST_DATETIME>2016-05-17T22:00:37Z</LAST_TEST_DATETIME>
  <LAST_UPDATE_DATETIME>2016-05-17T22:00:37Z</LAST_UPDATE_DATETIME>
  <IS_IGNORED>0</IS_IGNORED>
  <IS_DISABLED>0</IS_DISABLED>
  <AFFECT_RUNNING_KERNEL>0</AFFECT_RUNNING_KERNEL>
</DETECTION>
```

Qualys API Release Notes 105
VM - Detection API - Identify vulnerabilities related to running and non-running kernels

<LAST_UPDATE_DATETIME>2016-05-17T22:07:45Z</LAST_UPDATE_DATETIME>
<IS_IGNORED>0</IS_IGNORED>
<IS_DISABLED>0</IS_DISABLED>
<TIMES_FOUND>3</TIMES_FOUND>
<AFFECT_RUNNING_KERNEL>1</AFFECT_RUNNING KERNEL>
</DETECTION>

<DETECTION>
  <QID>122088</QID>
  <TYPE>Confirmed</TYPE>
  <SEVERITY>3</SEVERITY>
  <SSL>0</SSL>
  <RESULTS><![CDATA[Package          Installed Version       Required Version
libxml2 2.7.6-4.el6_2.4.x86_64 2.7.6-14.el6_5.1
libxml2-python 2.7.6-4.el6_2.4.x86_64 2.7.6-14.el6_5.1]]></RESULTS>
  <STATUS>Active</STATUS>
  <FIRST_FOUND_DATETIME>2016-02-25T20:09:55Z</FIRST_FOUND_DATETIME>
  <LAST_FOUND_DATETIME>2016-05-17T22:00:37Z</LAST_FOUND_DATETIME>
  <LAST_TEST_DATETIME>2016-05-17T22:00:37Z</LAST_TEST_DATETIME>
  <LAST_UPDATE_DATETIME>2016-05-17T22:07:45Z</LAST_UPDATE_DATETIME>
  <IS_IGNORED>0</IS_IGNORED>
  <IS_DISABLED>0</IS_DISABLED>
  <TIMES_FOUND>3</TIMES_FOUND>
</DETECTION>

DTD update:
<base_url>/api/2.0/fo/asset/host/vm/detection/host_list_vm_detection_output.dtd

...
VM - Detection API - Identify vulnerabilities related to running and non-running kernels

Sample API call with CSV output

This sample shows one row of each type for “Affect Running Kernel”. Value is blank for 1st detection, 0 for 2nd, 1 for 3rd.

**API request:**
```
curl -u "username:password" -H "X-Requested-With:curl demo2" -d "action=list&truncation_limit=50&ips=10.10.31.98&active_kernels_only=0&output_format=CSV" "https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/
```

**CSV output:**
```
----BEGIN_RESPONSE_HEADER_CSV
----END_RESPONSE_HEADER_CSV
----BEGIN_RESPONSE_BODY_CSV
"Host ID","IP Address","Tracking Method","Network ID","Operating System","DNS Name","Netbios Name","QG HostID","Ec2 Instance ID","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","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","Affect Running Kernel"

"3036262","10.10.31.98","IP","0","Red Hat Enterprise Linux Server 6.3","","","","","2016-05-17T22:07:23Z","","","","","","","","","","","","","","","","","","","","","","","","","","","",0

"3036262","10.10.31.98","IP","0","Red Hat Enterprise Linux Server 6.3","","","","","2016-05-17T22:07:23Z","","","","","","","","","","","","","","","","","","","","","","","","","","","",1

"3036262","10.10.31.98","IP","0","Red Hat Enterprise Linux Server 6.3","","","","","2016-05-17T22:07:23Z","","","","","","","","","","","","","","","","","","","","","","","","","","","",2
```

Qualys API Release Notes
VM - Filter Detections Updated Before a Specific Date and Time

You can now filter the Host List VM Detection API (/api/2.0/fo/asset/host/vm/detection/) based on when the detection status was last updated.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| detection_updated_before=[value]       | (Optional) Show only detections whose detection status changed before a certain date and time. Valid date format is: YYYY-MMDD[THH:MM:SSZ] format (UTC/GMT), like “2017-02-15” or “2017-02-15T23:15:00Z”.

Tip: You can use this parameter in conjunction with the detection_updated_since parameter to limit the detections shown to a specific date range.

API request:
```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d "action=list&ips=10.10.10.37&show_igs=1&detection_updated_before=2017-01-12T06:33:46Z" "https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/"
```

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_list_vm_detection_output.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-02-21T09:37:05Z</DATETIME>
    <HOST_LIST>
      <HOST>
        <ID>5683411</ID>
        <IP>10.10.10.37</IP>
        <TRACKING_METHOD>IP</TRACKING_METHOD>
        <OS><![CDATA[MacOS X]]></OS>
        <LAST_SCAN_DATETIME>2017-01-17T06:30:29Z</LAST_SCAN_DATETIME>
        <LAST_VM_SCANNED_DATE>2017-01-17T06:30:29Z</LAST_VM_SCANNED_DATE>
        <LAST_VM_SCANNED_DURATION>182</LAST_VM_SCANNED_DURATION>
        <LAST_PC_SCANNED_DATE>2016-11-11T13:03:49Z</LAST_PC_SCANNED_DATE>
        <DETECTION_LIST>
          <DETECTION>
```

Qualys API Release Notes
<QID>6</QID>
<Type>Info</Type>
<RESULTS><![CDATA[IP address Host name 10.10.10.37 No registered hostname]]></RESULTS>
</DETECTION>

<Detection>
<QID>12488</QID>
<Type>Confirmed</Type>
<Severity>4</Severity>
<Port>22</Port>
<Protocol>tcp</Protocol>
<Ssl>0</Ssl>
<RESULTS><![CDATA[234881026 2547012 -rw-r--r-- 1 qualys admin 0 13865 Mar 22 17:31:52 2011
2007
Jul 23 01:13:16 2007
Feb 9 17:58:07 2011
Jul 23 01:13:16 2007
4096 32 0 /Applications/ColdFusion9/wwwroot/WEB-INF/exception/detail.cfm]]></RESULTS>
</DETECTION>
</DETECTION_LIST>
</HOST>
</HOST_LIST>
</RESPONSE>
VM - Editing vulnerabilities

A new API /api/2.0/fo/knowledge_base/vuln/ is introduced to edit, reset and then list the edited vulnerabilities in the Qualys Vulnerability KnowledgeBase.

Edit a vulnerability

You can change the severity level and/or add comments to Threat, Impact or Solution.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action=edit</td>
<td>(Required) The action required for the API request: edit. The POST method must be used.</td>
</tr>
<tr>
<td>qid={value}</td>
<td>(Required) QID of the vulnerability to be edited.</td>
</tr>
<tr>
<td>severity={value}</td>
<td>(Optional) Severity level between 1 to 5. Changing the severity level of a vulnerability impacts how the vulnerability appears in reports and how it is eventually prioritized for remediation. For example, by changing a vulnerability from a severity 2 to a severity 5, remediation tickets for the vulnerability could have a higher priority and shorter deadline for resolution.</td>
</tr>
<tr>
<td>disable={0</td>
<td>1}</td>
</tr>
<tr>
<td>threat_comment</td>
<td>(Optional) Threat comments in plain text.</td>
</tr>
<tr>
<td>impact_comment</td>
<td>(Optional) Impact comments in plain text.</td>
</tr>
<tr>
<td>solution_comment</td>
<td>(Optional) Solution comments in plain text.</td>
</tr>
</tbody>
</table>

Comments added for Threat, Impact, or Solution are appended to the service-provided descriptions in the vulnerability details within scan reports and other online views within your account.

Note: Providing at least one optional parameter is mandatory.

API request:

XML output:

```xml
<?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>2017-03-02T08:51:59Z</DATETIME>
    <TEXT>Custom Vuln Data has been updated successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>qid</KEY>
        <VALUE>27014</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

**Reset a vulnerability**

You can change the vulnerability settings back to original.

**New parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action=reset</td>
<td>(Required) The action required for the API request: reset. The POST method must be used.</td>
</tr>
<tr>
<td>qid=[value]</td>
<td>(Required) QID of the vulnerability to be reset.</td>
</tr>
</tbody>
</table>

**API request:**

```bash
```

XML output:

```xml
<?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>2017-03-02T08:55:11Z</DATETIME>
    <TEXT>Custom Vuln Data has been reset successfully</TEXT>
  </RESPONSE>
</SIMPLE_RETURN>
```
**List edited vulnerabilities**

You can list the vulnerabilities that are edited.

**New parameter:**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action=custom</td>
<td>(Required) The action required for the API request: custom. The GET or POST method should be used.</td>
</tr>
</tbody>
</table>

**API request:**

```bash
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST "action=custom" "https://qualysapi.qualys.com/api/2.0/fo/knowledge_base/vuln/"
```

**XML output:**

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE KB_CUSTOM_VULN_LIST_OUTPUT SYSTEM "https://qualysapi.qualys.com/api/2.0/fo/knowledge_base/vuln/kb_custom_vuln_list_output.dtd">
<KB_CUSTOM_VULN_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-03-02T08:47:52Z</DATETIME>
    <CUSTOM_VULN_LIST>
      <CUSTOM_VULN_DATA>
        <QID>27014</QID>
        <SEVERITY_LEVEL>5</SEVERITY_LEVEL>
        <ORIGINAL_SEVERITY_LEVEL>5</ORIGINAL_SEVERITY_LEVEL>
        <IS_DISABLED>1</IS_DISABLED>
        <UPDATED_DATETIME>2017-03-02T05:58:40Z</UPDATED_DATETIME>
        <UPDATED_BY>mr_md</UPDATED_BY>
        <THREAT_COMMENT>test threat123</THREAT_COMMENT>
        <IMPACT_COMMENT>test impact</IMPACT_COMMENT>
        <SOLUTION_COMMENT>sol123</SOLUTION_COMMENT>
      </CUSTOM_VULN_DATA>
    </CUSTOM_VULN_LIST>
  </RESPONSE>
</KB_CUSTOM_VULN_LIST_OUTPUT>
```
New DTD:
https://qualysapi.qualys.com/api/2.0/fo/knowledge_base/vuln/kb_custom_vuln_list_output.dtd

<!-- QUALYS KB_CUSTOM_VULN_LIST_OUTPUT DTD -->

<!ELEMENT KB_CUSTOM_VULN_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)>
<!ELEMENT POST_DATA (#PCDATA)>
<!ELEMENT RESPONSE (DATETIME, (CUSTOM_VULN_LIST)?, WARNING?)>
<!ELEMENT CUSTOM_VULN_LIST (CUSTOM_VULN_DATA*)>
<!ELEMENT CUSTOM_VULN_DATA (QID, SEVERITY_LEVEL, ORIGINAL_SEVERITY_LEVEL, IS_DISABLED, UPDATED_DATETIME, UPDATED_BY, THREAT_COMMENT?, IMPACT_COMMENT?, SOLUTION_COMMENT?)>
<!ELEMENT QID (#PCDATA)>
<!ELEMENT ORIGINAL_SEVERITY_LEVEL (#PCDATA)>
<!ELEMENT SEVERITY_LEVEL (#PCDATA)>
<!ELEMENT UPDATED_DATETIME (#PCDATA)>
<!ELEMENT THREAT_COMMENT (#PCDATA)>
<!ELEMENT IMPACT_COMMENT (#PCDATA)>
<!ELEMENT SOLUTION_COMMENT (#PCDATA)>
<!ELEMENT IS_DISABLED (#PCDATA)>
<!ELEMENT UPDATED_BY (#PCDATA)>
<!ELEMENT WARNING (CODE?, TEXT, URL?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!-- URL already defined -->
<!-- EOF -->
VM - EC2 asset information in scan report

EC2 asset information is now included in the scan report which makes it easy to identify the hosts that need patching. This information is included in the report only when the respective option is enabled in the template used for generating the report, and the results are sorted by host.

Scan report will now include the following EC2 asset information:

- Public DNS Name
- Image Id
- VPC Id
- Instance State
- Private DNS Name
- Instance Type

API request:


CSV output:

"IP","DNS","EC2 Instance ID","NetBIOS","QG Host ID","IP Interfaces","Public Hostname","Image ID","VPC ID","Instance State","Private Hostname","Instance Type","Tracking Method","OS","IP Status","QID","Title","Vuln Status","Type","Severity","Port","Protocol","FQDN","SSL","First Detected","Last Detected","Times Detected","Date Last Fixed","CVE ID","Vendor Reference","Bugtraq ID","Results","PCI Vuln","Ticket State","Instance","Category","Associated Tags","10.90.2.100","ip-10-90-2-100.ec2.internal","l-0b68f500c10e6a3c0","","ec2-52-85-152-105.compute-1.amazonaws.com","ami-2d4ed53a","vpc-1e37cd76","RUNNING","ip-10-90-2-100.ec2.internal","t2.medium","EC2","Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP","host scanned, found vuln","34011","Firewall"

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>10.90.2.30</IP>
  <TRACKING_METHOD></TRACKING_METHOD>
  <ASSET_TAGS>
    <ASSET_TAG><![CDATA[EC2]]></ASSET_TAG>
    <ASSET_TAG><![CDATA[TG1]]></ASSET_TAG>
    <ASSET_TAG><![CDATA[Virginia]]></ASSET_TAG>
    <ASSET_TAG><![CDATA[agec2]]></ASSET_TAG>
  </ASSET_TAGS>
  <DNS><![CDATA[ip-10-90-2-30.ec2.internal]]></DNS>
  <EC2_INSTANCE_ID><![CDATA[i-0b11bd19771f17ed]]></EC2_INSTANCE_ID>
  <EC2_INFO>
    <PUBLIC_DNS_NAME><![CDATA[ec2-184-73-79-113.compute-1.amazonaws.com]]></PUBLIC_DNS_NAME>
    <IMAGE_ID><![CDATA[ami-2d4ed53a]]></IMAGE_ID>
    <VPC_ID><![CDATA[vpc-1e37cd76]]></VPC_ID>
    <INSTANCE_STATE><![CDATA[RUNNING]]></INSTANCE_STATE>
    <PRIVATE_DNS_NAME><![CDATA[ip-10-90-2-30.ec2.internal]]></PRIVATE_DNS_NAME>
    <INSTANCE_TYPE><![CDATA[t2.medium]]></INSTANCE_TYPE>
  </EC2_INFO>
</HOST>
VM - EC2 asset information in scan report

**DTD update:**
https://qualysapi.qualys.com/asset_data_report.dtd

```xml
<!-- 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?, EC2_INSTANCE_ID?,
IP_INTERFACES?, EC2_INFO?, OPERATING_SYSTEM?,
OS_CPE?, ASSET_GROUPS?, VULN_INFO_LIST?)>)>
...
<!ELEMENT EC2_INSTANCE_ID (#PCDATA)>  
<!ELEMENT IP_INTERFACES (IP*)>  
<!ELEMENT EC2_INFO
(PUBLIC_DNS_NAME?, IMAGE_ID?, VPC_ID?, INSTANCE_STATE?, PRIVATE_DNS_NAME?, INST
ANCE_TYPE?)>
<!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 OPERATING_SYSTEM (#PCDATA)>  
<!ELEMENT OS_CPE (#PCDATA)>  
<!ELEMENT ASSET_GROUPS (ASSET_GROUP_TITLE+)>
<!ELEMENT VULN_INFO_LIST (VULN_INFO+)>
```
VM - Scan Report in XML Format - Ability to Exclude Glossary data

This update applies to the Scan Report in XML format only. Previously the <GLOSSARY> tag was always included in the scan report XML format regardless of template sub option settings under Vulnerability Details (e.g. Threat, Impact, Solution - Patches and Workarounds, etc). Now you can exclude the <GLOSSARY> tag and this will reduce the size of your reports.

What are the changes?
- the <GLOSSARY> tag will be excluded from the XML format if none of the “Vulnerability Details” sub options are selected
- the <GLOSSARY> tag will be included in the XML format if any one of the “Vulnerability Details” sub options is selected
- the Scan Report DTD (asset_data_report.dtd) has been updated; the QID “id” attribute changed from IDREF to CDATA

Sample Scan Report XML without <GLOSSARY> tag

This Scan Report in XML format was generated using a scan report template with no Vulnerability Details sub options selected. You’ll notice there’s no <GLOSSARY> tag after </HOST_LIST>.

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

<!DOCTYPE ASSET_DATA_REPORT SYSTEM "https://qualysapi.qualys.com/asset_data_report.dtd">
<ASSET_DATA_REPORT>
  <HEADER>
    <COMPANY><![CDATA[Acme, Inc.]]></COMPANY>
    <USERNAME>acme_ak1</USERNAME>
    <GENERATION_DATETIME>2017-03-29T19:34:21Z</GENERATION_DATETIME>
    <TEMPLATE><![CDATA[My Report Template w/o Vulnerability Details]]></TEMPLATE>
  </HEADER>
  <TARGET>
    <USER_IP_LIST>
      <RANGE>
        <START>10.10.24.77</START>
        <END>10.10.24.77</END>
      </RANGE>
    </USER_IP_LIST>
    <COMBINED_IP_LIST>
      <RANGE>
        <START>10.10.24.77</START>
        <END>10.10.24.77</END>
      </RANGE>
    </COMBINED_IP_LIST>
  </TARGET>
  <RISK_SCORE_SUMMARY>
    <TOTAL_VULNERABILITIES>11</TOTAL_VULNERABILITIES>
    <AVG_SECURITY_RISK>3.1</AVG_SECURITY_RISK>
    <BUSINESS_RISK>17/100</BUSINESS_RISK>
  </RISK_SCORE_SUMMARY>
</ASSET_DATA_REPORT>

<HOSTS>
  <IP_ADDRESS>10.10.24.77</IP_ADDRESS>
  <TOTAL_VULNERABILITIES>11</TOTAL_VULNERABILITIES>
  <SECURITY_RISK>3.1</SECURITY_RISK>
</HOSTS>

<HOST>
  <IP>10.10.24.77</IP>
  <TRACKING_METHOD>IP</TRACKING_METHOD>
  <DNS><![CDATA[2k3x64ie7-24-77.patch.ad.acme.com]]></DNS>
  <NETBIOS><![CDATA[2K3X64IE7-24-77]]></NETBIOS>
  <OPERATING_SYSTEM><![CDATA[Windows 2003 R2 Service Pack 1]]></OPERATING_SYSTEM>
</HOST>

<ASSET_GROUPS>
  <ASSET_GROUP_TITLE><![CDATA[AG 24]]></ASSET_GROUP_TITLE>
</ASSET_GROUPS>

<VULN_INFO_LIST>
  <VULN_INFO>
    <QID id="qid_90783">90783</QID>
    <TYPE>Vuln</TYPE>
  </VULN_INFO>
</VULN_INFO_LIST>
<SSL>false</SSL>
<FIRST_FOUND>2017-01-09T19:34:34Z</FIRST_FOUND>
<LAST_FOUND>2017-01-09T19:34:34Z</LAST_FOUND>
<TIMES_FOUND>1</TIMES_FOUND>
<VULN_STATUS>New</VULN_STATUS>
</VULN_INFO>
<VULN_INFO>
<QID id="qid_105500">105500</QID>
<TYPE>Vuln</TYPE>
<SSL>false</SSL>
<FIRST_FOUND>2017-01-09T19:34:34Z</FIRST_FOUND>
<LAST_FOUND>2017-01-09T19:34:34Z</LAST_FOUND>
<TIMES_FOUND>1</TIMES_FOUND>
<VULN_STATUS>New</VULN_STATUS>
</VULN_INFO>
<VULN_INFO>
<QID id="qid_90464">90464</QID>
<TYPE>Vuln</TYPE>
<SSL>false</SSL>
<FIRST_FOUND>2017-01-09T19:34:34Z</FIRST_FOUND>
<LAST_FOUND>2017-01-09T19:34:34Z</LAST_FOUND>
<TIMES_FOUND>1</TIMES_FOUND>
<VULN_STATUS>New</VULN_STATUS>
</VULN_INFO>
Scan Report DTD

The Scan Report DTD (asset_data_report.dtd) was updated. Specifically the “id” attribute for the QID element was changed from IDREF to CDATA.

id attribute prior to Qualys 8.10:

```xml
<!ELEMENT QID (#PCDATA>)
<!ATTLIST QID id IDREF #REQUIRED>
```

id attribute for Qualys 8.10:

```xml
<!ELEMENT QID (#PCDATA>)
<!ATTLIST QID id CDATA #REQUIRED>
```
**VM - Hide target information from scan list**

You can now use the ignore_target parameter to hide the target information returned by the scan list API api/2.0/fo/scan.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ignore_target=[0</td>
<td>1]</td>
</tr>
</tbody>
</table>

**API request:**

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

**XML output:**

```xml
<?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>2017-03-21T05:47:59Z</DATETIME>
    <SCAN_LIST>
      <SCAN>
        <REF>scan/1487758254.03044</REF>
        <TYPE>On-Demand</TYPE>
        <TITLE><![CDATA[FF1]]></TITLE>
        <USER_LOGIN>netwr_ne</USER_LOGIN>
        <LAUNCH_DATETIME>2017-02-22T10:10:54Z</LAUNCH_DATETIME>
        <DURATION>N/A</DURATION>
        <PROCESSING_PRIORITY>0 - No Priority</PROCESSING_PRIORITY>
        <PROCESSED>0</PROCESSED>
        <STATUS>
          <STATE>Error</STATE>
        </STATUS>
      </SCAN>
    </SCAN_LIST>
  </RESPONSE>
</SCAN_LIST_OUTPUT>
```

**DTD update:**

https://qualysapi.qualys.com/api/2.0/fo/scan/scan_list_output.dtd

```xml
<!DOCTYPE SCAN_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/scan_list_output.dtd">
</DOCTYPE>
```

Qualys API Release Notes
<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POST_DATA?)>
...<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be urlencoded -->
<![ELEMENT POST_DATA (#PCDATA)>
<![ELEMENT RESPONSE (DATETIME, SCAN_LIST?)>
<![ELEMENT SCAN_LIST (SCAN+)>
<![ELEMENT SCAN (ID?, REF, TYPE, TITLE, USER_LOGIN, LAUNCH_DATETIME, DURATION, PROCESSING_PRIORITY?, PROCESSED, STATUS?, TARGET?, ASSET_GROUP_TITLE_LIST?, OPTION_PROFILE?)>
...<!ELEMENT STATE (#PCDATA)>
<![ELEMENT SUB_STATE (#PCDATA)>
<![ELEMENT TARGET (#PCDATA)>
<![ELEMENT ASSET_GROUP_TITLE_LIST (ASSET_GROUP_TITLE+)>
<![ELEMENT ASSET_GROUP_TITLE (#PCDATA)>
<![ELEMENT OPTION_PROFILE (TITLE, DEFAULT_FLAG?)>
<![ELEMENT DEFAULT_FLAG (#PCDATA)>
<!-- EOF -->
VM - New tag added to KnowledgeBase API

We added a new element called AUTOMATIC_PCI_FAIL to the DTDs for the KnowledgeBase API (/api/2.0/fo/knowledge_base/vuln/) and the KnowledgeBase Download API (/msp/knowledgebase_download.php).

Note - This new element is for internal use only.

KnowledgeBase API

DTD updated: knowledge_base_vuln_list_output.dtd

...
<!ELEMENT VULN_LIST (VULN*)>
   <!ELEMENT VULN (QID, VULN_TYPE, SEVERITY_LEVEL, TITLE, CATEGORY?,
               DETECTION_INFO?, LAST_CUSTOMIZATION?,
               LAST_SERVICE_MODIFICATION_DATETIME?, PUBLISHED_DATETIME,
               BUGTRAQ_LIST?, PATCHABLE, SOFTWARE_LIST?, VENDOR_REFERENCE_LIST?,
               CVE_LIST?, DIAGNOSIS?, DIAGNOSIS_COMMENT?, CONSEQUENCE?,
               CONSEQUENCE_COMMENT?, SOLUTION?, SOLUTION_COMMENT?,
               COMPLIANCE_LIST?, CORRELATION?, CVSS?, CVSS_V3?, PCI_FLAG?,
               AUTOMATIC_PCI_FAIL?, PCI_REASONS?, THREAT_INTELLIGENCE?,
               SUPPORTED_MODULES?, DISCOVERY, IS_DISABLED?)>
...
<!ELEMENT AUTOMATIC_PCI_FAIL (#PCDATA)>
...

KnowledgeBase Download API

DTD updated: knowledgebase_download.dtd

...
<!ELEMENT VULN (QID, VULN_TYPE, SEVERITY_LEVEL, TITLE, CATEGORY?,
               DETECTION_INFO?, LAST_UPDATE?, BUGTRAQ_ID_LIST?, PATCHABLE,
               VENDOR_REFERENCE_LIST?, CVE_ID_LIST?, DIAGNOSIS?, CONSEQUENCE?,
               SOLUTION?, COMPLIANCE?, CORRELATION?, CVSS_BASE?, CVSS_TEMPORAL?,
               CVSS3_BASE?, CVSS3_TEMPORAL?, CVSS_ACCESS_VECTOR?,
               CVSS_ACCESS_COMPLEXITY?, CVSS_AUTHENTICATION?,
               CVSS_CONFIDENTIALITY_IMPACT?, CVSS_INTEGRITY_IMPACT?,
               CVSS_AVAILABILITY_IMPACT?, CVSS_EXPLOITABILITY?, CVSS_REMEDIATION_LEVEL?,
               CVSS_REPORT_CONFIDENCE?, PCI_FLAG?, AUTOMATIC_PCI_FAIL?, PCI_REASONS?,
               THREAT_INTELLIGENCE?, SUPPORTED_MODULES?, DISCOVERY, IS_DISABLED?)>
...
<!ELEMENT AUTOMATIC_PCI_FAIL (#PCDATA)>
...
PC - Remediation Information Displayed in PC Reports

Remediation information is now displayed in XML and CSV output formats for PC reports.

We have updated the Report API to include remediation information in XML and CSV formats for PC reports.

Report launch API request:

curl -H "X-Requested-With: curl" -u "USERNAME:PASSWORD" -X POST -d "policy_id=131345&ips=10.10.10.10, 10.10.30.129, 10.10.30.229, 10.10.30.231, 10.11.65.194-10.11.65.195&template_id=89178&output_format=xml" "https://qualysapi.qualys.com/api/2.0/fo/report/?action=launch"

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>2017-04-03T10:16:13Z</DATETIME>
    <TEXT>New report launched</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>153007</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>

Report fetch API request:

Use the Id returned in the Report launch API output for the Report fetch API request.


XML output:

<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE COMPLIANCE_POLICY_REPORT SYSTEM "https://qualysapi.qualys.com/compliance_policy_report.dtd">
<COMPLIANCE_POLICY_REPORT>
  <HEADER>
    <NAME><![CDATA[Template with all 3 Remediation Data]]></NAME>
    <GENERATION_DATETIME>2017-04-03T10:16:19Z</GENERATION_DATETIME>
    <COMPANY_INFO>...
      <INSTANCE><![CDATA[os]]></INSTANCE>
      <STATUS><![CDATA[Passed]]></STATUS>
      <REMEDIATION>Configure the policy value for User Configuration &gt; Administrative Templates &gt; Windows Components &gt; Attachment Manager &gt; "Notify antivirus programs when opening attachments" to "Enabled".</REMEDIATION>
    </TECHNOLOGY>
    <INSTANCIE><![CDATA[os]]></INSTANCIE>
    <STATUS><![CDATA[Passed]]></STATUS>
    <REMEDIATION>To establish the recommended configuration via GP, set the following UI path to RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Configure encryption types allowed for Kerberos</REMEDIATION>
    <TECHNOLOGY>
      <ID><![CDATA[37]]></ID>
      <NAME>Windows 7</NAME>
    </TECHNOLOGY>
    ...
  </INSTANCIE>
  </RESULTS>
</COMPLIANCE_POLICY_REPORT>

DTD Update:
<?xml version="1.0" encoding="UTF-8"?>
<!-- QUALYS COMPLIANCE POLICY REPORT DTD -->
<!-- $Revision$ -->
<!ELEMENT COMPLIANCE_POLICY_REPORT (ERROR | (HEADER, (SUMMARY), (RESULTS)))>
<!ELEMENT ERROR (#PCDATA)>
<!ATTLIST ERROR number CDATA #IMPLIED>
...
<!ELEMENT CONTROL_LIST (CONTROL*)>
PC - Remediation Information Displayed in PC Reports

<!ELEMENT CID (#PCDATA)>
<!ELEMENT STATEMENT (#PCDATA)>
<!ELEMENT CONTROL_REFERENCES (#PCDATA)>
<!ELEMENT RATIONALE (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT REMEDIATION (#PCDATA)>
<!ELEMENT TECHNOLOGY (ID, NAME)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT EVALUATION_DATE (#PCDATA)>
<!ELEMENT INSTANCE (#PCDATA)>
...
<!ELEMENT STATS (#PCDATA)>
<!ELEMENT SEARCH_DURATION (#PCDATA)>
<!ELEMENT ERRORS (#PCDATA)>
**PC - New API Support for Docker Authentication**

We now support compliance scans for Docker versions from 1.9 to 1.12, running on Linux hosts. Unix authentication is required so you’ll also need a Unix record for the host running the docker.

This record type is only available in accounts with PC (Policy Compliance) and only supported for compliance scans.

We have added new authentication API (/api/2.0/fo/auth/docker/) to support the new record type. Actions supported by the API are: Create, Update, List, Delete.

The auth_records.dtd is also updated to add the AUTH_DOCKER_IDS element.

**Docker API**

You can now create, update, list and delete Docker authentication records.

**Create Docker Authentication Record**

Use the parameter “action=create” to create a new record in your account.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>title={value}</td>
<td>(Required) The record title.</td>
</tr>
<tr>
<td>echo_request=[0</td>
<td>1]</td>
</tr>
<tr>
<td></td>
<td>parameters (names and values) in the XML output. When</td>
</tr>
<tr>
<td></td>
<td>not specified, parameters are not included in the XML</td>
</tr>
<tr>
<td></td>
<td>output. Specify 1 to view parameters in the XML output.</td>
</tr>
<tr>
<td>comments={value}</td>
<td>(Optional) User defined comments.</td>
</tr>
<tr>
<td>docker_deamon_conf_file={value}</td>
<td>(Optional) Location of the configuration file for the docker daemon.</td>
</tr>
<tr>
<td>docker_command={value}</td>
<td>(Optional) The docker command to connect to a local docker daemon.</td>
</tr>
<tr>
<td>ips={value}</td>
<td>(Required) IPs to add to your docker record.</td>
</tr>
<tr>
<td>network_id=[1</td>
<td>0]</td>
</tr>
</tbody>
</table>

**API request:**

curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl demo" -d "action=create&title=docker_sample&ips=10.10.30.159&docker_deamon_conf_file=/etc/docker/daemon.json&docker_command=/usr/bin/docker&echo_request=1" "https://qualysapi.qualys.com/api/2.0/fo/auth/docker/"
PC - New API Support for Docker Authentication

XML output:

```xml
<?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>2017-03-09T06:09:46Z</DATETIME>
    <USER_LOGIN>username</USER_LOGIN>
    <RESOURCE>https://qualysapi.qualys.com/api/2.0/fo/auth/docker/</RESOURCE>
    <PARAM_LIST>
      <PARAM>
        <KEY>action</KEY>
        <VALUE>create</VALUE>
      </PARAM>
      <PARAM>
        <KEY>title</KEY>
        <VALUE>docker_sample</VALUE>
      </PARAM>
      <PARAM>
        <KEY>ips</KEY>
        <VALUE>10.10.30.159</VALUE>
      </PARAM>
      <PARAM>
        <KEY>docker_deamon_conf_file</KEY>
        <VALUE>/etc/docker/daemon.json</VALUE>
      </PARAM>
      <PARAM>
        <KEY>docker_command</KEY>
        <VALUE>/usr/bin/docker</VALUE>
      </PARAM>
      <PARAM>
        <KEY>echo_request</KEY>
        <VALUE>1</VALUE>
      </PARAM>
    </PARAM_LIST>
  </REQUEST>
  <RESPONSE>
    <DATETIME>2017-03-09T06:09:46Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>72685</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```
Update Docker Authentication Record

Use the parameter “action=update” to update a Docker authentication record in your account. You’ll need to include the ID for the record you’re updating.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>title={value}</td>
<td>(Optional) The record title.</td>
</tr>
<tr>
<td>echo_request={0</td>
<td>1}</td>
</tr>
<tr>
<td>comments={value}</td>
<td>(Optional) User defined comments.</td>
</tr>
<tr>
<td>docker_deamon_conf_file= {value}</td>
<td>(Optional) Location of the configuration file for the docker daemon.</td>
</tr>
<tr>
<td>docker_command={value}</td>
<td>(Optional) The docker command to connect to a local docker daemon.</td>
</tr>
<tr>
<td>network_id={1</td>
<td>0}</td>
</tr>
<tr>
<td>ids={value}</td>
<td>(Required) ID of the record you’re updating.</td>
</tr>
<tr>
<td>add_ips={value}</td>
<td>(Optional) IPs to be added to your record.</td>
</tr>
<tr>
<td>remove_ips={value}</td>
<td>(Optional) IPs to be removed from your record.</td>
</tr>
</tbody>
</table>

**API request:**


**XML output:**

```xml
<?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>2017-03-09T06:12:57Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>72685</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```
Delete Docker Authentication Record

Use the parameter “action=delete” and specify the ID of the Docker authentication record to delete its details.

**Parameter** | **Description**
--- | ---
`echo_request=[0|1]` | (Optional) Specifies whether to echo the request’s input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.

`ids=[value]` | (Required) ID of the record you’re deleting.

**API request:**

```bash
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl demo" -d "action=delete&ids=72685" "https://qualysapi.qualys.com/api/2.0/fo/auth/docker/
```

**XML output:**

```xml
<?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>2017-03-09T06:13:57Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Deleted</TEXT>
        <ID_SET>
          <ID>72685</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```
List Authentication Record

Use the parameter “action=list” to list the record defined in your account. To view a specific Docker record, specify the ID or title of the record.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>title={value}</td>
<td>(Optional) The record title.</td>
</tr>
<tr>
<td>echo_request=[0</td>
<td>1]</td>
</tr>
<tr>
<td>comments={value}</td>
<td>(Optional) User defined comments.</td>
</tr>
<tr>
<td>ids={value}</td>
<td>(Optional) ID of the record you’re listing.</td>
</tr>
<tr>
<td>id_min={value}</td>
<td>(Optional) Show only those authentication records in your subscription that have an ID number greater than or equal to an ID number you specify.</td>
</tr>
<tr>
<td>id_max={value}</td>
<td>(Optional) Show only those authentication records in your subscription that have an ID number less than or equal to an ID number you specify.</td>
</tr>
</tbody>
</table>

**API request:**

curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl demo" -d "action=list&ids=72685" "https://qualysapi.qualys.com/api/2.0/fo/auth/docker/"

**XML output:**

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_DOCKER_LIST_OUTPUT SYSTEM "https://qualysapi.qualys.com/api/2.0/fo/auth/docker/auth_docker_list_output.dtd">
<AUTH_DOCKER_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-03-09T06:11:39Z</DATETIME>
    <AUTH_DOCKER_LIST>
      <AUTH_DOCKER>
        <ID>72685</ID>
        <TITLE><![CDATA[docker_sample]]></TITLE>
      </AUTH_DOCKER>
      <DAEMON_CONFIGURATION_FILE>/etc/docker/daemon.json</DAEMON_CONFIGURATION_FILE>
      <DOCKER_COMMAND>/usr/bin/docker</DOCKER_COMMAND>
      <IP_SET>
        <IP>10.10.30.159</IP>
      </IP_SET>
    </AUTH_DOCKER_LIST>
  </RESPONSE>
</AUTH_DOCKER_LIST_OUTPUT>
```
PC - New API Support for Docker Authentication

<CREATED>
  <DATETIME>2017-03-09T06:09:46Z</DATETIME>
  <BY>username</BY>
</CREATED>

<LAST_MODIFIED>
  <DATETIME>2017-03-09T06:09:46Z</DATETIME>
</LAST_MODIFIED>

<AUTH_DOCKER>
  /AUTH_DOCKER_LIST
</AUTH_DOCKER_LIST>
</RESPONSE>
</AUTH_DOCKER_LIST_OUTPUT>

New DTD:

<!-- QUALYS AUTH_DOCKER_LIST_OUTPUT DTD -->
<!-- $Revision: $ -->
<!ELEMENT AUTH_DOCKER_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_DOCKER_LIST|ID_SET)?, WARNING_LIST?, GLOSSARY?)>  
<!ELEMENT AUTH_DOCKER_LIST (AUTH_DOCKER+)>  

<!ELEMENT AUTH_DOCKER (ID, TITLE, DAEMON_CONFIGURATION_FILE?, DOCKER_COMMAND?, IP_SET, NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)>  
<!ELEMENT ID (#PCDATA)>  
<!ELEMENT TITLE (#PCDATA)>  
<!ELEMENT DAEMON_CONFIGURATION_FILE (#PCDATA)>  
<!ELEMENT DOCKER_COMMAND (#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)>
PC - New API Support for Docker Authentication

<!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 -->

DTD Update:

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

...  
...  
...  
<!ELEMENT AUTH_DOCKER_IDS (ID_SET)>  
<!ELEMENT AUTH_ORACLE_WEBLOGIC_IDS (ID_SET)>  

<!ELEMENT AUTH_DOCKER_IDS (ID_SET)>  

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

<!-- EOF -->
PC - New API Support for PostgreSQL Authentication

With this release PostgreSQL authentication is supported for compliance scans using Qualys PC. The PostgreSQL Record API (/api/2.0/fo/auth/postgresql/) allows you manage PostgreSQL records for performing authenticated scans of PostgreSQL Version 9.0 instances running on Unix.

Tip - We strongly recommend you create one or more dedicated user accounts to be used solely by the Qualys Cloud Platform to authenticate to PostgreSQL database instances.

List all record types

Supported parameters for Authentication Record List API call (/api/2.0/fo/auth/?action=list) are described in the current Qualys API V2 User Guide under Authentication Record List (in Chapter 8).

API request:

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

XML output:

```xml
<?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>2017-04-12T18:43:57Z</DATETIME>
<AUTH_RECORDS>
<AUTH_UNIX_IDS>
<ID_SET>
<ID>1003</ID>
<ID>78176</ID>
</ID_SET>
</AUTH_UNIX_IDS>
<AUTH_WINDOWS_IDS>
<ID_SET>
<ID>5325</ID>
<ID_RANGE>34902-34909</ID_RANGE>
<ID>35076</ID>
<ID>79233</ID>
</ID_SET>
</AUTH_WINDOWS_IDS>
<AUTH_SYBASE_IDS>
>ID_SET>
<ID>77260</ID>
</ID_SET>
</AUTH_SYBASE_IDS>
```
PC - New API Support for PostgreSQL Authentication

<AUTH_POSTGRESQL_IDS>
  <ID_SET>
    <ID>78148</ID>
    <ID>78153</ID>
    <ID_RANGE>78166-78167</ID_RANGE>
    <ID>78171</ID>
  </ID_SET>
</AUTH_POSTGRESQL_IDS>

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

New AUTH_POSTGRESQL_IDS element identifies PostgreSQL record IDs.

<!-- QUALYS AUTH_RECORDS_OUTPUT DTD -->
<!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)>  
<!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_ID?, AUTH_IBMDB2_ID?, AUTH_VMWARE_ID?, AUTH_MS_IIS_ID?, 
  AUTH_APACHE_ID?, AUTH_IBMWEBSPHERE_ID?, AUTH_HTTP_ID?, 
  AUTH_SYBASE_ID?, AUTH_MYSQL_ID?, AUTH_TOMCAT_ID?, 
  AUTH_ORACLE_WEBLOGIC_ID?, AUTHDOCKER_ID?, AUTH_POSTGRESQL_ID?)>

<!ELEMENT AUTH_UNIX_IDS (ID_SET)>  
<!ELEMENT AUTH_WINDOWS_IDS (ID_SET)>
List PostgreSQL records

Supported parameters for PostgreSQL Authentication Record List API call
(`/api/2.0/fo/auth/postgresql/?action=list`) are described in the current Qualys API V2
User Guide under Authentication Record List by Type (in Chapter 8).

Example: List PostgreSQL records

API request:
```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d "action=list&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/auth/postgresql/" > file.xml
```

XML output:
```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_POSTGRESQL_LIST_OUTPUT SYSTEM "https://qualysapi.qualys.com/api/2.0/fo/auth/postgresql/auth_postgresql_list_output.dtd">
```
<AUTH_POSTGRESQL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-04-24T22:01:50Z</DATETIME>
    <AUTH_POSTGRESQL_LIST>
      <AUTH_POSTGRESQL>
        <ID>79518</ID>
        <TITLE><![CDATA[PostgresSQL1]]></TITLE>
        <USERNAME><![CDATA[acme_as1]]></USERNAME>
        <DATABASE><![CDATA[mydb1]]></DATABASE>
        <PORT>5432</PORT>
        <SSL_VERIFY><![CDATA[0]]></SSL_VERIFY>
        <IP_SET>
          <IP>10.10.10.45</IP>
        </IP_SET>
        <UNIX_CONF_FILE><![CDATA[/var/lib/pgsql/9.3/data/postgresql.conf]]></UNIX_CONF_FILE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2017-04-13T23:42:50Z</DATETIME>
          <BY>acme_as1</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2017-04-20T23:35:42Z</DATETIME>
        </LAST_MODIFIED>
        <COMMENTS><![CDATA[my comments]]></COMMENTS>
      </AUTH_POSTGRESQL>
      <AUTH_POSTGRESQL>
        <ID>82110</ID>
        <TITLE><![CDATA[POstgreSQL2]]></TITLE>
        <USERNAME><![CDATA[acme_as1]]></USERNAME>
        <DATABASE><![CDATA[mydb2]]></DATABASE>
        <PORT>5432</PORT>
        <SSL_VERIFY><![CDATA[1]]></SSL_VERIFY>
        <HOSTS>
          <HOST><![CDATA[cent-31-107.ml2k8.vuln.qa.qualys.com]]></HOST>
        </HOSTS>
        <IP_SET>
          <IP>10.20.31.107</IP>
        </IP_SET>
        <UNIX_CONF_FILE><![CDATA[/var/lib/pgsql/9.3/data/postgresql.conf]]></UNIX_CONF_FILE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2017-04-20T20:12:48Z</DATETIME>
          <BY>acme_as1</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2017-04-20T21:53:25Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_POSTGRESQL>
    </AUTH_POSTGRESQL_LIST>
  </RESPONSE>
</AUTH_POSTGRESQL_LIST_OUTPUT>
PC - New API Support for PostgreSQL Authentication

</AUTH_POSTGRESQL>

<AUTH_POSTGRESQL>
  <ID>82111</ID>
  <TITLE><![CDATA[PostgreSQL3]]></TITLE>
  <USERNAME><![CDATA[acme_as1]]></USERNAME>
  <DATABASE><![CDATA[mydb3]]></DATABASE>
  <PORT>5432</PORT>
  <SSL_VERIFY><![CDATA[1]]></SSL_VERIFY>
  <IP_SET>
    <IP>10.10.10.10</IP>
  </IP_SET>
  <UNIX_CONF_FILE><![CDATA[]]></UNIX_CONF_FILE>
  <NETWORK_ID>0</NETWORK_ID>
  <CREATED>
    <DATETIME>2017-04-20T20:59:28Z</DATETIME>
    <BY>acme_as1</BY>
  </CREATED>
  <LAST_MODIFIED>
    <DATETIME>2017-04-21T16:58:47Z</DATETIME>
  </LAST_MODIFIED>
</AUTH_POSTGRESQL>

...</AUTH_POSTGRESQL_LIST>
</RESPONSE>
</AUTH_POSTGRESQL_LIST_OUTPUT>

DTD:
<base_url>/api/2.0/fo/auth/sysbase/auth_postgresql_list_output.dtd

<!-- QUALYS AUTH_POSTGRESQL_LIST_OUTPUT DTD -->
<!ELEMENT AUTH_POSTGRESQL_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)>
<!ELEMENT POST_DATA (#PCDATA)>
<!ELEMENT RESPONSE (DATETIME, (AUTH_POSTGRESQL_LIST|ID_SET)?, WARNING_LIST?, GLOSSARY?)>
<!ELEMENT AUTH_POSTGRESQL_LIST (AUTH_POSTGRESQL+)>
<!ELEMENT AUTH_POSTGRESQL (ID, TITLE, USERNAME, DATABASE, PORT, SSL_VERIFY, HOSTS?, IP_SET?, LOGIN_TYPE?, DIGITAL_VAULT?, UNIX_CONF_FILE, PRIVATE_KEY_CERTIFICATE_LIST?, NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>

Qualys API Release Notes 139
PC - New API Support for PostgreSQL Authentication

<\!ELEMENT TITLE (#PCDATA)>
<\!ELEMENT USERNAME (#PCDATA)>
<\!ELEMENT PRIVATE_KEY_CERTIFICATE_LIST (PRIVATE_KEY_CERTIFICATE)*>

<\!ELEMENT PRIVATE_KEY_CERTIFICATE (ID, PRIVATE_KEY_INFO, PASSPHRASE_INFO, CERTIFICATE?)>+
<\!ELEMENT PRIVATE_KEY_INFO (PRIVATE_KEY|DIGITAL_VAULT)>
<\!ATTLIST PRIVATE_KEY_INFO>
<!-- Private key contents will never be rendered -->
<\!ELEMENT PRIVATE_KEY EMPTY>
<\!ELEMENT PASSPHRASE_INFO (DIGITAL_VAULT?)>
<\!ATTLIST PASSPHRASE_INFO type (basic|vault) "basic""
<!-- Certificate contents will never be rendered -->
<\!ELEMENT CERTIFICATE EMPTY>

<\!ELEMENT PORT (#PCDATA)>
<\!ELEMENT DATABASE (#PCDATA)>
<\!ELEMENT SSL_VERIFY (#PCDATA)>
<\!ELEMENT HOSTS (HOST+)>
<\!ELEMENT HOST (#PCDATA)>
<\!ELEMENT IP_SET (IP|IP_RANGE)+
<\!ELEMENT IP (#PCDATA)>
<\!ELEMENT IP_RANGE (#PCDATA)>
<\!ELEMENT LOGIN_TYPE (#PCDATA)>
<\!ELEMENT UNIX_CONF_FILE (#PCDATA)>
<\!ELEMENT CLIENT_CERT (#PCDATA)>
<\!ELEMENT CLIENT_KEY (#PCDATA)>
<\!ELEMENT CERT_PASSPHASE (#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)>
<\!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_USERNAME?, VAULT_FOLDER?, VAULT_FILE?,
VAULT_EP_CONT?)>
Create / Update PostgreSQL record

Use these parameters to create or update a PostgreSQL record. For an update request, all parameters are optional except “ids” which is required.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action=create</td>
<td>update</td>
</tr>
<tr>
<td>ids={id1,id2,...}</td>
<td>(Required for update request, Invalid for create request) The IDs of the PostgreSQL records you want to update. Valid IDs are required. Multiple IDs are comma separated.</td>
</tr>
<tr>
<td>echo_request={0</td>
<td>1}</td>
</tr>
<tr>
<td>title={value}</td>
<td>(Required for create request) A title for the Sybase record. The title must be unique. Maximum 255 characters (ascii).</td>
</tr>
<tr>
<td>ips={value}</td>
<td>(Required for a create request) A single IP, multiple IPs and/or ranges. Multiple entries are comma separated.</td>
</tr>
<tr>
<td>add_ips={value}</td>
<td>(Optional for an update request) A single IP, multiple IPs and/or ranges to be added to this record. Multiple entries are comma separated.</td>
</tr>
<tr>
<td>remove_ips={value}</td>
<td>(Optional for an update request) A single IP, multiple IPs and/or ranges to be removed from this record. Multiple entries are comma separated.</td>
</tr>
<tr>
<td>network_id={value}</td>
<td>(Optional and valid when the networks feature is enabled) The network ID for the record.</td>
</tr>
<tr>
<td>pgsql_unix_conf_file={value}</td>
<td>(Required for create request) The full path to the PostgreSQL configuration file on your Unix assets (IP addresses). The file must be in the same location on all assets for this record.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>comments={value}</td>
<td>(Optional) Specifies user defined notes about the PostgreSQL record. The comments may include a maximum of 1999 characters (ascii); if comments have 2000 or more characters an error is returned and comments are not saved. Tags (such as &lt;script&gt;) cannot be included; if tags are included an error is returned and the request fails.</td>
</tr>
<tr>
<td>username={value}</td>
<td>(Required for create request) The username of the account to be used for authentication. If password is specified this is the username of a PostgreSQL account. If login_type=vault is specified, this is the username of a vault account. Maximum 255 characters (ascii).</td>
</tr>
<tr>
<td>password={value}</td>
<td>(For create request, password or login_type=vault is required) The password of the PostgreSQL account to be used for authentication. Maximum 100 characters (ascii).</td>
</tr>
<tr>
<td>pgsql_db_name={value}</td>
<td>(Required for create request) The database instance you want to authenticate to.</td>
</tr>
<tr>
<td>port={value}</td>
<td>(Optional) The port where the database instance is running. Default is 5432.</td>
</tr>
<tr>
<td>hosts={value}</td>
<td>(Required if ssl_verify=1) A list of FQDNs for all host IP addresses on which a custom SSL certificate signed by a trusted root CA is installed.</td>
</tr>
<tr>
<td>ssl_verify={0</td>
<td>1}</td>
</tr>
<tr>
<td>login_type=vault</td>
<td>(For create request, password or login_type=vault is required) The password of the PostgreSQL account to be used for authentication. Maximum 100 characters (ascii).</td>
</tr>
<tr>
<td></td>
<td><strong>Vault parameters:</strong></td>
</tr>
<tr>
<td></td>
<td>Vault parameters are required when login_type=vault is specified e.g. vault_id={value}, vault_type={value}, and vault specific settings. For details see the Qualys API V2 User Guide under Unix Record Properties: Vault (in Chapter 8).</td>
</tr>
<tr>
<td></td>
<td><strong>Supported vault_type values:</strong></td>
</tr>
<tr>
<td></td>
<td>CA Access Control</td>
</tr>
<tr>
<td>client_key_type={value}</td>
<td>(Optional) Client key type basic (default) or vault.</td>
</tr>
<tr>
<td>client_key={value}</td>
<td>(Optional for create request if client_key_type=basic) Client key content, if private key not in vault.</td>
</tr>
<tr>
<td>client_key_vault_type={value}</td>
<td>(Required for create request if client_key_type=vault) Select vault type: Cyber-Ark AIM or BeyondTrust PBPS.</td>
</tr>
</tbody>
</table>
### PC - New API Support for PostgreSQL Authentication

#### Example: Create PostgreSQL record

**API request:**

curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl sample" -d "action=create&title=API_POSTGRE_2&username=root&password=abc123&pgsql_db_name=presql&ips=10.10.10.35&pgsql_unix_conf_path=/etc&network_id=4002" "https://qualysapi.qualys.com/api/2.0/fo/auth/postgresql/" > file.xml

**XML output:**

```xml
<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>2017-04-27T20:17:42Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>84307</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>client_key_vault_id={value}</td>
<td>(Required for create request if client_key_type=vault) The ID of the vault to get the private key from. <strong>Vault parameters:</strong> client_key_folder={value} and client_key_file={value} are required vault settings. For details see the Qualys API V2 User Guide under Unix Record Properties: Vault (in Chapter 8).</td>
</tr>
<tr>
<td>passphrase_type={value}</td>
<td>(Optional) Passphrase type can be basic (default) or vault.</td>
</tr>
<tr>
<td>passphrase={value}</td>
<td>(Optional for create request if passphrase_type=basic) The passphrase value.</td>
</tr>
<tr>
<td>client_cert={value}</td>
<td>(Optional for create request if passphrase_type=basic) The passphrase certificate content.</td>
</tr>
<tr>
<td>passphrase_vault_type={value}</td>
<td>(Required if passphrase_type=vault) The vault where the private key passphrase is stored: CA Access Control</td>
</tr>
<tr>
<td>passphrase_vault_id={value}</td>
<td>(Required if passphrase_type=vault) The ID of the vault to get the passphrase from.</td>
</tr>
</tbody>
</table>
Example: Update PostgreSQL record

API request:
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d "action=update&ids=84307&add_ips=10.10.10.40-10.10.10.42" "https://qualysapi.qualys.com/api/2.0/fo/auth/postgresql/" > file.xml

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>2017-04-10T21:01:57Z</DATETIME> 
    <BATCH_LIST> 
      <BATCH> 
        <TEXT>Successfully Updated</TEXT> 
        <ID_SET> 
          <ID>78782</ID> 
        </ID_SET> 
      </BATCH> 
      <BATCH_LIST> 
      </RESPONSE> 
  </BATCH_RETURN>

Delete PostgreSQL records

Use these parameters to delete a PostgreSQL record.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action=delete</td>
<td>(Required)</td>
</tr>
<tr>
<td>echo_request=[0</td>
<td>1]</td>
</tr>
<tr>
<td>ids=[value]</td>
<td>(Required) Delete only PostgreSQL records with certain IDs and/or ID ranges. Valid IDs are required. Multiple entries are comma separated.</td>
</tr>
</tbody>
</table>

Example: Delete PostgreSQL record

API request:
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d "action=delete&ids=78187,78783-78784&echo_request=1" "https://qualysapi.qualys.com/api/2.0/fo/auth/postgresql/" > file.xml
**XML output:**

```xml
<?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>2017-04-10T21:27:22Z</DATETIME>
    <USER_LOGIN>enter_ss</USER_LOGIN>
    <RESOURCE>https://qualysapi.qualys.com/api/2.0/fo/auth/postgresql/</RESOURCE>
    <PARAM_LIST>
      <PARAM>
        <KEY>action</KEY>
        <VALUE>delete</VALUE>
      </PARAM>
      <PARAM>
        <KEY>ids</KEY>
        <VALUE>78187,78783-78784</VALUE>
      </PARAM>
      <PARAM>
        <KEY>echo_request</KEY>
        <VALUE>1</VALUE>
      </PARAM>
    </PARAM_LIST>
  </REQUEST>
  <RESPONSE>
    <DATETIME>2017-04-10T21:27:22Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Deleted</TEXT>
        <ID_SET>
          <ID>78187</ID>
          <ID_RANGE>78187,78783-78784</ID_RANGE>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```
The new Sybase Authentication Record API (/api/2.0/fo/auth/sybase/) allows you to manage Sybase records for authenticating to Sybase Adaptive Server Enterprise (ASE) instances.

This record type is only available in accounts with PC (Policy Compliance) and only supported for compliance scans.

Tip - We strongly recommend you create one or more dedicated user accounts to be used solely by the Qualys Cloud Platform to authenticate to Sybase database instances.

Click here for Sybase Authentication Set Up Instructions

List all record types

Supported parameters for Authentication Record List API call (/api/2.0/fo/auth/?action=list) are described in the current Qualys API V2 User Guide under Authentication Record List (in Chapter 8).

API request:
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample"
-d "action=list" "https://qualysapi.qualys.com/api/2.0/fo/auth/" > file.xml

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>2017-04-12T18:43:57Z</DATETIME>
<AUTH_RECORDS>
<AUTH_UNIX_IDS>
<ID_SET>
<ID>1003</ID>
<ID>78176</ID>
</ID_SET>
</AUTH_UNIX_IDS>
<AUTH_WINDOWS_IDS>
<ID_SET>
<ID>5325</ID>
<ID_RANGE>34902-34909</ID_RANGE>
<ID>35076</ID>
<ID>79233</ID>
</ID_SET>
</AUTH_WINDOWS_IDS>
</RESPONSE>
</AUTH_RECORDS_OUTPUT>
PC - New API Support for Sybase Authentication

```xml
<ID_SET>
  <ID>77260</ID>
  <ID>77262</ID>
  <ID>78148</ID>
  <ID>78153</ID>
  <ID_RANGE>78166-78167</ID_RANGE>
  <ID>78171</ID>
  <ID>78173</ID>
  <ID>78175</ID>
  <ID_RANGE>78830-78831</ID_RANGE>
  <ID>78985</ID>
  <ID>79003</ID>
  <ID>79008</ID>
  <ID_RANGE>79012-79013</ID_RANGE>
  <ID>79230</ID>
</ID_SET>

</AUTH_SYBASE_IDS>
</AUTH_RECORDS>
</RESPONSE>
</AUTH_RECORDS_OUTPUT>

**DTD:**
<base_url>/api/2.0/fo/auth/auth_records.dtd

New **AUTH_SYBASE_IDS** element identifies Sybase record IDs.

<!-- QUALYS AUTH_RECORDS_OUTPUT DTD -->

<!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)>
<!ELEMENT POST_DATA (#PCDATA)>

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

<!ELEMENT RESPONSE (DATETIME, AUTH_RECORDS?, WARNING_LIST?)>
```
List Sybase records

Supported parameters for Sybase Authentication Record List API call (/api/2.0/fo/auth/sybase/?action=list) are described in the current Qualys API V2 User Guide under Authentication Record List by Type (in Chapter 8).

Example: List Sybase Records

API request:
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d "action=list&details=All" "https://qualysapi.qualys.com/api/2.0/fo/auth/sybase/" > file.xml
XML output:
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_SYBASE_LIST_OUTPUT SYSTEM "https://qualysapi.qualys.com/api/2.0/fo/auth/sybase/auth_sybase_list_output.dtd">
<AUTH_SYBASE_LIST_OUTPUT>
 <RESPONSE>
   <DATETIME>2017-04-10T21:32:21Z</DATETIME>
 <AUTH_SYBASE_LIST>
  <AUTH_SYBASE>
   <ID>78177</ID>
   <TITLE><![CDATA[api_syb_basic_2IPs_NW2]]></TITLE>
   <USERNAME><![CDATA[api_user1]]></USERNAME>
   <DATABASE><![CDATA[api_sybDB1]]></DATABASE>
   <PORT>444</PORT>
   <IP_SET>
    <IP_RANGE>10.10.24.12-10.10.24.13</IP_RANGE>
   </IP_SET>
   <NETWORK_ID>19019</NETWORK_ID>
   <CREATED>
    <DATETIME>2017-04-08T00:17:17Z</DATETIME>
    <BY>enter_ss</BY>
   </CREATED>
   <LAST_MODIFIED>
    <DATETIME>2017-04-08T00:17:17Z</DATETIME>
   </LAST_MODIFIED>
  </AUTH_SYBASE>
  <AUTH_SYBASE>
   <ID>78186</ID>
   <TITLE><![CDATA[api_syb_basic_2IPs_Global]]></TITLE>
   <USERNAME><![CDATA[api_user1]]></USERNAME>
   <DATABASE><![CDATA[api_sybDB1]]></DATABASE>
   <PORT>444</PORT>
   <IP_SET>
    <IP_RANGE>10.10.24.12-10.10.24.13</IP_RANGE>
   </IP_SET>
   <NETWORK_ID>0</NETWORK_ID>
   <CREATED>
    <DATETIME>2017-04-08T01:04:0Z</DATETIME>
    <BY>enter_ss</BY>
   </CREATED>
   <LAST_MODIFIED>
    <DATETIME>2017-04-08T01:04:0Z</DATETIME>
   </LAST_MODIFIED>
  </AUTH_SYBASE>
 ...
PC - New API Support for Sybase Authentication

DTL:
<base_url>/api/2.0/fo/auth/sybase/auth_sypbase_list_output.dtd

<!-- QUALYS AUTH_SYBASE_LIST_OUTPUT DTD -->

<!ELEMENT AUTH_SYBASE_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_SYBASE_LIST|ID_SET)?, WARNING_LIST?, GLOSSARY?)>
<!ELEMENT AUTH_SYBASE_LIST (AUTH_SYBASE+)>

<!ELEMENT AUTH_SYBASE (ID, TITLE, USERNAME, DATABASE, PORT, INSTALLATION_DIR?, IP_SET?, LOGIN_TYPE?, DIGITAL_VAULT?, NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>  
<!ELEMENT TITLE (#PCDATA)>  
<!ELEMENT USERNAME (#PCDATA)>  
<!ELEMENT DATABASE (#PCDATA)>  
<!ELEMENT PORT (#PCDATA)>  
<!ELEMENT INSTALLATION_DIR (#PCDATA)>  
<!ELEMENT IP_SET (IP|IP_RANGE)+>  
<!ELEMENT IP (#PCDATA)>  
<!ELEMENT IP_RANGE (#PCDATA)>  

<!ELEMENT LOGIN_TYPE (#PCDATA)>  
<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE, DIGITAL_VAULT_TITLE, VAULT_USERNAME?, VAULT_FOLDER?, VAULT_FILE?, VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_NS_TYPE?, VAULT_NS_NAME?)>
<!ELEMENT DIGITAL_VAULT_ID (#PCDATA)>  
<!ELEMENT DIGITAL_VAULT_TYPE (#PCDATA)>  
<!ELEMENT DIGITAL_VAULT_TITLE (#PCDATA)>  
<!ELEMENT VAULT_USERNAME (#PCDATA)>  
<!ELEMENT VAULT_FOLDER (#PCDATA)>  
<!ELEMENT VAULT_FILE (#PCDATA)>  
<!ELEMENT VAULT_SECRET_NAME (#PCDATA)>  
<!ELEMENT VAULT_SYSTEM_NAME (#PCDATA)>  
<!ELEMENT VAULT_NS_TYPE (#PCDATA)> 

Qualys API Release Notes 150
Create / Update Sybase record

Use these parameters to create or update a Sybase record. For an update request, all parameters are optional except “ids” which is required.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action=create</td>
<td>(Required) The action for the API call, create or update.</td>
</tr>
<tr>
<td>ids=</td>
<td>(Required for update request, Invalid for create request) The IDs of the Sybase records you want to update. Valid IDs are required. Multiple IDs are comma separated.</td>
</tr>
<tr>
<td>echo_request=</td>
<td>(Optional) Show (echo) the request's input parameters (names and values) in the XML output. When not specified, parameters are not included in the XML output. Specify 1 to view parameters in the XML output.</td>
</tr>
<tr>
<td>title=</td>
<td>(Required for create request) A title for the Sybase record. The title must be unique. Maximum 255 characters (ascii).</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>username={value}</td>
<td>(Required for create request) The username of the account to be used for authentication. If password is specified this is the username of a Sybase account. If login_type=vault is specified, this is the username of a vault account. Maximum 255 characters (ascii).</td>
</tr>
<tr>
<td>password={value}</td>
<td>(For create request, password or login_type=vault is required) The password of the Sybase account to be used for authentication. Maximum 100 characters (ascii).</td>
</tr>
<tr>
<td>login_type=vault</td>
<td>(For create request, password or login_type=vault is required) The password of the Sybase account to be used for authentication. Maximum 100 characters (ascii). <strong>Vault parameters:</strong> Vault parameters are required when login_type=vault is specified e.g. vault_id={value}, vault_type={value}, and vault specific settings. For details see the <a href="#">Qualys API V2 User Guide</a> under Unix Record Properties: Vault (in Chapter 8). <strong>Supported vault_type values:</strong> Cyber-Ark PIM Suite</td>
</tr>
<tr>
<td>port={value}</td>
<td>(Required for create request) The port the Sybase database is on.</td>
</tr>
<tr>
<td>database={value}</td>
<td>(Required for create request) The name of the Sybase database you want to authenticate to.</td>
</tr>
<tr>
<td>install_dir={value}</td>
<td>(Required for create request if this record will be used for scanning Unix hosts) The database installation directory for scanning Unix hosts.</td>
</tr>
<tr>
<td>ips={value}</td>
<td>(Required for a create request) A single IP, multiple IPs and/or ranges. Multiple entries are comma separated.</td>
</tr>
<tr>
<td>network_id={value}</td>
<td>(Optional and valid when the networks feature is enabled) The network ID for the record.</td>
</tr>
<tr>
<td>comments={value}</td>
<td>(Optional) Specifies user defined notes about the Sybase record. The comments may include a maximum of 1999 characters (ascii); if comments have 2000 or more characters an error is returned and comments are not saved. Tags (such as <code>&lt;script&gt;</code>) cannot be included; if tags are included an error is returned and the request fails.</td>
</tr>
</tbody>
</table>

**Qualys API Release Notes**
Example: Create Sybase Record

**API request:**
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d "action=create&title=sybase_record&network_id=19015&username=acme_ac123&password=password&port=444&database=sybaseDB1&ips=10.10.24.12,10.10.24.13,10.10.24.15&installation_dir=/dir123&comments=This%20Sybase%20comments" "https://qualysapi.qualys.com/api/2.0/fo/auth/sybase/" > file.xml

**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>2017-04-10T20:52:31Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>78782</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>

Example: Create Sybase Record using Cyber-Ark PIM Suite vault

**API request:**

**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>2017-04-13T18:54:36Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>78782</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
<BATCH>
  <TEXT>Successfully Created</TEXT>
  <ID_SET>
    <ID>88888</ID>
  </ID_SET>
  </BATCH>
</BATCH_LIST>
</RESPONSE>
</BATCH_RETURN>

**Example: Update Sybase Record**

**API request:**

**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>2017-04-10T21:01:57Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>78782</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
Delete Sybase records

Use these parameters to delete a Sybase record.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action=delete</td>
<td>(Required)</td>
</tr>
<tr>
<td>echo_request={0</td>
<td>1}</td>
</tr>
<tr>
<td>ids={value}</td>
<td>(Required) Delete only Sybase records with certain IDs and/or ID ranges. Valid IDs are required. Multiple entries are comma separated.</td>
</tr>
</tbody>
</table>

Example: Delete Sybase Record

**API request:**

curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d "action=delete&ids=78187,78783-78784&echo_request=1" "https://qualysapi.qualys.com/api/2.0/fo/auth/sybase/" > file.xml

**XML output:**

```xml
<?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>2017-04-10T21:27:22Z</DATETIME>
<USER_LOGIN>enter_ss</USER_LOGIN>
<RESOURCE>https://qualysapi.qualys.com/api/2.0/fo/auth/sybase/</RESOURCE>
<PARAM_LIST>
<PARAM>
<KEY>action</KEY>
.VALUE>delete</VALUE>
</PARAM>
<PARAM>
<KEY>ids</KEY>
.VALUE>78187,78783-78784</VALUE>
</PARAM>
<PARAM>
<KEY>echo_request</KEY>
.VALUE>1</VALUE>
</PARAM>
</PARAM_LIST>
</REQUEST>
</RESPONSE>
```
PC - New API Support for Sybase Authentication

<DATETIME>2017-04-10T21:27:22Z</DATETIME>
<BATCH_LIST>
  <BATCH>
    <TEXT>Successfully Deleted</TEXT>
    <ID_SET>
      <ID>78187</ID>
      <ID_RANGE>78783-78784</ID_RANGE>
    </ID_SET>
  </BATCH>
</BATCH_LIST>
</RESPONSE>
</BATCH_RETURN>
PC - Introducing Qualys Custom Controls in Library Policies

Library policies provided by Qualys may now include a new control type called Qualys Custom Control (QCC). With this new control type we can quickly provide to users new controls that are similar to user-defined controls.

**Good to Know**

- When you import a library policy with QCCs and you pick the option “Create user-defined controls” at the time of import, the QCCs are added to your controls list. Once added, you can make a copy of any QCC to create a UDC that you can customize to meet your exact needs.

- The QCC itself cannot be edited or deleted. Like service-provided controls, Qualys may update QCCs in subsequent releases to provide new technology support, updates to values, etc. This will not have any impact to the QCCs added to policies.

- In order for us to ensure that we don’t add duplicate controls to your list when importing the same library policy multiple times these controls get an internal UDC ID assigned. You’ll see the UDC ID when you export a QCC from your account, and when you export a library policy that includes a QCC from your account.

- We made updates to the Policy Export Output DTD and to the ImportableControl.xsd schema to include the new UDC_ID element.

**Export a Library Policy to XML**

You can export a library compliance policy from your account to an XML file. Just like with user created policies you must specify the input parameter `show_user_controls=1` to include UDCs in the output. When the policy includes a Qualys Custom Control you’ll see the UDC ID for the control in the output.

**API request:**

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d "action=export&ids=991742279&show_user_controls=1" "https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/
```

**XML output:**

```
<POLICY>
  <TITLE><![CDATA[Library Policy with 2 UDC v.2.0]]></TITLE>
  <EXPORTED><![CDATA[2017-04-17T15:02:56Z]]></EXPORTED>
  <COVER_PAGE><![CDATA[]]></COVER_PAGE>
  <STATUS><![CDATA[active]]></STATUS>
  <TECHNOLOGIES total="2">
    <TECHNOLOGY>
      ...
    </TECHNOLOGY>
  </TECHNOLOGIES>
</POLICY>
```
DTD Update:
The Policy Export Output DTD (policy_export_output.dtd) was updated to include the new element UDC_ID. We also added ID (Control ID) under USER_DEFINED_CONTROL.

<!-- QUALYS POLICY_EXPORT_OUTPUT DTD -->

...
Export a Library Policy to CSV (UI Only)

You can export a policy to CSV format from the Qualys UI. Select the option “Include user defined controls” to include UDCs in the output and to see the UDC_ID column. When the policy includes a Qualys Custom Control you’ll see the UDC ID for the control in the output. You’ll see N/A for system-defined controls.

CSV output:

"Policy Information"
"Title","Cover Page"
"Library Policy with 2 UDC v.2.0",

"Technologies (2)"
"ID","Name"
"2","Windows 2003 Server"
"12","Windows 2000"

"Control Information"
"Section No.","Section Heading","Reference","CID","UDC_ID","Statement","Description","Technology ID","Technology Name","Criticality Label","Criticality Value","Evaluation"
"1","Untitled",,"100005","55449d95-1877-7ee5-829a-4eededacb04f","Registry Value Existence",".*","2","Windows 2003 Server","MINIMAL","1","NA

* * * * * Expected Value(s) * * * * *
true
"1","Untitled",,"100005","55449d95-1877-7ee5-829a-4eededacb04f","Registry Value Existence",".*","12","Windows 2000","MINIMAL","1","NA

* * * * * Expected Value(s) * * * * *
true

Export a Qualys Custom Control to XML

When you export a Qualys Custom Control (QCC) from your account to XML you’ll see the UDC ID in the output.

XML output:

<CONTROL_LIST total="1">
  <CONTROL>
    <ID>100005</ID>
    <UDC_ID>55449d95-1877-7ee5-829a-4eededacb04f</UDC_ID>
    <CHECK_TYPE>Registry Value Existence</CHECK_TYPE>
  </CONTROL>
</CONTROL_LIST>
<CATEGORY>
<ID>3</ID>
<NAME><![CDATA[Access Control Requirements]]></NAME>
</CATEGORY>

<SUBCATEGORY>
<ID>1007</ID>
<NAME><![CDATA[Authentication/Passwords]]></NAME>
</SUBCATEGORY>

...  

Schema Update:  
The ImportableControl.xsd schema is used when importing and exporting controls. It was updated to include the new element UDC_ID. We also added ID (Control ID) under CONTROL.

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <xs:element name="CONTROL_LIST">  
    <xs:complexType>  
      <xs:sequence>  
        <xs:element maxOccurs="unbounded" ref="CONTROL" />  
      </xs:sequence>  
      <xs:attribute name="total" use="required" type="xs:integer" />  
    </xs:complexType>  
  </xs:element>

  <xs:element name="ID" type="xs:integer" />

  <xs:element name="CONTROL">  
    <xs:complexType>  
      <xs:sequence>  
        <xs:element ref="ID" minOccurs="0" maxOccurs="1" />  
        <xs:element ref="UDC_ID" minOccurs="0" maxOccurs="1" />  
        <xs:element ref="CHECK_TYPE" minOccurs="0" maxOccurs="1" />  
        <xs:element ref="CATEGORY" minOccurs="0" maxOccurs="1" />  
        <xs:element ref="SUB_CATEGORY" minOccurs="0" maxOccurs="1" />  
        <xs:element ref="STATEMENT" minOccurs="0" maxOccurs="1" />  
        <xs:element ref="CRITICALITY" minOccurs="0" maxOccurs="1" />  
        <xs:element ref="COMMENT" minOccurs="0" maxOccurs="1" />  
        <xs:element ref="IGNORE_ERROR" minOccurs="0" maxOccurs="1" />  
        <xs:element ref="IGNORE_ITEM_NOT_FOUND" minOccurs="0" maxOccurs="1" />  
        <xs:element ref="SCAN_PARAMETERS" minOccurs="0" maxOccurs="1" />  
        <xs:element ref="TECHNOLOGY_LIST" minOccurs="0" maxOccurs="1" />  
      </xs:sequence>  
    </xs:complexType>  
  </xs:element>
</xs:schema>
<xs:element ref="REFERENCE_LIST" maxOccurs="1" />
</xs:sequence>
</xs:complexType>
</xs:element>

<xs:element name="UDC_ID">
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:minLength value="0"/>
      <xs:maxLength value="36"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>

...
PC - Remediation Information Displayed in Reports

The Compliance Posture Info API v2 (/api/2.0/fo/compliance/posture/info/) with the action=list and new parameter show_remediation_info now displays remediation information in XML and CSV output formats for PC reports.

Parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action=list</td>
<td>(Required) The GET method may be used.</td>
</tr>
</tbody>
</table>
| show_remediation_info={0|1} | (Optional) Specifies whether to include the remediation information in the XML or CSV output. By default, the output does not include the remediation information. When not specified, the remediation information is not included in the output. Specify 1 to view the remediation information in the output.

API request (XML Format):

curl -n -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d "action=list&policy_id=131562&show_remediation_info=1" "https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/"

Sample Output (XML format):

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE POSTURE_INFO_LIST_OUTPUT SYSTEM "https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/posture_info_list_output.dtd">
<POSTURE_INFO_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-04-07T05:38:33Z</DATETIME>
    <INFO_LIST>...
      <INFO>
        <ID>1731930</ID>
        <HOST_ID>135113</HOST_ID>
        <CONTROL_ID>4156</CONTROL_ID>
        <TECHNOLOGY_ID>37</TECHNOLOGY_ID>
        <INSTANCE></INSTANCE>
        <STATUS>Passed</STATUS>
        <REMEDIATION>Configure the policy value for User Configuration - &gt; Administrative Templates -&gt; Windows Components -&gt; Attachment Manager -&gt; "Notify antivirus programs when opening attachments" to "Enabled".</REMEDIATION>
        <POSTURE_MODIFIED_DATE>2017-04-07T05:32:37Z</POSTURE_MODIFIED_DATE>
      </INFO>
    </INFO_LIST>
  </RESPONSE>
</POSTURE_INFO_LIST_OUTPUT>
```
To establish the recommended configuration via GP, set the following UI path to RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Configure encryption types allowed for Kerberos.

API request (CSV format):
curl -n -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d "action=list&policy_id=131562&show_remediation_info=1&output_format=csv" "https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/"

Sample Output (CSV format):

<table>
<thead>
<tr>
<th>NAME</th>
<th>POLICY ID</th>
<th>DATETIME</th>
<th>ID</th>
<th>IP</th>
<th>OS</th>
<th>DNS Name</th>
<th>NetBios</th>
<th>Tracking Method</th>
<th>Control ID</th>
<th>Control Statement</th>
<th>Criticality Label</th>
<th>Criticality Value</th>
<th>Technology ID</th>
<th>Technology Name</th>
<th>Posture</th>
<th>Remediation</th>
<th>Evaluation Date</th>
</tr>
</thead>
</table>
PC - Remediation Information Displayed in Reports

Settings\Local Policies\Security Options\Network Security: Configure encryption types allowed for Kerberos", 4/7/2017 5:24

...,

SUMMARY,

TOTAL ASSETS, TOTAL CONTROLS, TOTAL CONTROL INSTANCES, TOTAL PASSED CONTROL INSTANCES, TOTAL FAILED CONTROL INSTANCES, TOTAL ERROR CONTROL INSTANCES,

4, 3, 12, 4, 4, 4,

#NAME?,

Posture Info List Output DTD update:

Path: <base_url>/api/2.0/fo/compliance/posture/info/posture_info_list_output.dtd

<!DOCTYPE POSTURE_INFO_LIST_OUTPUT ["QUALYS POSTURE_INFO_LIST_OUTPUT DTD"]>

<!ELEMENT POSTURE_INFO_LIST_OUTPUT (REQUEST?, RESPONSE?)>

<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?, POSTDATA?)>

...,

<!ELEMENT POLICY (ID, DATETIME, INFO_LIST?, SUMMARY?, WARNING_LIST?, GLOSSARY?)>

<!ELEMENT INFO_LIST (INFO+)>

<!ELEMENT INFO (ID, HOST_ID, CONTROL_ID, TECHNOLOGY_ID, INSTANCE?, STATUS, REMEDIATION?, POSTURE_MODIFIED_DATE?, EXCEPTION?, EVIDENCE?)>

<!ELEMENT ID (#PCDATA)>

<!ELEMENT HOST_ID (#PCDATA)>

<!ELEMENT CONTROL_ID (#PCDATA)>

<!ELEMENT TECHNOLOGY_ID (#PCDATA)>

<!ELEMENT INSTANCE (#PCDATA)>

<!ELEMENT STATUS (#PCDATA)>

<!ELEMENT REMEDIATION (#PCDATA)>

<!ELEMENT POSTURE_MODIFIED_DATE (#PCDATA)>

<!ELEMENT EXCEPTION (ASSIGNEE, STATUS, END_DATETIME?, CREATED?, LAST_MODIFIED?, COMMENT_LIST?)>

<!ELEMENT ASSIGNEE (#PCDATA)>

<!ELEMENT END_DATETIME (#PCDATA)>

<!ELEMENT CREATED (BY, DATETIME)>

<!ELEMENT BY (#PCDATA)>

<!ELEMENT LAST_MODIFIED (BY, DATETIME)>

<!ELEMENT COMMENT_LIST (COMMENT+)>

<!ELEMENT COMMENT (DATETIME, BY, TEXT)>

<!ELEMENT TEXT (#PCDATA)>

...,

<!ELEMENT TOTAL_ERROR (#PCDATA)>

<!ELEMENT TOTAL_EXCEPTIONS (#PCDATA)>

<!-- EOF -->