Asset Management and Tagging API v2

User Guide
Version 2.34

August 28, 2018
CONTENTS

Preface

Chapter 1  Welcome
Get Started ..........................................................................................................................  6
Get API Notifications ........................................................................................................  6
Introduction to the API Framework ................................................................................  7
  Request URL ...............................................................................................................  7
  URL to the Qualys API Server ..................................................................................  7
  Authentication ............................................................................................................  9
  JSON Support ..............................................................................................................  9
Usage ................................................................................................................................. 10
Know your Portal Version .............................................................................................. 13

Chapter 2  Tag API
Get Tag Info................................................................................................................... ...  16
Create Tag..................................................................................................................... ....  18
  Get to know Groovy .................................................................................................  20
Update Tag ....................................................................................................................... 21
Search Tags....................................................................................................................... 24
Count Tags..................................................................................................................... ...  27
Delete Tag ......................................................................................................................... 29
Evaluate Tag................................................................................................................... ..  31
List Users with their Tags............................................................................................... 34
Tag Fields..........................................................................................................................  38

Chapter 3  Host Asset API
Get Host Asset Info ......................................................................................................... 40
Create Host Asset ............................................................................................................ 49
Update Host Asset........................................................................................................... 56
Search Hosts Assets........................................................................................................ 61
Count Host Assets ......................................................................................................... 75
Delete Host Asset.......................................................................................................... 77
Activate Host Asset......................................................................................................... 79
Host Asset Fields ............................................................................................................. 82

Chapter 4  Asset API
Get Asset Info ................................................................................................................. ..  85
Update Asset .................................................................................................................... 87
Search Assets.................................................................................................................. ..  91
Count Assets ................................................................................................................... 94
Delete Asset ...................................................................................................................... 96
### Contents

<table>
<thead>
<tr>
<th>Chapter 5  Host Instance Vulnerability API</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get Vulnerability Info ......................................................................................................... 103</td>
</tr>
<tr>
<td>Search Vulnerabilities ........................................................................................................... 105</td>
</tr>
<tr>
<td>Count Vulnerabilities ............................................................................................................ 108</td>
</tr>
<tr>
<td>Host Instance Vulnerability Fields ..................................................................................... 109</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 6  Asset Data Connector API</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get Connector Info ............................................................................................................ 111</td>
</tr>
<tr>
<td>Update Connector ................................................................................................................ 113</td>
</tr>
<tr>
<td>Search Connectors ................................................................................................................. 117</td>
</tr>
<tr>
<td>Count Connectors ................................................................................................................ 120</td>
</tr>
<tr>
<td>Delete Connector .................................................................................................................. 121</td>
</tr>
<tr>
<td>Run Connector ..................................................................................................................... 124</td>
</tr>
<tr>
<td>Connector Fields .................................................................................................................. 127</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 7  AWS Asset Data Connector API</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get AWS Connector Info .................................................................................................... 129</td>
</tr>
<tr>
<td>Create AWS Connector ......................................................................................................... 132</td>
</tr>
<tr>
<td>Support for AWS GovCloud .................................................................................................. 137</td>
</tr>
<tr>
<td>Support for China Region .................................................................................................... 139</td>
</tr>
<tr>
<td>Support for Cross-Account Role Authentication .................................................................. 142</td>
</tr>
<tr>
<td>Update AWS Connector ......................................................................................................... 146</td>
</tr>
<tr>
<td>Search AWS Connectors ........................................................................................................ 150</td>
</tr>
<tr>
<td>Count AWS Connectors .......................................................................................................... 153</td>
</tr>
<tr>
<td>Delete AWS Connector .......................................................................................................... 154</td>
</tr>
<tr>
<td>Run Connector ..................................................................................................................... 156</td>
</tr>
<tr>
<td>AWS Connector Fields .......................................................................................................... 157</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 8  AWS Authentication Record API</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get AWS Auth Record Info .................................................................................................... 160</td>
</tr>
<tr>
<td>Create AWS Auth Record ...................................................................................................... 161</td>
</tr>
<tr>
<td>Update AWS Auth Record ..................................................................................................... 163</td>
</tr>
<tr>
<td>Search AWS Auth Records ................................................................................................... 165</td>
</tr>
<tr>
<td>Count AWS Auth Records .................................................................................................... 168</td>
</tr>
<tr>
<td>Delete AWS Auth Records .................................................................................................... 169</td>
</tr>
<tr>
<td>AWS Auth Record Fields ...................................................................................................... 172</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Appendix A  JSON Support</th>
</tr>
</thead>
</table>

Qualifier Asset Management and Tagging API
Preface

Using the Qualys Asset Management and Tagging API, third parties can integrate the Qualys Security and Compliance solution into their own applications using an extensible XML interface. This user guide is intended for application developers who will use the Qualys Asset Management and Tagging API.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro.. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com.

Contact Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/.
Welcome

Welcome to Qualys Asset Management and Tagging API. The sections that follow describe how to use the Tags API, Host Asset API, Asset API and the Host Instance Vulnerability API.

Get Started

Introduction to the API Framework - We recommend you review important information about the API framework.

URL to the Qualys API Server - We’ll give you the basics about making API requests. The base URL depends on the platform where your Qualys account is located.

Authentication - We’ll tell you about the method used for authentication. API requests must authenticate using Qualys credentials.

Usage - Check out the basics about making requests and receiving data from our asset management application.

Know your Portal Version

Get API Notifications

We recommend you join our Community and subscribe to our API notifications so you’ll get email notifications telling you about important upcoming API enhancements and changes.

From our Community

Join our Community

Subscribe to API Notifications (select Receive email notifications)
Introduction to the API Framework

The Qualys Asset Management and Tagging API framework offers numerous innovations and new functionality compared to the other Qualys API frameworks.

Request URL

The URL for making Asset Management and Tagging API requests respects the following structure:

https://<baseurl>/qps/rest/2.0/<operation>/<module>/<object>/<object_id>

where the components are described below.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;baseurl&gt;</td>
<td>The Qualys API server URL that you should use for API requests depends on the platform where your account is located. The base URL for Qualys US Platform 1 is: <a href="https://qualysapi.qualys.com">https://qualysapi.qualys.com</a></td>
</tr>
<tr>
<td>&lt;operation&gt;</td>
<td>The request operation, such as get a list, get a count, search, create, and update.</td>
</tr>
<tr>
<td>&lt;module&gt;</td>
<td>The API module. For the Asset Management and Tagging API, the module is: “am”.</td>
</tr>
<tr>
<td>&lt;object&gt;</td>
<td>The module specific object.</td>
</tr>
<tr>
<td>&lt;object_id&gt;</td>
<td>(Optional) The module specific object ID, if appropriate.</td>
</tr>
</tbody>
</table>

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.

**Still have questions?** You can easily find the API server URL for your account. Just log in to your Qualys account and go to Help > About. You’ll see this information under Security Operations Center (SOC).
Authentication

The application must authenticate using Qualys account credentials (user name and password) as part of the HTTP request. The credentials are transmitted using the “Basic Authentication Scheme” over HTTPS.

For more information, see the “Basic Authentication Scheme” section of RFC #2617:

http://www.faqs.org/rfcs/rfc2617.html

The exact method of implementing authentication will vary according to which programming language is used.

The allowed methods, POST and/or GET, for each API request are documented with each API call in this user guide.

Example

Basic authentication - recommended option:

curl -u "USERNAME:PASSWORD"
https://qualysapi.qualys.com/qps/rest/2.0/count/am/hostasset

where portal.qualys.com is the base URL to the Qualys API server where your account is located.

JSON Support

Qualys Asset Management and Tagging API supports JSON requests and responses.

Learn more
Chapter 1 — Welcome

Usage

Object types

You have core objects, which represent domain objects for specific business goals and related objects which contain related information or collections of information. Related objects are often simplified representations of core objects but are not implicitly core objects. For example, the tags collection on Asset is a simpler form of the Tag core object, but the ports collection is not.

Collections

Collections of related objects are found within a container object called a QList. These lists will have a specific name for the type of objects they contain. For example, the tags collection Asset is a TagSimpleQList and will read and write TagSimple API objects. These lists can contain a number of sub elements.

<table>
<thead>
<tr>
<th>Element</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>(Read only) The total number of items returned in the list element</td>
</tr>
<tr>
<td>list</td>
<td>(Read only) The items contained in the collection on the server</td>
</tr>
<tr>
<td>set</td>
<td>A new collection of items to place in the server side object. Any existing items not in the list provided will be discarded.</td>
</tr>
<tr>
<td>add</td>
<td>A new item to be added to the server side object. The item may be keyed of one or more fields depending on the collection. In the even that that an item in the add collection collides with an existing entry, the existing entry will be updated with the fields provided.</td>
</tr>
<tr>
<td>remove</td>
<td>Removes an element from the list by the collections key, usually id. If the item does not exist, the entry will be ignored. Additional fields beyond the item key will also be ignored.</td>
</tr>
<tr>
<td>update</td>
<td>Updates item(s) in the collection. This allows you to update the fields of non-core items via the objects and reference them. Items will be resolved by the collection’s key, and then additional fields applied to the found object. In the event that the supplied item does not match an existing related object, it will be ignored.</td>
</tr>
</tbody>
</table>
Whitespace in XML tags

Whitespace (which includes line breaks) is not allowed in XML tags that are numbers.

<table>
<thead>
<tr>
<th>Invalid tag</th>
<th>Valid tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>This syntax will not work:</td>
<td>This syntax will work just fine:</td>
</tr>
<tr>
<td>&lt;id&gt; 34234 &lt;/id&gt;</td>
<td>&lt;id&gt;345254&lt;/id&gt;</td>
</tr>
</tbody>
</table>

Pagination

Some API actions will return a list of core objects but will limit the number returned (default is 100). You can change which objects are returned and the number of objects by specifying a preferences tag in the POST body of your request.

Preferences tag fields

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startFromOffset</td>
<td>The first item to return by index. The default is 1.</td>
</tr>
<tr>
<td>startFromId</td>
<td>The first item to return by primary key. No default value.</td>
</tr>
<tr>
<td>limitResults</td>
<td>The total number of items to return. The default is 100.</td>
</tr>
</tbody>
</table>

Example

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
    <preferences>
        <startFromOffset>100</startFromOffset>
        <limitResults>50</limitResults>
    </preferences>
</ServiceRequest>
```

Limit your results

Use the optional “fields” parameter for any Search or Get API request to limit the amount of information returned in the results. Simply specify the fields you want to include in the output, and all other information will be filtered out. Multiple fields are comma separated and wildcards are supported.

Example - Get Request

This get request will fetch tag ID 12345 and return the tag ID, name and creation date.

https://qualysapi.qualys.com/qps/rest/2.0/get/am/tag/12345?fields=
id, name, created

**Example - Search Request**

This search request will return the ID of the connector and the ID of any default tags attached to the connector:

https://qualysapi.qualys.com/qps/rest/2.0/search/am/awsassetdataconnector?fields=id,defaultTags.list.SimpleTag.id

Using wildcards, the example above could be represented as:

https://qualysapi.qualys.com/qps/rest/2.0/search/am/awsassetdataconnector?fields=id,defaultTags.*.*.id
Know your Portal Version

Using the Version API you can find out the installed version of Portal and its sub-modules that are available in your subscription.

URL: https://qualysapi.qualys.com/qps/rest/portal/version
Methods allowed: GET

Examples

Example 1: XML

API Request:

curl -u "USERNAME:PASSWORD" -X "GET" -H "Accept: application/xml"
https://qualysapi.qualys.com/qps/rest/portal/version

Response:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/version.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
    <data>
        <Portal-Version>
            <WAS-VERSION>6.0.0.0</WAS-VERSION>
            <FIM-VERSION>1.5.1</FIM-VERSION>
            <VM-VERSION>1.0.3</VM-VERSION>
            <CERTVIEW-VERSION>1.1.0.0</CERTVIEW-VERSION>
            <CM-VERSION>1.20.1</CM-VERSION>
            <MDS-VERSION>2.11.7.0</MDS-VERSION>
            <CA-VERSION>2.9.1.0</CA-VERSION>
            <IOC-VERSION>1.1.0</IOC-VERSION>
            <AV2-VERSION>0.1.0</AV2-VERSION>
            <QUESTIONNAIRE-VERSION>2.14.0.4</QUESTIONNAIRE-VERSION>
            <WAF-VERSION>2.7.0.0</WAF-VERSION>
        </Portal-Version>
    </data>
</ServiceResponse>
```
**Example 2: JSON**

**API Request:**

```bash
```

**Response:**

```json
{
    "ServiceResponse": {
        "data": [
            {
                "Portal-Version": {
                    "WAS-VERSION": "6.0.0.0",
                    "VM-VERSION": "1.0.3",
                    "CM-VERSION": "1.20.1",
                    "MDS-VERSION": "2.11.7.0",
                    "CA-VERSION": "2.9.1.0",
                    "QUESTIONNAIRE-VERSION": "2.14.0.4",
                    "WAF-VERSION": "2.7.0.0"
                }
            }
        ],
        "responseCode": "SUCCESS",
        "count": 1
    }
}
```
Tag API

The Tag API provides a suite of API functions for creating and managing tags. Also the related Admin User API lets you list users and their associated tags.

Operations
Get Tag Info
Create Tag
Update Tag
Search Tags
Count Tags
Delete Tag
Evaluate Tag
List Users with their Tags

Reference
Tag Fields
Get Tag Info

Returns a single tag by ID.

**URL**
https://<baseurl>/qps/rest/2.0/get/am/tag/<id>

**Method**
GET

**Limit your results**
Use the optional “fields” parameter to limit the amount of information returned for the tag. Learn more

**Permissions**

Managers with Full Scope

Users without Full Scope must have these account permissions:
- Access Permission “API Access”

**Example**

Fetch tag ID 12345.

**Request:**
curl -n -u "USERNAME:PASSWORD"
"https://qualysapi.qualys.com/qps/rest/2.0/get/am/tag/12345"

**Response:**
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xmlns="https://qualysapi.qualys.com/qps/xsd/2.0/am/tag.xsd">
 <responseCode>SUCCESS</responseCode>
 <count>1</count>
 <data>
  <Tag>
   <id>12345</id>
   <name>Test Tag</name>
   <created>2014-02-06T19:14:50Z</created>
   <modified>2014-02-06T19:14:50Z</modified>
   <color>#FFFFFF</color>
   <ruleText>asset.installedSoftwares.contains { it.name == "Windows" }</ruleText>
  </Tag>
 </data>
</ServiceResponse>
<ruleType>GROOVY</ruleType>
<children>
  <list/>
</children>
</Tag>
</data>
</ServiceResponse>
Create Tag

Create a new tag and possibly child tags.

**URL**
https://<baseurl>/qps/rest/2.0/create/am/tag

**Method**
POST

**Permissions**

Managers with Full Scope

Users without Full Scope must have these account permissions:
- Access Permission “API Access”
- Tag Permission “Create User Tag”
- Tag Permission “Modify Dynamic Tag Rules” (to create a dynamic tag)

**Example**

This example creates a new tag and 3 child tags.

**Request:**
curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST" --data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/create/am/tag" < file.xml

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

**Request POST data (file.xml):**

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <data>
    <Tag>
      <name>Parent Tag</name>
      <ruleType>Groovy</ruleType>
      <ruleText>if(asset.getAssetType() != Asset.AssetType.HOST)
        return false;
      return asset.hasVulnsWithSeverity(4,5)</ruleText>
      <created>2014-02-06T19:14:50Z</created>
      <modified>2014-02-06T19:14:50Z</modified>
      <color>#FFFFFF</color>
      <children>
```
<set>
  <TagSimple>
    <name>Child 1</name>
  </TagSimple>
  <TagSimple>
    <name>Child 2</name>
  </TagSimple>
  <TagSimple>
    <name>Child 3</name>
  </TagSimple>
</set>
</children>
</Tag>
</data>
</ServiceRequest>

Response:
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/tag.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <Tag>
      <id>1589217</id>
      <name>Parent Tag</name>
      <created>2014-02-06T19:14:50Z</created>
      <modified>2014-02-06T19:14:50Z</modified>
      <color>#FFFFFF</color>
      <ruleText>if(asset.getAssetType()!=Asset.AssetType.HOST) return false;
      return asset.hasVulnsWithSeverity(4,5)</ruleText>
      <ruleType>GROOVY</ruleType>
      <children>
        <list>
          <TagSimple>
            <id>1</id>
            <name>Child 1</name>
          </TagSimple>
        </list>
      </children>
    </Tag>
  </data>
</ServiceResponse>
<TagSimple>
  <id>2</id>
  <name>Child 2</name>
</TagSimple>
<TagSimple>
  <id>3</id>
  <name>Child 3</name>
</TagSimple>
</list>
</children>
</Tag>
</data>
</ServiceResponse>

**Get to know Groovy**

Check out the following article on our Community to learn how to create asset tags using the Groovy programming language. You'll also get several Groovy rule examples that you can start using today.

---

**From our Community**

*Create Asset Tags using Groovy*
Update Tag

Update fields for a tag and collections of tags.

**URL**

<table>
<thead>
<tr>
<th>Method</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST</td>
<td>https://&lt;baseurl&gt;/qps/rest/2.0/update/am/tag/&lt;id&gt; or https://&lt;baseurl&gt;/qps/rest/2.0/update/am/tag</td>
</tr>
</tbody>
</table>

Using the NOT EQUALS operator for updating tags could result in accidental update of unknown tags without any warning. To prevent accidental updates of unknown tags, we do not support NOT EQUALS operator for update actions.

**Permissions**

**Managers with Full Scope**

**Users without Full Scope** must have these account permissions:
- Access Permission “API Access”
- Tag Permission “Edit User Tag”
- Tag Permission “Modify Dynamic Tag Rules” (to update a dynamic tag)

**Example**

**Request:**

This example renames parent tag 12345 and removes some of its child tags.

```bash
```

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

**Request POST data (file.xml):**

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <data>
    <Tag>
      <name>Parent Tag (Updated)</name>
      <children>
        <remove>
```
**Chapter 2 — Tag API**

**Update Tag**

```xml
<TagSimple><id>123</id></TagSimple>
<TagSimple><id>456</id></TagSimple>
</remove>
</children>
</Tag>
</data>
</ServiceRequest>

**Response:**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/gps/xsd/2.0/am/tag.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
    <data>
        <Tag>
            <id>12345</id>
            <name>Tag</name>
            <created>2014-02-06T19:14:50Z</created>
            <modified>2014-02-06T19:14:50Z</modified>
            <color>#FFFFFF</color>
            <ruleText>asset.installedSoftwares.contains { it.name == "Windows" }</ruleText>
            <ruleType>GROOVY</ruleType>
        </Tag>
    </data>
</ServiceResponse>
```

---

22 Qualys Asset Management and Tagging API
<id>123</id>
  <name>Linked Child 1</name>
</TagSimple>
</Tag>
</list>
</children>
</Tag>
</data>
</ServiceResponse>
Chapter 2 — Tag API

Search Tags

Returns a list of tags that match the provided criteria.

**URL**
https://<baseurl>/qps/rest/2.0/search/am/tag

**Method**
POST

**Pagination**
A maximum of 100 tags are returned by default. To customize this specify a “preferences” tag in the POST body of your request.

**Limit your results**
Use the optional “fields” parameter to limit the amount of information returned for each tag. Learn more

Searchable Fields

These fields can be used to search for tags.

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>id (Integer)</td>
<td>ruleType (Keyword: STATIC, GROOVY, OS_REGEX, NETWORK_RANGE, NAME_CONTAINS, INSTALLED_SOFTWARE, OPEN_PORTS, VULN_EXIST, ASSET_SEARCH, CLOUD_ASSET)</td>
</tr>
<tr>
<td>name (Text)</td>
<td>color (Text formatted as #FFFFFF where F can be any value between 0-9 and A-F)</td>
</tr>
<tr>
<td>parentTagId (Integer)</td>
<td></td>
</tr>
</tbody>
</table>

Allowed Operators

<table>
<thead>
<tr>
<th>Type</th>
<th>Operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integer</td>
<td>EQUALS, NOT EQUALS, GREATER, LESSER, IN</td>
</tr>
<tr>
<td>Text</td>
<td>CONTAINS, EQUALS, NOT EQUALS</td>
</tr>
<tr>
<td>Date</td>
<td>EQUALS, NOT EQUALS, GREATER, LESSER</td>
</tr>
<tr>
<td>Keyword</td>
<td>EQUALS, NOT EQUALS, IN</td>
</tr>
<tr>
<td>Boolean</td>
<td>(true/false) EQUALS, NOT EQUALS</td>
</tr>
</tbody>
</table>
Permissions

Managers with Full Scope

Users without Full Scope must have this account permission:
- Access Permission “API Access”

Example

Find all tags with Groovy Script tag rules.

Request:
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/search/am/tag" <
file.xml

Request POST data (file.xml):
<ServiceRequest>
  <filters>
    <Criteria field="ruleType" operator="EQUALS">GROOVY</Criteria>
  </filters>
</ServiceRequest>

Response:
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/tag.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>2</count>
  <data>
    <Tag>
      <id>12345</id>
      <name>Tag</name>
      <created>2014-02-06T19:14:50Z</created>
      <modified>2014-02-06T19:14:50Z</modified>
      <color>#FF0000</color>
      <ruleText>asset.installedSoftwares.contains { it.name == "Windows" }</ruleText>
    </Tag>
  </data>
</ServiceResponse>
<ruleType>GROOVY</ruleType>
<children>
  <list>
    <SimpleTag>
      <id>123</id>
      <name>Red</name>
    </SimpleTag>
    <list>
  </children>
</Tag>

<Tag>
  <id>12346</id>
  <name>Another Red Tag</name>
  <created>2014-02-06T19:14:50Z</created>
  <modified>2014-02-06T19:14:50Z</modified>
  <color>#FF0000</color>
  <ruleText>asset.installedSoftwares.contains { it.name == "Windows" }</ruleText>
  <ruleType>GROOVY</ruleType>
  <children>
    <list>
      <SimpleTag>
        <id>123</id>
        <name>Red</name>
      </SimpleTag>
      <list>
    </children>
  </Tag>
</ServiceResponse>
Count Tags

Count all the children of a tag.

**URL**
https://<baseurl>/qps/rest/2.0/count/am/tag

**Method**
POST

**Fields**

These fields can be used to count tags.

<table>
<thead>
<tr>
<th>id (Integer)</th>
<th>ruleType (Keyword: STATIC, GROOVY, OS_REGEX, NETWORK_RANGE, NAME_CONTAINS, INSTALLED_SOFTWARE, OPEN_PORTS, VULN_EXIST, ASSET_SEARCH, CLOUD_ASSET)</th>
</tr>
</thead>
<tbody>
<tr>
<td>name (Text)</td>
<td>color (Text formatted as #FFFFFF where F can be any value between 0-9 and A-F)</td>
</tr>
<tr>
<td>parentTagId (Integer)</td>
<td></td>
</tr>
</tbody>
</table>

**Allowed Operators**

<table>
<thead>
<tr>
<th>Type</th>
<th>Operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integer</td>
<td>EQUALS, NOT EQUALS, GREATER, LESSER, IN</td>
</tr>
<tr>
<td>Text</td>
<td>CONTAINS, EQUALS, NOT EQUALS</td>
</tr>
<tr>
<td>Date</td>
<td>EQUALS, NOT EQUALS, GREATER, LESSER</td>
</tr>
<tr>
<td>Keyword</td>
<td>EQUALS, NOT EQUALS, IN</td>
</tr>
<tr>
<td>Boolean</td>
<td>(true/false) EQUALS, NOT EQUALS</td>
</tr>
</tbody>
</table>
Permissions

Managers with Full Scope

Users without Full Scope must have this account permission:
- Access Permission “API Access”

Example

Get a count of all the children of tag ID 12345

Request:
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @- "https://qualysapi.qualys.com/qps/rest/2.0/count/am/tag" <
file.xml

Request POST data (file.xml):
<ServiceRequest>
  <filters>
    <Criteria field="parent" operator="EQUALS">12345</Criteria>
  </filters>
</ServiceRequest>

Response:
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/tag.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>2</count>
</ServiceResponse>
Delete Tag

Delete tags one or more tags.

**URL**

- `https://<baseurl>/qps/rest/2.0/delete/am/tag/<id>`
- `https://<baseurl>/qps/rest/2.0/delete/am/tag`

**Method**

- POST

Using the NOT EQUALS operator for deleting tags could result in accidental deletion of unknown tags without any warning. To prevent accidental deletion of unknown tags, we do not support NOT EQUALS operator for delete actions.

**Permissions**

Managers with Full Scope

Users without Full Scope must have these account permissions:
- Access Permission “API Access”
- Tag Permission “Delete User Tag”

**Examples**

Delete the tag that has the ID 12345.

**Request:**

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --data-binary @- "https://qualysapi.qualys.com/qps/rest/2.0/delete/am/tag/12345"
```

**Response:**

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/tag.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
    <data>
        <SimpleTag>
            <id>12345</id>
        </SimpleTag>
    </data>
</ServiceResponse>
```
Chapter 2 — Tag API
Delete Tag

</data>
</ServiceResponse>
Evaluate Tag

Force re-evaluation of one or more tags. Assets will be tagged only if they match the tag rule and are visible to the user. The dynamic tag evaluation feature must be turned on for your subscription in order to run this API.

**URL**

https://<baseurl>/qps/rest/2.0/evaluate/am/tag/<id>

or

https://<baseurl>/qps/rest/2.0/evaluate/am/tag

**Method**

POST

**Fields**

These fields can be used to evaluate tags.

<table>
<thead>
<tr>
<th>id (Integer)</th>
<th>ruleType (Keyword: STATIC, GROOVY, OS_REGEX, NETWORK_RANGE, NAME_CONTAINS, INSTALLED_SOFTWARE, OPEN_PORTS, VULN_EXIST, ASSET_SEARCH, CLOUD_ASSET)</th>
</tr>
</thead>
<tbody>
<tr>
<td>name (Text)</td>
<td>color (Text formatted as #FFFFFF where F can be any value between 0-9 and A-F)</td>
</tr>
<tr>
<td>parentTagId (Integer)</td>
<td></td>
</tr>
</tbody>
</table>

**Allowed Operators**

- **Integer**: EQUALS, NOT_EQUALS, GREATER, LESSER, IN
- **Text**: CONTAINS, EQUALS, NOT_EQUALS
- **Date**: EQUALS, NOT_EQUALS, GREATER, LESSER
- **Keyword**: EQUALS, NOT_EQUALS, IN
- **Boolean**: (true/false) EQUALS, NOT_EQUALS
Chapter 2 — Tag API
Evaluate Tag

Permissions

Managers with Full Scope

Users without Full Scope must have this account permission:
- Access Permission “API Access”

Examples

Evaluate all tags that have Groovy Script tag rules.

Request:
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/evaluate/am/tag"

Request POST data (file.xml):

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <filters>
    <Criteria field="ruleType" operator="EQUALS">GROOVY</Criteria>
  </filters>
</ServiceRequest>
```

Response:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/tag.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <Tag>
      <id>12345</id>
      <name>Tag</name>
      <created>2014-02-06T19:14:50Z</created>
      <modified>2014-02-06T19:14:50Z</modified>
      <color>#FF0000</color>
      <ruleText>asset.installedSoftwares.contains { it.name == "Windows" }</ruleText>
    </Tag>
  </data>
</ServiceResponse>
```
<ruleType>GROOVY</ruleType>
<children>
  <list>
    <SimpleTag>
      <id>123</id>
      <name>Red</name>
    </SimpleTag>
  </list>
</Tag>
</data>
</ServiceResponse>
List Users with their Tags

The Admin User API (/qps/rest/1.0/{action}/admin/user) gives information on users along with their tags to the authorized user. Currently, we support three actions for the users: search, count, and get details of a user.

**URL:**
https://qualysapi.qualys.com/qps/rest/1.0/{action}/admin/user

**Method allowed:** POST, GET

**Search Users (POST)**

You can search for users by using different filters for user ID, username, email, tags, and module names. If no filter is specified, all users in the user’s scope are listed.

**XSD:** User.XSD

**API Request:**
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @-
"https://qualysapi.qualys.com/qps/rest/1.0/search/admin/user" < file.xml

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

**Request POST Data (file.xml):**

```
<ServiceRequest>
   <filters>
      <Criteria field="username" operator="CONTAINS">10</Criteria>
   </filters>
</ServiceRequest>
```

**XML response:**

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/1.0/admin/user.xsd">  
   <responseCode>SUCCESS</responseCode>
   <count>1</count>
   <hasMoreRecords>false</hasMoreRecords>
   <data>
      <User>
         <id>3989626</id>
         <username>user_js10</username>
         <firstName><![CDATA[John]]></firstName>
         <lastName><![CDATA[Smith]]></lastName>
         <emailAddress>john.smith@afco.com</emailAddress>
```

```
Count Users (POST)

Returns the total number of users in the user’s scope.

XSD: User.XSD

API Request:

curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" 
--data-binary @-
"https://qualysapi.qualys.com/qps/rest/1.0/count/admin/user" < file.xml

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

Request POST Data (file.xml):

<ServiceRequest>
  <filters>
    <Criteria field="username" operator="CONTAINS">10</Criteria>
  </filters>
</ServiceRequest>

XML response:

<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
List Users with their Tags

Get details of a User

View details for a user in the user’s scope. You can use search action to find a user ID to use as input.

XSD: User.XSD

API Request:

curl -u "USERNAME:PASSWORD" -X GET -H "Content-type: text/xml" "https://qualysapi.qualys.com/qps/rest/1.0/get/admin/user/3989626" <

XML response:

<?xml version="1.0" encoding="UTF-8"?>
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <User>
      <id>3989626</id>
      <username>user_js10</username>
      <firstName><![CDATA[John]]></firstName>
      <lastName><![CDATA[Smith]]></lastName>
      <emailAddress>john.smith@afco.com</emailAddress>
      <tags>
        <count>1</count>
        <list>
          <Tag>
            <id>8721654</id>
            <name><![CDATA[Unassigned Business Unit]]></name>
          </Tag>
        </list>
      </tags>
      <modules>
        <count>5</count>
        <list>
          <Module>WAS</Module>
          <Module>ADMIN</Module>
        </list>
      </modules>
    </User>
  </data>
</ServiceResponse>
Chapter 2 — Tag API
List Users with their Tags

<ServiceResponse>
  <data>
    <User>
      <list>
        <Module>QWEB_PCI</Module>
        <Module>ASSET_MANAGEMENT</Module>
        <Module>QWEB_VM</Module>
      </list>
    </User>
  </data>
</ServiceResponse>
Tag Fields

<table>
<thead>
<tr>
<th>Writable</th>
<th>Read only</th>
</tr>
</thead>
<tbody>
<tr>
<td>parentTagId (Integer)</td>
<td>created (Date)</td>
</tr>
<tr>
<td>color (Text)</td>
<td>modified (Date)</td>
</tr>
<tr>
<td>ruleText (Text)</td>
<td></td>
</tr>
<tr>
<td>srcAssetGroupId (Integer)</td>
<td></td>
</tr>
<tr>
<td>srcBusinessUnitId (Integer)</td>
<td></td>
</tr>
<tr>
<td>srcOperatingSystemName (Text)</td>
<td></td>
</tr>
<tr>
<td>children (TagSimpleQList)</td>
<td></td>
</tr>
</tbody>
</table>

Associations

TagSimpleQList - Asset tags on the associated asset. This collection to be added to and removed from is provided as a tag ID wrapped in a TagSimple element.

TagSimple

<table>
<thead>
<tr>
<th>id</th>
<th>long (tag primary key)</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>string (tag name)</td>
</tr>
</tbody>
</table>
Host Asset API

The Host Asset API provides a suite of API functions for managing host assets. In many cases these are hosts detected by our cloud scanners. Host assets can also be added manually by the Qualys API or user interface. The HostAsset members identify operating system, NetBIOS, tags, open ports, NICs, installed software, EC2 source information and current vulnerabilities (all instances).

**Operations**
- Get Host Asset Info
- Create Host Asset
- Update Host Asset
- Search Hosts Assets
- Count Host Assets
- Delete Host Asset
- Activate Host Asset

**Reference**
- Host Asset Fields
Get Host Asset Info

Returns a single host asset by ID. This API returns additional EC2 metadata of Amazon EC2 hosts when inventoried using the Qualys EC2 Connector.

**URL**

https://<baseurl>/qps/rest/2.0/get/am/hostasset/<id>

**Method**

GET

**Limit your results**

Use the optional “fields” parameter to limit the amount of information returned for the host asset. [Learn more](#)

**Permissions**

Managers with Full Scope

Users without Full Scope must have these account settings: 1) scope includes the requested asset, and 2) permissions include:
- Access Permission “API Access”
- Asset Management Permission “Read Asset”

**Example**

**Example 1: Fetch host asset ID and list asset details**

**Request:**

curl -n -u "USERNAME:PASSWORD"
"https://qualysapi.qualys.com/qps/rest/2.0/get/am/hostasset/84021"

**Response:**

```xml
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <hasMoreRecords>false</hasMoreRecords>
  <data>
    <HostAsset>
      <id>84021</id>
      <name>10.10.23.245</name>
      <created>2016-02-12T06:21:54Z</created>
    </HostAsset>
  </data>
</ServiceResponse>
```
<modified>2016-02-13T01:14:34Z</modified>
<type>HOST</type>
<tags>
  <list>
    <TagSimple>
      <id>7539414</id>
      <name>Cloud Agent</name>
    </TagSimple>
  </list>
</tags>
<sourceInfo>
  <list>
    <AssetSource/>
  </list>
</sourceInfo>
<qwebHostId>18903</qwebHostId>
<os>Microsoft Windows XP Professional 5.1.2600 Service Pack 3 Build 2600</os>
<dnsHostName>XPSP2-32-27-145</dnsHostName>
<netbiosName>XPSP2-32-27-145</netbiosName>
<address>10.10.23.245</address>
<trackingMethod>QAGENT</trackingMethod>
<manufacturer>VMware, Inc.</manufacturer>
<model>VMware Virtual Platform</model>
<totalMemory>2047</totalMemory>
<timezone>-07:00</timezone>
<biosDescription>INTEL - 6040000</biosDescription>
<openPort>
  <list>
    <HostAssetOpenPort>
      <port>1900</port>
      <protocol>UDP</protocol>
    </HostAssetOpenPort>
    <HostAssetOpenPort>
      <port>7055</port>
      <protocol>TCP</protocol>
    </HostAssetOpenPort>
  </list>
</openPort>
<software>
  <list>
<HostAssetSoftware>
    <name>Security Update for Windows XP (KB2347290)</name>
    <version>1</version>
</HostAssetSoftware>
<HostAssetSoftware>
    <name>Security Update for Windows XP (KB950974)</name>
    <version>1</version>
</HostAssetSoftware>
</list>
</software>
<vuln>
    <list>
        <HostAssetVuln>
            <qid>118956</qid>
            <hostInstanceVulnId>296963</hostInstanceVulnId>
            <firstFound>2016-02-12T08:42:43Z</firstFound>
            <lastFound>2016-02-13T01:13:04Z</lastFound>
        </HostAssetVuln>
        <HostAssetVuln>
            <qid>119053</qid>
            <hostInstanceVulnId>296965</hostInstanceVulnId>
            <firstFound>2016-02-12T08:42:43Z</firstFound>
            <lastFound>2016-02-13T01:13:04Z</lastFound>
        </HostAssetVuln>
    </list>
</vuln>
<processor>
    <list>
        <HostAssetProcessor>
            <name>Intel Celeron processor</name>
            <speed>2799</speed>
        </HostAssetProcessor>
    </list>
</processor>
<volume>
    <list>
        <HostAssetVolume>
<name>A:</name>
<size>0</size>
<free>0</free>
</HostAssetVolume>
<HostAssetVolume>
  <name>C:</name>
  <size>16106090496</size>
  <free>2418925568</free>
</HostAssetVolume>
</list>
</volume>
<account>
  <list>
    <HostAssetAccount>
      <username>Administrator</username>
    </HostAssetAccount>
    <HostAssetAccount>
      <username>Guest</username>
    </HostAssetAccount>
  </list>
</account>
<networkInterface>
  <list>
    <HostAssetInterface>
      <hostname>XPSP2-32-27-145</hostname>
      <interfaceName>VMware Accelerated AMD PCNet Adapter - Packet Scheduler Miniport</interfaceName>
      <macAddress>00:50:56:A9:46:72</macAddress>
      <type>LOCAL</type>
      <address>10.10.23.245</address>
      <gatewayAddress>10.10.23.1</gatewayAddress>
    </HostAssetInterface>
  </list>
</networkInterface>
</HostAsset>
</data>
</ServiceResponse>
Example 2: Fetch host asset ID of AWS EC2 asset and list asset details

Request:
curl -n -u "USERNAME:PASSWORD" "https://qualysapi.qualys.com/qps/rest/2.0/get/am/hostasset/709838"

Response:
Tags for the EC2 asset appear in the `<Ec2AssetSourceSimple>` element, shown in bold below.

```xml
<?xml version="1.0" encoding="UTF-8"?>
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <HostAsset>
      <id>709838</id>
      <name>my-ec2-target</name>
      <created>2017-07-27T18:14:28Z</created>
      <modified>2017-07-27T18:21:31Z</modified>
      <type>HOST</type>
      <tags>
        <list/>
      </tags>
      <sourceInfo>
        <list>
          <Ec2AssetSourceSimple>
            <firstDiscovered>2017-07-27T18:14:28Z</firstDiscovered>
            <lastUpdated>2017-07-27T19:51:03Z</lastUpdated>
            <assetId>709838</assetId>
            <ec2InstanceTags>
              <tags>
                <list>
                  <EC2Tags>
                    <key>Department</key>
                    <value>Security</value>
                  </EC2Tags>
                  <EC2Tags>
                    <key>Owner</key>
                    <value>Jason Kim</value>
                  </EC2Tags>
                  <EC2Tags>
                    <key>Email</key>
                    <value>jkim@acme.com</value>
                  </EC2Tags>
                </list>
              </tags>
            </ec2InstanceTags>
          </Ec2AssetSourceSimple>
        </list>
      </sourceInfo>
    </HostAsset>
  </data>
</ServiceResponse>
```
<EC2Tags>
    <key>JIRA</key>
    <value>POR-6719</value>
</EC2Tags>

<EC2Tags>
    <key>Name</key>
    <value>my-ec2-target</value>
</EC2Tags>

<EC2Tags>
    <key>Lifecycle</key>
    <value>20171231</value>
</EC2Tags>

<availabilityZone>us-east-1e</availabilityZone>
<instanceId>i-023b166432bic7afc</instanceId>
<instanceType>t2.medium</instanceType>
<createdDate>2017-07-27T19:58:34Z</createdDate>
<instanceState>STOPPED</instanceState>
<groupId>sg-6b619117</groupId>
<groupName>default</groupName>
<spotInstance>true</spotInstance>
<accountId>205767712438</accountId>
<subnetId>subnet-7bbcd56</subnetId>
<vpcId>vpc-2da7154b</vpcId>
<region>us-east-1</region>
<zone>VPC</zone>
<imageId>ami-22ce4934</imageId>
<pUBLICIpAddress>127.0.0.1</publicIpAdDress>
<privateIpAddress>10.97.15.117</privateIpAddress>
<monitoringEnabled>false</monitoringEnabled>
</Ec2AssetSourceSimple>
</sourceInfo>
/qwebHostId>12864</qwebHostId>
<os>Linux</os>
<address>10.97.15.117</address>
<trackingMethod>INSTANCE_ID</trackingMethod>
<openPort>
    <list/>
</openPort>
<software>
    <list/>
</software>
<vuln>
    <list/>
</vuln>
<processor>
Chapter 3 — Host Asset API
Get Host Asset Info

Example 3: Fetch host asset ID with docker information

Request:
curl -n -u "USERNAME:PASSWORD"
"https://qualysapi.qualys.com/qps/rest/2.0/get/am/hostasset/7727721"

Response:
Tags for the docker information appear in the <dockerInfo> element, shown in bold below.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/hostasset.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
    <data>
        <HostAsset>
            <id>7727721</id>
            <name>10.113.198.121</name>
            <created>2018-06-15T11:51:26Z</created>
            <modified>2018-06-15T11:51:26Z</modified>
            <type>HOST</type>
            <tags>
                <list/>
            </tags>
        </HostAsset>
    </data>
</ServiceResponse>
```
<TagSimple>
  <id>8910214</id>
  <name>SSD27701</name>
</TagSimple>
<TagSimple>
  <id>9252992</id>
  <name>All_data1</name>
</TagSimple>

<qwebHostId>707520</qwebHostId>
<lastVulnScan>2018-06-15T11:48:58Z</lastVulnScan>
<os>CentOS Linux 7.2.1511</os>
<address>10.113.198.121</address>
<trackingMethod>IP</trackingMethod>

<openPort>
  <list>
    <HostAssetOpenPort>
      <port>8080</port>
      <protocol>TCP</protocol>
      <serviceId>1180</serviceId>
      <serviceName>HyperText Transport Protocol</serviceName>
    </HostAssetOpenPort>
  </list>
</openPort>

<vuln>
  <list>
    <HostAssetVuln>
      <qid>45038</qid>
      <hostInstanceVulnId>151189845</hostInstanceVulnId>
      <lastFound>2018-06-15T11:48:58Z</lastFound>
    </HostAssetVuln>
  </list>
</vuln>

<networkInterface>
  <list>
    <HostAssetInterface>
      <type>LOCAL</type>
      <address>10.113.198.121</address>
    </HostAssetInterface>
  </list>
</networkInterface>

<isDockerHost>true</isDockerHost>
<dockerInfo>
  <dockerVersion>18.06.0-ce-rc1</dockerVersion>
  <noOfContainers>1</noOfContainers>
  <noOfImages>2</noOfImages>
</dockerInfo>
Chapter 3 — Host Asset API
Get Host Asset info

```xml
</dockerInfo>
</HostAsset>
</data>
</ServiceResponse>
```
Create Host Asset

Create one or more host assets using writable fields and collections. It is a good idea to attach tags that will make new assets visible to the current user if that user does not have permission to see all assets. Otherwise users will not be able to see or modify the new assets until an administrator or process attaches the appropriate tags to them.

What’s next? Once you’ve created new host assets you need to activate the assets in order to make them available for scanning and reporting in the Vulnerability Management (VM) module. See Activate Host Asset

**Permissions**

Managers with Full Scope

Users without Full Scope must have these account permissions:
- Access Permission “API Access”
- Asset Management Permission “Create Asset”

**Example**

**Example 1: Create new host asset with tags**

**Request:**

curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST" --data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/create/am/hostasset" < file.xml

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

**Request POST data (file.xml):**

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <data>
    <HostAsset>
      <name>My Windows Asset</name>
      <os>Windows 7</os>
      <dnsHostName>localhost</dnsHostName>
      <netbiosName>TEST</netbiosName>
    </HostAsset>
  </data>
</ServiceRequest>
```

URL: https://<baseurl>/qps/rest/2.0/create/am/hostasset

Method: POST
<netbiosNetworkId>10</netbiosNetworkId>
<networkGuid>66bf43c8-7392-4257-b856-a320fde231eb</networkGuid>
<address>127.0.0.1</address>
<trackingMethod>IP</trackingMethod>
<tags>
  <set>
    <TagSimple><id>12345</id></TagSimple>
    <TagSimple><id>54321</id></TagSimple>
  </set>
</tags>
<software>
  <set>
    <HostAssetSoftware>
      <name>Photoshop</name>
      <version>9</version>
    </HostAssetSoftware>
  </set>
</software>
</HostAsset>
</data>
</ServiceRequest>

Response:
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/hostasset.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <HostAsset>
      <id>2020094</id>
      <name>My Windows Asset</name>
      <created>2014-02-06T19:16:35Z</created>
      <modified>2014-02-06T19:16:35Z</modified>
      <type>HOST</type>
      <tags>
        <list>
          <TagSimple>
Example 2: Bulk creation of assets

Request:

curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST" --data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/create/am/hostasset" < file.xml

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

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
    <data>
        <HostAsset>
            <name>My Windows Asset</name>
            <os>Windows 8</os>
            <dnsHostName>localhost13</dnsHostName>
            <netbiosName>TEST</netbiosName>
            <netbiosNetworkId>10</netbiosNetworkId>
            <networkGuid>66bf43c8-7392-4257-b856-a320fde231eb</networkGuid>
            <address>13.0.0.1</address>
            <trackingMethod>IP</trackingMethod>
            <software>
                <set>
                    <HostAssetSoftware>
                        <name>Photoshop</name>
                        <version>9</version>
                    </HostAssetSoftware>
                </set>
            </software>
        </HostAsset>
        <HostAsset>
            <name>My Windows Asset</name>
            <os>Windows 8</os>
            <dnsHostName>localhost14</dnsHostName>
            <netbiosName>TEST</netbiosName>
            <netbiosNetworkId>10</netbiosNetworkId>
            <networkGuid>66bf43c8-7392-4257-b856-a320fde231eb</networkGuid>
            <address>14.0.0.1</address>
            <trackingMethod>IP</trackingMethod>
            <software>
                <set>
                    <HostAssetSoftware>
                        <name>Photoshop</name>
                        <version>9</version>
                    </HostAssetSoftware>
                </set>
            </software>
        </HostAsset>
    </data>
</ServiceRequest>
```
Response:

<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/hostasset.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>2</count>
  <data>
    <HostAsset>
      <id>2899060</id>
      <name>My Windows Asset</name>
      <created>2016-04-01T16:57:50Z</created>
      <modified>2016-04-01T16:57:50Z</modified>
      <type>HOST</type>
      <tags>
        <list/>
      </tags>
      <sourceInfo>
        <list/>
      </sourceInfo>
      <os>Windows 8</os>
      <dnsHostName>localhost13</dnsHostName>
      <netbiosName>TEST</netbiosName>
      <netbiosNetworkId>10</netbiosNetworkId>
      <networkGuid>66bf43c8-7392-4257-b856-a320fde231eb</networkGuid>
      <address>13.0.0.1</address>
      <trackingMethod>IP</trackingMethod>
      <openPort>
        <list/>
      </openPort>
      <software>
        <list>
          <HostAssetSoftware>
            <name>Photoshop</name>
            <version>9</version>
        </HostAssetSoftware>
      </software>
    </HostAsset>
  </data>
</ServiceResponse>
Create Host Asset

</HostAssetSoftware>
</list>
</software>
<vuln>
<list/>
</vuln>
<processor>
<list/>
</processor>
</HostAsset>
</HostAsset>

<HostAsset>
<id>2899061</id>
<name>My Windows Asset</name>
<created>2016-04-01T16:57:51Z</created>
<modified>2016-04-01T16:57:51Z</modified>
<type>HOST</type>
<tags>
<list/>
</tags>
<sourceInfo>
<list/>
</sourceInfo>
<os>Windows 8</os>
<dnsHostName>localhost14</dnsHostName>
<netbiosName>TEST</netbiosName>
<netbiosNetworkId>10</netbiosNetworkId>
<networkGuid>66bf43c8-7392-4257-b856-a320fde231eb</networkGuid>
<address>14.0.0.1</address>
<trackingMethod>IP</trackingMethod>
<openPort>
<list/>
</openPort>
<software>
<list>
<HostAssetSoftware>
<name>Photoshop</name>
<version>9</version>
</HostAssetSoftware>
</list>
</software>
<vuln>
<list/>
</vuln>
<processor>
<list/>
</processor>
<volume>
<list/>
</volume>
<account>
<list/>
</account>
<networkInterface>
<list>
<HostAssetInterface>
<hostname>localhost14</hostname>
<type>LOCAL</type>
<address>14.0.0.1</address>
</HostAssetInterface>
</list>
</networkInterface>
</HostAsset>
</data>
</ServiceResponse>
Update Host Asset

Update fields for a host asset and collections of host assets.

**URL**

https://<baseurl>/qps/rest/2.0/update/am/hostasset/<id>

or

https://<baseurl>/qps/rest/2.0/update/am/hostasset

**Method**

POST

Using the NOT EQUALS operator for updating host assets could result in accidental update of unknown host assets without any warning. To prevent accidental updates of unknown host assets, we do not support NOT EQUALS operator for update actions.

**Permissions**

Managers with Full Scope

Users without Full Scope must have these account settings: 1) scope includes the requested asset(s), and 2) permissions include:
- Access Permission “API Access”
- Asset Management Permission “Update Asset”

**Example**

**Request 1:**

Update some of the fields for host asset ID 12345.

```bash
```

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

**Request POST data (file.xml):**

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <Asset><data>
    <HostAsset>
      <name>Updated Name</name>
      <os>WINDOWS 95</os>
    </HostAsset>
  </Asset>
</ServiceRequest>
```

56 Qualys Asset Management and Tagging API
<dnsHostName>win95.old.corp.net</dnsHostName>
</HostAsset>
</data>
</ServiceRequest>

Response:
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/hostasset.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <HostAsset>
      <id>2020094</id>
      <name>Updated Name</name>
      <os>WINDOWS 95</os>
      <dnsHostName>win95.old.corp.net</dnsHostName>
      <created>2014-02-06T19:16:35Z</created>
      <modified>2014-02-06T19:16:35Z</modified>
      <type>HOST</type>
      <tags>
        <list />
      </tags>
      <sourceInfo>
        <list/>
      </sourceInfo>
      <netbiosName>TEST</netbiosName>
      <netbiosNetworkId>10</netbiosNetworkId>
      <networkGuid>66bf43c8-7392-4257-b856-a320fde231eb</networkGuid>
      <address>127.0.0.1</address>
      <trackingMethod>IP</trackingMethod>
      <openPort>
        <list/>
      </openPort>
      <software>
        <list/>
      </software>
      <vuln>
        <list/>
      </vuln>
    </HostAsset>
  </data>
</ServiceResponse>
Chapter 3 — Host Asset API
Update Host Asset

```xml
  <ServiceResponse>
    <data>
      <HostAsset>
        <tags>
          <add>
            <TagSimple><id>12345</id></TagSimple>
          </add>
          <remove>
            <TagSimple><id>54321</id></TagSimple>
          </remove>
        </tags>
        <software>
          <set>
            <HostAssetSoftware>
              <name>Windows</name>
              <version>95</version>
            </HostAssetSoftware>
          </set>
        </software>
        <openPort>
          <add>
            <HostAssetOpenPort>
```

**Request 2:**

Update some of the fields for host assets that have names containing the word OLD.

```bash
curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST"
--data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/update/am/hostasset" < file.xml
```

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

**Request POST data (file.xml):**

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <filters>
    <Criteria field="name" operator="CONTAINS">OLD</Criteria>
  </filters>
  <data>
    <HostAsset>
      <tags>
        <add>
          <TagSimple><id>12345</id></TagSimple>
        </add>
        <remove>
          <TagSimple><id>54321</id></TagSimple>
        </remove>
      </tags>
      <software>
        <set>
          <HostAssetSoftware>
            <name>Windows</name>
            <version>95</version>
          </HostAssetSoftware>
        </set>
      </software>
      <openPort>
        <add>
          <HostAssetOpenPort>
```

58 Qualys Asset Management and Tagging API
Chapter 3 — Host Asset API

Update Host Asset

<port>8080</port>
<protocol>TCP</protocol>
</HostAssetOpenPort>
</add>
</openPort>
</HostAsset>
</data>
</ServiceRequest>

Response:
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/hostasset.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
    <data>
        <HostAsset>
            <id>2020094</id>
            <name>Updated Name</name>
            <os>WINDOWS 95</os>
            <dnsHostName>win95.old.corp.net</dnsHostName>
            <created>2014-02-06T19:16:35Z</created>
            <modified>2014-02-06T19:16:35Z</modified>
            <type>HOST</type>
            <tags>
                <list>
                    <TagSimple>
                        <id>12345</id>
                        <name>Simple Tag 1</name>
                    </TagSimple>
                </list>
            </tags>
            <sourceInfo>
                <list/>
            </sourceInfo>
            <netbiosName>TEST</netbiosName>
            <netbiosNetworkId>10</netbiosNetworkId>
            <networkGuid>66bf43c8-7392-4257-b856-a320fde231eb</networkGuid>
        </HostAsset>
    </data>
</ServiceResponse>
<address>127.0.0.1</address>
<trackingMethod>IP</trackingMethod>
<openPort>
  <list>
    <HostAssetOpenPort>
      <port>8080</port>
      <protocol>TCP</protocol>
    </HostAssetOpenPort>
  </list>
</openPort>
<software>
  <list>
    <HostAssetSoftware>
      <name>Windows</name>
      <version>95</version>
    </HostAssetSoftware>
  </list>
</software>
<vuln>
  <list/>
</vuln>
</HostAsset>
</data>
</ServiceResponse>
Search Hosts Assets

Returns a list of host assets matching the provided criteria. Assets are returned when they are visible to the user (i.e. in the user’s scope).

**URL**

https://<baseurl>/qps/rest/2.0/search/am/hostasset

**Method**

POST

**Pagination**

A maximum of 100 host assets are returned by default. To customize this specify a “preferences” tag in the POST body of your request.

**Limit your results**

Use the optional “fields” parameter to limit the amount of information returned for each host asset. Learn more

**Searchable Fields**

These fields can be used to search for host assets.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>qwebHostId (Integer)</td>
<td>netbiosName (Text)</td>
</tr>
<tr>
<td>lastVulnScan (Date)</td>
<td>netbiosNetworkID (Text)</td>
</tr>
<tr>
<td>lastComplianceScan (Date)</td>
<td>networdGuid (Text)</td>
</tr>
<tr>
<td>informationGatheredUpdated (Date)</td>
<td>trackingMethod (Keyword: NONE, IP, DNSNAME, NETBIOS, INSTANCE_ID, QAGENT)</td>
</tr>
<tr>
<td>os (Text)</td>
<td>port (Integer)</td>
</tr>
<tr>
<td>dnsHostName (Text)</td>
<td>installedSoftware (Text)</td>
</tr>
<tr>
<td>address (Text)</td>
<td>tagName (Text)</td>
</tr>
<tr>
<td>vulnsUpdated (Date)</td>
<td>tagId (Integer)</td>
</tr>
<tr>
<td>id (Integer)</td>
<td>netbiosName (Text)</td>
</tr>
<tr>
<td>name (Text)</td>
<td>netbiosNetworkId (Text)</td>
</tr>
<tr>
<td>created (Date)</td>
<td>update (Date)</td>
</tr>
<tr>
<td>type (Text)</td>
<td>agentVersion (String)</td>
</tr>
<tr>
<td>activationKey (String)</td>
<td>agentConfigurationId (Long)</td>
</tr>
<tr>
<td>agentConfigurationName (String)</td>
<td>lastCheckedIn (Date)</td>
</tr>
</tbody>
</table>
**Chapter 3 — Host Asset API**

Search Hosts Assets

Allowed Operators

<table>
<thead>
<tr>
<th>Type</th>
<th>Operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integer</td>
<td>EQUALS, NOT EQUALS, GREATER, LESSER, IN</td>
</tr>
<tr>
<td>Text</td>
<td>CONTAINS, EQUALS, NOT EQUALS</td>
</tr>
<tr>
<td>Date</td>
<td>EQUALS, NOT EQUALS, GREATER, LESSER</td>
</tr>
<tr>
<td>Keyword</td>
<td>EQUALS, NOT EQUALS, IN</td>
</tr>
<tr>
<td>Boolean</td>
<td>(true/false) EQUALS, NOT EQUALS</td>
</tr>
</tbody>
</table>

These fields can be used to search for cloud agents installed on host assets.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Allowed Operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>agentVersion (String)</td>
<td>EQUALS, LESSER, GREATER</td>
</tr>
<tr>
<td>activationKey (String)</td>
<td>EQUALS</td>
</tr>
<tr>
<td>agentConfigurationId (Long)</td>
<td>EQUALS</td>
</tr>
<tr>
<td>agentConfigurationName (String)</td>
<td>EQUALS, CONTAINS</td>
</tr>
<tr>
<td>lastCheckedIn (Date)</td>
<td>EQUALS, LESSER, GREATER</td>
</tr>
</tbody>
</table>

**Permissions**

Managers with Full Scope

Users without Full Scope must have these account permissions:
- Access Permission “API Access”
- Asset Management Permission “Read Asset”
Example

Request 1:
Find host assets with a Windows operating system that are tracked by Instance ID.
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/search/am/hostasset" <
file.xml

Request POST data (file.xml):
<pre>
<ServiceRequest>
  <filters>
    <Criteria field="os" operator="EQUALS">Windows</Criteria>
    <Criteria field="trackingMethod" operator="EQUALS">INSTANCE_ID</Criteria>
  </filters>
</ServiceRequest>
</pre>

Response:
<pre>
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/hostasset.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <HostAsset>
      <id>2020094</id>
      <name>Updated Name</name>
      <os>Windows</os>
      <dnsHostName>win95.old.corp.net</dnsHostName>
      <created>2014-02-06T19:16:35Z</created>
      <modified>2014-02-06T19:16:35Z</modified>
      <type>HOST</type>
      <tags>
        <list />
      </tags>
      <sourceInfo>
        <list/>
      </sourceInfo>
    </HostAsset>
  </data>
</ServiceResponse>
</pre>
<netbiosName>TEST</netbiosName>
<netbiosNetworkId>10</netbiosNetworkId>
<networkGuid>66bf43c8-7392-4257-b856-a320fde231eb</networkGuid>
<address>127.0.0.1</address>
<trackingMethod>INSTANCE_ID</trackingMethod>
<openPort>
  <list/>
</openPort>
<software>
  <list/>
</software>
<vuln>
  <list/>
</vuln>
</HostAsset>
</data>
</ServiceResponse>

Request 2:
Find cloud agents with a specific agent version.

```
```

Request POST data (host_asset_search.xml):
```
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <filters>
    <Criteria field="agentVersion" operator="EQUALS">1.4.5.168</Criteria>
    <Criteria field="tagName" operator="EQUALS">Cloud Agent</Criteria>
  </filters>
</ServiceRequest>
```

Response:
```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
<responseCode>SUCCESS</responseCode>
<count>6</count>
<hasMoreRecords>false</hasMoreRecords>
<data>
  <HostAsset>
    <id>3043442</id>
    <name>102115-M83</name>
    <created>2016-11-04T11:43:40Z</created>
    <modified>2016-11-08T22:35:53Z</modified>
    <type>HOST</type>
    <tags>
      <list>
        <TagSimple>
          <id>8832525</id>
          <name>Cloud Agent</name>
        </TagSimple>
      </list>
    </tags>
    <sourceInfo>
      <list>
        <AssetSource/>
      </list>
    </sourceInfo>
    <qwebHostId>12688456922</qwebHostId>
    <dnsHostName>102115-M83</dnsHostName>
    <agentInfo>
      <agentVersion>1.4.5.168</agentVersion>
      <agentId>2e689bb2-53ab-4a58-be0a-a7576964f310</agentId>
      <status>STATUS_INACTIVE</status>
      <lastCheckedIn>2016-10-21T19:03:30Z</lastCheckedIn>
      <connectedFrom>10.100.11.163</connectedFrom>
      <chirpStatus>Manifest Downloaded</chirpStatus>
      <platform>Windows</platform>
      <agentConfiguration>
        <id>8099</id>
        <name>Initial Profile - SSN3</name>
      </agentConfiguration>
      <activationKey>
Host Asset API

Search Hosts Assets

Request 3:

Find host assets with specific ID containing docker information.

Chapter 3 — Host Asset API
Search Hosts Assets

Request POST data (file.xml):

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceRequest>
  <filters>
    <Criteria field="id" operator="EQUALS">7727721</Criteria>
  </filters>
</ServiceRequest>
```

Response:

```xml
<?xml version="1.0" encoding="UTF-8"?>
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <hasMoreRecords>false</hasMoreRecords>
  <data>
    <HostAsset>
      <id>7727721</id>
      <name>10.113.198.121</name>
      <created>2018-06-15T11:51:26Z</created>
      <modified>2018-06-15T11:51:26Z</modified>
      <type>HOST</type>
      <tags>
        <list>
          <TagSimple>
            <id>8910214</id>
            <name>SSD27701</name>
          </TagSimple>
          <TagSimple>
            <id>9252992</id>
            <name>All_data1</name>
          </TagSimple>
        </list>
      </tags>
      <qwebHostId>707520</qwebHostId>
      <lastVulnScan>2018-06-15T11:48:58Z</lastVulnScan>
      <os>CentOS Linux 7.2.1511</os>
      <address>10.113.198.121</address>
      <trackingMethod>IP</trackingMethod>
      <openPort>
```

67   Qualys Asset Management and Tagging API
<list>
  <HostAssetOpenPort>
    <port>8080</port>
    <protocol>TCP</protocol>
    <serviceId>1180</serviceId>
    <serviceName>HyperText Transport Protocol</serviceName>
  </HostAssetOpenPort>
</list>

<vuln>
  <list>
    <HostAssetVuln>
      <qid>6</qid>
      <hostInstanceVulnId>151189838</hostInstanceVulnId>
      <lastFound>2018-06-15T11:48:58Z</lastFound>
    </HostAssetVuln>
    <HostAssetVuln>
      <qid>45038</qid>
      <hostInstanceVulnId>151189845</hostInstanceVulnId>
      <lastFound>2018-06-15T11:48:58Z</lastFound>
    </HostAssetVuln>
  </list>
</vuln>

<networkInterface>
  <list>
    <HostAssetInterface>
      <type>LOCAL</type>
      <address>10.113.198.121</address>
    </HostAssetInterface>
  </list>
</networkInterface>

<isDockerHost>true</isDockerHost>
<dockerInfo>
  <dockerVersion>18.06.0-ce-rc1</dockerVersion>
  <noOfContainers>1</noOfContainers>
Chapter 3 — Host Asset API
Search Hosts Assets

Request 4:
Find host assets with specific ID containing split manifest version information for VM, PC, or SCA.

API request:

Request POST data: (Contents of file.xml)
<?xml version="1.0" encoding="UTF-8"?>
<ServiceRequest>
  <filters>
    <Criteria field="id" operator="EQUALS">7866685</Criteria>
  </filters>
</ServiceRequest>

XML output:
<?xml version="1.0" encoding="UTF-8"?>
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <hasMoreRecords>false</hasMoreRecords>
  <data>
    <HostAsset>
      <id>7866685</id>
      <name>ip-172-31-3-82.ap-south-1.compute.internal</name>
      <created>2018-08-01T09:34:44Z</created>
      <modified>2018-08-10T08:39:49Z</modified>
      <type>HOST</type>
      <tags>
<list>
  <TagSimple>
    <id>10125654</id>
    <name>Cloud Agent</name>
  </TagSimple>
</list>
</tags>
<sourceInfo>
  <list>
    <AssetSource/>
    <Ec2AssetSourceSimple>
      <assetId>7866685</assetId>
      <type>EC_2</type>
      <firstDiscovered>2018-08-01T09:34:45Z</firstDiscovered>
      <lastUpdated>2018-08-01T09:34:45Z</lastUpdated>
      <reservationId>r-0cd44450f874d4a08</reservationId>
      <availabilityZone>ap-south-1b</availabilityZone>
      <privateDnsName>ip-172-31-3-82.ap-south-1.compute.internal</privateDnsName>
      <publicDnsName>ec2-13-232-170-59.ap-south-1.compute.amazonaws.com</publicDnsName>
      <localHostname>ip-172-31-3-82.ap-south-1.compute.internal</localHostname>
      <instanceId>i-0ce729520a8a7d696</instanceId>
      <instanceType>t2.micro</instanceType>
      <instanceState>RUNNING</instanceState>
      <groupId>sg-608b270a</groupId>
      <groupName>launch-wizard-4</groupName>
      <spotInstance>false</spotInstance>
      <accountId>383031258652</accountId>
      <subnetId>subnet-5a0d6a17</subnetId>
      <vpcId>vpc-39ccea50</vpcId>
      <region>ap-south-1</region>
      <zone>VPC</zone>
      <imageId>ami-5b673c34</imageId>
    </Ec2AssetSourceSimple>
  </list>
</sourceInfo>
<publicIpAddress>13.232.170.59</publicIpAddress>
<privateIpAddress>172.31.3.82</privateIpAddress>
  <macAddress>0a:da:e8:58:09:fe</macAddress>
  <monitoringEnabled>false</monitoringEnabled>
</Ec2AssetSourceSimple>
</list>
</sourceInfo>
<qwebHostId>753424</qwebHostId>
<lastComplianceScan>2018-08-10T00:25:12Z</lastComplianceScan>
<lastVulnScan>2018-08-10T04:55:06Z</lastVulnScan>
<lastSystemBoot>2018-08-01T09:23:42Z</lastSystemBoot>
<lastLoggedOnUser>ec2-user</lastLoggedOnUser>
<os>Red Hat Enterprise Linux Server 7.5</os>
<dnsHostName>ip-172-31-3-82.ap-south-1.compute.internal</dnsHostName>
<agentInfo>
  <agentVersion>1.7.1.38</agentVersion>
  <agentId>66fb86e4-9609-4324-8eec-48ab6cb7f260</agentId>
  <status>STATUS_ACTIVE</status>
  <lastCheckedIn>2018-08-10T08:39:42Z</lastCheckedIn>
  <connectedFrom>13.232.170.59</connectedFrom>
  <location>Mumbai,Maharashtra India</location>
  <locationGeoLatitude>18.975</locationGeoLatitude>
  <locationGeoLongtitude>72.8258</locationGeoLongtitude>
  <chirpStatus>Inventory Scan Complete</chirpStatus>
  <platform>Linux</platform>
</agentInfo>
<activatedModule>AGENT_VM,AGENT_PC</activatedModule>
<manifestVersion>
  <vm>VULNSIGS-VM-0.12.1.0-17</vm>
  <pc>VULNSIGS-PC-0.17.0.0-27</pc>
</manifestVersion>
<agentConfiguration>
  <id>514001</id>
  <name>My Default</name>
</agentConfiguration>
<activationKey>
  <activationId>f9391862-de71-4106-9478-ca14042980dd</activationId>
</activationKey>
<activationKey/>
</agentInfo>
<networkGuid>6b48277c-0742-61c1-82bb-cac0f9c4094a</networkGuid>
<address>13.232.170.59</address>
<trackingMethod>QAGENT</trackingMethod>
<totalMemory>990</totalMemory>
<timezone>UTC</timezone>
<openPort>
<li>
<HostAssetOpenPort>
<header>323</header>
<protocol>UDP</protocol>
</HostAssetOpenPort>
...
</li>
</openPort>
<software>
<li>
<HostAssetSoftware>
<header>GeoIP</header>
<version>1.5.0-11.el7</version>
</HostAssetSoftware>
<HostAssetSoftware>
<header>NetworkManager</header>
<version>1.10.2-13.el7</version>
</HostAssetSoftware>
...
</li>
</software>
<vuln>
<li>
<HostAssetVuln>
<header>370198</header>
</HostAssetVuln>
<hostInstanceId>157377851</hostInstanceId>
<firstFound>2018-08-06T10:08:37Z</firstFound>
<lastFound>2018-08-10T04:55:06Z</lastFound>
</HostAssetVuln>
<HostAssetVuln>
<header>370472</header>
</HostAssetVuln>
<macAddress>0a:da:e8:58:09:fe</macAddress>
<type>LOCAL</type>

<address>fe80:0:0:0:8da:e8ff:fe58:9fe</address>
  <gatewayAddress>172.31.0.1</gatewayAddress>
</HostAssetInterface>
...
</list>
</networkInterface>
</HostAsset>
</data>
</ServiceResponse>
Count Host Assets

Returns the number of host assets that match the provided criteria. A host asset is counted when the asset is visible to the user (i.e. it is in the user’s scope).

**URL**
https://<baseurl>/qps/rest/2.0/count/am/hostasset

**Method**
POST

**Fields**

These fields can be used to count host assets.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>qwebHostId (Integer)</td>
<td>netbiosName (Text)</td>
</tr>
<tr>
<td>lastVulnScan (Date)</td>
<td>netbiosNetworkID (Text)</td>
</tr>
<tr>
<td>lastComplianceScan (Date)</td>
<td>networdGuid (Text)</td>
</tr>
<tr>
<td>informationGatheredUpdated (Date)</td>
<td>trackingMethod (Keyword: NONE, IP, DNSNAME, NETBIOS, INSTANCE_ID, QAGENT)</td>
</tr>
<tr>
<td>os (Text)</td>
<td>port (Integer)</td>
</tr>
<tr>
<td>dnsHostName (Text)</td>
<td>installedSoftware (Text)</td>
</tr>
<tr>
<td>address(Text)</td>
<td>tagName (Text)</td>
</tr>
<tr>
<td>vulnsUpdated(Date)</td>
<td>tagId (Integer)</td>
</tr>
<tr>
<td>id (Integer)</td>
<td>netbiosName (Text)</td>
</tr>
<tr>
<td>name (Text)</td>
<td>netbiosNetworkId (Text)</td>
</tr>
<tr>
<td>created (Date)</td>
<td>update (Date)</td>
</tr>
<tr>
<td>type (Text)</td>
<td></td>
</tr>
</tbody>
</table>

**Allowed Operators**

- Integer: EQUALS, NOT EQUALS, GREATER, LESSER, IN
- Text: CONTAINS, EQUALS, NOT EQUALS
- Date: EQUALS, NOT EQUALS, GREATER, LESSER
- Keyword: EQUALS, NOT EQUALS, IN
- Boolean: (true/false) EQUALS, NOT EQUALS
Permissions

Managers with Full Scope

Users without Full Scope must have these account permissions:
- Access Permission “API Access”
- Asset Management Permission “Read Asset”

Example

Request:

curl -u "USERNAME:PASSWORD" -X POST --data-binary @-
https://qualysapi.qualys.com/qps/rest/2.0/count/am/hostasset -H
vContent-Type: application/xml" < file.xml

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

Request POST data (file.xml):

<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <filters>
    <Criteria field="os" operator="EQUALS">Windows</Criteria>
  </filters>
</ServiceRequest>

Response:

<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/hostasset.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>235</count>
</ServiceResponse>
Delete Host Asset

Delete one or more host assets.

**URL**

https://<baseurl>/qps/rest/2.0/delete/am/hostasset/<id>

or

https://<baseurl>/qps/rest/2.0/delete/am/hostasset

**Method**

POST

Using the NOT EQUALS operator for deleting host assets could result in accidental deletion of unknown host assets without any warning. To prevent accidental deletion of unknown host assets, we do not support NOT EQUALS operator for delete actions.

**Permissions**

Managers with Full Scope

Users without Full Scope must have these account settings: 1) scope includes the requested asset(s), and 2) permissions include:

- Access Permission “API Access”
- Asset Management Permission “Delete Asset”

**Example**

Delete host assets with the tag “To Delete”.

**Request:**

curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @- "https://qualysapi.qualys.com/qps/rest/2.0/delete/am/hostasset" < file.xml

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

**Request POST data (file.xml):**

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <filters>
    <Criteria field="tagName" operator="EQUALS">To Delete</Criteria>
  </filters>
</ServiceRequest>
```
Chapter 3 — Host Asset API
Delete Host Asset

Response:
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/hostasset.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
    <data>
        <HostAsset>
            <id>2020094</id>
        </HostAsset>
    </data>
</ServiceResponse>
Activate Host Asset

Activate one or more assets to make them available in your account for scanning and reporting. You’ll want to activate newly created hosts to make them available in the Vulnerability Management (VM) application module and/or the Policy Compliance (PC) module.

**URL for VM assets**

https://<baseurl>/qps/rest/2.0/activate/am/hostasset/<id>?
module=QWEB_DM
or
https://<baseurl>/qps/rest/2.0/activate/am/hostasset?
module=QWEB_DM

**URL for PC assets**

https://<baseurl>/qps/rest/2.0/activate/am/hostasset/<id>?
module=QWEB_PC
or
https://<baseurl>/qps/rest/2.0/activate/am/hostasset?
module=QWEB_PC

**Method**

POST

**Fields**

These fields can be used to activate host assets.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>qwebHostId (Integer)</td>
<td>qwebHostId (Text)</td>
</tr>
<tr>
<td>lastVulnScan (Date)</td>
<td>lastVulnScan (Text)</td>
</tr>
<tr>
<td>lastComplianceScan (Date)</td>
<td>lastComplianceScan (Text)</td>
</tr>
<tr>
<td>informationGatheredUpdated (Date)</td>
<td>informationGatheredUpdated (Text)</td>
</tr>
<tr>
<td>os (Text)</td>
<td>os (Text)</td>
</tr>
<tr>
<td>dnsHostName (Text)</td>
<td>dnsHostName (Text)</td>
</tr>
<tr>
<td>address (Text)</td>
<td>address (Text)</td>
</tr>
<tr>
<td>vulnsUpdated(Date)</td>
<td>vulnsUpdated(Date)</td>
</tr>
<tr>
<td>id (Integer)</td>
<td>id (Integer)</td>
</tr>
<tr>
<td>name (Text)</td>
<td>name (Text)</td>
</tr>
<tr>
<td>created (Date)</td>
<td>created (Date)</td>
</tr>
<tr>
<td>type (Text)</td>
<td>type (Text)</td>
</tr>
<tr>
<td>netbiosName (Text)</td>
<td>netbiosName (Text)</td>
</tr>
<tr>
<td>netbiosNetworkID (Text)</td>
<td>netbiosNetworkID (Text)</td>
</tr>
<tr>
<td>trackingMethod (Keyword: NONE, IP, DNSNAME, NETBIOS, INSTANCE_ID, QAGENT)</td>
<td>trackingMethod (Keyword: NONE, IP, DNSNAME, NETBIOS, INSTANCE_ID, QAGENT)</td>
</tr>
<tr>
<td>port (Integer)</td>
<td>port (Integer)</td>
</tr>
<tr>
<td>installedSoftware (Text)</td>
<td>installedSoftware (Text)</td>
</tr>
<tr>
<td>tagName (Text)</td>
<td>tagName (Text)</td>
</tr>
<tr>
<td>tagId (Integer)</td>
<td>tagId (Integer)</td>
</tr>
<tr>
<td>networdGuid (Text)</td>
<td>networdGuid (Text)</td>
</tr>
<tr>
<td>informationGatheredUpdated (Date)</td>
<td>informationGatheredUpdated (Text)</td>
</tr>
<tr>
<td>name (Text)</td>
<td>name (Text)</td>
</tr>
<tr>
<td>netbiosName (Text)</td>
<td>netbiosName (Text)</td>
</tr>
<tr>
<td>netbiosNetworkId (Text)</td>
<td>netbiosNetworkId (Text)</td>
</tr>
<tr>
<td>created (Date)</td>
<td>created (Date)</td>
</tr>
<tr>
<td>update (Date)</td>
<td>update (Date)</td>
</tr>
</tbody>
</table>
Chapter 3 — Host Asset API

Activate Host Asset

Allowed Operators

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integer</td>
<td>EQUALS, NOT EQUALS, GREATER, LESSER, IN</td>
</tr>
<tr>
<td>Text</td>
<td>CONTAINS, EQUALS, NOT EQUALS</td>
</tr>
<tr>
<td>Date</td>
<td>EQUALS, NOT EQUALS, GREATER, LESSER</td>
</tr>
<tr>
<td>Keyword</td>
<td>EQUALS, NOT EQUALS, IN</td>
</tr>
<tr>
<td>Boolean</td>
<td>(true/false) EQUALS, NOT EQUALS</td>
</tr>
</tbody>
</table>

Permissions

Managers with Full Scope

Users without Full Scope must have these account settings: 1) scope includes the requested asset(s), and 2) permissions include:
- Access Permission “API Access”

For PC assets, the Policy Compliance (PC) module must be enabled

Example

Activate the host assets with the tag “Export to VM”.

Request:

curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/activate/am/hostasset"
< file.xml

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

Request POST data (file.xml):

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <filters>
    <Criteria field="tagName" operator="EQUALS">Export to VM</Criteria>
  </filters>
</ServiceRequest>
```
See also Activate Asset
# Host Asset Fields

<table>
<thead>
<tr>
<th>Writable</th>
<th>Read only</th>
</tr>
</thead>
<tbody>
<tr>
<td>os (string)</td>
<td>qwebHostId (long)</td>
</tr>
<tr>
<td>dnsHostName (string)</td>
<td>lastVulnScan (date)</td>
</tr>
<tr>
<td>netbiosName (string)</td>
<td>lastComplianceScan (date)</td>
</tr>
<tr>
<td>netbiosNetworkId (integer)</td>
<td>vulnsUpdated (date)</td>
</tr>
<tr>
<td>networkGuid (uuid)</td>
<td>informationGatheredUpdated (date)</td>
</tr>
<tr>
<td>address (string)</td>
<td>account (HostAssetAccount)</td>
</tr>
<tr>
<td>trackingMethod (AssetTrackingMethod: NONE, IP, DNSNAME, NETBIOS, INSTANCE_ID, QAGENT)</td>
<td>biosDescription (string)</td>
</tr>
<tr>
<td>openPort (HostAssetOpenPortQList)</td>
<td>manufacturer (string)</td>
</tr>
<tr>
<td>software (HostAssetSoftwareQList)</td>
<td>model (string)</td>
</tr>
<tr>
<td></td>
<td>networkInterface (HostAssetInterface)</td>
</tr>
<tr>
<td></td>
<td>processor (HostAssetProcessor)</td>
</tr>
<tr>
<td></td>
<td>timezone (string)</td>
</tr>
<tr>
<td></td>
<td>totalMemory (long)</td>
</tr>
<tr>
<td></td>
<td>volume (HostAssetVolume)</td>
</tr>
</tbody>
</table>

## Associations

HostAssetOpenPortQList - Open ports (HostAssetOpenPortList) detected or explicitly added to the asset. This collection is keyed off of the port and protocol.

<table>
<thead>
<tr>
<th>HostAssetOpenPortList</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>port integer</td>
<td>protocol Protocol (TCP, UDP, ICMP)</td>
</tr>
</tbody>
</table>
HostAssetOpenPortList

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>serviceId</td>
<td>integer</td>
</tr>
<tr>
<td>serverName</td>
<td>string</td>
</tr>
</tbody>
</table>

HostAssetSoftwareQList - A list of software (HostAssetSoftware) installed on the machine, keyed on the name.

HostAssetSoftware

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>string</td>
</tr>
<tr>
<td>version</td>
<td>string</td>
</tr>
</tbody>
</table>

HostAssetVulnQList - A list of vulnerabilities detected on the host. Only vulnerabilities flagged as found will be returned. More detailed information about each detected vulnerability can be obtained from the HostInstanceVuln resource, cross referenced by the hostInstanceVulnId field. The HostInstanceVuln can also be used to find previously detected vulnerabilities that are currently marked as not found.

HostInstanceVuln

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>qid</td>
<td>long</td>
</tr>
<tr>
<td>hostInstanceVulnID</td>
<td>long</td>
</tr>
<tr>
<td>firstFound</td>
<td>date</td>
</tr>
<tr>
<td>lastFound</td>
<td>date</td>
</tr>
</tbody>
</table>
Asset API

The Asset API is a subset of the Host Asset API. The Asset members identify name, tags, and EC2 source information.

**Operations**
- Get Asset Info
- Update Asset
- Search Assets
- Count Assets
- Delete Asset
- Activate Asset

**Reference**
- Asset Fields
Get Asset Info

Returns a single asset by ID.

**URL**
https://<baseurl>/qps/rest/2.0/get/am/asset/<id>

**Method**
GET

**Limit your results**
Use the optional “fields” parameter to limit the amount of information returned for the asset. Learn more

Permissions

Managers with Full Scope

Users without Full Scope must have these account settings: 1) scope includes the requested asset, and 2) permissions include:
- Access Permission “API Access”
- Asset Management Permission “Read Asset”

Example

This example fetches the asset ID 12345 and lists asset details.

**Request:**
curl -n -u "USERNAME:PASSWORD"
"https://qualysapi.qualys.com/qps/rest/2.0/get/am/asset/12345"

**Response:**
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/asset.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
    <data>
        <Asset>
            <id>12345</id>
            <name>My Windows Asset</name>
            <created>2014-02-06T19:16:35Z</created>
            <modified>2014-02-06T19:16:35Z</modified>
            <type>HOST</type>
        </Asset>
    </data>
</ServiceResponse>
Chapter 4 — Asset API
Get Asset Info

<tags>
  <list>
    <TagSimple>
      <id>12345</id>
      <name>Tag 1</name>
    </TagSimple>
    <TagSimple>
      <id>54321</id>
      <name>Tag 2</name>
    </TagSimple>
  </list>
</tags>
</Asset>
</data>
</ServiceResponse>
Update Asset

Update fields for an asset and collections of assets. Only the name and tags can be modified.

**URL**
https://<baseurl>/qps/rest/2.0/update/am/asset/<id>
or
https://<baseurl>/qps/rest/2.0/update/am/asset

**Method**
POST

Using the NOT EQUALS operator for updating assets could result in accidental update of unknown assets without any warning. To prevent accidental updates of unknown assets, we do not support NOT EQUALS operator for update actions.

**Permissions**

Managers with Full Scope

Users without Full Scope must have these account settings: 1) scope includes the requested asset(s), and 2) permissions include:
- Access Permission “API Access”
- Asset Management Permission “Update Asset”

**Example**

**Request 1:**
Update tag 12345 and give it another name.

```
```

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

**Request POST data (file.xml):**

```
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <data>
    <Asset>
      <name>Updated Name</name>
    </Asset>
  </data>
</ServiceRequest>
```
Response:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/asset.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <Asset>
      <id>12345</id>
      <name>Updated Name</name>
      <created>2014-02-06T19:16:35Z</created>
      <modified>2014-02-06T19:16:35Z</modified>
      <type>HOST</type>
      <tags>
        <list>
          <TagSimple>
            <id>12345</id>
            <name>Tag 1</name>
          </TagSimple>
          <TagSimple>
            <id>54321</id>
            <name>Tag 2</name>
          </TagSimple>
        </list>
      </tags>
    </Asset>
  </data>
</ServiceResponse>
```

**Request 2:**
Update tags that have tag names containing the word DELETED.

```bash
curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST"
    --data-binary @- "https://qualysapi.qualys.com/qps/rest/2.0/update/am/asset" <
    file.xml
```
Note: “file.xml” contains the request POST data.

Request POST data (file.xml):

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <filters>
    <Criteria field="name" operator="CONTAINS">DELETED</Criteria>
  </filters>
  <data>
    <Asset>
      <tags>
        <add>
          <TagSimple><id>12345</id></TagSimple>
        </add>
      </tags>
    </Asset>
  </data>
</ServiceRequest>
```

Response:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/asset.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <Asset>
      <id>543</id>
      <name>Old Asset (DELETED)</name>
      <created>2014-02-06T19:16:35Z</created>
      <modified>2014-02-06T19:16:35Z</modified>
      <type>HOST</type>
      <tags>
        <list>
          <TagSimple>
            <id>12345</id>
            <name>Tag 1</name>
          </TagSimple>
        </list>
      </tags>
    </Asset>
  </data>
</ServiceResponse>
```
Chapter 4 — Asset API
Update Asset

</TagSimple>
</list>
</tags>
</Asset>
</data>
</ServiceResponse>
Search Assets

Returns a list of assets matching the provided criteria. Assets are returned when they are visible to the user (i.e. in the user’s scope).

**URL**

https://<baseurl>/qps/rest/2.0/search/am/asset

**Method**

POST

**Pagination**

A maximum of 100 assets are returned by default. To customize this specify a “preferences” tag in the POST body of your request.

**Limit your results**

Use the optional “fields” parameter to limit the amount of information returned for each asset. [Learn more]

Searchable Fields

These fields can be used to search for assets.

<table>
<thead>
<tr>
<th>id (Integer)</th>
<th>type (Keyword: UNKOWN, HOST, SCANNER, WEBAPP, MALWARE_DOMAIN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>name (Text)</td>
<td>tagName (Text)</td>
</tr>
<tr>
<td>created (Date)</td>
<td>tagId (Text)</td>
</tr>
<tr>
<td>updated (Date)</td>
<td>solrQuery (Text, an asset solr query)</td>
</tr>
</tbody>
</table>

Allowed Operators

| Integer     | EQUALS, NOT EQUALS, GREATER, LESSER, IN |
| Text        | CONTAINS, EQUALS, NOT EQUALS             |
| Date        | EQUALS, NOT EQUALS, GREATER, LESSER     |
| Keyword     | EQUALS, NOT EQUALS, IN                  |

For tagName and tagID, parents of the tag will also match. For example if tag A had child tag B and an asset has tag A, then a search for tag B will return assets with tags A and B.
Permissions

Managers with Full Scope

Users without Full Scope must have these account permissions:
- Access Permission “API Access”
- Asset Management Permission “Read Asset”

Example

Find an asset with a particular tag.

Request:

curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/search/am/asset" <
file.xml

Request POST data (file.xml):

<ServiceRequest>
  <filters>
    <Criteria field="tagName" operator="EQUALS">To Delete</Criteria>
  </filters>
</ServiceRequest>

Response:

<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/asset.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <Asset>
      <id>543</id>
      <name>Old Asset (To Delete)</name>
      <created>2014-02-06T19:16:35Z</created>
      <modified>2014-02-06T19:16:35Z</modified>
      <type>HOST</type>
      <tags>

92 Qualys Asset Management and Tagging API
<list>
  <TagSimple>
    <id>12345</id>
    <name>Tag 1</name>
  </TagSimple>
  <TagSimple>
    <id>54321</id>
    <name>Tag 2</name>
  </TagSimple>
  <TagSimple>
    <id>67890</id>
    <name>Tag 3</name>
  </TagSimple>
</list>
</tags>
</Asset>
</data>
</ServiceResponse>
Count Assets

Returns the number of assets that match the provided criteria. A host asset is counted when the asset is visible to the user (i.e. in the user’s scope).

**URL**

https://<baseurl>/qps/rest/2.0/count/am/asset

**Method**

POST

**Fields**

These fields can be used to count assets.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id (Integer)</td>
<td>type (Keyword: UNKOWN, HOST, SCANNER, WEBAPP, MALWARE_DOMAIN)</td>
</tr>
<tr>
<td>name (Text)</td>
<td>tagName (Text)</td>
</tr>
<tr>
<td>created (Date)</td>
<td>tagId (Text)</td>
</tr>
<tr>
<td>updated (Date)</td>
<td>solrQuery (Text, an asset solr query)</td>
</tr>
</tbody>
</table>

**Allowed Operators**

- Integer: EQUALS, NOT_EQUALS, GREATER, LESSER, IN
- Text: CONTAINS, EQUALS, NOT_EQUALS
- Date: EQUALS, NOT_EQUALS, GREATER, LESSER
- Keyword: EQUALS, NOT_EQUALS, IN

**Permissions**

Managers with Full Scope

Users without Full Scope must have these account permissions:
- Access Permission “API Access”
- Asset Management Permission “Read Asset”

**Example**

**Request:**

```
curl -u "USERNAME:PASSWORD"
"https://qualysapi.qualys.com/qps/rest/2.0/count/am/asset" <
```
file.xml

Request POST data (file.xml):

```xml
<ServiceRequest>
  <filters>
    <Criteria field="tagName" operator="EQUALS">To Delete</Criteria>
  </filters>
</ServiceRequest>
```

Response:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/asset.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
</ServiceResponse>
```
Delete Asset

Delete one or more assets.

**URL**

- https://<baseurl>/qps/rest/2.0/delete/am/asset/<id>
- or
- https://<baseurl>/qps/rest/2.0/delete/am/asset

**Method**

POST

Using the NOT EQUALS operator for deleting assets could result in accidental deletion of unknown assets without any warning. To prevent accidental deletion of unknown assets, we do not support NOT EQUALS operator for delete actions.

**Permissions**

Managers with Full Scope

Users without Full Scope must have these account settings: 1) scope includes the requested asset(s), and 2) permissions include:
- Access Permission “API Access”
- Asset Management Permission “Delete Asset”

**Examples**

Delete assets with a particular tag.

**Request:**

curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/delete/am/asset" < file.xml

**Request POST data (file.xml):**

```xml
<ServiceRequest>
  <filters>
    <Criteria field="tagName" operator="EQUALS">To Delete</Criteria>
  </filters>
</ServiceRequest>
```

**Response:**

```xml
<?xml version="1.0" encoding="UTF-8"?>
```
Chapter 4 — Asset API
Delete Asset

<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/asset.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <Asset>
      <id>1972521</id>
    </Asset>
  </data>
</ServiceResponse>
Activate Asset

Activate one or more assets to make them available in your account for scanning and reporting. You’ll want to activate newly created hosts to make them available in the Vulnerability Management (VM) application module and/or the Policy Compliance (PC) module.

URL for VM assets
https://<baseurl>/qps/rest/2.0/activate/am/asset/<id>?
module=QWEB_VM
or
https://<baseurl>/qps/rest/2.0/activate/am/asset?module=QWEB_VM

URL for PC assets
https://<baseurl>/qps/rest/2.0/activate/am/asset/<id>?
module=QWEB_PC
or
https://<baseurl>/qps/rest/2.0/activate/am/asset?module=QWEB_PC

Method
POST

Searchable Fields

These fields can be used to search for assets.

<table>
<thead>
<tr>
<th>Field</th>
<th>Allowed Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>id (Integer)</td>
<td>type (Keyword: UNKNOWN, HOST, SCANNER, WEBAPP, MALWARE_DOMAIN)</td>
</tr>
<tr>
<td>name (Text)</td>
<td>tagName (Text)</td>
</tr>
<tr>
<td>created (Date)</td>
<td>tagId (Text)</td>
</tr>
<tr>
<td>updated (Date)</td>
<td>solrQuery (Text, an asset solr query)</td>
</tr>
</tbody>
</table>

Allowed Operators
- Integer: EQUALS, NOT_EQUALS, GREATER, LESSER, IN
- Text: CONTAINS, EQUALS, NOT_EQUALS
- Date: EQUALS, NOT_EQUALS, GREATER, LESSER
- Keyword: EQUALS, NOT_EQUALS, IN
Permissions

Managers with Full Scope

Users without Full Scope must have these account settings: 1) scope includes the requested asset(s), and 2) permissions include:
- Access Permission “API Access”

For PC assets, the Policy Compliance (PC) module must be enabled

Example

Activate assets with the tag “Export to VM”.

Request:
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/activate/am/asset?module=QWEB_VM" < file.xml

Request POST data (file.xml):

```
<ServiceRequest>
    <filters>
        <Criteria field="tagName" operator="EQUALS">Export to VM</Criteria>
    </filters>
</ServiceRequest>
```

Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/asset.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
    <data>
        <Asset>
            <id>1972521</id>
            <name>Test Asset</name>
            <created>2013-12-11T05:12:45Z</created>
            <modified>2014-02-04T23:55:54Z</modified>
            <type>HOST</type>
        </Asset>
    </data>
</ServiceResponse>
```
<ServiceResponse>
  <data>
    <Asset>
      <tags>
        <list>
          <SimpleTag>
            <id>12345</id>
            <name>Export to VM</name>
          </SimpleTag>
        </list>
      </tags>
      <sourceInfo>
        <list>
          <Ec2AssetSourceSimple>
            <firstDiscovered>2014-02-06T19:14:50Z</firstDiscovered>
            <lastUpdated>2014-02-06T19:14:50Z</lastUpdated>
            <assetId>1972521</assetId>
            <availabilityZone>us-east</availabilityZone>
            <privateDnsName>ip-10-90-0-73.qualys.com</privateDnsName>
            <instanceId>i-8b545eef</instanceId>
            <instanceType>t1.micro</instanceType>
            <imageId>ami-03ad6e6a</imageId>
            <privateIpAddress>127.0.0.1</privateIpAddress>
            <monitoringEnabled>false</monitoringEnabled>
          </Ec2AssetSourceSimple>
        </list>
      </sourceInfo>
      <openPort>
        <list/>
      </openPort>
      <software>
        <list/>
      </software>
      <vuln>
        <list/>
      </vuln>
    </Asset>
  </data>
</ServiceResponse>
Asset Fields

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>id (long)</td>
</tr>
<tr>
<td>tags (string)</td>
<td>created (date)</td>
</tr>
<tr>
<td></td>
<td>modified (date)</td>
</tr>
<tr>
<td></td>
<td>type (Asset type: UNKNOWN, HOST, SCANNER, WEBAPP, MALWARE_DOMAIN)</td>
</tr>
<tr>
<td></td>
<td>sourceInfo (AssetSourceQList)</td>
</tr>
</tbody>
</table>

Associations

TagSimpleQList - Asset tags on the associated asset. This collection to be added to and removed from by providing a tag ID wrapped in a TagSimple element.

TagSimple

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>long (tag primary key)</td>
</tr>
<tr>
<td>name</td>
<td>string (tag name)</td>
</tr>
</tbody>
</table>

AssetSourceQList - Source information for the associated asset. At the moment this is used exclusively for assets that are in Amazon EC2 but may contain additional types in the future. As such, elements will always be of type Ec2AssetSourceSimple.

Ec2AssetSourceSimple

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>availabilityZone</td>
<td>imageID (string)</td>
</tr>
<tr>
<td>privateDNSName</td>
<td>publicIPAddress (string)</td>
</tr>
<tr>
<td>publicDNSName</td>
<td>privateIPAddress (string)</td>
</tr>
<tr>
<td>instanceID</td>
<td>monitoringEnabled (boolean)</td>
</tr>
<tr>
<td>instanceType</td>
<td>instanceState</td>
</tr>
<tr>
<td></td>
<td>(AssetSourceStateCode: PENDING, RUNNING, SHUTTING_DOWN, TERMINATED, STOPPING, STOPPED, UNSUPPORTED)</td>
</tr>
</tbody>
</table>
Host Instance Vulnerability API

The Host Instance Vulnerability API provides a suite of API functions for managing vulnerability instances found on host assets. The supported Host Instance Vulnerability operations are get, count and search.

**Operations**

- Get Vulnerability Info
- Search Vulnerabilities
- Count Vulnerabilities

**Reference**

- Host Instance Vulnerability Fields
Get Vulnerability Info

Returns a single host instance vulnerability data by ID. See Vulnerability Fields

**URL**
https://<baseurl>/qps/rest/2.0/get/am/hostinstancevuln/<id>

**Method**
GET

**Limit your results**
Use the optional “fields” parameter to limit the amount of information returned for the host instance vulnerability. Learn more

**Permissions**

Managers with Full Scope

Users without Full Scope must have these account settings: 1) scope includes the requested asset, and 2) permissions include:
- Access Permission “API Access”
- Asset Management Permission “Read Asset”

**Example**

Fetch the host instance vulnerability with the ID 12345.

**Request:**
curl -n -u "USERNAME:PASSWORD" "https://qualysapi.qualys.com/qps/rest/2.0/get/am/hostinstancevuln/12345"

**Response:**
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/hostinstancevuln.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <HostInstanceVuln>
      <id>9534081</id>
      <hostAssetId>1543621</hostAssetId>
    </HostInstanceVuln>
  </data>
</ServiceResponse>
<qid>38167</qid>
<port>25</port>
<ssl>true</ssl>
<found>true</found>
<ignored>false</ignored>
<disabled>false</disabled>
<updated>2012-10-19T21:56:23Z</updated>
<protocol>TCP</protocol>
<source>HOST</source>
</HostInstanceVuln>
</data>
</ServiceResponse>
Search Vulnerabilities

Returns a list of host instance vulnerabilities that match the provided criteria. These vulnerabilities are returned when the hosts are visible to the user (i.e. in the user’s scope).

**URL**
https://<baseurl>/qps/rest/2.0/search/am/hostinstancevuln

**Method**
POST

**Pagination**
A maximum of 100 instances are returned by default. To customize this specify a “preferences” tag in the POST body of your request.

**Limit your results**
Use the optional “fields” parameter to limit the amount of information returned for each vulnerability. Learn more

### Searchable Fields

These fields can be used to search for host instance vulnerabilities. See Vulnerability Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id (Integer)</td>
<td>ignored (Boolean)</td>
</tr>
<tr>
<td>hostAssetId (Integer)</td>
<td>disabled (Boolean)</td>
</tr>
<tr>
<td>qid (Integer)</td>
<td>firstFound (Date)</td>
</tr>
<tr>
<td>fqdn (string)</td>
<td>lastFound (Date)</td>
</tr>
<tr>
<td>port (Integer)</td>
<td>lastScanned (Date)</td>
</tr>
<tr>
<td>ssl (Boolean)</td>
<td>updated (Date)</td>
</tr>
<tr>
<td>found (Boolean)</td>
<td>protocol (Protocol: TCP, UDP or ICMP)</td>
</tr>
<tr>
<td></td>
<td>source (Source: HOST, ORACLE or HSSQL, OTHER)</td>
</tr>
</tbody>
</table>

**Allowed Operators**

<table>
<thead>
<tr>
<th>Type</th>
<th>Operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integer</td>
<td>EQUALS, NOT EQUALS, GREATER, LESSER, IN</td>
</tr>
<tr>
<td>Text</td>
<td>CONTAINS, EQUALS, NOT EQUALS</td>
</tr>
<tr>
<td>Date</td>
<td>EQUALS, NOT EQUALS, GREATER, LESSER</td>
</tr>
<tr>
<td>Keyword</td>
<td>EQUALS, NOT EQUALS, IN</td>
</tr>
<tr>
<td>Boolean</td>
<td>(true/false) EQUALS, NOT EQUALS</td>
</tr>
</tbody>
</table>
Permissions

Managers with Full Scope

Users without Full Scope must have these account permissions:
- Access Permission “API Access”
- Asset Management Permission “Read Asset”

Example

Find all vulnerabilities that were previously detected on a host, and that have since been resolved.

Request:
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/search/am/hostinstancevuln" < file.xml

Request POST data (file.xml):
<ServiceRequest>
  <filters>
    <Criteria field="hostAssetId" operator="EQUALS">12345</Criteria>
    <Criteria field="found" operator="EQUALS">false</Criteria>
  </filters>
</ServiceRequest>

Response:
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/hostinstancevuln.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <HostInstanceVuln>
      <id>9534081</id>
      <hostAssetId>12345</hostAssetId>
      <qid>38167</qid>
      <port>25</port>
    </HostInstanceVuln>
  </data>
</ServiceResponse>
<ssl>true</ssl>
<found>true</found>
<ignored>false</ignored>
<disabled>false</disabled>
<updated>2012-10-19T21:56:23Z</updated>
<protocol>TCP</protocol>
<source>HOST</source>
</HostInstanceVuln>
</data>
</ServiceResponse>
Count Vulnerabilities

Returns the number of host instance vulnerabilities that match the provided criteria. A host instance vulnerability is counted when the asset visible to the user (i.e. it is in the user’s scope).

URL
https://<baseurl>/qps/rest/2.0/count/am/hostinstancevuln

Method
POST

Permissions

Managers with Full Scope

Users without Full Scope must have these account permissions:
- Access Permission “API Access”
- Asset Management Permission “Read Asset”

Example

Count the number of host instance vulnerabilities across all visible assets.

Request:
curl -u "USERNAME:PASSWORD"
"https://qualysapi.qualys.com/qps/rest/2.0/count/am/hostinstancevuln"< file.xml
Note: “file.xml” contains the request POST data.

<ServiceRequest>
  <filters>
    <Criteria field="found" operator="EQUALS">true</Criteria>
  </filters>
</ServiceRequest>

Response:
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/hostinstancevuln.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
</ServiceResponse>
### Host Instance Vulnerability Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id (long)</td>
<td>The primary host instance vulnerability key.</td>
</tr>
<tr>
<td>hostAssetId (long)</td>
<td>The ID of the host asset where the vulnerability was found.</td>
</tr>
<tr>
<td>created (date)</td>
<td>The date the vulnerability was added to the KnowledgeBase.</td>
</tr>
<tr>
<td>found (boolean)</td>
<td>Set to true if the QID was detected on the host by the latest scan of that host.</td>
</tr>
<tr>
<td>firstFound (date)</td>
<td>The date/time the vulnerability was first detected on the host.</td>
</tr>
<tr>
<td>lastfound (date)</td>
<td>The most recent date/time the vulnerability was detected on the host.</td>
</tr>
<tr>
<td>lastScanned (date)</td>
<td>The most recent date/time the vulnerability was tested for the host.</td>
</tr>
<tr>
<td>qid (long)</td>
<td>The Qualys vulnerability ID of the vulnerability.</td>
</tr>
<tr>
<td>disabled (long)</td>
<td>Set to true if the QID is marked as disabled in your subscription. Set to false if the QID is not marked disabled.</td>
</tr>
<tr>
<td>fqdn (string)</td>
<td>The fully qualified domain name of the host.</td>
</tr>
<tr>
<td>ssl (boolean)</td>
<td>Set to true if the vulnerability was detected over SSL. Set to false if the vulnerability was not detected over SSL. This element is not returned for information gathered.</td>
</tr>
<tr>
<td>updated (date)</td>
<td>The last date/time the vulnerability data was updated for the host.</td>
</tr>
<tr>
<td>ignored (boolean)</td>
<td>Set to true if the QID/host/port is marked as ignored in your subscription. Set to false if the QID/host/port is not marked ignored.</td>
</tr>
<tr>
<td>protocol (Protocol: TCP, UDP, ICMP)</td>
<td>The protocol the vulnerability was detected on.</td>
</tr>
<tr>
<td>port (integer)</td>
<td>The port number the vulnerability was detected on.</td>
</tr>
<tr>
<td>source(VulnSource: HOST, ORACLE, HSSQL, OTHER)</td>
<td>The vulnerability source.</td>
</tr>
</tbody>
</table>
Asset Data Connector API

The Asset Data Connector API provides a suite of API functions for managing Qualys asset data connectors.

**Operations**
- Get Connector Info
- Update Connector
- Search Connectors
- Count Connectors
- Delete Connector
- Run Connector

**Reference**
- Connector Fields
Get Connector Info

Returns a single asset data connector by ID.

**URL**

https://<baseurl>/qps/rest/2.0/get/am/assetdataconnector/<id>

**Method**

GET

**Limit your results**

Use the optional “fields” parameter to limit the amount of information returned for the asset data connector. [Learn more](#)

**Permissions**

Managers with Full Scope

**Example**

Fetch the asset data connector with the ID 12345.

**Request:**

curl -n -u "USERNAME:PASSWORD" 
"https://qualysapi.qualys.com/qps/rest/2.0/get/am/assetdataconnector/12345"

**Response:**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/assetdataconnector.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <hasMoreRecords>false</hasMoreRecords>
  <data>
    <AssetDataConnector>
      <id>12345</id>
      <name>new connector</name>
      <lastSync>2014-11-26T08:44:05Z</lastSync>
      <lastError>Invalid EC2 AuthRecord</lastError>
      <connectorState>ERROR</connectorState>
      <type>AWS</type>
    </AssetDataConnector>
  </data>
</ServiceResponse>
```
<defaultTags>
  <list>
    <TagSimple>
      <id>1</id>
      <name>EC2</name>
    </TagSimple>
  </list>
</defaultTags>
<activation>
  <ActivationModule>VM</ActivationModule>
</activation>
</AssetDataConnector>
</data>
</ServiceResponse>
Update Connector

Updates writable fields and collections. Only the name and tags can be modified.

**URL**

https://<baseurl>/qps/rest/2.0/update/am/assetdataconnector/

or

https://<baseurl>/qps/rest/2.0/update/am/assetdataconnector

**Method**

POST

Using the NOT EQUALS operator for updating connectors could result in accidental update of unknown connectors without any warning. To prevent accidental updates of unknown connectors, we do not support NOT EQUALS operator for update actions.

**Permissions**

Managers with Full Scope

**Example**

**Request 1:**

Change the name of an asset data connector with the ID 12345 and add a tag with the ID of 1 to the defaultTags collection.

```bash
curl -u "USERNAME:PASSWORD" "https://qualysapi.qualys.com/qps/rest/2.0/update/am/assetdataconnector/asset/12345" < file.xml
```

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

**Request POST data (file.xml):**

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <data>
    <AssetDataConnector>
      <name>Updated Name</name>
      <defaultTags>
        <add>
          <TagSimple>
            <id>1</id>
          </TagSimple>
        </add>
      </defaultTags>
    </AssetDataConnector>
  </data>
</ServiceRequest>
```

113 | Qualys Asset Management and Tagging API
Chapter 6 — Asset Data Connector API

Update Connector

<defaultTags>
  <TagSimple>
    <id>1</id>
    <name>EC2</name>
  </TagSimple>
</defaultTags>
</AssetDataConnector>
</data>
</ServiceRequest>

Response:

<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/assetdataconnector.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <hasMoreRecords>false</hasMoreRecords>
  <data>
    <AssetDataConnector>
      <id>12345</id>
      <name>External VPC</name>
      <lastSync>2014-11-26T08:44:05Z</lastSync>
      <lastError />
      <connectorState>SUCCESS</connectorState>
      <type>AWS</type>
      <defaultTags>
        <list>
          <TagSimple>
            <id>1</id>
            <name>EC2</name>
          </TagSimple>
        </list>
      </defaultTags>
      <activation>
        <ActivationModule>VM</ActivationModule>
      </activation>
    </AssetDataConnector>
  </data>
</ServiceResponse>
Request 2:
Add a tag to all asset data connectors who’s names contains External.

```
```

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

Request POST data (file.xml):
```
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
   <filters>
      <Criteria field="name" operator="CONTAINS">External</Criteria>
   </filters>
   <data>
      <Asset>
         <tags>
            <add>
               <TagSimple><id>2</id></TagSimple>
            </add>
         </tags>
      </Asset>
   </data>
</ServiceRequest>
```

Response:
```
<?xml version="1.0" encoding="UTF-8"?>
   <responseCode>SUCCESS</responseCode>
   <count>13</count>
   <hasMoreRecords>false</hasMoreRecords>
   <data>
      <AssetDataConnector>
         <id>12345</id>
         <name>External VPC</name>
         <lastSync>2014-11-26T08:44:05Z</lastSync>
   </AssetDataConnector>
</ServiceResponse>
```
<lastError />
<connectorState>SUCCESS</connectorState>
<type>AWS</type>
<defaultTags>
  <list>
    <TagSimple>
      <id>2</id>
      <name>External</name>
    </TagSimple>
  </list>
</defaultTags>
<activation>
  <ActivationModule>VM</ActivationModule>
</activation>
</AssetDataConnector>
...
</data>
</ServiceResponse>
Search Connectors

Returns a list of asset data connectors that match the provided criteria.

**URL**

https://<baseurl>/qps/rest/2.0/search/am/assetdataconnector

**Method**

POST

**Pagination**

A maximum of 100 instances are returned by default. To customize this specify a “preferences” tag in the POST body of your request.

**Limit your results**

Use the optional “fields” parameter to limit the amount of information returned for each asset data connector. Learn more

**Searchable Fields**

These fields can be used to search for asset data connectors.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id (Integer)</td>
<td>Primary key</td>
</tr>
<tr>
<td>name (Text)</td>
<td></td>
</tr>
<tr>
<td>description (Text)</td>
<td></td>
</tr>
<tr>
<td>lastSync (Date)</td>
<td></td>
</tr>
<tr>
<td>lastError (Text)</td>
<td></td>
</tr>
<tr>
<td>connectorState (Keyword)</td>
<td>PENDING, RUNNING, SUCCESS, ERROR</td>
</tr>
<tr>
<td>activation (Keyword)</td>
<td>VM or PC</td>
</tr>
<tr>
<td>defaultTags.name (Text)</td>
<td>The name of a tag in the defaultTags collection</td>
</tr>
<tr>
<td>defaultTag (Integer)</td>
<td>The ID of a tag in the defaultTags collection</td>
</tr>
<tr>
<td>disabled (Boolean)</td>
<td>Whether execution of the connector is disabled (YES). If disabled the connector will not synchronize assets.</td>
</tr>
</tbody>
</table>

**Allowed Operators**

<table>
<thead>
<tr>
<th>Type</th>
<th>Operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integer</td>
<td>EQUALS, NOT EQUALS, GREATER, LESSER, IN</td>
</tr>
<tr>
<td>Text</td>
<td>CONTAINS, EQUALS, NOT EQUALS</td>
</tr>
</tbody>
</table>
Chapter 6 — Asset Data Connector API

Search Connectors

<table>
<thead>
<tr>
<th>Date</th>
<th>EQUALS, NOT EQUALS, GREATER, LESSER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keyword</td>
<td>EQUALS, NOT EQUALS, IN</td>
</tr>
<tr>
<td>Boolean</td>
<td>(true/false) EQUALS, NOT EQUALS</td>
</tr>
</tbody>
</table>

Permissions

Managers with Full Scope

Example

Find all asset data connectors with tag name USA.

**Request:**

curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/search/am/assetdataconnector" < file.xml

**Request POST data (file.xml):**

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <filters>
    <Criteria field="defaultTags.name" operator="EQUALS">USA</Criteria>
  </filters>
</ServiceRequest>
```

**Response:**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/assetdataconnector.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>13</count>
  <hasMoreRecords>false</hasMoreRecords>
  <data>
    <AssetDataConnector>
      <id>12345</id>
    </AssetDataConnector>
  </data>
</ServiceResponse>
```
<name>DB1</name>
<lastSync>2014-11-26T08:44:05Z</lastSync>
<lastError />
<connectorState>SUCCESS</connectorState>
<type>AWS</type>
<defaultTags>
  <list>
    <TagSimple>
      <id>3</id>
      <name>USA</name>
    </TagSimple>
  </list>
</defaultTags>
<activation>
  <ActivationModule>VM</ActivationModule>
  <ActivationModule>PC</ActivationModule>
</activation>
<AssetDataConnector>
</data>
</ServiceResponse>
Count Connectors

Returns the number of asset data connectors that match the provided criteria.

**URL**

https://<baseurl>/qps/rest/2.0/count/am/assetdataconnector

**Method**

POST

**Permissions**

Managers with Full Scope

**Example**

Count the number of asset data connectors with the tag name USA.

**Request:**

curl -u "USERNAME:PASSWORD" "https://qualysapi.qualys.com/qps/rest/2.0/count/am/assetdataconnector"< file.xml

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

**Request POST data (file.xml):**

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <filters>
    <Criteria field="defaultTags.name" operator="EQUALS">USA</Criteria>
  </filters>
</ServiceRequest>
```

**Response:**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/assetdataconnector.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
</ServiceResponse>
```
Delete Connector

Delete one or more asset data connectors.

**URL**

https://<baseurl>/qps/rest/2.0/delete/am/assetdataconnector/<id>

or

https://<baseurl>/qps/rest/2.0/delete/am/assetdataconnector

**Method**

POST

Using the NOT EQUALS operator for deleting connectors could result in accidental deletion of unknown connectors without any warning. To prevent accidental deletion of unknown connectors, we do not support NOT EQUALS operator for delete actions.

**Permissions**

Managers with Full Scope

**Examples**

**Request 1:**

Delete a single asset data connector.

curl -n -u "USERNAME:PASSWORD"
"https://qualysapi.qualys.com/qps/rest/2.0/delete/am/assetdataconnector/12345"

**Response:**

<xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:noNamesapceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/assetdataconnector.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <AssetDataConnector>
      <id>12345</id>
    </AssetDataConnector>
  </data>
</ServiceResponse>
Chapter 6 — Asset Data Connector API
Delete Connector

</ServiceResponse>
Request 2:
Delete several asset data connectors tagged with the To Delete tag.

curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/delete/am/assetdataconnector" < file.xml

Request POST data (file.xml):
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <filters>
    <Criteria field="tagName" operator="EQUALS">To Delete</Criteria>
  </filters>
</ServiceRequest>

Response:
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/assetdataconnector.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <AssetDataConnector>
      <id>1972521</id>
    </AssetDataConnector>
  </data>
</ServiceResponse>
Chapter 6 — Asset Data Connector API

Run Connector

Request that one or more asset data connectors are run. The connectors may be run immediately, or queued to run when there is capacity. The response will almost always indicate that the connector is pending. Use GET calls to monitor the status of connectors.

**URL**

https://<baseurl>/qps/rest/2.0/run/am/assetdataconnector/<id>

or

https://<baseurl>/qps/rest/2.0/run/am/assetdataconnector

**Method**

POST

**Permissions**

Managers with Full Scope

**Examples**

Request 1:

Run a single connector.

```bash
curl -n -u "USERNAME:PASSWORD"
"https://qualysapi.qualys.com/qps/rest/2.0/run/am/assetdataconnector/12345"
```

Response:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/xsd/2.0/am/assetdataconnector.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <hasMoreRecords>false</hasMoreRecords>
  <data>
    <AssetDataConnector>
      <id>12345</id>
      <name>DB1</name>
      <lastSync>2014-11-26T08:44:05Z</lastSync>
      <lastError />
    </AssetDataConnector>
  </data>
</ServiceResponse>
```
Chapter 6 — Asset Data Connector API

Run Connector

Request 2:
Re-run all errored connectors.


Request POST data (file.xml):

<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <filters>
    <Criteria field="connectorState" operator="EQUALS">ERROR</Criteria>
  </filters>
</ServiceRequest>

Response:

<?xml version="1.0" encoding="UTF-8" ?>
  <responseCode>SUCCESS</responseCode>
</ServiceResponse>
<count>13</count>
<hasMoreRecords>false</hasMoreRecords>
<data>
  <AssetDataConnector>
    <id>12345</id>
    <name>DB1</name>
    <lastSync>2014-11-26T08:44:05Z</lastSync>
  </AssetDataConnector>
  ...
  <AssetDataConnector>
    <id>12346</id>
    <name>DB2</name>
    <lastSync>2015-01-07T01:50:05Z</lastSync>
  </AssetDataConnector>
  ...
</data>
Chapter 6 — Asset Data Connector API

Connector Fields

<table>
<thead>
<tr>
<th>Name (type)</th>
<th>Description</th>
<th>Writable</th>
</tr>
</thead>
<tbody>
<tr>
<td>id (long)</td>
<td>Primary key</td>
<td>No</td>
</tr>
<tr>
<td>name (string)</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>description (string)</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>lastSynch (date)</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>lastError (string)</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>connectorState (AssetDataConnectorState)</td>
<td>PENDING, RUNNING, SUCCESS, ERROR</td>
<td>No</td>
</tr>
<tr>
<td>type (AssetDataConnectorType)</td>
<td>AWS</td>
<td>No</td>
</tr>
<tr>
<td>defaultTags (TagSimpleQList)</td>
<td>Tags applied to any asset discovered by the connector</td>
<td>Yes</td>
</tr>
<tr>
<td>activation (List&lt;ActivationModule&gt;)</td>
<td>Assets discovered by the connector will be activated for the modules specified</td>
<td>Yes</td>
</tr>
<tr>
<td>disabled (boolean)</td>
<td>Whether execution of the connector is disabled (YES). If disabled the connector will not synchronize assets.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Associations

TagSimpleQList - Asset tags to be applied to assets found by the connector. This collection to be added to and removed from by providing a tag ID wrapped in a TagSimple element.

TagSimple

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>long (tag primary key)</td>
</tr>
<tr>
<td>name</td>
<td>string (tag name)</td>
</tr>
</tbody>
</table>
AWS Asset Data Connector API

The AWS Asset Data Connector API provides a suite of API functions for managing AWS asset data connectors, used to scan EC2 instances.

**Operations**
- Get AWS Connector Info
- Create AWS Connector
- Support for AWS GovCloud
- Update AWS Connector
- Search AWS Connectors
- Count AWS Connectors
- Delete AWS Connector
- Run Connector

**Reference**
- AWS Connector Fields
Get AWS Connector Info

Returns a single AWS connector by ID.

**URL**

`https://<baseurl>/qps/rest/2.0/get/am/awsassetdataconnector/<id>`

**Method**

GET

**Limit your results**

Use the optional “fields” parameter to limit the amount of information returned for the AWS connector. Learn more

**Permissions**

Managers with Full Scope

**Examples**

Fetch the asset data connector with the ID 12345.

**Request:**

```
curl -n -u "USERNAME:PASSWORD" "https://qualysapi.qualys.com/qps/rest/2.0/get/am/awsassetdataconnector/12345"
```

**Response:**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="http://qualysapi.qualys.com/qps/xsd/2.0/am/awsassetdataconnector.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
    <hasMoreRecords>false</hasMoreRecords>
    <data>
        <AwsAssetDataConnector>
            <id>12345</id>
            <name>new connector</name>
            <lastSync>2014-11-26T09:27:48Z</lastSync>
            <lastError>Invalid EC2 AuthRecord</lastError>
            <connectorState>ERROR</connectorState>
            <type>AWS</type>
        </AwsAssetDataConnector>
    </data>
</ServiceResponse>
```
Get connector details

Here’s how to get details on a connector using GET request. This connector is using ARN. For more information on ARN authentication, refer to Support for Cross-Account Role Authentication.

**API request:**

curl -n -u "USERNAME:PASSWORD" 
"https://qualysapi.qualys.com/qps/rest/2.0/get/am/awsassetdataconn
ector/19201"

**Response:**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="http://qualysapi.qualys.com/qps/xsd/2.0/am
/aws_asset_data_connector.xsd">
  <responseCode>SUCCESS</responseCode>
</ServiceResponse>
```
<count>1</count>
<data>
  <AwsAssetDataConnector>
    <id>19201</id>
    <name>user_john</name>
    <lastSync>2018-02-15T12:51:00Z</lastSync>
    <connectorState>FINISHED_SUCCESS</connectorState>
    <type>AWS</type>
    <defaultTags>
      <list/>
    </defaultTags>
    <activation>
      <list/>
    </activation>
    <disabled>false</disabled>
    <isGovCloudConfigured>false</isGovCloudConfigured>
    <arn>arn:aws:iam::205767712438:role/qualys_dev_test</arn>
    <externalId>1518689351038</externalId>
    <qualysAwsAccountId>383031258652</qualysAwsAccountId>
    <authRecord1/>
    <endpoints>
      <list>
        <AwsEndpointSimple>
          <regionCode>ap-south-1</regionCode>
        </AwsEndpointSimple>
      </list>
    </endpoints>
  </AwsAssetDataConnector>
</data>
</ServiceResponse>
Create AWS Connector

Creates an AWS asset data connector.

**URL**

https://<baseurl>/qps/rest/2.0/create/am/awsassetdataconnector

**Method**

POST

*disabled* (boolean) is used to disable an EC2 connector. This parameter can be set for a “create” or “update” request. When set to “true” the connector is disabled and will not run.

- If a single connector is run and it is disabled an error is returned.
- If multiple connectors are run and all are disabled an error is returned.
- If multiple connectors are run and some are disabled, only connectors that are enabled will run.

**Permissions**

Managers with Full Scope

**Example**

**Example 1: Create new AWS asset data connector**

**Request:**

```
curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST"
--data-binary @- "https://qualysapi.qualys.com/qps/rest/2.0/create/awsassetdataconnector" < file.xml
```

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

**Request POST data (file.xml):**

```
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <data>
    <AwsAssetDataConnector>
      <name>new connector</name>
      <defaultTags>
        <set>
          <TagSimple>
```

---

132 Qualys Asset Management and Tagging API
Chapter 7 — AWS Asset Data Connector API

Create AWS Connector

_Response:_

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/awsassetdataconnector.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>13</count>
  <hasMoreRecords>false</hasMoreRecords>
  <data>
    <AwsAssetDataConnector>
      <id>12345</id>
      <name>new connector</name>
      <lastSync />
      <lastError />
      <connectorState>PENDING</connectorState>
      <type>AWS</type>
      <defaultTags>
        <list>
          <TagSimple>
            <id>1</id>
            <name>EC2</name>
          </TagSimple>
        </list>
    </defaultTags>
  </AwsAssetDataConnector>
</data>
</ServiceResponse>
```
Example 2: Create new AWS asset data connector in disabled state

Request:

```
```

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

Request POST data (file.xml):

```
<ServiceRequest>
  <data>
    <AwsAssetDataConnector>
      <name>conn-disabled</name>
      <activation>
        <set>
          <ActivationModule>VM</ActivationModule>
        </set>
        <ActivationModule>PC</ActivationModule>
      </activation>
      <authRecord>
        <id>90802</id>
      </authRecord>
    </AwsAssetDataConnector>
  </data>
</ServiceResponse>
```
Chapter 7 — AWS Asset Data Connector API
Create AWS Connector

Response:
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/awsassetdataconnector.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <AwsAssetDataConnector>
      <id>254401</id>
      <name>disabled-connector</name>
      <connectorState>DISABLED</connectorState>
      <type>AWS</type>
      <defaultTags>
        <list/>
      </defaultTags>
      <activation>
        <list>
          <ActivationModule>VM</ActivationModule>
          <ActivationModule>PC</ActivationModule>
        </list>
      </activation>
      <disabled>true</disabled>
      <isGovCloudConfigured>false</isGovCloudConfigured>
      <authRecord/>
      <endpoints>
        <list>
          <AwsEndpointSimple>
            <regionCode>us-west-1</regionCode>
          </AwsEndpointSimple>
          <AwsEndpointSimple>
            <regionCode>ap-northeast-1</regionCode>
          </AwsEndpointSimple>
        </list>
    </AwsAssetDataConnector>
  </data>
</ServiceResponse>
<AwsEndpointSimple>
  <regionCode>eu-west-1</regionCode>
</AwsEndpointSimple>

...

<AwsEndpointSimple>
  <regionCode>us-east-2</regionCode>
</AwsEndpointSimple>
</list>
</endpoints>
<allRegions>true</allRegions>
</AwsAssetDataConnector>
</data>
</ServiceResponse>
Support for AWS GovCloud

`isGovCloudConfigured` (boolean) is used to enable the GovCloud (US) region for an EC2 connector. This parameter can be set for a “create” or “update” request, and is valid only when the GovCloud (US) option is enabled for your subscription.

When `isGovCloudConfigured` is set to “true”
- The connector is configured to pull instance info from the GovCloud (US) region only.
- The connector can’t be configured with `allRegions` set to “true”.

API Request:


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

Request POST data (file.xml):

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <data>
    <AwsAssetDataConnector>
      <name>gov-cloud</name>
      <activation>
        <set>
          <ActivationModule>VM</ActivationModule>
          <ActivationModule>PC</ActivationModule>
        </set>
      </activation>
      <isGovCloudConfigured>true</isGovCloudConfigured>
      <authRecord>
        <id>134601</id>
      </authRecord>
      <allRegions>false</allRegions>
      <disabled>false</disabled>
    </AwsAssetDataConnector>
  </data>
</ServiceRequest>
```
Response:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/awsassetdataconnector.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
    <data>
        <AwsAssetDataConnector>
            <id>149008</id>
            <name>gov-cloud</name>
            <connectorState>PENDING</connectorState>
            <type>AWS</type>
            <defaultTags>
                <list/>
            </defaultTags>
            <activation>
                <list>
                    <ActivationModule>VM</ActivationModule>
                    <ActivationModule>PC</ActivationModule>
                </list>
            </activation>
            <disabled>false</disabled>
            <isGovCloudConfigured>true</isGovCloudConfigured>
            <authRecord/>
            <endpoints>
                <list>
                    <AwsEndpointSimple>
                        <regionCode>us-gov-west-1</regionCode>
                    </AwsEndpointSimple>
                </list>
            </endpoints>
            <allRegions>false</allRegions>
        </AwsAssetDataConnector>
    </data>
</ServiceResponse>
```
Support for China Region

You can easily scan EC2 instances included in the AWS China region for vulnerabilities and policy compliance using the Qualys Cloud Platform. You can create/update EC2 connectors to pull instance info from the China region, activate discovered instances for the VM, PC or SCA module, and scan them using our EC2 scan workflow.

`isChinaConfigured` (boolean) is used to enable the China region for an EC2 connector using the AWS Asset Data Connector API (awsassetdataconnector). This parameter can be set for a “create” or “update” request, and is valid only when AWS China option is enabled for your subscription.

When `isChinaConfigured` is set to “true”

- The connector is configured to pull instance info from the China region only.
- The connector can’t be configured with allRegions set to “true”.

Example

API request:

curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST" --data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/create/awsassetdataconnector" < file.xml

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

Request POST data (file.xml):

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
<data>
<AwsAssetDataConnector>
  <name>cn-north-1-conn1</name>
  <authRecord>
    <id>132601</id>
  </authRecord>
  <endpoints>
    <add>
      <AwsEndpointSimple>
        <regionCode>cn-north-1</regionCode>
      </AwsEndpointSimple>
    </add>
  </endpoints>
</AwsAssetDataConnector>
</data>
</ServiceRequest>
```
Chapter 7 — AWS Asset Data Connector API
Support for China Region

<isChinaConfigured>true</isChinaConfigured>
<disabled>false</disabled>
</AwsAssetDataConnector>
</data>
</ServiceRequest>

XML output:
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/gps/xsd/2.0/am/aws_asset_data_connector.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <AwsAssetDataConnector>
      <id>136605</id>
      <name>cn-north-1-conn1</name>
      <connectorState>QUEUED</connectorState>
      <type>AWS</type>
      <defaultTags>
        <list/>
      </defaultTags>
      <activation>
        <list/>
      </activation>
      <disabled>false</disabled>
      <isGovCloudConfigured>false</isGovCloudConfigured>
      <isChinaConfigured>true</isChinaConfigured>
      <authRecord>
        <id>132601</id>
        <name>china-auth</name>
      </authRecord>
      <endpoints>
        <list>
          <AwsEndpointSimple>
            <regionCode>cn-north-1</regionCode>
          </AwsEndpointSimple>
        </list>
      </endpoints>
      <allRegions>false</allRegions>
    </AwsAssetDataConnector>
  </data>
</ServiceResponse>
<ServiceResponse>

</ServiceResponse>
Support for Cross-Account Role Authentication

Qualys supports the creation of EC2 connectors using a cross-account access role. This allows you to grant Qualys access to your AWS EC2 instances without sharing your AWS security credentials. Qualys will access your AWS EC2 instances by assuming the IAM role that you create in your AWS account.

To get started you’ll need an IAM role created using your AWS account. You can update your existing EC2 connectors to now use cross-account access roles. Note that this migration of your existing EC2 connector to cross account role is unidirectional and cannot be reverted.

You can create only one connector for each unique AWS account. It’s recommended that you merge multiple EC2 connectors into one by removing duplicate connectors before you upgrade to ARN.

Examples

Create new connector

Use this method to create a new connector when you already have the ARN generated from your AWS account.

API request:

```
curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST"
--data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/create/am/awsassetdataconnector" < file.xml
```

Request POST data (file.xml):

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <data>
    <AwsAssetDataConnector>
      <name>user_john</name>
      <arn>arn:aws:iam::705355653965:role/ARN_UPGRADE</arn>
      <externalId>1234567890</externalId>
    <endpoints>
      <add>
        <AwsEndpointSimple>
          <regionCode>ap-south-1</regionCode>
        </AwsEndpointSimple>
      </add>
    </endpoints>
  </AwsAssetDataConnector>
</ServiceRequest>
```

Note: "file.xml" contains the request POST data.
Chapter 7 — AWS Asset Data Connector API
Support for Cross-Account Role Authentication

Response:
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://qualysapi.qualys.com/qps/xsd/2.0/am/aws_asset_data_connector.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <AwsAssetDataConnector>
      <id>19803</id>
      <name>user_john</name>
      <connectorState>QUEUED</connectorState>
      <type>AWS</type>
      <defaultTags>
        <list/>
      </defaultTags>
      <activation>
        <list/>
      </activation>
      <disabled>false</disabled>
      <isGovCloudConfigured>false</isGovCloudConfigured>
      <isChinaConfigured>false</isChinaConfigured>
      <arn>arn:aws:iam::705355653965:role/ARN_UPGRADE</arn>
      <externalId>1234567890</externalId>
      <qualysAwsAccountId>383031258652</qualysAwsAccountId>
      <authRecord/>
      <endpoints>
        <list>
          <AwsEndpointSimple>
            <regionCode>ap-south-1</regionCode>
          </AwsEndpointSimple>
        </list>
      </endpoints>
      <allRegions>false</allRegions>
    </AwsAssetDataConnector>
  </data>
</ServiceResponse>
Create new connector (provide ARN later)

If you have dependencies and cannot provide the ARN at the time of creation, you could always provide the ARN at a later stage. In this case, the AWS connector is created with an INCOMPLETE state.

**API request:**

```bash
curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST" --data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/create/am/awsassetdataconnector" < file.xml
```

Note: "file.xml" contains the request POST data.

**Request POST data (file.xml):**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceRequest>
  <data>
    <AwsAssetDataConnector>
      <name>user_john</name>
      <endpoints>
        <add>
          <AwsEndpointSimple>
            <regionCode>ap-south-1</regionCode>
          </AwsEndpointSimple>
        </add>
      </endpoints>
      <disabled>false</disabled>
    </AwsAssetDataConnector>
  </data>
</ServiceRequest>
```

**Response:**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="http://qualysapi.qualys.com/qps/xsd/2.0/am/aws_asset_data_connector.xsd">
  <responseCode>SUCCESS</responseCode>
</ServiceResponse>
```
<count>1</count>
<data>
<AwsAssetDataConnector>
  <id>19201</id>
  <name>my-aws-connector</name>
  <connectorState>INCOMPLETE</connectorState>
  <type>AWS</type>
  <defaultTags>
    <list/>
  </defaultTags>
  <activation>
    <list/>
  </activation>
  <disabled>false</disabled>
  <isGovCloudConfigured>false</isGovCloudConfigured>
  <externalId>1518689351038</externalId>
  <qualysAwsAccountId>383031258652</qualysAwsAccountId>
  <endpoints>
    <list>
      <AwsEndpointSimple>
        <regionCode>ap-south-1</regionCode>
      </AwsEndpointSimple>
    </list>
  </endpoints>
  <allRegions>false</allRegions>
</AwsAssetDataConnector>
</data>
</ServiceResponse>
Chapter 7 — AWS Asset Data Connector API

Update AWS Connector

Updates writable fields and collections.

**URL**

https://<baseurl>/qps/rest/2.0/update/am/awsassetdataconnector/<id>

or

https://<baseurl>/qps/rest/2.0/update/am/awsassetdataconnector

**Method**

POST

Using the NOT EQUALS operator for updating AWS connectors could result in accidental update of unknown AWS connectors without any warning. To prevent accidental updates of unknown AWS connectors, we do not support NOT EQUALS operator for update actions.

**Permissions**

Managers with Full Scope

**Examples**

Change the name of an asset data connector with ID of 12345, add a tag with the ID of 1 to the defaultTags collection, and add us-east-1 as scanned region.

**Request**:


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

**Request POST data (file.xml):**

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <data>
    <AwsAssetDataConnector>
      <name>Updated Name</name>
      <defaultTags>
        <add>
          <TagSimple>
            <id>1</id>
          </TagSimple>
        </add>
      </defaultTags>
      <scannedRegion>
        <add>
          <Value>us-east-1</Value>
        </add>
      </scannedRegion>
    </AwsAssetDataConnector>
  </data>
</ServiceRequest>
```

146 Qualys Asset Management and Tagging API
Chapter 7 — AWS Asset Data Connector API

Update AWS Connector

Response:

<?xml version="1.0" encoding="UTF-8"?><ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/awsassetdataconnector.xsd"><responseCode>SUCCESS</responseCode><count>1</count><hasMoreRecords>false</hasMoreRecords><data><AssetDataConnector><id>12345</id><name>External VPC</name><lastSync>2014-11-26T08:44:05Z</lastSync><lastError /></AssetDataConnector><defaultTags><list><TagSimple><id>1</id><name>EC2</name></TagSimple></list></defaultTags><activation><ActivationModule>VM</ActivationModule></activation></ServiceResponse>
Update existing key-based connector to cross-account role

Here’s how to update an existing connector to use a cross-access account role. You’ll need the ARN generated from your AWS account. Note that this migration of your existing EC2 connector to cross account role is unidirectional and cannot be reverted.

**API request:**

```
curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST" --data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/update/am/awsassetdataconnector/12345" < file.xml
```

Note: "file.xml" contains the request POST data.

**Request POST data (file.xml):**

```
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <data>
    <AwsAssetDataConnector>
      <arn>arn:aws:iam::205767712438:role/qualys_dev_test</arn>
      <externalId>123456789</externalId>
    </AwsAssetDataConnector>
  </data>
</ServiceRequest>
```

**Response:**

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://qualysapi.qualys.com/qps/xsd/2.0/am/aws_asset_data_connector.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <AwsAssetDataConnector>
      <id>19201</id>
    </AwsAssetDataConnector>
  </data>
</ServiceResponse>
```
Chapter 7 — AWS Asset Data Connector API
Update AWS Connector

</AwsAssetDataConnector>
</data>
</ServiceResponse>
Search AWS Connectors

Returns a list of AWS connectors that match the provided criteria.

**URL**
https://<baseurl>/qps/rest/2.0/search/am/awsassetdataconnector

**Method**
POST

**Pagination**
A maximum of 100 instances are returned by default. To customize this specify a “preferences” tag in the POST body of your request.

**Limit your results**
Use the optional “fields” parameter to limit the amount of information returned for each AWS connector. [Learn more](#)

### Searchable Fields

These fields can be used to search for AWS connectors.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id (Integer)</td>
<td>Primary key</td>
</tr>
<tr>
<td>name (Text)</td>
<td></td>
</tr>
<tr>
<td>description (Text)</td>
<td></td>
</tr>
<tr>
<td>lastSync (Date)</td>
<td></td>
</tr>
<tr>
<td>lastError (Text)</td>
<td></td>
</tr>
<tr>
<td>connectorState (Keyword)</td>
<td>PENDING, RUNNING, SUCCESS, ERROR</td>
</tr>
<tr>
<td>activation (Keyword)</td>
<td>VM or PC</td>
</tr>
<tr>
<td>defaultTags.name (Text)</td>
<td>The name of a tag in the defaultTags collection</td>
</tr>
<tr>
<td>defaultTag (Integer)</td>
<td>The ID of a tag in the defaultTags collection</td>
</tr>
<tr>
<td>allRegions (Boolean)</td>
<td></td>
</tr>
<tr>
<td>serviceType (Keyword)</td>
<td>EC2</td>
</tr>
<tr>
<td>endpoint.region (Text)</td>
<td>AWS region code</td>
</tr>
<tr>
<td>authRecord (Integer)</td>
<td>The ID of the authentication record</td>
</tr>
</tbody>
</table>
Chapter 7 — AWS Asset Data Connector API

Search AWS Connectors

151 Qualys Asset Management and Tagging API

Permissions

Managers with Full Scope

Example

Find all asset data connectors with tag name USA.

Request:

Request POST data (file.xml):

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <filters>
    <Criteria field="defaultTags.name" operator="EQUALS">USA</Criteria>
  </filters>
</ServiceRequest>
```

Response:

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

<table>
<thead>
<tr>
<th>authRecord.name (Text)</th>
<th>The name of the authentication record</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled (Boolean)</td>
<td>Whether execution of the connector is disabled (YES). If disabled the connector will not synchronize assets.</td>
</tr>
</tbody>
</table>

Allowed Operators

<table>
<thead>
<tr>
<th>Type</th>
<th>Operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integer</td>
<td>EQUALS, NOT EQUALS, GREATER, LESSER, IN</td>
</tr>
<tr>
<td>Text</td>
<td>CONTAINS, EQUALS, NOT EQUALS</td>
</tr>
<tr>
<td>Date</td>
<td>EQUALS, NOT EQUALS, GREATER, LESSER</td>
</tr>
<tr>
<td>Keyword</td>
<td>EQUALS, NOT EQUALS, IN</td>
</tr>
<tr>
<td>Boolean</td>
<td>(true/false) EQUALS, NOT EQUALS</td>
</tr>
</tbody>
</table>
instance"
  xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/xsd/2.0/am/awsassetdataconnector.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>13</count>
  <hasMoreRecords>false</hasMoreRecords>
  <data>
    <AwsAssetDataConnector>
      <id>12345</id>
      <name>NEW Connector</name>
      <lastSync>2014-11-26T09:27:48Z</lastSync>
      <lastError>Invalid EC2 AuthRecord</lastError>
      <connectorState>ERROR</connectorState>
      <type>AWS</type>
      <defaultTags>
        <list>
          <TagSimple>
            <id>1</id>
            <name>USA</name>
          </TagSimple>
        </list>
      </defaultTags>
      <activation/>
      <authRecord>
        <id>1</id>
        <name>my ec2</name>
      </authRecord>
      <endpoints>
        <list>
          <AwsEndpointSimple>
            <regionCode>us-east-1</regionCode>
          </AwsEndpointSimple>
        </list>
      </endpoints>
      <allRegions>false</allRegions>
    </AwsAssetDataConnector>
  </data>
</ServiceResponse>
Count AWS Connectors

Returns the number of AWS connectors that match the provided criteria.

URL
https://<baseurl>/qps/rest/2.0/count/am/awsassetdataconnector

Method
POST

Permissions
Managers with Full Scope

Example

Count the number of AWS connectors with the tag name USA.

Request:

curl -u "USERNAME:PASSWORD"
"https://qualysapi.qualys.com/qps/rest/2.0/count/am/assetdataconnector" < file.xml

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

Request POST data (file.xml):

<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <filters>
    <Criteria field="defaultTags.name" operator="EQUALS">USA</Criteria>
  </filters>
</ServiceRequest>

Response:

<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/awsassetdataconnector.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
</ServiceResponse>
Delete AWS Connector

Delete one or more AWS connectors.

**URL**

https://<baseurl>/qps/rest/2.0/delete/am/awsassetdataconnector/<id>

or

https://<baseurl>/qps/rest/2.0/delete/am/awsassetdataconnector

**Method**

POST

Using the NOT EQUALS operator for deleting AWS connectors could result in accidental deletion of AWS connectors without any warning. To prevent accidental deletion of unknown AWS connectors, we do not support NOT EQUALS operator for delete actions.

**Permissions**

Managers with Full Scope

**Examples**

**Request 1:**
Delete a single AWS connector.

curl -n -u "USERNAME:PASSWORD" "https://qualysapi.qualys.com/qps/rest/2.0/delete/am/awsassetdataconnector/12345"

**Response:**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/awsassetdataconnector.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>1</count>
    <data>
        <AssetDataConnector><id>12345</id></AssetDataConnector>
    </data>
</ServiceResponse>
```
Delete several AWS connectors tagged with the To Delete tag.

curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/delete/am/awsassetdataconnector" < file.xml

**Request POST data (file.xml):**

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <filters>
    <Criteria field="tagName" operator="EQUALS">To Delete</Criteria>
  </filters>
</ServiceRequest>
```

**Response:**

```xml
<?xml version="1.0" encoding="UTF-8"?>
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <AssetDataConnector>
      <id>1972521</id>
    </AssetDataConnector>
  </data>
</ServiceResponse>
```
Run Connector

Request that one or more asset data connectors are run. The connectors may be run immediately, or queued to run when there is capacity. The response will almost always indicate that the connector is pending. Use GET calls to monitor the status of connectors.

**URL**

https://<baseurl>/qps/rest/2.0/run/am/assetdataconnector/<id>

or

https://<baseurl>/qps/rest/2.0/run/am/assetdataconnector

**Method**

POST

**Permissions**

Managers with Full Scope

**See also**

See also Run Connector
AWS Connector Fields

<table>
<thead>
<tr>
<th>Name (type)</th>
<th>Description</th>
<th>Writable</th>
</tr>
</thead>
<tbody>
<tr>
<td>id (long)</td>
<td>Primary key</td>
<td>No</td>
</tr>
<tr>
<td>name (string)</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>description (string)</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>lastSynch (date)</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>lastError (string)</td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>connectorState (AssetDataConnectorState)</td>
<td>PENDING, RUNNING, SUCCESS, ERROR, DISABLED, INCOMPLETE</td>
<td>No</td>
</tr>
<tr>
<td>type (AssetDataConnectorType)</td>
<td>AWS</td>
<td>No</td>
</tr>
<tr>
<td>defaultTags (TagSimpleQList)</td>
<td>Tags applied to any asset discovered by the connector</td>
<td>Yes</td>
</tr>
<tr>
<td>activation (List&lt;ActivationModule&gt;)</td>
<td>Assets discovered by the connector will be activated for the modules specified</td>
<td>Yes</td>
</tr>
<tr>
<td>authRecord (AwsAuthRecordSimple)</td>
<td>The AWS authentication record the connector will use to connect to AWS. When writing/updating it is looked up by the ID field.</td>
<td>Yes</td>
</tr>
<tr>
<td>serviceType (AwsServiceType)</td>
<td>EC2</td>
<td>Yes</td>
</tr>
<tr>
<td>allRegions (boolean)</td>
<td>If true the end point’s collection will be ignored an all AWS regions scanned</td>
<td>Yes</td>
</tr>
<tr>
<td>disabled (boolean)</td>
<td>Whether execution of the connector is disabled (YES). If disabled the connector will not synchronize assets.</td>
<td>Yes</td>
</tr>
<tr>
<td>arn</td>
<td>Generated by AWS. Ensure that you provide the same ARN that is generated by AWS.</td>
<td>yes</td>
</tr>
<tr>
<td>externalId</td>
<td>Random string which is unique for each user.</td>
<td>yes</td>
</tr>
</tbody>
</table>

Associations

AwsEndpointSimpleQList - A basic wrapper with one field: regionCode. This is the AWS region code, e.g. us-east-1.
AwsAuthRecordSimple - The authentication record a connector will use to communicate with AWS. id (long) is the connector ID, and name (string) is a human readable name to identify the connector key.
AWS Authentication Record API

The AWS Authentication Record API provides a suite of API functions for managing AWS authentication records, used to scan EC2 instances.

Operations
Get AWS Auth Record Info
Create AWS Auth Record
Update AWS Auth Record
Search AWS Auth Records
Count AWS Auth Records
Delete AWS Auth Record

Reference
AWS Auth Record Fields
Get AWS Auth Record Info

Returns a single AWS authentication record by ID.

**URL**
https://<baseurl>/qps/rest/2.0/get/am/awsauthrecord/<id>

**Method**
GET

**Limit your results**
Use the optional “fields” parameter to limit the amount of information returned for the authentication record. Learn more

**Permissions**
Managers with Full Scope

**Example**

Fetch the authentication record with the ID 12345.

**Request:**
curl -n -u "USERNAME:PASSWORD" "https://qualysapi.qualys.com/qps/rest/2.0/get/am/awsauthrecord/12345"

**Response:**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/awsauthrecord.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <AwsAuthRecord>
      <id>12345</id>
      <name>Auth Record</name>
      <created>2014-02-06T19:14:50Z</created>
      <modified>2014-02-06T19:14:50Z</modified>
    </AwsAuthRecord>
  </data>
</ServiceResponse>
```
Create AWS Auth Record

Creates a new authentication record.

**URL**
https://<baseurl>/qps/rest/2.0/create/am/awsauthrecord

**Method**
POST

**Permissions**
Managers with Full Scope

**Example**
Create a new authentication record.

**Request:**
curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST" --data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/create/awsauthrecord" < file.xml

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

**Request POST data (file.xml):**
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <data>
    <AwsAuthRecord>
      <name>Simple Auth Record</name>
      <description>Production Auth Record</description>
      <accessKeyId>AAAAAAAAAAAAAAA11A</accessKeyId><secretKey>1aAa1aaallaaaAaaAaa1Aaa1AaaAaaAaaA</secretKey>
    </AwsAuthRecord>
  </data>
</ServiceRequest>

**Response:**
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xs
Create AWS Auth Record

```
d/2.0/am/awsauthrecord.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <AwsAuthRecord>
      <id>12345</id>
      <name>Simple Auth Record</name>
      <description>Production Auth Record</description>
      <created>2014-02-06T19:14:50Z</created>
      <modified>2014-02-06T19:14:50Z</modified>
    </AwsAuthRecord>
  </data>
</ServiceResponse>
```
Update AWS Auth Record

Updates writable fields.

**URL**

https://<baseurl>/qps/rest/2.0/update/am/awsauthrecord/<id>

or

https://<baseurl>/qps/rest/2.0/update/am/awsauthrecord

**Method**

POST

Using the NOT EQUALS operator for updating AWS authentication records could result in accidental update of unknown AWS authentication records without any warning. To prevent accidental updates of unknown AWS authentication records, we do not support NOT EQUALS operator for update actions.

**Permissions**

Managers with Full Scope

**Example**

Update the secret key of auth record 12345

**Request:**

curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST" --data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/update/am/awsauthrecord/12345" < file.xml

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

**Request POST data (file.xml):**

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <data>
    <AwsAuthRecord>
      <secretKey>1aA1aa1aaaa1aAaAaaAaaAaa1Aaaaa11aaAAAAaaaA</secretKey>
    </AwsAuthRecord>
  </data>
</ServiceRequest>
```

**Response:**

163 Qualys Asset Management and Tagging API
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/awsauthrecord.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <AwsAuthRecord>
      <id>12345</id>
      <name>Simple Auth Record</name>
      <description>Production Auth Record</description>
      <created>2014-02-06T19:14:50Z</created>
      <modified>2014-02-06T19:14:50Z</modified>
    </AwsAuthRecord>
  </data>
</ServiceResponse>
Search AWS Auth Records

Returns a list of authentication records that match the provided criteria.

**URL**
https://<baseurl>/qps/rest/2.0/search/am/awsauthrecord

**Method**
POST

**Pagination**
A maximum of 100 instances are returned by default. To customize this specify a “preferences” tag in the POST body of your request.

**Limit your results**
Use the optional “fields” parameter to limit the amount of information returned for each authentication record. Learn more

### Searchable Fields

These fields can be used to search for authentication records.

<table>
<thead>
<tr>
<th>Field</th>
<th>Type</th>
<th>Operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Integer</td>
<td>EQUALS, NOT EQUALS, GREATER, LESSER, IN</td>
</tr>
<tr>
<td>name</td>
<td>Text</td>
<td>CONTAINS, EQUALS, NOT EQUALS</td>
</tr>
<tr>
<td>description</td>
<td>Text</td>
<td></td>
</tr>
<tr>
<td>created</td>
<td>Date</td>
<td>EQUALS, NOT EQUALS, GREATER, LESSER</td>
</tr>
<tr>
<td>modified</td>
<td>Date</td>
<td></td>
</tr>
</tbody>
</table>

**Permissions**

Managers with Full Scope

**Example**

Find all authentication records that have a name that contains the string AUTH.

**Request**

curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --data-binary @-

165 Qualys Asset Management and Tagging API
Chapter 8 — AWS Authentication Record API
Search AWS Auth Records

"https://qualysapi.qualys.com/qps/rest/2.0/search/am/awsauthrecord" < file.xml

Request POST data (file.xml):

<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
    <filters>
        <Criteria field="name" operator="CONTAINS">Simple</Criteria>
    </filters>
</ServiceRequest>

Response:

<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/awsauthrecord.xsd">
    <responseCode>SUCCESS</responseCode>
    <count>4</count>
    <hasMoreRecords>false</hasMoreRecords>
    <data>
        <AwsAuthRecord>
            <id>66013771</id>
            <name>Simple Auth Record 1</name>
            <modified>2014-12-22T18:36:44Z</modified>
        </AwsAuthRecord>
        <AwsAuthRecord>
            <id>66023771</id>
            <name>Simple Auth Record 2</name>
            <modified>2014-12-22T18:36:58Z</modified>
        </AwsAuthRecord>
        <AwsAuthRecord>
            <id>66033771</id>
            <name>Simple Auth Record 3</name>
            <modified>2014-12-22T18:37:01Z</modified>
        </AwsAuthRecord>
        <AwsAuthRecord>
            <id>66043771</id>
            <name>Simple Auth Record 4</name>
            <modified>2014-12-22T19:11:18Z</modified>
        </AwsAuthRecord>
    </data>
</ServiceResponse>
</AwsAuthRecord>
</data>
</ServiceResponse>
Count AWS Auth Records

Returns the number of authentication records that match the provided criteria.

**URL**
https://<baseurl>/qps/rest/2.0/count/am/awsauthrecord

**Method**
POST

**Permissions**
Managers with Full Scope

**Example**

Count the number of authentication records that have a name that contains the string AUTH.

**Request:**

curl -u "USERNAME:PASSWORD"
"https://qualysapi.qualys.com/qps/rest/2.0/count/am/awsauthrecord"
< file.xml

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

**Request POST data (file.xml):**

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <filters>
    <Criteria field="name" operator="CONTAINS">AUTH</Criteria>
  </filters>
</ServiceRequest>
```

**Response:**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/awsauthrecord.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
</ServiceResponse>
```
Delete AWS Auth Record

Delete one or more authentication records.

**URL**

- https://<baseurl>/qps/rest/2.0/delete/am/awsauthrecord/
  - <id>
- or
- https://<baseurl>/qps/rest/2.0/delete/am/awsauthrecord

**Method**

POST

Using the NOT EQUALS operator for deleting AWS authentication records could result in accidental deletion of unknown AWS authentication records without any warning. To prevent accidental deletion of unknown AWS authentication records, we do not support NOT EQUALS operator for delete actions.

**Permissions**

Managers with Full Scope

**Examples**

**Request 1:**

Delete a single authentication record.

curl -n -u "USERNAME:PASSWORD"
"https://qualysapi.qualys.com/qps/rest/2.0/delete/am/awsauthrecord/12345"

**Response:**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/awsauthrecord.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <AssetDataConnector>
      <id>12345</id>
    </AssetDataConnector>
  </data>
</ServiceResponse>
```
Chapter 8 — AWS Authentication Record API
Delete AWS Auth Record

</ServiceResponse>
Request 2:
Delete several authentication records whose names contain the string "delete me".

```
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --data-binary @-
"https://qualysapi.qualys.com/qps/rest/2.0/delete/am/awsauthrecord"
" < file.xml
```

Request POST data (file.xml):
```
<?xml version="1.0" encoding="UTF-8" ?>
<ServiceRequest>
  <filters>
    <Criteria field="name" operator="CONTAINS">delete me</Criteria>
  </filters>
</ServiceRequest>
```

Response:
```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/2.0/am/awsauthrecord.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <AwsAuthRecord>
      <id>2020094</id>
    </AwsAuthRecord>
  </data>
</ServiceResponse>
```
# AWS Auth Record Fields

<table>
<thead>
<tr>
<th>Name (type)</th>
<th>Description</th>
<th>Writable</th>
</tr>
</thead>
<tbody>
<tr>
<td>name (string)</td>
<td>Name of the authentication record</td>
<td>Yes</td>
</tr>
<tr>
<td>description (string)</td>
<td>Brief description of the authentication record</td>
<td>Yes</td>
</tr>
<tr>
<td>created (date)</td>
<td>When record was created</td>
<td>No</td>
</tr>
<tr>
<td>modified (date)</td>
<td>When record was last modified</td>
<td>No</td>
</tr>
<tr>
<td>secretKey (string)</td>
<td>The AWS secret key - write only, cannot be read</td>
<td>Yes</td>
</tr>
<tr>
<td>accessKeyId (string)</td>
<td>The AWS access key - write only, cannot be read</td>
<td>Yes</td>
</tr>
</tbody>
</table>
JSON Support

Qualys Asset Management and Tagging API supports JSON requests and responses starting with version 2.11. Samples are shown below.

**Headers used in samples**

- Send JSON request: "Content-Type: application/json"
- Get response in JSON: "Accept: application/json"

**Example 1: Create a tag**

**Request:**

```bash
```

**POST data:**

```json
{
  "ServiceRequest": {
    "data": {
      "Tag": {
        "name": "Parent Tag",
        "ruleType": "NAME_CONTAINS",
        "ruleText": "windows",
        "color": "#FFFFFF",
        "children": {
          "set": {
            "TagSimple": [
              { "name": "Child 1" },
              { "name": "Child 2" }
            ]
          }
        }
      }
    }
  }
}
```
Appendix A — JSON Support

Response:

{
  "ServiceResponse": {
    "data": [
      {
        "Tag": {
          "ruleText": "windows",
          "color": "#FFFFFF",
          "modified": "2016-01-04T19:51:56Z",
          "name": "Parent Tag",
          "children": {
            "list": [
              {
                "TagSimple": {
                  "name": "Child 2",
                  "id": 2066216
                }
              },
              {
                "TagSimple": {
                  "name": "Child 1",
                  "id": 2066217
                }
              }
            ]
          },
          "created": "2016-01-04T19:51:56Z",
          "ruleType": "NAME_CONTAINS",
          "id": 2066215
        }
      }
    ],
    "count": 1,
    "responseCode": "SUCCESS"
  }
}
Example 2: Search tags

Request:

```
"https://qualysapi.qualys.com/qps/rest/2.0/search/am/tag"
```

POST data:

```json
{
    "ServiceRequest": {
        "filters": [
            {
                "field": "parent",
                "operator": "EQUALS",
                "value": "2035617"
            },
            {
                "field": "name",
                "operator": "CONTAINS",
                "value": "child"
            },
            {
                "field": "id",
                "operator": "IN",
                "value": "2035619,2035618,2029815"
            },
            {
                "field": "ruleType",
                "operator": "EQUALS",
                "value": "GROOVY"
            },
            {
                "field": "color",
                "operator": "EQUALS",
                "value": "#EC7000"
            }
        ]
    }
}
```

Response:

```json
{
    "ServiceResponse": {
        "data": [
            {
                "id": "2035619",
                "name": "child",
                "parent": "2035617",
                "color": "#EC7000",
                "ruleType": "GROOVY"
            }
        ]
    }
}
```
"Tag": {
  "ruleText": "windows",
  "color": "#FFFFFF",
  "modified": "2016-01-04T19:51:56Z",
  "name": "Parent Tag",
  "children": [
    "list": [
      "TagSimple": {
        "name": "Child 2",
        "id": 2066216
      }
    ],
    "TagSimple": {
      "name": "Child 1",
      "id": 2066217
    }
  ],
  "created": "2016-01-04T19:51:56Z",
  "ruleType": "NAME_CONTAINS",
  "id": 2066215
}
}
"count": 1,
"responseCode": "SUCCESS"