Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.12

May 27, 2021 (Updated June 22, 2021)

This new version of the Qualys Cloud Platform (VM, PC) includes improvements to the Qualys API. You'll find all the details in our user guides, available at the time of release. Just log in to your Qualys account and go to Help > Resources.

What's New

Qualys API Server URL

The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click here to identify your Qualys platform and get the API URL

This documentation uses the API server URL for Qualys US Platform 1 (https://qualysapi.qualys.com) in sample API requests. If you're on another platform, please replace this URL with the appropriate server URL for your account.

VM Host List and VM Host List Detection - Option to Return Host Metadata for All Cloud Providers

APIs affected	/api/2.0/fo/asset/host/?action=list /api/2.0/fo/asset/host/vm/detection/?action=list
New or Updated API	Updated
DTD or XSD changes	No

Starting in this release, users can specify host_metadata=all when making a Host List or Host List Detection API call. This returns metadata information for cloud assets across all cloud providers in the same request. Prior to this, users could only return metadata information for one cloud provider at a time using host_metadata with a value of ec2, google or azure. Tip - Use host_metadata=all with host_metadata_fields to only return data for certain attributes.

Please note that there is no change to the XML output format or DTD for Host List or Host List Detection. The only change is that prior to this release, the response included metadata for a single cloud provider and now the response includes metadata for all cloud providers when host_metadata=all is specified. Similarly, the CSV output format for Host List Detection has not changed, except that metadata for all cloud providers is shown when host_metadata=all is specified.

Input Parameters

Use these input parameters with Host List and Host List Detection APIs. Refer to the Qualys API (VM,PC) User Guide for details on all available input parameters.

Parameter	Description
host_metadata={value}	(Optional) Specify “all” to list all cloud assets with their metadata or specify the name of the cloud provider to show only the assets managed by the cloud provider. Valid values: all, ec2, google, azure
host_metadata_fields={value1,value2}	(Optional when host_metadata is specified) Specify metadata fields to only return data for certain attributes.

Host List Detection API Sample

In this sample, the output will include cloud asset metadata for all cloud providers.

API request:

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_VM_DETECTION_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/dtd/outp
ut.dtd">
<HOST_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-05-27T19:24:29Z</DATETIME>
    <HOST_LIST>
      <HOST>
        <ID>1003</ID>
        <IP>10.20.30.40</IP>
        <TRACKING_METHOD>AGENT</TRACKING_METHOD>
        <NETWORK_ID>6000</NETWORK_ID>
        <OS><![CDATA[NetScaler]]></OS>
        <DNS><![CDATA[abc.sample.qualys.com]]></DNS>
        <DNS_DATA>
          <HOSTNAME><![CDATA[abc]]></HOSTNAME>
          <DOMAIN><![CDATA[sample.qualys.com]]></DOMAIN>
          <FQDN><![CDATA[abc.sample.qualys.com]]></FQDN>
        </DNS_DATA>
        <CLOUD_PROVIDER><![CDATA[Azure]]></CLOUD_PROVIDER>
        <CLOUD_SERVICE><![CDATA[VM]]></CLOUD_SERVICE>
        <CLOUD_RESOURCE_ID><![CDATA[2b21e19a-01b6-45f4-b54d-
1c4e0c5b6564]]></CLOUD_RESOURCE_ID>
        <!-- <EC2_INSTANCE_ID> tag has been deprecated. Please refer to
<CLOUD_RESOURCE_ID> tag for the same information //-->
        <EC2_INSTANCE_ID><![CDATA[2b21e19a-01b6-45f4-b54d-
1c4e0c5b6564]]></EC2_INSTANCE_ID>
        <LAST_SCAN_DATETIME>2020-07-18T01:08:27Z</LAST_SCAN_DATETIME>
        <LAST_VM_SCANNED_DATE>2020-07-15T19:18:07Z</LAST_VM_SCANNED_DATE>
        <LAST_VM_SCANNED_DURATION>611</LAST_VM_SCANNED_DURATION>
        <LAST_VM_AUTH_SCANNED_DATE>2019-07-
24T00:00:00Z</LAST_VM_AUTH_SCANNED_DATE>
        <METADATA>
          <AZURE>
            <ATTRIBUTE>
              <NAME><![CDATA[ipv6]]></NAME>
              <LAST_STATUS>Success</LAST_STATUS>
              <VALUE><![CDATA[]]></VALUE>
              <LAST_SUCCESS_DATE>2019-07-24T00:00:00Z</LAST_SUCCESS_DATE>
              <LAST_ERROR_DATE></LAST_ERROR_DATE>
              <LAST_ERROR><![CDATA[]]></LAST_ERROR>
            </ATTRIBUTE>
            <ATTRIBUTE>
              <NAME><![CDATA[latest/dynamic/instance-
identity/document/privateIp]]></NAME>
```

```
              <LAST_STATUS>Success</LAST_STATUS>
              <VALUE><![CDATA[10.20.30.40]]></VALUE>
              <LAST_SUCCESS_DATE>2019-07-24T00:00:00Z</LAST_SUCCESS_DATE>
              <LAST_ERROR_DATE></LAST_ERROR_DATE>
              <LAST_ERROR><![CDATA[]]></LAST_ERROR>
            </ATTRIBUTE>
            <ATTRIBUTE>
              <NAME><![CDATA[latest/dynamic/instance-
identity/document/version]]></NAME>
              <LAST_STATUS>Success</LAST_STATUS>
              <VALUE><![CDATA[7.5.20180815]]></VALUE>
              <LAST_SUCCESS_DATE>2019-07-24T00:00:00Z</LAST_SUCCESS_DATE>
              <LAST_ERROR_DATE></LAST_ERROR_DATE>
              <LAST_ERROR><![CDATA[]]></LAST_ERROR>
            </ATTRIBUTE>
            ...
          </AZURE>
        </METADATA>
        <DETECTION_LIST>
        ...
        </DETECTION_LIST>
      </HOST>
      <HOST>
        <ID>2001</ID>
        <IP>10.40.50.60</IP>
        <TRACKING_METHOD>AGENT</TRACKING_METHOD>
        <NETWORK_ID>6000</NETWORK_ID>
        <DNS><![CDATA[ec2-54.compute-1.amazonaws.com]]></DNS>
        <DNS_DATA>
          <HOSTNAME><![CDATA[ec2-54]]></HOSTNAME>
          <DOMAIN><![CDATA[compute-1.amazonaws.com]]></DOMAIN>
          <FQDN><![CDATA[ec2-54.compute-1.amazonaws.com]]></FQDN>
        </DNS_DATA>
        <CLOUD_PROVIDER><![CDATA[AWS]]></CLOUD_PROVIDER>
        <CLOUD_SERVICE><![CDATA[EC2]]></CLOUD_SERVICE>
        <CLOUD_RESOURCE_ID><![CDATA[i-
065afe5fa179422e6]]></CLOUD_RESOURCE_ID>
        <!-- <EC2_INSTANCE_ID> tag has been deprecated. Please refer to
<CLOUD_RESOURCE_ID> tag for the same information //-->
       <EC2_INSTANCE_ID><![CDATA[i-065afe5fa179422e6]]></EC2_INSTANCE_ID>
        <LAST_SCAN_DATETIME>2020-07-18T01:08:17Z</LAST_SCAN_DATETIME>
        <LAST_VM_SCANNED_DATE>2020-07-13T20:44:23Z</LAST_VM_SCANNED_DATE>
        <LAST_VM_SCANNED_DURATION>436</LAST_VM_SCANNED_DURATION>
        <METADATA>
          <EC2>
            <ATTRIBUTE>
              <NAME><![CDATA[firstDiscovered]]></NAME>
              <LAST_STATUS>Success</LAST_STATUS>
              <VALUE><![CDATA[1591600285000]]></VALUE>
```

```
            <LAST_SUCCESS_DATE>2020-06-30T00:00:00Z</LAST_SUCCESS_DATE>
            <LAST_ERROR_DATE></LAST_ERROR_DATE>
            <LAST_ERROR><![CDATA[]]></LAST_ERROR>
          </ATTRIBUTE>
          <ATTRIBUTE>
            <NAME><![CDATA[groupId]]></NAME>
            <LAST_STATUS>Success</LAST_STATUS>
            <VALUE><![CDATA[sg-68a08f1d]]></VALUE>
            <LAST_SUCCESS_DATE>2020-06-30T00:00:00Z</LAST_SUCCESS_DATE>
            <LAST_ERROR_DATE></LAST_ERROR_DATE>
            <LAST_ERROR><![CDATA[]]></LAST_ERROR>
          </ATTRIBUTE>
          <ATTRIBUTE>
            <NAME><![CDATA[groupName]]></NAME>
            <LAST_STATUS>Success</LAST_STATUS>
            <VALUE><![CDATA[group-108]]></VALUE>
            <LAST_SUCCESS_DATE>2020-06-30T00:00:00Z</LAST_SUCCESS_DATE>
            <LAST_ERROR_DATE></LAST_ERROR_DATE>
            <LAST_ERROR><![CDATA[]]></LAST_ERROR>
          </ATTRIBUTE>
          ...
        </EC2>
      </METADATA>
      <DETECTION_LIST>
      ...
      </DETECTION_LIST>
    </HOST>
  </HOST_LIST>
 </RESPONSE>
</HOST_LIST_VM_DETECTION_OUTPUT>
```

Host List API Sample

In this sample, the output will include cloud asset metadata for all cloud providers but only metadata fields location and firstDiscovered are returned.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/?action=list&host_met
adata=all&host_metadata_fields=location,firstDiscovered" >
host_list_specific_metadata_all_cloud_provider.xml
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE HOST_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/dtd/list/output.dtd">
<HOST_LIST_OUTPUT>
```

```
  <RESPONSE>
    <DATETIME>2021-05-27T19:18:13Z</DATETIME>
    <HOST_LIST>
      <HOST>
        <ID>1003</ID>
        <IP>10.11.12.13</IP>
        <TRACKING_METHOD>Cloud Agent</TRACKING_METHOD>
        <NETWORK_ID>6000</NETWORK_ID>
        <DNS><![CDATA[abc.sample.qualys.com]]></DNS>
        <DNS_DATA>
          <HOSTNAME><![CDATA[abc]]></HOSTNAME>
          <DOMAIN><![CDATA[sample.qualys.com]]></DOMAIN>
          <FQDN><![CDATA[abc.sample.qualys.com]]></FQDN>
        </DNS_DATA>
        <CLOUD_PROVIDER><![CDATA[Azure]]></CLOUD_PROVIDER>
        <CLOUD_SERVICE><![CDATA[VM]]></CLOUD_SERVICE>
        <CLOUD_RESOURCE_ID><![CDATA[2b21e19a-01b6-45f4-b54d-
1c4e0c5b6564]]></CLOUD_RESOURCE_ID>
        <!-- <EC2_INSTANCE_ID> tag has been deprecated. Please refer to
<CLOUD_RESOURCE_ID> tag for the same information //-->
        <EC2_INSTANCE_ID><![CDATA[2b21e19a-01b6-45f4-b54d-
1c4e0c5b6564]]></EC2_INSTANCE_ID>
        <OS><![CDATA[NetScaler]]></OS>
        <QG_HOSTID><![CDATA[a731f9b5-80d2-422c-91f7-
6cd41d0428d6]]></QG_HOSTID>
        <METADATA>
          <AZURE>
            <ATTRIBUTE>
              <NAME><![CDATA[location]]></NAME>
              <LAST_STATUS>Success</LAST_STATUS>
              <VALUE><![CDATA[eastus]]></VALUE>
              <LAST_SUCCESS_DATE>2019-07-24T00:00:00Z</LAST_SUCCESS_DATE>
              <LAST_ERROR_DATE></LAST_ERROR_DATE>
              <LAST_ERROR><![CDATA[]]></LAST_ERROR>
            </ATTRIBUTE>
          </AZURE>
        </METADATA>
      </HOST>
      <HOST>
        <ID>2000</ID>
        <IP>10.11.12.14</IP>
        <TRACKING_METHOD>Cloud Agent</TRACKING_METHOD>
        <NETWORK_ID>6000</NETWORK_ID>
        <DNS><![CDATA[ec2-52.compute-1.amazonaws.com]]></DNS>
        <DNS_DATA>
          <HOSTNAME><![CDATA[ec2-52]]></HOSTNAME>
          <DOMAIN><![CDATA[compute-1.amazonaws.com]]></DOMAIN>
          <FQDN><![CDATA[ec2-52.compute-1.amazonaws.com]]></FQDN>
        </DNS_DATA>
```

```
        <CLOUD_PROVIDER><![CDATA[AWS]]></CLOUD_PROVIDER>
        <CLOUD_SERVICE><![CDATA[EC2]]></CLOUD_SERVICE>
        <CLOUD_RESOURCE_ID><![CDATA[i-
06c788ce177fad52b]]></CLOUD_RESOURCE_ID>
        <!-- <EC2_INSTANCE_ID> tag has been deprecated. Please refer to
<CLOUD_RESOURCE_ID> tag for the same information //-->
       <EC2_INSTANCE_ID><![CDATA[i-06c788ce177fad52b]]></EC2_INSTANCE_ID>
        <OS><![CDATA[Amazon Linux 2018.03]]></OS>
        <QG_HOSTID><![CDATA[a6382021-3de0-47de-83e0-
47a380a03948]]></QG_HOSTID>
        <METADATA>
          <EC2>
            <ATTRIBUTE>
              <NAME><![CDATA[firstDiscovered]]></NAME>
              <LAST_STATUS>Success</LAST_STATUS>
              <VALUE><![CDATA[1588156107000]]></VALUE>
              <LAST_SUCCESS_DATE>2020-06-30T00:00:00Z</LAST_SUCCESS_DATE>
              <LAST_ERROR_DATE></LAST_ERROR_DATE>
              <LAST_ERROR><![CDATA[]]></LAST_ERROR>
            </ATTRIBUTE>
          </EC2>
        </METADATA>
      </HOST>
    </HOST_LIST>
  </RESPONSE>
</HOST_LIST_OUTPUT>
```

MS SQL Authentication Now Supported for Unix

APIs affected	/api/2.0/fo/auth/ms_sql/ with action=create|update
New or Updated API	Updated
DTD or XSD changes	No
APIs affected	/api/2.0/fo/auth/ms_sql/ with action=list
New or Updated API	Updated
DTD or XSD changes	Yes

We're expanding MS SQL Server authentication support to allow authentication to MS SQL Server database accounts on Unix hosts. We already support this type of authentication on Windows hosts. We added a new input parameter when creating and updating MS SQL authentication records to identify the OS authentication type (windows or unix) and new inputs for specifying the Unix instance directory path and Unix configuration file path.

Good to Know

- We support these MS SQL technologies for Unix: MS SQL 2017 and MS SQL 2019

- Certain input parameters for creating and updating MS SQL records only apply to the Windows OS type and do not apply to Unix OS type, including windows_domain, member_domain, kerberos, ntlmv2 and ntlmv1.

- The auto_discover_instances parameter is only supported for Windows, however the auto_discover_databases and auto_discover_ports parameters are supported for both Windows and Unix. For auto discovery on Windows, you'll also need a Windows authentication record for the host running the database. For auto discovery on Unix, you'll also need a Unix authentication record for the host running the database.

Create/Update MS SQL Record

New and updated parameters are listed below. Refer to the Qualys API (VM,PC) User Guide for details on all the input parameters available for the MS SQL record type.

Parameter	Description
db_local={0|**1**}	(Optional to create or update record) Set to 1 when login credentials are for a MS SQL Server database account (for Windows or Unix). Set to 0 when login credentials are for a Microsoft Windows operating system account that is associated with a MS SQL Server database account. For create record, if the db_local parameter is unspecified, the flag is set to 1.
auth_os_type={unix|windows}	(Optional when db_local=1) Specify "unix" when the OS type is Unix and "windows" when the OS type is Windows.

mssql_unix_insta_path={value}	(Optional when auth_os_type=unix) Specify the path to the MS SQL Server instance directory on Unix hosts. Sample value: /var/opt/mssql
mssql_unix_conf_path={value}	(Optional when auth_os_type=unix) Specify the path to the MS SQL Server configuration file on Unix hosts. Sample value: /var/opt/mssql/mssq.conf
instance={value}	(Optional to create or update record for Windows, Required to create record for Unix and Optional to update record for Unix) The name of the database instance to be scanned. This is the instance name assigned to the TCP/IP port. Important: This is not the host name that is assigned to the MS SQL Server instance name (see "MS SQL Server Instance Name" in the Qualys online help for information). The instance name may include a maximum of 128 characters (ascii). If the instance parameter is not specified for Windows, the instance name is set to "MSSQLSERVER". These parameters are mutually exclusive: instance and auto_discover_instances=1.
auto_discover_instances={**0**|1}	(Optional when auth_os_type=windows) Set auto_discover_instances=1 and we'll find all MS SQL Server instance names on each Windows host. Note that Windows authentication is required in order for us to auto discover instance names. Set up Windows authentication records for the hosts running MS SQL Servers. These parameters are mutually exclusive: instance and auto_discover_instances=1.
database={value}	(Optional to create or update record) The database name of the database to be scanned. The database name may contain a maximum of 128 characters. For a create request, if the database name is unspecified, the database name is set to "master".
auto_discover_databases={**0**|1}	Set auto_discover_databases=1 and we'll find all MS SQL Server database names on each host. These parameters are mutually exclusive: database and auto_discover_databases=1.

port={value}	(Required to create record, optional to update record) The port number assigned to the database instance to be scanned. To create a record you must specify one of these parameters: port or auto_discover_ports=1. These parameters are mutually exclusive.
auto_discover_ports={**0**|1}	Set auto_discover_ports=1 and for each host we'll find all ports MS SQL Server is running on. Note that Unix/Windows authentication is required for us to auto discover ports. Set up Unix/Windows authentication records for your hosts running MS SQL Server. To create a record you must specify one of these parameters: port or auto_discover_ports=1. These parameters are mutually exclusive.

Sample Create MS SQL Record

In this sample, we are creating a new MS SQL record for Unix.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=create&title=MSSQL_UNIX&username=root&password=root&db_local=1&ip
s=10.10.10.10&auto_discover_ports=1&auto_discover_databases=1&auth_os_typ
e=unix&instance=mssql&mssql_unix_conf_path=/var/opt/mssql/mssql.conf&mssq
l_unix_insta_path=/var/opt/mssql"
"https://qualysapi.qualys.com/api/2.0/fo/auth/ms_sql/"
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
 <RESPONSE>
   <DATETIME>2021-05-17T08:26:31Z</DATETIME>
   <BATCH_LIST>
     <BATCH>
       <TEXT>Successfully Created</TEXT>
       <ID_SET>
         <ID>103473</ID>
       </ID_SET>
     </BATCH>
   </BATCH_LIST>
 </RESPONSE>
</BATCH_RETURN>
```

Sample Update MS SQL Record

In this sample, we are updating a MS SQL record for Unix.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=update&ids=103474&username=root&password=root&db_local=1&auth_os_
type=unix&instance=MSSQLSERVER&mssql_unix_conf_path=/mssql/rd.conf&mssql_
unix_insta_path=/mssql/update"
"https://qualysapi.qualys.com/api/2.0/fo/auth/ms_sql/"
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2021-05-17T09:31:51Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>103474</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

List MS SQL Records

When you list MS SQL records, you'll see new Unix parameters in the response.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list&ids=103474"
"https://qualysapi.qualys.com/api/2.0/fo/auth/ms_sql/"
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MS_SQL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/ms_sql/auth_ms_sql_list_out
put.dtd">
<AUTH_MS_SQL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-05-17T09:48:22Z</DATETIME>
```

```
    <AUTH_MS_SQL_LIST>
      <AUTH_MS_SQL>
        <ID>103474</ID>
        <TITLE><![CDATA[MSSQL_UNIX]]></TITLE>
        <USERNAME><![CDATA[root]]></USERNAME>
        <NTLM_V1>0</NTLM_V1>
        <NTLM_V2>0</NTLM_V2>
        <KERBEROS>0</KERBEROS>
        <AUTO_DISCOVER_INSTANCES>0</AUTO_DISCOVER_INSTANCES>
        <AUTO_DISCOVER_DATABASES>1</AUTO_DISCOVER_DATABASES>
        <AUTO_DISCOVER_PORTS>1</AUTO_DISCOVER_PORTS>
        <DB_LOCAL>1</DB_LOCAL>
        <AUTH_OS_TYPE><![CDATA[unix]]></AUTH_OS_TYPE>

<UNIX_CONF_PATH><![CDATA[/var/opt/mssql/mssql.conf]]></UNIX_CONF_PATH>
        <UNIX_INSTA_PATH><![CDATA[/var/opt/mssql]]></UNIX_INSTA_PATH>
        <IP_SET>
          <IP_RANGE>10.10.10.10-10.10.10.11</IP_RANGE>
        </IP_SET>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2021-05-17T08:34:08Z</DATETIME>
          <BY>joe_user</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2021-05-17T09:40:39Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_MS_SQL>
    </AUTH_MS_SQL_LIST>
  </RESPONSE>
</AUTH_MS_SQL_LIST_OUTPUT>
```

DTD update:

DTD: <platform>/api/2.0/fo/auth/ms_sql/auth_ms_sql_list_output.dtd

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

<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
```

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

<!ELEMENT RESPONSE (DATETIME, (AUTH_MS_SQL_LIST|ID_SET)?, WARNING_LIST?,
GLOSSARY?)>
<!ELEMENT AUTH_MS_SQL_LIST (AUTH_MS_SQL+)>

<!-- If DB_LOCAL=1 then WINDOWS_DOMAIN cannot be set -->
<!ELEMENT AUTH_MS_SQL (ID, TITLE, USERNAME, NTLM_V1?, NTLM_V2?, KERBEROS?,
(INSTANCE | AUTO_DISCOVER_INSTANCES), (DATABASE |
AUTO_DISCOVER_DATABASES), (PORT|AUTO_DISCOVER_PORTS), DB_LOCAL,
AUTH_OS_TYPE?, UNIX_CONF_PATH?, UNIX_INSTA_PATH?, WINDOWS_DOMAIN?,
(IP_SET|MEMBER_DOMAIN), NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT NTLM_V1 (#PCDATA)>
<!ELEMENT NTLM_V2 (#PCDATA)>
<!ELEMENT KERBEROS (#PCDATA)>
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT DATABASE (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT DB_LOCAL (#PCDATA)>
<!ELEMENT AUTH_OS_TYPE (#PCDATA)>
<!ELEMENT UNIX_CONF_PATH (#PCDATA)>
<!ELEMENT UNIX_INSTA_PATH (#PCDATA)>
<!ELEMENT WINDOWS_DOMAIN (#PCDATA)>
<!ELEMENT AUTO_DISCOVER_INSTANCES (#PCDATA)>
<!ELEMENT AUTO_DISCOVER_DATABASES (#PCDATA)>
<!ELEMENT AUTO_DISCOVER_PORTS (#PCDATA)>

...
```

Issues Addressed

- In Qualys 10.10, we added 3 fields (Hostname, Domain and FQDN) to the CSV and CEF formats of the Host List Detection API output in error. In Qualys 10.12, we are reverting these changes and will remove the additional fields from the CSV and CEF formats.
- Fixed an issue that resulted in an error when trying to add a Netblock with a single IP through the API. This is now consistent with the UI and you can add Netblock with single IP through both, UI and API.
- Fixed an issue where the Compliance List API was converting special characters to plain text in XML format. Previously, for tag name, the API returned "<TAG_NAME>C&S Windows 2019</TAG_NAME>". With this release, the tag name will be returned in CDATA tag as follows:

  <TAG_NAME>
  <![CDATA[C&S Windows 2019]]>
  </TAG_NAME>
- Fixed an issue where the Compliance Posture Info API did not list IP-specific response when the IP filter was used in the API call.
- We discovered an issue where the "os" instance was not displayed in the Posture Info API output. This is now fixed.
- We made a correction to the tracking_method parameter description in the API User Guide for IP List endpoint.