Qualys Integration with Azure Sentinel

API User Guide

August 04, 2021

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

About this guide

Welcome to Qualys Cloud Platform and integration of Qualys Cloud Platform with Azure Sentinel! We'll help you get acquainted with the Qualys solutions for integrating Azure Sentinel with the Qualys Cloud Security Platform.

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

Qualys Support

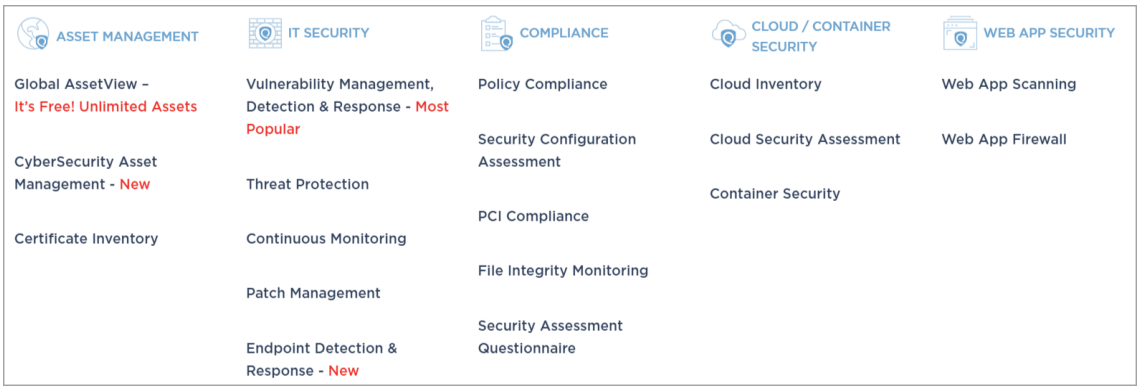
Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/

Introduction

Welcome to Qualys Cloud Platform that brings you solutions for securing your Cloud IT Infrastructure as well as your traditional IT infrastructure. In this guide, we'll be talking about integrating Qualys findings with Microsoft Azure Sentinel that you can further use in security analytics of your entire enterprise.

Qualys Integrated Security Platform

With Qualys Cloud Platform you get a single view of your security and compliance - in real time. If you're new to Qualys we recommend you to visit the Qualys Cloud Platform web page to know more about our cloud platform.



Qualys Support for Azure Sentinel

Azure Sentinel provides intelligent security analytics at cloud scale for entire enterprise. Azure Sentinel makes it easy to collect security data across entire hybrid organization from devices, to users, to apps, to servers on any cloud.

You can now access Qualys vulnerability assessment findings in Azure Sentinel. The Azure Sentinel provides a comprehensive view of the high-priority security alerts and compliance status across their accounts. By integrating the findings from Qualys Vulnerability Management (VM/VMDR) with Azure Sentinel, you can get near real-time, up-to-date visibility of your security posture in Azure Sentinel console. These findings, gained by the correlation of Qualys information with other data in Azure Sentinel, allow customers to quickly detect risks and take rapid, automated remedial actions.

Currently, we support findings from only VM/VMDR app in Azure Sentinel integration.

Qualys Sensors

Qualys sensors, a core service of the Qualys Cloud Platform, make it easy to extend your security throughout your global enterprise. These sensors are remotely deployable, centrally managed and self updating. They collect the data and automatically transmit it up to the Qualys Cloud Platform, which has the computing power to continuously analyze and correlate the information in order to help you identify threats and eliminate vulnerabilities.

Virtual Scanner Appliances
Remote scan across your networks - hosts and applications

Cloud Agents
Continuous security view and platform for additional security

Azure Cloud Connectors
Sync cloud instances and its metadata

Internet Scanners
Perimeter scan for edge facing IPs and URLs

Web Application Firewalls
Actively defend intrusions and secure applications

Pre-requisites

These options must be enabled for your Qualys user account.

- Qualys Applications: Vulnerability Management (VM/VMDR), Cloud Agent (CA). Ensure that you have executed scans and the scan reports (including vulnerability information) are available in your user account.

- Qualys Sensors: Virtual Scanner Appliances or Cloud Agents, as required

- Ensure API Access permission is enabled for the user account

- Manager or Unit Manager role

- Ensure that you have created Log Analytics Workspace on Azure Sentinel console.

- Ensure that you create an AWS account and provide access to Qualys.

- Ensure that you have accepted all the Qualys terms and conditions, raise CRM, and reach out to the Qualys Support team for the integration process.

It's easy to get started

You might already be familiar with Qualys Cloud Suite, its features and user interface. If you're new to Qualys, we recommend these overview tutorials - it just takes a few minutes!

Video Tutorials get you familiar with basics

Vulnerability Management Detection and Response. (3 mins)

Quick Steps: Integrating Azure Sentinel with Qualys

Here's the user flow for integrating Qualys with Azure Sentinel.

1 - Getting Started with Azure Sentinel Integration.

2 - Configuring Integration with Qualys using APIs available to configure integration with Qualys Cloud Platform.

3 - Configuring Insights on Azure Sentinel Console (Optional).

Helpful resources Always up to date with the information you need

From the Community

Qualys Training | Free self paced classes, video series, online classes

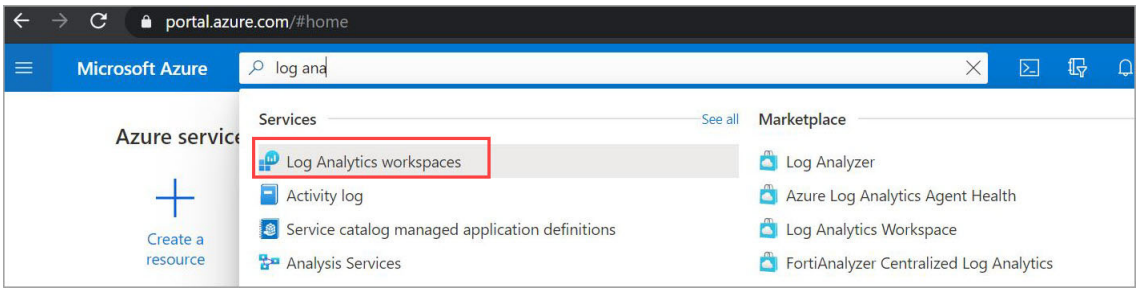
Qualys Documentation | Getting started guides, quick references, API docs

Getting Started with Azure Sentinel Integration

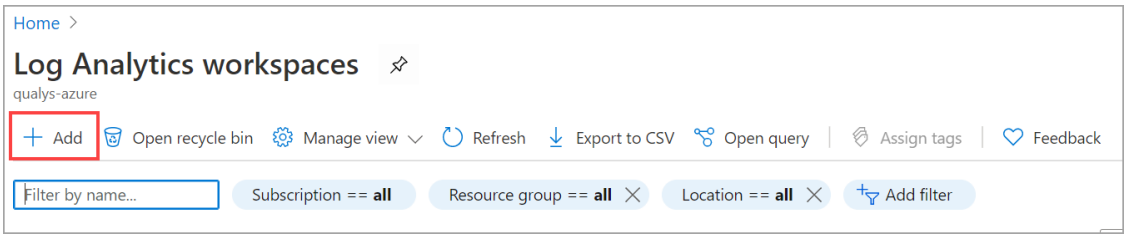
Just create a workspace on Azure Sentinel console. Once you create a workspace, you can use the workspace details such as workspace Id and primary key during integration. We'll walk you through the steps.

Creating Workspace

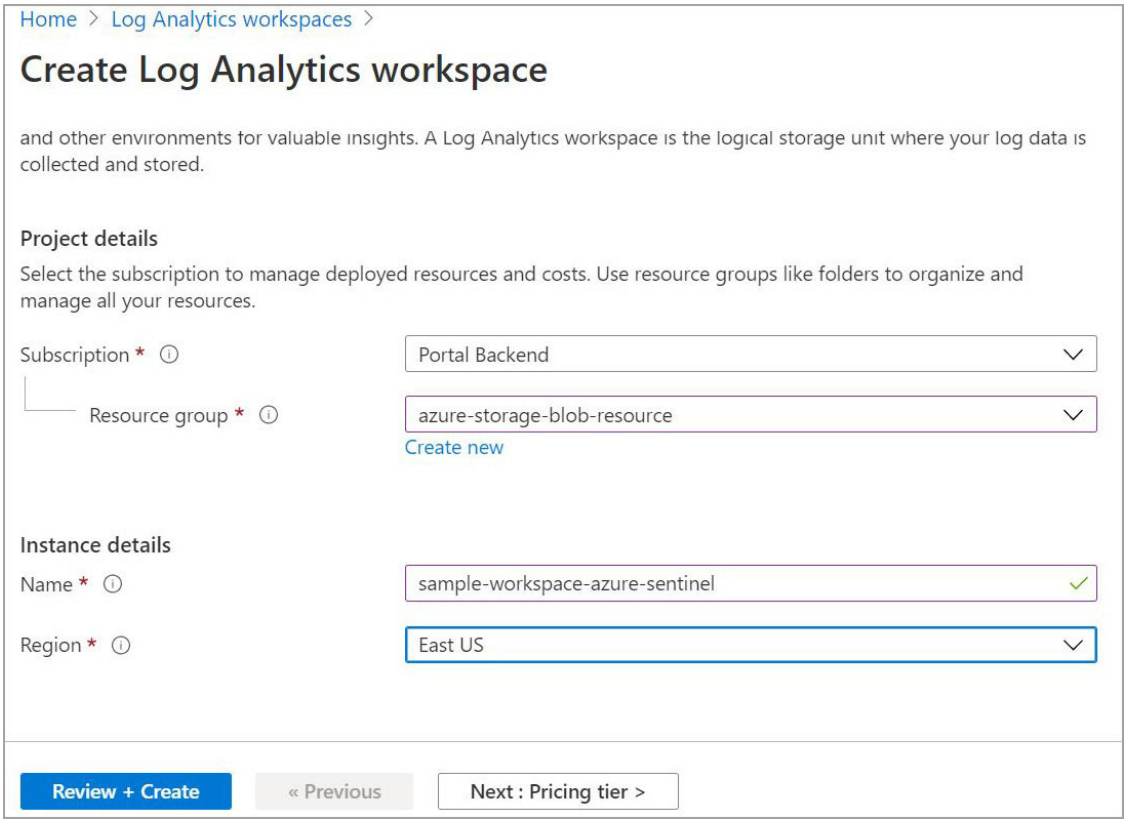
1. Login to Azure portal (https://portal.azure.com/) and search for Log Analytics workspaces in the search bar.



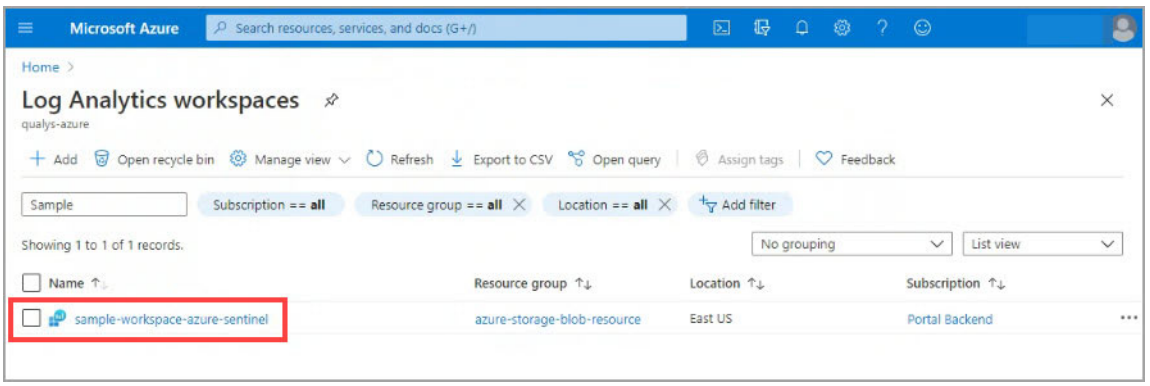
2. Click **Add** to create new Log Analytics workspace.



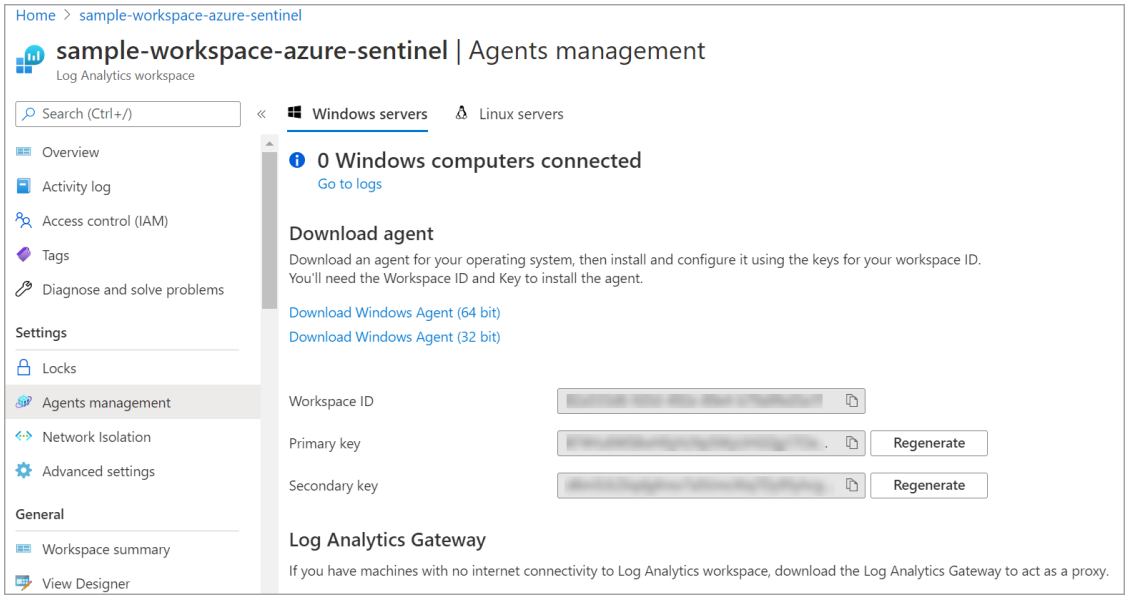
3.Provide the relevant details such as subscription, resource group, instance details and so on. Click **Review+Create** to create the workspace..



4. Once workspace is created, go to Log analytics workspaces and search for your workspace. Click the workspace to open.



5. Go to **Agents Management** and locate workspace ID and primary key to be used for Azure Sentinel Integration with Qualys.



Configuring Integration with Qualys

We provide APIs (JSON) to fasten and simplify the integration process with Azure Sentinel. The integration process is a single step with Qualys using APIs: adding the Azure Sentinel integration. Once you add it, you can use it to fetch details, update the existing configuration of Azure Sentinel, or delete the Azure Sentinel integration as well.

Add Azure Sentinel Integration

Update Azure Sentinel Integration

Get Details of the Azure Sentinel Integration

Delete Azure Sentinel Integration Details

URL to the Qualys API Server

Before you proceed with the APIs, you need to know the Qualys API Server. 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 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 Qualys API Server and URL for your account.

Add Azure Sentinel Integration

<Qualys_API_URL>/qps/rest/2.0/add/integration/azure/sentinel/vm

[POST]

The first step towards the integration is creation of Azure Sentinel integration. To add the Azure Sentinel integration, you need to provide workspace Id, primary key in the API request body. The workspace Id and primary key can be obtained from Azure workspace that you create. You can specify other optional parameters (base category, minimum severity, etc) as per your requirement.

Once you create the Azure Sentinel integration, the response provides an unique integration identifier (id) for the Azure Sentinel integration.

Input Parameters

Parameter	Description
workspaceId={value}	(Required) Provide the unique Id assigned to the workspace in Azure Sentinel.
primaryKey={value}	(Required) Provide the primary key Id assigned to the workspace in Azure Sentinel.
name={value}	(Required) Provide a unique name for the integration in the API request. The maximum length allowed for name is 50 characters.
baseCategory={IG|Potential|Confirmed}	Category of the vulnerabilities fetched from Qualys (VM/VMDR app) to be posted on the Azure Sentinel. The valid values are IG, Confirmed, and Potential. By default, it is configured to Confirmed. In this case, only confirmed vulnerabilities are included. If you configure the baseCategory as Potential, both Potential and Confirmed vulnerabilities are included.If you configure the baseCategory as IG, all three categories: IG, Potential and Confirmed vulnerabilities are included.
customLogName={value}	Provide a unique name for the data collector APIs. You can identify the log details with the name you provide. If you do not provide a custom log name, we use QUALYS_SECURITY_VM_FINDINGS by default. **Note**: The custom log name can only contain letters, numbers, and underscore (_), and should not exceed 100 characters.
minSeverity={value}	The minimum severity level of the vulnerabilities fetched from Qualys (VM/VMDR app) to be posted on the Azure Sentinel. By default, it is configured to severity level 3 and above. For example, if you set the value to 1, all findings with severity level 1 to 5 are fetched and available on Azure Sentinel.
resultSectionNeeded={true|false}	Set this to true to include the result section in the response. If you want to exclude the result section, set this parameter to false. By default, the resultSectionNeeded parameter is configured to false.
apiVersion={value}	Azure Sentinel data collector API version. By default, 2016-04-01 API version is used. Click here for information on supported API versions.

Add Azure Sentinel Integration

API request:

```
curl -u 'username:password' -X POST --header 'Content-
Type:application/json'
'https://qualysapi.qualys.com/qps/rest/2.0/add/integration/azure/sentinel
/vm' --data '@integration.json'
```

Note: “integration.json” contains the request POST data.

<u>Request POST Data (integration.json):</u>

```
{
  "workspaceId": "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
  "primaryKey":
"XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXX",
  "minSeverity": 4,
  "baseCategory": "Potential",
  "customLogName": "QUALYS_FINDINGS",
  "name": "Sample Integration",
  "resultSectionNeeded": false,
  "apiVersion": "2016-04-01"
}
```

<u>JSON output:</u>

```
{
    "ServiceResponse": {
        "data": [
            "integrationId=68"
        ],
        "count": 1,
        "responseCode": "SUCCESS"
    }
}
```

Update Azure Sentinel Integration

<Qualys_API_URL>/qps/rest/2.0/update/integration/azure/sentinel/{integrationId}/vm [PUT]

Once you add the Azure Sentinel integration, you can update the name, minSeverity, baseCategory, resultSectionNeeded, apiVersion of the Azure Sentinel integration with Qualys.

Input Parameters

Parameter	Description
integrationId={value}	Provide the unique Id assigned of Azure Sentinel integration.
workspaceId={value}	Provide the unique Id assigned to the workspace in Azure Sentinel.
primaryKey={value}	Provide the primary key Id assigned to the workspace in Azure Sentinel.
name={value}	Provide a unique name for the integration in the API request. The maximum length allowed for name is 50 characters.
baseCategory={IG|Potential|Confirmed}	Category of the vulnerabilities fetched from Qualys (VM/VMDR app) to be posted on the Azure Sentinel. The valid values are IG, Confirmed, and Potential. By default, it is configured to Confirmed. In this case, only confirmed vulnerabilities are included. If you configure the baseCategory as Potential, both Potential and Confirmed vulnerabilities are included.If you configure the baseCategory as IG, all three categories: IG, Potential and Confirmed vulnerabilities are included.
customLogName={value}	Provide a unique name for the data collector APIs. You can identify the log details with the name you provide. If you do not provide a custom log name, we use QUALYS_SECURITY_VM_FINDINGS by default. **Note**: The custom log name can only contain letters, numbers, and underscore (_), and should not exceed 100 characters.
minSeverity={value}	The minimum severity level of the vulnerabilities fetched from Qualys (VM/VMDR app) to be posted on the Azure Sentinel. By default, it is configured to severity level 3 and above. For example, if you set the value to 1, all findings with severity level 1 to 5 are fetched and available on Azure Sentinel.
resultSectionNeeded={true|false}	Set this to true to include the result section in the response. If you want to exclude the result section, set this parameter to false. By default, the resultSectionNeeded is configured to false.
apiVersion={value}	Azure Sentinel data collector API version. By default, 2016-04-01 version is used. Click here for information on supported API versions.

Update Azure Sentinel Integration details.

Let us now see an example to update the configuration details of the Azure Sentinel integration. Provide the configuration details to be updated in the PUT request.

API request:

```
curl -u 'username:password' -X PUT --header 'Content-
Type:application/json'
'https://qualysapi.qualys.com/qps/rest/2.0/update/integration/azure/senti
nel/{integrationId}/vm' --data '@integration.json'
```

Note: “integration.json” contains the request PUT data.

Request PUT Data (integration.json):

```
{
  "workspaceId": "XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
  "primaryKey":
"XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
  "minSeverity": 4,
  "baseCategory": "Potential",
  "customLogName": "CUSTOM_LOG",
  "name": "Sample Name change",
  "resultSectionNeeded": false,
  "apiVersion": "2016-04-01"
}
```

JSON output:

```
{
    "ServiceResponse": {
        "data": [
            "Azure Sentinel integration successfully updated."
        ],
        "responseCode": "SUCCESS",
        "count": 1
    }
}
```

Get Details of the Azure Sentinel Integration

<Qualys_API_URL>/qps/rest/2.0/get/integration/azure/sentinel/{integrationId}/vm [GET]

<Qualys_API_URL>/qps/rest/2.0/get/integration/azure/sentinel/vm [GET]

When you want to get details of a particular Azure Sentinel integration, you can fetch the configuration and integration details using the unique integration identifier (id) of the Azure Sentinel integration. You can fetch the configuration and integration details with or without the unique integration identifier (id) of the Azure Sentinel integration.

Currently, you can only fetch details for the VM/VMDR app.

Get integration details of the Azure Sentinel integration

Let us now see an example to fetch the integration details of Azure Sentinel integration.

API request:

```
curl -u 'username:password' -X GET
'https://qualysapi.qualys.com/qps/rest/2.0/get/integration/azure/sentinel
/{integrationId}/vm'
OR
```

Note: If you are not aware of the integration ID, use the following request to fetch details without integration Id

```
curl -u 'username:password' -X GET
```

```
'https://qualysapi.qualys.com/qps/rest/2.0/get/integration/azure/sentinel
/vm'
```

JSON output:

```
{
    "ServiceResponse": {
        "data": [
            "{integrationId=68,
            name='Sample Integration',
            customerId=123456,
            customerUUID='a48f05df-ff6f-704e-83ba-c0692b0a64f9',
            workspaceId='XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX',
            minSeverity=3,
            baseCategory=IG,
            customLogName='Test',
            apiVersion='2016-04-01',
            resultSectionNeeded=true}"
        ],
        "count": 1,
        "responseCode": "SUCCESS"
    }
}
```

Delete Azure Sentinel Integration Details

<Qualys_API_URL>/qps/rest/2.0/delete/integration/azure/sentinel/{integrationId}/vm [DELETE]

For an Azure Sentinel integration, you could delete the integration using the unique identifier associated with the integration.

Delete the Azure Sentinel integration

API request:

```
curl -u 'username:password' -X DELETE
'https://qualysapi.qualys.com/qps/rest/2.0/delete/integration/azure/senti
nel/{integrationId}/vm '
```

where, integrationId is the unique integration identifier of the Azure Sentinel

JSON output:

```
{
    "ServiceResponse": {
        "data": [
            "Azure Sentinel integration successfully deleted."
        ],
        "count": 1,
        "responseCode": "SUCCESS"
    }
}
```

Findings and Insights

Let us the see the detailed steps for viewing findings and insights on Azure Sentinel console.

View Findings on Azure Sentinel Console

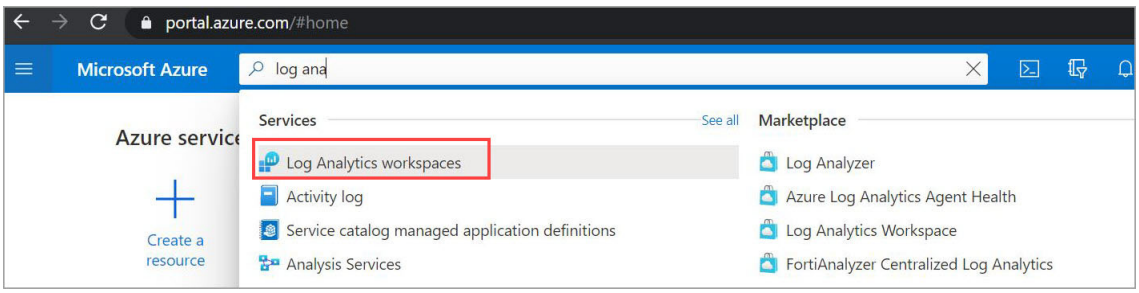
Troubleshooting Tips

View Findings on Azure Sentinel Console

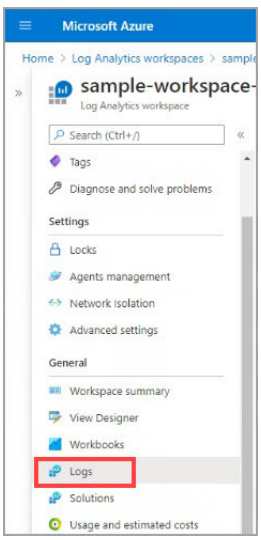
Before you view findings on Azure Sentinel console, ensure that you have met the pre-requisites, completed all the configurations with Azure and Qualys, and have findings available in your Qualys subscription.

Let us the see the detailed steps to view the findings.

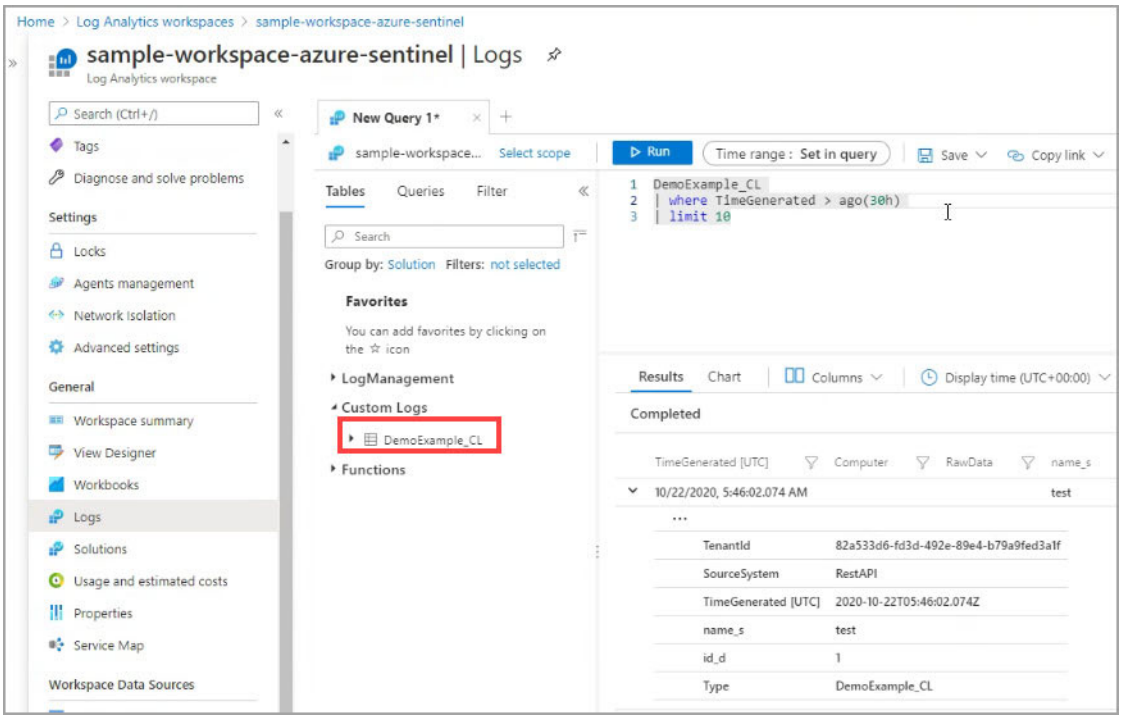
1 - Login to Azure portal (https://portal.azure.com/) and search for Log Analytics workspaces in the search bar.



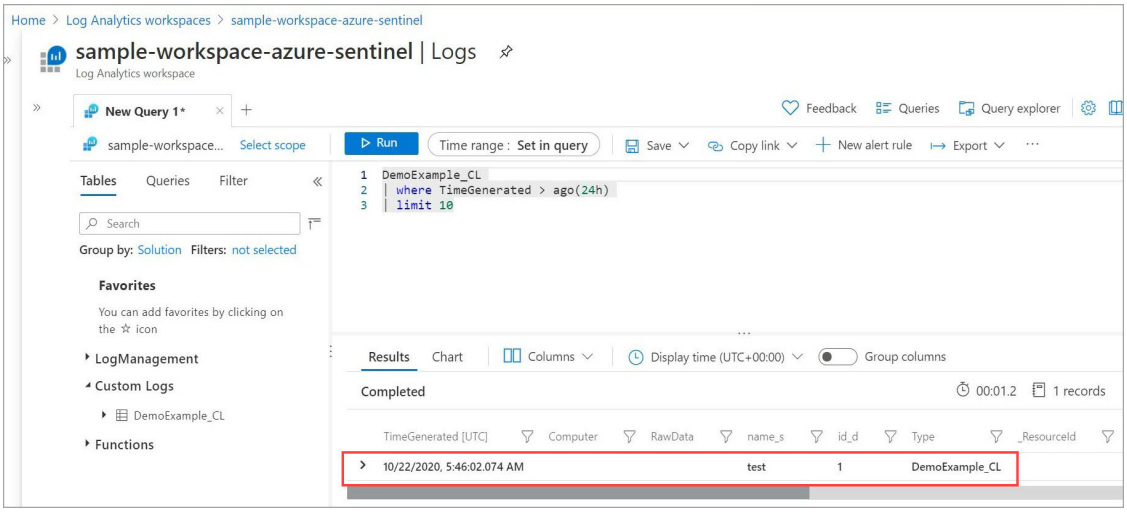
2 - Locate the workspace you associated with the integration. In the worskpace, navigate to the logs section.



The Log Management section displays the default logs. If you have provided customized log name during the integration, navigate to the custom log section.



By default, we use QUALYS_SECURITY_VM_FINDINGS as the custom log name. You can view the logs in the table. CL is appended to the custom log name you provide. For example, if DemoExample is the custom log name, the table name would be DemoExample_CL.



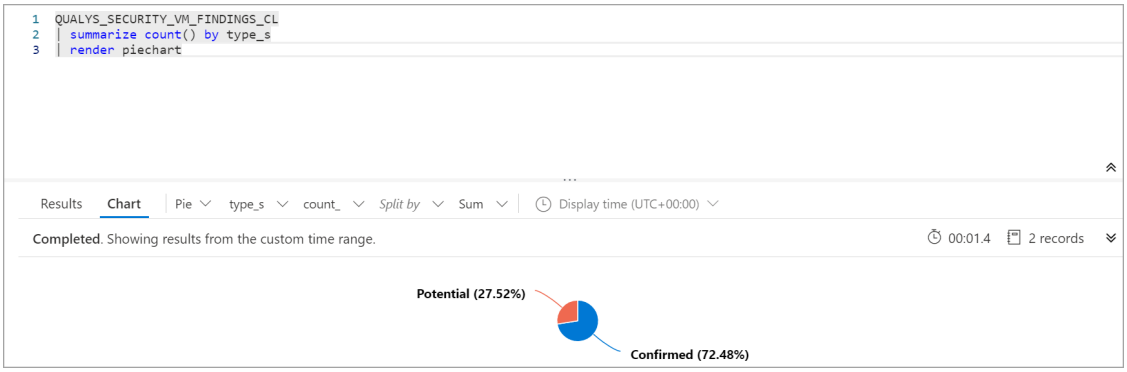
There are multiple ways in which you could visualize the findings in Azure Sentinel. Let us see few examples of the same.

Get count of vulnerabilities by type (confirmed/potential)

QUALYS_SECURITY_VM_FINDINGS_CL

| summarize count() by type_s

| render piechart



Get count of Patchable and Exploitable Vulnarabilities with Severity 3 and more, per asset

QUALYS_SECURITY_VM_FINDINGS_CL

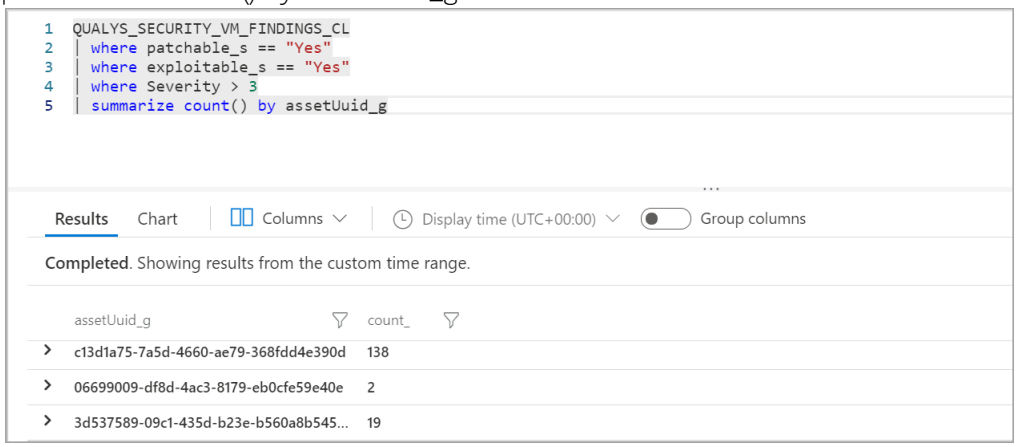
| where TimeGenerated > ago(24h)

| where patchable_s == "Yes"

| where exploitable_s == "Yes"

| where Severity > 3

| summarize count() by assetUuid_g



Troubleshooting Tips

Let us see scenarios that will help you debug the common issues.

Scenario: Qualys Findings not visible in Qualys subscription

Workaround: To view Qualys findings in your subscription ensure the following:

- Qualys sensors are deployed on the endpoints
- Vulnerability scans are conducted

Scenario: Qualys Findings not visible on Azure Sentinel console

Workaround: To view Qualys findings on Azure Sentinel console ensure the following:

- Qualys sensors are deployed on the endpoints
- Vulnerability assessment and findings are available in your Qualys subscription
- Integration configuration with Qualys and Azure Sentinel console is complete

For any such issues related to Azure Sentinel Integration with Qualys, reach out to Qualys Support.