Qualys Integration with S3 Object Storage

User Guide

June 25, 2024

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 the integration of Qualys Cloud Platform with S3 Object Storage! This guide will help you get acquainted with the Qualys solutions for integrating S3 Object Storage with Qualys Cloud 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 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 online 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.

On Qualys Cloud Platform, you can view and retrieve vulnerability findings using multiple methods such as interactive dashboards, reports, and APIs.

An S3 Object Storage is any On-prem or cloud storage service which supports S3 protocol and is authenticated by the following parameters:

- Access key
- Secret key
- Certificate required to connect to S3 server

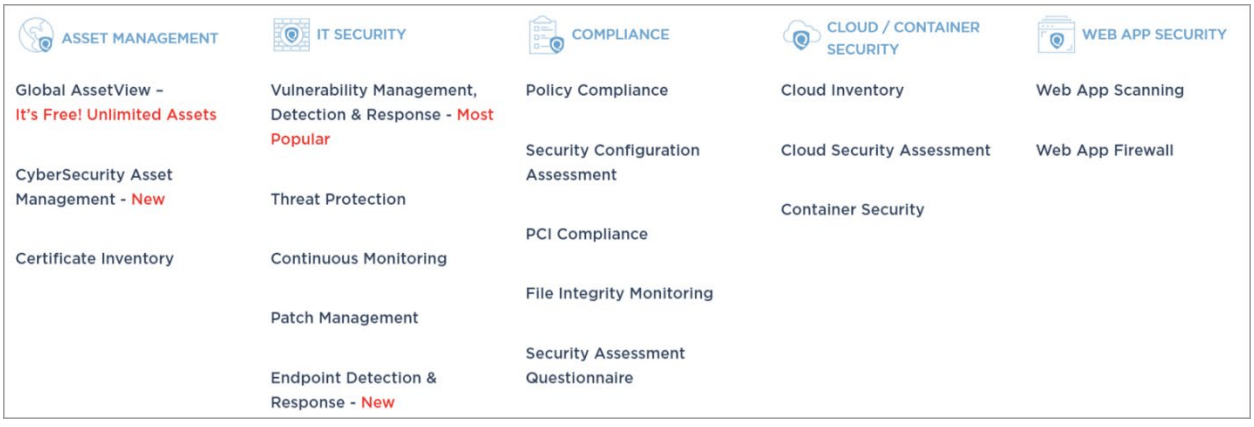
By integrating with S3 Object Storage, you get the data of your asset inventory directly on your S3 Object Storage bucket in near real-time, without having to run any API calls or generate any reports. CIPS (Cloud Integration Partner Service) proactively retrieves the data from Qualys Cloud Platform and transfers it to the S3 Object Storage Bucket.

With the S3 Object Storage integration, you get a near real-time and up-to-date visibility of your security in your storage console. You can then use this data in correlation with other data in your cloud storage to know your exact security posture and take rapid remedial actions.

In this guide, you will find information about integrating Qualys findings with S3 Object Storage using CIPS (Cloud Integration Partner Service), so that you can use the findings further in your enterprise.

Qualys Integrated Security Platform

With Qualys Cloud Platform you get a single view of your security- in near real time. If you are new to Qualys, you can visit the Qualys Cloud Platform web page to know more about the platform.



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 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

AWS 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

Qualys Support for S3 Object Storage

You can now integrate with S3 Object Storage-based cloud, which is an object storage service. The service provides high scalability, data availability, security, and performance.

You can now access Qualys vulnerability assessment findings data in the S3 Object Storage Bucket. By integrating the findings from Qualys Vulnerability Management (VM/VMDR) with S3 Object Storage, you can get near real-time and up-to-date visibility of your security on the S3 Object Storage console. These findings, gained by the correlation of Qualys information with other data in S3 Object Storage, allow you to quickly detect risks and take rapid and automated remedial actions.

Currently, Qualys supports findings from only VM/VMDR for S3 Object Storage integration.

Benefits

You get the following benefits on integrating with S3 Object Storage Bucket for VM/VMDR data:

- Instantaneous and near real-time transfer of vulnerability and posture data to your preferred storage platform
- Automatic transfer of data to your storage platform without having to make any API calls. This eliminates the process of pulling large data from Qualys Cloud Platform using APIs.
- Easy and seamless postprocessing as the data is transferred in JSON format
- Flexibility to use this feature alongside the Qualys API services

Configure a S3 Object Storage Integration

Integration for VM/VMDR

By integrating VM/VMDR with S3 Object Storage, you get the vulnerability findings for your asset inventory directly on your S3 Object Storage Bucket in near real time, without having to run any API calls or generate any reports.

The integration allows you to get a near real-time and up-to-date visibility of your security posture in your storage bucket and take rapid remedial actions.

Prerequisites

- Ensure that you accept all the Qualys Terms and Conditions. Reach out to the Qualys Support team for the integration process.
- **Qualys Applications**: You must have enabled Vulnerability Management (VM/VMDR) and Cloud Agent (CA) for your subscription. Ensure that you have executed scans and the scan reports (including vulnerability information) are available in your user account.
- **Qualys Sensors**: You must have Virtual Scanner Appliances or Cloud Agents, as required.
- **Permissions**: The API Access permission must be enabled for your account.
- **Role**: You must have the Manager or Unit Manager role

APIs for Creating and Managing the Integration

The following are the APIs for creating and managing the integration:

Note: Select the integration_type as s3-object-storage for the below APIs.

API	URL	Operator	Description
Generate a JWT Token	/auth	POST	Generates a new JWT token.
Register/Onboard Integration	/partner-integration/vm	POST	Registers an integration.
Update Integration	/partner-integration/vm/{integration_type}	PUT	Updates integration details such as bucket name, bucket region, accessKey,SecreteKey,StorageURL.etc. of the S3 Object Storage bucket with Qualys.
Get Details of an Integration	/partner-integration/vm/{integration_type}	GET	Gets details of a particular S3 Object Storage integration.

Add Certificate	/partner-integration/netapp/certificate	POST	Add certificate details of a NetApp Integration.
Get Certificate	/partner-integration/netapp/certificate	GET	Gets certificate details of a NetApp integration.
De-Register/Delete Integration	/partner-integration/vm/{integration_type}	DELETE	Removes a customer association by deleting the integration details or deregistering the customer.

URL to the Qualys API Server

Before you proceed with the APIs, you need to know the Qualys API gateway. The Qualys gateway URL you should use for API requests depends on the Qualys platform where your account is located.

Gateway base URLs for different Qualys pods can be found at:
https://www.qualys.com/platform-identification/

This document uses <qualys_gateway_url> in sample API requests. Replace this URL with the appropriate Qualys API gateway URL (for example, https://gateway.qg1.apps.qualys.com) for your account.

Generate a JWT Token

Generates a new JWT token for authentication.

URL	/auth
Operator	POST

API Request

```
curl -X POST
"<qualys_gateway_url>/auth"
-d "username=value1&password=passwordValue&token=true"
-H "ContentType: application/x-www-form-urlencoded"
```

Output

a JWT token

(Pass this token in the rest of the APIs for Authorization. It is valid for 4 hours once generated. Once it is expired, you have to regenerate it.)

Register/Onboard an Integration

Registers an integration.

URL	/partner-integration/vm
Operator	POST

Input Parameters

Parameter	Description
Name={value}	(Required) Provide a unique name for the integration in the API request. The maximum length allowed for the name is 50 characters.
integrationType={value}	(Required) Provide the inetgrationType as **"s3-object-storage**" for S3 Object Storage Integration.
accessKey={value}	(Required)Provide the accessKey of the S3 Object Storage bucket where the findings are to be sent.
secretKey={value}	(Required)Provide the secreteKey of the S3 Object Storage bucket where the findings are to be sent.
storageUrl={value}	(Required)Provide the Storage URL of the S3 Object Storage bucket.
bucket={value}	(Required)Provide the name of the S3 Object Storage bucket to which the findings are to be sent.
region={value}	(Required)Provide the region on which the S3 Object Storage bucket is hosted.
sendResultSection={true|false}	Set this to true to include the result section in the finding. If you want to exclude the result section, set this parameter to false. By default, the resultSectionNeeded parameter is configured to false.
sendVulnInfo ={true|false}	Set this to true if you need the vulnerability information. If you want to exclude the vulnerability information, set this parameter to false. By default, the sendVulnInfo parameter is configured to false.
compressData ={true|false}	Set this to true to compress the data in the response. It saves on disk and network IO. If you want to exclude the compression, set this parameter to false. By default, the compressData parameter is configured to true.
sendAlerts={true|false}	(Boolean) Set to true to receive ProActive alert

	notifications.
errorEmails=[“value”]	When sendAlerts is set to true, provide the email list for ProActive Alert notifications. Add upto a List of maximum 5 email addresses as comma-separated values.
filterQuery	Filter vulnerabilities and assets using the supported tokens.

Filter Query Tokens

The Qualy Query Language is used to build search queries and fetch information from the Qualys database. You can pick the tokens from our repository and build your own query to find the relevant information.

For example, the below query fetches assessments of a specified qid, discovers ignored vulnerabilities and searches from the specified range of dates.

```
"vuln" : "qId: 11547 ignored: true AND lastUpdate: [2023-07-06 .. 2023-07-07]"
```

The below query fetches information of a specified asset id within the provided IP range.

```
"asset" : "assetUuid: `151334c4-3811-40b5-ba92-cfd0064eb9f4` AND ip: (1.1.1.1
.. 5.5.5.5)"
```

Learn more about building search queries using the Qualys Query Language (QQL) here.

Note: The “Now” keyword is not supported for QQL currently. Building search queries with it will not produce any results.

The tokens listed below can be used to create the filterQuery for vulnerabilities and assets.

Vulnerbility Filter Tokens:

Token	Data Type
qid	LONG
port	LONG
ignored	BOOLEAN
Disabled	BOOLEAN
filterQuery	Optional
ssl	BOOLEAN
protocol	STRING
timesFound	LONG
status	STRING
firstFound	STRING

lastUpdate	STRING
lastProcessed	STRING
lastReopened	STRING
lastFixed	STRING
lastFound	STRING
lastTest	STRING

Asset Filter Tokens:

Token	Data Type
assetId	LONG
assetUuid	STRING
hostId	LONG
netBios	STRING
dns	STRING
ip	STRING
os	STRING
trackingMethod	STRING

API Request

```
curl -H 'Authorization: Bearer <token>''Content-Type:application/json'
  <qualys_gateway_url>/partner-integration/vm --data '@integration.json'
```

Note: "integration.json" contains the request POST data.

Request POST Data (integration.json)

```
{
   "name": "<Integration_name>",
   "integrationConfig": {
      "integrationType": "s3-object-storage",
      "accessKey": "<accesskey of the S3 Object Storage bucket>",
      "secretKey": "<secreteKey of the S3 Object Storage bucket>",
      "storageUrl": "<storageURL of the S3 Object Storage bucket>",
      "bucket": "<bucketName>",
      "region": "<region>"
   },
   "moduleConfig": {
      "sendResultSection": true,
      "sendVulnInfo": true,
      "compressData": true
   },
   "sendAlerts": true,
   "errorEmails": [
      "email address 1",
         "email address 2"
   ],
   "filterQuery": {
```

```
      "asset": "assetId: <assetID>",
      "vuln": "qid: <qId>"
   }
}
```

Output

```
{
    "integrationId": <integration ID>,
    "integrationValidated": false,
    "sendAlerts": true
}
```

Update an Integration

Updates the integration details such as bucket name, bucket region, secreteKey,accessKey,storageUrl, name, resultSectionNeeded, sendVulnInfo, compressData,etc. of the S3 Object Storage Integration with Qualys.

URL	/partner-integration/vm/{integration_type}
Operator	PUT

Input Parameters

Parameter	Description
Name={value}	(Required) Provide a unique name for the integration in the API request. The maximum length allowed for the name is 50 characters.
integrationType={value}	(Required) Provide the inetgrationType as "**s3-object-storage**" for S3 Object Storage Integration
accessKey={value}	(Required) Provide the accessKey of the S3 Object Storage bucket where the findings are to be sent
secretKey={value}	(Required) Provide the secreteKey of the S3 Object Storage bucket where the findings are to be sent
storageUrl={value}	(Required) Provide the Storage URL of the S3 Object Storage bucket
bucket={value}	(Required) Provide the name of the S3 Object Storage bucket to which the findings are to be sent
region={value}	(Required) Provide the region on which the S3 Object Storage bucket is hosted
sendResultSection={true|false}	Set this to true to include the result section in the finding. If you want to exclude the result section, set this parameter to false. By default, the resultSectionNeeded parameter is configured to false.
sendVulnInfo ={true|false}	Set this to true if you need the vulnerability information. If you want to exclude the vulnerability

	information, set this parameter to false. By default, the sendVulnInfo parameter is configured to false
compressData ={true|false}	Set this to true to compress the data in the response. It saves on disk and network IO. If you want to exclude the compression, set this parameter to false. By default, the compressData parameter is configured to true.
sendAlerts={true|false}	Boolean) Set to true to receive ProActive alert notifications.
errorEmails=[“value1”, “value2”]	When sendAlerts is set to true, provide the email list for ProActive Alert notifications. Add upto a List of maximum 5 email addresses as comma-separated values.

API Request

```
curl -X PUT
--header 'Content-Type:application/json'
'<qualys_gateway_url> /partner-integration/vm/{integration_type}'
--data '@integration.json'
-H "Authorization: Bearer <token>"
```

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

Request PUT Data (integration.json)

```
{
      "name": "<Integration_name>",
      "integrationConfig": {
         "integrationType": "s3-object-storage",
         "accessKey": "<accesskey of the S3 Object Storage bucket>",
         "secretKey": "<secreteKey of the S3 Object Storage bucket>",
         "storageUrl": "<storageURL of the S3 Object Storage bucket>",
         "bucket": "<bucketName>",
         "region": "<region>"
       },
      "moduleConfig": {
        "sendResultSection": true,
        "sendVulnInfo": true,
        "compressData": true
       },
      "sendAlerts": true,
      "errorEmails": [
         "email address 1",
         “email address 2”
        ],
      "filterQuery": {
      "asset": "assetId: <assetID>",
      "vuln": "qid: <qId>"
       }
```

```
}
```

Output

```
    {
      "message": "VM integration successfully updated."
    }
```

Get Details of an Integration

When you want to get details of a particular S3 Object Storage integration, you can fetch the configuration and integration details using the unique JWT token and Integration_type. You can fetch the configuration and integration details without the unique integration identifier (id) of the S3 Object Storage integration.

Note: Select the integration_type as **s3-object-storage**.

URL	/partner-integration/vm/{integration_type}
Operator	GET

API Request

```
curl -X GET
'<qualys_gateway_url>/partner-integration/vm/{integration_type}'
-H "Authorization: Bearer <token>"
```

Output

```
{
   "integrationId": <integration_id>,
   "name": "<integrationName>","customerId": <customerId>,
   "customerUUID": "<customerUUID>",
   "integrationValidated": false,
   "sendAlerts": false,
   "errorEmails": [
      "email address for proactive alerts"
   ],
   "integrationConfig": "<integration config details like
bucket,region,secretKey,accessKey,S3 Object Storage certificate,etc>",
   "filterQuery": "<filterQuery Details if provided while enabling the inetgration >",
   "moduleConfig": "VmIntegrationConfig(sendResultSection=true, sendVulnInfo=true,
compressData=true)"
}
```

Add Certificate

You need to add a valid NetApp certificate to validate the NetApp integration. Not adding the NetApp certificate may result in the integration not validating and not sending vulnerability information to the NetApp bucket.

Note: Select the integration_type as **s3-object-storage**.

URL	/partner-integration/netapp/certificate
Operator	POST

API Request:

```
curl -X POST '<qualys_gateway_URL>/partner integration/netapp/certificate'
 --header 'Authorization: Bearer <Token>'
 --form 'certificateFile=@"<path of the NetApp Certificate>"'
```

Output:

```
{
  "message": "<certificate Added while validating the integration>"
}
```

Get Certificate

You can get the NetApp certificate details with the GET certificate API.

Note: Select the integration_type as **s3-object-storage**.

URL	/partner-integration/netapp/certificate
Operator	POST

API Request:

```
curl -X GET '<qualys_gateway_URL>/partner-integration/netapp/certificate'
--header 'Authorization: Bearer <Token>'
```

Output:

```
{
  "message": "<certificate Added while validating the integration>"
}
```

De-Register/Delete an Integration

You can remove a customer association by deleting the integration details or deregistering the customer. You need to provide the integration_type with a JWT token to identify the integration to be deleted.
Note: Select the integration_type as **s3-object-storage**.

URL	/partner-integration/vm/{integration_type}
Operator	DELETE

API Request

```
curl -X DELETE '<qualys_gateway_url>/partner-integration/vm/s3-object-storage'\
--header 'Authorization: Bearer <Token>'
```

Output

```
{
  "messsage": "VM integration successfully deleted."
}
```

Findings and Insights

Let us the see the detailed steps for viewing findings and insights in the S3 Object Storage bucket.

View Findings on S3 Object Storage Bucket

Before you view findings in the S3 Object Storage bucket, ensure that you have met the pre-requisites, completed all the configurations with S3 Object Storage and Qualys, and have findings available in your Qualys subscription..

Troubleshooting Tips

The following scenarios help you debug the common issues:

Scenario	Workaround
Qualys Findings are not visible in Qualys subscription	To view Qualys findings in your subscription, ensure the following: • Qualys sensors are deployed on the endpoints. • Vulnerability scans are performed.
Qualys Findings are not visible on S3 Object Storage bucket.	To view Qualys findings on the S3 Object Storage bucket, ensure the following: • Qualys sensors are deployed on the endpoints. • Vulnerability assessment and findings are available in your Qualys subscription. • The integration configuration between Qualys and S3 Object Storage is complete.

For any such issues related to S3 Object Storage Integration with Qualys, reach out to Qualys Support.