

Qualys OCI Vulnerability Scanning Service BYOL

Onboarding Guide

March 13, 2023

Copyright 2023 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

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

Table of Contents

Introduction to OCI BYOL Support	;
Pre-requisites	:
Deploying Qualys Agent on OCI Platform	;
Generate Qualys Cloud Agent License Code	1
Create a Vault to Store the Qualys License Information	
Define a Secret for Scan Recipe	
Create a Scan Recipe for Host Instances	
Create a Target to Assign a Scan Recipe12	
Appendix A: Permissions and Policies	
Grant Access to the VSS Service	
Grant Permission to Group of Administrators to Access to VSS Service	
Set up the Policies and Dynamic Groups for VSS – Qualys BYOL14	

Introduction to OCI BYOL Support

BYOL is a Bring Your Own License. With this feature users can use Oracle Cloud Infrastructure (OCI) with their Own Qualys License. BYOL enables Qualys VM scanning for instances on OCI. OCI Vulnerability Scanning Service (VSS) is integrated with Qualys. VSS can set up Qualys Agent on OCI instances.

Users can configure a Qualys Agent based scan from the OCI console. Qualys agents collect the instances data and push it to Qualys VMDR where scanning is performed. The count of unique vulnerabilities out of the identified or detected vulnerability and then forward the result to VSS.

VSS displays the results in the VSS application and forwards the result to Cloud Guard for global alerting of security problems. Qualys VMDR, VSS and Cloud Guard provides the complete security posture of the instances.

Pre-requisites

For using BYOL feature, following are the pre-requisites:

- Ensure that Oracle has enabled the OCI BYOL features for your account. Oracle VSS is required for the functionality of this feature.
- Ensure VSS agent is installed.
- Set up policies:
 - Grant access to the VSS service.
 - Grant permission to group of administrators to access to VSS.

For more details on policies, refer to Appendix A.

Deploying Qualys Agent on OCI Platform

Users can create one scan recipe, one target and start viewing findings about their host (compute) instances. For implementing integration between the OCI platform and Qualys platform, follow these steps:

- 1. Generate Qualys Cloud Agent License Code
- 2. Create a Vault to Store the Qualys License Information
- 3. Define a Secret for Scan Recipe
- 4. Create a Scan Recipe for Host Instances
- 5. Create a Target to Assign a Scan Recipes

Generate Qualys Cloud Agent License Code

You need to generate the license code. To generate a license, you must generate a Cloud Agent Activation Key and enable OCI for the Qualys cloud agent. Perform these tasks using the Cloud Agent application.

Follow these steps to generate a license code:

- 1. Login to **Cloud Agent** (CA) application.
- 2. Navigate to **Agent Management** > **Activation Keys** (or go to the Activation Keys tab).
- 3. Select **New Key** to create a new activation key.

An activation key is used to install agents.

- 4. Select the activation key and click **Install Agent** from the **Actions** menu.
- 5. In the **Install Agents** screen, click **Install instructions** for the required agent > **Deploying in OCI Cloud.**

Install Agents x	2
You are ready to install the agent.	
Current agent version : 4.8.0.31 Hash-SHA-	
Deploying in Azure Cloud Deploying in OCI Cloud	
OCI BYOL Installation Requirements	
Active Oracle Cloud account	
Steps to Install the OCI BYOL Agent	
Qualys agent deployment is integrated into OCI partner solutions for vulnerability assessment, follow the below steps to get started.	t
1. Login into the OCI portal.	
Navigate to Identity & Security -> Scanning -> Scan Recipes.	
3. Create a new Scan Recipe.	
a. Enable agent based scanning.	
 Select Qualys Agent as the agent to use. 	
c. Copy and paste the license code into the license box.	
License code	
eyJja WQiC NVcm Vx5cy5j	
psov6sxvavxepssvarepsicramasia6psaor100iup6stun=	
	7
Liose Back Download .exe	3

6. Copy the **License code**.

You have license code now, you need this license code while creating a vault and secret.

Create a Vault to Store the Qualys License Information

You can store your Qualys License information in a vault secret. You need to create the vault, define the secrete. Follow these steps to create a vault.

- 1. Log in to Oracle Cloud > Vault > Create Vault.
- 2. From **Create in Compartment**, select the compartment and provide the **Name** for the vault.

Note: Ensure you have vault permissions.

The vault is created. A listing page with all the vaults is displayed.

Define a Secret for Scan Recipe

You need to define a secret for scan recipe. Secret is used to store the Qualys license information in the vault.

Follow these steps to create a secret:

Before creating a secret, create a secret key.

1. From the vault detail, click **Create Key**.

V	q 12				
ACTIVE	Vault Information General Information Comparison of the series of the		Virtual Privale: No Cryptographic Endpoint: <u>Ellen</u> and Management Endpoint: <u>Management Endpoint: <u>Management Endpoint</u>: <u>Jacob</u></u>	Antrodominance. Antrodominance. Santalestadad com () Santa de Composition de C	
Resources	Master Encryption Keys in dev-Ixag	Compartment			
Master Encryption Keys	Create Key				
Secrets	Name	State	Protection Mode (i)	Algorithm	Created -
List scope		Enabled	HSM	AES	Tue, Dec 6, 2022, 09:56:08 UTC
Compartment					Showing 1 Item $\ \ < \ 1$ of 1 $\ >$
d ig Califyria (root) i prospradiengi neeringi peresengeperetworki dev-kag					¢
Filters					

The Create Key window is displayed.

2. From **Create in Compartment**, select the compartment, **Protection Mode** as HSM and provide the **Name** of the key.

Create Key		
Create in Compartment		
derally		\$
ualysinc (root)/q-nonprod/engineering/qa-engops-network/dev-lxag		
Protection Mode (i)		
HSM		\$
Name		
gk ala -key		
Key Shape: Algorithm 🕡	Key Shape: Length	
AES (Symmetric key used for Encrypt and Decrypt)	256 bits	\$
Import External key		
Create a new key by importing a wrapped file containing key data that matches th	a specified key shape. For more information, see Importing Keys	
Orease a new key by importing a wrapped me containing key data that matches the	e specified key shape. For more mormation, see <u>importing Keys</u> .	
Show advanced options		

3. To encript the key, go to **Secrets** and click **Create Secret**.

Identity & Security > Vaults > Vault Deta	alis QUIIII Delete Vault Edit Name Add tags Move Resource Delete Vault		
	Vault Information Tags		
	General Information		
	Compartment: qualy	ixag	Virtual Private: No
ACTIVE	OCID:fqa5sa <u>Show Copy</u> Created: Tue, Dec 6, 2022, 09:53:11 UTC HSM Key Version Usage: 4 (2)		Cryptographic Endpoint: <u>https://efry6eihaacsc-</u> crypto.kms.us- sanjose- 1.oci.oraclecloud.com (i)
			Management Endpoint: <u>https://eflyGeihaacsc-</u> management.kms.us- sabjose: 1.oci.oraciecloud.com ()
Resources	Secrets in dev-lxag Compartmen	ıt	
Master Encryption Keys	Create Secret		
Secrets	Name S	Status	Created
		Active	Tue Dec 6 2022 09:59:46 UTC

- 4. From **Create in Compartment**, provide **Name** and **Description**, and select the **Encryption Key**.
- 5. Select the **Secret Type Template** from the list and paste the license code you copied into the **Secret Contents**.
- 6. To store the information, click **Crete Secret**.

Create Secret	<u>Help</u>
Create in Compartment	
ag	\$
qualysinc (root)/q-nonprod/engineering/qa-engops-network/dev-lxag	
Name	
gła od4	
Description	
Encryption Key in dev-Ixag ④ (Change Compartment)	
gi d4	٥
Secret Type Template	
Base64	\$
Secret Contents	
eyJjaWQiOi iLCJwd3NV	3Y
Show advanced options	
Create Secret Cancel	

The Secret is created for scan recipe.

Create a Scan Recipe for Host Instances

Oracle Cloud Infrastructure Vulnerability Scanning Service creates recipes that scan target host's instances. To create a scan recipe, follow these steps:

1. Go to **Identity & Security** > **Scanning** > **Scan Recipes**.

Q Search	Identity & Security		
Home Compute Storage Networking Oracle Database Databases Analytics & Al Developer Services Identity & Security Observability & Management Hybrid Migration & Disaster Recovery Billing & Cost Management Governance & Administration	Identity Users Groups Dynamic Groups Network Sources Policies Compartments Federation Authentication Settings Cloud Guard Overview Problems Recommendations Threat monitoring Targets Responder activity Defector recipes	Security Zones Overview Recipes Security Advisor Threat intelligence Overview Threat inclator Database Firewalls Network Firewall Policies Web Application Firewall Policies Network Address Lists Edge Policy Resources	 Scanning Vulnerability Reports Scanning Reports Targets Scan Recipes Vauit Managed Access Access Requests Approval Templates Resource Settings Bastion Compliance Audit
Marketplace	Responder recipes	Overview	

2. From the Hosts tab, click **Create**.

Scanning	Create a recipe to control how resource	es are scanned. After creating a	ment recipe, assign it to targets. <u>Learn more</u>	
Vulnerability Reports	(i) Qualys BYOL option now avail	lable. See the agent option in h	ost <u>scan recipe</u>	
Scanning Reports				
Targets	Hosts Container image			
Scan Recipes				
	Create			
List scope	Name	Status	Created	•
Compartment				
c g ≎	<u>au5</u>	Active	Wed, Jan 11, 2023, 08:08:11 UTC	:
ualysinc (root)/q-nonprod/engineering/qa-engops- etwork/dev-lxag	gk6 an_recipe	Active	Tue, Jan 10, 2023, 11:45:54 UTC	:
	BYOI Lag	Active	Wed, Dec 7, 2022, 10:54:27 UTC	:
ilters	<u>B'</u> cipe	Active	Tue, Dec 6, 2022, 10:04:32 UTC	:
tate			Showing 4 items 🗸 Page 1	
Any state 🗘				-
ag filters add I clear				
o tao filters applied				-

- Enter the Name for the recipe.
 From Create in Compartment, select the compartment where you want to store the recipe.
- 5. Select Qualys for the **Agent based scanning**, and select the vault and secret that you stored your Qualys license.

Note: You can enter the license information directly into a new secret

6. Click **Create scan recipe** to save the information.

Create scan recipe	Held
туре	
Compute	\$
Name	
BYOLrecipe	
Create in compartment ()	
d hg	\$
alysinc (root)/q-nonprod/engineeringiqa-engops-network/dev-bag	
ublic IP port scanning ()	
Standard (Top 1000 ports)	0
Agent based scanning	
Vou must give permission to the Scanning service to install agents onto your compute instances. Learn more Agent to use	
OCI	Qualys
Oracle Cloud infrastructure - Free agent	Premier offering Agents and Dashboard Price - BYOL 🗸
To create a Qualys agent scan recipe, you must first select a vauit in which to create the recipe define a secret for the A secret has been defined but policies are missing. You must define the missing policies. Learn more Select a vauit in dev.txag ③ (Charge Compariment)	recipe, and then schedule the scan. Learn more
qual k12	\$
Define a secret 🕡	
vr 12	a 🎽
To configure the Qualys agent scanning schedule or any other Qualys agent configurations, go to the Qualys dashboard.	
Create scan recipe Save as stack <u>Cance</u>	·

Scan recipe to scan target host instances is created.

Create a Target to Assign a Scan Recipe

A target is a group of cloud resources you want to be scanned for vulnerabilities. Create a target for assigning it to scan recipe.

- 1. Click **Create target** from the Scan recipe details window.
 - This new target uses the scan recipe that you have just created.
- 2. Enter **Name** of the target.
- 3. From **Create in Compartment,** select the compartment.
- 4. Provide **Decription** and select scan recipe from the list.
- 5. Select the **Target compartment**, and scan all or a subset of your instances as required.
- 6. To save the target, click **Create target** from Create target window.

ORACLE Cloud Search resources, services, documentation, and Marketplace		US West (San Jose) ∨ 🕢	₽ @ ⊕ 9
Scanning > Scan recipes > Scan recipe details	Create tar	get	Help
Active Image: second secon	cipe, click the button below: 20080 20080 1 Second Computer 20080 2		

You can view the target Target Information tab's details and status in Computer instances.

Scanning » Targets » Target details		
-	Next step Click the button below to view the scan results. Results are typically available 15 minutes after creating a new target. View scan result Never show this information again	
	gk 4_target Edit Move resource Add tags Dekte	
ACTIVE	Target information Tags	
	OCID: _ 2mbuba <u>Show Copy</u> Target compartment: qualysinc (root) Me kag () Compartment: qualysinc (root)\q-nc s-network/c rag Description: - - Scan recipe: <u>BYOL-anul-test-trag</u> Created: Tue, Jan 10, 2023, 11:47:16 UTC	
	Type: Compute	
Resources	Compute instances	A
Compute instances Compute instances with errors	Name	
		Showing 1 item

You have completed the set up now, you can see the results in VSS (Vulnerability Scanning Service).

Appendix A: Permissions and Policies

To use the BYOL feature, you must set up policies in VSS (Vulnerability Scanning Service). Refer the following policies and permission required:

- Grant the following:
 - Permission access to the VSS service
 - Permission to group of administrators to access to VSS service
- Set up the policies and dynamic groups for VSS Qualys BYOL

Grant Access to the VSS Service

- Allow VSS access in tenancy OR compartment.
- Allow to manage instances.
- Allow to read compartments, vnics, vnics-attachements.
- Allow to read repos for VSS OCIR container image scans.

Grant Permission to Group of Administrators to Access to VSS Service

- Allow groups access to VSS in the tenancy OR compartment.
- Allow admins to manage vss-family to allow all scan settings.
- Allow admins to read repos for container image scanning.

Statemen	ts
Edit Policy Stat	ements
Allow Service vuln	erability-scanning-service to manage instances in tenancy
Allow Service vuln	erability-scanning-service to read compartments in tenancy
Allow service vuln	erability-scanning-service to read vnics in tenancy
Allow service vuln	erability-scanning-service to read vnic-attachments in tenancy
Allow Group VSS_	Admins to manage vss-family in tenancy
Allow Group VSS_	Admins to read repos in tenancy

Set up the Policies and Dynamic Groups for VSS - Qualys BYOL

Create a dynamic group of instances that you want to scan.

For example:

The dynamic group includes instances that meet the criteria defined by any of the following rules. (Select - Match any rules defined)

Any {instance.compartment.id = '<compartment-ocid-of-your-instances-or-Thiscould-even-be-the-whole-tenancy>'}

Edit All Matching Rules
Matching Rules
Rules define what resources are members of this dynamic group. All instances that meet the criteria are added automatically.
Example: Any {instance.id = 'ocid1.instance.oc1.iadexampleuniqueid1', instance.compartment.id = 'ocid1.compartment.oc1exampleuniqueid2')
Match any rules defined below Match all rules defined below
Rule 1
Any (instance.compartment.id = 'gcig1 g1aacoon " " " " " " " " " " " " " " " " " "

Policy for granting permission for the instances to access secrets

This allows the Qualys agents to get the Qualys license data and send that in communications to the Qualys data center.

- Allow dynamic-group <your-qualys-instances-group > to read vaults in the tenancy
- Allow dynamic-group <your-qualys-instances-group > to read keys in the tenancy.
- Allow dynamic-group <your-qualys-instances-group> to read secret-family in the tenancy

Need to get access to the data sent back from Qualys

- Define tenancy ocivssprod as ocid1.tenancy.oc1..aaaaaaaa6zt5ejxod5pgthsq4apr5z2uzde7dmbpduc5ua3mic4z v3g5ttma
- Endorse dynamic-group <your-qualys-instances-group> to read objects in tenancy ocivssprod

Following screenshot shows policies set up for dynamic group of instances.

Statements
Edit Policy Statements
Define tenancy ocivssprod as ocid1.tenancy.oc1aaaaaaaaugj2axq2hd2sia3jcegwdyvurggbgpdrvwda2u4b2uzkelgam64q
Endorse dynamic-group bb_vss_tuagarwa_dg to read objects in tenancy ocivssprod
Allow dynamic-group bb_vss_tuagarwa_dg to read vaults in tenancy
Allow dynamic-group bb_vss_tuagarwa_dg to read keys in tenancy
Allow dynamic-group bb_vss_tuagarwa_dg to read secret-family in tenancy