Qualys Context XDR (Extended Detection and Response)

Oracle OCI Audit

Data Mapping Guide

February 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

About this Guide

Thank you for your interest in Extended Detection and Response (XDR). Qualys Context XDR expands the capabilities of the Qualys Cloud Platform to integrate data points from other Qualys products offer a unified view of your organization's security posture. Context XDR integrates data points (events/logs) from your enterprise's ecosystem that comprises of several heterogenous sources. This data is normalized, enriched and then categorized before storing it in the Qualys Context XDR data model. This unified database that holds data points from multiple security applications is then used to offer a 360° view of your organization's security posture — all from a single solution.

The Data Mapping Guides provide a list of the fields received through a data source and how these fields are mapped to the Context XDR data model.

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 http://www.qualys.com/support/.

Overview

Qualys Context Extended Detection and Response (XDR) can be configured to ingest data from several different data sources. Each data source has its own data points, and this Data Mapping Guide offers insight into how these data points are interpreted, normalized, and mapped in Qualys Context XDR.

This guide focuses on the data mapping between Oracle OCI Audit fields and the Qualys data model.

Note: For a complete list of sources that Qualys XDR supports, on the Qualys XDR UI, navigate to **Configuration** > **Data Collection** > **Catalog**. If the source you are looking for is not in the catalog, you can add a request for support using the **Not in the list?** card.

Device Details

- **Device Type** – Cloud Infrastructure
- **Device Vendor** – Oracle
- **Device Product** – Oracle OCI Audit
- **Supported Versions** – Limited Support. Contact your TAM for further information.

Supported Formats

In Qualys Context XDR, you can configure to receive data from Oracle OCI Audit using the following formats:

- **Cloud**

For information on configuring collectors, refer to the Deploying a Collector section in the Online Help.

Data Field Mappings

This section provides a detailed mapping of the data source fields to the Qualys Context XDR.

deviceType – Cloud Infrastructure
deviceVendor – Oracle

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
data.additionalDetails.bucketName	accountName	LOCAL_QWEB1 DXB	A container object for attributes unique to the resource emitting the event.
data.availabilityDomain	sourceDomain	DXB-AD-1	The availability domain where the resource resides.
data.compartmentName	Oracle_Audit_CompartmentName	dxb01-prod-data	The name of the compartment of the resource emitting the event.
data.eventName	eventName	GetBucket	Name of the API operation that generated this event.
data.identity.authType	Oracle_Audit_AuthType	null	The type of authentication used.
data.identity.callerName	userName	null	The name of the user or service issuing the request. This value is the friendly name associated with callerId.
data.identity.ipAddress	sourceIpv4	10.192.19.145	The IP address of the source of the request.
data.identity.principalName	Oracle_Audit_PrincipalName	objectstorage-me-dubai-1	The name of the user or service. This value is the friendly name associated with principalId.
data.identity.userAgent	userAgent	Oracle-JavaSDK/2.0.1-preview1-SNAPSHOT (Linux/4.1.12-124.61.2.el7uek.x86_64; Java/1.8.0_331; Java HotSpot(TM) 64-Bit Server VM GraalVM EE 21.3.2/25.331-b09-jvmci-21.3-b11)	The user agent of the client that made the request.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
data.message	message	Bucket details retrieved	A friendly description of overall log
data.request.action	method	GET	The HTTP method of the request.
data.request.heards.authorization.algorithm	Oracle_Audit_AuthAlgo	rsa-pss-sha256	The algorithm used for authorization.
data.request.path	Oracle_Audit_RequestPath	/n/axtqwmwbaayf/b/LOCAL_QWEB1DXB?fields=approximateCount	The full path of the API request.
data.response.responseTime	updateTime	2022-06-02T11:13:59.579Z	The time of the response to the audited request, expressed in RFC 3339 timestamp format.
data.response.status	status	200	The status code of the response.
id	externalId	60fdd411-c9d8-a45f-588d-cd4eef34b80b	Associated ID given in the event by the event source.
oracle.compartmentid	Oracle_CompartmentId	ocid1.compartment.oc1..aaaaaaaaya3e34hpwvlrgahoyagk4sjkxs4l7sx7acc22t75vhydswadnxgq	OCID of the compartment the log group is in.
oracle.ingestedtime	receivedTime	2022-06-02T11:13:59.955Z	Time the log was ingested by OCI Logging.
oracle.loggroupid	Oracle_LogGroupId	_Audit	OCID of the log group.
oracle.tenantid	Oracle_TenantId	ocid1.tenancy.oc1..aaaaaaaamnz63ivd7pl6capmzk7y3mlmt5sd5i6v7qxhufn6gqlwcxtbrkpa	OCID of the tenant.
source	sourceUser	LOCAL_QWEB1DXB	The resource that produced the event.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
time	eventTime	2022-06-02T11:13:59.579Z	Event Time when log was logged
type	eventType	com.oraclecloud.objectstorage.getbucket	Type of the event.

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
DeviceType	Cloud Infrastructure
DeviceModel	Oracle OCI Audit
DeviceVendor	Oracle
DeviceHost	-
CustomerId	d656b196-edb7-45e6-8485-3748a740d002
CollectorId	ae102769-bd05-415d-af3c-2cc59681cbab
EventSourceId	1ae639f0-0944-4cbc-81ef-87c040ca9eb2
EventId	d656b196-edb7-45e6-8485-3748a740d002
CollectorReceivedTime	Jun 01, 2021 11:29:04 AM