Qualys Context Extended Detection and Response

OpenLDAP

Data Mapping Guide

February 18, 2022

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 Qualys 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 OpenLDAP fields and the Qualys data model.

Note: For a complete list of sources that Qualys Context XDR supports, on the Qualys Context 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. Based on the requests coming in, Qualys will prioritize and attempt to add support at the earliest.

Device Details

- **Device Type** – Application
- **Device Vendor** – OpenLDAP
- **Device Product** – LDAP
- **Supported Versions** – Limited Support – Contact your TAM for further information.

Supported Collectors

In Qualys Context XDR, you can configure to receive data from OpenLDAP using the following collectors:

- **Syslog**

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 – Application
deviceVendor – OpenLDAP

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Time Stamp	eventTime	9/24/2021 3:50	Time of the event
Device Name	deviceName	ds-consumer-prodXX	LDAP Consumer Server
Process Name	processName	slapd	LDAP Daemon
Process ID	processId	1268	LDAP Daemon Process ID
conn	baseEventId	339280	Connection Number
fd	customNumber1	69	File Descriptor
Outcome	outcome	ACCEPT	LDAP Connection
IP	sourceIpv4	64.39.96.133	Source IP
Source Port	sourcePort	39488	Source Port
IP	destinationIpv4	0.0.0.0	Destination IP
Destination Port	destinationPort	636	Destination Port
tls_ssf	customNumber3	256	Security Strength Factor. Possible Values are: 0 - No Protection 1 - Integrity Protection 56 -DES 112 - 3DES 128, 192, 256 - AES
ssf	customNumber4	256	
Event Name	eventName	ACCEPT from IP=64.39.96.133:39488 (IP=0.0.0.0:636)	
op	customNumber2	0	
Event Subtype	eventSubType	BIND	Request Type
dn	customString6	cn=acg,dc=montana,dc=edu	Distinguished Name
method	customString7	Simple Bind with user password	

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
base	customString8	"ou=people,dc=montana,dc=edu"	
scope	customString9	wholeSubtree	
filter	customString10	(&(objectClass=posixGroup)(cn=aux-ssh-allow))	
attr	customString11	cn userPassword memberUid gidNumber uniqueMember	
tag	customNumber12	Result from a client bind operation	
nentries	count	0	
Event Type	eventType	LDAP Request/LDAP Response	Type of the event
Syncrepl Class	object	syncrepl_message_to_entry	group/policy/registry/domain change
Description	description	rid=006 DN: uid=j68z134,ou=people,dc=montana,dc=edu, UUID: 74586086-ed78-1031-82b5-55fe6eef9d35	Rest of the fields from raw message
rid	externalId	6	Associated ID given in the event by the event source.

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Application
deviceModel	LDAP
deviceVendor	OpenLDAP
deviceHost	DC2-PA-XXX.npi.int
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