Qualys Context XDR (Extended Detection and Response)

Citrix Loadbalancer

Data Mapping Guide

March 15, 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 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 Citrix Loadbalancer 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** – Loadbalancer
- **Device Vendor** – Citrix
- **Device Product** – Citrix Loadbalancer
- **Supported Versions** – 13.0

Supported Formats

In Qualys Context XDR, you can configure to receive data from Citrix Loadbalancer using the following formats:

- **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 – Loadbalancer
deviceVendor – Citrix

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Timestamp	eventTime	09/23/2021:05:16:03 GMT	Time of the event
Device	deviceName	citrixhost	Hostname of the device where event is produced/logged
	deviceIPAddress	10.10.10.11	IP address of the device on which the event is produced
Type	eventType	GUI	Type of the event
Event Name	eventName	CMD_EXECUTED	Brief standard meaning of the message easy to read for Analyst
SessionID	sessionId	35760	Unique number given to every log
User	sourceUser	nsroot	Username using/logged-in the source machine (the username present in the log audit as per the log audit logged by the device)
Source	sourceIpv4	10.100.100.100	IPv4 address of the source machine (the machine who has generated this event as per the log audit)
Command	command	show system bwserver 0	This field captures the 'command' used in the audit log
Status	outcome	Success / ERROR	Status of the request.
Failure_reason	reason	Operation not supported	Failure reason due to which the server was denied access
Destination	destinationIpv4	127.0.0.1	IPv4 address of the destination machine (the machine who has generated this event as per the log audit)
act	action	Deny	Action taken in the event log
Source Port	sourcePort	13693	Original session source IP port

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Destination Port	destinationPort	5000	Original session destination IP port
Start Time	beginningTime	10/01/2021:06:30:00 GMT	Time the log was sent at the management plane
End Time	endTime	10/01/2021:06:30:00 GMT	Time the log was received at the management plane
Total_bytes_recv	inByte	5345	Number of bytes in the server-to-client direction of the session
Total_bytes_send	outByte	4337	Number of bytes in the client-to-server direction of the session
NATSourceIP	natSourceIP	127.0.0.2	Natted IP address of the source machine (the machine who has generated this event as per the log audit)
NATSourcePort	natSourcePort	43108	Natted port on the source machine (the machine who has generated this event as per the log audit)
Vserver	additionalIP	10.100.100.101	Virtual Server through where These are the connections are being tracked by netscaler like HTTP

Qualys Internal Fields

Qualys Context XDR QQL Tokens	**Sample Values**
deviceType	Loadbalancer
deviceModel	ADC
devisceVendor	Citrix
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
Severity	Informational