



Qualys Context XDR v1.x

Release Notes

Version 1.0.6

September 20, 2022

Here's what's new in Qualys Context XDR 1.0.6!

- [New Definition Column Added for Special Objects](#)
- [Enhancements to the Appliance Details](#)
- [Additional Fields Added for Windows Events ID 4688](#)
- [Enhancements to the Rules Criticality Rating](#)
- [Support for Microsoft Sysmon Source](#)
- [DLQ Events Moved to Events Tab](#)
- [Newly Introduced Log Source Monitoring/Storage Management Notes](#)

Context XDR 1.0.6 brings you more improvements and updates!

New Definition Column Added for Special Objects

With this release, we have now added a **Definition** column for Special Objects page, where you can view the type of object: **Static** or **Dynamic**.

- **Static** - Allows you to configure the values/attributes that are controlled from the UI.
- **Dynamic** - Allows you to configure multiple rules that can add or remove fields/values from the special object.

Navigate to **Configuration > Special Objects** and you view the **Definition** column added. You can click **New Object** and select Static or Dynamic type of special object you want to create. Then, enter the required details for the special object to be created. For more information, you can refer to the online help.

XDR							
HOME DASHBOARD THREAT MANAGEMENT ADVANCED ANALYTICS RULES CONFIGURATION							
Special Objects							
519 Total Special Objects		1 - 50 of 519					
New Object							
LAST UPDATED	OBJECT NAME	DEFINITION	CREATED BY	TYPE	VALUE COUNT	VALUES	RULES
4 days ago	simple so so testing	STATIC	dashb_du	String	1	asd	0
4 days ago	simple so 2 so testing	STATIC	dashb_du	String	1	asd	0
4 days ago	simple so 1 so testing	STATIC	dashb_du	String	1	asd	0
5 days ago	Test test DSO	DYNAMIC	dashb_du	String	0		0
5 days ago		DYNAMIC	dashb_ph	String	0		0
6 days ago	Test flow flow	DYNAMIC	dashb_hr	String	0		0

Notes:

- Under **Special Objects**, sorting of data for the **Definition** column needs enhancement.
- The Special Object search results may include events with Null/Blank values for Dynamic Special Objects.
- For Dynamic Special Objects, Search functionality for **Associated Rules** tab may not display accurate results.

Enhancements to the Appliance Details

We have newly added MTU and NIC details under Summary page of an Appliance.

- **MTU** - Maximum Transmission Unit (MTU) is the maximum size of the packet that can be transmitted from a network interface.
- **NIC** - Network Interface Controller (NIC) is a hardware component which a device or machine can be connected over a network.

You can navigate to **Configuration > Data Collection > Appliances** tab. Select any appliance and click **View Details** from the quick actions menu. Then, you can view the **Summary** page for the **MTU** and **NIC** details.

← Appliance Details: DataMonitoring_Test_Appliance

Summary
List of Services

4 Collectors
20 Event Sources

Lookup code
ff201188-a4da-4b14-9ada-303b0797217a ⓘ

General Details

Description:	
Activation Key:	8681194508
Status:	Active
Appliance ID:	3c6770d2-f2cb-4cd5-8952-869ca03ee6cf
Memory Usage (%):	43.18
Current Root Disk Usage (%):	40
Last Root Disk Usage (%):	40
Current Secondary Disk Usage (%):	1
Last Secondary Disk Usage (%):	1
Last updated on:	a few seconds ago
Created on:	6 months ago
Deployment Location:	Pune
Ipv4 Address:	10.44.150.51
Host Name:	CAMSD
Name Servers:	10.44.148.41,10.44.148.55
MTU:	1500
NIC:	6

We have also added new columns for **Status**, **Network IO**, and **Block IO** details on List of Services page of an Appliance.

- **Status** - Displays the current status of a service.
- **Network IO** - Displays the total bytes received and transmitted over the network by the corresponding container.
- **Block IO** - Displays the number of bytes written/read from your container to the disk.

Simply, navigate to **Configuration > Data Collection > Appliances** tab. Select any appliance and click **View Details** from the quick actions menu. Then, click **List of Services** to view the details of newly added columns.

← Appliance Details: P01_10.114.252.235

Summary

List of Services

List of Services

STATUS	SERVICE NAME	BUILD VERSION	LAST UPDATED	MEMORY	CPU	UPTIME	NETWORK IO	BLOCK IO
Running	cams-rsyslog	1.4.0-7	6 days ago	0.06 / 0.06	0.03 / 0.04	Up 6 days	487MB / 9.38MB	19.3MB / 2.43MB
Running	syslog-collector	1.3.4-6	3 hours ago	1.57 / 1.57	0.57 / 0.4	Up 3 hours	0B / 0B	0B / 10.2MB
Running	syslog-cloud-output	1.3.4-6	3 hours ago	0.06 / 0.05	0.01 / -	Up 3 hours	0B / 0B	0B / 0B
Running	cams-logstash	1.4.0-7	6 days ago	1.58 / 1.57	0.89 / 1.02	Up 6 days	206MB / 251MB	89.8MB / 552MB
Running	CAMSD	1.4.0-7	6 days ago	0.54 / 0.62	0.26 / 75.56	Up 6 days	0B / 0B	20.2GB / 622MB
Running	ad-collector	1.3.4-6	2 hours ago	2.79 / 2.24	5.33 / 2.46	Up 2 hours	323kB / 232kB	0B / 336kB
Running	on-prem-monitoring	1.3.4-6	3 hours ago	2.73 / 2.7	0.81 / 5.32	Up 3 hours	447kB / 539kB	0B / 635kB
Running	conf-fetcher	1.3.4-6	3 hours ago	2.3 / 2.26	0.88 / 1.03	Up 3 hours	634kB / 330kB	0B / 483kB

Additional Fields Added for Windows Events ID 4688

With this release, you can view the new event values added such as command, destinationProcess, ProcessId, WinLogMandatoryLabel, winLogTargetLogonId, and winLogTokenElevationType fields for Windows Events ID 4688.

You can navigate to **Threat Management > Events** tab. Then, use search tokens filter with 'deviceType:`Operating System`' and externalId:'4688' and destinationProcess:*' to view the Windows OS events. Click **Events Values** to view the newly added fields.

The screenshot shows the XDR Threat Management interface. The top navigation bar includes XDR, HOME, DASHBOARD, THREAT MANAGEMENT (selected), ADVANCED ANALYTICS, RULES, and CONFIGURATION. The left sidebar shows 'Threat Management' with a '5 Total Events' indicator and a 'DEVICE TYPE' filter set to 'Operating System'. The main content area displays a search filter: 'deviceType:`Operating System` and externalId:'4688' and destinationProcess:*'. Below the filter, a dropdown shows 'Apr 28, 2022 03:50 PM 19 days ago'. A detailed event entry is shown with fields like action, collectorId, collectorReceivedTime, command, destinationProcess, destinationUserId, deviceEventId, deviceHost, and deviceModel. The 'EVENT VALUES (31)' tab is selected, showing a list of values. The 'command' and 'destinationProcess' fields are highlighted with a red box.

EVENT VALUES (31)	JSON VIEW	RAW MESSAGE
action	Process Creation	
collectorId	3fa85f64-5717-4562-b3fc-2c963f66afa6	
collectorReceivedTime	Apr 1, 2022 01:01 AM	
command	C:\Windows\System32\WScript.exe	
destinationProcess	Registry	
destinationUserId	S-1-0-0	
deviceEventId	Microsoft-Windows-Security-Auditing:4688	
deviceHost	DESKTOP-HRS9VRH	
deviceModel	Windows	

This screenshot shows a detailed view of the event values for Windows Events ID 4688. The search filter remains the same. The 'EVENT VALUES (31)' tab is selected, displaying a list of values. The 'processId', 'winLogMandatoryLabel', 'winLogTargetLogonId', and 'winLogTokenElevationType' fields are highlighted with red boxes.

guid	54849625-5478-4994-a5ba-3e3b0328c30d
osDetails	19044.1586
outcome	success
processId	0x4
tags	Windows
timezone	UTC
version	10.0
winlogComputerName	DESKTOP-HRS9VRH
winLogMandatoryLabel	S-1-16-16384
winlogSubjectLogonId	0x3e7
winlogSubjectSid	S-1-5-18
winLogTargetLogonId	0x0
winLogTokenElevationType	%%1936

Enhancements to Rules Criticality Rating

We have now enhanced the rule criticality rating from low, med, and high to **Rule Score** rating from level 1 to level 5 based on the Common Vulnerability Scoring System (CVSS).

When creating a new rule, you need to select the rule score from 1 to 10. Based on the selected rule score, the **Risk score** rating is displayed on the UI.

Simply, navigate to **Rules** tab and you can view the newly added **Rule Score** column on the **Rules** sub-tab.

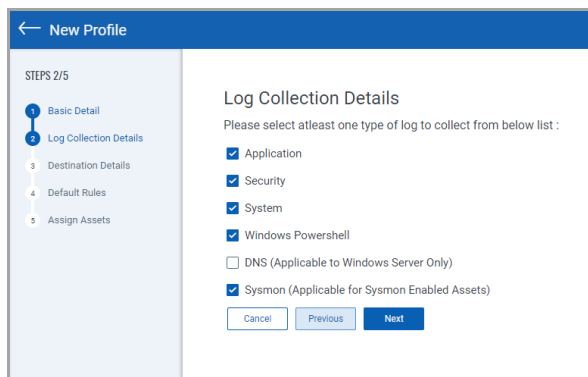
LAST UPDATED	RULE NAME	LOG SOURCES	STATUS	RULE SCORE	TACTICS	TECHNIQUES	SIGNALS
21 hours ago	TippingPoint-Sample Rule Jun 8, 2022 01:39 pm	ips	Inactive	■■■■■	-	-	0
a day ago	T1190 - [Cisco Sourcefire] F5 BIG-IP IContr... May 31, 2022 11:38 am	ips	Threshold paused	■■■■■	Initial Access	Exploit Public-Facing Applicati...	10K
a day ago	T1498.002 - [Cisco Sourcefire] NTP Amplifi... May 31, 2022 11:38 am	ips	Threshold paused	■■■■■	Impact	Network Denial of Service	10K
a day ago	TA0002 - Cisco Sourcefire: Executable Cod... Dec 15, 2021 03:06 pm	ips	Threshold paused	■■■■■	Execution	-	10.2K
a day ago	Cisco Sourcefire: Executable Code Detecte... Dec 10, 2021 01:33 pm	ips	Threshold paused	■■■■■	Execution	-	10.2K
a day ago	destinationzone May 24, 2022 03:25 pm	ips	Threshold paused	■■■■■	-	-	10.2K
a day ago	Rule IPS SourceFire DSO May 23, 2022 06:50 pm	ips	Threshold paused	■■■■■	-	-	10.2K
2 days ago	T1484.001 - Cisco ISE, Multiple Configurat... Jun 21, 2022 08:59 pm	iam	Active	■■■■■	Defense Evasion	Group Policy Modification	0
2 days ago	T1484.002 - Windows_Domain Trust Chan... Jun 21, 2022 08:36 pm	Windows	Active	■■■■■	Privilege Escalation,I	-	0

Support for Microsoft Sysmon Source

With this release, we now support **Sysmon** source to ingest the event logs into context XDR for enriched data.

To configure the sysmon source, navigate to **Configuration > Cloud Agent Profiles > Profiles** and click **New Profile**. Enter the basic details such as Name and Description of profile, select **Windows** as the Operating System, and click **Next**. Then, select Sysmon (applicable for Sysmon Enabled Assets) and proceed to the next steps for configuration.

Note: you can ingest the event logs only from the Sysmon-enabled assets.

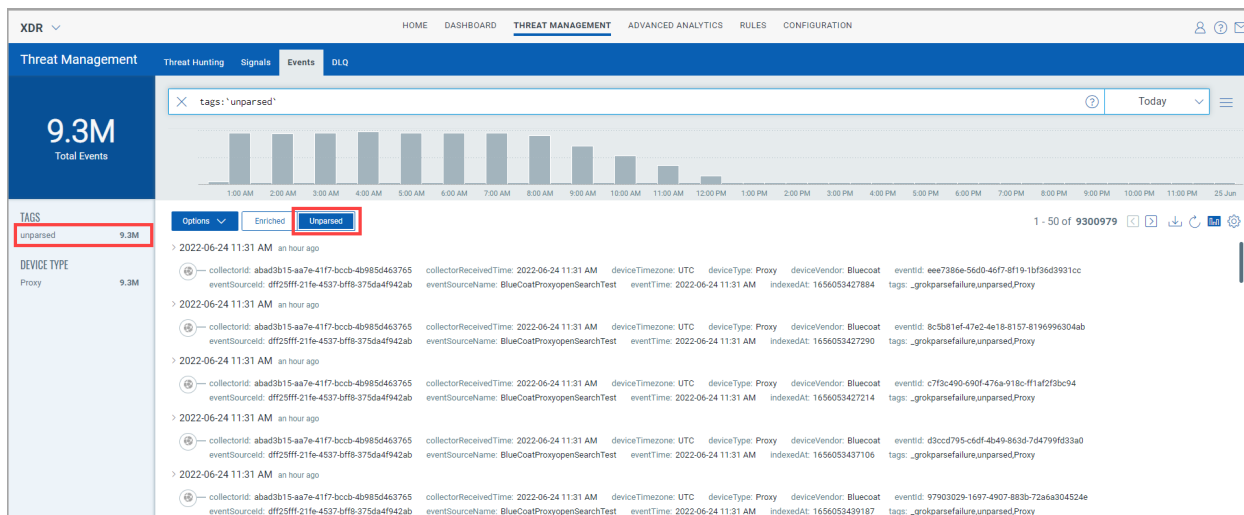


After the profile is successfully saved, Qualys Cloud Agents starts to collect logs from the assets you selected and forwards them to the destination you configured.

DLQ Events Moved to Events Tab

With this release, you can view the unparsed events under the **Events** tab directly. The DLQ feature is deprecated and will be available for older logs.

Navigate to **Threat Management > Events** tab, and click **Unparsed** to view to the unparsed events.



Collector ID	Collector Received Time	Device Timezone	Device Type	Device Vendor	Event ID	Event Source Name	Event Time	Indexed At	Tags
ab3d3b15-aa7e-4177-bccb-4b985d463765	2022-06-24 11:31 AM	UTC	Proxy	Bluecoat	eee7386e-56d0-46f7-8f19-1bf36d3931cc	BlueCoatProxyOpenSearchTest	2022-06-24 11:31 AM	1656053427884	tags: _grokparsefailure,unparsedProxy
ab3d3b15-aa7e-4177-bccb-4b985d463765	2022-06-24 11:31 AM	UTC	Proxy	Bluecoat	8c5b81ef-47e2-4e18-8157-8196996304ab	BlueCoatProxyOpenSearchTest	2022-06-24 11:31 AM	1656053427290	tags: _grokparsefailure,unparsedProxy
ab3d3b15-aa7e-4177-bccb-4b985d463765	2022-06-24 11:31 AM	UTC	Proxy	Bluecoat	c7f3c490-690f-476a-918c-f1af2f3bc94	BlueCoatProxyOpenSearchTest	2022-06-24 11:31 AM	1656053427214	tags: _grokparsefailure,unparsedProxy
ab3d3b15-aa7e-4177-bccb-4b985d463765	2022-06-24 11:31 AM	UTC	Proxy	Bluecoat	d3cc0795-cd6f-4b49-863d-7d479f9d33a0	BlueCoatProxyOpenSearchTest	2022-06-24 11:31 AM	1656053437106	tags: _grokparsefailure,unparsedProxy
ab3d3b15-aa7e-4177-bccb-4b985d463765	2022-06-24 11:31 AM	UTC	Proxy	Bluecoat	97903029-1697-4907-883b-72a6a304524e	BlueCoatProxyOpenSearchTest	2022-06-24 11:31 AM	1656053439187	tags: _grokparsefailure,unparsedProxy

Newly Introduced Log Source Monitoring/Storage Management

We have now introduced a new feature for monitoring, alerting, and limiting the data storage utilization of various device types. As Context XDR is licensed on a per asset basis with storage guardrails to ensure that you do not overuse the storage and explode back-end cloud storage costs for Hadoop. The storage guardrail is now set to 50 GB per asset with a historical retention period of 6 months.

- **Monitoring:**– Allows you to view the amount of allocated data and usage of consumed data.
- **Alerting:**– Notifies to the user when the allocated data usage has reached/crossed over 80%, and data is being aged-out.
- **Limiting:**– Limit the age-out data (first-in and first-out) to ensure the data remains within applied guardrails.

Notes

- Cloud agent XDR filebeat and QGS proxy works with https_proxy=http://<ip>:Port format.
Example: https_proxy=<http://10.114.252.191:8080>