YouTestMe

Log Monitoring and Event Logging

File name	YTM Log Monitoring and Event Logging
Author	YouTestMe
Confidentiality	Public
Last save date	Thursday, October-20-2022 at 11:37:00 PM

Table of Contents

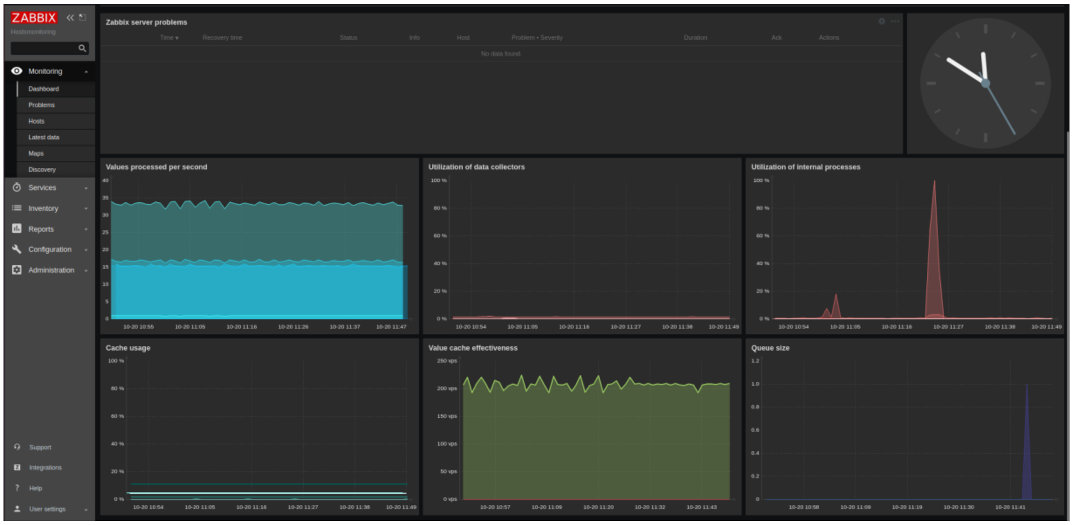
1 Introduction

Effective event logging ensures network and application health, performance, and security. This document represents the types of events logged by tools used in YouTestMe.

2 Monitoring and Event Logging Tools

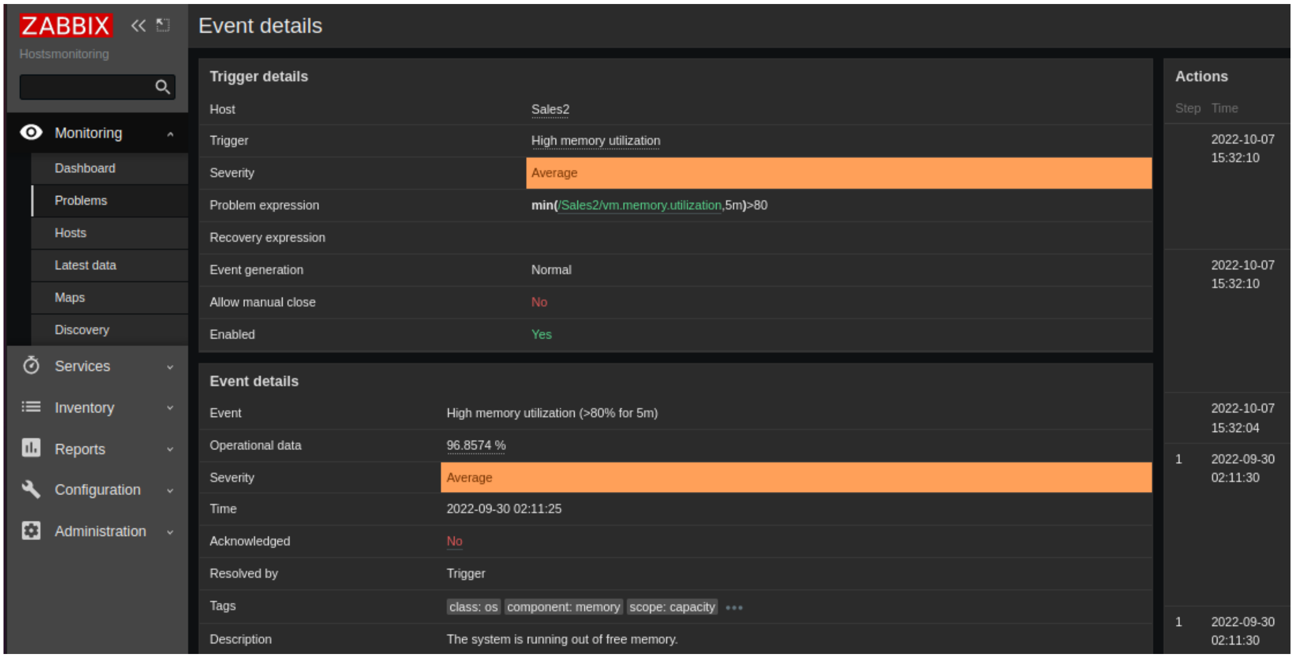
2.1 Zabbix

Zabbix is an open-source software tool to monitor IT infrastructure such as networks, servers, virtual machines, and cloud services.



Zabbix monitors many system resources, the current performance of servers, network load, and server availability. It also monitors resources for the server applications such as Apache Tomcat, Apache Web server, PostgreSQL, and many others.

Some of the most outstanding features are problem notifications and event reports.



Event details

Trigger details

Host	Sales2
Trigger	High memory utilization
Severity	Average
Problem expression	min(/Sales2/vm.memory.utilization,5m)>80
Recovery expression	
Event generation	Normal
Allow manual close	No
Enabled	Yes

Event details

Event	High memory utilization (>80% for 5m)
Operational data	96.8574 %
Severity	Average
Time	2022-09-30 02:11:25
Acknowledged	No
Resolved by	Trigger
Tags	class: os component: memory scope: capacity •••
Description	The system is running out of free memory.

Actions

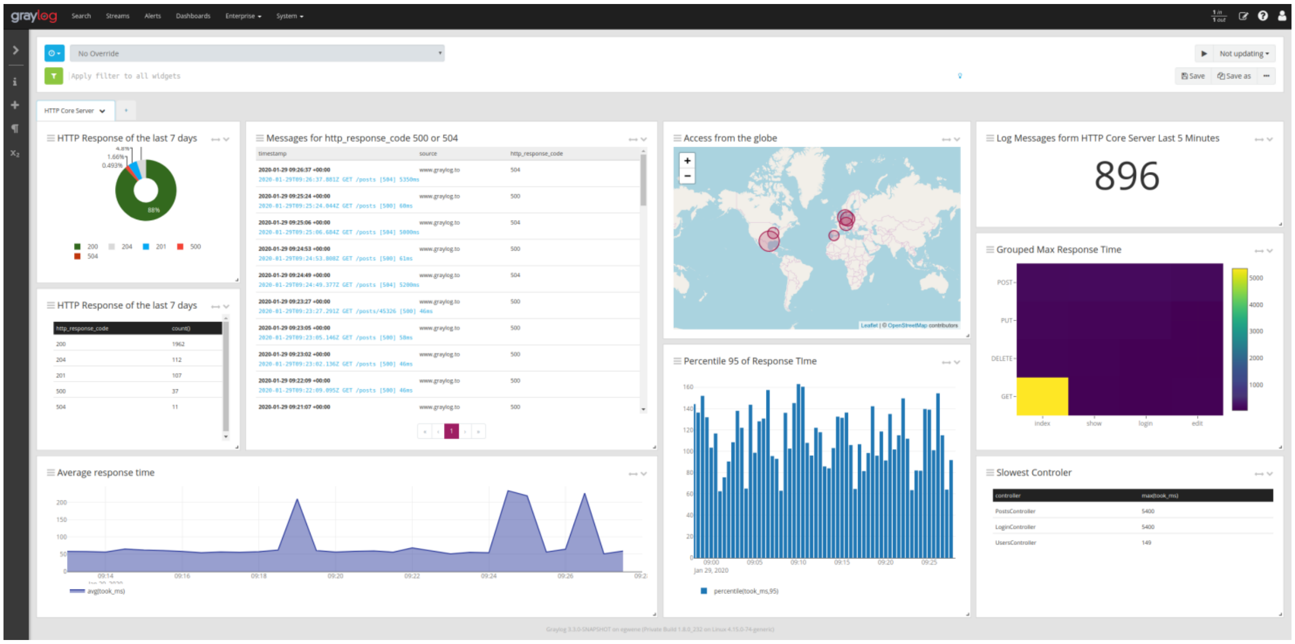
Step	Time
	2022-10-07 15:32:10
	2022-10-07 15:32:10
	2022-10-07 15:32:04
1	2022-09-30 02:11:30
1	2022-09-30 02:11:30

2.2 Graylog

Graylog is defined in terms of a log management platform for collecting, indexing, and analyzing both structured and unstructured data from almost any source.

Centralized logging provides essential benefits:

- Placing all the records in a single location simplifies log analysis and correlation tasks.
- Providing a secure storage area for log data



HTTP Response of the last 7 days

http_response_code	count()
200	1962
204	112
201	107
500	37
504	11

Messages for http_response_code 500 or 504

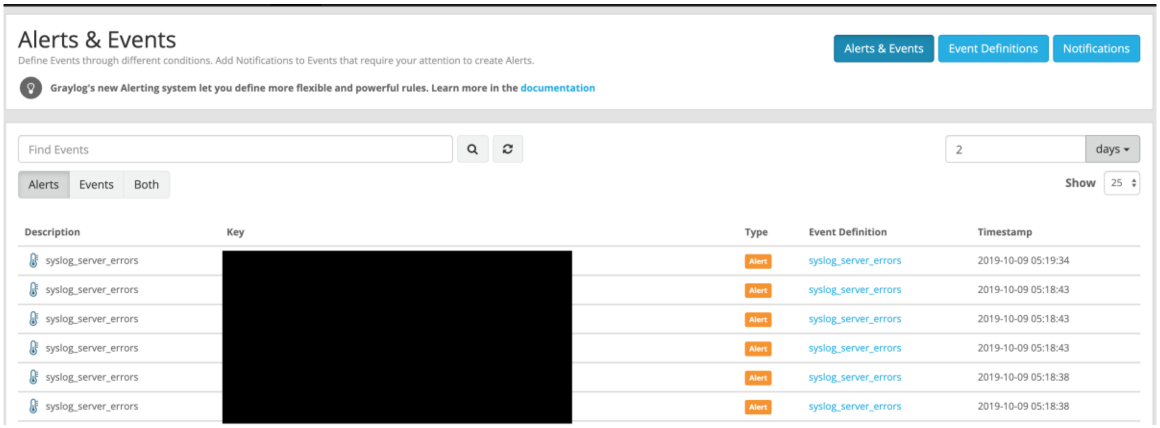
timestamp	source	http_response_code
2020-01-29 09:26:37 +00:00 2020-01-29T09:26:37.881Z GET /posts [504] 5350ms	www.graylog.to	504
2020-01-29 09:25:24 +00:00 2020-01-29T09:25:24.044Z GET /posts [500] 60ms	www.graylog.to	500
2020-01-29 09:25:06 +00:00 2020-01-29T09:25:06.684Z GET /posts [504] 5000ms	www.graylog.to	504
2020-01-29 09:24:53 +00:00 2020-01-29T09:24:53.808Z GET /posts [500] 61ms	www.graylog.to	500
2020-01-29 09:24:49 +00:00 2020-01-29T09:24:49.377Z GET /posts [504] 5200ms	www.graylog.to	504
2020-01-29 09:23:27 +00:00 2020-01-29T09:23:27.291Z GET /posts/45326 [500] 46ms	www.graylog.to	500
2020-01-29 09:23:05 +00:00 2020-01-29T09:23:05.146Z GET /posts [500] 58ms	www.graylog.to	500
2020-01-29 09:23:02 +00:00 2020-01-29T09:23:02.136Z GET /posts [500] 46ms	www.graylog.to	500
2020-01-29 09:22:09 +00:00 2020-01-29T09:22:09.095Z GET /posts [500] 46ms	www.graylog.to	500
2020-01-29 09:21:07 +00:00	www.graylog.to	500

Slowest Controler

controller	max(took_ms)
PostsController	5400
LoginController	5400
UsersController	149

Graylog allows aggregating data from multiple sources, initiating a search across multiple parameters, and analyzing, visualizing, and reporting on the data. Alerts could also be triggered when certain thresholds are exceeded, or suspicious patterns emerge.

Graylog alerts are periodical searches that can trigger notifications when a defined condition is satisfied.



Alerts & Events

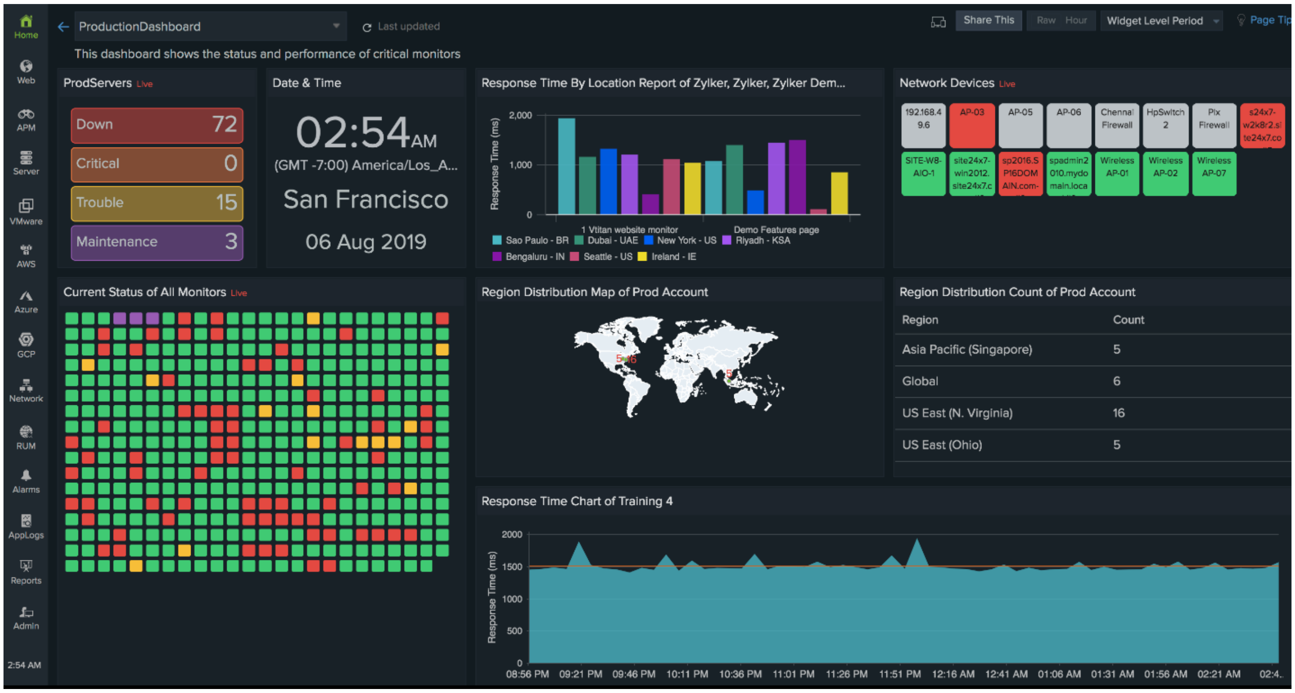
Define Events through different conditions. Add Notifications to Events that require your attention to create Alerts.

Graylog's new Alerting system let you define more flexible and powerful rules. Learn more in the documentation

Description	Key	Type	Event Definition	Timestamp
syslog_server_errors	[redacted]	Alert	syslog_server_errors	2019-10-09 05:19:34
syslog_server_errors	[redacted]	Alert	syslog_server_errors	2019-10-09 05:18:43
syslog_server_errors	[redacted]	Alert	syslog_server_errors	2019-10-09 05:18:43
syslog_server_errors	[redacted]	Alert	syslog_server_errors	2019-10-09 05:18:43
syslog_server_errors	[redacted]	Alert	syslog_server_errors	2019-10-09 05:18:38
syslog_server_errors	[redacted]	Alert	syslog_server_errors	2019-10-09 05:18:38

2.3 Site24x7

Site24x7 brings together metrics, traces, and logs monitoring under one console for different layers of cloud architecture. Monitor the uptime and performance of websites, online applications, and servers.



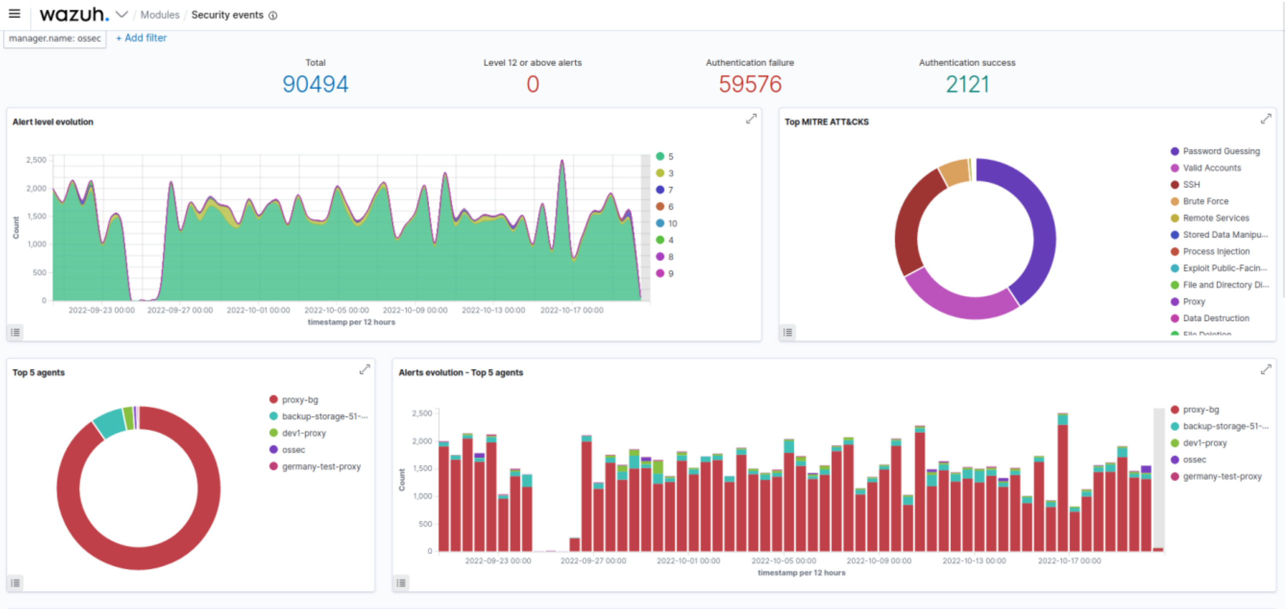
Region Distribution Count of Prod Account

Region	Count
Asia Pacific (Singapore)	5
Global	6
US East (N. Virginia)	16
US East (Ohio)	5

Site24x7 is mostly used to detect downtime and latency on the applications.

2.4 Wazuh

Wazuh is a free, open-source, enterprise-ready security monitoring solution for threat detection, integrity monitoring, incident response, and compliance.



manager.name: ossec

Total	Level 12 or above alerts	Authentication failure	Authentication success
90494	0	59576	2121

Wazuh detects attack attempts by analyzing system logs and matching them with known patterns. Detected attacks with high severity levels are reported immediately via email.

All detected attempts are later listed in generated reports with suggested solutions and vulnerabilities found in the system.