

Logging Best Practices in the CI/CD Era

A Guide for Modern Infrastructure



Ariel Assaraf

Co-founder & CEO

Coralogix

ariel@coralogix.com



Coralogix

Agenda

- » Formats – unstructured Vs JSON
- » Log severity definition
- » Logging best practices
- » Alerts: why you need them
- » Alerts: How to properly define
- » Alerts: to push or not to push
- » Logging to enhance your CICD
- » Benchmark versions
- » The power of logs for custom metrics generation
- » A new approach towards logging
- » Bonus: why logs are called logs?

Format

Why JSON?

- » Easier to filter and group
- » Easier to visualize
- » Easily read
- » Supported by most coding languages and loggers

Why JSON

Example log:

- 1) Ariel, 29, 33 Bilu, Tel-Aviv, Israel, 2012-09-28
- 2) Lior, 32, 110 Ben Gurion, Herzelia, Israel, 2012-09-29

We want to find all users who are 29 years old:

```
$ grep 29 file.log | cut -d , -f 2 | sort | uniq -c | sort -nr
```

What do we get?

- 1) Ariel, 29, 33 Bilu Sharet, Tel-Aviv, Israel, 2012-09-28
- 2) Lior, 32, 110 Ben Gurion, Herzelia, Israel, 2012-09-29

Log severity definition

- » Debug/Verbose – *‘Number of messages in the user creation queue = 3482’*
- » Info – *‘Money transaction completed successfully’*
- » Warning – *‘Received illegal character for username – “Jame\$”, ignoring char’*
- » Error – *‘Failed to execute query for user ID 3424098’*
- » Critical/Fatal – *‘No connection to DB, failed to register user’*

Logging best practices

- » Log communications between components – Microservices, spot instances.
- » Log communications with external API's
- » Add valuable metadata to your logs
- » Remember that you are not the only one reading these logs
- » Combine textual and metric fields

Alerts

- » Why you need them
- » How to properly define alerts
- » The different types of alerts
- » Creating the right structure for alert handling
- » To push, or not to push.

Logging to enhance your CI/CD

- » What to collect
- » How to use

The screenshot displays the Coralogix dashboard interface. At the top, there's a navigation bar with icons for Dashboard, Logs, Insights, Alerts, LiveTail, Tags, ROI, and Kibana. Below this, a header section shows 'Logs (114)' and 'Loggregation' tabs, along with buttons for 'Create Alert', 'Save View', 'Open', 'Clear', and a time range selector set to '07/07/2020 15:06:16.000 - 07/07/2020 15:06:55.000'. A search bar with a 'GO' button is also present.

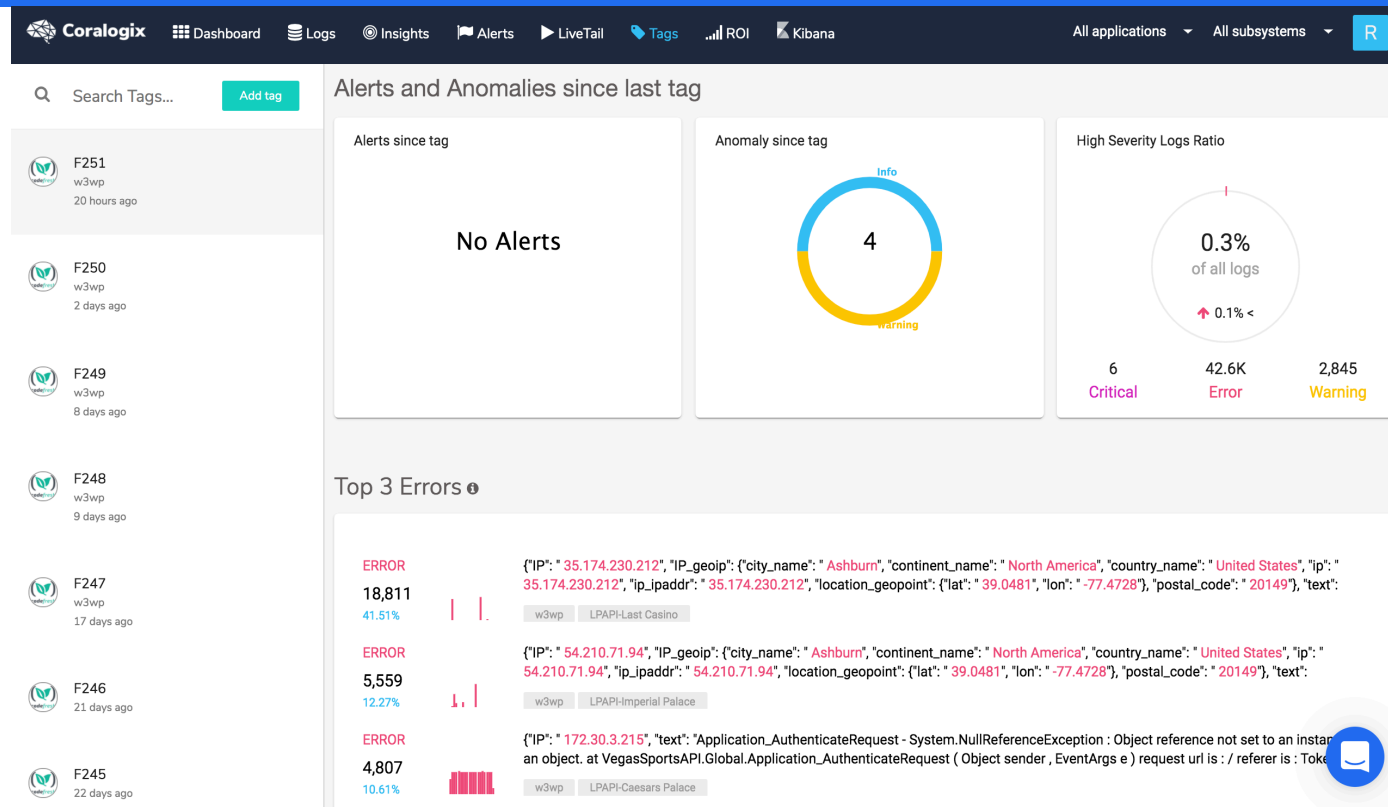
On the left side, there's a 'Manage Columns' panel with a 'Find Filter...' search bar. It lists filters for 'Application' (test app (114), logstash_test_integration (0), nginx (0), test (0)) and 'Subsystem' (test sys (114), access (0), coralogix.com (0), logstash_test_integration (0), test (0)). Below this, a 'Severity' section shows 6 selected filters: Debug (114), Verbose (0), Info (0), Warning (0), and Error (0).

The main area displays a log entry with the following details:

#	Timestamp	Severity	Text
8	07/07/2020 15:06:37.750 pm	DEBUG	<pre>{ "@timestamp" : "2020-07-07T12:06:37.544Z", "path" : "/var/log/test.log", "tags" : ["multiline"], "host" : "9eba213d187f", "message" : " \nSwitched to context \"mydemoAkscluster@BizSpark Plus\". \nv3.0.3+gac925eb \n\"cf-stable\" has been added to your repositories \n\"cf-helm-default\" has been added to your repositories \nRelease \"my-go-chart-prod\" has been upgraded. Happy Helming! \nNAME: my-go-chart-prod \nLAST DEPLOYED: Mon Jun 15 10:30:47 2020 \nNAMESPACE: default \nSTATUS: deployed \nREVISION: 2 \nTEST SUITE: None ", "type" : "test", "@version" : "1" }</pre>


Logging to enhance your CI/CD

- » What to collect
- » How to use



Logging to enhance your CI/CD

- » What to collect
- » How to use

 **Coralogix**

Dashboard

Logs

Insights

Alerts

LiveTail

Tags


ROI


Kibana


All applications ▾ All subsystems ▾ R


Search Tags...


Add tag


 **F251**
w3wp
20 hours ago


 **F250**
w3wp
2 days ago

 **F249**
w3wp
8 days ago

 **F248**
w3wp
9 days ago

 **F247**
w3wp
17 days ago

 **F246**
w3wp
21 days ago

 **F245**
w3wp
22 days ago

Suspected Error ⓘ

CRITICAL

4

Current

4

Normal

0

Over 1000% above normal

*UpdateBalance - wont update balance!! TypeID *63 , UserID *2639232449067475 , Cash = *0 , Coins = *720000 , transaction CurrentBalance = *2513138 , Current user balance = *33138

w3wp LPAPI-Last Casino

CRITICAL

2

Current

2

Normal

0

Over 1000% above normal

{ "IP": " 172.30.3.63", "text": "could not connect to redis Instance at 172.30.3.63 : 6379" }

w3wp LPAPI-Caesars Palace

ERROR

54

Current

54

Normal

0

Over 1000% above normal

{ "IP": " 75.172.11.242", "IP_geopip": { "city_name": " Tacoma", "continent_name": " North America", "country_name": " United States", "ip": " 75.172.11.242", "ip_ipaddr": " 75.172.11.242", "location_geopoint": { "lat": " 47.2067", "lon": " -122.4414", "postal_code": " 98408" }, "text": "user is blocked by ip *75.172.11.242 - at *VegasSportsAPI.Authentication.AuthenticationServi... (String *userToken , String originAppUserID , String deviceName , String ver , String deviceID , Boolean isReload *, String deviceIDFA , Int64 sub , String deviceIDFARealOne , Int64 ebid , String galD , Int32 appld , String *Variable campaign)" }

w3wp LPAPI-Last Casino

15,031 Newly introduced Logs ⓘ

#	Timestamp	Severity	Text	Applicati...
1	08/07/2020 20:15:45.805 pm	ERROR	Error occured while handling webhook from facebook : The best overloaded method match for 'BL.Users.Payments.FBPaymentsStatus.FullFillPayment(BL.Facebook.FacebookCreditsPackage, BL.Users.BaseU arguments paymentid: 3155307821251846	w3wp
2	08/07/2020 20:10:22.819 pm	ERROR	Exception of type 'System.Exception' was thrown. - at VegasSportsAPI.SideGamesServices.SpiningWheelService w3wp	w3wp

Benchmark versions

- » What do we look for after a deployment
- » How to handle issues
- » The feedback loop

Log2Metric

- » The limitation of time series DBs
- » Why do we need custom metrics
- » Why are logs the answer



Coralogix- A New Approach For Logging



Signup for a **FREE** account with **UNLIMITED** builds

& schedule a 1:1 with
our experts at
<https://codefresh.io>

Questions?

(Want to know why are logs called logs? Hit us on our chat at [Coralogix.com](https://coralogix.com))