## Introduction

The objective of this document is to understand the tools used for TikTok production environment monitoring. This document contains…

- Monitoring methods & tools
- Type of Grafana dashboards to be monitored
- ERT dashboard – high level idea
- ERT dashboard – detailing of each graph
  - Understanding of each graph
    - What to monitor
    - How to monitor
    - When to escalate
- iCinga alerts
- NewRelic alerts

| | |
|---|---|
| | |

# 1 Production Monitoring Methods & Tools

TikTok Production Monitoring entails observing overall health of various components deployed on TikTok Production Server. In case of any abnormalities in the System Health Indicators and/or threshold breach of critical metrics, ER Team is required to notify the relevant teams on Skype group as well as escalate to Duty Manager/Escalation Manager as per the guidelines.

Following tools are used by ERT team to monitor TikTok Production Server.

I. **Graffana**: This is a Graphical Monitoring UI tool, which comprises of System Health Indicators and other business critical metrics. ERT is required to continuously monitor the multiple dashboards installed on Graffana.

II. **iCinga Email Alerts**: iCinga tool sends email alerts when a critical metrics crosses the defined thresholds.

III. **NewRelic Monitoring Tool**: This tool provides in depth performance details of the various components deployed on the production server. It sends email notification only in case of critical issues (real P1/P2 issues).

Graffana, NewRelic and iCinga are being used by TikTok for production monitoring. ERT team will also start monitoring the NewRelic tool in near future.

## 1.1 iCinga Alerts

iCinga tool sends email alerts when a critical metrics crosses the defined thresholds.

Four types of severity raised via this iCinga tool, Sev-1 to Sev-4.

- Whenever Sev-1 or Sev-2 type of alert raised, IT HD team notifies it on Sev-1 Skype group. Concerned team (MSO) works on the alert and tries to fix it. IT HD team keep track of it and closely work with concern team to close the alert.
- Sev-3 & Sev-4 alerts are directly assigned to MSO team and they work on it and take it towards closure. IT HD team does not involve in it.

| | |
|---|---|
| | |

**Note**: Initially the alert was coming from IT Group hd@sasf.com, but now after migration it has started coming via GTS gts@asdasd.com

## 1.2 NewRelic Alerts

This tool provides in depth performance details of the various components deployed on the production server. It sends email notification only in case of critical issues (real P1/P2 issues).

- This alert is very critical as the alert raised in case of P1/P2 issues.
- Inform L2 team to check fallouts if any
- If alert is for 3rd party then inform TikTok to check if any issue or planned activity is in progress

1. **Handling NewRelic Alert:**

   If any NewRelic alert turns out to be real issue having some impact (*High no. of errors, Performance degradation, KPI crossing thresholds),* we need to check if any old ticket already exists for that issue –
   - **If ticket exists with status OPEN**: update the ticket with new occurrence and details
   - **If old ticket exists with status CLOSED**: Reopen the ticket and update with new occurrence details
   - **If ticket doesn't exist**: open a new ticket after collecting the issue details (from NewRelic tool /Greylog), logs (if required as advised by Duty manager, seek MSO help to collect the logs)

2. **Creation of ticket**:
   - Consult with the duty manager about the issue
   - If issue is related to performance impact (*CPU utilization is high, High DB response time, High eCare response time*) :

     → Create a **GTS ticket** and assign to ***XYZ***
   - If issue is functional (High no of business/application errors) :

     → Create a **TMS ticket** and assign to ***(L2 lead)***. Also inform L2 TOMS person in shift about the ticket

This is to note that we will receive two emails of each alert, with Opened & Closed state.

**Sample alert screenshot**: Same alert with **Opened** & **Closed** state.

| | |
|---|---|
| | |

## 2 Alert Incoming Sources

ERT has to take action for any alert coming from below sources –

- **ERT dashboard** :
  - Any System Health Indicator turning to **Yellow** or **Red** or **Purple**
  - Any threshold breach (crossing the **WARNING** or **CRITICAL** line) on the KPI graphs

- **Mailbox** : NewRelic email alert

- **Skype/Viber group** : Any issue reported on the group either by Vendor management or TikTok IT/business

| | |
|---|---|
| | |

# 3 Grafana Dashboard Monitoring

Grafana is a graphical monitoring tool. This tool comprises of System Health indicators and other business critical metrics.

There are multiple dashboards available in Grafana tool to monitor health of system, portal, database, 3rd party solution response etc.

We will be mainly focusing on below two dashboards:

1) **TikTok Health Dashboard**:
   - This dashboard contains System Health indicators and around 90+ other graphs.
   - It also includes the number of “Active Subscribers” and “Sales Orders”
   - This dashboard is extended one where system, portal, database, sessions, TBAPI etc. all information available.
   - Below is the link to access TikTok Health dashboard.
     Dashboard

2) **TikTok ERT Dashboard**:
   - This dashboard contains System Health indicators and **CRITICAL** business KPI metrics which needs to be closely monitored.
   - The System Health indicators are related to LB (load balancer), DB, 3rd party integrations and about application nodes.
   - Critical KPIs like, portal response, DB & App CPU utilization & responses, Hogging threads & stuck threads etc.
   - Below is the link to access TikTok ERT dashboard.
     Dashboard

| | |
|---|---|
| | |

## 3.1 TikTok ERT Dashboard

As mentioned above, ERT dashboard is very critical and contains important metrics and system health indicators.

The dashboard is divided into two parts

1) **System Health Indicators**
2) **ERT Dashboard KPIs (Graphs)**

### 3.1.1 System Health Indicators:

System health indictors shows the current state of a system.

The indicators are for

1. **LB (load balancers)**: The accessibility of corresponding components from the load balancer.
2. **DB Health**: Health check of BSS Database Components.
3. **3p integrations**: Connectivity checks from BSS to 3rd Party Integrations
4. **Health**: Health check of the BSS individual node of particular component
5. **Sanda Health**

**The indicator color changes if there is an issue observed. ERT has to take action if** -

- Any System Health Indicator turning to **Yellow** or **Red** or **Purple**

Sometimes the indicators automatically turns back to Green from Red or Purple.

If any System Health Indicator is **Yellow** or **Red** or **Purple**

- Click on the indicator box, which would open iCinga dashboard, verify if the process status is yellow or red or purple there as well
- If it's Green, go back to the ERT dashboard, refresh and verify if the indicator turns back to green
- If it's Yellow/Red/Purple, click on the process box and "*Check now*" link on the process dashboard. Repeat this 3-4 times with a gap of few sec. If the status turns back to Green, go back to the ERT dashboard, refresh and verify if the indicator turns back to green
- If the status remains Yellow/Red/Purple even after multiple refresh, follow Alert Handling Procedure.