

Mock Interview: Prometheus + Grafana + Alertmanager + Slack

1. Prometheus

Q1: Prometheus là gì?

A1: Prometheus là hệ thống giám sát mã nguồn mở, thu thập và lưu trữ dữ liệu dạng time-series (theo thời gian) từ các target thông qua HTTP pull model.

Q2: Prometheus thu thập dữ liệu như thế nào?

A2: Prometheus định kỳ “scrape” (kéo) dữ liệu từ các endpoint có định dạng /metrics (ví dụ từ Node Exporter). Dữ liệu được lưu vào TSDB (Time Series Database).

Q3: Scrape interval là gì?

A3: Là khoảng thời gian giữa hai lần Prometheus thu thập dữ liệu từ target (ví dụ 15s, 30s...).

Q4: PromQL là gì?

A4: PromQL là ngôn ngữ truy vấn của Prometheus, cho phép lấy, tổng hợp, tính toán và hiển thị dữ liệu metric.

Q5: Prometheus xử lý alert như thế nào?

A5: Prometheus đánh giá các biểu thức cảnh báo (alert rules) trong file `alert_rules.yml`. Khi điều kiện đúng, Prometheus gửi alert đến Alertmanager.

2. Node Exporter

Q6: Node Exporter là gì?

A6: Là một agent chạy trên máy chủ, thu thập các metric hệ thống như CPU, RAM, disk, network và expose tại port 9100 cho Prometheus.

Q7: Tại sao cần Node Exporter?

A7: Vì Prometheus không trực tiếp thu thập metric từ OS. Node Exporter giúp cung cấp các thông tin chi tiết về hiệu năng hệ thống.

3. Alertmanager

Q8: Alertmanager có vai trò gì?

A8: Alertmanager nhận các alert từ Prometheus, quản lý, gộp nhóm (grouping), giảm nhiễu (deduplication), và gửi đến các kênh thông báo như Slack, email...

Q9: Tại sao cần Alertmanager thay vì gửi trực tiếp từ Prometheus?

A9: Vì Alertmanager giúp tránh spam, gom nhóm alert cùng loại và cung cấp nhiều phương thức thông báo linh hoạt.

Q10: File cấu hình chính của Alertmanager là gì?

A10: Là `alertmanager.yml`, chứa cấu hình route, receiver, webhook, Slack channel...

Q11: Route trong Alertmanager dùng để làm gì?

A11: Route quyết định alert nào được gửi tới receiver nào (ví dụ gửi warning tới Slack, critical tới email).

4. Slack Integration

Q12: Làm sao để tích hợp Alertmanager với Slack?

A12: 1. Tạo Slack App tại <https://api.slack.com/apps>

2. Kích hoạt Incoming Webhook

3. Sao chép URL Webhook

4. Thêm vào phần `api_url` trong `alertmanager.yml`

Q13: Slack Webhook hoạt động thế nào?

A13: Khi có alert, Alertmanager gửi POST request chứa JSON message đến Slack Webhook URL → Slack hiển thị thông báo trong kênh.

5. Grafana

Q14: Grafana là gì?

A14: Là công cụ visualization, giúp hiển thị dữ liệu từ Prometheus bằng biểu đồ, dashboard trực quan.

Q15: Làm sao để kết nối Grafana với Prometheus?

A15: Trong Grafana → Configuration → Data Sources → Add Prometheus → URL: `http://localhost:9090`.

Q16: Dashboard ID 1860 là gì?

A16: Là dashboard mẫu "Node Exporter Full" — hiển thị CPU, RAM, Disk, Network... phổ biến cho monitoring server.

6. Alert Flow

Q17: Mô tả luồng cảnh báo từ đầu đến cuối.

A17: 1. Node Exporter thu thập metric hệ thống.

2. Prometheus scrape dữ liệu từ Node Exporter.

3. Prometheus đánh giá rule → tạo alert nếu điều kiện đúng.

4. Alert được gửi đến Alertmanager.

5. Alertmanager gửi thông báo qua Slack.

6. Grafana hiển thị biểu đồ realtime.

Q18: Khi CPU cao, cảnh báo hoạt động thế nào?

A18: Prometheus phát hiện CPU > 80% trong >2 phút theo rule → tạo alert `HighCPUUsage` → Alertmanager → Slack notification.

7. Thực hành & Kiểm thử

Q19: Làm sao kiểm tra Prometheus đang hoạt động?

A19: Truy cập `http://localhost:9090` và vào mục Targets để xem danh sách job đang được scrape.

Q20: Cách test alert bằng công cụ?

A20: Dùng `stress --cpu 8 --timeout 300` để tăng tải CPU, sau vài phút alert sẽ kích hoạt.

8. Tổng hợp kiến thức

Thành phần	Port	Vai trò
Prometheus	9090	Thu thập & đánh giá metric
Node Exporter	9100	Cung cấp metric hệ thống
Alertmanager	9093	Quản lý và gửi cảnh báo
Grafana	3000	Hiển thị dashboard
Slack	—	Nhận thông báo

✓ Mẹo phòng vấn: - Hãy mô tả **luồng dữ liệu giám sát** từ Node Exporter → Prometheus → Alertmanager → Slack → Grafana.

- Nắm rõ file cấu hình: `prometheus.yml`, `alert_rules.yml`, `alertmanager.yml`.
 - Biết dùng `PromQL` để viết biểu thức giám sát CPU, Memory.
 - Giải thích lý do tách Alertmanager khỏi Prometheus (độc lập, linh hoạt).
 - Biết cách test alert thực tế bằng `stress`.
-

Tài liệu khuyên đọc thêm: - <https://prometheus.io/docs/introduction/overview/> - <https://grafana.com/docs/> - <https://prometheus.io/docs/alerting/latest/alertmanager/> - <https://api.slack.com/messaging/webhooks>