7: Monitoring Framework

WHY THIS FRAMEWORK IS IMPORTANT

Ephemeral clusters and oscillating applications make monitoring your Kubernetes environment health tricky.

This framework focuses on tools for visualization, tracing, and alerting. You may need multiple frameworks if monitoring is different between Production, Development, QA, and etcd.

EXERCISE

2 Hours

Medium Difficulty

Enterprise Architect
Head of Operations
Security Manager

What solution is used to collect container logs?

- □ Fluentd
- □ Graylog
- □ Loki
- □ Logstash
- □ Other

What solution is used to visualize logs?

- □ Grafana
- □ Kibana
- □ Other

Do you use role based access control for different users?

- □ Yes
- □ No
- □ Unknown

What solution is used within clusters for general system health?

- □ Prometheus
- □ Dynatrace
- □ Datadog
- □ Sysdig
- □ Cloud native tools
- □ Icinga/Nagios
- □ EFK
- □ Jaeger
- □ Splunk
- □ Other _______________

What is the maximum time between an issue occurring and monitoring system awareness?

□ Less than 1 minute
□ 1 - 10 minutes
□ 10 - 60 minutes
□ Unknown

Does the notification speed meet organizational expectations?

□ Yes
□ No

Is there an external monitoring solution being used to ensure internal infrastructure monitoring is operational?

□ Yes
□ No

Have full length tests been run to ensure all health checks work as expected?

□ Yes
□ No

Does a reduction in systems performance cause a financial concern to require an application performance monitoring (APM) solution?

□ Yes
□ No

If yes, has a financial analysis been performed?

□ Yes
□ No

What APM tool is used currently?

□ Dynatrace
□ AppDynamics
□ Instana
□ Sysdig
□ Cloud native tools
□ New Relic
□ Datadog
□ AWS Cloudwatch
□ Grafana
□ Other

Does the current APM solution monitor all interconnected systems & services residing both in and out of Kubernetes?

□ Yes
□ No

Has the current APM solution been configured beyond the default settings to fully optimize MTTR (mean-time-to-resolution)?

□ Yes
□ No

Is there a separate tracing solution currently in place? If so, what solution is it?

□ Yes ____
□ No

What solution is being leveraged within clusters to gather container metrics?

□ Dynatrace
□ AppDynamics
□ Instana
□ SumoLogic
□ Splunk
□ New Relic
□ Datadog
□ ELK Stack
□ Prometheus + Grafana
□ Other

What solution/s is currently being used to visualize metrics?

□ APM/Metric Solution
□ Grafana
□ Other___________________________________

Is a centralized incident management/alert aggregation system in place? If so, what is it?

□ Yes_____________________________________
□ No

Are alerts from each monitoring system shipped to your centralized management system?

□ Yes
□ No

Is a backup/redundancy system in place for shipping alerts if the primary does not respond?

- □ Yes
- □ No

Is there a formalized process to triage incidents?

- □ Yes
- □ No

Is there a solution to monitor, manage & observe kubernetes workloads across multiple clusters?

- □ Yes
- □ No

NEXT STEPS

Count the number of times you answered “Yes” and compare it to the number of times you answered “No.” This will give you a sense of how well your Cloud, Clusters, Containers and Code is monitored to ensure Kubernetes environment health.

If you identify multiple tools in place, don’t be concerned. These tools can be rationalized with a comprehensive monitoring system that can scale with ease.