Observability

[observability-guide.pdf (lightstep.com)](#)

[The Open Source Observability Landscape (honeycomb.io)](#)

[A Guide to Open Source Monitoring Tools | Logz.io](#)

Observability vs Monitoring

Three pillars of Observability (Logging, Distributed Tracing, Metrics)

Monitoring / SRE

[Google - Site Reliability Engineering (sre.google)](#)

Diagnosing and Fixing problems in production

Service Level Objectives (SLOs)

Service Level Indicators (SLIs)

Service Level Agreement (SLAs)

Site Reliability Engineer (SRE)

MTTR (Mean Time to Recovery), MTTI

What is Error Budgets

The Four Golden Signals

Distributed Tracing

[Distributed Tracing: A Complete Guide (Updated for 2021) (lightstep.com)](#)

[Distributed tracing for dummies | Java Code Geeks - 2021](#)

[Distributed Tracing with Zipkin - javatpoint](#)

[How to Implement Distributed Logging & Tracing using Sleuth & Zipkin? | Making Java easy to learn (javatechonline.com)](#)

[Spring Cloud Zipkin and Sleuth Example - HowToDoInJava](#)

[Monitoring Microservices With Spring Cloud Sleuth, ELK, and Zipkin - DZone Performance](#)

Logging using ELK\EFK

[(K8S) Logging in Kubernetes with EFK Stack | The Complete Guide by Nana Janashia. 18/11/20 - YouTube](#)

[The Complete Guide to the ELK Stack | Logz.io](#)

[How to monitor distributed logs in Kubernetes with the EFK stack. | by Christiaan Vermeulen | Medium](#)

Observability

Monitoring concepts

Q: What is white-box monitoring? A: White box monitoring is where you know the internals of the system. And the system has instrumentation in place to emit telemetry—metrics, logs, traces, etc (https://www.scalyr.com/blog/black-box-monitoring-track-opaque-systems/)

Q: What is black-box monitoring? A: Black box monitoring is where you don't have control and don't know what's happening inside the system. You only monitor the system from the outside—its behavior. (https://www.scalyr.com/blog/black-box-monitoring-track-opaque-systems/)_

Q: What is the purpose of external monitoring? A: To ensure that your users can access your website (and that performance is acceptable). External monitoring helps detect CDN/ ISP issues.

Q: What are some factors to consider with external monitoring? A: Cost (usually there is a cost to each test and/ or frequency). Ensuring that you do not DOS systems.

Q: Explain TTD, TTR and the importance of measuring it? A:

> TTD: Time to detect
> TTR: Time to resolve
> Measuring these provide Key Performance Indicators (KPI) if your incident response is improving

Distributed Tracing

Q: What are the benefits of distributed tracing? A: You can get rich signals into where things are unhealthy in your system

Q: What are some of the challenges with distributed tracing? A: Sampling, bias.

Human-Ops

Q: How to you detect alert fatigue? A: Report on how many alerts are firing for each team/ service

Auto-remediation

Q: Describe the pros of an auto-remediation system? A:

> Can be used to remediate live-sit incidents
> Can be used to perform automatic investigation during live-site incident

Q: Describe the cons of an auto-remediation system? A:

Can easily hide issues that get swept under the rug

Q: What are the key features of an auto-remediation system? A:

Ability to deploy
Ability to auto-scale
Ability to perform remote-execution
Ability to query monitoring/ alerting sources

Postmortems

Q: What is the purpose of postmortems? A: Understand all contributing root causes, document the incident for future reference and pattern discovery, and enact effective preventative actions to reduce the likelihood or impact of recurrence.

Q: How do you practice blameless postmortems? A:

Incident postmortems focused on growth – without the blame game. ...
Communicate an open, mistake-friendly approach up front. ...
Encourage honesty and acceptance of failure. ...
Share information and build a timeline. ...
Be consistently blameless. ...
Get C-suite buy-in. ...
Collaborate. ...
Make decisions, but get approval.

Q: What methods would you use to ensure postmortems are being held? A:

Domain Name System (DNS)

Virtualization, Containers, and Kubernetes

Cloud Computing vs Cloud Native

Databases

Relational –

MySQL, Postgres, Oracle and so on.

NoSQL-

Key/value Stores: Cassandra, etcd, Memcached and MemcacheDB, Redis

Document stores: CouchbaseDB, MongoDB

Graph stores: Neo4j, OrientDB

[Top Prometheus Interview Questions and Answers (2021) | TechGeekNxt >> (techgeeknext.com)](techgeeknext.com)

[Top Prometheus Interview Questions (2021) | CodeUsingJava](CodeUsingJava)