[Disaster Recovery]

↳ Ability to restore access, functionality to IT infrastructure after disaster event -

↳ Machine failure

↳ power outage, fire, explosion

↳ Natural disasters.

How disaster recovery works

Disaster recovery relies on having a solid plan to get critical applications and infrastructure up and running after an outage—ideally within minutes.

An effective DR plan addresses three different elements for recovery:

- **Preventive:** Ensuring your systems are as secure and reliable as possible, using tools and techniques to prevent a disaster from occurring in the first place. This may include backing up critical data or continuously monitoring environments for configuration errors and compliance violations.
- **Detective:** For rapid recovery, you'll need to know when a response is necessary. These measures focus on detecting or discovering unwanted events as they happen in real time.
- **Corrective:** These measures are aimed at planning for potential DR scenarios, ensuring backup operations to reduce impact, and putting recovery procedures into action to restore data and systems quickly when the time comes.

Types of disaster recovery

The types of disaster recovery you'll need will depend on your IT infrastructure, the type of backup and recovery you use, and the assets you need to protect.

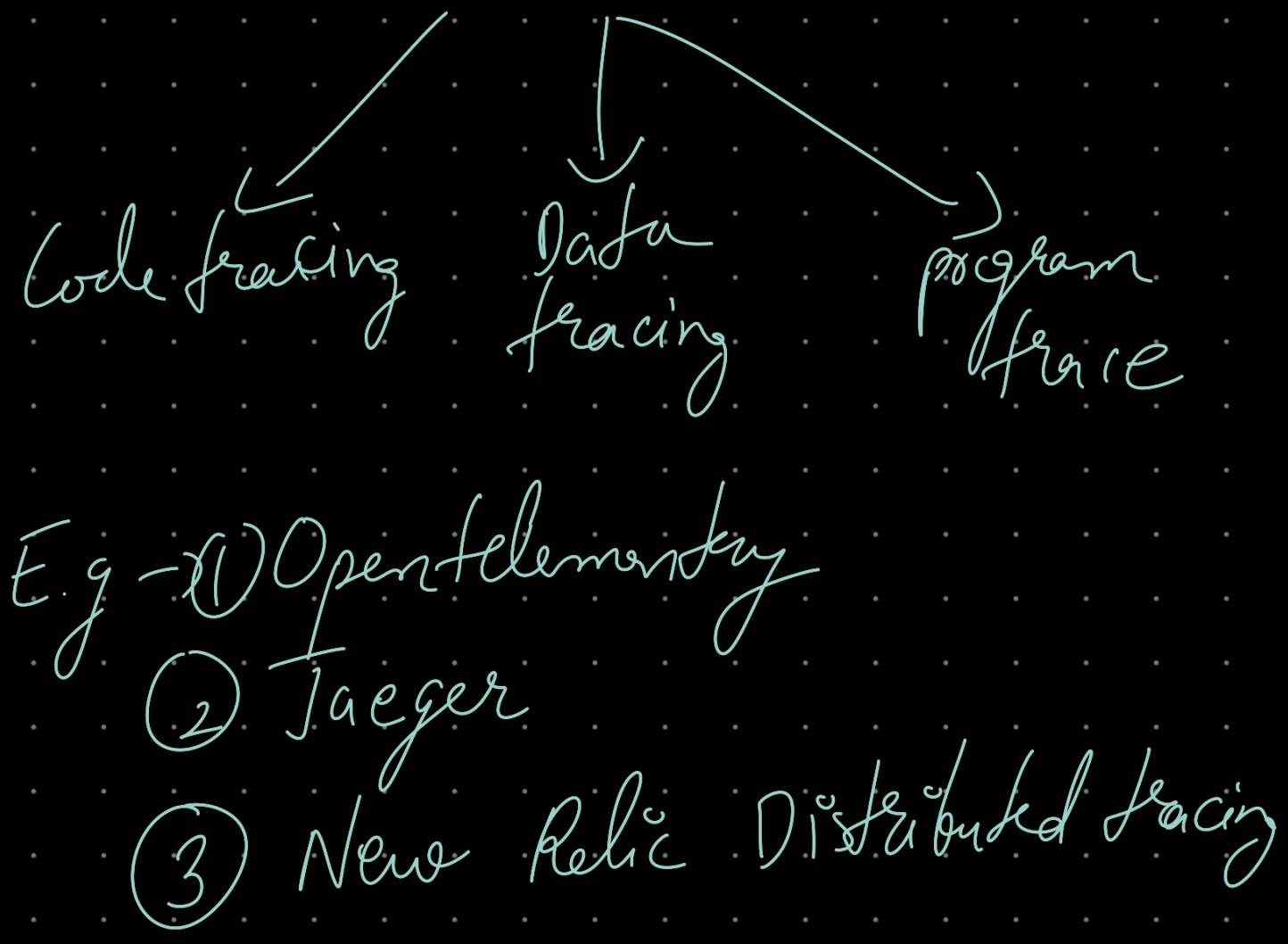
Here are some of the most common technologies and techniques used in disaster recovery:

- **Backups:** With backups, you back up data to an offsite system or ship an external drive to an offsite location. However, backups do not include any IT infrastructure, so they are not considered a full disaster recovery solution.
- **Backup as a service (BaaS):** Similar to remote data backups, BaaS solutions provide regular data backups offered by a third-party provider.
- **Disaster recovery as a service (DRaaS):** Many cloud providers offer DRaaS, along with cloud service models like IaaS and PaaS. A DRaaS service model allows you to back up your data and IT infrastructure and host them on a third-party provider's cloud infrastructure. During a crisis, the provider will implement and orchestrate your DR plan to help recover access and functionality with minimal interruption to operations.
- **Point-in-time snapshots:** Also known as point-in-time copies, snapshots replicate data, files, or even an entire database at a specific point in time. Snapshots can be used to restore data as long as the copy is stored in a location unaffected by the event. However, some data loss can occur depending on when the snapshot was made.
- **Virtual DR:** Virtual DR solutions allow you to back up operations and data or even create a complete replica of your IT infrastructure and run it on offsite virtual machines (VMs). In the event of a disaster, you can reload your backup and resume operation quickly. This solution requires frequent data and workload transfers to be effective.
- **Disaster recovery sites:** These are locations that organizations can temporarily use after a disaster event, which contain backups of data, systems, and other technology infrastructure.

[Distributed Tracing]

* Capturing and recording information about a request which traverse through Different Services in Distributed architecture.

* In Monolithic, it's easier. It difficult to find fault in Distributed Service



Example Workflow

Imagine a web application with three microservices:

1. **Frontend Service**
2. **Backend Service**
3. **Database Service**
4. A user sends a request to the **Frontend Service**.
5. The frontend makes a call to the **Backend Service**, which in turn queries the **Database Service**.
6. Each service logs a span for its work:
    - Frontend logs a span for handling the request.
    - Backend logs a span for its API logic.
    - Database logs a span for the query execution.
7. The trace ID is propagated across services so all spans can be correlated into a single trace.
8. The tracing system visualizes the trace, showing how long each service took and where any errors occurred.