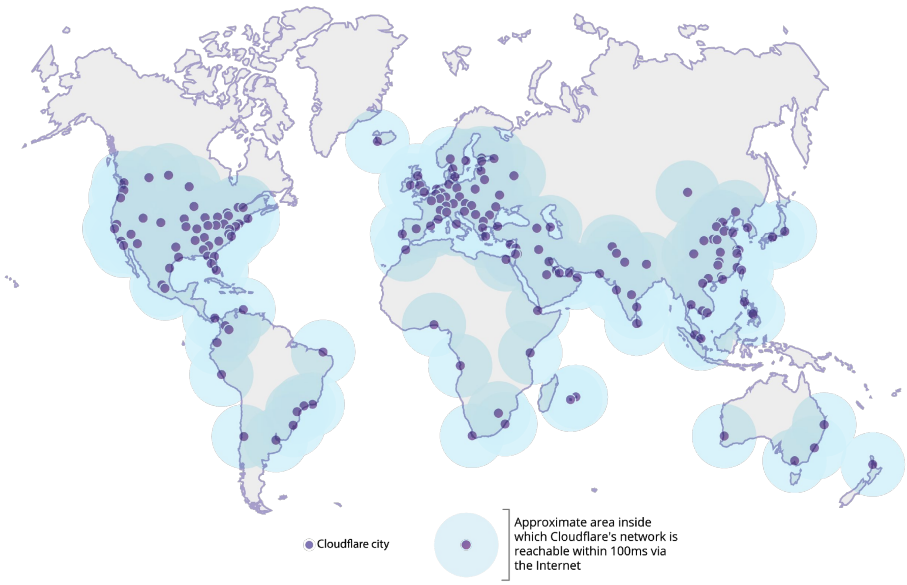
Cloudflare Disaster Recovery Overview

Global Distributed Network Overview

Cloudflare's edge network is designed to be resilient and fault tolerant. Our network of 200+ Points of Presence (PoPs) represent a true N+1 architecture where the failure of an individual PoP, or even several PoPs, will not compromise our fulfillment of services. Cloudflare employs Anycast routing to ensure web users are automatically routed to their nearest PoP and around any failures. The combination of this architecture and network produces a reliable, high-performance service. For up-to-date information related to the status of the sites, please visit cloudflarestatus.com



Disaster Recovery

With Cloudflare's resilient global network, the disaster recovery plan is focused on our Core Data Centers which are located in the West Coast of the United States and in the European Union. Core Data Centers house critical services including customer dashboard settings, product configurations, logs and analytics.

The geographically separate Core Data Centers allow Cloudflare Services to have continued operations from an adverse event. The Core Data Center located in the West Coast (US) is an active data center. In the event of a disaster that affects the active data center, Cloudflare will failover and continue operations from the EU data center.

Core Data Center Replications and Backups

Critical services are replicated between Cloudlfare's Core Data Centers. During an adverse event, data can be sourced from any of the data center locations.

As an additional measure, databases are backed up daily and to an off-site location to ensure that Cloudflare has the ability to fully restore customer configurations if an adverse event impacted all of Cloudflare's Core Data Centers (US and EU).

Plan and Failover Tests

Cloudflare maintains a disaster recovery plan and performs testing and exercises on at least an annual basis to ensure recovery preparedness. The annual test stimulates a disaster and performs a cutover test by interrupting the replication between the two Core Data Centers and testing the ability to sufficiently restore the services in the EU. Test results are documented and reviewed by the Technical Teams.

The last annual DR exercise and tests was conducted in December 2019. The Technical Teams were able to successfully restore critical services from the Core Data Center in the EU and met the established Recovery Point Objective (RPO) and Recovery TIme Objective (RTO).

For More Information

If you have more questions related to Cloudflare's architecture or disaster recovery capabilities, please contact the Cloudflare team at support.cloudflare.com