Reliability & Security

At Gelato, we are committed to upholding industry-standard best practices to guarantee the reliability and availability of our services. Our systems are designed with High Availability (HA) and fault tolerance as fundamental principles, resulting in a resilient and robust infrastructure. This approach is essential for mitigating service disruptions and guaranteeing consistent performance.

Reliability

Multi-cloud

All Gelato infrastructure benefits from a multi-cloud and multi-region strategy, distributed globally across various clouds and regions. Our approach guarantees operational continuity, enhancing stability against regional variances, optimizing response times, and delivering a seamless experience to users worldwide.

Data Recovery

Ensuring maximum data preservation and maintaining the safety and security of your operations, even in unforeseen circumstances.

Autoscaling RPC nodes

We dynamically adjust resources to match your transaction volume and deliver best-in-class performance.

Response times & Escalation Guidelines

Effective and timely response and resolution are key to maintaining our high service reliability. We prioritize incidents and issues based on their urgency and define response times accordingly. Our response time framework is as follows:

P1 (High Priority): 2 business hours response

P2 (Medium Priority): 6 business hours response

P3 (Low Priority): 8 business hours response

Internal Alert System

Our system effectively triggers alerts and pages relevant personnel for immediate action. It is crucial for our operations, providing dependability and swift response capabilities.

Security

Multi-Signature Rollup Security

Gelato employs a multi-signature system for managing its rollup contracts, necessitating consensus among multiple team members for critical decisions. It enhances security by distributing authority, thus safeguarding the system and user funds even in scenarios of potential compromise.

Secure Encryption

All communications and data transfers, including hot wallet keys, are fully encrypted to ensure comprehensive protection.

Advanced Security for Key Management

Advanced security methods are employed to manage keys and secrets, to ensure a secure and tightly controlled access to sensitive data. This ensures safe key injection into applications without direct access by the provider.

DDoS Protection

Protect your rollups from hostile attempts to overwhelm your public RPC endpoints with traffic. This robust defense mechanism safeguards against malicious attacks, ensuring the security and availability of your system

Previous Avail Next Scaling Solutions Wiki Last updated2 months ago On this page *Reliability * Multi-cloud * Data Recovery * Autoscaling RPC nodes * Response times & Escalation Guidelines * Internal Alert System * Security * Multi-Signature Rollup Security * Secure Encryption * Advanced Security for Key Management * DDoS Protection