

# Incident Feb 6, 2023: FastStore WebOps Outage

Availability: **All accounts that use FastStore as their storefront.**

% of clients affected: **less than 0.5%**

Duration of incident: **40 minutes, 26 minutes of stores' downtime.**

## Symptoms

From 15h30 UTC to 16h10 UTC, FastStore WebOps faced an outage caused by its Router service. FastStore WebOps is the underlying platform where clients using FastStore deploy their stores.

## Summary

At 15h30 UTC, our alerts triggered downtime in several stores on FastStore WebOps. We immediately identified that we were facing a complete outage on the platform.

At 15h40 UTC, we identified that our router service had been deleted, and we promptly started the restore process. Meanwhile, we opened a separate investigation to map what happened. At 15h48 UTC, we finished the main cluster mitigation and started restoring other support infrastructure.

At 15h56 UTC, FastStore traffic was restored, but a secondary service used to serve optimized images was still unreachable. At 16h10 UTC, our image optimizer service was restored.

Later, we identified that a manual deletion process was triggered at 15h17 UTC to remove unused router components on the underlying infrastructure. The removal process accidentally removed active routers from our FastStore WebOps clusters.

For us to continue to be the trusted partner to the success of our clients, our team is working on follow-up actions (*see the section below*) to ensure that this incident does not

happen again and that we identify and recover from future incidents faster. We are committed to improving our systems to guarantee a reliable and trusted platform.

## Timeline

**[2023-02-06 15:17 UTC]** During the removal of unused routers services, some still-in-use routers were inadvertently removed due to the incomplete information our clouder provider portal provided regarding the router's activeness.

**[2023-02-06 15:30 UTC]** Automated alarms used to monitor the status of production stores triggered an automated incident.

**[2023-02-06 15:40 UTC]** Internal communication between the team that removed the load balancers and the team responsible for hosting FastStore ensured a quick understanding of what was happening, and the removed load balancers were reprovisioned.

**[2023-02-06 15:48 UTC]** Most DNS records and CDN servers automatically picked up the newly spun routers, but we needed to execute other manual configurations.

**[2023-02-06 15:56 UTC]** Store traffic was restored, but a secondary service used to serve optimized images was still unreachable.

**[2023-02-06 16:10 UTC]** Our image optimizer service was restored.

**[2023-02-06 16:10~16:50 UTC]** Secondary services such as Faststore CI/CD, Faststore previews, Sonarqube, and Lighthouse were restored.

## Mitigation strategy

We reestablished normal operation of the platform by reprovisioning the removed routers services and, when necessary, manually updating DNS entries and CDN configurations, beginning with the most critical services (production servers, image hosting) and then in descending order of priority.

## Follow-up actions: preventing future failures

After the incident, we mapped important follow-up actions to avoid this incident from happening again:

- Launch our automated infrastructure provisioning system this quarter, ensuring the timely removal of unused routers, which would completely remove the need for manual housekeeping.
- Review services that still require manual updates to DNS entries to recover from such a scenario. The infrastructure for automatic DNS updates is already in place and used by most services.
- Explore the feasibility of self-healing routers.