



Major Incident Report – Core Banking Server Outage

Organization: Bank of Ontario
Incident ID: BOO-IT-2024-0231
Reported By: Dana Iqbal, Director of IT Operations
Incident Start: August 14, 2024 – 03:41 AM EST
Resolved: August 14, 2024 – 11:58 AM EST
Status: Resolved
Severity: Critical
Prepared On: August 21, 2024
Reviewed By: CIO Office, Cybersecurity & Risk Board

1. Executive Summary

On **August 14, 2024**, Bank of Ontario experienced a **critical infrastructure outage** affecting its **core banking backend cluster** hosted in the **primary Toronto datacenter**. This incident resulted in **widespread customer-facing service disruption** from 3:41 AM to 11:58 AM EST. Approximately **100,000 retail customers** were unable to access their online banking accounts, ATMs, or perform transactions via mobile apps during the disruption window.

The root cause was determined to be a **corrupted shared filesystem** on a core **NFS-based mount point** used by both customer session services and core transaction processing containers. The situation was aggravated by a **missing failover rule** in the container orchestrator’s health checks, preventing automatic relocation to the secondary DR site.

2. Incident Impact Summary

Area Affected	Description
Customer Access	100,000+ customers unable to access bank accounts
ATM & POS Services	27% of ATM network showed degraded service; Interac POS failed for some

Online & Mobile Banking	Outage persisted for over 8 hours
Customer Support	Contact center received 11,400+ support calls during outage window
Business Losses	Estimated financial impact: CAD \$1.1M in missed FX transactions, delayed settlements, and compensation
Reputational Risk	Significant complaints on social media and news coverage on CBC Business

3. Timeline of Events (All times EST)

Time	Event
03:41 AM	Automated monitoring alert: <code>/core-fs-mnt</code> not responding on node <code>cb-trx-07</code>
03:43 AM	Container orchestrator fails 3 pods but fails to relocate others due to bad liveness probe syntax
04:00 AM	Tier 1 NOC escalates to Platform Ops and Infra Lead
04:30 AM	Internal app health checks begin failing on <code>/auth</code> , <code>/balance</code> , <code>/transaction</code> endpoints
05:10 AM	Failover to DR site attempted manually—blocked by live socket lock on stale NFS mount
07:00 AM	Deloitte SRE consultants brought in for filesystem recovery
08:30 AM	Corrupted inode map identified on NetApp NFS cluster due to crash from expired firmware bug
09:15 AM	Hot patch applied to NetApp and partial rehydration started from hourly snapshot
10:52 AM	Stale locks cleared; orchestrator instructed to reinitiate container migration to DR
11:58 AM	All critical services restored; services online; customers able to log in

4. Root Cause Analysis (RCA)

Immediate Root Cause:

- **Filesystem corruption on NetApp NFS mount** used by `/core-fs-mnt` path, affecting Kubernetes pods tied to session and transaction layers.

Contributing Factors:

- **Expired firmware bug** (NetApp ONTAP 9.8P3) caused crash during routine volume deduplication.
- **Liveness probe** YAML misconfiguration in container health check prevented relocation.
- **DR failover blocked** by NFS stale lock, not accounted for in existing DR runbook.
- **No periodic integrity check** on the filesystem layer under high IOPS workloads.

5. Technical Diagnosis

Component	Finding
Kubernetes Cluster	Did not failover due to misconfigured <code>initialDelaySeconds</code> and <code>failureThreshold</code>
NetApp Filesystem	ONTAP firmware triggered known bug under <code>volume efficiency start</code> cron job
Alerting/Monitoring	Zabbix and Prometheus sent alerts, but orchestration self-healing failed
Service Dependencies	Hard mount prevented retry logic; lacked retry-with-timeout pattern in backend code

6. Resolution Summary

- Restored access via hourly NetApp snapshot on DR site
 - Cleared stale socket locks manually via NFS admin console
 - Corrected orchestration health probe configuration
 - Re-patched NetApp ONTAP firmware across HA cluster
 - Tested failover plan using Ansible-automated recovery post-incident
-

7. Financial Impact

Category	Cost
Missed transaction revenue	CAD \$430,000
SLA breach & service credits	CAD \$285,000
Customer compensation (credits/refunds)	CAD \$120,000
Deloitte SRE engagement	CAD \$80,000
Reputation management (PR & media)	CAD \$85,000
Total Estimated Loss	CAD \$1,100,000

8. Remediation Actions

Immediate Fixes

- Patched NetApp ONTAP firmware to 9.8P11 (per Cisco + NetApp advisory)
- Corrected Kubernetes liveness probe configuration and redeployed
- Added forced NFS timeout + lazy unmount on DR orchestration workflows

Medium-Term

- Implemented **Ansible-based DR runbooks** for NFS mounts, app redeploy, and DNS failover
- Added **chaos testing** (Gremlin) to simulate FS failures monthly
- Rolled out **Prometheus alert rule** for degraded NFS mount + latency deviation

Long-Term

- Upgrading to **container-native storage (Ceph)** for all critical stateful apps by Q4 2025
- Incorporate **immutable infrastructure** with GitOps pipelines for core banking apps
- Initiate monthly **disaster recovery drills with Red Hat Ansible Automation Platform**

9. Communication & Disclosures




Audience	Action Taken
Customers	Transparent update posted on website, mobile app, and email blast
Regulators	Notified FINTRAC and FSRAO (no mandatory reporting required due to no data loss)
Employees	Internal postmortem shared across Engineering, Ops, and Customer Experience teams
Media	Official response published via press release and social media handles

10. Lessons Learned

Lesson	Remediation
Reliance on shared NFS volume introduces cascading failure risk	Migrate to container-native storage with HA capabilities

Health checks must be tested for operational reliability	CI pipeline now includes runtime validation of YAML probes
DR workflows must include mount unblocking procedures	Automated using Ansible playbooks with NFS lock cleanup
Real-time customer communication is critical	CX team has prebuilt incident response templates for web & app

11. Sign-Offs

Name	Role	Signature
Amira Dosanjh	VP Cybersecurity Operations	
Dana Iqbal	Director of IT Operations	
Behnam Hajian	Principal Solutions Architect	
Kate Young	Deloitte Cyber Resilience Lead	