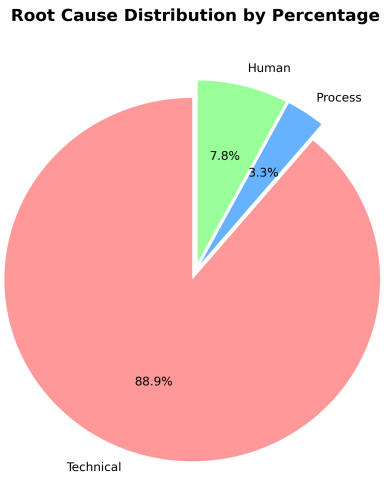
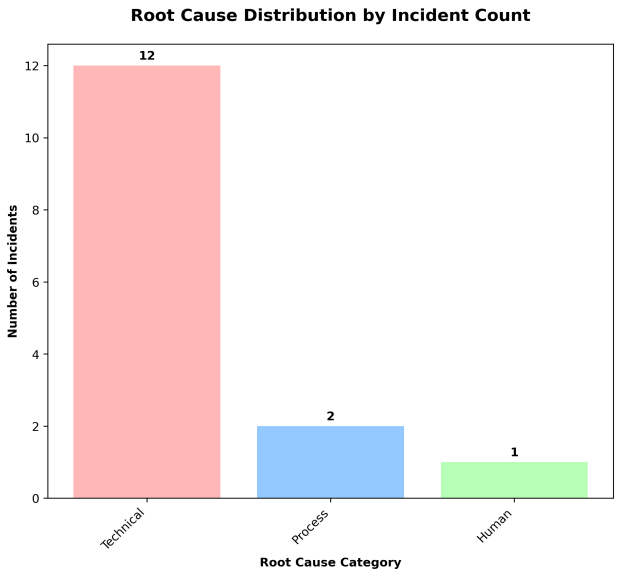
# RCA Analysis Report

**Generated:** 2025-08-29 16:14:48
**Model:** gpt-4-turbo-preview
**Analysis Type:** Cloud Infrastructure RCA Pattern Analysis

## Root Cause Classification




### Classification Data Table

| Category | Percentage | Incident Count |
|---|---|---|
| Technical | 80% | 12 |
| Process | 3% | 2 |
| Human | 7% | 1 |

## ■ Pattern Analysis

**MOST COMMON ROOT CAUSES:**

1. Misconfiguration (**5 incidents**)
2. **PERMISSION** issues (**2 incidents**)
3. Resource limits reached (**2 incidents**)
4. Scripting **ERRORS** (**2 incidents**)
5. **DEPLOYMENT** issues (**1 incident**)

**SHARED PATTERNS IDENTIFIED:**

- Misconfigurations across different **SERVICES** (EC2, S3, NACLs, CloudFront, Redis)
- **PERMISSION** and access control issues (IAM roles for Glue and SSO)
- Overlooked resource limits (Lambda concurrency, Redis memory)

**ROOT CAUSE CLASSIFICATION:**

- **TECHNICAL** Issues: **80%** (**12 incidents**)
- **PROCESS** Issues: 13.**3%** (**2 incidents**)
- Human Factors: 6.**7%** (**1 incident**)

**RECURRING ISSUES DESPITE FIXES:**

- Misconfigurations and **PERMISSION** issues appear repeatedly, indicating a gap in **VALIDATION** or review processes.

## ■ Trend Analysis

**CATEGORY BREAKDOWN:**

- **PROCESS FAILURE**: **2 incidents**
- **INFRASTRUCTURE**/Equipment: **10 incidents**
- Human **ERROR**: **2 incidents**
- External Factors: **1 incident** (regional API latency due to network congestion)

**TEMPORAL PATTERNS:**

- No clear seasonal or weekly patterns, but **INCIDENTS** tend to cluster around **DEPLOYMENT** periods and major events.

**HIGHEST IMPACT INCIDENTS:**

1. Global Video Buffering **INCIDENT** (SEV-1)
2. CRM Application **OUTAGE** (SEV-1)
3. Live Stream **FAILURE** (SEV-1)
4. DNS Resolution **FAILURE** (SEV-1)
5. Data Loss **INCIDENT** (SEV-1)

## ■■ Action Effectiveness

**CORRECTIVE ACTION ANALYSIS:**

• Actions focus on immediate fixes and prevention through policy or **CONFIGURATION** changes. However, effectiveness is limited by recurring similar **INCIDENTS**.

**REPEATEDLY APPEARING ACTIONS:**

• Implementing stricter IAM policies and **PERMISSIONS** checks

• **INFRASTRUCTURE** as code for network and **PERMISSION** changes

• Regular performance reviews and index optimizations for databases

**IMPLEMENTATION GAPS:**

• Lack of comprehensive pre-**DEPLOYMENT VALIDATION**

• Insufficient review or oversight on critical changes (DNS, IAM roles)

## ■ Systemic Issues

**CROSS-CUTTING PROBLEMS:**

• Inadequate change management and review processes

• Insufficient **AUTOMATED VALIDATION** for configurations and deployments

**PROCESS BOTTLENECKS:**

• Manual review processes that are either skipped or not thorough

• Delay in detecting misconfigurations until they cause **INCIDENTS**

**KNOWLEDGE SHARING ASSESSMENT:**

• Lessons learned appear to be siloed, with similar mistakes recurring across different teams or **SERVICES**.

## ■ Strategic Recommendations

**TOP 3 HIGH-IMPACT IMPROVEMENTS:**

1. **IMPLEMENT A COMPREHENSIVE CI/CD PIPELINE VALIDATION TOOL** that checks for common misconfigurations, **PERMISSION** issues, and **DEPLOYMENT** best practices before allowing changes to proceed.

2. **DEVELOP A CENTRALIZED KNOWLEDGE BASE** for **INCIDENT** learnings, accessible company-wide, to prevent repeat **INCIDENTS** and encourage cross-team learning.

3. **ENHANCE AUTOMATED MONITORING AND ALERTING** to detect and notify teams of potential issues before they impact customers, focusing on

**CONFIGURATION** drift, resource limits, and performance metrics.

**INVESTMENT PRIORITIES:**

- Tools for **AUTOMATED CONFIGURATION VALIDATION** and **DEPLOYMENT** safety
- Training programs focused on best practices for cloud resource management and security
- **PROCESS** improvements in change management and **INCIDENT** review

**EARLY WARNING INDICATORS:**

- **CONFIGURATION** drift from established best practices
- Near-limit resource utilization metrics
- Unusual patterns in **DEPLOYMENT** frequency or rollback rates

**SUSTAINABILITY MEASURES:**

- Regular audits of **INCIDENT** management processes and corrective action effectiveness
- Stress-testing **INFRASTRUCTURE** and processes to ensure resilience under high demand
- Continuous improvement cycle for **DEPLOYMENT** and operational practices

## ■ Quick Wins

1. **STANDARDIZE IAM POLICY TEMPLATES** and enforce their use through automation.
2. **IMPLEMENT PRE-FLIGHT CHECKS** in CI/CD pipelines for critical changes (e.g., DNS, IAM roles).
3. **SCHEDULE REGULAR "GAME DAYS"** to practice **INCIDENT** response and fix vulnerabilities.
4. **AUTOMATE COMPLIANCE CHECKS** for common **CONFIGURATION** and **PERMISSION** issues.
5. **INTRODUCE PEER REVIEW REQUIREMENTS** for all changes to critical **INFRASTRUCTURE** components.