LogZilla AI Copilot

InfraOps Analysis Report

Generated: December 6, 2025 17:30:00 EST | Analysis Period: Last 2 hours vs. 26-24 hours ago | Events: 120,883

QUERY PROMPT

"Analyze all infrastructure events from the last 2 hours compared to the same 2-hour window yesterday. Correlate storage failures, power supply events, RAID degradation, and capacity exhaustion across all systems. Predict potential outages and provide remediation commands."

Executive Summary

CRITICAL INFRASTRUCTURE EMERGENCY

The infrastructure is experiencing a **cascading failure** across multiple layers with **120,883 critical events** in the last 2 hours compared to **ZERO events** in the same window yesterday.

Severity Breakdown

Severity	Count	Percentage
ALERT (Severity 1)	1,876	2.5%
CRITICAL (Severity 2)	6,742	9.1%
ERROR (Severity 3)	37,914	51.1%
WARNING (Severity 4)	27,775	37.4%

Critical Findings

1. Storage Subsystem Failure

Buffer I/O Errors: 100+ events across multiple hosts

- jump-srv-01.company.com
- web-srv-01.company.com
- app-srv-01.company.com
- db-srv-01.company.com

RAID Array Degradation: 100+ events - Multiple disk failures (6-100 drives) across RAID arrays with vSAN disk groups being removed from clusters.

2. Database Layer Collapse

Error Code	Description	Impact
Error 2002	Connection/communication failures	Critical
Error 1045	Access denied	High
Error 1213	Deadlock conditions	Critical
Error 1205	Lock wait timeouts	High

3. Power Supply Failures

Network Infrastructure: 100+ events

- nexus-core-01 (187 events)
- nexus-core-02 (221 events)
- nexus-dist-01 (187 events)
- nexus-access-01 (213 events)

4. VMware Infrastructure Instability

vMotion Failures: 100+ events - Failed VM migrations correlate with storage controller battery degradation and RAID array degradation.

5. Capacity Exhaustion

Memory at 95%+ usage:

- order-processor (99%), search-api (99%)
- inventory-svc (99%), payment-api (96%)
- user-auth (96%), notification-svc (97%)

Risk Assessment Matrix

Component	Risk Level	Failure Probability	MTTR Estimate
Storage Subsystem	CRITICAL	Imminent (hours)	4-8 hours
Database Layer	CRITICAL	In Progress	2-4 hours
Power Infrastructure	CRITICAL	Imminent (hours)	1-2 hours
VMware Platform	HIGH	In Progress	2-4 hours
Network Core	HIGH	Imminent (hours)	1-2 hours

Predicted Outages (Next 4 Hours)

Imminent (0-1 hour)

1. **Complete database service failure** - Storage full conditions will cause database crashes
2. **Network core failure** - Power supply failures will cause switch failures
3. **ESXi host crashes** - Power supply and storage failures will cause hypervisor failures

Likely (1-2 hours)

4. **Complete VM infrastructure collapse** - ESXi failures will cascade to all VMs
5. **Storage array failure** - RAID degradation will progress to complete failure
6. **Firewall failover exhaustion** - HA synchronization failures will cause security gaps

---

Remediation Commands

PRIORITY 1: IMMEDIATE (Execute Now)

1.1 Free Database Disk Space

```
# On each database server
ssh root@db-master-01.company.com

# Emergency cleanup - remove old binary logs
mysql -e "PURGE BINARY LOGS BEFORE DATE_SUB(NOW(), INTERVAL 1 DAY);"

# Clear old slow query logs
> /var/lib/mysql/slow-query.log

# Check space
df -h /var/lib/mysql
```

1.2 Restart Critical Database Services

```
# Restart in order to clear locks and connections
ssh root@db-master-01.company.com
systemctl restart mysql

ssh root@postgres-01.company.com
systemctl restart postgresql

ssh root@redis-01.company.com
systemctl restart redis
```

PRIORITY 2: URGENT (Within 15 minutes)

2.1 Investigate Power Supplies

```
# Check power supply status on critical servers
for host in esxi-01 esxi-02 app-srv-01 db-srv-01 storage-01; do
  echo "=== ${host} ==="
  ssh root@${host}.company.com "ipmitool sensor list | grep -i 'PS\|Power'"
done

# For Cisco Nexus switches
```

```
ssh admin@nexus-core-01 "show environment power"
ssh admin@nexus-core-02 "show environment power"
```

2.2 Stabilize RAID Arrays

```
# Check RAID status on all affected hosts
for host in backup-srv-01 db-srv-01 nas-01 san-01 file-srv-01; do
  echo "=== ${host} ==="
  ssh root@${host}.company.com "cat /proc/mdstat"
  ssh root@${host}.company.com "mdadm --detail /dev/md0"
done

# If drives are marked as failed but physically OK
ssh root@db-srv-01.company.com
mdadm --manage /dev/md0 --re-add /dev/sda1

# Monitor rebuild progress
watch -n 5 'cat /proc/mdstat'
```

Root Cause Analysis

Primary Root Cause: Power supply failures across network and server infrastructure are triggering a cascading failure:

1. **Power failures** → Storage controller battery degradation
2. **Battery degradation** → RAID write cache disabled → I/O performance degradation
3. **I/O degradation** → Disk queue saturation → Buffer I/O errors
4. **I/O errors** → Database disk full → Storage engine failures
5. **Storage failures** → Application connection failures → Service outages
6. **ESXi storage issues** → vMotion failures → VM instability

> **IMMEDIATE ACTION REQUIRED:** This infrastructure is in a critical state and requires immediate intervention. Begin executing Priority 1 remediation steps NOW to prevent complete infrastructure failure.

Report Generated: 2025-12-06 17:30:00 EST

Analysis Period: Last 2 hours (15:30-17:30 EST)

Total Events Analyzed: 120,883