



Crash to Recovery: The PostgreSQL DBA's Emergency Playbook

Emre Baransel
Utku Demir

straDATA 



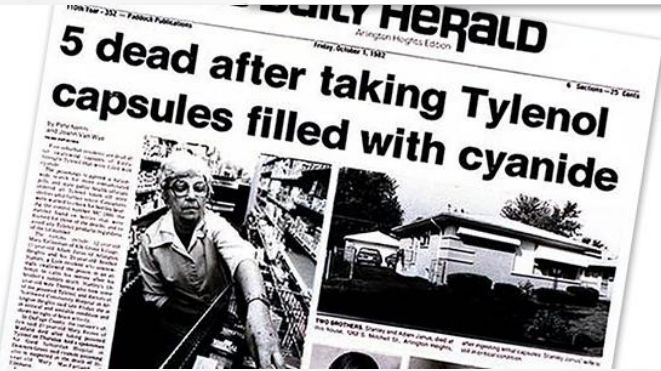
CONTENTS

- 1 # Understand
- 2 # Prepare
- 3 # Act



WIKIPEDIA
The Free Encyclopedia

Crisis management is the process by which an organization deals with a disruptive and unexpected event that threatens to harm the organization or its stakeholders.^[1] The study of crisis management originated with large-scale industrial and environmental disasters in the 1980s.^{[2][3]} It is considered to be the most important process in public relations.^[3]



Google suffers global outage with Gmail, YouTube and majority of services affected

Error was due to lack of storage space in authentication tools causing system to crash



COMMON CAUSES OF DATABASE OUTAGES



Change Issues

- *** Number 1 cause of outage
- Upgrade, patch, migration etc.
- Infrastructural changes
- Application changes
- Crucial to have tested rollback plans and procedures



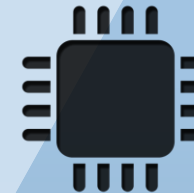
Load Issues

- Don't work close to limits
- Be ready for the peaks



Data Corruption

- Be prepared with corruption detection / prevention settings
- "fsync", "full_page_writes", "synchronous_commit"
- Do not consider as sacrifice from performance



Hardware Issues

- Use redundant hardware
- Keep spare parts



Human Impact

- Cyber attack
- Administrative errors



A database crash is rarely just a technical issue.

Like a dropped stone in still water, it disturbs far more than just the surface;

- *damaging customer trust*
- *shaking financial records*
- *loosing money*
- *disrupting legal commitments*
- *vaporizing reputations*





Before anything else,
preparation is the key to success.

Alexander Graham Bell

“ quote fancy ”

MOTIVATION OF PREPERATION AND HOW TO PREPARE

Very hard to make healthy decisions under pressure.

Not possible to clearly see every option you have.

Many crisis go deeper because of one or consecutive wrong decisions.

CRISIS MANAGEMENT PLAN

Responsibilities, communication chain, decision owners etc.

TECHNICAL PROCEDURES

DB specific scenarios and step by step procedures

PERIODIC TESTS

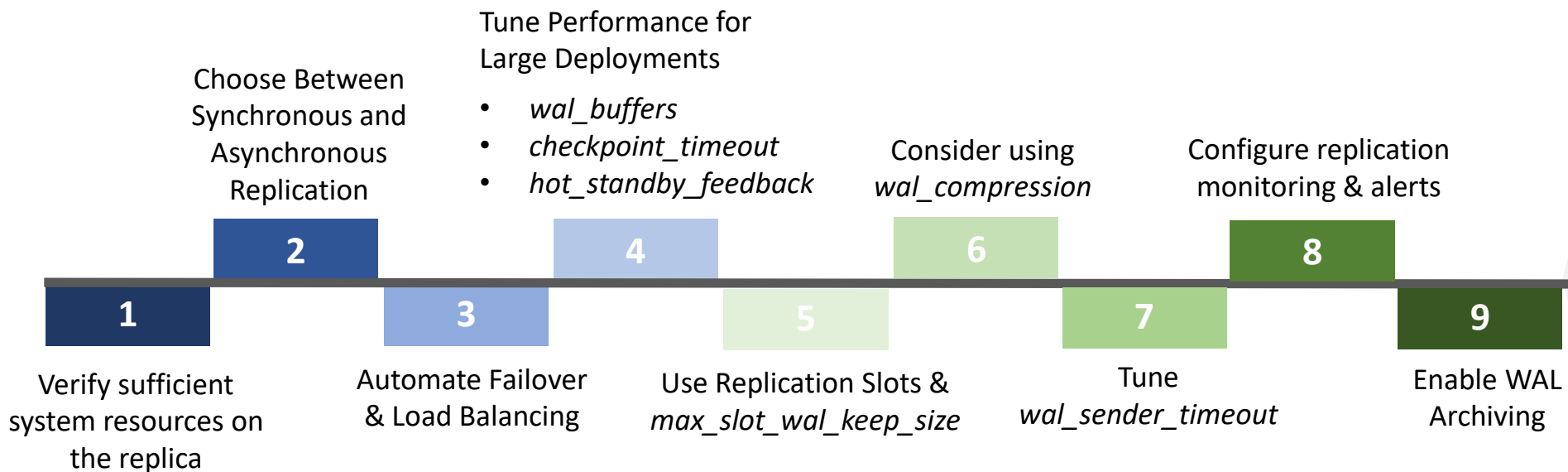
Running failure scenarios, DR tests



POSTGRESQL HIGH AVAILABILITY

- Write-Ahead Log Shipping
- Shared Disk Failover
- Block Device Replication
- Logical Replication
- Trigger-Based Primary-Standby Replication
- SQL-Based Replication Middleware (CDC)
- Asynchronous Multimaster Replication

CONFIGURATIONAL BEST PRACTICES FOR WAL REPLICATION



CONFIGURATIONAL BEST PRACTICES FOR BACKUP

1

Configure monitoring
and alerts
& keep backup logs

2

Enable Parallel
Processing

pgbackrest: "process-max=4"
barman: "parallel_jobs = 4"

3

Test restore/recovery
& Check Backup Integrity

pgbackrest: "check & verify"
barman: "check"

4

Use a Dedicated
Backup Repository
& Enable Multiple
Repositories for
Redundancy

5

Compression to Save
Space

compress-type=zstd
compress-level=3





Losing your head in a crisis
is a good way to become the crisis.

C.J. Redwine

DON'T FORGET YOUR ROLE AND PURPOSE

DBA is the firefighter and goal is:

- => response to the problem *calmly*
- => go to the solution with *reportable actions*

Purpose is resolving the issue with

minimum time
minimum data loss

01

Inform

First step is signaling

- => manager, team, partners, consultants
- => IT crisis management procedure triggered
- => Logging started

02

Ask For Help

- => Open a ticket to the support company
- => Ask for a complete system check by all IT teams

03

Understand

Try to understand the issue and detect the cause

- => Don't try to be a hero
- => Work with other teams, consultants

GOLDEN RULES

- Workspace, number of people working on the issue.
- Specifying the communication chain
- Who is the decision owner?
- Roles and responsibilities of DBA team leader, senior DBAs, junior DBAs, manager
- Logging, reporting every step
- Give brake, go outside the room





PRE-RESTORE

Validate backup files, PostgreSQL version, Ensure disk space

Crosscheck “wal_level” value

Ensure all required WAL segments are available before restoring

Parallelism of restore

Use Tablespace Remapping If Needed

Check target filesystem mount options

Consider using rsync for retryable restore operation

For PG_DUMP adjust PostgreSQL Configuration for Faster Restore

POST-RESTORE & POST FAILOVER

Change parameters if necessary, restore original values if changed

Check pg_hba.conf file

Check versions of components

Check log files before opening application

Deploy new backup and replication policy





Crash to Recovery: The PostgreSQL DBA's Emergency Playbook

Emre Baransel
Utku Demir

straDATA 