You don’t need a Database Backup Policy

Karen Jex | Senior Solutions Architect @ Crunchy Data

PGDay/MED | San Giljan, Malta | April 2023

Introduction

Agenda

- Why Take Backups?
- What are your Recovery Requirements?
- Backup Methods and Tools
- Creating a Disaster Recovery Policy
- Putting it all Together
- Testing and Maintaining your DR Policy
- Conclusions

Agenda

- **Why Take Backups?**
- What are your Recovery Requirements?
- Backup Methods and Tools
- Creating a Disaster Recovery Policy
- Putting it all Together
- Testing and Maintaining your DR Policy
- Conclusions

Why Take Backups?

- ~~For fun~~
- Safeguard critical business data
- Recover from database failure
- Support your DB recovery policy

Why Take Backups?

What could go wrong?

What could go wrong?

What could go wrong?

What could go wrong?

What could go wrong?

Why Take Backups?

What could go wrong?

- Data centre failure
- Database server failure
- Storage array failure
- Incorrect batch process
- Human error
- Willful destruction
- Corrupted data file
- Want a copy of the database

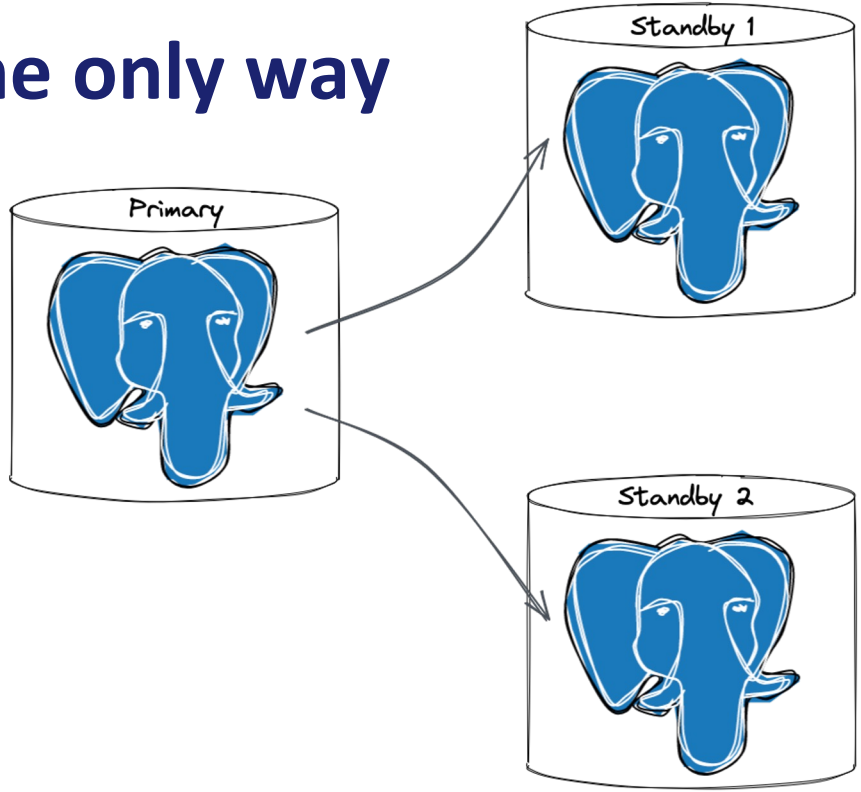
Why Take Backups?

How can you Recover?

- If all else fails…
- Restore from database backup
- Recover to just before the failure

Why Take Backups?

Backups aren't the only way

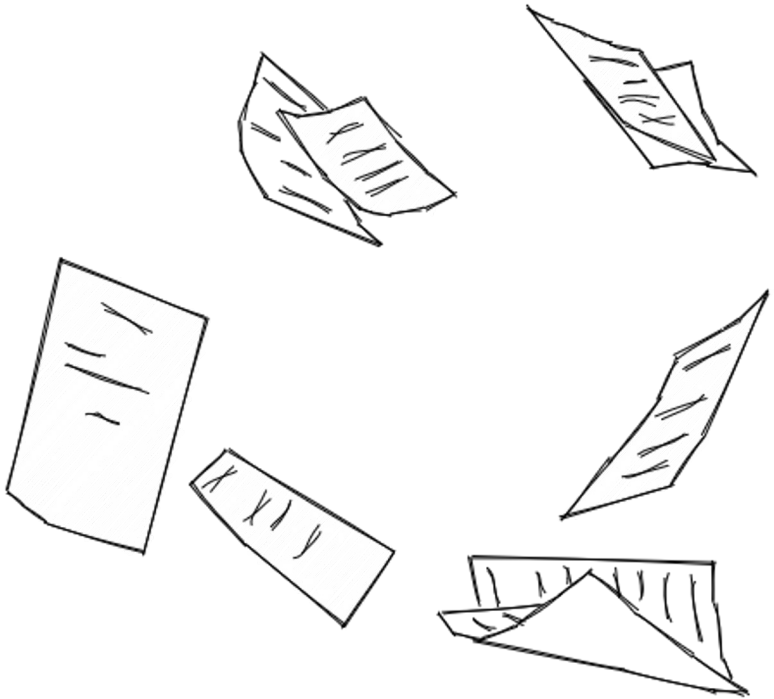


Agenda

- Why Take Backups?
- **What are your Recovery Requirements?**
- Backup Methods and Tools
- Creating a Disaster Recovery Policy
- Putting it all Together
- Testing and Maintaining your DR Policy
- Conclusions

What are your Recovery Requirements?

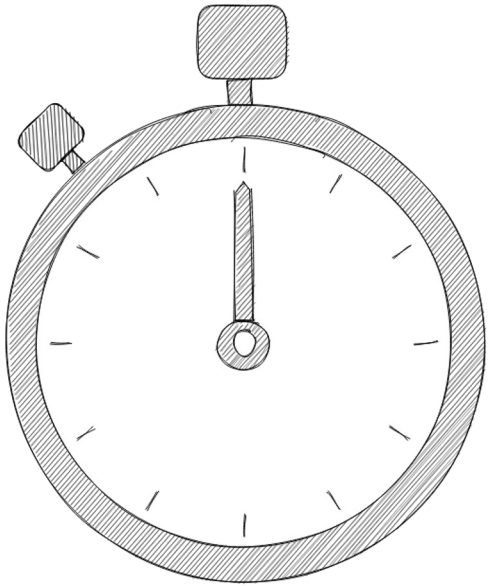
RPO



- Recovery Point Objective
- Maximum Permitted Data Loss

What are your Recovery Requirements?

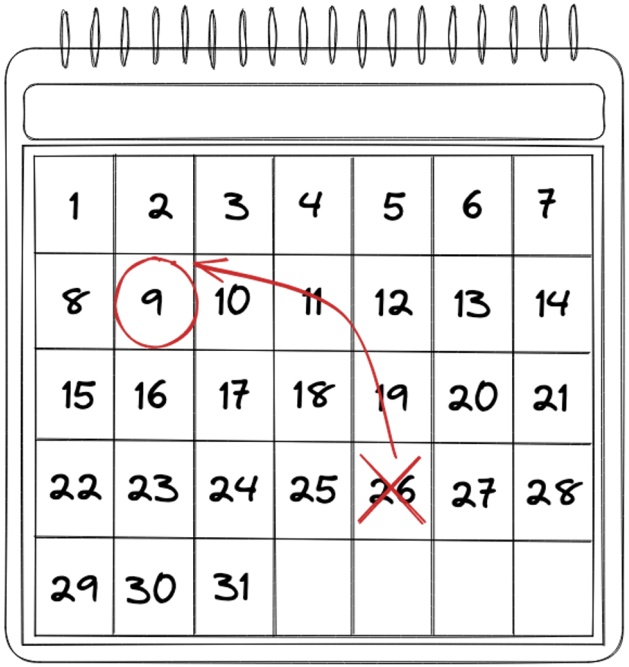
RTO



- Recovery Time Objective
- Maximum Outage
- MTTR - Mean Time to Recover

What are your Recovery Requirements?

Retention



- How far back?
- Backup Retention

What are your Recovery Requirements?

Who Defines the Requirements

- Business
- SLAs
- Make sure they’re defined

Agenda

- Why Take Backups?
- What are your Recovery Requirements?
- **Backup Methods and Tools**
- Creating a Disaster Recovery Policy
- Putting it all Together
- Testing and Maintaining your DR Policy
- Conclusions

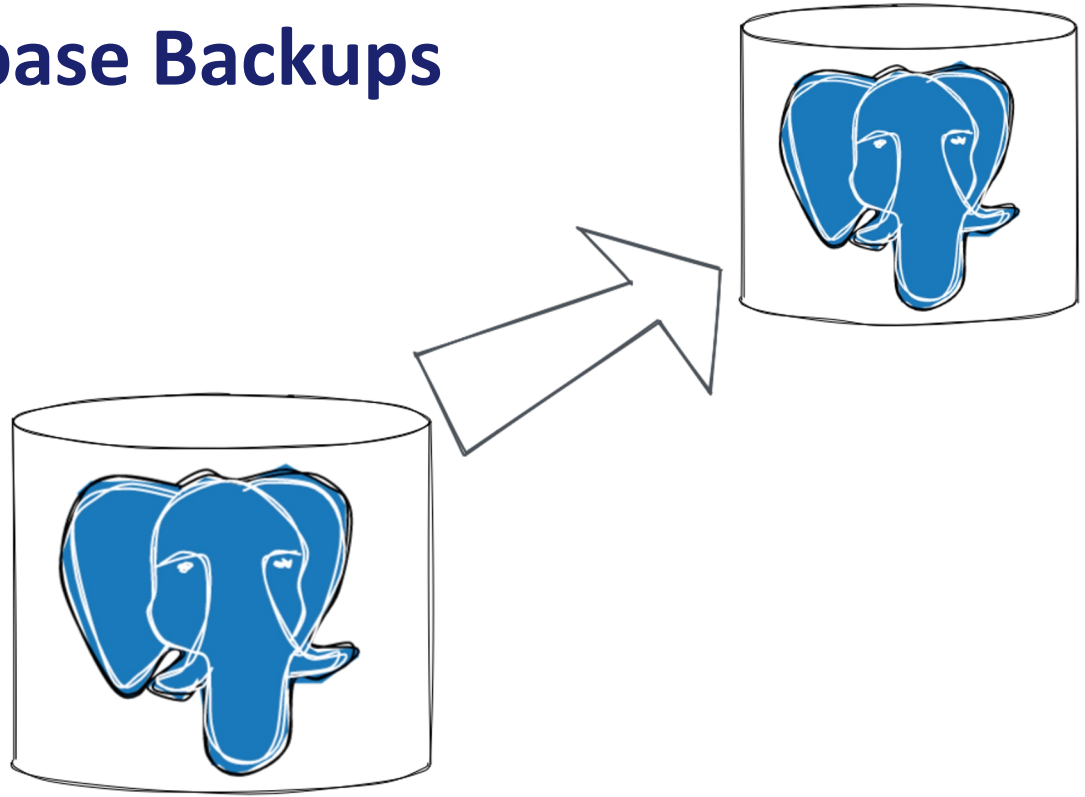
Backup Methods

Physical Database Backups

- Offline

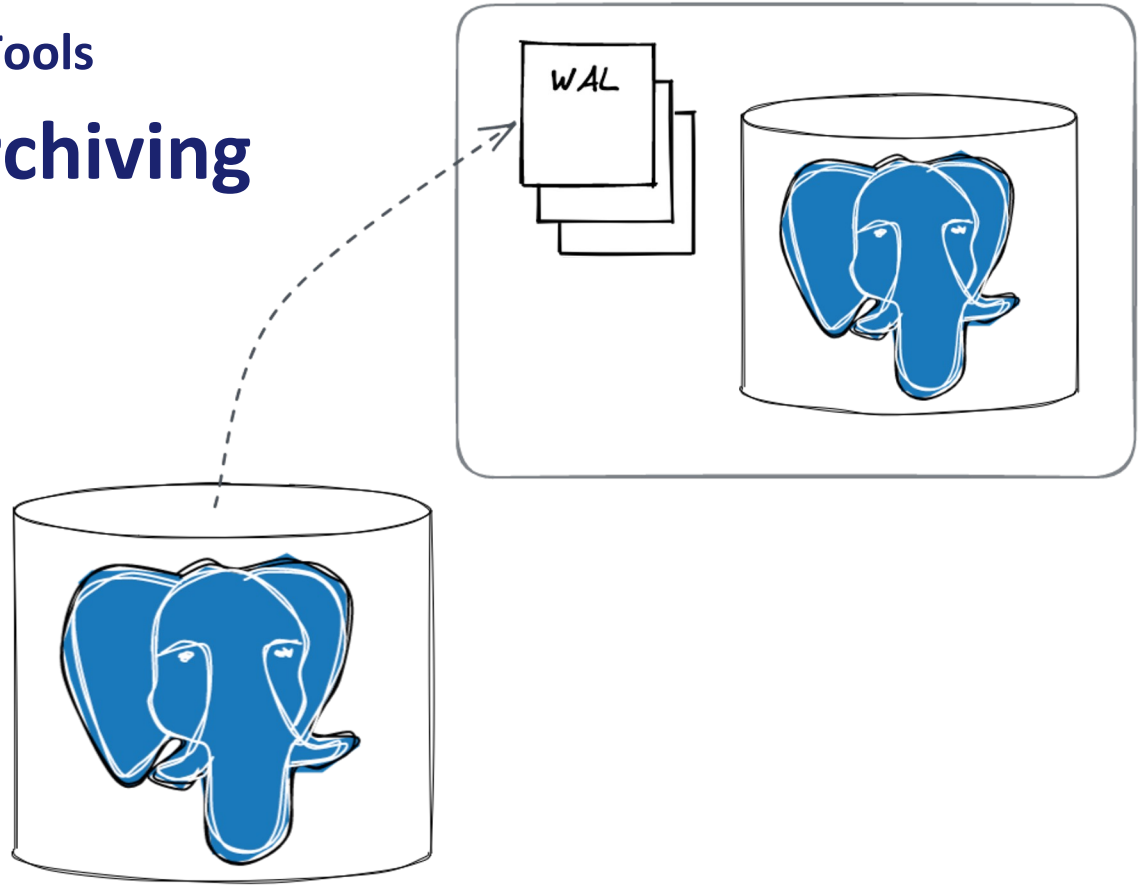
  or

- Online

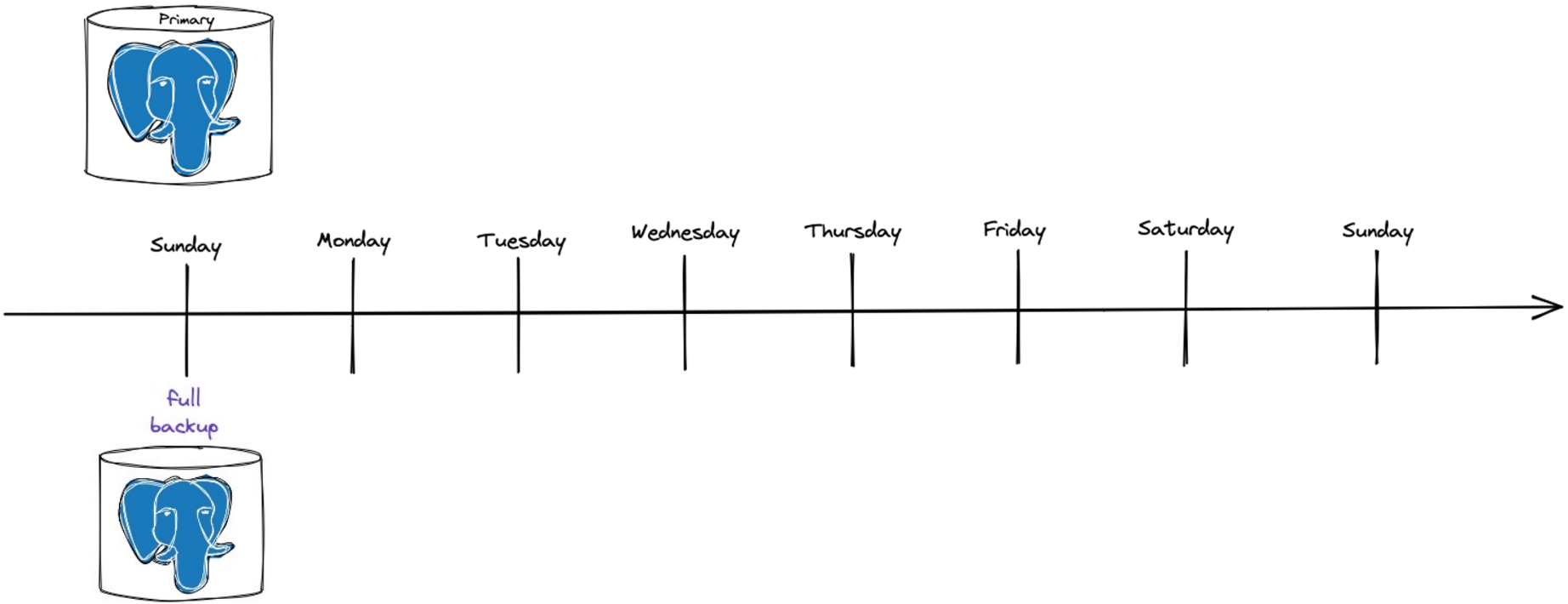


Continuous Archiving

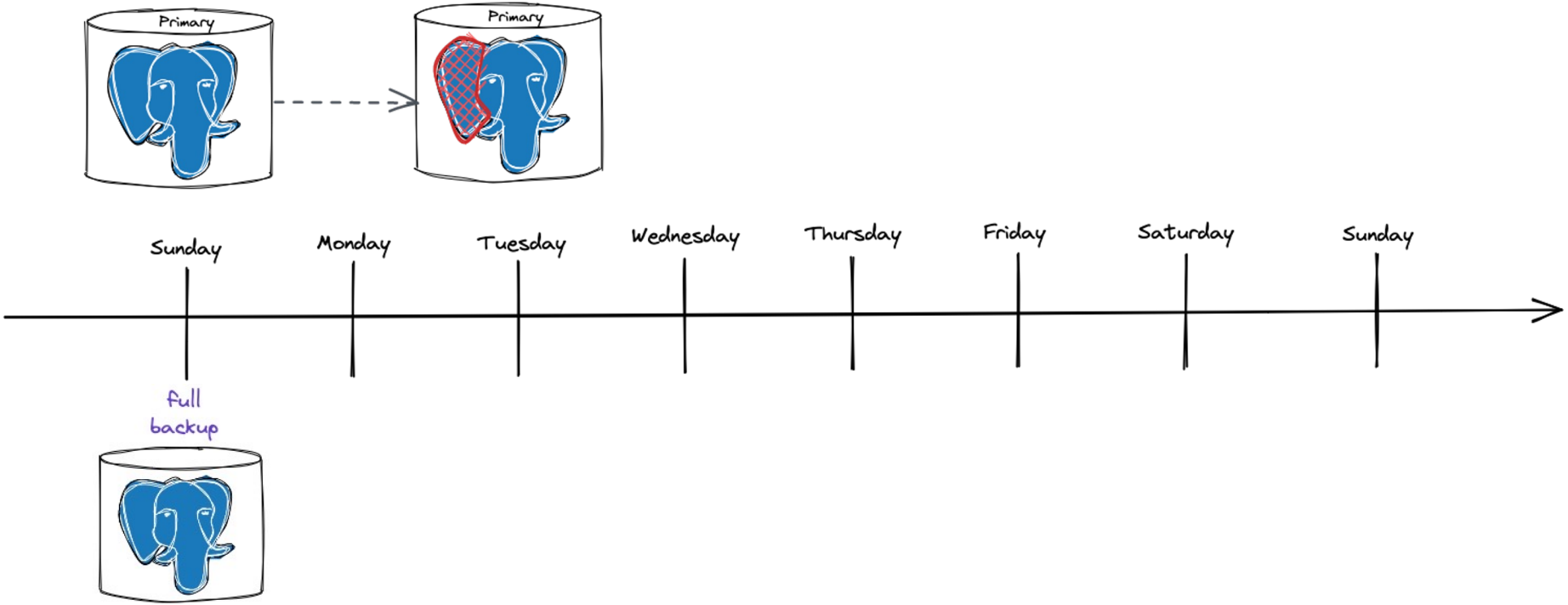
- Allows PITR



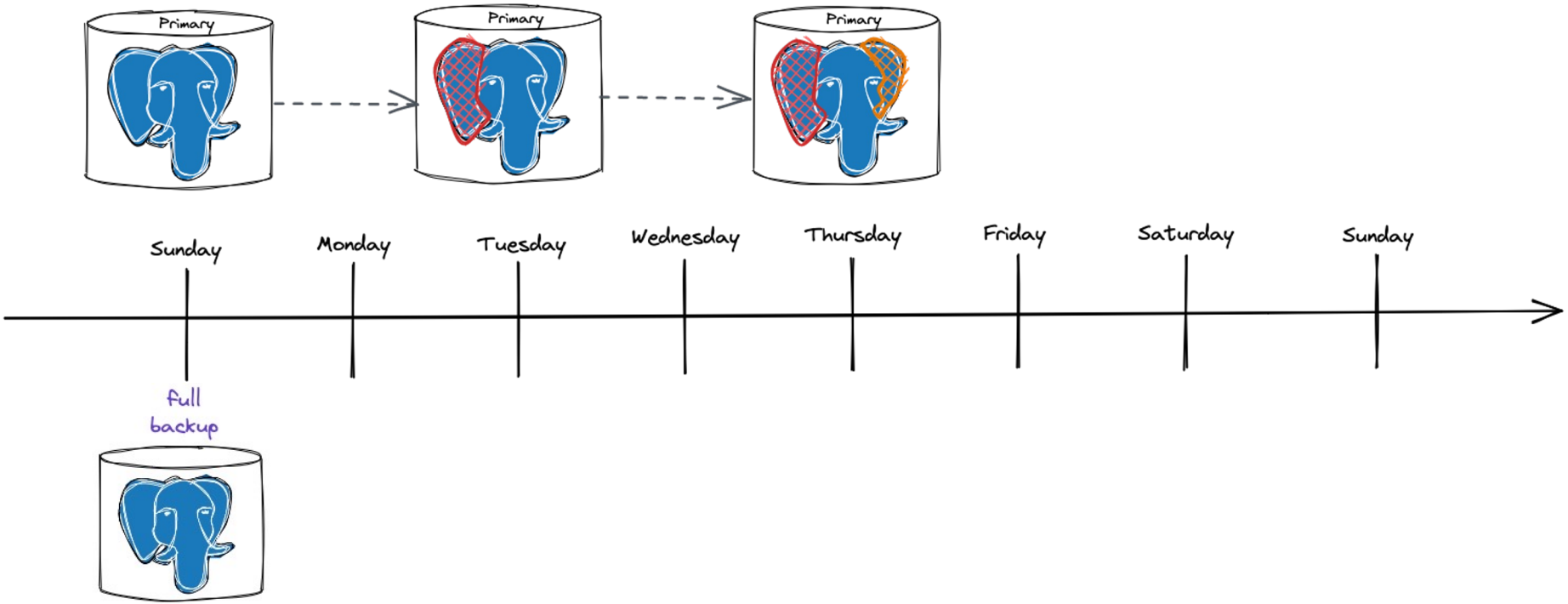
Full, Incremental and Differential Backups



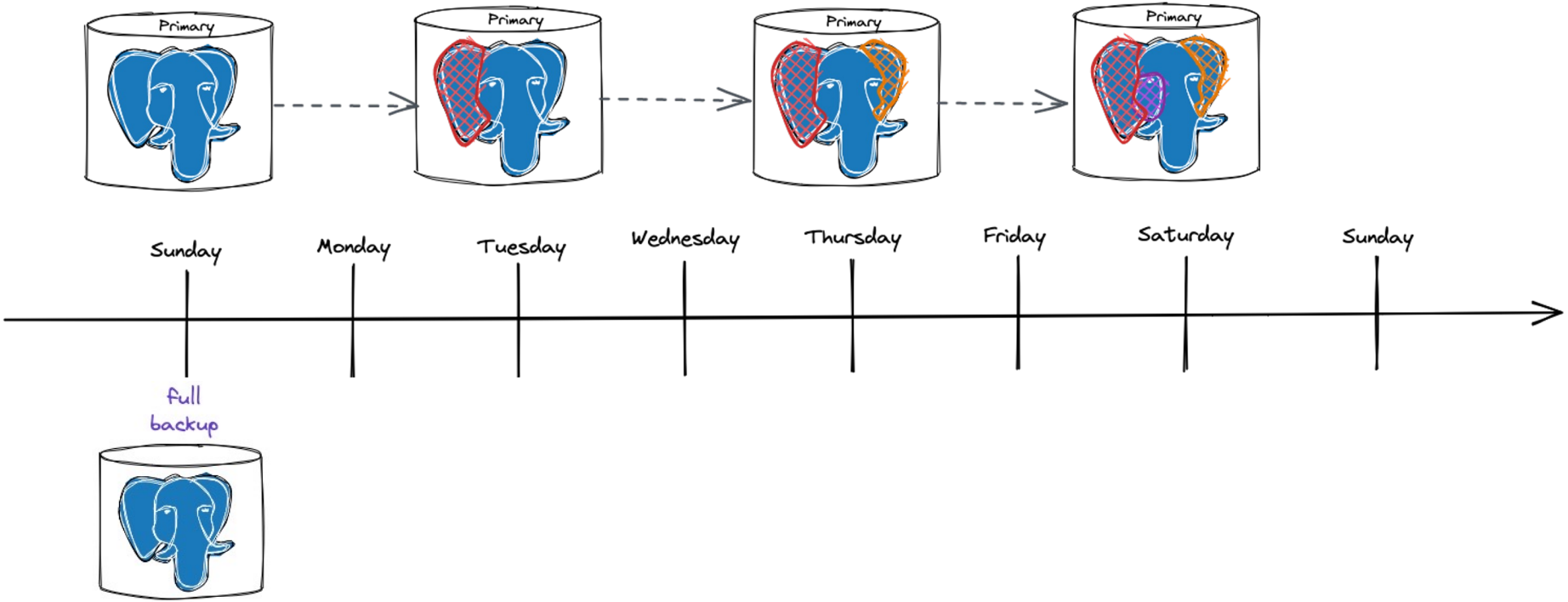
Full, Incremental and Differential Backups



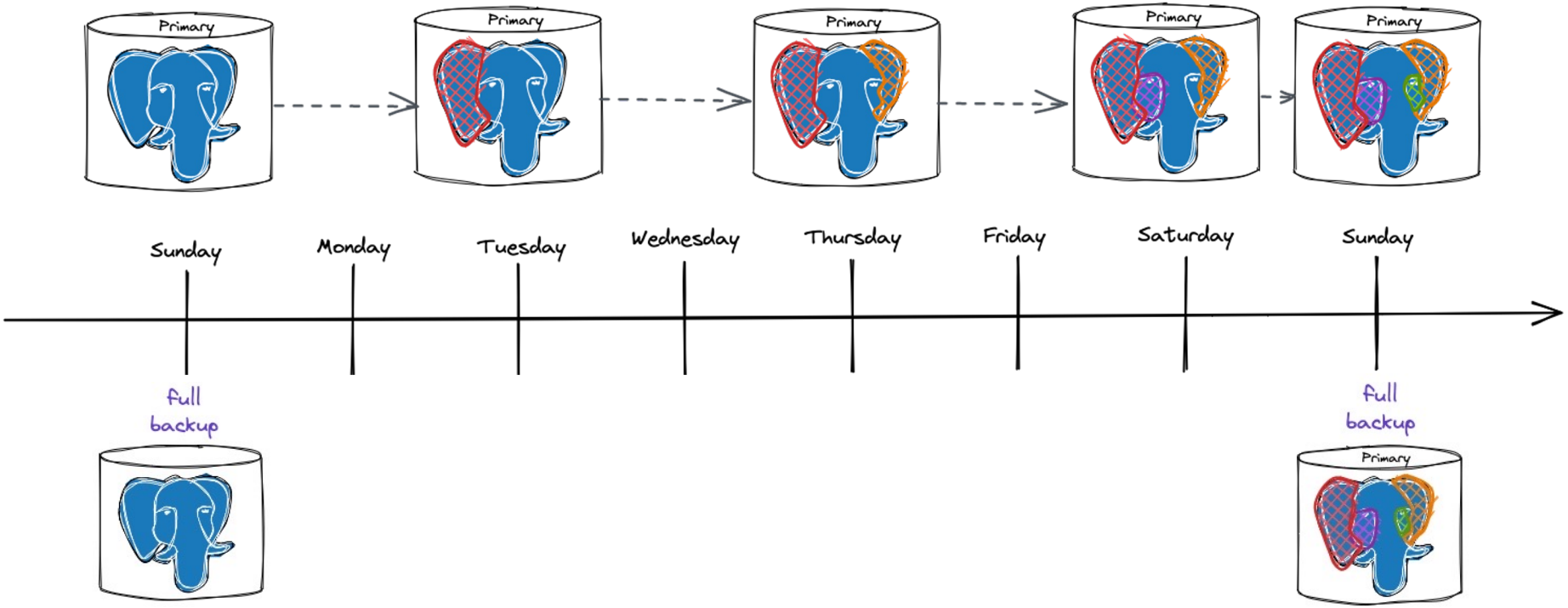
Full, Incremental and Differential Backups



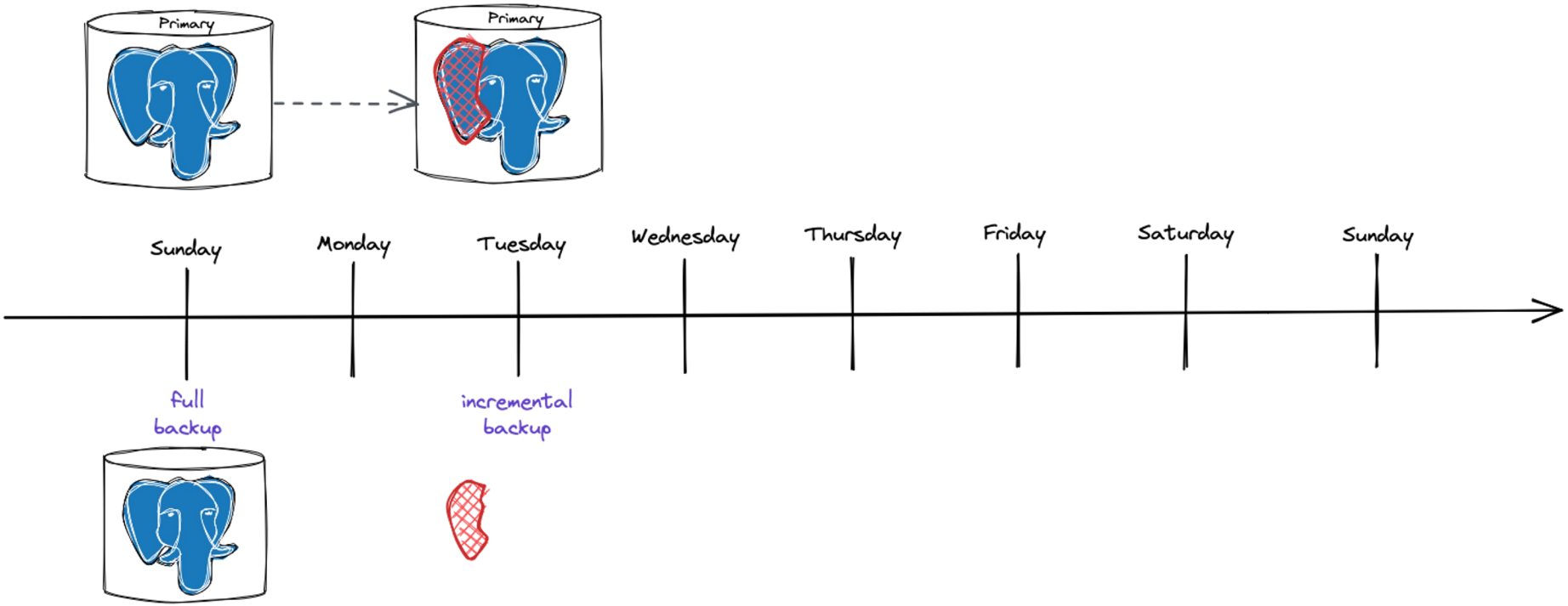
Full, Incremental and Differential Backups



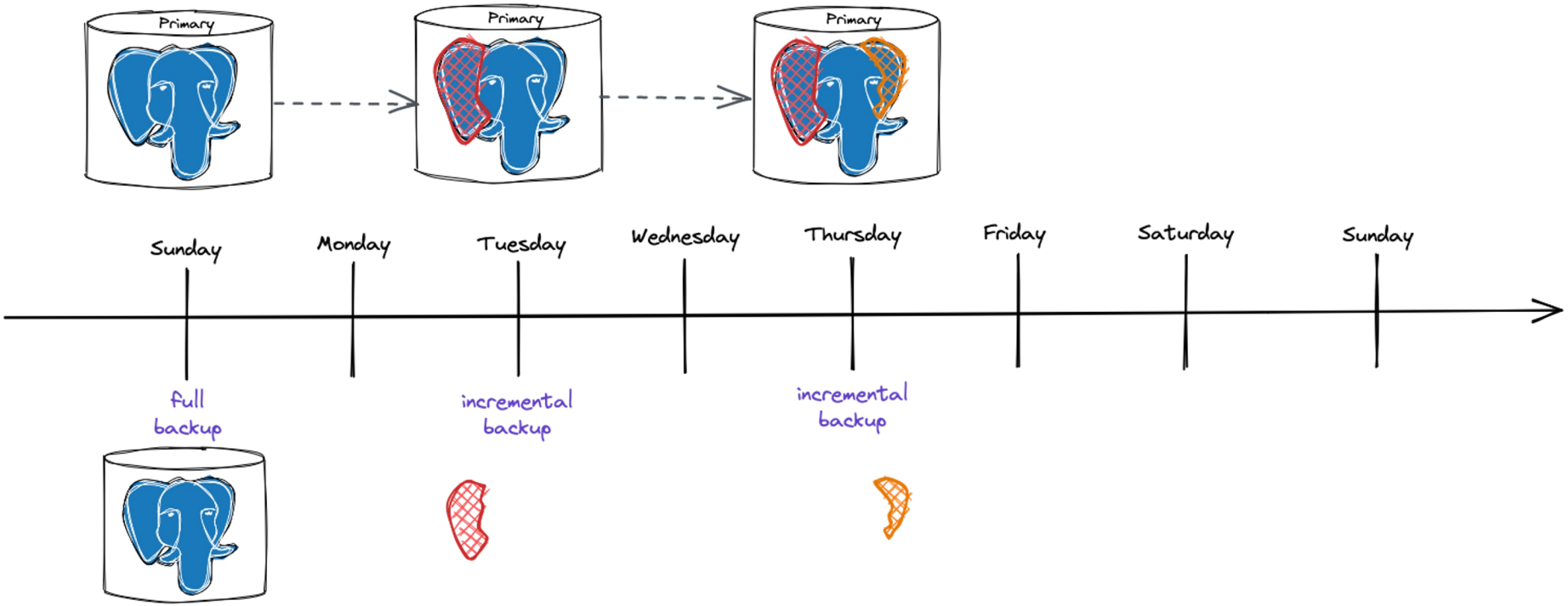
Full, Incremental and Differential Backups



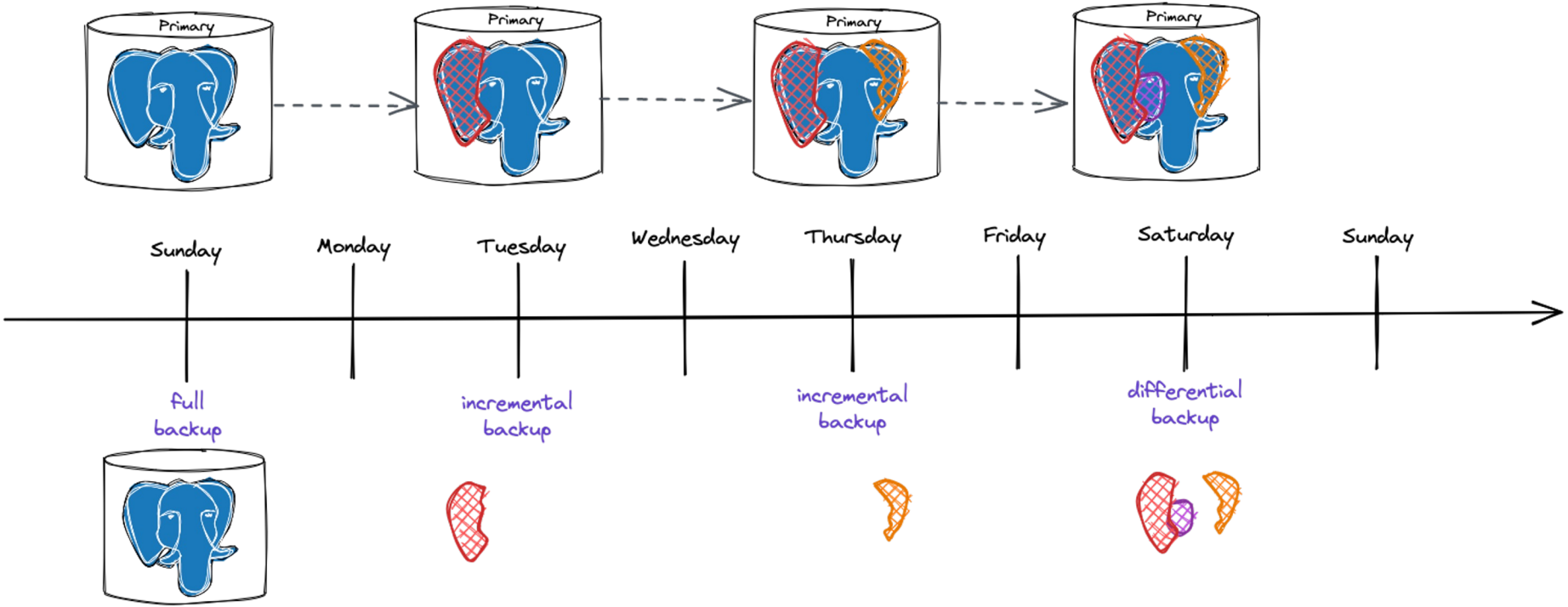
Full, Incremental and Differential Backups



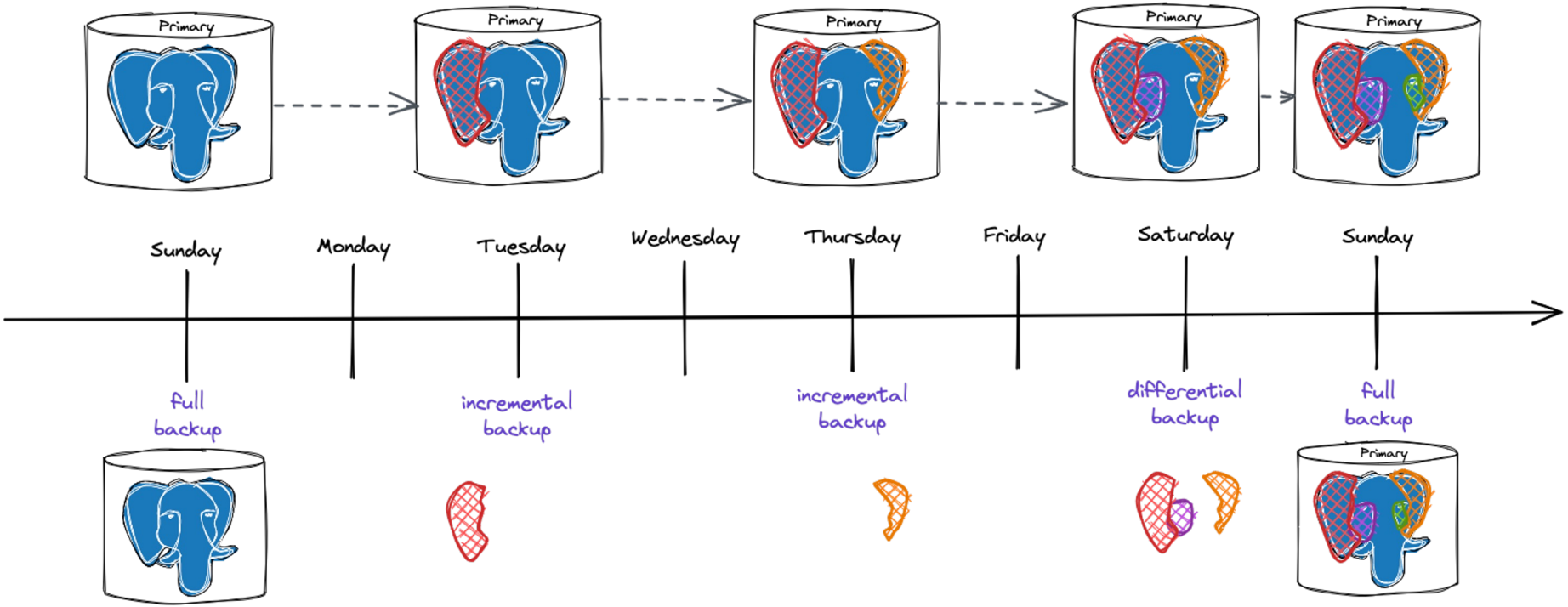
Full, Incremental and Differential Backups



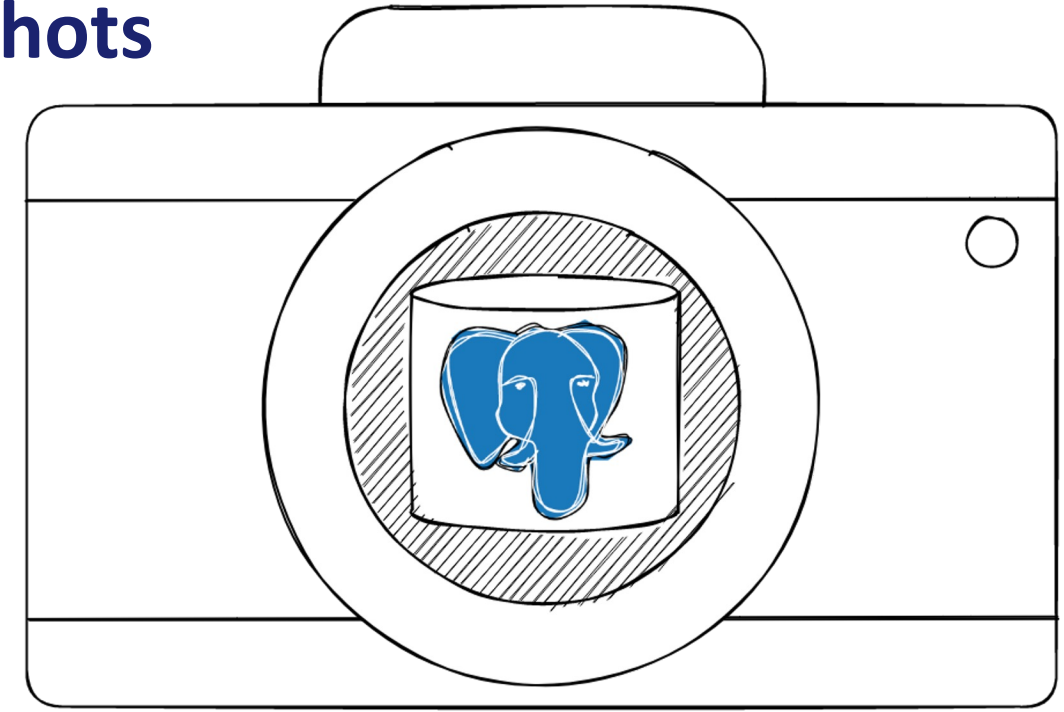
Full, Incremental and Differential Backups



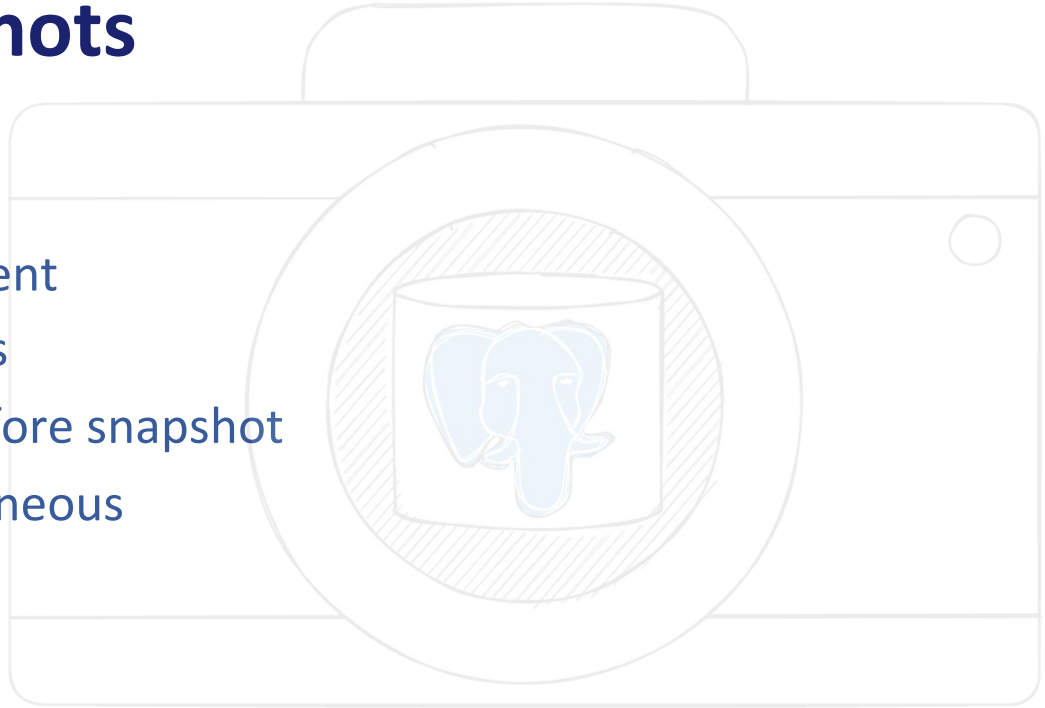
Full, Incremental and Differential Backups



Storage Snapshots



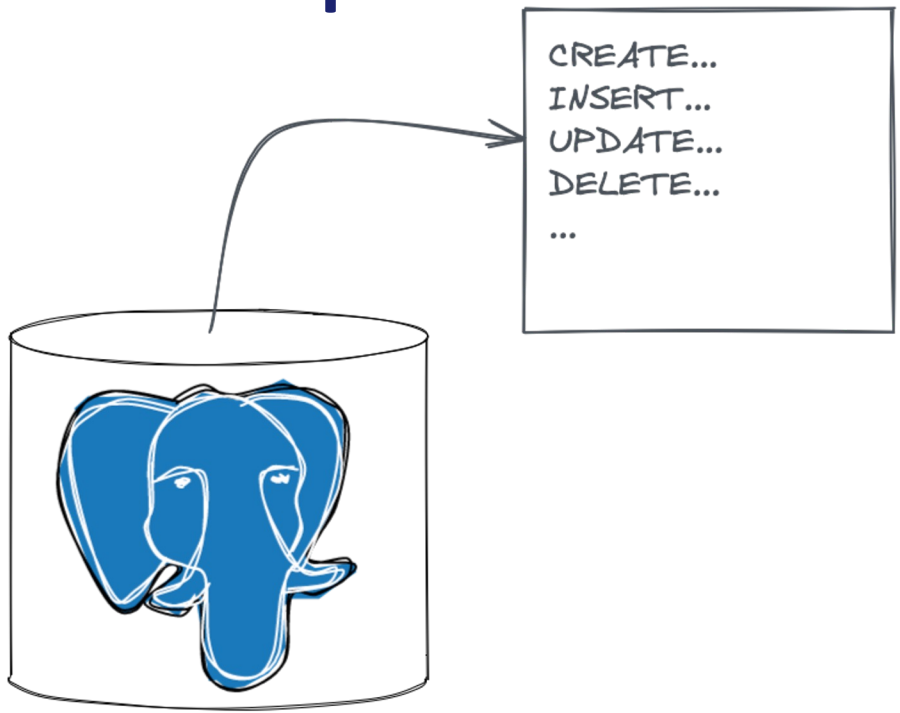
Storage Snapshots



- Must be Consistent
- Backup WAL files
- CHECKPOINT before snapshot
- Must be Simultaneous
- TEST, TEST, TEST

Logical Database Backups

- pg_dump
- pg_dumpall
- pg_restore



Comparison of Backup Methods

	PITR	Database up during backup	Restore individual objects	cross-version/ cross-platform
Offline Backup				
Online Backup		✓		
Continuous archiving	✓	✓		
Logical Backup		✓	✓	✓

Backup Tools

Backup and Recovery Tool Requirements

- PITR
- Central backup architecture
- Scheduling
- Backup Catalogue
- Backup/WAL Retention
- Multiple Backup Locations
- WAL archiving
- Monitoring and alerting
- Backup/WAL File Compression
- Incremental/Differential Backups
- Restore individual objects
- Backup to Cloud Storage

Tools for Physical Backups

- pgBackRest

  https://pgbackrest.org

- Barman

  https://pgbarman.org/

- pg_basebackup

  https://www.postgresql.org/docs/current/app-pgbasebackup.html

Comparison of Physical Backup and Recovery Tools

	PITR	Backup Retention	Manage archived WAL	Centralised architecture	Compression	Single Database Restore	Cloud backups
pgBackRest	✓	✓	✓	✓	✓	(✓)	✓
Barman	✓	✓	✓	✓	(WAL)		(✓)
pg_basebackup	✓				✓		

Tools for Logical Backups

- pg_dump

  https://www.postgresql.org/docs/current/app-pgdump.html

- pg_restore

  https://www.postgresql.org/docs/current/app-pgrestore.html

- pg_dumpall

  https://www.postgresql.org/docs/current/app-pg-dumpall.html

Agenda

- Why Take Backups?
- What are your Recovery Requirements?
- Backup Methods and Tools
- **Creating a Disaster Recovery Policy**
- Putting it all Together
- Testing and Maintaining your DR Policy
- Conclusions

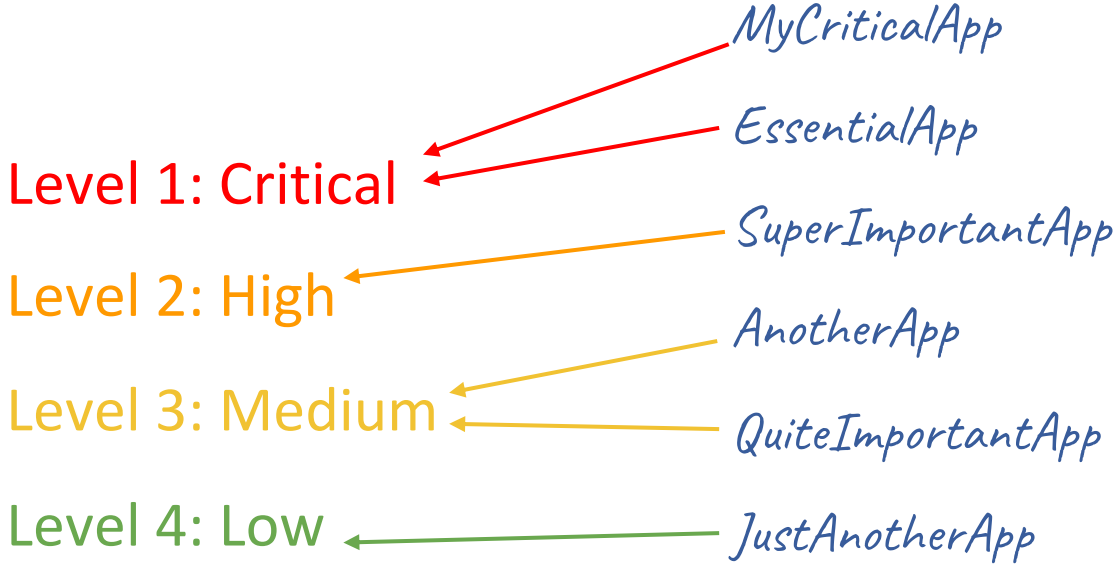
Creating a Disaster Recovery Policy
What should it include?

Creating a Disaster Recovery Policy
What should it include?

Recovery Requirements

Creating a Disaster Recovery Policy - Recovery Requirements

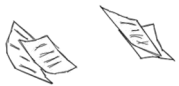
Application Categories



Creating a Disaster Recovery Policy - Recovery Requirements

Level 1 (critical) Applications

15 minutes



5 minutes

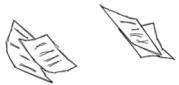
6 months

High availability architecture

Creating a Disaster Recovery Policy - Recovery Requirements

Level 4 (low priority) Applications

4 hours



1 day

1 week

Standalone database

Recovery Procedures

Creating a Disaster Recovery Policy - Recovery Procedures

Consider Possible Failures

- Impact of the failure
- How to recover
- Data loss
- Time to Recover

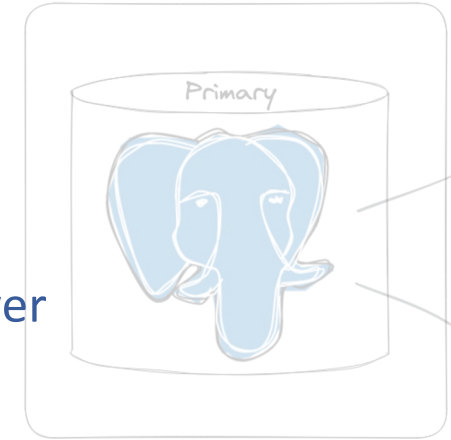
Failed (Primary) Database Node

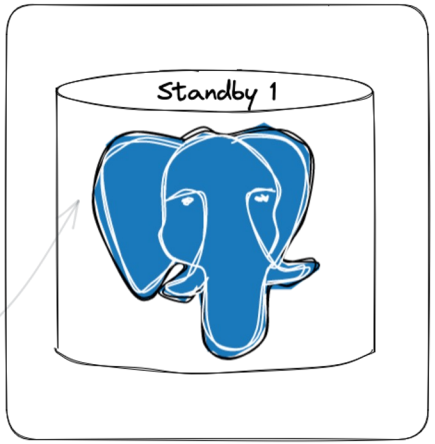
Recovery Procedures - Failed (Primary) Database Node

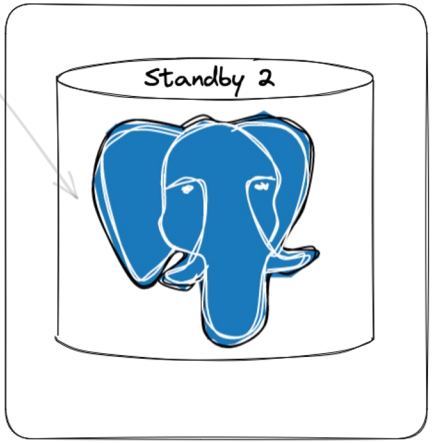
With HA Architecture

Impact: unavailability

Recovery: automatic failover







Recovery Procedures - Failed (Primary) Database Node

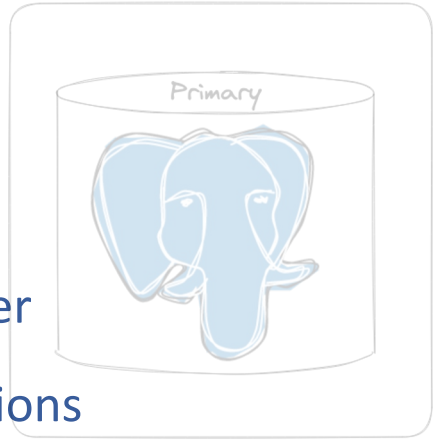
With HA Architecture

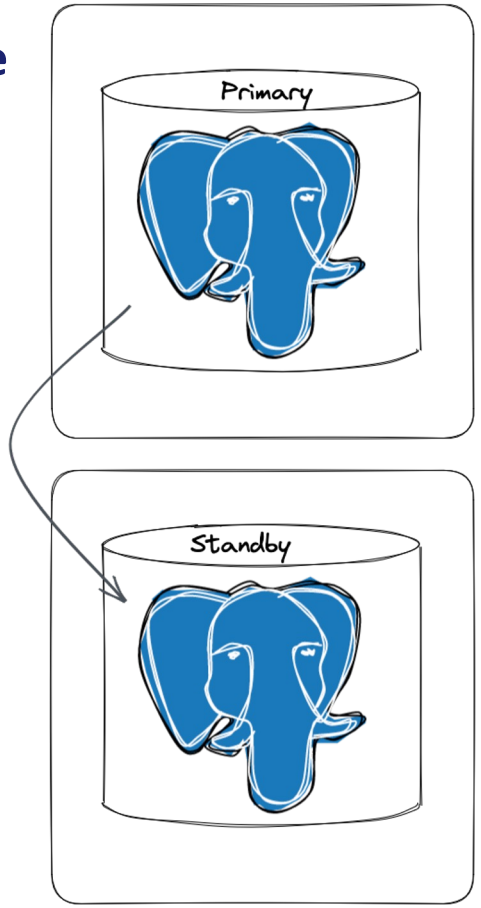
Impact: unavailability

Recovery: automatic failover

Data loss: in-flight transactions

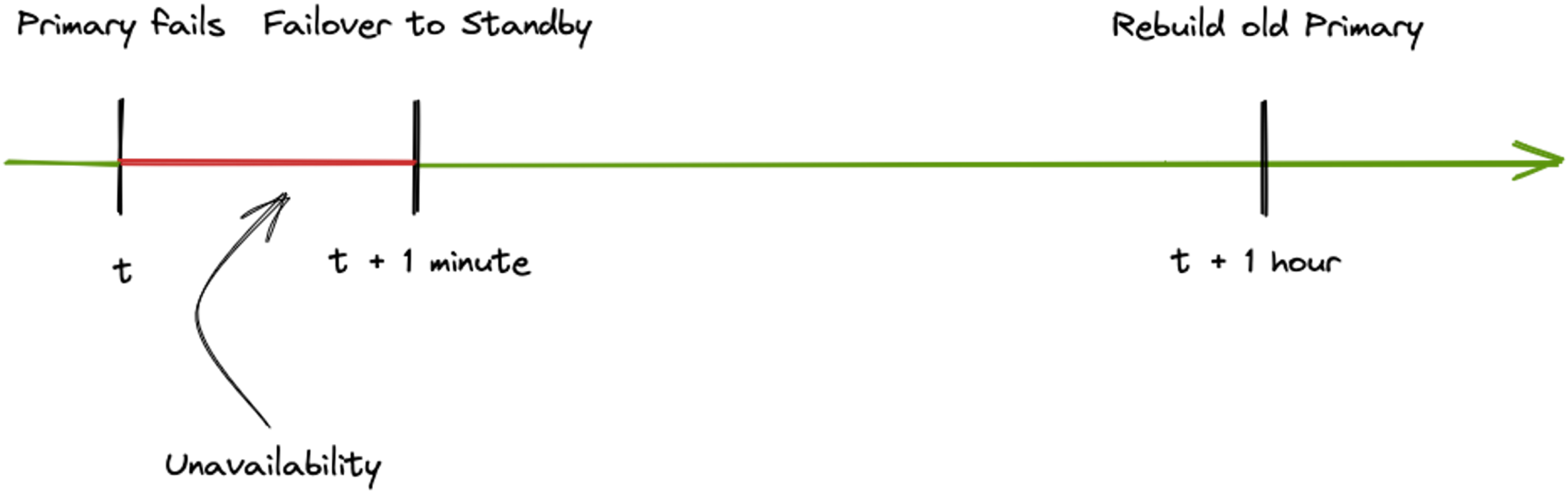
Recovery time: seconds





Recovery Procedures - Failed (Primary) Database Node

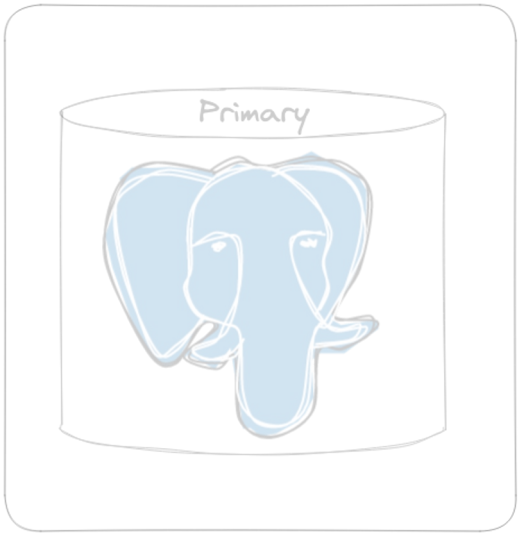
With HA Architecture



Recovery Procedures - Failed (Primary) Database Node

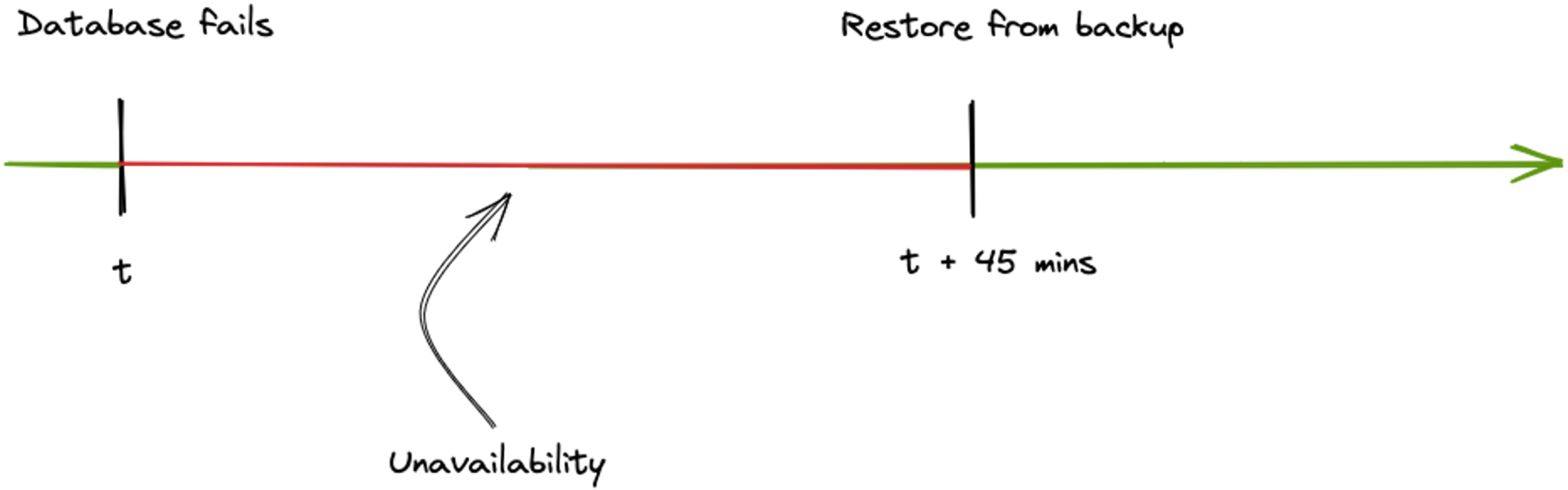
Standalone Database

Impact:	unavailability
Recovery:	restore from backup
Data loss:	minimal if wal archiving
Recovery time:	minutes to hours



Recovery Procedures - Failed (Primary) Database Node

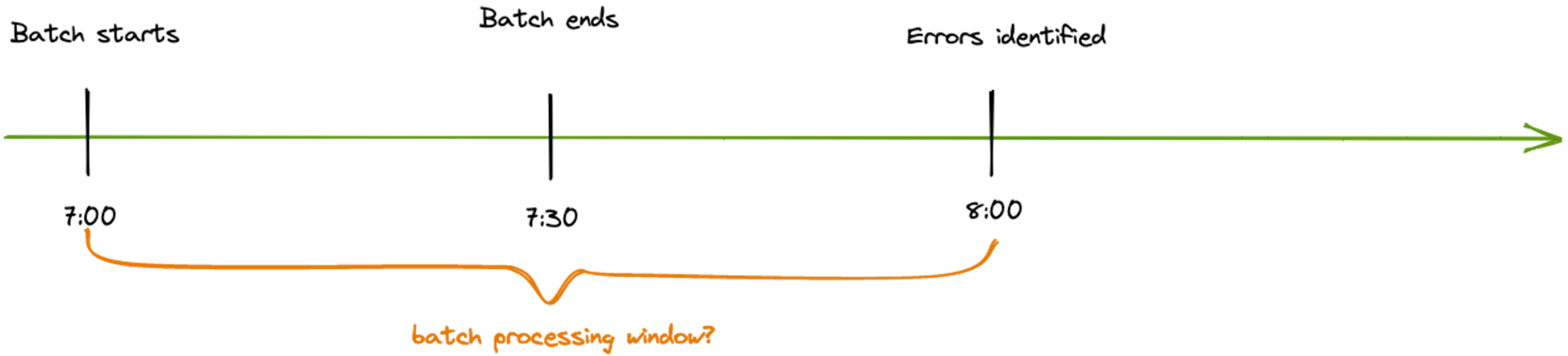
Standalone Database



Batch Process Incorrectly Modified Data

Batch Process Incorrectly Modified Data

Timeline



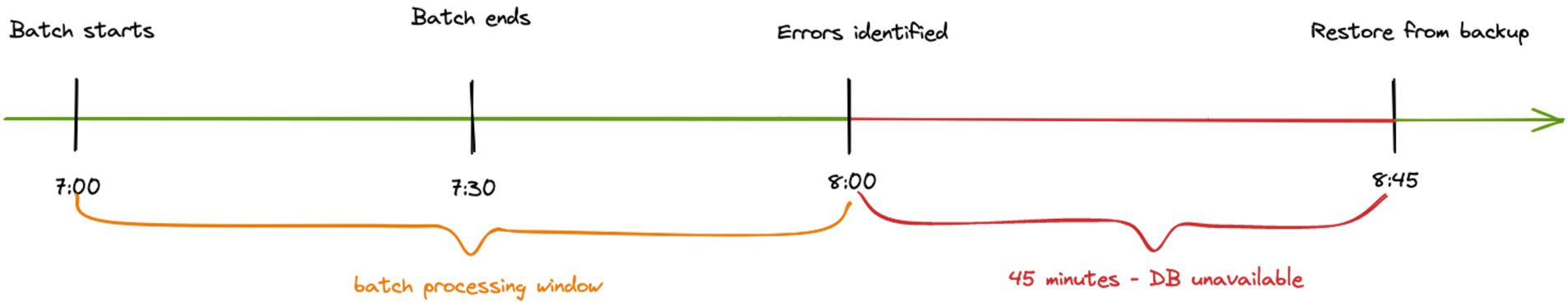
Batch Process Incorrectly Modified Data

Recovery Options

- In-place restore and PITR
- Restore a copy, export and import
- Correct data in-place

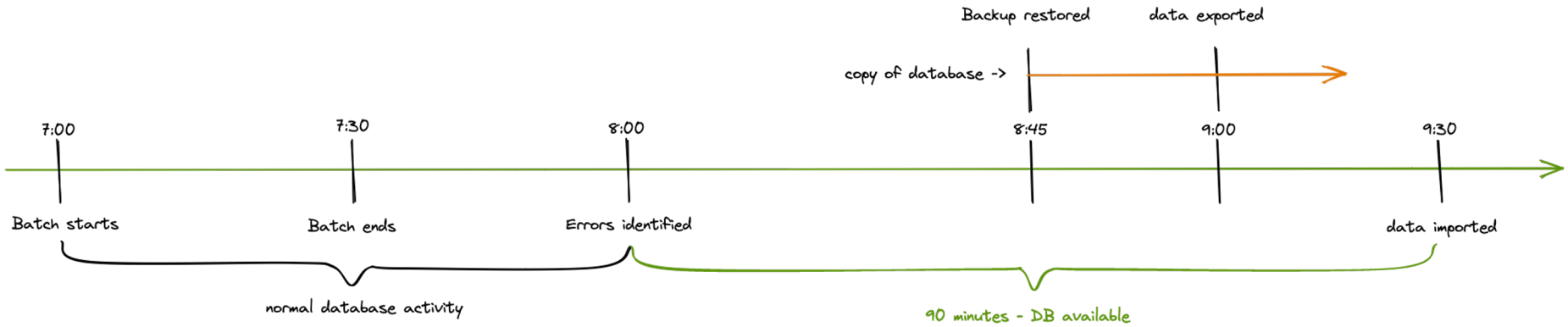
Batch Process Incorrectly Modified Data

In-place PITR



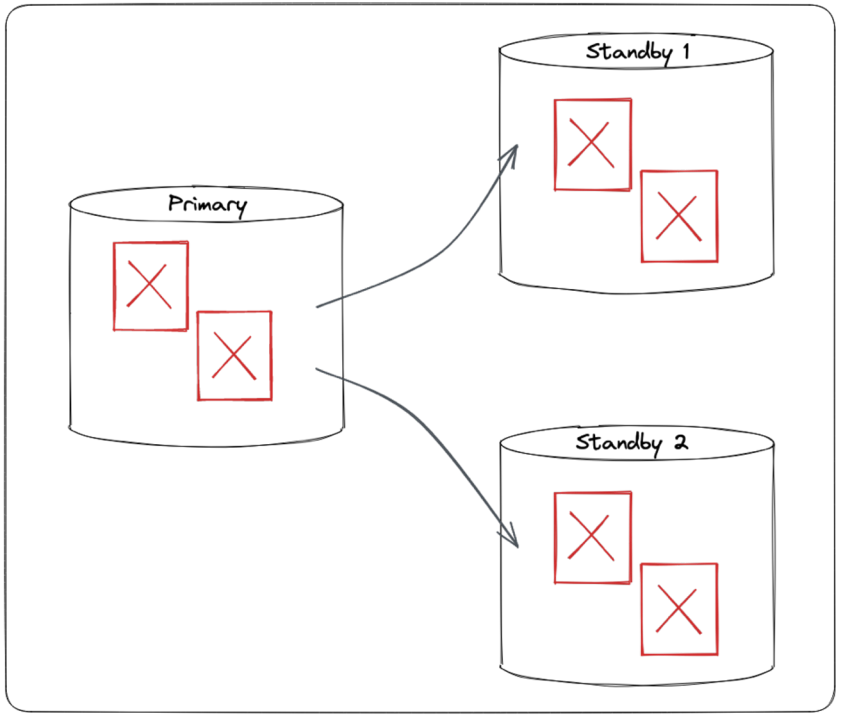
Batch Process Incorrectly Modified Data

Extract Data from a Restored DB Copy



Batch Process Incorrectly Modified Data

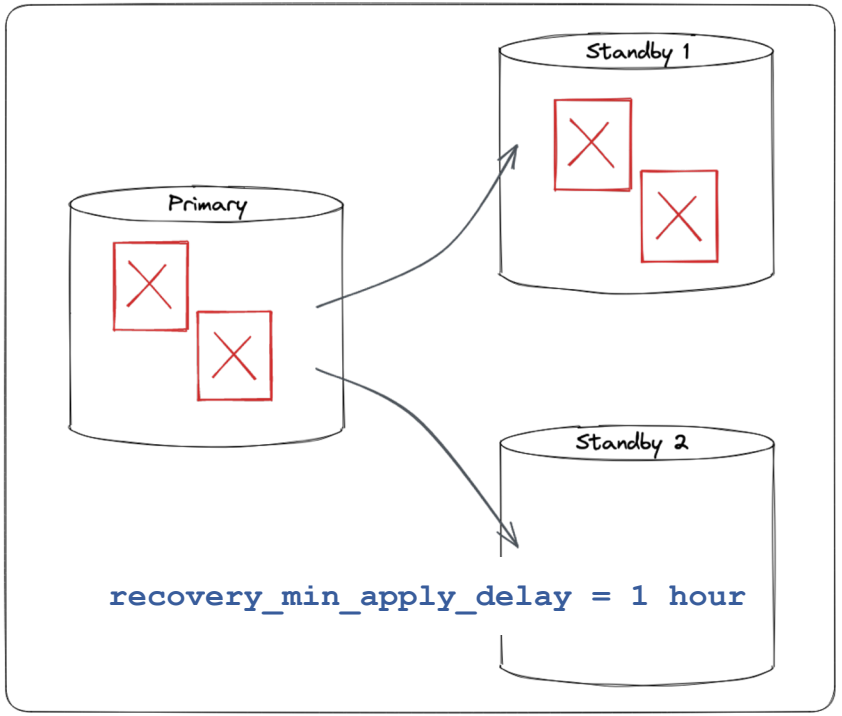
HA Environment



Batch Process Incorrectly Modified Data

Delayed Replica

- Promote delayed replica
- Export/import



Creating a Disaster Recovery Policy

Test each scenario

- Document, Automate
- Test
- Note Timings
- Test again
- Plan more testing

Backup Strategy

Creating a Disaster Recovery Policy

Backup Strategy

For each category of application:

- Backup method(s)
- Backup tool(s)
- Frequency of backups
- Location
- Retention period

Creating a Disaster Recovery Policy

Backup Strategy - Monitoring

- Size
- Space
- Time
- Validity

Agenda

- Why Take Backups?
- What are your Recovery Requirements?
- Backup Methods and Tools
- Creating a Disaster Recovery Policy
- **Putting it all Together**
- Testing and Maintaining your DR Policy
- Conclusions

Putting it all together

Sample Disaster Recovery Policy

Agenda

- Why Take Backups?
- What are your Recovery Requirements?
- Backup Methods and Tools
- Creating a Disaster Recovery Policy
- Putting it all Together
- **Testing and Maintaining your DR Policy**
- Conclusions

Test Strategy

- Repeated tests
- Confidence in your backups
- Confidence in your process
- DB restore will be an emergency

Test Strategy

- How often
- What will be tested
- Expected outcome
- Who will test

Creating a Disaster Recovery Policy

Review and Update the Policy

- Annually
- Major architecture change
- Requirements
- Tools
- Database size

Maintaining your Recovery Procedures

- How often
- Who will review and change
- Per category

Agenda

- Why Take Backups?
- What are your Recovery Requirements?
- Backup Methods and Tools
- Creating a Disaster Recovery Policy
- Putting it all Together
- Testing and Maintaining your DR Policy
- **Conclusions**

Conclusions

- Backup strategy just part of DR policy
- Define recovery requirements first
- Create backup strategy that responds to requirements
- May involve multiple methods and tools
- Collaborate with other teams
- Test and Practice
- Keep policies up to date

Thank You!

@karenhjex | @karenhjex@mastodon.online | karen.jex@crunchydata.com

Image acknowledgements

- Fireball: Image par Gerd Altmann de Pixabay
- Fire: Image par Enrique de Pixabay
- Tsunami: Image par Samir Halder de Pixabay
- Cyclone: Image par 0fjd125gk87 de Pixabay
- Whiteboard: Image par Gerd Altmann de Pixabay