

# HA, backup i disaster recovery

Domeny awarii i mierzalne odtworzenie usługi

---

mgr inż. Jakub Woźniak

Zarządzanie Systemami Rozproszonymi · Semestr zimowy 2026/27

| Mechanizm         | Chroni przed              | Nie wystarcza przy         |
|-------------------|---------------------------|----------------------------|
| HA                | Awarią części komponentów | Wspólnym błędzie aplikacji |
| Replikacja        | Utratą jednej kopii       | Powielonym DELETE          |
| Backup / historia | Utratą poprawnego stanu   | Braku procedury restore    |

- Zakres ochrony musi wskazywać konkretny scenariusz awarii.

*Google Cloud — DR planning*



- Health check odsuwa niedostępny endpoint.
- Pozostałe repliki muszą mieć pojemność na ruch po awarii.
- Failover bazy: wybór nowego lidera i odcięcie starego od zapisów.
- Dwa niezależnie zapisujące primary mogą spowodować rozbieżność danych.

*PostgreSQL — Standby servers*

## Trzy elementy wymagane jednocześnie

$A = A1 \times A2 \times A3$ ; przy niezależnych awariach i 99,9% każdego:  $A = 0,999^3 \approx$   
**99,7003%.**

- Wspólne przyczyny awarii naruszają założenie niezależności.
- Redundancja, cache i kolejka zmieniają model zachowania.
- SLA składników nie można po prostu przepisać jako SLO aplikacji.

*Obliczenie dydaktyczne modelu szeregowego, nie prognoza dostępności tego systemu.*

| Cel | Pytanie                                       | Przykład                |
|-----|-----------------------------------------------|-------------------------|
| RTO | Jak szybko przywrócić wymagany poziom usługi? | Do 45 min od zakłócenia |
| RPO | Jak stary może być ostatni odzyskany stan?    | Do 5 min utraty zapisów |

- Cele odróżnić od zmierzonych wyników ćwiczenia.
- „Usługa przywrócona”: także poprawne dane, dostęp i zdolność realizacji.

*NIST SP 800-34 Rev. 1*

09:57: ostatni odzyskiwalny zapis



10:00: awaria



10:40: usługa

- Luka danych: 3 min; cel RPO = 5 min → spełniony w tym teście.
- Przerwa usługi: 40 min; cel RTO = 45 min → spełniony.
- Mierzyć ostatni faktycznie odzyskany zapis, nie sam czas uruchomienia backupu.

*Przykład zakłada, że zapisy z 09:57-10:00 nie są odzyskiwalne inną drogą.*

| Etap sekwencyjny                   | Czas      |
|------------------------------------|-----------|
| Wykrycie + decyzja                 | 5 + 5 min |
| Przygotowanie infrastruktury       | 8 min     |
| Odtworzenie danych                 | 12 min    |
| Walidacja i uruchomienie aplikacji | 8 min     |
| Przełączenie ruchu                 | 2 min     |
| Razem                              | 40 min    |

- Zapas do RTO 45 min: tylko 5 min.
- Część prac można zrównoleglić dopiero po sprawdzeniu zależności.



- Potrzebny spójny backup bazowy i wymagane segmenty WAL.
- Zwykły dump nie daje samodzielnie odtworzenia do dowolnej sekundy.
- Przerwa w archiwizacji może ograniczyć odzyskiwalny punkt.

*PostgreSQL — Continuous archiving and PITR*

| Tryb           | Potwierdzenie zapisu                          | Kompromis                          |
|----------------|-----------------------------------------------|------------------------------------|
| Synchroniczny  | Czeka na wybrany poziom potwierdzenia repliki | Opóźnienie i zależność dostępności |
| Asynchroniczny | Nie czeka na replikę                          | Możliwa utrata ostatnich zapisów   |

- Gwarancja zależy od konfiguracji potwierdzeń i scenariusza awarii.
- Oba tryby mogą odtworzyć na replice błędne usunięcie danych.

*PostgreSQL — Streaming replication*

| Obszar    | Dowód                                              |
|-----------|----------------------------------------------------|
| Dane      | Spójność, liczby rekordów i przykładowe zamówienia |
| Aplikacja | Zapis i realizacja testowego zamówienia            |
| Dostęp    | Klucze, role, DNS i sekrety dostępne               |
| Czas      | Pomiar całej ścieżki do przywrócenia usługi        |

- Środowisko odizolowane od produkcyjnych płatności i wysyłek.
- Wynik, brakujące kroki, właściciel poprawki i termin kolejnego testu.

| Strategia       | Gotowość zapasowa          | Koszt / czas                        |
|-----------------|----------------------------|-------------------------------------|
| Backup-restore  | Kopie i deklaracje         | Mniejszy stały koszt, dłuższy start |
| Warm standby    | Działający mniejszy system | Koszt gotowości i skalowania        |
| Aktywne regiony | Ruch w więcej niż jednym   | Złożoność spójności i routingu      |

*Google Cloud — Disaster recovery planning*



- Kopia zaszyfrowana kluczem dostępnym tylko w utraconym regionie może być nieużyteczna.
- Control plane potrzebny do utworzenia zasobów może być niedostępny.
- Próbę prowadzić z uwzględnieniem niedostępności regionu podstawowego.

## Dane

Błędnie usunięto 200 zamówień. Wykrycie o 09:50. Replika zawiera to samo usunięcie. Od 09:40 przyjęto 340 nowych zamówień. Dostępne base backup i pełne WAL.

- Do jakiego punktu odtworzyć dane?
- Czy można podmienić produkcję bazą sprzed DELETE?
- Jak odzyskać brakujące rekordy bez utraty nowych i podwójnej realizacji?

- NIST SP 800-34 Rev. 1 — Contingency Planning
- PostgreSQL — Continuous archiving and PITR
- PostgreSQL — Standby servers
- Google Cloud — DR planning guide

*Dokumentacja sprawdzona: 26.09.2026. Dane przypadków: przykłady dydaktyczne.*