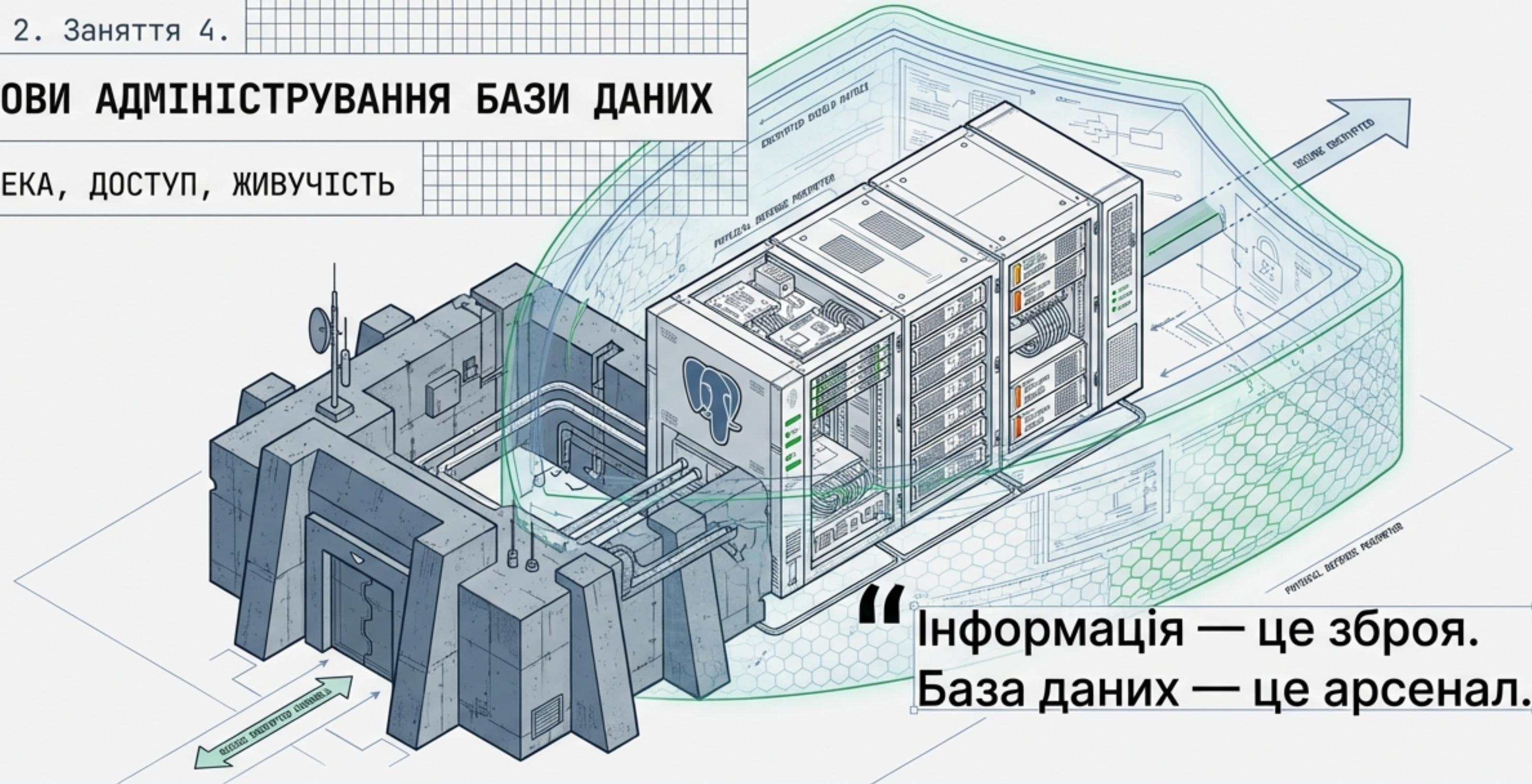


ОСНОВИ АДМІНІСТРУВАННЯ БАЗИ ДАНИХ

БЕЗПЕКА, ДОСТУП, ЖИВУЧІСТЬ



КОНТЕКСТ

Військовий аналітик діє в умовах, відмінних від цивільних: обмежені ресурси, нестабільний зв'язок та постійна кіберзагроза.



МІСІЯ

Адміністрування PostgreSQL у військовому контексті — це забезпечення інформаційної безпеки та безперервності командування.



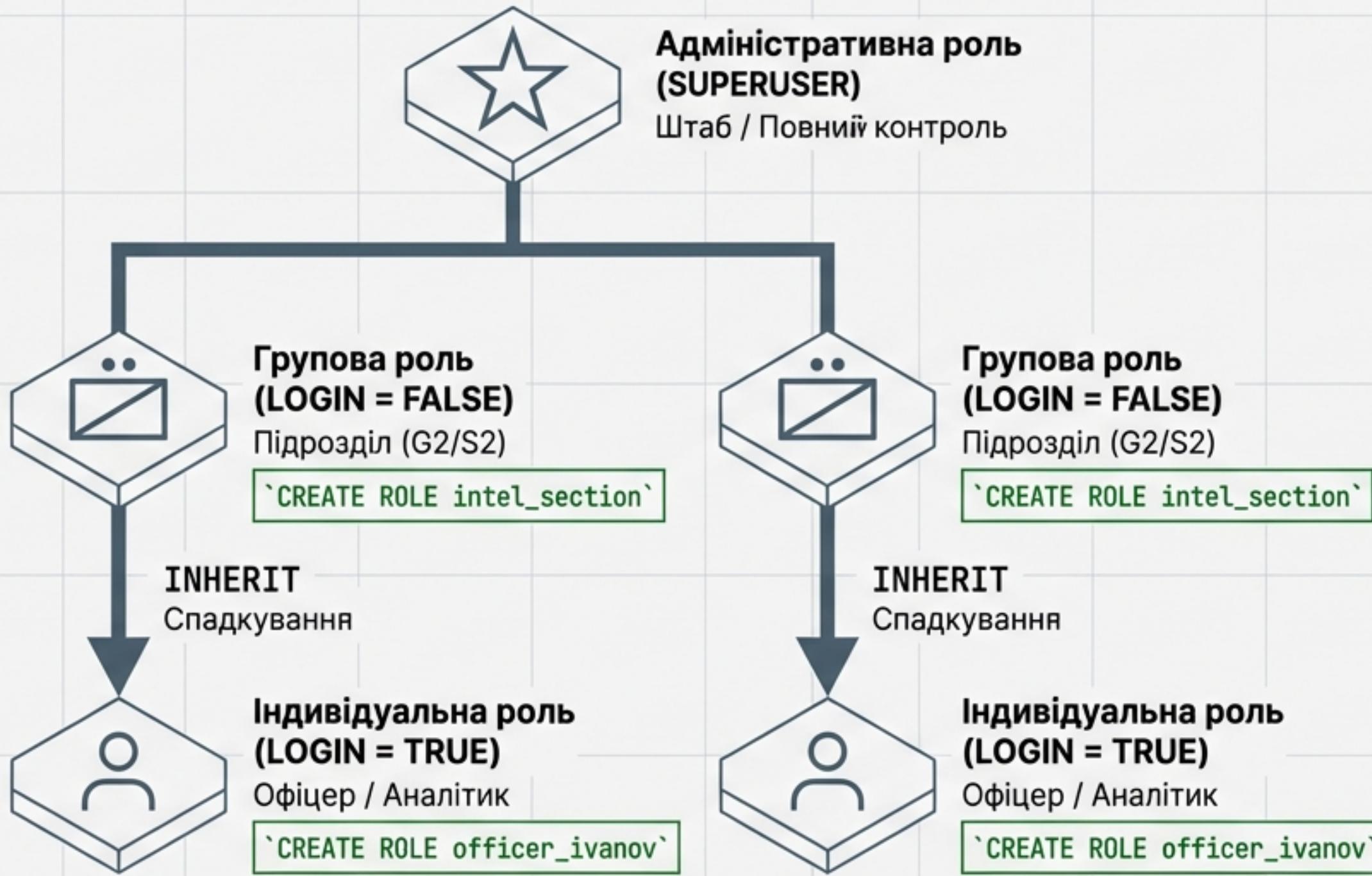
НАВИЧКИ

Адаптація структури під розвідувальні повідомлення, захист облікових записів та гарантія збереження даних при захопленні або знищенні вузла зв'язку.



АРХІТЕКТУРА УПРАВЛІННЯ ДОСТУПОМ: ІЕРАРХІЯ РОЛЕЙ

Концепція відповідності структури даних військовій вертикалі



КРИТИЧНЕ ПРАВИЛО

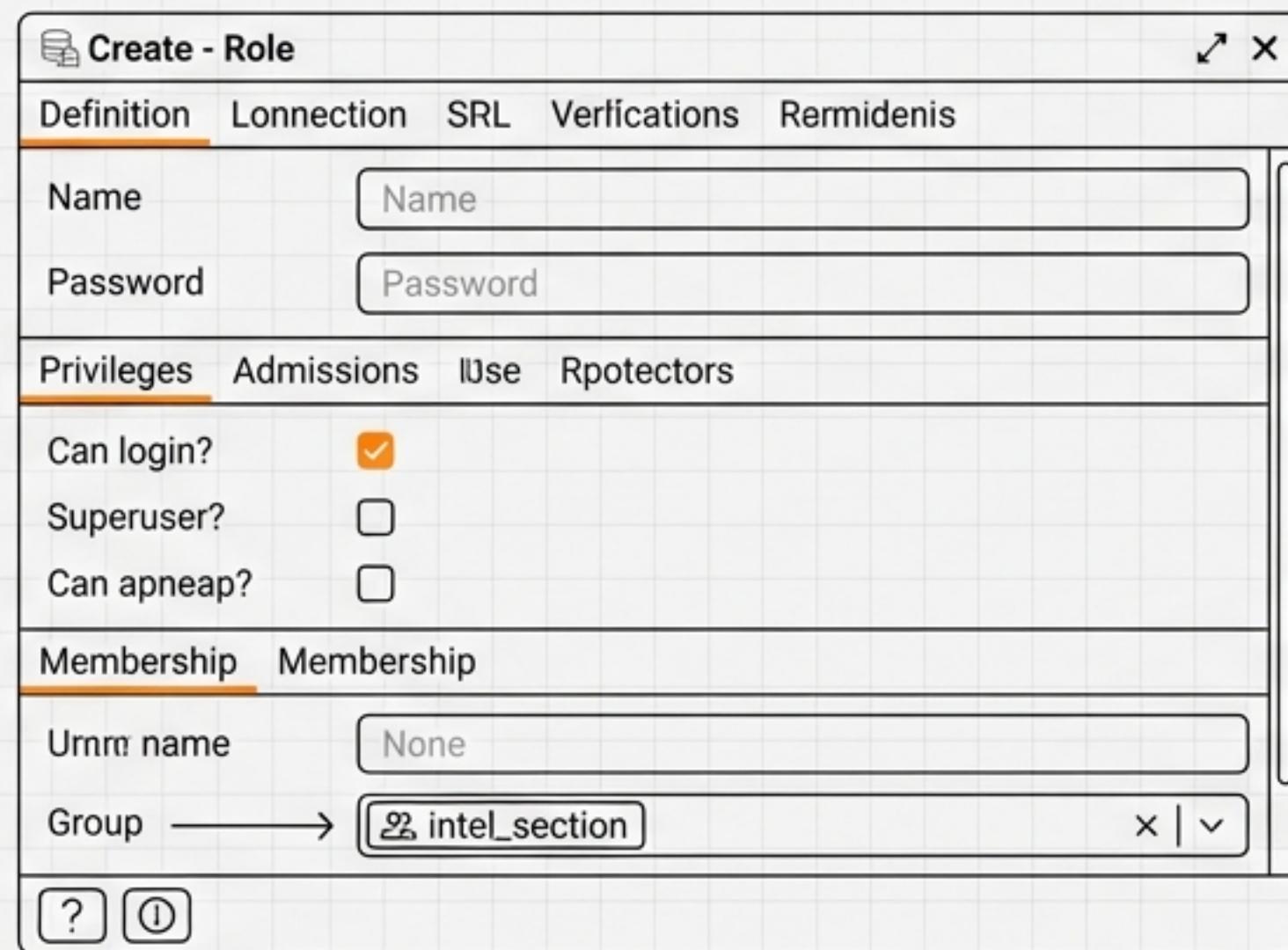
Ефективне адміністрування вимагає використання груп. Права надаються групі `intel_group`, а аналітики стають її членами. Зміни прав автоматично спадають.

PostgreSQL використовує уніфіковану концепцію «ролей» замість жорсткого поділу на користувачів та групи.

ТАКТИЧНЕ РОЗГОРТАННЯ: ІНСТРУМЕНТАРІЙ СТВОРЕННЯ АКАУНТІВ

МЕТОД 1: pgAdmin4 (GUI)

Швидке налаштування у польових штабах



Алгоритм: Правий клік "Login/Group Roles" -> "Create"

МЕТОД 2: VS Code (Code)

Масштабування та автоматизація

```
-- Створення групи
CREATE ROLE intel_section;

-- Створення користувача
CREATE ROLE officer_ivanov
LOGIN
PASSWORD 'StrongPass123'
IN ROLE intel_section;
```

IntelliSense підказує синтаксис та зменшує помилки.

МАТРИЦЯ ПРИВІЛЕЇВ ТА ПРИНЦИП НАЙМЕНШОГО ДОСТУПУ

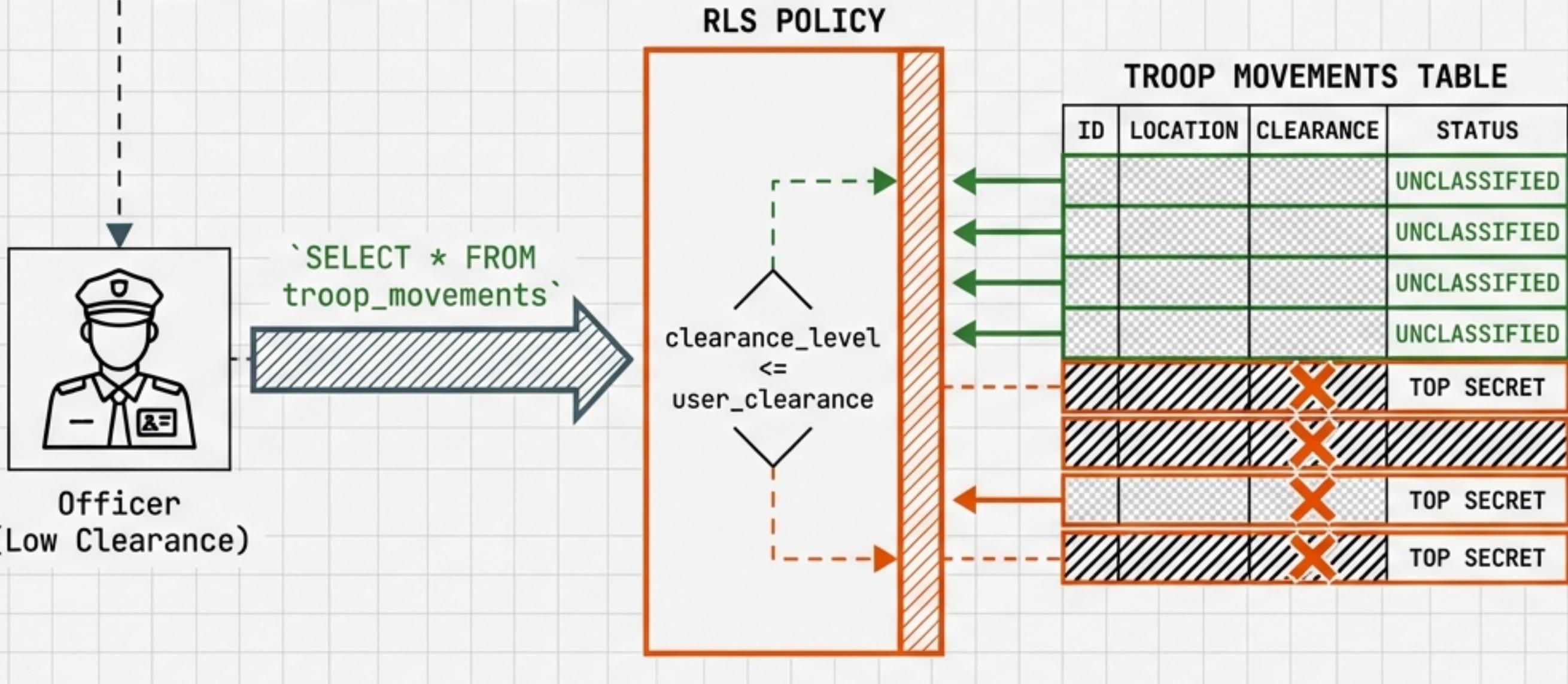
Стандарти безпеки (STIG): Доступ лише за потребою

CONNECT (Database)		Inter: Дозвіл на вхід (КПП бази даних).
USAGE (Schema)		Inter: Дозвіл бачити об'єкти всередині схеми (Доступ до приміщення).
SELECT (Table)		Inter: Читання звітів та карт (Тільки очі).
INSERT (Table)		Inter: Внесення нових цілей (Ввід даних).
UPDATE/DELETE		Inte: Зміна статусу або видалення помилкових даних.

КОНФІГУРАЦІЯ ЗА ЗАМОВЧУВАННЯМ:

```
REVOKE ALL ON SCHEMA public FROM PUBLIC; -- Закрити вільний доступ  
GRANT USAGE ON SCHEMA intelligence TO field_reporter;  
GRANT INSERT ON TABLE targets TO field_reporter;
```

РОЗМЕЖУВАННЯ ЗА ГРИФОМ СЕКРЕТНОСТІ: ROW-LEVEL SECURITY (RLS)



ПРОБЛЕМА

В одній таблиці зберігаються дані рівнів «Таємно» та «ДСК».

РІШЕННЯ

Політики безпеки RLS фільтрують рядки автоматично. База даних приховує рядки з грифом «Таємно», ніби їх не існує.

КОНФІГУРАЦІЯ RLS

```
ALTER TABLE troop_movements ENABLE ROW LEVEL SECURITY;
CREATE POLICY classification_filter ON troop_movements
USING (clearance_level <= (SELECT u_clearance FROM users WHERE name = current_user));
```

АУДИТ ТА МОНІТОРИНГ: «ЧОРНА СКРИНЬКА» СИСТЕМИ



1. ІНСТРУМЕНТ: pgAudit

Стандартні логи недостатні. pgAudit записує деталі сесії, забезпечуючи прозорість дій.



2. КОНФІГУРАЦІЯ (`postgresql.conf`)

`pgaudit.log = 'write, ddl, role'` Логування змін даних, структури та прав доступу.

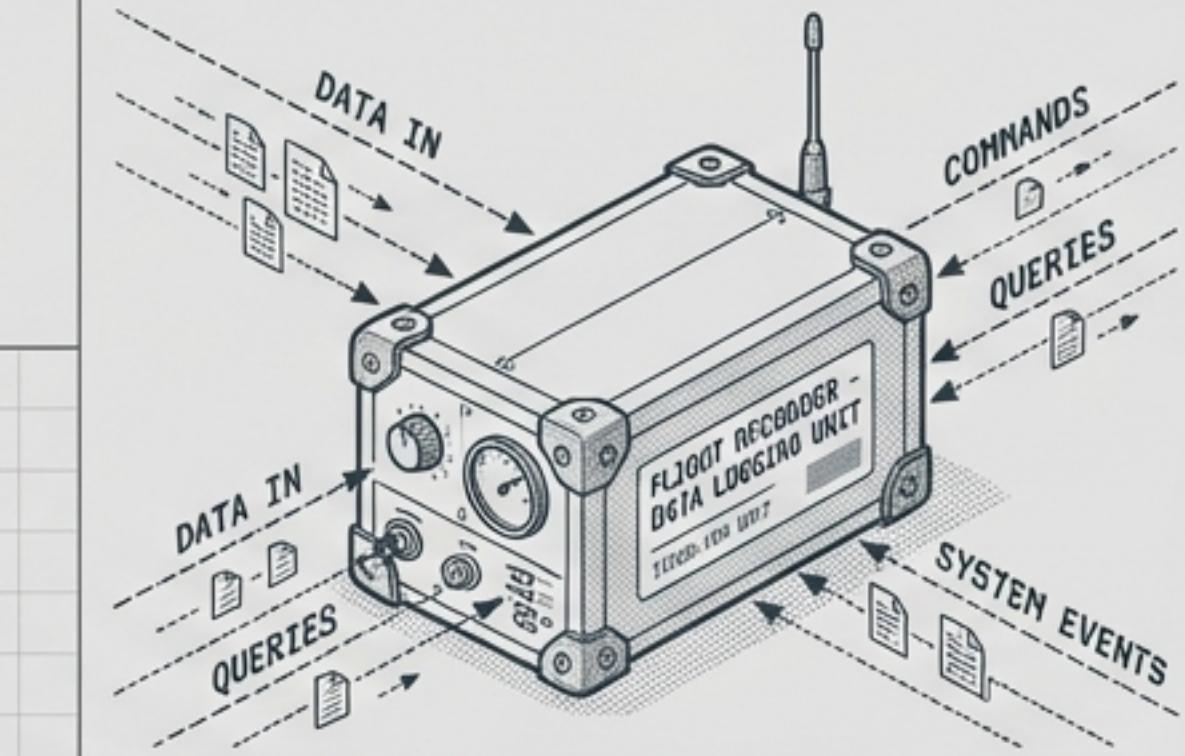
`pgaudit.log_parameter = on`

Запис конкретних значень (наприклад, передані координати), а не просто факту виконання команди.



3. АНАЛІЗ

Використання VS Code для пошуку в логах (**RegEx**) підозрілої активності, наприклад, масового вивантаження даних вночі.

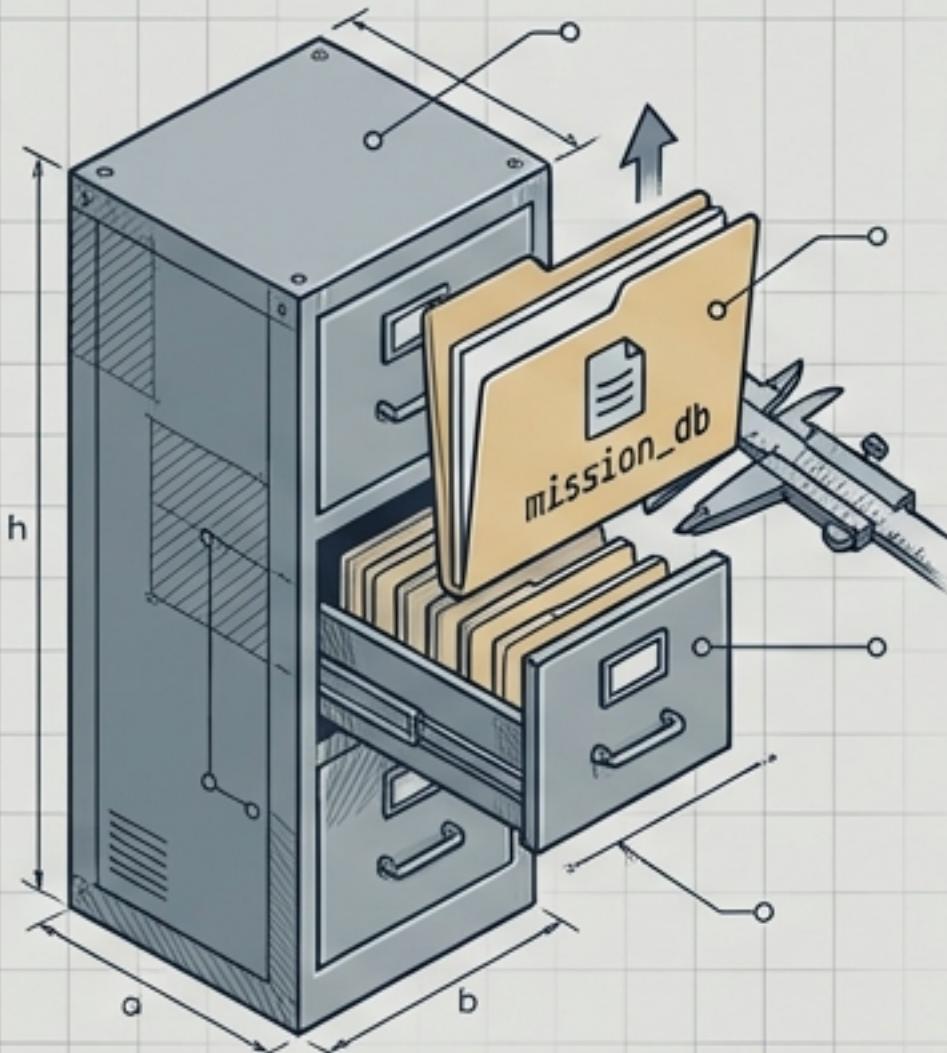


МОНІТОРИНГ НЕ ДЛЯ ШПИГУНСТВА, А ДЛЯ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ.

СТРАТЕГІЧНІ РЕЗЕРВИ: ФІЛОСОФІЯ РЕЗЕРВНОГО КОПІЮВАННЯ

Неперевірений бекап – це відсутність бекапу.

Логічне копіювання (`pg_dump`)



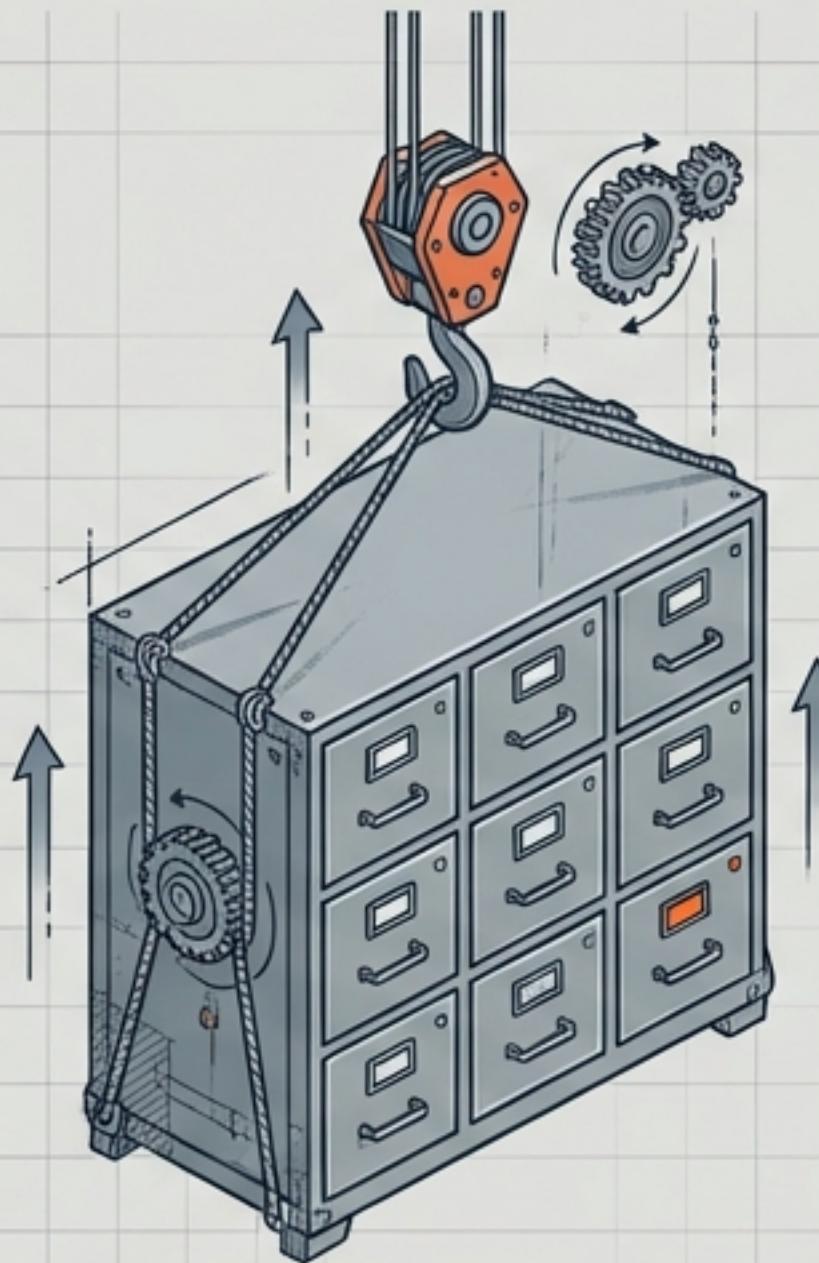
Сфера застосування:

Одна конкретна база
(наприклад,
'mission_db').

Операційне використання:

Збереження
оперативних даних
місії. Не блокує
роботу аналітиків.

Глобальне копіювання (`pg_dumpall`)



Сфера застосування:

Весь кластер:
Бази + Ролі + Табличні
простори.

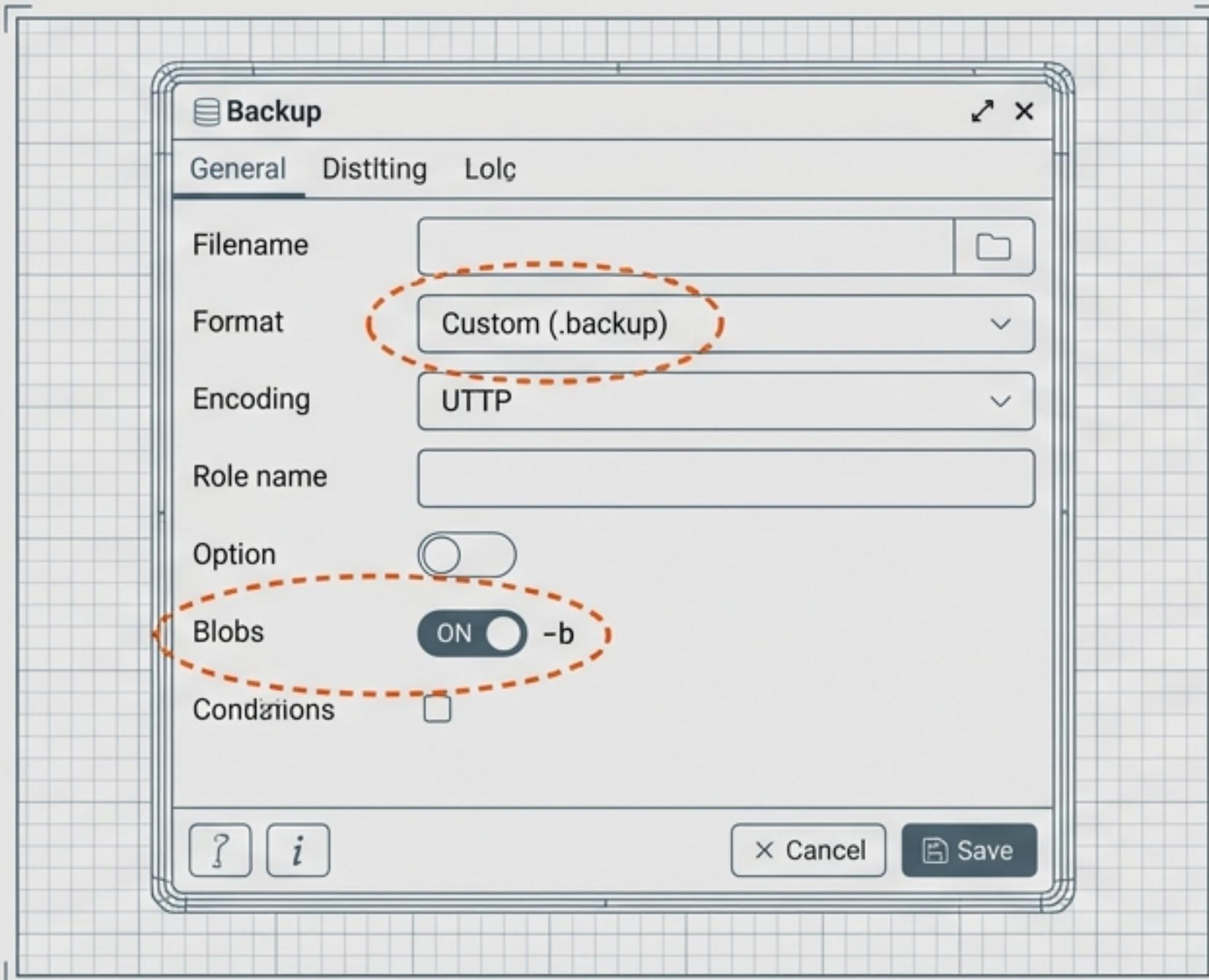
Операційне використання:

Міграція
інфраструктури. Без
цього доведеться
вручну створювати
користувачів на
новому сервері.

У разі обстрілу або кібератаки, копія бази – єдиний шанс відновити ситуаційну обізнаність.

ВИКОНАННЯ БЕКАПУ: ФОРМАТИ ТА НАЛАШТУВАННЯ

Інструмент: pgAdmin4



Format: Custom (.backup)

Рекомендований стандарт. Забезпечує стиснення (економія місця на захищених носіях) та дозволяє вибіркове відновлення.

Format: Plain Text (.sql)

Дозволяє редагування в VS Code (наприклад, зміна власника), але займає більше місця.

Option: -v (Verbose)

Докладне логування помилок.

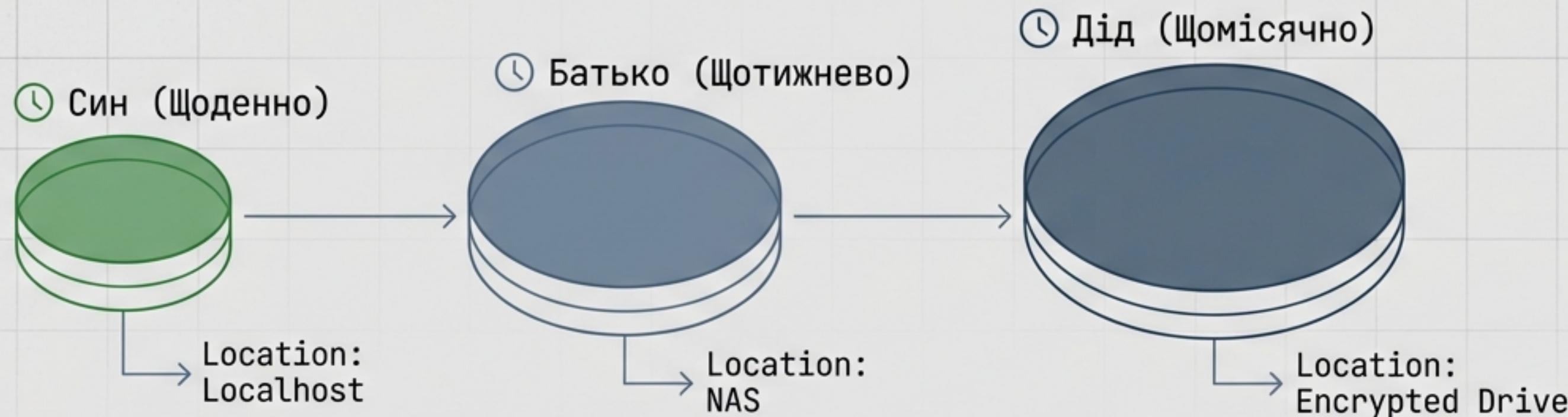
Option: -b (Blobs)

Обов'язково, якщо база містить супутникові знімки або скани документів.

АВТОМАТИЗАЦІЯ В ПОЛЬОВИХ УМОВАХ

Протокол «Встановив і забув»

Схема ротації: Дід-Батько-Син

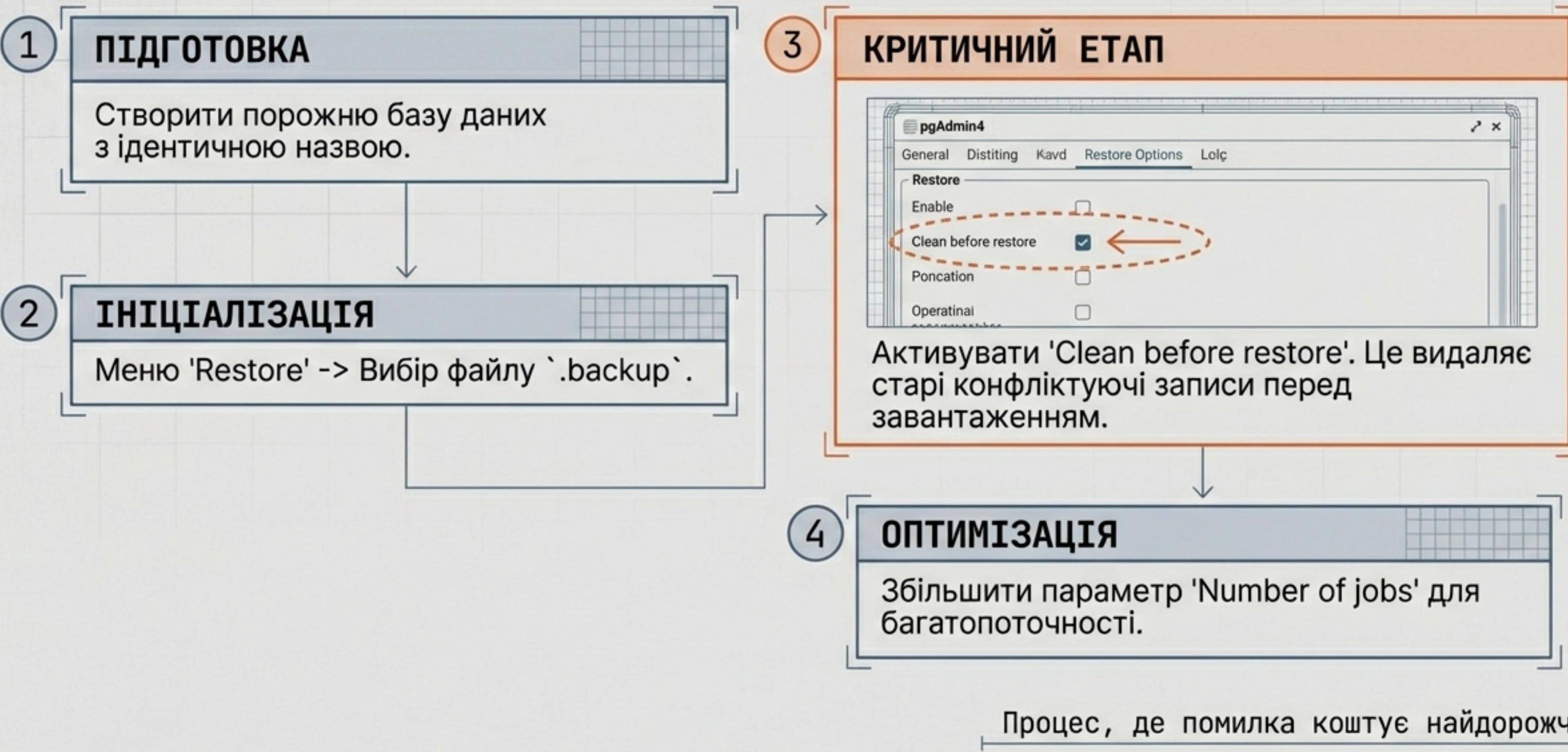


Аналітик не повинен покладатися на пам'ять.
Використовувати Cron (Linux) або Task Scheduler (Windows).

```
#!/bin/bash
# Автоматичний бекап бази даних розвідки
pg_dump -h localhost -U db_admin -F c -f "/backups/intel_db_$(date +%Y%m%d).backup" mission_db
```

ПРОТОКОЛ ВІДНОВЛЕННЯ: СТАНДАРТНА ПРОЦЕДУРА

Операція повернення часу (pgAdmin4)



АВАРІЙНІ СИТУАЦІЇ: ПОШКОДЖЕННЯ ДАНИХ

Інструменти останньої надії



Alert Box

Сценарій: Збій диска або живлення.

Помилка: `page verification failed`. Сервер не запускається.

The Nuclear Option (`pg_resetwal`)

Інструмент «останньої надії». Скидає журнали транзакцій (WAL), щоб примусово запустити базу.

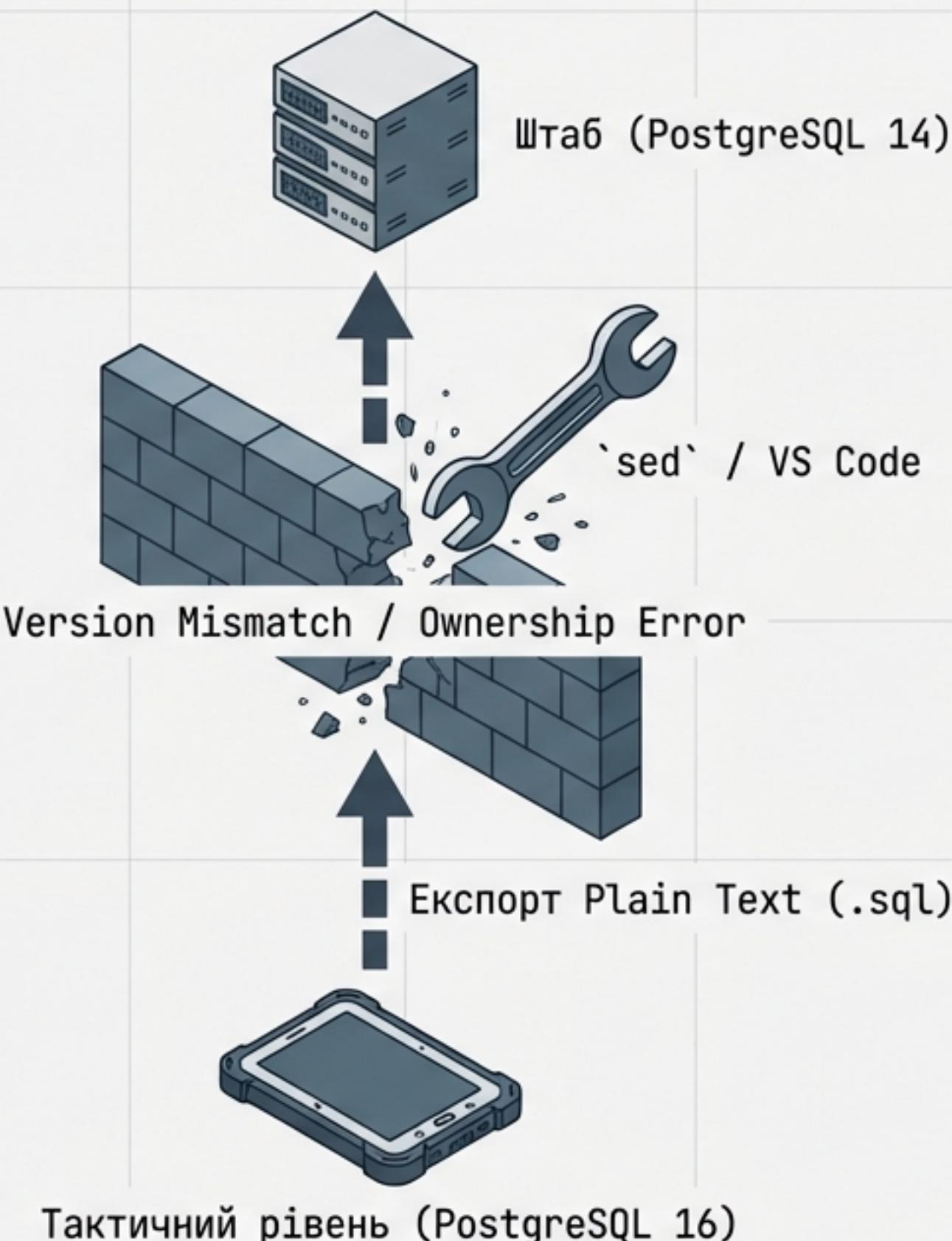
Можлива втрата останніх транзакцій, але порятунок основного масиву даних.

```
pg_resetwal -D /var/lib/postgresql/data
```

PITR (Point-In-Time Recovery)

Якщо ведеться архівація WAL, можливо відновити стан на 1 секунду до моменту помилки.

МІГРАЦІЯ ДАНИХ МІЖ ЕШЕЛОНAMI



Виклик:

Помилка `role 'postgres' does not exist` через розбіжність версій.

Рішення:

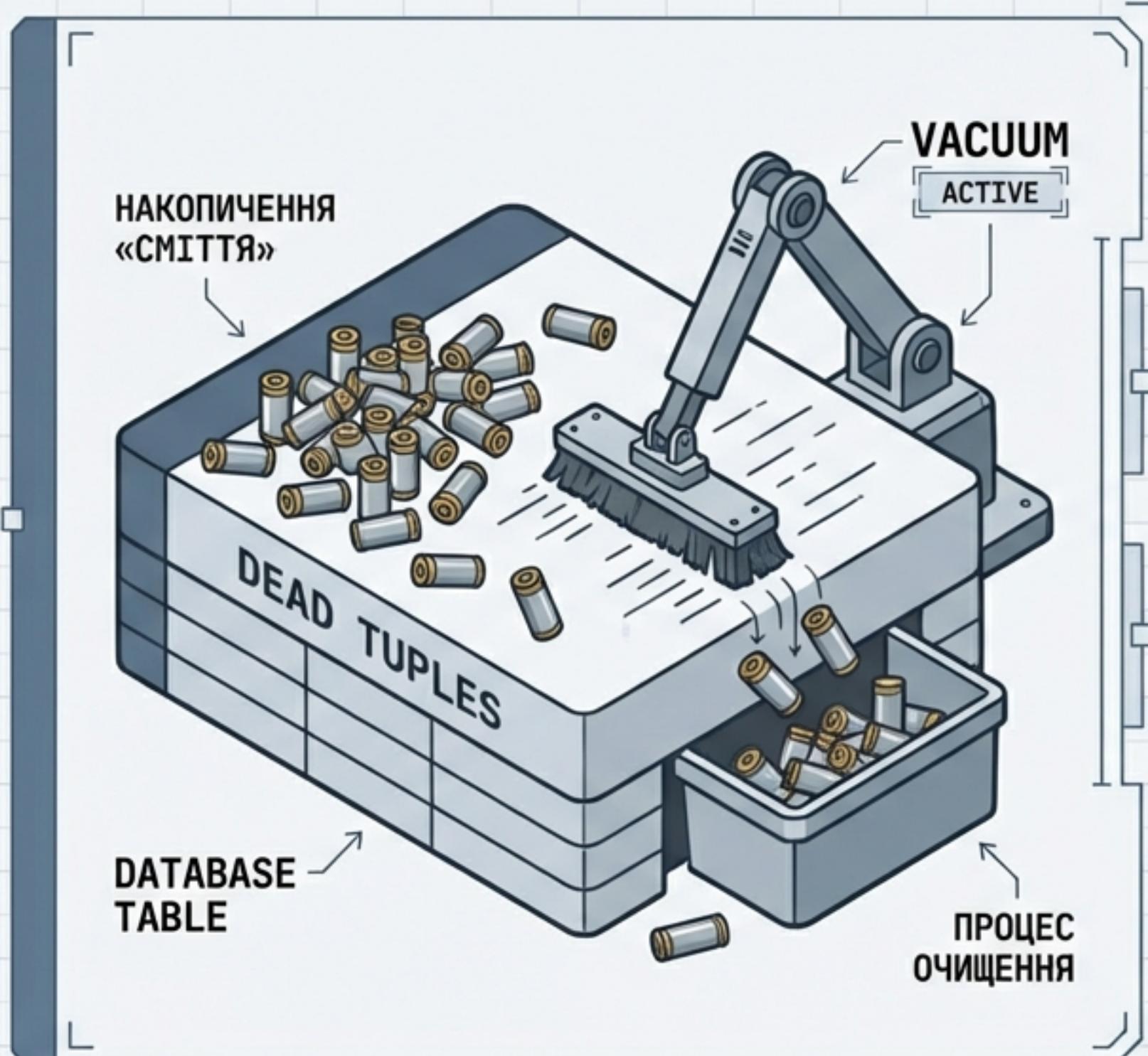
1. Використання формату **Plain Text (.sql)**.
2. Редагування власника через команду `sed`:

```
sed -i 's/OWNER TO postgres;/OWNER TO  
local_user;/g' backup.sql
```

Інструменти:

VS Code Extension дозволяє порівнювати схеми (Compare) та генерувати скрипти синхронізації.

ОБСЛУГОВУВАННЯ: ЗАБЕЗПЕЧЕННЯ БОЄЗДАТНОСТІ СИСТЕМИ



ПРОБЛЕМА: MVCC

Механізм версійності накопичує «сміття» (мертві кортежі). Без чистки база сповільнюється.

ПРОЦЕДУРА 1: VACUUM

Очищає місце, зайняте видаленими записами (як прибирання гільз після стрільби).

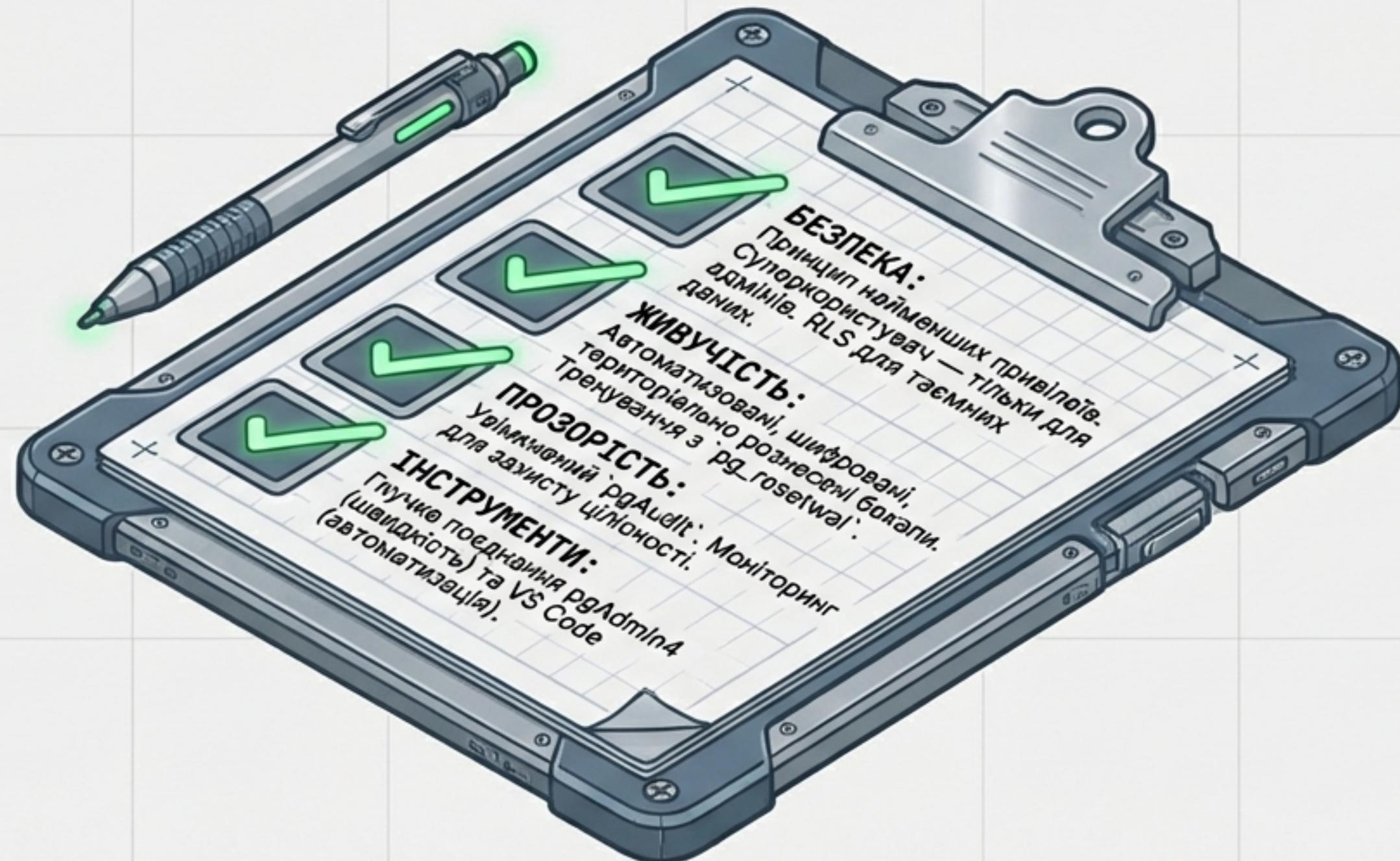
ПРОЦЕДУРА 2: ANALYZE

Оновлює статистику для планувальника запитів (пристрілка прицілу).

РЕКОМЕНДАЦІЯ

У періоди затишня запускати примусовий `VACUUM ANALYZE` через pgAgent для гарантії максимальної швидкодії перед активними фазами.

КОНТРОЛЬНИЙ СПИСОК АДМІНІСТРАТОРА



СТАЙКІСТЬ БАЗИ ДАНИХ — ЦЕ СТАЙКІСТЬ ПРИЙНЯТТЯ РІШЕНЬ КОМАНДИРОМ.