Разработка серверной части приложений PostgreSQL 16 **(dev-1)**

PL/pgSQL
Динамические команды

Темы

Причины использования

Выполнение динамического запроса

Способы формирования динамического запроса

Динамический SQL

Текст SQL-команды формируется в момент выполнения

Причины использования

- дополнительная гибкость в приложении
- формирование нескольких конкретных запросов вместо одного универсального для оптимизации

Цена

- операторы не подготавливаются
- возрастает риск внедрения SQL-кода
- возрастает сложность сопровождения

Выполнение запроса

Оператор EXECUTE

- выполняет строковое представление SQL-запроса
- позволяет использовать параметры
- переменные PL/pgSQL не становятся неявными параметрами

Может использоваться вместо SQL-запроса

- сам по себе
- при открытии курсора
- в цикле по запросу
- в предложении RETURN QUERY

Формирование команды

Подстановка значений параметров

- предложение USING
- гарантируется невозможность внедрения SQL-кода

Экранирование значений

- идентификаторы: `format('%I')`, `quote_ident`
- литералы: `format('%L')`, `quote_literal`, `quote_nullable`
- внедрение SQL-кода невозможно при правильном использовании

Обычные строковые функции

- конкатенация и др.
- возможно внедрение SQL-кода!

Итоги

Динамические команды дают дополнительную гибкость

Позволяют формировать отдельные запросы для разных значений параметров с целью оптимизации

Не подходят для коротких, частых запросов

Увеличивается сложность поддержки