PostgreSQL and Model Context Protocol (MCP)

What is

PostgreSQL

PostgreSQL is a powerful, open-source
relational database management system (RDBMS)
known for its reliability, robustness, and feature-rich design.
It supports complex queries, transactions, and data integrity,
making it suitable for everything from small apps
to large-scale enterprise systems.

What is

Model Context Protocol

Open Standard for AI Connectivity.
MCP is an open protocol (released November 25, 2024 by Anthropic)
that standardizes how large-language models (LLMs) connect to
external data sources and tools.

Think of MCP as a universal adapter for AI: one protocol to plug your
model into any service—databases, APIs, file stores, and more.

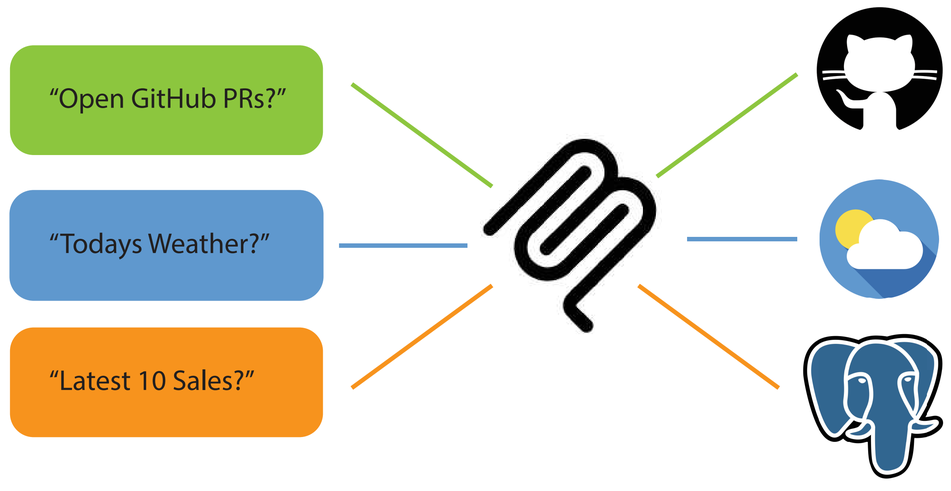
How It Works:
- The MCP Client (the LLM) speaks the MCP's wire protocol. (JSON-RPC 2.0)
- MCP Servers (connectors) wrap each target system behind that same protocol.
- The MCP Client can ask the MCP Server what it can do and how to call it.

Context is everything

LLMs generate best answers when they have the right background
information—everything else is just guessing.

Static vs. Dynamic
- Training data is a snapshot in time.
- Real-world questions often need up-to-date data,
  domain rules, or user-specific info.

Beyond the Prompt
- A few lines of text can't capture entire databases, APIs, or documentation.
- Injecting external context on demand fills the gaps.



Combining MCP and PostgreSQL

Open-Source MCP Servers for PostgreSQL

There are already several community-maintained MCP servers you can
deploy to bridge your LLM with a Postgres database.
These projects typically wrap your database behind the MCP
wire protocol and expose a common set of "tools" that the model can invoke.

Typical "tools" that may be exposed by a Postgres MCP server:

Tool Call

connect()

list_schemas(conn_id)

execute_sql(conn_id, sql)

Tool Response

```
{
  "conn_id": "12345"
}
```

```
{
  "public": ["users", "orders", "products"],
  "analytics": ["page_views", "sessions"]
}
```

```
[
  {"user_id":42,"total_spent":1200.50},
  {"user_id":17,"total_spent":1100.00},
  …
]
```

MCP servers may also offer "prompt tools" at a higher level that allow
clients to receive prompts from prompt templates bundled with data
from the server.

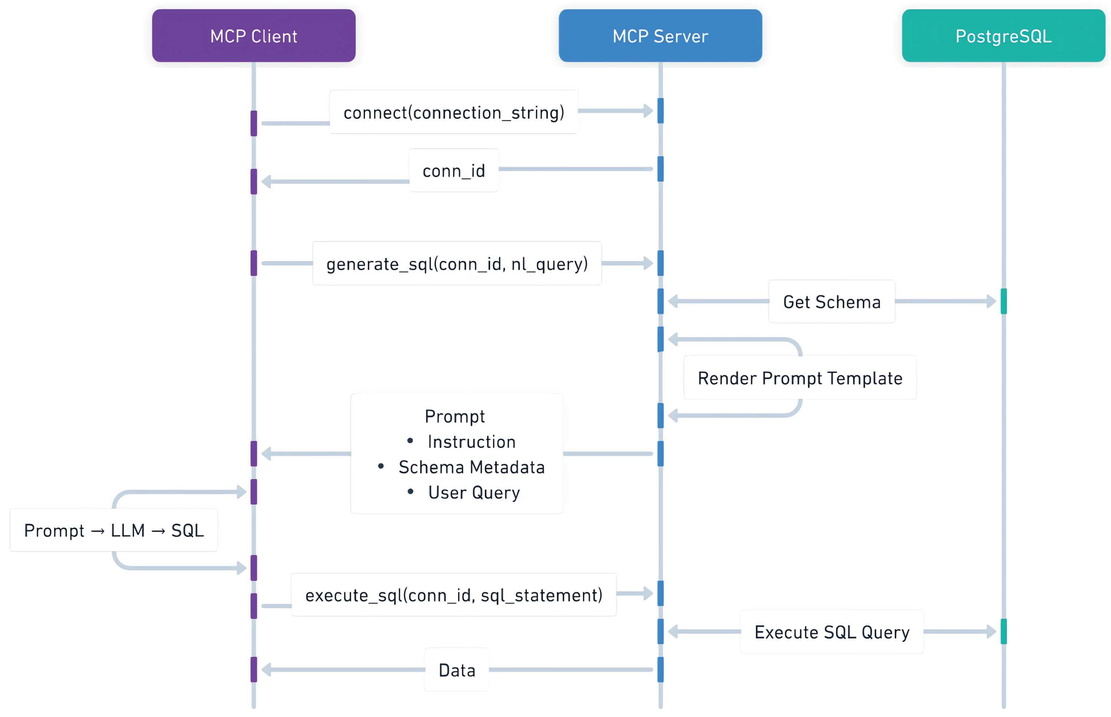
generate_sql(
conn_id=12345
nl_query="Give me all users")

```
{
  "role": "user",
  "content": "You are an expert PostgreSQL
              database query assistant. Your task is ...
              ... (Database schema here) ...
              ... Natural Language: Give me all users"
}
```

Create a MCP Client

MCP lets developers create tailored LLM agents for any task.
For example, you could build a simple chat interface where
users ask questions in plain English and instantly receive live
database results—no SQL required.

The following sequence diagram shows a simple client that
converts natural language into SQL and queries data through MCP.



IFS is developing a more advanced MCP PostgreSQL client that intelligently
validates and optimizes SQL queries before executing them and returning
the results to users.

IFS Institut für Software