# Release Notes

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Sponsors</td>
<td>3</td>
</tr>
<tr>
<td>2 Motivation</td>
<td>5</td>
</tr>
<tr>
<td>3 Declarative Programming</td>
<td>7</td>
</tr>
<tr>
<td>4 Leak-proof Abstraction</td>
<td>9</td>
</tr>
<tr>
<td>5 One Thing Well</td>
<td>11</td>
</tr>
<tr>
<td>6 Getting Support</td>
<td>13</td>
</tr>
<tr>
<td>6.1 v5.2.0</td>
<td>13</td>
</tr>
<tr>
<td>6.2 v6.0.2</td>
<td>14</td>
</tr>
<tr>
<td>6.3 v7.0.0</td>
<td>15</td>
</tr>
<tr>
<td>6.4 v7.0.1</td>
<td>17</td>
</tr>
<tr>
<td>6.5 v8.0.0</td>
<td>18</td>
</tr>
<tr>
<td>7 Tutorials</td>
<td>23</td>
</tr>
<tr>
<td>7.1 Tutorial 0 - Get it Running</td>
<td>23</td>
</tr>
<tr>
<td>7.2 Tutorial 1 - The Golden Key</td>
<td>26</td>
</tr>
<tr>
<td>8 Reference guides</td>
<td>33</td>
</tr>
<tr>
<td>8.1 Tables and Views</td>
<td>33</td>
</tr>
<tr>
<td>8.2 Resource Embedding</td>
<td>41</td>
</tr>
<tr>
<td>8.3 Insertions / Updates</td>
<td>47</td>
</tr>
<tr>
<td>8.4 Deletions</td>
<td>50</td>
</tr>
<tr>
<td>8.5 Custom Queries</td>
<td>51</td>
</tr>
<tr>
<td>8.6 Stored Procedures</td>
<td>51</td>
</tr>
<tr>
<td>8.7 Binary Output</td>
<td>55</td>
</tr>
<tr>
<td>8.8 OpenAPI Support</td>
<td>56</td>
</tr>
<tr>
<td>8.9 OPTIONS</td>
<td>56</td>
</tr>
<tr>
<td>8.10 Switching Schemas</td>
<td>57</td>
</tr>
<tr>
<td>8.11 HTTP Logic</td>
<td>58</td>
</tr>
<tr>
<td>8.12 Configuration</td>
<td>61</td>
</tr>
<tr>
<td>8.13 Environment Variables</td>
<td>68</td>
</tr>
<tr>
<td>8.14 Configuration Reloading</td>
<td>68</td>
</tr>
<tr>
<td>8.15 In-Database Configuration</td>
<td>68</td>
</tr>
</tbody>
</table>
# Topic guides

9.1 Overview of Role System ................................................. 73
9.2 Client Auth ................................................................. 77
9.3 Schema Isolation ............................................................ 80
9.4 SQL User Management .................................................... 80
9.5 Schema Isolation ............................................................ 83
9.6 Functions ................................................................. 83
9.7 Views ................................................................. 84
9.8 Hardening PostgREST .................................................. 85
9.9 Debugging .............................................................. 87
9.10 Daemonizing ............................................................. 89
9.11 Alternate URL Structure .............................................. 89
9.12 Installation ............................................................... 90
9.13 Running PostgREST ................................................... 90
9.14 Docker ................................................................. 91
9.15 Building from Source .................................................. 93
9.16 Deploying to Heroku ................................................... 94

# How-to guides

10.1 Casting a type to a custom JSON object ................................ 95
10.2 Embedding a table from another schema ................................ 96
10.3 Providing images for `<img> ........................................ 98

# Ecosystem

11.1 Community Tutorials ................................................... 101
11.2 Example Apps .......................................................... 101
11.3 DevOps ............................................................... 102
11.4 External Notification .................................................. 102
11.5 Extensions .............................................................. 103
11.6 Client-Side Libraries .................................................. 103

# Release Notes

12 ........................................................................ 105

# In Production

13 ........................................................................ 107

# Testimonials

14 ........................................................................ 109

# Contributing

15 ........................................................................ 111
PostgREST is a standalone web server that turns your PostgreSQL database directly into a RESTful API. The structural constraints and permissions in the database determine the API endpoints and operations.
CHAPTER 1

Sponsors

CYBERTEC
DATA SCIENCE & POSTGRESQL

2ndQuadrant®
PostgreSQL

Retool
PostgREST for the backend.
Retool for the frontend.

GNUHOST

supabase

Oblivious
Using PostgREST is an alternative to manual CRUD programming. Custom API servers suffer problems. Writing business logic often duplicates, ignores or hobbles database structure. Object-relational mapping is a leaky abstraction leading to slow imperative code. The PostgREST philosophy establishes a single declarative source of truth: the data itself.
Declarative Programming

It’s easier to ask PostgreSQL to join data for you and let its query planner figure out the details than to loop through rows yourself. It’s easier to assign permissions to db objects than to add guards in controllers. (This is especially true for cascading permissions in data dependencies.) It’s easier to set constraints than to litter code with sanity checks.
Leak-proof Abstraction

There is no ORM involved. Creating new views happens in SQL with known performance implications. A database administrator can now create an API from scratch with no custom programming.
PostgREST has a focused scope. It works well with other tools like Nginx. This forces you to cleanly separate the data-centric CRUD operations from other concerns. Use a collection of sharp tools rather than building a big ball of mud.
The project has a friendly and growing community. Join our chat room for discussion and help. You can also report or search for bugs/features on the Github issues page.

6.1 v5.2.0

- **Explicit qualification** introduced in v5.0 is no longer necessary, this section will not be included from this version onwards. A `db-extra-search-path` configuration parameter was introduced to avoid the need to explicitly qualify database objects. If you install PostgreSQL extensions on the public schema, they’ll work normally from now on.
- Now you can filter *Table / Columns with spaces*.
- Included the ability to quote columns that have *Reserved characters*.
- Thanks to Zhou Feng, now is possible to reference an external file in `db-uri`.
- Thanks to Russell Davies, Json Web Key Sets are now accepted by `jwt-secret`.

6.1.1 Thanks

This release was made possible thanks to:

- Daniel Babiak
- Michel Pelletier
- Tsingson Qin
- Jay Hannah
- Victor Adossi
- Petr Beles

If you like to join them please consider supporting PostgREST development.
6.2 v6.0.2

Full changelog is available at PostgREST releases page.

6.2.1 Added

- Ignoring payload keys for insert/update can be now done with the \texttt{?columns} query parameter. See \textit{Specifying Columns}. – @steve-chavez
- \texttt{websearch_to_tsquery} can now be used through the \texttt{wfts} operator. See \textit{Full-Text Search}. – @herulume
- Resource Embedding on materialized views is now possible. See \textit{Embedding Views}. – @vitorbaptista
- Bulk calling an RPC is now allowed. See \textit{Bulk Call}. – @steve-chavez
- It’s now possible to request a \texttt{text/plain} output. See \textit{Plain Text Output}. – @steve-chavez
- Config option for specifying PostgREST database pool timeout. See \texttt{db-pool-timeout}. – @Qu4tro
- Config option for binding the PostgREST web server to an unix socket. See \texttt{server-unix-socket}. – @Dansvidania
- Config option for extending the supported media types. See \texttt{raw-media-types}. – @Dansvidania
- We now offer an statically linked binary for Linux. Look for \texttt{postgrest-<version>-linux-x64-static.tar.xz} on the releases page. – @clojurians-org
- A \textit{How-to guides} section was added to the documentation.

6.2.2 Changed

- \texttt{SIGHUP} support was removed. You should use \texttt{SIGUSR1} instead. See \textit{Schema Cache Reloading}.
- server-host default of 127.0.0.1 was changed to \texttt{!4}. See \texttt{server-host}.

6.2.3 Thanks

This release is sponsored by:

- Daniel Babiak
- Evans Fernandes
• Tsingson Qin
• Michel Pelletier
• Jay Hannah
• Robert Stolarz
• Kofi Gumbs
• Nicholas DiBiase
• Christopher Reid
• Nathan Bouscal

If you like to join them please consider supporting PostgREST development.

6.3 v7.0.0

You can download this release at the PostgREST v7.0.0 release page.

6.3.1 Added

• Support for Switching to a schema defined in db-schema. – @steve-chavez, @mahmoudkassem
• Support for Planned Count and Estimated Count. – @steve-chavez, @LorenzHenk
• Support for the on_conflict query parameter to UPSERT based on a unique constraint. – @ykst
• Support for Resource Embedding Disambiguation. – @steve-chavez
• Support for user defined socket permission via server-unix-socket-mode config option – @Dansvidania
• HTTP logic improvements – @steve-chavez
  – Support for HTTP HEAD requests.
  – GUCs for Accessing Request Path and Method.
  – Support for Setting headers via pre-request.
  – Allow overriding provided headers(Content-Type, Location, etc) by Setting Response Headers
  – Access to the Authorization header value through request.header.authorization
• Documentation improvements
  – Explanation for Schema Structure.
  – Reference for Embedding on Stored Procedures.
  – Reference for Embedding after Insertions/Updates/Deletions.
  – Reference for filters on JSON Columns.
  – How-to for Providing images for <img>.
  – Added Community Tutorials section.
6.3.2 Fixed

- Allow embedding a view when its source table foreign key is UNIQUE – @bwbroersma
- Accept: application/vnd.pgrst.object+json behavior is now enforced for POST/PATCH/DELETE regardless of Prefer: return=minimal – @dwagin
- Fix self join resource embedding on PATCH – @herulume, @steve-chavez
- Allow PATCH/DELETE without Prefer: return=minimal on tables with no SELECT privileges – @steve-chavez
- Fix many to many resource embedding for RPC/PATCH – @steve-chavez

6.3.3 Changed

- **Bulk Call** should now be done by specifying a Prefer: params=multiple-objects header. This fixes a performance regression when calling stored procedures.
- Resource Embedding now outputs an error when multiple relationships between two tables are found, see **Embedding Disambiguation**.
- server-proxy-uri config option has been renamed to openapi-server-proxy-uri.
- Default Unix Socket file mode from 755 to 660

6.3.4 Thanks

This release was made possible thanks to:

- Daniel Babiak
- Evans Fernandes
- Jan Sommer
- Tsingson Qin
- Michel Pelletier
- Jay Hannah
- Robert Stolarz
PostgREST Documentation, Release 8.0.0

• Kofi Gumbs
• Nicholas DiBiase
• Christopher Reid
• Nathan Bouscal
• Daniel Rafaj
• David Fenko

If you like to join them please consider supporting PostgREST development.

6.4 v7.0.1

You can see the full changelog at PostgREST v7.0.1 release page.

6.4.1 Fixed

• Fix overloaded computed columns on RPC – @wolfgangwalther
• Fix POST, PATCH, DELETE with ?select= and Prefer: return=minimal and PATCH with empty body – @wolfgangwalther
• Fix missing openapi-server-proxy-uri config option – @steve-chavez
• Fix Content-Profile not working for POST RPC – @steve-chavez
• Fix PUT restriction for including all columns in payload – @steve-chavez
• Documentation improvements
  – Added package managers to Installation.

6.4.2 Changed

• From this version onwards, the release page will include a single Linux static executable that can be run on any Linux distribution.

6.4.3 Thanks

This release was made possible thanks to:

![CYBERTEC](image)

![2ndQuadrant](image)
If you’d like to join them, consider supporting PostgREST development.

6.5 v8.0.0

You can download this release at the PostgREST v8.0.0 release page.

6.5.1 Added

- Allow HTTP status override through the `response.status` GUC. – @steve-chavez
- Allow Calling variadic functions. – @wolfgangwalther
- Allow Embedding Chains of Views recursively to any depth. – @wolfgangwalther
- No downtime when reloading the schema cache. See Schema Cache Reloading. – @steve-chavez
- Allow schema cache reloading using PostgreSQL `NOTIFY` command. This enables Automatic Schema Cache Reloading. – @steve-chavez
- Allow sending the header `Prefer: headers-only` to get a response with a `Location` header. See Insertions / Updates. – @laurenceisla
- Allow Using External Connection Poolers such as PgBouncer in transaction pooling mode. – @laurenceisla
- Allow Configuration Reloading by sending a SIGUSR2 signal. – @steve-chavez
- Allow Bearer with and without capitalization as authentication schema. See Client Auth. – @wolfgangwalther
- In-Database Configuration that can be reloaded with NOTIFY. – @steve-chavez
- Allow OPTIONS to generate HTTP methods based on views triggers. See OPTIONS requests. – @laurenceisla
• Show timestamps for server diagnostic information. See Logging. – @steve-chavez
• Config options for showing a full OpenAPI output regardless of the JWT role privileges and for disabling it altogether. See openapi-mode. – @steve-chavez
• Config option for logging level. See log-level. – @steve-chavez
• Config option for enabling or disabling prepared statements. See db-prepared-statements. – @steve-chavez
• Config option for specifying how to terminate the transactions (allowing rollbacks, useful for testing). See db-tx-end. – @wolfgangwalther
• Documentation improvements
  – Added the Schema Cache page.
  – Moved the Schema Cache Reloading reference from Hardening PostgREST to Schema Cache

### 6.5.2 Changed

• Docker images are now optimized to be built from the scratch image. This reduces the compressed image size from over 30 MB to about 4 MB. For more details, see Docker image built with Nix. – @monacoremo
• The Docker image no longer has an internal /etc/postgrest.conf file, you must use Environment Variables to configure it. – @wolfgangwalther
• The pg_listen utility is no longer needed to automatically reload the schema cache and it’s replaced entirely by database notifications. See Automatic Schema Cache Reloading. – @steve-chavez
• POST requests for insertions no longer include a Location header in the response by default and behave the same way as having a Prefer: return=minimal header in the request. This prevents permissions errors when having a write-only table. See Insertions / Updates. – @laurenceisla
• Modified the default logging level from info to error. See log-level. – @steve-chavez
• Changed the error message for a not found RPC on a stale schema (see Stale Function Signature) and for the unsupported case of overloaded functions with the same argument names but different types. – @laurenceisla
• Changed the error message for the no relationship found error. See Stale Foreign Key Relationships. – @laurenceisla

### 6.5.3 Fixed

• Fix showing UNKNOWN on postgrest --help invocation. – @monacoremo
• Removed single column restriction to allow composite foreign keys in join tables. – @goteguru
• Fix expired JWTs starting an empty transaction on the db. – @steve-chavez
• Fix location header for POST request with select= without PK. – @wolfgangwalther
• Fix error messages on connection failure for localized PostgreSQL on Windows. – @wolfgangwalther
• Fix application/octet-stream appending charset=utf-8. – @steve-chavez
• Fix overloading of functions with unnamed arguments. – @wolfgangwalther
• Return 405 Method not Allowed for GET of volatile RPC instead of 500. – @wolfgangwalther
• Fix RPC return type handling and embedding for domains with composite base type. – @wolfgangwalther
• Fix embedding through views that have COALESCE with subselect. – @wolfgangwalther
• Fix parsing of boolean config values for Docker environment variables, now it accepts double quoted truth values ("true", "false") and numbers ("1", "0"). – @wolfgangwalther

• Fix using `app.settings.xxx` config options in Docker, now they can be used as `PGRST_APP_SETTINGS_xxx`. – @wolfgangwalther

• Fix panic when attempting to run with unix socket on non-unix host and properly close unix domain socket on exit. – @monacoremo

• Disregard internal junction (in non-exposed schema) when embedding. – @steve-chavez

• Fix requests for overloaded functions from HTML forms to no longer hang. – @laurenceisla

6.5.4 Thanks

Big thanks from the PostgREST team to our sponsors!

- Evans Fernandes
- Jan Sommer
- Franz Gusenbauer
- Daniel Babiak
- Tsingson Qin
- Michel Pelletier
- Jay Hannah
- Robert Stolarz
- Nicholas DiBiase
- Christopher Reid
- Nathan Bouscal
• Daniel Rafaj
• David Fenko
• Remo Rechkemmer
• Severin Ibarluzea
• Tom Saleeba
• Pawel Tyll

If you like to join them please consider supporting PostgREST development.
Are you new to PostgREST? This is the place to start!

7.1 Tutorial 0 - Get it Running

author begriffs

Welcome to PostgREST! In this pre-tutorial we’re going to get things running so you can create your first simple API.

PostgREST is a standalone web server which turns a PostgreSQL database into a RESTful API. It serves an API that is customized based on the structure of the underlying database.

To make an API we’ll simply be building a database. All the endpoints and permissions come from database objects like tables, views, roles, and stored procedures. These tutorials will cover a number of common scenarios and how to model them in the database.

By the end of this tutorial you’ll have a working database, PostgREST server, and a simple single-user todo list API.

7.1.1 Step 1. Relax, we’ll help

As you begin the tutorial, pop open the project chat room in another tab. There are a nice group of people active in the project and we’ll help you out if you get stuck.
7.1.2 Step 2. Install PostgreSQL

If you’re already familiar with using PostgreSQL and have it installed on your system you can use the existing installation (see Postgres dependency for minimum requirements). For this tutorial we’ll describe how to use the database in Docker because database configuration is otherwise too complicated for a simple tutorial.

If Docker is not installed, you can get it here. Next, let’s pull and start the database image:

```
sudo docker run --name tutorial -p 5433:5432 \\
-e POSTGRES_PASSWORD=mysecretpassword \\
-d postgres
```

This will run the Docker instance as a daemon and expose port 5433 to the host system so that it looks like an ordinary PostgreSQL server to the rest of the system.

7.1.3 Step 3. Install PostgREST

PostgREST is distributed as a single binary, with versions compiled for major distributions of Linux/BSD/Windows. Visit the latest release for a list of downloads. In the event that your platform is not among those already pre-built, see Building from Source for instructions how to build it yourself. Also let us know to add your platform in the next release.

The pre-built binaries for download are .tar.xz compressed files (except Windows which is a zip file). To extract the binary, go into the terminal and run

```
# download from https://github.com/PostgREST/postgrest/releases/latest
tar xJf postgrest-<version>-<platform>.tar.xz
```

The result will be a file named simply postgrest (or postgrest.exe on Windows). At this point try running it with

```
./postgrest
```

If everything is working correctly it will print out its version and information about configuration. You can continue to run this binary from where you downloaded it, or copy it to a system directory like /usr/local/bin on Linux so that you will be able to run it from any directory.

**Note:** PostgREST requires libpq, the PostgreSQL C library, to be installed on your system. Without the library you’ll get an error like “error while loading shared libraries: libpq.so.5.” Here’s how to fix it:

7.1.4 Step 4. Create Database for API

Connect to the SQL console (psql) inside the container. To do so, run this from your command line:

```
sudo docker exec -it tutorial psql -U postgres
```

You should see the psql command prompt:

```
psql (9.6.3)
Type "help" for help.
postgres=#
```
The first thing we’ll do is create a named schema for the database objects which will be exposed in the API. We can choose any name we like, so how about “api.” Execute this and the other SQL statements inside the psql prompt you started.

```sql
create schema api;
```

Our API will have one endpoint, /todos, which will come from a table.

```sql
create table api.todos (
    id serial primary key,
    done boolean not null default false,
    task text not null,
    due timestamptz
);
insert into api.todos (task) values ('finish tutorial 0'), ('pat self on back');
```

Next make a role to use for anonymous web requests. When a request comes in, PostgREST will switch into this role in the database to run queries.

```sql
create role web_anon nologin;
grant usage on schema api to web_anon;
grant select on api.todos to web_anon;
```

The `web_anon` role has permission to access things in the `api` schema, and to read rows in the `todos` table.

It’s a good practice to create a dedicated role for connecting to the database, instead of using the highly privileged `postgres` role. So we’ll do that, name the role `authenticator` and also grant him the ability to switch to the `web_anon` role:

```sql
create role authenticator noinherit login password 'mysecretpassword';
grant web_anon to authenticator;
```

Now quit out of psql; it’s time to start the API!

```sql
\q
```

### 7.1.5 Step 5. Run PostgREST

PostgREST uses a configuration file to tell it how to connect to the database. Create a file `tutorial.conf` with this inside:

```ini
[database]
db-uri = "postgres:///authenticator:mysecretpassword@localhost:5433/postgres"
db-schema = "api"
db-anon-role = "web_anon"
```

The configuration file has other options, but this is all we need. If you are not using Docker, make sure that your port number is correct and replace `postgres` with the name of the database where you added the todos table.

Now run the server:

```bash
./postgrest tutorial.conf
```

You should see
Listening on port 3000
Attempting to connect to the database...
Connection successful

It’s now ready to serve web requests. There are many nice graphical API exploration tools you can use, but for this tutorial we’ll use curl because it’s likely to be installed on your system already. Open a new terminal (leaving the one open that PostgREST is running inside). Try doing an HTTP request for the todos.

curl http://localhost:3000/todos

The API replies:

```
[
  
  {
    "id": 1,
    "done": false,
    "task": "finish tutorial 0",
    "due": null
  },

  {
    "id": 2,
    "done": false,
    "task": "pat self on back",
    "due": null
  }
]
```

With the current role permissions, anonymous requests have read-only access to the todos table. If we try to add a new todo we are not able.

curl http://localhost:3000/todos -X POST \
   -H "Content-Type: application/json" \
   -d '{"task": "do bad thing"}'

Response is 401 Unauthorized:

```
{
  "hint": null,
  "details": null,
  "code": "42501",
  "message": "permission denied for relation todos"
}
```

There we have it, a basic API on top of the database! In the next tutorials we will see how to extend the example with more sophisticated user access controls, and more tables and queries.

Now that you have PostgREST running, try the next tutorial, Tutorial 1 - The Golden Key

### 7.2 Tutorial 1 - The Golden Key

**author** begriffs

In Tutorial 0 - Get it Running we created a read-only API with a single endpoint to list todos. There are many directions we can go to make this API more interesting, but one good place to start would be allowing some users to change data in addition to reading it.
7.2.1 Step 1. Add a Trusted User

The previous tutorial created a `web_anon` role in the database with which to execute anonymous web requests. Let’s make a role called `todo_user` for users who authenticate with the API. This role will have the authority to do anything to the todo list.

```
-- run this in psql using the database created
-- in the previous tutorial
create role todo_user nologin;
grant todo_user to authenticator;
grant usage on schema api to todo_user;
grant all on api.todos to todo_user;
grant usage, select on sequence api.todos_id_seq to todo_user;
```

7.2.2 Step 2. Make a Secret

Clients authenticate with the API using JSON Web Tokens. These are JSON objects which are cryptographically signed using a password known to only us and the server. Because clients do not know the password, they cannot tamper with the contents of their tokens. PostgREST will detect counterfeit tokens and will reject them.

Let’s create a password and provide it to PostgREST. Think of a nice long one, or use a tool to generate it. Your password must be at least 32 characters long.

**Note:** Unix tools can generate a nice password for you:

```
# Allow "tr" to process non-utf8 byte sequences
export LC_CTYPE=C

# read random bytes and keep only alphanumerics
< /dev/urandom tr -dc A-Za-z0-9 | head -c32
```

Open the `tutorial.conf` (created in the previous tutorial) and add a line with the password:

```
# PASSWORD MUST BE AT LEAST 32 CHARS LONG
# add this line to tutorial.conf:
jwt-secret = "<the password you made>"
```

If the PostgREST server is still running from the previous tutorial, restart it to load the updated configuration file.

7.2.3 Step 3. Sign a Token

Ordinarily your own code in the database or in another server will create and sign authentication tokens, but for this tutorial we will make one “by hand.” Go to jwt.io and fill in the fields like this:

**Remember to fill in the password you generated rather than the word “secret”**. After you have filled in the password and payload, the encoded data on the left will update. Copy the encoded token.

**Note:** While the token may look well obscured, it’s easy to reverse engineer the payload. The token is merely signed, not encrypted, so don’t put things inside that you don’t want a determined client to see.
7.2.4 Step 4. Make a Request

Back in the terminal, let’s use `curl` to add a todo. The request will include an HTTP header containing the authentication token.

```
export TOKEN="<paste token here>"

curl http://localhost:3000/todos -X POST \  
-H "Authorization: Bearer $TOKEN" \  
-H "Content-Type: application/json" \  
-d '{"task": "learn how to auth"}'
```

And now we have completed all three items in our todo list, so let’s set `done` to true for them all with a `PATCH` request.

```
curl http://localhost:3000/todos -X PATCH \  
-H "Authorization: Bearer $TOKEN" \  
-H "Content-Type: application/json" \  
-d '{"done": true}'
```

A request for the todos shows three of them, and all completed.

```
curl http://localhost:3000/todos
```

```json
[
  {
    "id": 1,
    "done": true,
    "task": "finish tutorial 0",
    "due": null
  }
]  
```
7.2.5 Step 5. Add Expiration

Currently our authentication token is valid for all eternity. The server, as long as it continues using the same JWT password, will honor the token.

It’s better policy to include an expiration timestamp for tokens using the exp claim. This is one of two JWT claims that PostgREST treats specially.

<table>
<thead>
<tr>
<th>Claim</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>role</td>
<td>The database role under which to execute SQL for API request</td>
</tr>
<tr>
<td>exp</td>
<td>Expiration timestamp for token, expressed in “Unix epoch time”</td>
</tr>
</tbody>
</table>

**Note:** Epoch time is defined as the number of seconds that have elapsed since 00:00:00 Coordinated Universal Time (UTC), January 1st 1970, minus the number of leap seconds that have taken place since then.

To observe expiration in action, we’ll add an exp claim of five minutes in the future to our previous token. First find the epoch value of five minutes from now. In psql run this:

```
select extract(epoch from now() + '5 minutes'::interval) :: integer;
```

Go back to jwt.io and change the payload to

```
{
  "role": "todo_user",
  "exp": 123456789
}
```

**NOTE:** Don’t forget to change the dummy epoch value 123456789 in the snippet above to the epoch value returned by the psql command.

Copy the updated token as before, and save it as a new environment variable.

```
export NEW_TOKEN="<paste new token>"
```

Try issuing this request in curl before and after the expiration time:

```
curl http://localhost:3000/todos
  -H "Authorization: Bearer $NEW_TOKEN"
```
After expiration, the API returns HTTP 401 Unauthorized:

```json
{
  "message": "JWT expired"
}
```

### 7.2.6 Bonus Topic: Immediate Revocation

Even with token expiration there are times when you may want to immediately revoke access for a specific token. For instance, suppose you learn that a disgruntled employee is up to no good and his token is still valid.

To revoke a specific token we need a way to tell it apart from others. Let’s add a custom `email` claim that matches the email of the client issued the token.

Go ahead and make a new token with the payload

```json
{
  "role": "todo_user",
  "email": "disgruntled@mycompany.com"
}
```

Save it to an environment variable:

```bash
export WAYWARD_TOKEN="<paste new token>"
```

PostgREST allows us to specify a stored procedure to run during attempted authentication. The function can do whatever it likes, including raising an exception to terminate the request.

First make a new schema and add the function:

```sql
create schema auth;
grant usage on schema auth to web_anon, todo_user;
create or replace function auth.check_token() returns void language plpgsql
as $$
begin
  if current_setting('request.jwt.claim.email', true) = 'disgruntled@mycompany.com' then
    raise insufficient_privilege using hint = 'Nope, we are on to you';
  end if;
end $$;
```

Next update `tutorial.conf` and specify the new function:

```bash
# add this line to tutorial.conf
pre-request = "auth.check_token"
```

Restart PostgREST for the change to take effect. Next try making a request with our original token and then with the revoked one.

```bash
# this request still works

```
curl http://localhost:3000/todos -X PATCH \
-H "Authorization: Bearer STOKEN" \ 
-H "Content-Type: application/json" \
```

(continues on next page)
# this one is rejected


The server responds with 403 Forbidden:

```json
{
  "hint": "Nope, we are on to you",
  "details": null,
  "code": "42501",
  "message": "insufficient_privilege"
}
```

- Tutorial 0 - Get it Running
- Tutorial 1 - The Golden Key

Also have a look at Installation and Community Tutorials.
CHAPTER 8

Reference guides

Technical references for PostgREST’s functionality.

8.1 Tables and Views

All views and tables in the exposed schema and accessible by the active database role for a request are available for querying. They are exposed in one-level deep routes. For instance the full contents of a table `people` is returned at

```
GET /people HTTP/1.1
```

There are no deeply/nested/routes. Each route provides OPTIONS, GET, HEAD, POST, PATCH, and DELETE verbs depending entirely on database permissions.

**Note:** Why not provide nested routes? Many APIs allow nesting to retrieve related information, such as `/films/1/director`. We offer a more flexible mechanism (inspired by GraphQL) to embed related information. It can handle one-to-many and many-to-many relationships. This is covered in the section about Resource Embedding.

8.1.1 Horizontal Filtering (Rows)

You can filter result rows by adding conditions on columns, each condition a query string parameter. For instance, to return people aged under 13 years old:

```
GET /people?age=lt.13 HTTP/1.1
```

Multiple parameters can be logically conjoined by:

```
GET /people?age=gte.18&student=is.true HTTP/1.1
```

Multiple parameters can be logically disjoined by:
GET /people?or=(age.gte.14,age.lte.18) HTTP/1.1

Complex logic can also be applied:

GET /people?and=(grade.gte.90,student.is.true,or(age.gte.14,age.is.null)) HTTP/1.1

Operators

These operators are available:

<table>
<thead>
<tr>
<th>Abbrivation</th>
<th>In PostgreSQL</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>eq</td>
<td>=</td>
<td>equals</td>
</tr>
<tr>
<td>gt</td>
<td>&gt;</td>
<td>greater than</td>
</tr>
<tr>
<td>gte</td>
<td>&gt;=</td>
<td>greater than or equal</td>
</tr>
<tr>
<td>lt</td>
<td>&lt;</td>
<td>less than</td>
</tr>
<tr>
<td>lte</td>
<td>&lt;=</td>
<td>less than or equal</td>
</tr>
<tr>
<td>neq</td>
<td>&lt;&gt; or !=</td>
<td>not equal</td>
</tr>
<tr>
<td>like</td>
<td>LIKE</td>
<td>LIKE operator (use * in place of %)</td>
</tr>
<tr>
<td>ilike</td>
<td>ILIKE</td>
<td>ILIKE operator (use * in place of %)</td>
</tr>
<tr>
<td>in</td>
<td>IN</td>
<td>one of a list of values, e.g. ?a=in.(1,2,3) – also supports commas in quoted strings like ?a=in.(&quot;hi,there&quot;,&quot;yes,you&quot;)</td>
</tr>
<tr>
<td>is</td>
<td>IS</td>
<td>checking for exact equality (null,true,false)</td>
</tr>
<tr>
<td>fts</td>
<td>@@</td>
<td>Full-Text Search using to_tsquery</td>
</tr>
<tr>
<td>plfts</td>
<td>@@</td>
<td>Full-Text Search using plainto_tsquery</td>
</tr>
<tr>
<td>phfts</td>
<td>@@</td>
<td>Full-Text Search using phraseto_tsquery</td>
</tr>
<tr>
<td>wfts</td>
<td>@@</td>
<td>Full-Text Search using websearch_to_tsquery</td>
</tr>
<tr>
<td>cs</td>
<td>@&gt;</td>
<td>contains e.g. ?tags=cs.(example, new)</td>
</tr>
<tr>
<td>cd</td>
<td>@&lt;</td>
<td>contained in e.g. ?values=cd.(1,2,3)</td>
</tr>
<tr>
<td>ov</td>
<td>&amp;&amp;</td>
<td>overlap (have points in common), e.g. ?period=ov.[2017-01-01,2017-06-30] – also supports array types, use curly braces instead of square brackets e.g. :code: ?arr=ov.{1,3}</td>
</tr>
<tr>
<td>sl</td>
<td>&lt;&lt;</td>
<td>strictly left of, e.g. ?range=sl.(1,10)</td>
</tr>
<tr>
<td>sr</td>
<td>&gt;&gt;</td>
<td>strictly right of</td>
</tr>
<tr>
<td>nxr</td>
<td>&amp;&lt;</td>
<td>does not extend to the right of, e.g. ?range=nxr.(1,10)</td>
</tr>
<tr>
<td>nxl</td>
<td>&gt;&amp;</td>
<td>does not extend to the left of</td>
</tr>
<tr>
<td>adj</td>
<td>-=</td>
<td>is adjacent to, e.g. ?range=adj.(1,10)</td>
</tr>
<tr>
<td>not</td>
<td>NOT</td>
<td>negates another operator, see below</td>
</tr>
</tbody>
</table>

To negate any operator, prefix it with not like ?a=not.eq.2 or ?not.and=(a.gte.0,a.lte.100).

For more complicated filters you will have to create a new view in the database, or use a stored procedure. For instance, here’s a view to show “today’s stories” including possibly older pinned stories:

```sql
CREATE VIEW fresh_stories AS
  SELECT *
  FROM stories
  WHERE pinned = true
    OR published > now() - interval '1 day'
  ORDER BY pinned DESC, published DESC;
```

The view will provide a new endpoint:
GET /fresh_stories HTTP/1.1

Full-Text Search

The fts filter mentioned above has a number of options to support flexible textual queries, namely the choice of plain vs phrase search and the language used for stemming. Suppose that tsearch is a table with column my_tsv, of type tsvector. The following examples illustrate the possibilities.

GET /tsearch?my_tsv=fts(french).amusant HTTP/1.1

GET /tsearch?my_tsv=plfts.The%20Fat%20Cats HTTP/1.1

GET /tsearch?my_tsv=not.phfts(english).The%20Fat%20Cats HTTP/1.1

GET /tsearch?my_tsv=not.wfts(french).amusant HTTP/1.1

Using phrase search mode requires PostgreSQL of version at least 9.6 and will raise an error in earlier versions of the database.

Using websearch_to_tsquery requires PostgreSQL of version at least 11.0 and will raise an error in earlier versions of the database.

8.1.2 Vertical Filtering (Columns)

When certain columns are wide (such as those holding binary data), it is more efficient for the server to withhold them in a response. The client can specify which columns are required using the select parameter.

GET /people?select=first_name,age HTTP/1.1

[  
  {"first_name": "John", "age": 30},  
  {"first_name": "Jane", "age": 20}  
]

The default is *, meaning all columns. This value will become more important below in Resource Embedding.

Renaming Columns

You can rename the columns by prefixing them with an alias followed by the colon : operator.

GET /people?select=fullName:full_name,birthDate:birth_date HTTP/1.1

[  
  {"fullName": "John Doe", "birthDate": "04/25/1988"},  
  {"fullName": "Jane Doe", "birthDate": "01/12/1998"}  
]

Casting Columns

Casting the columns is possible by suffixing them with the double colon :: plus the desired type.
### JSON Columns

You can specify a path for a `json` or `jsonb` column using the arrow operators (-> or ->>) as per the PostgreSQL docs.

```plaintext
GET /people?select=id, json_data->blood_type, json_data->phones HTTP/1.1

[ 
  { "id": 1, "blood_type": "A-", "phones": ["country_code": "61", "number": "917-929-5745" ] },
  { "id": 2, "blood_type": "O+", "phones": ["country_code": "43", "number": "512-446-4988" ] },
] 
```

```plaintext
GET /people?select=id, json_data->phones->0->number HTTP/1.1

[ 
  { "id": 1, "number": "917-929-5745" },
  { "id": 2, "number": "512-446-4988" }
] 
```

This also works with filters:

```plaintext
GET /people?select=id, json_data->blood_type&json_data->blood_type=eq.A- HTTP/1.1

[ 
  { "id": 1, "blood_type": "A-" },
  { "id": 3, "blood_type": "A-" },
  { "id": 7, "blood_type": "A-" }
] 
```

Note that ->> is used to compare `blood_type` as text. To compare with an integer value use ->:

```plaintext
GET /people?select=id, json_data->age&json_data->age=gt.20 HTTP/1.1

[ 
  { "id": 11, "age": 25 },
  { "id": 12, "age": 30 },
  { "id": 15, "age": 35 }
] 
```

### Computed Columns

Filters may be applied to computed columns (a.k.a. virtual columns) as well as actual table/view columns, even though the computed columns will not appear in the output. For example, to search first and last names at once we can create a computed column that will not appear in the output but can be used in a filter:
CREATE TABLE people {
  fname text,
  lname text
};

CREATE FUNCTION full_name(people) RETURNS text AS $$
  SELECT $1.fname || ' ' || $1.lname;
$$ LANGUAGE SQL;

-- (optional) add an index to speed up anticipated query
CREATE INDEX people_full_name_idx ON people
  USING GIN (to_tsvector('english', full_name(people)));

A full-text search on the computed column:

GET /people?full_name=fts.Beckett HTTP/1.1

As mentioned, computed columns do not appear in the output by default. However you can include them by listing them in the vertical filtering select parameter:

GET /people?select=*,full_name HTTP/1.1

Important: Computed columns must be created under the exposed schema to be used in this way.

8.1.3 Unicode support

PostgREST supports unicode in schemas, tables, columns and values. To access a table with unicode name, use percent encoding.

To request this:

GET / HTTP/1.1

Do this:

GET /%D9%85%D9%88%D8%A7%D8%B1%D8%AF HTTP/1.1

Table / Columns with spaces

You can request table/columns with spaces in them by percent encoding the spaces with %20:

GET /Order%20Items?Unit%20Price=lt.200 HTTP/1.1

Reserved characters

If filters include PostgREST reserved characters(,,:,) you’ll have to surround them in percent encoded double quotes %22 for correct processing.

Here Hebdon, John and Williams, Mary are values.

GET /employees?name=\%22Hebdon, John\%22, \%22Williams, Mary\%22) HTTP/1.1
Here information.cpe is a column name.

```
GET /vulnerabilities?%22information.cpe%22=like.%5CMS%5E HTTP/1.1
```

**Note:** Some HTTP libraries might encode URLs automatically (e.g., axios). In these cases you should use double quotes "" directly instead of %22.

### 8.1.4 Ordering

The reserved word `order` reorders the response rows. It uses a comma-separated list of columns and directions:

```
GET /people?order=age.desc,height.asc HTTP/1.1
```

If no direction is specified it defaults to ascending order:

```
GET /people?order=age HTTP/1.1
```

If you care where nulls are sorted, add `nullsfirst` or `nullslast`:

```
GET /people?order=age.nullsfirst HTTP/1.1
```

```
GET /people?order=age.desc.nullslast HTTP/1.1
```

You can also use *Computed Columns* to order the results, even though the computed columns will not appear in the output.

### 8.1.5 Limits and Pagination

PostgREST uses HTTP range headers to describe the size of results. Every response contains the current range and, if requested, the total number of results:

```
HTTP/1.1 200 OK
Range-Unit: items
Content-Range: 0-14/*
```

Here items zero through fourteen are returned. This information is available in every response and can help you render pagination controls on the client. This is an RFC7233-compliant solution that keeps the response JSON cleaner.

There are two ways to apply a limit and offset rows: through request headers or query parameters. When using headers you specify the range of rows desired. This request gets the first twenty people.

```
GET /people HTTP/1.1
Range-Unit: items
Range: 0-19
```

Note that the server may respond with fewer if unable to meet your request:

```
HTTP/1.1 200 OK
Range-Unit: items
Content-Range: 0-17/*
```

You may also request open-ended ranges for an offset with no limit, e.g. `Range: 10-`. The other way to request a limit or offset is with query parameters. For example
GET /people?limit=15&offset=30 HTTP/1.1

This method is also useful for embedded resources, which we will cover in another section. The server always responds with range headers even if you use query parameters to limit the query.

### 8.1.6 Exact Count

In order to obtain the total size of the table or view (such as when rendering the last page link in a pagination control), specify `Prefer: count=exact` as a request header:

HEAD /bigtable HTTP/1.1
Range-Unit: items
Range: 0-24
Prefer: count=exact

Note that the larger the table the slower this query runs in the database. The server will respond with the selected range and total

HTTP/1.1 206 Partial Content
Range-Unit: items
Content-Range: 0-24/3573458

### 8.1.7 Planned Count

To avoid the shortcomings of exact count, PostgREST can leverage PostgreSQL statistics and get a fairly accurate and fast count. To do this, specify the `Prefer: count=planned` header.

HEAD /bigtable?limit=25 HTTP/1.1
Prefer: count=planned

HTTP/1.1 206 Partial Content
Content-Range: 0-24/3572000

Note that the accuracy of this count depends on how up-to-date are the PostgreSQL statistics tables. For example in this case, to increase the accuracy of the count you can do `ANALYZE bigtable`. See `ANALYZE` for more details.

### 8.1.8 Estimated Count

When you are interested in the count, the relative error is important. If you have a planned count of 1000000 and the exact count is 1001000, the error is small enough to be ignored. But with a planned count of 7, an exact count of 28 would be a huge misprediction.

In general, when having smaller row-counts, the estimated count should be as close to the exact count as possible.

To help with these cases, PostgREST can get the exact count up until a threshold and get the planned count when that threshold is surpassed. To use this behavior, you can specify the `Prefer: count=estimated` header. The threshold is defined by `max-rows`.

Here’s an example. Suppose we set `max-rows=1000` and `smalltable` has 321 rows, then we’ll get the exact count:

HEAD /smalltable?limit=25 HTTP/1.1
Prefer: count=estimated
If we make a similar request on bigtable, which has 3573458 rows, we would get the planned count:

```
HEAD /bigtable?limit=25 HTTP/1.1
Prefer: count=estimated
```

```
HTTP/1.1 206 Partial Content
Content-Range: 0-24/3572000
```

### 8.1.9 Response Format

PostgREST uses proper HTTP content negotiation (RFC7231) to deliver the desired representation of a resource. That is to say the same API endpoint can respond in different formats like JSON or CSV depending on the client request.

Use the Accept request header to specify the acceptable format (or formats) for the response:

```
GET /people HTTP/1.1
Accept: application/json
```

The current possibilities are:

- */*
- text/csv
- application/json
- application/openapi+json
- application/octet-stream

The server will default to JSON for API endpoints and OpenAPI on the root.

### 8.1.10 Singular or Plural

By default PostgREST returns all JSON results in an array, even when there is only one item. For example, requesting `/items?id=eq.1` returns

```
[
  { "id": 1 }
]
```

This can be inconvenient for client code. To return the first result as an object unenclosed by an array, specify `vnd.pgrst.object` as part of the Accept header

```
GET /items?id=eq.1 HTTP/1.1
Accept: application/vnd.pgrst.object+json
```

This returns

```
{ "id": 1 }
```

When a singular response is requested but no entries are found, the server responds with an error message and 406 Not Acceptable status code rather than the usual empty array and 200 status:
Note: Many APIs distinguish plural and singular resources using a special nested URL convention e.g. /stories vs /stories/1. Why do we use /stories?id=eq.1? The answer is because a singular resource is (for us) a row determined by a primary key, and primary keys can be compound (meaning defined across more than one column). The more familiar nested urls consider only a degenerate case of simple and overwhelmingly numeric primary keys. These so-called artificial keys are often introduced automatically by Object Relational Mapping libraries.

Admittedly PostgREST could detect when there is an equality condition holding on all columns constituting the primary key and automatically convert to singular. However this could lead to a surprising change of format that breaks unwary client code just by filtering on an extra column. Instead we allow manually specifying singular vs plural to decouple that choice from the URL format.

8.2 Resource Embedding

In addition to providing RESTful routes for each table and view, PostgREST allows related resources to be included together in a single API call. This reduces the need for multiple API requests. The server uses foreign keys to determine which tables and views can be returned together. For example, consider a database of films and their awards:

Important: PostgREST needs FOREIGN KEY constraints to be able to do Resource Embedding.
As seen above in *Vertical Filtering (Columns)* we can request the titles of all films like this:

```
GET /films?select=title HTTP/1.1
```

This might return something like

```
{
  "title": "Workers Leaving The Lumière Factory In Lyon",
  "title": "The Dickson Experimental Sound Film",
  "title": "The Haunted Castle"
}
```

However because a foreign key constraint exists between Films and Directors, we can request this information be included:

```
GET /films?select=title,directors(id,last_name) HTTP/1.1
```

Which would return
In this example, since the relationship is a forward relationship, there is only one director associated with a film. As the table name is plural it might be preferable for it to be singular instead. An table name alias can accomplish this:

```
GET /films?select=title,director:directors(id,last_name) HTTP/1.1
```

**Important:** Whenever FOREIGN KEY constraints change in the database schema you must refresh PostgREST’s schema cache for Resource Embedding to work properly. See the section *Schema Cache Reloading.*

### 8.2.1 Embedding through join tables

PostgREST can also detect relationships going through join tables. Thus you can request the Actors for Films (which in this case finds the information through Roles).

```
GET /actors?select=films(title,year) HTTP/1.1
```

### 8.2.2 Embedded Filters

Embedded resources can be shaped similarly to their top-level counterparts. To do so, prefix the query parameters with the name of the embedded resource. For instance, to order the actors in each film:

```
GET /films?select=*,actors(*)&actors.order=last_name,first_name HTTP/1.1
```

This sorts the list of actors in each film but does *not* change the order of the films themselves. To filter the roles returned with each film:

```
GET /films?select=*,roles(*)&roles.character=IN.(Chico,Harpo,Groucho) HTTP/1.1
```

Once again, this restricts the roles included to certain characters but does not filter the films in any way. Films without any of those characters would be included along with empty character lists.

An *or* filter can be used for a similar operation:
Limit and offset operations are possible:

```
GET /films?select=* & actors.limit=10 & actors.offset=2 HTTP/1.1
```

Embedded resources can be aliased and filters can be applied on these aliases:

```
GET /films?select=*,actors(*) & actors.limit=10 & actors.offset=2 HTTP/1.1
```

8.2.3 Embedding Views

Embedding a view is possible if the view contains columns that have foreign keys defined in their source tables.

As an example, let’s create a view called nominations_view based on the nominations table.

```sql
CREATE VIEW nominations_view AS
SELECT rank, competition_id, film_id
FROM nominations;
```

Since it contains competition_id and film_id — and each one has a foreign key defined in its source table — we can embed competitions and films:

```
GET /nominations_view?select=rank,competitions(name,year),films(title) & rank=eq.5 HTTP/1.1
```

It’s also possible to embed Materialized Views.

**Warning:** It’s not guaranteed that all kinds of views will be embeddable. In particular, views that contain UNIONS will not be made embeddable.

Why? PostgREST detects source table foreign keys in the view by querying and parsing pg_rewrite. This may fail depending on the complexity of the view.

Report an issue if your view is not made embeddable so we can keep continue improving foreign key detection.

In the future we’ll include a way to manually specify views source foreign keys to address this limitation.

**Important:** If view definitions change you must refresh PostgREST’s schema cache for this to work properly. See the section Schema Cache Reloading.

8.2.4 Embedding Chains of Views

Views can also depend on other views, which in turn depend on the actual source table. For PostgREST to pick up those chains recursively to any depth, all the views must be in the search path, so either in the exposed schema (db-schema) or in one of the schemas set in db-extra-search-path. This does not apply to the source table, which could be in a private schema as well. See Schema Isolation for more details.
8.2.5 Embedding on Stored Procedures

If you have a *Stored Procedure* that returns a table type, you can embed its related resources.

Here’s a sample function (notice the `RETURNS SETOF films`).

```sql
CREATE FUNCTION getallfilms()
RETURNS SETOF films AS $$
SELECT * FROM films;
$$
LANGUAGE SQL IMMUTABLE;
```

A request with directors embedded:

```
GET /rpc/getallfilms?select=title,directors(id,last_name)&title=like.*Workers* HTTP/1.1

[{
   "title": "Workers Leaving The Lumière Factory In Lyon",
   "directors": {
      "id": 2,
      "last_name": "Lumière"
   }
}]
```

8.2.6 Embedding after Insertions/Updates/Deletions

You can embed related resources after doing *Insertions / Updates or Deletions*.

Say you want to insert a film and then get some of its attributes plus embed its director.

```
POST /films?select=title,year,director:directors(first_name,last_name) HTTP/1.1
Prefer: return=representation

{
   "id": 100,
   "director_id": 40,
   "title": "127 hours",
   "year": 2010,
   "rating": 7.6,
   "language": "english"
}
```

Response:

```
{
   "title": "127 hours",
   "year": 2010,
   "director": {
      "first_name": "Danny",
      "last_name": "Boyle"
   }
}
```
8.2.7 Embedding Disambiguation

For doing resource embedding, PostgREST infers the relationship between two tables based on a foreign key between them. However, in cases where there’s more than one foreign key between two tables, it’s not possible to infer the relationship unambiguously by just specifying the tables names.

Target Disambiguation

For example, suppose you have the following `orders` and `addresses` tables:

And you try to embed `orders` with `addresses` (this is the target):

```
GET /orders?select=*,addresses(*) HTTP/1.1
```

Since the `orders` table has two foreign keys to the `addresses` table — an order has a billing address and a shipping address — the request is ambiguous and PostgREST will respond with an error:

```
HTTP/1.1 300 Multiple Choices
```

If this happens, you need to disambiguate the request by adding precision to the target. Instead of the table name, you can specify the foreign key constraint name or the column name that is part of the foreign key.

Let’s try first with the foreign key constraint name. To make it clearer we can name it:

```
ALTER TABLE orders
  ADD CONSTRAINT billing_address foreign key (billing_address_id) references addresses(id),
  ADD CONSTRAINT shipping_address foreign key (shipping_address_id) references addresses(id);
```

-- Or if the constraints names were already generated by PostgreSQL we can rename them
-- ALTER TABLE orders
--   RENAME CONSTRAINT orders_billing_address_id_fkey TO billing_address,
--   RENAME CONSTRAINT orders_shipping_address_id_fkey TO shipping_address;

```
GET /orders?select=*,addresses(billing_address) HTTP/1.1
```

```
GET /orders?select=*,addresses(shipping_address) HTTP/1.1
```
Now we can unambiguously embed the billing address by specifying the `billing_address` foreign key constraint as the `target`.

```
GET /orders?select=name,billing_address(name) HTTP/1.1
[
  {
    "name": "Personal Water Filter",
    "billing_address": {
      "name": "32 Glenlake Dr.Dearborn, MI 48124"
    }
  }
]
```

Alternatively, you can specify the column name of the foreign key constraint as the `target`. This can be aliased to make the result more clear.

```
GET /orders?select=name,billing_address:billing_address_id(name) HTTP/1.1
[
  {
    "name": "Personal Water Filter",
    "billing_address": {
      "name": "32 Glenlake Dr.Dearborn, MI 48124"
    }
  }
]
```

**Hint Disambiguation**

If specifying the `target` is not enough for unambiguous embedding, you can add a `hint`. For example, let’s assume we create two views of `addresses`: `central_addresses` and `eastern_addresses`.

Since PostgREST supports `Embedding Views` by detecting source foreign keys in the views, embedding with the foreign key as the `target` will not be enough for an unambiguous embed:

```
GET /orders?select=*,billing_address(*) HTTP/1.1
HTTP/1.1 300 Multiple Choices
```

For solving this case, in addition to the `target`, we can add a `hint`. Here we specify `central_addresses` as the `target` and the `billing_address` foreign key as the `hint`:

```
GET /orders?select=*,central_addresses!billing_address(*) HTTP/1.1
HTTP/1.1 200 OK
[ ... ]
```

Similarly to the `target`, the `hint` can be a `table name`, `foreign key constraint name` or `column name`.

### 8.3 Insertions / Updates

All tables and auto-updatable views can be modified through the API, subject to permissions of the requester’s database role.
To create a row in a database table post a JSON object whose keys are the names of the columns you would like to create. Missing properties will be set to default values when applicable.

```plaintext
POST /table_name HTTP/1.1
{ "col1": "value1", "col2": "value2" }
```

If the table has a primary key, the response can contain a Location header describing where to find the new object by including the header Prefer: return=headers-only in the request. Make sure that the table is not write-only, otherwise constructing the Location header will cause a permissions error.

On the other end of the spectrum you can get the full created object back in the response to your request by including the header Prefer: return=representation. That way you won’t have to make another HTTP call to discover properties that may have been filled in on the server side. You can also apply the standard Vertical Filtering (Columns) to these results.

URL encoded payloads can be posted with Content-Type: application/x-www-form-urlencoded.

```plaintext
POST /people HTTP/1.1
Content-Type: application/x-www-form-urlencoded
name=John+Doe&age=50&weight=80
```

**Note:** When inserting a row you must post a JSON object, not quoted JSON.

```plaintext
Yes
{ "a": 1, "b": 2 }

No
"{"a": 1, "b": 2 }"
```

Some JavaScript libraries will post the data incorrectly if you’re not careful. For best results try one of the Client-Side Libraries built for PostgREST.

To update a row or rows in a table, use the PATCH verb. Use Horizontal Filtering (Rows) to specify which record(s) to update. Here is an example query setting the category column to child for all people below a certain age.

```plaintext
PATCH /people?age=lt.13 HTTP/1.1
{ "category": "child" }
```

Updates also support Prefer: return=representation plus Vertical Filtering (Columns).

**Warning:** Beware of accidentally updating every row in a table. To learn to prevent that see Block Full-Table Operations.

### 8.3.1 Bulk Insert

Bulk insert works exactly like single row insert except that you provide either a JSON array of objects having uniform keys, or lines in CSV format. This not only minimizes the HTTP requests required but uses a single INSERT statement on the back-end for efficiency. Note that using CSV requires less parsing on the server and is much faster.

To bulk insert CSV simply post to a table route with Content-Type: text/csv and include the names of the columns as the first row. For instance
An empty field (__,,) is coerced to an empty string and the reserved word NULL is mapped to the SQL null value. Note that there should be no spaces between the column names and commas.

To bulk insert JSON post an array of objects having all-matching keys

<table>
<thead>
<tr>
<th>POST /people HTTP/1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type: application/json</td>
</tr>
<tr>
<td>{</td>
</tr>
<tr>
<td>&quot;name&quot;: &quot;J Doe&quot;, &quot;age&quot;: 62, &quot;height&quot;: 70 },</td>
</tr>
<tr>
<td>&quot;name&quot;: &quot;Janus&quot;, &quot;age&quot;: 10, &quot;height&quot;: 55 }</td>
</tr>
</tbody>
</table>

8.3.2 Specifying Columns

By using the columns query parameter it’s possible to specify the payload keys that will be inserted/updated and ignore the rest of the payload.

<table>
<thead>
<tr>
<th>POST /datasets?columns=source,publication_date,figure HTTP/1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type: application/json</td>
</tr>
<tr>
<td>{</td>
</tr>
<tr>
<td>&quot;source&quot;: &quot;Natural Disaster Prevention and Control&quot;,</td>
</tr>
<tr>
<td>&quot;publication_date&quot;: &quot;2015-09-11&quot;,</td>
</tr>
<tr>
<td>&quot;figure&quot;: 1100,</td>
</tr>
<tr>
<td>&quot;location&quot;: &quot;...&quot;,</td>
</tr>
<tr>
<td>&quot;comment&quot;: &quot;...&quot;,</td>
</tr>
<tr>
<td>&quot;extra&quot;: &quot;...&quot;,</td>
</tr>
<tr>
<td>&quot;stuff&quot;: &quot;...&quot;</td>
</tr>
<tr>
<td>}</td>
</tr>
</tbody>
</table>

In this case, only source, publication_date and figure will be inserted. The rest of the JSON keys will be ignored.

Using this also has the side-effect of being more efficient for Bulk Insert since PostgREST will not process the JSON and it’ll send it directly to PostgreSQL.

8.3.3 UPSERT

You can make an UPSERT with POST and the Prefer: resolution=merge-duplicates header:

<table>
<thead>
<tr>
<th>POST /employees HTTP/1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefer: resolution=merge-duplicates</td>
</tr>
<tr>
<td>[</td>
</tr>
<tr>
<td>{ &quot;id&quot;: 1, &quot;name&quot;: &quot;Old employee 1&quot;, &quot;salary&quot;: 30000 },</td>
</tr>
<tr>
<td>{ &quot;id&quot;: 2, &quot;name&quot;: &quot;Old employee 2&quot;, &quot;salary&quot;: 42000 },</td>
</tr>
<tr>
<td>{ &quot;id&quot;: 3, &quot;name&quot;: &quot;New employee 3&quot;, &quot;salary&quot;: 50000 }</td>
</tr>
<tr>
<td>]</td>
</tr>
</tbody>
</table>
By default, UPSERT operates based on the primary key columns, you must specify all of them. You can also choose to ignore the duplicates with *Prefer: resolution=ignore-duplicates*. This works best when the primary key is natural, but it’s also possible to use it if the primary key is surrogate (example: “id serial primary key”). For more details read this issue.

**Important:** After creating a table or changing its primary key, you must refresh PostgREST schema cache for UPSERT to work properly. To learn how to refresh the cache see *Schema Cache Reloading*.

### On Conflict

By specifying the `on_conflict` query parameter, you can make UPSERT work on a column(s) that has a UNIQUE constraint.

```plaintext
POST /employees?on_conflict=name HTTP/1.1
Prefer: resolution=merge-duplicates

[
  { "name": "Old employee 1", "salary": 40000 },
  { "name": "Old employee 2", "salary": 52000 },
  { "name": "New employee 3", "salary": 60000 }]
```

### PUT

A single row UPSERT can be done by using **PUT** and filtering the primary key columns with *eq*:

```plaintext
PUT /employees?id=eq.4 HTTP/1.1

{ "id": 4, "name": "Sara B.", "salary": 60000 }
```

All the columns must be specified in the request body, including the primary key columns.

**Note:** Upsert features are only available starting from PostgreSQL 9.5 since it uses the ON CONFLICT clause.

### 8.4 Deletions

To delete rows in a table, use the DELETE verb plus Horizontal Filtering (Rows). For instance deleting inactive users:

```plaintext
DELETE /user?active=is.false HTTP/1.1
```

Deletions also support *Prefer: return=representation* plus Vertical Filtering (Columns).

```plaintext
DELETE /user?id=eq.1 HTTP/1.1
Prefer: return=representation

{"id": 1, "email": "johndoe@email.com"}
```
Warning: Beware of accidentally deleting all rows in a table. To learn to prevent that see Block Full-Table Operations.

8.5 Custom Queries

The PostgREST URL grammar limits the kinds of queries clients can perform. It prevents arbitrary, potentially poorly constructed and slow client queries. It’s good for quality of service, but means database administrators must create custom views and stored procedures to provide richer endpoints. The most common causes for custom endpoints are

- Table unions
- More complicated joins than those provided by Resource Embedding
- Geo-spatial queries that require an argument, like “points near (lat,lon)”

8.6 Stored Procedures

Every stored procedure in the API-exposed database schema is accessible under the /rpc prefix. The API endpoint supports POST (and in some cases GET) to execute the function.

```
POST /rpc/function_name HTTP/1.1
```

Such functions can perform any operations allowed by PostgreSQL (read data, modify data, and even DDL operations). To supply arguments in an API call, include a JSON object in the request payload and each key/value of the object will become an argument.

For instance, assume we have created this function in the database.

```
CREATE FUNCTION add_them(a integer, b integer)
RETURNS integer AS $$
SELECT a + b;
$$
LANGUAGE SQL IMMUTABLE;
```

Important: Whenever you create or change a function you must refresh PostgREST’s schema cache. See the section Schema Cache Reloading.

The client can call it by posting an object like

```
POST /rpc/add_them HTTP/1.1
{
  "a": 1,
  "b": 2
}
```

```
3
```

Procedures must be declared with named parameters. Procedures declared like

```
CREATE FUNCTION non_named_args(integer, text, integer) ...
```

cannot be called with PostgREST, since we use named notation internally.

Note that PostgreSQL converts identifier names to lowercase unless you quote them like:
CREATE FUNCTION "someFunc"("someParam" text) ...

PostgreSQL has four procedural languages that are part of the core distribution: PL/pgSQL, PL/Tcl, PL/Perl, and PL/Python. There are many other procedural languages distributed as additional extensions. Also, plain SQL can be used to write functions (as shown in the example above).

**Note:** Why the /rpc prefix? One reason is to avoid name collisions between views and procedures. It also helps emphasize to API consumers that these functions are not normal restful things. The functions can have arbitrary and surprising behavior, not the standard “post creates a resource” thing that users expect from the other routes.

### 8.6.1 Immutable and stable functions

PostgREST executes POST requests in a read/write transaction except for functions marked as `IMMUTABLE` or `STABLE`. Those must not modify the database and are executed in a read-only transaction compatible for read-replicas.

Procedures that do not modify the database can be called with the HTTP GET verb as well, if desired. PostgREST executes all GET requests in a read-only transaction. Modifying the database inside read-only transactions is not possible and calling volatile functions with GET will fail.

**Note:** The volatility marker is a promise about the behavior of the function. PostgreSQL will let you mark a function that modifies the database as `IMMUTABLE` or `STABLE` without failure. However, because of the read-only transaction this would still fail with PostgREST.

Because `add_them` is `IMMUTABLE`, we can alternately call the function with a GET request:

```
GET /rpc/add_them?a=1&b=2 HTTP/1.1
```

The function parameter names match the JSON object keys in the POST case, for the GET case they match the query parameters `?a=1&b=2`.

### 8.6.2 Calling functions with a single JSON parameter

You can also call a function that takes a single parameter of type JSON by sending the header `Prefer: params=single-object` with your request. That way the JSON request body will be used as the single argument.

```
CREATE FUNCTION mult_them(param json) RETURNS int AS $$
    SELECT (param->>'x')::int * (param->>'y')::int
$$ LANGUAGE SQL;
```

```
POST /rpc/mult_them HTTP/1.1
Prefer: params=single-object

{ "x": 4, "y": 2 }
```

### 8.6.3 Calling functions with array parameters

You can call a function that takes an array parameter:
**create function** plus_one(arr int[])  **returns**  int[]  **as**  $$
SELECT array_agg(n + 1) FROM unnest($1) AS n;
$$  **language sql**;

```sql
POST /rpc/plus_one HTTP/1.1
Content-Type: application/json

{"arr": [1,2,3,4]}

[2,3,4,5]
```

For calling the function with GET, you can pass the array as an array literal, as in \{1, 2, 3, 4\}. Note that the curly brackets have to be urlencoded(\{ is %7B and \} is %7D).

```sql
GET /rpc/plus_one?arr=%7B1,2,3,4%7D HTTP/1.1
```

**Note:** For versions prior to PostgreSQL 10, to pass a PostgreSQL native array on a POST payload, you need to quote it and use an array literal:

```sql
POST /rpc/plus_one HTTP/1.1

{"arr": "{1,2,3,4}"}

[2,3,4,5]
```

In these versions we recommend using function parameters of type JSON to accept arrays from the client.

### 8.6.4 Calling variadic functions

You can call a variadic function by passing a JSON array in a POST request:

```sql
create function plus_one(variadic v int[])  **returns**  int[]  **as**  $$
SELECT array_agg(n + 1) FROM unnest($1) AS n;
$$  **language sql**;

POST /rpc/plus_one HTTP/1.1
Content-Type: application/json

{"v": [1,2,3,4]}

[2,3,4,5]
```

In a GET request, you can repeat the same parameter name:

```sql
GET /rpc/plus_one?v=1&v=2&v=3&v=4 HTTP/1.1
```

Repeating also works in POST requests with **Content-Type: application/x-www-form-urlencoded**:

```sql
POST /rpc/plus_one HTTP/1.1
Content-Type: application/x-www-form-urlencoded

v=1&v=2&v=3&v=4
```

### 8.6. Stored Procedures
8.6.5 Scalar functions

PostgREST will detect if the function is scalar or table-valued and will shape the response format accordingly:

```
GET /rpc/add_them?a=1&b=2 HTTP/1.1
3
```

```
GET /rpc/best_films_2017 HTTP/1.1
[
  { "title": "Okja", "rating": 7.4},
  { "title": "Call me by your name", "rating": 8},
  { "title": "Blade Runner 2049", "rating": 8.1}
]
```

8.6.6 Bulk Call

It’s possible to call a function in a bulk way, analogously to Bulk Insert. To do this, you need to add the `Prefer: params=multiple-objects` header to your request.

```
POST /rpc/add_them HTTP/1.1
Content-Type: text/csv
Prefer: params=multiple-objects

a,b
1,2
3,4
```

```
[ 3, 7 ]
```

If you have large payloads to process, it’s preferable you instead use a function with an array parameter or JSON parameter, as this will be more efficient.

It’s also possible to Specify Columns on functions calls.

8.6.7 Function filters

A function that returns a table type response can be shaped using the same filters as the ones used for tables and views:

```
CREATE FUNCTION best_films_2017() RETURNS SETOF films ..
```

```
GET /rpc/best_films_2017?select=title,director:directors(*) HTTP/1.1
```

```
GET /rpc/best_films_2017?rating=gt.8&order=title.desc HTTP/1.1
```

8.6.8 Overloaded functions

You can call overloaded functions with different number of arguments.
Important: Overloaded functions with the same argument names but different types are not supported.

8.7 Binary Output

If you want to return raw binary data from a `bytea` column, you must specify `application/octet-stream` as part of the `Accept` header and select a single column `?select=bin_data`.

GET /items?select=bin_data&id=eq.1 HTTP/1.1
Accept: application/octet-stream

You can also request binary output when calling Stored Procedures and since they can return a scalar value you are not forced to use `select` for this case.

CREATE FUNCTION closest_point(..) RETURNS bytea ..

POST /rpc/closest_point HTTP/1.1
Accept: application/octet-stream

If the stored procedure returns non-scalar values, you need to do a `select` in the same way as for GET binary output.

CREATE FUNCTION overlapping_regions(..) RETURNS SETOF TABLE(geom_twkb bytea, ..) ..

POST /rpc/overlapping_regions?select=geom_twkb HTTP/1.1
Accept: application/octet-stream

Note: If more than one row would be returned the binary results will be concatenated with no delimiter.

8.7.1 Plain Text Output

You can get raw output from a `text` column by using `Accept: text/plain`.

GET /workers?select=custom_psv_format HTTP/1.1
Accept: text/plain

09310817|JOHN|DOE|15/04/88|
42152780|FRED|BLOGGS|20/02/85|
43006541|OTTO|NORMALVERBRAUCHER|01/07/90|
02452492|ERIKA|MUSTERMANN|11/01/80|

This follows the same rules as Binary Output.
8.8 OpenAPI Support

Every API hosted by PostgREST automatically serves a full OpenAPI description on the root path. This provides a list of all endpoints (tables, foreign tables, views, functions), along with supported HTTP verbs and example payloads.

**Note:** By default, this output depends on the permissions of the role that is contained in the JWT role claim (or the `db-anon-role` if no JWT is sent). If you need to show all the endpoints disregarding the role’s permissions, set the `openapi-mode` config to `ignore-privileges`.

For extra customization, the OpenAPI output contains a “description” field for every SQL comment on any database object. For instance,

```sql
COMMENT ON SCHEMA mammals IS
   'A warm-blooded vertebrate animal of a class that is distinguished by the secretion of milk by females for the nourishment of the young';

COMMENT ON TABLE monotremes IS
   'Freakish mammals lay the best eggs for breakfast';

COMMENT ON COLUMN monotremes.has_venomous_claw IS
   'Sometimes breakfast is not worth it';
```

These unsavory comments will appear in the generated JSON as the fields, `info.description`, `definitions.monotremes.description` and `definitions.monotremes.properties.has_venomous_claw.description`.

Also if you wish to generate a `summary` field you can do it by having a multiple line comment, the `summary` will be the first line and the `description` the lines that follow it:

```sql
COMMENT ON TABLE entities IS
$$Entities summary
   Entities description that
      spans
      multiple lines$$;
```

You can use a tool like Swagger UI to create beautiful documentation from the description and to host an interactive web-based dashboard. The dashboard allows developers to make requests against a live PostgREST server, and provides guidance with request headers and example request bodies.

**Important:** The OpenAPI information can go out of date as the schema changes under a running server. To learn how to refresh the cache see `Schema Cache Reloading`.

8.9 OPTIONS

You can verify which HTTP methods are allowed on endpoints for tables and views by using an OPTIONS request. These methods are allowed depending on what operations *can* be done on the table or view, not on the database permissions assigned to them.

For a table named `people`, OPTIONS would show:
OPTIONS /people HTTP/1.1

HTTP/1.1 200 OK
Allow: OPTIONS, GET, HEAD, POST, PUT, PATCH, DELETE

For a view, the methods are determined by the presence of INSTEAD OF TRIGGERS.

<table>
<thead>
<tr>
<th>Method allowed</th>
<th>View’s requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPTIONS, HEAD</td>
<td>None (Always allowed)</td>
</tr>
<tr>
<td>POST</td>
<td>INSTEAD OF INSERT TRIGGER</td>
</tr>
<tr>
<td>PUT</td>
<td>INSTEAD OF INSERT TRIGGER, INSTEAD OF UPDATE TRIGGER, also requires the presence of a primary key</td>
</tr>
<tr>
<td>PATCH</td>
<td>INSTEAD OF UPDATE TRIGGER</td>
</tr>
<tr>
<td>DELETE</td>
<td>INSTEAD OF DELETE TRIGGER</td>
</tr>
</tbody>
</table>

All the above methods are allowed for auto-updatable views.

For functions, OPTIONS requests are not supported.

**Important:** Whenever you add or remove tables or views, or modify a view’s INSTEAD OF TRIGGERS on the database, you must refresh PostgREST’s schema cache for OPTIONS requests to work properly. See the section *Schema Cache Reloading.*

### 8.9.1 CORS

PostgREST sets highly permissive cross origin resource sharing, that is why it accepts Ajax requests from any domain.

### 8.10 Switching Schemas

You can switch schemas at runtime with the Accept-Profile and Content-Profile headers. You can only switch to a schema that is included in `db-schema`.

For GET or HEAD, the schema to be used can be selected through the Accept-Profile header:

**Note:** These headers are based on the nascent “Content Negotiation by Profile” spec: [https://www.w3.org/TR/dx-prof-conneg](https://www.w3.org/TR/dx-prof-conneg)
8.11 HTTP Logic

8.11.1 Accessing Request Headers, Cookies and JWT claims

You can access request headers, cookies and JWT claims by reading GUC variables set by PostgREST per request. They are named `request.header.XYZ`, `request.cookie.XYZ` and `request.jwt.claim.XYZ`.

```sql
-- To read the value of the User-Agent request header:
SELECT current_setting('request.header.user-agent', true);

-- To read the value of sessionId in a cookie:
SELECT current_setting('request.cookie.sessionId', true);

-- To read the value of the email claim in a jwt:
SELECT current_setting('request.jwt.claim.email', true);
```

Note: `request.jwt.claim.role` defaults to the value of `db-anon-role`.

8.11.2 Accessing Request Path and Method

You can also access the request path and method with `request.path` and `request.method`.

```sql
-- You can get the path of the request with
SELECT current_setting('request.path', true);

-- You can get the method of the request with
SELECT current_setting('request.method', true);
```

8.11.3 Setting Response Headers

PostgREST reads the `response.headers` SQL variable to add extra headers to the HTTP response. Stored procedures can modify this variable. For instance, this statement would add caching headers to the response:

```sql
-- tell client to cache response for two days
SELECT set_config('response.headers',
  '[["Cache-Control": "public"],
   ["Cache-Control": "max-age=259200"]]', true);
```

Notice that the variable should be set to an array of single-key objects rather than a single multiple-key object. This is because headers such as `Cache-Control` or `Set-Cookie` need to be repeated when setting multiple values and an object would not allow the repeated key.

Note: PostgREST provided headers such as `Content-Type`, `Location`, etc. can be overridden this way.

Setting headers via pre-request

By using a `pre-request` function, you can add headers to GET/POST/PATCH/PUT/DELETE responses. As an example, let’s add some cache headers for all requests that come from an Internet Explorer(6 or 7) browser.
create or replace function custom_headers() returns void as $$
declare
  user_agent text := current_setting('request.header.user-agent', true);
begin
  if user_agent similar to '%MSIE (6.0|7.0)%' then
    perform set_config('response.headers', '[]', false);
  end if;
end;
$$
language plpgsql;

-- set this function on postgrest.conf
-- pre-request = custom_headers

Now when you make a GET request to a table or view, you’ll get the cache headers.

```
GET /people HTTP/1.1
User-Agent: Mozilla/4.01 (compatible; MSIE 6.0; Windows NT 5.1)

HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Cache-Control: no-cache, no-store, must-revalidate

...```

### 8.11.4 Setting Response Status Code

You can set the `response.status` GUC to override the default status code PostgREST provides. For instance, the following function would replace the default 200 status code.

```
create or replace function teapot() returns json as $$
begin
  perform set_config('response.status', '418', true);
  return json_build_object('message', 'The requested entity body is short and stout.',
    'hint', 'Tip it over and pour it out.');
end;
$$
language plpgsql;

GET /rpc/teapot HTTP/1.1

HTTP/1.1 418 I'm a teapot

{"message" : "The requested entity body is short and stout.",
"hint" : "Tip it over and pour it out."}
```

If the status code is standard, PostgREST will complete the status message (I’m a teapot in this example).

### 8.11.5 Raise errors with HTTP Status Codes

Stored procedures can return non-200 HTTP status codes by raising SQL exceptions. For instance, here’s a saucy function that always responds with an error:

```
CREATE OR REPLACE FUNCTION just_fail() RETURNS void
LANGUAGE plpgsql
```

(continues on next page)
Calling the function returns HTTP 400 with the body

```json
{
  "message": "I refuse!",
  "details": "Pretty simple",
  "hint": "There is nothing you can do.",
  "code": "P0001"
}
```

**Note:** Keep in mind that `RAISE EXCEPTION` will abort the transaction and rollback all changes. If you don’t want this, you can instead use the `response.status GUC`.

One way to customize the HTTP status code is by raising particular exceptions according to the PostgREST error to status code mapping. For example, `RAISE insufficient_privilege` will respond with HTTP 401/403 as appropriate.

For even greater control of the HTTP status code, raise an exception of the `PTxyz` type. For instance to respond with HTTP 402, raise ‘PT402’:

```sql
RAISE sqlstate 'PT402' using
  message = 'Payment Required',
  detail = 'Quota exceeded',
  hint = 'Upgrade your plan';
```

Returns:

```
HTTP/1.1 402 Payment Required
Content-Type: application/json; charset=utf-8

{"hint": "Upgrade your plan", "details": "Quota exceeded"}
```

### 8.11.6 HTTP Status Codes

PostgREST translates PostgreSQL error codes into HTTP status as follows:
<table>
<thead>
<tr>
<th>PostgreSQL error code(s)</th>
<th>HTTP status</th>
<th>Error description</th>
</tr>
</thead>
<tbody>
<tr>
<td>08*</td>
<td>503</td>
<td>pg connection err</td>
</tr>
<tr>
<td>09*</td>
<td>500</td>
<td>triggered action exception</td>
</tr>
<tr>
<td>0L*</td>
<td>403</td>
<td>invalid grantor</td>
</tr>
<tr>
<td>0P*</td>
<td>403</td>
<td>invalid role specification</td>
</tr>
<tr>
<td>23503</td>
<td>409</td>
<td>foreign key violation</td>
</tr>
<tr>
<td>23505</td>
<td>409</td>
<td>uniqueness violation</td>
</tr>
<tr>
<td>25006</td>
<td>405</td>
<td>read only sql transaction</td>
</tr>
<tr>
<td>25*</td>
<td>500</td>
<td>invalid transaction state</td>
</tr>
<tr>
<td>28*</td>
<td>403</td>
<td>invalid auth specification</td>
</tr>
<tr>
<td>2D*</td>
<td>500</td>
<td>invalid transaction termination</td>
</tr>
<tr>
<td>38*</td>
<td>500</td>
<td>external routine exception</td>
</tr>
<tr>
<td>39*</td>
<td>500</td>
<td>external routine invocation</td>
</tr>
<tr>
<td>3B*</td>
<td>500</td>
<td>savepoint exception</td>
</tr>
<tr>
<td>40*</td>
<td>500</td>
<td>transaction rollback</td>
</tr>
<tr>
<td>53*</td>
<td>503</td>
<td>insufficient resources</td>
</tr>
<tr>
<td>54*</td>
<td>413</td>
<td>too complex</td>
</tr>
<tr>
<td>55*</td>
<td>500</td>
<td>obj not in prerequisite state</td>
</tr>
<tr>
<td>57*</td>
<td>500</td>
<td>operator intervention</td>
</tr>
<tr>
<td>58*</td>
<td>500</td>
<td>system error</td>
</tr>
<tr>
<td>F0*</td>
<td>500</td>
<td>config file error</td>
</tr>
<tr>
<td>HV*</td>
<td>500</td>
<td>foreign data wrapper error</td>
</tr>
<tr>
<td>P0001</td>
<td>400</td>
<td>default code for “raise”</td>
</tr>
<tr>
<td>P0*</td>
<td>500</td>
<td>PL/pgSQL error</td>
</tr>
<tr>
<td>XX*</td>
<td>500</td>
<td>internal error</td>
</tr>
<tr>
<td>42883</td>
<td>404</td>
<td>undefined function</td>
</tr>
<tr>
<td>42P01</td>
<td>404</td>
<td>undefined table</td>
</tr>
<tr>
<td>42501</td>
<td></td>
<td>if authenticated 403, else 401</td>
</tr>
<tr>
<td>other</td>
<td>400</td>
<td>insufficient privileges</td>
</tr>
</tbody>
</table>

8.12 Configuration

PostgREST reads a configuration file to determine information about the database and how to serve client requests. There is no predefined location for this file, you must specify the file path as the one and only argument to the server:

`. /postgrest /path/to/postgrest.conf`

Note: Configuration can be reloaded without restarting the server. See Configuration Reloading.

The configuration file must contain a set of key value pairs. At minimum you must include these keys:

```bash
# postgrest.conf
# The standard connection URI format, documented at
# https://www.postgresql.org/docs/current/libpq-connect.html#LIBPQ-CONNSTRING
```

(continues on next page)
The user specified in the db-uri is also known as the authenticator role. For more information about the anonymous vs authenticator roles see the *Overview of Role System*.

Here is the full list of configuration parameters.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>db-uri</td>
<td>String</td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>db-schema</td>
<td>String</td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>db-anon-role</td>
<td>String</td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>db-pool</td>
<td>Int</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>db-pool-timeout</td>
<td>Int</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>db-extra-search-path</td>
<td>String</td>
<td>public</td>
<td></td>
</tr>
<tr>
<td>db-channel</td>
<td>String</td>
<td>pgrst</td>
<td></td>
</tr>
<tr>
<td>db-channel-enabled</td>
<td>Boolean</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td>db-prepared-statements</td>
<td>Boolean</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td>db-tx-end</td>
<td>String</td>
<td>commit</td>
<td></td>
</tr>
<tr>
<td>db-config</td>
<td>Boolean</td>
<td>True</td>
<td></td>
</tr>
<tr>
<td>server-host</td>
<td>String</td>
<td>!4</td>
<td></td>
</tr>
<tr>
<td>server-port</td>
<td>Int</td>
<td>3000</td>
<td></td>
</tr>
<tr>
<td>server-unix-socket</td>
<td>String</td>
<td></td>
<td></td>
</tr>
<tr>
<td>server-unix-socket-mode</td>
<td>String</td>
<td>660</td>
<td></td>
</tr>
<tr>
<td>log-level</td>
<td>String</td>
<td>error</td>
<td></td>
</tr>
<tr>
<td>openapi-mode</td>
<td>String</td>
<td>follow-privileges</td>
<td></td>
</tr>
<tr>
<td>openapi-server-proxy-uri</td>
<td>String</td>
<td></td>
<td></td>
</tr>
<tr>
<td>jwt-secret</td>
<td>String</td>
<td></td>
<td></td>
</tr>
<tr>
<td>jwt-aud</td>
<td>String</td>
<td></td>
<td></td>
</tr>
<tr>
<td>secret-is-base64</td>
<td>Boolean</td>
<td>False</td>
<td></td>
</tr>
<tr>
<td>max-rows</td>
<td>Int</td>
<td>∞</td>
<td></td>
</tr>
<tr>
<td>pre-request</td>
<td>String</td>
<td></td>
<td></td>
</tr>
<tr>
<td>app.settings.*</td>
<td>String</td>
<td></td>
<td></td>
</tr>
<tr>
<td>role-claim-key</td>
<td>String</td>
<td>.role</td>
<td></td>
</tr>
<tr>
<td>raw-media-types</td>
<td>String</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 8.12.1 db-uri

The standard connection PostgreSQL URI format. Symbols and unusual characters in the password or other fields should be percent encoded to avoid a parse error. If enforcing an SSL connection to the database is required you can use `sslmode` in the URI, for example `postgres://user:pass@host:5432/dbname?sslmode=require`.

When running PostgREST on the same machine as PostgreSQL, it is also possible to connect to the database using a Unix socket and the Peer Authentication method as an alternative to TCP/IP communication and authentication with a password, this also grants higher performance. To do this you can
omit the host and the password, e.g. `postgres://user@/dbname`, see the libpq connection string documentation for more details.

On older systems like Centos 6, with older versions of libpq, a different db-uri syntax has to be used. In this case the URI is a string of space separated key-value pairs (key=value), so the example above would be "host=host user=user port=5432 dbname=dbname password=pass".

Choosing a value for this parameter beginning with the at sign such as `@filename` (e.g. `@./configs/my-config`) loads the secret out of an external file.

### 8.12.2 db-schema

The database schema to expose to REST clients. Tables, views and stored procedures in this schema will get API endpoints.

```plaintext
db-schema = "api"
```

This schema gets added to the `search_path` of every request.

#### List of schemas

You can also specify a list of schemas that can be used for schema-based multitenancy and api versioning by Switching Schemas. Example:

```plaintext
db-schema = "tenant1, tenant2"
```

If you don’t Switch Schemas, the first schema in the list(`tenant1` in this case) is chosen as the default schema.

*Only the chosen schema* gets added to the `search_path` of every request.

**Warning:** Never expose private schemas in this way. See Schema Isolation.

### 8.12.3 db-anon-role

The database role to use when executing commands on behalf of unauthenticated clients. For more information, see Overview of Role System.

### 8.12.4 db-pool

Number of connections to keep open in PostgREST’s database pool. Having enough here for the maximum expected simultaneous client connections can improve performance. Note it’s pointless to set this higher than the `max_connections` GUC in your database.

### 8.12.5 db-pool-timeout

Time to live, in seconds, for an idle database pool connection. If the timeout is reached the connection will be closed. Once a new request arrives a new connection will be started.
8.12.6 **db-extra-search-path**

Extra schemas to add to the `search_path` of every request. These schemas tables, views and stored procedures don’t get API endpoints, they can only be referred from the database objects inside your `db-schema`.

This parameter was meant to make it easier to use PostgreSQL extensions (like PostGIS) that are outside of the `db-schema`.

Multiple schemas can be added in a comma-separated string, e.g. `public, extensions`.

8.12.7 **db-channel**

The name of the notification channel that PostgREST uses for Schema Cache Reloading and configuration reloading.

8.12.8 **db-channel-enabled**

When this is set to `true`, the notification channel specified in `db-channel` is enabled.

You should set this to `false` when using PostgresSQL behind an external connection pooler such as PgBouncer working in transaction pooling mode. See this section for more information.

8.12.9 **db-prepared-statements**

Enables or disables prepared statements.

When disabled, the generated queries will be parameterized (invulnerable to SQL injection) but they will not be prepared (cached in the database session). Not using prepared statements will noticeably decrease performance, so it’s recommended to always have this setting enabled.

You should only set this to `false` when using PostgresSQL behind an external connection pooler such as PgBouncer working in transaction pooling mode. See this section for more information.

8.12.10 **db-tx-end**

Specifies how to terminate the database transactions.

```plaintext
# The transaction is always committed
db-tx-end = "commit"

# The transaction is committed unless a "Prefer: tx=rollback" header is sent
db-tx-end = "commit-allow-override"

# The transaction is always rolled back
db-tx-end = "rollback"

# The transaction is rolled back unless a "Prefer: tx=commit" header is sent
db-tx-end = "rollback-allow-override"
```

8.12.11 **db-config**

Enables the in-database configuration.
8.12.12 server-host

Where to bind the PostgREST web server. In addition to the usual address options, PostgREST interprets these reserved addresses with special meanings:

- * - any IPv4 or IPv6 hostname
- *4 - any IPv4 or IPv6 hostname, IPv4 preferred
- !4 - any IPv4 hostname
- *6 - any IPv4 or IPv6 hostname, IPv6 preferred
- !6 - any IPv6 hostname

8.12.13 server-port

The TCP port to bind the web server.

8.12.14 server-unix-socket

Unix domain socket where to bind the PostgREST web server. If specified, this takes precedence over server-port. Example:

```
server-unix-socket = "/tmp/pgrst.sock"
```

8.12.15 server-unix-socket-mode

Unix file mode to be set for the socket specified in server-unix-socket. Needs to be a valid octal between 600 and 777.

```
server-unix-socket-mode = "660"
```

8.12.16 log-level

Specifies the level of information to be logged while running PostgREST.

```
# Only startup and db connection recovery messages are logged
log-level = "crit"

# All the "crit" level events plus server errors (status 5xx) are logged
log-level = "error"

# All the "error" level events plus request errors (status 4xx) are logged
log-level = "warn"

# All the "warn" level events plus all requests (every status code) are logged
log-level = "info"
```

Because currently there's no buffering for logging, the levels with minimal logging (crit/error) will increase throughput.
8.12.17 openapi-mode

Specifies how the OpenAPI output should be displayed.

```lang-none
# Follows the privileges of the JWT role claim (or from db-anon-role if the
# JWT is not sent)
# Shows information depending on the permissions that the role making the
# request has
openapi-mode = "follow-privileges"

# Ignores the privileges of the JWT role claim (or from db-anon-role if the
# JWT is not sent)
# Shows all the exposed information, regardless of the permissions that the
# role making the request has
openapi-mode = "ignore-privileges"

# Disables the OpenApi output altogether.
# Throws a `404 Not Found` error when accessing the API root path
openapi-mode = "disabled"
```

8.12.18 openapi-server-proxy-uri

Overrides the base URL used within the OpenAPI self-documentation hosted at the API root path. Use a complete URI syntax scheme://[//[user:password@]host[:port]][/]path[?query][#fragment]. Ex. https://postgrest.com

```json
{
    "swagger": "2.0",
    "info": {
        "version": "0.4.3.0",
        "title": "PostgREST API",
        "description": "This is a dynamic API generated by PostgREST"
    },
    "host": "postgrest.com:443",
    "basePath": "/",
    "schemes": ["https"
    }
}
```

8.12.19 jwt-secret

The secret or JSON Web Key (JWK) (or set) used to decode JWT tokens clients provide for authentication. For security the key must be at least 32 characters long. If this parameter is not specified then PostgREST refuses authentication requests. Choosing a value for this parameter beginning with the at sign such as @filename loads the secret out of an external file. This is useful for automating deployments. Note that any binary secrets must be base64 encoded. Both symmetric and asymmetric cryptography are supported. For more info see Asymmetric Keys.

8.12.20 jwt-aud

 Specifies the JWT audience claim. If this claim is present in the client provided JWT then you must set this to the same value as in the JWT, otherwise verifying the JWT will fail.
8.12.21 secret-is-base64

When this is set to true, the value derived from jwt-secret will be treated as a base64 encoded secret.

8.12.22 max-rows

A hard limit to the number of rows PostgREST will fetch from a view, table, or stored procedure. Limits payload size for accidental or malicious requests.

8.12.23 pre-request

A schema-qualified stored procedure name to call right after switching roles for a client request. This provides an opportunity to modify SQL variables or raise an exception to prevent the request from completing.

8.12.24 app.settings.*

Arbitrary settings that can be used to pass in secret keys directly as strings, or via OS environment variables. For instance: app.settings.jwt_secret = "$(MYAPP_JWT_SECRET)" will take MYAPP_JWT_SECRET from the environment and make it available to postgresql functions as current_setting('app.settings.jwt_secret').

8.12.25 role-claim-key

A JSPath DSL that specifies the location of the role key in the JWT claims. This can be used to consume a JWT provided by a third party service like Auth0, Okta or Keycloak. Usage examples:

```sql
# { "postgrest": { "roles": [ "other", "author" ] } }
role-claim-key = ".postgrest.roles[1]"

# { "https://www.example.com/role": { "key": "author" } }
role-claim-key = ".\"https://www.example.com/role\".key"
```

8.12.26 raw-media-types

This serves to extend the Media Types that PostgREST currently accepts through an Accept header. These media types can be requested by following the same rules as the ones defined in Binary Output. As an example, the below config would allow you to request an image and a XML file by doing a request with Accept: image/png or Accept: text/xml, respectively.

```
raw-media-types="image/png, text/xml"
```
8.13 Environment Variables

You can also set these configuration parameters using environment variables. They are capitalized, have a PGRST_ prefix, and use underscores. For example: PGRST_DB_URI corresponds to db-uri and PGRST_APP_SETTINGS_* to app.settings.*.

8.14 Configuration Reloading

To reload the configuration without restarting the PostgREST server, send a SIGUSR2 signal to the server process. 

```
killall -SIGUSR2 postgrest
```

This method does not reload Environment Variables and it will not work for reloading a Docker container configuration. In these cases, you need to restart the PostgREST server or use the In-Database Configuration as an alternative.

**Important:** The following settings will not be reread when reloading the configuration. You will need to restart PostgREST in that case.

- db-uri
- db-pool
- db-pool-timeout
- server-host
- server-port
- server-unix-socket
- server-unix-socket-mode

8.15 In-Database Configuration

By adding settings to the authenticator role (see Overview of Role System), you can make the database the single source of truth for PostgREST’s configuration. This is enabled by db-config.

For example, you can configure db-schema and jwt-secret like this:

```
ALTER ROLE authenticator SET pgrst.db_schema = "tenant1, tenant2, tenant3"
ALTER ROLE authenticator SET pgrst.jwt_secret = "REALYREALYREALYREALYREALYVERYSAFE"
```

Note that underscores(_) need to be used instead of dashes(–) for the in-database config options.

**Important:** For altering a role in this way, you need a SUPERUSER. You might not be able to use this configuration mode on cloud-hosted databases.

When using both the configuration file and the in-database configuration, the latter takes precedence.
Danger: If direct connections to the database are allowed, then it’s not safe to use the in-db configuration for storing the `jwt-secret`. The settings of every role are PUBLIC - they can be viewed by any user that queries the `pg_catalog.pg_db_role_setting` table. In this case you should keep the `jwt-secret` in the configuration file or as environment variables.

8.15.1 In-database configuration reloading

To reload the in-database configuration from within the database, you can use a NOTIFY command.

```
NOTIFY pgrst, 'reload config'
```

The "pgrst" notification channel is enabled by default. For configuring the channel, see `db-channel` and `db-channel-enabled`.

8.16 Schema Cache

Certain PostgREST features require metadata from the database schema. Getting this metadata requires executing expensive queries, so in order to avoid repeating this work, PostgREST uses a schema cache.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Required Metadata</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Embedding</td>
<td>Foreign key constraints</td>
</tr>
<tr>
<td>Stored Functions</td>
<td>Function signature (parameters, return type, volatility and overloading)</td>
</tr>
<tr>
<td>Upserts</td>
<td>Primary keys</td>
</tr>
<tr>
<td>Insertions</td>
<td>Primary keys (optional: only if the Location header is requested)</td>
</tr>
<tr>
<td>OPTIONS requests</td>
<td>View INSTEAD OF TRIGGERS and primary keys</td>
</tr>
<tr>
<td>OpenAPI Support</td>
<td>Table columns, primary keys and foreign keys</td>
</tr>
<tr>
<td></td>
<td>View columns and INSTEAD OF TRIGGERS</td>
</tr>
<tr>
<td></td>
<td>Function signature</td>
</tr>
</tbody>
</table>

8.16.1 The Stale Schema Cache

When you make changes on the metadata mentioned above, the schema cache will turn stale on a running PostgREST. Future requests that use the above features will need the `schema cache to be reloaded`; otherwise, you’ll get an error instead of the expected result.

For instance, let’s see what would happen if you have a stale schema cache for foreign key relationships and function signatures.

Stale Foreign Key Relationships

Suppose you add a `cities` table to your database and define a foreign key that references an existing `countries` table. Then, you make a request to get the `cities` and their belonging `countries`.

```
GET /cities?select=name,country:countries(id,name) HTTP/1.1
```

The result will be an error:
As you can see, PostgREST couldn’t find the newly created foreign key in the schema cache. See **Schema Cache Reloading** and **Automatic Schema Cache Reloading** to solve this issue.

### Stale Function Signature

The same issue will occur on newly created functions on a running PostgREST.

```sql
CREATE FUNCTION plus_one(num integer)
RETURNS integer AS $$
SELECT num + 1;
$$ LANGUAGE SQL IMMUTABLE;
```

```bash
GET /rpc/plus_one?num=1 HTTP/1.1
```

Here, PostgREST tries to find the function on the stale schema to no avail. See **Schema Cache Reloading** and **Automatic Schema Cache Reloading** to solve this issue.

### 8.16.2 Schema Cache Reloading

To reload the cache without restarting the PostgREST server, send a SIGUSR1 signal to the server process.

```bash
killall -SIGUSR1 postgrest
```

For docker you can do:

```bash
docker kill -s SIGUSR1 <container>
# or in docker-compose
docker-compose kill -s SIGUSR1 <service>
```

There’s no downtime when reloading the schema cache. The reloading will happen on a background thread while requests keep being served.

### Reloading with NOTIFY

There are environments where you can’t send the SIGUSR1 Unix Signal (like on managed containers in cloud services or on Windows systems). For this reason, PostgREST also allows you to reload its schema cache through PostgreSQL NOTIFY as follows:
The "pgrst" notification channel is enabled by default. For configuring the channel, see `db-channel` and `db-channel-enabled`.

### 8.16.3 Automatic Schema Cache Reloading

You can do automatic schema cache reloading in a pure SQL way and forget about stale schema cache errors with an event trigger and NOTIFY.

```sql
-- Create an event trigger function
CREATE OR REPLACE FUNCTION public.pgrst_watch() RETURNS event_trigger
    LANGUAGE plpgsql
AS $$
BEGIN
    NOTIFY pgrst, 'reload schema';
END;
$$;

-- This event trigger will fire after every ddl_command_end event
CREATE EVENT TRIGGER pgrst_watch
    ON ddl_command_end
    EXECUTE PROCEDURE public.pgrst_watch();
```

Now, whenever the `pgrst_watch` trigger is fired in the database, PostgREST will automatically reload the schema cache.

To disable auto reloading, drop the trigger:

```sql
DROP EVENT TRIGGER pgrst_watch
```

- API
- Configuration
- Schema Cache
Explanations of some key concepts in PostgREST.

9.1 Overview of Role System

PostgREST is designed to keep the database at the center of API security. All authorization happens through database roles and permissions. It is PostgREST’s job to authenticate requests – i.e. verify that a client is who they say they are – and then let the database authorize client actions.

9.1.1 Authentication Sequence

There are three types of roles used by PostgREST, the authenticator, anonymous and user roles. The database administrator creates these roles and configures PostgREST to use them.
The authenticator should be created `NOINHERIT` and configured in the database to have very limited access. It is a chameleon whose job is to “become” other users to service authenticated HTTP requests. The picture below shows how the server handles authentication. If auth succeeds, it switches into the user role specified by the request, otherwise it switches into the anonymous role.

Here are the technical details. We use JSON Web Tokens to authenticate API requests. As you’ll recall a JWT contains a list of cryptographically signed claims. All claims are allowed but PostgREST cares specifically about a claim called `role`.
When a request contains a valid JWT with a role claim PostgREST will switch to the database role with that name for the duration of the HTTP request.

```
SET LOCAL ROLE user123;
```

Note that the database administrator must allow the authenticator role to switch into this user by previously executing

```
GRANT user123 TO authenticator;
```

If the client included no JWT (or one without a role claim) then PostgREST switches into the anonymous role whose actual database-specific name, like that of with the authenticator role, is specified in the PostgREST server configuration file. The database administrator must set anonymous role permissions correctly to prevent anonymous users from seeing or changing things they shouldn’t.

### 9.1.2 Users and Groups

PostgreSQL manages database access permissions using the concept of roles. A role can be thought of as either a database user, or a group of database users, depending on how the role is set up.

**Roles for Each Web User**

PostgREST can accommodate either viewpoint. If you treat a role as a single user then the JWT-based role switching described above does most of what you need. When an authenticated user makes a request PostgREST will switch into the role for that user, which in addition to restricting queries, is available to SQL through the `current_user` variable.

You can use row-level security to flexibly restrict visibility and access for the current user. Here is an example from Tomas Vondra, a chat table storing messages sent between users. Users can insert rows into it to send messages to other users, and query it to see messages sent to them by other users.

```sql
CREATE TABLE chat (
  message_uuid UUID PRIMARY KEY DEFAULT uuid_generate_v4(),
  message_time TIMESTAMP NOT NULL DEFAULT now(),
  message_from NAME NOT NULL DEFAULT current_user,
  message_to NAME NOT NULL,
  message_subject VARCHAR(64) NOT NULL,
  message_body TEXT
);
```

```
ALTER TABLE chat ENABLE ROW LEVEL SECURITY;
```

We want to enforce a policy that ensures a user can see only those messages sent by him or intended for him. Also we want to prevent a user from forging the `message_from` column with another person’s name.

PostgreSQL (9.5 and later) allows us to set this policy with row-level security:

```sql
CREATE POLICY chat_policy ON chat
  USING ((message_to = current_user) OR (message_from = current_user))
  WITH CHECK (message_from = current_user)
```
Anyone accessing the generated API endpoint for the chat table will see exactly the rows they should, without our needing custom imperative server-side coding.

**Warning:** Roles are namespaced per-cluster rather than per-database so they may be prone to collision.

### Web Users Sharing Role

Alternately database roles can represent groups instead of (or in addition to) individual users. You may choose that all signed-in users for a web app share the role webuser. You can distinguish individual users by including extra claims in the JWT such as email.

```
{
  "role": "webuser",
  "email": "john@doe.com"
}
```

SQL code can access claims through GUC variables set by PostgREST per request. For instance to get the email claim, call this function:

```sql
current_setting('request.jwt.claim.email', true)
```

This allows JWT generation services to include extra information and your database code to react to it. For instance the RLS example could be modified to use this `current_setting` rather than `current_user`. The second ‘true’ argument tells `current_setting` to return NULL if the setting is missing from the current configuration.

### Hybrid User-Group Roles

You can mix the group and individual role policies. For instance we could still have a webuser role and individual users which inherit from it:

```
CREATE ROLE webuser NOLOGIN;
-- grant this role access to certain tables etc

CREATE ROLE user000 NOLOGIN;
GRANT webuser TO user000;
-- now user000 can do whatever webuser can

GRANT user000 TO authenticator;
-- allow authenticator to switch into user000 role
-- (the role itself has nologin)
```

### 9.1.3 Custom Validation

PostgREST honors the `exp` claim for token expiration, rejecting expired tokens. However it does not enforce any extra constraints. An example of an extra constraint would be to immediately revoke access for a certain user. The configuration file parameter `pre-request` specifies a stored procedure to call immediately after the authenticator switches into a new role and before the main query itself runs.

Here’s an example. In the config file specify a stored procedure:

```text
pre-request = "public.check_user"
```
In the function you can run arbitrary code to check the request and raise an exception to block it if desired.

```sql
CREATE OR REPLACE FUNCTION check_user() RETURNS void AS $$
BEGIN
    IF current_user = 'evil_user' THEN
        RAISE EXCEPTION 'No, you are evil'
            USING HINT = 'Stop being so evil and maybe you can log in';
    END IF;
END $$
LANGUAGE plpgsql;
```

### 9.2 Client Auth

To make an authenticated request the client must include an Authorization HTTP header with the value `Bearer <jwt>`. For instance:

```
GET /foo HTTP/1.1
Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
   --eyJyb2xlIjoiamRvZSI6ImlvQ29tcHJvYmF0ZSIsImV4cCI6MTQ3NTUxNjI1MH0.GYD2V3yM0gqvutEJmfpp1LBXSYnke_--PvniOtbKAjB4
```

The `Bearer` header value can be used with or without capitalization(`bearer`).

#### 9.2.1 JWT Generation

You can create a valid JWT either from inside your database or via an external service. Each token is cryptographically signed with a secret key. In the case of symmetric cryptography the signer and verifier share the same secret passphrase. In asymmetric cryptography the signer uses the private key and the verifier the public key. PostgREST supports both symmetric and asymmetric cryptography.

**JWT from SQL**

You can create JWT tokens in SQL using the `pgjwt` extension. It’s simple and requires only `pgcrypto`. If you’re on an environment like Amazon RDS which doesn’t support installing new extensions, you can still manually run the SQL inside `pgjwt` (you’ll need to replace `extschema@` with another schema or just delete it) which creates the functions you will need.

Next write a stored procedure that returns the token. The one below returns a token with a hard-coded role, which expires five minutes after it was issued. Note this function has a hard-coded secret as well.

```sql
CREATE TYPE jwt_token AS (
    token text
);

CREATE FUNCTION jwt_test() RETURNS public.jwt_token AS $$
SELECT
    public.sign(
        row_to_json(r), 'reallyreallyreallyreallyverysafe'
    ) AS token
FROM
    (
        SELECT
            'my_role'::text as role,
            extract(epoch from now())::integer + 300 AS exp
        )
$$;
```

(continues on next page)
PostgREST exposes this function to clients via a POST request to /rpc/jwt_test.

Note: To avoid hard-coding the secret in stored procedures, save it as a property of the database.

```sql
-- run this once
ALTER DATABASE mydb SET "app.jwt_secret" TO 'reallyreallyreallyreallyverysafe';

-- then all functions can refer to app.jwt_secret
SELECT sign(
    row_to_json(r), current_setting('app.jwt_secret')
) AS token
FROM ...
```

**JWT from Auth0**

An external service like Auth0 can do the hard work transforming OAuth from Github, Twitter, Google etc into a JWT suitable for PostgREST. Auth0 can also handle email signup and password reset flows.

To use Auth0, create an application for your app and an API for your PostgREST server. Auth0 supports both HS256 and RS256 scheme for the issued tokens for APIs. For simplicity, you may first try HS256 scheme while creating your API on Auth0. Your application should use your PostgREST API’s API identifier by setting it with the audience parameter during the authorization request. This will ensure that Auth0 will issue an access token for your PostgREST API. For PostgREST to verify the access token, you will need to set jwt-secret on PostgREST config file with your API’s signing secret.

Note: Our code requires a database role in the JWT. To add it you need to save the database role in Auth0 app metadata. Then, you will need to write a rule that will extract the role from the user’s app_metadata and set it as a custom claim in the access token. Note that, you may use Auth0’s core authorization feature for more complex use cases. Metadata solution is mentioned here for simplicity.

```javascript
function (user, context, callback) {

    // Follow the documentations at
    // https://postgrest.org/en/latest/configuration.html#role-claim-key
    // to set a custom role claim on PostgREST
    // and use it as custom claim attribute in this rule
    const myRoleClaim = 'https://myapp.com/role';

    user.app_metadata = user.app_metadata || {};
    context.accessToken[myRoleClaim] = user.app_metadata.role;
    callback(null, user, context);
}
```

**Asymmetric Keys**

As described in the Configuration section, PostgREST accepts a jwt-secret config file parameter. If it is set to a simple string value like “reallyreallyreallyreallyverysafe” then PostgREST interprets it as an HMAC-SHA256
passphrase. However you can also specify a literal JSON Web Key (JWK) or set. For example, you can use an RSA-256 public key encoded as a JWK:

```
{
    "alg":"RS256",
    "e":"AQAB",
    "key_ops": ["verify"],
    "kty":"RSA",
    "n":"9zKKNYTaYGfGmltBMpRT6Fx0YrM720Ghxddtcc02uyakYSEHU2IJz9QG_ML1E14-WWWYoS_
    →QKFupw3s7aPY1aaAjamG22rAnvWu-rRk5sSSkKvud_IgKL4iE6Y2WJx2Bk11XUFkdZ8wiEUR601ft3TS4uA-
    →qKifsZ43CahzAjyUezOH9shI--tirC0281Ng7671dEki3WnVr3zokSujC9YJ_9XXjw2hFBfmJUrNb0-
    →wldvxQbFUB8PXip-GQ_JPTrCT2hrzGFepWvhA6Rgmc3b1PhM9jY7DurlsjYWYVyX1FNCK3c-
    →6feo5W1Rfe1aCWmwZQh60I8eTmLeTeT4nWYkDzQ"
}
```

**Note:** This could also be a JSON Web Key Set (JWKS) if it was contained within an array assigned to a `keys` member, e.g. `{ keys: [jwk1, jwk2] }`.

Just pass it in as a single line string, escaping the quotes:

```
jwt-secret = "{" "alg":"RS256"", ... }
```

To generate such a public/private key pair use a utility like latchset/jose.

```
jose jwk gen -i '{"alg" : "RS256"}' -o rsa.jwk
jose jwk pub -i rsa.jwk -o rsa.jwk.pub
```

# now rsa.jwk.pub contains the desired JSON object

You can specify the literal value as we saw earlier, or reference a filename to load the JWK from a file:

```
jwt-secret = "@rsa.jwk.pub"
```

### JWT security

There are at least three types of common critiques against using JWT: 1) against the standard itself, 2) against using libraries with known security vulnerabilities, and 3) against using JWT for web sessions. We’ll briefly explain each critique, how PostgREST deals with it, and give recommendations for appropriate user action.

The critique against the JWT standard is voiced in detail elsewhere on the web. The most relevant part for PostgREST is the so-called `alg=none` issue. Some servers implementing JWT allow clients to choose the algorithm used to sign the JWT. In this case, an attacker could set the algorithm to `none`, remove the need for any signature at all and gain unauthorized access. The current implementation of PostgREST, however, does not allow clients to set the signature algorithm in the HTTP request, making this attack irrelevant. The critique against the standard is that it requires the implementation of the `alg=none` at all.

Critiques against JWT libraries are only relevant to PostgREST via the library it uses. As mentioned above, not allowing clients to choose the signature algorithm in HTTP requests removes the greatest risk. Another more subtle attack is possible where servers use asymmetric algorithms like RSA for signatures. Once again this is not relevant to PostgREST since it is not supported. Curious readers can find more information in this article. Recommendations about high quality libraries for usage in API clients can be found on jwt.io.

The last type of critique focuses on the misuse of JWT for maintaining web sessions. The basic recommendation is to stop using JWT for sessions because most, if not all, solutions to the problems that arise when you do, do not work.
The linked articles discuss the problems in depth but the essence of the problem is that JWT is not designed to be secure and stateful units for client-side storage and therefore not suited to session management.

PostgREST uses JWT mainly for authentication and authorization purposes and encourages users to do the same. For web sessions, using cookies over HTTPS is good enough and well catered for by standard web frameworks.

### 9.3 Schema Isolation

You can isolate your api schema from internal implementation details, as explained in *Schema Isolation*. For an example of wrapping a private table with a public view see the *Public User Interface* section below.

### 9.4 SQL User Management

#### 9.4.1 Storing Users and Passwords

As mentioned, an external service can provide user management and coordinate with the PostgREST server using JWT. It’s also possible to support logins entirely through SQL. It’s a fair bit of work, so get ready.

The following table, functions, and triggers will live in a `basic_auth` schema that you shouldn’t expose publicly in the API. The public views and functions will live in a different schema which internally references this internal information.

First we’ll need a table to keep track of our users:

```sql
-- We put things inside the basic_auth schema to hide
-- them from public view. Certain public procs/views will
-- refer to helpers and tables inside.
create schema if not exists basic_auth;
create table if not exists basic_auth.users (
    email  text primary key check ( email ~ '^\+.+@.+.+$' ),
    pass   text not null check (length(pass) < 512),
    role   name not null check (length(role) < 512)
);
```

We would like the role to be a foreign key to actual database roles, however PostgreSQL does not support these constraints against the `pg_roles` table. We’ll use a trigger to manually enforce it.

```sql
create or replace function basic_auth.check_role_exists()
    returns trigger as $$
begin
    if not exists (select 1 from pg_roles as r where r.rolname = new.role) then
        raise foreign_key_violation using message =
            'unknown database role: ' || new.role;
        return null;
    end if;
    return new;
end
$$ language plpgsql;

drop trigger if exists ensure_user_role_exists on basic_auth.users;
create constraint trigger ensure_user_role_exists
    after insert or update on basic_auth.users
```

(continues on next page)
Next we’ll use the pgcrypto extension and a trigger to keep passwords safe in the users table.

```sql
create extension if not exists pgcrypto;
create or replace function basic_auth.encrypt_pass() returns trigger as $$
begin
    if tg_op = 'INSERT' or new.pass <> old.pass then
        new.pass = crypt(new.pass, gen_salt('bf'));
    end if;
    return new;
end
$$ language plpgsql;

drop trigger if exists encrypt_pass on basic_auth.users;
create trigger encrypt_pass
    before insert or update on basic_auth.users
    for each row
    execute procedure basic_auth.encrypt_pass();
```

With the table in place we can make a helper to check a password against the encrypted column. It returns the database role for a user if the email and password are correct.

```sql
create or replace function basic_auth.user_role(email text, pass text) returns name language plpgsql as $$
begin
    return (select role from basic_auth.users
        where users.email = user_role.email
        and users.pass = crypt(user_role.pass, users.pass));
end;
$$
```

### 9.4.2 Public User Interface

In the previous section we created an internal table to store user information. Here we create a login function which takes an email address and password and returns JWT if the credentials match a user in the internal table.

**Logins**

As described in *JWT from SQL*, we’ll create a JWT inside our login function. Note that you’ll need to adjust the secret key which is hard-coded in this example to a secure (at least thirty-two character) secret of your choosing.

```sql
-- add type
CREATE TYPE basic_auth.jwt_token AS (token text);
```
-- login should be on your exposed schema
create or replace function
login(email text, pass text) returns basic_auth.jwt_token as $$
declare
_role name;
result basic_auth.jwt_token;
begin
-- check email and password
select basic_auth.user_role(email, pass) into _role;
if _role is null then
raise invalid_password using message = 'invalid user or password';
end if;

select sign(
    row_to_json(r), 'reallyreallyreallyreallyverysafe'
) as token
from (  
    select _role as role, login.email as email,
        extract(epoch from now())::integer + 60*60 as exp  
) r
into result;
return result;
end;
$$ language plpgsql security definer;

An API request to call this function would look like:

POST /rpc/login HTTP/1.1

{ "email": "foo@bar.com", "pass": "foobaz" }

The response would look like the snippet below. Try decoding the token at jwt.io. (It was encoded with a secret of reallyreallyreallyreallyverysafe as specified in the SQL code above. You'll want to change this secret in your app!)

```
{
    "token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
        eyjlWfpbCl61mZvb0BiYXJuY29cIiwiGFzcyI6ImZvb2JhciJ9.37066TTRlh-
        1hXhnA9oO9Pj61gL6zFuJU0iCHhuCFno"
}
```

Permissions

Your database roles need access to the schema, tables, views and functions in order to service HTTP requests. Recall from the Overview of Role System that PostgREST uses special roles to process requests, namely the authenticator and anonymous roles. Below is an example of permissions that allow anonymous users to create accounts and attempt to log in.

```
-- the names "anon" and "authenticator" are configurable and not
-- sacred, we simply choose them for clarity
create role anon noinherit;
create role authenticator noinherit;
grant anon to authenticator;
```
grant execute on function login(text, text) to anon;

Since the above login function is defined as security definer, the anonymous user anon doesn’t need permission to read the basic_auth.users table. It doesn’t even need permission to access the basic_auth schema. grant execute on function is included for clarity but it might not be needed, see Functions for more details.

Note: This page is a work in progress.

9.5 Schema Isolation

A PostgREST instance exposes all the tables, views, and stored procedures of a single PostgreSQL schema (a namespace of database objects). This means private data or implementation details can go inside different private schemas and be invisible to HTTP clients.

It is recommended that you don’t expose tables on your API schema. Instead expose views and stored procedures which insulate the internal details from the outside world. This allows you to change the internals of your schema and maintain backwards compatibility. It also keeps your code easier to refactor, and provides a natural way to do API versioning.

9.6 Functions

By default, when a function is created, the privilege to execute it is not restricted by role. The function access is PUBLIC — executable by all roles (more details at PostgreSQL Privileges page). This is not ideal for an API schema. To disable this behavior, you can run the following SQL statement:

```
ALTER DEFAULT PRIVILEGES REVOKE EXECUTE ON FUNCTIONS FROM PUBLIC;
```

This will change the privileges for all functions created in the future in all schemas. Currently there is no way to limit it to a single schema. In our opinion it’s a good practice anyway.

Note: It is however possible to limit the effect of this clause only to functions you define. You can put the above statement at the beginning of the API schema definition, and then at the end reverse it with:

```
ALTER DEFAULT PRIVILEGES GRANT EXECUTE ON FUNCTIONS TO PUBLIC;
```

This will work because the alter default privileges statement has effect on function created after it is executed. See PostgreSQL alter default privileges for more details.

After that, you’ll need to grant EXECUTE privileges on functions explicitly:
GRANT EXECUTE ON FUNCTION login TO anonymous;
GRANT EXECUTE ON FUNCTION signup TO anonymous;

You can also grant execute on all functions in a schema to a higher privileged role:

GRANT EXECUTE ON ALL FUNCTIONS IN SCHEMA api TO web_user;

### 9.6.1 Security definer

A function is executed with the privileges of the user who calls it. This means that the user has to have all permissions to do the operations the procedure performs. If the function accesses private database objects, your API roles won’t be able to successfully execute the function.

Another option is to define the function with the `SECURITY DEFINER` option. Then only one permission check will take place, the permission to call the function, and the operations in the function will have the authority of the user who owns the function itself.

```sql
-- login as a user which has privileges on the private schemas
-- create a sample function
create or replace function login(email text, pass text) returns jwt_token as $$
begin
  -- access to a private schema called 'auth'
  select auth.user_role(email, pass) into _role;
  -- other operations
  -- ...
end;
$$ language plpgsql security definer;
```

Note the `SECURITY DEFINER` keywords at the end of the function. See [PostgreSQL documentation](https://www.postgresql.org) for more details.

### 9.7 Views

Views are invoked with the privileges of the view owner, much like stored procedures with the `SECURITY DEFINER` option. When created by a SUPERUSER role, all row-level security will be bypassed unless a different, non-SUPERUSER owner is specified.

For changing this, we can create a non-SUPERUSER role and make this role the view’s owner.

```sql
CREATE ROLE api_views_owner NOINHERIT;
ALTER VIEW sample_view OWNER TO api_views_owner;
```

### 9.7.1 Rules

Insertion on views with complex rules might not work out of the box with PostgREST. It’s recommended that you use triggers instead of rules. If you want to keep using rules, a workaround is to wrap the view insertion in a stored procedure and call it through the [Stored Procedures](https://example.com) interface. For more details, see [this github issue](https://github.com/postgres/postgres/issues/2000).
9.8 Hardening PostgREST

PostgREST is a fast way to construct a RESTful API. Its default behavior is great for scaffolding in development. When it’s time to go to production it works great too, as long as you take precautions. PostgREST is a small sharp tool that focuses on performing the API-to-database mapping. We rely on a reverse proxy like Nginx for additional safeguards.

The first step is to create an Nginx configuration file that proxies requests to an underlying PostgREST server.

```nginx
http {
  # ...
  # upstream configuration
  upstream postgrest {
    server localhost:3000;
  }
  # ...
  server {
    # ...
    # expose to the outside world
    location /api/ {
      default_type application/json;
      proxy_hide_header Content-Location;
      add_header Content-Location /api/$upstream_http_content_location;
      proxy_set_header Connection "";
      proxy_http_version 1.1;
      proxy_pass http://postgrest/;
    }
    # ...
  }
}
```

**Note:** For ubuntu, if you already installed nginx through `apt` you can add this to the config file in `/etc/nginx/sites-enabled/default`.

9.8.1 Block Full-Table Operations

Each table in the admin-selected schema gets exposed as a top level route. Client requests are executed by certain database roles depending on their authentication. All HTTP verbs are supported that correspond to actions permitted to the role. For instance if the active role can drop rows of the table then the DELETE verb is allowed for clients. Here’s an API request to delete old rows from a hypothetical logs table:

```
DELETE /logs?time=lt.1991-08-06 HTTP/1.1
```

However it’s very easy to delete the **entire table** by omitting the query parameter!

```
DELETE /logs HTTP/1.1
```

This can happen accidentally such as by switching a request from a GET to a DELETE. To protect against accidental operations use the `pg-safeupdate` PostgreSQL extension. It raises an error if UPDATE or DELETE are executed without specifying conditions. To install it you can use the PGXN network:

```
sudo -E pgxn install safeupdate
```

(continues on next page)
# then add this to postgresql.conf:
# shared_preload_libraries='safeupdate';

This does not protect against malicious actions, since someone can add a url parameter that does not affect the result set. To prevent this you must turn to database permissions, forbidding the wrong people from deleting rows, and using row-level security if finer access control is required.

## 9.8.2 Count-Header DoS

For convenience to client-side pagination controls PostgREST supports counting and reporting total table size in its response. As described in *Limits and Pagination*, responses ordinarily include a range but leave the total unspecified like

```
HTTP/1.1 200 OK
Range-Unit: items
Content-Range: 0-14/*
```

However including the request header `Prefer: count=exact` calculates and includes the full count:

```
HTTP/1.1 206 Partial Content
Range-Unit: items
Content-Range: 0-14/3573458
```

This is fine in small tables, but count performance degrades in big tables due to the MVCC architecture of PostgreSQL. For very large tables it can take a very long time to retrieve the results which allows a denial of service attack. The solution is to strip this header from all requests:

```
-- Pending nginx config: Remove any prefer header which contains the word count
```

## 9.8.3 HTTPS

PostgREST aims to do one thing well: add an HTTP interface to a PostgreSQL database. To keep the code small and focused we do not implement HTTPS. Use a reverse proxy such as NGINX to add this, here's how. Note that some Platforms as a Service like Heroku also add SSL automatically in their load balancer.

## 9.8.4 Rate Limiting

NGINX supports “leaky bucket” rate limiting (see official docs). Using standard NGINX configuration, routes can be grouped into request zones for rate limiting. For instance we can define a zone for login attempts:

```
limit_req_zone $binary_remote_addr zone=login:10m rate=1r/s;
```

This creates a shared memory zone called “login” to store a log of IP addresses that access the rate limited urls. The space reserved, 10 MB (10m) will give us enough space to store a history of 160k requests. We have chosen to allow only allow one request per second (1r/s).

Next we apply the zone to certain routes, like a hypothetical stored procedure called `login`.

```
location /rpc/login/ {
    # apply rate limiting
    limit_req zone=login burst=5;
}
```
The burst argument tells Nginx to start dropping requests if more than five queue up from a specific IP.

Nginx rate limiting is general and indiscriminate. To rate limit each authenticated request individually you will need to add logic in a Custom Validation function.

### 9.8.5 Using External Connection Poolers

PostgREST manages its own pool of connections and uses prepared statements by default in order to increase performance. However, this setting is incompatible with external connection poolers such as PgBouncer working in transaction pooling mode. In this case, you need to set the `db-prepared-statements` config option to false. On the other hand, session pooling is fully compatible with PostgREST, while statement pooling is not compatible at all.

**Note:** If prepared statements are enabled, PostgREST will quit after detecting that transaction or statement pooling is being used.

You should also set the `db-channel-enabled` config option to false, due to the LISTEN command not being compatible with transaction pooling, although it should not give any errors if it’s left enabled by default.

### 9.9 Debugging

#### 9.9.1 Server Version

When debugging a problem it’s important to verify the PostgREST version. At any time you can make a request to the running server and determine exactly which version is deployed. Look for the Server HTTP response header, which contains the version number.

#### 9.9.2 Logging

PostgREST logs basic request information to stdout, including the requesting IP address and user agent, the URL requested, and HTTP response status.

```text
127.0.0.1 - - [26/Jul/2021:01:56:38 -0500] "GET /clients HTTP/1.1" 200 - "" "curl/7.64.0"
127.0.0.1 - - [26/Jul/2021:01:56:48 -0500] "GET /unexistent HTTP/1.1" 404 - "" "curl/7.64.0"
```

For diagnostic information about the server itself, PostgREST logs to stderr.

```text
12/Jul/2021:17:47:39 -0500: Attempting to connect to the database...
```

**Note:** When running it in an SSH session you must detach it from stdout or it will be terminated when the session closes. The easiest technique is redirecting the output to a log file or to the syslog:
ssh foo@example.com \
  'postgrest foo.conf </dev/null >/var/log/postgrest.log 2>&1 &' 

PostgREST logging provides limited information for debugging server errors. It’s helpful to get full information about both client requests and the corresponding SQL commands executed against the underlying database.

### 9.9.3 HTTP Requests

A great way to inspect incoming HTTP requests including headers and query parameters is to sniff the network traffic on the port where PostgREST is running. For instance on a development server bound to port 3000 on localhost, run this:

```
# sudo access is necessary for watching the network
sudo ngrep -d lo0 port 3000
```

The options to ngrep vary depending on the address and host on which you’ve bound the server. The binding is described in the *Configuration* section. The ngrep output isn’t particularly pretty, but it’s legible.

### 9.9.4 Database Logs

Once you’ve verified that requests are as you expect, you can get more information about the server operations by watching the database logs. By default PostgreSQL does not keep these logs, so you’ll need to make the configuration changes below. Find *postgresql.conf* inside your PostgreSQL data directory (to find that, issue the command `show data_directory;`). Either find the settings scattered throughout the file and change them to the following values, or append this block of code to the end of the configuration file.

```
# send logs where the collector can access them
log_destination = "stderr"

# collect stderr output to log files
logging_collector = on

# save logs in pg_log/ under the pg data directory
log_directory = "pg_log"

# (optional) new log file per day
log_filename = "postgresql-%Y-%m-%d.log"

# log every kind of SQL statement
log_statement = "all"
```

Restart the database and watch the log file in real-time to understand how HTTP requests are being translated into SQL commands.

**Note:** On Docker you can enable the logs by using a custom init.sh:

```
#!/bin/sh
echo "log_statement = 'all'" >> /var/lib/postgresql/data/postgresql.conf
```

After that you can start the container and check the logs with `docker logs`. 
docker run -v "$(pwd)/init.sh":"/docker-entrypoint-initdb.d/init.sh" -d postgres
docker logs -f <container-id>

9.9.5 Schema Reloading

Changing the schema while the server is running can lead to errors due to a stale schema cache. To learn how to refresh the cache see *Schema Cache Reloading*.

9.10 Daemonizing

For Linux distributions that use *systemd* (Ubuntu, Debian, Archlinux) you can create a daemon in the following way.

First, create postgrest configuration in `/etc/postgrest/config`

```plaintext
db-uri = "postgres://<your_user>:<your_password>@localhost:5432/<your_db>"
db-schema = "<your_exposed_schema>"
db-anon-role = "<your_anon_role>"
db-pool = 10
server-host = "127.0.0.1"
server-port = 3000
jwt-secret = "<your_secret>"
```

Then create the systemd service file in `/etc/systemd/system/postgrest.service`

```plaintext
[Unit]
Description=REST API for any PostgreSQL database
After=postgresql.service

[Service]
ExecStart=/bin/postgrest /etc/postgrest/config
ExecReload=/bin/kill -SIGUSR1 $MAINPID

[Install]
WantedBy=multi-user.target
```

After that, you can enable the service at boot time and start it with:

```bash
systemctl enable postgrest
systemctl start postgrest
```

```bash
## For reloading the service
# systemctl restart postgrest

9.11 Alternate URL Structure

As discussed in *Singular or Plural*, there are no special URL forms for singular resources in PostgREST, only operators for filtering. Thus there are no URLs like `/people/1`. It would be specified instead as
This allows compound primary keys and makes the intent for singular response independent of a URL convention. Nginx rewrite rules allow you to simulate the familiar URL convention. The following example adds a rewrite rule for all table endpoints, but you’ll want to restrict it to those tables that have a numeric simple primary key named “id.”

```bash
# support /endpoint/:id url style
location ~ ^/([a-z_]+)/([0-9]+) {
    # make the response singular
    proxy_set_header Accept 'application/vnd.pgrst.object+json';
    # assuming an upstream named "postgrest"
    proxy_pass http://postgrest/$1?id=eq.$2;
}
```

### 9.12 Installation

The release page has pre-compiled binaries for Mac OS X, Windows, Linux and FreeBSD. The Linux binary is a static executable that can be run on any Linux distribution.

If you use **macOS Homebrew**, then you can install PostgREST from the official repo.

```bash
brew install postgrest
```

If you use **FreeBSD**, then you can install PostgREST from the official ports.

```bash
pkg install hs-postgrest
```

If you use **Arch Linux**, then you can install PostgREST from the community repo.

```bash
pacman -S postgrest
```

If you use **Nix**, then you can install PostgREST from nixpkgs.

```bash
nix-env -i haskellPackages.postgrest
```

If you use Windows, you can install PostgREST using **Chocolatey** or **Scoop**.

```bash
choco install postgrest
scoop install postgrest
```

### 9.13 Running PostgREST

If you downloaded PostgREST from the release page, first extract the compressed file to obtain the executable.

```bash
# For UNIX platforms
tar Jxf postgrest-{version}-{platform}.tar.xz

# On Windows you should unzip the file
```
Now you can run PostgREST with the `--help` flag to see usage instructions:

```
# Running postgrest binary
./postgrest --help

# Running postgrest installed from a package manager
postgrest --help

# You should see a usage help message
```

The PostgREST server reads a configuration file as its only argument:

```
postgrest /path/to/postgrest.conf

# You can also generate a sample config file with
# postgrest 2> postgrest.conf
# You'll need to edit this file and remove the usage parts for postgrest to read it
```

For a complete reference of the configuration file, see `Configuration`.

**Note:** If you see a dialog box like this on Windows, it may be that the `pg_config` program is not in your system path.

It usually lives in `C:\Program Files\PostgreSQL\<version>\bin`. See this article about how to modify the system path.

To test that the system path is set correctly, run `pg_config` from the command line. You should see it output a list of paths.

### 9.13.1 PostgreSQL dependency

To use PostgREST you will need an underlying database. We require PostgreSQL 9.5 or greater. You can use something like Amazon RDS but installing your own locally is cheaper and more convenient for development. You can also run PostgreSQL in a **docker container**.

### 9.14 Docker

You can get the official PostgREST Docker image with:

```
docker pull postgrest/postgrest
```

To configure the container image, use `Environment Variables`.

There are two ways to run the PostgREST container: with an existing external database, or through docker-compose.
9.14.1 Containerized PostgREST with native PostgreSQL

The first way to run PostgREST in Docker is to connect it to an existing native database on the host.

```bash
# Run the server
docker run --rm --net=host -p 3000:3000 \
   -e PGRST_DB_URI="postgres://postgres@localhost/postgres" \
   -e PGRST_DB_SCHEMA="public" \
   -e PGRST_DB_ANON_ROLE="postgres" \
postgrest/postgrest
```

The database connection string above is just an example. Adjust the role and password as necessary. You may need to edit PostgreSQL's `pg_hba.conf` to grant the user local login access.

**Note:** Docker on Mac does not support the `--net=host` flag. Instead you'll need to create an IP address alias to the host. Requests for the IP address from inside the container are unable to resolve and fall back to resolution by the host.

```bash
sudo ifconfig lo0 10.0.0.10 alias
```

You should then use 10.0.0.10 as the host in your database connection string. Also remember to include the IP address in the `listen_addresses` within `postgresql.conf`. For instance:

```
listen_addresses = 'localhost,10.0.0.10'
```

You might also need to add a new IPv4 local connection within `pg_hba.conf`. For instance:

```
host all all 10.0.0.10/32 trust
```

9.14.2 Containerized PostgREST and db with docker-compose

To avoid having to install the database at all, you can run both it and the server in containers and link them together with docker-compose. Use this configuration:

```yaml
# docker-compose.yml
version: '3'
services:
  server:
    image: postgrest/postgrest
    ports:
      - "3000:3000"
    environment:
      PGRST_DB_URI: postgres://app_user:password@db:5432/app_db
      PGRST_DB_SCHEMA: public
      PGRST_DB_ANON_ROLE: app_user #In production this role should not be the same as the one used for the connection
      PGRST_OPENAPI_SERVER_PROXY_URI: http://127.0.0.1:3000
    depends_on:
      - db
  db:
    image: postgres
    ports:
      - "5432:5432"
```

(continues on next page)
Go into the directory where you saved this file and run `docker-compose up`. You will see the logs of both the database and PostgREST, and be able to access the latter on port 3000.

If you want to have a visual overview of your API in your browser you can add `swagger-ui` to your `docker-compose.yml`:

```yaml
swagger:
  image: swaggerapi/swagger-ui
  ports:
    - "8080:8080"
  expose:
    - "8080"
  environment:
    API_URL: http://localhost:3000/
```

With this you can see the swagger-ui in your browser on port 8080.

### 9.15 Building from Source

When a pre-built binary does not exist for your system you can build the project from source.

**Note:** We discourage building and using PostgREST on **Alpine Linux** because of a reported GHC memory leak on that platform.

You can build PostgREST from source with Stack. It will install any necessary Haskell dependencies on your system.

- Install Stack for your platform
- Install Library Dependencies

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ubuntu/Debian</td>
<td>libpq-dev, libgmp-dev, zlib1g-dev</td>
</tr>
<tr>
<td>CentOS/Fedora/Red Hat</td>
<td>postgresql-devel, zlib-devel, gmp-devel</td>
</tr>
<tr>
<td>BSD</td>
<td>postgresql12-client</td>
</tr>
<tr>
<td>OS X</td>
<td>libpq, gmp</td>
</tr>
</tbody>
</table>

- Build and install binary

```bash
git clone https://github.com/PostgREST/postgrest.git
cd postgrest

# adjust local-bin-path to taste
stack build --install-ghc --copy-bins --local-bin-path /usr/local/bin
```
Note:

- If building fails and your system has less than 1GB of memory, try adding a swap file.
- `--install-ghc` flag is only needed for the first build and can be omitted in the subsequent builds.
- Check that the server is installed: `postgrest --help`.

### 9.16 Deploying to Heroku

Assuming you’re making modifications locally and then pushing to GitHub, it’s easy to deploy to Heroku.

1. Create a new app on Heroku
2. In Settings add the following buildpack [https://github.com/PostgREST/postgrest-heroku](https://github.com/PostgREST/postgrest-heroku)
3. Add the require Config Vars in Heroku
4. Modify your `postgrest.conf` file as required to match your Config Vars in Heroku
5. Create your `Procfile` and add `./env-to-config ./postgrest postgrest.conf`
6. Push your changes to GitHub
7. Set Heroku to automatically deploy from Main and then manually deploy the branch for the first build

- **Authentication**
- **Schema Structure**
- **Administration**
- **Installation**
How-to guides

These are recipes that’ll help you address specific use-cases.

10.1 Casting a type to a custom JSON object

author steve-chavez

While using PostgREST you might have noticed that certain PostgreSQL types translate to JSON strings when you would have expected a JSON object or array. For example, let’s see the case of range types.

```
-- example taken from https://www.postgresql.org/docs/current/rangetypes.html
create table reservations (  
    room int,
    during tsrange
);

insert into reservations
values
    (1108, tsrange('2010-01-01 14:30', '2010-01-01 15:30'));
```

Here we have a column named during as a tsrange type, we would like to get it as JSON through PostgREST.

```
curl "http://localhost:3000/reservations"
```

Result:

```json
[
  {
    "room": 1108,
    "during": "[2010-01-01 14:30:00", "2010-01-01 15:30:00"]"
  }
]
```
The *during* value is probably not the in the format you want. We get a JSON string because by default PostgreSQL casts the type to JSON by using its text representation. We can change this representation to a custom JSON object by creating a CAST.

To do this, first we’ll define the function that will do the conversion from `tsrange` to `json`.

```sql
create or replace function tsrange_to_json(tsrange) returns json as $$
select json_build_object(
   'lower', lower($1)
   , 'upper', upper($1)
   , 'lower_inc', lower_inc($1)
   , 'upper_inc', upper_inc($1)
);
$$ language sql;
```

Using this function we’ll create the CAST.

```sql
create cast (tsrange as json) with function tsrange_to_json(tsrange) as assignment;
```

And we’ll do the request and *cast the column*.

```bash
curl "http://localhost:3000/reservations?select=room,during::json"
```

The result now is:

```json
[{
   "room" : 1108,
   "during":{
      "lower" : "2010-01-01T14:30:00",
      "upper" : "2010-01-01T15:30:00",
      "lower_inc": true,
      "upper_inc": false
   }
}]
```

You can use the same idea for creating custom casts for different types.

**Note:** If you don’t want to modify casts for built-in types, an option would be to create a custom type for your own `tsrange` and add its own cast.

```sql
create type mytsrange as range (subtype = timestamp, subtype_diff = tsrange_subdiff);
-- define column types and casting function analogously to the above example
-- ...
create cast (mytsrange as json) with function mytsrange_to_json(mytsrange) as assignment;
```

## 10.2 Embedding a table from another schema

**author** steve-chavez

Suppose you have a *people* table in the public schema and this schema is exposed through PostgREST’s `db-schema`.
create table public.people(
  id int primary key,
  full_name text
);

And you want to embed the **people** table with a **details** table that’s in another schema named **private**.

```sql
create schema if not exists private;

-- For simplicity’s sake the table is devoid of constraints/domains on email, phone, etc.
create table private.details(
  id int primary key references public.people,
  email text,
  phone text,
  birthday date,
  occupation text,
  company text
);

-- other database objects in this schema
-- ...
-- ...
```

To solve this, you can create a view of **details** in the **public** schema. We’ll call it **public_details**.

```sql
create view public.public_details as
select id, occupation, company
from private.details;
```

Since PostgREST supports **Embedding Views**, you can embed **people** with **public_details**.

Let’s insert some data to test this:

```sql
insert into public.people values (1, 'John Doe'), (2, 'Jane Doe');
insert into private.details values (1, 'jhon@fake.com', '772-323-5433', '1990-02-01', 'Transportation attendant', 'Body Fate'), (2, 'jane@fake.com', '480-474-6571', '1980-04-21', 'Geotechnical engineer', 'Earthworks Garden Kare');
```

**Important:** Make sure PostgREST’s schema cache is up-to-date. See **Schema Cache Reloading**.

Now, make the following request:
curl "http://localhost:3000/people?select=full_name,public_details(occupation,company)"

The result should be:

```
[{
  "full_name": "John Doe",
  "public_details": [
    {
      "occupation": "Transportation attendant",
      "company": "Body Fate"
    }
  ]
}, {
  "full_name": "Jane Doe",
  "public_details": [
    {
      "occupation": "Geotechnical engineer",
      "company": "Earthworks Garden Kare"
    }
  ]
}]
```

## 10.3 Providing images for `<img>`

**author** pkel

In this how-to, you will learn how to create an endpoint for providing images to HTML `<img>` tags without client side JavaScript. The resulting HTML might look like this:

```
<img src="http://host/files/42/cats.jpeg" alt="Cute Kittens"/>
```

In fact, the presented technique is suitable for providing not only images, but arbitrary files.

We will start with a minimal example that highlights the general concept. Afterwards we present are more detailed solution that fixes a few shortcomings of the first approach.

### 10.3.1 Minimal Example

PostgREST returns binary data on requests that set the `Accept: application/octet-stream` header. The general idea is to configure the reverse proxy in front of the API to set this header for all requests to `/files/`. We will show how to achieve this using Nginx.

First, we need a public table for storing the files.

```sql
create table files(
  id int primary key,
  blob bytea
);
```

Let’s assume this table contains an image of two cute kittens with id 42. We can retrieve this image in binary format from our PostgREST API by requesting `/files?select=blob&id=eq.42` with the `Accept: application/octet-stream` header. Unfortunately, putting the URL into the `src` of an `<img>` tag will not work. That’s because browsers do not send the required header.

Luckily, we can configure our *Nginx reverse proxy* to fix this problem for us. We assume that PostgREST is running on port 3000. We provide a new location `/files/` that redirects requests to our endpoint with the `Accept` header set to `application/octet-stream`.

```nginx
server {
  # rest of reverse proxy and web server configuration
...

  location /files/ {
    # /files/<id>/* ---> /files?select=blob&id=eq.<id>
```
With this setup, we can request the cat image at `localhost/files/42/cats.jpeg` without setting any headers. In fact, you can replace `cats.jpeg` with any other filename or simply omit it. Putting the URL into the `src` of an `<img>` tag should now work as expected.

### 10.3.2 Improved Version

The basic solution has some shortcomings:

1. The response `Content-Type` header is set to `application/octet-stream`. This might confuse clients and users.
2. Download requests (e.g. Right Click -> Save Image As) to `files/42` will propose `42` as filename. This might confuse users.
3. Requests to the binary endpoint are not cached. This will cause unnecessary load on the database.

The following improved version addresses these problems. First, we store the media types and names of our files in the database:

```sql
create table files(
  id int primary key,
  type text,
  name text,
  blob bytea
);
```

Next, we set up an RPC endpoint that sets the content type and filename. We use this opportunity to configure some basic, client-side caching. For production, you probably want to configure additional caches, e.g. on the reverse proxy.

```sql
create function file(id int) returns bytea as $$
declare headers text;
declare blob bytea;
begin
  select format(
    '[{"Content-Type": "%s"},
    "{"Content-Disposition": "inline; filename="%s"}",
    "{Cache-Control": "max-age=259200"}]'
  , files.type, files.name)
  from files where files.id = file.id into headers;
  perform set_config('response.headers', headers, true);
  select files.blob from files where files.id = file.id into blob;
  if found
```

(continues on next page)
With this, we can obtain the cat image from /rpc/file?id=42. Consequently, we have to replace our previous rewrite rule in the Nginx recipe with the following.

```bash
rewrite /files/([^/]+).*/rpc/file?id=$1 break;
```

- **Casting a type to a custom JSON object**
- **Embedding a table from another schema**
- **Providing images for `<img>`**
- **How PostgreSQL triggers work when called with a PostgREST PATCH HTTP request**
PostgREST has a growing ecosystem of examples, libraries, and experiments. Here is a selection.

## 11.1 Community Tutorials

- **Building a Contacts List with PostgREST and Vue.js** - In this video series, DigitalOcean shows how to build and deploy an Nginx + PostgREST(using a managed PostgreSQL database) + Vue.js webapp in an Ubuntu server droplet.
- **PostgREST + Auth0: Create REST API in mintutes, and add social login using Auth0** - A step-by-step tutorial to show how to dockerize and integrate Auth0 to PostgREST service.
- **PostgREST + PostGIS API tutorial in 5 minutes** - In this tutorial, GIS•OPS shows how to perform PostGIS calculations through PostgREST *Stored Procedures* interface.

## 11.2 Example Apps

- **chronicle** - tracking a tree of personal memories
- **cloudgov-demo-postgrest** - demo for a federally-compliant REST API on cloud.gov
- **code-du-travail-backoffice** - data administration portal for the official French Labor Code and Agreements
- **compose-postgrest** - docker-compose setup with Nginx and HTML example
- **delibrium-postgrest** - example school API and front-end in Vue.js
- **elm-workshop** - building a simple database query UI
- **ember-postgrest-dynamic-ui** - generating Ember forms to edit data
- **ETH-transactions-storage** - indexer for Ethereum to get transaction list by ETH address
• ext-postgrest-crud - browser-based spreadsheet
• general - example auth back-end
• goodfilm - example film API
• guild-operators - example queries and functions that the Cardano Community uses for their Guild Operators’ Repository
• handsontable-postgrest - an excel-like database table editor
• heritage-near-me - Elm and PostgREST with PostGIS
• ng-admin-postgrest - automatic database admin panel
• pgrst-dev-setup - docker-compose and tmuxp setup for experimentation.
• postgres-postgrest-cloudflared-example - docker-compose setup exposing PostgREST using cloudfared
• postgrest-demo - multi-tenant logging system
• postgrest-example - sqitch versioning for API
• postgrest-sessions-example - example for cookie-based sessions
• postgrest-translation-proxy - calling to external translation service
• postgrest-ui - ClojureScript UI components for PostgREST
• postgrest-vercel - run PostgREST on Vercel (Serverless/AWS Lambda)
• PostgresSkeleton - Docker Compose, PostgREST, Nginx and Auth0
• PostGUI - React Material UI admin panel
• prospector - data warehouse and visualization platform
• svelte-postgrest-template - Svelte/SvelteKit, PostgREST, EveryLayout and social auth

11.3 DevOps

• jbkarle/postgrest - helm chart with a demo database for development and test purposes
• cloudstark/helm-charts - helm chart to deploy PostgREST to a Kubernetes cluster via a Deployment and Service

11.4 External Notification

These are PostgreSQL bridges that propagate LISTEN/NOTIFY to external queues for further processing. This allows stored procedures to initiate actions outside the database such as sending emails.

• pg-bridge - Amazon SNS
• pg-kinesis-bridge - Amazon Kinesis
• pg-notify-webhook - trigger webhooks from PostgreSQL’s LISTEN/NOTIFY
• pgsql-listen-exchange - RabbitMQ
• postgres-websockets - expose web sockets for PostgreSQL’s LISTEN/NOTIFY
• postgresql-to-amqp - AMQP
• postgresql2websocket - Websockets
• skeeter - ZeroMQ

11.5 Extensions

• aiodata - Python, event-based proxy and caching client.
• pg-safeupdate - prevent full-table updates or deletes
• postgrest-auth (criles25) - email based auth/signup
• postgrest-auth (svmotn) - OAuth2-inspired external auth server
• postgrest-node - Run a PostgREST server in Node.js via npm module
• postgrest-oauth - OAuth2 WAI middleware
• postgrest-oauth/api - OAuth2 server
• PostgREST-writeAPI - generate nginx rewrite rules to fit an OpenAPI spec
• spas - allow file uploads and basic auth

11.6 Client-Side Libraries

• aor-postgrest-client - JS, admin-on-rest
• elm-postgrest - Elm
• general-angular - TypeScript, generate UI from API description
• jarvus-postgrest-apikit - JS, Sencha framework
• mithril-postgrest - JS, Mithril
• ng-postgrest - Angular app for browsing, editing data exposed over PostgREST.
• postgrest-client - JS
• postgrest-csharp - C#
• postgrest-dart - Dart
• postgrest-ex - Elixir
• postgrest-go - Go
• postgrest-js - TypeScript/JavaScript
• postgrest-kt - Kotlin
• postgrest-py - Python
• postgrest-request - JS, SuperAgent
• postgrest-rs - Rust
• postgrest-sharp-client (needs maintainer) - C#, RestSharp
• postgrest-swift - Swift
• postgrest-url - JS, just for generating query URLs
• postgrest_python_requests_client - Python
• postgrester - JS + Typescript
- postgrestR - R
- py-postgres - Python
- redux-postgres - TypeScript/JS, client integrated with (React) Redux.
- vue-postgres - Vue.js
- Example Apps
- External Notification
- Extensions
- Client-Side Libraries
Release Notes

Here we’ll include the most relevant changes so you can migrate to newer versions easily. You can see the full changelog of each release in the PostgREST repository.

- v8.0.0
- v7.0.0
- v6.0.2
- v5.2.0
Here are some companies that use PostgREST in production.

- Catarse
- Datrium
- Drip Depot
- eGull
- Image-charts
- Moat
- MotionDynamic - Fast highly dynamic video generation at scale
- Netwo
- Nimbus - See how Nimbus uses PostgREST in Paul Copplestone’s blog post.
- OpenBooking
- Redsmin
- Sompani
- Supabase
“It’s so fast to develop, it feels like cheating!”

—François-Guillaume Ribreau

“I just have to say that, the CPU/Memory usage compared to our Node.js/Waterline ORM based API is ridiculous. It’s hard to even push it over 60/70 MB while our current API constantly hits 1GB running on 6 instances (dynos).”

—Louis Brauer

“I really enjoyed the fact that all of a sudden I was writing microservices in SQL DDL (and v8 JavaScript functions). I dodged so much boilerplate. The next thing I knew, we pulled out a full rewrite of a Spring+MySQL legacy app in 6 months. Literally 10x faster, and code was super concise. The old one took 3 years and a team of 4 people to develop.”

—Simone Scarduzio

“I like the fact that PostgREST does one thing, and one thing well. While PostgREST takes care of bridging the gap between our HTTP server and PostgreSQL database, we can focus on the development of our API in a single language: SQL. This puts the database in the center of our architecture, and pushed us to improve our skills in SQL programming and database design.”

—Eric Bréchemier, Data Engineer, eGull SAS

“PostgREST is performant, stable, and transparent. It allows us to bootstrap projects really fast, and to focus on our data and application instead of building out the ORM layer. In our k8s cluster, we run a few pods per schema we want exposed, and we scale up/down depending on demand. Couldn’t be happier.”

—Anupam Garg, Datrium, Inc.
Please see the Contributing guidelines in the main PostgREST repository.