Name

pg_integrity_check — calculate and validate checksums for controlled files

Synopsis

pg_integrity_check [*connection-option*...] [-s | --system] [-u | --user] [-c | --catalog]
[-o | --output] [-D *datadir*] [-f] [-? | --help]

Description

pg_integrity_check is a utility provided with that can calculate and validate checksums for the objects you would like to control. When running pg_integrity_check, you must specify at least one of the options that define the type of the controlled objects: -s, -u, or -c for read-only files, additional files, or system catalog tables, respectively.

If you use the -o option, pg_integrity_check calculates the checksums and writes them into configuration files under the share/security/ directory. You must have write access to the corresponding files to perform this command. You cannot use the -o option together with the -s option, since the checksum for read-only files cannot be overwritten.

If you omit the -o option, pg_integrity_check compares the calculated checksums with the corresponding checksums in the configuration files. If the checksums differ for any of the controlled objects, pg_integrity_check displays a message indicating the difference.

For details on using pg_integrity_check, see Section 32.2, "Integrity Checks".

Options

connection-option

> Standard options for connecting to a database (d/h/p/U). For details, see psql.

-s
--system

> Validate checksums for read-only files.

-u
--user

> Validate checksums for additional files.

-c
--catalog

> Validate checksums for system catalog tables. For the -c option to work correctly, you must also specify connection parameters for the database. The database server must be started and accept connections.

-o
--output

> Write the checksum into a file.

-D *datadir*

> Data directory of the database cluster. By default, the value is taken from the PGDATA environment variable. This option is required to define the filenames for the generated configuration files when using -u or -c options.

`-f`

> When the `-f` option is specified, `pg_integrity_check` utility reads the configuration file `share/security/pg_integrity_check.conf` and chooses a validation mode that corresponds to the parameters specified in `pg_integrity_check.conf`. This mode can only be used at the server startup. Do not use this option when running `pg_integrity_check` manually.

`-?`
`--help`

> Print command-line help.

Return Values

0 — checksums are calculated successfully.

1 — an error occurred during the initial checksum calculation for read-only files.

2 — checksum validation revealed changes in one or more of the controlled objects.

3 — an unexpected error occurred during checksum validation.

Examples

`pg_integrity_check -s -u -c -U postgres`

Check integrity of all controlled objects using the `postgres` user to connect to the database. For other connection parameters, default values are used.

`pg_integrity_check -u -o -D /usr/local/pgsql/data`

Compute checksums for additional files and write them into the `share/security/_usr_local_pgsql_data.user.conf` configuration file.