

Audit Report

Solution: postgresSQL
Auditor: hafsa akzoun
Date: 2025-06-24 01:26:07

| Rule | Result | Current Value | Expected Value |
|---|--------|---|------------------|
| Control 3.1.13 Ensure the program name for PostgreSQL syslog messages is correct (Automated): | PASS | syslog_ident is set to postgres | |
| Control 3.1.14 Ensure the correct messages are written to the server log: | PASS | log_min_messages is set to warning | |
| Control 3.1.15 Ensure the correct SQL statements generating errors are recorded (Automated): | PASS | log_min_error_statement is set to error | |
| Control 3.1.16 Ensure 'debug_print_parse' is disabled: | PASS | debug_print_parse is set to off | |
| Control 3.1.17 Ensure 'debug_print_rewritten' is disabled (Automated): | PASS | debug_print_rewritten is set to off | |
| Control 3.1.19 Ensure 'debug_pretty_print' is enabled (Automated): | PASS | debug_print_plan is set to off | |
| Control 3.1.19 Ensure 'debug_pretty_print' is enabled (Automated): | PASS | debug_pretty_print is enabled | |
| Control 3.1.20 Ensure 'log_connections' is enabled: | FAIL | log_connections is off | on |
| Control 3.1.21 Ensure 'log_disconnections' is enabled (Automated): | FAIL | log_disconnections is off | on |
| Control 3.1.22 Ensure 'log_error_verbosity' is set correctly: | FAIL | log_error_verbosity is set to default | "verbose" |
| Control 3.1.23 Ensure 'log_hostname' is set correctly (Automated): | PASS | log_hostname is set to off | |
| Control 3.1.24 Ensure 'log_line_prefix' is set correctly (Automated): | PASS | log_line_prefix contains %m [%p] | |
| Control 3.1.25 Ensure 'log_statement' is set correctly (Automated): | FAIL | log_statement is set to none | ddl, mod, or all |

| Rule | Result | Current Value | Expected Value |
|---|--------|---|--|
| Control 3.1.26 Ensure 'log_timezone' is set correctly (Automated): | FAIL | log_timezone is set to Etc/GMT0 | UTC (or organization-defined equivalent) |
| Control 3.2 Ensure the PostgreSQL Audit Extension (pgAudit) is enabled (Automated): | FAIL | pgaudit is NOT included in shared_preload_libraries (). | |
| Control 3.2 Ensure the PostgreSQL Audit Extension (pgAudit) is enabled (Automated): | FAIL | pgaudit.log is empty or not properly configured. | |
| Control 4.2 Ensure excessive administrative privileges are revoked (Manual): | PASS | Role "pg_database_owner" does not have elevated privileges. | |
| Control 4.2 Ensure excessive administrative privileges are revoked (Manual): | PASS | Role "pg_read_all_data" does not have elevated privileges. | |
| Control 4.2 Ensure excessive administrative privileges are revoked (Manual): | PASS | Role "pg_write_all_data" does not have elevated privileges. | |
| Control 4.2 Ensure excessive administrative privileges are revoked (Manual): | PASS | Role "pg_monitor" does not have elevated privileges. | |
| Control 4.2 Ensure excessive administrative privileges are revoked (Manual): | PASS | Role "pg_read_all_settings" does not have elevated privileges. | |
| Control 4.2 Ensure excessive administrative privileges are revoked (Manual): | PASS | Role "pg_read_all_stats" does not have elevated privileges. | |
| Control 4.2 Ensure excessive administrative privileges are revoked (Manual): | PASS | Role "pg_stat_scan_tables" does not have elevated privileges. | |
| Control 4.2 Ensure excessive administrative privileges are revoked (Manual): | PASS | Role "pg_read_server_files" does not have elevated privileges. | |
| Control 4.2 Ensure excessive administrative privileges are revoked (Manual): | PASS | Role "pg_write_server_files" does not have elevated privileges. | |
| Control 4.2 Ensure excessive administrative privileges are revoked (Manual): | PASS | Role "pg_execute_server_program" does not have elevated privileges. | |
| Control 4.2 Ensure excessive administrative privileges are revoked (Manual): | PASS | Role "pg_signal_backend" does not have elevated privileges. | |
| Control 4.2 Ensure excessive administrative privileges are revoked (Manual): | PASS | Role "pg_checkpoint" does not have elevated privileges. | |
| Control 4.2 Ensure excessive administrative privileges are revoked (Manual): | PASS | Role "pg_use_reserved_connections" does not have elevated privileges. | |

| Rule | Result | Current Value | Expected Value |
|---|--------|--|----------------|
| Control 4.2 Ensure excessive administrative privileges are revoked (Manual): | PASS | Role "pg_create_subscription" does not have elevated privileges. | |
| Control 4.3 Ensure excessive function privileges are revoked (Automated): | PASS | No unauthorized SECURITY DEFINER functions found. | |
| Control 6.2 Ensure 'backend' runtime parameters are configured correctly (Automated): | FAIL | log_connections is off | "on" |
| Control 6.2 Ensure 'backend' runtime parameters are configured correctly (Automated): | FAIL | log_disconnections is off | "on" |
| Control 6.2 Ensure 'backend' runtime parameters are configured correctly (Automated): | PASS | All backend runtime parameters are correctly set | |
| Control 6.8 Ensure TLS is enabled and configured correctly: | FAIL | TLS/SSL is not enabled (ssl = off) | |
| Control 6.8 Ensure TLS is enabled and configured correctly: | PASS | TLS/SSL is enabled and certificate/key are configured properly | |
| Control 6.9 Ensure the pgcrypto extension is installed and configured correctly (Manual): | FAIL | pgcrypto extension is not installed or available in the cluster | |
| Control 7.1 Ensure a replication-only user is created and used for streaming replication: | FAIL | Only the default "postgres" user has replication privileges. Create a dedicated replication-only user. | |
| Control 7.2 Ensure logging of replication commands is configured (Manual): | FAIL | log_replication_commands is set to off | "on" |
| Control 7.4 Ensure WAL archiving is configured and functional: | FAIL | archive_mode is not set to "on" | |
| Control 7.4 Ensure WAL archiving is configured and functional: | FAIL | No WAL files have been archived yet (archived_count = 0) | |
| Control 8.1 Ensure PostgreSQL subdirectory locations are outside the data cluster (Manual): | FAIL | allow_in_place_tablespace is NOT outside the data cluster (off). | |
| Control 8.1 Ensure PostgreSQL subdirectory locations are outside the data cluster (Manual): | FAIL | data_directory is NOT outside the data cluster (/Library/PostgreSQL/16/data). | |

| Rule | Result | Current Value | Expected Value |
|---|--------|--|----------------|
| Control 8.1 Ensure PostgreSQL subdirectory locations are outside the data cluster (Manual): | FAIL | default_tablespace is NOT outside the data cluster (). | |
| Control 8.1 Ensure PostgreSQL subdirectory locations are outside the data cluster (Manual): | FAIL | log_directory is NOT outside the data cluster (log). | |
| Control 8.1 Ensure PostgreSQL subdirectory locations are outside the data cluster (Manual): | FAIL | temp_tablespaces is NOT outside the data cluster (). | |
| Control 8.1 Ensure PostgreSQL subdirectory locations are outside the data cluster (Manual): | FAIL | 5 setting(s) are still inside the data cluster. | |