Huawei GaussDB Kernel V500R001C20SPC100+V500R001C20HP1015

Security Target

Issue   0.18

Date   2022-06-07

HUAWEI TECHNOLOGIES CO., LTD.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base

Bantian, Longgang

Shenzhen 518129

People's Republic of China

Website: https://e.huawei.com

Contents

1 About This Document

Purpose

This document provides description about Security Target (ST) against PP.

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

Date	Version	Updated Section	Description	Owner
2021-01-31	0.1	All	This is the first draft.	Huawei Technologies Co., Ltd.
2021-03-04	0.2	All	Changed based on internal review results.	Huawei Technologies Co., Ltd.
2021-04-21	0.3	Title & 2.1	Update version matching filename.	Huawei Technologies Co., Ltd.
		2.3.2	Updated description of TOE type in section 2.3.2.	
		4.2.1	Description of the assets removed from section 4.2.1.	
		5.3.1.1	O.ACCESS_HISTORY Removed from the Security Objectives Rationale from section 5.3.1.1.	
		6	FIA_USB_(EXT).2.4 highlighted in bold to mark the new requirements.	
		3 7.5	Fixed the component level of the augmentation ALC_FLR.	
		7.4	Fixed a typo in the mapping of FAU_SEL.1.	
		7.2.2.2	FDP_ACF.1 updated to clarify the security	

Date	Version	Updated Section	Description	Owner
			attributes and the subjects.	
		7.2.3.4	Subjects and initial administrator terms identified in FIA_USB_(EXT).2 have been clarified.	
		8	Chapter name updated.	
		7.3 7.3.1 7.4 8.1.3	Updated references to FIA_UAU and FIA_UID to identify the correct level.	
		8.1.1	Updated description to match FAU_SEL.1.1.	
		8.1.4	Updated the TSS description to match FMT_SMF.1.1.	
2021-05-20	0.4	2.4.2	Update Delivery method	Huawei Technologies Co., Ltd.
2021-06-07	0.5	2.4.2	Update Delivery method	Huawei Technologies Co., Ltd.
2021-06-09	0.6	2.4.2	Separate Table,Update Delivery method	Huawei Technologies Co., Ltd.
2021-06-10	0.7	2.2 2.2.3	Update the TOE Overview, mention the TOE Commercial name and TOE Technical name	Huawei Technologies Co., Ltd.
2021-07-19	0.8	2.3 2.3.3	Remove the PyGreSQL 5.03, add Libpq	Huawei Technologies Co., Ltd.
		2.4.1.1 2.4.1.2	Update Figure 2-1 Single-node server database configuration Update Figure 2-2 One-Primary-Multi-Standby cluster database configuration	Huawei Technologies Co., Ltd.
2021-08-20	0.9	6.2.4 7.2.3.4 8.1.2 8.1.4	Update FIA_USB_(EXT).2.3 Update FPT_TRC.1 Update FDP_RIP.1.1	Huawei Technologies Co., Ltd.
2021-09-15	0.10	8.1.2 5.3.1.1	Update FIA_USB_(EXT).2.3 to match the user guidance. Table 5-5 updated to identify T.IA_MASQUERADE.	Huawei Technologies Co., Ltd.

Date	Version	Updated Section	Description	Owner
2021-09-16	0.11	8.1.2	Updated TSS description for FIA_USB_(EXT).2.3	Huawei Technologies Co., Ltd
2021-10-08	0.12	2.3.2 4.2.1	Updated to address certifier feedback: - Changed term *free* by *discretionary* in section 2.3.2 - Changed *thread* by *threat* in section 4.2.1	Huawei Technologies Co., Ltd
2021-10-25	0.13	2.4.2.2 2.4.4	Updated TOE guidance documents Updated TOE configuration	Huawei Technologies Co., Ltd
2021-11-22	0.14	2.3.3 2.4.1.1 3.1 8.1.1	Added evaluation hardware in table 2-1; Updated figures 2-1 and 2-2; Added PP rationale; Removed log file paths.	Huawei Technologies Co., Ltd
2022-02-14	0.15	2.2 2.4.2.1 2.4.2.2 2.4.4	Add hotpatch information.	Huawei Technologies Co., Ltd
2022-02-28	0.16	2.4.2.2	Update the product guidance documents Version	Huawei Technologies Co., Ltd
2022-04-11	0.17	Title & 2.1 & 2.2 & 2.4.2.2	Update the version and date information	Huawei Technologies Co., Ltd
2022-06-07	0.18	2.4.2.2	Update TOE guidance documents	Huawei Technologies Co., Ltd

2 ST Introduction

2.1 ST Identification

ST title: Huawei GaussDB Kernel V500R001C20SPC100+V500R001C20HP1015 Security Target

Version: 0.18

Date: 2022-06-07

Developer: Huawei Technologies Co., Ltd.

2.2 TOE Identification

Name: Huawei GaussDB(openGauss) Database Management System (DBMS)

Version: V500R001C20SPC100+V500R001C20HP1015

Developer: Huawei Technologies Co., Ltd.

2.3 TOE Overview

The TOE Commercial name is the Huawei GaussDB (openGauss) Database Management System (DBMS). Technical name is Huawei GaussDB Kernel, it is a next-generation enterprise-level relational database developed by Huawei. It supports x86 and Huawei Kunpeng hardware architectures. It provides high-throughput and strong-consistency transaction processing capabilities, financial-level HA capabilities, and high-performance big data query capabilities, and applies to key core systems in industries such as finance, telecom, and government. The database provides the following functions:

- Supports standard SQL

Supports standard SQL92, SQL99, SQL2003 and SQL2011, GBK, UTF-8, SQL ASCII and Latin-1 character sets, SQL standard functions, analytical functions, and SQL Procedural Language.

- Supports APIs

Supports standard JDBC 4.0, ODBC 3.5, Psycopg 2.0 and Libpq.

- Provides database storage management

Supports tablespaces and table partition.

- Provides component management

Supports query the status of each component and primary-standby arbitration.

- Provides high availability (HA) of data nodes

Supports atomicity, consistency, isolation, and durability (ACID) features of database transactions, recovery from single node failure.

- Provides high-performance with big-data query capabilities

Supports column-based storage, vectorized execution engine, symmetric multi-processing, Just-In-Time, and SQL by pass.

2.3.1 TOE Type

The TOE is a DBMS. It provides a relational database engine providing mechanisms for user accesses, identification and authentication, data protection, and security audit. It mainly focuses on online transaction processing scenarios with large data volumes and high concurrency.

This TOE is a software-only TOE.

2.3.2 TOE Usage and Major Security Features

The Target of Evaluation (TOE) described in this ST is a DBMS, which can restrict the access of authorized users to the TOE, implement discretionary access control on objects controlled by the DBMS based on users or roles, and can clarify users' responsibilities by their behavior.

TOE security functions include security audit, user data protection, identity identification and authentication, security management, data backup and restoration, ensuring database security.

2.3.3 Non-TOE Hardware and Software

The following hardware resources are out of scope and thus not included in the TOE but are necessary for its operation:

Server hardware and OS are out of scope and thus not included in the TOE. They provide the required environment for installing and running the TOE.

Manager Network channel is also out of scope and thus not included in the TOE. It is used to monitor the status of each node instance in the cluster and send control information.

Item	Requirement
CPU	Dual-socket 32-core Intel processor or Kunpeng 920 processor
	Both the CPU hyper-threading mode and non-hyper-threading mode are supported. The mode setting must be the same for all the nodes in the cluster.
RAM	The physical memory must be no less than 128 GB.
	Complex queries require high memory. In high concurrency scenarios, the memory may be insufficient. In this case, you are advised to use a

Item	Requirement
	large memory server or use load management to restrict the system concurrency.
Hard disk	The space of the OS disk is greater than or equal to 600 GB, and the space of each non-OS disk is greater than or equal to 600 GB.
Switch	Switch is also out of scope and thus not included in the TOE. It is used to connect node instances in a cluster.
OS	**Evaluation OSs**: EulerOS V2.0SP5, x86_64 **Supported OSs**: • EulerOS V2.0SP8, ARM
Software	The Software of Python v2.7 is out of scope and thus not included in the TOE. The Software of Huawei JDK1.8.0 is out of scope and thus not included in the TOE.
Clients	Clients (including local and remote clients: GSQL, JDBC, ODBC, Psycopg,Libpq) are also out of scope and thus not included in the TOE. They are used to interact with the TOE.
Cluster Manager Components	Cluster Manage Components (including CM Agent, Om Monitor, and CM Server, ETCD) are also out of scope and thus not included in the TOE. They are used to manage and monitor the running status of the TOE, ensure stable running of the TOE.
Operation Manager Server	Operation Manager Server (including gs_ctl, gs_dump, gs_restore, gs_upgrade, gs_redis) are also out of scope and thus not included in the TOE. They offer the operation tools and configuration manage interfaces.
Evaluation Hardware	Servers with dual-socket 32-core Intel processor.

Table 2-1 Non-TOE hardware and software items

2.4 TOE Description

This chapter provides an architectural overview of the Huawei GaussDB Kernel including a detailed description of the software architecture, the definition of the TOE subject to evaluation and a summary of security functions provided by the TOE.

2.4.1 TOE Environment

Huawei GaussDB Kernel supports several deployment modes. Figure 2-1 shows the pure single-node server database configuration, and Figure 2-2 shows the one-primary-multi-standby (like 1 master 2 standby as shown in Figure 2-2) database configuration.

2.4.1.1 Client Server Database Configuration

Figure 2-1 Single-node server database configuration
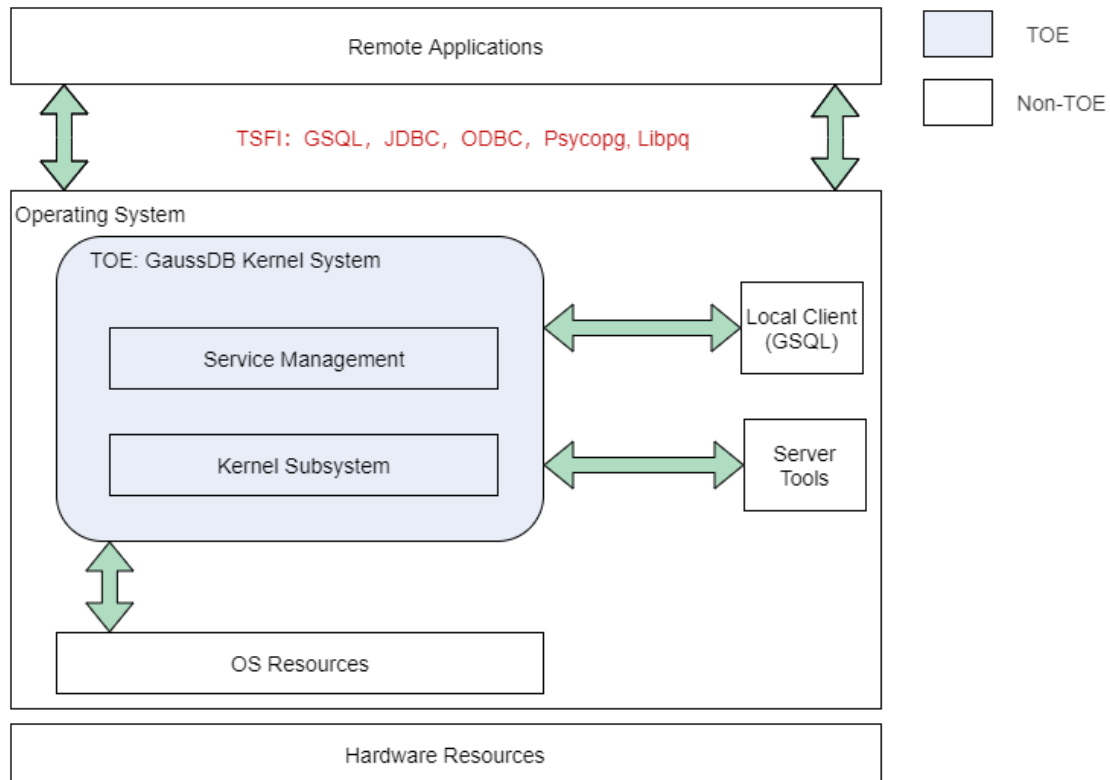
As shown in Figure 2.1, the deployment of single-node database consists of the following units:

- **Remote Applications** (Non-TOE) can access GaussDB Kernel systems through several interfaces, like JDBC, ODBC and so on. They can perform SQL operations by sending queries to GaussDB Kernel server.

- For DBAs, they can log into the backend and management the whole system by using GSQL locally.

- **GaussDB Kernel Server** (TOE) is mainly responsible for processing operation requests sent by different APIs, even Management interface, and returning the data processing results to APIs.

GaussDB Kernel Server provides the mechanism for identification and authorization, only authorized users or roles can access to TOE and perform query statement. The Kernel Subsystem consists of the SQL engine, storage engine. After a query is sent in, the SQL engine parses and compiles the query, checks the permissions to determine whether the current user can access the object that associated with this query, optimize the query, generate and cache the query plan, and run the query statement in the memory, the storage engine is responsibility for physical and logical storage management of the data, make sure the transaction atomicity, consistency, isolation, durability (ACID), flush, and concurrency control.

- **The Operating System** (Non-TOE) hosts the TOE. As the TOE is software only it lives as a process in the Operating System (OS) and uses the resources of the OS like the memory management features.

- **Hardware Resources** (Non-TOE) refers to the hardware resources required for TOE operation, including CPU, memory and hard disk resources. See Table 2-1.

2.4.1.2 One-Primary-Multi-Standby Database Configuration

Figure 2-2 One-Primary-Multi-Standby cluster database configuration
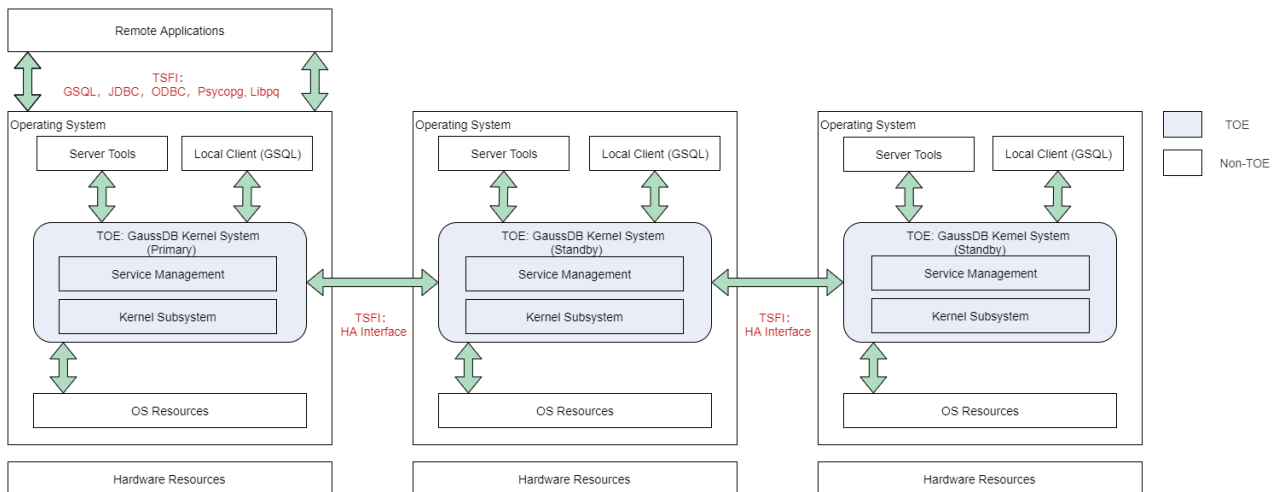
As shown in Figure 2-2, it differs from Figure 2-1 in that three database servers (it can be more) are deployed, which is a highly reliable deployment mode. When the primary server fails, the ETCD is no longer capable for database switchover required O&M engineer manual check choose the new primary node and do switchover, after that, the new primary node can offer service. The primary server can provide database services to Remote SQL Client, it connects the standby server through HA interface, and the content of the primary server will be replicated to standby server, with assurances that the consistency of the data is maintained.

2.4.2 Physical Scope

This TOE is a software-only TOE and physically consists of GaussDB Kernel packages and related guidance documents, as described in the following table. These software packages, signature files, and guidance documents are provided in support web.

2.4.2.1 TOE Binary

The TOE Binary is a database server program named GaussDB in "GaussDB_Kernel_V500R001C20SPC100B003_X86_Centralized_SERVER_PACKAGE.tar.gz" and Hotpatch program named "GaussDB_Kernel_V500R001C20HP1015B001_X86_Centralized.tar.gz"

Table 2-2 TOE Binary

Binary file	SHA256 Value	Version	Delivery method
GaussDB_Kernel_V500R001C20SPC100B003_X86_Centralized_SERVER_PACKAGE.tar.gz	8ac03a263e2d1b71a0483a806a35567cf3147fed2bfcf04a4f30891f237c3041	GaussDB Kernel V500R001C20SPC100	CMC (Huawei Version Management Platform) https://cmc-szv.clouddragon.huawei.com/cmcversion/index/rele

Binary file	SHA256 Value	Version	Delivery method
			aseView?deltaId=410988 9970766080
GaussDB_Kernel_V 500R001C20HP101 5B001_X86_Centra lized.tar.gz	591d5b876d4595f4b592a423 de6e010761208b561f27e645 3096319a304d995a	GaussDB Kernel V500R001C20HP1015	CMC (Huawei Version Management Platform) https://cmc-szv.clouddragon.huawei.c om/cmcversion/index/rele aseView?deltaId=591140 7598109056&isSelect=So ftware&url_data=Centrali zed>Euler2.5_X86_64

2.4.2.2 TOE Guide

The following product guidance documents are provided with the TOE.

Table 2-3 TOE Guide

Document Name	Version	Delivery method
GaussDB Kernel V500R001C20SPC100 Product Documentation	0.4	Delivered by email as electronic document
GaussDB Kernel V500R001C20SPC100 Communication Matrix	3	
HUAWEI GaussDB Kernel V500R001C20SPC100+V500R001C20HP1015 AGD_OPE	0.11	
HUAWEI GaussDB Kernel V500R001C20SPC100+V500R001C20HP1015 AGD_PRE	0.12	

2.4.3 Logical Scope

The TOE logically includes all interfaces and functions within the physical scope. The following table describes the logical scope of the TOE. For details about each function, see 8.1 TOE Security Function.

Table 2-4 TOE logical scope

Function	Description
Security Audit	Audit entries are generated for security related events. Audit policies may be created to generate logs based on details such as the object being accessed, event type or success or failure of the operation. Only privileged user can review these logs. Moreover, the TOE is able to select the set of events to be audited based on the following attributes, like user name, the

Function	Description
	object being accessed, IP address, and so on.
User Data Protection	The TOE provides a discretionary access control policy (RBAC) to provide access control between users and database objects (such as schemas, tables, columns, views, triggers, functions, and procedures) or metadata. It further controls that only authorized administrators are able to manage the TOE.
Identification and Authentication	Identification and identity authentication are performed before users are allowed to access database objects. During login, user identification is associated with the role making access control decisions and the permission information about the user.
Security Management	The security functions associated with audit, access control, and user accounts are provided by the SQL command line interface (like gsql, JDBC) and the parameter configuration tool (gs_guc) on the server. Only authorized administrators are allowed to do these operations, and can be revoked once something wrong happened.
Protection of the TSF	The consistency of replicated TSF data is protected by ensuring the consistency of the replicated TSF data upon reconnection before processing any requests. Data shall be consistently replicated to a secondary DBMS server.
TOE Access	The Session Handling mechanism which limits the possibilities of users to establish sessions with the TOE and maintains a separate execution context for every operation. Also the Memory Management functionality belongs to the area of Session Handling and ensures that any previous information in memory is made unavailable before the memory is used either by overwriting the memory explicitly with a certain pattern or by overwriting the memory completely with new information.

2.4.4 TOE Evaluation Configuration

To configure the evaluation, prepare the following OSs and hardware. Three servers are used in the evaluated configuration.

Table 2-5 Hardware and software requirements for each server

Type	Requirement
TOE	GaussDB_Kernel_V500R001C20SPC100B003_X86_Centralized_SERVER_PACKAGE.tar.gz. GaussDB_Kernel_V500R001C20HP1015B001_X86_Centralized.tar.gz
TOE configuration	Client Server Database Configuration.
CPU	16 cores and 2.0 GHz.
Memory	128GB.
Hard disk	2048GB disk space.
OS type and version	EulerOS Server V2.0SP5 (EulerOS), x86_64
Software	Huawei JDK 1.8.0 Python v2.7 UnixODBC-2.3.7 as an ODBC client

3 Conformance Claims

This Security Target is [CC] Part 2 extended and Part 3 conformant, with a claimed Evaluation Assurance Level of EAL 4, augmented by ALC_FLR.2. The Common Criteria version 3.1 revision 5 has been taken as the basis for this conformance claim.

This Security Target makes a claim of strict conformance on the following Protection Profile.

[DBMSPP]: Protection Profile for Database Management Systems (Base Package), Version 2.12 dated March 23rd, 2017. BSI-CC-PP-0088-V2

This Protection Profile has been evaluated and is listed on the BSI website as a validated protection pro-file (certification ID BSI-CC-PP-0088-V2). See [BSI- PP] for more information.

3.1 PP rationale

This Security Target uses the same Security Problem Definition, Statement of Security Objectives and Statement of Security Functional Requirements as [DBMSPP], including the extended components defined in the PP. The Assurance package required by the PP is augmented to EAL4 + ALC_FLR.2, being this the only addition with respect to the PP for which the Security Target claims conformance.

4 Security Problem Definition

In this section, the security problem definition (SPD) for a DBMS is described. First, the informal discussion of the SPD is presented followed by a more formal description in terms of the identified threats, policies, and assumptions that will be used to identify the specific security requirements addressed by this PP.

4.1 Informal Discussion

Given their common usage as repositories of high value data, attackers routinely target DBMS installations for compromise. Vulnerabilities that attackers may take advantage of are:

- Design flaws and programming bugs in the DBMS and the associated programs and systems, creating various security vulnerabilities (e.g. weak or ineffective access controls) which can lead to data loss/corruption, performance degradation etc.

- Unauthorized or unintended activity or misuse by authorized database users, or network/systems managers, or by unauthorized users or hackers (e.g. inappropriate access to sensitive data, metadata or functions within databases, or inappropriate changes to the database programs, structures or security configurations).

- Malware infections causing incidents such as unauthorized access, leakage or disclosure of personal or proprietary data, deletion of or damage to the data or programs, interruption or denial of authorized access to the database, attacks on other systems and the unanticipated failure of database services.

- Data corruption and/or loss caused by the entry of invalid data or commands, mistakes in database or system administration processes, sabotage/criminal damage etc.

4.2 Assets and Threat Agents

4.2.1 Agents

The following external entities interact with the TOE:

- Administrator: The administrator is authorized to perform the administrative operations and able to use the administrative functions.

- User: A person who wants to use the TOE.

- Threat agent: An attacker is any individual who is attempting to subvert the operation of the TOE. The intention may be to gain unauthorized access to the assets protected by the TOE.

4.3 Threats

The following table identifies the threats to the TOE. These threats have been directly taken from [PP] without any modifications.

Table 4-1 Threats to the TOE

Threat	Definition
T.ACCESS_TSFDATA	A threat agent may read or modify TSF data using functions of the TOE without the proper authorization.
T.ACCESS_TSFFUNC	A threat agent may use or manage TSF, bypassing the protection mechanisms of the TSF.
T.IA_MASQUERADE	A user or a process acting on behalf of a user may masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources.
T.IA_USER	A threat agent may gain access to user data, TSF data, or TOE resources with the exception of public objects without being identified and authenticated.
T.RESIDUAL_DATA	A user or a process acting on behalf of a user may gain unauthorized access to user or TSF data through reallocation of TOE resources from one user or process to another.
T.TSF_COMPROMISE	A user or a process acting on behalf of a user may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or may compromise executable code within the TSF.
T.UNAUTHORIZED_ACCESS	A threat agent may gain unauthorized access to user data for which they are not

Threat	Definition
	authorized according to the TOE security policy.

4.4 Organizational Security Policies

Organizational Security Policies (OSPs) are a set of security rules, procedures, or guidelines imposed by an organization in operational environment. This chapter identifies the organizational security policies applicable to the TOE. These organizational security policies have been taken from [PP] without any changes.

Table 4-2 Organizational Security Policies

Policy	Definition
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ROLES	Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible supporting only the administrative duties the person has. This role shall be separate and distinct from other authorized users.
P.USER	Authority shall only be given to users who are trusted to perform the actions correctly.

4.5 Assumptions

The following table lists all the assumptions about the environment of the TOE. These assumptions have been directly taken from [PP] without any modification.

Table 4-3 Assumptions

Assumption	Description
Physical aspects	
A.PHYSICAL	It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.
Personnel aspects	
A.AUTHUSER	Authorized users possess the necessary

Assumption	Description
	authorization to access at least some of the information managed by the TOE.
A.MANAGE	The TOE security functionality is managed by one or more competent administrators. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.
A.TRAINEDUSER	Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.
Procedural aspects	
A.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration, and support of the DBMS.
A.PEER_FUNC_&_MGT	All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.
A.SUPPORT	Any information provided by a trusted entity in the IT environment and used to support the provision of time and date, information used in audit capture, user authentication, and authorization that is used by the TOE is correct and up to date.
Connectivity aspects	
A.CONNECT	All connections to and from remote trusted IT systems and between separate parts of the TSF are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.

5 Security Objectives

This section identifies the Security Objectives of the TOE and its supporting environment. The security objectives consists of the security objectives for the TOE and the security objectives for the Operational Environment. The security objectives for the TOE and the security objectives for the Operational Environment are copied from the Protection Profile for Database Management Systems (Base Package), Version 2.12 dated March 23rd, 2017, ("DBMS PP").

5.1 TOE Security Objectives

This section identifies and describes the security objectives that are to be addressed by the TOE.

Table 5-1 TOE security objectives

Security Objective	Description
O.ADMIN_ROLE	The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.
O.AUDIT _GENERATION	The TSF must be able to record defined security-relevant events (which usually include security-critical actions of users of the TOE). The information recorded for security-relevant events must contain the time and date the event happened and, if possible, the identification of the user that caused the event, and must be in sufficient detail to help the authorized user detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.
O.DISCRETIONARY _ACCESS	The TSF must control access of subjects and/or users to named resources based on identity of the object, subject, or user. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific

Security Objective	Description
	named object in that access mode.
O.I&A	The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.
O.MANAGE	The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.
O.MEDIATE	The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.
O.RESIDUAL_INFORM ATION	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not inappropriately disclosed when the resource is reallocated.
O.TOE_ACCESS	The TOE will provide functionality that controls a user's logical access to user data and to the TSF.

5.2 Operational Environment Security Objectives

This section identifies and describes the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

5.2.1 Security Objectives of the Operational Environment

The following table describes the operational environment security objectives.

Table 5-2 Operational environment security objectives

Security Objective	Description
OE.ADMIN	Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
OE.INFO_PROTECT	Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate

Security Objective	Description
	physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration, and support of the DBMS.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.

5.2.2 Operational Environment IT Domain Security Objectives

The following table describes the operational environment IT security objectives.

Table 5-3 Operational Environment IT Domain Security Objectives

Security Objective	Description
OE.IT_I&A	Any information provided by a trusted entity in the environment and used to support user authentication and authorization used by the TOE is correct and up to date.
OE.IT_REMOTE	If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions, required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.
OE.IT_TRUSTED _SYSTEM	The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and are physically and

Security Objective	Description
	logically protected equivalent to the TOE.

5.3 Security Objectives Rationale

The following table maps the security objectives to the assumptions, threats, and organizational security policies.

Table 5-4 Mapping between security objectives, threats, organizational security policies, and assumptions

-	T.ACCESS_TSFDATA	T.ACCESS_TSFFUNC	T.IA_MASQUERADE	T.IA_USER	T.RESIDUAL_DATA	T.TSF_COMPROMISE	T.UNAUTHORIZED_ACCESS	P.ACCOUNTABILITY	P.ROLES	P.USER	A.PHYSICAL	A.AUTHUSER	A.MANAGE	A.TRAINEDUSER	A.NO_GENERAL_PURPOSE	A.PEER_FUNC_&_MGT	A.SUPPORT	A.CONNECT
O.ADMIN_ROLE		X						X	X									
O.AUDIT_GENERATION						X		X										
O.DISCRETIONARY _ACCESS			X				X											
O.I&A	X	X	X	X				X										
O.MANAGE	X	X					X			X								
O.MEDIATE			X	X			X											
O.RESIDUAL_INFORMATION	X	X			X													
O.TOE_ACCESS	X	X	X	X		X		X	X	X								
OE.ADMIN								X	X	X			X					
OE.INFO_PROTECT						X	X	X			X	X	X	X	X			X
OE.NO_GENERAL_PURPOSE		X				X									X			
OE.PHYSICAL						X					X							X
OE.IT_I&A																	X	
OE.IT_REMOTE						X					X					X		X
OE.IT_TRUSTED_SYSTEM						X					X					X		X

5.3.1 Security Objectives Rationale Related to Threats

The security objectives rationale related to threats traces the security objectives for the TOE and the operational environment back to the threats addressed by the TOE. The TOE security objectives and the operational environment security threats are separately described to ensure consistency with the PP.

5.3.1.1 Threats Mapped to TOE Security Objectives

Table 5-5 Threats Mapped to TOE Security Objectives

Threat	TOE Security Objectives Addressing the Threat	Rationale
T.ACCESS_TSFDATA — A threat agent may read or modify TSF data using functions of the TOE without the proper authorization.	O.I&A The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.	O.I&A supports this policy by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE is defined to provide to authenticated users only.
	O.MANAGE The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.	O.MANAGE diminishes this threat since it ensures that functions and facilities used to modify TSF data are not available to unauthorized users.
	O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not inappropriately disclosed when the resource is reallocated.	O.RESIDUAL_INFORMATION diminishes this threat since information contained in protected resources will not be easily available to the threat agent through reallocation attacks.
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS diminishes this threat since it makes it more unlikely that a threat agent has access to the TOE.

Threat	TOE Security Objectives Addressing the Threat	Rationale
T.ACCESS_TSFFUNC A threat agent may use or manage TSF, bypassing the protection mechanisms of the TSF.	O.ADMIN_ROLE The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.	O.ADMIN_ROLE diminishes this threat by providing isolation of privileged actions.
	O.I&A The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.	O.I&A diminishes this threat since the TOE requires successful authentication to the TOE prior to gaining access to any controlled-access content. By implementing strong authentication to gain access to these services, an attacker's opportunity to masquerade as another entity in order to gain unauthorized access to data or TOE resources is reduced.
	O.MANAGE The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.	O.MANAGE diminishes this threat because an access control policy is specified to control access to TSF data. This objective is used to dictate who is able to view and modify TSF data, as well as the behavior of TSF functions.
	O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not inappropriately disclosed when the resource is reallocated.	O.RESIDUAL_INFORMATION diminishes this threat by ensuring that TSF data and user data is not persistent when resources are released by one user/process and allocated to another user/process.
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS diminishes this threat since it makes it more unlikely that a threat agent has access to the TOE.

Threat	TOE Security Objectives Addressing the Threat	Rationale
T.IA_MASQUERADE A user or a process acting on behalf of a user may masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources	O.I&A The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.	O.I&A diminishes this threat by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE has defined to provide to authenticated users only
	O.MEDIATE The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.	O.MEDIATE diminishes this threat by ensuring that all access to user data are subject to mediation, unless said data has been specifically identified as public data. The TOE requires successful authentication to the TOE prior to gaining access to any controlled access content. By implementing strong authentication to gain access to these services, an attacker's opportunity to masquerade as another entity in order to gain unauthorized access to data or TOE resources is reduced.
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	O.TOE_ACCESS diminishes this threat by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication mechanism this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can

Threat	TOE Security Objectives Addressing the Threat	Rationale
		generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE.
T.IA_USER A threat agent may gain access to user data, TSF data or TOE resources with the exception of public objects without being identified and authenticated.	O.DISCRETIONARY_ACCESS The TSF must control access of subjects and/or users to named resources based on identity of the object, subject, or user. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.	O.DISCRETIONARY_ACCESS diminishes this threat by requiring that data including user data stored with the TOE, have discretionary access control protection.
	O.I&A The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.	O.I&A diminishes this threat by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE is defined to provide to authenticated users only.
	O.MEDIATE The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.	O.MEDIATE diminishes this threat by ensuring that all access to user data are subject to mediation, unless said data has been specifically identified as public data. The TOE requires successful authentication to the TOE prior to gaining access to any controlled access content. By implementing strong authentication to gain access to these services, an attacker's opportunity to masquerade as another entity in order to gain unauthorized access to data or TOE resources is reduced.

Threat	TOE Security Objectives Addressing the Threat	Rationale
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	O.TOE_ACCESS diminishes this threat by controlling logical access to user data, TSF data or TOE resources.
T.RESIDUAL_DATA A user or process may gain unauthorized access to user or TSF data through reallocation of TOE resources from one user or process to another.	O.RESIDUAL_INFORMATION The TOE will ensure that any information contained in a protected resource within its Scope of Control is not inappropriately disclosed when the resource is reallocated.	O.RESIDUAL_INFORMATION diminishes this threat because even if the security mechanisms do not allow a user to view TSF data, if TSF data were to reside inappropriately in a resource that was made available to a user, that user would be able to view the TSF data without authorization.
T.TSF_COMPROMISE A malicious user or process may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or may compromise executable code within the TSF.	O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security relevant events associated with users.	O.AUDIT_GENERATION diminishes this threat by providing the authorized administrator with the appropriate audit records supporting the detection of compromise of the TSF.
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	O.TOE_ACCESS diminishes this threat since controlled user's logical access to the TOE will reduce the opportunities for an attacker's access to configuration data.
T.UNAUTHORIZED_AC CESS A user may gain unauthorized access to user data for which they are not authorized	O.DISCRETIONARY_ACCESS The TSF must control access of subjects and/or users to named resources based on identity of the object, subject or user. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access	O.DISCRETIONARY_ACCESS diminishes this threat by requiring that data including TSF data stored with the TOE, have discretionary access control protection.

Threat	TOE Security Objectives Addressing the Threat	Rationale
	mode.	
	O.MANAGE The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.	O.MANAGE diminishes this threat by ensuring that the functions and facilities supporting that authorized users can be held accountable for their actions by authorized administrators are in place.
	O.MEDIATE The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.	O.MEDIATE diminishes this threat because it ensures that all access to user data are subject to mediation, unless said data has been specifically identified as public data. The TOE requires successful authentication to the TOE prior to gaining access to any controlled-access content. By implementing strong authentication to gain access to these services, an attacker's opportunity to conduct a man-in-the-middle and/or password guessing attack successfully is greatly reduced. Lastly, the TSF will ensure that all configured enforcement functions (authentication, access control rules, etc.) must be invoked prior to allowing a user to gain access to TOE or TOE mediated services. The TOE restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc. to the administrator. This feature ensures that no other user can modify the information flow policy to bypass the intended

Threat	TOE Security Objectives Addressing the Threat	Rationale
		TOE security policy.

5.3.1.2 Threats Mapped to Security Objectives for the Operational Environment

Table 5-6 Threats Mapped to Security Objectives for the Operational Environment

Threat	Environmental Objective Addressing the Threat	Rationale
T.IA_MASQUERADE A user or a process acting on behalf of a user may masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources.	OE.NO_GENERAL_PURPOSE There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on DMBS servers, other than those services necessary for the operation, administration, and support of the DBMS.	OE.NO_GENERAL_PURPOSE The DBMS server must not include any general-purpose computing or storage capabilities. This diminishes the threat of masquerade since only users with DBMS or related functions will be defined in the TOE environment.

Threat	Environmental Objective Addressing the Threat	Rationale
T.TSF_COMPROMISE A user or a process acting on behalf of a user may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or may compromise executable code within the TSF.	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	OE.INFO_PROTECT diminishes the threat by ensuring that all network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques.
	OE.IT_REMOTE If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions, required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.	OE.IT_REMOTE diminishes the threat by ensuring that remote trusted IT systems are sufficiently protected.

Threat	Environmental Objective Addressing the Threat	Rationale
	OE.IT_TRUSTED_SYSTEM The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are managed according to known, accepted and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.	OE.IT_TRUSTED_SYSTEM diminishes the threat by ensuring that remote trusted IT systems are managed according to known, accepted and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.
	OE.NO_GENERAL_PURPOSE There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on DMBS servers, other than those services necessary for the operation, administration, and support of the DBMS	OE.NO_GENERAL_PURPOSE diminishes this threat by reducing the opportunities to subvert non TOE related capabilities in the TOE environment.
	OE.PHYSICAL Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.	OE.PHYSICAL diminishes the threat of a TSF compromise due to exploitation of physical weaknesses or vulnerabilities as a vector in an attack.

Threat	Environmental Objective Addressing the Threat	Rationale
T.UNAUTHORIZED_ACCESS A user may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	OE.INFO_PROTECT diminishes the threat by ensuring that the logical and physical threats to network and peripheral cabling are appropriately protected. DAC protections if implemented correctly may support the identification of unauthorized accesses.

5.3.2 Security Objectives Related to OSPs

The security objectives rationale related to OSPs traces the security objectives for the TOE and the Operational Environment back to the OSPs applicable to the TOE. The TOE security objectives and the operational environment OSPs are separately described to ensure consistency with the PP.

5.3.2.1 OSPs Mapped to Security Objectives for the TOE

Table 5-7 OSPs Mapped to Security Objectives for the TOE

Policy	TOE Security Objectives Addressing the Policy	Rationale
P.ACCOUNTABILITY — The authorized users of the TOE shall be held accountable for their actions within the TOE.	O.ADMIN_ROLE — The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.	O.ADMIN_ROLE — supports this policy by ensuring that the TOE has an objective to provide authorized administrators with the privileges needed for secure administration.
	O.AUDIT_GENERATION — The TOE will provide the capability to detect and create records of security relevant events associated with users	O.AUDIT_GENERATION — supports this policy by ensuring that audit records are generated. Having these records available enables accountability.
	O.I&A — The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.	O.I&A — supports this policy by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE is defined to provide to authenticated users only.
	O.TOE_ACCESS — The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS — supports this policy by providing a mechanism for controlling access to authorized users.
P.USER — Authority shall only be given to users who are trusted to perform the actions correctly.	O.MANAGE — The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.	O.MANAGE — supports this policy by ensuring that the functions and facilities supporting the authorized administrator role are in place.

Policy	TOE Security Objectives Addressing the Policy	Rationale
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS supports this policy by providing a mechanism for controlling access to authorized users.
	OE.ADMIN Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of information it contains.	OE.ADMIN supports this policy by ensuring that the authorized administrator role is understood and used by competent administrators.
P.ROLES Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible supporting only the administrative duties the person has. This role shall be separate and distinct from other authorized users.	O.ADMIN_ROLE The TOE will provide a mechanism (e.g.a "role") by which the actions using administrative privileges may be restricted.	O.ADMIN_ROLE The TOE has the objective of providing an authorized administrator role for secure administration. The TOE may provide other roles as well, but only the role of authorized administrator is required.
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.	O.TOE_ACCESS supports this policy by ensuring that an authorized administrator role can be distinguished from other authorized users.

5.3.2.2 OSPs Mapped to Security Objectives for the Operational Environment

Table 5-8 OSPs Mapped to Security Objectives for the Operational Environment

Policy	Environmental Objective Addressing the Policy	Rationale
P.ACCOUNTABILITY The authorized users of the TOE shall be held accountable for their actions within the TOE.	OE.ADMIN Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of information it contains.	OE.ADMIN supports the policy that the authorized administrators are assumed competent in order to help ensure that all the tasks and responsibilities are performed effectively.
	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. •Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	OE.INFO_PROTECT supports the policy by ensuring that the authorized users are trained and have procedures available to support them and that the DAC protections function and are able to provide sufficient information to inform those pursuing accountability.

Policy	Environmental Objective Addressing the Policy	Rationale
P.ROLES The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.	OE.ADMIN Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of information it contains.	OE.ADMIN supports the policy by ensuring that an authorized administrator role for secure administration of the TOE is established.
P.USER Authority shall only be given to users who are trusted to perform the actions correctly.	OE.ADMIN Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of information it contains.	OE.ADMIN supports the policy by ensuring that the authorized administrators, responsible for giving appropriate authorities to users, are trustworthy.

Policy	Environmental Objective Addressing the Policy	Rationale
	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	OE.INFO_PROTECT supports the policy by ensuring that users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data and that DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly.

5.3.3 Security Objectives Rationale Related to Assumptions

The security objectives rationale related to assumptions traces the security objectives for the operational environment back to the assumptions for the TOE's operational environment.

Table 5-9 Security Objectives Rationale Related to Assumptions

Assumption	Environmental Objective Addressing the Assumption	Rationale
A.AUTHUSER Authorized users possess the necessary authorization to access at least some of the information managed by the TOE	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. •Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	OE.INFO_PROTECT supports the assumption by ensuring that users are authorized to access parts of the data managed by the TOE and is trained to exercise control over their own data. Having trained, authorized users, who are provided with relevant procedures for information protection supports the assumption of co-operation.
	OE.IT_REMOTE If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions, required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.	OE.IT_REMOTE supports this assumption by ensuring that remote systems that form part of the IT environment are protected. This gives confidence that the environment is benign.
	OE.IT_TRUSTED_SYSTEM The remote trusted IT systems implement the protocols and mechanisms required by the	OE.IT_TRUSTED_SYSTEM supports this assumption by providing confidence that systems in the TOE IT

Assumption	Environmental Objective Addressing the Assumption	Rationale
	TSF to support the enforcement of the security policy. These remote trusted IT systems are managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.	environment contribute to a benign environment.
A.CONNECT All connections to and from remote trusted IT systems and between separate parts of the TSF are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.	OE.IT_REMOTE If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions, required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.	OE.IT_REMOTE supports the assumption by levying a requirement in the environment that connections between trusted systems or physically separated parts of the TOE are sufficiently protected from any attack that may cause those functions to provide false results.
	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authentication databases) shall always be set up correctly.	OE.INFO_PROTECT supports the assumption by requiring that All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques

Assumption	Environmental Objective Addressing the Assumption	Rationale
	• Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	
	OE.IT_TRUSTED_SYSTEM The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are managed according to known, accepted and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.	OE.IT_TRUSTED_SYSTEM supports the assumption by ensuring that remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy.
	OE.PHYSICAL Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.	OE.PHYSICAL supports the assumption by ensuring that appropriate physical security is provided within the domain.
A.SUPPORT Any information provided by a trusted entity in the IT environment and used to support the provision of time and date, information used in audit capture, user authentication, and authorization that is	OE.IT_I&A Any information provided by a trusted entity in the environment and used to support user authentication and authorization used by the TOE is correct and up to date.	OE.IT_I&A supports the assumption implicitly.
A. M AN AG E The	OE.ADMIN	OE.ADMIN

Assumption	Environmental Objective Addressing the Assumption	Rationale
	Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of information it contains.	supports the assumption since the authorized administrators are assumed competent in order to help ensure that all the tasks and responsibilities are performed effectively.
	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authentication databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	OE.INFO_PROTECT supports the assumption by ensuring that the information protection aspects of the TOE and the system(s) and relevant connectivity that form the platform for the TOE is vital to addressing the security problem, described in this PP. Managing these effectively using defined procedures is reliant on having competent administrators.

Assumption	Environmental Objective Addressing the Assumption	Rationale
A.NO_GENERAL_PURPOSE There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation,	OE.NO_GENERAL_PURPOSE There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on DMBS servers, other than those services necessary for the operation, administration, and support of the DBMS.	OE.NO_GENERAL_PURPOSE The DBMS server must not include any general-purpose computing or storage capabilities. This will protect the TSF data from malicious processes. The environmental objective is tightly related to the assumption, which when fulfilled will address the assumption
A.PEER_FUNC_&_MGT All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.	OE.IT_REMOTE If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions, required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.	OE.IT_REMOTE The assumption that connections between trusted systems or physically separated parts of the TOE is addressed by the objective specifying that such systems are sufficiently protected from any attack that may cause those functions to provide false results.
	OE.IT_TRUSTED_SYSTEM The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.	OE.IT_TRUSTED_SYSTEM The assumption on all remote trusted IT systems to implement correctly the functionality used by the TSF consistent with the assumptions defined for this functionality is supported by physical and logical protections and the application of trusted policies commensurate with those applied to the TOE.

Assumption	Environmental Objective Addressing the Assumption	Rationale
A.PHYSICAL It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.	**OE.PHYSICAL** Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.	**OE.PHYSICAL** The TOE, the TSF data, and protected user data is assumed to be protected from physical attack (e.g., theft, modification, destruction, or eavesdropping). Physical attack could include unauthorized intruders into the TOE environment, but it does not include physical destructive actions that might be taken by an individual that is authorized to access the TOE environment.
	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authentication databases) shall always be set up correctly. •Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	**OE.INFO_PROTECT** supports the assumption by requiring that all network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques.

Assumption	Environmental Objective Addressing the Assumption	Rationale
A.TRAINEDUSER Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.	OE.INFO_PROTECT Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authentication databases) shall always be set up correctly. •Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.	OE.INFO_PROTECT supports the assumption by ensuring that users are authorized to access parts of the data managed by the TOE and is trained to exercise control over their own data.

6 Definition of Extended Components

FIA_USB_(EXT).2   Enhanced user-subject binding

FIA_USB_(EXT).2 is analogous to FIA_USB.1 except that it adds the possibility to specify rules whereby subject security attributes are also derived from TSF data other than user security attributes.

Component leveling

FIA_USB_(EXT).2 is hierarchical to FIA_USB.1.

Management

See management description specified for FIA_USB.1 in [CC].

Audit

See audit requirement specified for FIA_USB.1 in [CC].

FIA_USB_(EXT).2 Enhanced user-subject binding

Hierarchical to: FIA_USB.1 User-subject binding

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB_(EXT).2 .1

The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: list of user security attributes].

FIA_USB_(EXT).2 .2

The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: rules for the initial association of attributes].

FIA_USB_(EXT).2 .3

The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: rules for the changing of attributes].

FIA_USB_(EXT).2 .4

The TSF shall enforce the following rules for the assignment of subject security attributes not derived from user security attributes when a subject is created: [assignment: rules for the initial association of the subject security attributes not derived from user security attributes].

7 Security Requirements

This section provides security functional and assurance requirements that must be satisfied by a compliant TOE. The section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) for the TOE. The requirements in this section have been drawn from the Protection Profile for Database Management Systems (Base Package), Version 2.12 dated March 23rd, 2017, ("DBMS PP").

7.1   Conventions

7.2   Security Functional Requirements

7.3   Security Functional Requirements Rationale

7.4   Dependency Rationale

7.5   Security Assurance Requirements

7.1 Conventions

The CC allows several operations to be performed on functional requirements; refinement, selection, assignment, and iteration are defined in clause 8 of Part 1 of the CC [REF 1a]. Each of these operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text** or in the case of deletions, by ~~**crossed out bold text**~~.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted by *italicized text*, selections to be filled in by the Security Target (ST) author appear in square brackets with an indication that a selection is to be made, [selection:], and are not italicized.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing the value in square brackets, [assignment_value], assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:].

The **iteration** operation is used when a component is repeated with varying operations.

Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration number).

The CC paradigm also allows protection profile and security target authors to create their own requirements. Such requirements are termed "extended requirements" and are permitted if the CC does not offer suitable requirements to meet the author's needs. **Extended requirements** must be identified and are required to use the CC class/family/component model in articulating the requirements. In this ST, extended requirements will be indicated with the "(EXT)" following the component name.

Application Notes are provided to help the developer, either to clarify the intent of a requirement, identify implementation choices, or to define "pass-fail" criteria for a requirement. For those components where Application Notes are appropriate, the Application Notes will follow the requirement component.

7.2 Security Functional Requirements

This section defines the functional requirements for the TOE. Functional requirements in this ST were drawn directly from Part 2 of the CC [1b], or were based on Part 2 of the CC, including the use of extended components. These requirements are relevant to supporting the secure operation of the TOE.

Table 7-1 Security functional requirements

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SEL.1	Selective audit
User Data Protection (FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_RIP.1	Subset residual information protection
Identification and Authentication (FIA)	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
	FIA_USB_(EXT).2	Enhanced user-subject binding
Security Management (FMT)	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data

Class	Identifier	Name
	FMT_REV.1(1)	Revocation (user attributes)
	FMT_REV.1(2)	Revocation (subject, object attributes)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_TRC.1	Internal TSF consistency
TOE Access (FTA)	FTA_MCS.1	Basic limitation on multiple concurrent sessions
	FTA_TSE.1	TOE session establishment

7.2.1 Security Audit (FAU)

7.2.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1   The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *minimum* level of audit **listed in Table 7-2:**Auditable Events; and

c) [Start-up and shutdown of the DBMS;

d) Use of special permissions (e.g., those often used by authorized administrators to circumvent access control policies); and

e) [selection: "no additional events"]].

Application Note: *If no additional (**CC** or extended) **SFRs** are included, or if additional **SFRs** are included that do not have "minimal" audit associated with them then it is acceptable to assign "no additional events" in this item.*

FAU_GEN.1.2   The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of **Table 7-2** Auditable Events, below].

Application Note: *In column 3 of the table below, "Additional Audit Record Contents" is used to designate data that should be included in the audit record if it "makes sense" in the context of the event which generates the record. If no other information is required (other than that listed in item a) above) for a particular auditable event type, then an assignment of "none" is acceptable.*

Table 7-2 Auditable Events

Security Functional Requirement	Auditable Event(s)	Additional Audit Record Contents
FAU_GEN.1	None	None
FAU_GEN.2	None	None
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	The identity of the authorized administrator that made the change to the audit configuration
FDP_ACC.1	None	None
FDP_ACF.1	Successful requests to perform an operation on an object covered by the SFP	The identity of the subject performing the operation
FDP_RIP.1	None	None
FIA_ATD.1	None	None
FIA_UAU.2	Unsuccessful use of the authentication mechanism	None
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided	None
FIA_USB_(EXT).2	Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject)	None
FMT_MOF.1	None	None
FMT_MSA.1	None	None
FMT_MSA.3	None	None
FMT_MTD.1	None	None
FMT_REV.1(1)	Unsuccessful revocation of security attributes	Identity of individual attempting to revoke security attributes
FMT_REV.1(2)	Unsuccessful revocation of security attributes	Identity of individual attempting to revoke security attributes
FMT_SMF.1	Use of the management functions	Identity of the administrator performing these functions
FMT_SMR.1	Modifications to the group of users that are part of a role	Identity of authorized administrator modifying the role definition

Security Functional Requirement	Auditable Event(s)	Additional Audit Record Contents
FPT_TRC.1	Restoring consistency	None
FTA_MCS.1	Rejection of a new session based on the limitation of multiple concurrent sessions	None
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism	Identity of the individual attempting to establish a session

7.2.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1   For audit events resulting from actions of identified users **and any identified groups**, the TSF shall be able to associate each auditable event with the identity of the [**selection**: "user"] that caused the event.

7.2.1.3 FAU_SEL.1 Selective Audit

FAU_SEL.1.1   The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) object identity;

b) user identity;

c) [selection: "**no other identities**"];

d) event type;

e) [success of auditable security events;

f) failure of auditable security events; and

g) [selection: [assignment: date and time of the event, database, client connection information, instance name, thread ID, local port, and remote port]].]

Application Note: *The intent of this requirement is to capture enough audit data to allow the administrators to perform their task, not necessarily to capture only the needed audit data. In other words, the DBMS does not necessarily need to include or exclude auditable events based on all attributes at any given time.*

7.2.2 User Data Protection (FDP)

7.2.2.1 FDP_ACC.1 Subset Access Control

FDP_ACC.1.1   The TSF shall enforce the [Discretionary Access Control policy] to objects on [all subjects, all DBMS-controlled objects, and all operations among them].

7.2.2.2 FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1   The TSF shall enforce the [Discretionary Access Control Policy] to objects based on the following: [assignment:

a) Subjects: database users;

b) Subject attributes: database role, system permissions;

c) Objects: database objects;

d) Object attributes: object permissions, object ownership.]

Application Note: *DBMS-controlled objects may be implementation-specific objects that are presented to authorized users at the user interface to the DBMS. They may include, but are not limited to tables, views, sequences, stored procedures, functions, and triggers. Data structures that are not presented to authorized users at the DBMS user interface, but are used internally, are internal TSF data structures. Internal TSF data structures are not controlled according to the rules specified in FDP_ACF.1.*

FDP_ACF.1.2   The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: A user can access an object when the user meets one of the following requirements:

a) The user is the owner of the object or has been granted the specific object permissions;

b) The user has been granted specific system permissions;

c) The user is a member of a role that has been granted specific object permissions;

d) The object is accessible by 'PUBLIC'.]

FDP_ACF.1.3   The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: users with the SYSADMIN attribute has the same permissions as the object owner].

FDP_ACF.1.4   The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: users without the permissions granted by the object owner cannot access objects created by a role with the INDEPENDENT attribute].

7.2.2.3 FDP_RIP.1 Subset Residual Information Protection

FDP_RIP.1.1   The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* the following objects: [assignment: tables, rows].

7.2.3 Identification and Authentication (FIA)

7.2.3.1 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1   The TSF shall maintain the following list of security attributes belonging to individual users:

a) [Database user identifier and any associated group memberships;

b) Security-relevant database roles; and

c) [assignment: role security attributes described in column one of Table 7-3 Role security attributes, below]].

Application Note   *The intent of this requirement is to specify the TOE security attributes that the TOE utilizes to determine access. These attributes may be controlled by the environment or by the TOE itself.*

Table 7-3 Role security attributes

Attribute	Default Value	Field in the pg_authid System Table	Description
SYSADMIN	NOSYSADMIN	rolsystemadmin	Determines whether a new role is a system administrator. Roles having the SYSADMIN attribute have the highest permission. The default value is **f**, indicating false or NOSYSADMIN.
MONADMIN	NOMONADMIN	rolmonitoradmin	Determines whether a new role is a monitor administrator. The default value is f, indicating false or NOMONADMIN.
OPRADMIN	NOOPRADMIN	roloperatoradmin	Determines whether a new role is a operator administrator. The default value is **f**, indicating false or NOOPRADMIN.
POLADMIN	NOPOLADMIN	rolpolicyadmin	Determines whether a new role is a security policy administrator. The default value is **f**, indicating false or NOOPRADMIN.
AUDITADMIN	NOAUDITADMIN	rolauditadmin	Determines whether a role has the audit and management attributes. The default value is **f**, indicating false or NOAUDITADMIN.
CREATEDB	NOCREATEDB	rolcreatedb	Defines a role's ability to create databases. The default value is **f**, indicating false or NOCREATEDB.
CREATEROLE	NOCREATEROLE	rolcreaterole	Determines whether a role can create new roles. A role with the

Attribute	Default Value	Field in the pg_authid System Table	Description
			CREATEROLE permission can also modify and delete other roles. The default value is **f**, indicating false or NOCREATEROLE.
LOGIN	NOLOGIN	rolcanlogin	Determines whether a role is allowed to log in to a database. A role having the LOGIN attribute can be considered as a user. The default value is **f**, indicating false or NOLOGIN.
INDEPENDENT	NOINDEPENDENT	rolkind	Defines private, independent roles. For a role with the INDEPENDENT attribute, administrators' rights to control and access this role are separated. The default value is **n**, indicating normal or NOINDEPENDENT. Specific rules are as follows: • Administrators have no permission to add, delete, query, modify, copy, or authorize the corresponding table objects without the authorization from the INDEPENDENT role. • If permissions related to private user tables are granted to non-private users, the system administrator will obtain the same permissions. • System administrators and security administrators with the CREATEROLE attribute have no permission to modify the inheritance relationship of the INDEPENDENT role without the authorization of the INDEPENDENT role. • System administrators have no permission to modify the owner of the table objects for the INDEPENDENT role. • System administrators and security administrators with the CREATEROLE attribute have no permission to remove the INDEPENDENT attribute of the INDEPENDENT role. • System administrators and security administrators with the CREATEROLE attribute have no permission to change the database

Attribute	Default Value	Field in the pg_authid System Table	Description
			password of the INDEPENDENT role. The INDEPENDENT role must manage its own password. If the password is lost, it cannot be reset. • The SYSADMIN attribute of a user cannot be changed to the INDEPENDENT attribute.
CONNECTION LIMIT	-1	rolconnlimit	Indicates how many concurrent connections the role can make. The default value **-1** means no limit.
VALID BEGIN	none	rolvalidbegin	Sets a date and time when the role's password becomes valid.
VALID UNTIL	none	rolvaliduntil	Sets a date and time after which the role's password is no longer valid.
PERM SPACE	unlimited	roltabspace	Sets the space used for users.
VCADMIN	NOVCADMIN	rolkind	Define the logical cluster administrator role. Role with attributes of logical cluster administrator.
REPLICATION	NOREPLICATION	rolreplication	Determines whether a role is allowed to initiate streaming replication or put the system in and out of backup mode. A role having the REPLICATION attribute is specific to replication. If not specified, NOREPLICATION is the default
INHERIT	NOINHERIT	rolinherit	Determines whether a role "inherits" the permissions of roles in the same group. It is not recommended.
PERSISTENCE	NOPERSISTENCE		Only the initial administrator can create the permanent user through the PERSISTENCE attribute

7.2.3.2 FIA_UAU.2 User authentication before any action

FIA_UAU.2.1   The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

7.2.3.3 FIA_UID.2 User identification before any action

FIA_UID.2.1   The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

7.2.3.4 FIA_USB_(EXT).2 Enhanced User-Subject Binding

FIA_USB_(EXT).2 .1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: role security attributes described in column one of **Table 7-3** Role security attributes].
FIA_USB_(EXT).2 .2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: User security attributes can be initialized by using parameters. If parameters are omitted, the default values described in column two of **Table 7-3** Role security attributes are used.].
FIA_USB_(EXT).2 .3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on behalf of users: [assignment: The changer has required permissions and changes the attributes by running ALTER ROLE.
	a) Initial administrator user can modify any user security attributes of any roles, excluding roles with independent attributes.
	b) Users having the SYSADMIN attribute can modify any user security attributes of other roles, excluding the initial administrator and roles with independent attributes.
	c) Users with the CREATEROLE attribute can modify the security attributes of other roles or delete the roles, excluding the initial administrator and roles with the SYSADMIN security attribute and roles with independent attributes.].
FIA_USB_(EXT).2 .4	The TSF shall enforce the following rules for the assignment of subject security attributes not derived from user security attributes when a subject is created: [assignment: No other security attributes can be assigned except the ones derived from user security attributes when the subject is created.]
Application Note	*The initial administrator is DBMS install time predefined user, this user has the highest control authority of the database system, this usesysid is 10, cannot be drop from the DBMS.*

7.2.4 Security Management (FMT)

7.2.4.1 FMT_MOF.1 Management of Security Function Behavior

FMT_MOF.1.1	*The TSF shall restrict the ability to disable and enable the functions [relating to the specification of events to be audited] to [authorized administrators].*
Application Note	*The authorized administrator are whose user with SYSADMIN attribute as defined in FIA_ATD.1.*

7.2.4.2 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1   The TSF shall enforce the [Discretionary Access Control Policy] to restrict the ability to *manage* [all] the security attributes to [authorized administrators].

Application Note   *The ST author should ensure that all attributes identified in FIA_ATD.1 are adequately managed and protected.*

7.2.4.3 FMT_MSA.3 Static Attribute Initialization

FMT_MSA.3.1   The TSF shall enforce the [Discretionary Access Control Policy] to provide *restrictive* default values for security attributes that are used to enforce the SFP.

Application Note   *This requirement applies to new container objects at the top-level (e.g., tables). When lower-level objects are created (e.g., rows, cells), these may inherit the permissions of the top-level objects by default. In other words, the permissions of the 'child' objects can take the permissions of the 'parent' objects by default.*

FMT_MSA.3.2   The TSF shall allow ~~the~~ [no user] to specify alternative initial values to override the default values when an object or information is created.

7.2.4.4 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1   The TSF shall restrict the ability to *include or exclude* the [auditable events] to [authorized administrators].

7.2.4.5 FMT_REV.1 (1) Revocation (User Attribute)

FMT_REV.1.1(1)   The TSF shall restrict the ability to revoke [assignment: system permissions, roles] associated with the *users* under the control of the TSF to [the authorized administrator].

FMT_REV.1.2(1)   The TSF shall enforce the rules [assignment: granting and revoking of directly assigned permissions take effect immediately].

7.2.4.6 FMT_REV.1 (2) Revocation (Subject, Object Attribute)

FMT_REV.1.1(2)   The TSF shall restrict the ability to revoke [assignment: object permissions] associated with the *objects* under the control of the TSF to [the authorized administrator] **and database users with sufficient privileges as allowed by the Discretionary Access Control Policy.**

FMT_REV.1.1(2)   The TSF shall enforce the rules [assignment:

a) authorized administrators and object owners may revoke object

permissions; and

b) object owners may grant other users permissions to grant and revoke object permissions].

7.2.4.7 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1   The TSF shall be capable of performing the following security management functions: [assignment:

- Database configuration
- User and role management
- Management of groups
- Adding or removing a database
- Revocation of security attributes
- Configuration of the maximum number of concurrent sessions
- Configuration of TSF replication and consistency
- Configuration of TOE access information rules
- management of the events to be audited
- granting or revoking of system permissions
- granting or revoking of object permissions
- IP address whitelist and IP address blacklist]

7.2.4.8 FMT_SMR.1 Security Roles

FMT_SMR.1.1   The TSF shall maintain the roles [authorized administrator and [assignment: custom role]].

FMT_SMR.1.2   The TSF shall be able to associate users with roles.

Application Note   *This requirement identifies a minimum set of management roles. The role of administrator granting rights is also the database administrator (**DBA**).*

7.2.5 Protection of the TSF (FPT)

7.2.5.1 FPT_TRC.1 Internal TSF Consistency

FPT_TRC.1.1   The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

FPT_TRC.1.2   When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for

[assignment: queries].

Application Note *In general, it is impossible to achieve complete, constant consistency of TSF data that is distributed to remote portions of a TOE because distributed portions of the TSF may be active at different times or disconnected from one another. This requirement attempts to address this situation in a practical manner by acknowledging that there will be TSF data inconsistencies but that they will be corrected without undue delay. For example, a TSF could provide timely consistency through periodic broadcast of TSF data to all TSF nodes maintaining replicated TSF data. Another example approach is for the TSF to provide a mechanism to explicitly probe remote TSF nodes for inconsistencies and respond with action to correct the identified inconsistencies.*

7.2.6 TOE Access (FTA)

7.2.6.1 FTA _MCS.1 Basic Limitation on Multiple Concurrent Sessions

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of [assignment: an administrator configurable number of] sessions per user.

Application Note *The ST author is reminded that the CC [REF 1b] para 473 allows that the default number may be defined as a management function in FMT.*

7.2.6.2 FTA _TSE.1 TOE Session Establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [assignment: attributes that can be set explicitly by authorized administrator(s), including user identity, [selection: [assignment: number of connections, user whitelist, IP whitelist, and IP blacklist]]].

7.3 Security Functional Requirements Rationale

The following table provides a mapping between the security functional requirements and security objectives.

Table 7-4 Security functional requirements rationale

-	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.DISCRETIONARY_ACCESS	O.I&A	O.MANAGE	O.MEDIATE	O.RESIDUAL_INFORMATION	O.TOE_ACCESS
FAU_GEN.1		X						
FAU_GEN.2		X						
FAU_SEL.1		X						
FDP_ACC.1			X			X		X
FDP_ACF.1			X			X		X
FDP_RIP.1							X	
FIA_ATD.1				X				X
FIA_UAU.2				X				
FIA_UID.2				X				
FIA_USB_(EXT).2				X				
FMT_MOF.1					X			
FMT_MSA.1					X			
FMT_MSA.3					X			
FMT_MTD.1					X			
FMT_REV.1(1)					X			
FMT_REV.1(2)					X			
FMT_SMF.1					X			
FMT_SMR.1	X				X			
FPT_TRC.1						X		
FTA_MCS.1								X
FTA_TSE.1								X

7.3.1 SFR Rationale Related to Security Objectives

The following table provides the rationale for the selection of the security functional requirements. It traces each TOE security objective to the identified security functional requirements.

Security Objective: O.ADMIN_ROLE	The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.	
Security Functional Requirement	FMT_SMR.1	Security roles
Rationale	The TOE will establish, at least, an authorized administrator role. The authorized administrator will be given privileges to perform certain tasks that other users will not be able to perform. These privileges include, but are not limited to, access to audit information and security functions. [FMT_SMR.1]	

Security Objective: O.AUDIT_GENERATION	The TSF must be able to record defined security-relevant events (which usually include security-critical actions of users of the TOE). The information recorded for security-relevant events must contain the time and date the event happened and, if possible, the identification of the user that caused the event, and must be in sufficient detail to help the authorized user detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.	
Security Functional Requirement	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SEL.1	Selective audit
Rationale	FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that the administrator has the ability to audit any security relevant events that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements an ST author adds to the ST. [FAU_GEN.1]	
	FAU_GEN.2 ensures that the audit records associate a user and any associated group identity with the auditable event. In the case of authorized users, the association is accomplished with the user ID. In the case of authorized groups, the association is accomplished with the group ID. [FAU_GEN.2]	
	FAU_SEL.1 allows the administrator to configure which auditable events will be recorded in the audit trail. This provides the administrator with the flexibility in recording only those events that are deemed necessary by site policy, thus reducing the amount of resources	

	consumed by the audit mechanism. [FAU_SEL.1]

Security Objective: O.DISCRETION-ARY_ACCESS	The TSF must control access of subjects and/or users to named resources based on identity of the object, subject, or user. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.	
Security Functional Requirement	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
Rationale	The TSF must control access to resources based on the identity of users that are allowed to specify which resources they want to access for storing their data. The access control policy must have a defined scope of control [FDP_ACC.1]. The rules for the access control policy are defined [FDP_ACF.1].	

Security Objective: O.I&A	The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.	
Security Functional Requirement	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
	FIA_USB_(EXT).2	Enhanced user-subject binding
Rationale	The TSF must ensure that only authorized users gain access to the TOE and its resources. Users authorized to access the TOE must use an identification and authentication process [FIA_UID.2, FIA_UAU.2]. To ensure that the security attributes used to determine access are defined and available to the support authentication decisions. [FIA_ATD.1] Proper authorization for subjects acting on behalf of users is also ensured [FIA_USB_(EXT).2]. The appropriate strength of the authentication mechanism is ensured.	

Security Objective: O.MANAGE	The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.

Security Functional Requirement	FMT_MOF.1	Management of security functions behavior
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_REV.1(1)	Revocation (user attributes)
	FMT_REV.1(2)	Revocation (subject, object attributes)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Rationale	FMT_MOF.1 requires that the ability to use particular TOE capabilities be restricted to the administrator. [FMT_MOF.1]	
	FMT_MSA.1 requires that the ability to perform operations on security attributes be restricted to particular roles. [FMT_MSA.1]	
	FMT_MSA.3 requires that default values used for security attributes are restrictive. [FMT_MSA.3]	
	FMT_MTD.1 requires that the ability to manipulate TOE content is restricted to administrators. [FMT_MTD.1]	
	FMT_REV.1 restricts the ability to revoke attributes to the administrator. [FMT_REV.1(1), FMT_REV.1(2)]	
	FMT_SMF.1 identifies the management functions that are available to the authorized administrator. [FMT_SMF.1]	
	FMT_SMR.1 defines the specific security roles to be supported. [FMT_SMR.1]	

Security Objective: **O.MEDIATE**	The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.	
Security Functional Requirement	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FPT_TRC.1	Internal TSF consistency
Rationale	The FDP requirements were chosen to define the policies, the subjects, objects, and operations for how and when mediation takes place in the TOE.	
	FDP_ACC.1 defines the Access Control policy that will be enforced on a list of subjects acting on the behalf of users attempting to gain access to a list of named objects. All the operations between subject and object covered are defined by the TOE's policy. [FDP_ACC.1]	
	FDP_ACF.1 defines the security attribute used to provide access control to objects based on the TOE's access control policy. [FDP_ACF.1]	
	FPT_TRC.1 ensures replicated TSF data that specifies attributes for access control must be consistent across distributed components of the	

	TOE. The requirement is to maintain consistency of replicated TSF data. [FPT_TRC.1]

Security Objective: **O.RESIDUAL _INFORMAT ION**	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not inappropriately disclosed when the resource is reallocated.	
Security Functional Requirement	FDP_RIP.1	Subset residual information protection
Rationale	FDP_RIP.1 is used to ensure the contents of resources are not available to subjects excepting those explicitly granted access to the data. [FDP_RIP.1]	

Security Objective: **O.TOE_ACCE SS**	The TOE will provide functionality that controls a user's logical access to user data and to the TSF.	
Security Functional Requirement	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FIA_ATD.1	User attribute definition
	FTA_MCS.1	Basic limitation on multiple concurrent sessions
	FTA_TSE.1	TOE session establishment
Rationale	FDP_ACC.1 requires that each identified access control SFP be in place for a subset of the possible operations on a subset of the objects in the TOE. [FDP_ACC.1]	
	FDP_ACF.1 allows the TSF to enforce access based upon security attributes and named groups of attributes. Furthermore, the TSF may have the ability to explicitly authorize or deny access to an object based upon security attributes. [FDP_ACF.1]	
	FIA_ATD.1 defines the security attributes for individual users including the user's identifier and any associated group memberships. Security relevant roles and other identity security attributes. [FIA_ATD.1]	
	FTA_MCS.1 ensures that users may only have a maximum of a specified number of active sessions open at any given time. [FTA_MCS.1]	
	FTA_TSE.1 allows the TOE to restrict access to the TOE based on certain criteria. [FTA_TSE.1]	

7.4 Dependency Rationale

The following table identifies the SFRs from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

Table 7-5 Dependency rationale

Security Functional Requirement	Dependency	Description
FAU_GEN.1	FPT_STM.1	This requirement is satisfied by the assumption on the IT environment, given in A.SUPPORT.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Satisfied by FAU_GEN.1 Satisfied by FIA_UID.2
FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	Satisfied by FAU_GEN.1 Satisfied by FMT_MTD.1
FDP_ACC.1	FDP_ACF.1	Satisfied by FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	Satisfied by FDP_ACC.1 Satisfied by FMT_MSA.3
FDP_RIP.1	None	N/A
FIA_ATD.1	None	N/A
FIA_UAU.2	FIA_UID.1	Satisfied by FIA_UID.2
FIA_UID.2	None	N/A
FIA_USB_(EXT).2	FIA_ATD.1	Satisfied by FIA_ATD.1
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Satisfied by FMT_SMR.1 Satisfied by FMT_SMF.1
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Satisfied by FDP_ACC.1 Satisfied by FMT_SMR.1 Satisfied by FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Satisfied by FMT_MSA.1 Satisfied by FMT_SMR.1
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	Satisfied by FMT_SMF.1 Satisfied by FMT_SMR.1
FMT_REV.1(1)	FMT_SMR.1	Satisfied by FMT_SMR.1
FMT_REV.1(2)	FMT_SMR.1	Satisfied by FMT_SMR.1
FMT_SMF.1	None	N/A
FMT_SMR.1	FIA_UID.1	Satisfied by FIA_UID.2

Security Functional Requirement	Dependency	Description
FPT_TRC.1	FPT_ITT.1	FPT_ITT.1 is not applicable. For a distributed TOE, the dependency is satisfied through the assumption on the environment, A.CONNECT, that assures the confidentiality and integrity of the transmitted data.
FTA_MCS.1	FIA_UID.1	Satisfied by FIA_UID.2
FTA_TSE.1	None	N/A

7.5 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 4 components as specified in [CC] Part 3, augmented with ALC_FLR.2. No operations are applied to the assurance components.

Table 7-6 Security assurance requirements

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level
Development	ADV_ARC	1
	ADV_FSP	4
	ADV_IMP	1
	ADV_INT	NA
	ADV_SPM	NA
	ADV_TDS	3
Guidance documents	AGD_OPE	1
	AGD_PRE	1
Life-cycle support	ALC_CMC	4
	ALC_CMS	4
	ALC_DEL	1
	ALC_DVS	1
	ALC_FLR	2

	ALC_LCD	1	
	ALC_TAT	1	
Security Target evaluation	ASE_CCL	1	
	ASE_ECD	1	
	ASE_INT	1	
	ASE_OBJ	2	
	ASE_REQ	2	
	ASE_SPD	1	
	ASE_TSS	1	
Tests	ATE_COV	2	
	ATE_DPT	1	
	ATE_FUN	1	
	ATE_IND	2	
Vulnerability assessment	AVA_VAN	3	

7.5.1 Security Assurance Requirements Rationale

The evaluation assurance level has been chosen to commensurate with the threat environment that is experienced by typical consumers of the TOE.

8 TOE Summary Specification

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

8.1 TOE Security Function

The following sections describe TOE security functions one by one.

8.1.1 Security Audit

FAU_GEN.1.1

The TOE's auditable events and audit enabling/disabling are as follows:

- The **audit_enabled** GUC-parameter specifies whether to enable the audit log generation function. The default value is on, indicating that the audit function is enabled. The settings of audit_enabled can be dynamically loaded and take effect immediately during database running. The enabling and disabling of the audit function are recorded in operation logs.

- Besides **audit_enabled**, the TOE provides 11 audit items, each audit item controls the effective of audit functions that corresponding to different events. The audit function modifications can take effect immediately during database running. Audit items control whether DML, DCL, DDL, and other operations are audited. For example, the audit item **audit_login_logout** controls whether user logins and logouts are audited. The value 0 indicates that the audit of user logins and logouts is disabled. **audit_database_process** controls whether database startup, stop, recovery and switchover are audited. **audit_user_locker** controls wheter user lock and unlock are audited. **audit_grant_revoke** controls whether user privileges granting and revoking are audited. **audit_system_object** controls whether DDL operations on database objects, such as CREATE, ALTER, and DROP, are audited. **audit_dml_state** control whether DML operations (except SELECT) on tables are audited. **audit_dml_state_select** controls whether SELECT operations are audited.

- Audit logs or run logs are recorded based on the auditable events described in the second column of Table 7-2. The following details should be noted:

  a. To meet the auditing requirements of FPT_TRC.1 (that is, restoring consistency), the TOE can back up and restore management and user data in the system, including audit logs.

  b. To meet the auditing requirements of FTA_MCS.1 (that is, rejection of a new session based on the limitation of multiple concurrent sessions), if the number of sessions exceeds the value of the max_connections parameter, the login fails and run logs are printed to show that the number of connections exceeds the upper limit; if the number of user connections exceeds the

value of the connection limit parameter, the login fails and an error code is returned to show that the number of connections exceeds the upper limit.

- When the overall audit parameter **audit_enabled** is set to be on (default value), all audit item function takes effect immediately. Each audit item is independent with each other. By default, user login/logout, database startup, stop, recovery, and switch over, create, alter, and drop on database objects, grant and revoke of all privileges include system and object privileges support recording audit logs.

  FAU_GEN.1.2

  Each audit record contains the date and time of the event, type of event, outcome of event, object name, thread id, and additional information in the third column of Table 7-2.

  FAU_GEN.2.1

  Each audit record contains the user id information, so that each auditable event can be associated with the user that causes the event, even the users have the same name. A user is a role with the login permission. A role can be regarded as a database user or a user group, depending on how the role is defined.

  FAU_SEL.1.1

  For each audit item, TOE allows to set different values of these items, each value associates with different event. By setting different values of audit item, TOE can select the set of events to be audited from the set of all auditable events based on the following attributes:

  - **time**: time when an event occurs
  - **type**: event type
  - **result**: event result
  - **userid**: user id
  - **username**: username
  - **database**: database name
  - **client_conninfo**: IP address of a client requesting access
  - **thread_id**: thread ID
  - **node_name**: name of the node whose logs are audited, Alias is"Instance name".
  - **detail_info**: event execution result details
  - **object_name**: operation database object name
  - **local_port**: local service port
  - **remote_port**: remote service port

  The TOE allows for a customized audit log path and limits the maximum number and size of audit logs.

  TOE security functional requirements: FAU_GEN.1, FAU_GEN.2, and FAU_SEL.1

8.1.2 User Data Protection

FDP_ACC.1.1, FDP_ACF.1.1, FDP_ACF.1.2, FDP_ACF.1.3, FDP_ACF.1.4

FDP_ACC.1 and FDP_ACF.1 are used to describe how database users are granted with the permissions to access database objects. Database objects are any objects that can be operated using SQL statements in the database, including but not limited to tables, indexes, sequences,

views, functions, databases, and stored procedures. You can grant access permissions in one of the following ways:

a. Object permissions

Users having object permissions can perform various operations on database objects. The permissions include SELECT, INSERT, UPDATE, DELETE, ALTER and DROP. The owner of an object has all the permissions for the object, and can grant all or part of the permissions (for example, read-only access) of the object to other users.

b. System permissions

Users having system permissions can perform certain operations, including login and authorization. The system administrator has all system permissions, and can grant or revoke permissions from other users.

c. Role permissions

A role is a set of permissions. Users and permissions can be associated. To grant different users with the same permissions, you can create a role, grant permissions to the role, and assign the role to the users. The users will inherit all the object permissions of the role and can perform the operations that are allowed for the role.

d. PUBLIC permissions

PUBLIC is a set default user permissions preset in the system. A user has all the PUBLIC permissions by default. In this case, if a permission is granted to the 'PUBLIC' role, all database users will have this permission. The role is special and does not appear in any role list.

FDP_RIP.1.1

Residual information protection is enforced through the implementation of "write before read". Storage for a row is allocated at the time that is in inserted or updated status and the new values are written into the allocated space. Data storage and retrieval relies upon indexes and links and there is no way for users to directly visit unallocated disk space and see the context. TOE manages its all objects and the corresponding space. After a table/row object is deleted, TOE ensures that the space been occupied by those objects cannot be accessed by any functions unless the space has been returned back to free space and been occupied by new object. This ensures that even deleted table/rows cannot be accessed using TOE functions until it is occupied by another table/row object and can been seen by new transaction.

TOE does not immediately remove the old version of a row from a table. This approach is necessary to gain the benefits of concurrency control. A row version must not be deleted, while it still may be needed by another transaction. However, eventually, an outdated or deleted row version is no longer of interest to any transaction. The space it occupies must be reclaimed for reuse by new rows, to avoid infinite growth of disk space requirements. TOE monitors table activity and reclaims space as necessary.

TOE provide backend threads Vacuum worker, the main function of this thread is to automatically clean up the garbage data of the database periodically.

TOE security functional requirements: FDP_ACC.1, FDP_ACF.1, and FDP_RIP.1

8.1.3 User identification and authentication

FIA_ATD.1.1

The TOE uses roles to manage database object access permissions. A role is an entity that owns database objects and permissions. In different environments, a r ole can be considered a user, a group, or both. The role is a user who does not have the database login permission or schema with the same name. After a role (user) is granted to a user through **GRANT**, the user will have all database object permissions of the role (user). Role-based authorization inherits only the database object permissions of the role. System attributes (such as **SYSADMIN, MONADMIN, OPRADMIN, POLADMIN, AUDITADMIN, CREATEDB, CREATEROLE, LOGIN, INDEPENDENT, CONNECTION LIMIT, VALID BEGIN, VALID UNTIL, PERM SPACE, VCADMIN, REPLICATION, INHERIT and PERSISTENCE**) of roles (including users) are not included. It is recommended that roles be used to efficiently grant permissions. For example, you can create different roles of design, development, and maintenance personnel, grant the roles to users, and then grant specific data permissions required by different users. When permissions are granted or revoked at the role level, these changes take effect on all members of the role.

FIA_UAU.2.1, FIA_UAU.2.2, FIA_UID.2.1, FIA_UID.2.2

Users are not allowed to access the TOE before they are identified and authenticated in the authentication mode set by the authorization administrator.

The client identity authentication is controlled by the **pg_hba.conf** configuration file on the server. The general format of the **pg_hba.conf** file is a set of records, including the connection type, client IP address range (depending on the connection type), database name, username, and authentication method for connection. The first record that contains the matching connection type, client address, requested database, and username is used for authentication. If a record is selected and the authentication fails, subsequent records will not be authenticated. If there are no matching records, the access will be denied.

The following table lists the authentication modes supported by the TOE.

Table 8-1 Authentication modes

Authentication Mode	Description
trust	Trusts only the connection initiated from the local server using **gsql** without the **-U** parameter specified. In this case, no password is required. The trust authentication mode is not allowed for remote connections to the TOE.
reject	Rejects connection unconditionally. This authentication mode is usually used for filtering certain hosts.
md5	Requires that the client must provide an MD5-encrypted password for authentication. This authentication mode is retained to be compatible with third-party tools. It is not recommended.
sha256	Requires that the client must provide an SHA256-encrypted password for authentication.
cert	Requires that the client must provide the certification needed by SSL protocol and enable SSL, by using this mode, no password is needed.

FIA_USB_(EXT).2.1

The TOE associates roles with the security attributes listed in the first column of Table 7-3.

FIA_USB_(EXT).2.2

By default, the values of the security attributes specified in the second column of Table 7-3 are assigned to users, that is, common users.

FIA_USB_(EXT).2.3

Users with sufficient permissions can use the **ALTER ROLE** statement to modify the security attributes of a role based on the following rules:

a) Initial administrator user can modify any user security attributes of any roles, excluding roles with independent attributes.

b) Users having the **SYSADMIN** attribute can modify any user security attributes of other roles, excluding the initial administrator and roles with independent attributes.

c) Users with the **CREATEROLE** attribute can modify the security attributes of other roles or delete the roles, excluding the initial administrator and roles with the SYSADMIN security attribute and roles with independent attributes.

FIA_USB_(EXT).2.4

The system does not assign any other security attributes to users except default security attributes and the security attributes modified based on the preceding rules.

TOE security functional requirements: FIA_ATD.1, FIA_UAU.2, FIA_UID.2, and FIA_USB_(EXT).2

8.1.4 Security Management

FMT_MOF.1.1

Authorized administrators can enable or disable audit functions. They can enable or disable audit logs by setting audit parameters, and can include or exclude audit items by setting parameters. For details, see 8.1.1 Security Audit.

FMT_MSA.1.1, FMT_MSA.3.1, FMT_MSA.3.2

Authorized administrators can configure discretionary access control policies to manage all security attributes, such as system permissions, object permissions, and roles. Default system permissions and attributes automatically defined for an object upon the object creation cannot be modified by any user. After an object is created, its permissions and attributes can be granted or revoked by the owner or users granted with required permissions, by running the **GRANT** or **REVOKE** statement. Attribute values cannot be accessed before the access permission is granted by an authorized administrator or object owner.

FMT_MTD.1

Authorized administrators can increase or reduce events to be audited by setting audit item parameters and audit levels.

FMT_REV.1.1(1), FMT_REV.1.1(2)

Authorized administrators can revoke system permissions and roles. The revoking of a system permission that is directly assigned to a user or role takes effect immediately.

FMT_REV.1.2(1), FMT_REV.1.2(2)

Authorized administrators and object owners can revoke object permissions. They can determine whether other users can grant or revoke these object permissions.

FMT_SMF.1.1

Authorized administrators can run commands to perform configuration for database security management including:

- Database configuration
- User and role management
- Management of groups
- Adding or removing a database
- Revocation of security attributes
- Configuration of the maximum number of concurrent sessions
- Configuration of TSF replication and consistency
- Configuration of TOE access information rules
- Management of the events to be audited
- Granting or revoking of system permissions
- Granting or revoking of object permissions
- IP address whitelist and IP address blacklist

FMT_SMR.1.1, FMT_SMR.1.2

Security management maintains authorized administrators (users with the SYSADMIN attribute), database users, and other roles defined by authorized administrators. An initial administrator is automatically created upon database creation. Other management roles can be created by an authorized administrator. After a role is granted to a user by using the **GRANT** statement, the user has all the rights of the role. The user can use the database but does not have system management permissions.

TOE security functional requirements: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_REV.1(1), FMT_REV.1(2), FMT_SMF.1, and FMT_SMR.1

8.1.5 Protection of the TOE Security Functions(FPT)

FPT_TRC.1.1, **FPT_TRC.1.2**

1) Single node deployment scenario:

In a single-node deployment scenario, TOE does not contain physically separated parts, hence, the SFR FPT_TRC.1 is trivially met as intended by the application note in [PP, 7.1.5.1] Page is the smallest storage unit of TOE, for data replication in the system, the consistency check of the data replication will be completed through the CRC Checksum value of the Page.

2) Primary and standby deployment scenarios:

Through **Quorum** protocol ensures the consistency of data synchronization and replication. Incremental Xlogs playback is adopted on the standby nodes to achieve data synchronization with the primary node.

Quorum protocol guarantees that primary node machine transaction can only be submitted after   more than half of the nodes in the TOE machines completes the Xlogs synchronization of the above transaction finished redo process. If the standby node machine lost the connection with the primary node machine, then primary node machine transaction commit will be blocked and cache. Only when the standby node machine reconnection with the primary node machine send synchronization request and finished the incremental XLogs

replication. Then primary node machine transaction can be commit and flush data into the disk

TOE security functional requirements: FPT_TRC.1

8.1.6 TOE Access

FTA_MCS.1.1, FTA_MCS.1.2

The TSF restricts the maximum number of database sessions and the maximum number of concurrent sessions for a user through parameter settings in the configuration file or user security attributes. Each parameter has a value range and a default value. During the session setup, the database name, username, and client IP address are verified based on the **pg_hba.conf** file. After this process is successful, the server attempts to connect to the database. In this case, the server determines whether the maximum number of connections allowed by the server is reached. If the number of current sessions reaches the threshold, new connections will be denied. The maximum number of connections of each server node can be specified by the **max_connections** parameter in the **postgresql.conf** configuration file. The default value is **200**. The maximum number of connections for each role is determined by the **CONNECTION LIMIT** security attribute of the role. The default value of this security attribute is **-1**, indicating that there is no limit on the number of connections. During session establishment, the system checks whether the number of connections of the current role exceeds the value of th   is parameter.

FTA_TSE.1.1

The TSF filters session connections through a user identity, login date, or IP address, controls login permissions through session establishment permissions, and specifies password expiration time and maximum login attempts. The TSF can reject the session establishment based on the user identifier, group identifier, database name, primary IP address, subnet address in the **pg_hba.conf** file, and the maximum number of connections allowed by the server node in the **postgresql.conf** file. The TSF can determine whether to allow session establishment based on the validity period of the role specified by the **VALID BEGIN** and **VALID UNTIL** clauses in the **CREATE ROLE** command. To let a user out of its validity period establish a session, the administrator or a user with the **CREATEROLE** attribute shall reset the validity period and update this period into **pg_authid** catalog table, or the session establishment will be denied.

TOE security functional requirements: FTA_MCS.1, FTA_TSE.1

9 Terminology, Acronyms, and References

9.1 Term

Table 9-1 Term

Term	Description
Access	Interaction between an entity and an object that results in the flow or modification of data.
Access control	Security service that controls the use of resources and the disclosure and modification of data.
Accountability	Property that allows activities in an IT system to be traced to the entity responsible for the activity.
Administrator	A user who has been specifically granted the authority to manage some portion or the entire TOE and whose actions may affect the TOE security policy. Administrators may possess special privileges that provide capabilities to override portions of the TOE security policy.
Assurance	A measure of confidence that the security features of an IT system are sufficient to enforce its security policy.
Attack	An intentional act attempting to violate the security policy of an IT system.
Authentication	Security measure that verifies a claimed identity.
Authorization	Permission, granted by an entity authorized to do so, to perform functions and access data.

Term	Description
Authorized Administrator	The authorized person in contact with the Target of Evaluation who is responsible for maintaining its operational capability.
Authorized user	An authenticated user who may, in accordance with the TOE security policy, perform an operation.
Compromise	Violation of a security policy.
Confidentiality	A security policy pertaining to the disclosure of data.
Configuration data	Data used in configuring the TOE.
Database Management System (DBMS)	A suite of programs that typically manage large structured sets of persistent data, offering ad hoc query facilities to many users. They are widely used in business applications.
Discretionary access control (DAC)	A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. Those controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.
Entity	A subject, object, user or another IT device, which interacts with TOE objects, data, or resources.
Executable code within the TSF	The software that makes up the TSF which is in a form that can be run by the computer.
Identity	A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Save	Security policy related to data damage and the TSF mechanism.
Named Object	An object that exhibits all of the following characteristics: This object can be used to transfer information between different users and/or group identities within the TSF. Subjects in the TOE must be able to require a specific instance of the object. The name used to refer to a specific instance of the object must exist in a context that potentially allows subjects with different user and/or group identities to require the same instance of the object.
Object	An entity within the TOE scope of control that contains or receives information and upon which subjects perform operations.
Public Object	An object for which the TSF unconditionally permits all entities "read" access. Only the TSF or authorized

Term	Description
	administrators may create, delete, or modify the public objects.
Security attributes	TSF data associated with subjects, objects, and users that are used for the enforcement of the TOE security policy.
Subject	An entity within the TOE scope of control that causes operation to be performed.
Threat	Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.
TOE resources	Anything useable or consumable in the TOE.
Unauthorized user	A user who may obtain access only to system provided public objects if any exist.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Vulnerability	A weakness that can be exploited to violate the TOE security policy.

9.2 Acronyms

Table 9-2 Acronyms

Acronym	Definition
ACID	atomicity, consistency, isolation, and durability
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
DAC	Discretionary Access Control
DBA	database administrator
DBMS	Database Management System
DBMS PP	Base Protection Profile for Database Management Systems
EAL	Evaluation Assurance Level
GUI	graphical user interface

Acronym	Definition
HA	high availability
I&A	Identification and Authentication
IT	Information Technology
O&M	Operation and Maintenance
OSP	Organizational Security Policy
PP	Protection Profile
RDBMS	Relational Database Management System
RIP	Residual Information Protection
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SPD	security problem definition
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
MPP	massively parallel processing

9.3 References

- [CC] Common Criteria for Information Technology Security Evaluation, Part 1-3, Version 3.1 Revision 5, April 2017
- [CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 Revision 5, April 2017
- [DBMSPP] Protection Profile for Database Management Systems (Base Package), Version 2.12 dated March 23rd, 2017. BSI-CC-PP-0088-V2