HUAWEI GaussDB 200 6.5.1

Security Target

Issue	0.7
Date	2021-07-02

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

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).

Change History

Date	Version	Updated Section	Description	Owner
2019-08-30	0.1	All	This is the first draft.	Huawei Technologies Co., Ltd.
2020-04-03	0.2	All	Updated the document based on review comments.	Huawei Technologies Co., Ltd.
2020-05-20	0.3	All	Updated the document based on review comments.	Huawei Technologies Co., Ltd.
2020-10-27	0.4	All	Updated the document based on review comments.	Huawei Technologies Co., Ltd.
2020-12-31	0.5	All	Updated the document based on review comments.	Huawei Technologies Co., Ltd.
2021-03-18	0.6	All	Updated the document based on review comments.	Huawei Technologies Co., Ltd.
2021-07-02	0.7	All	Updated the document based on review	Huawei Technologies Co., Ltd.

Date	Version	Updated Section	Description	Owner
			comments.	

2 ST Introduction

2.1 ST Identification

ST title: Huawei GaussDB 200 6.5.1 Security Target

Version: 0.7

Date: 2021-07-02

Developer: Huawei Technologies Co., Ltd.

2.2 TOE Identification

Name: Huawei GaussDB 200

Version: 6.5.1 Build e3690037

Developer: Huawei Technologies Co., Ltd.

2.3 TOE Overview

The TOE is the Huawei GaussDB 200 Database Management System (DBMS). Huawei GaussDB 200 is an enterprise-level relational database for massively parallel processing (MPP), which adopts the MPP architecture, supports row and column storage, provides the capabilities of processing petabytes of data, and is oriented to massive data online analysis. The database provides the following functions:

- Supports standard SQL

  Supports standard SQL92 and SQL2003, GBK and UTF-8 character sets, SQL standard functions, analytical functions, and SQL Procedural Language.

- Provides database storage management

  Supports tablespaces and online scaling.
- Provides component management and high availability (HA) of data nodes

  Supports atomicity, consistency, isolation, and durability (ACID) features of database transactions, recovery from single node failure, and load balancing.
- Provides data analysis capabilities

  Supports full-text index, unified management of structured and semi-structured data, unified SQL access, and collaborative analysis between homogeneous clusters across data centers.
- Supports APIs

  Supports standard JDBC 4.0 and ODBC 3.5.
- Provides security functions

  Provides functions including security audit, user data protection, identity identification and authentication, security management, data backup and restoration, and session management, ensuring database security.

2.3.1 TOE Type

The TOE is a DBMS. It provides a relational database engine providing mechanisms for access control, identification and authentication, and security audit. It mainly focuses on online data analysis processing scenarios with large data volumes.

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 designed for a DBMS, which can restrict the access of authorized users to the TOE, implement free access control on objects controlled by the DBMS based on users or roles, and can clarify users' responsibilities by their behavior.

TOE security functions are as follows:

- Security audit: Audit entries are generated for security related events. Audit policies may be created to generate logs based on details such as the user, the object being accessed, event type or success or failure of the operation.
- User data protection: The TOE provides a discretionary access control policy to provide access control between users and database objects (such as tables, columns, views, triggers, functions, and procedures) or metadata. Once data is allocated to a resource, the previous information content is no longer available. It further controls that only authorized administrators are able to manage the TOE.
- User 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 (**gsql**) and the parameter configuration tool (**gs_guc**) on the server.

- Protection of the TSF: The TSF is protected through backup and restoration solutions and data reliability assurance mechanisms, ensuring fault recovery consistency and replication consistency.
- 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.

2.3.3 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.

Data Network channel is also out of scope and thus not included in the TOE. It is used to transmit service data between node instances in a cluster.

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 24 cores Intel processor or Dual-socket 32-core Kunpeng 916 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 256 GB. Complex queries require high memory. In high concurrency scenarios, the memory may be insufficient. In this case, you are advised to use a 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.
OS	**Evaluation OSs**: SUSE Linux Enterprise Server 12 (SUSE 12) SP3, x86_64 **Supported OSs**: ● SUSE 11 SP1/SP2/SP3/SP4 ● SUSE 12 SP0/SP1/SP2/SP3 ● RedHat 6.4/6.5/6.6/6.7/6.8/6.9 ● RedHat 7.0/7.1/7.2/7.3/7.4/7.5 ● CentOS 6.4/6.5/6.6/6.7/6.8/6.9 ● CentOS 7.0/7.1/7.2/7.3/7.4 ● EulerOS 2.3/2.8 ● CentOS 7.5/7.6

Item	Requirement
	• NeoKylin 7.6
Software	The Software of Python v2.7.5 is also out of scope and thus not included in the TOE. JDK v1.8 (server version) FusionInsight_BASE_6.5.1_SLES.tar.gz FusionInsight_Manager_6.5.1_SLES.tar.gz FusionInsight_SetupTool_6.5.1_SLES.tar.gz
Clients	Clients (including local and remote clients: gsql 6.5.1, JDBC, ODBC) are also out of scope and thus not included in the TOE. They are used to interact with the TOE.
Server Tools	Server Tools (this is, all tools listed in section 7.3 of *GaussDB 200 6.5.1 Product Documentation 09.pdf*) are also out of scope and thus not included in the TOE. They are used to manager and monitor the TOE.
Firewall	Used to protect TOE interfaces.

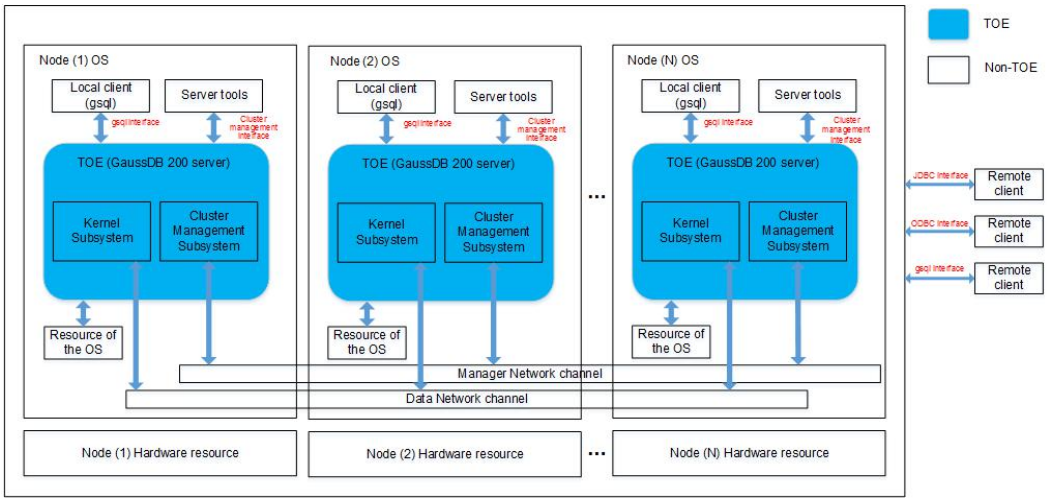
Table 2-1 Non-TOE hardware and software items

2.4 TOE Description

2.4.1 TOE Environment

The following figure shows the TOE (including its internal structure) and its immediate environment.

Figure 2-2 TOE structure



As shown in the figure, at least three nodes are required for TOE reliability deployment. The nodes are connected through the management network and data network. GaussDB 200 uses the Share-nothing architecture and consists of multiple independent nodes that do not share system resources such as CPUs, memory, and storage. Service data is stored on more than one physical node in the shared-nothing architecture system and data analysis tasks are assigned for execution in locations near the data storage locations. A considerable amount of data is processed in coordination with a control module, which enables rapid data processing responses.

The TOE consists of the following subsystems:

Kernel Subsystem provides interfaces for external applications, authorizes and authenticates external requests, optimizes global execution plans, distributes the execution plans to Datanode instances, stores service data, executes data query tasks, and returns execution results.

Cluster Management Subsystem provides management interfaces and tools for routine cluster **O&M** and configuration management. It manages and monitors the running status of functional units and physical resources in the distributed system, ensuring stable running of the entire system.

2.4.2 Physical Scope

This TOE is a software-only TOE and physically consists of GaussDB 200 packages and related guidance documents, as described in the following table. These software packages and guidance documents are provided in the DVD-ROM.

2.4.2.1 TOE Binary

The TOE Binary is a database server program named gaussdb in **GaussDB_200_6.5.1_SLES.tar.gz** package and its patch **GaussDB_200_6.5.1_SUSE-64bit.tar.gz** provided in the DVD-ROM.

File Name	SHA256 Value
GaussDB_200_6.5.1_SLES.tar.gz	f3790bf3d37521f2aaa13f05bfb2ee52717bf057b7a8382f2dc3a2d729391f0a
GaussDB-200-6.5.1-SUSE-64bit.tar.gz	88a06b27aa5b8e77ed2013dec8cce91bcc70aec17a70c780d1156dc8cf92f13e
GaussDB_200_6.5.1_SLES.tar.gz.asc	-

In addition, the DVD-ROM includes a set of packages necessary to install the TOE:

File Name	SHA256 Value
FusionInsight_BASE_6.5.1_SLES.tar.gz	6b4b69b2588994f616e15c31c61241f8e738b8a66860b27f429df6a8a625f9c7
FusionInsight_Manager_6.5.1_SLES.tar.gz	96f6f55f087aa446aaa21ab00f6eb1aeddcaee2055ee1855bc0173a3b4a1257a
FusionInsight_SetupTool_6.5.1_SLES.tar.gz	e6a5936c4bdfedb523a422633ff806d760b9f7acbe1f505e3ff019419a3fd4da

2.4.2.2 TOE Guide

The following product guidance documents are provided with the TOE. The documents are available to download from the DVD-ROM.

Table 2-2 TOE Guide

Document Name	SHA256 Value	Version
GaussDB 200 6.5.1 Product Documentation 09.pdf	ffa61309d2580c184867fb1265700aa344d42779a3ce07cdd0b2485b812ce93b	V09
GaussDB 200 6.5.1 Administrator Guide 02.pdf	e32d5b4009b31bfe3fff343b17313a1c7873f4832fb62ab7154224f28533f2af	V02
GaussDB 200 6.5.1 Capacity Adjustment Guide 05.docx	a767e08cbd71c603b20103eb04d092b0f55ce0e18daacdbbaf52cae989071ef4	V05
GaussDB 200 6.5.1 Communication Matrix 02.xlsx	ebf6c07685a2c5fdd8eee423675c70880e41b9217c7f3ea69dfb1cb82c72fcd6	V02
GaussDB 200 6.5.1 Developer Guide 08.pdf	fad4167fc2e38f3d177006c632131926988c7612b5ff23c7d9c8742d1f7a7624	V08
GaussDB 200 6.5.1 Health Check Guide 01.pdf	ac39348a3aa5e8ac01159d2cb460131f3b261ffe7343ea9414bba5193725cf7e	V01
GaussDB 200 6.5.1 Security Hardening Guide 01.pdf	88857ed642b4f5a3e8de303a3578706e9b7383d4a327839bcc4a6c6045bcb282	V01
GaussDB 200 6.5.1 Security Maintenance Guide 01.pdf	5c085317e28a4ed8646756eadeff78d154b223cb63447c39ea5ab5f0a3877faf	V01
GaussDB 200 6.5.1 Software Installation 03.pdf	ea1ca758a453d584c1f841c71645a18964da26f92884d9333c0a4f00d8d2cd5e	V03
HUAWEI GaussDB 200 6.5.1 AGD_OPE V0.6.pdf	3673113836f215f39252dab3bc6acbf4393099942eb113f2da977a685ba35ae3	V06
HUAWEI GaussDB 200 6.5.1 AGD_PRE V0.7.pdf	8f086c3933cc5c26f43a53db246a0bd3db08f449453a723b6610d1abcdfd0d45	V07

Note: the main document to start the installation is the *HUAWEI GaussDB 200 6.5.1 AGD_PRE V0.7.pdf*

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 2-3 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 user, the object being accessed, event type or success or failure of the operation.
User Data Protection	The TOE provides a discretionary access control policy to provide access control between users and database objects (such as tables, columns, views, triggers, functions, and procedures) or metadata. Residual Information Protection (RIP) is used to ensure that the previous content of a resource is no longer available once the resource is allocated to a table, row, or other database object.
Identification and Authentication	Users must be identified and authenticated prior to TOE access. Authentication modes are configured to implement the access control policy.
Security Management	The TOE provides the management function by executing SQL statements on the client and using server tools. The management function allows administrators to configure audit and access control options (including granting and revoking permissions), and the security attributes of users and roles.
Protection of the TSF	The TSF is protected through backup and restoration solutions and data reliability assurance mechanisms, ensuring fault recovery consistency and replication consistency.
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

Function	Description
	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 with the following characteristics.

Table 2-4 Hardware and software requirements for each server

Type	Requirement
TOE	"**GaussDB_200_6.5.1_SLES.tar.gz**". The TOE Binary is a database server program named **gaussdb** in the package labelled as "**GaussDB_200_6.5.1_SLES.tar.gz**" "GaussDB-200-6.5.1-SUSE-64bit.tar.gz" The TOE patch.
Server Nodes	2 Control Management nodes 1 Data node
TOE operation mode	OPEN mode (see section 3 Operation Mode of *Huawei GaussDB 200 6.5.1 AGD_OPE v0.6*)
CPU	x86_64 Dual socket 24 cores Intel processor 2.6 GHz
Memory	256 GB.
Hard disk	1.2 TB disk space.
OS type and version	SUSE Linux Enterprise Server 12 (SUSE 12) SP3, x86_64
Software	Python v2.7.5
Clients	gsql 6.5.1, JDBC, ODBC
Server Tools	All tools listed in section 7.3 of *GaussDB 200 6.5.1 Product Documentation 09.pdf*)
Firewall	Protection of the TOE interfaces (see section 6.7 Configuring Firewalls of *Huawei GaussDB 200 6.5.1 AGD_PRE v0.7*)

3 Conformance Claims

This Security Target is [CC] Part 2 extended and Part 3 conformant, with a claimed Evaluation Assurance Level of EAL 2, 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.

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.
- Attacker: 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.

4.2.2 Assets

The TOE maintains confidentiality and integrity of two types of data which represent the assets: the user data and TSF data.

User data is the main asset, including:

- The user data stored in or as database objects;
- The definitions of user databases and database objects, commonly known as DBMS metadata;
- User-developed queries or procedures that the DBMS maintains for users.

The secondary assets comprise the TSF data that the TOE maintains and uses for its own operation. It specifically includes:

- Configuration parameters,
- User security attributes,
- Security audit instructions and records.

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

Threat	Definition
	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 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 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

Assumption	Description
	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_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.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: **T.ACCESS_TSF DATA**	A threat agent may read or modify TSF data using functions of the TOE without the proper authorization.	
Objective	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.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.TOE_ACCESS	The TOE will provide functionality that controls a user's logical access to user data and to the TSF.
Rationale	O.I&A supports 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.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 diminishes this threat since information contained in protected resources will not be easily available to the threat agent through reallocation attacks. O.TOE_ACCESS diminishes this threat since it makes it more unlikely that a threat agent has access to the TOE.	

Threat: **T.ACCESS_TSF FUNC**	A threat agent may use or manage TSF, bypassing the protection mechanisms of the TSF.	
Objective	O.ADMIN_RO	The TOE will provide a mechanism (e.g. a "role") by

	LE	which the actions using administrative privileges may be restricted.
	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.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.TOE_ACCESS	The TOE will provide functionality that controls a user's logical access to user data and to the TSF.
Rationale	O.ADMIN_ROLE diminishes this threat by providing isolation of privileged actions. 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 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 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 diminishes this threat since it makes it more unlikely that a threat agent has access to the TOE.	

Threat: **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.	
Objective	O.I&A	The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.
	O.MEDIATE	The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.

	O.TOE_ACCESS	The TOE will provide functionality that controls a user's logical access to user data and to the TSF.
Rationale	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 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 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 generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE.	

Threat: **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.	
Objective	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.I&A	The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.
	O.MEDIATE	The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.
	O.TOE_ACCESS	The TOE will provide functionality that controls a user's logical access to user data and to the TSF.
Rationale	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 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 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 diminishes this threat by controlling logical access to user data, TSF data or TOE resources.

Threat: **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.	
Objective	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.
Rationale	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.	

Threat: **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.	
Objective	O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security relevant events associated with users.
	O.TOE_ACCESS	The TOE will provide functionality that controls a user's logical access to user data and to the TSF.
Rationale	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 diminishes this threat since controlled user's logical access to the TOE will reduce the opportunities for an attacker's access to configuration data.	

Threat: **T.UNAUTHORIZED_ACCESS**	A user may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.	
Objective	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.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.
Rationale	O.DISCRETIONARY_ACCESS diminishes this threat by requiring that data including TSF data stored with the TOE, have discretionary access control protection. 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 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 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 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: **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.	
Objective	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.
Rationale	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: **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.	
Objective	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.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 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 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.
Rationale	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 diminishes the threat by ensuring that remote trusted IT systems are sufficiently protected. 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 diminishes this threat by reducing the opportunities to subvert non TOE related capabilities in the TOE environment. OE.PHYSICAL diminishes the threat of a TSF compromise due to exploitation of physical weaknesses or vulnerabilities as a vector in an attack.	

Threat: **T.UNAUTHORIZED_ACCESS**	A user may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.	
Objective	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.
Rationale	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: **P.ACCOUNTABILITY**	The authorized users of the TOE shall be held accountable for their actions within the TOE.	
Objective	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 TOE will provide the capability to detect and create records of security relevant events associated with users.
	O.I&A	The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.
	O.TOE_ACCESS	The TOE will provide functionality that controls a user's logical access to user data and to the TSF.
Rationale	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 supports this policy by ensuring that audit records are generated. Having these records available enables accountability. 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 supports this policy by providing a mechanism for controlling access to authorized users.	

Policy: **P.USER**	Authority shall only be given to users who are trusted to perform the actions correctly.	
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.
	O.TOE_ACCESS	The TOE will provide functionality that controls a user's logical access to user data and to the TSF.
Rationale	O.MANAGE supports this policy by ensuring that the functions and facilities supporting the authorized administrator role are in place. O.TOE_ACCESS supports this policy by providing a mechanism for controlling access to authorized users.	

Policy: **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.	
Objective	O.ADMIN_ROLE	The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.
	O.TOE_ACCESS	The TOE will provide functionality that controls a user's logical access to user data and to the TSF.
Rationale	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 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: **P.ACCOUNTABILITY**	The authorized users of the TOE shall be held accountable for their actions within the TOE.	
Objective	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 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.
Rationale	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 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: **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.	
Objective	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.
Rationale	OE.ADMIN supports the policy by ensuring that an authorized administrator role for secure administration of the TOE is established.	

Policy: **P.USER**	Authority shall only be given to users who are trusted to perform the actions correctly.	
Objective	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 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.
Rationale	OE.ADMIN supports the policy by ensuring that the authorized administrators, responsible for giving appropriate authorities to users, are trustworthy. 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: A.AUTHUSER	Authorized users possess the necessary authorization to access at least some of the information managed by the TOE.	
Objective	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.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 logically protected

		equivalent to the TOE.
Rationale	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 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 supports this assumption by providing confidence that systems in the TOE IT environment contribute to a benign environment.	

Assumption: 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.	
Objective	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.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.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.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.
Rationale	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 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. 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 supports the assumption by ensuring that appropriate physical security is provided within the domain.	

Assumption: 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.	
Objective	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.
Rationale	OE.IT_I&A supports the assumption implicitly.	

Assumption: 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.	
Objective	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 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.
Rationale	OE.ADMIN 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 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: **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.	
Objective	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.
Rationale	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.	

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.	
Objective	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 logically protected equivalent to the TOE.
Rationale	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 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: 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.	
Objective	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.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.
Rationale	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 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: **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.	
Objective	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.
Rationale	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

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 PP, 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

The security functional requirements for this ST consist of the following components from Part 2 of the CC and extended components defined in Section 5, summarized in the following table.

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.1	Timing of authentication
	FIA_UID.1	Timing of identification
	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
	FMT_REV.1(1)	Revocation (user attributes)
	FMT_REV.1(2)	Revocation (subject, object

Class	Identifier	Name
		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	Additional Audit Record Content
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.1	Unsuccessful use of the authentication mechanism	None
FIA_UID.1	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	Additional Audit Record Content
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 **and group**] 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, any attribute]

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: the system administrator 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: administrators 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)

Application Note: *The identification and authentication family was written in such a way that the SFRs is used in the case that I&A services are performed by the TOE itself*

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: Attribute, 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
SUPER	NOSUPER	rolsuper(The default value is **f**, indicating false or nosuper.)	Determines whether the role is the initial system administrator with the highest permission.
INHERIT	NOINHERIT	rolinherit(The default value is **f**, indicating false or noinherit.)	Determines whether the role inherits permissions for this type of roles.
SYSADMIN	NOSYSADMIN	rolsystemadmin (The default value is **f**, indicating false or nosysadmin.)	Determines whether a new role is a system administrator.
AUDITADMIN	NOAUDITADMIN	rolauditadmin (The default value is **f**,	Determines whether a role has the audit and management attributes.

Attribute	Default Value	Field in the pg_authid System Table	Description
		indicating false or noauditadmin.)	
CREATEDB	NOCREATEDB	rolcreatedb (The default value is **f**, indicating false or nocreatedb.)	Defines a role's ability to create databases.
CREATEROLE	NOCREATEROLE	rolcreaterole (The default value is **f**, indicating false or nocreaterole.)	Determines whether a role can create new roles. A role with the **CREATEROLE** permission can also modify and delete other roles.
LOGIN	NOLOGIN	rolcanlogin (The default value is **f**, indicating false or nologin.)	Determines whether a role is allowed to log in to a database. A role having the **LOGIN** attribute can be considered as a user.
INDEPENDENT	NOINDEPENDENT	rolkind (The default value is **n**, indicating normal or noindependent.)	Defines private, independent roles. For a role with the **INDEPENDENT** attribute, administrators' rights to control and access this role are separated. Specific rules are as follows: ● Administrators have no rights to add, delete, query, modify, copy, or authorize the corresponding table objects without the authorization from the INDEPENDENT role. ● Administrators have no rights to modify the inheritance relationship of the INDEPENDENT role without the authorization from this role. ● Administrators have no rights to modify the owner of the table objects for the INDEPENDENT role. ● Administrators have no rights to delete the INDEPENDENT attribute of the INDEPENDENT role. ● Administrators have no rights to change the database password of the INDEPENDENT role. The INDEPENDENT role must manage its own password, which cannot be reset if lost. ● The **SYSADMIN** attribute of a user cannot be changed to the **INDEPENDENT** attribute.
CONNECTION	-1	rolconnlimit	Indicates how many concurrent connections the role can make. The

Attribute	Default Value	Field in the pg_authid System Table	Description
LIMIT			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.
CATUPDATE	NO CATUPDATE	rolcatupdate(The default value is **f**, indicating false or nocatupdate.)	Determines whether the role can update system tables directly. Only the initial system administrator has this permission.
REPLICATION	NOREPLICATION	rolreplication(The default value is **f**, indicating false or noreplication.)	Determines whether the role can be replicated.
RESPOOL	default_pool	rolrespool	Indicates resource pool that a user can use
PARENTID	PG_AUTHID.rolparentid	rolparentid(It's the reference of PG_AUTHID.rolparentid)	Indicates OID of a group user to which the user belongs
CONFIG	-	rolconfig(The default value is emtpy.)	Indicates role-specific session defaults for runtime configuration variables
OID	PG_AUTHID.oid	Oid(It's the reference of pg_authid.oid)	Indicates ID of the role
USEFT	NOUSEFT	roluseft(The default value is **f**, indicating false or nouseft.)	Determines whether the role can perform operations on foreign tables
NODEGROUP	-	nodegroup(The default value is emtpy.)	Indicates name of the logical cluster associated with the role. If no logical cluster is associated, this column is left empty.

7.2.3.2 FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1 The TSF shall allow [assignment: no actions] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 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.1 Timing of Identification

FIA_UID.1.1	The TSF shall allow [assignment: no actions] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	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 the first column of Table 7-3].
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 the second column of Table 7-3 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 the behalf of users: [assignment: The changer has required permissions and changes the attributes by running ALTER ROLE. a) A subject having the initial administrator role can modify any user security attributes of any roles. b) Users having the SYSADMIN attribute can modify any user security attributes of other roles, excluding the initial administrator. c) Users with the CREATEROLE attribute can modify the security attributes of other roles or delete the roles, excluding the initial administrator and roles having the SYSADMIN security attribute.].
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.]

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].

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 *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

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

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 management functions: [assignment:

a) management of the events to be audited;

b) granting or revoking of system permissions;

c) granting or revoking of object permissions;

d) changes to user accounts (including authentication) and roles;

e) configuration of the maximum number of concurrent sessions for an individual user; and

f) 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						

-	O.ADMIN_ROLE	O.AUDIT _GENERATION	O.DISCRETIONARY_ACCESS	O.I&A	O.MANAGE	O.MEDIATE	O.RESIDUAL_INFORMATION	O.TOE_ACCESS
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.1				X				
FIA_UID.1				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:	The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.

O.ADMIN_ROLE		
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_ACCES**	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

S	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.1	Timing of authentication
	FIA_UID.1	Timing of identification
	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.1, FIA_UAU.1]. 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_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.

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_ACCESS**	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

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.1
FAU_SEL.1	FAU_GEN.1 FAU_MTD.1	Satisfied by FAU_GEN.1 Satisfied by FAU_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.1	FIA_UID.1	Satisfied by FIA_UID.1
FIA_UID.1	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.1
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

Security Functional Requirement	Dependency	Description
		confidentiality and integrity of the transmitted data.
FTA_MCS.1	FIA_UID.1	Satisfied by FIA_UID.1
FTA_TSE.1	None	N/A

7.5 Security Assurance Requirements

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw reporting procedures (ALC_FLR.2). This is the assurance level described in the claimed PP.

The TOE type is a database management system and it is consistent with the TOE type required in Protection Profile for Database Management Systems (Base Package), Version 2.12 dated March 23rd, 2017, (“DBMS PP”).

7.5.1 Security Assurance Requirements Rationale

The following table lists the security assurance requirements.

Table 7-6 Security assurance requirements

Assurance Class	Assurance Component	
	Identifier	Name
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Lifecycle support	ALC_CMC.2	Usage of a Configuration Management (CM) system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Security Target	ASE_CCL.1	Conformance claims

Evaluation	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability evaluation	AVA_VAN.2	Vulnerability analysis

8 TOE Security Summary

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** parameter specifies whether to enable the audit log 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 gs_guc log. gs_guc log is located in $GAUSSLOG/bin/gs_guc/gs_guc-yyyy-mm-dd_xxx-current.log.
- After the audit function is enabled, each audit item takes effect only if its corresponding audit function is enabled. 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, and recovery are audited. **audit_grant_revoke** controls whether user rights granting and reclaiming are audited. **audit_system_object** controls whether DDL operations on database objects, such as CREATE, ALTER, and DROP, are audited. **audit_dml_state** and **audit_dml_state_select** control whether DML operations on tables are audited. **audit_dml_state_select** controls whether SELECT operations are audited.
- The startup and shutdown of the database are recorded in operation logs. The operation logs are stored in $GAUSSLOG/om/gs_om-xxxx.log by default.
- The audit item audit_database_process control whether database startup and stop. Its default value is 1, indicating that the database startup and stop audit function is enabled. The audit logs can be viewed through “SELECT * FROM pgxc_query_audit(starttime, endtime) where type = 'system_start' or type = 'system_stop';”

Audit 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, supporting two backup types, multiple backup and restoration solutions, and data reliability assurance mechanisms. This mechanism requires that the transaction logs of all transactions be written to the log files of both the primary and standby instances of the Datanode before the transactions are committed. In addition, the redo log data must be available in at least one instance of the Datanode. When a primary/standby switchover occurs in the TOE, the original standby Datanode instance becomes the primary one. In this case, the new primary Datanode instance in the TOE writes redo logs to its corresponding secondary Datanode instance to ensure data consistency.

In addition, the TOE is a distributed architecture (this not means that is a distributed TOE). It uses the two-phase commit protocol to ensure data consistency among all instances. If a transaction fails to be executed on one or more Datanode instances, the transaction must be rolled back on all Datanode instances to ensure data consistency.

The TOE adopts a distributed architecture, and the two-phase commit of the transaction guarantees the coordinated operation of each Coordinator and Datanode, thereby ensuring data consistency.

The scenario is as follows:

DDL transactions are sent to each Datanode through the Coordinator. Normally, the Coordinator waits for all Datanodes to return the transaction execution results (stage one). If all the Datanodes return successful execution, the Coordinator notifies all Datanodes to submit transactions, and the Coordinator continues to wait for all The result of the Datanode transaction submission (stage two). If all of them return a successful submission, the DDL transaction data is consistent on all Coordinators and Datanodes. Regardless of phase one or phase two, if one Datanode fails to return, or does not respond, the Coordinator will notify all Datanodes to perform transaction rollback, and eventually the data is consistent on all Datanodes.

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 the 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.

- The audit item audit_database_process control whether database startup and stop. Its default value is 1, indicating that the database startup and stop audit function is enabled. The audit logs can be viewed through “SELECT * FROM pgxc_query_audit(starttime, endtime) where type = 'system_start' or type = 'system_stop';”

When the overall audit switch audit_enabled is set to be on (default value), the overall audit function takes effect immediately. Each audit item has an independent switch. 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. Audit logs are recorded in the $GAUSSLOG/pg_audit/cn-xxxx/xx_adt.

FAU_GEN.1.2

Each audit record contains the date and time of the event, event type, entity ID, event result, and additional information in the third column of Table 7-2.

FAU_GEN.2.1

Each audit record contains a user name so that each auditable event can be associated with the user that causes the event. 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 set.

FAU_SEL.1.1

Each audit record contains the following fields: event date and time, event type, event result, user name, database name, client connection information, object name, node name, thread ID, local port, and remote port. You can filter required audit records from audit logs based on the information.

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, and DELETE. 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

Once a resource is allocated to a table, row, or other database object, the previous content of that resource is no longer available. RIP is implemented by performing "read before write". A space with the size of a row is allocated during data insert or update. The new value is written to the allocated space. Data storage and retrieval depend on indexes and links, and users cannot access unallocated disk space.

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 role 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**, **AUDITADMIN**, and **CREATEROLE**) 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.1.1, FIA_UAU.1.2, FIA_UID.1.1, FIA_UID.1.2

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 path of pg_hba.conf can be found using cm_ctl query -Cvd, which is the same as the data directory of the node instance.

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

Table 8-1 Authentication modes

Authentication Mode	Description
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.

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) The initial administrator can modify any user security attributes of any roles.

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

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

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.1, FIA_UID.1, 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 parameters and audit levels.

FMT_REV.1.1(1), FMT_REV.1.2(1)

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.1.1(2), 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:

a. Management of the events to be audited

b. Changes to system permissions (granting or revoking)

c. Changes to object permissions (granting or revoking)

d. Changes to user accounts (including changes to the settings of authentication parameters) and roles

e. Configuration of the maximum number of concurrent sessions for a user

f. IP address whitelist and IP address blacklist

FMT_SMR.1.1, FMT_SMR.1.2

Security management maintains authorized administrators, database users, and other roles defined by authorized administrators. A user having the administrator role 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 TSF

FPT_TRC.1.1, **FPT_TRC.1.2**

Backup and restoration are a collection of concepts, procedures, and strategies to protect data loss caused by invalid media or misoperations. For database security purposes, the TOE can back up and restore management and user data in the system, supporting two backup types, multiple backup and restoration solutions, and data reliability assurance mechanisms. This mechanism requires that the transaction logs of all transactions be written to the log files of both the primary and standby instances of the Datanode before the transactions are committed. In addition, the redo log data must be available in at least one instance of the Datanode. When a primary/standby switchover occurs in the TOE, the original standby Datanode instance becomes the primary one. In this case, the new primary Datanode instance in the TOE writes redo logs to its corresponding secondary Datanode instance to ensure data consistency.

In addition, the TOE is a distributed architecture. It uses the two-phase commit protocol to ensure data consistency among all instances. If a transaction fails to be executed on one or more Datanode instances, the transaction must be rolled back on all Datanode instances to ensure data consistency.

Table 8-2 Data types

Data Type	Backup Content
Management data	Database data (excluding alarm data) and configuration data in the cluster management system User information (about usernames, passwords, keys, password policies, and user groups)
User data	Cluster-level and table-level full backup and cluster-level incremental backup

Database administrators can design, implement, and manage backup and restoration policies. Backup and restoration can be logical and physical, as shown in the following table.

Table 8-3 Backup and restoration types

Backup and Restoration Type	Description
Logical backup and restoration	Backs up data by logically exporting it. This method dumps data that is backed up at a certain time point, and can restore data only to this backup point. A logical backup does not back up data processed between failure occurrence and the last backup. It applies to scenarios where data rarely changes. Such data damaged due to misoperation can be quickly restored using a logical backup.
Physical backup and restoration	Copies physical files, copying data in the unit of disk blocks from the primary instance to the standby to back up a database. Files, such as data files and archive log files that have been backed up, can be restored.

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 **800**. 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 this 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, and the maximum number of connections allowed by the server node in the **pg_hba.conf** file. The TSF can determine whether to allow session establishment based on the start time and end time of the role validity period 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, 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,

Term	Description
	to perform functions and access data.
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.

Term	Description
Public Object	An object for which the TSF unconditionally permits all entities "read" access. Only the TSF or authorized 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

Acronym	Definition
GUI	graphical user interface
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

