Security Target of Huawei GaussDB 100

V300R001C00B300

Issue 0.6

Date 2020-10-10

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: http://www.huawei.com

Email: support@huawei.com

Contents

1 About This Document

Overview

This document describes Security Targets (STs).

Change History

Date	Version	Updated Section	Description	Owner
2019-02-11	0.1	All	This is the first draft.	Huawei Technologies Co., Ltd.
2019-07-05	0.2	All	Refresh according to review opinion	Huawei Technologies Co., Ltd.
2019-09-22	0.3	All	Refresh according to review opinion	Huawei Technologies Co., Ltd.
2019-10-24	0.4	All	Refresh according to review opinion	Huawei Technologies Co., Ltd.
2020-05-29	0.5	All	Refresh according to review opinion	Huawei Technologies Co., Ltd.
2020-10-10	0.6	All	Refresh according to observation report	Huawei Technologies Co., Ltd.

2 ST Introduction

2.1 ST Identification

ST title: Security Target of Huawei GaussDB 100 V300R001C00B300

Version: 0.6

Date: 2020-10-10

Developer: Huawei Technologies Co., Ltd.

2.2 TOE Identification

Name: Huawei GaussDB 100 V300R001C00B300

Version: V300R001C00B300 Release 3da6647

Developer: Huawei Technologies Co., Ltd.

2.3 TOE Overview

2.3.1 TOE Type

GaussDB 100 is a relational database management system (RDBMS) from Huawei Corporation. The system is built around a relational database framework in which data objects may be directly accessed by users, or an application front end, through structured query language (SQL). GaussDB 100 is a database architecture typically used by global enterprises to manage and process data across wide and local area networks.

2.3.2 TOE usage and major security feature

The product type of the TOE described in this ST is a database management system (DBMS) with the capability to limit TOE access to authorized users, enforce Discretionary Access Controls (DAC) on objects under the control of the database management system based on user and/or role authorizations, and to provide user accountability via audit of users' actions.

The security functionality in GaussDB 100 includes:

Security auditing: Configurable audit capture.

User data protection: DAC is based on object and system privileges, as well as roles.

User identification and authentication: Identification and identity authentication are performed before users are allowed to access database objects. On login, the user identity is associated with role and privilege information that is used to make access control decisions.

Security management: The security functionality associated with audit, access control, and user accounts are provided through the SQL command line interface (**zsql**), JDBC interface and ODBC interface.

Protection of the TOE Security Functionality (TSF): Consistent replication. The content of a database may be replicated to another server, with assurances that the consistency of the data is maintained.

TOE access: The number of concurrent user sessions may be limited by policy. Information on successful and unsuccessful login attempts is collected and user login may be restricted based on user identities, IP addresses, and dates.

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:

- CPU (higher than 4 cores and 2.0 GHz)
- Memory (8 GB or larger)
- Hard disk (at least 25 GB disk)

The operating system (OS) (EulerOS Server V2.0SP3 (EulerOS), x86_64) is also out of scope and thus not included in the TOE. In addition, the TOE can be executed in other supported OSs (that are not included under the Common Criteria Certificate):

- Red Hat Enterprise Linux Server release 7.4(Red Hat), x86_64
- SUSE Linux Enterprise Server 12.4 (SUSE 12), x86_64
- EulerOS Server V2.0SP3 (EulerOS), x86_64
- EulerOS Server V2.0SP5 (EulerOS), x86_64
- EulerOS Server V2.0SP8 (EulerOS), ARM_64

The Software of JDK 8u144 is also out of scope and thus not included in the TOE.

The Software of Python v2.7.5 is also out of scope and thus not included in the TOE.

The Software of Putty v0.73 is also out of scope and thus not included in the TOE.

The Software of UnixODBC-2.3.7 is also out of scope and thus not included in the TOE.

2.4 TOE Description

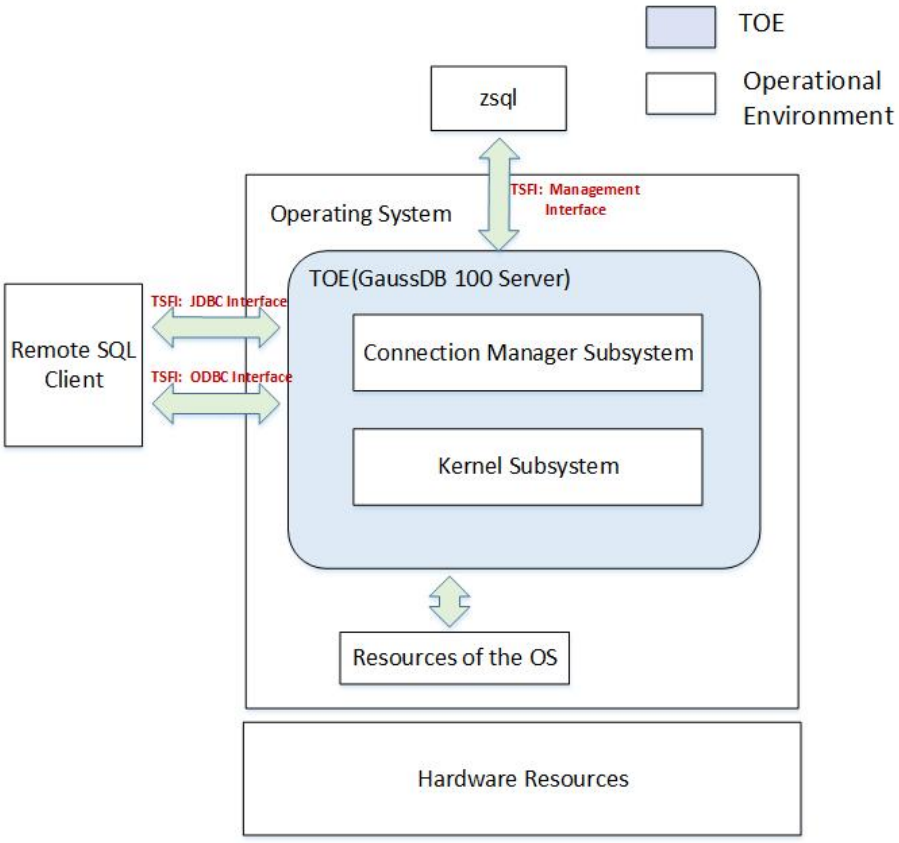
This chapter provides an architectural overview of the Huawei GaussDB 100 V300R001C00B300 Release 3da6647 including a detailed description of the software architecture, the definition of the TOE subject to evaluation and a summary of security functions provided by the TOE.

2.4.1 TOE Environment

Huawei GaussDB 100 V300R001C00B300 Release 3da6647 supports two physical deployment modes. Figure 2-1 shows the client server database configuration, and Figure 2-2 shows the primary and standby database configuration. Configuration of Figure 2-2 is going to be used in the evaluated configuration.

2.4.1.1 Client Server Database Configuration

Figure 2-1 Client server database configuration



As shown in Figure 2-1, the deployment of client and server consists of the following units:

- **Remote SQL Client** (Non-TOE) can access GaussDB 100 server through JDBC interface or ODBC interface, and perform SQL operations and database management operations.

- **zsql** (Non-TOE) accesses GaussDB 100 server through the management interface and performs SQL operations and database management operations.
- **GaussDB 100 Server** (TOE) is mainly responsible for processing operation requests sent by JDBC interface, ODBC interface and Management interface, and returning the data processing results to Remote SQL Client and zsql, and it includes the following units:

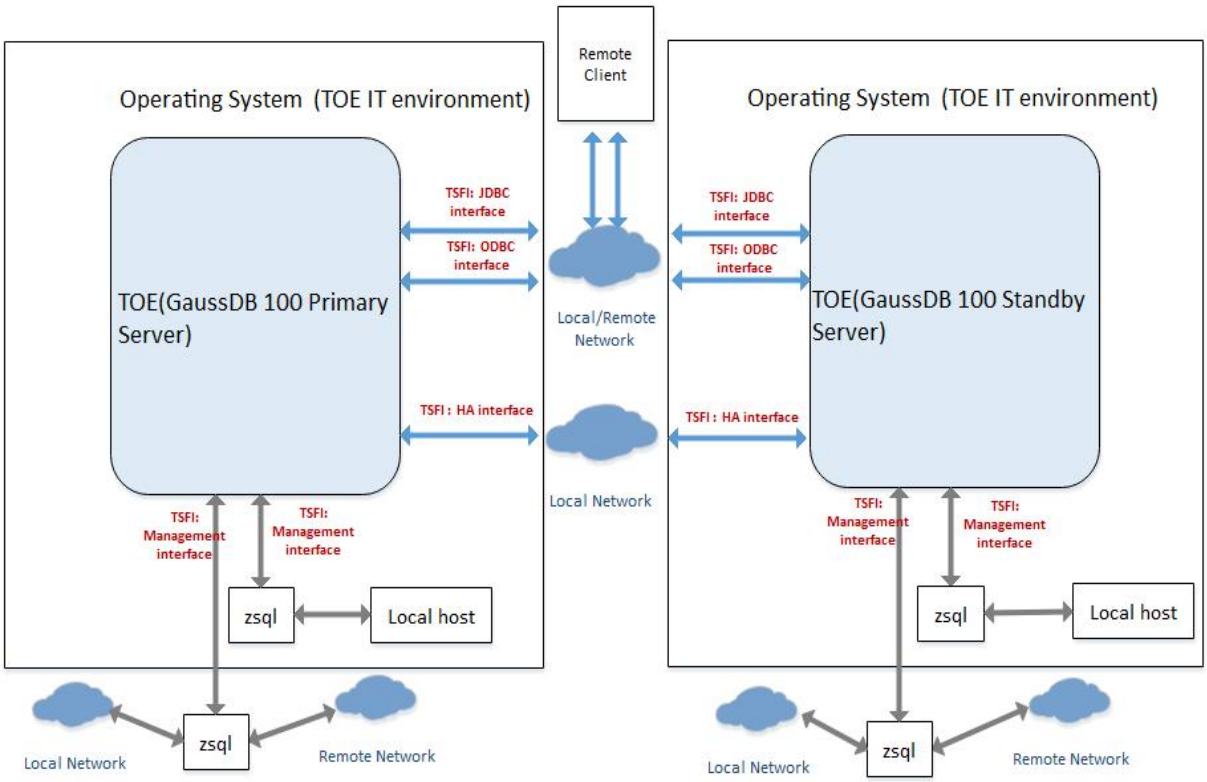
Connection Manager Subsystem, which establishes service monitoring, initializes the thread pool and memory, and opens the control file and data files.

Kernel Subsystem, which consists of the SQL engine and storage engine. The SQL engine parses and compiles SQL statements, checks permissions to determine whether a user associated with a request can execute a statement, optimizes the query, generates and caches the query plan, and run the statement. The storage engine is responsible for physical and logical storage management of data, and implements core mechanisms, such as data access, metadata, transaction atomicity, consistency, isolation, durability (ACID), flush, and concurrency control.

- **The Operating System** (Non-TOE) hosts the TOE. As the TOE is software only it lives as a process in the Operating System (OS) and uses **the resources of the OS** like the memory management features.
- **Hardware Resources** (Non-TOE) refers to the hardware resources required for TOE operation, including CPU, memory and hard disk resources. See Table 2-1.

2.4.1.2 Primary and Standby Database Configuration

Figure 2-2 Primary and standby database configuration



As shown in Figure 2-2, it differs from Figure 2-1 in that two database servers are deployed, which is a highly reliable deployment mode. when the primary server fails, the standby server can take charge of the primary server to provide database services. The primary server can provide database services to Remote SQL Client, it connects the standby server through HA interface, and the content of the primary server will be replicated to standby server, with assurances that the consistency of the data is maintained.

2.4.2 Physical Scope

The GaussDB 100 is a software-only TOE, the physical scope of the TOE includes TOE Binary and TOE Guides.

2.4.2.1 TOE Binary

The main package that is contained in the DVD-ROM delivered to the customer by a transport shipment company is "GAUSSDB100-V300R001C00B300-EULER20SP3-64bit_release.tar.gz". And the TOE Binary is a database server program named **zengine** in the package labelled as "GAUSSDB100-V300R001C00B300-DATABASE-EULER20SP3-64bit.tar.gz" that is contained in the main package.

2.4.2.2 TOE Guides

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

Table 2-1 SHA256 of TOE guides

Documents Name	SHA256 Value
AGD_PRE of Huawei GaussDB 100 V300R001C00B300 V0.5.doc	5E214668D59B2E245002B5563636466C93F353DFD63BF8B5508BBC1A7F0F8B2F
AGD_OPE of Huawei GaussDB 100 V300R001C00B300 V0.5.doc	345EE25A930B79491C74CD065A9DCA264BBC09582433AEE09F27129EC3D619B1
GaussDB 100 V300R001C00B300 Feature Description 03.pdf	FD54E2F2C64745B63F56C265C74F75D9A56A8F18BD85065AB17E7666F9FFDF86
GaussDB 100 V300R001C00B300 Product Description 03.pdf	AAD41993F7DC3A4F69704655606B357A2C167C7BB9F6759C138B5C52F4E113DE
GaussDB 100 V300R001C00B300 R&D Documentation 06.pdf	43886F33B6C8D9B73E922AE2779BE8A4F720D740E4FF757C705DAAE7B040A263
GaussDB 100 V300R001C00B300 Security Hardening Guide 04.pdf	D8C7F3D5C6E3D27E4EAEA20AE70D4CE99C32D8C9110BAFE62A68EFE8C3402149
GaussDB 100 V300R001C00B300 Security Maintenance Guide 03.pdf	012A17C976E732FF19A8E3D16B3379B449D2629D54BACEC67CF263A60DC675BD
GaussDB 100 V300R001C00B300 Security Technical White Paper 03.pdf	56560FB470DA65EFD77FE1B18AB2F324957290BFE9B566246421061BBD7D3FF5
GaussDB 100 V300R001C00B300 User Guide 05.pdf	03FE43963A2BB544DA957327D9F0FB2D379108E2E78C4D911500A96983CE46CE

2.4.3 Logical Scope

The logical scope of the TOE contains all interfaces and functions within the physical scope. The following table describes the logical scope.

Table 2-2 TOE logical scope

Function Item	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 fine-grained access

Function Item	Description
	control between users and database objects. Once data is allocated to a resource, the previous information content is no longer available.
User Identification and Authentication	Users must identify and authenticate prior to TOE access. Attributes are maintained to support the access control policy.
Security Management	The TOE provides management capabilities via SQL statements. Management functions allow the administrators to configure auditing and access control options (including granting and revoking privileges), configure users (including the maximum number of concurrent sessions) and roles, and configure primary and standby options.
Protection of the TSF	The database supports maximum protection mode, which ensures that data is consistently replicated to a secondary DBMS server without losing any data.
TOE Access	The number of concurrent user sessions may be limited by policy. Information on successful and unsuccessful login attempts is collected and user login may be restricted based on user identities, dates, and IP addresses.

2.4.4 TOE Evaluated Configuration

The following OS and hardware components are required for operation of the TOE in the evaluated configuration.

Table 2-3 Hardware and software

Type	Requirement
TOE	"GAUSSDB100-V300R001C00B300-EULER20SP3-64bit_release.tar.gz". And the TOE Binary is a database server program named **zengine** in the package labelled as "GAUSSDB100-V300R001C00B300-DATABASE-EULER20SP3-64bit.tar.gz"
TOE configuration	Primary and Standby Database Configuration.
TOE operation mode	OPEN mode.
CPU	72 cores and 2.0 GHz.
Memory	512 GB.

Type	Requirement
Hard disk	1.9 TB disk space.
OS type and version	EulerOS Server V2.0SP3 (EulerOS), x86_64
Software	JDK 8u144 as a JDBC client Python v2.7.5 Putty v0.73 UnixODBC-2.3.7 as an ODBC client

3 Conformance Claim

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 web site as a validated protection pro-file (certification ID BSI-CC-PP-0088-V2). See [BSI- PP] for more information.

4 TOE Security Problem Definition

The security problem definition consists of the threats to security, organizational security policies, and usage assumptions. The threats, policies and assumptions are copied from the Protection Profile for Database Management Systems (Base Package), Version 2.12 dated March 23rd, 2017, ("DBMS PP").

4.1 IT assets to be protected

4.1.1 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.

4.1.2 Assets

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

4.2 Threats

The following threats are identified and resolved by the TOE and should be read with 5.3 Security Objectives Rationale.

The conformant TOE will provide security functions to resolve the threats to the TOE and enforce laws or regulations.

Table 4-1 Threats to the TOE

Threat	Definition
T.ACCESS_TSFDATA	A threat agent may read or modify TSF data using functions of the TOE without the proper authorization.
T.ACCESS_TSFFUNC	A threat agent may use or manage TSF, bypassing the protection mechanisms of the TSF.
T.IA_MASQUERADE	A user or a process acting on behalf of a user may masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources.
T.IA_USER	A threat agent may gain access to user data, TSF data, or TOE resources with the exception of public objects without being identified and authenticated.
T.RESIDUAL_DATA	A user or a process acting on behalf of a user may gain unauthorized access to user or TSF data through reallocation of TOE resources from one user or process to another.
T.TSF_COMPROMISE	A user or a process acting on behalf of a use 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.

4.3 OSP

Organizational Security Policies (OSPs) are a set of security rules, procedures, or guidelines imposed by an organization in operational environment. The following table describes the OSPs assumed to be imposed on TOE or its operational environment by the organization that implements the TOE in the Common Criteria (CC) evaluation configuration.

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.

4.4 Assumptions

This section contains assumptions regarding the IT environment in which the TOE will reside.

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.

Assumption	Description
A.TRAINEDUSER	Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.
Procedural aspects	
A.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration, and support of the DBMS.
A.PEER_FUNC_&_MGT	All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.
A.SUPPORT	Any information provided by a trusted entity in the IT environment and used to support the provision of time and date, information used in audit capture, user authentication, and authorization that is used by the TOE is correct and up to date.
Connectivity aspects	
A.CONNECT	All connections to and from remote trusted IT systems and between separate parts of the TSF are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.

5 Security Objectives

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 Objectives for the TOE

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.

Security Objective	Description
O.DISCRETIONARY _ACCESS	The TSF must control access of users to named resources based on identity of the user. The TSF must allow authorized users to specify for each access mode which users 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.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 access to user data and to the TSF.

5.2 Objectives for the Operational Environment

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

5.2.1 Operational Environment Security Objectives

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 Objective	Description
	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.
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.

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 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

Security Objective	Description
	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.

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													

-	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.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 rationale tracing the threats to the security objectives for the TOE and to the Operational Environment have been separated to provide consistency with the claimed PP.

5.3.1.1 Threats Mapped to Security Objectives for the TOE

Table 5-5 Threats mapped to security objectives for the TOE

Threat: T.ACCESS_TSFDATA	A threat agent may read or modify TSF data using functions of the TOE without the proper authorization.	
Objectives:	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	The TOE will ensure that any information contained

	_INFORMATION	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 mechanisms that control a user's logical access to user data and to the TSF.
Rationale:	O.I&A supports this policy by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE is defined to provide to authenticated users only. O.MANAGE 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_TSFFUNC**	A threat agent may use or manage TSF, bypassing the protection mechanisms of the TSF.	
Objectives:	O.ADMIN_ROLE	The TOE will provide a mechanism (e.g. a "role") by 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 mechanisms that control 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.	
Objectives:	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 mechanisms that control a user's logical access to user data and to the TSF.
Rationale:	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.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.

Objectives:	O.DISCRETIONARY_ACCESS	The TSF must control access of users to named resources based on identity of the user. The TSF must allow authorized users to specify for each access mode which users 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 mechanisms that control 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 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.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.	
Objectives:	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_COMP**	A user or a process acting on behalf of a use may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or

ROMISE	may compromise executable code within the TSF.	
Objectives:	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 mechanisms that control 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.UNAUTHOR-IZED_ACCESS**	A threat agent may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.	
Objectives:	O.DISCRETIONARY_ACCESS	The TSF must control access of users to named resources based on identity of the user. The TSF must allow authorized users to specify for each access mode which users 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 user 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 may masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources.	
Objectives:	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 use may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or may compromise executable code within the TSF.	
Objectives:	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	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 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.
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 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. OE.PHYSICAL supports the assumption by ensuring that appropriate physical security is provided within the domain.	

Threat: **T.UNAUTHOR-IZED_ACCESS**	A threat agent may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.

Objectives:	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 rationale tracing the OSPs to the security objectives for the TOE and to the Operational Environment have been separated to provide consistency with the claimed 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.	
Objectives:	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 mechanisms that control 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.	
Objectives:	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 mechanisms that control 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.	
Objectives:	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 mechanisms that control 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.	
Objectives:	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.USER**	Authority shall only be given to users who are trusted to perform the actions correctly.	
Objectives:	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.	

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.	
Objectives:	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.	

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 support 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 systems and relevant connectivity that form the platform for the TOE is vital to addressing the security problem, described in this ST and the PP. Managing these effectively using defined procedures is reliant on having competent administrators.	

Assumption: A.NO_GENER	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services

AL_PURPOSE	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 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.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:	It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets

A.PHYSICAL	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 are 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.TRAINED-USER**	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 Extended Components Definition

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

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).

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 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

Class	Identifier	Name
		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: *For the selection, select "no additional events".*

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	The identity of the authorized administrator that made the change to the audit configuration

Security Functional Requirement	Auditable Event	Additional Audit Record Content
	operating	
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
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	Identity of the individual attempting to establish a session

Security Functional Requirement	Auditable Event	Additional Audit Record Content
	mechanism	

7.2.1.2 FAU_GEN.2 User identity association

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

7.2.1.3 FAU_SEL.1 Selective audit

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

a) Object identity;

b) User identity;

c) [selection: "host identity"];

d) event type;

e) [success of auditable security events;

f) failure of auditable security events; and

g) [selection: [assignment: event date and time]].]

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:

Subjects: database users

Subject attributes: database role, system privileges

Objects: Database object

Object attributes: object privileges, object access control rules, object identities]

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, records, files, indexes, views, constraints, stored queries, and metadata. 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 may access an object if:

a. The user is the owner of the object or has been granted the specific object privilege,

b. The user has been granted specific system privileges and has been authorized for the realm;

c. The user is a member of a role that has been granted specific object and/or system privileges;

d. The object is accessible by the user 'PUBLIC'.]

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: no additional rules].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: no additional rules].

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: table, row].

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: object privileges, system privileges]].

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.*

7.2.3.2 FIA_UAU.1 timing of authentication

FIA_UAU.1.1 The TSF shall allow [assignment: no other 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 other 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 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: database user identifier, roles, privileges].

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: the session initially has all the security attributes of the user including user identifier, roles, privileges.].

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: granting and revoking of directly assigned privileges are effective immediately (except granting or revoking create session privilege)].

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: when a session is established, it also has the security properties of the system's default profile.].

7.2.4 Security Management (FMT)

7.2.4.1 FMT_MOF.1 Management of security functions 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

)	privileges, 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 privileges are effective 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 privileges] 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.1.2(2)	The TSF shall enforce the rules [assignment: a. authorized administrators and object owners may revoke object privileges; and b. object owners may grant other users privileges to grant and revoke object privileges].

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 privileges; c. granting or revoking of object privileges; d. Changes to user accounts (including authentication) and roles; e. configuration of data protection modes; f. configuration of the maximum number of concurrent sessions for an individual user; and g. configuration of the IP whitelist/IP blacklist].

7.2.4.8 FMT_SMR.1 Security roles

FMT_SMR.1.1	The TSF shall maintain the roles [authorized administrator and [assignment: base object creation role, connection role, 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. A ST or operational environment may contain a finer-grain decomposition of roles that correspond to the roles identified here (e.g., database non-administrative user or database operator). Here changes the names of the roles identified above but the "new" roles still perform the functions that the FMT requirements in the PP have defined.*

7.2.5 Protection of the TOE Security Functions (FPT)

Application Note: *The security domain boundary in the first element is TSF domain and its intent is to protect the TSF from untrusted subjects at the TSFIs. The security domain boundary in the second element covers the complete TOE Scope of Control and its intent is to maintain separation between any subjects within the TOE Scope of Control.*

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. the TSF could provide timely consistency through periodic broadcast of TSF data to all TSF nodes maintaining replicated TSF data.*

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 CC [REF 1b] para 473 allows that the default number may be defined as a management function in FMT, but here it is consistent with DBMS PP.*

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, and [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 7-3 Security functional requirements rationale

-	O.ADMIN_ROLE	O.AUDIT _GENERATION	O.DISCRETIONARY_ACCESS	O.I&A	O.MANAGE	O.MEDIATE	O.RESIDUAL_INFORMATION	O.TOE_ACCESS
FAU_GEN.1		X						
FAU_GEN.2		X						
FAU_SEL.1		X						
FDP_ACC.1			X			X		X
FDP_ACF.1			X			X		X
FDP_RIP.1							X	
FIA_ATD.1				X				X
FIA_UAU.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		

-	O.ADMIN_ROLE	O.AUDIT _GENERATION	O.DISCRETIONARY_ACCESS	O.I&A	O.MANAGE	O.MEDIATE	O.RESIDUAL_INFORMATION	O.TOE_ACCESS
FTA_MCS.1								X
FTA_TSE.1								X

7.3.1 SFR Rationale Related to Security Objectives

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

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

Security Objective: **O.AUDIT _GENERATION**	The TSF must be able to record defined security-relevant events (which usually include security-critical actions of users of the TOE). The information recorded for security-relevant events must contain the time and date the event happened and, if possible, the identification of the user that caused the event, and must be in sufficient detail to help the authorized user detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.	
Security Functional Requirement	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SEL.1	Selective audit
Rationale	FAU_GEN.1 defines the set of events that the TOE must be capable of	

	recording. This requirement ensures that the administrator has the ability to audit any security relevant events that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements an ST author adds to the ST. [FAU_GEN.1] FAU_GEN.2 ensures that the audit records associate a user and any associated group identity with the auditable event. In the case of authorized users, the association is accomplished with the user ID. In the case of authorized groups, the association is accomplished with the group ID. [FAU_GEN.2] FAU_SEL.1 allows the administrator to configure which auditable events will be recorded in the audit trail. This provides the administrator with the flexibility in recording only those events that are deemed necessary by site policy, thus reducing the amount of resources consumed by the audit mechanism. [FAU_SEL.1]

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

Security Objective: **O.I&A**	The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.	
Security Functional Requirement	FIA_ATD.1	User attribute definition
	FIA_UAU.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	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control

Requirement	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 other than those explicitly granted access to the data. [FDP_RIP.1]	

Security Objective: **O.TOE_ACCESS**	The TOE will provide mechanisms that control 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 7-4 Dependency rationale

Security Functional Requirement	Dependency	Description
FAU_GEN.1	FPT_STM.1	This requirement is satisfied by the assumption on the IT environment, given in A.SUPPORT.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Satisfied by FAU_GEN.1 Satisfied by FIA_UID.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	Satisfied by FDP_ACC.1 Satisfied by FMT_SMR.1

Security Functional Requirement	Dependency	Description
	FMT_SMF.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 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, because the TOE type is a database management system which introduced in section 2.3.1, 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”), so the TOE assurance requirements have been copied from 7.2 section of it.

7.5.1 Security Assurance Requirements Rationale

The following table lists the security assurance requirements.

Table 7-5 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
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
Security Target Evaluation	ASE_CCL.1	Conformance claims
	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

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

- GaussDB 100 writes certain operations performed by users on the database into audit logs (e.g. $GSDB_DATA/log/audit/zengine.aud). The **AUDIT_LEVEL** parameter specifies whether to enable the log audit function and whether to enable the audit of **DML**, **DDL**, **DCL**, or **PL** operations.

The **DML** level is used to audit the operation of insert, delete, select and alter data in database tables. The **DDL** level is used to audit the create or alter of objects in the database, such as tables, indexes, views, synonyms, databases, sequences, users, roles, table spaces, profiles, sessions, etc. The **DCL** level is used to audit setting or changing database transactions, user privileges, and lock table operations. The **PL** level is used to audit the execution of stored procedures.

The start-up and shutdown of the audit functions are recorded in the audit log.

- GaussDB 100 writes the database running information in the run log, if there is a fault during the running, examine the zengine.rlog file to locate the fault (e.g. $GSDB_DATA/log/run/zengine.rlog). The parameter _LOG_LEVEL specifies the level for logging, the default value is 7, it means the database will record the "**ERROR** + **WARNING** + **INFORMATION**" level of **RUN** log. see the _LOG_LEVEL parameter in Chapter 7.1.7.2 of *GaussDB 100 V300R001C00B300 User Guide 05*.
- Audit logs or run logs are recorded based on the auditable events described in the second column of Table 7-2 in *Security Target of Huawei GaussDB 100 V300R001C00B300 V0.6*. The following details should be noted:

a. To meet the auditing requirements of FPT_TRC.1 (that is, restoring consistency), restoration operations (such as rollforward and rollback) are performed and then recorded to

run logs upon database startup. When "recovery real end with file:x,point:y,lfn:z" recorded in the run log (e.g. $GSDB_DATA/log/run/zengine.rlog), it means the data corresponding to the log before the lfn z and the y point of the log x has been restored, the database has reached restoring consistency, at this time the _LOG_LEVEL parameter needs to be set to 7.

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 **SESSIONS** parameter, the login fails and run logs are printed to show that the number of connections exceeds the upper limit; if the number of user connections exceeds the value of the **SESSIONS_PER_USER** parameter, the login fails and an error code is returned to show that the number of connections exceeds the upper limit.

- The start-up of the database system and the shutdown of the database system are recorded in the zctl log (e.g. $GSDB_DATA/log/zctl-yyyy-mm-dd_xxx.log).
- When the audit level is adjusted to DCL level, the grant and revoke of all privileges include system and object privileges support recording audit logs.

FAU_GEN.1.2

- In each audit, the following information is audited: event date and time (event timestamp), event type (operation name), subject identity (user ID), audit event result and executed SQL statement (including database object name). The RETURNCODE in audit log reflects audit event outcome. A RETURNCODE of 0 indicates the success of the event, and a RETURNCODE of non-zero indicates the failure of the event. The meaning of the non-zero RETURNCODE can be found in Chapter 5 of the *GaussDB 100 V300R001C00B300 R&D Documentation 06.* RETURNCODE corresponds to the error code in Chapter 5 of the *GaussDB 100 V300R001C00B300 R&D Documentation 06.* For example, if the RETURNCODE is two digits xy, the corresponding error code is GS-000xy. The RETURNCODE is three digits xyz, and the corresponding error code is GS-00xyz.
- Audit logs are recorded based on the auditable events described in the third column of Table 7-2 in *Security Target of Huawei GaussDB 100 V300R001C00B300 V0.6*.

FAU_GEN.2.1

Each audit record in the audit log includes the user name so that each audit event can be associated with the identity of the user that caused the event.

FAU_SEL.1.1

In each audit, the following information is audited: event date and time (event timestamp), event type (operation name), subject identity (user ID), audit event result and executed SQL statement (including database object name). Based on this information, the audit records needed can be filtered from the audit log. In GaussDB, the audit log path can be customized to limit the maximum number and the maximum capacity of audit logs.

TOE security functional requirements addressed: 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 privileges 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. Access may be granted in one of the following ways:

a. Object privileges

Users having object privileges can perform various operations on database objects. The privileges include SELECT, INSERT, UPDATE, DELETE, INDEX, READ, REFERENCES, ALTER, and EXECUTE. The owner of an object has all the privileges for the object, and can grant all or part of the privileges (for example, read-only access) of the object to other users. For a list of database-supported object privileges, see Table 3-52 in Chapter 3.12.44 of *GaussDB 100 V300R001C00B300 R&D Documentation 06*.

b. System privileges

Users having system privileges can create, delete, modify, and query objects, and can perform other operations, such as login and authorization. The system administrator has all system privileges, and can grant or revoke privileges from other users. For a list of database-supported object privileges, see Table 3-51 in Chapter 3.12.44 of *GaussDB 100 V300R001C00B300 R&D Documentation 06*.

c. Privileges inheritance through a role

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

d. Object privileges granting through the **PUBLIC** user

PUBLIC is an internal user preset in the system. A common user has all the object privileges of the **PUBLIC** user by default. In this case, if a privilege is granted to **PUBLIC**, all database users will have this privilege.

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.

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

8.1.3 User Identification and Authentication

FIA_ATD.1.1

- To create a user, an administrator must provide a user account name and a password, and limitations on the resources available to the user. These limitations are specified in a profile. The profile associates the user with session limitations (for example, the number of concurrent sessions allowed) and password parameters (for example, the number of failed login attempts allowed before the account is locked).
- Users are granted privileges, such as the right to run a particular type of SQL statement, or the right to access an object that belongs to another user. Roles are created to group together privileges and other roles, making it easier to grant multiple privileges to a new user. A role must first be created by identifying the role, and then adding privileges. Once the role is defined, it may be granted to a user.
- In addition to granting object and system privileges to users through roles, these privileges may also be granted to users individually.

FIA_UAU.1.1 FIA_UAU.1.2 FIA_UID.1.1 FIA_UID.1.2

GaussDB 100 ensures that users are identified and authenticated prior to being allowed to access database objects or resources. Although several authentication mechanisms are supported, only local/remote username and password authentication is examined for the purposes of this evaluation.

FIA_USB_(EXT).2.1

When a user logging in to the database with client like zsql, the database will start a session. All the operations of this session on the database are actually the operations of the user on the database. So this session is the subject acting on the behalf of the user and it has the user's security attributes including user identifier, roles and privileges.

FIA_USB_(EXT).2.2

When the user successfully logs in to the database, the session is established, and initially has all the security attributes of the user including user identifier, the roles of the user and all the privileges of the user.

FIA_USB_(EXT).2.3

The operations of granting and revoking privileges take effect immediately (except granting or revoking create session privilege). Such operations include granting or revoking object or system privileges from a user, granting or revoking object or system privileges from a role, or granting roles to users or revoking the roles.

FIA_USB_(EXT).2.4

When the user successfully logs in to the database, the session is established, it not only has all the security properties of the user, but also has the security properties of the system's default profile.

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

8.1.4 Security Management

FMT_MOF.1.1

The TSF allows authorized administrators to enable or disable functions relating to events to be audited. For example, they can enable or disable audit logs and specify audit items by setting audit parameters.

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.1.1

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 privileges and roles. Revocation of directly assigned system privileges (i.e. system privileges granted directly to a user or a role) takes effect immediately.

FMT_REV.1.1(2) FMT_REV.1.2(2)

Authorized administrators and object owners may revoke object privileges. The ability to grant and revoke object privileges may also be granted to other users by an authorized administrator, or the object owner.

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. granting or revoking of system privileges;

c. granting or revoking of object privileges;

d. Changes to user accounts (including authentication) and roles;

e. configuration of data protection modes;

f. configuration of the maximum number of concurrent sessions for an individual user; and

g. configuration of the IP whitelist/IP blacklist.

FMT_SMR.1.1 FMT_SMR.1.2

Security management maintains authorized administrators, database users, and other roles defined by authorized administrators. Authorized administrators are automatically created upon database creation. Other management roles can be created by authorized administrators. Database roles include DBA, RESOURCE, CONNECT and CUSTOM roles. The DBA role is the authorized administrator role, the RESOURCE role is used to create base database objects, the CONNECT role is used to connect to the database, and the CUSTOM role is customize roles, usually used for permission grant management. Database users make use of the database, but do not have administrative system privileges.

TOE security functional requirements addressed: 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

The TOE provides replication of data using the Data Protect feature. Primary database transactions generate redo records. A redo record is made up of a group of change vectors, each of which is a description of a change made to a single block in the database. For example, if a value is changed in a table, a redo record containing change vectors that describe changes to the data segment block for the table, the undo segment data block and the transaction table of the undo segments is generated. Data Protect works by shipping the redo to the replicated database and then applying that redo to ensure the consistency of the data.

TSF data synchronized by the primary and the standby includes **user**, **role**, **profile**, **system privileges** and **object privileges**:

user: all users in the database system, and it can be obtained by querying the dba_users view, see the dba_users definition in Chapter 4.2.58 of *GaussDB 100 V300R001C00B300 R&D Documentation 06*.

role: all roles in the database system, and it can be obtained by querying the dba_roles view, see the dba_roles definition in Chapter 4.2.39 of *GaussDB 100 V300R001C00B300 R&D Documentation 06*.

all roles information for all users, and it can be obtained by querying the dba_role_privs view, see the dba_role_privs definition in Chapter 4.2.40 of *GaussDB 100 V300R001C00B300 R&D Documentation 06*.

profile: all system profile information, and it can be obtained by querying the dba_profiles view, see the dba_profiles definition in Chapter 4.2.38 of *GaussDB 100 V300R001C00B300 R&D Documentation 06*.

system privileges: all system privileges granted to the all users, and it can be obtained by querying the all_user_sys_privs view, see the all_user_sys_privs definition in Chapter 4.2.6 of *GaussDB 100 V300R001C00B300 R&D Documentation 06*.

object privileges: all object authorization information for all users in the system. and it can be obtained by querying the dba_tab_privs view, see the dba_tab_privs definition in Chapter 4.2.55 of *GaussDB 100 V300R001C00B300 R&D Documentation 06*.

FPT_TRC.1.2

The maximum protection mode provided by security functions ensures that no data will be lost. In this mode, transaction logs are not only written into local log files, but also into the log files of standby databases. Transactions are committed in the primary database only when data is available in at least one standby database. Log files of the primary database are replayed on standby databases for data consistency between the primary and standby databases. If standby databases are unavailable due to a fault (for example, network disconnection), services on the primary database will be blocked to prevent data loss.

TOE security functional requirements addressed: 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. Each parameter has a value range and a default value.

FTA_TSE.1.1

- Authorized administrators can configure user whitelists, and security functions can filter session connections based on username identities configured in user whitelists.
- Authorization administrators can create user validity, and refuse to login to the database when the user exceeds the validity.
- Authorization administrators can configure the maximum number of connections for users and refuse to login to the database when the number of connections initiated exceeds the maximum number.
- Authorized administrators can configure IP whitelist or IP blacklist, and security functions can filter session connections based on IP whitelist or blacklist configuration.

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

9 Terminology, Acronyms, and References

9.1 Term

Table 9-1 Term

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

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

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

9.2 Acronyms

Table 9-2 Acronyms

Acronym	Definition
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
DAC	Discretionary Access Control
DBMS	Database Management System
DBMS PP	Base Protection Profile for Database Management Systems
EAL	Evaluation Assurance Level
GUI	Graphical user interface
I&A	Identification and Authentication
IT	Information Technology
OSP	Organizational Security Policy

Acronym	Definition
PP	Protection Profile
RDBMS	Relational Database Management System
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

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