FUJ00232864

Document Title:	STANDARDISE DATABASE LOGGING CONFIGURATIONS
Document Reference:	ARC/SOL/PSD/4703
CP/CWO Reference:	CP2876
Abstract:	High level design for auditing users in BRDB and tying sysdba activities back to AD users
Document Status:	APPROVED
Author & Dept:	GARETH SEEMUNGAL
External Distribution:	(Specify those individuals outside of the Post Office Account who require approved version only. For POA Document Management to distribute following approval)
Information Classification:	See section 0.9

Approval Authorities:

Name	Role	
Simon Wilson	Chief Technical Officer	See Dimensions for record
		See Dimensions for record

FUJ00232864

0 Document Control

0.1 Table of Contents

FUJ00232864

0.2 Document History

Only integer versions are authorised for development.

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change CWO, CP, CCN or PEAK Reference
0.1	14/10/2022	Initial version	R40.50
0.2	20/10/2022	Updates after comments, ready for review.	
1.0	16/11/2022	Approved	

0.3 Review Details

Review Comments by:	16th November 2022
Review Comments to:	Gareth.seemunga GRO + POA Document Management

Mandatory Review	
Role	**Name**
Host Architecture	Pete Jobson
Service Architecture Manager	Alex Kemp
Security Architect	Dave Haywood*
Service Architect	Phil Boardman
Network Architect	Ravi Saini
POA CISO	Steve Browell*
SSC Manager	Adam Woodley; sscdm GRO
UK PODG Bridge Team Lead	Susan Brindley
Network Operations Manager	Chris Harrison

Optional Review	
Role	**Name**
CTO	Simon Wilson
Host Bridge Team Lead	Gyan Patel
Data Centre Development Manager	Pavan Vejendla
Project Management	Abi Loveday
Project Management	Peter Bowen
Host Team	Akshyakumar Nahak
Host Team	Mandakini Nayak
Host Team	Praveen Kumar M.
Chief Architect	Torstein Godeseth
Unix Team	Andrew Gibson
DBA Team	Stuart Johnston
DBA Team	Niall McKeefry
Information Security Management	Farzin Denbali; Chris Stevens

FUJ00232864

Test Delivery Manager	Joan Duhaney
Test Managers	Mark Ascott; Trevor Leahy
Release Management and Operational Change Manager	Matt Swain

(*) = Reviewers that returned comments

Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	**Name**

0.4 Associated Documents (Internal & External)

References should normally refer to the latest approved version in Dimensions; only refer to a specific version if necessary.

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 *(DO NOT REMOVE)*	See note above	See note above	POA Generic Document Template	Dimensions
PGM/DCM/ION/0001 *(DO NOT REMOVE)*			POA Document Reviewers/Approvers Role Matrix	Dimensions
SVM/SEC/POL/0003			POA Information Security Policy	Dimensions
SVM/SEC/POL/0005			Community Information Security Policy (CISP) for Horizon	Dimensions
ARC/SEC/ARC/0003			Technical Security Architecture	Dimensions
SVM/SEC/MAN/0003			Information Security Management System (ISMS) Manual	Dimensions
DES/GEN/TEM/2227			Information Technology Health Check (ITHC) Template	Dimensions
DES/APP/HLD/0020			Branch Database High Level Design	Dimensions
DES/APP/HLD/0023			Branch Support Database High Level Design	Dimensions
ARC/SOL/PSD/4429			Refinement of Access Rights to Oracle Databases	Dimensions

0.5 Abbreviations

Abbreviation	Definition
AD	Active Directory
BDB	3 character platform code for BRDB
BDS	3 character platform code for BRDB Standby
BRDB	Branch Database
DBA	Database Administrator
SSC	Software Support Centre, 3rd line support group

0.6 Glossary

Term	Definition
DAT	Solaris platform code

FUJ00232864

0.7 Changes Expected

Changes

0.8 Accuracy

Fujitsu Services endeavours to ensure that the information contained in this document is correct but, while every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

0.9 Information Classification

The author has assessed the information in this document for risk of disclosure and has assigned an information classification of FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE).

FUJ00232864

1 Scope

This document is produced under CP2876.

This document provides a view of the changes necessary to satisfy the auditability and traceability requirements around DBA & Unix user access and activities when connected to HNG-X Oracle databases.

In addition this document includes the changes necessary to align BRDB with the other HNG-X Oracle databases in terms of auditability of SQL queries submitted by all support users.

Support users include the SSC as well as Unix and DBA users.

1.1 Purpose of Document

This document intends to specify the changes necessary to both the HNG-X Oracle databases, their platforms and potentially processes involved with operational support access.

1.2 Target Audience for this Document

This document is intended to be read by

- Host Development
- Host Architecture
- 3rd Line Support (SSC)
- 1st Line Support (Unix & DBAs)
- Test
- Service

1.3 Background

The method for sysdba privileged access by Support staff (e.g. DBAs) to Oracle databases currently relies on sudo to unix user 'oracle' first. Unfortunately this use of sudo to 'oracle' removes the direct audit trail back to the user who originally initiated the sudo action. Note this activity can be inferred today based on the sudo and sysdba audit logs.

Sections 2.1, 2.2 & 2.3 seek to address this break in traceability for sysdba logins.

BRDB will also be updated to include auditing of all DML SQL statements for support users. This change will bring BRDB in line with the other databases which were updated at R36.50 (CP2831) to enable this feature.

FUJ00232864

2 Security and Data Privacy

2.1 Security Profile

2.1.1 Risks

Number	Risk	Owner	Probability	Impact	Action
R001	Support staff lose ability to carry out authorised data changes due to flawed implementation	Fujitsu	Low	High	Prove solution within each environment, ensuring LST signoff remains as a gate prior to Live implementation. Ensure DBAs, Unix and SSC are involved or at least consulted during testing of the solution. Provide breakglass option for DBAs to sudo directly as oracle if the solution does not provide privileges necessary to support the estate.
R002	Support staff activities produce large amounts of audit, resulting in the audit tablespace filling up. This would stop support staff from logging in.	Fujitsu	Low	High	The Operational DBAs must ensure the audit tablespaces are never below an agreed freespace level (currently alerts are configured to appear at <= 10% free space). If space becomes an issue then the DBAs will need to increase the tablespace by 10% to 20% and then raise a TFS call for 4th line support to analyse the growth profile. The DBAs can add additional data files if the tablespace is 100% full.

Table 4 Security – Risks

FUJ00232864

3 Overview of Changes

This section provides a high level summary of

- the changes that will be common across all impacted databases
  - APOP
  - BRDB
  - BRSS
  - DRS
  - NPS
  - TES
  - RDMC
  - RDDS
- the changes specific to each database where relevant

3.1 Active Directory Update

The DBA support users in Belfast will have their AD profiles altered to include the 'DBA' unix group. This update will allow DBA users escalate their sqlplus login to sysdba using their own login (i.e. without the use of sudo to oracle).

3.2 Configure Users' Profiles

The Host team to deliver a benign file to /etc/ (e.g. via UNIX_SUPPORT_UTILS_V2 for Linux and Solaris) that will contain the Oracle related environment variables for user profiles. Each DBA can then update their profiles to reference this /etc/ hosted file to allow sqlplus logins.

3.3 SUDO'ing to Oracle for Sqlplus Access

The DBA and Unix users shall not switch to the oracle unix user for sqlplus / as sysdba access. Instead support shall use their own AD profiles for sqlplus access by default.

If there is an exceptional requirement to invoke sqlplus as sysdba via 'oracle' then the breakglass process (to be agreed via a new SecOps Policy document – reference TBA) must be used.

3.4 BRDB Auditing Alignment

3.4.1 Ensure SYS Auditing is Enabled

Ensure database parameter audit_sys_operations is set to TRUE if not already enabled.

3.4.2 Existing DBA, Unix & SSC Support Users

Existing database support users will have their select/update/insert/delete SQL statements, executed procedures and their logins audited by default.

SecOps will ensure that the User Access Database and JML forms are updated to reflect these new role clarifications.

3.4.3 Existing APPSUP Escalation Process

The existing SSC APPSUP escalation process will be maintained for BRDB.

3.4.4 BRDB Audit Tablespace Sizing Considerations

FUJ00232864

The current live BRDB currently has ample space for additional audit logging information. The sizing information here is from 2022-10-14.

DB	Tablespace	Used MB	Free MB	Total MB	Pct. Free
BRDB	BRDB_AUDIT	1.56	5,907	6000	98.44

***Design Note for Test**: testing within LST should confirm whether the additional audit logging overhead might result in a much larger impact on storage requirements than currently anticipated.*

FUJ00232864

4 Solution Design

4.1 Active Directory Update

AD profiles with the following group membership should also be assigned the 'dba' group

- `is-dba`
- `is-unix`

4.2 DAT & Linux /etc/profile Update

Create a new file /etc/oracle_profile to set the following environmental variables (note paths will be different depending on the platform type e.g. Linux versus Solaris)

- `ORACLE_BASE`
- `ORACLE_TERM`
- `GRID_HOME`
- `ORACLE_HOME`
- `LD_LIBRARY_PATH`

Ensure the file permissions allow all users to invoke "source /etc/oracle_profile".

4.3 SecOps Policy Update

A new SecOps Policy document will be generated to provide guidance around the use of the 'oracle' unix user.

In particular, it will be expected that the DBAs will typically NOT sudo to oracle in order to access sqlplus. The change to their AD groups will allow DBAs to escalate their sqlplus access to sysdba level using their unix profile.

The SecOps policy may allow the direct use of the oracle user via the use of TfS (but this is beyond the scope of this technical design document).

FUJ00232864

4.4 BRDB Specific Changes

4.4.1 Enable Database Audit & Extended Audit

Enable Extended Audit via the following command and then schedule in a database restart to activate.

```
alter system set audit_trail='DB','EXTENDED' scope=spfile;
```

4.4.2 Existing DBA, Unix & SSC Support Users

Users identified as being part of the following groups

- SSC
- Unix
- DBA

in BRDB (at the time of this solution's deployment) shall have the following actions applied

Action	Action
Enable User Audit	AUDIT ALL BY <user> BY ACCESS; AUDIT SELECT TABLE, UPDATE TABLE, INSERT TABLE, DELETE TABLE BY <user> BY ACCESS; AUDIT EXECUTE PROCEDURE BY <user> BY ACCESS; GRANT RESOURCE TO <user>; GRANT CONNECT TO <user>;

4.4.2.1 Identifying Support Users

The following SQL is one possible way of identifying existing support usernames on BRDB (including those accounts that have been disabled as part of the JML process).

```
select distinct grantee
from   dba_role_privs
where  grantee not in ('SYS','SYSTEM')
and    granted_role in ('DB_MONITOR', 'SSC', 'UNXADM')
and    grantee not in ('OPS$SUPPORTTOOLUSER')
order  by 1
```