International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

Hybrid Data Protection Framework to Enhance A2O Functionality in Production Database Virtualization

N. Z. Azeemi, Z. Hayat, G. Al-Utaibi, O. Al-Basheer

Abstract*: Deluge of information flows in the unprecedented scenario of smart city development trend, hence prone to issues on stability, reliability and availability. Smart data storage resources are vulnerable to provide functionality Always Available Online (A2O) due to their inherent heavy dependence on System Down Time (SDT), Redundant Systems and Software Failure (RS2F) or whole/ multiple site failures. In the absence of Production Database Management Services (PDMS), duplicate deployment of similar data on disjoint but similar architecture provides a Tightly Coupled Ultimate System (TCUS), which assures A2O mutually exclusive services. In this paper, we investigated active Data Guard (aDG) and Data Guard (DG) role management or switchover for a real time transition performed for database at standby state to cope up both planned maintenance and accidental RS2F events. We expose our results for deep integration of aDGs with ODB in-terms of Fast Sync to align synchronously at an ease of zero of wait states for disk I/O and configurability to Null Data Loss (NDL). Over a large range of remote or standby databases NDL make it certain to zero failover. The impact of aDG Fast-Start Failover in the cloud proximity make sure guaranteed NDL in synchronously and near NDL protection asynchronously. Hence, avoids unusual overhead impeding disk I/O and eventually on a primary database. We observe the key performance indicator in failover does not restart the standby database for primary role resumption, but introduce cloud proximity as a new primary database and the process is performed without any intervention of manual migration. The reliability of aDG Redo is flexible across not only standby databases but also primary sites running different operating system over diverse hardware platforms. The Redo capability enables migration with minimal downtime for any transaction in the clouds, therefore adds an inevitable functionality to big data applications.

Keywords: Active Data Guard, Smart Data Storage, Cloud Applications, Fault Tolerant, Smart City.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
***** Correspondence Author
Naeem Zafar Azeemi*, School of Engineering and Technology, Al Dar University College, Dubai, UAE. Email: naeemazeemi@gmail.com; naeem@aldar.ac.ae
Zulqarnain Hayat, Ankabut IT, Khalifa University of sCience and Technology, Abu Dhabi, UAE. Zulqarnain.hayat@kustar.ac.ae
Ghassan Al Utaibi, School of Business Administration, Al Dar University College, Dubai, UAE. ghassanalutaibi@aldar.ac.ae
Omar Al Basheer, School of Engineering and Technology, Al Dar University College, Dubai, UAE. omar@aldar.ac.ae

I. INTRODUCTION

Disparate engineering silos harnessed across diverse digital data fields or over the smart networks are vulnerable in term of Transaction-based Big Data (TB2D). Reducing downtime, in line with Null data Loss (NDL) by introducing redundancy applied in mission critical clustered databases may not be adequately protected as suggested by [1, 2, 3] in Tightly Coupled Ultimate System (TCUS), which assures A2O mutually exclusive services. The 7Rs-centric automated processing proposed in [3] framework (TB2D-7R) is reliable for analyzing complex, interdependent systems and environments that may span multiple engineering and job specialties. Despite the promising 7Rs-centric automated processing framework (TB2D-7R), guaranteeing the availability of supporting big data is hitherto uncertain. [4, 5] highlighted the ever increasing information growth due to convergence of computing and communication and increase demand to extract useful information from TB2D as required in medical imaging sampled by [1] Wireless Sensor Networks (WSN) deployment and 5G evolution aggregated the fact that if *data* is characterized as recorded facts, then *information* is the fact the huge amount of information is concealed in set of patterns, or expectations, that underlie the data [6].

High Availability (HA) of cloud database systems is essential, while grilling huge amount of information locked up in databases—information that is potentially important but has not yet been discovered or articulated [7, 8]. An Active Data Guard support Oracle Multitenant maintain a production database remotely with synchronously physical replicated topology. Data intensive activities across the Exploration and Production (E&P) value chain in the upstream oil and gas industry are no longer garnering actionable knowledge from traditional stochastic or nondeterministic studies [1]. Plethora of data is generated when hidden surface patterns are mined to enhance the intelligence, especially in Digital Oilfield of the Future (DOFFs) with permanently deployed Wireless Adhoc Sensor Network (WASN), across the deep offshore assets, steam-assisted gravity drainage, intelligent wells drilled in coal seam gas, and shale plays unconventional reservoirs [7].

We suggest in this work the importance of data guard topology, operating at a deeper level of database container in typical Oracle databases enables effective data recovery against any malfunctioning, attributed to human or natural disaster. Such multitenant container database (CDB) maintains consistent data tiers located across the globe may or may not be geographically co-located, but yet connected in consolidated environment. The benefit offered in Oracle Real Application Cluster as highlighted in [8, 9, 10] allows enables layers of single Oracle database server to behave like multiple servers offering diversity of data transactional services as shown in Figure 1.

A unique virtual IP address turns each server having its own database instance but embedded with external network access in backbone communication, allow to act all an instance of single data base. The architecture of the RAC is provides fault tolerance and a great power of treatment. In practice Oracle, proactive data services with administration privileges, at some course limits the freedom of administrative tasks maneuverability though SYSDG in place; yet resolved with aDG, as reflected in Section 2 and Section 3 for our proposed framework profile.

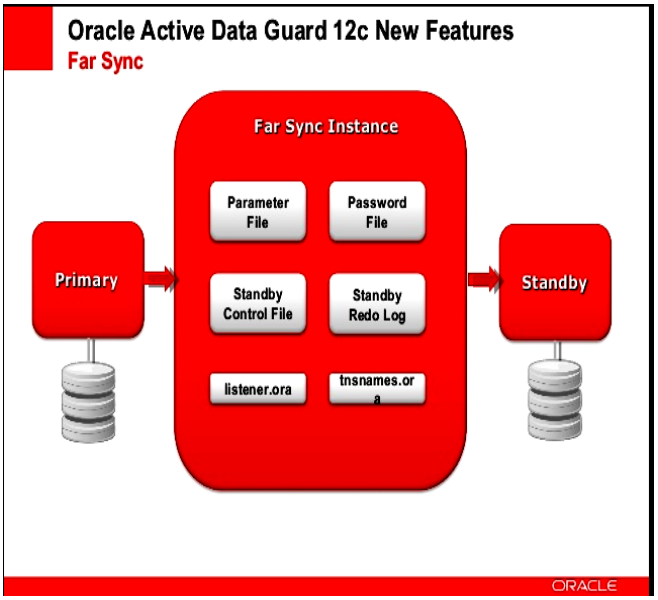

Figure 1. Oracle Active Data Guard Far Sync Activity [7]

The enhanced capability of Oracle Database 12c with additional tier of Oracle Active Data Guard provide further its strategic objective that is preventing data loss and higher instances of availability, risk elimination, turned out promising increasing return on investment. At the same time though simple to deploy and manage, they offer highly functional active disaster recovery. Oracle aDGs eliminate single points of failure for mission critical Oracle Databases, eventually a natural most comprehensive A2O solution, preventing data loss and system downtime in an enterprise network, appear as the simplest and most economical manner as shown in Figure 2. Physical replica of a production database at a remote location is a strategic feature in synchronized maintenance and access. [8, 9, 10]. Client seamlessly connects quickly, and transparently in some configurations when a situation arises where production database is unavailable for any reason such as failover to the synchronized replica or restore services, to name a scenario.

High Availability (HA) of cloud database systems is essential, while grilling huge amount of information locked up in databases—information that is potentially important but has not yet been discovered or articulated [8, 9, 10]. An Active Data Guard support Oracle Multitenant maintain a production database remotely with synchronously physical replicated topology. Data intensive activities across the Exploration and Production (E&P) value chain in the upstream oil and gas industry are no longer garnering actionable knowledge from traditional stochastic or nondeterministic studies [5, 6]. Plethora of data is generated when hidden surface patterns are mined to enhance the intelligence, especially in Digital Oilfield of the Future (DOFFs) with permanently deployed Wireless Adhoc Sensor Network (WASN), across the deep offshore assets, steam-assisted gravity drainage, intelligent wells drilled in coal seam gas, and shale plays unconventional reservoirs [7].

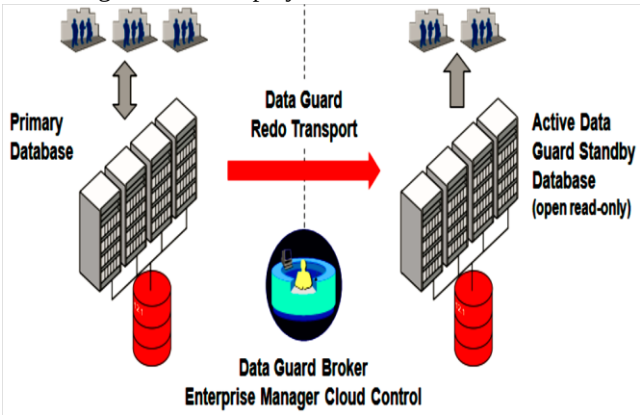

Figure 2. aDG Redo Transport Mechanism [10]

We suggest in this work the importance of data guard topology, operating at a deeper level of database container in typical Oracle databases enables effective data recovery against any malfunctioning, attributed to human or natural disaster. Such multitenant container database (CDB) maintains consistent data tiers located across the globe may or may not be geographically co-located, but yet connected in consolidated environment. The benefit offered in Oracle Real Application Cluster as highlighted in [11, 12] allows enables layers of single Oracle database server to behave like multiple servers offering diversity of data transactional services. A unique virtual IP address turns each server having its own database instance but embedded with external network access in backbone communication, allow to act all an instance of single data base. The architecture of the RAC is provides fault tolerance and a great power of treatment. In practice Oracle, proactive data services with administration privileges, at some course limits the freedom of administrative tasks maneuverability though SYSDG in place; yet resolved with aDG, as reflected in Section 2 and Section 3 for our proposed framework profile. The enhanced capability of Oracle Database 12c with additional tier of Oracle Active Data Guard provide further its strategic objective that is preventing data loss and higher instances of availability, risk elimination, turned out promising increasing return on investment. At the same time though simple to deploy and manage, they offer highly functional active disaster recovery.

Oracle aDGs eliminate single points of failure for mission critical Oracle Databases, eventually a natural most comprehensive A2O solution, preventing data loss and system downtime in an enterprise network, appear as the simplest and most economical manner. Physical replica of a production database at a remote location is a strategic feature in synchronized maintenance and access [8, 9, 10]. Client seamlessly connects quickly, and transparently in some configurations when a situation arises where production database is unavailable for any reason such as failover to the synchronized replica or restore services, to name a scenario.

II. FRAMEWORK AND ORGANIZATION

A. Preliminary Configuration in Oracle Data Guard

Our A2O-aDG framework is flexible to accommodate one primary database, mirroring about thirty destinations. The flexibility is achieved exploiting Oracle Data Guard in the backbone**.** Members of the network may be located at mutually non-exclusive geo-points, but Oracle Net brought forth a seamless integration. Enabling the connectivity across the network inline with valid permissions and cloning remains indiscrete to each members, as long as they are configured in association with Oracle Data Guard. Two standby geographically apart databases in any data center can have a standby database co-located with the primary database in similar data center. Oracle Data Guard broker interfaces can be used to access both primary and standby databases. Database management is also possible with the SQL conventional command line interface. In our work, we used Oracle Enterprise Manager Cloud Control to establish a broker interface, embed with a command-line interface (DGMGRL) and reciprocate similar access control to a distant or mutually exclusive graphical user interface..

B. The Integration of Production Database

More often referred as primary database, an Oracle Data Guard implicitly supports one production database, which functions in the primary role. Most of user applications access aforementioned database. A single instantiation is created for database such as may Oracle database in association with application database clusters, Oracle Real Application Clusters (Oracle RAC) database, to name a few. Particularly primary database is made transnationally consistent with its peer copy of standby database. About 30 standby databases are created, consistent with the any primary database backup copy integrating and eventually configured for Oracle Data Guard. After initiation standby databases are automatically managed by Oracle Data Guard with a mechanism of redo data transmission successively activation of both primary database and standby database. It may be worth to mention, we found a single instance initiation of Oracle database or an Oracle RAC database not only enhance data maintenance in a primary database but extended to a standby database.

C. Physical Standby Database

An identical primary standby database mirrors exactly the physical database. It also reflects database schema in concurrency with the primary database. While autonomous configuration of ‘Redo Apply’ synchronize between the aforementioned databases. Physical standby database updates are followed by the successively applied redo data mechanism in coherence with the primary database.

D. Logical Standby Database (LSD)

Though data structures and organization could be different physically, the production database mirrors the same logical information—hence termed as logical standby database. SQL Apply maintains the synchronization between the continuous updates in primary database and LSD. The redo receive mechanism make sure the data conformance across the two databases, i.e., LSD mirrors standby database as a consequence of SQL instruction.

The rolling management with zero downtime make sure the upgrade in Oracle Database software patch sets and database releases while maintaining the flexibility of LSDs. It also implements the transient LSDs upgrade process with updated aDGs from its revision 11gs. It is upward compatible for physical standby databases.

E. Snapshot Standby Database (SSD)

We kept mirroring the standby databases gradually updated snapshots of any maintenance in primary databases. Redo data mechanism in proposed framework (Section 3), receive and archive snapshots either from primary databases or LSDs. Snapshot standby databases do not mimic the redo data apply sequence as they do in primary databases or LSDs. However SSD snapshots are flagged applied if and only if discarded local changes to SSD are tagged, and then redo data enables the transformation of SSD snapshot into physical standby database.

F. Far Sync Instances (FSI)

A remote aDG is a type of an aDG far sync instance, which accepts and reply remotely ‘redo’ aDG configurations to the primary databases. The maintenance of control file in FSI transform ‘redo’ received into standby redo logs (SRLs). Whereas local archived logs of SRLs are managed till the similarity across standby logs is concluded. Any FSI cannot perform operations like open, access, run redo, apply redo, type conversion i.e., any primary role functionality is beyond the scope of FSI. Such mechanism is mandatory to ensure the integrity and continuous reliable update. In Oracle Database 12c extended functionality omits the acknowledgement of the transaction on the standby, hence called ‘Fast Sync’ that has slightly different redo transportation. However an active Oracle aDG license is required to enable part of Oracle aDG FSI new features.

G. Zero Data Loss Recovery Appliance (ZDLRA)

Oracle enterprise level backup solution incorporates recovery appliances with discrete repository, another feature of its Zero Data Loss Recovery Appliance for all Oracle databases transactional backups. Oracle Database backup and restores are offloads in recovery appliances while imitating backup systems as centralized repository systems. ZDLRA is significantly efficient in utilization of storage, backup management, performance enhancement and zero latency.

III. RESULTS (CONFIGURATION AND PERFORMANCE)

In this section we exposed our framework performance for aforementioned LSDs, SSDs and FSIs configurations to achieve Active Data Guard in smart data centers collocated virtually at diversified geographical regions using virtually distinct IPs, hence mimic an enterprise global network.

Configuration screen shots are provided, wherever deem necessary either tailoring our framework or proposed by Oracle 12c. We configured and recorded various activities in diverse scenarios, described subsequently below.

To exploit feature that came with 12c about Data Guard that called Fast sync standby database. Actually this is a transmitter between primary database and standby database. This database is pretty simple. It contains parameter file control file, standby log file and you can think this database as archive log repository. As you know data guard maximum protection mode provides zero data loss during the primary fail. When you commit a transaction redo log must reach standby database and acknowledge must come from standby database to complete commit operation [8, 9, 10].

We consider that standby database is far away from primary database at this situation commit time can be very long. Oracle 12c enables this functionality by considering bandwidth as a performance indicator to evaluate primary databases, standby databases and communication network. This evaluation is inherent to 12c, readers are encouraged to refer [8, 9, 10] for immersion in the topology. The archived primary database logs are prepared as well as maintained consistency with standby archived logs.

We consider 'sync' as primary FSI or standby FSI databases, while tagged as 'async' wherever they are only physically standby databases are maintained or referred. In Section 3, whole configuration process is depicted with screen shots in Oracle aDG configurations. The environmental parameter configuration is also reflected in screen shots, as followed next.

Roles	IP	db_unique_name
primary	10.x.x.x	NONCDB
far sync	10.x.x.x	FarSyncDB
standby	10.x.x.x	noncdbsy

In order to retain the focus on framework, we leave standard Oracle 12c configuration details to reader and encourage them to refer [10, 11, 12]. However detail subject to interface with our framework shall be depicted in screen snapshots. We have three phases in order to do this structure and will be discuss each in detail.

A) Create Far Sync Standby Database.

B) Configure Primary Database.

C) Create Physical Standby Database.

A. Creating Far Sync Standby Database

We mentioned before that this database tailors with standard Oracle 12c. It contains parameter file, controlfile and standby redo logfile. We build this database.styled.

1) First we create a controlfile for far sync databases either at standby or primary repository.

```
SQL> alter database create far sync instance controlfile as
'/tmp/far_sync_standby.ctl';
Database altered.
```

2) The initiation instance to access primary database and standby database we add tns entry to far sync standby database tnsnames.ora file.

```
NONCDB_PR=
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.48.28)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = NONCDB)
)

NONCDB_DR=
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.48.42)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = noncdbsy)
)
)
FARSYNCDB =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.48.30)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = farsydb)
)
)
```

3) A 'pfile' is created first from spfile for far sync standby database in the primary database.

```
SQL> create pfile='/tmp/pfile_farsync_standby.ora' from spfile;
File created.
```

4) We update far sync standby database to copy created password file and controlfile and password file..

```
[oracle@vprimary tmp]$ scp far_sync_standby.ctl pfile_farsync_standby.ora
oracle@10.100.48.30:/tmp
The authenticity of host '10.100.48.30 (10.100.48.30)' can't be established.
RSA key fingerprint is 63:b7:06:67:62:9d:db:82:e1:c6:03:38:c9:15:7a:35.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.100.48.30' (RSA) to the list of known hosts.
oracle@10.100.48.30's password:
far_sync_standby.ctl                                  100%
9808KB   9.6MB/s   00:00
pfile_farsync_standby.ora                             100%
1034     1.0KB/s   00:00
```

```
[oracle@vprimary dbs]$ scp orapwNONCDB
oracle@10.100.48.30:/oracle12c/12.2home/dbs/orapwfarsydb
oracle@10.100.48.30's password:
orapwNONCDB                                           100%
7680     7.5KB/s   00:00
```

5) The 'pfile' is edited next for far sync database and create required directory.

```
##Dataguard Parameter
*.db_unique_name=farsydb
*.log_archive_config='dg_config=(noncdb,farsydb,noncdbsy)'
*.fal_server='NONCDB_PR'
*.log_archive_dest_1 ='location=USE_DB_RECOVERY_FILE_DEST
VALID_FOR=(ALL_LOGFILES,ALL_ROLES)'
*.log_archive_dest_2='SERVICE=NONCDB_DR
VALID_FOR=(STANDBY_LOGFILES,STANDBY_ROLE)
DB_UNIQUE_NAME=NONCDBSY'
*.LOG_ARCHIVE_DEST_STATE_2=ENABLE
```

6) The control file in FSI and parameter control file for standby are copied next to true location.

```
[oracle@vnode1 tmp]$ cp far_sync_standby.ctl /oracle12c/oradata/control01.ctl
[oracle@vnode1 tmp]$ cp pfile_farsync_standby.ora
/oracle12c/12.2home/dbs/initfarsydb.ora
```

7) We set oracle parameter and start far sync standby database.

```
[oracle@vnode1 12.2home]$ export ORACLE_HOME=/oracle12c/12.2home
[oracle@vnode1 12.2home]$ export ORACLE_SID=farsydb
[oracle@vnode1 12.2home]$ /oracle12c/12.2home/bin/sqlplus / as sysdba
SQL*Plus: Release 12.1.0.2.0 Production on Fri Aug 22 09:54:21 2014
Copyright (c) 1982, 2014, Oracle.  All rights reserved.
Connected to an idle instance.
```

FSI is initiated to provide total global system are in terms of fixed, variable sizes and databases/ redo buffers, eventually mounts the database.

8) We check far sync database listener and connections are establish for tcp address protocols, while host is maintained similar to port 21.

```
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for Linux: Version 12.1.0.2.0 – Production
Start Date                22-AUG-2014 09:53:07
Uptime                    0 days 0 hr. 1 min. 48 sec
Trace Level               off
Security                  ON: Local OS Authentication
SNMP                      OFF
Listener Parameter File   /oracle12c/12.2home/network/admin/listener.ora
Listener Log File         /oracle12c/diag/tnslsnr/vnode1/listener/alert/log.xml
Listening Endpoints Summary…
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=10.100.48.30)(PORT
=1521)))
(DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=extproc)))
Services Summary…
Service "farsydb" has 1 instance(s).
Instance "farsydb", status READY, has 1 handler(s) for this service…
The command completed successfully
```

9) Database roles are checked once we open far sync standby database to ensure FAR SYNC

```
SQL> select database_role from v$database;
DATABASE_ROLE
----------------
FAR SYNC
```

10) Redo logs are created for standby as per recommendation of Oracle. It is de facto standard redo log file are one less than the standby redo logs.

```
ALTER DATABASE ADD STANDBY LOGFILE THREAD 1 GROUP 4 SIZE
50M, GROUP 5 SIZE 50M, group 6 size 50M,group 7 size 50M;
```

We prepare next standby database, once FSI standby database is ready. It sequentially followed by the dataguard configuration for the primary database.

B. Configure Primary Database

While configuring aDG environment variables, the archive log mode is ensured to enable for primary database. .

1) In order to reach far sync standby database, we edit a file tnsnames.ora. screen snapshot for tnsnames.ora below, indicates primary database address protocol, host port and connection parameters.

```
NONCDB =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.48.28)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = NONCDB)
)
)

NONCDB_DR=
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.48.42)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = NONCDBSY)
)
)

FARSYNCDB =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.48.30)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = farsydb)
)
)
```

2) We edit some parameter for data guard.

```
SQL> alter system set log_archive_dest_2='SERVICE=FARSYNCDB SYNC
COMPRESSION=ENABLE
VALID_FOR=(ONLINE_LOGFILES,PRIMARY_ROLE)
DB_UNIQUE_NAME=farsydb' scope=both;
System altered.

SQL> alter system set LOG_ARCHIVE_DEST_STATE_2=ENABLE
scope=both;
System altered.

SQL> alter system set
log_archive_config='dg_config=(noncdb,farsydb,noncdbsy)' scope=both;
System altered.

NOTE: If we use pfile for database we must add this parameter to pfile.
```

3) A 'redo log' is created for standby as recommended by Oracle that should be number of redo log files by plus one.

```
ALTER DATABASE ADD STANDBY LOGFILE THREAD 1 GROUP 4 SIZE
50M, GROUP 5 SIZE 50M, group 6 size 50M,group 7 size 50M;

SQL> select member from v$logfile where type='STANDBY';

MEMBER
--------------------------------------------------------------------------------
/oracle12c/oradata/NONCDB/onlinelog/o1_mf_4_9zfw6v58_.log
/oracle12c/fast_recovery_area/NONCDB/onlinelog/o1_mf_4_9zfw6v8z_.log
/oracle12c/oradata/NONCDB/onlinelog/o1_mf_5_9zfw6vho_.log
/oracle12c/fast_recovery_area/NONCDB/onlinelog/o1_mf_5_9zfw6voz_.log
/oracle12c/oradata/NONCDB/onlinelog/o1_mf_6_9zfw6vvv_.log
/oracle12c/fast_recovery_area/NONCDB/onlinelog/o1_mf_6_9zfw6w3k_.log
/oracle12c/oradata/NONCDB/onlinelog/o1_mf_7_9zfw6wb3_.log
/oracle12c/fast_recovery_area/NONCDB/onlinelog/o1_mf_7_9zfw6wk3_.log
```

C. Preparing Standby Database

In this section we shall mimic geographically apart virtual servers to create an enterprise smart data center. Standby database shall be created next. As per our framework the creation of standby database will be preceded with duplication of active database..

1) A file tnsnames.ora is created enable far sync standby database access.

```
NONCDB_PR=
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.48.28)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = NONCDB)
)
)

NONCDB_DR=
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.48.42)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = NONCDBSY)
)
)
```

```
FARSYNCDB =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.48.30)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = farsydb)
)
)
```

2) A 'pfile' file is copied along with password file to access primary database. We need to edit this file to maintain physical standby and standby database, and also maintained in 'pfile'.

```
[oracle@vprimary dbs]$ scp orapwNONCDB initNONCDB.ora
oracle@10.100.48.42:/tmp
oracle@10.100.48.42's password:
orapwNONCDB                                   100%
7680     7.5KB/s   00:00
initNONCDB.ora                                100%
1034     1.0KB/s   00:00
```

3) c) Next step is to create audit files, trails and maintain control file compatibility in 'require directory'. The steps for creation are depicted in screen shots below.

```
##Dataguard Parameter
*.db_unique_name='noncdbsy'
*.log_archive_config= 'dg_config=(noncdb,farsydb,noncdbsy)'
*.fal_server='FARSYNCDB'
*.log_archive_dest_1 =
'location=USE_DB_RECOVERY_FILE_DESTVALID_FOR=(ALL_LOGFILE
S,ALL_ROLES) DB_UNIQUE_NAME=noncdbsy'
*.log_archive_dest_2='SERVICE=FARSYNCDB
VALID_FOR=(STANDBY_LOGFILES,STANDBY_ROLE)
DB_UNIQUE_NAME=farsydb'
*.log_archive_dest_state_2=ENABLE
```

4) The file 'listener.ora' is configured as depicted below.

```
[oracle@vstandby tmp]$ vi /oracle12c/12.2home/network/admin/listener.ora
LISTENER=
(DESCRIPTION=
(ADDRESS_LIST=
(ADDRESS=(PROTOCOL=tcp)(HOST=10.100.48.42)(PORT=1521))
(ADDRESS=(PROTOCOL=ipc)(KEY=extproc))))
```

5) Oracle parameter needed to be configured for export and creation of start standby instances. It also provide total global system area memory footprint.

```
[oracle@vstandby ~]$ export ORACLE_HOME=/oracle12c/12.2home
[oracle@vstandby ~]$ export ORACLE_SID=noncdbsy

[oracle@vstandby ~]$ /oracle12c/12.2home/bin/sqlplus / as sysdba
SQL*Plus: Release 12.1.0.2.0 Production on Fri Aug 22 08:53:04 2014
Copyright (c) 1982, 2014, Oracle.  All rights reserved.
Connected to an idle instance.
```

6) Active database duplication is enabled successively with various allocation steps for standby database, followed by NONCDB database channels allocation connection as target and auxiliary noncdbsy.

```
RMAN> run{
2> allocate channel prmy1 type disk;
3> allocate channel prmy2 type disk;
4> allocate auxiliary channel c1 device type disk;
5> allocate auxiliary channel c2 device type disk;
6> duplicate target database for standby from active database nofilenamecheck;
7> }
contents of Memory Script:
{
switch clone datafile all;
}
executing Memory Script
datafile 1 switched to datafile copy
input datafile copy RECID=7 STAMP=856256738 file
name=/oracle12c/oradata/NONCDBSY/datafile/o1_mf_system_9zfqf1fm_.dbf
datafile 3 switched to datafile copy
input datafile copy RECID=8 STAMP=856256738 file
name=/oracle12c/oradata/NONCDBSY/datafile/o1_mf_sysaux_9zfqf033_.dbf
datafile 4 switched to datafile copy
input datafile copy RECID=9 STAMP=856256738 file
name=/oracle12c/oradata/NONCDBSY/datafile/o1_mf_undotbs1_9zfqfj2b_.dbf
datafile 5 switched to datafile copy
input datafile copy RECID=10 STAMP=856256738 file
name=/oracle12c/oradata/NONCDBSY/datafile/o1_mf_noncdbtb_9zfqfj33_.dbf
datafile 6 switched to datafile copy
input datafile copy RECID=11 STAMP=856256738 file
name=/oracle12c/oradata/NONCDBSY/datafile/o1_mf_users_9zfqfk4x_.dbf
```

Alert standby database are recovered which triggers the initiation standby database while applying start logs. The alteration in database is depicted in screen snapshot below.

```
SQL> alter database recover managed standby database using current logfile
disconnect;
Database altered.
```

The process of dataguard is regulated in ensuring our dataguard machines is correctly enabled to perform according to our log files.A Primary tier of database is depicted in screen shot below.

```
SQL> select
process,status,thread#,sequence#,delay_mins,active_agents,client_process from
v$managed_standby;
PROCESS   STATUS        THREAD#  SEQUENCE# DELAY_MINS
ACTIVE_AGENTS CLIENT_P
--------- ------------ ---------- ---------- ---------- ------------ --------
ARCH      CLOSING            1         68          0            0 ARCH
ARCH      CLOSING            1         69          0            0 ARCH
ARCH      CLOSING            1         50          0            0 ARCH
ARCH      OPENING            1         69          0            0 ARCH
LGWR      WRITING            1         70          0            0 LGWR
```

We have successfully configured and mount all databases. As can be seen in code snapshots, each database is rolling at various virtual IPs, seamlessly integrated as one unit and fault resilient that is zero downtime or latency in case of failure. We can also check at any time of instantiation whether Far Sync Standby Database, Configuration of Primary Database and Creation of Physical Standby Database are integrated and regulated to produce one discreet data center.

We shall demonstrate two screen shots for core threads, such as FSI database and SSDs as follows:

Far sync Standby Database:

```
SQL> select
process,status,thread#,sequence#,delay_mins,active_agents,client_process from
v$managed_standby;
PROCESS   STATUS        THREAD#  SEQUENCE# DELAY_MINS
ACTIVE_AGENTS CLIENT_P
--------- ------------ ---------- ---------- ---------- ------------ --------
ARCH      CLOSING            1         49          0            0 ARCH
ARCH      CLOSING            1         51          0            0 ARCH
ARCH      CONNECTED          0          0          0            0 ARCH
ARCH      CLOSING            1         69          0            0 ARCH
RFS       IDLE               0          0          0            0 ARCH
RFS       IDLE               0          0          0            0 UNKNOWN
RFS       IDLE               0          0          0            0 UNKNOWN
LNS       WRITING            1         70          0            0 LNS
RFS       IDLE               0          0          0            0 ARCH
RFS       IDLE               0          0          0            0 UNKNOWN
RFS       IDLE               0          0          0            0 UNKNOWN
```

Standby database:

```
SQL> select
process,status,thread#,sequence#,delay_mins,active_agents,client_process from
v$managed_standby;
PROCESS   STATUS        THREAD#  SEQUENCE# DELAY_MINS
ACTIVE_AGENTS CLIENT_P
--------- ------------ ---------- ---------- ---------- ------------ --------
ARCH      OPENING            1         68          0            0 ARCH
ARCH      CONNECTED          0          0          0            0 ARCH
ARCH      CLOSING            1         69          0            0 ARCH
ARCH      OPENING            1         69          0            0 ARCH
MRP0      APPLYING_LOG       1         70          0            5 N/A
RFS       IDLE               0          0          0            0 UNKNOWN
RFS       IDLE               0          0          0            0 UNKNOWN
RFS       IDLE               0          0          0            0 UNKNOWN
RFS       IDLE               1         70          0            0 LGWR
```

IV. CONCLUSION

Hybrid data protection ensures the data availability in aDG and provides a yet simplistic approach in Oracle database management either in primary database, production database. The economical balance is a major tradeoff while spreading database location geographically to produce explicit replica or mirroring them over the various distant remotely locations. Our hybrid data protection framework configuration and always available online functionality with zero latency in case of tolerance against fault or downtime, indicate a major player to meet the economical and remote access challenges. The functionality of production database management embedded with active data approach turned out to be a simple yet effective approach in our framework, especially geared for corporate and multi-national stacked database tiers though geographically apart. Mechanism configuration such as synchronization of multiple copies in production database management, remote-storage or replication, logical or physical ensure the integrity of data and mentioned as step-by-step procedure in this work. We observe the key performance indicator in failover does not restart the standby database for primary role resumption, but introduce cloud proximity as a new primary database and the process is performed without any intervention of manual migration. The reliability of aDG Redo is flexible across not only standby databases but also primary sites running different operating system over diverse hardware platforms. The Redo capability enables migration with minimal downtime for any transaction in the clouds, therefore adds an inevitable functionality to big data applications.

In the same vein aDG hybrid data protection framework is aligned with commitment to user operational cost, network complexity, data corruption identification, auto detection and repar, and its enhanced A2O incur at investment return, to name a few. Aforementioned framework is promising in smart city or corporate level Oracle database deployment with reasonably significant integration across deeper layers and yet to achieve protection at blockchain or real time A2O-aDG paradigm.

REFERENCES

1. O. W. Pfeifer, "Garmin International Inc. Oracle Exadata Database Machine, Oracle White Paper " (2012) [Last visited 2016]. Available at: http://www.oracle.com/technetwork/database/availability/garmin-1667151.pdf
2. Muhammad Asad, Naeem Zafar Azeemi, Muhammad Faisal Zafar, `Early Stage Breast Cancer Detection through Mammographic Feature Analysis' (2011) in proceeding of 5th International Conference on Bioinformatics and Biomedical Engineering, (iCBBE) 2011, Wuhan, China, May 10-12, 2011 ISSN: 2151-7614 Print ISBN: 978-1-4244 5088-6, pages 103-107
3. N. Zafar Azeemi, M. Ghanam, F. Taktak, M. Shahzad Akbar, 'Seven Rs Framework—A Fast Track Uncertainty Performance Assessment of Complex Digital Oilfields,' (2017) in proceeding of Middle East Heavy Oil Congress, Bahrain, April 2017. (Accepted for publication)
4. S. Akbar Khan, N. Zafar Azeemi, 'Statistical Correlation Between Consumer Tendency and Health Insurance Performance in UAE,' (2016) in International Journal of Business and General Management Vol. 13, Issue 4, Dec 2016; pp. 45-58N. Zafar Azeemi, 'Delivering 4G (LTE) to 5G Migration with Supply Chain Management,' (2017) in International Journal of Electronics and Communication Engineering, Vol. 6, Issue 1, Dec - Jan 2017; pp. 21-32
5. N. Zafar Azeemi, 'Value Networks Dynamics in Decision Support System for Sustainable Apparel Industry,' (2016) in the Journal of Engineering and Applied Sciences, Vol 35, Issue 2, July - December 2016.
6. N. Zafar Azeemi, A. Khan, 'On-Site Ultra Wide Band Construction Material Tracking System (UWB - CMTS),' (2014) in European Journal of Scientific Research UK, ISSN Print: 1450-216X or Online: 1450-202X Volume 126 No 2, November 2014, pages.152–161.
7. N. Zafar Azeemi, O. Farooq, I. Ali, T. Rasool, `Migration of Multimedia Legacy Applications to Battery-Conscious Mobile Architectures', (2008) in Proceeding of IEEE International Conference on (ICIAF 2008), pages 112 - 117, Colombo, Sri Lanka, December 12-14, 2008.
8. O. support, "Create Dataguard Broker Configuration, published (2016)": Doc-ID 1583588.1).Available at: https://support.oracle.com/epmos/faces/DocumentDisplay?id=1583588.1.
9. O. support , "Using Oracle Enterprise Manager Cloud Control 12c with High Availibility (Doc ID 1937831.1) (2016) [Last update 2016).Available at: https://support.oracle.com/epmos/faces/DocumentDisplay?id=1937831.1
10. Oracle, "Disaster Recovery to the Oracle Cloud Production on Premises, DR in the Cloud (2016)," [Online]. Available at: www.oracle.com/technetwork/database/availability/dr-to-oracle-cloud-2615770.pdf
11. Oracle, "Oracle Data Guard Concepts and Administration " (2015)[Last visted 2019]. Available at : https://docs.oracle.com/database/121/SBYDB/E48552-07.pdf
12. Oracle, "Oracle Active Data Guard Real-Time Data Protection and Availability ORACLE WHITE PAPER (2015)," [Online]. Available at: http://www.oracle.com/technetwork/database/availability/active-data-guard-wp-12c-1896127.pdf.

AUTHORS PROFILE

Naeem Zafar Azeemi (Ph.D., Austria) is an internationally reputed Academician, Industrialist, and Consultant. Having 3 Cited Patents on his credit, for last 25 years he is engaged in industries of 5G, LTE, Internet-of-Thing (IoT) customized solution, Smart Grid Energy Control & PLC Instrumentation, SCADA/DCS deployment at Siemens Europe (EU), British Telecom UK and Philips Silicon Valley USA. He is also Founder President of various Industrial-Academia initiatives, Centennial Chapter of MobileMonday Forum, Senior Advisor to Inter Governmental Organization UNESCO France, UNIDO Austria, COMSATS Italy, PEC-Washington Accord to name a few. He can be contacted at naeemazeemi@gmail.com.

Zulqarnain Hayat, DBD is a Database Specialist at Khalifa University Abu Dhabi UAE, combining with combination of functional and technical skills coupled with over 14 years of experience, he is expert in Banner UDC technology stack Higher Education, Oracle Applications DBA EBS R12 ERP Expert and Oracle Database11G, 12C Database Expert.

He is proficient Oracle Business Intelligence Administration Oracle BI Intermediate, to evaluate platforms such Oracle Web Logic Application Server, Sun Solaris Administration Operating System, Sun Cluster Administration Operating System, Linux Red Hat, Oracle Linux, Oracle OVM Operating System, Windows Server Administration Operating System, Oracle Data Warehouse Builder Data Warehousing Intermediate, SQL Server Administration Database, Project Management Miscellaneous Intermediate, Systems audit and control Miscellaneous, Oracle OAM 11G,OSSO 10G EBS R12 Oracle, Data Center design and implementation Technology. Equipped with unique experience in Virtualization such as VMware Infrastructure Virtualization Technology, EMC Storage and Legato Networker Storage, as one lead layout designer.

Professor Ghassan Al-Utaibi, PhD is highly experienced and successful academic, and business consultant with extensive experience and a proven track record of successful consulting projects in the UAE, Jordan, and the UK, among other countries. He specializes in decision support and scenario planning for future foresight and strategic planning. The areas of expertise include working with major international organizations such as the United Nations Development Program in a number of countries, the USAID, USTD, the German Agency for Technical Cooperation, and the Arab Administrative Development Organization. Projects implemented in the UAE focused on education, excellence, strategic foresight. Prof. Al-Utaibi designed an award for excellence with a major component related to innovation management. He has over 20 years of experience in excellence awards assessment especially in the UAE and also in providing advice related to the qualifying of institutions for these awards. rofile which contains their education details, their publications, research work, membership, achievements, with photo that will be maximum 200-400 words.