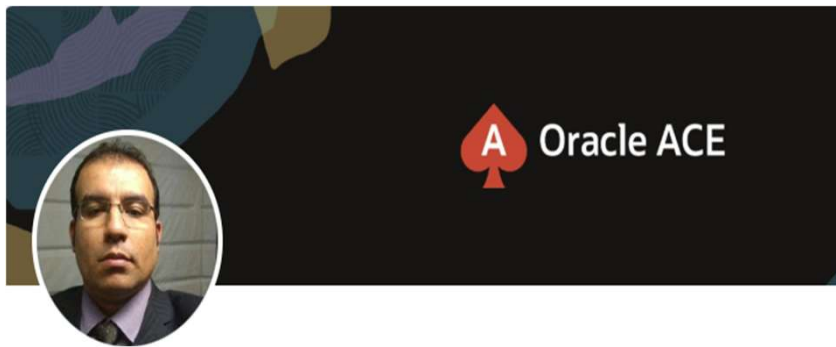
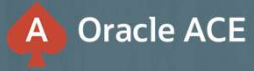


Who am I?



Regis Araujo

- Oracle Database Specialist
- Cylla Group
- 20/01/2026
- LinkedIn: <https://www.linkedin.com/in/dbaregisaraujo/>
- ACE Profile: <https://ace.oracle.com/ords/ace/profile/dbaregisaraujo>
- Blog: <https://fromdbatosgbd.wordpress.com/>



Tech Superstars Unite

Get worldwide recognition as an Oracle ACE



Oracle.com profile page



Swag, certification exam credit & event passes



Exclusive content



Networking events




Your own Oracle cloud account



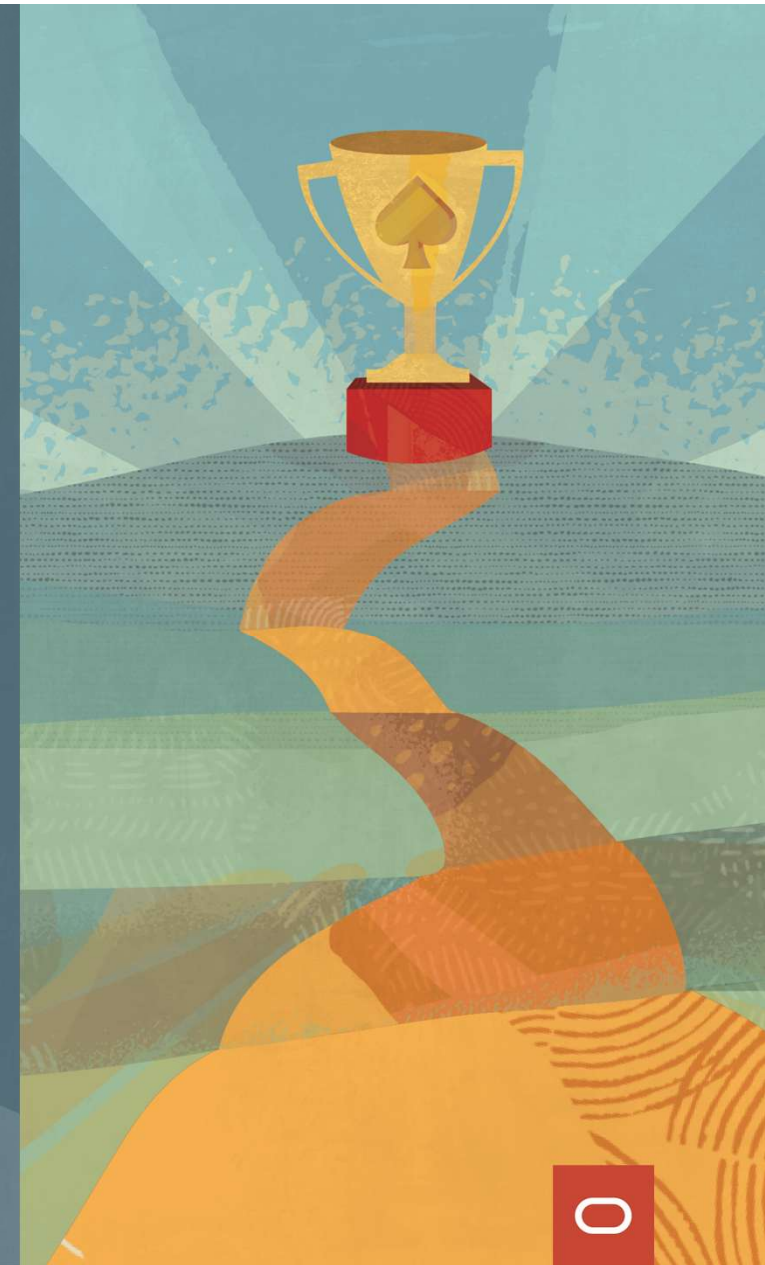
Travel support

 @oracleace

 [Linkedin.com/groups/72183](https://www.linkedin.com/groups/72183)

 @oracleace.bsky.social

Learn more at:
ace.oracle.com



HOW ORACLE DATAGUARD CAN SAVE THE DAY

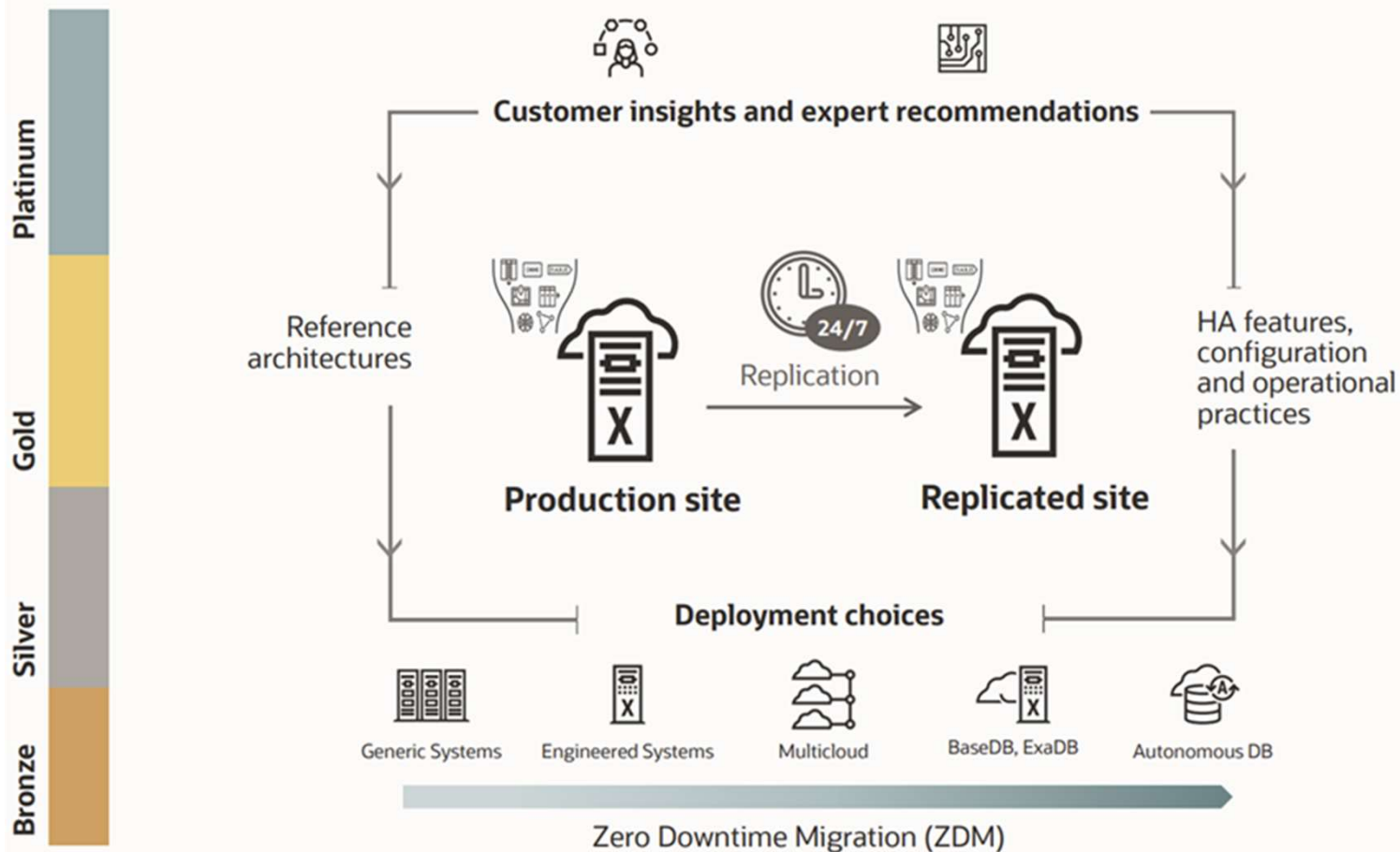
Oracle DataGuard Introduction

What is Oracle DataGuard

- Oracle Data Guard is a solution part of MAA architecture, that uses one or more copies of an Oracle Database, with the aim of implementing high availability, disaster Recovery and DataProtection;

Oracle Maximum Availability Architecture (MAA)

Standard Reference Architectures for Never-Down Deployments



Platinum
Gold
Silver
Bronze

- High performance**
 - Resource Management
 - Database In-Memory
 - True Cache
- Continuous availability**
 - Application Continuity
 - Online Redefinition
 - Edition-based Redefinition
- Data protection**
 - Flashback
 - RMAN
 - ZDLRA+ ZRCV
- Active replication**
 - Active Data Guard
 - Full Stack DR
 - GoldenGate
- Scale out & Lifecycle**
 - RAC
 - Globally Distributed Database
 - FPP
 - Real Application Testing

ORACLE DATA GUARD ROLES

PRIMARY		Is the main Database; <u>There can only be ONE in the configuration</u>
STANDBY	PHYSICAL	Identical copy of the Primary Database; Similar, block level disk structure; Synced via Redo apply.
	SNAPSHOT	Standby opened in Read-Write mode; After you can convert again in <i>Physical Standby</i> .
	LOGICAL	Same logical information as the database <i>Primary</i> ; Structure and physical organization may be different; Sync via sql instruction received from archive (Execute the same sql statement to sync).

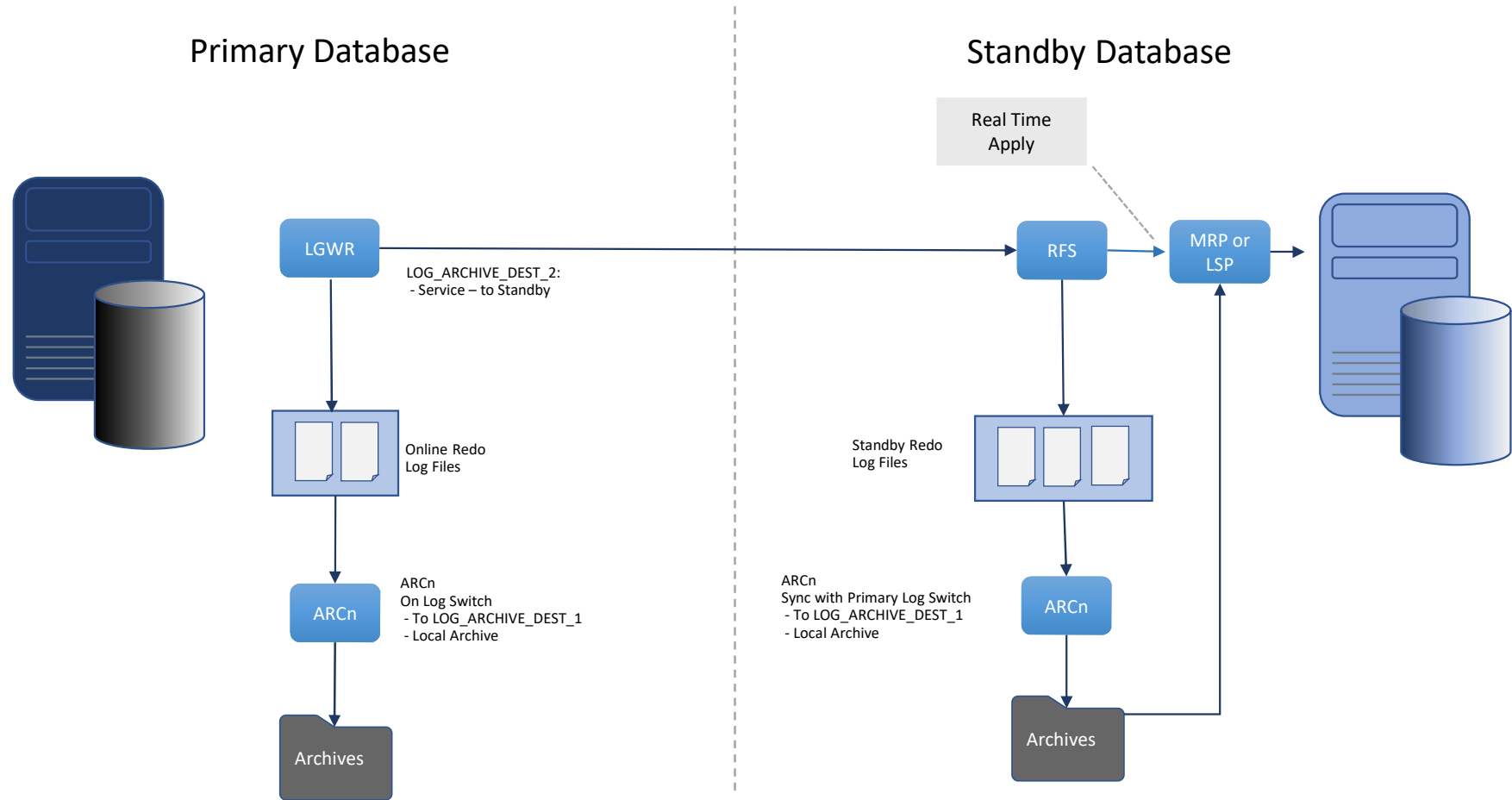
PROTECTION MODES

Protection Mode	Description	Data Protection
Maximum Availability	<ul style="list-style-type: none"> Database transactions are not acknowledged to an application as committed until an acknowledgement is received from the standby database that it has received all redo needed to recover the transaction; If standby don't return "received" information until NetTimeout parameter, the Standby will work as maximum performance until the response is under NetTimeout value. 	<ul style="list-style-type: none"> Any time that there is a loss of communication between the primary and standby database, Data Guard continuously pings the standby and automatically resynchronizes the configuration after the connection is reestablished. There is a potential for data loss if another outage impacts the production database before automatic resynchronization.
Maximum Performance <small>(default protection mode)</small>	<ul style="list-style-type: none"> This protection mode provides the highest level of data protection that is possible without affecting the performance of a primary database. This is accomplished by allowing transactions to commit as soon as all redo data generated by those transactions has been written to the online log. Redo data is also written to one or more standby databases. 	<ul style="list-style-type: none"> This protection mode offers slightly less data protection than maximum availability mode and has minimal impact on primary database performance.
Maximum Protection <small>(Recommendation minimum of 2 standby)</small>	<ul style="list-style-type: none"> Maximum protection is similar to maximum availability but provides an additional level of data protection in the event of multiple failure events. Unlike maximum availability, which allows the primary to continue processing if it is unable to receive acknowledgement from a standby database, maximum protection shuts the primary database down rather than allowing it to continue processing transactions that are unprotected. 	<ul style="list-style-type: none"> Prevent data loss.

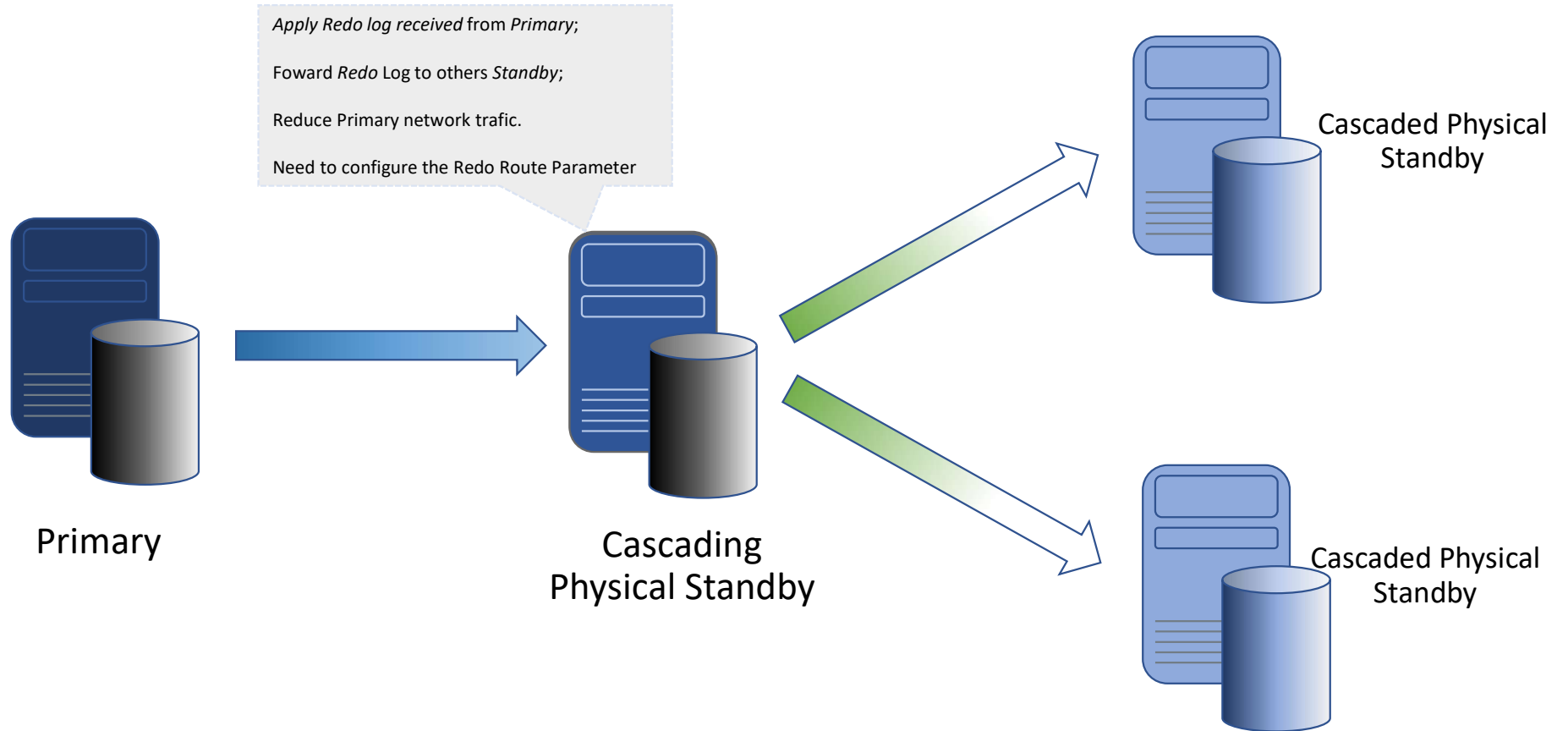
Advantages of Oracle Dataguard

- Integrates the maximul availability architecture for Oracle Databases;
- Offers greater data protection;
- Allows load Distribution:
 - You can use database copies for reports and to perform backup routines;
- Allows you to reduce downtime when updating Oracle Database.
- Offers easy recovery of database in case of disaster

Redo Transport and Redo Application Physical Standby



CASCADING



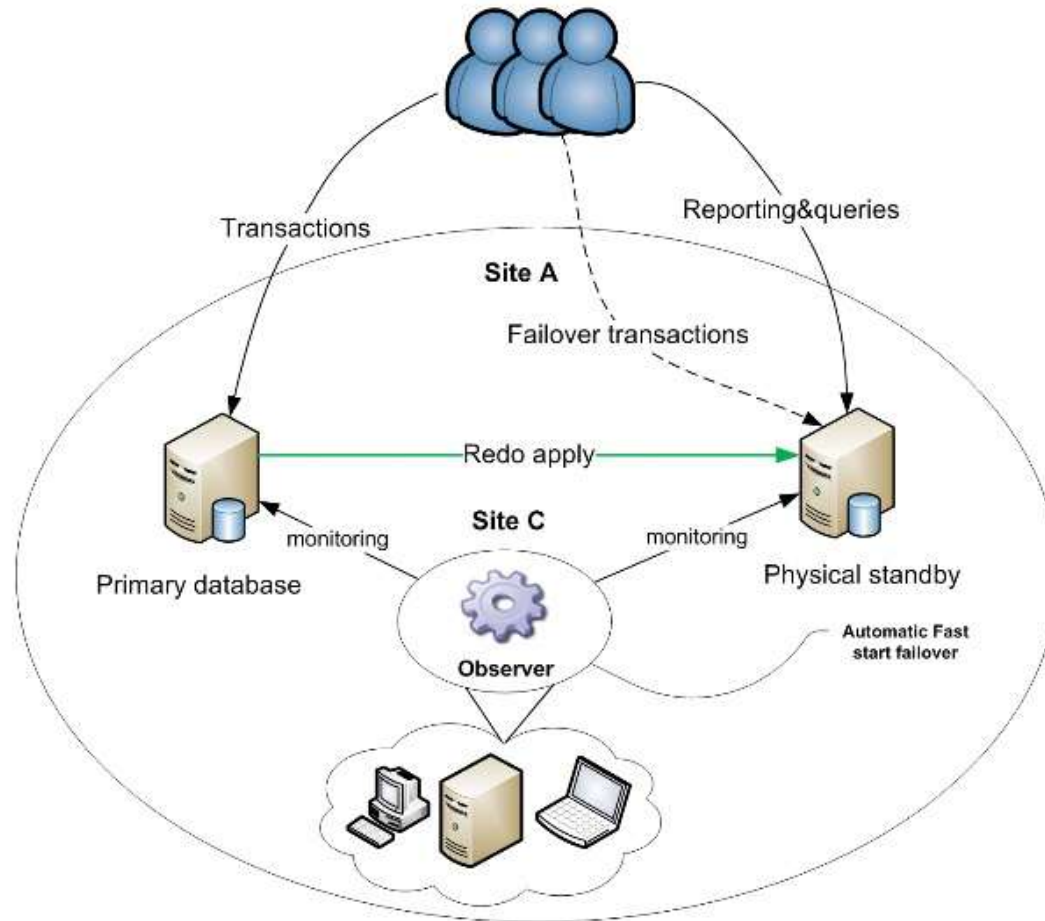
Real-time Cascading need licence "Oracle Active Data Guard Option".

Delay Apply

Delaymins

- The DelayMins configurable property specifies the number of minutes log apply services will delay applying the archived redo log data on the standby database.
- In case of any logical problem or human error (update without where)
- Recover can be executed stopping the apply and perform insert as select / merge / export import (snapshot standby).

OBSERVER – FAST START FAILOVER



CONDITIONS – FAST START FAILOVER

```
DGMGRL> ENABLE FAST_START FAILOVER CONDITION "Inaccessible Logfile";
Succeeded.
DGMGRL> show fast_start failover;
```

Fast-Start Failover: Enabled in Observe-Only Mode

```
Protection Mode: MaxAvailability
Lag Limit:      0 seconds

Threshold:      30 seconds
Active Target:  ██████████
Potential Targets: "██████████"
goldsl9c valid
Observer:       ██████████.oralocal
Shutdown Primary: TRUE
Auto-reinstate: TRUE
Observer Reconnect: (none)
Observer Override: FALSE
```

Configurable Failover Conditions

```
Health Conditions:
Corrupted Controlfile      YES
Corrupted Dictionary      YES
Inaccessible Logfile      YES
Stuck Archiver             NO
Datafile Write Errors     YES
```

```
Oracle Error Conditions:
(none)
```

DGMGRL>

```
DGMGRL> ENABLE FAST_START FAILOVER CONDITION 240;
Succeeded.
DGMGRL> show fast_start failover;
```

Fast-Start Failover: Enabled in Observe-Only Mode

```
Protection Mode: MaxAvailability
Lag Limit:      0 seconds

Threshold:      30 seconds
Active Target:  ██████████
Potential Targets: "██████████"
goldsl9c valid
Observer:       ██████████.oralocal
Shutdown Primary: TRUE
Auto-reinstate: TRUE
Observer Reconnect: (none)
Observer Override: FALSE
```

Configurable Failover Conditions

```
Health Conditions:
Corrupted Controlfile      YES
Corrupted Dictionary      YES
Inaccessible Logfile      NO
Stuck Archiver             NO
Datafile Write Errors     YES
```

Oracle Error Conditions:

```
ORA-240: control file enqueue held for more than *s seconds
```

Continuous Oracle Data Validation

Data Validation

- A Data Guard standby is an independent Oracle Database that uses media recovery to apply the changes to the standby database to maintain a synchronized physical replica of the primary. Oracle Database recovery processes perform continuous validation as changes are applied to the standby. This validation uses knowledge of Oracle redo and data block structures to check for physical data corruption, logical intra-block corruption and lost write corruption to insure the highest level of isolation between primary and standby

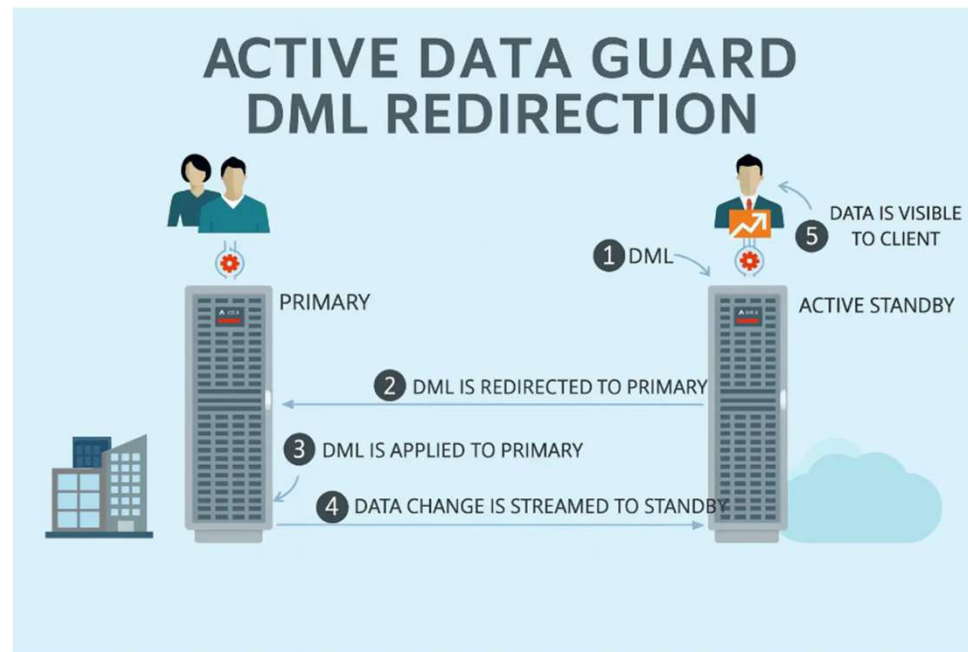
Automatic Repair

- Active Data Guard makes block level corruption invisible to users with no changes to application code. Block level corruption is caused by intermittent random I/O errors that can occur independently at either primary or standby databases. Under normal operation when an Oracle Database reads a block and detects corruption it marks the block as corrupt and reports the error to the application. No subsequent read of the block is successful until the block is recovered manually - unless you are using Active Data Guard. Active Data Guard automatically repairs physical block corruption at a primary database by retrieving a good version of the block(s) from the active standby. Conversely, corrupt blocks detected by either the apply process or by read-only users on the standby database are automatically repaired using the good version from the primary database. Both HA and data protection are maintained at all times

DML Redirection

Redirect Update/Delete/Insert to Primary

- Oracle Database 19c introduces the capability to execute Data Manipulation Language (DML) operations directly on an Active Data Guard standby database. This feature allows applications to benefit from using Active Data Guard for standby operations that require occasional writes, seamlessly redirecting DML operations to the primary database.
- When a DML operation is issued on the Active Data Guard standby database, it is transparently redirected to the primary database, where it is executed. The transaction's redo data is then sent back to the standby database to keep it synchronized.



Global Temporary Tables

Create Global Temporary Tables on Dataguard

- Oracle Database 18c introduces the capability to create global temporary tables to accept Data Manipulation Language (DML) operations directly on an Active Data Guard standby database.

Snapshot Standby

Open Standby in Read Write mode

- A snapshot standby database is a fully updateable standby database created by converting a physical standby database into a snapshot standby database.
- A snapshot standby database receives and archives, but does not apply, redo data from a primary database. The redo data received from the primary database is applied once a snapshot standby database is converted back into a physical standby database, after discarding all local updates to the snapshot standby database.
- Test Upgrade/Patch
- Troubleshooting
- Restore objects
- Validate new application features

Transparent Application Failover

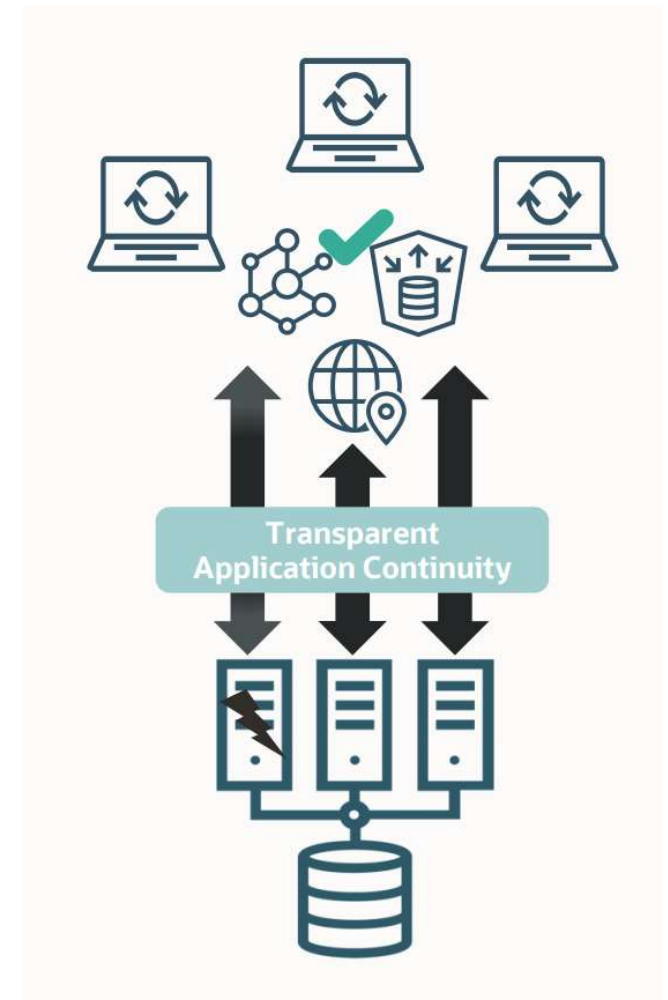
Oracle TAF

- TAF is a feature dating back to Oracle8i. Following an instance failure, TAF creates a new session and, when using SELECT mode, on demand, replays queries back to where they were before the failure occurred

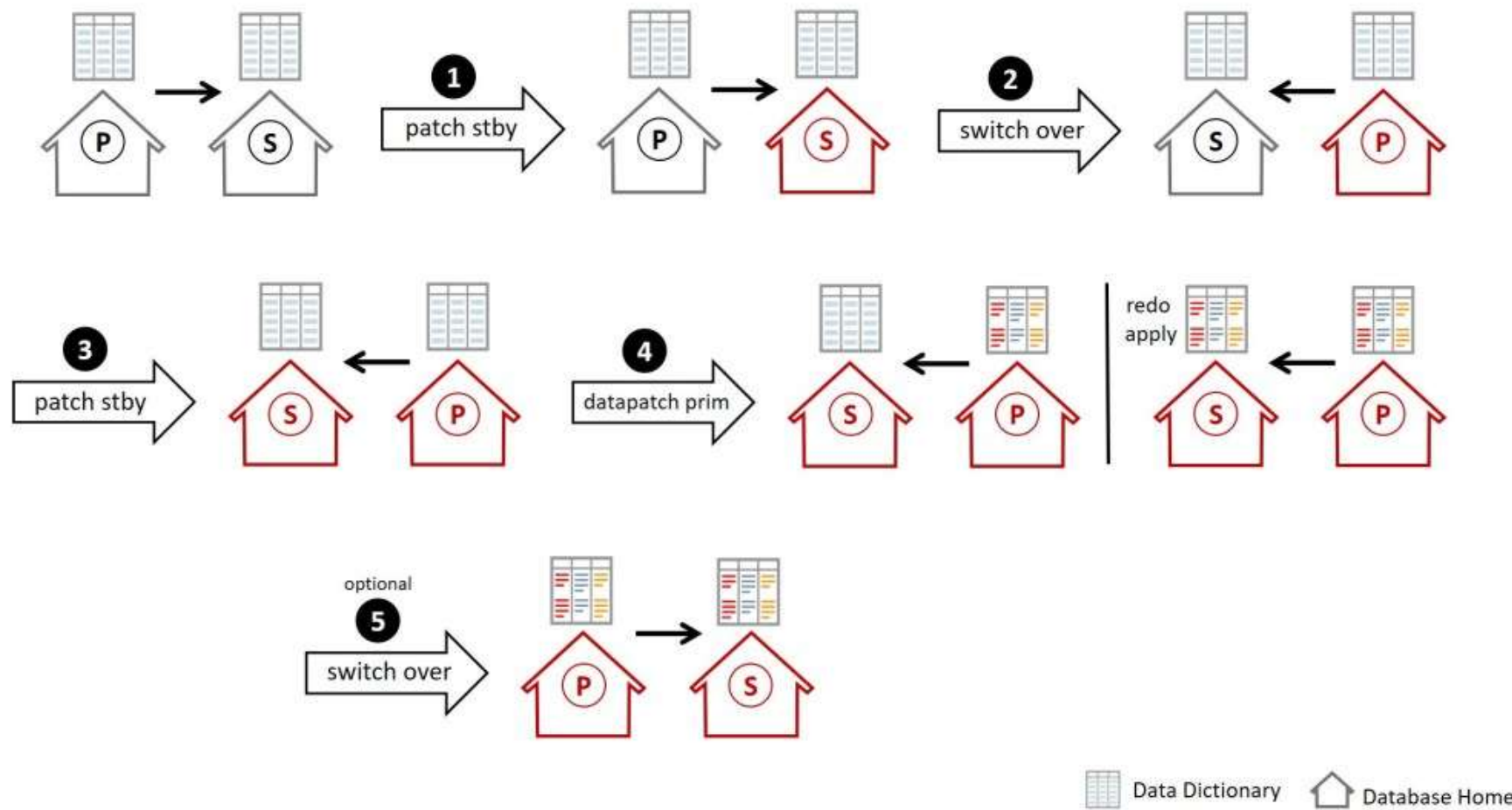
Transparent Application Continuity

Oracle TAC

- Starting with Oracle Database 18c, Transparent Application Continuity (TAC) transparently tracks and records session and transactional state so the database session can be recovered following recoverable outages. This is done without relying on application knowledge or code changes, allowing Transparent Application Continuity to be enabled for your applications. Application transparency and failover are achieved by consuming the state tracking information that captures and categorizes the session state usage as the application issues user calls.



Minimal Downtime Migration





That's all Folks!