Oracle Maximum
Availability Architecture

Deploying the Zero Data Loss Recovery Appliance in a Data Guard Configuration

ORACLE WHITE PAPER | MARCH 2018

ORACLE

Table of Contents

.

Introduction

The Zero Data Loss Recovery Appliance is the Oracle optimized solution for backup and recovery. The Recovery Appliance fundamentally changes how backup and recovery is performed by enabling incremental forever backups and efficient any point-in-time restore. No other backup and recovery solution can match the Recovery Appliance in terms of data protection, operational and system resource efficiency, its ability to scale, and its unique level of backup validation that ensures successful recovery.

Data Guard is the real-time data protection and availability solution for the Oracle Database. It is the Oracle solution for maintaining a synchronized, hot copy of an Oracle Database at a remote location for disaster recovery and availability. Data Guard is differentiated from the Recovery Appliance by its ability to provide an already running, synchronized copy of the production database that can immediately resume a full level of service should an outage occur – no restore required.

This best practice paper is intended for a technical audience wishing to deploy Recovery Appliances in multiple locations that also host Data Guard configurations:

- Data Guard is used to provide High Availability (HA) and disaster protection by enabling immediate failover to a synchronized copy at a second location should a database or site go offline.
- Recovery Appliances are deployed at each location to provide local backup and recovery for databases hosted at that location – including Data Guard primary or standby databases.
- Finally, because a Data Guard physical standby database is an exact copy of production, real-time backups taken by either Recovery Appliance can be used to restore primary or standby databases at either location should a local appliance be unavailable.

The recommendations included in this paper result in achieving the optimal level of HA and data protection while conserving network bandwidth. All procedures described in the following sections apply equally to either Data Guard or Active Data Guard physical standby databases.

Overview

This paper describes two scenarios that have the same configuration as an end-goal: a Data Guard primary database in London backing up to a Recovery Appliance in London and a remote standby database in Philly that backs up to a Recovery Appliance also located in Philly. See Figure 1.

Each scenario has a different starting configuration:

- The first scenario begins with an existing Data Guard configuration that includes both a primary and a standby database, and adds a Recovery Appliance at each site.
- The second scenario begins with only a production database and a Recovery Appliance in London, and adds a Data Guard standby and a Recovery Appliance in Philly.

The last section of this paper explains what happens after a Data Guard role transition in the fully-integrated Data Guard and Recovery Appliances environment.

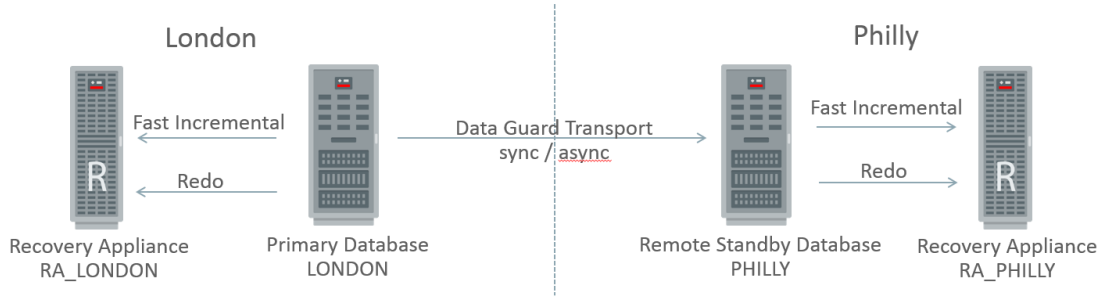

Figure 1. Final Configuration for Both Integration Scenarios

The Data Guard standby databases in this paper utilize the RMAN block change tracking file to perform fast incremental backups and Real-Time Cascade to forward redo to the local Recovery Appliance in real time. An Active Data Guard license is required to use fast incremental backup on a standby database. An Active Data Guard license is not required when only using real-time cascade from standby to local Recovery Appliance. The same procedures apply whether the standby is Data Guard or Active Data Guard.

Prerequisites

The procedures described in this paper were validated against Oracle Database 11gR2 (11.2.0.4) and Oracle Database 12c (12.1.0.2), and they assume the following:

- The Recovery Appliances (RA_LONDON and RA_PHILLY) have already been deployed and discovered as targets in Enterprise Manager Cloud Control.
- The database targets have also been discovered.
- For the first scenario, the remote standby database has been discovered, and Data Guard Broker is configured and running.

Deploying Recovery Appliances with an Existing Data Guard Environment

The first scenario begins with a primary database (SIEBEL_LONDON) and a standby database (SIEBEL_PHILLY), as shown in Figure 2.

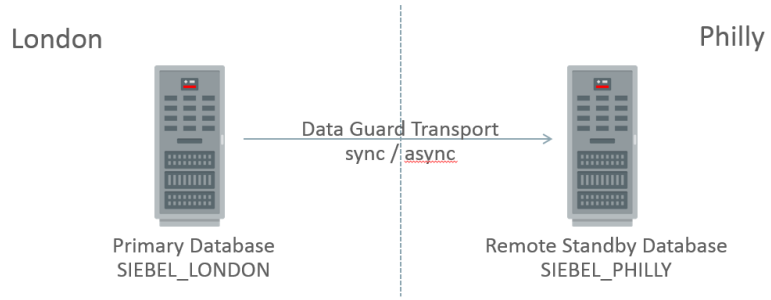

Figure 2. Initial Configuration of the Data Guard Environment

The procedure adds two Recovery Appliances, RA_LONDON and RA_PHILLY, in their respective locations, as shown in Figure 3. Each database in the Data Guard configuration can perform fast-incremental backups and ship redo in real time to the local Recovery Appliance. Either database can use the remote Recovery Appliance for recovery in the event that its local Recovery Appliance is unavailable. Data Guard redo transport between the primary and the standby eliminates the need to replicate backups between Recovery Appliances.

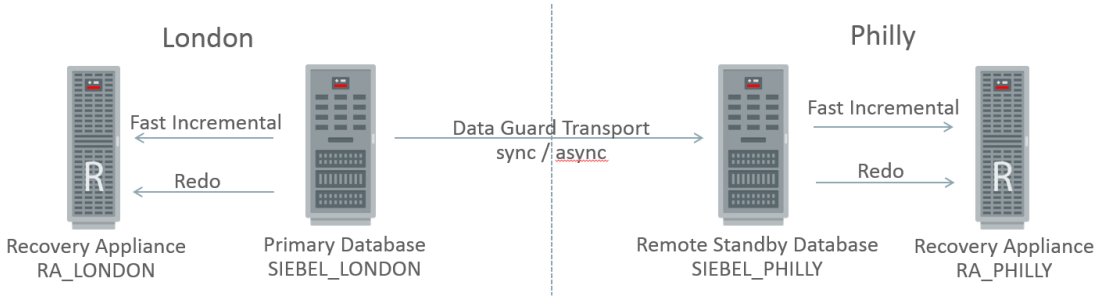

Figure 3. Final Configuration with Recovery Appliances Integrated into the Data Guard Environment

There are two steps to this procedure: adding the first Recovery Appliance in London and then adding the second Recovery Appliance in Philly.

Add the RA_LONDON Recovery Appliance to the Configuration

This step of the procedure produces the configuration shown in Figure 4.

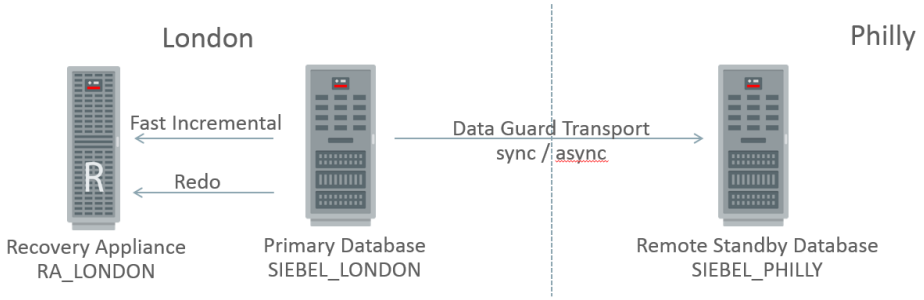

Figure 4. Recovery Appliance RA_LONDON Added to the Data Guard Environment

- Ensure that the following preconditions are met:
  - Both the primary and the standby databases were correctly discovered in Enterprise Manager Cloud Control.
  - Both databases have Flashback Database enabled with a 1-hour flashback retention target.
  - The RA_LONDON Recovery Appliance was discovered in Enterprise Manager.
- Create a protection policy on the RA_LONDON Recovery Appliance (if required):
  - Log in to Enterprise Manager Cloud Control, navigate to Targets -> Recovery Appliances, and select the RA_LONDON Recovery Appliance.
  - Navigate to the Recovery Appliance -> Protection Policies page, and click **Create**.
- Create the Recovery Appliance user in the RA_LONDON database (if required):
  - Navigate to the Schema -> Users page for the RA_LONDON cluster database target.

The Recovery Appliance user account must have the "create session" system privilege only. No other system privilege or role should be granted to this account.

- Add the SIEBEL_LONDON database to the desired protection policy on RA_LONDON:
  - Navigate to the Recovery Appliance -> Protected Databases page, and click **Add** to add the SIEBEL_LONDON database.
  - Click **Add**, and select the SIEBEL_LONDON database that has previously been discovered in Enterprise Manager.
  - Select the desired protection policy.
  - Specify the amount of space to be reserved for the SIEBEL_LONDON database.
  - Add the new Recovery Appliance user or select an existing named credential, and click **OK**.
- Register the SIEBEL_LONDON database with the RA_LONDON appliance:
  - Navigate to the Availability -> Backup & Recovery -> Backup Settings page for the SIEBEL_LONDON cluster database target.
  - Select the Recovery Appliance and virtual private catalog user from the drop-down lists, and click **Apply**.

- Enroll the SIEBEL_PHILLY database with the RA_LONDON appliance to allow the database to be restored directly from RA_LONDON to SIBEL_PHILLY:
  - Navigate to the Availability -> Backup & Recovery -> Backup Settings page for the SIEBEL_PHILLY cluster database target.
  - Select **Configure this physical standby database to send backups to the specified Recovery Appliance**, and click **Apply**.
- Change configuration settings for the SIEBEL_LONDON and SIEBEL_PHILLY databases:
  - The following changes are considered best practices when working with the Recovery Appliance, and can be set from Enterprise Manager or from the Recovery Manager CLI:
    - CONFIGURE BACKUP OPTIMIZATION ON;
    - CONFIGURE CONTROLFILE AUTOBACKUP ON;
    - CONFIGURE DEFAULT DEVICE TYPE TO 'SBT_TAPE';
    - CONFIGURE DEVICE TYPE 'SBT_TAPE' PARALLELISM 8;
    - Enable the Block Change Tracking File feature.
    - Enable the Flashback Database feature with a minimum of 60 minute retention to avoid recreation of the standby database following a failover.
- Back up the SIEBEL_LONDON database to the RA_LONDON appliance.
  - The following Recovery Manager script is considered best practice when creating the first backup with the Recovery Appliance:
    - RMAN> backup cumulative incremental level 0 filesperset 1 section size 64g database plus archivelog filesperset 32;
  - RMAN tags may be added as required.
- Create the virtual private catalog user on the SIEBEL_LONDON database:
  - Navigate to the Schema -> Users page for the SIEBEL_LONDON cluster database target.

The virtual private catalog user must be created in the protected database to allow Data Guard Redo Transport to continue to operate between the primary database and the physical standby database.

The virtual private catalog user must have "create session" and "sysoper" system privileges. Optionally, for Oracle Database 12c protected databases, you may grant the "sysdg" system privilege to the user. No other system privilege or role should be granted to this user.

  - Force a log switch before continuing, and ensure that the redo has been applied on all standby databases.
- Copy the password file to all Data Guard environments.

The previous step modified the current password file by adding the virtual private catalog user. This step is required to replicate the password file modification to all standby databases.

  - Use the ASMCMD utility with O/S tools to copy the password file from the SIEBEL_LONDON database to the SIEBEL_PHILLY database.

» Enable real-time redo transport from the SIEBEL_LONDON database to the RA_LONDON appliance.

The steps immediately below are applicable only for Oracle Database 12c protected databases. The step requires an outage because the database must be restarted. The restart is required to allow the Oracle instances to access the newly created wallet that will be used by the log transport mechanism to send real-time redo to the Recovery Appliance. If a database outage is not possible now, you can perform this step manually and in a rolling fashion, by restarting one instance at a time. For instructions on how to do this, see Appendix 1.

For Oracle Database 11gR2 protected databases, follow the instructions in Appendix 1.

- » Navigate to the Availability -> Data Guard Administration page for the SIEBEL_LONDON cluster database target.
- » Click **Add Recovery Appliance**, and select the RA_LONDON appliance and the appropriate virtual private catalog (VPC) user from the drop-down list.
- » Select the named credentials for the SIEBEL_LONDON and SIEBEL_PHILLY databases, and click **Submit**.

At this point, the primary database should be using real-time redo transport to send redo to the RA_LONDON appliance.

» For Oracle Database 12c protected databases, configure RedoRoutes to ensure that SIEBEL_LONDON always sends redo to the RA_LONDON appliance:

- » Navigate to the Availability -> Data Guard page for the SIEBEL_LONDON cluster database target.
- » Click **Edit** to edit the primary cluster database properties, and click the **Common Properties** tab on the Edit Primary Database Properties page.
- » Enter the RedoRoutes string as follows, and click **Apply**:

```
(siebel_london : siebel_philly, zdlra2 ASYNC)(siebel_philly : zdlra2 ASYNC)
```

The context of the string is the database being edited, i.e., SIEBEL_LONDON. This string is interpreted as: "When SIEBEL_LONDON is the primary database, configure its log archive destinations to send redo to both SIEBEL_PHILLY and to the appliance ("zdlra2" is the alias for the RA_LONDON appliance). When SIEBEL_PHILLY is the primary database, configure SIEBEL_LONDON's log archive destination to send redo only to the appliance (zdlra2)."

» For Oracle Database 12c protected databases, configure RedoRoutes to ensure that SIEBEL_PHILLY never sends redo to the RA_LONDON appliance:

- » Navigate to the Availability -> Data Guard page for the SIEBEL_LONDON cluster database target.
- » Select the SIEBEL_PHILLY standby cluster database, click **Edit** to edit the standby database properties, and click the **Common Properties** tab on the Edit Primary Database Properties page.
- » Enter the RedoRoutes string as follows, and click **Apply**:

```
(siebel_philly: siebel_london)
```

The context of the string is the database being edited, i.e., SIEBEL_PHILLY. This string is interpreted as: "When SIEBEL_PHILLY is the primary database, configure its log archive destinations to send redo to SIEBEL_LONDON. If SIEBEL_PHILLY is not the primary database, then do not configure any log archive destinations for it."

Add the RA_PHILLY Recovery Appliance to the Configuration

This step of the procedure produces the final configuration, shown in Figure 5.

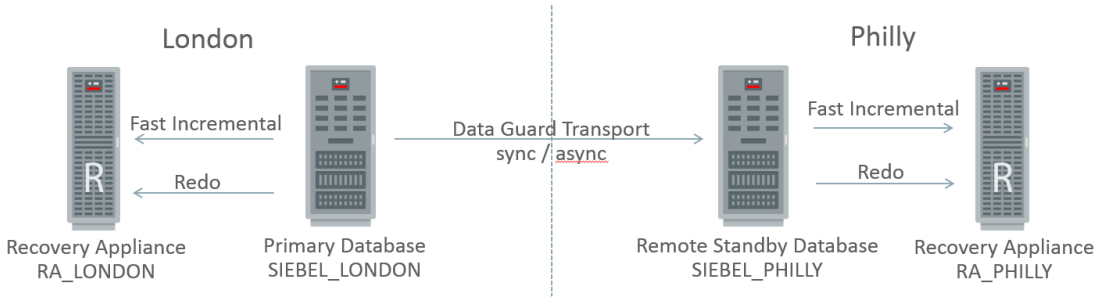

Figure 5. Final Configuration with Recovery Appliance Integrated into the Data Guard Environment

» Create a protection policy on the Recovery Appliance RA_PHILLY (if required):
  » Navigate to the Recovery Appliance -> Protection Policies page, and click **Create**.

The values for the protection policy on the RA_PHILLY appliance can be different from those on the RA_LONDON appliance.

» Create the Recovery Appliance user in the RA_PHILLY database (if required):
  » Navigate to the Schema -> Users page for the RA_PHILLY cluster database target.

The Recovery Appliance user account must have the "create session" system privilege only. No other system privilege or role should be granted to the user.

» Add the SIEBEL_LONDON database to the desired protection policy on RA_PHILLY:

If you select the SIEBEL_PHILLY database in this step, then before you perform the step to register the database, you must perform a Data Guard switchover to make SIEBEL_PHILLY the primary cluster database. If you cannot perform the switchover to SIEBEL_PHILLY, the SIEBEL_PHILLY database will still be backed up to the RA_PHILLY appliance, but the RA_PHILLY appliance Protected Databases page will display SIEBEL_LONDON.

The procedure assumes a switchover is not performed at this time. Therefore, SIEBEL_LONDON is the primary cluster database.

- Navigate to the Recovery Appliance -> Protected Databases page, and click **Add** to add the SIEBEL_LONDON database.
- Click **Add**, and select the SIEBEL_LONDON database that was previously discovered in Enterprise Manager.
- Select the desired protection policy.
- Specify the amount of space to be reserved for the SIEBEL_LONDON database.
- Add the new Recovery Appliance user or select an existing named credential, and click **OK**.

- Register the SIEBEL_LONDON database with the RA_PHILLY appliance:
  - Navigate to the Availability -> Backup & Recovery -> Backup Settings page for the SIEBEL_LONDON cluster database target.
  - (The Recovery Appliance setting will display the RA_LONDON appliance.) Click **Clear Configuration**.
  - Select the Philly Recovery Appliance and the virtual private catalog user from the drop-down lists, and click **Apply**.
- Enroll the SIEBEL_PHILLY database with the RA_PHILLY appliance:
  - Navigate to the Availability -> Backup & Recovery -> Backup Settings page for the SIEBEL_PHILLY cluster database target.
  - (The Recovery Appliance setting will display the RA_LONDON appliance.) Click **Clear Configuration**.
  - Select **Configure this physical standby database to send backups to the specified Recovery Appliance**. The greyed-out box will display the Philly Recovery Appliance.
  - Click **Apply**.
- Re-enroll the SIEBEL_LONDON database with the RA_LONDON appliance:
  - Navigate to the Availability -> Backup & Recovery -> Backup Settings page for the SIEBEL_LONDON cluster database target.
  - (The Recovery Appliance setting will display the RA_PHILLY appliance.) Click **Clear Configuration**.
  - Select the London Recovery Appliance and the virtual private catalog user for SIEBEL_LONDON from the drop-down lists, and click **Apply**.
- Back up the SIEBEL_PHILLY database to RA_PHILLY appliance:
  - The following Recovery Manager script is considered best practice when creating the first backup on the Recovery Appliance:
    - RMAN> backup cumulative incremental level 0 filesperset 1 section size 32g database plus archivelog filesperset 32;
  - RMAN tags may be added as required.
- Enable real-time redo transport from the SIEBEL_PHILLY database to the RA_PHILLY appliance:

The steps immediately below are applicable only for Oracle Database 12c protected databases. The step requires an outage because the database must be restarted. The restart is required to allow the Oracle instances to access the newly created wallet that will be used by the log transport mechanism to send real-time redo to the Recovery Appliance.

If an outage is not possible now, you can perform this step manually and in a rolling fashion, by restarting one instance at a time. For instructions on how to do this, see Appendix 2.

For Oracle Database 11gR2 protected databases, follow the instructions in Appendix 2.

Additionally, the Data Guard page will report the Data Guard status as being in ERROR, and that the newly added RA_PHILLY is not receiving redo data. This ERROR will be resolved when the RedoRoutes are configured in the next step.

  - » Navigate to the Availability -> Data Guard page for the SIEBEL_PHILLY cluster database target.
  - » Click **Add Recovery Appliance**, and select the RA_PHILLY appliance and the appropriate virtual private catalog (VPC) user from the drop-down list.
  - » Select the named credentials for the SIEBEL_PHILLY and SIEBEL_LONDON databases, and click **Submit**.
- » For Oracle Database 12c protected databases, configure RedoRoutes to ensure that SIEBEL_PHILLY always sends redo to the RA_PHILLY appliance:
  - » Navigate to the Availability -> Data Guard page for the SIEBEL_PHILLY cluster database target.
  - » Click **Edit** to edit the standby cluster database properties, and click the **Common Properties** tab on the Edit Primary Database Properties page.
  - » Enter the RedoRoutes string as follows, and click **Apply**:

```
(siebel_philly : siebel_london, zdlra6 ASYNC)(siebel_london : zdlra6 ASYNC)
```

The context of the string is the database being edited, i.e., SIEBEL_PHILLY. The string is interpreted as "When SIEBEL_PHILLY is the primary database, configure its archive destinations to send redo to both SIEBEL_LONDON and the appliance ("zdlra6" is the alias for the RA_PHILLY appliance). When SIEBEL_LONDON is the primary database, configure the log archive destinations of the SIEBEL_PHILLY database to send redo only to the appliance (zdlra6)."

- » For Oracle Database 12c protected databases, configure the RMAN channel for the SIEBEL_LONDON database to connect to the RA_LONDON appliance:
  - » If the Data Guard Add Recovery Appliance wizard was used, then the RMAN channel definition for the SIEBEL_LONDON database points to the RA_PHILLY Recovery Appliance. Change only the credential_alias ENV variable in the CONFIGURE CHANNEL DEVICE TYPE SBT clause to point the alias to the RA_LONDON appliance instead, e.g.:
    - CONFIGURE CHANNEL DEVICE TYPE 'SBT_TAPE' FORMAT '%d_%U' PARMS "SBT_LIBRARY=/u01/app/oracle/product/12.1.0.2/dbhome_3/lib/libra.so, ENV=(RA_WALLET='location=file:/u01/app/oracle/product/12.1.0.2/dbhome_3/dbs/zdlra credential_alias=**scaz10ingest-scan1:1521/zdlra6:dedicated**')";
  - » Must be changed to:
    - CONFIGURE CHANNEL DEVICE TYPE 'SBT_TAPE' FORMAT '%d_%U' PARMS "SBT_LIBRARY=/u01/app/oracle/product/12.1.0.2/dbhome_3/lib/libra.so, ENV=(RA_WALLET='location=file:/u01/app/oracle/product/12.1.0.2/dbhome_3/dbs/zdlra credential_alias=**scas10ingest-scan5:1521/zdlra2:dedicated**')";
- » Configure the RMAN archive log deletion policy for the SIEBEL_LONDON and SIEBEL_PHILLY databases.
  - » To allow the Flash Recovery Area to be purged automatically after the archive logs have been sent to the Recovery Appliance and applied on the physical standby database:
    - CONFIGURE ARCHIVELOG DELETION POLICY TO APPLIED ON ALL STANDBY BACKED UP 1 TIMES TO 'SBT_TAPE';
- » Configure the RMAN db_unique_name connection strings.
  - » To allow RMAN to log in to the primary database in order to resync the catalog, the following changes are required on the SIEBEL_LONDON database:
    - CONFIGURE DB_UNIQUE_NAME 'siebel12c_london' CONNECT IDENTIFIER 'scam06client-scan1/siebel12c_london';

- CONFIGURE DB_UNIQUE_NAME 'siebel12c_philly' CONNECT IDENTIFIER 'scam06client-scan5/siebel12c_philly';

» To replicate these settings in the SIEBEL_PHILLY database, use RMAN to connect to the SIEBEL_LONDON target database and the RA_PHILLY catalog:
  - $ rman target / catalog /@scaz10ingest-scan1:1521/zdlra6:dedicated
  - RMAN> resync catalog;
  - RMAN> show db_unique_name;

At this point you should have a fully-configured Data Guard environment with a Recovery Appliance in each data center. The system will provide the following benefits:

» Backup windows are greatly reduced because incremental backups are sent to the local Recovery Appliance.
» Data loss is minimized, even for double failures, because redo is sent to the local Recovery Appliance.
» Restore operations can leverage either Recovery Appliance.
» Recovery time is minimal because you can fail over by using Data Guard.

Creating a New Data Guard Configuration and Deploying Recovery Appliances

This procedure starts with a standalone database PSFT_LONDON, as shown in Figure 6. It achieves the same outcome as the previous scenario; the only difference is that it includes the creation of the standby database in addition to the deployment of Recovery Appliances.

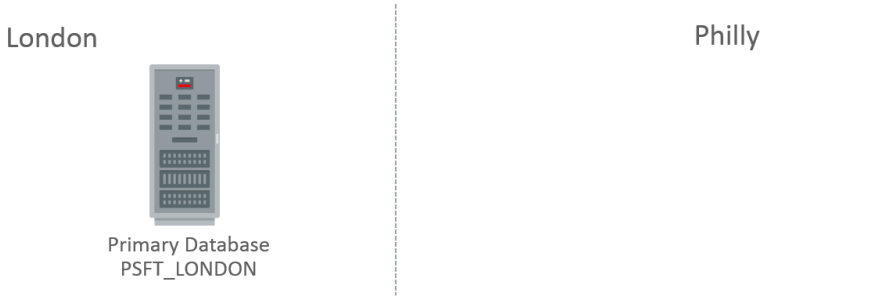

Figure 6. Initial Configuration with the Primary Database

This procedure has three steps: adding a Recovery Appliance (RA_LONDON), adding a Data Guard database (PSFT_PHILLY), and adding a Recovery Appliance (RA_PHILLY). The final configuration is shown in Figure 7.

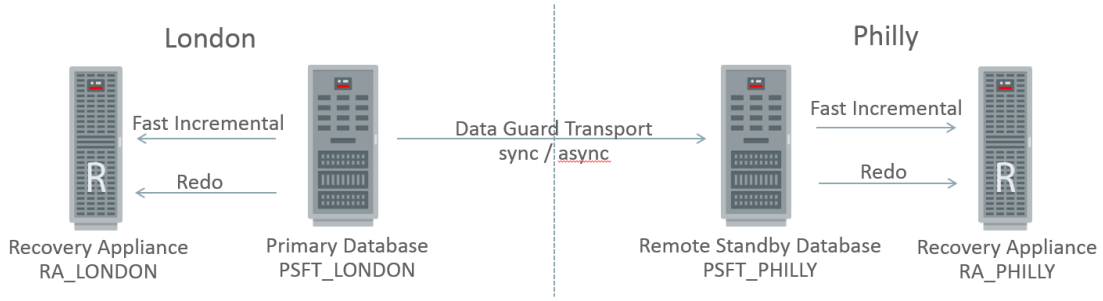

Figure 7. Final Configuration with Recovery Appliances and a Remote Standby Database Fully Integrated

Add the RA_LONDON Recovery Appliance to the Configuration

This step of the procedure produces the configuration shown in Figure 8.

Figure 8. Recovery Appliance RA_LONDON Added to the Primary Database

- Ensure that the following preconditions are met:
  - The primary database is discovered in Enterprise Manager Cloud.Control.
  - The RA_LONDON Recovery Appliance is discovered in Enterprise Manager.
- Create a protection policy on the RA_LONDON Recovery Appliance (if required):
  - In Enterprise Manager Cloud Control, navigate to the Recovery Appliance -> Protection Policies page, and click **Create**.
- Create the Recovery Appliance user in the RA_LONDON database (if required):
  - Navigate to the Schema -> Users page for the RA_LONDON cluster database target.

The Recovery Appliance user account must have the "create session" system privilege only. No other system privilege or role should be granted to this account.

- Add the PSFT_LONDON database to the desired protection policy on the RA_LONDON appliance:
  - Navigate to the Recovery Appliance -> Protected Databases page, and click **Add** to add the PSFT_LONDON database.
  - Click **Add**, and select the PSFT_LONDON database that was previously discovered in Enterprise Manager.
  - Select the desired protection policy.

- Specify the amount of space to be reserved for the PSFT_LONDON database.
- Add the new Recovery Appliance user or select an existing named credential, and click **OK**.

» Register the PSFT_LONDON database with the RA_LONDON appliance:

- Navigate to the Availability -> Backup & Recovery -> Backup Settings page for the PSFT_LONDON cluster database target.
- Select the Recovery Appliance and virtual private catalog user from the drop-down lists, and click **Apply**.

» Change configuration settings for PSFT_LONDON database:

- The following changes are considered best practices when working with the Recovery Appliance, and can be set from Enterprise Manager or from the Recovery Manager CLI:
  - CONFIGURE BACKUP OPTIMIZATION ON;
  - CONFIGURE CONTROLFILE AUTOBACKUP ON;
  - CONFIGURE DEFAULT DEVICE TYPE TO 'SBT_TAPE';
  - CONFIGURE DEVICE TYPE 'SBT_TAPE' PARALLELISM 8;
  - Enable the Block Change Tracking File feature.
  - Enable the Flashback Database feature with a minimum of 60 minute retention to avoid recreation of the standby database following a failover.

» Back up the PSFT_LONDON database to the RA_LONDON appliance.

- The following Recovery Manager script is considered best practice when creating the first backup with the Recovery Appliance:
  - RMAN> backup cumulative incremental level 0 filesperset 1 section size 32g database plus archivelog filesperset 32;
- RMAN tags may be added as required.

» Create the virtual private catalog user on the PSFT_LONDON database:

This step is a prerequisite for adding the physical standby database. You can perform the step at a later time, but doing so would require an additional outage.

When Data Guard is configured outside of a Recovery Appliance environment, the redo_transport_user parameter is left as null and the system uses the SYS user as the default. Because the primary and standby databases have a SYS user, this step is not normally performed. To use a redo transport user other than SYS for Data Guard transport, you must create this Oracle user in the primary database and grant the necessary system privileges before the standby database is instantiated.

The subsequent step that enables the real-time redo transport user sets the database init.ora parameter redo_transport_user to "vpcuser". This step does not need to create the Oracle user in the protected database because that database will not receive redo from the appliance. However, the creation of the redo transport user in the PSFT_LONDON database is needed for creating the physical standby database in a later step, and performing this step later would require an additional restart.

For Oracle Database 11gR2, ensure that you refresh the orapwd file for all nodes in the cluster.

- Navigate to the Schema -> Users page for the PSFT_LONDON cluster database target.

The virtual private catalog user must have "create session" and "sysoper" system privileges. Optionally, for Oracle Database 12c protected databases, the "sysdg" system privilege may also be granted to the user. No other system privilege or role should be granted to the user.

- Force a log switch before continuing, and ensure that the redo has been applied on all standby databases.

» Enable real-time redo transport from the PSFT_LONDON database to the RA_LONDON appliance.

This step requires an outage because the database must be restarted. The restart is required to allow the Oracle instances to access the newly created wallet that will be used by the log transport mechanism to send real-time redo to the Recovery Appliance.

If a database outage is not possible now, you can perform this step manually and in a rolling fashion, by restarting one instance at a time. For instructions on how to do this, see Appendix 3.

- Navigate to the Availability -> Backup & Recovery -> Backup Settings page for the PSFT_LONDON cluster database target.
- In the Recovery Appliance Settings section, select **Enable Real-Time Redo Transport**, and click **Apply**.

At this point you should be able to back up the PSFT_LONDON database to the RA_LONDON appliance. Also, the database should be using real-time redo transport to send redo to the RA_LONDON appliance.

Add the PSFT_PHILLY Remote Standby Database to the Configuration

This step of the procedure produces the configuration shown in Figure 9.

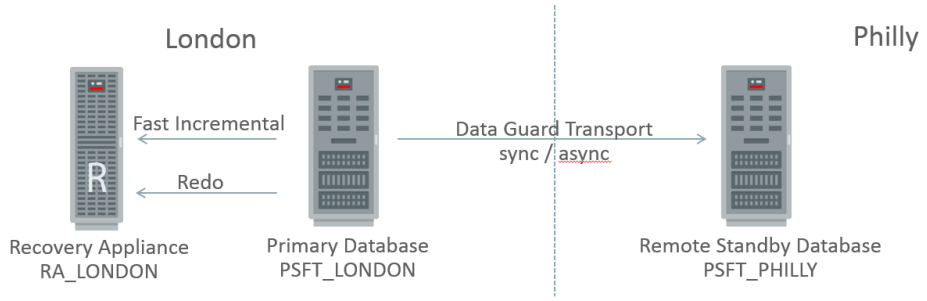

Figure 9. Remote Standby Database PSFT_PHILLY Added to the Configuration

» If you have not already done so, create the virtual private catalog user for the PSFT_LONDON database:

- Navigate to the Schema -> Users page for the PSFT_LONDON cluster database target.

The virtual private catalog user must have "create session" and "sysoper" system privileges. Optionally, the "sysdg" system privilege may be granted to the user. No other system privilege or role should be granted to the user.

- Force a log switch before continuing, and ensure that the redo has been applied on all standby databases.

- Create the physical standby database PSFT_PHILLY:
  - Navigate to the Availability -> Add Standby Database wizard, and follow the steps to complete the process.
- Manually correct the database instance name recorded in the Oracle Cluster Registry:

This step is required for Oracle Bug# 20365706.

  - $ srvctl config database –d PSFT_PHILLY
  - $ srvctl modify database –d PSFT_PHILLY –l psft
- Change configuration settings for the PSFT_PHILLY database:
  - The control file for PSFT_PHILLY was copied from PSFT_LONDON as part of the Add Standby Database wizard. Correct the location of the SNAPSHOT CONTROLFILE:
    - CONFIGURE SNAPSHOT CONTROLFILE NAME TO '+RECOC1/PSFT_PHILLY/snapcf_psft.f';
    - Enable the Block Change Tracking File feature.
    - Enable the Flashback Database feature with a minimum of 60 minute retention to avoid recreation of the standby database following a failover.
- Add the Recovery Appliance RA_LONDON to the Data Guard broker configuration:

This step is only for Oracle Database 12c protected databases. The step will restart the physical standby database, but should not restart the primary database.

  - Navigate to the Availability -> Data Guard page for the PSFT_LONDON cluster database target.
  - Click **Add Recovery Appliance**, and select the RA_LONDON appliance and the appropriate virtual private catalog user from the drop-down list.
  - Select the named credentials for the PSFT_LONDON and PSFT_PHILLY databases, and click **Submit**.
- For Oracle Database 12c protected databases, configure RedoRoutes to ensure that PSFT_LONDON always sends redo to the RA_LONDON appliance:
  - Navigate to the Availability -> Data Guard page for the PSFT_LONDON cluster database target.
  - Click **Edit** to edit the primary cluster database properties, and click the **Common Properties** tab on the Edit Primary Database Properties page.
  - Enter the RedoRoutes string as follows, and click **Apply**:

```
(psft_london : psft_philly, zdlra2 ASYNC)(psft_philly : zdlra2 ASYNC)
```

The context of the string is the database being editing, i.e., PSFT_LONDON. The string is interpreted as "When PSFT_LONDON is the primary database, configure its log archive destinations to send redo to both PSFT_PHILLY and to the appliance ("zdlra2" is the alias for the RA_LONDON appliance). When PSFT_PHILLY is the primary database, configure its log archive destinations to send redo only to the appliance (zdlra2)."

- For Oracle Database 12c protected databases, configure RedoRoutes to ensure that PSFT_PHILLY never sends redo to the RA_LONDON appliance:
  - Navigate to the Availability -> Data Guard page for the PSFT_LONDON cluster database target.
  - Select the PSFT_PHILLY standby cluster database, click **Edit** to edit the standby database properties, and click the **Common Properties** tab on the Edit Primary Database Properties page.
  - Enter the RedoRoutes string as follows, and click **Apply**:

```
(psft_philly: psft_london)
```

The context of the string is the database being edited, i.e., PSFT_PHILLY. This string is interpreted as "When PSFT_PHILLY is the primary database, configure its log archive destinations to send redo to PSFT_LONDON. If PSFT_PHILLY is not the primary database, then do not configure any log archive destinations for it."

Add the RA_PHILLY Recovery Appliance to the Configuration

This step of the procedure produces the final configuration, shown in Figure 10.

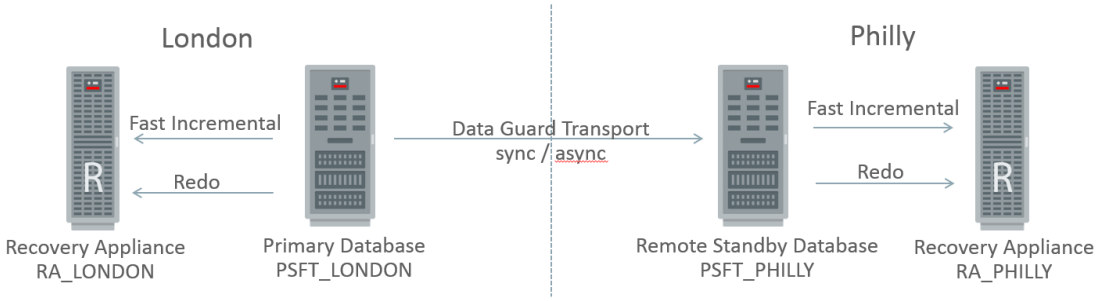

Figure 10. Final Configuration with Recovery Appliances and the Standby Database Integrated into the Environment

- Create a protection policy on the Recovery Appliance RA_PHILLY (if required):
  - Navigate to the Recovery Appliance -> Protection Policies page, and click **Create**.

The values for the protection policy on the RA_PHILLY appliance can be different from those on the RA_LONDON appliance.

- Create the Recovery Appliance user in the RA_PHILLY database (if required):
  - Navigate to the Schema -> Users page for the RA_PHILLY cluster database target.

The Recovery Appliance user must have the "create session" system privilege only. No other system privilege or role should be granted to the user.

- Add the PSFT_PHILLY database to the desired protection policy on the RA_PHILLY appliance:

If you select the PSFT_PHILLY database in this step, then before you perform the step to register the database, you must perform a Data Guard switchover to make PSFT_PHILLY the primary cluster database. If you cannot perform the switchover to PSFT_PHILLY,the PSFT_PHILLY database will still be backed up to the RA_PHILLY appliance, but the RA_PHILLY appliance Protected Databases page will display PSFT_LONDON.

The procedure assumes a switchover is not performed at this time. Therefore, PSFT_LONDON is the primary cluster database.

- Navigate to the Recovery Appliance -> Protected Databases page, and click **Add** to add the PSFT_LONDON database.
- Click **Add**, and select the PSFT_LONDON database that was previously discovered in Enterprise Manager.
- Select the desired protection policy.
- Specify the amount of space to be reserved for the PSFT_LONDON database.
- Add the new Recovery Appliance user or select an existing named credential, and click **OK**.

» Register the PSFT_LONDON database with the RA_PHILLY appliance:

- Navigate to the Availability -> Backup & Recovery -> Backup Settings page for the PSFT_LONDON cluster database target.
- (The Recovery Appliance setting will display the RA_LONDON appliance.) Click **Clear Configuration**.
- Select the Philly Recovery Appliance and the virtual private catalog user from the drop-down lists, and click **Apply**.

» Configure the PSFT_PHILLY database to backup to the RA_PHILLY appliance:

- Navigate to the Availability -> Backup & Recovery -> Backup Settings page for the PSFT_PHILLY cluster database target.
- (The Recovery Appliance setting will display the RA_PHILLY appliance.) Click **Clear Configuration**.
- Select **Configure this physical standby database to send backups to the specified Recovery Appliance**. The Recovery Appliance shown in the greyed out box will be RA Philly, click **Apply**.

» Re-configure the PSFT_LONDON database to backup to the RA_LONDON appliance:

- Navigate to the Availability -> Backup & Recovery -> Backup Settings page for the PSFT_LONDON cluster database target.
- (The Recovery Appliance setting will display the RA_PHILLY appliance.) Click the **Clear Configuration**.
- Select the London Recovery Appliance and the virtual private catalog user from the drop-down lists, and click **Apply**.

» Enable real-time redo transport from the PSFT_PHILLY database to the RA_PHILLY appliance:

The steps immediately below are applicable only for Oracle Database 12c protected databases. The step requires an outage because the database must be restarted. The restart is required to allow the Oracle instances to access the newly created wallet that will be used by the log transport mechanism to send real-time redo to the Recovery Appliance.

If an outage is not possible now, you can perform this step manually and in a rolling fashion, by restarting one instance at a time. For instructions on how to do this, see Appendix 4.

For Oracle Database 11gR2 protected databases, follow the instructions in Appendix 4.

Additionally, the Data Guard page will report the Data Guard status as being in ERROR, and that the newly added RA_PHILLY is not receiving redo data. This ERROR will be resolved when the RedoRoutes are configured in the next step.

- Navigate to the Availability -> Data Guard page for the PSFT_PHILLY cluster database target.

- Click **Add Recovery Appliance**, and select the RA_PHILLY appliance and the appropriate virtual private catalog user from the drop-down list.
- Select the named credentials for the PSFT_PHILLY and PSFT_LONDON databases, and click **Submit**.

- For Oracle Database 12c protected database, configure RedoRoutes to ensure that PSFT_PHILLY always sends redo to the RA_PHILLY appliance:
  - Navigate to the Availability -> Data Guard page for the PSFT_PHILLY cluster database target.
  - Click **Edit** to edit the primary cluster database properties, and click the **Common Properties** tab on the Edit Primary Database Properties page.
  - Enter the RedoRoutes string as follows, and click **Apply**:

```
(psft_philly : psft_london, zdlra6 ASYNC)(psft_london : zdlra6 ASYNC)
```

The context of the string is the database being edited, i.e., PSFT_PHILLY. The string is interpreted as "When PSFT_PHILLY is the primary database, configure its log archive destinations to send redo to both PSFT_LONDON and to the appliance ("zdlra6" is the alias for the RA_PHILLY appliance). When PSFT_LONDON is the primary database, configure the log archive destinations of the PSFT_PHILLY database to send redo only to the appliance (zdlra6)."

- For Oracle Database 12c protected databases, configure the RMAN channel for the PSFT_LONDON database to connect to the RA_LONDON appliance:
  - If you used the Data Guard Add Recovery Appliance wizard, then the RMAN channel definition for the PSFT_LONDON database points to the RA_PHILLY Recovery Appliance. Change only the credential_alias ENV variable in the CONFIGURE CHANNEL DEVICE TYPE SBT clause to point the alias to the RA_LONDON appliance instead, e.g..
    - CONFIGURE CHANNEL DEVICE TYPE 'SBT_TAPE' FORMAT '%d_%U' PARMS "SBT_LIBRARY=/u01/app/oracle/product/12.1.0.2/dbhome_3/lib/libra.so, ENV=(RA_WALLET='location=file:/u01/app/oracle/product/12.1.0.2/dbhome_3/dbs/zdlra credential_alias=**scaz10ingest-scan1:1521/zdlra6:dedicated**')";
  - Must change to:
    - CONFIGURE CHANNEL DEVICE TYPE 'SBT_TAPE' FORMAT '%d_%U' PARMS "SBT_LIBRARY=/u01/app/oracle/product/12.1.0.2/dbhome_3/lib/libra.so, ENV=(RA_WALLET='location=file:/u01/app/oracle/product/12.1.0.2/dbhome_3/dbs/zdlra credential_alias=**scas10ingest-scan5:1521/zdlra2:dedicated**')";
- Configure the RMAN archive log deletion policy for the PSFT_LONDON and PSFT_PHILLY databases.
  - To allow the Flash Recovery Area to be purged automatically, after the archive logs have been sent to the Recovery Appliance and applied on the physical standby database:
    - CONFIGURE ARCHIVELOG DELETION POLICY TO APPLIED ON ALL STANDBY BACKED UP 1 TIMES TO 'SBT_TAPE';
- Configure RMAN db_unique_name connection strings.
  - To allow RMAN to log in to the primary database in order to resync the catalog, the following changes are required on the PSFT_LONDON database:
    - CONFIGURE DB_UNIQUE_NAME 'psft_london' CONNECT IDENTIFIER 'scam06client-scan1/psft_london';
    - CONFIGURE DB_UNIQUE_NAME 'psft_philly' CONNECT IDENTIFIER 'scam06client-scan5/psft_philly';
  - To replicate these settings in the PSFT_PHILLY database, use RMAN to connect to the PSFT_LONDON target database and the RA_PHILLY catalog:
    - $ rman target / catalog /@scaz10ingest-scan1:1521/zdlra6:dedicated
    - RMAN> resync catalog;

- RMAN> show db_unique_name;

Data Guard Role Transition

The procedures in the previous sections for the two scenarios are designed to have database backups run at each location (London and Philly) to the local Recovery Appliance (RA_LONDON and RA_PHILLY, respectively). Because of this, when a role transition occurs, no changes to the running RMAN backup jobs are required.

When a switchover occurs, new backups will continue to run, but any backup in progress at the time of the switchover might need to be restarted.

When a failover occurs, backups will continue to run against the new primary database. The original primary database will need to be reinstated, but with Flashback Database enabled, there should be no need to restore the database from the local Recovery Appliance if the outage is temporary. For a larger outage, the database can be restored from the local Recovery Appliance by using the standard procedures.

Conclusion

The two procedures documented in this best practice paper cover the integration of Recovery Appliances for local backup and recovery of both a primary and a standby database in a Data Guard configuration (physical standby). Each database can use either Recovery Appliance (local or remote) for recovery should one of the appliances be unavailable for any reason. Data Guard redo transport between the primary and the standby databases eliminates the need to replicate backups between the Recovery Appliances.

References

Zero Data Loss Recovery Appliance overview

MAA Best Practices - Zero Data Loss Recovery Appliance

Oracle Database Online Documentation 12c Release 1 (12.1)

Oracle Support Document 1683791.2 - Information Center: Overview Zero Data Loss Recovery Appliance

Appendix 1

This appendix details the steps required to manually configure and enable real-time redo transport by restarting each instance of the primary database one node at a time.

The following procedure reconfigures two init.ora parameters and configures a new log archive destination.

- Reconfigure the redo_transport_user parameter on the primary and standby databases used to send redo between the databases and to add the RA_LONDON appliance:
  - On both SIEBEL_LONDON and SIEBEL_PHILLY, the redo_transport_user parameter specifies the virtual private catalog (VPC) user that the protected database will use.
    - ALTER SYSTEM SET redo_transport_user='VPCSIEBEL' SCOPE=SPFILE;
- Restart each instance on both SIEBEL_LONDON and SIEBEL_PHILLY, one at a time, to use the new redo transport user.
- Add the RA_LONDON appliance to the Oracle Data Guard Broker configuration:
  - For Oracle Database 12c, log in to the Data Guard Broker CLI using the SYS password, and add, and then enable the Recovery Appliance “zdlra2” in the broker configuration:

For versions earlier than Oracle Database 12.1.0.2 Bundle Patch 6, use “backup_appliance” instead of “recovery_appliance” in the code that follows.

    - DGMGRL> add recovery_appliance zdlra2 as connect identifier is 'scas10ingest-scan5:1521/zdlra2:dedicated';
    - DGMGRL> enable recovery_appliance zdlra2;
  - For Oracle Database 11g, log in to SQL*Plus using the SYS password, and set an available log archive destination:
    - SQL> alter system set log_archive_config='dg_config=(zdlrabel,hiatt_belmont,hiatt_nashua)' scope=BOTH sid='*';
    - SQL>alter system set log_archive_dest_20='service="scas10ingest-scan5:1521/zdlra2:dedicated"','ASYNC NOAFFIRM delay=0 optional compression=disable max_failure=0 max_connections=1 reopen=300 db_unique_name="zdlra2" net_timeout=30', 'valid_for=(all_logfiles,all_roles)'

Appendix 2

This appendix details the steps required to manually configure and enable real-time redo transport for the physical standby database by restarting each instance of the physical standby database one node at a time.

This procedure differs from the procedure in Appendix 1 where the redo_transport_user parameter is also set. The procedure here assumes that step has already been completed.

- Restart each instance on both SIEBEL_LONDON and SIEBEL_PHILLY, one at a time, to use the new redo transport user.
- Add the RA_PHILLY appliance to the Oracle Data Guard Broker configuration:
  - For Oracle Database 12c, log in to the Data Guard Broker CLI using the SYS password, and add, and then enable the Recovery Appliance “zdlra6” in the broker configuration:

For versions earlier than Oracle Database 12.1.0.2 Bundle Patch 6, use "backup_appliance" instead of "recovery_appliance" in the code that follows.

- DGMGRL> add recovery_appliance zdlra6 as connect identifier is 'scaz10ingest-scan1:1521/zdlra6:dedicated';
- DGMGRL> enable recovery_appliance zdlra6;

» For Oracle Database 11g, log in to SQL*Plus using the SYS password, and set an available log archive destination:

- SQL> alter system set log_archive_config='dg_config=(zdlransh,hiatt_nashua,hiatt_belmont)' scope=BOTH sid='*';
- SQL>alter system set log_archive_dest_20='service="scaz10ingest-scan1:1521/zdlra6:dedicated"','ASYNC NOAFFIRM delay=0 optional compression=disable max_failure=0 max_connections=1 reopen=300 db_unique_name="zdlra6" net_timeout=30', 'valid_for=(all_logfiles,all_roles)'

Appendix 3

This appendix details the steps required to manually configure and enable real-time redo transport by restarting each instance of the primary database one node at a time.

The procedure reconfigures two init.ora parameters and configures a new log archive destination.

» Reconfigure the redo_transport_user parameter on the primary databases used to send redo to the RA_LONDON appliance:

» On PSFT_LONDON, the redo_transport_user parameter specifies the virtual private catalog (VPC) user that the protected database will use.

- ALTER SYSTEM SET redo_transport_user='VPCPSFT' SCOPE=SPFILE;

» Restart each instance on PSFT_LONDON, one at a time, to use the new redo transport user.

» Log in to SQL*Plus using the SYS password, and set an available log archive destination as follows:

- SQL> alter system set log_archive_config='dg_config=(zdlra2,psft_london)';
- SQL>alter system set log_archive_dest_20='service="scas10ingest-scan5:1521/zdlra2:dedicated"', 'valid_for=(all_logfiles,all_roles) ASYNC DB_UNIQUE_NAME=zdlra2';

Appendix 4

This appendix details the steps required to manually configure and enable real-time redo transport for the physical standby database by restarting each instance of the physical standby database one node at a time.

This procedure differs from the procedure in Appendix 3 where the redo_transport_user parameter is also set. The procedure here assumes that step has already been completed.

» Restart each instance on both PSFT_LONDON and PSFT_PHILLY, one at a time, to use the new redo transport user.

» Add the RA_LONDON appliance to the Oracle Data Guard Broker configuration:

» For Oracle Database 12c, log in to the Data Guard Broker CLI using the SYS password, and add, and then enable the Recovery Appliance "zdlra2" in the broker configuration:

For versions earlier than Oracle Database 12.1.0.2 Bundle Patch 6, use "backup_appliance" instead of "recovery_appliance" in the code that follows.

  - DGMGRL> add recovery_appliance zdlra6 as connect identifier is 'scaz10ingest-scan1:1521/zdlra6:dedicated';
  - DGMGRL> enable recovery_appliance zdlra6;
- For Oracle Database 11g, log in to SQL*Plus using the SYS password, and set an available log archive destination as follows:
  - SQL> alter system set log_archive_config='dg_config=(zdlra2,psft_london,psft_philly,zdlra6)';
- For Oracle Database 11g, log in to SQL*Plus using the SYS password on the PSFT_LONDON database, and re-establish the log archive destination set in Appendix 3 but cancelled when the RA_PHILLY was added to the configuration:
  - SQL>alter system set log_archive_dest_20='service="scas10ingest-scan5:1521/zdlra2:dedicated"', 'valid_for=(all_logfiles,all_roles) ASYNC DB_UNIQUE_NAME=zdlra2';
  - SQL> alter system set log_archive_dest_state_20=enable;
- For Oracle Database 11g, log in to SQL*Plus using the SYS password on the PSFT_PHILLY database, and set the log archive destination:
  - SQL>alter system set log_archive_dest_20='service="scaz10ingest-scan1:1521/zdlra6:dedicated"', 'valid_for=(all_logfiles,all_roles)ASYNC DB_UNIQUE_NAME=zdlra6';
  - SQL> alter system set log_archive_dest_state_20=enable;

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US


blogs.oracle.com/oracle


facebook.com/oracle


twitter.com/oracle


oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2015, Oracle and/or its affiliates. All rights reserved. This document is provided *for* information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0615

Deploying the Zero Data Loss Recovery Appliance in a Data Guard Configuration
March 2018
Author: Andrew Babb


Oracle is committed to developing practices and products that help protect the environment