

Oracle Maximum
Availability Architecture

Oracle Data Guard構成におけるZero Data Loss Recovery Applianceの導入

Oracleホワイト・ペーパー | 2015年11月



目次

| | |
|--|----|
| はじめに | 1 |
| 概要 | 2 |
| 前提条件 | 2 |
| 既存のData Guard環境へのRecovery Applianceの導入 | 3 |
| RA_LONDON Recovery Applianceの構成への追加 | 4 |
| RA_PHILLY Recovery Applianceの構成への追加 | 7 |
| 新しいData Guard構成の作成およびRecovery Applianceの導入 | 10 |
| RA_LONDON Recovery Applianceの構成への追加 | 11 |
| PSFT_PHILLYリモート・スタンバイ・データベースの構成への追加 | 13 |
| RA_PHILLY Recovery Applianceの構成への追加 | 15 |
| Data Guardのロール移行 | 18 |
| 結論 | 18 |
| 参考資料 | 18 |
| 付録1: | 19 |
| 付録2: | 19 |
| 付録3: | 20 |
| 付録4: | 20 |

はじめに

Zero Data Loss Recovery Applianceは、バックアップおよびリカバリ用に最適化されたオラクルのソリューションです。基本的に、常時の増分バックアップおよび任意のポイント・イン・タイム・リストアを可能にすることでバックアップとリカバリの実行方法を変更します。データ保護、運用リソース効率、システム・リソース効率、スケーラビリティ、そしてリカバリの成功を確実にする独自水準のバックアップ検証の点において、Recovery Applianceに匹敵するバックアップ・ソリューションおよびリカバリ・ソリューションはありません。

Data Guardは、Oracle Database向けのリアルタイム・データ保護およびデータ可用性のソリューションです。ディザスタ・リカバリおよび可用性のため、リモートの場所に、Oracle Databaseの同期化された最新コピーを維持するオラクルのソリューションです。Data Guardは、停止が発生した場合に、フル・レベルのサービスをただちに再開できるよう、すでに実行されている本番データベースの同期化されたコピーを提供する機能により、Recovery Applianceと差別化しています。

ベスト・プラクティスをまとめたこのホワイト・ペーパーは、Data Guard構成もホストする複数の場所にRecovery Applianceの導入を考えている技術担当者を対象としています。

- » Data Guardは、データベースまたはサイトがオフラインになってしまった場合に、セカンダリの場所にある同期化されたコピーにただちにフェイルオーバーできるようにすることで高可用性（HA）とディザスタ・リカバリを提供するために使用します。
- » Recovery Applianceは、データベースがホストされている各場所（Data Guardのプライマリ・データベースまたはスタンバイ・データベースを含む）にローカルのバックアップとリカバリを提供するために導入します。
- » Data Guardフィジカル・スタンバイ・データベースは本番データベースの正確なコピーであるため、ローカルのアプライアンスが使用できなくなった場合でも、いずれかの場所のRecovery Applianceで作成されたリアルタイム・バックアップを使用し、いずれかの場所でプライマリ・データベースまたはスタンバイ・データベースをリストアすることができます。

このホワイト・ペーパーに示される推奨事項を実施することで、ネットワーク帯域幅の効率的な使用、最適な水準のHAおよびデータ保護を達成できます。以下のセクションに示すすべての手順は、Data GuardまたはActive Data Guardのどちらのフィジカル・スタンバイ・データベースにも適用されます。

概要

このホワイト・ペーパーでは、ロンドンにData Guardプライマリ・データベースがあり、ロンドンのRecovery Applianceにバックアップするシナリオと、リモート・スタンバイ・データベースがフィラデルフィアにあり、同じフィラデルフィアのRecovery Applianceにバックアップするシナリオという、最終目的が同じ構成となる2つのシナリオを取り上げています。図1を参照してください。

各シナリオはスタートの構成が異なります。

- » 1つめのシナリオは、プライマリとスタンバイの両方のデータベースを含むData Guard構成があり、各サイトにRecovery Applianceを追加します。
- » 2つめのシナリオは、ロンドンに本番データベースとRecovery Applianceがあり、フィラデルフィアにData Guardスタンバイ・データベースとRecovery Applianceを追加します。

このホワイト・ペーパーの最後のセクションでは、完全に統合されたData GuardとRecovery Applianceの環境において、Data Guardのロールが移行した後何が起きるかについて説明しています。

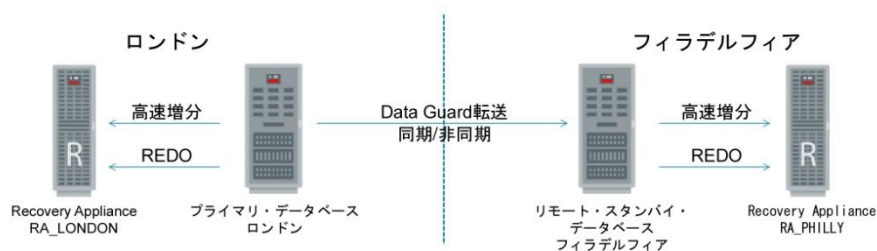


図1：両方の統合シナリオにおける最終的な構成

このホワイト・ペーパーのData Guardスタンバイ・データベースは、Recovery Managerのブロック・チェーン・トラッキング・ファイルを使用して高速な増分バックアップを実行し、リアルタイム・カスケードを使用してローカルのRecovery ApplianceにリアルタイムでREDOを転送します。バックアップ・ターゲットおよび転送先がRecovery Applianceである場合、これらの機能を使用するためにOracle Active Data Guardライセンスは必要ありません。スタンバイ・データベースがData GuardまたはActive Data Guardのどちらであっても同じ手順が適用されます。

前提条件

このホワイト・ペーパーに示す手順は、以下の前提で、Oracle Database 11g Release 2 (11.2.0.4) および Oracle Database 12c (12.1.0.2) について検証済みです。

- » Recovery Appliance (RA_LONDONおよびRA_PHILLY) がすでに導入され、Enterprise Manager Cloud Controlでターゲットとして検出されている。
- » データベース・ターゲットも検出されている。
- » 1つめのシナリオについて、リモート・スタンバイ・データベースが検出されていて、Data Guard Brokerが構成され、実行されている。

既存のData Guard環境へのRecovery Applianceの導入

1つめのシナリオは、プライマリ・データベース（SIEBEL_LONDON）およびスタンバイ・データベース（SIEBEL_PHILLY）から始まります（図2参照）。



図2：Data Guard環境の初期構成

この手順では2つのRecovery Appliance（RA_LONDONおよびRA_PHILLY）をそれぞれの場所に追加します（図3参照）。Data Guard構成内の各データベースは、ローカルのRecovery Applianceに対して、高速増分バックアップを実行したり、リアルタイムでREDOを転送したりできます。いずれのデータベースも、ローカルのRecovery Applianceが使用できない場合、リモートのRecovery Applianceをリカバリに使用できます。プライマリとスタンバイの間のData Guard REDO転送により、Recovery Appliance間でのバックアップのレプリケートが不要となります。

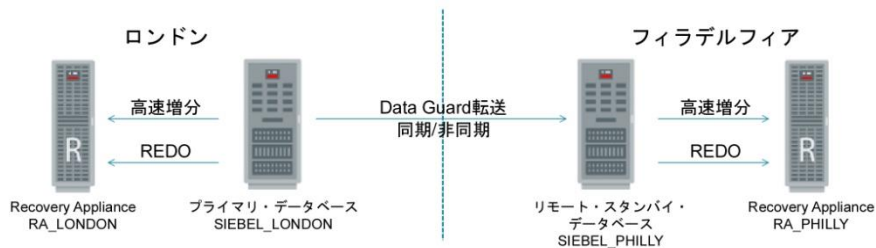


図3：Data Guard環境に統合されたRecovery Applianceを含む最終構成

この手順は、最初のRecovery Applianceをロンドンで追加し、次のRecovery Applianceをフィラデルフィアで追加する、2つの手順からなっています。

RA_LONDON Recovery Applianceの構成への追加

この手順を実行すると、図4に示すような構成となります。

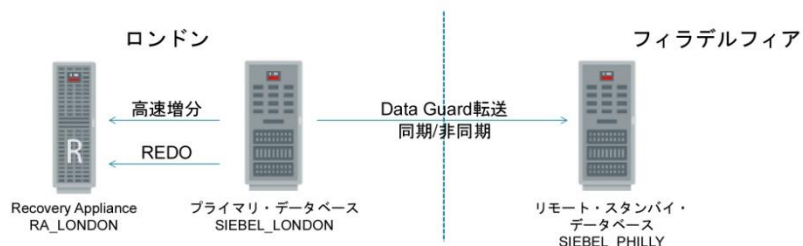


図4：Data Guard環境に追加されたRA_LONDON Recovery Appliance

- » 以下の前提条件を満たしていることを確認します。
 - » プライマリ・データベースおよびスタンバイ・データベースの両方がEnterprise Manager Cloud Controlで正しく検出されている。
 - » 両方のデータベースにおいて、1時間のフラッシュバック保存ターゲットの設定で、フラッシュバック・データベースが有効になっている。
 - » RA_LONDON Recovery ApplianceがEnterprise Managerで検出されている。
- » RA_LONDON Recovery Applianceにおける保護ポリシーを作成します（必要な場合）。
 - » Enterprise Manager Cloud Controlにログインし、Targets→Recovery Appliancesにナビゲートし、「RA_LONDON Recovery Appliance」を選択します。
 - » Recovery Appliance→Protection Policiesページにナビゲートし、「Create」をクリックします。
- » RA_LONDONデータベースでRecovery Applianceユーザーを作成します（必要な場合）。
 - » RA_LONDONクラスター・データベース・ターゲットについて、Schema→Usersページにナビゲートします。

Recovery Applianceユーザー・アカウントには"create session"システム権限のみを与えてください。このアカウントには、それ以外のシステム権限またはロールを許可しないでください。

- » RA_LONDONについての希望の保護ポリシーにSIEBEL_LONDONデータベースを追加します。
 - » Recovery Appliance→Protected Databasesページにナビゲートし、「Add」をクリックしてSIEBEL_LONDONデータベースを追加します。
 - » 「Add」をクリックし、Enterprise Managerで先に検出されているSIEBEL_LONDONデータベースを選択します。
 - » 希望の保護ポリシーを選択します。
 - » SIEBEL_LONDONデータベース用に予約する領域のサイズを指定します。
 - » 新しいRecovery Applianceユーザーを追加する、または既存の名前付き資格証明を選択し、「OK」をクリックします。
- » SIEBEL_LONDONデータベースをRA_LONDONアプライアンスに登録します。
 - » SIEBEL_LONDONクラスター・データベース・ターゲットについて、Availability→Backup & Recovery→Backup Settingsページにナビゲートします。
 - » Recovery Applianceを選択し、ドロップダウン・リストから仮想プライベート・カタログ・ユーザーを選択して、「Apply」をクリックします。

- » SIEBEL_PHILLYデータベースをRA_LONDONアプライアンスに登録し、RA_LONDONからSIEBEL_PHILLYにデータベースを直接リストアできるようにします。
- » SIEBEL_PHILLYクラスタ・データベース・ターゲットについて、Availability→Backup & Recovery→Backup Settingsページにナビゲートします。
- » 「Configure this physical standby database to send backups to the specified Recovery Appliance」を選択し、「Apply」をクリックします。
- » SIEBEL_LONDONデータベースおよびSIEBEL_PHILLYデータベースについて、構成の設定を変更します。
- » Recovery Applianceを使用する場合、以下の変更がベスト・プラクティスと考えられます。これらの変更は、Enterprise Managerから、またはRecovery Manager CLIを使用して設定できます。
 - CONFIGURE BACKUP OPTIMIZATION ON;
 - CONFIGURE CONTROLFILE AUTOBACKUP ON;
 - CONFIGURE DEFAULT DEVICE TYPE TO 'SBT_TAPE';
 - CONFIGURE DEVICE TYPE 'SBT_TAPE' PARALLELISM 8;
 - ブロック・チェンジ・トラッキング・ファイル機能を有効にします。
 - フラッシュバック・データベース機能を有効にします。フェイルオーバー後のスタンバイ・データベースの再作成を避けるため、最小限の60分間の保存に設定します。
- » SIEBEL_LONDONデータベースをRA_LONDONアプライアンスにバックアップします。
- » 次のRecovery Managerスクリプトは、Recovery Applianceに最初のバックアップを作成するときのベスト・プラクティスと考えられます。
 - RMAN> backup cumulative incremental level 0 filesperset 1 section size 64g database plus archivelog filesperset 32;
- » Recovery Managerタグを必要に応じて追加できます。
- » SIEBEL_LONDONデータベース上に仮想プライベート・カタログ・ユーザーを作成します。
- » SIEBEL_LONDONクラスタ・データベース・ターゲットについて、Schema→Usersページにナビゲートします。

仮想プライベート・カタログ・ユーザーは、プライマリ・データベースとフィジカル・スタンバイ・データベースとの間でData Guard REDO転送が継続して動作するようにするため、保護されたデータベース内で作成しなければなりません。

仮想プライベート・カタログ・ユーザーには、"create session"および"sysoper"のシステム権限が必要です。Oracle Database 12c保護データベースの場合、必要に応じて、仮想プライベート・カタログ・ユーザーに"sysdg"システム権限を付与できます。このユーザーには、それ以外のシステム権限またはロールを許可しないでください。

-
- » 次に進む前にログを強制的に切り替えて、すべてのスタンバイ・データベースにREDOが適用されるようにします。
 - » すべてのData Guard環境のパスワード・ファイルをコピーします。

前の手順において、仮想プライベート・カタログ・ユーザーを追加することによって現在のパスワード・ファイルが修正されます。この手順は、すべてのスタンバイ・データベースにパスワード・ファイルの修正をレプリケートするために必要です。

-
- » O/SツールとともにASMCMDユーティリティを使用し、パスワード・ファイルをSIEBEL_LONDONデータベースからSIEBEL_PHILLYデータベースにコピーします。

» SIEBEL_LONDONデータベースからRA_LONDONアプライアンスへのリアルタイムREDO転送を有効にします。

すぐ下の手順は、Oracle Database 12c保護データベースについてのみ適用可能です。この手順は、データベースを再起動しなければならないため、データベースの停止が必要です。再起動は、ログ転送メカニズムがRecovery ApplianceへのリアルタイムREDO送信に使用する、新たに作成されたウォレットにOracleインスタンスがアクセスするのに必要です。データベースの停止が不可能な場合は、この手順を手動により、一度に1個のインスタンスを再起動するローリング方式で実行できます。詳しい手順については、「付録1」を参照してください。

Oracle Database 11g Release 2保護データベースの場合は、「付録1」の手順に従ってください。

- » SIEBEL_LONDONクラスタ・データベース・ターゲットについて、Availability→Data Guard Administrationページにナビゲートします。
- » 「Add Recovery Appliance」をクリックし、RA_LONDONアプライアンスを選択し、ドロップダウン・リストから該当の仮想プライベート・カタログ (VPC) ユーザーを選択します。
- » SIEBEL_LONDONデータベースおよびSIEBEL_PHILLYデータベースについて、名前付き資格証明を選択し、「Submit」をクリックします。

この時点では、プライマリ・データベースは、リアルタイムREDO転送を使用してRA_LONDONアプライアンスにREDOを送信しています。

- » Oracle Database 12c保護データベースの場合、RedoRoutesを設定し、SIEBEL_LONDONがREDOを常にRA_LONDONアプライアンスに送信するようにします。
- » SIEBEL_LONDONクラスタ・データベース・ターゲットについて、Availability→Data Guardページにナビゲートします。
- » 「Edit」をクリックしてプライマリ・クラスタ・データベースのプロパティを編集し、Edit Primary Database Propertiesページの「Common Properties」タブをクリックします。
- » 次のRedoRoutes文字列を入力し、「Apply」をクリックします。

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

文字列のコンテキストは編集対象のデータベース、すなわちSIEBEL_LONDONです。この文字列は次のように解釈されます。"SIEBEL_LONDONがプライマリ・データベースのとき、SIEBEL_PHILLYとそのアプライアンスの両方にREDOを送信するよう、ログ・アーカイブ宛先を設定する ("zdlra2"はRA_LONDONアプライアンスのエイリアス)。SIEBEL_PHILLYがプライマリ・データベースのとき、SIEBEL_LONDONのアプライアンス (zdlra2) にのみREDOを送信するよう、SIEBEL_LONDONのログ・アーカイブ宛先を設定する"

- » Oracle Database 12c保護データベースの場合、RedoRoutesを設定し、SIEBEL_PHILLYがREDOをRA_LONDONアプライアンスに送信しないようにします。
- » SIEBEL_LONDONクラスタ・データベース・ターゲットについて、Availability→Data Guardページにナビゲートします。
- » SIEBEL_PHILLYスタンバイ・クラスタ・データベースを選択し、「Edit」をクリックしてスタンバイ・データベースのプロパティを編集し、Edit Primary Database Propertiesページの「Common Properties」タブをクリックします。
- » 次のRedoRoutes文字列を入力し、「Apply」をクリックします。

```
(siebel_philly: siebel_london)
```


この文字列のコンテキストは編集対象のデータベース、すなわちSIEBEL_PHILLYです。この文字列は次のように解釈されます。"SIEBEL_PHILLYがプライマリ・データベースのとき、SIEBEL_LONDONにREDOを送信するよう、ログ・アーカイブ宛先を設定する。SIEBEL_PHILLYがプライマリ・データベースでない場合は、SIEBEL_PHILLYのログ・アーカイブ宛先を設定しない"

RA_PHILLY Recovery Applianceの構成への追加

この手順を実行すると、最終構成は図5のようになります。

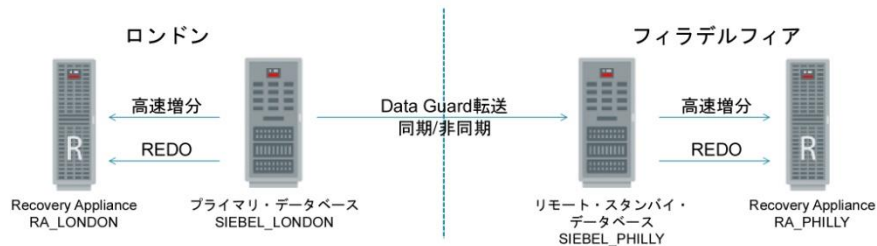


図5：Data Guard環境に統合されたRecovery Applianceを含む最終構成

- » RA_PHILLY Recovery Applianceにおける保護ポリシーを作成します（必要な場合）。
 - » Recovery Appliance→Protection Policiesページにナビゲートし、「Create」をクリックします。

RA_PHILLYアプライアンスに対する保護ポリシーの値は、RA_LONDONアプライアンスに対する保護ポリシーの値と同じものにしなくてもかまいません。

- » RA_PHILLYデータベースでRecovery Applianceユーザーを作成します（必要な場合）。
 - » RA_PHILLYクラスタ・データベース・ターゲットについて、Schema→Usersページにナビゲートします。

Recovery Applianceユーザー・アカウントには"create session"システム権限のみを与えてください。このユーザーには、それ以外のシステム権限またはロールを許可しないでください。

- » RA_PHILLYについての希望の保護ポリシーにSIEBEL_LONDONデータベースを追加します。

この手順でSIEBEL_PHILLYデータベースを選択する場合は、データベースを登録する手順を実行する前に、Data Guardスイッチオーバーを実行してSIEBEL_PHILLYをプライマリ・クラスタ・データベースにしなければなりません。SIEBEL_PHILLYへのスイッチオーバーを実行できない場合、SIEBEL_PHILLYデータベースは引き続きRA_PHILLYアプライアンスにバックアップされますが、RA_PHILLYアプライアンスのProtected DatabasesページにはSIEBEL_LONDONが表示されます。

この手順は、この時点でスイッチオーバーは実行されていないと仮定しています。そのため、SIEBEL_LONDONがプライマリ・クラスタ・データベースです。

- » Recovery Appliance→Protected Databasesページにナビゲートし、「Add」をクリックしてSIEBEL_LONDONデータベースを追加します。
- » 「Add」をクリックし、Enterprise Managerで先に検出されていたSIEBEL_LONDONデータベースを選択します。
- » 希望の保護ポリシーを選択します。
- » SIEBEL_LONDONデータベース用に予約する領域のサイズを指定します。
- » 新しいRecovery Applianceユーザーを追加する、または既存の名前付き資格証明を選択し、「OK」をクリックします。
- » SIEBEL_LONDONデータベースをRA_PHILLYアプライアンスに登録します。

- » SIEBEL_LONDONクラスタ・データベース・ターゲットについて、Availability→Backup & Recovery→Backup Settingsページにナビゲートします。
- » (Recovery Applianceの設定にはRA_LONDONアプライアンスが表示されます。) 「Clear Configuration」をクリックします。
- » フィラデルフィアのRecovery Applianceを選択し、ドロップダウン・リストから仮想プライベート・カタログ・ユーザーを選択して、「Apply」をクリックします。
- » SIEBEL_PHILLYデータベースをRA_PHILLYアプライアンスに再登録します。
 - » SIEBEL_PHILLYクラスタ・データベース・ターゲットについて、Availability→Backup & Recovery→Backup Settingsページにナビゲートします。
 - » (Recovery Applianceの設定にはRA_LONDONアプライアンスが表示されます。) 「Clear Configuration」をクリックします。
 - » 「Configure this physical standby database to send backups to the specified Recovery Appliance」を選択します。灰色のボックスにフィラデルフィアのRecovery Applianceが表示されます。
 - » 「Apply」をクリックします。
- » SIEBEL_LONDONデータベースをRA_LONDONアプライアンスに再登録します。
 - » SIEBEL_LONDONクラスタ・データベース・ターゲットについて、Availability→Backup & Recovery→Backup Settingsページにナビゲートします。
 - » (Recovery Applianceの設定にはRA_PHILLYアプライアンスが表示されます。) 「Clear Configuration」をクリックします。
 - » ロンドンのRecovery Applianceを選択し、ドロップダウン・リストからSIEBEL_LONDONの仮想プライベート・カタログ・ユーザーを選択して、「Apply」をクリックします。
- » SIEBEL_PHILLYデータベースをRA_PHILLYアプライアンスにバックアップします。
 - » 次のRecovery Managerスクリプトは、Recovery Applianceに最初のバックアップを作成するときのベスト・プラクティスと考えられます。
 - RMAN> backup cumulative incremental level 0 filesperset 1 section size 32g database plus archivelog filesperset 32;
 - » Recovery Managerタグを必要に応じて追加できます。
- » SIEBEL_PHILLYデータベースからRA_PHILLYアプライアンスへのリアルタイムREDO転送を有効にします。

すぐ下の手順は、Oracle Database 12c保護データベースについてのみ適用可能です。この手順は、データベースを再起動しなければならないため、データベースの停止が必要です。再起動は、ログ転送メカニズムがRecovery ApplianceへのリアルタイムREDO送信に使用する、新たに作成されたウォレットにOracleインスタンスがアクセスするのに必要です。

データベースの停止が不可能な場合は、この手順を手動により、一度につき1個のインスタンスを再起動するローリング方式で実行できます。詳しい手順については、「付録2」を参照してください。

Oracle Database 11g Release 2保護データベースの場合は、「付録2」の手順に従ってください。

Data Guardページには、Data GuardのステータスがERRORであり、新たに追加されたRA_PHILLYがREDOデータを受信していないというレポートが表示されます。このERRORは、次の手順でRedoRoutesを設定すると解決します。

- » SIEBEL_PHILLYクラスタ・データベース・ターゲットについて、Availability→Data Guardページにナビゲートします。
- » 「Add Recovery Appliance」をクリックし、RA_PHILLYアプライアンスを選択し、ドロップダウン・リストから該当の仮想プライベート・カタログ (VPC) ユーザーを選択します。

- » SIEBEL_PHILLYデータベースおよびSIEBEL_LONDONデータベースについて、名前付き資格証明を選択し、「Submit」をクリックします。
- » Oracle Database 12c保護データベースの場合、RedoRoutesを設定し、SIEBEL_PHILLYがREDOを常にRA_PHILLYアプライアンスに送信するようにします。
 - » SIEBEL_PHILLYクラスタ・データベース・ターゲットについて、Availability→Data Guardページにナビゲートします。
 - » 「Edit」をクリックしてスタンバイ・クラスタ・データベースのプロパティを編集し、Edit Primary Database Propertiesページの「Common Properties」タブをクリックします。
 - » 次のRedoRoutes文字列を入力し、「Apply」をクリックします。

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

この文字列のコンテキストは編集対象のデータベース、すなわちSIEBEL_PHILLYです。この文字列は、"SIEBEL_PHILLYがプライマリ・データベースのとき、SIEBEL_LONDONとそのアプライアンスの両方にREDOを送信するようアーカイブ宛先を設定する ("zdlra6"はRA_PHILLYアプライアンスのエイリアス)。SIEBEL_LONDONがプライマリ・データベースのとき、SIEBEL_PHILLYのアプライアンス (zdlra6) にのみREDOを送信するよう、SIEBEL_PHILLYデータベースのログ・アーカイブ宛先を設定する"と解釈されます。

- » Oracle Database 12c保護データベースの場合、SIEBEL_LONDONデータベースがRA_LONDONアプライアンスに接続するよう、Recovery Managerチャンネルを設定します。
 - » Data Guard Add Recovery Applianceウィザードを使用した場合、SIEBEL_LONDONデータベースについてのRecovery Managerチャンネルの定義は、RA_PHILLY Recovery Applianceを参照しています。CONFIGURE CHANNEL DEVICE TYPE SBT句のcredential_alias ENV変数のみを変更し、代わりにRA_LONDONアプライアンスのエイリアスを参照するようにします。たとえば次のようになっています。
 - 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');
 - » これを次のように変更する必要があります。
 - 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');
- » SIEBEL_LONDONデータベースおよびSIEBEL_PHILLYデータベースについて、Recovery Managerのアーカイブ・ログ削除ポリシーを設定します。
 - » アーカイブ・ログがRecovery Applianceに送信され、フィジカル・スタンバイ・データベースに適用された後、フラッシュ・リカバリ領域が自動的に消去されるようにするには次のようにします。
 - CONFIGURE ARCHIVELOG DELETION POLICY TO APPLIED ON ALL STANDBY BACKED UP 1 TIMES TO 'SBT_TAPE';
- » Recovery Manager db_unique_nameコネクション文字列を設定します。
 - » カタログを再同期化するため、Recovery Managerでプライマリ・データベースにログインできるようにするには、SIEBEL_LONDONデータベースに以下の変更が必要です。
 - CONFIGURE DB_UNIQUE_NAME 'siebel12c_london' CONNECT IDENTIFIER 'scam06client-scan1/siebel12c_london';
 - CONFIGURE DB_UNIQUE_NAME 'siebel12c_philly' CONNECT IDENTIFIER 'scam06client-

```
scan5/siebel12c_philly';
```

- » SIEBEL_PHILLYデータベースのこれらの設定をレプリケートするには、Recovery Managerを使用して、SIEBEL_LONDONターゲット・データベースおよびRA_PHILLYカタログに接続します。
 - \$ rman target / catalog /@scsz10ingest-scan1:1521/zdlra6:dedicated
 - RMAN> resync catalog;
 - RMAN> show db_unique_name;

この時点で、各データセンターにRecovery Applianceの備わった、完全に構成されたData Guard環境となります。このシステムには次の利点があります。

- » 増分バックアップがローカルのRecovery Applianceに送信されるため、バックアップ・ウィンドウが大幅に削減されます。
- » REDOがローカルのRecovery Applianceに送信されるため、二重の障害が発生した場合でもデータ損失が最小限に抑えられます。
- » リストア操作において、いずれかのRecovery Applianceを利用できます。
- » Data Guardの使用によりフェイルオーバーできるため、リカバリ時間を最小限にできます。

新しいData Guard構成の作成およびRecovery Applianceの導入

この手順は、スタンドアロン・データベースPSFT_LONDONから始まります（図6参照）。前のシナリオと同じ結果になりますが、Recovery Applianceの導入に加え、スタンバイ・データベースを作成する点だけが異なります。

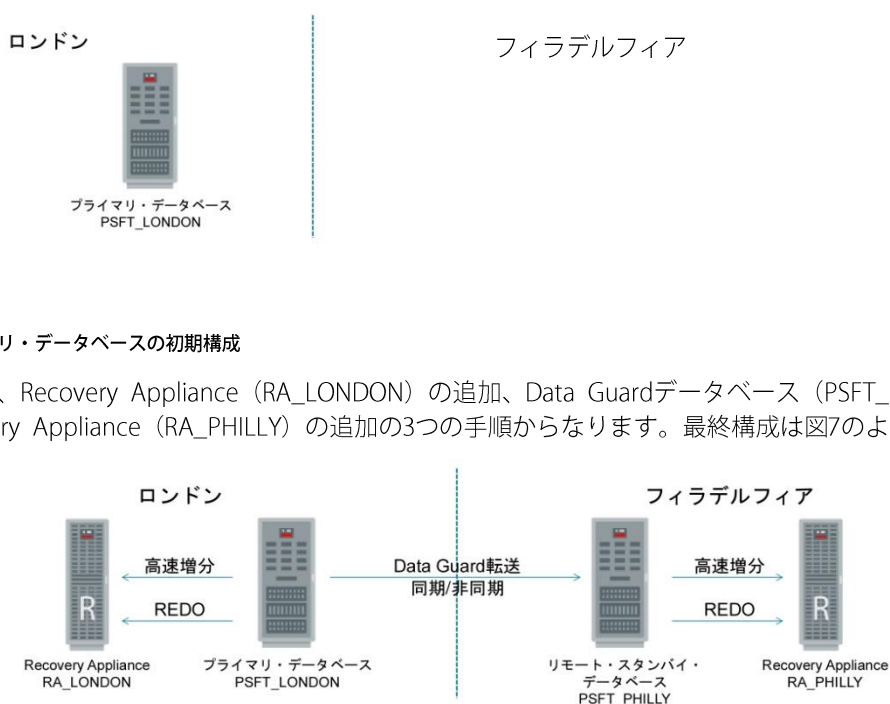


図6：プライマリ・データベースの初期構成

この手順は、Recovery Appliance (RA_LONDON) の追加、Data Guardデータベース (PSFT_PHILLY) の追加、Recovery Appliance (RA_PHILLY) の追加の3つの手順からなります。最終構成は図7のようになります。

図7： Recovery Applianceとリモート・スタンバイ・データベースが完全に統合された最終構成

RA_LONDON Recovery Applianceの構成への追加

この手順を実行すると、図8に示すような構成となります。

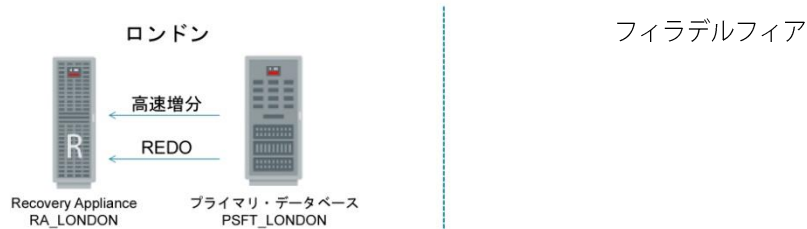


図8： プライマリ・データベースに追加されたRA_LONDON Recovery Appliance

- » 以下の前提条件を満たしていることを確認します。
 - » プライマリ・データベースがEnterprise Manager Cloud Controlで検出されている。
 - » RA_LONDON Recovery ApplianceがEnterprise Managerで検出されている。
- » RA_LONDON Recovery Applianceにおける保護ポリシーを作成します（必要な場合）。
 - » Enterprise Manager Cloud Controlで、Recovery Appliance→Protection Policiesページにナビゲートし、「Create」をクリックします。
- » RA_LONDONデータベースでRecovery Applianceユーザーを作成します（必要な場合）。
 - » RA_LONDONクラスター・データベース・ターゲットについて、Schema→Usersページにナビゲートします。

Recovery Applianceユーザー・アカウントには"create session"システム権限のみを与えてください。このアカウントには、それ以外のシステム権限またはロールを許可しないでください。

- » RA_LONDONアプライアンスについての希望の保護ポリシーにPSFT_LONDONデータベースを追加します。
 - » Recovery Appliance→Protected Databasesページにナビゲートし、「Add」をクリックしてPSFT_LONDONデータベースを追加します。
 - » 「Add」をクリックし、Enterprise Managerで先に検出されていたPSFT_LONDONデータベースを選択します。
 - » 希望の保護ポリシーを選択します。

- » PSFT_LONDONデータベース用に予約する領域のサイズを指定します。
- » 新しいRecovery Applianceユーザーを追加する、または既存の名前付き資格証明を選択し、「OK」をクリックします。
- » PSFT_LONDONデータベースをRA_LONDONアプライアンスに登録します。
 - » PSFT_LONDONクラスタ・データベース・ターゲットについて、Availability→Backup & Recovery→Backup Settings ページにナビゲートします。
 - » Recovery Applianceを選択し、ドロップダウン・リストから仮想プライベート・カタログ・ユーザーを選択して、「Apply」をクリックします。
- » PSFT_LONDONデータベースについての構成設定を変更します。
 - » Recovery Applianceを使用する場合、以下の変更がベスト・プラクティスと考えられます。これらの変更は、Enterprise Managerから、またはRecovery Manager CLIを使用して設定できます。
 - CONFIGURE BACKUP OPTIMIZATION ON;
 - CONFIGURE CONTROLFILE AUTOBACKUP ON;
 - CONFIGURE DEFAULT DEVICE TYPE TO 'SBT_TAPE';
 - CONFIGURE DEVICE TYPE 'SBT_TAPE' PARALLELISM 8;
 - ブロック・チェンジ・トラッキング・ファイル機能を有効にします。
 - フラッシュバック・データベース機能を有効にします。フェイルオーバー後のスタンバイ・データベースの再作成を避けるため、最小限の60分間の保存に設定します。
- » PSFT_LONDONデータベースをRA_LONDONアプライアンスにバックアップします。
 - » 次のRecovery Managerスクリプトは、Recovery Applianceに最初のバックアップを作成するときのベスト・プラクティスと考えられます。
 - RMAN> backup cumulative incremental level 0 filesperset 1 section size 32g database plus archivelog filesperset 32;
 - » Recovery Managerタグを必要に応じて追加できます。
- » PSFT_LONDONデータベース上に仮想プライベート・カタログ・ユーザーを作成します。

この手順は、フィジカル・スタンバイ・データベースを追加するための前提条件です。この手順を後で実行することもできますが、その分追加の停止が必要になります。

Data GuardがRecovery Appliance環境の外側に構成されている場合、redo_transport_userパラメータはNULLのままであり、システムはデフォルトとしてSYSユーザーを使用します。プライマリ・データベースとスタンバイ・データベースにはSYSユーザーがすでにあるため、通常この手順は実行されません。Data Guard転送についてSYS以外のREDO転送ユーザーを使用するには、スタンバイ・データベースがインスタンス化される前に、このOracleユーザーをプライマリ・データベースに作成し、必要なシステム権限を付与する必要があります。

リアルタイムREDO転送ユーザーを有効にするこの後の手順では、database init.oraパラメータのredo_transport_userを"vpcuser"に設定します。この手順では、保護データベースがアプライアンスからのREDOを受信しないため、そのデータベースでOracleユーザーを作成する必要はありません。ただし、PSFT_LONDONデータベースでのREDO転送ユーザー作成は、後の手順でフィジカル・スタンバイ・データベースを作成するために必要です。この手順を後で実行すると、追加の再起動が必要になります。

Oracle Database 11g Release 2の場合、クラスタのすべてのノードについてorapwdファイルをリフレッシュしてください。

- » PSFT_LONDONクラスタ・データベース・ターゲットについて、Schema→Usersページにナビゲートします。

仮想プライベート・カタログ・ユーザーには、"create session"および"sysoper"のシステム権限が必要です。Oracle Database 12c保護データベースの場合、必要であれば"sysdg"システム権限を仮想プライベート・カタログ・ユーザーに付与することもできます。このユーザーには、それ以外のシステム権限またはロールを許可しないでください。

- » 次に進む前にログを強制的に切り替えて、すべてのスタンバイ・データベースにREDOが適用されるようにします。
- » PSFT_LONDONデータベースからRA_LONDONアプライアンスへのリアルタイムREDO転送を有効にします。

この手順は、データベースを再起動しなければならないため、データベースの停止が必要です。再起動は、ログ転送メカニズムがRecovery ApplianceへのリアルタイムREDO送信に使用する、新たに作成されたウォレットにOracleインスタンスがアクセスするのに必要です。

データベースの停止が不可能な場合は、この手順を手動により、一度に1個のインスタンスを再起動するローリング方式で実行できます。詳しい手順については、「付録3」を参照してください。

- » PSFT_LONDONクラスタ・データベース・ターゲットについて、Availability→Backup & Recovery→Backup Settingsページにナビゲートします。
- » Recovery Appliance Settingsセクションで、「Enable Real-Time Redo Transport」を選択し、「Apply」をクリックします。

この時点では、PSFT_LONDONデータベースをRA_LONDONアプライアンスにバックアップできます。そして、PSFT_LONDONデータベースはリアルタイムREDO転送を使用して、RA_LONDONアプライアンスにREDOを送信しています。

PSFT_PHILLYリモート・スタンバイ・データベースの構成への追加

この手順を実行すると、図9に示すような構成となります。

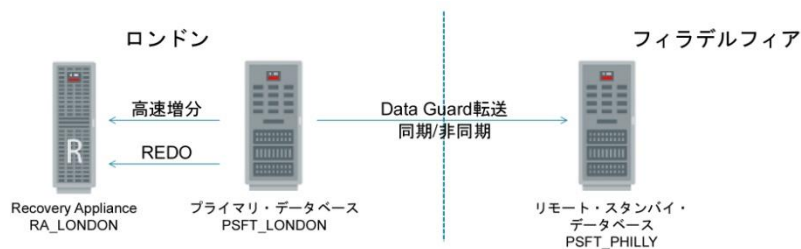


図9：構成に追加されたPSFT_PHILLYリモート・スタンバイ・データベース

- » まだ作成していない場合は、PSFT_LONDONデータベースについて仮想プライベート・カタログ・ユーザーを作成します。
- » PSFT_LONDONクラスタ・データベース・ターゲットについて、Schema→Usersページにナビゲートします。

仮想プライベート・カタログ・ユーザーには、"create session"および"sysoper"のシステム権限が必要です。必要であれば、仮想プライベート・カタログ・ユーザーに"sysdg"システム権限を付与することもできます。このユーザーには、それ以外のシステム権限またはロールを許可しないでください。

- » 次に進む前にログを強制的に切り替えて、すべてのスタンバイ・データベースにREDOが適用されるようにします。
- » PSFT_PHILLYフィジカル・スタンバイ・データベースを作成します。
 - » Availability→Add Standby Databaseウィザードにナビゲートし、次の手順に従って作成します。
- » Oracle Cluster Registryに記録されているデータベース・インスタンス名を手動で修正します。

この手順は、Oracle Bug# 20365706に関連して必要です。

- `$ srvctl config database -d PSFT_PHILLY`
- `$ srvctl modify database -d PSFT_PHILLY -i psft`
- » PSFT_PHILLYデータベースについての構成設定を変更します。
 - » PSFT_PHILLY用の制御ファイルは、Add Standby Databaseウィザードの一部としてPSFT_LONDONからコピーされています。SNAPSHOT CONTROLFILEの場所を修正します。
 - `CONFIGURE SNAPSHOT CONTROLFILE NAME TO '+RECOC1/PSFT_PHILLY/snapcf_psft.f';`
 - ブロック・チェンジ・トラッキング・ファイル機能を有効にします。
 - フラッシュバック・データベース機能を有効にします。フェイルオーバー後のスタンバイ・データベースの再作成を避けるため、最小限の60分間の保存に設定します。
- » RA_LONDON Recovery ApplianceをData Guard Broker構成に追加します。

この手順はOracle Database 12c保護データベースにのみ必要です。この手順は、フィジカル・スタンバイ・データベースを再起動しますが、プライマリ・データベースは再起動しません。

- » PSFT_LONDONクラスタ・データベース・ターゲットについて、Availability→Data Guardページにナビゲートします。
- » 「Add Recovery Appliance」をクリックし、RA_LONDONアプライアンスを選択し、ドロップダウン・リストから該当の仮想プライベート・カタログ・ユーザーを選択します。
- » PSFT_LONDONデータベースおよびPSFT_PHILLYデータベースについて、名前付き資格証明を選択し、「Submit」をクリックします。
- » Oracle Database 12c保護データベースの場合、RedoRoutesを設定し、PSFT_LONDONがREDOを常にRA_LONDONアプライアンスに送信するようにします。
 - » PSFT_LONDONクラスタ・データベース・ターゲットについて、Availability→Data Guardページにナビゲートします。
 - » 「Edit」をクリックしてプライマリ・クラスタ・データベースのプロパティを編集し、Edit Primary Database Propertiesページの「Common Properties」タブをクリックします。
 - » 次のRedoRoutes文字列を入力し、「Apply」をクリックします。

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

この文字列のコンテキストは編集対象のデータベース、すなわちPSFT_LONDONです。この文字列は、"PSFT_LONDONがプライマリ・データベースのとき、PSFT_PHILLYとそのアプライアンスの両方にREDOを送信するよう、ログ・アーカイブ宛先を設定する ("zdlra2"はRA_LONDONアプライアンスのエイリアス)。PSFT_PHILLYがプライマリ・データベースのとき、RA_LONDONアプライアンス (zdlra2) にのみREDOを送信するよう、PSFT_PHILLYのログ・アーカイブ宛先を設定する"と解釈されます。

- » Oracle Database 12c保護データベースの場合、RedoRoutesを設定し、PSFT_PHILLYがREDOをRA_LONDONアプライアンスに送信ないようにします。
 - » PSFT_LONDONクラスタ・データベース・ターゲットについて、Availability→Data Guardページにナビゲートします。

- » PSFT_PHILLYスタンバイ・クラスタ・データベースを選択し、「Edit」をクリックしてスタンバイ・データベースのプロパティを編集し、Edit Primary Database Propertiesページの「Common Properties」タブをクリックします。
- » 次のRedoRoutes文字列を入力し、「Apply」をクリックします。

(psft_philly: psft_london)

この文字列のコンテキストは編集対象のデータベース、すなわちPSFT_PHILLYです。この文字列は、"PSFT_PHILLYがプライマリ・データベースのとき、PSFT_LONDONにREDOを送信するよう、PSFT_PHILLYのログ・アーカイブ宛先を設定する。PSFT_PHILLYがプライマリ・データベースでない場合は、PSFT_PHILLYのログ・アーカイブ宛先を設定しない"と解釈されます。

RA_PHILLY Recovery Applianceの構成への追加

この手順を実行する、最終構成は図10のようになります。

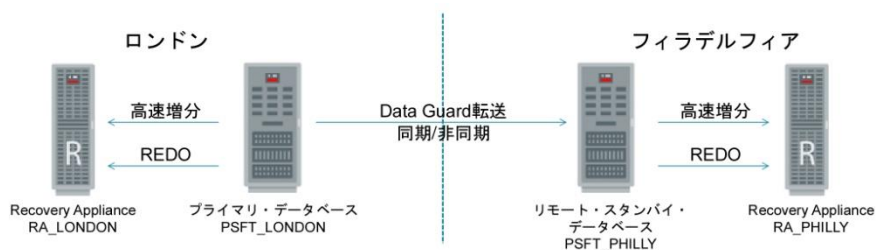


図10：Recovery Applianceとスタンバイ・データベースが環境に統合された最終構成

- » RA_PHILLY Recovery Applianceにおける保護ポリシーを作成します（必要な場合）。
 - » Recovery Appliance→Protection Policiesページにナビゲートし、「Create」をクリックします。

RA_PHILLYアプライアンスに対する保護ポリシーの値は、RA_LONDONアプライアンスに対する保護ポリシーの値と同じものにしないでかまいません。

- » RA_PHILLYデータベースでRecovery Applianceユーザーを作成します（必要な場合）。
 - » RA_PHILLYクラスタ・データベース・ターゲットについて、Schema→Usersページにナビゲートします。

Recovery Applianceユーザーには"create session"システム権限のみを与えてください。このユーザーには、それ以外のシステム権限またはロールを許可しないでください。

- » RA_PHILLYアプライアンスについての希望の保護ポリシーにPSFT_PHILLYデータベースを追加します。

この手順でPSFT_PHILLYデータベースを選択する場合は、データベースを登録する手順を実行する前に、Data Guardスイッチオーバーを実行してPSFT_PHILLYをプライマリ・クラスタ・データベースにしなければなりません。PSFT_PHILLYへのスイッチオーバーを実行できない場合、PSFT_PHILLYデータベースは引き続きRA_PHILLYアプライアンスにバックアップされますが、RA_PHILLYアプライアンスのProtected DatabasesページにはPSFT_LONDONが表示されます。

この手順は、この時点でスイッチオーバーは実行されていないと仮定しています。そのため、PSFT_LONDONがプライマリ・クラスタ・データベースです。

- » Recovery Appliance→Protected Databasesページにナビゲートし、「Add」をクリックしてPSFT_LONDONデータベースを追加します。
- » 「Add」をクリックし、Enterprise Managerで先に検出されていたPSFT_LONDONデータベースを選択します。
- » 希望の保護ポリシーを選択します。
- » PSFT_LONDONデータベース用に予約する領域のサイズを指定します。
- » 新しいRecovery Applianceユーザーを追加する、または既存の名前付き資格証明を選択し、「OK」をクリックします。
- » PSFT_LONDONデータベースをRA_PHILLYアプライアンスに登録します。
 - » PSFT_LONDONクラスタ・データベース・ターゲットについて、Availability→Backup & Recovery→Backup Settingsページにナビゲートします。
 - » (Recovery Applianceの設定にはRA_LONDONアプライアンスが表示されます。) 「Clear Configuration」をクリックします。
 - » フィラデルフィアのRecovery Applianceを選択し、ドロップダウン・リストから仮想プライベート・カタログ・ユーザーを選択して、「Apply」をクリックします。
- » PSFT_PHILLYデータベースがRA_PHILLYアプライアンスにバックアップされるよう設定します。
 - » PSFT_PHILLYクラスタ・データベース・ターゲットについて、Availability→Backup & Recovery→Backup Settingsページにナビゲートします。
 - » (Recovery Applianceの設定にはRA_PHILLYアプライアンスが表示されます。) 「Clear Configuration」をクリックします。
 - » 「Configure this physical standby database to send backups to the specified Recovery Appliance」を選択します。灰色表示のボックスに表示されるRecovery ApplianceはRA Phillyです。「Apply」をクリックします。
- » PSFT_LONDONデータベースがRA_LONDONアプライアンスにバックアップされるよう再設定します。
 - » PSFT_LONDONクラスタ・データベース・ターゲットについて、Availability→Backup & Recovery→Backup Settingsページにナビゲートします。
 - » (Recovery Applianceの設定にはRA_PHILLYアプライアンスが表示されます。) 「Clear Configuration」をクリックします。
 - » ロンドンのRecovery Applianceを選択し、ドロップダウン・リストから仮想プライベート・カタログ・ユーザーを選択して、「Apply」をクリックします。
- » PSFT_PHILLYデータベースからRA_PHILLYアプライアンスへのリアルタイムREDO転送を有効にします。

すぐ下の手順は、Oracle Database 12c保護データベースについてのみ適用可能です。この手順は、データベースを再起動しなければならないため、データベースの停止が必要です。再起動は、ログ転送メカニズムがRecovery ApplianceへのリアルタイムREDO送信に使用する、新たに作成されたウォレットにOracleインスタンスがアクセスするのに必要です。

データベースの停止が不可能な場合は、この手順を手動により、一度に1個のインスタンスを再起動するローリング方式で実行できます。詳しい手順については、「付録4」を参照してください。

Oracle Database 11g Release 2保護データベースの場合は、「付録4」の手順に従ってください。

Data Guardページには、Data GuardのステータスがERRORであり、新たに追加されたRA_PHILLYがREDOデータを受信していないというレポートが表示されます。このERRORは、次の手順でRedoRoutesを設定すると解決します。

-
- » PSFT_PHILLYクラスタ・データベース・ターゲットについて、Availability→Data Guardページにナビゲートします。

- » 「Add Recovery Appliance」をクリックし、「RA_PHILLY」アプライアンスを選択し、ドロップダウン・リストから該当の仮想プライベート・カタログ・ユーザーを選択します。
- » PSFT_PHILLYデータベースおよびPSFT_LONDONデータベースについて、名前付き資格証明を選択し、「Submit」をクリックします。
- » Oracle Database 12c保護データベースの場合、RedoRoutesを設定し、PSFT_PHILLYがREDOを常にRA_PHILLYアプライアンスに送信するようにします。
 - » PSFT_PHILLYクラスタ・データベース・ターゲットについて、Availability→Data Guardページにナビゲートします。
 - » 「Edit」をクリックしてプライマリ・クラスタ・データベースのプロパティを編集し、Edit Primary Database Propertiesページの「Common Properties」タブをクリックします。
 - » 次のRedoRoutes文字列を入力し、「Apply」をクリックします。

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

この文字列のコンテキストは編集対象のデータベース、すなわちPSFT_PHILLYです。この文字列は、"PSFT_PHILLYがプライマリ・データベースのとき、PSFT_LONDONとそのアプライアンスの両方にREDOを送信するよう、ログ・アーカイブ宛先を設定する ("zdlra6"はRA_PHILLYアプライアンスのエイリアス)。PSFT_LONDONがプライマリ・データベースのとき、RA_PHILLYのアプライアンス (zdlra6) にのみREDOを送信するよう、PSFT_PHILLYデータベースのログ・アーカイブ宛先を設定する"と解釈されます。

- » Oracle Database 12c保護データベースの場合、PSFT_LONDONデータベースがRA_LONDONアプライアンスに接続するよう、Recovery Managerチャンネルを設定します。
 - » Data Guard Add Recovery Applianceウィザードを使用した場合、PSFT_LONDONデータベースについてのRecovery Managerチャンネルの定義は、RA_PHILLY Recovery Applianceを参照しています。CONFIGURE CHANNEL DEVICE TYPE SBT句のcredential_alias ENV変数のみを変更し、代わりにRA_LONDONアプライアンスのエイリアスを参照するようにします。たとえば次のようになっています。
 - 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');
 - » これを次のように変更する必要があります。
 - 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');
- » PSFT_LONDONデータベースおよびPSFT_PHILLYデータベースについて、Recovery Managerのアーカイブ・ログ削除ポリシーを設定します。
 - » アーカイブ・ログがRecovery Applianceに送信され、フィジカル・スタンバイ・データベースに適用された後、フラッシュ・リカバリ領域が自動的に消去されるようにするには次のようにします。
 - CONFIGURE ARCHIVELOG DELETION POLICY TO APPLIED ON ALL STANDBY BACKED UP 1 TIMES TO 'SBT_TAPE';
- » Recovery Manager db_unique_nameコネクション文字列を設定します。
 - » カタログを再同期化するため、Recovery Managerでプライマリ・データベースにログインできるようにするには、PSFT_LONDONデータベースに以下の変更が必要です。
 - CONFIGURE DB_UNIQUE_NAME 'psft_london' CONNECT IDENTIFIER 'scam06client-scan1/psft_london';

- CONFIGURE DB_UNIQUE_NAME 'psft_philly' CONNECT IDENTIFIER 'scam06client-scan5/psft_philly';
- » PSFT_PHILLYデータベースのこれらの設定をレプリケートするには、Recovery Managerを使用してPSFT_LONDONターゲット・データベースおよびRA_PHILLYカタログに接続します。
 - \$ rman target / catalog /@scaz10ingest-scan1:1521/zdra6:dedicated
 - RMAN> resync catalog;
 - RMAN> show db_unique_name;

Data Guardのロール移行

2つのシナリオに対するこれまでのセクションの手順は、それぞれの場所（ロンドンおよびフィラデルフィア）において、それぞれのローカルRecovery Appliance（ロンドンはRA_LONDON。フィラデルフィアはRA_PHILLY）にデータベース・バックアップを実行するよう設計されています。

このため、ロールの移行が発生する場合、実行中のRecovery Managerバックアップ・ジョブに対する変更は必要ありません。

スイッチオーバーが発生すると、新しいバックアップが続いて実行されますが、スイッチオーバー時点で進行中だったバックアップは再起動が必要となる場合があります。

フェイルオーバーが発生すると、新しいプライマリ・データベースに対して、引き続きバックアップが実行されます。元のプライマリ・データベースを回復する必要がありますが、フラッシュバック・データベースが有効になっていれば、停止が一時的な場合はローカルRecovery Applianceからデータベースをリストアする必要はありません。大規模な停止の場合、標準的な手順を使用してローカルRecovery Applianceからデータベースをリストアできます。

結論

ベスト・プラクティスを取り上げたこのペーパーに示した2つの手順は、ローカル・バックアップに関するRecovery Applianceの統合、そしてData Guard構成（フィジカル・スタンバイ）におけるプライマリとスタンバイの両データベースのリカバリを対象としています。何らかの理由でアプライアンスのうちの1つが使用できなくなった場合、各データベースはどちらか（ローカルまたはリモート）のRecovery Applianceをリカバリに使用できます。プライマリ・データベースとスタンバイ・データベースの間のData Guard REDO転送により、Recovery Appliance間でのバックアップのレプリケートが不要となります。

参考資料

[Zero Data Loss Recovery Applianceの概要](#)

[MAA ベスト・プラクティス - 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](#)

付録1：

この付録は、プライマリ・データベースの各インスタンスを一度に1ノードずつ再起動することにより、リアルタイムREDO転送を手動で設定して有効化するのに必要な手順を詳しく示します。

次の手順は、2つのinit.oraパラメータを再設定し、新しいログ・アーカイブ宛先を設定します。

- » データベース間のREDO送信およびRA_LONDONアプライアンスの追加に使用するプライマリ・データベースとスタンバイ・データベースについて、redo_transport_userパラメータを再設定します。
 - » SIEBEL_LONDONとSIEBEL_PHILLYの両方について、redo_transport_userパラメータは、保護データベースが使用する仮想プライベート・カタログ (VPC) ユーザーを指定します。
 - ALTER SYSTEM SET redo_transport_user='VPCSIEBEL' SCOPE=SPFILE;
- » 新しいREDO転送ユーザーを使用するため、SIEBEL_LONDON上とSIEBEL_PHILLY上のインスタンスを一度に1つずつ再起動します。
- » RA_LONDONアプライアンスをOracle Data Guard Broker構成に追加します。
 - » Oracle Database 12cの場合、SYSパスワードを使用してData Guard Broker CLIにログインし、Recovery Appliance "zdlra2"をData Guard Broker構成に追加し、さらに有効にします。

Oracle Database 12.1.0.2 Bundle Patch 6よりも前のバージョンでは、次のコードにおいて、"recovery_appliance"の代わりに"backup_appliance"を使用してください。

- DGMGRL> add recovery_appliance zdlra2 as connect identifier is 'scas10ingest-scan5:1521/zdlra2:dedicated';
- DGMGRL> enable recovery_appliance zdlra2;
- » Oracle Database 11gの場合、SYSパスワードを使用してSQL*Plusにログインし、使用可能なログ・アーカイブ宛先を設定します。
 - 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)'

付録2：

この付録は、フィジカル・スタンバイ・データベースの各インスタンスを一度に1ノードずつ再起動することにより、フィジカル・スタンバイ・データベースに対するリアルタイムREDO転送を手動で設定し、有効化するのに必要な手順を詳しく示します。

この手順は、redo_transport_userパラメータも設定する「付録1」の手順とは異なります。この手順は、redo_transport_userパラメータの設定が完了していることが前提です。

- » »新しいREDO転送ユーザーを使用するため、SIEBEL_LONDON上とSIEBEL_PHILLY上のインスタンスを一度に1つずつ再起動します。
- » RA_PHILLYアプライアンスをOracle Data Guard Broker構成に追加します。

- » Oracle Database 12cの場合、SYSパスワードを使用してData Guard Broker CLIにログインし、Recovery Appliance "zdlra6"をData Guard Broker構成に追加し、さらに有効にします。

Oracle Database 12.1.0.2 Bundle Patch 6よりも前のバージョンでは、以下に示すコードにおいて、"recovery_appliance"の代わりに"backup_appliance"を使用してください。

- DGMGRL> add recovery_appliance zdlra6 as connect identifier is 'scaz10ingest-scan1:1521/zdlra6:dedicated';
- DGMGRL> enable recovery_appliance zdlra6;
- » Oracle Database 11gの場合、SYSパスワードを使用してSQL*Plusにログインし、使用可能なログ・アーカイブ宛先を設定します。
 - 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 'ASYNCR 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)'

付録3：

この付録は、プライマリ・データベースの各インスタンスを一度に1ノードずつ再起動することにより、リアルタイムREDO転送を手動で設定して有効化するのに必要な手順を詳しく示します。

この手順は、2つのinit.oraパラメータを再設定し、新しいログ・アーカイブ宛先を設定します。

- » RA_LONDONアプライアンスへのREDO送信に使用するプライマリ・データベースについて、redo_transport_userパラメータを再設定します。
 - » PSFT_LONDONについて、redo_transport_userパラメータは、保護データベースが使用する仮想プライベート・カタログ (VPC) ユーザーを指定します。
 - ALTER SYSTEM SET redo_transport_user='VPCPSFT' SCOPE=SPFILE;
- » 新しいREDO転送ユーザーを使用するため、PSFT_LONDON上のインスタンスを一度に1つずつ再起動します。
- » SYSパスワードを使用してSQL*Plusにログインし、次に示すように、使用可能なログ・アーカイブ宛先を設定します。
 - 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) ASYNCR DB_UNIQUE_NAME=zdlra2';

付録4：

この付録は、フィジカル・スタンバイ・データベースの各インスタンスを一度に1ノードずつ再起動することにより、フィジカル・スタンバイ・データベースに対するリアルタイムREDO転送を手動で設定し、有効化するのに必要な手順を詳しく示します。

この手順は、redo_transport_userパラメータも設定する「付録3」の手順とは異なります。この手順は、redo_transport_userパラメータの設定が完了していることが前提です。

- » 新しいREDO転送ユーザーを使用するため、PSFT_LONDON上とPSFT_PHILLY上のインスタンスを一度に1つずつ再起動します。
- » RA_LONDONアプライアンスをOracle Data Guard Broker構成に追加します。
 - » Oracle Database 12cの場合、SYSパスワードを使用してData Guard Broker CLIにログインし、Recovery Appliance "zdlra2"をData Guard Broker構成に追加し、さらに有効にします。

Oracle Database 12.1.0.2 Bundle Patch 6よりも前のバージョンでは、以下に示すコードにおいて、"recovery_appliance"の代わりに"backup_appliance"を使用してください。

- DGMGRL> add recovery_appliance zdlra6 as connect identifier is 'scaz10ingest-scan1:1521/zdlra6:dedicated';
- DGMGRL> enable recovery_appliance zdlra6;
- » Oracle Database 11gの場合、SYSパスワードを使用してSQL*Plusにログインし、次に示すように、使用可能なログ・アーカイブ宛先を設定します。
 - SQL> alter system set log_archive_config='dg_config=(zdlra2,psft_london,psft_philly,zdlra6);
- » Oracle Database 11gの場合、PSFT_LONDONデータベース上でSYSパスワードを使用してSQL*Plusにログインし、付録3で設定し、RA_PHILLYを構成に追加した後キャンセルしたログ・アーカイブ宛先を再確立します。
 - 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;
- » Oracle Database 11gの場合、PSFT_PHILLYデータベース上でSYSパスワードを使用してSQL*Plusにログインし、ログ・アーカイブ宛先を設定します。
 - 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

海外からのお問い合わせ窓口：
電話：+1.650.506.7000
ファクシミリ：+1.650.506.7200

Integrated Cloud Applications & Platform Services

CONNECT WITH US



Copyright © 2015, Oracle and/or its affiliates. All rights reserved.

本文書は情報提供のみを目的として提供されており、ここに記載される内容は予告なく変更されることがあります。本文書は、その内容に誤りがないことを保証するものではなく、また、口頭による明示的保証や法律による黙示的保証を含め、商品性ないし特定目的適合性に関する黙示的保証および条件などのいかなる保証および条件も提供するものではありません。

オラクルは本文書に関するいかなる法的責任も明確に否認し、本文書によって直接的または間接的に確立される契約義務はないものとします。本文書はオラクルの書面による許可を前もって得ることなく、いかなる目的のためにも、電子または印刷を含むいかなる形式や手段によっても再作成または送信することはできません。

OracleおよびJavaはOracleおよびその子会社、関連会社の登録商標です。その他の名称はそれぞれの会社の商標です。

IntelおよびIntel XeonはIntel Corporationの商標または登録商標です。すべてのSPARC商標はライセンスに基づいて使用されるSPARC International, Incの商標または登録商標です。AMD、Opteron、AMDロゴおよびAMD Opteronロゴは、Advanced Micro Devicesの商標または登録商標です。UNIXは、The Open Groupの登録商標です。0615

Oracle Data Guard構成におけるZero Data Loss Recovery Applianceの導入

2015年11月

著者：Andrew Babb



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