

Oracle Maximum
Availability Architecture

Oracle ホワイト・ペーパー
2012年8月16日

Oracle Exalogicのバックアップとリカバリの ベスト・プラクティス

概要.....	1
はじめに	3
概念.....	4
バックアップとリカバリの概要.....	4
Oracle Secure Backupの概要.....	9
外部デバイスとExalogicマシンの接続.....	11
リモート・ストレージ・アプライアンスとの接続	11
テープ管理デバイスとの接続.....	13
バックアップ・ネットワークの作成.....	16
VLANを使用した外部デバイスの接続.....	26
Exalogicディスクの構成.....	30
ディスクのレイアウト	30
スナップショットの可視性.....	32
バックアップの実行	32
ディスク・バックアップ	32
テープ・バックアップ.....	36
オペレーティング・システムのバックアップ	43
スイッチのバックアップ.....	43
バックアップのリストア	44
ディスクから	44
テープから	47
スイッチのリストア	48
結論.....	49
参考資料	49

概要

Oracle Maximum Availability Architecture (MAA) は、オラクルの高可用性テクノロジーを実装するためのベスト・プラクティス構想です。Maximum Availability Architectureは、Oracle Fusion Middlewareのエンタープライズ・デプロイメントの主要な要件の1つです。Oracle Fusion Middlewareには、プロセス停止の検出と再起動、サーバーのクラスタ化、サーバーの移行、クラスタウェアの統合、GridLink、ロードバランシング、フェイルオーバー、バックアップとリカバリ、ローリング・アップグレード、ローリング構成の変更など、豊富な高可用性機能が含まれています。これらは、エンタープライズ・デプロイメントを計画外のダウンタイムから保護し、計画ダウンタイムの必要性を最小限に減らすことができます。

Oracle Exalogicは、各種アプリケーションおよびワークロードに対応する完全なプラットフォームを提供するために設計された、ハードウェアとソフトウェアの統合システムです。Exalogicは、大規模でパフォーマンスに影響されやすい、ミッション・クリティカルなアプリケーションの展開を対象としています。Exalogicシステムには多くの冗長コンポーネントが含まれるため、1つのコンポーネントの障害がシステム全体の可用性に影響することはありません。この組み込みの冗長性は、ハードウェア・コンポーネントの障害には対処できますが、次の障害から保護することはできません。

- Exalogicシステム全体の障害
- メディア障害
- ユーザー・エラー - ユーザーが誤って更新または削除した場合など

このようなエラーからリカバリするには、システムを同じハードウェアまたは新しいハードウェアにリストアできる必要があります。重要なシステムは、多くの場合、ディザスタ・リカバリ (DR) テクノロジーで保護されます。DRテクノロジーでは通常、オフサイトに同様のシステムが配置されます。このシステムは、プライマリ・システムが変更されると自動的に最新の状態となります。このため、プライマリ・システムの障害時にホット・スタンバイ機能を提供できます。

ホット・スタンバイ・システムはビジネスの継続性には非常に便利ですが、維持にコストがかかり、追加のインフラストラクチャが必要です。簡単なユーザー・エラーなどの場合、DRシステムにフェイルオーバーするより問題を解決した方が早い場合があります。DNSの更新が必要な場合は特にそうです。

ほとんどの本番システムでは、サイトのディザスタ・リカバリ・ソリューションの有無に関わらず、標準運用手順の一部としてシステムの定期的なバックアップを実行しています。このため、元のファイルまたはシステム全体に問題が発生しても、個々のファイルを柔軟にリストアできます。バックアップをオフサイトのセキュアな場所に保存することもできます。Exalogicでのバックアップは、Exalogicシステム内で、ディスク間、およびディスクとテープ間で実行できます。このホワイト・ペーパーでは、これらすべての場合にExalogicで使用できるオプションについて説明します。特定のデプロイメントで使用する必要がある特定の組合せは、サイトの要件によって異なります。

ExalogicにはSun ZFS Storage 7320アプライアンスが付属しています。このホワイト・ペーパーでは、ディスク・ベースのバックアップでストレージの組込み機能を利用する方法について説明します。テープにバックアップする場合、Network Data Management Protocol (NDMP) か、コンピュート・ノードにデプロイされているバックアップ・エージェントを使用できます。NDMPではテープ・バックアップ・ソフトウェアを使用し、オペレーティング・システム経由ではなく直接ストレージ・アプライアンスと連携できるため、より高速で、Exalogicのコンピュート・ノードでのオーバーヘッドがありません。ただし、ローカル・ストレージに保存されているオペレーティング・システムやその他のファイルのバックアップには使用できません。バックアップ速度が問題の場合、最速の解決方法はNDMPを使用することですが、コンピュート・ノードからバックアップを取る方が柔軟です。

Oracle ExadataマシンとOracle Exalogicマシンのバックアップおよびリカバリ・ソリューションは、それぞれOracle DatabaseとOracle Fusion Middlewareの確立されたソリューション上に構築されています。このホワイト・ペーパーで説明するディスクからテープへのバックアップではOracle Secure Backupを使用しますが、このメカニズムはどのテープ・メディア管理ソリューションにも適用できます。

はじめに

このホワイト・ペーパーでは、Oracle Exalogicマシン内に保持されているデータのバックアップ（およびリストア）に特化して説明します。

Oracle Exalogicマシンに含まれる、バックアップが必要なデータは次のとおりです。

- Exalogicオペレーティング・システム
- ソフトウェア・バイナリ
- 構成情報
- JMSキューとしてのトランザクション・ログなどのトランザクション・データ
- スイッチ構成
- ディスクに保存されているその他のアーティファクト

これらのオブジェクトは、以下にバックアップできます。

- 同じストレージ・アプライアンス内のディスク
- 同じストレージ・タイプ（ZFS）を使用するリモート・マシン上のディスク
- 別のストレージ・タイプを使用するリモート・マシン上のディスク
- テープ

バックアップ戦略には、上記のうち複数を使用することが考えられます。このホワイト・ペーパーでは、これらのバックアップの実行と、そのバックアップからリストアする最適な方法について説明します。

概念

バックアップとリカバリの概要

変更度

オブジェクトは変更度によってグループ化できます。たとえば、オペレーティング・システムはごくまれにしか変更されないため、変更頻度の高いトランザクション・データのように頻繁にバックアップする必要はありません。一般的なExalogicデプロイメント・オブジェクトは、次のカテゴリにグループ化できます。

変更度グループ

変更度	オブジェクトの例
低	<input type="checkbox"/> Oracleバイナリ <input type="checkbox"/> オペレーティング・システム
中	<input type="checkbox"/> 構成情報 <ul style="list-style-type: none"> - WLSドメイン - Oracleインスタンス
高	<input type="checkbox"/> ファイル・ベースのJMSキュー <input type="checkbox"/> 永続ストア

バックアップの頻度

データの変更度によって、バックアップ頻度を定めることができます。変更度のほか、次の要素もデータのバックアップ頻度に影響する場合があります。

- バックアップするデータのボリューム
- 使用可能なバックアップ・ウィンドウ
- 規制要件

上記の変更度グループを使用した場合、適切なバックアップ頻度は次のとおりです。

バックアップ・スケジュール

変更度グループ	バックアップの頻度
低	毎月
中	毎週
高	毎日

定期的なバックアップのほか、主要なイベントの発生時には随時バックアップを実行することをお勧めします。たとえば、パッチ適用やアップグレードの後には、Oracleバイナリを別途バックアップしてください。

保存期間

バックアップ戦略を決める際、バックアップの保存期間を考慮に入れる必要があります。これはおもに、ビジネスや規制の要件によりますが、上記の例では次の値が適切です。

保存期間

変更度グループ	保存期間
低	3年
中	6か月
高	7日

バックアップ・タイプ

利用できるバックアップには、完全バックアップと増分バックアップの2種類があります。完全バックアップでは、ある時点でのファイル・システム全体がそのままバックアップされます。増分バックアップでは、最後のバックアップ以降に変更されたデータのみがバックアップされます。増分バックアップには、累積または差分があります。累積バックアップでは最後の完全バックアップ以降の変更がすべてバックアップされ、差分バックアップでは最後の差分バックアップ以降の変更がバックアップされます。差分バックアップは、ZFSストレージ・アプライアンスではサポートされていませんが、テープにバックアップする場合は幅広く使用できます。

増分バックアップはレベル化できます。レベル0（完全バックアップ）は月ごと、レベル1（増分バックアップ）は日曜日ごと、レベル2（増分バックアップ）は平日ごとに実行できます。このタイプの戦略を実装すると、最後のレベル1バックアップ以降に変更されたデータのみがバックアップされます。たとえば火曜日にバックアップされるのは、その前の日曜日に実行した最後のレベル1バックアップ以降に変更されたデータです。増分バックアップは、バックアップするデータのボリュームが多い場合は便利です。

完全バックアップの利点は、リストアの実行に必要な情報がすべて含まれていることです。増分バックアップ戦略では、多くの場合、リストアで複数のバックアップが使用されます。上記の3レベルのバックアップ戦略では、最後のレベル0バックアップと実行した最後のレベル1バックアップ、および実行した最後のレベル2バックアップが必要です。バックアップするデータのボリュームが小さい場合は、増分バックアップよりも完全バックアップを毎回実行する方が簡単な場合がありますが、これはバックアップするデータのボリュームによって決まります。

増分バックアップは、Oracle Secure Backupとオペレーティング・システムのdumpコマンドでサポートされています。

注：増分バックアップ戦略の一般的な使用方法では、完全バックアップを週に1回、増分の累積バックアップを日に1回実行します。ただしデータ・ボリュームが増えるにしたがって、マルチレベル方式の方が適切な可能性があります。

プロセスが停止した場合、ホット・バックアップ（プロセスの実行時）またはコールド・バックアップを実行できます。コールド・バックアップの利点は、実行時にすべてが一貫性のある状態であることです。コールド・バックアップの欠点は、バックアップの実行中にシステムを使用できないことです。次のいくつかの方法で、ダウンタイムなしで一貫性のあるバックアップを実行できます。ホット・バックアップが可能かどうかは、バックアップ中のアーティファクトによって変わります。ソフトウェア・ベンダーに問い合わせ、バックアップ対象の製品を実行しながらバックアップできるかどうかを確認してください。Oracle Fusion Middlewareでは、ホット・バックアップがサポートされています。

Exalogicのバックアップ・テクノロジー

スナップショット

ZFSでは、Copy-on-Writeのトランザクション・モデルが使用されます。つまり、ZFSで新規データが書き込まれると、古いデータを含むブロックが保存されます。スナップショットは、ある時点で最新のデータ・ブロックの内部コピーです。スナップショットではブロックの場所のみが保存され、既存のデータ・ブロックを直接バックアップする必要がないため、高速に実行できます。このため、スナップショットでは容量をほとんど消費しません。

利点：

- バックアップとリストアを高速に実行できます。
- 所定の時点で一貫性のあるバックアップを実行できます。
- ディスクでスナップショットを使用可能にすると、個々のファイルをリストアできます。
- ディザスタ・リカバリ戦略の一部として使用できます。
- テープにバックアップできます。
- スナップショットをZFSのリモート・アプライアンスに複製すると、リモート・サーバーにアクセスできるホストにそのスナップショットをマウントし、そこからテープにバックアップできるため、ソース・マシンでオーバーヘッドがほとんど発生しません。

欠点：

- スナップショットをリストアすると、スナップショット・データセット全体がリストアされます。
- ローカル・ファイル・システム（オペレーティング・システムなど）のバックアップには使用できません。
- 完全なストレージ・アプライアンスの障害からは、保護できません。

オペレーティング・システム・ユーティリティ

これらはバックアップ実行の従来の方法です。この方法には、オペレーティング・システムのコマンド（tar、dump、rsyncなど）を使用したバックアップ・ファイルの手動作成が含まれます。

利点：

- どのシステムでもリストアできます。
- 個々のファイルをリストアできます。

欠点：

- 作成に時間がかかる場合があります。これは、関連する共有数によって変わります。
- 特定の時点での一貫性のあるバックアップは保証されません。ただし、スナップショットからのバックアップによって、この問題を軽減できます。

ZFSストレージ・アプライアンスへのリモート・ディスク・バックアップ

リモート・ディスクにバックアップできます。リモート・ディスクが他のZFSストレージ・アプライアンスの場合、この操作はスナップショット・レプリケーションを使用して実行できます。

利点

- ストレージ・アプライアンス全体の損失を防ぎます。
- DR計画に組み込むことができます。
- ストレージ・アプライアンスの組込み機能を使用します。

欠点

- ローカル・ディスクのバックアップには使用できません。

ZFS以外のストレージ・アプライアンスへのリモート・ディスク・バックアップ

リモート・ディスクにバックアップできます。リモート・ディスクがZFSストレージ・アプライアンスでない場合は、ネットワーク・マウントに書き込むオペレーティング・システム・ユーティリティを使用してバックアップできます。

利点

- ・ ストレージ・アプライアンス全体の損失を防ぎます。
- ・ ローカル・ディスクのバックアップに使用できます。

欠点

- ・ ストレージ・アプライアンスの組込み機能は使用できません。
- ・ ネットワークとバックアップ・ボリュームによっては、作成に時間がかかる場合があります。

テープ・メディア・マネージャ

テープへのアーカイブには、テープ・メディア・マネージャが必要です。テープ・メディア・マネージャによって、物理テープ・メディアのカatalogへの追加と管理が行われます。また、テープ・メディア・マネージャは、Exalogicマシンとテープ・ライブラリ間のインタフェースとして機能します。メディア・マネージャによって、物理または仮想テープ・ライブラリにバックアップできます。この用途には、必要に応じて他の方法も使用できますが、Oracle Secure Backupの使用を推奨します。テープへのバックアップと他のバックアップ方法を組み合わせて使用して、階層型のアプローチを提供できます。

利点

- ・ 多種多様なバックアップ・バージョンを無期限に保存できます。
- ・ バックアップを複数のオフサイトの場所に複製および保持できます。
- ・ 物理テープは、メディア・マネージャによって管理されます。
- ・ 仮想テープ・ライブラリを使用して、物理テープ・ライブラリやディスクにバックアップできます。

欠点

- ・ 環境によっては、バックアップ速度が低下する場合があります。
- ・ リストアするバックアップがオンサイトやテープ・ライブラリにないと、リストア速度が低下する場合があります。

バックアップ戦略

バックアップ戦略の統合には多くの方法があり、これらの多くは、動作中のバックアップ・デバイスに依存します。実行可能なバックアップ戦略は次のとおりです。

1. ローカル・スナップショットを作成し、ユーザー・エラーから迅速にリストアおよびリカバリする。
2. マシン障害に備えて、アーカイブ・ストレージのテープ・バックアップを作成する。

完全リカバリ・セットの場合、スナップショットをテープに直接バックアップできます。ニア・ライン・ディスク・バックアップが必要な場合は、ZFS ストレージへのリモート・レプリケーションを使用したディスク間バックアップを推奨します。また、テープへのバックアップはリモート・ストレージ以外で実行できます。

注：Exalogicマシンをバックアップする場合、接続されているデータベースとの間でバックアップ・スケジュールを調整し、一貫性のあるリストアを実行できるようにします。

Oracle Secure Backupの概要

Oracle Secure Backupは、オラクルのエンタープライズ・テープ管理システムです。Oracle Secure Backupによってテープ・デバイスにバックアップでき、これらのバックアップを暗号化することでセキュリティを強化できます。Oracle Secure Backupによってテープへのバックアップが簡単になるほか、次の利点があります。

- バックアップ対象とバックアップ場所を追跡できます。
- メディアを再利用できるタイミングを追跡できます。
- テープ・ホールディングを実行できます。

このドキュメントでは、Oracle Secure Backupを使用してExalogicマシンをテープにバックアップする方法を説明します。Oracle Secure Backupは、以下の多くのコンポーネントで構成されます。

管理ドメイン

Oracle Secure Backupの管理ドメインは、バックアップ対象の管理サーバー、メディア・サーバー、テープ・ライブラリ、およびすべてのホストで構成されます。

管理サーバー

管理サーバーは、管理ドメインの構成情報を保存するホストです。管理サーバーには、バックアップ・カタログと、バックアップとリストアを開始するジョブ・スケジューラが含まれます。

メディア・サーバー

メディア・サーバーは、テープ・ドライブやサイロが接続されているコンピュータまたはサーバーです。メディア・サーバーは、直接接続されているテープ・デバイス、またはストレージ・エリア・ネットワークで接続されているテープ・デバイスとの間でデータを転送します。

クライアント

クライアントとは、Oracle Secure Backupのバックアップやリストアの対象となるファイルが含まれるコンピュータまたはストレージ・デバイスです。

バックアップの実行に使用されるのは、クライアントです。Exalogicマシンでは、バックアップ対象のExalogicコンピュート・ノードにOracle Secure Backupソフトウェアをインストールします。

Oracle Secure Backupはストレージ・アプライアンスと直接連携できるため、Oracle Secure Backupクライアント・ソフトウェアをインストールする必要はありません。この操作は、Network Data Management Protocol (NDMP) を使用して実行できます。NDMPプロトコルを使用した場合、NDMPのバックアップ・タイプであるzfsまたはダンプのオプションを使用して、ZFSストレージ・アプライアンスをバックアップすることもできます。

NDMPダンプを使用すると、ファイルはファイル単位でバックアップおよびリストアできるため、データの読取りが一貫して表示され、NDMPダンプによってまずスナップショットが開始されます。

NDMPのバックアップ・タイプであるzfsを使用すると、プロジェクトやファイル・システム全体が一度にバックアップされます。この操作では、まずスナップショットが作成され、バックアップの完了後に処理されます。この方法の欠点は個々のファイルをリストアできないことですが、パフォーマンスは非常に高くなります。この問題を解決するには、バックアップを別の場所にリストアし、そこから個々のファイルを抽出します。

メディア・ファミリ

メディア・ファミリとは、共通の属性を持つテープを論理的に分類したテープ・プールです。メディア・ファミリによって、同じテープへの保存期間、複製、およびボールティングの要件が似ているバックアップをグループ化します。

たとえば、変更度が高いバックアップを7日間、変更度が低いバックアップを1年間保持したい場合、保存期間が7日間と1年間の、2種類のメディア・ファミリを持つことになります。

バックアップ・カタログ

Oracle Secure Backupカタログは、管理サーバーに保存されます。このカタログには次のような、バックアップ・ドメインに関するあらゆる情報が保存されます。

- ホスト、デバイス、ユーザーなどに関する構成データ
- バックアップ・メタデータ
- ユーザー定義のバックアップ・スケジュール

- ・ テープ – 関連するバックアップ、複製、保存期間および場所

以上のリストから分かるように、バックアップ・カタログに含まれる情報は、管理ドメイン内のExalogicマシンのバックアップとリストアに非常に重要です。このカタログもバックアップする必要があります。この方法について詳しくは、『[Oracle Secure Backup管理者ガイド](#)』を参照してください。

Oracle Secure Backupの構成

Oracle Secure Backupの構成については、このドキュメントでは説明しません。Oracle Secure Backupの構成方法について詳しくは、[Oracle Secure Backupのドキュメント](#)を参照してください。

外部デバイスとExalogicマシンの接続

この項では、リモート・バックアップの実行用に、Exalogicマシンと外部デバイスを接続、構成する方法を説明します。次のいずれかのバックアップ・タイプを実行する場合は、外部デバイスを接続します。

- ・ リモートのZFSストレージ・デバイスへのバックアップ
- ・ ZFSを利用しない、リモート・ストレージ・アプライアンスへのバックアップ
- ・ リモート・テープへのバックアップ

リモート・ストレージ・アプライアンスとの接続

接続方法は、リモート・ストレージ・アプライアンスがサポートするネットワークの種類によって異なります。接続先がZFSストレージ・アプライアンスの場合はInfiniBandで接続できますが、リモート・ストレージ・アプライアンスがInfiniBandをサポートしていない場合は、使用できる最速のイーサネット接続で接続する必要があります。

図1 - ExalogicとZFSの接続

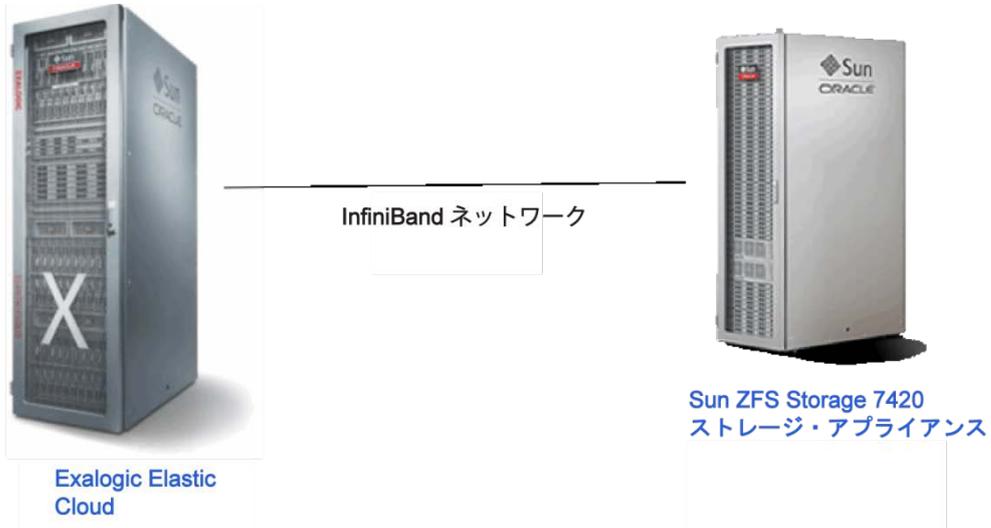
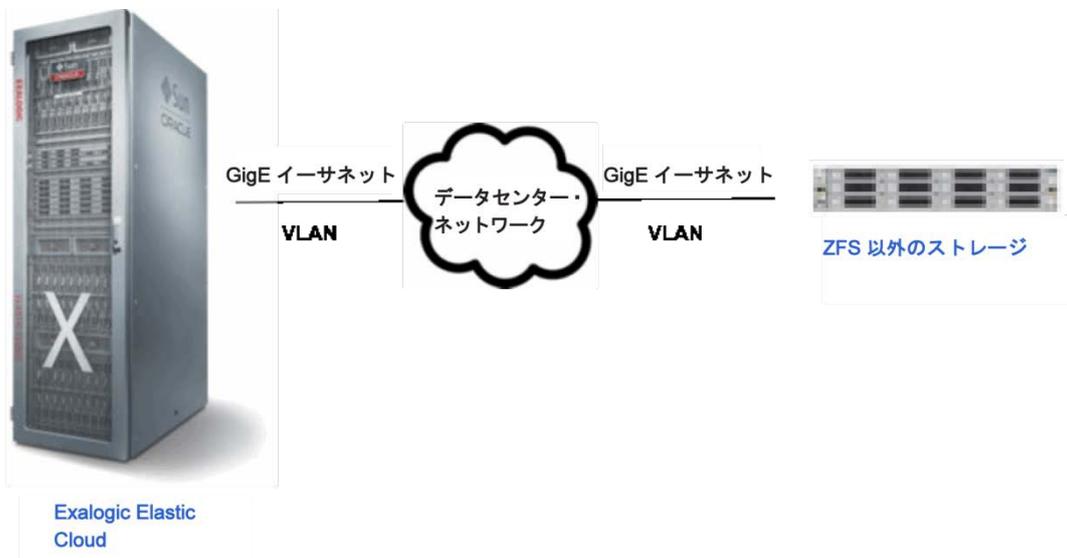


図2 - ExalogicとZFS以外のストレージの接続



- 図1は、既存のInfiniBandフレームワークを使用して、ZFSストレージ・アプライアンスとExalogicマシンを直接接続するリモート・ディスク・バックアップ・ソリューションを示しています。
- 図2は、イーサネットを使用して、ストレージ・アプライアンスとExalogicマシンを直接接続するリモート・ディスク・バックアップ・ソリューションを示しています。

注：リモートZFSアプライアンスをInfiniBandで接続することは必須ではありません。

InfiniBand経由でストレージ・アプライアンスを接続する場合、ストレージ・アプライアンスごとに、InfiniBand Quad Data Rate (QDR) ホスト・チャンネル・アダプタ (HCA) か、Exalogic InfiniBandネットワークに準拠した推奨されるデュアルポートのInfiniBand QDR HCAが必要です。InfiniBandでバックアップに使用されるネットワーク・プロトコルはIpoIBです。このプロトコルではホストのTCP/IPフレームワークが使用されるため、バックアップ・ソフトウェアに対して透過的です。

InfiniBandとギガビット・イーサネット・ネットワークのいずれを使用しても、バックアップ・ソフトウェアの動作は同じです。InfiniBand接続では、スパイン・スイッチではなくリーフ・スイッチを使用する必要があります。

テープ管理デバイスとの接続

図3 - ExalogicとStorageTekの接続

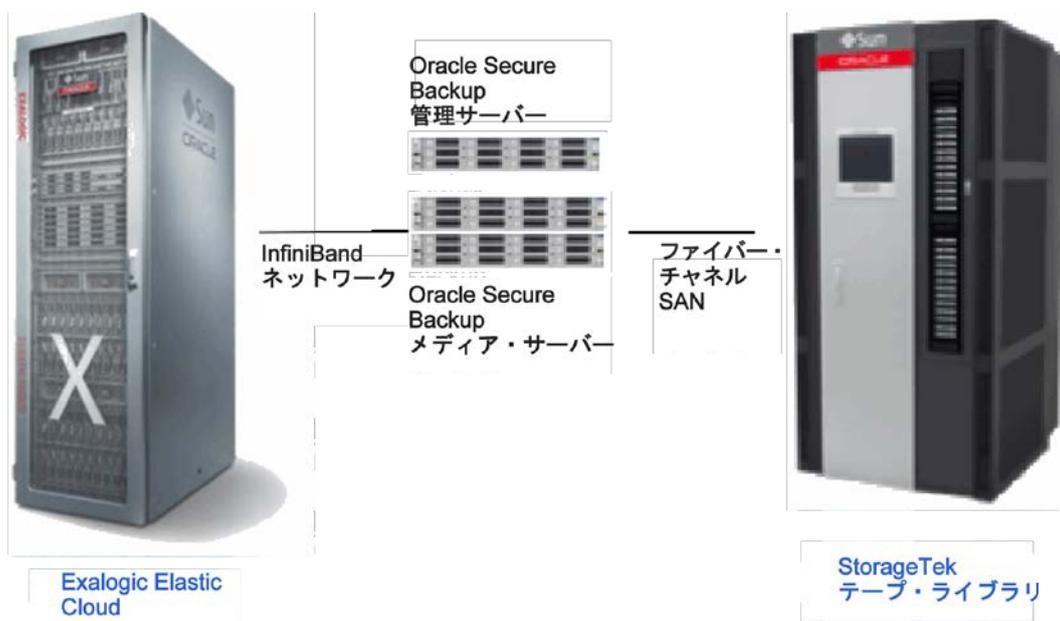


図4 - ExalogicおよびExadataとStorageTekの接続

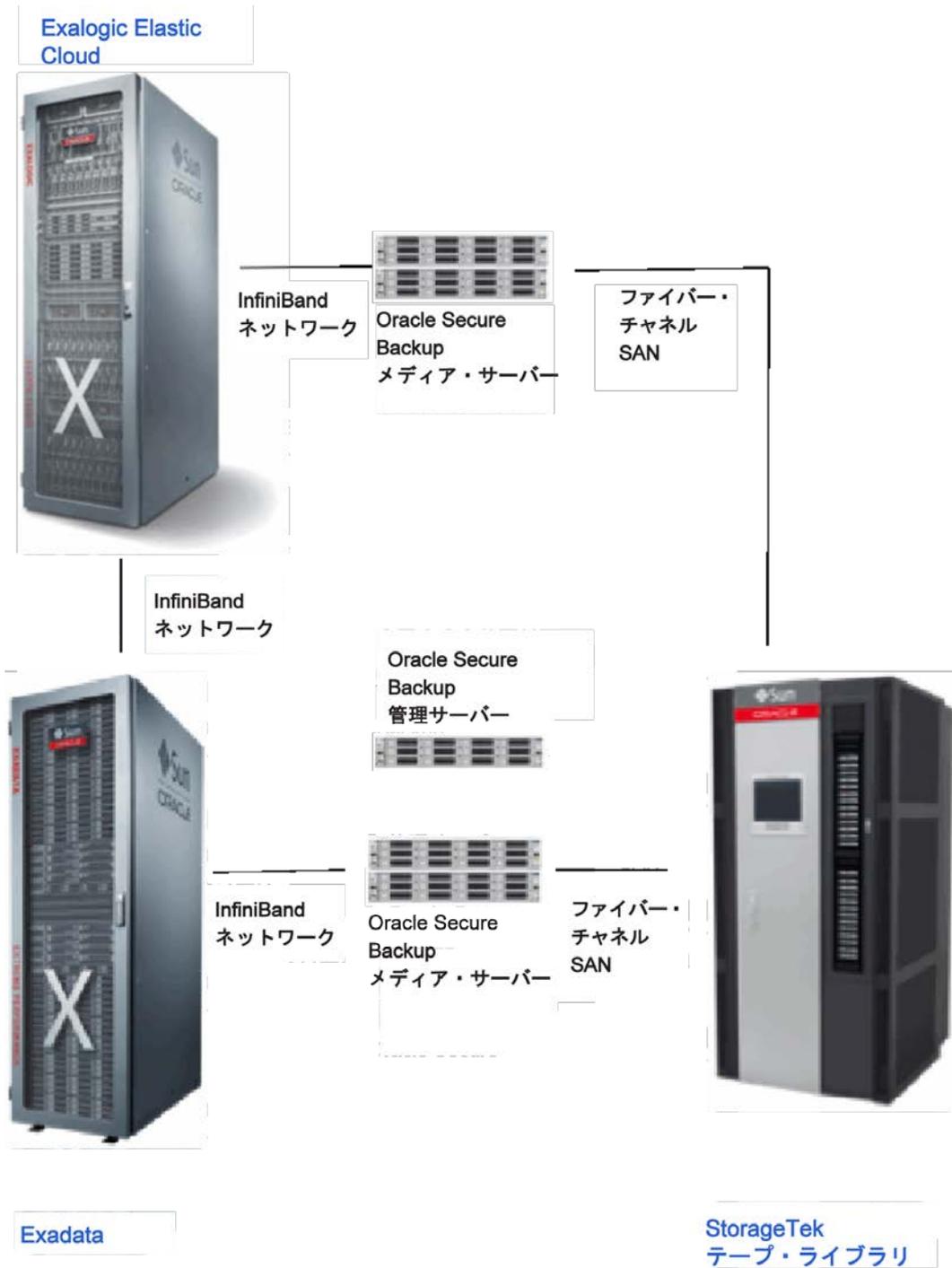
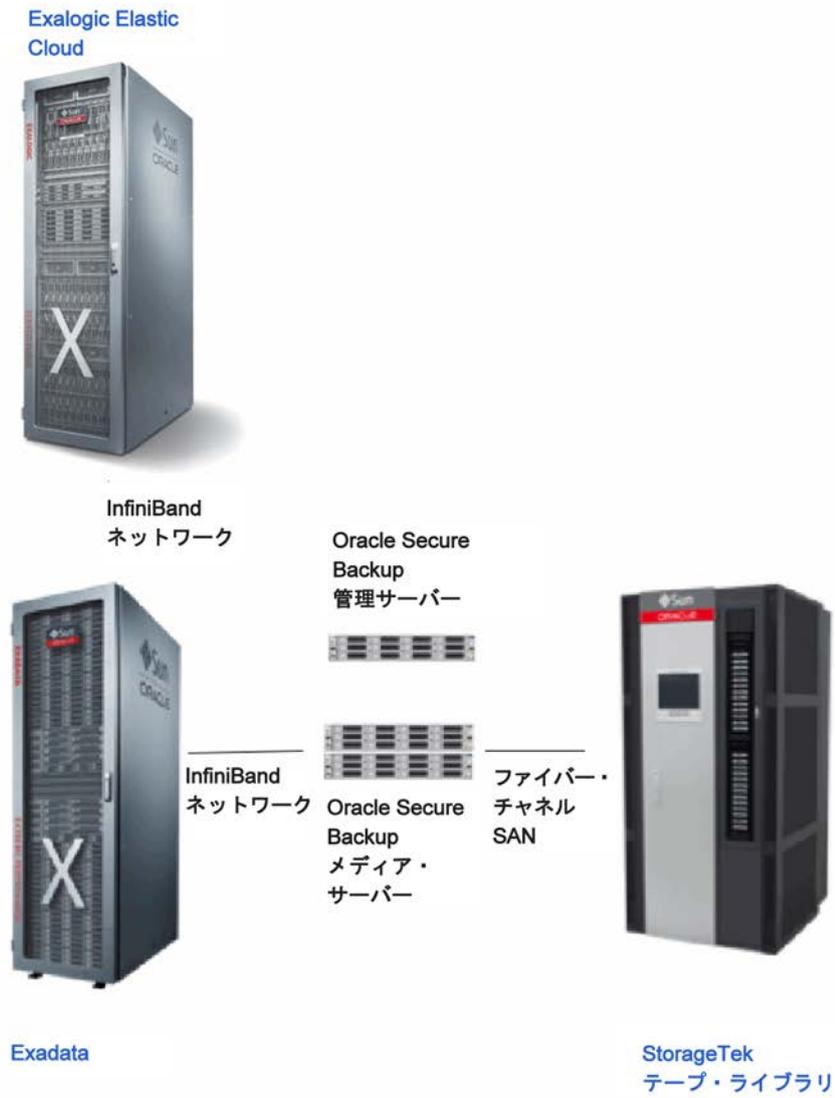


図5 - ExalogicとExadataの共有インフラストラクチャ



- 図3は、Exalogicマシンに直接接続されている2台または3台のメディア・サーバーによるテープ・バックアップ・ソリューションを示しています。
- 図4は、マシンごとに独自のOracle Secure Backupメディア・サーバー・セットがあるExalogicとExadataのハイブリッド・トポロジを示しています。
- 図5は、各マシンが同じメディア・サーバー・セットを共有しているExalogicとExadataのハイブリッド・トポロジを示しています。

それぞれのケースで、メディア・サーバーは、ExalogicおよびExadataマシンで使用可能なスペアのHAボンディング・ポートを使用して、既存のInfiniBandファブリックに接続されています。選択するソリューションは、バックアップ対象のデータのボリュームによって異なります。Exadataマシンのデータ以外のデータ量が少ない場合は、オプション3が最適です。

メディア・サーバーごとにInfiniBand QDR HCAが必要です。InfiniBand経由のバックアップで使用されるネットワーク・プロトコルはiPoBプロトコルであるため、データベース・サーバーとメディア・サーバー上のバックアップ・ソフトウェアから透過的に使用できます。InfiniBandとギガビット・イーサネット・ネットワークのいずれを使用しても、バックアップ・ソフトウェアの動作は同じです。

メディア・サーバーは、スパイン・スイッチではなくリーフ・スイッチに接続する必要があります。

メディア・サーバーがInfiniBandリーフ・スイッチに直接接続されている既存のExadataシステムに、Exalogicシステムを接続することはできますが、これは推奨しません。このメディア・サーバーをExalogic InfiniBandファブリックからセキュアに分離できないためです。このようなメディア・サーバーは、イーサネット経由で接続することを推奨します。

Oracle Secure Backupを使用する場合は、Oracle Secure Backupを次のような検証済みのハードウェア構成にインストールすることを推奨します。

- X2270 M2、X4170 M2、X4270 M2またはX4470 M2サーバー
- Sun InfiniBand QDRホスト・チャンネル・アダプタ : Exalogicシステム用と同じドライバ・バージョンのロー・プロファイル
- Oracle Linux UEK 64ビット、バージョン5 Update 5（以降）またはSolaris 11

データベース用にExalogicマシンとOracle Exadataマシンを組み合わせている場合、この2台のマシンで同じバックアップ・インフラストラクチャを共有できます。

バックアップ・ネットワークの作成

リモート・デバイス（ディスクやテープ）にバックアップする場合、専用のバックアップ・ネットワークを作成する必要があります。バックアップ・ネットワークを作成すると、バックアップ・トラフィックとユーザー・トラフィックを分けて、これら2つのトラフィックが競合しないようにすることができます。

リモート・ストレージ・アプライアンスへのリモート・ディスク・バックアップを実行する場合は、専用のバックアップ・ネットワークを作成して、クライアント・ネットワークでの競合を避けることを推奨します。リモートのZFSストレージ・サーバーにバックアップする場合、ストレージ・レプリケーション・チャンネルを作成すればクライアント・ネットワークでの競合を避けることができます。

ZFS以外のリモート・ストレージ・アプライアンスにバックアップする場合、Exalogicマシンとリモート・ストレージ・サーバーの間に専用のイーサネット・ネットワークを作成する必要があります。これは、InfiniBandではなくイーサネットでOracle Secure Backupメディア・サーバーとExalogicマシンを接続する場合も同じです。

ストレージ・レプリケーション・チャンネルの作成

ストレージ・レプリケーション・チャンネルは、特に、本番サイトとバックアップ・サイトのSun ZFS Storage 7320アプライアンス間のレプリケーション・トラフィック専用のネットワーク・チャンネルです。リモート・レプリケーションの構成前に、本番サイトとスタンバイ・サイトの両方で、ストレージ・レプリケーション・チャンネルを構成する必要があります。この項では、ストレージ・レプリケーション・チャンネルの構成手順を説明します。

前提条件

1. Exalogic マシンの両方のストレージ・ヘッドから、Exalogic マシン内に組み込まれた Cisco Catalyst 4948 スイッチにポート igb2 を接続します。
2. Exalogic マシンの両方のストレージ・ヘッドから、データセンターのネットワーク・ドロップにポート igb3 を接続します。これがデータセンターでの分散スイッチになります。
3. レプリケーション・チャンネルに割り当てる IP アドレスがプロビジョニングされており、DNS にあることを確認します。
4. 管理 IP サブネットとは別のサブネットで、レプリケーション・チャンネルの IP アドレスをプロビジョニングすることを推奨します。

ストレージ・レプリケーション・チャンネルの作成

次の手順に従って、ストレージ・レプリケーション・チャンネルを構成します。これらの手順はすべて、本番サイトとスタンバイ・サイトの両方で完了する必要があります。

1. ストレージ・ヘッドのブラウザ・ユーザー・インターフェース (BUI) を開きます。
2. 「**Configuration**」 → 「**Network**」 に移動し、Network 画面を表示します。
3. 組み込みデバイス igb2 と igb3 が接続されて、稼働していることを検証します。
4. これら 2 台のデバイスのデータリンクを作成します。
5. 最初のデータリンクを次の手順で作成します。表 Datalinks の横の「+」をクリックして、Network Datalink 画面を表示します。次の詳細を入力します。

Name : データリンクの名前を入力します。例 : **repl-1-dl**

Devicesで「igb2」を選択します。

その他のフィールドはすべて、デフォルト値のままにします。

「Apply」をクリックして、変更を適用します。

- 2番目のデータリンクを次の手順で作成します。表 Datalinks の横の「+」をクリックして、Network Datalink 画面を表示します。次の詳細を入力します。

Name : データリンクの名前を入力します。例 : **repl-2-dl**

Devicesで「igb3」を選択します。

その他のフィールドはすべて、デフォルト値のままにします。

「Apply」をクリックして、変更を適用します。

- 次に、手順 5 と 6 で作成した 2 つのデータリンクのインターフェースを作成します。
- 最初のインターフェースを次の手順で作成します。表 Interfaces の横の「+」をクリックして、Network Interfaces 画面を表示します。

次の詳細を入力します。

Name : インターフェースの名前を入力します。例 : **repl-1-interface**

Propertiesの「Allow Administration」の選択を解除します。

「Use IPv4 Protocol」を選択します。

Use IPv4 Protocolセクションで、次の手順を実行します。

- 「Static Address List」を選択します。
- IP Addressに、0.0.0.0/8と入力します。

Datalinksセクションで、「**repl-1-dl**」を選択します。

その他のフィールドはすべて、デフォルト値のままにします。

「Apply」をクリックして、変更を適用します。

- 2番目のインターフェースを次の手順で作成します。表 Interfaces の横の「+」をクリックして、Network Interfaces 画面を表示します。

次の詳細を入力します。

Name : インターフェースの名前を入力します。例 : **repl-2-interface**

Propertiesの「Allow Administration」の選択を解除します。

「Use IPv4 Protocol」を選択します。

Use IPv4 Protocolセクションで、次の手順を実行します。

- 「Static Address List」を選択します。
- IP Addressに、0.0.0.0/8と入力します。

Datalinksセクションで、「**repl-2-dl**」を選択します。

その他のフィールドはすべて、デフォルト値のままにします。

「Apply」をクリックして、変更を適用します。

10. 手順 8 と 9 で作成したインタフェース間に、アクティブ/パッシブのボンディング・インタフェースを作成します。このためには、IPMP グループ (IP マルチパス) を構成します。
11. IPMP グループを次の手順で作成します。表 Interfaces の横の「+」をクリックして、Network Interfaces 画面を表示します。

次の詳細を入力します。

Name : インタフェースの名前を入力します。例 : bak-repl-interface

「Allow Administration」の選択を解除します。

「Use IPv4 Protocol」を選択します。

Use IPv4 Protocolセクションで、次の手順を実行します。

- 「Static Address List」を選択します。
- 本番サイトのストレージ・レプリケーション・チャネル用にプロビジョニングしたIPアドレスを入力します。IPv4アドレス/マスクの形式を使用します。たとえば、10.204.77.120/24のようになります。この場合、10.204.77.120はIPアドレス、24はサブネット・ネットマスクです。
- この手順をスタンバイ・サイトで実行する場合は、スタンバイ・サイトのストレージ・レプリケーション・チャネル用にプロビジョニングしたIPアドレスを使用します。

「IP MultiPathing Group」を選択します。

インタフェースのリストから、手順9と10で作成したインタフェースを選択します。たとえば、**repl-1-interface**と**repl-2-interface**を選択します。

1つのインタフェースを**Active**に、もう1つのインタフェースを**Standby**に設定します。

「Apply」をクリックして、変更を適用します。

12. Network ページの「Apply」をクリックして、構成変更を適用します。
13. レプリケーション・インタフェースのルーティング表エントリを作成します。

「Configuration」 → 「Network」 → 「Routing」に移動します。

次の手順でRouting Table Entryを作成します。表Routing Table Entryの横の「+」をクリックして、Insert Route画面を表示します。

次の詳細を入力します。

- Family : 「IPv4」を選択します。
- Kind : **デフォルト**
- Gateway : レプリケーション・チャネルのIPアドレスのゲートウェイIPです。本番サイトとスタンバイ・サイトの適切なゲートウェイIPアドレスを使用します。
- Interface : 手順11で作成したIPMPグループを選択します。例 : **bak-repl- interface**
- 「Add」をクリックして、エントリを追加します。

14. どれか1つからレプリケーション・チャンネルのIPアドレスをpingして構成を検証します。

リモートのNFSサーバー/メディア・サーバーへのギガビット・イーサネット (GigEまたは10GigE) ネットワークの構成

メディア・サーバーとExalogicマシンをイーサネット経由で接続したり、Exalogicストレージ・アプリケーションとリモート・ディスク (ZFS以外) をイーサネット経由で接続したりする場合は、ストレージ・アプリケーションのGigEインタフェースの1つを使用して、データセンター・ネットワークに接続します。高可用性を実現するため、Exalogicストレージ・サーバーの複数のネットワーク・インタフェースと、リモートのNFSディスクやメディア・サーバーの複数のネットワーク・インタフェースをまとめてボンディングできます。この構成では、インタフェースをアクティブ/パッシブに構成します。

スループットが心配な場合は、各Exalogicストレージ・サーバーから、両方のGigEインタフェースをデータセンターの冗長ネットワークに直接接続します。これにより、2つのインタフェースが冗長かつ集約された形でボンディングされるため、スループットと冗長性が向上します。次のベスト・プラクティスに従います。

- ギガビットまたは10ギガビットのイーサネット・スイッチ構成を構成します。

スループットと可用性を最適化するには、ギガビット・スイッチにハードウェア・リンク・アグリゲーションを設定します。Link Aggregation Control Protocol (LACP) は、IEEE 802.1AX - 2008標準の一部として定義されています。また、ストレージ・サーバーとメディア・サーバーのオペレーティング・システムで使用できるその他のソフトウェア対応ボンディング・オプションを使用することもできます。

LACPを使用している場合、Src XOR Dst TCP/UDP Portのイーサネット・スイッチでLACPがサポートおよび構成されていることを確認します。送信元および宛先ポートのロードバランシング設定について、詳しくはベンダーのギガビット・スイッチのドキュメントを参照してください。

- メディア・サーバーのギガビットまたは10ギガビットのイーサネットを構成します。

次の推奨事項は、Oracle Enterprise Linux Version 5.3 (またはそれ以降) もしくはRed Hat Enterprise Linux Version 5.3 (またはそれ以降) を実行しているメディア・サーバーにのみ適用されます。メディア・サーバーで上記以外のオペレーティング・システムを使用している場合、適切なギガビット構成についてはベンダーに問い合わせてください。

ストレージ・サーバーのギガビット・イーサネット構成と同様に、メディア・サーバーに特別な変更を加える必要はありません。ただし、バックアップ速度を向上させるには、マルチポートのギガビットまたは10ギガビットのイーサネット構成を作成します。メディア・サーバーでボンディングを構成する手順は、データベース・サーバーの場合と同じです。詳細手順については、『Oracle Exadata Storage Server Software User's Guide』を参照してください。

InfiniBandネットワークの構成

Exalogicマシンには利用可能なInfiniBandポートがあるため、メディア・サーバーにInfiniBand Quad Data Rateのホスト・チャンネル・アダプタを追加すると、InfiniBandをサポートするメディア・サーバーやリモート・ストレージ・アプライアンスをInfiniBandファブリックに直接接続できます。高可用性を実現するには、HCAを2個の別々のExalogicマシンInfiniBandリーフ・スイッチに接続して、スイッチがシングル・ポイント障害にならないようにします。これにより、いずれかのポートへの接続が切断された場合、シームレスなフェイルオーバーが実行されます。

次のベスト・プラクティスに従います。

注：各項目に含まれる例は、Linuxオペレーティング・システムで実行されるメディア・サーバーに基づきます。InfiniBandをサポートしているストレージ・アプライアンスの場合は、ベンダーのドキュメントを参照してください。

- メディア・サーバーでInfiniBandインタフェースのボンディングを構成します。

次のボンディングib0とib1の例は、Linux環境固有のものです。

1. /etc/modprobe.confファイルを変更し、ファイルの最後に次の2行を追加します。これにより、ボンディング用のエイリアスとオプションが追加されます。

```
alias bondib0 bonding
options bonding max_bonds=10
```

注：メディア・サーバーで必要なボンディング・ネットワーク・インタフェースの数によっては、それに応じて、この値の調整が必要な場合があります。この例では、10の値を前提とします。

ファイルは次の例のようになります。このファイルから、事前にbond0に対してボンディングが設定されていたことが分かります。

```
alias ib0 ib_ipoib
alias ib1 ib_ipoib
alias bondeth0 bonding
alias bondib0 bonding
options bonding max_bonds=2
```

2. 以下のとおりに、/etc/sysconfig/network-scripts/ifcfg-bondib0ファイルを作成します。

```
DEVICE=bondib0
USERCTL=no
```

```
BOOTPROTO=none
ONBOOT=yes
IPADDR=<IP Address for bondib0 within the same subnet as the existing
InfiniBand network>
NETMASK=<Netmask must be the same as the existing InfiniBand network>
NETWORK=<Network calculated using ipcalc-n ip_address netmask>
BONDING_OPTS="mode=active-backup miimon=100
downndelay=5000 updelay=5000"
IPV6INIT=no
```

3. ib0とib1の現在の構成ファイルのコピーを作成します。コピーしたファイルの名前の先頭に、ifcfg-ib0が付かないようにします。backup-などの接頭辞を付け、-backupなどの接尾辞は付けません。たとえば、次のようになります。

```
cd /etc/sysconfig/network-scripts/
cp ifcfg-ib0 backup-ifcfg-ib0
cp ifcfg-ib1 backup-ifcfg-ib1
```

4. ib0とib1の現在の構成ファイルを変更し、これらがbondib0インタフェースのスレーブとして動作するよう設定します。ファイルは、次のようになります。

* ifcfg-ib0ファイル：

```
DEVICE=ib0
USERCTL=no
ONBOOT=yes
MASTER=bondib0
SLAVE=yes
HOTPLUG=no
BOOTPROTO=none
MTU=65520
```

* ifcfg-ib1ファイル：

```
DEVICE=ib1
```

```
USERCTL=no
ONBOOT=yes
MASTER=bondib0
SLAVE=yes
HOTPLUG=no
BOOTPROTO=none
MTU=65520
```

5. 必要に応じて、システム、ネットワーク・インタフェース、サービスを再起動します。
6. システムが再起動したら、rootユーザーとしてログインし、NICボンディングが正しく実行されていることを確認します。

```
# cat /proc/net/bonding/bondib0
```

```
Ethernet Channel Bonding Driver: v3.5.0 (November 4, 2008)
```

```
Bonding Mode: load balancing (round-robin)
```

```
MII Status: down
```

```
MII Polling Interval (ms):0
```

```
Up Delay (ms):0
```

```
Down Delay (ms):0
```

```
[root@adce01cn03 ~]# cat /proc/net/bonding/bond0
```

```
Ethernet Channel Bonding Driver: v3.5.0 (November 4, 2008)
```

```
Bonding Mode: fault-tolerance (active-backup) (fail_over_mac active)
```

```
Primary Slave:None
```

```
Currently Active Slave: ib1
```

```
MII Status: up
```

```
MII Polling Interval (ms):100
```

```
Up Delay (ms):5000
```

```
Down Delay (ms):5000
```

```
Slave Interface: ib0
```

```
MII Status: up
Link Failure Count:2
Permanent HW addr:80:00:00:4a:fe:80
```

```
Slave Interface: ib1
MII Status: up
Link Failure Count:0
Permanent HW addr:80:00:00:4b:fe:80
```

- メディア・サーバーでOpenFabrics Enterprise Distributionを更新します。
Exalogicマシンのバージョンと互換性のあるOpenFabrics Enterprise Distribution (OFED)バージョンを、メディア・サーバーで使用する必要があります。OFEDは、My Oracle Support Note 888828.1からダウンロードできます。
- 最高のパフォーマンスを出すには、InfiniBand IPoIB接続モードを構成します。
Exalogic 11g Release 2 (11.2.0.2) 以降を実行しているExalogicマシンのコンピュート・ノードを変更する必要はありません。ただし、カスタム構成の場合は、以下の設定を検証する必要があります。

次のコマンドは、Linuxオペレーティング・システムを前提とします。

1. 以下のとおり、Connectedモードがシステムで有効になっていることを確認します。

```
# cat /sys/class/net/ib0/mode
connected
# cat /sys/class/net/ib1/mode
connected
```

ステータスが“Datagram”の場合は、手順2と手順3に進みます。

2. /etc/ofed/openib.confファイルを編集してSET_IPOIB_CMを検索し、その値を変更して“yes”と指定します。

```
# Enable IPoIB Connected Mode
SET_IPOIB_CM=yes
IPOIB_LOAD=yes
```

3. サーバーを再起動し、手順1の方法に従って接続モードを再確認します。

- データ転送速度を上げるには、InfiniBandでMTUサイズを65520に構成します。

Exalogic 11g Release 2 (11.2.0.2) 以降のリリースを実行しているExalogicマシンのコンピュータ・ノードを変更する必要はありません。ただし、カスタム構成の場合は、以下の設定を検証する必要があります。

1. /etc/sysconfig/network-scripts/ifcfg-ib* と /etc/sysconfig/network-scripts/ifcfg-bondib0のファイルを編集し、MTU=65520のエントリを追加します。例：

```
MTU=65520
```

2. 次のように、MTUサイズが65520になっていることを確認します。

```
# ifconfig ib0 | grep MTU
```

```
UP BROADCAST RUNNING SLAVE MULTICAST MTU:65520 Metric:1
```

```
# ifconfig ib1 | grep MTU
```

```
UP BROADCAST RUNNING SLAVE MULTICAST MTU:65520 Metric:1
```

```
# ifconfig bondib0 | grep MTU
```

```
UP BROADCAST RUNNING MASTER MULTICAST MTU:65520 Metric:1
```

3. サーバーを再起動し、手順1の方法に従ってMTUサイズを再確認します。

- InfiniBandネットワークを使用できるようにメディア・サーバーを構成します。

バックアップとリストアのトラフィックをInfiniBandファブリックに流すには、メディア管理ソフトウェアをInfiniBand用に構成します。メディア管理ソフトウェアのタイプごとに、この構成を有効にする独自のメソッドがあります。

たとえば、Oracle Secure Backupには優先ネットワーク・インタフェースの概念があり、特定のクライアント・リストのメディア・サーバーに設定できます。他のメディア管理ソフトウェアでは、ソフトウェアをインストールする際に、この構成を定義する必要があります。特定のネットワーク経由でトラフィックを送信する方法について、詳しくはご使用のメディア管理ソフトウェアを確認してください。

テープ・デバイスの固定バインディングの構成

SAN環境では、永続バインディングを構成してデバイス・アドレスが変更されないようにする必要があります。デバイス・アドレスが変更されると、Oracle Secure Backup内でデバイス構成を更新しない限り、メディア・サーバーはそのデバイスにアクセスできません。そのため、環境で一貫したデバイス・アドレスを保持することが非常に重要です。

永続バインディングはOracle Secure Backup内では構成されませんが、インフラストラクチャ設定の一部です。HBAやオペレーティング・システム経由で永続バインディングを構成できます。構成手順は、プラットフォームやベンダーによって異なる場合があります。デバイス接続の永続バインディングの作成例については、My Oracle Support Note 971386.1を参照してください。

VLANを使用した外部デバイスの接続

既存のデータセンター・ネットワークを使用してリモート・バックアップ・デバイスを接続している場合は、データセンター・ネットワーク内の既存システムへ接続する際に仮想LAN (VLAN) の使用が必要になる場合があります。Exalogicシステムは、ネットワークで802.1Q標準のVLAN実装をサポートしています。次のいくつかの項では、Exalogic内の各種コンポーネントでこのような構成を行う方法について、必要な情報を提供します。詳細情報については、各コンポーネントのドキュメントも参照してください。

Exalogicコンピュート・ノードからの、VLANベースのネットワーク・インタフェースの作成

Exalogicコンピュート・ノードには、2種類のネットワーク・インタフェースがあります。

- a) 4個の1Gbpsイーサネット・ポート
- b) 2個のInfiniBandポート

ネットワーク全体の設計とアーキテクチャによって、これらのいずれかを使用して外部システムに接続し、VLANを使ってバックアップとリカバリを実行できます。分かりやすくするため、この項は2つの部分に分かれています。

スタンドアロンの1GbEネットワーク・インタフェースでの手動によるVLAN構成

管理ネットワーク用に、4個の1Gbpsイーサネット・ポートのうち1個以上が内部のCiscoスイッチに配線済みです。残りのいずれかのポートを使用して、ギガビット・ネットワーク経由でコンピュート・ノードに直接アクセスできます。Linuxでは、次の手順でVLANタグのインタフェースを作成できます。

1. 必要なカーネル・モジュールをロードします。

```
# modprobe 8021q
```
2. このモジュールがロードされていることを確認します。

```
# lsmod | grep 8021q
```
3. VLANタグをインタフェースに追加します。たとえば、VLAN 25をeth3に追加します。

```
# vconfig add eth3 25
```
4. VLANがインタフェースに追加されたことを確認します。

```
# cat /proc/net/vlan/config
```

VLANタグが付けられたインタフェースにIPアドレスを割り当てます。このインタフェースは、Linuxで[Interface_Name]:[Vlan_Tag]と表示されます。

```
# ifconfig eth3.25 <ip address> <subnet mask> up
```

再起動後もこの構成を永続的にするには、Linuxの他のインタフェースと同様にスクリプトを作成する必要があります。

```
/etc/sysconfig/network-scripts/ifcfg-eth3.25
```

VLANベースのインタフェース・スクリプトの2つの固有パラメータを必ず更新します。

```
DEVICE=eth3.25 # This means the device is eth3 with VLAN ID 25
```

```
VLAN=yes
```

Linuxボンディング・インタフェース経由でのVLAN構成

高可用性を実現するには、VLANで1組の物理ボンディング・インタフェースを使用できます。まず、2つ以上の物理インタフェースを使用してボンディング・インタフェースを作成してから、そのボンディング・インタフェースにVLANタグを割り当てることを推奨します。たとえば、eth2とeth3からbond3を作成してから、VLANタグをbond3に割り当てます。次のようになります。

まず、2つのインタフェース（eth2とeth3）を選択し、アクティブなスタンバイのLinuxボンディング構成で準備します。次の内容で、/etc/sysconfig/network-scripts/にifcfg-eth2とifcfg-eth3を作成します。

```
DEVICE=<device name># Use eth2 and eth3 respectively in each
ifcfg- file

BOOTPROTO=none

HWADDR=<device' mac address> # Use corresponding MAC address
here

TYPE=Ethernet

ONBOOT=yes

# Settings for Bond

MASTER=bond3

SLAVE=yes
```

次の内容で、/etc/sysconfig/network-scripts/にifcfg-bond3.25を作成します。

```
DEVICE=bond3.25

IPADDR=<IP address>

NETMASK=<Subnet Mask>

GATEWAY=<Gateway>

USERCTL=no

BOOTPROTO=none
```

```
ONBOOT=yes
```

```
VLAN=yes
```

次のコマンドで、2つの物理インタフェースと、関連付けたbond3.25インタフェースを表示します。

```
# ifup bond3.25
```

VLANタグの付いたボンディング・インタフェースのステータスは次のようになります。

```
# ifconfig eth2
```

```
# ifconfig eth3
```

```
# ifconfig bond3.25
```

```
# cat /proc/net/vlan/config
```

```
# cat /proc/net/bonding/bond3
```

バックアップとリカバリにおけるInfiniBandネットワークの使用

ここでは、データセンター・ネットワーク間のバックアップとリカバリにおける、InfiniBandポートとその使用方法を説明します。InfiniBandには、OSIレイヤード・モデルで使用できる2種類のネットワーク・インタフェースがあります。

a) IP over InfiniBand (IPoIB)

b) Ethernet over InfiniBand (EoIB)

バックアップとリカバリにIPoIBネットワークを使用することは推奨しません。これらのネットワークは、ローカルLANのみに限定されるためです。EoIBは、バックアップとリカバリに使用できます。

まず、NM2GWスイッチでEoIBネットワーク・インタフェースを作成する必要があります。詳しくは、ExalogicやNM2GWのユーザー・ガイドを参照してください。要約すると、NM2GWで次のコマンドを実行すると、EoIBインタフェースが作成されます。これらのインタフェースは、仮想NICまたはVNICとも呼ばれます。

```
# createvnic <GW ETH port> -guid <Host_port_guid> -mac  
<assigned_mac> [-vlan <vlan_tag> -pkey <partiton_key>]
```

ここで、VNICの作成中にVLANタグの割当てが可能なが分かります。この操作を実行すると、コンピュータ・ノードのLinux環境でインタフェースがインスタンス化されます。これで、IPアドレスを割り当てられます。

ホストで使用できるVNICを確認します

```
# mlx4_vnic_info -l
```

IPアドレスを割り当てます

```
# ifconfig <vnic> <IP_address> <subnet_mask> up
```

再起動後にこのようなVNICを再構成するには、起動スクリプトを作成する必要があります。ifcfgの各起動スクリプトにVNICのMACアドレスを含めることは非常に重要です。詳しくは、Exalogicのユーザー・ガイドを参照してください。

Exalogic ZFSストレージ・アプライアンスからのVLANベースのネットワーク・インタフェースの作成

Exalogic内のストレージ・マシン（ZFSSA）には、外部接続に使用できる2つのインタフェースがあります。VLANタグは、ブラウザ・ユーザー・インタフェースまたはコマンドライン構成で実装できます。詳しくは、Oracle ZFS 7320のユーザー・ガイドを参照してください。

ブラウザ・ユーザー・インタフェースからのVLANタグ付きのネットワーク・インタフェースの構成

1. ブラウザを起動してBUIにアクセスします。
2. 「**Configuration**」 → 「**Network**」 に移動します。
3. 使用予定のネットワーク・デバイスにアクティブ・リンクがあることを確認します。タイトル“Devices”の最初の列を確認します。
4. Datalinksの近くの「+」をクリックすると、インタフェース構成用の小さいポップアップ・ウィンドウが表示されます。
5. 使用予定のデバイスの名前を入力します。デバイスと同じ名前（igb2など）を使用することを推奨します。すべてのチェック・ボックスをオフのままにします。リストからデバイスを選択し、「Apply」をクリックします。
6. 高可用性のためにペアを使用予定の場合は、以上の手順をもう一度繰り返して、別のデータリンクを作成します。たとえば、igb3を選択します。

ここで、作成したデータリンクにVLANタグを追加できます。

7. Datalinksの近くの「+」を再度クリックして、同じポップアップ・ウィンドウを表示して構成します。
8. 「VLAN」 オプションをオンにします。
9. VLANタグの付いたデータリンクに、igb2-25やigb3-25などの名前を割り当てます。
10. VLANテキスト・ボックスに、使用するVLAN IDを入力します。
11. 下のリストからインタフェース・データリンクを選択し、「Apply」をクリックします。
12. メイン・ウィンドウの「Apply」をクリックし、データリンクの変更をコミットします。
13. メイン・ブラウザ・ウィンドウで、Interfacesの近くの「+」をクリックし、IPアドレスとIPMP構成を追加します。
14. インタフェースに、igb2-25-Aやigb3-25-Bなどの名前を割り当てます。
15. IPv4セクションで、IPアドレス0.0.0.0/8を割り当てます。

16. 以前に作成した、igb2-25やigb3-25などのデータリンクを選択します。
17. Propertiesセクションの両方のチェック・ボックスがオンになっており、管理が有効で可能であることを確認します。
18. 「Apply」をクリックして保存します。
19. 高可用性を構成している場合は、手順を繰り返して別のインタフェースを作成します。
20. Interfacesの近くの「+」を再度クリックし、IPMPベースのインタフェースを作成します。
21. igb2-3-25-ipmpなどの名前を割り当てます。
22. このネットワークで使用予定のIPアドレス、たとえば10.23.12.54/22を入力します。
23. 「IP MultiPathing Group」をオンにします。
24. 前の手順で作成した2つのインタフェースを選択し、「Apply」をクリックします。
25. いずれかのインタフェースで「Standby」を選択し、アクティブなスタンバイ構成を作成します。
26. メイン・ページで「Apply」をクリックし、すべての変更を確認します。

Exalogicディスクの構成

このホワイト・ペーパー用に、次の点を除き、『Oracle Fusion Middleware Exalogicエンタープライズ・デプロイメント・ガイド』に従って、Exalogicマシンを設定しています。

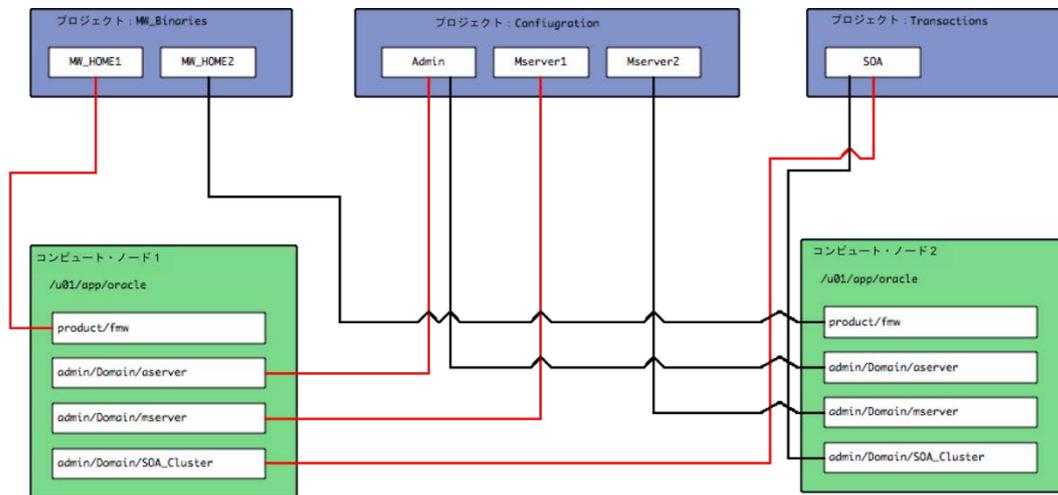
ディスクのレイアウト

プロジェクト

上記の変更度グループを反映するストレージ領域を作成するには、『Oracle Fusion Middleware Exalogicエンタープライズ・デプロイメント・ガイド』に記載されているプロジェクトのほか、次のプロジェクトを定義する必要があります。

これらのプロジェクトの作成方法については、『Oracle Fusion Middleware Exalogicエンタープライズ・デプロイメント・ガイド』を参照してください。

たとえば、Oracle Fusion Middlewareのエンタープライズ・デプロイメント・ガイドの1つに基づいてFusion Middlewareデプロイメントを作成していた場合、以下のように作成することが必要な場合があります。



このために、次のプロジェクトを作成します。

プロジェクト名: MW BINARIES

プロパティ名:	値	コメント
Quota	100GB	スナップショットを含むプロジェクトの割当て制限。割当て制限は、要件に基づいて割り当てる必要があります。
Mount Point	/export/product/	
その他すべての設定	デフォルト	
Share Name	mw_home1	マウント・ポイント、/export/product/fmwを共有 apphost1に/u01/app/oracle/productとしてマウントされます。
Share Name	mw_home2	マウント・ポイント、/export/product/fmwを共有 apphost2に/u01/app/oracle/productとしてマウントされます。

プロジェクト名: CONFIGURATION

プロパティ名	値	コメント
Quota	500GB	スナップショットを含むプロジェクトの割当て制限。割当て制限は、要件に基づいて割り当てる必要があります。
Mount Point	/export/config	
その他すべての設定	デフォルト	
Share Name	aserver	apphost1とapphost2に/u01/app/oracle/admin/IDMDomain/aserverとしてマウントされます。 管理サーバーのドメイン構成が含まれます。
Share Name	mserver_host	WebLogicサーバーを実行するコンピュータ・ノードあたり1つ。 各アプリケーション・サーバーに、/u01/app/oracle/admin/DomainName/mserverとしてマウントされます。 管理対象サーバーのドメイン構成が含まれます。 例: /export/config/mserver_apphost1は、/u01/app/oracle/admin/DomainName/mserverとしてapphost1にマウントされ、export/config/mserver_apphost2は、/u01/app/oracle/admin/domainname/mserverとしてapphost2にマウントされます。
Share Name	oinstance_host	Oracle HTTP Server、Oracle Internet Directory、Oracle Virtual DirectoryなどのOracle_instanceを使用する製品を実行するコンピュータ・ノードごとに1つ。 /u01/app/oracle/admin/Instance_nameとして、各アプリケーション・サーバーにマウントされます。 管理対象サーバーのドメイン構成が含まれます。

プロジェクト名：TRANSACTIONS

プロパティ名	値	コメント
Quota	200GB	スナップショットを含むプロジェクトの割当て制限。割当て制限は、要件に基づいて割り当てる必要があります。
Mount Point	/export/txn	
その他すべての設定	デフォルト	
Share Name	soa	マウント・ポイント、/export/txn/soaを共有 /u01/app/oracle/admin/soa_clusterにマウントされるapphost1、apphost2にマウントされます。 JMSの共有場所 ディレクトリはドメインのクラスタごとに作成され、JMSとトランザクション・ログの永続ストアのサブディレクトリが含まれます。

スナップショットの可視性

ディスク・スナップショットの使用を予定しており、個々のファイルの抽出やテープへのスナップショットのバックアップのためにスナップショットに直接アクセスしたい場合は、プロジェクト・スナップショットを可視化する必要があります。これを行うには、次の手順を実行します。

1. BUIにログインします。
2. 「Shares」をクリックします。
3. 「Projects」をクリックします。
4. Projectを編集します。
5. 「Snapshots」を選択します。
6. .zfs/snapshotの可視性をVisibleに設定します。

バックアップの実行

この項では、所定のコンピュート・ノードからバックアップを取る方法を説明します。Exalogicマシン全体をバックアップする場合、コンピュート・ノードごとにバックアップする必要があります。各コンピュート・ノードでの手順は同じです。

ほとんどの操作は、ZFSストレージ・アプライアンス、ブラウザ・ユーザー・インタフェース (BUI) 、またはコマンドライン・ユーティリティを使用して実行できます。簡潔にするため、このドキュメントではBUIのみを使用します。

ディスク・バックアップ

スナップショット

自動スナップショットのスケジューリング

スナップショットは、GUIまたはコマンドライン経由でスケジューリングできます。

http://storagenode:215/にアクセスして、ストレージ・ヘッドのブラウザ・ユーザー・インタフェース (BUI) を開きます。

1. 「Share」 をクリックします。
2. 「Disk Schedules」 をクリックします。
3. 「+」 をクリックします。
4. 以下の情報を入力します。

スケジュール情報

プロパティ名	値
Frequency	half hour、hour、day、weekまたはmonthから選択します。
Offset	スナップショットを取る時刻を指定します (Sunday at 02:00hrsなど)。
Keep at most	これは保存方針です。保存するスナップショットのコピー数を選択します。増分スナップショット・ポリシーを作成すると、スナップショットは、そのスナップショットに依存するすべてのスナップショットが廃止されるまで削除されません。

非定型の作成

1. スナップショットは、次の手順でBUIから作成できます。
2. 「Snapshots」 をクリックします。
3. スナップショットのリストが表示されたら、「+」を選択します。
4. 詳細を入力して、「Apply」 をクリックします。

OSのdumpコマンドを使用したバックアップ

ダンプによってext2ファイル・システム上のファイルが調べられ、バックアップが必要なファイルが決められます。これらのファイルが所定のディスク、テープ、またはその他のストレージ・メディアにコピーされ、安全に保存されます。出力メディアより大きいダンプは、複数のボリュームに分けられます。ほとんどのメディアでは、メディア終端の指示が返されるまで書き込むことで、サイズが決定されます。

dumpコマンドの例は次のとおりです。

```
dump -f mybackupfile filesystems_to_be_backed_up
```

dumpコマンドによってレベル化されたバックアップを実行できます。-fスイッチで提供されるファイルは、リモート・ディスクにある可能性があります。

dumpコマンドの使用可能なオプションや使用方法について詳しくは、オペレーティング・システムのドキュメントを参照してください。

リモート・ディスクへのバックアップ

ZFSサーバー

ZFSボリュームは、オンデマンドまたはディザスタ・リカバリ戦略の一部として、リモート・ディスク・アレイに複製できます。この操作は、暗黙のスナップショットの作成によって実行できます。

バックアップ/リカバリのユースケースでは、通常リモート・ストレージがデータセンターにあり、DRのユースケースでは、リモート・ストレージがリモート・データセンターにあります。ディザスタ・リカバリ戦略の設定方法について詳しくは、ホワイト・ペーパー

『[Disaster Recovery for Oracle Exalogic Elastic Cloud](#)』を参照してください。

リモートのZFSアプライアンスにスナップショットを複製するには、次の手順を実行する必要があります。

1. <https://storageappliance:215/>のURLを使用して、BUIにログインします。
2. ソース・サーバーとターゲット・サーバーの両方で、レプリケーション・サービスが有効であることを確認します。
 - i. 「Configuration」 → 「Services」 を選択します。
 - ii. リモート・レプリケーション・サービスのステータスが有効でない場合は、「Enable Service」 ボタンをクリックします。
3. レプリケーション・ターゲットを作成します。
 - i. 「Configuration」 → 「Services」 から 「Remote Replication」 をクリックします。
 - ii. 「Add Target」 をクリックします。
 - iii. 次の情報を入力します。

Name : このターゲットの名前

Host Name : ターゲットのZFSサーバーのホスト名またはIPアドレス

Root Password : ターゲット・サーバーのrootパスワード

データセンターでレプリケーションを実行する場合は、SSLを無効にしてパフォーマンスを向上させることができます。
 - iv. 「Add」 をクリックします。
4. 複製するプロジェクトを選択します。
 - i. 「Shares」 → 「Projects」 サブタブをクリックします。
 - ii. 複製するプロジェクトを選択して、「Edit Entry」 をクリックします。
 - iii. 「Replication」 タブをクリックします。
 - iv. 「Add」 をクリックします。
 - v. 次の情報を入力します。

Target - ドロップダウン・リストから、上で作成したターゲットを選択します。

「enabled」 を選択します。

手動または選択した時間隔でモードを選択します。

5. これで、事前定義した時間隔または手動でレプリケーションをスケジュールできます。自動的にスケジュールするには、スケジュールの横の「Add Entry」をクリックします（随時バックアップする場合は、スケジュールを作成しないでください）。

次の情報を入力します。

Frequency：リモート・バックアップを取る頻度です。

Mins past the hour：毎時何分にバックアップを取るかを設定します。

6. 「Add」をクリックします。
7. 「Update Now」をクリックして、レプリケーションが機能することを確認します。バックアップを実行すると、最後のSyncフィールドが移入されます。
8. 次の手順を実行して、リモート・サーバーでバックアップが実行されたことを検証します。

- i. <https://storageappliance:215/>のURLを使用して、BUIにログインします。
- ii. 「Shares」をクリックします。
- iii. 「Project」をクリックします。
- iv. 「Replica」のサブタブをクリックします。
- v. 先程実行したバックアップが表示されます。
- vi. リモートのZFSアプライアンスにバックアップがあるため、そのアプライアンスにアクセスできるホストにバックアップをマウントして、検証やテープへのバックアップを実行できます。このために、リモート・マシンで次の操作を実行します。

<https://storageappliance:215/>のURLを使用して、GUIにログインします。

「Shares」をクリックします。

「Replica」のサブタブをクリックします。

バックアップを選択して、「Edit Entry」をクリックします。

「Inherit from Project」の選択を解除します。

「Export」をクリックします。

マウント・ポイントを選択します。

「Apply」をクリックします。

次のようなfstabエントリを使用して、バックアップ・ホストにファイル・システムをマウントします。

```
storagehost:/export/product/fmw /u01/app/oracle/product nfs4
rw,bg,hard,nointr,rsize=131072,wsiz=131072
```

- vii. テープ・バックアップの項で説明した方法で、テープにバックアップします。

ZFS以外のサーバー

ZFSを実行していないリモート・ディスク・アレイに、リモートでデータをバックアップするには、次の手順を実行します。

- GigE、10GigEまたはInfiniBandのインターフェースを使用して、IPベースのプロトコル経由でExalogicマシンに接続されているNASアプライアンスを使用します。
- NASアプライアンスを使用できない場合は、NFSまたはiSCSIを使用して、そのアプライアンスを設定する必要があります。イーサネット経由で、SANやファイバー・チャンネルに直接接続することはできません。NFS経由で接続する場合、バックアップ対象のデータのボリュームによっては、パフォーマンスの問題が発生する可能性があります。
- Exalogicマシンにリモート・ディスク・アレイを接続したら、これをファイル・システムとしてマウントし、オペレーティング・システムのコマンド（tarやdumpなど）、またはベンダーに依存しないその他のファイル・コピー・ユーティリティを使用して、このファイル・システムに直接バックアップします。

テープ・バックアップ

次の例はOracle Secure Backupに基づきますが、プリンシパルは任意のメディア管理製品に引き継ぐことができます。Oracle Secure Backup内でスナップショットをバックアップすることはできませんが、Oracle Fusion Middlewareのインストールにおけるデータ・ボリュームは大きくないので、標準的なファイル・システム・バックアップを推奨します。これで、必要に応じて個々のファイルをリストアできます。

このホワイト・ペーパーでは、Exalogicマシンのバックアップの実行に必要なタスクに関連する場合を除き、Oracle Secure Backupのインストールと構成の方法は説明しません。たとえばこのホワイト・ペーパーには、すべて完了している必要がある次のタスクは含まれません。

- Oracle Secure Backupのインストール。
- 管理サーバー、メディア・サーバー、テープ・デバイスなどのOracle Secure Backupドメインの構成。
- メディア・ファミリ、テープの複製やボールティングなどのメディア・ライフ・サイクル・ポリシー。

ファイル・システムのバックアップには、おもに次の6つの構成要素があります。

- Oracle Secure Backupクライアント・ホスト
- メディア・ファミリ
- バックアップ・ウィンドウ
- データセット
- バックアップのスケジュールとトリガー
- バックアップのトリガー

以下に詳細を説明します。

Oracle Secure Backupクライアント・ホスト

ホストによって、次の2つのうちいずれかの方法でOracle Secure Backupホストをバックアップできます。

- 1) ホストにOracle Secure Backupをインストールして、ローカル・ファイル・システムのバックアップを実行する従来のバックアップ操作（obアクセス・モード）
- 2) ホストにOracle Secure Backupをインストールせず、代わりにNDMPのバックアップ/リストアを使用するNetwork Attached Storage（NAS）のNDMPバックアップ（NDMPアクセス・モード）

どちらの方法でも、Oracle Secure Backupドメイン内でホストを構成する必要があります。

Oracle Secure Backupクライアント

これを行うには、次の手順を実行します。

1. <https://osbadminserver/>のURLを使用して、Oracle Secure Backup GUIにログインします。
2. 「Configure」タブをクリックします。
3. 「Hosts」タブをクリックします。
4. 「Add」をクリックします。
5. 以下の情報を入力します。
 - Host：ホストの名前。
 - ホストのIPインターフェース名、DNS名またはIPアドレス（バックアップ・ネットワークを定義済みの場合は、このネットワーク上のホストのDNS名/IPアドレスになります）。
 - Roles：クライアント
 - Access Method：ob
 - その他の値は、すべてデフォルトのままにすることも、環境の構成に合わせて変更することもできます。
6. 「OK」をクリックします。

NDMPクライアント

これを行うには、次の手順を実行します。

1. <https://osbadminserver/>のURLを使用してOracle Secure Backup GUIにログインします。
2. 「Configure」タブをクリックします。
3. 「Hosts」タブをクリックします。
4. 「Add」をクリックします。
5. 以下の情報を入力します。

- Host : ホストの名前。
- ストレージ・ホストのIPインタフェース名、DNS名またはIPアドレス (バックアップ・ネットワークを定義済みの場合は、このネットワーク上のストレージ・ホストのDNS名/IPアドレスになります)。
- Roles : クライアント
- Access Method : NDMP
- User Name / Password : ストレージ・アプライアンスのNDMPサービス設定で定義したDMAユーザー名とパスワード。
- Backup Type : 実行するバックアップの種類。オプションはzfs、tar、またはdumpです。
- その他の値は、すべてデフォルトのままにすることも、環境の構成に合わせて変更することもできます。

6. 「OK」をクリックします。

メディア・ファミリ

メディア・ファミリとは、共通の属性（保存期間など）を共有するボリュームの論理的な分類です。変更度グループごとにボリューム・グループを作成したい場合もあるでしょう。

Oracle Secure Backupでメディア・ファミリを定義するには、次の手順を実行します。

- <https://osbadmserver/>のURLを使用して、Oracle Secure Backup GUIにログインします。
- 「Configure」タブをクリックします。
- 「Add」をクリックします。
- 以下の情報を入力します。
- Name : メディア・ファミリの識別名。
- Volume Expiration : 有効期限ポリシーを選択します。たとえばバックアップを7日間保存したい場合は、Time Managed and Keep volumeで7 daysを選択します。
- インストールに関連するその他の値を選択して、「OK」をクリックします。

バックアップ・ウィンドウ

バックアップ・ウィンドウでは、Oracle Secure Backupでスケジューリングされたバックアップ・ジョブを実行する時間の範囲を定義します。

たとえば、バックアップ・ウィンドウは、18:00 – 08:30のようになります。

Oracle Secure Backupでバックアップ・ウィンドウを定義するには、次の手順を実行します。

- <https://osbadmserver/>のURLを使用して、Oracle Secure Backup GUIにログインします。
- 「Configure」タブをクリックします。
- 「Backup Windows」をクリックします。

- 「Add」をクリックします。
- バックアップ・ウィンドウの種類（Dayの範囲またはDate）を選択します。定期的なバックアップの場合はDayを選択する必要があります。
- Dayの範囲を選択した場合は、バックアップ・ウィンドウを適用する日を選択します。オプションは次のとおりです。

Daily – 毎日

Weekdays – 月曜日から金曜日

Weekend – 土曜日と日曜日

- 時間フィールドのLocal Time Rangeを入力します。時刻は24時間形式で表示されます。
- 「OK」をクリックして、バックアップ・ウィンドウを作成します。

このドキュメント用に、2時～6時のDailyバックアップ・ウィンドウを作成します。

データセット

データセットによって、バックアップ対象のファイルが決定されます。これは、軽量のテキスト言語を使用して実行されます。

データセットは、次のように定義できます。

Inclusions：バックアップに含めるファイル/ディレクトリ

Exclusions：バックアップ中に省略するファイル/ディレクトリ

または、上記2つの組合せです。

次のデータセットが定義されます。

名前	INCLUSIONS	EXCLUSIONS
オペレーティング・システム	/	/u01/app/oracle/product/fmw /u01/app/oracle/admin /u01/app/oracle/txn
バイナリ	/u01/app/oracle/product/fmw	
構成	/u01/app/oracle/admin	
トランザクション	/u01/app/oracle/txn	

Oracle Secure Backupでデータセットを作成するには、データセット・ファイルを作成します。データセット・ファイルは、1台または複数台のコンピュータ・ノードで使用できます。

通常は、バックアップ対象のホストごとに1つのデータセット・ファイルを作成します。必要に応じて、ホストと変更度グループの組合せごとに1つ作成できます。

データセット定義のサンプル

例1 – wls host1の/u01/app/oracle/adminのバックアップ

```
include host wls host1
include path /u01/app/oracle/admin
```

例2 – wls host1およびwls host2上のルート・ファイル・システムのバックアップ

```
include host wls host1
include host wls host2
```

```
include path / {
    exclude path /u01/app/oracle/admin
    exclude path /u01/app/oracle/product/fmw
    exclude path /u01/app/oracle/txn
    exclude name core
    exclude name *.bak
}
```

例3 – NDMPダンプを使用した、ストレージ・デバイス上の/export/configのバックアップ

```
include host zfsappliance name
include path /export/config
```

例4 – NDMP zfsを使用した、ストレージ・アプライアンス上のプロジェクトDomainのバックアップ

最初に、プロジェクトのZFSボリューム名を決定します。この情報は、zfsのBUIにあります。

1. BUIにログインします。
2. 「Shares」をクリックします。
3. 「Projects」をクリックします。
4. バックアップ対象のプロジェクトを編集します。
5. 画面の上部にボリューム名がExalogic/local/ProjectNameのように表示されます。

データセットの例

```
include host zfsappliance name
include path Exalogic/local/ProjectName
```

例5 – スナップショットのバックアップ

```
include host wlshost1
```

```
include path /u01/app/oracle/product/fmw/.zfs/snapshots/mysnapshot
```

注：この方法でスナップショットをバックアップするには、スナップショットが表示されている必要があります。詳しくは、Exalogicディスクのレイアウトを参照してください。

データセットの作成

Oracle Secure Backupでデータセット・ファイルを作成するには、次の手順を実行します。

1. Oracle Secure BackupのGUIにログインします。
2. 「Backup」タブをクリックします。
3. 「Datasets」をクリックします。
4. 「Add」をクリックすると、新規データセットのページが表示されます。
5. Dataset Typeリストから「Directory」を選択します。
6. データセットの名前を指定します。
7. テンプレート・データセットが表示されます。
8. 上記のようなデータセット定義を編集し、変更度グループごとに1つ作成します。
9. 「Save」をクリックします。
10. データセットが作成されました。データセットを選択し、「Check Dataset」をクリックして検証します。

バックアップのスケジュールとトリガー

バックアップ・スケジュールとは、バックアップ対象のデータセットとデバイスの制限事項の説明です。

バックアップ・スケジュールごとにバックアップ・トリガーを1つ以上作成する必要があります。バックアップ・トリガーでは、バックアップの頻度、バックアップの時刻とレベル、およびこのスケジュールで使用するメディア・ファミリを定義します。上記のバックアップ要件に基づき、次のスケジュールを設定できます。

スケジュール	選択可能な時間	データセット	レベル
Low_volatility	毎月1日、02:00 毎週日曜日、02:00	オペレーティング・システム バイナリ	完全 レベル1増分
Med_volatility	毎週日曜日、01:00 毎日、03:00	構成	完全 レベル1増分
High_volatility	毎日、03:30 3時間ごと	トランザクション	完全 レベル1増分

Oracle Secure Backupでバックアップ・スケジュールを作成するには、次の手順を実行します。

1. Oracle Secure BackupのGUIにログインします。
2. 「Backup」タブをクリックします。
3. 「Schedules」をクリックします。
4. 「Add」をクリックします。新規スケジュール・ページが表示されます。
5. スケジュールの名前を入力します。
6. スケジュールの優先順位値を入力します（同時刻に複数のバックアップ・スケジュールを作成した場合は、優先順位の順序で実行されます）。
7. 含めるデータセットを入力します。
8. バックアップ・スケジュールに付けるコメントを入力します。
9. 「OK」をクリックします。

バックアップ・スケジュールを定義したので、実行時期を指定する必要があります。これを行うには、次の手順を実行します。

1. Oracle Secure BackupのGUIにログインします。
2. 「Backup」をクリックします。
3. 「Schedules」をクリックします。
4. 作成したバックアップ・スケジュールをクリックします。
5. 「Triggers」をクリックします。
6. 次の情報を入力します。
7. Backup Level：完全または増分
8. Backup at：バックアップの開始時刻
9. Trigger Type：DayまたはMonth（毎週バックアップを実行する場合はDayを選択）
10. Media Family：使用するテープ・セットを選択します。

11. バックアップを実行する曜日を選択します。
12. 「Add」をクリックします。

オペレーティング・システムのバックアップ

Exalogicマシンでは、オペレーティング・システムがローカル・ディスクに（各コンピュータ・ノードに1つ）インストールされます。オペレーティング・システムはこのようにインストールされるため、NDMPを使用してスナップショットを取ったりテープにバックアップしたりすることはできません。オペレーティング・システムをバックアップするには、ディスクの場合はtarまたはdump、Oracle Secure Backupの場合はobtar（デフォルトのクライアント・バックアップ）を使用する必要があります。

スイッチのバックアップ

InfiniBandスイッチNM2GWおよびNM2-36Pは、Exalogicマシン構成の不可欠な部分であり、オペレーティング・システムと一緒にバックアップする必要があります。ILOM CLIからInfiniBandスイッチをバックアップするには、次の手順を実行します。

1. バックアップをエンコードします
 - > set /SP/config passphrase=*phrase*
 - ** パスフレーズは、バックアップの保護に使用するテキスト・パスワードです **
たとえば次のとおりです。
 - > set /SP/config/passphrase=mypassword1
 - > Set 'passphrase to 'mypassword1'
2. 構成のバックアップ
 - > set /SP/config dump_uri=URI
 - ここで、URLはバックアップの実行用のコマンドです。
 - 次に例を示します。
 - set /SP/config dump_uri=scp://root:rootpwd@123.45.67.89/opt/dump/switch.backup
 - ここで、IPアドレスはバックアップ・ファイルのターゲット・ホストのアドレスです。
 - ここで、/opt/dump/switch.backupはバックアップ・ファイルの名前です。
 - ファイルがファイル・システムにあれば、オペレーティング・システム・バックアップの一部として、より永続的なストレージにバックアップできます。
3. さらに、次のファイルを同じ場所にバックアップする必要があります。
 - /etc/opensm/opensm.conf

- /conf/bx.conf
- /conf/partitions.current

バックアップのリストア

この項では、上記で実行したバックアップのリストア方法について説明します。このホワイト・ペーパーでは“ベア・メタル”リストアについては説明しません。ベア・メタル・リストアとは、バックアップ実行時に新規マシンを同じ状態にリストアするプロセスです。この操作の実行が必要な場合は、まず通常の方法で、1つのコマンドを使用してExalogicマシンをプロビジョニングする必要があります。これが完了すれば、上記で実行したバックアップをリストアできます。

ディスクから

ローカル・スナップショット

スナップショット全体、または個々のファイルをリストアできます。個々のファイルをリストアする場合、これらのファイルは、非表示のディレクトリ.zfs/snapshot/*snapshotname/path_to_file*にあります。たとえば、/u01/app/oracle/product/fmwの場所にあるコンピュート・ノードにマウントされているFMW_Binariesというプロジェクトがあり、スナップショットADHOC1から/u01/app/oracle/product/fmw/mydir1/myfileというファイルをリストアするとします。このファイルのバックアップ・コピーは、/u01/app/oracle/product/fmw/.zfs/snapshots/ADHOC1/mydir1/myfileにあります。

スナップショット全体をリストアする場合は、BUIから次の手順でリストアできます。

1. 「Snapshots」をクリックします。
2. スナップショットを選択し、「Restore」をクリックします。

コマンドライン

リモート・スナップショット

リモート・ディスク・バックアップからリストアするには、まずレプリケーションの方向を逆にして、リモート・バックアップがプライマリ・サイトに返されるようにする必要があります。この操作は、BUIから次の手順で実行できます。

リモート・マシンの場合：

1. 「Shares」を選択します。
2. 「Projects」サブタブをクリックします
3. 「Replicas」を選択します。
4. プライマリ・マシンにリストアするレプリカをクリックし、「Edit」をクリックします。
5. 「Replication」サブタブをクリックします。
6. 「Reverse the direction of replication」 ボタンをクリックします。

7. 新規プロジェクト名の入力を求められます。これは一時的な名前です。プロジェクトは、この名前でリモート・サーバーに作成されます。
8. 「Apply」をクリックします。
9. レプリケーションが停止されるという警告が表示されたら、「OK」をクリックします。
10. 「Shares」をクリックします。
11. 「Projects」をクリックします。
12. 上記の10で作成したプロジェクトを見つけます。
13. 「Edit」をクリックします。
14. 「Replication」サブタブをクリックします。
15. 「Edit」をクリックします。
16. 「Include Snapshots」と、オプションで「SSL」を選択します。
17. 「Apply」をクリックします。
18. 「Update Now」をクリックして、バックアップをプライマリ・マシンにリストアします。

この時点で、バックアップは、レプリカとしてプライマリ・マシンに戻ります。ただし、このバックアップをコンピューター・ノードで使用することはできません。このバックアップをマウント可能にするには、次の2つの操作のいずれかを実行する必要があります。

- 複製したパッケージのクローンを作成し、クローンをマウントします。
- レプリケーションを逆方向で再実行します。この方法では、ファイル・システムを再度マウントできるだけでなく、リモート・バックアップが再開されるため、より一般的です。

プライマリ・マシンの場合：

まず、再作成する古いプロジェクトを削除します。

1. 「Shares」をクリックします。
2. 「Projects」をクリックします。
3. リストアするプロジェクトを見つけ、「Remove」をクリックするか、その横のエントリを破棄して削除します。
4. プロジェクトの削除の確認を求められたら、確定します。

レプリケーションを逆方向で再実行します。

5. 「Shares」を選択します。
6. 「Projects」サブタブをクリックします。
7. 「Replicas」を選択します。
8. プライマリ・マシンにリストアするレプリカをクリックし、「Edit」をクリックします。
9. 「Replication」サブタブをクリックします。
10. 「Reverse the direction of replication」ボタンをクリックします。
11. 新規プロジェクト名の入力を求められます。これは上記の3で削除したプロジェクトの名前です。
12. 「Apply」をクリックします。
13. レプリケーションが停止されるという警告が表示された場合は、「OK」をクリックします。

この時点で、プロジェクトを再マウントでき、バックアップがリストアされています。最後に、リモート・バックアップの再起動を実行する必要があります。

14. 「Shares」をクリックします。
15. 「Projects」をクリックします。
16. 上記の10で作成したプロジェクトを見つけます。
17. 「Edit」をクリックします。
18. 「Replication」サブタブをクリックします。
19. 「Edit」をクリックします。
20. 「Include Snapshots」と、オプションで「SSL」を選択します。
21. スケジュール情報が正しいことを確認し、正しくない場合は編集します。
22. 「Apply」をクリックします。
23. 「Update Now」をクリックしてバックアップを実行し、レプリケーションが再度実行されていることを確認します。

プライマリからスタンバイにレプリケーションを停止します。

GUIからリバース・ボタンを選択します。

ダンプ

ダンプは、OSコマンドrestoreを使用して、リストアします。restoreコマンドを使用するには、次の手順を実行します。

1. ファイルのリストア先のrootにディレクトリを変更します。
2. バックアップ全体をリストアするには、次のようなコマンドを実行します。

```
restore -rf backup_file_name
```

個々のファイルやバックアップの一部をリストアするには、次のようなコマンドを実行します。

```
restore -if backup_file_name
```

これでインタラクティブ・モードになり、addコマンドを使用して、抽出するファイルを選択できます。すべてのファイルを選択したら、コマンドextractを実行してリストアします。

restoreコマンドについて詳しくは、オペレーティング・システムのドキュメントを参照してください。

テープから

Oracle Secure Backupを使用する場合、ファイル・ベースのバックアップをリストアするには3つの方法があります。このドキュメントでは、カタログ・ベースのリストアだけを説明します。その他の種類のリストアについては、[Oracle Secure Backupのドキュメント](#)を参照してください。

カタログ・ベースのリストアを実行するには、Oracle Secure Backupカタログでバックアップ済みのオブジェクトを確認し、リストアするオブジェクトを決定します。

これを行うには、次の手順を実行します。

1. Oracle Secure BackupのGUIにログインします。
2. 「Restore」タブをクリックします。
3. 「Backup Catalog」をクリックします。
4. Host Name列からホストを選択します。
5. Data Selector列から、リストアするバックアップを選択します。リストアできるバックアップの種類は、所定の日付の最新と最古のバックアップ、バックアップIDです。
6. 検索オプションを追加して、検索対象を絞り込みます。
7. リストアするファイルのパスを入力します。
8. 「Browse host」をクリックします。
9. リストア対象を決定したら、「Add」をクリックします。
10. リストア先のホストを選択します（デフォルトはソース・ホストです）。
11. リストア・ページが表示されます。
12. Browse hostペインで、リストアするファイルやディレクトリを選択します。

13. 「Add」をクリックします。
14. リストア・ダイアログ・ページが表示されたら、使用するテープ・デバイスと、必要に応じて、代替リストア・パスを選択できます。終了したら、「OK」をクリックします。
15. リストア対象のファイルやディレクトリごとに、12~14を繰り返します。
16. 「GO」をクリックして、リストア・ジョブを送信します。

スイッチのリストア

スイッチ・バックアップをファイル・システムにリストアすると、スイッチにリストアできます。この操作は、ILOM CLI経由で次の手順で実行できます。

1. バックアップをエンコードします。
-> set /SP/config passphrase=*phrase*
ここでのpassphraseは、バックアップ時に使用したものです。たとえば次のとおりです。
-> set /SP/config/passphrase=mypassword1
-> Set 'passphrase to 'mypassword1'
2. 構成をバックアップします。
-> set /SP/config load_uri=URI
ここで、URLはリストアの実行用のコマンドです。
次に例を示します。
set /SP/config load_uri=scp://root:rootpwd@123.45.67.89/opt/dump/switch.backup
ここでのIPアドレスは、バックアップ・ファイルのターゲット・ホストのアドレスです。
/opt/dump/switch.backupは、バックアップ・ファイルの名前です。
3. 次のファイルを、手動で元の場所にコピーし直します。
 - /etc/opensm/opensm.conf
 - /conf/bx.conf
 - /conf/partitions.current

結論

バックアップ戦略の作成時には、次のような多くの考慮事項があります。

- バックアップ戦略によって、どのような損失（人為的または災害）からのリカバリを予定しているか
- 使用するバックアップ・テクノロジーのタイプ。たとえばディスク間、またはディスクからテープなど
- オブジェクトの変更度
- 使用するバックアップ頻度
- 実装する保存方針

これらはすべて、バックアップおよびリカバリ戦略の実装方法に影響します。このホワイト・ペーパーでは、これらの機能のさまざまな実装方法を検討し、実装する最適なポリシーを決定しました。これは、ユーザーおよびマシン障害の両方に対応し、ディスクとテープのバックアップ・テクノロジーを組み合わせたものです。

1. ディスク・ベースのスナップショットを作成し、ユーザー・エラーから迅速にリカバリする。
2. テープ・ベースのバックアップを作成し、長期にわたり、オフサイトでアーカイブする。

テープにバックアップする場合、NDMPかコンピュート・ノードを使用できます。NDMPによるバックアップの方が高速で、コンピュート・ノードでのオーバーヘッドもありませんが、ローカル・ストレージに保存されているオペレーティング・システムやその他のファイルのバックアップには使用できません。バックアップ速度が問題の場合、最速の解決方法はNDMPを使用することですが、クライアントからバックアップを取る方がより柔軟な場合があります。

参考資料

- [Oracle Exalogicドキュメント・ライブラリ](#)
- [ExadataセルおよびOracle Exadata Database Machineを使用したバックアップおよびリカバリのパフォーマンスとベスト・プラクティス](#)
- [Oracle Databaseバックアップおよびリカバリ・ユーザーズ・ガイド](#)
- [Oracle Secure Backup](#)



Oracle Exalogicのバックアップとリカバリ
2011年9月

著者：Michael Rhys

共著者：Pradeep Bhat、Andrew Babb、
Donna Cooksey、Neeraj Gupta

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

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

oracle.com



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

Copyright © 2011, 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。本文書は一切間違いがないことを保証するものではなく、さらに、口述による明示または法律による黙示を問わず、特定の目的に対する商品性もしくは適合性についての黙示的な保証を含み、いかなる他の保証や条件も提供するものではありません。オラクル社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。本文書はオラクル社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。

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。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。UNIXはX/Open Company, Ltd.によってライセンス提供された登録商標です。1010

Hardware and Software, Engineered to Work Together