

Zero Data Loss Recovery Appliance

ビジネス・データを保護するための今日のストレージ・ソリューションを使用して、ミッション・クリティカルな企業データベースのニーズを満たすことは簡単ではありません。これらのソリューションでは、リストアのたびに最大で1日分のビジネス・データを失う可能性があり、データベース・レベルのリカバリ能力を検証する機能に欠け、バックアップ中の本番サーバーに大きな負荷をかけ、増大し続けるデータベースのニーズに応じてスケーリングすることができません。これらの課題のおもな原因は、データベースを特定の整合性とリカバリの要件のあるトランザクション・システムとして処理せず、基本的に一連の分散ファイルとしてコピーするという処理方法を利用しているためです。ランサムウェア攻撃に直面すると、ビジネスへの影響はさらに深刻化します。ランサムウェア攻撃によって、検知されることなく本番データとバックアップ・データの両方が侵害され、企業のデータとリカバリ能力が人質に取られる可能性があります。

オラクルのZero Data Loss Recovery Appliance (Recovery Appliance : RA) は、Oracle Databaseと緊密に統合して、これらの要件に真っ向から対処する革新的なデータ保護ソリューションです。データ損失を排除し、リカバリを高速化し、本番サーバーへのデータ保護のオーバーヘッドを激減させます。さらに、Recovery Applianceはランサムウェア攻撃に対するデータの整合性とリカバリ能力を継続的に検証し、数千ものデータベースを保護するためにスケーリングし、ライフサイクル全体を通じてディスク・バックアップ、クラウド・アーカイブ、リモート・レプリケーション、テープ・アーカイブにおいてバックアップを保護します。

今日のデータベース保護の課題

今日のデータベース保護ソリューションの根本的な課題は次のとおりです。

- バックアップ方法とリカバリ方法が従来の夜間バックアップ・パラダイムに基づいており、最大で1日分の貴重なデータをリストアごとに失う可能性がある
- バックアップ中、データの変更の有無に関係なく、すべてのデータベース・データを処理することで、本番サーバーとネットワークにバックアップの大きなオーバーヘッドがかかっている
- データの増加が止まらないため、バックアップ期間がますます拡大



Oracle Zero Data Loss Recovery Appliance RA23

おもな機能

- リアルタイムのREDO転送
- エンド・ツー・エンドのデータ検証
- 永久増分バックアップ戦略
- 省スペースの仮想全体バックアップ
- バックアップ操作のオフロード
- データベース・レベルの保護ポリシー
- データベース対応の領域管理
- クラウド規模のアーキテクチャ
- 効率的なレプリケーション
- クラウド/ZFS/テープへのポリシー駆動型アーカイブ
- 統合された管理と制御
- ラックあたり最大1.57 PBのバックアップ容量
- ラックあたり最大35 TB/時のバックアップおよびリストア・スループット

- 拡張性に乏しいバックアップ・アプライアンスでは、データセンターの数百から数千のデータベースを保護できない
- ディスクからクラウド、レプリケーション、またはテープまで、完全なデータ保護ライフサイクルを十分に可視化し制御することができない

Zero Data Loss Recovery Applianceの紹介

Oracle Zero Data Loss Recovery Appliance (Recovery Appliance) は、特にデータベースを保護するように設計された世界初のエンジニアド・システムです。

Recovery Applianceはすべてのデータベースを継続的に保護しながら、すべてのバックアップ処理においてオフロードを実現し、本番サーバーにおけるオーバーヘッドを最小限に抑えます。

このアプライアンスは、ベース・ラック構成で開始して小規模Oracle環境に対応でき、そこからスケールアウトして、データセンターの数百から数千のデータベースのデータ保護要件をサポートできます。

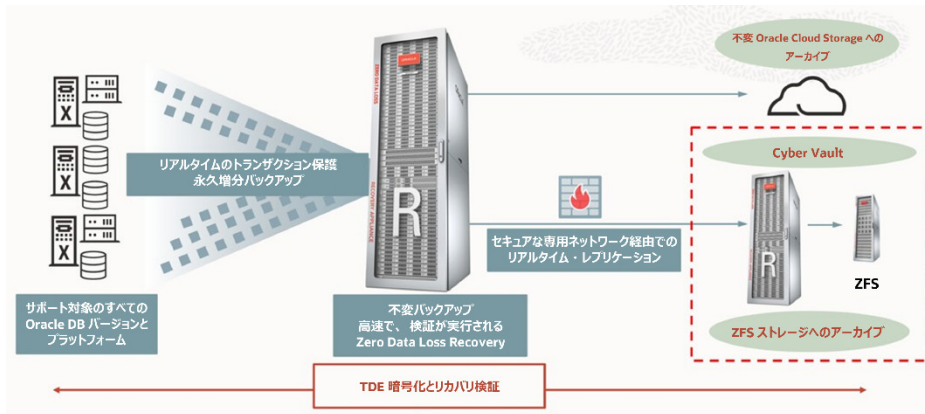


図1：Zero Data Loss Recovery Appliance：アーキテクチャ概要

Recovery ApplianceはOracle DatabaseおよびRecovery Manager (RMAN) と緊密に統合して、他のデータ保護ソリューションでは提供できないデータ保護機能とパフォーマンスを実現します。

データ損失の排除

Recovery Applianceのおもな設計目標は、他のデータ保護ソリューションを利用する場合は生じるおそれのあるデータ損失の危険をなくすことです。

リアルタイムのREDO転送

REDOログは、Oracleデータベース内でトランザクションでの変更の実装にて基礎をなす手段です。Oracle Database 12cおよびそれ以降のバージョンのデータベースはすべて、インメモリ・ログ・バッファからREDOを継続的にRecovery Applianceに直送できます。これにより、独自のリアルタイムのデータ保護を実現し、データベースの最後の1秒未満まで保護できます。REDOはデータベース共有メモリから送信されるため、本番システムへのオーバーヘッドが極めて低くなります。

おもな利点

- データ損失の排除
- 高速で最適化されたリカバリ
- 最小限の影響しか及ぼさないバックアップ
- データベース・レベルのリカバリ能力
- クラウドへの統合アーカイブ
- クラウドスケールの容量とパフォーマンス

Recovery Applianceのおもな設計目標は、既存のデータ保護ソリューションを使っていたら失う可能性のある重要なデータベース・データの損失をなくすことです。

「当社はデータ・ドメインをオラクルのZero Data Loss Recovery Applianceに換えて、リアルタイムの増分バックアップを実現し、毎月のクレジット・カードの取引でデータを失うことなく、8億5千万米ドル以上を回収しています。また、平均バックアップ・サイズが30分の1に減少し、バックアップ容量が65%増えました。」

KEB Hana Card Co., Ltd.、ITチーム、シニア・マネージャー、Iljoon Lee氏

リアルタイムのREDO転送はオラクルのData Guardテクノロジーに初めて実装され、世界中の数千ものミッション・クリティカルなデータベースで導入されています。Recovery Applianceはこのテクノロジーの対象をシンプルにコスト効率よく最上位のデータベース層の外まで広げます。Recovery Applianceは、Data Guardの高速ファイルオーバーと問合せオフロード機能を必ずしも必要としないデータベースに対し、今日のData Guardと同等レベルのデータ保護を実現します。

効率的なレプリケーション

ローカルRecovery Appliance上のバックアップは、サイトの停止や地域の災害からの保護対策として、リモートRecovery Applianceに簡単に素早く複製できます。レプリケーション・トポロジは、データセンターの要件に合わせてカスタマイズできます。たとえば、レプリケーションをシンプルな1方向のトポロジに設定したり、2台のRecovery Applianceを相互複製に対応できるように設定したり、中央のRecovery Applianceへの複製が可能になるように複数のサテライトRecovery Applianceを設定したりすることができます。ローカルRecovery Applianceを使用できない場合、データをローカルでステージングしなくても、リストア操作をリモートRecovery Applianceから直接実行できます。

アプライアンスは"Backup Anywhere"ペア・レプリケーション構成でセットアップすることもでき、その場合は一方のシステムに取られたバックアップが他方のシステムに自動的に同期されます。これにより、どちらかのシステムに影響を与える障害が発生した場合でも、バックアップとリカバリ操作のための高可用性を維持できます。

すべてのトポロジで、変更されたブロックだけが複製されるので、WANネットワークの使用を最小限に抑えられます。

クラウド/ZFS/テープへのポリシー駆動型アーカイブ

Oracle Cloudとの統合により、低コストのオフサイト・ストレージに直接アクセスできます。これにより、物理メディアの紛失やオフサイトへの送付忘れなど、物理メディアの移動に伴うリスクが軽減されます。また、物理メディアの到着を待つ必要がないため、必要なときに、はるかに早くリカバリ・プロセスを開始できます。

Oracle Cloudに保存されたバックアップはネイティブのRMAN形式であるため、Recovery Applianceとは関係なくアクセスできます。これらのバックアップは、クラウドへの移行、テスト、開発、または既存のバックアップからクラウド・データベースをインスタンス化してコンプライアンス関連のリクエストを満たすために使用します。クラウド・バックアップをOracle Cloud Databaseに直接リカバリできるのであれば、オンプレミスのリソースの割り当てに時間を費やす必要はありません。

オンプレミスのバックアップ・アーカイブが必要なお客様のために、Recovery Applianceは、ZFS OCIオブジェクト・ストレージ・インタフェースとの統合により、Oracle ZFS Storageへのフル・バックアップと増分バックアップをオフロードします。アーカイブとリストア操作は、ZFSとの間で直接25 Gbまたは100 Gb接続で実行できます。

また、32 Gbファイバ・チャンネル・アダプタ経由でテープにオフロードすることもできます。データは、付属のOracle Secure Backupメディア管理ソフトウェアを使用してテープ・ライブラリに直接送信されます。これにより企業は、既存のテープ・ライブラリを使い続けながら、本番サーバー上の高価なメディア・マネージャ・データベース・バックアップ・エージェントを排除することができます。

Recovery Applianceを使用すると、企業はクラウド・ストレージの利用を拡張するか、またはテープへの投資を保護し、現在のテープベースのデータ保存戦略を継続することができます。

オラクルのStorageTekテープなど、Oracle Secure Backup対応のテープ・ハードウェア製品はすべてRecovery Applianceでサポートされます。あるいは、他社製テープ・バックアップ・エージェントをRecovery Applianceにデプロイして、既存のテープ・バックアップ・ソフトウェア、メディア・サーバー、プロセスに統合することもできます。

テープやクラウドへのアーカイブのためのこのプロセスは、Recovery Applianceに完全にオフロードされ、本番データベースからこれらのバックアップを作成する影響は排除されます。従来の週次フルおよび日次増分アーカイブ戦略は、拡張リカバリ期間要件を満たすために採用でき、ポイントインタイム・アーカイブ・バックアップ（RMAN KEEPバックアップに類似）は、数か月または数年のコンプライアンス保持要件を満たすために作成できます。すべてのアーカイブ操作はアプライアンスから1日中実行でき、本番システムの速度を低下させることなく、リソース使用率の向上とコスト削減を可能にします。

確実なリカバリ：エンド・ツー・エンドのデータ検証

Recovery ApplianceはOracleデータベース内部のブロック形式を認識し、深いレベルのデータ検証を実現します。バックアップ・データとREDOブロックはすべて、Recovery Applianceで受信されたとき、クラウド/テープにコピーされたとき、複製されたときに自動的に検証されます。また、バックアップ・ブロックは定期的にディスク上で検証されます。そのため、リカバリ操作によって常に有効なデータがリストアされます。これは、Recovery Applianceに特有のデータベースとの深い統合がないと実現しないもう1つの差別化要因です。検証中に破損が検出されると、Recovery Applianceを支えるストレージ・ソフトウェアによって、ミラー・コピーから正常なブロックが自動的に読み取られて、破損したブロックが即座に修復されます。

さらに、Recovery Applianceストレージ・ソフトウェアは、基盤のハード・ディスクを定期的に検査します。不良セクターが検出されると、ミラー・コピーから即座に修復されます。

すべてのバックアップ・データとREDOブロックが各ライフサイクル・ステージで独立して自動的に検証されます。

最小限の影響しか及ぼさないバックアップ

24時間365日体制の要件があっても、多くの企業は依然として数時間のバックアップ期間を設ける必要があり、その間業務処理のジョブが影響を受けます。バックアップ期間はビジネスのメリットに直結せず、ピーク時間以外の処理時間をめぐってビジネスに不可欠なレポーティングおよびバッチ・ワークロードと時間を奪い合う事態を招いています。グローバル経済が成長する中、バックアップに利用可能な時間帯は縮小し続けていますが、データ量は増大しています。

現在のディスクベースのデータ保護ソリューションの影響

現在のディスクベースのデータ保護ソリューションは、本番システムに大きな負荷を課しています。データベースが拡大し続ける中、この影響はこれからも大きくなります。おもな課題のいくつかを以下に挙げます。

- 重複排除アプライアンスは定期的に全体バックアップを取得する必要があります。全体バックアップではデータベース全体が読み取られるため、本番ストレージ、サーバー、ネットワークに大きな影響が及ぶ上に、長時間に及ぶバックアップ期間を必要以上に長く設ける必要があります。

- ソース側の重複排除を使ってネットワーク要件を軽減する場合、本番サーバーに高いCPUとメモリの負荷がかかるという悪影響が生じます。
- リカバリ・フェーズの間、データベースを開く前に、増分バックアップをリストア済みのデータファイルに適用する必要があります。このプロセスでは、増分の変更適用期間が数日間に渡り、かつ、適用操作は通常、ネットワーク全体で実行されるため、リカバリに非常に長い時間を要することがあります。

永久増分バックアップ・アーキテクチャ

Recovery Applianceの2番目の設計目標は、本番データベース・システムでのバックアップ関連の処理を可能な限り最小限に減らして、実際に変更されたデータだけを送信することです。不要なバックアップ処理の排除により、本番システムは本来の目標である、ビジネスに不可欠なワークロードの処理に集中できるようになります。

Recovery Applianceは永久増分バックアップ・アーキテクチャを実装して、本番システムへの影響を最小限に抑えます。このアーキテクチャは、次の2つの革新的なテクノロジーをベースにしています。それは、Delta PushとDelta Storeです。

Recovery Applianceを使用すると、本番データベース・サーバーは、本番ワークロードを処理する本来の仕事に専念でき、バックアップやリカバリのタスクに忙殺されることがなくなります。

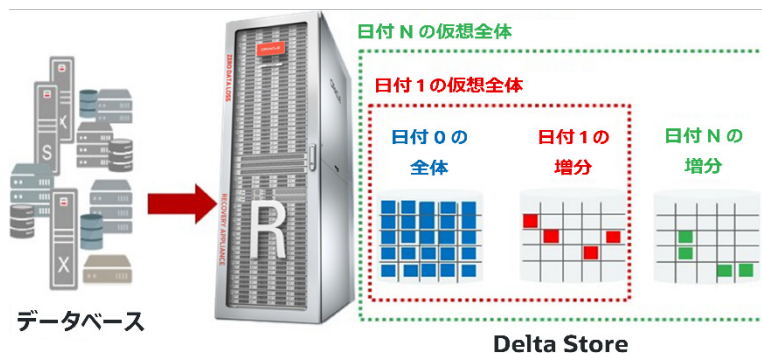


図2 : Zero Data Loss Recovery Appliance : Delta PushとDelta Store

Delta Push

Delta Pushを使用すると、保護されたデータベースは、一意の変更を含む増分バックアップだけをRecovery Applianceに送信します。全体バックアップを繰り返す必要はありません。Delta Pushは"永久増分"としても知られています。1回の全体バックアップ後、増分バックアップだけが本番システムで実行されるためです。Delta Pushは実質的に、データベース向けに高度に最適化されたソース側での重複排除です。

Recovery Managerのブロック・チェンジ・トラッキングを使用すると、本番データベース上の変更されたブロックが非常に効率的に識別されるため、変更されていないデータを読み取る必要がなくなります。

保護されたデータベースとRecovery Appliance間の特別な統合により、コミットされたUNDO表領域、未使用の表領域、ドロップされた表領域ブロックがバックアップ・ストリームから排除されて、オーバーヘッドと領域の消費が大幅に減ります。Delta Pushは、全体

バックアップではなく変更されたデータだけを送信するので、他のソリューションに比べてネットワーク・トラフィックが大幅に軽減されます。これにより、低コストなイーサネットをバックアップに使用できます。また、ネットワーク・トラフィックを最小限に減らすことで、保護されたデータベースからさらに遠くにRecovery Applianceを配置でき、場合によってはWAN越しのリモート・データセンターに配置できます。

Delta Store

Delta StoreはRecovery Applianceソフトウェア・エンジンの“ブレイン”です。Delta Storeは、変更され受信したデータ・ブロックを検証してから圧縮し、索引を付けて保存します。変更されたこれらのブロックは、**仮想のデータベース全体バックアップ**の基盤となるものであり、仮想データベース全体バックアップ（Virtual full）は、増分バックアップの断面を、スペース効率に優れたポイントベースで表現した物理全体バックアップです。仮想全体バックアップは、データセットおよび保護されたデータベースの変更率に応じて10倍以上ストレージを効率化できます。

たとえば、100 TBのデータベース、1%の変更率、30日のリカバリ期間ポリシーの場合、従来どおりに全体バックアップを毎週、増分バックアップを毎日実行する手法だと、次のような結果になります。

- 全体バックアップ：（100 TB×5回のバックアップ）
- 増分バックアップ：（1 TB×30回のバックアップ）
- 合計：530 TB¹

これと比較してRecovery Applianceの場合は、次のような結果になります。

- 全体バックアップ：100 TB
- 増分バックアップ：（1 TB×29回のバックアップ）
- 合計：129 TB

従来のバックアップよりもストレージ消費量をほぼ5倍節約できます。Recovery Applianceのオンディスク圧縮を考慮すると、合計節約量は10倍以上に達する可能性があります。

Delta Storeアーキテクチャの劇的な領域効率により、大量の仮想全体バックアップをオンラインに維持することができ、ディスクベースのリカバリ期間を大きく広げることができます。

リストア操作が必要な場合、Delta Storeはもっとも最近取得された増分バックアップに基づいて、効率的に物理全体バックアップを再作成します。リストア操作は、Recovery Applianceの基盤となるハードウェア・アーキテクチャの大規模なスケーラビリティとパフォーマンスによって支えられています。

Recovery Applianceからリストアする場合、全体バックアップをリストアした後、すべての関連増分バックアップをリストアおよび適用する従来の低速プロセスが排除されます。Recovery Applianceによるリストア・パフォーマンスはより予測しやすく、SLAを満たすのに役立ちます。

¹ R日のポイント・イン・タイム・リカバリ期間ポリシーを維持する毎週の全体バックアップと毎日の増分バックアップ手法で、合計R + 7日間のバックアップをストレージに保持するには、さらに7日間のバックアップ（1日の全体バックアップ + 6日の増分バックアップ）が必要です。これはデータベース・リカバリ設計が原因です。このリカバリ設計では、R日以上経過した全体バックアップを少なくとも1つ、リストア操作のために保持する必要があり、その後、増分バックアップとアーカイブ・ログ・バックアップを使って、R日のリカバリ期間の開始時点へとさかのぼってリカバリされます。

「OracleのZero Data Loss Recovery Applianceは頼りになり、とても安心です。かつてはリフレッシュ・タスクに多くの時間を費やしていましたが、今ではDBAチームの生産性が大幅に向上し、Enterprise Managerによっていつでも制御下のOracleデータベースを保護し、緊急のリストアが必要な場合でも、非常に素早く実行して、最新のトランザクションまでリストアできるという確信が持てるようになりました。」

Every, リード・データベース・アーキテクト、
Nazrul Islam氏

リストアの高速化は、(1) データベースのテスト/開発のリフレッシュの高速化、および (2) レガシーOSプラットフォームからOracle Exadataなどの最新プラットフォームへの移行の高速化も意味します。Recovery Applianceは、革新的な仮想全体リストア・テクノロジーに基づき、最小限のダウンタイム、クロスプラットフォーム、クロスバージョンのデータベース移行作業に活用できます。

ほとんどのバックアップ操作をオフロード

バックアップ関連の処理は実質的にすべて、Recovery Applianceにオフロードされます。これには、時間のかかる圧縮、バックアップの削除、検証、保守操作が含まれます。その結果、バックアップ期間外のときでも本番システムのリソースが解放されて、本番システムのパフォーマンスが向上します。

つまり、リアルタイムのREDO転送とDelta Pushにより、保護されたデータベースは最小限のバックアップ関連作業を実行し、変更されたデータだけをRecovery Applianceに送信します。クラウド/テープ・バックアップなど他のすべてのバックアップおよびリカバリ関連の処理はRecovery Applianceによって実行されます。これは、Recovery Applianceの主要なアーキテクチャ上のイノベーションのひとつであり、今日のバックアップ・ソリューションをはるかに凌駕します。

Database Protection as a Private Cloud Service (プライベート・クラウド・サービスとしてのデータベース保護)

Recovery Applianceの3つ目の設計目標は、クラウド規模のデータベース保護サービスをデータセンターの数十から数千のデータベースに提供することです。複数のRecovery Applianceのテクノロジーがこの目標を実現します。

ポリシー・ベースのデータ保護管理

Recovery Applianceは保護ポリシーの概念を導入して、アプライアンスとクラウドまたはテープ上でデータベースごとに達成するリカバリ目標を定義します。保護ポリシーを使用することで、データベースはリカバリ・サービス層で容易にグループ化することができます。Recovery Applianceには事前定義済みの“Platinum”、“Gold”、“Silver”、“Bronze”のポリシーがあり、これらをカスタマイズしてさまざまなビジネスレベルでの品質保証(SLA)を実現できます。たとえば、Goldポリシーのデータベース・バックアップはローカルRecovery Appliance上で35日、クラウド上で90日のリカバリ期間を目標とし、Silverポリシーで管理されるバックアップはローカルRecovery Appliance上で10日、テープ上で30日のリカバリ期間を目標としています。階層化保護ポリシーは、リモートでレプリケートされたRecovery Applianceにも個別に適用できます。

追加のデータベースを作成した場合、既存の保護ポリシーの1つに容易に追加できます。たとえば、新しいFinanceデータベースをGold保護ポリシーに容易に追加できます。追加後、ポリシーのリカバリ期間目標が自動的にこのデータベースのバックアップに適用されます。この自動ポリシー・ベースのフレームワークにより、企業は社内全体でDatabase Protection as a Serviceを簡単に実装できます。

データベースを理解した領域管理

「シームレスで信頼性の高い通信サービスと金融サービスを提供するというSafaricomの約束は、Oracle ExadataとOracle Recovery Applianceの比類ないパフォーマンスとデータ保護機能によって支えられています。業界をリードするこれらのソリューションにより、優れたカスタマー・エクスペリエンスを提供し、貴重なデータ資産の最大限のセキュリティと整合性を確保することができます。」

Safaricom PLC、ITインフラストラクチャとエンタープライズの部門責任者、
Mark Oyier氏

Recovery Applianceを使用すると、データ保護のレベルをアプリケーションのビジネスの重要度にはるかに的確に合わせることができ、物理的なビットとバイトのレベルに制限されることがありません。

Recovery Applianceは保護ポリシーをベースに使用しながら、各データベースのリカバリ期間目標に応じてすべてのバックアップ・ストレージ領域を完全に管理します。たとえば、Goldポリシーのメンバーである“Finance Database”は過去35日以内にリカバリできる一方で、Silverポリシーのメンバーである“Products Database”は過去10日以内にリカバリできます。Delta Storeに空き領域がある場合、リカバリ期間目標より古いバックアップが保持されて、実質的にリカバリ可能期間が延長されます。ストレージ領域にあまり余裕がない場合、Recovery Applianceはバックアップを消去し、データベース間で領域を自動的に再プロビジョニングして、保護されたそれぞれのデータベースのリカバリ期間目標を満たします。また、すべてのデータベースのリカバリ期間目標を満たすために、領域が少なくなる前に、領域の使用履歴を基にバックアップを先見的に消去することもできます。データファイル、REDOログ、制御ファイル間の依存関係を認識した上で、領域はデータベース内でインテリジェントに消去されます。

このリカバリ期間指向の領域管理手法は、通常の汎用バックアップ・アプライアンスのように不明瞭なストレージボリューム・レベルで領域を管理しなければならない工数をなくします。この革新的な手法では、各アプリケーションのビジネスの重要度に合わせてデータが保護され、手動による領域のリバランシングは不要となります。

大容量でクラウド規模のアーキテクチャ

Recovery ApplianceはOracle Exadataアーキテクチャをベースにしているため、その実証済みのスケラビリティ、冗長性、パフォーマンスを継承しています。社内の追加のデータベースはRecovery Applianceによって保護され、コンピューティング・サーバーとストレージ・サーバーはアプライアンスに容易に追加できます。その結果、ビジネスの成長をシームレスにサポートする、シンプル、無停止のスケールアウト・データ保護クラウドが実現します。

Recovery Applianceの構成

ベース・ラックおよびフル・ラック構成

Recovery Appliance RA23の基本構成では、100 Gb/秒のRemote Direct Memory Access (RDMA) over Converged Ethernet (RoCE) を使って2台のコンピューティング・サーバーと3台のストレージ・サーバーが内部接続されています。RoCEはクラウド規模の超高速ネットワーク・ファブリックの最新世代であり、あるコンピュータがオペレーティング・システムやCPUを介さずに別のコンピュータのデータに直接アクセスできるため、高帯域幅で待機時間の短いアクセスが可能になります。

ベース・ラック構成では、バックアップ格納用に274 TBの使用可能容量を持つ高可用性構成が提供されます。ベース・ラックは、追加のストレージ・サーバーをラックに追加することで段階的にアップグレードでき、最大17台のストレージ・サーバーをフル・ラックに収納できます。各ストレージ・サーバーにより、使用可能な容量が92 TB増えます。フル・ラックの使用可能な総容量は1.57 PBで、**仮想全体バックアップの有効容量は最大15ペタバイト**になります。²

Recovery Applianceは、通常10日間のリカバリ期間にわたって、アプライアンスの使用可能な容量とほぼ同じ合計サイズのデータベースを保護できます。たとえば、2台のコンピューティング・サーバーと1.57 PBの使用可能な容量を持つ17台のストレージ・サーバーからなる単一フル・ラック構成では、

「Recovery Applianceにより、バックアップの構成時間は数週間かかっていたところが5分に短縮でき、バックアップ量も40%削減できました。」

Swisscom、ヘッド・アーキテクト、
Christoph Lutz氏

「Recovery ApplianceはData Protection as a Service (DPaaS) を提供し、データベースのパフォーマンスを加速化し、非常に細かいレベルの粒度でリカバリすることを可能にします。」

Enterprise Strategy Group、
上級アナリスト、
Jason Buffington氏、
プラクティス・ディレクターおよび
上級アナリスト、
Mark Peters氏、
調査アナリスト、
Monya Keane氏

² 有効容量は、毎日の変更率10%に基づいて計算されます。

約1.57 PBのソース・データベースを10日間のリカバリ期間の間保護することができ、その10日間で生成された10個の1.57 PBの仮想全体バックアップおよびすべてのREDOデータを保存できます。Recovery Applianceの正確なサイジングは、初期データベースのサイズと増加率、TEMPとUNDOで消費されるストレージ、空き領域、データベースの変更率、REDO生成率、目的のリカバリ期間、データベースの圧縮性など、保護されたデータベースに関わる複数の要因によります。

完全スケールアウト・アーキテクチャ

フル・ラックを超える追加容量が必要な場合は、2台目のベース・ラックを100 Gb/秒RoCE経由で最初のラックに接続できます。2台目のラックにも、2台のコンピューティング・サーバーが収容されており、構成の接続性と処理能力を強化します。最初のラックと同様に、ストレージ容量はストレージ・サーバーの段階的な追加によって容易に拡張できます。最大搭載済み構成のラックを、最大18台結合し単一アプライアンスとしてまとめて接続して、28.2 PBの使用可能な容量、つまり、**282ペタバイトの仮想全体バックアップ**を実現できます。

Recovery Applianceスケールアウト・アーキテクチャのパワーと柔軟性は、追加のデータベースをサポートする必要がある場合、またはビジネス・データが増加する場合に役立ちます。ストレージ、コンピューティング、ネットワークの容量をバランスよく段階的に追加することで、高いパフォーマンスが維持されます。通常、2台のコントローラに制限されていて、ストレージ、ネットワーク、コンピューティングをボトルネックのないバランスの取れた方法ではスケールリングできない従来のバックアップ・アプライアンスよりも、このアーキテクチャの方がはるかに優れています。

パフォーマンス特性

スループットが極めて高いコンピューティング、ネットワーク、ストレージの組合せとRecovery Applianceの独自のデータベース統合により、データセンター全体のデータ保護のニーズを容易にサポートするパフォーマンス・レベルが実現します。

2台のコンピューティング・サーバーと17台のストレージ・サーバーからなる単一のフル・ラックRecovery Appliance RA23は、最大**350 TB/時**の実効速度で実行される仮想全体バックアップもサポートできます。この速度は他の市販製品をはるかに上回ります。このような速度が可能なのは、Recovery Applianceで読み取り、送信し、処理する必要があるのが変更されたデータだけだからです。その結果、他の製品より作業量がはるかに減少します。

単一ラックのRecovery Applianceは、最大35 TB/時の持続的な差分取得速度を実現できます。つまり、35 TB/時で変更データを受信して、**350 TB/時**の仮想バックアップに変換できます。最大35 TB/時のリストア速度にも対応できます。

ラックを構成に追加すると、パフォーマンスと容量の両方が直線的に増強されます。18ラックのRecovery Applianceは、最大**6ペタバイト/時**の仮想全体バックアップ、630 TB/時の差分取得およびリストアを達成します。

Zero Data Loss Recovery Applianceを使用すると、完全スケールアウト・ストレージとコンピューティング・サーバーで容量とスループットを拡張できます。

Recovery Applianceは単一のフル・ラックで最大**15ペタバイトの仮想全体バックアップ**を、18台のフル・ラック最大構成で**282ペタバイト以上の仮想全体バックアップ**をサポートできます。

単一のRecovery Applianceフル・ラックは、最大**350 TB/時**の実効速度で実行される仮想全体バックアップをサポートし、18台のフル・ラック構成は**6ペタバイト/時**をサポートします。

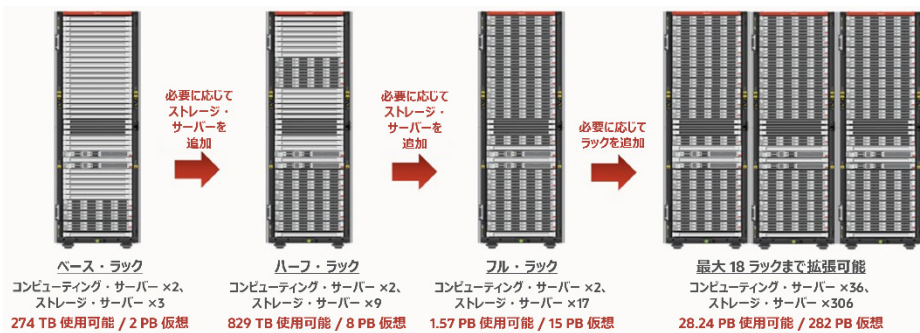


図3： Recovery Appliance RA23のスケールアウト・ラック構成

RA23からは、Recovery Applianceを100 Gb ToRスイッチで構成することで、Exadata上にある、保護されたデータベースの専用バックアップ/リカバリ・ネットワークを構築できます。これにより、Recovery Applianceがデータセンターのバックアップ・ネットワークを共有する必要がなくなり、全体的なスループットが最適化されます。これは大量のデータベース・バックアップには特にメリットとなる可能性があります。このネットワーク構成は、以下に示すように、ExadataシステムをRecovery Applianceに設置された100 Gb ToRスイッチに接続することで実現します。

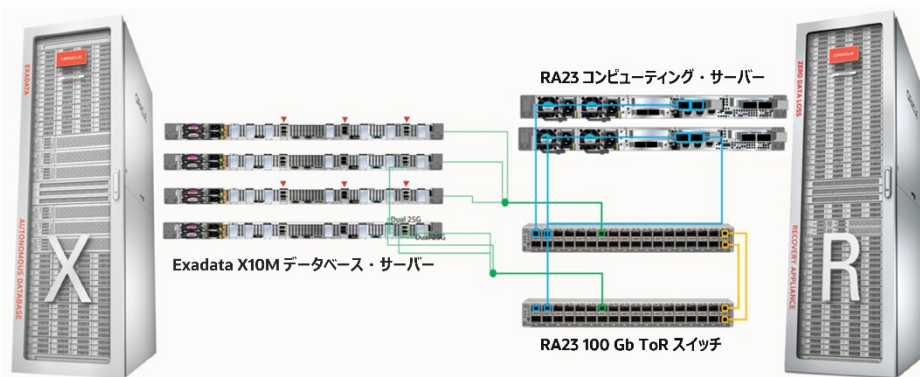


図4： Recovery Appliance RA23 100 Gb ToRスイッチ構成

ソフトウェア構成

Recovery Applianceの実行に必要なソフトウェアはすべて1つのソフトウェア・ライセンスに付属しています。

- バックアップ、リカバリ、およびレプリケーション
- メタデータおよびRecovery Managerのリカバリ・カタログ用の組込みOracleデータベース
- Recovery Appliance用のRMANバックアップ・モジュール
- ストレージ・ソフトウェア
- クラウド・ソフトウェアへのアーカイブ
- Oracle Secure Backupのソフトウェア
- Oracle Enterprise Managerによる監視および管理

通常のOracleライセンスと同様に、Recovery Applianceライセンスは新しいアプライアンスに完全に移転可能です。ライセンスの基準はストレージのテラバイト数ではなく、ストレージ・ディスク・ドライブであるため、ディスク・ドライブがはるかに大規模でプロセッサが高速な新しいアプライアンスで既存のライセンスを使用できます。

エンド・ツー・エンドのデータ保護管理

データ保護管理タスクは通常、データベース管理者、バックアップ管理者、ストレージ管理者などのITの役割に合わせて細分化された複数の管理領域に分散されています。したがって、Recovery Managerを使って開始されたバックアップが中間レイヤーで問題を起こさずに、バックアップ先（テープなど）に達したかどうかをDBAが判断することは、ほとんどの場合ほぼ不可能です。

Recovery Applianceは、完全に自動化された統合データ保護管理でこの問題を解決します。

Oracle Enterprise Manager Cloud Controlによる統合管理

Recovery Applianceは、バックアップがRecovery Managerを使って開始されたときから、ディスク、クラウド、テープに保存されるかリモート・データセンターの他のRecovery Applianceに複製されるまでのデータ保護ライフサイクルを、Oracle Enterprise Manager Cloud Controlを使ってエンド・ツー・エンドかつ一元的に表示します。すべてのバックアップの保存場所がRecovery Applianceによって追跡されるので、Recovery Managerのリストア操作とリカバリ操作によって、保存されている場所に関係なく最適なバックアップを取得できます。きめ細かいストレージとパフォーマンスのメトリックを含め、データ保護ライフサイクルへのこのレベルのエンド・ツー・エンドの可視性を提供できるのはRecovery Applianceだけです。

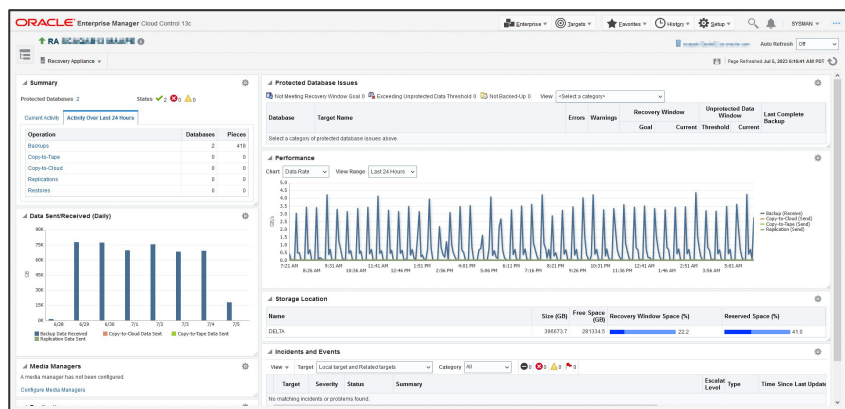


図5：一元化された保護管理 – ストレージとパフォーマンスのメトリック

Recovery Applianceは高度なストレージの監視とレポート機能を搭載して、データの増加に基づく容量の要件に加えて、現在と将来のスループットを効果的に管理します。Recovery Appliance管理下の各データベースに必要な領域の量は、そのバックアップ領域の使用履歴とリカバリ期間目標を基に予測的に計算されます。必要な領域はEnterprise Managerでデータベースごとに明確に表示され、アプライアンスはすべてのデータベースに必要な総領域を、使用可能なストレージ合計のパーセンテージとして集計して、データ増加の対応から不確定要素を排除します。現在のデータの増加を基に、容量がいつ超過するかを知りたい場合は、Oracle Analytics Server (OAS)で利用可能なRecovery Appliance Capacity Reportさえ見れば、ストレージの使用率、7日、31日、365日の平均および最大スループットに関するサマリーと詳細、およびCPU、メモリ、IOPSの詳細を確認できます。また、必要な領域が使用可能な総領域の15%以内（またはユーザーによる構成が可能な他のしきい値）である場合は、警告を生成できます。

「企業は、従来の手法を使用する場合に起こりがちな停止時間やデータ損失なしで、主要ビジネス・アプリケーションの重要なデータをリアルタイムで保護する必要があります。Zero Data Loss Recovery Applianceは、簡単なスケーリングによってデータベースを社内全体で保護し、厳格化するリカバリ・ポイント目標を満たす、シンプルでありながら強力なソリューションでこのニーズに対応します。」

IDC、ストレージ・プラクティス、
プログラム・バイス・プレジデント、
Laura Dubois氏

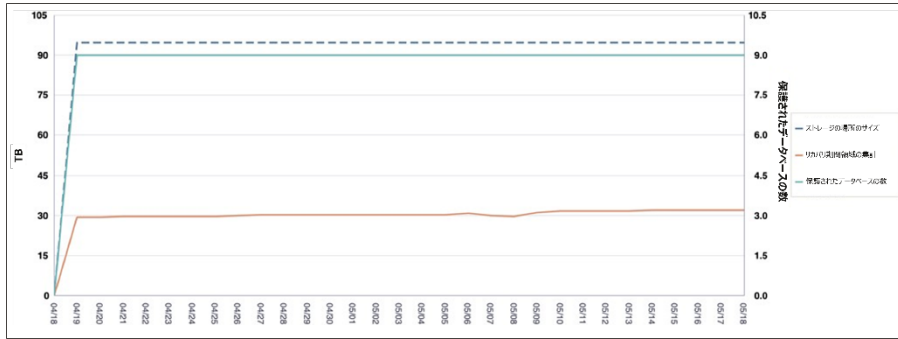


図6: 容量計画 – 保護されたデータベースと領域の使用履歴

Oracle Databaseのデータ保護に対応する統合管理の簡素性は、データベースをRecovery Appliance保護管理に効率的に追加できることから明らかです。

- 新しいデータベースを追加する場合、Recovery Applianceの管理者はEnterprise Managerの"Add Protected Database"ウィザードを使って、データベースを適切な保護ポリシーに関連付け、データベースの資格証明を確立します。
- 次にデータベース管理者はデータベースのEnterprise ManagerのBackup Settings ページを使って、Recovery Applianceをバックアップ先に選択し、リアルタイムのREDO 転送を任意で有効にして継続的にデータを保護します。

ランサムウェアに対するレジリエンスとリカバリ

近年、サイバー攻撃は、多様なアプローチとその破壊的な性質により、すべてのお客様にとって大きな懸念事項となっています。主要な業界アナリストによれば、マルウェアやランサムウェアの被害者は年々倍増しており、たとえば、公開リーク・サイトにデータが流出してしまった被害者は前年の1,300人から1年で2,400人を超えるまでになりました。³ ミッション・クリティカルなデータベースにとって、データの損失やシステムの停止時間につながるこのような攻撃は、収益、業務、評判にとってマイナスになり、違約金を発生させる可能性もあるなど、ビジネス全体に広範囲な悪影響を与える可能性があります。

Recovery Applianceは本番データベースから障害が波及しないように設計されているため、ランサムウェア攻撃が本番データベースを襲っても、アプライアンスが侵害されることはありません。これは、次のような主要なアーキテクチャ特性に起因します。

エンド・ツー・エンドのデータ検証

³ 出典: PwC Cyber Threats 2021:A Year in Retrospect : <https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf>

検証は、バックアップ・ライフサイクル全体を通して破損したバックアップ・データを検出することにおもな役割を果たしますが、ランサムウェア攻撃を受けたデータを検出するためにも等しく重要です。このアプライアンスによって、Oracleブロックの正確性とリカバリ能力について、受信、オンディスク、複製のすべてのバックアップが検証されるため、マルウェアやランサムウェア攻撃の悪影響を受けたバックアップ・データがあれば検出、記録され、管理者にアラートが出されます。その後DBAと連携して、データベースをネットワークから切り離してさらに調査するなどのアクションを取ることができます。さらに、複製されたバックアップは、プライマリ・アプライアンスやその管理者が削除したり変更したりすることはできません。これらはレプリカ・アプライアンスによって独立的に検証および管理されます。したがって、プライマリ・アプライアンスに対する攻撃の影響からは保護されています。代替または補足的な保護戦略として、バックアップはセカンダリ・バックアップ・コピーのための安全な場所としてOracle Cloud Storageにアーカイブし、バックアップ暗号化キーについてはキー・ストアとしてOracle Key Vaultを使用することができます。すべてのバックアップはCloud Storageに暗号化されたまま保存され、リストア操作を実行するにはRecovery ApplianceとOracle Key Vaultにアクセスする必要があります。このアプライアンスは、Oracle Secure Backup経由でファイバ接続のテープ・ライブラリにバックアップをアーカイブすることもできます。アーカイブ・テープは、ネットワークから切り離された、ランサムウェア攻撃を受けにくいオフサイトの場所に発送して保管できます。

不変バックアップ

不変バックアップは、バックアップ・データの不正な、または悪意のある、削除や変更から保護されて整合性を維持します。これは、歴史的には規制に基づくコンプライアンス要件を満たすために重要でしたが、最近では、マルウェアやランサムウェアの攻撃に対する追加の防御層として重要な役割を果たしています。Recovery Applianceは、規定のコンプライアンス保持期間内は不変となるバックアップを強制することができ、文書化されたインターフェースを使用した削除操作や保持期間の短縮は、これらのバックアップには影響を与えません。第2に、バックアップは政府や企業の措置により訴訟ホールドモードにすることができ、ホールドが解除されるまで無期限に保持されます。最後に、不変バックアップをOCIまたはZFS規制コンプライアンス・バケットにアーカイブすることで、より長期的な不変保持期間を設定できます。最終的に、このアーキテクチャは、ローカル・アプライアンスでのバックアップ作成から、DRサイトのレプリカ・アプライアンス、さらにクラウド・ストレージに至るまで、エンド・ツー・エンドの不変ソリューションを効果的に提供します。そのすべてはデータベース環境全体でEnterprise Managerにより一元的に管理および追跡されます。

職務の分離とクォラム・ユーザーの承認

システムへのアクセスは、DBAとアプライアンス管理者のロール間の厳格な職務の分離によって制御されます。DBAには、特権データベースをバックアップおよびリカバリするためのVirtual Private Catalog (VPC) ユーザー・ロールが与えられるだけであり、アプライアンス上のバックアップへのアクセスや、その変更および削除はできません。Recovery Applianceの管理者は、システムを管理および監視するアクセス権のみを有し、保護されたデータベースをバックアップ、リカバリ、または変更することはできません。さらに、アプライアンスは、指名された管理ユーザーを文書化されたインターフェースに制限し、SSHとOSへの直接アクセスを禁止します。これにより、汎用OSユーザー、データベース、その他のサービスが作成されてインストールされるのを防ぐことができます。ルート・アクセスは、クォラム・ユーザーの承認によってのみ許可されます。つまり、他の

2人の指名された管理者ユーザーが、特定の期間、ルート・リクエストを承認する必要があります。

ネットワーク・アクセスの制限

ネットワーク・プロトコルに関しては、VPCユーザーは、SQL*Net経由でのみアプライアンスに接続できます。TLSは、SQL*Net経由で転送中のリアルタイムREDO、およびRecovery Appliance Backup Module (HTTPS) 経由のRMANバックアップとリストアのトラフィックを暗号化するために有効にすることができます。保護されたデータベースからのそれ以外のアクセスは許可されません。さらに、アプライアンスはVLANタグ付きネットワークのサポートによりネットワークの分離を実施し、バックアップとリストアのトラフィックが、保護されたデータベースの特定のネットワーク・ゾーン間で完全に分離され、ルーティング不可になるようにします。このようにして、影響を受ける可能性のあるバックアップが、エンタープライズの他の部分に公開されることはなくなります。

Cyber Vault(サイバー金庫)の導入

バックアップを不正アクセスやランサムウェア攻撃の横展開からさらに分離するために、アプライアンスをCyber Vaultの場所に展開することができます。Cyber Vaultへのデータ送信を、本番の場所にあるアプライアンスからプライベート・レプリケーション・ネットワーク経由でしかできなくします。このネットワークは"エア・ギャップ"として構成できます。つまり、通常Cyber Vaultへの接続は閉ざされ、アクセスがファイアウォール、ゲートウェイ、またはその他のネットワーク管理機能によって制御されます。ネットワークは、レプリケーションによる、Cyber Vaultと新しい本番バックアップとの定期的な同期のためにのみ開かれます。このアプライアンスは、効率的な永久増分バックアップを利用し、結果としてレプリケーションにも使用されるため、開かれている接続期間は非常に短く保たれ、悪意のある侵入の可能性は最小限に抑えられます。さらに、Cyber Vaultアプライアンスの管理者資格証明やEnterprise Managerも、本番アプライアンスとDRアプライアンスの管理者とは完全に分離してセットアップできるため、ロケーション間の職務の分離層を構築できます。すべてのネットワークおよびレプリケーション・アクティビティは、Cyber Vault内から開始できます。Cyber Vaultの導入について詳しくは、Zero Data Loss Recovery Applianceサイバー・セキュリティ・アーキテクチャの資料を参照してください⁴。

優れたレジリエンス

アプライアンス自体も、従来のバックアップ・アプライアンスと比較して、ランサムウェア攻撃に対するはるかに優れたレジリエンス能力を持っています。Exadataハードウェアとストレージ上に構築されたOracle Engineered Systemとして、アプライアンスは、コンピューティング・サーバーとストレージ・サーバーの攻撃領域を削減する、レジリエンスがあるアーキテクチャを継承しています。これには、強化されたパスワード・ポリシー、OSおよびDBユーザーの監査、ファイアウォールのサポート、Oracle ILOM (Integrated Lights Out Management) が含まれます。⁵

Zero Data Loss Recovery

⁴ Zero Data Loss Recovery Applianceサイバー・セキュリティ・アーキテクチャ :

<https://www.oracle.com/technetwork/database/availability/recovery-appliance-cyber-twp-6729502.pdf>

⁵ Oracle Exadata Security Guide : <https://docs.oracle.com/en/engineered-systems/exadata-database-machine/dbmsq/index.html>

関連製品

- Oracle Database 19c、21c
- Oracle Cloud Infrastructure ストレージ
- Oracle ZFS Storage
- Oracle Secure Backup
- Oracleテーブ
- Enterprise Manager
- Oracle Database Zero Data Loss Autonomous Recovery Service

関連サービス

オラクルで利用できるサービスは次のとおりです。

- Oracle Advanced Customer Services
- Oracle Premier Support for Systems
- Oracle Platinum Services
- Oracle Consulting Services

最後に、データベース・サーバーが攻撃を受け、そのバックアップを別のサーバーにリカバリする必要がある場合、Recovery ApplianceのリアルタイムREDO転送によって、攻撃発生直前の最終トランザクションまでリカバリができます。これはランサムウェア攻撃では特に重要です。その攻撃では、犯人の要求に応じて金銭を渡したからといっても、必ずしもデータが元の状態で戻ってくるとは限りません。Recovery Applianceを使用すれば、要求された金銭を支払うことなく、データベースを分離された安全な場所にデータ損失なくリカバリするだけです。

SEC 17a-4 (f) 独立監査人による評価レポート

サイバー攻撃やランサムウェア攻撃の急増は、特に金融サービス部門において意識されており、それに伴い、電子記録の記録と保持に関する要件を定めたSEC規則17a-4 (f) の適用にあらためて注目が集まっています。米国を拠点とする、あるいは米国での業務をサポートするすべての主要な金融機関は、次の5つのおもな要件で構成されるこの規制の対象となる可能性があります。

- 要求されている保持期間中のバックアップの上書きや消去を防ぐ（不変性を維持する）
- バックアップの品質と正確性を自動的に検証する
- バックアップを一意に保存する
- レポートやバックアップの検索用に、すぐに利用できるインデックスを維持する
- バックアップの複製コピーを保存する

大手の情報ガバナンス・コンサルティング会社であるCohasset Associatesは、Recovery Applianceの機能の独自評価を実施し、利用する顧客が上記の規制要件を適正に満たせることを確認しました。レポート⁶では、各要件の詳細と、Recovery Applianceによって各要件をどのように満たすことができるかを示しています。これは金融サービス部門または同様の製品評価を必要とする他の規制業種を問わず、すべての顧客が利用できます。

パブリック・クラウドのOracle Database保護

お客様がクラウドへの移行を検討するときに、Recovery Applianceによって提供されるデータベース保護機能が、OCI上で実行するOracle Databaseサービス向けのZero Data Loss Autonomous Recovery Serviceとともに使用できるようになりました。Recovery Serviceによって、ランサムウェアのリスクを軽減するというビジネス・クリティカルなニーズ、運用効率の向上という財務要件、そしてクラウド・サービスのシンプルさを求めるユーザーの期待に応えることができます。詳細情報と参考資料については、[発表に関するブログ](#)⁷および[製品Webサイト](#)を参照してください。⁸

まとめ：Oracle Database保護の再定義

既存のデータ保護ソリューションはデータベースを、特定のデータの整合性、パフォーマンス、可用性の要件を持つトランザクション・システムとしてではなく、単にコピー対象の汎用ファイルとして扱っているため、重要なデータベースのニーズを満たすことができません。

⁶ Oracle Zero Data Loss Recovery Appliance SEC 17a-4(f) Compliance Assessment Report, Cohasset Associates : <https://www.oracle.com/a/ocom/docs/engineered-systems/recovery-appliance-compliance-assessment-report.pdf>

⁷ Introducing Oracle Database Zero Data Loss Autonomous Recovery Service : <https://blogs.oracle.com/maa/post/introducing-recovery-service>

⁸ Oracle Database Zero Data Loss Autonomous Recovery Service : <https://www.oracle.com/recovery-service>

今日のレガシー・ソリューションでは、ビジネス・データは失われ、エンドユーザーが影響を受け、デプロイメントと管理が複雑で断片化します。

オラクルのZero Data Loss Recovery Applianceは高度なデータ保護テクノロジーをOracle Databaseと緊密に統合して、オンプレミス環境のこれらの課題に対処します。また、クラウド・データベース向けに類似の機能を提供する新しいZero Data Loss Autonomous Recovery Serviceの基盤の役割も果たします。Recovery Applianceは、次のことを実現する革新的な最新手法でデータベース保護環境を再定義します。

- **データ損失の排除**：独自のデータベース統合により、REDOデータをRecovery Applianceに継続的に転送して、最新のトランザクションをリアルタイムで保護できるため、データを失うことなくデータベースをリストアできます。
- **災害からのデータ保護**：Recovery ApplianceはリモートRecovery Applianceにリアルタイムでデータを複製し、定期的にバックアップをクラウドまたはテープにアーカイブすることで、ビジネス・データをサイト停止から保護できます。データベース・ブロックが継続的に検証されるので、転送または処理のどのステージでもデータ破損が排除されます。
- **本番環境への影響の排除**：Oracle Databaseに統合されたバックアップ・アルゴリズムは、変更されたデータだけをRecovery Applianceに送信して、本番データベースへの影響、I/Oトラフィック、ネットワーク負荷を最小限に抑えます。費用のかかるバックアップ処理はすべて、Recovery Applianceにオフロードされます。非生産的なバックアップ期間は不要になり、ビジネス継続性が妨げられることはもうありません。
- **アーカイブ操作のオフロード**：Recovery Applianceはバックアップを低コストなクラウドまたはテープ・ストレージに直接アーカイブできるので、本番データベース・サーバーへの負荷が解消されます。アーカイブ操作は日中と夜間の両方の時間帯で実行できるので、リソースの使用率が向上します。
- **どの時点にもリストア可能**：アプライアンスに保存されたデータベースの変更データを使って、希望するどの時点でも仮想データベース全体コピーを効率的に作成できます。
- **クラウド規模の保護を提供**：単一のRecovery Applianceにより、データセンターまたは地域の数千ものデータベースのデータ保護要件に対処できます。停止時間を設けなくても、容量をペタバイト単位のストレージにシームレスに拡張できます。企業はポリシー・ベースの手法を使ってDatabase Protection as a Serviceを実装できるようになりました。その結果、管理者はエンタープライズ・データベース保護の状態をいつでもエンド・ツー・エンドで表示できます。
- **ランサムウェアに対するフォルト・トレランス**：アプライアンスは、本番データベースとは別の、独立して管理されるシステムであり、ランサムウェア攻撃に対するレジリエンスを考慮して設計されています。すべての受信、保存、送信バックアップ・データは、Oracleブロックの正確性について継続的に検証されます。これにより、侵害されたデータがあればすぐにアラートを受け取れます。不変保持期間は、データベース・レベルで設定して、重要なバックアップの悪意ある削除や変更を防ぐことができます。ユーザー・アクセスに関しては、DBAとアプライアンス管理者の間で職務の分離が厳格に実施されます。DBAは、バックアップ/リストアのみを行うことができ、バックアップの削除やアプライアンスの変更にはアクセスできません。管理者はその逆で、アプライアンスを管理しますが、データベースのバックアップ/リストアを行うアクセス権限はありません。さらに、複製されたバックアップはプライマリ・バックアップから独立して管理および検証されるため、プライマリ・アプライアンスへの攻撃により悪影響を受けたデータの影響を受けることはありません。システム・アクセス自体は、日常業務へのアクセスを制限し、ルート・アクセスを禁止する、指名された管理者のユーザー・モデルによって保護および記録されます。バックアップ・データをさらに分離するために、アプライアンスはエア・ギャップのあるCyber Vaultの場所に、個別のユーザー・アクセス資格証明とともに展開することができ、必要な場合には、永久増分レプリケーションによって本番バックアップと効率的に同期させることができます。

このアプライアンスは、業界をリードするExadataインフラストラクチャを活用し、強固なパスワードポリシー、きめ細かなアクセス制御、包括的な監査、セキュアな完全自動管理を実現することで、さまざまなレジリエンスと監視機能を提供します。最後に、本番データベース自体が攻撃によって侵害された場合、Recovery Applianceを使用して、攻撃時点までのすべてのトランザクションを含むすべてのデータを、別の安全な場所にリストアできます。

Recovery Appliance RA23サーバー・ハードウェア

サーバー・タイプ	ストレージ	ネットワーク
コンピューティング・サーバー (ラックあたり 2台)	2 x NVMeフラッシュSSD (ホットスワップ対応)	<ul style="list-style-type: none"> • 2 x デュアル・ポート10/25 GbイーサネットSFP28 <ul style="list-style-type: none"> ○ 2 x 10/25 Gb光 (取込み) ○ 2 x 10/25 Gb光 (レプリケーション) • 2 x デュアル・ポート100 GbイーサネットQSFP28 <ul style="list-style-type: none"> ○ 2 x 100 Gb光 (取込み) ○ 2 x 100 Gb光 (レプリケーション) • 1 x クアッド・ポート10 GbイーサネットRJ45 <ul style="list-style-type: none"> ○ 2 x 10 Gb銅 (取込み) ○ 2 x 10 Gb銅 (レプリケーション) • Sun Storage Dual 32 Gbファイバ・チャネルPCIe Universal HBA、QLogic (テープ接続用オプション) • 2 x 100 Gb QSFP28 RoCEファブリック・ポート • 1 x 1 Gbイーサネット銅ポート (管理) • 1 x ILOMイーサネットポート • 2 x 10 Gbポート、2 x 25 Gbポート、または2 x 100 Gbポート (最大)、インジェスト・ネットワーク用 • 2 x 10 Gbポート、2 x 25 Gbポート、または2 x 100 Gbポート (最大)、レプリケーション・ネットワーク用
ストレージ・サーバー	12 x 22 TB 7,200 RPMディスク 2 x NVMeフラッシュ・ アクセラレーション・カード	<ul style="list-style-type: none"> • 2 x 100 Gb QSFP28 RoCEファブリック・ポート • 1 x 1 Gbイーサネット銅ポート (管理) • 1 x ILOMイーサネットポート

¹すべてのサーバーに、冗長化されたホットスワップ対応ファンと電源が組み込まれています。

Recovery Appliance RA23の構成

ラック・サイズ	コンピューティング・サーバー	ストレージ・サーバー	使用可能な容量 (標準冗長性)	使用可能な容量 (高冗長性)
ベース・ラック	コンピューティング・サーバー x 2	ストレージ・サーバー x 3	274 TB	174 TB
+ストレージ・サーバー	該当なし	最大14台の追加ストレージ・サーバー	ストレージ・サーバーあたり92 TB	ストレージ・サーバーあたり60 TB

¹各ラックの高さは42 RU (ラック・ユニット) で、冗長配電ユニット (PDU) 2台、36ポート100 Gb/秒RoCEスイッチ2個、および管理用に48ポート管理イーサネット・スイッチ1個を収容します。
単一ラックに最大17台のストレージ・サーバー。フル・ラックの使用可能容量:

- 標準冗長性: 1.57 PB
- 高冗長性: 1 PB

フル・ラックのバックアップおよびリストアのスループット:

- 100 Gb x 4 (コンピューティングあたり100 Gb LACPのボンディング x 2) : 35 TB/時
- 25 Gb x 4 (コンピューティングあたり25 Gb LACPのボンディング x 2) : 24 TB/時
- 10 Gb x 4 (コンピューティングあたり10 Gb LACPのボンディング x 2) : 12 TB/時

Recovery Appliance RA23ストレージ・サーバーの環境仕様

メトリック	仕様
高さ	86.9 mm (3.42インチ)
幅	445.0 mm (17.52インチ)
奥行き	759.0 mm (29.88インチ)
騒音 (動作時)	8.1 B
重量	31.3 kg (69ポンド)
最大消費電力	0.5 kW (0.5 kVA)
標準消費電力 ¹	0.4 kW (0.4 kVA)
最大使用時の冷却能力	1,825 BTU/時
	1,926 kJ/時
標準使用時の冷却能力	1,278 BTU/時
	1,348 kJ/時
最大使用時のエアフロー ²	85 CFM
標準使用時のエアフロー ²	59 CFM

動作時温度/湿度: 5 °C~32 °C (41 °F~89.6 °F)、10%~90%相対湿度、結露なし
動作時高度: 最大3,048 m (高度900 m以上では300 m上昇するごとに最大周囲温度が1 °C低下)
¹標準消費電力は、アプリケーションの負荷によって変わります。
²エアフローは前面から背面へと流れる必要があります

Recovery Appliance RA23の環境仕様

メトリック	ベース・ラック	フル・ラック
高さ	2,000 mm (78.74インチ)	
幅	601 mm (23.66インチ)	
奥行き	1,197 mm (47.13インチ)	
騒音 (動作時)	9.1 B	9.5 B
重量	418.6 kg (922.8ポンド)	934.4 kg (2,060.0ポンド)
最大消費電力	4.0 kW (4.1 kVA)	11.5 kW (11.8 kVA)
標準消費電力 ¹	2.8 kW (2.9 kVA)	8.1 kW (8.2 kVA)
最大使用時の冷却能力	13,782 BTU/時 (14,540 kJ/時)	39,339 BTU/時 (41,502 kJ/時)
標準使用時の冷却能力	9,647 BTU/時 (10,178 kJ/時)	27,537 BTU/時 (29,052 kJ/時)
最大使用時のエアフロー ²	638 CFM	1,821 CFM
標準使用時のエアフロー ²	447 CFM	1,275 CFM

動作時温度/湿度: 5 °C~32 °C (41 °F~89.6 °F)、10 %~90 %相対湿度、結露なし
 動作時高度: 最大3,048 m (高度900 m以上では300 m上昇するごとに最大周囲温度が1 °C低下)
¹ 標準消費電力は、アプリケーションの負荷によって変わります。
² エアフローは前面から背面へと流れる必要があります。

Recovery Appliance RA23 : 準拠規格と認定規格

準拠規格 ^{1, 2, 3}	安全性:	UL/CSA 60950-1, EN 60950-1, IEC 60950-1 CB Scheme (各国の規定に準拠) UL/CSA 62368-1, EN 62368-1, IEC 62368-1 CB Scheme (各国の規定に準拠)
	EMC	
	排出量:	FCC CFR 47 Part 15, ICES-003, EN55032, KN32, EN61000-3-11, EN61000-3-12
	イミュニティ:	EN55024, KN35
認定規格 ^{2, 3}		NRTL (北米)、CE (欧州連合)、International CB Scheme、HSE Exemption (インド)、BSMI (台湾)、CCC (PRC)、EAC (ロシアを含むEAEU)、KC (韓国)、RCM (オーストラリア)、VCCI (日本)、UKCA (イギリス)
EU指令 ³		2014/35/EU 低電圧指令、2014/30/EU EMC指令、2011/65/EU RoHS指令、2012/19/EU WEEE指令

¹ 言及した準拠規格と認定規格はすべて、最新の正式版です。詳細については、販売担当者にお問い合わせください。
² その他の国の準拠規格/認定規格が適用される場合もあります。
³ 準拠規格や認定規格の遵守は、シールドレベルのシステムのみで実現されている場合があります。

Recovery Applianceサポート・サービス

- ハードウェア保証：1年間、通常営業時間内（月～金の午前8時から午後5時まで）に4時間のWeb/電話対応、2営業日のオンサイト対応/パーツ交換
- Oracle Premier Support for Systems：Oracle Linuxのサポートと、24時間365日のサポート、2時間のオンサイト・ハードウェア・サービス対応（サービスセンターまでの距離による）
- Oracle Premier Support for Operating Systems
- Oracle Customer Data and Device Retention
- システム設置サービス
- ソフトウェア構成サービス
- Oracle Platinum Services
- Business Critical Service for Systems
- システム・アップグレード・サポート・サービス（ハードウェアの取り付けとソフトウェアの構成を含む）
- Oracle Auto Service Request（Oracle ASR）

お客様が用意したイーサネット・スイッチをRecovery Applianceにインストールするオプション

各Recovery Applianceラックの上部には2Uサイズの空きがあり、お客様は、独自のクライアント・ネットワークのイーサネット・スイッチを、別個のラックではなくアプライアンス・ラックにインストールできます。設置スペース、電力、冷却に関する一部の制限が適用されます。

Connect with us

+1.800.ORACLE1までご連絡いただくか、[oracle.com](https://www.oracle.com)をご覧ください。北米以外の地域では、[oracle.com/contact](https://www.oracle.com/contact)で最寄りの営業所をご確認いただけます。

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle

Copyright © 2023, 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、ここに記載されてい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。

本デバイスは、連邦通信委員会のルールに基づいた認可を未取得です。認可を受けるまでは、このデバイスの販売またはリースを提案することも、このデバイスを販売またはリースすることはありません。

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。0723

免責事項：データ・シートにこの免責事項の記載が必要かどうか分からない場合は、収益認識方針を参照してください。ホワイトペーパーの内容と免責事項の要件についてさらに質問がある場合は、REVREC_US@oracle.com宛てに電子メールでご連絡ください。