ZFS STORAGE APPLIANCE

Oracleテクニカル・ホワイトペーパー
2014年11月

Oracle ZFS Storage Applianceでの暗号化の導入と暗号化鍵の管理に関するベスト・プラクティス

目次

はじめに 4
暗号化の使用が重要な理由 4
暗号化のおもな概念 4
Oracle Transparent Data Encryption. 6
ZFSの暗号化 6
Oracle ZFS Storage Applianceでの鍵の管理. 7
鍵管理権限の定義. 8
ローカル鍵管理のためのロール認可の定義 8
Oracle Key Managerによる鍵管理. 8
Oracle ZFS Storage Applianceでの暗号化の設定. 9
キーストアの設定 9
ローカル・キーストアの設定. 9
Oracle Key Managerキーストアの設定 10
Oracle Key Managerの初期構成セットアップ手順の実行. 12
暗号化シェアの作成 16
バックアップによるキーストアの保護. 18
ローカル・キーストアのバックアップの作成 18
Oracle Key Managerキーストアのバックアップの作成 18
暗号化シェアのスナップショットとクローンの作成. 19
暗号化シェアのレプリケーション 19
暗号化使用時のベスト・プラクティス 19
データ・セキュリティ・アーキテクチャ. 19
ネットワーク・アーキテクチャの設計. 20
Oracle Key Managerのアーキテクチャの設計. 20
ラッピング鍵のバックアップの作成 20
暗号化されたデータシェアのバックアップとリストア. 20
シェアのレプリケーションの使用 21
暗号化されていないシェアと暗号化されているシェアとの間の移行. 22
暗号化シェアでの重複排除/圧縮の併用. 22
さまざまな暗号化オプションのパフォーマンスに関する考慮事項. 23

データベース・リポジトリを使用するアプリケーションに対する推奨事項 23
鍵管理のベスト・プラクティス 24
鍵の保護を徹底する 24
定期的に鍵を変更する 24
鍵の割当て方法と割り当てるユーザーを管理する 24
鍵の範囲を決める 25
付録A：参考資料 26
付録B：略語および用語の索引 27

はじめに

データの暗号化について検討する場合、データには保存された状態と転送されておる状態の2種類の状態があることを意識することが重要です。このような2つの状態のデータには、それぞれ異なる暗号化テクノロジーを使用する必要があります。保存データは、暗号化してディスクまたはテープに格納されます。転送データの場合は、送信元と送信先の間のデータ通信に使用するトランスポート・レイヤーで暗号化を行います。このホワイトペーパーでは、Oracle ZFS Storage Appliance上の保存データの暗号化についてのみ説明します。

保存データを暗号化すると、データ記憶媒体の悪用による不正アクセスから個人または企業の極秘情報が保護されます。また、ハードウェア障害やハードウェア・アップグレードによりデータ記憶媒体を交換する場合は、コストをかけずにデータ記憶媒体を安全に破棄できます。データの暗号化に使用されていた暗号化鍵を破棄すれば、データは安全に消去されたと見なされます。

このホワイトペーパーでは、Oracle ZFS Storage Applianceの暗号化機能の導入方法、関連する鍵の管理、およびこれらの機能の実装に関するベスト・プラクティスについて説明します。

暗号化の使用が重要な理由

個人データや企業の極秘データを含むさまざまなデータを不正アクセスから保護するうえで、暗号化は重要な要素です。政府の各種機関は現在、IT環境内のデータ・ストレージ・デバイスに暗号化を使用することを義務づけ始めています。

データ機密保護違反が発生すると、組織は次のような深刻な影響を受ける恐れがあります。

- 評判の失墜
- 罰金や事業損失による財政面への打撃
- 訴訟（特に民事訴訟）を起こされるリスク

保存データを暗号化することは、こうしたリスクを軽減するための比較的簡単で効果的な解決策です。

暗号化のおもな概念

データの暗号化は不正アクセスからデータを保護する場合に使用されます。暗号化テクノロジーには、さまざまなアルゴリズムを使用した鍵方式の暗号化があります。どのテクノロジーも目的は、情報を保護することです。それには、情報を読取り不能な形式にエンコードしたり、対象とするユーザーまたはサービス以外は読取りや処理ができない形式でデータの格納や送信を行う方法を使用します。次に示すのは、個別の鍵暗号化セキュリティ・サービスです。

機密保護　暗号化テクノロジーを使用して機密保護機能を提供します。ほとんどの場合、データは対称鍵を使用して暗号化されます。

認証　暗号化された認証アイテムを提供することで、リソースへのアクセスを要求に対してアイデンティティを検証します。アイデンティティはデジタル証明を使用して検証されます。

整合性　データが変更されたり操作されたりしていないか検証するときに使用されます。暗

号化ハッシング・アルゴリズムは、データが本物であるかどうかを判定するために必要なデータ固有の識別情報を作成するときに使用されます。

否認防止　メッセージの送信元を証明するサービスです。メッセージが送信されるときに、送信者を識別するメッセージ固有の識別情報がメッセージにタグ付けされます。

適切なビジネス・セキュリティ・プランには、上記4つのセキュリティの項目がすべて含まれています。

データ暗号化は、2つのタイプのデータ、すなわち転送データと保存データに適用できます。エンド・ツー・エンドのデータ・セキュリティを提供するには、両方に対処する必要があります。

転送データを暗号化する場合は認証を組み合わせることが多く、送信者と受信者のアイデンティティ、および相互にデータを交換するために必要な権限を両者が持っているかどうかを認証時に判定します。

保存データを暗号化すると、記憶媒体を悪用された場合でも、不正アクセスからデータを保護できます。オペレーティング・ストレージ・サブシステムでの不正アクセスからデータを保護するには、LDAPやActive Directoryのような適切な認証システムを使用する必要があります。

データ・ストレージの暗号化は保存データ、すなわちディスクまたはテープに対して実行されます。データへのアクセスは暗号化鍵を使用して制御されます。ストレージ・サブシステムは、特定のシェア上のデータを暗号化するときに使用された暗号化鍵を使用して、そのシェアのデータにアクセス（復号化）します。

データ・ストレージを暗号化する方法はいくつかあります。

- ディスク・ハードウェアまたはテープ・ハードウェアに埋め込まれた暗号化機能を使用する方法
  この方法を使用する場合は高価なストレージ・デバイスが必要なうえに、鍵の管理が複雑になります。また、暗号化を適用できる範囲が制限されます。
- ディスク・ストレージ・サブシステムとアプリケーションとの間で暗号化アプライアンスを使用する方法
  既存のインフラストラクチャに暗号化を実装する必要がある場合は、この方法を検討する価値があります。ただし、データのパフォーマンス・ボトルネックになる可能性があったり、鍵の管理に関わるデバイスとベンダーが増えて複雑になる問題があります。
- サーバーまたはデスクトップ上で暗号化ソフトウェアを使用する方法
  これは、テープの紛失や盗難に起因する不正アクセスからデータを保護することを目的に、ローカルに保管されているデータやバックアップ・ソフトウェアを暗号化する方法で、モバイル機器やサーバーでよく使用されます。ディスク・ドライブの交換時やハードウェアの紛失時または盗難時に不正アクセスが発生するリスクからデータを保護するには、サーバーまたはクライアントに個別のソフトウェアをインストールする必要があります。サーバーまたはデスクトップごとに暗号化ソフトウェアが必要であるため、コストが高くなり、管理がしにくくなります。

- ストレージ・サブシステムに暗号化を埋め込む方法。
  データの暗号化と鍵の管理はストレージ・サブシステムで行われます。ハードウェア・コンポーネントやソフトウェア・コンポーネントを新たに追加する必要はありません。暗号化はストレージ・サブシステムのコントローラ・レベルで実施されます。ある種のシーケンシャルワークロードの場合はパフォーマンスに影響が出る場合がありますが、パフォーマンスへの影響をはるかにしのぐ低コスト、柔軟性、容易な鍵管理というメリットがあります。
- データベース・レイヤーに埋め込む方法。データベース・レイヤーで暗号化を使用すると、特定のデータベース列またはアプリケーション・データベース全体を暗号化できるようになるほか、関連するデータベース管理ツールとユーザー認証機能を緊密に統合できます。

Oracle ZFS Storage Applianceのような新しいストレージ・サブシステムには、ストレージ・サブシステムのパフォーマンスに著しい影響を与えずに暗号化機能や鍵管理機能を処理できるだけのCPU性能があります。したがって、高価な専用の暗号化デバイスや追加の暗号化アプライアンスを使用する必要はありません。

外部鍵の管理については、すべてのデータ・ストレージ暗号化コンポーネントの鍵を一元管理できるOracle Key Managerソリューションで対応できます。Oracle Key Managerをクラスタ化すれば、暗号化鍵の紛失や鍵管理サーバーの障害によるデータ・アクセスの喪失を防止できます。

鍵管理の権限は、鍵管理ポリシー・ロールごとに定義されます。ユーザーには、それぞれの業務責任に適合する一定のロールを付与できます。

Oracle Transparent Data Encryption

Oracle Transparent Data Encryption（Oracle TDE）はデータの暗号化とユーザー認証を緊密に統合するソリューションです。TDEは、保存データをデータベース・レイヤーで暗号化することで、潜在的な攻撃者がデータベースをバイパスしてストレージから機密情報を読み取ることを阻止します。データベース認証が済んだアプリケーションおよびユーザーは、（アプリケーション・コードまたは構成変更なしで）透過的にアプリケーション・データへのアクセスを維持することができますが、表領域ファイルから機密データを読み取ろうとするOSユーザーによる攻撃や、盗み取ったディスクまたはバックアップから情報を読み取ろうとする窃盗犯の攻撃によるクリアテキスト・データへのアクセスは拒否されます。TDEは、Oracle Advanced Compression、Oracle Automatic Storage Management（Oracle ASM）、Oracle Recovery Manager（Oracle RMAN）、Oracle Data Pump、Oracle GoldenGateなど、頻繁に使用されるOracle Databaseの各種ツールやテクノロジーに直接統合されています。

ZFSの暗号化

Oracle ZFS Storage Applianceでは、Oracle ZFSのファイル・システム機能を使用してデータ・ストレージ暗号化機能を提供します。使用するのは、堅牢なAdvanced Encryption Standard（AES）128、192および256ビットの2層セキュリティ鍵アーキテクチャです。このアーキテクチャの中で、ZFS暗号化鍵は2つ目の256ビット暗号化レイヤーでさらにラッピングされ、ラッピング鍵として存在します。1つの鍵をシステム全体で使用したり、プロジェクトごとやシェア/LUNレベルごとに1つの鍵を使用できます。

1つのシェアについて暗号化を有効にすると、そのシェア上のすべてのデータと関連メタデータ（アクセス制御リスト（ACL）や割当て制限情報など）が暗号化されて、そのシェアに割り当てられているディスクに格納されます。ZFSプールには暗号化シェアと非暗号化シェアの両方を含めることができます。この暗号化サービスは他のファイル・システム・サービス（圧縮、重複排除など）とプロトコル（CIFS、NFSなど）に対して完全に透過的です。

ZFSシェアの暗号化と鍵管理は、ZFSプロパティ構造を通じて制御されます。つまり、通常のZFSプロパティの継承ルールがここでも適用されます。

データ暗号化鍵は、シェアデータの暗号化と復号化の実行に使用されます。暗号化鍵はシェアの作成時にZFSによって生成され、暗号化された状態でシェア内に格納されます。ラッピング鍵はデータ暗号化鍵の暗号化と復号化に使用されます。ZFSがシェアをマウントするときに、シェアへのアクセス権を取得するために使用するのが、このラッピング鍵です。データ鍵が復号化された後は、シェアがアンマウントされるかラッピング鍵が削除されるまで、この鍵はZFSのキャッシュに保持されます。

Oracle ZFS Storage Appliance上でデータ暗号化を使用する場合は、シェア内のデータの暗号化/復号化に使用されるZFS鍵を鍵管理者が管理する必要は一切ありません。鍵管理者は、キーストアに格納されているラッピング鍵を管理します。

Oracle ZFS Storage Applianceは、Oracle ZFS Storage Appliance上のローカル・キーストアと、Oracle Key Managerが管理するキーストアの両方をサポートしています。

シェア/LUNの暗号化が有効な場合は、そのラッピング鍵の値を変更できます。データ暗号化鍵は単純に再暗号化され、データ暗号化鍵を新たに暗号化した値がディスク上のシェア/LUNのZFSメタデータ内に格納されます。データ暗号化鍵の値そのものは変更できません。

ラッピング鍵を削除すると、そのラッピング鍵を使用している関連シェアも自動的にオフラインになります。（万が一、誤ってラッピング鍵を削除してしまっても、）バックアップからラッピング鍵をリストアすれば、シェアは自動的にオンラインに戻ります。ラッピング鍵を完全に削除した場合は、関連するシェア上のデータへのアクセスが失われ、データはセキュアに消去されたものと見なされます。

クラスタ構成のOracle ZFS Storage Applianceでは、2つのノード間で自動的にキーストアが同期化されます。キーストアでラッピング鍵を追加、削除、更新すると、クラスタに含まれる両方のノードでキーストア全体が更新されます。

注：Oracle ZFS Storage ApplianceのドキュメントやBUI/CLIでは、ラッピング鍵を‘暗号化鍵’と呼ぶことがあります。

Oracle ZFS Storage Applianceでの鍵の管理

暗号化シェアへのアクセスの有効化に使用されるラッピング鍵はすべて、Oracle ZFS Storage Applianceのキーストアに保持されます。したがって、キーストアの鍵を管理することが鍵の管理ということになります。Oracle Key Managerのキーストアを使用する場合は、Oracle ZFS Storage Applianceが使用するOracle Key Managerの鍵グループに含まれる鍵も管理する必要があります。鍵管理ポリシーとこのポリシーに関連付ける管理権限は、組織全体の鍵管理ポリシー（KMP：Key Management Policy）および関連する鍵管理運用規定（KMPS：Key Management Practices Statement）の一環として規定する必要があります。このようなドキュメントには、認可および保護の対象と、暗号データの生成、配布、アカウンティング、保管、使用および廃棄に適用する制約を含める必要

があります。

米国商務省所管の国立標準技術研究所（NIST：National Institute of Standards and Technology）が、鍵管理に関する勧告文書（**Recommendation for Key Management**（Draft NIST Special Publication 800-57））を発行しています。暗号化鍵管理の使用、およびKMPとKMPSに関するドキュメントの要件についての詳しいガイダンスは、この文書に記載されています。

鍵管理権限の定義

NISTの要件に合わせて監査、管理、セキュリティの各職務を分離するために、複数の権限（ロール）を作成し、それぞれ異なるユーザーに割り当てることができます。

ローカル鍵管理のためのロール認可の定義

Oracle ZFS Storage Applianceではローカルでの管理とOracle Key Managerのキーストアを管理するために、次のロールが定義されています。

ロールID	説明	
Keystore	キーストアの管理に関連するすべての認可オプションが含まれます	
	認可の種類	説明
	listKeystore	キーストアに存在する鍵をリストします
	modifyKeystore	キーストアの修正を許可します
	readKeystore	キーストア内の機密値への読取りアクセスを許可します

Oracle Key Managerによる鍵管理

Oracle Key Managerのキーストアでは、種類の異なる複数のクライアントの鍵が一元管理されるため、Oracle Key Managerノードにはさらに多くのロールが存在します。Oracle ZFS Storage Applianceのエージェントを Oracle Key Managerで設定する際には、これらのロールを考慮する必要があります。各種ロールとその機能を次に示します。それぞれの例については次の項で説明します。

ロールID	説明
監査者	KMAクラスタに関する情報を表示します
バックアップ・オペレータ	バックアップを実行します
コンプライアンス責任者	鍵ポリシーと鍵グループを管理します
オペレータ	エージェント、データ・ユニット、鍵を管理します
定足数メンバー	定足数の承認が必要な保留中の操作の資格証明を表示および追加します
セキュリティ責任者	セキュリティ設定、ユーザー、サイトおよび転送パートナーを管理します

Oracle ZFS Storage Applianceでの暗号化の設定

Oracle ZFS Storage Applianceで暗号化を設定する場合は、次に示す構成要件および関連オプションを考慮する必要があります。

キーストアの設定

Oracle ZFS Storage Applianceで暗号化シェアを使用するには、アプライアンス上にキーストアを設定する必要があります。ZFSで使用するデータ暗号化鍵へのアクセスに使用されるラッピング鍵は、キーストアで保持します。Oracle ZFS Storage Applianceでは、シェアごとに固有の暗号化鍵を保持します。この暗号化鍵は、暗号化されてからシェアのメタデータに格納されます。ラッピング鍵はこの鍵の暗号化と復号化に使用されます。

キーストアには、ローカル・キーストアとOracle Key Managerキーストアの2種類があります。アプライアンス自体でラッピング鍵を管理および格納する場合は、ローカル・キーストアを使用します。Oracle Key Managerキーストア・オプションを使用する場合は、Oracle Key Manager上でラッピング鍵の生成と管理を行います。

ローカル・キーストアを使用するメリットは、ハードウェアを追加しなくても暗号化機能を使用できることです。ラッピング鍵のセキュア・バックアップやラッピング鍵のリサイクルのような鍵管理機能は、暗号化機能を使用するOracle ZFS Storage Applianceごとに慎重に管理する必要があります。

Oracle Key Managerで一元管理するラッピング鍵は、エージングのポリシーを自動化して使用します。Oracle Key Managerをクラスタ構成にして使用すると、ラッピング鍵が格納されているノードの喪失によるラッピング鍵の紛失を防ぐことができます。なお、ラッピング鍵を紛失すると、そのラッピング鍵を使用していたシェア上のデータも失われます。つまり、シェアはセキュアに消去されたと見なされます。

キーストアおよび暗号化シェアを設定する前に、鍵の管理と暗号化シェアのバックアップ計画の要件について検討する必要があります。

暗号化鍵の格納および管理に使用するビジネス・ポリシーはどのような内容なのか。そのポリシーでは、ストレージ・サブシステム内で鍵の格納と管理を行うことを許可しているのか。それとも、一元管理や別の場所からの管理が必要なのか。こうした情報から、ローカルとリモートのいずれのキーストアを使用できるかが決まります。

使用するキーストアをローカルとリモートのいずれにするかを決定する2つ目の要素は、バックアップの暗号化に関する要件です。テープ・バックアップにデータ暗号化を使用する場合は、Oracle StorageTek T10Kを使用する必要があります。ユーザーの鍵管理ポリシーによりますが、Oracle ZFS Storage Appliance上のデータと同じOracle Key Manager鍵ライフサイクル・ポリシーをテープ・バックアップでも使用できます。

これらのトピックについては、ベスト・プラクティスの項で詳しく説明します。

ローカル・キーストアの設定

ラッピング鍵は、Master Passphraseから生成されたAES 256ビット鍵を使用して暗号化したうえでローカル・キーストアに格納されます。Master Passphraseは、キーストアを作成するときに指定する必要があります（次のOracle ZFS Storage Appliance BUIスクリーンショット参照）。

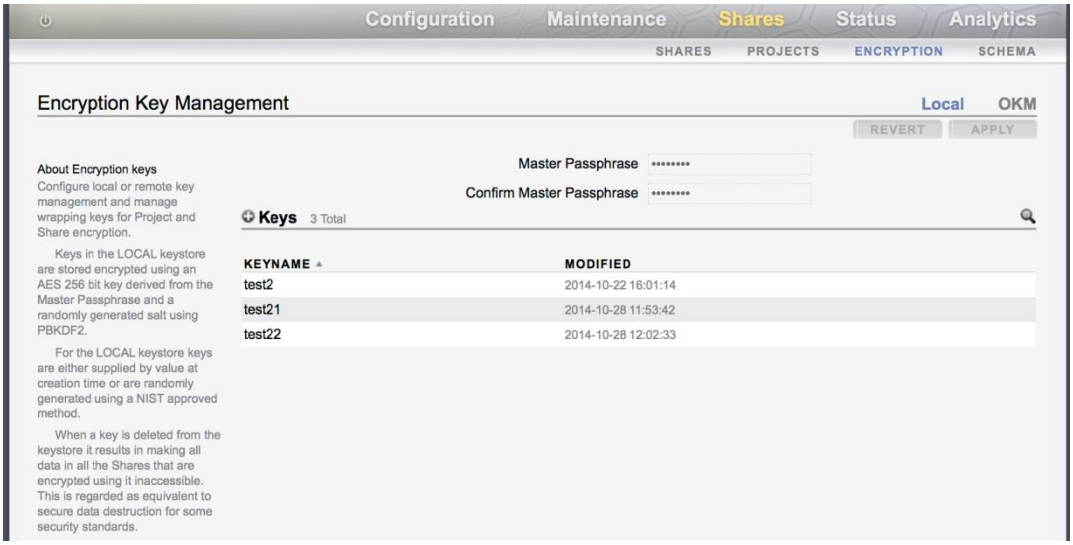

図1.Oracle ZFS Storage Appliance BUIでのローカル・キーストアの構成

キーストアの作成が完了したら、ランダム鍵を生成する方法か作成時に値を指定する方法で、キーストアに鍵を追加できます。

Oracle Key Managerキーストアの設定

Oracle Key Manager（Oracle ZFS Storage BUIではOKM）は、鍵の配布と鍵の保存を一元的に設定および管理することができます。

Oracle Key ManagerにOracle ZFS Storage Applianceをエージェントとして登録する前に、Oracle Key Managerが適切に構成されているかどうか、またOracle Key ManagerのGUIにアクセスできるかどうかを確認する必要があります。鍵管理アプライアンス（KMA）の監視と構成はOracle Key ManagerのGUIを使用して実行できます。KMAには2つのネットワーク接続が必要です。1つは管理ネットワークに接続するためのもので、もう1つはいわゆるサービス・ネットワークです。次の図に示すように、それぞれに異なるサブネットの設定を推奨します。

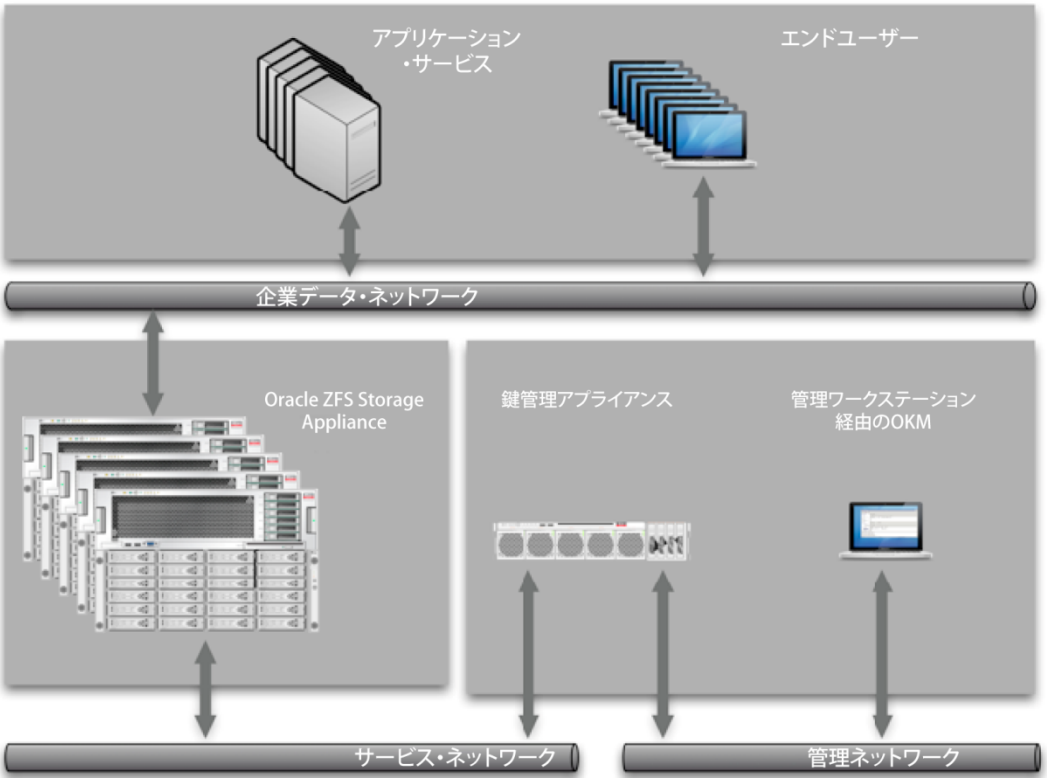

図2. 適切に構成された鍵管理システム・コンポーネントの概略図

GUIからKMAへは管理ネットワークを経由して接続します。サービス・ネットワークは、KMAとそこに登録されているエージェント（この例ではOracle ZFS Storage Appliance）との間で鍵を交換する場合の通信に使用されます。

構成プロパティの設定は次の手順に従う必要があります。

1. 鍵ポリシーの定義、鍵グループの設定、サイトの場所の設定、エージェントの登録ができるロールを持つユーザーを（1人以上）設定します。
2. サイトの場所を設定します。これは、Oracle ZFS Storage ApplianceをOracle Key Managerに登録するときに使用します（オプション）。この設定にはOracle Key Managerセキュリティ責任者のロール資格証明が必要です。
3. 鍵ポリシーを設定します。鍵グループを作成するときに使用します。この設定にはコンプライアンス責任者のロール資格証明が必要です。
4. 鍵グループを設定します。Oracle ZFS Storage ApplianceをOracle Key Managerに登録するときに使用します。この設定にはOracle Key Managerコンプライアンス責任者のロール資格証明が必要です。
5. KMA（鍵管理アプライアンス）ノードを1つ使用する場合は、Oracle Key Managerの鍵のバックアップを取り、KMAで使用する鍵を解放できるようにします。バックアップの作成後、KMA上の鍵は*generated（生成済み）の状態*からready（準備完了）の状態に変わります。

Oracle ZFS Storage Applianceで鍵を要求できるようにするには、KMA上の鍵が*readyの状態*に変わっている必要があるため、この手順は重要です。この設定にはOracle Key Managerバックアップ・オペレータのロール資格証明が必要です。

6. Oracle ZFS Storage Applianceを登録します。この設定にはOracle Key Managerオペレータのロール資格証明が必要です。
7. Oracle ZFS Storage Applianceで、Oracle Key Managerからラッピング鍵を要求します。これにはユーザーrootの資格証明、または‘Permit keystore modification’認可を含むロールを持つOracle ZFS Storage Applianceのユーザーが必要です。

Oracle Key Managerの初期構成セットアップ手順の実行

次の例では、1人のユーザーを作成して複数のロールを割り当て、前述した構成手順をすべてこのユーザーで実行できるようにしています。実際の運用では、1人のユーザーが複数の権限ロールを所有できないようにするほうがよいでしょう。

Oracle Key Managerに登録するOracle ZFS Storage Applianceをサービス・ネットワーク・サブネットに接続します。

Oracle Key Managerの設定がすでに完了していて、ユーザー、鍵ポリシー、鍵グループの構成がすでに済んでいる場合は、最初の方の手順を飛ばして手順6（Oracle ZFS Storage ApplianceをOracle Key Managerエージェントとして登録）から開始してください。

1. Oracle Key Managerの管理ユーザーを作成します。

   必須ロールを持つユーザーがまだKMAに存在しないことを確認します。存在しない場合は、図に示すロールを有効にした新しい管理ユーザーを作成します。

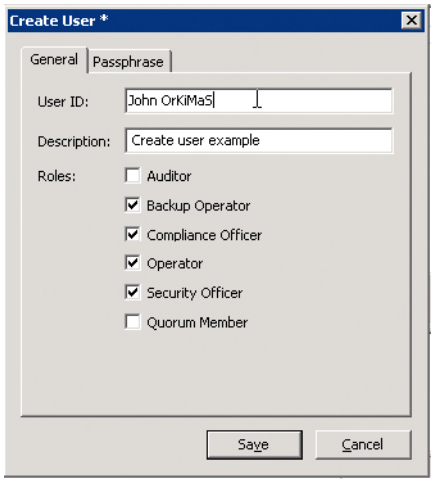

図3. Oracle Key Managerの必須ロールを持つユーザーの作成

2. サイトの場所を作成します（オプション）。

   Oracle ZFS Storage Applianceを別のサイトまたは建物に設置している場合は、サイトの場所を使用することをお勧めします。

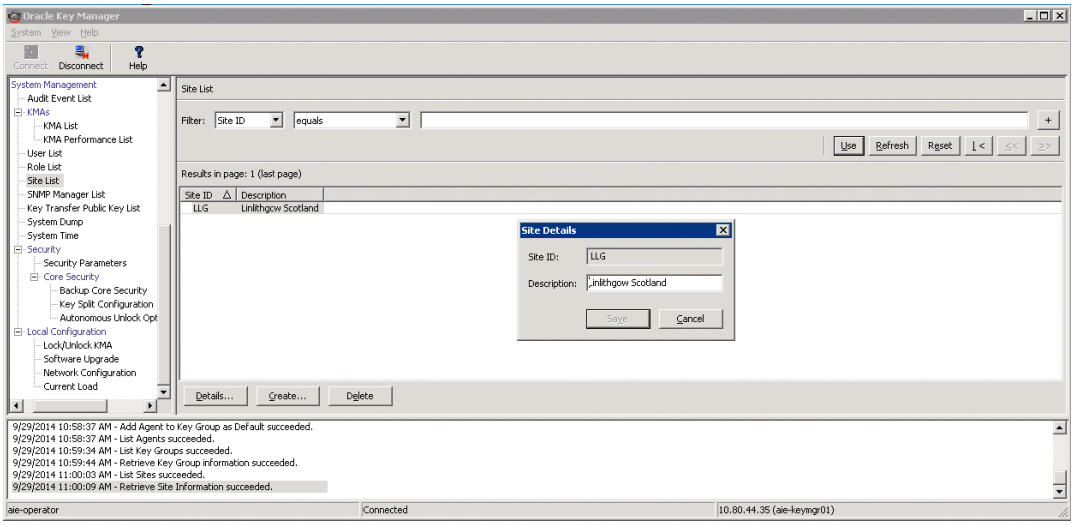

図4. Oracle Key Managerでのサイトの場所の詳細設定

3. 鍵ポリシーを作成します。

   鍵ポリシーを設定し、要件に適合する保存方針を選択し、必要に応じて‘Allow Import To’オプション、‘Allow Export From’オプションを有効にします。

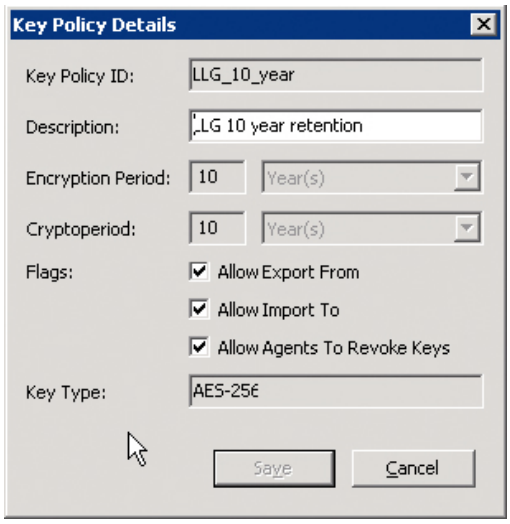

図5. Oracle Key Managerでの鍵ポリシーの詳細設定

オプション‘Allow Agents To Revoke Keys’を設定した場合は、Oracle ZFS Storage Applianceでラッピング鍵を削除すると、Oracle Key Managerの関連鍵が無効になります。‘Allow Agents to Revoke Keys’を設定しない場合は、関連するラッピング鍵をOracle ZFS Storage Applianceキーストアから削除すると、Oracle ZFS Storage ApplianceではOracle Key Managerの鍵が使用されなくなります。関連鍵は、鍵のライフサイクルが完了するか、セキュリティ責任者がOracle Key Managerの鍵を無効にするまで、Oracle Key Managerに存続します。

4. 鍵グループを作成します。

   鍵グループは、エージェントが使用する鍵のプールです。Oracle ZFS Storage Applianceは必ず、デフォルトの鍵グループとしてエージェントに割り当てられているOracle Key Manager鍵グループから鍵を要求します。

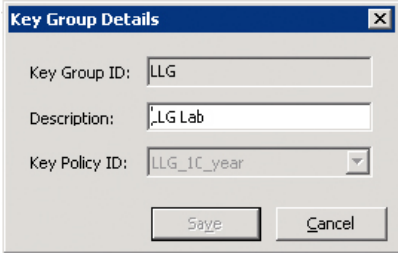

図6. Oracle Key Managerの鍵グループの詳細設定

5. 鍵のバックアップを作成します。

   （KMAクラスタ構成ではなく）単一ノードのKMAを使用する場合は、エージェントに割り当てられているデフォルト鍵グループからの鍵を要求される前にOracle Key Managerの鍵のバックアップを作成しておく必要があります。

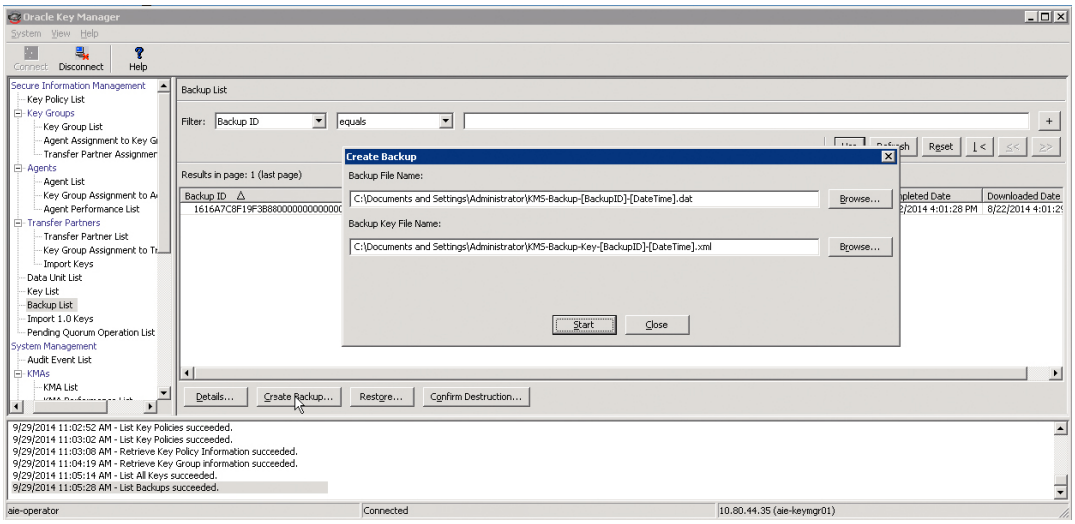

図7. 鍵のバックアップの作成

   鍵のバックアップが作成されると、鍵の状態が‘Generated’から‘Ready’に変わります。鍵のステータスは、GUIのナビゲーション・ツリー・ペインから‘Key List’オプションを選択すれば確認できます。

6. Oracle ZFS Storage ApplianceをOracle Key Managerのエージェントとして登録します。Oracle ZFS Storage ApplianceをOracle Key Managerに登録するには、先にOracle Key Managerでエージェントを作成しておく必要があります。Oracle ZFS Storage Applianceで使用する鍵グルー

プを選択し、パスフレーズを定義します。このパスフレーズは、Oracle ZFS Storage ApplianceからOracle Key Managerへ登録要求を発行するときに使用されます。

重要：Oracle ZFS Storage Applianceをクラスタ構成にしている場合は、各アプライアンス・ノードから1回ずつ、合計2回の登録要求がOracle Key Managerに対して行われてしまうため、'One Time Passphrase' オプション（'Flags'の横にチェック・ボックスとして表示されています）は使用しないでください。また、このオプションを使用するとアプライアンス・ノードの再登録が難しくなります。再登録は、アプライアンス・ハードウェアの交換、または工場出荷時のデフォルトにリセットした後の再構成に伴って行う必要があるためです。クラスタ構成のOracle ZFS Storage Applianceを登録する場合は、エージェントを1つだけKMAに作成する必要があります。

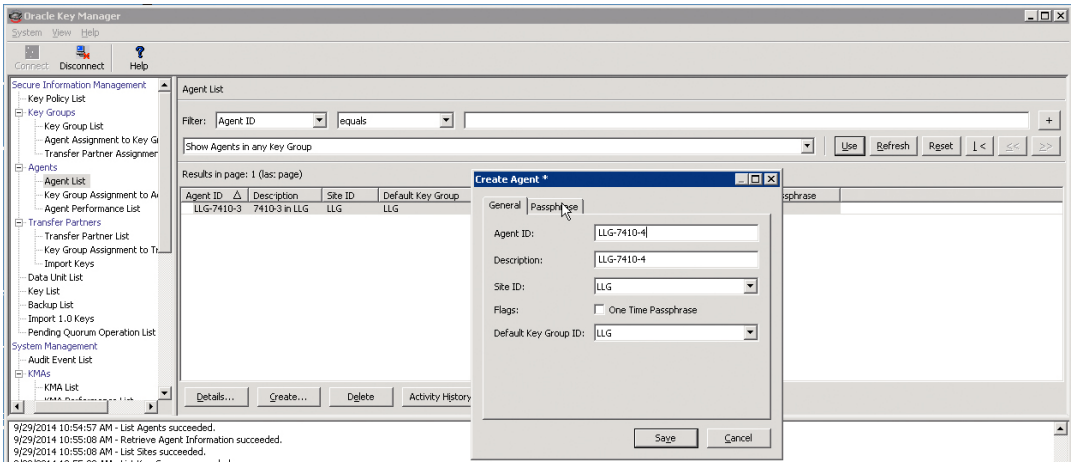

図8. Oracle Key Managerでの新しいエージェントのパスフレーズの設定

7. Oracle Key Managerでエージェントを作成したら、Oracle ZFS Storage Applianceから登録要求を発行する必要があります。

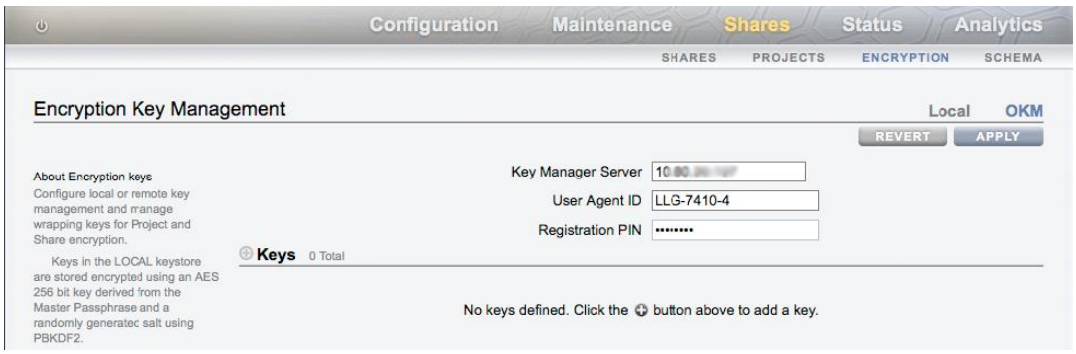

図9. Oracle ZFS Storage Appliance BUIでのキー登録要求の開始

8. 1つまたは複数のラッピング鍵を要求します。

これで、Oracle ZFS Storage ApplianceとOracle Key Managerとの間の通信は確立されましたので、Oracle Key Managerからラッピング鍵を要求できます。

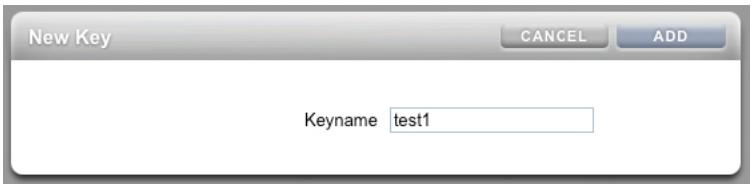

図10.Oracle Key Managerでの新しいラッピング鍵の要求

暗号化シェアの作成

Oracle ZFS Storage Applianceは、この時点で、暗号化されたファイル・システムおよびLUNを使用できる状態になっています。

プロジェクトを作成する場合は、プロジェクト内のすべてのシェアについて暗号化を有効にするかどうかを選択できます。暗号化を選択すると、そのプロジェクト内のシェアの暗号化を個別に無効化することはできません。‘暗号化した’プロジェクト内にシェアを作成する場合は、暗号化のレベルをシェアごとに選択できます。

図11.Oracle ZFS Storage ApplianceのCreate Projectダイアログ・ウィンドウでのEncryptionの切り替え

暗号化シェアは、既存のプロジェクトまたは新規作成した暗号化プロジェクトに作成できます。シェアを作成する場合は、ファイル・システムでのデータ暗号化に使用する暗号化のレベルを選択します。ローカル・キーストアまたはOracle Key Managerキーストアのいずれかを選択し、使用するラッピング鍵を選択します。

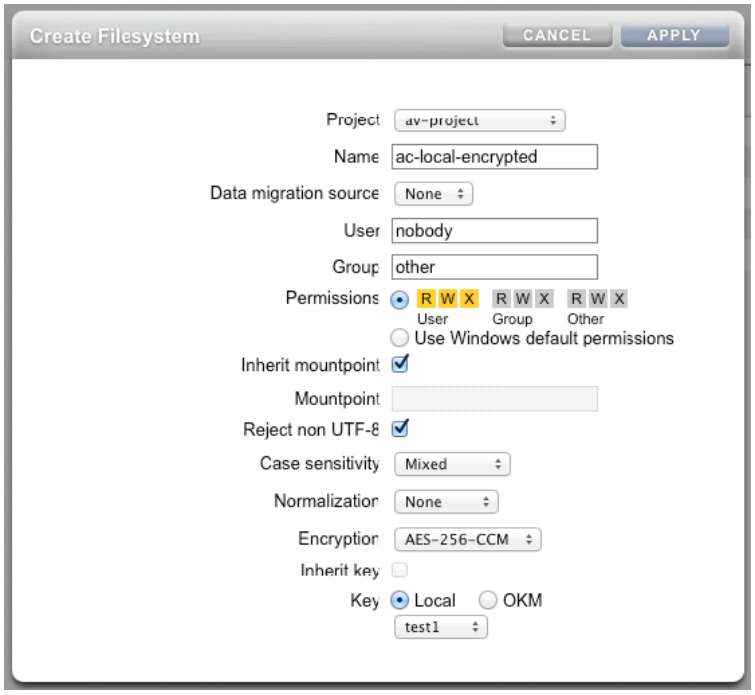

図12. 暗号化のレベル、キーストア、およびラッピング鍵が指定されたファイル・システムの作成

‘Inherit key’オプションは、シェアに選択したプロジェクトで、シェアの暗号化が設定されている場合に使用できます。継承オプションを選択すると、そのプロジェクトで選択したラッピング鍵が新しいシェアに継承されます。ただし、この設定は後から変更できません。

Oracle ZFS Storage Appliance BUIでは、暗号化を使用しているシェアに南京錠の記号が付きます。使用できないシェアには黄色いLEDステータスが付きます。シェアを使用できない理由の1つとして考えられるのは、そのシェアのラッピング鍵が削除されていることです。

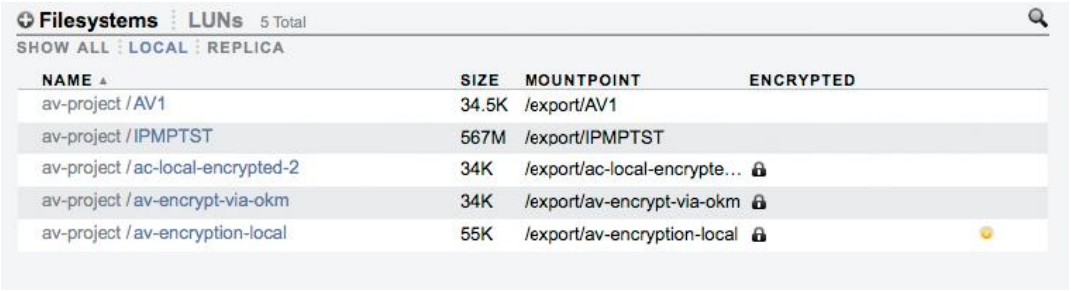

図13. 暗号化および使用不可を示すステータス・アイコンが付いたシェアの表示

‘inherit key’オプションをオンにして作成したシェアは、元の鍵を所有するプロジェクトの外に移動することができません。

バックアップによるキーストアの保護

キーストア内のラッピング鍵を喪失すると、そのキーストアのラッピング鍵を使用するシェア上のすべてのデータにアクセスできなくなります。つまり、データは消去されたと見なされますので注意が必要です。そこで重要になってくるのが、ハードウェア障害やその他の種類のシステム障害によってキーストア内のラッピング鍵が失われないようにすることです。Oracle Key Managerをクラスタ構成で使用する場合は、Oracle Key Managerクラスタ内のKMAノード間で自動的にキーストアがレプリケートされるため、ラッピング鍵の喪失やキーストアへのアクセスの喪失を防ぐことができます。クラスタ構成でない場合は、定期的にキーストアをバックアップする必要があります。

ローカル・キーストアのバックアップの作成

Oracle ZFS Storage Appliance上のキーストアのバックアップを作成するには、Oracle ZFS Applianceの構成のバックアップを作成します。このバックアップには、Oracle ZFS Storage Applianceのすべてのローカル暗号化構成とローカル・キーストアの内容が含まれます。このバックアップを使用すれば、Oracle ZFS Storage Applianceのすべての構成情報をリストアできます。ただし、このバックアップはOracle ZFS Storage Appliance自体に作成されるため、Oracle ZFS Storage Applianceのコントローラ・ハードウェアを交換する必要があるといったシナリオから保護するには、安全と思われる別の場所にバックアップ・ファイルを保存する必要があります。

個々の鍵の値をバックアップするには、CLIで次のコマンドを使用します。

```
shares encryption local keys
select keyname=1
get key
```

Oracle Key Managerキーストアのバックアップの作成

Oracle Key Manager構成からキーストアを使用する場合は、次の項目を把握しておく必要があります。

- ApplianceをOracle Key Managerエージェントのセットアップに登録したときに使用した、Oracle ZFS Storage Applianceに関する構成情報
- Oracle ZFS Storage Applianceの受信に使用されるOracle Key Managerの構成情報とOracle Key Manager上のキーストア。

Oracle ZFS Storage Appliance上の構成情報の喪失を防ぐには、構成のバックアップを作成して安全な場所に格納する必要があります。

Oracle Key Managerをクラスタ構成で使用している場合は、すべてのOracle Key Manager情報がOracle Key Managerクラスタ内のすべてのKMAノードに格納されるため、KMAノード（へのアクセス）の喪失を防ぐことができます。ただし、KMAを単一ノード構成で使用する場合は、KMAキーストアのバックアップを作成して安全な場所に格納する必要があります。

暗号化シェアのスナップショットとクローンの作成

シェアのスナップショットには、元のシェアのラッピング鍵が常に継承されます。スナップショットのクローンを作成する場合は、この依存関係が維持されます。会社のセキュリティ要件によっては、クローンのラッピング鍵を変更することを検討したほうがよい場合があります。

暗号化シェアのレプリケーション

Oracle ZFS Storage Appliance上の暗号化シェアは、他の種類のシェアと同じ方法で複製できます。データは暗号化を解除してシェアから取り出され、ターゲットのOracle ZFS Storage Applianceに送信され、そこで暗号化してから格納されます。

重要な点は、ソース側のシェアのメタデータにラッピング鍵の名前が格納されていることです。ターゲット側のOracle ZFS Storage Appliance上のレプリケーション・プロセスは、初めてレプリケーションを開始した時点では、ターゲット側のOracle ZFS Storage Applianceのキーストア（ローカルまたはOKM）に同じ名前のラッピング鍵があるものと想定しています。ラッピング鍵の値は同じでなくても構いません。したがって、多数のシェアを初めてレプリケーションする場合は、レプリケーションを開始する前に、それらのシェアで使用しているラッピング鍵の名前をターゲット・マシンのキーストアに作成しておくことが重要です。

レプリケーション環境でOracle Key Managerを使用する場合は、Oracle Storage ZFS Applianceレプリケーション・ソース・ノードのOKMエージェントとOracle ZFS Storage Applianceレプリケーション・ターゲット・ノードのOKMエージェントが両方とも、デフォルト・グループとして同じOKM鍵グループを使用している必要があります。

暗号化使用時のベスト・プラクティス

Oracle ZFS Storage Applianceによる暗号化の適用を計画する際には、これから紹介する推奨事項、ベスト・プラクティス、および原則を考慮してください。

データ・セキュリティ・アーキテクチャ

暗号化は、より広範囲にわたるデータ・セキュリティ・アーキテクチャの一部として計画する必要があります。このアーキテクチャは、データ・セキュリティ種別の概要を示し、遵守すべきデータ規定を明確にし、そうした要件の実行について詳述したものである必要があります。また、認証ロールと認証グループも明確にする必要があります。

「The Twenty Critical Security Controls for Effective Cyber Defense（サイバーディフェンスのための20の重大なセキュリティコントロール）」、通称「コンセンサス監査ガイドライン（CAG）」は、コンピュータ・セキュリティに関するベスト・プラクティス・ガイドラインをまとめた刊行物です。CAGで紹介されている推奨事項はほとんどがテクノロジー・ソリューションに特化したものであるため、これよりはるかに包括的なNISTのガイドラインに置き換わるものではありません。CAGは、新しいセキュリティ・プランの見直しまたは実装を進めている組織のガイドラインとなるものです。

データへの不正アクセスに対する保護を強化するには、ユーザー認証サービス（LDAP、ADなど）、ACL、データ・ネットワークのゾーニング/セグメンテーション（VLAN）テクノロジーを導入する必要があります。

ネットワーク・アーキテクチャの設計

Oracle ZFS Storage Appliance上に管理アクセス用のネットワーク・インタフェースを確保し、管理作業専用の独立したIPサブネットに接続することをお勧めします。こうすることで、本番または会社のデータ・ネットワークで万が一ネットワーク・インフラストラクチャの問題が発生しても、Applianceへの管理アクセスが失われるリスクを回避できます。詳しくは、「付録A：参考資料」に挙げられているホワイトペーパー『Oracle ZFS Storage Applianceを使用したネットワークのベスト・プラクティス』を参照してください。

Oracle Key Managerのアーキテクチャの設計

Oracle Key Manager構成を使用してOracle ZFS Storage Applianceのラッピング鍵を管理および提供する場合は、第3のIPサブネットを用意して、管理用IPネットワークおよびデータ用IPネットワークから鍵管理トラフィックを独立させる必要があります。先ほど「Oracle Key Managerキーストアの設定」の項の図で示したとおり、KMAノードにはネットワーク・インタフェースが2つあるので、それぞれに異なるサブネットを構成する必要があります。

ラッピング鍵のバックアップの作成

ラッピング鍵とは、そのラッピング鍵に関連するシェアへのアクセス鍵にアクセスするための唯一の鍵です。ラッピング鍵を喪失するとシェアのデータも失われます。

ラッピング鍵が使用できなくなる理由としては、次のようなことが考えられます。

- キーストアから鍵が削除される。違う鍵を誤って選択したために削除された可能性があります。
- 暗号化をサポートしていないリリースに対してOracle ZFS Storage Appliance上でロールバックが実行される。
- キーストアがまだ作成されていないリリースに対してOracle ZFS Storage Appliance上でロールバックが実行される。
- Appliance構成のバックアップが作成されておらず、Appliance構成ファイルのバックアップがAppliance以外の場所に存在せず、現行のブート・イメージに（最新の）キーストアが存在しないリリースに対して、Oracle ZFS Storage Appliance上でロールバックが実行され、キーストアの内容が失われた。
- KMAへのアクセスが失われた。

暗号化されたデータシェアのバックアップとリストア

暗号化シェアのバックアップは、NDMP zfsバックアップ形式の使用を推奨します。この方法を選択した場合は、zfs暗号化鍵へのアクセスに使用したラッピング鍵の名前などの暗号化設定がシェアに維持されます。

キーストアとラッピング鍵値は、シェアのNDMPバックアップ・ストリームに含まれません。シェアをリストアするときに、シェアのリストア先となるファイル・システムに同じ名前のシェアがあってはなりません。

シェアをリストアする前に、リストアするシェアで使用していたラッピング鍵の名前を含むキース

トアがすでに存在している必要があります。テープの保存データに適切なセキュリティを確実に施すには、テープのデータを暗号化するバックアップ装置を使用します。このバックアップ装置でも同じOracle Key Manager鍵管理システムを使用し、単一の一元化された鍵管理システムを利用できます（次の図を参照）。

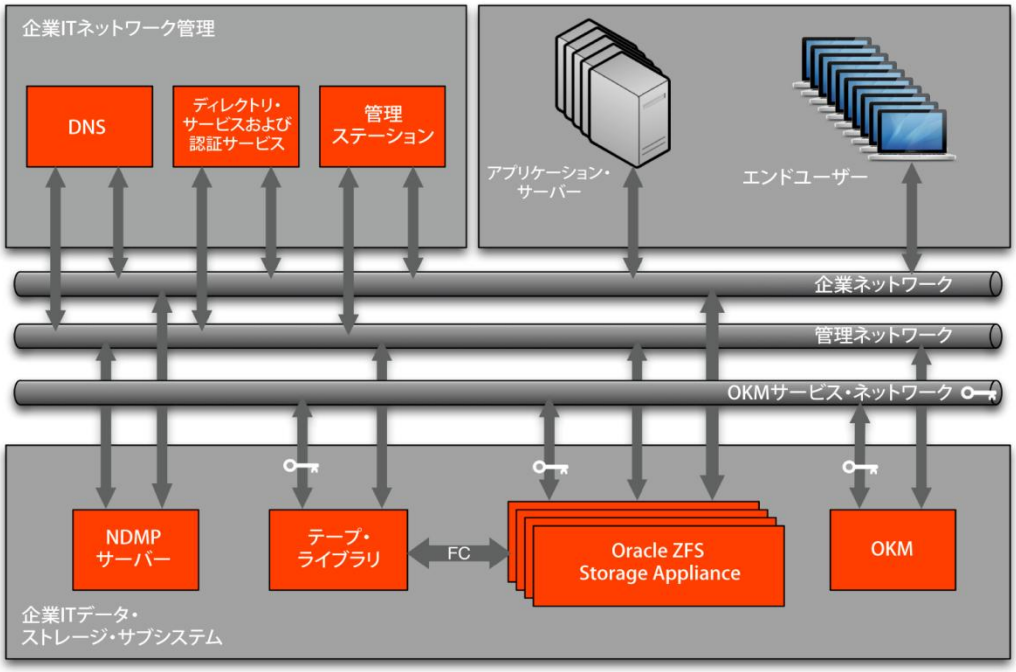

図14. Oracle Key Managerの鍵管理システムを活用するバックアップ・サブシステム

シェアのレプリケーションの使用

シェアをレプリケートすると、どのアプリケーションの場合とも同様に、ソースからデータが読み取られます。つまり、データは暗号化、圧縮、重複排除がともに解除されます。暗号化が有効になっているシェアからレプリケートする場合は、レプリケーション・リンクの設定時に、ソースおよびターゲットのOracle ZFS Storage Applianceノード間のレプリケーション接続にSSL/TLSセキュリティ・オプションを使用し、データのセキュリティを維持するよう強くお勧めします。

図15. 暗号化を有効にしたシェアのレプリケーションに対するSSL/TLSの使用

暗号化されていないシェアと暗号化されているシェアとの間の移行

シェアの作成後に暗号化機能を有効にすることはできないため、暗号化機能はシェアの作成時に指定する必要があります。

Oracle ZFS Storage Applianceの既存のデータセットに暗号化が必要な場合は、シャドウ移行オプションを使用できます。その場合は、既存の各シェアについて、Create Filesystemダイアログ・ウィンドウの'Data migration source'オプションで既存のシェアをシャドウとして指定して、新しいシェアを作成する必要があります。

複数のシェアについてシャドウ移行を実行しようと考えている場合は、現行プールのRAIDオプションが、データセットの可用性の要件に引き続き一致していることを確認してください。一致していない場合は、この時点で新しいプールを作成し、暗号化を有効にした新しいプロジェクト定義を使用して全てのシェアを新しいプールに移行します。

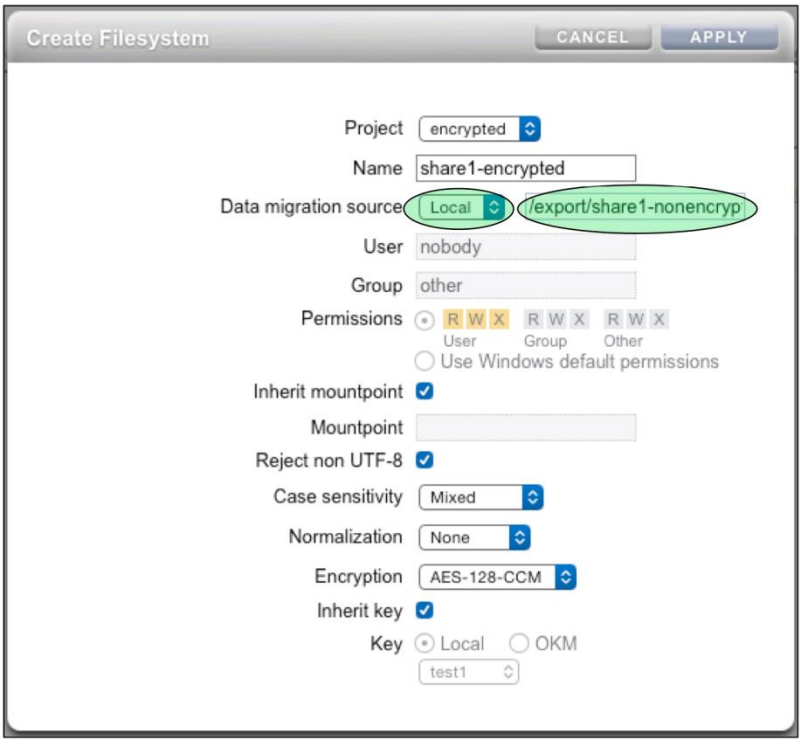

図16. 移行を介した新しいシェアの作成による暗号化ステータスの変更

シェアでの暗号化を解除する必要がある場合も、（上記の同じプロセスによる）シャドウ移行を使用できます。

暗号化シェアでの重複排除/圧縮の併用

シェアで使用できるオプションとプロトコルは、暗号化を有効にしたシェアでもすべて使用できますが、例外が1つあります。AES-GCM暗号化アルゴリズムの性質上、重複排除を使用した場合に得られるメリットはどれも得られません。そのため、重複排除を組み合わせて使用しているシェアには、AES-XXX-CCM暗号化方式のいずれかの鍵オプションを使用することを強くお勧めします。

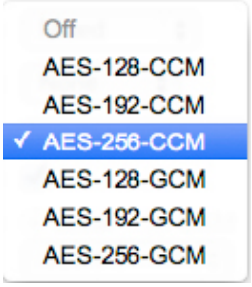

図17.Oracle ZFS Storage Applianceの暗号化方式のオプション・メニュー

さまざまな暗号化オプションのパフォーマンスに関する考慮事項

使用する暗号化方式は、プロジェクトまたはシェアの作成時に選択できます。どの方式を選択するかは、いくつかの要素、規制要件、パフォーマンスへの影響、（前述した）重複排除の使用の有無によって異なります。次の表に、各暗号化オプションの特長をまとめます。

暗号化の方式	説明		
オフ	シェアやプロジェクトは暗号化されません	シェアやプロジェクトは暗号化されません	重複排除可
AES-128-CCM	CPUへの影響がもっとも低い暗号化モード		重複排除可
AES-192-CCM			重複排除可
AES-256-CCM			重複排除可
AES-128-GCM		NIST SP800-38Dで推奨	重複排除不可
AES-192-GCM		NIST SP800-38Dで推奨	重複排除不可
AES-256-GCM	CPUへの影響がもっとも高い暗号化モード	NIST SP800-38Dで推奨	重複排除不可

シェア上で暗号化を使用すると、アプリケーションのパフォーマンスに影響しますが、影響の程度は、アプリケーションで作成されるワークロードの種類によって異なります。

一般的には、ブロック・サイズが大きめ（128KB～1MB）のシェアを使用するシーケンシャル書込み中心のワークロードの場合は影響が大きく、その結果データ・スループットが低下します。GSM（General System for Mobile）方式の暗号化は、このような順次型ワークロードのI/Oスループットへの影響がもっとも高くなります。

DRAMからのキャッシュ読取りヒット率が高いI/Oワークロードのアプリケーションの場合は、データが直接キャッシュから取得され、ディスクまたはSSDキャッシュのデータを復号化する必要がないため、影響は最小限に抑えられます。

データベース・リポジトリを使用するアプリケーションに対する推奨事項

データベース型アプリケーションを使用する場合は、Oracle Transparent Data Encryption（TDE）機能を使用することをお勧めします。この機能を使用すると、暗号化とユーザー認証セキュリティ機能が結合され、最適な統合型セキュリティ・ソリューションとなります。TDEでは、データベースの列またはアプリケーションの表領域全体を暗号化できます。暗号化操作は高速であるため、アプリケーションで発生するパフォーマンス・オーバーヘッドはほとんどの場合無視できます。TDEは、Oracle Advanced Compression、Oracle Automatic Storage Management（Oracle ASM）、Oracle Recovery Manager（Oracle RMAN）、Oracle Data Pump、Oracle GoldenGateなど、頻繁に使用されるOracle Databaseの各種ツールやテクノロジーに直接統合されています。

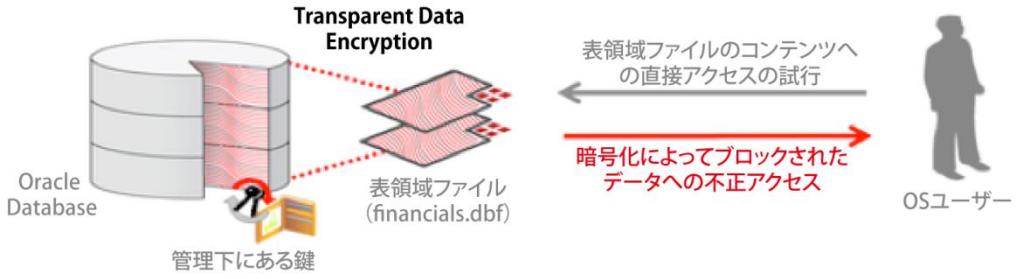

図18.Oracle DatabaseへのOracle Transparent Data Encryptionの適用

鍵管理のベスト・プラクティス

鍵管理は、ベスト・プラクティスを組み込んだ強力なポリシーや手続きの定義および施行を重視したものである必要があります。こうしたポリシーや手続きは、会社またはビジネス上のセキュリティ要件、業界の規制要件、行政による規制要件やセキュリティ要件によって異なります。また、地理的立地ごとに異なる場合もあります。

次に示す内容は常識的なものですが、検討を始めるための材料として役立ちます。

鍵の保護を徹底する

これはキーストアとキーストアの内容のバックアップの両方について言えることです。該当する職務に就くユーザーに適切なロールとアクセス権を割り当て、キーストアへのアクセスとキーストアの内容の管理を確実に制御します。コピーが保存されている場所へのアクセスも、厳しく制御する必要があります。キーストアへのアクセスのセキュリティが適切であっても、キーストアの内容のバックアップ・コピーが保存されているUSBスティックをオフィスの机の上に放置していては意味がありません。

定期的に鍵を変更する

ラッピング鍵の変更をポリシーとして規定することをお勧めします。ラッピング鍵は、Oracle ZFS Storage Applianceの暗号化シェア上でいつでも変更できます。鍵を変更しても、シェア内のデータを再暗号化するサイクルは必要ありません。ラッピング鍵（の内容）を変更すると、暗号化シェア上のZFSで使用されている暗号化鍵が再暗号化されます。

鍵の割当て方法と割り当てるユーザーを管理する

ポリシーおよびセキュリティ・プランで識別されたユーザーのみが、割り当てられているセキュリ

ティ・レベルに従ってキーストアにアクセスし、鍵を操作できるようにします。

鍵の範囲を決める

シェアを暗号化する場合は、暗号化を実行する範囲をOracle ZFS Storage Applianceにするのか、プロジェクトまたはシェアにするのかを決める必要があります。ビジネス領域ごとに異なるプロジェクトやシェアを使用したり、暗号化の方式や鍵の保存方針などに異なる要件を適用したりできます。

付録A：参考資料

- Oracleストレージ製品に関する情報
  http://www.oracle.com/jp/products/storage/overview/index.html
- Oracle ZFS Storage Applianceのテクニカル・ホワイトペーパーとソリューション概要

  http://www.oracle.com/technetwork/jp/server-storage/sun-unified-storage/documentation/index.html
- Oracle ZFS Storage Applianceの技術ドキュメント・ライブラリ
  http://docs.oracle.com/cd/E51475_01/index.html

  『*Oracle ZFS Storage Appliance Administration Guide*』はOracle ZFS Storage Applianceのヘルプ・コンテキストでも参照できます。
  Oracle ZFS Storage Applianceのヘルプ機能には、ブラウザ・ユーザー・インタフェースからアクセスできます。
- 『Oracle Key Manager 3 管理ガイド』（付録C「Solaris ZFS暗号化によるOKMの使用」）
  https://docs.oracle.com/cd/E50985_03/ja/E52217/html/okmag_apc_zfs_take1.htm#sthref799
- 「Critical Security Controls」 SANS Institute。コンセンサス監査ガイドライン（CAG）：
  http://www.sans.org/critical-security-controls
- 「Recommendation for Key Management – Part 2:Best Practices for Key Management Organization」 *Computer Security*. 2012. Elaine Barker, William Barker, William Burr, William Polk, and Miles Smid. National Institute of Standards and Technology. Special Publication 800-57.
  http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf

付録B：略語および用語の索引

AES	Advanced Encryption Standard。
エージェント	データの暗号化および復号化に使用され、暗号化鍵の管理にOKMを使用するストレージ・デバイス。エージェント・リスナーは、各ストレージ・デバイスのOKMで作成する必要があります。
暗号化鍵	データのエンコードおよびデコードに使用されるデータ暗号化鍵
キーストア	セキュリティ証明書のリポジトリ。Oracle ZFS Storage Applianceでは、ZFSで使用する実際の暗号化鍵の暗号化および復号化に使用するラッピング鍵がキーストアに保持されます。ZFSでは、ZFSシェア暗号化鍵を使用して、ZFSシェア内のデータを暗号化および復号化します。
NIST	National Institute of Standards and Technology, Department of Commerce of the U.S. Government（米国商務省、国立標準技術研究所）。
OKM	Oracle Key Manager。次の3つの主要コンポーネントで構成されます。 **鍵管理アプライアンス**（KMA）：ポリシーベースの鍵管理、認証、アクセス制御、鍵プロビジョニングの各サービスを提供する、セキュリティが強化されたハードウェアです。複数のKMAを使用してKMAクラスタを作成し、鍵の保存の信頼性および冗長性を強化することができます。 **鍵管理ソフトウェア**：2つのオプション（GUIバージョンまたはCLIバージョン）があり、KMAのセットアップおよび鍵管理機能の実行に使用します。このソフトウェアは、Oracle Solaris、Microsoft WindowsまたはLinuxベースのワークステーションにインストールできます。 **ハードウェア・セキュリティ・モジュール**（HSM）：ハードウェア暗号化アクセラレータ・カード。
ロール	特定の操作を実行できるようにするために、Oracle ZFS Storage ApplianceおよびOKMのユーザーに付与される権限のセット。監査者、バックアップ・オペレータ、コンプライアンス責任者、オペレータ、セキュリティ責任者などがあります。
RSA	鍵を暗号化するためのアルゴリズム。
ラッピング鍵	ZFS暗号化鍵の復号化および暗号化に使用される鍵。ラッピング鍵はOracle ZFS Storage Applianceのキーストアに格納されます。

Oracle ZFS Storage Applianceでの
暗号化の導入と暗号化鍵の管理に関する
ベスト・プラクティス
2014年11月、バージョン1.0、
著者：Peter Brouwer

お問い合わせ窓口
Oracle Direct
TEL 0120-155-096
URL oracle.com/jp/direct

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

Copyright © 2014, 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。

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X/Open Company, Ltd.によってライセンス提供された登録商標です。0611

Hardware and Software, Engineered to Work Together