Oracleホワイト・ペーパー
2013年10月

Oracle Database Vault
ベスト・プラクティス

概要

Oracle Database Vaultは強力なセキュリティ制御機能を提供することで、アプリケーションや機密データを保護します。また、特権ユーザーによるアプリケーション・データへのアクセスを防止し、非定型のデータベース変更を制限し、誰が、いつ、どこで、どのようにしてアプリケーション・データにアクセスできるかを制御します。さらにOracle Database Vaultは、既存のデータベース環境を透過的に保護することで、コストと時間のかかるアプリケーション変更が不要になります。

このホワイト・ペーパーでは、Oracle Database Vaultによる保護を迅速に導入し、データベース内の機密アプリケーション・データを保護するベスト・プラクティスを説明します。おもなトピックは次のとおりです。

1. インストール
2. 職務の分離
3. データベース管理
4. Oracle Database Vaultを使用した保護の定義
5. インストール後の作業
6. 保守の考慮事項

インストール

Oracle Database 12c以降、Oracle Database Vaultはデフォルトでインストールされていますが、有効にはなっていません。顧客はDatabase Configuration Assistant（DBCA）を使用するか、SQL*Plusを使用してコマンドラインからわずか数分でOracle Database Vaultを有効にできます。

Oracle Database Vaultを有効にすると、Oracleやサード・パーティのアプリケーションをインストール済みの既存環境で実行できます。その後に新規アプリケーションをインストールしたり、パッチを適用したりするには、Oracle Database VaultのDV_PATCH_ADMINロールを実行ユーザーに付与する必要があります。

インストール前の注意事項

有効化プロセスの実行中に、DBCAはアカウント管理権限の作成機能を提供します。Oracle Database Vaultの管理、データベース・アカウントの管理、DBA業務の間での職務分離を強化するため、オラクルはこの権限作成を推奨しています。Oracle Database Vaultの管理には、Oracle Enterprise Manager Cloud Control 12cを使用できます。

職務の分離

職務の分離は、過去10年間にその重要性を増してきています。多くの組織にとって、職務の分離は発展し続けるための新しい概念です。データベース統合、規制遵守、およびアウトソーシングは、増加した職務の分離におけるほんの一部の要因にすぎません。Database Vaultの職務の分離では、セキュリティ関連の管理作業をDBAの日々の業務から切り離すことで、セキュリティを強化します。Database Vaultを使用している組織は、Database Vaultの職務の分離の実装を調整して、現在および将来のビジネス要件に容易に適応させることができます。小規模な組織は限られたリソースでセキュリティ・プロファイルを高めようとするため、特に柔軟性が必要になります。

職務の分離を正しく実行するには、自社の環境で基本的な管理タスクを行うのは誰なのか、それらの管理タスクはどのようなものなのかを事前に理解する必要があります。1人のDBAが新しいデータベース・アカウントのプロビジョニングおよびアプリケーション・パッチの両方の管理に責任を持っている場合でも、それぞれのタスクを文書化して、計画することが重要になります。このようなタイプのタスクに独立した管理アカウントを使用することで、アカウンタビリティを高め、各タスクに伴うリスクを減らすことができます。中規模から大規模の組織のデータベース管理者は、一般的な管理タスクを実行する必要はありますが、アプリケーションによって管理されているビジネス・データにアクセスする必要はありません。職務分離のマトリックスを作成することは、Database Vaultの導入を計画する際に役立ちます。このリストには、追加のタスクや関連するユーザーを追加できます。この情報は、組織の総合的なエンタープライズ・セキュリティ・ドキュメントの一部となります。

職務分離のマトリックス

ユーザー、プロセスまたはアプリケーション	アカウント作成	データベース管理					セキュリティ管理
		SYSDBA	バックアップ	チューニング	パッチの適用	監視	
JoeSmith	X					X	
SteveHardy							X
PeterKestner			X				
RobertTyler					X		
SusanAnderson				X			
SYSTEM							
RMAN		X	X				
……							

図1.職務分離のマトリックス

場合によっては、一部のシステム管理タスクで、特定のツールやプログラムを使用して、一時的にデータにアクセスする必要があります。この一時的または緊急アクセスに対するプロビジョニングは、Database Vaultのアプリケーション保護ルールに組み込む必要があります。

Oracle Databaseの管理

オラクルでは、Oracle SYSTEMアカウントを一般的なDBAの目的で使用する場合、それぞれのデータベース管理者に名前付きのDBAアカウントを作成することを推奨します。そうすることで、データベース内の管理アクションに対するアカウンタビリティを高めることができます。

Oracle SYSTEMユーザー

過去に開発された多くのアプリケーションは、Oracleユーザー・アカウントのSYSTEMを使用して一部のアプリケーション表を保持しています。そのため、一部のアプリケーションを正常に機能させ続けるために、レルム認可にSYSTEMアカウントを追加する必要が生じる場合があります。このようなシナリオでは、SYSTEMアカウントに制限を設定することでセキュリティを高めることができます。たとえば、Oracle Database Vaultのルール・セットを使用して、SYSTEMユーザーによる特定のIPアドレスへの接続を制限できます。

Oracle SYSDBAのアクセス

オラクルでは、SYSDBAロールを使用する接続は厳しく制限することを推奨しています。SYSDBAロールを使用したデータベース接続は、絶対に必要な場合、およびOracle RMANや必須のパッチ・プロセスなどの、現在でもSYSDBA接続を必要とするアプリケーションに限定してください。それ以外の場合は、名前付きのデータベース・アカウントを作成して、日々のデータベース管理を実行します。将来的に、オラクルはすべてのアクティビティをSYSDBAでの接続なしで実行できるようにする予定です。

ROOTおよびその他のオペレーティング・システム・アクセス

『Oracle Database Vault管理者ガイド』に記載されているように、Oracle Database Vaultは、特権付きオペレーティング・システム・ユーザーがデータベース・ファイルに直接アクセスすることを防げません。このような保護には、Oracle Transparent Data Encryption（透過的データ暗号化）を使用することを推奨します。また、オペレーティング・システムへの直接アクセスを慎重に確認して制限することも推奨しています。

オラクルは、オペレーティング・システムにアクセスするための個別アカウントを設定することを推奨します。LinuxまたはUNIX環境でこれらの個別アカウントを使用する場合、必要に応じて、オラクル・ソフトウェアの所有者に対してsudoを実行する必要があります。sudoを実行することで、各個別ユーザーが実行できる特定のコマンドを制御できます。

ネーミング規則

Database Vaultのセキュリティ・ポリシーを作成する際に、一貫性のある優れたネーミング規則を使用すると、セキュリティ管理者、監査人、およびビジネス・ユーザーが、保護されている対象やさまざまなセキュリティ要素が互いにどのように関連しているのかを理解するのに役立ちます。Database Vaultのセキュリティ・ポリシーを作成する際は、次のネーミング規則を使用します。

レルム	• 保護されたアプリケーションの名前をレルム名として使用します。 • レルムの説明で、特定のアプリケーション保護のビジネス目的を記述し、レルムの保護を補完するその他すべてのセキュリティ・ポリシーを文書化します。レルムの認可を受けたユーザー、それぞれの目的、および可能な緊急認可についても文書化する必要があります。
ルール・セット	• 名前は名詞で始めて、ルール・セットを関連付けるレルムまたはコマンド・ルールの名前で終えます。 • 説明フィールドに、ルール・セットのビジネス要件を記述します。
ルール	• 名前は動詞で始めて、ルールの目的で終えます。 • ルールには説明フィールドがないため、名前は明確なものにして、90文字以上で設定します。
ファクタ	• 名前は名詞で始めて、生成された値の説明で終えます。

図2.ネーミング規則

Oracle Database Vaultのレルムの定義

Oracle Database Vaultをインストールすると、標準で4つのレルムが作成されます。デフォルト・レルムの1つは、Data Dictionaryレルムと呼ばれるものです。指名された管理者は、所有者または参加者としてData Dictionaryレルムに追加する必要があります。Oracle SYSTEMアカウントを認可ユーザーとしてData Dictionaryレルムに追加できますが、オラクルでは、この汎用的なデータベース・アカウントの使用は推奨していません。

Oracle Database Vaultのレルムは、単一のオブジェクトまたはアプリケーション・スキーマ全体を保護できます。ほとんどの場合、アプリケーション全体を保護することで、簡素化された堅牢な保護モデルを実現できます。レルムを作成したら、複数のユーザーにそのレルムへのアクセスを認可できます。データベース・オブジェクト（アカウント、ロール...）は、複数のレルムで認可できます。

ロールに対するレルム認可の割当て

レルム認可として追加する予定のロールに現在付与されている権限に注意してください。ロールのレルム認可は誤って付与されることがあり、すぐには分からない場合があります。これは、データベース・ロールの作成者が、ロールの作成時に暗黙のうちに付与していることがあるためです。その結果、SYSTEMのようなアカウントでロールを作成し、そのあと、Oracle Database Vault管理者がこのロールをレルム認可として追加した場合、SYSTEMユーザーは、そのレルムへのアクセスを暗黙のうちに付与されることになります。これは、ロールを作成するアカウントが、その作成時にロールを暗黙的に付与されるためです。ベスト・プラクティスとしては、レルム所有者としてレルム固有のロールを常に作成するようにします。

レルムの認可

1. *アプリケーション所有者* - アプリケーション所有者は、一般的に、そのアプリケーションに関連付けられているオブジェクトを含むスキーマに対応します。このユーザーをレルム所有者として指定できます。アプリケーション・サーバーは、一般的に、アプリケーション所有者のアカウントを使用してアプリケーションに接続します。また、サーバー・ベースのバッチ・ジョブは、直接またはプロキシ接続を経由して、アプリケーション所有者に接続します。
2. *アプリケーション・ユーザー* - アプリケーション・ユーザーは通常、中間層に認証され、単一のビッグ・ユーザー・モデルを介してバックエンド・データベースと通信します。単一のビッグ・ユーザー接続は、通常アプリケーション所有者に対して認証されます。アプリケーション所有者アカウントからデータベースへの中間層プロセスを介したアクセスを限定し、中間層サーバーのIPアドレスまたはホスト名へのアクセスを制限できます。この制限を行うには、ルール・セットを作成する必要があります。このルール・セットには、アプリケーション・ユーザー、ユーザー接続に使用する中間層プロセス、中間層のIPアドレスまたはコンピュータ名を指定します。その後、このルール・セットに対して、接続ユーザーがアプリケーション・ユーザーでない場合にtrueと判定する別のルールを追加する必要があります。Rule Set Evaluation Optionsは、Any Trueに設定する必要があります。この設定を終えると、CONNECTコマンドのコマンド・ルールを作成して、ルール・セットを関連付けることができます。この設定の例については、PeopleSoft用に公開されているOracle Database Vaultのセキュリティ・ポリシーを参照してください。
3. *アプリケーションDBA* - このユーザーを参加者としてアプリケーションのレルムに追加して、ルール・セットに関連付けることができます。このルール・セットでは、アプリケーションに必要なすべてのパッチおよび保守の実行が許可されますが、アプリケーション・データに対するSELECTの実行は禁止されます。このユーザーに対する制限を追加し、データベースにアクセスする曜日、時間、使用するコンピュータまたはサブネットを制限することもできます。顧客のセキュリティ要件に基づいて、さらに顧客固有の制限を追加できます。

Oracle Database Vaultのルール・セットの定義

時間、特定のホスト、サブネット、またはDatabase Vaultに標準搭載されたその他のファクタに基づいて、アクセスを制限するルール・セットを作成できます。さらに、Oracle Application Contextを使用して、カスタム・ファクタを作成することもできます。

- 各認可ユーザーは、Database Vaultの異なるルール・セットに関連付けることができます。
- 各認可ユーザーは、レルムで保護されているオブジェクトへのアクセスに関する条件および制限を指定する異なるルール・セットと関連付けることができます。

コマンド・ルール

Oracle Database Vaultのコマンド・ルールを使用して、アプリケーション・オブジェクトの変更を防止できます。たとえば、コマンド・ルールを使用して、drop tableコマンドに制限を設定できます。作成したコマンド・ルールは、Disabledと呼ばれるDatabase Vaultのルール・セットと関連付けることができます。パッチまたは保守操作用にコマンド・ルールを編集し、Enabledと呼ばれるルール・セットに関連付けることができます。

作成する必要があるコマンド・ルールの推奨リストが別のホワイト・ペーパーで公開されており、OTN（Oracle Technology NetworkのWebサイト：http://otn.oracle.com）からダウンロードできます。

ルール・セットを利用することで、個々のルールを意味のある1つのセットに簡単にグループ化できます。ルールは、複数のルール・セット間で共有できます。そのため、再利用可能なルール表現のライブラリを作成できます。オラクルは、それぞれ個別の目的を持つ表現になるようにルールを設計することを推奨します。ネーミング規則として、ルールの名前は動詞で始めて、ルールの目的で終えます。たとえば、特定のIPアドレスからの接続を許可するルールを作成する場合、"Allow Connect from Middle Tier IP Addresses"という名前になります。ルール・セットの名前の場合は、名詞で始めて、関連付けるコマンド・ルール、ファクタ、またレルム認可の名前で終えます。たとえば、SADMユーザーのSiebelレルムへのアクセスに関連付けるルール・セットの名前は、"Siebel SADM Realm Access"となります。Rule Set Descriptionフィールドには、このルール・セットで実現されるビジネス要件を記述します。

Oracle Database Vaultのファクタをルール表現で利用すると、強力なチェックを実施できます。また、Oracle内に手動でコンテキスト値を定義しなくてよいため、総合的なセキュリティが向上します。簡単に言うと、ファクタはセキュリティ・ルール表現内で使用するためのコンテキスト情報を提供します。

カスタム・イベント・ハンドラを使用して、Oracle Database Vaultのセキュリティ・ポリシーを拡張し、エラー処理やアラート表示を行うために外部システムと統合できます。『Oracle Database Vault管理者ガイド』には、UTL_TCP、UTL_HTTP、UTL_MAIL、UTL_SMTP、DBMS_AQなどのユーティリティ・パッケージを使用して、この種の統合を実現したり、電子メール・アラートを送信したりする方法が記載されています。電子メール・アラートの送信例については、『Oracle Database Vault Administration Guide』を参照してください。

ルール・セットは十分にテストする必要があります。一部のルール・セットをテストする際は、Database Vaultのセキュリティ管理者として、独立した接続を同時に確保しておくことが特に重要になります。たとえば、CONNECT操作のルール・セットを作成する場合、変更を加えたり問題を修正したりできるようにルール・セットを無効にする必要があります。Database Vault管理者が同時にログインしていることで、ルール・セットを無効にできます。それ以外の場合、誤ったルール・セットによって、データベースからロックアウトされることがあります。

また、機密データを保護するため、個々のルールおよびルール・セットを適用する前に、非本番環境またはテスト環境でテストすることが重要です。ルール表現は、次のSQL文を使用して直接テストできます。

```
SQL> SELECT SYSDATE from DUAL where [ルール表現をここに指定];
```

ルール表現は、単一のルール内にネストできます。ネストすることで、ルールのサブセットに論理ANDを、残りのルールに論理ORを必要とするような、より複雑な状況にも対応できます。例については、『Oracle Database Vault管理者ガイド』の第5-8項を参照してください。

Oracle Database Vaultを使用した保護の計画

保護の計画は、Oracle Database Vaultの導入における重要な要素です。Oracle Database Vaultのレルム、コマンド・ルール、ルール・セット、およびファクタは、高い粒度で使用できます。

ただし、先に進む前に、アプリケーションと相互作用する中間層接続、バッチ・ジョブ、およびプロセスについて理解する必要があります。

アプリケーション・アーキテクチャの理解

まず、保護するアプリケーションの基本的なアーキテクチャを理解することが重要になります。たとえば、アプリケーションに関連付けられたオブジェクトが複数のデータベース・スキーマにまたがっているのか、または単一データベース・スキーマに含まれているのかを知る必要があります。この分析には、表、ビュー、マテリアライズド・ビュー、ストアド・プロシージャなどのアプリケーション・データに関連するすべてのオブジェクトを含める必要があります。アプリケーション・オブジェクトと相互作用するプログラム、プロセス、中間層接続、データベース・ユーザー、およびアプリケーション管理者を特定します。この情報を取得したら、Oracle Databaseのレルム定義を作成して、アプリケーション・データにアクセスできるユーザーを認可します。アプリケーションのエンドユーザーは、一般的に中間層を介してアプリケーション・データにアクセスします。一部のレガシー・アプリケーションは、エンドユーザーがデータベースに独自のアカウントを保持するクライアント/サーバー・アーキテクチャをまだ使用している可能性があります。より高度なアプリケーションは、おそらく、Oracle Databaseをホストするサーバー上で稼働するアプリケーション固有のプロセスを使用します。

アプリケーション保護のマトリックス

アプリケーション保護のマトリックスを作成することで、Database Vaultの導入時に認可要件を見落とす可能性が低くなります。次の図3.0は、PeopleSoft保護のマトリックスを示しています。y軸は保護タイプ（レルム、コマンド・ルール）を、x軸は認可と関連ルール・セットを示しています。このマトリックスは、独自のカスタム・アプリケーション用のマトリックスを作成するための例として使用できます。

ルール・セットに対する認可 / **保護タイプ**	**SYSADM**	**PSFTDBA**	SYSTEM	SYSDBA
PeopleSoftのレルム	所有者	所有者	アクセスなし	アクセスなし
Select コマンド・ルール		Limit PSFTDB ルール・セット	アクセスなし	アクセスなし
Connect コマンド・ルール	PeopleSoft Access ルール・セット		アクセスなし	アクセスなし
Drop Tablespace コマンド・ルール	Disabled ルール・セット	Disabled ルール・セット	Disabled ルール・セット	Disabled ルール・セット

図3.PeopleSoft用保護のマトリックスの例

インストール後の作業

ドキュメント

セキュリティ・ポリシーを文書化することは、内部監査人および外部監査人に制御プロセスを示すとともに、操作の継続性を提供するために重要です。文書化する際は、以下の点を考慮してください。

プロセスおよびプロシージャ	• バックアップ • パッチの適用 • チューニングと監視
データベース・アカウント	• 目的 • 本番ステータス • SYSDBAアクセス
SYSTEMアクセス	• どのような場合にSYSTEMを使用するか
SYSDBA	• どのような場合にSYSDBAを使用するか
レポート	• レポートの名前 • レポートの頻度 • レポートの配布
緊急プロシージャ	• どのような場合にセキュリティ・ポリシーを無効化するか

図4.セキュリティ文書のマトリックス

緊急アクセス

場合によっては、管理タスクを実行するために、レルム保護を一時的に緩和する必要があります。オラクルは、Security Manager（DV_ADMINまたはDV_OWNER）でログインして、名前付きのアカウントをレルムの認可アカウントに追加し、認可ルールをEnabledに設定することを推奨します。このアプローチの場合、保護は依然として有効であり、新しい認可は制限されているため、レルムを一時的に無効にする方法よりも優れています。次に、有効なルール・セットで、ルール・セットに対するすべての監査を有効にします。レルム認可は、管理タスクが完了したときに削除できます。このケースは、緊急時および一般的に"Break The Glass"と呼ばれるシナリオにも当てはまります。また、保守作業中にも保護の必要な非常に機密性の高い表を保護するために、必須レルムを使用できます。このような表に対して必須レルムを設定して有効にし、保守作業と緊急アクセスが終了したら無効にできます。

付録A - コマンド・ルールのヒント

コマンド・ルールを設定する際のガイドラインを次に示します。

- 保守を容易にするために、より詳細なコマンド・ルールを作成します。たとえば、特定のスキーマでのSELECT文の実行を防止するには、すべてのケースでSELECT文をブロックするのではなく、特定のスキーマや表に対するSELECT文を停止するようなコマンド・ルールを設計します。
- CONNECTイベントのルールを設計する際は、Oracle Database Vaultの所有者または管理者を誤ってロックアウトすることがないロジックを含めるようにします。CONNECTコマンド・ルールに関連付けられているルール・セットがすべてのセッションをブロックする場合、正しいルール・セットの設計を再開する前に、Oracle Database Vaultと関連ルール・セットを無効にしてから、再びDatabase Vaultを有効にする必要があります。詳しくは、『Oracle Database Vault管理者ガイド』の付録Bにある"Oracle Database Vaultの有効化および無効化"を参照してください。
- 管理タスクを実行するために、有効なコマンド・ルールを一時的に緩和する必要がある場合があります。このような場合は、コマンド・ルールを無効にする代わりに、Security Manager（DV_ADMINまたはDV_OWNERロールのアカウント）でログインして、ルール・セットをEnabledに設定し、有効になっているルール・セットに対する監査をSuccessまたはFailureに設定します。その後でタスクが完了したら、コマンド・ルールを元のルール・セットに設定し直します。
- コマンド・ルールを設計する際は、プロシージャが誤って無効にされる可能性があるバックアップなどの自動化プロセスについて慎重に検討します。Oracle Database Vaultの一連のファクタがtrueだと分かっている場合にコマンドを許可するルールを作成すると、これらのタスクを把握できます。ファクタの例は、使用されているプログラム、使用されているアカウント、またはクライアント・プログラムを実行しているコンピュータやネットワークなどです。

付録B - ファクタのヒント

ファクタを設定する際のガイドラインを次に示します。

- ファクタのIDがBy Factorsで特定されるように設定されている場合は、取得メソッドを指定しないでください。取得メソッドは、ファクタをBy MethodまたはBy Constantに設定した場合のみ必要です。
- ファクタに割当てルール・セットがある場合は、検証メソッドの使用を検討します。そうすることで、無効なIDが送信されないように検証できます。
- 取得メソッドから返される値が同じセッション内の複数の呼出し間で変わる可能性がある場合は、By Accessの評価オプションだけを指定します。たとえば、時間ベースのファクタが挙げられます。
- 従来のSQLおよびPL/SQLの最適化テクニックを使用して、ファクタの取得メソッドに使用する関数の内部ロジックを最適化します。パフォーマンスと最適化について、詳しくは『Oracle Database/パフォーマンス・チューニング・ガイド』を参照してください。
- 取得メソッドから返される個別の値が分かっている場合は、それぞれの値に信頼レベルを割り当てられるように各値のIDを定義します。ファクタに基づいたアプリケーション・ロジックで信頼レベルを使用できるため、信頼レベルによってファクタに値が追加されます。
- 複数のファクタに基づくセキュリティ・ポリシーの方が、少ないファクタに基づくセキュリティ・ポリシーより強力になります。他のファクタによって特定される新しいファクタを作成して、ファクタの組合せを、IDマップを使用する論理グループに格納できます。クライアントが提供するファクタは、クライアント・ソフトウェアが信頼されており、クライアント・ソフトウェアからの通信チャネルが保護されていると分かっている場合のみ信頼できます。複数ファクタ認可を使用すると、セキュリティ・レベルが大幅に向上します。
- 1つまたは複数のセキュリティ、エンドユーザー、または環境属性を渡すデータベース・クライアント・アプリケーションを設計して、関連するデータベース・セッションで利用可能になります。これを行うには、各属性に単一のファクタを作成し、割当てルール・セットを使用して、それらの属性を割り当てられるケースを制御します。たとえば、指定した名前のアプリケーション・サーバー・コンピュータで特定のWebアプリケーションを使用する場合のみ、などと指定できます。この方法で使用するOracle Database Vaultのファクタは、Oracleプロシージャの DBMS_SESSION.SET_IDENTIFIERとよく似ていますが、ファクタを設定できるケースを制御する機能も含まれています。DBMS_SESSION/パッケージついて、詳しくは『Oracle Database PL/SQL/パッケージ・プロシージャおよびタイプ・リファレンス』を参照してください。

Oracle Database Vaultベスト・プラクティス
2013年10月

著者：Kamal Tbeileh
共著者：Paul Needham

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

www.oracle.com

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

1010

Hardware and Software, Engineered to Work Together