Oracle® Database
Real Application Security 管理コンソール (RASADM)ユーザーズ・ガイド
19c

F16129-01(原本部品番号:E96298-01)

2019年1月

Oracle Database Real Application Security管理コンソール(RASADM)ユーザーズ・ガイド, 19c

F16129-01

目次

Oracle Database Real Application Security管理(RASADM)では、グラフィカル・ユーザー・インタフェースを使用して、Real Application Securityデータ・セキュリティ・ポリシーを作成できます。

Real Application Securityの概念を熟知していて、データ・セキュリティ・ポリシーを作成するための設計およびフローを理解している場合、はじめの5つのトピックに簡単に目を通したあと、トピック6および7に進み、ホーム・ページ・レイアウトの概要および操作の開始方法を理解します。ドキュメントのアクセシビリティの詳細は、トピック8を参照してください。

Real Application Security管理(RASADM)のインストールおよび構成

前提条件、インストールおよび構成タスクを実行し、その後、RASADMアプリケーションを実行します。

この節の内容は以下のとおりです。

前提条件

RASADMをインストールする前に、Oracle DatabaseインスタンスとApplication Expressの両方が起動され実行中であることを確認してください。

次の前提条件が必要です。

- Oracle Databaseリリース12.1.0.1以降
- Application Expressリリース5.0以降

インストール

OTNからRASADMをダウンロードしてインストールし、RASADMスキーマおよびRASADM APEXワークスペースを作成してAPEXセキュリティ機能を設定します。インストールでは、RASADMという名前のスキーマ・ユーザーが作成されます。外部プリンシパル・ストア(LDAP)のホストが提供されている場合は、LDAPが構成されます。

RASADMをインストールするには、次の手順を実行します。

1. OTNからRASADMをダウンロードします(Oracle Real Application Security (RAS)のダウンロード)。

2. ダウンロードしたzipファイルを選択したディレクトリに解凍します。

3. 解凍されたディレクトリ内で、ディレクトリをinstallerディレクトリに変更します。

4. AS SYSDBAをSQL*Plusに接続し、次のPL/SQLスクリプトを実行してRASADMをインストールします。

```
SQL> @rasadm_ins.sql
```

インストール・スクリプトを実行すると、次の出力が表示されます。

```
.
. Oracle RASADM installation
.........................................
.
. Creating schema user with privileges
.

RASADM provides data realm preview capability. If enabled, the administrator
will be able to view the data in any user table in the database.
Enable data preview capability? [No]

Enter a password for the RASADM admin user(admin): password
. Creating APEX workspace and admin user.
.
. Importing APEX application
.
Enter LDAP host name if you use external user and group (press ENTER if not):hostname
. Post configuration
.
. Done. Please review rasadm_ins.log for any errors.
.....................................
.
```

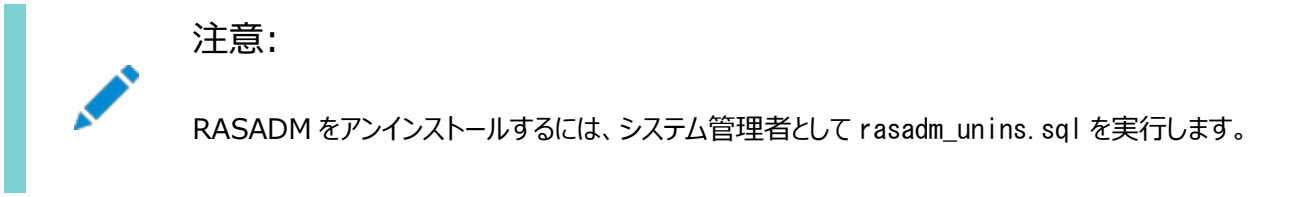
インストール・スクリプトでは次のことが行われます。

1. ロック済アカウントと期限切れのパスワードを持つRASADMという名前のスキーマ・ユーザーを作成し、特定のAPIをコンパイルするために必要な、ユーザーに制限された権限を、そのユーザーに付与します。

2. データ・レルムのプレビュー機能は、RASロールRASADM_POLICY_ADMINに付与され、このロールは管理者に付与されます。

3. Application Express管理者のUIを使用してRASADMワークスペースを作成し、RASADMアプリケーション・コードをRASADMワークスペースにインポートしてから、Application Expressセキュリティ機能を設定します。

4. 外部プリンシパル・ストア(LDAP)を構成します。LDAPホストが指定されている場合、指定したLDAPホストおよびポートでのCONNECTおよびRESOLVE権限をRASADMユーザーに付与するため、ネットワークACLが作成されます。
RASADMユーザーは、インストール後にRASADM UIから外部プリンシパル・ストア(LDAP)を構成するよう選択することもできます。その場合、データ・セットにネットワークACLを手動で付与することは、RASADM管理者の職責です。



注意:

RASADM をアンインストールするには、システム管理者として rasadm_unins.sql を実行します。

構成

ユーザー管理の一部として、RASADMにログイン可能なadminユーザーを構成し、その後Application Expressおよびワークスペース構成を実行してSSL設定を実行します。

次の項では、構成タスクについて説明します。

- ユーザー管理
- Application Expressインスタンス・レベルの構成

ユーザー管理

これは、RASADMにログインできるadminユーザーです。RASADMランタイム・ユーザーは、データベースに直接ログオンできる、パスワードが指定されたReal Application Securityユーザーです。RASADMにアクセスするには、ユーザーは、Real Application Securityロール(RASADM_POLICY_ADMINまたはRASADM_USER_ADMIN、あるいは両方のロール)が付与されている必要があります。

RASでは、2つの管理ロール(RASADM_POLICY_ADMINおよびRASADM_USER_ADMIN)が提供されています。

RASADM_POLICY_ADMINは、Real Application Securityロールで、ポリシー管理を実行する権限があります。たとえば、このロールを持つReal Application Securityユーザーは、ポリシー、権限、権限クラス、ネームスペース、通常のロールおよび動的ロールを作成できます。このユーザーは、Real Application Securityユーザーを作成することはできません。

RASADM_USER_ADMINは、Real Application Securityロールで、ユーザー管理を実行する権限があります。たとえば、このロールを持つReal Application Securityユーザーは、ユーザー、通常のロールおよび動的ロールを作成できます。このユーザーは、RASADMで提供される残りの機能を使用することはできません。

ただし、両方のロールには、すべてのページでレポートを表示する権限があります。

RASADMユーザーは、データベースでReal Application Security管理API (PL/SQL内)を使用して作成できます。

RASADMには、2つの種類のユーザーが必要です。1つは、ポリシー管理タスクのみを実行できるユーザー、もう1つは、ポリシー管理とユーザー管理の両方を実行できるユーザーです。前者には、RASADM_POLICY_ADMIN Real Application Securityロールを付与する必要があり、後者には、RASADM_POLICY_ADMINとRASADM_USER_ADMINの両方のReal Application Securityロールを付与する必要があります。

関連項目:

構文および必要な権限については、『Oracle Database Real Application Security管理者および開発者ガイド』のReal Application Security管理API (PL/SQL)に関する項を参照してください。

この項には次のトピックが含まれます:

- データ・レルムのプレビュー機能の有効化
- RASADMランタイム・ユーザーの作成
- パスワード・ポリシーの実装

データ・レルムのプレビュー機能の有効化

インストール・スクリプトの外部で、データ・レルムのプレビュー機能をRASADM_POLICY_ADMIN Real Application

Securityロールを持つユーザーに対して有効であることを確認する必要があり、インストール時に選択されているオプションが「いいえ」の場合は、SYSユーザーとして次を実行します。

表でのSELECT権限を、プレビュー機能を必要とするRASADM_DB_POLICY_ADMINロールに明示的に付与します。それ以外の場合、SELECT ANY TABLEシステム権限をRASADM_DB_POLICY_ADMINロールに付与できます。

また、Real Application Securityポリシーのセキュリティ・チェックを省略するために、EXEMPT ACCESS POLICY権限をRASADM_DB_POLICY_ADMINロールに付与できます。

前述の権限をユーザー定義の任意のデータベース・ロールに付与することもできます。このロールはRASADM_POLICY_ADMIN Real Application Securityロールに付与される必要があります。

RASADMランタイム・ユーザーの作成

SYS管理者のみが、Real Application SecurityロールRASADM_POLICY_ADMINまたはRASADM_USER_ADMINあるいは両方のロールを持つこのadminユーザーを作成する次のPL/SQLスクリプトを実行することによって、RASADM直接ログオン・アプリケーション・ユーザーを追加で作成できます。

SYS管理者が作成できる2つのタイプのユーザーは、次のとおりです。

- ポリシー管理とユーザー管理の両方を実行できる管理者ユーザー。

```
-- Create runtime user to perform both Policy and User Administration for RASADM
DECLARE
  rg_list XS$ROLE_GRANT_LIST;
BEGIN
  xs_principal.create_user(name=>'admin');
  sys.xs_principal.set_password('admin', 'welcome1', XS_PRINCIPAL.XS_SALTED_SHA1);
  rg_list :=
XS$ROLE_GRANT_LIST(XS$ROLE_GRANT_TYPE('RASADM_POLICY_ADMIN'),XS$ROLE_GRANT_TYPE('RASADM_USER_A
DMIN'));
  xs_principal.grant_roles('admin', rg_list);
END;
/
```

- ポリシー管理のみを実行できる管理者ユーザー。

```
-- Create runtime user to perform both Policy Administration for RASADM
DECLARE
  rg_list XS$ROLE_GRANT_LIST;
BEGIN
  xs_principal.create_user(name=>'admin');
  sys.xs_principal.set_password('admin', 'welcome1', XS_PRINCIPAL.XS_SALTED_SHA1);
  rg_list := XS$ROLE_GRANT_LIST(XS$ROLE_GRANT_TYPE('RASADM_POLICY_ADMIN'));
  xs_principal.grant_roles('admin', rg_list);
END;
/
```

パスワード・ポリシーの実装

adminユーザーのパスワード・ポリシーを実装します。

adminユーザーのパスワード・ポリシーは、Real Application Securityで直接サポートされています。

関連項目:

『Oracle Database Real Application Security管理者および開発者ガイド』の、直接ログイン・ユーザーの作成、プロファイルの作成およびパスワードの設定の手順に関する項。

Application Expressインスタンス・レベルの構成

Application ExpressおよびワークスペースのApplication Express管理者によってApplication Expressインスタンス・レベルで、またはワークスペース管理者によってワークスペース・レベルで行う必要がある構成です。

この構成には、SSL設定の実行が含まれています。SSLを次のように使用することを強くお薦めします。

- ブラウザとHTTP Server間

  『Oracle Application Expressアプリケーション・ビルダー・ユーザーズ・ガイド』のSecure Sockets Layer (SSL)の利用に関する項、および『Oracle Application Expressアプリケーション・ビルダー・ユーザーズ・ガイド』のHTTPSの必要性に関する項を参照してください。

  SSLの設定の詳細は、HTTP Serverのドキュメントを参照してください。

- HTTP Serverとデータベース間

  『Oracle Application Express管理ガイド』のウォレット情報の構成に関する項、および『Oracle XML DB開発者ガイド』のHTTPリスナーのSSLの使用の有効化に関する項を参照してください。『Oracle Databaseセキュリティ・ガイド』のSecure Sockets Layer認証の構成に関する項を参照してください。

- データベースとLDAP間

  『*Oracle Fusion Middleware Oracle Internet Directory*管理者ガイド』のSecure Sockets Layer (SSL)の構成に関する項、『*Oracle Fusion Middleware Oracle Internet Directory*管理者ガイド』のLDAPコマンドの使用によるSSLの構成に関する項、および『Oracle Application Expressアプリケーション・ビルダー・ユーザーズ・ガイド』のLDAPディレクトリ検証の設定に関する項を参照してください。

> 注意:
>
> RASADM のインストール・スクリプトの一部として、Application Express は、「セキュリティ設定」で「Real Application Security の許可」を「はい」に設定するように、インスタンス・レベルで変更されます。

関連項目:

詳細は、『Oracle Application Expressアプリケーション・ビルダー・ユーザーズ・ガイド』のアプリケーション・セキュリティの管理に関する章を参照してください。

RASADMアプリケーションの実行

RASADMにログインするユーザーの種類に基づいて、特定のUIコンポーネント(ボタンなど)は、権限のないユーザーには非表示になります。たとえば、「ユーザー管理」のすべてのボタンは、これらのアクションを実行する権限を持たないユーザーには非表示になります。

次のURLは単なる例で、実際のURLは、現在のApplication Express構成に基づいています。正しいURLを指定してくださ

い。次に、インストール時に指定したのと同じパスワードを使用してRASADM管理者としてログインします。

RASADMアプリケーションを実行するには、ブラウザで次のようなURL (https://www.example.com:8080/apex/f?p=rasadm)を入力します。

HTTPSをオンにすることをお薦めします。

RASADM adminユーザー、またはインストール時に指定されたパスワードを使用したインストール後に作成された任意のユーザーとして、ログインできます。

詳細情報

詳細は、Real Application Securityディスカッション・フォーラムおよびReal Application Securityドキュメントを参照してください。

詳細は、次のリソースを参照してください。

- Real Application Securityディスカッション・フォーラム: Database Security - 一般的なディスカッション
- Real Application Securityドキュメント: 『Oracle Database Real Application Security管理者および開発者ガイド』

Oracle Database Real Application Securityによるデータ・セキュリティについて

有効なセキュリティでは、どのアプリケーション・ユーザー、アプリケーションまたは機能が、どのような種類の操作を実行するために、どのデータにアクセスできるかを定義する必要があります。

したがって、有効なセキュリティには次の3つの次元があります。

1. どのアプリケーション・ユーザーか(**プリンシパル**)
2. どの操作を実行できるか(**アプリケーション権限**)
3. どのデータを対象とするか(**データ・レルム**)

これらの3つの次元について、それぞれ(1)プリンシパル、(2)アプリケーション権限および(3)オブジェクト(データ・レルム)を定義します。プリンシパルは、ユーザーおよびロールです。ユーザーはアプリケーション・ユーザーで、ロールは、アプリケーション・ユーザーの属性、システムの状態、またはコードの一部を表します。

プリンシパルは、ACLでアプリケーション権限を付与されます。次に、これらのACLは、表データの行および列を保護するデータ・セキュリティ・ポリシーを定義することで、データに関連付けられます。

RASADMを使用して、次のようにReal Application Securityデータ・セキュリティ・ポリシーを作成します。

1. 「Real Application Securityで使用される用語」で説明されている、データ・セキュリティ・ポリシーの基本的な要素を理解します。
2. 「設計フェーズ」で説明されている段階的な方法で、これらの基本的な要素を結合する方法を理解します。
3. 「開発フロー」で説明されている段階的な方法で、RASADMを使用してデータ・セキュリティ・ポリシーを作成します。

Real Application Securityで使用される用語

RASADMアプリケーションで使用されているReal Application Securityの概念をより深く理解できるように用語を定義します。

アプリケーション・ユーザーは、データベースに認識されているアプリケーション・エンド・ユーザー・アイデンティティです。これらのユーザーは、スキーマがなく、データベース・オブジェクトまたはリソースを所有しません。アプリケーション・ユーザーは、中間層を介してデータベースにアプリケーション・セッションを作成し、直接ログオン・アプリケーション・ユーザー・アカウントを介してデータベースにアプリケーション・セッションを直接作成できます。RASADMを使用して、アプリケーション・ユーザーを作成できます。

アプリケーション権限は、アプリケーション・レベルの操作の実行を制御する名前付き権限です。操作は、データまたはアプリケーション・アーティファクト(ワークフロー・タスクを表すUIアーティファクトやWebアプリケーションのボタンおよびページなど)に対して指定できます。アプリケーション権限は、Real Application Security DML権限クラスのSELECT、INSERTおよびDELETEなどの他のアプリケーション権限を暗示できます。

アプリケーション・ロールは、ロールが付与されたアプリケーション・ユーザーのグループを表します。アクセス制御リスト(ACL)内で、権限をロールに付与できます。これは、ロールが付与されたすべてのユーザーにこれらの権限を付与することと同じ結果になります。アプリケーション・ロールは、アプリケーション・ユーザーまたはアプリケーション・ロールにのみ付与できます。

動的アプリケーション・ロールは、ユーザーがSSLを使用してログオンする場合や、特定の期間ログオンする場合など、一定の状況下でのみ有効になるアプリケーション・ロールです。動的アプリケーション・ロールを他のアプリケーション・ロールまたはユーザーに付与することはできませんが、他のアプリケーション・ロールを動的アプリケーション・ロールに付与することは可能です。

権限クラスは、アプリケーション権限のセットの有効範囲です。権限クラスは、データ・セキュリティ・ポリシーのアクセス制御リスト(ACL)内で付与できる権限のセットを定義します。

アクセス制御エントリ(ACE)は、特定のプリンシパル(アプリケーション・ユーザーまたはアプリケーション・ロール)に対してアプリケーション権限を付与または拒否します。

アクセス制御リスト(ACL)は、権限付与の名前付きリストです。Oracle Real Application Security ACLでは、権限付与に様々な制約(所定の権限の剥奪など)を付けることができます。作成したACLが独自の権限クラスで定義されたカスタム・アプリケーション権限のセットに依存している場合、その権限クラスでのみ権限を付与できます。

データ・レルムは、ACLに関連付けられた関連するアプリケーション表のグループ内の、行の論理セットのコレクションです。データ・レルムは、アプリケーション・レベルのリソースやビジネス・オブジェクトを表し、SQL述語を使用して定義されます。認可はACLで定義され、ACLはどの権限がデータ・セット上のどのプリンシパルに付与されるかを指定します。RASADMでは、次のデータ・レルム・タイプがサポートされています。

- 標準 - 保護されるデータ・セット、および認可の実行に使用されるACLの一部をSQL述語で指定する際にデータ・セットを保護します。
- パラメータ化 - 使用されるパラメータをSQL述語で、および権限が付与されるそのパラメータの値をACLで指定する際にデータ・セットを保護します。たとえば、department=&DEPT_IDを考えてみます。パラメータ名DEPT_IDが記号&に続いています。この場合、パラメータ名DEPT_IDは、様々な部門IDに関連付けられています。これにより、各DEPT_IDの値に部門ID固有の多くのデータ・レルムを作成することなく、部門IDに基づいて権限付与を作成できます。
- 継承 - マスター・ディテール・ポリシーと呼ばれ、マスター・オブジェクトを指すことにより、マスター・オブジェクトのポリシーを使用してディテール・オブジェクトを保護します。親スキーマと親オブジェクト(列)をマスターとして指定し、親列と子列(ディテール)オブジェクトまたは定数値との間の1対1の関係を構築します。複数の親=子ペアを使用して、関係を構築できます。複数の親=子ペアを使用する場合、定数値は、結合条件として他の親=子ペアを使用して、1対1の関係を形成する必要があります。親のオブジェクト・ポリシーを使用してさらに子列を保護する場合、オプションでwhen条件を入力できます。

データ・セキュリティ・ポリシーは、ACLと関連付けることで、データ・レルムを保護します。データベース・レコードは、行レベルと列レベルの両方で、ファイングレイン・アクセス制御を使用して保護できます。データ・セキュリティ・ポリシーは、次の2つの機能を実行します。

- データ・レルム認可。

データ・レルム認可は、1つ以上の行のデータ・レルムで保護するデータを指定し、1つのアクセス制御リスト(ACL)に各データ・レルムを関連付けます。ACLは、アプリケーション権限を使用したどの種類のアクセスが特定のプリンシパルに付与または拒否されるかを指定します。これにより、データ・レルムの行へのアクセスを制御して、データ・レルム認可と呼ばれるものを作成します。指定されたACLは、指定されたデータ・レルムを保護し、特定のアプリケーション・ユーザーまたはアプリケーション・ロール(プリンシパル)へのアクセスを制御します。

- 列認可。

  列認可では、オプションで、特定の列を保護するために追加のアプリケーション権限を適用します。これは、追加のカスタム・アプリケーション権限を関連付ける機密列データの列認可セキュリティを追加する必要がある場合に便利です。

つまり、ログインしたアプリケーション・ユーザーは、関連付けられたACLのアプリケーション権限に基づいて、データ・レルム内のレコード(データの個々の行を含む)に対してDMLなどの操作の実行のみが許可されます。このように、データ・セキュリティ・ポリシーは、関連付けられたACLに含まれるアプリケーション権限を持つアプリケーション・ユーザーにアクセスを許可することでデータ・レルムを保護するデータ・レルム認可および列認可で構成されます。

認可サービスは、権限がユーザーに付与されているかどうかを確認します。

セッション・**ネームスペース**属性は、アクセス制御ポリシーが関連付けられたアプリケーション・ネームスペースでの属性/値ペアのコレクションです。アプリケーションは、通常、異なるアプリケーション・セッション全体で同じネームスペースを使用する必要があります。ネームスペース・テンプレートを作成して、ネームスペースを定義および初期化できます。ネームスペース・テンプレートは、ネームスペースとそのプロパティを定義します。これを使用して、アプリケーション・セッションでネームスペースを初期化します。

アプリケーション・セッションは、データベース内でアプリケーション・ユーザーのセキュリティ・コンテキスト、ロールおよびネームスペース属性に対応する、アプリケーション・ユーザーのセッションです。

設計フェーズ

設計フェーズには、データ・アクセスを制御するためにアプリケーション権限を必要とする、アプリケーションが実行するすべてのタスクの識別が含まれます。

たとえば、設計フェーズ中に、アプリケーション・ポリシー・デザイナは次を識別する必要があります。

1. アクセス制御が必要な一連のアプリケーション・レベル操作。
2. アプリケーション・レベル操作の中でアクセスできる表やビューの行と列。
3. それらの操作を実行できる一連のアクターまたはプリンシパル(ユーザーおよびロール)。
4. 表またはビューの行を特定するランタイム・アプリケーション・セッション属性。これらの属性名は、認可する行を選択する述語内で使用され、属性の値はアプリケーションの実行時に設定されます。

開発フロー

開発フェーズでは、RASADM管理者として、RASADMを使用してデータ・セキュリティ・ポリシーを開発します。

次の手順に従い、データ・セキュリティ・ポリシーを開発します。

1. 対応するアプリケーション・ユーザーおよびロールを作成します。外部ディレクトリ・サーバーを使用している場合は、そのディレクトリ・サーバーでアプリケーション・ユーザーおよびロールまたはユーザー・グループを作成します。次の手順に従って、これらのプリンシパルをデータベース固有になるように作成します。

   a. アプリケーション・ロールを作成し、必要に応じてアプリケーション・ロールをアプリケーション・ロールに付与します。「アプリケーション・ロールの作成」を参照してください。

b. アプリケーション・ユーザーを作成し、アプリケーション・ロールをアプリケーション・ユーザーに付与します。「アプリケーション・ユーザーの作成」を参照してください。

c. 外部ストアのプリンシパルを使用している場合、ユーザーおよびロールをフェッチするディレクトリ・サーバーを構成します。「構成」を参照してください。

d. 外部ディレクトリ・サーバーのユーザーおよびロールの場合、RASADMをディレクトリ・サーバーとともに使用するためのパラメータ設定を管理します。「設定の管理」を参照してください。

2. アプリケーションのセキュリティ・ポリシーの開発に使用する各権限クラスを作成します。各権限クラスは、ACLで定義して参照可能で、アプリケーション・ユーザーおよびアプリケーション・ロールに付与することもできる1つ以上の適切な権限で構成されます。各権限クラスは、ACLを使用して、データ・セキュリティ・ポリシーの必要なアプリケーション・レベルの操作を認可します。「アプリケーション権限クラスの作成」を参照してください。

3. 異なるアプリケーション・セッション間で使用できる1つ以上のセッション・ネームスペースを作成します。これは、セッション・ネームスペース、そのプロパティ(アプリケーション属性)のセット、リストからの選択または作成が可能な、関連付けられたアクセス制御ポリシーまたはACLの定義で構成されます。「ネームスペースの作成」を参照してください。

4. 各データ・レルムとACLを関連付けることで、データ・セキュリティ・ポリシーを作成します。必要に応じて、データ・レルム認可と列認可の両方を作成します。このプロセスは、次の4つの部分で構成されます。

a. ポリシー情報 - 保護されるオブジェクトと、オブジェクトを保護する権限クラスを選択し、ポリシー名を指定して、ポリシー所有者を選択します。「データ・セキュリティ・ポリシーの作成」の手順3を参照してください。

b. 列レベルの認可 - 保護される列の名前を選択し、列にアクセスするために付与される権限を選択します。この列は手順3aで選択した権限クラスに関連付けられています。「データ・セキュリティ・ポリシーの作成」の手順4を参照してください。

c. データ・レルム認可 - 保護されるデータ・レルムを表すSQL述語を作成し、それぞれをデータ・レルム付与リストに追加します。それから、データ・レルムを保護するACLを選択または作成します。次に、各プリンシパルと、適切な権限を選択することでそのプリンシパルが許可された認可か拒否された認可かどうかで構成される、権限付与リストに追加される権限付与を作成します。「データ・セキュリティ・ポリシーの作成」の手順5を参照してください。

d. ポリシーの適用 - 作成しているデータ・セキュリティ・ポリシーを適用、削除、有効化または無効化でき、特定の適用オプションを指定するよう選択できます。これにより、表またはビューの所有者は、このデータ・セキュリティ・ポリシー、およびこのポリシーの文タイプを施行するかどうかを省略できます。「データ・セキュリティ・ポリシーの作成」の手順6を参照してください。

Real Application Security管理の「ホーム」ページ

Real Application Security管理の**「ホーム」**ページでは、データ・セキュリティ・ポリシー・アクティビティの概要が提供されます。

次の内容について説明します。

- 概要
- ポリシー変更レポート
- 監査レポート

概要

Real Application Security管理の概要を説明します。

データ・セキュリティ・ポリシーの作成手順を示します。

ポリシー・サマリー・レポート

ポリシー・サマリー・レポートは、2つのレポートで構成されます。

内容は次のとおりです。

- 「ユーザーとロール」レポート
- データ・セキュリティ・レポート

「ユーザーとロール」レポート

アプリケーション・ユーザーおよびロールのエンティティが外部ストアからおよびデータベース内で作成された数を表示します。

「件数」リンクをクリックして、エンティティのサマリー・レポートを表示します。

データ・セキュリティ・レポート

データ・セキュリティ・エンティティ(データ・セキュリティ・ポリシー、データ・レルム、権限クラスなど)が作成された数を表示します。

「件数」リンクをクリックして、エンティティのサマリー・レポートを表示します。

ポリシー変更レポート

ポリシー変更レポートは、5つのレポートで構成されます。

内容は次のとおりです。

- 変更数レポート
- データ・セキュリティ・ポリシー・レポート
- データ・レルムへの権限付与レポート
- データベース内のアプリケーション・ロール・レポート
- データベース内のアプリケーション・ユーザー・レポート

変更数レポート

各期間に各エンティティで発生した変更の数を表示します。

データ・セキュリティ・ポリシー・レポート

ポリシーが変更および作成された場合、その名前と説明、ターゲット・オブジェクトおよび現在のステータスを、ポリシーごとに表示します。

「次」をクリックして、次のレコードのセットを表示します。

データ・レルムへの権限付与レポート

データ・レルムが変更および作成された場合、ポリシー名、ACLが付与されたデータ・レルム名、およびデータ・レルムに付与されたACLを、データ・レルムごとに表示します。

「次」をクリックして、次のレコードのセットを表示します。

データベース内のアプリケーション・ロール・レポート

プリンシパル・タイプ、ロールまたは動的ロールが変更および作成された場合、そのロール名、説明、およびタイプをそれぞれ表示します。

「次」をクリックして、次のレコードのセットを表示します。

データベース内のアプリケーション・ユーザー・レポート

ユーザーが変更および作成された場合、そのユーザー名、説明、およびステータスを、ユーザーごとに表示します。

「次」をクリックして、次のレコードのセットを表示します。

監査レポート

監査レポートは、2つのレポートで構成されます。

内容は次のとおりです。

- 監査ポリシー
- 有効化された監査ポリシー

監査ポリシー

監査ポリシーの名前および他の重要な情報を表示します。

監査ポリシーに関連付けられた条件、監査ポリシーで定義された監査オプション、監査ポリシーの条件に関連付けられた評価オプション(STATEMENT、SESSIONまたはINSTANCE)、および監査ポリシーが非CDBで共通の監査ポリシー(YES)、またはローカル(NO)、またはNULLであるかを表示します。**「次」**をクリックして、次のレコードのセットを表示します。

有効化された監査ポリシー

ポリシー有効化の対象のデータベース・ユーザー名および他の重要な情報を表示します。

監査ポリシーがすべてのユーザーで有効な場合、その値はALL USERSです。監査ポリシーの名前、監査ポリシーの有効なオプション(BY、EXCEPTまたはDISABLED)は、監査ポリシーが監査成功イベントで有効である(YES)か有効でない(NO)かを示し、監査ポリシーが監査失敗イベントで有効である(YES)か有効でない(NO)かを示します。**「次」**をクリックして、次のレコードのセットを表示します。

概要

Real Application Security管理の**「ホーム」**ページから、アプリケーションを保護するためのデータ・セキュリティ・ポリシーの開発を開始できます。

次のタブに移動してタスクを実行できます。

注意:

RASADM アプリケーションを使用して作成されたすべての Real Application Security エンティティの名前

は、大文字と小文字が区別されます。

- **ポリシー** - データ・セキュリティ・ポリシーを作成、更新および削除します(データ・レルムおよび列認可の追加および削除など)。定義された各ポリシーに対して、ポリシーを有効化、無効化、適用または削除するようステータスを設定します。
- **権限** - 権限クラスを作成、更新および削除します(権限クラスへのアプリケーション権限の追加または権限クラスからのアプリケーション権限の削除など)。
- **ネームスペース** - ネームスペースを作成、更新および削除します(ネームスペースへのアプリケーション属性の追加またはネームスペースからのアプリケーション属性の削除など)。
- **ユーザー** - アプリケーション・ユーザーを作成、更新および削除します(アプリケーション・ユーザーへのアプリケーション・ロールの付与およびアプリケーション・ユーザーからのアプリケーション・ロールの取消しなど)。
- **ロール** - アプリケーション・ロールおよび動的アプリケーション・ロールを作成、更新および削除します(アプリケーション・ロールの場合、アプリケーション・ロールへのロール付与の追加またはアプリケーション・ロールからのロール付与の削除、および動的アプリケーション・ロールの場合、動的アプリケーション・ロールへのオブジェクト権限付与の追加または動的アプリケーション・ロールからのオブジェクト権限付与の削除など)。
- **設定** - Real Application Security管理をディレクトリ・サーバーとともに使用するためのパラメータ設定を更新します。

Real Application Security管理を使用すると、アプリケーションを保護するためのデータ・セキュリティ・ポリシーを開発する次のタスクを実行できます。

1. アプリケーション・ユーザーの管理
2. アプリケーション・ロールおよび動的アプリケーション・ロールの管理
3. アプリケーション権限クラスの管理
4. アプリケーションのデータ行およびデータ列を保護するためのデータ・セキュリティ・ポリシーの管理
5. ネームスペースの管理
6. 設定の管理

次に続くトピックでは、Real Application Security管理を使用してこれらの各タスクを実行する方法の詳細を説明します。

アプリケーション・ユーザーの管理

「ユーザー」タブから、RASADMユーザーはデータベースに既知のアプリケーション・ユーザーを作成、更新または削除します。アプリケーション・ユーザーは、中間層を介してデータベースにアプリケーション・セッションを作成し、直接ログオン・アプリケーション・ユーザー・アカウントを介してデータベースにアプリケーション・セッションを直接作成できます。

アプリケーション・ユーザーの管理には、次のトピックがあります。

- アプリケーション・ユーザーの作成
- アプリケーション・ユーザーの更新
- アプリケーション・ユーザーの削除

アプリケーション・ユーザーの作成

「ユーザー」タブで、このアプリケーションのデータ・セキュリティ・ポリシーに追加する必要がある各アプリケーション・ユーザーを作成します。

アプリケーション・ユーザーを作成するには、次の手順を実行します。

1. **「ユーザー」**タブをクリックします。

> 注意:
>
> RASADM_USER_ADMIN Real Application Security ロールを持たないユーザーには、手順 2 から 5 は適用されません。

2. **「ユーザー」**ページで、**「作成」**をクリックします。

> 注意:
>
> RASADM_USER_ADMIN Real Application Security ロールを持たないユーザーには、**「作成」**ボタンは表示されません。

3. **「アプリケーション・ユーザー」**セクションの**「ユーザーの管理」**ページで、次のフィールドに情報を入力します。赤いアスタリスクは必須フィールドを示しています。

   - **ユーザー名** - アプリケーション・ユーザーの名前を入力します。名前は大文字と小文字が区別されます。
   - **説明** - このアプリケーション・ユーザーに関する簡単な説明を入力します。
   - **デフォルトのスキーマ** - (^)をクリックして、アクセスするこのアプリケーション・ユーザーのスキーマを選択します。
   - **ロール・デフォルト有効** - デフォルトのアプリケーション・ロールが有効である(「はい」)か有効でない(「いいえ」)かを選択します。
   - **ステータス** - アプリケーション・ユーザーがアクティブか非アクティブになるかを選択します。
   - **開始日** - カレンダ・アイコンをクリックして、このアプリケーション・ユーザーの有効な開始日を選択するか、フィールドを空白のままにします。開始日を指定しないと、このアプリケーション・ユーザーは常に有効であることを意味します。
   - **終了日** - カレンダ・アイコンをクリックして、このアプリケーション・ユーザーの有効な終了日を選択するか、フィールドを空白のままにします。終了日を指定しないと、このアプリケーション・ユーザーは常に有効であることを意味します。開始日を指定する場合、終了日も指定する必要があります。

   「ロール付与」セクションで、アプリケーション・ユーザーに付与されるアプリケーション・ロールを選択します。これを選択するには、アプリケーション・ロールがすでに作成されている必要があります。赤いアスタリスクは必須フィールドを示しています。次のフィールドに情報を入力します。

   - **ロール」** - (^)をクリックして、このアプリケーション・ユーザーに付与されるアプリケーション・ロールを選択します。
   - **開始日** - カレンダ・アイコンをクリックして、このロール付与の有効な開始日を選択するか、フィールドを空白の

ままにします。開始日を指定しないと、このロール付与は常に有効であることを意味します。

- **終了日** - カレンダ・アイコンをクリックして、このロール付与の有効な終了日を選択するか、フィールドを空白のままにします。終了日を指定しないと、このロール付与は常に有効であることを意味します。開始日を指定する場合、終了日も指定する必要があります。

「追加」をクリックして、ロールを付与します。

このアプリケーション・ユーザーにさらにアプリケーション・ロールを付与するには、別のロールを選択し、必要に応じて開始日と終了日を選択して、**「追加」**などをクリックします。

このユーザーから1つ以上のアプリケーション・ロールを削除するには、各ロールを選択し、**「削除」**をクリックします。

4. **「変更の適用」**をクリックして、このアプリケーション・ユーザーを作成します。
5. このアプリケーションのデータ・セキュリティ・ポリシーに追加する必要がある各アプリケーション・ユーザーに対して、手順1から4を繰り返します。

アプリケーション・ユーザーの更新

「ユーザー」タブから、アプリケーション内のアプリケーション・ユーザーを更新します。RASADMユーザーは、追加のアプリケーション・ロールを付与したり、アプリケーション・ユーザーから一部のアプリケーション・ロールを削除したりできます。

アプリケーション・ユーザーの情報を更新するには、次の手順を実行します。

1. **「ユーザー」**タブをクリックします。
2. 更新する**「ユーザー」**列で、アプリケーション・ユーザーの名前を選択します。
3. **「ユーザーの管理」**ページで、更新を行います。

   アプリケーション・ユーザーにさらにアプリケーション・ロールを付与するには、別のロールを選択し、必要に応じて開始日と終了日を入力して、**「追加」**をクリックします。

   アプリケーション・ユーザーから1つ以上のアプリケーション・ロールを削除するには、**直接ロール付与**セクションで削除される各ロールを選択し、**「削除」**をクリックします。

   アプリケーション・ユーザーが1つ以上のアプリケーション・ロールに間接的に付与されている場合、これらのアプリケーション・ロールは、ルート・ロールの名前と付与パスとともに、**間接ロール付与**セクションにリストされます。

注意:

RASADM_USER_ADMIN Real Application Security ロールを持たないユーザーには、**「取消」**を除くすべてのボタンは表示されません。

4. **「変更の適用」**をクリックして、変更を保存します。

関連項目:

「ユーザーの管理」ページ上のフィールドの詳細は、「アプリケーション・ユーザーの作成」を参照してください。

アプリケーション・ユーザーの削除

「ユーザー」タブから、このアプリケーションには不要となったアプリケーション・ユーザーをすべて削除します。

アプリケーション・ユーザーを削除するには、次の手順を実行します。

1. **「ユーザー」**タブをクリックします。
2. **「ユーザー」**ページの**「ユーザー」**列で、削除するアプリケーション・ユーザーの名前をクリックします。
3. **「ユーザーの管理」**ページの**「アプリケーション・ユーザー」**セクションで、**「削除」**をクリックします。

> 注意:
>
> RASADM_USER_ADMIN Real Application Security ロールを持たないユーザーには、**「削除」**ボタンは表示されません。

アプリケーション・ロールおよび動的アプリケーション・ロールの管理

「ロール」タブから、標準アプリケーション・ロールと動的アプリケーション・ロールを作成および付与します。アプリケーション・ロールは、アプリケーション・ユーザーまたは別のアプリケーション・ロールに対して付与できます。動的アプリケーション・ロールは、別のアプリケーションまたはアプリケーション・ロールに対しては付与できず、特定の状況化でのみ有効化されます。

アプリケーション・ロールおよび動的アプリケーション・ロールの管理には、次のトピックがあります。

- アプリケーション・ロールの作成
- アプリケーション・ロールの更新
- アプリケーション・ロールの削除

アプリケーション・ロールの作成

このアプリケーションのデータ・セキュリティ・ポリシーに必要なアプリケーション・ロールおよび動的ロールを作成します。

アプリケーション・ロールを作成するには:

1. **「ロール」**タブをクリックします。
2. **「ロール」**ページで、**「ロールの作成」**をクリックします。
3. **「アプリケーション・ロール」**セクションの**「ロールの管理」**ページで、次のフィールドに情報を入力します。赤いアスタリスクは必須フィールドを示しています。
    - **ロール名** - アプリケーション・ロールの名前を入力します。名前は大文字と小文字が区別されます。
    - **説明** - このアプリケーション・ロールの簡単な説明を入力します。
    - **ロール・タイプ** - 「標準」または「動的」を選択します。**「ロール・タイプ」**: 「標準」 = アプリケーション・ロール、「動的」 = 動的アプリケーション・ロール。
        - **REGULAR**

          デフォルトで有効 - 作成時にこのアプリケーション・ロールを有効にする(「はい」)か有効にしない

(「いいえ」) (デフォルト)かを選択します。

開始日 - カレンダ・アイコンをクリックして、このアプリケーション・ロールの有効な開始日を選択するか、フィールドを空白のままにします。開始日を指定しないと、このアプリケーション・ロールは常に有効であることを意味します。

終了日 - カレンダ・アイコンをクリックして、このアプリケーション・ロールの有効な終了日を選択するか、フィールドを空白のままにします。終了日を指定しないと、このアプリケーション・ロールは常に有効であることを意味します。開始日を指定する場合、終了日も指定する必要があります。

- **DYNAMIC**

  継続期間 - 動的アプリケーション・ロールの期間(分単位)を入力します。

  有効範囲 - 動的アプリケーション・ロールの有効範囲属性を入力します。**「セッション」**は、デフォルトで、有効化された動的アプリケーション・ロールは、セッションから連結解除して再度セッションに連結した場合でも、有効な状態が続く(セッションの再連結時に無効化するように明示的に指定していない場合)ことを意味します。**「リクエスト」**は、動的アプリケーション・ロールはセッションの連結解除後に無効になることを意味します。

「ロール付与」セクションで、アプリケーション・ロールに付与されるアプリケーション・ロールを選択します。これを付与するには、ロールがすでに作成されている必要があります。赤いアスタリスクは必須フィールドを示しています。次のフィールドに情報を入力します。

- **ロール」** - (^)をクリックして、このアプリケーション・ロールに付与されるアプリケーション・ロールを選択します。
- **開始日** - カレンダ・アイコンをクリックして、このロール付与の有効な開始日を選択するか、フィールドを空白のままにします。開始日を指定しないと、このロール付与は常に有効であることを意味します。
- **終了日** - カレンダ・アイコンをクリックして、このロール付与の有効な終了日を選択するか、フィールドを空白のままにします。終了日を指定しないと、このロール付与は常に有効であることを意味します。開始日を指定する場合、終了日も指定する必要があります。

「追加」をクリックして、ロールを付与します。

このアプリケーション・ロールにさらにアプリケーション・ロールを付与するには、別のアプリケーション・ロールを選択し、必要に応じて開始日と終了日を選択して、**「追加」**などをクリックします。

このアプリケーション・ロールから1つ以上の付与されたアプリケーション・ロールを削除するには、削除される各ロールを選択し、**「削除」**をクリックします。

4. **「変更の適用」**をクリックして、アプリケーション・ロールを作成します。
5. このアプリケーションのデータ・セキュリティ・ポリシーに追加する必要がある各アプリケーション・ロールに対して、手順1から4を繰り返します。

関連項目:

アプリケーション・ロールおよび動的アプリケーション・ロールの詳細は、「Real Application Securityで使用される用語」を参照してください。

アプリケーション・ロールの更新

「ロール」タブから、アプリケーション・ロールに追加のアプリケーション・ロールを付与する、またはアプリケーション・ロールから1つ以上のアプリケーション・ロールを削除します。アプリケーション・ロールに1つ以上のアプリケーション・ロールが間接的に付与されている場合は、**間接ロール付与**セクションを確認します。

アプリケーション・ロールの情報を更新するには、次の手順を実行します。

1. **「ロール」**タブをクリックします。
2. **「ロール」**ページの**「ロール」**列で、更新するアプリケーション・ロールの名前を選択します。
3. **「ロールの管理」**ページで、更新を行います。

   アプリケーション・ロールにさらにアプリケーション・ロールを付与するには、別のアプリケーション・ロールを選択し、必要に応じて開始日と終了日を選択して、**「追加」**をクリックします。

   アプリケーション・ロールから1つ以上の付与されたアプリケーション・ロールを削除するには、**「ロール付与」**セクションで削除される各ロールを選択し、**「削除」**をクリックします。

   アプリケーション・ロールが1つ以上のアプリケーション・ロールに間接的に付与されている場合、これらのアプリケーション・ロールは、ルート・ロールの名前と付与パスとともに、**間接ロール付与**セクションにリストされます。
4. **「変更の適用」**をクリックして、変更を保存します。

関連項目:

「ロールの管理」ページ上のフィールドの詳細は、「アプリケーション・ロールの作成」を参照してください。

アプリケーション・ロールの削除

「ロール」タブから、このアプリケーションのデータ・セキュリティ・ポリシーで不要となったロールを削除します。

アプリケーション・ロールを削除するには:

1. **「ロール」**タブをクリックします。
2. **「ロール」**ページの**「ロール」**列で、削除するアプリケーション・ロールの名前をクリックします。
3. **「ロールの管理」**ページの**「アプリケーション・ロール」**セクションで、**「削除」**をクリックします。

アプリケーション権限クラスの管理

「権限」タブから、アプリケーション権限クラスを作成、更新および削除します。アプリケーション権限は、アプリケーション・レベルの操作の実行を制御する名前付き権限です。アプリケーション権限クラスを作成して、このアプリケーションのデータ・セキュリティ・ポリシーに追加します。

アプリケーション権限の管理には、次のトピックがあります。

- 「アプリケーション権限クラスの作成」
- 「アプリケーション権限クラスの更新」
- 「アプリケーション権限クラスの削除」

アプリケーション権限クラスの作成

「権限」タブから、このアプリケーションのデータ・セキュリティ・ポリシーに追加する必要がある各アプリケーション権限クラスを作成します。

アプリケーション権限クラスを作成するには、次の手順を実行します。

1. **「権限」**タブをクリックします。
2. **「権限」**ページで、**「作成」**をクリックします。
3. **権限クラス・セクション**の**「権限の管理」**ページで、次のフィールドに情報を入力します。赤いアスタリスクは必須フィールドを示しています。
   - **権限クラス・スキーマ** - (^)をクリックして、スキーマ名を選択します。
   - **権限クラス名** - 権限クラスの名前を入力します。名前は大文字と小文字が区別されます。
   - **説明** - 権限クラスの簡単な説明を入力します。

   アプリケーション権限セクションで、次のフィールドに情報を入力します。赤いアスタリスクは必須フィールドを示しています。
   - **権限名** - 権限の名前を入力します。
   - **説明** - この権限の簡単な説明を入力します。
   - **暗黙権限** - 暗黙権限になるようリストされている1つ以上のDML権限を選択します。アプリケーション権限がプリンシパルに付与されると、その暗黙権限も付与されます。

   「追加」をクリックして、このアプリケーション権限クラスにアプリケーション権限を追加します。

   この手順を繰り返して、このアプリケーション権限クラスに追加のアプリケーション権限を追加します。
4. **「変更の適用」**をクリックして、アプリケーション権限クラスを作成します。
5. このアプリケーションのデータ・セキュリティ・ポリシーに追加する必要がある各権限クラスに対して、手順1から4を繰り返します。

アプリケーション権限クラスの更新

「権限」タブから、新しいアプリケーション権限をアプリケーション権限クラスに追加する、またはアプリケーション権限クラスから1つ以上のアプリケーション権限を削除します。

アプリケーション権限クラスの情報を更新するには、次の手順を実行します。

1. **「権限」**タブをクリックします。
2. **「権限」**ページの**権限クラス**列で、更新する権限クラスの名前を選択します。
3. **「権限の管理」**ページで、更新を行います。

   この権限クラスに新規アプリケーション権限を追加するには、権限名、権限の簡単な説明を入力し、このアプリケーション権限の暗黙権限になるDML権限を選択して、**「追加」**をクリックします。

   権限クラスから1つ以上のアプリケーション権限を削除するには、**アプリケーション権限**セクションで削除される各権限を選択し、**「削除」**をクリックします。
4. **「変更の適用」**をクリックして、変更を保存します。

関連項目:

「権限の管理」ページ上のフィールドの詳細は、「アプリケーション権限クラスの作成」を参照してください。

アプリケーション権限クラスの削除

「権限」タブから、このアプリケーションのデータ・セキュリティ・ポリシーからアプリケーション権限クラスを削除します。

アプリケーション権限クラスを削除するには、次の手順を実行します。

1. **「権限」**タブをクリックします。
2. **「権限」**ページの**権限クラス**列で、削除する権限クラスの名前をクリックします。
3. **「権限の管理」**ページの**権限クラス**・セクションで、**「削除」**をクリックしてから、**「OK」**をクリックして、権限クラスを削除します。

アプリケーションのデータ行およびデータ列を保護するためのデータ・セキュリティ・ポリシーの管理

「ポリシー」タブから、このアプリケーションの表またはビューのデータ行およびデータ列を保護するためのデータ・セキュリティ・ポリシーを作成、更新または削除します。

データ・セキュリティ・ポリシーの管理には、次のトピックがあります。

- データ・セキュリティ・ポリシーの作成
- 「データ・セキュリティ・ポリシーの更新」
- 「データ・セキュリティ・ポリシーの削除」

データ・セキュリティ・ポリシーの作成

「ポリシー」タブから、このアプリケーションのための表のデータ行およびデータ列を保護するためのデータ・セキュリティ・ポリシーを作成します。

データ・セキュリティ・ポリシーを作成するには、次の手順を実行します。

1. **「ポリシー」**タブをクリックします。
2. **「ポリシー」**ページで、**「作成」**をクリックします。
3. **ポリシー情報**次のフィールドに情報を入力します。赤いアスタリスクは必須フィールドを示しています。
    - **ポリシー所有者** - (^)をクリックして、ポリシー所有者を選択します。
    - **ポリシー名** - データ・セキュリティ・ポリシーの名前を入力します。名前は大文字と小文字が区別されます。
    - **説明** - データ・セキュリティ・ポリシーの簡単な説明を入力します。
    - **権限クラス** - (^)をクリックして、権限クラスを選択します。または、**「新規」**をクリックして新規権限クラスを作成するか、**「変更」**をクリックして選択した権限クラスを更新します。
    - **保護されたオブジェクトのスキーマ** - (^)をクリックして、保護されるオブジェクトのスキーマの名前を選択し

ます。

注意:

認可されたスキーマのみが、値リストに表示されます。特定のスキーマが表示されない場合、ターゲット・オブジェクトに SELECT 権限を付与する必要があります。

- **保護されたオブジェクト** - (^)をクリックして、保護されるオブジェクトを選択します。

「ポリシー情報」セクションに情報を入力したら、**「次」**をクリックして続行します。

4. **列認可**。次の情報を入力して、列認可を作成します。
   - **列** - (^)をクリックして、保護される列の名前を選択します。
   - **権限** - (^)をクリックして、列に適用される権限を選択します。権限はすでに作成されている必要があります。表示される権限のリストは、手順3の**「ポリシー情報」**ページで選択した**権限クラス**に関連付けられた権限です。

   「追加」をクリックして、**作成済列認可**リストに列認可を追加します。この手順を繰り返して、追加の列認可を追加します。

   列認可セクションに情報を入力したら、**「次」**をクリックして続行します。

5. **データ・レルム認可**。次のフィールドに情報を入力します。
   - **名前** - データ・レルムの名前を入力します。名前は大文字と小文字が区別されます。
   - **説明** - このデータ・レルムに関する簡単な説明を入力します。
   - **レルム・タイプ** - データ・レルムのタイプを選択します。
     - **標準** - データ・レルムまたはACLに関連付けられたデータのセットを作成できます。データ・セットはSQL述語によって定義され、認可はACLで定義されます。ACLは、どの権限がデータ・セット上のどのプリンシパルに付与されるかを指定します。**「標準」**データ・レルムの場合、SQL述語およびACLを指定します。

       たとえば、HRスキーマにIDが60のDEPARTMENT表のデータ・レルムを作成する場合、DEPARTMENT_ID=60のSQL述語を指定します。定義されたACLは、SELECT権限をプリンシパル・ストアDATABASEのプリンシパルEMPLOYEEに付与し、VIEW_SALARY権限をプリンシパル・ストアDATABASEのプリンシパルEMPLOYEEに付与します。これにより、IDが60のこの部門の従業員のみが、自身の給与を表示できます。

       ACL

       次の情報を入力します。

       ACL名 - (^)をクリックして、ACL名を選択します。または、**「新規」**をクリックして、ACLを作成します。または、ACL名を選択し、**「変更」**をクリックしてACLを変更します。

     - **継承** - マスター・ディテールとも呼ばれ、マスター・オブジェクトを指すことにより、マスター・オブジェクトのポリシーを使用してディテール・オブジェクトを保護できます。そのため、ディテール・オブジェクト上に別の重複したポリシーを作成する必要がありません。**「継承」**データ・レルムの場合、**「親スキーマ」**および**「親オブジェクト」**を選択する必要があり、オプションで**「WHEN条件」**を入力します。**「WHEN**

条件」を使用して、親から子への関係を満たす子表レコードをさらにフィルタします。parent.column = child.columnを指定することによって、親から子への関係が定義されます。

たとえば、**HR**スキーマを使用していて、**DEPARTMENTS**親表と**EMPLOYEES**子表の間にマスター・ディテール・ポリシーを作成する場合、**「親スキーマ」**としてHRを指定し、**「親オブジェクト」**としてDEPARTMENTSを指定し、**「WHEN条件」**に1=1を入力します。次に、**レルム継承**の場合、**「親列」**としてDEPARTMENT_ID(NUMBER)を選択し、**「子タイプ」**としてCOLUMN NAMEを選択し、値としてDEPARTMENT_ID(NUMBER)を選択してから、**「追加」**をクリックします。**レルム継承**リストには次のエントリが表示されます: (HR.DEPARTMENTS) DEPARTMENT_ID= (HR.EMPLOYEES) DEPARTMENT_ID。これは、親=子ペアの結合条件を確立して、1:1の関係を形成します。

次のフィールドに情報を入力します。

親スキーマ - マスター・オブジェクトとして親スキーマの名前を選択します。

親オブジェクト - マスター・オブジェクトとして親オブジェクトの名前を選択します。

WHEN条件 - 述語を入力して、親のオブジェクト・ポリシーによって保護される子レコードをさらにフィルタするか、述語ビルダーを使用して、述語を作成します。

レルム継承

次のフィールドに情報を入力します。

親列 - 親列を選択します。

子タイプ - 子タイプを選択します。**「列名」**が選択されている場合、隣接するフィールドの(^)をクリックして、列名を選択します。**「値」**が選択されている場合、右側のフィールドに値を入力します。

「追加」をクリックして、このレルム継承をリストに追加します。

このプロセスを繰り返して、**レルム継承**リストにレルム継承をさらに追加します。

レルム継承 - すでに作成されているレルム継承関係をリストします。

作成済データ・レルム - 作成されたデータ・レルムをリストします。

- **パラメータ化** - department=&DEPT_IDなど、レルムのSQL述語でパラメータを使用できます。パラメータを表すには、パラメータ名の前に記号&を使用することに注意してください。パラメータ化されたデータ・レルムを使用すると、複数の"値-ACL"を1つのパラメータに指定できます。これにより、そのパラメータ化されたデータ・レルムを、複数の標準のデータ・レルムとしてインスタンス化できます。そのため、複数の標準のデータ・レルムを作成する必要がありません。**「パラメータ化」**データ・レルムの場合、SQL述語およびACLを指定する必要があります。

  たとえば、DEPARTMENT_ID=&DEPT_IDを指定した場合、パラメータ名DEPT_IDは様々な部門IDに関連付けられており、それぞれ権限を付与されています。これにより、各DEPT_IDの値に部門ID固有の多くのデータ・レルムを作成することなく、部門IDに基づいて権限付与を作成できます。

  ACLパラメータ

  次のフィールドに情報を入力します。

  ACL - (^)をクリックして、ACL名を選択します。または、**「新規」**をクリックしてACLを作成するか、**「変更」**をクリックして選択したACLを更新します。

  パラメータ名 - パラメータ名を入力するか、(^)をクリックして、リストからパラメータ名を選択します。パラメータ名は、述語から自動的に抽出され、このリストに表示されます。

パラメータ・タイプ - パラメータ・タイプをNUMBERまたはVARCHARから選択します。

パラメータ値 - パラメータ値を入力します。

「追加」をクリックして、このACLパラメータをリストに追加します。

このプロセスを繰り返して、**「ACLパラメータ」**リストにACLパラメータをさらに追加します。

ACLパラメータ - すでに定義されているACLパラメータをリストします。

- **SQL述語** - (**^**)をクリックして、SQL述語を選択します。または、(**>**)をクリックして**述語ビルダー・**フィールドを展開し、次のフィールドに情報を入力します。
  - **列名** - (**^**)をクリックして、列名を選択します。選択元の列のリストは、手順3の**「ポリシー情報」**ページで選択した**保護されたオブジェクト**に関連付けられた列です。
  - **演算子** - (**^**)をクリックして、演算子を選択します。
  - **値** - 値を入力します。値フィールドでは、入力された値に一致する選択肢の値が自動的に移入されるように、オートコンプリートが行われます。パラメータ化されたデータ・レルムの場合、&を入力すると、以前に定義されたパラメータが必要なパラメータの選択元から自動的に入力されます。
  - **AND/OR** - 必要に応じて、(**v**)をクリックし、**「AND」**または**「OR」**を選択して、SQL述語をさらに開発します。
  - **述語構成** - SQL述語を構成する際には、SQL述語はこのフィールドに構成され、述語が有効で完全であるかどうかについてのフィードバックを提供して、この操作を支援します。

  「プレビュー」をクリックして、SQL述語をテストします。表示される問合せ結果を調べます。必要な結果を得られた場合、**「適用」**をクリックして、**SQL述語**フィールドに述語を追加します。

  「次」をクリックして、**データ・レルム認可**リストにデータ・レルムを追加します。

  このプロセスを繰り返して、追加のデータ・レルムを作成し、それを**作成済データ・レルム・**リストに追加します。

  作成済データ・レルム・リストで、(**^**)または(**v**)をクリックして、各データ・レルムの評価順序を変更します。リストの最初のデータ・レルムが最初に評価され、2番目のデータ・レルムが次に評価されます。

  データ・レルム付与リストから1つ以上のデータ・レルムを削除するには、データ・レルムを選択し、**「削除」**をクリックします。

ACL

ACLを作成するには、**アクセス制御リスト(ACL)**セクションで、次のフィールドに情報を入力します。

- **ACL名** - ACLの名前を入力します。名前は大文字と小文字が区別されます。
- **説明** - ACLの簡単な説明を入力します。
- **ACL継承** - (**>**)をクリックして、フィールドを展開します。次の情報を入力します。
  - **親** - (**^**)をクリックして、親ACLを選択します。
  - **継承モード** - **「拡張」**または**制約**を選択します。

    「拡張」は、ACL継承を拡張する(または順序付けされた評価を使用する)ことを意味します。このオプションにより、ACEは継承ツリーの下から上に、子から親に評価されることが決定されます。

    制約は、制約ACL継承(AND)では、ACLの確認でtrueに評価されるように、子と親の両方のACLでアプリケーション権限を付与する必要があることを意味します。

「権限の付与」に、次の情報を入力します。

- **プリンシパル** - (**<-**)をクリックして、プリンシパルを検索するための検索基準を指定し、プリンシパルを選択します。検索基準で、**「プリンシパル・タイプ」**を「ロール」または「ユーザー」に、**プリンシパル・ストア**を「データ ベース」または「外部」に指定し、**「検索」**をクリックします。戻りリストからプリンシパルを選択します。ここで記述されている**データ ベース**という語は、Real Application Securityアプリケーションのユーザーおよびロールではプリンシパル・ストアを意味することに注意してください。
- **次を除くすべて** - 指定した権限を除くすべての権限をプリンシパルに付与する場合はこのオプションを選択し、指定した権限のみを付与または拒否する場合はこのオプションを選択解除したままにします。
- **権限** - (**v**)をクリックして、アプリケーション権限を選択します。
- **権限タイプ** - このプリンシパルにこのアプリケーション権限を付与する場合は**「権限付与」**を選択し、このプリンシパルからこのアプリケーション権限を拒否する場合は**「拒否」**を選択します。
- **開始日** - カレンダ・アイコンをクリックして、この権限付与の有効な開始日を選択するか、フィールドを空白のままにします。開始日を指定しないと、この権限付与は常に有効であることを意味します。
- **終了日** - カレンダ・アイコンをクリックして、この権限付与の有効な終了日を選択するか、フィールドを空白のままにします。終了日を指定しないと、この権限付与は常に有効であることを意味します。開始日を指定する場合、終了日も指定する必要があります。

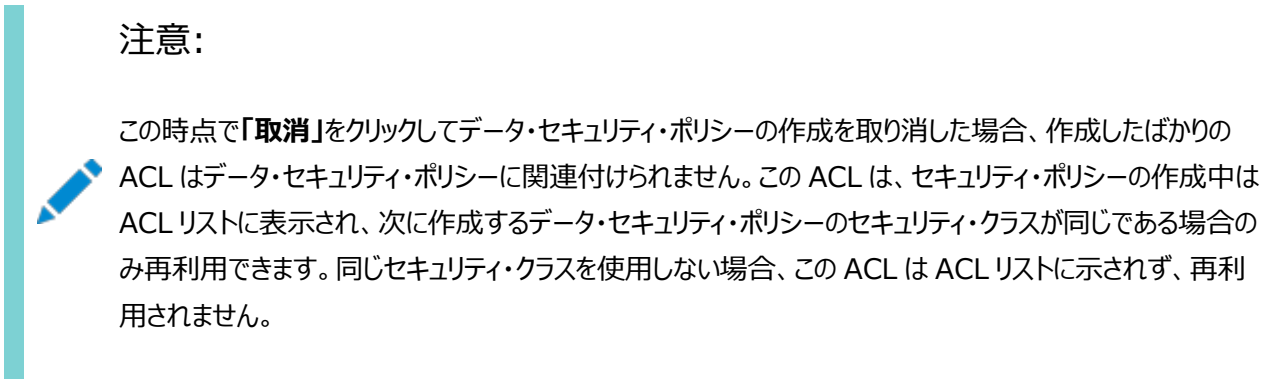
「追加」をクリックして、この権限付与をACLに追加します。

このプロセスを繰り返して、別の権限付与をACLに追加します。

「権限の付与」リストで、(^)または(**v**)をクリックして、各権限付与の評価順序を変更します。リストの最初の権限付与が最初に評価され、2番目の権限付与が次に評価されます。

ACLから1つ以上の権限付与を削除するには、権限付与を選択し、**「削除」**をクリックします。

「変更の適用」をクリックして、ACLを作成します。



「追加」をクリックして、**作成済データ・レルム**・リストにこのデータ・レルムを追加します。

データ・レルム認可セクションに情報を入力したら、**「次」**をクリックして続行します。

6. **ポリシーの適用「ポリシー名」**および**「オブジェクト名」**の名前は、データ・セキュリティ・ポリシーに対して表示されます。次の情報を入力します。
   - **ポリシーの適用**フィールドで、このポリシーのポリシー・ステータスを、「適用」、「削除」、「有効化」また

は「無効化」のいずれかに指定します。「適用」を選択した場合、**「適用オプション」**を指定します。

- (**>**)をクリックして、**「適用オプション」**を展開します。次のフィールドに情報を入力します。
  - **行当たりのACL** - ポリシーが非表示列を作成するかどうか。「True」または「False」。デフォルトは「False」です。値「True」は、非表示列SYS_ACLODを作成します。
  - **所有者の省略** - 行の所有者がデータ・セキュリティ・ポリシーを省略できるかどうか。「True」または「False」。デフォルトは「False」です。
  - **文タイプ** - このポリシーのすべての文タイプ(「選択」、「挿入」、「更新」、「削除」)を施行するかどうか。必要に応じて、文タイプを選択解除します。デフォルトでは、すべての文タイプが選択されています。

「変更の適用」をクリックして、データ・セキュリティ・ポリシーを作成します。

関連項目:

権限クラスについては、**「新規」**をクリックすると、新しい権限クラスが作成されます。権限クラスの作成の詳細は、「アプリケーション権限クラスの作成」を参照してください。

データ・セキュリティ・ポリシーの更新

「ポリシー」タブから、表またはビューなど、他のオブジェクトと同じポリシーを適用してデータ・セキュリティ・ポリシーを更新し、これらのデータ行および列を保護します。

データ・セキュリティ・ポリシーの情報を更新するには、次の手順を実行します。

1. **「ポリシー」**タブをクリックします。
2. **「ポリシー」**ページの**「ポリシー」**列で、更新するポリシー名を選択します。
3. **「ポリシー定義」**ページで、更新を行います。

   行うことができる更新は、他のオブジェクト(表やビューなど)への同じポリシーの適用であることに注意してください。これを行うには、**「ポリシー定義」**ページの**保護されたオブジェクト**・フィールドの隣にある**「追加」**をクリックします。保護するオブジェクトを選択し、**「変更の適用」**をクリックすると、**ポリシーの適用**ページが表示され、ここでは、**「変更の適用」**をクリックして、新規オブジェクトにポリシーを適用できます。適用操作中に検証が実行され、新規オブジェクトに適用可能な列認可およびレルム認可を検証します。列認可がこの新規オブジェクトで有効ではない場合、RASADMは適用操作を完了できません。レルム述語が有効ではない場合、オブジェクトの名前の隣に警告が表示されますが、RASADMはポリシーを適用できます。
4. **「変更の適用」**をクリックして、変更を保存します。

関連項目:

「ポリシー定義」ページ上のフィールドの詳細は、「データ・セキュリティ・ポリシーの作成」を参照してください。

データ・セキュリティ・ポリシーの削除

「ポリシー」タブから、このアプリケーションで不要となった表またはビューのデータ・セキュリティ・ポリシーを削除します。

データ・セキュリティ・ポリシーを削除するには、次の手順を実行します。

1. **「ポリシー」**タブをクリックします。
2. **「ポリシー」**ページの**「ポリシー」**列で、削除するポリシー名をクリックします。
3. **「ポリシー定義」**ページの**「ポリシー」**セクションで、**「削除」**をクリックしてから、**「OK」**をクリックして、ポリシーを削除します。

ネームスペースの管理

「ポリシー」タブから、アプリケーションで異なるセッション間で使用できるセッション・ネームスペースを作成します。セッションのネームスペースのテンプレートを作成して、ネームスペースおよびそのプロパティを定義し、アプリケーション・セッションでネームスペースを初期化します。

ネームスペースの管理には、次のトピックがあります。

- ネームスペースの作成
- ネームスペースの更新
- ネームスペースの削除

ネームスペースの作成

「ネームスペース」タブから、このアプリケーションのデータ・セキュリティ・ポリシーに追加する必要があるセッションのネームスペースを作成します。

ネームスペースを作成するには、次の手順を実行します。

1. **「ネームスペース」**タブをクリックします。
2. **「ネームスペース」**ページで、**「作成」**をクリックします。
3. **アプリケーション・ネームスペース**・セクションの**ネームスペースの管理**ページで、次のフィールドに情報を入力します。赤いアスタリスクは必須フィールドを示しています。
    - **ネームスペース名** - ネームスペースの名前を入力します。名前は大文字と小文字が区別されます。
    - **説明** - ネームスペースの簡単な説明を入力します。
    - **ACL** - (^)をクリックして、このネームスペースのACLを選択します。

      または、**「新規」**をクリックしてACLを作成するか、**「変更」**をクリックして選択したACLを更新し、**アクセス制御リスト(ACL)**ページで、次の情報を入力または変更します。
        - **ACL名** - ACLの名前を入力します。この名前は変更できません。
        - **説明** - ACLの簡単な説明を入力します。

      ACL継承で、(**>**)をクリックします。次の情報を入力します。
        - **親** - (^)をクリックして、親ACLを選択します。
        - **継承モード** - **「拡張」**または**制約**を選択します。

          「拡張」は、ACL継承を拡張する(または順序付けされた評価を使用する)ことを意味します。このオ

プションにより、ACEは継承ツリーの下から上に、子から親に評価されることが決定されます。

制約は、制約ACL継承(AND)では、ACLの確認でtrueに評価されるように、子と親の両方のACLでアプリケーション権限を付与する必要があることを意味します。

「権限の付与」に、次の情報を入力します。

- **プリンシパル** - (**<-**)をクリックして、プリンシパルを選択します。**「プリンシパル・タイプ」**の「ロール」または「**ユーザー**」、**プリンシパル・ストア**の「**データ ベース**」または「**外部**」を選択し、オプションで**プリンシパル・フィルタ**・フィールドにフィルタ情報を入力し、**「検索」**をクリックします。表示される検索結果から、**「選択」**をクリックして、目的の**プリンシパル**名を選択します。

  「**データ ベース**」は、データベース・ストアが使用されることを意味します。ここで記述されている**データ ベース**という語は、Real Application Securityアプリケーションのユーザーおよびロールではプリンシパル・ストアを意味することに注意してください。

  「外部」で、オプションで**プリンシパル・フィルタ**・フィールドにフィルタ情報を入力し、**再フェッチ**・オプションを選択し、**プリンシパル・ストア・パスワード**・フィールドにパスワードを入力し、**「検索」**をクリックします。表示される結果から、**「選択」**をクリックして、目的の**プリンシパル**名を選択します。

- **次を除くすべて** - 指定した権限を除くすべての権限をプリンシパルに付与する場合はこのオプションを選択し、指定した権限のみを付与または拒否する場合はこのオプションを選択解除したままにします。

- **権限** - (**v**)をクリックして、アプリケーション権限を選択します。

- **権限タイプ** - このプリンシパルにこのアプリケーション権限を付与する場合は**「権限付与」**を選択し、このプリンシパルからこのアプリケーション権限を拒否する場合は**「拒否」**を選択します。

- **開始日** - カレンダ・アイコンをクリックして、この権限付与の有効な開始日を選択するか、フィールドを空白のままにします。開始日を指定しないと、この権限付与は常に有効であることを意味します。

- **終了日** - カレンダ・アイコンをクリックして、この権限付与の有効な終了日を選択するか、フィールドを空白のままにします。終了日を指定しないと、この権限付与は常に有効であることを意味します。開始日を指定する場合、終了日も指定する必要があります。

「追加」をクリックして、権限付与をACLに追加します。

このプロセスを繰り返して、ACLに追加する別の権限付与を作成します。

「権限の付与」リストで、(**^**)または(**v**)をクリックして、各権限付与の評価順序を変更します。リストの最初の権限付与が最初に評価され、2番目の権限付与が次に評価されます。

ACLから1つ以上の権限付与を削除するには、権限付与を選択し、**「削除」**をクリックします。

- **イベント・ハンドラ** - イベント・ハンドラが必要かどうかを示します。「**いいえ**」または「**はい**」。「はい」を示した場合、(^)をクリックして、**「ハンドラ・スキーマ」**、**「ハンドラ・パッケージ」**および**「ハンドラ関数」**を選択します。

「アプリケーション属性」セクションで、ネームスペース属性とそのデフォルト値を追加できます。次のフィールドに情報を入力します。

- **属性**および**デフォルト値** - **「追加」**をクリックして、ネームスペース属性とそのデフォルト値を追加します。**「属性」**列に属性名を入力し、**「デフォルト値」**列にその属性のデフォルト値を入力します。**属性イベント**の「**なし**」、**初回読取り**、「**変更**」または**初回読取りおよび変更**を選択します。次に、**「追加」**をクリックして、このアプリケーション属性を追加します。

「追加」をクリックして、別のネームスペース属性名とそのデフォルト値を追加します。

4. **「変更の適用」**をクリックして、ネームスペースを作成します。
5. このアプリケーションのデータ・セキュリティ・ポリシーに追加する必要がある各ネームスペースに対して、手順1から4を繰り返します。

関連項目:

「イベント・ハンドラ」については、イベント・ハンドラが必要であることに「はい」と答えた場合、ネームスペース・ハンドラおよびPL/SQLを使用したネームスペース・ハンドラの作成方法の詳細は、『Oracle Database Real Application Security管理者および開発者ガイド』のネームスペース・テンプレートのコンポーネントに関する項を参照してください。

ネームスペースの更新

「ネームスペース」タブから、以前に存在しない場合はイベント・ハンドラを追加するか、またはアプリケーション属性を追加または削除するか、いずれかによって既存のネームスペースを更新します。

ネームスペースの情報を更新するには、次の手順を実行します。

1. **「ネームスペース」**タブをクリックします。
2. **「ネームスペース」**ページの**アプリケーション・ネームスペース**列で、更新するネームスペース名をクリックします。
3. **ネームスペースの管理**ページで、更新を行います。

   以前にイベント・ハンドラが不要であると示し、現在イベント・ハンドラが必要になった場合、「はい」を選択し、(^)をクリックして、**「ハンドラ・スキーマ」**、**「ハンドラ・パッケージ」**および**「ハンドラ関数」**を選択します。

   「追加」をクリックして、別のアプリケーション属性を追加します。属性名とそのデフォルト値を入力します。このプロセスを繰り返して、追加の各属性とそのデフォルト値を追加します。

   1つ以上のアプリケーション属性を削除するには、**「アプリケーション属性」**セクションで削除される各属性を選択し、**「削除」**をクリックします。
4. **「変更の適用」**をクリックして、変更を保存します。

関連項目:

ネームスペースの管理ページ上のフィールドの詳細は、「ネームスペースの作成」を参照してください。

ネームスペースの削除

「ネームスペース」タブから、このアプリケーションのデータ・セキュリティ・ポリシーで不要となったセッション・ネームスペースを削除します。

ネームスペースを削除するには、次の手順を実行します。

1. **「ネームスペース」**タブをクリックします。
2. **「ネームスペース」**ページの**アプリケーション・ネームスペース**列で、削除するネームスペース名をクリックします。

3. **ネームスペースの管理**ページの**アプリケーション・ネームスペース**・セクションで、**「削除」**をクリックしてから、**「OK」**をクリックして、ネームスペースを削除します。

設定の管理

「設定」タブから、Real Application Security管理をディレクトリ・サーバーとともに使用するためのパラメータ設定を更新します。

LDAPユーザーまたはLDAPグループのいずれかのパラメータ設定の管理には、次のトピックがあります。

- 「LDAPユーザーのパラメータ設定の更新」
- 「LDAPグループのパラメータ設定の更新」

LDAPユーザーのパラメータ設定の更新

「設定」タブから、LDAPユーザーのパラメータ設定を更新します。

これらのパラメータ設定の情報を更新するには、次の手順を実行します。

1. **「設定」**タブをクリックします。
2. **「設定」**ページの**「名前」**列で、すでに入力されているグループ名を選択します。たとえば、LDAP_USERを選択します。
3. **「設定の管理」**ページで、更新を行います。

> 注意:
>
> **「パラメータ」**セクションで誤った設定を行うと、ディレクトリ・サーバーへの接続に悪影響を及ぼす可能性があるため、これらの設定は慎重に変更してください。

LDAPグループの名前が**「設定」**セクションに表示されます。**「設定」**および**「パラメータ」**セクションで、次のフィールドを更新できます。

- **説明** - ユーザー名の説明。
- **ホスト** - ディレクトリ・サーバーが実行されているホストの名前。
- **ポート** - ディレクトリ・サーバーのポート番号。
- **ユーザー** - ディレクトリ情報ツリー(DIT)でのユーザー・エンティティの場所
- **ベース** - ディレクトリ・サーバーへのユーザー・エントリの格納に使用されるネーミング・コンテキスト。
- **名前属性** - 名前属性と値のペア。
- **ID属性** - ID属性と値のペア。**「ID属性」**は、「ベース」によって指定される、LDAPエントリの属性である必要があります。ユーザーをグローバルに識別します。通常、GUIDが使用されます。Oracle Internet Directory (OID)の場合は`orclguid`、Microsoft Active Directory (AD)の場合は`objectGUID`にする必要があります。
- **説明属性** - 説明属性と値のペア。
- **SSLウォレット・ロケーション** - ファイル・システム上のウォレットへのパス(`file:/home/mywallet`など)。

file:という語を接頭辞として使用する必要があります。

- **SSL認証モード** - モードの値: 認証が不要な場合は1、一方向認証が必要な場合は2、双方向認証が必要な場合は3。

4. **「変更の適用」**をクリックして、変更を保存します。

LDAPグループのパラメータ設定の更新

「設定」タブから、LDAPグループのパラメータ設定を更新します。

これらのパラメータ設定の情報を更新するには、次の手順を実行します。

1. **「設定」**タブをクリックします。
2. **「設定」**ページの**「名前」**列で、すでに入力されているグループ名を選択します。たとえば、LDAP_GROUPを選択します。
3. **「設定の管理」**ページで、更新を行います。

> 注意:
>
> **「パラメータ」**セクションで誤った設定を行うと、ディレクトリ・サーバーへの接続に悪影響を及ぼす可能性があるため、これらの設定は慎重に変更してください。

LDAPグループの名前が**「設定」**セクションに表示されます。**「設定」**および**「パラメータ」**セクションで、次のフィールドを更新できます。

- **説明** - グループ名の説明。
- **ホスト** - ディレクトリ・サーバーが実行されているホストの名前。
- **ポート** - ディレクトリ・サーバーのポート番号。
- **ユーザー** - ディレクトリ情報ツリー(DIT)でのグループ・エンティティの場所。
- **ベース** - ディレクトリ・サーバーへのグループ・エントリの格納に使用されるネーミング・コンテキスト。
- **名前属性** - 名前属性と値のペア。
- **ID属性** - ID属性と値のペア。**「ID属性」**は、「ベース」によって指定される、LDAPエントリの属性である必要があります。グループをグローバルに識別します。通常、GUIDが使用されます。Oracle Internet Directory (OID)の場合はorclguid、Microsoft Active Directory (AD)の場合はobjectGUIDにする必要があります。
- **説明属性** - 説明属性と値のペア。
- **SSLウォレット・ロケーション** - ファイル・システム上のウォレットへのパス(file:/home/mywalletなど)。file:という語を接頭辞として使用する必要があります。
- **SSL認証モード** - モードの値: 認証が不要な場合は1、一方向認証が必要な場合は2、双方向認証が必要な場合は3。

4. **「変更の適用」**をクリックして、変更を保存します。

ドキュメントのアクセシビリティについて

Oracleのアクセシビリティについての詳細情報は、Oracle Accessibility ProgramのWebサイト(http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc)を参照してください。

Oracleサポートへのアクセス

サポートを購入したオラクル社のお客様は、My Oracle Supportを介して電子的なサポートにアクセスできます。詳細情報は(http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info)か、聴覚に障害のあるお客様は(http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs)を参照してください。