CA SiteMinder®

ディレクトリ設定ガイド

r12.0 SP3

technologies

CA 製品リファレンス

このマニュアルでは、以下の CA 製品に言及しています。

- CA SiteMinder®
- CA SiteMinder® Federation セキュリティ サービス

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト（http://www.ca.com/jp/support/）をご覧ください。

目次

第 1 章: 本書の内容

このセクションには、以下のトピックが含まれます。

ディレクトリ構成の概要

この「ディレクトリ設定ガイド」では、以下のディレクトリ サーバおよびリレーショナル データベースのユーザ ストアまたはポリシー ストアとしての設定について説明します。

- Critical Path inJoin Directory Server v4.2
- IBM DB2 データベース
- IBM Directory Server
- MySQL サーバ
- Novell eDirectory
- Oracle Internet Directory Server
- OpenLDAP サーバ
- Red Hat Directory Server 7.1
- Siemens DirX 6.0 D00 Directory Server
- Siemens DirX EE 2.0 Directory Server

Microsoft ADAM、Sun Java System など、その他のサポートされているディレクトリ サーバおよびリレーショナル データベースの詳細については、以下のガイドを参照してください。

- ポリシー サーバ設定ガイド
- ポリシー サーバ インストール ガイド
- アップグレード ガイド

第 2 章: Critical Path inJoin Directory Server

このセクションには、以下のトピックが含まれています。

SiteMinder スキーマ ファイルのダウンロード

SiteMinder スキーマを設定するのに必要な 1 つ以上のスキーマ ファイルが、ポリシー サーバ インストールに含まれていません。これらのファイルは CA SiteMinder Tier 2 ディレクトリ製品コンポーネント ダウンロードにあります。

Tier 2 ディレクトリ製品コンポーネントをダウンロードする方法

1. テクニカル サポート サイトにログインします。
2. [Support]の下の[Download Center]をクリックします。

   [Download Center]画面が表示されます。
3. [Select a Product]フィールドに「SiteMinder」と入力します。
4. [Select a Release]リストからリリースを選択します。
5. [Select a Gen Level]リストからサービス パックを選択します。
6. [Go]をクリックします。

   [Product Downloads]画面が表示されます。Tier 2 ディレクトリ コンポーネント ダウンロードはリストの下のほうにあります。
7. zip ファイルをローカルに保存し、ポリシー サーバ ホスト システムにファイルを抽出します。

ポリシー サーバからポリシー ストアへの参照の設定

ポリシー サーバからポリシー ストアへの参照を設定し、ポリシー サーバがポリシー ストアにアクセスできるようにします。

ポリシー サーバからポリシー ストアへの参照を設定する方法

1. ポリシー サーバ管理コンソールを開きます。

   重要: Windows Server 2008 上でこのグラフィカル ユーザ インターフェースにアクセスする場合は、管理者としてシステムにログインしている場合でも、管理者権限でショートカットを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

2. [データ]タブをクリックします。

   データベース設定が表示されます。

3. [データベース]リストから[ポリシー ストア]を選択します。

4. [ストレージ]リストから[LDAP]を選択します。

5. [LDAP ポリシー ストア]グループ ボックスで、以下を設定します。

   - LDAP IP アドレス
   - 管理者ユーザ名
   - パスワード
   - パスワードの確認
   - DN

   注: フィールド、コントロール、およびそれぞれの要件については、[ヘルプ]をクリックしてください。

6. [適用]をクリックします。

   ポリシー ストアの設定が保存されます。

7. [LDAP 接続のテスト]をクリックします。

   SiteMinder は、ポリシー サーバがポリシー ストアにアクセスできることを示す確認を返します。

ポリシー ストアとしての inJoin Directory Server の設定

Critical Path の iCon GUI を使用して、Critical Path inJoin Directory Server（IDS）をポリシー ストアとして設定することができます。

Critical Path inJoin Directory Server（IDS）をポリシー ストアとして設定する方法

1. DSA を起動します。
2. ポリシー サーバがインストールされているマシン上の *policy_server_home*¥bin に移動します。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。
3. 以下のコマンドを実行します。

   ```
   ldapmodify -hhost -pport -dAdminDN -wAdminPW -c
   -fpath¥criticalpath¥IDS_Add_Schema_R12sp3.ldif
   ```

   -h*host*

   LDAP サーバの IP アドレスを指定します。

   -p*port*

   LDAP サーバのポート番号を指定します。

   -d*AdminDN*

   LDAP ディレクトリ サーバ上に新規の LDAP スキーマを作成する権限を持つ LDAP ユーザの名前を指定します。

   例: cn=manager

   -w*AdminPW*

   LDAP ディレクトリ サーバ上に新規の LDAP スキーマを作成する権限を持つ LDAP ユーザのパスワードを指定します。

   -c

   連続モードを指定します（エラーで停止しません）。

   -f*path*

   Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。
4. スキーマを再ロードするか、またはスキーマが更新されたことを確認します。

5. 以下のコマンドを実行します。

   ```
   ldapmodify -hhost -pport -dAdminDN -wAdminPW -c
   -fpath¥xps¥criticalpath¥CriticalPath.ldif
   ```

   -fpath

   Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。

6. スキーマを再ロードするか、またはスキーマが更新されたことを確認します。
7. [DSA]-[Comms]-[LDAP]に移動し、paging mode オプションを「always」に変更して、DSA を再起動します。

   r12.0 SP3 に対するポリシー ストア スキーマが作成されます。

8. Critical Path の iCon DIT 管理者インターフェースを使用して、以下のルートノードを手動で作成します。
   - ou=Netegrity
   - ou=SiteMinder
   - ou=PolicySvr4
   - ou=XPS
9. smreg ユーティリティを *policy_server_home*¥bin にコピーします。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

10. 以下のコマンドを実行します。

    ```
    smreg -su password
    ```

    password

    デフォルトの SiteMinder 管理者のパスワードを指定します。

    制限:

    - パスワードは 6 文字以上、24 文字以下である必要があります。
    - パスワードには、アンパサンド(&)またはアスタリスク(*)を含むことはできません。
    - パスワードにスペースが含まれている場合は、引用符でパスフレーズを囲みます。

    注: パスワードは、Oracle ポリシー ストアに保管する場合を除き、大文字小文字が区別されません。

11. *policy_server_home*¥bin から smreg ユーティリティを削除します。smreg を削除すると、既存のパスワードを把握していない限り、パスワードを変更することはできなくなります。

    デフォルトの SiteMinder 管理者アカウントのパスワードが設定されます。

12. 以下のコマンドを実行します。

    ```
    smobjimport -ipolicy_server_home/db/smdif/smpolicy.smdif
    -dsiteminder_super_user_name -wsiteminder_super_user_password -v
    ```

    -i

    インポート ファイルのパスと名前を指定します。

    -v

    トレースをオンにして、エラー メッセージ、警告メッセージ、およびコメント メッセージを出力します。

    ベース ポリシー ストア データを、ファイル smpolicy.smdif からインポートします。

13. 以下のコマンドを実行します。

    ```
    smobjimport -ipolicy_server_home¥db¥smdif¥ampolicy.smdif
    -dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
    ```

    -i

    インポート ファイルのパスと名前を指定します。

    -d*siteminder_super_user_name*

    SiteMinder スーパーユーザ アカウントの名前を指定します。

    -w*siteminder_super_user_password*

    SiteMinder スーパーユーザ アカウントのパスワードを指定します。

    -f

    重複するオブジェクトをオーバーライドします。

    -v

    追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

    デフォルト値: stdout

-l

ログ ファイルを作成します。

-c

smdif 入力ファイルに暗号化されていないデータが含まれていることを示します。

smobjimport によって、ポリシー ストア オブジェクトがインポートされます。これらのオブジェクトは、適切な場所に自動的にインポートされます。

注: ampolicy.smdif をインポートすると、Federation セキュリティ サービス、Web サービス変数、および eTelligent ルール機能が使用可能になります。eTelligent ルール機能は、SiteMinder から別個にライセンスが提供されます。この eTelligent ルール機能を使用する予定がある場合は、ライセンスの詳細について、CA アカウント担当者に問い合わせてください。

Critical Path inJoin Directory Server（IDS）がポリシー ストアとして設定されます。

注: これで、ポリシー ストア データ定義をインポートできます。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*¥xps¥dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。

3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   必要なポリシー ストア データ定義がすべてインポートされました。

管理 UI 登録の準備

管理 UI に初めてログインする場合は、デフォルトの SiteMinder スーパーユーザ アカウント(siteminder)を使用します。初めてログインするときは、ポリシー サーバに 管理 UI を登録する必要があります。これで、両方のコンポーネントの間に信頼関係が作成されます。

XPSRegClient ユーティリティを使用してスーパーユーザ アカウントの名前とパスワードを指定して、登録の準備をします。ポリシー サーバは、これらの認証情報を使用して、登録要求が有効であること、および信頼関係を確立できることを検証します。

以下の点について考慮してください。

- 認証情報を指定してから最初の 管理 UI ログインまでの時間は、24 時間に制限されています。24 時間以内に 管理 UI をインストールする予定がない場合は、管理 UI をインストールする前に以下を実行します。
- （UNIX）XPSRegClient を使用する前に、SiteMinder 環境変数が設定されていることを確認してください。環境変数が設定されていない場合は、手動で設定します。

管理 UI 登録を準備する方法

1. ポリシー サーバ ホスト システムにログインします。
2. 以下のコマンドを実行します。

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

デフォルトの SiteMinder スーパーユーザ アカウント（siteminder）のパスワードを指定します。

注: パスフレーズを指定しないと、XPSRegClient により、パスフレーズの入力とその確認を求めるプロンプトが表示されます。

-adminui–setup

管理 UI が初めてポリシー サーバに登録されていることを指定します。

-t *timeout*

（任意）管理 UI をインストールしてから、ログインしてポリシー サーバとの信頼関係を作成するまでの割り当て時間を指定します。タイムアウト値を超過すると、ポリシー サーバは登録リクエストを拒否します。

測定単位: 分

デフォルト: 240（4 時間）

最小制限: 1

最大制限: 1440（24 時間）

-r *retries*

(任意) 管理 UI の登録時に許容される試行の失敗回数を指定します。試行に失敗する原因としては、初めて 管理 UI にログインするときに間違った SiteMinder 管理者クレデンシャルをサブミットしたことが考えられます。

デフォルト: 1

最大制限: 5

-c *comment*

(任意) 指定されたコメントを情報目的で登録ログ ファイルに挿入します。

注: コメントは引用符で囲んでください。

-cp

(任意) 登録ログ ファイルに複数行のコメントが含まれることを指定します。ユーティリティにより複数行のコメントが求められ、指定されたコメントが情報目的で登録ログ ファイルに挿入されます。

注: コメントは引用符で囲んでください。

-l *log path*

(任意) 登録ログ ファイルをエクスポートする場所を指定します。

デフォルト: *siteminder_home*¥log

siteminder_home

ポリシー サーバのインストール パスを指定します。

-e *error_path*

(任意) 例外を指定されたパスに送信します。

デフォルト: stderr

-vT

(任意) 詳細レベルを TRACE に設定します。

-vI

（任意）詳細レベルを INFO に設定します。

-vW

（任意）詳細レベルを WARNING に設定します。

-vE

（任意）詳細レベルを ERROR に設定します。

-vF

（任意）詳細レベルを FATAL に設定します。

3. Enter キーを押します。

   XPSRegClient は、ポリシー サーバに管理者クレデンシャルを提供します。ポリシー サーバは、管理 UI への最初のログイン時に、登録リクエストを確認するためにこれらのクレデンシャルを使用します。

IDS での LDAP トレースの有効化

IDS で LDAP トレースを有効にする方法

1. DSA を停止します。
2. テキスト エディタに、DSA ディレクトリ（c:¥ids¥icon¥dsa1）内にある実行ファイルを開きます。
3. odsldap3 プロセスのスイッチを追加します。

   例：

   1r odsldap3 -ldap:1708 -ldaps:0 -http:0 -https:0 -diag:5

   -diag:n 0 はオフです。値が大きいほど、提供される出力は多くなります。

   1=FATAL, 2=SEVERE, 3=ERROR, 4=WARNING,5=INFO, 6=ENTRY/EXIT
4. iCon を使用して、DSA を開始します。

   ログ ファイルは iCon 内にあります。
5. ［DSA］を選択します。
6. トップ メニューの comms オプションを選択します。
7. LDAP プロセスを選択します。
8. odsldap3.out.000 というファイルをクリックします。

ユーザ ディレクトリの設定例 - Critical Path InJoin Directory Server

以下に、ユーザ ディレクトリの設定例を示します。

ディレクトリのセットアップ

- ネームスペース: LDAP
- サーバ: 123.456.7.8
- ルート: o=companyname、c=us
- DN 検索の先頭文字列: (cn=)
- DN 検索の終端文字列:)

認証情報と接続

- 管理者ユーザ名 : cn=manager
- 管理者パスワード: ********

ユーザ属性

- ユニバーサル ID (R): cn
- 無効フラグ (RW): description
- パスワードの属性 (RW): userpassword
- パスワード データ (RW): audio
- チャレンジ/レスポンス (RW): jpegPhoto

注: DMS のユーザ属性名に大文字小文字の区別があるかどうかは、属性単位で異なります。

ポリシー サーバの設定例 - Critical Path InJoin Directory Server

以下に、ポリシー サーバの設定例を示します。

LDAP

- LDAP IP アドレス: 12.3.4.5
- 管理者ユーザ名 : cn=manager
- 管理者パスワード: ********
- パスワードの確認入力: ********
- ルート DN : o=companyname、c=us
- ポリシー ストアの使用 : (チェック ボックスをオン)
- Netscape 証明書データベース ファイル : pathname

6.x ポリシー ストアをアップグレードする方法

r12.0 SP3 ポリシー ストアに、新規のディレクトリ サーバ インスタンスは必要ありません。既存のポリシー ストアを r12.0 SP3 にアップグレードできます。

ポリシー ストアをアップグレードするには、以下の手順を実行します。

1. ポリシー ストア スキーマを拡張します。

   注:既存の r6.x ポリシー ストア スキーマは、変更されていません。r12.0 SP3 の移行では、ポリシー ストア スキーマをアップグレードして、r12.0 SP3 によって必要とされるオブジェクトのポリシー ストアを拡張する必要があります。

2. ベース ポリシー ストア オブジェクトをインポートします。
3. ポリシー ストア データ定義をインポートします。

注: サポート マトリックスにリストされているディレクトリ サーバまたはデータベースで、本書に記載されていないものをアップグレードする場合は、「SiteMinder アップグレード ガイド」を参照してください。

inJoin ポリシー ストア スキーマの拡張

Critical Path の iCon GUI を使用して、r12.0 SP3 によって導入されたオブジェクトを含めるように既存の 6.x ポリシー ストア スキーマを拡張することができます。既存の 6.x ポリシー ストア スキーマに加える変更はありません。

既存の inJoin ポリシー ストア スキーマを拡張する方法

1. DSA を起動します。
2. *policy_server_home*/bin に移動します。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。
3. 以下のコマンドを実行します。

   ```
   ldapmodify -hhost -pport -dAdminDN -wAdminPW -c
   -fpath¥xps¥CriticalPath.ldif
   ```

   -h*host*

   LDAP サーバの IP アドレスを指定します。

   -p*port*

   LDAP サーバのポート番号を指定します。

   -d*AdminDN*

   LDAP ディレクトリ サーバ上に新規の LDAP スキーマを作成する権限を持つ LDAP ユーザの名前を指定します。

   例: cn=manager

   -w*AdminPW*

   LDAP ディレクトリ サーバ上に新規の LDAP スキーマを作成する権限を持つ LDAP ユーザのパスワードを指定します。

   -c

   連続モードを指定します(エラーで停止しません)。

   -f*path*

   r12.0 SP3 で提供される XPS アップグレード ファイルのパスおよび名前を指定します。

   注: ldapmodify を実行するには、Critical Path inJoin Directory Server のバージョン 4.2 が必要です。

4. スキーマを再ロードするか、またはスキーマが更新されたことを確認します。
5. [DSA]-[Comms]-[LDAP]に移動し、paging mode オプションを「always」に変更して、DSA を再起動します。

   r12.0 SP3 によって導入されたオブジェクトを含めるようにポリシー ストア スキーマが拡張されます。

ベース ポリシー ストア オブジェクトのインポート

デフォルトの SiteMinder オブジェクトをインポートすると、管理 UI で使用するポリシー ストアがアップグレードされます。デフォルトの SiteMinder オブジェクトは、ポリシー ストアにポリシー情報を格納するために必要です。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. 以下のコマンドを実行します。

   ```
   smobjimport -ipolicy_server_home¥db¥smdif¥upgrade_smdif_file_name
   -dsiteminder_super_user_name -wsiteminder_super_user_password
   -v -f
   ```

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

   upgrade_smdif_file_name

   インポート ファイルの名前を指定します。

   - **r60 から r12.0 SP3:** sm_upgrade_60_to_R12sp3.smdif
   - **r60 SP1 から r12.0 SP3:** sm_upgrade_60sp1_to_R12sp3.smdif
   - **r60 SP2 から r12.0 SP3:** sm_upgrade_60sp2_to_R12sp3.smdif
   - **r60 SP3 から r12.0 SP3:** sm_upgrade_60sp3_to_R12sp3.smdif
   - **r60 SP4 から r12.0 SP3:** sm_upgrade_60sp4_to_R12sp3.smdif
   - **r60 SP5 から r12.0 SP3:** sm_upgrade_60sp5_to_R12sp3.smdif
   - **r60 SP6 から r12.0 SP3:** sm_upgrade_60sp6_to_r12sp3.smdif

-d*siteminder_super_user_name*

SiteMinder 管理者アカウントの名前を指定します。

-w*siteminder_super_user_password*

SiteMinder 管理者アカウントのパスワードを指定します。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト出力： stdout

-f

重複するポリシー ストア オブジェクトを、r12.0 SP3 のもので上書きします。

引数にスペースが含まれる場合、引数全体の前後に二重引用符を使用します。

Windows の例： smobjimport

```
-i"C:¥Program Files¥CA¥siteminder¥db¥smdif¥smpolicy.smdif" -d"SM Admin"
-wPassword -v
```

UNIX の例： smobjimport

-i$NETE_PS_ROOT/db/smdif/smpolicy.smdif -d"SM Admin" -wPassword -v

ベース ポリシー ストア オブジェクトがインポートされます。

2. 以下のコマンドを実行します。

重要：ampolicy.smdif が以前にポリシー ストアにインポートされている場合は再インポートしないでください。

```
smobjimport -ipolicy_server_home¥db¥smdif¥ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

-policy_server_home

インポート ファイルのパスと名前を指定します。

-d*siteminder_super_user_name*

SiteMinder 管理者アカウントの名前を指定します。

-w*siteminder_super_user_password*

SiteMinder 管理者アカウントのパスワードを指定します。

-f

重複するオブジェクトを上書きします。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト値: stdout

-l

ログ ファイルを作成します。

-c

smdif 入力ファイルに暗号化されていないデータが含まれていることを示します。

注: ampolicy.smdif をインポートすると、SiteMinder から別々にライセンスされるフェデレーション セキュリティ サービス、Web サービス変数、および eTelligent ルール機能が使用可能になります。eTelligent ルール機能を使用する予定の場合は、ライセンス情報について CA ジャパン ダイレクトに問い合わせてください。

これで、ポリシー ストア データ定義をインポートできるようになりました。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*¥xps¥dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。

3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

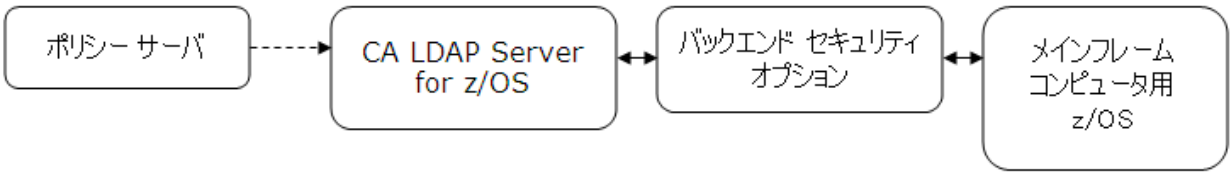
   必要なポリシー ストア データ定義がすべてインポートされました。

第 3 章: CA LDAP Server for z/OS

このセクションには、以下のトピックが含まれています。

CA LDAP Server for z/OS の概要

ポリシー サーバから LDAP サーバへの接続を設定することにより、CA LDAP Server for z/OS をユーザ ストアとして設定できます。ポリシー サーバから LDAP サーバへの接続を設定する方法は、LDAP サーバを保護するために使用しているバックエンド オプションによって異なります。



CA は、CA LDAP サーバに対して以下のバックエンド セキュリティ オプションをサポートします。

- CA Top Secret r12 (TSS)

ポリシー サーバから LDAP サーバへの接続を設定する前に、このバックエンド セキュリティ オプションに関するオブジェクト クラス階層を理解し、LDAP ネームスペース内のポリシー サーバ レジストリにバックエンド関連のオブジェクト クラスを追加します。

注: z/OS はメインフレーム コンピュータ用の IBM オペレーティング システムです。

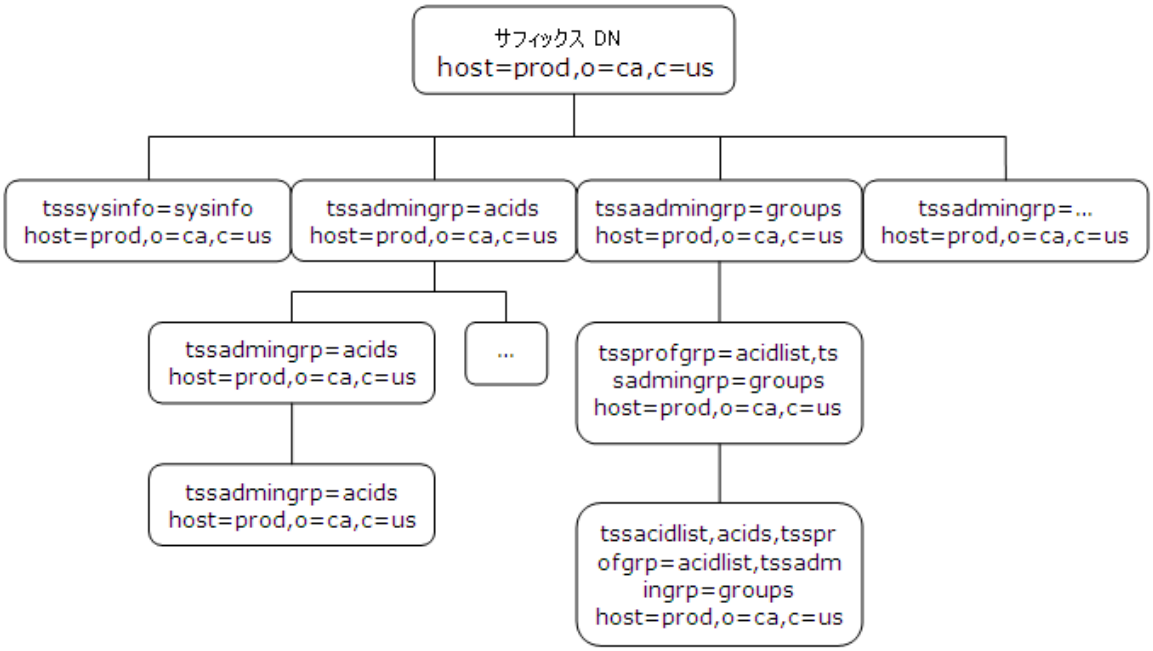
CA Top Secret r12（TSS）バックエンド セキュリティ オプション

CA LDAP Server for z/OS を保護するために TSS を使用している場合は、ポリシー サーバから CA LDAP サーバへの接続を設定する前に、以下の手順を実行してください。

1. TSS オブジェクト クラス階層について理解します。
2. LDAP ネームスペースでポリシー サーバ レジストリに TSS オブジェクト クラスを追加します。

TSS オブジェクト クラス階層

以下の図は、CA Top Secret ディレクトリ情報ツリー（DIT）内のオブジェクト クラス エントリの階層を示しています。図の下に各オブジェクト クラスの説明があります。



オブジェクト クラス host

CA Top Secret データベースに関するオブジェクト クラス階層へのアクセスを開始するために使用されるオブジェクト クラス。

オブジェクト クラス tsssysinfo

host の下のオブジェクト クラス階層にブランチを作成するために使用されるオブジェクト クラス。

オブジェクト クラス tssadmingrp

host の下のオブジェクト クラス階層にブランチを作成するために使用されるオブジェクト クラス。

値は以下のとおりです。

- acids
- profiles
- groups
- departments
- divisions
- zones

オブジェクト クラス tssacid

すべてのユーザ タイプについて ACID レコード フィールドにアクセスするために使用されるオブジェクト クラス。

オブジェクト クラス tssacidgrp

acid の下のオブジェクト クラス階層にブランチを作成するために使用されるオブジェクト クラス。

ポリシー サーバ レジストリ エントリの TSS 用の設定

CA LDAP Server for z/OS には他の LDAP サーバとは異なるオブジェクト クラスが含まれています。ポリシー サーバから CA LDAP サーバへの接続を設定する前に、LDAP ネームスペースで以下のポリシー サーバ レジストリ エントリに TSS オブジェクト クラスを追加し、デフォルト値に対して以下の値を使用します。

registry_entry_home

以下のレジストリ エントリの場所を指定します。

HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥CurrentVersion¥ Ds.

default_value

レジストリ エントリのデフォルト値を指定します。

replacement_value

レジストリ エントリの TSS オブジェクト クラスが含まれる新しい値を指定します。

- registry_entry_home¥ClassFilters

  class_filters_default_value:

  organization,organizationalUnit,groupOfNames,groupOfUniqueNames, group

  class_filters_replacement_value:

  class_filters_default_value,eTTSSAcidName,tssacidgrp,tssadmingrp

- registry_entry_home¥GroupClassFilters

  group_class_filters_default_value:

  groupOfNames,groupOfUniqueNames,group

  group_class_filters_replacement_value:

  group_class_filters_default_value,eTTSSAcidName,tssacidgrp,tssadmingrp

- registry_entry_home¥PolicyClassFilters

  policy_class_filters_default_value:

  organizationalPerson,inetOrgPerson,organization,organizationalUnit, groupOfNames,groupOfUniqueNames,group

  policy_class_filters_replacement_value:

  policy_class_filters_default_value,eTTSSAcidName,tssacidgrp,tssadmingrp

- registry_entry_home¥PolicyResolution

このレジストリ エントリに以下の TSS オブジェクト クラスを追加します。

TSS オブジェクト クラス	レジストリ キー タイプ	データ
eTTSSAcidName	REG_DWORD	0x00000001(1)
tssacidgrp	REG_DWORD	0x00000002(2)
tssadmingrp	REG_DWORD	0x00000003(3)

ポリシー サーバから CA LDAP Server for z/OS への接続の設定

ポリシー サーバから CA LDAP Server for z/OS への接続を設定するには、管理 UI に新規ユーザ ディレクトリ オブジェクトを作成します。

ポリシー サーバから CA LDAP サーバへの接続を設定する方法

1. [インフラストラクチャ]-[ディレクトリ]-[ユーザ ディレクトリ]-[ユーザ ディレクトリの作成]をクリックします。

   [ユーザ ディレクトリの作成]ペインが表示されます。

   注: フィールド、コントロール、およびそれぞれの要件については、[ヘルプ]をクリックしてください。

2. [一般]グループ ボックスのフィールドに、新規のユーザ ディレクトリ オブジェクトの名前と説明を入力します。

3. [ディレクトリのセットアップ]グループ ボックスで、[ネームスペース]リストから[LDAP]を選択し、[サーバ]フィールドに IP アドレスとポート番号を入力します。

   注: 負荷分散とフェールオーバはこの LDAP サーバではサポートされていません。

4. [クレデンシャルが必要]チェック ボックスをオンにして、[管理者クレデンシャル]グループ ボックスのフィールドに管理者のフル DN とパスワードを入力し、ディレクトリ接続に SSL を使用するかどうかを指定します。

   注: TSS ではユーザ ストアへの匿名のバインドが許可されないため、この手順は必須です。

5. [LDAP 検索]グループ ボックスで、[最大時間]フィールドに 100 秒の値を指定します。

   注: ポリシー サーバではこの LDAP サーバからのデータの取得により多くの時間を費やすため、この手順は必須です。

6. [LDAP ユーザ DN の検索]グループ ボックスのフィールドに値を入力します。

7. （任意）[ユーザ属性]グループ ボックスの各フィールドに、SiteMinder 用に予約されているユーザ ディレクトリ プロファイル属性を指定します。

8. （任意）[属性マッピング リスト]グループ ボックスで[作成]をクリックします。

   [属性マッピングの作成]ペインが開きます。

9. [サブミット]をクリックします。

   ユーザ ディレクトリの作成タスクが処理のためにサブミットされます。

CA LDAP Server for z/OS でサポートされていない SiteMinder 機能

CA LDAP Server for z/OS では、以下の SiteMinder 機能がサポートされていません。

匿名バインド

CA Top Secret LDAP サーバをユーザ ストアとして設定する場合、[ユーザ ディレクトリの作成]ペインで[管理者クレデンシャル]グループ ボックスのフィールドに値を指定する必要があります。

ユーザ名でサポートされていない文字

ユーザ名では以下の文字がサポートされていません。

- 空白
- 一重引用符
- 左丸かっこ
- 右丸かっこ
- カンマ
- 円記号

負荷分散およびフェイルオーバー

負荷分散とフェールオーバはサポートされていません。

パスワード サービス

パスワード サービスはサポートされていません。

ユーザ グループとポリシー

ユーザ グループをポリシーに追加し、そのグループ内のユーザの許可を試行すると失敗します。

第 4 章: IBM DB2

このセクションには、以下のトピックが含まれています。

IBM DB2 データベースをデータ ストアとして設定する方法

SiteMinder に用意されているスキーマ ファイルを使用して、IBM DB2 データベースに、ポリシー、キー、監査データ、およびセッション データを格納するためのスキーマを作成することができます。スキーマ ファイル(または SQL スクリプト)は、ZIP ファイルで SiteMinder に用意されています。

IBM DB2 データベースをデータ ストアとして設定する方法は、以下の 4 段階のプロセスです。

1. SiteMinder スキーマ ファイルをダウンロードします。
2. SiteMinder スキーマを含む DB2 データベースの作成
3. SiteMinder 用の DB2 Server データ ソースを設定します。
4. ポリシー サーバがそのデータベースを参照するようにします。
5. SiteMinder スーパーユーザ パスワードを設定します。
6. デフォルトのポリシー ストア オブジェクトをインポートします。
7. ポリシー ストア データ定義をインポートします。
8. 管理 UI の登録を準備します。

SiteMinder スキーマ ファイルのダウンロード

SiteMinder スキーマを設定するのに必要な 1 つ以上のスキーマ ファイルが、ポリシー サーバ インストールに含まれていません。これらのファイルは CA SiteMinder Tier 2 ディレクトリ製品コンポーネント ダウンロードにあります。

Tier 2 ディレクトリ製品コンポーネントをダウンロードする方法

1. テクニカル サポート サイトにログインします。
2. [Support]の下の[Download Center]をクリックします。

   [Download Center]画面が表示されます。
3. [Select a Product]フィールドに「SiteMinder」と入力します。
4. [Select a Release]リストからリリースを選択します。
5. [Select a Gen Level]リストからサービス パックを選択します。
6. [Go]をクリックします。

   [Product Downloads]画面が表示されます。Tier 2 ディレクトリ コンポーネント ダウンロードはリストの下のほうにあります。
7. zip ファイルをローカルに保存し、ポリシー サーバ ホスト システムにファイルを抽出します。

SiteMinder スキーマを含む DB2 データベースの作成

DB2 データベースに SiteMinder スキーマを作成する方法

1. *path*¥ibmdb2 に移動します。

   path

   Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。
2. テキスト エディタに以下のファイルを開き、ファイル全体の内容をコピーします。

   sm_db2_ps.sql

   DB2 データベース内のポリシー ストアまたはキー ストア用のスキーマを指定します。

3. クエリにファイルの内容を貼り付けて、クエリを実行します。

   ポリシー ストアまたはキー ストアのスキーマが、DB2 データベースに作成されます。

4. (任意)ステップ 2 と 3 を繰り返して、監査ログ、セッション サーバ、またはサンプル ユーザ スキーマを DB2 データベースに作成します。

   sm_db2_logs.sql

   DB2 データベース内の監査ログ ストア用のスキーマを指定します。

   sm_db2_ss.sql

   DB2 データベース内のセッション サーバ用のスキーマを指定します。

   smsampleusers_db2.sql

   DB2 データベース内のサンプル ユーザ用のスキーマを指定し、データベースにサンプル ユーザを読み込みます。

   対応する SiteMinder スキーマが DB2 データベースに作成されます。

   注: 1 つの DB2 データベースに対して複数の SiteMinder スキーマを作成するか、または別々のデータベースに各スキーマを作成し、必要に応じて以下のストアを作成することができます。

   - ポリシー ストア
   - キー ストア
   - 監査ログ ストア
   - セッション ストア
   - サンプル ユーザ ストア

5. DB2 ホスト システムに以下の XPS スキーマ ファイルをコピーします。

   path¥xps¥db¥DB2.sql

   path

   Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。

6. コマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   db2 -td@ [-v] -f path¥DB2.sql
   ```

   path

   DB2 設定ファイルへのパスを指定します。

   ポリシー ストア スキーマが作成されます。

SiteMinder に対する DB2 データ ソースの設定

ODBC を使用している場合は、DB2 ワイヤ プロトコル ドライバ用のデータ ソースを設定する必要があります。

Windows システムでの DB2 データ ソースの作成

ODBC を使用している場合は、DB2 ワイヤ プロトコル ドライバ用の DB2 データ ソースを作成できます。

DB2 データ ソースを作成する方法

1. [プログラム]-[管理ツール]-[データ ソース(ODBC)]を選択して、ODBC データ ソース アドミニストレータにアクセスします。
2. [システム DSN]タブをクリックして、[追加]をクリックします。
3. 下にスクロールして[SiteMinder DB2 Wire Protocol]を選択し、[完了]をクリックします。
4. [ODBC DB2 Wire Protocol ドライバのセットアップ]ダイアログ ボックスの[全般]タブで、以下の操作を行います。
   a. [データ ソース名]フィールドに、任意の名前を入力します。

      例: SiteMinder DB2 Wire Data Source

   b. (省略可)[説明]フィールドに、DB2 ワイヤ プロトコル データ ソースの説明を入力します。
   c. [IP アドレス]フィールドに、DB2 データベースがインストールされている場所の IP アドレスを入力します。
   d. [Tcp ポート]フィールドに、DB2 が受信待機するマシン上のポート番号を入力します。
   e. [接続のテスト]をクリックします。

      接続がテストされます。
5. [OK]をクリックします。

   [ODBC DB2 Wire Protocol ドライバのセットアップ]ダイアログ ボックスが閉じて、選択内容が保存されます。DB2 データ ソースが Windows システム上に作成されます。

注: これで、作成したデータ ソースを使用するように SiteMinder を設定できます。

UNIX システムでの DB2 データ ソースの作成

SiteMinder ODBC データ ソースは、system_odbc.ini ファイルを使用して設定します。このファイルは、policy_server_home/db にある db2wire.ini の名前を system_odbc.ini に変更することによって作成できます。この system_odbc.ini ファイルには、使用可能な ODBC データ ソースの名前すべてと、それらのデータ ソースと関連付けられた属性が含まれています。このファイルは、サイトごとに機能するようカスタマイズする必要があります。また、SiteMinder 用のその他の ODBC ユーザ ディレクトリを定義するなど、このファイルに別のデータ ソースを追加することもできます。

system_odbc.ini ファイルの最初のセクション [ODBC Data Sources] には、現在使用可能なデータ ソースすべてのリストが含まれています。「=」の前の名前は、個別のデータ ソースそれぞれを説明する、ファイルの後続のセクションを示しています。「=」の後には、コメント フィールドがあります。

system_odbc.ini ファイル内には、各データ ソースの属性を記述するセクションがあります。最初の属性は、このデータ ソースが SiteMinder で使用されるときにロードされる ODBC ドライバです。残りの属性は、そのドライバに固有です。

DB2 データ ソースを追加するには、ファイルの［ODBC Data Sources］セクションに新規データ ソース名を追加し、データ ソースと同じ名前を使用してデータ ソースを表すセクションを追加します。新しいサービス名を作成したり、別のドライバを使用する場合は、system_odbc.ini ファイルを変更する必要があります。［SiteMinder Data Source］の下に、DB2 ドライバのエントリが必要です。

すでに説明したように、DB2 データ ソースを設定するには、まず、policy_server_home/db ディレクトリに system_odbc.ini ファイルを作成する必要があります。これを行うには、policy_server_home/db にある db2wire.ini の名前を system_odbc.ini に変更する必要があります。

注: policy_server_home にはポリシー サーバのインストール パスを指定します。

DB2 ワイヤ プロトコル ドライバの設定

以下の表に、DB2 データ ソースの設定パラメータを示します。これらのパラメータを編集することで、キー、監査ログ、セッション、およびサンプル ユーザ データベース別にデータ ソースを設定することができます。

パラメータ	説明	編集方法
データ ソース名	データ ソースの名前。	データ ソース名を角かっこで囲んで入力します。
ドライバ	SiteMinder DB2 ワイヤ プロトコル ドライバの完全パス。	「nete_ps_root」を、SiteMinder のインストール ディレクトリに置き換えます。
説明	データ ソースの説明。	任意の希望する説明を入力します。
データベース	DB2 UDB データベースの名前。	「nete_database」を、DB2 UDB サーバ上に設定されたデータベースの名前に置き換えます。
ログオン ID	データベースにアクセスするために必要なユーザ名。	「uid」を、DB2 UDB 管理者のユーザ名に置き換えます。
パスワード	データベースにアクセスするために必要なパスワード。	「pwd」を、DB2 UDB 管理者のパスワードに置き換えます。
IP アドレス	DB2 UDB サーバの IP アドレスまたはホスト名。	「nete_server_ip」を、DB2 UDB サーバの IP アドレスまたはホスト名に置き換えます。
TCP ポート	DB2 UDB サーバの TCP ポート番号。	デフォルト値の 50000 を、DB2 UDB サーバの実際の TCP ポート番号に置き換えます。
パッケージ	動的 SQL を処理するパッケージの名前。	「nete_package」を、作成するパッケージの名前に置き換えます。
PackageOwner	(任意)パッケージに割り当てられた AuthID。	デフォルトは空です。この DB2 AuthID には、パッケージ内のすべての SQL を実行するための権限が必要です。
GrantAuthid	パッケージの実行権限が付与される AuthID。	デフォルトは「PUBLIC」です。パッケージの実行権限を制限したい場合は、必要な AuthID を指定します。

GrantExecute	GrantAuthid にリストされている AuthID に実行権限を付与するかどうかを指定します。	1 または 0 のどちらかを指定できます。デフォルトでは 0 に設定されます。
IsolationLevel	システムがロックを獲得および解放する方法。	デフォルトは CURSOR_STABILITY です。
DynamicSections	DB2 Wire Protocol ドライバ パッケージが 1 人のユーザに用意できるステートメントの数。	デフォルトは 100 です。必要なステートメント数を入力します。

ポリシー サーバに対する参照データベースの指定

ポリシー サーバがポリシー ストア内の SiteMinder データにアクセスできるように、ポリシー サーバがデータベースを参照するようにします。

ポリシー サーバがデータ ストアを参照するようにする方法

1. ポリシー サーバ管理コンソールを開き、[データ]タブをクリックします。

   データベース設定が表示されます。

2. [ストレージ]リストから[ODBC]を選択します。

   ODBC 設定が表示されます。

3. [データベース]リストから[ポリシー ストア]を選択します。

4. [データ ソース情報]フィールドにデータ ソースの名前を入力します。

   - (Windows)このエントリは、データ ソースを作成したときに[データ ソース名]フィールドに入力した名前と一致する必要があります。
   - (UNIX)このエントリは、system_odbc.ini ファイルのデータ ソース エントリの最初の行と一致している必要があります。デフォルトでは、このファイルの最初の行は [SiteMinder Data Sources] です。最初のエントリを変更した場合は、正しい値を入力していることを確認します。

5. それぞれのフィールド内にデータベース インスタンスへのフル アクセス権限を持つデータベース アカウントのユーザ名およびパスワードを入力し確認します。

6. SiteMinder に割り当てるデータベース接続の最大数を指定します。

   注: 最適なパフォーマンスを得るためにデフォルトの 25 の接続を保持することをお勧めします。

7. [適用]をクリックします。

   設定が保存されます。

8. [データベース]リストから[キー ストア]を選択します。

   データ ソース情報が表示されます。

9. [ポリシー ストアを使用]チェック ボックスをオンにして、[適用]をクリックします。

10. [データベース]リストから[監査ログ]を選択します。

    データ ソース設定が表示されます。

11. [ポリシー ストアを使用]チェック ボックスをオンにして、[適用]をクリックします。

12. [接続のテスト]をクリックします。

    SiteMinder によって、ポリシー サーバがデータ ストアにアクセスできるという確認が返されます。

13. [OK]をクリックします。

    ポリシー サーバは、ポリシー ストア、キー ストア、およびログ データベースとしてそのデータベースを使用するように設定されます。

SiteMinder スーパーユーザ パスワードの設定

デフォルトの SiteMinder 管理者アカウントの名前は siteminder です。このアカウントは最大の権限を持っています。その他の SiteMinder 管理者を作成できるまで SiteMinder のユーザ インターフェースとユーティリティの管理に使用できるように、このアカウントのパスワードを設定します。

注: smreg ユーティリティは、ポリシー サーバ インストール キットの最上位レベルにあります。

スーパーユーザのパスワードを設定する方法

1. smreg ユーティリティを *policy_server_home*¥bin にコピーします。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   ```
   smreg -su password
   ```

   重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

   password

   デフォルトの SiteMinder 管理者のパスワードを指定します。

   制限:

   - パスワードは 6 文字以上、24 文字以下である必要があります。
   - パスワードには、アンパサンド(&)またはアスタリスク(*)を含むことはできません。
   - パスワードにスペースが含まれている場合は、引用符でパスフレーズを囲みます。

   注: パスワードは、Oracle ポリシー ストアに保管する場合を除き、大文字小文字が区別されません。

3. *policy_server_home*¥bin から smreg ユーティリティを削除します。smreg を削除すると、既存のパスワードを把握していない限り、パスワードを変更することはできなくなります。

   デフォルトの SiteMinder 管理者アカウントのパスワードが設定されます。

注: 日常的な作業にはデフォルトのスーパーユーザを使用しないことをお勧めします。デフォルトのスーパーユーザは、以下の場合に使用してください。

- デフォルトのポリシー ストア オブジェクトをインポートする場合。
- FSS 管理 UI および 管理 UI に初めてアクセスする場合。スーパーユーザ権限を持つ別の管理者を作成することをお勧めします。

詳細情報:

インストール メディアの検索 (P. 236)

デフォルトのポリシー ストア オブジェクトのインポート

デフォルトのポリシー ストア オブジェクトをインポートすると、管理 UI で使用するポリシー ストアがセットアップされます。ポリシー ストアにポリシー情報を格納するには、デフォルトのポリシー ストア オブジェクトが必要です。

注: FIPS 専用モードでポリシー サーバをインストールした場合は、デフォルトのポリシー ストア オブジェクトをインポートするときに必ず -cf 引数を使用してください。

デフォルトのポリシー ストア オブジェクトをインポートする方法

1. 以下のコマンドを実行します。

   ```
   smobjimport -ipolicy_server_home¥db¥smdif¥smpolicy.smdif
   -dsiteminder_super_user_name -wsiteminder_super_user_password -v
   ```

   引数にスペースが含まれる場合、引数全体の前後に二重引用符を使用します。

   Windows の例: smobjimport

   ```
   -i"C:¥Program Files¥CA¥siteminder¥db¥smdif¥smpolicy.smdif" -d"SM Admin"
   -wPassword -v
   ```

   UNIX の例: smobjimport

   ```
   -i$NETE_PS_ROOT/db/smdif/smpolicy.smdif -d"SM Admin" -wPassword -v
   ```

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

   -d*siteminder_super_user_name*

   SiteMinder スーパーユーザ アカウントの名前を指定します。

   デフォルト: siteminder

   -w*siteminder_super_user_password*

   SiteMinder スーパーユーザ アカウントのパスワードを指定します。

   -v

   追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

   デフォルト値: stdout

-cf

（任意）FIPS 対応の暗号化を使用して機密データをインポートします。

注: この引数は、ポリシー サーバが FIPS 専用モードで動作している場合にのみ必要です。

smobjimport によって、ポリシー ストア オブジェクトがインポートされます。オブジェクトは、適切な場所に自動的にインポートされます。

2. 以下のコマンドを実行します。

```
smobjimport -ipolicy_server_home¥db¥smdif¥ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

policy_server_home

ポリシー サーバのインストール パスを指定します。

-d*siteminder_super_user_name*

SiteMinder スーパーユーザ アカウントの名前を指定します。

デフォルト: siteminder

-w*siteminder_super_user_password*

SiteMinder スーパーユーザ アカウントのパスワードを指定します。

-f

重複するオブジェクトを上書きします。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト値: stdout

-l

ログ ファイルを作成します。

-c

smdif 入力ファイルに暗号化されていないデータが含まれていることを示します。

smobjimport によって、ポリシー ストア オブジェクトがインポートされます。これらのオブジェクトは、適切な場所に自動的にインポートされます。

注: ampolicy.smdif をインポートすると、Federation セキュリティ サービス、Web サービス変数、および eTelligent ルール機能が使用可能になります。eTelligent ルール機能は、SiteMinder から別個にライセンスが提供されます。この eTelligent ルール機能を使用する予定がある場合は、ライセンスの詳細について、CA アカウント担当者に問い合わせてください。

これで、ポリシー ストア データ定義をインポートできるようになりました。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*¥xps¥dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。
2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。

3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   必要なポリシー ストア データ定義がすべてインポートされました。

管理 UI 登録の準備

管理 UI に初めてログインする場合は、デフォルトの SiteMinder スーパーユーザ アカウント(siteminder)を使用します。初めてログインするときは、ポリシー サーバに 管理 UI を登録する必要があります。これで、両方のコンポーネントの間に信頼関係が作成されます。

XPSRegClient ユーティリティを使用してスーパーユーザ アカウントの名前とパスワードを指定して、登録の準備をします。ポリシー サーバは、これらの認証情報を使用して、登録要求が有効であること、および信頼関係を確立できることを検証します。

以下の点について考慮してください。

- 認証情報を指定してから最初の 管理 UI ログインまでの時間は、24 時間に制限されています。24 時間以内に 管理 UI をインストールする予定がない場合は、管理 UI をインストールする前に以下を実行します。
- (UNIX) XPSRegClient を使用する前に、SiteMinder 環境変数が設定されていることを確認してください。環境変数が設定されていない場合は、手動で設定します。

管理 UI 登録を準備する方法

1. ポリシー サーバ ホスト システムにログインします。
2. 以下のコマンドを実行します。

   ```
   XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
   comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

passphrase

デフォルトの SiteMinder スーパーユーザ アカウント（siteminder）のパスワードを指定します。

注：パスフレーズを指定しないと、XPSRegClient により、パスフレーズの入力とその確認を求めるプロンプトが表示されます。

-adminui–setup

管理 UI が初めてポリシー サーバに登録されていることを指定します。

-t *timeout*

（任意）管理 UI をインストールしてから、ログインしてポリシー サーバとの信頼関係を作成するまでの割り当て時間を指定します。タイムアウト値を超過すると、ポリシー サーバは登録リクエストを拒否します。

測定単位： 分

デフォルト： 240（4 時間）

最小制限： 1

最大制限： 1440（24 時間）

-r *retries*

（任意）管理 UI の登録時に許容される試行の失敗回数を指定します。試行に失敗する原因としては、初めて 管理 UI にログインするときに間違った SiteMinder 管理者クレデンシャルをサブミットしたことが考えられます。

デフォルト： 1

最大制限： 5

-c *comment*

（任意）指定されたコメントを情報目的で登録ログ ファイルに挿入します。

注：コメントは引用符で囲んでください。

-cp

（任意）登録ログ ファイルに複数行のコメントが含まれることを指定します。ユーティリティにより複数行のコメントが求められ、指定されたコメントが情報目的で登録ログ ファイルに挿入されます。

注：コメントは引用符で囲んでください。

-l *log path*

（任意）登録ログ ファイルをエクスポートする場所を指定します。

デフォルト: *siteminder_home*¥log

siteminder_home

ポリシー サーバのインストール パスを指定します。

-e *error_path*

（任意）例外を指定されたパスに送信します。

デフォルト: stderr

-vT

（任意）詳細レベルを TRACE に設定します。

-vI

（任意）詳細レベルを INFO に設定します。

-vW

（任意）詳細レベルを WARNING に設定します。

-vE

（任意）詳細レベルを ERROR に設定します。

-vF

（任意）詳細レベルを FATAL に設定します。

3. Enter キーを押します。

XPSRegClient は、ポリシー サーバに管理者クレデンシャルを提供します。ポリシー サーバは、管理 UI への最初のログイン時に、登録リクエストを確認するためにこれらのクレデンシャルを使用します。

6.x セッション サーバのアップグレード

6.x のセッション サーバがインストールされている場合は、r12.0 SP3 の機能を利用するようにアップグレードすることができます。

注: r12.0 SP3 セッション サーバ スキーマは、r6.0 SP5 以降変わっていません。r6.0 SP5 以降のセッション サーバがある場合、スキーマをアップグレードする必要はありません。

既存のセッション ストア データベースに、以下のいずれかの SQL スキーマ スクリプトをインポートします。

6.0、6.0 SP1、または 6.0 SP2 から r12.0 SP3 へのアップグレード

dir_config_home¥ibmdb2¥sm_db2_ss_upgrade_60_60sp1or2_to_R12sp3.sql

6.0 SP3 または 6.0 SP4 から r12.0 SP3 へのアップグレード

dir_config_home¥ibmdb2¥sm_db2_ss_upgrade_60sp3or4_to_R12sp3.sql

dir_config_home

ディレクトリ構成のインストール パスを指定します。

DB2 データベース セッション ストアが、6.x から r12.0 SP3 にアップグレードされて、新規の Expiry Data テーブルがセッション ストアに追加されます。

注: セッション ストア データベースへの SQL スクリプトのインポートの詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

6.x ポリシー ストアをアップグレードする方法

r12.0 SP3 ポリシー ストアに、新規のディレクトリ サーバ インスタンスは必要ありません。既存のポリシー ストアを r12.0 SP3 にアップグレードできます。

ポリシー ストアをアップグレードするには、以下の手順を実行します。

1. ポリシー ストア スキーマを拡張します。

   注:既存の r6.x ポリシー ストア スキーマは、変更されていません。r12.0 SP3 の移行では、ポリシー ストア スキーマをアップグレードして、r12.0 SP3 によって必要とされるオブジェクトのポリシー ストアを拡張する必要があります。

2. ベース ポリシー ストア オブジェクトをインポートします。
3. ポリシー ストア データ定義をインポートします。

注: サポート マトリックスにリストされているディレクトリ サーバまたはデータベースで、本書に記載されていないものをアップグレードする場合は、「SiteMinder アップグレード ガイド」を参照してください。

IBM DB2 ポリシー ストア スキーマの拡張

r12.0 SP3 によって導入されたオブジェクトを含めるように既存の 6.x ポリシー ストア スキーマを拡張することができます。既存の 6.x ポリシー ストア スキーマに加える変更はありません。

既存の IBM DB2 ポリシー ストア スキーマを拡張する方法

1. DB2 ホスト システムにログインします。
2. DB2 ホスト システムに以下の XPS スキーマ ファイルをコピーします。

   path¥xps¥db¥DB2.sql

   path

   Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。
3. コマンド プロンプトを開き、以下のコマンドを実行します。

   db2 -td@ [-v] -f *path*¥DB2.sql

   path

   DB2 設定ファイルへのパスを指定します。

   ポリシー ストア スキーマが拡張されます。

ベース ポリシー ストア オブジェクトのインポート

デフォルトの SiteMinder オブジェクトをインポートすると、管理 UI で使用するポリシー ストアがアップグレードされます。デフォルトの SiteMinder オブジェクトは、ポリシー ストアにポリシー情報を格納するために必要です。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. 以下のコマンドを実行します。

```
smobjimport -ipolicy_server_home¥db¥smdif¥upgrade_smdif_file_name
-dsiteminder_super_user_name -wsiteminder_super_user_password
-v -f
```

policy_server_home

ポリシー サーバのインストール パスを指定します。

upgrade_smdif_file_name

インポート ファイルの名前を指定します。

- **r60 から r12.0 SP3:** sm_upgrade_60_to_R12sp3.smdif
- **r60 SP1 から r12.0 SP3:** sm_upgrade_60sp1_to_R12sp3.smdif
- **r60 SP2 から r12.0 SP3:** sm_upgrade_60sp2_to_R12sp3.smdif
- **r60 SP3 から r12.0 SP3:** sm_upgrade_60sp3_to_R12sp3.smdif
- **r60 SP4 から r12.0 SP3:** sm_upgrade_60sp4_to_R12sp3.smdif
- **r60 SP5 から r12.0 SP3:** sm_upgrade_60sp5_to_R12sp3.smdif
- **r60 SP6 から r12.0 SP3:** sm_upgrade_60sp6_to_r12sp3.smdif

-d*siteminder_super_user_name*

SiteMinder 管理者アカウントの名前を指定します。

-w*siteminder_super_user_password*

SiteMinder 管理者アカウントのパスワードを指定します。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト出力: stdout

-f

重複するポリシー ストア オブジェクトを、r12.0 SP3 のもので上書きします。

引数にスペースが含まれる場合、引数全体の前後に二重引用符を使用します。

Windows の例: smobjimport

```
-i"C:¥Program Files¥CA¥siteminder¥db¥smdif¥smpolicy.smdif" -d"SM Admin"
-wPassword -v
```

UNIX の例: smobjimport

-i$NETE_PS_ROOT/db/smdif/smpolicy.smdif -d"SM Admin" -wPassword -v

ベース ポリシー ストア オブジェクトがインポートされます。

2. 以下のコマンドを実行します。

重要: ampolicy.smdif が以前にポリシー ストアにインポートされている場合は再インポートしないでください。

```
smobjimport -ipolicy_server_home¥db¥smdif¥ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

-policy_server_home

インポート ファイルのパスと名前を指定します。

-d*siteminder_super_user_name*

SiteMinder 管理者アカウントの名前を指定します。

-w*siteminder_super_user_password*

SiteMinder 管理者アカウントのパスワードを指定します。

-f

重複するオブジェクトを上書きします。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト値: stdout

-l

ログ ファイルを作成します。

-c

smdif 入力ファイルに暗号化されていないデータが含まれていることを示します。

注: ampolicy.smdif をインポートすると、SiteMinder から別々にライセンスされるフェデレーション セキュリティ サービス、Web サービス変数、および eTelligent ルール機能が使用可能になります。eTelligent ルール機能を使用する予定の場合は、ライセンス情報について CA ジャパン ダイレクトに問い合わせてください。

これで、ポリシー ストア データ定義をインポートできるようになりました。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*¥xps¥dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。
2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。

3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   必要なポリシー ストア データ定義がすべてインポートされました。

第 5 章: IBM Directory Server

このセクションには、以下のトピックが含まれています。

ポリシー ストアとしての IBM Directory Server

Windows または UNIX システムのいずれかにインストールされたポリシー サーバは、IBM Secureway/Directory Server をポリシー ストアとして使用することができます。

以下のセクションでは、ポリシー ストアとしてディレクトリ サーバを設定する方法について詳しく説明します。

IBM Directory Server

IBM Directory Server をポリシー ストアとして設定する前に、以下の前提条件を満たしていることを確認してください。

1. V3 Matchingrules ファイルの編集

   注: 必要に応じて、IBM Directory Server 構成ツールを使用して、サーバ サフィックスを作成またはロードします。

2. ディレクトリ エントリとルート ノードの作成
3. スキーマ ファイルを管理する SiteMinder スキーマ ファイルの追加

V3 Matchingrules ファイルの編集

ディレクトリ サーバにデフォルトのポリシー ストア オブジェクトを作成する前に、V3.matchingrulesR12sp3 ファイルを編集します。

ファイルを編集する方法

1. *siteminder_home*¥IBMDirectoryServer に移動します。

   siteminder_home

   ポリシー サーバのインストール パスを指定します。

2. V3.matchingrulesR12sp3 ファイルを開きます。
3. 以下の行を追加します。

   ```
   MatchingRules=(2.5.13.15 NAME
   'integerOrderingMatch' SYNTAX 1.3.6.1.4.1.1466.115.121.1.27)
   ```

4. ファイルを保存します。

   V3.matchingrulesR12sp3 ファイルが更新されて、デフォルトのポリシー ストア オブジェクトを安全に作成することができます。

ディレクトリ エントリとルート ノードの作成

IBM Tivoli Directory Server Web 管理ツールを使用して、ディレクトリ エントリとルート ノードを作成します。

ディレクトリ エントリとルート ノードを作成する方法

1. ポリシー サーバ データのルート DN に対する新規のディレクトリ エントリを作成します。

   例: ou=Nete

2. ou=Nete の下に、以下のルート ノードを作成します。

   ou=Netegrity,ou=SiteMinder,ou=PolicySvr4,ou=XPS

スキーマ ファイルを管理する SiteMinder スキーマ ファイルの追加

IBM Directory Server 構成ツールを使用して、スキーマ ファイルを管理するための SiteMinder 提供のスキーマ ファイルを追加します。

SiteMinder スキーマ ファイルを追加する方法

1. *siteminder_home*¥IBMDirectoryServer に移動します。

   siteminder_home

   ポリシー サーバのインストール パスを指定します。

2. IBM Directory Server V3.siteminderR12sp3 スキーマ ファイルを、スキーマ構成の［Manage Schema Files］セクションに移動します。
3. IBM Directory Server を再起動します。

   ファイルが追加され、スキーマ変更が有効になります。

ディレクトリ サーバ情報の収集

LDAP ディレクトリ サーバをポリシー ストアとして設定するか、または既存のポリシー ストアをアップグレードするには、特定のディレクトリ サーバ情報が必要です。作業を始める前に、以下の情報を収集してください。値を記録するためにポリシー ストアのワークシートを使用できます。

注: ポリシー ストアおよびデータ ストアの各ワークシートが用意されているので、SiteMinder データ ストアを設定またはアップグレードする前の情報の収集および記録に使用することができます。作業を始める前に、該当するワークシートを印刷し、そのワークシートに必要な情報を記録しておくことができます。

ホスト情報

ディレクトリ サーバの完全修飾ホスト名または IP アドレスを指定します。

ポート情報

（任意）標準以外のポートを指定します。

デフォルト値: 636（SSL）および 389（SSL 以外）

管理 DN

LDAP ツリー内のポリシー ストア ルート オブジェクトの下でオブジェクトの作成、読み取り、変更、および削除を行う権限を持つユーザの LDAP ユーザ名を指定します。

管理パスワード

管理 DN のパスワードを指定します。

ポリシー サーバのルート DN

ポリシー ストア オブジェクトを定義する、LDAP ツリー内のノードの識別名を指定します。

SSL クライアント証明書

SSL クライアント証明書データベース ファイルがあるディレクトリのパス名を指定します。

制限: SSL のみ

ポリシー ストアを設定する方法

IBM Directory Server をポリシー ストアとして設定するには、以下の手順に従います。

1. IBM Directory Server の前提条件を満たしていることを確認します。
2. 必要な情報を収集したことを確認します。
3. 以下の手順に従います。
   a. ポリシー サーバからポリシー ストアへの参照の設定
   b. SiteMinder スーパーユーザ パスワードの設定

      注: SiteMinder スーパーユーザ パスワードがすでにある場合は、この手順を実行する必要はありません。
   c. ポリシー ストア スキーマの作成
   d. デフォルトのポリシー ストア オブジェクトのインポート
   e. ポリシー ストア データ定義のインポート
   f. ポリシー サーバの再起動
   g. 管理 UI 登録の準備

ポリシー サーバからポリシー ストアへの参照の設定

ポリシー サーバからポリシー ストアへの参照を設定し、ポリシー サーバがポリシー ストアにアクセスできるようにします。

ポリシー サーバからポリシー ストアへの参照を設定する方法

1. ポリシー サーバ管理コンソールを開きます。

   重要: Windows Server 2008 上でこのグラフィカル ユーザ インターフェースにアクセスする場合は、管理者としてシステムにログインしている場合でも、管理者権限でショートカットを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

2. [データ]タブをクリックします。

   データベース設定が表示されます。

3. [データベース]リストから[ポリシー ストア]を選択します。

4. [ストレージ]リストから[LDAP]を選択します。

5. [LDAP ポリシー ストア]グループ ボックスで、以下を設定します。

   - LDAP IP アドレス
   - 管理者ユーザ名
   - パスワード
   - パスワードの確認
   - DN

   注: フィールド、コントロール、およびそれぞれの要件については、[ヘルプ]をクリックしてください。

6. [適用]をクリックします。

   ポリシー ストアの設定が保存されます。

7. [LDAP 接続のテスト]をクリックします。

   SiteMinder は、ポリシー サーバがポリシー ストアにアクセスできることを示す確認を返します。

ポリシー ストア スキーマの作成

ポリシー ストアおよびストア SiteMinder オブジェクトとしてディレクトリ サーバが機能できるように、ポリシー ストア スキーマを作成します。

ポリシー ストア スキーマを作成する方法

1. 以下のコマンドを実行します。

```
smldapsetup ldgen -hhost -pport -dAdminDN -wAdminPW
-rroot -ssl1/0 -ccert -ffile_name
```

注: smldapsetup ツールの詳細については、「ポリシー サーバ管理ガイド」を参照してください。

-h*host*

ディレクトリ サーバの IP アドレスを指定します。

例: 123.123.12.12

-p*port*

ディレクトリ サーバが受信待機するポート番号を指定します。

例: 3500

-d*AdminDN*

新規の LDAP ルートを作成する権限を持つ LDAP ユーザ アカウントの名前を指定します。

例: "cn=Directory Manager"

-w*AdminPW*

新規の LDAP ルートを作成する権限を持つ LDAP ユーザ アカウントのパスワードを指定します。

例: MyPassword123

-r*root*

ディレクトリ サーバのルートを指定します。

例: c=domain、dc=com

-ssl

(任意) SSL 接続を指定します。

制限: 0=no または 1=yes

デフォルト: 0

-ccert

(ssl が 1 に設定されている場合にのみ必須) SSL クライアント証明書データベースの絶対パスを定義します。

-ffile_name

ポリシー ストア用に作成するスキーマ ファイルの名前を指定します。

2. 以下のコマンドを実行します。

```
smldapsetup ldmod -ffile_name
```

-ffile_name

ポリシー ストア用に作成したスキーマ ファイルの名前を指定します。

3. *policy_server_home*¥xps¥db に移動し、以下のファイルを見つけます。次に、IBM Directory Server 構成ツールを使用してスキーマ構成の[Manage Schema Files]セクションにそのファイルを追加します。

IBMDirectoryServer.ldif

4. IBM Directory Server を再起動します。

ポリシー ストア スキーマが作成されます。

SiteMinder スーパーユーザ パスワードの設定

デフォルトの SiteMinder 管理者アカウントの名前は siteminder です。このアカウントは最大の権限を持っています。その他の SiteMinder 管理者を作成できるまで SiteMinder のユーザ インターフェースとユーティリティの管理に使用できるように、このアカウントのパスワードを設定します。

注: smreg ユーティリティは、ポリシー サーバ インストール キットの最上位レベルにあります。

スーパーユーザのパスワードを設定する方法

1. smreg ユーティリティを *policy_server_home*¥bin にコピーします。

policy_server_home

ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   ```
   smreg -su password
   ```

   重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

   password

   デフォルトの SiteMinder 管理者のパスワードを指定します。

   制限:

   - パスワードは 6 文字以上、24 文字以下である必要があります。
   - パスワードには、アンパサンド(&)またはアスタリスク(*)を含むことはできません。
   - パスワードにスペースが含まれている場合は、引用符でパスフレーズを囲みます。

   注: パスワードは、Oracle ポリシー ストアに保管する場合を除き、大文字小文字が区別されません。

3. *policy_server_home*¥bin から smreg ユーティリティを削除します。smreg を削除すると、既存のパスワードを把握していない限り、パスワードを変更することはできなくなります。

   デフォルトの SiteMinder 管理者アカウントのパスワードが設定されます。

注: 日常的な作業にはデフォルトのスーパーユーザを使用しないことをお勧めします。デフォルトのスーパーユーザは、以下の場合に使用してください。

- デフォルトのポリシー ストア オブジェクトをインポートする場合。
- FSS 管理 UI および 管理 UI に初めてアクセスする場合。スーパーユーザ権限を持つ別の管理者を作成することをお勧めします。

詳細情報:

インストール メディアの検索 (P. 236)

デフォルトのポリシー ストア オブジェクトのインポート

デフォルトのポリシー ストア オブジェクトをインポートすると、管理 UI で使用するポリシー ストアがセットアップされます。ポリシー ストアにポリシー情報を格納するには、デフォルトのポリシー ストア オブジェクトが必要です。

注: FIPS 専用モードでポリシー サーバをインストールした場合は、デフォルトのポリシー ストア オブジェクトをインポートするときに必ず -cf 引数を使用してください。

デフォルトのポリシー ストア オブジェクトをインポートする方法

1. 以下のコマンドを実行します。

   ```
   smobjimport -ipolicy_server_home¥db¥smdif¥smpolicy.smdif
   -dsiteminder_super_user_name -wsiteminder_super_user_password -v
   ```

   引数にスペースが含まれる場合、引数全体の前後に二重引用符を使用します。

   Windows の例: smobjimport

   ```
   -i"C:¥Program Files¥CA¥siteminder¥db¥smdif¥smpolicy.smdif" -d"SM Admin"
   -wPassword -v
   ```

   UNIX の例: smobjimport

   ```
   -i$NETE_PS_ROOT/db/smdif/smpolicy.smdif -d"SM Admin" -wPassword -v
   ```

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

   -d*siteminder_super_user_name*

   SiteMinder スーパーユーザ アカウントの名前を指定します。

   デフォルト: siteminder

   -w*siteminder_super_user_password*

   SiteMinder スーパーユーザ アカウントのパスワードを指定します。

   -v

   追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

   デフォルト値: stdout

-cf

（任意）FIPS 対応の暗号化を使用して機密データをインポートします。

注: この引数は、ポリシー サーバが FIPS 専用モードで動作している場合にのみ必要です。

smobjimport によって、ポリシー ストア オブジェクトがインポートされます。オブジェクトは、適切な場所に自動的にインポートされます。

2. 以下のコマンドを実行します。

```
smobjimport -ipolicy_server_home¥db¥smdif¥ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

policy_server_home

ポリシー サーバのインストール パスを指定します。

-d*siteminder_super_user_name*

SiteMinder スーパーユーザ アカウントの名前を指定します。

デフォルト: siteminder

-w*siteminder_super_user_password*

SiteMinder スーパーユーザ アカウントのパスワードを指定します。

-f

重複するオブジェクトを上書きします。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト値: stdout

-l

ログ ファイルを作成します。

-c

smdif 入力ファイルに暗号化されていないデータが含まれていることを示します。

smobjimport によって、ポリシー ストア オブジェクトがインポートされます。これらのオブジェクトは、適切な場所に自動的にインポートされます。

注: ampolicy.smdif をインポートすると、Federation セキュリティ サービス、Web サービス変数、および eTelligent ルール機能が使用可能になります。eTelligent ルール機能は、SiteMinder から別個にライセンスが提供されます。この eTelligent ルール機能を使用する予定がある場合は、ライセンスの詳細について、CA アカウント担当者に問い合わせてください。

これで、ポリシー ストア データ定義をインポートできるようになりました。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*¥xps¥dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。
2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。

3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   必要なポリシー ストア データ定義がすべてインポートされました。

ポリシー サーバの再起動

ポリシー ストアやその他のデータ ストアの設定を有効にするために、ポリシー サーバを再起動します。

注: UNIX システムでは、stop-all コマンドの後に start-all コマンドを使用することで、ポリシー サーバを再起動できます。

ポリシー サーバを再起動するには、以下の手順に従います。

1. ポリシー サーバ管理コンソールを開きます。
2. [ステータス]タブをクリックし、[ポリシー サーバ]グループ ボックスで[停止]をクリックします。

   赤色の信号アイコンが表示されて、ポリシー サーバが停止します。
3. [開始]をクリックします。

   緑色の信号アイコンが表示されて、ポリシー サーバが起動します。

管理 UI 登録の準備

管理 UI に初めてログインする場合は、デフォルトの SiteMinder スーパーユーザ アカウント(siteminder)を使用します。初めてログインするときは、ポリシー サーバに 管理 UI を登録する必要があります。これで、両方のコンポーネントの間に信頼関係が作成されます。

XPSRegClient ユーティリティを使用してスーパーユーザ アカウントの名前とパスワードを指定して、登録の準備をします。ポリシー サーバは、これらの認証情報を使用して、登録要求が有効であること、および信頼関係を確立できることを検証します。

以下の点について考慮してください。

- 認証情報を指定してから最初の 管理 UI ログインまでの時間は、24 時間に制限されています。24 時間以内に 管理 UI をインストールする予定がない場合は、管理 UI をインストールする前に以下を実行します。
- （UNIX）XPSRegClient を使用する前に、SiteMinder 環境変数が設定されていることを確認してください。環境変数が設定されていない場合は、手動で設定します。

管理 UI 登録を準備する方法

1. ポリシー サーバ ホスト システムにログインします。
2. 以下のコマンドを実行します。

   ```
   XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

   passphrase

   デフォルトの SiteMinder スーパーユーザ アカウント（siteminder）のパスワードを指定します。

   注: パスフレーズを指定しないと、XPSRegClient により、パスフレーズの入力とその確認を求めるプロンプトが表示されます。

   -adminui–setup

   管理 UI が初めてポリシー サーバに登録されていることを指定します。

   -t *timeout*

   （任意）管理 UI をインストールしてから、ログインしてポリシー サーバとの信頼関係を作成するまでの割り当て時間を指定します。タイムアウト値を超過すると、ポリシー サーバは登録リクエストを拒否します。

   測定単位: 分

   デフォルト: 240（4 時間）

   最小制限: 1

   最大制限: 1440（24 時間）

-r *retries*

(任意) 管理 UI の登録時に許容される試行の失敗回数を指定します。試行に失敗する原因としては、初めて 管理 UI にログインするときに間違った SiteMinder 管理者クレデンシャルをサブミットしたことが考えられます。

デフォルト: 1

最大制限: 5

-c *comment*

(任意) 指定されたコメントを情報目的で登録ログ ファイルに挿入します。

注: コメントは引用符で囲んでください。

-cp

(任意) 登録ログ ファイルに複数行のコメントが含まれることを指定します。ユーティリティにより複数行のコメントが求められ、指定されたコメントが情報目的で登録ログ ファイルに挿入されます。

注: コメントは引用符で囲んでください。

-l *log path*

(任意) 登録ログ ファイルをエクスポートする場所を指定します。

デフォルト: *siteminder_home*¥log

siteminder_home

ポリシー サーバのインストール パスを指定します。

-e *error_path*

(任意) 例外を指定されたパスに送信します。

デフォルト: stderr

-vT

(任意) 詳細レベルを TRACE に設定します。

-vI

（任意）詳細レベルを INFO に設定します。

-vW

（任意）詳細レベルを WARNING に設定します。

-vE

（任意）詳細レベルを ERROR に設定します。

-vF

（任意）詳細レベルを FATAL に設定します。

3. Enter キーを押します。

   XPSRegClient は、ポリシー サーバに管理者クレデンシャルを提供します。ポリシー サーバは、管理 UI への最初のログイン時に、登録リクエストを確認するためにこれらのクレデンシャルを使用します。

6.x ポリシー ストアをアップグレードする方法

r12.0 SP3 ポリシー ストアに、新規のディレクトリ サーバ インスタンスは必要ありません。既存のポリシー ストアを r12.0 SP3 にアップグレードできます。

ポリシー ストアをアップグレードするには、以下の手順を実行します。

1. ポリシー ストア スキーマを拡張します。

   注：既存の r6.x ポリシー ストア スキーマは、変更されていません。r12.0 SP3 の移行では、ポリシー ストア スキーマをアップグレードして、r12.0 SP3 によって必要とされるオブジェクトのポリシー ストアを拡張する必要があります。

2. ベース ポリシー ストア オブジェクトをインポートします。
3. ポリシー ストア データ定義をインポートします。

注：サポート マトリックスにリストされているディレクトリ サーバまたはデータベースで、本書に記載されていないものをアップグレードする場合は、「SiteMinder アップグレード ガイド」を参照してください。

IBM Directory Server ポリシー ストア スキーマの拡張

r12.0 SP3 によって導入されたオブジェクトを含めるように既存の 6.x ポリシー ストア スキーマを拡張することができます。既存の 6.x ポリシー ストア スキーマに加える変更はありません。

IBM Directory Server ポリシー ストア スキーマを拡張する方法

1. IBM Tivoli Directory Server Web Administration Tool を使用してポリシー ストア ルート ノードを更新します。ou=PolicySvr4 の下に以下のルート ノードを作成します。

   ou=XPS

2. *siteminder_home*¥xps¥db に移動し、以下のファイルを見つけます。次に、IBM Directory Server 構成ツールを使用してスキーマ構成の[Manage Schema Files]セクションにそのファイルを追加します。

   IBMDirectoryServer.ldif

   siteminder_home

   ポリシー サーバのインストール パスを指定します。

3. IBM Directory Server を再起動します。

   r12.0 SP3 によって導入されたオブジェクトを含めるようにポリシー ストア スキーマが拡張されます。

ベース ポリシー ストア オブジェクトのインポート

デフォルトの SiteMinder オブジェクトをインポートすると、管理 UI で使用するポリシー ストアがアップグレードされます。デフォルトの SiteMinder オブジェクトは、ポリシー ストアにポリシー情報を格納するために必要です。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. 以下のコマンドを実行します。

```
smobjimport -ipolicy_server_home¥db¥smdif¥upgrade_smdif_file_name
-dsiteminder_super_user_name -wsiteminder_super_user_password
-v -f
```

policy_server_home

ポリシー サーバのインストール パスを指定します。

upgrade_smdif_file_name

インポート ファイルの名前を指定します。

- **r60 から r12.0 SP3:** sm_upgrade_60_to_R12sp3.smdif
- **r60 SP1 から r12.0 SP3:** sm_upgrade_60sp1_to_R12sp3.smdif
- **r60 SP2 から r12.0 SP3:** sm_upgrade_60sp2_to_R12sp3.smdif
- **r60 SP3 から r12.0 SP3:** sm_upgrade_60sp3_to_R12sp3.smdif
- **r60 SP4 から r12.0 SP3:** sm_upgrade_60sp4_to_R12sp3.smdif
- **r60 SP5 から r12.0 SP3:** sm_upgrade_60sp5_to_R12sp3.smdif
- **r60 SP6 から r12.0 SP3:** sm_upgrade_60sp6_to_r12sp3.smdif

-d*siteminder_super_user_name*

SiteMinder 管理者アカウントの名前を指定します。

-w*siteminder_super_user_password*

SiteMinder 管理者アカウントのパスワードを指定します。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト出力: stdout

-f

重複するポリシー ストア オブジェクトを、r12.0 SP3 のもので上書きします。

引数にスペースが含まれる場合、引数全体の前後に二重引用符を使用します。

Windows の例: smobjimport

```
-i"C:¥Program Files¥CA¥siteminder¥db¥smdif¥smpolicy.smdif" -d"SM Admin"
-wPassword -v
```

UNIX の例: smobjimport

-i$NETE_PS_ROOT/db/smdif/smpolicy.smdif -d"SM Admin" -wPassword -v

ベース ポリシー ストア オブジェクトがインポートされます。

2. 以下のコマンドを実行します。

重要: ampolicy.smdif が以前にポリシー ストアにインポートされている場合は再インポートしないでください。

```
smobjimport -ipolicy_server_home¥db¥smdif¥ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

-policy_server_home

インポート ファイルのパスと名前を指定します。

-d*siteminder_super_user_name*

SiteMinder 管理者アカウントの名前を指定します。

-w*siteminder_super_user_password*

SiteMinder 管理者アカウントのパスワードを指定します。

-f

重複するオブジェクトを上書きします。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト値: stdout

-l

ログ ファイルを作成します。

-c

smdif 入力ファイルに暗号化されていないデータが含まれていることを示します。

注: ampolicy.smdif をインポートすると、SiteMinder から別々にライセンスされるフェデレーション セキュリティ サービス、Web サービス変数、および eTelligent ルール機能が使用可能になります。eTelligent ルール機能を使用する予定の場合は、ライセンス情報について CA ジャパン ダイレクトに問い合わせてください。

これで、ポリシー ストア データ定義をインポートできるようになりました。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*¥xps¥dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。
2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。

3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   必要なポリシー ストア データ定義がすべてインポートされました。

第 6 章: MySQL サーバ

このセクションには、以下のトピックが含まれています。

ポリシー ストアとしての MySQL

MySQL ポリシー ストアは以下として機能できます。

- キー ストア
- 監査ログ データベース

  注: SiteMinder セッション情報は別のデータベースに格納される必要があります。セッション情報を格納するためにポリシー ストアを使用することはできません。

単一のデータベースを使用すると管理タスクが簡略化されます。後続のセクションでは、SiteMinder データを格納するように 1 つのデータベース サーバを設定する方法について説明します。

データベース情報の収集

ポリシー ストアまたは他のタイプの SiteMinder データ ストアとして機能するよう単一の MySQL Server データベースを設定するには、特定のデータベース情報が必要です。

ポリシー ストアまたは他のタイプの SiteMinder データ ストアを設定する前に以下の情報を収集します。

- **データベース ホスト** -- データベース ホスト システムの名前。
- **データベース インスタンス名** -- ポリシー ストアまたはデータ ストアとして機能するデータベース インスタンスの名前。

- **ポート** -- データベースがリスンするポート。
- **管理者アカウント** -- データベース内でオブジェクトを作成、読み取り、変更、削除する権限を持つ管理者アカウントのログイン ID。
- **管理者パスワード** -- 管理者アカウントのパスワード。

詳細情報:

キー情報を MySQL に格納する方法 (P. 97)
監査ログを MySQL に格納する方法 (P. 100)
セッション情報を MySQL に格納する方法 (P. 103)

ポリシー ストアを設定する方法

ポリシー ストアとして MySQL Server データベースを設定するには、以下の手順に従います。

注: 開始する前に、必要なデータベース情報が収集されていることを確認してください。以下の手順のうちのいくつかは、この情報を必要とします。

1. MySQL が必ずデフォルト文字セット(Latin1)を使用してインストールされていることを確認します。MySQL がデフォルト文字セットを使用してインストールされていない場合、SiteMinder データ ストアを設定する前に MySQL を再インストールします。
2. ポリシー ストアとして機能する MySQL データベースにポリシー サーバ ホスト システムからアクセス可能であることを確認します。
3. ベンダー固有のユーザ インターフェースを使用して、SiteMinder データ ストア用のデータベース インスタンスを作成します。
4. SiteMinder スキーマ ファイルをダウンロードします。
5. SiteMinder スキーマを作成します。
6. SiteMinder 用の MySQL データ ソースを設定します。
   - (Windows) MySQL データ ソースを作成します。
   - (UNIX) UNIX システム上に MySQL データ ソースを作成します。
   - (UNIX) MySQL ワイヤ プロトコル ドライバを設定します。
7. ポリシー サーバがそのデータベースを参照するようにします。
8. SiteMinder スーパーユーザ パスワードを設定します。

9. デフォルトの SiteMinder オブジェクトをインポートします。
10. ポリシー ストア データ定義をインポートします。
11. ポリシー サーバを再起動します。
12. 管理 UI の登録を準備します。

SiteMinder スキーマ ファイルのダウンロード

SiteMinder スキーマを設定するのに必要な 1 つ以上のスキーマ ファイルが、ポリシー サーバ インストールに含まれていません。これらのファイルは CA SiteMinder Tier 2 ディレクトリ製品コンポーネント ダウンロードにあります。

Tier 2 ディレクトリ製品コンポーネントをダウンロードする方法

1. テクニカル サポート サイトにログインします。
2. [Support]の下の[Download Center]をクリックします。

   [Download Center]画面が表示されます。
3. [Select a Product]フィールドに「SiteMinder」と入力します。
4. [Select a Release]リストからリリースを選択します。
5. [Select a Gen Level]リストからサービス パックを選択します。
6. [Go]をクリックします。

   [Product Downloads]画面が表示されます。Tier 2 ディレクトリ コンポーネント ダウンロードはリストの下のほうにあります。
7. zip ファイルをローカルに保存し、ポリシー サーバ ホスト システムにファイルを抽出します。

SiteMinder スキーマの作成

SiteMinder スキーマを作成することによって、MySQL データベースにポリシー、キー、監査ログ情報を格納できるようにします。

MySQL データベースに SiteMinder スキーマを作成する方法

1. *path*¥MySQL に移動します。

   path

   Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。

2. テキスト エディタに以下のファイルを開き、ファイル全体の内容をコピーします。

   sm_mysql_ps.sql

3. クエリにファイルの内容を貼り付けて、クエリを実行します。

   ポリシーおよびキー ストアのスキーマが作成されます。

   注: このスキーマ ファイルを使用してスタンドアロン キー ストアを作成できます。

4. (任意) 手順 2 と 3 を繰り返して、監査ログまたはサンプル ユーザ用のスキーマを作成します。

   sm_mysql_logs.sql

   監査ログ ストア用のスキーマを指定します。

   smsampleusers_mysql.sql

   サンプル ユーザ用のスキーマを指定し、データベースにサンプル ユーザを読み込みます。

   対応する SiteMinder スキーマが作成されます。

   注: ポリシー ストアを使用してキー、監査、サンプル ユーザを格納することは任意です。これらのタイプの SiteMinder データ ストアとして個別に機能するよう別のデータベースを使用することができます。

5. *path*¥xps¥MySQL に移動します。

   path

   Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。

6. テキスト エディタに以下のファイルを開き、ファイル全体の内容をコピーします。

   MySQL.sql

7. クエリにファイルの内容を貼り付けて、クエリを実行します。

   ポリシー ストア スキーマが作成されます。

SiteMinder 用の MySQL データ ソースの設定

ポリシー サーバが SiteMinder データ ストアと通信できるようデータ ソースを設定します。

詳細情報:

キー情報を MySQL に格納する方法 (P. 97)
監査ログを MySQL に格納する方法 (P. 100)
セッション情報を MySQL に格納する方法 (P. 103)
MySQL ユーザ ストアを設定する方法 (P. 107)

Windows での MySQL データ ソースの作成

MySQL ワイヤ プロトコル ドライバ用に MySQL データ ソースを作成します。

MySQL データ ソースを作成する方法

1. ポリシー サーバ ホスト システムにログインします。
2. ODBC データ ソース アドミニストレータが開きます。
3. [システム DSN]をクリックします。

   システム データ ソースのリストに利用可能なすべてのデータ ソースがリスト表示されます。

4. [追加]をクリックします。

   [データ ソースの新規作成]ダイアログ ボックスが表示されます。

5. 下にスクロールして SiteMinder MySQL Wire Protocol を選択し、[完了]をクリックします。

   ODBC MySQL Wire Protocol ドライバのセットアップ ダイアログ ボックスが表示されます。

6. ［全般］タブで以下のフィールドに入力します。
   a. ［データ ソース名］フィールドにデータ ソース名を入力します。

      例: SiteMinder MySQL Wire Data Source

   b. ［ホスト名］フィールドに MySQL データベース ホスト システムの名前を入力します。
   c. ［ポート番号］フィールドに MySQL データベースがリスンするポートを入力します。
   d. ［データベース名］フィールドに MySQL データベースの名前を入力します。
7. ［接続のテスト］をクリックします。

   接続設定がテストされます。設定が有効な場合、接続に成功したことを伝えるメッセージが表示されます。
8. ［OK］をクリックします。

   データ ソースが作成され、システム データ ソースのリストに表示されます。

注: ポリシー サーバが SiteMinder データ ストアを参照するよう設定できます。

UNIX システムでの MySQL データ ソースの作成

SiteMinder ODBC データ ソースは、system_odbc.ini ファイルを使用して設定します。このファイルを作成するには mysqlwire.ini の名前を system_odbc.ini に変更します。mysqlwire.ini ファイルは *siteminder_home*/db 内にあります。

siteminder_home

ポリシー サーバのインストール パスを指定します。

この system_odbc.ini ファイルには、使用可能な ODBC データ ソースのすべての名前と、それらのデータ ソースに関連付けられている属性が含まれています。このファイルは、サイトごとに機能するようカスタマイズする必要があります。 また、このファイルにはデータ ソースを追加できます。たとえば、SiteMinder 用の追加の ODBC ユーザ ディレクトリを定義できます。

system_odbc.ini ファイルの最初のセクション [ODBC Data Sources] には、現在使用可能なデータ ソースすべてのリストが含まれています。「=」の前の名前は、個別のデータ ソースそれぞれを説明する、ファイルの後続のセクションを示しています。「=」の後には、コメント フィールドがあります。

注: データ ソース エントリの最初の行([SiteMinder Data Source])を変更する場合、値を記録しておいてください。この値は、データベースをポリシー ストアとして設定する場合に必要になります。

system_odbc.ini ファイル内には、各データ ソースの属性を記述するセクションがあります。最初の属性は、SiteMinder でこのデータ ソースを使用するときにロードされる ODBC ドライバです。残りの属性は、そのドライバに固有です。

MySQL データ ソースを追加すると以下が追加されます。

- ファイルの [ODBC Data Sources] セクションに新しいデータ ソース名を追加。
- データ ソースと同じ名前を使用してデータ ソースについて説明するセクションを追加。

新規サービス名を作成するか、別のドライバを使用する場合は、system_odbc.ini ファイルを更新します。[SiteMinder Data Source] の下に、MySQL ドライバのエントリが必要です。

ここでも、MySQL データ ソースを設定するために、mysqlwire.ini の名前を system_odbc.ini に変更して system_odbc.ini ファイルを作成します。

MySQL ワイヤ プロトコル ドライバの作成

ワイヤ プロトコル ドライバを設定し、データベースに接続するために SiteMinder が使用する設定を指定します。

注: この手順は、ポリシー サーバが UNIX システムにインストールされる場合にのみ、適用されます。以下のいずれかのファイルをコピーし、名前を「system_odbc.ini」に変更します(まだ行っていない場合)。名前を変更するファイルは、SiteMinder データ ストアとして設定しているデータベース ベンダーによって異なります。

- sqlserverwire.ini
- oraclewire.ini
- mysqlwire.ini

これらのファイルは *siteminder_home*/db にあります。

system_odbc.ini ファイルは、以下のセクションで構成されています。設定しているデータ ソースにより、編集するセクションが決定されます。

[SiteMinder Data Source]

ポリシー ストアとして機能するデータベースに接続するために、SiteMinder が使用する設定を指定します。

[SiteMinder Logs Data Source]

監査ログ データベースとして機能するデータベースに接続するために、SiteMinder が使用する設定を指定します。

[SiteMinder Keys Data Source]

キー ストアとして機能するデータベースに接続するために、SiteMinder が使用する設定を指定します。

[SiteMinder Session Data Source]

セッション ストアとして機能するデータベースに接続するために、SiteMinder が使用する設定を指定します。

[SmSampleUsers Data Source]

サンプル ユーザ データ ストアとして機能するデータベースに接続するために、SiteMinder が使用する設定を指定します。

ワイヤ プロトコル ドライバを設定する方法

1. system_odbc.ini ファイルを開きます。
2. [ODBC Data Sources] の下に、以下を入力します。

   ```
   SiteMinder Data Source=DataDirect 6.0 MySQL Wire Protocol.
   ```

3. 設定するデータ ソースに応じて、以下の情報を使用して 1 つ以上のデータ ソース セクションを編集します。

   ```
   Driver=nete_ps_root/odbc/lib/NSmysql24.so
   Description=DataDirect 6.0 MySQL Wire Protocol
   Database=database_name
   HostName=host_name
   LogonID=root_user
   Password=root_user_password
   PortNumber=mysql_port
   ```

   注: データ ソース情報を編集する場合は、番号記号(#)を使用しないでください。番号記号(#)を入力すると、その情報はコメント化され、値が切り捨てられます。値が切り捨てられると、ODBC 接続に失敗する場合があります。

nete_ps_root

ポリシー サーバのインストール パスを指定します。この値は、環境変数を使用せず、明示的なパスとして入力します。

例: /export/smuser/siteminder

database_name

SiteMinder データ ストアとして機能する MySQL データベースの名前を指定します。

host_name

MySQL データベース ホスト システムの名前を指定します。

root_user

MySQL root ユーザのログイン ID を指定します。

root_user_password

MySQL root ユーザのパスワードを指定します。

mysql_port

MySQL データベースがリスンするポートを指定します。

4. ファイルを保存します。

   ワイヤ プロトコル ドライバが設定されます。

ポリシー サーバに対する参照データベースの指定

ポリシー サーバがポリシー ストア内の SiteMinder データにアクセスできるように、ポリシー サーバがデータベースを参照するようにします。

ポリシー サーバがデータ ストアを参照するようにする方法

1. ポリシー サーバ管理コンソールを開き、[データ]タブをクリックします。

   データベース設定が表示されます。

2. [ストレージ]リストから[ODBC]を選択します。

   ODBC 設定が表示されます。

3. [データベース]リストから[ポリシー ストア]を選択します。

4. [データ ソース情報]フィールドにデータ ソースの名前を入力します。
   - (Windows)このエントリは、データ ソースを作成したときに[データ ソース名]フィールドに入力した名前と一致する必要があります。
   - (UNIX)このエントリは、system_odbc.ini ファイルのデータ ソース エントリの最初の行と一致している必要があります。デフォルトでは、このファイルの最初の行は [SiteMinder Data Sources] です。最初のエントリを変更した場合は、正しい値を入力していることを確認します。
5. それぞれのフィールド内にデータベース インスタンスへのフル アクセス権限を持つデータベース アカウントのユーザ名およびパスワードを入力し確認します。
6. SiteMinder に割り当てるデータベース接続の最大数を指定します。

   注: 最適なパフォーマンスを得るためにデフォルトの 25 の接続を保持することをお勧めします。
7. [適用]をクリックします。

   設定が保存されます。
8. [データベース]リストから[キー ストア]を選択します。

   データ ソース情報が表示されます。
9. [ポリシー ストアを使用]チェック ボックスをオンにして、[適用]をクリックします。
10. [データベース]リストから[監査ログ]を選択します。

    データ ソース設定が表示されます。
11. [ポリシー ストアを使用]チェック ボックスをオンにして、[適用]をクリックします。
12. [接続のテスト]をクリックします。

    SiteMinder によって、ポリシー サーバがデータ ストアにアクセスできるという確認が返されます。
13. [OK]をクリックします。

    ポリシー サーバは、ポリシー ストア、キー ストア、およびログ データベースとしてそのデータベースを使用するように設定されます。

SiteMinder スーパーユーザ パスワードの設定

デフォルトの SiteMinder 管理者アカウントの名前は siteminder です。このアカウントは最大の権限を持っています。その他の SiteMinder 管理者を作成できるまで SiteMinder のユーザ インターフェースとユーティリティの管理に使用できるように、このアカウントのパスワードを設定します。

注: smreg ユーティリティは、ポリシー サーバ インストール キットの最上位レベルにあります。

スーパーユーザのパスワードを設定する方法

1. smreg ユーティリティを *policy_server_home*¥bin にコピーします。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   `smreg -su password`

   重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

   password

   デフォルトの SiteMinder 管理者のパスワードを指定します。

   制限:

   - パスワードは 6 文字以上、24 文字以下である必要があります。
   - パスワードには、アンパサンド(&)またはアスタリスク(*)を含むことはできません。
   - パスワードにスペースが含まれている場合は、引用符でパスフレーズを囲みます。

   注: パスワードは、Oracle ポリシー ストアに保管する場合を除き、大文字小文字が区別されません。

3. *policy_server_home*¥bin から smreg ユーティリティを削除します。smreg を削除すると、既存のパスワードを把握していない限り、パスワードを変更することはできなくなります。

   デフォルトの SiteMinder 管理者アカウントのパスワードが設定されます。

注: 日常的な作業にはデフォルトのスーパーユーザを使用しないことをお勧めします。デフォルトのスーパーユーザは、以下の場合に使用してください。

- デフォルトのポリシー ストア オブジェクトをインポートする場合。
- FSS 管理 UI および 管理 UI に初めてアクセスする場合。スーパーユーザ権限を持つ別の管理者を作成することをお勧めします。

詳細情報:

インストール メディアの検索 (P. 236)

デフォルトのポリシー ストア オブジェクトのインポート

デフォルトのポリシー ストア オブジェクトをインポートすると、管理 UI で使用するポリシー ストアがセットアップされます。ポリシー ストアにポリシー情報を格納するには、デフォルトのポリシー ストア オブジェクトが必要です。

注: FIPS 専用モードでポリシー サーバをインストールした場合は、デフォルトのポリシー ストア オブジェクトをインポートするときに必ず -cf 引数を使用してください。

デフォルトのポリシー ストア オブジェクトをインポートする方法

1. 以下のコマンドを実行します。

   ```
   smobjimport -ipolicy_server_home¥db¥smdif¥smpolicy.smdif
   -dsiteminder_super_user_name -wsiteminder_super_user_password -v
   ```

   引数にスペースが含まれる場合、引数全体の前後に二重引用符を使用します。

   Windows の例: smobjimport

   ```
   -i"C:¥Program Files¥CA¥siteminder¥db¥smdif¥smpolicy.smdif" -d"SM Admin"
   -wPassword -v
   ```

   UNIX の例: smobjimport

   ```
   -i$NETE_PS_ROOT/db/smdif/smpolicy.smdif -d"SM Admin" -wPassword -v
   ```

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

   -d*siteminder_super_user_name*

   SiteMinder スーパーユーザ アカウントの名前を指定します。

   デフォルト: siteminder

-w*siteminder_super_user_password*

SiteMinder スーパーユーザ アカウントのパスワードを指定します。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト値: stdout

-cf

（任意）FIPS 対応の暗号化を使用して機密データをインポートします。

注: この引数は、ポリシー サーバが FIPS 専用モードで動作している場合にのみ必要です。

smobjimport によって、ポリシー ストア オブジェクトがインポートされます。オブジェクトは、適切な場所に自動的にインポートされます。

2. 以下のコマンドを実行します。

```
smobjimport -ipolicy_server_home¥db¥smdif¥ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

policy_server_home

ポリシー サーバのインストール パスを指定します。

-d*siteminder_super_user_name*

SiteMinder スーパーユーザ アカウントの名前を指定します。

デフォルト: siteminder

-w*siteminder_super_user_password*

SiteMinder スーパーユーザ アカウントのパスワードを指定します。

-f

重複するオブジェクトを上書きします。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト値: stdout

-l

ログ ファイルを作成します。

-c

smdif 入力ファイルに暗号化されていないデータが含まれていることを示します。

smobjimport によって、ポリシー ストア オブジェクトがインポートされます。これらのオブジェクトは、適切な場所に自動的にインポートされます。

注: ampolicy.smdif をインポートすると、Federation セキュリティ サービス、Web サービス変数、および eTelligent ルール機能が使用可能になります。eTelligent ルール機能は、SiteMinder から別個にライセンスが提供されます。この eTelligent ルール機能を使用する予定がある場合は、ライセンスの詳細について、CA アカウント担当者に問い合わせてください。

これで、ポリシー ストア データ定義をインポートできるようになりました。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*¥xps¥dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。

3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   必要なポリシー ストア データ定義がすべてインポートされました。

ポリシー サーバの再起動

ポリシー ストアやその他のデータ ストアの設定を有効にするために、ポリシー サーバを再起動します。

注: UNIX システムでは、stop-all コマンドの後に start-all コマンドを使用することで、ポリシー サーバを再起動できます。

ポリシー サーバを再起動するには、以下の手順に従います。

1. ポリシー サーバ管理コンソールを開きます。
2. [ステータス]タブをクリックし、[ポリシー サーバ]グループ ボックスで[停止]をクリックします。

   赤色の信号アイコンが表示されて、ポリシー サーバが停止します。
3. [開始]をクリックします。

   緑色の信号アイコンが表示されて、ポリシー サーバが起動します。

管理 UI 登録の準備

管理 UI に初めてログインする場合は、デフォルトの SiteMinder スーパーユーザ アカウント(siteminder)を使用します。 初めてログインするときは、ポリシー サーバに 管理 UI を登録する必要があります。これで、両方のコンポーネントの間に信頼関係が作成されます。

XPSRegClient ユーティリティを使用してスーパーユーザ アカウントの名前とパスワードを指定して、登録の準備をします。ポリシー サーバは、これらの認証情報を使用して、登録要求が有効であること、および信頼関係を確立できることを検証します。

以下の点について考慮してください。

- 認証情報を指定してから最初の 管理 UI ログインまでの時間は、24 時間に制限されています。24 時間以内に 管理 UI をインストールする予定がない場合は、管理 UI をインストールする前に以下を実行します。
- (UNIX) XPSRegClient を使用する前に、SiteMinder 環境変数が設定されていることを確認してください。環境変数が設定されていない場合は、手動で設定します。

管理 UI 登録を準備する方法

1. ポリシー サーバ ホスト システムにログインします。
2. 以下のコマンドを実行します。

   ```
   XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
   comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

   passphrase

   デフォルトの SiteMinder スーパーユーザ アカウント(siteminder)のパスワードを指定します。

   注: パスフレーズを指定しないと、XPSRegClient により、パスフレーズの入力とその確認を求めるプロンプトが表示されます。

   -adminui–setup

   管理 UI が初めてポリシー サーバに登録されていることを指定します。

-t *timeout*

(任意) 管理 UI をインストールしてから、ログインしてポリシー サーバとの信頼関係を作成するまでの割り当て時間を指定します。タイムアウト値を超過すると、ポリシー サーバは登録リクエストを拒否します。

測定単位: 分

デフォルト: 240 (4 時間)

最小制限: 1

最大制限: 1440 (24 時間)

-r *retries*

(任意) 管理 UI の登録時に許容される試行の失敗回数を指定します。試行に失敗する原因としては、初めて 管理 UI にログインするときに間違った SiteMinder 管理者クレデンシャルをサブミットしたことが考えられます。

デフォルト: 1

最大制限: 5

-c *comment*

(任意) 指定されたコメントを情報目的で登録ログ ファイルに挿入します。

注: コメントは引用符で囲んでください。

-cp

(任意) 登録ログ ファイルに複数行のコメントが含まれることを指定します。ユーティリティにより複数行のコメントが求められ、指定されたコメントが情報目的で登録ログ ファイルに挿入されます。

注: コメントは引用符で囲んでください。

-l *log path*

(任意) 登録ログ ファイルをエクスポートする場所を指定します。

デフォルト: *siteminder_home*¥log

siteminder_home

ポリシー サーバのインストール パスを指定します。

-e *error_path*

(任意) 例外を指定されたパスに送信します。

デフォルト: stderr

-vT

（任意）詳細レベルを TRACE に設定します。

-vI

（任意）詳細レベルを INFO に設定します。

-vW

（任意）詳細レベルを WARNING に設定します。

-vE

（任意）詳細レベルを ERROR に設定します。

-vF

（任意）詳細レベルを FATAL に設定します。

3. Enter キーを押します。

   XPSRegClient は、ポリシー サーバに管理者クレデンシャルを提供します。ポリシー サーバは、管理 UI への最初のログイン時に、登録リクエストを確認するためにこれらのクレデンシャルを使用します。

MySQL データ ストアの設定

SiteMinder キーおよび SiteMinder 監査情報はそれぞれ別のデータベースに格納できます。

以下の点について考慮してください。

- シングル サイン オン機能を実装するために、個別のデータベース内にキーを格納することが必要となる場合があります。キー管理の詳細については、「ポリシー サーバ管理ガイド」を参照してください。
- SiteMinder セッション情報は別のデータベースに格納される必要があります。セッション情報を格納するためにポリシー ストアを使用することはできません。

以下のセクションでは、個別のデータ ストアを設定する方法について詳しく説明します。

キー情報を MySQL に格納する方法

MySQL をスタンドアロン キーストアとして設定するには、以下の手順に従います。

1. MySQL が必ずデフォルト文字セット(Latin1)を使用してインストールされていることを確認します。MySQL がデフォルト文字セットを使用してインストールされていない場合、SiteMinder データ ストアを設定する前に MySQL を再インストールします。
2. SiteMinder スキーマ ファイルをダウンロードします。
3. データベース情報を収集します。
4. キー ストア スキーマを作成します。
5. SiteMinder 用の MySQL データ ソースを設定します。
6. ポリシー サーバがそのデータベースを参照するようにします。
7. ポリシー サーバを再起動します。

詳細情報:

データベース情報の収集 (P. 79)
SiteMinder 用の MySQL データ ソースの設定 (P. 83)

SiteMinder スキーマ ファイルのダウンロード

SiteMinder スキーマを設定するのに必要な 1 つ以上のスキーマ ファイルが、ポリシー サーバ インストールに含まれていません。これらのファイルは CA SiteMinder Tier 2 ディレクトリ製品コンポーネント ダウンロードにあります。

Tier 2 ディレクトリ製品コンポーネントをダウンロードする方法

1. テクニカル サポート サイトにログインします。
2. [Support]の下の[Download Center]をクリックします。

   [Download Center]画面が表示されます。
3. [Select a Product]フィールドに「SiteMinder」と入力します。
4. [Select a Release]リストからリリースを選択します。
5. [Select a Gen Level]リストからサービス パックを選択します。

6. ［Go］をクリックします。

   ［Product Downloads］画面が表示されます。Tier 2 ディレクトリ コンポーネント ダウンロードはリストの下のほうにあります。

7. zip ファイルをローカルに保存し、ポリシー サーバ ホスト システムにファイルを抽出します。

キー ストア スキーマの作成

MySQL データベースがキー情報を格納できるように、キー ストア スキーマを作成します。

キー ストア スキーマを作成する方法

1. *path*¥MySQL に移動します。

   path

   Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。

2. テキスト エディタに以下のファイルを開き、ファイル全体の内容をコピーします。

   sm_mysql_ps.sql

   注: ポリシー ストア スキーマ ファイルは、スタンドアロン キー ストアを作成するために使用されます。

3. クエリにファイルの内容を貼り付けて、クエリを実行します。

   キー ストア スキーマが作成されます。

ポリシー サーバに対する参照データベースの指定

ポリシー サーバが、キー情報を読み取りおよび保存できるように、ポリシー サーバに、参照するデータベースを指定します。

ポリシー サーバがデータ ストアを参照するようにする方法

1. ポリシー サーバ管理コンソールを開き、［データ］タブをクリックします。

   データベース設定が表示されます。

2. ［ストレージ］リストから［ODBC］を選択します。

   ODBC 設定が表示されます。

3. [データベース]リストから[キー ストア]を選択し、[ポリシーストアを使用]チェック ボックスをオフにします。

   データ ソース設定がアクティブになります。

4. [データ ソース情報]フィールドにデータ ソースの名前を入力します。

   - (Windows)このエントリは、データ ソースを作成したときに[データ ソース名]フィールドに入力した名前と一致する必要があります。
   - (UNIX)このエントリは、system_odbc.ini ファイルのデータ ソース エントリの最初の行と一致している必要があります。デフォルトでは、このファイルの最初の行は [SiteMinder Data Sources] です。最初のエントリを変更した場合は、正しい値を入力していることを確認します。

5. それぞれのフィールド内にデータベース インスタンスへのフル アクセス権限を持つデータベース アカウントのユーザ名およびパスワードを入力し確認します。

6. SiteMinder に割り当てるデータベース接続の最大数を指定します。

   注: 最適なパフォーマンスを得るためにデフォルトの設定を保持することを推奨します。

7. [適用]をクリックします。

   設定が保存されます。

8. [接続のテスト]をクリックします。

   SiteMinder によって、ポリシー サーバがデータ ストアにアクセスできるという確認が返されます。

9. [OK]をクリックします。

   ポリシー サーバはキー ストアとしてそのデータベースを使用するように設定されます。

ポリシー サーバの再起動

ポリシー ストアやその他のデータ ストアの設定を有効にするために、ポリシー サーバを再起動します。

注: UNIX システムでは、stop-all コマンドの後に start-all コマンドを使用することで、ポリシー サーバを再起動できます。

ポリシー サーバを再起動するには、以下の手順に従います。

1. ポリシー サーバ管理コンソールを開きます。
2. [ステータス]タブをクリックし、[ポリシー サーバ]グループ ボックスで[停止]をクリックします。

   赤色の信号アイコンが表示されて、ポリシー サーバが停止します。
3. [開始]をクリックします。

   緑色の信号アイコンが表示されて、ポリシー サーバが起動します。

監査ログを MySQL に格納する方法

MySQL をスタンドアロン監査ログ ストアとして設定するには、以下の手順に従います。

1. MySQL が必ずデフォルト文字セット(Latin1)を使用してインストールされていることを確認します。MySQL がデフォルト文字セットを使用してインストールされていない場合、SiteMinder データ ストアを設定する前に MySQL を再インストールします。
2. SiteMinder スキーマ ファイルをダウンロードします。
3. データベース情報を収集します。
4. 監査ログスキーマを作成します。
5. SiteMinder 用の MySQL データ ソースを設定します。
6. ポリシー サーバがそのデータベースを参照するようにします。
7. ポリシー サーバを再起動します。

詳細情報:

データベース情報の収集 (P. 79)
SiteMinder 用の MySQL データ ソースの設定 (P. 83)

SiteMinder スキーマ ファイルのダウンロード

SiteMinder スキーマを設定するのに必要な 1 つ以上のスキーマ ファイルが、ポリシー サーバ インストールに含まれていません。これらのファイルは CA SiteMinder Tier 2 ディレクトリ製品コンポーネント ダウンロードにあります。

Tier 2 ディレクトリ製品コンポーネントをダウンロードする方法

1. テクニカル サポート サイトにログインします。
2. [Support]の下の[Download Center]をクリックします。

   [Download Center]画面が表示されます。
3. [Select a Product]フィールドに「SiteMinder」と入力します。
4. [Select a Release]リストからリリースを選択します。
5. [Select a Gen Level]リストからサービス パックを選択します。
6. [Go]をクリックします。

   [Product Downloads]画面が表示されます。Tier 2 ディレクトリ コンポーネント ダウンロードはリストの下のほうにあります。
7. zip ファイルをローカルに保存し、ポリシー サーバ ホスト システムにファイルを抽出します。

監査ログスキーマの作成

MySQL データベースが監査ログを格納できるように、監査ログ スキーマを作成します。

監査ログ スキーマを作成する方法

1. *path*¥MySQL に移動します。

   path

   Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。
2. テキスト エディタに以下のファイルを開き、ファイル全体の内容をコピーします。

   sm_mysql_logs.sql
3. クエリにファイルの内容を貼り付けて、クエリを実行します。

   監査ログ スキーマが作成されます。

ポリシー サーバに対する参照データベースの指定

ポリシー サーバが、監査ログを読み取りおよび保存できるように、ポリシー サーバに、参照するデータベースを指定します。

ポリシー サーバがデータ ストアを参照するようにする方法

1. ポリシー サーバ管理コンソールを開き、[データ]タブをクリックします。

   データベース設定が表示されます。

2. [ストレージ]リストから[ODBC]を選択します。

   ODBC 設定が表示されます。

3. [データベース]リストから[監査ログ]を選択します。

4. [ストレージ]リストから[ODBC]を選択します。

   データ ソース設定がアクティブになります。

5. [データ ソース情報]フィールドにデータ ソースの名前を入力します。

   - (Windows)このエントリは、データ ソースを作成したときに[データ ソース名]フィールドに入力した名前と一致する必要があります。
   - (UNIX)このエントリは、system_odbc.ini ファイルのデータ ソース エントリの最初の行と一致している必要があります。デフォルトでは、このファイルの最初の行は [SiteMinder Data Sources] です。最初のエントリを変更した場合は、正しい値を入力していることを確認します。

6. それぞれのフィールド内にデータベース インスタンスへのフル アクセス権限を持つデータベース アカウントのユーザ名およびパスワードを入力し確認します。

7. SiteMinder に割り当てるデータベース接続の最大数を指定します。

   注: 最適なパフォーマンスを得るためにデフォルトの設定を保持することを推奨します。

8. [適用]をクリックします。

   設定が保存されます。

9. [接続のテスト]をクリックします。

   SiteMinder によって、ポリシー サーバがデータ ストアにアクセスできるという確認が返されます。

10. [OK]をクリックします。

    ポリシー サーバは監査ログ データベースとしてそのデータベースを使用するように設定されます。

ポリシー サーバの再起動

ポリシー ストアやその他のデータ ストアの設定を有効にするために、ポリシー サーバを再起動します。

注: UNIX システムでは、stop-all コマンドの後に start-all コマンドを使用することで、ポリシー サーバを再起動できます。

ポリシー サーバを再起動するには、以下の手順に従います。

1. ポリシー サーバ管理コンソールを開きます。
2. [ステータス]タブをクリックし、[ポリシー サーバ]グループ ボックスで[停止]をクリックします。

   赤色の信号アイコンが表示されて、ポリシー サーバが停止します。

3. [開始]をクリックします。

   緑色の信号アイコンが表示されて、ポリシー サーバが起動します。

セッション情報を MySQL に格納する方法

MySQL をスタンドアロン セッション ストアとして設定するには、以下の手順に従います。

1. MySQL が必ずデフォルト文字セット(Latin1)を使用してインストールされていることを確認します。MySQL がデフォルト文字セットを使用してインストールされていない場合、SiteMinder データ ストアを設定する前に MySQL を再インストールします。
2. SiteMinder スキーマ ファイルをダウンロードします。
3. データベース情報を収集します。
4. セッション ストア スキーマを作成します。
5. SiteMinder 用の MySQL データ ソースを設定します。

6. ポリシー サーバがそのデータベースを参照するようにします。
7. ポリシー サーバを再起動します。

詳細情報:

データベース情報の収集 (P. 79)
SiteMinder 用の MySQL データ ソースの設定 (P. 83)

SiteMinder スキーマ ファイルのダウンロード

SiteMinder スキーマを設定するのに必要な 1 つ以上のスキーマ ファイルが、ポリシー サーバ インストールに含まれていません。これらのファイルは CA SiteMinder Tier 2 ディレクトリ製品コンポーネント ダウンロードにあります。

Tier 2 ディレクトリ製品コンポーネントをダウンロードする方法

1. テクニカル サポート サイトにログインします。
2. [Support]の下の[Download Center]をクリックします。

   [Download Center]画面が表示されます。
3. [Select a Product]フィールドに「SiteMinder」と入力します。
4. [Select a Release]リストからリリースを選択します。
5. [Select a Gen Level]リストからサービス パックを選択します。
6. [Go]をクリックします。

   [Product Downloads]画面が表示されます。Tier 2 ディレクトリ コンポーネント ダウンロードはリストの下のほうにあります。
7. zip ファイルをローカルに保存し、ポリシー サーバ ホスト システムにファイルを抽出します。

セッション ストア スキーマの作成

MySQL データベースがセッション情報を格納できるように、セッション ストア スキーマを作成します。

監査ログ スキーマを作成する方法

1. *path*¥MySQL に移動します。

   path

   Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。

2. テキスト エディタに以下のファイルを開き、ファイル全体の内容をコピーします。

   sm_mysql_ss.sql

3. クエリにファイルの内容を貼り付けて、クエリを実行します。

   セッション ストア スキーマが作成されます。

ポリシー サーバに対する参照データベースの指定

ポリシー サーバが、セッション情報を読み取りおよび保存できるように、ポリシー サーバに、参照するデータベースを指定します。

ポリシー サーバがデータ ストアを参照するようにする方法

1. ポリシー サーバ管理コンソールを開き、[データ]タブをクリックします。

   データベース設定が表示されます。

2. [データベース]リストからセッション サーバを選択します。

   データ ソース設定がアクティブになります。

3. [データ ソース情報]フィールドにデータ ソースの名前を入力します。

   - (Windows)このエントリは、データ ソースを作成したときに[データ ソース名]フィールドに入力した名前と一致する必要があります。
   - (UNIX)このエントリは、system_odbc.ini ファイルのデータ ソース エントリの最初の行と一致している必要があります。デフォルトでは、このファイルの最初の行は [SiteMinder Data Sources] です。最初のエントリを変更した場合は、正しい値を入力していることを確認します。

4. それぞれのフィールド内にデータベース インスタンスへのフル アクセス権限を持つデータベース アカウントのユーザ名およびパスワードを入力し確認します。
5. SiteMinder に割り当てるデータベース接続の最大数を指定します。

   注: 最適なパフォーマンスを得るためにデフォルトの設定を保持することを推奨します。
6. [適用]をクリックします。

   設定が保存されます。
7. [接続のテスト]をクリックします。

   SiteMinder によって、ポリシー サーバがデータ ストアにアクセスできるという確認が返されます。
8. [OK]をクリックします。

   ポリシー サーバはセッション ストアとしてそのデータベースを使用するように設定されます。

ポリシー サーバの再起動

ポリシー ストアやその他のデータ ストアの設定を有効にするために、ポリシー サーバを再起動します。

注: UNIX システムでは、stop-all コマンドの後に start-all コマンドを使用することで、ポリシー サーバを再起動できます。

ポリシー サーバを再起動するには、以下の手順に従います。

1. ポリシー サーバ管理コンソールを開きます。
2. [ステータス]タブをクリックし、[ポリシー サーバ]グループ ボックスで[停止]をクリックします。

   赤色の信号アイコンが表示されて、ポリシー サーバが停止します。
3. [開始]をクリックします。

   緑色の信号アイコンが表示されて、ポリシー サーバが起動します。

MySQL ユーザ ストアを設定する方法

MySQL をユーザ ストアとして設定するには、以下の手順に従います。

1. （任意）SiteMinder サンプル ユーザをインポートします。
2. SiteMinder の MySQL データ ソースを作成します。
3. ユーザ ディレクトリ接続を設定します。

詳細情報:

SiteMinder 用の MySQL データ ソースの設定 (P. 83)

SiteMinder サンプル ユーザのインポート

SiteMinder サンプル ユーザのインポートは任意です。これらのユーザをインポートすると、データベースに架空の SiteMinder ユーザが入力されます。

SiteMinder サンプル ユーザをインポートする方法

1. *path*¥MySQL に移動します。

   path

   Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。

2. テキスト エディタに以下のファイルを開き、ファイル全体の内容をコピーします。

   smsampleusers_mysql.sql

3. クエリにファイルの内容を貼り付けて、クエリを実行します。

   サンプル ユーザがデータベースにインポートされます。

MySQL サーバ ディレクトリ接続の設定

ポリシー サーバから MySQL サーバ ユーザ ストアへの接続を設定するには、新規のユーザ ディレクトリ オブジェクトを作成します。

ポリシー サーバから MySQL サーバ ユーザ ストアへの接続を設定する方法

1. ［インフラストラクチャ］-［ディレクトリ］をクリックします。

2. [ユーザ ディレクトリ]、[ユーザ ディレクトリの作成]をクリックします。

   [ユーザ ディレクトリの作成]ペインが表示されます。

   注: このペインで、ユーザ ディレクトリのプロパティを指定できます。フィールド、設定、およびオプションの詳細については、[ヘルプ]をクリックしてください。

3. [一般]グループ ボックスのフィールドに、新規のユーザ ディレクトリ オブジェクトの名前と説明を入力します。

4. [ネームスペース]リストから[ODBC]を選択し、[ディレクトリのセットアップ]グループ ボックスの[データ ソース]フィールドに、データ ソース名を入力します。

5. [認証情報が必要]チェック ボックスをオンにし、[管理者認証情報]グループ ボックスのフィールドに管理者の完全 DN とパスワードを入力します。

6. [SQL クエリ方式]グループ ボックスの[SQL クエリ方式]リストから、クエリ方式を選択します。

7. (省略可)[ユーザ属性]グループ ボックスのフィールドに入力します。

   a. [ユニバーサル ID]フィールドにユニバーサル ID を入力します。

      属性タイプ: 文字列

   b. [無効フラグ]フィールドに、無効なユーザを追跡するフラグを入力します。

      属性タイプ: 文字列

   c. [パスワード]フィールドに、ユーザ パスワードのロケーションを入力します。

      属性タイプ: バイナリ

   d. [パスワード データ]フィールドに、ユーザ パスワード履歴のロケーションを入力します。

      属性タイプ: バイナリ

      注: この属性は、パスワード サービスに必要です。

   e. [匿名 ID]フィールドに、ユーザの匿名 ID を入力します。

      属性タイプ: 文字列

   f. [電子メール]フィールドは空のままにしておきます。

      注: 電子メール機能は、SiteMinder の現行バージョンには実装されていません。

g. [チャレンジ/レスポンス]フィールドに、レスポンスを入力します。

属性タイプ: 文字列

注: この文字列は、各チャレンジ後にユーザに送信されます。

8. (省略可)[属性マッピング リスト]グループ ボックスで[作成]をクリックします。

[属性マッピングの作成]ペインが開きます。

注: ユーザ属性マッピングの詳細については、「ポリシー サーバ設定ガイド」を参照してください。

9. [サブミット]をクリックします。

ユーザ ディレクトリの作成タスクが処理のためにサブミットされます。

第 7 章: Novell eDirectory

このセクションには、以下のトピックが含まれています。

ポリシー ストアとしての Novell eDirectory

Windows または UNIX システムのいずれかにインストールされたポリシー サーバは、Novell eDirectory をポリシー ストアとして使用することができます。

作業を始める前に、以下がインストールされていることを確認してください。

- Novell eDirectory
- Novell Windows Login Client
- Novell ConsoleOne for Windows、UNIX、および Netware システム

以下のセクションでは、ポリシー ストアとしてディレクトリ サーバを設定する方法について詳しく説明します。

ディレクトリ サーバ情報の収集

LDAP ディレクトリ サーバをポリシー ストアとして設定するか、または既存のポリシー ストアをアップグレードするには、特定のディレクトリ サーバ情報が必要です。作業を始める前に、以下の情報を収集してください。値を記録するためにポリシー ストアのワークシートを使用できます。

注: ポリシー ストアおよびデータ ストアの各ワークシートが用意されているので、SiteMinder データ ストアを設定またはアップグレードする前の情報の収集および記録に使用することができます。作業を始める前に、該当するワークシートを印刷し、そのワークシートに必要な情報を記録しておくことができます。

ホスト情報

ディレクトリ サーバの完全修飾ホスト名または IP アドレスを指定します。

ポート情報

(任意)標準以外のポートを指定します。

デフォルト値: 636(SSL)および 389(SSL 以外)

管理 DN

LDAP ツリー内のポリシー ストア ルート オブジェクトの下でオブジェクトの作成、読み取り、変更、および削除を行う権限を持つユーザの LDAP ユーザ名を指定します。

管理パスワード

管理 DN のパスワードを指定します。

ポリシー サーバのルート DN

ポリシー ストア オブジェクトを定義する、LDAP ツリー内のノードの識別名を指定します。

SSL クライアント証明書

SSL クライアント証明書データベース ファイルがあるディレクトリのパス名を指定します。

制限: SSL のみ

ポリシー ストアを設定する方法

Novell eDirectory をポリシー ストアとして設定するには、以下の手順に従います。

1. ポリシー ストア スキーマ ファイルの編集
2. Novell XPS スキーマ ファイルの編集
3. ポリシー サーバからポリシー ストアへの参照の設定
4. SiteMinder スーパーユーザ パスワードの設定

   注: SiteMinder スーパーユーザ パスワードがすでにある場合は、この手順を実行する必要はありません。
5. ポリシー ストア スキーマの作成
6. デフォルトのポリシー ストア オブジェクトのインポート
7. ポリシー ストア データ定義のインポート

8. LDAP サーバのリフレッシュ
9. ポリシー サーバの再起動
10. 管理 UI 登録の準備

ポリシー ストア スキーマ ファイルの編集

Novell サーバ DN 情報を格納するように、Novell ポリシー ストア スキーマ ファイルを編集します。Novell Client から、Novell ポリシー ストア スキーマ ファイルを編集します。

ポリシー ストア スキーマ ファイルを編集する方法

1. ポリシー サーバ ホスト システム上の *policy_server_home*¥bin に移動します。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   ```
   ldapsearch -h host -p port -b container -s sub -d AdminDN -w AdminPW
   objectclass=ncpServer dn
   ```

   例:

   ```
   ldapsearch -h192.168.1.47 -p389 -bo=nwqa47container -ssub
   -dcn=admin,o=nwqa47container -wpassword objectclass=ncpServer dn
   ```

   Novell サーバ DN が表示されます。

3. Novell ポリシー ストア スキーマ ファイルを開きます。

   policy_server_home¥novell¥Novell_ADD_SMR12sp3.ldif

4. 各 NCP_Server 変数を、手順 2 で確認した Novell サーバ DN の値に置き換えることによって、開いている LDIF ファイルを手動で編集します。

   例: Novell サーバ DN の値が cn=servername,o=servercontainer の場合は、NCP_Server の各インスタンスを cn=servername,o=servercontainer に置き換えます。

5. LDIF ファイルを保存して閉じます。

   Novell ポリシー ストア スキーマ ファイルに、Novell サーバ DN 情報が格納されます。

Novell XPS スキーマ ファイルの編集

Novell サーバ DN の適切な情報を格納するように、Novell XPS スキーマ ファイル Novell.ldif を編集します。Novell Client から Novell XPS スキーマ ファイルを編集します。

Novell XPS スキーマ ファイルを編集する方法

1. ポリシー サーバがインストールされているマシン上の、*policy_server_home*¥bin または *policy_server_home*/bin に移動します。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   ```
   ldapsearch -hhost -pport -bcontainer -ssub -dAdminDN -wAdminPW
   objectclass=ncpServer dn
   ```

   例:

   ```
   ldapsearch -h192.168.1.47 -p389 -bo=nwqa47container -ssub
   -dcn=admin,o=nwqa47container -wpassword objectclass=ncpServer dn
   ```

   Novell サーバ DN が表示されます。

3. Novell XPS スキーマ ファイルを開きます。

   policy_server_home¥xps¥db¥Novell.ldif

4. 各 NCP_Server 変数を、手順 2 で確認した Novell サーバ DN の値に置き換えることによって、開いている XPS ファイルを手動で編集します。

   例: Novell サーバ DN の値が cn=servername,o=servercontainer の場合は、NCP_Server の各インスタンスを cn=servername,o=servercontainer に置き換えます。

5. XPS ファイルを保存して閉じます。

   Novell XPS スキーマ ファイルに、Novell サーバ DN の情報が格納されます。

ポリシー サーバからポリシー ストアへの参照の設定

ポリシー サーバからポリシー ストアへの参照を設定し、ポリシー サーバがポリシー ストアにアクセスできるようにします。

ポリシー サーバからポリシー ストアへの参照を設定する方法

1. ポリシー サーバ管理コンソールを開きます。

   重要: Windows Server 2008 上でこのグラフィカル ユーザ インターフェースにアクセスする場合は、管理者としてシステムにログインしている場合でも、管理者権限でショートカットを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

2. [データ]タブをクリックします。

   データベース設定が表示されます。

3. [データベース]リストから[ポリシー ストア]を選択します。

4. [ストレージ]リストから[LDAP]を選択します。

5. [LDAP ポリシー ストア]グループ ボックスで、以下を設定します。

   - LDAP IP アドレス
   - 管理者ユーザ名
   - パスワード
   - パスワードの確認
   - DN

   注: フィールド、コントロール、およびそれぞれの要件については、[ヘルプ]をクリックしてください。

6. [適用]をクリックします。

   ポリシー ストアの設定が保存されます。

7. [LDAP 接続のテスト]をクリックします。

   SiteMinder は、ポリシー サーバがポリシー ストアにアクセスできることを示す確認を返します。

ポリシー ストア スキーマの作成

ポリシー ストアおよびストア SiteMinder オブジェクトとしてディレクトリ サーバが機能できるように、ポリシー ストア スキーマを作成します。smldapsetup ツールを使用して、ポリシー ストア スキーマを追加します。

ポリシー ストア スキーマを作成する方法

1. コマンド プロンプトを開き、*policy_server_home*¥bin または *policy_server_home*/bin に移動します。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   ```
   smldapsetup ldmod -v
   -fpolicy_server_home/novell/Novell_Add_SMR12sp3.ldif
   ```

   -v

   トレースをオンにして、エラー メッセージ、警告メッセージ、およびコメント メッセージを出力します。

   -f

   r12.0 SP3 で提供されるスキーマ ファイルの名前を指定します。

3. 以下のコマンドを実行します。

   ```
   smldapsetup ldmod -v -fpolicy_server_home¥xps¥db¥Novell.ldif
   ```

   -f

   r12.0 SP3 で提供される XPS スキーマ ファイルのパスおよび名前を指定します。

   r12.0 SP3 に対するポリシー ストア スキーマが作成されます。

SiteMinder スーパーユーザ パスワードの設定

デフォルトの SiteMinder 管理者アカウントの名前は siteminder です。このアカウントは最大の権限を持っています。その他の SiteMinder 管理者を作成できるまで SiteMinder のユーザ インターフェースとユーティリティの管理に使用できるように、このアカウントのパスワードを設定します。

注: smreg ユーティリティは、ポリシー サーバ インストール キットの最上位レベルにあります。

スーパーユーザのパスワードを設定する方法

1. smreg ユーティリティを *policy_server_home*¥bin にコピーします。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   `smreg -su` *password*

   重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

   password

   デフォルトの SiteMinder 管理者のパスワードを指定します。

   制限:

   - パスワードは 6 文字以上、24 文字以下である必要があります。
   - パスワードには、アンパサンド(&)またはアスタリスク(*)を含むことはできません。
   - パスワードにスペースが含まれている場合は、引用符でパスフレーズを囲みます。

   注: パスワードは、Oracle ポリシー ストアに保管する場合を除き、大文字小文字が区別されません。

3. *policy_server_home*¥bin から smreg ユーティリティを削除します。smreg を削除すると、既存のパスワードを把握していない限り、パスワードを変更することはできなくなります。

   デフォルトの SiteMinder 管理者アカウントのパスワードが設定されます。

注: 日常的な作業にはデフォルトのスーパーユーザを使用しないことをお勧めします。デフォルトのスーパーユーザは、以下の場合に使用してください。

- デフォルトのポリシー ストア オブジェクトをインポートする場合。
- FSS 管理 UI および 管理 UI に初めてアクセスする場合。スーパーユーザ権限を持つ別の管理者を作成することをお勧めします。

詳細情報:

インストール メディアの検索 (P. 236)

デフォルトのポリシー ストア オブジェクトのインポート

デフォルトのポリシー ストア オブジェクトをインポートすると、管理 UI で使用するポリシー ストアがセットアップされます。ポリシー ストアにポリシー情報を格納するには、デフォルトのポリシー ストア オブジェクトが必要です。

注: FIPS 専用モードでポリシー サーバをインストールした場合は、デフォルトのポリシー ストア オブジェクトをインポートするときに必ず -cf 引数を使用してください。

デフォルトのポリシー ストア オブジェクトをインポートする方法

1. 以下のコマンドを実行します。

   ```
   smobjimport -ipolicy_server_home¥db¥smdif¥smpolicy.smdif
   -dsiteminder_super_user_name -wsiteminder_super_user_password -v
   ```

   引数にスペースが含まれる場合、引数全体の前後に二重引用符を使用します。

   Windows の例: smobjimport

   ```
   -i"C:¥Program Files¥CA¥siteminder¥db¥smdif¥smpolicy.smdif" -d"SM Admin"
   -wPassword -v
   ```

   UNIX の例: smobjimport

   ```
   -i$NETE_PS_ROOT/db/smdif/smpolicy.smdif -d"SM Admin" -wPassword -v
   ```

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

   -d*siteminder_super_user_name*

   SiteMinder スーパーユーザ アカウントの名前を指定します。

   デフォルト: siteminder

-w*siteminder_super_user_password*

SiteMinder スーパーユーザ アカウントのパスワードを指定します。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト値: stdout

-cf

(任意) FIPS 対応の暗号化を使用して機密データをインポートします。

注: この引数は、ポリシー サーバが FIPS 専用モードで動作している場合にのみ必要です。

smobjimport によって、ポリシー ストア オブジェクトがインポートされます。オブジェクトは、適切な場所に自動的にインポートされます。

2. 以下のコマンドを実行します。

```
smobjimport -ipolicy_server_home¥db¥smdif¥ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

policy_server_home

ポリシー サーバのインストール パスを指定します。

-d*siteminder_super_user_name*

SiteMinder スーパーユーザ アカウントの名前を指定します。

デフォルト: siteminder

-w*siteminder_super_user_password*

SiteMinder スーパーユーザ アカウントのパスワードを指定します。

-f

重複するオブジェクトを上書きします。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト値: stdout

-l

ログ ファイルを作成します。

-c

smdif 入力ファイルに暗号化されていないデータが含まれていることを示します。

smobjimport によって、ポリシー ストア オブジェクトがインポートされます。これらのオブジェクトは、適切な場所に自動的にインポートされます。

注: ampolicy.smdif をインポートすると、Federation セキュリティ サービス、Web サービス変数、および eTelligent ルール機能が使用可能になります。eTelligent ルール機能は、SiteMinder から別個にライセンスが提供されます。この eTelligent ルール機能を使用する予定がある場合は、ライセンスの詳細について、CA アカウント担当者に問い合わせてください。

これで、ポリシー ストア データ定義をインポートできるようになりました。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*¥xps¥dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。

3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   必要なポリシー ストア データ定義がすべてインポートされました。

LDAP サーバのリフレッシュ

変更が Novell eDirectory で有効になるように、LDAP サーバをリフレッシュします。LDAP サーバをリフレッシュするには、Novell Client を使用します。

LDAP サーバをリフレッシュする方法

1. ConsoleOne を開きます。
2. ディレクトリ ツリーで LDAP サーバをダブルクリックします。
3. [LDAP サーバを今すぐリフレッシュ]をクリックします。

   LDAP サーバがリフレッシュされます。

ポリシー サーバの再起動

ポリシー ストアやその他のデータ ストアの設定を有効にするために、ポリシー サーバを再起動します。

注: UNIX システムでは、stop-all コマンドの後に start-all コマンドを使用することで、ポリシー サーバを再起動できます。

ポリシー サーバを再起動するには、以下の手順に従います。

1. ポリシー サーバ管理コンソールを開きます。
2. [ステータス]タブをクリックし、[ポリシー サーバ]グループ ボックスで[停止]をクリックします。

   赤色の信号アイコンが表示されて、ポリシー サーバが停止します。
3. [開始]をクリックします。

   緑色の信号アイコンが表示されて、ポリシー サーバが起動します。

管理 UI 登録の準備

管理 UI に初めてログインする場合は、デフォルトの SiteMinder スーパーユーザ アカウント(siteminder)を使用します。初めてログインするときは、ポリシー サーバに 管理 UI を登録する必要があります。これで、両方のコンポーネントの間に信頼関係が作成されます。

XPSRegClient ユーティリティを使用してスーパーユーザ アカウントの名前とパスワードを指定して、登録の準備をします。ポリシー サーバは、これらの認証情報を使用して、登録要求が有効であること、および信頼関係を確立できることを検証します。

以下の点について考慮してください。

- 認証情報を指定してから最初の 管理 UI ログインまでの時間は、24 時間に制限されています。24 時間以内に 管理 UI をインストールする予定がない場合は、管理 UI をインストールする前に以下を実行します。
- (UNIX) XPSRegClient を使用する前に、SiteMinder 環境変数が設定されていることを確認してください。環境変数が設定されていない場合は、手動で設定します。

管理 UI 登録を準備する方法

1. ポリシー サーバ ホスト システムにログインします。
2. 以下のコマンドを実行します。

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

デフォルトの SiteMinder スーパーユーザ アカウント（siteminder）のパスワードを指定します。

注：パスフレーズを指定しないと、XPSRegClient により、パスフレーズの入力とその確認を求めるプロンプトが表示されます。

-adminui–setup

管理 UI が初めてポリシー サーバに登録されていることを指定します。

-t *timeout*

（任意）管理 UI をインストールしてから、ログインしてポリシー サーバとの信頼関係を作成するまでの割り当て時間を指定します。タイムアウト値を超過すると、ポリシー サーバは登録リクエストを拒否します。

測定単位： 分

デフォルト： 240（4 時間）

最小制限： 1

最大制限： 1440（24 時間）

-r *retries*

（任意）管理 UI の登録時に許容される試行の失敗回数を指定します。試行に失敗する原因としては、初めて 管理 UI にログインするときに間違った SiteMinder 管理者クレデンシャルをサブミットしたことが考えられます。

デフォルト： 1

最大制限： 5

-c *comment*

（任意）指定されたコメントを情報目的で登録ログ ファイルに挿入します。

注：コメントは引用符で囲んでください。

-cp

（任意）登録ログ ファイルに複数行のコメントが含まれることを指定します。ユーティリティにより複数行のコメントが求められ、指定されたコメントが情報目的で登録ログ ファイルに挿入されます。

注: コメントは引用符で囲んでください。

-l *log path*

（任意）登録ログ ファイルをエクスポートする場所を指定します。

デフォルト: *siteminder_home*¥log

siteminder_home

ポリシー サーバのインストール パスを指定します。

-e *error_path*

（任意）例外を指定されたパスに送信します。

デフォルト: stderr

-vT

（任意）詳細レベルを TRACE に設定します。

-vI

（任意）詳細レベルを INFO に設定します。

-vW

（任意）詳細レベルを WARNING に設定します。

-vE

（任意）詳細レベルを ERROR に設定します。

-vF

（任意）詳細レベルを FATAL に設定します。

3. Enter キーを押します。

XPSRegClient は、ポリシー サーバに管理者クレデンシャルを提供します。ポリシー サーバは、管理 UI への最初のログイン時に、登録リクエストを確認するためにこれらのクレデンシャルを使用します。

Novell eDirectory でのポリシー ストア オブジェクトの制限

Novell eDirectory でポリシー ストア オブジェクトを使用する場合は、以下の点を考慮してください。

- ポリシー ストアが Novell eDirectory にある場合、eDirectory では属性を 64 文字を超える値に設定できないため、ポリシー ストア オブジェクトに 64 文字より長い名前を付けることはできません。これは、特に証明書マップに影響します。通常、証明書マップには意図的に長い名前が付けられています。
- ポリシー サーバは、Novell eDirectory にあるポリシー ストアの LDAP リフェラルをサポートしていません。

6.x ポリシー ストアをアップグレードする方法

r12.0 SP3 ポリシー ストアに、新規のディレクトリ サーバ インスタンスは必要ありません。既存のポリシー ストアを r12.0 SP3 にアップグレードできます。

サポートされている LDAP またはリレーショナル データベースのポリシー ストアをアップグレードするには、以下の手順に従います。

1. Novell XPS スキーマ ファイルを編集します。
2. ポリシー ストア スキーマを拡張します。

   注:既存の r6.x ポリシー ストア スキーマは、変更されていません。r12.0 SP3 の移行では、ポリシー ストア スキーマをアップグレードして、r12.0 SP3 によって必要とされるオブジェクトのポリシー ストアを拡張する必要があります。
3. ベース ポリシー ストア オブジェクトをインポートします。
4. ポリシー ストア データ定義をインポートします。

注: 本書には記載されていないけれども、サポート マトリックスにはリストされているディレクトリ サーバまたはデータベースをアップグレードする場合は、以下の該当するガイドを参照してください。

- *ポリシー サーバ設定ガイド*
- *ポリシー サーバ インストール ガイド*
- *アップグレード ガイド*

Novell XPS スキーマ ファイルの編集

Novell サーバ DN の適切な情報を格納するように、Novell XPS スキーマ ファイル Novell.ldif を編集します。Novell Client から Novell XPS スキーマ ファイルを編集します。

Novell XPS スキーマ ファイルを編集する方法

1. ポリシー サーバがインストールされているマシン上の、*policy_server_home*¥bin または *policy_server_home*/bin に移動します。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   ```
   ldapsearch -hhost -pport -bcontainer -ssub -dAdminDN -wAdminPW
   objectclass=ncpServer dn
   ```

   例:

   ```
   ldapsearch -h192.168.1.47 -p389 -bo=nwqa47container -ssub
   -dcn=admin,o=nwqa47container -wpassword objectclass=ncpServer dn
   ```

   Novell サーバ DN が表示されます。

3. Novell XPS スキーマ ファイルを開きます。

   policy_server_home¥xps¥db¥Novell.ldif

4. 各 NCP_Server 変数を、手順 2 で確認した Novell サーバ DN の値に置き換えることによって、開いている XPS ファイルを手動で編集します。

   例: Novell サーバ DN の値が cn=servername,o=servercontainer の場合は、NCP_Server の各インスタンスを cn=servername,o=servercontainer に置き換えます。

5. XPS ファイルを保存して閉じます。

   Novell XPS スキーマ ファイルに、Novell サーバ DN の情報が格納されます。

Novell ポリシー ストア スキーマの拡張

r12.0 SP3 によって導入されたオブジェクトを含めるように Novell 6.0 ポリシー ストア スキーマを拡張することができます。既存の 6.0 ポリシー ストア スキーマまたはデータに加える変更はありません。

Novell ポリシー ストア スキーマを拡張する方法

以下のコマンドを実行します。

```
smldapsetup ldmod -fpolicy_server_home/xps/db/Novell.ldif
```

-f

r12.0 SP3 で提供される XPS スキーマ ファイルのパスおよび名前を指定します。

policy_server_home

ポリシー サーバのインストール パスを指定します。

r12.0 SP3 によって導入されたオブジェクトを含めるようにポリシー ストア スキーマが拡張されます。

注: これで、ポリシー ストア データ定義をインポートできます。

ベース ポリシー ストア オブジェクトのインポート

デフォルトの SiteMinder オブジェクトをインポートすると、管理 UI で使用するポリシー ストアがアップグレードされます。デフォルトの SiteMinder オブジェクトは、ポリシー ストアにポリシー情報を格納するために必要です。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. 以下のコマンドを実行します。

```
smobjimport -ipolicy_server_home¥db¥smdif¥upgrade_smdif_file_name
-dsiteminder_super_user_name -wsiteminder_super_user_password
-v -f
```

policy_server_home

ポリシー サーバのインストール パスを指定します。

upgrade_smdif_file_name

インポート ファイルの名前を指定します。

- **r60 から r12.0 SP3:** sm_upgrade_60_to_R12sp3.smdif
- **r60 SP1 から r12.0 SP3:** sm_upgrade_60sp1_to_R12sp3.smdif
- **r60 SP2 から r12.0 SP3:** sm_upgrade_60sp2_to_R12sp3.smdif
- **r60 SP3 から r12.0 SP3:** sm_upgrade_60sp3_to_R12sp3.smdif
- **r60 SP4 から r12.0 SP3:** sm_upgrade_60sp4_to_R12sp3.smdif
- **r60 SP5 から r12.0 SP3:** sm_upgrade_60sp5_to_R12sp3.smdif
- **r60 SP6 から r12.0 SP3:** sm_upgrade_60sp6_to_r12sp3.smdif

-d*siteminder_super_user_name*

SiteMinder 管理者アカウントの名前を指定します。

-w*siteminder_super_user_password*

SiteMinder 管理者アカウントのパスワードを指定します。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト出力: stdout

-f

重複するポリシー ストア オブジェクトを、r12.0 SP3 のもので上書きします。

引数にスペースが含まれる場合、引数全体の前後に二重引用符を使用します。

Windows の例: smobjimport

```
-i"C:¥Program Files¥CA¥siteminder¥db¥smdif¥smpolicy.smdif" -d"SM Admin"
-wPassword -v
```

UNIX の例: smobjimport

-i$NETE_PS_ROOT/db/smdif/smpolicy.smdif -d"SM Admin" -wPassword -v

ベース ポリシー ストア オブジェクトがインポートされます。

2. 以下のコマンドを実行します。

   重要: ampolicy.smdif が以前にポリシー ストアにインポートされている場合は再インポートしないでください。

   ```
   smobjimport -ipolicy_server_home¥db¥smdif¥ampolicy.smdif
   -dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
   ```

   -policy_server_home

   インポート ファイルのパスと名前を指定します。

   -d*siteminder_super_user_name*

   SiteMinder 管理者アカウントの名前を指定します。

   -w*siteminder_super_user_password*

   SiteMinder 管理者アカウントのパスワードを指定します。

   -f

   重複するオブジェクトを上書きします。

   -v

   追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

   デフォルト値: stdout

   -l

   ログ ファイルを作成します。

   -c

   smdif 入力ファイルに暗号化されていないデータが含まれていることを示します。

   注: ampolicy.smdif をインポートすると、SiteMinder から別々にライセンスされるフェデレーション セキュリティ サービス、Web サービス変数、および eTelligent ルール機能が使用可能になります。eTelligent ルール機能を使用する予定の場合は、ライセンス情報について CA ジャパン ダイレクトに問い合わせてください。

これで、ポリシー ストア データ定義をインポートできるようになりました。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*¥xps¥dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。
2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。
3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。
4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。
5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   必要なポリシー ストア データ定義がすべてインポートされました。

第 8 章: Oracle Internet Directory Server

このセクションには、以下のトピックが含まれています。

ポリシー ストアとしての Oracle Internet Directory

Windows および UNIX システムにインストールされたポリシー サーバは、Oracle Internet Directory (OID) をポリシー ストアとして使用することができます。以下のセクションで、OID をポリシー ストアとして設定する方法を詳しく説明します。

ディレクトリ サーバ情報の収集

LDAP ディレクトリ サーバをポリシー ストアとして設定するか、または既存のポリシー ストアをアップグレードするには、特定のディレクトリ サーバ情報が必要です。作業を始める前に、以下の情報を収集してください。値を記録するためにポリシー ストアのワークシートを使用できます。

注: ポリシー ストアおよびデータ ストアの各ワークシートが用意されているので、SiteMinder データ ストアを設定またはアップグレードする前の情報の収集および記録に使用することができます。作業を始める前に、該当するワークシートを印刷し、そのワークシートに必要な情報を記録しておくことができます。

ホスト情報

ディレクトリ サーバの完全修飾ホスト名または IP アドレスを指定します。

ポート情報

(任意) 標準以外のポートを指定します。

デフォルト値: 636 (SSL) および 389 (SSL 以外)

管理 DN

LDAP ツリー内のポリシー ストア ルート オブジェクトの下でオブジェクトの作成、読み取り、変更、および削除を行う権限を持つユーザの LDAP ユーザ名を指定します。

管理パスワード

管理 DN のパスワードを指定します。

ポリシー サーバのルート DN

ポリシー ストア オブジェクトを定義する、LDAP ツリー内のノードの識別名を指定します。

SSL クライアント証明書

SSL クライアント証明書データベース ファイルがあるディレクトリのパス名を指定します。

制限: SSL のみ

ポリシー サーバを設定する方法

OID をポリシー ストアとして設定するには、以下の手順に従います。

1. SiteMinder スキーマ ファイルをダウンロードします。
2. Oracle Internet Directory でドメインを設定します。
3. ディレクトリ サーバにポリシー サーバを示します。
4. ポリシー ストア スキーマを作成します。
5. SiteMinder スーパーユーザ パスワードを設定します。

   注: SiteMinder スーパーユーザ パスワードがすでにある場合は、この手順を実行する必要はありません。
6. デフォルトのポリシー ストア オブジェクトをインポートします。
7. ポリシー ストア データ定義をインポートします。
8. ポリシー サーバを再起動します。
9. 管理 UI の登録を準備します。

SiteMinder スキーマ ファイルのダウンロード

SiteMinder スキーマを設定するのに必要な 1 つ以上のスキーマ ファイルが、ポリシー サーバ インストールに含まれていません。これらのファイルは CA SiteMinder Tier 2 ディレクトリ製品コンポーネント ダウンロードにあります。

Tier 2 ディレクトリ製品コンポーネントをダウンロードする方法

1. テクニカル サポート サイトにログインします。
2. [Support]の下の[Download Center]をクリックします。

   [Download Center]画面が表示されます。
3. [Select a Product]フィールドに「SiteMinder」と入力します。
4. [Select a Release]リストからリリースを選択します。
5. [Select a Gen Level]リストからサービス パックを選択します。
6. [Go]をクリックします。

   [Product Downloads]画面が表示されます。Tier 2 ディレクトリ コンポーネント ダウンロードはリストの下のほうにあります。
7. zip ファイルをローカルに保存し、ポリシー サーバ ホスト システムにファイルを抽出します。

Oracle Internet Directory でのドメインの設定

OID をポリシー ストアとして設定するには、まず OID にドメインを作成します。

Oracle Internet Directory にドメインを設定する方法

1. Oracle Data Manager（ODM）を開きます。
2. [Entry Management]を右クリックし、[Create]を選択します。

   [Distinguished Name]ダイアログ ボックスが開きます。
3. 識別名の値として **dc=dcbok** を入力します。
4. dc の値として **dc** を入力します。
5. 組織単位を作成します。
6. 組織単位を選択します。

7. 識別名の値として **ou=bok、dc=dcbok** を入力します。
8. ou の値として **bok** を入力します。

   OID ドメインが設定されます。

ポリシー サーバからディレクトリ サーバへの参照の設定

ポリシー サーバが、ポリシー ストアに対して情報の読み取りおよび書き込みを行うために必要なシステム情報と管理権限を持つことができるように、ポリシー サーバから LDAP ディレクトリ サーバへの参照を設定します。

ポリシー サーバからディレクトリ サーバへの参照を設定する方法

1. ポリシー サーバ ホスト システムから以下コマンドを実行します。

   ```
   smldapsetup status -hhost -pport -dAdminDN
   -wAdminPW -rroot -ssl1/0 -ccert
   ```

   -h*host*

   LDAP サーバのホスト システムの IP アドレスを指定します。

   -p*port*

   LDAP サーバが受信待機するポートを指定します。

   -d*AdminDN*

   LDAP ディレクトリ サーバに LDAP スキーマを作成する権限を持つ LDAP ユーザの名前を指定します。

   ADAM または AD LDS: guid 値を含め、ディレクトリ サーバ管理者の完全なドメイン名を指定します。

   例: CN=user1,CN=People,CN=Configuration,CN,{guid}

   -w*AdminPW*

   LDAP ディレクトリ サーバに LDAP スキーマを作成する権限を持つ LDAP ユーザのパスワードを指定します。

   -r*root*

   LDAP ディレクトリ内の SiteMinder データの DN ロケーションを指定します。

   ADAM または AD LDS: ポリシー ストア スキーマ データを置く、ADAM または AD LDS サーバ内のアプリケーション パーティションの既存のルート DN ロケーションを指定します。

-ssl1|0

SSL 接続を指定します。

制限: 0=no | 1=yes

デフォルト: 0

-c*cert*

(ssl 値が 1 の場合にのみ必須)SSL クライアント証明書データベース ファイル(cert7.db)があるディレクトリのパスを指定します。

LDAP ポリシー ストア接続パラメータの設定が適正かどうかが検証されます。

2. 以下のコマンドを実行します。

```
smldapsetup reg -hhost -pport -dAdminDN
-wAdminPW -rroot -ssl1/0 -ccert
```

LDAP ディレクトリ サーバの接続がテストされ、サーバが SiteMinder ポリシー ストアとして設定されます。

ポリシー ストア スキーマの作成

r12.0 SP3 によって導入されたオブジェクトを含めるためのポリシー ストア スキーマを作成することができます。

ポリシー ストア スキーマを作成する方法

1. 以下のコマンドを実行します。

```
smldapsetup ldgen -ffile_name.ldif
```

-f

作成するスキーマ ファイルの名前を指定します。

2. 以下のコマンドを実行します。

```
smldapsetup ldmod -ffile_name.ldif
```

-f

作成したスキーマ ファイルの名前を指定します。

3. 以下のコマンドを実行します。

```
ldapmodify -hhost -pport -dAdminDN -wAdminPW
-c -fpath/xps/oid_10g/OID_10g.ldif
-Z -Pcert
```

注: スキーマ ファイルはバージョンに固有ですが、このファイルを使用して 、サポートされる OID のすべてのバージョンのポリシー ストア スキーマをインポートすることができます。

-h*host*

LDAP ディレクトリ サーバの IP アドレスを指定します。

例: 123.123.12.12

-p*port*

LDAP ディレクトリ サーバのポート番号を指定します。

例: 3500

-d*AdminDN*

LDAP ディレクトリ サーバに新規の LDAP スキーマを作成するために必要な権限を持つ LDAP ユーザの名前を指定します。

-w*AdminPW*

-d オプションで指定された管理者のパスワードを指定します。

-c

連続モードを指定します(エラーで停止しません)。

-f*path*

Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。

-Z

SSL 暗号化接続を指定します。

-P*cert*

SSL クライアント証明書データベース ファイル（cert7.db）のパスを指定します。

例:

cert7.db が app/siteminder/ssl に存在する場合は、以下を指定します。

```
-Papp/siteminder/ssl
```

r12.0 SP3 に対するポリシー ストア スキーマが作成されます。

SiteMinder スーパーユーザ パスワードの設定

デフォルトの SiteMinder 管理者アカウントの名前は siteminder です。このアカウントは最大の権限を持っています。その他の SiteMinder 管理者を作成できるまで SiteMinder のユーザ インターフェースとユーティリティの管理に使用できるように、このアカウントのパスワードを設定します。

注: smreg ユーティリティは、ポリシー サーバ インストール キットの最上位レベルにあります。

スーパーユーザのパスワードを設定する方法

1. smreg ユーティリティを *policy_server_home*¥bin にコピーします。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   ```
   smreg -su password
   ```

   重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

   password

   デフォルトの SiteMinder 管理者のパスワードを指定します。

制限:

- パスワードは 6 文字以上、24 文字以下である必要があります。
- パスワードには、アンパサンド(&)またはアスタリスク(*)を含むことはできません。
- パスワードにスペースが含まれている場合は、引用符でパスフレーズを囲みます。

注: パスワードは、Oracle ポリシー ストアに保管する場合を除き、大文字小文字が区別されません。

3. *policy_server_home*¥bin から smreg ユーティリティを削除します。smreg を削除すると、既存のパスワードを把握していない限り、パスワードを変更することはできなくなります。

   デフォルトの SiteMinder 管理者アカウントのパスワードが設定されます。

注: 日常的な作業にはデフォルトのスーパーユーザを使用しないことをお勧めします。デフォルトのスーパーユーザは、以下の場合に使用してください。

- デフォルトのポリシー ストア オブジェクトをインポートする場合。
- FSS 管理 UI および 管理 UI に初めてアクセスする場合。スーパーユーザ権限を持つ別の管理者を作成することをお勧めします。

詳細情報:

インストール メディアの検索 (P. 236)

デフォルトのポリシー ストア オブジェクトのインポート

デフォルトのポリシー ストア オブジェクトをインポートすると、管理 UI で使用するポリシー ストアがセットアップされます。ポリシー ストアにポリシー情報を格納するには、デフォルトのポリシー ストア オブジェクトが必要です。

注: FIPS 専用モードでポリシー サーバをインストールした場合は、デフォルトのポリシー ストア オブジェクトをインポートするときに必ず -cf 引数を使用してください。

デフォルトのポリシー ストア オブジェクトをインポートする方法

1. 以下のコマンドを実行します。

   ```
   smobjimport -ipolicy_server_home¥db¥smdif¥smpolicy.smdif
   -dsiteminder_super_user_name -wsiteminder_super_user_password -v
   ```

   引数にスペースが含まれる場合、引数全体の前後に二重引用符を使用します。

   Windows の例: smobjimport

   ```
   -i"C:¥Program Files¥CA¥siteminder¥db¥smdif¥smpolicy.smdif" -d"SM Admin"
   -wPassword -v
   ```

   UNIX の例: smobjimport

   ```
   -i$NETE_PS_ROOT/db/smdif/smpolicy.smdif -d"SM Admin" -wPassword -v
   ```

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

   -d*siteminder_super_user_name*

   SiteMinder スーパーユーザ アカウントの名前を指定します。

   デフォルト: siteminder

   -w*siteminder_super_user_password*

   SiteMinder スーパーユーザ アカウントのパスワードを指定します。

   -v

   追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

   デフォルト値: stdout

-cf

（任意）FIPS 対応の暗号化を使用して機密データをインポートします。

注: この引数は、ポリシー サーバが FIPS 専用モードで動作している場合にのみ必要です。

smobjimport によって、ポリシー ストア オブジェクトがインポートされます。オブジェクトは、適切な場所に自動的にインポートされます。

2. 以下のコマンドを実行します。

```
smobjimport -ipolicy_server_home¥db¥smdif¥ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

policy_server_home

ポリシー サーバのインストール パスを指定します。

-d*siteminder_super_user_name*

SiteMinder スーパーユーザ アカウントの名前を指定します。

デフォルト: siteminder

-w*siteminder_super_user_password*

SiteMinder スーパーユーザ アカウントのパスワードを指定します。

-f

重複するオブジェクトを上書きします。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト値: stdout

-l

ログ ファイルを作成します。

-c

smdif 入力ファイルに暗号化されていないデータが含まれていることを示します。

smobjimport によって、ポリシー ストア オブジェクトがインポートされます。これらのオブジェクトは、適切な場所に自動的にインポートされます。

注: ampolicy.smdif をインポートすると、Federation セキュリティ サービス、Web サービス変数、および eTelligent ルール機能が使用可能になります。eTelligent ルール機能は、SiteMinder から別個にライセンスが提供されます。この eTelligent ルール機能を使用する予定がある場合は、ライセンスの詳細について、CA アカウント担当者に問い合わせてください。

これで、ポリシー ストア データ定義をインポートできるようになりました。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*¥xps¥dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。
2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。

3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   必要なポリシー ストア データ定義がすべてインポートされました。

ポリシー サーバの再起動

ポリシー ストアやその他のデータ ストアの設定を有効にするために、ポリシー サーバを再起動します。

注: UNIX システムでは、stop-all コマンドの後に start-all コマンドを使用することで、ポリシー サーバを再起動できます。

ポリシー サーバを再起動するには、以下の手順に従います。

1. ポリシー サーバ管理コンソールを開きます。
2. [ステータス]タブをクリックし、[ポリシー サーバ]グループ ボックスで[停止]をクリックします。

   赤色の信号アイコンが表示されて、ポリシー サーバが停止します。
3. [開始]をクリックします。

   緑色の信号アイコンが表示されて、ポリシー サーバが起動します。

管理 UI 登録の準備

管理 UI に初めてログインする場合は、デフォルトの SiteMinder スーパーユーザ アカウント(siteminder)を使用します。初めてログインするときは、ポリシー サーバに 管理 UI を登録する必要があります。これで、両方のコンポーネントの間に信頼関係が作成されます。

XPSRegClient ユーティリティを使用してスーパーユーザ アカウントの名前とパスワードを指定して、登録の準備をします。ポリシー サーバは、これらの認証情報を使用して、登録要求が有効であること、および信頼関係を確立できることを検証します。

以下の点について考慮してください。

- 認証情報を指定してから最初の 管理 UI ログインまでの時間は、24 時間に制限されています。24 時間以内に 管理 UI をインストールする予定がない場合は、管理 UI をインストールする前に以下を実行します。
- （UNIX）XPSRegClient を使用する前に、SiteMinder 環境変数が設定されていることを確認してください。環境変数が設定されていない場合は、手動で設定します。

管理 UI 登録を準備する方法

1. ポリシー サーバ ホスト システムにログインします。
2. 以下のコマンドを実行します。

   ```
   XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
   comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

   passphrase

   デフォルトの SiteMinder スーパーユーザ アカウント（siteminder）のパスワードを指定します。

   注: パスフレーズを指定しないと、XPSRegClient により、パスフレーズの入力とその確認を求めるプロンプトが表示されます。

   -adminui–setup

   管理 UI が初めてポリシー サーバに登録されていることを指定します。

   -t *timeout*

   （任意）管理 UI をインストールしてから、ログインしてポリシー サーバとの信頼関係を作成するまでの割り当て時間を指定します。タイムアウト値を超過すると、ポリシー サーバは登録リクエストを拒否します。

   測定単位: 分

   デフォルト: 240（4 時間）

   最小制限: 1

   最大制限: 1440（24 時間）

-r *retries*

(任意) 管理 UI の登録時に許容される試行の失敗回数を指定します。試行に失敗する原因としては、初めて 管理 UI にログインするときに間違った SiteMinder 管理者クレデンシャルをサブミットしたことが考えられます。

デフォルト: 1

最大制限: 5

-c *comment*

(任意) 指定されたコメントを情報目的で登録ログ ファイルに挿入します。

注: コメントは引用符で囲んでください。

-cp

(任意) 登録ログ ファイルに複数行のコメントが含まれることを指定します。ユーティリティにより複数行のコメントが求められ、指定されたコメントが情報目的で登録ログ ファイルに挿入されます。

注: コメントは引用符で囲んでください。

-l *log path*

(任意) 登録ログ ファイルをエクスポートする場所を指定します。

デフォルト: *siteminder_home*¥log

siteminder_home

ポリシー サーバのインストール パスを指定します。

-e *error_path*

(任意) 例外を指定されたパスに送信します。

デフォルト: stderr

-vT

(任意) 詳細レベルを TRACE に設定します。

-vI

（任意）詳細レベルを INFO に設定します。

-vW

（任意）詳細レベルを WARNING に設定します。

-vE

（任意）詳細レベルを ERROR に設定します。

-vF

（任意）詳細レベルを FATAL に設定します。

3. Enter キーを押します。

   XPSRegClient は、ポリシー サーバに管理者クレデンシャルを提供します。ポリシー サーバは、管理 UI への最初のログイン時に、登録リクエストを確認するためにこれらのクレデンシャルを使用します。

6.x ポリシー ストアをアップグレードする方法

r12.0 SP3 ポリシー ストアに、新規のディレクトリ サーバ インスタンスは必要ありません。既存のポリシー ストアを r12.0 SP3 にアップグレードできます。

ポリシー ストアをアップグレードするには、以下の手順を実行します。

1. ポリシー ストア スキーマを拡張します。

   注：既存の r6.x ポリシー ストア スキーマは、変更されていません。r12.0 SP3 の移行では、ポリシー ストア スキーマをアップグレードして、r12.0 SP3 によって必要とされるオブジェクトのポリシー ストアを拡張する必要があります。

2. ベース ポリシー ストア オブジェクトをインポートします。
3. ポリシー ストア データ定義をインポートします。

注：サポート マトリックスにリストされているディレクトリ サーバまたはデータベースで、本書に記載されていないものをアップグレードする場合は、「SiteMinder アップグレード ガイド」を参照してください。

Oracle Internet Directory ポリシー ストア スキーマの拡張

r12.0 SP3 によって導入されたオブジェクトを含めるように 6.x ポリシー ストア スキーマを拡張することができます。既存の 6.x ポリシー ストア スキーマに加える変更はありません。

Oracle Internet Directory ポリシー ストア スキーマを拡張する方法

1. *policy_server_home*/bin または *policy_server_home*¥bin に移動します。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   ```
   ldapmodify -hhost -pport -dAdminDN -wAdminPW
   -c -fpath/xps/oid_10g/OID_10g.ldif
   -Z -Pcert
   ```

   -h*host*

   LDAP ディレクトリ サーバの IP アドレスを指定します。

   例: 123.123.12.12

   -p*port*

   LDAP ディレクトリ サーバのポート番号を指定します。

   例: 3500

   -d*AdminDN*

   LDAP ディレクトリ サーバに新規の LDAP スキーマを作成するために必要な権限を持つ LDAP ユーザの名前を指定します。

   -w*AdminPW*

   -d オプションで指定された管理者のパスワードを指定します。

   -c

   連続モードを指定します(エラーで停止しません)。

   -f*path*

   Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。

   -Z

   SSL 暗号化接続を指定します。

-P*cert*

SSL クライアント証明書データベースファイル（cert7.db）があるディレクトリのパスを指定します。

例:

cert7.db が app/siteminder/ssl に存在する場合は、以下を指定します。

```
-Papp/siteminder/ssl
```

r12.0 SP3 によって導入されたオブジェクトを含めるようにポリシー ストア スキーマが拡張されます。

ベース ポリシー ストア オブジェクトのインポート

デフォルトの SiteMinder オブジェクトをインポートすると、管理 UI で使用するポリシー ストアがアップグレードされます。デフォルトの SiteMinder オブジェクトは、ポリシー ストアにポリシー情報を格納するために必要です。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. 以下のコマンドを実行します。

```
smobjimport -ipolicy_server_home¥db¥smdif¥upgrade_smdif_file_name
-dsiteminder_super_user_name -wsiteminder_super_user_password
-v -f
```

policy_server_home

ポリシー サーバのインストール パスを指定します。

upgrade_smdif_file_name

インポート ファイルの名前を指定します。

- **r60 から r12.0 SP3:** sm_upgrade_60_to_R12sp3.smdif
- **r60 SP1 から r12.0 SP3:** sm_upgrade_60sp1_to_R12sp3.smdif
- **r60 SP2 から r12.0 SP3:** sm_upgrade_60sp2_to_R12sp3.smdif
- **r60 SP3 から r12.0 SP3:** sm_upgrade_60sp3_to_R12sp3.smdif
- **r60 SP4 から r12.0 SP3:** sm_upgrade_60sp4_to_R12sp3.smdif

- **r60 SP5 から r12.0 SP3:** sm_upgrade_60sp5_to_R12sp3.smdif
- **r60 SP6 から r12.0 SP3:** sm_upgrade_60sp6_to_r12sp3.smdif

-d*siteminder_super_user_name*

SiteMinder 管理者アカウントの名前を指定します。

-w*siteminder_super_user_password*

SiteMinder 管理者アカウントのパスワードを指定します。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト出力: stdout

-f

重複するポリシー ストア オブジェクトを、r12.0 SP3 のもので上書きします。

引数にスペースが含まれる場合、引数全体の前後に二重引用符を使用します。

Windows の例: smobjimport

```
-i"C:¥Program Files¥CA¥siteminder¥db¥smdif¥smpolicy.smdif" -d"SM Admin"
-wPassword -v
```

UNIX の例: smobjimport

-i$NETE_PS_ROOT/db/smdif/smpolicy.smdif -d"SM Admin" -wPassword -v

ベース ポリシー ストア オブジェクトがインポートされます。

2. 以下のコマンドを実行します。

重要: ampolicy.smdif が以前にポリシー ストアにインポートされている場合は再インポートしないでください。

```
smobjimport -ipolicy_server_home¥db¥smdif¥ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

-policy_server_home

インポート ファイルのパスと名前を指定します。

-d*siteminder_super_user_name*

SiteMinder 管理者アカウントの名前を指定します。

-w*siteminder_super_user_password*

SiteMinder 管理者アカウントのパスワードを指定します。

-f

重複するオブジェクトを上書きします。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト値: stdout

-l

ログ ファイルを作成します。

-c

smdif 入力ファイルに暗号化されていないデータが含まれていることを示します。

注: ampolicy.smdif をインポートすると、SiteMinder から別々にライセンスされるフェデレーション セキュリティ サービス、Web サービス変数、および eTelligent ルール機能が使用可能になります。eTelligent ルール機能を使用する予定の場合は、ライセンス情報について CA ジャパン ダイレクトに問い合わせてください。

これで、ポリシー ストア データ定義をインポートできるようになりました。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*¥xps¥dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。

3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   必要なポリシー ストア データ定義がすべてインポートされました。

第 9 章: OpenLDAP サーバ

このセクションには、以下のトピックが含まれています。

SiteMinder スキーマ ファイルのダウンロード

SiteMinder スキーマを設定するのに必要な 1 つ以上のスキーマ ファイルが、ポリシー サーバ インストールに含まれていません。これらのファイルは CA SiteMinder Tier 2 ディレクトリ製品コンポーネント ダウンロードにあります。

Tier 2 ディレクトリ製品コンポーネントをダウンロードする方法

1. テクニカル サポート サイトにログインします。
2. [Support]の下の[Download Center]をクリックします。

   [Download Center]画面が表示されます。
3. [Select a Product]フィールドに「SiteMinder」と入力します。
4. [Select a Release]リストからリリースを選択します。
5. [Select a Gen Level]リストからサービス パックを選択します。
6. [Go]をクリックします。

   [Product Downloads]画面が表示されます。Tier 2 ディレクトリ コンポーネント ダウンロードはリストの下のほうにあります。
7. zip ファイルをローカルに保存し、ポリシー サーバ ホスト システムにファイルを抽出します。

Slapd 構成ファイルを設定する方法

OpenLDAP ディレクトリ サーバをポリシー ストアとして使用できるようにするには、事前に OpenLDAP ディレクトリ サーバで追加設定を行っておく必要があります。設定手順は以下のとおりです。

1. SiteMinder スキーマ ファイルを指定します。
2. 認証を有効にします。
3. データベース ディレクティブを指定します。
4. 構成ファイルをテストします。
5. OpenLDAP サーバのを起動します。

SiteMinder スキーマ ファイルの指定

slapd 構成ファイル（slapd.conf）の include セクションにスキーマ ファイルを指定することによって、slapd プロセス（LDAP ディレクトリ サーバ デーモン）は追加の構成情報を読み取ることができます。含めるファイルは、適切な slapd 設定ファイル形式に従う必要があります。

スキーマ ファイルを指定する方法

1. OpenLDAP インストール ディレクトリ内のスキーマ フォルダに、以下のスキーマ ファイルをコピーします。
   - *path*/openldap/openldap_attribute.schema
   - *path*/openldap/openldap_object.schema
   - *path*/xps/openldap/openldap_attribute_XPS.schema
   - *path*/xps/openldap/openldap_object_XPS.schema

   path

   Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。
2. slapd 構成ファイルの include セクションに、以下を入力します。

```
....
.....
include /usr/local/etc/openldap/schema/openldap_attribute.schema
include /usr/local/etc/openldap/schema/openldap_object.schema
```

```
include /usr/local/etc/openldap/schema/openldap_attribute_XPS.schema
include /usr/local/etc/openldap/schema/openldap_object_XPS.schema
```

注: この手順は、OpenLDAP サーバが /usr/local/etc/openldap にあり、スキーマ ファイルが schema サブディレクトリにあることを前提としています。

r12.0 SP3 に対するポリシー ストア スキーマが作成されます。

ユーザ認証の有効化

ユーザ認証を有効にすることにより、サポートされた認証方式でリソースを保護することができます。

ユーザ認証を有効にするには、slapd 設定ファイルに以下の行を追加します。

```
access to attr=userpassword
by self write
by anonymous auth
by * none
```

データベース ディレクティブの指定

slapd 設定ファイルには、さらにデータベース ディレクティブの値が必要です。

ディレクティブを指定するには、以下を編集します。

database

任意のサポートされているバックエンド タイプを指定します。

例: bdb

suffix

データベースのサフィックスを指定します。

例: dc=example、dc=com

rootdn

ルートの DN を指定します。

例: cn=Manager、dc=example、dc=com

rootpw

ルートのパスワードを指定します。

directory

データベース ディレクトリのパスを指定します。

例: /usr/local/var/openldap-data

注: データベース ディレクトリは、slapd を実行する前に存在していることが必要です。slapd プロセスにアクセス可能である必要があるのは、このディレクトリのみです。

クライアント サイドの並べ替えのサポート

サポートされている LDAP ディレクトリで、サーバ サイドの並べ替えをサポートしていないのは OpenLDAP のみです。代わりに、OpenLDAP では、すべての並べ替えをクライアント サイドで実行する必要があります。このために、すべての XPS オブジェクトは、サーバ サイドのページングを使用して起動時に取得されます。

クライアント サイドの並べ替えをサポートするには、OpenLDAP ディレクトリの管理者が、slapd.conf ファイルで以下の設定を行う必要があります。

- ルート DSE の読み取りを有効にします。

  この設定により、XPS クライアントは OpenLDAP ディレクトリのタイプおよび機能を読み取ることが可能になります。

- 検索操作から返すことのできる項目の最大数を 500 以上に設定します。

  この設定により、サーバ サイドのページングによって 500 個単位で取得される XPS オブジェクトに対応します。

- シンプル V2 バインドを許可します。

  この設定により、smconsole はシンプル V2 バインドを使用して LDAP 接続をテストすることが可能になります。

クライアント サイドの並べ替えをサポートする方法

1. slapd.conf ファイルに、以下の行を追加します。

   ```
   access to *
   by users read
   by anonymous read
   access to dn.base=ACL by users read
   ```

   ACL

   アクセス制御リストまたは権限のリストを指定します。

   注: ACL を指定する方法の詳細については、http://www.openldap.org/doc/admin24/access-control.html を参照してください。

2. slapd.conf ファイルで sizelimit ディレクティブによって指定された値が 500 以上であることを確認します。

   ```
   sizelimit 500
   ```

   注: sizelimit のデフォルト値は 500 です。詳細については、http://www.openldap.org/doc/admin24/slapdconfig.html を参照してください。

3. slapd.conf ファイルに、以下の行を追加します。

   ```
   allow bind_v2
   ```

slapd.conf ファイルが、クライアント サイドの並べ替えをサポートするように設定されます。

設定ファイルのテスト

設定ファイルをテストすることで、ファイルを正しい形式にすることができます。

設定ファイルをテストする方法

1. OpenLDAP サーバ ディレクトリに移動します。

2. 以下のコマンドを実行します。

   ```
   ./slapd
   ```

   注: レベル 0 を含め、デバッグ レベルが指定されていない限り、slapd は自動的にフォークして、制御端末から自身を切り離し、バックグラウンドで実行します。

3. 以下のコマンドを実行します。

   ```
   ./slapd -Tt
   ```

   slapd 設定ファイルがテストされます。

OpenLDAP サーバの再起動

OpenLDAP ディレクトリ サーバを再起動すると、SiteMinder スキーマがロードされます。ディレクトリ サーバをポリシー ストアとして使用できるように、ポリシー サーバは、事前に SiteMinder スキーマをロードしておくことを必要とします。

ディレクトリ サーバを再起動する方法

1. 以下のコマンドを使用して、ディレクトリ サーバを停止します。

   ```
   kill ?INT 'cat path_of_var/run_directory/slapd.pid'
   ```

   path_of_var/run_directory

   データベース ディレクトリのパスを指定します。

   例: kill ?INT 'cat /usr/local/var/run/slapd.pid'

2. 以下のコマンドを使用して、ディレクトリ サーバを起動します。

   ```
   ./slapd
   ```

データベースを作成する方法

以下のプロセスに、ポリシー ストア用のディレクトリ サーバ データベースを作成するための手順を示します。

1. ベース ツリー構造を作成します。
2. エントリを追加します。

ベース ツリー構造の作成

ポリシー ストアにベース ツリー構造を作成することができます。

ルート DN の下に、以下を指定します。

```
ou=Netegrity,ou=SiteMinder,ou=PolicySvr4,ou=XPS
```

ベース ツリー構造がポリシー ストアに作成されます。

エントリの追加

SiteMinder が必要な組織情報および組織ロール情報を保持するように、ディレクトリ サーバにエントリを追加します。

データベース エントリを追加する方法

1. LDIF ファイルを作成します。

   例: 以下の例には、entries.ldif の組織エントリおよび組織ロール エントリが含まれます。

   ```
   # Organization for example.com
   dn: root_DN (example.com)
   objectClass: dcObject
   objectClass: organization
   dc: example
   o: Example Corporation

   # Organizational Role for Directory Manager
   dn: cn=Manager,root_DN
   objectClass: organizationalRole
   objectClass: top
   cn: Manager
   description: Directory Manager
   ```

2. 以下のコマンドを使用して、エントリを追加します。

   ```
   ldapadd -<file_name.ldif>
   -D "cn=Manager,dc=example,dc=com" -w<password>
   ```

ディレクトリ サーバをポリシー ストアとして設定する方法

ポリシー サーバ管理コンソールおよび 管理 UI を使用して、ディレクトリ サーバをポリシー ストアとして設定することができます。以下に、ディレクトリ サーバをポリシー ストアとして使用するための手順を示します。

1. ポリシー ストアを作成
2. ポリシー ストアに接続

ポリシー サーバからディレクトリ サーバへの参照の設定

ポリシー サーバが、ポリシー ストアに対して情報の読み取りおよび書き込みを行うために必要なシステム情報と管理権限を持つことができるように、ポリシー サーバから LDAP ディレクトリ サーバへの参照を設定します。

ポリシー サーバからディレクトリ サーバへの参照を設定する方法

1. ポリシー サーバ ホスト システムから以下コマンドを実行します。

```
smldapsetup status -hhost -pport -dAdminDN
-wAdminPW -rroot -ssl1/0 -ccert
```

-h*host*

LDAP サーバのホスト システムの IP アドレスを指定します。

-p*port*

LDAP サーバが受信待機するポートを指定します。

-d*AdminDN*

LDAP ディレクトリ サーバに LDAP スキーマを作成する権限を持つ LDAP ユーザの名前を指定します。

ADAM または AD LDS: guid 値を含め、ディレクトリ サーバ管理者の完全なドメイン名を指定します。

例: CN=user1,CN=People,CN=Configuration,CN,{guid}

-w*AdminPW*

LDAP ディレクトリ サーバに LDAP スキーマを作成する権限を持つ LDAP ユーザのパスワードを指定します。

-rroot

LDAP ディレクトリ内の SiteMinder データの DN ロケーションを指定します。

ADAM または AD LDS: ポリシー ストア スキーマ データを置く、ADAM または AD LDS サーバ内のアプリケーション パーティションの既存のルート DN ロケーションを指定します。

-ssl1|0

SSL 接続を指定します。

制限: 0=no | 1=yes

デフォルト: 0

-ccert

(ssl 値が 1 の場合にのみ必須) SSL クライアント証明書データベース ファイル (cert7.db) があるディレクトリのパスを指定します。

LDAP ポリシー ストア接続パラメータの設定が適正かどうかが検証されます。

2. 以下のコマンドを実行します。

```
smldapsetup reg -hhost -pport -dAdminDN
-wAdminPW -rroot -ssl1/0 -ccert
```

LDAP ディレクトリ サーバの接続がテストされ、サーバが SiteMinder ポリシー ストアとして設定されます。

ポリシー ストアの作成

OpenLDAP ディレクトリ サーバをポリシー ストアとして設定するには、ベース ポリシー ストア データをインポートします。

ポリシー ストアを作成する方法

1. ポリシーサーバー管理コンソールを起動します。
2. [データ]タブをクリックします。
3. [ルート DN]フィールドにルート DN を入力し、[OK]をクリックします。

   ルート DN が保存されます。
4. policy_server_home/bin に移動します。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

5. 以下のコマンドを実行します。

   smreg -su *adminPW*

   管理者のパスワードが保存されます。

6. 以下のコマンドを実行します。

   smobjimport -i*policy_server_home*¥db¥smdif¥smpolicy.smdif -d*AdminDN* -w*AdminPW* -v

   -i

   インポート ファイルの名前を指定します。

   -d*AdminDN*

   LDAP ディレクトリに新規の LDAP スキーマを作成する権限を持つ LDAP ユーザの名前を指定します。

   -w*AdminPW*

   LDAP ディレクトリに新規の LDAP スキーマを作成する権限を持つ LDAP ユーザのパスワードを指定します。

   -v

   トレースをオンにして、エラー メッセージ、警告メッセージ、およびコメント メッセージを出力します。

   ベース ポリシー ストア データを、ファイル smpolicy.smdif からインポートします。

7. 以下のコマンドを実行します。

   smobjimport -i*policy_server_home*¥db¥smdif¥ampolicy.smdif
   -d*siteminder_super_user_name* -w*siteminder_super_user_password* -f -v -l -c

   -d*siteminder_super_user_name*

   SiteMinder スーパーユーザ アカウントの名前を指定します。

   -w*siteminder_super_user_password*

   SiteMinder スーパーユーザ アカウントのパスワードを指定します。

   -f

   重複するオブジェクトをオーバーライドします。

   -v

   追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

   デフォルト値: stdout

-l

ログ ファイルを作成します。

-c

smdif 入力ファイルに暗号化されていないデータが含まれていることを示します。

smobjimport によって、ポリシー ストア オブジェクトがインポートされます。これらのオブジェクトは、適切な場所に自動的にインポートされます。

注: ampolicy.smdif をインポートすると、Federation セキュリティ サービス、Web サービス変数、および eTelligent ルール機能が使用可能になります。eTelligent ルール機能は、SiteMinder から別個にライセンスが提供されます。この eTelligent ルール機能を使用する予定がある場合は、ライセンスの詳細について、CA アカウント担当者に問い合わせてください。

注: これで、ポリシー ストア データ定義をインポートできます。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*¥xps¥dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。

3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   必要なポリシー ストア データ定義がすべてインポートされました。

管理 UI 登録の準備

管理 UI に初めてログインする場合は、デフォルトの SiteMinder スーパーユーザ アカウント(siteminder)を使用します。初めてログインするときは、ポリシー サーバに 管理 UI を登録する必要があります。これで、両方のコンポーネントの間に信頼関係が作成されます。

XPSRegClient ユーティリティを使用してスーパーユーザ アカウントの名前とパスワードを指定して、登録の準備をします。ポリシー サーバは、これらの認証情報を使用して、登録要求が有効であること、および信頼関係を確立できることを検証します。

以下の点について考慮してください。

- 認証情報を指定してから最初の 管理 UI ログインまでの時間は、24 時間に制限されています。24 時間以内に 管理 UI をインストールする予定がない場合は、管理 UI をインストールする前に以下を実行します。
- （UNIX）XPSRegClient を使用する前に、SiteMinder 環境変数が設定されていることを確認してください。環境変数が設定されていない場合は、手動で設定します。

管理 UI 登録を準備する方法

1. ポリシー サーバ ホスト システムにログインします。
2. 以下のコマンドを実行します。

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

デフォルトの SiteMinder スーパーユーザ アカウント（siteminder）のパスワードを指定します。

注：パスフレーズを指定しないと、XPSRegClient により、パスフレーズの入力とその確認を求めるプロンプトが表示されます。

-adminui–setup

管理 UI が初めてポリシー サーバに登録されていることを指定します。

-t *timeout*

（任意）管理 UI をインストールしてから、ログインしてポリシー サーバとの信頼関係を作成するまでの割り当て時間を指定します。タイムアウト値を超過すると、ポリシー サーバは登録リクエストを拒否します。

測定単位： 分

デフォルト： 240（4 時間）

最小制限： 1

最大制限： 1440（24 時間）

-r *retries*

(任意) 管理 UI の登録時に許容される試行の失敗回数を指定します。試行に失敗する原因としては、初めて 管理 UI にログインするときに間違った SiteMinder 管理者クレデンシャルをサブミットしたことが考えられます。

デフォルト: 1

最大制限: 5

-c *comment*

(任意) 指定されたコメントを情報目的で登録ログ ファイルに挿入します。

注: コメントは引用符で囲んでください。

-cp

(任意) 登録ログ ファイルに複数行のコメントが含まれることを指定します。ユーティリティにより複数行のコメントが求められ、指定されたコメントが情報目的で登録ログ ファイルに挿入されます。

注: コメントは引用符で囲んでください。

-l *log path*

(任意) 登録ログ ファイルをエクスポートする場所を指定します。

デフォルト: *siteminder_home*¥log

siteminder_home

ポリシー サーバのインストール パスを指定します。

-e *error_path*

(任意) 例外を指定されたパスに送信します。

デフォルト: stderr

-vT

(任意) 詳細レベルを TRACE に設定します。

-vI

（任意）詳細レベルを INFO に設定します。

-vW

（任意）詳細レベルを WARNING に設定します。

-vE

（任意）詳細レベルを ERROR に設定します。

-vF

（任意）詳細レベルを FATAL に設定します。

3. Enter キーを押します。

   XPSRegClient は、ポリシー サーバに管理者クレデンシャルを提供します。ポリシー サーバは、管理 UI への最初のログイン時に、登録リクエストを確認するためにこれらのクレデンシャルを使用します。

ディレクトリ サーバをユーザ ストアとして設定する方法

OpenLDAP ディレクトリ サーバをユーザ ストアとして使用することができます。以下に、ディレクトリ サーバをユーザ ストアとして使用するための手順を示します。

1. ユーザ ストアを作成
2. ユーザ ストアに接続

ユーザ ストアの作成

OpenLDAP ディレクトリ サーバをユーザ ストアとして使用することができます。

ユーザ ストアを作成する方法

1. LDIF ファイルを使用して、ルート DN の下に ou=People を作成します。
2. 組織単位の下にユーザを作成します。

ポリシー サーバから OpenLDAP ユーザ ストアへの接続の設定

ポリシー サーバから OpenLDAP ユーザ ストアへの接続を設定するには、新規のユーザ ディレクトリ オブジェクトを作成します。

ポリシー サーバから OpenLDAP ユーザ ストアへの接続を設定する方法

1. [インフラストラクチャ]-[ディレクトリ]をクリックします。
2. [ユーザ ディレクトリ]、[ユーザ ディレクトリの作成]をクリックします。

   [ユーザ ディレクトリの作成]ペインが表示されます。

   注: このペインで、ユーザ ディレクトリのプロパティを指定できます。フィールド、設定、およびオプションの詳細については、[ヘルプ]をクリックしてください。
3. [一般]グループ ボックスのフィールドに、新規のユーザ ディレクトリ オブジェクトの名前と説明を入力します。
4. [ネームスペース]リストから[LDAP]が選択されていることを確認し、[ディレクトリのセットアップ]グループ ボックスの[サーバ]フィールドに、IP アドレスとポート番号を入力します。

   注: ポリシー サーバが FIPS モードで動作し、ユーザ ディレクトリ接続が安全な SSL 接続である場合、ポリシー サーバとディレクトリ ストアが使用する証明書は FIPS 準拠である必要があります。
5. [認証情報が必要]チェック ボックスをオンにし、[管理者認証情報]グループ ボックスのフィールドに管理者の完全 DN とパスワードを入力します。
6. [LDAP 検索]グループ ボックスのフィールドに、ルート ノードと検索パラメータを入力します。
7. [LDAP ユーザ DN の検索]グループ ボックスのフィールドに、先頭テキスト文字列と終端テキスト文字列を入力します。

   注: 先頭テキスト文字列、ユーザ名、および終端テキスト文字列を組み合わせて、ユーザ ディレクトリ ツリーを検索する場合に使用する文字列を作成します。
8. (任意)[ユーザ属性]グループ ボックスのフィールドに入力します。
   a. [ユニバーサル ID]フィールドにユニバーサル ID を入力します。

      属性タイプ: 文字列

b. [無効フラグ]フィールドに、無効なユーザを追跡するフラグを入力します。

属性タイプ: 文字列

c. [パスワード]フィールドに、ユーザ パスワードのロケーションを入力します。

属性タイプ: バイナリ

d. [パスワード データ]フィールドに、ユーザ パスワード履歴のロケーションを入力します。

属性タイプ: バイナリ

注: この属性は、パスワード サービスに必要です。

e. [匿名 ID]フィールドに、ユーザの匿名 ID を入力します。

属性タイプ: 文字列

f. [電子メール]フィールドは空のままにしておきます。

注: 電子メール機能は、SiteMinder の現行バージョンには実装されていません。

g. [チャレンジ/レスポンス]フィールドに、レスポンスを入力します。

属性タイプ: 文字列

注: この文字列は、各チャレンジ後にユーザに送信されます。

9. (任意)[属性マッピング リスト]グループ ボックスで[作成]をクリックします。

[属性マッピングの作成]ペインが開きます。

注: ユーザ属性マッピングの詳細については、「ポリシー サーバ設定ガイド」を参照してください。

10. [サブミット]をクリックします。

ユーザ ディレクトリの作成タスクが処理のためにサブミットされます。

詳細情報:

SSL を使った LDAP ユーザ ディレクトリ接続を設定する方法 (P. 223)

ポリシー ストアに対する SSL の設定

ポリシー ストアは Secure Socket Layer（SSL）をサポートしています。ポリシー サーバ管理コンソールから、SSL に対応するようにポリシー ストアを設定します。

この手順では、以下を前提としています。

- OpenLDAP 環境が SSL 対応に設定されています。
- 証明機関（CA）のルート証明書（cacert.pem）が、SSL を使用してディレクトリ サーバと通信する各マシン上の Netscape cert7.db データベースにインストールされています。
- key3.db ファイルが作成されています。

  注: SiteMinder では、ルート証明書が Netscape ファイル形式に準拠している必要があります。証明書のインストールに Microsoft IE を使用することはできません。

ポリシー ストアに対して SSL を設定する方法

1. ポリシーサーバー管理コンソールを起動します。
2. ［データ］タブをクリックします。

   ［データ］タブが開きます。
3. ［SSL を使用］を選択します。
4. Netscape 証明書データベース ファイルのフィールドに、cert7.db の絶対パスを入力します。

   注: 以下の点を考慮してください。

   - 既知の制限により、ファイル名をパスに含める必要があります。完全な絶対パスを提供すると、この問題を解決することができます。レジストリの CertDbPath 変数で最後のサブストリング（cert7.db）を削除することにより、パスを修正します。
   - key3.db ファイルも、cert7.db ファイルと同じディレクトリに必要です。
5. ［OK］をクリックします。

   SSL がポリシー ストアに対して有効になります。

6.x ポリシー ストアをアップグレードする方法

r12.0 SP3 ポリシー ストアに、新規のディレクトリ サーバ インスタンスは必要ありません。既存のポリシー ストアを r12.0 SP3 にアップグレードできます。

ポリシー ストアをアップグレードするには、以下の手順を実行します。

1. ポリシー ストア スキーマを拡張します。

   注:既存の r6.x ポリシー ストア スキーマは、変更されていません。r12.0 SP3 の移行では、ポリシー ストア スキーマをアップグレードして、r12.0 SP3 によって必要とされるオブジェクトのポリシー ストアを拡張する必要があります。

2. ベース ポリシー ストア オブジェクトをインポートします。
3. ポリシー ストア データ定義をインポートします。

注: サポート マトリックスにリストされているディレクトリ サーバまたはデータベースで、本書に記載されていないものをアップグレードする場合は、「SiteMinder アップグレード ガイド」を参照してください。

OpenLDAP ポリシー ストア スキーマの拡張

slapd 設定ファイル(slapd.conf)の include セクションにスキーマ ファイルを指定することにより、r12.0 SP3 によって導入されたオブジェクトを含めるように既存の 6.x ポリシー ストア スキーマを拡張することができます。これで、slapd プロセス(LDAP ディレクトリ サーバ デーモン)は追加の設定情報を読み取ることができます。含めるファイルは、適切な slapd 設定ファイル形式に従う必要があります。既存の 6.x ポリシー ストア スキーマに加える変更はありません。

既存の OpenLDAP ポリシー ストア スキーマを拡張する方法

1. ou=Netegrity,ou=SiteMinder,ou=PolicySvr4 に以下のルート ノードを追加します。

   ou=XPS

2. 以下のスキーマ ファイルを、*path*¥xps¥openldap から OpenLDAP インストール ディレクトリ内のスキーマ フォルダにコピーします。

   - openldap_attribute_XPS.schema
   - openldap_object_XPS.schema

   path

   Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。

3. slapd 構成ファイルの include セクションに、以下を入力します。

   ```
   ....
   .....
   include /usr/local/etc/openldap/schema/openldap_attribute_XPS.schema
   include /usr/local/etc/openldap/schema/openldap_object_XPS.schema
   ```

   注: この手順は、OpenLDAP サーバが /usr/local/etc/openldap にあり、スキーマ ファイルが schema サブディレクトリにあることを前提としています。

   r12.0 SP3 によって導入されたオブジェクトを含めるようにポリシー ストア スキーマが拡張されます。

ベース ポリシー ストア オブジェクトのインポート

デフォルトの SiteMinder オブジェクトをインポートすると、管理 UI で使用するポリシー ストアがアップグレードされます。デフォルトの SiteMinder オブジェクトは、ポリシー ストアにポリシー情報を格納するために必要です。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. 以下のコマンドを実行します。

```
smobjimport -ipolicy_server_home¥db¥smdif¥upgrade_smdif_file_name
-dsiteminder_super_user_name -wsiteminder_super_user_password
-v -f
```

policy_server_home

ポリシー サーバのインストール パスを指定します。

upgrade_smdif_file_name

インポート ファイルの名前を指定します。

- **r60 から r12.0 SP3:** sm_upgrade_60_to_R12sp3.smdif
- **r60 SP1 から r12.0 SP3:** sm_upgrade_60sp1_to_R12sp3.smdif
- **r60 SP2 から r12.0 SP3:** sm_upgrade_60sp2_to_R12sp3.smdif
- **r60 SP3 から r12.0 SP3:** sm_upgrade_60sp3_to_R12sp3.smdif
- **r60 SP4 から r12.0 SP3:** sm_upgrade_60sp4_to_R12sp3.smdif
- **r60 SP5 から r12.0 SP3:** sm_upgrade_60sp5_to_R12sp3.smdif
- **r60 SP6 から r12.0 SP3:** sm_upgrade_60sp6_to_r12sp3.smdif

-d*siteminder_super_user_name*

SiteMinder 管理者アカウントの名前を指定します。

-w*siteminder_super_user_password*

SiteMinder 管理者アカウントのパスワードを指定します。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト出力: stdout

-f

重複するポリシー ストア オブジェクトを、r12.0 SP3 のもので上書きします。

引数にスペースが含まれる場合、引数全体の前後に二重引用符を使用します。

Windows の例: smobjimport
-i"C:¥Program Files¥CA¥siteminder¥db¥smdif¥smpolicy.smdif" -d"SM Admin" -wPassword -v

UNIX の例: smobjimport

-i$NETE_PS_ROOT/db/smdif/smpolicy.smdif -d"SM Admin" -wPassword -v

ベース ポリシー ストア オブジェクトがインポートされます。

2. 以下のコマンドを実行します。

重要: ampolicy.smdif が以前にポリシー ストアにインポートされている場合は再インポートしないでください。

smobjimport -i*policy_server_home*¥db¥smdif¥ampolicy.smdif
-d*siteminder_super_user_name* -w*siteminder_super_user_password* -f -v -l -c

-*policy_server_home*

インポート ファイルのパスと名前を指定します。

-d*siteminder_super_user_name*

SiteMinder 管理者アカウントの名前を指定します。

-w*siteminder_super_user_password*

SiteMinder 管理者アカウントのパスワードを指定します。

-f

重複するオブジェクトを上書きします。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト値: stdout

-l

ログ ファイルを作成します。

-c

smdif 入力ファイルに暗号化されていないデータが含まれていることを示します。

注: ampolicy.smdif をインポートすると、SiteMinder から別々にライセンスされるフェデレーション セキュリティ サービス、Web サービス変数、および eTelligent ルール機能が使用可能になります。eTelligent ルール機能を使用する予定の場合は、ライセンス情報について CA ジャパン ダイレクトに問い合わせてください。

これで、ポリシー ストア データ定義をインポートできるようになりました。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*¥xps¥dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。
2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。

3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   必要なポリシー ストア データ定義がすべてインポートされました。

OpenLDAP のトラブルシューティング

OpenLDAP のトラブルシューティングについては、以下のトピックを参照してください。

- Cyrus SASL のインストール
- Berkeley データベース バージョン不一致エラー
- openSSL のビルドおよびインストール

Cyrus SASL のインストール

症状:

Cyrus SASL をインストールするときに、コンパイル問題が発生しました。

解決方法:

Cyrus SASL インストール問題のトラブルシューティングの詳細については、以下を参照してください。

http://marc.theaimsgroup.com/?l=cyrus-sasl&m=111835942621184&w=2

Berkeley データベース バージョン不一致エラー

症状:

Berkeley データベース バージョン不一致エラーが発生しました。

解決方法:

Berkeley データベース バージョン不一致エラーの詳細については、以下を参照してください。

http://www.openldap.org/faq/data/cache/1113.html

openSSL のビルドおよびインストール

症状:

openSSL をビルドおよびインストールする際に問題が発生しました。

解決方法:

openSSL のビルドおよびインストールの詳細については、以下を参照してください。

http://www.proscrutiny.com/howtos/OpenLDAP.html#confssl-co

第 10 章: Red Hat Directory Server

このセクションには、以下のトピックが含まれています。

ポリシー サーバから Red Hat ユーザ ストアへの接続の設定

ポリシー サーバから Red Hat ユーザ ストアへの接続を設定するには、SiteMinder 管理 UI でユーザ ディレクトリ オブジェクトを作成します。

ポリシー サーバから Red Hat ユーザ ストアへの接続を設定する方法

1. [インフラストラクチャ]-[ディレクトリ]をクリックします。
2. [ユーザ ディレクトリ]、[ユーザ ディレクトリの作成]をクリックします。

   [ユーザ ディレクトリの作成]ペインが表示されます。

   注: このペインで、ユーザ ディレクトリのプロパティを指定できます。フィールド、設定、およびオプションの詳細については、[ヘルプ]をクリックしてください。
3. [一般]グループ ボックスのフィールドに、新規のユーザ ディレクトリ オブジェクトの名前と説明を入力します。
4. [ネームスペース]リストから[LDAP]が選択されていることを確認し、[ディレクトリのセットアップ]グループ ボックスの[サーバ]フィールドに、IP アドレスとポート番号を入力します。
5. [認証情報が必要]チェック ボックスをオンにし、[管理者認証情報]グループ ボックスのフィールドに管理者の完全 DN とパスワードを入力します。
6. [LDAP 検索]グループ ボックスのフィールドに、ルート ノードと検索パラメータを入力します。
7. [LDAP ユーザ DN の検索]グループ ボックスのフィールドに、先頭テキスト文字列と終端テキスト文字列を入力します。

   注: 先頭テキスト文字列、ユーザ名、および終端テキスト文字列を組み合わせて、ユーザ ディレクトリ ツリーを検索する場合に使用する文字列を作成します。

8. （省略可）[ユーザ属性]グループ ボックスのフィールドに入力します。
   a. [ユニバーサル ID]フィールドにユニバーサル ID を入力します。

      属性タイプ: 文字列

   b. [無効フラグ]フィールドに、無効なユーザを追跡するフラグを入力します。

      属性タイプ: 文字列

   c. [パスワード]フィールドに、ユーザ パスワードのロケーションを入力します。

      属性タイプ: バイナリ

   d. [パスワード データ]フィールドに、ユーザ パスワード履歴のロケーションを入力します。

      属性タイプ: バイナリ

      注: この情報は、パスワード サービスに必要です。

   e. [匿名 ID]フィールドに、ユーザの匿名 ID を入力します。

      属性タイプ: 文字列

   f. [電子メール]フィールドは空のままにしておきます。

      注: 電子メール機能は、SiteMinder の現行バージョンには実装されていません。

   g. [チャレンジ/レスポンス]フィールドに、レスポンスを入力します。

      属性タイプ: 文字列

      注: この文字列は、各チャレンジ後にユーザに送信されます。

9. （省略可）[属性マッピング リスト]グループ ボックスで[作成]をクリックします。

   [属性マッピングの作成]ペインが開きます。

   注: ユーザ属性マッピングの詳細については、「ポリシー サーバ設定ガイド」を参照してください。

10. [サブミット]をクリックします。

    ユーザ ディレクトリの作成タスクが処理のためにサブミットされます。

Red Hat Directory Server をポリシー ストアとして設定する方法

Red Hat Directory Server をポリシー ストアとして設定する方法は、7 段階のプロセスです。

1. ポリシー サーバがポリシー ストア（Red Hat Directory Server）を参照するよう設定します。
2. Red Hat Directory Server に、ポリシー ストア スキーマを作成します。
3. SiteMinder スーパーユーザ パスワードを設定します。
4. デフォルトのポリシー ストア オブジェクトをインポートします。
5. ポリシー ストア データ定義をインポートします。
6. ポリシー サーバを再起動します。
7. 管理 UI の登録準備をします。

SiteMinder スキーマ ファイルのダウンロード

SiteMinder スキーマを設定するのに必要な 1 つ以上のスキーマ ファイルが、ポリシー サーバ インストールに含まれていません。これらのファイルは CA SiteMinder Tier 2 ディレクトリ製品コンポーネント ダウンロードにあります。

Tier 2 ディレクトリ製品コンポーネントをダウンロードする方法

1. テクニカル サポート サイトにログインします。
2. [Support]の下の[Download Center]をクリックします。

   [Download Center]画面が表示されます。
3. [Select a Product]フィールドに「SiteMinder」と入力します。
4. [Select a Release]リストからリリースを選択します。
5. [Select a Gen Level]リストからサービス パックを選択します。
6. [Go]をクリックします。

   [Product Downloads]画面が表示されます。Tier 2 ディレクトリ コンポーネント ダウンロードはリストの下のほうにあります。
7. zip ファイルをローカルに保存し、ポリシー サーバ ホスト システムにファイルを抽出します。

ポリシー サーバからポリシー ストアへの参照の設定

ポリシー サーバからポリシー ストアへの参照を設定し、ポリシー サーバがポリシー ストアにアクセスできるようにします。

ポリシー サーバからポリシー ストアへの参照を設定する方法

1. ポリシー サーバ管理コンソールを開きます。

   重要: Windows Server 2008 上でこのグラフィカル ユーザ インターフェースにアクセスする場合は、管理者としてシステムにログインしている場合でも、管理者権限でショートカットを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

2. [データ]タブをクリックします。

   データベース設定が表示されます。

3. [データベース]リストから[ポリシー ストア]を選択します。

4. [ストレージ]リストから[LDAP]を選択します。

5. [LDAP ポリシー ストア]グループ ボックスで、以下を設定します。

   - LDAP IP アドレス
   - 管理者ユーザ名
   - パスワード
   - パスワードの確認
   - DN

   注: フィールド、コントロール、およびそれぞれの要件については、[ヘルプ]をクリックしてください。

6. [適用]をクリックします。

   ポリシー ストアの設定が保存されます。

7. [LDAP 接続のテスト]をクリックします。

   SiteMinder は、ポリシー サーバがポリシー ストアにアクセスできることを示す確認を返します。

Red Hat Directory Server でのポリシー ストア スキーマの作成

Red Hat Directory Server に、ポリシー ストア スキーマを作成することができます。

Red Hat Directory Server にポリシー ストア スキーマを作成する方法

1. コマンド ウィンドウで *policy_server_home*/bin に移動します。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   ```
   smldapsetup ldgen -fschema_file
   ```

   schema_file

   作成する LDIF ファイルの名前を指定します。

   LDIF ファイルが、ポリシー ストア スキーマを使用して作成されます。

3. 以下のコマンドを実行します。

   ```
   smldapsetup ldmod -fschema_file
   ```

   schema_file

   作成した LDIF ファイルの名前を指定します。

   ポリシー ストア スキーマが、LDIF ファイルから Red Hat Directory Server にインポートされます。

4. 以下のコマンドを実行します。

   ```
   smldapsetup ldmod
   -fpath/xps/redhat/RedHat_7_1.ldif
   ```

   path

   Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。

   ポリシー ストア スキーマが、Red Hat Directory Server で XPS 向けに拡張されます。

ポリシー ストア スキーマが、Red Hat Directory Server に作成されます。

SiteMinder スーパーユーザ パスワードの設定

デフォルトの SiteMinder 管理者アカウントの名前は siteminder です。このアカウントは最大の権限を持っています。その他の SiteMinder 管理者を作成できるまで SiteMinder のユーザ インターフェースとユーティリティの管理に使用できるように、このアカウントのパスワードを設定します。

注: smreg ユーティリティは、ポリシー サーバ インストール キットの最上位レベルにあります。

スーパーユーザのパスワードを設定する方法

1. smreg ユーティリティを *policy_server_home*¥bin にコピーします。

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   `smreg -su` *password*

   重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

   password

   デフォルトの SiteMinder 管理者のパスワードを指定します。

   制限:

   - パスワードは 6 文字以上、24 文字以下である必要があります。
   - パスワードには、アンパサンド(&)またはアスタリスク(*)を含むことはできません。
   - パスワードにスペースが含まれている場合は、引用符でパスフレーズを囲みます。

   注: パスワードは、Oracle ポリシー ストアに保管する場合を除き、大文字小文字が区別されません。

3. *policy_server_home*¥bin から smreg ユーティリティを削除します。smreg を削除すると、既存のパスワードを把握していない限り、パスワードを変更することはできなくなります。

   デフォルトの SiteMinder 管理者アカウントのパスワードが設定されます。

注: 日常的な作業にはデフォルトのスーパーユーザを使用しないことをお勧めします。デフォルトのスーパーユーザは、以下の場合に使用してください。

- デフォルトのポリシー ストア オブジェクトをインポートする場合。
- FSS 管理 UI および 管理 UI に初めてアクセスする場合。スーパーユーザ権限を持つ別の管理者を作成することをお勧めします。

詳細情報:

インストール メディアの検索 (P. 236)

デフォルトのポリシー ストア オブジェクトのインポート

デフォルトのポリシー ストア オブジェクトをインポートすると、管理 UI で使用するポリシー ストアがセットアップされます。ポリシー ストアにポリシー情報を格納するには、デフォルトのポリシー ストア オブジェクトが必要です。

注: FIPS 専用モードでポリシー サーバをインストールした場合は、デフォルトのポリシー ストア オブジェクトをインポートするときに必ず -cf 引数を使用してください。

デフォルトのポリシー ストア オブジェクトをインポートする方法

1. 以下のコマンドを実行します。

   ```
   smobjimport -ipolicy_server_home¥db¥smdif¥smpolicy.smdif
   -dsiteminder_super_user_name -wsiteminder_super_user_password -v
   ```

   引数にスペースが含まれる場合、引数全体の前後に二重引用符を使用します。

   Windows の例: smobjimport

   ```
   -i"C:¥Program Files¥CA¥siteminder¥db¥smdif¥smpolicy.smdif" -d"SM Admin"
   -wPassword -v
   ```

   UNIX の例: smobjimport

   ```
   -i$NETE_PS_ROOT/db/smdif/smpolicy.smdif -d"SM Admin" -wPassword -v
   ```

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

   -d*siteminder_super_user_name*

   SiteMinder スーパーユーザ アカウントの名前を指定します。

   デフォルト: siteminder

-w*siteminder_super_user_password*

SiteMinder スーパーユーザ アカウントのパスワードを指定します。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト値: stdout

-cf

(任意) FIPS 対応の暗号化を使用して機密データをインポートします。

注: この引数は、ポリシー サーバが FIPS 専用モードで動作している場合にのみ必要です。

smobjimport によって、ポリシー ストア オブジェクトがインポートされます。オブジェクトは、適切な場所に自動的にインポートされます。

2. 以下のコマンドを実行します。

```
smobjimport -ipolicy_server_home¥db¥smdif¥ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

policy_server_home

ポリシー サーバのインストール パスを指定します。

-d*siteminder_super_user_name*

SiteMinder スーパーユーザ アカウントの名前を指定します。

デフォルト: siteminder

-w*siteminder_super_user_password*

SiteMinder スーパーユーザ アカウントのパスワードを指定します。

-f

重複するオブジェクトを上書きします。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト値: stdout

-l

ログ ファイルを作成します。

-c

smdif 入力ファイルに暗号化されていないデータが含まれていることを示します。

smobjimport によって、ポリシー ストア オブジェクトがインポートされます。これらのオブジェクトは、適切な場所に自動的にインポートされます。

注: ampolicy.smdif をインポートすると、Federation セキュリティ サービス、Web サービス変数、および eTelligent ルール機能が使用可能になります。eTelligent ルール機能は、SiteMinder から別個にライセンスが提供されます。この eTelligent ルール機能を使用する予定がある場合は、ライセンスの詳細について、CA アカウント担当者に問い合わせてください。

これで、ポリシー ストア データ定義をインポートできるようになりました。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*¥xps¥dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。

3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   必要なポリシー ストア データ定義がすべてインポートされました。

ポリシー サーバの再起動

ポリシー ストアやその他のデータ ストアの設定を有効にするために、ポリシー サーバを再起動します。

注: UNIX システムでは、stop-all コマンドの後に start-all コマンドを使用することで、ポリシー サーバを再起動できます。

ポリシー サーバを再起動するには、以下の手順に従います。

1. ポリシー サーバ管理コンソールを開きます。
2. [ステータス]タブをクリックし、[ポリシー サーバ]グループ ボックスで[停止]をクリックします。

   赤色の信号アイコンが表示されて、ポリシー サーバが停止します。
3. [開始]をクリックします。

   緑色の信号アイコンが表示されて、ポリシー サーバが起動します。

管理 UI 登録の準備

管理 UI に初めてログインする場合は、デフォルトの SiteMinder スーパーユーザ アカウント(siteminder)を使用します。初めてログインするときは、ポリシー サーバに 管理 UI を登録する必要があります。これで、両方のコンポーネントの間に信頼関係が作成されます。

XPSRegClient ユーティリティを使用してスーパーユーザ アカウントの名前とパスワードを指定して、登録の準備をします。ポリシー サーバは、これらの認証情報を使用して、登録要求が有効であること、および信頼関係を確立できることを検証します。

以下の点について考慮してください。

- 認証情報を指定してから最初の 管理 UI ログインまでの時間は、24 時間に制限されています。24 時間以内に 管理 UI をインストールする予定がない場合は、管理 UI をインストールする前に以下を実行します。
- (UNIX) XPSRegClient を使用する前に、SiteMinder 環境変数が設定されていることを確認してください。環境変数が設定されていない場合は、手動で設定します。

管理 UI 登録を準備する方法

1. ポリシー サーバ ホスト システムにログインします。
2. 以下のコマンドを実行します。

   ```
   XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
   comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

   passphrase

   デフォルトの SiteMinder スーパーユーザ アカウント(siteminder)のパスワードを指定します。

   注: パスフレーズを指定しないと、XPSRegClient により、パスフレーズの入力とその確認を求めるプロンプトが表示されます。

   -adminui–setup

   管理 UI が初めてポリシー サーバに登録されていることを指定します。

-t *timeout*

(任意) 管理 UI をインストールしてから、ログインしてポリシー サーバとの信頼関係を作成するまでの割り当て時間を指定します。タイムアウト値を超過すると、ポリシー サーバは登録リクエストを拒否します。

測定単位: 分

デフォルト: 240 (4 時間)

最小制限: 1

最大制限: 1440 (24 時間)

-r *retries*

(任意) 管理 UI の登録時に許容される試行の失敗回数を指定します。試行に失敗する原因としては、初めて 管理 UI にログインするときに間違った SiteMinder 管理者クレデンシャルをサブミットしたことが考えられます。

デフォルト: 1

最大制限: 5

-c *comment*

(任意) 指定されたコメントを情報目的で登録ログ ファイルに挿入します。

注: コメントは引用符で囲んでください。

-cp

(任意) 登録ログ ファイルに複数行のコメントが含まれることを指定します。ユーティリティにより複数行のコメントが求められ、指定されたコメントが情報目的で登録ログ ファイルに挿入されます。

注: コメントは引用符で囲んでください。

-l *log path*

(任意) 登録ログ ファイルをエクスポートする場所を指定します。

デフォルト: *siteminder_home*¥log

siteminder_home

ポリシー サーバのインストール パスを指定します。

-e *error_path*

(任意) 例外を指定されたパスに送信します。

デフォルト: stderr

-vT

（任意）詳細レベルを TRACE に設定します。

-vI

（任意）詳細レベルを INFO に設定します。

-vW

（任意）詳細レベルを WARNING に設定します。

-vE

（任意）詳細レベルを ERROR に設定します。

-vF

（任意）詳細レベルを FATAL に設定します。

3. Enter キーを押します。

   XPSRegClient は、ポリシー サーバに管理者クレデンシャルを提供します。ポリシー サーバは、管理 UI への最初のログイン時に、登録リクエストを確認するためにこれらのクレデンシャルを使用します。

Red Hat Directory Server への安全な接続を設定する方法

ポリシー サーバから Red Hat ユーザ ストアまたはポリシー ストアへの安全な接続を設定することができます。

ポリシー サーバから Red Hat ユーザ ストアへの安全な接続の設定

ポリシー サーバから Red Hat ユーザ ストアへの安全な接続を設定することができます。

注: ポリシー サーバが FIPS モードで動作し、ディレクトリ接続が安全な SSL 接続である場合、ポリシー サーバとディレクトリ サーバが使用する証明書は FIPS 準拠である必要があります。

ポリシー サーバから Red Hat ユーザ ストアへの安全な接続を設定する方法

1. SSL を使用して Red Hat ユーザ ストアと通信する各コンピュータ上の Netscape cert7.db データベースに、証明機関のルート証明書をインストールします。

   注: ポリシー サーバでは、ルート証明書を Netscape cert7.db 形式にする必要があります。証明書のインストールに Microsoft Internet Explorer を使用しないでください。

2. SiteMinder 管理 UI で、[インフラストラクチャ]-[ディレクトリ]をクリックします。
3. [ユーザ ディレクトリ]-[ユーザ ディレクトリの変更]をクリックします。

   [ユーザ ディレクトリの変更]ペインが開きます。
4. 検索条件を指定して[検索]をクリックします。

   検索条件と一致するユーザ ディレクトリのリストが開きます。

   注: すべてのユーザ ディレクトリを表示するには、検索フィールドを空のままにして、[検索]をクリックします。
5. リストから Red Hat ユーザ ディレクトリを選択し、[OK]をクリックします。

   [ユーザ ディレクトリの変更: 名前]ペインが開きます。
6. [ディレクトリのセットアップ]グループ ボックスの[安全な接続]チェック ボックスをオンにして、[サブミット]をクリックします。

ポリシー サーバから Red Hat ユーザ ストアの間に、安全な接続が設定されます。

ポリシー サーバから Red Hat ポリシー ストアへの安全な接続の設定

ポリシー サーバから Red Hat ポリシー ストアへの安全な接続を設定することができます。

注: ポリシー サーバが FIPS モードで動作し、ディレクトリ接続が安全な SSL 接続である場合、ポリシー サーバとディレクトリ サーバが使用する証明書は FIPS 準拠である必要があります。

ポリシー サーバから Red Hat ポリシー ストアへの安全な接続を設定する方法

1. SSL を使用して Red Hat ポリシー ストアと通信する各コンピュータ上の Netscape cert7.db データベースに、証明機関のルート証明書をインストールします。

   注: ポリシー サーバでは、ルート証明書を Netscape cert7.db 形式にする必要があります。証明書のインストールに Microsoft Internet Explorer を使用しないでください。

2. ポリシー サーバがインストールされているサーバで、ポリシー サーバ管理コンソールを開き、[データ]タブを選択します。
3. [データ]タブで、以下の手順を実行します。
   a. [SSL を使用]チェック ボックスをオンにします。
   b. Netscape 証明書データベース ファイルのフィールドに、cert7.db ファイルのパスを入力します。
4. [適用]をクリックします。

ポリシー サーバから Red Hat ポリシー ストアの間に、安全な接続が設定されます。

第 11 章: Siemens DirX 6.0 D00 Directory Server

このセクションには、以下のトピックが含まれています。

SiteMinder スキーマ ファイルのダウンロード

SiteMinder スキーマを設定するのに必要な 1 つ以上のスキーマ ファイルが、ポリシー サーバ インストールに含まれていません。これらのファイルは CA SiteMinder Tier 2 ディレクトリ製品コンポーネント ダウンロードにあります。

Tier 2 ディレクトリ製品コンポーネントをダウンロードする方法

1. テクニカル サポート サイトにログインします。
2. [Support]の下の[Download Center]をクリックします。

   [Download Center]画面が表示されます。
3. [Select a Product]フィールドに「SiteMinder」と入力します。
4. [Select a Release]リストからリリースを選択します。
5. [Select a Gen Level]リストからサービス パックを選択します。
6. [Go]をクリックします。

   [Product Downloads]画面が表示されます。Tier 2 ディレクトリ コンポーネント ダウンロードはリストの下のほうにあります。
7. zip ファイルをローカルに保存し、ポリシー サーバ ホスト システムにファイルを抽出します。

ポリシー ストアとしての DirX 6.0 D00 Directory Server の設定

Siemens DirX 6.0 D00 Directory Server を SiteMinder r12.0 SP3 ポリシー ストアとして設定することができます。

Siemens DirX 6.0 D00 Directory Server をポリシー ストアとして設定する方法

1. DirX 6.0 D00 をインストールします。インストールする際は、デフォルトをすべて受け入れます。

   注: 既存のデータベースがない場合は、サンプル データベースをインストールしてください。

2. 以下のファイルを、*path*¥dirx から

   DirX_install_path¥scripts¥security¥Netegrity¥SiteMinder にコピーします。

   - dirxabbr-ext.SiteMinderR12sp3
   - schema_ext_for_SiteMinderR12sp3.adm
   - subschema_ext_for_SiteMinderR12sp3.cp
   - bind.tcl
   - l-bind.cp
   - _setup.bat
   - setup.bat
   - GlobalVar.tcl

   重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

   path

   Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。

   DirX_install_path

   DirX のインストール パスを指定します。

   例: C:¥program files¥siemens¥dirx

3. 以下のファイルを、*path*¥xps¥dirx から

   DirX_install_path¥scripts¥security¥Netegrity¥SiteMinder にコピーします。

   - dirxabbr-ext.XPS
   - schema_ext_for_XPS.adm
   - subschema_ext_for_XPS.cp

4. 以下のファイルの名前を変更します。

   - schema_ext_for_SiteMinderR12sp3.adm から schema_ext_for_SiteMinder.adm に変更します。
   - subschema_ext_for_SiteMinderR12sp3.cp から subschema_ext_for_SiteMinder.cp に変更します。

5. 以下のファイルを、*DirX_install_path*¥client¥conf にコピーします。

   - dirxabbr-ext.SiteMinderR12sp3
   - dirxabbr-ext.XPS

6. dirxabbr-ext.SiteMinderR12sp3 の名前を dirxabbr-ext.SiteMinder に変更します。

7. DirX サービスを停止し、再起動します。

8. GlobalVar.tcl を編集して、DirX スクリプトが参照するグローバル変数を更新します。

   デフォルト値:

   - LDAP ポート: 389
   - ルート DN: o=pqr
   - 管理者ユーザ名 : cn=admin、o=pqr
   - 管理者パスワード: dirx

9. setup.bat を実行し、生成されたログ ファイル（setup.log）でエラーを確認します。

10. DirXmanage ツールを使用して、DSA に再バインドします。

    注: エラーに注意してください。

11. DirXmanage ツールを使用して、ベース ツリー構造を作成します。

    a. o=PQR の下に、ou=Netegrity を作成します。

    b. ou=Netegrity の下に、ou=SiteMinder を作成します。

    c. ou=SiteMinder の下に、ou=PolicySvr4 を作成します。

    d. ou=PolicySvr4 の下に ou=XPS を作成します。

    r12.0 SP3 に対するポリシー ストア スキーマが作成されます。

12. ポリシー サーバ管理コンソールの[データ]タブを使用して、ポリシー サーバが DirX Directory Server を参照するようにします。

    サンプル値:

    - LDAP IP アドレス: 123.456.7.8
    - ルート DN: o=pqr
    - 管理者ユーザ名 : cn=admin、o=pqr
    - 管理者パスワード: ********

13. 以下のコマンドを実行します。

    ```
    smreg -su password
    ```

    SiteMinder スーパーユーザ パスワードが設定されます。

14. *policy_server_hom*/bin に移動します。

    policy_server_home

    ポリシー サーバのインストール パスを指定します。

15. 以下のコマンドを実行します。

    ```
    smobjimport -ipolicy_server_home¥db¥smdif¥smpolicy.smdif -v
    -dsiteminder_super_user_name -wsiteminder_super_user_password
    ```

    -i

    インポート ファイルのパスと名前を指定します。

    -v

    トレースをオンにして、エラー メッセージ、警告メッセージ、およびコメント メッセージを出力します。

    注: ログ ファイルに出力して、エラーを確認することができます。

    ベース ポリシー ストア データを、ファイル smpolicy.smdif からインポートします。

16. 以下のコマンドを実行します。

```
smobjimport -ipolicy_server_home¥db¥smdif¥ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

-i

インポート ファイルのパスと名前を指定します。

-d*siteminder_super_user_name*

SiteMinder スーパーユーザ アカウントの名前を指定します。

-w*siteminder_super_user_password*

SiteMinder スーパーユーザ アカウントのパスワードを指定します。

-f

重複するオブジェクトをオーバーライドします。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト値: stdout

-l

ログ ファイルを作成します。

-c

smdif 入力ファイルに暗号化されていないデータが含まれていることを示します。

smobjimport によって、ポリシー ストア オブジェクトがインポートされます。これらのオブジェクトは、適切な場所に自動的にインポートされます。

注: ampolicy.smdif をインポートすると、Federation セキュリティ サービス、Web サービス変数、および eTelligent ルール機能が使用可能になります。eTelligent ルール機能は、SiteMinder から別個にライセンスが提供されます。この eTelligent ルール機能を使用する予定がある場合は、ライセンスの詳細について、CA アカウント担当者に問い合わせてください。

DirX Directory Server がポリシー ストアとして設定されます。

注: これで、ポリシー ストア データ定義をインポートできます。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*¥xps¥dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。
2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。
3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。
4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。
5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   必要なポリシー ストア データ定義がすべてインポートされました。

管理 UI 登録の準備

管理 UI に初めてログインする場合は、デフォルトの SiteMinder スーパーユーザ アカウント(siteminder)を使用します。初めてログインするときは、ポリシー サーバに 管理 UI を登録する必要があります。これで、両方のコンポーネントの間に信頼関係が作成されます。

XPSRegClient ユーティリティを使用してスーパーユーザ アカウントの名前とパスワードを指定して、登録の準備をします。ポリシー サーバは、これらの認証情報を使用して、登録要求が有効であること、および信頼関係を確立できることを検証します。

以下の点について考慮してください。

- 認証情報を指定してから最初の 管理 UI ログインまでの時間は、24 時間に制限されています。24 時間以内に 管理 UI をインストールする予定がない場合は、管理 UI をインストールする前に以下を実行します。
- (UNIX) XPSRegClient を使用する前に、SiteMinder 環境変数が設定されていることを確認してください。環境変数が設定されていない場合は、手動で設定します。

管理 UI 登録を準備する方法

1. ポリシー サーバ ホスト システムにログインします。
2. 以下のコマンドを実行します。

   ```
   XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
   comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
   ```

   passphrase

   デフォルトの SiteMinder スーパーユーザ アカウント(siteminder)のパスワードを指定します。

   注: パスフレーズを指定しないと、XPSRegClient により、パスフレーズの入力とその確認を求めるプロンプトが表示されます。

   -adminui–setup

   管理 UI が初めてポリシー サーバに登録されていることを指定します。

-t *timeout*

(任意) 管理 UI をインストールしてから、ログインしてポリシー サーバとの信頼関係を作成するまでの割り当て時間を指定します。タイムアウト値を超過すると、ポリシー サーバは登録リクエストを拒否します。

測定単位: 分

デフォルト: 240 (4 時間)

最小制限: 1

最大制限: 1440 (24 時間)

-r *retries*

(任意) 管理 UI の登録時に許容される試行の失敗回数を指定します。試行に失敗する原因としては、初めて 管理 UI にログインするときに間違った SiteMinder 管理者クレデンシャルをサブミットしたことが考えられます。

デフォルト: 1

最大制限: 5

-c *comment*

(任意) 指定されたコメントを情報目的で登録ログ ファイルに挿入します。

注: コメントは引用符で囲んでください。

-cp

(任意) 登録ログ ファイルに複数行のコメントが含まれることを指定します。ユーティリティにより複数行のコメントが求められ、指定されたコメントが情報目的で登録ログ ファイルに挿入されます。

注: コメントは引用符で囲んでください。

-l *log path*

(任意) 登録ログ ファイルをエクスポートする場所を指定します。

デフォルト: *siteminder_home*¥log

siteminder_home

ポリシー サーバのインストール パスを指定します。

-e *error_path*

(任意) 例外を指定されたパスに送信します。

デフォルト: stderr

-vT

（任意）詳細レベルを TRACE に設定します。

-vI

（任意）詳細レベルを INFO に設定します。

-vW

（任意）詳細レベルを WARNING に設定します。

-vE

（任意）詳細レベルを ERROR に設定します。

-vF

（任意）詳細レベルを FATAL に設定します。

3. Enter キーを押します。

   XPSRegClient は、ポリシー サーバに管理者クレデンシャルを提供します。ポリシー サーバは、管理 UI への最初のログイン時に、登録リクエストを確認するためにこれらのクレデンシャルを使用します。

ユーザ ディレクトリの設定例 - Siemens DirX 6.0

以下に、ユーザ ディレクトリの設定例を示します。

ディレクトリのセットアップ

- ネームスペース: LDAP
- サーバ: 123.456.7.8
- ルート: o=pqr
- DN 検索の先頭文字列: (cn=)
- DN 検索の終端文字列:)

認証情報と接続

- 管理者ユーザ名 : cn=admin、o=pqr
- 管理者パスワード: dirx

ユーザ属性

- ユニバーサル ID (R): cn
- 無効フラグ (RW): description
- パスワードの属性 (RW): userpassword
- パスワード データ (RW): audio
- チャレンジ/レスポンス (RW): jpegPhoto

注: 前述のユーザ属性は、DirX でユーザ オブジェクトに追加せずに使用することができます。

注: DMS のユーザ属性名に大文字小文字の区別があるかどうかは、属性単位で異なります。

6.x ポリシー ストアをアップグレードする方法

r12.0 SP3 ポリシー ストアに、新規のディレクトリ サーバ インスタンスは必要ありません。既存のポリシー ストアを r12.0 SP3 にアップグレードできます。

ポリシー ストアをアップグレードするには、以下の手順を実行します。

1. ポリシー ストア スキーマを拡張します。

   注:既存の r6.x ポリシー ストア スキーマは、変更されていません。r12.0 SP3 の移行では、ポリシー ストア スキーマをアップグレードして、r12.0 SP3 によって必要とされるオブジェクトのポリシー ストアを拡張する必要があります。

2. ベース ポリシー ストア オブジェクトをインポートします。
3. ポリシー ストア データ定義をインポートします。

注: サポート マトリックスにリストされているディレクトリ サーバまたはデータベースで、本書に記載されていないものをアップグレードする場合は、「SiteMinder アップグレード ガイド」を参照してください。

Siemens DirX ポリシー ストア スキーマの拡張

r12.0 SP3 によって導入されたオブジェクトを含めるように既存の 6.x ポリシー ストア スキーマを拡張することができます。既存の 6.x ポリシー ストア スキーマに加える変更はありません。

既存の Siemens DirX ポリシー ストア スキーマを拡張する方法

1. DirXmanage ツールを使用して、ベース ツリー構造を更新します。u=PolicySvr4 の下に ou=XPS を作成します。
2. 以下のファイルを、*path*¥xps¥dirx から

   DirX_install_path¥scripts¥security¥Netegrity¥SiteMinder にコピーします。

   - _setup.bat
   - bind.tcl
   - dirxabbr-ext.XPS
   - GlobalVar.tcl
   - l-bind.cp
   - schema_ext_for_XPS.adm
   - setup.bat
   - subschema_ext_for_XPS.cp

   path

   Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。

   DirX_install_path

   DirX のインストール パスを指定します。

   例: C:¥program files¥siemens¥dirx
3. dirxabbr-ext.XPS を *DirX_install_path*¥client¥conf にコピーします。
4. DirX サービスを停止し、再起動します。
5. GlobalVar.tcl を編集して、DirX スクリプトが参照するグローバル変数を更新します。

   デフォルト値:

   - LDAP ポート: 389
   - ルート DN: o=pqr

- 管理者ユーザ名 : cn=admin、o=pqr
- 管理者パスワード : dirx

6. setup.bat を実行し、生成されたログ ファイル（setup.log）でエラーを確認します。
7. DirXmanage ツールを使用して、DSA に再バインドします。

   注: エラーに注意してください。

r12.0 SP3 によって導入されたオブジェクトを含めるようにポリシー ストア スキーマが拡張されます。

ベース ポリシー ストア オブジェクトのインポート

デフォルトの SiteMinder オブジェクトをインポートすると、管理 UI で使用するポリシー ストアがアップグレードされます。デフォルトの SiteMinder オブジェクトは、ポリシー ストアにポリシー情報を格納するために必要です。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. 以下のコマンドを実行します。

```
smobjimport -ipolicy_server_home¥db¥smdif¥upgrade_smdif_file_name
-dsiteminder_super_user_name -wsiteminder_super_user_password
-v -f
```

policy_server_home

ポリシー サーバのインストール パスを指定します。

upgrade_smdif_file_name

インポート ファイルの名前を指定します。

- **r60 から r12.0 SP3:** sm_upgrade_60_to_R12sp3.smdif
- **r60 SP1 から r12.0 SP3:** sm_upgrade_60sp1_to_R12sp3.smdif
- **r60 SP2 から r12.0 SP3:** sm_upgrade_60sp2_to_R12sp3.smdif

- **r60 SP3 から r12.0 SP3:** sm_upgrade_60sp3_to_R12sp3.smdif
- **r60 SP4 から r12.0 SP3:** sm_upgrade_60sp4_to_R12sp3.smdif
- **r60 SP5 から r12.0 SP3:** sm_upgrade_60sp5_to_R12sp3.smdif
- **r60 SP6 から r12.0 SP3:** sm_upgrade_60sp6_to_r12sp3.smdif

-d*siteminder_super_user_name*

SiteMinder 管理者アカウントの名前を指定します。

-w*siteminder_super_user_password*

SiteMinder 管理者アカウントのパスワードを指定します。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト出力: stdout

-f

重複するポリシー ストア オブジェクトを、r12.0 SP3 のもので上書きします。

引数にスペースが含まれる場合、引数全体の前後に二重引用符を使用します。

Windows の例: smobjimport

```
-i"C:¥Program Files¥CA¥siteminder¥db¥smdif¥smpolicy.smdif" -d"SM Admin"
-wPassword -v
```

UNIX の例: smobjimport

-i$NETE_PS_ROOT/db/smdif/smpolicy.smdif -d"SM Admin" -wPassword -v

ベース ポリシー ストア オブジェクトがインポートされます。

2. 以下のコマンドを実行します。

重要: ampolicy.smdif が以前にポリシー ストアにインポートされている場合は再インポートしないでください。

```
smobjimport -ipolicy_server_home¥db¥smdif¥ampolicy.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
```

-policy_server_home

インポート ファイルのパスと名前を指定します。

-d*siteminder_super_user_name*

SiteMinder 管理者アカウントの名前を指定します。

-w*siteminder_super_user_password*

SiteMinder 管理者アカウントのパスワードを指定します。

-f

重複するオブジェクトを上書きします。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト値: stdout

-l

ログ ファイルを作成します。

-c

smdif 入力ファイルに暗号化されていないデータが含まれていることを示します。

注: ampolicy.smdif をインポートすると、SiteMinder から別々にライセンスされるフェデレーション セキュリティ サービス、Web サービス変数、および eTelligent ルール機能が使用可能になります。eTelligent ルール機能を使用する予定の場合は、ライセンス情報について CA ジャパン ダイレクトに問い合わせてください。

これで、ポリシー ストア データ定義をインポートできるようになりました。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*¥xps¥dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。
2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。
3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。
4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。
5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   必要なポリシー ストア データ定義がすべてインポートされました。

第 12 章: Siemens DirX EE 2.0 Directory Server

このセクションには、以下のトピックが含まれています。

Siemens DirX EE 2.0 ポリシー ストアを設定する方法

Siemens DirX EE 2.0 Directory Server を r12.0 SP3 ポリシー ストアとして設定するには、以下の手順を実行します。

1. SiteMinder スキーマ ファイルをダウンロードします。
2. ポリシー ストアとして DirX EE 2.0 Directory Server を設定します。
3. ポリシー ストア データ定義をインポートします。
4. 管理 UI の登録を準備します。

SiteMinder スキーマ ファイルのダウンロード

SiteMinder スキーマを設定するのに必要な 1 つ以上のスキーマ ファイルが、ポリシー サーバ インストールに含まれていません。これらのファイルは CA SiteMinder Tier 2 ディレクトリ製品コンポーネント ダウンロードにあります。

Tier 2 ディレクトリ製品コンポーネントをダウンロードする方法

1. テクニカル サポート サイトにログインします。
2. [Support]の下の[Download Center]をクリックします。

   [Download Center]画面が表示されます。
3. [Select a Product]フィールドに「SiteMinder」と入力します。
4. [Select a Release]リストからリリースを選択します。
5. [Select a Gen Level]リストからサービス パックを選択します。

6. ［Go］をクリックします。

   ［Product Downloads］画面が表示されます。Tier 2 ディレクトリ コンポーネント ダウンロードはリストの下のほうにあります。

7. zip ファイルをローカルに保存し、ポリシー サーバ ホスト システムにファイルを抽出します。

r12.0 SP3 ポリシー ストアとしての DirX EE 2.0 Directory Server の設定

Siemens DirX EE 2.0 Directory Server を r12.0 SP3 ポリシー ストアとして設定する方法

1. DirX EE 2.0 をインストールします。
2. DirX EE Manager を開き、ポリシー ストア データを保持する以下のベース ツリー構造を作成します。
   a. o=MyCompany の下に、ou=netegrity を作成します。
   b. ou=netegrity の下に、ou=Siteminder を作成します。
   c. ou=Siteminder の下に、ou=PolicySvr4 を作成します。
   d. u=PolicySvr4 の下に ou=XPS を作成します。
3. 以下のファイルを、*path*¥dirxee20 から

   DirX_EE_install_path¥scripts¥stand_alone¥extensions にコピーします。

   - DirXEE20_SMR12sp3_Schema.ldif
   - add_PS_Indexes.adm

   path

   Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。

   DirX_EE_install_path

   DirX EE のインストール パスを指定します。
4. 以下のファイルを、*path*¥xps¥dirxee20 から *DirX_EE_install_path*¥scripts¥stand_alone¥extensions にコピーします。
   - XPS_SchemaExt.ldif
   - add_XPS_Indexes.adm
5. コマンド プロンプトから、以下のディレクトリに変更します。

   DirX_EE_install_path¥scripts¥stand_alone¥extensions

6. 以下のコマンドを実行します。

   dirxmodify -f DirXEE20_SMR12sp3_Schema.ldif -D cn=admin,o=MyCompany -w dirx

   -f

   LDIF ファイルの名前を指定します。

   -D

   バインド DN を指定します。

   例: cn=admin,o=MyCompany

   -w

   パスワードを指定します。

   例: dirx

   -h

   (任意)ホストを指定します。

   デフォルト: localhost

   -p

   (任意)ポート番号を指定します。

   デフォルト: 389

7. 以下のコマンドを実行します。

   dirxadm add_PS_Indexes.adm

8. 以下のコマンドを実行します。

   dirxmodify -f XPS_SchemaExt.ldif -D cn=admin,o=MyCompany -w dirx

9. 以下のコマンドを実行します。

   dirxadm add_XPS_Indexes.adm

   XPS スキーマが作成されます。

10. ポリシー サーバ管理コンソールを開き、[データ]タブをクリックして、タブのフィールドに以下の情報を指定します。

    - LDAP IP アドレス

      ポリシー ストアの IP アドレスを指定します。

    - ルート DN

      例: o=MyCompany

- 管理者ユーザ名

  例: cn=admin,o=MyCompany

- パスワード

  例: dirx

ポリシー サーバは DirX EE ポリシー ストアを参照します。

11. 以下のコマンドを実行します。

    smreg –su *password*

    SiteMinder 管理者パスワードが設定されます。

12. 以下のコマンドを実行します。

    smobjimport –i*policy_server_home*¥db¥smdif¥smpolicy.smdif –v

    -d*siteminder_super_user_name* -w*siteminder_super_user_password*

    policy_server_home

    ポリシー サーバのインストール パスを指定します。

    -i

    インポート ファイルのパスと名前を指定します。

    -v

    トレースをオンにして、エラー メッセージ、警告メッセージ、およびコメント メッセージを出力します。

    注: ログ ファイルに出力して、エラーを確認することができます。

    ベース ポリシー ストア データが、ファイル smpolicy.smdif から DirX EE ポリシー ストアにインポートされます。

13. 以下のコマンドを実行します。

    smobjimport -i*policy_server_home*¥db¥smdif¥ampolicy.smdif
    -d*siteminder_super_user_name* -w*siteminder_super_user_password* -f -v -l -c

    -i

    インポート ファイルのパスと名前を指定します。

    -d*siteminder_super_user_name*

    SiteMinder スーパーユーザ アカウントの名前を指定します。

    -w*siteminder_super_user_password*

    SiteMinder スーパーユーザ アカウントのパスワードを指定します。

-f

重複するオブジェクトをオーバーライドします。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト値: stdout

-l

ログ ファイルを作成します。

-c

smdif 入力ファイルに暗号化されていないデータが含まれていることを示します。

注: ampolicy.smdif をインポートすると、Federation セキュリティ サービス、Web サービス変数、および eTelligent ルール機能が使用可能になります。eTelligent ルール機能は、SiteMinder から別個にライセンスが提供されます。eTelligent ルール機能を使用する予定の場合は、CA 担当者までお問い合わせください。

これで、ポリシー ストア データ定義をインポートできるようになりました。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*¥xps¥dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。

3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   必要なポリシー ストア データ定義がすべてインポートされました。

管理 UI 登録の準備

管理 UI に初めてログインする場合は、デフォルトの SiteMinder スーパーユーザ アカウント(siteminder)を使用します。初めてログインするときは、ポリシー サーバに 管理 UI を登録する必要があります。これで、両方のコンポーネントの間に信頼関係が作成されます。

XPSRegClient ユーティリティを使用してスーパーユーザ アカウントの名前とパスワードを指定して、登録の準備をします。ポリシー サーバは、これらの認証情報を使用して、登録要求が有効であること、および信頼関係を確立できることを検証します。

以下の点について考慮してください。

- 認証情報を指定してから最初の 管理 UI ログインまでの時間は、24 時間に制限されています。24 時間以内に 管理 UI をインストールする予定がない場合は、管理 UI をインストールする前に以下を実行します。
- （UNIX）XPSRegClient を使用する前に、SiteMinder 環境変数が設定されていることを確認してください。環境変数が設定されていない場合は、手動で設定します。

管理 UI 登録を準備する方法

1. ポリシー サーバ ホスト システムにログインします。
2. 以下のコマンドを実行します。

```
XPSRegClient siteminder[:passphrase] -adminui-setup -t timeout -r retries -c
comment -cp -l log_path -e error_path -vT -vI -vW -vE -vF
```

passphrase

デフォルトの SiteMinder スーパーユーザ アカウント（siteminder）のパスワードを指定します。

注：パスフレーズを指定しないと、XPSRegClient により、パスフレーズの入力とその確認を求めるプロンプトが表示されます。

-adminui–setup

管理 UI が初めてポリシー サーバに登録されていることを指定します。

-t *timeout*

（任意）管理 UI をインストールしてから、ログインしてポリシー サーバとの信頼関係を作成するまでの割り当て時間を指定します。タイムアウト値を超過すると、ポリシー サーバは登録リクエストを拒否します。

測定単位： 分

デフォルト： 240（4 時間）

最小制限： 1

最大制限： 1440（24 時間）

-r *retries*

(任意) 管理 UI の登録時に許容される試行の失敗回数を指定します。試行に失敗する原因としては、初めて 管理 UI にログインするときに間違った SiteMinder 管理者クレデンシャルをサブミットしたことが考えられます。

デフォルト: 1

最大制限: 5

-c *comment*

(任意) 指定されたコメントを情報目的で登録ログ ファイルに挿入します。

注: コメントは引用符で囲んでください。

-cp

(任意) 登録ログ ファイルに複数行のコメントが含まれることを指定します。ユーティリティにより複数行のコメントが求められ、指定されたコメントが情報目的で登録ログ ファイルに挿入されます。

注: コメントは引用符で囲んでください。

-l *log path*

(任意) 登録ログ ファイルをエクスポートする場所を指定します。

デフォルト: *siteminder_home*¥log

siteminder_home

ポリシー サーバのインストール パスを指定します。

-e *error_path*

(任意) 例外を指定されたパスに送信します。

デフォルト: stderr

-vT

(任意) 詳細レベルを TRACE に設定します。

-vI

（任意）詳細レベルを INFO に設定します。

-vW

（任意）詳細レベルを WARNING に設定します。

-vE

（任意）詳細レベルを ERROR に設定します。

-vF

（任意）詳細レベルを FATAL に設定します。

3. Enter キーを押します。

   XPSRegClient は、ポリシー サーバに管理者クレデンシャルを提供します。ポリシー サーバは、管理 UI への最初のログイン時に、登録リクエストを確認するためにこれらのクレデンシャルを使用します。

6.x ポリシー ストアをアップグレードする方法

r12.0 SP3 ポリシー ストアに、新規のディレクトリ サーバ インスタンスは必要ありません。既存のポリシー ストアを r12.0 SP3 にアップグレードできます。

ポリシー ストアをアップグレードするには、以下の手順を実行します。

1. ポリシー ストア スキーマを拡張します。

   注：既存の r6.x ポリシー ストア スキーマは、変更されていません。r12.0 SP3 の移行では、ポリシー ストア スキーマをアップグレードして、r12.0 SP3 によって必要とされるオブジェクトのポリシー ストアを拡張する必要があります。

2. ベース ポリシー ストア オブジェクトをインポートします。
3. ポリシー ストア データ定義をインポートします。

注：サポート マトリックスにリストされているディレクトリ サーバまたはデータベースで、本書に記載されていないものをアップグレードする場合は、「SiteMinder アップグレード ガイド」を参照してください。

6.x から r12.0 SP3 への DirX EE 2.0 ポリシー ストアのアップグレード

6.x のポリシー ストアから r12.0 SP3 のポリシー ストアに Siemens DirX EE 2.0 Directory Server をアップグレードするには、ポリシー ストアに XPS スキーマを作成します。

DirX EE 2.0 ポリシー ストアを 6.x から r12.0 SP3 にアップグレードする方法

1. DirX EE Manager を開き、ベース ツリー構造を更新します。u=PolicySvr4 の下に ou=XPS を作成します。
2. 以下のファイルを、*path*¥dirxee20 から *DirX_EE_install_path*¥scripts¥stand_alone¥extensions にコピーします。

   add_PS_Indexes.adm

   path

   Tier 2 ディレクトリ zip から抽出されたスキーマ ファイルへのパスを指定します。

   DirX_EE_install_path

   DirX EE のインストール パスを指定します。
3. 以下のファイルを、*path*¥xps¥dirxee20 から *DirX_EE_install_path*¥scripts¥stand_alone¥extensions にコピーします。
   - XPS_SchemaExt.ldif
   - add_XPS_Indexes.adm
4. コマンド プロンプトから、以下のディレクトリに変更します。

   DirX_EE_install_path¥scripts¥stand_alone¥extensions
5. 以下のコマンドを実行します。

   dirxadm add_PS_Indexes.adm
6. 以下のコマンドを実行します。

   dirxmodify -f XPS_SchemaExt.ldif -D cn=admin,o=MyCompany -w dirx

   -f

   LDIF ファイルの名前を指定します。

   -D

   バインド DN を指定します。

   例: cn=admin,o=MyCompany

-w

パスワードを指定します。

例: dirx

-h

(任意)ホストを指定します。

デフォルト: localhost

-p

(任意)ポート番号を指定します。

デフォルト: 389

7. 以下のコマンドを実行します。

   dirxadm add_XPS_Indexes.adm

XPS スキーマが作成されます。これで、ポリシー ストア データ定義をインポートできるようになりました。

ベース ポリシー ストア オブジェクトのインポート

デフォルトの SiteMinder オブジェクトをインポートすると、管理 UI で使用するポリシー ストアがアップグレードされます。デフォルトの SiteMinder オブジェクトは、ポリシー ストアにポリシー情報を格納するために必要です。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. 以下のコマンドを実行します。

   ```
   smobjimport -ipolicy_server_home¥db¥smdif¥upgrade_smdif_file_name
   -dsiteminder_super_user_name -wsiteminder_super_user_password
   -v -f
   ```

   policy_server_home

   ポリシー サーバのインストール パスを指定します。

upgrade_smdif_file_name

インポート ファイルの名前を指定します。

- **r60 から r12.0 SP3:** sm_upgrade_60_to_R12sp3.smdif
- **r60 SP1 から r12.0 SP3:** sm_upgrade_60sp1_to_R12sp3.smdif
- **r60 SP2 から r12.0 SP3:** sm_upgrade_60sp2_to_R12sp3.smdif
- **r60 SP3 から r12.0 SP3:** sm_upgrade_60sp3_to_R12sp3.smdif
- **r60 SP4 から r12.0 SP3:** sm_upgrade_60sp4_to_R12sp3.smdif
- **r60 SP5 から r12.0 SP3:** sm_upgrade_60sp5_to_R12sp3.smdif
- **r60 SP6 から r12.0 SP3:** sm_upgrade_60sp6_to_r12sp3.smdif

-d*siteminder_super_user_name*

SiteMinder 管理者アカウントの名前を指定します。

-w*siteminder_super_user_password*

SiteMinder 管理者アカウントのパスワードを指定します。

-v

追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

デフォルト出力: stdout

-f

重複するポリシー ストア オブジェクトを、r12.0 SP3 のもので上書きします。

引数にスペースが含まれる場合、引数全体の前後に二重引用符を使用します。

Windows の例: smobjimport

```
-i"C:¥Program Files¥CA¥siteminder¥db¥smdif¥smpolicy.smdif" -d"SM Admin"
-wPassword -v
```

UNIX の例: smobjimport

-i$NETE_PS_ROOT/db/smdif/smpolicy.smdif -d"SM Admin" -wPassword -v

ベース ポリシー ストア オブジェクトがインポートされます。

2. 以下のコマンドを実行します。

   重要: ampolicy.smdif が以前にポリシー ストアにインポートされている場合は再インポートしないでください。

   ```
   smobjimport -ipolicy_server_home¥db¥smdif¥ampolicy.smdif
   -dsiteminder_super_user_name -wsiteminder_super_user_password -f -v -l -c
   ```

   -policy_server_home

   インポート ファイルのパスと名前を指定します。

   -d*siteminder_super_user_name*

   SiteMinder 管理者アカウントの名前を指定します。

   -w*siteminder_super_user_password*

   SiteMinder 管理者アカウントのパスワードを指定します。

   -f

   重複するオブジェクトを上書きします。

   -v

   追跡を有効にし、エラー、警告、およびコメント メッセージを詳細形式で出力して、インポートのステータスを監視できるようにします。

   デフォルト値: stdout

   -l

   ログ ファイルを作成します。

   -c

   smdif 入力ファイルに暗号化されていないデータが含まれていることを示します。

   注: ampolicy.smdif をインポートすると、SiteMinder から別々にライセンスされるフェデレーション セキュリティ サービス、Web サービス変数、および eTelligent ルール機能が使用可能になります。eTelligent ルール機能を使用する予定の場合は、ライセンス情報について CA ジャパン ダイレクトに問い合わせてください。

これで、ポリシー ストア データ定義をインポートできるようになりました。

ポリシー ストア データ定義のインポート

ポリシー ストア データ定義のインポートは、管理 UI でポリシー ストアを使用するために必要です。ベース定義は、ポリシー ストア データを記述します。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ベース ポリシー ストア オブジェクトをインポートする方法

1. コマンド ウィンドウを開いて、以下のいずれかの場所に移動します。
   - **Windows** - *policy_server_home*¥xps¥dd
   - **UNIX** - *policy_server_home*/xps/dd

   policy_server_home

   ポリシー サーバのインストール パスを指定します。
2. 以下のコマンドを実行します。

   重要: XPSDDInstall ツールは、データ定義ファイルを使用して以下の順序で実行します。それ以外の順序で実行すると、インポートは失敗します。

   ```
   XPSDDInstall SmObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。

   注: 初めてこのファイルをインポートする場合は、ポリシー データが見つからないという警告メッセージが表示されます。これは予期された動作で、インポートに影響しません。
3. 以下のコマンドを実行します。

   ```
   XPSDDInstall EPMObjects.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。
4. 以下のコマンドを実行します。

   ```
   XPSDDInstall SecCat.xdd
   ```

   XPSDDInstall は必要なデータ定義をインポートします。
5. 以下のコマンドを実行します。

   ```
   XPSDDInstall FssSmObjects.xdd
   ```

   必要なポリシー ストア データ定義がすべてインポートされました。

付録 A: SiteMinder の SSL 接続の設定

このセクションには、以下のトピックが含まれています。

SSL を使った LDAP ユーザ ディレクトリ接続を設定する方法

LDAP ユーザ ディレクトリの SSL 接続を設定するには、証明書データベース ファイルを使用するように SiteMinder を設定する必要があります。

SSL 接続を設定するには、以下の手順に従います。

1. SSL 接続を設定する前に以下を実行します。
2. NSS ユーティリティをインストールします。
3. 証明書データベース ファイルを作成します。
4. 証明書データベースに証明機関（CA）を追加します。
5. 証明書データベースにサーバ証明書を追加します。
6. 証明書データベース内の証明書を一覧表示します。
7. ユーザ ディレクトリの SSL 接続を設定します。
8. ポリシー サーバが証明書データベースを参照するようにします。
9. SSL 接続を検証します。

SSL 接続を設定する前に

SSL による LDAP ユーザ ディレクトリ接続を設定する前に、以下の点を確認してください。

- ディレクトリ サーバが SSL 対応であること。

  注: SSL を介して通信するようにディレクトリ サーバを設定する方法の詳細については、ベンダー別の資料を参照してください。

- SiteMinder は、Netscape LDAP SDK を使用して、LDAP ディレクトリと通信します。その結果、SiteMinder では、データベース ファイルを Netscape バージョン ファイル形式(cert7.db)にする必要があります。

  重要: cert7.db データベース ファイルへの証明書のインストールに Microsoft Internet Explorer を使用しないでください。

- SSL 証明書の管理には、Netscape と互換性のある、サードパーティの証明書ユーティリティが必要です。Mozilla® Network Security Services(NSS)ユーティリティ、バージョン 3.2.2 の使用をお勧めします。

  注: cert7.db 形式をサポートするには、バージョン 3.2.2 が必要です。それ以降のバージョンを使用しないでください。

- (Active Directory)以下の点を考慮してください。
  - SiteMinder ユーザ ディレクトリ接続が AD ネームスペースを使用して設定されている場合は、以下のプロセスは適用されません。SSL 接続を確立するときに、AD ネームスペースは、ネイティブの Windows 証明書リポジトリを使用します。SSL を介して通信するように AD ネームスペースを設定する場合は、以下の点を確認してください。
    - SiteMinder ユーザ ディレクトリ接続が、安全な接続になるように設定されていること。詳細については、「ユーザ (P. 232)ディレクトリの SSL 接続の設定」を参照してください。
    - Active Directory インスタンスをホストしているマシンで、ルート CA 証明書およびサーバ証明書が、サービスの証明書ストアに追加されていること。

    注: SSL を介して通信するように Active Directory を設定する方法の詳細については、Microsoft の資料を参照してください。
  - SiteMinder ユーザ ディレクトリ接続が LDAP ネームスペースを使用して設定されている場合は、以下のプロセスを実行して、SSL 接続を設定します。

NSS ユーティリティのインストール

証明書データベース ファイルを管理する NSS ユーティリティをインストールします。

注: Netscape Portable Runtime（NSPR）またはポリシー サーバがインストールされているシステムに、このユーティリティをインストールします。システムに、どちらかのコンポーネントと一緒にこのユーティリティをインストールすると、必要な DLL または共有オブジェクトが使用可能になります。

NSS ユーティリティをインストールする方法

1. Mozilla NSS 3.2.2 FTP サイトにアクセスします。
2. ご使用のオペレーティング システムに対応する zip または tar をダウンロードします。

   注: Windows Server 2003 用の zip は用意されていません。Windows NT 用の zip をダウンロードしてください。
3. 証明書データベース ファイルを管理しているシステム上の一時ロケーションに、NSS ユーティリティを解凍します。

証明書データベース ファイルの作成

ポリシー サーバでは、証明書データベース ファイルを Netscape バージョン ファイル形式(cert7.db)にする必要があります。NSS ユーティリティを使用して、証明書データベース ファイルを作成することができます。

注: 以下の手順では、タスクを実行するための具体的なオプションおよび引数について詳しく説明します。NSS ユーティリティのオプションおよび引数の全リストについては、NSS プロジェクト ページにある Mozilla マニュアルを参照してください。

証明書データベース ファイルを作成する方法

1. コマンド プロンプトから、NSS ユーティリティを解凍したロケーション内の bin ディレクトリに移動します。

   例: C:¥nss¥bin

   注: Windows には固有の certutil ユーティリティがあります。NSS ユーティリティの bin ディレクトリから作業するようにしてください。間違えて Windows certutil ユーティリティを実行していることがあります。

2. 以下のコマンドを入力します。

   `certutil -N -d certificate_database_directory`

   -N

   cert7.db、key3.db、および secmod.db の証明書データベース ファイルを作成します。

   -d *certificate_database_directory*

   NSS ユーティリティが証明書データベース ファイルを作成するディレクトリを指定します。

   注: ファイル パスにスペースがある場合は、そのパスを引用符で囲んでください。

   このユーティリティは、データベース キーを暗号化するためにパスワードの入力を求めます。

3. パスワードを入力および確認します。

   NSS は、必要な証明書データベース ファイルを作成します。

   - cert7.db
   - key3.db
   - secmod.db

例: 証明書データベース ファイルの作成

```
certutil -N -d C:¥certdatabase
```

証明書データベースへのルート証明機関の追加

ルート証明機関(CA)を追加して、SSL 通信で使用できるようにします。

注: 以下の手順では、タスクを実行するための具体的なオプションおよび引数について詳しく説明します。NSS ユーティリティのオプションおよび引数の全リストについては、NSS プロジェクト ページにある Mozilla マニュアルを参照してください。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

証明書データベースにルート CA 証明書を追加する方法

1. コマンド プロンプトから、NSS ユーティリティを解凍したロケーション内の bin ディレクトリに移動します。

   例: C:¥nss¥bin

   注: Windows には固有の certutil ユーティリティがあります。NSS ユーティリティの bin ディレクトリから作業するようにしてください。間違えて Windows certutil ユーティリティを実行していることがあります。

2. 以下のコマンドを実行して、データベース ファイルにルート CA を追加します。

   ```
   certutil -A -n alias -t trust_arguments -i root_CA_path -d
   certificate_database_directory
   ```

   -A

   証明書データベースに証明書を追加します。

   -n *alias*

   証明書の別名を指定します。

   注: 別名にスペースがある場合は、その別名を引用符で囲んでください。

   -t *trust_arguments*

   証明書データベースに証明書を追加するときに証明書に適用する信頼性属性を指定します。各証明書には、3 つの使用可能な信頼性カテゴリがあります。これらのカテゴリを表記する順序は、「SSL、電子メール、オブジェクト署名」です。ルート CA が信頼されて SSL 証明書を発行できるように、適切な信頼性引数を指定します。それぞれのカテゴリ位置に、以下の属性引数を 0 個以上使用することができます。

   p

   有効なピア。

   P

   信頼されたピア。この引数は p を意味します。

   c

   有効な CA。

   T

   クライアント証明書を発行する信頼された CA。この引数は c を意味します。

   C

   サーバ証明書を発行する信頼された CA（SSL のみ）。この引数は c を意味します。

   重要: これは SSL 信頼性カテゴリに必須の引数です。

   u

   証明書は認証または署名に使用できます。

-i *root_CA_path*

ルート CA ファイルのパスを指定します。以下の点について考慮してください。

- パスには証明書名も含める必要があります。
- 証明書の有効な拡張子には、.cert、.cer、および .pem があります。

注: ファイル パスにスペースがある場合は、そのパスを引用符で囲んでください。

-d *certificate_database_directory*

証明書データベースが入っているディレクトリのパスを指定します。

注: ファイル パスにスペースがある場合は、そのパスを引用符で囲んでください。

NSS によって、証明書データベースにルート CA が追加されます。

例: 証明書データベースへのルート CA の追加

```
certutil -A -n "My Root CA"  -t "C,," -i C:¥certificates¥cacert.cer -d C:¥certdatabase
```

証明書データベースへのサーバ証明書の追加

証明書データベースにサーバ証明書を追加して、SSL 通信で使用できるようにします。

注: 以下の手順では、タスクを実行するための具体的なオプションおよび引数について詳しく説明します。NSS ユーティリティのオプションおよび引数の全リストについては、NSS プロジェクト ページにある Mozilla マニュアルを参照してください。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

証明書データベースにサーバ証明書を追加する方法

1. コマンド プロンプトから、NSS ユーティリティを解凍したロケーション内の bin ディレクトリに移動します。

   例: C:¥nss¥bin

   注: Windows には固有の certutil ユーティリティがあります。NSS ユーティリティの bin ディレクトリから作業するようにしてください。間違えて Windows certutil ユーティリティを実行していることがあります。

2. 以下のコマンドを実行して、データベース ファイルにルート証明書を追加します。

   `certutil -A -n alias -t trust_arguments -i server_certificate_path -d certificate_database_directory`

   -A

   証明書データベースに証明書を追加します。

   -n *alias*

   証明書の別名を指定します。

   注: 別名にスペースがある場合は、その別名を引用符で囲んでください。

   -t *trust_arguments*

   証明書データベースに証明書を追加するときに証明書に適用する信頼性属性を指定します。各証明書には、3 つの使用可能な信頼性カテゴリがあります。これらのカテゴリを表記する順序は、「SSL、電子メール、オブジェクト署名」です。証明書が信頼されるように、適切な信頼性引数を指定します。各カテゴリ位置では、以下の属性引数を 0 個以上使用することができます。

   p

   有効なピア。

   P

   信頼されたピア。この引数は p を意味します。

   重要: これは SSL 信頼性カテゴリに必須の引数です。

-i *server_certificate_path*

サーバ証明書のパスを指定します。以下の点について考慮してください。

- パスには証明書名も含める必要があります。
- 証明書の有効な拡張子には、.cert、.cer、および .pem があります。

注: ファイル パスにスペースがある場合は、そのパスを引用符で囲んでください。

-d *certificate_database_directory*

証明書データベースが入っているディレクトリのパスを指定します。

注: ファイル パスにスペースがある場合は、そのパスを引用符で囲んでください。

NSS によって、証明書データベースにサーバ証明書が追加されます。

例: 証明書データベースへのサーバ証明書の追加

```
certutil -A -n "My Server Certificate" -t "P,," -i C:¥certificates¥servercert.cer -d C:¥certdatabase
```

証明書データベース内の証明書の一覧表示

証明書が証明書データベースに追加されたことを確認するために、証明書を一覧表示します。

注: 以下の手順では、タスクを実行するための具体的なオプションおよび引数について詳しく説明します。NSS ユーティリティのオプションおよび引数の全リストについては、NSS プロジェクト ページにある Mozilla マニュアルを参照してください。

重要: Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

証明書データベース内の証明書を一覧表示する方法

1. コマンド プロンプトから、NSS ユーティリティを解凍したロケーション内の bin ディレクトリに移動します。

   例: C:¥nss¥bin

   注: Windows には固有の certutil ユーティリティがあります。NSS ユーティリティの bin ディレクトリから作業するようにしてください。間違えて Windows certutil ユーティリティを実行していることがあります。

2. 以下のコマンドを実行します。

   `certutil -L -d certificate_database_directory`

   -L

   証明書データベース内のすべての証明書を一覧表示します。

   -d *certificate_database_directory*

   証明書データベースが入っているディレクトリのパスを指定します。

   注: ファイル パスにスペースがある場合は、そのパスを引用符で囲んでください。

   NSS によって、証明書データベースに証明書を追加するときに指定した、ルート CA の別名、サーバ証明書の別名、および信頼性属性が表示されます。

例: 証明書データベース内の証明書の一覧表示

```
certutil -L -d C:¥certdatabase
```

ユーザ ディレクトリの SSL 接続の設定

ポリシー サーバとユーザ ストアが通信するときに SSL 接続が使用されるように、ユーザ ストア接続を設定します。

注: FSS 管理 UI にポリシー サーバ オブジェクトを作成または変更するときは、ASCII 文字を使用します。ASCII 文字以外でのオブジェクトの作成または変更はサポートされていません。

ユーザ ストアの SSL 接続を設定する方法

1. 管理 UI にログインします。
2. [インフラストラクチャ]-[ディレクトリ]をクリックします。

3. [ユーザ ディレクトリ]-[ユーザ ディレクトリの変更]をクリックします。

   [ユーザ ディレクトリの変更]ペインに、既存のユーザ ディレクトリ接続の一覧が表示されます。

4. 目的のユーザ ディレクトリ接続を選択し、[選択]をクリックします。

   ユーザ ディレクトリの設定が表示されます。

5. [安全な接続]チェック ボックスをオンにして、[サブミット]をクリックします。

   ユーザ ディレクトリ接続が、SSL を介して通信するように設定されます。

ポリシー サーバから証明書データベースへの参照の設定

ポリシー サーバが証明書データベースを参照するように設定し、SSL を介してユーザ ディレクトリと通信するようにポリシー サーバを設定します。

注: FSS 管理 UI にポリシー サーバ オブジェクトを作成または変更するときは、ASCII 文字を使用します。ASCII 文字以外でのオブジェクトの作成または変更はサポートされていません。

ポリシー サーバから証明書データベースへの参照を設定する方法

1. ポリシーサーバー管理コンソールを起動します。

   重要: Windows Server 2008 上でこのグラフィカル ユーザ インターフェースにアクセスする場合は、管理者としてシステムにログインしている場合でも、管理者権限でショートカットを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

2. [データ]タブをクリックします。

3. Netscape 証明書データベース ファイルのフィールドに、Netscape 証明書データベース ファイルのパスを入力します。

   例: C:¥certdatabase¥cert7.db

   注: key3.db ファイルも、cert7.db ファイルと同じディレクトリに含まれている必要があります。

4. ポリシー サーバを再起動します。

ポリシー サーバが、SSL を介してユーザ ディレクトリと通信するように設定されます。

SSL 接続の検証

SSL 接続を検証して、ユーザ ディレクトリとポリシー サーバが SSL を介して通信していることを確認します。

注: FSS 管理 UI にポリシー サーバ オブジェクトを作成または変更するときは、ASCII 文字を使用します。ASCII 文字以外でのオブジェクトの作成または変更はサポートされていません。

SSL 接続を検証する方法

1. 管理 UI にログインします。
2. [インフラストラクチャ]-[ディレクトリ]をクリックします。
3. [ユーザ ディレクトリ]-[ユーザ ディレクトリの表示]をクリックします。

   [ユーザ ディレクトリの表示]ペインに、既存のユーザ ディレクトリ接続の一覧が表示されます。
4. 目的の接続を選択し、[選択]をクリックします。

   ユーザ ディレクトリの設定が表示されます。
5. [内容の表示]をクリックします。

   SSL が正しく設定されている場合は、[ディレクトリのコンテンツ]ウィンドウに、ユーザ ディレクトリの内容が表示されます。

付録 B: プラットフォーム サポートおよびインストール メディア

このセクションには、以下のトピックが含まれています。

SiteMinder プラットフォーム サポート マトリックスへのアクセス

SiteMinder によりサポートされる CA およびサードパーティ コンポーネントの全体的なリストについては、テクニカル サポート サイトを参照してください。

サポート サイトからサポート マトリックスを参照する方法

1. テクニカル サポート サイトにログインします。
2. [Support]の下で、[Support By Product]をクリックします。
3. [Select a Product Page]フィールドに「CA SiteMinder」を入力し、Enter キーを押します。

   CA SiteMinder 製品ページが表示されます。
4. [Product Status]セクションをスクロールし、CA SiteMinder Family of Products Platform Support Matrices をクリックします。

注: 最新の JDK および JRE バージョンは、Sun Developer Network でダウンロードできます。

マニュアル選択メニューの使用

SiteMinder マニュアル選択メニューはテクニカル サポート サイトで提供されています。

サポート サイトからサポート マトリックスを参照する方法

1. テクニカル サポート サイトにアクセスします。

   注: ログインする必要はありません。

2. (任意)[Get Support]タブが前面にない場合は、[Get Support]をクリックします。
3. [Find Product News and Support]の下で[Product Pages]をクリックします。

   [Support by Product]ページが表示されます。

4. [Select a Product Page]フィールドに CA SiteMinder を入力して Enter キーを押します。

   CA SiteMinder 製品ページが表示されます。

5. マニュアル選択メニューをクリックします。
6. 必要なリリースのリンクをクリックします。

   SiteMinder マニュアル選択メニューのメイン ページが表示されます。

インストール メディアの検索

SiteMinder インストール メディアの全体的なリストは、テクニカル サポート サイトで見つけることができます。

サポート サイトからサポート マトリックスを参照する方法

1. テクニカル サポート サイトにログインします。
2. [Support]の下で、[Download Center]-[Products]をクリックします。

   [Download Center]画面が表示されます。
3. [Select a Product]フィールドに SiteMinder を入力します。
4. [Select a Release]リストからリリースを選択します。
5. [Select a Gen Level]リストからサービス パックを選択します。
6. [Go]をクリックします。

   [Product Downloads]画面が表示されます。SiteMinder のインストール実行可能ファイルがすべて一覧表示されます。

索引

S

T

U

V

W

あ

か

さ

た

は

ま

や