

SiteMinder

ポリシー サーバ インストール ガイド

12.52 SP1



このドキュメント（組み込みヘルプシステムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社（以下「CA」）により随時、変更または撤回されることがあります。本ドキュメントは、CA が知的財産権を有する機密情報であり、CA の事前の書面による承諾を受けずに本書の全部または一部を複写、譲渡、変更、開示、修正、複製することはできません。

本ドキュメントで言及されている CA ソフトウェア製品のライセンスを受けたユーザは、社内でユーザおよび従業員が使用する場合に限り、当該ソフトウェアに関連する本ドキュメントのコピーを妥当な部数だけ作成できます。ただし、CA のすべての著作権表示およびその説明を当該複製に添付することを条件とします。

本ドキュメントを印刷するまたはコピーを作成する上記の権利は、当該ソフトウェアのライセンスが完全に有効となっている期間内に限定されます。いかなる理由であれ、上記のライセンスが終了した場合には、お客様は本ドキュメントの全部または一部と、それらを複製したコピーのすべてを破棄したことを、CA に文書で証明する責任を負います。

準拠法により認められる限り、CA は本ドキュメントを現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対して侵害のないことについて、黙示の保証も含めいかなる保証もしません。また、本ドキュメントの使用に起因して、逸失利益、投資損失、業務の中断、営業権の喪失、情報の喪失等、いかなる損害（直接損害か間接損害かを問いません）が発生しても、CA はお客様または第三者に対し責任を負いません。CA がかかる損害の発生の可能性について事前に明示に通告されていた場合も同様とします。

本ドキュメントで参照されているすべてのソフトウェア製品の使用には、該当するライセンス契約が適用され、当該ライセンス契約はこの通知の条件によっていかなる変更も行われません。

本書の制作者は CA および CA Inc. です。

「制限された権利」のもとでの提供：アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section 252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2014 CA. All rights reserved. 本書に記載されたすべての商標、商号、サービス・マークおよびロゴは、それぞれの各社に帰属します。

CA Technologies 製品リファレンス

このマニュアルが参照している CA Technologies の製品は以下のとおりです。

- CA Directory
- SiteMinder
- CA Business Intelligence

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。

マニュアルの変更点

SiteMinder の旧リリースで発見された問題の結果として、12.52 SP1 のドキュメントに以下の更新が行われました。

- [レポート サーバの再起動](#) (P. 533) - LD_LIBRARY_PATH 変数の値を更新しました。
- [ポリシー ストア スキーマ ファイルの編集](#) (P. 177) - Novell eDirectory ポリシー ストア の設定に対して使用されるポリシー ストア スキーマ ファイルを編集するためのコマンドが更新されました。
- [Linux で Korn シェル \(ksh\) パッケージが必要](#) (P. 68) - ポリシー サーバ のインストールにこのパッケージが必要であることを説明するために追加されました。
- [監査ストア スキーマの作成](#) (P. 431) - DB2 手順の改訂。アサーション全体ではなく、各アサーションから NULL キーワードのみを削除します。
- [MBCS URL をサポートする認証方式](#) (P. 694) - 誤字を修正しました。この更新により、CQ171840 が解決されます。
- [Microsoft SQL Server 情報](#) (P. 42) - SiteMinder スキーマがデータベース内にすでに存在する場合、作成権限を持つ管理者の認証情報は必要とされないことが注意事項として追加されました。
- [ポリシー ストアの設定方法 \(MySQL\)](#) (P. 323) - ユニコード文字をサポートする新規スキーマ ファイルを含めるために、このトピックおよびトピック「[SiteMinder スキーマの作成](#) (P. 324)」を改訂しました。この更新により、CQ178545 が解決されます。
- Java Cryptographic Extension (JCE) の必須パッチ - この項目では、Java によって提供される暗号化アルゴリズムを使用するために、更新が必要なファイルについて詳しく説明します。CQ 174929 を解決します。
- [必須 Linux ライブラリ](#) (P. 24) - 64 ビットの Red Hat 6.x に必要なすべての RPM パッケージは 32 ビットのパッケージであるという旨の注を追加しました。この修正は CQ 177043 を解決します。
- [ポリシー ストアとしての Oracle Directory Server](#) (P. 206) - smldapsetup コマンド定義に変更を加えました。この更新は CQ 177321 を解決します。

- [Oracle ポリシー ストアの設定](#) (P. 372)、[MySQL ポリシー ストアの設定](#) (P. 322)、および [SQL Server ポリシー ストアの設定](#) (P. 338) - DataDirect 6.0 ドライバ (サポートは停止されました) の指示を DataDirect 7.1 ドライバの指示に置換するために、更新されました。CQ 177973 を解決します。
- [Microsoft SQL Server 情報](#) (P. 42) - CA SiteMinder スキーマがデータベースにすでに存在する場合、ウィザードは作成権限を持ったデータベース管理者の認証情報を必要としないという旨の注を追加しました。CQ 176984 を解決します。
- [Oracle Virtual Directory をポリシー ストアとして設定する方法](#) (P. 250) - Oracle Virtual Directory をポリシー ストアとして設定する方法について説明するセクションを追加しました。CQ 174391 を解決します。
- [Oracle Unified Directory をポリシー ストアとして設定する方法](#) (P. 233) - Oracle Unified Directory をポリシー ストアとして設定する方法について説明するセクションを追加しました。CQ 172420 を解決します。
- [SiteMinder 用の Oracle Data Source の設定](#) (P. 380) - SCAN (Single Client Access Name) 機能で、Oracle Real Application Clusters 11g R2 用にデータソースを作成する方法について説明するコンテンツを追加しました。CQ171215 を解決します。
- [必須の Linux ライブラリ](#) (P. 24) - 必須 Linux ライブラリおよび含められるトピックを「管理 UI インストールの要件」の章に追加しました。CQ 169427 および 171403 を解決します。STAR イシュー 21343328-04 および 21436925-1 を解決します。
- [ポリシー ストア スキーマの作成](#) (P. 211) -- 追加のコマンドをいくつかの手順に追加しました。RTC の問題 117824 を解決します。

このガイドの第 2 版では、以下の点が変更されています。

ドキュメントのみの変更

- [コンソール モードでの設定ウィザードの実行](#) (P. 93) -- コンソールモードで Advanced Authentication Server を有効にする手順によりトピックが更新されました。ドキュメントは 12.52 SP1 で更新されています。この変更によって、CQ 182427 および STAR 21708422-1 が解決されます。
- [必要とされる Linux ライブラリ](#) (P. 24) -- ncurses パッケージの要件について記載するためにトピックが更新されました。ドキュメントは 12.52 SP1 で更新されています。この変更によって、CQ 184220 が解決されます。

目次

第 1 章: ポリシー サーバのインストール要件	19
Windows	19
UNIX	20
第 2 章: 管理 UI インストール要件	23
Windows UI ホストのシステム要件を確認する	23
UNIX UI ホストのシステム要件を確認する	23
必要とされる Linux ライブラリ	24
第 3 章: レポート サーバ インストール要件	27
システム要件	27
Windows	27
UNIX	28
Solaris で必要なパッチ クラスタ	28
Red Hat で必要なパッチ クラスタ	29
レポート データベース要件	29
接続要件	30
第 4 章: Windows システムでのポリシー サーバのインストール	31
インストール ロード マップ	32
Windows でポリシー サーバをインストールする前に	33
Windows でポリシー サーバをインストールする方法	33
ポリシー サーバ コンポーネントの考慮事項	34
ポリシー ストアの考慮事項	35
FIPS の考慮点	37
インストーラのための情報の収集	38
ポリシー サーバ インストーラの実行	45
SNMP イベント トラップの有効化	46
ポリシー サーバ インストールのトラブルシューティング	47
ポリシー サーバ 設定ウィザード	48
設定ウィザードを使用する方法	49
ポリシー サーバの再インストール	56
Windows でポリシー サーバをアンインストールする方法	56

Path 変数での JRE の設定	57
エージェント ホスト ファイルからのポリシー サーバの参照の削除.....	57
すべての SiteMinder プロセスの停止	58
ポリシー サーバのアンインストール	58
残存アイテムの削除.....	59
残りのサービスの削除.....	59
スクリプト インターフェース	60

第 5 章: UNIX システムでのポリシー サーバのインストール 61

インストール ロード マップ	62
Solaris 10 ゾーン サポート.....	63
グローバル ゾーン サポート	63
疎ルート ゾーン サポート	64
完全ルート ゾーン サポート	64
ポリシー サーバのインストールの準備方法	65
必要とされる Linux ライブラリ	66
Linux 上で Korn シェル (ksh) パッケージが必要.....	68
新規 UNIX アカウントの作成.....	68
UNIX システム パラメータの変更.....	69
ローカライズ変数の設定解除.....	70
LANG 環境変数の設定解除.....	70
UNIX でポリシー サーバをインストールする前に	70
UNIX でポリシー サーバをインストールする方法	71
ポリシー サーバコンポーネントの考慮事項	72
ポリシー ストアの考慮事項.....	73
FIPS の考慮点.....	75
インストーラのための情報の収集.....	76
GUI モードによるポリシー サーバのインストール	83
コンソールモードによるポリシー サーバのインストール	85
Security-Enhanced Linux への例外の追加.....	88
SNMP デーモンの再起動	88
ポリシー サーバインストールのトラブルシューティング	89
自動スタートアップの設定	89
ポリシー サーバ設定ウィザード	90
設定ウィザードを使用する方法.....	91
UNIX でポリシー サーバをアンインストールする方法	94
エージェント ホスト ファイルからのポリシー サーバの参照の削除.....	94
PATH 変数での JRE の設定.....	95
すべての SiteMinder プロセスの停止	95

ポリシー サーバのアンインストール	96
IWS からの SiteMinder 参照の削除.....	97
StartServletExec からの SiteMinder 参照の削除.....	98
残存アイテムの削除.....	99

第 6 章: SiteMinder データを格納するように LDAP ディレクトリ サーバを設定 101

ポリシーまたはキー ストアとしての LDAP ディレクトリ サーバ	101
インストール ロードマップ	102
重要な考慮事項.....	103
デフォルトのポリシー ストア オブジェクトに関する考慮事項.....	104
ポリシー ストアとしての CA Directory.....	105
ディレクトリ サーバ情報の収集.....	105
ポリシー ストアを設定する方法.....	106
セッションストアとしての CA Directory.....	120
セッション ストアを設定する方法.....	120
ポリシー ストアとしての Active Directory	126
ディレクトリ サーバ情報の収集.....	126
ポリシー ストアを設定する方法.....	127
Active Directory ObjectCategory インデックス属性のサポート	137
ObjectCategory 属性サポートの有効化または無効化.....	138
ポリシー ストアとしての Domino Directory Server	139
Domino Directory Server をポリシー ストアとして設定する方法	139
ポリシー ストアとしての IBM Directory Server	151
ディレクトリ サーバ情報の収集.....	151
ポリシー ストアを設定する方法.....	152
ポリシー ストアとしての Microsoft Active Directory LDS.....	162
Active Directory LDS の前提条件.....	163
ディレクトリ サーバ情報の収集.....	164
ポリシー ストアを設定する方法.....	164
ポリシー ストアとしての Novell eDirectory	174
Novell eDirectory でのポリシー ストア オブジェクトの制限	175
ディレクトリ サーバ情報の収集.....	175
ポリシー ストアを設定する方法.....	176
ポリシー ストアとしての OpenLDAP.....	188
ディレクトリ サーバ情報の収集.....	188
ポリシー ストアを設定する方法.....	189
ポリシー ストアとしての Oracle Directory Server	206
ディレクトリ サーバ情報の収集.....	206

ポリシー ストアを設定する方法	207
ポリシー ストアとしての Oracle Internet Directory	219
ディレクトリ サーバ情報の収集	220
ポリシー ストアを設定する方法	220
Oracle Unified Directory をポリシー ストアとして設定する方法	233
ディレクトリ サーバ情報の収集	234
Oracle Unified Directory インスタンスを設定する方法	235
データベースを作成する方法	239
ポリシー サーバからポリシー ストアへの参照の設定	242
SiteMinder スーパーユーザ パスワードの設定	243
ポリシー ストア データ定義のインポート	244
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	245
Advanced Authentication Server の有効化	247
管理 UI 登録の準備	247
Oracle Virtual Directory をポリシー ストアとして設定する方法	250
ディレクトリ サーバ情報の収集	251
SiteMinder スキーマ ファイルで OVD ローカル スキーマを拡張する	253
既存のポリシー ストアに接続するための Oracle Virtual Directory アダプタを作成する	254
ポリシー サーバからポリシー ストアへの参照の設定	256
SiteMinder スーパーユーザ パスワードの設定	257
Advanced Authentication Server の有効化	258
ポリシー サーバの再起動	259
管理 UI 登録の準備	259
ポリシー ストアとしての Red Hat Directory Server	262
ディレクトリ サーバ情報の収集	262
ポリシー ストアを設定する方法	263
ポリシー ストアとしての Siemens DirX	272
ディレクトリ サーバ情報の収集	273
ポリシー ストアを設定する方法	273
個別キー ストアの設定	285
キー ストアとしての Microsoft Active Directory	285
ポリシー ストアとしての Microsoft AD LDS	290
ポリシー ストアとしての Oracle Directory Server Enterprise Edition	296
ポリシー ストアとしての Oracle Internet Directory Server	304
キー ストアとしての Red Hat Directory Server	308
 第 7 章: リレーショナル データベースでの SiteMinder データ ストアの設定	313
ポリシーまたはキーのストアとしてのリレーショナル データベース	314
インストール ロード マップ	314

重要な考慮事項.....	316
デフォルトのポリシー ストア オブジェクトに関する考慮事項.....	316
リレーショナルデータベース用のスキーマ ファイル	317
IBM DB2 スキーマ ファイル	318
MySQL スキーマ ファイル.....	319
SQL Server のスキーマ ファイル.....	320
PostgreSQL Server のスキーマ ファイル	321
Oracle スキーマ ファイル	322
MySQL ポリシー ストアの設定.....	322
データベース情報の収集.....	323
ポリシー ストアを設定する方法.....	323
SQL Server ポリシー ストアの設定.....	338
データベース情報の収集.....	339
ポリシー ストアを設定する方法.....	340
PostgreSQL サーバポリシー ストアを設定する方法.....	356
PostgreSQL データベース情報の収集.....	357
PostgreSQL 用の SiteMinder スキーマの作成.....	358
Windows での PostgreSQL データ ソースの作成.....	359
UNIX での PostgreSQL データ ソースの作成.....	360
PostgreSQL Server ワイヤプロトコルドライバの設定	362
ポリシー サーバに対する参照データベースの指定	364
SiteMinder スーパーユーザ パスワードの設定	365
ポリシー ストア データ定義のインポート	366
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	367
Advanced Authentication Server の有効化.....	369
ポリシー サーバの再起動.....	369
管理 UI 登録の準備	370
Oracle ポリシー ストアの設定.....	372
Oracle 10 g データベースに対する前提条件.....	373
Oracle 12c データベースに対する前提条件	375
データベース情報の収集.....	375
ポリシー ストアを設定する方法.....	378
IBM DB2 ポリシー ストアの設定	400
データベース情報の収集.....	401
ポリシー ストアを設定する方法.....	402
セッション情報を IBM DB2 に格納する方法	416
セッション ストア スキーマの作成	416
ポリシー サーバに対する参照データベースの指定	417
ポリシー サーバの再起動.....	418
セッション情報を MySQL に格納する方法.....	418

セッションストアスキーマの作成	419
ポリシーサーバに対する参照データベースの指定	419
ポリシーサーバの再起動	421
Oracle でセッション情報を格納する方法	421
セッションストアスキーマの作成	422
ポリシーサーバに対する参照データベースの指定	423
ポリシーサーバの再起動	424
SQL Server 内にセッション情報を格納する方法	424
セッションストアスキーマの作成	425
ポリシーサーバに対する参照データベースの指定	425
ポリシーサーバの再起動	427
セッション情報を PostgreSQL に格納する方法	427
セッションストアスキーマの作成	428
ポリシーサーバに対する参照データベースの指定	428
ポリシーサーバの再起動	430
監査ログを IBM DB2 に格納する方法	430
監査ストアスキーマの作成	431
ポリシーサーバに対する参照データベースの指定	432
ポリシーサーバの再起動	433
監査ログを MySQL に格納する方法	433
監査ログスキーマの作成	434
ポリシーサーバに対する参照データベースの指定	434
ポリシーサーバの再起動	436
Oracle で監査ログを格納する方法	436
監査ログスキーマの作成	437
ポリシーサーバに対する参照データベースの指定	437
ポリシーサーバの再起動	439
SQL Server 内に監査ログを格納する方法	439
監査ログスキーマの作成	440
ポリシーサーバに対する参照データベースの指定	440
ポリシーサーバの再起動	442
監査ログを PostgreSQL に格納する方法	442
監査ログスキーマの作成	442
ポリシーサーバに対する参照データベースの指定	443
ポリシーサーバの再起動	445
キー情報を IBM DB2 に格納する方法	445
キーストアスキーマの作成	446
ポリシーサーバに対する参照データベースの指定	446
ポリシーサーバの再起動	448
キー情報を MySQL に格納する方法	448

キー ストア スキーマの作成	449
ポリシー サーバに対する参照データベースの指定	449
ポリシー サーバの再起動	451
Oracle でキー情報を格納する方法	451
キー ストア スキーマの作成	452
ポリシー サーバに対する参照データベースの指定	452
ポリシー サーバの再起動	454
SQL Server 内にキー情報を格納する方法	454
キー ストア スキーマの作成	455
ポリシー サーバに対する参照データベースの指定	455
ポリシー サーバの再起動	457
キー情報を PostgreSQL に格納する方法	457
キー ストア スキーマの作成	457
ポリシー サーバに対する参照データベースの指定	458
ポリシー サーバの再起動	460
サンプル ユーザディレクトリ	460
IBM DB2 サンプル ユーザディレクトリの設定	460
MySQL サンプル ユーザディレクトリの設定	461
Oracle サンプル ユーザディレクトリの設定	462
SQL Server サンプル ユーザディレクトリの設定	463

第 8 章: 管理 UI のインストール 465

UI とポリシー サーバの間の信頼関係	465
管理 UI インストール チェックリストを完了します。	466
管理 UI をインストールする方法	466
インストーラのための情報の収集	467
管理 UI 登録ウィンドウのリセット	468
管理 UI をインストールする方法	470
管理 UI インストールのトラブルシューティング	475
管理 UI を登録する方法	476
FIPS 環境変数の作成	476
アプリケーション サーバの起動	477
管理 UI の登録	478
アプリケーション サーバを停止します。	481
管理者認証情報	481
(オプション) 高可用性向けの追加の 管理 UI のインストールと設定	482
管理 UI 用の追加のポリシー サーバ接続	482
管理 UI 登録ツールの実行	483
登録情報の収集	486

ポリシー サーバへの接続設定	487
デフォルト ポリシー サーバ接続の変更	488
ポリシー サーバ接続の削除	488
（オプション） 管理 UI のアンインストール	489
UNIX 上の 管理 UI のアンインストール	490
Web エージェント インストールのためのポリシー サーバの準備	491

第 9 章: レポートのインストール 495

インストール ロード マップ	495
インストール チェックリストのレポート	496
レポート サーバ	497
レポート データベースおよび監査データベース	499
レポート データベースおよび監査データベース	501
レポートの考慮事項	503
レポート インストールのしくみ	505
レポート サーバをインストールする方法	506
インストーラのための情報の収集	506
レポート サーバのインストール	510
レポート サーバインストールのトラブルシューティング	521
レポート テンプレートをインストールする方法	521
インストーラのための情報の収集	522
レポート テンプレートのインストール	522
ジョブ サーバ サービス タイムアウト値の増加	526
レポート サーバを登録する方法	527
クライアント名とパスフレーズの作成	528
登録情報の収集	531
ポリシー サーバにレポート サーバを登録します	531
レポート サーバの再起動	533
管理 UI への接続の設定	535
監査データベースを設定する方法	536
管理 UI での監査データベースの登録	536
監査データベースおよびレポート サーバの接続性	538
レポート スケジューラの開始	539
レポート サーバの停止	540
レポートをアンインストールする方法	542
Windows からのレポート サーバ設定ウィザードのアンインストール	542
UNIX からのレポート サーバ設定ウィザードのアンインストール	543
Windows からのレポート サーバのアンインストール	543
UNIX からのレポート サーバのアンインストール	544

Windows アイテムの削除.....	545
UNIX アイテムの削除.....	546
レポート データベース テーブルの削除	546
管理 UI へのレポート サーバ接続の削除.....	547
レポート サーバの再インストール	547

第 10 章: OneView モニタの設定 549

OneView モニタの概要	549
OneView モニタのシステム要件	550
OneView モニタの設定	550
同じマシン上の OneView モニタ GUI/IIS Web エージェントの制限.....	551
Windows/IIS 上で OneView モニタ GUI を設定する方法	551
Windows に ServletExec をインストールするための前提条件.....	552
Windows IIS 上での ServletExec のインストール.....	552
ServletExec インストール後の IIS ユーザ用権限の設定	553
UNIX/Sun Java System 上で OneView モニタ GUI を設定する方法.....	553
ServletExec をインストールするための前提条件.....	554
Sun Java System 6.0 でのサーブレットの無効化.....	554
UNIX/Sun Java システムでの ServletExec/AS のインストール.....	554
OneView モニタ サービスの起動	556
OneView モニタ GUI へのアクセス	556
ポリシー サーバクラスタの監視	557

第 11 章: SNMP サポート 559

SNMP サポートの概要	559
Windows と UNIX のシステムの場合の SNMP 前提条件	561
Windows の前提条件.....	561
UNIX システムの前提条件.....	562
Windows 上での SNMP エージェントの設定	562
Windows で SNMP イベント トラップを設定する方法	564
UNIX システムでの SNMP エージェントの設定	565
UNIX システムで SNMP イベント トラップを設定する方法	566
Red Hat Enterprise Linux Advanced Server に対する SNMP Get のテスト.....	567

第 12 章: 既存アプリケーション サーバへの 管理 UI のインストール 569

管理 UI インストール要件.....	569
管理 UI システム要件	569
アプリケーション サーバ要件	571

UI とポリシー サーバの間の信頼関係.....	574
管理 UI インストール チェックリスト.....	575
管理 UI をインストールする方法.....	576
必要とされる Linux ライブラリ.....	577
アプリケーションサーバ情報の収集.....	579
管理 UI のインストール.....	580
管理 UI を登録する方法.....	584
管理 UI 登録ウィンドウのリセット.....	585
FIPS 環境変数の作成.....	588
アプリケーションサーバの起動.....	589
管理 UI の登録.....	590
アプリケーションサーバを停止します。.....	592
管理者認証情報.....	593
管理 UI の高可用性.....	594
Windows での管理 UI のアンインストール.....	594
UNIX での管理 UI のアンインストール.....	595

第 13 章: トラブルシューティング 597

ポリシー サーバのトラブルシューティング.....	597
Solaris 上の NETE_PS_ALT_CONF_FILE 環境変数.....	597
ポリシー サーバがインストール後に起動しない.....	598
SiteMinder 環境変数がプロファイル ファイルに設定されていない.....	598
Winsock エラー 10054 メッセージ.....	599
SiteMinder ライセンスの使用.....	599
英語以外の入力文字にジャンク文字が含まれる.....	601
アンインストール中に Java エラー メッセージが表示される.....	602
Adobe Acrobat Reader がインストールされない.....	603
ユーザストアとしての Active Directory の使用に関する問題.....	603
AE がライブラリ「smjavaapi」のロードに失敗した システム エラー.....	604
ポリシー ストアのトラブルシューティング.....	604
多数のオブジェクトを含むポリシー ストア.....	604
SSL 初期化に失敗する.....	605
ODBC ポリシー ストア インポートが UserDirectory エラーで失敗する.....	605
OneView モニタのトラブルシューティング.....	607
変更された UNIX/Sun Java System Web Server 設定ファイルの修正.....	607
/sitemindermonitor への Windows/IIS 仮想パスが存在しない.....	608
管理 UI のトラブルシューティング.....	609
管理 UI がハングアップする.....	609
未処理の例外を持つ WebSphere クラッシュ.....	610

ポリシー サーバ接続が登録できない	610
API エラーが表示される	610
「ファイルに登録がありません」エラーが表示される	611
「無効な登録ファイルです」エラーが表示される	613
タイムアウトすることなく登録が失敗する	614
管理 UI 登録ログが見つからない	615
検索がタイムアウトエラーで失敗する	615
デフォルトのログ ファイルが見つからない場合	617
デフォルトのログ ファイルは、十分な情報を提供しません。	618
レポート サーバのトラブルシューティング	618
レポート サーバのインストールは、文字に関するエラーで失敗します。	619
レポート サーバインストーラにファイル不足エラーが表示される	619
アンインストールでアプリケーションを閉じるよう要求される	620
監査を基にしたレポートが結果を返さない	620
ポリシー分析レポートが実行できない	621
管理 UI によるファイル不足エラーの表示	622

第 14 章: 無人インストール 623

無人インストール	623
無人インストールのガイドライン	623
デフォルト プロパティ ファイル	624
ポリシー サーバプロパティ ファイル	624
管理 UI プロパティ ファイル	624
レポート プロパティ ファイル	625
ポリシー サーバの無人インストールを実行する方法	626
ポリシー サーバインストーラのプロパティ ファイルの変更	627
ポリシー サーバインストーラの実行	639
ポリシー サーバインストーラのトラブルシューティング	640
ポリシー サーバの無人インストールの停止	641
管理 UI の無人インストールを実行する方法	642
必須インストーラのプロパティ ファイルの変更	643
管理 UI インストーラのプロパティ ファイルの変更	644
管理 UI インストーラの実行	647
レポート サーバの無人インストールを実行する方法	650
Windows 用レポート サーバ応答ファイルの変更	651
UNIX 用レポート サーバ応答ファイルの変更	670
SiteMinder レポート サーバ設定ウィザードのプロパティ ファイルの変更	684
レポート サーバインストーラの実行	685
レポート テンプレートのインストール	687

付録 A: 国際環境用のポリシー サーバの設定 689

国際環境内のポリシー サーバ	689
ポリシー サーバのインストールを計画する際の注意事項	689
マルチバイト文字をサポートしているポリシー サーバ コンポーネント	690
マルチバイト文字 URL のサポート	691
国際文字をサポートする SiteMinder データ ストア の設定	694
SQL Server 内の国際 SiteMinder データ ストア の設定	694
Oracle での国際 SiteMinder データ ストア の設定	695
SQL Server で Unicode をサポートするユーザ ストア の設定	696
Oracle 内での日本語ユーザ ストア の設定	698

付録 B: 変更される環境変数 699

変更された Windows 環境変数	699
変更された UNIX 環境変数	700

第 1 章: ポリシー サーバのインストール要件

Windows

ポリシー サーバがインストールされる Windows システムは、以下の最小システム要件を満たす必要があります。

- CPU -- x86 または x64
- メモリ - 2 GB のシステム RAM

注: ポリシー サーバ処理には 2 GB の RAM を推奨します。ポリシー サーバ ホスト システムには少なくとも 4GB の RAM が利用可能であることを推奨します。

- 使用可能なディスク領域:
 - インストール場所に 4 GB の空きディスク領域
 - システムの一時的なファイル保存場所に 3 GB の空き領域

注: これらの要件は、およそ 1,000 ポリシーの中規模ポリシー データベースに基づきます。

- JDK - JDK で配布される必須 JRE がポリシー サーバ ホスト システムにインストールされていることを確認します。
- JCE-- 最新の JCE (Java Cryptography Extension) Unlimited Strength Jurisdiction パッチが必要です。使用しているプラットフォーム用の JCE パッケージを見つけるには、Oracle の Web サイトを参照してください。

システム上の以下のファイルにパッチを適用します。

- local_policy.jar
- US_export_policy.jar

これらのファイルはディレクトリ `jre_home¥lib¥security` にあります。

`jre_home`

この変数は、Java Runtime Environment がインストールされる場所を指定します。

- **LDAP ディレクトリ サーバまたはリレーショナルデータベース - ポリシー ストアとして、サポートされている LDAP ディレクトリ サーバまたはリレーショナル データベースを使用していることを確認します。**

注: サポートされている **CA** およびサードパーティ コンポーネントのリストについては、テクニカル サポート サイトの **SiteMinder 12.52 SP1** プラットフォームのサポート マトリックスを参照してください。

UNIX

ポリシー サーバをインストールする UNIX システムは、以下の最小システム要件を満たす必要があります。

- **CPU**

- **Solaris - UltraSparc 440MHz またはそれ以上**
- **Red Hat-x86 または x64**

注: Red Hat オペレーティング システムはそのパフォーマンスをエントロピーに依存します。コンポーネントをインストールする前に、エントロピーを増やしてください。そうしない場合、インストールの完了までに非常に時間がかかります。また、ランタイム中に 管理 UI のレスポンスが遅くなります。

以下のコマンドを使用します。

```
mv /dev/random /dev/random.org  
ln -s /dev/urandom /dev/random
```

- **メモリ - 2 GB のシステム RAM**

注: ポリシー サーバ処理には **2 GB** の **RAM** を推奨します。ポリシー サーバ ホスト システムには少なくとも **4GB** の **RAM** が利用可能であることを推奨します。

- **使用可能なディスク領域 :**

- **4 GB の空きディスク領域**
- **/tmp 内に 3 GB の空きディスク領域**

注: ポリシー サーバの日常の運用には、通常 **/tmp** 内に **10 MB** の空きディスク領域が必要です。ポリシー サーバは、**/tmp** の下にファイルおよび名前付きパイプを作成します。パスは変更できません。

- **JRE - ポリシー サーバをインストールするシステムに必要な JRE バージョンがインストールされていることを確認します。**

- **JCE** - 現在の Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction パッチは Java の暗号化アルゴリズムを使用するのに必要です。使用しているプラットフォーム用の JCE パッケージを見つけるには、Oracle の Web サイトを参照してください。

システム上の以下のファイルにパッチを適用します。

- local_policy.jar
- US_export_policy.jar

これらのファイルはディレクトリ `jre_home¥lib¥security` にあります。

`jre_home`

この変数は、Java Runtime Environment がインストールされる場所を指定します。

- **LDAP** ディレクトリ サーバまたはリレーショナルデータベース - ポリシーストアとして、サポートされている LDAP ディレクトリ サーバまたはリレーショナルデータベースを使用していることを確認します。

注: サポートされている CA およびサードパーティ コンポーネントのリストについては、テクニカルサポート サイトの SiteMinder 12.52 SP1 プラットフォームのサポート マトリックスを参照してください。

第 2 章：管理 UI インストール要件

Windows UI ホストのシステム要件を確認する

スタンドアロンインストール用の Windows 管理 UI ホスト システムは以下の最小限のシステム要件を満たす必要があります。

- **CPU** --x86 または x64、1.2 GHz 以上
- **メモリ** - 1 GB のシステム RAM 2 GB をお勧めします。
- **使用可能なディスク領域** - 840 MB
- **一時ディレクトリ領域** - 3 GB
- **画面解像度** - 管理 UI を正常に表示するための解像度 1024 x 768 以上、256 色以上

プラットフォーム サポート マトリックスを使用して、オペレーティング環境および他の必要なサードパーティ コンポーネントがサポートされていることを確認します。

UNIX UI ホストのシステム要件を確認する

スタンドアロンインストール用の UNIX 管理 UI ホスト システムは以下の最小限のシステム要件を満たす必要があります。

- **CPU**
 - Solaris -- UltraSparc、440 MHz 以上
 - Red Hat Linux -- x86 または x64、700 MHz 以上

注：Red Hat 6 オペレーティング システムはパフォーマンスのエントロピーに依存します。コンポーネントをインストールする前に、エントロピーを増やしてください。そうしない場合、インストールの完了までに非常に時間がかかります。また、ランタイム中に管理 UI のレスポンスが遅くなります。

以下のコマンドを使用します。

```
mv /dev/random /dev/random.org
ln -s /dev/urandom /dev/random
```

- メモリ - 1 GB のシステム RAM 2 GB をお勧めします。
- 使用可能なディスク領域 - 840 MB
- 一時ディレクトリ領域 - 3 GB
- 画面解像度 - 管理 UI を正常に表示するための解像度 1024 x 768 以上、256 色以上

プラットフォーム サポート マトリックスを使用して、オペレーティング環境および他の必要なサードパーティ コンポーネントがサポートされていることを確認します。

必要とされる Linux ライブラリ

Linux オペレーティング環境上で動作するコンポーネントには、特定のライブラリ ファイルが必要です。正しいライブラリをインストールしないと、以下のエラーを引き起こす場合があります。

```
java.lang.UnsatisfiedLinkError
```

このコンポーネントの Linux バージョンをインストール、設定、またはアップグレードする場合は、ホスト システム上で以下のパッケージが必要になります。

Red Hat 5.x

- `compat-gcc-34-c++-3.4.6-patch_version.i386`
- `libstdc++-4.x.x-x.el5.i686.rpm`
- `libidn.so.11.rpm`
- `ncurses`

Red Hat 6.x

- libstdc++-4.x.x-x.el6.i686.rpm
- libidn-1.18-2.el6.i686
- libXext.i686.rpm
- libXrender.i686.rpm
- libXtst.i686.rpm
- libidn.so.11.rpm
- ncurses

Red Hat 6.x (64 ビット) の場合はさらに以下 :

注: 64 ビット Red Hat 6.x に必要な RPM パッケージはすべて、32 ビットのパッケージです。

- libXau-1.0.5-1.el6.i686.rpm
- libxcb-1.5-1.el6.i686.rpm
- compat-db42-4.2.52-15.el6.i686.rpm
- compat-db43-4.3.29-15.el6.i686.rpm
- libX11-1.3-2.el6.i686.rpm
- libXrender-0.9.5-1.el6.i686.rpm
- libexpat.so.1 (expat-2.0.1-11.el6_2.i686.rpm により提供)
- libfreetype.so.6 (freetype-2.3.11-6.el6_2.9.i686.rpm により提供)
- libfontconfig.so.1 (fontconfig-2.8.0-3.el6.i686.rpm により提供)
- libICE-1.0.6-1.el6.i686.rpm
- libuuid-2.17.2-12.7.el6.i686.rpm
- libSM-1.1.0-7.1.el6.i686.rpm
- libXext-1.1-3.el6.i686.rpm
- compat-libstdc++-33-3.2.3-69.el6.i686.rpm
- compat-db-4.6.21-15.el6.i686.rpm
- libXi-1.3-3.el6.i686.rpm
- libXtst-1.0.99.2-3.el6.i686.rpm
- libXft-2.1.13-4.1.el6.i686.rpm
- libXt-1.0.7-1.el6.i686.rpm

- libXp-1.0.0-15.1.el6.i686.rpm
- libstdc++.i686.rpm
- compat-libtermcap.rpm
- libidn.i686.rpm
- ncurses

第 3 章: レポート サーバ インストール要件

システム要件

以下のセクションは、レポート サーバをインストールするための最小のシステム要件を詳述します。

注: サポートされている CA およびサードパーティ コンポーネントのリストについては、テクニカル サポート サイトの **SiteMinder 12.52 SP1** プラットフォームのサポート マトリックスを参照してください。

Windows

レポート サーバをインストールする Windows システムは、以下の最小のシステム要件を満たす必要があります。

- **CPU** - Intel® Pentium™ 4 クラスのプロセッサ (2.0 GHz)
- **メモリ** - 2 GB の RAM
- **使用可能なディスク領域** - 10 GB

注: この要件は、レポート サーバをインストールするために必要なスペースです。この要件は、レポートを格納するのに必要なディスク スペースを示したものではありません。

- **一時ディレクトリ領域** - 1 GB
- **画面解像度** - 管理 UI でレポートを正常に表示するための解像度 1024 x 768 以上、256 色以上

UNIX

レポートサーバをインストールする UNIX システムは、以下の最小のシステム要件を満たす必要があります。

- **CPU**
 - (Solaris) SPARC v8plusSparc
 - (Red Hat Linux) Intel Pentium 4 クラスのプロセッサ (2.0 GHz)
- **メモリ - 2 GB の RAM**
- **使用可能なディスク領域 - 10 GB**

注: この要件は、レポートサーバをインストールするために必要なスペースです。この要件は、レポートを格納するのに必要なディスクスペースを示したものではありません。
- **一時ディレクトリ領域 - 1 GB**
- **画面解像度** - 管理 UI でレポートを正常に表示するための解像度 1024 x 768 以上、256 色以上

Solaris で必要なパッチ クラスタ

レポートサーバは特定の Solaris パッチ クラスタを必要とします。レポートサーバをインストールする前に、Solaris システムを更新します。

重要: 必要なパッチをインストールしない場合、レポートサーバのインストールは失敗します。

注: Solaris パッチ クラスタの詳細については、「ポリシー サーバリリースノート」を参照してください。

Red Hat で必要なパッチ クラスタ

レポート サーバは特定の Red Hat パッチ クラスタを必要とします。レポート サーバをインストールする前に、Red Hat システムを更新してください。

重要: 必要なパッチをインストールしない場合、レポート サーバのインストールは失敗します。

注: Red Hat パッチ クラスタの詳細については、「ポリシー サーバリリースノート」を参照してください。

レポート データベース要件

レポート サーバは、レポートを実行するためにレポート データベースを必要とします。レポート サーバインストーラは、Sun Microsystems MySQL™ (MySQL) の埋め込みバージョンを、レポート データベースとして機能するようにインストールすることができます。

MySQL の埋め込みバージョンをインストールしない場合は、以下のサポートされているバージョンが使用できます。

- Microsoft® SQL Server® (SQL Server)
- Oracle®

重要: レポート サーバは、CA 製品が共有できる CA の共通コンポーネントです。そのため、SiteMinder を除く他の製品でサポートされるデータベースのタイプおよびバージョンに及ぶまで、レポート データベースとしてインストーラで設定することができます。サポートされているデータベースのタイプおよびバージョンのリストについては、「SiteMinder 12.52 SP1 プラットフォーム サポート マトリクス」を参照してください。

接続要件

レポート サーバは、以下と通信するためにドライバを必要とします。

- SQL Server または Oracle のレポート データベース

注: MySQL の埋め込みバージョンを使用する場合は、レポート データベースの接続要件はありません。

- SiteMinder 監査ストア

サポートされている Microsoft SQL Server ドライバまたは Oracle Net クライアントを、必ずレポート サーバ ホスト システムにインストールしてください。

注: サポートされている CA およびサードパーティ コンポーネントのリストについては、テクニカルサポート サイトの SiteMinder 12.52 SP1 プラットフォームのサポート マトリックスを参照してください。

第 4 章: Windows システムでのポリシー サーバのインストール

このセクションには、以下のトピックが含まれています。

[インストールロードマップ](#) (P. 32)

[Windows でポリシー サーバをインストールする前に](#) (P. 33)

[Windows でポリシー サーバをインストールする方法](#) (P. 33)

[SNMP イベント トラップの有効化](#) (P. 46)

[ポリシー サーバインストールのトラブルシューティング](#) (P. 47)

[ポリシー サーバ設定ウィザード](#) (P. 48)

[ポリシー サーバの再インストール](#) (P. 56)

[Windows でポリシー サーバをアンインストールする方法](#) (P. 56)

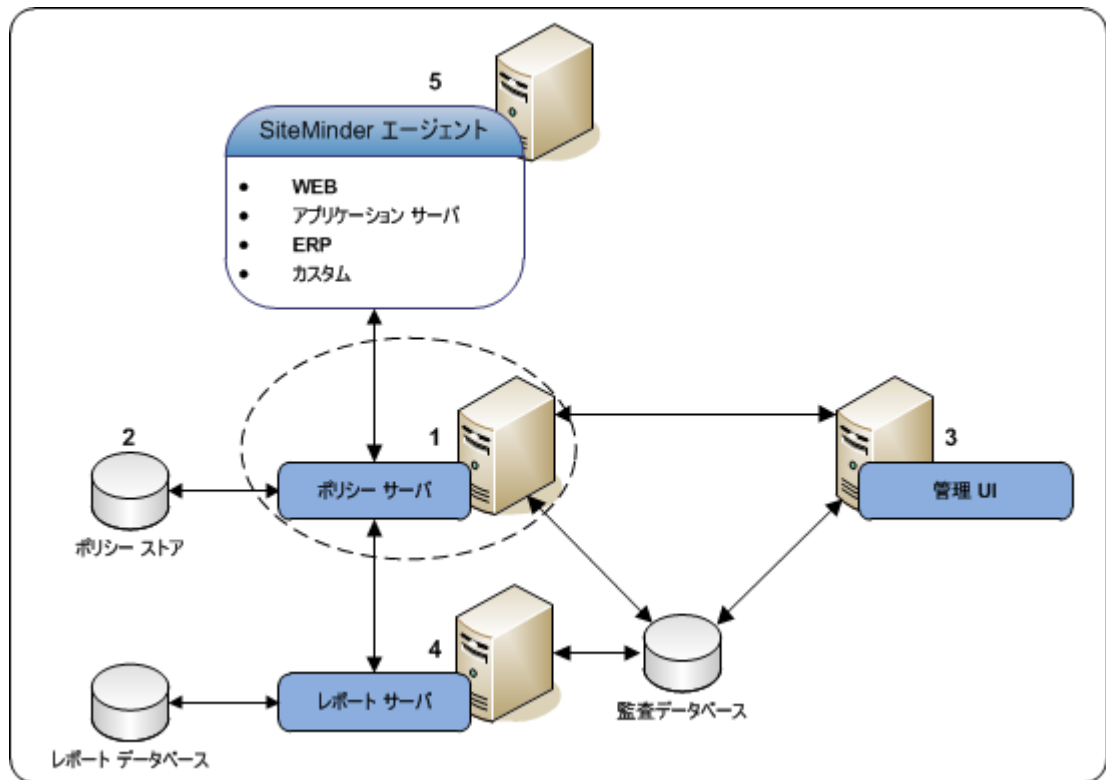
[スクリプト インターフェース](#) (P. 60)

インストール ロード マップ

以下の図はサンプル SiteMinder のインストールを示しており、各コンポーネントのインストールおよび設定の指示がリスト表示されています。以下の点を考慮します。

- ポリシー サーバのホスト システムが、最小のシステム要件を満たすことを確認します。ポリシー サーバのインストールする前に確認することをお勧めします。
- 点線で囲まれているのがポリシー サーバです。このコンポーネントをすぐにインストールします。

図1: インストール ロードマップ



Windows でポリシー サーバをインストールする前に

ポリシー サーバをインストールする前に以下の点を考慮します。

- **管理者権限** -- ローカル管理者権限を持つ Windows アカウントはポリシー サーバをインストールする必要があります。
- **システム パスの長さ** -- システム パスの長さが 1024 文字を超える場合、ポリシー サーバのインストールは失敗します。この制限は、SiteMinder によって追加されたディレクトリの有無にかかわらず適用されます。

注: 最適の結果を得るには、SiteMinder の前のシステム パスを約 700 文字にトリミングすることをお勧めします。

- **(Windows 2008) ファイアウォール設定** -- ポリシー サーバを Windows 2008 にインストールしている場合は、Windows ファイアウォール設定を更新し、以下のポートへの受信接続を可能にします。
 - 44441
 - 44442
 - 44443

これらのポートはデフォルトのポリシー サーバアカウントिंग、認証および認可ポートです。ポリシー サーバをインストールした後にこれらのポートを変更する場合は、必ずそれぞれのポートへの受信接続を許可します。

注: 詳細については、Microsoft のドキュメントを参照してください。

- **環境変数** -- ポリシー サーバインストールによって環境変数が変更されます。

Windows でポリシー サーバをインストールする方法

ポリシー サーバをインストールするには、以下の手順に従います。

1. ポリシー サーバ コンポーネントの考慮事項を確認します。
2. ポリシー ストアの考慮事項を確認します。
3. FIPS の注意事項を確認します。
4. ポリシー サーバ インストーラ用の情報を収集します。
5. ポリシー サーバのインストーラを実行します。

6. (オプション) SNMP を設定した場合は、SNMP イベント トラッピングを有効にします。
7. (オプション) ポリシー ストアを設定するためにポリシー サーバ インストーラを使用しない場合は、手動でポリシー ストアを設定します。

詳細情報:

[ポリシー サーバの再インストール](#) (P. 56)

ポリシー サーバ コンポーネントの考慮事項

ポリシー サーバに加えて、インストーラは以下のコンポーネントをインストールし設定できます。ポリシー サーバをインストールする前に以下の点を確認します。

- OneView モニタ

OneView モニタは、SiteMinder コンポーネントの監視を有効にします。

注: OneView モニタの設定には、サポートされている Java SDK および ServletExec/AS が必要です。

- ポリシー ストア

注: キー ストアおよび証明書データ ストアは自動的に設定され、ポリシー ストアと連結されます。

- SNMP

ポリシー サーバをインストールする前に、Windows オペレーティングシステムに SNMP サービス (マスタ OS エージェント) がインストールされていることを確認してください。

注: SNMP サービスのインストールの詳細については、Windows オンライン ヘルプ システムを参照してください。

■ 監査ログ

リレーショナル データベースまたはテキスト ファイルのいずれかに監査ログを格納できます。ポリシー サーバをインストールした後、デフォルトでは監査ログは ODBC ではなくテキスト ファイルに設定されます。

注: サポートされている CA およびサードパーティ コンポーネントのリストについては、テクニカル サポート サイトの **SiteMinder 12.52 SP1** プラットフォームのサポート マトリックスを参照してください。

ポリシー ストアの考慮事項

ポリシー サーバ インストーラまたはポリシー サーバ設定ウィザードを実行する前に、以下の点を考慮します。

- ポリシー サーバ インストーラおよびポリシー サーバ設定ウィザードは、以下のいずれかのストアをポリシー ストアとして自動的に設定できます。
 - Microsoft Active Directory 軽量ディレクトリ サービス (AD LDS)
注: ポリシー ストアとして AD LDS を設定するための要件を満たしていることを確認してください。
 - Oracle® Directory Enterprise Edition (以前の Sun Java™ System ディレクトリ サーバ)
重要: ポリシー サーバ インストーラおよびポリシー サーバ設定ウィザードは、SSL で接続されているポリシー ストアを自動的に設定することができません。
 - Microsoft SQL Server®
 - Oracle RDBMS
- (RDB ポリシー ストア) ポリシー サーバ インストーラまたはポリシー サーバ設定ウィザードは、特定のデータベース情報を使用してポリシー ストア データ ソースを作成します。ポリシー サーバは、このデータ ソースを使用してポリシー ストアと通信します。以下の点を考慮します。
 - データ ソースの名前は CA SiteMinder DSN です。
 - インストーラは、Microsoft ODBC データ ソース管理ツールの [システム DSN] タブにこのデータ ソースを保存します。

- (RDB ポリシー ストア) ポリシー ストアをホストするデータベースサーバが UTF-8 形式でオブジェクトを格納するように設定されていることを確認します。この設定によってポリシー ストア破損の可能性を回避します。
 - (Oracle) データベースが UTF-8 形式でオブジェクトを格納するように設定されていることを確認します。Oracle は、多くのユニコードの文字セットをサポートします。オブジェクトを UTF-8 形式で格納するためのデータベース設定の詳細については、ベンダー固有のドキュメントを参照してください。
 - (SQL Server) データベースがデフォルトの照合 (SQL_Latin1_General_CP1_CI_AS) を使用して設定されていることを確認してください。大文字/小文字を区別した照合を使用すると、予期しない動作をする場合があります。デフォルトの照合を使用してオブジェクトを格納するためのデータベース設定の詳細については、ベンダー固有のドキュメントを参照してください。
- 証明書データ ストアは、ポリシー ストアと自動的に連結されます。
- ポリシー サーバをインストールした後に、他のサポートされたディレクトリ サーバまたはポリシー ストアとしてのリレーショナルデータベースを手動で設定します。ポリシー ストアの手動設定については、このドキュメントに詳述されています。

詳細情報:

[リレーショナルデータベースでの SiteMinder データ ストアの設定 \(P. 313\)](#)

FIPS の考慮点

ポリシー サーバは、米国連邦情報処理規格（FIPS）140-2 準拠と認定された暗号ライブラリを使用します。FIPS は、AES（Advanced Encryption Standard：高度暗号化標準）に適合する暗号モジュールを信用するために使用される米国政府のコンピュータ セキュリティ標準です。SiteMinder 環境が機密データを暗号化するために FIPS 準拠のアルゴリズムを使用する場合のみ、ライブラリは FIPS 操作モードを提供します。

以下の FIPS 操作モードのうちの 1 つで、ポリシー サーバをインストールすることができます。

注: ポリシー サーバが作動する FIPS モードは、システム固有のものです。詳細については、[テクニカル サポート サイト](#)の「SiteMinder 12.52 SP1 プラットフォーム サポート マトリクス」を参照してください。

- **FIPS 互換モード** - インストール中のデフォルト FIPS 操作モードは、FIPS 互換モードです。FIPS 互換モードでは、環境は機密データを暗号化するために既存の SiteMinder アルゴリズムを使用し、旧バージョンの SiteMinder と互換性があります。
 - 環境内での FIPS 準拠のアルゴリズムの使用はオプションです。
 - 組織が FIPS 準拠のアルゴリズムの使用を必要としない場合は、FIPS 互換モードでポリシー サーバをインストールします。追加設定は必要ありません。

- **FIPS 移行モード** - FIPS 移行モードでは、FIPS 互換モードで実行されている 12.52 SP1 環境を FIPS 専用モードに移行することができます。

FIPS 移行モードでは、FIPS 準拠のアルゴリズムのみを使用するために 12.52 SP1 環境を移行する間、12.52 SP1 ポリシー サーバは既存の SiteMinder 暗号化アルゴリズムを使用し続けます。

FIPS 準拠のアルゴリズムのみを使用するために既存の環境を設定している途中の場合は、FIPS 移行モードでポリシー サーバをインストールします。

- **FIPS 専用モード** - FIPS 専用モードでは、環境は機密データを暗号化するために FIPS 準拠のアルゴリズムのみを使用します。

既存の環境が 12.52 SP1 にアップグレードされ、FIPS 準拠のアルゴリズムのみを使用するように設定される場合は、FIPS 専用モードでポリシー サーバをインストールします。

重要: FIPS 専用モードで実行されている 12.52 SP1 環境は、FIPS を完全にサポートしない SiteMinder のバージョン (r12.0 よりも前のバージョン) では動作できません。この制限は、すべてのエージェント、エージェント API の旧バージョンを使用するカスタム ソフトウェア、および PM API またはポリシー サーバが公開するその他の API を使用するカスタム ソフトウェアに適用されます。そのようなソフトウェアをすべて対応する SDK の 12.52 SP1 バージョンと再リンクして、必要な FIPS サポートを実現します。

注: FIPS 準拠のアルゴリズムのみを使用した環境への移行の詳細については、「アップグレードガイド」を参照してください。

インストーラのための情報の収集

ポリシー サーバインストーラは、ポリシー サーバおよびオプション コンポーネントをインストールするために、特定の情報を必要とします。

必要な情報

ポリシー サーバインストーラまたは設定ウィザードを実行する前に以下の必要な情報を収集します。値を記録するために、必要な情報のワークシートを使用できます。

- **Java バージョン** - 使用するポリシー サーバのサポートされた Java ランタイム環境のバージョンを確認します。UNIX で、JAVA_HOME システム変数が JRE の場所に設定されていることを確認します。JAVA_HOME システム変数の設定が間違っている場合、インストーラは JRE を見つけることができません。
- **ポリシー サーバのインストール場所** - インストーラがポリシー サーバをインストールする場所を決定します。

デフォルト : C:\Program Files\CA

- **SiteMinder 暗号化キー値** - 暗号化キー値を決定します。暗号化キーは、大文字小文字の区別がある英数字のキーであり、ポリシー サーバとポリシー ストアの間で送信されるデータを保護します。1 つのポリシー ストアを共有するポリシー サーバはすべて同じ暗号化キーを使用する必要があります。セキュリティ保護を強化する場合には、長い暗号化キーを定義します。

制限：6 ～ 24 文字

- **Advanced Authentication Server 暗号化キー値** - 暗号化キー値を決定します。大文字と小文字を区別し、英数字の値を使用します。このキーは、ポリシー サーバと Advanced Authentication Server (CA SiteMinder for Secure Proxy Server に実行される) の間で送信されるデータを保護します。CA SiteMinder for Secure Proxy Server およびすべてのポリシー サーバで同じキーが必要です。セキュリティ保護を強化する場合には、長い暗号化キーを定義します。

制限：6 ～ 24 文字。

Active Directory LDS サーバ情報

以下の必要な情報を収集し、ポリシー ストアとして Microsoft Active Directory LDS を設定します。

- **システム IP アドレス** - ディレクトリ サーバホストシステムの IP アドレスを識別します。
- **ポート番号** - ディレクトリ サーバがリスンしているポート番号を識別します。
- **アプリケーションパーティションのルート DN** - ポリシー ストア スキーマ データがインストールされるべきディレクトリ サーバ内の、アプリケーションパーティションのルート DN の場所を識別します。

例：dc=ca,dc=com

- **管理者ドメイン名** - guid 値を含む、ディレクトリ管理者のフルドメイン名を識別します。

例：CN=user1、CN=people、CN=Configuration、CN=guid

- **管理者パスワード** - ディレクトリ管理者のパスワードを識別します。

- **代替ユーザ アカウント** - デフォルトでは、SiteMinder はディレクトリサーバと通信するために管理者アカウントを使用します。ただし、ポリシー ストアを管理するために別のユーザ アカウントを使用できます。代替ユーザ アカウントを使用してポリシー ストアを管理するように SiteMinder を設定するための、完全な管理者 DN およびパスワードを識別します。

注: このユーザは、属性およびパスワードを変更するための権限を持っている必要があります。

- **SiteMinder スーパーユーザ パスワード** - デフォルトの SiteMinder スーパーユーザ アカウントは、最大の権限を持っています。デフォルトのスーパーユーザ アカウントのパスワードを決定します。デフォルトアカウントの名前は次のとおりです。

siteminder

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、引用符でパスワードを囲みます。

注: デフォルトのスーパーユーザを日常の操作に使用しないことをお勧めします。正しくは、最初にデフォルトのスーパーユーザを使用して管理 UI にアクセスし、それからスーパーユーザの権限を持つ管理者を作成します。

Oracle Directory Server 情報

ポリシー ストアとして機能する Oracle Directory Server を設定するために以下の必要な情報を収集します。

- **システム IP アドレス** - Oracle Directory Server ホスト システムの IP アドレスを決定します。
- **ディレクトリ インスタンス ポート番号** - Oracle Directory Server インスタンスのポート番号を決定します。

デフォルト: 389

- **ルート DN** - Oracle Directory Server のルート DN を特定します。

例: o=yourorg.com

- **管理者アカウント** - LDAP 管理者アカウント用のユーザ名（バインド DN）を識別します。
例： cn=Directory Manager
- **管理者パスワード** - Oracle Directory Server 管理者用のパスワードを特定します。
- **代替 LDAP 管理者** - デフォルトでは、SiteMinder は LDAP サーバと通信するために LDAP 管理者アカウントを使用します。ただし、ポリシー ストアを管理するために別の LDAP ユーザ アカウントを使用することができます。このように SiteMinder を設定するために、完全な管理者 DN およびパスワードを識別します。

注：このユーザは、属性およびパスワードを変更するための権限を持っている必要があります。

- **SiteMinder スーパーユーザ パスワード** - デフォルトの SiteMinder スーパーユーザ アカウントは、最大の権限を持っています。デフォルトのスーパーユーザ アカウントのパスワードを決定します。デフォルトアカウントの名前は次のとおりです。

siteminder

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、引用符でパスワードを囲みます。

注：デフォルトのスーパーユーザを日常の操作に使用しないことをお勧めします。正しくは、最初にデフォルトのスーパーユーザを使用して管理 UI にアクセスし、それからスーパーユーザの権限を持つ管理者を作成します。

Microsoft SQL Server 情報

Microsoft SQL Server をポリシー ストアとして設定するには、以下の必要な情報を収集します。

データベース サーバ名

データベース ホスト システムの IP アドレスまたは名前を指定します。

注: IPv6 サポートの詳細については、[SiteMinder プラットフォーム サポート マトリクス](#)を参照してください。

データベース名

ポリシー ストアとして機能するデータベースの名前または名前付きインスタンスを指定します。

データベース ポート

データベースがリスンするポートを指定します。

データベース管理者のユーザ名およびパスワード

以下の操作に対する権限を持つ管理者アカウントの名前とパスワードを指定します。

- スキーマの作成。
- オブジェクトの作成、読み取り、変更、削除。

注: SiteMinder スキーマがデータベース内にすでにある場合、作成権限を持つデータベース管理者の認証情報はウィザードで必要とされません。詳細については、「[SQL Server ポリシー ストアの設定 \(P. 338\)](#)」を参照してください。

SiteMinder スーパーユーザ パスワード

デフォルトの SiteMinder スーパーユーザ アカウントには最大の権限があります。デフォルトのスーパーユーザ アカウントのパスワードを決定します。デフォルト アカウントの名前は次のとおりです。

siteminder

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、引用符でパスワードを囲みます。

注: デフォルトのスーパーユーザを日常の操作に使用しないことをお勧めします。正しくは、最初にデフォルトのスーパーユーザを使用して管理 UI にアクセスし、それからスーパーユーザの権限を持つ管理者を作成します。

Oracle RDBMS 情報

ポリシー ストアとして Oracle RDBMS を設定するために以下の必要な情報を収集します。

データベース サーバ名

データベース ホスト システムの IP アドレスまたは名前を指定します。

注: IPv6 サポートの詳細については、SiteMinder プラットフォーム サポート マトリクスを参照してください。

データベース サービス名

ポリシー ストアとして機能するデータベースのサービス名を指定します。

データベース ポート

データベースがリスンするポートを指定します。

データベース管理者ユーザ名

以下の操作に対して権限を持つ管理者アカウントの名前を指定します。

- スキーマの作成。
- オブジェクトの作成、読み取り、変更、削除。

データベース管理者パスワード

管理者アカウントのパスワードを指定します。

SiteMinder スーパーユーザ パスワード

デフォルトの SiteMinder スーパーユーザ アカウントには最大の権限があります。デフォルトのスーパーユーザ アカウントのパスワードを決定します。デフォルト アカウントの名前は次のとおりです。

siteminder

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、引用符でパスワードを囲みます。

注：デフォルトのスーパーユーザを日常の操作に使用しないことをお勧めします。正しくは、最初にデフォルトのスーパーユーザを使用して管理 UI にアクセスし、それからスーパーユーザの権限を持つ管理者を作成します。

OneView モニタ情報

OneView モニタ情報を収集する必要があるのは、OneView モニタを設定する場合のみです。

OneView モニタを設定するには、以下の必要な情報を収集します。
OneView モニタ情報のワークシートを使用して値を記録できます。

- **JDK パス** - 必要な JDK バージョンへのパスを特定します。
- **ServletExec インストールディレクトリ** - ServletExec のインストールディレクトリを特定します。

例： /usr/local/NewAtlanta/ServletExecAS

- **ServletExec ポート番号** - インスタンス用のポート番号を決定します。
- **Sun Java System 管理者ディレクトリ** - 以下の情報を判別します。
 - Sun Java System のインストール場所。
 - Sun Java System Web サーバのインストール場所。

例： /sunjavasystem_home/location

sunjavasystem home

Sun Java System のインストール場所を指定します。

location

Sun Java System Web サーバのインストール場所を指定します。

- **複数の ServletExec インスタンス** - 複数の ServletExec インスタンスがある場合、OneView モニタ GUI を設定するインスタンスを決定します。

ポリシー サーバ インストーラの実行

テクニカル サポート サイトで、インストール メディアを使用してポリシー サーバをインストールします。

注: インストール メディア名のリストについては、「ポリシー サーバリリース ノート」を参照してください。

以下の手順に従います。

1. システムが Windows 要件を満たすことを確認してください。
2. 実行中のすべてのアプリケーションを終了します。
3. 使用している Windows バージョンに応じて以下の手順を実行します。
 - **Windows 2008、Windows 7:** *installation_media* を右クリックし、[管理者として実行] を選択します。
 - **その他の Windows バージョン:** *installation_media* をダブルクリックします。

installation_media

ポリシー サーバのインストール実行可能ファイルの名前を指定します。

インストーラが起動します。

4. ポリシー サーバのインストールおよびポリシー サーバ コンポーネントの設定のために収集された、システムおよびコンポーネント情報を使用します。インストーラを実行するときは、以下の点を考慮します。
 - FIPS 操作モードを選択するよう要求されます。FIPS モードの選択に関する詳細については、「[FIPS の考慮事項 \(P. 37\)](#)」を参照してください。
 - コンポーネントを選択するよう要求されたときに、ポリシー ストアを自動的に設定しない場合は、[ポリシー ストア] チェックボックスをオフにします。ポリシー ストアとしてどのストアが自動設定されるかについての詳細は、「[ポリシー ストアの考慮事項 \(P. 35\)](#)」を参照してください。
 - ポリシー ストアを初期化する場合、デフォルトの SiteMinder ユーザ アカウント用パスワードを入力するよう要求されます。デフォルトのアカウント名は次のとおりです。

siteminder

- 証明書データストアにデフォルトの認証機関証明書をインストールするように促すメッセージが表示されます。インストール後に、証明書データストアに追加の証明書および秘密キーを追加することができます。
- IPv6 アドレスを使用している場合は、エントリを角かっこで囲みます。

例：[2001:db8::1428:57ab]

- Advanced Authentication Server 用の暗号化キーを作成します。環境内のすべてのポリシー サーバに同じキーを使用します。

5. インストール設定を確認し、[インストール] をクリックします。
ポリシー サーバおよび選択されたすべてのコンポーネントが、インストールおよび設定されます。
6. (オプション) インストーラを使用してポリシー ストアを設定しなかった場合は、手動でポリシー ストアを設定します。

注: インストール中に問題があった場合は、インストール ログ ファイルおよびポリシー ストア詳細ファイルを

`siteminder_home¥siteminder¥install_config_info` に置くことができます。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

SNMP イベントトラップの有効化

この手順はオプションです。SNMP トラッピングを有効にする必要があるのは、ポリシー サーバをインストールするときにこの機能を設定した場合のみです。

注: この手順を完了する前に、Windows システムに SNMP サービスがインストールされていることを確認します。

SNMP のイベント トラップを有効にするには、XPSCConfig ユーティリティを使用して、XPSAudit リストにイベントハンドラライブラリ (eventsnmp.dll) を設定します。eventsnmp.dll のデフォルトの場所は `policy_server_home¥bin` です。

`policy_server_home`

ポリシー サーバのインストール場所を示します。

注: イベント ハンドラ ライブラリを設定するための XPSConfig ユーティリティの使用の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

SNMP イベント トラッピングの設定を完了するには、snmptrap.conf ファイルを設定します。必要な SNMP 前提条件および手順の詳細については、SNMP サポートを参照してください。

詳細情報:

[SNMP サポートの概要](#) (P. 559)

ポリシー サーバ インストールのトラブルシューティング

ポリシー サーバ インストールのトラブルシューティングには、以下のファイルを使用します。

- CA_SiteMinder_Policy_Server_release_InstallLog.log

インストール ログは、インストール中に発生した成功、警告、致命的でないエラーおよびエラーの数をリスト表示するサマリ セクションを含みます。個別のインストール アクションは、それぞれのステータスと共にリスト表示されます。

release

ポリシー サーバのリリースを指定します。

場所: *siteminder_home*¥*siteminder*¥*install_config_info*

- ca-ps-details.log

ポリシー ストア ログは、ポリシー ストア ステータスを詳述します。

場所: *siteminder_home*¥*siteminder*¥*install_config_info*

- **smpls.log**

smpls.log は、ポリシー サーバが開始されるときに作成されます。ポリシー サーバが正常にインストールされた場合、このログは以下の行を含みます。

[Info] ジャーナル スレッドが開始され、 60 分以上前のコマンドを削除します。

場所 : *siteminder_home*¥*siteminder*¥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。

ポリシー サーバ設定ウィザード

ポリシー サーバのインストール後、以下のコンポーネントを設定または再設定するためにポリシー サーバ設定ウィザードを使用します。

- ポリシー ストア。
- SNMP サポート。
- OneView モニタ UI。

注: ポリシー サーバ設定ウィザードを使用してポリシー サーバ **FIPS** 操作モードを変更することはできません。ポリシー サーバ **FIPS** 操作モードの変更についての詳細は、「**SiteMinder アップグレードガイド**」を参照してください。

重要: **OneView モニタ UI** または **SNMP** に対し **Oracle iPlanet Web** サーバインスタンスを設定した場合は、ウィザードを使用して新規インスタンスを設定しないでください。新しい **Web** サーバインスタンスを設定すると、既存の **Web** サーバインスタンスが失敗する場合があります。

詳細情報:

[ポリシー ストアの考慮事項 \(P. 35\)](#)

設定ウィザードを使用する方法

ポリシー サーバ設定ウィザードを使用するには、以下の手順に従います。

1. [ポリシー ストアの考慮事項](#) (P. 35)を確認します。
2. ポリシー ストアとして **OneView モニタ UI** または以下のいずれかのストアを設定している場合は、ウィザードに関する情報を収集します。
 - Active Directory LDS
 - Oracle Directory Server
 - SQL Server
 - Oracle RDBMS
3. ウィザードを実行します。

設定ウィザード用の情報の収集

ポリシー サーバ設定ウィザードは、ポリシー サーバ コンポーネントを設定するための具体的情報を必要とします。

注: インストール ワークシートは、ポリシー サーバ インストール ウィザードまたはポリシー サーバ設定ウィザードを使用して、ポリシー サーバ コンポーネントをインストールまたは設定する前に情報を収集し、記録するのに役立つように提供されています。これらのワークシートを印刷し、いずれかのウィザードを実行する前に必要な情報を記録するために使用することをお勧めします。

Active Directory LDS サーバ情報

以下の必要な情報を収集し、ポリシー ストアとして **Microsoft Active Directory LDS** を設定します。

- **システム IP アドレス** - ディレクトリ サーバ ホスト システムの IP アドレスを識別します。
- **ポート番号** - ディレクトリ サーバがリスンしているポート番号を識別します。
- **アプリケーションパーティションのルート DN** - ポリシー ストア スキーマ データがインストールされるべきディレクトリ サーバ内の、アプリケーションパーティションのルート DN の場所を識別します。

例 : dc=ca,dc=com

- **管理者ドメイン名** - `guid` 値を含む、ディレクトリ管理者のフルドメイン名を識別します。

例：CN=user1、CN=people、CN=Configuration、CN=*guid*

- **管理者パスワード** - ディレクトリ管理者のパスワードを識別します。
- **代替ユーザアカウント** - デフォルトでは、SiteMinder はディレクトリサーバと通信するために管理者アカウントを使用します。ただし、ポリシーストアを管理するために別のユーザアカウントを使用できます。代替ユーザアカウントを使用してポリシーストアを管理するように SiteMinder を設定するための、完全な管理者 DN およびパスワードを識別します。

注：このユーザは、属性およびパスワードを変更するための権限を持っている必要があります。

- **SiteMinder スーパーユーザパスワード** - デフォルトの SiteMinder スーパーユーザアカウントは、最大の権限を持っています。デフォルトのスーパーユーザアカウントのパスワードを決定します。デフォルトアカウントの名前は次のとおりです。

siteminder

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、引用符でパスワードを囲みます。

注：デフォルトのスーパーユーザを日常の操作に使用しないことをお勧めします。正しくは、最初にデフォルトのスーパーユーザを使用して管理 UI にアクセスし、それからスーパーユーザの権限を持つ管理者を作成します。

Oracle Directory Server 情報

ポリシー ストアとして機能する Oracle Directory Server を設定するために以下の必要な情報を収集します。

- **システム IP アドレス** - Oracle Directory Server ホスト システムの IP アドレスを決定します。
- **ディレクトリ インスタンス ポート番号** - Oracle Directory Server インスタンスのポート番号を決定します。

デフォルト : 389

- **ルート DN** - Oracle Directory Server のルート DN を特定します。

例 : o=yourorg.com

- **管理者アカウント** - LDAP 管理者アカウント用のユーザ名 (バインド DN) を識別します。

例 : cn=Directory Manager

- **管理者パスワード** - Oracle Directory Server 管理者用のパスワードを特定します。

- **代替 LDAP 管理者** - デフォルトでは、SiteMinder は LDAP サーバと通信するために LDAP 管理者アカウントを使用します。ただし、ポリシー ストアを管理するために別の LDAP ユーザアカウントを使用することができます。このように SiteMinder を設定するために、完全な管理者 DN およびパスワードを識別します。

注: このユーザは、属性およびパスワードを変更するための権限を持っている必要があります。

- **SiteMinder スーパーユーザ パスワード** - デフォルトの SiteMinder スーパーユーザアカウントは、最大の権限を持っています。デフォルトのスーパーユーザアカウントのパスワードを決定します。デフォルトアカウントの名前は次のとおりです。

siteminder

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、引用符でパスワードを囲みます。

注: デフォルトのスーパーユーザを日常の操作に使用しないことをお勧めします。正しくは、最初にデフォルトのスーパーユーザを使用して管理 UI にアクセスし、それからスーパーユーザの権限を持つ管理者を作成します。

Microsoft SQL Server 情報

Microsoft SQL Server をポリシー ストアとして設定するには、以下の必要な情報を収集します。

データベース サーバ名

データベース ホスト システムの IP アドレスまたは名前を指定します。

注: IPv6 サポートの詳細については、SiteMinder プラットフォーム サポート マトリクスを参照してください。

データベース名

ポリシー ストアとして機能するデータベースの名前または名前付きインスタンスを指定します。

データベース ポート

データベースがリスンするポートを指定します。

データベース管理者のユーザ名およびパスワード

以下の操作に対する権限を持つ管理者アカウントの名前とパスワードを指定します。

- スキーマの作成。
- オブジェクトの作成、読み取り、変更、削除。

注: SiteMinder スキーマがデータベース内にすでにある場合、作成権限を持つデータベース管理者の認証情報はウィザードで必要とされません。詳細については、「[SQL Server ポリシー ストアの設定 \(P. 338\)](#)」を参照してください。

SiteMinder スーパーユーザ パスワード

デフォルトの SiteMinder スーパーユーザ アカウントには最大の権限があります。デフォルトのスーパーユーザ アカウントのパスワードを決定します。デフォルト アカウントの名前は次のとおりです。

siteminder

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、引用符でパスワードを囲みます。

注：デフォルトのスーパーユーザを日常の操作に使用しないことをお勧めします。正しくは、最初にデフォルトのスーパーユーザを使用して管理 UI にアクセスし、それからスーパーユーザの権限を持つ管理者を作成します。

Oracle RDBMS 情報

ポリシー ストアとして Oracle RDBMS を設定するために以下の必要な情報を収集します。

データベース サーバ名

データベース ホスト システムの IP アドレスまたは名前を指定します。

注：IPv6 サポートの詳細については、SiteMinder プラットフォーム サポート マトリクスを参照してください。

データベース サービス名

ポリシー ストアとして機能するデータベースのサービス名を指定します。

データベース ポート

データベースがリスンするポートを指定します。

データベース管理者ユーザ名

以下の操作に対して権限を持つ管理者アカウントの名前を指定します。

- スキーマの作成。
- オブジェクトの作成、読み取り、変更、削除。

データベース管理者パスワード

管理者アカウントのパスワードを指定します。

SiteMinder スーパーユーザ パスワード

デフォルトの SiteMinder スーパーユーザ アカウントには最大の権限があります。デフォルトのスーパーユーザ アカウントのパスワードを決定します。デフォルト アカウントの名前は次のとおりです。

siteminder

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、引用符でパスワードを囲みます。

注：デフォルトのスーパーユーザを日常の操作に使用しないことをお勧めします。正しくは、最初にデフォルトのスーパーユーザを使用して管理 UI にアクセスし、それからスーパーユーザの権限を持つ管理者を作成します。

OneView モニタ情報

OneView モニタ情報を収集する必要があるのは、OneView モニタを設定する場合のみです。

OneView モニタを設定するには、以下の必要な情報を収集します。
OneView モニタ情報のワークシートを使用して値を記録できます。

- **JDK パス** - 必要な JDK バージョンへのパスを特定します。
- **ServletExec インストールディレクトリ** - ServletExec のインストールディレクトリを特定します。

例：/usr/local/NewAtlanta/ServletExecAS

- **ServletExec ポート番号** - インスタンス用のポート番号を決定します。
- **Sun Java System 管理者ディレクトリ** - 以下の情報を判別します。
 - Sun Java System のインストール場所。
 - Sun Java System Web サーバのインストール場所。

例：/sunjavasystem_home/location

sunjavasystem home

Sun Java System のインストール場所を指定します。

location

Sun Java System Web サーバのインストール場所を指定します。

- 複数の **ServletExec** インスタンス - 複数の **ServletExec** インスタンスがある場合、OneView モニタ GUI を設定するインスタンスを決定します。

設定ウィザードの実行

設定ウィザードを実行する方法

1. 実行中のすべてのアプリケーションを終了します。
2. `siteminder_home¥siteminder¥install_config_info` に移動し、`ca-ps-config.exe` をダブルクリックします。

ポリシー サーバ設定ウィザードが起動します。

siteminder_home

ポリシー サーバのインストールパスを指定します。

重要: Windows Server 2008 上でこのウィザードを実行している場合は、実行ファイルを管理者権限で実行します。管理者としてシステムにログインしている場合でも、これらの権限を使用します。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。

3. ポリシー ストアおよび個別のコンポーネントを設定するために収集したシステムおよびコンポーネント情報を使用します。

注: LDAP インスタンスを初期化するように要求されたときは、新しいポリシー ストア インスタンスを設定するためにのみ、初期化します。

4. インストール設定を確認し、[インストール] をクリックします。

ウィザードによって、選択したコンポーネントをポリシー サーバと連動するように設定します。

注: これには数分間かかる場合があります。

5. [完了] をクリックし、システムを再起動します。

選択したコンポーネントが設定されます。

注: 問題が発生する場合、`siteminder_home¥siteminder¥install_config_info` にあるインストール ログ ファイルおよびポリシー ストア詳細ファイルを参照してください。

siteminder_home

ポリシー サーバのインストールパスを指定します。

詳細情報:

[ポリシー サーバインストールのトラブルシューティング \(P. 47\)](#)

ポリシー サーバの再インストール

同じバージョンの既存のポリシー サーバにポリシー サーバを再インストールすると、失われたアプリケーション ファイルをリストアしたり、ポリシー サーバのデフォルト インストール設定をリストアできます。

ポリシー サーバを再インストールする方法

1. ポリシー サーバ管理コンソールを使用して、ポリシー サーバを停止します。
注: ポリシー サーバの停止および起動の詳細については、「ポリシー サーバ管理ガイド」を参照してください。
2. ポリシー サーバ管理コンソールを閉じます。
3. ポリシー サーバをインストールします。
4. ポリシー サーバ管理コンソールを使用して、ポリシー サーバを起動します。

Windows でポリシー サーバをアンインストールする方法

ポリシー サーバをアンインストールするには、以下の手順に従います。

1. パス システム変数に JRE を設定します。
2. ポリシー サーバ管理コンソールのすべてのインスタンスをシャットダウンします。
3. エージェント ホスト ファイルからポリシー サーバの参照を削除します。
4. ポリシー サーバをアンインストールします。

Path 変数での JRE の設定

ポリシー サーバ、Web エージェントおよび SDK をアンインストールする際は、Path 変数に JRE を設定します。これにより、アンインストールプログラムが停止して以下のエラー メッセージを発行するのを防ぎます。

- "Could not find a valid Java virtual machine to load. You need to reinstall a supported Java virtual machine."
- "No Java virtual machine could be found from your PATH environment variable. You must install a VM prior to running this program."

PATH 変数に JRE を設定する方法

1. Windows のコントロールパネルを開きます。
2. [システム] をダブルクリックします。
3. [環境変数] ダイアログ ボックスで、Path システム変数に JRE の場所を追加します。

エージェント ホスト ファイルからのポリシー サーバの参照の削除

ポリシー サーバをアンインストールしたら、Web エージェントからの予期しない結果を防止するために、SmHost.conf ファイルからポリシー サーバの参照を削除します。

ポリシー サーバの参照を削除する方法

1. `web_agent_home/config` に移動します。

`web_agent_home`

Web エージェントのインストール ディレクトリを示します。

2. テキスト エディタで SmHost.conf ファイルを開きます。
3. 「policyserver=」 から始まる行を削除します。

注: この行は、アンインストールしているポリシー サーバの IP アドレスおよびポート番号を含んでいます。

4. SmHost.conf を保存します。

これで SmHost.conf ファイルは、アンインストールするポリシー サーバを参照しなくなります。

すべての SiteMinder プロセスの停止

ポリシー サーバをアンインストールする前に、ポリシー サーバファイルが安全に削除されるように、**SiteMinder** プロセスをすべて停止します。

次の手順に従ってください:

1. Windows システムにログインします。
2. [管理ツール] から、[サービス] を開きます。
3. **SiteMinder** ポリシー サーバ サービスまでスクロールし、[停止] を選択します。

すべての **SiteMinder** プロセスが停止します。

ポリシー サーバのアンインストール

ポリシー サーバが不要になった場合は、アンインストールします。

次の手順に従ってください:

1. Windows の [コントロール パネル] を開き、プログラムのリストに移動します。
2. **CA SiteMinder** ポリシー サーバを右クリックします。
3. [アンインストール/変更] をクリックします。
4. ウィザードの指示に従います。

注: 共有ファイルを削除するように促される場合は、[すべていいえ] をクリックします。

5. 要求された場合はシステムを再起動します。

ポリシー サーバがアンインストールされます。

残存アイテムの削除

ポリシー サーバをアンインストールした後に以下のフォルダ、ファイル、レジストリ設定および仮想ディレクトリを手動で削除します。

■ Windows システム

- `siteminder_home¥bin`
- `siteminder_home¥install_config_info`
- `C:¥Program Files¥ZeroG Registry¥com.zerog.registry.xml`

重要: ポリシー サーバを再インストールする前にアイテムをすべて削除します。

- **AdventNet ソフトウェア レジストリ エントリ** — ポリシー サーバをインストールする前に、ソフトウェアがシステム上になかった場合にのみ、AdventNet ソフトウェア レジストリ エントリを削除します。このレジストリ エントリは `HKEY_LOCAL_MACHINE¥SOFTWARE¥Advent,Inc.` にあります。
- **IIS 仮想ディレクトリ** — IIS Microsoft 管理コンソールを使用して以下の SiteMinder 仮想ディレクトリを削除します。
 - 'SiteMinder'
 - 'SiteMinderCgi'
 - 'SiteMinderMonitor'
 - 'netegrity_docs'

残りのサービスの削除

ポリシー サーバをアンインストールし、マシンを再起動した後、以下のサービスが削除されていない場合があります。

- SiteMinder 状態監視サービス
- SiteMinder ポリシー サーバ
- SNMP エージェント

手動で残りのサービスを削除する方法

1. 各サービスを停止します。
2. 必要に応じて、以下の Windows レジストリ キーを削除します。

`HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥<Registry_Key_Name>`

Registry_Key_Name

削除するサービスのレジストリ キー名を指定します。

- SMServMon (SiteMinder 状態監視サービス)
- SMPolicySrv (SiteMinder ポリシー サーバ)
- エージェント サービス (SNMP エージェント)

残りのサービスが削除されます。

スクリプト インターフェース

コマンドライン インターフェースでは、Perl のスクリプトを作成して、ポリシー ストアを設定および管理できます。 インストールプログラムによって、Perl の完全版がインストールされ、*siteminder_installation/CLI* ディレクトリ内にインターフェース ファイルが配置されます。

siteminder_installation

SiteMinder のインストール場所を示します。

例： /home/smuser/siteminder/CLI

コマンドライン インターフェースを使用するには、ユーザのシステムの PATH 環境変数で、以下のディレクトリがユーザのマシン上の他の Perl の bin ディレクトリの前にあることを確認します。

例： /home/smuser/siteminder/CLI/bin

注: スクリプト インターフェースの詳細については、「Programming Guide for Perl」を参照してください。

第 5 章: UNIX システムでのポリシー サーバのインストール

このセクションには、以下のトピックが含まれています。

[インストールロードマップ](#) (P. 62)

[Solaris 10 ゾーン サポート](#) (P. 63)

[ポリシー サーバのインストールの準備方法](#) (P. 65)

[UNIX でポリシー サーバをインストールする前に](#) (P. 70)

[UNIX でポリシー サーバをインストールする方法](#) (P. 71)

[ポリシー サーバインストールのトラブルシューティング](#) (P. 89)

[自動スタートアップの設定](#) (P. 89)

[ポリシー サーバ設定ウィザード](#) (P. 90)

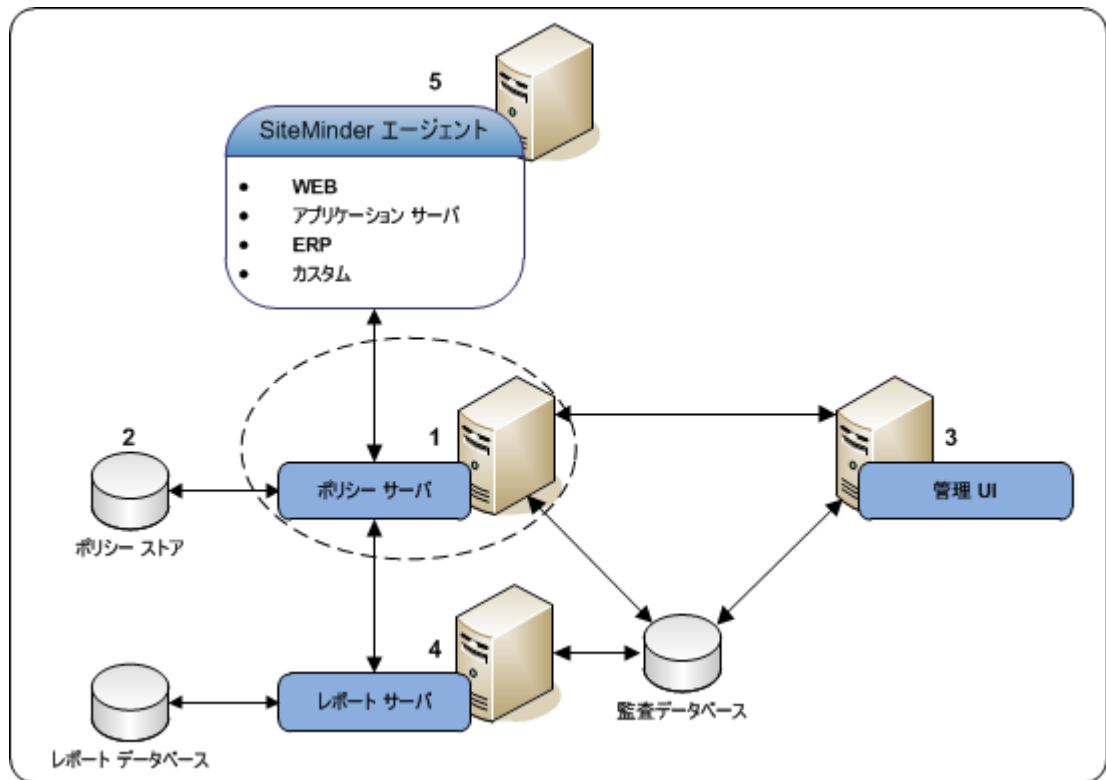
[UNIX でポリシー サーバをアンインストールする方法](#) (P. 94)

インストール ロード マップ

以下の図はサンプル SiteMinder のインストールを示しており、各コンポーネントのインストールおよび設定の指示がリスト表示されています。以下の点を考慮します。

- ポリシー サーバのホスト システムが、最小のシステム要件を満たすことを確認します。ポリシー サーバのインストールする前に確認することをお勧めします。
- 点線で囲まれているのがポリシー サーバです。このコンポーネントをすぐにインストールします。

図2: インストール ロードマップ



Solaris 10 ゾーン サポート

SiteMinder ポリシー サーバは以下のゾーンでサポートされています。

- グローバル ゾーン
- 疎ルート ゾーン
- 完全ルート ゾーン

Solaris 10 環境で 1 つ以上のポリシー サーバの実行を予定する場合は、以下のシナリオを考慮します。

グローバル ゾーン サポート

グローバル ゾーン設定は、すべてのゾーンにわたって、実装を単一のポリシー サーバ インスタンスに限定します。 具体的な内容は次のとおりです。

- 単一のポリシー サーバ インスタンスのみが、グローバル ゾーンでサポートされています。
- グローバル ゾーンに別のポリシー サーバ インスタンスがある場合、ポリシー サーバ インスタンスは疎ルート ゾーンでサポートされません。
- グローバル ゾーンに別のポリシー サーバ インスタンスがある場合、ポリシー サーバ インスタンスは完全ルート ゾーンでサポートされません。

例: グローバル ゾーン サポート

疎ルートまたは完全ルートゾーン 1 (ポリシー サーバのサポートなし)	疎ルートまたは完全ルートゾーン 2 (ポリシー サーバのサポートなし)	疎ルートまたは完全ルートゾーン 3 (ポリシー サーバのサポートなし)
グローバルゾーン (ポリシー サーバ 1)		

注: ただし、Web エージェントはいずれかのゾーンで同時に実行される場合があります。

疎ルート ゾーン サポート

疎ルート ゾーン設定は、複数の疎ルート ゾーンで実行されている複数のポリシー サーバインスタンスをサポートします。具体的な内容は次のとおりです。

- 1つのポリシー サーバインスタンスのみが、各疎ルート ゾーンでサポートされています。
- 各疎ルート または完全ルート ゾーンに 1つのポリシー サーバインスタンスがあれば、同時ポリシー サーバインスタンスは疎ルート ゾーンおよび完全ルート ゾーンでサポートされます。
- グローバル ゾーンおよび疎ルート ゾーンでのポリシー サーバインスタンスの同時実行はサポートされません。

例: 疎ルートゾーン サポート

疎ルートゾーン 1 (ポリシー サーバ 1)	疎ルートゾーン 2 (ポリシー サーバ 2)	疎ルートゾーン 3 (ポリシー サーバ 3)	完全ルートゾーン 1 (ポリシー サーバ 4)
グローバルゾーン (ポリシー サーバのサポートなし)			

注: ただし、Web エージェントはいずれかのゾーンで同時に実行される場合があります。

完全ルートゾーン サポート

完全ルート ゾーンの設定は、複数の完全ルート ゾーンで実行されている複数のポリシー サーバインスタンスをサポートします。具体的な内容は次のとおりです。

- 1つのポリシー サーバインスタンスのみが、各完全ルート ゾーンでサポートされています。
- 各完全ルート ゾーンまたは疎ルート ゾーンに 1つのポリシー サーバインスタンスがあれば、同時ポリシー サーバインスタンスは完全ルート ゾーンおよび疎ルート ゾーンでサポートされます。
- グローバル ゾーンおよび完全ルート ゾーンでのポリシー サーバインスタンスの同時実行はサポートされません。

例: 完全ルートゾーンサポート

疎ルートゾーン 1 (ポリシー サーバ 1)	疎ルートゾーン 2 (ポリシー サーバ 2)	疎ルートゾーン 3 (ポリシー サーバ 3)	完全ルートゾーン 1 (ポリシー サーバ 4)
グローバルゾーン (ポリシー サーバのサポートなし)			

注: ただし、Web エージェントはいずれかのゾーンで同時に実行される場合があります。

ポリシー サーバのインストールの準備方法

UNIX システムにポリシー サーバをインストールする前に、必要に応じて、以下の手順を完了します。

1. ポリシー サーバ ホスト システムが最小のオペレーティング システムパッチ要件を満たすかどうかを確認します。詳細については、「ポリシー サーバリリース ノート」を参照してください。
2. (Red Hat Linux) Red Hat オペレーティング システムはパフォーマンスのエントロピーに依存します。コンポーネントをインストールする前にエントロピーを増やします。十分なエントロピーがないと、インストールの完了までに非常に時間がかかることがあります。以下のコマンドを使用します。

```
mv /dev/random /dev/random.org
ln -s /dev/urandom /dev/random
```

3. (Linux) 必要な Linux ライブラリがポリシー サーバのホスト システムにインストールされていることを確認します。
4. 新規 UNIX アカウントを作成します。
5. UNIX システム パラメータを変更します。
6. ローカライズ変数を設定解除します。
7. LANG 環境変数を設定解除します。

必要とされる Linux ライブラリ

Linux オペレーティング環境上で動作するコンポーネントには、特定のライブラリ ファイルが必要です。正しいライブラリをインストールしないと、以下のエラーを引き起こす場合があります。

```
java.lang.UnsatisfiedLinkError
```

このコンポーネントの Linux バージョンをインストール、設定、またはアップグレードする場合は、ホスト システム上で以下のパッケージが必要になります。

Red Hat 5.x

- `compat-gcc-34-c++-3.4.6-patch_version.l386`
- `libstdc++-4.x.x-x.el5.i686.rpm`
- `libidn.so.11.rpm`
- `ncurses`

Red Hat 6.x

- libstdc++-4.x.x-x.el6.i686.rpm
- libidn-1.18-2.el6.i686
- libXext.i686.rpm
- libXrender.i686.rpm
- libXtst.i686.rpm
- libidn.so.11.rpm
- ncurses

Red Hat 6.x (64 ビット) の場合はさらに以下 :

注: 64 ビット Red Hat 6.x に必要な RPM パッケージはすべて、32 ビットの
パッケージです。

- libXau-1.0.5-1.el6.i686.rpm
- libxcb-1.5-1.el6.i686.rpm
- compat-db42-4.2.52-15.el6.i686.rpm
- compat-db43-4.3.29-15.el6.i686.rpm
- libX11-1.3-2.el6.i686.rpm
- libXrender-0.9.5-1.el6.i686.rpm
- libexpat.so.1 (expat-2.0.1-11.el6_2.i686.rpm により提供)
- libfreetype.so.6 (freetype-2.3.11-6.el6_2.9.i686.rpm により提供)
- libfontconfig.so.1 (fontconfig-2.8.0-3.el6.i686.rpm により提供)
- libICE-1.0.6-1.el6.i686.rpm
- libuuid-2.17.2-12.7.el6.i686.rpm
- libSM-1.1.0-7.1.el6.i686.rpm
- libXext-1.1-3.el6.i686.rpm
- compat-libstdc++-33-3.2.3-69.el6.i686.rpm
- compat-db-4.6.21-15.el6.i686.rpm
- libXi-1.3-3.el6.i686.rpm
- libXtst-1.0.99.2-3.el6.i686.rpm
- libXft-2.1.13-4.1.el6.i686.rpm
- libXt-1.0.7-1.el6.i686.rpm

- libXp-1.0.0-15.1.el6.i686.rpm
- libstdc++.i686.rpm
- compat-libtermcap.rpm
- libidn.i686.rpm
- ncurses

Linux 上で Korn シェル(ksh)パッケージが必要

Linux プラットフォームでのポリシー サーバのインストールおよびアップグレードに、ksh Korn シェルが必要です。ユーザの Linux 環境に適したバージョンがインストールされていることを確認します。

Red Hat 5.x(32 ビット)

ksh-20100621-12.el5.i386.rpm

Red Hat 5.x(64 ビット)

ksh-20100621-12.el5.x86_64.rpm

Red Hat 6.x(32 ビット)

ksh-20100621-16.el6.i686.rpm

Red Hat 6.x(64 ビット)

ksh-20100621-16.el6.x86_64.rpm

新規 UNIX アカウントの作成

ksh としてデフォルト シェルを持つ UNIX アカウントを作成します。以下のようにアカウントに名前を付けます。

smuser

重要: 以下の Web サーバ上で OneView モニタ UI を設定するためにインストーラを使用しないでください。

- Oracle iPlanet
- Linux 上の Apache

インストーラは、Web サーバの設定ファイルを変更します。新しい UNIX アカウントには必要なルート権限がありません。

ポリシー サーバをインストールした後、**OneView** モニタ UI を設定するためにルートとしてポリシー サーバ設定ウィザードを使用します。

UNIX システム パラメータの変更

ポリシー サーバがロードの下に配置されると、多数のソケットおよびファイルを開きます。デフォルト制限パラメータがロードに適切でない場合、多くのソケットおよびファイルで問題が起きる場合があります。関連する問題を回避するためにデフォルト制限パラメータを変更します。

デフォルト制限パラメータを表示するには、シェル ウィンドウで以下のコマンドを入力します。

```
ulimit -a
```

以下の例のようなメッセージがシステムに表示されます。

```
$ ulimit -a
time(seconds)                unlimited
file(blocks)                  unlimited
data(kbytes)                   2097148
stack(kbytes)                   8192
coredump(blocks)               unlimited
nofiles(descriptors)           256
vmemory(kbytes)                unlimited
```

例では、**nofiles** パラメータは **256** に設定されています。このパラメータは、このシェルと子シェルが割り当てられたファイル（ソケット + ファイル記述子）の総数です。このパラメータが十分に高い値に設定されていない場合、ポリシー サーバは多数のソケット エラーを返します。最もよく見られるソケット エラーは **10024**、つまり、開いているファイルが多すぎるというエラーです。

ロードでポリシー サーバが適切に動作するように `nofiles` パラメータ値を増やします。この値は、以下のコマンドを実行すると変更できます。

```
ulimit -n
```

たとえば、値を **1024** に設定するには、`smuser` アカウントのプロファイルファイルに以下のコマンドを配置します。

```
ulimit -n 1024
```

ポリシー サーバは、それへの接続数について、`smuser` アカウント `ulimit` 内の `nofiles` パラメータによってバインドされます。

ローカライズ変数の設定解除

`LC_*` 変数は、`smuser` アカウントのプロファイルファイルにデフォルトで設定されることがあります。`LC_*` 環境変数の使用は許可されません。ポリシー サーバをインストールする前にこれらを設定解除します。

`LC_*` 環境変数を設定解除するには、`smuser` アカウントのプロファイルファイルを開き、これらを設定解除します。

LANG 環境変数の設定解除

`LANG` 環境変数は許可されません。ポリシー サーバをインストールする前に設定解除します。

変数を設定解除するには、`smuser` アカウントのプロファイルファイルに `LANG` の設定解除コマンドを追加します。

UNIX でポリシー サーバをインストールする前に

ポリシー サーバをインストールする前に以下の点を考慮します。

- **/tmp の空き容量** - ポリシー サーバのインストールには、`/tmp` ディレクトリに少なくとも **3 GB** の空き容量を必要とします。

- **システム パスの長さ** -- システム パスの長さが 1024 文字を超える場合、ポリシー サーバのインストールは失敗します。この制限は、SiteMinder によって追加されたディレクトリの有無にかかわらず適用されます。
注: 最適な結果を得るには、インストール パスが 700 文字を超えない場所に SiteMinder をインストールすることを推奨します。
- **Telnet または他の端末エミュレーション ソフトウェア** - Telnet または他の端末エミュレーション ソフトウェアを使用してポリシー サーバをインストールする予定である場合、コンソール ウィンドウを使用してインストールを完了します。GUI モードでインストールすると、Java 例外が発生し、インストーラが終了します。
- **Exceed X-windows アプリケーション** -- Exceed X-windows アプリケーションを使用してポリシー サーバインストーラまたはポリシー サーバ設定ウィザード (ca-ps-config.bin) を実行すると、ウィンドウ内のテキストが切り捨てられることがあります。その制限は Exceed 内の利用できないフォントによるものであり、ポリシー サーバのインストールまたは設定には影響ありません。
- **環境変数** -- ポリシー サーバインストールによって環境変数が変更されます。

UNIX でポリシー サーバをインストールする方法

ポリシー サーバをインストールするには、以下の手順に従います。

1. ポリシー サーバ コンポーネントの考慮事項を確認します。
2. ポリシー ストアの考慮事項を確認します。
3. FIPS の注意事項を確認します。
4. ポリシー サーバインストーラ用の情報を収集します。
5. ポリシー サーバのインストーラを実行します。
6. (Linux) Security-Enhanced Linux が有効な場合、SiteMinder に固有の例外を追加します。
7. (オプション) SNMP を設定した場合は、SNMP デーモンを再起動します。

ポリシー サーバコンポーネントの考慮事項

ポリシー サーバに加えて、インストーラは以下のコンポーネントをインストールし設定できます。ポリシー サーバをインストールする前に以下の点を確認します。

- **OneView モニタの UI**

OneView モニタは、SiteMinder コンポーネントの監視を有効にします。

注: OneView モニタを使用するためには、サポートされている Java SDK および ServletExec/AS がシステムにインストールされている必要があります。

- **SNMP**

SNMP サポートを有効にするために以下のアイテムが必要です。

- ルート ユーザのパスワード
- ネイティブ SunSolstice マスタ エージェント

- **ポリシー ストア**

注: キー ストアおよび証明書データ ストアは自動的に設定され、ポリシーと連結されます。

- **監査ログ**

リレーショナルデータベースまたはテキスト ファイルのいずれかに監査ログを格納できます。ポリシー サーバをインストールした後、デフォルトでは監査ログは ODBC ではなくテキスト ファイルに設定されます。

注: サポートされている CA およびサードパーティ コンポーネントのリストについては、テクニカル サポート サイトの SiteMinder 12.52 SP1 プラットフォームのサポート マトリックスを参照してください。

ポリシー ストアの考慮事項

ポリシー サーバインストーラまたはポリシー サーバ設定ウィザードを実行する前に、以下の事項を考慮します。

- ポリシー サーバインストーラおよびポリシー サーバ設定ウィザードは、以下のいずれかのストアをポリシー ストアとして自動的に設定できます。
 - Microsoft Active Directory 軽量ディレクトリ サービス (AD LDS)
注: ポリシー ストアとして AD LDS を設定するための要件を満たしていることを確認してください。
 - Oracle® Directory Enterprise Edition (以前の Sun Java™ System Directory Server)
重要: ポリシー サーバインストーラおよびポリシー サーバ設定ウィザードは、SSL で接続されているポリシー ストアを自動的に設定することができません。
 - Microsoft SQL Server®
 - Oracle RDBMS
- (RDB ポリシー ストア) ポリシー サーバインストーラまたはポリシー サーバ設定ウィザードは、特定のデータベース情報を使用してポリシー ストア データ ソースを作成します。ポリシー サーバは、このデータ ソースを使用してポリシー ストアと通信します。以下の点を考慮します。
 - データ ソースの名前は CA SiteMinder DSN です。
 - インストーラは、system_odbc.ini ファイル (siteminder_home/db 内) にこのデータ ソースを保存します。

siteminder_home

ポリシー サーバのインストールパスを指定します。

- (RDB ポリシー ストア) ポリシー ストアをホストするデータベースサーバが UTF-8 形式でオブジェクトを格納するように設定されていることを確認します。この設定によってポリシー ストア破損の可能性を回避します。
 - (Oracle) データベースが UTF-8 形式でオブジェクトを格納するように設定されていることを確認します。Oracle は、多くのユニコードの文字セットをサポートします。オブジェクトを UTF-8 形式で格納するためのデータベース設定の詳細については、ベンダー固有のドキュメントを参照してください。
 - (SQL Server) データベースがデフォルトの照合 (SQL_Latin1_General_CP1_CI_AS) を使用して設定されていることを確認してください。大文字/小文字を区別した照合を使用すると、予期しない動作をする場合があります。デフォルトの照合を使用してオブジェクトを格納するためのデータベース設定の詳細については、ベンダー固有のドキュメントを参照してください。
- 証明書データ ストアは、ポリシー ストアと自動的に連結されます。
- ポリシー サーバをインストールした後に、他のサポートされたディレクトリ サーバまたはポリシー ストアとしてのリレーショナルデータベースを手動で設定します。ポリシー ストアの手動設定については、このドキュメント内で詳述されています。

詳細情報:

[リレーショナルデータベースでの SiteMinder データ ストアの設定 \(P. 313\)](#)

FIPS の考慮点

ポリシー サーバは、米国連邦情報処理規格（FIPS）140-2 準拠と認定された暗号ライブラリを使用します。FIPS は、AES（Advanced Encryption Standard：高度暗号化標準）に適合する暗号モジュールを信用するために使用される米国政府のコンピュータ セキュリティ 標準です。SiteMinder 環境が機密データを暗号化するために FIPS 準拠のアルゴリズムを使用する場合のみ、ライブラリは FIPS 操作モードを提供します。

以下の FIPS 操作モードのうちの 1 つで、ポリシー サーバをインストールすることができます。

注: ポリシー サーバが作動する FIPS モードは、システム固有のものです。詳細については、[テクニカル サポート サイト](#)の「SiteMinder 12.52 SP1 プラットフォーム サポート マトリクス」を参照してください。

- **FIPS 互換モード** - インストール中のデフォルト FIPS 操作モードは、FIPS 互換モードです。FIPS 互換モードでは、環境は機密データを暗号化するために既存の SiteMinder アルゴリズムを使用し、旧バージョンの SiteMinder と互換性があります。
 - 環境内での FIPS 準拠のアルゴリズムの使用はオプションです。
 - 組織が FIPS 準拠のアルゴリズムの使用を必要としない場合は、FIPS 互換モードでポリシー サーバをインストールします。追加設定は必要ありません。

- **FIPS 移行モード** - FIPS 移行モードでは、FIPS 互換モードで実行されている 12.52 SP1 環境を FIPS 専用モードに移行することができます。

FIPS 移行モードでは、FIPS 準拠のアルゴリズムのみを使用するために 12.52 SP1 環境を移行する間、12.52 SP1 ポリシー サーバは既存の SiteMinder 暗号化アルゴリズムを使用し続けます。

FIPS 準拠のアルゴリズムのみを使用するために既存の環境を設定している途中の場合は、FIPS 移行モードでポリシー サーバをインストールします。

- **FIPS 専用モード** - FIPS 専用モードでは、環境は機密データを暗号化するために FIPS 準拠のアルゴリズムのみを使用します。

既存の環境が 12.52 SP1 にアップグレードされ、FIPS 準拠のアルゴリズムのみを使用するように設定される場合は、FIPS 専用モードでポリシー サーバをインストールします。

重要: FIPS 専用モードで実行されている 12.52 SP1 環境は、FIPS を完全にサポートしない SiteMinder のバージョン (r12.0 よりも前のバージョン) では動作できません。この制限は、すべてのエージェント、エージェント API の旧バージョンを使用するカスタム ソフトウェア、および PM API またはポリシー サーバが公開するその他の API を使用するカスタム ソフトウェアに適用されます。そのようなソフトウェアをすべて対応する SDK の 12.52 SP1 バージョンと再リンクして、必要な FIPS サポートを実現します。

注: FIPS 準拠のアルゴリズムのみを使用した環境への移行の詳細については、「アップグレードガイド」を参照してください。

インストーラのための情報の収集

ポリシー サーバインストーラは、ポリシー サーバおよびオプション コンポーネントをインストールするために、特定の情報を必要とします。

必要な情報

ポリシー サーバインストーラまたは設定ウィザードを実行する前に以下の必要な情報を収集します。

- **JRE の場所** - インストーラがサポートされている JRE を見つけることができるフォルダを特定します。JRE が PATH 変数に正しく設定されていることを確認します。JRE が PATH 変数に正しく設定されていない場合、インストーラはそれを見つけることができません。
- **ポリシー サーバのインストール場所** - インストーラがポリシー サーバをインストールする場所を決定します。

- **暗号化キー値** - 暗号化キー値を決定します。暗号化キーは、大文字小文字の区別がある英数字のキーであり、ポリシー サーバとポリシー ストアの間で送信されるデータを保護します。1つのポリシー ストアを共有するポリシー サーバはすべて同じ暗号化キーを使用する必要があります。セキュリティ保護を強化する場合には、長い暗号化キーを定義します。

制限：6 ～ 24 文字

- **Advanced Authentication Server 暗号化キー値** - 暗号化キー値を決定します。暗号化キーは、大文字小文字の区別がある英数字のキーであり、ポリシー サーバと Advanced Authentication Server（CA SiteMinder for Secure Proxy Server で実行される）の間で送信されるデータを保護します。CA SiteMinder for Secure Proxy Server およびすべてのポリシー サーバで同じキーを共有します。セキュリティ保護を強化する場合には、長い暗号化キーを定義します。

制限：6 ～ 24 文字。

Active Directory LDS サーバ情報

以下の必要な情報を収集し、ポリシー ストアとして Microsoft Active Directory LDS を設定します。

- **システム IP アドレス** - ディレクトリ サーバホストシステムの IP アドレスを識別します。
- **ポート番号** - ディレクトリ サーバがリスンしているポート番号を識別します。
- **アプリケーションパーティションのルート DN** - ポリシー ストア スキーマ データがインストールされるべきディレクトリ サーバ内の、アプリケーションパーティションのルート DN の場所を識別します。

例：dc=ca,dc=com

- **管理者ドメイン名** - guid 値を含む、ディレクトリ管理者のフルドメイン名を識別します。

例：CN=user1、CN=people、CN=Configuration、CN=guid

- **管理者パスワード** - ディレクトリ管理者のパスワードを識別します。

- **代替ユーザ アカウント** - デフォルトでは、SiteMinder はディレクトリサーバと通信するために管理者アカウントを使用します。ただし、ポリシー ストアを管理するために別のユーザ アカウントを使用できます。代替ユーザ アカウントを使用してポリシー ストアを管理するように SiteMinder を設定するための、完全な管理者 DN およびパスワードを識別します。

注: このユーザは、属性およびパスワードを変更するための権限を持っている必要があります。

- **SiteMinder スーパーユーザ パスワード** - デフォルトの SiteMinder スーパーユーザ アカウントは、最大の権限を持っています。デフォルトのスーパーユーザ アカウントのパスワードを決定します。デフォルトアカウントの名前は次のとおりです。

siteminder

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、引用符でパスワードを囲みます。

注: デフォルトのスーパーユーザを日常の操作に使用しないことをお勧めします。正しくは、最初にデフォルトのスーパーユーザを使用して管理 UI にアクセスし、それからスーパーユーザの権限を持つ管理者を作成します。

Oracle Directory Server 情報

ポリシー ストアとして機能する Oracle Directory Server を設定するために以下の必要な情報を収集します。

- **システム IP アドレス** - Oracle Directory Server ホスト システムの IP アドレスを決定します。
- **ディレクトリ インスタンス ポート番号** - Oracle Directory Server インスタンスのポート番号を決定します。

デフォルト: 389

- **ルート DN** - Oracle Directory Server のルート DN を特定します。

例: o=yourorg.com

- **管理者アカウント** - LDAP 管理者アカウント用のユーザ名（バインド DN）を識別します。
例：cn=Directory Manager
- **管理者パスワード** - Oracle Directory Server 管理者用のパスワードを特定します。
- **代替 LDAP 管理者** - デフォルトでは、SiteMinder は LDAP サーバと通信するために LDAP 管理者アカウントを使用します。ただし、ポリシー ストアを管理するために別の LDAP ユーザ アカウントを使用することができます。このように SiteMinder を設定するために、完全な管理者 DN およびパスワードを識別します。

注：このユーザは、属性およびパスワードを変更するための権限を持っている必要があります。

- **SiteMinder スーパーユーザ パスワード** - デフォルトの SiteMinder スーパーユーザ アカウントは、最大の権限を持っています。デフォルトのスーパーユーザ アカウントのパスワードを決定します。デフォルトアカウントの名前は次のとおりです。

siteminder

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、引用符でパスワードを囲みます。

注：デフォルトのスーパーユーザを日常の操作に使用しないことをお勧めします。正しくは、最初にデフォルトのスーパーユーザを使用して管理 UI にアクセスし、それからスーパーユーザの権限を持つ管理者を作成します。

Microsoft SQL Server 情報

Microsoft SQL Server をポリシー ストアとして設定するには、以下の必要な情報を収集します。

データベース サーバ名

データベース ホスト システムの IP アドレスまたは名前を指定します。

注: IPv6 サポートの詳細については、[SiteMinder プラットフォーム サポート マトリクス](#)を参照してください。

データベース名

ポリシー ストアとして機能するデータベースの名前または名前付きインスタンスを指定します。

データベース ポート

データベースがリスンするポートを指定します。

データベース管理者のユーザ名およびパスワード

以下の操作に対する権限を持つ管理者アカウントの名前とパスワードを指定します。

- スキーマの作成。
- オブジェクトの作成、読み取り、変更、削除。

注: SiteMinder スキーマがデータベース内にすでにある場合、作成権限を持つデータベース管理者の認証情報はウィザードで必要とされません。詳細については、「[SQL Server ポリシー ストアの設定 \(P. 338\)](#)」を参照してください。

SiteMinder スーパーユーザ パスワード

デフォルトの SiteMinder スーパーユーザ アカウントには最大の権限があります。デフォルトのスーパーユーザ アカウントのパスワードを決定します。デフォルト アカウントの名前は次のとおりです。

siteminder

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、引用符でパスワードを囲みます。

注: デフォルトのスーパーユーザを日常の操作に使用しないことをお勧めします。正しくは、最初にデフォルトのスーパーユーザを使用して管理 UI にアクセスし、それからスーパーユーザの権限を持つ管理者を作成します。

Oracle RDBMS 情報

ポリシー ストアとして Oracle RDBMS を設定するために以下の必要な情報を収集します。

データベース サーバ名

データベース ホスト システムの IP アドレスまたは名前を指定します。

注: IPv6 サポートの詳細については、SiteMinder プラットフォーム サポート マトリクスを参照してください。

データベース サービス名

ポリシー ストアとして機能するデータベースのサービス名を指定します。

データベース ポート

データベースがリスンするポートを指定します。

データベース管理者ユーザ名

以下の操作に対して権限を持つ管理者アカウントの名前を指定します。

- スキーマの作成。
- オブジェクトの作成、読み取り、変更、削除。

データベース管理者パスワード

管理者アカウントのパスワードを指定します。

SiteMinder スーパーユーザ パスワード

デフォルトの SiteMinder スーパーユーザ アカウントには最大の権限があります。デフォルトのスーパーユーザ アカウントのパスワードを決定します。デフォルト アカウントの名前は次のとおりです。

siteminder

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、引用符でパスワードを囲みます。

注: デフォルトのスーパーユーザを日常の操作に使用しないことをお勧めします。正しくは、最初にデフォルトのスーパーユーザを使用して管理 UI にアクセスし、それからスーパーユーザの権限を持つ管理者を作成します。

OneView モニタ情報

OneView モニタ情報を収集する必要があるのは、OneView モニタを設定する場合のみです。

OneView モニタを設定するには、以下の必要な情報を収集します。
OneView モニタ情報のワークシートを使用して値を記録できます。

- **JDK パス** - 必要な JDK バージョンへのパスを特定します。
- **ServletExec インストールディレクトリ** - ServletExec のインストールディレクトリを特定します。

例: /usr/local/NewAtlanta/ServletExecAS

- **ServletExec ポート番号** - インスタンス用のポート番号を決定します。
- **Sun Java System 管理者ディレクトリ** - 以下の情報を判別します。
 - Sun Java System のインストール場所。
 - Sun Java System Web サーバのインストール場所。

例: /sunjavasystem_home/location

sunjavasystem home

Sun Java System のインストール場所を指定します。

location

Sun Java System Web サーバのインストール場所を指定します。

- **複数の ServletExec インスタンス** - 複数の ServletExec インスタンスがある場合、OneView モニタ GUI を設定するインスタンスを決定します。

GUI モードによるポリシー サーバのインストール

テクニカル サポート サイトで、インストール メディアを使用してポリシー サーバをインストールします。以下の点を考慮します。

- 実行可能権限があることを確認してください。インストール メディアへ実行権限を追加するには、以下のコマンドを実行します。

```
chmod +x installation_media  
installation_media
```

ポリシー サーバ インストーラの実行ファイルを指定します。

- 別のサブネットにわたってポリシー サーバ インストーラを実行すると、クラッシュする場合があります。その問題を回避するために、ホスト システムにポリシー サーバを直接インストールします。

次の手順に従ってください:

1. フォアグラウンド アプリケーションをすべて終了します。
2. シェルを開き、インストール メディアに移動します。
3. 以下のコマンドを入力します。

```
./ca-ps-12.5-cr-unix_version  
cr
```

累積リリース番号を指定します。ベース **r12.5** リリースには累積リリース番号が含まれません。

```
unix_version
```

UNIX バージョンを指定します: **sol** または **linux**。

インストーラが起動します。

注: インストール メディア名のリストについては、「ポリシー サーバ リリース ノート」を参照してください。

4. ポリシー サーバをインストールするために収集した、システムおよびコンポーネント情報を使用します。

インストーラを実行するときは、以下の点を考慮します。

- このシステムに初めてポリシー サーバをインストールする場合には、**OneView モニタ UI** を設定しないでください。インストーラは、UI をホストする **Web** サーバの設定ファイルを変更します。smuser アカウントには必要なルート権限がありません。ポリシー サーバをインストールした後、**OneView モニタ UI** を設定するためにルートとしてポリシー サーバ設定ウィザードを使用します。
- **FIPS** 操作モードを選択するよう要求されます。**FIPS** モードの選択に関する詳細については、「[FIPS の考慮事項 \(P. 75\)](#)」を参照してください。
- ポリシー ストアを手動で設定している場合は、コンポーネントを選択するときに [ポリシー ストア] オプションをクリアします。ポリシー ストアとしてどのストアが自動設定されるかについての詳細は、「[ポリシー ストアの考慮事項 \(P. 73\)](#)」を参照してください。
- ポリシー ストアを初期化する場合、デフォルトの **SiteMinder** ユーザアカウント用パスワードを入力するよう要求されます。デフォルトのアカウント名は以下です。

siteminder

- デフォルトの証明機関 (CA) 証明書を証明書データ ストアにインストールするよう促されます。インストール後に、証明書データストアに追加の証明書および秘密キーを追加することができます。
- IPv6 アドレスを使用している場合は、エントリを角かっこで囲みます。

例 :

[2001:db8::1428:57ab]

- パス情報を切り取ってウィザードに貼り付ける場合は、文字を入力して [次へ] ボタンを有効にします。

5. インストール設定を確認し、[インストール] をクリックします。
ポリシー サーバおよび選択されたすべてのコンポーネントが、インストールおよび設定されます。
注: インストールには数分かかる場合があります。
6. [終了] をクリックします。
インストーラが閉じます。
7. (オプション) ポリシー ストアを設定するためにインストーラを使用しなかった場合は、手動でポリシーを設定します。

注: インストール中に問題があった場合は、インストール ログ ファイルおよびポリシー ストア詳細ファイルを `siteminder_home/siteminder/install_config_info` に置くことができます。

詳細情報:

[ポリシー サーバインストールのトラブルシューティング \(P. 89\)](#)

コンソール モードによるポリシー サーバのインストール

テクニカル サポート サイトで、インストール メディアを使用してポリシー サーバをインストールします。以下の点を考慮します。

- 実行可能権限があることを確認してください。インストール メディアへ実行権限を追加するには、以下のコマンドを実行します。

```
chmod +x installation_media  
installation_media
```

ポリシー サーバインストーラの実行ファイルを指定します。

- 別のサブネットにわたってポリシー サーバインストーラを実行すると、クラッシュする場合があります。その問題を回避するために、ホスト システムにポリシー サーバを直接インストールします。

以下の手順に従います。

1. 実行中のすべてのアプリケーションを終了します。
2. シェルを開き、インストール メディアに移動します。
3. 以下のコマンドを実行します。

```
./ca-ps-12.5-cr-unix_version -i console
```

cr

累積リリース番号を指定します。ベース **r12.5** リリースには累積リリース番号が含まれません。

unix_version

UNIX バージョンを指定します：**sol** または **linux**。

インストーラが起動します。

注: インストール メディア名のリストについては、「[ポリシー サーバ リリース ノート](#)」を参照してください。

4. ポリシー サーバをインストールするために収集した、システムおよびコンポーネント情報を使用します。

情報を入力する場合には、以下の点を考慮します。

- このシステムに初めてポリシー サーバをインストールする場合には、**OneView モニタ UI** を設定しないでください。インストーラは、UI をホストする **Web サーバ** の設定ファイルを変更します。**smuser** アカウントには必要なルート権限がありません。ポリシー サーバをインストールした後、**OneView モニタ UI** を設定するためにルートとしてポリシー サーバ設定ウィザードを使用します。
- **FIPS 操作モード** を選択するよう要求されます。**FIPS モード** の選択に関する詳細については、「[FIPS の考慮事項 \(P. 75\)](#)」を参照してください。
- 設定するコンポーネントを選択するよう要求されます。エントリはカンマ (,) で区切ります。どの機能も選択しないためには、カンマのみを入力します。
- ポリシー ストアを手動で設定している場合は、[ポリシー ストア] を選択しないでください。ポリシー ストアとしてどのストアが自動設定されるかについての詳細は、「[ポリシー ストアの考慮事項 \(P. 73\)](#)」を参照してください。

- ポリシー ストアを初期化する場合、デフォルトの SiteMinder ユーザ アカウント用パスワードを入力するよう要求されます。デフォルトのアカウント名は以下です。

siteminder

- デフォルトの証明機関 (CA) 証明書を証明書データ ストアにインストールするよう促されます。インストール後に、証明書データ ストアに追加の証明書および秘密キーを追加することができます。
- IPv6 アドレスを使用している場合は、エントリを角かっこで囲みます。

例 :

[2001:db8::1428:57ab]

- 新しいポリシー ストア インスタンスを設定する場合は、ポリシー ストアを初期化するだけです。

5. インストール設定を確認し、Enter キーを押します。

ポリシー サーバおよび選択されたすべてのコンポーネントが、インストールおよび設定されます。

注: インストールには数分かかる場合があります。

6. Enter キーを押します。

インストーラが閉じます。

7. (オプション) ポリシー ストアを設定するためにインストーラを使用しなかった場合は、手動でポリシーを設定します。

注: インストール中に問題があった場合は、インストール ログ ファイルおよびポリシー ストア詳細ファイルを

`siteminder_home/siteminder/install_config_info` に置くことができます。

詳細情報:

[ポリシー サーバインストールのトラブルシューティング \(P. 89\)](#)

Security-Enhanced Linux への例外の追加

Security-Enhanced Linux がポリシー サーバ ホスト システム上で有効な場合、環境に SiteMinder- 例外を追加します。例外を追加することで Security-Enhanced Linux テキストの再配置拒否を防ぎます。

次の手順に従ってください:

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

```
chcon -t textrel_shlib_t /siteminder_home/lib/*  
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. 以下のコマンドを実行します。

```
chcon -t textrel_shlib_t /JDK_home/lib/i386/*  
JDK_home
```

必要な JDK のインストールパスを指定します。

4. 以下のコマンドを実行します。

```
chcon -t textrel_shlib_t /JDK_home/lib/i386/server/*  
JDK_home
```

必要な JDK のインストールパスを指定します。

SiteMinder に固有の例外が追加されました。

SNMP デーモンの再起動

SNMP デーモンを再起動する必要があるのは、ポリシー サーバのインストール中に SNMP を設定した場合のみです。

SNMP デーモンを再起動する方法

1. /etc/rc3.d 内で「S76snmpdx stop」と入力します。
SNMP デーモンが停止します。
2. /etc/rc3.d 内で「S76snmpdx start」と入力します。
SNMP デーモンが起動します。

ポリシー サーバ インストールのトラブルシューティング

ポリシー サーバ インストールのトラブルシューティングには、以下のファイルを使用します。

- CA_SiteMinder_Policy_Server_release_InstallLog.log

インストール ログは、インストール中に発生した成功、警告、致命的でないエラーおよびエラーの数をリスト表示するサマリ セクションを含みます。個別のインストール アクションは、それぞれのステータスと共にリスト表示されます。

release

ポリシー サーバのリリースを指定します。

場所： *siteminder_home*¥*siteminder*¥*install_config_info*

- ca-ps-details.log

ポリシー ストア ログは、ポリシー ストア ステータスを詳述します。

場所： *siteminder_home*¥*siteminder*¥*install_config_info*

- smps.log

smps.log は、ポリシー サーバが開始されるときに作成されます。ポリシー サーバが正常にインストールされた場合、このログは以下の行を含みます。

[Info] ジャーナル スレッドが開始され、 60 分以上前のコマンドを削除します。

場所： *siteminder_home*¥*siteminder*¥*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。

自動スタートアップの設定

UNIX システムを再起動するときにポリシー サーバが自動的に再起動するように自動スタートアップを設定します。

次の手順に従ってください:

1. 文字列「`nete_ps_root`」のすべてのインスタンスを **SiteMinder** インストールディレクトリへの明示的なパスに置換することにより、**S98M** スクリプトを変更します。

例: `/export/ca/siteminder`

2. ディレクトリを **siteminder** インストールディレクトリに変更します。
3. 「**su**」と入力して **Enter** キーを押します。

注: **suse** コマンドを使用しないでください。

パスワードの入力を要求されます。

4. **root** パスワードを入力し、**Enter** キーを押します。
5. 「`$ cp S98sm/etc/rc2.d`」と入力し、**Enter** キーを押します。

s98sm は **stop-all** および **start-all** 実行可能ファイルを自動的に呼び出します。これにより、**UNIX** システムが再起動するときに、ポリシー サーバのサービスが停止し、起動します。

注: ポリシー ストアとしてローカル **LDAP** ディレクトリ サーバを使用している場合、ポリシー サーバを自動的に起動する前に、**LDAP** ディレクトリが自動的に起動するように設定する必要があります。

ポリシー サーバ設定ウィザード

ポリシー サーバのインストール後、以下のコンポーネントを設定または再設定するためにポリシー サーバ設定ウィザードを使用します。

- ポリシー ストア。
- **SNMP** サポート。
- **OneView** モニタ UI。

注: ポリシー サーバ設定ウィザードを使用してポリシー サーバ **FIPS** 操作モードを変更することはできません。ポリシー サーバ **FIPS** 操作モードの変更についての詳細は、「**SiteMinder** アップグレードガイド」を参照してください。

重要: OneView モニタ UI または SNMP に対し Oracle iPlanet Web サーバインスタンスを設定した場合は、ウィザードを使用して新規インスタンスを設定しないでください。新しい Web サーバインスタンスを設定すると、既存の Web サーバインスタンスが失敗する場合があります。

詳細情報:

[ポリシー ストアの考慮事項 \(P. 35\)](#)

設定ウィザードを使用する方法

ポリシー サーバ設定ウィザードを使用するには、以下の手順に従います。

1. 設定ウィザードの要件を確認します。
2. [ポリシー ストアの考慮事項 \(P. 73\)](#)を確認します。
3. ポリシー ストアとして OneView モニタ UI または以下のいずれかのストアを設定している場合は、[ウィザードに関する情報を収集します \(P. 49\)](#)。
 - Active Directory LDS
 - Oracle Directory Server
 - SQL Server
 - Oracle RDBMS
4. ウィザードを実行します。

設定ウィザードの要件

ポリシー サーバ設定ウィザードを使用する前に以下の要件を満たす必要があります。

- ポリシー サーバ設定ウィザードには、/tmp に少なくとも 150 MB の空き領域が必要です。
- ローカル管理者権限を持つ UNIX ユーザとしてウィザードを実行します。
- 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。

GUI モードでの設定ウィザードの実行

ポリシー サーバ設定ウィザードを実行し、個別のポリシー サーバコンポーネントを設定します。

次の手順に従ってください:

1. 実行中のアプリケーションをすべて終了します。
2. SiteMinder インストール ディレクトリから `ksh` シェルで以下のスクリプトを実行します。

```
./ca_ps_env.ksh
```

注: ピリオド (.) の間にスペースがあることを確認します。

3. シェルを開き、以下のコマンドを実行します。

```
./ca-ps-config.bin gui
```

設定ウィザードが起動します。

4. ポリシー ストアおよび個別のコンポーネントを設定するために収集したシステムおよびコンポーネント情報を使用します。

注: 新しいポリシー ストア インスタンスを設定する場合にのみ、ポリシー ストア インスタンスを初期化してください。

5. インストール設定を確認し、[インストール] をクリックします。
ウィザードによって、選択したコンポーネントをポリシー サーバと連動するように設定します。

注: インストールには数分かかる場合があります。

6. [終了] をクリックします。

選択したコンポーネントが設定されます。

注: 問題が発生する場合、`siteminder_home/siteminder/install_config_info` にあるインストール ログ ファイルおよびポリシー ストア詳細ファイルを参照してください。

詳細情報:

[ポリシー サーバインストールのトラブルシューティング \(P. 89\)](#)

コンソール モードでの設定ウィザードの実行

ポリシー サーバ設定ウィザードを実行し、個別のポリシー サーバ コンポーネントを設定します。

次の手順に従ってください:

1. 実行中のアプリケーションをすべて終了します。
2. SiteMinder インストール ディレクトリから `ksh` シェルで以下のスクリプトを実行します。

```
./ca_ps_env.ksh
```

注: ピリオド (.) の間にスペースがあることを確認します。

3. シェルを開き、以下のコマンドを実行します。

```
./ca-ps-config.bin -i console
```

設定ウィザードが起動します。

4. ポリシー ストアおよび個別のコンポーネントを設定するために収集したシステムおよびコンポーネント情報を使用します。

注:

- 新しいポリシー ストア インスタンスを設定する場合にのみ、ポリシー ストア インスタンスを初期化してください。
- **Advanced Authentication Server** を設定するには、設定の選択を求められたときに上記のいずれも選択せずに、**Advanced Authentication Server** のマスタ暗号化キーを入力します。

5. インストール設定を確認し、**Enter** キーを押します。

ウィザードによって、選択したコンポーネントをポリシー サーバと連動するように設定します。

注: インストールには数分かかる場合があります。

6. **Enter** キーを押します。

インストーラが閉じます。 選択したコンポーネントが設定されます。

注: 問題が発生する場合、`siteminder_home/siteminder/install_config_info` にあるインストール ログ ファイルおよびポリシー ストア詳細ファイルを参照してください。

詳細情報:

[ポリシー サーバインストールのトラブルシューティング \(P. 89\)](#)

UNIX でポリシー サーバをアンインストールする方法

ポリシー サーバをアンインストールするには、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のすべてのインスタンスをシャットダウンします。
注: ポリシー サーバ管理コンソールのシャットダウンの詳細については、「ポリシー管理ガイド」を参照してください。
2. Path 変数に JRE を設定します。
3. エージェント ホスト ファイルからポリシー サーバの参照を削除します。
4. SiteMinder プロセスをすべて停止します。
5. ポリシー サーバをアンインストールします。
6. IWS から SiteMinder 参照を削除します。
7. ServletExec/AS から SiteMinder 参照を削除します。
8. 残りのアイテムを削除します。

エージェント ホスト ファイルからのポリシー サーバの参照の削除

ポリシー サーバをアンインストールしたら、Web エージェントからの予期しない結果を防止するために、SmHost.conf ファイルからポリシー サーバの参照を削除します。

ポリシー サーバの参照を削除する方法

1. `web_agent_home/config` に移動します。
`web_agent_home`
Web エージェントのインストールディレクトリを示します。
2. テキスト エディタで SmHost.conf ファイルを開きます。

3. 「policyserver=」から始まる行を削除します。

注: この行は、アンインストールしているポリシー サーバの IP アドレスおよびポート番号を含んでいます。

4. SmHost.conf を保存します。

これで SmHost.conf ファイルは、アンインストールするポリシー サーバを参照しなくなります。

PATH 変数での JRE の設定

ポリシー サーバ、Web エージェント、SDK、およびドキュメントをアンインストールする際は、PATH 変数に JRE を設定し、アンインストールプログラムが停止して、以下のエラー メッセージのいずれかが発行されるのを防止します。

PATH 変数に JRE を設定する方法

1. 以下のコマンドを実行します。

```
PATH=$PATH:<JRE>/bin
```

```
JRE
```

JRE の場所を指定します。

2. 以下のコマンドを実行します。

```
export PATH
```

JRE が PATH 変数に設定されます。

すべての SiteMinder プロセスの停止

SiteMinder プロセスをすべて停止し、ポリシー サーバファイルが安全に削除されるようにします。

SiteMinder プロセスをすべて停止する方法

1. smuser アカウントを使用して UNIX システムにログインします。
2. stop-all を実行します。これは、/siteminder ディレクトリにあります。
すべての SiteMinder プロセスが停止します。

ポリシー サーバのアンインストール

ポリシー サーバが不要になった場合は、アンインストールします。

注: このコンポーネントをアンインストールする際には、手動でインストールディレクトリを削除しません。アンインストール シェル スクリプトを実行します。インストールディレクトリのみを削除すると、関連するレジストリはそのまま残されます。このホスト システムにこのコンポーネントを再インストールしようとする場合、エントリは成功したインストールを回避できます。

次の手順に従ってください:

1. ポリシー サーバをインストールしたユーザとしてポリシー サーバ ホスト システムにログインします。

注: ポリシー サーバをインストールしたユーザは必要な **SiteMinder** スクリプトをソースする必要があります。 **SiteMinder** スクリプトがログイン時にソースされない場合、または別のユーザとしてログインした場合は、以下のスクリプトをソースします。

```
smprofile.ksh  
ca_ps_env.ksh
```

2. コンソール ウィンドウ内の以下のディレクトリに移動します。

```
siteminder_home/siteminder/install_config_info/ca-ps-uninstall  
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. 以下のコマンドを実行します。

```
./uninstall
```

アンインストール プログラムが表示されます。

4. Enter キーを押します。

ステータス インジケータは進捗状況を表示します。

5. ディレクトリを **SiteMinder** インストールディレクトリの 1 つ上に変更します。

例: **SiteMinder** インストールディレクトリが
`/export/smuser/ca/siteminder` である場合は、以下に移動します。
`/export/smuser/ca`

6. 以下のコマンドを入力して Enter キーを押します。

```
$ rm -rf siteminder
```

SiteMinder インストール ディレクトリが削除されます。

7. HOME ディレクトリから以下のファイルを開きます。

```
.profile
```

8. smprofile.ksh を含む行を見つけて削除します。

例 :

```
./export/smuser/siteminder/smpfile.ksh
```

9. ファイルを保存します。

ポリシー サーバがアンインストールされます。

IWS からの SiteMinder 参照の削除

ポリシー サーバをアンインストールした後に IWS から手動で SiteMinder 参照を削除します。SiteMinder 参照が obj.conf ファイルおよび magnus.conf ファイルの中に残されています。

IWS から SiteMinder 参照を削除する方法

1. Web サーバの設定にアクセスおよび変更する権限を持つアカウントにログインします。
2. Solaris コマンドラインで、以下に移動します。

```
<SunJavaSystem_home>/https-<hostname>/config
```

obj.conf および magnus.conf ファイルがコンフィグ フォルダ内に表示されます。

3. obj.conf を開き、以下の行を削除します。

```
NameTrans fn="assign-name" from="/servlet/*" name="<MySQLServletExec_instance
name>"
NameTrans fn="assign-name" from="*.jsp*" name="<ServletExec_instance name>"
NameTrans fn="pfx2dir" from="/sitemindermonitor"
dir="/<WebSpheresiteminder_installation>/monitor"
NameTrans fn="pfx2dir" from="/sitemindercgi"
dir="/<MySQLsiteminder_installation>/admin" name="cgi"
NameTrans fn="pfx2dir" from="/siteminder"
dir="/<IWSsiteminder_installation>/admin"
NameTrans fn="pfx2dir" from="/netegrity_docs"
dir="/netegrity/netegrity_documents"
<Object name="<ServletExec_instance name>">
Service fn="ServletExecService" group="<ServletExec_instance name>"
</Object>
```

4. obj.conf ファイルを保存して閉じます。
5. magnus.conf を開き、以下の行を削ぎします。

```
Init fn="init-cgi" SM_ADM_UDP_PORT="44444" SM_ADM_TCP_PORT="44444"
Init fn="load-modules"
shlib="/<Servlet_Exec_Install>/bin/ServletExec_Adapter.so"
funcs="ServletExecInit,ServletExecService"
Init fn="ServletExecInit" <ServletExec_instance
name>.instances="<IP_Address>:<port_number>"
```

6. magnus.conf を保存して閉じます。
7. Web サーバを再起動します。

SiteMinder 参照が IWS から削除されます。

SiteMinder 参照は、IWS 内に表示されなくなります。

StartServletExec からの SiteMinder 参照の削除

StartServletExec から参照を削除する方法

1. ServletExec 設定にアクセスおよび変更する権限を持つアカウントにログインします。
2. Solaris コマンドラインで、
/usr/NewAtlanta/ServletExecAS/ServletExec_instance name フォルダに移動します。

3. StartServletExec スクリプトから以下の行を削除します。

```
CLASSPATH=${NA_LIB}/servlet-api.jar:${NA_LIB}/jsp-  
api.jar:${NA_LIB}/ServletExec60.jar:${NA_LIB}/ServletExecAdmin.jar:${NA_LIB}/  
el-  
api.jar:${NA_LIB}/jasper-el.jar:${JL}/tools.jar:${NA_LIB}/jstl.jar:${NA_LIB}/  
appserv-  
jstl.jar:${NA_LIB}/activation.jar:${NA_LIB}/mail.jar:${HOMEDIRPATH}/classes:/  
siteminder_home/monitor/  
smmonui.jar:/siteminder_home/lib/smconapi.jar:/siteminder_home/lib/smmonclien  
tapi.jar  
$SENAME $HOMEDIR $MIMEFILE $DOCR00TDIR -allow 127.0.0.1 -port $PORT $SEOPTS"  
$SENAME $HOMEDIR $MIMEFILE $DOCR00TDIR -allow 127.0.0.1 -port $PORT $SEOPTS -addl  
"/sitemindermonitor=/siteminder_home/monitor"  
  
siteminder_home
```

ポリシー サーバのインストールパスを指定します。

4. StartServletExec スクリプトを保存して閉じます。
5. ServletExec を再起動します。
アンインストールが完了します。

残存アイテムの削除

ユーザが [ポリシー サーバ] をアンインストールした後、
com.zerog.registry.xml ファイルはシステムに残されます。このファイルを
削除します。

以下のいずれかにこのファイルを置くことができます。

- \$HOME/.com.zerog.registry.xml
- /var/.com.zerog.registry.xml

第 6 章: SiteMinder データを格納するように LDAP ディレクトリ サーバを設定

このセクションには、以下のトピックが含まれています。

[ポリシーまたはキー ストアとしての LDAP ディレクトリ サーバ](#) (P. 101)

[インストール ロードマップ](#) (P. 102)

[重要な考慮事項](#) (P. 103)

[デフォルトのポリシー ストア オブジェクトに関する考慮事項](#) (P. 104)

[ポリシー ストアとしての CA Directory](#) (P. 105)

[セッションストアとしての CA Directory](#) (P. 120)

[ポリシー ストアとしての Active Directory](#) (P. 126)

[ポリシー ストアとしての Domino Directory Server](#) (P. 139)

[ポリシー ストアとしての IBM Directory Server](#) (P. 151)

[ポリシー ストアとしての Microsoft Active Directory LDS](#) (P. 162)

[ポリシー ストアとしての Novell eDirectory](#) (P. 174)

[ポリシー ストアとしての OpenLDAP](#) (P. 188)

[ポリシー ストアとしての Oracle Directory Server](#) (P. 206)

[ポリシー ストアとしての Oracle Internet Directory](#) (P. 219)

[Oracle Unified Directory をポリシー ストアとして設定する方法](#) (P. 233)

[Oracle Virtual Directory をポリシー ストアとして設定する方法](#) (P. 250)

[ポリシー ストアとしての Red Hat Directory Server](#) (P. 262)

[ポリシー ストアとしての Siemens DirX](#) (P. 272)

[個別キー ストアの設定](#) (P. 285)

ポリシーまたはキー ストアとしての LDAP ディレクトリ サーバ

SiteMinder ポリシー ストアとは、すべてのポリシー関連情報のためのリポジトリです。SiteMinder インストールでのすべてのポリシー サーバは、直接またはレプリケーションを通じて、同じポリシー ストア データを共有する必要があります。SiteMinder は、管理者がポリシー ストア データがある格納場所から別の格納場所に移動できるツールを使用してインストールされます。

ポリシー サーバをインストールするとき、自動的にポリシー ストアとして以下のディレクトリ サーバのうちの 1 つを設定できます。

- Microsoft Active Directory 軽量ディレクトリ サービス (AD LDS)
- Oracle Directory Server (以前の Sun Java System ディレクトリ サーバ)

ポリシー ストアを自動的に設定するためにポリシー サーバを使用しない場合は、ポリシー サーバのインストール後に手動でポリシー ストアを設定することができます。さらに、ポリシー サーバのインストール後、ポリシー サーバ管理コンソールを使用してポリシー サーバを既存のポリシー ストアに示すことができます。

注: サポートされている CA およびサードパーティ コンポーネントのリストについては、テクニカルサポートサイトの **SiteMinder 12.52 SP1** プラットフォームのサポートマトリックスを参照してください。

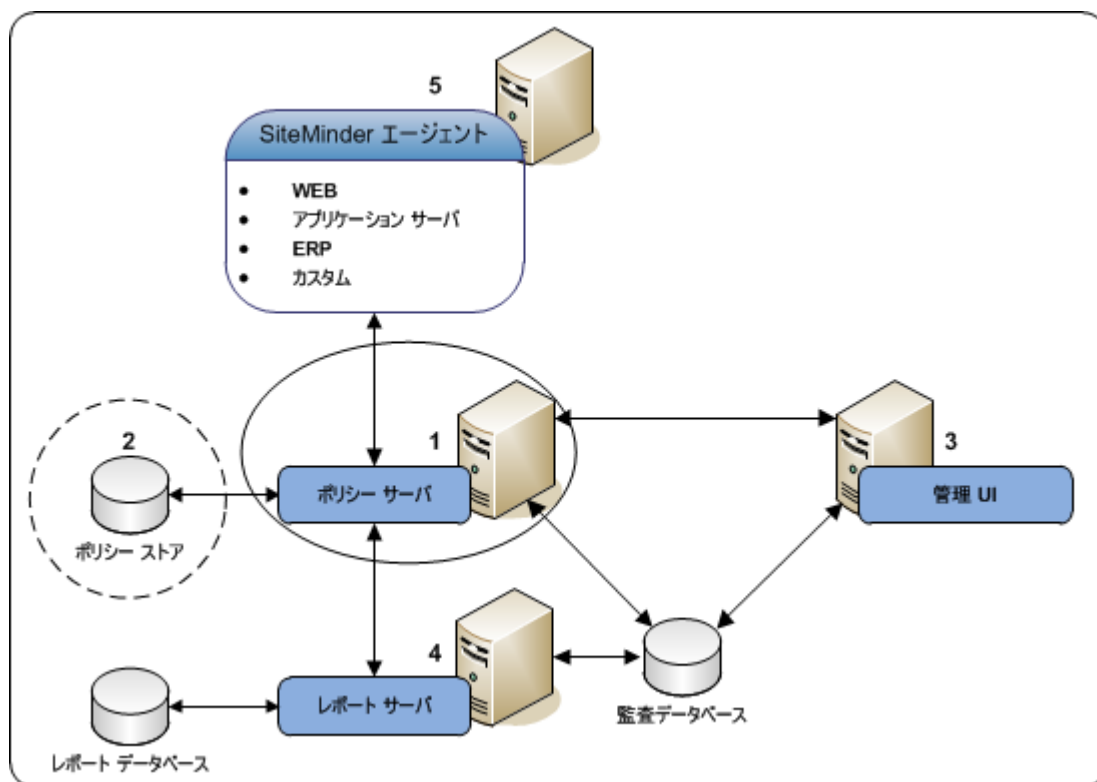
インストール ロード マップ

以下の図はサンプル **SiteMinder** のインストールを示しており、各コンポーネントのインストールおよび設定の指示がリスト表示されています。

- 実線で囲まれているのがポリシー サーバです。ポリシー ストアを設定する前に必要です。ポリシー サーバが環境に含まれていない場合は、続行前にそれをインストールします。
- 点線で囲まれているのがポリシー ストアです。このコンポーネントをすぐに設定します。

以下の図は、単一のポリシー/キー ストア インスタンスを示します。図示されていませんが、環境は個別のポリシーおよびキー ストア用の個別のインスタンスを使用できます。

数式 1: インストール ロードマップ



重要な考慮事項

ポリシー ストアの破損を回避するには、ポリシー ストアを配置するサーバが、UTF-8 形式でオブジェクトを格納するように設定されていることを確認します。UTF-8 形式でオブジェクトを格納するためのサーバの設定の詳細については、そのサーバ用のドキュメントを参照してください。

デフォルトのポリシー ストア オブジェクトに関する考慮事項

ポリシー ストアを設定するとき、以下のデフォルトのポリシー ストア オブジェクト ファイルが利用可能です。

- smpolicy.xml
- smpolicy-secure.xml

両方のファイルには、ポリシー ストアが必要とするデフォルトのオブジェクトが含まれます。

- ポリシー ストアを自動的に設定するためにポリシー サーバ設定ウィザードを使用する場合、ウィザードは単に smpolicy.xml を使用します。
- smpolicy-secure.xml を使用したい場合は、ポリシー ストアを手動で設定します。

両方のファイルはデフォルトのセキュリティ設定を提供します。これらの設定は、管理 UI で利用可能なデフォルトのエージェント設定オブジェクト (ACO) テンプレートで利用可能です。smpolicy-secure ファイルはより制限の厳しいデフォルトのセキュリティ設定を提供します。

smpolicy.xml を選択すると、より制限の厳しいデフォルトのセキュリティ設定を使用する制限はありません。管理 UI を使用して、デフォルトの ACO 設定を変更できます。

以下の表では、両方のファイルに関するセキュリティ設定の概要について説明します。

パラメータ名	smpolicy 値	smpolicy-secure 値
BadCssChars	値なし	<, >, ', ;,), (, &, +, %00
BadQueryChars	値なし	<, >, ', ;,), (, &, +, %00
BadUrlChars	//, ./, /., /*, *., ~, ¥, %00-%1f, %7f-%ff, %25	smpolicy.smdif 値プラス : <, >, ', ;,), (, &, +
EnableCookieProvider	はい	いいえ
IgnoreExt	.class, .gif, .jpg, .jpeg, .png, .fcc, .scc, .sfcc, .ccc, .ntc	すべての smpolicy 値
LimitCookieProvider	いいえ	はい

パラメータ名	smpolicy 値	smpolicy-secure 値
ValidTargetDomain	このファイルには、このパラメータは含まれません。	このパラメータにはデフォルト値はありません。有効なリダイレクトドメインを提供します。 例： validtargetdomain=".example.com"

ポリシー ストアとしての CA Directory

CA Directory はポリシー ストアとして機能できます。1つのディレクトリ サーバ インスタンスは以下として機能させることができます。

- ポリシー ストア
- キーストア

単一のディレクトリ サーバを使用すると管理タスクが簡略化されます。以下のセクションでは、ポリシー データと暗号化キーを格納するよう1つのディレクトリ サーバ インスタンスを設定する方法について説明します。実装に必要な場合は、別のキー ストアを設定できます。

ディレクトリ サーバ情報の収集

CA Directory をポリシー ストアとして設定するには、特定のディレクトリ サーバ情報が必要です。ポリシー ストアを設定する前に、以下の情報を収集します。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。

- **ホスト情報** - CA Directory が実行されているシステムの完全修飾ホスト名または IP アドレスを決定します
- **DSA ポート番号** - DSA がリスニングするポートを決定します。
- **ベース DN** - ポリシー ストア オブジェクトが定義される LDAP ツリーのノードの識別名を決定します。
- **管理 DN** - DSA 内のオブジェクトを管理するために SiteMinder が使用するアカウントの LDAP ユーザ名を決定します。
- **管理者パスワード** - InfoView 管理ユーザのパスワードを決定します。

ポリシー ストアを設定する方法

ポリシー ストアとして CA ディレクトリを設定するには、以下の手順に従います。

1. [ポリシー ストア用の DSA を作成します](#) (P. 106)。
2. [ポリシー ストア スキーマを作成します](#) (P. 107)。
3. [DSA を開きます](#) (P. 109)。
4. [ポリシー ストア データ用のベース ツリー構造を作成します](#) (P. 110)。
5. [DSA 用のスーパーユーザ管理者を作成します](#) (P. 111)。
6. [ポリシー サーバをポリシー ストアにポイントします](#) (P. 111)。
7. [SiteMinder スーパーユーザ パスワードを設定します](#) (P. 112)。
8. [CA Directory キャッシュ設定を確認します](#) (P. 114)。
9. [ポリシー ストア データ定義をインポートします](#) (P. 115)。
10. [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](#) (P. 115)。
11. [管理 UI 登録の準備をします](#) (P. 117)。

ポリシー ストア用の DSA の作成

以下のコマンドを実行して DSA を作成します。

```
dxnewdsa DSA_Name port "o=DSA_Name,c=country_code"
```

DSA_Name

DSA の名前を指定します。

ポート

DSA がリスンするポートを指定します。

o=DSA_Name,c=country_code

DSA プレフィックスを指定します。

例 : "o=psdsa,c=US"

dxnewdsa ユーティリティが新しい DSA を起動します。

注: DSA が自動的に起動しない場合は、以下を実行します。

```
dxserver start DSA_Name
```

ポリシー ストア スキーマの作成

ディレクトリ サーバがポリシー ストアとして機能できるように、ポリシー ストア スキーマを作成します。

重要: デフォルトでは、CA Directory 設定ファイルは読み取り専用です。変更が必要なすべての CA Directory ファイルは書き込み権限で更新される必要があります。ファイルが一度更新されたら、読み取り専用の権限に戻すことができます。また、CA Directory によって提供された default.xxx ファイルはすべて、CA Directory のアップグレード中に上書きされます。読み取り専用ファイルを変更するときは注意が必要です。

次の手順に従ってください:

1. CA Directory `DXHOME¥config¥schema` ディレクトリに以下のファイルをコピーします。

- netegrity.dxc
- etrust.dxc

`DXHOME`

ディレクトリ サーバのインストール パスを示します。

注: netegrity.dxc ファイルは、ポリシー サーバと共に `siteminder_home¥eTrust` にインストールされます。注: etrust.dxc ファイルは、ポリシー サーバとともに `siteminder_home¥xps¥db` にインストールされます。

`siteminder_home`

ポリシー サーバのインストール パスを指定します。

- Windows %DXHOME%
- Unix/Linux : \$DXHOME

2. default.dxc スキーマ ファイルをコピーしてその名前を変更することにより、SiteMinder スキーマ ファイルを作成します。

注: default.dxc スキーマ ファイルは、`DXHOME¥config¥schema¥default.dxc` にあります。

例: default.dxc スキーマ ファイルをコピーし、そのコピーの名前を `smdsa.dxc` に変更します。

3. 新しい SiteMinder スキーマ ファイルの下部への以下の行を追加します。

```
#CA Schema
source "netegrity.dxc";
source "etrust.dxc";
```

4. スキーマを default.dxc から新しい SiteMinder スキーマ ファイルに変更することにより、DSA の DXI ファイル (DSA_Name.dxi) を編集します。

DSA_Name

ポリシーストア用に作成した DSA の名前を表します。

注: DXI ファイルは `DXHOME¥config¥servers` にあります。

5. DSA の DXI ファイルの終わりに、以下の行を追加します。

■ r12

```
# cache configuration
set max-cache-size = 100;
set cache-attrs = all-attributes;
set cache-load-all = true;
set ignore-name-bindings = true;
```

注: max-cache-size エントリは MB 単位の合計キャッシュ サイズです。CA Directory サーバで利用可能な合計メモリとポリシー ストアの合計サイズに基づいてこの値を調整します。

■ r12 SP1 以降

```
# cache configuration
set ignore-name-bindings = true;
```

6. DSA のデフォルト制限 DXC ファイル (default.dxc) をコピーして、SiteMinder DXC ファイルを作成します。

例: デフォルト DXC ファイルをコピーし、そのコピーの名前を `smdsa.dxc` に変更します。

注: デフォルトの DXC ファイルは `DXHOME¥dxserver¥config¥limits` 内にあります。

7. 以下のように新しい DXC ファイル内の設定を編集します。

```
# size limits
set max-users = 1000;
set credits = 5;
set max-local-ops = 1000;
```

```
set max-op-size = 4000;
set multi-write-queue = 20000;
```

注: サイズ制限設定を編集すると、キャッシュ サイズ エラーが CA Directory ログ ファイルに表示されなくなります。

重要: 複数の書き込みキュー設定は、テキスト ベースの設定でのみ使用できます。DSA が DXmanager でセットアップされる場合は、この設定を省略します。

8. DXC ファイルを保存します。
9. default.dxc から新しい SiteMinder 制限ファイルに制限設定を変更することにより、DSA の DXI ファイル (*DSA_Name.dxi*) を編集します。

例: default.dxc から smdsa.dxc に制限設定を変更します。

DSA_Name

ポリシーストア用に作成した DSA の名前を表します。

注: DSA の DXI ファイルは `DXHOME¥config¥servers` にあります。DXmanager を使用して DSA を作成した場合、既存の制限ファイルの名前は `dxmanager.dxc` になります。

10. DSA ユーザとして、以下のコマンドを使用して DSA を停止して再起動します。

```
dxserver stop DSA_Name
dxserver start DSA_Name
```

DSA_Name

DSA の名前を指定します。

ポリシー ストア スキーマが作成されます。

DSA を開く

ディレクトリ サーバのビューを作成し、オブジェクトを管理します。

次の手順に従ってください:

1. データベースは、必ず匿名のログインに対して設定します。
 2. JXplorer GUI を起動します。
 3. 接続アイコンをクリックします。
- 接続設定が表示されます。

4. [ホスト名] フィールドに *host_name_or_IP_address* を入力します。

host_name_or_IP_address

CA Directory が実行されているシステムのホスト名または IP アドレスを指定します。

5. [ポート番号] フィールドに *port_number* を入力します。

port_number

DSA がリスニングするポートを指定します。

6. [ベース DN] フィールドに「*o=DSA_Name,c=country_code*」と入力します。

例： *o=psdsa,c=US*

7. レベル リストから [匿名] を選択して、[接続] をクリックします。

DSA のビューが表示されます。

ポリシーストア データ用のベース ツリー構造の作成

ポリシーストア データを保持するためのベース ツリー構造を作成します。JXplorer GUI を使用し、組織単位を作成します。

次の手順に従ってください：

1. DSA のルート要素を選択します。
2. ルート要素の下に、以下の名前を持つ組織単位を作成します。

Netegrity

3. Netegrity の下に、以下の名前を持つ組織単位（ルート要素）を作成します。

SiteMinder

4. SiteMinder の下に、以下の名前の組織単位（ルート要素）を作成します。

PolicySvr4

5. PolicySvr4 の下に以下の名前の組織単位（ルート要素）を作成します。

XPS

ベース ツリー構造が作成されます。

DSA のスーパーユーザ管理者の作成

SiteMinder が DSA にアクセスするために 使用できる管理者アカウントがない場合にのみ、スーパーユーザ管理者を作成する必要があります。ポリシー サーバは、ポリシー ストアに接続するためにこの情報を必要とします。

次の手順に従ってください:

1. JXplorer GUI を使用して DSA にアクセスします。
2. ポリシー ストアに接続するために SiteMinder が使用できる管理者を作成します。

注: 以下のオブジェクト タイプでユーザを作成します。

`inetOrgPerson`

3. 管理者 DN とパスワードを書き留めておきます。ポリシー サーバからポリシー ストアを参照する場合に、認証情報を使用します。

例:

`dn:cn=admin,o=yourcompany,c=in`

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。

次の手順に従ってください:

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、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。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. データベース リストから以下の値を選択します。

ポリシー ストア

4. ストレージ リストから以下の値を選択します。

LDAP

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
- パスワードの確認入力
- ルート 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。

7. [LDAP 接続のテスト] をクリックして、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確認します。

8. データベース リストから以下の値を選択します。

キーストア

9. ストレージ リストから以下の値を選択します。

LDAP

10. 以下のオプションを選択します。

ポリシー ストア データベースの使用

11. [OK] をクリックします。

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次のとおりです。

siteminder

このアカウントは最大の権限を持っています。

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。

- 管理 UI に初めてアクセスする場合。
- 初めて SiteMinder ユーティリティを管理する場合。
- スーパーユーザ権限で別の管理者を作成する場合。

次の手順に従ってください:

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

`siteminder_home`

ポリシー サーバのインストール パスを指定します。

注: このユーティリティは、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。

2. 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、引用符でパスワードを囲みます。

注: Oracle ポリシー ストアを設定している場合、パスワードは大文字と小文字を区別します。他のすべてのポリシー ストアの場合は、パスワードの大文字と小文字を区別しません。

3. `siteminder_home¥bin` から `smreg` 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。

CA ディレクトリ キャッシュ設定の確認

DXconsole を使用して、DXcache の設定が有効であることを確認することができます。

注: デフォルトでは、DxConsole はローカル ホストからのみアクセス可能です。DxConsole にリモート システムからの接続を承諾させる `set dsa` コマンドの使用の詳細については、「ディレクトリ設定ガイド」を参照してください。

次の手順に従ってください:

1. DSA DXConsole ポートに Telnet を実行するために、コマンドプロンプトから以下のコマンドを入力します。

```
telnet DSA_Host DXconsole_Port
```

DSA_Host

DSA をホストしているシステムのホスト名または IP アドレスを指定します。

注: ローカル ホスト上にいる場合は、「**localhost**」を入力します。ホスト名または IP アドレスを入力すると接続できません。

DXConsole_Port

DXconsole がリスニングするポートを指定します。この値が以下のファイルの `console-port` パラメータに表示されます。

`DXHOME¥config¥knowledge¥DSA_Name.dxc`

デフォルト: DXconsole ポートは `DSA port + 1` の値に設定されます。

例: DSA がポート 19389 で実行されている場合、DXconsole ポートは 19390 です。

DSA 管理コンソールが表示されます。

2. 以下のコマンドを入力します。

```
get cache;
```

DSA 管理コンソールは現在の DSA DXcache の設定を表示し、ディレクトリ キャッシング状態を指定します。

3. 以下のコマンドを入力します。

```
logout;
```

DXconsole を閉じて、システム プロンプトに戻ります。

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 データ定義をインポートすると、ポリシー ストアで作成および格納できるオブジェクトのタイプが定義されます。

次の手順に従ってください:

1. コマンド ウィンドウを開き、*siteminder_home*¥xps¥dd 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. 以下のコマンドを実行します。

```
XPSDDInstall SmMaster.xdd
```

```
XPSDDInstall
```

必要なデータ定義をインポートします。

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 とポリシー サーバで使用するポリシー ストアが設定されます。

以下の点を考慮します。

- 必ず *siteminder_home*¥bin への書き込みアクセス権があることを確認してください。インポートユーティリティは、ポリシー ストア オブジェクトをインポートするためにこの権限を必要とします。

siteminder_home

ポリシー サーバのインストールパスを指定します。

- 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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン 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。

次の手順に従ってください:

1. コマンド ウィンドウを開き、*siteminder_home¥db* に移動します。
2. 以下のファイルのいずれかをインポートします。

- *smpolicy.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy.xml -npass
```

- *smpolicy-secure.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy-secure.xml -npass
```

```
npass
```

パスフレーズが必要ではないことを指定します。デフォルトポリシー ストア オブジェクトには暗号化されたデータが含まれていません。

両方のファイルに、デフォルトのポリシー ストア オブジェクトが含まれています。これらのオブジェクトにはデフォルトのエージェント設定オブジェクト (ACO) テンプレート内のデフォルトセキュリティ設定が含まれます。 *smpolicy-secure* ファイルはより制限の厳しいセキュリティ設定を提供します。詳細については、「[デフォルトのポリシー ストア オブジェクトの考慮事項 \(P. 104\)](#)」を参照してください。

- **Option Pack** 機能をインポートするには、以下のコマンドを実行します。

```
XPSImport ampolicy.xml -npass
```

- フェデレーション機能をインポートするには、以下のコマンドを実行します。

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

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。

注: *smpolicy.xml* をインポートすると、**SiteMinder** から別個にライセンスが付与される レガシー フェデレーション および **Web** サービスの変数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。

Advanced Authentication Server の有効化

ユーザのポリシー サーバの設定の一部として、Advanced Authentication Server を有効にします。

次の手順に従ってください:

1. ポリシー サーバ設定ウィザードを実行します。
2. ウィザードの最初の画面にあるチェックボックスをすべてオフのままにします。
3. [次へ] をクリックします。
4. Advanced Authentication Server 用のマスタ暗号化キーを作成します。

注: 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。

5. ポリシー サーバ設定ウィザードの残りの手順を完了します。

Advanced Authentication Server が有効になります。

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。

以下の点を考慮します。

- 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の手順を実行します。
- (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](#) (P. 598) します。

次の手順に従ってください:

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: 15

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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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 サーバに管理者認証情報を提供します。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認証情報を使用します。

セッション ストアとしての CA Directory

CA Directory をセッション ストアとして設定できます。

注: サポートされているバージョンの詳細については、「**12.52 SP1**
SiteMinder プラットフォーム サポート マトリックス」を参照してください。

セッション ストアを設定する方法

CA Directory をセッション ストアとして設定するには、以下の手順に従います。

1. セッション ストア スキーマ ファイルを取得します。
2. セッション ストア用の DSA を作成します。
3. セッション ストア管理ユーザおよびルート DN を追加します。
4. セッション ストア スキーマを作成します。
5. ポリシー サーバがそのセッション ストアを参照するように指定します。

セッション ストア スキーマ ファイルの取得

必要なセッション ストア スキーマ ファイルはすべてポリシー サーバとともにインストールされます。SiteMinder 管理者に連絡して、以下のファイルをリクエストします。

`netegrity.dxc`

DSA セッション ストア スキーマを作成します。スキーマにより、DSA で SiteMinder ユーザのセッション情報を格納および取得できます。

ファイルは `siteminder_home\%Trust` 内に存在します。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

セッションストア用の DSA の作成

DSA を作成して、セッションストア専用にします。専用 DSA は、セッションストアのパフォーマンスを最大化するのに役立ちます。

次の手順に従ってください:

1. CA Directory 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て、データ DSA を作成します。

```
dxnewdsa dsa_name port prefix
```

dsa_name

セッションストア DSA の名前を指定します。

port

セッションストアがリクエストをリスンする必要があるポートを指定します。

prefix

ネームスペース プレフィックスを指定します。プレフィックスを指定するために LDAP 構文を使用します。

例: セッションストア用のデータ DSA を作成します。

```
dxnewdsa smsessionstore 1234 o=forwardinc,c=us
```

注: Forward, Inc. は架空の会社名であり、厳密に説明のみを目的として使用されています。現存する会社を参照するものではありません。

セッションストア管理ユーザおよびルート DN の追加

ポリシー サーバには以下が必要です。

- DSA 内のユーザの完全な識別名 (DN) およびパスワード。ポリシーサーバではこれらの認証情報を使用して、セッションストアを管理します。
- セッション情報を書き込むことができるルート DN。

次の手順に従ってください：

1. 以下のいずれかの方法で匿名の認証を使用して、DSA にアクセスします。
 - JXplorer ツールを使用します
 - CA Directory [コマンドラインインターフェース](#)を使用します。
2. SiteMinder でセッションストアを管理するために使用できるユーザを作成します。
 - 必ず以下の OBJECT CLASS のみでユーザを作成してください。
inetOrgPerson
 - 認証情報を書き留めます。認証情報は、ポリシー サーバがそのセッションストア DSA を参照するように指定するために必要です。
3. JXplorer から切断します。
4. JXplorer を起動します。
5. DSA にアクセスできることを確認するために、作成した管理ユーザの完全な DN を使用して、DSA にログインします。
例：cn=admin,o=forwardinc,c=us
6. セッションストアのルート DN として機能する組織単位を手動で作成します。
Example: ou=sessionstore
7. JXplorer から切断します。

注：セッションストアへの不正なアクセスを防ぐために、匿名認証は無効にすることをお勧めします。

セッションストアスキーマの作成

DSA では SiteMinder ユーザのセッション情報を格納および取得するためにスキーマが必要です。

次の手順に従ってください：

1. CA Directory ホストシステムにログインします。
2. 以下のコマンドを使って、DSA を停止します。
dxserver stop DSA_Name

3. SiteMinder セッションストア スキーマ ファイル (`netegrity.dxc`) を `DXHOME¥config¥schema` に追加します。
4. `DXHOME¥config¥schema` に移動します。
5. DSA のデフォルト スキーマ ファイル (`default.dxc`) をコピーし、読み取り専用属性を削除して、その名前を変更することにより、セッションストア スキーマを作成します。

例: `default.dxc` をコピーし、コピーの名前を `smsession.dxc` に変更します。

6. 以下のようにセッションストア スキーマ ファイルを編集します。
 - a. ファイルの最後に以下の行を追加します。

```
#CA Schema
source "netegrity.dxc";
```
 - b. ファイルを保存します。
 - c. 読み取り専用属性を適用します。
7. `DXHOME¥dxserver¥config¥limits` に移動します。
8. デフォルト制限ファイル (`default.dxc`) をコピーし、読み取り専用属性を削除して、その名前を変更することにより、セッションストア制限ファイルを作成します。

例: `default.dxc` をコピーし、コピーの名前を `smsession.dxc` に変更します。

9. 以下のようにセッションストア デフォルト制限ファイルを編集します。
 - a. 以下の値に一致するように `max-local-ops` 属性を編集します。

```
set max-op-size = 1000;
```

この属性は [サイズ制限] セクションにあり、高い制限を表します。セッションストアでは、検索クエリ当たり 1,000 を超えるオブジェクトを返すことが想定されていません。
 - b. ファイルを保存します。
 - c. 読み取り専用属性を適用します。
10. `DXHOME¥config¥servers` に移動し、セッションストア初期化ファイル (`DSA_name.dxi`) を開きます。

`DSA_name`

セッションストア DSA の名前を指定します。

11. 以下のようにセッションストア初期化ファイルを編集します。

- a. スキーマ参照を **default.dxc** からセッションストアスキーマファイルへと編集します。

この参照は [スキーマ] セクションにあります。

例: **default.dxc** を **smsession.dxc** に変更します。

- b. サービス制限参照ファイルを **default.dxc** からセッションストア制限ファイルへと編集します。

この参照は [サービス制限] セクションにあります。

例: **default.dxc** を **smsession.dxc** に変更します。

- c. 以下の設定に一致するように **set-cache** インデックス属性を編集します。

```
set cache-index-all-except = smVariableValue,smsessionblob;
```

Note: 以下の属性の前に **cache index all** 属性が設定されていることを確認してください。

```
set lookup-cache = true;
```

この属性は [グリッド設定] セクションにあります。

- d. (オプション) メモリに、より多くのセッションオブジェクトを格納するために以下の属性を圧縮します。

```
smVariableValue
```

- e. (オプション) パフォーマンスを改善するためにトランザクションロギングを無効にします。

重要: トランザクションロギングを無効にした場合のデータ回復への影響を考慮してください。詳細については、**CA Directory** のドキュメントを参照してください。

12. 以下のコマンドを使って、DSA を起動します。

```
dxserver start DSA_Name
```

セッションストアスキーマが作成されます。

ポリシー サーバがセッション ストアを参照するように指定

ポリシー サーバがセッション ストア DSA を参照するように指定して、SiteMinder でセッション ストアを管理できるようにします。

次の手順に従ってください:

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 インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。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. [データベース] リストからセッション ストアを選択します。
4. [ストレージ] リストから CA Directory を選択します。
5. [セッション ストアが有効です] オプションを選択します。
6. [LDAP セッション ストア] セクションで、以下の操作を実行します。
 - a. セッション ストア DSA の IP アドレスとポートを入力します。
 - b. セッション ストア DSA の ルート DN を入力します。
例: ou=sessionstore,o=fowardinc,c=us
 - c. DSA 内の管理ユーザの完全な DN を入力します。
例: cn=admin,o=forwardinc,c=us
 - d. 管理ユーザのパスワードを入力します。
7. [LDAP 接続のテスト] をクリックして、接続を検証します。
8. [OK] をクリックします。

SiteMinder がセッション ストアを管理するように設定されます。

ポリシー ストアとしての Active Directory

Active Directory はポリシー ストアとして機能できます。1 つのディレクトリ サーバ インスタンスは以下として機能させることができます。

- ポリシー ストア
- キーストア

単一のディレクトリ サーバを使用すると管理タスクが簡略化されます。以下のセクションでは、ポリシー データと暗号化キーを格納するよう 1 つのディレクトリ サーバ インスタンスを設定する方法について説明します。実装に必要な場合は、別のキー ストアを設定できます。

注: Active Directory が SSL を使用してポリシー サーバと通信する予定である場合は、SSL クライアント証明書に **SubjectDN** の **CN** が含まれている必要があります。SSL クライアント証明書にこの情報が含まれない場合、ポリシー サーバはクラッシュします。

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。

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

ポリシー ストアとして **Active Directory** ディレクトリ サーバを設定するには、以下の手順に従います。

1. (オプション) 該当する場合、ベンダー固有のソフトウェアを使用して、LDAP ディレクトリ サーバのインスタンスを作成します。
2. (オプション) 該当する場合、ベンダー固有のソフトウェアを使用して、以下の権限を持つユーザを作成します。

- create
- read
- modify
- 削除

LDAP ツリー内のポリシー ストア ルート オブジェクトの下にこのユーザを作成します。

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。
6. ポリシー ストア データ定義をインポートします。
7. 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。
8. ポリシー サーバを再起動します。
9. 管理 UI 登録の準備をします。

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。

次の手順に従ってください:

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 インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。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. データベース リストから以下の値を選択します。

ポリシー ストア

4. ストレージ リストから以下の値を選択します。

LDAP

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
- パスワードの確認入力
- ルート 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。
7. [LDAP 接続のテスト] をクリックして、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確認します。
8. データベース リストから以下の値を選択します。

キーストア

9. ストレージ リストから以下の値を選択します。

LDAP

10. 以下のオプションを選択します。

ポリシー ストア データベースの使用

11. [OK] をクリックします。

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。

重要: Active Directory スキーマはルート ドメインによって所有されます。スキーマ変更はすべて、**SchemaAdmins** 権限を持つアカウントを使用して、スキーマ マスタを保持するルート ドメイン コントローラ上で行われる必要があります。スキーマ変更は、子ドメイン (レプリカ) からは実行できません。

次の手順に従ってください：

1. ポリシー サーバ ホスト システム上で以下のコマンドを実行します。

```
smlldapsetup ldgen -ffile_name  
file_name
```

作成する LDIF ファイルの名前を指定します。

SiteMinder スキーマと共に LDIF ファイルが作成されます。

2. 以下のコマンドを実行します。

```
smlldapsetup ldmod -ffile_name  
file_name
```

作成した LDIF の名前を指定します。

ユーティリティがポリシー ストア スキーマをインポートします。

3. `policy_server_home\%ps%\db` に移動し、以下のファイルを開きます。

ActiveDirectory.ldif

4. <RootDN> の各インスタンスを、ポリシー ストア スキーマの場所 (ポリシー ストア オブジェクトの場所ではなく) を表す DN に手動で置換します。

例：以下のルート DN がポリシー ストア オブジェクトを表す場合、

ou=policystore,dc=domain,dc=com

<RootDN> の各インスタンスを以下の DN で置き換えます。

dc=domain,dc=com

5. 以下のコマンドを実行します。

```
smldapsetup ldmod  
-fpolicy_server_home¥xps¥db¥ActiveDirectory.ldif  
  
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。

ポリシー ストア スキーマが拡張されます。ポリシー ストア スキーマを作成しました。

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次のとおりです。

siteminder

このアカウントは最大の権限を持っています。

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。

- 管理 UI に初めてアクセスする場合。
- 初めて SiteMinder ユーティリティを管理する場合。
- スーパーユーザ権限で別の管理者を作成する場合。

次の手順に従ってください:

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

siteminder_home

ポリシー サーバのインストールパスを指定します。

注: このユーティリティは、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。

2. 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、引用符でパスワードを囲みます。

注: Oracle ポリシー ストアを設定している場合、パスワードは大文字と小文字を区別します。他のすべてのポリシー ストアの場合は、パスワードの大文字と小文字を区別しません。

3. `siteminder_home¥bin` から `smreg` 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。

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 データ定義をインポートすると、ポリシー ストアで作成および格納できるオブジェクトのタイプが定義されます。

次の手順に従ってください：

1. コマンド ウィンドウを開き、`siteminder_home¥xps¥dd` 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. 以下のコマンドを実行します。

```
XPSDDInstall SmMaster.xdd
```

```
XPSDDInstall
```

必要なデータ定義をインポートします。

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 とポリシー サーバで使用するポリシー ストアが設定されます。

以下の点を考慮します。

- 必ず `siteminder_home¥bin` への書き込みアクセス権があることを確認してください。インポートユーティリティは、ポリシー ストア オブジェクトをインポートするためにこの権限を必要とします。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

- 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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン 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。

次の手順に従ってください:

1. コマンド ウィンドウを開き、*siteminder_home¥db* に移動します。
2. 以下のファイルのいずれかをインポートします。

- *smpolicy.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy.xml -npass
```

- *smpolicy-secure.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy-secure.xml -npass
```

```
npass
```

パスフレーズが必要ではないことを指定します。デフォルトポリシー ストア オブジェクトには暗号化されたデータが含まれていません。

両方のファイルに、デフォルトのポリシー ストア オブジェクトが含まれています。これらのオブジェクトにはデフォルトのエージェント設定オブジェクト (ACO) テンプレート内のデフォルトセキュリティ設定が含まれます。 *smpolicy-secure* ファイルはより制限の厳しいセキュリティ設定を提供します。詳細については、「[デフォルトのポリシー ストア オブジェクトの考慮事項 \(P. 104\)](#)」を参照してください。

- **Option Pack** 機能をインポートするには、以下のコマンドを実行します。

```
XPSImport ampolicy.xml -npass
```

- フェデレーション機能をインポートするには、以下のコマンドを実行します。

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

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。

注: *smpolicy.xml* をインポートすると、**SiteMinder** から別個にライセンスが付与される レガシー フェデレーション および **Web** サービスの変数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。

Advanced Authentication Server の有効化

ユーザのポリシー サーバの設定の一部として、Advanced Authentication Server を有効にします。

次の手順に従ってください:

1. ポリシー サーバ設定ウィザードを実行します。
2. ウィザードの最初の画面にあるチェックボックスをすべてオフのままにします。
3. [次へ] をクリックします。
4. Advanced Authentication Server 用のマスタ暗号化キーを作成します。
注: 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。
5. ポリシー サーバ設定ウィザードの残りの手順を完了します。

Advanced Authentication Server が有効になります。

ポリシー サーバの再起動

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、`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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

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。

以下の点を考慮します。

- 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の手順を実行します。
- (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](#) (P. 598) します。

次の手順に従ってください:

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： 15

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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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 サーバに管理者認証情報を提供します。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認証情報を使用します。

Active Directory ObjectCategory インデックス属性のサポート

他の LDAP 互換のディレクトリとは異なり、**Active Directory** は、デフォルトでは、ポリシー ストア オブジェクトのインデックス付けに **objectClass** 属性を使用しません。代わりに、オブジェクトには **objectCategory** 属性によってインデックスが付けられます。検索機能を強化するために、インデックスを付けることができる属性 (**Active Directory** ドキュメントを参照) として **objectClass** を設定するか、またはポリシー サーバ内の **objectCategory** サポートを有効にすることができます。

ObjectCategory 属性サポートの有効化または無効化

Windows の場合

次の手順に従ってください:

1. Windows レジストリ エディタを起動します。
2. キー
HKLM¥SOFTWARE¥Wow6432Node¥Netegrity¥SiteMinder¥CurrentVersion¥
DS¥LDAPProvider を見つけます。
 - a. サポートを有効にするには、EnableObjectCategory 値を 1 に設定します。
 - b. サポートを無効にするには、EnableObjectCategory 値を 0 に設定します。

注: デフォルト値は 0 です。

UNIX の場合

次の手順に従ってください:

1. テキスト エディタで、<sitefinder_installation>/registry にある SiteMinder sm.registry ファイルを開きます。
2. 以下のキーを見つけてください。
HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥Netegrity¥SiteMinder
¥CurrentVersion¥Ds¥LDAPProvider
 - a. サポートを有効にするには、EnableObjectCategory 値を 1 に設定します。
 - b. サポートを無効にするには、EnableObjectCategory 値を 0 に設定します。

注: デフォルト値は 0 です。

ポリシー ストアとしての Domino Directory Server

Domino Directory Server はポリシー ストアとして機能できます。1 つのディレクトリ サーバ インスタンスは以下として機能させることができます。

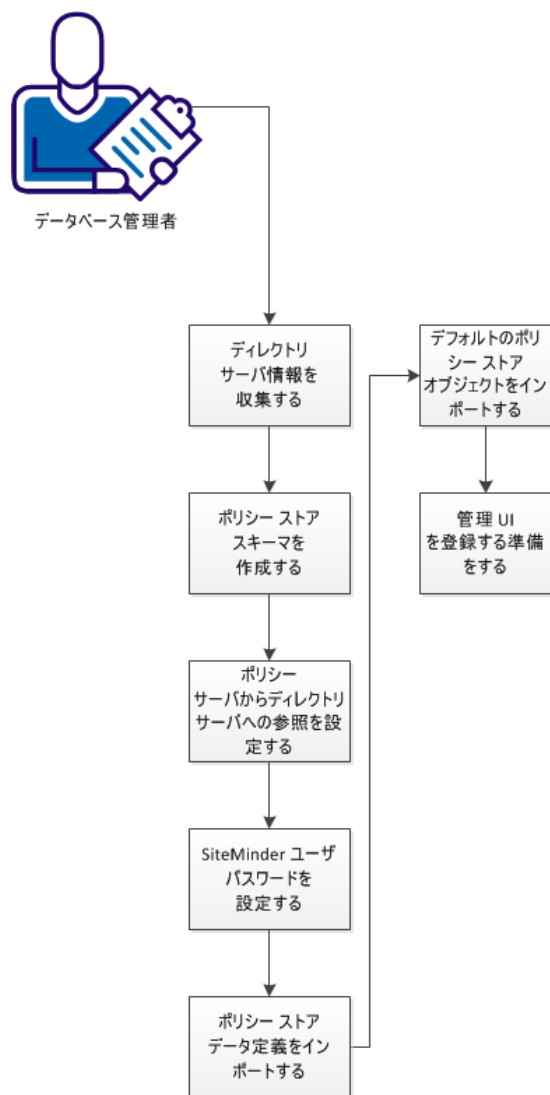
- ポリシー ストア
- キーストア

単一のディレクトリ サーバを使用すると管理タスクが簡略化されます。以下のセクションでは、ポリシー データと暗号化キーを格納するよう 1 つのディレクトリ サーバ インスタンスを設定する方法について説明します。実装に必要な場合は、別のキー ストアを設定できます。

Domino Directory Server をポリシー ストアとして設定する方法

このシナリオでは、データベース管理者が SiteMinder ポリシー ストアとして Domino ディレクトリ サーババージョン 8.5 を設定する方法について説明します。

この設定プロセスには、いくつかの別の手順が含まれます。以下の図では、ワークフローを表しています。



SiteMinder ポリシー ストア、次の手順に従ってください：として Domino ディレクトリ サーババージョン 8.5 を設定する方法

1. [ディレクトリ サーバ情報を収集します](#) (P. 126)。
2. [ポリシー ストア スキーマを作成します](#) (P. 142)。
3. [ディレクトリ サーバにポリシー サーバを示します](#) (P. 111)。
4. [SiteMinder スーパーユーザ パスワードを設定します](#) (P. 112)。
5. [ポリシー ストア データ定義をインポートします](#) (P. 115)。
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](#) (P. 115)。
7. [管理 UI 登録の準備をします](#) (P. 117)。

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。

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 スキーマの作成

Domino ディレクトリ サーバがポリシー ストアとして作動できるように、ポリシー ストア スキーマを作成します。

次の手順に従ってください：

1. ドミノ ディレクトリ サービスを停止します。
2. Domino ディレクトリ サーバに以下のファイルのバックアップ コピーを作成します。

```
domino_home\data\schema.nsf
```

3. ポリシー サーバに以下のファイルを置きます。

```
policy_server_home\db\tier2\IBM_Lotus_Domino_DirectoryServer\schema.nsf
```

4. 手順 3 のファイルを Domino ディレクトリ サーバの以下のフォルダにコピーします。

```
domino_home\data
```

5. Domino のディレクトリ サービスを開始します。
6. Domino ディレクトリ サーバで `schema.nsf` ファイルを開きます。
7. `xps` および `SiteMinder` オブジェクトと属性がすべて存在することを確認します。
8. LDAP ブラウザを使用して、Domino LDAP ディレクトリに接続します。
9. SiteMinder 用の以下のベース DN を作成します。
`Netegrity/SiteMinder/PolicySvr4`
10. Domino ディレクトリ サービスを再起動します。
11. コンソール モード内のサービスを開きます。

12. 以下のコマンドでディレクトリのインデックスを更新します。

```
load updall -r
```

13. Domino ディレクトリ サービスを再起動します。

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。

次の手順に従ってください:

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 インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。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. データベース リストから以下の値を選択します。

ポリシー ストア

4. ストレージ リストから以下の値を選択します。

LDAP

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
- パスワードの確認入力
- ルート 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。

7. [LDAP 接続のテスト] をクリックして、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確認します。

8. データベース リストから以下の値を選択します。
キーストア
9. ストレージ リストから以下の値を選択します。
LDAP
10. 以下のオプションを選択します。
ポリシー ストア データベースの使用
11. [OK] をクリックします。

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次のとおりです。

`siteminder`

このアカウントは最大の権限を持っています。

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。

- 管理 UI に初めてアクセスする場合。
- 初めて SiteMinder ユーティリティを管理する場合。
- スーパーユーザ権限で別の管理者を作成する場合。

次の手順に従ってください:

1. `smreg` ユーティリティを `siteminder_home\bin` にコピーします。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

注: このユーティリティは、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。

2. 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、引用符でパスワードを囲みます。

注: Oracle ポリシー ストアを設定している場合、パスワードは大文字と小文字を区別します。他のすべてのポリシー ストアの場合は、パスワードの大文字と小文字を区別しません。

3. `siteminder_home¥bin` から `smreg` 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。

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 データ定義をインポートすると、ポリシー ストアで作成および格納できるオブジェクトのタイプが定義されます。

次の手順に従ってください:

1. コマンド ウィンドウを開き、`siteminder_home¥xps¥dd` 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. 以下のコマンドを実行します。

```
XPSDDInstall SmMaster.xdd
```

```
XPSDDInstall
```

必要なデータ定義をインポートします。

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 とポリシー サーバで使用するポリシー ストアが設定されます。

以下の点を考慮します。

- 必ず `siteminder_home¥bin` への書き込みアクセス権があることを確認してください。インポートユーティリティは、ポリシー ストア オブジェクトをインポートするためにこの権限を必要とします。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

- 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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン 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。

次の手順に従ってください:

1. コマンド ウィンドウを開き、*siteminder_home¥db* に移動します。
2. 以下のファイルのいずれかをインポートします。

- *smpolicy.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy.xml -npass
```

- *smpolicy-secure.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy-secure.xml -npass
```

```
npass
```

パスフレーズが必要ではないことを指定します。デフォルトポリシー ストア オブジェクトには暗号化されたデータが含まれていません。

両方のファイルに、デフォルトのポリシー ストア オブジェクトが含まれています。これらのオブジェクトにはデフォルトのエージェント設定オブジェクト (ACO) テンプレート内のデフォルトセキュリティ設定が含まれます。 *smpolicy-secure* ファイルはより制限の厳しいセキュリティ設定を提供します。詳細については、「[デフォルトのポリシー ストア オブジェクトの考慮事項 \(P. 104\)](#)」を参照してください。

- **Option Pack** 機能をインポートするには、以下のコマンドを実行します。

```
XPSImport ampolicy.xml -npass
```

- フェデレーション機能をインポートするには、以下のコマンドを実行します。

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

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。

注: *smpolicy.xml* をインポートすると、**SiteMinder** から別個にライセンスが付与される レガシー フェデレーション および **Web** サービスの変数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。

Advanced Authentication Server の有効化

ユーザのポリシー サーバの設定の一部として、Advanced Authentication Server を有効にします。

次の手順に従ってください:

1. ポリシー サーバ設定ウィザードを実行します。
2. ウィザードの最初の画面にあるチェックボックスをすべてオフのままにします。
3. [次へ] をクリックします。
4. Advanced Authentication Server 用のマスタ暗号化キーを作成します。
注: 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。
5. ポリシー サーバ設定ウィザードの残りの手順を完了します。

Advanced Authentication Server が有効になります。

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。

以下の点を考慮します。

- 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の手順を実行します。
- (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](#) (P. 598) します。

次の手順に従ってください:

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: 15

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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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 サーバに管理者認証情報を提供します。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認証情報を使用します。

ポリシー ストアとしての IBM Directory Server

IBM Tivoli Directory Server はポリシー ストアとして機能できます。1 つのディレクトリ サーバインスタンスは以下として機能させることができます。

- ポリシー ストア
- キーストア

単一のディレクトリ サーバを使用すると管理タスクが簡略化されます。以下のセクションでは、ポリシー データと暗号化キーを格納するよう 1 つのディレクトリ サーバ インスタンスを設定する方法について説明します。実装に必要な場合は、別のキー ストアを設定できます。

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。

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. 必要な情報を収集したことを確認します。
2. ディレクトリ エントリとルート ノードの作成。
3. ポリシー ストアにポリシー 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。
6. ポリシー ストア データ定義をインポートします。
7. 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。
8. ポリシー サーバを再起動します。
9. 管理 UI 登録の準備をします。

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。

注: 必要に応じて、IBM Tivoli 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。

次の手順に従ってください:

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

例:

`ou=Nete`

2. ルート DN 下で以下のルート ノードを作成します。

例:

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

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。

次の手順に従ってください:

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 インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。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. データベース リストから以下の値を選択します。

ポリシー ストア

4. ストレージ リストから以下の値を選択します。

LDAP

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
- パスワードの確認入力
- ルート 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。
7. [LDAP 接続のテスト] をクリックして、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確認します。
8. データベース リストから以下の値を選択します。
キーストア
9. ストレージ リストから以下の値を選択します。
LDAP
10. 以下のオプションを選択します。
ポリシー ストア データベースの使用
11. [OK] をクリックします。

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。

次の手順に従ってください:

1. IBM ディレクトリ サーバ設定ツールを使用して、ディレクトリ サーバ
にアクセスします。
2. `policy_server_home`¥IBMDirectoryServer 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. IBM ディレクトリ サーバ構成ツールを使用して、スキーマ設定の [スキーマ ファイルの管理] セクションに `V3.siteminderrelease` スキーマ ファイルを追加します。

release

SiteMinder リリースを指定します。

4. `policy_server_home\%ps%\db` に移動します。
5. 以下のファイルを見つけます。

`IBMDirectoryServer.ldif`

6. IBM ディレクトリ サーバ構成ツールを使用して、スキーマ設定の [Manage Schema Files] セクションにファイルを追加します。
7. ディレクトリ サーバを再起動します。
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次のとおりです。

`siteminder`

このアカウントは最大の権限を持っています。

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。

- 管理 UI に初めてアクセスする場合。
- 初めて SiteMinder ユーティリティを管理する場合。
- スーパーユーザ権限で別の管理者を作成する場合。

次の手順に従ってください:

1. `smreg` ユーティリティを `siteminder_home\bin` にコピーします。

siteminder_home

ポリシー サーバのインストールパスを指定します。

注: このユーティリティは、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。

2. 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、引用符でパスワードを囲みます。

注: Oracle ポリシー ストアを設定している場合、パスワードは大文字と小文字を区別します。他のすべてのポリシー ストアの場合は、パスワードの大文字と小文字を区別しません。

3. `siteminder_home\bin` から `smreg` 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。

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 データ定義をインポートすると、ポリシー ストアで作成および格納できるオブジェクトのタイプが定義されます。

次の手順に従ってください：

1. コマンド ウィンドウを開き、`siteminder_home\bin` 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. 以下のコマンドを実行します。

```
XPSDDInstall SmMaster.xdd
```

```
XPSDDInstall
```

必要なデータ定義をインポートします。

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 とポリシー サーバで使用するポリシー ストアが設定されます。

以下の点を考慮します。

- 必ず `siteminder_home\bin` への書き込みアクセス権があることを確認してください。インポートユーティリティは、ポリシー ストア オブジェクトをインポートするためにこの権限を必要とします。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

- 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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン 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。

次の手順に従ってください:

1. コマンド ウィンドウを開き、*siteminder_home¥db* に移動します。
2. 以下のファイルのいずれかをインポートします。

- *smpolicy.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy.xml -npass
```

- *smpolicy-secure.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy-secure.xml -npass
```

```
npass
```

パスフレーズが必要ではないことを指定します。デフォルトポリシー ストア オブジェクトには暗号化されたデータが含まれていません。

両方のファイルに、デフォルトのポリシー ストア オブジェクトが含まれています。これらのオブジェクトにはデフォルトのエージェント設定オブジェクト (ACO) テンプレート内のデフォルトセキュリティ設定が含まれます。 *smpolicy-secure* ファイルはより制限の厳しいセキュリティ設定を提供します。詳細については、「[デフォルトのポリシー ストア オブジェクトの考慮事項 \(P. 104\)](#)」を参照してください。

- Option Pack 機能をインポートするには、以下のコマンドを実行します。

```
XPSImport ampolicy.xml -npass
```

- フェデレーション機能をインポートするには、以下のコマンドを実行します。

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

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。

注: *smpolicy.xml* をインポートすると、SiteMinder から別個にライセンスが付与される レガシー フェデレーション および Web サービスの変数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。

Advanced Authentication Server の有効化

ユーザのポリシー サーバの設定の一部として、Advanced Authentication Server を有効にします。

次の手順に従ってください:

1. ポリシー サーバ設定ウィザードを実行します。
2. ウィザードの最初の画面にあるチェックボックスをすべてオフのままにします。
3. [次へ] をクリックします。
4. Advanced Authentication Server 用のマスタ暗号化キーを作成します。
注: 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。
5. ポリシー サーバ設定ウィザードの残りの手順を完了します。

Advanced Authentication Server が有効になります。

ポリシー サーバの再起動

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、`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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

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。

以下の点を考慮します。

- 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の手順を実行します。
- (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](#) (P. 598) します。

次の手順に従ってください:

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： 15

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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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 サーバに管理者認証情報を提供します。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認証情報を使用します。

ポリシー ストアとしての Microsoft Active Directory LDS

Microsoft Active Directory LDS はポリシー ストアとして機能できます。1 つのディレクトリ サーバインスタンスは以下として機能させることができます。

- ポリシー ストア
- キーストア

単一のディレクトリ サーバを使用すると管理タスクが簡略化されます。以下のセクションでは、ポリシー データと暗号化キーを格納するよう 1 つのディレクトリ サーバ インスタンスを設定する方法について説明します。実装に必要な場合は、別のキー ストアを設定できます。

注: ポリシー サーバ環境設定ウィザードを使用して、このタイプの LDAP ディレクトリ サーバをポリシー ストアとして自動的に設定できます。

Active Directory LDS の前提条件

設定パーティション内の管理ユーザのみが、ポリシー ストア スキーマをインポートできます。このユーザは、ポリシー ストア パーティションを含む設定パーティションおよびすべてのアプリケーション パーティションにおける管理者権限を持っている必要があります。

次の手順に従ってください:

1. ADSI 編集コンソールを開きます。
2. 設定パーティション内の以下の場所に移動します。
`cn=directory service, cn=windows nt, cn=services, cn=configuration, cn={guid}`
3. msDS-Other-Settings 属性を検索します。
4. msDS-Other-Settings 属性に以下の新しい値を追加します。
`ADAMAllowADAMSecurityPrincipalsInConfigPartition=1`
5. 設定およびポリシー ストア アプリケーション パーティション内では、以下を実行します。
 - a. CN=Administrators, CN=Role に移動します。
 - b. CN=Administrators のプロパティを開きます。
 - c. メンバ属性を編集します。
 - d. [DN を追加する] をクリックして、設定パーティションで作成したユーザのフル DN をペーストします。
 - e. 作成したユーザのプロパティに移動し、以下のオブジェクトの値を確認します。

`msDS-UserAccountDisabled`

値は必ず `false` に設定してください。

管理ユーザには、ポリシー ストア パーティションを含む設定パーティションおよびすべてのアプリケーション パーティションにおける権限があります。

ディレクトリ サーバ情報の収集

ポリシー ストアとして **Active Directory LDS** を設定するには、特定のディレクトリ サーバ情報が必要です。ポリシー ストアを設定する前に、以下の情報を収集します。

- **ホスト情報** - ディレクトリ サーバ ホスト システムの完全修飾名または IP アドレスを決定します。
- **ポート情報** - ディレクトリ サーバが標準でないポートでリスンするかどうかを決定します。ポート情報を提供しない場合には、ポリシー ストアの設定に使用される **SiteMinder** ユーティリティが、ポート **389** (非 SSL) および **636** (SSL) をデフォルトに設定します。
- **管理者 DN** - **guid** 値を含む、ディレクトリ サーバ管理者のフル ドメイン名を決定します。
例 : CN=user1,CN=People,CN=Configuration,CN,{guid}
- **管理者パスワード** - ディレクトリ サーバ管理者用のパスワードを決定します。
- **アプリケーションパーティションのルート DN** - ポリシー ストア スキーマ データがインストールされるべきディレクトリ サーバ内の、アプリケーションパーティションのルート DN の場所を識別します。
- (オプション) **SSL クライアント証明書** - ディレクトリ 接続が SSL で行われる場合には、SSL クライアント証明書データベースを含んでいるディレクトリのパスを決定します。

ポリシー ストアを設定する方法

Active Directory LDS 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. **Active Directory LDS** 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. 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。
6. ポリシー ストア データ定義をインポートします。
7. デフォルトの **SiteMinder** オブジェクト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 登録の準備をします。

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。

注: ポリシー サーバはプロキシ オブジェクトを使用して、AD LDS ポリシー ストアにバインドできます。プロキシ オブジェクトは AD LDS 上で作成され、アカウントのセキュリティ識別子によって **Active Directory** アカウントと関連付けられます。プロキシ オブジェクトを使用して AD LDS インスタンスにバインドする詳細については、**Microsoft** のドキュメントを参照してください。プロキシ オブジェクトを使用してポリシー サーバ接続を設定し、パスワード ポリシーを使用する予定の場合は、SSL に対し AD LDS を設定します。

次の手順に従ってください:

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 インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。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. データベース リストから以下の値を選択します。

ポリシー ストア

4. ストレージ リストから以下の値を選択します。

LDAP

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

guid 値を含む、ディレクトリ サーバ管理者のフル ドメイン名を指定します。

- パスワード

- パスワードの確認入力
- ルート DN

AD LDS サーバでアプリケーション パーティションの既存のルート DN の場所を指定します。既存のルート DN の場所はポリシー ストア スキーマがインポートされる場所です。

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。

6. [\[適用\]](#) をクリックします。
7. [\[LDAP 接続のテスト\]](#) をクリックして、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確認します。
8. データベース リストから以下の値を選択します。
キーストア
9. 以下のオプションを選択します。
ポリシー ストア データベースの使用
10. [\[OK\]](#) をクリックします。

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。

次の手順に従ってください:

1. 以下のコマンドを実行します。

```
smldapsetup ldgen -ffile_name  
file_name
```

作成する LDIF ファイルの名前を指定します。

SiteMinder スキーマと共に LDIF ファイルが作成されます。

2. 以下のコマンドを実行します。

```
smldapsetup ldmod -ffile_name  
file_name
```

作成した LDIF の名前を指定します。

smldapsetup はポリシー ストア スキーマをインポートします。

3. `siteminder_home¥xps¥db` に移動し、以下のファイルを開きます。

`ADLDS.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。

4. `{guid}` の各インスタンスを、中かっこ内の実際の `guid` の値に置換し、ファイルを保存します。

例： `{CF151EA3-53A0-44A4-B4AC-DA0EBB1FF200}`

5. 以下のコマンドを実行します。

```
smldapsetup ldmod -fsiteminder_home¥xps¥db¥ADLDS.ldif
```

ポリシー ストア スキーマが拡張されます。ポリシー ストア スキーマを作成しました。

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次のとおりです。

`siteminder`

このアカウントは最大の権限を持っています。

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。

- 管理 UI に初めてアクセスする場合。
- 初めて SiteMinder ユーティリティを管理する場合。
- スーパーユーザ権限で別の管理者を作成する場合。

次の手順に従ってください:

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

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

注: このユーティリティは、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。

2. 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、引用符でパスワードを囲みます。

注: Oracle ポリシー ストアを設定している場合、パスワードは大文字と小文字を区別します。他のすべてのポリシー ストアの場合は、パスワードの大文字と小文字を区別しません。

3. `siteminder_home\bin` から `smreg` 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。

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 データ定義をインポートすると、ポリシー ストアで作成および格納できるオブジェクトのタイプが定義されます。

次の手順に従ってください：

1. コマンド ウィンドウを開き、`siteminder_home\bin` 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. 以下のコマンドを実行します。

```
XPSDDInstall SmMaster.xdd
```

```
XPSDDInstall
```

必要なデータ定義をインポートします。

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 とポリシー サーバで使用するポリシー ストアが設定されます。

以下の点を考慮します。

- 必ず *siteminder_home*¥bin への書き込みアクセス権があることを確認してください。インポートユーティリティは、ポリシー ストア オブジェクトをインポートするためにこの権限を必要とします。

siteminder_home

ポリシー サーバのインストールパスを指定します。

- 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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン 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。

次の手順に従ってください:

1. コマンド ウィンドウを開き、*siteminder_home¥db* に移動します。
2. 以下のファイルのいずれかをインポートします。

- *smpolicy.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy.xml -npass
```

- *smpolicy-secure.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy-secure.xml -npass
```

```
npass
```

パスフレーズが必要ではないことを指定します。デフォルトポリシー ストア オブジェクトには暗号化されたデータが含まれていません。

両方のファイルに、デフォルトのポリシー ストア オブジェクトが含まれています。これらのオブジェクトにはデフォルトのエージェント設定オブジェクト (ACO) テンプレート内のデフォルトセキュリティ設定が含まれます。*smpolicy-secure* ファイルはより制限の厳しいセキュリティ設定を提供します。詳細については、「[デフォルトのポリシー ストア オブジェクトの考慮事項 \(P. 104\)](#)」を参照してください。

- **Option Pack** 機能をインポートするには、以下のコマンドを実行します。

```
XPSImport ampolicy.xml -npass
```

- フェデレーション機能をインポートするには、以下のコマンドを実行します。

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

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。

注: *smpolicy.xml* をインポートすると、**SiteMinder** から別個にライセンスが付与される レガシー フェデレーション および **Web** サービスの変数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。

Advanced Authentication Server の有効化

ユーザのポリシー サーバの設定の一部として、Advanced Authentication Server を有効にします。

次の手順に従ってください:

1. ポリシー サーバ設定ウィザードを実行します。
2. ウィザードの最初の画面にあるチェックボックスをすべてオフのままにします。
3. [次へ] をクリックします。
4. Advanced Authentication Server 用のマスタ暗号化キーを作成します。
注: 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。
5. ポリシー サーバ設定ウィザードの残りの手順を完了します。

Advanced Authentication Server が有効になります。

ポリシー サーバの再起動

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、`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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

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。

以下の点を考慮します。

- 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の手順を実行します。
- (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](#) (P. 598) します。

次の手順に従ってください:

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： 15

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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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 サーバに管理者認証情報を提供します。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認証情報を使用します。

ポリシー ストアとしての Novell eDirectory

Novell eDirectory はポリシー ストアとして機能できます。1つのディレクトリ サーバ インスタンスは以下として機能させることができます。

- ポリシー ストア
- キーストア

単一のディレクトリ サーバを使用すると管理タスクが簡略化されます。以下のセクションでは、ポリシー データと暗号化キーを格納するよう1つのディレクトリ サーバ インスタンスを設定する方法について説明します。実装に必要な場合は、別のキー ストアを設定できます。

開始する前に、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 Windows Login Client
- Novell ConsoleOne for Windows、UNIX、および Netware システム

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。

- 15 文字以内のポリシー ストア ルート DN を使用してください。
Novell eDirectory DN は 256 文字を超えてはいけません。241 文字以上の SiteMinder オブジェクトもあります。ルート DN が 15 文字より長いと、オブジェクトによっては 256 バイト制限を超える場合があります。
- ポリシー ストアが Novell eDirectory にある場合、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。
eDirectory では、属性は 64 より長い値に設定できません。この制限は、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るためです。
- 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。

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。

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 ファイルを編集します。
2. ポリシー ストアにポリシー サーバを示します。
3. 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。

4. ポリシー ストア スキーマを作成します。
5. ポリシー ストア データ定義をインポートします。
6. 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. LDAP サーバをリフレッシュします。
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。

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。

次の手順に従ってください:

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 -hhost -pport -bbasedn -ssub -Dadmin_DN -wAdminPwD  
objectclass=ncpServer dn
```

-hhost

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。

-pport

LDAP ディレクトリ サーバがリスンするポートを指定します。

-bbasedn

検索のためのベース DN を指定します。

-Dadmin_dn

ディレクトリ サーバにバインドできる管理者アカウントの DN を指定します。

-wadmin_pw

管理者アカウントのパスワードを指定します。

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. *policy_server_home*¥novell に移動します。
4. Novell ポリシー ストア スキーマ ファイルを開きます。

5. 各 <ncpsrvr> 変数を、Novell サーバ DN の手順 2 で発見した値に置き換えることで、ポリシーストアスキーマ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、<ncpsrvr> の各インスタンスを「cn=servername,o=servercontainer」に置き換えます。

6. ポリシーストアスキーマファイルを保存し閉じます。
7. `policy_server_home¥xps¥db` に移動します。
8. 以下の Novell ポリシーストアスキーマファイルを開きます。

`Novell.ldif`

9. 各 <ncpsrvr> 変数を、Novell サーバ DN の手順 2 で発見した値に置き換えることで、ポリシーストアスキーマ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、<ncpsrvr> の各インスタンスを「cn=servername,o=servercontainer」に置き換えます。

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。

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。

次の手順に従ってください：

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、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。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. データベースリストから以下の値を選択します。

ポリシーストア

4. ストレージ リストから以下の値を選択します。

LDAP

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
- パスワードの確認入力
- ルート 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。
7. [LDAP 接続のテスト] をクリックして、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確認します。
8. データベース リストから以下の値を選択します。

キーストア

9. ストレージ リストから以下の値を選択します。

LDAP

10. 以下のオプションを選択します。

ポリシー ストア データベースの使用

11. [OK] をクリックします。

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。

次の手順に従ってください：

1. 以下のコマンドを実行します。

```
smldapsetup ldmod -v
-fpolicy_server_home%novell%Novell_Add_release.ldif
-fpolicy_server_home
```

ポリシー サーバのインストールパスを指定します。

-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。

release

SiteMinder リリースを指定します。

2. 以下のコマンドを実行します。

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

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次のとおりです。

siteminder

このアカウントは最大の権限を持っています。

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。

- 管理 UI に初めてアクセスする場合。
- 初めて SiteMinder ユーティリティを管理する場合。
- スーパーユーザ権限で別の管理者を作成する場合。

次の手順に従ってください:

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

siteminder_home

ポリシー サーバのインストールパスを指定します。

注: このユーティリティは、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。

2. 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、引用符でパスワードを囲みます。

注: Oracle ポリシー ストアを設定している場合、パスワードは大文字と小文字を区別します。他のすべてのポリシー ストアの場合は、パスワードの大文字と小文字を区別しません。

3. `siteminder_home¥bin` から `smreg` 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。

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 データ定義をインポートすると、ポリシー ストアで作成および格納できるオブジェクトのタイプが定義されます。

次の手順に従ってください：

1. コマンド ウィンドウを開き、`siteminder_home¥xps¥dd` 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. 以下のコマンドを実行します。

```
XPSDDInstall SmMaster.xdd
```

```
XPSDDInstall
```

必要なデータ定義をインポートします。

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 とポリシー サーバで使用するポリシー ストアが設定されます。

以下の点を考慮します。

- 必ず `siteminder_home¥bin` への書き込みアクセス権があることを確認してください。インポートユーティリティは、ポリシー ストア オブジェクトをインポートするためにこの権限を必要とします。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

- 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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン 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。

次の手順に従ってください:

1. コマンド ウィンドウを開き、*siteminder_home¥db* に移動します。
2. 以下のファイルのいずれかをインポートします。

- *smpolicy.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy.xml -npass
```

- *smpolicy-secure.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy-secure.xml -npass
```

```
npass
```

パスフレーズが必要ではないことを指定します。デフォルトポリシー ストア オブジェクトには暗号化されたデータが含まれていません。

両方のファイルに、デフォルトのポリシー ストア オブジェクトが含まれています。これらのオブジェクトにはデフォルトのエージェント設定オブジェクト (ACO) テンプレート内のデフォルトセキュリティ設定が含まれます。 *smpolicy-secure* ファイルはより制限の厳しいセキュリティ設定を提供します。詳細については、「[デフォルトのポリシー ストア オブジェクトの考慮事項 \(P. 104\)](#)」を参照してください。

- **Option Pack** 機能をインポートするには、以下のコマンドを実行します。

```
XPSImport ampolicy.xml -npass
```

- フェデレーション機能をインポートするには、以下のコマンドを実行します。

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

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。

注: *smpolicy.xml* をインポートすると、**SiteMinder** から別個にライセンスが付与される レガシー フェデレーション および **Web** サービスの変数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。

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。

次の手順に従ってください:

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。

Advanced Authentication Server の有効化

ユーザのポリシー サーバの設定の一部として、Advanced Authentication Server を有効にします。

次の手順に従ってください:

1. ポリシー サーバ設定ウィザードを実行します。
2. ウィザードの最初の画面にあるチェックボックスをすべてオフのままにします。
3. [次へ] をクリックします。
4. Advanced Authentication Server 用のマスタ暗号化キーを作成します。

注: 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。

5. ポリシー サーバ設定ウィザードの残りの手順を完了します。

Advanced Authentication Server が有効になります。

ポリシー サーバの再起動

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、`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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

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。

以下の点を考慮します。

- 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の手順を実行します。
- (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](#) (P. 598) します。

次の手順に従ってください:

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: 15

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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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 サーバに管理者認証情報を提供します。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認証情報を使用します。

ポリシー ストアとしての OpenLDAP

OpenLDAP はポリシー ストアとして機能できます。1つのディレクトリ サーバ インスタンスは以下として機能させることができます。

- ポリシー ストア
- キーストア

単一のディレクトリ サーバを使用すると管理タスクが簡略化されます。以下のセクションでは、ポリシー データと暗号化キーを格納するよう1つのディレクトリ サーバ インスタンスを設定する方法について説明します。実装に必要な場合は、別のキー ストアを設定できます。

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。

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

ポリシー ストアとして OpenLDAP ディレクトリ サーバを設定するには、以下の手順に従います。

1. `sldap` 設定ファイルを設定します。
2. データベースを作成します。
3. ディレクトリ サーバにポリシー サーバを示します。
4. SiteMinder スーパーユーザ パスワードを設定します。
5. ポリシー ストア データ定義をインポートします。
6. 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. 管理 UI 登録の準備をします。

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. ポリシー ストア インデックスを指定します。
3. 認証を有効にします。
4. データベース ディレクティブを指定します。
5. クライアントサイドの並べ替えのサポート
6. 構成ファイルをテストします。
7. OpenLDAP サーバを再起動します。

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) が設定され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。

次の手順に従ってください:

1. ポリシー サーバ ホスト システムにログインします。
2. *siteminder_home/db/tier2/OpenLDAP* に移動し、以下のファイルを 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.schema*
- *openldap_object.schema*

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. *siteminder_home/xps/db* に移動し、以下のファイルを 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*
4. slapd 構成ファイルの include セクションに、以下のエントリを入力します。

```
....
.....
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。

SiteMinder スキーマ ファイルが指定されます。

ポリシー ストア インデックスの指定

ポリシー ストアとして OpenLDAP を使用する slapd.conf ファイルでインデックスを指定します。

次の手順に従ってください:

1. slapd インスタンスを停止します。
2. slapd.conf ファイルをテキスト エディタで開きます。
3. 以下の行を確認します。

```
# Indices to maintain
index objectClass eq
```

4. ファイルに新しい行を挿入し、次に、以下の行を追加します。

```
index smAdminOID4 pres,eq
index smAuthDirOID4 pres,eq
index smAzDirOID4 pres,eq
index smcertmapOID4 pres,eq
index smIsRadius4 pres,eq
index smIsAffiliate4 pres,eq
index smParentRealmOID4 pres,eq
index smPasswordPolicyOID4 pres,eq
index smAgentGroupOID4 pres,eq
index smKeyManagementOID4 pres,eq
index smAgentOID4 pres,eq
index smAgentKeyOID4 pres,eq
index smRootConfigOID4 pres,eq
index smAGAgents4 pres,eq
index smDomainAdminOIDs4 pres,eq
index smDomainOID4 pres,eq
index smvariableoid5 pres,eq
index smNestedVariableOIDs5 pres,eq
index smvariabletypeoid5 pres,eq
index smActiveExprOID5 pres,eq
index smDomainUDs4 pres,eq
index smVariableOIDs5 pres,eq
index smusractiveexpoid5 pres,eq
index smPropertyOID5 pres,eq
index smPropertySectionOID5 pres,eq
index smPropertyCollectionOID5 pres,eq
index smFilterClass4 pres,eq
index smTaggedStringOID5 pres,eq
index smNoMatch5 pres,eq
index smTrustedHostOID5 pres,eq
index smIs4xTrustedHost5 pres,eq
index smDomainMode5 pres,eq
# index smImsEnvironmentOIDs5 pres,eq
```

```
index smSecretRolloverEnabled6 pres,eq
index smSecretGenTime6 pres,eq
index smSecretUsedTime6 pres,eq
index smSharedSecretPolicyOID6 pres,eq
index smFilterPath4 pres,eq
index smPolicyLinkOID4 pres,eq
index smIPAddress4 pres,eq
index smRealmOID4 pres,eq
index smSelfRegOID4 pres,eq
index smAzUserDirOID4 pres,eq
index smResourceType4 pres,eq
index smResponseAttrOID4 pres,eq
index smResponseGroupOID4 pres,eq
index smResponseOID4 pres,eq
index smRGResponses4 pres,eq
index smRGRules4 pres,eq
index smRuleGroupOID4 pres,eq
index smRuleOID4 pres,eq
index smSchemeOID4 pres,eq
index smisTemplate4 pres,eq
index smisUsedbyAdmin4 pres,eq
index smSchemeType4 pres,eq
index smUserDirectoryOID4 pres,eq
index smODBCQueryOID4 pres,eq
index smUserPolicyOID4 pres,eq
index smAgentTypeAttrOID4 pres,eq
index smAgentTypeOID4 pres,eq
index smAgentTypeperfcid4 pres,eq
index smAgentTypeType4 pres,eq
index smAgentCommandOID4 pres,eq
index smTimeStamp4 pres,eq
index smServerCommandOID4 pres,eq
index smAuthAzMapOID4 pres,eq
index xpsParameter pres,eq
index xpsValue pres,eq
index xpsNumber pres,eq
index xpsCategory pres,eq
index xpsGUID pres,eq
index xpsSortKey pres,eq
index xpsIndexedObject pres,eq
```

5. ファイルを保存し、テキスト エディタを閉じます。
6. 以下のコマンドを実行します。

```
slapindex -f slapd.conf
```

7. slapd インスタンスを再起動します。

OpenLDAP 用のポリシー ストア インデックスが指定されます。

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 attrs=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、サーバ側の並べ替えをサポートしていないのは OpenLDAP のみです。そこで、OpenLDAP では、すべての並べ替えをクライアント側で実行する必要があります。これを可能にするため、すべての XPS オブジェクトは、サーバ側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。

次の手順に従ってください:

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。

次の手順に従ってください：

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。

次の手順に従ってください：

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 オブジェクトを格納するためにベース ツリー構造を作成できます。

ルート DN の下に、以下のエントリを指定します。

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

ベース ツリー構造が作成されます。

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。

次の手順に従ってください:

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。

```
# CA, example.com
dn: ou=Netegrity,dc= example,dc=com
ou: CA
objectClass: organizationalUnit
objectClass: top

# SiteMinder, CA, example.com
dn: ou=SiteMinder,ou=CA,dc= example,dc=com
ou: SiteMinder
objectClass: organizationalUnit
objectClass: top

# PolicySvr4, SiteMinder, CA, example.com
dn: ou=PolicySvr4,ou=SiteMinder,ou=CA,dc= example,dc=com
ou: PolicySvr4
objectClass: organizationalUnit
objectClass: top

# XPS, policysvr4, siteminder, ca, example.com
dn: ou=XPS,ou=policysvr4,ou=siteminder,ou=ca,dc= example,dc=com
ou: XPS
objectClass: organizationalUnit
objectClass: top
```

2. 以下のコマンドを使用して、エントリを追加します。

```
ldapadd -f <file_name.ldif> -D "cn=Manager,dc=example,dc=com"
-w<password>
```

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。

次の手順に従ってください:

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、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。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. データベース リストから以下の値を選択します。

ポリシー ストア

4. ストレージ リストから以下の値を選択します。

LDAP

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
- パスワードの確認入力
- ルート 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。
7. [LDAP 接続のテスト] をクリックして、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確認します。

8. データベース リストから以下の値を選択します。

キーストア

9. ストレージ リストから以下の値を選択します。

LDAP

10. 以下のオプションを選択します。

ポリシー ストア データベースの使用

11. [OK] をクリックします。

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次のとおりです。

siteminder

このアカウントは最大の権限を持っています。

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。

- 管理 UI に初めてアクセスする場合。
- 初めて SiteMinder ユーティリティを管理する場合。
- スーパーユーザ権限で別の管理者を作成する場合。

次の手順に従ってください:

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

siteminder_home

ポリシー サーバのインストールパスを指定します。

注: このユーティリティは、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。

2. 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、引用符でパスワードを囲みます。

注: Oracle ポリシー ストアを設定している場合、パスワードは大文字と小文字を区別します。他のすべてのポリシー ストアの場合は、パスワードの大文字と小文字を区別しません。

3. `siteminder_home¥bin` から `smreg` 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。

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 データ定義をインポートすると、ポリシー ストアで作成および格納できるオブジェクトのタイプが定義されます。

次の手順に従ってください：

1. コマンド ウィンドウを開き、`siteminder_home¥xps¥dd` 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. 以下のコマンドを実行します。

```
XPSDDInstall SmMaster.xdd
```

```
XPSDDInstall
```

必要なデータ定義をインポートします。

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 とポリシー サーバで使用するポリシー ストアが設定されます。

以下の点を考慮します。

- 必ず `siteminder_home¥bin` への書き込みアクセス権があることを確認してください。インポートユーティリティは、ポリシー ストア オブジェクトをインポートするためにこの権限を必要とします。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

- 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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン 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。

次の手順に従ってください:

1. コマンド ウィンドウを開き、`siteminder_home¥db` に移動します。
2. 以下のファイルのいずれかをインポートします。

- `smpolicy.xml` をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy.xml -npass
```

- `smpolicy-secure.xml` をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy-secure.xml -npass
```

```
npass
```

パスフレーズが必要ではないことを指定します。デフォルトポリシー ストア オブジェクトには暗号化されたデータが含まれていません。

両方のファイルに、デフォルトのポリシー ストア オブジェクトが含まれています。これらのオブジェクトにはデフォルトのエージェント設定オブジェクト (ACO) テンプレート内のデフォルトセキュリティ設定が含まれます。`smpolicy-secure` ファイルはより制限の厳しいセキュリティ設定を提供します。詳細については、「[デフォルトのポリシー ストア オブジェクトの考慮事項 \(P. 104\)](#)」を参照してください。

- **Option Pack** 機能をインポートするには、以下のコマンドを実行します。

```
XPSImport ampolicy.xml -npass
```

- フェデレーション機能をインポートするには、以下のコマンドを実行します。

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

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。

注: `smpolicy.xml` をインポートすると、**SiteMinder** から別個にライセンスが付与される レガシー フェデレーション および **Web** サービスの変数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。

Advanced Authentication Server の有効化

ユーザのポリシー サーバの設定の一部として、Advanced Authentication Server を有効にします。

次の手順に従ってください:

1. ポリシー サーバ設定ウィザードを実行します。
2. ウィザードの最初の画面にあるチェックボックスをすべてオフのままにします。
3. [次へ] をクリックします。
4. Advanced Authentication Server 用のマスタ暗号化キーを作成します。

注: 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。

5. ポリシー サーバ設定ウィザードの残りの手順を完了します。

Advanced Authentication Server が有効になります。

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。

以下の点を考慮します。

- 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の手順を実行します。
- (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](#) (P. 598) します。

次の手順に従ってください:

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: 15

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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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 サーバに管理者認証情報を提供します。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認証情報を使用します。

ポリシー ストアとしての Oracle Directory Server

Oracle Directory Server（以前の Sun Java System ディレクトリ サーバ）はポリシー ストアとして機能できます。1つのディレクトリ サーバインスタンスは以下として機能させることができます。

- ポリシー ストア
- キーストア

単一のディレクトリ サーバを使用すると管理タスクが簡略化されます。以下のセクションでは、ポリシー データと暗号化キーを格納するよう1つのディレクトリ サーバ インスタンスを設定する方法について説明します。実装に必要な場合は、別のキー ストアを設定できます。

注: ポリシー サーバ環境設定ウィザードを使用して、このタイプの LDAP ディレクトリ サーバをポリシー ストアとして自動的に設定できます。

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。

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

Oracle Directory Server Enterprise Edition（以前の Sun Directory Server Enterprise Edition）をポリシー ストアとして設定するには、以下の手順を完了します。

1. （オプション）該当する場合、ベンダー固有のソフトウェアを使用して、LDAP ディレクトリ サーバのインスタンスを作成します。
2. （オプション）該当する場合、ベンダー固有のソフトウェアを使用して、以下の権限を持つ管理者を作成します。
 - create
 - read
 - modify
 - 削除

LDAP ツリー内のポリシー ストア ルート オブジェクトの下にこのユーザを作成します。

3. Oracle Directory Server の考慮事項を確認します。
4. ディレクトリ サーバにポリシー サーバを示します。
5. ポリシー ストア スキーマを作成します。
6. SiteMinder スーパーユーザ パスワードを設定します。
7. ポリシー ストア データ定義をインポートします。
8. デフォルトの SiteMinder オブジェクトをインポートします。
9. ポリシー サーバを再起動します。
10. 管理 UI 登録の準備をします。

Oracle Directory Server Enterprise Edition の考慮事項

Oracle Directory Server Enterprise Edition をポリシー ストアとして使用している場合、以下の点を考慮します。

smldapsetup および Oracle Directory Enterprise Edition

smldapsetup ユーティリティは `ou=Netegrity`、`root` サブ サフィックス、`PolicySvr4` データベースを作成します。

root

ポリシー サーバ管理コンソールの [データ] タブ上の [ルート DN] フィールドに指定したディレクトリ ルート。この変数は、既存のルート サフィックスまたはサブ サフィックスのいずれかである必要があります。

例： ルート サフィックスが `dc=netegrity,dc=com` である場合、smldapsetup を実行すると、ディレクトリ サーバに以下が生成されます。

- ルート サフィックス、`dc=netegrity,dc=com`、対応する `userRoot` データベース。
- サブ サフィックス、`ou=Netegrity,dc=netegrity,dc=com`、対応する `PolicySvr4` データベース。

例： ポリシー ストアを `ou=apps,dc=netegrity,dc=com` の下に置く場合、`ou=apps,dc=netegrity,dc=com` は、ルート サフィックス `dc=netegrity,dc=com` のルートまたはサブ サフィックスのいずれかである必要があります。

サブ サフィックスである場合、smldapsetup を実行すると以下が作成されます。

- ルート サフィックス、`dc=netegrity,dc=com`、対応する `userRoot` データベース。
- サブ サフィックス、`ou=apps,dc=netegrity,dc=com`、対応する `Apps` データベース。
- サブ サフィックス、`ou=Netegrity,ou=apps,dc=netegrity,dc=com`、対応する `PolicySvr4` データベース。

注： ルートおよびサブ サフィックスの詳細については、Oracle の [ドキュメント](#) を参照してください。

Oracle Directory Server Enterprise Edition ポリシー ストアのレプリケート

SiteMinder 12.52 SP1 では、UserRoot および PolicySvr4 データベースを作成します。PolicySvr4 データベースにはそれを指すサフィックス マッピングがあります。このポリシー ストアをレプリケートするには、PolicySvr4 データベース ディレクトリ用のレプリケーション アグリーメントをセットアップする必要があります。

注: レプリケーション アグリーメントに関する詳細については、Oracle の [ドキュメント](#) を参照してください。

レプリケーション アグリーメントを作成した後、SiteMinder インデックスをレプリケートします。

次の手順に従ってください:

1. 以下のように SiteMinder インデックスを生成します。

```
smldapsetup ldgen -x -findexes.ldif
```

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

2. レプリカ サーバ上で以下のようにインデックスをセットアップします。

```
smldapsetup ldmod -x -findexes.ldif -hhost -preplicaport  
-dAdminDN -wAdminPW
```

host

レプリカ ホストを指定します。

replicaport

レプリカ ポート番号を指定します。

AdminDN

レプリカ管理者 DN を指定します。

例: cn=directory manager

AdminPW

レプリカ管理者パスワードを指定します。

SiteMinder インデックスがレプリケートされます。

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。

次の手順に従ってください:

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、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。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. データベース リストから以下の値を選択します。

ポリシー ストア

4. ストレージ リストから以下の値を選択します。

LDAP

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
- パスワードの確認入力
- ルート 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。
7. [LDAP 接続のテスト] をクリックして、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確認します。
8. データベース リストから以下の値を選択します。

キーストア

9. ストレージ リストから以下の値を選択します。

LDAP

10. 以下のオプションを選択します。

ポリシー ストア データベースの使用

11. [OK] をクリックします。

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。以下のディレクトリ サーバ製品にはこの手順を使用します。

- Oracle 10g、11g (32 ビット)
- Sun Java System 6.1、7.0

以下の前提条件を実行します。

- LDAP インスタンスを作成します。
- SiteMinder 管理コンソールを開き、[データ] タブをクリックし、LDAP インスタンスのポリシー ストアとキー ストアに関する情報を入力します。

次の手順に従ってください：

1. ポリシー サーバ ホスト システムから以下のコマンドを実行します。

```
smldapsetup ldgen -ffile_name
```

file_name

作成する LDIF ファイルの名前を指定します。

SiteMinder スキーマと共に LDIF ファイルが作成されます。

2. 以下のコマンドを実行します。

```
smldapsetup ldmod -ffile_name
```

file_name

作成した LDIF 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 -fpolicy_server_home¥xps¥db¥OracleDirectoryServer.ldif
```

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。

4. お使いのディレクトリ サーバの管理者として以下のコマンドを実行します。

```
dsconf reindex -h localhost -p port_number -e "ou=Netegrity,root_dn"
```

5. 以下の ldif ファイルを編集します。

```
policy_server_home/xps/db/OracleDirectoryServerBrowse.ldif
```

6. 次に進む前に LDAP ディレクトリ に以下のパスが含まれていることを確認します (Root DN をお使いの PC のルート DN と置き換えます)。

```
ou=xps,ou=PolicySvr4,ou=siteminder,ou=netegrity,<Root DN>¥
```

7. ファイルに <root dn> の値がある 2 箇所に前の手順からの <root dn> 値を入力し、以下の LDIF ファイルを編集します。

8. Policy_server_home/xps/db/OracleDirectoryServerBrowser.ldifRun および次のコマンド：

```
smldapsetup ldmod -fOracleDirectoryServerBrowse.ldif -v
```

9. データベースを停止し、以下のコマンドを使用して VLV- のインデックスを再作成します。

```
dsadm stop Instance_Path
```

```
dsadm reindex -bl -t "Sort xpsSortKey" Instance_Path policysvr4
```

```
dsadm reindex -bl -t "Sort modifyTimestamp" Instance_Path policysvr4
```

```
dsadm reindex -b -t xpsNumber -t xpsValue -t xpsSortKey -t xpsCategory -t
```

```
xpsParameter -t xpsIndexedObject -t xpsTombstone instance_path policysvr4
```

10. 以下のコマンドを入力してインストールを開始します。

```
dsadm start Instance_Path
```

ポリシー ストア スキーマが拡張されます。ポリシー ストア スキーマを作成しました。

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次のとおりです。

`siteminder`

このアカウントは最大の権限を持っています。

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。

- 管理 UI に初めてアクセスする場合。
- 初めて SiteMinder ユーティリティを管理する場合。
- スーパーユーザ権限で別の管理者を作成する場合。

次の手順に従ってください:

1. `smreg` ユーティリティを `siteminder_home\bin` にコピーします。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

注: このユーティリティは、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。

2. 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、引用符でパスワードを囲みます。

注: Oracle ポリシー ストアを設定している場合、パスワードは大文字と小文字を区別します。他のすべてのポリシー ストアの場合は、パスワードの大文字と小文字を区別しません。

3. *siteminder_home*¥bin から *smreg* 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。

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 データ定義をインポートすると、ポリシー ストアで作成および格納できるオブジェクトのタイプが定義されます。

次の手順に従ってください:

1. コマンド ウィンドウを開き、*siteminder_home*¥xps¥dd 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. 以下のコマンドを実行します。

```
XPSDDInstall SmMaster.xdd
```

```
XPSDDInstall
```

必要なデータ定義をインポートします。

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 とポリシー サーバで使用するポリシー ストアが設定されます。

以下の点を考慮します。

- 必ず *siteminder_home*¥bin への書き込みアクセス権があることを確認してください。インポートユーティリティは、ポリシー ストア オブジェクトをインポートするためにこの権限を必要とします。

siteminder_home

ポリシー サーバのインストールパスを指定します。

- 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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン 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。

次の手順に従ってください:

1. コマンド ウィンドウを開き、*siteminder_home*¥db に移動します。
2. 以下のファイルのいずれかをインポートします。

- *smpolicy.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy.xml -npass
```

- *smpolicy-secure.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy-secure.xml -npass
```

```
npass
```

パスフレーズが必要ではないことを指定します。デフォルトポリシー ストア オブジェクトには暗号化されたデータが含まれていません。

両方のファイルに、デフォルトのポリシー ストア オブジェクトが含まれています。これらのオブジェクトにはデフォルトのエージェント設定オブジェクト (ACO) テンプレート内のデフォルトセキュリティ設定が含まれます。 *smpolicy-secure* ファイルはより制限の厳しいセキュリティ設定を提供します。詳細については、「[デフォルトのポリシー ストア オブジェクトの考慮事項 \(P. 104\)](#)」を参照してください。

- **Option Pack** 機能をインポートするには、以下のコマンドを実行します。

```
XPSImport ampolicy.xml -npass
```

- フェデレーション機能をインポートするには、以下のコマンドを実行します。

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

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。

注: *smpolicy.xml* をインポートすると、**SiteMinder** から別個にライセンスが付与される レガシー フェデレーション および **Web** サービスの変数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。

Advanced Authentication Server の有効化

ユーザのポリシー サーバの設定の一部として、Advanced Authentication Server を有効にします。

次の手順に従ってください:

1. ポリシー サーバ設定ウィザードを実行します。
2. ウィザードの最初の画面にあるチェックボックスをすべてオフのままにします。
3. [次へ] をクリックします。
4. Advanced Authentication Server 用のマスタ暗号化キーを作成します。
注: 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。
5. ポリシー サーバ設定ウィザードの残りの手順を完了します。

Advanced Authentication Server が有効になります。

ポリシー サーバの再起動

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、`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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

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。

以下の点を考慮します。

- 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の手順を実行します。
- (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](#) (P. 598) します。

次の手順に従ってください:

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： 15

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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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 サーバに管理者認証情報を提供します。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認証情報を使用します。

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

Oracle Internet Directory (OID) はポリシー ストアとして機能できます。1 つのディレクトリ サーバ インスタンスは以下として機能させることができます。

- ポリシー ストア
- キーストア

単一のディレクトリ サーバを使用すると管理タスクが簡略化されます。以下のセクションでは、ポリシー データと暗号化キーを格納するよう 1 つのディレクトリ サーバ インスタンスを設定する方法について説明します。実装に必要な場合は、別のキー ストアを設定できます。

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。

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

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. 必要な属性にインデックスを付けます。
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。
6. ポリシー ストア データ定義をインポートします。
7. 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。
8. ポリシー サーバを再起動します。
9. 管理 UI 登録の準備をします。

必須属性へのインデックス付け

以下の属性にインデックスをつけることで、デフォルト ポリシー ストア オブジェクトをインポートするときに発生するエラーを防ぐことができます。

`modifyTimestamp`

次の手順に従ってください:

1. Oracle Internet Directory ホスト システムにログインします。
2. Oracle カタログ コマンド ライン ツールを使用して以下のコマンドを実行します。

```
oracle_home/ldap/bin/catalog connect=conn_str add=TRUE  
attribute=modifyTimestamp
```

`oracle_home`

Oracle Internet Directory のインストール パスを指定します。

`conn_str`

ディレクトリ データベース接続文字列を指定します。

`tnsnames.ora` ファイルを設定している場合、ファイルに指定された
ネット サービス名を入力します。

属性がインデックス付けされます。

注: カタログ コマンド ライン ツールの詳細については、Oracle のドキュメントを参照してください。

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。

次の手順に従ってください:

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。
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。

次の手順に従ってください:

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 インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。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. データベース リストから以下の値を選択します。

ポリシー ストア

4. ストレージ リストから以下の値を選択します。

LDAP

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
- パスワードの確認入力
- ルート 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。

7. [LDAP 接続のテスト] をクリックして、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確認します。

8. データベース リストから以下の値を選択します。

キーストア

9. ストレージ リストから以下の値を選択します。

LDAP

10. 以下のオプションを選択します。

ポリシー ストア データベースの使用

11. [OK] をクリックします。

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。

次の手順に従ってください:

1. 以下のコマンドを実行します。

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

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  
-ffile_name
```

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 -fsiteminder_home/xps/db/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。

-hhost

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

-pport

LDAP ディレクトリ サーバのポート番号を指定します。

例 : 3500

-dAdminDN

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

-wAdminPW

-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）。

-fsiteminder_home

ポリシー サーバのインストールパスを指定します。

-Z

（任意）SSL-encrypted 接続を指定します。

-P cert

（オプション）SSL クライアント証明書データベース ファイル
(cert8.db) のパスを指定します。

例：

cert8.db が app/siteminder/ssl に存在する場合は、以下を指定します。

-Papp/siteminder/ssl

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次のとおりです。

siteminder

このアカウントは最大の権限を持っています。

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。

- 管理 UI に初めてアクセスする場合。
- 初めて SiteMinder ユーティリティを管理する場合。
- スーパーユーザ権限で別の管理者を作成する場合。

次の手順に従ってください：

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

siteminder_home

ポリシー サーバのインストールパスを指定します。

注：このユーティリティは、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。

2. 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、引用符でパスワードを囲みます。

注: Oracle ポリシー ストアを設定している場合、パスワードは大文字と小文字を区別します。他のすべてのポリシー ストアの場合は、パスワードの大文字と小文字を区別しません。

3. `siteminder_home\bin` から `smreg` 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。

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 データ定義をインポートすると、ポリシー ストアで作成および格納できるオブジェクトのタイプが定義されます。

次の手順に従ってください：

1. コマンド ウィンドウを開き、`siteminder_home\bin` 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. 以下のコマンドを実行します。

```
XPSDDInstall SmMaster.xdd
```

```
XPSDDInstall
```

必要なデータ定義をインポートします。

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 とポリシー サーバで使用するポリシー ストアが設定されます。

以下の点を考慮します。

- 必ず *siteminder_home*¥bin への書き込みアクセス権があることを確認してください。インポートユーティリティは、ポリシー ストア オブジェクトをインポートするためにこの権限を必要とします。

siteminder_home

ポリシー サーバのインストールパスを指定します。

- 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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン 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。

次の手順に従ってください:

1. コマンド ウィンドウを開き、*siteminder_home*¥db に移動します。
2. 以下のファイルのいずれかをインポートします。

- *smpolicy.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy.xml -npass
```

- *smpolicy-secure.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy-secure.xml -npass
```

```
npass
```

パスフレーズが必要ではないことを指定します。デフォルトポリシー ストア オブジェクトには暗号化されたデータが含まれていません。

両方のファイルに、デフォルトのポリシー ストア オブジェクトが含まれています。これらのオブジェクトにはデフォルトのエージェント設定オブジェクト (ACO) テンプレート内のデフォルトセキュリティ設定が含まれます。 *smpolicy-secure* ファイルはより制限の厳しいセキュリティ設定を提供します。詳細については、「[デフォルトのポリシー ストア オブジェクトの考慮事項 \(P. 104\)](#)」を参照してください。

- Option Pack 機能をインポートするには、以下のコマンドを実行します。

```
XPSImport ampolicy.xml -npass
```

- フェデレーション機能をインポートするには、以下のコマンドを実行します。

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

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。

注: *smpolicy.xml* をインポートすると、SiteMinder から別個にライセンスが付与される レガシー フェデレーション および Web サービスの変数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。

Advanced Authentication Server の有効化

ユーザのポリシー サーバの設定の一部として、Advanced Authentication Server を有効にします。

次の手順に従ってください:

1. ポリシー サーバ設定ウィザードを実行します。
2. ウィザードの最初の画面にあるチェックボックスをすべてオフのままにします。
3. [次へ] をクリックします。
4. Advanced Authentication Server 用のマスタ暗号化キーを作成します。
注: 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。
5. ポリシー サーバ設定ウィザードの残りの手順を完了します。

Advanced Authentication Server が有効になります。

ポリシー サーバの再起動

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、`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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

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。

以下の点を考慮します。

- 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の手順を実行します。
- (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](#) (P. 598) します。

次の手順に従ってください：

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： 15

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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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 サーバに管理者認証情報を提供します。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認証情報を使用します。

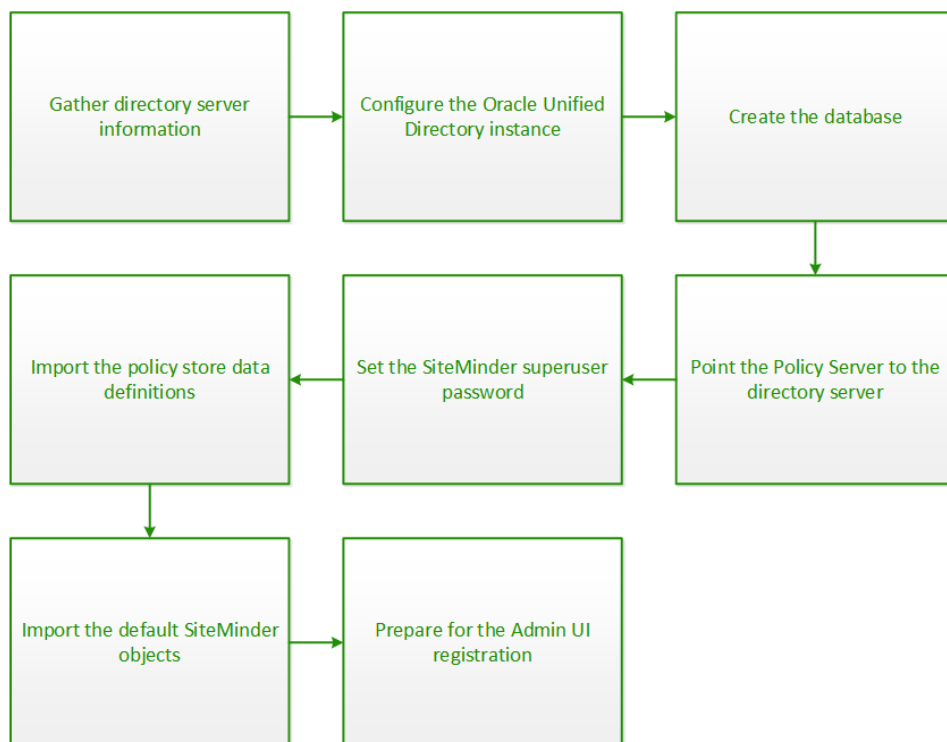
Oracle Unified Directory をポリシー ストアとして設定する方法

Oracle Unified Directory (OUD) はポリシー ストアとして機能できます。1 つのディレクトリ サーバインスタンスは以下として機能させることができます。

- ポリシー ストア
- キーストア

単一のディレクトリ サーバを使用すると管理タスクが簡略化されます。このシナリオでは、ポリシー データと暗号化キーを格納するために 1 つのディレクトリ サーバインスタンスを設定する方法について説明します。

注: 実装に必要な場合は、別のキー ストアを設定できます。



ポリシー ストアとして Oracle Unified Directory を設定するには、以下の手順を実行します。

1. [ディレクトリ サーバの情報の収集](#) (P. 126)
2. [Oracle Unified Directory インスタンスを設定します](#) (P. 235)。
3. [データベースを作成します](#) (P. 239)。

4. [ポリシー サーバがディレクトリ サーバを指すようにします](#) (P. 111)。
5. [SiteMinder スーパーユーザ パスワードを設定します](#) (P. 112)。
6. [ポリシー ストア データ定義をインポートします](#) (P. 115)。
7. [デフォルトの SiteMinder オブジェクトをインポートします](#) (P. 115)。
8. [管理 UI 登録の準備をします](#) (P. 117)。

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。

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

Oracle Unified Directory インスタンスを設定する方法

ポリシー ストアとして Oracle Unified Directory を使用できるようにするには、さらに設定が必要です。設定手順は以下のとおりです。

1. [Windows](#) (P. 235) または [UNIX](#) (P. 236) で SiteMinder スキーマ ファイルを指定します。
2. [Windows](#) (P. 236) または [UNIX](#) (P. 238) でポリシー ストア インデックスを設定します。

Windows で SiteMinder スキーマ ファイルを指定します。

SiteMinder スキーマ ファイルを指定します。

次の手順に従ってください:

1. ポリシー サーバ ホスト システムにログインします。
2. `ps_home¥db¥tier2¥OUD` に移動し、以下のファイルを Oracle Unified Directory インストール ディレクトリ内のスキーマ フォルダ (`oud_instance¥config¥schema`) にコピーします。

`oud_sm_schema.ldif`

`ps_home`

ポリシー サーバのインストールパスを指定します。

`oud_instance`

Oracle Unified Directory インスタンスの名前を指定します。

3. `ps_home¥xps¥db¥schema_extension¥db¥OUD` に移動し、以下のファイルを Oracle Unified Directory インストール ディレクトリ内のスキーマ フォルダ (`oud_instance¥config¥schema`) にコピーします。

`oud_XPS_schema.ldif`

SiteMinder スキーマ ファイルが指定されます。

UNIX で SiteMinder スキーマ ファイルを指定します。

SiteMinder スキーマ ファイルを指定します。

次の手順に従ってください:

1. ポリシー サーバ ホスト システムにログインします。
2. *ps_home/db/tier2/OUT* に移動し、以下のファイルを Oracle Unified Directory インストール ディレクトリのスキーマ フォルダ (*oud_instance¥config¥schema*) にコピーします。

oud_sm_schema.ldif

ps_home

ポリシー サーバのインストールパスを指定します。

oud_instance

Oracle Unified Directory インスタンスの名前を指定します。

3. *ps_home/xps/db/schema_extension/db/OUT* に移動し、以下のファイルを Oracle Unified Directory インストール ディレクトリ内のスキーマ フォルダ (*oud_instance¥config¥schema*) にコピーします。

oud_XPS_schema.ldif

SiteMinder スキーマ ファイルが指定されます。

Windows でのポリシー ストア インデックスの設定

ポリシー ストアとして Oracle Unified Directory を使用するには、Oracle Unified Directory インスタンス構成ファイル (*oud_instance¥config¥config.ldif*) でインデックスを指定します。

次の手順に従ってください:

1. Oracle Unified Directory インスタンスを停止します。
2. テキスト エディタで *oud_instance¥config¥config.ldif* ファイルを開きます。

oud_instance

Oracle Unified Directory インスタンスの名前を指定します。

3. 以下の行を確認します。

```
dn: cn=Index,cn=userRoot,cn=Workflow Elements,cn=config
objectClass: top
objectClass: ds-cfg-branch
cn: Index
```

4. ファイルに新しい行を挿入し、次に以下のファイルからコンテンツを追加します。

- `ps_home¥db/tier2¥OUD¥oud_sm_indexes.ldif`
- `ps_home¥xps¥db¥ schema_extension¥db¥OUD¥oud_xps_index.ldif`

5. ファイルを保存し、テキスト エディタを閉じます。

6. インデックスを再構築するには、`oud_instance¥bat` に移動し以下のコマンドを実行します。

```
rebuild-index.bat -b base_dn --rebuildAll -h hostname -p OUD_administration_port
-D "cn=Directory Manager" -j <bindpasswordfile> -X -t 0 --completionNotify
emailAddress
```

base_dn

インデックスをサポートするバック エンドのベース DN を指定します。インデックスは任意のベース DN の適用範囲内で再構築されます。

hostname

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。指定しない場合は、デフォルトで `localhost` になります。

OUD_administration_port

ディレクトリ サーバの管理ポートを指定します。指定しない場合、デフォルトの管理ポート（`44444`）が使用されます。

bindpasswordfile

ディレクトリ サーバに対して認証するときに使用するバインドパスワードが含まれるファイルを指定します。

completionNotify

タスクが完了すると通知を受ける受信者の電子メールアドレスを指定します。このオプションは、単一コマンドで 2 回以上指定できます。

7. 再構築タスクが完了した後、Oracle Unified Directory インスタンスを再起動します。

Oracle Unified Directory 用のポリシー ストア インデックスが指定されます。

UNIX でのポリシー ストア インデックスの指定

ポリシー ストアとして Oracle Unified Directory を使用するには、Oracle Unified Directory インスタンス構成ファイル (*oud_instance/config/config.ldif*) でインデックスを指定します。

次の手順に従ってください:

1. Oracle Unified Directory インスタンスを停止します。
2. テキスト エディタで *oud_instance/config/config.ldif* ファイルを開きます。

oud_instance

Oracle Unified Directory インスタンスの名前を指定します。

3. 以下の行を確認します。

```
dn: cn=Index,cn=userRoot,cn=Workflow Elements,cn=config
objectClass: top
objectClass: ds-cfg-branch
cn: Index
```

4. ファイルに新しい行を挿入し、次に以下のファイルからコンテンツを追加します。

- *ps_home/db/tier2/OUd/oud_sm_indexes.ldif*
- *ps_home/xps/db/schema_extension/db/OUd/oud_xps_index.ldif*

ps_home

ポリシー サーバのインストールパスを指定します。

5. ファイルを保存し、テキスト エディタを閉じます。

6. *oud_instance/bin* に移動し、インデックスを再構築するために以下のコマンドを実行します。

```
rebuild-index -b base_dn --rebuildAll -h hostname -p OUD_administration_port -D  
"cn=Directory Manager" -j bindpasswordfile -X -t 0 --completionNotify  
emailAddress
```

base_dn

インデックスをサポートするバック エンドのベース DN を指定します。インデックスは任意のベース DN の適用範囲内で再構築されます。

hostname

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。指定しない場合は、デフォルトで **localhost** になります。

OUD_administration_port

ディレクトリ サーバの管理ポートを指定します。指定しない場合、デフォルトの管理ポート (**44444**) が使用されます。

bindpasswordfile

ディレクトリ サーバに対して認証するときに使用するバインドパスワードが含まれるファイルを指定します。

completionNotify

タスクが完了すると通知を受ける受信者の電子メールアドレスを指定します。このオプションは、単一コマンドで 2 回以上指定できます。

7. 再構築タスクが完了した後、Oracle Unified Directory インスタンスを再起動します。

Oracle Unified Directory 用のポリシー ストア インデックスが指定されます。

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 オブジェクトを格納するためにベース ツリー構造を作成するには、ルート DN の下に以下のエントリを指定します。

```
ou=Netegrity, ou=SiteMinder, ou=PolicySvr4
```

データベースへのエントリの追加

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。

次の手順に従ってください:

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。

```
# CA, example.com
dn: ou=Netegrity,dc= example,dc=com
ou: CA
objectClass: organizationalUnit
objectClass: top

# SiteMinder, CA, example.com
dn: ou=SiteMinder,ou=CA,dc= example,dc=com
ou: SiteMinder
objectClass: organizationalUnit
objectClass: top
```



```
# PolicySvr4, SiteMinder, CA, example.com
dn: ou=PolicySvr4,ou=SiteMinder,ou=CA,dc= example,dc=com
ou: PolicySvr4
objectClass: organizationalUnit
objectClass: top
```

2. 以下のコマンドを実行して、エントリを追加します。

```
ldapmodify -h hostname -p port -D bindDN -j pwd_file -a -f LDIF_file_name
```

hostname

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。

デフォルト : localhost

port

ディレクトリ サーバにアクセスするポートを指定します。

デフォルト : 389

BindDN

ディレクトリ サーバを認証するバインド DN を指定します。

デフォルト : cn=Directory Manager

pwd_file

ディレクトリ サーバの認証に使用するバインドパスワードが含まれるファイルを指定します。

LDIF_file_name

手順 1 で作成した LDIF ファイルを指定します。

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。

次の手順に従ってください:

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、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。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. データベース リストから以下の値を選択します。

ポリシー ストア

4. ストレージ リストから以下の値を選択します。

LDAP

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
- パスワードの確認入力
- ルート 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。
7. [LDAP 接続のテスト] をクリックして、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確認します。
8. データベース リストから以下の値を選択します。

キーストア

9. ストレージ リストから以下の値を選択します。

LDAP

10. 以下のオプションを選択します。

ポリシー ストア データベースの使用

11. [OK] をクリックします。

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次のとおりです。

siteminder

このアカウントは最大の権限を持っています。

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。

- 管理 UI に初めてアクセスする場合。
- 初めて SiteMinder ユーティリティを管理する場合。
- スーパーユーザ権限で別の管理者を作成する場合。

次の手順に従ってください:

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

siteminder_home

ポリシー サーバのインストールパスを指定します。

注: このユーティリティは、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。

2. 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、引用符でパスワードを囲みます。

注: Oracle ポリシー ストアを設定している場合、パスワードは大文字と小文字を区別します。他のすべてのポリシー ストアの場合は、パスワードの大文字と小文字を区別しません。

3. `siteminder_home\bin` から `smreg` 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。

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 データ定義をインポートすると、ポリシー ストアで作成および格納できるオブジェクトのタイプが定義されます。

次の手順に従ってください：

1. コマンド ウィンドウを開き、`siteminder_home\bin` 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. 以下のコマンドを実行します。

```
XPSDDInstall SmMaster.xdd
```

```
XPSDDInstall
```

必要なデータ定義をインポートします。

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 とポリシー サーバで使用するポリシー ストアが設定されます。

以下の点を考慮します。

- 必ず *siteminder_home*¥bin への書き込みアクセス権があることを確認してください。インポートユーティリティは、ポリシー ストア オブジェクトをインポートするためにこの権限を必要とします。

siteminder_home

ポリシー サーバのインストールパスを指定します。

- 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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン 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。

次の手順に従ってください:

1. コマンド ウィンドウを開き、`siteminder_home¥db` に移動します。
2. 以下のファイルのいずれかをインポートします。

- `smpolicy.xml` をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy.xml -npass
```

- `smpolicy-secure.xml` をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy-secure.xml -npass
```

```
npass
```

パスフレーズが必要ではないことを指定します。デフォルトポリシー ストア オブジェクトには暗号化されたデータが含まれていません。

両方のファイルに、デフォルトのポリシー ストア オブジェクトが含まれています。これらのオブジェクトにはデフォルトのエージェント設定オブジェクト (ACO) テンプレート内のデフォルトセキュリティ設定が含まれます。`smpolicy-secure` ファイルはより制限の厳しいセキュリティ設定を提供します。詳細については、「[デフォルトのポリシー ストア オブジェクトの考慮事項 \(P. 104\)](#)」を参照してください。

- **Option Pack** 機能をインポートするには、以下のコマンドを実行します。

```
XPSImport ampolicy.xml -npass
```

- フェデレーション機能をインポートするには、以下のコマンドを実行します。

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

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。

注: `smpolicy.xml` をインポートすると、**SiteMinder** から別個にライセンスが付与される レガシー フェデレーション および **Web** サービスの変数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。

Advanced Authentication Server の有効化

ユーザのポリシー サーバの設定の一部として、Advanced Authentication Server を有効にします。

次の手順に従ってください:

1. ポリシー サーバ設定ウィザードを実行します。
2. ウィザードの最初の画面にあるチェックボックスをすべてオフのままにします。
3. [次へ] をクリックします。
4. Advanced Authentication Server 用のマスタ暗号化キーを作成します。
注: 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。
5. ポリシー サーバ設定ウィザードの残りの手順を完了します。

Advanced Authentication Server が有効になります。

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。

以下の点を考慮します。

- 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の手順を実行します。
- (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](#) (P. 598) します。

次の手順に従ってください:

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: 15

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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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 サーバに管理者認証情報を提供します。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認証情報を使用します。

Oracle Virtual Directory をポリシー ストアとして設定する方法

Oracle Virtual Directory (OVD) はポリシー ストアとして機能できます。1 つのディレクトリ サーバインスタンスは以下として機能させることができます。

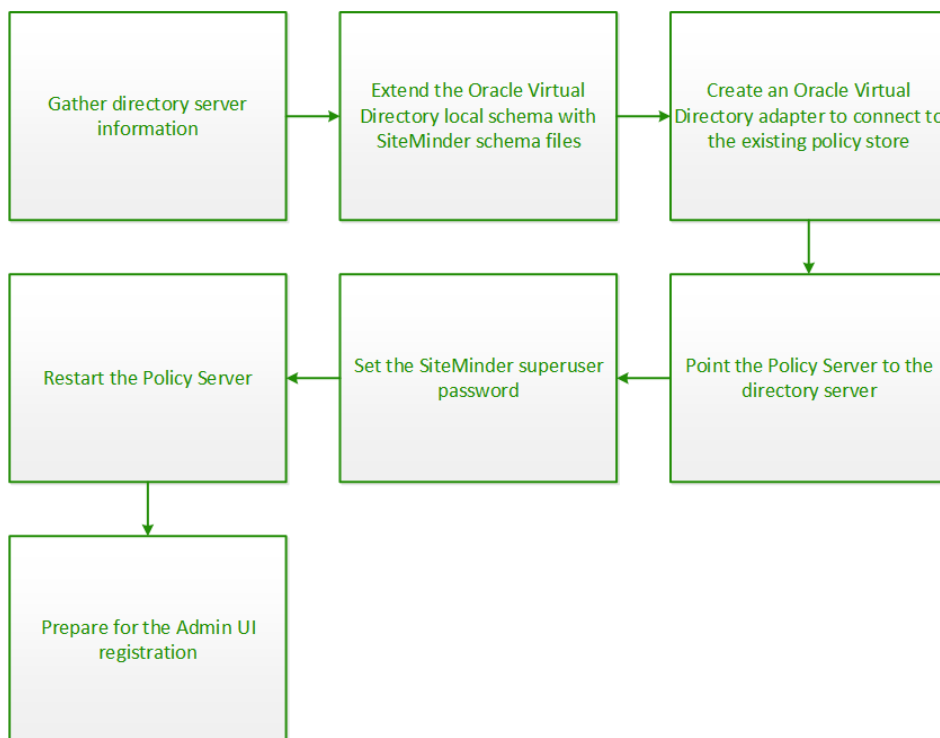
- ポリシー ストア
- キーストア

単一のディレクトリ サーバを使用すると管理タスクが簡略化されます。このシナリオでは、ポリシー データと暗号化キーを格納するために 1 つのディレクトリ サーバインスタンスを設定する方法について説明します。

注: 実装に必要な場合は、別のキー ストアを設定できます。



Database Administrator



ポリシー ストアとして Oracle Virtual Directory を設定するには、以下の手順を実行します。

1. [ディレクトリ サーバの情報の収集](#) (P. 126)
2. [SiteMinder スキーマ ファイルで Oracle Virtual Directory ローカル スキーマを拡張します](#) (P. 253)。
3. [既存のポリシー ストアに接続するための Oracle Virtual Directory アダプタを作成します](#) (P. 254)。
4. [ポリシー サーバがディレクトリ サーバを指すようにします](#) (P. 111)。
5. [SiteMinder スーパーユーザ パスワードを設定します](#) (P. 112)。
6. [ポリシー サーバを再起動します](#) (P. 134)。
7. [管理 UI 登録の準備をします](#) (P. 117)。

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。

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

SiteMinder スキーマ ファイルで OVD ローカル スキーマを拡張する

以下の SiteMinder スキーマ ファイルで Oracle Virtual Directory を拡張します。

- `ovd_sm_schema.ldif`
- `ovd_xps_schema.ldif`

次の手順に従ってください:

1. ポリシー サーバ ホスト システムにログインします。
2. `siteminder_home/db/tier2/Oracle Virtual Directory` に移動し、OVD ホスト システムに以下のファイルをコピーします。

```
ovd_sm_schema.ldif
```

3. `siteminder_home/xps/db/schema_extension/db/Oracle Virtual Directory` に移動し、OVD ホスト システムに以下のファイルをコピーします。

```
ovd_xps_schema.ldif
```

4. Oracle Virtual Directory システムにログインします。
5. お使いのディレクトリ サーバの管理者として以下のコマンドを実行し、SiteMinder スキーマ ファイルでローカル スキーマを拡張します。

```
ldapmodify -h OVD_Host -p OVD_Port -D cn=Admin -w Admin_Password -v -a -f  
ovd_sm_schema.ldif
```

```
ldapmodify -h OVD_Host -p OVD_Port -D cn=Admin -w Admin_Password -v -a -f  
ovd_xps_schema.ldif
```

```
dsconf reindex -h localhost -p OVD_Port -e "ou=Netegrity,root_database"
```

OVD_Host

OVD システム IP アドレスまたは完全修飾ドメイン名を指定します。

OVD_Port

OVD インスタンスが実行されているポートを指定します。

cn=Admin

スキーマを変更する権限を持つ OVD サーバの管理者を指定します。

Admin_Password

サーバの管理者のパスワードを指定します。

既存のポリシー ストアに接続するための Oracle Virtual Directory アダプタを作成する

既存のポリシー ストアに接続するための Oracle Virtual Directory LDAP アダプタを作成するには、Oracle Directory Services Manager を使用します。

次の手順に従ってください:

1. Oracle Directory Services Manager にログインします。
2. タスク選択バーから [Adapter] を選択します。 [Adapter] ナビゲーション ツリーが表示されます。
3. [Create Adapter] ボタンをクリックします。新規アダプタ ウィザードが表示されます。
4. [Type] 画面で以下の値を指定します。

アダプタタイプ

[LDAP] を選択します。

アダプタ名

LDAP アダプタの一意の名前を入力します。

アダプタ テンプレート

既存のポリシー ストアのディレクトリ タイプに対応するアダプタ テンプレートを選択します。

5. [Next] をクリックします。

6. [Connection] 画面で以下の値を入力します（他のすべての設定はデフォルトにします）。

Use DNS for Auto Discovery

[No] を選択します。

Host

リモート ホストのホスト名または IP アドレスを入力します。

Port

リモート ホスト インスタンスが実行されているポートを入力します。

Server proxy Bind DN

ディレクトリ コンテンツを変更する権限があるディレクトリ ユーザの認証情報を入力します。

Proxy Password

[Secure proxy Bind DN] フィールドで指定したユーザのパスワード。

7. [Next] をクリックします。
8. [Connection Test] 画面の接続ステータスが OK の場合、[Next] をクリックします。それ以外の場合は、[Back] をクリックして接続設定のトラブルシューティングを行います。
9. [Namespace] 画面で以下の値を入力します（他のすべての設定はデフォルトにします）。

Remote Base

[Browse] をクリックし、ポリシー データが保存される DN を選択します。

Mapped Namespace

ポリシー データをマップするローカル DN を入力します。

10. [Summary] ページを確認して [Finish] をクリックします。

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。

次の手順に従ってください:

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、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。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. データベース リストから以下の値を選択します。

ポリシー ストア

4. ストレージ リストから以下の値を選択します。

LDAP

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
- パスワードの確認入力
- 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。
7. [LDAP 接続のテスト] をクリックして、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確認します。
8. [OK] をクリックします。

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次のとおりです。

`siteminder`

このアカウントは最大の権限を持っています。

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。

- 管理 UI に初めてアクセスする場合。
- 初めて SiteMinder ユーティリティを管理する場合。
- スーパーユーザ権限で別の管理者を作成する場合。

次の手順に従ってください：

1. `smreg` ユーティリティを `siteminder_home\bin` にコピーします。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

注： このユーティリティは、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。

2. 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、引用符でパスワードを囲みます。

注： Oracle ポリシー ストアを設定している場合、パスワードは大文字と小文字を区別します。他のすべてのポリシー ストアの場合は、パスワードの大文字と小文字を区別しません。

3. `siteminder_home\bin` から `smreg` 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。

Advanced Authentication Server の有効化

ユーザのポリシー サーバの設定の一部として、Advanced Authentication Server を有効にします。

次の手順に従ってください:

1. ポリシー サーバ設定ウィザードを実行します。
2. ウィザードの最初の画面にあるチェックボックスをすべてオフのままにします。
3. [次へ] をクリックします。
4. Advanced Authentication Server 用のマスタ暗号化キーを作成します。

注: 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。

5. ポリシー サーバ設定ウィザードの残りの手順を完了します。

Advanced Authentication Server が有効になります。

ポリシー サーバの再起動

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、`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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

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。

以下の点を考慮します。

- 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の手順を実行します。
- (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](#) (P. 598) します。

次の手順に従ってください:

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: 15

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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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 サーバに管理者認証情報を提供します。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認証情報を使用します。

ポリシー ストアとしての Red Hat Directory Server

Red Hat Directory Server はポリシー ストアとして機能できます。1 つのディレクトリ サーバ インスタンスは以下として機能させることができます。

- ポリシー ストア
- キーストア

単一のディレクトリ サーバを使用すると管理タスクが簡略化されます。以下のセクションでは、ポリシー データと暗号化キーを格納するよう 1 つのディレクトリ サーバ インスタンスを設定する方法について説明します。実装に必要な場合は、別のキー ストアを設定できます。

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。

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

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

1. ポリシー ストアにポリシー サーバを示します。
2. 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. ポリシー ストア データ定義をインポートします。
5. 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。
6. ポリシー サーバを再起動します。
7. 管理 UI 登録の準備をします。

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。

次の手順に従ってください：

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 インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。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. データベース リストから以下の値を選択します。

ポリシー ストア

4. ストレージ リストから以下の値を選択します。

LDAP

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
- パスワードの確認入力
- ルート 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。

7. [LDAP 接続のテスト] をクリックして、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確認します。

8. データベース リストから以下の値を選択します。

キーストア

9. ストレージ リストから以下の値を選択します。

LDAP

10. 以下のオプションを選択します。

ポリシー ストア データベースの使用

11. [OK] をクリックします。

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。

次の手順に従ってください:

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。

```
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 スキーマがインポートされます。

4. 以下の手順を実行します。

- a. ディレクトリ サーバを再起動します。ポリシー ストア スキーマを正しく保存するにはディレクトリ サーバの再起動が必要です。
- b. 手順 3 を繰り返します。ディレクトリ サーバを再起動するとポリシー ストア ルートが削除されます。ポリシー ストア ルートを作成するには、ポリシー ストア スキーマを再度インポートする必要があります。

5. 以下のコマンドを実行します。

```
smldapsetup ldmod  
-fsiteminder_home/xps/db/RedHat_7_1.ldif  
-fsiteminder_home
```

ポリシー サーバのインストールパスを指定します。

XPS に対するポリシー ストア スキーマが拡張されます。

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次のとおりです。

`siteminder`

このアカウントは最大の権限を持っています。

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。

- 管理 UI に初めてアクセスする場合。
- 初めて SiteMinder ユーティリティを管理する場合。
- スーパーユーザ権限で別の管理者を作成する場合。

次の手順に従ってください:

1. `smreg` ユーティリティを `siteminder_home/bin` にコピーします。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

注: このユーティリティは、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。

2. 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、引用符でパスワードを囲みます。

注: Oracle ポリシー ストアを設定している場合、パスワードは大文字と小文字を区別します。他のすべてのポリシー ストアの場合は、パスワードの大文字と小文字を区別しません。

3. `siteminder_home¥bin` から `smreg` 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。

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 データ定義をインポートすると、ポリシー ストアで作成および格納できるオブジェクトのタイプが定義されます。

次の手順に従ってください:

1. コマンド ウィンドウを開き、`siteminder_home¥xps¥dd` 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. 以下のコマンドを実行します。

```
XPSDDInstall SmMaster.xdd
```

```
XPSDDInstall
```

必要なデータ定義をインポートします。

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 とポリシー サーバで使用するポリシー ストアが設定されます。

以下の点を考慮します。

- 必ず `siteminder_home¥bin` への書き込みアクセス権があることを確認してください。インポートユーティリティは、ポリシー ストア オブジェクトをインポートするためにこの権限を必要とします。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

- 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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン 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。

次の手順に従ってください:

1. コマンド ウィンドウを開き、`siteminder_home¥db` に移動します。
2. 以下のファイルのいずれかをインポートします。

- `smpolicy.xml` をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy.xml -npass
```

- `smpolicy-secure.xml` をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy-secure.xml -npass
```

```
npass
```

パスフレーズが必要ではないことを指定します。デフォルトポリシー ストア オブジェクトには暗号化されたデータが含まれていません。

両方のファイルに、デフォルトのポリシー ストア オブジェクトが含まれています。これらのオブジェクトにはデフォルトのエージェント設定オブジェクト (ACO) テンプレート内のデフォルトセキュリティ設定が含まれます。`smpolicy-secure` ファイルはより制限の厳しいセキュリティ設定を提供します。詳細については、「[デフォルトのポリシー ストア オブジェクトの考慮事項 \(P. 104\)](#)」を参照してください。

- **Option Pack** 機能をインポートするには、以下のコマンドを実行します。

```
XPSImport ampolicy.xml -npass
```

- フェデレーション機能をインポートするには、以下のコマンドを実行します。

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

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。

注: `smpolicy.xml` をインポートすると、**SiteMinder** から別個にライセンスが付与される レガシー フェデレーション および **Web** サービスの変数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。

Advanced Authentication Server の有効化

ユーザのポリシー サーバの設定の一部として、Advanced Authentication Server を有効にします。

次の手順に従ってください:

1. ポリシー サーバ設定ウィザードを実行します。
2. ウィザードの最初の画面にあるチェックボックスをすべてオフのままにします。
3. [次へ] をクリックします。
4. Advanced Authentication Server 用のマスタ暗号化キーを作成します。
注: 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。
5. ポリシー サーバ設定ウィザードの残りの手順を完了します。

Advanced Authentication Server が有効になります。

ポリシー サーバの再起動

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、`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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

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。

以下の点を考慮します。

- 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の手順を実行します。
- (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](#) (P. 598) します。

次の手順に従ってください:

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： 15

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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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 サーバに管理者認証情報を提供します。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認証情報を使用します。

ポリシー ストアとしての Siemens DirX

Siemens DirX はポリシー ストアとして機能できます。1 つのディレクトリ サーバ インスタンスは以下として機能させることができます。

- ポリシー ストア
- キーストア

単一のディレクトリ サーバを使用すると管理タスクが簡略化されます。以下のセクションでは、ポリシー データと暗号化キーを格納するよう 1 つのディレクトリ サーバ インスタンスを設定する方法について説明します。実装に必要な場合は、別のキー ストアを設定できます。

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。

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

Siemens DirX 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 スキーマを作成します。
2. ポリシー ストアにポリシー サーバを示します。

3. SiteMinder スーパーユーザ パスワードを設定します。
4. ポリシー ストア データ定義をインポートします。
5. 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。
6. 管理 UI 登録の準備をします。

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。

前提条件

特定のポリシー ストア操作では、**SiteMinder** 属性での検索が必要です。**DirX** ディレクトリは、検索処理を実行するために属性にインデックスを付ける必要があります。

デフォルトでは、**DirX** ディレクトリは **20** の属性にインデックスを付けます。**SiteMinder** には、このデフォルト制限より多くの属性が含まれます。ディレクトリが最大限インデックスを付けることができる属性の数を増やします。値は **800** にすることを推奨します。

属性インデックス制限を増加させるには、データベース プロファイルを初期化すると同時に以下のコマンドを使用します。

```
dbamboot -Pdatabase_profile_name -aindexing_value
```

例 :

```
dbamboot -Pprofile1 -a800
```

スキーマの作成

次の手順に従ってください:

1. ディレクトリ サーバ ホスト システム上で以下のディレクトリ構造を作成します。

```
DirX_installation¥scripts¥security¥CA¥SiteMinder
```

```
DirX_installation
```

DirX のインストールパスを指定します。

2. ポリシー サーバ ホスト システムにログインします。

3. *siteminder_home¥db¥tier2¥SiemensDirx* に移動し、以下のファイルを *DirX_installation¥scripts¥security¥CA¥SiteMinder* にコピーします。

- *dirxabbr-ext.SiteMinderrelease*
- *schema_ext_for_SiteMinderrelease.adm*
- *bind.tcl*
- *l-bind.cp*
- *GlobalVar.tcl*

siteminder_home

ポリシー サーバのインストールパスを指定します。

release

SiteMinder リリースを指定します。

4. *siteminder_home¥xps¥db¥Siemens_DirX* に移動し、以下のファイルを *DirX_installation¥scripts¥security¥CA¥SiteMinder* にコピーします。

- *dirxabbr-ext.XPS*
- *schema_ext_for_XPS.adm*

5. 以下のファイルの名前を変更します。

- *schema_ext_for_SiteMinderrelease.adm* から *schema_ext_for_SiteMinder.adm* に変更します。
- *dirxabbr-ext.SiteMinderrelease* から *dirxabbr-ext.SiteMinder* に変更します。

siteminder_home

ポリシー サーバのインストールパスを指定します。

release

SiteMinder リリースを指定します。

6. 以下のファイルを、*DirX_installation¥client¥conf* にコピーします。

- *dirxabbr-ext.SiteMinder*
- *dirxabbr-ext.XPS*

7. DirX サービスを再起動します。

8. *DirX_installation¥scripts¥security¥CA¥SiteMinder* に移動して、*GlobalVar.tcl* ファイルを編集し、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=My-Company
- 管理者ユーザ名：cn=admin、o=My-Company
- 管理者パスワード：dirx

9. コマンドプロンプトから、*DirX_installation¥scripts¥security¥CA¥SiteMinder* に移動し、以下のコマンドを実行します。

- *dirxadm schema_ext_for_siteminder.adm*
- *dirxadm schema_ext_for_XPS.adm*

10. DirX サービスを再起動します。

11. DirX がインストールされているシステムで、属性 *modifyTimestamp* にインデックスを付けます。このタスクは手動でまたは *DirX Manager* によって実行します。

DirX Manager を使用した手順を以下に示します。

- a. DSA に再度バインドします。
- b. 左側パネルの [スキーマ] をクリックします。
- c. [データベース] をクリックします。
- d. 「インデックスが割り当てられていない属性を非表示にする」 (Hide attributes with no index assigned) をオフにします。
- e. [編集] をクリックします。
- f. [インデックス] 行で、属性 *modifyTimestamp* を選択します。
- g. 変更を保存します。
- h. [データベース] を右クリックし、属性インデックスの一貫性を確認します。

12. DirX 管理ツールを使用して、以下の項目を完了します。

- a. DSA に再度バインドします。
- b. 以下のベース ツリー構造の作成
 - o=My-Company の下に、ou=Netegrity を作成します。
 - ou=Netegrity の下に、ou=SiteMinder を作成します。
 - ou=SiteMinder の下に ou=PolicySvr4 を作成します。
 - ou=PolicySvr4 の下に ou=XPS を作成します。

ポリシー ストア スキーマが作成されます。

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。

次の手順に従ってください:

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 インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。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. データベース リストから以下の値を選択します。

ポリシー ストア

4. ストレージ リストから以下の値を選択します。

LDAP

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

- パスワードの確認入力
- ルート 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。
7. [LDAP 接続のテスト] をクリックして、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確認します。
8. データベース リストから以下の値を選択します。
キーストア
9. ストレージ リストから以下の値を選択します。
LDAP
10. 以下のオプションを選択します。
ポリシー ストア データベースの使用
11. [OK] をクリックします。

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次のとおりです。

siteminder

このアカウントは最大の権限を持っています。

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。

- 管理 UI に初めてアクセスする場合。
- 初めて SiteMinder ユーティリティを管理する場合。
- スーパーユーザ権限で別の管理者を作成する場合。

次の手順に従ってください:

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

siteminder_home

ポリシー サーバのインストール パスを指定します。

注: このユーティリティは、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。

2. 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、引用符でパスワードを囲みます。

注: Oracle ポリシー ストアを設定している場合、パスワードは大文字と小文字を区別します。他のすべてのポリシー ストアの場合は、パスワードの大文字と小文字を区別しません。

3. *siteminder_home*¥bin から smreg 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。

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 データ定義をインポートすると、ポリシー ストアで作成および格納できるオブジェクトのタイプが定義されます。

次の手順に従ってください:

1. コマンド ウィンドウを開き、*siteminder_home*¥xps¥dd 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. 以下のコマンドを実行します。

```
XPSDDInstall SmMaster.xdd
```

```
XPSDDInstall
```

必要なデータ定義をインポートします。

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 とポリシー サーバで使用するポリシー ストアが設定されます。

以下の点を考慮します。

- 必ず *siteminder_home*¥bin への書き込みアクセス権があることを確認してください。インポートユーティリティは、ポリシー ストア オブジェクトをインポートするためにこの権限を必要とします。

siteminder_home

ポリシー サーバのインストールパスを指定します。

- 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する前に、管理者権限でコマンドラインウィンドウを開きます。アカウントに管理者権限がある場合でも、このように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。

次の手順に従ってください:

1. コマンド ウィンドウを開き、`siteminder_home¥db` に移動します。
2. 以下のファイルのいずれかをインポートします。

- `smpolicy.xml` をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy.xml -npass
```

- `smpolicy-secure.xml` をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy-secure.xml -npass
```

```
npass
```

パスフレーズが必要ではないことを指定します。デフォルトポリシー ストア オブジェクトには暗号化されたデータが含まれていません。

両方のファイルに、デフォルトのポリシー ストア オブジェクトが含まれています。これらのオブジェクトにはデフォルトのエージェント設定オブジェクト (ACO) テンプレート内のデフォルトセキュリティ設定が含まれます。`smpolicy-secure` ファイルはより制限の厳しいセキュリティ設定を提供します。詳細については、「[デフォルトのポリシー ストア オブジェクトの考慮事項 \(P. 104\)](#)」を参照してください。

- **Option Pack** 機能をインポートするには、以下のコマンドを実行します。

```
XPSImport ampolicy.xml -npass
```

- フェデレーション機能をインポートするには、以下のコマンドを実行します。

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

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。

注: `smpolicy.xml` をインポートすると、**SiteMinder** から別個にライセンスが付与される レガシー フェデレーション および **Web** サービスの変数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。

Advanced Authentication Server の有効化

ユーザのポリシー サーバの設定の一部として、Advanced Authentication Server を有効にします。

次の手順に従ってください:

1. ポリシー サーバ設定ウィザードを実行します。
2. ウィザードの最初の画面にあるチェックボックスをすべてオフのままにします。
3. [次へ] をクリックします。
4. Advanced Authentication Server 用のマスタ暗号化キーを作成します。
注: 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。
5. ポリシー サーバ設定ウィザードの残りの手順を完了します。

Advanced Authentication Server が有効になります。

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。

以下の点を考慮します。

- 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の手順を実行します。
- (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](#) (P. 598) します。

次の手順に従ってください:

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: 15

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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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 サーバに管理者認証情報を提供します。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認証情報を使用します。

個別キー ストアの設定

連結されたポリシー/キー ストアがある場合、ポリシー サーバを設定して個別のキー ストアを使用できます。

個別のキー ストアとして機能するディレクトリ サーバのタイプにより、ストアの設定方法が決まります。

- **SiteMinder smldapsetup** ユーティリティを使用してポリシー ストアを設定できる場合、キー ストアに固有のスキーマを使用して、個別のキー ストアを設定できます。以下のディレクトリ サーバはこのように設定できます。
 - Microsoft Active Directory
 - Microsoft AD LDS
 - Oracle Directory Server Enterprise Edition
 - Oracle Internet Directory Server
 - Red Hat Directory Server
 - **SiteMinder smldapsetup** ユーティリティを使用してポリシー ストアを設定できない場合は、以下のことを行う必要があります。
 - a. ポリシー ストア スキーマのみを有する個別のディレクトリ サーバインスタンスを設定します。ポリシー ストア スキーマにはキー ストア スキーマが含まれます。以下を行う必要はありません。
 - SiteMinder スーパーユーザ パスワードの設定
 - 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。
 - ポリシー ストア データ定義をインポートします。個別のキー ストアはこれらのオブジェクトを必要としません。
 - b. ポリシー サーバを設定して、キー ストアのみとしてこのポリシー ストア インスタンスを使用します。
- 注: 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。

キー ストアとしての Microsoft Active Directory

個別のキー ストアとして **Microsoft Active Directory** を設定できます。

キー ストアを設定する方法

キー ストアを作成するために以下のタスクを完了します。

1. キー ストアとして機能するディレクトリ サーバインスタンスを作成します。 **SiteMinder** キーを格納するルート サフィックスおよびルート オブジェクトを必ず作成します。

注: 詳細については、各ベンダーのドキュメントを参照してください。

2. スキーマの作成、およびキー ストア ルート オブジェクト下の **LDAP** ツリー内のオブジェクトの読み取り、変更および削除を行う権限を有する **LDAP** ユーザを作成します。

注: 詳細については、各ベンダーのドキュメントを参照してください。

3. キー ストアを登録します。
4. キー ストア スキーマを作成します。
5. キー ストア スキーマをインポートします。
6. ポリシー サーバを再起動します。

ディレクトリ サーバ情報の収集

個別のキー ストアを設定するには具体的情報が必要です。以下の情報を確認しておきます。

ホスト

ディレクトリ サーバ ホスト システムの完全修飾名または IP アドレス

ポート

ディレクトリ サーバ インスタンスがリスンするポート この値は、インスタンスが標準でないポートでリスンする場合にのみ必要です。

デフォルト値: 636 (SSL) および 389 (SSL 以外)

管理 DN

以下を行う権限を有するユーザの **LDAP** ユーザ名を指定します。

- スキーマの作成

注: この許可はキー ストア スキーマをインポートする場合にのみ必要です。キー ストアを展開した後、許可がないユーザとポリシー サーバを設定できます。

- read

- write
- modify
- delete

管理パスワード

管理 DN のパスワードを指定します。

キー ストア ルート DN

キー ストア オブジェクトをインポートする、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

キー ストアの登録

キー ストアを登録すると、キー ストアとポリシー サーバの間の接続が設定されます。ポリシー サーバは、キー ストアを管理するためにユーザが提供する認証情報を使用します。

重要：登録により、個別のキー ストアを使用するためのポリシー サーバは設定されません。ポリシー サーバが再起動されるまで、設定は有効になりません。キー ストアが設定され、それを展開する準備ができるまで、ポリシー サーバを再起動しないでください。

次の手順に従ってください:

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て、接続を設定します。

```
smlldapsetup reg -hhost -pport -dadmin_user -wadmin_password -rroot -k1
```

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

注: これらのモードおよび引数の詳細については、「ポリシー サーバ 管理ガイド」を参照してください。

例:

```
smlldapsetup reg -host172.16.0.0 -p389 -d"cn=directory manager" -wpassword -r"dc=test" -k1
```

3. ポリシー サーバ管理コンソールを起動し、[データ] タブを開きます。
4. 以下の手順のいずれかを完了します。
 - ポリシー サーバがデータ リレーショナル データベースを使用するように設定される場合:
 - a. [データベース] リストから [キー ストア] を選択します。
 - b. [ストレージ] リストから LDAP を選択し、接続設定および管理認証情報を表示します。
 - c. 接続設定および管理ユーザ設定が表示されていることを確認します。
 - d. [LDAP 接続のテスト] をクリックして、ポリシー サーバがキー ストア インスタンスと通信できることを確認します。
 - ポリシー サーバがディレクトリ サーバを使用するように設定される場合:
 - a. [データベース] リストから [キー ストア] を選択します。
 - b. 接続設定および管理ユーザ設定が表示されていることを確認します。
 - c. [LDAP 接続のテスト] をクリックして、ポリシー サーバがキー ストア インスタンスと通信できることを確認します。

注: [ポリシー ストアを使用] データベース設定がクリアされます。クリアされた設定は予期された正常な動作です。ポリシー サーバは、ポリシー ストアと連結させたキー ストアを引き続き使用します。

5. ポリシー サーバ管理コンソールを終了します。
個別のキーがポリシー サーバに登録されます。

キー ストア スキーマの作成

キー ストア インスタンスは、SiteMinder Web エージェント キーを格納および取得するようスキーマに要求します。smldapsetup ユーティリティを使用して、キー ストア スキーマ ファイルを作成します。

次の手順に従ってください:

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て、キー ストア スキーマ ファイルを作成します。

```
smldapsetup ldgen -ffile_name -k1
```

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

注: これらのモードおよび引数の詳細については、「ポリシー サーバ 管理ガイド」を参照してください。

例: `smldapsetup ldgen -fkeystoreschema -k1`

キー ストア スキーマ ファイルが作成されます。

キー ストア スキーマのインポート

キー ストア インスタンスは、SiteMinder Web エージェント キーを格納および取得するようスキーマに要求します。 `smlldapsetup` ユーティリティを使用して、キー ストア スキーマ ファイルをインポートします。

以下の手順に従います。

1. ポリシー サーバ ホスト システムにログインします。
2. キー ストア スキーマをインポートするために以下のコマンドを実行します。

```
smlldapsetup ldmod -ffile_name -k1
```

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

以下の点を考慮します。

- これらのモードおよび引数の詳細については、「ポリシー サーバ管理ガイド」を参照してください。
- 標準出力は、インポートされているポリシー ストア スキーマをすべて表示します。その動作は正常で予期されるものです。ユーティリティは単にキー ストアに固有のスキーマをインポートします。

例: `smlldapsetup ldmod -fkeystoreschema -k1`

キー ストアに固有のスキーマがインポートされます。

ポリシー サーバの再起動

ポリシー サーバは、再起動されるまで連結されたキー ストアを引き続き使用します。個別のキー ストアの使用を開始するにはポリシー サーバを再起動します。

注: 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。

ポリシー ストアとしての Microsoft AD LDS

個別のキー ストアとして Microsoft AD LDS を設定できます。

キー ストアを設定する方法

キー ストアを作成するために以下のタスクを完了します。

1. キー ストアとして機能するディレクトリ サーバインスタンスを作成します。 **SiteMinder** キーを格納するルート サフィックスおよびルート オブジェクトを必ず作成します。

注: 詳細については、各ベンダーのドキュメントを参照してください。

2. スキーマの作成、およびキー ストア ルート オブジェクト下の LDAP ツリー内のオブジェクトの読み取り、変更および削除を行う権限を有する LDAP ユーザを作成します。

注: 詳細については、各ベンダーのドキュメントを参照してください。

3. ディレクトリ サーバがキー ストア的前提条件を満たすことを確認してください。
4. キー ストアを登録します。
5. キー ストア スキーマを作成します。
6. キー ストア スキーマをインポートします。
7. ポリシー サーバを再起動します。

キーストアの前提条件

ポリシー ストアを設定する前に、以下の要件を満たすことを確認してください。

1. キー ストア パーティションを作成します。
2. 設定パーティション内にユーザを作成できることを確認してください。設定パーティション内の管理ユーザのみが、ポリシー ストア スキーマをインポートできます。

設定パーティション内でのユーザ作成を許可します。

設定パーティション内の管理ユーザのみが、ポリシー ストア スキーマをインポートできます。このユーザは、キー ストア パーティションを含む設定パーティションおよびすべてのアプリケーション パーティションにおける管理者権限を持っている必要があります。

以下の手順に従います。

1. ADSI 編集コンソールを開きます。

2. 設定パーティション内の以下の場所に移動します。

cn=directory service, cn=windows nt,
cn=services, cn=configuration, cn={guid}

3. msDS-Other-Settings 属性を検索します。
4. msDS-Other-Settings 属性に以下の新しい値を追加します。
ADAMAllowADAMSecurityPrincipalsInConfigPartition=1
5. 設定およびポリシー ストア アプリケーション パーティション内では、
以下を実行します。

- a. CN=Administrators, CN=Role に移動します。
- b. CN=Administrators のプロパティを開きます。
- c. メンバ属性を編集します。
- d. [DN を追加する] をクリックして、設定パーティションで作成したユーザのフル DN をペーストします。
- e. 作成したユーザのプロパティに移動し、以下のオブジェクトの値を確認します。

msDS-UserAccountDisabled

値は必ず **false** に設定してください。

管理ユーザには、キー ストア パーティションを含む設定パーティションおよびすべてのアプリケーション パーティションにおける権限があります。

ディレクトリ サーバ情報の収集

個別のキー ストアを設定するには具体的情報が必要です。以下の情報を確認しておきます。

ホスト

ディレクトリ サーバ ホスト システムの完全修飾名または IP アドレス

ポート

ディレクトリ サーバ インスタンスがリスンするポート この値は、インスタンスが標準でないポートでリスンする場合にのみ必要です。

デフォルト値： 636 (SSL) および 389 (SSL 以外)

■ 管理者 DN

guid 値を含む、ディレクトリ サーバ管理者のフル ドメイン名

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

このユーザは以下の権限を必要とします。

- スキーマの作成

注：この許可はキー ストア スキーマをインポートする場合にのみ必要です。キー ストアを展開した後、許可がないユーザとポリシー サーバを設定できます。

- read
- write
- modify
- 削除

管理者パスワード

ディレクトリ サーバ管理者のパスワード

アプリケーション パーティションのルート DN

キー ストア スキーマをインポートする必要がある場合アプリケーション パーティションのルート DN の場所

(オプション) SSL クライアント証明書

ディレクトリ接続が SSL で行われる場合は、SSL クライアント証明書データベースを含むディレクトリのパス

キー ストアの登録

キー ストアを登録すると、キー ストアとポリシー サーバの間の接続が設定されます。ポリシー サーバは、キー ストアを管理するためにユーザが提供する認証情報を使用します。

重要：登録により、個別のキー ストアを使用するためのポリシー サーバは設定されません。ポリシー サーバが再起動されるまで、設定は有効になりません。キー ストアが設定され、それを展開する準備ができるまで、ポリシー サーバを再起動しないでください。

次の手順に従ってください:

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て、接続を設定します。

```
smlldapsetup reg -hhost -pport -dadmin_user -wadmin_password -rroot -k1
```

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

注: これらのモードおよび引数の詳細については、「ポリシー サーバ 管理ガイド」を参照してください。

例:

```
smlldapsetup reg -host172.16.0.0 -p389 -d"cn=directory manager" -wpassword -r"dc=test" -k1
```

3. ポリシー サーバ管理コンソールを起動し、[データ] タブを開きます。
4. 以下の手順のいずれかを完了します。
 - ポリシー サーバがデータ リレーショナル データベースを使用するように設定される場合:
 - a. [データベース] リストから [キー ストア] を選択します。
 - b. [ストレージ] リストから LDAP を選択し、接続設定および管理認証情報を表示します。
 - c. 接続設定および管理ユーザ設定が表示されていることを確認します。
 - d. [LDAP 接続のテスト] をクリックして、ポリシー サーバがキー ストア インスタンスと通信できることを確認します。
 - ポリシー サーバがディレクトリ サーバを使用するように設定される場合:
 - a. [データベース] リストから [キー ストア] を選択します。
 - b. 接続設定および管理ユーザ設定が表示されていることを確認します。
 - c. [LDAP 接続のテスト] をクリックして、ポリシー サーバがキー ストア インスタンスと通信できることを確認します。

注: [ポリシー ストアを使用] データベース設定がクリアされます。クリアされた設定は予期された正常な動作です。ポリシー サーバは、ポリシー ストアと連結させたキー ストアを引き続き使用します。

5. ポリシー サーバ管理コンソールを終了します。
個別のキーがポリシー サーバに登録されます。

キー ストア スキーマの作成

キー ストア インスタンスは、**SiteMinder Web** エージェント キーを格納および取得するようスキーマに要求します。 **smldapsetup** ユーティリティを使用して、キー ストア スキーマ ファイルを作成します。

次の手順に従ってください:

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て、キー ストア スキーマ ファイルを作成します。

```
smldapsetup ldgen -ffile_name -k1
```

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

注: これらのモードおよび引数の詳細については、「ポリシー サーバ 管理ガイド」を参照してください。

例: **smldapsetup ldgen -fkeystoreschema -k1**

キー ストア スキーマ ファイルが作成されます。

キー ストア スキーマのインポート

キー ストア インスタンスは、SiteMinder Web エージェント キーを格納および取得するようスキーマに要求します。smlldapsetup ユーティリティを使用して、キー ストア スキーマ ファイルをインポートします。

以下の手順に従います。

1. ポリシー サーバ ホスト システムにログインします。
2. キー ストア スキーマをインポートするために以下のコマンドを実行します。

```
smlldapsetup ldmod -ffile_name -k1
```

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

以下の点を考慮します。

- これらのモードおよび引数の詳細については、「ポリシー サーバ管理ガイド」を参照してください。
- 標準出力は、インポートされているポリシー ストア スキーマをすべて表示します。その動作は正常で予期されるものです。ユーティリティは単にキー ストアに固有のスキーマをインポートします。

例: smlldapsetup ldmod -fkeystoreschema -k1

キー ストアに固有のスキーマがインポートされます。

ポリシー サーバの再起動

ポリシー サーバは、再起動されるまで連結されたキー ストアを引き続き使用します。個別のキー ストアの使用を開始するにはポリシー サーバを再起動します。

注: 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。

ポリシー ストアとしての Oracle Directory Server Enterprise Edition

別のキー ストアとして Oracle Directory Server Enterprise Edition を設定できます。

キー ストアを設定する方法

キー ストアを作成するために以下のタスクを完了します。

1. キー ストアとして機能するディレクトリ サーバインスタンスを作成します。**SiteMinder** キーを格納するルート サフィックスおよびルート オブジェクトを必ず作成します。

注: 詳細については、各ベンダーのドキュメントを参照してください。

2. スキーマの作成、およびキー ストア ルート オブジェクト下の LDAP ツリー内のオブジェクトの読み取り、変更および削除を行う権限を有する LDAP ユーザを作成します。

注: 詳細については、各ベンダーのドキュメントを参照してください。

3. キー ストアの考慮事項を確認します。
4. ディレクトリ サーバの情報を収集します。
5. キー ストアを登録します。
6. キー ストア スキーマを作成します。
7. キー ストア スキーマをインポートします。
8. ポリシー サーバを再起動します。

キー ストアの考慮事項

`smldapsetup` ユーティリティは `ou=Netegrity`、`root` サブ サフィックス、`PolicySvr4` データベースを作成します。

`root`

キー ストアを登録するときに指定するディレクトリ ルート この変数は、既存のルート サフィックスまたはサブ サフィックスのいずれかである必要があります。

例: ルート サフィックスが `dc=netegrity,dc=com` である場合、`smldapsetup` を実行すると、ディレクトリ サーバに以下のエントリが生成されます。

- ルート サフィックス、`dc=netegrity,dc=com`、対応する `userRoot` データベース。
- サブ サフィックス、`ou=Netegrity,dc=netegrity,dc=com`、対応する `PolicySvr4` データベース。

例：キー ストアを `ou=apps,dc=netegrity,dc=com` の下に置く場合、`ou=apps,dc=netegrity,dc=com` は、ルート サフィックス `dc=netegrity,dc=com` のルートまたはサブ サフィックスのいずれかである必要があります。

サブ サフィックスである場合、`smldapsetup` を実行すると以下のエントリが作成されます。

- ルート サフィックス、`dc=netegrity,dc=com`、対応する `userRoot` データベース。
- サブ サフィックス、`ou=apps,dc=netegrity,dc=com`、対応する `Apps` データベース。
- サブ サフィックス、`ou=Netegrity,ou=apps,dc=netegrity,dc=com`、対応する `PolicySvr4` データベース。

注：ルートおよびサブ サフィックスの詳細については、各ベンダーのドキュメントを参照してください。

ディレクトリ サーバ情報の収集

個別のキー ストアを設定するには具体的情報が必要です。以下の情報を確認しておきます。

ホスト

ディレクトリ サーバ ホスト システムの完全修飾名または IP アドレス

ポート

ディレクトリ サーバ インスタンスがリスンするポート この値は、インスタンスが標準でないポートでリスンする場合にのみ必要です。

デフォルト値：636（SSL）および 389（SSL 以外）

管理 DN

以下を行う権限を有するユーザの LDAP ユーザ名を指定します。

- スキーマの作成

注：この許可はキー ストア スキーマをインポートする場合にのみ必要です。キー ストアを展開した後、許可がないユーザとポリシー サーバを設定できます。

- read
- write

- modify
- delete

管理パスワード

管理 DN のパスワードを指定します。

キー ストア ルート DN

キー ストア オブジェクトをインポートする、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

キー ストアの登録

キー ストアを登録すると、キー ストアとポリシー サーバの間の接続が設定されます。ポリシー サーバは、キー ストアを管理するためにユーザが提供する認証情報を使用します。

重要: 登録により、個別のキー ストアを使用するためのポリシー サーバは設定されません。ポリシー サーバが再起動されるまで、設定は有効になりません。キー ストアが設定され、それを展開する準備ができるまで、ポリシー サーバを再起動しないでください。

次の手順に従ってください:

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て、接続を設定します。

```
smlldapsetup reg -hhost -pport -dadmin_user -wadmin_password -rroot -k1
```

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

注: これらのモードおよび引数の詳細については、「ポリシー サーバ 管理ガイド」を参照してください。

例:

```
smlldapsetup reg -host172.16.0.0 -p389 -d"cn=directory manager" -wpassword -r"dc=test" -k1
```

3. ポリシー サーバ管理コンソールを起動し、[データ] タブを開きます。
4. 以下の手順のいずれかを完了します。
 - ポリシー サーバがデータ リレーショナル データベースを使用するように設定される場合:
 - a. [データベース] リストから [キー ストア] を選択します。
 - b. [ストレージ] リストから LDAP を選択し、接続設定および管理認証情報を表示します。
 - c. 接続設定および管理ユーザ設定が表示されていることを確認します。
 - d. [LDAP 接続のテスト] をクリックして、ポリシー サーバがキー ストア インスタンスと通信できることを確認します。
 - ポリシー サーバがディレクトリ サーバを使用するように設定される場合:
 - a. [データベース] リストから [キー ストア] を選択します。
 - b. 接続設定および管理ユーザ設定が表示されていることを確認します。
 - c. [LDAP 接続のテスト] をクリックして、ポリシー サーバがキー ストア インスタンスと通信できることを確認します。

注: [ポリシー ストアを使用] データベース設定がクリアされます。クリアされた設定は予期された正常な動作です。ポリシー サーバは、ポリシー ストアと連結させたキー ストアを引き続き使用します。

5. ポリシー サーバ管理コンソールを終了します。
個別のキーがポリシー サーバに登録されます。

キー ストア スキーマの作成

キー ストア インスタンスは、**SiteMinder Web** エージェント キーを格納および取得するようスキーマに要求します。 **smldapsetup** ユーティリティを使用して、キー ストア スキーマ ファイルを作成します。

次の手順に従ってください:

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て、キー ストア スキーマ ファイルを作成します。

```
smldapsetup ldgen -ffile_name -k1
```

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

注: これらのモードおよび引数の詳細については、「ポリシー サーバ 管理ガイド」を参照してください。

例: **smldapsetup ldgen -fkeystoreschema -k1**

キー ストア スキーマ ファイルが作成されます。

キー ストア スキーマのインポート

キー ストア インスタンスは、SiteMinder Web エージェント キーを格納および取得するようスキーマに要求します。 `smlldapsetup` ユーティリティを使用して、キー ストア スキーマ ファイルをインポートします。

以下の手順に従います。

1. ポリシー サーバ ホスト システムにログインします。
2. キー ストア スキーマをインポートするために以下のコマンドを実行します。

```
smlldapsetup ldmod -ffile_name -k1
```

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

以下の点を考慮します。

- これらのモードおよび引数の詳細については、「ポリシー サーバ管理ガイド」を参照してください。
- 標準出力は、インポートされているポリシー ストア スキーマをすべて表示します。その動作は正常で预期されるものです。ユーティリティは単にキー ストアに固有のスキーマをインポートします。

例: `smlldapsetup ldmod -fkeystoreschema -k1`

キー ストアに固有のスキーマがインポートされます。

ポリシー サーバの再起動

ポリシー サーバは、再起動されるまで連結されたキー ストアを引き続き使用します。個別のキー ストアの使用を開始するにはポリシー サーバを再起動します。

注: 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。

Oracle Directory Server キー ストアのレプリケート

SiteMinder では、UserRoot および PolicySvr4 データベースを作成します。サフィックス マッピングは PolicySvr4 データベースを参照しています。キー ストアのレプリケートには、PolicySvr4 データベース ディレクトリのレプリケーション アグリーメントのセットアップが必要です。

次の手順に従ってください:

1. 各ベンダーのドキュメントで詳述されるとおりレプリケーション アグリーメントを設定します。
2. ポリシー サーバ ホスト システムにログインします。
3. 以下のコマンドを実行して SiteMinder インデックスを生成します。

```
smldapsetup ldgen -x -findexes.ldif
```

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

4. レプリカ サーバ上で以下のようにインデックスをセットアップします。

```
smldapsetup ldmod -x -findexes.ldif -hhost -prelicaport  
-dAdminDN -wAdminPW
```

host

レプリカ ホストを指定します。

replicaport

レプリカ ポート番号を指定します。

AdminDN

レプリカ管理者 DN を指定します。

例: cn=directory manager

AdminPW

レプリカ管理者パスワードを指定します。

SiteMinder インデックスがレプリケートされます。

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

別のキー ストアとして **Oracle Internet Directory Server** を設定できます。

キー ストアを設定する方法

キー ストアを作成するために以下のタスクを完了します。

1. キー ストアとして機能するディレクトリ サーバインスタンスを作成します。**SiteMinder** キーを格納するルート サフィックスおよびルート オブジェクトを必ず作成します。

注: 詳細については、各ベンダーのドキュメントを参照してください。

2. スキーマの作成、およびキー ストア ルート オブジェクト下の **LDAP** ツリー内のオブジェクトの読み取り、変更および削除を行う権限を有する **LDAP** ユーザを作成します。

注: 詳細については、各ベンダーのドキュメントを参照してください。

3. キー ストアを登録します。
4. キー ストア スキーマを作成します。
5. キー ストア スキーマをインポートします。
6. ポリシー サーバを再起動します。

ディレクトリ サーバ情報の収集

個別のキー ストアを設定するには具体的情報が必要です。以下の情報を確認しておきます。

ホスト

ディレクトリ サーバ ホスト システムの完全修飾名または **IP アドレス**

ポート

ディレクトリ サーバ インスタンスがリスンするポート この値は、インスタンスが標準でないポートでリスンする場合にのみ必要です。

デフォルト値: 636 (SSL) および 389 (SSL 以外)

管理 DN

以下を行う権限を有するユーザの LDAP ユーザ名を指定します。

- スキーマの作成

注: この許可はキー ストア スキーマをインポートする場合にのみ必要です。キー ストアを展開した後、許可がないユーザとポリシー サーバを設定できます。

- read
- write
- modify
- delete

管理パスワード

管理 DN のパスワードを指定します。

キー ストア ルート DN

キー ストア オブジェクトをインポートする、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

キー ストアの登録

キー ストアを登録すると、キー ストアとポリシー サーバの間の接続が設定されます。ポリシー サーバは、キー ストアを管理するためにユーザが提供する認証情報を使用します。

重要: 登録により、個別のキー ストアを使用するためのポリシー サーバは設定されません。ポリシー サーバが再起動されるまで、設定は有効になりません。キー ストアが設定され、それを展開する準備ができるまで、ポリシー サーバを再起動しないでください。

次の手順に従ってください:

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て、接続を設定します。

```
smlldapsetup reg -hhost -pport -dadmin_user -wadmin_password -rroot -k1
```

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

注: これらのモードおよび引数の詳細については、「ポリシー サーバ 管理ガイド」を参照してください。

例:

```
smlldapsetup reg -host172.16.0.0 -p389 -d"cn=directory manager" -wpassword -r"dc=test" -k1
```

3. ポリシー サーバ管理コンソールを起動し、[データ] タブを開きます。
4. 以下の手順のいずれかを完了します。
 - ポリシー サーバがデータ リレーショナル データベースを使用するように設定される場合:
 - a. [データベース] リストから [キー ストア] を選択します。
 - b. [ストレージ] リストから LDAP を選択し、接続設定および管理認証情報を表示します。
 - c. 接続設定および管理ユーザ設定が表示されていることを確認します。
 - d. [LDAP 接続のテスト] をクリックして、ポリシー サーバがキー ストア インスタンスと通信できることを確認します。
 - ポリシー サーバがディレクトリ サーバを使用するように設定される場合:
 - a. [データベース] リストから [キー ストア] を選択します。
 - b. 接続設定および管理ユーザ設定が表示されていることを確認します。
 - c. [LDAP 接続のテスト] をクリックして、ポリシー サーバがキー ストア インスタンスと通信できることを確認します。

注: [ポリシー ストアを使用] データベース設定がクリアされます。クリアされた設定は予期された正常な動作です。ポリシー サーバは、ポリシー ストアと連結させたキー ストアを引き続き使用します。

5. ポリシー サーバ管理コンソールを終了します。
個別のキーがポリシー サーバに登録されます。

キー ストア スキーマの作成

キー ストア インスタンスは、**SiteMinder Web** エージェント キーを格納および取得するようスキーマに要求します。 **smldapsetup** ユーティリティを使用して、キー ストア スキーマ ファイルを作成します。

次の手順に従ってください:

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て、キー ストア スキーマ ファイルを作成します。

```
smldapsetup ldgen -ffile_name -k1
```

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

注: これらのモードおよび引数の詳細については、「ポリシー サーバ 管理ガイド」を参照してください。

例: **smldapsetup ldgen -fkeystoreschema -k1**

キー ストア スキーマ ファイルが作成されます。

キー ストア スキーマのインポート

キー ストア インスタンスは、SiteMinder Web エージェント キーを格納および取得するようスキーマに要求します。 `smldapsetup` ユーティリティを使用して、キー ストア スキーマ ファイルをインポートします。

以下の手順に従います。

1. ポリシー サーバ ホスト システムにログインします。
2. キー ストア スキーマをインポートするために以下のコマンドを実行します。

```
smldapsetup ldmod -ffile_name -k1
```

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

以下の点を考慮します。

- これらのモードおよび引数の詳細については、「ポリシー サーバ管理ガイド」を参照してください。
- 標準出力は、インポートされているポリシー ストア スキーマをすべて表示します。その動作は正常で予期されるものです。ユーティリティは単にキー ストアに固有のスキーマをインポートします。

例: `smldapsetup ldmod -fkeystoreschema -k1`

キー ストアに固有のスキーマがインポートされます。

ポリシー サーバの再起動

ポリシー サーバは、再起動されるまで連結されたキー ストアを引き続き使用します。個別のキー ストアの使用を開始するにはポリシー サーバを再起動します。

注: 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。

キー ストアとしての Red Hat Directory Server

別のキー ストアとして Red Hat Directory Server を設定できます。

キー ストアを設定する方法

キー ストアを作成するために以下のタスクを完了します。

1. キー ストアとして機能するディレクトリ サーバインスタンスを作成します。 **SiteMinder** キーを格納するルート サフィックスおよびルート オブジェクトを必ず作成します。

注: 詳細については、各ベンダーのドキュメントを参照してください。

2. スキーマの作成、およびキー ストア ルート オブジェクト下の **LDAP** ツリー内のオブジェクトの読み取り、変更および削除を行う権限を有する **LDAP** ユーザを作成します。

注: 詳細については、各ベンダーのドキュメントを参照してください。

3. キー ストアを登録します。
4. キー ストア スキーマを作成します。
5. キー ストア スキーマをインポートします。
6. ポリシー サーバを再起動します。

キー ストアの登録

キー ストアを登録すると、キー ストアとポリシー サーバの間の接続が設定されます。ポリシー サーバは、キー ストアを管理するためにユーザが提供する認証情報を使用します。

重要: 登録により、個別のキー ストアを使用するためのポリシー サーバは設定されません。ポリシー サーバが再起動されるまで、設定は有効になりません。キー ストアが設定され、それを展開する準備ができるまで、ポリシー サーバを再起動しないでください。

次の手順に従ってください:

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て、接続を設定します。

```
smlldapsetup reg -hhost -pport -dadmin_user -wadmin_password -rroot -k1
```

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

注: これらのモードおよび引数の詳細については、「ポリシー サーバ 管理ガイド」を参照してください。

例:

```
smlldapsetup reg -host172.16.0.0 -p389 -d"cn=directory manager" -wpassword -r"dc=test" -k1
```

3. ポリシー サーバ管理コンソールを起動し、[データ] タブを開きます。
4. 以下の手順のいずれかを完了します。
 - ポリシー サーバがデータ リレーショナル データベースを使用するように設定される場合:
 - a. [データベース] リストから [キー ストア] を選択します。
 - b. [ストレージ] リストから LDAP を選択し、接続設定および管理認証情報を表示します。
 - c. 接続設定および管理ユーザ設定が表示されていることを確認します。
 - d. [LDAP 接続のテスト] をクリックして、ポリシー サーバがキー ストア インスタンスと通信できることを確認します。
 - ポリシー サーバがディレクトリ サーバを使用するように設定される場合:
 - a. [データベース] リストから [キー ストア] を選択します。
 - b. 接続設定および管理ユーザ設定が表示されていることを確認します。
 - c. [LDAP 接続のテスト] をクリックして、ポリシー サーバがキー ストア インスタンスと通信できることを確認します。

注: [ポリシー ストアを使用] データベース設定がクリアされます。クリアされた設定は予期された正常な動作です。ポリシー サーバは、ポリシー ストアと連結させたキー ストアを引き続き使用します。

5. ポリシー サーバ管理コンソールを終了します。
個別のキーがポリシー サーバに登録されます。

キー ストア スキーマの作成

キー ストア インスタンスは、SiteMinder Web エージェント キーを格納および取得するようスキーマに要求します。smlldapsetup ユーティリティを使用して、キー ストア スキーマ ファイルを作成します。

次の手順に従ってください:

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て、キー ストア スキーマ ファイルを作成します。

```
smlldapsetup ldgen -ffile_name -k1
```

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

注: これらのモードおよび引数の詳細については、「ポリシー サーバ 管理ガイド」を参照してください。

例: smlldapsetup ldgen -fkeystoreschema -k1

キー ストア スキーマ ファイルが作成されます。

キー ストア スキーマのインポート

キー ストア インスタンスは、SiteMinder Web エージェント キーを格納および取得するようスキーマに要求します。smlldapsetup ユーティリティを使用して、キー ストア スキーマ ファイルをインポートします。

次の手順に従ってください:

1. ポリシー サーバ ホスト システムにログインします。
2. キー ストア スキーマをインポートするために以下のコマンドを実行します。

```
smlldapsetup ldmod -ffile_name -k1
```

注:

- これらのモードおよび引数の詳細については、「ポリシー サーバ管理ガイド」を参照してください。
- 標準出力は、インポートされているポリシー ストア スキーマをすべて表示します。その動作は正常で予期されるものです。ユーティリティは単にキー ストアに固有のスキーマをインポートします。ユーティリティは単にキー ストアに固有のスキーマをインポートします。

例:

```
smldapsetup ldmod -fkeystoreschema -k1
```

キー ストアに固有のスキーマがインポートされます。

3. 以下の手順を実行します。

- a. ディレクトリ サーバを再起動します。ディレクトリ サーバの再起動は、キー ストア スキーマを正しく保存するために必要です。
- b. 手順 2 を繰り返します。ディレクトリ サーバの再起動により、キー ストア ルートが削除されました。キー ストア ルートを作成するには、キー ストア スキーマを再度インポートする必要があります。

キー ストアに固有のスキーマがインポートされます。

ポリシー サーバの再起動

ポリシー サーバは、再起動されるまで連結されたキー ストアを引き続き使用します。個別のキー ストアの使用を開始するにはポリシー サーバを再起動します。

注: 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。

第 7 章: リレーショナル データベースでの SiteMinder データ ストアの設定

このセクションには、以下のトピックが含まれています。

[ポリシーまたはキーのストアとしてのリレーショナル データベース \(P. 314\)](#)

[インストール ロードマップ \(P. 314\)](#)

[重要な考慮事項 \(P. 316\)](#)

[デフォルトのポリシー ストア オブジェクトに関する考慮事項 \(P. 316\)](#)

[リレーショナル データベース用のスキーマ ファイル \(P. 317\)](#)

[MySQL ポリシー ストアの設定 \(P. 322\)](#)

[SQL Server ポリシー ストアの設定 \(P. 338\)](#)

[PostgreSQL サーバ ポリシー ストアを設定する方法 \(P. 356\)](#)

[Oracle ポリシー ストアの設定 \(P. 372\)](#)

[IBM DB2 ポリシー ストアの設定 \(P. 400\)](#)

[セッション情報を IBM DB2 に格納する方法 \(P. 416\)](#)

[セッション情報を MySQL に格納する方法 \(P. 418\)](#)

[Oracle でセッション情報を格納する方法 \(P. 421\)](#)

[SQL Server 内にセッション情報を格納する方法 \(P. 424\)](#)

[セッション情報を PostgreSQL に格納する方法 \(P. 427\)](#)

[監査ログを IBM DB2 に格納する方法 \(P. 430\)](#)

[監査ログを MySQL に格納する方法 \(P. 433\)](#)

[Oracle で監査ログを格納する方法 \(P. 436\)](#)

[SQL Server 内に監査ログを格納する方法 \(P. 439\)](#)

[監査ログを PostgreSQL に格納する方法 \(P. 442\)](#)

[キー情報を IBM DB2 に格納する方法 \(P. 445\)](#)

[キー情報を MySQL に格納する方法 \(P. 448\)](#)

[Oracle でキー情報を格納する方法 \(P. 451\)](#)

[SQL Server 内にキー情報を格納する方法 \(P. 454\)](#)

[キー情報を PostgreSQL に格納する方法 \(P. 457\)](#)

[サンプル ユーザ ディレクトリ \(P. 460\)](#)

ポリシーまたはキーのストアとしてのリレーショナル データベース

SiteMinder ポリシー ストアとは、すべてのポリシー関連情報のためのリポジトリです。SiteMinder インストールでのすべてのポリシー サーバは、直接またはレプリケーションを通じて、ポリシー ストア データを共有する必要があります。SiteMinder は、管理者がポリシー ストア データをある格納場所から別の格納場所に移動できるツールを使用してインストールされます。

ポリシー サーバをインストールするとき、自動的にポリシー ストアとして以下のリレーショナルデータベースのうちの 1 つを設定できます。

- Microsoft SQL Server
- Oracle RDBMS

ポリシー サーバをインストールした後、必要に応じて、手動でポリシー ストアを設定できます。また、ポリシー サーバのインストール後、ポリシー サーバ管理コンソールを使用してポリシー サーバを既存のポリシー ストアに示すこともできます。

注: サポートされている CA およびサードパーティ コンポーネントのリストについては、テクニカルサポート サイトの **SiteMinder 12.52 SP1** プラットフォームのサポート マトリックスを参照してください。

ポリシー ストアのサポートに加え、リレーショナル データベースを使用して SiteMinder キー、監査ログ、セッション データを格納することができます。

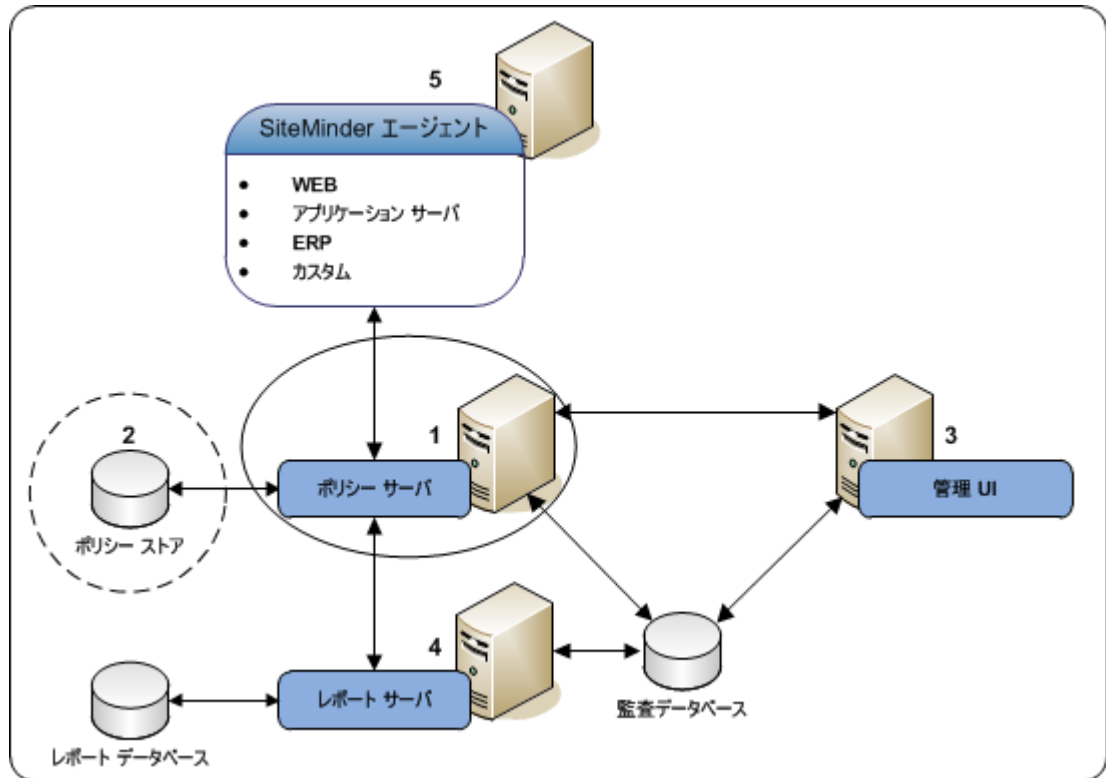
インストール ロード マップ

以下の図はサンプル SiteMinder のインストールを示しており、各コンポーネントのインストールおよび設定の指示がリスト表示されています。

- 実線で囲まれているのがポリシー サーバです。ポリシー ストアを設定する前に必要です。ポリシー サーバが環境に含まれていない場合は、続行前にそれをインストールします。
- 点線で囲まれているのがポリシー ストアです。このコンポーネントをすぐに設定します。

以下の図は、単一のポリシー/キー ストア インスタンスを示します。図示されていませんが、環境は個別のポリシーおよびキー ストア用の個別のインスタンスを使用できます。

数式 2: インストール ロードマップ



重要な考慮事項

ポリシー ストアを設定する前に、以下の問題を考慮します。

- 起こり得るポリシー ストアの破損を回避します。以下のように、ポリシー ストアをホストするデータベース サーバが **UTF-8** 形式でオブジェクトを格納するように設定されていることを確認してください。
 - (Oracle) データベースが **UTF-8** 形式でオブジェクトを格納するように設定されていることを確認してください。Oracle は、多くのユニコードの文字セットをサポートします。
 - (SQL Server) データベースがデフォルトの照合 (SQL_Latin1_General_CP1_CI_AS) を使用して設定されていることを確認してください。大文字/小文字を区別した照合を使用すると、予期しない動作をする場合があります。
- IPv6 ODBC データ ソースを使用する場合、IP アドレスを角かっこで囲むと接続に失敗します。

例：[fec0::9255:20c:29ff:fe47:8089] ではなく fec0::9255: 20c 29ff fe47 8089 を使用

デフォルトのポリシー ストア オブジェクトに関する考慮事項

ポリシー ストアを設定するとき、以下のデフォルトのポリシー ストア オブジェクト ファイルが利用可能です。

- smpolicy.xml
- smpolicy-secure.xml

両方のファイルには、ポリシー ストアが必要とするデフォルトのオブジェクトが含まれます。

- ポリシー ストアを自動的に設定するためにポリシー サーバ設定ウィザードを使用する場合、ウィザードは単に smpolicy.xml を使用します。
- smpolicy-secure.xml を使用したい場合は、ポリシー ストアを手動で設定します。

両方のファイルはデフォルトのセキュリティ設定を提供します。これらの設定は、管理 UI で利用可能なデフォルトのエージェント設定オブジェクト（ACO）テンプレートで利用可能です。 **smpolicy-secure** ファイルはより制限の厳しいデフォルトのセキュリティ設定を提供します。

smpolicy.xml を選択すると、より制限の厳しいデフォルトのセキュリティ設定を使用する制限はありません。管理 UI を使用して、デフォルトの ACO 設定を変更できます。

以下の表では、両方のファイルに関するセキュリティ設定の概要について説明します。

パラメータ名	smpolicy 値	smpolicy-secure 値
BadCssChars	値なし	<, >, ', ;,), (, &, +, %00
BadQueryChars	値なし	<, >, ', ;,), (, &, +, %00
BadUrlChars	//, ./, /., /*, *., ~, ¥, %00-%1f, %7f-%ff, %25	smpolicy.smdif 値プラス : <, >, ', ;,), (, &, +
EnableCookieProvider	はい	いいえ
IgnoreExt	.class, .gif, .jpg, .jpeg, .png, .fcc, .scc, .sfcc, .ccc, .ntc	すべての smpolicy 値
LimitCookieProvider	いいえ	はい
ValidTargetDomain	このファイルには、このパラメータは含まれません。	このパラメータにはデフォルト値はありません。有効なリダイレクトドメインを提供します。 例 : validtargetdomain=".example.com"

リレーショナル データベース用のスキーマ ファイル

SiteMinder では、以下の SiteMinder データ ストアを設定するためのスキーマ ファイルを提供します。

- ポリシー ストア
- キー ストア
- ログ データベース

- セッション ストア
- サンプル ユーザ データベース

注: SiteMinder スキーマ ファイルはポリシー サーバと共にインストールされます。UNIX システムでは、*siteminder_home/db/SQL* ディレクトリにあるスキーマ ファイルを、データベースがある Windows システム上の一時ディレクトリ (C:¥temp) にコピーします。

siteminder_home

ポリシー サーバのインストール パスを指定します。

IBM DB2 スキーマ ファイル

以下の SQL Server スキーマ ファイルが *siteminder_home¥db¥tier2¥DB2* ディレクトリ内に提供されています。

siteminder_home

ポリシー サーバのインストール パスを指定します。

sm_db2_ps.sql

ポリシー ストアおよびキー ストア用のスキーマを作成します。

注: 別のデータベース内にキーを格納する場合、このスキーマ ファイルによってそのキー ストア データ用のスキーマが作成されます。

sm_db2_logs.sql

監査ログのスキーマを作成します。[このスクリプトを編集](#) (P. 431) してから、それを使用して監査ストアを作成してください。

sm_db2_ss.sql

セッション ストア用のスキーマを作成します。

smsampleusers_db2.sql

サンプル ユーザ データベース用のスキーマを作成し、サンプル ユーザをデータベースに読み込みます。

以下の IBM DB2 スキーマ ファイルが *siteminder_home¥xps¥db* ディレクトリ内に提供されています。

DB2.sql

ポリシー ストア用の XPS スキーマを作成します。

MySQL スキーマ ファイル

以下の SQL Server スキーマ ファイルが *siteminder_home¥db¥tier2¥MySQL* ディレクトリ内に提供されています。

siteminder_home

ポリシー サーバのインストール パスを指定します。

sm_mysql_ps.sql

ポリシー ストアおよびキー ストア用のスキーマを作成します。

注: 別のデータベース内にキーを格納する場合、このスキーマ ファイルによってそのキー ストア データ用のスキーマが作成されます。

sm_mysql_logs.sql

監査ログのスキーマを作成します。

sm_mysql_ss.sql

セッション ストアのスキーマを作成します。

sm_sampleusers_mysql.sql

サンプル ユーザ データベース用のスキーマを作成し、サンプル ユーザをデータベースに読み込みます。

以下の MySQL スキーマ ファイルが *siteminder_home¥xps¥db* ディレクトリ内にあります。

MySQL.sql

ポリシー ストア用の XPS スキーマを作成します。

SQL Server のスキーマ ファイル

以下の SQL Server スキーマ ファイルが *siteminder_home¥db¥SQL* ディレクトリ内に提供されています。

siteminder_home

ポリシー サーバのインストール パスを指定します。

sm_mssql_ps.sql

ポリシー ストアおよびキー ストア用のスキーマを作成します。

注: 別のデータベース内にキーを格納する場合、このスキーマ ファイルによってそのキー ストア データ用のスキーマが作成されます。

sm_mssql_logs.sql

監査ログのスキーマを作成します。

sm_mssql_ss.sql

セッション ストアのスキーマを作成します。

注: セッション ストア内に **Unicode** 文字を格納する予定がない場合は、このファイルを使用します。

sm_mssql_ss.sql.unicode

SiteMinder セッション ストア用のスキーマを作成します。

注: セッション ストア内に **Unicode** 文字を格納する予定がある場合は、このファイルを使用します。

sm_sampleusers_sqlserver.sql

SiteMinder サンプル ユーザ データベース用のスキーマを作成し、サンプル ユーザをデータベースに読み込みます。

以下の SQL Server スキーマ ファイルが *siteminder_home¥xps¥db* 内に提供されています。

SQLServer.sql

ポリシー ストア用の XPS スキーマを作成します。

PostgreSQL Server のスキーマ ファイル

以下の PostgreSQL スキーマ ファイルが *siteminder_home*¥db¥PostgreSQL ディレクトリ内に提供されています。

siteminder_home

ポリシー サーバのインストール パスを指定します。

sm_postgresql_ps.sql

ポリシー ストアおよびキー ストア用のスキーマを作成します。

注: 別のデータベース内にキーを格納する場合、このスキーマ ファイルによってそのキー ストア データ用のスキーマが作成されます。

sm_postgresql_logs.sql

監査ログのスキーマを作成します。

sm_postgresql_ss.sql

セッション ストアのスキーマを作成します。

注: セッション ストア内に **Unicode** 文字を格納する予定がない場合は、このファイルを使用します。

sm_sampleusers_postgresql.sql

SiteMinder サンプル ユーザ データベース用のスキーマを作成し、サンプル ユーザをデータベースに読み込みます。

以下の PostgreSQL サーバ スキーマ ファイルが *siteminder_home*¥xps¥db 内に提供されています。

PostgreSQL.sql

ポリシー ストア用の **XPS** スキーマを作成します。

Oracle スキーマ ファイル

以下の Oracle スキーマ ファイルが *siteminder_home*¥db¥SQL ディレクトリ内にあります。

siteminder_home

ポリシー サーバのインストール パスを指定します。

sm_oracle_ps.sql

ポリシー ストアおよびキー ストア用のスキーマを作成します。

注: 別のデータベース内にキーを格納する場合、このスキーマ ファイルによってそのキー ストア データ用のスキーマが作成されます。

sm_oracle_logs.sql

監査ログのスキーマを作成します。

sm_oracle_ss.sql

セッション ストアのスキーマを作成します。

sm_sampleusers_oracle.sql

サンプル ユーザ データベース用のスキーマを作成し、サンプル ユーザをデータベースに読み込みます。

以下の Oracle スキーマ ファイルが *policy_server_home*¥xps¥db ディレクトリ内に提供されています。

Oracle.sql

ポリシー ストア用の XPS スキーマを作成します。

MySQL ポリシー ストアの設定

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: セッション情報は個別のデータベースに格納されます。ポリシー ストアを使用してセッション情報を格納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、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。
- **データベース ポート** -- データベースがリスンするポートを特定します。
- **管理者アカウント** -- データベース内でオブジェクトを管理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。

ポリシー ストアを設定する方法

ポリシー ストアの設定を開始する前に、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。

次の手順に従ってください:

1. MySQL が Latin1 または UTF8 文字セットを使用していることを確認します。Unicode 文字をサポートするために、UTF8 文字セットを使用します。
2. ポリシー ストアとして動作している MySQL データベースがポリシー 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、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。
 - Unicode 文字用のデータベース インスタンスを作成するには、UTF8 に対して文字セットおよび照合を使用します。
 - Unicode 文字用のデータベース インスタンスを作成するには、Latin1 に対して文字セットおよび照合を使用します。
4. SiteMinder 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。
 - (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。
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. SiteMinder スーパーユーザ パスワードを設定します。
8. ポリシー ストア データ定義をインポートします。
9. 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。
10. ポリシー サーバを再起動します。
11. 管理 UI 登録の準備をします。

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。

次の手順に従ってください:

1. クエリ ブラウザを起動し、ポリシー サーバ データベースの管理者としてログインします。
2. [データベース] リストからデータベース インスタンスを選択します。
3. 以下の場所に移動します。

`siteminder_home¥db¥tier2¥MySQL.`

`siteminder_home`

ポリシー サーバのインストール パスを指定します。

4. テキスト エディタで以下のファイルのいずれかを開きます。
 - ポリシー ストアに Unicode 文字を格納するには、`sm_mysql_ps.sql.unicode` を開きます。
 - ポリシー ストアに Unicode 以外の文字を格納するには、`sm_mysql_ps.sql` を開きます。
5. `sm_mysql_ps` ファイルで以下の行を見つけます。

```
DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$  
CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
```

6. 'databaseName' の各インスタンスをポリシー ストアとして機能するデータベースの名前に置換します。
7. databaseName インスタンスを置換した後、ファイル全体の内容をコピーします。
8. 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 スキーマがデータベースに追加されます。
9. 以下の場所に移動します。

`siteminder_home¥xps¥db¥Tier2DirSupport¥MySQL`

10. テキスト エディタで以下のファイルのいずれかを開き、ファイル全体の内容をコピーします。
 - ポリシー ストアに Unicode 文字を格納するには、MySQL.sql.unicode を開きます。
 - ポリシー ストアに Unicode 以外の文字を格納するには、MySQL.sql を開きます。

11. 適切な MySQL ファイルからスキーマをクエリに貼り付けて、クエリを実行します。

ポリシー ストア スキーマが拡張されます。

12. 監査ログ データベースとしてポリシー ストアを使用するには、手順 3 および 4 を繰り返しますが、以下のログ記録スキーマ ファイルを使用します。

`sm_mysql_logs.sql`

データベースに SiteMinder データを格納できます。

注: ほかの SiteMinder データを格納するためにポリシー ストアを設定する必要はありません。別の監査ログ データベース、キー ストア、セッション ストアとして機能するよう個別のデータベースを設定することができます。

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。

注: MySQL 5.1.x を使用している場合は、DSN を作成するために使用するユーザ名に TRIGGER 権限が割り当てられていることを確認します。

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。

以下の手順に従います。

1. ポリシー サーバ ホスト システムにログインします。
2. 以下のいずれかを実行します。
 - サポートされた 32 ビットの Windows オペレーティング システムを使用している場合は、[スタート] をクリックし、[プログラム] - [管理ツール] - [ODBC データ ソース] を選択します。
 - サポートされる 64 ビットの Windows オペレーティング システムを使用している場合：
 - a. `install_home¥Windows¥SysWOW64` に移動します。
 - b. `odbcad32.exe` をダブルクリックします。[ODBC データ ソース アドミニストレータ] が表示されます。
3. [システム DSN] をクリックします。
4. [追加] をクリックします。
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。
6. [全般] タブで以下の手順を行います。
 - 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。
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にカスタマイズする必要があります。また、このファイルには他のデータ ソースを追加できます。たとえば、SiteMinder 用の他の 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: データベースをポリシー ストアとして設定する場合、データ ソースエントリの最初の行の値が必要です。

`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] セクションの新しいデータ ソース名。
- 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。

新しいサービス名を作成する場合は、`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あります。

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`
- `postgresqlwire.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。

以下の手順に従います。

1. `system_odbc.ini` ファイルを開きます。
2. **[ODBC Data Sources]** の下に、以下の行を入力します。
SiteMinder Data Source=DataDirect 7.1 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/NSmysql27.so
Description=DataDirect 7.1 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、ポンド記号 (#) を使用しないでください。ポンド記号 (#) 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。

次の手順に従ってください:

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。
2. ストレージ リストから以下の値を選択します。

ODBC

3. データベース リストから以下の値を選択します。

ポリシー ストア

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] をクリックして設定を保存します。

8. データベース リストから以下の値を選択します。

キーストア

9. ストレージ リストから以下の値を選択します。

ODBC

10. 以下のオプションを選択します。

ポリシー ストア データベースの使用

11. データベース リストから以下の値を選択します。

監査ログ

12. ストレージ リストから以下の値を選択します。

ODBC

13. 以下のオプションを選択します。

ポリシー ストア データベースの使用

14. [適用] をクリックして設定を保存します。

15. (オプション) [接続のテスト] をクリックしてポリシー サーバがポリシー ストアにアクセスできることを確認します。

16. [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次のとおりです。

`siteminder`

このアカウントは最大の権限を持っています。

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。

- 管理 UI に初めてアクセスする場合。
- 初めて SiteMinder ユーティリティを管理する場合。
- スーパーユーザ権限で別の管理者を作成する場合。

次の手順に従ってください:

1. `smreg` ユーティリティを `siteminder_home\bin` にコピーします。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

注: このユーティリティは、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。

2. 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、引用符でパスワードを囲みます。

注: Oracle ポリシー ストアを設定している場合、パスワードは大文字と小文字を区別します。他のすべてのポリシー ストアの場合は、パスワードの大文字と小文字を区別しません。

3. *siteminder_home*¥bin から *smreg* 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。

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 データ定義をインポートすると、ポリシー ストアで作成および格納できるオブジェクトのタイプが定義されます。

次の手順に従ってください:

1. コマンド ウィンドウを開き、*siteminder_home*¥xps¥dd 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. 以下のコマンドを実行します。

```
XPSDDInstall SmMaster.xdd
```

```
XPSDDInstall
```

必要なデータ定義をインポートします。

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 とポリシー サーバで使用するポリシー ストアが設定されます。

以下の点を考慮します。

- 必ず *siteminder_home*¥bin への書き込みアクセス権があることを確認してください。インポートユーティリティは、ポリシー ストア オブジェクトをインポートするためにこの権限を必要とします。

siteminder_home

ポリシー サーバのインストールパスを指定します。

- 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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン 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。

次の手順に従ってください:

1. コマンド ウィンドウを開き、`siteminder_home¥db` に移動します。
2. 以下のファイルのいずれかをインポートします。

- `smpolicy.xml` をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy.xml -npass
```

- `smpolicy-secure.xml` をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy-secure.xml -npass
```

```
npass
```

パスフレーズが必要ではないことを指定します。デフォルトポリシー ストア オブジェクトには暗号化されたデータが含まれていません。

両方のファイルに、デフォルトのポリシー ストア オブジェクトが含まれています。これらのオブジェクトにはデフォルトのエージェント設定オブジェクト (ACO) テンプレート内のデフォルトセキュリティ設定が含まれます。`smpolicy-secure` ファイルはより制限の厳しいセキュリティ設定を提供します。詳細については、「[デフォルトのポリシー ストア オブジェクトの考慮事項 \(P. 104\)](#)」を参照してください。

- **Option Pack** 機能をインポートするには、以下のコマンドを実行します。

```
XPSImport ampolicy.xml -npass
```

- フェデレーション機能をインポートするには、以下のコマンドを実行します。

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

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。

注: `smpolicy.xml` をインポートすると、**SiteMinder** から別個にライセンスが付与される レガシー フェデレーション および **Web** サービスの変数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。

Advanced Authentication Server の有効化

ユーザのポリシー サーバの設定の一部として、Advanced Authentication Server を有効にします。

次の手順に従ってください:

1. ポリシー サーバ設定ウィザードを実行します。
2. ウィザードの最初の画面にあるチェックボックスをすべてオフのままにします。
3. [次へ] をクリックします。
4. Advanced Authentication Server 用のマスタ暗号化キーを作成します。
注: 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。
5. ポリシー サーバ設定ウィザードの残りの手順を完了します。

Advanced Authentication Server が有効になります。

ポリシー サーバの再起動

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、`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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

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。

以下の点を考慮します。

- 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の手順を実行します。
- (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](#) (P. 598) します。

次の手順に従ってください:

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： 15

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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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 サーバに管理者認証情報を提供します。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認証情報を使用します。

SQL Server ポリシー ストアの設定

1 つの SQL Server データベースは以下として機能させることができます。

- ポリシー ストア
- キー ストア
- ログ データベース

注: 個別のデータベースに SiteMinder セッション情報を格納します。ポリシー ストアを使用してセッション情報を格納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。

以下の点を考慮します。

- SQL Server ポリシー ストアを手動で設定するか、またはポリシー サーバ インストーラを使用してポリシー ストアを自動的に設定することができます。
- データベースは Windows システムにインストールされている必要があります。また、SiteMinder スキーマ ファイルはポリシー サーバと共にインストールされます。ポリシー サーバが UNIX システムにインストールされている場合、*policy_server_home/db/SQL* ディレクトリにあるスキーマ ファイルを、Windows システム上の一時ディレクトリにコピーします。

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に単一の SQL 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。

注：(W) が前に付いた情報は、ポリシー サーバが Windows システムにインストールされる場合にのみ必要です。(U) が付いた情報は、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必要です。SQL Server データ ソースを設定する場合には、別の情報が必要です。

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。値を記録するために SQL Server 情報のワークシートを使用できます。

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を決定します。

管理アカウントの名前とパスワード

データベース内のオブジェクトに対して作成、読み取り、変更、削除の権限があるアカウントのユーザ名とパスワードを決定します。

(W) データソース名

データ ソースの識別に使用する名前を決定します。

例：SM SQL Server Wire DS.

(W)SQL Server 名

ポリシー ストアとして機能するインスタンスを含む SQL Server データベースの名前を決定します。

(U)ポリシー サーバルート

ポリシー サーバがインストールされる場所への明確なパスを指定します。

(U)IP アドレス

SQL Server データベースの IP アドレスを指定します。

ポリシー ストアを設定する方法

ポリシー ストアとして SQL 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一部でこの情報が必要となります。

1. SiteMinder データを含んでいる SQL Server データベース インスタンスが、ポリシー サーバシステムからアクセス可能であることを確認してください。
2. SQL Server エンタープライズ マネージャを使用して、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。

例 :

`smdatastore`

3. SiteMinder スキーマを作成します。
4. SiteMinder 用の SQL Server データ ソースを設定します。
 - (Windows) SQL Server データ ソースを作成します。
 - (UNIX) UNIX システム上に SQL Server データ ソースを作成します。
 - (UNIX) SQL Server ワイヤ プロトコル ドライバを設定します。
5. 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。
6. SiteMinder スーパーユーザ パスワードを設定します。
7. ポリシー ストア データ定義をインポートします。
8. デフォルトの SiteMinder オブジェクトをインポートします。

9. ポリシー サーバを再起動します。
10. 管理 UI 登録の準備をします。

SiteMinder スキーマの作成

SQL Server データベースにポリシー、キー、および監査ログ情報を格納できるように、SiteMinder スキーマを作成します。

ポリシー ストアおよび監査ログ スキーマ ファイルを実行すると、以下の警告が表示されます。この警告はポリシー ストア設定に影響しません。

- 警告：テーブル 'smvariable5' が作成されましたが、その最大行サイズ（8746）が 1 行あたりの最大バイト数（8060）を超えています。このテーブルで INSERT または UPDATE を実行しても、行が 8060 バイトを超える場合は失敗します。
- 警告：テーブル 'smodbcquery4' が作成されましたが、その最大行サイズ（64635）が 1 行あたりの最大バイト数（8060）を超えています。このテーブルで INSERT または UPDATE を実行しても、行が 8060 バイトを超える場合は失敗します。
- 警告：テーブル 'smaccesslog4' が作成されましたが、その最大行サイズ（9668）が 1 行あたりの最大バイト数（8060）を超えています。このテーブルで INSERT または UPDATE を実行しても、行が 8060 バイトを超える場合は失敗します。

以下の手順に従います。

1. クエリ アナライザを起動し、ポリシー サーバ データベースの管理者としてログインします。
2. [データベース] リストからデータベース インスタンスを選択します。
3. テキスト エディタで sm_mssql_ps.sql を開き、ファイル全体の内容をコピーします。
4. sm_mssql_ps.sql からスキーマをクエリに貼り付け、クエリを実行します。
ポリシーおよびキー ストア スキーマがデータベースに追加されます。
5. テキスト エディタで SQLServer.sql を開き、ファイル全体の内容をコピーします。

6. `SQLServer.sql` からクエリにスキーマを貼り付け、クエリを実行します。
ポリシー ストア スキーマが拡張されます。
7. ポリシー ストアを監査ログ データベースとして使用するため手順 3 と 4 を繰り返します。以下のスキーマ ファイルを使用します。

`sm_mssql_logs.sql`

注: ほかの SiteMinder データを格納するためにポリシー ストアを設定する必要はありません。別の監査ログ データベース、キー ストア、セッション ストアとして機能するよう個別のデータベースを設定することができます。

データベースに SiteMinder データを格納できます。

SiteMinder 用の SQL Server データ ソースを設定する

ODBC を使用している場合、SiteMinder が SiteMinder データ ストアと通信できるようデータ ソースを設定する必要があります。

詳細情報:

[SQL Server 認証モードの考慮事項 \(P. 342\)](#)

SQL Server 認証モードの考慮事項

SiteMinder データ ソースは Windows 認証をサポートしません。データベースに格納されるユーザのクレデンシャルで SiteMinder データ ソースを設定します。

注: SQL 認証モードの詳細については、ベンダー固有のドキュメントを参照してください。

Windows システムでの SQL Server データ ソースの作成

ODBC は、SQL Server ワイヤ プロトコル用にデータ ソースを設定することが必要です。

注: この手順は、ポリシー サーバを Windows システムにインストールする場合のみを対象としています。

以下の手順に従います。

1. 以下のいずれかの操作を実行します。
 - サポートされた 32 ビットの Windows オペレーティング システムを使用している場合は、[スタート] をクリックし、[プログラム] - [管理ツール] - [ODBC データ ソース] を選択します。
 - サポートされた 64 ビットの Windows オペレーティング システムを使用している場合：
 - a. C:\Windows\SysWOW64 に移動します。
 - b. odbcad32.exe をダブルクリックします。[ODBC データ ソース アドミニストレータ] が表示されます。
2. [システム DSN] タブをクリックします。
システム データ ソース設定が表示されます。
3. [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。
4. SiteMinder SQL Server Wire Protocol を選択し、[完了] をクリックします。

ODBC SQL Server 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。
5. [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 Data Source
注： 指定したデータ ソース名を書き留めます。この情報は、ポリシー ストアとしてデータベースを設定するときに必要です。
6. [サーバ] フィールドに SQL Server ホスト システムの名前を入力します。
7. [データベース名] フィールドにデータベース名を入力します。
8. [テスト] をクリックします。
接続設定がテストされ、接続に成功したことを示すメッセージが表示されます。
9. [OK] をクリックします。
SQL Server データ ソースが設定され、[システム データ ソース] リストに表示されます。

UNIX システムでの SQL Server 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_installation/db` にある `sqlserverwire.ini` の名前を `system_odbc.ini` に変更することによって作成します。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に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である [SiteMinder Data Source] を変更する場合、変更内容を書き留めておきます。この値は、ODBC データベースをポリシー ストアとして設定するときに必要なになります。

`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、このデータ ソースが SiteMinder によって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。

MS SQL Server データ ソースを追加する場合は、ファイルの [ODBC Data Sources] セクションに新しいデータ ソース名を追加し、データ ソースと同じ名前を使用してデータ ソースを記述するセクションを追加する必要があります。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 Oracle または SQL ドライバのエントリがあります。

MS SQL Server データ ソースを設定するには、最初に `policy_server_installation/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。このためには、`policy_server_installation/db` にある `sqlserverwire.ini` の名前を `system_odbc.ini` に変更する必要があります。

SQL Server ワイヤ プロトコル ドライバの設定

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
- postgresqlwire.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。

以下の手順に従います。

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 7.1 SQL Server 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/NSsqls27.so

Description=DataDirect 7.1 SQL Server Wire Protocol

Database=SiteMinder Data

Address=myhost, 1433

QuotedId=No

AnsiNPW=No

注: データ ソース情報を編集する場合は、ポンド記号 (#) を使用しないでください。ポンド記号 (#) 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

環境変数を持ったパスではなく、ポリシー サーバインストールの明確なパスを指定します。

例: export/smuser/siteminder

SiteMinder Data

SQL Server データベースのインスタンス名を指定します。

myhost

SQL Server データベースの IP アドレスを指定します。

1433

SQL Server 用のデフォルトのリスン ポートを表します。

4. 任意の SiteMinder ストアとして機能するために Microsoft SQL Server 2008 を使用している場合は、以下のように [ODBC] セクションを編集します。

TraceFile=nete_ps_root/db/odbctrace.out

TraceDll=nete_ps_root/odbc/lib/NStrc27.so

InstallDir=nete_ps_root/odbc

nete_ps_root

ポリシー サーバインストール ディレクトリに明確なパスを指定します。このパスには環境変数を含めることができません。

5. 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。

次の手順に従ってください:

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。
2. ストレージ リストから以下の値を選択します。
ODBC
3. データベース リストから以下の値を選択します。
ポリシー ストア
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] をクリックして設定を保存します。
8. データベース リストから以下の値を選択します。
キーストア
9. ストレージ リストから以下の値を選択します。
ODBC

10. 以下のオプションを選択します。

ポリシー ストア データベースの使用

11. データベース リストから以下の値を選択します。

監査ログ

12. ストレージ リストから以下の値を選択します。

ODBC

13. 以下のオプションを選択します。

ポリシー ストア データベースの使用

14. [適用] をクリックして設定を保存します。

15. (オプション) [接続のテスト] をクリックしてポリシー サーバがポリシー ストアにアクセスできることを確認します。

16. [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次のとおりです。

siteminder

このアカウントは最大の権限を持っています。

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。

- 管理 UI に初めてアクセスする場合。
- 初めて SiteMinder ユーティリティを管理する場合。
- スーパーユーザ権限で別の管理者を作成する場合。

次の手順に従ってください:

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

siteminder_home

ポリシー サーバのインストール パスを指定します。

注: このユーティリティは、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。

2. 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、引用符でパスワードを囲みます。

注: Oracle ポリシー ストアを設定している場合、パスワードは大文字と小文字を区別します。他のすべてのポリシー ストアの場合は、パスワードの大文字と小文字を区別しません。

3. *siteminder_home*¥bin から smreg 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。

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 データ定義をインポートすると、ポリシー ストアで作成および格納できるオブジェクトのタイプが定義されます。

次の手順に従ってください:

1. コマンド ウィンドウを開き、*siteminder_home*¥xps¥dd 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. 以下のコマンドを実行します。

```
XPSDDInstall SmMaster.xdd
```

```
XPSDDInstall
```

必要なデータ定義をインポートします。

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 とポリシー サーバで使用するポリシー ストアが設定されます。

以下の点を考慮します。

- 必ず *siteminder_home*¥bin への書き込みアクセス権があることを確認してください。インポートユーティリティは、ポリシー ストア オブジェクトをインポートするためにこの権限を必要とします。

siteminder_home

ポリシー サーバのインストールパスを指定します。

- 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する前に、管理者権限でコマンドラインウィンドウを開きます。アカウントに管理者権限がある場合でも、このように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。

次の手順に従ってください:

1. コマンド ウィンドウを開き、*siteminder_home¥db* に移動します。
2. 以下のファイルのいずれかをインポートします。

- *smpolicy.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy.xml -npass
```

- *smpolicy-secure.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy-secure.xml -npass
```

```
npass
```

パスフレーズが必要ではないことを指定します。デフォルトポリシー ストア オブジェクトには暗号化されたデータが含まれていません。

両方のファイルに、デフォルトのポリシー ストア オブジェクトが含まれています。これらのオブジェクトにはデフォルトのエージェント設定オブジェクト (ACO) テンプレート内のデフォルトセキュリティ設定が含まれます。 *smpolicy-secure* ファイルはより制限の厳しいセキュリティ設定を提供します。詳細については、「[デフォルトのポリシー ストア オブジェクトの考慮事項 \(P. 104\)](#)」を参照してください。

- Option Pack 機能をインポートするには、以下のコマンドを実行します。

```
XPSImport ampolicy.xml -npass
```

- フェデレーション機能をインポートするには、以下のコマンドを実行します。

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

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。

注: *smpolicy.xml* をインポートすると、SiteMinder から別個にライセンスが付与される レガシー フェデレーション および Web サービスの変数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。

Advanced Authentication Server の有効化

ユーザのポリシー サーバの設定の一部として、Advanced Authentication Server を有効にします。

次の手順に従ってください:

1. ポリシー サーバ設定ウィザードを実行します。
2. ウィザードの最初の画面にあるチェックボックスをすべてオフのままにします。
3. [次へ] をクリックします。
4. Advanced Authentication Server 用のマスタ暗号化キーを作成します。
注: 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。
5. ポリシー サーバ設定ウィザードの残りの手順を完了します。

Advanced Authentication Server が有効になります。

ポリシー サーバの再起動

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、`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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

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。

以下の点を考慮します。

- 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の手順を実行します。
- (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](#) (P. 598) します。

次の手順に従ってください:

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： 15

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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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

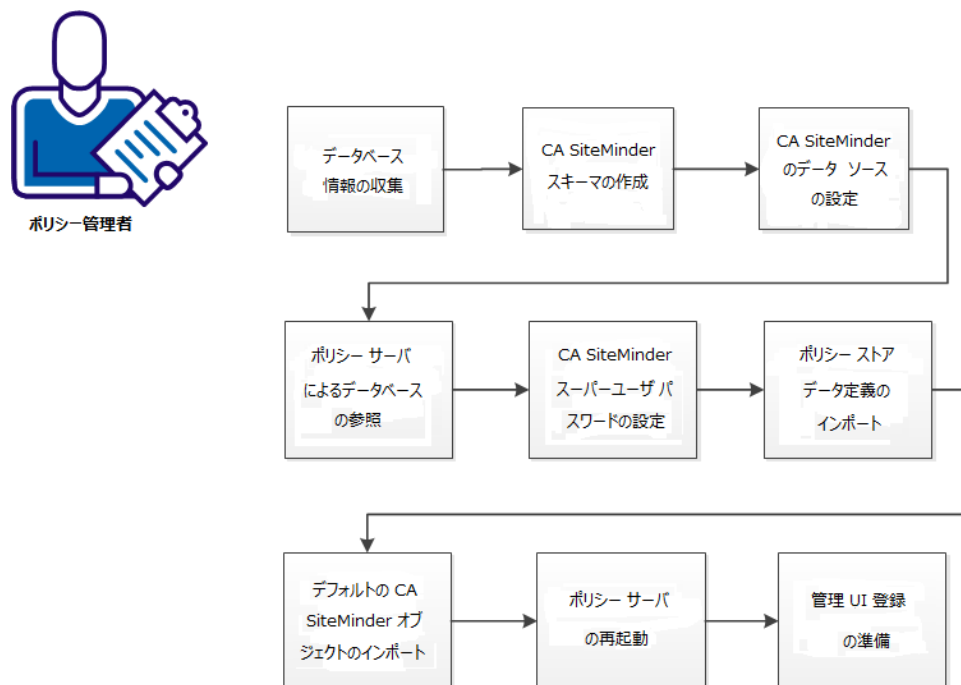
(任意) 詳細レベルを **FATAL** に設定します。

3. Enter キーを押します。

XPSRegClient は、ポリシー サーバに管理者認証情報を提供します。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認証情報を使用します。

PostgreSQL サーバポリシー ストアを設定する方法

以下の図では、PostgreSQL サーバデータベースをポリシー ストアとして設定するプロセスを示します。



前提条件

- SiteMinder データを含んでいる PostgreSQL データベース インスタンスが、ポリシー サーバシステムからアクセス可能であることを確認してください。
- 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。

例：

smdatastore

次の手順に従ってください：

1. PostgreSQL データベース情報を収集します。
2. SiteMinder スキーマを作成します。

3. SiteMinder 用の PostgreSQL データ ソースを設定します。
 - (Windows) PostgrSQL データ ソースを作成します。
 - (UNIX) UNIX システム上に PostgreSQL データ ソースを作成します。
 - (UNIX) PostgreSQL ワイヤ プロトコル ドライバを設定します。
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. ポリシー ストア データ定義をインポートします。
7. デフォルトの SiteMinder オブジェクト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 登録の準備をします。

PostgreSQL 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に単一の PostgreSQL サーバ 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 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を決定します。

管理アカウントの名前とパスワード

データベース内のオブジェクトに対して作成、読み取り、変更、削除の権限があるアカウントのユーザ名とパスワードを決定します。

データソース名

データ ソースの識別に使用する名前を決定します。

例：SM PostgreSQL Server Wire DS.

PostgreSQL サーバ名

ポリシー ストアとして機能するインスタンスを含む PostgreSQL サーバ データベースの名前を決定します。

ポリシー サーバルート

ポリシー サーバがインストールされる場所への明確なパスを指定します。

IP アドレス

PostgreSQL サーバ データベースの IP アドレスを指定します。

PostgreSQL 用の SiteMinder スキーマの作成

SQL Server データベースにポリシー、キー、セッション、および監査ログ情報を格納できるように、SiteMinder スキーマを作成します。

次の手順に従ってください:

1. PostgreSQL クライアントを起動し、ポリシー サーバ データベースの管理者としてログインします。
2. [データベース] リストからデータベース インスタンスを選択します。
3. テキスト エディタで *policy_server_home/db/SQL/sm_postgresql_ps.sql* を開き、ファイル全体の内容をコピーします。
4. *sm_postgresql_ps.sql* からスキーマをクエリに貼り付け、クエリを実行します。

ポリシーおよびキー ストア スキーマがデータベースに追加されます。

5. テキスト エディタで *policy_server_home/xps/db/PostgreSQL.sql* を開き、ファイル全体の内容をコピーします。
6. *PostgreSQL.sql* からクエリにスキーマを貼り付け、クエリを実行します。
ポリシー ストア スキーマが拡張されます。
7. ポリシー ストアを監査ログ データベースとして使用するため手順 3 と 4 を繰り返します。以下のスキーマ ファイルを使用します。

sm_postgresql_logs.sql

注: ほかの SiteMinder データを格納するためにポリシー ストアを設定する必要はありません。別の監査ログ データベース、キー ストア、セッション ストアとして機能するよう個別のデータベースを設定することができます。

データベースに SiteMinder データを格納できます。

Windows での PostgreSQL データソースの作成

ODBC は、SQL Server ワイヤ プロトコル用にデータ ソースを設定することが必要です。

次の手順に従ってください:

1. 以下のいずれかの操作を実行します。
 - サポートされた 32 ビットの Windows オペレーティングシステムを使用している場合は、[スタート] をクリックし、[プログラム] - [管理ツール] - [ODBC データ ソース] を選択します。
 - サポートされる 64 ビットの Windows オペレーティングシステムを使用している場合：
 - a. C:\Windows\SysWOW64 に移動します。
 - b. odbcad32.exe をダブルクリックします。[ODBC データ ソース アドミニストレータ] が表示されます。
2. [システム DSN] タブをクリックします。
3. [追加] をクリックします。
4. SiteMinder PostgreSQL Server Wire Protocol を選択し、[完了] をクリックします。
5. [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 Data Source

注: 指定したデータ ソース名を書き留めます。この情報は、ポリシー ストアとしてデータベースを設定するときに必要です。

6. [サーバ] フィールドに PostgreSQL ホスト システムの名前を入力します。
7. [データベース名] フィールドにデータベース名を入力します。

8. [テスト] をクリックします。

接続設定がテストされ、接続に成功したことを示すメッセージが表示されます。

9. [OK] をクリックします。

PostgreSQL データ ソースが設定され、[システム データ ソース] リストに表示されます。

UNIX での PostgreSQL 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_installation/db`にある `postgresqlwire.ini` の名前を `system_odbc.ini` に変更することによって作成します。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に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である [SiteMinder Data Source] を変更する場合、変更内容を書き留めておきます。この値は、ODBC データベースをポリシー ストアとして設定するときに使用します。

`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 によって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。

PostgreSQL サーバ データ ソースを追加する場合は、ファイルの [ODBC Data Sources] セクションに新しいデータ ソース名を追加すること、データ ソースと同じ名前を使用して、データ ソースを記述するセクションを追加することが必要になります。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 Oracle または SQL ドライバのエントリがあります。

PostgreSQL Server ワイヤ プロトコル ドライバの設定

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
- postgresqlwire.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。

次の手順に従ってください:

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。
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。

SiteMinder Data Source=DataDirect 7.1 PostgreSQL Server Wire Protocol

Driver=*nete_ps_root*/odbc/lib/NSpsql27.so
 Description=DataDirect 7.1 PostgreSQL Server Wire Protocol
 Database=*SiteMinder Data*
 Address=*myhost*, 1433
 QuotedId=No
 AnsiNPW=No

注: データソース情報を編集する場合は、ポンド記号 (#) を使用しないでください。ポンド記号 (#) 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

環境変数を持ったパスではなく、ポリシー サーバインストールの明確なパスを指定します。

例: `export/smuser/siteminder`

SiteMinder Data

PostgreSQL Server データベースのインスタンス名を指定します。

myhost

PostgreSQL Server データベースの IP アドレスを指定します。

1433

PostgreSQL Server 用のデフォルトのリスンポートを表します。

4. 以下のように [ODBC] セクションを編集します。

TraceFile=*nete_ps_root*/db/odbctrace.out
 TraceDll=*nete_ps_root*/odbc/lib/NStrc27.so
 InstallDir=*nete_ps_root*/odbc

nete_ps_root

ポリシー サーバインストールディレクトリに明確なパスを指定します。このパスには環境変数を含めることができません。

5. 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。

次の手順に従ってください:

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。
2. ストレージリストから以下の値を選択します。
ODBC
3. データベース リストから以下の値を選択します。
ポリシー ストア
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] をクリックして設定を保存します。
8. データベース リストから以下の値を選択します。
キーストア
9. ストレージリストから以下の値を選択します。
ODBC
10. 以下のオプションを選択します。
ポリシー ストア データベースの使用

11. データベース リストから以下の値を選択します。

監査ログ

12. ストレージ リストから以下の値を選択します。

ODBC

13. 以下のオプションを選択します。

ポリシー ストア データベースの使用

14. [適用] をクリックして設定を保存します。

15. (オプション) [接続のテスト] をクリックしてポリシー サーバがポリシー ストアにアクセスできることを確認します。

16. [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次のとおりです。

siteminder

このアカウントは最大の権限を持っています。

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。

- 管理 UI に初めてアクセスする場合。
- 初めて SiteMinder ユーティリティを管理する場合。
- スーパーユーザ権限で別の管理者を作成する場合。

次の手順に従ってください:

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

siteminder_home

ポリシー サーバのインストールパスを指定します。

注: このユーティリティは、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。

2. 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、引用符でパスワードを囲みます。

注: Oracle ポリシー ストアを設定している場合、パスワードは大文字と小文字を区別します。他のすべてのポリシー ストアの場合は、パスワードの大文字と小文字を区別しません。

3. `siteminder_home\bin` から `smreg` 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。

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 データ定義をインポートすると、ポリシー ストアで作成および格納できるオブジェクトのタイプが定義されます。

次の手順に従ってください：

1. コマンドウィンドウを開き、`siteminder_home\bin` 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. 以下のコマンドを実行します。

```
XPSDDInstall SmMaster.xdd
```

```
XPSDDInstall
```

必要なデータ定義をインポートします。

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 とポリシー サーバで使用するポリシー ストアが設定されます。

以下の点を考慮します。

- 必ず *siteminder_home*¥bin への書き込みアクセス権があることを確認してください。インポートユーティリティは、ポリシー ストア オブジェクトをインポートするためにこの権限を必要とします。

siteminder_home

ポリシー サーバのインストールパスを指定します。

- 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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン 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。

次の手順に従ってください:

1. コマンド ウィンドウを開き、`siteminder_home¥db` に移動します。
2. 以下のファイルのいずれかをインポートします。

- `smpolicy.xml` をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy.xml -npass
```

- `smpolicy-secure.xml` をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy-secure.xml -npass
```

```
npass
```

パスフレーズが必要ではないことを指定します。デフォルトポリシー ストア オブジェクトには暗号化されたデータが含まれていません。

両方のファイルに、デフォルトのポリシー ストア オブジェクトが含まれています。これらのオブジェクトにはデフォルトのエージェント設定オブジェクト (ACO) テンプレート内のデフォルトセキュリティ設定が含まれます。 `smpolicy-secure` ファイルはより制限の厳しいセキュリティ設定を提供します。詳細については、「[デフォルトのポリシー ストア オブジェクトの考慮事項 \(P. 104\)](#)」を参照してください。

- **Option Pack** 機能をインポートするには、以下のコマンドを実行します。

```
XPSImport ampolicy.xml -npass
```

- フェデレーション機能をインポートするには、以下のコマンドを実行します。

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

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。

注: `smpolicy.xml` をインポートすると、**SiteMinder** から別個にライセンスが付与される レガシー フェデレーション および **Web** サービスの変数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。

Advanced Authentication Server の有効化

ユーザのポリシー サーバの設定の一部として、Advanced Authentication Server を有効にします。

次の手順に従ってください:

1. ポリシー サーバ設定ウィザードを実行します。
2. ウィザードの最初の画面にあるチェックボックスをすべてオフのままにします。
3. [次へ] をクリックします。

4. Advanced Authentication Server 用のマスタ暗号化キーを作成します。

注: 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。

5. ポリシー サーバ設定ウィザードの残りの手順を完了します。

Advanced Authentication Server が有効になります。

ポリシー サーバの再起動

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、`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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

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。

以下の点を考慮します。

- 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の手順を実行します。
- (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](#) (P. 598) します。

次の手順に従ってください:

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： 15

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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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 サーバに管理者認証情報を提供します。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認証情報を使用します。

Oracle ポリシー ストアの設定

1 つの Oracle のデータベースは以下として機能させることができます。

- ポリシー ストア
- キー ストア
- ログ データベース

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。

Oracle ポリシー ストアを手動で設定するか、またはポリシー サーバインストーラを使用してポリシー ストアを自動的に設定することができます。

Oracle 10 g データベースに対する前提条件

Oracle 10g データベースをインストールした後、以下の前提条件を完了します。

- ポリシー ストア用の表領域の作成
- データベース内のこの表領域を管理するための適切な権限を持ったユーザの作成

ポリシー ストア用の Oracle 10 g 表領域の作成

ポリシー ストア用の表領域の作成は、Oracle 10 g データベースのみの前提条件です。

次の手順に従ってください：

1. Oracle Enterprise Manager 10g Database Control で、Oracle データベースを管理するための適切な権限を持つ SYSDBA ユーザとしてログインします。
2. Oracle のグローバル データベースの設定画面で、[Administration] - [Tablespaces] を選択します。
3. [Tablespaces] 画面で、[Create] をクリックします。
4. [Create Tablespaces] 画面で、表領域名を入力し、[ADD] をクリックします。

例：/NETE_TB

5. [Create Tablespaces: Add Datafile] 画面で、次の操作を実行します。
 - a. ファイル名を入力します。
例：/NETE_TB
 - b. ファイルサイズを指定します。
例：100 MB
 - c. [続行] をクリックします。

表領域が作成され、[Tablespaces] 画面に表示されます。

ポリシー ストア用の表領域を管理するユーザを作成することにより、前提条件を完了します。

詳細情報:

[ポリシー ストアの表領域を管理する Oracle 10 g ユーザの作成 \(P. 374\)](#)

ポリシー ストアの表領域を管理する Oracle 10 g ユーザの作成

ポリシー ストア用の表領域を管理するユーザを作成することは、Oracle 10 g データベースのみの前提条件です。

次の手順に従ってください:

1. Oracle のグローバル データベースの設定画面で、[Administration] - [Users] を選択します。
2. [Create Tablespaces] 画面で、[Create] をクリックします。
3. [Create User] 画面で、以下を入力します。
 - ユーザの名前。
例: NETE
 - ユーザのパスワード。
 - 作成したデフォルトの表領域
 - 一時表領域。
例: TEMP
4. [Roles] をクリックします。
5. [Modify] を選択します。
6. [Modify Roles] 画面で、以下の操作を実行します。
 - a. CONNECT と RESOURCE をこのユーザのロールとして選択します。
 - b. [適用] をクリックします。
7. 以下を入力することで、コマンド ウィンドウで sqlplus を起動します。
 - a. sqlplus
 - b. [Create User] 画面上で作成されたポリシー ストア ユーザのクレデンシャル。

Oracle 10 g データベース用の前提条件を完了しました。データベース用の SiteMinder データ ストアを設定できるようになりました。

Oracle 12c データベースに対する前提条件

Oracle 12c データベースをインストールした後に、以下の手順を実行します。

1. ポリシー ストア用のテーブルスペースを作成します。
2. データベース内のテーブルスペースを管理するための以下の権限を持つユーザを作成します。
 - Connect
 - Resource
 - Unlimited Tablespace

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に単一の Oracle 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。

(U) が前に付いた情報は、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必要な情報です。 この情報は、UNIX に対して Oracle データ ソースを設定する場合に必要です。

必要な情報

サポートされている Oracle または Oracle RAC データベースをポリシー ストアまたは他のタイプの SiteMinder データ ストアとして設定する前に、以下の特定の必須情報を収集します。

- (U) ポリシー サーバのインストールパス - ポリシー サーバがインストールされている場所への明示的なパスを指定します。
- データ ソース - Oracle データ ソースの識別に使用する名前を決定します。

例 : SM Oracle Server Wire DS

- **データベース管理アカウント** - データベース内のオブジェクトを作成、読み取り、変更、および削除する権限があるアカウントのユーザ名を決定します。

注: 管理アカウントに DB ロールがないことを確認します。管理アカウントに DB ロールがある場合、監査を基にしたレポートで正しい結果が返されません。

- **データベース管理パスワード** - 管理アカウントのパスワードを決定します。

Oracle データベースの情報

以下の情報は、ポリシー ストアまたは他のタイプの SiteMinder データ ストアとしてサポートされている Oracle データベースを設定する場合にのみ、収集します。

- **Oracle マシン名** - Oracle データベースがインストールされているマシンの名前を決定します。
- **Oracle インスタンスサービス名** - 接続するデータベース インスタンスのサービス名を決定します。tnsnames.ora ファイルはサービス名を指定します。
- **Oracle ポート番号** - Oracle データベースがリスニングするポート番号を決定します。

Oracle RAC データベース(SCAN なし)情報

以下の情報は、ポリシー ストアまたは他の SiteMinder データ ストアとしてサポートされている Oracle RAC データベースを設定する場合にのみ収集します (SCAN 機能の設定なし)。

- **Oracle RAC システム サービス名** - システム全体のサービス名を決定します。

例: 以下の tnsnames.ora ファイルでは、SMDB がシステム全体用のサービス名です。

```
SMDB=
(Description =
  (ADDRESS = PROTOCOL = TCP)(HOST = nete_servername1)(PORT=1521)
  (ADDRESS = PROTOCOL = TCP)(HOST = nete_servername2)(PORT=1521)
  (ADDRESS = PROTOCOL = TCP)(HOST = nete_servername3)(PORT=1521))
  (LOAD_BALANCE = yes)
  (CONNECT_DATA=
    (SERVER = DEDICATED)
    (SERVER_NAME = SMDB))
)
```

- **Oracle RAC ノード サービス名** - システム内の各ノードのサービス名を決定します。
- **Oracle RAC ノード IP アドレス** - Oracle RAC システム内の各ノードの IP アドレスを決定します。

注: Oracle RAC 10g を使用している場合は、システム内の各ノードの仮想 IP アドレスを決定します。

- **Oracle RAC ノード ポート番号** - Oracle RAC システム内の各ノードのポート番号を決定します。

Oracle RAC データベース(SCAN あり)情報

Oracle RAC Single Client Access Name (SCAN) 機能は、クラスタで実行されるあらゆる Oracle データベースにクライアントがアクセスするための単一の名前を指定します。

Oracle RAC データベースを **SCAN** 機能と共にポリシー ストアまたは他の SiteMinder データ ストアとして設定している場合は、以下の情報を収集します。

- **Oracle RAC システム サービス名** - システム全体のサービス名を決定します。

例: 以下の tnsnames.ora ファイルでは、**SMDB** がシステム全体用のサービス名です。

```
SMDB=
(DESCRIPTION =
  (ADDRESS = (PROTOCOL = TCP)(HOST = clus-scan.example.com)(PORT = 1521))
  (CONNECT_DATA =
    (SERVER = DEDICATED)
    (SERVICE_NAME = SMDB)
  )
)
```

- **Oracle RAC SCAN アドレス** -- Oracle RAC システム **SCAN** の **FQDN** を確定します。
- **Oracle RAC SCAN ポート番号** -- Oracle RAC システム **SCAN** 用のポート番号を確定します。

ポリシー ストアを設定する方法

単一の Oracle データベースを、ポリシー ストア、キー ストア、ログ データベースとして設定するには、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一部でこの情報が必要となります。

1. SiteMinder データを含んでいる Oracle データベース インスタンスが、ポリシー サーバ システムからアクセス可能であることを確認してください。tnsping または sqlplus を使用して、通信をテストします。
2. SiteMinder スキーマを作成します。
3. 以下のように、SiteMinder 用の Oracle データ ソースを設定します。
 - (Windows) Windows システムでの Oracle データ ソースの作成
 - (Windows) Windows システムでの Oracle RAC データ ソースの作成
 - (UNIX) UNIX での Oracle データ ソースの作成

- (UNIX) ワイヤプロトコル ドライバの設定
 - (UNIX) Oracle ワイヤプロトコル ドライバの設定
 - (UNIX) Oracle RAC ワイヤプロトコル ドライバの設定
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. ポリシー ストア データ定義をインポートします。
 7. 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。
 8. ポリシー サーバを再起動します。
 9. 管理 UI 登録の準備をします。

SiteMinder スキーマの作成

SiteMinder スキーマを作成して、1 つの Oracle 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。

以下の手順に従います。

1. sqlplus または他の Oracle ユーティリティを使用して、ポリシー サーバ データベース情報を管理するユーザとして Oracle にログインします。

注: SYS ユーザや SYSTEM ユーザで SiteMinder スキーマを作成しないことをお勧めします。必要な場合は、SMOWNER などの Oracle ユーザを作成し、そのユーザでスキーマを作成します。

2. 以下のスクリプトをインポートします。

```
$NETE_PS_ROOT/db/sql/sm_oracle_ps.sql
```

注: 環境変数は Oracle の SQL ユーティリティ内では機能しない場合があります。ユーティリティを使用して、スクリプトをインポートしようとする問題が発生する場合は、明示的なパスを指定します。

ポリシー ストアとキーのストア スキーマがデータベースに追加されます。

3. 以下のスクリプトを実行します。

```
$NETE_PS_ROOT/xps/db/Oracle.sql
```

ポリシー ストア スキーマが拡張されます。

4. ポリシー ストアを監査ログ データベースとして使用するため、以下のスクリプトをインポートします。

`sm_oracle_logs.sql`.

注: ほかの SiteMinder データを格納するためにポリシー ストアを設定する必要はありません。別の監査ログ データベース、キー ストア、セッション ストアとして機能するよう個別のデータベースを設定することができます。

データベースに SiteMinder データを格納できます。

SiteMinder 用の Oracle データソースの設定

ODBC を使用している場合、Oracle 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 での Oracle データソースの作成

Oracle データベース用の ODBC データ ソースを作成します。

次の手順に従ってください:

1. 以下のいずれかを実行します。
 - サポートされた 32 ビットの Windows オペレーティングシステムを使用している場合は、[スタート] をクリックし、[プログラム] - [管理ツール] - [ODBC データ ソース] を選択します。
 - サポートされた 64 ビットの Windows オペレーティングシステムを使用している場合：
 - a. `install_home¥Windows¥SysWOW64` に移動します。
 - b. `odbcad32.exe` をダブルクリックします[ODBC データ ソース アドミニストレータ] が表示されます。
2. システム [システム DSN] タブをクリックし、次に [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。
3. SiteMinder Oracle Wire Protocol を選択し、[完了] をクリックします。
ODBC Oracle 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。 [一般] タブが前面に移動します。

4. [データ ソース名] フィールドにデータ ソースを識別する名前を入力します。

注: この名前を記録しておいてください。このデータ ソース名は、ポリシー サーバに参照データベースを指定するときに必要です。

5. [ホスト名] フィールドに、Oracle データベースがインストールされているマシンの名前を入力します。
6. [ポート番号] フィールドに、マシン上で Oracle データベースがリスニングするポートの番号を入力します。
7. [SID] フィールドに、接続する Oracle インスタンスの名前を入力します。

注: サービス名は `tnsnames.ora` ファイル内で指定されます。SID はデータベース インスタンス用のシステム識別子です。`tnsnames.ora` ファイルは、Oracle インスタンスを識別し、接続するために Oracle が使用するサービス名と詳細が含まれています。

例: `tnsnames.ora` ファイルが Oracle インスタンスの以下のエントリを含んでいる場合、[SID] フィールドに `instance1` を入力します。

```
instance1=
  (Description=
    (Address = (PROTOCOL = TCP)(Host = myhost)(Port=1521))
    (Connect_DATA_ = (SID = SIDofinstance1))
  )
```

8. [テスト接続] をクリックします。

接続設定がテストされ、接続に成功したことを示すメッセージが表示されます。

9. [OK] をクリックします。

Oracle のデータ ソースがワイヤ プロトコル ドライバに対して設定されます。

Windows での Oracle RAC (SCAN なし) データ ソースの作成

SCAN 機能を使用しない Oracle RAC データベース用の ODBC データ ソースを作成します。

次の手順に従ってください:

1. 以下のいずれかを実行します。
 - サポートされた 32 ビットの Windows オペレーティングシステムを使用している場合は、[スタート] をクリックし、[プログラム] - [管理ツール] - [ODBC データ ソース] を選択します。
 - サポートされた 64 ビットの Windows オペレーティングシステムを使用している場合：
 - a. C:\Windows\SysWOW64 に移動します。
 - b. odbcad32.exe をダブルクリックします[ODBC データ ソース アドミニストレータ] が表示されます。
2. システム [システム DSN] タブをクリックし、次に [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。
3. SiteMinder Oracle Wire Protocol を選択し、[完了] をクリックします。

ODBC Oracle 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。 [一般] タブが前面に移動します。
4. [データ ソース名] フィールドにデータ ソースを識別する名前を入力します。

注: この名前を記録しておいてください。 このデータ ソース名は、ポリシー サーバに参照データベースを指定するときに必要です。

5. [ホスト] フィールドに Oracle RAC システム内の最初のノードの IP アドレスを入力します。

Oracle RAC 10g : 仮想 IP アドレスを入力します。

6. [サービス名] フィールドに Oracle RAC システム全体用のサービス名を入力します。

例：以下の `tnsnames.ora` ファイルでは、`SMDB` 値が Oracle RAC システム全体用のサービス名であり、Oracle RAC システムには 3 つのノードが含まれています。

```
SMDB=
  (Description =
    (ADDRESS = (Protocol = TCP)(HOST = nete_servername1)(PORT = 1521))
    (ADDRESS = (Protocol = TCP)(HOST = nete_servername2)(PORT = 1521))
    (ADDRESS = (Protocol = TCP)(HOST = nete_servername3)(PORT = 1521))
    (LOAD_BALANCE = yes)
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = SMDB)
    )
  )
```

7. [フェールオーバー] タブをクリックします。
フェールオーバー設定が表示されます。
8. その環境の残りの Oracle RAC ノードに対するホスト名または仮想 IP アドレス、ポート番号、およびサービス名を代替サーバフィールドに指定します。

注：ServiceName は Oracle RAC システム全体用のサービス名です。

9. プライマリ サーバが接続を受け付けない場合に、他の Oracle ノードに接続フェールオーバーを提供する代替サーバを指定します。エントリは次のような形式で指定する必要があります。

```
(HostName=nete_servername2:PortNumber=1521:ServiceName=nete_servi
cename[,...])
```

10. [LoadBalancing] を選択します。
11. [OK] ボタンをクリックします。

Oracle RAC データ ソースが、Wire Protocol ドライバに対して設定されます。

Windows での Oracle RAC (SCAN あり) データソースの作成

SCAN 機能を使用する Oracle RAC データベース用の ODBC データ ソースを作成します。

次の手順に従ってください:

1. 以下のいずれかを実行します。
 - サポートされた 32 ビットの Windows オペレーティングシステムを使用している場合は、[スタート] をクリックし、[プログラム] - [管理ツール] - [ODBC データ ソース] を選択します。
 - サポートされる 64 ビットの Windows オペレーティングシステムを使用している場合：
 - a. C:\Windows\SysWOW64 に移動します。
 - b. `odbcad32.exe` をダブルクリックします[ODBC データ ソース アドミニストレータ] が表示されます。
2. システム [システム DSN] タブをクリックし、次に [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。
3. CA SiteMinder Oracle Wire Protocol を選択し、[完了] をクリックします。
ODBC Oracle 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。 [一般] タブが前面に移動します。
4. [データ ソース名] フィールドにデータ ソースを識別する名前を入力します。
注: この名前を記録しておいてください。 このデータ ソース名は、ポリシー サーバに参照データベースを指定するときに必要です。
5. [ホスト] フィールドに SCAN の FQDN または IP アドレスを入力します。
6. [ポート番号] フィールドに SCAN のポート番号を入力します。

7. [サービス名] フィールドに Oracle RAC システム全体用のサービス名を入力します。

例：以下の tnsnames.ora ファイルでは、SMDB 値が SCAN を含む Oracle RAC システム全体用のサービス名です。

```
SMDB =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = clus-scan.rac.com)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = ORCL)
    )
  )
```

8. [OK] ボタンをクリックします。

Oracle RAC データ ソースが、Wire Protocol ドライバに対して設定されます。

UNIX システムでの Oracle データソースの作成

使用可能な ODBC データ ソースの名前と、system_odbc.ini ファイルでこれらのデータ ソースと関連付けられる属性を設定します。

system_odbc.ini ファイルを作成する方法

1. policy_server_installation/db に移動します
2. oraclewire.ini という名前を "system_odbc.ini" に変更します。

各サイトの system_odbc.ini ファイルをカスタマイズします。このファイルにはさらにデータ 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、変更を記録しておいてください。この値は、ODBC データベースをポリシー ストアとして設定するのに必要です。

`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。

Oracle データ ソースを追加する方法

1. ファイルの **[ODBC Data Sources]** セクションに新しいデータ ソース名を定義します。
2. 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します。

サービス名を作成するか、別のドライバを使用するには、`system_odbc.ini` ファイルを編集します。 **[SiteMinder Data Source]** の下に **SQL Server** または **Oracle** ドライバのエントリがあります。

Oracle ワイヤ プロトコル ドライバの設定

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`
- `postgreswire.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。

以下の手順に従います。

1. system_odbc.ini ファイルを開きます。
2. 設定するデータ ソースに応じて、以下の情報を使用して適用可能なデータ ソース セクションを編集します。

```
Driver=nete_ps_root/odbc/lib/NSora27.so
Description=DataDirect 7.1 Oracle Wire Protocol
LoginID=uid
Password=pwd
HostName=nete_servername
PortNumber=1521
SID=nete_serverid
CatalogOptions=0
ProcedureResults=0
EnableDisableParam=0
EnableStaticCursorsForLongData=0
ApplicationUsingThreads=1
```

注: データ ソース情報を編集する場合は、ポンド記号 (#) を使用しないでください。ポンド記号 (#) 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。省略された値は ODBC 接続を失敗させる場合があります。

nete_ps_root

ポリシー サーバインストールの明確なパスを指定します。

uid

データベースへのフルアクセス権限があるデータベース アカウ
ントのユーザ名を指定します。

pwd

データベースへのフルアクセス権限があるデータベース アカウ
ント用のパスワードを指定します。

nete_servername

Oracle データベース ホスト システムの名前を指定します。

nete_serverid

Oracle インスタンス サービス名 (SID) を指定します。SID はデー
タベース インスタンス用のシステム識別子です。

例：以下のサンプル `tnsnames.ora` ファイルでは、`instance1` の値は
SID です。

```
instance1=
(Description =
  (ADDRESS = (Protocol = TCP)(Host = myhost)(Port = 1521)
    (CONNECT_DATA = (SID = instance1))
  )
```

3. ファイルを保存します。

Oracle ワイヤプロトコル ドライバが設定されます。

Oracle RAC (SCAN なし) の Oracle ワイヤ プロトコル ドライバ の設定

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
- postgresqlwire.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。

以下の手順に従います。

1. system_odbc.ini ファイルを開きます。
2. 設定するデータ ソースに応じて、以下の情報を使用して適用可能なデータ ソース セクションを編集します。
 - ServiceName=nete_servicename を追加
 - AlternateServers= を追加
 - Loadbalancing=1 を追加
 - SID=nete_serverid を削除またはコメント化

変更したデータ ソースは、以下のように表記されている必要があります。

```
Driver=nete_ps_root/odbc/lib/NSora27.so
Description=DataDirect 7.1 Oracle Wire Protocol
Logon=uid
Password=pwd
HostName=nete_servername1
PortNumber=1521
ServiceName=nete_servicename
CatalogOptions=0
ProcedureRetResults=0
EnableDescribeParam=0
EnableStaticCursorsForLongData=0
ApplicationUsingThreads=1
AlternateServers=
LoadBalancing=1
```

注: データ ソース情報を編集する場合は、ポンド記号 (#) を使用しないでください。ポンド記号 (#) 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 接続が失敗する場合があります。

nete_ps_root

ポリシー サーバがインストールされているディレクトリへの明確なパスを指定します。

uid

データベースへのフルアクセス権限があるデータベース アカウントのユーザ名を指定します。

pwd

データベースへのフルアクセス権限があるデータベース アカウント用のパスワードを指定します。

nete_servername1

最初の Oracle RAC ノードの IP アドレスを指定します。

(Oracle 10g) 最初の Oracle RAC ノードの IP アドレスを指定します。

nete_servicename

Oracle RAC システム全体に対する RAC システムサービス名を指定します。

AlternateServers=

プライマリ サーバが接続を受理していない場合、他の Oracle ノードに接続フェールオーバーを指定します。

例 :

(HostName=nete_servername2:PortNumber=1521:ServiceName=nete_servicename[,...])

LoadBalancing=1

クライアント負荷分散を有効にして、RAC ノードが接続リクエストに対応できなくなる事態を避けるために、新規接続を分散します。有効な場合は、プライマリおよび代替データベース サーバにアクセスする順番はランダムです。

3. ファイルを保存します。

Oracle 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。

次の手順に従ってください:

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。

2. ストレージ リストから以下の値を選択します。

ODBC

3. データベース リストから以下の値を選択します。

ポリシー ストア

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ount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] をクリックして設定を保存します。
8. データベース リストから以下の値を選択します。

キーストア
9. ストレージ リストから以下の値を選択します。

ODBC
10. 以下のオプションを選択します。

ポリシー ストア データベースの使用
11. データベース リストから以下の値を選択します。

監査ログ
12. ストレージ リストから以下の値を選択します。

ODBC
13. 以下のオプションを選択します。

ポリシー ストア データベースの使用
14. [適用] をクリックして設定を保存します。

15. (オプション) [接続のテスト] をクリックしてポリシー サーバがポリシー ストアにアクセスできることを確認します。
16. [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次のとおりです。

`siteminder`

このアカウントは最大の権限を持っています。

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。

- 管理 UI に初めてアクセスする場合。
- 初めて SiteMinder ユーティリティを管理する場合。
- スーパーユーザ権限で別の管理者を作成する場合。

次の手順に従ってください:

1. `smreg` ユーティリティを `siteminder_home\bin` にコピーします。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

注: このユーティリティは、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。

2. 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、引用符でパスワードを囲みます。

注: Oracle ポリシー ストアを設定している場合、パスワードは大文字と小文字を区別します。他のすべてのポリシー ストアの場合は、パスワードの大文字と小文字を区別しません。

3. `siteminder_home¥bin` から `smreg` 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。

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 データ定義をインポートすると、ポリシー ストアで作成および格納できるオブジェクトのタイプが定義されます。

次の手順に従ってください：

1. コマンド ウィンドウを開き、`siteminder_home¥xps¥dd` 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. 以下のコマンドを実行します。

```
XPSDDInstall SmMaster.xdd
```

```
XPSDDInstall
```

必要なデータ定義をインポートします。

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 とポリシー サーバで使用するポリシー ストアが設定されます。

以下の点を考慮します。

- 必ず `siteminder_home\bin` への書き込みアクセス権があることを確認してください。インポートユーティリティは、ポリシー ストア オブジェクトをインポートするためにこの権限を必要とします。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

- 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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン 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。

次の手順に従ってください:

1. コマンド ウィンドウを開き、`siteminder_home¥db` に移動します。
2. 以下のファイルのいずれかをインポートします。

- `smpolicy.xml` をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy.xml -npass
```

- `smpolicy-secure.xml` をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy-secure.xml -npass
```

```
npass
```

パスフレーズが必要ではないことを指定します。デフォルトポリシー ストア オブジェクトには暗号化されたデータが含まれていません。

両方のファイルに、デフォルトのポリシー ストア オブジェクトが含まれています。これらのオブジェクトにはデフォルトのエージェント設定オブジェクト (ACO) テンプレート内のデフォルトセキュリティ設定が含まれます。`smpolicy-secure` ファイルはより制限の厳しいセキュリティ設定を提供します。詳細については、「[デフォルトのポリシー ストア オブジェクトの考慮事項 \(P. 104\)](#)」を参照してください。

- **Option Pack** 機能をインポートするには、以下のコマンドを実行します。

```
XPSImport ampolicy.xml -npass
```

- フェデレーション機能をインポートするには、以下のコマンドを実行します。

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

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。

注: `smpolicy.xml` をインポートすると、**SiteMinder** から別個にライセンスが付与される レガシー フェデレーション および **Web** サービスの変数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。

Advanced Authentication Server の有効化

ユーザのポリシー サーバの設定の一部として、Advanced Authentication Server を有効にします。

次の手順に従ってください:

1. ポリシー サーバ設定ウィザードを実行します。
2. ウィザードの最初の画面にあるチェックボックスをすべてオフのままにします。
3. [次へ] をクリックします。
4. Advanced Authentication Server 用のマスタ暗号化キーを作成します。
注: 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。
5. ポリシー サーバ設定ウィザードの残りの手順を完了します。

Advanced Authentication Server が有効になります。

ポリシー サーバの再起動

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、`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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

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。

以下の点を考慮します。

- 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の手順を実行します。
- (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](#) (P. 598) します。

次の手順に従ってください：

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： 15

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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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 サーバに管理者認証情報を提供します。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認証情報を使用します。

IBM DB2 ポリシー ストアの設定

1 つの IBM DB2 データベースは以下として機能させることができます。

- ポリシー ストア
- キー ストア
- ログ データベース

注: 個別のデータベースに **SiteMinder** セッション情報を格納します。ポリシー ストアを使用してセッション情報を格納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 IBM DB2 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。

以下の点を考慮します。

- W から始まる情報は Windows の要件を表します。
- U から始まる情報は UNIX の要件を表します。

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。IBM DB2 情報のワークシートを使用して値を記録できます。

- **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を決定します。
- **管理アカウント** - データベース内のオブジェクトを作成、読み取り、変更、および削除する権限があるアカウントのユーザ名を決定します。
- **管理パスワード** - 管理アカウントのパスワードを決定します。
- **IP アドレス** - データベース ホスト システムの IP アドレスを決定します。
- **TCP ポート** - データベースがリスンするポートを決定します。
- **(W) データ ソース名** - データ ソースを識別する名前を決定します。
- **(U) ポリシー サーバルート** - ポリシー サーバがインストールされている場所への明示的なパスを決定します。
- **(U) パッケージ** -- 動的な SQL を処理するパッケージの名前を決定します。
- **(U) パッケージ所有者** -- パッケージに割り当てられた AuthID を決定します。この 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。
- **(U) 付与 AuthID** - パッケージに対する実行権限を制限する場合は、パッケージに対する実行権限に付与される AuthID を決定します。

デフォルト ワイヤプロトコル設定：パブリック

- (U) 分離レベル - システムがロックを取得しリリースする方法を決定します。

デフォルト ワイヤプロトコル設定 : CURSOR_STABILITY

- (U) ダイナミック セクション - ワイヤプロトコル ドライバ パッケージが 1 人のユーザに用意できるセッションの数を決定します。

デフォルト ワイヤプロトコル設定 : 100

ポリシー ストアを設定する方法

単一の IBM DB2 データベースを、ポリシー ストア、キー ストア、ログ データベースとして設定するには、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一部でこの情報が必要となります。

1. SiteMinder データを含んでいる IBM DB2 データベース インスタンスが、ポリシー サーバ システムからアクセス可能であることを確認してください。
2. 以下のデータベース インスタンス設定を確認します。
 - ポリシー ストアのみを設定している場合、テーブルスペース ページ サイズ (page_size) およびバッファプール ページ サイズ設定を、それぞれ 16k 以上に設定する必要があります。

各設定に対するデフォルト DB2 値は SiteMinder ポリシー ストア スキーマでは十分ではありません。
 - ポリシー ストアと監査ストアのみを設定している場合、テーブルスペース ページ サイズ (page_size) およびバッファプール ページ サイズ設定を、それぞれ 32k 以上に設定する必要があります。

各設定に対するデフォルト DB2 値は SiteMinder ポリシー ストアおよび監査ストア スキーマでは十分ではありません。
3. SiteMinder スキーマを作成します。
4. SiteMinder 用の DB2 データ ソースを設定します。
5. 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。
6. SiteMinder スーパーユーザ パスワードを設定します。
7. ポリシー ストア データ定義をインポートします。
8. 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。

9. ポリシー サーバを再起動します。
10. 管理 UI 登録の準備をします。

SiteMinder スキーマの作成

次の手順に従ってください:

1. `siteminder_home¥db¥tier2¥DB2` 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. 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 ストアおよびキー 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。
12.52 SP1 の場合、[このスクリプトを編集](#) (P. 431)してから、監査ストアを作成します。

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

```
siteminder_home¥xps¥db¥DB2.sql
```

```
siteminder_home
```

ポリシー サーバのインストール 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 用の IBM DB2 データソースを設定します。

ODBC を使用している場合は、SiteMinder 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。

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。

以下の手順に従います。

1. 以下のいずれかの操作を実行します。
 - サポートされた 32 ビットの Windows オペレーティング システムを使用している場合は、[スタート] をクリックし、[プログラム] - [管理ツール] - [ODBC データ ソース] を選択します。
 - サポートされた 64 ビットの Windows オペレーティング システムを使用している場合：
 - a. `install_home¥Windows¥SysWOW64` に移動します。
 - b. `odbcad32.exe` をダブルクリックします[ODBC データ ソース アドミニストレータ] が表示されます。
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. (オプション) [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 がシステムでリスンする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、SiteMinder を設定して作成したデータ ソースを使用できます。

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に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。
Driver	SiteMinder DB2 ワイヤ プロトコル ドライバの完全パス。	「 <code>nete_ps_root</code> 」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。
Database	DB2 UDB データベースの名前。	「 <code>nete_database</code> 」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。

次の手順に従ってください:

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。
2. ストレージ リストから以下の値を選択します。
ODBC
3. データベース リストから以下の値を選択します。
ポリシー ストア
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] をクリックして設定を保存します。
8. データベース リストから以下の値を選択します。
キーストア
9. ストレージ リストから以下の値を選択します。
ODBC
10. 以下のオプションを選択します。
ポリシー ストア データベースの使用
11. データベース リストから以下の値を選択します。
監査ログ

12. ストレージ リストから以下の値を選択します。

ODBC

13. 以下のオプションを選択します。

ポリシー ストア データベースの使用

14. [適用] をクリックして設定を保存します。

15. (オプション) [接続のテスト] をクリックしてポリシー サーバがポリシー ストアにアクセスできることを確認します。

16. [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次のとおりです。

siteminder

このアカウントは最大の権限を持っています。

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。

- 管理 UI に初めてアクセスする場合。
- 初めて SiteMinder ユーティリティを管理する場合。
- スーパーユーザ権限で別の管理者を作成する場合。

次の手順に従ってください:

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

siteminder_home

ポリシー サーバのインストールパスを指定します。

注: このユーティリティは、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。

2. 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、引用符でパスワードを囲みます。

注: Oracle ポリシー ストアを設定している場合、パスワードは大文字と小文字を区別します。他のすべてのポリシー ストアの場合は、パスワードの大文字と小文字を区別しません。

3. `siteminder_home\bin` から `smreg` 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。

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 データ定義をインポートすると、ポリシー ストアで作成および格納できるオブジェクトのタイプが定義されます。

次の手順に従ってください：

1. コマンド ウィンドウを開き、`siteminder_home\bin` 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. 以下のコマンドを実行します。

```
XPSDDInstall SmMaster.xdd
```

```
XPSDDInstall
```

必要なデータ定義をインポートします。

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 とポリシー サーバで使用するポリシー ストアが設定されます。

以下の点を考慮します。

- 必ず `siteminder_home¥bin` への書き込みアクセス権があることを確認してください。インポートユーティリティは、ポリシー ストア オブジェクトをインポートするためにこの権限を必要とします。

`siteminder_home`

ポリシー サーバのインストールパスを指定します。

- 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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン 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。

次の手順に従ってください:

1. コマンド ウィンドウを開き、*siteminder_home¥db* に移動します。
2. 以下のファイルのいずれかをインポートします。

- *smpolicy.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy.xml -npass
```

- *smpolicy-secure.xml* をインポートするには、以下のコマンドを実行します。

```
XPSImport smpolicy-secure.xml -npass
```

```
npass
```

パスフレーズが必要ではないことを指定します。デフォルトポリシー ストア オブジェクトには暗号化されたデータが含まれていません。

両方のファイルに、デフォルトのポリシー ストア オブジェクトが含まれています。これらのオブジェクトにはデフォルトのエージェント設定オブジェクト (ACO) テンプレート内のデフォルトセキュリティ設定が含まれます。 *smpolicy-secure* ファイルはより制限の厳しいセキュリティ設定を提供します。詳細については、「[デフォルトのポリシー ストア オブジェクトの考慮事項 \(P. 104\)](#)」を参照してください。

- Option Pack 機能をインポートするには、以下のコマンドを実行します。

```
XPSImport ampolicy.xml -npass
```

- フェデレーション機能をインポートするには、以下のコマンドを実行します。

```
XPSImport fedpolicy-12.52 SP1.xml -npass
```

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。

注: *smpolicy.xml* をインポートすると、SiteMinder から別個にライセンスが付与される レガシー フェデレーション および Web サービスの変数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。

Advanced Authentication Server の有効化

ユーザのポリシー サーバの設定の一部として、Advanced Authentication Server を有効にします。

次の手順に従ってください:

1. ポリシー サーバ設定ウィザードを実行します。
2. ウィザードの最初の画面にあるチェックボックスをすべてオフのままにします。
3. [次へ] をクリックします。
4. Advanced Authentication Server 用のマスタ暗号化キーを作成します。
注: 別の (n 番目の) ポリシー サーバをインストールしている場合は、以前使用した Advanced Authentication Server に対して同じ暗号化キーを使用します。
5. ポリシー サーバ設定ウィザードの残りの手順を完了します。

Advanced Authentication Server が有効になります。

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。

以下の点を考慮します。

- 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の手順を実行します。
- (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](#) (P. 598) します。

次の手順に従ってください:

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: 15

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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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 サーバに管理者認証情報を提供します。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認証情報を使用します。

セッション情報を IBM DB2 に格納する方法

セッションストアとして IBM DB2 データベースを設定するには、以下の手順に従います。

1. 必要なデータベース情報を収集したことを確認してください。
2. セッションストア スキーマを作成します。
3. SiteMinder 用の IBM DB2 データ ソースを設定します。
4. ポリシー サーバがそのセッションストアを参照するように指定します。

詳細情報:

[データベース情報の収集 \(P. 401\)](#)

[SiteMinder 用の IBM DB2 データ ソースを設定します。 \(P. 404\)](#)

セッションストア スキーマの作成

IBM DB2 データベースがセッション情報を格納できるように、SiteMinder スキーマを作成します。

以下の手順に従います。

1. ポリシー サーバ ホスト システムにログインします。
2. `siteminder_home¥db¥tier2¥DB2` 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。

3. 以下のファイルを開き、内容をテキスト エディタにコピーします。

`sm_db2_ss.sql`

4. クエリに内容を貼り付けて、クエリを実行します。

注: クエリを実行する詳細については、IBM のドキュメントを参照してください。

セッションストア スキーマがデータベースに追加されます。

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. [Apply] をクリックします。
設定が保存されます。
7. [テスト接続] 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

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、**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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

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. データベース情報を収集します。
3. セッションストア スキーマを作成します。
4. SiteMinder 用の MySQL データ ソースを設定します。
5. 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。
6. 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 \(P. 323\)](#)

[SiteMinder 用の MySQL データ ソースの設定 \(P. 325\)](#)

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。

次の手順に従ってください:

1. ポリシー サーバ ホスト システムにログインします。
2. 以下の場所に移動します。

```
siteminder_home¥db¥tier2¥MySQL.
```

```
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. テキストエディタで次のファイルを開きます。

```
sm_mysql_ss.sql
```

4. 以下の行を確認します。

```
DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$  
CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
```

5. 'databaseName' の各インスタンスをセッション ストアとして機能するデータベースの名前に置換します。
6. 全ファイルの内容をコピーします。
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。
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. [Apply] をクリックします。

設定が保存されます。
7. [テスト接続] 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

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、**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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

Oracle でセッション情報を格納する方法

セッション ストアとして Oracle データベースを設定するには、以下の手順に従います。

1. データベース情報を収集します。
2. セッション ストア スキーマを作成します。
3. SiteMinder 用の Oracle 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. ポリシー サーバを再起動します。

詳細情報:

[SiteMinder 用の Oracle データ ソースの設定](#) (P. 380)

[データベース情報の収集](#) (P. 375)

セッション ストア スキーマの作成

Oracle 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。

次の手順に従ってください:

1. データベース情報を管理するユーザとして **Oracle** にログインします。
sqlplus などの **Oracle** ユーティリティでログインします。

注: SYS ユーザや SYSTEM ユーザでスキーマを作成しないことをお勧めします。必要な場合は、SMOWNER などの **Oracle** ユーザを作成し、そのユーザでスキーマを作成します。

2. Unicode 文字を格納するには、**Oracle** データベースの文字セットが正しく設定されていることを確認します。英語の文字のみを使用する場合は、この手順をスキップします。

- a. 文字セットを検索するには、以下のクエリを使用します。

```
SELECT value$ FROM sys.props$ WHERE name = 'NLS_CHARACTERSET' ;
```

- b. スキーマをインポートする前に、文字セットが AL32UTF8 または UTF8 であることを確認します。

3. 以下のスクリプトをインポートします。

```
$NETE_PS_ROOT/db/sql/sm_oracle_ss.sql
```

注: 一部の **Oracle SQL** ユーティリティには、環境変数に関する問題があります。ユーティリティを使用して、スクリプトをインポートしようとする問題が発生する場合は、明示的なパスを指定します。

4. セッション ストア用のテーブルスペースを作成します。
5. データベース内のテーブルスペースを管理するための以下の権限を持つユーザを作成します。

- Connect
- Resource
- Unlimited Tablespace

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. [Apply] をクリックします。
設定が保存されます。
7. [テスト接続] 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

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、`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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

SQL Server 内にセッション情報を格納する方法

スタンドアロンセッションストアとして SQL Server データベースを設定するには、以下の手順に従います。

1. データベース情報を収集します。
2. セッションストア スキーマを作成します。
3. SiteMinder 用の SQL 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. ポリシー サーバを再起動します。

詳細情報:

[SiteMinder 用の SQL Server データ ソースを設定する](#) (P. 342)

[データベース情報の収集](#) (P. 339)

セッション ストア スキーマの作成

SQL Server データベースがセッション情報を格納および読み取ることができるよう、セッション ストア スキーマを作成します。

セッション ストア スキーマを作成する方法

1. 以下のいずれかを実行します。
 - セッション ストアに Unicode 文字を格納する予定がある場合、`sm_mssql_ss.sql.unicode` をテキスト エディタで開き、ファイル全体のコンテンツをコピーします。
 - セッション ストアに Unicode 文字を格納する予定がない場合、`sm_mssql_ss.sql` をテキスト エディタで開き、ファイル全体のコンテンツをコピーします。
2. クエリ アナライザを起動し、ポリシー サーバ データベースの管理者としてログインします。
3. [データベース] リストからデータベース インスタンスを選択します。
4. スキーマをクエリに貼り付けます。
5. クエリを実行します。
セッション ストア スキーマがデータベース内に作成されます。

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. [Apply] をクリックします。

設定が保存されます。
7. [テスト接続] 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

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、`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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

セッション情報を PostgreSQL に格納する方法

スタンドアロンセッションストアとして PostgreSQL Server データベースを設定するには、以下の手順に従います。

1. データベース情報を収集します。
2. セッションストアスキーマを作成します。
3. SiteMinder 用の PostgreSQL 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. ポリシー サーバを再起動します。

セッション ストア スキーマの作成

SQL Server データベースがセッション情報を格納および読み取ることができるように、セッション ストア スキーマを作成します。

セッション ストア スキーマを作成する方法

1. テキスト エディタで `sm_postgresql_ss.sql` を開き、ファイル全体の内容をコピーします。
2. `psql` などの SQL クライアントを使用し、ポリシー サーバ データベースの管理者としてログインします。
3. [データベース] リストからデータベース インスタンスを選択します。
4. スキーマをクエリに貼り付けます。
5. クエリを実行します。

セッション ストア スキーマがデータベース内に作成されます。

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. [テスト接続] 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

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、**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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

監査ログを IBM DB2 に格納する方法

監査ログを格納するように IBM DB2 データベースを設定するには、以下の手順に従います。

1. 必要なデータベース情報を収集したことを確認してください。
2. データベース インスタンスのテーブルスペース ページサイズ (**page_size**) およびバッファプール ページサイズ設定が、それぞれ 16k 以上に設定されていることを確認してください。

各設定に対するデフォルト DB2 値は SiteMinder 監査ログ スキーマでは十分ではありません。

3. 監査ストア スキーマを作成します。
4. SiteMinder 用の IBM DB2 データ ソースを設定します。
5. ポリシー サーバがその監査ストアを参照するように指定します。
6. ポリシー サーバの再起動

詳細情報:

[データベース情報の収集 \(P. 401\)](#)

[SiteMinder 用の IBM DB2 データ ソースを設定します。 \(P. 404\)](#)

監査ストア スキーマの作成

IBM DB2 データベースが監査ログを格納できるように、SiteMinder スキーマを作成します。

次の手順に従ってください:

1. ポリシー サーバ ホスト システムにログインします。
2. `siteminder_home¥db¥tier2¥DB2` 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。

3. 以下のファイルを開き、内容をテキスト エディタにコピーします。

`sm_db2_logs.sql`

4. 以下の行から NULL を削除します。

```
sm_assertion_id          VARCHAR(255) NULL,
sm_assertion_issuerid    VARCHAR(255) NULL,
sm_assertion_destinationurl VARCHAR(4096) NULL,
sm_assertion_statuscode  VARCHAR(255) NULL,
sm_assertion_NotOnBefore  TIMESTAMP,
sm_assertion_notonorafter  TIMESTAMP,
sm_assertion_sess_starttime  TIMESTAMP,
sm_assertion_sess_notonorafter  TIMESTAMP,
sm_assertion_authcontext  VARCHAR(255) NULL,
sm_assertion_versionid    VARCHAR(255) NULL,
sm_assertion_claims       VARCHAR(255) NULL,
sm_application_name       VARCHAR(255) NULL,
sm_tenant_name            VARCHAR(255) NULL,
sm_authentication_method  VARCHAR(255) NULL
```

5. ファイルの変更を保存します。
6. クエリに内容を貼り付けて、クエリを実行します。

注: クエリを実行する詳細については、IBM のドキュメントを参照してください。

監査ストア スキーマがデータベースに追加されます。

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. [Apply] をクリックします。
設定が保存されます。

9. [テスト接続] 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

特定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。

次の手順に従ってください:

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。
- 注: UNIX または Linux オペレーティング環境では、**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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

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. データベース情報を収集します。
3. 監査ログスキーマを作成します。
4. SiteMinder 用の MySQL データ ソースを設定します。

5. 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。
6. 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 \(P. 323\)](#)

[SiteMinder 用の MySQL データ ソースの設定 \(P. 325\)](#)

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。

次の手順に従ってください:

1. ポリシー サーバ ホスト システムにログインします。
2. 以下の場所に移動します。

```
siteminder_home%db%tier2%MySQL.
```

```
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. テキストエディタで次のファイルを開きます。

```
sm_mysql_logs.sql
```

4. 以下の行を確認します。

```
DROP FUNCTION IF EXISTS `databaseName`.`getdate` $$  
CREATE FUNCTION `databaseName`.`getdate` () RETURNS DATE
```

5. 'databaseName' の各インスタンスを監査ストアとして機能するデータベースの名前に置換します。
6. 全ファイルの内容をコピーします。
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。
監査ストア 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、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. [Apply] をクリックします。
設定が保存されます。
9. [テスト接続] 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

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、**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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

Oracle で監査ログを格納する方法

監査ログを格納するよう Oracle データベースを設定するには、以下の手順に従います。

1. データベース情報を収集します。
2. 監査ストア スキーマを作成します。
3. SiteMinder 用の Oracle 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. ポリシー サーバを再起動します。

詳細情報:

[SiteMinder 用の Oracle データ ソースの設定](#) (P. 380)

[データベース情報の収集](#) (P. 375)

監査ログスキーマの作成

Oracle 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。

次の手順に従ってください:

1. sqlplus または他の Oracle ユーティリティを使用して、ポリシー サーバ データベース情報を管理するユーザとして Oracle にログインします。

注: SYS または SYSTEM のユーザで SiteMinder スキーマを作成しないことをお勧めします。必要な場合は、SMOWNER などの Oracle ユーザを作成し、そのユーザでスキーマを作成します。

2. 以下のスクリプトをインポートします。

`$NETE_PS_ROOT/db/sql/sm_oracle_logs.sql`

注: 環境変数は Oracle の SQL ユーティリティ内では機能しない場合があります。ユーティリティを使用して、スクリプトをインポートしようとする問題が発生する場合は、明示的なパスを指定します。

3. 監査ログ スキーマ用のテーブルスペースを作成します。
4. データベース内のテーブルスペースを管理するための以下の権限を持つユーザを作成します。
 - Connect
 - Resource
 - Unlimited Tablespace

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. [Apply] をクリックします。
設定が保存されます。
9. [テスト接続] 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

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、`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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

SQL Server 内に監査ログを格納する方法

スタンドアロン監査ログ データベースとして SQL Server データベースを設定するには、以下の手順に従います。

1. データベース情報を収集します。
2. 監査ストア スキーマを作成します。
3. SiteMinder 用の SQL 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. ポリシー サーバを再起動します。

詳細情報:

[SiteMinder 用の SQL Server データ ソースを設定する](#) (P. 342)

[データベース情報の収集](#) (P. 339)

監査ログスキーマの作成

SQL Server データベースが監査ログを格納できるように、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. テキスト エディタで `sm_mssql_logs.sql` を開き、ファイル全体の内容をコピーします。
2. クエリ アナライザを起動し、ポリシー サーバ データベースを管理するユーザとしてログインします。
3. [データベース] リストからデータベース インスタンスを選択します。
4. `sm_mssql_logs.sql` からクエリにスキーマを貼り付けます。
5. クエリを実行します。

SiteMinder 監査ログ ストア スキーマがデータベース内に作成されます。

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. [Apply] をクリックします。

設定が保存されます。
9. [テスト接続] 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

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、`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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

監査ログを PostgreSQL に格納する方法

スタンドアロン監査ログ データベースとして PostgreSQL データベースを設定するには、以下の手順に従います。

1. データベース情報を収集します。
2. 監査ストア スキーマを作成します。
3. SiteMinder 用の PostgreSQL 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. ポリシー サーバを再起動します。

監査ログスキーマの作成

PostgreSQL Server データベースが監査ログを格納できるように、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. テキスト エディタで `sm_postgresql_logs.sql` を開き、ファイル全体の内容をコピーします。
2. `psql` などの SQL クライアントを起動し、ポリシー サーバ データベースの管理者ユーザとしてログインします。
3. [データベース] リストからデータベース インスタンスを選択します。
4. `sm_postgresql_logs.sql` からクエリにスキーマを貼り付けます。
5. クエリを実行します。

監査ログ ストア スキーマがデータベース内に作成されます。

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. [テスト接続] 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

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、`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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

キー情報を IBM DB2 に格納する方法

スタンドアロン キー ストアとして IBM DB2 データベースを設定するには、以下の手順に従います。

1. データベース情報を収集します。
2. キー ストア スキーマを作成します。
3. SiteMinder 用の IBM DB2 データ ソースを設定します。
4. ポリシー サーバがそのキー ストアを参照するように指定します。
5. 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 \(P. 401\)](#)

[SiteMinder 用の IBM DB2 データ ソースを設定します。 \(P. 404\)](#)

キー ストア スキーマの作成

IBM DB2 データベースがキー情報を格納できるように、SiteMinder スキーマを作成します。

以下の手順に従います。

1. ポリシー サーバ ホスト システムにログインします。
2. `siteminder_home¥db¥tier2¥DB2` 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。

3. 以下のファイルを開き、内容をテキスト エディタにコピーします。

`sm_db2_ps.sql`

4. クエリに内容を貼り付けて、クエリを実行します。

注: クエリを実行する詳細については、IBM のドキュメントを参照してください。

キー ストア スキーマがデータベースに追加されます。

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. [Apply] をクリックします。

設定が保存されます。
8. [テスト接続] 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

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、**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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

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. データベース情報を収集します。
3. キー ストア スキーマを作成します。
4. SiteMinder 用の MySQL データ ソースを設定します。
5. 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。
6. 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 \(P. 323\)](#)

[SiteMinder 用の MySQL データ ソースの設定 \(P. 325\)](#)

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。

次の手順に従ってください:

1. ポリシー サーバ ホスト システムにログインします。
2. 以下の場所に移動します。

```
siteminder_home¥db¥tier2¥MySQL.
```

```
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. テキストエディタで次のファイルを開きます。

```
sm_mysql_ps.sql
```

4. 以下の行を確認します。

```
DROP FUNCTION IF EXISTS `dbName`.`getdate` $$  
CREATE FUNCTION `dbName`.`getdate` () RETURNS DATE
```

5. 'dbName' の各インスタンスをキー ストアとして機能するデータベースの名前に置換します。
6. 全ファイルの内容をコピーします。
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。
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. [Apply] をクリックします。
設定が保存されます。
8. [テスト接続] 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

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、**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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

Oracle でキー情報を格納する方法

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

1. データベース情報を収集します。
2. キー ストア スキーマを作成します。
3. SiteMinder 用の Oracle 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. ポリシー サーバを再起動します。

詳細情報:

[SiteMinder 用の Oracle データ ソースの設定 \(P. 380\)](#)

[データベース情報の収集 \(P. 375\)](#)

キー ストア スキーマの作成

Oracle 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。

次の手順に従ってください:

1. sqlplus または他の Oracle ユーティリティを使用して、ポリシー サーバ データベース情報を管理するユーザとして Oracle にログインします。

注: SYS または SYSTEM のユーザで SiteMinder スキーマを作成しないことをお勧めします。必要な場合は、SMOWNER などの Oracle ユーザを作成し、そのユーザでスキーマを作成します。

2. 以下のスクリプトをインポートします。

`$NETE_PS_ROOT/db/sql/sm_oracle_ps.sql`

注: 環境変数は Oracle の SQL ユーティリティ内では機能しない場合があります。ユーティリティを使用して、スクリプトをインポートしようとする問題が発生する場合は、明示的なパスを指定します。

3. キー ストア用のテーブルスペースを作成します。
4. データベース内のテーブルスペースを管理するための以下の権限を持つユーザを作成します。
 - Connect
 - Resource
 - Unlimited Tablespace

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. [Apply] をクリックします。
設定が保存されます。
8. [テスト接続] 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

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、`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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

SQL Server 内にキー情報を格納する方法

スタンドアロン キー ストアとして SQL Server データベースを設定するには、以下の手順に従います。

1. データベース情報を収集します。
2. キー ストア スキーマを作成します。
3. SiteMinder 用の SQL 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. ポリシー サーバを再起動します。

詳細情報:

[SiteMinder 用の SQL Server データ ソースを設定する](#) (P. 342)

[データベース情報の収集](#) (P. 339)

キー ストア スキーマの作成

SQL Server 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. テキスト エディタで `sm_mssql_ps.sql` を開き、ファイル全体の内容をコピーします。
2. クエリ アナライザを起動し、ポリシー サーバ データベースの管理者としてログインします。
3. [データベース] リストからデータベース インスタンスを選択します。
4. `sm_mssql_ps.sql` からクエリにスキーマを貼り付けます。
5. クエリを実行します。

SiteMinder キー ストア スキーマがデータベース内に作成されます。

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. [Apply] をクリックします。

設定が保存されます。
8. [テスト接続] 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

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、`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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

キー情報を PostgreSQL に格納する方法

スタンドアロン キー ストアとして PostgreSQL Server データベースを設定するには、以下の手順に従います。

1. データベース情報を収集します。
2. キー ストア スキーマを作成します。
3. SiteMinder 用の PostgreSQL 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. ポリシー サーバを再起動します。

キー ストア スキーマの作成

SQL Server 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. テキスト エディタで `sm_postgresql_ps.sql` を開き、ファイル全体の内容をコピーします。
2. `psql` などの SQL クライアントを開き、ポリシー サーバ データベースの管理者としてログインします。
3. [データベース] リストからデータベース インスタンスを選択します。
4. `sm_postgresql_ps.sql` からクエリにスキーマを貼り付けます。
5. クエリを実行します。

SiteMinder キー ストア スキーマがデータベース内に作成されます。

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. [テスト接続] 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

特定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。

次の手順に従ってください:

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。

注: UNIX または Linux オペレーティング環境では、**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 サーバを再起動することもできます。これらのコマンドは、ポリシー サーバ管理コンソールの代わりとなります。

サンプル ユーザ ディレクトリ

SiteMinder は、所有者のユーザストアの使用を必要としません。ただし、SiteMinder は、サンプル ユーザをリレーショナル データベースに読み込むスキーマ ファイルを提供します。

IBM DB2 サンプル ユーザ ディレクトリの設定

サンプル ユーザ ディレクトリを設定し、サンプル ユーザをデータベースに読み込みます。

以下の手順に従います。

1. ポリシー サーバ ホスト システムにログインします。
2. `siteminder_home¥db¥tier2¥DB2` 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。

3. 以下のファイルを開き、内容をテキスト エディタにコピーします。

`smsampleusers_db2.sql`

4. クエリに内容を貼り付けて、クエリを実行します。

注: クエリを実行する詳細については、IBM のドキュメントを参照してください。

ユーザ ディレクトリに、サンプル ユーザが読み込まれます。

5. ポリシー サーバへのユーザ ディレクトリ接続を設定します。

注: ユーザ ディレクトリ接続の設定の詳細については、「ポリシー サーバ 構成ガイド」を参照してください。

MySQL サンプル ユーザ ディレクトリの設定

サンプル ユーザ ディレクトリを設定し、サンプル ユーザをデータベースに読み込みます。

次の手順に従ってください:

1. ポリシー サーバ ホスト システムにログインします。
2. 以下の場所に移動します。

`siteminder_home\db\tier2\MySQL.`

`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. テキストエディタで次のファイルを開きます。

`smampleusers_mysql.sql`

4. 以下の行を確認します。

```
DROP FUNCTION IF EXISTS `dbName`.`getdate` $$
CREATE FUNCTION `dbName`.`getdate` () RETURNS DATE
```

5. 'dbName' の各インスタンスをサンプル ユーザ ストアとして機能するデータベースの名前に置換します。
6. 全ファイルの内容をコピーします。

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。

注: クエリを実行する詳細については、MySQL のドキュメントを参照してください。

ユーザストアに、サンプルユーザが読み込まれます。

8. ポリシーサーバへのユーザディレクトリ接続を設定します。

注: ユーザディレクトリ接続の設定の詳細については、「ポリシーサーバ構成ガイド」を参照してください。

Oracle サンプル ユーザ ディレクトリ の設定

サンプルユーザディレクトリを設定し、サンプルユーザをデータベースに読み込みます。

次の手順に従ってください:

1. sqlplus または他の Oracle ユーティリティを使用して、ポリシーサーバデータベース情報を管理するユーザとして Oracle にログインします。

注: SYS または SYSTEM のユーザで SiteMinder スキーマを作成しないことをお勧めします。必要な場合は、SMOWNER などの Oracle ユーザを作成し、そのユーザでスキーマを作成します。

2. 以下のスクリプトをインポートします。

`$NETE_PS_ROOT/db/sql/smsampleusers_oracle.sql`

注: 環境変数は Oracle の SQL ユーティリティ内では機能しない場合があります。ユーティリティを使用して、スクリプトをインポートしようとする問題が発生する場合は、明示的なパスを指定します。

ユーザ ディレクトリに、サンプル ユーザが読み込まれます。

3. ユーザ ディレクトリ用のテーブルスペースを作成します。
4. データベース内のテーブルスペースを管理するための以下の権限を持つユーザを作成します。
 - Connect
 - Resource
 - Unlimited Tablespace

5. ポリシー サーバへのユーザ ディレクトリ接続を設定します。

注: ユーザ ディレクトリ接続の設定の詳細については、「ポリシー サーバ 構成ガイド」を参照してください。

SQL Server サンプル ユーザ ディレクトリの設定

サンプル ユーザ ディレクトリを設定し、サンプル ユーザをデータベースに読み込みます。

サンプル ユーザ ディレクトリを設定する方法

1. テキスト エディタで `smsampleusers_sqlserver.sql` を開き、ファイル全体の内容をコピーします。
2. クエリ アナライザを起動し、ポリシー サーバ データベースを管理するユーザとしてログインします。
3. [データベース] リストからデータベース インスタンスを選択します。
4. `smsampleusers_sqlserver.sql` からクエリにスキーマを貼り付けます。

5. クエリを実行します。

ユーザ ディレクトリに、サンプル ユーザが読み込まれます。

6. ポリシー サーバへのユーザ ディレクトリ接続を設定します。

注:ユーザ ディレクトリ接続の設定の詳細については、「ポリシー サーバ 構成ガイド」を参照してください。

第 8 章：管理 UI のインストール

UI とポリシー サーバの間の信頼関係

デフォルト スーパーユーザのアカウント（**siteminder**）およびパスワードを使用して最初に 管理 UI にログインするときに、管理 UI とポリシー サーバの間の信頼関係が確立します。この関係はユーザの環境を管理するのに必要です。

スーパーユーザ アカウントの認証情報はポリシー ストアに格納されます。ポリシー サーバのインストール中にデフォルト ポリシー ストアの 1 つを設定する場合、これらの認証情報はインストーラにより自動的にサブミットされます。ポリシー サーバのインストールと関係なくポリシー ストアを設定する場合は、**XPSRegClient** ユーティリティを使用して、認証情報をポリシー サーバにサブミットしてください。ポリシー サーバは、登録リクエストが有効でありリレーションシップが構築できることを確認するために、これらの認証情報を使用します。

重要：スーパーユーザ アカウント認証情報がポリシー ストアにサブミットされる時間と管理者が 管理 UI にログインする時間の間には、**24 時間**の制限が存在します。認証情報が設定されてから **24 時間**以内に 管理 UI への最初のログインを実行しなかった場合は、**XPSRegClient** ユーティリティを使用して認証情報をリセットしてください。

管理 UI インストール チェックリストを完了します。

インストールプログラムにより、必要なアプリケーション サーバインフラストラクチャが作成されます。このインフラストラクチャには、埋め込みアプリケーション サーバ (JBoss) および必要な JDK が含まれます。インストールを開始する前に、管理 UI ホスト システムが最小のシステム要件を満たすことを確認します。

管理 UI のインストールを開始する前に、以下の手順を完了してください。

- サポートされているオペレーティング システムを使用していることを確認してください。
- 管理 UI ホスト システムが最小のシステム要件を満たすことを確認してください。
- (Linux) 必要な Linux ライブラリが管理 UI ホスト システムにインストールされていることを確認します。
- ポリシー ストアがいつ設定されたか決定します。

ポリシー ストアが 24 時間以上前に設定された場合は、管理 UI をインストールする前に XPSRegClient ユーティリティを使用して、デフォルトの SiteMinder スーパーユーザ アカウント認証情報をポリシー サーバにサブミットします。ポリシー サーバは、管理 UI との信頼できるリレーションシップを構築するためにこれらの認証情報を必要とします。

注: サポートされている CA およびサードパーティ コンポーネントのリストについては、テクニカル サポート サイトの SiteMinder 12.52 SP1 プラットフォームのサポート マトリックスを参照してください。

管理 UI をインストールする方法

管理 UI をインストールするには、以下の手順に従います。

1. 管理 UI インストール チェックリストを必ず確認してください。
2. (Linux) 必要な Linux ライブラリ要件を確認します。
3. インストーラ用の情報を収集します。
4. (オプション) 登録ウィンドウをリセットします。

5. 管理 UI をインストールします。
6. 管理 UI を登録します。

以下の点について考慮してください。

- **Windows** インストールが完了したら、ポリシー サーバに 管理 UI を登録するため、**SiteMinder** 管理 UI ログイン画面が表示され、アプリケーション サーバが自動的に開始されます。
- **UNIX** インストールが完了したら、アプリケーション サーバを手動で開始させ、登録を完了するために 管理 UI にログインします。詳細については、「管理 UI の登録方法」を参照してください。

インストーラのための情報の収集

管理 UI をインストールおよび登録する前に、以下の情報を収集します。

- **インストール場所** - 管理 UI のインストールパスを決定します。
- **管理 UI システム名** - 管理 UI ホスト システムの完全修飾名を識別します。
- **サーバポート** - JBoss が HTTP リクエストをリスンすべきポートを識別します。
- **SiteMinder スーパーユーザ アカウント パスワード** - デフォルト ユーザ アカウント (siteminder) のパスワードを識別します。
- **ポリシー サーバ システム名** - 以下を識別します。
 - 管理 UI が登録されるポリシー サーバ。
 - ポリシー サーバ ホスト システムの完全修飾名。
- **ポリシー サーバ 認証ポート** - ポリシー サーバのインストール後にデフォルトの設定を変更した場合は、ポリシー サーバ 認証ポートを識別します。ポリシー サーバ 管理コンソール内の設定タブは、アクセス制御ポートをリスト表示します。

管理 UI 登録ウィンドウのリセット

以下のいずれかのアクションが **24 時間** よりも前に実行した場合は、この手順が必要です。

- ポリシー サーバインストール ウィザードを使用してポリシー ストアを自動的に設定しました。
- XPSRegClient ユーティリティを使用して、SiteMinder スーパーユーザ認証情報をポリシー サーバにサブミットしました。

注: (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](#) (P. 598) します。

次の手順に従ってください:

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

siteminder_administrator

SiteMinder の管理者を指定します。以下の一部として 管理 UI をインストールする場合

- 新しい **12.52 SP1** 環境で、以下のデフォルト アカウントを指定します。

siteminder

- アップグレードの一部としてインストールする場合は、ポリシー ストア内でのスーパーユーザ権限のある SiteMinder 管理者アカウントを指定します。ポリシー ストア内でのスーパーユーザアカウントを持たない場合は、**smreg** ユーティリティを使用してデフォルト アカウントを作成します。

passphrase

SiteMinder 管理者アカウントのパスワードを指定します。

-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

(オプション) 管理 UI をインストールしてログインした後、登録処理を完了する必要がある時間を指定します。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： 1440 (24 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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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。

ユーティリティは、ポリシー サーバに管理者認証情報を提供します。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認証情報を使用します。

管理 UI をインストールする方法

以下のセクションでは、スタンドアロン インストール オプションの一部として、必須インストーラを使用して管理 UI をインストールする方法について説明します。

前提条件情報の確認

管理 UI をインストールする前に、以下の点を考慮してください。

- テクニカルサポートサイトで、インストール メディアを使用して 管理 UI をインストールします。

注: インストール メディア名のリストについては、「ポリシー サーバリリース ノート」を参照してください。

- インストールすべきスタンドアロン オプションを使用している場合には、以下の手順が適用されます。既存のアプリケーション サーバインフラストラクチャにインストールする場合は、「既存アプリケーションサーバへの管理 UI のインストール」を参照してください。
- (Windows) 管理 UI ホスト システムからインストーラを実行します。マップされたネットワーク共有または UNC パスからインストーラを実行しないでください。
- インストール zip は、必須インストーラおよび管理 UI インストーラを含みます。
 - Windows で必須インストーラを実行する場合は、両方の実行ファイルが同じ場所にあることを確認してください。必須インストーラは、インストールを完了させるために、自動的に 管理 UI インストーラを開始させます。
 - UNIX で必須インストーラを実行する場合は、両方の実行ファイルが同じ場所にあることを確認してください。ただし、インストールを完了させるために手動で 管理 UI インストーラを開始させます。必須インストーラは、自動的に 管理 UI インストーラを開始させません。
- インストール zip には、インストール メディアと同じレベルに `layout.properties` ファイルが含まれています。インストール zip を展開した後にインストール メディアを移動した場合、プロパティ ファイルを同じ場所に移動しないと、インストールに失敗します。
- (Red Hat Linux) Red Hat 6 オペレーティング システムはパフォーマンスのエントロピーに依存します。コンポーネントをインストールする前にエントロピーを増やします。十分なエントロピーがないと、インストールの完了までに非常に時間がかかることがあります。シンボリック リンクを設定するために、以下のコマンドを使用します。

```
mv /dev/random /dev/random.org
ln -s /dev/urandom /dev/random
```

- (UNIX) 権限に応じて、以下のコマンドを実行し、実行可能権限をインストールメディアが含まれるディレクトリに追加します。

```
chmod -R+x directory
```

directory

インストールメディアが存在するディレクトリを指定します。

- (UNIX) 別のサブネットにまたがって管理 UI インストーラを実行した場合、クラッシュすることがあります。ホストシステムに管理 UI を直接インストールします。

詳細情報:

[管理 UI のインストール](#) (P. 580)

管理 UI のインストールと登録(Windows)

必須インストーラを実行し、次に管理 UI インストーラを実行します。

次の手順に従ってください:

1. 実行中のすべてのアプリケーションを終了します。
2. インストールメディアに移動します。
3. *prerequisite_installation_media* をダブルクリックします。

prerequisite_installation_media

管理 UI 必須インストーラの実行ファイルを指定します。

インストーラが起動します。

4. [インストール] をクリックします。
必要なコンポーネントがインストールされます。
5. [終了] をクリックします。
管理 UI インストーラが起動します。
6. プロンプトに従って [インストール] をクリックします。
これで、管理 UI がインストールされました。SiteMinder 管理 UI のログイン画面が表示されます。
7. [ユーザ名] フィールドに、「siteminder」を入力します。

8. [パスワード] フィールドに、**siteminder** のアカウント パスワードを入力します。

注: スーパーユーザ アカウントのパスワードにドル記号 (\$) 文字が含まれている場合は、ドル記号文字の各インスタンスを **\$DOLLAR\$** に置換します。たとえば、**SiteMinder** スーパーユーザ アカウント パスワードが **\$password** の場合は、パスワード フィールドに「**\$DOLLAR\$password**」と入力します。

9. [サーバ] フィールドに、ポリシー サーバ ホストの完全修飾名を入力します。

以下の点を考慮します。

- 有効な **IPv4** アドレスまたは **IPv6** アドレスに入ることができます。
- ポートを指定しない場合、デフォルトのポリシー サーバ 認証ポートである **44442** がデフォルトで登録されます。

管理 UI が開き、ポリシー サーバに登録されます。

管理 UI のインストール (UNIX システム)

管理コンソールを提供するために、管理 UI および必須コンポーネントをインストールします。この手順では、UNIX システムに 管理 UI をインストールする方法について説明します。

これらの手順は **GUI** および **コンソール モード** をインストールするためのものです。2 つのモードの手順は同じですが、コンソール モードについては以下に示す例外があります。

- コンソール モードの手順には、コマンド **-i console** が含まれます。
- 対応する番号を入力して、オプションを選択します。
- 各手順の後に **ENTER** キーを押してプロセスを続行します。
- 前の手順に戻るには「**BACK**」を入力します。

次の手順に従ってください:

1. 実行中のすべてのアプリケーションを終了します。
2. シェルを開き、インストール メディアに移動します。
3. 以下のいずれかのコマンドを入力します。

GUI モード

```
./prerequisite_installation_media
```

コンソール モード

```
./prerequisite_installation_media -i console
```

```
prerequisite_installation_media
```

管理 UI 必須インストーラの実行ファイルを指定します。

インストーラが起動します。

4. [インストール] をクリックします。

必要なコンポーネントがインストールされます。管理 UI インストーラを実行するよう要求されます。

5. 以下のいずれかのコマンドを入力します。

GUI モード

```
./installation_media
```

コンソール モード

```
./installation_media -i console
```

```
installation_media
```

管理 UI インストーラの実行ファイルを指定します。

管理 UI インストーラが起動します。

6. プロンプトに従って [インストール] をクリックします。

これで、管理 UI がインストールされました。

注: 管理 UI は、ポリシー サーバに登録するまで使用できません。

UNIX インストールが完了したら、アプリケーション サーバを手動で開始させ、登録を完了するために 管理 UI にログインします。詳細については、「管理 UI の登録方法」を参照してください。

管理 UI インストールのトラブルシューティング

管理 UI インストールのトラブルシューティングには、以下のファイルを使用します。

- **Administrative_UI_Prerequisite_Installer_InstallLog.log**

スタンドアロンインストール オプションを使用した場合、このログには、前提条件のインストール中に発生した成功、警告、致命的でないエラー、およびエラーの数が示されます。個別のインストールアクションは、それぞれのステータスと共にリスト表示されます。

Location:

`administrative_ui_home¥CA¥SiteMinder¥adminui¥install_config_info`
`administrative_ui_home`

管理 UI インストールパスを指定します。

- **CA_SiteMinder_Administrative_UI_InstallLog.log**

このログには、管理 UI のインストール中に発生した成功、警告、致命的でないエラー、およびエラーの数が示されます。個別のインストールアクションは、それぞれのステータスと共にリスト表示されます。

Location:

`administrative_ui_home¥CA¥SiteMinder¥adminui¥install_config_info`
`administrative_ui_home`

管理 UI インストールパスを指定します。

管理 UI を登録する方法

SiteMinder オブジェクトの管理に使用できるようにするために、あらかじめ管理 UI を登録する必要があります。管理 UI を登録すると、管理 UI とポリシー サーバとの間に信頼できる接続が作成されます。以下の点を考慮します。

- (UNIX) アプリケーション サーバを手動で開始させ、登録を完了させるために管理 UI にログインするよう要求されます。
- (Windows) Windows に管理 UI をインストールした後、SiteMinder 管理 UI ログイン画面が表示され、アプリケーション サーバが自動的に開始されます。これらのアクションにより、すぐに管理 UI を登録することができます。インストール直後に管理 UI を登録しなかった場合は、以下のプロセスを完了します。

次の手順に従ってください:

1. r12.52 SP1 より前のバージョンの場合は、[FIPS 環境変数を作成します](#) (P. 476)。
2. [アプリケーション サーバを起動します](#) (P. 477)。
3. 管理 UI を登録します。

詳細情報:

[管理 UI を登録する方法](#) (P. 584)

FIPS 環境変数の作成

ユーザの環境が以下の基準を両方とも満たす場合、管理 UI を初めて登録するために FIP 環境変数を作成する必要があります。

- 登録しているポリシー サーバは FIP 専用モードで作動しています。
- 管理 UI は、ポリシー サーバホストシステムにインストールされません。

以下の手順に従います。

1. 以下のいずれかの操作を実行します。
 - (Windows) 管理者ユーザとして 管理 UI ホスト システムにログインします。
 - (UNIX) 管理 UI をインストールしたユーザとして 管理 UI ホスト システムにログインします。
2. 以下の環境変数を設定します。
`CA_SM_PS_FIPS140=ONLY`
注: 環境変数の設定の詳細については、お使いの OS のドキュメントを参照してください。
3. 管理 UI を正しく実行する Windows または UNIX シェルが
`CA_SM_PS_FIPS140` 変数を認識することを確認してください。

アプリケーション サーバの起動

管理 UI をインストールするためにスタンドアロン オプションを使用した場合には、以下の手順が適用されます。既存のアプリケーション サーバを備えたシステムに 管理 UI をインストールした場合は、既存のアプリケーション サーバに 管理 UI をインストールするための手順に進んでください。

アプリケーション サーバを起動する方法

1. 管理 UI ホスト システムから、以下のいずれかを実行します。
 - **Windows** - Microsoft Services コンソールを開きます。
Windows に 管理 UI がインストールされると、アプリケーション サーバが自動的に開始されます。インストール後にアプリケーション サーバを開始させる必要はありません。
 - **UNIX** - `install_home/CA/siteminder/adminui/bin` に移動します。
`install_home`
管理 UI インストールパスを指定します。

2. 以下のいずれかを実行します。

- **Windows** - SiteMinder 管理 UI サービスを開始させます。
- **UNIX** - 「run.sh」を入力し、Enter キーを押します。

アプリケーション サーバが開始されます。

詳細情報:

[既存アプリケーションサーバへの 管理 UI のインストール \(P. 569\)](#)

[アプリケーションサーバの起動 \(P. 589\)](#)

管理 UI の登録

環境の管理を始めるために、ポリシー サーバに 管理 UI を登録します。

次の手順に従ってください:

1. 以下のいずれかの操作を実行します。

■ Windows の場合 :

- (推奨) 管理 UI ショートカットを使用して 管理 UI を開きます。ショートカットを使用するには、SSL を介して 管理 UI を登録します。ショートカットへのアクセス権がない場合は、Web ブラウザを開き以下の場所に移動します。

`https://host:8443/iam/siteminder/adminui`

注: 10 年間有効な自己署名証明書が作成され、接続に使用されます。証明書は RSA 2048 キーの強度で作成されます。

- Web ブラウザを開き、以下の場所に移動します。

`http://host:8080/iam/siteminder/adminui`

■ UNIX の場合 :

- (推奨) SSL を介して 管理 UI を登録するには、Web ブラウザを開き以下の場所に移動します。

`https://host:8443/iam/siteminder/adminui`

- ブラウザを開き、以下の場所に移動します。

`http://host:8080/iam/siteminder/adminui`

注: ホスト システムに Web ブラウザがない場合には、ログイン画面にリモート アクセスすることもできます。

host

管理 UI ホスト システムの完全修飾名を指定します。

SiteMinder 管理 UI のログイン画面が表示されます。

2. [ユーザ名] フィールドに以下の値を入力します。

`siteminder`

3. [パスワード] フィールドに、SiteMinder スーパーユーザアカウントのパスワードを入力します。

注: スーパーユーザアカウントのパスワードにドル記号 (\$) 文字が含まれている場合は、ドル記号文字の各インスタンスを `$DOLLAR$` に置換します。たとえば、SiteMinder スーパーユーザアカウントパスワードが `$password` の場合は、パスワードフィールドに「`$DOLLAR$password`」と入力します。

4. [サーバ] フィールドに、ポリシー サーバ ホストの完全修飾名を入力します。

以下の点を考慮します。

- 有効な IPv4 アドレスまたは IPv6 アドレスに入ることができます。
- ポートを指定しない場合、デフォルトのポリシー サーバ認証ポートである **44442** がデフォルトで登録されます。

管理 UI が開き、ポリシー サーバに登録されます。

詳細情報:

[「ファイルに登録がありません」エラーが表示される](#) (P. 611)

[HTTPS を使用した 管理 UI の登録](#) (P. 480)

HTTPS を使用した 管理 UI の登録

HTTPS を使用して 管理 UI を登録する場合は、アプリケーション サーバの context.xml ファイルを変更して安全な Cookie を有効にします。

次の手順に従ってください:

1. アプリケーション サーバをシャットダウンします。
2. 以下の場所に移動します。

`user_console.war¥WEB-INF`

3. context.xml ファイルを開きます。
4. 以下のパラメータを SessionCookie タグに追加します。

`secure="true"`

5. ファイルを保存して閉じます。
6. アプリケーション サーバを再起動します。

context.xml ファイルが更新され、安全な Cookie が有効化されます。

詳細情報:

[アプリケーション サーバの起動 \(P. 477\)](#)

[アプリケーション サーバを停止します。 \(P. 481\)](#)

アプリケーション サーバを停止します。

管理 UI をインストールするためにスタンドアロン オプションを使用した場合には、以下の手順が適用されます。既存のアプリケーション サーバを備えたシステムに 管理 UI をインストールした場合は、既存のアプリケーション サーバに 管理 UI をインストールするための手順に進んでください。

アプリケーション サーバを停止する方法

1. 管理 UI ホストから、以下のいずれかを実行します。
 - **Windows** - Microsoft Services コンソールを開きます。
 - **UNIX** - `install_home/CA/siteminder/adminui/bin` に移動します。
`administrative_ui_install`
管理 UI インストールパスを指定します。
2. 以下のいずれかを実行します。
 - **Windows** - SiteMinder 管理 UI サービスを停止します。
 - **UNIX** - 「shutdown.sh」を入力し、Enter キーを押します。
アプリケーション サーバが停止します。

詳細情報:

[既存アプリケーション サーバへの 管理 UI のインストール \(P. 569\)](#)
[アプリケーション サーバを停止します。 \(P. 592\)](#)

管理者認証情報

デフォルトでは、管理 UI は SiteMinder 管理者認証情報用のソースとしてポリシー ストアを使用します。たとえばコーポレート ディレクトリのような外部ストアを使用するために、管理 UI を設定することができます。

注: 外部管理者ユーザ ストアの設定の詳細については、「ポリシー サーバ 設定ガイド」を参照してください。

(オプション)高可用性向けの追加の 管理 UI のインストールと設定

予期しない機能停止で SiteMinder オブジェクトの管理が妨げられないように、複数の 管理 UI をインストールします。別の 管理 UI をインストールする前に、以下を考慮します。

- まだ 管理 UI との信頼できる接続を共有していないポリシー サーバに、管理 UI を登録します。別のポリシー サーバに登録することで、1 つのポリシー サーバが機能停止しても両方の GUI が無効になることはありません。
- 管理 UI は、複数のポリシー サーバにフェールオーバーできません。ただし、複数のポリシー サーバを管理するために 管理 UI を設定することができます。
- 既存の 管理 UI が外部 SiteMinder 管理者認証に対して設定されている場合。
 - 同じ外部ストアで新しい 管理 UI を設定します。同じ外部ストアを使用して新しい 管理 UI の設定することにより、すべての SiteMinder 管理者がすべての GUI で利用可能になります。
 - 同じネットワーク識別子を使用して同じ外部ストアへの後続の 管理 UI 接続を設定してください。同じ外部ストアへの複数の 管理 UI 接続で異なるネットワーク識別子を使用することはサポートされていません。

例：最初の接続で 172.16.0.0 を設定した場合は、後続の接続の作成でも 172.16.0.0 を使用します。最初の接続で comp001@example.com を設定した場合は、後続の接続の作成でも comp001@example.com を使用します。

管理 UI 用の追加のポリシー サーバ接続

デフォルトでは、管理 UI は単一のポリシー サーバで設定されます。追加のポリシー サーバ接続を設定して、管理 UI からこれらのサーバを管理できます。たとえば、開発およびステージングの環境で、ポリシー サーバを管理するための接続を作成することができます。

複数のポリシー サーバに接続する 管理 UI については、外部管理者ストアを使用します。外部ユーザ ストアは、追加のポリシー サーバを接続する場合の要件です。ストアに管理者 ID 用の管理者アカウントを作成します。このアカウントにより、管理 UI で、外部ストアに管理者レコードを置けるようになります。

管理者ストアおよび外部管理者ストアの詳細については、「[ポリシーサーバ設定ガイド](#)」を参照してください。

次の手順に従ってください:

1. 管理 UI から外部管理者ユーザ ストアへの接続を設定します。

注: 管理 UI が管理者アイデンティティのソースとしてポリシー ストアを使用している場合は、追加のポリシー サーバ接続を設定することができません。

2. 登録ツールを実行します。
3. ポリシー サーバへの接続を設定します。

管理 UI 登録ツールの実行

クライアント名とパスフレーズを作成するには、管理 UI 登録ツールを実行します。クライアント名とパスフレーズの組み合わせは、登録する 管理 UI を識別するためにポリシー サーバが使用する値です。登録処理を完了するには、管理 UI からクライアントとパスフレーズの値をサブミットします。

登録ツールを実行する方法

1. ポリシー サーバ ホスト システムからコマンド プロンプトを開きます。
2. 以下のコマンドを実行します。

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

注: *client_name* と *[:passphrase]* の間にスペースを挿入すると、エラーが発生します。

client_name

登録する 管理 UI を識別します。

制限： この値は一意である必要があります。たとえば、管理 UI の登録にすでに `smui1` を使用している場合は、「`smui2`」と入力します。

注： この値は記録しておいてください。この値は、管理 UI から登録処理を完了するときに使用します。

passphrase

管理 UI の登録の完了に必要なパスワードを指定します。

制限：

- パスフレーズは 6 文字以上にする必要があります。
- パスフレーズには、アンパサンド (&) またはアスタリスク (*) を含めることができません。
- パスフレーズにスペースが含まれる場合、引用符で囲む必要があります。
- 管理 UI をアップグレードの一部として登録する場合、以前のパスフレーズを再利用できます。

注： この手順でパスフレーズを指定しない場合、`XPSRegClient` でパスフレーズの入力と確認が求められます。

重要： パスフレーズを記録して、後で参照できるようにします。

-adminui

管理 UI の登録を指定します。

-t timeout

(オプション) 管理 UI からの登録処理を完了する必要がある時間を指定します。タイムアウト値に到達すると、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 (1 日)

-r retries

(オプション) 管理 UI からの登録処理を完了するまでに許容される試行の失敗回数を指定します。登録処理時にポリシー サーバに間違ったクライアント名またはパスフレーズをサブミットすると、登録に失敗することがあります。

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。登録ツール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

(オプション)。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。

登録ログ ファイルの名前が一覧表示され、パスフレーズが求められます。

3. Enter キーを押します。

登録ツールにより、クライアント名およびパスフレーズの組み合わせが作成されます。

これで、ポリシー サーバに 管理 UI を登録できるようになりました。管理 UI からの登録処理が完了しました。

登録情報の収集

管理 UI では、ユーザがポリシー サーバに登録するために、登録処理に関する具体的情報が必要です。

管理 UI にログインする前に、以下の情報を集めます。

- クライアント名 - XPSRegClient ツールを使用して指定したクライアント名。
- パスフレーズ - XPSRegClient ツールを使用して指定したパスフレーズ。
- ポリシー サーバ ホスト - ポリシー サーバ ホスト システムの IP アドレスまたは名前。
- ポリシー サーバの認証ポート - ポリシー サーバが認証リクエストをリスニングするポート。

デフォルト : 44442

ポリシー サーバへの接続設定

管理 UI を SiteMinder オブジェクトの管理に使用できるようにするために、接続を設定します。

ポリシー サーバ接続を設定する方法

1. スーパーユーザ権限を持つアカウントで管理 UI にログインします。
2. [管理] - [管理 UI] をクリックします。
3. [ポリシー サーバ接続] - [ポリシー サーバ接続の登録] をクリックします。
4. [名前] フィールドに接続名を入力します。
5. [ポリシー サーバ ホスト] フィールドにポリシー サーバのホスト名または IP アドレスを入力します。
6. [ポリシー サーバ ポート] フィールドに、ポリシー サーバ認証ポートを入力します。

注: この値は、ポリシー サーバ管理コンソールの [設定] タブにある [認証ポート] (TCP) フィールドの値と一致する必要があります。デフォルトの認証ポートは **44442** です。ポート番号を決定するために、ポリシー サーバ管理コンソールの [設定] タブを開きます。

7. それぞれのフィールドに、登録ツールを使用して作成したクライアント名およびパスフレーズを入力します。
8. FIPS モードを選択します。
 - FIPS 互換モードでポリシー サーバをインストールした場合には、互換モードを選択します。
 - 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には、専用モードを選択します。
9. [サブミット] をクリックします。

管理 UI とポリシー サーバとの間の接続が設定されます。

管理 UI ログイン画面は、管理 UI が登録されるポリシー サーバのリストを含んでいます。デフォルトでは、最初に登録されたポリシー サーバはデフォルト接続です。

デフォルト ポリシー サーバ接続の変更

管理 UI ログイン画面は、管理 UI が登録されるポリシー サーバのリストを含んでいます。デフォルトでは、最初に登録されたポリシー サーバがデフォルト接続として表示されます。リストを変更し、別のポリシー サーバ接続をデフォルトとして表示できます。

次の手順に従ってください:

1. [管理] - [管理 UI] をクリックします。
2. [ポリシー サーバ接続] - [ポリシー サーバ接続の変更] をクリックします。
3. 検索条件を指定し、[検索] をクリックします。
条件と一致する 管理 UI 接続が表示されます。
4. 目的の接続を選択し、[選択] をクリックします。
5. [詳細] グループ ボックス内の矢印アイコンをクリックします。
6. [デフォルト接続] チェック ボックスをオンにし、[サブミット] をクリックします。
ポリシー サーバ接続がデフォルト接続として設定されます。

ポリシー サーバ接続の削除

管理 UI ログイン画面は、管理 UI が登録されるポリシー サーバのリストを含んでいます。接続が必要でなくなった場合には、リストから削除するためにポリシー サーバ接続を削除します。

次の手順に従ってください:

1. [管理] - [管理 UI] をクリックします。
2. [ポリシー サーバ接続] - [ポリシー サーバ接続の削除] をクリックします。
3. 検索条件を指定し、[検索] をクリックします。
条件と一致する 管理 UI 接続が表示されます。

4. 目的の接続を選択し、[選択] をクリックします。
接続を削除してもかまわないか確認するように促されます。
5. [はい] をクリックします。
ポリシー サーバへの接続が削除されます。

(オプション) 管理 UI のアンインストール

システムで不用になった場合は、管理 UI をアンインストールします。

注: 管理 UI をインストールするためにスタンドアロン オプションを使用した場合には、以下の手順が適用されます。既存のアプリケーション サーバを備えたシステムに 管理 UI をインストールした場合は、既存のアプリケーション サーバに 管理 UI をインストールするための手順に進んでください。

次の手順に従ってください:

1. アプリケーション サーバを停止します。
2. Windows の [コントロール パネル] を開き、プログラムのリストに移動します。
3. CA SiteMinder 管理 UI を右クリックします。
4. [アンインストール/変更] をクリックします。
5. ウィザードの指示に従います。

注: 共有ファイルを削除するように促される場合は、[すべていいえ] をクリックします。

6. 要求された場合はシステムを再起動します。
7. Windows の [コントロール パネル] を開き、プログラムのリストに移動します。
8. 管理 UI 必須インストーラを右クリックします。

9. ウィザードの指示に従います。

注: 共有ファイルを削除するように促される場合は、[すべていいえ]をクリックします。

10. 要求された場合はシステムを再起動します。

管理 UI および必要なサードパーティ コンポーネントがアンインストールされます。

詳細情報:

[既存アプリケーションサーバへの 管理 UI のインストール \(P. 569\)](#)

[Windows での 管理 UI のアンインストール \(P. 594\)](#)

UNIX 上の 管理 UI のアンインストール

システムで不用になった場合は、管理 UI をアンインストールします。

以下の点を考慮します。

- このコンポーネントをアンインストールする際には、手動でインストールディレクトリを削除しません。アンインストールシェルスクリプトを実行します。インストールディレクトリのみを削除すると、関連するレジストリはそのまま残されます。このホストシステムにこのコンポーネントを再インストールしようとする場合、エントリは成功したインストールを回避できます。
- 管理 UI をインストールするためにスタンドアロン オプションを使用した場合には、以下の手順が適用されます。既存のアプリケーションサーバを備えたシステムに 管理 UI をインストールした場合は、既存のアプリケーションサーバに 管理 UI をインストールするための手順に進んでください。

以下の手順に従います。

1. アプリケーションサーバを停止します。
2. シェルを開き、以下に移動します。

```
administrative_ui_home/CA/SiteMinder/adminui/install_config_info
```

```
administrative_ui_home
```

管理 UI 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。

```
./sm-wamui-uninstall.sh
```

管理 UI を削除するプロセスが開始されます。

4. プロンプトに従って、管理 UI をアンインストールします。

管理 UI がアンインストールされる時、インストーラはプロンプトを表示します。

5. コマンド ウィンドウを開き、以下に移動します。

```
administrative_ui_home/CA/SiteMinder/webadmin/install_config_info
```

```
administrative_ui_home
```

管理 UI インストールパスを指定します。

6. 以下のコマンドを実行します。

```
./prerequisite-uninstall.sh
```

7. プロンプトに従って、管理 UI の必須コンポーネントをアンインストールします。

サードパーティ コンポーネントがアンインストールされる時、インストーラはプロンプトを表示します。

管理 UI および必要なサードパーティ コンポーネントがアンインストールされます。

詳細情報:

[既存アプリケーションサーバへの 管理 UI のインストール \(P. 569\)](#)

Web エージェント インストールのためのポリシー サーバの準備

Web エージェントをインストールする前に、以下を完了している必要があります。

- ポリシー サーバのインストール
- ポリシー サーバと通信するためのポリシー ストアおよびキー ストアの設定

- 管理 UI のインストールおよび登録
- Web エージェントをインストールするシステムとポリシー サーバが通信できることの確認

ユーザが Web エージェントのサイトでトラステッドホストを登録するには、その前に、以下のオブジェクトを管理 UI で設定する必要があります。

注: 以下の各オブジェクトの設定の詳細については、「ポリシー サーバ構成ガイド」を参照してください。

エージェントを集中管理するには、管理 UI を使用して、以下を設定します。

- **トラステッドホストを登録する権限を持つ SiteMinder 管理者** - トラステッドホストは 1 つ以上の SiteMinder Web エージェントがインストールされているクライアント コンピュータです。トラステッドホストは、物理システムを指します。トラステッドホストを登録する権限を持つ管理者がいる必要があります。デフォルト SiteMinder 管理者はこの権限を持っています。
- **エージェント識別情報** - エージェント識別情報により、Web エージェントをホストしている Web サーバインスタンスの名前と IP アドレスの間にマッピングが確立されます。管理 UI でエージェントオブジェクトからのエージェント識別情報を定義します。エージェント識別情報に名前を割り当て、エージェントタイプを Web エージェントとして指定します。

注: エージェントに割り当てる名前は、エージェント設定オブジェクトの DefaultAgentName パラメータで指定するのと同じ名前です。

- **ホスト設定オブジェクト** - トラステッドホストとポリシー サーバの間の最初の接続が確立された後、ホスト設定オブジェクトによって、トラステッドホストとポリシー サーバの間の通信が定義されます。

ホスト設定オブジェクトとトラステッドホスト設定ファイル

(SmHost.conf) を混同しないでください。SmHost.conf は、ホスト登録の成功後にトラステッドホストでインストールされます。

SmHost.conf ファイル内の設定によってポリシー サーバにホストが接続されるのは最初の接続のみです。後の接続は、ホスト設定オブジェクトによって管理されます。

- エージェント設定オブジェクト - エージェント設定オブジェクトには、Web エージェント設定を定義するパラメータが含まれています。以下に示す基本的な操作のために、いくつかの必須パラメータを設定する必要があります。

注: エージェント パラメータの詳細については、「Web エージェント 設定ガイド」を参照してください。

- すべてのエージェントについて - エージェント設定オブジェクトには、DefaultAgentName の値が含まれている必要があります。DefaultAgentName は、エージェント オブジェクトで指定したエージェント識別名と一致している必要があります。DefaultAgentName は、Web エージェントがその Web サーバ上でエージェント識別情報が割り当てられていない IP アドレスを検出したときに使用するエージェント識別情報を識別します。
- Domino Web エージェントについて - エージェント設定オブジェクトには、以下のパラメータの値が含まれている必要があります。
 - DominoDefaultUser - ユーザが Domino ディレクトリに含まれず、SiteMinder によって別のユーザディレクトリに対して認証されている場合、Domino Web エージェントはこの名前を使用して、ユーザを Domino サーバに対して識別します。DominoDefaultUser 値は暗号化できます。
 - DominoSuperUser - SiteMinder に正常にログインしたすべてのユーザが、DominoSuperUser として Domino にログインされていることを確認します。DominoSuperUser 値は暗号化できます。
- IIS Web エージェント - エージェント設定オブジェクトは、DefaultUserName と DefaultPassword のパラメータの値を含んでいる必要があります。DefaultUserName と DefaultPassword は、SiteMinder で保護されている IIS Web サーバ上のリソースにアクセスするための十分な権限を持つ既存の NT ユーザ アカウントを識別します。SiteMinder で保護されている IIS Web サーバのリソースにアクセスする必要があるユーザが、必要なサーバアクセス権限を持っていないことがあります。Web エージェントが、SiteMinder によってアクセスを許可されたユーザのプロキシユーザアカウントとして機能するためには、管理者によって事前に割り当てられた Windows アカウントを使用する必要があります。

注: NTLM 認証方式を使用する場合、または Windows ユーザセキュリティ コンテキスト機能を有効にする場合には、これらの IIS Web エージェント パラメータに値を指定しないでください。

第 9 章: レポートのインストール

このセクションには、以下のトピックが含まれています。

- [インストール ロードマップ](#) (P. 495)
- [インストール チェックリストのレポート](#) (P. 496)
- [レポートの考慮事項](#) (P. 503)
- [レポート インストールのしくみ](#) (P. 505)
- [レポート サーバをインストールする方法](#) (P. 506)
- [レポート テンプレートをインストールする方法](#) (P. 521)
- [レポート サーバを登録する方法](#) (P. 527)
- [監査データベースを設定する方法](#) (P. 536)
- [レポート スケジューラの開始](#) (P. 539)
- [レポート サーバの停止](#) (P. 540)
- [レポートをアンインストールする方法](#) (P. 542)
- [管理 UI へのレポート サーバ接続の削除](#) (P. 547)
- [レポート サーバの再インストール](#) (P. 547)

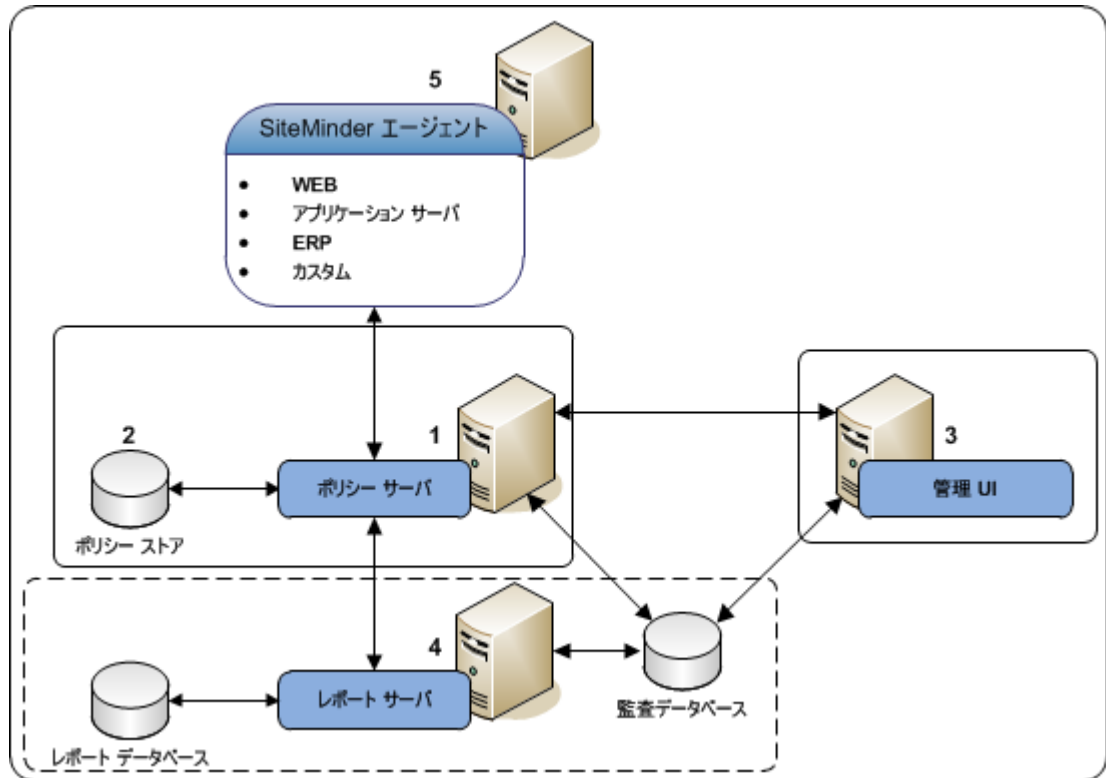
インストール ロードマップ

以下の図はサンプル SiteMinder のインストールを示しており、各コンポーネントのインストールおよび設定の指示がリスト表示されています。

- 実線で囲まれているのは、レポートのインストールおよび設定前に必要なコンポーネントです。これらには、以下のコンポーネントが含まれます。
 - ポリシー サーバ
 - ポリシー ストア
 - ポリシー サーバに登録された 管理 UI
- 点線で囲まれているのは、今からインストールおよび設定するコンポーネントです。これらには、以下のコンポーネントが含まれます。
 - レポート サーバ
 - レポート データベース

- SiteMinder 監査データベース

図3: レポート サーバインストール ロードマップ



インストール チェックリストのレポート

以下の確認のために、レポート サーバおよびレポート データベース チェックリストを確認します。

- 環境が最小のオペレーティング システムおよびデータベース要件を満たしている
- 要件となる設定を完了している

レポート サーバ

- レポート サーバ ホスト システムが最小のオペレーティング システム要件を満たすことを確認してください。
 - [Windows](#) (P. 27)
 - UNIX
- (Solaris) レポート サーバ ホスト システムに、必要なオペレーティング システムのパッチをインストールします。

注: 詳細については、「ポリシー サーバ リリース ノート」を参照してください。
- レポート サーバ ホストが[接続要件](#) (P. 30) を満たすことを確認してください。
- レポート サーバ ホスト名には以下の文字がいずれも含まれないようにしてください。
 - アンダースコア (_)
 - ピリオド (.)
 - スラッシュ (/) または円記号 (¥)
- レポート サーバを再インストールする場合は、現在のインスタンスをアンインストールします。既存のインスタンスに上書きしてインストールしようとする、インストールは失敗します。
- Windows インストール
 - ローカル管理者グループのメンバであるユーザアカウントにアクセスできることを確認してください。 インストーラを実行するユーザアカウントは、ローカル管理者グループのメンバである必要があります。

重要: デフォルトの **Windows** セキュリティ設定がローカル管理者グループ用に変更されたシステムへのインストールは、サポートされていません。
 - インストールされるシステムがドメイン コントローラではないことを確認してください。 ドメイン コントローラへのインストールは、サポートされていません。
- UNIX インストール
 - IP 解決の問題を回避するため、レポート サーバ ホスト IP が `/etc/hosts` ファイルに正しく設定されていることを確認してください。

- root ユーザ アカウントおよび非 root ユーザ アカウントにアクセスできることを確認してください。 インストールを開始するためには root ユーザ アカウントを必要とし、インストールを完了させるためには非 root ユーザ アカウントを必要とします。 非 root ユーザ アカウントが以下であることを確認してください。
 - 有効なホーム ディレクトリの所有者である。
 - ホーム ディレクトリへの書き込み権限がある。
- 以下のコマンドおよびユーティリティがオペレーティング システムにインストールされており、root ユーザ アカウント用の PATH 環境変数で使用可能であることを確認してください。
 - /bin/sh
 - uname
 - awk
 - tar
 - stty
 - pwd
 - expr
 - chown
 - id
 - ulimt
 - read
 - hostname
 - grep
 - dirname
 - which
 - touch
 - sed
 - tail
 - gzip

- root ユーザアカウント用の PATH 環境変数に、コア システムのコマンドライン ツールの GNU やサードパーティ製のそれに相当するものが含まれていないこと、またはこのツールの個別にダウンロードおよびコンパイルされたバージョンが含まれていないことを確認してください。
- 以下の変数の少なくとも 1 つを、有効な utf8/UTF-8 ロケールに設定します。
 - LC_ALL
例 : export LC_ALL=en_US.UTF-8
 - LANG
例 : export LANG=en_US.UTF-8
 - LC_CTYPE
例 : export LC_CTYPE=en_US.UTF-8

レポート データベースおよび監査データベース

- 埋め込みの MySQL バージョンを使用していない場合
 - データベース サーバ ホスト システムに、固定されたホスト名が使用されていることを確認します。
 - サポートされるデータベースを [レポート データベース](#) (P. 29) として使用していることを確認します。
 - 新しい空のデータベースが使用可能であることを確認します。
 - データベース クライアントおよびサーバが UTF8 文字エンコーディングを使用するよう設定されていることを確認します。
Unicode 設定に必要な設定の詳細については、ベンダー固有のドキュメントを参照してください。
- (SQL Server) SQL Server をレポート データベース、監査データベースまたはその両方として使用する場合は、レポート サーバ ホスト システム上で以下の処理を実行します。
 - SiteMinder がサポートする SQL Server ドライバを、必ずレポート サーバ ホスト システムにインストールしてください。
 - 各データベースを識別するデータ ソース名 (DSN) を作成します。
レポート サーバは、各データベースと通信するために DSN を使用します。

- (Oracle) レポート データベース、監査データベース、またはその両方に Oracle を使用している場合：

- レポート サーバ ホスト システムで以下の処理を実行します。
 - サポートされた Oracle Net クライアントがインストールされていることを確認します。
 - Oracle Net サービス名を使用して、tnsnames.ora ファイル内に各データベースを特定します。レポート サーバは、このサービス名を使用して各データベースと通信します。
 - NLS_LANG 変数を以下の UTF-8 設定のいずれかに設定します。
 - AMERICAN_AMERICA.WE8MSWIN1252
 - AMERICAN_AMERICA.AL32UTF8
 - ORACLE_HOME 変数を *Oracle_Net_client* に設定します。

Oracle_Net_client

Oracle Net クライアントのインストールパスを指定します。

Windows の例： C:\oracle\product\10.2.0\client

UNIX の例： export

ORACLE_HOME=/opt/oracle/product/10.2.0/client1

- (Windows) ORACLE_HOME 変数をシステム環境変数に追加します。

例： %Oracle_Home%\bin

- (UNIX) LD_LIBRARY_PATH 変数を \$ORACLE_HOME/lib32:\$ORACLE_HOME/lib に設定します。

例：

LD_LIBRARY_PATH=\$ORACLE_HOME/lib32:\$ORACLE_HOME/lib:\$LD_LIBRARY_PATH

- (UNIX) パス変数を \$ORACLE_HOME/bin:\$PATH に設定します。

例： export PATH=\$ORACLE_HOME/bin:\$PATH

- データベース サーバ ホスト システム上で次の処理を行います：
NLS_LANG 変数を以下の UTF-8 設定のいずれかに設定します。
 - AMERICAN_AMERICA.WE8MSWIN1252
 - AMERICAN_AMERICA.AL32UTF8

レポート データベースおよび監査データベース

- 埋め込みの MySQL バージョンを使用していない場合
 - データベース サーバ ホスト システムに固定のホスト名が使用されていることを確認します。
 - サポートされているデータベースを[レポート データベース](#) (P. 29) として使用していることを確認します。
 - 新しい空のデータベースが使用可能であることを確認します。
 - データベース クライアントおよびサーバが **UTF-8** 文字エンコーディングを使用するように設定されていることを確認します。
Unicode 設定に必要な設定の詳細については、ベンダー固有のドキュメントを参照してください。
- (SQL Server) SQL Server をレポート データベース、監査データベースまたはその両方として使用する場合は、レポート サーバ ホスト システム上で以下の処理を実行します。
 - SiteMinder がサポートする SQL Server ドライバがレポート サーバ ホスト システムにインストールされていることを確認します。
 - 各データベースを識別するデータ ソース名 (DSN) を作成します。
レポート サーバは、各データベースと通信するために DSN を使用します。
 - データベースで UTF-8 文字エンコーディングが有効であることを確認します。 Unicode 設定に必要な設定の詳細については、SQL Server のドキュメントを参照してください。

- (Oracle) レポート データベース、監査データベース、またはその両方に Oracle を使用している場合：

- レポート サーバ ホスト システムで以下の処理を実行します。

- サポートされている **Oracle Net** クライアントがインストールされていることを確認します。
- データベース クライアントおよびサーバが **UTF-8** 文字エンコーディングを使用するように設定されていることを確認します。Unicode 設定に必要な設定の詳細については、ベンダー固有のドキュメントを参照してください。
- **Oracle Net** サービス名を使用して、**tnsnames.ora** ファイル内に各データベースを特定します。レポート サーバは、このサービス名を使用して各データベースと通信します。
- **NLS_LANG** 変数を以下の **UTF-8** 設定のいずれかに設定します。
 - **AMERICAN_AMERICA.WE8MSWIN1252**
 - **AMERICAN_AMERICA.AL32UTF8**
- **ORACLE_HOME** 変数を *Oracle_Net_client* に設定します。

Oracle_Net_client

Oracle Net クライアントのインストールパスを指定します。

Windows の例： C:¥oracle¥product¥10.2.0¥client

UNIX の例： export

ORACLE_HOME=/opt/oracle/product/10.2.0/client1

- (Windows) **ORACLE_HOME** 変数をシステム環境変数に追加します。

例： %Oracle_Home%¥bin

- (UNIX) **LD_LIBRARY_PATH** 変数を
\$ORACLE_HOME/lib32:\$ORACLE_HOME/lib に設定します。

例：

LD_LIBRARY_PATH=\$ORACLE_HOME/lib32:\$ORACLE_HOME/lib:\$LD_LIBRARY_PATH

- (UNIX) パス変数を **\$ORACLE_HOME/bin:\$PATH** に設定します。

例： export **PATH**=\$ORACLE_HOME/bin:\$PATH

- データベース サーバ ホスト システム上で次の処理を行います：
NLS_LANG 変数を以下の UTF-8 設定のいずれかに設定します。
 - AMERICAN_AMERICA.WE8MSWIN1252
 - AMERICAN_AMERICA.AL32UTF8

レポートの考慮事項

レポート サーバをインストールする前に、以下の点を考慮します。

- 他の SiteMinder コンポーネントを備えたホスト システムにレポート サーバをインストールすることはサポートされていません。別のホスト システムにレポート サーバをインストールしてください。
- UNIX インストールには数時間かかる場合があります。インストールの前に、ページサイズを 4GB またはそれ相当の RAM サイズに増やしてください。インストールが 4 時間より長くかかる場合は、インストールを停止し、ページサイズを増やします。
- レポート サーバ ホスト システムに JBoss がインストールされる場合、ポートのコンフリクトが発生する場合があります。レポート サーバのインストール後にポートのコンフリクトが発生した場合、以下のファイル内に JBoss ポート情報を置くことができます。

- jboss-service.xml

デフォルトの場所：*jboss_home*¥*server*¥*server_configuration*¥*conf*

- server.xml

デフォルトの場所：

jboss_home¥*server*¥*server_configuration*¥*deploy*¥*jbossweb-tomcat55.sar*

jboss_home

JBoss のインストールパスを指定します。

server_configuration

サーバ設定の名前を指定します。

デフォルト値：default

注: これらのファイルのどちらかを変更する場合は、JBoss を再起動します。詳細については、Red Hat のドキュメントを参照してください。

- service-bindings.xml

スタンドアロン オプションを使用して、管理 UI がレポート サーバ
ホスト システムにインストールされた場合、このファイルはただ
存在しているだけです。

デフォルトの場所: *administrative_ui_install¥webadmin¥conf*
administrative_ui_installation

管理 UI インストールパスを指定します。

注: このファイルを変更する場合は、管理 UI アプリケーション
サーバを再起動します。

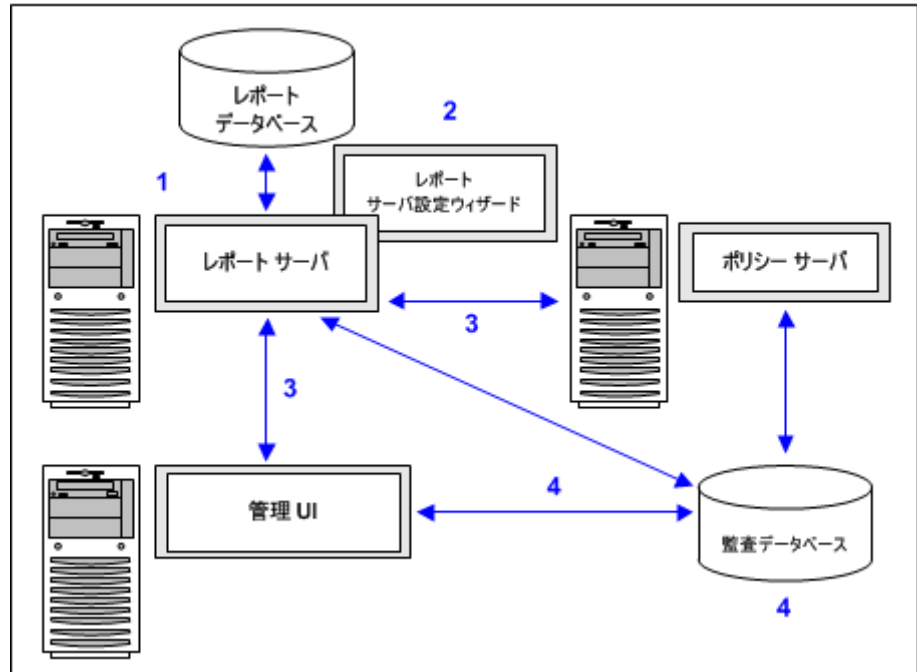
詳細情報:

[アプリケーションサーバの起動](#) (P. 477)

[アプリケーションサーバを停止します。](#) (P. 481)

レポート インストールのしくみ

SiteMinder レポート機能は、SiteMinder ポリシー分析および監査ベースのレポートを管理するために、レポートサーバ、レポートデータベースおよび SiteMinder 監査データベースのインストールおよび設定を必要とします。以下の図はサンプル SiteMinder 環境を詳述しており、各コンポーネントのインストールまたは設定の指示がリスト表示されています。



以下のリストで、示された各ステップについて説明します。

1. **レポート サーバのインストール** - レポート サーバのインストールがプロセスの第 1 段階です。インストール中にレポート データベースを設定します。
2. **SiteMinder レポート テンプレートのインストール** - SiteMinder レポート テンプレートのインストールがプロセスの第 2 段階です。
SiteMinder レポート サーバ 設定ウィザードは、1 セットの SiteMinder ポリシー分析および監査レポート テンプレートを使用するために、レポート サーバを設定します。
3. **レポート サーバの登録** - レポート サーバの登録がプロセスの第 3 段階です。登録には、以下の間の接続設定が必要です。
 - レポート サーバおよびポリシー サーバ
 - レポート サーバおよび管理 UI

4. **SiteMinder 監査データベースの設定** - SiteMinder 監査データベースの設定がプロセスの第 4 段階です。監査ベースのレポートを実行するために、管理 UI に登録された個別の SiteMinder 監査データベースが必要です。

レポート サーバをインストールする方法

レポート サーバをインストールするには、以下の手順に従います。

1. インストール チェックリストを確認します。
2. インストーラ用の情報を収集します。
3. レポート サーバをインストールします。

インストーラのための情報の収集

レポート サーバ インストーラが必要とする情報を識別するために、以下のセクションを確認します。

インストール認証情報

インストールするオペレーティング システムによって、インストーラは以下のような認証情報を必要とします。

- **(Windows および UNIX) BusinessObjects 管理者パスワード**

インストーラは、デフォルトの SAP BusinessObjects Enterprise 管理者アカウント (administrator) を作成します。このアカウントを使用して、SiteMinder レポート テンプレートをインポートし、BusinessObjects Content Management Console にアクセスします。このアカウントのパスワードを決定します。

パスワードは以下の構成基準を満たす必要があります：

- パスワードは 6 文字以上である必要があります。
- パスワードは、どのような形であっても「administrator」という語を含むことはできません。

- パスワードには、以下の文字タイプのうち少なくとも 2 種類を含む必要があります。
 - 大文字
 - 小文字
 - 数字
 - 記号
- (UNIX) 非 root ユーザ アカウント - インストールを開始するためには root ユーザ アカウントを必要とし、インストールを完了させるためには非 root ユーザ アカウントを必要とします。以下のように、非 root ユーザ アカウントを識別します。
 - User name
 - グループ名

MySQL レポート データベース

埋め込みの MySQL バージョンをレポート データベースとして使用する場合、インストーラは以下の情報を必要とします。 インストールを開始する前に、レポート データベース インストール ワークシートを使用して以下の情報を収集します。

- **MySQL root パスワード**
MySQL root ユーザ アカウントのパスワード
注: root ユーザ アカウントの名前を変更することはできません。 インストーラは、名前をデフォルトで **root** にします。
- **ユーザ**
レポート データベース管理者アカウントの名前。
インストーラ デフォルト : sa
- **パスワード**
レポート データベース管理者アカウントのパスワード。

SQLAnywhere レポート データベース

組み込みの **SQLAnywhere** バージョンをレポート データベースとして使用する場合、インストーラは以下の情報を必要とします。 インストールを開始する前に、レポート データベース インストール ワークシートを使用して以下の情報を収集します。

- **SQLAnywhere root パスワード**

SQLAnywhere root ユーザ アカウントのパスワード

注: root ユーザ アカウントの名前を変更することはできません。 インストーラは、名前をデフォルトで **root** にします。

- **ユーザ**

レポート データベース管理者アカウントの名前。

インストーラ デフォルト : **sa**

- **パスワード**

レポート データベース管理者アカウントのパスワード。

Microsoft SQL Server レポート データベース

Microsoft SQL Server をレポート データベースとして使用する場合、インストーラは以下の情報を必要とします。 インストールを開始する前に、レポート データベース インストール ワークシートを使用して以下の情報を収集します。

- **Data Source Name (DSN)**

レポート サーバがレポート データベースと通信するために使用する DSN。

注: レポート サーバは、**32 ビット ネイティブ バイナリ**としてコンパイルされ、**32 ビット データ ソース ミドルウェア接続**を使用するように設定されます。 **Windows 64 ビット オペレーティング システム**にインストールしている場合は、必ず **odbcad32.exe** を使用して **DSN** を作成してください。 この実行ファイルは、以下の場所にあります。

`install_home¥Windows¥SysWOW64`

`install_home`

Windows オペレーティング システムのインストール パスを指定します。

- **ログイン ID**

レポート データベース管理者アカウントの名前。このアカウントにはデフォルト (DBO) のアカウント権限が必要です。

- **パスワード**

レポート データベース管理者アカウントのパスワード。

Oracle レポート データベース

Oracle をレポート データベースとして使用する場合、インストーラは以下の情報を必要とします。 インストールを開始する前に、レポート データベース インストール ワークシートを使用して以下の情報を収集します。

- **Oracle Net クライアント サービス名**

レポート サーバがレポート データベースと通信するために使用するサービス名。

- (Windows) インストーラは Oracle Net クライアント サービス名をサーバとして参照します。
- (UNIX) インストーラは Oracle Net クライアント サービス名を TNSNAME として参照します。

- **User name**

レポート データベース管理者アカウントの名前。このアカウントには以下の権限が必要です。

- セッションの作成 (create session)
- 表の作成 (create table)
- プロシージャの作成 (create procedure)

注: 管理者アカウントは、CONNECT と RESOURCE のロールを有効にして使用することもできます。両方のロールに対して Admin Option 設定は必ず無効にしてください。

- **パスワード**

レポート データベース管理者アカウントのパスワード。

Apache Tomcat のインストール

SiteMinder では、レポート サーバ インストールに埋め込まれた Apache Tomcat のバージョンのみをサポートします。 インストールを開始する前に、Web アプリケーション インストール ワークシートを使用して以下の情報を収集します。

- 接続ポート

Apache Tomcat が接続してリクエストを待機するポート。

インストーラ デフォルト： 8080

- リダイレクト ポート

Apache Tomcat がリクエストをリダイレクトするポート。

インストーラ デフォルト： 8443

- シャットダウン ポート

Apache Tomcat SHUTDOWN コマンドが発行されるポート。

インストーラ デフォルト： 8005

レポートサーバのインストール

以下のセクションは、Windows および UNIX にレポートサーバをインストールする方法を詳述します。

インストールする前に

レポートサーバをインストールする前に、以下の点を考慮してください。

- 他の SiteMinder コンポーネントを備えたホスト システムにレポートサーバをインストールすることはサポートされていません。別のホスト システムにレポートサーバをインストールしてください。
- テクニカル サポート サイトで、インストール メディアを使用してレポートサーバをインストールします。

注: インストール メディア名のリストについては、「ポリシー サーバリリース ノート」を参照してください。

- レポートサーバは、32 ビット ネイティブ バイナリとしてコンパイルされ、32 ビット データ ソース ミドルウェア接続を使用するよう設定されます。Windows 64 ビット オペレーティング システムにインストールしている場合は、必ず `odbcad32.exe` を使用して DSN を作成してください。この実行ファイルは、以下の場所にあります。

`install_home¥Windows¥SysWOW64`

`install_home`

Windows オペレーティング システムのインストール パスを指定します。

- UNIX コンソールのインストールはサポートされていません。
- レポート サーバインストールには、プロセスとして実行する以下のコンポーネントが含まれます。
 - Content Management Server
 - Server Intelligence Agent

これらのコンポーネントでは、通信に TCP/IP ポートが必要です。インストーラでは、レポート サーバ ホスト システム上のポート競合を防ぐためにデフォルト設定を変更することができます。

- **重要:** インストール zip には、複数のフォルダが含まれています。インストーラ実行ファイルには、このフォルダ構造が必要です。zip を展開した後にレポート サーバ インストーラを移動した場合、フォルダ構造全体を同じ場所にコピーします。このフォルダ構造からインストール メディアを実行します。

- **重要:** (UNIX) レポートサーバをインストールするユーザアカウントは、インストールメディアが含まれるディレクトリに対して実行権限を持っている必要があります。ユーザアカウントにこれらの権限がない場合は、以下のコマンドを実行します。

```
chmod -R+x directory
```

directory

インストールメディアが存在するディレクトリを指定します。

- (UNIX) 別のサブネットにまたがってレポートサーバインストールを実行した場合、クラッシュすることがあります。ホストシステムにレポートサーバを直接インストールします。
- (UNIX) レポートサーバを RHEL 6 マシンにインストールする前に、RHEL 6 マシン上で以下のタスクを完了してください。
 - 以下の RPM をインストールします。
 - ncurses-libs.i686
 - Compat-libstdc++-33.3.3-69.el6.i686
 - libXext-1.1-3.el6.i686
 - libXext-devel-1.1-3.el6.i686
 - ncurses-base
 - ncurses-libs 5.9-7.20121017
 - xorg-x11-libX11-7.6-23.1.2.i586
 - xorg-x11-libXau-7.6_1.0.6-9.1.1.i586
 - xorg-x11-libxcb-7.6_1.7-8.1.i586
 - LD_LIBRARY_PATH 環境変数を 32 ビットの libncurses.so.5 ライブラリの場所に設定します。

Windows

次の手順に従ってください:

1. [インストールチェックリスト](#) (P. 496)を確認します。
2. [インストーラに必要な情報](#) (P. 506)が収集されたことを確認します。
3. 実行中のすべてのアプリケーションを終了します。

4. *installation_media* をダブルクリックします。

installation_media

レポートサーバのインストール実行ファイルを指定します。

CA Business Intelligence インストール ウィザードが表示され、ロケールの指定が要求されます。

注: インストール メディア名のリストについては、「ポリシー サーバリリース ノート」を参照してください。

5. 英語を選択し、[OK] をクリックします。

インストーラの導入画面が表示されます。

6. [次へ] をクリックします。

CA 使用許諾契約が表示されます。

7. 使用許諾契約に同意し、[次へ] をクリックします。

CA サンプル テンプレートをインストールするかどうかを確認されます。

8. [いいえ] を選択して、[次へ] をクリックします。

注: CA サンプル テンプレートは、SiteMinder レポート テンプレートとは関係がありません。SiteMinder レポート サーバ設定ウィザードが、必要なレポート テンプレートをインストールします。このウィザードは、レポートサーバをインストールした後に実行します。

サイレント インストール用の応答ファイルを保存するかどうかを確認されます。

9. [はい] を選択して [次へ] をクリックします。

インストールのサマリが表示されます。

10. サマリを確認して [インストール] をクリックします。

コンポーネントがインストールされます。CA Business Intelligence セットアップウィザードが表示されます。

11. [次へ] をクリックします。

インストーラの導入画面が表示されます。

12. [次へ] をクリックします。

SAP BusinessObjects Enterprise 使用許諾契約が表示されます。

13. 使用許諾契約に同意し、[次へ] をクリックします。

言語パックの選択が要求されます。英語がデフォルトで選択されています。

14. デフォルトの英語のままにして [次へ] をクリックします。

インストール タイプの選択が要求されます。

15. [New] を選択し、以下の手順のいずれかを実行して、レポート (CMS) データベースを設定します。

- (推奨) 埋め込みの MySQL バージョンをインストールするには、[Install MySQL Database Server] を選択して [次へ] をクリックします。
- 既存の Microsoft SQL Server または Oracle データベースを設定するには、[Use an existing database server] を選択して [次へ] をクリックします。

Content Management Server のポートおよび SAP BusinessObjects Enterprise 管理者アカウントのパスワードの入力が要求されます。

16. 以下の手順を実行します。

- a. Content Management Server がリスンするポートを指定します。
- b. デフォルトの SAP BusinessObjects Enterprise 管理者のパスワードを指定します。

重要: [Configure the SAP BusinessObjects Enterprise Administrator password at a later time] は選択しないでください。

- c. [次へ] をクリックします。

Server Intelligence Agent のノード名およびポートの入力が要求されます。

17. ノード名とポートを指定します。 [次へ] をクリックします。

レポート (CMS) データベースの設定が要求されます。

重要: レポート サーバは、CA 製品が共有できる CA の共通コンポーネントです。そのため、SiteMinder を除く他の製品でサポートされるデータベースのタイプおよびバージョンに及ぶまで、レポート データベースとしてインストーラで設定することができます。サポートされているデータベースのタイプおよびバージョンのリストについては、

「SiteMinder 12.52 SP1 プラットフォーム サポート マトリクス」を参照してください。

18. 以下のいずれかを実行します。

- (推奨) MySQL を設定している場合は、root ユーザ アカウントのパスワードおよびレポート データベース管理者の認証情報を入力します。
- Microsoft SQL Server を設定している場合：
 - a. SQL Server (ODBC) を選択し、[Browse] をクリックして SQL Server のログオン画面を開きます。
 - b. DSN を選択し、管理者の認証情報を入力します。

注: Windows の 64 ビット バージョンにインストールしている場合、[Consume DSN created under WOW64] を選択します。このオプションによって、32 ビット DSN を使用することが可能になります。

- c. [OK] をクリックします。
- Oracle を設定している場合は、サービス名および管理者認証情報に対する必要な値を入力します。

注: Auditing Database は設定しません。このコンポーネントは SiteMinder の監査ベースのレポートとは関係がありません。

Content Management Server Auditing Database は、レポート サーバに固有のアクティビティを監査するために使用され、SiteMinder には使用されません。SiteMinder 監査データベースは、監査ベースのレポートの実行に必要となります。

19. [次へ] をクリックします。

Web アプリケーション サーバの選択が要求されます。

20. 以下の手順を実行します。

- a. [Install Tomcat application server and deploy to it] を選択します。

注: SiteMinder は、埋め込みの Apache Tomcat バージョンのみをサポートします。

- b. [IIS Web Application Server] オプションをオフにします。

- c. [次へ] をクリックします。

Apache Tomcat 情報を入力するよう要求されます。

21. Apache Tomcat ポートを入力し、[Next] をクリックします。

インストールを開始するよう要求されます。

22. [Next] をクリックして、インストールを開始します。

インストールが完了したら、インストーラのプロンプトが表示されます。

23. [Launch SAP BusinessObjects Administration Console] オプションをオフにして [Finish] をクリックします。

レポート サーバがインストールされます。

UNIX

次の手順に従ってください:

1. [インストールチェックリスト](#) (P. 496)を確認します。
2. [インストーラに必要な情報](#) (P. 506)が収集されたことを確認します。
3. root ユーザアカウントを使用してインストールを開始します。
4. 実行中のすべてのアプリケーションを終了します。
5. Bourne シェルを開き、インストール メディアに移動します。
6. 以下のコマンドを入力します。

```
./installation_media -i console  
installation_media
```

レポート サーバのインストール実行ファイルを指定します。

CA Business Intelligence インストーラが開始し、ロケールの指定が要求されます。

注: インストール メディア名のリストについては、「ポリシー サーバリリース ノート」を参照してください。

7. 英語用の値を入力し、Enter キーを押します。
インストーラの導入画面が表示されます。
8. Enter キーを押します。
CA 使用許諾契約が表示されます。
9. 以下の手順を実行します。
 - a. Enter キーを押して使用許諾契約を進めます。
 - b. y と入力して、使用許諾契約に同意します。
 - c. Enter キーを押します。
非 root ユーザ認証情報を入力するよう要求されます。
10. ユーザ名とグループ名を入力し Enter キーを押します。
CA 共有コンポーネントディレクトリへのパスの指定が要求されます。
11. デフォルト値のままにして Enter キーを押します。
CA サンプルテンプレートをインストールするかどうかを確認されます。
12. N を入力し、Enter キーを押します。

注: CA サンプルテンプレートは、SiteMinder レポート テンプレートとは関係がありません。SiteMinder レポート サーバ設定ウィザードが、必要なレポートテンプレートをインストールします。このウィザードは、レポートサーバをインストールした後に実行します。

サイレントインストール用の応答ファイルを保存するかどうかを確認されます。
13. 「Y」と入力して Enter キーを押します。
インストールのサマリが表示されます。
14. サマリを確認し、Enter キーを押します。
コンポーネントがインストールされます。SAP BusinessObjects Enterprise インストーラによって、インストール言語の選択が要求されます。
15. English を選択して Enter キーを押します。
SAP BusinessObjects Enterprise 使用許諾契約が表示されます。
16. y を入力して使用許諾契約に同意します。
レポート サーバインストール ディレクトリの入力が必要とされます。

17. Tab キーを押してデフォルト設定を自動入力し、Enter キーを押します。

言語パックの選択が要求されます。英語がデフォルトで選択されています。

18. デフォルト値のままにして Enter キーを押します。

インストール タイプの選択が要求されます。

19. [User – Regular SAP BusinessObjects Enterprise installation] を選択して Enter キーを押します。

インストール タイプの選択が要求されます。

20. [New] を選択して Enter キーを押します。

注: [Enable servers upon installation] はオフにしないでください。

Content Management Server のポートおよび SAP BusinessObjects Enterprise 管理者アカウントのパスワードの入力が要求されます。

21. 以下の手順を実行します。

- a. Content Management Server が接続してリクエストをリスンするポートを指定します。
- b. デフォルトの SAP BusinessObjects Enterprise 管理者のパスワードを指定します。
- c. Enter キーを押します。

レポート (CMS) データベースとして機能するデータベースのタイプを選択することが要求されます。

22. 以下のいずれかの操作を実行します。

- (推奨) 埋め込みの MySQL バージョンをインストールするには、MySQL のインストールを選択して Enter キーを押します。
- 既存の Oracle データベースを設定するには、既存のデータベースサーバの使用を選択して Enter キーを押します。
- (RHEL 6) SQLAnywhere をインストールするには、SQLAnywhere のインストールを選択して Enter キーを押します。

重要: レポートサーバは、CA 製品が共有できる CA の共通コンポーネントです。そのため、**SiteMinder** を除く他の製品でサポートされるデータベースのタイプおよびバージョンに及ぶまで、レポートデータベースとしてインストーラで設定することができます。サポートされているデータベースのタイプおよびバージョンのリストについては、「**SiteMinder 12.52 SP1 プラットフォーム サポート マトリクス**」を参照してください。

追加のレポート データベース情報が要求されます。

23. 以下のいずれかの操作を実行します。

- (MySQL/SQLAnywhere) root ユーザ アカウントおよびレポートデータベース管理者認証情報に対する必要な値を入力します。
- (Oracle) 以下の手順を実行します。
 - a. Oracle を選択して Enter キーを押します。
データベース情報が要求されます。
 - b. サービス名および管理者認証情報を入力します。

24. Enter キーを押します。

- 埋め込みの MySQL バージョンをインストールしている場合、Auditing Database 情報が要求されます。
- Oracle を設定している場合、Auditing Database のインストールが要求されます。

Auditing Database は SiteMinder の監査ベースのレポートとは関係がありません。Content Management Server Auditing Database は、レポートサーバに固有のアクティビティを監査するために使用され、SiteMinder には使用されません。SiteMinder 監査データベースは、監査ベースのレポートの実行に必要となります。

25. 以下のいずれかの操作を実行します。

- (MySQL/SQLAnywhere) デフォルトのままにして Enter キーを押します。
- (Oracle) 以下の手順を実行します。
 - a. [Do not install Auditing Database] オプションを選択します。
 - b. Enter キーを押します。
データベースの再初期化が要求されます。
 - c. Yes を選択して Enter キーを押します。

Service Intelligence Agent のノード名およびポートの指定が要求されます。

26. ノード名とポートを入力して Enter キーを押します。

Web アプリケーション サーバの選択が要求されます。

27. [Install Tomcat deploy web applications] オプションを選択します。

注: SiteMinder は、埋め込みの Apache Tomcat バージョンのみをサポートします。

Apache Tomcat ポートを入力するよう要求されます。

28. 必要な Apache Tomcat ポート情報を入力して Enter キーを押します。

インストーラに、インストール ディレクトリのパスが表示されます。

29. Enter キーを押してインストールを開始します。

インストールの進捗状況が表示され、インストールの完了を確認します。

30. Enter キーを押してインストーラを終了します。

レポート サーバ インストールのトラブルシューティング

レポート サーバ インストールのトラブルシューティングには、以下のファイルを使用します。

- CA_Business_Intelligence_InstallLog.log

報告されたエラーを表示するために、まずこのログを開くことをお勧めします。

- ca-install.log

報告されたエラーを表示するために、このファイルの下部までスクロールすることをお勧めします。「BIEK_GetExitCode」を検索し、「BIEK_GetExitCode」関数の戻り値を確認します。戻り値が 0 でない場合は、インストールエラーがあります。エラーの原因を判定するため、以下のキーワードを検索します。

- エラー
- 警告
- CMS
- InfoStore

ログ ファイルは、インストール中は一時的な保存場所にあります。システム上の TEMP 環境プロパティは、一時的な保存場所を決定します。インストールが失敗した場合、ログ ファイルはこの一時的な保存場所で見つけることができます。インストール成功後、ログ ファイルはレポート サーバ インストール ディレクトリの最上位にあります。

レポート テンプレートをインストールする方法

レポート テンプレートをインストールするには、以下の手順に従います。

1. インストーラ用の情報を収集します。
2. レポート テンプレートをインストールします。
3. レポート サーバを再起動します。
4. Job Server サービスのタイムアウト値を増加させます。

インストーラのための情報の収集

レポート サーバ設定ウィザードは、以下の情報を必要とします。

- **BusinessObjects 管理者パスワード** - デフォルトの BusinessObjects 管理者アカウント用のパスワードを識別します。 レポート サーバインストーラは、インストール中にデフォルトの管理アカウントを作成します。 インストールを完了させるために、このアカウント用のパスワードが必要です。 レポート サーバ設定ウィザードは、レポート テンプレートをインストールするために、デフォルトの管理アカウントを使用するためのパスワードを必要とします。
- **SiteMinder 監査データベース タイプ** - SiteMinder 監査データベースとして機能するデータベースのタイプを識別します。 監査ベースのレポートを実行するために、個別の SiteMinder 監査データベースが必要です。 レポート サーバ設定ウィザードは、監査データベースタイプに基づいた 1 セットのレポート テンプレートを使用するために、レポート サーバを設定するためのデータベース タイプを必要とします。

注: レポート サーバ設定ウィザードを実行する前に、SiteMinder 監査データベースを設定する必要はありません。

ワークシートは、レポート テンプレートのインストール前に必要な情報を収集および記録するために提供されます。

レポートテンプレートのインストール

レポート サーバ設定ウィザードで、SiteMinder レポート テンプレートをインストールします。 以下のセクションは、Windows および UNIX でレポート サーバ設定ウィザードを実行する方法を詳述します。

インストールする前に

レポートテンプレートをインストールする前に、以下の点を考慮します。

- テクニカルサポートサイトで、インストールメディアを使用してレポートサーバ設定ウィザードを実行します。

注: インストールメディア名のリストについては、「ポリシー サーバリリース ノート」を参照してください。

重要: (UNIX) インストールメディアは実行権限を必要とします。以下のコマンドを実行して、権限を追加します。

```
chmod +x installation_media
```

installation_media

レポートサーバ設定ウィザードのインストール実行ファイルの名前を指定します。

- (UNIX) 別のサブネットにわたってレポートサーバ設定ウィザードを実行すると、クラッシュする場合があります。レポートサーバホストシステムに、レポートテンプレートを直接インストールします。

Windows

Windows にレポートテンプレートをインストールする方法

1. [インストーラに必要な情報](#) (P. 522) が収集されたことを確認します。
2. 実行中のすべてのアプリケーションを終了します。
3. *installation_media* をダブルクリックします。

installation_media

レポートサーバ設定ウィザードのインストール実行ファイルの名前を指定します。

インストーラが起動します。

注: インストールメディア名のリストについては、「ポリシー サーバリリース ノート」を参照してください。

4. 各プロンプトについては、完了したレポートサーバ設定ワークシートを使用して必要な値を入力します。

5. インストール設定を確認し、[インストール] をクリックします。
レポートテンプレートがインストールされます。
6. レポートサーバを再起動します。
レポートサーバは、**SiteMinder** レポートテンプレートを使用するように設定されます。

UNIX GUI

UNIX GUI を使用して、レポートテンプレートをインストールする方法

1. [インストーラに必要な情報](#) (P. 522) が収集されたことを確認します。
2. 実行中のすべてのアプリケーションを終了します。
3. シェルを開き、インストールメディアに移動します。
4. 以下のコマンドを入力します。

```
./installation_media  
installation_media
```

レポートサーバ設定ウィザードのインストール実行ファイルの名前を指定します。

インストーラが起動します。

注: インストールメディア名のリストについては、「ポリシーサーバリリースノート」を参照してください。

5. 各プロンプトについては、完了したレポートサーバ設定ワークシートを使用して必要な値を入力します。

注: Oracle は Solaris レポートサーバ用にサポートされている唯一の監査データベースです。Solaris にレポートサーバをインストールした場合には、監査データベースタイプの指定を要求されません。レポートサーバ設定ウィザードは、自動的に Oracle 固有のレポートテンプレートをインストールします。

6. インストール設定を確認し、[インストール] をクリックします。
レポートテンプレートがインストールされます。
7. レポートサーバを再起動します。
レポートサーバは、**SiteMinder** レポートテンプレートを使用するように設定されます。

UNIX コンソール

UNIX コンソールを使用して、レポートテンプレートをインストールする方法

1. [インストーラに必要な情報](#) (P. 522) が収集されたことを確認します。
2. 実行中のすべてのアプリケーションを終了します。
3. シェルを開き、インストール メディアに移動します。
4. 以下のコマンドを入力します。

```
./installation_media -i console
```

```
installation_media
```

レポート サーバ設定ウィザードのインストール実行ファイルの名前を指定します。

```
-i console
```

UNIX コンソール内で開始するインストールを指定します。

インストーラが起動します。

注: インストール メディア名のリストについては、「ポリシー サーバリリース ノート」を参照してください。

5. 各プロンプトについては、完了したレポート サーバ設定ワークシートを使用して必要な値を入力します。

注: Oracle は Solaris レポート サーバ用にサポートされている唯一の監査データベースです。Solaris にレポート サーバをインストールした場合には、監査データベース タイプの指定を要求されません。レポート サーバ設定ウィザードは、自動的に Oracle 固有のレポート テンプレートをインストールします。

6. インストール設定を確認し、Enter キーを押します。

レポート テンプレートがインストールされます。

7. レポート サーバを再起動します。

レポート サーバは、SiteMinder レポート テンプレートを使用するように設定されます。

ジョブ サーバ サービス タイムアウト値の増加

いくつかのレポート サーバ サービスには、10 分のデフォルト タイムアウトがあります。 レポート サーバが大きな分析レポートを生成するためには、10 分以上かかる場合があります。

大きな分析レポートが正常に生成されるように、Crystal Reports Job Server サービスのタイムアウト値を増加させます。

Windows でのタイムアウト値の増加

以下の手順に従います。

1. [スタート] - [プログラム] - [BusinessObjects XI 3.1] - [BusinessObjects Enterprise] - [Central Configuration Manager] をクリックします。

Central Configuration Manager コンソールが表示されます。

2. [Crystal Reports Job Server] を右クリックし、[停止] を選択します。

Crystal Reports Job Server サービスが停止します。

3. [Crystal Reports Job Server] を右クリックし、[プロパティ] を選択します。

Crystal Reports Job Server プロパティ ダイアログ ボックスが表示されます。

4. プロパティ タブから、コマンド フィールド内の文字列の最後に以下のエントリを追加します。

```
-requesttimeout 6000000
```

注: タイムアウト値はミリ秒で測定されます。6000000 に指定すると、タイムアウト値は 1 時間に増加されます。

5. [OK] をクリックします。

Central Configuration Manager が表示されます。

6. [Crystal Reports Job Server] を右クリックし、[開始] を選択します。

Crystal Reports Job Server サービスが開始されます。

7. Central Configuration Manager を終了します。

Crystal Reports Job Server サービス用のタイムアウト値は 1 時間に設定されます。

UNIX でのタイムアウト値の増加

以下の手順に従います。

1. `report_server_home/CommonReporting3/bobje` に移動します。

`report_server_home`

レポートサーバのインストールパスを指定します。

2. `ccm.config` ファイルを開き、`reportjobserverLAUNCH` キー用の値の最後に以下のエントリを追加します。

`-requesttimeout 6000000`

注: タイムアウト値はミリ秒で測定されます。6000000 に指定すると、タイムアウト値は 1 時間に増加されます。

3. `ccm.config` ファイルを保存して閉じます。

Crystal Reports Job Server サービス用のタイムアウト値は 1 時間に設定されます。

レポートサーバを登録する方法

レポートサーバの登録は、ポリシーサーバホストシステム、レポートサーバホストシステムおよび管理 UI ホストシステムへのアクセスを必要とします。登録プロセス

- レポートサーバとポリシーサーバの間に、信頼できるリレーションシップを確立します。
- レポートサーバと管理 UI の間に、信頼できるリレーションシップを確立します。

レポートサーバを登録するには、以下の手順に従います。

1. クライアント名とパスフレーズを作成します。
2. 登録情報を収集します。
3. ポリシーサーバにレポートサーバを登録します。
4. レポートサーバを再起動します。
5. 管理 UI への接続を設定します。

クライアント名とパスフレーズの作成

XPSRegClient ユーティリティを実行すると、クライアント名とパスフレーズを作成できます。クライアント名とパスフレーズは、以下のような値です。

- 登録するレポートサーバを識別するためにポリシーサーバが使用する値
- ポリシーサーバにレポートサーバを登録するために XPSRegClient ツールで使用する値

登録ツールを実行する方法

1. ポリシーサーバホストシステムからコマンドラインウィンドウを開きます。
2. *siteminder_home/bin* 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。

3. 以下のコマンドを実行します。

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

client_name

登録するレポートサーバの名前を識別します。

制限： 値は一意である必要があります。たとえば、すでに **reportserver1** を使用している場合は、「**reportserver2**」と入力します。

注： この値は記録しておいてください。この値は、レポートサーバホストシステムから登録処理を完了するときが必要です。

passphrase

レポートサーバ登録を完了するのに必要なパスワードを指定します。

制限： パスフレーズは

- 6文字以上にする必要があります。
- パスフレーズには、アンパサンド (&) またはアスタリスク (*) を含めることができません。
- パスフレーズにスペースが含まれる場合、引用符で囲む必要があります。

この手順でパスフレーズを指定しない場合、XPSRegClient でパスフレーズの入力と確認が求められます。

注： この値は記録しておいてください。 この値は、レポートサーバホストシステムから登録処理を完了するときに必要です。

-report

レポートサーバの登録を指定します。

-t timeout

(オプション) レポートサーバホストシステムからの登録処理を完了する必要がある時間を指定します。 タイムアウト値に到達すると、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 (1 日)

-r retries

(オプション) レポートサーバホストシステムからの登録処理を完了するまでに許容される試行の失敗回数を指定します。 登録時に間違ったパスフレーズをサブミットすると、登録に失敗することがあります。

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。登録ツール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` はポリシーサーバがインストールされている場所です。

-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。

登録ログ ファイルの名前が一覧表示されます。パスフレーズを指定しなかった場合、入力が求められます。

4. Enter キーを押します。

登録ツールにより、クライアント名とパスフレーズが作成されます。

これで、ポリシーサーバにレポートサーバを登録できるようになりました。レポートサーバホストシステムからの登録処理が完了しました。

登録情報の収集

レポートサーバとポリシーサーバの間で登録処理を完了するには、特定の情報が必要です。レポートサーバホストシステムから XPSRegClient ユーティリティを実行する前に、以下の情報を集めます。

- クライアント名 - XPSRegClient ツールを使用して指定したクライアント名。
- パスフレーズ - XPSRegClient ツールを使用して指定したパスフレーズ。
- ポリシーサーバホスト - ポリシーサーバホストシステムの IP アドレスまたは名前。

ポリシーサーバにレポートサーバを登録します

ポリシーサーバにレポートサーバを登録して、両方のコンポーネント間に信頼関係を作成します。レポートサーバ登録ツールを使用して、レポートサーバホストシステムからの接続を設定します。

以下の手順に従います。

1. レポートサーバホストシステムからコマンドライン ウィンドウを開き、*report_server_home/external/scripts* に移動します。

report_server_home

レポートサーバのインストール場所を指定します。

デフォルト: (Windows) C:\Program Files\CA\SC\CommonReporting3

デフォルト: (UNIX) /opt/CA/SharedComponents/CommonReporting3

2. 以下のいずれかのコマンドを実行します。

■ (Windows)

```
regreportserver.bat -pshost host_name -client client_name -passphrase  
passphrase -psport portnum -fipsmode 0|1
```

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する前に、管理者権限でコマンドラインウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドラインウィンドウを開きます。

■ (UNIX)

```
regreportserver.sh -pshost host_name -client client_name -passphrase  
passphrase -psport portnum -fipsmode 0|1
```

-pshost *host name*

レポートサーバを登録するポリシーサーバホストシステムの IP アドレスまたは名前を指定します。

-client *client name*

クライアント名を指定します。クライアント名は、登録するレポートサーバのインスタンスを識別します。

注: この値は、ポリシーサーバホストシステムでレポートサーバを登録したときに、XPSRegClient ユーティリティを使用して指定したクライアント名と一致する必要があります。

例: XPSRegClient ユーティリティを使用したときに「reportserver1」を指定した場合、「reportserver1」と入力します。

-passphrase *passphrase*

クライアント名とペアになるパスフレーズを指定します。クライアント名は、登録するレポートサーバのインスタンスを識別します。

注: この値は、ポリシーサーバホストシステムでレポートサーバを登録したときに、XPSRegClient ユーティリティを使用して指定したパスフレーズと一致する必要があります。

例: XPSRegClient ユーティリティを使用したときに「SiteMinder」を指定した場合、「SiteMinder」と入力します。

`-psport portnum`

(オプション) ポリシーサーバが登録リクエストをリスニングしているポートを指定します。

`fipsmode`

(オプション) レポートサーバとポリシーサーバとの間の通信を暗号化する方法を指定します。

デフォルト: 0

- 0 は FIPS 互換モードを指定します。
- 1 の場合、FIPS のみのモードを指定します。

3. Enter キーを押します。

登録が成功したことを示すメッセージが表示されます。

レポートサーバの再起動

(Windows) 次の手順に従ってください:

1. [スタート] - [プログラム] - [BusinessObjects XI 3.1] - [BusinessObjects Enterprise] - [Central Configuration Manager] をクリックします。
Central Configuration Manager コンソールが表示されます。
2. Apache Tomcat および Server Intelligence Agent サービスを停止します。
レポートサーバが停止します。
3. Apache Tomcat および Server Intelligence Agent サービスを開始します。
レポートサーバが再起動されます。

(UNIX) 次の手順に従ってください:

1. レポートサーバをインストールした、root ではないユーザとしてシステムにログインします。
2. 以下の環境変数の少なくとも 1 つは、必ず有効な utf8/UTF-8 ロケールに設定してください。
 - LC_ALL
 - LANG
 - LC_CTYPE

3. *report_server_home*/CommonReporting3/external/scripts に移動し、以下のコマンドを実行します。

```
../setupenv.sh
```

report_server_home

レポートサーバのインストールパスを指定します。

4. 以下を確認してください。

- IAM_RPTSRV_HOME 変数は、*report_server_home*/CommonReporting3 に設定されます。

report_server_home

レポートサーバのインストールパスを指定します。

- (Oracle レポート データベースのみ) LD_LIBRARY_PATH 変数は以下のように設定されます。

```
$ORACLE_HOME/lib32:$ORACLE_HOME/lib:$LD_LIBRARY_PATH
```

例：

エクスポート

```
LD_LIBRARY_PATH=$ORACLE_HOME/lib32:$ORACLE_HOME/lib:$LD_LIBRARY_PATH
```

5. *report_server_home*/CommonReporting3/bobje に移動し、以下のコマンドを実行します。

```
./stopservers
```

report_server_home

レポートサーバのインストールパスを指定します。

6. 以下のコマンドを実行します。

```
./tomcatshutdown.sh
```

レポートサーバが停止します。

7. 以下のコマンドを実行します。

```
./startservers
```

8. 以下のコマンドを実行します。

```
./tomcatstartup.sh
```

レポートサーバが再起動されます。

管理 UI への接続の設定

レポートサーバと 管理 UI の接続を設定し、両方のコンポーネント間の信頼関係を設定します。 管理 UI からの接続を設定します。

注: 管理 UI にはポリシーサーバとの信頼関係を 1 つ以上設定できます。ただし、各信頼関係で確立できるレポートサーバ接続は 1 つだけです。新しいレポートサーバに接続する必要がある場合、現在のレポートサーバ接続を削除するか、別のポリシーサーバに接続して、接続を設定します。

管理 UI への接続を設定する方法

1. 管理 UI にログインします。
2. [管理] - [管理 UI] をクリックします。
3. [レポート接続] - [レポートサーバ接続の作成] をクリックします。
[レポートサーバ接続の作成] ペインが表示されます。

注:それぞれの要件および制限など、設定とコントロールの説明を参照するには、[ヘルプ] をクリックします。

4. [接続名] フィールドに接続名を入力します。
5. [サーバホストのレポート] フィールドに、レポートサーバホストシステム名または IP アドレスを入力します。
6. [Tomcat ポート] フィールドに Apache Tomcat 接続ポートを入力します。

注: この値は、レポートサーバをインストールするときに入力した Web サーバポートです。

7. それぞれのフィールドに管理者パスワードを入力します。

注: この値は、レポートサーバをインストールしたときに、デフォルト BusinessObjects 管理者アカウント用に入力したパスワードです。

8. [サブミット] をクリックします。

レポートサーバと 管理 UI の間の接続が設定されます。

レポートサーバのインストールおよび登録が完了しました。これで、ポリシー分析レポートを実行できるようになりました。

注: 監査レポートの作成および管理には個別の監査データベースが必要です。

監査データベースを設定する方法

SiteMinder 監査ベースのレポートを実行するために、SiteMinder 監査データベースが必要です。

注: 監査情報をテキスト ファイルに書き込むことは可能ですが、監査ベースのレポートを作成および管理するために、サポートされている ODBC データベース内に監査情報を格納する必要があります。サポートされているバージョンのリストについては、「SiteMinder 12.52 SP1 プラットフォーム サポート マトリクス」を参照してください。

以下の手順を完了して、監査データベースを設定します。

1. (オプション) まだ実行していない場合は、SiteMinder 監査データベースを設定します。

重要: Oracle 内の監査データベースを設定する場合には、提供するユーザアカウントに DB ロールがないことを確認してください。ユーザアカウントに DB ロールがある場合、監査ベースのレポートは正しい結果を返しません。

2. 管理 UI に監査データベースを登録します。
3. 監査データベースとレポート サーバの間の接続を設定します。

管理 UI での監査データベースの登録

管理 UI に監査データベースを登録し、コンポーネント間のトラステッド接続を作成します。管理 UI に監査データベースを登録すると、SiteMinder 管理者が監査に基づいたレポートを作成および管理できるようになります。

注: 管理 UI にはポリシー サーバとの信頼関係を 1 つ以上設定できます。ただし、監査データベースへの接続は、各信頼関係に 1 つのみです。新しい監査データベースに接続する必要がある場合、現在の接続を削除するか、別のポリシー サーバに接続して、接続を設定します。

次の手順に従ってください:

1. 管理 UI にログインします。
2. [管理] - [管理 UI] をクリックします。

3. [レポート接続] - [監査レポート接続の作成] をクリックします。

[監査レポート接続の作成] ペインが表示されます。

注:それぞれの要件および制限など、設定とコントロールの説明を参照するには、[ヘルプ] をクリックします。

4. [データベース ベンダー] ドロップダウン リストからデータベース ベンダーを選択します。

ベンダー固有のフィールドが表示されます。

5. [接続名] フィールドに接続の名前を入力します。

6. [データベース サーバ ホスト] フィールド内に監査データベース ホスト システム名または IP アドレスを入力します。

7. [DSN] フィールドに、以下のように監査データベース データ ソース 情報を入力します。

- **Oracle** - 監査データベース DSN を作成するときに指定した Oracle Net サービス名を入力します。

注: このサービス名は、ポリシー サーバへの監査データベース接続を設定するときに、ポリシー サーバ管理コンソールの [データ] タブで入力した DSN と関連付けられている必要があります。 サービス名は、レポート サーバ上で作成する DSN に一致する必要があります。

- **SQL Server** - DSN を入力します。

注: この DSN 名は、ポリシー サーバへの監査データベース接続を設定するときに、ポリシー サーバ管理コンソールの [データ] タブで指定した DSN と一致している必要があります。 DSN 名は、レポート サーバ上で作成する DSN にも一致する必要があります。

8. [データベース サーバ ポート] フィールドに監査データベース サーバがリスニングするポートを入力します。

9. 以下のいずれかの操作を実行します。

- **Oracle** - [サービス名] フィールドに Oracle Net サービス名を再入力します。

- **SQL Server** - [データベース名] フィールドに監査データベース名を入力します。

10. それぞれのフィールドに監査データベース用の管理者認証情報を入力します。

注: 管理者クレデンシアルは、ポリシー サーバへの監査データベース接続を設定するときに、ポリシー サーバ管理コンソールの [データ] タブで指定したクレデンシアルと一致する必要があります。

11. [サブミット] をクリックします。

監査データベースが 管理 UI に登録されます。

監査データベースおよびレポート サーバの接続性

レポート サーバは、監査ベースのレポートを作成するために SiteMinder 監査データベースに接続します。 監査ベースのレポートが 管理 UI にスケジュールされるとき、管理 UI は以下の接続情報をレポート サーバに渡します。

- (Oracle) 監査データベースを識別する Oracle Net サービス名
- (Microsoft SQL Server) 以下の名前
 - 監査データベース
 - 監査データベースに接続するためのデータ ソース
- 監査データベースへのアクセスに必要なユーザ アカウント認証情報

監査データベースとレポート サーバの間の接続を設定するために、以下のいずれかを実行します。

- (Oracle) 以下を確認してください。
 - Oracle Net クライアントはレポート サーバ ホスト システムにインストールされます。
 - 監査データベースを識別する Oracle Net サービス名は、レポート サーバ ホスト システム上の tnsnames.ora ファイル内にあります。
- (Microsoft SQL Server) 監査データベースへの接続に使用されたデータ ソースがレポート サーバ ホスト システム上にあることを確認してください。

注: サポートされているデータベース ドライバの詳細については、「12.52 SP1 SiteMinder プラットフォーム サポート マトリクス」を参照してください。

レポート スケジューラの開始

(Windows) 以下の手順に従います。

1. [スタート] - [プログラム] - [BusinessObjects XI 3.1] - [BusinessObjects Enterprise] - [Central Configuration Manager] をクリックします。

Central Configuration Manager コンソールが表示されます。

2. Apache Tomcat および Server Intelligence Agent サービスを開始します。
レポート サーバが開始されます。

(UNIX) 以下の手順に従います。

1. レポート サーバをインストールした、`root` ではないユーザとしてシステムにログインします。
2. 以下の環境変数の少なくとも 1 つは、必ず有効な `utf8/UTF-8` ロケールに設定してください。

- `LC_ALL`
- `LANG`
- `LC_CTYPE`

3. `report_server_home/CommonReporting3/external/scripts` に移動し、以下のスクリプトを実行します。

```
../setupenv.sh
```

report_server_home

レポート サーバのインストールパスを指定します。

4. 以下を確認してください。

- `IAM_RPTSRV_HOME` 変数は、`report_server_home/CommonReporting3` に設定されます。

report_server_home

レポート サーバのインストールパスを指定します。

- (Oracle レポート データベースのみ) `LD_LIBRARY_PATH` 変数は、`$ORACLE_HOME/lib32:$ORACLE_HOME/lib:$ETPKIHOME/lib:$LD_LIBRARY_PATH` に設定されます。

例 : エクスポート

```
LD_LIBRARY_PATH=$ORACLE_HOME/lib32:$ORACLE_HOME/lib:$ETPKIHOME/lib:$LD_LIBRARY_PATH
```

- ETPKIHOME 変数は、*report_server_home/CommonReporting3* に設定されます。

report_server_home

レポートサーバのインストールパスを指定します。

5. *report_server_home/CommonReporting3/bobje* に移動します。

report_server_home

レポートサーバのインストールパスを指定します。

6. 以下のコマンドを実行します。

`./startservers`

7. 以下のコマンドを実行します。

`./tomcatstartup.sh`

レポートサーバが開始されます。

レポートサーバの停止

(Windows) 以下の手順に従います。

1. [スタート] - [プログラム] - [BusinessObjects XI 3.1] - [BusinessObjects Enterprise] - [Central Configuration Manager] をクリックします。

Central Configuration Manager コンソールが表示されます。

2. Apache Tomcat および Server Intelligence Agent サービスを停止します。

レポートサーバが停止します。

(UNIX) 以下の手順に従います。

1. レポートサーバをインストールした、**root** ではないユーザとしてシステムにログインします。
2. 以下の環境変数の少なくとも 1 つは、必ず有効な utf8/UTF-8 ロケールに設定してください。

- LC_ALL

- LANG

- LC_CTYPE

3. *report_server_home*/CommonReporting3/external/scripts に移動し、以下のコマンドを実行します。

```
../setupenv.sh
```

report_server_home

レポート サーバのインストールパスを指定します。

4. 以下を確認してください。

- IAM_RPTSRV_HOME 変数は、*report_server_home*/CommonReporting3 に設定されます。

report_server_home

レポート サーバのインストールパスを指定します。

- (Oracle レポート データベースのみ) LD_LIBRARY_PATH 変数は、\$ORACLE_HOME/lib32:\$ORACLE_HOME/lib:\$ETPKIHOME/lib:\$LD_LIBRARY_PATH に設定されます。

例：エクスポート

```
LD_LIBRARY_PATH=$ORACLE_HOME/lib32:$ORACLE_HOME/lib:$ETPKIHOME/lib:$LD_LIBRARY_PATH
```

- ETPKIHOME 変数は、*report_server_home*/CommonReporting3 に設定されます。

report_server_home

レポート サーバのインストールパスを指定します。

5. *report_server_home*/CommonReporting3/bobje に移動します。

report_server_home

レポート サーバのインストールパスを指定します。

6. 以下のコマンドを実行します。

```
./stopservers
```

7. 以下のコマンドを実行します。

```
./tomcatshutdown.sh
```

レポート サーバが停止します。

レポートをアンインストールする方法

SiteMinder レポートをアンインストールするには、以下の手順に従います。

1. SiteMinder レポート サーバ設定ウィザードをアンインストールします。
2. レポート サーバをアンインストールします。
3. 残りのアイテムを削除します。
4. レポート データベース テーブルを削除します。

Windows からのレポート サーバ設定ウィザードのアンインストール

以下の手順に従います。

1. 実行中のすべてのアプリケーションを終了します。
2. `report_server_home¥CommonReporting3¥Uninstall_CASiteMinder_ConfigurationWizard` に移動します。

`report_server_home`

レポート サーバのインストールパスを指定します。

重要: Windows Server 2008 上でこのウィザードを実行している場合は、実行ファイルを管理者権限で実行します。管理者としてシステムにログインしている場合でも、これらの権限を使用します。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。

3. `uninstall.exe` をダブルクリックします。

ウィザードが開始します。

4. プロンプトに従います。

注: 共有ファイルを削除するよう要求するメッセージが表示された場合は、[No to All] をクリックします。

5. 要求された場合はシステムを再起動します。

レポート サーバ設定ウィザードがアンインストールされます。

UNIX からのレポート サーバ設定ウィザードのアンインストール

以下の手順に従います。

1. 実行中のすべてのアプリケーションを終了します。
2. `report_server_home/CommonReporting3/Uninstall_CASiteMinder_ConfigurationWizard` に移動します。

`report_server_home`

レポート 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。

```
./uninstall
```

プロセスが開始します。

4. プロンプトに従います。

レポート サーバ設定ウィザードがアンインストールされます。

Windows からのレポート サーバのアンインストール

以下の手順に従います。

1. 実行中のすべてのアプリケーションを終了します。
2. `report_server_home¥CommonReporting3¥Uninstall CA Business Intelligence 3.2` に移動します。

`report_server_home`

レポート サーバのインストールパスを指定します。

3. `Uninstall CA Business Intelligence 3.2.exe` をダブルクリックします。

重要: Windows Server 2008 上でこのウィザードを実行している場合は、実行ファイルを管理者権限で実行します。管理者としてシステムにログインしている場合でも、これらの権限を使用します。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。

アンインストーラが開始されます。

注: レポート サーバをサイレント インストールした場合、アンインストーラはサイレントで開始されます。ウィザードを使用してアンインストールする場合は、以下のようになります。

- a. コマンドプロンプトを開きます。

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する前に、管理者権限でコマンドラインウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドラインウィンドウを開きます。

- b. `report_server_home¥CommonReporting3¥Uninstall CA Business Intelligence 3.2` に移動します。
- c. 以下のコマンドを入力します。

```
Uninstall CA Business Intelligence 3.2.exe -i swing
```

4. プロンプトに従います。

以下の点を考慮します。

- 共有ファイルを削除するようメッセージが表示された場合は、[No to All] をクリックします。
- Java Platform SE binary および BOE120MySQL を閉じるようメッセージが表示された場合は、[Do not close applications] を選択して [OK] をクリックします。

5. 要求された場合はシステムを再起動します。

レポート サーバがアンインストールされます。

注: レポート サーバをアンインストールしてもレポート データベース内のテーブルは削除されません。これらのテーブルは手動で削除する必要があります。

UNIX からのレポート サーバのアンインストール

このコンポーネントをアンインストールする際には、手動でインストールディレクトリを削除しません。アンインストール シェル スクリプトを実行します。インストールディレクトリのみを削除すると、関連するレジストリはそのまま残されます。このホストシステムにこのコンポーネントを再インストールしようとする場合、エントリは成功したインストールを回避できます。

以下の手順に従います。

1. Bourne シェルを開き、*report_server_home*/CommonReporting3/Uninstall に移動します。

report_server_home

レポート 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。

`./UninstallCABusinessIntelligence 3.2`

プロセスが開始します。

3. プロンプトに従います。

レポート サーバがアンインストールされます。

注: レポート サーバをアンインストールしてもレポート データベース内のテーブルは削除されません。これらのテーブルは手動で削除する必要があります。

Windows アイテムの削除

システムをできるだけきれいに保つために、残存するアイテムを手動で削除します。同じシステムにレポート サーバを再インストールする場合、残存アイテムを削除することでレポート サーバのインストールの失敗を防ぎます。

以下の手順に従います。

1. *report_server_home* に移動します。

report_server_home

レポート サーバのインストール パスを指定します。

2. 以下のディレクトリを削除します。

CommonReporting3

残っていたアイテムが削除されました。

UNIX アイテムの削除

システムをできるだけきれいに保つために、残存するアイテムを手動で削除します。同じシステムにレポート サーバを再インストールする場合、残存アイテムを削除することでレポート サーバのインストールの失敗を防ぎます。

重要: 他の CA 製品は `SharedComponents` ディレクトリを共有できます。`profile.CA` ファイルは、この場所の環境変数を設定します。このファイルを削除する前に他の CA 製品が `SharedComponets` ディレクトリを共有していないことを確認します。

以下の手順に従います。

1. `report_server_home` に移動します。

`report_server_home`

レポート サーバのインストールパスを指定します。

2. 以下のフォルダを削除します。

`CommonReporting`

3. `/etc` に移動します。

4. 以下のファイルを削除します。

`profile.CA`

残っていたアイテムが削除されました。

レポート データベース テーブルの削除

レポート サーバをアンインストールしてもレポート データベース内のテーブルは削除されません。レポート データベースとして機能するデータベースにアクセスし、すべてのテーブルを手動で削除する必要があります。

管理 UI へのレポート サーバ接続の削除

接続が必要でなくなった場合、レポート サーバ接続を削除します。

次の手順に従ってください：

1. [管理] - [管理 UI] をクリックします。
2. [レポート接続] - [レポート サーバ接続の削除] をクリックします。
3. 検索条件を指定し、[検索] をクリックします。
4. 接続を選択し、[選択] をクリックします。

接続を削除してもかまわないか確認するように促されます。

5. [はい] をクリックします。

レポート サーバ接続が削除されます。

レポート サーバの再インストール

レポート サーバを再インストールする場合は、再インストール前に既存のインスタンスをアンインストールします。既存のインスタンスに上書きして再インストールすると、インストールは失敗します。

詳細情報：

[レポートをアンインストールする方法 \(P. 542\)](#)

第 10 章: OneView モニタの設定

このセクションには、以下のトピックが含まれています。

[OneView モニタの概要 \(P. 549\)](#)

[OneView モニタのシステム要件 \(P. 550\)](#)

[OneView モニタの設定 \(P. 550\)](#)

[同じマシン上の OneView モニタ GUI/IIS Web エージェントの制限 \(P. 551\)](#)

[Windows/IIS 上で OneView モニタ GUI を設定する方法 \(P. 551\)](#)

[UNIX/Sun Java System 上で OneView モニタ GUI を設定する方法 \(P. 553\)](#)

[OneView モニタ サービスの起動 \(P. 556\)](#)

[OneView モニタ GUI へのアクセス \(P. 556\)](#)

[ポリシー サーバ クラスタの監視 \(P. 557\)](#)

OneView モニタの概要

OneView モニタのインフラストラクチャは、SiteMinder コンポーネントの監視を可能にする多くのモジュールで構成されています。JRE (Java Runtime Environment) のコンテキストの中で実行される監視プロセスが含まれています。このモニターの GUI の HTML ページは、JSP (Java Server Pages) と、ポリシー サーバと同じマシン上で実行される ServletExec サーブレット エンジン上でホストされたサーブレットによって生成されます。

OneView モニタ ユーティリティは以下の SiteMinder コンポーネントを監視します。

- ポリシー サーバ
- Web エージェント

注: OneView モニタの使用の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

OneView モニタのシステム要件

OneView モニタ GUI を設定するシステムは、少なくとも次のシステム要件を満たす必要があります。

- **JDK** - Java SDK の必須バージョンがシステムにインストールされている。
- **Servlet Engine** - ServletExec の必要なバージョンがシステムにインストールされます。

注: ポリシー サーバ インストール キットには以下の場所に ServletExec/AS のインストール実行可能ファイルが含まれています。

thirdparty-tools¥servlet-engine-6.0

- **Web サーバ** - サポートされている Web サーバが、システムにインストールされている。

注: サポートされている CA およびサードパーティ コンポーネントのリストについては、テクニカル サポート サイトの **SiteMinder 12.52 SP1** プラットフォームのサポート マトリックスを参照してください。

OneView モニタの設定

ポリシー サーバをインストールするときに **OneView モニタ GUI** を設定しなかった場合、ポリシー サーバ設定ウィザードを使用して設定できます。

Windows の場合は、*siteminder_home¥siteminder¥install_config_info* に、UNIX の場合は、*siteminder_home/siteminder/install_config_info* に、以下のポリシー サーバ設定ウィザード実行可能ファイルがあります。

- **ca-ps-config.exe**

重要: Windows Server 2008 上でこのウィザードを実行している場合は、実行ファイルを管理者権限で実行します。管理者としてシステムにログインしている場合でも、これらの権限を使用します。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。

- **ca-ps-config.bin**

siteminder_home

ポリシー サーバがインストールされている場所へのパスを指定します。

同じマシン上の OneView モニタ GUI/IIS Web エージェントの制限

エージェントで登録サービスが有効になっている場合、CA は、同じマシン上に IIS ベースの OneView モニタ GUI と IIS Web エージェントを設定することをサポートしていません。この設定では、ServletExec の同じインスタンスと競合します。

Windows/IIS 上で OneView モニタ GUI を設定する方法

Windows/IIS 上で OneView モニタ GUI を設定するには、以下の手順に従います。

1. Windows に ServletExec をインストールするための前提条件を確認します。
2. Windows/IIS 上で ServletExec/ISAPI をインストールします。

注: モニター GUI の HTML ページは、ポリシー サーバと同じマシン上で実行されている ServletExec サブレットエンジン上でホストされている、Java Server Pages (JSP) およびサブレットによって生成されます。

3. `policy_server_home¥monitor¥setting` フォルダのインターネット ゲスト アカウントに変更権限を割り当てます。
4. IIS ユーザに対して権限を設定します。
5. ポリシー サーバインストールプログラムで OneView モニタ GUI を自動設定しなかった場合は、ポリシー サーバ設定ウィザードを実行して設定します。
6. OneView モニタ サービスの起動
7. OneView モニタ GUI にアクセスします。

Windows に ServletExec をインストールするための前提条件

ServletExec をインストールする前に以下の前提条件を考慮します。

- ServletExec はサードパーティ製品です。コンポーネントをインストールする前に、ServletExec のドキュメントを一読することをお勧めします。

注: 詳細については、New Atlanta の [Web サイト](#) を参照してください。

- ポリシー サーバをサポートされる 64 ビットの Windows オペレーティングシステムにインストールした場合、32 ビットの JDK が必要です。ユーザが 64 ビットの Windows オペレーティングシステムに ServletExec/AS 6.0 をインストールしている場合、ServletExec には 64 ビットの JVM が必要です。必要な場合、ServletExec をインストールする前に 64 ビットの JVM をインストールします。

Windows IIS 上での ServletExec のインストール

以下の手順に従います。

1. 旧バージョンの ServletExec がある場合は、それをバックアップします。
2. ServletExec インストール実行可能ファイルを起動します。

注: ポリシー サーバインストールキットには以下の場所に ServletExec/AS 6.0 のインストール実行可能ファイルが含まれています。

thirdparty-tools¥servlet-engine-6.0

注: ServletExec のアップグレードおよびインストールの詳細については、New Atlanta の [ドキュメント](#) を参照してください。

3. ServletExec/AS 前提条件として 64 ビットの JVM をインストールした場合は、以下の手順を完了します。
 - a. ServletExec サービスを停止するには、[コントロール パネル] の [サービス] を使用します。
 - b. (オプション) 64 ビットの JVM をアンインストールします。

- c. StartServletExec.bat および StopServletExec.bat ファイルを編集して 32 ビット JVM を参照するようにします。
 - d. ServletExec サービスを開始するには、[コントロール パネル] の [サービス] を使用します。
4. IIS Admin Web サービスおよび IIS Web サーバを停止してから再起動します。

ServletExec インストール後の IIS ユーザ用権限の設定

ServletExec/AS は IIS プロセスの一部として実行されるので、実行されるたびに別のユーザとして扱われます。その結果、ServletExec インストールディレクトリおよびサブディレクトリ用に以下の権限を設定する必要があります。

ServletExec のインストール後に IIS ユーザ用権限を設定するために、IIS（たとえばネットワーク サービス）を実行するユーザが C:\Program Files\New Atlanta 以下のディレクトリ ツリー全体に読み取りおよび書き込みアクセスができることを確認してください。

UNIX/Sun Java System 上で OneView モニタ GUI を設定する方法

UNIX/Sun Java System 上で OneView モニタ GUI を設定するには、以下の手順に従います。

1. ServletExec のインストールの前提条件を確認します。
2. Sun Java System (Sun One/iPlanet) 6.0 のサーブレットを無効にします。
3. UNIX/Sun Java System に ServletExec/AS をインストールします。
4. ポリシー サーバインストールプログラムで OneView モニタ GUI を自動設定しなかった場合は、ポリシー サーバ設定ウィザードを実行して設定します。
5. OneView モニタ サービスを起動します。
6. OneView モニタ GUI にアクセスします。

ServletExec をインストールするための前提条件

CA は、ServletExec をインストールする前に、ServletExec のドキュメントを一読することをお勧めします。ServletExec が適切に実行されていない場合、OneView モニタ GUI は機能しません。OneView モニタは ServletExec のサーブレットエンジンに依存しているためです。

[New Atlanta Web サイト](#)で ServletExec ドキュメントを参照できます。

Sun Java System 6.0 でのサーブレットの無効化

ServletExec をインストールする前に、このセクションの手順に従っていることを確認します。

Sun Java System 6.0 内のサーブレットを無効にする方法

1. ブラウザで次の URL を入力することにより、Sun Java System Enterprise 管理サーバのホーム ページを開きます：
`http://<yourserver.com>:<portnumber>`
yourserver.com
Enterprise Administration Server のドメイン名を指定します。
ポート
ポート番号を指定します。
2. [Select a Server] ドロップダウン メニューで、ターゲット サーバを選択し、[Manage] をクリックします。
3. [Java] タブを選択します。
4. [Enable Java for class defaultclass] および [Enable Java Globally] をオフにし、[OK] をクリックします。
5. Web サーバを停止してから再起動し、設定が有効になるようにします。

UNIX/Sun Java システムでの ServletExec/AS のインストール

このモニターの GUI の HTML ページは、JSP (Java Server Pages) と、ポリシー サーバと同じマシン上で実行される ServletExec サーブレットエンジン上でホストされたサーブレットによって生成されます。

ServletExec をインストールする方法

1. ポリシー サーバをインストールする UNIX アカウントにログインします。

注: Sun Java System Web Server をインストールしたユーザと同じユーザとしてログインする必要があります。

2. ServletExec AS インストーラを実行します。

注: ServletExec AS インストーラの実行の詳細については、New Atlanta Communication の ServletExec のドキュメントを参照してください。

ServletExec をインストールする前に以下の点を考慮します。

- /tmp に新規ファイルを作成する権限を持っていることを確認します。New Atlanta は /usr/local/NewAtlanta 内に ServletExec をインストールすることをお勧めします。/usr/local/NewAtlanta 内に ServletExec をインストールすると、obj.conf ファイルおよび Sun Java System 起動スクリプトに対する権限が変更される場合があります。インストールの後、obj.conf および起動スクリプトの所有者が Web サーバを所有するユーザと同じであることを確認します。
- 画面の指示に従って、Web サーバアダプタおよび ServletExec のインスタンスをインストールします。
- 画面の指示に従って、インストーラによって Web サーバの設定ファイルを変更しないことを確認します。インストーラに Web サーバの obj.conf および magnus.conf 設定ファイルの変更を許可すると、このインスタンス上の OneView モニタ GUI を設定した後、Web サーバインスタンスの実行に失敗します。

3. インストールプログラムが完了したら、Web サーバを再起動します。

詳細情報:

[OneView モニタ サービスの起動 \(P. 556\)](#)

OneView モニタ サービスの起動

次の手順に従ってください:

1. IPC ポート番号が使用可能であることを確認します。

OneView モニタは、ポリシー サーバプロセスとの通信に以下のポート番号を使用します。

- 監視エージェント : 44449
- モニタ : 44450

どのポート番号が使用不可なのかを調べるには、コマンド ウィンドウを開き、以下のコマンドを入力します。

```
netstat -an
```

注: ポート番号の変更の詳細については、ポリシーサーバ管理ガイドを参照してください。

2. ポリシー サーバ管理コンソールの [ステータス] タブを使用して、監視サービスを起動します。

OneView モニタ GUI へのアクセス

次の手順に従ってください:

ブラウザで以下の URL を入力します。

```
http://server:<portnumber>/sitemindermonitor
```

server

Web サーバの IP アドレスを指定します

portnumber

ポート番号を指定します。

ポリシー サーバ クラスタの監視

OneView モニタは、1 つのポリシー サーバがクラスタ内の他のポリシー サーバを集中監視するポリシー サーバとしてセットアップされている場合、ポリシー サーバ クラスタを監視するように設定できます。

注: **OneView** モニタの使用の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

第 11 章: SNMP サポート

このセクションには、以下のトピックが含まれています。

[SNMP サポートの概要](#) (P. 559)

[Windows と UNIX のシステムの場合の SNMP 前提条件](#) (P. 561)

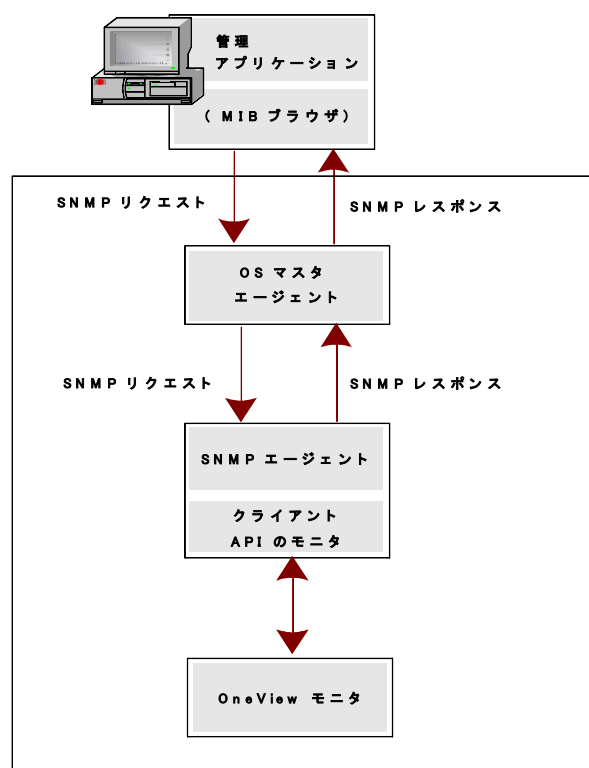
[Windows 上での SNMP エージェントの設定](#) (P. 562)

[UNIX システムでの SNMP エージェントの設定](#) (P. 565)

SNMP サポートの概要

SNMP サポートには、MIB (Management Information Base)、SNMP エージェント、イベント SNMP トラップ ライブラリが含まれています。SNMP エージェントとイベント SNMP トラップ ライブラリは独立して設定できます。一方を有効にして、他方を無効にすることができます。SNMP エージェントによって、監視アプリケーションは OneView モニタから動作データを取得できます。SNMP エージェントは SNMP マネージャへデータを送信し、SNMP リクエスト処理をサポートします。

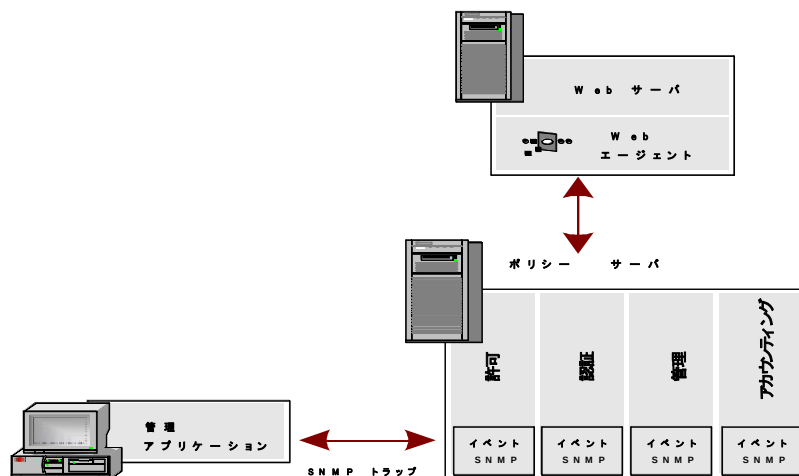
以下の図は、管理アプリケーション、OS マスタ エージェント、SNMP エージェント、および OneView モニタの間のアーキテクチャを示しています。



ネイティブ Solaris SunSolstice マスタ エージェントなどの OS マスタ エージェントは、ユーザがマスタ エージェントを再起動すると SNMP エージェントを呼び出します。OS マスタ エージェントは、管理アプリケーションから SNMP リクエストを受信すると、SNMP エージェントにその SNMP リクエストを転送します。SNMP エージェントは、OneView モニタと通信し、Monitor Client API を使用して必要な情報を取得し、次にマスタ エージェントにレスポンスを送信します。その後、マスタ エージェントは、そのレスポンスを管理アプリケーションに転送します。

ポリシー サーバのインストール中に SNMP エージェントを設定しなくても、後でそのエージェントを使用するときのために SNMP ファイルがすべてインストールされます。ただし、エージェントを実行するには、Windows または UNIX のシステム上で SNMP エージェントを設定することにより、エージェントを手動で起動する必要があります。

イベント SNMP トラップ ライブラリは、以下の図に示すように、いくつかの SiteMinder イベントを SNMP トラップに変換してから、それらを管理アプリケーションに送信します。トラップ ライブラリは、ポリシー サーバによって送信されたイベントをキャプチャし、そのイベントについて SNMP トラップが生成されることになっているかどうかを判別し、トラップを生成します。



注: SNMP エージェントおよび OneView モニタの詳細については、「ポリシー サーバ管理ガイド」を参照してください。

Windows と UNIX のシステムの場合の SNMP 前提条件

SNMP エージェントをインストールまたは使用する前にオペレーティングシステムにマスタ エージェントをインストールしておく必要があります。

Windows の前提条件

Windows 上の SiteMinder SNMP サポートで SNMP サービスが必要 SNMP サービスのインストールの詳細については、Windows オンライン ヘルプ システムを参照してください。

UNIX システムの前提条件

以下のセクションでは、SNMP をサポートするための UNIX の前提条件について説明します。

Solaris

ネイティブ Solaris SunSolstice マスタ エージェントが必要です。マスタ エージェントはオペレーティング システムに含まれています。

Linux

Red Hat Advanced Server 3.0 でサポートされているマスタ エージェントについては、net-snmp パッケージを net-snmp-5.1-2.1 以降にアップグレードします。

net-snmp パッケージを net-snmp-5.1-2.1 以降にアップグレードするには、net-snmpd コマンド用の snmpd.conf ファイルで以下の設定を使用します。

```
proxy -c public -v 1 localhost:8001 .1.3.6.1.4.1.2552
```

注: net-snmp パッケージをアップグレードした後、snmpd.conf ファイルにプロキシサポートを追加します。

SiteMinder に固有の snmpd.conf ファイルは以下の場所にあります（通常、ホストには多くの snmpd.conf ファイルがあります）。

```
/opt/siteminder/etc/snmp/conf/snmpd.conf
```

Windows 上での SNMP エージェントの設定

次の手順に従ってください:

1. NETE_PS_ROOT 環境変数が SiteMinder インストール ディレクトリに設定されていることを確認します。通常、これは、ポリシー サーバ インストール プログラムによってすでに行われています。
2. `siteminder_home¥config¥snmp.conf` ファイルを開き、最後の行を編集して `siteminder_home¥log¥snmp.log` へのフルパスが含まれるようにします。

注: これを実行する必要があるのは、ポリシー サーバ インストール プログラムに SNMP を自動的に設定するように指定しなかった場合のみです。

正しい例 : LOG_FILE=C:¥Program
Files¥Netegrity¥siteminder¥log¥snmp.LOG

正しくない例 : LOG_FILE=\$NETE_PS_ROOT¥log¥snmp.log

3. <Windows_dir>/java_service.ini ファイルを編集します。

注: これを実行する必要があるのは、ポリシー サーバインストールプログラムに SNMP を自動的に設定するように指定しなかった場合のみです。

- a. SERVICE_BINARY_NAME に JavaService.exe のフルパス名を設定します。

例 : SERVICE_BINARY_NAME=c:¥winnt¥JavaService.exe

- b. WORKING_DIR にディレクトリ siteminder_home¥bin へのフルパスを設定します。

例 : WORKING_DIR=C:¥Program files¥Netegrity¥siteminder¥bin

- c. JRE_PATH に javaw.exe のフルパスを設定します。

4. siteminder_home¥bin¥thirdparty¥proxyreg.exe を実行し、apadll.dll および snmp.conf のレジストリ キーを以下のように変更します。

proxyreg.exe full_path_for_apadll.dll full_path_for_snmp.conf

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する前に、管理者権限でコマンドラインウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドラインウィンドウを開きます。

例 : proxyreg.exe "c:¥program
files¥netegrity¥siteminder¥ bin¥ thirdparty¥apadll.dll"
"c:¥programfiles¥netegrity¥ siteminder¥ config¥ snmp.conf"

5. <WINNT dir>/JavaService.exe を -install オプションを指定して実行し、Netegrity SNMP エージェントを WINNT サービスとして登録します。
6. Windows サービス ダイアログ ボックスを使用して Netegrity SNMP エージェントを起動します。
7. SNMP サービスを再起動します。

Windows で SNMP イベントトラップを設定する方法

Windows で SNMP イベントトラップを設定するために必要なことは、以下のとおりです。

1. SNMP イベントトラップの有効化
2. snmptrap.config の設定

SNMP イベントトラップの有効化

SNMP のイベントトラップを有効にするには、XPSCConfig ユーティリティを使用して、XPSAudit リストにイベントハンドラライブラリ (eventsnmp.dll) を設定します。eventsnmp.dll のデフォルトの場所は *policy_server_home¥bin* です。

policy_server_home

ポリシーサーバのインストール場所を示します。

注: イベントハンドラライブラリを設定するための XPSCConfig ユーティリティの使用の詳細については、「ポリシーサーバ管理ガイド」を参照してください。

SNMP イベントトラップを有効にした後に、snmptrap.conf ファイルを設定します。

snmptrap.conf の設定

SNMP 設定ファイルを設定する方法

1. snmptrap.conf を編集します。

注: snmptrap.conf は、*policy_server_home¥config* にあります。

policy_server_home

ポリシーサーバのインストール場所を示します。

2. 受信するように指定するトラップについては、該当する行をコメント解除します。
3. トラップの送信先とする IP アドレス、ポート番号、およびコミュニティを指定します。
4. 新しい変更を含む snmptrap.config ファイルを保存します。
5. ポリシーサーバを再起動します。

詳細情報:

[ポリシー サーバの停止と再起動 \(P. 567\)](#)

UNIX システムでの SNMP エージェントの設定

次の手順に従ってください:

1. NETE_PS_ROOT 環境変数が SiteMinder インストール ディレクトリに設定されていることを確認します。通常、これは、ポリシー サーバ インストール プログラムによってすでに行われています。

例: /home/smuser/siteminder

2. ファイル /etc/snmp/conf/RunSubagent.sh を以下のように編集します。
 - a. 以下のように正しい JRE パスを設定します。
JAVA_HOME=\$INSTALL_HOME/bin/jdk/<required_version>/jr
 - b. 正しい SiteMinder パスを設定します。

例: INSTALL_HOME=/home/smuser/siteminder

注: INSTALL_HOME 変数には、SiteMinder インストール ディレクトリのフルパスが含まれます。

3. Solaris での SNMP デーモンの再起動
 - a. root としてログインします。
 - b. /etc/rc3.d に移動します。
 - c. S76snmpdx スクリプトを以下のように 2 回実行します。

sh S76snmpdx stop を実行し、実行中の Solaris マスタ エージェントを停止します。

sh S76snmpdx start を実行し、Solaris マスタ エージェントおよび Netegrity サブエージェントを起動します。

UNIX システムで SNMP イベントトラップを設定する方法

UNIX システムで SNMP イベント トラップを設定するために必要なことは、以下のとおりです。

1. SNMP イベント トラップの有効化
2. `snmptrap.config` の設定

SNMP イベントトラップの有効化

SNMP のイベント トラップを有効にするには、XPSConfig ユーティリティを使用して、イベント ハンドラ ライブラリ (`libeventsnmp.so`) を XPSAudit リストに設定します。 `libeventsnmp.so` のデフォルトの場所は `policy_server_home/lib` です。

`policy_server_home`

ポリシー サーバのインストール場所を示します。

注: イベント ハンドラ ライブラリを設定するための XPSConfig ユーティリティの使用の詳細については、「ポリシー サーバ管理ガイド」を参照してください。

SNMP のイベント トラッピングを有効にした後、`snmptrap.config` ファイルを設定します。

`snmptrap.config` の設定

`snmptrap.config` を設定する方法

1. `/home/smuser/siteminder/config` にある `snmptrap.config` を編集します。
2. 受信するように指定するトラップについては、該当する行をコメント解除します。
3. トラップの送信先とする IP アドレス、ポート番号、およびコミュニティを指定します。
4. 新しい変更を含む `snmptrap.config` ファイルを保存します。
5. ポリシー サーバを再起動します。

詳細情報:

[ポリシー サーバの停止と再起動](#) (P. 567)

ポリシー サーバの停止と再起動

SNMP の設定変更を有効にするには、ポリシー サーバ管理コンソールの [ステータス] タブを使用して、ポリシー サーバを停止してから再起動する必要があります。

Red Hat Enterprise Linux Advanced Server に対する SNMP Get のテスト

SNMP を設定した後に SNMP Get をテストする必要があります。

SNMP Get をテストする方法

1. ネイティブ SNMP マスタ エージェントを起動します。Red Hat AS では、Solaris や HP-UX の場合のようにマスタ エージェントが自動的に起動することはありません。マスタ エージェントを起動するには、`/etc/rc1.d` ディレクトリに移動し、以下のコマンドを `root` として実行します。

```
K50snmpd start
```

2. 以下コマンドを `root` として実行し、Netegrity サブエージェントを起動します。

```
sh /etc/init.d/NetegrityAgent
```

3. Red Hat AS 上で Netegrity サブエージェントを停止するには、`root` として以下のコマンドを実行します。

```
sh $NETE_PS_ROOT/etc/snmp/conf/StopSubagent.sh
```


第 12 章：既存アプリケーション サーバへの 管理 UI のインストール

管理 UI インストール要件

管理 UI は、既存のアプリケーション サーバにインストールできます。管理 UI インストーラにより、アプリケーション サーバ固有の情報および必要な JDK の場所を要求されます。インストールを開始する前に、管理 UI ホスト システムがシステムおよびサードパーティーのコンポーネント要件すべてを満たすことを確認します。

以下のセクションは、既存のアプリケーション サーバインフラストラクチャに 管理 UI をインストールするための最小のシステムおよびアプリケーション サーバ要件を詳述します。

管理 UI システム要件

管理 UI ホストは、以下の最小のシステム要件を満たす必要があります。

注： サポートされている CA およびサードパーティ コンポーネントのリストについては、テクニカルサポート サイトの **SiteMinder 12.52 SP1** プラットフォームのサポート マトリックスを参照してください。

Windows システム要件の確認

既存のアプリケーション サーバに 管理 UI をインストールしている場合は、Windows システムが以下の最小限のシステム要件を満たすことを確認します。

- **CPU** --x86 または x64、1.2 GHz 以上
- **メモリ** - 1 GB のシステム RAM 2 GB をお勧めします。

注： WebSphere を実行している場合、2 GB のシステム RAM が必要です。

- **使用可能なディスク領域** - 540 MB

注： WebSphere を実行している場合、2 GB の使用可能なディスク領域が必要です。

- 一時ディレクトリ領域 - 3 GB
- **JDK** -- 管理 UI をインストールするシステムに必須 JDK バージョンが、インストールされていること。
- **画面解像度** - 管理 UI を正常に表示するための解像度 1024 x 768 以上、256 色以上

UNIX システム要件の確認

既存のアプリケーションサーバに 管理 UI をインストールする場合、UNIX システムは以下の最小システム要件を満たす必要があります。

- **CPU**

- Solaris -- UltraSparc、440 MHz 以上
- Red Hat Linux -- x86 または x64、700 MHz 以上

注: Red Hat 6 オペレーティング システムはパフォーマンスのエントロピーに依存します。コンポーネントをインストールする前にエントロピーを増やします。十分なエントロピーがないと、インストールの完了までに非常に時間がかかることがあります。シンボリック リンクを設定するために、以下のコマンドを使用します。

```
mv /dev/random /dev/random.org
ln -s /dev/urandom /dev/random
```

- **メモリ** - 1 GB のシステム RAM 2 GB をお勧めします。

注: WebSphere を実行している場合、2 GB のシステム RAM が必要です。

- **使用可能なディスク領域** - 540 MB

注: WebSphere を実行している場合、2 GB の使用可能なディスク領域が必要です。

- 一時ディレクトリ領域 - 3 GB

- **JDK** -- 管理 UI をインストールするシステムに必須 JDK バージョンが、インストールされていること。

注: アプリケーションサーバが Red Hat Linux オペレーティング システム上で実行される場合は、管理 UI をインストールするときに IBM JDK 用の無制限の暗号 jar ファイルをインストールします。

- **画面解像度** - 管理 UI を正常に表示するための解像度 1024 x 768 以上、256 色以上

アプリケーション サーバ要件

管理 UI は J2EE アプリケーションで、サポートされているアプリケーション サーバを必要とします。以下の点に注意してください。

- JBoss、WebLogic または WebSphere のサポートされているバージョンは、管理 UI をホストするシステムにインストールされます。
- 管理 UI はアプリケーション サーバ上で展開する唯一のアプリケーションです。

注: サポートされている CA およびサードパーティ コンポーネントのリストについては、テクニカルサポート サイトの **SiteMinder 12.52 SP1** プラットフォームのサポート マトリックスを参照してください。

JBoss

管理 UI インストールのために JBoss を準備するには、HDScanner サービスを無効にします。

次の手順に従ってください:

1. `jboss_home/server/server_profile/deploy` に移動します。

`jboss_home`

JBoss のインストールパスを指定します。

`server_profile`

アプリケーション サーバで展開したサーバ プロファイルの名前を指定します。

例: デフォルト

2. サービスを無効にするために以下のファイルを削除します。

`hdscanner-jboss-beans.xml`

アプリケーション サーバとしての WebLogic

以下のセクションでは、SiteMinder アプリケーション サーバとして WebLogic を使用するための基本的な手順について説明します。

WebLogic のインストール

SiteMinder によってサポートされている WebLogic サーバのバージョンをインストールします。

注: WebLogic サーバのインストールの詳細については、[BEA の WebLogic サーバ ドキュメント](#)を参照してください。

WebLogic アプリケーション サーバ インスタンスの作成

管理 UI をインストールする前に、WebLogic インストールの一部である設定ウィザードを使用して WebLogic ドメインを作成し、以下の操作を実行します。

- ドメイン名を書き留めます。管理 UI をインストールするときにドメイン名が必要になります。
- [Basic WebLogic Server Domain] テンプレートを選択します。
- JAVA_HOME 変数が setDomainEnv.cmd/.sh ファイルで必須 Java 環境用のパスに設定されていることを確認します。このファイルは `web_logic_home¥user_projects¥domains¥weblogic_domain¥bin` にあります。

`web_logic_home`

WebLogic サーバのインストールパスを示します。

`weblogic_domain`

作成した WebLogic ドメインの名前を示します。

WebLogic ドメインの確認

以下の点を確認します。

- WebLogic が実行されている。
- `http://server.domain.port/console` で WebLogic コンソールにアクセスできる。
例 : `http://myserver.mycompany.com:7001/console`
- WebLogic コンソールの [Domain Configurations] の下で、ドメインリンクを選択し、作成した WebLogic ドメインが既存のドメインのリスト内に表示されている。

注: 検証を完了したら、管理 UI インストールの準備をするためにアプリケーションサーバをシャットダウンします。

アプリケーション サーバとしての WebSphere

以下のセクションでは、SiteMinder アプリケーションサーバとして WebSphere を使用するための基本的な手順について説明します。

WebSphere のインストール

WebSphere をインストールするために IBM ドキュメントを使用します。

WebSphere をインストールする際は、以下の点を考慮します。

- [サーバとクライアント] オプションを選択します。
- Administrative Security オプションを無効にします。
- (Solaris) Embedded Messaging サービスをインストールする前に以下を行います。
 - 以下のグループを設定します。
 - mqm
 - mqbrkrs
 - 以下のユーザを設定します。
 - mqm
 - root

注: 詳細については、IBM のドキュメントを参照してください。

WebSphere が動作していることの確認

管理 UI をインストールする前に、IBM によって提供される **snoop** ユーティリティを使用して、WebSphere が正しくインストールされることを確認します。

WebSphere が動作していることを確認する方法

1. WebSphere が正しくインストールされていることを確認するには、「`http://<fqdn:port>/snoop`」と入力します。

例 : `http:MyServer.MyCompany.com:9080/snoop`.

WebSphere が正しくインストールされている場合、ブラウザに [Snoop Servlet—Request Client Information] ページが表示されます。

2. WebSphere アプリケーション サーバ プラグインが正しくインストールされていることを確認するには「`http://<fqdn>/snoop`」と入力します。

例 : `http://MyServer.MyCompany.com/snoop`

WebSphere が正しくインストールされている場合、ブラウザに同じ [Snoop Servlet—Request Client Information] ページが表示されます。

これで WebSphere が正常に動作していることを確認しました。

注: WebSphere について追加の支援が必要な場合は、IBM 技術サポートにお問い合わせください。

UI とポリシー サーバの間の信頼関係

デフォルト スーパーユーザのアカウント (**siteminder**) およびパスワードを使用して最初に 管理 UI にログインするときに、管理 UI とポリシー サーバの間の信頼関係が確立します。 この関係はユーザの環境を管理するのに必要です。

スーパーユーザ アカウントの認証情報はポリシー ストアに格納されます。ポリシー サーバのインストール中にデフォルト ポリシー ストアの 1 つを設定する場合、これらの認証情報はインストーラにより自動的にサブミットされます。ポリシー サーバのインストールと関係なくポリシー ストアを設定する場合は、**XPSRegClient** ユーティリティを使用して、認証情報をポリシー サーバにサブミットしてください。ポリシー サーバは、登録リクエストが有効でありリレーションシップが構築できることを確認するために、これらの認証情報を使用します。

重要: スーパーユーザ アカウント認証情報がポリシー ストアにサブミットされる時間と管理者が 管理 UI にログインする時間の間には、24 時間の制限が存在します。認証情報が設定されてから 24 時間以内に 管理 UI への最初のログインを実行しなかった場合は、**XPSRegClient** ユーティリティを使用して認証情報をリセットしてください。

管理 UI インストール チェックリスト

管理 UI のインストールを開始する前に、以下を完了してください。

- サポートされているオペレーティング システムを使用していることを確認してください。
- 管理 UI ホスト システムが最小のシステム要件を満たすことを確認してください。
- (Linux) 必要な Linux ライブラリが 管理 UI ホスト システムにインストールされていることを確認します。
- サポートされたアプリケーション サーバが 管理 UI ホスト システム上にインストールされることを確認してください。

- 必要な JDK が管理 UI ホストシステムにインストールされることを確認してください。
- ポリシーストアがいつ設定されたか決定します。

ポリシーストアが 24 時間以上前に設定された場合は、管理 UI をインストールする前に XPSRegClient ユーティリティを使用して、デフォルトの SiteMinder スーパーユーザアカウント認証情報をポリシーサーバにサブミットします。ポリシーサーバは、管理 UI との信頼できるリレーションシップを構築するためにこれらの認証情報を必要とします。

注: サポートされている CA およびサードパーティコンポーネントのリストについては、テクニカルサポートサイトの SiteMinder 12.52 SP1 プラットフォームのサポートマトリックスを参照してください。

詳細情報:

[アプリケーションサーバ要件 \(P. 571\)](#)

[管理 UI システム要件 \(P. 569\)](#)

管理 UI をインストールする方法

管理 UI をインストールするには、以下の手順に従います。

1. インストールチェックリストを確認してください。
2. (Linux) 必要な Linux ライブラリ要件を確認します。
3. 管理 UI インストーラ用のアプリケーションサーバ情報を収集します。
4. 管理 UI をインストールします。
5. アプリケーションサーバを起動します。

必要とされる Linux ライブラリ

Linux オペレーティング環境上で動作するコンポーネントには、特定のライブラリ ファイルが必要です。正しいライブラリをインストールしないと、以下のエラーを引き起こす場合があります。

```
java.lang.UnsatisfiedLinkError
```

このコンポーネントの Linux バージョンをインストール、設定、またはアップグレードする場合、ホスト システム上で以下のライブラリが必要になります。

Red Hat 5.x

```
compat-gcc-34-c++-3.4.6-patch_version.i386
```

Red Hat 6.x(32 ビット)

```
libstdc++-4.4.6-3.el6.i686.rpm
```

オペレーティング環境用の適切な 32 ビット C ランタイム ライブラリを使用するには、上記の rpm をインストールします。

Red Hat 6.x (64 ビット)

libXau-1.0.5-1.el6.i686.rpm

libxcb-1.5-1.el6.i686.rpm

libstdc++-4.4.6-4.el6.i686.rpm

compat-db42-4.2.52-15.el6.i686.rpm

compat-db43-4.3.29-15.el6.i686.rpm

libX11-1.3-2.el6.i686.rpm

libXrender-0.9.5-1.el6.i686.rpm

libexpat.so.1 (expat-2.0.1-11.el6_2.i686.rpm により提供)

libfreetype.so.6 (freetype-2.3.11-6.el6_2.9.i686.rpm により提供)

libfontconfig.so.1 (fontconfig-2.8.0-3.el6.i686.rpm により提供)

libICE-1.0.6-1.el6.i686.rpm

libuuid-2.17.2-12.7.el6.i686.rpm

libSM-1.1.0-7.1.el6.i686.rpm

libXext-1.1-3.el6.i686.rpm

compat-libstdc++-33-3.2.3-69.el6.i686.rpm

compat-db-4.6.21-15.el6.i686.rpm

libXi-1.3-3.el6.i686.rpm

libXtst-1.0.99.2-3.el6.i686.rpm

libXft-2.1.13-4.1.el6.i686.rpm

libXt-1.0.7-1.el6.i686.rpm

libXp-1.0.0-15.1.el6.i686.rpm

アプリケーション サーバ情報の収集

管理 UI インストーラは、管理 UI ホストシステムにインストールされるアプリケーション サーバに関する特定の情報を必要とします。

以下のセクションは、アプリケーション サーバのタイプに応じた必要な情報を詳述します。

注: ワークシートは、管理 UI のインストール前に必要な情報を収集および記録するために提供されます。

JBoss 情報

管理 UI をインストールおよび登録する前に、JBoss に関する以下の情報を収集します。

JBoss インストール フォルダ

JBoss がインストールされているフォルダへのパス

JBoss URL

JBoss ホスト システムの完全修飾 URL

JDK

必須 JDK のインストール場所

WebLogic 情報

管理 UI をインストールおよび登録する前に、以下の情報を収集します。

WebLogic バイナリ フォルダ

WebLogic インストール ディレクトリへのパス

WebLogic ドメイン フォルダ

管理 UI 用に作成した WebLogic ドメインへのパス

WebLogic サーバ名

WebLogic ドメインを設定する WebLogic サーバの名前

アプリケーション サーバ URL およびポート

WebLogic ホスト システムの完全修飾 URL

JDK

必須 JDK のインストール場所

WebSphere 情報

管理 UI をインストールおよび登録する前に、WebSphere に関する以下の情報を収集します。

WebSphere インストール フォルダ

WebSphere がインストールされているフォルダへの完全パス

WebSphere URL

WebSphere ホスト システムの完全修飾 URL

Server name

アプリケーション サーバの名前

プロファイル名

管理 UI に使用されているプロファイルの名前

セル名

サーバが存在するセルの名前

ノード名

サーバが存在するノードの名前

JDK

必須 JDK のインストール場所

管理 UI のインストール

以下のセクションでは、既存のアプリケーション サーバインフラストラクチャに 管理 UI をインストールする方法について詳しく説明します。

インストールする前に

管理 UI をインストールする前に、以下の点を考慮してください。

- テクニカルサポートサイトで、インストールメディアを使用して管理 UI をインストールします。

注: インストールメディア名のリストについては、「ポリシー サーバリリース ノート」を参照してください。

- 既存のアプリケーション サーバインフラストラクチャにインストールする場合には、以下の手順が適用されます。インストールするべきスタンドアロン オプションを使用している場合には、「管理 UI のインストール」を参照してください。
- (Windows) 管理 UI ホスト システムからインストーラを実行します。マップされたネットワーク共有または UNC パスからインストーラを実行しないでください。
- インストール zip には、インストールメディアと同じレベルに `layout.properties` ファイルが含まれています。インストール zip を展開した後にインストールメディアを移動した場合、プロパティ ファイルを同じ場所に移動しないと、インストールに失敗します。
- (Red Hat Linux) Red Hat 6 オペレーティング システムはパフォーマンスのエントロピーに依存します。コンポーネントをインストールする前にエントロピーを増やします。十分なエントロピーがないと、インストールの完了までに非常に時間がかかることがあります。シンボリック リンクを設定するために、以下のコマンドを使用します。

```
mv /dev/random /dev/random.org
ln -s /dev/urandom /dev/random
```

- (UNIX) 権限に応じて、以下のコマンドを実行し、実行可能権限をインストールメディアが含まれるディレクトリに追加します。

```
chmod -R+x directory
directory
```

インストールメディアが存在するディレクトリを指定します。

- (UNIX) 管理 UI をインストールするユーザは、アプリケーション サーバがインストールされるディレクトリ用の読み取り/書き込み権限を持っている必要があります。
- (UNIX) 別のサブネットにまたがって管理 UI インストーラを実行した場合、クラッシュすることがあります。ホストシステムに管理 UI を直接インストールします。

詳細情報:

[管理 UI のインストール](#) (P. 465)

[管理 UI をインストールする方法](#) (P. 470)

Windows システムに 管理 UI をインストールする

管理 UI を既存のアプリケーション サーバにインストールして、アクセス制御、レポートおよびポリシーに関連しているすべてのタスクに対する管理コンソールを提供します。

次の手順に従ってください:

1. 実行中のすべてのアプリケーションを終了します。
2. インストール メディアに移動します。
3. *installation_media* をダブルクリックします。

installation_media

管理 UI インストール実行可能ファイルを指定します。

インストーラが起動します。

注: インストール メディア名のリストについては、「ポリシー サーバリリース ノート」を参照してください。

4. 収集した情報に基づいて、インストールに必要な値を入力します。
5. インストール設定を確認し、[インストール] をクリックします。

これで、管理 UI がインストールされました。

注: ポリシー サーバに 管理 UI を登録するまでは、環境管理のために 管理 UI を使用することができません。

GUI を使用した 管理 UI のインストール

管理 UI を既存のアプリケーション サーバにインストールして、アクセス制御、レポートおよびポリシー分析に関連しているすべてのタスクに対する管理コンソールを提供します。

以下の手順に従います。

1. フォアグラウンドで実行しているアプリケーションをすべて終了します。
2. シェルを開き、インストール メディアに移動します。

3. 以下のコマンドを入力します。

```
./installation_media gui
```

```
installation_media
```

管理 UI インストール実行可能ファイルを指定します。

インストーラが起動します。

注: インストール メディア名のリストについては、「ポリシー サーバリリース ノート」を参照してください。

4. 完了したインストール ワークシートを使用して、必要な値を入力します。
5. インストール設定を確認し、[インストール] をクリックします。
これで、管理 UI がインストールされました。
6. [完了] をクリックし、システムを再起動します。

これで、管理 UI がインストールされました。

注: ポリシー サーバに 管理 UI を登録するまでは、環境管理のために 管理 UI を使用することができません。

詳細情報:

[管理 UI を登録する方法](#) (P. 584)

UNIX コンソールを使用した 管理 UI のインストール

管理 UI を既存のアプリケーション サーバにインストールして、アクセス制御、レポートおよびポリシー分析に関連しているすべてのタスクに対する管理コンソールを提供します。

以下の手順に従います。

1. フォアグラウンドで実行しているアプリケーションをすべて終了します。

2. シェルを開き、インストール メディアに移動します。
3. 以下のコマンドを入力します。

```
./installation_media -i console  
installation_media
```

管理 UI インストール実行可能ファイルを指定します。

インストーラが起動します。

注: インストール メディア名のリストについては、「ポリシー サーバリリース ノート」を参照してください。

4. 完了したインストール ワークシートを使用して、必要な値を入力します。
5. インストール設定を確認し、**Enter** キーを押します。
これで、管理 UI がインストールされました。

6. **Enter** キーを押します。
インストーラが閉じます。

7. システムを再起動します。
これで、管理 UI がインストールされました。

注: ポリシー サーバに 管理 UI を登録するまでは、環境管理のために 管理 UI を使用することができません。

詳細情報:

[管理 UI を登録する方法](#) (P. 584)

管理 UI を登録する方法

管理 UI を使用する前にそれを登録して環境を管理します。管理 UI を登録すると、管理 UI とポリシー サーバとの間に信頼できる接続が作成されます。

このプロセスは、既存のアプリケーション サーバインフラストラクチャにインストールされた 管理 UI の登録方法について説明します。スタンドアロン オプションを使用してインストールした 管理 UI を登録するには、「管理 UI のインストール」を参照してください。

次の手順に従ってください:

1. [登録ウィンドウをリセットします](#) (P. 468)。
2. 必要な場合、[FIPS 環境変数を作成します](#) (P. 476)。
3. [アプリケーション サーバを起動します](#) (P. 589)。
4. [管理 UI を登録します](#) (P. 590)。

詳細情報:

[管理 UI のインストール](#) (P. 465)

[管理 UI を登録する方法](#) (P. 476)

管理 UI 登録ウィンドウのリセット

以下のいずれかのアクションが 24 時間よりも前に実行した場合は、この手順が必要です。

- ポリシー サーバインストール ウィザードを使用してポリシー ストアを自動的に設定しました。
- XPSRegClient ユーティリティを使用して、SiteMinder スーパーユーザ認証情報をポリシー サーバにサブミットしました。

注: (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](#) (P. 598) します。

次の手順に従ってください:

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

siteminder_administrator

SiteMinder の管理者を指定します。以下の一部として 管理 UI をインストールする場合

- 新しい 12.52 SP1 環境で、以下のデフォルト アカウントを指定します。

siteminder

- アップグレードの一部としてインストールする場合は、ポリシー ストア内でのスーパーユーザ権限のある **SiteMinder** 管理者アカウントを指定します。ポリシー ストア内でのスーパーユーザアカウントを持たない場合は、**smreg** ユーティリティを使用してデフォルト アカウントを作成します。

passphrase

SiteMinder 管理者アカウントのパスワードを指定します。

-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

(オプション) 管理 UI をインストールしてログインした後、登録処理を完了する必要がある時間を指定します。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：1440 (24 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。試行の失敗は、管理 UI への最初のログイン時に、誤った SiteMinder 管理者認証情報をサブミットすることに起因する場合があります。

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。

ユーティリティは、ポリシー サーバに管理者認証情報を提供します。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認証情報を使用します。

FIPS 環境変数の作成

ユーザの環境が以下の基準を両方とも満たす場合、管理 UI を初めて登録するために FIP 環境変数を作成する必要があります。

- 登録しているポリシー サーバは FIP 専用モードで作動しています。
- 管理 UI は、ポリシー サーバ ホスト システムにインストールされません。

以下の手順に従います。

1. 以下のいずれかの操作を実行します。

- (Windows) 管理者ユーザとして 管理 UI ホスト システムにログインします。
- (UNIX) 管理 UI をインストールしたユーザとして 管理 UI ホスト システムにログインします。

2. 以下の環境変数を設定します。

CA_SM_PS_FIPS140=ONLY

注: 環境変数の設定の詳細については、お使いの OS のドキュメントを参照してください。

3. 管理 UI を正しく実行する Windows または UNIX シェルが **CA_SM_PS_FIPS140** 変数を認識することを確認してください。

アプリケーション サーバの起動

既存のアプリケーション サーバ インフラストラクチャにインストールした場合には、以下の手順が適用されます。 スタンドアロン オプションを使用して、管理 UI をインストールした場合には、「管理 UI のインストール」を参照してください。

以下の手順に従います。

1. 以下のいずれかの操作を実行します。

- **JBoss** - コマンド プロンプトから *jboss_home¥bin* に移動します。

jboss_home

JBoss のインストール パスを指定します。

- **WebLogic** - コマンド プロンプトから *domains¥bin* に移動します。

domains

管理 UI 用に作成した WebLogic ドメインのパスを指定します。

例 : C:¥bea¥user_projects¥domains¥mydomain

- **WebSphere** - コマンド プロンプトから *profile¥bin* に移動します。

profile

管理 UI 用に作成した WebSphere プロファイル名のパスを指定します。

例 : C:¥Program

Files¥IBM¥WebSphere¥AppServer¥profiles¥AppSvr01¥bin

2. 以下のいずれかの操作を実行します。

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

- **JBoss**

- Windows : 以下のコマンドを入力し Enter キーを押します。

run.bat

- UNIX : 以下のコマンドを入力し Enter キーを押します。

run.sh

■ WebLogic

- Windows : 以下のコマンドを入力し Enter キーを押します。
`startWebLogic.cmd`
- UNIX : 以下のコマンドを入力し Enter キーを押します。
`startWebLogic.sh`

■ WebSphere

- Windows : 以下のコマンドを入力し Enter キーを押します。
`startServer.bat identifier`
- UNIX : 以下のコマンドを入力し Enter キーを押します。
`startServer.sh identifier`

identifier

WebSphere インストール用の識別子を指定します。

例 : `startServer.bat Server1`

アプリケーション サーバが開始されます。

詳細情報:

[管理 UI のインストール](#) (P. 465)

[アプリケーション サーバの起動](#) (P. 477)

管理 UI の登録

環境管理を始めるために、ポリシー サーバに 管理 UI を登録します。

以下の手順に従います。

1. 以下のいずれかの操作を実行します。

- (Windows) 管理 UI ショートカットを使用して 管理 UI を開きます。
- (UNIX) Web ブラウザを開き、以下の場所に移動します。

`host:port/iam/siteminder/adminui`

注: ホスト システムに Web ブラウザがない場合には、ログイン画面にリモートアクセスすることもできます。

ホスト

管理 UI ホスト システムの完全修飾名を指定します。

ポート

JBoss が HTTP リクエストをリスンするポートを指定します。

SiteMinder 管理 UI のログイン画面が表示されます。

2. [ユーザ名] フィールドに以下の値を入力します。

siteminder

3. [パスワード] フィールドに、SiteMinder スーパーユーザ アカウントのパスワードを入力します。

注: スーパーユーザ アカウントのパスワードにドル記号 (\$) 文字が含まれている場合は、ドル記号文字の各インスタンスを \$DOLLAR\$ に置換します。たとえば、SiteMinder スーパーユーザ アカウント パスワードが \$password の場合は、パスワード フィールドに「\$DOLLAR\$password」と入力します。

4. [サーバ] フィールドに、ポリシー サーバ ホストの完全修飾名を入力します。

以下の点を考慮します。

- 有効な IPv4 アドレスまたは IPv6 アドレスに入ることができます。
- ポートを指定しない場合、デフォルトのポリシー サーバ 認証ポートである 44442 がデフォルトで登録されます。

管理 UI が開き、ポリシー サーバに登録されます。

詳細情報:

[「ファイルに登録がありません」エラーが表示される \(P. 611\)](#)

アプリケーション サーバを停止します。

既存のアプリケーション サーバ インフラストラクチャにインストールした場合には、以下の手順が適用されます。 スタンドアロン オプションを使用して、管理 UI をインストールした場合には、「管理 UI のインストール」を参照してください。

アプリケーション サーバを停止する方法

1. 以下のいずれかを実行します。

- **JBoss** - 管理 UI ホスト システムから、開始タスク エンジン コマンド プロンプトを開きます。
- **WebLogic** - 管理 UI ホスト システムから、開始タスク エンジン コマンド プロンプトを開きます。
- **WebSphere** - コマンド プロンプトから *profile¥bin* に移動します。

profile

管理 UI 用に作成した WebSphere プロファイル名のパスを指定します。

例 : C:¥Program

Files¥IBM¥WebSphere¥AppServer¥profiles¥AppSvr01¥bin

2. 以下のいずれかを実行します。

- **JBoss** - 以下のキーボードの組み合わせを入力します。
Ctrl + C
- **WebLogic** - 以下のキーボードの組み合わせを入力します。
Ctrl + C

■ WebSphere

- Windows : 識別子「stopServer.bat」を入力し、Enter キーを押します。

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する前に、管理者権限でコマンドラインウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドラインウィンドウを開きます。

- UNIX : 識別子「stopServer.sh」を入力し、Enter キーを押します。

identifier

WebSphere インストール用の識別子を指定します。

例 : stopServer.bat Server1

アプリケーション サーバが停止します。

詳細情報:

[管理 UI のインストール](#) (P. 465)

[アプリケーション サーバを停止します。](#) (P. 481)

管理者認証情報

デフォルトでは、管理 UI は SiteMinder 管理者認証情報用のソースとしてポリシーストアを使用します。たとえばコーポレートディレクトリのような外部ストアを使用するために、管理 UI を設定することができます。

注: 外部管理者ユーザストアの設定の詳細については、「ポリシー サーバ設定ガイド」を参照してください。

管理 UI の高可用性

予期しない機能停止で SiteMinder オブジェクトの管理が妨げられないように、複数の 管理 UI をインストールします。別の 管理 UI をインストールする前に、以下を考慮します。

- まだ 管理 UI との信頼できる接続を共有していないポリシー サーバに、管理 UI を登録します。別のポリシー サーバに登録することで、1 つのポリシー サーバが機能停止しても両方の GUI が無効になることはありません。
- 管理 UI は、複数のポリシー サーバにフェールオーバーできません。ただし、複数のポリシー サーバを管理するために 管理 UI を設定することができます。
- 既存の 管理 UI が外部 SiteMinder 管理者認証に対して設定されている場合。
 - 同じ外部ストアで新しい 管理 UI を設定します。同じ外部ストアを使用して新しい 管理 UI の設定することにより、すべての SiteMinder 管理者がすべての GUI で利用可能になります。
 - 同じネットワーク識別子を使用して同じ外部ストアへの後続の 管理 UI 接続を設定してください。同じ外部ストアへの複数の 管理 UI 接続で異なるネットワーク識別子を使用することはサポートされていません。

例：最初の接続で 172.16.0.0 を設定した場合は、後続の接続の作成でも 172.16.0.0 を使用します。最初の接続で comp001@example.com を設定した場合は、後続の接続の作成でも comp001@example.com を使用します。

Windows での管理 UI のアンインストール

システムで不要になった場合は、既存のアプリケーション サーバから 管理 UI をアンインストールします。

次の手順に従ってください：

1. アプリケーション サーバを停止します。
2. Windows の [コントロール パネル] を開き、プログラムのリストに移動します。
3. CA SiteMinder 管理 UI を右クリックします。

4. [アンインストール/変更] をクリックします。
5. ウィザードの指示に従います。

注: 共有ファイルを削除するように促される場合は、[すべていいえ] をクリックします。

6. 要求された場合はシステムを再起動します。
管理 UI がアンインストールされます。

詳細情報:

[\(オプション\) 管理 UI のアンインストール \(P. 489\)](#)

UNIX での管理 UI のアンインストール

システムで不要になった場合は、既存のアプリケーション サーバから 管理 UI をアンインストールします。

注: このコンポーネントをアンインストールする際には、手動でインストールディレクトリを削除しません。アンインストール シェル スクリプトを実行します。インストールディレクトリのみを削除すると、関連するレジストリはそのまま残されます。このホスト システムにこのコンポーネントを再インストールしようとする場合、エントリは成功したインストールを回避できます。<tref/>

以下の手順に従います。

1. アプリケーション サーバを停止します。
2. シェルを開き、以下のディレクトリに移動します。

```
administrative_ui_home/CA/adminui/install_config_info  
administrative_ui_home
```

管理 UI 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。

```
./smwam-ui-uninstall.sh
```

管理 UI をアンインストールするプロセスが開始されます。

4. プロンプトに従って、管理 UI をアンインストールします。
管理 UI が削除される時、インストーラはプロンプトを表示します。
管理 UI がアンインストールされます。

詳細情報:

[管理 UI のインストール](#) (P. 465)

[UNIX 上の 管理 UI のアンインストール](#) (P. 490)

第 13 章: トラブルシューティング

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 サーバのトラブルシューティング](#) (P. 597)

[ポリシー ストアのトラブルシューティング](#) (P. 604)

[OneView モニタのトラブルシューティング](#) (P. 607)

[管理 UI のトラブルシューティング](#) (P. 609)

[レポート サーバのトラブルシューティング](#) (P. 618)

ポリシー サーバのトラブルシューティング

以下のセクションでは、インストール中にポリシー サーバで発生する可能性がある一般的な問題と、その解決方法案について詳しく説明します。

Solaris 上の NETE_PS_ALT_CONF_FILE 環境変数

Solaris 上にポリシー サーバをインストールした後、`nete_ps_env.ksh` スクリプトに以下のエントリが含まれている場合があります。

```
export NETE_PS_ALT_CONF_FILE=/export/siteminder/config/.siteminder.conf
```

NETE_PS_ALT_CONF_FILE 環境変数は、`stop-all` および `start-all` スクリプトによって使用されます。これらのスクリプトはそれぞれ、ポリシー サーバのサービスを停止、または起動します。`.siteminder.conf` ファイルはこれらのスクリプトによって作成された一時ランタイム ファイルであり、これによってユーザの SiteMinder 設定が変更されることはありません。

NETE_PS_ALT_CONF_FILE 環境変数を変更しないでください。

ポリシー サーバがインストール後に起動しない

Windows および UNIX システムで有効

問題の状況:

ポリシー サーバをインストールしましたが、起動しません。

解決方法:

不正な JRE バージョンをインストールした可能性があります。正しい JRE バージョンを使用していることを確認します。

注: サポートされている CA およびサードパーティ コンポーネントのリストについては、テクニカルサポート サイトの **SiteMinder 12.52 SP1** プラットフォームのサポート マトリックスを参照してください。

SiteMinder 環境変数がプロファイル ファイルに設定されていない

UNIX で該当

症状:

ポリシー サーバがインストールされましたが、SiteMinder 環境変数 (smprofile.ksh) が .profile ファイルに追加されませんでした。そのため、SiteMinder 環境変数を手動で設定する必要があります。

解決方法:

SiteMinder 環境変数を追加する方法

1. ポリシー サーバ ホスト システムにログインします。
2. シェルを開き、*siteminder_home* 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。

3. 以下のコマンドを実行します。

```
smprofile.ksh
```

SiteMinder 環境変数が設定されます。

Winsock エラー 10054 メッセージ

Windows で該当

問題の状況:

ポリシー サーバにログインしようとする、「続行できません。winsock エラー 10054」という内容のメッセージが表示されます。

解決方法:

問題の原因は、以下のいずれかの可能性があります。

- ポリシー ストアに、適切な **SiteMinder** スキーマが含まれていません。正しい **SiteMinder** スキーマをインポートしたことを確認します。
- ポリシー サーバが実行されていません。このサーバを起動するには、ポリシー サーバ管理コンソールの [ステータス] タブを使用します。

重要: Windows Server 2008 上でこのグラフィカル ユーザ インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。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。

- ポリシー サーバが、ポリシー ストアに正しく接続されていません。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、[テスト接続] をクリックし、ポリシー ストアが正常に接続することを確認します。正しく接続していない場合、ポリシー ストアでポリシー サーバに指定することにより、[データ] タブのデータ ソース情報の値をもう一度入力します。

SiteMinder ライセンスの使用

症状:

- 現在ポリシー サーバ評価版ライセンスを使用しており、正式なライセンスを取得して追加する必要があります。
- SiteMinder ライセンスを持っていますが見つかりません。
- SiteMinder ライセンスを持っていますが、新しい製品キーで更新する方法がわかりません。

解決方法:

SiteMinder ライセンスを要求する方法

1. [テクニカル サポート サイト](#)に移動します。
2. [CA Licensing Inquires] をクリックします。このリンクは [Address Licensing Needs] の下にあります。
[CA Customer Care] サイトが新規ウィンドウで開きます。
3. [Licensing Issue Request] をクリックします。このリンクは [Contact Us] の下にあります。
オンラインのリクエスト フォームが新規ウィンドウで開きます。
4. 必要な情報を入力して、[Submit] をクリックします。

正式な SiteMinder ライセンスをポリシー サーバに追加する方法

1. SiteMinder ライセンスを要求します。
2. ポリシー サーバ ホスト システムにアクセスします。
3. 以下のいずれかを実行します。
 - (Windows) `siteminder_home\license` に移動します
 - (UNIX) `siteminder_home/license` 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。
4. ライセンス ディレクトリに `license.dat` ファイルをコピーします。
5. ポリシー サーバを再起動します。

既存の SiteMinder ライセンスを見つける方法

1. [テクニカル サポート サイト](#)にログインします。
2. [Licensing] をクリックします。[Licensing] は [Support] の下にあります。
[CA Licensing] 画面が表示されます。
3. [View Licenses] をクリックします。[View Licenses] は [SiteMinder and Identity Manager Licenses] の下にあります。
それぞれのキーが含まれるライセンス詳細のすべてが表示されます。

ライセンス ファイルに SiteMinder ライセンス キーを適用する方法

1. ポリシー サーバ ホスト システムにアクセスします。
2. 以下のいずれかを実行します。
 - (Windows) `siteminder_home¥license` に移動します
 - (UNIX) `siteminder_home/license` 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。
3. `license.dat` ファイルを開きます。
4. サポート サイトから獲得したライセンス キーをコピーし、ライセンス ファイルに貼り付けます。
5. ライセンス ファイルを保存します。
6. ポリシー サーバを再起動します。

英語以外の入力文字にジャンク文字が含まれる

UNIX/Linux 上で有効

症状:

英語以外の入力文字の一部がコンソール ウィンドウに正しく表示されません。 -

解決方法:

コンソール ウィンドウのターミナルの設定を確認します。 コンソールが入力文字の高位 (8) ビットをクリアしないことを確認します。 以下のコマンドを実行します。

```
stty -istrip
```

アンインストール中に Java エラー メッセージが表示される

問題の状況:

ポリシー サーバ、Web エージェント、SDK、またはドキュメントをアンインストールしようとしたときに、アンインストール プログラムが停止し、以下のエラー メッセージの 1 つが表示されます。

- "Could not find a valid Java virtual machine to load. You need to reinstall a supported Java virtual machine."
- "No Java virtual machine could be found from your PATH environment variable. You must install a VM prior to running this program."

解決方法:

JRE が PATH 変数に設定されていることを確認します。

Windows 上で PATH 変数に JRE を設定します

PATH 変数に JRE を設定する方法

1. [コントロール パネル] に移動します。
2. [システム] をダブルクリックします。
3. [環境変数] ダイアログ ボックスで、Path システム変数に JRE の場所を追加します。

Solaris 上の PATH 変数での JRE の設定

PATH 変数に JRE を設定する方法

以下のコマンドを実行します。

1. `PATH=$PATH:<JRE>/bin`
JRE
JRE の場所を指定します。
2. `export PATH`

Adobe Acrobat Reader がインストールされない

Windows で該当

問題の状況:

Adobe Acrobat をインストールしようとする、インストールプログラムが停止します。

解決方法:

ポリシー サーバサービスの実行中に、Acrobat Reader のインストールプログラムが停止する場合は、ポリシー サーバ管理コンソールの [ステータス] タブを使用して、ポリシー サーバサービスを停止します。サービスを停止すると、インストールプログラムが起動します。

重要: Windows Server 2008 上でこのグラフィカル ユーザ インターフェイスにアクセスする場合は、管理者権限でショートカットを開きます。管理者としてシステムにログインしている場合でも、管理者権限を使用します。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。

ユーザ ストアとしての Active Directory の使用に関する問題

問題の状況:

ユーザ ストアとして Active Directory を使用するとき、ポリシー サーバがこのストアへ接続できないというエラー メッセージが発行されます。

解決方法:

Active Directory ベースのユーザ ストアを作成するときは、管理 UI で完全修飾ホスト名（たとえば `host.domain.com`）を指定します。マシンの IP アドレスを使用しないでください。また、Active Directory によって、その完全修飾ホスト名で識別されたポリシー サーバにリフェラルが送信されるため、ポリシー サーバがインストールされているマシンから `host.domain.com` および `domain.com` に ping できることを確認します。完全修飾ホスト名が無効で到達できない場合、ポリシー サーバはエラーメッセージを発行します。

AE がライブラリ「smjavaapi」のロードに失敗した システム エラー

Windows および UNIX システムで有効

問題の状況:

許可中に、「AE failed to load library 'smjavaapi'. System error: The specified module could not be found.」というエラー メッセージが表示されます。

解決方法:

Windows の場合は、PATH 変数を

<SiteMinder_installation>%config%JVMOptions.txt に設定します。UNIX システムの場合は、LD_LIBRARY_PATH を

<SiteMinder_installation>/config/JVMOptions.txt に設定します。

ポリシー ストアのトラブルシューティング

以下のセクションでは、インストール中にポリシー ストアで発生する可能性がある一般的な問題と、その解決方法案について詳しく説明します。

多数のオブジェクトを含むポリシー ストア

Windows および UNIX システムで有効

問題の状況:

ポリシー ストアから 管理 UI に例外 java.lang.IndexOutOfBoundsException が返されました。

解決方法:

多くのオブジェクトを含むポリシー ストアは、管理 UI に例外 java.lang.IndexOutOfBoundsException を返す場合があります。

レジストリ キー

%HKEY_LOCAL_MACHINE%SOFTWARE%Wow6432Node%Netegrity%SiteMinder%CurrentVersion%ObjectStore%MaxObjects を 100 未満の値 (50 など) に定義します。

SSL 初期化に失敗する

Windows および UNIX システムで有効

問題の状況:

私の環境は **Oracle Directory Server** ポリシー ストアで設定されています。
ポリシー ストアは **SSL** を介して通信するように設定されています。

以下のエラー メッセージを受信しました。

SSL 初期化に失敗する

以下のコマンドを実行した後、メッセージが表示されます。

```
smlldapsetup ldmod -fpstore -ssl1 -c/app/siteminder/ssl/cert8.db
```

解決方法:

1. **key3.db** ファイルが、**cert8.db** ファイルと同じディレクトリにあることを確認してください。
2. **smlldapsetup** コマンドを再実行します。**-c** オプションを使用して **SSL** クライアント証明書データベース ファイルが存在するディレクトリのパスを指定します。

例:

```
-c/app/siteminder/ssl/cert8.db
```

ODBC ポリシー ストア インポートが UserDirectory エラーで失敗する

症状:

ODBC ポリシー ストアにポリシー ストア データをインポートするとき、オブジェクトタイプ「**UserDirectory**」に対してポリシー ストアが「保存」操作に失敗したというエラー メッセージが表示されます。

解決方法:

ODBC ストアの **userDirectory** オブジェクト内のサーバ名が **512** 文字より長い可能性があります。これは、デフォルトで **SiteMinder** に同梱されている **MS SQL Server** および **Oracle** のポリシー ストア スキーマ スクリプトによって許可された限度を越えています。

以下のいずれかを実行します。

MS SQL Server ポリシー ストアのサポートされているバージョンにポリシー データをインポートする場合

1. `sm_mssql_ps.sql` を開きます。

注: このスキーマ スクリプトは `policy_server_home¥db¥SQL` にあります。

2. 以下のテキストを探します。

```
CREATE TABLE smuserdirectory5
```

3. 必要に応じて、「server smstringreq512N」を、以下のうちの 1 つに変更します。

- server smstringreq1024,N
- server smstringreq4000,N

4. ポリシー ストア スキーマをポリシー ストアに再インポートします。
5. ポリシー ストア データをインポートします。

Oracle ポリシー ストアのサポートされているバージョンにポリシー データをインポートする場合

1. `sm_oracle_ps.sql` を開きます。

注: このスキーマ スクリプトは `policy_server_home¥db¥SQL` にあります。

2. 以下のテキストを探します。

```
CREATE TABLE smuserdirectory5
```

3. 必要に応じて、「server VARCHAR2(512) NOT NULL」を、以下のうちの 1 つに変更します。

- server VARCHAR2(1024) NOT NULL,
- server VARCHAR2(4000) NOT NULL,

4. ポリシー ストア スキーマをポリシー ストアに再インポートします。
5. ポリシー ストア データをインポートします。

OneView モニタのトラブルシューティング

以下のセクションでは、インストール中に **OneView** モニタで発生する可能性がある一般的な問題と、その解決方法案について詳しく説明します。

変更された UNIX/Sun Java System Web Server 設定ファイルの修正

ServletExec インストーラが Oracle iPlanet Web サーバ設定ファイルを変更した場合、**OneView** モニタ UI を設定した後で Web サーバインスタンスは失敗します。ServletExec インストーラによって、ポリシー サーバからのエントリと矛盾するエントリがこれらのファイル内に追加されます。

以下の手順に従います。

1. 以下の設定ファイルを開きます：
`/sunjavasystem_home/servers/https-web_server_instance_name.domain.com/config/magnus.conf`

2. 最初の行を削除します。

```
Init fn="ServletExecInit"  
ServExec_instance_name.instances="IP_address:port_number"  
  
ServExec_instance_name
```

ServletExec インスタンスの名前を指定します。

IP_address

ServletExec がインストールされたシステムの IP アドレスを指定します。

port_number

ServletExec インスタンスのポート番号を指定します。

注: ポリシー サーバ設定ウィザードによってファイルの最後に正しいエントリが追加されました。

3. 以下の設定ファイルを開きます：
`/sunjavasystem_home/servers/https-web_server_instance_name.domain.com/config/obj.conf`

4. 以下の手順を実行します。

a. ファイルの上から 4 番目と 5 番目行を削除します。

```
NameTrans fn="assign-name" from="/servlet/*"  
name="<ServExec_instance_name>"  
NameTrans fn="assign-name" from="*.jsp*"   
name="<ServExec_instance_name>"
```

重要: 2 番目と 3 番目行から以下のエントリを削除しないでください。ポリシー サーバ設定ウィザードによりこのエントリが追加されました。

```
name=se-ServExec_instance_name
```

b. ファイルの最後から 2 番目から最後のセクションを削除します。

```
<Object name="ServExec_instance_name"  
Service fn="ServletExecService" group="ServExec_instance_name"  
</Object>
```

重要: 以下のエントリを削除しないでください。ポリシー サーバ設定ウィザードによりこのエントリが追加されました。

```
<Object name="se-ServExec_instance_name">
```

5. 設定ファイルを保存し、Web サーバインスタンスを開始します。

/sitemindermonitor への Windows/IIS 仮想パスが存在しない

Windows で該当

問題の状況:

IIS Microsoft 管理コンソールの [既定の Web サイト] の下に、/sitemindermonitor への仮想パスが存在しません。

解決方法:

仮想パスを作成します。

仮想パスを作成する方法

1. [スタート] メニューから [プログラム] - [管理ツール] - [インターネット サービス マネージャ] を選択します。
2. [既定の Web サイト] を選択します。

3. [操作] メニューから [新規作成] - [仮想ディレクトリ] を選択します。
仮想ディレクトリ作成ウィザードが起動します。
4. 仮想ディレクトリの名前（エイリアス）を指定します。例：
`sitemindermonitor`
注: エイリアスには、たとえば、`sitemindermonitor` など、どのような名前も指定できます。
5. [次へ] をクリックします。
6. `<siteminder_installation>¥monitor¥` へのパスを指定します。
7. [次へ] をクリックします。
8. 以下の権限を選択します。
実行アクセス権の許可
9. [完了] をクリックします。

管理 UI のトラブルシューティング

以下のセクションでは、管理 UI の登録で発生する可能性がある一般的な問題と、その解決方法案について詳しく説明します。

管理 UI がハングアップする

症状:

管理 UI が登録されているポリシー サーバを再起動しました。管理 UI でタスクを開始しようとする、ハングアップします。

解決方法:

管理 UI を再起動します。

未処理の例外を持つ WebSphere クラッシュ

症状:

既存の WebSphere インフラストラクチャに 管理 UI をインストールしました。WebSphere がクラッシュし、`native_stderr` ログが、IBM Java Garbage Collector に未処理の例外をレポートします。

解決方法:

WebSphere 内の埋め込まれた Java SDK にパッチをあてます。

注: 詳細については、「[IBM の解決方法](#)」を参照してください。

ポリシー サーバ接続が登録できない

症状:

管理 UI が利用できないポリシー サーバに登録されるので、別のポリシー サーバ接続に登録しようとしています。スーパーユーザ権限を持つ管理者を使用して 管理 UI にログインするとき、「ポリシー サーバ接続の登録」タスクが表示されません。

解決方法:

外部管理者ストアへの接続が設定されたとき、単一ユーザはスーパーユーザ権限が委任されていました。このスーパーユーザアカウントを使用して 管理 UI にログインします。ポリシー サーバ接続が利用できなくなるとき、このスーパーユーザはポリシー サーバ接続に登録することができる唯一のユーザです。

API エラーが表示される

症状:

エージェント API の失敗メッセージが表示されて 管理 UI の登録が失敗します。

解決方法:

ポリシー サーバが起動されていません。ポリシー サーバ管理コンソールを使用して、ポリシー サーバを起動します。

「ファイルに登録がありません」エラーが表示される

症状:

ポリシー サーバへの 管理 UI の登録が、「ファイルに登録の記録がありません」というエラーメッセージと共に失敗します。

以下のときにこのメッセージが表示される場合があります。

- 管理 UI をインストールしており、ポリシー サーバに初めて 管理 UI を登録しようとしているとき
- 管理 UI を登録しており、追加のポリシー サーバ接続を登録しようとしているとき

解決方法:

以下のいずれかを実行します。

初めて 管理 UI を登録しようとしている場合

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_administrator[:passphrase] -adminui--setup  
siteminder_administrator
```

SiteMinder の管理者を指定します。以下の一部として 管理 UI をインストールする場合

- 新しい 12.52 SP1 環境の一部としてインストールする場合は、デフォルトの SiteMinder 管理者アカウント (siteminder) を指定します。
- アップグレードの一部としてインストールする場合は、ポリシー ストア内でのスーパーユーザ権限のある SiteMinder 管理者アカウントを指定します。

注: r12.0 SP1 からアップグレードして、スーパーユーザ アカウントを持たない場合は、デフォルトの SiteMinder 管理者 (siteminder) を作成するために smreg ユーティリティを使用します。smreg ユーティリティの使用に関する詳細については、「ポリシー サーバ管理ガイド」を参照してください。

passphrase

SiteMinder 管理者アカウントのパスワードを指定します。

制限：

- パスフレーズは 6 文字以上にする必要があります。
- パスフレーズには、アンパサンド (&) またはアスタリスク (*) を含めることができません。
- パスフレーズ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。

3. 登録を完了させるために、デフォルトの SiteMinder 管理者アカウントを使用して 管理 UI にログインします。

追加のポリシー サーバ接続を登録しようとしている場合

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 client_name[:passphrase] -adminui
```

client_name

登録する 管理 UI を識別します。

制限： この値は一意である必要があります。たとえば、管理 UI の登録にすでに *smui1* を使用している場合は、「*smui2*」と入力します。

passphrase

管理 UI の登録の完了に必要なパスワードを指定します。

制限：

- パスフレーズは 6 文字以上にする必要があります。
- パスフレーズには、アンパサンド (&) またはアスタリスク (*) を含めることができません。
- パスフレーズ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。

3. ポリシー サーバ接続を登録するために 管理 UI にログインします。

「無効な登録ファイルです」エラーが表示される

症状:

追加のポリシー サーバ接続を登録しようとしています。登録は、「無効な登録ファイルです」エラー メッセージと共に失敗します。

解決方法:

入力したパスフレーズが、**XPSRegClient** を使用して作成したパスフレーズと同一であることを確認します。作成した値は、管理 UI を使用して入力する値と一致する必要があります。

パスフレーズがない場合

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 client_name[:passphrase] -adminui
```

client_name

登録する 管理 UI を識別します。

制限: この値は一意である必要があります。たとえば、管理 UI の登録にすでに **smui1** を使用している場合は、「**smui2**」と入力します。

passphrase

管理 UI の登録の完了に必要なパスワードを指定します。

制限:

- パスフレーズは 6 文字以上にする必要があります。
- パスフレーズには、アンパサンド (&) またはアスタリスク (*) を含めることができません。
- パスフレーズ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。

3. ポリシー サーバ接続を登録するために 管理 UI にログインします。

タイムアウトすることなく登録が失敗する

症状:

管理 UI の登録がタイムアウトにならずに失敗します。

解決方法:

以下の手順を実行します。

- ポリシー サーバをホストしているマシンを ping して使用可能であることを確認します。
- `policy_server_home¥bin` にある、以下の登録ファイルを見つけます。

`name.XPSReg`

`policy_server_home`

ポリシー サーバインストールパスを指定します。

名前

管理 UI 登録ツール (XPSRegClient) を使用してクライアント名とパスフレーズを作成したときに指定したクライアント名を識別します。

登録ファイルが存在しない場合は、XPSRegClient を実行し、クライアント名とパスフレーズを作成します。

- ポリシー サーバログ ファイル (`smmps.log`) を開き、登録した時間の頃に発生した可能性があるエラーについてそれを確認します。

管理 UI 登録ログが見つからない

症状:

管理 UI 登録をトラブルシュートしようとしたましたが、ログ ファイルを見つけないことができません。

解決方法:

XPSRegClient は、ログ ファイルを *policy_server_home*¥log 内に作成および保存します。ファイル名は XPSRegClient.*date* です。

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。

date

XPSRegClient がファイルを作成した日付を示します。

例: XPSRegClient.2007-12-1.154002

注: 最後の 6 つの数字は、複数のファイルを同じ日に作成する場合、使用できる一意の識別子です。

検索がタイムアウトエラーで失敗する

症状:

ポリシー オブジェクトの検索を完了できません。管理 UI が、検索結果を返す代わりに接続タイムアウト エラーを表示します。

解決方法:

管理 UI を使用して、多くのポリシー オブジェクトで検索すると、以下の結果のどちらかまたは両方が発生します。

- 管理 UI とポリシー サーバの間の接続がタイムアウトする。
- ポリシー サーバ トンネル バッファが破損する。

後者は接続タイムアウト エラーをもたらします。この問題は、管理 UI ポリシー サーバ接続タイムアウトを調節し、ポリシー サーバ トンネル バッファ サイズに合ったレジストリ キーを作成することで解決します。

ポリシー サーバ接続タイムアウトを調整する方法

1. 管理 UI にログインします。
2. [管理] - [管理 UI] - [ポリシー サーバ接続] - [ポリシー サーバ接続の変更] - [検索] をクリックし、ポリシー サーバ接続オブジェクトを開きます。
3. 該当するポリシー サーバを選択し、[サブミット] をクリックします。
4. [詳細] セクションの [タイムアウト] フィールドを 2,000 秒などの大きな値に設定します。

これで、ポリシー サーバ接続タイムアウトの時間が長くなりました。

トンネル バッファ サイズに合ったレジストリ キーを作成する方法

1. 以下のポリシー サーバ レジストリ キーを作成します。

HKLM¥SOFTWARE¥Wow6432Node¥Netegrity¥SiteMinder¥CurrentVersion¥
PolicyServer¥

Max AdmComm Buffer Size

2. このレジストリ キーを 2,097,000 キロバイト (0x1FFF68) など大きな値に設定します。
3. 変更内容を保存して、レジストリを終了します。

注: 接続タイムアウトおよびバッファ サイズを変更しても問題が解決しない場合、管理 UI を再起動してください。

デフォルトのログ ファイルが見つからない場合

症状:

展開された 管理 UI インスタンスのトラブルシューティングを試みているが、デフォルトのアプリケーションサーバログ ファイルが見つかりません

解決方法:

スタンドアロン インストール オプションを使用した場合、デフォルトのログ ファイル名は `server.log` です。このログ ファイルは `administrative_ui_home¥CA¥SiteMinder¥adminui¥server¥default¥log.` にあります。

`administrative_ui_home`

管理 UI インストールパスを指定します。

注: JBoss、WebSphere または WebLogic の既存インスタンスに 管理 UI をインストールした場合は、デフォルト ログの詳細についてベンダー固有のドキュメントを参照してください。

デフォルトのログ ファイルは、十分な情報を提供しません。

症状:

展開された 管理 UI インスタンスのトラブルシューティングを試みているが、デフォルトのアプリケーション サーバ ログ ファイルは十分な情報を提供しません。

解決方法:

SiteMinder 固有のログの設定をするために、`SiteMinderLog4j` プロパティ ファイルを使用します。ファイルには、ログの設定に関するコメントが含まれます。ファイルの場所は、管理 UI をインストールするために使用されたインストール オプションに応じて決まります。

■ スタンドアロン インストール

スタンドアロン インストール オプションを使用した場合、プロパティ ファイルは

`administrative_ui_home¥CA¥SiteMinder¥adminui¥server¥default¥deploy¥iam_siteminder.ear¥user_console.war¥META-INF.` にあります。

`administrative_ui_home`

管理 UI インストール パスを指定します。

■ 既存のアプリケーション サーバ インフラストラクチャ

既存のアプリケーション サーバ インフラストラクチャに 管理 UI をインストールした場合、プロパティ ファイルは

`deploy¥iam_siteminder.ear¥user_console.war/META-INF` にあります。

`deploy`

アプリケーション サーバがアプリケーションを展開する場所を指定します。

注: 管理 UI を 12.52 SP1 にアップグレードした場合、プロパティ ファイル `deploy/IdentityMinder.ear/user_console.war/META-INF.` にあります。

レポート サーバのトラブルシューティング

以下のセクションでは、レポート サーバおよび解決方法案の使用で発生する可能性がある一般的な問題について詳しく説明します。

レポート サーバのインストールは、文字に関するエラーで失敗します。

症状:

インストールは、インストール パスで使用した文字に関連するエラーで失敗します。

解決方法:

レポート サーバのインストールは、インストール パス中で以下の文字タイプのみをサポートします。

- 英数字
- スペース
- ダッシュ
- アンダーライン

これらの文字タイプのみを含むように、インストール パスを変更します。

レポート サーバ インストーラにファイル不足エラーが表示される

Windows で該当

症状:

インストール中に、**vcredist.msi** ファイルがないというメッセージが表示されます。このメッセージでは、ファイルが存在するディレクトリにマップするよう要求されます。

解決方法:

以下の対処方法を試してください。

- Microsoft Visual C++ 2005 再頒布可能パッケージをアンインストールします。
- [キャンセル] をクリックしてインストールを続行します。

インストールが正常に完了します。Xcelsius アプリケーションに関して問題が発生した場合は、Microsoft の Web サイトから **vcredist.msi** をダウンロードしてインストールします。

アンインストールでアプリケーションを閉じるよう要求される

Windows 2008 R2 で有効

症状:

レポート サーバをアンインストールしているときに、インストーラによって、続行する前に以下のアプリケーションを閉じるよう要求されました。

- Java Platform SE binary
- BOE120MySQL

解決方法:

アプリケーションを閉じないオプションを選択し、[OK] をクリックします。

インストーラによって自動的にアプリケーションが閉じられると、プロセスは失敗します。

監査を基にしたレポートが結果を返さない

Oracle ベースの監査ストアに有効です。

症状:

監査を基にしたレポートが結果を返しません。

解決方法:

監査データベースを設定するときに使用されたユーザアカウントが DB ロールを持っているかどうかを判別します。ユーザアカウントに DB ロールがある場合は、それを削除します。DB ロールは、監査を基にしたレポートが正しい監査テーブルにクエリするのを妨げます。

ポリシー分析レポートが実行できない

Solaris で該当

症状:

ポリシー分析レポートを実行しようとする、以下の内容のメッセージでレポートが失敗します。

データベースからデータを取得できませんでした。

解決方法:

このエラーは以下のいずれかの問題に関連しています。

CRConfig.xml ファイルに Java クラスがありません。

1. `report_server_home/CommonReporting3/bobje/java` に移動します。

`report_server_home`

レポートサーバのインストールパスを指定します。

2. ファイルの `Classpath` セクションに以下のクラスが含まれていることを確認します。

- `smjavaagentapi.jar`
- `smanalyzer.jar`

3. `JavaBeans` セクションに以下のクラスが含まれていることを確認します。

`webadmin-report-ds.jar`

レポートサーバとポリシーサーバの間の接続が壊れています。

レポートサーバを再登録します。

レポートサーバが正しく起動しませんでした。

レポートサーバを再起動します。

詳細情報:

[レポートサーバを登録する方法](#) (P. 527)

管理 UI によるファイル不足エラーの表示

症状:

私はレポートサーバをインストールし設定しました。管理 UI が、レポートパラメータ定義ファイルが見つからないことを示すメッセージを表示します。

解決方法:

レポートテンプレートを再インストールします。

詳細情報:

[レポートテンプレートをインストールする方法](#) (P. 521)

第 14 章：無人インストール

無人インストール

SiteMinder コンポーネントをインストールした後、無人インストールを使用して、コンポーネントを再度インストールできます。無人インストールでは、ユーザによる操作なしにインストールを完了できます。無人インストールを使用して以下のコンポーネントをインストールすることができます。

- ポリシー サーバ
- 管理 UI
- レポート サーバ

無人インストールのガイドライン

各 SiteMinder コンポーネントは、そのプロパティ ファイルと関連付けられています。すべてのプロパティ ファイルに、以下のガイドラインが適用されます。無人インストールを開始する前に、以下を確認します。

- デフォルト プロパティ ファイルを変更する前に、バックアップします。
- パラメータ名、等号 (=) およびパラメータの値の間に、決して余分なスペースを追加しないでください。
- 変更後に、ファイルを保存します。
- 決して暗号化パスワードを手動で編集しないでください。これらのパスワードはセキュリティ上の理由で暗号化されており、プレーンテキストでは編集できません。プレーンテキストでパスワードを追加する場合には、暗号化パスワードのパラメータをコメントアウトして、プレーンテキストの参照をコメント解除します。

デフォルトプロパティファイル

デフォルトプロパティファイル内のパラメータを変更するために、テキストエディタを使用します。デフォルトパラメータは、最初のインストール中に入力された情報を反映します。

ポリシーサーバプロパティファイル

ポリシーサーバプロパティファイルのデフォルトの名前および場所は以下のとおりです。

名前

`ca-ps-installer.properties`

場所

`policy_server_home¥siteminder¥install_config_info`

`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。

管理UIプロパティファイル

管理UIのサイレントインストールには、プロパティファイルが1つだけ必要とされます。必要なファイルは、選択するインストールオプションによって異なります。利用可能なプロパティファイルのデフォルトの名前および場所は、以下のとおりです。

■ `smwamui-installer.properties`

既存のアプリケーションサーバインフラストラクチャにインストールする場合には、このファイルを使用します。

場所

`admin_ui_home¥siteminder¥adminui¥install_config_info`

`admin_ui_home`

管理UIインストールパスを指定します。

- prerequisite-installer.properties

スタンドアロンインストール オプションを使用してインストールする場合には、このファイルを使用します。

注: このファイルは、スタンドアロンインストール オプションを使用して 管理 UI があらかじめインストールされた場合のみ使用することができます。

場所

`admin_ui_home¥siteminder¥adminui¥install_config_info`

`admin_ui_home`

管理 UI インストールパスを指定します。

レポートプロパティファイル

SiteMinder レポートのサイレントインストールには、レポート サーバ用の応答ファイルおよび SiteMinder レポート サーバ設定ウィザード用の応答ファイルが必要です。これらのファイルの名前およびデフォルトの場所は以下のとおりです。

- cabiresponse.ini

このファイルを使用してレポート サーバをインストールします。

デフォルトの場所: `report_server_home¥CA¥SC¥CommonReporting3`

`report_server_home`

レポート サーバのインストールパスを指定します。

- reportserver_config_installer.properties

このファイルを使用して、SiteMinder レポート テンプレートをインストールします。

デフォルトの場所:

`report_server_home¥CommonReporting3¥install_config_info`

`report_server_home`

レポート サーバのインストールパスを指定します。

ポリシー サーバの無人インストールを実行する方法

ポリシー サーバの無人インストールを実行するには、以下の手順を完了します。

1. 無人インストールのガイドラインを確認します。
2. ポリシー サーバ プロパティ ファイルをポリシー サーバ ホスト システムからコピーします。
3. 以下のいずれかの操作を実行します。
 - ポリシー サーバを再インストールする場合は、ファイルを一時的な場所にコピーします。
 - ポリシー サーバを新しいシステムにインストールする場合は、ファイルをそのシステム上の一時的な場所にコピーします。

注: (UNIX) UNIX ユーザが、このディレクトリからインストールするための適切な権限を持っていることを確認してください。

4. ポリシー サーバのインストール メディアは、プロパティ ファイルと同じ場所にコピーします。
5. ポリシー サーバ インストーラのプロパティ ファイルを変更します。
6. ポリシー サーバのインストーラを実行します。
7. ポリシー サーバのインストールを確認します。

詳細情報:

[無人インストールのガイドライン \(P. 623\)](#)

ポリシー サーバ インストーラのプロパティファイルの変更

インストール変数を定義するために、ポリシー サーバ インストーラのプロパティ ファイルを変更します。このファイル内のデフォルトのパラメータ、パスワードおよびパスは、最初のポリシー サーバ インストール中に入力した情報を反映します。

重要: プロパティ テンプレートには、ポリシー サーバの **FIPS** モードの運用を指定する変数 **CA_SM_PS_FIPS140** が含まれています。ポリシー サーバを再インストールする場合は、この変数の値を変更しないでください。必要に応じて、ポリシー サーバを再インストールした後に、**FIPS** モードの運用を変更します。ポリシー サーバの **FIPS** モードの運用の変更の詳細については、「アップグレードガイド」を参照してください。

ポリシー サーバ全般情報

この全般情報セクションでは、以下を設定できます。

DEFAULT_INSTALL_DIR

ポリシー サーバ インストールの場所を指定します。

DEFAULT_SHORTCUTS_DIR

SiteMinder プログラム アイコンの場所を指定します。

例：C:\¥¥Documents and Settings¥¥All Users¥¥Start or /SiteMinder

注：アイコン機能は Windows 上でのみ有効です。

DEFAULT_JRE_ROOT

JRE のインストール場所を指定します。

DEFAULT_BROWSER

(UNIX のみ) ブラウザのインストール場所を指定します。

例：/usr/dt/appconfig/netscape/netscape

DEFAULT_SMPROFILE_CHOICE

(UNIX のみ) .profile ファイルに smprofile.ksh を追加するかどうかを指定します。「はい」の場合は **true** を、「いいえ」の場合は **false** を指定します。

DEFAULT_ENCRYPTKEY

クリア テキスト暗号化キーの入力を可能にします。このキーにより、ポリシー サーバとポリシー ストアの間で送信されるデータが保護されます。

注: ENCRYPTED_ENCRYPTKEY パラメータをコメントアウトし、DEFAULT_ENCRYPTKEY をコメント解除する場合、無人インストーラでは DEFAULT_ENCRYPTKEY からのクリア テキスト暗号化キー値が使用されます。DEFAULT_ENCRYPTKEY パラメータは、デフォルトでポリシー サーバの最初のインストールの後にコメントアウトされます。

ENCRYPTED_ENCRYPTKEY

暗号化された暗号化キーを表示します。このキーにより、ポリシー サーバとポリシー ストアの間で送信されるデータが保護されます。このキーは、ポリシー サーバの最初のインストール中に入力しており、変更できません。

重要: この暗号化された値は変更しないでください。変更すると、無人インストールを実行するときにポリシー サーバとポリシー ストアとの間の通信が損なわれます。

DEFAULT_ENCRYPTKEY パラメータをコメントアウトし、ENCRYPTED_ENCRYPTKEY をコメント解除する場合、無人インストーラでは ENCRYPTED_ENCRYPTKEY からの暗号化された暗号化キー値が使用されます。

CA_SM_PS_FIPS140

ポリシー サーバの FIPS モードの運用を指定します。

値: COMPAT、MIGRATE、または ONLY

重要: ポリシー サーバを再インストールする場合は、この値を変更しないでください。

ポリシー サーバ機能

[機能の選択] セクションでは、以下のパラメータを設定できます。

DEFAULT_OVMGUI_CHOICE

ポリシー サーバインストーラが、選択された Web サーバ上に OneView モニタ GUI を設定するかどうかを決定します。

有効値： true または false

true

インストーラは OneView モニタ GUI を設定します。

この値を true に設定すると、OneView モニタ GUI および Web サーバに追加の設定が必要になります。

false

インストーラは OneView モニタ GUI を設定しません。

DEFAULT_WEBSERVERS_CHOICE

ポリシー サーバインストーラが指定された Web サーバにフェデレーション セキュリティ サービスの UI を設定するかどうかを指定します。

有効値： true または false

true

インストーラは、指定された Web サーバでコンポーネントを設定します。

この値を true に設定すると、Web サーバに追加の設定が必要になります。

false

インストーラは、Web サーバでコンポーネントを設定しません。

DEFAULT_SNMP_CHOICE

ポリシー サーバ インストーラが、ポリシー サーバで SiteMinder SNMP サポートを設定するかどうかを決定します。

有効値： true または false

true

インストーラは SiteMinder SNMP サポートを設定します。

この値を true に設定すると、SNMP に追加の設定が必要になります。

false

インストーラは SiteMinder SNMP サポートを設定しません。

DEFAULT_POLICYSTORE_CHOICE

ポリシー サーバ インストーラが、ポリシー ストアを自動的に設定するかどうかを決定します。

有効値： true または false

true

インストーラはポリシー ストアを設定します。

この値を true に設定すると、ポリシー ストアに追加の設定が必要になります。

false

インストーラはポリシー ストアを設定しません。

OneView モニタの GUI

DEFAULT_OVMGUI_CHOICE パラメータを true に設定した場合、以下を設定します。

DEFAULT_JDK_ROOT

JDK のインストール場所を指定します。

DEFAULT_SERVLETEXEC_INSTANCE_NAME

(UNIX のみ) ServletExec インスタンスの名前を指定します。

例： se-testmachine-60psGUI

DEFAULT_SERVLETEXEC_ROOT

ServletExec のインストール場所を指定します。

例：C:\Program Files\New Atlanta\ServletExec ISAPI または
/export/NewAtlanta/ServletExecAS

DEFAULT_SERVLETEXEC_PORT

(UNIX のみ) ServletExec インスタンスのポート番号を指定します。

例：7676

SNMP

SNMP パスワードを変更する場合は、以下を設定します。

DEFAULT_ROOT_PW

UNIX システムの root ユーザ用のクリア テキスト SNMP パスワードの入力を可能にします。ENCRYPTED_ROOT_PW パラメータをコメントアウトし、DEFAULT_ROOT_PW をコメント解除する場合、無人インストーラでは DEFAULT_ROOT_PW からのクリア テキスト SNMP パスワードが使用されます。

デフォルト：DEFAULT_ROOT_PW パラメータは、ポリシー サーバの最初のインストールの後にコメントアウトされます。

ENCRYPTED_ROOT_PW

UNIX システムの root ユーザ用の暗号化された SNMP パスワードを表示します。このパスワードは、UNIX ポリシー サーバの最初のインストール中に入力してあり、変更できません。

重要：この暗号化されたパスワードは変更しないでください。変更するとポリシー サーバと SNMP エージェントとの間の通信が損なわれます。DEFAULT_ROOT_PW パラメータをコメントアウトし、ENCRYPTED_ROOT_PW をコメント解除する場合、無人インストーラでは ENCRYPTED_ROOT_PW からの暗号化されたパスワードが使用されます。

ポリシー ストア

DEFAULT_POLICYSTORE_CHOICE パラメータを **true** に設定した場合、以下のパラメータを設定します。

DEFAULT_POLICYSTORE_TYPE

ポリシー ストアとして機能するストアのタイプを指定します。

有効値： LDAP または RDB

LDAP

LDAP ポリシー ストアを指定します。

RDB

ODBC ポリシー ストアを指定します。

DEFAULT_POLICYSTORE_IP

(LDAP) LDAP ディレクトリ サーバホストシステムの IP アドレスまたは名前を指定します。

例： 172.16.0.0

DEFAULT_POLICYSTORE_PORT

(LDAP) LDAP ディレクトリ サーバがリスンするポートを指定します。

例： 1356.

DEFAULT_POLICYSTORE_ADMINDN

(LDAP) 以下の権限を持つ管理者の LDAP ユーザ名を指定します。

- スキーマの作成。
- ポリシー ストア ルート オブジェクト下の LDAP ツリーでのオブジェクトの作成、読み取り、変更、削除。

例： cn=Directory Manager

DEFAULT_POLICystore_ADMINPW

(LDAP) LDAP ディレクトリ サーバの管理者用にクリア テキスト パスワードを入力できます。

ENCRYPTED_POLICystore_ADMINPW パラメータをコメントアウトし、DEFAULT_POLICystore_ADMINPW をコメント解除した場合、無人インストーラでは DEFAULT_POLICystore_ADMINPW からのクリア テキストパスワードが使用されます。

デフォルト: DEFAULT_POLICystore_ADMINPW パラメータは、ポリシーサーバの最初のインストールの後にコメントアウトされます。

ENCRYPTED_POLICystore_ADMINPW

(LDAP) LDAP ディレクトリ サーバの管理者用の暗号化されたパスワードを表します。このパスワードは、ポリシー サーバインストールが最後にポリシー ストアを設定した時に入力されたものです。既存の暗号化された値を使用して、新規ポリシー ストア用の LDAP 管理者パスワードを提供することができます。このパスワードは変更できません。

重要: このパスワードは変更しないでください。パスワードは暗号化されます。DEFAULT_POLICystore_ADMINPW パラメータをコメントアウトし、ENCRYPTED_POLICystore_ADMINPW をコメント解除した場合、インストーラでは ENCRYPTED_POLICystore_ADMINPW からの暗号化されたパスワードが使用されます。

DEFAULT_POLICystore_ROOTDN

(LDAP) LDAP ディレクトリ サーバのルート DN を指定します。

Example: o=example.com

DEFAULT_POLICystore_USER_CHOICE

(LDAP) DEFAULT_POLICystore_ADMINDN パラメータは、スキーマを作成する権限を持つ LDAP 管理者ユーザ名を必要とします。デフォルトでは、ポリシー サーバはこのアカウントを使用してポリシー ストアを管理します。ポリシー ストアが設定された後、代替りの LDAP ユーザアカウントがポリシー ストアの SiteMinder データを管理することができます。代替りのアカウントは、オブジェクトの作成、読み取り、変更、削除の権限を持っている必要があります。

有効値： true または false

true

ポリシー ストアが設定された後、代替りの LDAP ユーザアカウントがポリシー ストアを管理することを指定します。

false

ポリシー ストアが設定された後、DEFAULT_POLICystore_ADMINDN パラメータによって指定される LDAP 管理者ユーザアカウントがポリシー ストアを管理することを指定します。

DEFAULT_POLICystore_USERDN

(LDAP) 代替りの LDAP ユーザアカウントの DN を指定します。

例：

uid=SMAdmin, ou=people, o=security.com

DEFAULT_POLICystore_USERPW

(LDAP) 代替りの LDAP ユーザのクリア テキスト パスワードを入力できます。ENCRYPTED_POLICystore_USERPW パラメータをコメントアウトし、DEFAULT_POLICystore_USERPW をコメント解除した場合、無人インストーラでは DEFAULT_POLICystore_USERPW からのクリア テキスト パスワードが使用されます。

デフォルト： DEFAULT_POLICystore_USERPW パラメータは、ポリシー サーバの最初のインストールの後にコメントアウトされます。

ENCRYPTED_POLICystore_USERPW

(LDAP) 代わりに LDAP ユーザの暗号化されたパスワードを表します。このパスワードは、ポリシー サーバインストーラが最後にポリシー ストアを設定した時に入力されたものです。既存の暗号化された値を使用して、新規ポリシー ストア用の代わりに管理者パスワードを設定することができます。このパスワードは変更できません。

重要: このパスワードは変更しないでください。パスワードは暗号化されます。

DEFAULT_POLICystore_USERPW をコメントアウトし、ENCRYPTED_POLICystore_USERPW をコメント解除した場合、インストーラでは ENCRYPTED_POLICystore_USERPW からの暗号化されたパスワードが使用されます。

DEFAULT_INIT_POLICystore_CHOICE

(LDAP/RDB) ポリシー サーバインストーラがポリシー ストアを初期化する必要があることを指定します。

有効値: true または false

true

インストーラはポリシー ストアを初期化します。

false

インストーラはポリシー ストアを初期化しません。

DEFAULT_SM_ADMINPW

(LDAP/RDB) SiteMinder スーパーユーザ アカウントのクリア テキストパスワードを入力します。

ENCRYPTED_SM_ADMINPW をコメントアウトし、DEFAULT_SM_ADMINPW をコメント解除した場合、インストーラでは DEFAULT_SM_ADMINPW からのクリア テキストパスワードが使用されます。

デフォルト: DEFAULT_SM_ADMINPW パラメータは、ポリシー サーバの最初のインストールの後にコメントアウトされます。

ENCRYPTED_SM_ADMINPW

(LDAP/RDB) SiteMinder スーパーユーザの暗号化されたパスワードを表します。このパスワードは、ポリシー サーバ インストーラが最後にポリシー ストアを設定した時に入力されたものです。既存の暗号化された値を使用して、新規ポリシー ストア用の SiteMinder スーパーユーザパスワードを設定することができます。このパスワードは変更できません。

重要: このパスワードは変更しないでください。パスワードは暗号化されます。

DEFAULT_SM_ADMINPW をコメントアウトし、ENCRYPTED_SM_ADMINPW をコメント解除した場合、インストーラでは ENCRYPTED_SM_ADMINPW からの暗号化されたパスワードが使用されます。

DEFAULT_RDB_DSN

(RDB) ポリシー サーバ インストーラが作成する DSN の名前を指定します。

DEFAULT_RDB_DBSERVER

(RDB) データベース ホスト システムの IP アドレスまたは名前を指定します。

DEFAULT_RDB_DBNAME

(RDB) 次の値のいずれかを指定します。

- (SQL Server) ポリシー ストアとして機能するデータベースの名前付きインスタンスまたはデータベース名。
- (PostgreSQL) ポリシー ストアとして機能する PostgreSQL の名前付きインスタンスまたはデータベース名。
- (Oracle) ポリシー ストアとして機能する Oracle のデータベースのサービス名。

DEFAULT_RDB_PORT

(RDB) データベースがリスニングするポートを指定します。

DEFAULT_RDB_USER_NAME

(RDB) 以下の権限を持つデータベース管理者アカウントの名前を指定します。

- スキーマの作成。
- オブジェクトの作成、読み取り、変更、削除。

DEFAULT_RDB_DBTYPE

ポリシー ストアとして機能するデータベースのタイプを指定します。

有効な値： DB_MSSQL、DB_ORACLE、および DB_POSTGRE。

DB_MSSQL

SQL Server ポリシー ストアを指定します。

DB_ORACLE

Oracle ポリシー ストアを指定します。

DB_POSTGRE

PostgreSQL ポリシー ストアを指定します。

DEFAULT_RDB_PASSWORD

(RDB) データベース管理者のクリア テキスト パスワードを入力できます。

デフォルト： このパラメータは、ポリシー サーバの最初のインストールの後にコメント アウトされます。

ENCRYPTED_RDB_PASSWORD をコメントアウトし、DEFAULT_RDB_PASSWORD をコメント解除した場合、インストーラでは DEFAULT_RDB_PASSWORD からのクリア テキスト パスワードが使用されます。

ENCRYPTED_RDB_PASSWORD

(RDB) インストーラが最後にポリシー ストアを設定した時に入力されたデータベース管理者パスワードの暗号化された値を表します。

デフォルト： このパラメータはコメント解除されます。このパラメータをコメントアウトせず、DEFAULT_RDB_PASSWORD がコメント解除されない限り、インストーラではこの値が使用されます。

DEFAULT_KEYSTORE_CONFIG

インストーラが SiteMinder キー ストアとポリシー ストアを連結する必要があるかどうかを指定します。

有効値 : true または false

true

インストーラはキー ストアとポリシー ストアを連結します。

false

インストーラはキー ストアを設定しません。ポリシー ストアを設定した後に、スタンドアロン キー ストアを設定します。

DEFAULT_SMKEYDB_IMPORT_CHOICE

デフォルトの CA 証明書が証明書データ ストアにインポートされる必要があるかどうかを指定します。

有効値 : true または false

true

デフォルトの CA 証明書をインポートします。

false

デフォルトの CA 証明書をインポートしません。

DeviceDNA™ による拡張セッション保証の設定

以下のアイテムが DeviceDNA™ による拡張セッション保証に適用されます。

MASTER_KEY=

Advanced Authentication Server (CA SiteMinder for Secure Proxy Server で実行される) 用のマスタ暗号化キーを指定します。マスタ暗号化キーをプレーンテキスト形式で格納します。

ENCRYPTED_MASTER_KEY=

Advanced Authentication Server (CA SiteMinder for Secure Proxy Server で実行される) 用のマスタ暗号化キーを指定します。マスタ暗号化キーを暗号化形式で格納します。

IS_SA_ENABLED=true

DeviceDNA™ による拡張セッション保証が有効かどうかを示します。このアイテムを編集しないでください。

ポリシー サーバ インストーラの実行

無人インストールを実行し、ユーザによる操作なしでポリシー サーバをインストールします。

インストールする前に

テクニカル サポート サイトで、インストール メディアを使用してポリシー サーバをインストールします。

注: インストール メディア名のリストについては、「ポリシー サーバリリース ノート」を参照してください。

Windows

ポリシー サーバの無人インストールを実行するには、ポリシー サーバインストール実行ファイルとプロパティ ファイルをコピーしたディレクトリから以下のコマンドを実行します。

```
installation_media -f ca-ps-installer.properties -i silent
```

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

installation_media

ポリシー サーバのインストール実行ファイルを指定します。

注: プロパティ ファイルがインストール メディアと同じディレクトリ内に存在しない場合は、その場所を指定します。引数にスペースが含まれている場合は、二重引用符を使用します。

-i silent

インストーラがサイレントで実行されるように指定します。

例:

```
installation_media -f "C:\Program  
Files\CA\siteminder\install_config_info\ca-ps-installer.properties  
" -i silent
```

インストールが始まります。ポリシー サーバをインストールするために、インストーラはプロパティ ファイル内の指定されたパラメータを使用します。

UNIX

以下の手順に従います。

1. シェルを開きます。
2. ポリシー サーバインストール実行ファイルおよびポリシー サーバインストール プロパティ ファイルをコピーしたディレクトリから以下のコマンドを実行します。

```
./installation_media -f ca-ps-installer.properties -i silent  
installation_media
```

ポリシー サーバのインストール実行ファイルを指定します。

-i silent

インストーラがサイレントで実行されるように指定します。

インストールが始まります。ポリシー サーバをインストールするために、インストーラはプロパティ ファイル内の指定されたパラメータを使用します。

ポリシー サーバ インストールのトラブルシューティング

ポリシー サーバインストールのトラブルシューティングには、以下のファイルを使用します。

■ CA_SiteMinder_Policy_Server_release_InstallLog.log

インストール ログは、インストール中に発生した成功、警告、致命的でないエラーおよびエラーの数をリスト表示するサマリ セクションを含みます。個別のインストール アクションは、それぞれのステータスと共にリスト表示されます。

release

ポリシー サーバのリリースを指定します。

場所 : *siteminder_home¥siteminder¥install_config_info*

■ ca-ps-details.log

ポリシー ストア ログは、ポリシー ストア ステータスを詳述します。

場所 : *siteminder_home¥siteminder¥install_config_info*

- **smpls.log**

smpls.log は、ポリシー サーバが開始されるときに作成されます。ポリシー サーバが正常にインストールされた場合、このログは以下の行を含みます。

[Info] ジャーナル スレッドが開始され、 60 分以上前のコマンドを削除します。

場所 : *siteminder_home*¥*siteminder*¥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。

ポリシー サーバの無人インストールの停止

ポリシー サーバの無人インストールを停止し、指定された Windows システムにポリシー サーバがインストールされないようにします。

インストールを停止する方法

- **Windows**

以下のプロセスを停止するために Windows のタスク マネージャを使用します。

ca-ps-12.5-win32.exe
ps_install.exe

- **UNIX**

Ctrl + C キーを押します。

管理 UI の無人インストールを実行する方法

管理 UI の無人インストールを実行するには、以下の手順を完了します。

1. 以下のいずれかを実行します。
 - 必須インストーラを使用している場合は、[インストールチェックリスト](#) (P. 466)を確認します。
 - 既存のアプリケーション サーバインフラストラクチャにインストールする場合は、[インストールチェックリスト](#) (P. 575)を確認します。
2. サイレントインストール用のガイドラインを確認します。
3. どのプロパティ ファイルを使用するか決定します。

注: 管理 UI インストール オプションが、使用されるプロパティ ファイルを決定します。

4. 管理 UI ホスト システムから、以下の手順を実行します。
 - a. プロパティ ファイルをコピーします。以下のいずれかを実行します。
 - 管理 UI を再インストールする場合には、このファイルを一時的な保存場所にコピーします。
 - 新しいシステムに 管理 UI をインストールする場合には、そのシステム上の一時的な保存場所にこのファイルをコピーします。
 - b. 必須インストーラを使用する場合には、`admin_ui_home¥SiteMinder¥adminui` に移動し、JBoss ライセンス使用条件 (JBoss-ORG-ULA.txt) を確認します。必須インストーラのプロパティ ファイルには、**Lesser General Public License** パラメータが含まれます。JBoss ライセンス使用条件に同意し、それを承諾することを確認するために、このパラメータを更新します。
5. プロパティ ファイルをコピーしたのと同じ場所に、インストール メディアをコピーします。

注: 管理 UI インストール オプションが、使用される実行ファイルを決定します。

6. プロパティ ファイルを変更します。
7. 管理 UI インストーラを実行します。
8. ポリシー サーバに 管理 UI を登録します。

必須インストーラのプロパティファイルの変更

管理 UI をインストールするためにスタンドアロン オプションを使用している場合は、インストール変数を定義するために必須インストーラのプロパティ ファイルを変更します。デフォルト値は、最後の 管理 UI インストール中に入力された情報を反映します。

一般情報

このセクションで、管理 UI インストールのルート フォルダを指定します。

DEFAULT_INSTALL_FOLDER

インストール中にすべてのサブフォルダが作成されるルート フォルダを指定します。

サーバ情報

このセクションで、JBoss および 管理 UI ホスト システムに関する情報を指定します。このセクションには、以下のパラメータがあります。

DEFAULT_APP_SERVER_PORT

JBoss が HTTP リクエストをリスンするポートを指定します。

DEFAULT_APP_SERVER_HOST

管理 UI ホスト システムの完全修飾名を指定します。

エンド ユーザ ライセンス使用条件

必須インストーラは JBoss をインストールします。これには、Lesser General Public License を承諾する必要があります。このセクションで、ライセンス使用条件の確認および同意を示します。

以下のようにして、ライセンスに同意します。

1. 必ず JBoss ライセンス使用条件 (JBossORG-EULA.txt) を確認してください。

ライセンスは以下の 管理 UI ホスト システムで入手することができます。

```
admin_ui_home¥siteminder¥adminui
```

```
admin_ui_home
```

管理 UI インストールパスを指定します。

2. ライセンス使用条件に同意する場合は、ACCEPT_LGPL_EULA の値を以下のように変更します。

はい

ライセンス使用条件を確認し同意することを示します。

管理 UI インストーラのプロパティファイルの変更

既存のアプリケーション サーバインフラストラクチャに 管理 UI をインストールする場合は、インストール変数を定義するために 管理 UI インストーラのプロパティ ファイルを変更します。このファイル内のデフォルト値は、最後の 管理 UI インストール中に入力された情報を反映します。

一般情報

このセクションで、管理 UI インストールのルート フォルダを指定します。

DEFAULT_INSTALL_FOLDER

インストール中にすべてのサブフォルダが作成されるルート フォルダを指定します。

アプリケーション サーバ情報

このセクションで、管理 UI が展開されるアプリケーション サーバの情報を指定します。このセクションには、以下のパラメータがあります。

DEFAULT_APP_SERVER

アプリケーション サーバタイプを指定します。このパラメータは以下の設定を使用します。

JBoss

アプリケーション サーバタイプを **JBoss** に指定します。

WebLogic9

アプリケーション サーバタイプを **WebLogic** に指定します。

WebSphere6

アプリケーション サーバタイプを **WebSphere** に指定します。

DEFAULT_NETE_JAVA_HOME

アプリケーション サーバに必要な **JDK** または **JRE** へのパスを指定します。この値は、アプリケーション サーバのタイプによって決まります。

JBoss

必要な **JDK** の最小バージョンへのパスを指定します。

WebLogic

必要な **JDK** または **JRE** の最小バージョンへのパスを指定します。

WebSphere

必要な **JDK** または **JRE** の最小バージョンへのパスを指定します。

DEFAULT_APP_SERVER_URL

アプリケーション サーバがインストールされるシステムの、完全修飾 **URL** を指定します。

JBoss 情報

このセクションで、JBoss に関する追加情報を指定します。

注: DEFAULT_APP_SERVER の値として JBoss を入力しなかった場合、このセクションに値は必要ありません。

このセクションには、以下のパラメータがあります。

DEFAULT_JBOSS_FOLDER

JBoss インストールディレクトリへのパスを指定します。

注: パスにスペースを含めることはできません。

WebLogic 情報

このセクションで、WebLogic に関する追加情報を指定します。

注: DEFAULT_APP_SERVER の値として WebLogic9 を入力しない場合、このセクションに値は必要ありません。

このセクションには、以下のパラメータがあります。

DEFAULT_BINARY_FOLDER

WebLogic インストールディレクトリへのパスを指定します。

DEFAULT_DOMAIN_FOLDER

管理 UI のために作成した WebLogic ドメインへのパスを指定します。

DEFAULT_SERVER_NAME

WebLogic ドメインを設定する WebLogic サーバの名前を指定します。

WebSphere 情報

このセクションで、WebSphere に関する追加情報を指定します。

注: DEFAULT_APP_SERVER の値として WebSphere6 を入力しない場合、このセクションに値は必要ありません。

このセクションには、以下のパラメータがあります。

DEFAULT_WEBSphere_FOLDER

WebSphere インストールディレクトリへのパスを指定します。

DEFAULT_WAS_NODE

アプリケーションサーバが存在するノードの名前を指定します。

DEFAULT_WAS_SERVER

アプリケーションサーバの名前を指定します。

DEFAULT_WAS_CELL

アプリケーションサーバが存在するセルの名前を指定します。

WAS_PROFILE

管理 UI に使用されているプロファイルの名前を指定します。

管理 UI インストーラの実行

無人インストールを実行し、ユーザによる操作なしで 管理 UI をインストールします。

インストールする前に

管理 UI をインストールする前に、以下の点を考慮します。

- テクニカルサポートサイトで、インストール メディアを使用して 管理 UI をインストールします。

注: インストール メディア名のリストについては、「ポリシー サーバリリース ノート」を参照してください。

- **重要:** インストール zip には、インストール メディアと同じレベルに `layout.properties` ファイルおよび `Framework` フォルダが含まれています。インストール zip を展開した後にインストール メディアを移動した場合、以下のものを同じ場所に移動しないと、インストールに失敗します。
 - `layout.properties` ファイル
 - `Framework` フォルダ
- インストール zip は、必須インストーラおよび管理 UI インストーラを含みます。

必須インストーラを使用して 管理 UI をインストールしている場合は、両方の実行ファイルを同じ場所に置いてください。必須インストーラは、インストールを完了させるために、自動的に 管理 UI インストーラを呼び出します。

Windows

管理 UI の無人インストールを実行するには、管理 UI インストール メディアおよびプロパティ ファイルをコピーしたディレクトリから以下のコマンドを実行します。

```
installation_media -f properties_file -i silent
```

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

installation_media

管理 UI のインストール実行ファイルの名前を指定します 管理 UI インストール オプションが、使用される実行ファイルを決定します。

-f properties_file

プロパティ ファイルへのパスを指定します。パスにはプロパティ ファイル名が含まれている必要があります。管理 UI インストール オプションが、使用されるプロパティ ファイルを決定します。

注: 引数がスペースを含んでいる場合は、二重引用符を使用します。

-i silent

インストーラがサイレントで実行されるように指定します。

例:

```
installation_media -f "C:\Program  
Files\CA\SiteMinder\adminui\install_config_info\properties_file" -i silent
```

管理 UI をインストールするために、インストーラはプロパティ ファイル内のパラメータを使用します。

ポリシー サーバに 管理 UI を登録してインストールを完了します。

- スタンドアロン オプションを使用して、管理 UI をインストールした場合には、「[管理 UI を登録する方法 \(P. 476\)](#)」を参照してください。
- 既存のアプリケーション サーバインフラストラクチャにインストールした場合には、「[管理 UI を登録する方法 \(P. 584\)](#)」を参照してください。

UNIX

以下の手順に従います。

1. シェルを開きます。
2. 管理 UI インストール メディアおよびプロパティ ファイルをコピーしたディレクトリから以下のコマンドを実行します。

```
./installation_media -f properties_file -i silent
```

installation_media

管理 UI のインストール実行ファイルの名前を指定します 管理 UI インストール オプションが、使用される実行ファイルを決定します。

-f properties_file

プロパティ ファイルへのパスを指定します。 パスにはプロパティ ファイル名が含まれている必要があります。 管理 UI インストール オプションが、使用されるプロパティ ファイルを決定します。

-i silent

インストーラがサイレントで実行されるように指定します。

管理 UI をインストールするために、インストーラはプロパティ ファイル内のパラメータを使用します。

3. 管理 UI をポリシー サーバに登録してインストールを完了します。
 - スタンドアロン オプションを使用して、管理 UI をインストールした場合には、「[管理 UI を登録する方法](#) (P. 476)」を参照してください。
 - 既存のアプリケーション サーバインフラストラクチャにインストールした場合には、「[管理 UI を登録する方法](#) (P. 584)」を参照してください。

レポート サーバの無人インストールを実行する方法

管理 UI の無人インストールを実行するには、以下の手順を完了します。

1. [インストールチェックリスト](#) (P. 496)を確認します。
2. インストーラに必要な情報を収集します。
3. サイレント インストール用のガイドラインを確認します。

4. レポート サーバの応答ファイルおよび **SiteMinder** レポート サーバ設定ウィザードのプロパティ ファイルにアクセスします。
5. 応答ファイルとプロパティ ファイルをレポート サーバ ホスト システム上の一時的な場所にコピーします。
6. レポート サーバおよび **SiteMinder** レポート サーバ設定ウィザードのインストール メディアを、レポート サーバ ホスト システム上の一時的な場所にコピーします。
注: インストール メディアは、テクニカル サポート サイトからダウンロードできます。
7. レポート サーバの応答ファイルを変更します。
8. **SiteMinder** レポート サーバ設定ウィザードのプロパティ ファイルを変更します。
9. レポート サーバのインストーラを実行します。
10. **SiteMinder** レポート サーバ設定ウィザードを実行します。
11. レポート サーバを登録します。

Windows 用レポート サーバ応答ファイルの変更

インストーラの応答ファイルを変更してインストール変数を定義します。デフォルトの値は、レポート サーバがインストールされ、応答ファイルが保存されたときの入力情報を反映します。

重要: ファイルを変更する前に、以下の点を考慮してください。

- 一部のパラメータは、レポート (CMS) データベースとして機能するデータベースのタイプを特定します。プロパティ ファイルを使用して、インストーラで設定されるデータベースのタイプを変更しないでください。レポート データベースのタイプを変更するには、インストーラを使用して別のプロパティ ファイルを作成します。
- コマンドラインでパラメータを渡すと、応答ファイルの対応する設定より優先されます。
- インストーラはいくつかのパラメータを自動で生成します。以下のパラメータは変更しません。
 - DATABASECONNECT
 - DATACONNECTION

- DATABASE_AUDIT_CONNSVR
- INSTALLDBTYPE
- INSTALL_DB_TYPE
- INSTALLLEVEL
- INSTALLSWITCH
- NEWCMSPASSWORD
- PRIVILEGED
- SINGLESERVER
- SKIP_DEPLOYMENT
- WCADOTNETINSTALL
- WCAJAVAINSTALL
- WCATOMCATINSTALL
- WDEPLOY_LANGUAGES
- WDEPLOY_LATER
- WEBSITE_METABASE_NUMBER
- WEBSITE_PORT
- ADDSOURCE
- ADVERTISE

Install

このセクションでは、応答ファイルの **Install** セクションのパラメータについて詳しく説明します。

AS_ADMIN_IS_SECURE

Web アプリケーション サーバにアクセスするには管理者認証情報を渡す必要があることを指定します。

SiteMinder 設定： この値を空にします。このパラメータは、SiteMinder がサポートしない **Web** アプリケーション サーバに適用されます。

AS_ADMIN_PASSWORD

Web アプリケーション サーバにアクセスする管理者アカウントのパスワードを指定します。埋め込みの Apache Tomcat バージョンがインストールされている場合、このパラメータの値は空です。SiteMinder は、埋め込みの Apache Tomcat バージョンのみをサポートします。

SiteMinder 設定： この値を空にします。

AS_ADMIN_PORT

Web アプリケーション サーバがリスンするポートを指定します。埋め込みの Apache Tomcat バージョンがインストールされている場合、この値はデフォルトで 8080 になります。SiteMinder は、埋め込みの Apache Tomcat バージョンのみをサポートします。

SiteMinder 設定： 8080

この値は、TOMCAT_CONNECTION_PORT の値と一致する必要があります。

AS_ADMIN_USERNAME

Web アプリケーション サーバにアクセスするために使用される管理者アカウントのアカウント名を指定します。埋め込みの Apache Tomcat バージョンがインストールされている場合、この値のデフォルトは以下のようになります。

admin

SiteMinder は、埋め込みの Apache Tomcat バージョンのみをサポートします。

SiteMinder 設定： admin

AS_DIR

埋め込みの Apache Tomcat バージョンがインストールされるパスを指定します。パスはインストールディレクトリを使用して自動的に設定されます。

注： パスに円記号が含まれる場合は、円記号を使用してエスケープしてください。

例： "C:¥¥Program Files¥¥CA¥¥SC¥¥CommonReporting3¥¥Tomcat55"

AS_INSTANCE

Web アプリケーション サーバ インスタンスの名前を指定します。埋め込みの Apache Tomcat バージョンがインストールされている場合、この値はデフォルトで **localhost** になります。SiteMinder は、埋め込みの Apache Tomcat バージョンのみをサポートします。

SiteMinder 設定： localhost

AS_SERVER

展開する Java Web アプリケーション サーバのタイプを指定します。埋め込みの Apache Tomcat バージョンがインストールされている場合、この値はデフォルトで **tomcat55** になります。SiteMinder は、埋め込みの Apache Tomcat バージョンのみをサポートします。

SiteMinder 設定： tomcat55

AS_SERVICE_NAME

Web アプリケーション サーバが **Windows** にサービスとしてインストールされる場合、サービスの名前を指定します。埋め込みの Apache Tomcat バージョンがインストールされている場合、この値のデフォルトは以下ようになります。

BOE120Tomcat

SiteMinder は、埋め込みの Apache Tomcat バージョンのみをサポートします。

SiteMinder 設定： BOE120Tomcat

AS_VIRTUAL_HOST

仮想化された環境にレポートサーバを展開している場合、アプリケーションがバインドされる仮想ホストを指定します。

SiteMinder 設定： この値を空にします。

AUDITINGALLOWED

Microsoft SQL Server または Oracle のレポート データベースを設定している場合、Content Management Server Auditing Database コンポーネントが設定可能であることを指定します。

0

監査が許可されることを示します。

1

監査が許可されないことを示します。

SiteMinder 設定 : 0

AUDITINGENABLED

Microsoft SQL Server または Oracle のレポート データベースを設定している場合、Content Management Server Auditing Database が有効であることを指定します。このパラメータは SiteMinder の監査ベースのレポートとは関係がありません。

Content Management Server Auditing Database は、レポート サーバに固有のアクティビティを監査するために使用され、SiteMinder には使用されません。SiteMinder 監査データベースは、監査ベースのレポートの実行に必要となります。

0

監査が有効であることを示します。

1

監査が有効でないことを示します。

SiteMinder 設定 : 1

CANODE

Service Intelligence Agent (SIA) ノードの名前を指定します。

注: スペースまたは英数字以外の文字は使用できません。

CADPORT

SIA が接続してリクエストを待機する必要があるポートを指定します。

デフォルト : 6410

CLIENTAUDITINGREPORT

Content Management Server Auditing Database コンポーネントが有効な場合、監査サービスがリスンする必要があるポートを指定します。このパラメータは SiteMinder の監査ベースのレポートとは関係がありません。Content Management Server Auditing Database は、レポートサーバに固有のアクティビティを監査するために使用され、SiteMinder には使用されません。

SiteMinder 監査データベースは、監査ベースのレポートの実行に必要となります。

SiteMinder 設定： デフォルト値（6420）のままにします。

CLIENTLANGUAGE

インストールする言語パックを指定します。

SiteMinder 設定： EN

CLUSTERCMS

既存の Content Management Server にサーバを追加しているかどうかを指定します。この値を変更する必要がある場合は、インストーラを使用して別の応答ファイルを作成することを推奨します。

SiteMinder 設定： False

CMSPASSWORD

既存の SAP BusinessObjects Enterprise 管理者アカウントのパスワードを指定します。このパラメータは、カスタムまたは Web 層のインストーラにのみ適用されます。

SiteMinder 設定： この値を空にします。

DATABASEAUDITDRIVER

Content Management Server Auditing Database に対してどのドライバを使用するかを指定します。このパラメータは SiteMinder の監査ベースのレポートとは関係がありません。Content Management Server Auditing Database は、レポートサーバに固有のアクティビティを監査するために使用され、SiteMinder には使用されません。

SiteMinder 監査データベースは、監査ベースのレポートの実行に必要となります。

SiteMinder 設定：

- 埋め込みの MySQL バージョンをインストールしている場合、デフォルト値（MySQLDatabaseSubSystem）のままにします。
- Microsoft SQL Server または Oracle のレポート データベースを設定している場合は、値を空にします。

DATABASEAUTHENTICATION

Microsoft SQL Server または Oracle のレポート データベースを設定している場合、このパラメータは自動的に生成されます。

SiteMinder 設定： この値を空にします。

DATABASEAUTHENTICATION_AUDIT

Microsoft SQL Server または Oracle のレポート データベースを設定している場合、このパラメータは自動的に生成されます。

SiteMinder 設定： この値を空にします。

DATABASECONNECT

このパラメータは変更しないでください。このパラメータは自動的に生成されます。

SiteMinder 設定： この値を空にします。

DATABASECONNECT_AUDIT

Microsoft SQL Server または Oracle のレポート データベースを設定している場合、このパラメータは自動的に生成されます。

SiteMinder 設定： この値を空にします。

DATABASEDB

レポート データベースの名前を指定します。

SiteMinder 設定：

- 埋め込みの MySQL バージョンをインストールしている場合、デフォルト値（BOE120）のままにします。
- Microsoft SQL Server レポート データベースを設定している場合は、デフォルト値（RSDB）のままにします。
- Oracle レポート データベースを設定している場合は、値を空にします。

DATABASEDB_AUDIT

Content Management Server の監査データベースの名前を指定します。このパラメータは SiteMinder の監査ベースのレポートとは関係ありません。Content Management Server Auditing Database は、レポートサーバに固有のアクティビティを監査するために使用され、SiteMinder には使用されません。

SiteMinder 監査データベースは、監査ベースのレポートの実行に必要となります。

SiteMinder 設定：

- 埋め込みの MySQL バージョンをインストールしている場合、デフォルト値 (BOE120_AUDIT) のままにします。
- Microsoft SQL Server または Oracle のレポート データベースを設定している場合は、値を空にします。

DATABASEDRIVER

レポート データベースに使用するドライバを指定します。

SiteMinder 設定： デフォルト値のままにします。この値を変更する必要がある場合は、インストーラを使用して別の応答ファイルを作成してください。

DATABASEDSN

レポート データベース用の ODBC 接続の名前を指定します。

SiteMinder 設定：

- 埋め込みの MySQL バージョンをインストールしている場合、デフォルト値 (Business Objects CMS) のままにします。
- Microsoft SQL Server の既存のインスタンスを使用している場合は、DSN を入力します。
- Oracle の既存のインスタンスを使用している場合は、値を空にしておきます。

DATABASEDSN_AUDIT

Content Management Server Auditing Database の ODBC 接続の名前を指定します。このパラメータは SiteMinder の監査ベースのレポートとは関係ありません。Content Management Server Auditing Database は、レポートサーバに固有のアクティビティを監査するために使用され、SiteMinder には使用されません。

SiteMinder 監査データベースは、監査ベースのレポートの実行に必要となります。

SiteMinder 設定： デフォルト値（Business Objects Audit Server）のままにします。

DATABASENWLAYER_AUDIT

Content Management Server Audit Database のタイプを指定します。このパラメータは SiteMinder の監査ベースのレポートとは関係ありません。Content Management Server Auditing Database は、レポートサーバに固有のアクティビティを監査するために使用され、SiteMinder には使用されません。

SiteMinder 監査データベースは、監査ベースのレポートの実行に必要となります。

SiteMinder 設定： デフォルト値（ODBC）のままにします。

DATABASEPORT

レポート データベースがリスンするポートを指定します。

SiteMinder 設定：

- 埋め込みの MySQL バージョンをインストールしている場合は、ポートを入力します。

デフォルト：3306

- Microsoft SQL Server または Oracle のレポート データベースを設定している場合は、値を空にします。

DATABASEPORT_AUDIT

Content Management Server Audit Database がリスンするポートを指定します。このパラメータは SiteMinder の監査ベースのレポートとは関係ありません。Content Management Server Auditing Database は、レポートサーバに固有のアクティビティを監査するために使用され、SiteMinder には使用されません。

SiteMinder 監査データベースは、監査ベースのレポートの実行に必要となります。

SiteMinder 設定： このパラメータの値は必要ありません。

- 埋め込みの MySQL バージョンをインストールしている場合は、ポートを入力します。

デフォルト： 3306

- Microsoft SQL Server または Oracle のレポート データベースを設定している場合は、このパラメータを空にします。SiteMinder では、Content Management Server の監査は必要とされません。

DATABASEPWD

レポート データベースにアクセスできる管理者アカウントのパスワードを指定します。

DATABASEPWD_AUDIT

Content Management Server Auditing Database にアクセスできる管理者アカウントのパスワードを指定します。このパラメータは SiteMinder の監査ベースのレポートとは関係がありません。Content Management Server Auditing Database は、レポート サーバに固有のアクティビティを監査するために使用され、SiteMinder には使用されません。

SiteMinder 監査データベースは、監査ベースのレポートの実行に必要となります。

SiteMinder 設定：

- 埋め込みの MySQL バージョンをインストールしている場合、この値を DATABASEPWD パラメータと一致させます。
- Microsoft SQL Server または Oracle のレポート データベースを設定している場合は、このパラメータを空にします。

DATABASEPWD_MYSQLROOT

埋め込みの MySQL バージョンをインストールしている場合、レポート データベースにアクセスできる MySQL root ユーザ アカウントのパスワードを指定します。

DATABASERDMS_AUDIT

Content Management Server Auditing Database のタイプを指定します。このパラメータは SiteMinder の監査ベースのレポートとは関係ありません。Content Management Server Auditing Database は、レポートサーバに固有のアクティビティを監査するために使用され、SiteMinder には使用されません。

SiteMinder 監査データベースは、監査ベースのレポートの実行に必要となります。

SiteMinder 設定： このパラメータのデフォルト値を使用します。

DATABASESERVER

Oracle レポート データベースを設定している場合、Oracle データベース サービスの名前を指定します。

注： このパラメータは、Microsoft SQL Server レポート データベースを設定する応答ファイルに含まれます。このフィールドは空にします。

DATABASESERVER_AUDIT

Content Management Server Auditing Database サーバ ホスト システムの名前を指定します。このパラメータは SiteMinder の監査ベースのレポートとは関係ありません。Content Management Server Auditing Database は、レポートサーバに固有のアクティビティを監査するために使用され、SiteMinder には使用されません。

SiteMinder 監査データベースは、監査ベースのレポートの実行に必要となります。

SiteMinder 設定：

- 埋め込みの MySQL バージョンをインストールしている場合、デフォルト値 (localhost) のままにします。
- Microsoft SQL Server または Oracle のレポート データベースを設定している場合は、このパラメータを空にします。

DATABASEDRIVER

レポート データベースに使用するドライバを指定します。

SiteMinder 設定： デフォルト値のままにします。この値を変更する必要がある場合は、インストーラを使用して別の応答ファイルを作成してください。

DATABASEUID

レポート データベースにアクセスできる管理者アカウント名を指定します。

SiteMinder 設定 :

- 埋め込みの MySQL バージョンをインストールしている場合、アカウント名を入力します。インストーラは、必要な権限で管理者アカウントを作成します。
- Microsoft SQL Server を設定している場合は、データベース所有者 (DBO) 権限を持つアカウント名を入力します。
- Oracle を設定している場合、次の権限が有効なアカウント名を入力します : create session、create table、create procedure。

また、CONNECT と RESOURCE のロールを有効にしたアカウント名を入力することもできます。両方のロールに対して Admin Option 設定は必ず無効にしてください。

DATABASE_UID_AUDIT

Content Management Server Auditing Database にアクセスできる管理者アカウント名を指定します。このパラメータは SiteMinder の監査ベースのレポートとは関係がありません。Content Management Server Auditing Database は、レポート サーバに固有のアクティビティを監査するために使用され、SiteMinder には使用されません。SiteMinder 監査データベースは、監査ベースのレポートの実行に必要となります。

SiteMinder 設定 :

- 埋め込みの MySQL バージョンをインストールしている場合、この値を DATABASEUID パラメータと一致させます。
- Microsoft SQL Server または Oracle のレポート データベースを設定している場合は、値を空にします。

DATABASEUSER

Microsoft SQL Server または Oracle のレポート データベースを設定している場合、このパラメータは自動的に生成され、DATABASEUID 値に一致します。

SiteMinder 設定 : この値は DATABASEUID 値と一致する必要があります。

DATABASEUSER_AUDIT

Microsoft SQL Server または Oracle のレポート データベースを設定している場合、このパラメータは自動的に生成され、空になります。

SiteMinder 設定： この値を空にします。

DATABASE_AUDIT_CONNSVR

このパラメータは変更しないでください。このパラメータは自動的に生成されます。

SiteMinder 設定： connsvr

ENABLELOGFILE

インストーラがインストール ログ ファイルを作成するかどうかを指定します。

0

ログ ファイルを作成しません。

1

ログ ファイルを作成します。

ENABLESERVERS

インストールが完了した時点でサーバを有効にする必要があるかどうかを指定します。

0

サーバを有効にしません。

1

サーバを有効にします。

SiteMinder 設定： 1

EXPANDCMS

Microsoft SQL Server または Oracle のレポート データベースを設定している場合、このパラメータは自動的に生成されます。このパラメータは変更しないでください。

SiteMinder 設定： 1

INSTALL.LP.EN.SELECTED

英語の言語パックをインストールすることを指定します。

SiteMinder 設定： 1

INSTALLDBTYPE

このパラメータは変更しないでください。このパラメータは自動的に生成されます。

INSTALLDIR

レポートサーバがインストールされるディレクトリを指定します。

注: パスに円記号が含まれる場合は、円記号を使用してエスケープしてください。

例: C:\Program Files\CA\SC\CommonReporting3\

INSTALLLEVEL

このパラメータは変更しないでください。このパラメータは自動的に生成されます。

INSTALLMODE

インストール方法を指定します。

新規

すべての必要なサーバとクライアント コンポーネントをインストールします。

カスタム

特定のサーバおよびクライアント コンポーネントを選択してインストールします。

Web 層

必要な Web アプリケーション サーバ コンポーネントのみをインストールします。

SiteMinder 設定: New

INSTALL_DB_TYPE

このパラメータは変更しないでください。このパラメータは自動的に生成されます。

MYSQLPORT

埋め込みの MySQL バージョンを使用している場合、MySQL が接続してリクエストをリスンするポートを指定します。

デフォルト : 3306

注: このパラメータは、Microsoft SQL Server をレポート データベースとして設定するプロパティ ファイルに含まれます。デフォルト値を使用します。

MYSQLSERVER

Microsoft SQL Server または Oracle のレポート データベースを設定している場合、このパラメータは自動的に生成されます。このパラメータは変更しないでください。

SiteMinder 設定 : この値を空にします。

MYSQLSERVER_AUDIT

Microsoft SQL Server または Oracle のレポート データベースを設定している場合、このパラメータは自動的に生成されます。このパラメータは変更しないでください。

SiteMinder 設定 : この値を空にします。

NEWCMSPASSWORD

デフォルトの SAP BusinessObjects Enterprise 管理者アカウントのパスワードを指定します。このパラメータは自動的に生成されます。

SiteMinder 設定 : このパラメータは変更しません。この値を変更する必要がある場合は、インストーラを使用して別の応答ファイルを作成してください。

MYSQL_REMOTE_ACCESS

埋め込みの MySQL バージョンをレポート データベースとして使用している場合、リモート アクセスを有効にするかどうかを指定します。

SiteMinder 設定 : この値を空にします。

注: このパラメータは、Microsoft SQL Server をレポート データベースとして設定するプロパティ ファイルに含まれます。この値は空にします。

NAMESERVER

レポート サーバ ホスト システムの名前を指定します。

NEWCMSPASSWORD

デフォルトの SAP BusinessObjects Enterprise 管理者アカウントのパスワードを指定します。

SiteMinder 設定： このパラメータは変更しません。このパラメータは自動的に生成されます。この値を変更する必要がある場合は、インストーラを使用して別の応答ファイルを作成してください。

NSPORT

Content Management Server がリスンするポートを指定します。

デフォルト： 6400

REINITIALIZE_CMS_DB

Microsoft SQL Server または Oracle のレポート データベースを設定している場合、データベースが再初期化されることを指定します。

SiteMinder 設定： 1

SINGLESERVER

このパラメータは変更しないでください。このパラメータは自動的に生成されます。このパラメータは変更しないでください。

SiteMinder 設定： この値を空にします。

SKIP_DEPLOYMENT

このパラメータは変更しないでください。このパラメータは自動的に生成されます。このパラメータは変更しないでください。

SiteMinder 設定： この値を空にします。

SelectODBCDSN

Microsoft SQL Server または Oracle のレポート データベースを設定している場合、このパラメータは自動的に生成されます。このパラメータは変更しないでください。

SiteMinder 設定： この値を空にします。

TOMCAT_CONNECTION_PORT

埋め込みの Apache Tomcat バージョンが接続してリクエストを待機するポートを指定します。

デフォルト： 8080

TOMCAT_REDIRECT_PORT

埋め込みの Apache Tomcat バージョンがリクエストをリダイレクトするポートを指定します。

デフォルト : 8443

TOMCAT_SHUTDOWN_PORT

埋め込みの Apache Tomcat バージョンの SHUTDOWN コマンドが発行される必要があるポートを指定します。

デフォルト : 8005

WCADOTNETINSTALL

このパラメータは変更しないでください。このパラメータは自動的に生成されます。

SiteMinder 設定 : False

WCAEXISTINGINSTALL

このパラメータは変更しないでください。このパラメータは自動的に生成されます。

SiteMinder 設定 : False

WCAJAVAINSTALL

このパラメータは変更しないでください。このパラメータは自動的に生成されます。

SiteMinder 設定 : False

WCATOMCATINSTALL

このパラメータは変更しないでください。このパラメータは自動的に生成されます。

SiteMinder 設定 : True

WDEPLOY_LANGUAGES

このパラメータは変更しないでください。このパラメータは自動的に生成されます。

SiteMinder 設定 : jp

WDEPLOY_LATER

このパラメータは変更しないでください。このパラメータは自動的に生成されます。

SiteMinder 設定 : この値は空白にします。

WEBSITE_METABASE_NUMBER

このパラメータは変更しないでください。このパラメータは自動的に生成されます。

SiteMinder 設定： 1

WEBSITE_NAME

IIS Web アプリケーション サーバを展開している場合、SAP BusinessObjects Enterprise アプリケーションが展開される IIS Web サイトの名前を指定します。

SiteMinder は、埋め込みの Apache Tomcat バージョンのみをサポートします。

SiteMinder 設定： デフォルトの Web サイト

WEBSITE_PORT

このパラメータは変更しないでください。このパラメータは自動的に生成されます。

SiteMinder 設定： 80

機能

このセクションでは、応答ファイルの **Features** セクションのパラメータについて詳しく説明します。

REMOVE

インストールしないクライアント、サーバ、Web 層、および他の SAP BusinessObjects Enterprise コンポーネントを指定します。

SiteMinder 設定： このパラメータの値は変更しません。この値を変更するには、インストーラを使用して別の応答ファイルを作成します。

ADDLOCAL

インストールするクライアント、サーバ、Web 層、および他の SAP BusinessObjects Enterprise コンポーネントを指定します。

SiteMinder 設定： このパラメータの値は変更しません。この値を変更するには、インストーラを使用して別の応答ファイルを作成します。

ADDSOURCE

このパラメータは変更しないでください。このパラメータは自動的に生成されます。

SiteMinder 設定： この値を空にします。

ADVERTISE

このパラメータは変更しないでください。このパラメータは自動的に生成されます。

SiteMinder 設定： この値を空にします。

BIEK

このセクションでは、応答ファイルの **BIEK** セクションのパラメータについて詳しく説明します。

BIEK_INSTALL_SAMPLES

インストーラが **CA** テンプレートをインストールする必要があるかどうかを指定します。このパラメータは、**SiteMinder** レポート テンプレートとは関係がありません。**SiteMinder** レポート サーバ設定ウィザードが、必要なレポート テンプレートをインストールします。このウィザードは、レポート サーバをインストールした後に実行します。

0

サンプルテンプレートをインストールしません。

1

サンプルテンプレートをインストールします。

SiteMinder 設定： 0

SUPPRESS_REBOOT

インストールが正常に完了した後に、コンピュータを再起動するかどうかを指定します。

0

インストールが正常に完了した後に、システムを再起動します。

1

インストールが正常に完了した後に、システムが再起動されないようにします。インストールを完了するためには手動でシステムを再起動します。

SiteMinder 設定： 1

UNIX 用レポート サーバ応答ファイルの変更

インストーラの応答ファイルを変更してインストール変数を定義します。デフォルトの値は、レポート サーバがインストールされ、応答ファイルが保存されたときに入力した情報を反映します。

重要: ファイルを変更する前に、以下の点を考慮してください。

- 一部のパラメータは、レポート データベースとして機能するデータベースのタイプを特定します。プロパティ ファイルを使用して、インストーラで設定されるデータベースのタイプを変更しないでください。レポート データベースのタイプを変更するには、インストーラを使用して別のプロパティ ファイルを作成します。
- コマンドラインでパラメータを渡すと、応答ファイルの対応する設定より優先されます。

レポート サーバインストーラは、いくつかのパラメータを自動的に生成します。以下のパラメータは変更しません。

- PRODUCTID_NAME
- BOBJVERSION
- DATACONNECTION
- PRODUCTID_VER
- FUNCTION
- LANGUAGES_TO_INSTALL
- EXPANDSERVERS

Manual Settings

このセクションでは、応答ファイルの **Manual Settings** セクションのパラメータについて詳しく説明します。

MACHINENAME

レポート サーバホストの名前を指定します。この値はローカルサーバ名より優先されます。値を提供しない場合、値はデフォルトでローカル ホスト システム名になります。

Paths

このセクションでは、応答ファイルの **Paths** セクションのパラメータについて詳しく説明します。

BOBJEDIR

bobje ディレクトリのパスを指定します。**bobje** ディレクトリは、共通のレポート ディレクトリ内に自動的に作成されます。

例： /opt/CA/SharedComponents/CommonReporting3/bobje/

CDDIR

レポート サーバインストール キットの **Disk1** ディレクトリへのパスを指定します。

LICENSEDIR

製品のライセンスが含まれているディレクトリへのパスを指定します。

注： レポート サーバのインストールでは、製品ライセンスを提供する必要はありません。

SiteMinder 設定： この値を空にします。

Product Information

このセクションでは、応答ファイルの **Product Information** セクションのパラメータについて詳しく説明します。

BOBJELANG

インストールで使用する言語設定を指定します。

SiteMinder 設定： jp

PRODUCTID_NAME

インストールされている製品の名前を指定します。

SiteMinder 設定： BusinessObjects

BOBJEVERSION

SAP BusinessObjects Enterprise のバージョンを指定します。

SiteMinder 設定： 12.0

PRODUCTID_VER

インストールされている製品のバージョンを指定します。

SiteMinder 設定： 12.3

BOBJELICENSEKEY

製品をインストールするのに必要なライセンス キーを指定します。この値は、暗号化されて表示されます。

SiteMinder 設定： この値は変更しません。

PIDKEY

製品 ID キーを指定します。この値は、暗号化されて表示されます。

SiteMinder 設定： この値は変更しません。

Installation Information

このセクションでは、応答ファイルの **Installation Information** セクションのパラメータについて詳しく説明します。

FUNCTION

このパラメータは変更しないでください。このパラメータは自動的に生成されます。

SiteMinder 設定： install

INSTALLTYPE

インストール方法を指定します。

new

すべての必要なサーバとクライアント コンポーネントをインストールします。

custom

特定のサーバおよびクライアント コンポーネントを選択してインストールします。

webtier

必要な **Web** アプリケーション サーバ コンポーネントのみをインストールします。

SiteMinder 設定： new

INSTALLMODE

レポート サーバ インストール オペレーティング モードのカンマ区切りリストを指定します。このパラメータは以下のオプションをサポートします。

- install
- modify
- remove
- interactive

SiteMinder 設定： install

LOCALNAMESERVER

レポート サーバ ホスト システムの名前を指定します。

BOBJEINSTALLLOCAL

ユーザまたはシステムのインストールのどちらを実行するかを指定します。

SiteMinder 設定： user

LANGPACKS_TO_INSTALL

インストールする言語パックを指定します。**SiteMinder** は英語の言語パックのみをサポートします。デフォルトで、英語の言語パックがインストールされます。

SiteMinder 設定： この値を空にします。

LANGUAGES_TO_INSTALL

SAP BusinessObjects Enterprise に含まれる言語をすべて指定します。これらの値は、インストールする言語パックではなく、使用可能な言語を表します。

SiteMinder 設定： 値のカンマ区切りリスト

BOBJEUSERNAME

root 以外のユーザ アカウントの名前を指定します。

SiteMinder 設定： この値は、応答ファイルの **BIEK** セクション内の **BIEK_INSTALL_USER** の値と一致する必要があります。

EXPANDSERVERS

このパラメータは変更しないでください。このパラメータは自動的に生成されます。

SiteMinder 設定： この値を空にします。

Tomcat

このセクションでは、応答ファイルの **Tomcat** セクションのパラメータについて詳しく説明します。

INSTALLTOMCAT

埋め込みの **Apache Tomcat** バージョンをインストールする必要があるかどうかを指定します。

SiteMinder 設定： yes

注： インストーラでは **Web** アプリケーション サーバの既存のインスタンスを設定できますが、**SiteMinder** では埋め込みの **Apache Tomcat** バージョンのみがサポートされます。

CONNECTORPORT

埋め込みの **Apache Tomcat** バージョンが接続してリクエストを待機するポートを指定します。

デフォルト： 8080

REDIRECTPORT

埋め込みの **Apache Tomcat** バージョンがリクエストをリダイレクトするポートを指定します。

デフォルト： 8443

SHUTDOWNPORT

埋め込みの **Apache Tomcat** バージョンの **SHUTDOWN** コマンドが発行される必要があるポートを指定します。

デフォルト： 8005

Application Server

このセクションでは、応答ファイルの **Application Server** セクションのパラメータについて詳しく説明します。

AS_DIR

埋め込みの **Apache Tomcat** バージョンがインストールされるパスを指定します。パスはインストールディレクトリを使用して自動的に設定されます。

例： /opt/CA/SharedComponents/CommonReporting3//bobje/tomcat/

AS_SERVER

展開する **Java Web** アプリケーション サーバのタイプを指定します。埋め込みの **Apache Tomcat** バージョンがインストールされている場合、この値はデフォルトで **tomcat55** になります。 **SiteMinder** は、埋め込みの **Apache Tomcat** バージョンのみをサポートします。

SiteMinder 設定： tomcat55

AS_INSTANCE

Web アプリケーション サーバインスタンスの名前を指定します。埋め込みの **Apache Tomcat** バージョンがインストールされている場合、この値はデフォルトで **localhost** になります。 **SiteMinder** は、埋め込みの **Apache Tomcat** バージョンのみをサポートします。

SiteMinder 設定： localhost

AS_VIRTUAL_HOST

仮想化された環境にレポート サーバを展開している場合、アプリケーションがバインドされる仮想ホストを指定します。

SiteMinder 設定： この値を空にします。

AS_ADMIN_PORT

Web アプリケーション サーバがリスンするポートを指定します。埋め込みの **Apache Tomcat** バージョンがインストールされている場合、値は空です。 **SiteMinder** は、埋め込みの **Apache Tomcat** バージョンのみをサポートします。

SiteMinder 設定： この値を空にします。

AS_ADMIN_USERNAME

Web アプリケーション サーバにアクセスするために使用される管理者アカウントのアカウント名を指定します。埋め込みの **Apache Tomcat** バージョンがインストールされている場合、値は空です。**SiteMinder** は、埋め込みの **Apache Tomcat** バージョンのみをサポートします。

SiteMinder 設定： この値を空にします。

AS_ADMIN_PASSWORD

Web アプリケーション サーバにアクセスできる管理者アカウントのパスワードを指定します。埋め込みの **Apache Tomcat** バージョンがインストールされている場合、値は空です。**SiteMinder** は、埋め込みの **Apache Tomcat** バージョンのみをサポートします。

SiteMinder 設定： この値を空にします。

AS_ADMIN_SECURE

Web アプリケーション サーバにアクセスするには管理者認証情報を渡す必要があることを指定します。このパラメータは、**SiteMinder** がサポートしない Web アプリケーション サーバに適用されます。

SiteMinder 設定： false

AS_APPSERVER_ID

アプリケーション サーバの名前を指定します。このパラメータは、**SiteMinder** がサポートしない Web アプリケーション サーバに適用されます。

SiteMinder 設定： この値を空にします。

AS_GROUP_ID

アプリケーション サーバのグループ ID を指定します。このパラメータは、**SiteMinder** がサポートしない Web アプリケーション サーバに適用されます。

SiteMinder 設定： この値を空にします。

WEBDEPLOYACTION

Web アプリケーション サーバ上で実行されるアクションを指定します。

SiteMinder 設定： deploy

REDEPLOYWEBAPPS

このパラメータは変更しないでください。このパラメータは自動的に生成されます。

SiteMinder 設定： true

CMS Cluster

このセクションでは、応答ファイルの **CMS Cluster** セクションのパラメータについて詳しく説明します。

CMSCLUSTER

既存の **Content Management Server** にサーバを追加しているかどうかを指定します。

SiteMinder 設定： no

CLUSTER_NAMESERVER

Content Management Server にサーバをクラスタ化している場合、**Content Management Server** の名前を指定します。

SiteMinder 設定： この値を空にします。

CLUSTERPORTNUMBER

Content Management Server にサーバをクラスタ化している場合、**Content Management Server** がリスンしているポートを指定します。この値はデフォルトで、**CMSPORTNUMBER** パラメータの値になります。パラメータは応答ファイルの **CMS** セクションにあります。

SiteMinder 設定： この値は **CMSPORTNUMBER** の値と一致する必要があります。

CMS

このセクションでは、応答ファイルの **CMS** セクションのパラメータについて詳しく説明します。

DBTYPE

レポート データベースとして機能するデータベースのタイプを指定します。

SiteMinder 設定 :

■ MySQL

重要: SiteMinder は、埋め込みの MySQL バージョンのみをサポートします。

■ Oracle

重要: レポート サーバは、CA 製品が共有できる CA の共通コンポーネントです。そのため、SiteMinder を除く他の製品でサポートされるデータベースのタイプおよびバージョンに及ぶまで、レポート データベースとしてインストーラで設定することができます。サポートされているデータベースのタイプおよびバージョンのリストについては、「SiteMinder 12.52 SP1 プラットフォーム サポート マトリクス」を参照してください。

SERVICENAME

レポート データベースとして機能する Oracle データベースのサービス名を指定します。

注: MySQL を設定している場合、この値はデフォルトで **BOE120** になります。デフォルト値を使用します。

DATABASEUID

レポート データベースにアクセスするために使用される管理者アカウントの名前を指定します。

SiteMinder 設定 :

- 埋め込みの MySQL バージョンをインストールしている場合、アカウント名を入力します。インストーラは、必要な権限で管理者アカウントを作成します。

- Oracle を設定している場合、次の権限が有効なアカウント名を入力します： `create session`、`create table`、`create procedure`。

また、**CONNECT** と **RESOURCE** のロールを有効にしたアカウント名を入力することもできます。両方のロールに対して **Admin Option** 設定は必ず無効にしてください。

DATABASEPASSWORD

レポート データベースにアクセスするために使用される管理者アカウントのパスワードを指定します。

CMSNAMESEVER

レポート サーバ ホスト システムの名前を指定します。

SiteMinder 設定： この値は、応答ファイルの **Installation Information** セクション内の **LOCALNAMESEVER** の値と一致する必要があります。

CMSPORTNUMBER

Content Management Server が接続してリクエストを待機するポートを指定します。

デフォルト： 6400

CMSPASSWORD

集中管理サーバにアクセスする管理者アカウントのパスワードを指定します。このパスワードは **SAP BusinessObjects Enterprise** システム管理者アカウント用です。

SIANODENAME

Service Intelligence Agent (SIA) ノードの名前を指定します。

注：スペースまたは英数字以外の文字は使用できません。

SIAPORTNUMBER

SIA が接続してリクエストを待機するポートを指定します。

デフォルト： 6410

REINIT

レポート データベースが再初期化される必要があるかどうかを指定します。このパラメータは変更しないでください。このパラメータは自動的に生成されます。

SiteMinder 設定： yes

MySQL

このセクションでは、応答ファイルの **MySQL** セクションのパラメータについて詳しく説明します。

INSTALLMYSQL

埋め込みの **MySQL** バージョンをインストールする必要があるかどうかを指定します。

SiteMinder 設定：

- 埋め込みの **MySQL** バージョンをインストールしている場合は、**yes** を入力します。
- **Oracle** レポート データベースを設定している場合は、値を空にします。

SERVICEPORT

埋め込みの **MySQL** バージョンをインストールしている場合、**MySQL** が接続してリクエストをリスンするポートを指定します。

デフォルト： 3306

注： **Oracle** レポート データベースを設定している場合は、デフォルト値のままにします。

MYSQLHOSTNAME

埋め込みの **MySQL** バージョンをインストールしている場合、**MySQL** ホストシステムの IP アドレスを指定します。**MySQL** ホストシステムはレポートサーバホストシステムと同じです。

MYSQLROOTPASSWORD

埋め込みの **MySQL** バージョンをインストールしている場合、**MySQL root** ユーザアカウントのパスワードを指定します。

Audit

このセクションでは、応答ファイルの **Audit** セクションのパラメータについて詳しく説明します。

これらのパラメータは、**SiteMinder** 監査ベースのレポートとは関係がありません。**Content Management Server Auditing Database** は、レポートサーバに固有のアクティビティを監査するために使用され、**SiteMinder** には使用されません。

SiteMinder 監査データベースは、監査ベースのレポートの実行に必要となります。

AUDITINGENABLED

Content Management Server Auditing Database を有効にするかどうかを指定します。

- 埋め込みの **MySQL** バージョンをインストールしている場合、**Auditing Database** は自動的に有効になります。

SiteMinder 設定 : yes

- **Oracle** レポート データベースを設定している場合は、**Content Management Server** の監査は必要ありません。

SiteMinder 設定 : no

SERVICENAME_AUDIT

Content Management Server によって使用される監査サービスの名前を指定します。**Audit Database** を有効にしていない場合、この値はデフォルトで **BOE120_AUDIT** になります。

SiteMinder 設定 : デフォルト値のままにします。

SERVICEPORT_AUDIT

Content Management Server Audit Database が接続してリクエストをリスンするポート番号を指定します。この値はデフォルトで **3306** になります。

SiteMinder 設定 :

- 埋め込みの **MySQL** バージョンをインストールしている場合、この値を応答ファイルの **MySQL** セクション内の **SERVICEPORT** パラメータと一致させます。
- **Oracle** レポート データベースを設定している場合は、デフォルト値のままにします。

MYSQLHOSTNAME_AUDIT

Content Management Server Audit Database ホスト システムの IP アドレスを指定します。

SiteMinder 設定 :

- 埋め込みの MySQL バージョンをインストールしている場合、この値を応答ファイルの MySQL セクション内の MYSQLHOSTNAME パラメータと一致させます。
- Oracle レポート データベースを設定している場合は、値を空にします。

DATABASEUID_AUDIT

Content Management Server Auditing Database へのアクセスに使用される管理者アカウントの名前を指定します。

SiteMinder 設定 :

- 埋め込みの MySQL バージョンをインストールしている場合、この値を応答ファイルの MySQL セクション内の DATABASEUID パラメータと一致させます。
- Oracle レポート データベースを設定している場合は、値を空にします。

DATABASEPWD_AUDIT

Content Management Server Auditing Database へのアクセスに使用される管理者アカウントのパスワードを指定します。

SiteMinder 設定 :

- 埋め込みの MySQL バージョンをインストールしている場合、この値を応答ファイルの MySQL セクション内の MYSQLROOTPWD パラメータと一致させます。
- Oracle レポート データベースを設定している場合は、値を空にします。

Marketing Products

このセクションでは、応答ファイルの **Marketing Products** セクションのパラメータについて詳しく説明します。

ENABLEMP

手動で有効にするクライアント、サーバ、**Web** 層、および他の **SAP BusinessObjects Enterprise** を指定します。

SiteMinder 設定： この値を空にします。

DISABLEMP

手動で無効にするクライアント、サーバ、**Web** 層、および他の **SAP BusinessObjects Enterprise** を指定します。

SiteMinder 設定： このパラメータの値を空にします。

BIEK

このセクションでは、応答ファイルの **BIEK** セクションのパラメータについて詳しく説明します。

BIEK_INSTALL_USER

インストーラが使用する、**root** ではないユーザアカウントを指定します。

BIEK_INSTALL_GROUP

root 以外のユーザが所属するグループを指定します。

BIEK_CASHCOMP

CA 共有コンポーネント環境変数 (**CASHComp**) が設定されるべきフルパスを指定します。 **CASHComp** がすでに設定されている場合、インストーラはこの値を無視します。

BIEK_INSTALL_SAMPLES

インストーラが **CA** テンプレートをインストールする必要があるかどうかを指定します。 このパラメータは、**SiteMinder** レポート テンプレートとは関係がありません。 **SiteMinder** レポート サーバ設定ウィザードが、必要なレポート テンプレートをインストールします。 このウィザードは、レポート サーバをインストールした後に実行します。

0

サンプルテンプレートをインストールしません。

1

サンプルテンプレートをインストールします。

SiteMinder 設定 : 0

BIEK_MIGRATE_CMS_DATA

このパラメータは変更しないでください。このパラメータはアップグレードでのみ使用されます。

SiteMinder 設定 : 0

BIEK_SOURCE_CMS_PASSWORD

このパラメータは変更しないでください。このパラメータはアップグレードでのみ使用されます。

SiteMinder 設定 : この値を空にします。

SiteMinder レポート サーバ設定ウィザードのプロパティファイルの変更

環境設定変数を定義するには、レポートサーバ設定ウィザードのプロパティファイルを変更します。このファイル内のデフォルトパラメータ、パスワード、およびパスには、ウィザードを最後に実行したときに入力した情報が反映されます。

このプロパティファイルには、以下のパラメータがあります。

DEFAULT_BOXI_INSTALL_PATH

レポートサーバのインストールパスを指定します。

DEFAULT_BOXI_PASSWORD

デフォルト **BusinessObjects** の管理者アカウントのパスワードを指定します。

注: **ENCRYPTED_BOXI_PASSWORD** に暗号化された値を使用する場合、このパラメータに値は必要ありません。

ENCRYPTED_BOXI_PASSWORD

デフォルト **BusinessObjects** の管理者アカウントの暗号化パスワードを指定します。

重要: この暗号化された値を変更しないでください。別のパスワードを入力するには、暗号化パスワードをコメント化し、**DEFAULT_BOXI_PASSWORD** に値を指定します。

DEFAULT_AUDIT_DATABASE_TYPE

SiteMinder 監査ストアとして機能するデータベースのタイプを指定します。

注: レポート サーバ設定ウィザードを実行する前に、SiteMinder 監査データベースを設定する必要はありません。

値: 1 または 2

1

Microsoft SQL Server を指定します。

2

Oracle を指定します。

レポート サーバ インストーラの実行

無人インストールを実行し、ユーザによる操作なしでレポート サーバをインストールします。

インストールする前に

レポート サーバをインストールする前に、以下の点を考慮します。

- テクニカルサポートサイトで、インストールメディアを使用してレポート サーバをインストールします。

注: インストールメディア名のリストについては、「ポリシー サーバリリース ノート」を参照してください。

- レポート サーバは、32 ビット ネイティブ バイナリとしてコンパイルされ、32 ビット データ ソース ミドルウェア接続を使用するよう設定されます。Windows 64 ビット オペレーティング システムにインストールしている場合は、必ず `odbcad32.exe` を使用して DSN を作成してください。この実行ファイルは、以下の場所にあります。

`install_home¥Windows¥SysWOW64`

`install_home`

Windows オペレーティング システムのインストール パスを指定します。

- レポート サーバインストールには、プロセスとして実行する以下のコンポーネントが含まれます。
 - Content Management Server
 - Server Intelligence Agentこれらのコンポーネントでは、通信に TCP/IP ポートが必要です。インストーラでは、レポート サーバ ホスト システム上のポート競合を防ぐためにデフォルト設定を変更することができます。
- **重要:** インストール zip には、複数のフォルダが含まれています。レポート サーバ インストーラは、このフォルダ構造を必要とします。zip を抽出した後にレポート サーバ インストーラを移動させた場合は、同じ場所にフォルダ構造全体をコピーします。必ずそのフォルダ構造からインストール メディアを実行してください。

Windows

以下の手順に従います。

1. 実行中のすべてのアプリケーションを終了します。
2. コマンド プロンプトを開きます。
3. ディレクトリを *temporary_location* に変更します。

temporary_location

インストール メディアをコピーした場所を示します。

4. 以下のコマンドを入力します。

installation_media *silent* *path_to_response_file*

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する前に、管理者権限でコマンドライン ウィンドウを開きます。アカウントに管理者権限がある場合でも、このようにコマンドライン ウィンドウを開きます。

installation_media

レポート サーバ インストール実行可能ファイルの名前を指定します。

注: インストール メディア名のリストについては、「ポリシー サーバリリース ノート」を参照してください。

path_to_response_file

ファイルへのパスを指定します。パスには応答ファイル名が含まれている必要があります。

注: 応答ファイルは、インストール実行ファイルと同じディレクトリ内になくてもかまいません。

サイレントインストールが開始されます。

UNIX

以下の手順に従います。

1. 実行中のすべてのアプリケーションを終了します。
2. root ユーザ権限のあるアカウントを使用していることを確認してください。
3. Bourne シェルを開き、*temporary_location* に移動します。

temporary_location

インストールメディアをコピーした場所を示します。

4. 以下のコマンドを入力します。

```
./installation_media silent path_to_response_file
```

installation_media

レポートサーバの実行ファイルの名前を指定します。

注: インストールメディア名のリストについては、「ポリシー サーバリリース ノート」を参照してください。

path_to_response_file

応答ファイルへのパスを指定します。パスには応答ファイル名が含まれている必要があります。

注: 応答ファイルは、インストール実行ファイルと同じディレクトリ内になくてもかまいません。

サイレントインストールが開始されます。

レポートテンプレートのインストール

無人インストールを実行し、ユーザによる操作なしで SiteMinder レポートテンプレートをインストールします。

インストールする前に

テクニカルサポートサイトで、インストールメディアを使用して SiteMinder レポート テンプレートをインストールします。

注: インストール メディア名のリストについては、「ポリシー サーバリリース ノート」を参照してください。

付録 A: 国際環境用のポリシー サーバの設定

このセクションには、以下のトピックが含まれています。

[国際環境内のポリシー サーバ \(P. 689\)](#)

[ポリシー サーバのインストールを計画する際の注意事項 \(P. 689\)](#)

[国際文字をサポートする SiteMinder データ ストアの設定 \(P. 694\)](#)

国際環境内のポリシー サーバ

ポリシー サーバは、Oracle または SQL Server のデータベース内にある SiteMinder データ ストア、および国際環境用の LDAP サーバをサポートします。

ポリシー サーバのインストールを計画する際の注意事項

ポリシー サーバをインストールする前に、以下の点を考慮します。

- サポートされているオペレーティング システムおよびサードパーティ ソフトウェアを使用します。
- サポートされているデータベースを作成します。
 - ポリシーまたはセッション データを格納するためのデータベースを作成する前に、それらが UTF-8 エンコーディングでフォーマットされることを確認します。
 - ユーザ ストア データベースは UTF-8 エンコーディングに制限されていません。ローカル文字セット エンコーディングでユーザ データベースを作成できます。

注: Active Directory ネームスペースはマルチバイト文字をサポートしません。使用しているコード ページに関係なく、SiteMinder は Unicode での定義に従って文字を処理します。コード ページは特殊文字を 1 バイトとして参照できますが、SiteMinder は、Unicode でその文字がマルチバイト文字として定義されていれば、マルチバイト文字として処理します。

- すべての 管理 UI フィールドがマルチバイト文字をサポートします。
- 一部のポリシー サーバ コンポーネントは、国際環境でマルチバイト文字および ASCII 文字をサポートします。
- SiteMinder はマルチバイト文字（MBCS） URL をサポートします。

注: サポートされている CA およびサードパーティ コンポーネントのリストについては、テクニカル サポート サイトの **SiteMinder 12.52 SP1** プラットフォームのサポート マトリックスを参照してください。

マルチバイト文字をサポートしているポリシー サーバ コンポーネント

以下のポリシー サーバ コンポーネントは、国際環境でマルチバイト文字および ASCII 文字をサポートします。

- 管理 UI
- ポリシー サーバ管理コンソール
- 認証方式
 - HTML フォーム
 - X.509 クライアント証明書
 - X.509 クライアント証明書および HTML フォーム
 - X.509 クライアント証明書または HTML フォーム
 - RADIUS CHAP/PAP
 - SecurID 認証
 - 匿名認証
 - カスタム認証
 - インパーソネーション認証
- パスワードサービス

注: パスワードサービスは ASCII 文字に制限されていますが、リダイレクト URL としてマルチバイト文字 URL をサポートできます。

- レスポンス
- Post 維持
- SiteMinder テスト ツール

- テキスト ファイルへの監査ログ
- ODBC データベースへの監査ログ
- smobjimport
- XPSExport と XPSImport
- Java エージェント API

マルチバイト文字 URL のサポート

SiteMinder は、マルチバイト文字 (MBCS) を含んでいる URL をサポートしています。MBCS URL のサポートには、以下のもののサポートが含まれます。

- 国際化ドメイン名 - IDN (*internationalized domain name*) は、発音区別符号の付いた文字、アラビア文字や中国文字など非ラテン文字を含む非 ASCII 文字を含むことができるインターネット ドメイン名です。
- **Internationalized Resource Identifier - IRI** (*Internationalized Resource Identifier*) は、URI (Uniform Resource Identifier) を国際化したものです。IRI には、MBCS セットからの 1 つ以上の ASCII 文字を含めることができます。URI は ASCII 文字のサブセットに制限されています。

MBCS URL のサポートによって、以下が可能になります。

- SiteMinder が、MBCS URL によってアクセスされるリソースを保護する。
- IDN と IRI を使用する特定の認証方式を設定する。

MBCS URL のサポートを有効にする方法

SiteMinder 環境内の MBCS URL のサポートには、以下のことが必要です。

- 保護されたリソースにアクセスするために使用される Web ブラウザが特定の要件を満たしていること。
- 環境内の Web サーバの実装が特定の要件を満たしていること。
- Web エージェント設定オブジェクトから、特定のデフォルト不正文字が削除されていること。

MBCS URL のサポートを有効にする方法

1. Web ブラウザが MBCS URL 用の要件を満たしていることを確認します。
2. Web サーバが MBCS URL 用の要件を満たしていることを確認します。
3. Web エージェント設定オブジェクトを設定します。

MBCS URL 用の Web ブラウザ要件

Web ブラウザは、UTF-8 形式でリソースを提供でき、そのドメイン名に非 ASCII 文字が含まれている Web サーバにリクエストを送信する必要があります。

保護されたリソースにアクセスするために使用される Web ブラウザは、以下の機能を備えている必要があります。

- IDN (Internationalized Domain Names: 国際化ドメイン名) のサポート。
- IRI (Internationalized Resource Identifiers) のサポート。
- UTF-8 形式でのリクエストの送信。

MBCS URL 用の Web サーバ要件

以下の要件の少なくとも 1 つを満たす場合、Web サーバは MBCS URL をサポートできます。

- Web サーバが UTF-8 リクエストをローカル文字セットエンコーディングに変換できる。

または

- Web サーバが UTF-8 形式でファイルを格納できる。したがって、Web サーバが、UTF-8 形式で Web ブラウザから IRI のリクエストを受け取った場合にファイルを提供できる。

マルチバイト文字サポートの有効化

MBCS サポートでは、Web エージェント設定オブジェクトから特定のハイビット ASCII 文字値を削除することが必要です。

注: ハイビット ASCII 文字を削除すると、Web エージェントが特定の文字をブロックするのを防ぎます。

MBCS サポートを有効にする方法

1. 管理 UI を開きます。
2. [インフラストラクチャ] - [エージェント] をクリックします。
3. [エージェント設定]-[エージェント設定の変更] をクリックします。
[エージェント設定の変更] ペインが表示されます。
4. 検索条件を入力し、[検索] をクリックします。
検索条件と一致するエージェント設定オブジェクトが表示されます。
5. 目的のエージェント設定オブジェクトを選択し、[選択] をクリックします。
[パラメータ] グループ ボックスにエージェント設定パラメータがリスト表示されます。
6. BadURLChars の [編集] アイコンをクリックします。
[パラメータの編集] ペインが表示されます。
7. [値] フィールドから以下を削除します。
 - %00-%1f
 - %7f-%ff
8. [OK] をクリックします。
編集された値が、BadURLChars フィールドで表示されます。
9. [サブミット] をクリックします。
Web エージェント設定オブジェクトが MBCS URL をサポートするように設定されます。

MBCS URL を持つリソースの保護

MBCS URL のサポートにより、SiteMinder は、非 ASCII 文字を含む URL によってアクセスされるリソースを保護できます。

レルムおよび関連付けられたルールを作成し、リソースを保護する場合、[リソース] フィールドに MBCS URL を入力できます。ユーザは IDN と IRI をサポートするブラウザを使用して、保護されているリソースにアクセスできます。

注: レルムおよびルールの作成の詳細については、「ポリシー サーバ設定ガイド」を参照してください。

MBCS URL をサポートする認証方式

[サーバ名] フィールドで IDN を指定し、[ターゲット] フィールドで IRI を指定して、以下の認証方式を設定できます。

- SSL を介した基本
- HTML フォーム テンプレート
- SSL を介した HTML フォーム テンプレート
- X509 クライアント証明書
- X509 クライアント証明書およびフォーム

注: Netscape と Firefox は、IDN を含む URL へのリダイレクトを受け付け理ません。 Punycode <http://en.wikipedia.org/wiki/Punycode> を使用しない限り、フォーム関連認証方式で IDN を入力すると、エラーになります。認証方式の設定の詳細については、「ポリシー サーバ設定ガイド」を参照してください。

国際文字をサポートする SiteMinder データストアの設定

SQL Server または Oracle データベース内に SiteMinder データストアを設定できます。これらのデータストアを設定する場合、ポリシー サーバでは UTF-8 エンコーディングのみがサポートされており、このエンコーディング タイプをサポートするデータベースを使用する必要があることに注意してください。

注: このセクションは、リレーショナルデータベース内の SiteMinder データストアの設定を対象としています。LDAP サーバ内でのこれらのストアの設定の詳細については、「ポリシー ストアまたはキー ストアとしての LDAP ディレクトリ サーバの設定」を参照してください。

SQL Server 内の国際 SiteMinder データストアの設定

ポリシー、キー、セッション、またはキー ストアを作成するには、SQL Server データベースに SiteMinder データストアを設定します。

注: デフォルトでは、SQL Server は UTF-8 文字エンコーディングをサポートします。

Oracle での国際 SiteMinder データストアの設定

Oracle での国際 SiteMinder データストアを設定する方法

1. Oracle がインストールされるマシンで、UTF-8 文字エンコーディングをサポートするカスタム Oracle データベースを作成します。

注: 詳細および手順については、Oracle のドキュメントを参照してください。

既存の Oracle データベースが UTF-8 文字エンコーディングをサポートしているかどうか確認するには、以下のクエリを実行します。

```
Select * from nls_database_parameters where parameter =  
'NLS_CHARACTERSET'
```

2. Oracle データベースに SiteMinder データストアを設定することにより、ポリシー サーバ用のポリシー、キー、セッション、またはキー ストアを作成します。

Solaris/LINUX Red Hat ポリシー サーバでの UTF-8 文字の Oracle データベースへのログ記録

Solaris/LINUX Red Hat ポリシー サーバは、Oracle 監査ログ データベースに UTF-8 文字をログ記録できます。この設定を有効にするために、以下の環境変数を設定する必要があります。

簡体字中国語オペレーティング システムの場合

- LANG=zh_CN.utf8

日本語オペレーティング システムの場合

- LANG=jp_JP.UTF-8

LANG 変数をシステム全体またはポリシー サーバプロセスに対してのみ設定します。

注: 他のアプリケーションに影響を与えないようにするために、ポリシー サーバプロセスに対してのみこの変数を設定してください。

データベース ドライバ変数

- IANAAppCodePage=utf-8

この変数は、<policy_server_installation>/db にインストールされた system_odbc.ini ファイルの該当するデータ ソース定義セクションで設定します。

Oracle クライアントの設定

ポリシー サーバでは Oracle ワイヤ プロトコル ドライバを使用するので、Oracle クライアントは必要ありません。ただし、監査ログ データベースからデータを読み取るために、環境に Oracle SQLPLUS クライアントが必要なときは、以下の環境変数のいずれかまたは両方を設定し、マルチバイト文字が正しく表示されるようにすることが必要な場合もあります。

簡体字中国語オペレーティング システムの場合

- LANG=zh_CN.utf8

日本語オペレーティング システムの場合

- LANG=jp_JP.UTF-8

Oracle SQLPlus クライアントの場合

- NLS_LANG (たとえば NLS_LANG=Japanese_Japan.UTF8)

注: 詳細については、オペレーティング システムおよびデータベースのクライアント設定マニュアルを参照してください。

SQL Server で Unicode をサポートするユーザ ストアの設定

ポリシー サーバと共にインストールされた smsampleusers_sqlserver.sql ファイルを使用すると、SQL Server データベース内にユーザ ストアを設定できます。このファイルは、*siteminder_installation¥db¥SQL* ディレクトリにインストールされます。

注: ユーザ ストアは UTF-8 形式に制限されていません。ローカル文字セットエンコーディングでユーザ ストアを作成できます。

次の手順に従ってください:

1. 以下を実行することにより、smsampleusers_sqlserver.sql ファイルを編集します。
 - a. すべての VARCHAR インスタンスを **nvarchar** に置換します。
 - b. 国際化文字列を含む INSERT ステートメントの前に **N** を配置します。

日本語の例

```
insert into SmUser ( UserID , Name, Password,
  LastName, FirstName, ...)
```

```
values (12, N'やまもと',
'siteminder','guest','guest','guest@mycompany.com...)
```

1. smsampleusers_sqlserver.sql ファイルをインポートします。
 注: smsampleusers_sqlserver.sql ファイルのインポートの詳細については、サンプルユーザディレクトリを参照してください。
2. ポリシー サーバユーザインターフェースの SiteMinder ODBC クエリ方式ダイアログ ボックスを開き、すべての = %s ステートメントの %s 参照の前に **N** を配置することにより、ポリシー ストアの SQL クエリ方式を変更します。

例:

以下のサンプル クエリ スキーム ステートメントがあるとします。

```
select Name, 'User' from SmUser where Name = '%s' Union select Name,
'Group' from SmGroup where Name = '%s'
```

これは、以下のようになります。

```
select Name, 'User' from SmUser where Name = N'%s' Union select Name,
'Group' from SmGroup where Name = N'%s'
```

1. ポリシー サーバを停止してから再起動します。
 これで、ユーザ ストア設定が完了し、マルチバイト文字がサポートされるようになります。

Oracle 内での日本語ユーザストアの設定

ポリシー サーバとともにインストールされた `smssampleusers_oracle.sql` ファイルを使用すると、Oracle データベース内にユーザストアを設定できます。このファイルは、`<siteminder_installation>\db\SQL` ディレクトリにインストールされます。

注: ユーザストアは UTF-8 形式に制限されていません。ローカル文字セットエンコーディングでユーザストアを作成できます。

Oracle 内に日本語ユーザストアを設定する方法

1. Oracle の UTF-8 NLS_CHARACTERSET エンコーディングをサポートするユーザデータ用のデータベースを作成します。
2. Oracle の SQL Plus を使用して、`smssampleusers_oracle.sql` ファイルをインポートします。

注: `smssampleusers_oracle.sql` ファイルのインポートの詳細については、サンプルユーザディレクトリを参照してください。日本語の文字を挿入する場合、日本語オペレーティングシステムからのファイルをインポートしてください。

ユーザストアの設定が完了しました。

付録 B: 変更される環境変数

このセクションには、以下のトピックが含まれています。

[変更された Windows 環境変数](#) (P. 699)

[変更された UNIX 環境変数](#) (P. 700)

変更された Windows 環境変数

ポリシー サーバ

ポリシー サーバのインストールは、Windows 環境内の以下の環境変数を追加および変更します。

- NETE_PS_ROOT = \$INSTALL_PATH\$
- NETE_PS_PATH = \$INSTALL_PATH\$/\$bin;
\$INSTALL_PATH\$/\$bin\$/\$thirdparty;\$INSTALL_PATH\$/\$lib
- NETEGRITY_LICENSE_FILE = %NETE_PS_ROOT%\$/\$license\$/\$license.dat
- NETE_JVM_OPTION_FILE = %NETE_PS_ROOT%\$/\$config\$/\$JVMOptions.txt
- NETE_DOC_ROOT=\$INSTALL_PATH\$/\$netegrity_documents
- NETE_PS_OPACK="INSTALLED"
- NETE_JRE_ROOT = HKEY_LOCAL_MACHINE¥SOFTWARE¥JavaSoft¥Java Runtime Environment¥1.7 in JAVAHOME value
- NETE_JAVA_PATH=%NETE_JRE_ROOT%\$/\$bin;%NETE_JRE_ROOT%\$/\$bin\$/\$server
- NETE_JDK_ROOT = HKEY_LOCAL_MACHINE¥SOFTWARE¥JavaSoft¥Java Development Kit¥1.7 in JAVAHOME value
- NETE_SHORTCUTS = C:¥Documents and Settings¥All Users¥Start Menu¥Programs¥SiteMinder

注: これがデフォルトの場所です。

管理 UI

管理 UI のインストールは、Windows 環境内の環境変数を追加しません。

レポート サーバ

レポート サーバのインストールは、Windows 環境内の以下の環境変数を追加および変更します。

- IAM_RPTSRV_HOME=\$REPORT_SERVER_LOC\$
- BOE_SSL_JVMOPTIONS="-Dcom.ca.rptsrv.home=%IAM_RPTSRV_HOME%
-Djava.library.path=%IAM_RPTSRV_HOME%/external/bin"

変更された UNIX 環境変数

ポリシー サーバ

ポリシー サーバのインストールは、UNIX 環境内の以下の環境変数を追加および変更します。

- NETE_PS_ROOT = \$INSTALL_PATH\$
- NETE_PS_PATH = \$INSTALL_PATH\$/\$bin;
\$INSTALL_PATH\$/\$bin\$/\$thirdparty;\$INSTALL_PATH\$/\$lib
- NETEGRITY_LICENSE_FILE = %NETE_PS_ROOT%\$/\$license\$/\$license.dat
- NETE_JVM_OPTION_FILE = %NETE_PS_ROOT%\$/\$config\$/\$JVMOPTIONS.txt
- NETE_DOC_ROOT=\$INSTALL_PATH\$/\$netegrity_documents
- NETE_PS_OPACK="INSTALLED"
- NETE_JDK_ROOT = \$JDK_PATH\$
- NETE_JRE_ROOT = \$JRE_PATH\$
- NETE_JAVA_PATH=%NETE_JRE_ROOT%\$/\$bin%;%NETE_JRE_ROOT%\$/\$bin\$/\$server

管理 UI

管理 UI のインストールは、UNIX 環境内の環境変数を追加しません。

レポートサーバ

レポートサーバのインストールは、UNIX 環境内の以下の環境変数を追加および変更します。

- `IAM_RPTSRV_HOME=$REPORT_SERVER_LOC$`
- `BOE_SSL_JVMOPTIONS="-Dcom.ca.rptsrv.home=$IAM_RPTSRV_HOME
-Djava.library.path=$IAM_RPTSRV_HOME%/external/bin"`