CA SiteMinder®

ポリシー サーバ管理ガイド

r12.0 SP3

ca technologies

CA 製品リファレンス

このマニュアルが参照している CA の製品は以下のとおりです。

- CA SiteMinder®
- CA SOA Security Manager
- CA Identity Manager
- CA CA Security Compliance Manager

CA への連絡先

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

目次

第 1 章: ポリシー サーバの管理

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 サーバ管理の概要

ポリシー サーバは、以下のような CA 製品と連携して動作するアクセス制御プラットフォームです。

- CA SiteMinder - ポリシー サーバと Web エージェントとを統合して、Web サーバのアクセス制御を行います。
- CA SOA Security Manager - XML ベースのトランザクションのアクセス制御を行います。この製品をご購入済みの場合、詳細については「*CA SOA Security Manager Policy Configuration Guide*」を参照してください。
- CA Identity Manager - ID 管理サービスを提供します。詳細については、「*CA Identity Manager Administration Guide*」を参照してください。

注: SiteMinder およびポリシーベースのリソース管理については、「*ポリシー サーバ設定ガイド*」を参照してください。

ポリシー サーバのコンポーネント

ポリシー サーバ環境は、次の 2 つのコアコンポーネントによって構成されます。

- **ポリシー サーバ** - ポリシー管理、認証、許可、およびアカウンティングの各サービスを提供します。
- **ポリシー ストア** - すべてのポリシー サーバ データが格納されます。

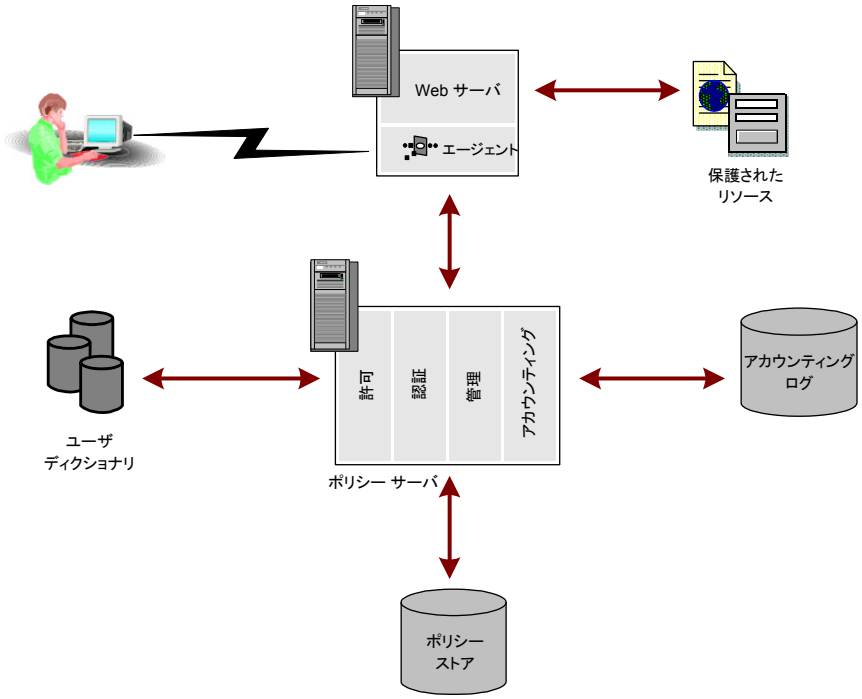
追加のコンポーネントとして、さまざまな CA 製品（SiteMinder エージェントなど）が含まれます。SiteMinder エージェントは、標準の Web サーバまたはアプリケーション サーバに統合されます。エージェントによって、SiteMinder では、事前定義されたセキュリティ ポリシーに基づいて Web アプリケーションおよびコンテンツへのアクセスを管理できるようになります。そのほかに、SiteMinder エージェントには、SiteMinder が Web 以外のエンティティへのアクセスを制御することを可能にするタイプもあります。たとえば、SiteMinder RADIUS エージェントは RADIUS デバイスへのアクセスを管理し、SiteMinder アフィリエイト エージェントはポータル サイトからアフィリエイトの Web サイトに渡された情報を管理します。

ポリシー サーバの処理

ポリシー サーバでは、アクセス制御とシングル サインオンが可能です。通常、個別の Windows または UNIX システム上で稼働し、以下の重要なセキュリティ処理を実行します。

- **認証** - ポリシー サーバはさまざまな認証方法をサポートします。ユーザ名とパスワード、トークン、フォーム ベースの認証、あるいは公開キー証明書などに基づいてユーザを認証します。
- **許可** - ポリシー サーバは、ポリシー サーバ管理者により作成されたアクセス制御ルールの管理、実行を行います。これらのルールは、保護された各リソースに対して許可された操作が定義されています。
- **管理** - ポリシー サーバは、管理 UI を使用して設定できます。UI を使用して設定情報をポリシーストアに記録することを可能にしているのが、ポリシーストアの管理サービスです。ポリシーストアとは、権限付与情報が保存されているデータベースです。
- **アカウンティング** - ポリシー サーバは、システム内で発生するイベントの監査情報を記録するログ ファイルを生成します。これらのログは、あらかじめ定義されたレポート形式で印刷して、セキュリティイベントや異常の分析に使用できます。
- **状態監視** - ポリシー サーバには、状態監視コンポーネントが用意されています。

以下の図は、SiteMinder Web エージェントを 1 つ含む SiteMinder 環境でのポリシー サーバの単純な実装を示しています。

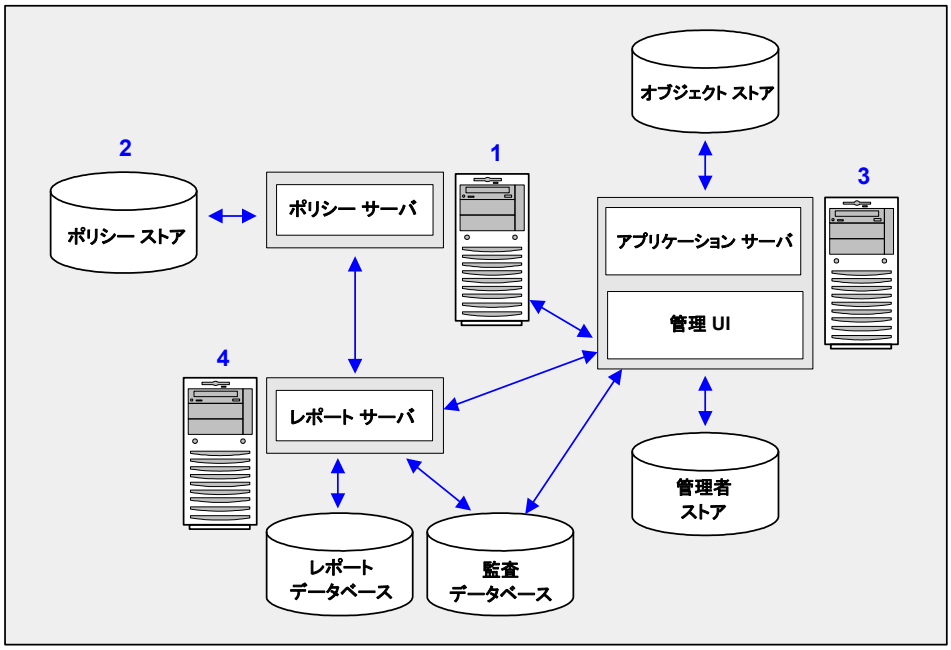


実際の Web 環境では、ユーザはブラウザを介してリソースをリクエストします。リクエストは、Web サーバが受信し、SiteMinder Web エージェントがインターセプトします。Web エージェントは、リソースが保護されているかどうかを判別し、保護されている場合は、ユーザのクレデンシャルを収集してポリシー サーバに渡します。ポリシー サーバは、ユーザ固有のディレクトリに照らし合わせてユーザを認証します。次に、ポリシーストア内のルールとポリシーに基づいて、リクエストしたリソースへのアクセスが認証されたユーザに許可されているかどうかを確認します。ユーザが認証され、許可されると、ポリシー サーバは保護されたリソースへのアクセス許可を付与し、権限と資格に関する情報を配信します。

注: カスタム エージェントは、SiteMinder エージェント API を使用して作成できます。詳細については、「*Programming Guide for C*」を参照してください。

ポリシー サーバ管理

以下の図は、ポリシー サーバの管理モデルを示しています。



1. **ポリシー サーバ** - ポリシー管理、認証、許可、およびアカウンティングの各種サービスを提供します。
2. **ポリシー ストア** - ポリシー サーバのすべてのデータを格納します。ポリシー ストアの設定は、サポートされている LDAP またはリレーショナル データベース内で行うことができます。
3. **管理 UI** - ポリシー サーバを介して、SiteMinder 管理者アカウント、オブジェクト、およびポリシー データを管理できます。管理 UI をインストールするときは、ディレクトリ XML ファイル、管理者ユーザ ストア、およびオブジェクト ストアを設定します。
   - **オブジェクト ストア** - 管理 UI はイベントベースおよびタスクベースの非同期アプリケーションです。 オブジェクト ストアはこの情報を格納します。オブジェクト ストアの設定は、Microsoft SQL Server または Oracle データベース内で行います。

- **管理者ユーザ ストア** - 管理 UI は管理者ユーザ ストアを使用して、SiteMinder 管理者アカウントを認証します。すべての管理者アカウントは 1 つの管理者ユーザ ストアに格納する必要があります。管理 UI をインストールするときは、サポートされている LDAP ディレクトリ サーバまたは ODBC データベース内で管理者ユーザ ストアを設定します。

4. **レポート サーバおよびレポート データベース** - SiteMinder の一連のポリシー分析および監査レポートを 管理 UI から作成し、管理できます。レポート サーバとレポート データベースは、レポート機能を使用するために必要になります。また、ポリシー分析レポートの実行にも必要です。レポート サーバと監査データベースは、監査ベースのレポートを実行するために必要になります。

ポリシー サーバの管理タスク

ポリシー サーバ管理者は、ユーザやユーザ セッションの管理だけではなく、必要に応じて、SiteMinder 環境のシステムレベルの設定や調整と、そのパフォーマンスの監視や維持作業を行う必要があります。

基本的なシステム構成タスクと管理タスクのほとんどは、ポリシー サーバ管理コンソールで行います。その他のタスクは、管理 UI を使用して実行します。

ポリシー サーバの管理タスクには、以下が含まれます。

- ポリシー サーバの起動と終了
- ポリシー サーバ エグゼクティブの設定
- キャッシュ管理
- 暗号化キーの設定と管理
- ユーザセッションとユーザアカウントの管理
- SiteMinder 環境の状態の監視
- レポートの実行

ポリシー サーバ管理コンソール

ポリシー サーバ管理コンソール（略して「管理コンソール」）には、ポリシー サーバ設定とシステム管理のための一連のオプションが備わっています。管理コンソールは、タブベースのユーザ インターフェースです。この UI では、情報や制御項目が機能ごとにグループ分けされて、1 つのウィンドウの各タブに表示されます。

重要: ポリシー サーバ管理コンソールを実行するのは、Microsoft Windows における管理者グループのメンバ ユーザに限定する必要があります。

管理コンソールの起動

管理コンソールを開く方法

- **Windows** -- SiteMinder プログラム グループ内の［ポリシー サーバ管理コンソール］アイコンを選択します。
- **UNIX** -- *installation_directory*/siteminder/bin/smconsole を実行します。

注: UNIX 上でポリシー サーバ管理コンソールを実行するには、X ディスプレイ サーバが実行され、ディスプレイが「export DISPLAY=n.n.n.n:0.0」の指定によって有効になっている必要があります。n.n.n.n はポリシー サーバが稼働しているマシンの IP アドレスです。

管理コンソール設定の変更内容の保存

管理コンソールのどのタブでも、次の操作を行うことができます。

- [適用] をクリックすると、設定は保存されますが、管理コンソールは開いたままになります。
- [OK] をクリックすると、設定が保存され、管理コンソールが閉じます。

注: 管理コンソール設定の変更内容を有効にするには、認証および許可プロセスを終了して再起動する必要があります。これらのサービスが再起動するまでは、ポリシー サーバで新しい設定を使用できません。

ポリシーサーバーユーザーインタフェース

ブラウザ ベースの CA SiteMinder 管理 UI の主な用途は、ポリシー サーバ オブジェクトの管理ですが、いくつかのシステム管理機能も備えています。

管理 UI にアクセスする方法

1. 以下のいずれかの操作を行います。
   - 管理 UI をホストしているコンピュータから、[スタート]-[プログラム]-[CA]-[SiteMinder]-[SiteMinder 管理 UI]をクリックします。
   - ブラウザで以下の URL を開きます。

     `http://host_name.domain:port_number/iam/siteminder`

   host_name は 管理 UI が実行されているコンピュータの名前です。完全修飾ドメイン名を使用してください。管理 UI がデフォルトの HTTP ポート(80 番)を使用*していない* 場合は、以下の例に示すようにポート番号を追加する必要があります。

   http://maincomputer.example.com:8080/iam/siteminder.

   管理 UI のログイン ページが表示されます。
2. それぞれのフィールドに、有効なユーザ名とパスワードを入力します。

   ポリシー サーバに初めてアクセスするときは、ポリシー サーバのインストール中に作成したデフォルトのスーパーユーザ管理者アカウントを使用します。
3. [Log In]をクリックします。

   管理 UI が開きます。

   ウィンドウの表示内容は、ログイン時に使用した管理者アカウントの権限に応じて変わります。アカウントにアクセス許可がある項目のみが表示されます。

XPS ツールへのアクセス許可の付与

SiteMinder に含まれる XPS ツールへのアクセス許可は、管理者が 管理 UI を使用して個々のユーザに付与する必要があります。

XPS ツールへのアクセス許可を付与する方法

1. 管理 UI にログインします。
2. [管理]タブをクリックします。
3. [管理者]をクリックし、以下のいずれかをクリックします。
   - 新しい管理者を追加するには、[管理者の作成]をクリックします。
   - 既存の管理者のアクセス許可を変更するには、[管理者の変更]をクリックします。
4. 管理者の名前と説明(省略可)をそれぞれのフィールドに入力します。
5. ユーザ パスを入力するか、[検索]ボタンをクリックし、既存のユーザ パスを選択します。

   注: XPS ツールによって制御される任意の設定への書き込みアクセスを行うには、ユーザ パス(管理者が 管理 UI または XPSSecurity ツールで指定)が必要です。ユーザ パスの形式は以下のとおりです。
   namespace://*directory_server*/*DN* または *Login_for_OS*
6. (オプション)スーパーユーザの権限を付与するには、[スーパーユーザ]チェック ボックスをオンにします。
7. [アクセス方法]グループ ボックスのコマンド ライン ツール セクションで、以下の任意のチェック ボックスをオンにします。

   XPSEvaluate Allowed

   XPS 式評価ツールへのアクセス許可を付与します。

   XPSExplorer Allowed

   XPS データベースを編集するツールへのアクセス許可を付与します。

   XPSRegClient Allowed

   Web Access Manager サーバまたは Reports サーバを権限のあるクライアントとして登録する XPS ツールへのアクセス許可を付与します。

XPSConfig Allowed

XPS 対応製品の XPS 設定を検査するツールへのアクセス許可を付与します。

XPSSecurity Allowed

XPS ユーザを作成し、XPS 関連の権限を指定するセキュリティ ツールへのアクセス許可を付与します。

8. (オプション) 付与するその他のアクセス許可のチェック ボックスをオンにします。
9. (オプション) ユーザのアクセスを特定のカテゴリに制限するには、[作成]ボタンをクリックし、希望するカテゴリを選択します。
10. [サブミット]をクリックします。

変更がサブミットされ、レスポンスが表示されます。

第 2 章: ポリシー サーバの起動と終了

このセクションには、以下のトピックが含まれています。

サービスとプロセスの概要

ポリシー サーバは、Windows 環境では 2 つのサービスを、UNIX 環境では 2 つのプロセスを実行します。ポリシー サーバのインストールプロセスでは、ポリシー サーバプロセスおよび監視プロセスを起動して、将来、システム起動時に自動的にプロセスを実行するようにエグゼクティブ アプリケーションを設定します。

Windows の主なポリシー サーバ プロセスを以下に示します。

ポリシー サーバ

認証、許可、監査/ログ、および管理 (有効になっている場合) のエージェントリクエストを処理します。

SiteMinder 状態監視サービス

認証サーバ、許可サーバ、および Web エージェントを監視する OneView モニタです。

UNIX の主なポリシー サーバ プロセスを以下に示します。

smpolicysrv

認証、許可、監査/ログ、および管理 (有効になっている場合) のエージェントリクエストを処理します。

smmon

認証サーバ、許可サーバ、および Web エージェントを監視する OneView モニタです。

Windows システムでのポリシー サーバ サービスの開始と終了

Windows システムでポリシー サーバ サービスを開始または終了する方法

- 管理コンソールの[ステータス]タブで、[開始]ボタンまたは[停止]ボタンをクリックします。
- Windows の[スタート]-[設定]-[コントロール パネル]-[サービス]の順にクリックすると表示される[Windows サービス]ダイアログ ボックスを使用します。ポリシー サーバプロセスを起動または終了すると、関連するエグゼクティブも起動または終了します。
- smpolicysrv を使用すると、コマンド ラインからポリシー サーバを停止できます。

  ```
  installation_path¥siteminder¥bin¥smpolicysrv -stop
  ```

注: Windows システムでは、リモート デスクトップまたはターミナル サービス ウィンドウから smpolicysr コマンドを実行しないでください。smpolicysrv コマンドはプロセス間通信に依存します。この通信は、リモート デスクトップまたは[ターミナル サービス]ウィンドウから smpolicysrv プロセスを実行した場合には機能しません。

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

UNIX システムでのポリシー サーバ プロセスの開始と終了

UNIX システムでポリシー サーバのプロセスを開始または終了するには、次のいずれかの操作を行います。

- 管理コンソールの[ステータス]タブで、対応する[開始]ボタンまたは[停止]ボタンをクリックします。
- 用意されているスクリプトを使用します。ポリシー サーバプロセスの起動と終了には、2 つのスクリプトが用意されています。ポリシー サーバプロセスが再起動されないように、これらのスクリプトによって UNIX エグゼクティブも終了されます。

  ```
  installation_path/siteminder/start-all
  installation_path/siteminder/stop-all
  ```

さらに、次のスクリプトをポリシー サーバ プロセスの起動と終了に使用できます。スクリプトを実行したときに UNIX エグゼクティブが起動されていなかった場合は、プロセスだけでなくエグゼクティブも起動されます。また、スクリプトは、以下のような同じコマンド ライン オプションで呼び出せます。

installation_path/siteminder/smpolsrv

コマンドラインオプション:

-stop

プロセスを終了します。

-start

プロセスを起動します。

-status

プロセスが起動されているかどうかを示します。

ポリシー サーバは、UNIX エグゼクティブの全アクティビティのログを *installation_directory*/log/smexec.log ファイルに記録します。ログのエントリは、常に既存のログファイルに追加されます。

ポリシー サーバ シャットダウン中のスレッド終了ウィンドウ

デフォルトでは、ポリシー サーバは、シャットダウンする前にすべてのスレッドの終了を 3 分間待機します。スレッドのいずれかが終了しない場合でも、ポリシー サーバは終了します。

レジストリ キーを作成することによって、ポリシー サーバがスレッドの終了を待機する最大の時間を変更することができます。

レジストリ キーを作成する方法

1. ポリシー サーバ ホスト システムにアクセスし、以下のいずれかを実行します。
   - (Windows) レジストリ エディタを開き、HKEY_LOCAL_MACHINE¥Software¥Netegrity¥SiteMinder¥CurrentVersion¥PolicyServer に移動します。
   - (UNIX) sm.registry ファイルを開きます。このファイルのデフォルトの場所は *siteminder_home*/registry です。

     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. MaxShutDownTime を作成し、レジストリ値のタイプは REG_DWORD にします。

   測定単位: 秒

   デフォルト値: 180

   最小値: 30

   最大値: 1800
3. 以下のいずれかの操作を行います。
   - (Windows) レジストリ エディタを終了します。
   - (UNIX) sm.registry ファイルを保存します。
4. ポリシー サーバを再起動します。

重要: シャットダウン中にポリシー サーバ スレッドが適切に終了しない場合は、SiteMinder サポートにお問い合わせください。

ポリシー サーバ エグゼクティブの設定

UNIX や Windows にポリシー サーバをインストールする場合、1 つまたは複数のエグゼクティブ アプリケーションによってポリシー サーバ プロセスのステータスが監視され、エラーが発生したプロセスは自動的に再起動されます。以下のセクションでは、お使いのプラットフォームに基づいてポリシー サーバ プロセスを開始および停止する方法、UNIX と Windows の実行ファイルを設定、無効化、有効化する方法について説明します。

Windows エグゼクティブの設定

Windows では、各ポリシー サーバプロセスは別々のエグゼクティブで監視されます。それぞれのエグゼクティブは、*Policy_Server_installation_path*¥config¥siteminder.conf 設定ファイルから、次のしきい値を読み込みます。

SMEXEC_UPTIME_THRESHOLD

ポリシー サーバ サービスの起動後、頻繁にエラーが発生するため関連するエグゼクティブが監視を停止するまでの間、ポリシー サーバ サービスを実行する必要最小時間を秒単位で指定します。このパラメータのデフォルト値は 60 秒です。

SMEXEC_RESTART_THRESHOLD

SMEXEC_UPTIME_THRESHOLD パラメータで指定した時間内に、エグゼクティブがサービスの再起動を試行する回数の最大値を指定します。このパラメータで指定した回数を超えるエラーがサービスで発生した場合、エグゼクティブはサービスの再起動を中止します。この試行回数のパラメータのデフォルト値は 5 回です。

しきい値パラメータを変更するには、siteminder.conf ファイルを編集し、ポリシー サーバ プロセスを再起動してください。

UNIX エグゼクティブの設定

UNIX では、ポリシー サーバプロセスと状態監視プロセスが 1 つのエグゼクティブで監視されます。エグゼクティブは、次の設定ファイルから設定を読み込みます。

installation_path/config/siteminder.conf

このファイルを編集すると、次の設定を変更できます。

POLICYSERVER_ENABLED

エグゼクティブの実行開始時の、ポリシー サーバ プロセスのステータスを指定します。エグゼクティブの起動時にプロセスを有効にするには、このパラメータを「YES」に設定します。

MONITOR_ENABLED

エグゼクティブの実行開始時の、状態監視プロセスのステータスを指定します。エグゼクティブの起動時にプロセスを有効にするには、このパラメータを「YES」に設定します。

SMEXEC_UPTIME_THRESHOLD

ポリシー サーバ サービスの起動後、頻繁にエラーが発生するため関連するエグゼクティブが監視を停止するまでの間、ポリシー サーバ サービスを実行する必要最小時間を秒単位で指定します。このパラメータのデフォルト値は 60 秒です。

SMEXEC_RESTART_THRESHOLD

SMEXEC_UPTIME_THRESHOLD パラメータで指定した時間内に、エグゼクティブがサービスの再起動を試行する回数の最大値を指定します。このパラメータで指定した回数を超えるエラーがサービスで発生した場合、エグゼクティブはサービスの再起動を中止します。この試行回数のパラメータのデフォルト値は 5 回です。

UNIX エグゼクティブのパラメータを変更する方法

1. *installation_path*/config/siteminder.conf ファイルを編集します。
2. コマンドラインで、次のスクリプトを実行します。

   ```
   installation_path/siteminder/bin/stop-all
   ```

   ポリシー サーバ プロセスが終了します。
3. コマンドラインで、次のスクリプトを実行します。

   ```
   installation_path/siteminder/bin/start-all
   ```

   UNIX エグゼクティブが、siteminder.conf ファイルの新しい設定を使用して再起動されます。

第 3 章: ポリシー サーバのデータ ストレージ オプションの設定

このセクションには、以下のトピックが含まれています。

データ ストレージ オプション設定の概要

管理コンソールの[データ]タブでは、ポリシー サーバのデータベース(ポリシー ストア、キー ストア、監査ログ)の格納場所を設定できます。

ポリシー サーバのデータ ストレージを設定する方法

1. ポリシーサーバー管理コンソールを起動します。

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

2. [データ]タブをクリックします。

   注: このタブ上での設定およびコントロールの詳細については、[ヘルプ]-[管理コンソール ヘルプ]をクリックしてください。

3. 設定するデータベースを[データベース]ドロップダウン リストから選択します。選択するデータベースによって、そのデータベース タイプで使用できるストレージ機能が決まり、[ストレージ]ドロップダウン リストに示されます。

   注: この手順の最後に示される表には、設定できるデータベースと、各データベースで使用できるストレージ オプションがリスト表示されます。これらの設定の組み合わせによって、その下方に示されるコンテキスト依存グループ ボックスに表示される設定項目が変化します。

4. 選択したデータベースのストレージ タイプを[ストレージ]ドロップダウン リストから選択します。

5. [データベース]および[ストレージ]のコントロールの下にあるコンテキスト依存グループ ボックスで、選択したポリシー サーバ データベースのデータ ストレージ オプションを設定します。

6. 設定が完了したら、[適用]をクリックして設定を保存するか、[OK]をクリックして設定を保存し、管理コンソールを終了します。

以下の表に、SiteMinder データベースのタイプと、各タイプで使用できるストレージ オプションを示します。

データベース	データベースの説明	使用可能なストレージ
ポリシーストア	ポリシーストアのデータベース。ポリシー ストア データベースは、*必ず*指定してください。	LDAP ODBC
キーストア	SiteMinder エージェントによって作成された cookie の暗号化に使用するキーを格納するデータベース。	LDAP ODBC
監査ログ	イベント情報を含む監査ログを保存するデータベース。	ODBC テキストファイル
セッション サーバ	セッション サーバが永続セッションデータを保存するデータベース。	ODBC

ポリシー ストア データベースの設定

ポリシー ストアは、すべてのポリシー サーバ オブジェクトが格納されるデータベースです。

ポリシー ストア データベースを設定する方法

1. [データベース]ドロップダウンリストから[ポリシーストア]を選択します。
2. 使用可能なストレージタイプ(LDAP または ODBC)を[ストレージ]ドロップダウンリストから選択します。
3. 選択したストレージ タイプに合わせてストレージ オプションを指定します。
4. [適用]をクリックして設定を保存するか、[OK]をクリックして設定を保存し、コンソールを終了します。
5. (オプション)ポリシー ストア データベースのストレージ タイプを LDAP に変更し、そのポリシー ストアをキー ストアとして使用する場合は、「ポリシー ストア データベースを使用するためのキー ストアまたは監査ログの設定 (P. 31)」で説明されている手順に従います。

   注: LDAP 対応のポリシー ストアと通信するポリシー サーバが 1 台以上ある場合は、各ポリシー サーバ システムの管理コンソールの設定を同じにする必要があります。

詳細情報:

LDAP ストレージ オプションの設定 (P. 35)

ポリシー ストア データベースを使用するためのキー ストアまたは監査ログの設定

ポリシーストアを設定した後、任意でデータベースを設定できます。ポリシー ストアが互換ストレージ タイプの場合(つまり、ポリシー ストアを、他のデータベースにも有効なストレージ オプションであるデータベースに格納されるように設定している場合)、ポリシー ストア データベースを使用して以下を保持するように、ポリシー サーバを設定できます。

- キーストア
- 監査ログ

重要: LDAP データベースをポリシー ストアとして使用している場合は、ポリシー ストア データベースを監査ログに使用しないでください。監査ログは LDAP データベースに書き込むことができません。SiteMinder サンプル データ ソース (SmSampleUsers) をポリシー ストアとして使用している場合は、ポリシー ストア データベースを監査ログに使用しないでください。監査ログは、このサンプル ポリシー ストアではサポートされていません。

別のデータベースがポリシー ストア データベースに格納されるように設定するには、[ポリシー ストアを使用]オプションをオンにします。このオプションは、[データベース]ドロップダウン リストからポリシー ストア以外のデータベースを選択すると、[データベース]ドロップダウン リストとストレージ オプション領域の間に表示されます。

[ポリシーストアを使用]オプションをオンにすると、[ストレージ]ドロップダウンリストとコンテキスト依存型のストレージ オプションが淡色表示になります。

キーストア用の個別のデータベースの設定

キー ストアは、SiteMinder エージェントによって作成された cookie の暗号化に使用するキーをポリシー サーバが格納する場所です。

キー ストア用の個別のデータベースを設定する方法

1. [データベース]ドロップダウンリストから、[キーストア]を選択します。
2. [ストレージ]ドロップダウンリストから、使用可能なストレージタイプ ([LDAP] または[ODBC]) を選択します。

   注: ポリシー サーバは、LDAP/ODBC 混合のポリシー ストアとキー ストアをサポートしています。ポリシー ストアは ODBC データベースに格納でき、キー ストアは LDAP ディレクトリ サーバに格納できます。また、その逆も可能です。サポートされているデータベースのリストについては、テクニカル サポート サイトにある SiteMinder プラットフォーム マトリックスを参照してください。
3. 選択したストレージ タイプに合わせてストレージ オプションを指定します。
4. [適用]をクリックして設定を保存するか、[OK]をクリックして設定を保存し、コンソールを終了します。

監査ログ用の個別のデータベースの設定

監査ログ データベースは、イベント情報を含む監査ログをポリシー サーバが格納する場所です。これらの設定によってポリシー サーバのパフォーマンスが低下する場合があります。パフォーマンスの低下が問題となる場合は、監査データをデータベースではなくテキスト ファイルに記録するように設定します。

監査ログ用の個別のデータベースを設定する方法

1. [データベース]ドロップダウンリストから[監査ログ]を選択します。
2. 使用可能なストレージタイプ(ODBC または テキスト ファイル)を[ストレージ]ドロップダウンリストから選択します。
3. 選択したストレージ タイプに合わせてストレージ オプションを指定します。
4. [適用]をクリックして設定を保存するか、[OK]をクリックして設定を保存し、コンソールを終了します。

ポリシー サーバの監査ログの格納先を ODBC データベースまたはテキスト ファイルのどちらにするかを決定するときは、以下の要素を考慮する必要があります。

- SiteMinder レポートでは、監査ログが ODBC データベースに書き込まれる必要があります。監査ログがテキストファイルに書き込まれる場合は、レポート機能を使用できません。
- ODBC データベースおよびテキスト ファイルへの SiteMinder 監査ロギングでは、国際化(I18N)がサポートされます。
- デフォルトでは、ポリシー ストア オブジェクトへの SiteMinder 管理者変更は監査データベースに書き込まれません。これらの変更は、デフォルトで、siteminder_home¥audit にあるテキスト ファイルのセットに書き込まれます。この情報は監査データベースには書き込まれませんが、レポート内にこれらのイベントを含めるよう SiteMinder を設定できます。
- ポリシー サーバが高負荷環境で稼働される場合は、ODBC データベースではなく、テキスト ファイルにログを記録することを検討してください。ただし、ODBC データベースにログを記録する場合は、高負荷環境で監査データが失われないようにするため、HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥CurrentVersion¥Database¥ で以下のレジストリ キー値を設定する必要があります。

ConnectionHangwaitTime

高負荷用に 60 秒に設定します。デフォルトは 30 秒です。

QueryTimeout

高負荷用に 30 秒に設定します。デフォルトは 15 秒です。

LoginTimeout

高負荷用に 30 秒に設定します。デフォルトは 15 秒です。

注: ConnectionHangwaitTime の値は常に、QueryTimeout と LoginTimeout の値の 2 倍以上である必要があります。

詳細情報:

ポリシー ストア オブジェクトに対して管理者が行った変更の記録 (P. 84)
SiteMinder 管理監査イベントをレポートに含める方法 (P. 87)

セッション サーバ用のデータベースの設定

セッション サーバ データベースは、ポリシー サーバのセッション サーバが永続セッション データを格納する場所です。

セッション サーバ用の個別のデータベースを設定する方法

1. [データベース]ドロップダウンリストから、[セッション サーバ]を選択します。
2. [ストレージ]ドロップダウンリストから、使用可能なストレージ タイプを選択します。
3. [セッション サーバの有効化]オプションをオンにします。

   1 つまたは複数のレルムで永続セッションを使用する予定がある場合にのみ、セッション サーバを有効にしてください。セッション サーバを有効にすると、ポリシー サーバのパフォーマンスが低下します。

   注: [ポリシー ストアを使用]チェック ボックスはオフになります。パフォーマンス上の理由から、セッション サーバをポリシーストアと同じデータベース上で動作させることはできません。
4. 選択したストレージ タイプに合わせてストレージ オプションを指定します。
5. [OK]をクリックして設定を保存し、コンソールを終了します。

高負荷環境でのセッション サーバ タイムアウトの設定

過度の高負荷環境では、アイドル タイムアウトしたセッションや期限切れになったセッションの削除など、セッション サーバの保守タスクに必要な、実行時間の長いクエリがタイムアウトになる可能性があります。保守スレッドによってタスクが正常に実行されるようにするには、MaintenanceQueryTimeout レジストリ設定の値を増やしてセッション サーバの保守タスクのタイムアウトを調整します（デフォルトでは 60 秒）。MaintenanceQueryTimeout レジストリ設定は次の場所にあります。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥CurrentVersion¥
SessionServer
```

LDAP ストレージ オプションの設定

コンテキスト依存型の LDAP ストレージ制御機能を使用すると、ポリシー情報を格納するポリシー ストアとして使用する LDAP ディレクトリや、キー ストアとして使用する LDAP ディレクトリを指定できます。

注: LDAP データベースに関するパラメータを更新する場合は、必ず、ポリシー サーバを再起動して新しいパラメータを有効にしてください。

LDAP データベースの設定

LDAP データベースを設定する方法

1. [LDAP IP アドレス]フィールドで、LDAP サーバのサーバ名または IP アドレスを指定します。パフォーマンス上の理由から、IP アドレスを入力することをお勧めします。

   注: LDAP サーバをフェイルオーバー構成にするために、このフィールドには複数のサーバを指定することができます。

2. [ルート DN]フィールドで、SiteMinder スキーマを配下に持つ LDAP ブランチを指定します（o=myorg.org など）。

3. ポリシー サーバが SSL を介して LDAP ディレクトリと通信する場合は、[SSL を使用]チェック ボックスをオンにします。

   注: このオプションをオンにした場合は、[Netscape 証明書データベース ファイル]フィールドで証明書データベースを指定する必要があります。

4. [管理ユーザ名]フィールドで、LDAP ディレクトリ管理者の DN を指定します (cn=Directory Manager など)。
5. [管理者のパスワード]フィールドに、LDAP ディレクトリの管理パスワードを入力します。
6. [パスワードの確認入力]フィールドで、LDAP ディレクトリの管理パスワードを確認します。
7. [LDAP 接続のテスト] をクリックして、入力したパラメータが正しいかどうか、および接続が作成できたかどうかを確認します。

LDAP フェイルオーバーの設定

複数の LDAP ディレクトリを使用する場合、ディレクトリをフェイルオーバー構成に設定できます。フェイルオーバーを有効にするには、[LDAP IP アドレス] フィールドに LDAP サーバの IP アドレスとポート番号を入力します。LDAP サーバのアドレスは、それぞれスペース (空白) で区切って入力します。サーバごとに固有のポートを指定できます。使用している LDAP サーバが標準ポート以外のポート (SSL 以外は 389、SSL は 636) で稼働している場合、コロン (「:」) を区切り文字として使用し、最後に指定されているサーバの IP アドレスにポート番号を追加します。たとえば、サーバがポート 511 とポート 512 で稼働している場合は、次のように入力できます。

```
123.123.12.11:511 123.123.12.22:512
```

ポート 511 の LDAP サーバ 123.123.12.11 がリクエストに応答しない場合、リクエストは自動的にポート 512 の 123.123.12.22 に渡されます。

使用しているすべての LDAP サーバが同じポートで稼働している場合は、最後に指定されているサーバの後ろにポート番号を追加できます。たとえば、サーバがポート 511 で稼働している場合は、次のように入力できます。

```
123.123.12.11 123.123.12.22:511
```

拡張 LDAP リフェラル処理の設定

SiteMinder の LDAP リフェラル処理は強化され、パフォーマンスと冗長性が向上しました。旧バージョンの SiteMinder がサポートしていたのは、LDAP SDK 層による自動 LDAP リフェラル処理でした。LDAP リフェラルが発生すると、これまでは LDAP SDK 層が、参照先サーバへのリクエストの実行を、ポリシー サーバと通信せずに処理していました。

現行バージョンの SiteMinder は、非自動（拡張） LDAP リフェラル処理をサポートしています。非自動リフェラル処理では、LDAP リフェラルは、LDAP SDK 層ではなくポリシー サーバに返されます。リフェラルには、リフェラルの処理に必要なすべての情報が含まれています。ポリシー サーバは、リフェラルで指定されている LDAP ディレクトリが使用できるかどうかを調べて、該当する LDAP ディレクトリが機能していない場合は、リクエストを中断させることができます。この機能により、オフラインのシステムへの LDAP リフェラルによってリクエスト待ち時間が恒常的に増加することによるパフォーマンスの低下が解消されます。このような待ち時間の増加は、SiteMinder でリクエストの飽和状態を発生させることがあります。

LDAP リフェラル処理を設定する方法

1. ポリシー サーバ管理コンソールを開きます。

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

2. ［データ］タブを選択します。

   機能強化型リフェラルの有効化

   このチェック ボックスをオンにすると、LDAP SDK 層による LDAP リフェラル処理を有効にせずに、ポリシー サーバで LDAP リフェラルの機能強化処理を実行できるようになります。

   最大引用ホップ数

   元のリクエストの処理試行で許可する連続リフェラルの最大数を指定します。リフェラルは、追加のリフェラルを必要とする位置を示すことができるため、この制限は、不適切な複製設定によってリフェラルループが発生するような場合に役立ちます。

3. 必要に応じて、値を変更します。
4. ポリシー サーバを再起動します。

大きな LDAP ポリシー ストアのサポートの設定

LDAP ポリシー ストアが大きいと、管理 UI のパフォーマンスに問題が生じる可能性があります。

そのような問題を防ぐため、以下の 2 つのレジストリ設定の値を変更できます。

Max AdmComm Buffer Size

管理 UI のバッファ サイズを指定します（具体的には、ポリシー サーバから管理 UI に渡されるデータの 1 パケットあたりの最大データ量をバイト単位で表したもの）。

Max AdmComm Buffer Size レジストリ設定は、次の場所で行う必要があります。

HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥CurrentVersion¥PolicyServ¥

大きなバッファを割り当てると全体的なパフォーマンスが低下するため、この値を設定するときは最大の注意を払ってください。Max AdmComm Buffer Size の指定可能範囲は 256 KB ～ 2 GB です。デフォルト値は 256 KB です（このレジストリ設定が存在しない場合も適用されます）。

SearchTimeout

LDAP ポリシー ストアの検索タイムアウトを秒単位で指定します。

SearchTimeout レジストリ設定は、次の場所で行う必要があります。

HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥CurrentVersion¥LdapPolicyStore¥SearchTimeout

この設定の適切な値は、ネットワーク速度、LDAP 検索クエリ レスポンスのサイズ、LDAP 接続の状態、LDAP サーバの負荷など、さまざまな要因によって変化します。LDAP サーバから大量のポリシー ストア データをフェッチするときに LDAP タイムアウトが発生しない程度の大きな値にする必要があります。デフォルト値は 20 秒です（このレジストリ設定が存在しない場合も適用されます）。

ODBC ストレージ オプションの設定

コンテキスト依存型ストレージ オプションの ODBC ストレージ制御機能を使用すると、ODBC データソースを設定して、ポリシー ストア、キー ストア、監査ログ、トークン データ、またはセッション サーバ データを保存することができます。

注: ODBC データ ソースのインストールの詳細については、「*ポリシー サーバ インストール ガイド*」を参照してください。

ODBC データソースの設定

ODBC データソースを設定する方法

1. [データ ソース情報]フィールドで、ODBC データ ソースの名前を指定します。このフィールドには、ODBC フェイルオーバーを有効にする複数のデータ ソースの名前を入力できます。

   データ ソース情報

   ODBC データソースの名前を入力します。このフィールドには、フェイルオーバーを有効にする複数のデータ ソースの名前を入力できます。

   ユーザ名

   必要に応じて、そのデータベースにアクセスするすべての権限を付与されたデータベースアカウントのユーザ名を入力します。

   パスワード

   データベースアカウントのパスワードを入力します。

   パスワードの確認

   確認のために、データベースアカウントのパスワードをもう一度入力します。

   最大接続数

   同時に使用できる、データベースごとの ODBC 接続の最大数を入力します。

2. [ODBC 接続のテスト]をクリックして、入力したパラメータが正しいかどうか、および接続が作成できたかどうかを確認します。

ODBC フェイルオーバーの設定

複数の ODBC データソースを使用していて、フェイルオーバーを設定する場合は、データソース名をカンマで区切って[データソース情報]フィールドに入力します。たとえば、[データソース名]フィールドに「SiteMinder Data Source1,SiteMinder Data Source2」と入力すると、ポリシー サーバは Data Source1 を最初に検索します。SiteMinder Data Source1 が応答しない場合は、自動的に SiteMinder Data Source2 を検索します。

注: 上記の方法を使用して、ポリシー ストア、キー ストア、セッション ストア、監査ログとして使用されているデータ ソースのフェイルオーバーを設定できます。

SQL クエリによって返されるレコードの最大数の設定

多くのレコード数を返す SQL クエリによって、ポリシー サーバがハングまたはクラッシュする場合があります。この状況を管理するため、返されるレコードの数が指定した最大値を超過した場合に SMPS ログに警告メッセージを出力することができます。

最大数を設定するには、レジストリ キー MaxResults を追加して、その値を 1 以上に設定します。クエリによって返されるレコードの数が MaxResults によって指定された上限値以上である場合、ポリシー サーバは警告を SMPS ログに出力します。MaxResults がゼロに設定されるか定義されなかった場合、警告メッセージは出力されません。

レジストリ キー MaxResults を追加しても、返されるレコードの数が変更されるわけではありません。このキーを追加することによって、結果の数が指定した上限を超えた場合にユーザに警告されます。このフィードバックを使用して、必要に応じて SQL クエリを修正し、返されるレコードの数を調整できます。

SQL クエリによって返されるレコード数の制限を設定する方法

1. レジストリ キー MaxResults を手動で追加します。

   Windows

   レジストリ キー MaxResults を以下の場所に追加します。

   ```
   HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥CurrentVersion¥Ds
   ¥ODBCProvider
   ```

Solaris

以下の行を sm.registry ファイルに追加します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥CurrentVersion¥Ds
¥ODBCProvider=35921
MaxResults=0x1; REG_DWORD
```

2. MaxResults に 1 以上の値を割り当てます。

テキスト ファイル ストレージ オプションの設定

テキスト ファイル ストレージ オプションを使用すると、ポリシー ストア監査ログの格納先となるテキスト ファイルを設定できます。

テキスト ファイルを指定するには、[ファイル名]フィールドにファイルのフル パスを入力するか、[参照]ボタンをクリックして必要なディレクトリを参照し、希望するファイルをクリックするか、そのファイルの名前を入力します。

ODBC の監査データ インポート ツール

ポリシー サーバは、監査データを ODBC データベースに格納したり、ファイルに出力したりできます。smauditimport ツールは、SiteMinder 監査データのテキスト ファイルを読み取り、5.x または 6.x 方式を使用して監査ストアとして設定されている ODBC データベースにデータをインポートします。

また、認証、許可、および管理データを、ODBC データベース内の対応するテーブルにインポートします。ODBC データベースに正常にインポートされた行の数はログに記録されます。また、正常にインポートされたテキスト ファイルの行ごとに、先頭文字の「[」がシャープ記号「#」に置き換えられます。ODBC データベースにインポートできない行については、その行番号がログに記録されます。

smauditimport ツールは同じファイルに対して何回でも実行できます。このツールは、ODBC データベースに正常にインポートされなかった行、または左角かっこ[「[」で始まる行を処理するだけです。テキスト ファイルを元の形式に復元するには、すべての行の先頭文字を左角かっこ「[」に置き換えます。

注: SiteMinder の一部のドキュメントでは、「監査」と「ロギング」という用語はほとんど同じ意味で使われています。

テキスト ファイルへのより多くの監査データ ログの記録

ポリシー サーバはデフォルトで、監査データ ログをテキスト ファイルよりも ODBC データベースに多く記録します。デフォルトより多くの監査データ ログをテキスト ファイルに記録することで、ODBC データベースのデータ量に合わせることができます。そのためには、レジストリ キー "Enable Enhance Tracing" を追加し、その値を 1 に設定します。"Enable Enhance Tracing" を無効にするには、値をゼロ (デフォルト) に設定します。

テキスト ファイルにより多くの監査データ ログを記録する方法

1. レジストリ キー "Enable Enhance Tracing" を手動で追加します。

   Windows

   以下のキーを追加します。

   ```
   TYPE=DWORD
   ¥netegrity¥SiteMinder¥CurrentVersion¥Reports
   ¥"Enable Enhance Tracing"
   ```

   Solaris

   以下の手順に従います。

   a. ファイル .../siteminder/registry/sm.registry を開きます。.

   b. 以下の行を検索します。

   ```
   HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder
   ¥CurrentVersion¥Reports=25089
   ```

   c. この行の下に、以下を追加します。

   ```
   "Enable Enhance Tracing"=0x1;    REG_DWORD
   ```

   d. ファイルを保存して閉じます。

2. "Enable Enhance Tracing" を 1 に設定します。

注: "Enable Enhance Tracing" の値は、Entitlement Management Services (EMS) イベントのログ記録には影響しません。

ODBC の監査データ インポートの前提条件

smauditimport ツールを実行する前に、以下の前提条件が満たされていることを確認してください。

- ポリシー サーバが Windows、Solaris、または Linux オペレーティング環境にインストールされている。

  注: Solaris および Linux プラットフォームの場合は、smauditimport ツールを実行する前に nete_ps_env.ksh を実行します。

- ODBC データベースが 5.x または 6.x 方式で監査(ログ)ストアとして設定されている。

  注: ODBC データベースを監査(ロギング)ストアとして設定する方法の詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

- レジストリ キー "Enable Enhance Tracing" が 1 に設定されている。

ODBC データベースへの監査データのインポート

smauditimport ツールは、SiteMinder 監査データ テキスト ファイルを読み取り、ODBC データベースにインポートします。このツールは、ポリシー サーバ インストール ディレクトリ下の ¥bin ディレクトリ内にあります。

重要: 監査データを ODBC データベースにインポートする前に、SiteMinder 5.x または 6.x 方式でデータベースを監査ストアとして設定する必要があります。SiteMinder スキーマを使用して ODBC データベースを設定する方法の詳細については、「ポリシー サーバ インストール ガイド」を参照してください。

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

ODBC データベースに監査データをインポートする方法

1. ポリシー サーバがインストールされているコンピュータで、*siteminder_installation*¥bin に移動します。

   siteminder_installation

   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。

   smauditimport *audit_file dsn user_name user_password* -f -v -b*bulk_load_size* -s5 | -s6

   audit_file

   監査データを含むテキスト ファイルのパスと名前を指定します。

   注: smauditimport ツールでは、監査データ テキスト ファイルの完全パス名を指定する必要があります。

   dsn

   ODBC データベースのデータ ソース名 (DSN) を指定します。

   user_name

   ODBC データベース管理者の名前を指定します。

   user_password

   ODBC データベース管理者のパスワードを指定します。

   -f

   (オプション) 監査データのインポート中にエラーが発生した場合に、行番号をログに記録し、処理を続行します。

   デフォルト: -f オプションを指定しない場合、行番号をログに記録しますが、処理を停止します。

   -v

   (オプション) テキスト ファイル内のフィールドの数、数値フィールドの値が指定の範囲内にあるかどうか、およびデータベースへの接続を検証し、エラーを出力します。

   注: smauditimport ツールを検証モードで実行するとき、データはデータベースにインポートされません。

   -b bulk_load_size

   (オプション) 読み取って ODBC データベースにインポートする行の数を指定します。

   デフォルト: 100

-s5 | -s6

(オプション) 5.x または 6.x 方式のいずれかで監査ストアとして設定された ODBC データベースをサポートします。

デフォルト: 6.x 方式で監査ストアとして設定された ODBC データベースをサポートします。

Netscape 証明書データベース ファイルの指定

LDAP ディレクトリを使用して、SSL 接続を介してポリシーやユーザ情報を保存している場合は、ポリシー サーバに、Netscape 証明書データベースファイルが含まれているディレクトリを示す必要があります。ディレクトリには、cert7.db ファイルと key3.db ファイルが含まれていなければなりません。

証明書データベース ファイルをインストールする前に、そのコピーを作ります。オリジナル ファイルの代わりにコピーしたファイルを使用してください。また、現在 Netscape Communicator で cert7.db が使用されている場合には、その使用を中止してください。

[Netscape 証明書データベースファイル] フィールドに証明書データベースの名前を入力するか、ディレクトリツリーを検索して保存先のデータベースを選択します。このフィールドには、Active Directory ネームスペースを使用して 管理 UI 内で設定される AD ユーザ ストアの値を入力する必要はありません。SSL 接続を確立する場合、AD ユーザ ストアではネイティブの Windows 証明書リポジトリが使用されます。

第 4 章: ポリシー サーバの一般的な設定

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 サーバの設定の概要

ポリシー サーバでは、その動作と実行の方法を決定するための多くの一般的な設定を、管理コンソールの[設定]タブで行うことができます。

- アクセス制御用の TCP ポート
- TCP ポートなどの管理設定と、アクティブでない状態時のタイムアウト
- 接続の設定
- RADIUS 設定
- パフォーマンスの設定
- OneView モニタの設定

ポリシー サーバの設定

ポリシー サーバの一般的な設定方法

1. ポリシーサーバー管理コンソールを起動します。

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

2. [設定]タブをクリックします。

   注: このタブ上での設定およびコントロールの詳細については、[ヘルプ]-[管理コンソール ヘルプ]をクリックしてください。

3. 希望する設定を調整します。
4. 設定が完了したら、[適用]をクリックして設定を保存するか、[OK]をクリックして設定を保存し、管理コンソールを終了します。

アクセス制御の設定

ポリシー サーバは、認証、許可、およびアカウンティングの目的で SiteMinder エージェントと通信する際に 3 つの異なる TCP ポートを使用します。

これらのエージェント通信ポートを有効または無効にしたり、各機能で使用する TCP ポートの番号を変更したりするには、[管理コンソールの設定]タブの[アクセス制御]グループ ボックスにあるコントロールを使用します。

ポリシー サーバ管理の設定

ポリシー サーバは、ブラウザベースのポリシー管理を可能にするため、TCP ポートを使用して 管理 UI と通信します。

管理 UI との通信で使用する TCP ポート番号を有効化、無効化、または変更したり、管理がアクティブでないときのタイムアウト値を指定したりするには、[管理コンソールの設定]タブの[管理]グループ ボックスにあるコントロールを使用します。

ポリシー サーバの接続オプションの設定

ポリシー サーバ スレッドの最大数と、ポリシー サーバへの接続のアイドル タイムアウトを指定するには、[管理コンソールの設定]タブの[接続オプション]グループ ボックスにあるコントロールを使用します。

ポリシー サーバのパフォーマンスの設定

ポリシー サーバのパフォーマンスを調整するキャッシュとスレッドを設定するには、[管理コンソールの設定]タブの[パフォーマンス]グループ ボックスを使用します。

RADIUS の設定

環境内の RADIUS コンポーネントのサポートを有効にする設定を指定するには、[管理コンソールの設定]タブの[RADIUS]グループ ボックスを使用します。

OneView モニタの設定

OneView モニタはデフォルトで、監視対象となるポリシー サーバ上でローカルに実行されます。

リモートで監視される他のポリシー サーバからの接続を受け入れるようにモニタを設定したり、クラスタ内のすべてのポリシー サーバを監視する集中監視用のリモート ポリシー サーバを指定したりするには、[管理コンソールの設定]タブの[OneView モニタ]グループ ボックスを使用します。

SiteMinder ポリシー データ同期の再スケジュール

SiteMinder は、XPSSweeper ツールを使用してポリシー データを自動的に同期します。このツールの実行頻度を変更するには、以下のパラメータを設定します。

AutosweepSchedule

XPSSweeper プロセスを実行する日と時刻(時間と分)を指定します。

デフォルト: 月曜日の 08:30

制限: 24 時間形式の GMT タイム ゾーン。エントリが複数ある場合は、カンマまたは空白で区切ります。

例: Mon@13:30,Tue@14:00

注: SiteMinder バイナリ ファイル(XPS.dll、libXPS.so、libXPS.sl)への書き込みアクセス許可がユーザに*ない* 場合は、管理者が 管理 UI または XPSSecurity ツールを使用して、関連する XPS コマンド ライン ツールを使用する権限を付与する必要があります。

SiteMinder データベースの同期を再スケジュールする方法

1. ポリシー サーバでコマンド ラインを開き、以下のコマンドを入力します。

   ```
   xpsconfig
   ```

   ツールが起動し、このセッションのログ ファイルの名前が表示されます。また、選択項目のメニューが開きます。

2. 次のコマンドを入力します。

   ```
   xps
   ```

   オプションのリストが表示されます。

3. 次のコマンドを入力します。

   ```
   8 (AutosweepSchedule)
   ```

   XPSSweeper ツールの現在のスケジュールが表示されます。

4. 「C」と入力し、希望する日付と時刻を入力します。複数の日付または時刻を入力する場合は、それらをカンマまたは空白で区切ります。以下の形式を使用します。

   ```
   Mon@13:30,Tue@14:00
   ```

   新しい設定と古い設定が表示されます。追加した値は「保留中の値」として設定の下に表示されます。

5. 以下の手順を実行します。

   a. 2 回「Q」と入力します。

   b. 「L」と入力します。

   c. 「Q」と入力して XPS セッションを終了します。

   変更が保存され、コマンド プロンプトが表示されます。

第 5 章: ポリシー サーバのスーパーユーザ パスワードの変更

このセクションには、以下のトピックが含まれています。

スーパーユーザ パスワードの概要

スーパーユーザとは、ポリシー サーバのインストール処理で自動的に設定される管理者アカウントです。スーパーユーザのパスワードは管理コンソールの[スーパーユーザ]タブから変更できます。

注: 以前に 管理 UI を使用してスーパーユーザを無効にした場合は、このダイアログ ボックスの[スーパーユーザ アカウント]グループ ボックスでパスワードを変更しても、スーパーユーザは有効になりません。

ポリシー サーバのスーパーユーザ パスワードの変更

スーパーユーザ アカウントのパスワードを変更する方法

1. ポリシーサーバー管理コンソールを起動します。

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

2. [スーパーユーザ]タブをクリックします。

   注: このタブ上での設定およびコントロールの詳細については、[ヘルプ]-[管理コンソール ヘルプ]をクリックしてください。

3. [古いパスワード]フィールドに、スーパーユーザの現在のパスワードを入力します。

4. [新しいパスワード]フィールドに、スーパーユーザの新しいパスワードを入力します。

   注: SiteMinder のスーパーユーザ管理者のパスワードには、パイプ記号(「|」)や不等号記号(「>」または「<」)は使用できません。

5. [パスワードの確認入力]フィールドに、新しいパスワードをもう一度入力します。

6. [適用]をクリックしてスーパーユーザに対する変更を保存するか、[OK]をクリックして設定を保存し、コンソールを終了します。

   注: スーパーユーザ アカウントのパスワードの変更は、ポリシー サーバ プロセスを再起動しなくても有効になります。

第 6 章: 暗号化キーの設定と管理

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 サーバの暗号化キーの概要

ポリシー サーバとエージェントは、暗号化キーを使用して、SiteMinder 環境のポリシー サーバとエージェントの間で転送される重要なデータの暗号化と復号化を行います。

- エージェント キーは、シングル サインオン環境のすべてのエージェントが読み込む SiteMinder cookie を暗号化するために使用されます。各エージェントは、他のエージェントによって暗号化された cookie を復号化する必要があるため、シングル サインオン環境のすべてのエージェントがエージェント キーを共有します。エージェント キーは、ポリシー サーバによって管理され、エージェントに定期的に配信されます。
- セッション チケット キーは、セッション チケットを暗号化するためにポリシー サーバによって使用されます。セッション チケットには、認証情報と、セッションに関連する他の情報 (ユーザ認証情報など) が含まれています。エージェントは、セッション チケットを SiteMinder cookie に埋め込みますが、その内容にアクセスすることはできません。これは、エージェントが、ポリシー サーバの外に出ることがないセッション チケット キーにアクセスできないためです。

どちらのタイプのキーも、ポリシー サーバのキーストアに保存され、実行時にエージェントに配信されます。デフォルトでは、キーストアはポリシー サーバの一部ですが、必要に応じて、個別のキーストアデータベースを作成することもできます。

これらのキー以外に、次の特別なキーがあります。

- ポリシー ストア キー - ポリシー ストア内にある特定のデータを暗号化するために使用されます。ポリシー ストア キーは、ディスク上のファイルに暗号化されて格納されます。ポリシー サーバが独自の技術を使用してポリシー ストア キーを暗号化します。ポリシー ストア キーは、ポリシー サーバのインストール時に指定した暗号化キーから取得されます。
- キー ストア キー - 個別に設定されるキー ストア内にあるエージェント キーやセッション チケット キーを暗号化するために使用されます。キー ストア キーは、ポリシー ストア キーを使用して暗号化されたレジストリ (または UNIX の同様の機能を持つ位置) に保存されます。

キー管理の概要

大規模な環境全体でキー情報を最新の状態に保つために、ポリシー サーバは、自動キー ロールオーバーメカニズムを提供します。同じキーストアを共有するポリシー サーバ環境でキーを自動的に更新することができます。自動キー変換により、キーの完全性も確保されます。SiteMinder エージェントがシングル サインオン用に設定されている場合は、キー ストアが複製され、シングル サインオン環境のすべての SiteMinder 環境で共有される必要があります。

ポリシー サーバは、ポリシー ストアとは別に設定されたキー ストアが使用不可能であると判断した場合、キー ストアへの再接続を試み、オンラインに戻ったかどうかを判断します。接続が失敗する場合、ポリシー サーバは以下のことを行います。

- 一時停止の状態になり、キー ストアがオンラインに戻るまで、確立された接続に対する新規リクエストをすべて拒否します。

  一時停止状態のポリシー サーバは、SuspendTimeout で指定された時間だけ起動したままです。SuspendTimeout で指定された時間に達すると、正常にシャットダウンします。SuspendTimeout がゼロの場合、キー ストア接続が再確立されるまで、ポリシー サーバは一時停止の状態になります。
- エラー ステータスを返し、Web エージェントが別のポリシー サーバにフェイルオーバーできるようにします。
- 適切なエラー メッセージをログに記録します。

また、ポリシー サーバの起動時にキー ストアが使用不可能である場合、そのポリシー サーバは正常にシャット ダウンします。

キーの管理は、[SiteMinder キー管理]ダイアログ ボックスを使用して行います。

FIPS 140-2

FIPS（Federal Information Processing Standards）140-2 は、取扱注意ではあるが機密扱いではないデータを保護するセキュリティ システム内で暗号化アルゴリズムを使用するための要件を規定します。SiteMinder には RSA の CryptoC ME v2.0 暗号化ライブラリが組み込まれています。このライブラリは、FIPS 140-2（*暗号化モジュールに関するセキュリティ要件*）に適合していることが確認されています。このモジュールの認証証明書番号は 608 です。

SiteMinder の Java ベースの API は、FIPS 準拠の CryptoJ 暗号化ライブラリを使用しています。

SiteMinder は、FIPS 以前のモードまたは FIPS 専用モードで動作できます。暗号化の相違点として、SiteMinder が暗号化を適用する方法は両方のモードで同じですが、アルゴリズムが異なります。

FIPS 専用モードの SiteMinder は以下のアルゴリズムを使用します。

- キーを暗号化する AES キー ラップ
- チャネルを暗号化する OFB モード（HMAC-SHA 256）の AES
- シングル サインオンを簡易化するために使用するトークンを暗号化する CBC モード（HMAC-SHA 224）の AES

SiteMinder のコア コンポーネントでは、暗号化されたデータが幅広く利用されます。

- Web エージェントは以下のものを暗号化します。
  - ポリシー サーバから取得したエージェント キーを使用する cookie
  - セッション キーを使用してポリシー サーバに送信されるデータ
  - ホスト キーを使用する共有秘密キー。暗号化された共有秘密キーはホスト設定ファイルに格納されます。

- ポリシー サーバは以下のものを暗号化します。
  - セッション キーを使用して Web エージェントに送信されるデータ
  - ホスト キーを使用するポリシー ストア キー
  - ポリシー ストア キーを使用するポリシー ストア内の機密データ
  - セッション チケット キーを使用するセッション仕様
  - セッション キーを使用して 管理 UI に送信されるデータ
  - セッション チケット キーを使用する、ユーザ ディレクトリ内のパスワード サービス データ

ポリシー ストアに格納される機密データの暗号化には、ポリシー ストア キーを使用します。このキーは、ポリシー ストアのインストール時に入力されるシード文字列から取得されます。ポリシー ストアもホスト キーで暗号化され、システムのローカル ファイルに格納されます。自動操作をサポートするため、ホスト キーはポリシー ストア コードに埋め込まれる固定キーです。エージェントは、この同じホスト キー メカニズムを使用して、それぞれの共有秘密キーのコピーを暗号化し、格納します。

セッション チケット キー（認証トークンを生成するためにポリシー サーバによって使用される）およびエージェント キー（cookie データを暗号化するために、主に Web エージェントによって使用される）は、ポリシー ストア（SiteMinder の設定によってはキー ストア）に暗号化された形で格納される暗号化キーです。これらのキーはポリシー ストア キーまたはキー ストア キーで暗号化されます。キー ストア キーはポリシー ストア内で暗号化されます。エージェントの共有秘密キー（エージェント認証および TLI ハンドシェイクで使用）も、その他の機密データと共に、ポリシー ストア キーで暗号化され、ポリシー ストアに格納されます。

エージェント キー

SiteMinder Web エージェントはエージェント キーを使用して、ユーザのブラウザに渡す前に cookie を暗号化します。SiteMinder cookie を受信すると、Web エージェントはエージェント キーを使用して cookie の内容を復号化します。キーは、ポリシー サーバと通信するすべての Web エージェントで、同じ値に設定してください。

ポリシー サーバは、次のタイプのエージェント キーを提供します。

- ダイナミック キー - ダイナミック キーはポリシー サーバのアルゴリズムにより生成され、接続されたポリシー サーバや関連する SiteMinder Web エージェントに配信されます。ダイナミック キーのロールオーバーは、定期的な実行や、管理 UI の[キー管理]ダイアログ ボックスを使用した実行が可能です。セキュリティ上の理由から、エージェント キーはこのタイプのキーにすることをお勧めします。
- スタティック キー - スタティック キーは不変です。ポリシー サーバのアルゴリズムによる生成や、手動での入力が可能です。SiteMinder 環境では、ユーザのマシン上の cookie に長期間保存される情報を必要とする機能のサブセットに対して、このタイプのキーが使用されます。

  注: スタティック エージェント キーは、常にインストール時に生成されます。また、エージェント キーとして使用する場合もしない場合も、スタティック キーは特定の他の製品機能 (ユーザ管理など) で使用されます。

ダイナミック エージェント キーのロールオーバー

ダイナミック エージェント キーのロールオーバーは、FSS 管理 UI の[キー管理]ダイアログ ボックスで設定します。Web エージェントはキーの更新を確認するため、ポリシー サーバに定期的にポーリングします。キーが更新されている場合、Web エージェントはポーリング時に変更内容を取得します。デフォルトのポーリング間隔は 30 秒ですが、Web エージェントの pspollinterval パラメータを変更して設定することもできます。

注: Web エージェントのパラメータを変更する方法については、「*SiteMinder Web エージェント設定ガイド*」を参照してください。

ポリシー サーバでは、ダイナミック キーを定期的に生成するアルゴリズムを使用しています。これらのキーはキー ストアに保存されます。Web エージェントは、新しいキーを検出すると、それらをキー ストアから取得します。

ダイナミック キーのロールオーバーで使用するエージェント キー

SiteMinder 環境では、以下のキーをダイナミック キーのロールオーバーで使用し、キー ストアで管理します。

- 前回キーは、現在の値の前にエージェント キーが使用していた、直前の値を持つダイナミック キーです。
- 現在キーは、現在のエージェント キーの値を持つダイナミック キーです。
- 予定キーは、エージェント キーのロールオーバーで現在キーとして使用される予定の、次回の値を持つダイナミック キーです。
- スタティック キー

ポリシー サーバがダイナミック エージェント キーのロールオーバーを処理すると、前回キーの値が現在キーの値に置き換えられます。また、現在キーの値は予定キーの値と置き換えられ、ポリシー サーバは予定キーの新しい値を生成します。

クライアントのブラウザから cookie を受信すると、Web エージェントはキーストアの現在キーを使用して cookie を復号化します。復号化された値が有効でなかった場合、Web エージェントは前回キーを使用し、必要に応じて予定キーも使用します。また、まだ更新されていないエージェントからの cookie を復号化したり、クライアントのブラウザから既存の cookie を復号化したりする際に、前回キーが必要な場合があります。更新されたエージェントが作成した cookie の場合でも、まだキーの更新をキーストアにポーリングしていないエージェントがその cookie を読み込む場合は、予定キーが必要です。

エージェント キーのロールオーバー間隔

指定した時間になると、エージェント キーのロールオーバー プロセスが開始されます。複数のポリシー サーバから複数のロールオーバーが実行されないようにするには、各サーバのロールオーバー待機時間を 30 分以内に設定します。待機時間が過ぎても更新が実行されなかった場合、ポリシー サーバはキーを更新します。

すべてのポリシー サーバは、キーの更新を待ってからエージェントに対して新しいキーを処理します。単一のポリシー サーバでも、更新時間はロールオーバー用に指定した時間より長くなります (30 分以内)。

エージェント キーのロールオーバー プロセスは、SiteMinder の[エージェント キー管理]ダイアログ ボックスで指定した時間に開始され、3 分以内に終了します。この時間内に、ポリシー サーバに接続されたすべての Web エージェントが更新されたキーを受け取ります。

注: 複数の複製ポリシー サーバがある環境の場合、エージェント キーの配布には最大 30 分かかる場合があります。

スタティック キー

スタティック キーは、一定で変化しないデータを暗号化するために使用される文字列です。エージェント キーのロールオーバー機能を使用する SiteMinder 環境では、スタティック キーを使用して、長期間にわたってユーザ情報を管理できます。

以下のような SiteMinder の機能および状況で、スタティック キーを使用します。

- HTML フォーム認証方式におけるユーザのクレデンシャルの保存

  HTML フォーム認証方式を使用してユーザがそのクレデンシャルを保存できるように設定されている場合、ポリシー サーバはスタティック キーを使用してユーザのクレデンシャルを暗号化します。

- ユーザ追跡

  ユーザ追跡がオンになっている場合、ポリシー サーバはスタティック キーを使用してユーザ識別情報を暗号化します。

- 複数のキー ストアでのシングル サインオン

  複数のキー ストアがある SiteMinder 環境では、スタティック キーをシングル サインオンに使用できます。この場合、SiteMinder エージェントはすべての cookie の暗号化にスタティック キーを使用します。

  注: スタティック キーを変更した場合、変更する前のスタティック キーで作成された cookie はすべて無効になります。このとき、ユーザは強制的に再認証され、ユーザの追跡情報は無効になります。また、シングル サインオンにスタティック キーを使用している場合、ユーザが別の cookie ドメインのリソースにアクセスしようとすると、クレデンシャルが要求されます。

セッション チケット キー

ユーザが、保護されたリソースへ正常にログインした場合、ポリシー サーバはセッション チケットを作成します。セッション チケットは、ユーザ認証の有効期間を決定するためにポリシー サーバによって使用されます。セッション チケットはセッション チケット キーで暗号化され、エージェント ユーザ キャッシュ内にキャッシュされます。

アルゴリズムを使用してポリシー サーバにセッション チケット キーを生成させるか、あるいは SiteMinder の[キー管理]ダイアログ ボックスでセッション チケット キーを入力します。セキュリティ上の理由から、キーはランダムに生成することをお勧めします。ただし、シングル サインオン環境で SiteMinder に複数のキー ストアがある場合は、すべてのキー ストアに対して同一のセッション チケット キーを入力する必要があります。

キー管理のシナリオ

シングル サインオンが必要な環境で、ポリシー サーバ、ポリシー ストア、およびキー ストアをどのように実装するかによって、キー管理には 3 つのシナリオがあります。以下にそのシナリオを示します。

- 共通のポリシーストアとキーストア

  このシナリオでは、ポリシー サーバ グループが 1 つのポリシー ストアとキー ストアを共有して、単一 cookie ドメインでアクセス制御とシングル サインオンを実現します。

  ポリシーストアデータは、1 つのポリシーストアに格納されます。キーデータは、1 つのキーストアに格納されます。キーストアは、ポリシーストアの一部とすることも、個別のストアとすることもできます。

  ポリシーストアとストアデータは、どちらもフェイルオーバーのために複製することができます。複製は、ポリシーストア用に選択したデータベースまたはディレクトリタイプに基づいて設定する必要があります。複製方式については、使用しているデータベースまたはディレクトリのベンダーから提供されているマニュアルを参照してください。

- 共通のキーストアがある複数のポリシーストア

  このシナリオでは、ポリシー サーバ グループが別々のポリシー ストアに接続し、1 つのキー ストアを共有して、複数の cookie ドメイン間のアクセス制御とシングル サインオンを実現します。

  各ポリシー サーバ グループのポリシ ーストア データは、1 つのポリシー ストアに格納されます。すべてのポリシー サーバ グループのキー データは、1 つのキー ストアに格納されます。個別のキー ストアにより、すべてのポリシー サーバに関連付けられたエージェントがキーを共有できるため、複数の個別 cookie ドメイン間のシングル サインオンが可能になります。

  ポリシーストアとストアデータは、どちらもフェイルオーバーのために複製することができます。複製は、ポリシーストア用に選択したデータベースまたはディレクトリタイプに基づいて設定する必要があります。複製方式については、使用しているデータベースまたはディレクトリのベンダーから提供されているマニュアルを参照してください。

- 複数のポリシー ストアと複数のキー ストア

  このシナリオでは、各ポリシー サーバ グループが 1 つのポリシー ストアとキー ストアを共有して、(各 cookie ドメインのポリシー サーバに個別のキーストアを実装することが望ましい) 複数の cookie ドメイン間のアクセス制御とシングル サインオンを実現します。

  各ポリシー サーバ グループのポリシ ーストア データは、1 つのポリシー ストアに格納されます。各ポリシー サーバ グループのキー データは、1 つのキー ストアに格納されます。キーストアは、ポリシーストアの一部とすることも、個別のストアとすることもできます。同一のスタティック キー セットを使用することによって、すべての Web エージェント間でのシングル サインオンが実現されます。

  ポリシーストアとストアデータは、どちらもフェイルオーバーのために複製することができます。複製は、ポリシーストア用に選択したデータベースまたはディレクトリタイプに基づいて設定する必要があります。複製方式については、使用しているデータベースまたはディレクトリのベンダーから提供されているマニュアルを参照してください。

キー管理に関する注意事項

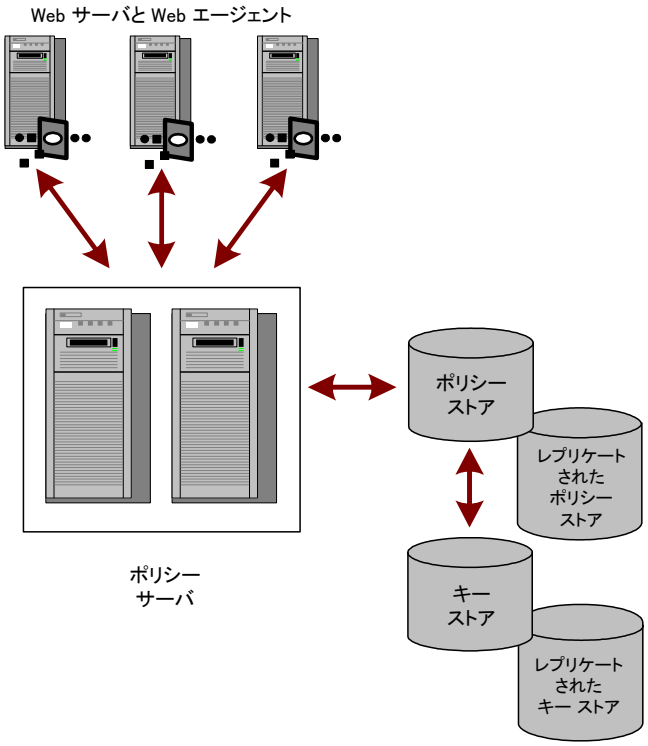
企業のキー管理のシナリオを決定する際には、以下の点に注意してください。

- 複数のポリシー サーバが共通のキーストアを共有する環境でダイナミック キーを設定する場合は、エージェント キーを生成する単一のポリシー サーバを指定する必要があります。他のすべてのポリシー サーバでは、必ずキー生成を無効にしてください。
- 複数のポリシー サーバが含まれるネットワーク構成では、ポリシー サーバ管理コンソールを使用して、各ポリシー サーバのポリシーストアを指定できます。ポリシー ストアは、SiteMinder オブジェクトとポリシー情報の主な格納場所であるマスタ ポリシー ストアにしたり、マスタ ポリシー ストアからコピーされるデータを使用する複製ポリシー ストアにしたりできます。
- マスタ/スレーブディレクトリまたはデータベースは、ディレクトリまたはデータベースのプロバイダの指定に従って設定する必要があります。ポリシー サーバでは、ポリシー ストアのフェイルオーバー順序を指定できますが、データ複製は制御されません。複製方式については、使用しているデータベースまたはディレクトリのプロバイダから提供されているマニュアルを参照してください。
- ダイナミック キーのロールオーバーを使用するネットワークの場合、ポリシー サーバのポリシーストアは必ずマスタ キー ストア、または複製されたスレーブ キー ストアのいずれかになります。マスタ キー ストアは、キーを生成するポリシー サーバ プロセスから直接キーを受け取ります。またスレーブ キー ストアは、マスタ キー ストアにあるキーのコピーを受け取ります。
- マスタ/スレーブ環境では、ポリシー サーバからマスタ ポリシー ストアおよびキーストアにキーが生成されるように設定する必要があります。マスタ ポリシー ストアおよびキー ストアのデータは、その後に、フェイルオーバー順の設定に含まれる他のすべてのポリシーストアおよびキー ストアに複製される必要があります。
- 複数の cookie ドメインがあるシングル サインオン環境では、マスタ キー ストアが 1 つある場合か、1 つのマスタ キー ストアから複製されたキーを持つスレーブ キー ストアがある場合のみ、ダイナミック キーを使用できます。
- ポリシー ストアとキー ストアは、LDAP と ODBC の混合ディレクトリにインストールできます。ポリシー ストアは ODBC データベースに格納でき、キー ストアは LDAP ディレクトリ サーバに格納できます。また、その逆も可能です。サポートされているデータベースのリストについては、テクニカル サポート サイトに移動し、SiteMinder r12.0 SP3 プラットフォーム サポート マトリックスを検索してください。

共通のポリシーストアとキーストア

キーのロールオーバーを使用する SiteMinder 設定の最も簡単なシナリオは、複数のポリシー サーバが 1 つのキーストアと共に、1 つのポリシー ストア (および関連するフェイルオーバー ポリシー ストア) を使用する場合です。

以下の図は、1 つのポリシー ストアを使用している複数のポリシー サーバを示しています。

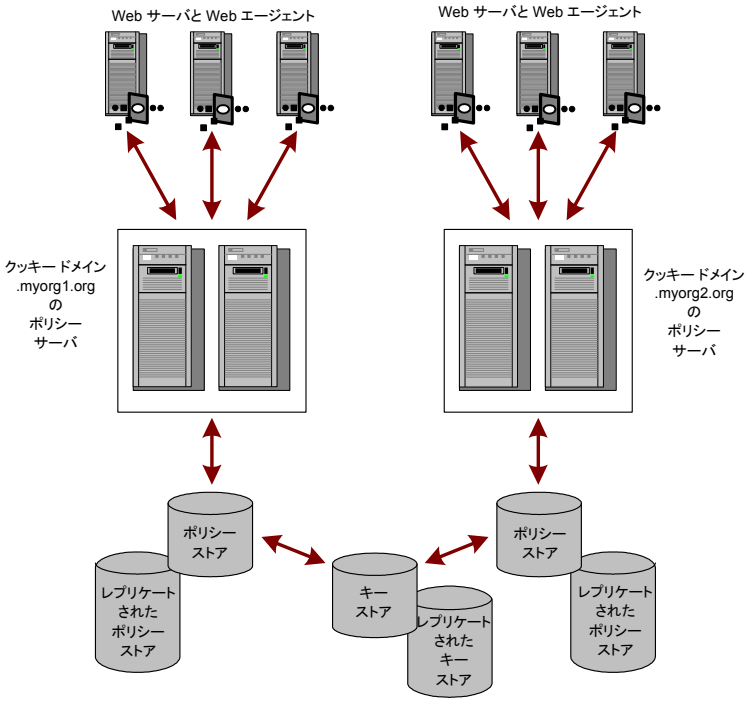


このタイプの設定では、ポリシー サーバはキー ストアからダイナミック キーを取得します。ポリシー サーバに関連付けられた Web エージェントは、ポリシー サーバから新しいキーを収集します。

共通のキーストアがある複数のポリシーストア

シングル サインオン環境において、個別のポリシーストアを持つ複数ポリシー サーバで構成されるネットワークを設定する場合、すべてのポリシー サーバがキーのロールオーバーで使用する共通のキーストアを持つことができます。

以下の図は、共通のキー ストアを使用している複数のポリシー サーバを示しています。



1 つのポリシー サーバがダイナミック キーを生成し、それを中央のキーストアに格納します。各ポリシー サーバは、中央のキー ストアを使用するように、ポリシー サーバ管理コンソールで設定されています。他のすべてのポリシー サーバでは、エージェント キーの生成を無効にする必要があります。エージェントは新しいキーを取得するために、各自のポリシー サーバをポーリングします。ポリシー サーバは共通のキー ストアから新しいキーを取得し、それを SiteMinder エージェントに渡します。

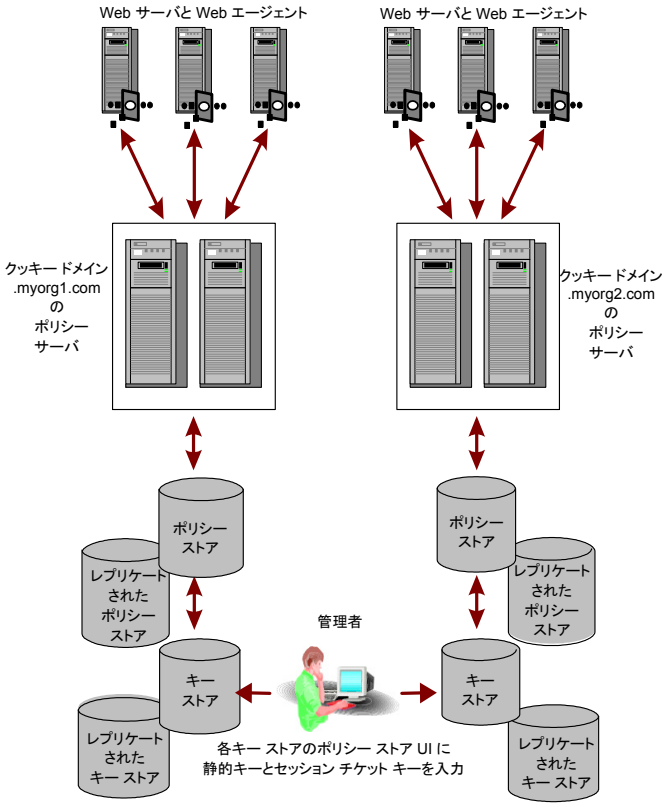
注: このシナリオでは、キーを生成していないポリシー サーバがキーの更新をキー ストアにポーリングするように、追加のレジストリ設定が必要です。

個別のキーストアがある複数のポリシーストア

複数のポリシー サーバ、ポリシーストア、およびマスタ キー ストアで構成されるネットワークを設定する場合、適切な権限を持つ管理者は、次のどちらかまたは両方を容易にするために、各ポリシーストアに対して同一のスタティック キーとセッション チケット キーを指定できます。

- すべてのエージェント間でのシングル サインオン
- 共通のユーザディレクトリによるパスワードサービス

以下の図は、複数のポリシー サーバとポリシー ストアが含まれる環境を示しています。



前の例では、SiteMinder Web エージェントが作成したすべての cookie の暗号化に、同じスタティック キーが使用されています。

r6.x ポリシー ストア暗号化キーのリセット

r6.x ポリシー ストア暗号化キーをリセットする方法

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

   `smobjexport -d*siteminder_administrator* -w*password* -o*file_name* -c`

   -d*siteminder_administrator*

   SiteMinder 管理者アカウントの名前を指定します。

   注: この管理者は、SiteMinder のすべてのドメイン オブジェクトを管理できる必要があります。

   -w*password*

   SiteMinder 管理者アカウントのパスワードを指定します。

   -o*file_name*

   以下を指定します。

   - 出力場所のパス
   - ユーティリティによって作成される smdif ファイルの名前

   注: この引数を指定しない場合、デフォルトの出力ファイル名は stdout.smdif と stdout.cfg になります。

   -c

   機密データをクリアテキストとしてエクスポートします。

   ポリシー ストア データが smdif ファイルにエクスポートされます。
3. smreg ユーティリティが *policy_server_home¥bin* にあることを確認します。

   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。

   注: ユーティリティがない場合は、サポート サイトで提供されているポリシー サーバ インストール メディアから入手できます。

4. 以下のコマンドを実行します。

   `smreg -key encryption_key`

   encryption_key

   新しい暗号化キーを指定します。

   制限: 6 ～ 24 文字

   ポリシー ストア暗号化キーが変更されます。

5. 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。

6. ポリシー ストア管理者パスワードを再入力し、[更新]をクリックします。

   管理者パスワードが新しい暗号化キーで暗号化されます。

7. 以下のコマンドを実行します。

   `smreg -su password`

   password

   SiteMinder スーパーユーザ パスワードを指定します。

   スーパーユーザ パスワードが設定され、新しい暗号化キーで暗号化されます。

8. 以下のコマンドを実行します。

   `smobjimport -dsiteminder_administrator -wpassword -ifile_name -r -f -c`

   -d*siteminder_administrator*

   SiteMinder 管理者アカウントの名前を指定します。

   注: この管理者は、SiteMinder のすべてのドメイン オブジェクトを管理できる必要があります。

   -w*password*

   SiteMinder 管理者アカウントのパスワードを指定します。

   -i*file_name*

   以下を指定します。

   - smdif ファイルのパス
   - smdif ファイルの名前

   注: この引数を指定しない場合、デフォルトの入力ファイル名は stdout.smdif と stdout.cfg になります。

-r

インポート中、重複するポリシー ストア情報を上書きできることを明示します。

-f

オブジェクトの名前の自動変更機能をオフにします。デフォルトでは、ターゲット ポリシー ストア内に存在する名前を持つオブジェクトをインポートしようとすると、重複するオブジェクトが作成されます。オブジェクトの名前は *nameoid* です。

name

オブジェクトの名前を指定します。

oid

新しい重複オブジェクトのオブジェクト ID を指定します。

ネーミングの競合が原因で作成できなかったすべてのオブジェクトに対しては、エラー メッセージが返されます

-c

入力ファイルに機密データをクリアテキストで格納することを明示します。

9. 以下のコマンドを実行します。

```
smreg -su password
```

password

SiteMinder スーパーユーザ パスワードを指定します。

スーパーユーザ パスワードが設定されます。

ポリシー ストア暗号化キーがリセットされます。

r12.x ポリシー ストア暗号化キーのリセット

r12.x ポリシー ストア暗号化キーをリセットする方法

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

   `XPSExport` *`output_file`* `-xa -xs -xc -passphrase` *`passphrase`*

   output_file

   ポリシー ストア データのエクスポート先となる XML ファイルの名前を指定します。

   -xa

   すべてのポリシー ストア データをエクスポートすることを明示します。

   -xs

   セキュリティ データをエクスポートすることを明示します。

   -xc

   設定データをエクスポートすることを明示します。

   -passphrase *passphrase*

   機密データの暗号化に必要なパスフレーズを指定します。

   制限: パスフレーズは以下の条件を満たしている必要があります。

   - 8 文字以上
   - 1 つ以上の大文字および 1 つ以上の小文字を含む
   - 1 つ以上の数字を含む

     注: パスフレーズに空白が含まれる場合は、パスフレーズ全体を二重引用符で囲みます。

   ポリシー ストア データが XML にエクスポートされます。
3. smreg ユーティリティが *policy_server_home¥bin* にあることを確認します。

   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。

   注: ユーティリティがない場合は、サポート サイトで提供されているポリシー サーバ インストール メディアから入手できます。

4. 以下のコマンドを実行します。

   `smreg -key` *`encryption_key`*

   encryption_key

   新しい暗号化鍵を指定します。

   制限: 6 ～ 24 文字

   ポリシー ストア暗号化キーが変更されます。

5. 以下のコマンドを実行します。

   `XPSImport` *`input_file`* `-fo -passphrase` *`passphrase`*

   input_file

   エクスポートされるポリシー ストア データを含む XML ファイルの名前を指定します。

   -fo

   既存のポリシー ストア データを上書きできます。

   -passphrase passphrase

   機密データの復号化に必要なパスフレーズを指定します。

   重要: ポリシー ストアのエクスポート時に入力されたパスフレーズに一致しない場合、機密データは復号化できず、インポートは失敗します。

   ポリシー ストア データがインポートされます。

   ポリシー ストア暗号化キーがリセットされます。

エージェント キー生成の設定

ポリシー サーバ管理コンソールの[キー]タブでは、ポリシー サーバにおけるエージェント キー生成の方法を設定します。

注: キー生成を有効にするのは、エージェント キーを生成させるポリシー サーバのみにしてください。

ポリシー サーバのエージェント キー生成を設定する方法

1. ポリシーサーバー管理コンソールを起動します。

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

2. [キー]タブをクリックします。

   注: このタブ上での設定およびコントロールの詳細については、[ヘルプ]-[管理コンソール ヘルプ]をクリックしてください。

3. [キー]タブに示されるフィールドとコントロールに値を入力して、エージェント キー生成を設定します。

4. 入力が終わったら、[適用]をクリックして変更内容を保存します。

エージェント キーの管理

管理 UI からアクセスできる[SiteMinder キー管理]ダイアログ ボックスでは、エージェント キーの定期的なロールオーバーの設定、手動によるロールオーバーの実行、およびスタティック キーの変更ができます また、セッション チケット キーの管理も可能です。

注: キーを管理するには、キーとパスワード ポリシーの管理権限を持つアカウントを使用して、管理 UI にログインしてください。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。

定期的なキー ロールオーバーの設定

ポリシー サーバでは、週次、日次、あるいは 1 日の内での、エージェント キーの定期的なロールオーバーを設定できます。ロールオーバー間隔の最小設定時間は 1 時間です。

注: 使用しているオペレーティング システムで夏時間のシステム時刻調整が設定されていない場合、キー ロールオーバーは 1 時間オフセットされる場合があります。予期した時間にキー ロールオーバーを確実に行うには、夏時間を認識するようにオペレーティング システムを設定します。

定期的なキー ロールオーバーを設定する方法

1. ポリシー サーバ管理コンソールの[キー]タブにある[エージェント キー生成を有効にする]チェック ボックスをオンにし、[OK]をクリックします。
2. 管理 UI にログインします。
3. [管理]タブで、[ポリシー サーバ]-[キー管理]を選択します。

   [キー管理]ペインが開きます。
4. [エージェント キー]グループ ボックスで、[ダイナミック エージェント キーを使用]を選択します。

   ペインが、ダイナミック キーに対応したものに変わります。
5. [ダイナミック キーの詳細]グループ ボックスで、[自動キー ロールオーバー]を選択し、[ロールオーバー間隔の設定]をクリックします。

   [ダイナミック キーのロールオーバー]グループ ボックスが表示されます。
6. 自動キー ロールオーバーの頻度を設定します。
7. [OK]をクリックします。

   [キー管理]ペインに戻ります。

キーの手動ロールオーバー

エージェント キー管理機能の 1 つに、ダイナミック エージェント キーのロールオーバーを手動で行えるようにするものがあります。この機能を使用するとキーをいつでもロールオーバーできるので、セキュリティが強化されます。また、ポリシー サーバにダイナミック キーを生成させるが、定期的にキーのロールオーバーをさせない場合にも、この機能を使用できます。

ダイナミック エージェント キーのロールオーバーを手動で実行する方法

1. 管理 UI にログインします。
2. [管理]タブから、[ポリシー サーバ]-[キー管理]を選択します。

   [キー管理]ペインが開きます。
3. [エージェント キー]グループ ボックスで、[ダイナミック エージェント キーを使用]を選択します。

   ペインが、ダイナミック キーに対応したものに変わります。
4. [ダイナミック キーの詳細]グループ ボックスで、[手動キー ロールオーバー]を選択します。
5. ダイナミック キーのロールオーバーを実行するには、[今すぐロールオーバーを実行] をクリックします。

   これを選択すると、ポリシー サーバが直ちに新しいエージェント キーを生成します。エージェント キーのロールオーバーを手動で実行しない限り、新しいダイナミック キーは自動的に生成されません。

   注: キーのロールオーバーを複数回実行する場合以外は、このボタンを何度もクリックしないでください。

   Web エージェントは、次回のポリシー サーバへのポーリング時に新しいキーを受け取ります。キャッシュとの同期をとるため、この処理には最長で 3 分かかります。セキュリティ上の理由により、まったく新しいキー セットを使用したい場合には、前回キーと現在キーの両方をキー ストアから削除するために、ダイナミック キーのロールオーバーを 2 回実行できます。

エージェント キー管理とセッション タイムアウトの調整

エージェント キーの更新とセッション タイムアウトを調整しないと、セッション情報を含む cookie が無効になる場合があります。企業のポリシー設計の担当者とダイナミックキーロールオーバーの設定の担当者が異なる場合があるので、この調整は重要です。

セッション タイムアウトは、エージェント キーのロールオーバー間隔の 2 倍以下に設定してください。セッション タイムアウトの前にエージェント キーのロールオーバーが 2 回実行されるように設定すると、1 回目のキー ロールオーバーの前に Web エージェントによって書き込まれた cookie は、セッションが終了する*前に*無効になり、ユーザは再度 ID の入力を求められます。

たとえば、3 時間ごとにキー ロールオーバーが実行されるように設定すると、複数のキー ロールオーバーによってセッション cookie が無効にならないように、最大セッション タイムアウトを 6 時間以下に設定する必要があります。

スタティック キーの変更

特定の SiteMinder 機能の識別情報を暗号化するために SiteMinder Web エージェントが使用するスタティック エージェント キーは変更できます。

重要: スタティック キーの変更は、いくつかの SiteMinder 機能が正しく動作するために必要なデータが失われる原因となるため、推奨されません。この場合、永続的な cookie に格納されている情報を組み立てて使用する機能が動作しなくなります。スタティック キーの変更は、セキュリティ侵害などのやむを得ない状況においてのみ行ってください。シングル サインオンが複数の SiteMinder インストール環境で機能する前に、認証されたユーザは強制的に再ログインを要求される可能性があります。

スタティック キーは、複数のポリシー サーバと複数のマスタ キー ストアが必要な環境で、シングル サインオン環境を維持するために使用されることもあります。

スタティック キーを変更する方法

1. 管理 UI にログインします。
2. [管理]タブで、[ポリシー サーバ]-[キー管理]を選択します。

   [キー管理]ペインが開きます。
3. [エージェント キー]グループ ボックスで、[スタティック エージェント キーを使用]を選択します。

   ペインが、スタティック キーに対応したものに変わります。

4. 以下のいずれかの操作を行います。
   - [ランダム エージェント キーを生成]グループ ボックスで、[今すぐロールオーバーを実行]をクリックして、ランダムな新しいスタティック キーを生成します。
   - [エージェント キーの指定]グループ ボックスで、以下のフィールドを設定してスタティック キーを入力します。

     スタティック キー

     ポリシー サーバがスタティック キーとして使用する値を指定します。このオプションは、シングル サインオン環境を維持するために 2 つのキー ストアでスタティック キーを使用する必要がある場合に使用します。

     キーの確認

     スタティック キーを再入力します。
5. [今すぐロールオーバーを実行] をクリックします。

   選択したオプションによって、ポリシー サーバは新しいスタティック キーを生成するか、または指定したスタティック キーを使用します。スタティック キーのロールオーバーは 3 分以内に終了します。
6. [サブミット]をクリックして、変更を保存します。

セッション チケット キーの管理

ポリシー サーバでは、アルゴリズムを使用したセッション チケット キーの生成や、手動によるセッション チケット キーの入力が可能です。セッション チケットは、ユーザの認証が正常に行われるたびに作成され、これによってポリシー サーバがユーザ セッションの継続時間を判断できるようになります。

注: セッション チケット キーを手動で割り当てる必要がある環境は、複数の独立したキー ストアがある環境だけです。ポリシー サーバは、自動的に生成したキーを複数の独立したキーストアに配信することができません。他のいかなる場合でも、ポリシー サーバのアルゴリズムによって生成されるセッション チケット キーを使用することをお勧めします。

セッション チケット キーの生成

ポリシー サーバでは、ダイナミック エージェント キーを生成するのと同様の方法で、セッション チケット キーを生成できます。セッション チケット キーをランダムに生成する場合、ポリシー サーバはアルゴリズムを使用して、暗号化と復号化に使用するキーを作成します。

セッション チケット キーを生成する方法

1. 管理 UI にログインします。
2. [管理]タブで、[ポリシー サーバ]-[キー管理]を選択します。

   [キー管理]ペインが開きます。
3. 以下の*いずれか*の操作を実行します。
   - [ランダム セッション チケット キーを生成]グループボックスで、[今すぐロールオーバーを実行]をクリックします。

     ポリシー サーバが新しいセッション チケット キーを生成します。セッション チケットの暗号化と復号化に使用されているキーが、直ちにこのキーと置き換えられます。
   - [セッション チケット キーの指定]グループ ボックスで、以下のフィールドに値を入力します。

     セッション チケット キー

     セッション チケット キーの値を入力します。ポリシー サーバが、セッション チケット キーを直ちに入力した値に置き換えます。

     確認

     セッション チケット キーを再入力します。
4. [今すぐロールオーバーを実行] をクリックします。
5. [サブミット]をクリックして、変更を保存します。

手動によるセッション チケット キーの入力

使用しているポリシー サーバが複数のキーストアの存在する環境に置かれている場合は、セッション チケット キーを手動で入力できます。

セッション チケット キー入力する方法

1. [管理]タブで、[ポリシー サーバ]-[キー管理]を選択します。

   [キー管理]ペインが開きます。

2. [セッション チケット キーの指定]グループ ボックスで、以下のフィールドに値を入力します。

   セッション チケット キー

   セッション チケット キーを入力します。

   確認

   セッション チケット キーを再入力します。

3. [今すぐロールオーバーを実行] をクリックします。

   ポリシー サーバが、セッション チケット キーを直ちに入力した値に置き換えます。

4. [サブミット]をクリックします。

EnableKeyUpdate レジストリ キーの設定

個別のポリシー ストアに接続し、中央のキー ストアを共有する複数のポリシー サーバが存在する環境で 1 つのポリシー サーバが暗号化キーを生成している場合は、追加のレジストリ設定が必要です。このレジストリ設定は、各ポリシー サーバが共通のキー ストアをポーリングし、新しい暗号化キーを定期的に取得するようにします。

Windows のポリシー サーバで EnableKeyUpdate レジストリ キーを設定する方法

1. Windows の[スタート]メニューから[ファイル名を指定して実行]を選択します。
2. [ファイル名を指定して実行]ダイアログボックスで「regedit」と入力し、[OK]をクリックします。
3. レジストリエディタで、次のレジストリ設定を確認します。

   ```
   HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥
   CurrentVersion¥ObjectStore
   ```

4. 以下のレジストリ値を変更します。

   "EnableKeyUpdate"=0

   以下に変更

   "EnableKeyUpdate"=1

5. ポリシー サーバを再起動します。

UNIX のポリシー サーバで EnableKeyUpdate レジストリ キーを設定する方法

1. 次のディレクトリに移動します。

   install_directory/siteminder/registry

2. テキストエディタを使用して sm.registry を開きます。

3. ファイル内にある次のテキストを確認します。

   HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥
   CurrentVersion¥ObjectStore

4. 以下のレジストリ値を変更します。

   "EnableKeyUpdate"=0

   以下に変更

   "EnableKeyUpdate"=1

5. ポリシー サーバを再起動します。

詳細情報:

共通のキーストアがある複数のポリシーストア (P. 64)

トラステッド ホストの共有秘密キー

トラステッド ホストを登録するときは、インストール プロセスによって、その Web エージェントの共有秘密キーが自動的に生成され、ホスト設定ファイル (SmHost.conf) に格納されます。トラステッド ホストの登録時に共有秘密キーのロールオーバーを有効にすると、トラステッド ホストの共有秘密キーをロールオーバーできるようになります。共有秘密キーのロールオーバーは、手動で実行することも、定期的に実行することもできます。

共有秘密キーの手動によるロールオーバーまたは定期的なロールオーバーの実行時には、共有秘密キーは、インストール時にロールオーバーの有効化を設定したエージェントについてのみロールオーバーされます。

Web エージェントのインストールとトラステッド ホストの登録については、「*SiteMinder Web エージェント インストール ガイド*」を参照してください。

共有秘密キーのロールオーバーが自動的に行われるのは、エージェント キーの生成を有効にするように設定されているサーバのみです。エージェント キーの生成を有効にするには、ポリシー サーバ管理コンソールの[キー]タブにある[エージェント キー生成を有効にする]チェック ボックスをオンにします。この設定は、デフォルトでは有効になっています。

重要: キーを生成する目的では、ポリシー サーバを 1 つのみ有効にすることをお勧めします。環境内に複数のポリシー ストアがあり、共有されるキー ストアが 1 つのみの場合、ポリシー ストア内の共有秘密キーは、キー生成が有効になっているポリシー サーバのポリシー ストア内にのみ自動的にロールオーバーされます。その他のポリシー ストアについては、手動でロールオーバーを実行できます。

共有秘密キーを手動でロールオーバーするには、ターゲット ポリシー ストアに対して設定されたポリシー サーバ上で動作している FSS 管理 UI または C Policy Management API を使用します。

注: 共有秘密キー ポリシー オブジェクトはキー ストア内に保持されるため、同じキー ストアを共有するすべてのポリシー ストアによって共有されます。共有秘密キーそのものは、ポリシー ストアの一部であるトラステッド ホスト オブジェクト内に保持されます。

トラステッド ホストの共有秘密キーのロールオーバー設定

ポリシー サーバは、トラステッド ホストの共有秘密キーの手動によるロールオーバーおよび定期的なロールオーバーをサポートしています。

定期的なロールオーバーは、時間、日、週、または月 単位で設定できます。ロールオーバーの設定可能な最短間隔は 1 時間です。ポリシー サーバは、日次、週次、または月次の特定の時間にロールオーバーを開始するのではなく、各トラステッド ホストの共有秘密キーの有効期限に基づいてロールオーバーを開始します。各共有秘密キーの有効期限が切れたときにそのキーをロールオーバーすることによって、ロールオーバー関連の処理が時間的に分散されるので、ポリシー サーバに大きな処理負荷がかかることを避けることができます。

手動ロールオーバー機能を使用すると、共有秘密キーのロールオーバーが有効になっているすべてのトラステッド ホストに対して新しい共有秘密キーが設定されるため、一般に、その後の定期的なロールオーバーは、すべてのトラステッド ホストに対して集中的に実行されることになります。

重要: 単一のポリシー ストアに関連付けられた複数のポリシー サーバでキーの生成を有効にすると、オブジェクト ストアの伝播遅延のために、同じ共有秘密キーが短期間に何回もロールオーバーされることがあります。その結果、ホストの新しい共有秘密キーが破棄され、ホストが孤立する場合があります。この潜在的な問題を解決するために、ポリシーストアごとに 1 つのポリシー サーバについてのみ共有秘密キーのロールオーバーを有効にするようにしてください。

トラステッド ホストの共有秘密キーのロールオーバーを設定する方法

1. ポリシー サーバ管理コンソールの[キー]タブにある[エージェント キー生成を有効にする]チェック ボックスがオンになっていることを確認します。
2. 管理 UI にログインします。
3. [管理]タブで、[ポリシー サーバ]-[共有秘密キーのロールオーバー]を選択します。

   [共有秘密キーのロールオーバー]ペインが開きます。
4. [共有秘密キーのロールオーバー]グループ ボックスで、以下の操作のいずれかを実行します。
   - ロールオーバーをただちに実行するには、[今すぐロールオーバーを実行]をクリックします。
   - 共有秘密キーがロールオーバーされないようにするには、[共有秘密キーのロールオーバーなし]を選択します。

- 定期的なロールオーバーを指定するには、[指定周期による共有秘密キーのロールオーバー]を選択し、以下のフィールドに値を入力します。

  ロールオーバー間隔

  ロールオーバーを実行する回数を整数で入力します。この数値はロールオーバー期間の値と連動します。

  ロールオーバー期間

  プルダウン リストから、ロールオーバーを実行する時間、日、週、または月を選択します。

ポリシー サーバは、共有秘密キーのロールオーバーの有効化が設定されているすべてのトラステッドホストについて、共有秘密キーのロールオーバーのプロセスを開始します。環境内のトラステッドホストの数によっては、ロールオーバーに多少時間がかかる場合があります。

5. [サブミット]をクリックして、変更を保存します。

第 7 章: ポリシー サーバ ログの設定

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 サーバによるロギングの概要

ポリシー サーバのログ ファイルには、ポリシー サーバのステータスに関する情報が記録されます。また、オプションで、ログ ファイル内の認証イベント、許可イベント、およびその他のイベントに関する、レベル設定可能な監査情報が記録されます。ポリシー サーバを RADIUS サーバとして設定している場合は、RADIUS アクティビティのログが RADIUS ログ ファイルに記録されます。

これらのログは管理コンソールの[ログ]タブで設定します。

ポリシー サーバ ログの設定

ポリシー サーバ ログを設定する方法

1. ポリシーサーバー管理コンソールを起動します。

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

2. [ログ]タブをクリックします。

   注: このタブ上での設定およびコントロールの詳細については、[ヘルプ]-[管理コンソール ヘルプ]をクリックしてください。

3. [ポリシー サーバ ログ]および[ポリシー サーバの監査ログ]グループ ボックスに示されている設定を調整して、ポリシー サーバ ログの場所、ロールオーバー特性、および監査ログに必要なレベルを設定します。

4. ポリシー サーバを RADIUS サーバとして設定している場合は、[RADIUS ログ]グループ ボックスに示されている設定を調整します。

5. [適用]をクリックして、変更内容を保存します。

ポリシー ストア オブジェクトに対して管理者が行った変更の記録

デフォルトでは、ポリシー ストア オブジェクトへの SiteMinder 管理者変更は、siteminder_home¥audit にある XPS テキスト ファイルのセットに書き込まれます。

以下の例に示すとおり、監査ログはテキスト ファイルとして保存されます。

policy_server_home/audit/xps-*process_id*-*start_time*-*audit_sequence*.*file_type*

各監査ログ ファイルの名前には、以下の情報が含まれます。

process_id

監査対象イベントに関連付けられているプロセスの数を示します。

開始時間

トランザクションが*開始された*時刻を以下の形式で示します。

YYYYMMDDHHMMSS

年が 4 桁、時刻が 24 時間形式で表記されます。

例: 20061204133000

audit_sequence

監査対象イベントのシーケンス番号を示します。

file_type

以下のいずれかのイベント タイプを示します。

access

以下のアクセス イベントを含む監査ログ ファイルを示します。

- 管理 UI またはレポート サーバが登録される
- 管理 UI またはレポート サーバが他のユーザの代わりにプロキシとして動作する
- リクエストしたアクションについて管理者がアクセスを拒否される

audit

以下のイベントを含む監査ログ ファイルを示します。

- オブジェクトが変更される(XPS ツールまたは 管理 UI を使用して)
- 管理者レコードが作成、変更、または削除される

txn

以下のトランザクション イベントを含む監査ログ ファイルを示します。

- XPS ツールが、オブジェクトへの変更を開始、コミット、または拒否する

注: SiteMinder バイナリ ファイル（XPS.dll、libXPS.so、libXPS.sl）への書き込みアクセス許可がユーザに*ない* 場合は、管理者が 管理 UI または XPSSecurity ツールを使用して、関連する XPS コマンド ライン ツールを使用する権限を付与する必要があります。

デフォルトの動作を変更する方法

1. ポリシー サーバ ホスト システムにアクセスします。
2. コマンド ライン セッションを開き、以下のコマンドを入力します。

   `xpsconfig`

   ツールが起動し、このセッションのログ ファイルの名前が表示されます。また、選択項目のメニューが開きます。
3. 以下のコマンドを入力します。

   `xps`

   オプションのリストが表示されます。
4. 以下のコマンドを入力します。

   `1`

   現在のポリシー ストア監査設定が表示されます。
5. 「C」と入力します。

   注: このパラメータは、TRUE または FALSE の値を使用します。値を変更すると、2 つの状態が切り替わります。

   更新されたポリシー ストア監査設定が表示されます。新しい値は「保留中の値」としてリストの下部に表示されます。
6. 以下の手順を実行します。

   a. 2 回「Q」と入力します。

   b. 「Q」と入力して XPS セッションを終了します。

   変更が保存され、コマンド プロンプトが表示されます。

古いログ ファイルを自動的に処理する方法

SiteMinder ポリシー サーバでは、以下のいずれかのスクリプトをカスタマイズすることによって、古いログ ファイルが自動的に処理されるように設定できます。

- Harvest.bat（Windows）
- Harvest.sh（UNIX または Linux）

以下のいずれかのイベントが発生すると、スクリプトが実行されます。

- XPSAudit プロセスが開始するとき（以下のオプションを使用して）

  CLEANUP

  ディレクトリ内のログ ファイルを一度にすべて処理します。
- ログ ファイルがロールオーバーされるとき常に
- XPSAudit プロセスが終了するとき

  ロールオーバーまたは終了中、ファイルは名前別に 1 つずつ処理されます。

ファイルを処理するスクリプトは自由にカスタマイズできます。たとえば、ファイルを削除したり、データベースに移動したり、別の場所へアーカイブしたりするようにスクリプトを変更することもできます。

注: このスクリプトはあくまでも例として提示しています。CA ではサポートされていません。

古いログ ファイルを自動的に処理するには、以下の手順に従います。

1. ポリシー サーバで以下のディレクトリを開きます。

   policy_server_home/audit/samples
2. 使用しているオペレーティング システムに合ったスクリプトをテキスト エディタで開き、コピーを以下のディレクトリに保存します。

   policy_server_home/audit/Harvest.*extension*

   注: ファイルの名前を変更したり、指定とは異なる場所にファイルを保存したりしないでください。
3. 自分のニーズに沿ってスクリプトをカスタマイズするためのガイドとして、スクリプトの中で注釈を使用してください。
4. カスタマイズしたスクリプトを保存し、テキスト エディタを終了します。

SiteMinder 管理監査イベントをレポートに含める方法

SiteMinder レポート サーバと監査データベースがすでにある場合は、SiteMinder を設定して、以下のレポート データベース タイプのいずれかをインポートできる管理監査イベントを収集できます。

- Oracle データベース
- Microsoft SQL Server データベース

データが smobjlog4 データベース テーブルにインポートされたら、SiteMinder レポート サーバを使用して生成するすべてのレポートにそのデータを含めることができます。

SiteMinder ポリシー サーバにはサンプルの Perl プログラムがインストールされており、ニーズに合わせてカスタマイズできます。

SiteMinder レポートに管理監査イベントを含めるには、以下の手順に従います。

1. 以下の方法で、ポリシー サーバ上のサンプル スクリプトをコピーします。
   a. 以下のディレクトリを開きます。

      policy_server_home¥audit¥samples

      注: 以下のディレクトリが *policy_server_home* 変数のデフォルトの場所です。

      - C:¥Program Files¥ca¥siteminder（Windows）
      - /opt/ca/siteminder（UNIX、Linux）

   b. 以下のファイルを探します。
      - Harvest.bat（Windows 用）
      - Harvest.sh（UNIX、Linux 用）
      - ProcessAudit.pl
      - Categories.txt

   c. 上記のファイルを以下のディレクトリにコピーします。

      policy_server_home¥audit
2. （オプション）ProcessAudit.pl スクリプトをカスタマイズします。

3. 次回にスケジュールされた XPSAudit コマンドの実行の後に、監査ログのコピーがカンマ区切り値（CSV）形式で作成され、.TMP ファイルとして以下のディレクトリに格納されます。

   policy_server_home¥audit_R6tmp

   注: .tmp ファイルに手動で生成される必要があるイベントがある場合は、policy_server_home¥audit ディレクトリで以下のコマンドを実行します。

   ```
   ProcessAudit.pl <Transaction id>
   ```

   smobjlog4 データベース テーブルには、以下の 11 の属性と値が含まれています。最初の 8 つのみが .TMP ファイルに生成されます。

   ```
   sm_timestamp        DATE DEFAULT SYSDATE NOT NULL,
   sm_categoryid       INTEGER DEFAULT 0 NOT NULL,
   sm_eventid          INTEGER DEFAULT 0 NOT NULL,
   sm_hostname         VARCHAR2(255) NULL,
   sm_sessionid        VARCHAR2(255) NULL,
   sm_username         VARCHAR2(512) NULL,
   sm_objname          VARCHAR2(512) NULL,
   sm_objoid           VARCHAR2(64) NULL,
   sm_fielddesc        VARCHAR2(1024) NULL,
   sm_domainoid        VARCHAR2(64) NULL,
   sm_status           VARCHAR2(1024) NULL
   ```

4. ポリシー サーバの上記のディレクトリから、監査データベースをホストしているサーバに .TMP ファイルをコピーします。

5. .TMP ファイルの CSV 形式の内容をデータベース スキーマにマップするため、以下のファイルのいずれか 1 つを作成します。

   - *control_file_name*.ctl（Oracle データベースの制御ファイル）
   - *format_file_name*.fmt（SQL Server データベースの形式ファイル）

   注: 詳細については、データベース ベンダーが提供するマニュアルまたはオンライン ヘルプを参照してください。

6. 監査データベースをホストしているサーバで、以下のコマンドのうち、データベースのタイプに適したほうのコマンドを実行します。

   - sqlldr（Oracle データベース用）
   - bcp（SQL Server データベース用）

   注: 詳細については、データベース ベンダーが提供するマニュアルまたはオンライン ヘルプを参照してください。

7. コマンドが完了したら、レポート サーバを使用して、管理イベントのレポートを生成します。

   管理監査イベントはレポートの中に表示されます。

Windows で ODBC 監査ログの内容をテキストベースの監査ログにミラーリングする

SiteMinder 監査ログをテキスト ファイルとして保存する場合、それらのファイルにはデフォルトで、利用可能なフィールドの部分的なリストが含まれます。監査ログが記録されるテキスト ファイルに利用可能なフィールドをすべて含める場合は（ODBC 監査データベースと同じように）、ポリシー サーバにレジストリ キーを追加できます。

ODBC 監査ログの内容をテキストベースの監査ログにミラーリングする方法

1. レジストリ エディタを開きます。
2. 以下の場所を展開します。

   `HKEY_LOCAL_MACHINE¥Netegrity¥SiteMinder¥CurrentVersion¥Reports¥`
3. 以下の名前を持つ新しい DWORD 値を作成します。

   `Enable Enhance Tracing`
4. この値を 1 に設定します。この設定を将来無効にする場合は、値を 0 に戻します。
5. ポリシー サーバを再起動します。

   ODBC 監査ログの内容が、テキストベースの監査ログに表示されます。

Solaris で ODBC 監査ログの内容をテキストベースの監査ログにミラーリングする

SiteMinder 監査ログをテキスト ファイルとして保存する場合、それらのファイルにはデフォルトで、利用可能なフィールドの部分的なリストが含まれます。監査ログが記録されるテキスト ファイルに利用可能なフィールドをすべて含める場合は(ODBC 監査データベースと同じように)、ポリシー サーバにレジストリ キーを追加できます。

ODBC 監査ログの内容をテキストベースの監査ログにミラーリングする方法

1. 以下のファイルを開きます。

   ```
   sm.registry
   ```

2. 次の行を検索します。

   ```
   -
   HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥CurrentVersion¥Reports=25089
   ```

3. この行の下に、以下のテキストで構成される新しい行を追加します。

   ```
   - Enable Enhance Tracing= 0x1; REG_DWORD
   ```

   注: この機能を将来無効にする場合は、0x1 を 0x0 に変更します。

4. ポリシー サーバを再起動します。

   ODBC 監査ログの内容が、テキストベースの監査ログに表示されます。

システム ログへの問題記録のレポート

監査ログを準備または実行しているときに発生する可能性のある例外について、その情報を Windows イベント ログ ビューアに記録するようポリシー サーバを設定できます。この設定により、デバッグ ログが無効になっている場合に、本稼働環境でそのような情報を見逃さないようにすることができます。この機能を設定するには、CategoryCount レジストリ キーの値を 7 に設定します。

CategoryCount レジストリ キーは次の場所にあります。

```
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥Eventlog¥Application
¥SiteMinder
```

これらのイベントは、イベント ログ カテゴリの ObjAuditLog および AccessAuditLog の下に記録されます。

オブジェクトが作成、更新、または削除されると、SiteMinder はオブジェクト イベントをコールします。SiteMinder オブジェクト監査ログを準備/実行する際に発生した例外は、Windows イベント ビューアの「ObjAuditLog」カテゴリ下に記録されます。

アクセス イベントはユーザ関連アクティビティによって発生し、認証、許可、管理、アフィリエイトのアクティビティのコンテキストで呼び出されます。SiteMinder アクセス監査ログを準備/実行する際に発生した例外は、Windows イベント ビューアの「AccessAuditLog」カテゴリ下に記録されます。

第 8 章: ポリシー サーバ プロファイラの設定

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 サーバ プロファイラの設定

ポリシー サーバ プロファイラを使用すると、ポリシー サーバの内部診断と処理機能をトレースできます。

プロファイラを設定する方法

1. ポリシーサーバー管理コンソールを起動します。

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

2. [プロファイラ]タブをクリックします。

   注: このタブ上での設定およびコントロールの詳細については、[ヘルプ]-[管理コンソール ヘルプ]をクリックしてください。

3. [プロファイリングの有効化]オプションを設定して、プロファイリングを有効にします。

4. プロファイラの設定を選択するには、以下のいずれかを実行します。

   - [設定ファイル]ドロップダウン リストに示されるデフォルトの smtracedefault.txt ファイルによって指定されるプロファイラ設定を受け入れます。
   - この管理セッションですでに選択されている別の設定ファイルを[設定ファイル]ドロップダウン リストから選択します。
   - [参照]ボタンをクリックして、別の設定ファイルを選択します。

5. プロファイラの設定ファイルに格納されているプロファイラ設定を変更し、その変更内容を同じファイルまたは新しいファイルに保存するには、[環境設定]ボタンをクリックして[ポリシー サーバ プロファイラ]ダイアログ ボックスを開きます。
6. [出力]グループ ボックスに示されている設定を調整して、ポリシー サーバ プロファイラによって生成される情報の出力形式を指定します。
7. [適用]をクリックして、変更内容を保存します。

注:

プロファイラ設定に対する変更は自動的に有効になります。ただし、ポリシー サーバを再起動すると、新しい出力ファイル(プロファイラでファイル出力が設定されている場合)が作成されます。既存のプロファイラ出力ファイルは、バージョン番号と共に自動的に保存されます。例:

```
smtracedefault.log.1
```

ロギング機能またはトレース機能の設定に対する変更がプロファイラ出力ファイルに関係がない場合(Windows でのコンソール ロギングの有効化または無効化など)、既存のファイルには新しい出力が追加され、そのバージョンは保存されません。

ポリシー サーバはデフォルトで、最大 10 個の出力ファイルを保持します(現在のファイルと 9 個のバックアップ ファイル)。10 個のファイル制限を超えると、古いファイルは新しいファイルに自動的に置き換えられます。保持するファイルの数を変更するには、TraceFilesToKeep DWORD レジストリ設定で希望する 10 進数を指定します。TraceFilesToKeep レジストリ設定は、以下の場所で作成される必要があります。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥CurrentVersion¥
LogConfig¥TraceFilesToKeep
```

プロファイラ設定の変更

ポリシー サーバがトレースするコンポーネントやデータ フィールドを指定したり、トレースの出力にフィルタを適用してプロファイラが特定のコンポーネントまたはデータ フィールドの特定の値だけを取得するように設定したりできます。

プロファイラを設定する方法

1. ポリシーサーバー管理コンソールを起動します。

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

2. [プロファイラ]タブをクリックします。

   注: このタブ上での設定およびコントロールの詳細については、[ヘルプ]-[管理コンソール ヘルプ]をクリックしてください。

3. [環境設定]ボタンをクリックします。

   注: このボタンは、[プロファイリングの有効化]チェック ボックスをオンにしたときだけ有効になります。

   [ポリシー サーバ プロファイラ]ダイアログ ボックスが開きます。

4. オプションで、特定のトレース タスクに適したコンポーネントおよびデータ フィールドの事前定義済みセットを含むプロファイラ テンプレート ファイルを[テンプレート]ドロップダウン リストから選択します。

   general_trace.template

   全般的な広範囲のトレース用オプションを提供します。

   authentication_trace.template

   ユーザ認証のトレース用オプションを提供します。

   authorization_trace.template.txt

   ユーザ許可のトレース用オプションを提供します。

   プロファイラ テンプレートは、プロファイラ設定の出発点として使用することもできます。テンプレートをロードしたら、テンプレートによって指定されるコンポーネントとデータ フィールドを手動で変更すると共に、データ フィルタを適用できます。

5. トレース オプションを確認または設定するには、以下の 1 つ以上の操作を行います。

   - コンポーネントの選択 -- [コンポーネント]タブで、トレースするコンポーネント(ポリシー サーバによって実行されるアクション)を指定します。

- データ フィールドの選択 -- [データ]タブで、トレースするデータ フィールド(タスク完了のためにポリシー サーバによって使用される実際のデータ)を指定します。
- フィルタの追加 -- [フィルタ]タブで、トレース処理に情報を追加する、またはトレース処理から情報を除外するデータ フィルタを指定します。

6. 新しい設定を保存するには、以下のいずれかを実行します。
   - 現在選択している設定ファイルに設定を保存するには、[OK]をクリックします。
   - 新しい設定ファイルに設定を保存するには、[ファイル]-[名前を付けて保存]を選択し、新しいテキスト ファイルを指定します。
7. [ファイル]-[閉じる]を選択してプロファイラを閉じ、ポリシー サーバ管理コンソールに戻ります。
8. [構成ファイル]フィールドの右にある[参照]ボタンをクリックします。

Windows 環境でのプロファイラ コンソールの出力に関する問題の回避

Windows 環境のポリシー サーバでは、コンソールのデバッグを有効にしたときに発生する問題を回避するために、簡易編集モードと挿入モードを無効にする必要があります。簡易編集モードと挿入モードは、Windows のコマンドプロンプトウィンドウで有効にできる機能です。

簡易編集モードと挿入モードを無効にする方法

1. コマンドプロンプトウィンドウを起動します。
2. ウィンドウのタイトルバーを右クリックして、プルダウンメニューを表示します。
3. [プロパティ]を選択します。
4. [簡易編集モード]または[挿入モード]がオンになっていたら、どちらもオフにします。
5. [OK]をクリックします。

プロファイラトレース ファイルの保持ポリシーの設定

ポリシー サーバはデフォルトで、最大 10 個の出力ファイルを保持します（現在のファイルと 9 個のバックアップ ファイル）。10 個のファイル制限を超えると、古いファイルは新しいファイルに自動的に置き換えられます。保持するファイルの数を変更するには、TraceFilesToKeep DWORD レジストリ設定で希望する 10 進数を指定します。TraceFilesToKeep レジストリ設定は、次の場所で行う必要があります。

HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥CurrentVersion¥LogConfig¥TraceFilesToKeep

プロファイラトレース ログ ファイルの手動によるロールオーバー

ポリシー サーバでは、smpolicysrv コマンドを使用して、ポリシー サーバ プロファイラのトレース ログ ファイルを手動でロールオーバーできます。

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している場合は、管理者としてシステムにログインしている場合でも、管理者権限でコマンド ライン ウィンドウを開きます。詳細については、お使いの SiteMinder コンポーネントのリリース ノートを参照してください。

ファイルへのトレース ロギングを開始するには、以下のコマンドを実行します。

```
smpolicysrv -starttrace
```

このコマンドは、トレース ファイルへのログの記録を開始し、コンソールへのトレース ロギングには影響しません。ポリシー サーバが稼働していない場合は、エラーを発行します。

ポリシー サーバがすでにトレース データのログを記録している場合に –starttrace コマンドを実行すると、現在のトレース ファイルの名前が変更され（ファイル名の最後にタイム スタンプを付けて *file_name*.YYYYMMDD_HHmmss.*extension* の形式で）、元の名前を持つ新しいトレース ファイルが作成されます。たとえば、ポリシー サーバ管理コンソールの［プロファイラ］タブでのトレース ファイル名が C:¥temp¥smtrace.log である場合、新しいファイルが生成されると、古いファイルは c:¥temp¥smtrace.20051007_121807.log として保存されます。タイム スタンプは、ファイルが 2005 年 10 月 7 日の午後 12:18 に作成されたことを示しています。

ポリシー サーバ管理コンソールの[プロファイラ]タブでファイルのトレース機能を有効にしていない場合は、このコマンドを実行しても何も起こりません。

ファイルへのトレース ロギングを中止するには、以下のコマンドを実行します。

```
smpolicysrv -stoptrace
```

このコマンドは、ファイルへのログの記録を中止し、コンソールへのトレース ロギングには影響しません。ポリシー サーバが稼働していない場合は、エラーを発行します。

注: Windows システムでは、リモート デスクトップまたはターミナル サービス ウィンドウから smpolicysr コマンドを実行しないでください。smpolicysrv コマンドはプロセス間通信に依存します。この通信は、リモート デスクトップまたは[ターミナル サービス]ウィンドウから smpolicysrv プロセスを実行した場合には機能しません。

指定された間隔でのトレース ファイルの動的なロールオーバー

指定された間隔でトレース ファイルをロールオーバーするためのスクリプトを作成することもできます。たとえば、新しいトレース ファイルを毎時間作成するには、以下のようなスクリプトを作成します。

```
smpolicysrv -starttrace
repeat forever
wait 1 hour
smpolicysrv -starttrace
end repeat
```

これは、ポリシー サーバ管理コンソールの[ログ]タブにある時間単位のロールオーバー オプションに似ています。

第 9 章: 管理ジャーナルとイベント ハンドラの設定

このセクションには、以下のトピックが含まれています。

管理ジャーナルとイベント ハンドラの概要

ポリシー サーバの管理ジャーナルの設定では、管理上の変更をポリシー サーバに適用する頻度、および適用した変更のリストがポリシー サーバによって保持される期間を指定できます。

イベント ハンドラは、特定のイベントを処理するためにポリシー サーバに追加できる共有ライブラリです。

ポリシー サーバの高度な設定

ポリシー サーバの高度な設定方法

1. ポリシーサーバー管理コンソールを起動します。

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

2. [詳細設定]タブをクリックします。

   注: このタブ上での設定およびコントロールの詳細については、[ヘルプ]-[管理コンソール ヘルプ]をクリックしてください。

3. [管理ジャーナル]グループ ボックスに示される設定を調整して、管理上の変更をポリシー サーバに適用する頻度、および適用した変更のリストがポリシー サーバによって保持される期間を設定します。

4. [適用]をクリックして、変更内容を保存します。

イベント ハンドラ ライブラリの追加

SiteMinder ポリシー サーバにはイベント ハンドラ ライブラリを追加できます。

注: SiteMinder バイナリ ファイル（XPS.dll、libXPS.so、libXPS.sl）への書き込みアクセス許可がユーザにない場合は、管理者が 管理 UI または XPSSecurity ツールを使用して、関連する XPS コマンド ライン ツールを使用する権限を付与する必要があります。

イベント ハンドラ ライブラリを追加する方法

1. ポリシー サーバでコマンド ラインを開き、以下のコマンドを入力します。

   ```
   xpsconfig
   ```

   ツールが起動し、このセッションのログ ファイルの名前が表示されます。また、選択項目のメニューが開きます。

2. 次のコマンドを入力します。

   ```
   xps
   ```

   オプションのリストが表示されます。

3. 次のコマンドを入力します。

   ```
   5 (AuditSMHandlers)
   ```

   イベント ハンドラ ライブラリの設定が表示されます。

4. 「C」と入力し、追加するイベント ハンドラ ライブラリのパスとファイル名を入力します。ライブラリの場所が複数ある場合はカンマで区切ります。

   イベント ハンドラ ライブラリの設定が表示されます。追加した値は「保留中の値」として設定の下に表示されます。

5. 以下の手順を実行します。

   a. 2 回「Q」と入力します。

   b. 「L」と入力します。

   c. 「Q」と入力して XPS セッションを終了します。

   変更が保存され、コマンド プロンプトが表示されます。

第 10 章: グローバル設定の調整

このセクションには、以下のトピックが含まれています。

ユーザ追跡の有効化

[ポリシー サーバ]-[グローバル ツール]から、ユーザ追跡を有効または無効にすることができます。ユーザ追跡を有効にすると、SiteMinder Web エージェントは GUID (グローバルな固有識別子)を cookie に保存します。匿名認証方式によって保護されているリソースにユーザが初めてアクセスするとき、Web エージェントはユーザの GUID を含む cookie を作成します。各 GUID は一意の値であるため、匿名ユーザの追跡および Web コンテンツのカスタマイズに利用できます。

アフィリエイトエージェントにはユーザ追跡が必要です。アフィリエイト エージェントを含むネットワークで SiteMinder を使用している場合は、次に説明する手順に従ってユーザ追跡を有効にしてください。

ユーザ追跡を有効にする方法

1. 管理 UI にログインします。
2. [管理]-[ポリシー サーバ]-[グローバル ツール]をクリックします。

   [グローバル ツール]ペインが開きます。
3. [グローバル設定]グループ ボックスの[ユーザ追跡を有効にする]を選択します。
4. [サブミット]をクリックします。

   これで、ポリシー サーバのユーザ追跡が有効になりました。

ネストされたセキュリティの有効化

管理 UI の[ポリシー サーバ]-[グローバル ツール]ペインでは、ネストされたセキュリティを有効または無効にすることができます。この機能は旧バージョンの SiteMinder に対する下位互換性を提供します。

ネストされたセキュリティ オプションを有効にする方法

1. 管理 UI にログインします。
2. [管理]-[ポリシー サーバ]-[グローバル ツール]をクリックします。

   [グローバル ツール]ペインが開きます。
3. [ネストされたセキュリティを有効にする]チェック ボックスをオンにします。
4. [サブミット]をクリックします。

   ネストされたセキュリティが有効になります。

Active Directory 統合の拡張の有効化

Active Directory 2000 および Active Directory 2003 には、Windows ネットワーク オペレーティング システム(NOS)に特有で、LDAP 標準によって必要とされない、ユーザ属性とドメイン属性がいくつかあります。属性は以下のとおりです。

- accountExpires
- userAccountControl
- pwdLastSet
- unicodePwd
- lastLogon
- lastLogonTimestamp
- badPasswordTime
- badPwdCount
- lockoutTime
- lockoutDuration
- pwdMaxAge

Active Directory をユーザ ストアとして使用するようにポリシー サーバを設定する場合は、管理 UI の[ポリシー サーバ]-[グローバル ツール]にある[Active Directory 統合を拡張]を有効にします。このオプションでは、Active Directory のユーザ属性と、SiteMinder でマップされるユーザ属性を同期することによって、ポリシー サーバのユーザ管理機能と Active Directory のパスワード サービスとの間の統合を強化します。

注: この機能は ADAM ではサポートされていません。

Active Directory 統合の拡張を有効にする方法

1. 管理 UI にログインします。
2. [管理]-[ポリシー サーバ]-[グローバル ツール]をクリックします。

   [グローバル ツール]ペインが開きます。
3. [Active Directory 統合を拡張]を選択します。デフォルトでは、この機能は無効になっています。

   注: この機能を有効にした後、AD ユーザ ストアを変更するには管理者クレデンシャルが、AD 属性を更新するには管理者権限がそれぞれ必要になります。これらのクレデンシャルおよび権限を持っていない場合は、エラー メッセージが返されます。
4. [サブミット]をクリックします。

   Active Directory 統合の拡張が有効になります。
5. [インフラストラクチャ]タブの[ユーザ ディレクトリ]ダイアログ ボックスに移動します。
6. 編集する Active Directory オブジェクトを開きます。
7. [ルート]フィールドに、ユーザ ディレクトリ ルートとして Windows ドメインのデフォルトの DN を入力します。以下に例を示します。

   ```
   dc=WindowsDomain,dc=com
   ```

   注: [ルート]フィールドに別の値を設定すると、AD 固有の機能は動作しない場合があります。
8. [サブミット]をクリックします。

注: Active Directory 統合の拡張を AD 2000 で有効にした場合、非アクティブ期間を過ぎた後にアカウントを無効にするパスワード ポリシーは正常に機能しません。そのため、ユーザ アカウントの非アクティブ機能の統合は AD 2000 ではサポートされていません。代わりに AD 2003 を使用してください。

第 11 章: キャッシュ管理

このセクションには、以下のトピックが含まれています。

キャッシュ管理の概要

SiteMinder には、いくつかのキャッシュがあります。最近アクセスしたデータ (ユーザ許可など) のコピーを保持するようにキャッシュを設定して、システムのパフォーマンスを向上させることができます。これらのキャッシュは、使用している環境のデータの特性に合わせて設定する必要がありますが、定期的に手動でクリアすることが必要になる場合もあります。

SiteMinder 環境では、ポリシー サーバの以下のキャッシュを保持するように設定できます。

- *ユーザ許可キャッシュ* - ポリシーのユーザ部分を基にしたユーザ識別名 (DN) を格納します。ユーザのグループ メンバシップも含まれます。

また、SiteMinder は、各 SiteMinder エージェント マシン上にエージェント キャッシュを保持します。エージェントキャッシュには、次の 2 つのコンポーネントがあります。

- エージェント リソース キャッシュ - さまざまなレルムによって保護されているリソースへのアクセス記録を格納します。エージェントが既に処理したリクエストのリソースに関する情報を持っているため、このキャッシュによってエージェントとポリシー サーバの通信がスピードアップします。
- エージェント ユーザ キャッシュ - ユーザの暗号化されたセッション チケットを保持します。ユーザ、レルム、リソース情報を格納し、セッション キャッシュとして動作します。ユーザがアクセスするレルムに指定されたタイムアウト値に基づいて、このキャッシュのエントリが無効になります。

キャッシュの設定

ポリシー サーバ キャッシュのリフレッシュ ステータスを表示し、FSS 管理 UI または 3 つの smpolicysrv コマンド ライン オプションによって、キャッシュのフラッシュを無効または有効にすることができます。これらのオプションを使用してキャッシュのフラッシュを一時停止および再開すると、ポリシー評価の問題を解決することができます。 これらのコマンドは、中央管理ポリシー サーバによって、すべてのセカンダリ ポリシー サーバに対して発行されます。

注: ポリシー サーバ コマンドはスレッド管理モデルによって処理されるため、キャッシュ ステータスの変更は smps.log ファイルにすぐには表示されません。

FSS 管理 UI によってキャッシュ ステータスを管理する方法

1. FSS 管理 UI にログインします。
2. メニュー バーから[ツール]-[キャッシュの管理]を選択します。

   SiteMinder [キャッシュ管理]ダイアログ ボックスが表示されます。
3. [キャッシュの更新]グループ ボックスでキャッシュ ステータスを確認します。

   無効: キャッシュのフラッシュは無効です。

   有効: キャッシュのフラッシュは有効です。
4. (オプション)[有効]/[無効]ボタンおよび[OK]をクリックして、キャッシュ ステータスを変更します。

コマンド ライン インターフェースによってキャッシュ ステータスを管理する方法

1. 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している場合、管理者としてシステムにログインしていても、必ず管理者権限でコマンド ライン ウィンドウを開くようにしてください。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. 以下のいずれかのコマンドを入力します。

   smpolicysrv -disablecacheupdates

   キャッシュのフラッシュを無効にします。

   smpolicysrv -enablecacheupdates

   キャッシュのフラッシュを有効にします。

smpolicysrv -statuscacheupdates

ポリシー サーバ キャッシュのリフレッシュ ステータスをログ ファイル smps.log に報告します。

無効: キャッシュのフラッシュは無効です。

有効: キャッシュのフラッシュは有効です。

注: Windows システムでは、リモート デスクトップまたはターミナル サービス ウィンドウから smpolicysr コマンドを実行しないでください。smpolicysrv コマンドはプロセス間通信に依存します。この通信は、リモート デスクトップまたは[ターミナル サービス]ウィンドウから smpolicysrv プロセスを実行した場合には機能しません。

キャッシュのクリア

SiteMinder オブジェクトを変更すると、適切なキャッシュ エントリが自動的にクリアされます。キャッシュ設定では、管理変更の適用間隔も指定します。非常に重要な変更(機密情報に対するアクセス権限の変更など)を行う場合は、SiteMinder キャッシュを手動でクリアするオプションがあります。この手動の手順により、キャッシュに格納されている情報に基づき、許可されていないユーザは保護されたリソースにアクセスできないようにすることができます。

キャッシュ管理の機能は、管理 UI の[ポリシー サーバ]-[グローバル ツール]ペインからアクセスできます。この機能は、以下のキャッシュを手動でクリアすることにより、SiteMinder データの更新を強制します。

すべてのキャッシュ

ユーザ セッション、リソース情報、ユーザ ディレクトリのキャッシュ(CRL を含む)など、すべてのキャッシュをクリアできます。

ユーザ セッションのキャッシュ

保護されたリソースにユーザがアクセスしようとするときに再認証を強制できます。

リソース キャッシュ

リソースに関するキャッシュ情報をクリアできます。

すべてのキャッシュのクリア

管理者は、キャッシュ管理のオプションを使用して、すべてのキャッシュの内容をクリアすることができます。すべてのキャッシュをクリアすると、Web サイトのパフォーマンスが低下する可能性があります。これは、キャッシュをクリアした直後に、すべてのリクエストがユーザディレクトリとポリシーストアから情報を取得するためです。ただし、重要なユーザ権限とポリシーの変更内容を直ちに有効にする場合は、このアクションが必要となります。

キャッシュ管理の機能を使用できるのは、ユーザの管理権限またはシステムとドメイン オブジェクトの管理権限のどちらかを持っている管理者だけです。[すべてクリア] ボタンは、システムとドメインオブジェクトの管理権限を持つ管理者だけが使用できます。このメニュー項目が使用できない場合は、ログインに使用した管理者アカウントの権限が、キャッシュ機能へのアクセスに対して適切でない可能性があります。

1 つのポリシー ストアを参照する 2 つのポリシー サーバが構成されている場合は、[すべてクリア]コマンドにプライマリ(オブジェクト キャッシュ)が含まれるようにすることができます。これによって、プライマリ キャッシュとセカンダリ キャッシュの両方がポリシー ストアから再構築されます。この機能を有効にするには、レジストリに以下のエントリを追加する必要があります。

レジストリ名 - FlushObjCache
タイプ - DWORD
値 - 0 (デフォルト)
場所 -
HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥CurrentVersion¥ObjectStore

すべてのキャッシュをクリアする方法

1. 管理 UI にログインします。
2. [管理]-[ポリシー サーバ]-[キャッシュ管理]をクリックします。

3. [すべてのキャッシュ]グループ ボックスで、[すべてクリア]をクリックします。

   注: [すべてクリア]ボタンは、ユーザの管理権限と SiteMinder オブジェクトの管理権限の両方を持つ管理者だけが使用できます。

   ポリシー サーバと関連する SiteMinder エージェントがすべてのキャッシュをクリアします。この処理にはポリシー サーバのポーリング間隔で指定した時間の 2 倍近くかかり、その間にポリシー サーバはキャッシュの同期をとっています。

4. [サブミット]をクリックします。

   キャッシュがすべてクリアされます。

ユーザ セッション キャッシュのクリア

ユーザ認証が正常に終了すると、ポリシー サーバは認証されたユーザに対してセッションを開始します。ユーザのセッション中、Web エージェントは許可情報をユーザ キャッシュに保存します。ただし、ユーザのアクセス権限を変更する場合は、ポリシー サーバで Web エージェント キャッシュ内のユーザ セッション情報を強制的にクリアする必要があります。これは、管理 UI の[グローバル ツールの変更]ペインから行うことができます。

ユーザ セッションをクリアする方法

1. 管理 UI にログインします。
2. [管理]-[ポリシー サーバ]-[キャッシュ管理]をクリックします。
   [グローバル ツールの変更]ペインが表示されます。

3. [ユーザ セッションのキャッシュ]グループ ボックスで、以下のオプションのいずれかを選択します。

   すべて

   ユーザ キャッシュからすべてのユーザ セッションをクリアします。

   特定のユーザ DN

   ユーザ キャッシュから特定の DN をクリアします。

   このラジオ ボタンを選択する場合は、削除する DN が含まれるユーザ ディレクトリを[ディレクトリ]ドロップダウン リストから選択し、その識別名を[DN]フィールドに入力します。グループの DN ではなく、ユーザの DN を指定する必要があります。DN がわからない場合は、[検索] をクリックして DN を検索します。

   注: ユーザ キャッシュをクリアするオプションは、ユーザの管理権限を持つ管理者だけが使用できます。

4. [クリア]をクリックします。

   オンにしたラジオボタンによって、SiteMinder がすべてのユーザまたは特定の DN をユーザキャッシュからクリアします。この処理にはポリシー サーバのポーリング間隔で指定した時間の 2 倍近くかかり、その間にポリシー サーバはキャッシュの同期をとっています。

5. [サブミット]をクリックします。
   ユーザ セッションのキャッシュがクリアされます。

リソース キャッシュのクリア

SiteMinder Web エージェントは、ユーザがアクセスした特定のリソースに関する情報をリソース キャッシュに格納します。リソース キャッシュには以下の情報が記録されます。

- ユーザがアクセスしたリソースの記録
- リソースが SiteMinder によって保護されているかどうか
- リソースが保護されている場合の保護方法

ルールやレルムを変更すると、その変更をすぐに有効にする必要が生じることがあります。そのような場合は、リソースキャッシュをクリアしてください。

注: レルムまたは特定ポリシーのリソース キャッシュのクリアについては、「*ポリシー サーバ設定ガイド*」を参照してください。

リソース キャッシュをクリアする方法

1. 管理 UI にログインします。
2. [管理]-[ポリシー サーバ]-[キャッシュ管理]をクリックします。
3. [リソース キャッシュ]グループ ボックスで、[クリア]をクリックします。

   すべてのリソースキャッシュをクリアすると、強制的に Web エージェントからポリシー サーバへ許可リクエストが送信されます。この処理にはポリシー サーバのポーリング間隔で指定した時間の 2 倍近くかかり、その間にポリシー サーバはキャッシュの同期をとっています。

   注: 特定のポリシー ドメインに対してドメイン オブジェクトの管理権限を持つ管理者がすべてのリソース キャッシュをクリアすると、そのポリシー ドメイン内のレルムに対するキャッシュだけがクリアされます。
4. [サブミット]をクリックします。

   リソース キャッシュがクリアされます。

ポリシー サーバのリクエスト キューのクリア

SiteMinder エージェントからのリクエストは、一定の期間が経過するとタイムアウトに設定されます。ただし、ポリシー サーバでは、タイムアウトになったリクエストを含むキュー内のすべてのエージェント リクエストを、受信した順序で処理します。以下の状況が発生した場合、ポリシー サーバが処理するよりも早く、キューがエージェント リクエストでいっぱいになる可能性があります。

- ポリシー サーバとポリシー ストア間またはポリシー サーバとユーザ ストア データベース間のネットワーク遅延
- ポリシー ストアまたはユーザ ストア データベースに対する高い負荷
- ポリシー サーバのパフォーマンスの問題

ポリシー サーバのリクエスト キューがエージェント リクエストでいっぱいになった場合は、タイムアウトになったエージェント リクエストをキューからクリアして、現在のエージェント リクエストだけを残すことができます。この手順を使用するのは、以下の場合に限られます。

1. ポリシー サーバ キュー内で待機しているエージェント リクエストがタイムアウトになった。
2. 1 つ以上のエージェントがタイムアウトしたリクエストを再送信して、キューがいっぱいになった。

重要: 通常の動作条件下では -flushrequests を使用しないでください。

ポリシー サーバのリクエスト キューをクリアする方法

1. ポリシー サーバでコマンド プロンプトを開きます。
2. 以下のコマンドを実行します。

   ```
   smpolicysrv -flushrequests
   ```

   リクエスト キューがクリアされます。

注: Windows システムでは、リモート デスクトップまたはターミナル サービス ウィンドウから smpolicysr コマンドを実行しないでください。smpolicysrv コマンドはプロセス間通信に依存します。この通信は、リモート デスクトップまたは[ターミナル サービス]ウィンドウから smpolicysrv プロセスを実行した場合には機能しません。

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

ポリシー ストア キャッシュのクリア

ポリシー ストア キャッシュをクリアすると、現在のエントリがすべてクリアされ、ポリシー ストア内のすべてのエントリによってキャッシュが再ロードされます。ポリシー ストア キャッシュのクリア時、キャッシュはオフラインになります。ポリシー サーバでは、ポリシー ストアを一時停止または直接使用して、ポリシーに関する決定を行います。

ポリシー ストア キャッシュをクリアする方法

1. レジストリ エディタを開きます。
2. ¥¥HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥CurrentVersion¥ObjectStore に移動します。
3. 以下の値を持つ FlushObjCache レジストリ キーを作成します。

   タイプ: DWORD

   値: 1 または 0

1

キーを有効にします。キーを有効にすると、[キャッシュ管理]ダイアログボックスの[すべてクリア]ボタンを使用して、ポリシー ストア キャッシュを含む、ポリシー サーバおよび関連する SiteMinder エージェントのキャッシュをすべてクリアできます。

0

キーを無効にします。キーを無効にすると、[キャッシュ管理]ダイアログボックスの[すべてクリア]ボタンを使用して、ポリシー ストア キャッシュを除く、ポリシー サーバおよび関連する SiteMinder エージェントのキャッシュをすべてクリアできます。

注: 値がない場合、キーは無効になります。

4. すべてのキャッシュをクリアするには、管理 UI の[キャッシュ管理]ダイアログボックスを使用します。

第 12 章: ユーザセッションとユーザアカウントの管理

このセクションには、以下のトピックが含まれています。

ユーザセッションとユーザアカウントの管理の前提条件

ポリシー サーバは、ユーザセッションとユーザアカウントを管理する機能を備えています。この機能を使用すると、セッション キャッシュをクリアしたり、ユーザを有効および無効にしたり、ユーザごとにパスワードを管理したりできます。

ユーザ セッションとユーザ アカウントを管理するには、以下の前提条件を満たす必要があります。

- ユーザの管理権限を持つ管理者アカウントを所有していること。
- ユーザアカウントを有効または無効にする場合は、ユーザ情報を含むユーザディレクトリのユーザの無効化に関する属性が設定されていること。
- パスワードの変更またはパスワード変更の強制を行う場合は、ポリシー サーバでパスワードポリシーが設定されており、ユーザ情報を含むユーザディレクトリのパスワードデータに関する属性が設定されていること。

注: 管理者権限、ユーザ ディレクトリ、およびパスワード ポリシー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。

ユーザの有効化と無効化

ユーザがログインして認証されると、SiteMinder は、ユーザセッションを開始します。SiteMinder は、ユーザ属性をユーザ セッション キャッシュに格納します。ユーザを無効にすると、エージェントは、セッション キャッシュをクリアして、ユーザ ID およびセッション情報を削除します。

ユーザが現在のセッションで追加のリソースにアクセスしようとする場合、Web エージェントのキャッシュからはユーザのデータがなくなっているため、エージェントはポリシー サーバと通信して、ユーザの再認証を試みます。ポリシー サーバは、このユーザがユーザ ディレクトリで無効になっていることを確認して、エージェントの認証リクエストを拒否するため、セッションが終了します。

ユーザ アカウントを有効または無効にする方法

1. 管理 UI にログインします。
2. [管理]-[ユーザ]-[ユーザ アカウントの管理]をクリックします。

   [ユーザ アカウントの管理]ペインが開きます。
3. 有効または無効にするユーザを含むディレクトリのユーザ ディレクトリ接続を選択します。
4. [検索] ボタンをクリックします。

   [ディレクトリ ユーザ]ペインが表示されます。
5. [ユーザ/グループ]グループ ボックスに検索条件を入力し、[実行]をクリックして、有効または無効にするユーザの検索を行います。検索条件は、選択したユーザ ディレクトリのタイプによって決まります。属性と値を入力するか、式を入力できます。検索条件をクリアするには、[リセット]をクリックします。

   [ユーザ/グループ]ダイアログ ボックスに検索結果が表示されます。
6. 検索結果のリストからユーザを 1 人選択します。

   [ユーザの状態の変更]グループ ボックスにはボタンが含まれます。このボタンのラベルは、ユーザが無効になっている場合は [有効] と、ユーザが有効になっている場合は [無効] と表示されています。
7. [有効] または [無効] をクリックします。

   選択したユーザのプロファイルの値が変更されて、ユーザが無効または有効にされます。

ユーザ パスワードを管理する方法

管理 UI の[ユーザ アカウントの管理]ペインでは、ユーザにパスワードの変更を強制したり、ユーザ パスワードを新しい値に変更したりできます。

ユーザにパスワードの変更を強制する前に、パスワードポリシーが存在していることを確認してください。パスワードポリシーが定義されていないと、ユーザは自分自身のパスワードを変更できません。また、保護されたリソースにもアクセスできません。

ユーザにパスワードの変更を強制するとき、ユーザが SSL 接続を使用していないエージェントを経由してリソースにアクセスしている場合は、ユーザの新しいパスワード情報は、安全性の低い接続を経由して受信されます。パスワードを安全に変更するには、パスワード変更時に SSL 接続を経由してユーザをリダイレクトするようにパスワードポリシーを設定します。

ユーザ パスワードを管理する方法

1. 管理 UI にログインします。
2. [管理]-[ユーザ]-[ユーザ アカウントの管理]をクリックします。
   [ユーザ アカウントの管理]ペインが開きます。
3. パスワード管理の対象となるユーザを含むディレクトリのユーザ ディレクトリ接続を選択します。
4. [検索] ボタンをクリックします。

   [ディレクトリ] ドロップダウンリストから選択したディレクトリタイプに関連した、ユーザディレクトリの検索ダイアログボックスが表示されます。
5. [ユーザ/グループ]グループ ボックスに検索条件を入力し、[実行]をクリックして、有効または無効にするユーザの検索を行います。検索条件は、選択したユーザ ディレクトリのタイプによって決まります。属性と値を入力するか、式を入力できます。検索条件をクリアするには、[リセット]をクリックします。

   [ユーザ/グループ]ダイアログ ボックスに検索結果が表示されます。
6. 検索結果のリストからユーザを 1 人選択します。
7. 選択したユーザの次回のログイン時にパスワードの変更を強制するには、[ユーザのパスワードをリセット]グループ ボックスの[パスワードの変更を強制]をクリックします。

8. ユーザのパスワードを新しい値に変更するには、[ユーザのパスワードの変更]グループ ボックスに新しいパスワードを入力します。確認のためにパスワードを再入力します。

   注: 指定するパスワードは、パスワード ポリシーによって制限されることはありませんが、ユーザのパスワード履歴に記録されます。

ユーザ許可の監査

Web エージェントの監査機能を使用して、ユーザ セッション キャッシュに格納されている正常に行われたユーザ許可を追跡し、記録することができます。これにより、ユーザの動作を追跡し、Web サイトでアプリケーションが使用される頻度を計測することができます。

このオプションを選択すると、Web エージェントは、ユーザがリソースへのアクセスをキャッシュから許可されるたびに、ポリシー サーバにメッセージを送信します。後で、ログレポートを実行して、各 SiteMinder セッションでのユーザの動作を表示させることができます。

監査が有効になっていない場合、Web エージェントは、認証と最初の許可のみを監査します。

注: 監査を有効にする方法については、「*Web エージェント設定ガイド*」を参照してください。

ユーザがリソースにアクセスすると、Web エージェントは、ユーザ名とアクセス情報を Web サーバのネイティブログファイルに自動的に記録します。監査ログには、ユーザ許可リクエストが成功するたびに Web エージェントが自動的に生成する固有のトランザクション ID が含まれています。また、SiteMinder がリソースへのユーザのアクセスを許可すると、エージェントは、この ID を HTTP ヘッダーに追加します。この後、トランザクション ID は、Web サーバ上のすべてのアプリケーションで利用できます。トランザクション ID は、Web サーバの監査ログにも記録されます。この ID を使用すると、ログを照合して、特定のアプリケーションに関するユーザの動作を調べることができます。

監査機能の出力を表示するには、管理 UI から SiteMinder レポートを実行します。

第 13 章: ポリシー サーバのクラスタ化

このセクションには、以下のトピックが含まれています。

クラスタ化されたポリシー サーバ

SiteMinder 環境のロードバランシング機能とフェイルオーバー機能は、高レベルのシステム可用性を実現し、SiteMinder エージェントからポリシー サーバへのリクエストの分散によってレスポンス時間を短縮させます。これらの機能にクラスタの定義を組み合わせることによって、システムの可用性とレスポンス時間はさらに向上します。

クラスタを使用しない従来のラウンドロビン方式のロードバランシングでは、リクエストが一連のサーバに均等に分散されます。ただし、この方法では、すべてのサーバが処理能力に関係なく同じ数のリクエストを受信するため、サーバの処理能力が異なる異機種環境では、最も効率的な方法であるとはいえません。

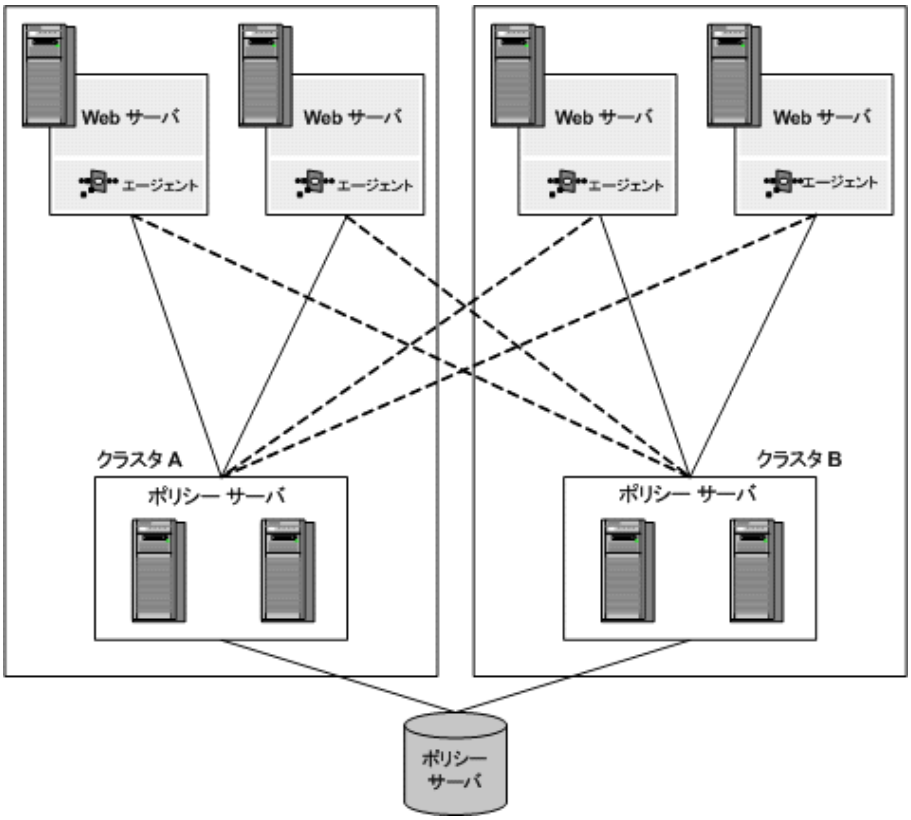
また、データセンターが地理的に離れた場所にあると、さらに効率が悪くなる場合があります。離れた場所にあるサーバへのリクエストの送信によって、ネットワーク通信のオーバーヘッドが増加することがあり、場合によっては、ネットワークの輻輳が発生します。

これらの問題を回避し、システムの可用性とレスポンス時間を向上させるために、ポリシー サーバと、ロードバランシングとフェイルオーバーを実行するように(ソフトウェアベース)設定された関連する Web エージェントのクラスタを定義することができます。

ポリシー サーバクラスタには、従来のロードバランシング/フェイルオーバー方式にはない次のような利点があります。

- 負荷は、サーバのレスポンス時間に基づいて、クラスタ内のサーバ間に動的に分散されます。
- クラスタは、クラスタ内の使用可能なサーバの数がしきい値(設定可能)を下回ったときに他のクラスタにフェイルオーバーするように設定できます。

以下の図は、2 つのクラスタを使用した単純な SiteMinder 環境を示しています。



クラスタ A とクラスタ B は、タイムゾーンの異なる離れた場所に配置されているものとします。独立したクラスタのそれぞれに Web エージェントとポリシー サーバを配置すると、離れた地域の間でのロードバランシングによるネットワークオーバーヘッドは、一方のクラスタのポリシー サーバがダウンし、もう一方のクラスタへのフェイルオーバーが必要になった場合にだけ発生します。

詳細情報:

フェイルオーバーのしきい値 (P. 121)
クラスタ化された環境の監視 (P. 141)

フェイルオーバーのしきい値

クラスタ化されたあらゆる SiteMinder 環境では、フェイルオーバーのしきい値を設定する必要があります。使用可能なポリシー サーバの数が、指定されたしきい値を下回ると、障害の発生したポリシー サーバクラスタで処理されることになっていたすべてのリクエストが、別のクラスタに転送されます。

フェイルオーバーのしきい値は、クラスタ内のポリシー サーバの割合 (%) で表されます。たとえば、4 つのポリシー サーバによるクラスタで、クラスタのフェイルオーバーのしきい値が 50% に設定されている場合、3 つのポリシー サーバがダウンすると、クラスタ障害となり、すべてのリクエストが次のクラスタにフェイルオーバーされます。

フェイルオーバーのしきい値のデフォルト設定は 0 です。この設定では、クラスタ内のすべてのサーバがダウンした場合にのみ、フェイルオーバーが発生します。

ハードウェア ロード バランシングの考慮事項

SiteMinder ポリシー サーバと Web エージェントの間でハードウェア ロード バランサを展開している場合は、以下の点を考慮します。

- ポリシー サーバ TCP ポートに対して TCP ハートビートまたはヘルス チェックを直接設定することはしません。ポリシー サーバの TCP ポートに対して直接適用されたハートビートおよびヘルス チェックは、その操作に悪影響を及ぼす可能性があります。
- ポリシー サーバの運用状況をテストするため、ロード バランサの包括的な機能を設計します。
- フェイルオーバーのアルゴリズムとして、Web エージェント上に 1 つのポリシー サーバを設定する場合、および複数のポリシー サーバを設定する場合の影響を比較します。

- Web エージェントとポリシー サーバのチューニングおよびモニタリングにおけるパフォーマンスと障害のシナリオを考慮します。
- プロキシ エージェントからポリシー サーバへの接続に対してロード バランサが設定されている場合、ロード バランサのタイムアウトおよびソケット状態を考慮します。

  注: Web エージェントとポリシー サーバの間にハードウェア ロード バランサを展開する詳細については、サポート サイト上で関連するナレッジ ベース記事(KB ID 21135)を参照してください。

詳細情報:

CAへの連絡先 (P. iii)

クラスタの設定

ポリシー サーバ クラスタは、ホスト設定オブジェクトの一部として定義されます。SiteMinder Web エージェントが初期化されると、ホスト設定オブジェクトの設定を使用してポリシー サーバとの通信が設定されます。

注: ホスト設定オブジェクトの詳細については、「*Web エージェント設定ガイド*」および「*ポリシー サーバ設定ガイド*」を参照してください。

クラスタを構成する方法

1. [インフラストラクチャ]タブを選択します。

   タスクのリストが表示されます。
2. [エージェント]-[ホスト設定の作成]を選択します。

   [ホスト設定の作成]ペインが表示されます。
3. [クラスタ] タブを選択します。
4. [クラスタ]グループ ボックスで、[追加]をクリックします。

   [クラスタのセットアップ]グループ ボックスが表示されます。

   注: フィールド、コントロール、およびそれぞれの要件の説明は、[ヘルプ]をクリックすると表示されます。
5. [ホスト]フィールドと[ポート]フィールドに、ポリシー サーバの IP アドレスとポート番号をそれぞれ入力します。

6. [クラスタへ追加]をクリックします。

   ポリシー サーバが [現在の設定] グループボックスのサーバ リストに表示されます。

7. 他のポリシー サーバをクラスタに追加するには、同じ手順を繰り返します。

8. [OK]をクリックして、変更を保存します。

   [ホスト設定]ペインに戻ります。ポリシー サーバ クラスタがテーブルにリスト表示されます。

9. [フェイルオーバーのしきい値パーセント]フィールドに、アクティブである必要のあるポリシー サーバの割合(%)を入力し、[適用]をクリックします。

   クラスタ内のアクティブなサーバの割合が、指定した割合を下回ると、クラスタは、クラスタのリスト内の次に使用可能なクラスタにフェイルオーバーします。この設定は、ホスト設定オブジェクトを使用するすべてのクラスタに適用されます。

   重要: [設定値]グループ ボックスで指定されたポリシー サーバは、クラスタ内で指定されたポリシー サーバによって上書きされます。クラスタを設定すると、[設定値]グループ ボックスで指定されたポリシー サーバは使用されなくなります。[設定値]グループ ボックス内のポリシー サーバ パラメータに適用する値について、クラスタ内のポリシー サーバは指定しないでください。クラスタを設定した後で、[設定値]グループ ボックスのポリシー サーバ パラメータを使用した単純なフェイルオーバー設定を優先してクラスタを削除する場合は、すべてのポリシー サーバ情報をクラスタから削除してください。

10. [サブミット]をクリックして、変更を保存します。

クラスタの集中監視用のポリシー サーバ設定

OneView モニタは、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。この設定を有効にするには、1 つのポリシー サーバを集中監視用に設定し、クラスタ化されている他のポリシー サーバがこのサーバの監視対象となるように設定する必要があります。

ポリシー サーバを集中監視用に設定する方法

1. ポリシーサーバー管理コンソールを起動します。

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

2. [設定]タブで[着信リモート接続を許可]をオンにします。

   注: このタブ上での設定およびコントロールの詳細については、[ヘルプ]-[管理コンソール ヘルプ]をクリックしてください。

3. [OK]をクリックして変更内容を保存し、ポリシー サーバ管理コンソールを閉じます。

4. OneView モニタを再起動します。

この設定により、集中監視用のポリシー サーバは、クラスタ化されている他のポリシー サーバからのリモート接続を受け入れることができるようになります。

注: ポリシー サーバと監視プロセスの間の通信には、セキュリティ保護されていないネットワーク チャネルが使用されます。

ポリシー サーバを集中監視用に設定した後、ポリシー サーバ管理コンソールを使用して、そのサーバをクラスタ化されている他のポリシー サーバが参照するよう設定する必要があります。

詳細情報:

ポート番号の設定 (P. 140)

クラスタ化されているポリシー サーバを集中監視用のポリシー サーバの監視対象にする

クラスタ化されているポリシー サーバを集中監視用のポリシー サーバの監視対象にする設定

1. 監視サービスの対象となる各ポリシー サーバについて、ポリシー サーバ管理コンソールを開きます。

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

2. [設定]タブで、OneView モニタの下の[リモート モニタに接続]をオンにします。

   注: このタブ上での設定およびコントロールの詳細については、[ヘルプ]-[管理コンソール ヘルプ]をクリックしてください。

3. その下にあるフィールドに、監視サービスが設定されているシステムのホスト名と TCP ポート番号を入力します。例:

   server.company.com:44449

4. [OK]をクリックして変更内容を保存し、ポリシー サーバ管理コンソールを閉じます。

5. ポリシー サーバを再起動します。

詳細情報:

クラスタ化されたポリシー サーバ (P. 119)

第 14 章: OneView モニタの使用

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

SiteMinder OneView モニタは、SiteMinder 環境のパフォーマンス ボトルネックを特定し、リソースの利用状況に関する情報を提供します。また、特定のイベント(コンポーネント障害など)が発生した場合に、アラートを表示します。この機能は、以下の SiteMinder コンポーネントから動作データを収集することによって実現されます。

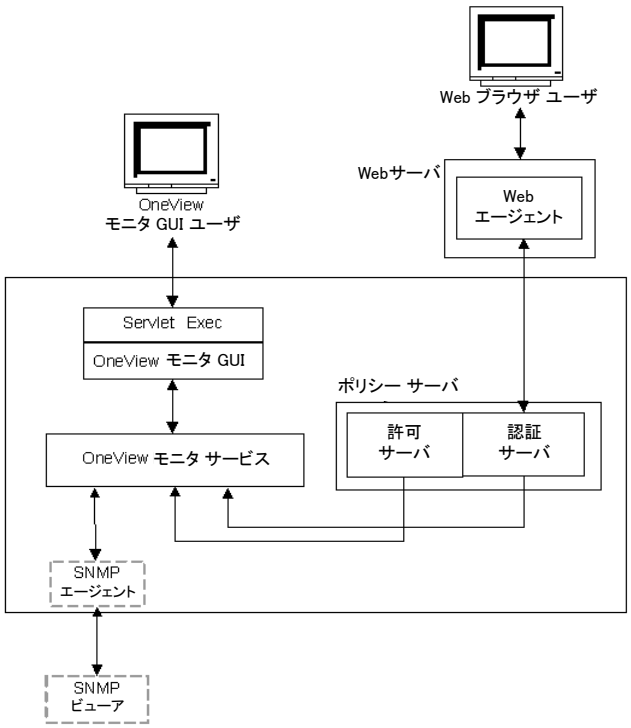
- ポリシー サーバ
- SiteMinder Web エージェント

これらのコンポーネントを SiteMinder 環境に追加すると、OneView モニタに自動的に登録されます。これらのコンポーネントを監視するように OneView モニタを設定する必要はありません。

監視対象のコンポーネントが存在する各マシンでは、OneView エージェントが動作します。このエージェントは、ポリシー サーバがインストールされているマシンに存在する OneView モニタに、動作データを送信します。OneView モニタは、動作データを Web ブラウザまたは必要に応じて SNMP エージェントに送信します。SNMP エージェントは、そのデータを SNMP マネージャに送信します。

OneView モニタのデータには、Web ブラウザやサードパーティ製の SNMP 監視アプリケーションからアクセスできます。

以下は、OneView モニタが統合された SiteMinder 環境を示しています。



OneView モニタは、プロパティ(コンポーネントのホスト マシンの IP アドレスなど)と、コンポーネントのアクティビティを示すカウンタ(ユーザがサイトにログインした回数など)を収集します。カウンタは、コンピュータを再起動するとリセットされます。

Web ベースの OneView ビューアを使用すると、管理者は、特定のコンポーネントの一部またはすべてのデータを表示するテーブルを定義できます。データのリフレッシュ間隔も設定できます。

SNMP がサポートされているため、監視アプリケーションが OneView モニタから動作データを取得できます。SNMP サポートには、MIB (Management Information Base) と SNMP エージェントが含まれています。

注: クラスタ化されたポリシー サーバを含む環境では、1 つの OneView モニタを指定して、そこからクラスタ内のすべてのポリシー サーバのアクティビティを監視することができます。集中監視モニタを設定するには、クラスタ内の各ポリシー サーバについて、ポリシー サーバ管理コンソールで OneView モニタの設定を調整する必要があります。

ポリシー サーバのデータ

ポリシー サーバ データのリストとその説明を以下に示します。

AgentTable

このサーバに接続されているエージェントのテーブル。

注: AgentTable は、SNMP を使用して利用することはできません。

AuthAcceptCount

成功した認証の数。

AuthRejectCount

失敗した認証試行の回数。これらの試行は、認証情報が無効であったために失敗しました。

AzAcceptCount

成功した許可試行の回数。

AzRejectCount

拒否された許可試行の回数。これらの試行は、必要なアクセス権限がなかったために拒否されました。

CacheFindCount

許可キャッシュ内での検索操作の回数。ユーザがポリシーに属するかどうかを許可プロセスが確認するごとに更新されます。

CacheFindCount/sec

毎秒あたり発生する許可キャッシュ検索操作の回数。

CacheHitCount

許可キャッシュでのヒット数。ユーザがポリシーに属するかどうかを許可プロセスが確認し、結果が真であるごとに更新されます。

CacheHitCount/sec

許可キャッシュでの毎秒あたりのヒット数。

CacheTTLMissCount

キャッシュ内に要素は見つかったものの古すぎるという理由で発生した、許可キャッシュミスの回数。

Component Path

ポリシー サーバのパス。これにより、サーバを一意に特定できます。Component Path には、次の情報が含まれています。

- ホストの IP アドレス
- コンポーネントのタイプ
- コンポーネントのインスタンス ID

注: Component Path は、SNMP を使用して利用することはできません。

Crypto bits

Web エージェントとポリシー サーバの間で送信されるデータの暗号化/復号化に使用される暗号化キーの長さ。

HitRate

許可検索操作に対する許可キャッシュ ヒットの比率。これは、許可キャッシュの有効性を示すインジケータです。

Host

認証サーバがインストールされているマシンの IP アドレス。

注: ホストの IP アドレスは、Component Path に含まれています。

IsProtectedCount

エージェントから受信した IsProtected コールの数。

Label

ポリシー サーバのビルド番号。

LastActivity

ポリシー サーバがワンビュー モニターと最後に通信した日時。

MaxSockets

ポリシー サーバへの同時リクエストをサブミットするために使用できる Web エージェント ソケットの最大数。

MaxThreads

スレッド プール内のワーカー スレッドの最大数。

MaximumThreadsEverUser

これまで使用された、スレッド プール内のワーカー スレッドの最大数。

PriorityQueueLength

優先キュー内のエントリ数。優先キューは優先度の高いエントリを保持します。「ServerQueueLength」を参照してください。

Platform

ポリシー サーバがインストールされているマシンのオペレーティング システム。

PolicyCacheEnabled

ポリシー キャッシュが有効になっているかどうかを示します。

Port

ポリシー サーバのポート番号。

Product

ポリシー サーバの製品名。

ServerQueueLength

標準キュー内のエントリ数。標準キューは優先度が標準のエントリを保持します。「PriorityQueueLength」を参照してください。

SocketCount

開いているソケットの数。この数は、ポリシー サーバと Web エージェントの間の開いている接続の数に対応します。

Status

ポリシー サーバのステータス。値は、Active または Inactive です。

Inactive は、指定された期間にわたってポリシー サーバとワンビュー モニターの間に通信がなかったことを示します。この期間は、ハートビート間隔によって決まります。

ThreadsAvailable

現在使用できる、スレッド プール内のワーカー スレッドの数。リクエストを処理するすべてのワーカー スレッドは、スレッド プールの中に整理されます。すべてのスレッドがただちにビジー状態になるとは限りません。十分な負荷が適用された場合に限られます。この値は、現在ビジー状態にないスレッドの数を示します。

ThreadsInUse

現在使用されている、スレッド プール内のワーカー スレッドの数。

Time Zone

ポリシー サーバがインストールされているマシンの設置場所のタイムゾーン。

Type

ポリシー サーバのタイプ

Universal Coordinated Time

ポリシー サーバが起動した日時。

UserAzCacheEnabled

ユーザ許可キャッシュが有効になっているかどうかを示します。

Update

最後に適用された更新ファイルのバージョン番号。

Version

ポリシー サーバのバージョン番号。

Web エージェントのデータ

Web エージェント データのリストとその説明を以下に示します。

AuthorizeAvgTime

ユーザの許可にかかった平均時間 (ミリ秒単位)。

AuthorizeCount

このエージェントによる許可試行の回数。許可試行は、ユーザが保護されたリソースにアクセスするためにポリシー サーバに認証情報を提示すると発生します。

AuthorizeErrors

この Web エージェントによる許可試行の際にエラーが発生した回数。エラーは、許可呼び出し時に Web エージェントとポリシー サーバの間で通信障害が発生したことを示しています。

AuthorizeFailures

失敗した許可試行の回数。ユーザがリソースへのアクセスに必要な権限を持っていないと、許可試行は失敗します。

BadCookieHitsCount

Web エージェントが復号できなかった cookie の数。

BadURLcharsHits

URL の文字が無効であったためにエージェントが拒否したリクエストの数。Web クライアントが SiteMinder ルールに反することを防ぐために、無効な URL 文字は、明示的にブロックされます。これらの文字は、Web エージェントの設定で指定します。

Component Path

Web エージェントのパス。Component Path には、次の情報が含まれています。

- ホストの IP アドレス
- コンポーネントのタイプ
- コンポーネントのインスタンス ID

注: Component Path は、SNMP を使用して利用することはできません。

CrosssiteScriptHits

クロスサイトスクリプティングを検出した回数。これは、サイトのページに埋め込まれた不正コードの数を示しています。

注: クロスサイト スクリプティングの詳細については、「*Web エージェント設定ガイド*」を参照してください。

Crypto bits

Web エージェントとポリシー サーバの間で送信されるデータの暗号化/復号化に使用される暗号化キーの長さ。

ExpiredCookieHitsCount

有効期限の切れた cookie を含んでいたリクエストの数。

Host

Web エージェントがインストールされているマシンの IP アドレス。

注: ホストの IP アドレスは、Component Path に含まれています。

IsProtectedAvgTime

リソースが保護されているかどうかを Web エージェントがポリシー サーバに確認するためにかかる平均時間 (ミリ秒単位)。

IsProtectedCount

リソースが保護されているかどうかを Web エージェントがポリシー サーバに確認した回数。

注: リソース キャッシュが 0 に設定されている場合、OneView モニタは、ログイン試行のたびに複数の IsProtected 呼び出しを記録することがあります。Web エージェントが情報をキャッシュしていない場合、Web エージェントは、Web サーバにリクエストがあるたびに、リソースが保護されているかどうかをポリシー サーバに確認する必要があります。

リソースキャッシュが 0 に設定されていない場合、OneView モニタは、1 回の IsProtected 呼び出しだけを記録します。この場合、Web エージェントは、ポリシー サーバに IsProtected 呼び出しを 1 回だけ実行します。同じリソースに関するその後の Web サーバへのリクエストは、Web エージェントのリソース キャッシュの有効期限が切れていないか、キャッシュがクリアされていない限り、キャッシュされた情報を使用して処理されます。

IsProtectedErrors

リソースが保護されているかどうかを Web エージェントがポリシー サーバに確認する際にエラーが発生した回数。エラーは、Web エージェントとポリシー サーバの間で通信障害が発生したことを示しています。

Label

Web エージェントのビルド番号。

Last Activity

Web エージェントの直前のアクティビティの日時。

LoginAvgTime

ユーザがログインするためにかかった平均時間。

LoginCount

この Web エージェントからのログイン試行の回数。

LoginErrors

ログイン試行の際にエラーが発生した回数。エラーは、Web エージェントとポリシー サーバの間で通信障害が発生したことを示しています。

LoginFailures

失敗したログイン試行の回数。ログインは、ユーザが無効な認証情報を提示すると失敗します。

Name

Web エージェントの名前。

Platform

Web エージェントがインストールされているマシンのオペレーティングシステム。

Product

Web エージェントの製品名。

ResourceCacheCount

リソースキャッシュのエントリ数。リソースキャッシュには、最近アクセスされたリソースに関する情報が保存されます。これにより、同じリソースに関するその後のリクエストの処理速度が向上します。

リソース キャッシュ内のエントリ数は、0 ～ *n* になります。*n* は、Web エージェントの設定で指定される最大キャッシュ サイズです。

ResourceCacheHits

Web エージェントがリソースキャッシュ内でリソースを検出した回数。この数は、SiteMinder がキャッシュされたリソースを使用する頻度を示しています。

ResourceCacheMax

リソースキャッシュが保持可能なエントリの最大数。この数は、Web エージェントの設定で指定します。

注: リソース キャッシュ サイズの設定の詳細については、「*Web エージェント設定ガイド*」を参照してください。

ResourceCacheMisses

- Web エージェントがリソースキャッシュ内でリソースを検出できなかった回数。次のような場合には、リソースを検出できません。
- そのリソースにまだ一度もアクセスしていない場合
- キャッシュされた情報の有効期限が切れた場合

SocketCount

開いているソケットの数。この数は、ポリシー サーバと Web エージェントの間の開いている接続の数に対応します。

注: Web エージェント アーキテクチャが変わったので、SocketCount には値がありません。

Status

Web エージェントのステータス。値は、Active または Inactive です。

Inactive は、指定された期間にわたって Web エージェントとワンビューモニターの間に通信がなかったことを示します。この期間は、ハートビート間隔によって決まります。

Time Zone

Web エージェントがインストールされているマシンの設置場所のタイムゾーン。

Type

監視対象のコンポーネントのタイプ。この場合は、Web エージェントです。

Universal Coordinated Time

Web エージェントがインストールされている Web サーバが起動した日時。

Update

最後に適用された更新ファイルのバージョン番号。

UserSessionCacheCount

ユーザセッション キャッシュのエントリ数。 ユーザ セッション キャッシュには、リソースに最近アクセスしたユーザに関する情報が保存されます。ユーザ情報を保存することによって、リソースリクエストの処理速度が向上します。

ユーザ セッション キャッシュ内のエントリ数は、0 ～ *n* になります。*n* は、Web エージェントの設定で指定される最大キャッシュサイズです。ユーザ セッション キャッシュ サイズの設定については、「*Web エージェント設定ガイド*」を参照してください。

注: ユーザ セッション キャッシュ数は、セッション キャッシュが存在する Web サーバによって異なります。

マルチスレッドキャッシュを使用する Web エージェント (Windows オペレーティングシステム環境で動作する IIS Web エージェント、iPlanet 4.*x*/6.0 Web エージェント、Windows および UNIX オペレーティングシステム環境で動作する Domino Web エージェントなど) の場合、OneView モニタは、ユーザが正常に認証され、Web エージェントからセッション cookie を受信したときに、ユーザ セッション キャッシュ数を増やします。

UNIX オペレーティング システム環境で動作し、マルチプロセス キャッシュを使用する Apache および iPlanet 4.*x*/6.0 Web エージェントでは、セッションのカウント方法が異なります。ユーザがセッション cookie を Web エージェントに提示するまでは、ユーザのセッションはセッション キャッシュに追加されません。Web エージェントは、ユーザが正常に認証された*後に*、ユーザのセッション cookie を作成します。SiteMinder は、ユーザから追加のリソース要求があると、この cookie を使用してユーザを認証します。つまり、ユーザの最初のログインは、ユーザ セッション キャッシュ数には含まれません。ユーザがもう一度リクエストし、SiteMinder がセッション cookie を使用してそのユーザを認証すると、ユーザ セッション キャッシュ数が増えます。

どの Web エージェントの場合でも、ユーザセッションは、1 つのレルム内のリソースに対して有効です。ユーザがセッション cookie を使用して異なるレルムのリソースにアクセスすると、ユーザには別のユーザセッションが与えられ、ユーザ セッション キャッシュ数が増えます。

UserSessionCacheHits

Web エージェントがユーザ セッション キャッシュにアクセスした回数。

UserSessionCacheMax

ユーザ セッション キャッシュが保持可能なエントリの最大数。この数は、Web エージェントの設定で指定します。

注: ユーザ セッション キャッシュ サイズの設定の詳細については、「*Web エージェント設定ガイド*」を参照してください。

UserSessionCacheMisses

Web エージェントがユーザ セッション キャッシュ内でユーザセッション情報を検出できなかった回数。次のような場合には、リソースを検出できません。

- そのリソースにまだ一度もアクセスしていない場合
- キャッシュされた情報の有効期限が切れた場合

ValidationAvgTime

ユーザの認証に使用される cookie の正当性の検証にかかった平均時間 (ミリ秒単位)。シングル サインオン環境では、ユーザの認証に cookie が使用される場合があります。

ValidationCount

特定の Web エージェントが、ユーザを認証するために、ユーザのクレデンシャルをユーザ ディレクトリ エントリと照合する代わりに、ポリシー サーバに対してセッション cookie の正当性の検証を試行した回数（Web エージェントは、ユーザが正常に認証されたときにユーザのブラウザ上にセッション cookie を作成し、その cookie を使用して、新しいリソースに対するその後のリクエストでユーザを認証します）。

ValidationCount には、次の条件が影響します。

ユーザ セッション キャッシュのサイズ

Web エージェントのユーザ セッション キャッシュが 0 よりも大きい値に設定されている場合は、ユーザのセッション情報がキャッシュに保存されます。Web エージェントは、ポリシー サーバではなくセッション キャッシュに対してセッションの正当性を検証するため、ValidationCount は増えません。ユーザ セッション キャッシュが 0 に設定されている場合は、Web エージェントがポリシー サーバに対してセッションの正当性を検証する必要があるため、保護されているリソースをユーザがリクエストするたびに ValidationCount が増えます。

マルチスレッド キャッシュとマルチプロセス キャッシュ

マルチスレッド キャッシュを使用する Web エージェント（Windows オペレーティング システム環境で動作する IIS Web エージェント、iPlanet 4.x/6.0 Web エージェント、Windows および UNIX オペレーティング システム環境で動作する Domino Web エージェントなど）は、ユーザが正常に認証されたときに、セッションをセッション キャッシュに追加します（セッション キャッシュ サイズが 0 よりも大きい場合）。認証されたユーザが同じレルムから追加のリソースをリクエストする場合は、Web エージェントがセッション キャッシュに対してユーザの正当性を検証するため、ValidationCount は増えません。

UNIX オペレーティングシステム環境で動作し、マルチプロセスキャッシュを使用する Apache および iPlanet 4.x/6.0 Web エージェントは、ユーザが、以前に認証されたレルムの別のリソースをリクエストするときに cookie を Web エージェントに提示するまで、セッション cookie をセッション キャッシュに追加しません。Web エージェントは、セッション cookie による最初のリクエストの正当性をポリシー サーバに対して検証します。このとき、ValidationCount が増えます。その後のリクエストの正当性は、キャッシュに対して検証されます。

ValidationErrors

Web エージェントによるユーザセッションの正当性の検証試行の際にエラーが発生した回数。エラーは、Web エージェントとポリシー サーバの間で通信障害が発生したことを示しています。

ValidationFailures

セッション cookie が無効であったために Web エージェントがユーザセッションの正当性を検証できなかった回数。

Version

Web エージェントのバージョン番号。

OneView モニタの設定

OneView モニタの設定には、以下が含まれます。

- データのリフレッシュ間隔とハートビートの設定
- ポート番号の設定

データのリフレッシュ間隔とハートビートの設定

次の設定を修正することによって、OneView モニタと監視対象のコンポーネントの間でデータが送信される間隔を変更できます。

- リフレッシュ間隔 - OneView モニタが認証サーバと許可サーバにデータをリクエストする間隔を指定します。デフォルトの間隔は 5 秒です。
- ハートビート - 監視対象のコンポーネントがワンビュー モニターにハートビートを送信する間隔を指定します。認証サーバおよび許可サーバに対しては、ハートビートはコンポーネントがアクティブかどうかを示します。Web エージェントに対しては、ハートビートはワンビュー モニターが Web エージェントの動作データを受信する間隔を指定します。デフォルト値は 30 秒です。

デフォルト値を変更する方法

1. *Policy_Server_installation*/monitor/mon.conf を開きます。
2. 必要に応じて、次のプロパティとペアになっている値を変更します。
   - リフレッシュ間隔: nete.mon.refreshPeriod
   - ハートビート: nete.mon.hbPeriod

   注: これらのプロパティの値は秒単位で指定します。

3. mon.conf を保存して閉じます。
4. OneView モニタを再起動します。

ポート番号の設定

OneView モニタは、以下のデフォルト ポート番号を使用します。

- OneView エージェント -- 44449

  注: デフォルト ポートが使用されている場合、OneView エージェントでは、そのポート上でのみリスンします。デフォルト ポートが変更された場合、OneView エージェントは、指定したポート上でリスンし、指定したリモート ホスト上で同じポートに接続します。たとえば、ポートを 55555 に変更した場合、OneView エージェントはポート 55555 上でリスンし、リモート ホスト上でポート 55555 に接続します。

- OneView モニタ -- 44450

デフォルトのポート番号を変更する方法

1. *Policy_Server_installation_directory*/config/conapi.conf ファイルをテキスト エディタで開きます。
2. 必要に応じて、以下の OneView エージェント プロパティの値を変更します。

   `nete.conapi.service.monagn.port=`*`port_number`*

   `nete.conapi.service.monagn.host=`*`fully_qualified_domain_name_of_remote_host`*
3. 必要に応じて、以下の OneView モニタ プロパティの値を変更します。

   `nete.conapi.service.mon.port=`*`port_number`*
4. conapi.conf ファイルを保存して閉じます。

   注: conapi.conf 内のプロパティの詳細については、conapi.conf ファイルの注記を参照してください。
5. OneView モニタを再起動します。

詳細情報:

Windows システムでのポリシー サーバ サービスの開始と終了 (P. 24)
UNIX システムでのポリシー サーバ プロセスの開始と終了 (P. 24)
クラスタの集中監視用のポリシー サーバ設定 (P. 124)

クラスタ化された環境の監視

クラスタ化されていない SiteMinder 環境では、監視プロセスは、ポリシー サーバと同じシステムに配置されます。 監視ユーザインタフェースと SNMP によって、単一のポリシー サーバの情報が提供されます。クラスタを監視するには、単一の監視プロセスで処理されるようクラスタ内のポリシー サーバを設定する必要があります。ポリシー サーバ管理コンソールを使用すると、監視プロセス ホストを指定できます。

クラスタ化された環境で監視機能を実装する場合は、以下の点を考慮します。

- ポリシー サーバと監視プロセスの間の通信には、セキュリティ保護されていないネットワークチャネルが使用されます。
- 監視プロセスに障害が発生すると、すべての監視作業が中断されます。また、監視ホストとの接続が切れると、監視作業が中断されます。
- クラスタでは、SNMP による監視がサポートされています。

注: クラスタ化を有効にしないことによって、すべてのサーバはデフォルト クラスタに含まれます。クラスタ化されていない環境に対しては、集中監視を有効にすることができます。

OneView ビューアへのアクセス

OneView ビューアにアクセスする前に、OneView モニタ サービスが動作していることを確認してください。

OneView ビューアにアクセスするには、ブラウザで次の URL を入力します。

http://*your_server.your_company.org:port*/siteminderモニター

ここで、*your_server.your_company.org:port* は、ホスト名または IP アドレス、および OneView モニタ用に Web サーバで設定されているポート番号です。

注: OneView モニタ用に Web サーバを設定する方法については、「ポリシー サーバ インストール ガイド」を参照してください。

OneView ビューアの保護

OneView ビューアを保護するには、siteminderモニター のリソースを保護する SiteMinder ポリシーを作成します。

監視対象コンポーネントの表示

OneView モニタには、4 つのデフォルト テーブルが用意されています。

- すべてのコンポーネント(表示済み)
- ポリシー サーバ
- エージェント

OneView を開くと、「すべてのコンポーネント」テーブルが表示されます。

注: Apache または iPlanet 6.0 Web サーバにインストールされている Web エージェントは、その Web エージェントがポリシー サーバにリソースが保護されているかどうかを確認するまでは、ワンビュー ビューアに表示されません。Web エージェントがポリシー サーバに情報をリクエストすると、Web エージェントが OneView モニタに登録されます。

OnewView ビューアは、設定可能なテーブルに動作データを表示します。テーブルには、[Details] 列を含めることができます。[Details] 列のアイコンをクリックすると、特定のコンポーネントのすべての監視対象データを表示するウィンドウが開きます。

OneView の表示をカスタマイズする方法

OneView の表示のカスタマイズには、以下が含まれます。

- テーブルのセットアップ (P. 143)
- アラートの設定 (P. 143)
- テーブルの表示 (P. 144)
- テーブルの並べ替え (P. 144)
- データ更新の設定 (P. 144)
- 設定の保存 (P. 145)
- デフォルトの表示の変更 (P. 145)
- 設定のロード (P. 146)

テーブルのセットアップ

テーブルをセットアップする方法

1. ［Configure］をクリックします。

   テーブル設定ダイアログ ボックスが表示されます。

2. 以下のいずれかのオプションを実行します。

   - [Existing Table] を選択します。リストボックスからテーブルを選択してください。
   - [New Custom Table] を選択します。[Table Name] フィールドに名前を入力してください。

3. テーブルに表示するコンポーネントを選択します。

4. テーブルに表示するフィールドを選択します。フィールドを選択し、上下矢印キーでフィールドの位置を変更して、フィールドを表示する順番を指定します。使用できるフィールドは、選択したコンポーネントのタイプによって決まります。

   注: 一部のフィールドの値は、継続的に増加する値（コンポーネントを再起動するとリセットされる）または平均値（最終更新時点以降）として表示することができます。平均値を表示するには、最後に [/sec] の付いているフィールド名を選択してください。

5. ［OK］をクリックします。

   注: 設定が完了したら、必ずテーブルを保存してください。

アラートの設定

アラートを設定する方法

1. ［Configure］をクリックします。
2. [Alerts] タブをクリックします。
3. 左側のリストボックスからフィールドを選択します。このリストボックスには、現在ロードされているテーブルのすべてのフィールドが含まれています。
4. 中央のリストボックスからオペレータを選択します。
5. 手順 3 で選択したフィールドの値を指定します。

6. 必要に応じて、[Highlight the table cell] をオンにします。これにより、OneView では、指定した基準が満たされたときに、指定されたテーブル セルを強調表示します。
7. 必要に応じて、[Pop up a warning message] を選択します。これにより、OneView ビューでは、指定した基準が満たされたときに、ポップアップ ウィンドウを表示します。

テーブルの表示

テーブルを表示するには、ビューアのメインページの［View Table］リストボックスからテーブルを選択します。このリストからテーブルを選択すると、OneView では、選択されたテーブルを既存のテーブルの下に表示します。

テーブルを非表示にするには、[Hide] ボタンをクリックします。

テーブルの並べ替え

テーブルの各列のデータを昇順または降順にソートすることができます。列のソートにより、テーブルの編成が容易になります。たとえば、[Status] に基づいてテーブルをソートすると、アクティブでないすべてのコンポーネントをまとめて表示することができます。

注: 列の見出しに表示される矢印は、その列に基づいて並べ替えが行われたことを示しています。

データ更新の設定

デフォルトでは、OneView は、30 秒ごとにデータを更新します。次の操作が可能です。

- 自動更新の間隔を変更
- ブラウザの表示を更新したときにだけデータを更新するように OneView を設定

データ更新を設定する方法

1. [更新] をクリックします。

   ［更新］ダイアログ ボックスが表示されます。

2. 次のいずれかをオンにします。
   - 自動更新 -- 指定した時間ごとにデータを更新します。秒単位で時間間隔を指定します。
   - 手動更新 -- ユーザがページの表示をリフレッシュしたときにデータを更新します。
3. ［OK］をクリックします。

設定の保存

設定を保存すると、次の項目が保存されます。

- テーブルの定義
- メインページの表示
- テーブルのソート
- 更新間隔

設定を保存する方法

1. [設定を保存] をクリックします。

   設定に名前を付けるためのダイアログ ボックスが表示されます。

2. テキストボックスに名前を入力します。
3. ［OK］をクリックします。

デフォルトの表示の変更

デフォルトの表示を変更する方法

1. *siteminder_installation*¥monitor¥settings にある defaults ファイルの名前を変更します。
2. OneView モニタ コンソールで、設定を行います。
3. 設定をデフォルトとして保存します。

設定のロード

設定をロードする方法

1. ［設定をロード］をクリックします。

   ロードする設定を選択するためのダイアログ ボックスが表示されます。
2. リストボックスから設定を選択します。
3. ［OK］をクリックします。

第 15 章: SNMP による SiteMinder の監視

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 監視

SiteMinder の SNMP モジュールを使用すると、SNMP 対応ネットワーク管理アプリケーションによる SiteMinder 環境のさまざまな動作ステータスの監視が可能になります。

SNMP の概要

ネットワーク管理には、2 つのタイプのシステムが関係しています。1 つは、制御するシステムで管理システムと呼ばれ、もう 1 つは、監視され、制御されるシステムで管理対象システムと呼ばれます。管理対象システムには、ホストやサーバ、それらのシステム上で動作するソフトウェアコンポーネント、あるいはネットワークコンポーネント (ルーター、インテリジェントリピータなど) が含まれる場合があります。

相互運用性を向上させるため、連携するシステムでは、業界標準の SNMP (Simple Network Management Protocol) をサポートしています。SNMP は、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。

完全な SNMP ソリューションには、次の 3 つのコンポーネントが含まれます。

- SNMP MIB（Management Information Base）- 管理対象オブジェクトのデータベースです。管理対象オブジェクト (変数) は、管理システムによって読み込まれ、管理対象システムに関する情報を提供します。
- SNMP エージェント - 管理対象システムに関する情報にアクセスして、その情報を管理システムが利用できるようにする低負荷のソフトウェア モジュールです。ソフトウェアシステムの場合、エージェント機能は、マスタエージェント (ホストオペレーティングシステムが提供) とサブエージェント (管理対象アプリケーションが提供) に分割される場合があります。

  注: SNMP エージェントは、すべての SNMP 実装に含まれる標準コンポーネントです。SiteMinder エージェントと混同しないでください。
- SNMP マネージャ - 一般には、HP OpenView などのネットワーク管理システム（NMS）アプリケーションです。

SiteMinder SNMP モジュールは、SiteMinder 環境で SNMP リクエスト処理機能と設定可能なイベントトラップ機能を実現します。その仕組みは、SiteMinder OneView モニタから動作データを収集し、そのデータを SNMP プロトコルをサポートするサードパーティ製 NMS アプリケーション（HP OpenView など）で利用できるように MIB に組み込むことです。

注: 6.0 SNMP エージェントは、SiteMinder 5.x ベースのすべてのエージェント アプリケーションと互換性があります。

SiteMinder SNMP モジュールのコンポーネント

SiteMinder SNMP モジュールは、以下のコンポーネントで構成されます。

- SiteMinder SNMP MIB - SNMP 対応ネットワーク管理システムによって監視できる SiteMinder オブジェクトのデータベースです。
- SiteMinder SNMP サブエージェント - SNMP マスタ エージェントから受信した SNMP リクエスト（GET および GETNEXT のみ）に応答します。
- SiteMinder イベント マネージャ - ポリシー サーバ イベントを取り込み、設定されている場合には SNMP トラップ（一部のイベントの発生を示すために SNMP エージェントが SNMP NMS に送信する非請求メッセージ）を生成します。

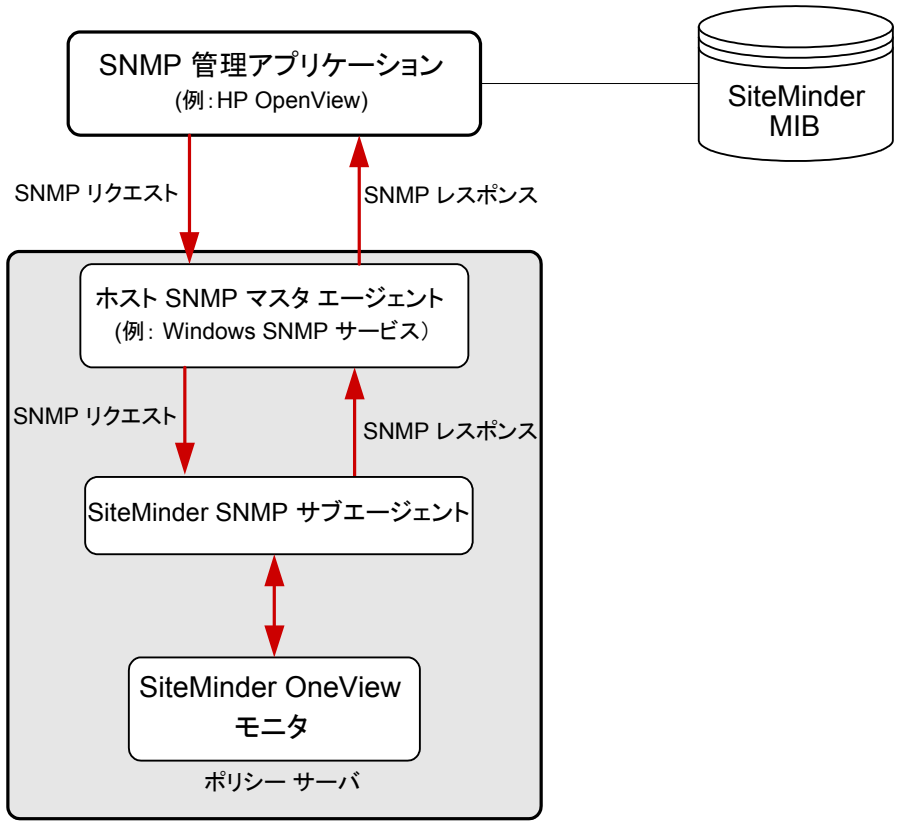
依存関係

SiteMinder SNMP モジュールには、以下の依存関係があります。

- **SiteMinder OneView モニタ** - SiteMinder SNMP モジュールは、OneView モニタから動作情報を取得します。SiteMinder SNMP モジュールを動作させるすべてのポリシー サーバで、OneView モニタも設定し、動作させる*必要があります*。
- **SNMP マスタ エージェント** - SiteMinder SNMP モジュールは、SNMP マスタ エージェントを提供*しません*。SiteMinder SNMP モジュールを動作させるポリシー サーバのオペレーティング システムに適した SNMP マスタ エージェント(Windows SNMP サービスまたは Solstice エンタープライズ マスタ エージェント)がインストールされ、有効になっていることも必ず確認するようにしてください。

SNMP コンポーネントのアーキテクチャとデータフロー

以下の図は、SNMP モジュールのデータフローを示しています。



SiteMinder SNMP のデータフローは以下のとおりです。

1. SNMP マスタエージェントが、管理アプリケーションから SNMP リクエストを受信します。
2. SNMP マスタエージェントが、SNMP リクエストを SNMP サブエージェントに転送します。
3. SiteMinder SNMP サブエージェントが、リクエストされた情報を OneView モニタから取得します。
4. SiteMinder SNMP サブエージェントが、取得した情報を SNMP マスタ エージェントに転送します。
5. SNMP マスタエージェントが、SNMP レスポンスを生成して、リクエスト元の管理アプリケーションに送信します。

SiteMinder MIB

SiteMinder MIB は、SiteMinder 環境のすべての監視対象コンポーネントについて、SNMPv2 に準拠したデータ表現を提供します。

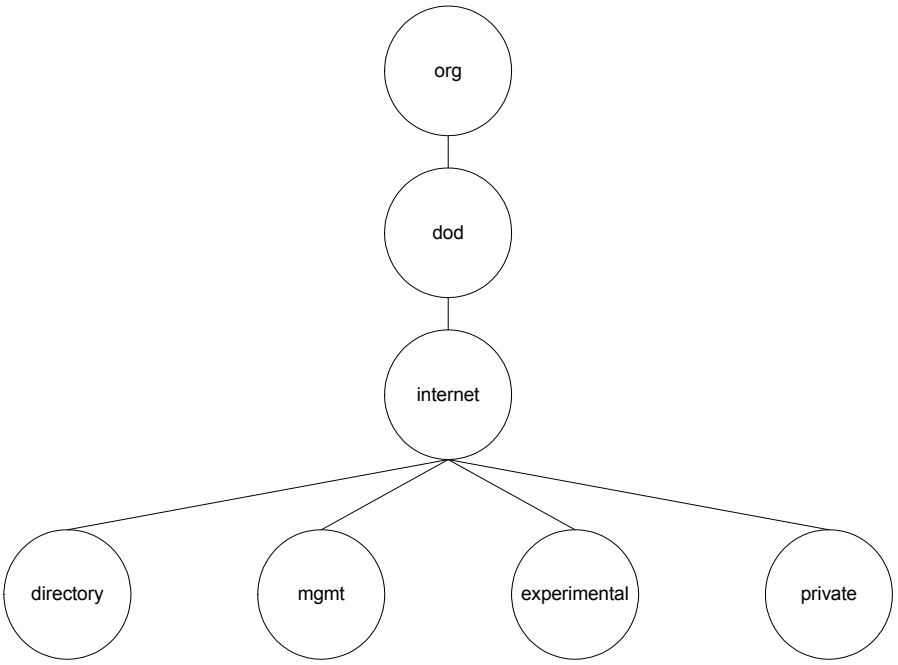
SiteMinder MIB は、次の ASCII テキスト形式のファイルです。

SiteMinder_Install_Directory¥mibs¥NetegritySNMP.mib。

MIB の概要

SNMP MIB の構造は、逆ツリー階層によって論理的に表現されます。SiteMinder のようなインターネットに関係する製品の MIB は、MIB 階層の ISO メイン ブランチの下にあります。

以下の図は、ISO ブランチの上部階層を示しています。

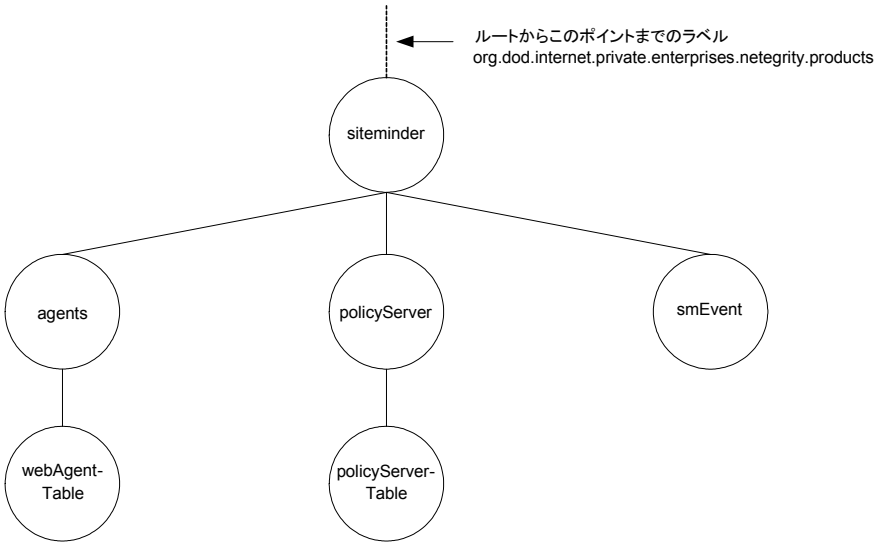


MIB ブランチ、MIB、および MIB 内の管理対象オブジェクトはすべて、短いテキスト文字列によって識別されます。完全な MIB 階層は、ブランチ識別子とオブジェクト識別子を連結して (ピリオド区切り) 表記することができます。たとえば、上の図に示されている internet エントリの private サブブランチは、*iso.org.dod.internet.private* と表記できます。

SiteMinder MIB 階層

SiteMinder MIB は、*iso.org.dod.internet.private.enterprises.netegrity.products.siteminder* と表記できます。

MIB オブジェクトによって表される、サポートされている管理対象コンポーネントは、ポリシー サーバと Web エージェントです。各コンポーネントの複数のインスタンスが存在する可能性があるため、これらのコンポーネントのそれぞれが持つ管理対象プロパティは、列オブジェクトになります。



STMNDR MIB には、以下の 3 つのサブブランチがあります。

PolicyServer

ポリシー サーバ（policyServerTable）オブジェクトが入っています。

agents

Web エージェント（webAgent）オブジェクトが入っています。

smEvent

システム イベントの SNMP トラップ タイプが入っています。

MIB オブジェクトの参照リスト

以下のセクションには、ポリシー サーバ、Web エージェント、およびイベント MIB オブジェクトの詳細を示したリストが含まれています。

認証サーバのデータ

以下の表は、SiteMinder MIB（iso.org.
... .siteminder.policyServer.policyServerTable）にオブジェクトとして示される認証サーバのプロパティのサブセットのリストです。

オブジェクト名	SNMP タイプ	オブジェクトの説明
policyServerIndex	Integer32	現在のポリシー サーバ インスタンスの固有識別子。
policyServerHostID	IP アドレス	ポリシー サーバがインストールされているマシンの IP アドレス。
policyServerType	表示可能な文字列	コンポーネントのタイプ。
policyServerStatus	Integer32	ポリシー サーバのステータス。値は、Active または Inactive です。
policyServerPort	Integer32	ポリシー サーバのポート番号。
policyServerProduct	表示可能な文字列	ポリシー サーバの製品名。
policyServerPlatform	表示可能な文字列	ポリシー サーバがインストールされているマシンのオペレーティング システム。
policyServerVersion	表示可能な文字列	ポリシー サーバのバージョン番号。
policyServerUpdate	表示可能な文字列	最後に適用された更新ファイルのバージョン番号。
policyServerLabel	表示可能な文字列	ポリシー サーバのビルド番号。
policyServerCrypto	Integer32	Web エージェントとポリシー サーバの間で送信されるデータの暗号化/復号化に使用される暗号化キーの長さ。
policyServerUTC	表示可能な文字列	ポリシー サーバがインストールされている Web サーバが起動した日時。日時は、万国標準時形式で示されます。
policyServerTime Zone	Integer32	ポリシー サーバがインストールされているマシンの設置場所のタイムゾーン。

オブジェクト名	SNMP タイプ	オブジェクトの説明
policyServerMaxSockets	Integer32	ポリシー サーバでサポート可能な開いているソケットの最大数 (開いているソケットの数はポリシー サーバと Web エージェントの間の開いている接続の数に対応します) 。
policyServerSocketCount	Gauge32	開いているソケットの数。この数は、ポリシー サーバと Web エージェントの間の開いている接続の数に対応します。
policyServerAuth AcceptCount	Counter32	成功した認証の数。
policyServerAuthReject-Count	Counter32	失敗した認証試行の回数。これらの試行は、認証情報が無効であったために失敗しました。
policyServerAzAccept-Count	Counter32	成功した許可の数。
policyServerAzReject-Count	Counter32	失敗した許可試行の回数。これらの試行は、認証情報が無効であったために失敗しました。
policyServerPolicy-Cache Enabled	真理値	ポリシーキャッシュが有効になっているかどうかを示す値。
policyServerL2Cache-Enabled	真理値	L2 キャッシュが有効になっているかどうかを示す値。

SiteMinder MIB 内の Web エージェント オブジェクト

以下の表は、SiteMinder MIB (iso.org. ～ siteminder.webAgentTable.webAgentEntry) にオブジェクトとして示される Web エージェントのプロパティのリストです。

オブジェクト名	SNMP タイプ	オブジェクトの説明
webAgentIndex	Integer32	現在の Web エージェントインスタンスの固有識別子。
webAgentHostID	IP アドレス	Web エージェントサーバがインストールされているマシンの IP アドレス。
webAgentType	表示可能な文字列	コンポーネントのタイプ。

オブジェクト名	SNMP タイプ	オブジェクトの説明
webAgentStatus	Integer32	Web エージェントのステータス。値は、Active または Inactive です。
webAgentPort	Integer32	Web エージェントのポート番号。
webAgentProduct	表示可能な文字列	Web エージェントの製品名。
webAgentPlatform	表示可能な文字列	Web エージェントがインストールされているマシンのオペレーティングシステム。
webAgentVersion	表示可能な文字列	Web エージェントのバージョン番号。
webAgentUpdate	表示可能な文字列	最後に適用された更新ファイルのバージョン番号。
webAgentLabel	表示可能な文字列	Web エージェントのビルド番号。
webAgentCrypto	Integer32	Web エージェントとポリシー サーバの間で送信されるデータの暗号化/復号化に使用される暗号化キーの長さ。
webAgentUTC	表示可能な文字列	Web エージェントがインストールされている Web サーバが起動した日時。日時は、万国標準時形式で示されます。
webAgentTime Zone	Integer32	Web エージェントがインストールされているマシンの設置場所のタイムゾーン。
webAgentSocketCount	Gauge32	開いているソケットの数。この数は、ポリシー サーバと Web エージェントの間の開いている接続の数に対応します。 **注**: Web エージェント アーキテクチャが変わったので、SocketCount には値がありません。
webAgentResource-CacheCount	Integer32	リソースキャッシュのエントリ数。リソースキャッシュには、最近アクセスされたリソースに関する情報が保存されます。これにより、同じリソースに関するその後のリクエストの処理速度が向上します。 リソース キャッシュ内のエントリ数は、0 ～ *n* になります。n は、Web エージェントの設定で指定される最大キャッシュ サイズです。

オブジェクト名	SNMP タイプ	オブジェクトの説明
webAgentResource-CacheHits	Integer32	リソースキャッシュがアクセスされた回数。この数は、キャッシュされたリソースを SiteMinder が使用する頻度を示しています。
webAgentResource-CacheMisses	Integer32	Web エージェントがリソースキャッシュ内でリソースを検出できなかった回数。次のような場合には、リソースを検出できません。 ■ そのリソースにまだ一度もアクセスしていない場合 ■ キャッシュされた情報の有効期限が切れた場合
webAgentUserSession-CacheCount	Integer32	ユーザセッション キャッシュのエントリ数。ユーザ セッション キャッシュには、リソースに最近アクセスしたユーザに関する情報が保存されます。ユーザ情報を保存することによって、リソースリクエストの処理速度が向上します。 ユーザ セッション キャッシュ内のエントリ数は、0 ～ *n* になります。*n* は、Web エージェントの設定で指定される最大キャッシュサイズです。 **注**: ユーザ セッション キャッシュ数は、セッション キャッシュが存在する Web サーバによって異なります。
webAgentUserSession-CacheHits	Integer32	Web エージェントがユーザ セッション キャッシュにアクセスした回数。
webAgentUserSession-CacheMisses	Integer32	Web エージェントがユーザ セッション キャッシュ内でユーザセッション情報を検出できなかった回数。次のような場合には、リソースを検出できません。 ■ そのリソースにまだ一度もアクセスしていない場合 ■ キャッシュされた情報の有効期限が切れた場合

オブジェクト名	SNMP タイプ	オブジェクトの説明
webAgentIsProtected-Count	Integer32	リソースが保護されているかどうかを Web エージェントがポリシー サーバに確認した回数。 **注**: リソースキャッシュが 0 に設定されている場合、ログイン試行のたびに複数の IsProtected 呼び出しが記録されることがあります。Web エージェントが情報をキャッシュしていない場合、Web エージェントは、Web サーバにリクエストがあるたびに、リソースが保護されているかどうかをポリシー サーバに確認する必要があります。 リソースキャッシュが 0 に設定されていない場合、1 回の IsProtected 呼び出しだけが記録されます。この場合、Web エージェントは、ポリシー サーバに IsProtected 呼び出しを 1 回だけ実行します。同じリソースに関するその後の Web サーバへのリクエストは、Web エージェントのリソース キャッシュの有効期限が切れていないか、キャッシュがクリアされていない限り、キャッシュされた情報を使用して処理されます。
webAgentIsProtected-Errors	Integer32	リソースが保護されているかどうかを Web エージェントがポリシー サーバに確認する際にエラーが発生した回数。エラーは、Web エージェントとポリシー サーバの間で通信障害が発生したことを示しています。
webAgentIsProtected-AvgTime	Unsigned 32	リソースが保護されているかどうかを Web エージェントがポリシー サーバに確認するためにかかる平均時間。
webAgentLoginCount	Counter 32	この Web エージェントからのログイン試行の回数。
webAgentLoginErrors	Counter 32	ログイン試行の際にエラーが発生した回数。エラーは、Web エージェントとポリシー サーバの間で通信障害が発生したことを示しています。
webAgentLoginFailures	Counter 32	ユーザがポリシー サーバによって認証または許可されていなかったために失敗したログイン試行の回数。
webAgentLoginAvgTime	Unsigned 32	ユーザがリソースにログインするためにかかった平均時間。

オブジェクト名	SNMP タイプ	オブジェクトの説明
webAgentValidation-Count	Counter 32	特定の Web エージェントが、ユーザを認証するために、ユーザのクレデンシャルをユーザ ディレクトリ エントリと照合する代わりに、ポリシー サーバに対してセッション cookie の正当性の検証を試行した回数 (Web エージェントは、ユーザが正常に認証されたときにユーザのブラウザ上にセッション cookie を作成し、その cookie を使用して、新しいリソースに対するその後のリクエストでユーザを認証します)。
webAgentValidation-Errors	Counter 32	Web エージェントによるユーザ セッションの正当性の検証試行の際にエラーが発生した回数。エラーは、Web エージェントとポリシー サーバの間で通信障害が発生したことを示しています。
webAgentValidation-Failures	Counter 32	セッション cookie が無効であったために Web エージェントがユーザセッションの正当性を検証できなかった回数。
webAgentValidation-AvgTime	Unsigned 32	ユーザの認証に使用される cookie の正当性の検証にかかった平均時間 (ミリ秒単位)。シングル サインオン環境では、ユーザの認証に cookie が使用される場合があります。
webAgentAuthorize-Count	Counter 32	このエージェントによる許可試行の回数。許可試行は、ユーザが保護されたリソースにアクセスするためにポリシー サーバに認証情報を提示すると発生します。
webAgentAuthorize-Errors	Counter 32	この Web エージェントによる許可試行の際にエラーが発生した回数。エラーは、許可呼び出し時に Web エージェントとポリシー サーバの間で通信障害が発生したことを示しています。
webAgentAuthorize-Failures	Counter 32	失敗した許可試行の回数。許可試行は、ユーザが無効な認証情報を入力すると失敗します。
webAgentAuthorize-AvgTime	Integer32	ユーザの許可にかかった平均時間 (ミリ秒単位)。
webAgentCrosssite-ScriptHits	Integer32	クロスサイトスクリプティングを検出した回数。これは、サイトのページに埋め込まれた不正コードの数を示しています。クロスサイト スクリプティングの詳細については、「*SiteMinder Web エージェント設定ガイド*」を参照してください。

オブジェクト名	SNMP タイプ	オブジェクトの説明
webAgentBadURL-charsHits	Integer32	URL の文字が無効であったためにエージェントが拒否したリクエストの数。Web クライアントが SiteMinder ルールに反することを防ぐために、無効な URL 文字は、明示的にブロックされます。これらの文字は、Web エージェントの設定で指定します。
webAgentBadCookie-HitsCount	Gauge32	Web エージェントが復号できなかった cookie の数。
webAgentExpired-CookieHitsCount	Gauge32	有効期限の切れた cookie を含んでいたリクエストの数。

イベントのデータ

以下の表は、SiteMinder イベント マネージャを使用して SNMP トラップにマップできるシステム イベント用の SiteMinder MIB（iso.org. … .siteminder.smEvents）のオブジェクトのリストです。

イベント名	イベント ID	イベント カテゴリ	イベントカテゴリのタイプ
serverInit	SmLogSystemEvent_ServerInit	サーバ アクティビティ	システム
serverUp	SmLogSystemEvent_ServerUP		
serverDown	SmLogSystemEvent_ServerDown		
serverInitFail	SmLogSystemEvent_ServerInitFail		
dbConnectionFailed	SmLogSystemEvent_DbConnectFail		
ldapConnection-Failed	SmLogSystemEvent_LDAP-ConnectFail		
logFileOpenFail	SmLogSystemEvent_LogFile-OpenFail	システム アクティビティ	
agentConnection-Failed	SmLogSystemEvent_Agent-ConnectionFail		

イベント名	イベント ID	イベント カテゴリ	イベントカテゴリのタイプ
authReject	SmLogAccessEvent_AuthReject	認証	アクセス
validateReject	SmLogAccessEvent_ValidateReject		
azReject	SmLogAccessEvent_AzReject	許可	
adminReject	SmLogAccessEvent_AdminReject	管理	
objectLoginReject	SmLogObjEvent_LoginReject	認証	オブジェクト
objectFailedLoginAttemptsCount	SmLogObjEvent_FailedLogin-AttemptsCount		
emsLoginFailed	SmLogEmsEvent_LoginFail	DirectorySession	EMS
emsAuthFailed	SmLogEmsAuthFail		

SiteMinder イベント マネージャの設定

ポリシー サーバのイベントを取り込むイベント マネージャ アプリケーション（EventSNMP.dll というライブラリ ファイルとして提供）は、そのイベントに対して、設定ファイルの指定に基づいて SNMP トラップを生成する必要があるかどうかを判断し、生成する必要がある場合には、指定された NMS に対して SNMP トラップを生成します。

SiteMinder イベント マネージャを設定するには、イベント設定ファイル（*SM_Install_Directory*¥config¥snmptrap.conf）を定義します。このファイルには、処理するイベントと、トラップの送信先となる NMS のアドレスが定義されています。

イベント設定ファイルの構文

snmptrap.conf は、編集可能な ASCII ファイルで、次のような単純な構文 (イベントごとに 1 行) が使用されます。

Event_Name Destination_Address

Event_Name

MIB イベントオブジェクトの名前 (またはカンマ区切りのイベントオブジェクト名のグループ)。

例:

serverUP

serverUp,serverDown

serverUp,serverDown,serverInitFail

Destination_Address

生成したトラップを送信する NMS のアドレス (またはカンマ区切りの NMS のアドレスのグループ)。各アドレスは、*HostID*:*port*:*community* という形式で指定する必要があります。

HostID

(必須) ホスト名または IP アドレスを入力します。

Port

(オプション) IP ポート番号。

デフォルト: 162

Community

(オプション) SNMP コミュニティ。コミュニティ名を指定する場合は、必ずポートも指定してください。

デフォルト: 「public」

例: 100.132.5.166

例: 100.132.5.166:162

例: victoria:162:public

注: イベントが重複しないように注意してください。つまり、同じイベントを複数のエントリに割り当てないでください。コメント行を追加することもできます。コメント行の先頭には「#」記号を付けてください。

イベント設定ファイルの例

```
ServerDown,serverUp     111.123.0.234:567:public
```

このエントリによって、イベントマネージャは、SNMP トラップの serverDown と serverUp を IP アドレス 111.123.0.234、ポート 567、コミュニティ名 public の NMS に送信するように設定されます。

```
agentConnectionFailed    111.123.0.234,victoria
```

このエントリによって、イベント マネージャは、agentConnectionFailed タイプの SNMP トラップを IP アドレス 111.123.0.234、ポート 567、コミュニティ名 public と、ホスト「victoria」、ポート 567、コミュニティ名 public に送信するように設定されます。

```
azReject
```

このエントリによって、イベントマネージャは、azReject タイプのすべてのイベントを破棄するように設定されます。そのため、トラップは送信されません。

SiteMinder SNMP サポートの開始と終了

ポリシー サーバのインストール時に SiteMinder SNMP サポートのインストールを選択すると、ポリシー サーバの初期化のたびに SiteMinder SNMP エージェント サービスが自動的に開始されます。

このセクションでは、Windows および UNIX 環境のポリシー サーバで SiteMinder SNMP サブエージェントを手動で開始および終了する方法について説明します。

Windows 環境の Netegrity SNMP エージェント サービスの開始と終了

Windows 環境のポリシー サーバで SiteMinder SNMP サブエージェントを開始する方法

1. コントロールパネルの[サービス]を開きます。
   - (Windows Server)[スタート]、[設定]、[コントロール パネル]、[管理ツール]、[サービス]の順に選択します。
   - (Windows NT)[スタート]、[設定]、[コントロール パネル]、[サービス]の順に選択します。
2. Netegrity SNMP Agent サービスを選択します。

3. [開始]をクリックします。

   注: Windows SNMP サービスを再起動した場合、Netegrity SNMP エージェント サービスも手動で再起動する必要があります。

Windows 環境のポリシー サーバで SiteMinder SNMP サブエージェントを終了する方法

1. コントロールパネルの[サービス]を開きます。
   - (Windows Server)[スタート]、[設定]、[コントロール パネル]、[管理ツール]、[サービス]の順に選択します。
   - (Windows NT)[スタート]、[設定]、[コントロール パネル]、[サービス]の順に選択します。
2. Netegrity SNMP Agent サービスを選択します。
3. [停止]をクリックします。

   注: Windows SNMP サービスを停止すると、Netegrity SNMP エージェント サービスが全般的に使用できなくなりますが、ポート 801 を使用してアクセスすることは可能です。

UNIX 環境のポリシー サーバでの SNMP サポートの開始と終了

UNIX 環境のポリシー サーバでは、Sun Solstice エンタープライズ マスタ エージェント(snmpdx)デーモンを開始または停止することによってのみ、SiteMinder サービスを開始または終了できます。

UNIX 環境のポリシー サーバで Netegrity SNMP エージェント サービスを開始する方法

1. スーパーユーザ (ルート) としてログインします。
2. cd /etc/rc3.d と入力します。
3. sh SXXsnmpdx (S76snmpdx) stop と入力します。

UNIX 環境のポリシー サーバで Netegrity SNMP エージェント サービスを終了する方法

1. スーパーユーザ (ルート) としてログインします。
2. cd /etc/rc3.d と入力します。
3. sh SXXsnmpdx (S76snmpdx) start と入力します。

   注: Sun Solstice エンタープライズ マスタ エージェントの動作を停止させると、UNIX ホスト上のすべての SNMP サービスが無効になります。

SiteMinder SNMP モジュールのトラブルシューティング

このセクションでは、SiteMinder への管理接続を確立できない場合や、SiteMinder から SNMP トラップを受信できない場合に、障害の原因を容易に特定できるようにするための手順および SiteMinder で用意されているツールについて説明します。

イベントが発生しても SNMP トラップが受信されない

症状:

SNMP トラップが生成されるはずのイベントが発生しても、SNMP トラップが受信されない。

解決方法:

1. NMS と監視対象ポリシー サーバの間のネットワーク接続を確認します。
2. ポリシー サーバ上で SiteMinder SNMP サブエージェントと SNMP マスタ エージェントが動作していることを確認します。
3. システム環境変数の NETE_SNMPLOG_ENABLED を設定して、トラップログを有効にします。

   SiteMinder は、sminstalldir/log に以下のログファイルを生成します。

   Windows の場合 :

   ```
   SmServAuth_snmptrap.log
   SmServAz_snmptrap.log
   SmServAcct_snmptrap.log
   SmServAdm_snmptrap.log
   ```

   UNIX の場合 :

   ```
   smservauth_snmptrap.log
   smservaz_snmptrap.log
   smservacct_snmptrap.log
   smservadm_snmptrap.log
   ```

重要: 生成されるログファイルは、急速に大きくなることがあります。トラップの受信に関する問題が解決したら、すぐにトラップログを無効にして、ファイルを削除してください。

第 16 章: SiteMinder レポート

このセクションには、以下のトピックが含まれています。

レポートの説明

SiteMinder レポートは以下の 2 つのグループに分けられます。

- 監査レポート
- 分析レポート

監査レポートは、ポリシー サーバの既存の監査機能から作成されます。データベースへの書き込みを行うようにポリシー サーバを設定する必要があります。

分析レポートは、実行時のポリシー評価に基づいています(どのユーザが何のタスクを実行できるかの評価など)。

SiteMinder 管理 UI を使用すると、以下のレポートを生成できます。

ユーザ別アクティビティ

指定された期間内のユーザ アクティビティをすべてリスト表示します。

管理者による管理上の操作

管理者によって行われるポリシー ストア内の管理操作をすべてリスト表示します。

アプリケーション

ユーザが使用を許可されている設定済みのアプリケーションをすべてリスト表示します。

ユーザ別アプリケーション

指定されたアプリケーション セットのユーザをすべてリスト表示します。

拒否された認可

拒否された認可をすべてリスト表示します。

拒否されたリソース

リクエストされたリソースの拒否をすべてリスト表示します。

ロールごとのポリシー

アプリケーション内の指定されたロール セットのポリシーをすべてリスト表示します。

保護されたリソース

保護されたリソースをすべてリスト表示します(レルムフィルタ + ルールフィルタ)。

リソース アクティビティ

リソース別の認証アクティビティと許可アクティビティをすべてリスト表示します。

ユーザ別リソース

指定されたユーザ セットのリソースをすべてリスト表示します。

アプリケーション別ロール

指定された各アプリケーションについて定義されたロールをすべてリスト表示します。

リソース別ロール

指定されたリソースについて定義されたロールをすべてリスト表示します。

リソース別ユーザ

指定された各リソースに関連付けられているユーザをすべてリスト表示します。

ロール別ユーザ

指定されたロールに属するユーザをすべてリスト表示します。

SiteMinder レポートのスケジュール

管理 UI の[レポート]タブでは、SiteMinder の監査レポートまたは分析レポートをスケジュールできます。

SiteMinder レポートのスケジュール方法

1. [レポート]タブをクリックし、[監査]または[分析]をクリックします。
2. 実行するレポートを選択します。
3. 必要なパラメータをすべて入力します。パラメータはレポートごとに異なります。
4. [次へ] をクリックします。
5. ドロップダウン リストから、以下のオプションのいずれかを選択します。
   - **今すぐ**

     今すぐレポートを実行します。
   - **1 回**

     1 回だけレポートを実行します。
   - **毎時間**

     指定された時間単位の間隔でレポートを繰り返し実行します。
   - **毎日**

     指定された日単位の間隔でレポートを繰り返し実行します。
   - **毎週**

     指定された曜日 (1 つまたは複数) にレポートを実行します。
   - **毎月**

     指定された月単位の間隔でレポートを繰り返し実行します。
   - **毎月 N 日目**

     毎月の指定された日付にレポートを繰り返し実行します。
   - **最初の月曜日**

     毎月の最初の月曜日にレポートを実行します。

- **昨日**

  毎月の最終日にレポートを実行します。

- **毎月第 N 週 X 日目**

  毎月の指定された週と日付にレポートを実行します。

6. 説明を入力します。
7. [サブミット]をクリックします。

SiteMinder レポートの表示

管理 UI の[レポート]タブでは、ステータスが[完了]になっているすべての SiteMinder レポートを表示できます。ステータスが[失敗]である場合は、そのステータスの詳細を見ることができます。

SiteMinder レポートを表示する方法

1. [レポート]-[一般]-[SiteMinder レポートの表示]をクリックします。

   [SiteMinder レポート検索]ペインが表示されます。

2. 表示するレポートのラジオ ボタンをクリックします。レポートが完了済みであることが[ステータス]フィールドに示されている必要があることに注意してください。
3. [選択]をクリックします。

   レポートが画面に表示されます。

4. (オプション)レポートをファイルに保存すれ場合は、ファイル アイコンをクリックします。ドロップダウン リストから出力ファイル形式を選択します。
5. (オプション)レポートを印刷する場合は、プリンタ アイコンをクリックします。
6. (オプション)レポートの各ページを読んだり、検索文字列を入力したりできます。
7. レポートをすべて見たら、[閉じる]をクリックします。

SiteMinder レポートの削除

管理 UI の[レポート]タブでは、1 つ以上の SiteMinder レポートを削除できます。

SiteMinder レポートを削除する方法

1. [レポート]-[一般]-[SiteMinder レポートの削除]をクリックします。

   [SiteMinder レポートの削除]ペインが開きます。

2. 削除する SiteMinder レポートをレポート名または説明を条件にして検索するか、すべての SiteMinder レポートを検索します。
3. 削除する 1 つ以上の SiteMinder レポートまたはすべての SiteMinder レポートを選択し、[サブミット]をクリックします。

SiteMinder レポートの削除タスクが処理のためにサブミットされます。

反復レポート

反復レポート機能を使用すると、複数回実行するようにスケジュールされた SiteMinder レポートを管理できます。この機能により、以下のタスクを実行できます。

反復レポートの削除

1 つ以上の SiteMinder 反復レポートを削除します。

反復レポートの変更

選択した SiteMinder 反復レポートのスケジュールを変更します。

反復レポートの表示

選択した SiteMinder 反復レポートのスケジュールを表示します。

反復レポートの削除

管理 UI の[レポート]タブでは、1 つ以上の SiteMinder 反復レポートを削除できます。

反復レポートを削除する方法

1. [レポート]-[一般]-[反復レポート]-[反復レポートの削除]をクリックします。

   [反復レポートの削除]ペインが開きます。

2. 削除する反復レポートをレポート名または説明を条件にして検索するか、すべての反復レポートを検索します。
3. 削除する 1 つ以上の反復レポートまたはすべての反復レポートを選択し、[削除]をクリックして[OK]をクリックします。

   反復レポートの削除タスクが処理のためにサブミットされます。

反復レポートの変更

管理 UI の[レポート]タブでは、SiteMinder 反復レポートのスケジュールを変更できます。

反復レポートを変更する方法

1. [レポート]-[一般]-[反復レポート]-[反復レポートの変更]をクリックします。

   [反復レポートの変更]ペインが開きます。

2. 変更する反復レポートをレポート名または説明を条件にして検索するか、すべての反復レポートを検索します。
3. 変更する反復レポートを 1 つ選択し、[OK]をクリックします。

   選択した反復レポートのスケジュールのタイプ、詳細、開始時刻、および終了時刻が表示されます。

4. 反復レポートのスケジュールを変更し、[サブミット]をクリックします。

   反復レポートの変更タスクが処理のためにサブミットされます。

反復レポートの表示

管理 UI の[レポート]タブでは、SiteMinder 反復レポートのスケジュールを表示できます。

反復レポートを表示する方法

1. [レポート]-[一般]-[反復レポート]-[反復レポートの表示]をクリックします。

   [反復レポートの表示]ペインが開きます。

2. 表示する反復レポートをレポート名または説明を条件にして検索するか、すべての反復レポートを検索します。

3. 表示する反復レポートを 1 つ選択し、[OK]をクリックします。

   選択した反復レポートのスケジュール情報が表示されます。

4. [閉じる]をクリックします。

   [反復レポートの表示]ペインが閉じます。

第 17 章: ポリシー サーバのツール

このセクションには、以下のトピックが含まれています。

ポリシー サーバ ツールの概要

SiteMinder には、SiteMinder 環境の管理を支援する数多くの管理ツールが用意されています。以下のリストで、各ツールの機能を説明します。

smobjexport

エクスポート用の各種引数を備えています。エクスポートの対象として、ポリシー ストア全体、指定されたポリシードメイン、指定されたポリシードメインとそのポリシードメインによって使用されるすべてのシステム オブジェクト（管理者、エージェント、認証方式、ユーザ ディレクトリなど）、およびポリシー ストアに格納されているエージェント キーとその他のポリシー ストア データがあります。デフォルトでは、キーはエクスポートに含まれません。ポリシー ストアに格納されているエージェント キーのみ、変数のみがエクスポートされます。

smobjimport

ポリシー データを SiteMinder ポリシー ストアにインポートします。

smkeyexport

キー ストアからキーをエクスポートします。

smkeyimport

キーをキー ストアにインポートします。

smldapsetup

LDAP ディレクトリ内の SiteMinder ポリシー ストアを管理します。

ODBC データベースの SQL スクリプト

ODBC データベースから SiteMinder ポリシー ストア、トークン データ、およびログ スキーマを削除します。

smpatchcheck

必要なパッチと推奨されるパッチがすべて Solaris マシンにインストールされていることを確認します。

smreadclog

ポリシー サーバによって生成された RADIUS ログ ファイルを読み取ります。

smreg

SiteMinder スーパーユーザ パスワードを変更できます。

SiteMinder には、ポリシー データを操作するためのツールもあります。以下のリストに、XPS ツール ファミリーの概要を示します。XPS ツールは、ポリシー ストア データを管理する目的で XPS 管理者が使用できる、プラットフォームに依存しないコマンド ライン ユーティリティです。特定のツールのオプションを表示するには、コマンド ラインでツール名に続いて -? パラメータを入力します。

XPSConfig

ベンダー、製品、製品パラメータなどの設定データを管理します。

注: XPSConfig を使用するには、XPSConfig の権限を持った管理者である必要があります。

XPSEvaluate

式を評価し、パフォーマンスのテストを許可します。

注: XPSEvaluate を使用するには、XPSEvaluate の権限を持った管理者である必要があります。

XPSExplorer

ベンダー、製品、アプリケーションなどのポリシー データを管理します。

注: XPSExplorer を使用するには、XPSExplorer の権限を持った管理者である必要があります。

XPSExport

XPS データ ストアからデータをエクスポートします。

XPSImport

XPS データ ストアにデータをインポートします。

XPSSecurity

XPS 管理者とその権限を対話形式で作成および編集できます。このツールを使用するには、SiteMinder インストール ファイル(CA からダウンロードしたファイル)の ¥win32¥tools または /solaris/tools から、policy_server_home¥bin ディレクトリにツールをコピーします。

policy_server_home

ポリシー サーバのインストール パスを指定します。

重要: XPSSecurity を使用した後は、不正使用を防ぐため、*policy_server_home*¥bin から削除してください。

注: XPSSecurity を使用するには、XPSSecurity の権限を持った管理者である必要があります。

XPSSweeper

XPS と SiteMinder のポリシー ストアを同期します。

注: XPSSweeper を使用するには、管理者である必要があります。その他の権限は必要はありません。

Windows 2008 ポリシー サーバ ツール要件

Windows Server 2008 上で SiteMinder ユーティリティまたは実行可能ファイルを実行している場合、管理者としてシステムにログインしていても、必ず管理者権限でコマンド ライン ウィンドウを開くようにしてください。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。

Linux Red Hat 上でポリシー サーバのツールを使用する場合の要件

ポリシー サーバのツール（smreg、smobjimport、smobjexport）を Linux Red Hat オペレーティング システム上で正しく動作させるには、/etc/hosts 内でポリシー サーバのホスト名を定義する必要があります。これらのユーティリティは adminoid と OID を生成するので、ホスト名はこの場所で定義されている必要があります。Linux Red Hat オペレーティング システムでは、これらの OID を生成するとき、Linux 関数の gethostid() および gettimeofday() が使用されます。

smobjexport

smobjexport ツールは、smobjexport によって作成される 2 つのファイル、.smdif（SiteMinderData Interchange Format）および .cfg（環境設定）ファイルを作成して、ポリシー ストア全体または 1 つのポリシー ドメインをエクスポートします。タイプの異なるポリシー ストアにインポートできるように、SiteMinder データは .smdif ファイルによって標準化されます。たとえば、.smdif 形式のファイルを ODBC データベースからエクスポートし、LDAP ディレクトリにインポートできます。

環境設定（.cfg）ファイルには、IP アドレス、リダイレクト URL、共有秘密キー、エージェント名、ロギング設定、.com 拡張子など、ポリシー ストアの環境固有のプロパティが含まれています。.cfg ファイル内のテキストはタブで区切られているので、任意のテキスト エディタまたは Microsoft Excel でタブ区切りファイルとして編集できます。

注: コマンド ライン インターフェースを使用すると、すべてのポリシー ストア オブジェクトではなく、特定のオブジェクトをインポートおよびエクスポートするための Perl スクリプトを作成できます。詳細については、「*Programming Guide for Perl*」を参照してください。

以下の表で、.cfg ファイルにあるサンプル登録方式エントリの 4 つのフィールドについて説明します。

オブジェクト OID	オブジェクト クラス	プロパティ タイプ	値
<*登録方式 OID*>	SelfReg	RegistrationURL	http://your.url.com

以下のような OID は長すぎて表示できないので、[オブジェクト OID]列は *OID* 変数によってのみ表されます。

reg_scheme_OID = 0d-6dc75be0-1935-11d3-95cc-00c04f7468ef

各エントリのフィールド([オブジェクト OID]、[オブジェクト クラス]、[プロパティ タイプ]、[値])は、テキスト エディタまたは Excel で編集できます。

注: 下位互換性のため、smobjexport コマンド ラインでは .smdif ファイルのみ参照されます。その結果、対応する環境設定ファイルは次の命名規則に従って作成されます。smobjexport コマンドで指定する出力ファイルが .smdif 拡張子(*file_name*.smdif など)を持っている場合、その拡張子は設定ファイルで .cfg (*file_name*.cfg など)に置き換えられます。ただし、指定する出力ファイルが .smdif 拡張子を持っていない場合は(*file_name*.txt など)、ファイル名と拡張子の後に .cfg が付加されます(*file_name*.txt.cfg など)。

smobjexport では、以下の引数を使用して、データのエクスポートに必要な情報を指定します。

-o*file_name*

.smdif 出力ファイルのパスとファイル名を指定します。この引数を指定しない場合、デフォルトの出力ファイル名は stdout.smdif と stdout.cfg になります。このファイル名は smldapsetup ldgen -f*file_name* に使用したもの以外である必要があります。そうでないと、エクスポートは上書きされます。

-f

既存の出力ファイルを上書きします。

-s*domain-name*

指定されたポリシー ドメインのみをエクスポートします。

-e*domain-name*

指定されたポリシー ドメインと、以下を含む、ポリシー ドメインによって使用されるすべてのシステム オブジェクト(管理者、エージェント、認証方式、ユーザ ディレクトリなど)をエクスポートします。

- システム オブジェクトのいずれかがホスト設定オブジェクトである場合は、すべてのホスト設定オブジェクトがエクスポートされます。

- システム オブジェクトのいずれかがエージェント設定オブジェクトである場合は、すべてのエージェント設定オブジェクトがエクスポートされます。
- システム オブジェクトのいずれかがアフィリエイト（ポリシー サーバ オプション パックがインストールされているとき）である場合は、アフィリエイトが属するドメイン全体がエクスポートされます。

-c

機密データをクリアテキストとしてエクスポートします。データをクリアテキストとしてエクスポートすると、1 つの暗号化キーを使用する SiteMinder 環境のポリシー データを、それとは別の暗号化キーを使用する他の SiteMinder 環境に移行できます。-c を使用するには、SiteMinder ドメイン オブジェクトをすべて管理できる SiteMinder 管理者のクレデンシャルが必要です。-d および -w の引数を使用して、クレデンシャルを入力します。

-cb

下位互換の暗号で暗号化された機密データをエクスポートします。

-cf

FIPS-140 互換の暗号で暗号化された機密データをエクスポートします。

-d*admin-name*

エクスポート対象となるポリシー ストア内の SiteMinder オブジェクトをすべて管理できる SiteMinder 管理者のログイン名を指定します。

-w*admin-pw*

-d で指定した SiteMinder 管理者のパスワードを指定します。

-k

ポリシー ストアに格納されているエージェント キーをその他のポリシー ストア データと共にエクスポートします。デフォルトでは、キーはエクスポートに含まれません。

-x

ポリシー ストアに格納されているエージェント キーのみをエクスポートします。

-v

詳細モードを有効にします。

-t

低レベルのトレース モードを有効にします。エクスポート プロセスのトラブルシューティングに使用できます。

-u

変数のみエクスポートします。

-l

ログ ファイルを作成します。*file_name*.smdif ファイルが .txt または他の拡張子ではなく、.smdif で終わっていることを確認してください。*file_name*.smdif ファイルが .smdif 拡張子で終わっていると、smobjexport では .log 拡張子が付いたログ ファイルが作成されます。*file_name*.smdif ファイルが .txt 拡張子で終わっていると、smobjexport では *file_name*.txt.log ファイルが作成されます。ログ ファイルは *file_name*.log の形式である必要があるので、このファイル名は正しくありません。

-m

IdentityMinder オブジェクトのみエクスポートします。

-i

特定の IdentityMinder オブジェクトおよび関連するすべてのシステム オブジェクトをエクスポートします。

-j

特定の IdentityMinder ディレクトリおよび関連するすべてのシステム オブジェクトをエクスポートします。

-?

ヘルプ メッセージを表示します。

注: 引数に空白が含まれる場合は、引数全体を二重引用符で囲みます。たとえば、SiteMinder 管理者の名前が *SiteMinder Admin* である場合、smobjexport に対する引数は
-d" SiteMinder Admin" となります。

依存関係を持つポリシー ストア オブジェクトのエクスポート

依存関係を持つポリシー ストア オブジェクトをエクスポートするときは、コマンド ライン インターフェースで、smobjexport を -e オプションを指定して実行するか、移行の方法を使用します。

- オブジェクトの依存関係のいずれかがホスト設定オブジェクトである場合は、すべてのホスト設定オブジェクトがエクスポートされます。
- オブジェクトの依存関係のいずれかがエージェント設定オブジェクトである場合は、すべてのエージェント設定オブジェクトがエクスポートされます。
- オブジェクトの依存関係のいずれかがアフィリエイト(ポリシー サーバ オプション パックがインストールされているとき)である場合は、アフィリエイトが属するアフィリエイト ドメイン全体がエクスポートされます。

注: -e オプションを使用してアフィリエイト ドメインをエクスポートすることはできません。

smobjimport によるポリシー データのインポート

smobjimport ツールを使用して、ポリシー ストア全体または 1 つのポリシー ドメインをインポートできます。

smobjimport を使用してポリシー データをインポートする方法

1. 次のいずれかのディレクトリに移動します。
   - Windows の場合: *SiteMinder_installation*¥bin

   SiteMinder_installation

   SiteMinder のインストール場所を示します。
   - UNIX の場合: *SiteMinder installation*/bin

   SiteMinder_installation

   SiteMinder のインストール場所を示します。
2. 以下のコマンドを入力します。

   `smobjimport -i`*`file_name`* `-d`*`admin-name`* `-w`*`admin-pw`* `-v -t`

   例: smobjimport -ipstore.smdif -dSiteMinder -wpassword -v -t

   注: 入力するのは .smdif ファイルと smobjimport コマンドだけです。.smdif ファイルと .cfg ファイルが同じディレクトリ内にあれば、どちらも自動的にインポートされます。.cfg ファイルに格納されている環境のプロパティは、.smdif ファイルに格納されている環境のプロパティに優先します。したがって、smobjimport を実行するときに .smdif ファイルを別の .cfg ファイルと組み合わせれば、環境のデータを上書きできます。

XML ベースのデータ形式の概要

エンタープライズ環境では、ポリシー ストア データを環境間で移動しなければならない場合があります(開発環境からステージング環境へ、など)。r12 より前のリリースでは、ポリシー オブジェクトは専用の SiteMinder Data Interchange Format (SMDIF)を使用して表現され、データの移行には smobjimport および smobjexport を使用していました。このエクスポート形式は XML ベースのエクスポート形式に置き換えられ、データ移行ツールは XPSExport および XPSImport になりました。

XML ベースのエクスポート形式では、以下の基本スキーマを使用します。

XPSDeployment.xsd

トップレベルのスキーマを記述します。この下にその他のスキーマが含まれます。ルート要素とサブ要素を定義します。このスキーマに準拠した XML ファイルは、データ ディクショナリ、ポリシー、およびセキュリティ データのインスタンスを含むことができます。

XPSDataDictionary.xsd

オブジェクト タイプとそれらのプロパティに関するメタデータ情報を記述します。

XPSPolicyData.xsd

ポリシー ストアに格納されるオブジェクト(ドメイン、ポリシー、ルール、アプリケーション、オブジェクト間のリレーションシップなど)に関するメタデータ情報を記述します。

XPSSecurityData.xsd

ポリシー ストア管理者および管理者のアクセス権限を表すために使用されるメタデータを記述します。

XPSGeneric.xsd

その他のスキーマ ファイル内で使用される一般的なデータ型の定義が含まれます。

この形式はポリシー データ全体のエクスポートとインポートをサポートしているだけでなく、ポリシー データのサブセットのエクスポートとインポートもサポートしています。オブジェクト単位のエクスポートでは、データのインポート方法に関する知識が要求されます。エクスポート時は、ポリシー データ全体またはデータの一部(オブジェクト識別子を使用)と、オプションで以下の 3 つのエクスポート タイプのいずれかを指定できます。

- Add - インポート時に追加のみ実行できることを明示します。
- Replace - インポート時に既存のポリシー データを上書きすることを明示します。
- Overlay - インポート時にポリシー データを更新することを明示します。

注: XPSExport および XPSImport ツールは、ポリシー サーバが動作している FIPS モードに基づいて機密データを暗号化します。これらのツールには、データ暗号化のために設定する追加パラメータはありません。

XPSExport

XPSExport ツールは、ポリシー ストア データを移行するための以下のタスクをサポートしています。

- 全データ ディクショナリのエクスポート
- 全セキュリティ データのエクスポート
- 全ポリシー データのエクスポート
- 全設定データのエクスポート
- 一部のポリシー データのエクスポート

ルート オブジェクトの識別子をコマンド ラインまたはファイルで指定すると(-xf パラメータを使用)、ポリシー データのサブセットをエクスポートできます。親クラスを持たないオブジェクトのみをエクスポートすることもできます。たとえば、レルム オブジェクトをエクスポートするには、レルムの親ドメインの識別子(XID)を指定します。

また、XPSExplorer の「ショッピング カート」(XCart)機能を使用すれば(xpsexplorer -xf)、カスタム エクスポート ファイルを作成および編集できます。XCart ファイル内では、個々のオブジェクト単位でインポート モード(ADD、OVERLAY、REPLACE、または DEFAULT)を設定できます。次に -xf パラメータを使用して、XCart ファイルを XSPExport に渡すことができます。

以下の点について考慮してください。

- XPSExport では、キー ストアからのキーのエクスポートは行いません。キーをエクスポートするには、smkeyexport を使用する必要があります。
- アップグレードまたはポリシー移行の一環として、SiteMinder ポリシーをある環境から別の環境に移動させる場合、環境に固有の一部のオブジェクトがエクスポート ファイルに含まれます。これらのオブジェクトにはたとえば以下のものがあります。
  - トラステッド ホスト
  - HCO ポリシー サーバ設定
  - 認証方式 URL
  - パスワード サービス リダイレクト
  - リダイレクト レスポンス

XPSExport を使用するときに選択したモードによって、これらのオブジェクトは新しい環境に追加されるか、または既存の設定を上書きします。オブジェクトをインポートする際は、環境設定を誤って変更することがないよう注意が必要です。

構文

XPSExport の構文は以下のとおりです。

```
XPSExport output_file [-xo object_XID] [-xo-add object_XID] [-xo-replace object_XID]
[-xo-overlay object_XID] [-xf file_name] [-xa] [-xd] [-xs] [-xc] [-passphrase phrase]
[-?] [-vT] [-vI] [-vW] [-vE] [-vF] [-l log_file] [-e err_file]
```

パラメータ

output_file

XML 出力ファイル。

-xo *object_XID*

オブジェクト単位のエクスポートで 1 つ以上のオブジェクトを指定します。以下のエクスポート タイプのいずれかを指定することもできます。

-xo-add *object_XID*

インポート時に追加のみ行うことを明示します。

-xo-replace *object_XID*

インポート時にポリシー データを上書きすることを明示します。

-xo-overlay *object_XID*

インポート時にポリシー データを更新することを明示します。

-xf *file_name*

(オプション) エクスポートするオブジェクトの XID のリストを含むファイルの絶対名を指定します。

ファイル内のエントリは以下の形式になります。

CA.SM::UserDirectory@0e-255e2456-556d-40fb-93cd-f2fed81f656e

ADD = CA.SM::AuthScheme@0d-4afc0e41-ae25-11d1-9cdd-006008aac24b

REPLACE = CA.SM::Agent@01-cb8b3401-a6aa-4794-964e-c569712269c0

OVERLAY = CA.SM::Domain@03-7bdf31f2-44d7-4d7b-a8f5-5de2eaa0b634

これらのエントリは、以下のコマンド ライン パラメータに対応します。

```
-xo CA.SM::UserDirectory@0e-255e2456-556d-40fb-93cd-f2fed81f656e
-xo-add CA.SM::AuthScheme@0d-4afc0e41-ae25-11d1-9cdd-006008aac24b
-xo-replace CA.SM::Agent@01-cb8b3401-a6aa-4794-964e-c569712269c0
-xo-overlay CA.SM::Domain@03-7bdf31f2-44d7-4d7b-a8f5-5de2eaa0b634
```

-xa

(オプション) ポリシー データ全体をエクスポートします。

注: このオプションを、-xo、-xo-add、-xo-replace、-xo-overlay、または -xf と一緒に使用することはできません。

-xd

(オプション) 全データ ディクショナリをエクスポートします。

-xs

(オプション) 全セキュリティ データをエクスポートします。

-xc

(オプション) 全設定データをエクスポートします。

-passphrase *phrase*

(オプション) 機密データの暗号化に必要なパスフレーズを指定します。パスフレーズは、長さが 8 文字以上で、1 つ以上の数字、1 つ以上の大文字、および 1 つ以上の小文字を含んでいる必要があります。引用符で囲まれた空白を含めることもできます。パスフレーズをコマンド ライン オプションとして指定しなかった場合、機密データをエクスポートするとき入力を求められます。

-?

コマンド ラインのヘルプを表示します。

-vT

(オプション) 詳細レベルを TRACE に設定します。

-vI

(オプション) 詳細レベルを INFO に設定します。

-vW

(オプション) 詳細レベルを WARNING に設定します (デフォルト)。

-vE

(オプション) 詳細レベルを ERROR に設定します。

-vF

（オプション）詳細レベルを FATAL に設定します。

-l log_file

（オプション）指定されたファイルにログを出力します。

-e err_file

（オプション）エラーと例外をログ記録するファイルを指定します。省略した場合、stderr が使用されます。

例

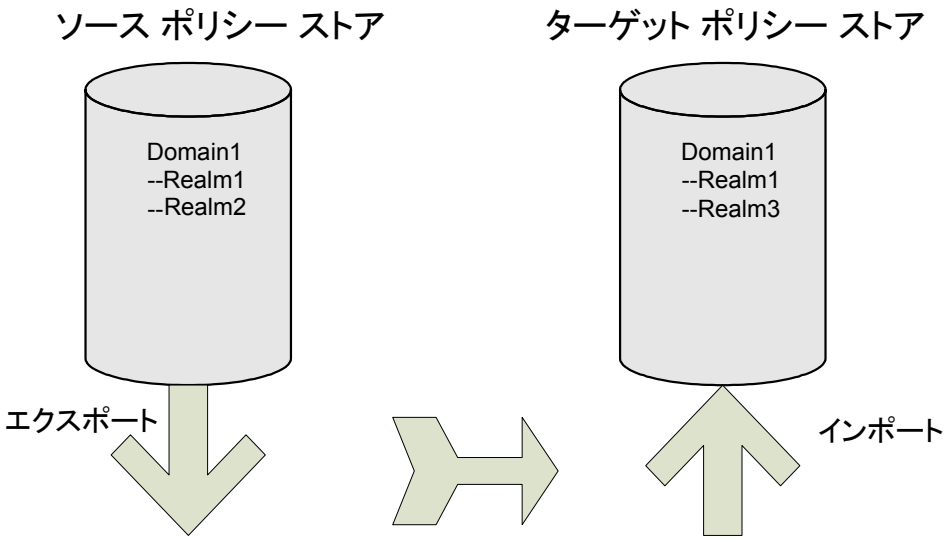
```
XPSExport PolicyData.xml -xo
CA.SM::UserDirectory@0e-255e2456-556d-40fb-93cd-f2fed81f656e
-xo-overlay CA.SM::Domain@03-7bdf31f2-44d7-4d7b-a8f5-5de2eaa0b634 -xd -e
C:¥tmp¥ExceptionLog.txt
```

注: オブジェクト単位のエクスポートでは、エクスポート タイプの指定は、コマンド ラインで明示的に行うか、コマンド ラインで指定されなかった場合は、データ ディクショナリ辞書から取得されます。ダンプ エクスポートでは、すべてのオブジェクトのエクスポート タイプ属性は Replace です（オブジェクト クラスに対して設定されているデータ ディクショナリ値に関係なく）。ポリシー データのロード インポートは実質的に、ポリシー ストア内の全ポリシー データを上書きするためです。

XPSExport の実行中にコマンド ライン オプションの解析でエラーが発生した場合、エクスポート ツールは実行が中止され、発生したエラーのログが例外ファイル（または stderr）に記録されます。 *任意の*オブジェクトのエクスポートが失敗した場合も、エクスポート プロセスは中止されます。その場合は、該当するエラーのログが例外ファイル（または stderr）に記録され、XML 出力ファイル（作成されている場合）が削除されます。

ポリシー データの追加

以下の図は、ソース ポリシー ストア内にある Domain1 という名前の SiteMinder ポリシー ドメインを示しています。Domain1 は、エクスポートして、ターゲット ポリシー ストアにインポートする必要があります。



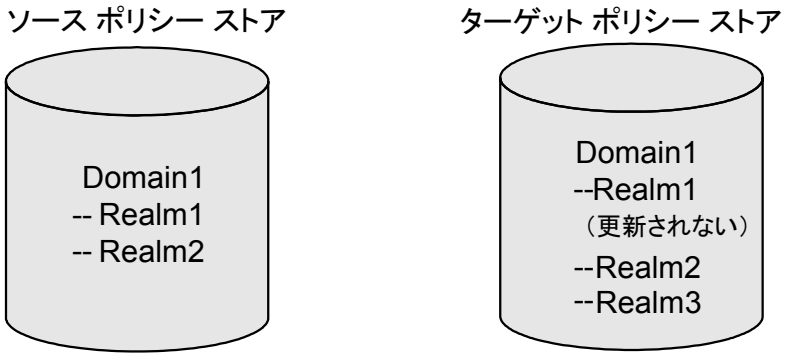
ターゲット ポリシー ストアには同じ名前を持つドメインがすでにありますが、この 2 つのドメインには以下のような違いがあります。

- ソース ポリシー ストアでは Realm1 のプロパティが更新されているため、ターゲット ポリシー ストアの Realm1 のプロパティとは異なる値を持ちます。
- Domain1 には、ターゲット ポリシー ストアには存在しない Realm2 があります。

ターゲット ポリシー ストアに 1 つのオブジェクト(Realm2)のみインポートする詳細インポートを指定するための、エクスポート時のコマンド ラインは以下のようになります。

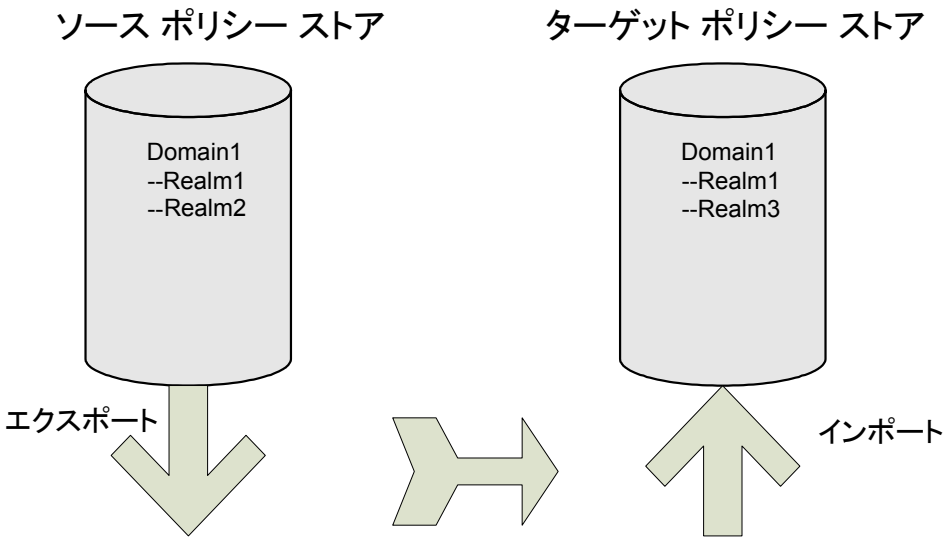
```
XPSExport gran-add.xml -xo-add
CA.SM: :Domain@03-0fb7bd02-6986-4bb9-b240-c232358958b1
```

インポートに成功すると、ターゲット ポリシー ストアの Domain1 には 3 つのレルムが含まれます。以下の図に示すとおり、Realm1 のプロパティは更新されません。



ポリシー データの上書き

以下の図は、ソース ポリシー ストア内にある Domain1 という名前の SiteMinder ポリシー ドメインを示しています。Domain1 は、エクスポートして、ターゲット ポリシー ストアにインポートする必要があります。



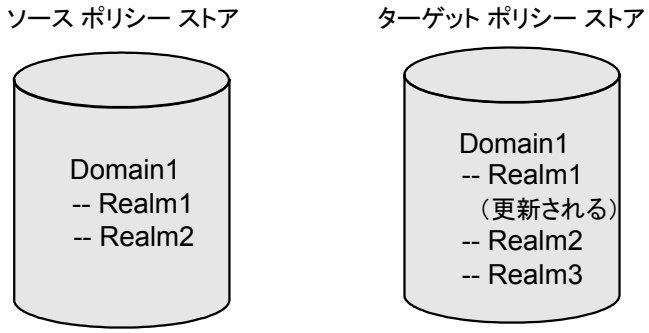
ターゲット ポリシー ストアには同じ名前を持つドメインがすでにありますが、この 2 つのドメインには以下のような違いがあります。

- ソース ポリシー ストアでは Realm1 のプロパティが更新されているため、ターゲット ポリシー ストアの Realm1 のプロパティとは異なる値を持ちます。
- Domain1 には、ターゲット ポリシー ストアには存在しない Realm2 があります。

ソース ポリシー ストアの最新の変更内容を使用してターゲット ポリシー ストアを更新する詳細インポートを指定するための、エクスポート時のコマンド ラインは以下のようになります。

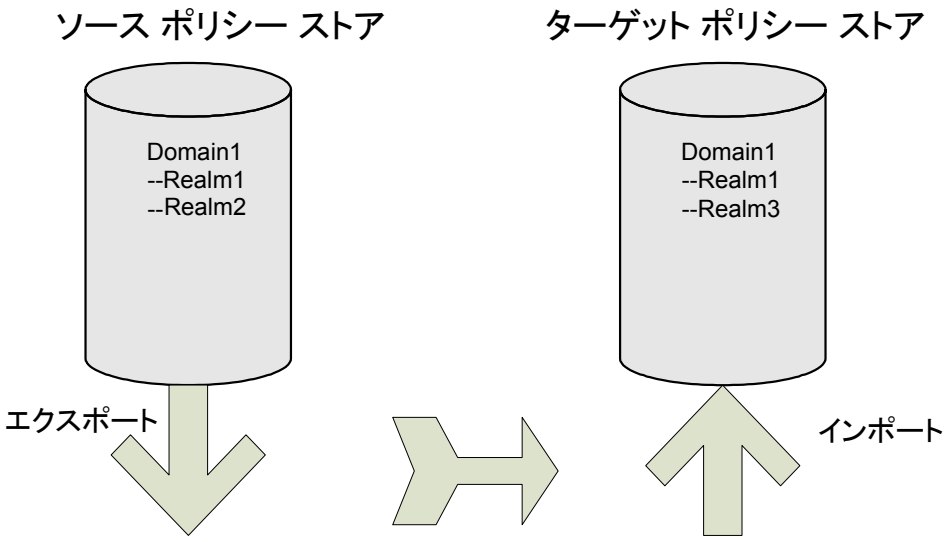
```
XPSExport gran-add.xml -xo-overlay
CA.SM: :Domain@03-0fb7bd02-6986-4bb9-b240-c232358958b1
```

以下の図に示すとおり、インポートに成功すると、ターゲット ポリシー ストアの Realm1 のプロパティが更新されます。



ポリシー データの置換

以下の図は、ソース ポリシー ストア内にある Domain1 という名前の SiteMinder ポリシー ドメインを示しています。Domain1 は、エクスポートして、ターゲット ポリシー ストアにインポートする必要があります。



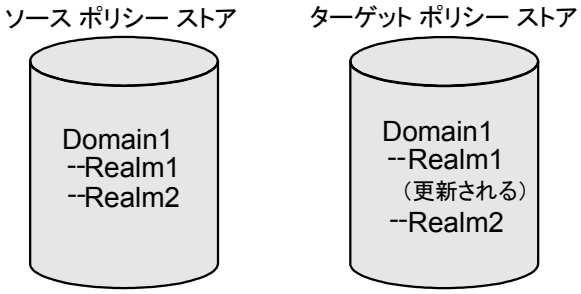
ターゲット ポリシー ストアには同じ名前を持つドメインがすでにありますが、この 2 つのドメインには以下のような違いがあります。

- ソース ポリシー ストアでは Realm1 のプロパティが更新されているため、ターゲット ポリシー ストアの Realm1 のプロパティとは異なる値を持ちます。
- Domain1 には、ターゲット ポリシー ストアには存在しない Realm2 があります。

ソース ポリシー ストアの内容をターゲット ポリシー ストアに複製するための、エクスポート時のコマンド ラインは以下のようになります。

```
XPSExport gran-add.xml -xo-replace
CA.SM: :Domain@03-0fb7bd02-6986-4bb9-b240-c232358958b1
```

以下の図に示すとおり、インポートに成功すると、ターゲット ポリシー ストアの Domain1 はソース ポリシー ストアの Domain1 とまったく同じになります。



XPSImport

XPSImport ツールは、ポリシー ストア データを移行するための以下のタスクをサポートしています。

- 全ポリシー データのインポート
- 一部のポリシー データのインポート
- 設定データのインポート

注: XPSImport ではキー ストアへのキーのインポートは行いません。キーをインポートするには、smkeyimport を使用する必要があります。

構文

XPSImport の構文は以下のとおりです。

```
XPSImport input_file [-passphrase phrase] [-validate] [-fo] [-vT] [-vI] [-vW] [-vE] [-vF] [-e
file_name] [-l log_path] [-?]
```

パラメータ

input_file

入力 XML ファイルを指定します。

-passphrase *phrase*

（オプション）機密データの復号化に必要なパスフレーズを指定します。パスフレーズはエクスポート時に指定されたものと同じである必要があります。異なっている場合、復号化は失敗します。

-validate

（オプション）データベースを更新せずに、XML 入力ファイルを検証します。

-fo

ダンプ ロードで既存のポリシー ストアの上書きを強制できます。

-vT

(オプション) 詳細レベルを TRACE に設定します。

-vI

(オプション) 詳細レベルを INFO に設定します。

-vW

(オプション) 詳細レベルを WARNING に設定します (デフォルト)。

-vE

(オプション) 詳細レベルを ERROR に設定します。

-vF

(オプション) 詳細レベルを FATAL に設定します。

-l *log_path*

(オプション) 指定されたパスにログ ファイルを出力します。

-e *file_name*

(オプション) エラーと例外をログ記録するファイルを指定します。省略した場合、stderr が使用されます。

-?

コマンド ラインのヘルプを表示します。

例

```
XPSImport PolicyData.xml -e C:¥¥tmp¥¥ExceptionLog.txt
```

この例では、PolicyData.xml ファイル内で指定されているポリシー データ オブジェクトをインポートします。インポートがダンプ ロードであるか、オブジェクト単位であるかどうかは、コマンド ラインからはすぐにはわかりません。ただし、その情報は、XML 入力ファイル内の <PolicyData> 要素の IsDumpExport 属性を見ることによって確認できます。この属性が true に設定されている場合は、XML 入力ファイルをダンプ ロードに使用する必要があることを意味します。

ポリシー データ転送のトラブルシューティング

ポリシー ストア データの転送時には、以下の要素が関連してくる可能性があります。

- エラーは、コンソール（stdout/stderr）に出力されるか、ファイルに転送されます。
- ロギングのレベルは以下のようにリスト表示されます。
  - トレース
  - 情報
  - 警告
  - クリティカル
  - 致命的
- すでにファイルが存在する場合、エクスポートは失敗します。
- XML ファイル内のオブジェクトについて検証が失敗した場合、インポートはロールバックされます。
- 追加タイプによってエクスポートしたオブジェクトがターゲット ポリシー ストア内にすでに存在する場合、詳細インポートは失敗します。

smkeyexport

smkeyexport ツールは、キー ストアからキーをエクスポートします。smkeyexport の構文は以下のとおりです。

smkeyexport -d*adminname* -w*adminpw* [-o*output_filename*] [-f] [-c] [-cb] [-cf] [-l] [-v] [-t] [-?]

-d

SiteMinder 管理者の名前を指定します。

-w

SiteMinder 管理者のパスワードを指定します。

-o

（オプション）。出力ファイルを指定します。デフォルトは stdout.smdif です。

-f

（オプション）既存の出力ファイルを上書きします。

-c

（オプション）。暗号化されていない機密データをエクスポートします。

-cb

（オプション）。下位互換の暗号で暗号化された機密データをエクスポートします。

-cf

（オプション）。FIPS 互換の暗号で暗号化された機密データをエクスポートします。

-l

（オプション）。指定されたファイル（filename.log）を作成し、エントリのログを記録します。

-v

（オプション）。詳細メッセージングを指定します。

-t

（オプション）。トレースを有効にします。

-?

（オプション）。コマンド オプションを表示します。

smldapsetup

smldapsetup ユーティリティを使用すると、コマンド ラインから LDAP ポリシー ストアを管理できます。smldapsetup では、LDAP ポリシー ストアの設定、LDIF ファイルの生成、およびポリシー ストア データとスキーマの削除が可能です。

smldapsetup を使用するには、モードを指定します。モードによって、smldapsetup が実行するアクションと、LDAP サーバの設定に使用する値を含む引数が決まります。

以下の表は、smldapsetup で使用できるモードと、各モードで使用される引数を示しています。

モード	引数
reg	-h*host*、-p*portnumber*、-d*userdn*、 -w*userpw*、-r*root*、 -ssl*1*|*0*、-c*certdb*、-k1
ldgen	-h*host*、-p*portnumber*、-d*userdn*、 -w*userpw*、-r*root*、 -m*n*、-ssl*1*|*0*、-c*certdb* -f*ldif*、-t*tool*、-s*suffix*、-e、-k
ldmod	-h*host*、-p*portnumber*、-d*userdn*、 -w*userpw*、-r*root*、 -ssl*1*|*0*、-c*certdb*、-f*ldif*、 -s*suffix*、-e、-k、-i
remove	-h*host*、-p*portnumber*、-d*userdn*、 -w*userpw*、 -r*root*、-ssl*1*|*0*、 -c*certdb*、-k
switch	なし
revert	-v
status	-v

smldapsetup を使用する方法

1. 次のいずれかのディレクトリに移動します。
   - （Windows）*siteminder_home*¥bin
   - （UNIX）*siteminder_home*/bin

   siteminder_home

   SiteMinder のインストール場所を示します。

2. 以下のコマンドを入力します。

   `smldapsetup` *mode arguments*

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

   例: smldapsetup reg -hldapserver.mycompany.com -d"LDAP User" -wMyPassword123 -ro=security.com

   注: smldapsetup を実行する場合は、指定する LDAP ユーザが LDAP ディレクトリ サーバ内のスキーマを変更するために適切な管理者権限を持っていることを確認してください。このユーザが適切な権限を持っていないと、LDAP サーバでのポリシー ストア スキーマの生成ができなくなります。smldapsetup コマンドを実行した後、このユーザはポリシー サーバ管理コンソールの[データ]タブにある[管理ユーザ名]フィールドに表示されます。

詳細情報:

smldapsetup のモード (P. 197)
smldapsetup の引数 (P. 199)

smldapsetup のモード

モードは smldapsetup が実行するアクションを指定します。LDAP サーバへの接続、LDIF ファイルの生成、LDAP ポリシー ストアの設定、およびポリシー データの削除を行うためのモードを指定できます。

smldapsetup のモードには、以下のものが含まれます。

reg

LDAP サーバへの接続をテストします。接続が成功する場合、-h*host*、-p*portnumber*、-*duserdn*、-w*userpw*、-r*root*、-ssl*1/0*、および -c*certdb* の各引数を使用して smldapsetup を実行すると、SiteMinder LDAP サーバがそのポリシー ストアに設定されます。

ldgen

サポートされている LDAP サーバを自動的に検出し、SiteMinder スキーマを使用して LDIF ファイルを生成します。生成されたファイルを smldapsetup ldmod と共に使用すると、SiteMinder スキーマが作成されます。-e 引数を指定して smldapsetup ldgen を実行すると、LDIF ファイルが作成され、この LDIF ファイルを ldmod と共に使用すると、SiteMinder スキーマを削除できます。LDAP サーバの自動検出をスキップするには、-m スイッチを使用します。以前に reg モードで設定されていない場合、ldgen モードを使用するには -f スイッチが必要です。

ldmod

ポリシー ストアにデータを入力せずに、LDAP サーバおよび SiteMinder スキーマに接続します。ldapmodify プログラム、および *-fldif* 引数と共に指定する LDIF ファイルが必要になります。-h*host*、-p*ort_number*、-d*userdn*、-w*userpw*、-r*root*、-ssl*1/0*、および -c*certdb* の各引数を指定して smldapsetup ldmod を実行すると、これらの引数によって指定される LDAP ディレクトリが変更されます。-h*host*、-p*portnumber*、-d*userdn*、-*wuserpw*、-r*root*、-ssl*1/0*、および -c*certdb* を指定しないで smldapsetup ldmod を実行すると、smldapsetup reg またはポリシー サーバ管理コンソールで以前に定義した LDAP ディレクトリが使用されます。

remove

LDAP サーバに接続し、現在のバージョンの smldapsetup に対応する SiteMinder LDAP ノード以下に格納されているポリシー データをすべて削除します。*-hhost*、-p*port_number*、-d*userdn*、-w*userpw*、-r*root*、-ssl*1/0*、および -c*certdb* の各引数を指定して smldapsetup remove を実行すると、これらの引数によって指定される LDAP ディレクトリからデータが削除されます。-h*host*、-p*port*、-d*userdn*、-w*userpw*、-r*root*、-*ssl1/0*、および -*ccertdb* を指定しないで smldapsetup を実行すると、smldapsetup reg またはポリシー サーバ管理コンソールで以前に定義した LDAP ディレクトリからポリシー データが削除されます。

switch

ODBC の代わりに LDAP を使用するようにポリシー サーバを再設定します。変更を行う前に LDAP ストアまたは LDAP 接続パラメータの準備はしません。

revert

ポリシー ストアを LDAP から ODBC に戻します。このモードで使用される唯一の引数は -v です。

status

LDAP ポリシー ストアの接続パラメータが正しく設定されていることを確認します。-v 引数が必要です。smldapsetup status を -h*host*、-p*port_number*、-d*userdn*、-w*userpw*、-r*root*、-ssl*1/0*、および -c*certdb* の各引数を指定して実行すると、これらの引数によって指定される LDAP ディレクトリへの接続がテストされます。-h*host*、-p*port_number*、-*duserdn*、-w*userpw*、-r*root*、-ssl*1/0*、および -c*certdb* を指定しないで smldapsetup status を実行すると、smldapsetup reg またはポリシー サーバ管理コンソールで以前に定義した LDAP ディレクトリへの接続が確認されます。

ポリシー サーバ管理コンソールの[データ]タブでは、reg、switch、および revert 機能を使用して行った設定を GUI インターフェースから表示または変更できます。ldgen、ldmod、remove、および status 機能を実行するには、smldapsetup を使用する必要があります。

smldapsetup の引数

引数を使用することによって、LDAP ポリシー ストアを管理するための各種モードで使用される情報を指定できます。引数を指定しないで smldapsetup を実行すると、ポリシー サーバ管理コンソールで設定した値が使用されます。

注: smldapsetup の場合、引数とその値との間に空白は使用できません。たとえば、-h 引数は以下のように指定する必要があります。
smldapsetup ldmod -hldapserver.mycompany.com

smldapsetup のコールで指定できる引数を以下に示します。

-h*host*

LDAP サーバの完全修飾名、マシンが同じドメイン内にある場合は相対名（hldapserver）、または IP アドレス（-h123.12.12.12）を指定します。ホストを指定しないで smldapsetup を実行すると、以前に設定した値がデフォルトで使用されます。

例: -hldapserver.mycompany.com

-p*ort_number*

非標準の LDAP ポートを指定します。LDAP サーバで非標準のポートを使用している場合、または別のポートを使用する新しいサーバに移行する場合（SSL を使用しているサーバから、SSL を使用していないサーバへの移行など）は、LDAP ポートを指定する必要があります。ポートを指定しない場合、以前の設定値が使用されます。以前のポート設定が指定されていない場合は、SSL を使用していないときのデフォルト ポート 389 か、SSL を使用しているときのデフォルト ポート 636 が使用されます。

-d*userdn*

新しい LDAP ディレクトリのスキーマとエントリを作成する権限のあるユーザの LDAP ユーザ名を指定します。必ずしも LDAP サーバ管理者のユーザ名であるとは限りません。ユーザ名を指定しないと、以前に設定した名前がデフォルトで使用されます。

-w*userpw*

-d 引数で指定されたユーザのパスワードを指定します。パスワードを指定しない場合、以前に設定した値が使用されます。

例: -wMyPassword123

-r*root*

SiteMinder がポリシー ストア スキーマを検索する LDAP ツリー内のノードの識別名を指定します。ルートを指定しない場合、以前に設定したルートが使用されます。

例: -ro=security.com

-e

smldapsetup ldgen と共に指定すると、SiteMinder スキーマを削除できる LDIF ファイルが生成されます。スキーマを削除するには、生成されたファイルを smldapsetup ldmod と共に使用する必要があります。

-m*n*

LDAP サーバの自動検出をスキップし、LDAP ポリシー ストアのタイプを指定します。*n* は以下のいずれかです。

2

iPlanet v4 LDAP サーバ

3

Active Directory (LDAP) サーバ

4

Oracle インターネット ディレクトリ

5

iPlanet v5

6

Sun Directory Server

9

Active Directory アプリケーション モード (ADAM)

-f*ldif*

smldapsetup の実行場所となるディレクトリから LDIF ファイルへの絶対パスまたは相対パスを指定します。

例: -f../siteminder/db/smldap.ldif

デフォルト: パスを指定しない場合、現在のディレクトリがデフォルトとして使用されます。

-t*tool*

ldapmodify コマンド ライン ユーティリティの絶対パスまたは相対パスを、ファイル名と拡張子を含めて指定します。ldapmodify は LDIF 形式のコマンドを使用しているサーバ スキーマを設定するために使用します。LDAP サーバおよび SiteMinder には、ldapmodify のコピーが用意されています。ユーティリティがデフォルトの場所にない場合は、この引数を使用して場所を指定します。

-ssl*1_or_0*

LDAP サーバに対して SSL 暗号化された接続を使用するときは -ssl1、非 SSL 接続を使用するときは -ssl0 を指定します。-ssl の値を指定しない場合、以前に設定した値が使用されます。LDAP 接続が以前に設定されていない場合、初期デフォルト値は 0 です。

-c*cert*

SSL 暗号化された（-ssl1） LDAP 接続を使用するときは、
この引数を指定する必要があります。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を指定します。このデータベース ファイルは Netscape Navigator Web ブラウザでは一般に cert7.db と呼ばれています。

例: cert7.db が /app/siteminder/ssl 内にある場合は、-c/app/siteminder/ssl を指定します（smldapsetup ldmod -f/app/siteminder/pstore.ldif -p81 -ssl1 -c/app/siteminder/ssl）。

注: Sun Java System LDAP に対して SSL 暗号化接続を使用しているポリシー ストアの場合は、cert7.db と同じディレクトリ内に key3.db ファイルがあることを確認してください。

-k-k1

別の LDAP ディレクトリにキー情報を格納する場合に、smldapsetup を使用してキー ストアをセットアップまたは変更できます。-k を指定すると、ポリシー サーバがキー ストアを参照しているかどうかが、任意の機能を実行する前に確認されます。ポリシー サーバがキー ストアを参照していない場合は、警告が出されます。ldgen および新しいポリシー ストア用の他の引数と共に -k1 を指定して smldapsetup を実行すると、指定した場所に別のキー ストアが作成されます。-k または -k1 を指定しないと、ポリシー ストアが変更されます。

-v

トラブルシューティングの詳細モードを有効にします。-v を指定して smldapsetup を実行すると、LDAP 移行の各手順で、コマンド ライン引数と設定エントリのログが記録されます。

-i*userDN*

ポリシー ストアに対する変更を行うために SiteMinder によって使用される必要のあるアカウントの識別名を指定します。この引数を使用すると、管理者アカウントで SiteMinder スキーマの制御を維持すると同時に、SiteMinder データの日常の変更のために使用される別のアカウントを有効にすることができます。管理 UI を使用して変更を行う場合は、この引数によって指定されるアカウントが使用されます。この引数を使用するときは、アカウントの全 DN を入力してください。

-q

何も質問が行われない Quiet モードを有効にします。

-u

6.x アップグレード スキーマ ファイル（LDIF）を作成します。

-x

ldmod に -x 引数を使用して、別の 5.x Sun Java System Directory Server Enterprise Edition（以前の Sun ONE/iPlanet）LDAP ディレクトリ サーバ用のレプリケーション インデックスを生成します。

-ssuffix

このオプションを使用すると、6.x ポリシー サーバのスキーマを Sun Java System Directory Server Enterprise Edition（以前の Sun ONE/iPlanet）LDAP ディレクトリに設定するときに、デフォルトの親サフィックス以外のサフィックスを指定することができます。

例: 以下のような状況を想定します。

ou=Apps,o=test.com はポリシー ストアのルートです。

o=test.com はルート サフィックスです。

ou=netegrity,ou=Apps,o=test.com はサブ サフィックスです。

smldapsetup で -s パラメータを使用しない場合、ポリシー サーバは ou=netegrity,ou=Apps,o=test.com の親サフィックスとして ou=Apps,o=test.com を割り当てます。これを変更し、適切な親サフィックスを設定するには、-s パラメータと o=test.com を指定して smldapsetup を実行します。

-?

ヘルプ メッセージを表示します。

注: 引数に空白が含まれる場合は、引数全体を二重引用符で囲む必要があります。たとえば、SiteMinder 管理者の名前が LDAP ユーザである場合、smldapsetup の引数は -d"LDAP user" となります。

smldapsetup と Sun Java System Directory Server Enterprise Edition

Sun Java System Directory Server Enterprise Edition（以前の Sun ONE/iPlanet）ディレクトリ サーバでは、smldapsetup によって ou=Netegrity, *root* サブ サフィックスおよび PolicySvr4 データベースが作成されます。

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 ルートです。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=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 サフィックスとサブ サフィックスの詳細については、Sun Microsystems の ドキュメントを参照してください。

smldapsetup による SiteMinder ポリシー ストアの削除

SiteMinder ポリシー ストア データとスキーマを LDAP ディレクトリから削除するには、最初にデータを削除し、次にスキーマを削除する必要があります。

重要:

- SiteMinder ポリシー ストア データを削除する前に、削除するデータを含むポリシー ストアをポリシー サーバが参照していることを確認してください。smldapsetup は、ポリシー サーバが参照しているポリシー ストアからデータを削除します。また、データを削除する前に、ポリシー ストア データを出力ファイルにエクスポートして、ファイルのバックアップを作成します。
- 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している場合、管理者としてシステムにログインしていても、必ず管理者権限でコマンド ライン ウィンドウを開くようにしてください。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。

smldapsetup を使用してポリシー ストアを削除する方法

1. 次のディレクトリに移動します。
   - （Windows）*siteminder_home*¥bin
   - （UNIX）*siteminder_home*/bin

   siteminder_home

   SiteMinder のインストール場所を指定します。
2. 以下コマンドを入力してポリシー ストア データを削除します。

   ```
   smldapsetup remove -hLDAP_IP_Address -pLDAP_Port
   -d LDAP_Admin -wLDAP_Admin_Password -rLDAP_Base_DN
   -v
   ```

   例: smldapsetup remove -h192.169.125.32 -p552 -d"cn=directory manager" -wfirewall -rdc=ad,dc=test,dc=com -v

   注: ポリシー ストア データの削除には多少の時間がかかる場合があります。
3. 以下のコマンドを入力して、スキーマの削除に使用する LDIF ファイルを生成します。

   ```
   smldapsetup ldgen -e -fldif
   ```

   ldif

   生成する LDIF ファイルの名前を指定します。

   例: smldapsetup ldgen -e -fdelete.ldif
4. 以下のコマンドを実行して、SiteMinder スキーマを削除します。

   ```
   smldapsetup ldmod -fldif
   ```

   ldif

   smldapsetup ldgen -e を使用して生成した LDIF ファイルの名前を指定します。

   例: smldapsetup ldmod -fdelete.ldif

ODBC データベース内の SiteMinder データの削除

SiteMinder には、ODBC データベースから SiteMinder スキーマを削除する SQL スクリプトが用意されています。以下のリストで各 SQL スクリプトについて説明します。

sm_oracle_ps_delete.sql

Oracle データベースから SiteMinder 6.x のポリシー ストアおよびデータを削除します。

sm_oracle_logs_delete.sql

Oracle データベースが sm_oracle_logs.sql を使用して作成されている場合に、データベースに格納されている SiteMinder 6.x のログを削除します。

sm_oracle_ss_delete.sql

Oracle データベースから SiteMinder 6.x セッション サーバのテーブルとデータを削除します。

sm_mssql_ps_delete.sql

SQL データベースから SiteMinder 6.x のポリシー ストアとデータを削除します。

sm_mssql_logs_delete.sql

SQL データベースが sm_mssql_logs.sql を使用して作成されている場合に、データベースに格納されている SiteMinder 6.x のログを削除します。

sm_mssql_ss_delete.sql

SQL データベースから SiteMinder 6.x セッション サーバのテーブルとデータを削除します。

sm_db2_ps_delete.sql

DB2 データベースから SiteMinder 6.x のポリシー ストアとデータを削除します。

sm_db2_logs_delete.sql

DB2 データベースが sm_db2_logs.sql を使用して作成されている場合に、データベースに格納されている SiteMinder 6.x のログを削除します。

sm_db2_ss_delete.sql

DB2 データベースから SiteMinder 6.x セッション サーバのテーブルとデータを削除します。

ODBC データベースの SQL スクリプトは以下の場所にあります。

- （Windows）*siteminder_home*¥db

  siteminder_home

  ポリシー サーバのインストール パスを指定します。

- （UNIX）*siteminder_home*/db

  siteminder_home

  ポリシー サーバのインストール パスを指定します。

データベース オブジェクトを削除するには、DB2、SQL Plus for Oracle、または SQL Server クエリ アナライザを使用して、適切な SQL スクリプトを実行します。

注: SQL スクリプトの実行については、お使いのデータベースのドキュメントを参照してください。

smpatchcheck

smpatchcheck ツールでは、お使いのシステムにインストールされたポリシー サーバおよび Web エージェントに必要な Solaris パッチが存在するかどうかを判断することができます。smpatchcheck は、SiteMinder プラットフォーム マトリックスに示されている Solaris バージョンで実行できます。このマトリックスにアクセスするには、テクニカル サポートに移動し、SiteMinder プラットフォーム サポート マトリックスを検索してください。

smpatchcheck を使用する方法

1. *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. 「smpatchcheck」と入力します。

   必須のパッチと推奨されるパッチが検索され、そのステータスが表示されます。

   例:

```
Testing for Required Patches:
  Testing for Patch: 106327-09 ... NOT Installed
Testing for Recommended Patches:
  Testing for Patch: 106541-08 ... Installed
 Testing for Patch: 106980-00 ... Installed
SiteMinder Patch Check: Failed
```

以下のいずれかのメッセージが返されます。

失敗

必須のパッチが 1 つ以上インストールされていません。

一部失敗

推奨されるパッチが 1 つ以上インストールされていません。

成功

必須のパッチと推奨されるパッチがすべてインストールされています。

SiteMinder テストツール

SiteMinder テスト ツールは、エージェントとポリシー サーバの間の対話をシミュレートするユーティリティです。このツールは、ポリシー サーバの機能をテストします。テスト ツールは、エージェントとしての役割を果たし、実際のエージェントと同じようにポリシー サーバに対して要求を送信します。これにより、SiteMinder の設定を実際に展開する前にテストできます。

注: このツールの詳細については、「ポリシー サーバ設定ガイド」を参照してください。

smreg

スーパーユーザ パスワードを変更する方法

1. ポリシー サーバが稼働中であり、設定済みのポリシー ストアを参照していることを確認します。
2. smreg ユーティリティが *policy_server_home¥bin* にあることを確認します。

   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。

   注: ユーティリティがない場合は、サポート サイトで提供されているポリシー サーバ インストール メディアから入手できます。
3. 以下のコマンドを実行します。

   `smreg -su password`

   password

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

   注: -su とパスワードの間に必ず空白を入れてください。

   スーパーユーザ アカウント パスワードが変更されます。
4. smreg ユーティリティを削除します。

   ユーティリティを削除することで、スーパーユーザ パスワードが他の人によって変更されることを防ぎます。

XPSCounter

SiteMinder ライセンスの条件に準拠するため、SiteMinder 環境内のユーザ数をカウントできます。以下の手順では、ディレクトリの設定方法と、ディレクトリ内に格納されている SiteMinder ユーザのカウント方法を説明します。

1. カウントするユーザ ディレクトリごとに以下の変更を加えます。

   注: 詳細については、「*SiteMinder ポリシー サーバ設定ガイド*」を参照してください。

   - 管理 UI でディレクトリ管理者のユーザ名とパスワードを入力して、管理者クレデンシャルの使用を強制します。
   - 管理 UI を使用して、ユニバーサル ID および他のユーザ属性のマッピングを定義します。

2. Microsoft Active Directory のユーザ ストアについては、管理 UI を使用して inetOrgPerson 属性をマップします。
3. SiteMinder ポリシーに関連付けられているユーザの数の確認

Active Directory の inetOrgPerson 属性のマッピング

SiteMinder ユーザ ストアのいずれかが Microsoft Active Directory サーバ上にある場合は、各 Active Directory サーバ内の inetOrgPerson をマップしてから、SiteMinder ユーザをカウントする必要があります。

inetOrgPerson 属性をマップする方法

1. 管理 UI を開きます。
2. [インフラストラクチャ]-[ディレクトリ]-[ユーザ ディレクトリ]-[ユーザ ディレクトリの変更]をクリックします。

   検索画面が表示されます。
3. 希望するディレクトリをクリックし、[選択]をクリックします。

   [ユーザ ディレクトリの変更: *Directory_Name*]ウィンドウが開きます。
4. [属性マッピング リスト]グループ ボックスで、[作成]をクリックします。

   [属性マッピングの作成]ダイアログ ボックスが表示されます。
5. [タイプ「属性マッピング」のオブジェクトの作成]をクリックし、[OK]をクリックします。

   [属性マッピングの作成]ダイアログ ボックスが表示されます。
6. [名前]フィールドをクリックし、以下を入力します。

   `inetOrgPerson`
7. (オプション)[説明]フィールドをクリックし、以下を入力することをお勧めします。

   `Active Directory ユーザをカウントするためのカスタム マッピング(XPSCounter による)`
8. [プロパティ]グループボックスで、以下の操作を実行します。
   a. [別名]ラジオ ボタンが選択されていることを確認します。
   b. [定義]フィールドをクリックし、以下を入力します。

      `User`
9. [OK]をクリックします。

   [ユーザ ディレクトリの変更]ウィンドウが表示されます。
10. [サブミット]をクリックします。

    変更が保存され、inetOrgPerson 属性がマップされます。

SiteMinder ポリシーに関連付けられているユーザの数の確認

SiteMinder ライセンスの条件に準拠するため、SiteMinder ポリシーに関連付ける組織内ユーザの数を確認することができます。

注: SiteMinder バイナリ ファイル（XPS.dll、libXPS.so、libXPS.sl）への書き込みアクセス許可がユーザに*ない* 場合は、管理者が 管理 UI または XPSSecurity ツールを使用して、関連する XPS コマンド ライン ツールを使用する権限を付与する必要があります。

ユーザの数を確認する方法

1. ポリシー サーバのコマンド ウィンドウを開いて、以下のコマンドを入力します。

   `XPSCounter`

   ツールが起動し、このセッションのログ ファイルの名前が表示されます。また、[ライセンスのパラメータ]メニューが開きます。

2. 「1」と入力します。

   [パラメータ]メニューが表示されます。

3. 「C」と入力します。

   [カウンタ]メニューが表示されます。

4. 「I」と入力します。

5. ユーザ ディレクトリ XID を検索するには、「?」と入力します。ポリシー ストアで定義されているユーザ ディレクトリのみがリストに表示されます。

6. カウント対象のユーザを含むディレクトリの数を入力します。

   注: このツールは、指定された各ディレクトリ内のユーザ *オブジェクト*の数をカウントします。これには、複数のディレクトリに示される同一のユーザ オブジェクトまたは 1 つのディレクトリ内にある同一ユーザの複数のユーザ オブジェクトは含まれません。このツールの実行結果を解釈するときは、このことを考慮する必要があります。

7. （オプション）結果を説明するコメントを入力します。

   ユーザがカウントされ、確認のメッセージが表示されます。

8. （オプション）別のディレクトリ内のユーザをカウントするには、手順 5 ～ 8 を繰り返します。

9. 「V」と入力します。

   カウントしたディレクトリ*ごとに*、以下の情報が表示されます。

   XID

   指定されたユーザ ディレクトリの一意の識別子を表示します。

   例:
   CA.SM::UserDirectory@0e-50ea30f0-b5c0-450c-a135-1e317dd25f11

   名前

   指定されたユーザ ディレクトリ(管理 UI で定義されている)の名前を表示します。

   : *count*

   指定されたユーザ ディレクトリの最新のユーザ数を表示します。カウンタに保存されている以前の値を削除する必要は*ありません*。この値はカウンタを実行するたびに自動的に更新されます。

   例: : 23

   総数

   カウントしたすべてのユーザ ディレクトリ内のユーザの合計数を表示します。たとえば、2 つの異なるディレクトリのユーザをカウントし、各ディレクトリに 23 人のユーザがいた場合、表示される合計数は 46 です。

XPSConfig

XPSConfig は、管理者および運用メンバが製品のパラメータを表示し、許可される場合はその設定を編集できるようにする、対話型のコマンド ライン ユーティリティです。XPSConfig は必須ツールではないので、XPS プログラミング インターフェースを使用した製品固有の設定ツールを独自に所有する一方で、オプションとして使用できます。

XPSConfig は、ベンダーごとおよびインストールされた製品ごとに、製品のデータ ディクショナリ内で定義されているパラメータまたは指定された設定を管理します。各製品では、独自のパラメータ設定の読み取り、書き込み、および検証が可能です。

XPSConfig を使用するには、XPSConfig の権限を持った管理者である必要があります。

パラメータには以下の属性があります。

Name

パラメータ名を指定します。

制限:

- 名前は、文字またはアンダースコアで始まり、文字、数字、およびアンダースコアのみで構成される必要があります。
- 32 文字まで指定できます。
- 名前では大文字と小文字が区別されません。

Type

パラメータ値の以下のデータ型を指定します。

```
Logical | Numeric | String
```

Logical

ブール値(TRUE または FALSE)を指定します。

Numeric

整数を指定します。

String

文字列を指定します。

Scope

パラメータの以下の値またはスコープを指定します。

```
Ask | Global | Local | Managed | Overrideable | Read Only
```

Ask

値が XPS ではなく製品によって管理され、読み取り専用であることを明示します。

Global

値がポリシー ストア内に保存され、そのポリシー ストアを共有するすべてのポリシー サーバによってアクセス可能であることを明示します。

Local

各ポリシー サーバが独自の値を保存することを明示します。

Managed

値が XPS ではなく製品によって管理され、読み取りと書き込みが可能であることを明示します。

Overrideable

値がポリシー サーバにローカルで保存され、共有ポリシー ストアにグローバルに保存されている値を上書きできることを明示します。

Read Only

値がデフォルト値であり、かつ読み取り専用であることを明示します。

Export

このパラメータをポリシー ストアのエクスポートに含めるかどうかを指定します。

型: ブール

Report

このパラメータをポリシー サーバの機能レポートに含めるかどうかを指定します。

型: ブール

RemoteAccess

リモート API がパラメータに対して持つアクセス許可のタイプを指定します。

`None | Read | ReadWrite`

Description

パラメータの目的を説明します。

LicenseType

ライセンス制限のタイプを指定します。

`None | SoftLimit | HardLimit | ExpDate`

None

パラメータがライセンス制限ではないことを明示します。

SoftLimit

パラメータが厳密でない忠告的なライセンス制限であることを明示します。

HardLimit

パラメータが厳密で絶対的なライセンス制限であることを明示します。

ExpDate

パラメータがライセンスが期限切れになる日付であることを明示します。

Default Value

現在の値が未定義の場合に使用するデフォルト値を指定します。

注: デフォルト値が未定義の場合、その値はデータ型に基づいて指定されます。

文字列

空白

数値

ゼロ

ブール値

FALSE

Visible

パラメータを XPSConfig で表示するかどうかを指定します。

型: ブール

構文

XPSConfig の形式は以下のとおりです。

```
XPSConfig [-vendor vendor] [-product product]
[-?] [-vT | -vI | -vW | -vE | -vF]
[-l log_path] [-e err_path] [-r rec_path]
```

パラメータ

XPSConfig には以下のオプションがあります。

-vendor

(オプション) データを表示するベンダーの名前を指定します。

-product

(オプション) データを表示する製品の名前を指定します。

-?

(オプション) このユーティリティのヘルプ情報を表示します。

-vT | -vI | -vW | -vE | -vF

(オプション) エラー情報のログをエラー ファイルに記録するタイミングと、記録する情報の量を指定します。

-vT

エラーをトレースできるように、詳細な情報をログに記録します。

-vI

エラーがあった場合は、情報をログに記録します。

-vW

警告、エラー、または致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vE

エラーまたは致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vF

致命的なエラーが発生した場合に、エラー情報をログに記録します。

-l

(オプション) 指定された場所にロギング情報を出力します。

デフォルト: stdout

-e

(オプション) 指定された場所にエラー情報を出力します。

デフォルト: stderr

-r

(オプション) 指定された場所にセッションのレコードを出力します。

XPSEvaluate

XPSEvaluate は、管理者およびアプリケーション開発者が式を評価し、パフォーマンスをテストできるようにする、対話型のコマンド ライン ユーティリティです。XPSEvaluate を使用するには、XPSEvaluate の権限を持った管理者である必要があります。

構文

XPSEvaluate の形式は以下のとおりです。

```
XPSEvaluate [-np] [-trace] [-dbg debuglist]
[-f DB | formulapath] [-c contextpath] [-u userpath] [-step]
[-?] [-vT | -vI | -vW | -vE | -vF]
[-l log_path] [-e err_path] [-r rec_path]
```

パラメータ

XPSEvaluate には以下のオプションがあります。

-np

(オプション)プロンプトを指定しません。

-trace

(オプション)トレースをオンにします。

-dbg

(オプション)デバッグ リストを指定します。

-f

(オプション)名前付き式の場所を指定します。

注: DB はポリシー ストアを指定します。

-c

(オプション)コンテキスト値の場所を指定します。

-u

(オプション)ユーザ属性の場所を指定します。

-step

(オプション)評価の手順を表示します。

-?

(オプション) このユーティリティのヘルプ情報を表示します。

-vT | -vI | -vW | -vE | -vF

(オプション) エラー情報のログをエラー ファイルに記録するタイミングと、記録する情報の量を指定します。

-vT

エラーをトレースできるように、詳細な情報をログに記録します。

-vI

エラーがあった場合は、情報をログに記録します。

-vW

警告、エラー、または致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vE

エラーまたは致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vF

致命的なエラーが発生した場合に、エラー情報をログに記録します。

-l

(オプション) 指定された場所にロギング情報を出力します。

デフォルト: stdout

-e

(オプション) 指定された場所にエラー情報を出力します。

デフォルト: stderr

-r

(オプション) 指定された場所にセッションのレコードを出力します。

XPSExplorer

XPSExplorer は、管理者またはアプリケーション開発者がポリシー ストアのデータを表示できるようにする、対話型のコマンド ライン ユーティリティです。XPSExplorer には以下の 2 つの用途があります。

- ドメインまたはレルムのリストを確認することによって、より詳細なレベルでのエクスポートまたはインポート用にオブジェクトの識別子を判別する
- オブジェクト ストアが破損し、手動で修復する必要がある場合に、そのストアを修復する。このアクションを実行する場合は、CA サポートの助言のもとでのみ実行する必要があります。

XPSExplorer を使用するには、XPSExplorer の権限を持った管理者である必要があります。

構文

XPSExplorer の形式は以下のとおりです。

```
XPSExplorer [-?] [-vT | -vI | -vW | -vE | -vF]
[-l log_path] [-e err_path] [-r rec_path]
```

パラメータ

XPSExplorer には以下のオプションがあります。

-?

(オプション)このユーティリティのヘルプ情報を表示します。

-vT | -vI | -vW | -vE | -vF

(オプション)エラー情報のログをエラー ファイルに記録するタイミングと、記録する情報の量を指定します。

-vT

エラーをトレースできるように、詳細な情報をログに記録します。

-vI

エラーがあった場合は、情報をログに記録します。

-vW

警告、エラー、または致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vE

エラーまたは致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vF

致命的なエラーが発生した場合に、エラー情報をログに記録します。

-l

(オプション) 指定された場所にロギング情報を出力します。

デフォルト: stdout

-e

(オプション) 指定された場所にエラー情報を出力します。

デフォルト: stderr

-r

(オプション) 指定された場所にセッションのレコードを出力します。

ポリシー ストア データのサブセットのエクスポート

ポリシー ストア データのサブセットをエクスポートするには、エクスポートするオブジェクトの識別子 (XID) が必要です。オブジェクト識別子の検索には XPSExplorer を使用できます。XPSExplorer を使用するには、XPSExplorer の権限を持った管理者である必要があります。

このユース ケースでは、以下のアカウンティング アプリケーションをエクスポートします。

- Accounts Payable (買掛管理)
- Accounts Receivable (売掛管理)
- General Ledger (総勘定元帳)
- Payroll (給与計算)

ポリシー ストア データのサブセットのエクスポート

1. ポリシー サーバをホストしているマシンでコマンド プロンプトを開きます。
2. 以下のコマンドを入力します。

   ```
   XPSExplorer
   ```

   [メイン]メニューが開き、ベンダー、製品、およびクラスがリスト表示されます。

   注: トップレベルのクラスにあるオブジェクトのみエクスポートできます。トップレベルのクラスはアスタリスクで示されます。
3. エクスポートするオブジェクトのクラスに対応する番号を入力します。

   [クラス]メニューが開きます。

   例: Accounting に対応する番号が 15 番の場合は、「15」を入力します。
4. 「S」と入力してクラス内のオブジェクトを表示します。

   [検索]メニューが開き、クラス内のオブジェクトがリスト表示されます。

   検索結果の例:

   1-CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8

   (I) Name : "Accounts Payable"

   (C) Desc : "accounts payable"

   2-CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244

   (I) Name : "Accounts Receivable"

   (C) Desc : "accounts receivable"

   3-CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92

   (I) Name : "General Ledger"

   (C) Desc : "general ledger"

   4-CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b

   (I) Name : "Payroll"

   (C) Desc : "payroll"

   5-CA.SM::Accounting@@12-88f119a0-3fd1-46d0-b8ac-c1e83f00f97d

   (I) Name : "Job Costing"

   (C) Desc : "job costing"

オブジェクト識別子（XID）の例：

CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8

CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244

CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92

CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b

CA.SM::Accounting@@12-88f119a0-3fd1-46d0-b8ac-c1e83f00f97d

5. 3 回「Q」と入力して、[検索]、[クラス]、および[メイン]の各メニューを終了し、コマンド プロンプトに戻ります。

6. コマンド プロンプトで、以下のコマンドを入力します。

```
XPSExport output_file -xo object_XID_1 -xo object_XID_2
-xo object_XID_3 -xo object_XID_4
```

output_file

ポリシー ストア データのエクスポート先となる XML ファイルを指定します。

-xo *object_XID*

エクスポートする各オブジェクトの識別子を指定します。

注: 検索結果からオブジェクト識別子（XID）をコピーし、それをコマンド ラインに貼り付けることができます。

例：

```
XPSExport accounting.xml
-xo CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8
-xo CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244
-xo CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92
-xo CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b
```

指定されたアカウンティング アプリケーションのポリシー ストア データが accounting.xml にエクスポートされます。

XCart 管理

XPSExplorer には XCart 機能が含まれます。XCart を使用すると、エクスポートするオブジェクトの識別子（XID）を収集し、後で使用できるようにファイルに保存できます。各 ID を手動でコピーおよび貼り付けする必要はありません。
XPSExplorer を使用するには、XPSExplorer の権限を持った管理者である必要があります。

XCart にアクセスするには、XPSExplorer のメイン メニューで XCart Management の「X」を入力します。XCart メニューが開き、XCart 内にあるオブジェクトがすべて表示されます。以下のオプションはコンテキスト依存のため、コンテキストに応じて表示されたり表示されなかったりします。

C - カートのクリア

XCart を空にします。

L - ファイルからカートをロード

- 初期ロード - 指定されたファイルの内容を XCart にロードし、指定されたファイル名を XCart ファイルとして記憶します。
- 後続のロード - 指定されたファイルの内容を XCart に追加します。

  注: XCart ファイルの名前は変わりません。

S - ファイルへのカートの保存: xcart_file

XCart の内容を XCart ファイルに保存します。

重要: S コマンドは、プロンプトを最初に表示せずに、XCart ファイルの内容を上書きします。

N - 新規ファイルへのカートの保存

XCart の内容を指定されたファイルに保存し、指定されたファイル名を XCart ファイルとして記憶します。

注: N コマンドは、指定されたファイルを上書きする前にプロンプトを表示します。

各オブジェクトには、XPS ファイルからポリシー ストアへのインポート方法を指定するインポート モードのタグが付けられます。

A - **インポート モードの設定**: ADD

新規オブジェクトを追加します。既存のオブジェクトは置換しません。

O - **インポート モードの設定**: OVERLAY

既存のオブジェクトを置換します。新規オブジェクトは追加しません。

R - **インポート モードの設定**: REPLACE

既存のオブジェクトを置換し、新規オブジェクトを追加します。

D - **インポート モードの設定**: **デフォルト値**

デフォルトのインポート モードを指定します。

注: 製品クラスごとに、製品のデータ ディクショナリで定義されたデフォルトのインポート モードがあります。

Q - **終了**

［XCart］メニューを終了し、［メイン］メニューに戻ります。

XCart によるポリシー ストア データのサブセットのエクスポート

ポリシー ストア データのサブセットをエクスポートするには、エクスポートするオブジェクトの識別子（XID）が必要です。 XPSExplorer の XCart 機能を使用すると、オブジェクトを検索し、エクスポートするときは後で使用できるように XCart ファイルに保存できます。たとえば、管理者は、運用のメンバが使用する XCart ファイルを必要に応じて設定できます。XPSExplorer を使用するには、XPSExplorer の権限を持った管理者である必要があります。

このユース ケースでは、以下の 4 つのアカウンティング アプリケーションを後で使用できるようにファイルに保存します。

- Accounts Payable（買掛管理）
- Accounts Receivable（売掛管理）
- General Ledger（総勘定元帳）
- Payroll（給与計算）

XCart によるポリシー ストア データのサブセットのエクスポート

1. ポリシー サーバをホストしているマシンでコマンド プロンプトを開きます。
2. 以下のコマンドを入力します。

   ```
   XPSExplorer
   ```

   メイン メニューが開き、ベンダー、製品、およびクラスがリスト表示されます。

   注: トップレベルのクラスにあるオブジェクトのみエクスポートできます。トップレベルのクラスはアスタリスクで示されます。

3. XCart Management の「X」を入力します。

   XCart メニューが開きます。

4. テキスト ファイルを作成します。

   例: C:¥xcart¥accounting.txt

   注: これは XCart の内容を保存する場所です。

5. ファイルからカートをロード(Load cart from file)オプションの「L」を入力します。
6. 作成したテキスト ファイルのパスと名前を入力します。

   指定したファイル名は XCart ファイルとして記憶されます。

   例: C:¥xcart¥accounting.txt

   注: ファイルは存在している必要があります。ファイルが存在していない場合、「L」は効果がありません。

7. 「Q」と入力してメイン メニューに戻ります。
8. エクスポートするオブジェクトのクラスに対応する番号を入力します。

   [クラス]メニューが開きます。

   例: Accounting に対応する番号が 15 番の場合は、「15」を入力します。

9. 「S」と入力してクラス内のオブジェクトを表示します。

   [検索]メニューが開き、クラス内のオブジェクトがリスト表示されます。

   検索結果の例:

   ```
   1-CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8
       (I) Name                : "Accounts Payable"
       (C) Desc                : "accounts payable"
   ```

2-CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244

(I) Name : "Accounts Receivable"

(C) Desc : "accounts receivable"

3-CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92

(I) Name : "General Ledger"

(C) Desc : "general ledger"

4-CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b

(I) Name : "Payroll"

(C) Desc : "payroll"

5-CA.SM::Accounting@@12-88f119a0-3fd1-46d0-b8ac-c1e83f00f97d

(I) Name : "Job Costing"

(C) Desc : "job costing"

10. アカウンティング アプリケーション 1 ～ 4 について、以下の手順に従います。
    a. アプリケーションに対応する番号を入力します。
    b. XCart への追加（Add to XCart）オプションの「X」を入力します。
    c. 「Q」と入力して［XCart］メニューを終了し、［検索］メニューに戻ります。

    注: アプリケーション名の先頭にアスタリスクが付いている場合は、そのアプリケーションが XCart 内にあることを意味します。
11. 2 回「Q」と入力して［検索］メニューと［クラス］メニューを終了し、［メイン］メニューに戻ります。
12. XCart Management の「X」を入力します。
13. 「S」と入力してカートを XCart ファイル（C:¥xcart¥accounting.txt）に保存します。
14. 2 回「Q」と入力して XCart メニューとメイン メニューを終了し、コマンド プロンプトに戻ります。
15. コマンド プロンプトで、以下のコマンドを入力します。

    `XPSExport output_file -xf xcart_file`

    output_file

    ポリシー ストア データのエクスポート先となる XML ファイルを指定します。

-xf *xcart_file*

エクスポートするオブジェクトの識別子（XID）を含む XCart ファイルのパスと名前を指定します。

例:

```
XPSExport accounting.xml C:¥xcart¥accounting.txt
```

XCart ファイルに保存されたアカウンティング アプリケーションのポリシー ストア データが accounting.xml にエクスポートされます。

XCart ファイルへのアプリケーションの追加

このユース ケースでは、XPSExplorer の XCart 機能を使用して、XCart ファイル（accounting.txt）内にすでに存在する以下の 4 つのアカウンティング アプリケーションに、5 つ目の監査アプリケーション（Job Costing）を追加します。

- Accounts Payable
- Accounts Receivable
- General Ledger
- Payroll

注: XPSExplorer を使用するには、XPSExplorer の権限を持った管理者である必要があります。

XCart ファイルへのアプリケーションの追加

1. ポリシー サーバをホストしているマシンでコマンド プロンプトを開きます。
2. 以下のコマンドを入力します。

   ```
   XPSExplorer
   ```

   メイン メニューが開き、ベンダー、製品、およびクラスがリスト表示されます。

   注: トップレベルのクラスにあるオブジェクトのみエクスポートできます。トップレベルのクラスはアスタリスクで示されます。

3. XCart Management の「X」を入力します。

   XCart メニューが開きます。

4. ファイルからカートをロード（Load cart from file）オプションの「L」を入力します。

5. 4 つのアカウンティング アプリケーションを含む既存のテキスト ファイルのパスと名前を入力します。

   指定したファイル名は XCart ファイルとして記憶されます。

   例: C:¥xcart¥accounting.txt

6. 「Q」と入力してメイン メニューに戻ります。

7. XCart ファイルに追加するクラスに対応する番号を入力します。

   [クラス]メニューが開きます。

   例: Accounting に対応する番号が 15 番の場合は、「15」を入力します。

8. 「S」と入力してクラス内のオブジェクトを表示します。

   [検索]メニューが開き、クラス内のオブジェクトがリスト表示されます。

   検索結果の例:

   1-CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8

   (I) Name : "Accounts Payable"

   (C) Desc : "accounts payable"

   2-CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244

   (I) Name : "Accounts Receivable"

   (C) Desc : "accounts receivable"

   3-CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92

   (I) Name : "General Ledger"

   (C) Desc : "general ledger"

   4-CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b

   (I) Name : "Payroll"

   (C) Desc : "payroll"

   5-CA.SM::Accounting@@12-88f119a0-3fd1-46d0-b8ac-c1e83f00f97d

   (I) Name : "Job Costing"

   (C) Desc : "job costing"

   注: アプリケーション名の先頭にアスタリスクが付いている場合は、そのアプリケーションが XCart 内にあることを意味します。

9. XCart ファイルに Job Costing を追加する方法
   a. Job Costing アプリケーションの「5」を入力します。
   b. XCart への追加（Add to XCart）オプションの「X」を入力します。
   c. 「Q」と入力して XCart メニューを終了し、[検索]メニューに戻ります。

      アプリケーション名の先頭にアスタリスクが付いている場合は、そのアプリケーションが XCart 内にあることを意味します。
   d. 2 回「Q」と入力して[検索]メニューと[クラス]メニューを終了し、メイン メニューに戻ります。
   e. XCart Management の「X」を入力します。
   f. 「S」と入力して XCart を XCart ファイル（C:¥xcart¥accounting.txt）に保存します。

      Job Costing が accounting.txt に保存されます。
10. 2 回「Q」と入力して XCart メニューとメイン メニューを終了し、コマンド プロンプトに戻ります。

XPSSecurity

XPSSecurity は、管理者および運用メンバが管理者を作成または削除し、その権限を編集できるようにする、対話型のコマンド ライン ユーティリティです。XPSSecurity を使用するには、XPSSecurity の権限を持った管理者である必要があります。

構文

XPSSecurity の形式は以下のとおりです。

```
XPSSecurity [-?] [-vT | -vI | -vW | -vE | -vF]
[-l log_path] [-e err_path] [-r rec_path]
```

パラメータ

XPSSecurity には以下のオプションがあります。

-?

（オプション）このユーティリティのヘルプ情報を表示します。

-vT | -vI | -vW | -vE | -vF

(オプション) エラー情報のログをエラー ファイルに記録するタイミングと、記録する情報の量を指定します。

-vT

エラーをトレースできるように、詳細な情報をログに記録します。

-vI

エラーがあった場合は、情報をログに記録します。

-vW

警告、エラー、または致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vE

エラーまたは致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vF

致命的なエラーが発生した場合に、エラー情報をログに記録します。

-l

(オプション) 指定された場所にロギング情報を出力します。

デフォルト: stdout

-e

(オプション) 指定された場所にエラー情報を出力します。

デフォルト: stderr

-r

(オプション) 指定された場所にセッションのレコードを出力します。

管理者をスーパーユーザにする

スーパーユーザは、外部管理者ストアへの接続を設定するときに定義されます。スーパーユーザを使用して、その他のすべての管理者アカウントを作成し、管理します。スーパーユーザがいない場合は、XPSSecurity を使用して外部ストア内の任意のユーザをスーパーユーザにすることができます。

管理者をスーパーユーザにする方法

1. XPSSecurity 権限のある SiteMinder 管理者アカウントを使用して、ポリシー サーバ ホスト システムにログインします。

   注: XPSSecurity 権限のある管理者がいない場合は、以下のいずれかでログインできます。

   - （Windows）システム管理者
   - （UNIX） root
   - ポリシー サーバをインストールしたユーザ

2. XPSSecurity ユーティリティが *policy_server_home*/bin にあることを確認します。

   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。

   注: ユーティリティがない場合は、サポート サイトで提供されているポリシー サーバ インストール メディアから入手できます。

3. コマンド ウィンドウを開き、以下のコマンドを実行します。

   ```
   XPSSecurity
   ```

   [メイン]メニューが表示されます。

4. 「A」と入力し、Enter キーを押します。

   [管理者]メニューに、外部ストアの SiteMinder 管理者がリスト表示されます。各管理者名の先頭には番号が付いています。

5. 管理者の番号を入力し、Enter キーを押します。

   [管理者]メニューに、選択した管理者に固有の属性が表示されます。各属性の先頭には番号が付いています。

6. 「2」と入力し、Enter キーを押します。

   [管理者]メニューがフラグ設定によって更新されます。

7. 疑問符(?)を入力し、Enter キーを押します。

   Disabled および Super User フラグが表示されます。各フラグの先頭には番号が付いています。

8. 「2」と入力し、Enter キーを押します。

   Super User フラグが選択されます。

9. 「Q」と入力し、Enter キーを押します。

   [管理者]メニューに、管理者固有の属性が表示されます。Flags 属性が Super User に設定されます。

10. 「U」と入力し、Enter キーを押します。

    管理者レコードが更新されます。

11. 「Q」と入力し、Enter キーを押します。

    [管理者]メニューに、外部ストアの SiteMinder 管理者がリスト表示されます。選択した管理者がスーパーユーザとして表示されます。

12. 次の 2 つのプロンプトで「Q」と入力し、Enter キーを押して、ユーティリティを終了します。

    選択した管理者はスーパーユーザです。この管理者を使用して、変更された権限または削除された権限を復元します。

-XPSSweeper

XPSSweeper は、バッチ ジョブとしても実行できるコマンド ライン ユーティリティです。 XPSSweeper を使用して、XPS と SiteMinder ポリシー ストアを同期できます。通常、XPS は異なるポリシー ストアの同期を行います。ただし、レガシー ツールを使用するときは、XPSSweeper を使用してポリシー ストアを再同期しなければならない場合があります。いずれにせよ、XPSSweeper によってポリシー ストアが破損することはないので、安全策として実行できます。

構文

XPSSweeper の形式は以下のとおりです。

```
XPSSweeper [-f] [-s seconds] [-m entries]
[-?] [-vT | -vI | -vW | -vE | -vF]
[-l log_path] [-e err_path]
```

パラメータ

XPSSweeper には以下のオプションがあります。

-f

（オプション） XPSSweeper をループ内で永久に実行します。

注: Ctrl + C キーを押すと終了します。

-s

（オプション）XPSSweeper が反復する間、指定された秒数だけスリープ状態になります。

-m

（オプション）指定された数のエントリがログに記録されるごとに、マイルストーン メッセージを出力します。

-?

（オプション）このユーティリティのヘルプ情報を表示します。

-vT | -vI | -vW | -vE | -vF

（オプション）エラー情報のログをエラー ファイルに記録するタイミングと、記録する情報の量を指定します。

-vT

エラーをトレースできるように、詳細な情報をログに記録します。

-vI

エラーがあった場合に、情報をログに記録します。

-vW

警告、エラー、または致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vE

エラーまたは致命的なエラーが発生した場合に、エラー情報をログに記録します。

-vF

致命的なエラーが発生した場合に、エラー情報をログに記録します。

-l

(オプション) 指定された場所にロギング情報を出力します。

デフォルト: stdout

-e

(オプション) 指定された場所にエラー情報を出力します。

デフォルト: stderr

バッチ ジョブとしての XPSSweeper の実行

XPSConfig を使用して以下の 2 つの XPS 設定パラメータを設定することにより、XPSSweeper をバッチ ジョブとして実行できます。

CA.XPS::$Autosweep

XPSweeper を Autosweep スケジュールに基づいて実行するか、あるいは XPSSweeper をまったく実行しないかを明示します。

型: ブール

CA.XPS::$AutosweepSchedule

Autosweep スケジュール (GMT 時間) を以下の形式で指定します。

```
DDD@{HH:MM}[,DDD@{HH:MM}] ... [,DDD@{HH:MM}]
```

DDD

(オプション) 曜日を指定します。

```
Sun | Mon | Tue | Wed | Thu | Fri | Sat
```

HH

時間を指定します。

範囲: 00 ～ 23

MM

分を指定します。

範囲: 00 ～ 59

例:

Sun@08:30

毎週日曜日の午前 8:30（GMT）

Tue@14:00

毎週火曜日の午後 2:00（GMT）

15:15

毎日の午後 3:15（GMT）

Sun@08:30,Tue@14:00,15:15

毎週日曜日の午前 8:30、毎週火曜日の午後 2:00、および火曜日を除く毎日の午後 3:15

注: 複数の Autosweep 時間を指定する場合は、カンマ、空白、またはセミコロンで区切ります。

ポリシー サーバは XPSSweeper の Autosweep 時間を以下のように管理します。

- キャッシュ チェックが数分おきに行われるため、XPSSweeper はスケジュールから数分ずれて実行される場合があります。
- XPSSweeper の実行がスケジュールされている時刻にすでに実行している場合は、停止または再起動されることなく、スイープ プロセスを完了できます。
- XPSSweeper はたとえスケジュールされたとしても、2 時間未満の間隔で実行されることはありません。

  例: XPSSweeper が毎週火曜日の午後 2:00 および毎日の午後 3:15 に実行されるようにスケジュールされた場合、後者のスイープは火曜日には実行されません。

XPSConfig による Autosweep の設定

このユース ケースでは、XPSSweeper を毎晩午後 10:00（GMT）に実行するように設定します。そのためには、XPSConfig を使用して、以下の 2 つの XPS 設定パラメータを設定します。

- CA.XPS::$Autosweep
- CA.XPS::$AutosweepSchedule

XPSConfig を使用して Autosweep を設定する方法

1. ポリシー サーバをホストしているマシンでコマンド プロンプトを開きます。
2. 以下のコマンドを入力します。

   ```
   XPSConfig
   ```

   [製品]メニューが開き、製品がリスト表示されます。
3. 拡張可能ポリシー ストアの場合は、「XPS」を入力します。

   [パラメータ]メニューが開き、XPS パラメータがリスト表示されます。
4. 自動スイープの場合は「7」を入力します。

   [移動スイープのパラメータ]メニューが開きます。
5. Autosweep 値が TRUE に設定されていることを確認するか、「C」と入力して値を TRUE に変更します。

   注: この手順によって、XPSSweeper を Autosweep スケジュールに従って実行することを明示します。
6. 「Q」と入力して[Autosweep Parameter]メニューを終了し、[パラメータ]メニューに戻ります。
7. [AutosweepSchedule]の「8」を入力します。

   [AutosweepSchedule パラメータ]メニューが開きます。
8. 「C」と入力して AutosweepSchedule パラメータの値を変更します。
9. [新しい値]に「22:00」と入力します。

   注: この手順によって、XPSSweeper を毎晩午後 10:00 (GMT)に実行することを明示します。
10. 3 回「Q」と入力して[AutosweepSchedule Parameter]、[パラメータ]、および[Products]の各メニューを終了し、コマンド プロンプトに戻ります。

第 18 章: ポリシー サーバ設定ファイル

このセクションには、以下のトピックが含まれています。

CA Compliance Security Manager 設定ファイル

SiteMinder には、コマンドライン ツール smcompliance が用意されています。このツールによって作成されるコンプライアンス レポートは CA Security Compliance Manager に手動でインポートできます。CA Compliance Security Manager 設定ファイル(compliance.conf)を使用すると、コンプライアンス レポートの内容を変更することができます。

場所: *siteminder_home*¥compliance¥config

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:

新しいコンプライアンス レポートの追加 (P. 249)
既存のコンプライアンス レポートの内容の変更 (P. 250)

Connection API 設定ファイル

Connection API ファイル（conapi.conf）は、Connection API によってサービスを設定するために使用されます。これらのサービスには OneView モニタが含まれます。

場所: *siteminder_home*¥config

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:

ポート番号の設定 (P. 140)

OneView モニタ設定ファイル

SiteMinder OneView モニタには以下の機能があります。

- SiteMinder 環境においてパフォーマンスのボトルネックを特定し、リソースの使用状況に関する情報を提供します。
- 特定のイベント（コンポーネント障害など）が発生した場合に、アラートを表示します。

OneView モニタ設定ファイル（mon.conf）を使用して以下を指定できます。

- OneView モニタが、登録済みのコンポーネントに対してデータを要求する頻度。
- 登録済みのコンポーネントが、OneView モニタにハートビート イベントを送信する頻度。
- ポリシー サーバ コンポーネントのインデックスが定数かどうか。

場所: *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。

詳細情報:

データのリフレッシュ間隔とハートビートの設定 (P. 139)

SiteMinder 設定ファイル

SiteMinder 設定ファイル（siteminder.conf）は以下の目的で使用されます。

- ポリシー サーバ プロセスの開始および停止
- 実行ファイルの設定、無効化、有効化

1 つ以上の実行のアプリケーションは、ポリシー サーバ プロセスのステータスを監視し、失敗した場合にプロセスを自動的に再起動します。

場所: *siteminder_home*¥config

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:

Windows エグゼクティブの設定 (P. 27)
UNIX エグゼクティブの設定 (P. 27)

SNMP の設定ファイル

SNMP 準拠のネットワーク管理アプリケーションでは、SiteMinder 環境の多くの運用上の要素を監視できます。SiteMinder SNMP モジュールは、これらのアプリケーションとの情報の交換を可能にします。

SNMP 設定ファイル（snmp.conf）は、SiteMinder SNMP モジュールの設定を提供します。

場所: *siteminder_home*¥config

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: このファイルの使用の詳細については、「ポリシー サーバ インストール ガイド」の「Windows 上での SNMP エージェントの設定」を参照してください。

SNMP イベントトラップ設定ファイル

SNMP イベントトラップ設定ファイル（snmptrap.conf）は、以下の設定を提供します。

- SNMP トラップにマップするシステム イベント。
- トラップの送信先のネットワーク管理システムのアドレス。

場所: *siteminder_home*¥config

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: このファイルに関連するタスクについては、「ポリシー サーバ インストール ガイド」の「Windows で SNMP イベントトラップを設定する方法」および「UNIX システムで SNMP イベントトラップを設定する方法」を参照してください。

詳細情報:

SiteMinder イベント マネージャの設定 (P. 160)
SiteMinder MIB (P. 150)
イベントのデータ (P. 159)

ポリシー サーバ レジストリ キー

ポリシー サーバ レジストリ キーは以下のいずれかにあります。

- （Windows）
  HKEY_LOCAL_MACHINE¥Software¥Netegrity¥SiteMinder¥CurrentVersion¥PolicyServer
- （UNIX）sm.registry ファイル

  このファイルのデフォルトの場所は *siteminder_home*/registry です。

  siteminder_home

  ポリシー サーバのインストール パスを指定します。

以下の点について考慮してください。

- 状況によっては、以下のいずれかを実行する必要があります。
  - 既存のレジストリ キーを変更する。
  - レジストリ キーを作成し、値を割り当てる。

  これらの場合、必要な手順は SiteMinder ドキュメントに説明されています。
- それ以外の場合は、SiteMinder ドキュメントの説明に従って、管理 UI またはポリシー サーバ管理コンソールを使用してポリシー サーバ設定を変更することをお勧めします。SiteMinder サポートまたはドキュメントによって指示されない限り、レジストリ キーを使用してポリシー サーバ設定を変更することはしないでください。

付録 A: SiteMinder と CA Security Compliance Manager

このセクションには、以下のトピックが含まれています。

SiteMinder と CA Security Compliance Manager の統合のしくみ

CA SiteMinder には、CA Security Compliance Manager に手動でインポートできるコンプライアンス レポートを作成するコマンド ライン ツール（smcompliance）が用意されています。smcompliance ツールはデフォルトで、以下のタイプのレポートを生成します。

ポリシー

コマンドの実行元となる SiteMinder ポリシー サーバに格納されているポリシーをすべてリスト表示します。

ユーザディレクトリ

ポリシー サーバに関連付けられているポリシー ストア内のユーザ ディレクトリをすべてリスト表示します。

ユーザ リソース

ユーザ、対応するユーザ ディレクトリ、および関連付けられているポリシーをリスト表示します。

SiteMinder コンプライアンス データを CA Security Compliance Manager にエクスポートするには、以下の手順に従います。

1. （オプション）以下のいずれかの操作を実行する場合は、コンプライアンス ツールの設定ファイルを更新します。
   - 既存レポートのレポート名またはフィールド名を変更する。
   - 新規レポートを追加する。
   - レポートを削除する。

2. ポリシー サーバ上でコンプライアンス ツールを実行してレポートを生成します。
3. 生成したレポートを組織の CA Security Compliance Manager 管理者に送信します。

コンプライアンス レポートの生成

CA Security Compliance Manager 用の SiteMinder コンプライアンス レポートは、コマンド ライン ツールを使用して生成します。レポートを生成したら、CA Security Compliance Manager にインポートするため、組織の CA Security Compliance Manager 管理者に送信する必要があります。

コンプライアンス レポートを生成する方法

1. ポリシー サーバをホストしているマシンでコマンド ライン ウィンドウを開きます。
2. 以下の任意のオプションを指定して smcompliance コマンドを実行します。

   -dir *directory_name*

   生成されたレポートを保存する出力ディレクトリの完全パスを指定します。このディレクトリがすでに存在する場合、既存のディレクトリはバックアップとして名前が変更されます。

   デフォルト: *siteminder_home*/compliance/output

   -conf *configuration_file*

   レポートの内容と形式を定義する設定ファイルの完全パスを指定します。デフォルトの設定ファイルには CA Security Compliance Manager の内容が含まれますが、自分のニーズに合わせてカスタマイズできます。

   デフォルト: *siteminder_home*/compliance/config

   -log *log_file*

   ログ ファイルの完全パスを指定します。

   デフォルト: *siteminder_home*/compliance/output

   -format *format_type*

   レポートに使用するファイルのタイプとして、以下のいずれか 1 つを指定します。

   - CSV (カンマ区切り値)ファイル
   - XML ファイル

   デフォルト: csv

   レポートとログ ファイルが生成されます。このファイルはすぐに CA Security Compliance Manager 管理者に送信できます。

使用可能なコンプライアンス レポートまたはそのフィールドのリストの表示

SiteMinder コンプライアンス レポート ツール（smcompliance）は、デフォルトで作成されるレポートに加えて、他のタイプのレポートも生成できます。

使用可能なコンプライアンス レポートのリストを表示する方法

1. ポリシー サーバでコマンド プロンプトを開きます。
2. 以下のコマンドを入力します。

   ```
   smcompliance -help reports
   ```

   レポート名のリストが表示されます。
3. （オプション）レポートに含まれるフィールドを確認するには、以下のコマンドを入力します。

   ```
   smcompliance -generate report_name
   ```

   report_name は、手順 2 のリストの名前に一致している必要があります。たとえば、エージェント レポートに含まれるフィールドを確認するには、以下のように入力します。

   smcompliance -generate agents

   レポートに含まれるフィールドのリストは XML 形式で表示されます。XML を設定ファイルに追加すれば、新しいレポートを生成できます。

新しいコンプライアンス レポートの追加

smcompliance ツールによって使用される設定ファイルに新規レポートを追加することによって、他のタイプのコンプライアンス レポートを生成できます。

新しいコンプライアンス レポートを追加する方法

1. 使用可能なコンプライアンス レポートのリストを smcompliance ツールで表示して、追加するレポートの名前を検証します。
2. 追加するレポートのフィールドを表示し、画面から XML 形式のテキストをコピーします。
3. ポリシー サーバの以下のディレクトリに移動します。

   siteminder_home¥compliance¥config
4. デフォルトの設定ファイル（compliance.conf）をテキスト エディタで開きます。
5. デフォルト ファイルのコピーを別の名前で保存します。
6. 既存の <report> セクションをコピーし、設定ファイルの下部にある </reports> タグの上に貼り付けます。
7. <columns> タグ間にある既存のテキストを削除します。
8. 手順 2 のテキストを <columns> タグ間に追加します。
9. <report> タグ内の name 属性の値を、手順 1 のレポートの名前に置き換えます。
10. <table> タグ内の name 属性の値を、新しいレポートの説明となるように変更します。生成されるレポート ファイルでは、この名前が使用されます。
11. 変更を保存し、新しい設定ファイルを閉じます。

    新しいレポートが追加されます。
12. smcompliance コマンドを実行し、新しい設定ファイルを指定します。

既存のコンプライアンス レポートの内容の変更

デフォルトの設定ファイルによって生成されたレポートは、CA Security Compliance Manager が必要とする一般的なコンプライアンス情報を提供します。組織内でニーズが異なる場合は、独自のカスタム設定ファイルを作成して、希望する情報を含むレポートを生成できます。

1. ポリシー サーバの以下のディレクトリに移動します。

   siteminder_home¥compliance¥config

2. デフォルトの設定ファイル（compliance.conf）をテキスト エディタで開きます。
3. デフォルト ファイルのコピーを別の名前で保存します。
4. 新しい設定ファイルのコピーに以下の任意の変更を加えます。
   - レポートを削除するには、削除するレポートが <report> タグと </report> タグの間にあることを確認し、そのセクションとタグを削除します。
   - レポートの名前を変更するには、<table> タグ内の name 属性の値を変更します。
   - レポート内のフィールドの名前を変更するには（フィールド内の情報 で *はなく*）、<column> タグ内の name 属性の値を変更します。
   - 追加する任意の列を、設定ファイルの <comment> セクションから <columns> セクションへ移動します。

付録 B: SiteMinder の一般的な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。

コマンド ラインからのポリシー サーバのトラブルシューティング

ポリシー サーバのトラブルシューティングを行う場合、デバッグ オプションをオンにすると、ポリシー サーバのプロセスを個別のウィンドウで対話式に実行できます。次のサーバ実行可能ファイルは、コマンドラインから実行できます。

install_dir/siteminder/bin/smpolicysrv

注: Windows システムでは、リモート デスクトップまたは[ターミナル サービス]ウィンドウから smpolicysrv コマンドを実行*しないでください*。smpolicysrv コマンドはプロセス間通信に依存します。この通信は、リモート デスクトップまたは[ターミナル サービス]ウィンドウから smpolicysrv プロセスを実行した場合には機能しません。

smpolicysrv コマンドでは以下のオプションを使用します。

-t*port_number*

このオプションは、サーバがエージェント接続用にバインドする TCP ポートを変更する場合に使用します。このスイッチが使用されなかった場合、サーバはポリシー サーバ管理コンソールで指定された TCP ポートをデフォルトで使用します。

-u*port_number*

このオプションは、サーバが RADIUS 接続用にバインドする UDP ポートを変更する場合に使用します。このスイッチが使用されなかった場合、サーバはポリシー サーバ管理コンソールで指定された UDP ポートをデフォルトで使用します。このスイッチは認証サーバとアカウンティング サーバにのみ適用できます。

-stop

このスイッチにより、サーバは可能な限り正式な手順を踏んでから停止します。この方法を使用すると、すべてのデータベース接続とネットワーク接続が適切に閉じられます。

-abort

このスイッチにより、サーバはデータベース接続とネットワーク接続を先に閉じるという手順を踏むことなく、ただちに停止します。

-stats

このスイッチは、現在のサーバの実行時の統計情報（スレッド プールの限度、スレッド プール メッセージ、接続数など）を生成します。

-resetstats

このスイッチは、ポリシー サーバを再起動せずに、現在のサーバの実行時の統計情報をリセットします。このスイッチは以下のカウンタをリセットします。

- 最大スレッド数は、現在のスレッド数の値にリセットされます。
- メッセージ キューの最大階層数は、現在の階層数にリセットされます。
- 最大接続数は、現在の接続数にリセットされます。
- メッセージ数、待機回数、ミス回数、および制限の超過回数はゼロにリセットされます。

このスイッチは以下のカウンタをリセットしません。

- スレッド プールの制限
- 現在のスレッド数
- メッセージ キューの現在の階層数
- 現在の接続数
- 接続数の制限

-publish

ポリシー サーバに関する情報を発行します。

-tadm*port_number*

管理サービス用の TCP ポートを設定します。

-uac*port_number*

RADIUS アカウンティング用の UDP ポートを設定します。

-uadm*port_number*

管理サービス用の UDP ポートを設定します。

-uauth*port_number*

Radius 認証用の UDP ポートを設定します。

-ac

エージェント API リクエストのサービスを有効にします。

-noac

エージェント API リクエストのサービスを無効にします。

-adm

管理リクエストのサービスを有効にします。

-noadm

管理リクエストのサービスを無効にします。

-radius

RADIUS リクエストのサービスを有効にします。

-noradius

RADIUS リクエストのサービスを無効にします。

-onlyadm

以下のオプションを統合して 1 つのオプションにします。

- -adm
- -noac
- -noradius

–starttrace

コマンドの説明

- トレース ファイルへのログの記録を開始し、コンソールへのトレース ロギングには影響しません。
- ポリシー サーバが稼働していない場合は、エラーを発行します。

ポリシー サーバがすでにトレース データのログを記録している場合に –starttrace コマンドを実行すると、

- 現在のトレース ファイルの名前が変更され(ファイル名の最後にタイムスタンプを付けて *file_name*.YYYYMMDD_HHmmss.*extension* の形式で)、
- 元の名前を持つ新しいトレース ファイルが作成されます。

  たとえば、ポリシー サーバ管理コンソールの[プロファイラ]タブでのトレース ファイル名が C:¥temp¥smtrace.log である場合、新しいファイルが生成されると、古いファイルは c:¥temp¥smtrace.20051007_121807.log として保存されます。タイム スタンプは、ファイルが 2005 年 10 月 7 日の午後 12:18 に作成されたことを示しています。ポリシー サーバ管理コンソールの[プロファイラ]タブでファイルのトレース機能を有効にしていない場合は、このコマンドを実行しても何も起こりません。

-stoptrace

コマンドの説明

- ファイルへのログの記録を中止し、コンソールへのトレース ロギングには影響しません。
- ポリシー サーバが稼働していない場合は、エラーを発行します。

smpolicysrv の 2 つのコマンド ライン オプション -dumprequests および -flushrequests を使用すれば、トラブルシューティングを行い、いっぱいになっているポリシー サーバのメッセージ キューの状態から早く回復できます。これらのオプションを使用するのは、以下の場合のみです。

1. ポリシー サーバのメッセージ キューで待機しているエージェント リクエストがタイムアウトになった。
2. タイムアウトになったリクエストが 1 つ以上のエージェントによって再送信され、メッセージ キューがいっぱいになった。

重要: 通常の動作条件下では -dumprequests および -flushrequests を使用しないでください。

-dumprequests

ポリシー サーバのメッセージ キュー内にある各リクエストの概要を監査ログに出力します。

-flushrequests

ポリシー サーバのメッセージ キュー全体をクリアし、リクエストが残っていない状態にします。

デバッグの動的な開始または停止

一部のコンポーネントのデバッグ機能は、ポリシー サーバを再起動 することなく、いつでも開始または停止できます。

注: この機能は、CA テクニカル サポート担当者からの指示があった場合にのみ使用することをお勧めします。

デバッグを動的に開始または停止する方法

1. ポリシー サーバをホストしているマシンでコマンド ウィンドウを開きます。
2. 以下のコマンドを入力します。

   ```
   smcommand -i SiteMinder
   ```

   オプションのリストが表示されます。
3. CA サポート担当者からの指示に従って、以下のデバッグ オプションのいずれかを選択します。

   CA.EPM::EPMObjects_Debug

   SiteMinderEPM コンポーネントのデバッグ状態を切り替えます。

   CA.XPS::Debug

   SiteMinderXPS コンポーネントのデバッグ状態を切り替えます。

   CA.XPS::XPSEval_Debug

   SiteMinderXPSEvaluate コンポーネントのデバッグ状態を切り替えます。

トレースの動的な開始または停止

一部のコンポーネントのトレース機能は、ポリシー サーバを再起動 することなく、いつでも開始または停止できます。

トレースを動的に開始または停止する方法

1. ポリシー サーバをホストしているマシンでコマンド ウィンドウを開きます。
2. 以下のコマンドを入力します。

   ```
   smcommand -i SiteMinder
   ```

3. オプションのリストが表示されます。トレース オプションには、現在の状態の *反対の状態*が表示されます。たとえば、CA XPS のトレースが現在無効になっている場合は、トレースをオンにするオプションが以下のように表示されます。

   item_number - CA.XPS::TraceOn

4. 希望するオプションの番号を入力して、以下のオプションのいずれかを選択します。

   CA.EPM::EPMObjects_Trace*State*

   EPM Objects コンポーネントのトレースをオンまたはオフに切り替えます。

   CA.XPS::Trace*State*

   XPS コンポーネントのトレースをオンまたはオフに切り替えます。

   CA.XPS::XPSEval_Trace*State*

   XPS Expression Evaluator コンポーネントのトレースをオンまたはオフに切り替えます。

   確認メッセージが表示されます。変更が反映されたオプションのリストが再表示されます。

5. （オプション）別のコンポーネントに対してトレースを開始または停止するには、手順 4 を繰り返します。
6. 「Q」と入力して終了します。

   トレースが動的に変更されます。

Web エージェント通信失敗後にポリシー サーバがハングする

症状:

ポリシー サーバ リクエストの処理中、たとえばネットワーク停止などで Web エージェントがオフラインになった場合、この通信失敗についてポリシー サーバに通知されないと、ポリシー サーバは、Web エージェント データを待機し続けます。Web エージェントがネットワーク機能を回復してポリシー サーバとの接続を閉じた後も、ポリシー サーバは待機を続けます。

この方法で、1 つまたは複数の Web エージェントから多くのリクエストが失われた場合、リクエストを処理するワーカー スレッドが解放されないため、ポリシー サーバが反応しなくなる可能性があります。

解決方法:

SiteMinder Enable TCP Keep Alive（SM_ENABLE_TCP_KEEPALIVE）環境変数を作成して有効にすると、アイドル状態の Web エージェント接続に対して KeepAlive パケットを送信するようポリシー サーバが設定されます。ポリシー サーバがパケットを送信する間隔は、OS 固有の TCP/IP パラメータに基づいて決まります。

パラメータを設定する場合には、以下の点を考慮します。

- ポリシー サーバがパケット送信をいつ開始する必要があるか。
- ポリシー サーバがパケットを送信する間隔。
- ポリシー サーバがパケットを何回送信したら、Web エージェント接続が失われたと判断されるか。

  注: TCP/IP パラメータ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。

アイドル状態の Web エージェント接続に KeepAlive パケットを送信するようポリシー サーバを設定する方法

1. ポリシー サーバ ホスト システムにログインします。
2. 以下のいずれかを行います。
   - （Windows）以下のシステム環境変数を作成して値を 1 に設定します。

     SM_ENABLE_TCP_KEEPALIVE

- （UNIX）
  a. 以下のシステム環境変数を作成します。

     SM_ENABLE_TCP_KEEPALIVE=1

  b. 環境変数をエクスポートします。

注: 値は 0（無効）または 1（有効）である必要があります。0 または 1 以外の値が設定された場合、環境変数は無効になります。環境変数が無効になった場合、ポリシー サーバは、アイドル状態の Web エージェント接続に対して KeepAlive パケットを送信しません。

インストールされている JDK のバージョンの確認

ポリシー サーバの起動に失敗した場合、適切なバージョンの JDK がインストールされているかどうかを確認してください。

ポリシー サーバ ログのローカル時間設定の無効化

ポリシー サーバ ログ ファイル（*install_dir*/siteminder/log/smps.log）には、ポリシー サーバがインストールされているマシンのオペレーティング システムで指定されているローカル タイムゾーンの時刻が表示されます。

このログファイルの時刻をグリニッジ標準時 (GMT) で表示するには、次の手順に従います。

1. 次のレジストリ設定を確認します。

   HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥
   CurrentVersion¥LogConfig¥LogLocalTime

2. 値を、1 (デフォルト設定) から 0 に変更します。

システム アプリケーション ログの確認

ポリシー サーバの起動に失敗した場合、イベントログ (Windows NT の場合) または syslog (UNIX の場合) を参照して、ポリシー サーバに関する情報がないかを確認します。

- Windows の場合、イベントビューアを使用してイベントログを参照します。イベントビューアの [ログ] メニューから [アプリケーション] を選択します。
- UNIX の場合、テキストエディタを使用して syslog を参照します。

LDAP SDK 層によって処理される LDAP リフェラル

SiteMinder の LDAP リフェラル処理は強化され、パフォーマンスと冗長性が向上しました。旧バージョンの SiteMinder がサポートしていたのは、LDAP SDK 層による自動 LDAP リフェラル処理でした。LDAP リフェラルが発生すると、これまでは LDAP SDK 層が、参照先サーバへのリクエストの実行を、ポリシー サーバと通信せずに処理していました。

現行バージョンの SiteMinder は、非自動（拡張） LDAP リフェラル処理をサポートしています。非自動リフェラル処理では、LDAP リフェラルは、LDAP SDK 層ではなくポリシー サーバに返されます。リフェラルには、リフェラルの処理に必要なすべての情報が含まれています。ポリシー サーバは、リフェラルで指定されている LDAP ディレクトリが使用できるかどうかを調べて、該当する LDAP ディレクトリが機能していない場合は、リクエストを中断させることができます。この機能により、オフラインのシステムへの LDAP リフェラルによってリクエスト待ち時間が恒常的に増加することによるパフォーマンスの低下が解消されます。このような待ち時間の増加は、SiteMinder でリクエストの飽和状態を発生させることがあります。

LDAP リフェラルの無効化

LDAP リフェラルによってエラーが発生する場合は、すべての LDAP リフェラルを無効にすることができます。LDAP リフェラルを無効にすると、使用しているディレクトリのすべてのリフェラルはエラーを返すようになります。

Windows 環境のポリシー サーバの LDAP リフェラル処理を無効にする方法

1. Windows の[スタート]メニューから[ファイル名を指定して実行]を選択します。
2. [ファイル名を指定して実行]ダイアログボックスで「regedit」と入力し、[OK]をクリックします。
3. レジストリエディタで、次のレジストリ設定を確認します。

   ```
   HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥
   CurrentVersion¥Ds¥LDAPProvider
   ```

4. 次のレジストリ値を変更します。

   注: 値は 16 進数で示されます。

   ```
   "EnableReferrals"=dword:00000001
   ```

   LDAP リフェラルをポリシー サーバによって処理するかどうかを決定します。0 に設定すると、LDAP リフェラルはポリシー サーバによって処理されません。1 に設定すると、LDAP リフェラルはポリシー サーバによって処理されます。

   LDAP リフェラルは、デフォルトでは有効になっています。この設定は、レジストリを編集するだけで変更できます。

5. ポリシー サーバを再起動します。

Solaris 環境のポリシー サーバの LDAP リフェラル処理を無効にする方法

1. 次のディレクトリに移動します。

   install_dir/siteminder/registry

2. テキストエディタを使用して sm.registry を開きます。
3. ファイル内にある次のテキストを確認します。

   ```
   HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥
   CurrentVersion¥Ds¥LDAPProvider
   ```

4. 手順 3 で確認した行の下に次のテキストで始まる行があることを確認します。

   ```
   EnableReferrals
   ```

5. セミコロンの直前にある値を、次の説明に従って変更します。

   注: 値は 16 進数に変換する必要があります。

   LDAP リフェラルをポリシー サーバによって処理するかどうかを決定します。0 に設定すると、LDAP リフェラルはポリシー サーバによって処理されません。1 に設定すると、LDAP リフェラルはポリシー サーバによって処理されます。

6. ポリシー サーバを再起動します。

バインド操作での LDAP リフェラルの処理

Windows 環境のポリシー サーバに対してバインド操作での LDAP リフェラルを設定する方法

1. Windows の[スタート]メニューから[ファイル名を指定して実行]を選択します。
2. [ファイル名を指定して実行]ダイアログボックスで「regedit」と入力し、[OK]をクリックします。
3. レジストリエディタで、次のレジストリ設定を確認します。

   ```
   HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥
   CurrentVersion¥Ds¥LDAPProvider
   ```

4. 次のレジストリ値を変更します。

   注: 値は 16 進数で示されます。

   ```
   "ChaseReferralsOnBind"=dword:00000001
   ```

   バインド操作での LDAP リフェラルを追跡するかどうかを決定します。ほとんどの LDAP ディレクトリ サーバは、バインド操作での LDAP リフェラルを処理します。使用しているディレクトリ サーバがバインド操作でのリフェラルを処理する場合、ChaseReferralsOnBind は無効です。ただし、ディレクトリ サーバが処理しない場合は、この設定によって、ポリシー サーバがバインドリフェラルを処理するようになります。

   使用しているサーバがバインド操作でのリフェラルを処理する場合は、この設定を 0 に変更して、ポリシー サーバのバインド リフェラル処理機能を無効にすることができます。

   バインド操作でのリフェラルの追跡は、デフォルトでは有効になっています。この設定は、レジストリを編集するだけで変更できます。

5. ポリシー サーバを再起動します。

Solaris 環境のポリシー サーバに対してバインド操作での LDAP リフェラルを設定する方法

1. 次のディレクトリに移動します。

   install_dir/siteminder/registry

2. テキストエディタを使用して sm.registry を開きます。
3. ファイル内にある次のテキストを確認します。

   ```
   HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥
   CurrentVersion¥Ds¥LDAPProvider
   ```

4. 手順 3 で確認した行の下に次のテキストで始まる行があることを確認します。

   ```
   ChaseReferralsOnBind
   ```

5. セミコロンの直前にある値を、次の説明に従って変更します。

   注: 値は 16 進数に変換する必要があります。

   バインド操作での LDAP リフェラルを追跡するかどうかを決定します。ほとんどの LDAP ディレクトリ サーバは、バインド操作での LDAP リフェラルを処理します。使用しているディレクトリ サーバがバインド操作でのリフェラルを処理する場合、ChaseReferralsOnBind は無効です。ただし、ディレクトリ サーバが処理しない場合は、この設定によって、ポリシー サーバがバインドリフェラルを処理するようになります。

   使用しているサーバがバインド操作でのリフェラルを処理する場合は、この設定を 0 に変更して、ポリシー サーバのバインド リフェラル処理機能を無効にすることができます。

6. ポリシー サーバを再起動します。

アイドルタイムアウトとステートフルインスペクションデバイス

ステートフルインスペクションデバイス (ファイアウォールなど) では、一般に、アイドルタイムアウトを設定できます。ポリシー サーバからエージェントへの SiteMinder 接続でも、アイドル タイムアウトを設定できます。

ポリシー サーバは、サービスに定期的にポーリングします。ポーリング間隔は、最大 5 分間です。つまり、アイドル接続は、設定された値から 5 分以内にタイムアウトになります。たとえば、タイムアウト値を 55 分間に設定すると、アイドル接続は 55 ～ 60 分間でタイムアウトになります。

デフォルトでは、ポリシー サーバと Web エージェントの間の接続は、非アクティブの状態が 10 分間続くとタイムアウトします。ポリシー サーバと Web エージェントの間にファイアウォールなどのステートフル ネットワーク デバイスがあり、接続のアイドル状態がデバイスのアイドル タイムアウト設定よりも長く続くと、デバイスは、ポリシー サーバや Web エージェントに通知せずに、接続を終了させます。

Web エージェントは、ネットワークデバイスによって終了された接続の使用を試行する際、ネットワークエラーを受信し、接続をリセットして、ブラウザに 500 エラー (20-0003) のメッセージを表示します。また、エージェントは、接続プール内の他の接続で、エラーを受信した接続以前に確立されたものをすべて閉じます。ただし、ポリシー サーバの方では、それらの接続のソケットは確立されたままです。サイトの負荷パターンによっては、ポリシー サーバの正常な動作を妨げるような接続の増加が発生する場合があります。

ファイアウォールなどのステートフル ネットワーク デバイスによるポリシー サーバと Web エージェントの間の接続の終了を防ぐには、ポリシー サーバのアイドル タイムアウトを設定する必要があります。ポリシー サーバは、TCP/IP 接続を閉じると、非アクティブな状態が指定された時間続くのを待ってから、RESET を送信して、サーバ側とクライアント側の両方で接続を適切に閉じます。非アクティブ状態の期間は、ポリシー サーバ管理コンソールの[設定]タブにあるアイドル タイムアウトの[分]フィールドで指定します。

注: アイドル タイムアウトの[分]フィールドは、管理者の総接続時間を制限するためにも使用できます。

インストール時、アイドル タイムアウトの値は 10 分に設定されます。ステートフルネットワークデバイスと共に使用する場合は、この値を、Web エージェントとポリシー サーバの間にあるデバイスの TCP/IP アイドルタイムアウトよりも短い時間に設定してください。 ポリシー サーバのタイムアウトが必ず先に発生するように、TCP アイドル セッション タイムアウトを、ステートフル デバイスのアイドル タイムアウトの 60% に設定することをお勧めします。

エラー -- Optional Feature Not Implemented

ポリシー サーバが ODBC データソースの使用を試行する際、データベースに接続できないと、次のエラーメッセージが表示されることがあります。

```
Optional feature not implemented.. Error code -1
```

多くの場合、このメッセージは、コンポーネントの不適切な組み合わせ、不適切な設定、または無効な認証情報を示しています。

注: CA の Intersolv または Merant ドライバの設定は、デフォルト設定とは異なります。

ODBC データソースをポリシー ストアとして使用しているとき、またはロギング用に使用しているときにこのメッセージが表示される場合は、「*ポリシー サーバ インストール ガイド*」の ODBC データソースの設定に関するセクションを参照してください。

管理者アクティビティの記録時に発生するエラーまたはパフォーマンスの低下

ポリシー サーバ管理コンソールの[監査]タブで、[管理者によるポリシー ストア オブジェクトの変更]を[すべてのイベントのログ取得]に設定している場合、ログを ODBC データソースに記録中に、以下のいずれかの状態になることがあります。

- 管理 UI でのオブジェクトの保存時に大きな遅延が発生する。
- 次のエラーメッセージが表示される。

  ```
  Exception occurred while executing audit log insert.
  ```

このような場合には、ODBC データソースの代わりにテキストファイルにログを記録してください。

キー ロールオーバー ログ メッセージ

ポリシー サーバが Web エージェントに対してキーのロールオーバー コマンドを発行した場合、それらのコマンドが正常に処理される場合もあれば、失敗する場合もあります。この状況のトラブルシューティングを容易にするため、ポリシー サーバでは、以下の 3 種類のメッセージを SMPS.log に記録します。

[情報]キーのロールオーバ リクエストが手動で開始されました。

このメッセージは、管理者がキーのロールオーバを手動で開始した場合に記録されます。

[情報]キーのロールオーバ リクエストがポリシー サーバによって自動的に開始されました。

このメッセージは、ポリシー サーバが自動的にキーのロールオーバを開始した場合に記録されます。

[情報]キーの配布がポリシー サーバによって開始されました。

このメッセージは、キーのロールオーバー リクエストが自動的または手動で開始された場合に記録されます。

キャッシュ更新ログ メッセージ

管理 UI またはコマンド ライン インターフェースによって、キャッシュのフラッシュまたは更新を有効化および無効化することができます。トラブルシューティングを容易にするため、ポリシー サーバは、以下の 2 種類のメッセージを SMPS.log に記録します。

[情報]サーバ 'enablecacheupdates' コマンドを受信しました。

このメッセージは、管理 UI またはコマンド ライン インターフェースのいずれかによって、キャッシュのフラッシュが有効にされた場合に記録されます。

[情報]サーバ 'disablecacheupdates' コマンドを受信しました。

このメッセージは、管理 UI またはコマンド ライン インターフェースのいずれかによって、キャッシュのフラッシュが無効にされた場合に記録されます。

ポリシー サーバ管理コンソールを開くときのイベント ハンドラ リスト設定に関する警告

症状:

SiteMinder r12.0 SP3 へのアップグレード後、初めてポリシー サーバ管理コンソールにログインすると、イベント ハンドラ リストを XPSAudit に設定する必要があることを示す警告メッセージが表示されます。

解決方法:

SiteMinder r12.0 SP3 の場合、ポリシー サーバ管理コンソールを使用してカスタム イベント ハンドラ ライブラリを追加することはできなくなりました。任意のカスタム イベント ハンドラ ライブラリを追加するには、XPSConfig コマンド ライン ツールを使用します。

SiteMinder ポリシー サーバの起動イベント ログ

症状:

ポリシー サーバが起動中にクラッシュしました。ポリシー サーバがクラッシュする前にどのような SiteMinder 起動イベントが発生したのかを知るにはどうしたら良いですか。

解決方法:

ポリシー サーバが起動中にクラッシュした場合は、起動イベントのログが以下のファイルに格納されます。

policy_server_home/audit/SmStartupEvents.audit

付録 C: ログファイルの説明

このセクションには、以下のトピックが含まれています。

smaccesslog4

次の表では、認証および許可アクティビティを記録する smaccesslog4 に示されるロギングについて説明します。

フィールド名	説明	NULL/NOT NULL	フィールド タイプ
sm_timestamp	エントリがデータベースに作成された日時をマークします。	NOT NULL	DATE
sm_categoryid	ロギングのタイプを示す識別子です。次のいずれかの値をとります。 ■ 1 = Auth ■ 2 = Az ■ 3 = Admin ■ 4 = Affiliate	NOT NULL	NUMBER(38)

フィールド名	説明	NULL/NOT NULL	フィールド タイプ
sm_eventid	ロギングを実行させた個別のイベントを示します。次のいずれかの値をとります。 ■ 1 = AuthAccept ■ 2 = AuthReject ■ 3 = AuthAttempt ■ 4 = AuthChallenge ■ 5 = AzAccept ■ 6 = AzReject ■ 7 = AdminLogin ■ 8 = AdminLogout ■ 9 = AdminReject ■ 10 = AuthLogout ■ 11 = ValidateAccept ■ 12 = ValidateReject ■ 13 = Visit	NOT NULL	NUMBER(38)
sm_hostname	サーバが動作しているマシンです。		VARCHAR2(255)
sm_sessionid	このユーザのアクティビティのセッション識別子です。		VARCHAR2(255)
sm_username	このセッションで現在ログインしているユーザのユーザ名です。		VARCHAR2(512)
sm_agentname	ポリシー サーバと共に使用されているエージェントに関連付けられている名前です。		VARCHAR2(255)
sm_realmname	ユーザが必要としているリソースが現在あるレルムです。		VARCHAR2(255)
sm_realmoid	レルムの固有識別子です。		VARCHAR2(64)
sm_clientip	保護されたリソースを利用しようとしているクライアント マシンの IP アドレスです。		VARCHAR2(255)
sm_domainoid	ユーザがアクセスしているレルムおよびリソースが存在するドメインの固有識別子です。		VARCHAR2(64)

フィールド名	説明	NULL/NOT NULL	フィールド タイプ
sm_authdirname	このフィールドは、レポート生成機能では使用されません。		VARCHAR2(255)
sm_authdirserver	このフィールドは、レポート生成機能では使用されません。		VARCHAR2(512)
sm_authdir-namespace	このフィールドは、レポート生成機能では使用されません。		VARCHAR2(255)
sm_resource	ユーザがリクエストしているリソース（Web ページなど）です。		VARCHAR2(512)
sm_action	HTTP アクション（Get、Post、および Put）です。		VARCHAR2(255)
sm_status	HTTP アクションに関するいくつかの説明文です。		VARCHAR2(1024)

フィールド名	説明	NULL/NOT NULL	フィールド タイプ
sm_reason	ロギングを実行する理由です。32000 以上はユーザが定義します。以下のとおりです。 ■ 0 = なし ■ 1 = PwMustChange ■ 2 = InvalidSession ■ 3 = RevokedSession ■ 4 = ExpiredSession ■ 5 = AuthLevelTooLow ■ 6 = UnknownUser ■ 7 = UserDisabled ■ 8 = InvalidSessionId ■ 9 = InvalidSessionIp ■ 10 = CertificateRevoked ■ 11 = CRLOutOfDate ■ 12 = CertRevokedKeyCompromised ■ 13 = CertRevokedAffiliationChange ■ 14 = CertOnHold ■ 15 = TokenCardChallenge ■ 16 = ImpersonatedUserNotInDi ■ 17 = Anonymous ■ 18 = PwWillExpire ■ 19 = PwExpired ■ 20 = ImmedPWChangeRequired ■ 21 = PWChangeFailed ■ 22 = BadPWChange ■ 23 = PWChangeAccepted ■ 24 = ExcessiveFailedLoginAttempts ■ 25 = AccountInactivity ■ 26 = NoRedirectConfigured ■ 27 = ErrorMessageIsRedirect	NOT NULL	NUMBER(38)

フィールド名	説明	NULL/NOT NULL	フィールド タイプ
sm_reason（続き）	■ 28 = Tokencode ■ 29 = New_PIN_Select ■ 30 = New_PIN_Sys_Tokencode ■ 31 = New_User_PIN_Tokencode ■ 32 = New_PIN_Accepted ■ 33 = Guest ■ 34 = PWSelfChange ■ 35 = ServerException ■ 36 = UnknownScheme ■ 37 = UnsupportedScheme ■ 38 = Misconfigured ■ 39 = BufferOverflow		
sm_transactionid	このフィールドは、レポート生成機能では使用されません。		VARCHAR2(255)
sm_domainname	ユーザがアクセスしているレルムおよびリソースが存在するドメインの名前です。	NULL	VARCHAR2(255)
sm_impersonator-name	別名セッションで別名ユーザとして動作している管理者のログイン名です。	NULL	VARCHAR2(512)
sm_impersonator-dirname	別名ユーザが含まれているディレクトリオブジェクトの名前です。	NULL	VARCHAR2(255)

smobjlog4

次の表では、管理イベントを記録する smobjlog4 に示されるロギングについて説明します。

フィールド名	説明	NULL/NOT NULL	タイプ
sm_timestamp	エントリがデータベースに作成された日時を示します。	NOT NULL	DATE

フィールド名	説明	NULL/NOT NULL	タイプ
sm_categoryid	ロギングのタイプを示す識別子です。次のいずれかの値をとります。 ■ 1 = Auth ■ 2 = Agent ■ 3 = AgentGroup ■ 4 = Domain ■ 5 = Policy ■ 6 = PolicyLink ■ 7 = Realm ■ 8 = Response ■ 9 = ResponseAttr ■ 10 = ResponseGroup ■ 11 = Root ■ 12 = Rule ■ 13 = RuleGroup ■ 14 = Scheme ■ 15 = UserDirectory ■ 16 = UserPolicy ■ 17 = Vendor ■ 18 = VendorAttr ■ 19 = Admin ■ 20 = AuthAzMap ■ 21 = CertMap ■ 22 = ODBCQuery ■ 23 = SelfReg ■ 24 = PasswordPolicy ■ 25 = KeyManagement ■ 26 = AgentKey ■ 27 = ManagementCommand ■ 28 = RootConfig	NOT NULL	NUMBER(38)

フィールド名	説明	NULL/NOT NULL	タイプ
sm_categoryid（続き）	■ 29 = Variable ■ 30 = VariableType ■ 31 = ActiveExpr ■ 32 = PropertyCollection ■ 33 = PropertySection ■ 34 = Property ■ 35 = TaggedString ■ 36 = TrustedHost ■ 37 = SharedSecretPolicy	NOT NULL	NUMBER(38)
sm_eventid	ロギングを実行させた個別のイベントを示します。次のいずれかの値をとります。 ■ 1 = Create ■ 2 = Update ■ 3 = UpdateField ■ 4 = Delete ■ 5 = Login ■ 6 = Logout ■ 7 = LoginReject ■ 8 = FlushAll ■ 9 = FlushUser ■ 10 = FlushUsers ■ 11 = FlushRealms ■ 12 = ChangeDynamicKeys ■ 13 = ChangePersistentKey ■ 14 = ChangeDisabledUserState ■ 15 = ChangeUserPassword ■ 16 = FailedLoginAttemptsCount ■ 17 = ChangeSessionKey	NOT NULL	NUMBER(38)

フィールド名	説明	NULL/NOT NULL	タイプ
sm_hostname	このフィールドは、管理ロギングのレポート生成機能では使用されません。		VARCHAR2(255)
sm_sessionid	このユーザのアクティビティのセッション識別子です。		VARCHAR2(255)
sm_username	この管理者のユーザ名です。		VARCHAR2(512)
sm_objname	管理者内のアクセスされているオブジェクトです。		VARCHAR2(512)
sm_objoid	管理者内のアクセスされているオブジェクトの固有識別子です。このフィールドは、レポート生成機能では使用されません。		VARCHAR2(64)
sm_fielddesc	管理者のアクションに関するいくつかの説明文です。		VARCHAR2(1024)
sm_domainoid	管理者内の、変更されているオブジェクトが含まれているドメインの固有識別子です。このフィールドは、レポート生成機能では使用されません。		VARCHAR2(64)
sm_status	HTTP アクションに関するいくつかの説明文です。このフィールドは、レポート生成機能では使用されません。		VARCHAR2(1024)

付録 D: 診断情報の発行

このセクションには、以下のトピックが含まれています。

診断情報の概要

ポリシー サーバには、SiteMinder 環境に関する診断情報を発行するためのコマンド ライン ツールが含まれています。このツールを使用すると、ポリシー サーバ、ポリシー ストア、ユーザ ディレクトリ、エージェント、およびカスタム モジュールに関する情報を発行できます。

コマンド ライン インターフェースの使用

ポリシー サーバには、情報を発行するための、コマンド ラインで実行するコマンドが用意されています。このコマンドは、*installation_dir*/siteminder/bin ディレクトリにあります。

情報を発行するには、smpolicysrv コマンドを、-publish スイッチを付けて使用します。例:

```
smpolicysrv -publish <optional file_name>
```

注: Windows システムでは、リモート デスクトップまたはターミナル サービス ウィンドウから smpolicysr コマンドを実行しないでください。smpolicysrv コマンドはプロセス間通信に依存します。この通信は、リモート デスクトップまたは[ターミナル サービス]ウィンドウから smpolicysrv プロセスを実行した場合には機能しません。

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

発行される情報の保存場所の指定

発行される情報は、指定したファイルに XML 形式で書き込まれます。指定したファイル名は以下のレジストリ キーに保存されます。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥CurrentVersion¥
Publish
```

このキーは、Windows システムではシステム レジストリにあり、UNIX システムでは *install_dir*/registry/sm.registry ファイルにあります。レジストリ設定のデフォルト値は以下のとおりです。

policy_server_install_dir>¥log¥smpublish.xml

コマンド ラインから **smpolicysrv -publish** を実行し、パスとファイル名を指定しない場合、発行される XML ファイルの保存場所はレジストリ設定の値によって決まります。

注: Windows システムでは、リモート デスクトップまたはターミナル サービス ウィンドウから smpolicysr コマンドを実行しないでください。smpolicysrv コマンドはプロセス間通信に依存します。この通信は、リモート デスクトップまたは[ターミナル サービス]ウィンドウから smpolicysrv プロセスを実行した場合には機能しません。

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

XML ファイルの保存場所を指定し、XML ファイル内に出力を生成する方法

1. コマンドラインで、次のディレクトリに移動します。

   installation_dir/siteminder/bin

2. 以下のコマンドを入力します。

   smpolicysrv -publish *path_and_file_name*

Windows 環境では、たとえば、次のように入力します。

```
smpolicysrv -publish c:¥netegrity¥siteminder¥published-data.txt
```

UNIX 環境では、たとえば、次のように入力します。

```
smpolicysrv -publish /netegrity/siteminder/published-data.txt
```

指定した場所に XML 出力が生成され、この場所に一致するように HKEY_LOCAL_MACHINE¥SOFTWARE¥Netegrity¥SiteMinder¥CurrentVersion¥Publish レジストリ キーの値が更新されます。

データの発行

このセクションでは、次のコンポーネントに関して発行できる情報の概要を示します。

- ポリシー サーバ
- ポリシー/キーストア
- ユーザ ディレクトリ
- エージェント
- カスタムモジュール

発行されるポリシー サーバ情報

ポリシー サーバ情報には、サーバ名、プラットフォーム、設定、およびサーバ バージョン情報が含まれます。さらに、ポリシー サーバの設定に使用されている任意のレジストリ設定を発行することもできます。

発行されるポリシー サーバ情報には、次のものが含まれます。

- 基本情報
  - 名前
  - バージョン

- プラットフォーム
- スレッドプールの統計情報

- サーバ設定 (ポリシー サーバ管理コンソールで設定されている値)
  - キー管理
  - ジャーナル
  - キャッシュ
  - イベントハンドラー
  - 追跡ロギング
  - 監査ロギング

発行されるポリシー サーバ XML 出力の形式

以下の例は、ポリシー サーバ情報がどのようにフォーマットされるかを示しています。

```
<SERVER>
     < SHORT_NAME>   smpolicysrv </SHORT_NAME>
     <FULL_NAME>    SiteMinder Policy Server </FULL_NAME>
     <PRODUCT_NAME> SiteMinder(tm) </PRODUCT_NAME>
     <VERSION>  6.0 </VERSION>
     <UPDATE>   01 </UPDATE>
     <LABEL>    283 </LABEL>
     <PLATFORM> Windows (Build 3790)
    </PLATFORM>
     <SERVER_PORT>     44442 </SERVER_PORT>
     <RADIUS_PORT> 0 </RADIUS_PORT>
     <THREADPOOL>
         <MSG_TOTALS>    15011 </MSG_TOTALS>
         <MSG_DEPTH>     2 </MSG_DEPTH>
         <THREADS_LIMIT> 8 </THREADS_LIMIT>
         <THREADS_MAX>   3 </THREADS_MAX>
         <THREADS_CURRENT> 3 </THREADS_CURRENT>
     </THREADPOOL>
     <CRYPTO> 128 </CRYPTO>
     <KEYMGT>
         <GENERATION> enabled </GENERATION>
         <UPDATE>     disabled </UPDATE>
     </KEYMGT>
     <JOURNAL>
         <REFRESH> 60 </REFRESH>
         <FLUSH>   60 </FLUSH>
     </JOURNAL>
     <PSCACHE>
         <STATE>           enabled </STATE>
         <PRELOAD>         enabled </PRELOAD>
     </PSCACHE>
     <USERAZCACHE>
         <STATE>    enabled </STATE>
         <MAX>      10 </MAX>
         <LIFETIME> 3600 </LIFETIME>
     </USERAZCACHE>
</SERVER>
```

以下の表に、発行されるポリシー サーバ情報を示します。

タグ	中身	説明	親タグ	必須
SERVER	要素	サーバに関する情報であることを示します	SMPUBLSIH	必須
SHORT_NAME	テキスト	サーバの略称	SERVER	必須
FULL_NAME	テキスト	稼働しているサーバのフルネーム	SERVER	必須
PRODUCT_NAME	テキスト	製品名	SERVER	必須
VERSION	テキスト	サーバのバージョン	SERVER	必須
UPDATE	テキスト	サービスパックのバージョン	SERVER	必須
LABEL	テキスト	ビルドまたは CR 番号	SERVER	必須
PLATFORM	テキスト	OS プラットフォーム識別データ	SERVER	必須
THREAD_POOL	要素	スレッド プールに関する情報	SERVER	必須
MSG_TOTAL	整数	処理されたスレッド プール メッセージの数	THREAD_POOL	必須
MSG_DEPTH	整数	スレッド プール内のメッセージの最大数	THREAD_POOL	必須
THREADS_LIMIT	整数	スレッドの最大数	THREAD_POOL	必須
THREADS_MAX	整数	使用されているスレッドの最大数	THREAD_POOL	必須
THREADS_CURRENT	整数	現在使用されているスレッドの数	THREAD_POOL	必須
PSCACHE	要素	ポリシー サーバ キャッシュ設定に関する情報であることを示します	SERVER	必須
PRELOAD	テキスト	有効か無効かを示します	PSCACHE	必須
JOURNAL	なし	ジャーナル設定(リフレッシュ間隔とクリア間隔)を示します	SERVER	必須

タグ	中身	説明	親タグ	必須
FLUSH	整数	クリア間隔	JOURNAL	必須
REFRESH	整数	リフレッシュ間隔	JOURNAL	必須
KEYMGT	なし	キー管理設定を示します (Generation: 自動キー生成が有効になっているかどうか) (Update: エージェント キーの自動更新が有効になっているかどうか)	SERVER	必須
GENERATION	enabled または disabled	自動キー生成が有効になっているかどうかを示します	KEYMGT	必須
UPDATE	enabled または disabled	エージェント キーの自動更新が有効になっているかどうかを示します	KEYMGT	必須
USERAZCACHE	要素	ユーザ許可キャッシュ設定に関する情報であることを示します	SERVER	必須
MAX	整数	キャッシュエントリの最大数	USERAZCACHE	必須
LIFETIME	整数	キャッシュされたオブジェクトの有効期間	USERAZCACHE	必須
PORT	整数	ポート番号	SERVER	必須
RADIUS_PORT	整数	RADIUS ポート番号 (有効になっている場合)	SERVER	必須
STATE	テキスト、enabled または disabled	あるものが有効か無効かを示します	さまざまなタグ	両方

発行されるオブジェクト ストア情報

ポリシー サーバは、以下のタイプのオブジェクト ストアに情報を格納できます。

- ポリシーストア
- キーストア

- 監査ログ ストア
- セッション サーバ ストア

発行されるオブジェクト ストア情報には、使用されているオブジェクト ストアのタイプ、バック エンド データベース情報、設定情報、および接続情報が含まれます。

発行されるポリシー/キーストア XML 出力の形式

以下の例は、ポリシー/キー ストア情報がどのようにフォーマットされるかを示します。

```
<POLICY_STORE>

   <DATASTORE>
      <NAME> Policy Store   </NAME>
      <USE_DEFAULT_STORE>  false </USE_DEFAULT_STORE>
      <LOADED> true </LOADED>
      <SERVER_LIST>
         <CONNECTION_INFO>
            <TYPE> ODBC</TYPE>
            <SERVICE_NAME> sm </SERVICE_NAME>
            <USER_NAME> sa </USER_NAME>
            <DBMS_NAME> Microsoft SQL Server <SQL/DBMS_NAME>
            <DRIVER_NAME> Microsoft SQL Server <SQL/DRIVER_NAME>
            <DBMS_VERSION> 08.00.0760 </DBMS_VERSION>
         </CONNECTION_INFO>
     </SERVER_LIST>
   </DATASTORE>

   <DATASTORE>
      <NAME>  Key Store </NAME>
      <USE_DEFAULT_STORE> true </USE_DEFAULT_STORE>
      <LOADED> true </LOADED>
   </DATASTORE>

   <DATASTORE>
      <NAME> Audit Log Store </NAME>
      <USE_DEFAULT_STORE> true </USE_DEFAULT_STORE>
      <LOADED> true </LOADED>
   </DATASTORE>

   <DATASTORE>
      <NAME> Session Server Store </NAME>
      <USE_DEFAULT_STORE>  false </USE_DEFAULT_STORE>
      <LOADED> false </LOADED>
   </DATASTORE>

</POLICY_STORE>
```

以下の表に、発行されるポリシー/キー ストア情報を示します。

タグ	中身	説明	親タグ	必須
POLICY_STORE	要素	すべてのデータストアに関する情報であることを示します	SMPUBLISH	必須
DATASTORE	要素	特定のオブジェクトストアに関する情報であることを示します。 ■ TYPE は、データ ストアのタイプを示します。 ■ USE_DEFAULT_STORE は、そのタイプのデフォルト オブジェクト ストアが使用されていることを示します。 ■ LOADED は、そのタイプがロードされているかどうかを示します。	POLICY_STORE	必須
NAME	テキスト	データストアの名前/タイプ	DATASTORE	必須
USE_DEFAULT_STORE	テキスト	ストレージがデフォルトの「ポリシー ストア」内にあるかどうか（true または false）を示します	DATASTORE	必須
LOADED	テキスト	データ ストアがロードされて、初期化されているかどうか（true または false）を示します	DATASTORE	必須
TYPE	テキスト	ポリシー ストアのタイプ（ODBC または LDAP）	DATASTORE	必須
SERVER_LIST	要素	データストア（ODBC）に使用されるフェイルオーバー サーバのリスト	DATASTORE	任意
CONNECTION_INFO	要素	サーバ接続のタイプ	SERVER_LIST	任意
DRIVER_NAME	テキスト	ODBC ドライバの名前	CONNECTION	任意
IP	テキスト	IP アドレス	DATASTORE	任意
LDAP_VERSION	テキスト	LDAP のバージョン	DATASTORE	任意

タグ	中身	説明	親タグ	必須
API_VERSION	テキスト	LDAP API のバージョン	DATASTORE	任意
PROTOCOL_VERSION	テキスト	LDAP プロトコルのバージョン	DATASTORE	任意
API_VENDOR	テキスト	API のベンダー	DATASTORE	任意
VENDOR_VERSION	テキスト	ベンダーのバージョン	DATASTORE	任意

発行されるユーザ ディレクトリ情報

ポリシー サーバによってロードおよびアクセスされたユーザ ディレクトリごとに、以下の情報を発行できます。

- 設定
- 接続
- バージョン

発行されるユーザ ディレクトリ XML 出力の形式

ユーザ ディレクトリ情報は、以下の例のような形式で発行されます。

注: 発行される情報は、ユーザ ディレクトリのタイプによって異なります。

```
< USER_DIRECTORIES>

   <DIRECTORY_STORE >
      <TYPE> ODBC </TYPE>
      <NAME> sql5.5sample </NAME>
      <MAX_CONNECTIONS> 15 </MAX_CONNECTIONS>
         <SERVER_LIST>
            <CONNECTION_INFO>
               <TYPE> ODBC</TYPE>
               <SERVICE_NAME> sql5.5sample </SERVICE_NAME>
               <USER_NAME> sa </USER_NAME>
               <DBMS_NAME> Microsoft SQL Server <SQL/DBMS_NAME>
               <DRIVER_NAME> Microsoft SQL Server <SQL/DRIVER_NAME>
               <DBMS_VERSION> 08.00.0760 </DBMS_VERSION>
            </CONNECTION_INFO>
         </SERVER_LIST>
   </DIRECTORY_STORE >
   <DIRECTORY_STORE>
      <TYPE> LDAP:  </TYPE>
      <NAME> LDAPsample </NAME>
      <FAILOVER_LIST> 172.26.14.101:12002 </FAILOVER_LIST>
      <VENDOR_NAME> Netscape-Directory/4.12 B00.193.0237
      </VENDOR_NAME>
      <SECURE_CONNECTION> disabled </SECURE_CONNECTION>
      <CREDENTIALS>       required </CREDENTIALS>
      <CONNECTION_INFO>
         <PORT_NUMBER> 12002 </PORT_NUMBER>
         <DIR_CONNECTION> 172.26.14.101:12002 </DIR_CONNECTION>
         <USER_CONNECTION> 172.26.14.101:12002 </USER_CONNECTION>
      </CONNECTION_INFO>
      <LDAP_VERSION>     1 </LDAP_VERSION>
      <API_VERSION>      2005 </API_VERSION>
      <PROTOCOL_VERSION> 3 </PROTOCOL_VERSION>
      <API_VENDOR>       mozilla.org </API_VENDOR>
      <VENDOR_VERSION>   500 </VENDOR_VERSION>
   </DIRECTORY_STORE>
</USER_DIRECTORIES>
```

以下の表に、発行されるユーザ ディレクトリ情報を示します。

タグ	中身	説明	親タグ	必須
USER_DIRECTORIES	要素	ロードされている一連のディレクトリ ストアに関する情報であることを示します	SMPUBLISH	必須
DIRECTORY_STORE	要素	特定のディレクトリ ストアに関する情報であることを示します	USER_DIRECTORIES	オプション
TYPE	テキスト	ディレクトリストアのタイプ	DIRECTORY_STORE	必須
NAME	テキスト	定義されているディレクトリストアの名前	DIRECTORY_STORE	必須
MAX_CONNECTIONS	整数	定義されている接続の最大数	DIRECTORY_STORE	オプション
SERVER_LIST	要素	一連のサーバ（ODBC）	DIRECTORY_STORE	オプション
FAILOVER_LIST	テキスト			

発行されるエージェント情報

発行されるエージェント情報は、現在ポリシー サーバに接続されているエージェント (IP アドレス、名前など) を示します。

発行されるエージェント XML 出力の形式

エージェント情報は、次の例のような形式で発行されます。

```
< AGENT_CONNECTION_MANAGER>
   <CURRENT>       4 </CURRENT>
   <MAX>           4 </MAX>
   <DROPPED>       0 </DROPPED>
   <IDLE_TIMEOUT> 0 </IDLE_TIMEOUT>
   <ACCEPT_TIMEOUT> 10 </ACCEPT_TIMEOUT>

   <AGENT_CONNECTION>
      <NAME> agent1 </NAME>
      <IP>   172.26.6.43 </IP>
      <API_VERSION> 1024 </API_VERSION>
      <LAST_MESSAGE_TIME> 0x05705E0C </LAST_MESSAGE_TIME>
   </AGENT_CONNECTION>
   <AGENT_CONNECTION>
      <NAME> agent1 </NAME>
      <IP>   172.26.6.43 </IP>
      <API_VERSION> 1024 </API_VERSION>
      <LAST_MESSAGE_TIME> 0x05705E0C </LAST_MESSAGE_TIME>
   </AGENT_CONNECTION>
   <AGENT_CONNECTION>
      <NAME> agent1 </NAME>
      <IP>   172.26.6.43 </IP>
      <API_VERSION> 1024 </API_VERSION>
      <LAST_MESSAGE_TIME> 0x05705E0C </LAST_MESSAGE_TIME>
   </AGENT_CONNECTION>
   <AGENT_CONNECTION>
      <NAME> 940c0728-d405-489c-9a0e-b2f831f78c56 </NAME>
      <IP>   172.26.6.43 </IP>
      <API_VERSION> 1482282902 </API_VERSION>
      <LAST_MESSAGE_TIME> 0x05705E0C </LAST_MESSAGE_TIME>
   </AGENT_CONNECTION>
</AGENT_CONNECTION_MANAGER>
```

注: エージェント接続情報は <AGENT_CONNECTION_MANAGER> タグ内に含まれています。

以下の表に、発行されるエージェント情報を示します。

タグ	中身	説明	親タグ	必須
AGENT_CONNECTION-_MANAGER	要素	エージェント接続に関する情報であることを示します	SM_PUBLISH	必須
CURRENT	整数	現在の接続数	AGENT_CONNECTION-_MANAGER	必須
MAX	整数	接続の最大数	AGENT_CONNECTION-_MANAGER	必須
DROPPED	整数	接続の最大数	AGENT_CONNECTION-_MANAGER	必須
IDLE_TIMEOUT	整数	アイドル接続がタイムアウトするまでの時間	AGENT_CONNECTION-_MANAGER	必須
ACCEPT_TIMEOUT	整数	接続試行がタイムアウトするまでの時間	AGENT_CONNECTION-_MANAGER	必須
AGENT_CONNECTION	要素	アクティブなエージェント接続に関する情報であることを示します	AGENT_CONNECTION-_MANAGER	オプション
IP	テキスト	エージェントの IP アドレス	AGENT_CONNECTION	必須
API_VERSION	整数	接続しているエージェントによって使用されている API のバージョン	AGENT_CONNECTION	必須
NAME	テキスト	エージェントの名前	AGENT_CONNECTION	必須
LAST_MESSAGE_TIME	整数	エージェントから最後にメッセージが送信されてからの経過時間	AGENT_CONNECTION	必須
AGENT_CONNECTION-_MANAGER	要素	エージェント接続に関する情報であることを示します	SM_PUBLISH	必須

発行されるカスタム モジュール情報

カスタム モジュールは、既存のポリシー サーバの機能を拡張するために作成できる DLL またはライブラリです。これには、いくつかのタイプ（イベント ハンドラ、認証モジュール、許可モジュール、ディレクトリ モジュール、トンネル モジュール）があります。認証モジュールは、一般に、カスタム認証方式と呼ばれ、許可モジュールは、アクティブポリシーと呼ばれます。トンネル モジュールは、エージェントとの安全な接続を定義するために使用されます。イベント モジュールは、イベント通知を受信するためのメカニズムを提供します。ポリシー サーバによってロードされているカスタムモジュールを示す情報を発行することができます。カスタム モジュールの各タイプは、独自の XML タグで定義されます。

発行されるカスタム モジュール XML 出力の形式

以下の表に、発行されるカスタム モジュール情報を示します。

タグ	中身	説明	親タグ	必須
EVENT_LIB	要素	イベント API カスタムモジュールに関する情報であることを示します	SMPUBLISH	任意
AUTH_LIB	要素	認証 API カスタムモジュールに関する情報であることを示します	SMPUBLISH	任意
DS_LIB	要素	ディレクトリ API カスタムモジュールに関する情報であることを示します	SMPUBLISH	任意
TUNNEL_LIB	要素	トンネル API カスタムモジュールに関する情報であることを示します	SMPUBLISH	任意
AZ_LIB	要素	許可 API カスタムモジュールに関する情報であることを示します	SMPUBLISH	任意

次のタグは、すべてのタイプのカスタムモジュールに共通です。

タグ	中身	説明	親タグ	必須
FULL_NAME	テキスト	ライブラリまたは DLL のパスを含む完全な名前		必須
CUSTOM_INFO	テキスト	カスタムライブラリによって提供される情報		任意
LIB_NAME	テキスト	ライブラリまたは DLL の名前		任意
VERSION	整数	サポートされている API のバージョン		任意

次のタグは、特定タイプのモジュール専用です。

タグ	中身	説明	API タイプ	必須
ACTIVE_FUNCTION	テキスト	アクティブな式としてコールできるようにロードされている関数の名前	許可 API	任意

付録 E: エラー メッセージ

このセクションには、以下のトピックが含まれています。

認証

メッセージ	関数	説明
1）検証のため新しい PIN を ACE/Server に送信しています	SmLoginLogoutMessage::Send-NewPinForValidation1	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカル サポートに連絡してください。
2）検証 %1s のため新しい PIN を ACE/Server に送信しています	SmLoginLogoutMessage::Send-NewPinForValidation2	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカル サポートに連絡してください。
ACE Server --- PIN ポリシーを取得できませんでした	SmLoginLogoutMessage::Sm-AuthAceGetPinPoliciesFail	SecurID 認証方式において、SecurID/ACE API コールを使用して ACE サーバのバックエンド PIN ポリシーを取得できない場合、このメッセージが表示されます。
ACE Server --- PIN パラメータを取得できませんでした	SmLoginLogoutMessage::Sm-AceHtmlPinParamFail	SecurID 認証方式において、SecurID/ACE API コールを使用して ACE の PIN パラメータを取得できない場合、このメッセージが表示されます。

メッセージ	関数	説明
ACE の状態が ACM_NEXT_CODE_ REQUIRED ではありません。状態 = %1i	SmLoginLogoutMessage::Ace-NextTokenCodeState	HTML SecurID 認証方式において、ユーザのトークン コード値の期限が切れているため、新しい認証を試行する前に次のコードを待つ必要がある場合、このメッセージが表示されます。
ACE/Server - 新しい PIN が必要です。isselectable PIN 属性について AceAPI によってあいまいな値が返されました。ACE 認証を完了できません	SmLoginLogoutMessage::Sm-AceHtmlPinRequired	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカル サポートに連絡してください。
ACE/Server - 新しい PIN が必要です。システム PIN を選択または承諾することができます。Sm_AuthApi_Reject、Sm_Api_Reason_New_PIN_ Select を返します。	SmLoginLogoutMessage::Sm-AceHtmlChooseNewOrSysPin	SecurID 認証方式において、ACE ユーザが自分で選択した PIN またはシステムによって生成された PIN を使用するように設定されている場合、このメッセージが表示されます。
ACE/Server - 新しい PIN が必要です。システム PIN を承諾する必要があります。Sm_Api_Reason_New_PIN_Sys_Tokencode が返されました	SmLoginLogoutMessage::Sm-AceHtmlCannotChoosePin	SecurID 認証方式において、ACE ユーザが常にシステムによって生成された PIN を使用するように設定されている場合、このメッセージが表示されます。
ACE/Server - 新しい PIN が必要です。PIN を選択する必要があります。Sm_AuthApi_Reject、Sm_Api_Reason_New_User_-PIN_Tokencode を返します	SmLoginLogoutMessage::Sm-AceHtmlChooseNewPin	SecurID 認証方式において、ACE ユーザが常に自分で選択した PIN を使用するように設定されている場合、このメッセージが表示されます。
ACE/Server: ACM_NEW_PIN_ACCEPTED は aceRetVal%1i で失敗しました	SmLoginLogoutMessage::Ace-ServerNewPinAcceptedFailed	HTML SecurID 認証方式で使用されます。新しいユーザ PIN が ACE サーバによって承諾されなかった場合に表示されます。

メッセージ	関数	説明
ACE/Server: ACM_NEW_PIN_ACCEPTED は aceRetVal%1i、 ACE ステータス %2i で失敗しました	SmLoginLogoutMessage::Not-WinAceServerNewPinAccepted-Failed	HTML SecurID 認証方式で使用されます。新しいユーザ PIN が ACE サーバによって承諾されなかった場合に表示されます。
ACE/Server: ACM_NEW_PIN_ACCEPTED に失敗しました	SmLoginLogoutMes-sage::NewPinAcceptedFailed	HTML SecurID 認証方式で使用されます。新しいユーザ PIN が ACE サーバによって承諾されなかった場合に表示されます。
ACE/Server によって AceCheck アクセスが拒否されました	SmLoginLogoutMessage::Ace-CheckAccessDenied	SecurID 認証方式において、認証リクエストが ACE サーバによって拒否された場合、このメッセージが表示されます。
AceCheck が処理されません。 aceRetVal = %1i	SmLoginLogoutMessage::Ace-CheckNotProcessed	SecurID 認証方式において、ACE/SecurID API を使用して ACE 認証プロセスを完了できない場合、このエラー メッセージが表示されます。
AceCheck が ACM_NEW_PIN_REQUIRED ではなく %1i を返しました	SmLoginLogoutMessage::Acm-NewPinRequiredFail	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカル サポートに連絡してください。
AceCheck が ACM_NEW_PIN_REQUIRED ではなく %1i を返しました	SmLoginLogoutMessage::Invalid-ReturnAceCheckNewPin	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカル サポートに連絡してください。
AceCheck: 拒否されました ---aceRetVal = %1i	SmLoginLogoutMessage::Sm-AuthAceCheck-Denial	SecurID 認証方式において、認証リクエストが ACE サーバによって拒否された場合、このメッセージが表示されます。
AceGetMaxPinLen の実行に失敗しました	#REF!	HTML SecurID 認証方式で使用されます。ACE サーバで許可されているユーザ PIN の最大長を取得できなかった場合、このメッセージが表示されます。

メッセージ	関数	説明
AceSendPin の実行に失敗しました	SmLoginLogoutMessage::Ace-SendPinFailed	HTML SecurID 認証方式において、ACE/SecurID API を使用してユーザ PIN を RSA ACE サーバに送信できなかった場合、このエラー メッセージが表示されます。認証方式によってリクエストは拒否されます。
AceServer - PIN を選択できません	SmLoginLogoutMessage::Ace-ServerCannotChoosePin	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカル サポートに連絡してください。
AceServer - PIN を選択する必要があります	SmLoginLogoutMessage::Ace-ServerMustChoosePin	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカル サポートに連絡してください。
AceServer :: Sm_Api_Reason_New_PIN_Select	SmLoginLogoutMessage::Sm-ApiNewPinSelectReason	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカル サポートに連絡してください。
AceServer が Sm_Api_Reason_New_PIN_Accepted から返ります	SmLoginLogoutMessage::Sm-ApiSuccessReason	HTML SecurID 認証方式で使用されます。ユーザ PIN がユーザによって正常に変更された場合、このメッセージが表示されます。
AceServer が Sm_AuthApi_Reject Sm_Api_Reason_New_PIN_Accepted を返しますが、不成功のメッセージが表示される可能性があります。ターゲットが不明です。	SmLoginLogoutMessage::Sm-ApiRejectReasonMessage	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカル サポートに連絡してください。
AceSetPasscode = %1s	SmLoginLogoutMessage::Sm-AuthAceSetPassCode	SecurID 認証方式において、ACE 認証のパスコードを ACE/SecurID API を使用して登録しようとしている場合、このメッセージが表示されます。

メッセージ	関数	説明
AceSetPasscode は aceRetVal = %1i で失敗しました	SmLoginLogoutMessage::Ace-SetPasscodeFailed	SecurID 認証方式において、ACE 認証のパスコードを ACE/SecurID API を使用して登録できなかった場合、このエラー メッセージが表示されます。認証方式によってリクエストは拒否されます。
AceSetPin の実行に失敗しました	SmLoginLogoutMessage::Ace-SetPinFailed	HTML SecurID 認証方式において、ACE/SecurID API を使用してユーザ PIN を設定できなかった場合、このエラー メッセージが表示されます。認証方式によってリクエストは拒否されます。
AceSetSelectionCode DECRYPT = %1s	SmLoginLogoutMessage::-SelectioncodeDecrypt	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカル サポートに連絡してください。
AceSetUsername は aceRetVal = %1i で失敗しました	SmLoginLogoutMessage::Ace-SetUserNameFailed	SecurID 認証方式において、ACE 認証のユーザ名を ACE/SecurID API を使用して登録できなかった場合、このメッセージが表示されます。認証方式によってリクエストは拒否されます。
AddCurrentPWToHistory - パスワード履歴情報を設定できません	SmLoginLogoutMes-sage::ErrorSettingPassword-History	最新のパスワードのリストに現在のパスワードを追加できませんでした。
AuthenticateUserDir - ユーザ BLOB データを更新できません	SmLoginLogoutMessage::Blob-UpdateFailed	認証プロセス中にパスワード BLOB データを更新できませんでした。
AceAlphanumeric を取得できません	SmLoginLogoutMessage::Get-AceAlphanumericFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceCancelPin を取得できません	SmLoginLogoutMessage::Get-AceCancelPinFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceCheck を取得できません	SmLoginLogoutMessage::Get-AceCheckFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceClientCheck を取得できません	SmLoginLogoutMessage::Get-AceClientCheckFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。

メッセージ	関数	説明
AceClose を取得できません	SmLoginLogoutMessage::Get-AceCloseFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceGetAuthenticationStatus を取得できません	SmLoginLogoutMessage::Ace-GetAuthenticationStatusFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceGetMaxPinLen を取得できません	SmLoginLogoutMessage::Null-AceGetMaxPinLen	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceGetMinPinLen を取得できません	SmLoginLogoutMessage::Null-AceGetMinPinLen	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceGetPinParams を取得できません	SmLoginLogoutMessage::Get-AcePinParamFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceGetShell を取得できません	SmLoginLogoutMessage::Ace-GetShellFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceGetSystemPin を取得できません	SmLoginLogoutMessage::Ace-GetSystemPinFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceGetTime を取得できません	SmLoginLogoutMessage::Ace-GetTimeFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceGetUserData を取得できません	SmLoginLogoutMessage::Ace-GetUserDataFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceGetUserSelectable を取得できません	SmLoginLogoutMessage::Ace-GetUserSelectable-Fail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceInit を取得できません	SmLoginLogoutMessage::Get-AceInitFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceInitialize を取得できません	SmLoginLogoutMessage::Ace-InitializeFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceLock を取得できません	SmLoginLogoutMessage::Ace-LockFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceSendNextPasscode を取得できません	SmLoginLogoutMessage::Ace-SendNextPasscodeFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceSendPin を取得できません	SmLoginLogoutMessage::Null-AceSendPin	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。

メッセージ	関数	説明
AceSetNextPasscode を取得できません	SmLoginLogoutMessage::Ace-SetNextPasscodeFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceSetPasscode を取得できません	SmLoginLogoutMessage::Ace-SetPasscodeFail	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカル サポートに連絡してください。
AceSetPin を取得できません	SmLoginLogoutMessage::Null-AceSetPin	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceSetUserClientAddress を取得できません	SmLoginLogoutMessage::Ace-SetUserClientAddressFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
AceSetUsername を取得できません	SmLoginLogoutMessage::Ace-SetUsernameFail	ACE クライアント ライブラリ内にメソッドが見つかりませんでした。
aceclnt.dll をロードできません	SmLoginLogoutMessage::Ace-IntDllLoadFail	ACE クライアント ライブラリをロードできませんでした。
パスワード メッセージから新しいパスワードを取得できません	SmLoginLogoutMessage::New-PasswordRetrieveFail	ログイン リクエストの処理中、パスワードを新しいものと古いものに分割しているとき、新しいパスワードを取得できませんでした。
パスワード メッセージから古いパスワードを取得できません	SmLoginLogoutMessage::Old-PasswordRetrieveFail	ログイン リクエストの処理中、パスワードを新しいものと古いものに分割しているとき、古いパスワードを取得できませんでした。
パスワード メッセージからトークンを取得できません	SmLoginLogoutMessage::Token-RetrieveFail	ログイン リクエストの処理中、パスワードを新しいものと古いものに分割しているとき、パスワード トークンを取得できませんでした。
ChangePassword - プロバイダを介してパスワードを変更できません	SmLoginLogoutMessage::Pwd-ChangeFailViaProvider	パスワード変更リクエストの処理中、ユーザ ディレクトリ内のパスワードを変更できませんでした。
ChangePassword - 新しいパスワードを検証できません	SmLoginLogout-Message::ChangePwdValidation-Fail	パスワード変更リクエストの処理中、ユーザ ディレクトリ内のパスワードを検証できませんでした。

メッセージ	関数	説明
CheckPasswordPolicies - パスワード ポリシーの誤設定のため、認証ステータスが「失敗」に変わりました	SmLoginLogout-Message::CheckPwdFailCause-Misconfig	パスワード ポリシーの確認中、ログイン試行を検証できませんでした。パスワード ポリシーが誤設定されている可能性があります。
%1s を削除する変数が見つかりませんでした	SmLoginLogout-Message::VariableFindErrorTo-Delete	セッション変数フラグがセッション変数名の前にリクエストの一部として渡されました。
CSmAuthUser - ChangePassword - ユーザ BLOB データを更新できません	SmLoginLogoutMes-sage::ChangePwdBlobUpdateFail	パスワード変更リクエストの処理中、パスワード BLOB データを更新できませんでした。
DelVariable: 内部エラー: 変数が見つかりませんでした	SmLoginLogoutMessage::Del-VariableFindError	セッション ストアから変数名を削除しようとしたとき、その変数名が空でした。
DelVariable が変数 %2s についてエラー %1i を返しました	SmLoginLogoutMessage::Del-VariableReturnError	セッション ストアからこの変数を削除できませんでした。
AceSetUsername = %1s が設定されませんでした	SmLoginLogoutMessage::Sm-AuthNotSetUserId	SecurID 認証方式において、ACE 認証のユーザ名を ACE/SecurID API を使用して登録できなかった場合、このメッセージが表示されます。認証方式によってリクエストは拒否されます。
削除する変数の名前の検索エラー %1s: 無効なインデックス %2i	SmLoginLogout-Message::VariableNameFind-InvalidIndexError	セッション変数フラグが、空の名前を持つセッション変数のリクエストの一部として渡されました。
方式設定パラメータ lpszServerParam 内にエラーがあります	SmLoginLogoutMessage::Error-SchemeConfigServerParam	SecurID 認証方式で使用されます。同上。
方式設定パラメータ内にエラーがあります: 空の文字列	SmLoginLogoutMessage::Error-SchemeConfigParam	基本的な SecurID 認証方式でも、フォームベースの SecurID 認証方式でも、「ディレクトリ内の ACE ユーザ ID 属性名」パラメータが必要です。このパラメータが見つからないか、間違って設定されている場合、このエラーが表示されます。

メッセージ	関数	説明
方式「%2s」を使用して ユーザ「%1s」を認証 できませんでした。サポートされていない API バージョンです	SmLoginLogoutMessage::User-AuthFail	認証プロバイダ ライブラリのバージョンが古いため、認証できませんでした。
認証レルム「%1s」が見つかりませんでした	SmLoginLogoutMessage::Auth-RealmFindFail	Radius 認証リクエストの処理中、指定されたエージェント/エージェント グループによって保護されているレルムが見つかりませんでした。
FindApplicablePassword ポリシー - ルートのフェッチ エラー	SmLoginLogoutMessage::Error-FetchingApplicablePolicyRoot	ロギング試行の検証中、ルート オブジェクトをフェッチできませんでした。
FindApplicablePassword ポリシー - 適合するパスワード ポリシーの 検索エラー	SmLoginLogoutMessage::Error-FindingMatchingPolicies	ロギング試行の検証中、パスワード ポリシー オブジェクトをフェッチできませんでした。
FindApplicablePassword ポリシー - ユーザ ディレクトリ %1s についてパスワード データ属性 が定義されていません	SmLoginLogout-Message::PasswordDataAttrib-NotDefined	使用しているユーザ ディレクトリで、BLOB の適切な属性が定義されていません。
FindApplicablePassword ポリシー - ユーザまたはディレクトリが NULL です	SmLoginLogoutMessage::Null-ApplicablePwdPolicyDir	ロギング試行の検証中、適用できるパスワード ポリシーを検索しているときにユーザ オブジェクトとディレクトリ オブジェクトが両方とも NULL でした。
GetRandomPassword - 最短長が最大長を超えています	SmLoginLogoutMessage::Long-PwdLength	作成されたランダム パスワードが、許容される最大長を超えています。
GetRedirect - 使用できるパスワード ポリシーが見つかりません	SmLoginLogoutMessage::Error-FindingPasswordPolicy	リダイレクト情報を含む最初の適用可能なパスワード ポリシーを検索しているとき、適切なポリシーが見つかりませんでした。

メッセージ	関数	説明
GetRedirect - パスワード ポリシーを取得できません	SmLoginLogoutMessage::Error-RetrievePasswordPolicy	新しいパスワードの検証中、パスワード ポリシー オブジェクトをフェッチできませんでした。
GetVariable: 内部エラー: DelVar %1s が Var: %2s に一致しません	SmLoginLogoutMessage::Get-VariableMatchError	フェッチされたときに削除される変数が、フェッチ用と削除用に異なる名前を持っています。
GetVariable(Del) が変数 %2s についてエラー %1i を返しました	SmLoginLogoutMessage::Get-VariableDelReturnError	セッション ストアからこの変数を削除できませんでした。
GetVariable(Fetch) が変数 %2s についてエラー %1i を返しました	SmLoginLogoutMessage::Get-VariableFetchReturnError	セッション ストア内にこの変数が見つかりませんでした。
GetVariable: 内部エラー: 変数が見つかりませんでした	SmLoginLogoutMessage::Get-VariableFindError	セッション変数を取得しようとしたとき、変数名が空でした。
SiteMinder が生成したユーザ属性 %1s の形式が無効です	SmLoginLogoutMessage::Invalid-SmUserAttribFormat	アプリケーション ロール ユーザ プロパティの形式に誤りがあります。
新しい PIN が承諾されました = %1s	SmLoginLogoutMessage::New-PinAccepted	HTML SecurID 認証方式で使用されます。ユーザ PIN がユーザによって正常に変更された場合、このメッセージが表示されます。
非標準の SelectionCode = %1s	SmLoginLogoutMessage::Ace-ServerNonStandard-Selectioncode	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカル サポートに連絡してください。
パスコードが割り当てられていません	SmLoginLogout-Message::PasscodeNot-Allocated	SecurID 認証方式で使用されますユーザ パスコード用のバッファが割り当てられていません。
PassCode1 が割り当てられていません	SmLoginLogoutMessage::Mem-AllocPasscode1Fail	SecurID 認証方式で使用されますユーザ パスコード用のバッファが割り当てられていません。
PassCode1 が割り当てられていません	SmLoginLogout-Message::Passcode1Not-Allocated	SecurID 認証方式で使用されます次のユーザ パスコード用のバッファが割り当てられていません。

メッセージ	関数	説明
PassCode1 が確認されていません。 エラー = %1i	SmLoginLogoutMes-sage::PassCode1NotChecked	SecurID 認証方式において、ACE/SecurID API を使用して ACE 認証プロセスを完了できない場合、このエラー メッセージが表示されます。
PassCode1 が設定されていません。 エラー = %1i	SmLoginLogoutMessage::Pass-Code1NotSet	SecurID 認証方式において、ACE 認証のパスコードを ACE/SecurID API を使用して登録しようとしている場合、このメッセージが表示されます。
PassCode1 が設定されていません。 エラー = %1i	SmLoginLogoutMessage::Pass-Code2NotSet	HTML SecurID 認証方式において、ACE 認証の次回のパスコードを ACE/SecurID API を使用して登録できなかった場合、このエラー メッセージが表示されます。認証方式によってリクエストは拒否されます。
PassCode2 が割り当てられていません	SmLoginLogoutMessage::Mem-AllocPasscode2Fail	SecurID 認証方式で使用されますユーザ パスコード用のバッファが割り当てられていません。
PassCode2 が NextPasscode として送信されません。エラー = %1i	SmLoginLogoutMessage::Pass-Code2NotSentAsNextPasscode	HTML SecurID 認証方式において、ACE/SecurID API を使用して次回のパスコードを ACE サーバに送信できなかった場合、このエラー メッセージが表示されます。認証方式によってリクエストは拒否されます。
パスワード メッセージを解析できませんでした	SmLoginLogout-Message::PasswordMessage-ParseFail	ログイン リクエストの処理中、パスワードを新しいものと古いものに分割しているとき、パスワード文字列を解析できませんでした。
PIN の割り当てに失敗しました	SmLoginLogoutMessage::Pin-AllocationFailed	HTML SecurID 認証方式で使用されます。ユーザ PIN 用のバッファが割り当てられていません。

メッセージ	関数	説明
pszBuf の割り当てに失敗しました	SmLoginLogoutMessage:pszBuf-AllocFail	SecurID 認証方式で使用されます SiteMinder ユーザ ディレクトリ内のユーザ ID 属性名 RSA SecurID 用のバッファが割り当てられていません。
暗号化されたシステム PIN が UserMsg 経由の Cookie で返ります	SmLoginLogoutMes-sage::ReturningEncrypted-SystemPin	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカル サポートに連絡してください。
SelectionCode が割り当てられていません	SmLoginLogout-Message::SelectionCodeNot-Allocated	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカル サポートに連絡してください。
方式「%2s」を使用してユーザ「%1s」を認証しているときに、サーバ例外が発生しました	SmLoginLogoutMessage::User-AuthException	認証プロセス中、不明なエラーが発生しました。認証プロバイダ ライブラリ内が最も可能性が高いと思われます。
ユーザ「%1s」の認証を検証しているときに、 サーバ例外が発生しました	SmLoginLogoutMessage::Valid-AuthException	認証プロセス中にコールされたとき、高度なパスワード サービス共有ライブラリ内でエラーが発生しました。
ユーザ名の設定エラー = %1i	SmLoginLogoutMessage::Set-UserNameError	SecurID 認証方式において、ACE 認証のユーザ名を ACE/SecurID API を使用して登録できなかった場合、このメッセージが表示されます。認証方式によってリクエストは拒否されます。
SetVariable: 内部 エラー: 変数が見つかりませんでした	SmLoginLogoutMessage::Set-VariableFindError	セッション ストア内に変数名を設定しようとしたとき、その変数名が空でした。
SetVariable: 内部エラー: 変数 %1s について NULL の値が見つかりました	SmLoginLogoutMessage::Set-VariableNullValueFound	セッション ストア内に変数値を設定しようとしたとき、その変数値が空でした。

メッセージ	関数	説明
SetVariable が変数 %2s について エラー %1i を返しました	SmLoginLogoutMessage::Set-VariableReturnError	この変数をセッション ストアに対して追加または更新できませんでした。
SmAuthenticate: AceInitialization に失敗しました	SmLoginLogoutMessage::Sm-AuthAceInitFail	ACE クライアント ライブラリを初期化できませんでした。
SmAuthenticate: イベントを作成できません	SmLoginLogoutMessage::Create-EventFail	SecurID 認証方式で使用されます SecurID 認証方式でイベント オブジェクトが作成されていません。
SmAuthenticate: PIN 用のメモリを割り当てることができませんでした	SmLoginLogoutMessage::Sm-AceHtmlPinMemAllocFail	SecurID 認証方式で使用されます ACE システムによって生成される PIN 用のバッファが割り当てられていません。
SmAuthenticate: AceSetPasscode = %1s が設定されませんでした	SmLoginLogoutMessage::Sm-AuthAceDidNotSetPassCode	SecurID 認証方式において、ACE 認証のパスコードを ACE/SecurID API を使用して登録できなかった場合、このエラー メッセージが表示されます。認証方式によってリクエストは拒否されます。
SmAuthenticate: SM_ACE_FAILOVER_ATTEMPTS 環境変数用の数値が見つかりませんでした。デフォルト値を使用します	SmLoginLogoutMessage::Zero-SmAuthAceFailover	RSA ACE/SecurID フェイルオーバーをサポートするため、SiteMinder ポリシー サーバには環境変数 SM_ACE_FAILOVER_ATTEMPTS があります。この変数はデフォルトで 3 に設定されます。 SM_ACE_FAILOVER_ATTEMPTS の値が 0 である場合、このエラー メッセージが表示されます。この場合、SiteMinder で RSA ACE/SecurID フェイルオーバーが正常に動作しない可能性があります。
SmAuthenticate: EventData 用のストレージを割り当てることができません	SmLoginLogoutMessage::Event-DataMemAllocFail	SecurID 認証方式で使用されます RSA SecurID API 構造体用のメモリが割り当てられていません。

メッセージ	関数	説明
SmAuthenticate: AceInit に進むことができません -- ACE 処理ではありません。 aceRetVal= %1i	SmLoginLogoutMessage::Sm-AuthAceInitProcessingFail	SecurID 認証方式において、ACE/SecurID API を初期化できなかった場合、このメッセージが表示されます。認証方式でリクエストは拒否され、認証は失敗します。
SmAuthenticate: AceCheck に進みませんでした。 aceRetVal= %1i	SmLoginLogoutMessage::Sm-AuthAceCheckDidNotContinue	SecurID 認証方式において、ACE/SecurID API を使用して ACE 認証プロセスを完了できない場合、このエラー メッセージが表示されます。
SmAuthenticate: AceInit 完了に進みませんでした。 pEventData->asynchAceRet= %1i	SmLoginLogoutMessage::Sm-AuthAceInitCompletionFail	SecurID 認証方式において、ACE/SecurID API を初期化できなかった場合、このメッセージが表示されます。認証方式でリクエストは拒否され、認証は失敗します。
SmAuthenticate: ACE/Server の通信障害によって、名前ロック リクエストが拒否されました	SmLoginLogoutMessage::Sm-AuthNameLockReqDenied	SecurID 認証方式において、ACE/SecurID API を初期化できなかった場合、このメッセージが表示されます。認証方式でリクエストは拒否され、認証は失敗します。
SmAuthenticate: スレッドの同期に失敗しました。 wRet= %1ul	SmLoginLogoutMessage::Sm-AuthThreadSyncFail	Windows プラットフォームの SecurID 認証方式において、非同期 ACE API コールに失敗した場合、このメッセージが表示されます。
SmAuthenticate: ユーザ名をロックできません。 aceRetVal= %1i	SmLoginLogoutMessage::Sm-AuthUserNameLockFail	SecurID 認証方式において、ACE サーバのユーザ名をロックできなかった場合、このメッセージが表示されます。この場合、SiteMinder の認証方式で認証リクエストは拒否されます。名前ロック機能は、RSA ACE 製品のバージョン 5.0 以上で使用できます。名前ロック機能の詳細については、RSA ACE 製品のマニュアルを参照してください。

メッセージ	関数	説明
SmAuthUser - 許可レルムをフェッチできませんでした	SmLoginLogoutMessage::Fetch-AzRealmFailed	アプリケーション ロール ユーザ プロパティを取得しているとき、ユーザのレルムが見つかりませんでした。
SmAuthUser - ドメイン オブジェクトをフェッチできませんでした。	SmLoginLogoutMessage::Fetch-DomainObjFailed	アプリケーション ロール ユーザ プロパティを取得しているとき、ユーザのドメインが見つかりませんでした。
新しい PIN に使用できるのは英数字のみです	SmLoginLogoutMessage::Alpha-NumericOnlyNewPin	HTML SecurID 認証方式において、ユーザが PIN の変更を要求されたときに英数字以外の文字を含む PIN を入力した場合、このメッセージが表示されます。
新しい PIN に使用できるのは数字のみです	SmLoginLogoutMessage::Digit-OnlyNewPin	HTML SecurID 認証方式において、ユーザが PIN の変更を要求されたときに数字が含まれない PIN を入力した場合、このメッセージが表示されます。
新しい PIN が長すぎます	SmLoginLogoutMessage::Long-NewPin	HTML SecurID 認証方式において、ユーザが PIN の変更を要求されたときに新しい PIN が長すぎる場合、このメッセージが表示されます。
新しい PIN が短すぎます	SmLoginLogoutMessage::Short-NewPin	HTML SecurID 認証方式において、ユーザが PIN の変更を要求されたときに新しい PIN が短すぎる場合、このメッセージが表示されます。
PIN の変更を続行できません。不明な PIN タイプです	SmLoginLogoutMessage::Ace-ServerUnableToProceedPin-Change	情報のみ。ACE/SecurID 認証方式で問題が発生している場合は、このメッセージをテクニカル サポートに連絡してください。
SmPasswordMsg_Change の検索中、予期しないメッセージ ID が見つかりました。 パスワード: %1ul	SmLoginLogout-Message::UnexpectedMessage-ID	ログイン リクエストの処理中、パスワードを新しいものと古いものに分割しているとき、パスワード フィールドに格納されているメッセージ ID が不明でした。

メッセージ	関数	説明
構文: %1s[:AppName]	SmLoginLogoutMessage::Usage-SmUserAttribFormat	アプリケーション ロール ユーザ プロパティの正しい書式設定を補助する文字列です。
UserPIN が割り当てられていません	SmLoginLogoutMessage::User-PinNotAllocated	SecurID 認証方式で使用されますユーザ PIN 用のバッファが割り当てられていません。
ValidateLoginAttempt - パスワード ポリシーの適用エラー	SmLoginLogoutMessage::Error-ApplyingPasswordPolicy	ロギング試行の検証中、パスワード ポリシーを適用できませんでした。
ValidateLoginAttempt - パスワード ポリシーのフェッチ エラー	SmLoginLogoutMessage::Error-FetchingPasswordPolicy	ロギング試行の検証中、パスワード ポリシー オブジェクトをフェッチできませんでした。
ValidateLoginAttempt - 使用できるパスワード ポリシーの検索エラー	SmLoginLogoutMessage::Error-FindingApplicablePolicy	ロギング試行の検証中、使用できるポリシーが見つかりませんでした。
ValidateNewPassword - パスワード変更情報を設定できません	SmLoginLogoutMessage::Error-PasswordChange	パスワード BLOB データを更新しようとしているときに、パスワード情報を設定できませんでした。
ValidateNewPassword - 一致正規表現のフェッチ エラー	SmLoginLogoutMessage::Match-ExprFetchError	パスワード ポリシーに必要な正規表現を取得できませんでした。
ValidateNewPassword - 不一致正規表現のフェッチ エラー	SmLoginLogoutMessage::No-MatchExprFetchError	パスワード ポリシーに必要な正規表現を取得できませんでした。
ValidateNewPassword - パスワード ポリシーのフェッチ エラー	SmLoginLogoutMessage::Err-FetchingValidPwdPolicy	新しいパスワードの検証中、パスワード ポリシー オブジェクトをフェッチできませんでした。
ValidateNewPassword - 使用できるパスワード ポリシーの検索エラー	SmLoginLogoutMessage::Err-FindingValidPwdPolicy	新しいパスワードの検証中、適用できるポリシーが見つかりませんでした。
ValidateNewPassword がコールアウト「%1s」をロードできませんでした	SmLoginLogoutMessage::Load-CalloutFail	パスワードを確認するための外部ライブラリをロードできませんでした。
ValidateNewPassword が「%2s」内の関数「%1s」を解決できませんでした。エラー: %3s	SmLoginLogoutMessage::Err-ResolveFuncValidPwd	パスワードを確認するための外部ライブラリ内にメソッドが見つかりませんでした。

許可

エラー メッセージ	関数	説明
不正な %1s リクエストが検出されました	SmIsAuthorizedMessage::Bad-RequestDetected	許可リクエスト メッセージが適切な形式に準拠していませんでした。
ライセンスされた eTelligent なしでは変数を含むアクティブな式を処理できません	SmIsAuthorizedMessage::CanNot-ProcessActiveExpr	eTelligent ルール機能のライセンスが見つかりませんでした。アクティブな式は処理されません。
変数の追加中に例外がキャッチされました	SmIsAuthorizedMessage::Exc-AddingVar	eTelligent ルール変数の解決中、ソフトウェア例外が発生しました。
IsOk で例外が発生しました。	SmIsAuthorizedMessage::Unk-ExcInIsOK	許可の実行中、不明の例外が発生しました。
IsOk で例外が発生しました。%1s	SmIsAuthorizedMessage::ExcIn-IsOK	許可の実行中、例外が発生しました。
アクティブな式 %1s をロードできませんでした	SmIsAuthorizedMessage::Failed-FetchActiveExpr	オブジェクト ストアからアクティブな式オブジェクトをフェッチできませんでした。
アクティブな式 %1s をロードできませんでした	SmIsAuthorizedMessage::Failed-LoadActiveExpr	アクティブな式をロードできませんでした。
ドメイン %1s をロードできませんでした	SmIsAuthorizedMessage::Failed-LoadDomain	eTelligent ルール変数の処理中、ドメイン オブジェクトを取得できませんでした。
変数 %1s をロードできませんでした	SmIsAuthorizedMessage::Failed-LoadVar	指定された eTelligent ルール変数を取得できませんでした。
変数タイプ %1s をロードできませんでした	SmIsAuthorizedMessage::Failed-LoadVarType	指定された変数のタイプを取得できませんでした。
アクティブな式 %1s の変数をロードできませんでした	SmIsAuthorizedMessage::Failed-LoadVarActiveExpr	変数の解決で問題が発生したため、アクティブな式は呼び出されません。

エラー メッセージ	関数	説明
アクティブな式 %1s の変数をロードできませんでした	SmIsAuthorizedMessage::Failed-LoadVarsForActiveExpr	アクティブな式の eTelligent ルール変数をロードできませんでした。
属性 %1s を解決できませんでした	SmIsAuthorizedMes-sage::FailedToResolveAttr	オブジェクト ストアからレスポンス属性オブジェクトをフェッチできませんでした。
ディクショナリ ベンダー属性 %1s を解決できませんでした	SmIsAuthorizedMes-sage::FailedToResolveDictVendAttr	指定されたベンダー属性がベンダー属性ディクショナリ内に見つかりませんでした。
レスポンス %1s を解決できませんでした	SmIsAuthorizedMes-sage::FailedToResolveResponse	オブジェクト ストアからレスポンス オブジェクトをフェッチできませんでした。
レスポンス グループ %1s を解決できませんでした	SmIsAuthorizedMes-sage::FailedToResolveResponseGp	オブジェクト ストアからレスポンス グループ オブジェクトをフェッチできませんでした。
ユーザ ポリシー %1u を解決できませんでした	SmIsAuthorizedMes-sage::FailedToResolveUserPolicy	オブジェクト ストアからユーザ ポリシー オブジェクトをフェッチできませんでした。
変数レスポンスを無視します - eTelligent オプションのライセンスがありません	SmIsAuthorizedMessage::No-eTelligentLicense	eTelligent ルール機能のライセンスが見つかりませんでした。変数は処理されません。
レスポンス属性 %1s が無効ですディクショナリの競合 - 属性がレスポンスにない可能性があります	SmIsAuthorizedMessage::Invalid-ResponseAttr	無効なレスポンス属性が許可レスポンスに含まれていませんでした。
IsOk に失敗しました。%1s	SmIsAuthorizedMessage::IsOK-Failed	許可を確認できませんでした。

サーバ

メッセージ	関数	説明
TCP サーバ ソケットを初期化できませんでした: ソケット エラー: %1i	SmServerMessage::TCP-ServerSocketInitFail	ソケット エラーの詳細については、オペレーティング システムのマニュアルを参照してください（最も一般的なエラーとして、システム上ですでに使用されているソケットを開こうとする場合や、ソケットに対する十分な権限がない場合が挙げられます）。
ポート %1ul 上の UDP サーバ ソケットを初期化できませんでした。ソケット エラー: %2i	SmServerMessage::UDP-ServerSocketInitFailOnPort	ソケット エラーの詳細については、オペレーティング システムのマニュアルを参照してください（最も一般的なエラーとして、システム上ですでに使用されているソケットを開こうとする場合や、ソケットに対する十分な権限がない場合が挙げられます）。
WinSock ライブラリを初期化できませんでした	SmServerMessage::WinSock-LibInitFail	（Windows システム）Windows Sockets Library を初期化できませんでした。ライブラリがインストールされていることと、そのバージョンがサポートされていることを確認してください。
TCP サーバ ソケットでリスンできませんでした。ソケット エラー%1i	SmServerMessage::TCP-ServerSocketListenFail	ソケット エラーの詳細については、オペレーティング システムのマニュアルを参照してください（最も一般的なエラーとして、システム上ですでに使用されているソケットを開こうとする場合や、ソケットに対する十分な権限がない場合が挙げられます）。
イベント ハンドラをロードできませんでした	SmServerMessage::Event-HandlerLoadFail	イベント ハンドラ ライブラリをロードできませんでした。設定されたイベント ハンドラのパス名とアクセス権限を確認してください。

メッセージ	関数	説明
ライブラリ「%1s」をロードできませんでした。 エラー : %2s	SmServerMessage::FailedTo-LoadLib	レポートされた認証方式ライブラリをロードできませんでした。表示されるエラー テキストの中に問題に関する説明がない場合は、指定されたライブラリが存在することと、ファイル システムの保護でアクセスが許可されていることを確認してください。
イベント プロバイダ「%1s」内で必要なエントリ ポイントを特定できませんでした	SmServerMessage::Req-EntryPointInEventProvider-LocateFail	指定されたライブラリは有効なイベント/監視ログ プロバイダではありません。
監査ログ レコードを書き込めませんでした。レコードは破棄されました	CSmReports::LogAccess	ポリシー サーバから監査ログに書き込めませんでした。監査ログ ストアのステータスを確認してください。
ホスト名を取得できませんでした。ソケット エラー %1i	SmServerMessage::Host-NameObtainError	監査ロガー プロバイダが、ネットワーク エラーと思われる原因により、ローカル システムのネットワーク ホスト名を取得できませんでした。表示されるエラー コード（UNIX システムの場合は errno、Windows システムの場合は SOCKET_ERROR）によって、詳細が示される場合があります。
ホスト名を取得できませんでした。ソケット エラー %1i	SmServerMessage::Host-NameObtainFail	ネットワーク エラーと思われる原因により、ローカル システムのネットワーク ホスト名を取得できませんでした。表示されるエラー コード（UNIX システムの場合は errno、Windows システムの場合は SOCKET_ERROR）によって、詳細が示される場合があります。

メッセージ	関数	説明
「%1s」を追加する監査ログ ファイルを開けませんでした	SmServerMessage::Audit-LogFileAppendFail	監査ロガー プロバイダが、エントリ追加のための指定されたファイルを開くことができませんでした。指定したパス名が有効であることと、ファイル アクセス権限が正しいことを確認してください。
RADIUS ログ ファイルを開けませんでした(ファイルが定義されていません)	SmServerMessage::Radius-LogFileNotDefined	RADIUS ログ ファイルの名前のエントリがレジストリにないか、名前が空の文字列です。
RADIUS ログ ファイルを開けませんでした: %1s	SmServerMessage::Radius-LogFileOpenFail	指定された名前を持つ RADIUS ログ ファイルを、上書き用に開くことができなかったか(すでに存在する場合)、作成できませんでした(存在しない場合)。ディレクトリとファイル(存在する場合)に対するアクセス権限を確認してください。。
認証方式「%1s」を照会できませんでした	SmServerMessage::Fail-QueryAuthScheme	指定された認証方式に対するポリシー サーバのクエリが失敗したため、認証方式を初期化できませんでした。
UDP ソケット上での読み取りに失敗しました。ソケット エラー %1i	SmServerMessage::UDP-SocketReadFail	ポリシー サーバで、管理サービス接続リクエストまたは RADIUS メッセージのいずれかを伝送する UDP パケットを読み取ろうとしているときに、予期しないネットワーク エラーが検出されました。表示されるエラー コード(UNIX システムの場合は errno、Windows システムの場合は SOCKET_ERROR)によって、詳細が示される場合があります。

メッセージ	関数	説明
セッション番号 %1i のリクエストを受信できませんでした: %2s/%3s: %4i。ソケット エラー %5s	SmServerMessage::Request-ReceiveOnSessionFail	ポリシー サーバで、指定されたセッションのエージェント リクエストを読み取ろうとしているときに、予期しないネットワーク エラーが検出されました。そのため、接続は閉じられました。表示されるエラー コード (UNIX システムの場合は errno、Windows システムの場合は SOCKET_ERROR) によって、詳細が示される場合があります。
エージェント キー「%1s」を解決できませんでした	SmServerMessage::Unresolved-AgentKey	エージェント キーの更新中、レポートされたエージェント キーがポリシー ストア内に見つかりませんでした。
エージェント キーを解決できませんでした	SmServerMessage::FailTo-ResolveAgentKeys	エージェント キー更新用のポリシー ストアの中に、アクセスできるエージェント キーがありませんでした。
エージェント キーを解決できませんでした	SmServerMessage::Agent-KeysResolveFail	エージェント キー更新用のポリシー ストアの中に、アクセスできるエージェント キーがありませんでした。
エージェント キー「%1s」を解決できませんでした	SmServerMessage::Fail-ToResolveAgentKey	エージェント キーの更新中、レポートされたエージェント キーがポリシー ストア内に見つかりませんでした。
エージェントまたはエージェント グループ %1s を解決できませんでした	SmServerMessage::Agent-OrAgentGroupResolveFail	指定されたエージェントまたはエージェント グループが存在しないか、そのポリシー ストア レコードが破損しています。
すべてのドメインを解決できませんでした	SmServerMessage::Domain-ResolutionFailed	ポリシー ストア内のドメイン ルート オブジェクト レコードが、見つからないか、破損しています。

メッセージ	関数	説明
すべてのベンダーを解決できませんでした。 ベンダー ディクショナリは作成されません	SmServerMessage::Failed-ToResolveVendors	ポリシー ストア内のベンダー ルート オブジェクト レコードが、見つからないか、破損しています。
認証/許可マッピング %1s を解決できませんでした	SmServerMessage::Fail-ToResolveAuthAzMap	指定された認証/許可マップが存在しないか、そのポリシー ストア レコードが破損しています。
「%2s」内の関数「%1s」を解決できませんでした。エラー: %3s	SmServerMessage::Failed-ToResolveFunc	指定された認証方式ライブラリ内のレポートされたエントリ ポイントを解決できませんでした(表示されるエラー テキストを参照)。そのため、ライブラリはロードされませんでした。
「%2s」内の関数「%1s」を解決できませんでした。エラー: %3s	SmServerMessage::Function-ResolveFail	指定された TransactEMS ライブラリ内のレポートされたエントリ ポイントを解決できませんでした(表示されるエラー テキストを参照)。そのため、ライブラリはロードされませんでした。
「%2s」内の関数「%1s」を解決できませんでした。エラー: %3s	SmServerMessage::Fail-ToResolveFunction	システム設定情報をレポートする指定のライブラリ内のレポートされたエントリ ポイントを解決できませんでした(表示されるエラー テキストを参照)。そのため、ライブラリはロードされませんでした。
保存できませんでした	SmServerMessage::Key-ManagementObjResolveFail	ポリシー サーバで、キー管理オブジェクトをポリシー ストアから読み取ろうとしたとき、エラーが検出されました。
キー管理オブジェクトを解決できませんでした	SmServerMessage::Resolve-KeyMgmtObjFail	エージェント キー管理オブジェクトをポリシー ストアから読み取ることができませんでした。

メッセージ	関数	説明
キー管理オブジェクト「%1s」を解決できませんでした	SmServerMessage::Key-ManagementObjResolve-FailwithVal	エージェント キー管理スレッドで、指定されたキー管理オブジェクトをポリシー ストアから読み取ろうとしたとき、エラーが検出されました。
認証/許可マッピングのリストを解決できませんでした	SmServerMessage::Fail-ToResolveAuthAzMapList	ポリシー ストア内の認証/許可マップ ルート オブジェクト レコードが、見つからないか、破損しています。
ログ ファイル名を解決できませんでした	SmServerMessage::Log-FileNameRosolveFail	監査ロガー プロバイダが、ログ ファイルの名前をレジストリから取得できませんでした。ファイル名が設定されていることを確認してください。
共有秘密キー ポリシー オブジェクトを解決できませんでした	SmServerMessage::Shared-SecretResolveFail	ポリシー ストア内の共有秘密キーのロールオーバー ポリシー オブジェクト レコードが、見つからないか、破損しています。
ユーザ ディレクトリ %1s を解決できませんでした	SmServerMessage::Fail-ToResolveUserDir	指定されたユーザ ディレクトリ オブジェクトが存在しないか、そのポリシー ストア レコードが破損しています。
ユーザ識別情報を解決できません。アクセスを拒否します	SmServerMessage::User-IdentityFail	適用可能なレルムのポリシーを検索しているときにエラーが発生したため、ユーザの識別情報を解決できず、アクセスが拒否されました。
「%2s」内のバージョン 6 関数「%1s」を解決できませんでした。エラー : %3s	SmServerMessage::Failed-ToResolveVer6Func	指定されたバージョン 6 認証方式ライブラリ内のレポートされたエントリ ポイントが見つかりませんでした（表示されるエラー テキストを参照）。そのため、ライブラリは使用されません。認証方式のバージョンが古くないことを確認してください。

メッセージ	関数	説明
監査ログのクリア間隔を取得できませんでした。無制限に設定します	SmServerMessage::Audit-LogFlushIntervalRetrieveFail	監査ロガー ODBC プロバイダは、クリアの間隔をレジストリから取得できませんでした。間隔が設定されていることを確認してください。
ネームスペース「%1s」の監査ログ プロバイダ ライブラリを取得できませんでした	SmServerMessage::AuditLog-ProviderLibRetrieveFail	指定された監査ログ プロバイダ ネームスペースのライブラリ名エントリがレジストリにありません。
監査ログのクリア行数を取得できませんでした。1000 に設定します	SmServerMessage::Audit-LogRowFlushCountRetrieveFail	ODBC 監査ログ プロバイダの非同期ロギングでの行のクリア数のエントリがレジストリにありません。そのため、デフォルトの 1000 が使用されます。
メッセージ キューからメッセージを取得できませんでした	SmServerMessage::Retrieve-FromMessageQueueFail	(Windows)ポリシー サーバ プロセスがその Windows アプリケーション キューに関するメッセージを取得しようとしたとき、エラーが発生しました。
トラステッド ホストの共有秘密キーをロールオーバーできませんでした	SmServerMessage::Trusted-HostSharedSecretsRolloverFail	トラステッド ホストの共有秘密キーをロールオーバーしようとしたとき、エラーが発生しました。ロールオーバー ポリシーが有効であることを確認してください。
キー管理オブジェクトを保存できませんでした	SmServerMessage::Save-NewMgmtKeyObjFail	新しい永続キーを保存することになっていたとき、エージェント キー管理オブジェクトをポリシー ストアから読み取ることができませんでした。
キー更新の後、キー管理オブジェクトを保存できませんでした	SmServerMessage::Save-NewMgmtKeyObjAfter-KeyUpdateFail	ポリシー サーバで、ロールオーバー用の新しいエージェント キーが生成されましたが、それらのキーが使用可能であることを記録できませんでした。

メッセージ	関数	説明
永続キー更新の後、キー管理オブジェクトを保存できませんでした	SmServerMessage::Save-NewMgmtKeyObjAfter-PersistentKeyUpdateFail	新しい永続キーを、ポリシー ストアのエージェント キー管理オブジェクト内に保存できませんでした。
セッション キー更新の後、キー管理オブジェクトを保存できませんでした	SmServerMessage::Save-NewMgmtKeyObjAfterSession-KeyUpdateFail	新しいエージェント セッション キーをポリシー ストア内に保存できませんでした。
新しい永続エージェント キー「%1s」を保存できませんでした	SmServerMessage::Save-NewCurrentAgentKeyFail	指定されたエージェント セッション キーを、エージェントの「現在の」キーとして保存できませんでした。
新しいキー管理オブジェクトを保存できませんでした	SmServerMessage::Agent-KeyManagementObjSaveFail	エージェント キー管理スレッドで、ロールオーバー用の新しいエージェント キーが生成されましたが、それらのキーが使用可能であることを記録できませんでした。
新しい「最後の」エージェント キー「%1s」を保存できませんでした	SmServerMessage::Save-NewLastAgentKeyFail	指定されたエージェント セッション キーを、エージェントの「最終」キーとしてポリシー ストア内に保存できませんでした。
新しい「次の」エージェント キー「%1s」を保存できませんでした	SmServerMessage::Save-NewNextAgentKeyFail	指定されたエージェント セッション キーを、エージェントの「次回」キーとしてポリシー ストア内に保存できませんでした。
新しい永続エージェント キー「%1s」を保存できませんでした	SmServerMessage::Failed-ToSaveNewPersistentAgentKey	指定された永続エージェント キーをポリシー ストア内に保存できませんでした。

メッセージ	関数	説明
セッション番号 %1i でレスポンスを送信できませんでした: %2s/%3s: %4i。ソケット エラー %5i	SmServerMessage::Response-SendOnSessionFail	ネットワーク エラー(あるいはエージェントの障害)が原因で、指定されたセッションでのエージェント リクエストに対するレスポンスを送信できませんでした。表示されるエラー コード(UNIX システムの場合は errno、Windows システムの場合は SOCKET_ERROR)によって、詳細が示される場合があります。
エージェント コマンド管理のウォッチドッグ スレッドを開始できませんでした	SmServerMessage::Agent-CommandManagementThread-CreationFail	エージェント コマンド管理スレッドが実行されることを保証する「ウォッチドッグ」スレッドが開始されませんでした。オペレーティング システムで設定されている、スレッドの最大数およびオープン ファイル記述子の最大数の、プロセスあたりの制限を確認してください。
ジャーナル管理スレッドを開始できませんでした	SmServerMessage::Journal-ThreadCreateFail	「ウォッチドッグ」スレッドが、ポリシー ストア ジャーナル クリーンアップ管理スレッドを開始(再開)できませんでした。オペレーティング システムで設定されている、スレッドの最大数およびオープン ファイル記述子の最大数の、プロセスあたりの制限を確認してください。
ジャーナル管理ウォッチドッグ スレッドを開始できませんでした	SmServerMessage::Journal-ManagementThreadFail	ポリシー ストア ジャーナル クリーンアップ管理スレッドが実行されることを保証する「ウォッチドッグ」スレッドが開始されませんでした。オペレーティング システムで設定されている、スレッドの最大数およびオープン ファイル記述子の最大数の、プロセスあたりの制限を確認してください。

メッセージ	関数	説明
キー管理スレッドを開始できませんでした	SmServerMessage::AgentKey-ThreadCreateFail	「ウォッチドッグ」スレッドがエージェント キー管理スレッドを開始（再開）できませんでした。オペレーティング システムで設定されている、スレッドの最大数およびオープン ファイル記述子の最大数の、プロセスあたりの制限を確認してください。
キー管理ウォッチドッグ スレッドを開始できませんでした	SmServerMessage::Key-ManagementThreadCreateFail	エージェント キー管理スレッドが実行されることを保証する「ウォッチドッグ」スレッドが開始されませんでした。オペレーティング システムで設定されている、スレッドの最大数およびオープン ファイル記述子の最大数の、プロセスあたりの制限を確認してください。
メイン応答スレッドを開始できませんでした	SmServerMessage::Main-ReactorThreadStartFail	ネットワーク IO ディスパッチャ スレッドが開始されませんでした。オペレーティング システムで設定されている、スレッドの最大数およびオープン ファイル記述子の最大数の、プロセスあたりの制限を確認してください。
オブジェクト ストア ジャーナル スレッドを開始できませんでした	SmServerMessage::Journal-StartFailed	「ウォッチドッグ」スレッドが、ポリシー ストア ジャーナル管理スレッドを開始（再開）できませんでした。オペレーティング システムで設定されている、スレッドの最大数およびオープン ファイル記述子の最大数の、プロセスあたりの制限を確認してください。

メッセージ	関数	説明
オブジェクト ストア ウォッチドッグ スレッドを開始できませんでした	SmServerMessage::Watchdog-Failed	ポリシー ストア ジャーナル管理スレッドが実行されることを保証する「ウォッチドッグ」スレッドが開始されませんでした。オペレーティング システムで設定されている、スレッドの最大数およびオープン ファイル記述子の最大数の、プロセスあたりの制限を確認してください。
管理コマンド チャネルを開始できませんでした	SmServerMessage::Stat-MangmCmdChannelFail	(UNIX/Linux) 既存のサーバ コマンド管理パイプ/ファイルの stat () が、予期せずに失敗しました。サーバ コマンド管理スレッドも開始されない場合は、他のポリシー サーバ プロセスが実行されていないことを確認し、パイプ/ファイルを手動で削除してください。
エージェント キーを更新できませんでした	SmServerMessage::FailTo-UpdateAgentKeys	キーがエージェントによって更新される管理者コマンドをポリシー ストア内に保存できませんでした。
サーバ コマンドからエージェント キーを更新できませんでした	SmServerMessage::Failed-ToUpdateAgentKeys	エージェントの新しい「現在の」セッション キーまたは「次の」セッションキーを、ポリシー ストア内に保存できませんでした。
エージェント キーへの変更を更新できませんでした	SmServerMessage::Fail-ToUpdateChangesToAgentKeys	キーがエージェントによって更新されるコマンドをポリシー ストア内に保存できませんでした。
永続キーを更新できませんでした	SmServerMessage::Failed-ToUpdatePersistentKey	エージェントの永続キーをポリシー ストア内に保存できませんでした。

メッセージ	関数	説明
UDP ソケット上での書き込みに失敗しました。ソケット エラー %1i	SmServerMessage::UDP-Socket WriteFail	ネットワーク エラー（あるいはエージェントの障害）が原因で、管理 GUI 初期化パケットまたは RADIUS レスポンス パケットを送信できませんでした。表示されるエラー コード（UNIX システムの場合は errno、Windows システムの場合は SOCKET_ERROR）によって、詳細が示される場合があります。
ファイルが見つかりません	SmServerMessage::File-NotFound	（Windows システム）ワンビュー モニターを開始するサービスが、bin¥smmon.bat ファイルを読み取ることができませんでした。
プロセッサ アフィニティを取得できませんでした	SmServerMessage::Get-ProcessorAffinityFail	（Windows）プロセッサ アフィニティのパフォーマンス調整パラメータを処理できませんでした。したがって、既存のアフィニティ設定は変更されません。
ハンドシェイク エラー：hello メッセージ内に不明のクライアント名「%1s」があります	SmServerMessage::Handshake-ErrorUnknownClient	クライアントからの接続試行時、レポート済みの名前が指定されましたが、その名前を持つエージェントはポリシー ストア内に見つかりませんでした。また、エージェントが間違ったに共有秘密キーを使用していることも原因です。
エージェント キー マーカー（%1i）が一致していません	SmServerMes-sage::Inconsistent Agent-KeyMarker	ポリシー ストア内のエージェント キー レコードに、指定された、未承認のキー タイプがあります。
エージェント キーの数（%1i）が一致していません	SmServerMes-sage::Inconsistent NumberOf-AgentKeys	ポリシー ストア内に、エージェント用に指定された不正な数のキーがあります。

メッセージ	関数	説明
レルム リスト計算時の内部エラー。アクセスを拒否します	SmServerMessage::Realm-Corrupt	レルム リストをフェッチしてアクセス許可を実行しようとしたとき、予期しないポリシー ストア障害が発生したため、アクセスは拒否されました。
エージェント キー マーカー (%1i) が不正です	SmServerMessage::Invalid-AgentKeyMarker	ポリシー ストア内のエージェント キー レコードに、指定された、未承認のキー タイプがあります。
IP アドレス リソース フィルタが IsOk によってまだサポートされていません	SmServerMessage::IPAddr-ResourceFilterNotSupported	レルム内のアクション ルールが一致しても、IP アドレスまたは範囲の照合はサポートされません。
IsInDictionary - パスワード ディクショナリをホルダ %1s に追加できませんでした	SmServerMessage::Add-PasswordDictToHolderFailed	指定されたパスワード ディクショナリをキャッシュできませんでした。100 を超えるディクショナリをキャッシュできません。ディクショナリ内のエントリに対して照合されるパスワードは、一致するものと見なされます。
IsInDictionary - パスワード ディクショナリ %1s を作成できませんでした	SmServerMessage::Create-PasswordDictFailed	指定されたパスワード ディクショナリをキャッシュする準備をしているときに、予期しないエラー (おそらくはメモリ不足) が発生しました。ディクショナリ内のエントリに対して照合されるパスワードは、一致するものと見なされます。
IsInDictionary - パスワード ディクショナリ %1s を設定できませんでした	SmServerMessage::Set-PasswordDictFailed	指定されたパスワード ディクショナリをキャッシュしているときに、エラーが発生しました。ディクショナリ内のエントリに対して照合されるパスワードは、一致するものと見なされます。

メッセージ	関数	説明
IsInDictionary - パスワード ディクショナリ %1s が開いていません	SmServerMessage::Open-PasswordDictFailed	指定されたパスワード ディクショナリはロードされましたが、予期せず開かれていません。ディクショナリ内のエントリに対して照合されるパスワードは、一致しないものと見なされます。
IsInProfileAttributes - プロパティ名のフェッチ エラー	SmServerMessage::Fetching-PropertyNameFail	パスワードをユーザ プロファイル属性値と比較しているとき、ユーザ属性名を取得できませんでした。そのため、パスワードは一致するものと見なされます。
IsInProfileAttributes - プロパティ値のフェッチ エラー	SmServerMessage::Fetching-PropertyValueFail	パスワードをユーザ プロファイル属性値と比較しているとき、属性値を取得できませんでした。そのため、パスワードは一致するものと見なされます。
未記録データの監視リクエスト、Null 値が返されました	SmServerMessage::MonReq-UnrecordedDataNullValue	ポリシー サーバは、監視対象データのリクエストで渡された名前を認識しませんでした。
エージェント暗号化キーが見つかりませんでした	SmServerMessage::Agent-EncryptionKeyNotFound	エージェントのキー セットをポリシー ストアからフェッチしたとき、完全なセットが見つかりませんでした。
エージェント キーがキー ストア内にありません	SmServerMessage::AgentKey-NotFoundInKeyStore	ポリシー ストア内のエージェント キーを更新しようとしたとき、キーが見つかりませんでした。
初期エージェント キーがありません	SmServerMessage::Empty-AgentKeys	ポリシー ストア内にエージェント キーが格納されておらず、キー生成が有効になっていません。
初期キー管理オブジェクトが見つかりませんでした。このポリシー サーバは読み取り専用キー管理モードで設定されています。続行できません	SmServerMessage::Key-ManagementObjNotFound	ポリシー ストア内に初期エージェント キー管理オブジェクトが格納されておらず、キー生成が有効になっていません。

メッセージ	関数	説明
監査ログ プロバイダが使用できるネームスペースがありません	SmServerMessage::No-NamespaceAvailForAudit-LogProvider	監査ログ プロバイダのネームスペースのエントリがレジストリにありません。
ルート設定オブジェクトが見つかりませんでした。smobjimport を実行して smpolicy.smdif をインポートしてください	SmServerMessage::Root-ConfigObjNotFound	ポリシー ストアが正常に初期化されていません。
リクエスト %1s の処理中、セッション ポインタが見つかりませんでした	SmServerMessage::Null-SessionPointer	指定されたエージェント リクエストは受信されましたが、対応するエージェント セッション オブジェクトが見つからなかったか、有効ではありませんでした。そのため、リクエスト パケットは処理されずに返されました。
ファイルの権限またはパスが有効かどうか確認してください	SmServerMessage::File-PermissionOrPathCheck	ファイルを開くことができませんでした。ファイルのパス名を示すエラー メッセージが、このメッセージの前に表示されるはずです。示されたパス名が有効であることと、ファイルへのアクセス権限が正しいことを確認してください。
ポリシー サーバが ProcessMessage で例外をキャッチしました(メッセージ テキストはありません)。	SmServerMessage::Unknown-PolSrvExcpCaught	ポリシー サーバで、エージェント リクエストの処理中に予期しない例外が発生しました。そのため、空のレスポンスが返されました。
ポリシー サーバが ProcessMessage で例外をキャッチしました テキスト: %1s	SmServerMessage::PolSrv-ExcpCaught	ポリシー サーバで、エージェント リクエストの処理中に予期しない例外が発生しました。そのため、空のレスポンスが返されました。表示されるテキストに、推奨される修正アクションが示される場合があります。
ポリシー ストアで、オブジェクト タイプ「%2s」の操作「%1s」に失敗しました。 %3s	SmServerMessage::Policy-StoreOperFail	ポリシー ストア オブジェクト レイヤで、記述された例外がキャッチされました。

メッセージ	関数	説明
プロセッサ アフィニティがデフォルト設定のままです。アフィニティをゼロに設定できません	SmServerMessage::Processor-AffinitySetZeroFail	(Windows)ゼロはプロセッサ アフィニティのパフォーマンス調整パラメータについて無効な値です。したがって、既存のアフィニティ設定は変更されません。
%1s の拒否: アクセス ログを書き込めませんでした	SmServerMessage::Write-FailInAccessLog	指定された拒否済みの認証または許可リクエストの監査ロギングに失敗しました。
DoManagement() コマンド%1s、リクエスト %2s 内のエージェント名を参照しました	SmServerMessage::Agent-NameInDoManagement	「Do Management」エージェント コマンドは拒否されました。
Logout() コマンド %1s、リクエスト %2s 内のエージェント名を参照しました	SmServerMessage::Agent-NameInLogout	ログアウト リクエストは拒否されました。
プロセッサ アフィニティを設定できませんでした	SmServerMessage::Set-ProcessorAffinityFail	(Windows)プロセッサ アフィニティのパフォーマンス調整パラメータを処理できませんでした。したがって、既存のアフィニティ設定は変更されません。
初期化中に SM 例外がキャッチされました(%1s)	SmServerMessage::SMExcp-DuringInit	ポリシー サーバ起動時の「GlobalInit」段階で例外がキャッチされたため、ポリシー サーバを起動できませんでした。表示されるテキストに、詳細が示される場合があります。
サーバのシャットダウン中に SM 例外がキャッチされました(%1s)	SmServerMessage::SMExcp-DuringServerShutdown	ポリシー サーバ停止時の「GlobalRelease」段階で例外がキャッチされました。表示されるテキストに、詳細が示される場合があります。
TCP ポートを初期化できませんでした	SmServerMessage::TCP-PortInitFail	ポリシー サーバの起動中、アクセス制御リクエストまたは管理リクエストについて有効化された TCP ポートを初期化できませんでした。そのため、起動は中止されました。

メッセージ	関数	説明
サービス ローダが %1s を開始できませんでした。エラー %2i %3s	SmServerMes-sage::SZSERVER_StartFail	(Windows) サービス ローダを開始できませんでした (エラー テキストを参照)。そのため、ポリシー サーバやワンビュー モニターを開始できませんでした。
このポリシー サーバにはセッション暗号化キーがありません	SmServerMessage::Session-EncryptKeyNotFound	ポリシー サーバが初期セッション キーを持っておらず、キー生成が有効になっていません。アクセス制御リクエストまたは管理リクエストが処理されるように設定されている場合、起動は中止されます。
スレッド プール スレッドで例外がキャッチされました	SmServerMessage::ExcpIn-ThreadPool	予期しない条件が発生したため、ポリシー サーバのワーカー スレッドが終了しました。代替のスレッドがスレッド プールに追加されます。
UDP ポートを初期化できませんでした	SmServerMessage::UDPPort-InitFail	ポリシー サーバの起動中、管理リクエストまたは RADIUS リクエストについて有効化された UDP ポートを初期化できませんでした。そのため、起動は中止されました。
UDP 処理例外	SmServerMessage::UDP-ProcessingExcp	管理 GUI 初期化パケットまたは RADIUS レスポンス パケットの処理中、予期しないエラーが発生しました。レスポンスは送信されません。
コンソール出力コレクタを作成できません。トレースは有効になりません	SmServerMessage::Trace-NotEnableConsoleOutput-CollecCreateFail	ポリシー サーバ プロセスが、プロファイラ (トレース) ログの出力先のコンソール (またはターミナル ウィンドウ) にアクセスできませんでした。コンソールを開くための適切なアクセス権限があることを確認してください。

メッセージ	関数	説明
ファイル出力コレクタを作成できません。トレースは有効になりません	SmServerMessage::Trace-NotEnableFileOutput-CollecCreateFail	プロファイラ(トレース)ログ ファイルを、上書き用に開くことができなかったか(すでに存在する場合)、作成できませんでした(存在しない場合)。ディレクトリとファイル(存在する場合)に対するアクセス権限を確認してください。。
共有秘密キーのロールオーバー ポリシー オブジェクトを作成できません	SmServerMessage::Shared-SecretCreateFail	ポリシー サーバの起動中、ポリシー ストア内に共有秘密キー ポリシー オブジェクトが見つからず、初期ポリシー オブジェクトを作成できませんでした。そのため、起動は中止されました。
トレースを有効にすることができません	SmServerMessage::Trace-NotEnable	プロファイラ(トレース)ロギングの初期設定は成功しましたが、それ以外は成功しませんでした。
ロガー オプションを動的にリセットできません	SmServerMessage::Dynamic-LoggerResetFail	ポリシー サーバの実行中にロガー設定オプションの変更を検出するスレッドを開始できませんでした。そのため、ポリシー サーバを再起動するまで、そのような変更は対処されません。
リクエスト %1s のエージェントを解決できません	SmServerMessage::Unresolved-AgentIdentity	エージェント識別情報を含めるにはエージェント リクエストが必要ですが、識別情報を検証できませんでした。リクエストは拒否されました。
エージェント名 %1s、リクエスト %2s を解決できません	SmServerMessage::AgentName-UnResolved	エージェント識別情報を含めるにはエージェント リクエストが必要ですが、指定されたエージェントの識別情報を検証できませんでした。リクエストは拒否されました。

メッセージ	関数	説明
パスワード BLOB データを更新できません	SmServerMessage::Blob-UpdateFailed	パスワード サービスのためのユーザの「パスワード BLOB」データをユーザ ストア内で更新できませんでした。設定に従って、ポリシー サーバはユーザの認証試行を拒否しました。
許可ライブラリの発行中、予期しない例外が発生しました	SmServerMes-sage::UnexpectedException-PublishingAzLibs	ロードされたカスタム許可モジュールで「発行」の診断情報を照会しているときに、予期しない例外が発生しました。そのため、カスタム許可ライブラリに関する情報は発行されません。
不明のエージェント キー タイプ %1i	SmServerMessage::Agent-KeyTypeUnknown	「Do Management」リクエストの処理中、指定された、未承認のキー タイプを持つエージェント キー レコードがポリシー ストア内で見つかりました。そのため、リクエストは拒否されました。
認証ライブラリの発行中、不明の例外がキャッチされました	SmServerMessage::Unknown-ExcpPublishAuthLibs	カスタム認証方式ライブラリで「発行」の診断情報を照会しているときに、予期しない例外が発生しました。そのため、ロードされたカスタム認証方式に関する情報は発行されません。
イベント ライブラリ情報の発行中、不明の例外がキャッチされました	SmServerMessage::Unknown-ExcpWhilePublishEventLibInfo	カスタム イベント ハンドラ ライブラリで「発行」の診断情報を照会しているときに、予期しない例外が発生しました。そのため、SiteMinder によってロードされたカスタム イベント ライブラリに関する情報は発行されません。
ソケット エラー 104	104 - bind() 関数のコールに失敗しました。	TLI レイヤを介して送信中にエラーが発生したため、このメッセージは返されました。

Java API

エラー メッセージ	関数	説明
%1s が管理者ディレクトリをフェッチできませんでした	SmJavaApiMes-sage::AdministratorDirectory-FetchFail	登録管理者ユーザ ディレクトリをフェッチできません。ポリシー ストアを確認してください。
%1s が登録ディレクトリをフェッチできませんでした	SmJavaApiMes-sage::RegistrationDirectory-FetchFail	登録ユーザ ディレクトリをフェッチできません。ポリシー ストアを確認してください。
%1s が登録ドメインをフェッチできませんでした	SmJavaApiMes-sage::RegistrationDomain-FetchFail	登録ドメインをフェッチできません。ポリシー ストアを確認してください。
%1s が登録レルムをフェッチできませんでした	SmJavaApiMes-sage::RegistrationRealm-FetchFail	登録レルムをフェッチできません。ポリシー ストアを確認してください。
%1s が登録方式をフェッチできませんでした	SmJavaApiMes-sage::RegistrationScheme-FetchFail	登録方式をフェッチできません。ポリシー ストアを確認してください。
%1s 無効なレルム OID（NULL）	SmJavaApiMessage::Invalid-RealmOid	レルム OID を取得できません。ユーザがログインに成功したことと、有効なセッション ID が使用可能であることを確認してください。
（CSmEmsCommand::Set-ObjectClasses）プロパティの設定に失敗した後、ディレクトリ ユーザ %1s のプロパティをロールバックできませんでした	SmJavaApiMessage::Csm-EmsSetObjectClasses-RollBackPropertiesFail	新しい値が拒否された後、ユーザのプロパティをリセットできません。 ユーザ ストアが正しく動作していることと、ポリシー サーバが接続を確立できることを確認してください。
（CSmEmsCommand::Set-Properties）プロパティの設定に失敗した後、ディレクトリ ユーザ %1s のプロパティをロールバックできませんでした	SmJavaApiMessage::CSm-EmsSetPropertiesRollback-PropertiesFail	新しい値が拒否された後、ユーザのプロパティをリセットできません。 ユーザ ストアが正しく動作していることと、ポリシー サーバが接続を確立できることを確認してください。
（CSmEmsCommandV2::Set-ObjectClasses）プロパティの設定に失敗した後、ディレクトリ ユーザ %1s のプロパティをロールバックできませんでした	SmJavaApiMessage::Set-ObjectClassesDir-UserRollbackFail	新しい値が拒否された後、ユーザのプロパティをリセットできません。 ポリシー ストアで定義されているディレクトリ接続を確認してください。

エラー メッセージ	関数	説明
(CSmEmsCommandV2::Set-Properties)プロパティの設定に失敗した後、ディレクトリ オブジェクト %1s のプロパティをロールバックできませんでした	SmJavaApiMessage::Set-PropertiesDirObjRollbackFail	新しい値が拒否された後、オブジェクトのプロパティをリセットできません。 ポリシー ストアで定義されているディレクトリ接続を確認してください。
Transact SessionTimeoutThread で例外が発生しました	SmJavaApiMessage::Unknown-ExcpTransactSessionTimeout-Thread	期限切れセッションの処理中に不明なエラーが発生しました。
Transact SessionTimeoutThread で例外が発生しました メッセージ: %1s	SmJavaApiMessage::Excp-TransactSessionTimeoutThread	期限切れセッションの処理中にエラーが発生しました。
EmsSession タイムアウト スレッドを作成できませんでした	SmJavaApiMessage::Ems-SessionTimeoutThread-CreateFail	新しいスレッドを作成するための十分なシステム リソースがありません。
EMS API ライブラリ「%1s」をロードできませんでした	SmJavaApiMessage::Ems-ApiLibLoadFail	DMS が正常にインストールされていない、あるいはカスタム ライブラリが存在しないか、正しい場所に配置されていません。
関数「%1s」、EMS API ライブラリ「%2s」をロードできませんでした	SmJavaApiMessage::EmsApi-LibLoadFuncFail	DMS が正常にインストールされていない、あるいはカスタム ライブラリが存在しないか、正しい場所に配置されていません。
すべてのドメインを解決できませんでした	SmJavaApiMessage::Domain-ResolveFail	現在の管理者に関連付けられているすべてのドメインを取得しているときに問題が発生しました。ポリシー ストアに破損がないかどうか確認してください。
getUsersDelegatedRoles の実行に失敗しました。エラー = %1s	SmJavaApiMessage::IMSget-UsersDelegatedRolesFail	このユーザのロールを取得できません。smobjims.dll (libsmobjims.so) ライブラリがインストールされていることを確認してください。

エラー メッセージ	関数	説明
getUsersDelegatedRolesInApp の実行に失敗しました。エラー = %1s	SmJavaApiMessage::IMSget-UsersDelegatedRolesInAppFail	アプリケーションのユーザ ロールを取得できません。smobjims.dll（libsmobjims.so）ライブラリがインストールされていることを確認してください。
getUsersDelegatedTasks の実行に失敗しました。エラー = %1s	SmJavaApiMessage::IMSget-UsersDelegatedTasksFail	このユーザのタスクを取得できません。smobjims.dll（libsmobjims.so）ライブラリがインストールされていることを確認してください。
getUsersDelegatedTasksInApp の実行に失敗しました。エラー = %1s	SmJavaApiMessage::IMS-getUsersDelegatedTasksIn-AppFail	アプリケーションのユーザ タスクを取得できません。smobjims.dll（libsmobjims.so）ライブラリがインストールされていることを確認してください。
getUsersRoles の実行に失敗しました。エラー = %1s	SmJavaApiMessage::IMS-getUsersRolesFail	このユーザのロールを取得できません。smobjims.dll（libsmobjims.so）ライブラリがインストールされていることを確認してください。
getUsersRolesInApp の実行に失敗しました。エラー = %1s	SmJavaApiMessage::IMS-getUsersRolesInAppFail	アプリケーションのユーザ ロールを取得できません。smobjims.dll（libsmobjims.so）ライブラリがインストールされていることを確認してください。
getUsersTasks の実行に失敗しました。エラー = %1s	SmJavaApiMessage::IMS-getUsersTasksFail	このユーザのタスクを取得できません。smobjims.dll（libsmobjims.so）ライブラリがインストールされていることを確認してください。
getUsersTasksInApp の実行に失敗しました。エラー = %1s	SmJavaApiMessage::IMS-getUsersTasksInAppFail	アプリケーションのユーザ タスクを取得できません。smobjims.dll（libsmobjims.so）ライブラリがインストールされていることを確認してください。
IMSObjectProviderFactory: getIMSBaseObjectProvider() - getProcAddress('%1s') の実行に失敗しました	SmJavaApiMessage::getIMSB-aseObjectProvider_getProc-AddressFail	smobjims.dll（libsmobjims.so）ライブラリがインストールされていることを確認してください。

エラー メッセージ	関数	説明
IMSObjectProviderFactory:get-Provider() - プロバイダ ライブラリの ロード エラー	SmJavaApiMes-sage::IMS_getProviderLib-LoadError	IdentityMinder がインストールされていないか、正しくインストールされていない場合、起動時にこのメッセージが生成されます。
%1s の IMSObjectProviderFactory:get-Provider() - getProcAddress の実行に失敗しました	SmJavaApiMes-sage::IMS_getProvider_get-ProcAddressFail	ライブラリが破損しています。あるいは、リソース不足のためポリシー サーバがライブラリをロードできませんでした。
%1s の ImsRBACProviderFactory:get-Provider() - getProcAddress の実行に失敗しました	SmJavaApiMessage::Ims-RBACProvider-Factory_getProviderFail	IdentityMinder がインストールされていないか、正しくインストールされていない場合、起動時にこのメッセージが生成されます。
IsAssociatedWithDirectory の実行に失敗しました。エラー = %1s	SmJavaApiMessage::IMSIs-AssociatedWithDirectoryFail	関連する IMS 環境についてユーザ ディレクトリが有効であるかどうかを判断しているときにエラーが発生しました。
IsUserAssignedRole の実行に失敗しました。 エラー = %1s	SmJavaApiMessage::IMSIs-UserAssignedRoleFail	ユーザがロールに属するかどうかを判断しているときにエラーが発生しました。
IsUserDelegatedRole の実行に失敗しました。エラー = %1s	SmJavaApiMessage::IMSIs-UserDelegatedRoleFail	ユーザがロールに属するかどうかを判断しているときにエラーが発生しました。
SmJavaAPI: クラス ActiveExpressionContext %1p の検索エラー	SmJavaApiMessage::MSG_E_-FINDING_CAEClog	結合中、JVM で Active Expression クラスを特定できませんでした。ポリシー サーバにオプション パックがインストールされていることを確認してください。smjavaapi.jar のクラスパスも確認してください。
SmJavaAPI: クラス NativeCallbackError %1p の検索エラー	SmJavaApiMessage::MSG_E_-FINDING_CNCElog	有効な smjavaapi.jar が存在し、クラスパスに含まれていることを確認してください。JVM バージョンがこのリリースについてサポートされているかどうかを確認してください。

エラー メッセージ	関数	説明
SmJavaAPI: クラス SmAuthenticationContext %1p の検索エラー	SmJavaApiMessage::MSG_E_-FINDING_CAUTHClog	有効な smjavaapi.jar が存在し、クラスパスに含まれていることを確認してください。
SmJavaAPI: クラス Throwable %1p の検索エラー	SmJavaApiMessage::MSG_E_-FINDING_CTHROWlog	JVM/JRE が正常にインストールされていない可能性があります。有効な rt.jar が存在するかどうかを確認してください。サポートされている JVM バージョンを使用するように SiteMinder が設定されていることを確認してください。
SmJavaAPI: クラス TunnelServiceContext %1p の検索エラー	SmJavaApiMessage::MSG_E_-FINDING_CTSClog	ポリシー サーバにオプション パックがインストールされていることと、有効な smjavaapi.jar が存在し、クラスパスに含まれていることを確認してください。
SmJavaAPI: クラス UserAuthenticationException %1p の検索エラー	SmJavaApiMessage::MSG_E_-FINDING_CUAElog	有効な smjavaapi.jar が存在し、クラスパスに含まれていることを確認してください。JVM バージョンがこのリリースについてサポートされているかどうかを確認してください。
SmJavaAPI: メソッド ActiveExpressionContext の検索エラー。 %1p を呼び出してください	SmJavaApiMessage::MSG_E_-FIND_MINVOKElog	ポリシー サーバにオプション パックがインストールされていることと、有効な smjavaapi.jar が存在し、クラスパスに含まれていることを確認してください。
SmJavaAPI: メソッド ActiveExpressionContext の検索エラー。 %1p を解放してください	SmJavaApiMessage::MSG_E_-FIND_MRELEASElog	ポリシー サーバにオプション パックがインストールされていることと、有効な smjavaapi.jar が存在し、クラスパスに含まれていることを確認してください。
SmJavaAPI: メソッド SmAuthenticationContext の検索エラー。 %1p を認証してください	SmJavaApiMessage::MSG_E_-FIND_MAUTHENTICATElog	有効な smjavaapi.jar が存在し、クラスパスに含まれていることを確認してください。JVM バージョンがこのリリースについてサポートされているかどうかを確認してください。

エラー メッセージ	関数	説明
SmJavaAPI: メソッド SmAuthenticationContext の検索エラー。 %1p を初期化してください	SmJavaApiMessage::MSG_E_-FIND_MAUTHINITlog	有効な smjavaapi.jar が存在し、クラスパスに含まれていることを確認してください。JVM バージョンがこのリリースについてサポートされているかどうかを確認してください。
SmJavaAPI: メソッド SmAuthenticationContext の検索エラー。 %1p を照会してください	SmJavaApiMessage::MSG_E_-FIND_MAUTHQUERYlog	有効な smjavaapi.jar が存在し、クラスパスに含まれていることを確認してください。JVM バージョンがこのリリースについてサポートされているかどうかを確認してください。
SmJavaAPI: メソッド SmAuthenticationContext の検索エラー。 %1p を解放してください	SmJavaApiMessage::MSG_E_-FIND_MAUTHRELEASElog	有効な smjavaapi.jar が存在し、クラスパスに含まれていることを確認してください。JVM バージョンがこのリリースについてサポートされているかどうかを確認してください。
SmJavaAPI: メソッド Throwable.getLocalized-Message %1p の検索エラー	SmJavaApiMessage::MSG_E_-FIND_GLMlog	JVM/JRE が正常にインストールされていない可能性があります。有効な rt.jar が存在するかどうかを確認してください。サポートされている JVM バージョンを使用するように SiteMinder が設定されていることを確認してください。
SmJavaAPI: メソッド TunnelServiceContext.tunnel %1p の検索エラー	SmJavaApiMessage::MSG_E_-FIND_MTUNNELlog	有効な smjavaapi.jar が存在し、クラスパスに含まれていることを確認してください。
SmJavaAPI: Java のアクティブな式 %1p の初期化エラー	SmJavaApiMessage::MSG_E_-ACTEXPR_INITlog	Active Expression ライブラリをロードできません。smactiveexpr.jar がクラスパスに含まれていることを確認してください。
SmJavaAPI: SMJavaAPI %1p に対する JNI 参照の初期化エラー	SmJavaApiMessage::MSG_E_-INIT_JNI_REFSlog	JVM で内部エラーが発生しました。JVM のインストールを確認してください。
SmJavaAPI: クラス ActiveExpressionContext %1p に対するグローバル参照の 実行エラー	SmJavaApiMessage::MSG_E_-GLOBAL_CAEClog	アクティブな式のコンテキストを確立しているとき、JVM で内部エラーが発生しました。

エラー メッセージ	関数	説明
SmJavaAPI: クラス NativeCallbackError %1p に対するグローバル参照の実行エラー	SmJavaApiMessage::MSG_E_-GLOBAL_CNCElog	有効な smjavaapi.jar が存在し、クラスパスに含まれていることを確認してください。JVM バージョンがこのリリースについてサポートされているかどうかを確認してください。
SmJavaAPI: クラス SmAuthenticationContext %1p に対するグローバル参照の実行エラー	SmJavaApiMessage::MSG_E_-GLOBAL_CAUTHClog	認証のコンテキストを確立しているとき、JVM で内部エラーが発生しました。
SmJavaAPI: クラス Throwable %1p に対するグローバル参照の実行エラー	SmJavaApiMessage::MSG_E_-GLOBAL_CTHROWlog	JVM/JRE が正常にインストールされていない可能性があります。有効な rt.jar が存在するかどうかを確認してください。サポートされている JVM バージョンを使用するように SiteMinder が設定されていることを確認してください。
SmJavaAPI: クラス TunnelServiceContext %1p に対するグローバル参照の実行エラー	SmJavaApiMessage::MSG_E_-GLOBAL_CTSClog	トンネル接続を確立しているとき、JVM で内部エラーが発生しました。
SmJavaAPI: クラス UserAuthenticationException %1p に対するグローバル参照の実行エラー	SmJavaApiMessage::MSG_E_-GLOBAL_CUAElog	有効な smjavaapi.jar が存在し、クラスパスに含まれていることを確認してください。JVM バージョンがこのリリースについてサポートされているかどうかを確認してください。
SmJavaAPI: Java アクティブ式 %1p に対する解放エラー	SmJavaApiMessage::MSG_E_-ACTEXPR_RELEASElog	JVM で内部エラーが発生しました。JVM のインストールを確認してください。
SmJavaAPI: SMJavaAPI %1p に対する JNI 参照の解放エラー	SmJavaApiMessage::MSG_E_-REL_JNI_REFSlog	JVM で内部エラーが発生しました。JVM のインストールを確認してください。
SmJavaAPI: JVM 環境 %1p を取得できません	SmJavaApiMessage::MSG_-ERR_GETTING_JVMlog	JVM で内部エラーが発生しました。JVM のインストールを確認してください。

エラー メッセージ	関数	説明
SmJavaAPI: JNI 参照 %1p を初期化できません	SmJavaApiMessage::MSG_-ERR_INIT_JNI_REFlog	JVM で内部エラーが発生しました。JVM のインストールを確認してください。
SmJavaAPI: JNI 参照 %1p を解放できません	SmJavaApiMessage::MSG_-ERR_REL_JNI_REFlog	ポリシー サーバは、許可の後またはシャットダウン中に、リソースを完全に解放できませんでした。
SmJVMSupport: スレッド %1p への JVM アタッチ エラー	SmJavaApiMessage::MSG_E_-ATTACH_TO_THREADlog	JVM が正常に初期化されなかった可能性があります。実行中の迷子の Java プロセスが存在しないことを確認してください。
SmJVMSupport: JVM %1p 作成エラー	SmJavaApiMessage::MSG_E_-CREATE_JVMlog	JVM が正しくインストールされていることと、jvm.dll（libjvm.so）ライブラリが有効であることを確認してください。
SmJVMSupport: JVM %1p の破棄エラー	SmJavaApiMessage::MSG_E_-DESTROYING_JAVA_VMlog	ポリシー サーバでクリーン シャットダウンが実行されませんでした。JVM リソースは解放されませんでした。
SmJVMSupport: スレッド %1p からの JVM 添付解除エラー	SmJavaApiMessage::MSG_E_-DETACH_THREADlog	ポリシー サーバでクリーン シャットダウンが実行されませんでした。JVM リソースは解放されませんでした。
SmJVMSupport: JVM %1p からリソースを解放するためのクラス System の検索エラー	SmJavaApiMessage::MSG_E_-JVM_RR_FSYSlog	ポリシー サーバでクリーン シャットダウンが実行されませんでした。JVM リソースは解放されませんでした。
SmJVMSupport: JVM %1p の作成時における CLASSPATH 環境変数取得エラー	SmJavaApiMessage::MSG_E_-GETENV_CPlog	CLASSPATH 変数が正しく定義されていることを確認してください。
SmJVMSupport: JVM %1p からリソースを解放するための JVM 環境の取得エラー	SmJavaApiMessage::MSG_E_-JVM_RR_ENVlog	ポリシー サーバでクリーン シャットダウンが実行されませんでした。JVM リソースは解放されませんでした。

エラー メッセージ	関数	説明
SmJVMSupport: JVM %1p からリソースを 解放するためのクラス System 上のメソッド GC の取得エラー	SmJavaApiMessage::MSG_E_-JVM_RR_GGClog	JVM がガーベッジ コレクションを実行できませんでした。rt.jar の有効性を確認してください。
SmJVMSupport: NETE_JVM_OPTION_FILE %1p のオープン エラー	SmJavaApiMessage::MSG_E_-OPEN_JVM_OPTION_FILElog	環境変数 NETE_JVM_OPTION_FILE が設定されていることと、ファイルが有効であることを確認してください。
SmJVMSupport: 作成された JVM %1p の取得エラー	SmJavaApiMessage::MSG_E_-GET_CREATED_JVM_LOG	JVM が正常に初期化 されなかった可能性があります。実行中の迷子の Java プロセスが存在しない ことを確認してください。
SmJVMSupport: JVM %1p の作成時にキャッチされた 不明のエラー	SmJavaApiMessage::MSG_E_-CAUGHT_CREATE_JVMlog	JVM が正しくインストールされていることと、jvm.dll (libjvm.so)ライブラリが有効であることを確認してください。

LDAP

エラー メッセージ	関数	説明
(AddMember)グループ DN: 「%1s」、ユーザ DN: 「%2s」。ステータス: エラー %3i。%4s	SmLdapMessage::ErrorLdap-AddMemberGroupDN	LDAP ユーザ ディレクトリ内の指定されたグループに対し、指定されたユーザを追加できませんでした。詳細については、LDAP エラー メッセージを参照してください。
(AuthenticateUser) DN: 「%1s」。ステータス: エラー %2i。 %3s	SmLdapMes-sage::AuthenticateUserDNLd-Error	ポリシー サーバで、LDAP ユーザ ディレクトリに対してユーザを認証できませんでした。このエラーは、ユーザが正しくないパスワードを入力するなど、さまざまな理由で発生することがあります。詳細については、LDAP エラー メッセージを参照してください。

エラー メッセージ	関数	説明
(Bind - init) サーバ: 「%1s」、ポート: %2ul。ステータス: エラー	SmLdapMessage::ErrorBindInit	ユーザ ディレクトリ用に設定された LDAP サーバを初期化できませんでした。エラー メッセージの中で示された LDAP サーバをトラブルシューティングしてください。
(Bind - init) サーバ: セキュリティ統合 ファイルをロードできませんでした	SmLdapMessage::BindInit-LoadSecurityIntegrationFileFail	(現在使用されていません)
(Bind - init) サーバ: セキュリティ統合 秘密キーをロード できませんでした	SmLdapMessage::BindInit-LoadSecurityIntegrationSecret-Fail	(現在使用されていません)
(Bind - ldap_set_option CONNECT_TIMEOUT)。ステータス: エラー %1i。%2s	SmLdapMessage::ErrorBind-LdapOptionConnectTimeout	LDAP オプションを設定できません。詳細については、エラー文字列を確認してください。
(Bind - ldap_set_option LDAP_OPT_PROTOCOL_-VERSION)。ステータス: エラー %1i。%2s	SmLdapMessage::ErrorBind-LdapOptionProtocolVersion	LDAP オプションを設定できません。詳細については、エラー文字列を確認してください。
(Bind - ldap_set_option LDAP_OPT_REFERRALS)。ステータス: エラー %1i。%2s	SmLdapMessage::ErrorBind-LdapOptionReferrals	自動リフェラル処理の有効化を設定できません。詳細については、エラー文字列を確認してください。
(Bind - ldap_set_option LDAPL_VERSION2)。ステータス: エラー %1i。%2s	SmLdapMessage::ErrorBind-LdapOptionVersion2	LDAP オプションを設定できません。詳細については、エラー文字列を確認してください。使用している LDAP サーバが、サポートされているバージョンのうちの 1 つであることを確認してください。
(Bind - ldap_set_option SIZELIMIT)。ステータス: エラー %1i。%2s	SmLdapMessage::ErrorBind-LdapOptionSizeLimit	LDAP オプションを設定できません。詳細については、エラー文字列を確認してください。

エラー メッセージ	関数	説明
(Bind - ldap_set_option THREAD_FN_PTRS)。ステータス: エラー %1i。%2s	SmLdapMessage::ErrorBind-LdapOptionThreadFnPirs	LDAP オプションを設定できません。詳細については、エラー文字列を確認してください。
(Bind - ldap_set_option TIMELIMIT)。ステータス: エラー %1i。%2s	SmLdapMessage::ErrorBind-LdapOptionTimeLimit	LDAP オプションを設定できません。詳細については、エラー文字列を確認してください。
(Bind - LDAP 初期化中、SSL クライアントを初期化できませんでした) サーバ:「%1s」、ポート: %2ul、証明書 DB:「%3s」。ステータス: エラー	SmLdapMessage::BindSSL-LdapClientInitFailed	LDAP サーバに接続できません。LDAP サーバが稼働していることと、LDAP サーバおよびポートが正しいことを確認してください (ポリシー サーバ マシンから ping を実行してみてください)。
(Bind - SSL client init) 証明書 DB:「%1s」。ステータス: エラー	SmLdapMessage::BindSSL-ClientCertDBFailed	ユーザ ディレクトリ用に設定された LDAP サーバへの SSL 接続のクライアント側の初期化に失敗しました。証明書データベースが正しく指定されているかどうかを確認してください。
(Bind - SSL init) サーバ:「%1s」、ポート: %2ul。ステータス: エラー。LDAP サーバおよびポートを確認してください。	SmLdapMessage::BindSSL-InitFailed LDAP サーバおよびポートを確認してください。	SSL を使用して LDAP サーバに対して初期化できません。LDAP サーバおよびポートを確認してください。LDAP サーバが SSL 用に設定されていることを確認してください。
(Bind) DN:「%1s」。ステータス: エラー %2i。%3s	SmLdapMessage::BindDN-RequireCredentialsError	LDAP サーバにバインドできません。クレデンシャルが正しいことを確認してください。SiteMinder 管理コンソールを参照してください。
(Bind) ステータス: エラー %1i。%2s	SmLdapMessage::Bind-StatusError	LDAP オプションを設定できません。詳細については、エラー文字列を確認してください。
(ChangeUserPassword) DN:「%1s」。ステータス: エラー %2i。 %3s	SmLdapMessage::Change-UserPasswordLdError	指定されたユーザのパスワードを変更できませんでした。そのユーザの古いパスワードを使用して LDAP サーバにバインドできなかったためです。詳細については、エラー メッセージを参照してください。

エラー メッセージ	関数	説明
(ChangeUserPassword) DN: 「%1s」。ステータス: エラー %2s	SmLdapMessage::Change-UserPasswordDNFail	指定されたユーザのパスワードを変更できませんでした。詳細については、エラー メッセージを参照してください。
(CSmDsLdapProvider::Add-Entry) DN:「%1s」。ステータス: エラー %2i。%3s	SmLdapMessage::ErrorLdap-AddEntryDN	指定された DN エントリを LDAP ユーザ ディレクトリに追加できませんでした。詳細については、LDAP エラー メッセージを参照してください。
(GetObjProperties) DN: 「%1s」。ステータス: エラー %2i。%3s	SmLdapMessage::GetObj-PropertiesDNLdError	ポリシー サーバで、LDAP ユーザ ディレクトリ内にあるリクエストされた DN のリクエストされたプロパティを取得できませんでした。詳細については、LDAP エラー メッセージを参照してください。
(GetUserProp) DN:「%1s」、フィルタ:「%2s」。ステータス: エラー %3i。%4s	SmLdapMessage::GetUser-PropDNLd-Error	指定された DN を検索しているとき、および取得される属性を指定しているときに、エラーが発生しました。詳細については、LDAP エラー メッセージを参照してください。
(GetUserProp) DN:「%1s」、フィルタ:「%2s」。ステータス: エラー %3i。%4s	SmLdapMessage::GetUser-PropsDNLdError	指定された DN を検索しているとき、および取得される属性を指定しているときに、エラーが発生しました。詳細については、LDAP エラー メッセージを参照してください。
(RemoveEntry) DN:「%1s」。ステータス: エラー %2i。%3s	SmLdapMessage::ErrorLdap-RemoveEntryDN	LDAP ユーザ ディレクトリから削除する DN エントリが見つかりませんでした。詳細については、LDAP エラー メッセージを参照してください。
(RemoveMember)グループ DN:「%1s」、ユーザ DN:「%2s」。ステータス: エラー %3i。%4s	SmLdapMessage::ErrorLdap-RemoveMemberGroupDN	LDAP ユーザ ディレクトリ内の指定されたグループから、指定されたユーザを削除できませんでした。詳細については、LDAP エラー メッセージを参照してください。

エラー メッセージ	関数	説明
(SetUserProp) DN:「%1s」、プロパティ名:「%2s」、プロパティ値:「%3s」。ステータス: エラー %4i。 %5s	SmLdapMessage::SetUser-PropDNError	LDAP ユーザ ディレクトリ内の指定された DN エントリを変更できませんでした。詳細については、LAP エラー メッセージを参照してください。
(SetUserProp) DN:「%1s」。ステータス: エラー %2i。%3s	SmLdapMessage::SetUser-PropsDNLdError	LDAP ユーザ ディレクトリ内の指定された DN エントリを変更できませんでした。詳細については、LDAP エラー メッセージを参照してください。
(SI Bind - init) サーバ:「%1s」、ポート: %2ul。ステータス: エラー	SmLdapMessage::ErrorSI-BindInit	ユーザ ディレクトリ用に設定された LDAP サーバを初期化できませんでした。エラー メッセージの中で示された LDAP サーバをトラブルシューティングしてください。
(SmDsLdap) サーバを取得できませんでした	SmLdapMessage::SmDs-LdapFailToGetServers	参照先の LDAP サーバに再バインドしているときに、内部エラーが発生しました。データを使用できない場合があります。
(SmDsLdapConnMgr(Bind): LDAP 初期化中、SSL クライアントを初期化できませんでした)。サーバ %1s: %2ul、証明書 DB: %3s	SmLdapMessage::Ldap-ConnMgrBindSSLCertDBInit-Fail	SSL を使用して LDAP サーバに対して初期化できません。LDAP サーバおよびポートを確認してください。LDAP サーバが SSL 用に設定されていることを確認してください。
(SmDsLdap-GetHandle) %1s 解析中のエラー LDAP URL。	SmLdapMessage::GetHandle-LdapURLParsingError	内部 LDAP URL を解析できませんでした。この URL は RFC 2255 形式に準拠している必要があります。
(SmDsLdap-LdapAdd) DN:「%1s」。ステータス: リフェラルを受け取りましたが、処理が実装されていません。	SmLdapMessage:SmDsLdap-AddHandlingImplError	リフェラル リクエストを返す Add コールでエラーが発生しました。
(SmDsLdap-LdapDelete) DN:「%1s」。ステータス: リフェラルを受け取りましたが、処理が実装されていません。	SmLdapMessage::SmDs-LdapDeleteHandlingImplError	リフェラル リクエストを返す Delete コールでエラーが発生しました。

エラー メッセージ	関数	説明
(SmDsLdap-LdapModify) DN: 「%1s」。ステータス: リフェラルを受け取りましたが、処理が実装されていません。	SmLdapMessage::SmDs-LdapModifyHandlingImplError	リフェラル リクエストを返す Modify コールでエラーが発生しました。
(SmDsLdap-Referral) %1s 解析中のエラー LDAP URL。	SmLdapMessage::Ldap-URLParsingError	ポリシー サーバで、指定された LDAP URL を解析できませんでした。このエラーの一般的な原因は、誤りのある LDAP URL がリフェラルとして渡されたことです。その場合は、LDAP トポロジが正しく定義されていることを確認し、ポリシー サーバ管理コンソールで拡張 LDAP リフェラル処理を無効にしてください。
CSmDsLdapConnMgr (ldap_unbind_s)。サーバ %1s: %2ul	SmLdapMessage::Error-LdapConnMgrUnbind	LDAP サーバからのバインド解除中にエラーが発生しました。
CSmDsLdapConnMgr (ldap_unbind_s)。サーバ %1s: %2ul	SmLdapMessage::Unknown-ExceptionLdapConnMgrUnbind	LDAP サーバからのバインド解除中に内部エラーが発生しました。
CSmDsLdapProvider::Search(): LDAP 検索フィルタの構文エラー: %1s	SmLdapMessage::Wrong-SyntaxLdapSearchFilter	LDAP 検索フィルタの構文が正しいかどうか確認してください。
CSmDsLdapProvider::Search-Binary(): LDAP 検索フィルタの構文エラー: %1s	SmLdapMessage::Wrong-SyntaxLdapSearchBinFilter	LDAP 検索フィルタの構文が正しいかどうか確認してください。
CSmDsLdapProvider::Search-Count(): LDAP 検索フィルタの構文エラー: %1s	SmLdapMessage::Wrong-SyntaxLdapSearchCountFilter	LDAP 検索フィルタの構文が正しいかどうか確認してください。
CSmObjLdapConnMgr 例外 (ldap_unbind_s)。サーバ %1s: %2ul	SmLdapMessage::Excp-CSmObjLdapConn-Mgrldap_unbind_s	SiteMinder ポリシー サーバで、ポリシー ストア用に設定された LDAP サーバからバインド解除できませんでした。エラー メッセージの中で示された LDAP サーバをトラブルシューティングしてください。

エラー メッセージ	関数	説明
ディレクトリの無効フラグ属性が CSmDsLdapProvider::Set-DisabledUserState のパスワード サービス機能について適切ではありません。	SmLdapMessage::DirDisabled-FlagNotProper	ユーザ ディレクトリの設定において無効フラグ属性として機能するように選択されたユーザ属性は、この目的には適していません。属性を選択し直してください。
CSmDsLDAPConn::Create-LDAPControls の例外（ldap_controls_free）	SmLdapMessage::Unknown-ExceptionFreeLDAPControls	内部オブジェクトを LDAP ライブラリに解放しているときに、予期しないエラーが発生しました。ポリシー サーバ システム上のメモリ エラーまたは設定エラーが原因であると思われます。
CSmDsLdapProvider::Search-Count の例外（ldap_count_entries）	SmLdapMessage::Unknown-ExceptionLdapCountEntries	ユーザ ディレクトリ プロバイダ レイヤ内での LDAP 検索の結果を処理しているときに、不明の例外が発生しました。
CSmDsLdapProvider::Get-GroupMembers の例外（ldap_explode_dn）	SmLdapMessage::Ldap-ExplodeExceptionGet-GroupMembers	DN をその構成部分に変換しているときに、不明の例外が発生しました。
CSmDsLdapProvider::Bind の例外（ldap_init）	SmLdapMessage::Unknown-ExceptionLdapInitBind	ユーザ ディレクトリ用に設定された LDAP サーバを初期化しているときに、不明の例外が発生しました。
SecurityIntegrationCheck の例外（ldap_init）	SmLdapMessage::Unknown-ExceptionLdapInit	ユーザ ディレクトリ用に設定された LDAP サーバを初期化しているときに、不明の例外が発生しました。
CSmDsLdapProvider::Add-Entry の例外（ldap_modify_s）	SmLdapMessage::Unknown-ExceptionLdapModifyAdd-Entries	LDAP ユーザ ディレクトリにエントリを追加しているときに、不明の例外が発生しました。
CSmDsLdapProvider::Set-UserProps の例外（ldap_modify_s）	SmLdapMessage::Unknown-ExceptionLdapModify-SetUserProps	LDAP ユーザ ディレクトリ内のエントリを変更しているときに、不明の例外が発生しました。
CSmDsLdapProvider::Ping-Server の例外（ldap_search_ext_s）	SmLdapMessage::Unknown-ExceptionPingServer	LDAP サーバに接続できません。LDAP サーバが稼働していることと、ポートが正しいことを確認してください（ポリシー サーバ マシンから ping を実行してみてください）。

エラー メッセージ	関数	説明
CSmDsLdap-Provider::Search の例外（ldap_search_ext_s）	SmLdapMessage::Unknown-ExceptionLdapSearchExt	ユーザ ディレクトリ プロバイダ レイヤ内で LDAP 検索を実行しているときに、不明の例外が発生しました。
CSmDsLdapProvider::-SearchBinary の例外（ldap_search_ext_s）	SmLdapMessage::Unknown-ExceptionLdapSearchBinExt	ユーザ ディレクトリ プロバイダ レイヤ内で LDAP 検索を実行しているときに、不明の例外が発生しました。
CSmDsLdapProvider::-SearchCount の例外（ldap_search_ext_s）	SmLdapMessage::Unknown-ExceptionSearchCount	ユーザ ディレクトリ プロバイダ レイヤ内で LDAP 検索を実行しているときに、不明の例外が発生しました。
CSmObjLdapProvider::Ping-Server の 例外（ldap_search_s）	SmLdapMessage::Unknown-ExceptionLdapSearchGet-ObjProperties	ユーザ ディレクトリ プロバイダ レイヤ内で LDAP 検索を実行しているときに、不明の例外が発生しました。
CSmObjLdapProvider::Ping-Server の 例外（ldap_search_s）	SmLdapMessage::Unknown-ExceptionLdapSearchGet-UserProp	ユーザ ディレクトリ プロバイダ レイヤ内で LDAP 検索を実行しているときに、不明の例外が発生しました。
CSmObjLdapProvider::Ping-Server の 例外（ldap_search_s）	SmLdapMessage::Unknown-ExceptionLdapSearchGet-UserProps	ユーザ ディレクトリ プロバイダ レイヤ内で LDAP 検索を実行しているときに、不明の例外が発生しました。
CSmObjLdapProvider::Ping-Server の 例外（ldap_search_st）	SmLdapMessage::Excp-Ldap_Search_S	ポリシー ストア用に設定された LDAP サーバに対して ping を実行できませんでした。この LDAP サーバが稼働しているかどうかを確認してください。
CSmObjLdapProvider::Ping-Server の 例外（ldap_search_st）	SmLdapMessage::Excpldap_-search_st	ポリシー ストア用に設定された LDAP サーバに対し、指定されたタイムアウト値を使って ping を実行できませんでした。この LDAP サーバが稼働しているかどうかを確認してください。
CSmDsLdapProvider::Bind の例外（ldap_simple_bind_s）	SmLdapMessage::Unknown-Exception-LdapSimpleBind	LDAP サーバに接続できません。LDAP サーバが稼働していることと、ポートが正しいことを確認してください（ポリシー サーバ マシンから ping を実行してみてください）。

エラー メッセージ	関数	説明
CSmDsLdapProvider::Add-Entry の例外（LdapModify）	SmLdapMessage::Unknown-ExceptionLdapModifyAddEntry	LDAP ユーザ ディレクトリにエントリを追加しているときに、不明の例外が発生しました。拡張リフェラル処理が役に立つかどうか試してみてください。
CSmDsLdapProvider::Add-Member の例外（LdapModify）	SmLdapMessage::Unknown-ExceptionLdapModifyAdd-Member	LDAP ユーザ ディレクトリ内のグループにメンバを追加しているときに、不明の例外が発生しました。拡張リフェラル処理が役に立つかどうか試してみてください。
CSmDsLdapProvider::Remove-Member の例外（LdapModify）	SmLdapMessage::Unknown-ExceptionLdapModify-RemoveMember	LDAP ユーザ ディレクトリ内のグループからメンバを削除しているときに、不明の例外が発生しました。拡張リフェラル処理が役に立つかどうか試してみてください。
CSmDsLdapProvider::Set-UserProp の例外（LdapModify）	SmLdapMessage::Unknown-ExceptionLdapModifySet-UserProp	LDAP ユーザ ディレクトリ内のエントリを変更しているときに、不明の例外が発生しました。拡張リフェラル処理が役に立つかどうか試してみてください。
CSmDsLdapProvider::Init-Instance の例外（ldapssl_client_init）	SmLdapMessage::Unknown-ExceptionLdapSSLClinetInit	ユーザ ディレクトリ用に設定された LDAP サーバへの SSL 接続のクライアント側の初期化に失敗しました。証明書データベースが正しく指定されているかどうかを確認してください。
CSmDsLdapProvider::Bind の例外（ldapssl_init）	SmLdapMessage::Unknown-ExceptionLdapSSLInitBind	SSL を使用して LDAP サーバに対して初期化できません。LDAP サーバおよびポートを確認してください。LDAP サーバが SSL 用に設定されていることを確認してください。

エラー メッセージ	関数	説明
CSmDsLDAPConn::Create-LDAPControls の例外	SmLdapMessage::Unknown-ExceptionCreateLDAPControls	LDAP ライブラリの内部オブジェクトをリクエストしているときに、予期しないエラーが発生しました。ポリシー サーバ システム上のメモリ エラーまたは設定エラーが原因であると思われます。
CSmDsLDAPConn::Free-LDAPControls の例外	SmLdapMessage::Unknown-exceptionCSmDsLDAP-Conn_FreeLDAPControls	LDAP コントロールの解放中に内部エラーが発生しました。
CSmDsLDAPConn::Parse-LDAPControls の例外	SmLdapMessage::Unknown-ExceptionParseLDAPControls	LDAP サーバからのレスポンスを解析できません。LDAP サーバは正常に稼働していますか。
CSmDsLdapProvider::Get-ObjProperties の例外	SmLdapMessage::Unknown-ExceptionGetObjProperties	ユーザ ディレクトリ プロバイダ レイヤ内での LDAP 検索の結果を処理しているときに、不明の例外が発生しました。
CSmDsLdapProvider::Get-UserProp の例外	SmLdapMessage::Unknown-ExceptionGetUserProp	ユーザ ディレクトリ プロバイダ レイヤ内での LDAP 検索の結果を処理しているときに、不明の例外が発生しました。
CSmDsLdapProvider::Get-UserProps の例外	SmLdapMessage::Unknown-ExceptionGetUserProps	ユーザ ディレクトリ プロバイダ レイヤ内での LDAP 検索の結果を処理しているときに、不明の例外が発生しました。
CSmDsLdapProvider::Search の例外	SmLdapMessage::Unknown-ExceptionCSmDsLdap-ProviderSearch	ユーザ ディレクトリ プロバイダ レイヤ内での LDAP 検索の結果を処理しているときに、不明の例外が発生しました。
CSmDsLdapProvider::Search-Binary の例外	SmLdapMessage::Unknown-ExceptionSearchBinary	ユーザ ディレクトリ プロバイダ レイヤ内での LDAP 検索の結果を処理しているときに、不明の例外が発生しました。

エラー メッセージ	関数	説明
SecurityIntegrationCheck で例外が発生しました	SmLdapMessage::Unknown-ExceptionSecurityIntegration-Check	ユーザ ディレクトリ用に設定された LDAP サーバが Security Integration LDAP のインスタンスであるかどうかを確認しているときに、不明の例外が発生しました。
ページング コントロールを作成できませんでした	SmLdapMessage::Create-PagingControlFail	LDAP ライブラリの内部オブジェクトをリクエストしているときに、内部エラーが発生しました。ポリシー サーバ システム上のメモリ エラーまたは設定エラーが原因であると思われます。
LDAP 並べ替えコントロールを作成できませんでした	SmLdapMessage::Create-SortLdapControlFail	LDAP ライブラリの内部オブジェクトをリクエストしているときに、内部エラーが発生しました。ポリシー サーバ システム上のメモリ エラーまたは設定エラーが原因であると思われます。
DN「%2s」のユーザ プロパティ「%1s」をフェッチできませんでした	SmLdapMessage::FailedTo-FetchUserPropertyForDN	指定された DN が、ユーザ ディレクトリ用に設定された LDAP サーバ上に存在しないか、指定されたプロパティを持っていません。たとえば、SiteMinderSDK アプリケーションが、存在しないグループに対してユーザを追加しようとすると、このようなエラーが発生する場合があります。
LDAP メッセージを解析できませんでした。	SmLdapMessage::Ldap-ParseMsgFail	LDAP サーバから無効なレスポンスを受け取りました。LDAP サーバは正常に稼働していますか。
サーバ側のレスポンス並べ替えコントロールを解析できませんでした	SmLdapMessage::Parsing-ServerSideResponse-ControlFail	LDAP サーバからのレスポンスを解析できません。LDAP サーバは正常に稼働していますか。
レスポンス仮想リスト表示コントロールを解析できませんでした	SmLdapMessage::Virtual-ListViewResponseControlFail	LDAP サーバからのレスポンスを解析できません。LDAP サーバは正常に稼働していますか。

エラー メッセージ	関数	説明
証明書 DB の場所をレジストリから取得できませんでした	SmLdapMessage::Retrieve-CertDBRegFailed	HKLM¥Software¥Netegrity¥SiteMinder¥CurrentVersion¥LdapPolicyStore¥CertDbPath レジストリ エントリが見つかりませんでした。そのエントリを作成し、SSL 証明書データベースの適切なパスを入力してください。SSL 接続を使用しない場合は、空のままにします。UNIX システムでは、<install-dir>/registry 内の sm.registry ファイルを使用します。
サーバ側の LDAP 並べ替えコントロールを解析できませんでした	SmLdapMessage::Server-SideSortingLdapExecFail	LDAP サーバからのレスポンスを解析できません。LDAP サーバは正常に稼働していますか。
ポリシー ストア内のアクティブな式エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::Admin-LimitExceedSearchFor-ActiveExpr	ポリシー ストア内のアクティブな式の検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシー ストア内のエージェント エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_Device	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のエージェント コマンド エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_AgentCommand	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。

エラー メッセージ	関数	説明
ポリシー ストア内のエージェント グループ エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_DeviceGroup	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のエージェント キー エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_AgentKey	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のエージェント タイプ エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::Admin-LimitExceedSearchFor-AgentType	ポリシー ストア内のエージェント タイプの検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシー ストア内のエージェント タイプ属性エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::Admin-LimitExceedSearchFor-AgentTypeAttr	ポリシー ストア内のエージェント タイプ属性の検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシー ストア内の認証/許可マップ エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_AuthAzMap	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。

エラー メッセージ	関数	説明
ポリシー ストア内の証明書マップ エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_CertMap	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のドメイン エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::LdapAdmin-SizeLimitExceeded_Domain	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のキー管理エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::LdapAdmin-SizeLimit-Exceeded_KeyManagement	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内の ODBC クエリ エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_ODBCQuery	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。

エラー メッセージ	関数	説明
ポリシー ストア内のパスワード ポリシー エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_PasswordPolicy	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のポリシー エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_Policy	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のポリシー リンク エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_PolicyLink	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のプロパティ エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::Admin-LimitExceedSearchFor-Property	ポリシー ストア内のプロパティ オブジェクトの検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシー ストア内のプロパティ コレクション エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::Admin-LimitExceedSearchFor-PropertyCollection	ポリシー ストア内のプロパティ コレクションの検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。

エラー メッセージ	関数	説明
ポリシー ストア内のサーバ コマンド エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::AdminLimit-ExceedSearchForProperty-Section	ポリシー ストア内のプロパティ セクションの検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシー ストア内のレルム エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::LdapAdmin-SizeLimitExceeded_Realm	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のレスポンス エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_Response	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のレスポンス属性エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::AdminLimit-ExceedSearchForRespAttr	ポリシー ストア内のレスポンス属性の検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシー ストア内のレスポンス グループ エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::AdminLimit-ExceedSearchForRespGroup	ポリシー ストア内のレスポンス グループの検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシー ストア内のルート設定エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::AdminLimit-ExceedSearchForRootConfig	ポリシー ストアにはルート設定オブジェクトを 1 つしか置くことができないので、このようなエラーが発生してはいけません。ポリシー ストアが破損している可能性があります。

エラー メッセージ	関数	説明
ポリシー ストア内のルール エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::AdminLimit-ExceedSearchForRule	ポリシー ストア内のルールの検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシー ストア内のルール グループ エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::AdminLimit-ExceedSearchForRuleGroup	ポリシー ストア内のルール グループの検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシー ストア内の方式エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::AdminLimit-ExceedSearchForScheme	ポリシー ストア内の認証方式の検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシー ストア内の自己登録エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::AdminLimit-ExceedSearchForSelfReg	ポリシー ストア内の登録方式の検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシー ストア内のサーバ コマンド エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::Admin-LimitExceedSearchForServer-Command	ポリシー ストア内のサーバ コマンドの検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシー ストア内の共有秘密キーポリシー エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::Admin-LimitExceedSearchFor-SharedSecretPolicy	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。

エラー メッセージ	関数	説明
ポリシー ストア内のタグ付き文字列エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::Admin-LimitExceedSearchFor-TaggedString	ポリシー ストア内のタグ付き文字列の検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシー ストア内のトラステッド ホスト エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::Admin-LimitExceedSearchFor-TrustedHost	ポリシー ストア内のトラステッド ホストの検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシー ストア内のユーザ ディレクトリ エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::Admin-LimitExceedSearchForUser-Directory	ポリシー ストア内のユーザ ディレクトリの検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシー ストア内のユーザ ポリシー エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::Admin-LimitExceedSearchForUser-Policy	ポリシー ストア内のユーザ ポリシーの検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシー ストア内の変数エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::Admin-LimitExceedSearchForVariable	ポリシー ストア内の変数の検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。
ポリシー ストア内の変数のタイプ エントリの検索で LDAP 管理制限を超えました	SmLdapMessage::Admin-LimitExceedSearchFor-VariableType	ポリシー ストア内の変数のタイプの検索で、LDAP インスタンスの設定に使用された検索制限を超えました。LDAP サーバ側の検索制限の値を増やしてください。

エラー メッセージ	関数	説明
ポリシー ストア内の管理者エントリの検索で LDAP 管理サイズ制限を超えました	SmLdapMessage::LdapAdmin-SizeLimitExceeded_Admin	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
IMSEnvironments の Domain_FetchProperty 内の LDAP エラー - IMS オブジェクトについてサポートされていないポリシー ストア バージョン	SmLdapMessage::Error-DomainFetchIMSEnv	ポリシー サーバのバージョンは 5.1 以上である必要があります。
IMSEnvironments の Domain_SaveProperty 内の LDAP エラー - IMS オブジェクトについてサポートされていないポリシー ストア バージョン	SmLdapMessage::Error-DomainSaveIMSEnv	ポリシー サーバのバージョンは 5.1 以上である必要があります。
ポリシー ストア内のアクティブな式エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForActiveExpr	ポリシー ストア内のアクティブな式の検索で、LDAP インスタンスの設定に使用されたサイズ制限を超えました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシー ストア内の管理者エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::LdapSize-LimitExceeded_Admin	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。

エラー メッセージ	関数	説明
ポリシー ストア内のエージェント エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::LdapSize-LimitExceeded_Device	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のエージェント コマンド エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::LdapSize-LimitExceeded_Agent-Command	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のエージェント グループ エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::LdapSize-LimitExceeded_DeviceGroup	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のエージェント キー エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::LdapSize-LimitExceeded_AgentKey	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のエージェント タイプ エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForAgentType	ポリシー ストア内のエージェント タイプの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超えました。LDAP サーバ側のサイズ制限の値を増やしてください。

エラー メッセージ	関数	説明
ポリシー ストア内のエージェント タイプ属性エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForAgent-TypeAttr	ポリシー ストア内のエージェント タイプ属性の検索で、LDAP インスタンスの設定に使用されたサイズ制限を超えました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシー ストア内の認証/許可マップ エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::LdapSize-LimitExceeded_AuthAzMap	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内の証明書マップ エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::LdapSize-LimitExceeded_CertMap	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のドメイン エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::LdapSize-LimitExceeded_Domain	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のキー管理エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::LdapSize-Limit-Exceeded_KeyManagement	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。

エラー メッセージ	関数	説明
ポリシー ストア内の ODBC クエリ エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::LdapSize-LimitExceeded_ODBCQuery	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のパスワード ポリシー エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::LdapSize-Limit-Exceeded_PasswordPolicy	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のポリシー エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::LdapSize-LimitExceeded_Policy	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のポリシー リンク エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::LdapSize-LimitExceeded_PolicyLink	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のプロパティ エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForProperty	ポリシー ストア内のプロパティ オブジェクトの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超えました。LDAP サーバ側のサイズ制限の値を増やしてください。

エラー メッセージ	関数	説明
ポリシー ストア内のプロパティ コレクション エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForProperty-Collection	ポリシー ストア内のプロパティ コレクションの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超えました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシー ストア内のプロパティ セクション エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForProperty-Section	ポリシー ストア内のプロパティ セクションの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超えました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシー ストア内のレルム エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::LdapSize-LimitExceeded_Realm	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のレスポンス エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::LdapSize-LimitExceeded_Response	特定の LDAP サーバのサイズ制限を確認してください (LDAP サーバのマニュアルを参照)。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のレスポンス属性エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForResponse-Attr	ポリシー ストア内のレスポンス属性の検索で、LDAP インスタンスの設定に使用されたサイズ制限を超えました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシー ストア内のレスポンス グループ エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForRespGroup	ポリシー ストア内のレスポンス グループの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超えました。LDAP サーバ側のサイズ制限の値を増やしてください。

エラー メッセージ	関数	説明
ポリシー ストア内のルート設定エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForRootConfig	ポリシー ストアにはルート設定オブジェクトを 1 つしか置くことができないので、このようなエラーが発生してはいけません。ポリシー ストアが破損している可能性があります。
ポリシー ストア内のルール エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForRule	ポリシー ストア内のルールの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超えました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシー ストア内のルール グループ エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForRuleGroup	ポリシー ストア内のルール グループの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超えました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシー ストア内の方式エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForScheme	ポリシー ストア内の認証方式の検索で、LDAP インスタンスの設定に使用されたサイズ制限を超えました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシー ストア内の自己登録エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForSelfReg	ポリシー ストア内の登録方式の検索で、LDAP インスタンスの設定に使用されたサイズ制限を超えました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシー ストア内のサーバ コマンド エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForServer-Command	ポリシー ストア内のサーバ コマンドの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超えました。LDAP サーバ側のサイズ制限の値を増やしてください。

エラー メッセージ	関数	説明
ポリシー ストア内の共有秘密キー ポリシー エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForShared-SecretPolicy	特定の LDAP サーバのサイズ制限を確認してください（LDAP サーバのマニュアルを参照）。また、SiteMinder 管理 UI を実行して、SiteMinder がこの LDAP サーバについて使用するサイズ制限を確認してください。この制限をサーバ設定と同じにします。
ポリシー ストア内のタグ付き文字列エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForTaggedString	ポリシー ストア内のタグ付き文字列の検索で、LDAP インスタンスの設定に使用されたサイズ制限を超えました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシー ストア内のトラステッド ホスト エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForTrustedHost	ポリシー ストア内のトラステッド ホストの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超えました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシー ストア内のユーザ ディレクトリ エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForUser-Directory	ポリシー ストア内のユーザ ディレクトリの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超えました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシー ストア内のユーザ ポリシー エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForUserPolicy	ポリシー ストア内のユーザ ポリシーの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超えました。LDAP サーバ側のサイズ制限の値を増やしてください。
ポリシー ストア内の変数エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForVariable	ポリシー ストア内の変数の検索で、LDAP インスタンスの設定に使用されたサイズ制限を超えました。LDAP サーバ側のサイズ制限の値を増やしてください。

エラー メッセージ	関数	説明
ポリシー ストア内の変数のタイプ エントリの検索で LDAP サイズ制限を超えました	SmLdapMessage::SizeLimit-ExceedSearchForVariableType	ポリシー ストア内の変数のタイプの検索で、LDAP インスタンスの設定に使用されたサイズ制限を超えました。LDAP サーバ側のサイズ制限の値を増やしてください。
入力された文字列の長さが、制限を超えています。詳細については、LDAP ストアのマニュアルを参照してください。	SmLdapMessage::Ldap-LengthConstrain-Violation_CertMap	検索で使用された値が長すぎました。
PingServer 内の SmDsLdapConnMgr（ldap_search_ext_s）: %1s	SmLdapMessage::ErrorLdap-ConnMgrPingServer	LDAP サーバに接続できません。LDAP サーバが稼働していることと、ポートが正しいことを確認してください（ポリシー サーバ マシンから ping を実行してみてください）。
SmDsLdapConnMgr バインド - 初期化。サーバ %1s: %2ul	SmLdapMessage::LdapConn-MgrBindInitFail	LDAP サーバに接続できません。LDAP サーバが稼働していることと、ポートが正しいことを確認してください（ポリシー サーバ マシンから ping を実行してみてください）。
SmDsLdapConnMgr バインド - SetOption CONNECT_TIMEOUT %1i。サーバ %2s: %3ul	SmLdapMessage::LdapConn-MgrBindSetOptionConnect-Timeout	LDAP オプションを設定できません。詳細については、エラー文字列を確認してください。
SmDsLdapConnMgr バインド - SSL 初期化。サーバ %1s: %2ul	SmLdapMessage::LdapConn-MgrBindSSLInitFail	SSL を使用して LDAP サーバに対して初期化できません。LDAP サーバおよびポートを確認してください。LDAP サーバが SSL 用に設定されていることを確認してください。
SmDsLdapConnMgr バインド。サーバ %1s: %2ul。エラー %3i - %4s	SmLdapMessage::ErrorLdap-ConnMgrBind	LDAP サーバに接続できません。LDAP サーバが稼働していることと、ポートが正しいことを確認してください（ポリシー サーバ マシンから ping を実行してみてください）。

エラー メッセージ	関数	説明
SmDsLdapConnMgr 例外(ldap_init)。 サーバ %1s: %2ul	SmLdapMessage::Unknow-ExceptionLdapConnMgrInit	LDAP サーバへの接続中に予期しないエラーが発生しました。LDAP サーバおよびポートの設定を確認してください。
SmDsLdapConnMgr 例外(ldap_simple_bind_s)。 サーバ %1s: %2ul	SmLdapMessage::Unknown-ExceptionLdapConnMgrSimpleBind	LDAP サーバへの接続中に予期しないエラーが発生しました。LDAP サーバおよびポートの設定を確認してください。
SmDsLdapConnMgr 例外(ldapssl_init)。 サーバ %1s: %2ul	SmLdapMessage::Unknow-ExceptionLdapConnMgrSSLInit	SSL を使用して LDAP サーバに接続しているときに、予期しないエラーが発生しました。LDAP サーバおよびポートの設定を確認してください。サーバは SSL 用に設定されていますか。
SmObjLdap で LDAP サーバ %1s にバインドできませんでした: %3s としての %2i。LDAP エラー %4i - %5s	SmLdapMessage::SmObj-LdapFailToBindToLdapServer	LDAP サーバに接続できません。LDAP サーバが稼働していることと、ポートが正しいことを確認してください (ポリシー サーバ マシンから ping を実行してみてください)。
SmObjLdap で %1s への LDAP 接続を初期化できません 初期化できませんでした: %2i	SmLdapMessage::SmObj-LdapInitLdapConnFail	LDAP サーバに接続できません。LDAP サーバが稼働していることと、ポートが正しいことを確認してください (ポリシー サーバ マシンから ping を実行してみてください)。
SmObjLdap で %1s への SSL LDAP 接続を初期化できませんでした: %2i	SmLdapMessage::SmObj-LdapInitSSLLdapFail	LDAP オプションを設定できません。ポリシー サーバ システム上の設定エラーが原因であると思われます。適切な LDAP ライブラリを使用していますか。
SmObjLdap で %1s を使用して SSL を初期化できませんでした	SmLdapMessage::SmObj-LdapInitSSLFail	SSL を使用して LDAP サーバに対して初期化できません。LDAP サーバおよびポートを確認してください。LDAP サーバが SSL 用に設定されていることを確認してください。

エラー メッセージ	関数	説明
SmObjLdap で LDAP TIMELIMIT オプションを設定できませんでした	SmLdapMessage::SmObj-LdapConnectTimeoutOptFail	LDAP オプションを設定できません。ポリシー サーバ システム上の設定エラーが原因であると思われます。適切な LDAP ライブラリを使用していますか。
SmObjLdap で LDAP PROTOCOL V3 オプションを設定できませんでした	SmLdapMessage::SmObj-LdapProtocolV3OptFail	LDAP オプションを設定できません。ポリシー サーバ システム上の設定エラーが原因であると思われます。適切な LDAP ライブラリを使用していますか。
SmObjLdap で LDAP TIMELIMIT オプションを設定できませんでした	SmLdapMessage::SmObj-LdapReconnectOptFail	LDAP オプションを設定できません。ポリシー サーバ システム上の設定エラーが原因であると思われます。適切な LDAP ライブラリを使用していますか。
SmObjLdap で LDAP TIMELIMIT オプションを設定できませんでした	SmLdapMessage::SmObjLdap-ThreadFnOptFail	LDAP オプションを設定できません。ポリシー サーバ システム上の設定エラーが原因であると思われます。適切な LDAP ライブラリを使用していますか。
SmObjLdap で LDAP TIMELIMIT オプションを設定できませんでした	SmLdapMessage::SmObjLdap-TimeoutOptFail	LDAP オプションを設定できません。ポリシー サーバ システム上の設定エラーが原因であると思われます。適切な LDAP ライブラリを使用していますか。
SmObjLdap で LDAP_OPT_REFERRALS オプションを設定できませんでした	SmLdapMessage::SmObj-LdapOptReferralsFail	LDAP オプションを設定できません。ポリシー サーバ システム上の設定エラーが原因であると思われます。適切な LDAP ライブラリを使用していますか。
SmObjLdapConnMgr Bind - init。サーバ: %1s: %2ul	SmLdapMessage::SmObj-LdapConnMgrBindinitServer	ポリシー ストア用に設定された LDAP サーバを初期化できませんでした。エラー メッセージの中で示された LDAP サーバをトラブルシューティングしてください。

エラー メッセージ	関数	説明
SmObjLdapConnMgr Bind - SetOption CONNECT_TIMEOUT %1i。サーバ %2s：%3ul	SmLdapMessage::SmObj-LdapConnMgrBindSetOption-CONNECT_TIMEOUT	ポリシー ストア用に設定された LDAP サーバで、LDAP_X_OPT_CONNECT_TIMEOUT オプション（Microsoft Active Directory SDK を使用しているときは LDAP_OPT_SEND_TIMEOUT）を設定できませんでした。エラー メッセージの中で示された LDAP サーバをトラブルシューティングしてください。
SmObjLdapConnMgr Bind - SSL client init。サーバ：%1s：%2ul、証明書 DB：%3s	SmLdapMessage::SmObj-LdapConnMgrBindSSLclientinit	ポリシー ストア用に設定された LDAP サーバへの SSL 接続のクライアント側の初期化に失敗しました。証明書データベースが正しく指定されているかどうかを確認してください。
SmObjLdapConnMgr Bind - SSL init。サーバ：%1s：%2ul	SmLdapMessage::SmObj-LdapConnMgrBindSSLinit	ポリシー ストア用に設定された LDAP サーバを SSL 接続時に初期化できませんでした。エラー メッセージの中で示された LDAP サーバをトラブルシューティングしてください。
SmObjLdapConnMgr バインド。サーバ %1s：%2ul。エラー %3i - %4s	SmLdapMessage::SmObj-LdapConnMgrBindServerError	SiteMinder ポリシー サーバから、ポリシー ストア用に設定された LDAP サーバにバインドできませんでした。詳細については、LDAP エラー メッセージを参照してください。ポリシー サーバで有効な LDAP 管理者クレデンシャルが使用されているかどうかも確認してください。クレデンシャルは、ポリシー サーバ管理コンソールの［データ］タブでリセットできます。
SmObjLdapConnMgr 例外（ldap_init）。サーバ %1s：%2ul	SmLdapMessage::ExcpSm-ObjLdapConnMgrldap_init	ポリシー ストア用に設定された LDAP サーバを初期化できませんでした。エラー メッセージの中で示された LDAP サーバをトラブルシューティングしてください。

エラー メッセージ	関数	説明
SmObjLdapConnMgr 例外(ldap_simple_bind_s)。 サーバ %1s: %2ul	SmLdapMessage::ExcpSm-ObjLdapConnMgrldap_simple_-bind_s	SiteMinder ポリシー サーバから、ポリシー ストア用に設定された LDAP サーバにバインドできませんでした。ポリシー サーバで有効な LDAP 管理者クレデンシャルが使用されているかどうかを確認してください。クレデンシャルは、ポリシー サーバ管理コンソールの[データ]タブでリセットできます。
SmObjLdapConnMgr 例外(ldapssl_client_init)。 サーバ %1s: %2ul	SmLdapMessage::ExcpSm-ObjLdapConnMgrldap-ssl_client_init	ポリシー ストア用に設定された LDAP サーバへの SSL 接続のクライアント側の初期化に失敗しました。証明書データベースが正しく指定されているかどうかを確認してください。
SmObjLdapConnMgr 例外(ldapssl_init)。 サーバ %1s: %2ul	SmLdapMessage::ExcpSm-ObjLdapConnMgrldapssl_init	ポリシー ストア用に設定された LDAP サーバを SSL 接続時に初期化できませんでした。エラー メッセージの中で示された LDAP サーバをトラブルシューティングしてください。
サーバ/プロセスを終了しています.....	SmLdapMes-sage::Terminating Server-Processes	重要な再設定が行われるように、サーバ プロセスをシャットダウンします。ログ内の前のエラーを参照してください。

エラー メッセージ	関数	説明
%1i を超えるデータ エントリをデータ ストアからフェッチできません。¥n %2s LDAP_SIZELIMIT_EXCEEDED。エラーが検出されました。¥n %3s ディレクトリ サーバの sizelimit パラメータを再設定するか、¥n %4s（ディレクトリ サーバのマニュアルを参照）¥n %5s ディレクトリ サーバをルート DN にバインドして、この問題を解決してください。¥n %6s 例: Iplanet / Netscape の場合は、ディレクトリ サーバを「cn=Directory Manager」としてバインドしてください	SmLdapMessage::Unable-ToFetchMoreEntriesFromData-Source	LDAP サーバの sizelimit パラメータの値を増やしてください。
LDAP ディレクトリ タイプを取得できません	SmLdapMessage::Unable-ToRetrieveLdapDir	LDAP のベンダーとタイプを判別できません。ターゲット サーバはサポートされている LDAP サーバのうちの 1 つですか。処理は続行されますが、予期しないエラーがさらに発生する場合があります。
データ ストアからこれ以上データ エントリを検索してフェッチすることができません。¥n %1s LDAP_SIZELIMIT_EXCEEDED。エラーが検出されました。¥n %2s ディレクトリ サーバの sizelimit パラメータを再設定するか ¥n %3s（ディレクトリ サーバのマニュアルを参照）、¥n %4s ディレクトリ サーバをルート DN にバインドして、この問題を解決してください。¥n %5s 例: Iplanet / Netscape の場合は、ディレクトリ サーバを「cn=Directory Manager」としてバインドしてください	SmLdapMessage::Unable-ToSearchFetchMore-EntriesFromDataSource	ポリシー サーバで、ディレクトリ サーバのデータをこれ以上取得できません。可能な設定変更があるかどうか、エラー メッセージ テキストを参照してください。

エラー メッセージ	関数	説明
rebindproc %1i の「arg」引数の値が想定外です	SmLdapMes-sage::UnexpectedValueArg-Argument	rebindproc コールで「arg」引数として不正な値が渡されています。rebindproc 関数は、自動リフェラル処理のための再バインド コールバックとして設定されます。代わりに、拡張リフェラル処理を有効にしてください。
rebindproc_sm %1i の「arg」引数の値が %1i	SmLdapMes-sage::UnexpectedValueArg-Argument2	rebindproc_sm コールで「arg」引数として不正な値が渡されています。rebindproc_sm 関数は、自動リフェラル処理のための再バインド コールバックとして設定されます。代わりに、拡張リフェラル処理を有効にしてください。
rebindproc_sm %1i の「freeit」引数の値が %1i	SmLdapMes-sage::UnexpectedValueFreeit-Argument	rebindproc コールで freeit 引数として不正な値が渡されています（許可されるのは 0 または 1 だけです）。rebindproc 関数は、自動リフェラル処理のための再バインド コールバックとして設定されます。代わりに、拡張リフェラル処理を有効にしてください。
rebindproc_sm %1i の「freeit」引数の値が %1i	SmLdapMes-sage::UnexpectedValue-FreeitArgument2	rebindproc_sm コールで freeit 引数として不正な値が渡されています（許可されるのは 0 または 1 だけです）。rebindproc_sm 関数は、自動リフェラル処理のための再バインド コールバックとして設定されます（Microsoft Active Directory SDK を使用している場合を除きます）。代わりに、拡張リフェラル処理を有効にしてください。

ODBC

エラー メッセージ	関数	説明
IMS 環境を保存できませんでした。スキーマ サポートがない可能性があります	SmOdbcMessage::IMSSave-ErrorMissingSchema	ポリシー サーバ データベースには IMS をサポートするスキーマがありません。
クエリ実行時のデータベース エラー。不明の障害です	SmOdbcMessage::Unknown-FailureDBExecQuery	指定された SQL ステートメントを実行しようとしているときに、不明なエラーまたは例外が発生しました。
クエリ実行時のデータベース エラー。不明の障害です	SmOdbcMessage::Unknown-FailureExecODBCQuery	指定された SQL ステートメントを実行しようとしているときに、不明なエラーまたは例外が発生しました。
クエリ実行時のデータベース エラー。エラー: %2s	SmOdbcMessage::DBError-ExecQuery	指定された SQL ステートメントを実行しようとしているときに、特定のエラーが発生しました。
クエリ実行時のデータベース エラー。不明の障害です	SmOdbcMessage::Unknown-ExceptionDBExecQuery	指定された SQL ステートメントを実行しようとしているときに、不明なエラーまたは例外が発生しました。
クエリ実行時のデータベース エラー。エラー: %1s	SmOdbcMessage::ErrorDB-ExecQuery	SQL クエリを実行しようとしているときに、特定のエラーが発生しました。
エスケープ文字取得中のデータベース エラー。エラー: %1s	SmOdbcMessage::DBError-GetEscapeChar	データベースで使用するエスケープ文字を確立しようとしているとき、エラーが発生しました。
エスケープ文字取得中のデータベース エラー: 不明の障害	SmOdbcMessage::Unknown-ExceptionDBGetEscapeChar	データベースで使用するエスケープ文字を確立しようとしているとき、不明の例外が発生しました。
DB 警告: データ値で切り捨てが行われます:「%1s」 実際の長さ:「%2u」 許可されている最大文字数:「%3u」	SmOdbcMessage::Data-TruncationInfo	指定された入力用のデータ値が、許可されている最大文字数を超えました。値は、指定されている最大文字数に切り捨てられます。
エラー コードは %1i、メッセージは「%2s」です	SmOdbcMessage::ErrorCode-AndMessage	指定されたデータ ソースに接続しようとしているとき、エラーが発生しました。問題を示すエラー コードとエラー メッセージが表示されます。

エラー メッセージ	関数	説明
エラー コードは %1i です	SmOdbcMessage::ErrorCode	指定されたデータ ソースに接続しようとしているとき、エラーが発生しました。問題を示すエラー コードが表示されます。
OID「%1s」でユーザ ディレクトリのクエリをフェッチできませんでした	SmOdbcMessage::FailedTo-AllocMemForUserDir	指定の OID によって指定されるユーザ ディレクトリで使用するクエリを割り当てることができませんでした。
データ ソース「%1s」のいずれにも接続できませんでした	SmOdbcMessage::FailedTo-ConnectToAnyOfDataSources	指定されたユーザ ディレクトリのいずれにも接続できませんでした。
データ ソース「%1s」に接続できませんでした	SmOdbcMessage::FailedTo-ConnectToDataSource	指定されたデータ ソースに接続しようとしているとき、エラーが発生しました。
OID「%1s」でユーザ ディレクトリのクエリをフェッチできませんでした	SmOdbcMessage::FailedTo-FetchQueryForUserDir	指定の OID を使用してユーザ ディレクトリ クエリを検索できませんでした。
OID「%1s」でユーザ ディレクトリをフェッチできませんでした	SmOdbcMessage::FailedTo-FetchUserDir	指定の OID を使用してユーザ ディレクトリを検索できませんでした。
データベース「%1s」のデータ ソース名が見つかりませんでした	SmOdbcMessage::FailedTo-FindDataSource	指定された SiteMinder データベースの「ProviderNameSpace」レジストリ キーが見つかりませんでした。
%1s のクエリ定義が見つかりませんでした	SmOdbcMessage::FailTo-FindQueryDefinition	指定されたクエリのクエリ定義が見つかりませんでした。
DataDirect ODBC ドライバを初期化できませんでした。ライブラリ「%2s」内の関数「%1s」をロードできません	DataDirectODBCDriverFunc-LoadFail	DataDirect ODBC ライブラリを初期化できませんでした。指定された初期化関数が、指定のライブラリ内に見つかりませんでした。
DataDirect ODBC ドライバを初期化できませんでした。ライブラリ「%1s」をロードできません	SmOdbcMessage::DataDirect-ODBCDriverLibLoadFail	指定された ODBC ライブラリをロードできませんでした。ライブラリ パスに SiteMinder ODBC ライブラリ ディレクトリが含まれているかどうかを確認してください。

エラー メッセージ	関数	説明
ODBC ブランド設定ライブラリ「%1s」をロードできませんでした	SmOdbcMessage::ODBC-BrandingLibraryLoadFail	SiteMinder によって使用されるようにブランド設定された ODBC ライブラリをロードできませんでした。
ODBC ブランド設定ライブラリの名前を解決できませんでした	SmOdbcMessage::ODBC-BrandingLibraryNameResolve-Fail	ブランド設定ライブラリの名前を解決できませんでした。このライブラリ名は、Netegrity/Siteminder/Database 以下のレジストリ内にある Key OdbcBrandingLib レジストリ キーから指定されます。
データベース「%1s」のデータベース レジストリ キーを取得できませんでした	SmOdbcMessage::FailedTo-RetrieveDBRegKeys	指定された SiteMinder データベースのレジストリ キー (データ ソース、ユーザ名、またはパスワード) のうちの 1 つが見つかりませんでした。
クレデンシャルが無効であるか、「%1s」サーバ「%2s」に接続を試みているサーバが見つかりません	SmOdbcMessage::Unable-ToConnect	SiteMinderODBC データベースへのアクセスのために入力されたクレデンシャルが無効です。
クエリ実行時の ODBC エラー (「%1s」)。エラー: %2s	SmOdbcMessage::ErrorExec-ODBCQuery	指定された SQL ステートメントを実行しようとしているときに、特定の ODBC エラーが発生しました。
クエリ実行時の ODBC エラー。エラー: %1s	SmOdbcMessage::Error-ODBCQueryExec	SQL クエリを実行しようとしているときに、特定の ODBC エラーが発生しました。
クエリ実行時の ODBC エラー。不明の障害です	SmOdbcMessage::Unknown-ExceptionExecODBCQuery	ODBC データベースに対して SQL クエリを実行しようとしているときに、不明の例外が発生しました。

ディレクトリ アクセス

メッセージ	メッセージ ID	説明
パス「%2s」で %1s に失敗しました	FuncFailForPath	ポリシー サーバで、カスタム プロバイダを使用してディレクトリ情報を取得できませんでした。
ADs EnumContainer に失敗しました。エラー %1xl。%2s	ADsEnumContainerFailed	ポリシー サーバで、ADSI インターフェースからコンテナ メンバを列挙できませんでした。
プロパティ「%1s」について ADs Get に失敗しました。 エラー %2xl。%3s	ADsGetFailForProperty	ポリシー サーバで、ADSI インターフェースからユーザ プロパティを取得できませんでした。
ADs GetGroups に失敗しました。 エラー %1xl。%2s	ADsGetGroupsFail	ポリシー サーバで、ユーザ グループを取得できませんでした。
プロパティ「%1s」について ADs Put に失敗しました。 エラー %2xl。%3s	ADsPutFailForProperty	ポリシー サーバで、ADSI インターフェースからユーザ プロパティを設定できませんでした。
ADs put_Filter に失敗しました。 エラー %1xl。%2s	ADsPutFilterFailed	ポリシー サーバで、ADSI インターフェースから列挙フィルタを作成できませんでした。
ADs Search に失敗しました。 エラー %1xl。%2s	ADsSearchFail	ポリシー サーバで、ADSI インターフェースから検索できませんでした。
ADsBuildEnumerator に失敗しました。エラー %1xl。%2s	ADsBuildEnumeratorFailed	ポリシー サーバで、ADSI インターフェースからコンテナ メンバを列挙できませんでした。
ADsBuildVarArrayStr に失敗しました。エラー %1xl。%2s	ADsBuildVarArrayStrFailed	ポリシー サーバで、ADSI インターフェースから変数の配列を作成できませんでした。
ADsEnumerateNext に失敗しました。 エラー %xl。%2s	ADsEnumerateNextFailed	ポリシー サーバで、ADSI インターフェースからコンテナ メンバを列挙できませんでした。

メッセージ	メッセージ ID	説明
ADsGetObject に失敗しました。エラー %1xl。%2s	ADsGetObjectFail	ポリシー サーバで、ADSI インターフェースからオブジェクト プロパティを取得できませんでした。
「%1s」で ADsOpenObject に「%1s」。ADSI エラー %2xl。%3s	ADsOpenObjectFailed	ポリシー サーバで、ADSI インターフェースへのハンドルを作成できませんでした。
アフィリエイトの PropertyCollection がグループ名と一致していません	AffiliatePropertyCollection-GroupNameMismatch	ポリシー サーバで、ポリシーに対するアフィリエイト リレーションシップを検証できませんでした。アフィリエイトのプロパティ コレクション名が、指定されたポリシー名に一致していません。
「%1s」関数を使用してプロパティをフェッチできませんでした	PropertiesFetchFail	ポリシー サーバで、カスタム プロバイダからオブジェクト プロパティをフェッチできませんでした。
SmDsObj で例外が発生しました	SmDsObjUnknownException	ポリシー サーバで、DS プロバイダを検索できませんでした。ポリシー サーバ プロセスによってプロバイダ共有ライブラリをロードできるかどうか確認してください。
SmDsObj で例外が発生しました: %1s	SmDsObjException	ポリシー サーバで、DS プロバイダを検索できませんでした。ポリシー サーバ プロセスによってプロバイダ共有ライブラリにアクセスできるかどうか確認してください。
アフィリエイトの PropertyCollections が見つかりませんでした	AffiliatePropertyCollectionsFail	ポリシー サーバで、アフィリエイト ドメインをフェッチできませんでした。ポリシー ストアの整合性を確認してください。
属性が見つかりませんでした	AttributeFindFail	ポリシー サーバで、指定されたユーザ属性が見つかりませんでした。
パスワード プロパティがプロパティ	PasswordPropertyFindFail	ポリシー サーバで、指定されたアフィリエイトのパスワードが見つかりませんでした。

メッセージ	メッセージ ID	説明
アフィリエイト ユーザとして機能している PropertySection でプロパティが見つかりませんでした	AffilateUserPropertyIn-PropertySectionFindFail	ポリシー サーバで、指定されたアフィリエイト プロパティをフェッチできませんでした。
アフィリエイト ユーザ ディレクトリとして機能している Property-Collection が見つかりませんでした	ActingAffiliateUserDirProps-FindFail	ポリシー サーバで、アフィリエイトドメインをフェッチできませんでした。ポリシー ストアの整合性を確認してください。
アフィリエイト ユーザとしての PropertySection が 見つかりませんでした	AffilateUserPropertySection-FindFail	ポリシー サーバで、指定されたアフィリエイトを検索できませんでした。
アフィリエイト ユーザ ディレクトリに PropertySection が見つかりませんでした	InAffiliateUserDirPropsFindFail	ポリシー サーバで、アフィリエイトドメインからアフィリエイトをフェッチできませんでした。ポリシー ストアの整合性を確認してください。
ルート オブジェクトが見つかりませんでした	RootObjFindFail	ポリシー サーバで、アフィリエイトドメインが見つかりませんでした。SiteMinder の管理 UI を使用したときにアフィリエイト オブジェクトが表示されるかどうか確認してください。
アフィリエイトの PropertyCollection にユーザが見つかりませんでした	AffiliatePropertyCollection-UserFindFail	ポリシー サーバで、指定されたアフィリエイトを検索できませんでした。
カスタム ディレクトリ API モジュール「%1s」を初期化できませんでした	CustomDirAPIModInitFail	ポリシー サーバで、カスタム プロバイダ ライブラリを初期化できませんでした。
カスタム ディレクトリ API ライブラリ「%1s」をロードできませんでした。システム エラー: %2s	CustormDirAPILibLoadFail	ポリシー サーバで、カスタム プロバイダ ライブラリをロードできませんでした。ポリシー サーバ プロセスによって適切なカスタム プロバイダ ライブラリにアクセスできるかどうか確認してください。

メッセージ	メッセージ ID	説明
カスタム ディレクトリ API ライブラリ「%2s」内の関数「%1s」を解決できませんでした。システム エラー: %3s	CustormDirAPILibFuncResovl-Fail	ポリシー サーバで、カスタム プロバイダ ライブラリを初期化できませんでした。ポリシー サーバ プロセスによって適切なカスタム プロバイダ ライブラリにアクセスできるかどうか確認してください。
ネームスペース ADSI では、Get Disabled State はサポートされていません	ADSIGetDisabledState-Supported	ポリシー サーバでは、ADSI インターフェースからのユーザ無効状態の取得をサポートしていません。
カスタム ディレクトリ API ライブラリ「%2s」で関数「%1s」を使用できません。	CustomDirAPILibFunctNot-Found	ポリシー サーバで、必要なメソッドの 1 つがカスタム プロバイダ ライブラリ内に見つかりませんでした。ポリシー サーバ プロセスによって適切なカスタム プロバイダ ライブラリにアクセスできるかどうか確認してください。
ネームスペース ADSI では、パスワードの変更はサポートされていません	ADSINoPasswordChange	ポリシー サーバでは、ADSI インターフェースからのユーザ パスワードの変更をサポートしていません。
ネームスペース LanMan では、パスワードの変更がサポートされていません	LanManPasswordChangeNot-Supported	ポリシー サーバでは、LanMan プロバイダからのユーザ パスワードの変更をサポートしていません。
QueryInterface（IID_IADsContainer）に失敗しました。 エラー %1s %2s %3i。%4s	IID_IADsContainerFail	ポリシー サーバで、ADSI インターフェースからコンテナ メンバを列挙できませんでした。
QueryInterface（IID_IADsContainer）に失敗しました。 エラー %1xl。%2s	QueryInterfaceIID_IADs-ContainerFail	ポリシー サーバで、ADSI インターフェースからコンテナ メンバを列挙できませんでした。
QueryInterface（IID_IADsUser）に失敗しました。エラー %1xl。%2s	IID_IADsUserFail	ポリシー サーバで、ユーザ グループを取得できませんでした。

メッセージ	メッセージ ID	説明
QueryInterface（IID_IDirectorySearch）に失敗しました。エラー %1xl。%2s	IID_IDirectorySearchFail	ポリシー サーバで、ADSI インターフェースから検索できませんでした。
ネームスペース ADSI では、Set Disabled State はサポートされていません	ADSISetDisabledState-Supported	ポリシー サーバでは、ADSI インターフェースからのユーザ無効状態の設定をサポートしていません。
サポートされていない関数がコールされました：SmDirAddEntry	UnsupportedFuncCallSmDir-AddEntry	SmDirAddEntry 関数はアフィリエイト プロバイダ ライブラリによってサポートされていません。
サポートされていない関数がコールされました：SmDirAddMemberToGroup	UnsupportedFuncCallSmDir-AddMemberToGroup	SmDirAddMemberToGroup 関数はアフィリエイト プロバイダ ライブラリによってサポートされていません。
サポートされていない関数がコールされました：SmDirAddMemberToRole	UnsupportedFuncCallSmDir-AddMemberToRole	SmDirAddMemberToRole 関数はアフィリエイト プロバイダ ライブラリによってサポートされていません。
サポートされていない関数がコールされました：SmDirChangeUserPassword	UnsupportedFuncCallSmDir-ChangeUserPassword	SmDirChangeUserPassword 関数は、アフィリエイト プロバイダ ライブラリによってサポートされていません。
サポートされていない関数がコールされました：SmDirGetGroupMembers	UnsupportedFuncCallSmDir-GetGroupMembers	SmDirGetGroupMembers 関数はアフィリエイト プロバイダ ライブラリによってサポートされていません。
サポートされていない関数がコールされました：SmDirGetRoleMembers	UnsupportedFuncCallSmDir-GetRoleMembers	SmDirGetRoleMembers 関数はアフィリエイト プロバイダ ライブラリによってサポートされていません。
サポートされていない関数がコールされました：SmDirGetUserAttrMulti	UnsupportedFuncCallSmDir-GetUserAttrMulti	SmDirGetUserAttrMulti 関数はアフィリエイト プロバイダ ライブラリによってサポートされていません。
サポートされていない関数がコールされました：SmDirGetUserClasses	UnsupportedFuncCallSmDir-GetUserClasses	SmDirGetUserClasses 関数はアフィリエイト プロバイダ ライブラリによってサポートされていません。
サポートされていない関数がコールされました：SmDirGetUserGroups	UnsupportedFuncCallSmDir-GetUserGroups	SmDirGetUserGroups 関数はアフィリエイト プロバイダ ライブラリによってサポートされていません。

メッセージ	メッセージ ID	説明
サポートされていない関数がコールされました: SmDirGetUserProperties	UnsupportedFuncCallSmDir-GetUserProperties	SmDirGetUserProperties 関数はアフィリエイト プロバイダ ライブラリによってサポートされていません。
サポートされていない関数がコールされました: SmDirGetUserRoles	UnsupportedFuncCallSmDir-GetUserRoles	SmDirGetUserRoles 関数はアフィリエイト プロバイダ ライブラリによってサポートされていません。
サポートされていない関数がコールされました: SmDirLookup	UnsupportedFuncCallSmDir-Lookup	SmDirLookup 関数はアフィリエイト プロバイダ ライブラリによってサポートされていません。
サポートされていない関数がコールされました: SmDirRemoveEntry	UnsupportedFuncCallSmDir-RemoveEntry	SmDirRemoveEntry 関数はアフィリエイト プロバイダ ライブラリによってサポートされていません。
サポートされていない関数がコールされました: SmDirRemoveMemberFrom-Group	UnsupportedFuncCallSmDir-RemoveMemberFromGroup	SmDirRemoveMemberFromGroup 関数はアフィリエイト プロバイダ ライブラリによってサポートされていません。
サポートされていない関数がコールされました: SmDirRemoveMemberFrom-Role	UnsupportedFuncCallSmDir-RemoveMemberFromRole	SmDirRemoveMemberFromRole 関数はアフィリエイト プロバイダ ライブラリによってサポートされていません。
サポートされていない関数がコールされました: SmDirSearch	UnsupportedFuncCallSmDir-Search	SmDirSearch 関数はアフィリエイト プロバイダ ライブラリによってサポートされていません。
サポートされていない関数がコールされました: SmDirSearchCount	UnsupportedFuncCallSmDir-SearchCount	SmDirSearchCount 関数はアフィリエイト プロバイダ ライブラリによってサポートされていません。
サポートされていない関数がコールされました: SmDirSetUserAttr	UnsupportedFuncCallSmDir-SetUserAttr	SmDirSetUserAttr 関数はアフィリエイト プロバイダ ライブラリによってサポートされていません。
サポートされていない関数がコールされました: SmDirSetUserAttrMulti	UnsupportedFuncCallSmDir-SetUserAttrMulti	SmDirSetUserAttrMulti 関数はアフィリエイト プロバイダ ライブラリによってサポートされていません。

メッセージ	メッセージ ID	説明
サポートされていない関数がコールされました: SmDirSetUserDisabledState	UnsupportedFuncCallSmDir-SetUserDisabledState	SmDirSetUserDisabledState 関数はアフィリエイト プロバイダ ライブラリによってサポートされていません。

トンネル

エラー メッセージ	関数	説明
不正なセキュリティ ハンドシェイクが行われようとしました。ハンドシェイク エラー: %1i	SmTunnelMessage::Hand-shakeAttemptError	定義済みのシステム エラーが発生したため、クライアント/サーバ セキュリティ ハンドシェイクに失敗しました。
ハンドシェイク中、クライアントはデータを正常に暗号化できません	SmTunnelMessage::Client-EncryptFail	クライアント/サーバ セキュリティ ハンドシェイクに失敗しました。クライアントはそのハンドシェイク メッセージを適切に暗号化できませんでした。
ハンドシェイク試行中に例外がキャッチされました	SmTunnelMessage::ExcpIn-HandshakeAttempt	クライアント/サーバ セキュリティ ハンドシェイク中、未定義のエラーが発生しました。
トンネル サービス ライブラリ「%1s」を初期化できませんでした。%2s	SmTunnelMessage::Tunnel-ServiceLibInitFail	リクエストされたトンネル サービス ライブラリが初期化に失敗しました。
トンネル サービス ライブラリ「%1s」をロードできませんでした。システム エラー: %2s	SmTunnelMessage::Tunnel-ServiceLibLoadFail	リクエストされたトンネル サービス ライブラリをロードできませんでした。
トンネル サービス ライブラリ「%2s」内の関数「%1s」を解決できませんでした。システム エラー: %3s	SmTunnelMessage::Tunnel-ServiceLibFuncResolveFail	システム エラーが発生したため、リクエストされた関数が、リクエストされたトンネル サービス ライブラリ内で見つかりませんでした。

エラー メッセージ	関数	説明
ハンドシェイク エラー: hello メッセージ内のホスト名が不正です	SmTunnelMessage::Hand-shakeErrorBadHostname	クライアント/サーバ セキュリティ ハンドシェイクに失敗しました。クライアントからサーバへの初期メッセージに不正なホスト名が含まれていました。
ハンドシェイク エラー: hello メッセージ内のバージョン番号が不正です	SmTunnelMessage::Hand-shakeErrorBadVersionNo	クライアント/サーバ セキュリティ ハンドシェイクに失敗しました。クライアントからサーバへの初期メッセージに不正なバージョン番号が含まれていました。
ハンドシェイク エラー: クライアントの ack を受信できませんでした。ソケット エラー %1i	SmTunnelMessage::Hand-shakeErrorToReceiveClientACK	クライアント/サーバ セキュリティ ハンドシェイクに失敗しました。サーバからクライアントへの初期メッセージが、クライアントによって受信確認されませんでした。
ハンドシェイク エラー: クライアントの hello メッセージを受信できませんでした。クライアントが切断されました	SmTunnelMessage::Hand-shakeErrorClientHelloNot-Receive	クライアント/サーバ セキュリティ ハンドシェイクに失敗しました。クライアントが初期メッセージを送信する前に接続を切断しました。
ハンドシェイク エラー: クライアントの hello メッセージを受け取れませんでした。ソケット エラー %1i	SmTunnelMessage::Hand-shakeErrorSocketError	クライアント/サーバ セキュリティ ハンドシェイクに失敗しました。クライアントが初期メッセージを送信しませんでした。
ハンドシェイク エラー: サーバの hello メッセージを送信できませんでした。ソケット エラー %1i	SmTunnelMessage::Hand-ShakeErrorInSendSocketError	クライアント/サーバ セキュリティ ハンドシェイクに失敗しました。通信障害が発生したため、サーバからクライアントへの初期メッセージを送信できませんでした。
ハンドシェイク エラー: このクライアントの共有秘密キーが不正です	SmTunnelMessage::Hand-shakeErrorSharedSecret-Incorrect	クライアント/サーバ セキュリティ ハンドシェイクに失敗しました。クライアントからサーバへの初期メッセージに不正な共有秘密キーが含まれていました。

エラー メッセージ	関数	説明
このポリシー サーバ バージョンは 3.6 エージェントをサポートしていません	SmTunnelMessage::Agent-VersionNotSupported	クライアント/サーバ セキュリティ ハンドシェイクに失敗しました。このバージョンのクライアントは、トンネル接続を確立することを許可されていません。
トンネル コーラーはリクエスト %1ul の実行を許可されていません	SmTunnelMessage::Tunnel-CallerExecDenied	トンネル コールで、禁止されているリクエストが行われようとしました。
予期しないハンドシェイク エラー	SmTunnelMessage::Hand-shakeErrorUnexpected	クライアント/サーバ セキュリティ ハンドシェイクが、予期しない理由で失敗しました。
トンネル ライブラリの発行中、予期しない例外がキャッチされました	SmTunnelMessage::Unknown-ExcpPublishTunnelLibs	トンネル サービス ライブラリがパブリッシング インターフェースを使用してそれ自身を記述しているときに、不明の例外が発生しました。

索引