IBM Security Directory Integrator
バージョン 7.2.0.1

パスワード同期プラグイン

SA88-7241-03
(英文原典：SC27-2708-03)

IBM Security Directory Integrator
バージョン 7.2.0.1

パスワード同期プラグイン

SA88-7241-03
(英文原典：SC27-2708-03)

お願い

本書および本書で紹介する製品をご使用になる前に、 109 ページの『特記事項』に記載されている情報をお読みください。

注: 本書は、*IBM Security Directory Integrator* ライセンス・プログラムのバージョン 7.2.0.1 (5724-K74)、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： SC27-2708-03
IBM Security Directory Integrator
Version 7.2.0.1
Password Synchronization Plug-ins

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

目次

本書について

本書には、IBM® Security Directory Integrator を構成するコンポーネントを使用してソリューションを開発する際に必要となる情報が記載されています。

IBM Security Directory Integrator の各コンポーネントは、ユーザー・ディレクトリーやその他のリソースを管理するネットワーク管理者向けのコンポーネントです。本書は、IBM Security Directory Integrator と IBM Security Directory Server の両方をインストールして使用した経験がある読者を想定しています。

また、本書は、IBM Security Directory Integrator を使用したソリューションの開発、インストール、管理を担当するユーザーを対象としています。本書の読者は、開発したソリューションの接続先となるシステムの概念や管理方法について習熟している必要があります。こうしたシステムには、ソリューションに応じて、以下に示す 1 つ以上の製品、システム、概念が含まれます (ただし、これらに限定されるわけではありません)。

- IBM Security Directory Server
- IBM Security Identity Manager
- IBM Java™ ランタイム環境 (JRE) または Oracle Java ランタイム環境
- Microsoft Active Directory
- Windows および UNIX オペレーティング・システム
- セキュリティー管理
- Hypertext Transfer Protocol (HTTP)、HyperText Transfer Protocol Secure (HTTPS)、Transmission Control Protocol/Internet Protocol (TCP/IP) などのインターネット・プロトコル (IP)
- Lightweight Directory Access Protocol (LDAP) およびディレクトリー・サービス
- サポートされるユーザー・レジストリー
- 認証と許可の概念
- SAP ABAP アプリケーション・サーバー

資料および用語集へのアクセス

IBM Security Directory Integrator バージョン 7.2.0.1 のライブラリーおよびオンラインでアクセスできる関連資料の説明をお読みください。

このセクションには、以下が含まれています。

- 『IBM Security Directory Integratorライブラリー』にある資料のリスト。
- vii ページの『オンライン資料』へのリンク。
- vii ページの『IBM Terminology Web サイト』へのリンク

IBM Security Directory Integratorライブラリー

IBM Security Directory Integrator ライブラリーでは以下の資料を入手できます。

- *IBM Security Directory Integrator バージョン 7.2.0.1 Federated Directory Server 管理ガイド*

  データ統合ソリューションの設計、実装、および管理のための Federated Directory Server コンソールの使用に関する情報が記載されています。 System for Cross-Domain Identity Management (SCIM) プロトコルおよびインターフェースを使用した ID 管理についても説明しています。
- *IBM Security Directory Integrator バージョン 7.2.0.1 スタートアップ・ガイド*

  IBM Security Directory Integrator の解説および概要です。対話の作成の例と、IBM Security Directory Integrator の実践学習を含んでいます。
- *IBM Security Directory Integrator バージョン 7.2.0.1 ユーザーズ・ガイド*

  IBM Security Directory Integrator の使用方法が記載されています。Security Directory Integrator デザイナー・ツール (構成エディター) を使用したソリューションの設計や、コマンド行からの既製ソリューションの実行について説明しています。また、インターフェース、概念、および AssemblyLine の作成に関する情報も記載されています。
- *IBM Security Directory Integrator バージョン 7.2.0.1 インストールおよび管理者ガイド*

  インストール、旧バージョンからのマイグレーション、ロギング機能の構成、および IBM Security Directory Integrator のリモート・サーバー API の基礎となるセキュリティー・モデルについて記載されています。ソリューションのデプロイおよび管理方法が含まれています。
- *IBM Security Directory Integrator バージョン 7.2.0.1 リファレンス・ガイド*

  IBM Security Directory Integrator の個々のコンポーネント (コネクター、関数コンポーネント、パーサー、オブジェクトなど) に関する詳細情報が記載されています。
- *IBM Security Directory Integrator バージョン 7.2.0.1 Problem Determination Guide*

  問題の識別と解決に役立つ IBM Security Directory Integrator のツール、リソース、および手法に関する情報が記載されています。
- *IBM Security Directory Integrator バージョン 7.2.0.1 メッセージ・ガイド*

  IBM Security Directory Integrator に関連する情報メッセージ、警告メッセージ、およびエラー・メッセージがすべて記載されています。
- *IBM Security Directory Integrator バージョン 7.2.0.1 パスワード同期プラグイン*

  5 つの IBM パスワード同期プラグイン (Windows 用 Password Synchronizer、Sun Directory Server 用 Password Synchronizer、IBM Security Directory Server 用 Password Synchronizer、Domino® 用 Password Synchronizer、UNIX および Linux 用 Password Synchronizer) それぞれのインストールおよび構成について詳細に説明しています。また、LDAP パスワード・ストアと JMS パスワード・ストアの構成手順についても説明します。
- *IBM Security Directory Integrator バージョン 7.2.0.1 リリース情報*

資料に記載されていない IBM Security Directory Integrator の新機能および最新情報を記載しています。

オンライン資料

IBM では、製品のリリース時および資料の更新時に、以下の場所に製品資料を掲載しています。

IBM Security Directory Integrator ライブラリー
製品資料サイト (http://www-01.ibm.com/support/knowledgecenter/SSCQGF/welcome) には、ライブラリーのウェルカム・ページとナビゲーションが表示されます。

IBM Security Systems Documentation Central
IBM Security Systems Documentation Central には、すべての IBM Security Systems 製品ライブラリーのアルファベット順のリストと、各製品のそれぞれのバージョンのオンライン資料へのリンクが掲載されています。

IBM Publications Center
IBM Publications Center サイト (http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss) には、必要なすべての IBM 資料を見つけるのに役立つカスタマイズ検索機能が用意されています。

関連情報

IBM Security Directory Integrator の関連情報は以下の場所で入手できます。

- IBM Security Directory Integrator では、Oracle の JNDI クライアントを使用しています。JNDI クライアントについては、「*Java Naming and Directory Interface™ Specification*」(http://download.oracle.com/javase/7/docs/technotes/guides/jndi/index.html) を参照してください。
- IBM Security Directory Integrator に関する疑問点を解決するために有用な情報が https://www-947.ibm.com/support/entry/myportal/over-accesspubsview/software/security_systems/tivoli_directory_integratorに記載されています。

IBM Terminology Web サイト

IBM Terminology Web サイトは、製品ライブラリーの用語を 1 つの場所にまとめたものです。Terminology Web サイトには、http://www.ibm.com/software/globalization/terminology からアクセスできます。

アクセシビリティー

アクセシビリティー機能は、運動障害または視覚障害など身体に障害を持つユーザーがソフトウェア・プロダクトを快適に使用できるようにサポートします。この製品では、インターフェースを音声化およびナビゲートするための支援テクノロジーをご利用になれます。マウスの代わりにキーボードを使用して、グラフィカル・ユーザー・インターフェースのすべての機能を操作することもできます。

追加情報については、「*Directory Integrator の構成*」の付録『アクセシビリティー』を参照してください。

技術研修

以下は英語のみの対応となります。技術研修の情報については、以下の IBM Education Web サイトを参照してください。 http://www.ibm.com/software/tivoli/education

サポート情報

以下は英語のみの対応となります。IBM サポートは、コード関連の問題や、インストールや使用方法に関するよくある短い質問に対する支援を提供します。IBM ソフトウェア・サポート・サイトには、http://www.ibm.com/software/support/probsub.html から直接アクセスすることができます。

「*トラブルシューティング*」では、以下が詳細に説明されています。

- IBM サポートへの連絡の前にご用意いただく情報。
- IBM サポートへの各種の問い合わせ方法。
- IBM Support Assistant の利用方法。
- 問題をお客様自身で特定し解決するために必要な説明および問題判別リソース。

適切なセキュリティーの実施に関する注意事項

IT システム・セキュリティーでは、企業内外からの不正アクセスを防止、検出し、それらへの対応を行って、システムや情報を保護することが求められます。不正アクセスにより、情報が改ざん、破壊、悪用されるおそれがあります。また、ご使用のシステムが損傷したり、他のシステムへの攻撃に使用されるなどの形で誤用されたりする可能性もあります。完全に安全と見なすことができる IT システムや IT 製品は存在せず、また、不正使用や不正アクセスを防ぐ上で完全に有効な単一の製品、サービス、セキュリティー対策も存在しません。IBM のシステム、製品およびサービスは、包括的なセキュリティーの取り組みの一部として設計されており、これらには必ず追加の運用手順が伴います。また、最高の効果を得るために、他のシステム、製品、またはサービスを必要とする場合があります。 IBM は、システム、製品、またはサービスが、第三者の悪意のある行為または不正な行為から影響を受けないことも、またこれらの行為がお客様の企業に影響を与えないことも保証しません。

第 1 章 パスワード同期プラグインの概要

IBM Security Directory Integrator が提供するインフラストラクチャーとすぐに利用可能なコンポーネントを使用すると、異種ソフトウェア混合環境でユーザー・パスワードを同期するソリューションを実装できます。

IBM Security Directory Integrator を使用して作成したパスワード同期ソリューションは、多数のソフトウェア・システム上のパスワード変更をインターセプトできます。インターセプトされた変更内容は、以下のシステムに送信できます。

- 同じソフトウェア・システム。
- 異なる一連のソフトウェア・システム

パスワードを同期するには、IBM Security Directory Integrator AssemblyLine を使用します。インターセプトされたパスワードを設定済みシステムに伝搬するように AssemblyLine を構成します。

パスワード同期ソリューションには、以下のコンポーネントが含まれます。

Password Synchronizer
パスワード変更が行われるシステムにデプロイされます。 Password Synchronizer は、パスワードの変更時、暗号化されていないパスワード値をインターセプトします。

Java プロキシー・プロセス
Password Synchronizer からパスワードを受信して、パスワード・ストアに転送します。

パスワード・ストア
インターセプトされたパスワードを受信して暗号化します。パスワード・ストアは、IBM Security Directory Integrator がアクセス可能なロケーションに、インターセプトされたパスワードを保管します。

コネクター
インターセプトされ、暗号化されたパスワードが保管されるロケーションに接続します。標準または特殊な IBM Security Directory Integrator コネクターを使用して、パスワードの取得および暗号化解除を行うことができます。

AssemblyLine
コネクターを使用して、インターセプトされたパスワードを取得します。次に、カスタム・ロジックを作成して、パスワードを他のソフトウェア・システムに送信します。

ソリューションの作成

パスワード同期ソリューションを実装するには、Password Synchronizer、パスワード・ストア、コネクターなどのすぐに使用可能なコンポーネントを構成して、デプロイする必要があります。このソリューションは、パスワードをインターセプトし、それを IBM Security Directory Integrator からアクセスできるようにします。

このソリューションでは、カスタム AssemblyLine を実装します。カスタム AssemblyLine は、さまざまな送信元からインターセプトされたパスワードを統合し、それをシステムに送信して同期します。 AssemblyLine の設計は、カスタム環境と特定のソリューション要件に応じて異なります。 IBM Security Directory Integrator には、これらのカスタマイズされた AssemblyLine は組み込まれていません。AssemblyLine を実装する必要があります。

パスワード同期 AssemblyLine は、イテレーター・コネクターを使用して、パスワード・ストアからパスワードを取得します。次に AssemblyLine は、他の標準の IBM Security Directory Integrator コネクターを使用して、これらのパスワードを他のシステム内に設定します。パスワードを設定するカスタム要件が同期対象のシステムにある場合は、AssemblyLine と、これらのパスワードを設定するコネクターを使用して、これらの要件に対処します。このようなカスタマイズでは、特定のコネクター・パラメーターを設定する必要があります。例えば、Active Directory でユーザー・パスワードを設定するには、LDAP コネクターの「**AD パスワードの自動マップ**」オプションをオンにする必要があります。より複雑なケースでは、スクリプトが必要になります。

同期プロセスを自動化するために、パスワード同期ソリューションには、**サーバー・モード**のコネクターを持つ IBM Security Directory Integrator AssemblyLine が含まれています。例えば、次のようにします。

- AssemblyLine は、インターセプトされたパスワードがパスワード・ストア・コンポーネントにより保管されるリポジトリーに変更がないかどうかを listen します。 AssemblyLine は、新規パスワードがインターセプトされるたびに同期 AssemblyLine を起動します。
- スケジュールに従って同期 AssemblyLine を開始する Timer ループと共に AssemblyLine を使用します。

Password Synchronizer の各コンポーネントは、動作を調整するために使用するインターフェースを備えています。ユーザーは、各種のコンポーネントを相互に組み合わせて、カスタム・ソリューションを作成することもできます。これらの主要な機能により、カスタム要件および制限を満たすソリューションを柔軟に作成できます。Password Synchronization Suite は、パスワードをインターセプトし、それを IBM Security Directory Integrator からアクセスできるようにする特殊なコンポーネントから構成されています。 IBM Security Directory Integrator は、そのコネクターを通じて、インターセプトされたパスワードにアクセスできます。柔軟性とオープンネスを備えたこのアーキテクチャーを使用することにより、パスワード取得プロセスの編成と、パスワードの他のシステムへの伝搬が可能となります。

Password Synchronizer のデプロイメントに関する制限

パスワード同期で 31 ページの『第 5 章 Sun Directory Server の Password Synchronizer』 と 37 ページの『第 6 章 IBM Security Directory Server Password Synchronizer』 を使用する場合は、より簡単な方法を使用してシンクロナイザーをデプロイしてください。

Password Synchronizer は、ハッシュ化されたパスワード値がディレクトリーの外部で使用できない場合にのみデプロイします。 IBM Security Directory Server と Sun Directory Server がサポートするパスワード暗号化では、パスワード値がディレクト

リーに保管される前に、パスワード値が暗号化されます。パスワード暗号化では、片方向または両方向の暗号変換が使用されます。片方向変換 (例えば、SHA-1 や MD-5 を使用してハッシュ化する変換) は不可逆です。片方向で暗号化されたパスワードからプレーン・テキスト値を取得することはできません。 Password Synchronizer は、プレーン・テキスト・パスワードをキャッチしてから、ハッシュ化して、ディレクトリーに保管します。ハッシュ化した値が宛先リポジトリーで使用される場合は、LDAP を介して同期が行われます。例えば、送信元システムと宛先システムの両方が同じハッシュ方式をサポートしている場合です。

IBM Security Directory Server のインスタンスと Sun Directory Server のインスタンス間でパスワードを同期するときは、Password Synchronizer は不要です。これらの両方の製品が同じ一連のパスワード・ハッシュ・アルゴリズムをサポートしているためです。この場合は、LDAP を介して 2 つのインスタンス間でパスワードをコピーします。Sun Directory Server に保管されている資格情報で、IBM Security Directory Server に対して認証を行う必要がある場合は、pass-through 認証オプションを使用します。

IBM Security Directory Server の複製に関する問題

複製トポロジーでは、Password Synchronizer をすべてのマスター・インスタンスにデプロイします。複製を構成すると、変更内容が LDAP 操作を介して複製コンシューマーに伝搬されます。 Password Synchronizer をコンシューマーにデプロイした場合、Password Synchronizer は、複製により起動された LDAP 操作をインターセプトします。 Password Synchronizer が複製からのパスワードを拒否した場合、複製は失敗します。こうした状況を避けるには、Password Synchronizer をすべての複製マスターにデプロイし、パスワードがディレクトリーに保存される前にパスワードを拒否するようにします。

複製トポロジーでパスワードをサプライヤー・ノードに設定すると、関連するコンシューマー・ノード上のシンクロナイザーがパスワード値をパスワード・ストアに同期させます。その結果、同じパスワードが複数回、パスワード・ストアに送信されます。この状況を避けるには、ハッシュ化されたパスワードを使用するように IBM Security Directory Server を構成します。 Password Synchronizer は、ハッシュ化されたパスワードを無視します。したがって、コンシューマー上の Password Synchronizer は、複製サプライヤーから受信した、既にハッシュ化されたパスワード値を無視します。

ハッシュ化されたパスワード

Password Synchronizer は、ハッシュ化されたパスワード値を無視するため、プレーン・テキスト・パスワードのみが同期されます。 Password Synchronizer がハッシュ化されたパスワードを受信するのは、以下の場合です。

- LDAP クライアントが既にハッシュ化されたパスワード値を送信した場合、IBM Security Directory Server は、そのパスワード値を受け入れます。ただし、Password Synchronizer は、プレーン・テキスト・パスワードを取得できず、無視します。例えば、LDAP クライアントが、mypass ではなく {SHA}5yfRRkrhJDbomacm2lsvEdg4GyY= を送信した場合、Password Synchronizer は、パスワードをパスワード・ストアに送信しません。

- パスワード暗号化が片方向変換 (crypt、MD5、SHA-1 など) に設定されている場合、パスワードは、ハッシュ化された形式でディレクトリーに保管されます。

特殊コンポーネント

IBM Security Directory Integrator で利用できるさまざまな特殊コンポーネントを使用して、パスワード同期ソリューションを作成および実装できます。

Password Synchronizer

Windows 用 Password Synchronizer
Windows ログイン・パスワードの変更をインターセプトします。 19 ページの『第 4 章 Windows Password Synchronizer』を参照してください。

Sun Directory Server 用 Password Synchronizer
Sun Directory Server のパスワードの変更をインターセプトします。 31 ページの『第 5 章 Sun Directory Server の Password Synchronizer』を参照してください。

IBM Security Directory Server 用 Password Synchronizer
IBM Security Directory Server のパスワード変更をインターセプトします。 37 ページの『第 6 章 IBM Security Directory Server Password Synchronizer』を参照してください。

IBM Domino 用 Password Synchronizer
IBM Notes ユーザーの HTTP パスワードの変更をインターセプトします。 41 ページの『第 7 章 IBM Domino HTTP Password Synchronizer』を参照してください。

UNIX および Linux 用 Password Synchronizer
PAM (Pluggable Authentication Module) が有効化されている場合に、UNIX および Linux ユーザー・パスワードの変更をインターセプトします。 69 ページの『第 8 章 UNIX および Linux 用 Password Synchronizer』を参照してください。

パスワード・ストア

LDAP パスワード・ストア
インターセプトしたユーザー・パスワードを LDAP ディレクトリー・サーバーに保管するための機能を提供します。 73 ページの『第 9 章 LDAP パスワード・ストア』を参照してください。

JMS パスワード・ストア
以前は IBM WebSphere® MQ Everyplace® パスワード・ストアという名称でした。 JMS パスワード・ストアは、インターセプトしたユーザー・パスワードを JMS プロバイダー・キューに保管します。そこから、どの JMS クライアントでも、ユーザー・パスワードを読み取ることができます。例えば、IBM Security Directory Integrator などです。 83 ページの『第 10 章 JMS パスワード・ストア』を参照してください。

Log パスワード・ストア
通常のパスワード・ストアによって実行されたすべてのアクションをログ記録します。このパスワード・ストアは、Java プロキシーとプラグインが正常に通信していることを検証するのに便利です。

特殊コネクター

JMS パスワード・ストア・コネクター

パスワード更新メッセージを JMS パスワード・ストアから取得し、それを IBM Security Directory Integrator に送信します。詳細は、「リファレンス」および 83 ページの『第 10 章 JMS パスワード・ストア』を参照してください。

IBM Security Identity Manager との統合

IBM Security Identity Manager と以下の Password Synchronizer を統合できます。

- Sun Directory Server の Password Synchronizer
- IBM Security Directory Server Password Synchronizer
- Windows Password Synchronizer
- UNIX および Linux 用 Password Synchronizer

詳しくは、101 ページの『第 13 章 IBM Security Identity Manager の統合』を参照してください。

パスワード同期のアーキテクチャーおよびワークフロー

IBM Security Directory Integrator の Password Synchronizer のアーキテクチャーは、4 つの層から成ります。これらの層を結合して、必要なパスワード同期ソリューションを作成することができます。

IBM Security Directory Integrator の Password Synchronizer のアーキテクチャーには、以下の図に示すようにいくつかの層があります。

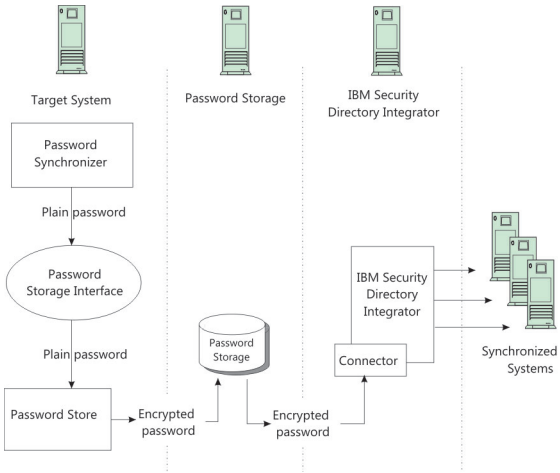

図 1. IBM Security Directory Integrator の Password Synchronizer のアーキテクチャー

図のターゲット・システムは、パスワード変更をインターセプトするソフトウェア・システムを示しています。 `Password Synchronizer` コンポーネントは、ターゲット・システムに備えられているカスタム・インターフェースを使用してターゲット・システムにフックします。 `Password Synchronizer` コンポーネントは、ターゲット・システムで起きたパスワード変更を、パスワードが不可逆的にハッシュされる前にインターセプトします。

Java プロキシー・コンポーネントは、サーバー・プラグインからパスワードを受信し、それをパスワード・ストレージ・コンポーネントにリダイレクトするプロキシーです。プロキシーは、パスワード・ストレージ・コンポーネントのコンテナーとして機能します。このコンポーネントは、パスワード・ストレージ・コンポーネントのライフサイクルを管理し、IBM Security Directory Integrator プラグインとのプロセス間通信を処理します。

Java プロキシーは、エラーが発生した場合、それを構成済みログ・ファイルに記録します。初期化エラーが生じた場合は、Java プロキシーでのそのロードは失敗します。ランタイム・エラーが発生した場合、そのエラーは後の調査のためログに記録されます。ただし、サーバーは継続して稼働するので、一時的な環境の変更や障害の際にも高可用性が確保されます。

パスワード・ストレージ・コンポーネントは、ターゲット・システムにデプロイされます。 Password Synchronizer は、パスワード変更をインターセプトすると、Java プロキシー・プロセスを使用してそのパスワードをパスワード・ストアに送信します。パスワード・ストアは、パスワードを暗号化して、パスワード・ストレージに送信します。

パスワード・ストレージ・コンポーネントは、アーキテクチャーの 2 番目の層です。これは、LDAP ディレクトリーや IBM WebSphere MQ Everyplace などの永続ストレージ・システムを表します。ストレージ・システムでは、インターセプト済みおよび暗号化済みのパスワードは、IBM Security Directory Integrator からアクセス可能なフォームおよびロケーションに保管されます。 パスワード・ストレージは、ターゲット・システム上または別のネットワーク・システム上に配置できます。

アーキテクチャーの 3 番目の層である IBM Security Directory Integrator は、コネクター・コンポーネントを使用して、パスワード・ストレージに接続して保管されているパスワードを取得します。パスワードは IBM Security Directory Integrator で暗号化解除され、AssemblyLine で使用できるようになります。 AssemblyLine は、他のシステムとのパスワードの同期を行います。 ターゲット・システムおよびパスワード・ストレージ・システムとは別のシステムに IBM Security Directory Integrator をデプロイできます。

ターゲット・システムとのパスワードの同期が行われるシステムは、アーキテクチャーのデータ・フロー方向でのその次の層を表します。パスワード同期の AssemblyLine は、このシステムへの接続とパスワードの更新を担当します。

Java プロキシー・プロセス認証

Java プロキシーは、Password Synchronizer からパスワードを受信して、パスワード・ストア・コンポーネントにリダイレクトします。 Java プロキシーは、パスワード・ストレージ・コンポーネントのライフサイクルを管理し、IBM Security Directory Integrator プラグインとのプロセス間通信を処理します。

プロキシーとディレクトリー・プラグインは、共通のバイナリー・コマンド・プロトコルを共有します。通信は、ソケットを介して行われます。プロキシーは、サーバーとして機能し、コマンドを listen します。ディレクトリー・プラグインは、プロキシーに接続し、コマンドを送信して応答を読み取ります。

構成によっては、Java プロキシーは、パスワード・ストレングスに関する事前検証も実行できます。リモートIBM Security Identity Manager サーバーでのみ定義されたパスワード・ポリシーを検証できます。 Java プロキシーは、プラグインが受信したパスワード変更を構成済みパスワード・ストアに保管します。

各種のプラグインと Java プロキシー間の通信は、ソケットを介して行われます。これは、ループバック・ネットワーク・インターフェースにのみ制限されています。クライアント・プラグインと Java プロキシー間に接続が確立されるたびに双方向認証が実行されます。認証は、ファイル・システム許可に基づいて行われます。認証手順では、pwsync.props ファイルが配置される場所である Authentication Folder が使用されます。 *Authentication Folder* は、ファイル・システム許可で保護する必要があります。これは、認証プロセスがワンタイムパスワードを作成し、ファイルとしてフォルダーに保管するためです。

Authentication Folder は、Password Synchronizer をセットアップした後に保護する必要があります。このフォルダーを保護するには、プラグインをロードしてプロセスを実行するユーザーのみが、このフォルダーへの読み取りまたは書き込みを行えるようにします。例えば、IBM Domino HTTP Password Synchronizer の場合、ユーザー notes は、IBM Domino サーバーを実行します。 Password Synchronizer を機能させるには、ユーザーが Authentication Folder を完全に制御できる必要があります。

注: Java プロキシー・プロセスは、プラグイン側から自動的に始動します。そのため、プラグインと同じ特権で実行されます。別のユーザーが手動で Java プロキシーを始動する場合は、読み取り権限と書き込み権限を Authentication Folder に付与する必要があります。例えば、**ユーザー**が *Authentication Folder* を完全に制御できる場合は、そのユーザーの特権でコマンドを実行して、認証を行います。

Windows の場合

```
runas /user:user startProxy.bat configuration_file
runas /user:user stopProxy.bat configuration_file
```

Linux および UNIX の場合

```
su - user
startProxy.sh configuration_file
stopProxy.sh configuration_file
```

Windows でのファイル・アクセスの制限

Windows Password Synchronizer では、**認証フォルダー**へのアクセスを制限する必要があります。フォルダーへのアクセス権限は、管理者グループにのみ認可します。

このタスクについて

Windows Password Synchronizer プラグインは、ローカル・システムのアカウントが所有するローカル・セキュリティー権限 (LSA) プロセスで実行されます。ユーザー・アカウントは管理者グループに属するので、そのグループにのみアクセス権限を認可します。別の Password Synchronizer をセットアップする場合、必要な特権を適切なユーザーまたはグループに認可します。

手順

1. Windows Explorer で、Authentication Folder を右クリックします。
2. メニューから「**プロパティ**」を選択します。
3. 「プロパティ」ウィンドウで、「**セキュリティー**」タブをクリックします。
4. 「**詳細設定**」をクリックします。
5. 親アクセス許可の伝搬を可能にするチェック・ボックスをクリアし、すべての子アクセス許可を置き換えるチェック・ボックスを選択します。
6. すべてのレコードを「**アクセス許可エントリ**」リストから削除します。
7. 「**追加**」をクリックします。
8. 管理者グループを追加し、フルコントロールのアクセス許可を付与します。
9. 「**OK**」をクリックします。

Linux および UNIX でのファイル・アクセスの制限

PAM Password Synchronizer では、認証フォルダーへのアクセスを制限する必要があります。認証フォルダーには、pwsync.props プラグイン構成ファイルが入っています。

手順

1. フォルダーの所有権を変更します。

   ```
   chown -R root:root auth_dir
   ```

   認証プロセスは、*auth_dir* フォルダー内で実行されます。
2. フォルダーのアクセス許可を変更します。

   ```
   chmod -R 700 auth_dir
   ```

パスワード・ストア・インターフェース

パスワード・ストアとは、Java プロキシーが受信したパスワードを保管する場所のことです。

必要があれば、Password Synchronizer によって使用されるパスワード・ストアを変更できます。例えば、IBM Security Directory Server 用の Password Synchronizer が LDAP パスワード・ストアを使用するようにデプロイして構成します。 JMS パスワード・ストアを使用する必要がある場合、パスワード・ストアを構成し、Password Synchronizer の単一のプロパティーを変更してから IBM Security Directory Server を再始動します。新規のパスワード変更は、指定の JMS パスワード・ストアに保管されます。同期ソリューションを再度インストールする必要はありません。

アーキテクチャーのオプション

パスワード同期ソリューションを作成して、複数のターゲット・システム上のパスワード変更をインターセプトするには、階層化されたパスワード同期アーキテクチャーを使用します。

階層化されたパスワード同期アーキテクチャーを使用すると、スケーラビリティーおよびカスタマイズ・オプションの点で以下の価値が得られます。

- インターセプトされたパスワードを同じパスワード・ストレージに保管するように、複数のターゲット・システムのパスワード・ストア・コンポーネントを構成できます。 IBM Security Directory Integrator AssemblyLine は、単一のコネクターを使用して、パスワード・ストレージに接続します。 AssemblyLine は、パスワードがインターセプトされ、このパスワード・ストレージに保管されるターゲット・システムの数の影響を受けません。
- 複数のイテレーター・コネクターを使用して多数のパスワード・ストレージに接続するように AssemblyLine を構成できます。この構成は、さまざまなパスワード・ストレージを使用するときや、IBM Security Directory Integrator 上のターゲット・システムを区別する必要があるときに便利です。

上記いずれか、または両方のアプローチでは、新機能に焦点を当てることにより、既存のソリューション内のターゲット・システムを追加、削除、または変更できます。ソリューションの残りの部分は、影響を受けません。

同期を維持するシステムでパスワードが更新されるデータ・フローにおいて、パスワード同期アーキテクチャーは、IBM Security Directory Integrator 固有のスケーラビリティーの恩恵を受けています。さらに別のシステムでパスワードを更新することは、コネクターをパスワード同期 AssemblyLine に追加することと同等のことです。

ターゲット・システムが、他のシステムからインターセプトされたパスワードで更新されるシステムの一つでもある場合は、循環更新を避ける必要があります。ソリューションを IBM Security Directory Integrator に実装するには、同じシステム上でインターセプトされたパスワードでシステムを更新しないロジックを作成する必要があります。

セキュリティー

公開鍵と秘密鍵のインフラストラクチャーを使用して、パスワード・データのセキュアなトランスポートおよび中間ストレージを実現することができます。

パスワード・ストア・コンポーネントでは、公開鍵を使用してパスワード・データを暗号化してからネットワークへの送信とパスワード・ストレージへの保管を行います。IBM Security Directory Integrator AssemblyLine または特殊コネクターには、対応する秘密鍵があります。この鍵を使用して、パスワード・ストレージから取得されたパスワード・データを暗号化解除します。

SSL をサポートするパスワード・ストア・コンポーネントにより、セキュリティーが強化されます。

ファイル・システムの適切なアクセス許可を設定して、各 Password Synchronizer のインストール・フォルダーとそのファイルを、ホスト・オペレーティング・システム上の信頼されないユーザーから保護します。信頼されないユーザーおよびグループに対して、Password Synchronizer のインストール・フォルダーやファイルに対する読み取り、書き込み、およびアクセスの実行を制限します。

信頼性

パスワードの同期解除の防止と、それが発生した場合に対処するための機能が、Password Synchronization のワークフローに組み込まれています。

Password Synchronizer と パスワード・ストア のコンポーネントは、外部ストレージ・システムを利用できない状態や、誤動作が発生している状態を連携して処理する機能を備えています。

パスワード・ストアは、パスワードがパスワード・ストレージに正常に保管されたかどうかを調べるため、Password Synchronizer に報告します。 Password Synchronizer コンポーネントは、以下の手法を使用してパスワードの同期解除を防止し、またそれが発生した場合の対処を行うことができます。

- Password Synchronizer は、有効になっているとき、ターゲット・システムでのパスワード変更を取り消します。取り消しが起きるのは、パスワードが使用不可またはその他の理由でパスワード・ストアに保管されていない、との報告をパスワード・ストレージが出したときです。
- 保管に失敗したときに必要になるパスワード変更の取り消しやロールバックをターゲット・システムが有効化できない場合には、ログに障害が記録されます。障害は、パスワード・ストレージにパスワードが保管されていないユーザーの情報と共にログに記録されます。管理者はログを調べて同期解除パスワードを解決できます。

第 2 章 パスワード同期プラグインのインストール

標準の IBM Security Directory Integrator インストーラーを使用してパスワード同期プラグインをインストールする必要があります。

Windows プラットフォームの場合、IBM Security Directory Integrator パスワード同期プラグインをインストールするユーザー ID は、管理者、または管理者のグループのメンバーのユーザー ID でなければなりません。 UNIX プラットフォームの場合、インストーラーでは、ユーザーが root ユーザーであることが必要です。ユーザーにこれらの特権がない場合、インストーラーは失敗します。

各パスワード同期プラグインのプラットフォーム要件について詳しくは、それぞれのパスワード同期プラグインのセクションにある『サポートされるプラットフォーム』セクションを参照してください。

IBM Security Directory Integrator パスワード同期プラグインをインストールするには、標準の IBM Security Directory Integrator インストーラーを使用します。インストール方法の説明については、「*インストールと管理*」を参照してください。

メインの製品をインストールするのではなく、カスタム・インストールを選択して、「**Password Synchronization Plug-ins**」オプションを選択します。

1. コマンド行からインストーラーを始動するか、またはインストーラーをダブルクリックします (Windows の場合)。
2. パスワード同期プラグインのインストール・ディレクトリーを選択します。
3. 「**カスタム**」を選択します。
4. 「**Password Synchronization Plug-ins**」を選択します。プラグインはすべて、*TDI_install_dir*/pwd_plugins ディレクトリーにインストールされます。

パスワード同期プラグインのインストールが完了したら、いくつかのインストール後のタスクを実行する必要があります。

Password Synchronization Plug-ins のアップグレードとマイグレーション

最初に Password Synchronization Plug-ins の既存の構成ファイルを保存してから、新しいバージョンをインストールする必要があります。

このタスクについて

既存のプラグイン構成ファイルのアップグレードやマイグレーションを行うことはできません。既存のバージョンの Password Synchronization Plug-ins をアンインストールしてから、新しいバージョンをインストールする必要があります。

手順

1. 以下に示す既存の構成ファイルを保存します。

- Windows の Password Synchronizer レジストリー項目: HKEY_LOCAL_MACHINE¥SOFTWARE¥IBM¥<*以前のバージョンの Security Directory Integrator*>¥Windows Password Synchronizer
- パスワード・ストア構成ファイル (mqepwstore.props や idipwstore.props など)。
- IBM WebSphere MQ Everyplace パスワード・ストア構成ファイル (mqeconfig.props など)。

2. 既存のバージョンをアンインストールします。
   a. IBM Security Directory Integrator Password Synchronization Plug-ins の _uninst ディレクトリーに移動します。
   b. アンインストーラーを実行します。

プラットフォーム	実行可能ファイル
Windows	uninstall.exe
上記以外のすべてのプラットフォーム	uninstall.bin

   c. システムを再起動します。
3. 新しいバージョンの Password Synchronization Plug-ins をインストールします。
4. ステップ 1 で保存した構成ファイルを復元します。

第 3 章 パスワード同期プラグインの共通の構成およびユーティリティー

パスワード同期プラグインおよび Java プロキシーは、pwsync.props 構成ファイルを共有しています。コマンド行ユーティリティーを使用して、Password Synchronizer の構成およびデータ・フロー・プロセスを制御することが可能です。

構成ファイル・パラメーター

プラグインを登録するときは、pwsync.props 構成ファイルのパスを指定する必要があります。指定した構成ファイルのパスは、始動時にプラグイン、またはプロキシーを始動するコマンド行ユーティリティーにより Java プロキシーに渡されます。

注: 標準の java.util.Properties クラスは、構成ファイルを構文解析し、制御文字に似た文字を実際の制御文字で置換します。例えば、¥¥n 文字は、¥n 文字に変換されます。したがって、Windows プラットフォーム上で構成ファイルにパスを設定するときは、¥ 文字にもう一つ円記号を追加して、¥¥ のようにする必要があります。

すべてのパスワード・プラグインに共通の、構成ファイルのパラメーターを以下に示します。

proxyStartExe
このストリング・パラメーターは、実行可能ファイル (バイナリーまたはシェル・スクリプト) のパスを保持し、Java プロキシーを始動するために使用されます。デフォルト値は、*TDI_install_dir*/pwd_plugins/bin/startProxy.bat(sh) です。

注: Java プロキシーがまだ実行されていない場合、パスワード・プラグインは Java プロキシーを自動的に始動します。 Java プロキシーの始動を手動で制御するには、**proxyStartExe** パラメーターをコメント化してください。Java プロキシーが実行されていない場合、パスワード・プラグインは、すべてのパスワード変更を拒否します。

serverPort
この整数プロパティーでは、Java プロキシーが listen するポート番号を指定します。このプロパティーは、Java プロキシーへの接続を確立するために、クライアント・プラグインによって読み取られます。デフォルト値 18001 です。

logFile このストリング・パラメーターでは、クライアント・プラグインのログ・ファイルを構成します。このパラメーターを設定しない場合は、ロギングを行うことができません。

注: PAM プラグインのログでは、このプロパティーではなく、UNIX syslog デーモンが使用されます。

checkRepository

この boolean プロパティーを使用すると、パスワード・ストレージが使用可能であるかどうかを検査する機能をオンまたはオフにできます。

このプロパティーに true を設定した場合、Password Synchronizer は、パスワード・ストレージが使用可能であるかどうかを検査します。使用可能である場合、パスワードは、ディレクトリー内で変更された後、パスワード・ストレージに送信されます。ストレージが使用可能でないことが検査で示されると、LDAP 操作 (パスワードの更新) は、ターゲット・システムで拒否されます。

checkRepository プロパティーに false を設定した場合、Password Synchronizer は、ストレージが使用可能であるかどうかを検査しません。パスワードは、ディレクトリー内で更新された後、パスワード・ストレージに保管されます。パスワードを保管できない場合は、パスワード同期が失敗したことを示すためにログ・ファイル (**logFile** プロパティーに対して指定される) にメッセージが記録されます。

デフォルト値は true です。

注: パスワード・ストレージが使用可能であるかどうかの検査は、すべてのパスワード・ストア・コンポーネントで機能します。

syncClass

この必須プロパティーでは、パスワード・ストア・コンポーネントの Java クラスのフルネームを定義します。デフォルト値は、com.ibm.di.plugin.pwstore.log.LogPasswordStore です。選択可能なパラメーターは以下のとおりです。

- **com.ibm.di.plugin.pwstore.log.LogPasswordStore**
- **com.ibm.di.plugin.pwstore.jms.JMSPasswordStore**
- **com.ibm.di.plugin.pwstore.ldap.LDAPPasswordStore**

javaLogFile

このストリング・パラメーターでは、Java プロキシーのログ・ファイルを構成します。このパラメーターを設定しない場合は、ロギングを行うことができません。

customData

このパラメーターでは、パスワードが変更されるたびに送信されるカスタム・ストリングを指定します。このパラメーターは、変更を生成するシステムまたはアプリケーションを固有に識別する場合に使用します。例えば、システム IP、アプリケーション名、バージョンなどを指定します。

注: Java プロキシーは、パスワード変更を処理するたびに同じカスタム・データを送信します。

debug この boolean プロパティーでは、デバッグをオンまたはオフにします。このプロパティーは、クライアント・プラグインと Java プロキシーの両方が検査します。デフォルト値は true です。

ProxyRetryAttempt

このプロパティーは、タイムアウトになるまでの再試行回数を指定する場合に使用します。デフォルト値は 15 です。

このプロパティーは、IBM Security Directory Integrator バージョン 7.2 以降から使用可能です。

構成ファイルからのパラメーターは、Java システム・プロパティーとして設定されます。いずれかのストアまたは IBM Security Identity Manager サーブレットと通信するために SSL が必要な場合は、構成ファイルに以下のプロパティーを設定します。

表 1. SSL Java プロパティー

プロパティー	値
javax.net.ssl.trustStore	JVM のトラストストアを指定します。
javax.net.ssl.trustStorePassword	トラストストアのパスワードを指定します。 **注:** このパスワードは、encryptPasswd ユーティリティーを使用して暗号化する必要があります。
javax.net.ssl.trustStoreType	トラストストアのタイプ。例: jks
javax.net.ssl.keyStore	JVM の鍵ストアを指定します。
javax.net.ssl.keyStorePassword	鍵ストアのパスワードを指定します。 **注:** このパスワードは、encryptPasswd ユーティリティーを使用して暗号化する必要があります。
javax.net.ssl.keyStoreType	鍵ストアのタイプ。例: jks

構成ファイル内のその他のパラメーターは、実際のパスワード・プラグインに固有のものです。

コマンド行ユーティリティー

Password Synchronizer の構成およびフロー・プロセスの特定の側面を制御するために、以下のユーティリティーが提供されています。

TDI_install_dir/**pwd_plugins/bin/encryptPasswd.bat(sh)**
パスワードを各種の構成ファイルに設定する前に、パスワードを暗号化します。

注: このユーティリティーは、対称アルゴリズムを使用してパスワードを暗号化します。スキルのあるユーザーであれば、パスワードを簡単に暗号化解除できます。信頼できるユーザー以外には、構成ファイルの読み取りを許可しないでください。

TDI_install_dir/**pwd_plugins/bin/startProxy.bat(sh)**
Java プロキシーを手動で始動します。このユーティリティーは、自動的にデフォルトの jars フォルダーを検索して、Java プロキシーのクラス・パスを作成します。デフォルトのフォルダーは、*TDI_install_dir*/pwd_plugins/jars/ です。例えば、IBM WebSphere MQ と共に機能するように JMS パスワード・ストアを構成した場合は、必要な IBM WebSphere MQ JAR ファイルを pwd_plugins/jars/ フォルダーに追加してから、Java プロキシーを始動します。

TDI_install_dir/**pwd_plugins/bin/stopProxy.bat(sh)**
実行中の Java プロキシー・プロセスに停止要求を送信します。 Java プロキシーは、すべての操作が完了するまで待機してから、正常終了します。

いずれかの Password Synchronizer を呼び出しているタスクがシャットダウンした場合、Java プロキシー・プロセスは自動的に終了しません。Password Synchronizer がプロキシー・プロセスに接続しているため (プロキシー・プロセスが既に実行されている場合)、プロキシーの終了は不要です。

TDI_install_dir¥pwd_plugins¥windows¥pwsync_admin.exe

Java プロキシーを開始または停止します。また、このユーティリティーでは、Windows プラグインを一時停止または再開することもできます。このユーティリティーは、32 ビット・バージョンに対応しています。 Windows 64 ビットのインストール済み環境の場合は、pwsync_admin_64.exe ファイルを使用します。

TDI_install_dir¥jvm¥jre¥bin¥keytool and *TDI_install_dir*¥jvm¥jre¥bin¥ikeyman

プラグインのセットアップ時に使用する鍵ストア/トラストストアを管理します。詳しくは、「*インストールと管理*」の『鍵ストアおよびトラストストアの管理 (Keystore and truststore management)』トピックを参照してください。

IBM Tivoli Monitoring での Java プロキシー

IBM Tivoli® Monitoring バージョン 6.2.2 フィックスパック 2.0 のエージェント管理サービスを使用して、Password Synchronizer の Java プロキシー・プロセスを管理できます。

特定のエージェントに対するエージェント管理サービスのモニター動作は、XML ベースのポリシー・ファイルの設定で制御されます。このポリシー・ファイルは、共通エージェント・パッケージ (CAP) ファイルと呼ばれます。このサービスは、Windows、Linux、および UNIX の各プラットフォーム用の IBM Tivoli Monitoring OS Monitoring Agent で使用可能です。エージェント管理サービスは、Java プロキシー・プロセスを常に使用可能にし、その状況に関する情報を Tivoli Enterprise Portal に提供するように設計されています。エージェント管理サービスについて詳しくは、http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/topic/com.ibm.itm.doc_6.2.2/itm_agentmgmtsvcs_intro.htm を参照してください。

IBM Tivoli Monitoring を使用した Java プロキシーの管理は、オプションです。

各 Password Synchronizer には、その Java プロキシー・プロセスが記述された、関連する CAP ファイルがあります。インストールが完了すると、すべての CAP ファイルが *TDI_install_dir*/pwd_plugins/cap/ ディレクトリーで使用可能になります。以下の表に、使用可能な CAP ファイルをリストします。

Password Synchronizer	**CAP ファイル**
Windows Password Synchronizer:	tdi_ad_plugin_default.xml
IBM Security Directory Server Password Synchronizer	tdi_tds_plugin_default.xml
Sun Directory Server の Password Synchronizer	tdi_sun_plugin_default.xml
PAM Password Synchronizer	tdi_pam_plugin_default.xml

Password Synchronizer	CAP ファイル
IBM Domino HTTP Password Synchronizer	tdi_domino_plugin_default.xml

プロキシーが管理可能であることを IBM Tivoli Monitoring が認識するには、該当する CAP ファイルを適切なディレクトリーにコピーする必要があります。

UNIX または Linux の場合、ディレクトリーは /opt/IBM/CAP です。

Windows の場合、ディレクトリーは %ALLUSERSPROFILE%¥ApplicationData¥IBM¥CAP です。

CAP ファイルを使用するには、事前に CAP ファイルを変更して、IBM Security Directory Integrator のインストール済み環境の正しいパスを含める必要があります。

第 4 章 Windows Password Synchronizer

Windows Password Synchronizer は、Windows オペレーティング・システム上のユーザー・アカウントのパスワード変更をインターセプトします。

概説

パスワードの変更は、以下のすべてのケースでインターセプトされます。

- ユーザーが Windows ユーザー・インターフェースを通してパスワードを変更した場合。
- 管理者が Windows の管理者用ユーザー・インターフェースを使用して、ユーザーのパスワードを変更する場合。
- LDAP 経由で Active Directory に対するパスワード変更要求が行われた場合。

IBM Security Directory Integrator Password Synchronizer プラグインは、Windows システムがパスワードを変更する前に、パスワード・ストアなどのリポジトリーにその変更を伝搬します。

IBM Security Directory Integrator Password Synchronizer は、LDAP サーバーまたは JMS パスワード・ストアなどのパスワード・ストアにユーザー・パスワードを保管します。

その変更は後で、IBM Security Directory Integrator AssemblyLine によって他のサーバーに伝搬されます。パスワードの保管後、制御は Windows システムに戻されるので、ユーザー・パスワードを変更できるようになります。

単一システムからの同期

単一のシステムからのパスワードを同期する場合は、Windows Password Synchronizer をスタンドアロンの Windows システムにインストールします。

Windows 2008 ドメインからの同期

Password Synchronizer は、パスワード変更を Windows 2008 ドメインから同期できます。同期を行うには、すべてのドメイン・コントローラーに Password Synchronizer をインストールする必要があります。

サンプル・シナリオ

Bob が Windows システムにログオンし、**Ctrl+Alt+Delete** を押し、パスワードの変更を要求します。パスワード変更は、Windows Password Synchronizer によってインターセプトされてから、LDAP パスワード・ストアまたは JMS パスワード・ストアなどの関連パスワード・ストアに委任されます。パスワードが正常に保管されたことがパスワード・ストアで確認されると、ローカル Windows システム上でパスワード変更が実行されます。その変更は、スタンドアロン・システムまたはドメイン・コントローラー上で行われます。パスワードを保管できなかったことをパスワード・ストアから示された場合は、ローカルの Windows システム上でのパスワードの変更は拒否されます。

LDAP および JNDI を介した Active Directory へのパスワード変更要求もインターセプトされて、Windows Password Synchronizer によって処理されます。

Windows Password Synchronizer のワークフロー

Windows Password Synchronizer がパスワード変更をインターセプトしてから、その変更は、Windows および Active Directory によって内部的にコミットされます。Password Synchronizer は新規パスワードをパスワード・ストアに受け渡します。

パスワードが正常に保管されたことがパスワード・ストアから示されると、Password Synchronizer は、Windows システムでのパスワード変更のコミットを可能にします。

パスワードが保管されなかったことがパスワード・ストアから示された場合は、Windows システム上でのパスワードの変更は拒否されます。 Windows ユーザー・インターフェースからパスワード変更を行った場合、次のようなエラー・メッセージが表示されます。

```
Windows cannot complete the password change for user_name because:
The password does not meet the password policy requirements.
Check the minimum password length, password complexity and password history
requirements.
```

Password Synchronizer とパスワード・ストア・コンポーネントのログ・ファイルに、パスワード・ストレージにパスワードを保管できなかった原因が示されます。

パスワード変更が正常に完了するたびに、Password Synchronizer はユーザーのフルネームと **displayName** 属性を Active Directory からパスワード・ストアに送信します。 JMS パスワード・ストアはそのデータを無視します。 LDAP パスワード・ストアは、詳細情報をユーザー項目の拡張データ属性に書き込みます。デフォルトでは、拡張データ属性は **ibm-diExtendedData** という名前です。

Password Synchronizer は、パスワードの変更後にユーザーの **sAMAccountName** 属性を返します。その名前は、Windows ドメインごとの固有名ですが、ドメイン・フォレスト・モデルでは固有名ではありません。残りのユーザー属性を取得するには、リンク基準として指定した **sAMAccountName** 属性を使用した検索がさらに必要になります。

Windows Password Synchronizer のフィルター

Windows Password Synchronizer には、フィルター機能が備えられています。フィルターが影響を及ぼすのは、パスワード変更がパスワード・ストアに送信される時のみであって、Windows ドメインがパスワード変更の受け入れまたは拒否を行う時ではありません。ユーザー・フィルターがユーザーを受け入れた場合、そのユーザーのパスワード変更はパスワード・ストアに送信されます。

ユーザー・フィルターは、以下の 2 つの基準に基づいて稼働します。

- グループ・メンバーシップ
- DN マッチング (LDAP サブツリー・ロケーションのマッチング)

グループ・メンバーシップは、ユーザーが特定の Windows グループのメンバーであるかどうかを示します。ユーザー・フィルターはネストされたグループを認識し

ません。ユーザーが、グループ B にネストされたグループ A のメンバーである場合、そのユーザーはグループ B のメンバーとは見なされません。

DN マッチングは、DN 接尾部がユーザーの識別名に一致するかどうかを扱います。例えば、ユーザーの識別名が cn=myuser,ou=myou,dc=mydc,dc=com である場合、それは DN 接尾部 dc=mydc,dc=com に一致しますが、dc=mydc には一致しません。

ユーザー・フィルターでは、グループ・メンバーシップと DN マッチングの両方の組み込みおよび除外ルールを使用できます。例えば、特定の Windows グループのメンバーであるすべてのユーザーを受け入れるようにユーザー・フィルターを構成できます (組み込みフォーム)。ただし、それらのユーザーは、他の Windows グループのメンバーではありません (除外フォーム)。

両方のルール (組み込みまたは除外) のグループ・メンバーシップと DN マッチングを結合できます。ただし、制限事項があります。 除外ルールは常に、組み込みルールより優先順位が高くなります。例えば、ユーザーが DN マッチングで組み込まれても、グループ・メンバーシップで除外された場合、ユーザー・フィルターはそのユーザーを受け入れられません。

以前のバージョンとの互換性を保つために、グループ・メンバーシップと DN マッチングに対して組み込みフォームが指定されなかった場合のデフォルト・フォームはすべて組み込み (include all) になります。グループ・メンバーシップと DN マッチングに対して除外フォームが指定されなかった場合のデフォルト・フォームは除外なし (exclude none) になります。

フィルター・メカニズムの例を以下に示します。

- ユーザー・フィルターに対して構成が指定されなかった場合、すべてのユーザーが受け入れられます (前のバージョンとの互換性)。
- ユーザー・フィルターに特定の組み込みルールは指定したが、除外ルールは指定しなかった場合、指定した組み込みルールに一致するユーザーが受け入れられます。
- ユーザー・フィルターに特定の除外ルールは指定したけが、組み込みルールは指定しなかった場合、どの除外ルールにも一致しないユーザーが受け入れられます。
- ユーザー・フィルターに特定の組み込みルールと特定の除外ルールを指定した場合、次のようなユーザーが受け入れられます。
  - 組み込みルールのいくつかに一致するユーザー
  - どの除外ルールにも一致しないユーザー

Windows Password Synchronizer のユーザー・フィルターは、『プラグイン構成ファイル』の中の以下の 4 つのストリング値を使用して構成されて、組み込みルールと除外ルールを定義します。

includeGroups

Windows グループのリスト。ユーザーがこのリスト上のグループのメンバーである場合、フィルターはそのユーザーを受け入れます。そのユーザーは、特定の**除外**リストによって除外されていないと想定されます。

excludeGroups
Windows グループのリスト。ユーザーがこのリスト上のグループのメンバーである場合、フィルターはそのユーザーを受け入れられません。

includeDNs
DN 接尾部のリスト。ユーザーの識別名がリスト中の特定の接尾部に一致した場合、フィルターはそのユーザーを受け入れます。そのユーザーは、特定の**除外**リストから除外されていないと想定されます。

excludeDNs
DN 接尾部のリスト。ユーザーの識別名がリスト中の特定の接尾部に一致した場合、フィルターはそのユーザーを受け入れられません。

上記のプロパティー・ストリング値はすべて、セミコロンで区切ったトークンを付けてリストされる必要があります。冗長な空白文字は使用できません。グループ・リストには、既存の Windows グループの名前のみを含める必要があります。識別名に対する DN 接尾部の突き合わせは、大/小文字を区別しないストリング比較によって行われます。空白文字に対する特別な取り扱いはありません。例えば、`DC=COM` 接尾部は `cn=myuser,dc=mydc,dc=com` 識別名に一致しますが、`dc = com` 接尾部は一致しません。

ユーザー・フィルターで問題が生じた場合、エラー・メッセージがログ記録され、Windows Password Synchronizer は、ユーザーがフィルターで受け入れられたものとして動作します。例えば、無効なグループ名が構成内にある場合があります。ユーザー・フィルターがユーザーを受け入れないと判別した場合、ログ記録についてのメッセージが表示されます。

各パスワード通知ごとに、ユーザー・フィルターの構成が再度読み取られます。したがって、構成に加えた変更は即時に有効になります。ユーザー・フィルターに加えた変更を有効にするために、Windows オペレーティング・システムを再始動する必要はありません。

注: Windows Password Synchronizer のユーザー・フィルター構成は、その構成に関係する Windows グループの変更の影響を受けます。次のような変更のいずれかが発生した場合、Windows Password Synchronizer を再始動する必要があります。それには、オペレーティング・システムの再始動が必要です。

- グループの Windows 名が変更された場合。その変更は、Active Directory 内の `sAMAccountName` 属性に対応します。
- グループの識別名が変更された場合。例えば、グループが別のコンテナーに移動された場合です。

この制約事項は、Windows Password Synchronizer の構成内に存在するすべてのグループに対して、その存続期間中に適用されます。

重要: Windows Password Synchronizer のユーザー・フィルター機能は、Windows ドメインに属するシステム上でのみ正しく機能します。ワークグループ・システムは、ユーザー・フィルターを使用できません。ユーザー・フィルターをワークグループ・システム上で構成した場合、以下に例を示したとおり、パスワード変更ごとにエラー・メッセージがプラグインでログ記録されます。その変更は、次のように、指定した構成に関係なくパスワード・ストアに送信されます。

```
User filtering failed: The specified domain either does not exist or could not
be contacted.
```

ユーザー・フィルターの構成を指定しない場合、フィルタリングは行われないので、プラグインは通常どおりに機能し、エラーがログ記録されることはありません。

サポートされるプラットフォーム

IBM Security Directory Integrator Windows Password Synchronization プラグインでは、次のようなプラットフォームがサポートされます。

- Windows 7 (x86)
- Windows (x86/x86 - 64)
- Windows 2008 Standard Edition (x86/x86 - 64)
- Windows 2008 Enterprise Edition (x86/x86 - 64)
- Windows 2008 Datacenter Edition (x86/x86 - 64)
- Windows 2008 R2 Standard Edition (x86/x86 - 64)
- Windows 2008 R2 Enterprise Edition (x86/x86 - 64)
- Windows 2008 R2 Datacenter Edition (x86/x86 - 64)
- Windows 2012 R2

デプロイメントおよび構成

Windows Password Synchronizer をデプロイする前に、インストール後の構成ステップを実行し、パスワード変更通知のために Password Synchronizer を登録する必要があります。

インストール後の構成

1. `TDI_install_dir¥pwd_plugins¥windows` ディレクトリーから Windows Password Synchronizer の `tdipwflt.dll` DLL をコピーします。
2. この DLL ファイルを Windows インストール・フォルダーの `System32` フォルダーに貼り付けます。 64 ビット Windows オペレーティング・システムの場合は、Password Synchronizer の 64 ビット DLL を `System32` フォルダーに貼り付ける必要があります。
3. Windows Password Synchronizer DLL の名前 (`tdipwflt`) を `HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥LSA¥Notification Packages` Windows レジストリー・キーに追加します。 Notification Packages にある既存データは、どれも削除しないでください。

4. *TDI_install_dir*¥pwd_plugins¥windows ディレクトリーから、Password Synchronizer に付属の registerpwsync.reg ファイルを実行します。以下に示す Windows Password Synchronizer 用のキーが Windows レジストリーに作成されます。

   ```
   HKEY_LOCAL_MACHINE¥SOFTWARE¥IBM¥Security Directory Integrator¥Windows
   Password Synchronizer
   ```

   また、ストリング値 ConfigFile が設定されます。これには、Windows Password Synchronizer の構成ファイルの絶対ファイル名が含まれます。 Windows レジストリーに追加されるパラメーターのリストについては、『Windows レジストリー内の構成パラメーター』を参照してください。
5. システムを再起動します。

パスワード・ストアのセットアップ情報

デフォルトでは、IBM Security Directory Integrator インストーラーは、Log パスワード・ストアを使用するように Password Synchronizer を構成します。

パスワード・ストアのセットアップについては、以下を参照してください。

- 83 ページの『第 10 章 JMS パスワード・ストア』
- 95 ページの『第 11 章 Log パスワード・ストア』

Windows レジストリー内の構成パラメーター

パスワード変更通知を受信するには、Windows Password Synchronizer を Windows LSA に登録する必要があります。また、外部ライブラリー名を特定のレジストリー・キーに登録する必要もあります。

PATH 環境変数で指定されたいずれかのディレクトリーに外部ライブラリーを保管します。外部ライブラリーをロードするには、オペレーティング・システムを再始動する必要があります。

注: 外部ライブラリー・ファイルが登録されているが、ロードできない場合は、Windows オペレーティング・システムが不安定になります。

Windows Password Synchronizer のネイティブ・モジュールが初期化されると、以下のレジストリー・キー・フォルダーから読み取りが行われます。

```
[HKEY_LOCAL_MACHINE¥SOFTWARE¥IBM¥Security Directory Integrator¥Windows Password
Synchronizer]
```

以下のレジストリー・キーには、Password Synchronizer の構成ファイルの場所が指定されています。

表 2. 1 次レジストリー・キー

鍵名	タイプ	説明	必須かどうか
ConfigFile	REG_SZ	Windows Password Synchronizer の構成ファイルの絶対パスを指定します。	true

以下の表は、Windows Password Synchronizer の動作に影響を与えるオプションのレ

ジストリー・キーを示しています。キーを設定するには、管理ツールを使用します。

注: キーを手動で設定してはなりません。

表 3. オプションのレジストリー・キー

鍵名	タイプ	説明	デフォルト	必須かどうか
disabled	REG_SZ	パスワード変更を Java プロキシー・プロセスに伝搬できるかどうかを指定します。	false	false
reconfigure	REG_SZ	次回のパスワード変更通知時にプラグインがその構成ファイルを再ロードできるかどうかを指定します。	false	false

以下のレジストリー・キー・フォルダーでキーを編集して、パスワード・フィルター・モジュールを登録します。

```
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥LSA
```

以下のキーが存在することを確認します。

表 4. オプションのレジストリー・キー

鍵名	タイプ	説明	デフォルト	必須かどうか
Notification Packages	REG_MULTI_SZ	通知用に登録する外部ライブラリーを指定します。	unknown	true

注: このキーの値は、どれも削除しないでください。ライブラリー名は、最後の行に含めます。入力する名前に .dll 拡張子は含めないでください。

Windows システムを再始動します。

構成ファイル内の構成パラメーター

Windows Password Synchronizer プラグインのテンプレート構成ファイルは、TDI_install_dir /pwd_plugins/windows/pwsync.props にインストールされています。

構成ファイルの構成パラメーターの多くは、すべてのパスワード・プラグインに共通です。 13 ページの『第 3 章 パスワード同期プラグインの共通の構成およびユーティリティー』の『構成ファイル・パラメーター』を参照してください。

includeGroups

Windows グループのオプションのリスト。ユーザーがリスト内のいずれかのグループのメンバーである場合、フィルターはそのユーザーを受け入れます。ただし、ユーザーがどの除外リストでも除外されていないことが前提です。

excludeGroups

Windows グループのオプションのリスト。ユーザーがリスト内のいずれのグループのメンバーでもない場合、フィルターはそのユーザーを受け入れません。

includeDNs

DN 接尾部のオプションのリスト。ユーザーの識別名がリスト上のいずれかの接尾部に一致した場合、フィルターはそのユーザーを受け入れます。ただし、ユーザーがどの除外リストでも除外されていないことが前提です。

excludeDNs

DN 接尾部のリスト。ユーザーの識別名がリスト上のいずれかの接尾部に一致した場合、フィルターはそのユーザーを受け入れません。

accountTypes

パスワード変更が報告されるアカウントのタイプを指定します。パラメーターの形式は、アカウント・タイプをスペースで区切ったリストとなります。

Password Synchronizer プラグインは、以下の Windows アカウント・タイプに対してパスワード変更を報告できます。

NORMAL_ACCOUNT

標準的なユーザーを表す、デフォルトのアカウント・タイプです。

TEMP_DUPLICATE_ACCOUNT

1 次アカウントが他のドメインに存在するユーザーのアカウントです。

INTERDOMAIN_TRUST_ACCOUNT

他のドメインを信頼するドメイン用のアカウントを信頼する許可です。

WORKSTATION_TRUST_ACCOUNT

このドメインのメンバーであるコンピューターのコンピューター・アカウントです。

SERVER_TRUST_ACCOUNT

このドメインのメンバーであるバックアップ・ドメイン・コントローラーのコンピューター・アカウントです。

この鍵値の例を以下に示します。

```
"NORMAL_ACCOUNT WORKSTATION_TRUST_ACCOUNT"
```

注: Password Synchronizer は、**AccountTypes** パラメーターに NORMAL_ACCOUNT が指定されているかどうかに関わらず、常に NORMAL_ACCOUNT タイプのアカウントにパスワード変更を報告します。

ローカル・セキュリティー・ポリシーの使用可能化

Windows Password Synchronizer をデプロイする前に、ローカル・セキュリティー・ポリシーの設定を変更する必要があります。

このタスクについて

ローカル・セキュリティー・ポリシーを以下のように変更します。

手順

1. 「**コントロール パネル**」 > 「**管理ツール**」 > 「**ローカル セキュリティ ポリシー**」を選択します。
2. 「**アカウント ポリシー**」 > 「**パスワードのポリシー**」を選択します。

3. 「**パスワードは、複雑さの要件を満たす必要がある**」 > 「**有効**」を選択します。

タスクの結果

注:

1. この変更を反映するために、システムを再始動します。パスワード・ストアのプロパティー・ファイルをセットアップしたことを確認してからシステムをリブートしてください。
2. Windows Server がドメイン・コントローラーとして構成されている場合は、「**パスワードは、複雑さの要件を満たす必要がある**」設定を Active Directory ドメインに適用する必要があります。したがって、**ドメイン・セキュリティー・ポリシー**・ツールを使用して、設定を変更する必要があります。

プラグイン管理ツール

プラグイン管理ツール `pwsync_admin.exe` は、管理用タスクを実行するコマンド行ツールです。

プラグイン管理ツールは、*TDI_install_dir*¥pwd_plugins¥windows ディレクトリーに置かれています。

このツールの主な目的は、Windows システムを再始動しなくても Windows Password Synchronizer を再構成できるようにすることにあります。例えば、このツールを使用すると、Windows をリブートしなくてもパスワード・ストアを変更できます。

注: システムをリブートしなくても、Windows は Windows `System32` ディレクトリー内の `tdipwflt.dll` プラグインを置き換えます。

管理ツールの使用

コマンド行から、以下を実行します。

`pwsync_admin.exe` – 32 ビット Windows 用のコマンド
`pwsync_admin_64.exe` – 64 ビット Windows 用のコマンド

この管理ツールは、単一のコマンド行パラメーターをとります。それには、以下の値のいずれかを指定できます。

suspend_plugin
ブール値を Windows レジストリーに書き込みます。 Windows のレジストリー設定を参照してください。この値は、後続のパスワード変更を Java プロキシーに伝搬してはならないことを表します。このコマンドを発行すると、 **resume_plugin** コマンドを発行するまでの間、以降のパスワード変更がスキップされます。

resume_plugin
ブール値を Windows レジストリーに書き込みます。 Windows のレジストリー設定を参照してください。この値は、後続のパスワード変更を Java プ

ロキシーに必ず伝搬する必要があることを表します。このコマンドを発行すると、 **suspend_plugin** コマンドを発行するまでの間、以降のパスワード変更が同期されます。

reconf_plugin
ブール値を Windows レジストリーに書き込みます。 Windows のレジストリー設定を参照してください。この値は、プラグインはその構成ファイルを必ず再ロードする必要があることを表します。再ロードが起きるのは、次のパスワード変更時のみです。新規構成中に何らかのエラーが発生しても、すぐには判明しません。テスト・アカウントのパスワード変更をトリガーして、再構成を実行できます。プラグインが中断された場合、再構成は延期されます。

query_plugin
プラグインの状況を照会して、プラグインがロード済みかどうか、およびその最後の初期化が正常に完了したかどうかをチェックします。

stop_proxy
管理ツールが Java プロキシーのコマンド・ソケット・ポートにソケットを使用して接続されるようにし、停止要求をプロキシーに送信します。この停止要求によりプロキシーは終了します。

start_proxy
Java プロキシーを開始し、それによりプロキシー構成が再ロードされます。

restart_proxy
stop_proxy コマンドおよび **start_proxy** コマンドと同等です。

query_proxy
Java プロキシーが実行中かどうかを判別します。

操作可能な Windows のレジストリー設定

Windows パスワード・プラグインとその操作に関連付けられた Windows レジストリー・キーには、以下のようにいくつかのものがあります。

注: プラグインのインストール後は、それらのキーは Windows レジストリー内にはありません。プラグインの通常の運用においては、これらのキーは不要です。

プラグインの有効化または無効化
suspend_plugin コマンドおよび **resume_plugin** コマンドは、次のレジストリー・キーを使用します。

```
[HKEY_LOCAL_system¥SOFTWARE¥IBM¥Security Directory Integrator¥Windows
Password Synchronizer] "disabled"="true"
```

キーに `true` 値が付いている場合、プラグインはパスワードを同期できません。この鍵がないか、値が `true` 以外であれば、プラグインはパスワードを同期します。プラグイン管理ツールは、初回の使用時にこのキーを作成します。

プラグイン構成の再ロード
reconf_plugin コマンドは、次のレジストリー・キーを使用します。

```
[HKEY_LOCAL_system¥SOFTWARE¥IBM¥Security Directory Integrator¥Windows
Password Synchronizer] "reconfigure"="true"
```

キーを true に設定した場合、次回のパスワード変更の際にプラグインはその構成ファイルを再ロードします。また、プラグインは値を false に設定して、ファイルが一度だけ再ロードされるようにします。

ロギング

管理ツールは、メッセージをコンソールとログ・ファイル pwsync_admin.log の両方に記録します。このファイルは、プラグインのインストール・ディレクトリーにあります。ログ・ファイルを使用して、ツール操作中に検出されたエラーを分析できます。また、ログ・ファイルを、このツールを使用して実行された操作の履歴参照として使用することもできます。

管理ツールの使用上の考慮事項

- プラグインが停止していると、プラグインはパスワード変更をスキップし、それを伝搬しません。プラグインが停止していると、ターゲットの同期システムでパスワード変更が喪失するなどの不整合が発生する可能性があります。
- プラグインが Java プロキシーの再開を試みるのは、プロキシーがまだ実行中でないときに再構成が要求された場合に限ります。詳細は、**reconf_plugin** 管理ツール・コマンドの項を参照してください。
- Java プロキシーが開始されると、パスワード・ストアの構成ファイルがロードされます。このファイルは、システムを再始動したときか、またはプラグインが停止していないときにロードされます。パスワード変更が発生すると、Java プロキシーは停止します。ユーザーが構成ファイルを編集中の場合、Java プロキシーは破損している可能性のある構成をロードするおそれがあります。
- プラグインが停止中ではなく、Java プロキシーが実行されていないときに「**Active Directory ユーザーとコンピューター**」ユーザー・インターフェース・ツールを使用してパスワード変更を実行した場合、そのパスワード変更は Windows によってプラグインに通知されます。この結果、同じパスワード更新が 2 度または 3 度伝搬されます。こうした更新が起きるのは、プラグインは次回のパスワード変更時にプロキシーを開始するものの、これにはしばらく時間がかかるためです。こうした更新の結果、Windows からプラグインへ同じパスワード変更が複数回通知されることになります。このような多重報告は、Java プロキシーが実行されていないときに最初のインスタンスで発生します。
- LDAP パスワード・ストアでプラグインを構成してあり、LDAP パスワード・ストアを非同期保管に設定 (LDAP ストアの構成ファイルに waitForStore=false を指定) してある場合、プラグインが停止していないと、 **stop_proxy** コマンドによっていくつかのパスワード変更がスキップされます。

以下の詳細を利用して、問題のトラブルシューティングを行えます。

- **suspend_plugin** コマンドを使用してプラグインを停止してから、**stop_proxy** コマンドまたは **restart_proxy** コマンドを実行します。
- 編集用に構成ファイルのコピーを作成します。すべての編集を完了したら古い構成ファイルを新規構成ファイルで置換します。
- 必要な構成変更は使用率の低い時間に行い、スキップされて伝搬されないパスワード変更がごく一部だけになるようにします。

Windows システムのリブートなしでの構成の変更

プラグインの構成設定は、パスワードが変更される可能性の低い、利用頻度の低い時間帯に変更する必要があります。

このタスクについて

注: 以下のステップが完了すると、プラグイン、Java プロキシー、およびパスワード・ストアが新しい構成設定を使用します。プラグインが中断される短い期間中は、パスワード変更をスキップできます。この変更は、Windows ドメイン・コントローラーで行われますが、プラグインにより伝搬されることはありません。

手順

1. 構成ファイルを一時的なロケーションにコピーします。
2. この一時的なロケーションにあるファイルを編集します。
3. 編集済みのファイルを元のロケーションにコピーします。
4. **pwsync_admin.exe suspend_plugin** コマンドを実行します。
5. **pwsync_admin.exe reconf_plugin** コマンドを実行します。
6. **pwsync_admin.exe stop_proxy** コマンドを実行します。
7. **pwsync_admin.exe start_proxy** コマンドを実行します。
8. **pwsync_admin.exe resume_plugin** コマンドを実行します。

タスクの結果

パスワード・ストアの設定を一部のみ変更する場合は、上記のステップの再構成コマンドをスキップすることもできます。ただし、設定がプラグインまたはプロキシーに関連していてはなりません。

Password Synchronizer の信頼性および可用性

プラグイン管理ツールおよびエラー・ログを使用して、Password Synchronizer の信頼性と可用性を分析できます。

初期化の失敗

Password Synchronizer が初期化に失敗すると、Windows はパスワード変更の通知を Password Synchronizer に送信できません。例えば、構成ファイルが使用できない場合などです。パスワード変更を行うことは可能ですが、Windows Password Synchronizer はそれをインターセプトできません。

Password Synchronizer が正常に初期化されたかどうかを判別する最も信頼性の高い方法は、そのエラー・ログをチェックすることです。また、プラグイン管理ツールの **query_plugin** コマンドを使用することもできます。

再構成の失敗

再構成が失敗すると、Password Synchronizer は初期化されていない状態になり、すべてのパスワード変更をリジェクトします。 Password Synchronizer のエラー・ログをチェックして、再構成が成功したかどうかを確認してください。 27 ページの『プラグイン管理ツール』を参照してください。

第 5 章 Sun Directory Server の Password Synchronizer

Sun Directory Server 用 Password Synchronizer は、Sun Directory Server での LDAP パスワードの変更をインターセプトします。

Sun Directory Password Synchronizer のコンポーネント

Sun Directory Server プラグインを使用しないでパスワードを同期するソリューションを作成できます。ソリューションの作成に関する詳細は、1 ページの『ソリューションの作成』を参照してください。

Sun Directory Password Synchronizer は、以下のパーツで構成されます。

Sun Directory Server プラグイン
このプラグインは、Sun Directory Server のプラグイン API を使用するネイティブ・バイナリーです。 Sun Directory Server プロセスで実行されます。

Java プロキシー
サーバー・プラグインによって開始または停止される別個の Java プロセスです。このプロセスの主な目的は、パスワード・ストレージ・コンポーネントをホストし、プラグインと通信することにあります。 Java プロキシーの詳細については、5 ページの『パスワード同期のアーキテクチャーおよびワークフロー』を参照してください。

パスワード・ストレージ・コンポーネント
Java プロキシー内で実行され、LDAP ディレクトリーやメッセージ・キューなどの特定のパスワード・ストアにパスワードを保管する Java コンポーネントです。パスワード・ストレージ・コンポーネントについて詳しくは、4 ページの『特殊コンポーネント』を参照してください。

Sun Directory Server 内のパスワードは、`userPassword` LDAP 属性に格納されます。Password Synchronizer は、`userPassword` LDAP 属性の更新をインターセプトします。

Sun Directory Server 用 Password Synchronizer は、すべてのオブジェクト・クラスのエントリーの `userPassword` 属性に対する変更をインターセプトします。

以下のタイプのエントリー変更におけるパスワード更新がインターセプトされます。

- 新規エントリーがディレクトリーに追加され、そのエントリーに `userPassword` 属性が含まれている。
- 既存のエントリーが変更され、変更された属性の 1 つが `userPassword` である。このエントリーには、次のようなケースが該当します。
  - `userPassword` 属性が追加された。例えば、エントリーに `userPassword` 属性がなかった場合などです。
  - `userPassword` 属性が変更された。例えば、エントリーにこの属性はあったが、その値は今回変更された場合などです。
  - `userPassword` 属性がエントリーから削除された。

注:

1. エントリーを削除した場合、このエントリーに `userPassword` 属性が含まれていても、Sun Directory Server 用 Password Synchronizer によるインターセプトは行われません。
2. Sun Directory Server 内の `userPassword` 属性は多値です。ユーザーは複数のパスワードを持つことができます。 Sun Directory Server 用 Password Synchronizer は、すべてのパスワード値のすべての変更をインターセプトして報告します。

ハッシュ済みパスワード

Password Synchronizer は、ハッシュ済みパスワード値を無視します。プレーン・テキスト・パスワードのみが同期されます。 Password Synchronizer は、ハッシュ済みパスワードを以下の場合に受信します。

- LDAP クライアントが、すでにハッシュされているパスワード値を送信し、Sun Directory Server がそれを受け入れた場合。ただし、Password Synchronizer はプレーン・テキスト・パスワードを取得できないので、それを無視します。例えば、LDAP クライアントが `"mypass"` ではなく `"{SHA}5yfRRkrhJDbomacm2lsvEdg4GyY="` を送信した場合、Password Synchronizer はパスワード・ストアにパスワードを送信しません。
- パスワードの暗号化が `"crypt"` や `"MD5"`、`"SHA-1"` のような一方向変換に設定されている場合、パスワードはハッシュ化された状態でディレクトリーに保管されます。複製操作は、ハッシュ済みパスワード値を使用して行われます。複製コンシューマー上の Password Synchronizer は、すでにハッシュ済みのパスワード値を受信します。

サポートされるプラットフォーム

Sun Directory Server 用 Password Synchronizer は、以下のプラットフォーム上の Sun Directory Server で使用可能です。

- Solaris 10 SPARC (32/64 ビット)、Sun ONE 5.2、Sun Java System Directory Server 7.0 (32/64 ビット)
- Solaris 11 SPARC (32/64 ビット)、Sun ONE 5.2、Sun Java System Directory Server 7.0 (32/64 ビット)

Sun Directory Server の Password Synchronizer のデプロイメントおよび構成

Sun Directory Server の Password Synchronization プラグインを構成するには、*TDI_install_dir*/pwd_plugins/sun/pwsync.props にインストールされているテンプレート構成ファイルを使用します。

Sun Directory Server プラグインが初期化されるとき、構成ファイルは、プラグインの登録行の最後のパラメーターとして設定されます。これにより、プラグインが構成ファイルを読み取るようになります。構成ファイルのいくつかのパラメーターは、プラグインと Java プロキシーで共有されます。サポートされるプロパティーの詳細なリストについては、13 ページの『第 3 章 パスワード同期プラグインの共通の構成およびユーティリティー』のセクションを参照してください。

以下のプロパティーは、Sun Directory Server の Password Synchronizer に固有のものです。

syncBase

このオプションのプロパティーを使用すると、パスワードがインターセプトされるディレクトリー・ツリーの部分を制限できます。指定するストリング値は、エントリーのパスワードがインターセプトされるツリーのルートの LDAP 識別名 (dn) です。例えば、`"o=ibm, c=us"` を指定したときは、以下のようになります。

- パスワード更新のインターセプト `"cn=Kyle Nguyen, ou=Austin, o=IBM, c=US"`。
- パスワード更新のスキップ `"cn=Henry Nguyen, o=SomeOtherCompany, c=US"`。

このプロパティーに値を設定していない場合、ディレクトリー・ツリー全体のパスワード更新がインターセプトされます。

Sun Directory Server への Sun Directory Server 用 Password Synchronizer の登録

Sun ONE Directory Server を登録するには、Directory Server Console を使用します。 Sun Java System Directory Server を登録するには、Sun Directory Server に付属する **dsconf** コマンド行ツールを使用する必要があります。

Sun ONE Directory Server 5.2 の登録

このタスクについて

プラグインを登録するには、Sun Directory Server を停止します。 Directory Server Management Console を使用して、Sun Directory Server の `dse.ldif` 構成ファイルに以下の行を追加します。

```
dn: cn=IBM DI PassSync,cn=plugins,cn=config
nsslapd-pluginPath: TDI_install_dir/pwd_plugins/sun/sunpwsync.dll
nsslapd-pluginEnabled: on
objectClass: top
objectClass: nsSlapdPlugin
objectClass: extensibleObject
cn: IBM DI PassSync
nsslapd-pluginType: object
nsslapd-pluginInitfunc: PWSyncInit
nsslapd-pluginarg0: TDI_install_dir/pwd_plugins/sun/pwsync.props
nsslapd-pluginId: ibmdi.pwsync
nsslapd-pluginVersion: 7.2
nsslapd-pluginVendor: IBM
nsslapd-pluginDescription: IBM Security Directory Integrator plug-in for password
synchronization
```

注: Solaris で実行中の 64 ビットの Sun Directory Server は、指定されたパスの下のディレクトリー内で 64 ビット・ライブラリーを検索します。

例えば、構成項目内の `nsslapd-pluginPath` の値を

```
nsslapd-pluginPath: TDI_install_dir/pwd_plugins/sun/libsunpwsync_64.so
```

に設定すると、Solaris オペレーティング環境で実行中の 64 ビットの Directory Server は、*TDI_install_dir*/pwd_plugins/sun/64/libsunpwsync_64.so という名前の 64 ビットのプラグイン・ライブラリーを検索します。

そのため Solaris では、Sun Directory Server 用 Password Synchronizer の 64 ビット・バイナリーがそのフォルダー内に付属します。

注: Sun Directory Server の dse.ldif 構成ファイルを手動で変更することがないようにする必要があります。以下のステップを実行し、LDIF ステートメントを Directory Server コンソールにインポートすることによって、プラグインを登録します。

1. LDIF コンテンツを LDIF ファイルに保存します。
2. Directory Server インスタンスを Directory Server コンソールで開きます。
3. 「**タスク**」タブに移動します。
4. 「**LDIF のインポート**」を選択します。
5. ファイルの場所を参照します。
6. 「**追加のみ**」のチェック・ボックスを選択します。
7. 「**エラー発生時に続行 (Continue on error)**」チェック・ボックスをクリアします。「**OK**」をクリックします。
8. Directory Server を再始動してプラグインをロードします。

Sun Java System Directory Server Enterprise Edition 7.0

このタスクについて

Directory Server が実行中であることを確認します。以下のステップを使用してプラグインを登録します。

手順

1. プラグイン・バイナリーを登録します。プラットフォームに応じて、以下の例のようにバイナリー名を sunpwsync.dll から libsunpwsync.so に変更します。

```
dsconf create-plugin <access options> -H
"TDI_install_dir/pwd_plugins/sun/sunpwsync.dll"
 -F PWSyncInit -Y object -G "TDI_install_dir/pwd_plugins/sun/pwsync.props"
"IBM DI PassSync"
```

2. プラグインを有効化します。

```
dsconf enable-plugin access-options "IBM DI PassSync"
```

3. Directory Server を再始動してプラグインをロードします。

タスクの結果

注:

- *access-options* プレースホルダーを、Directory Server への接続で使用するアクセス権限詳細および資格情報に置き換える必要があります。

  例えば、以下の場合は –p 1389 ––unsecured オプションを使用できます。
  - Directory Server がローカル・ホスト上にある場合。
  - それがポート 1389 で非 SSL 接続を受け入れる場合。

– それがデフォルトの管理者 DN cn=Directory Manager を使用する場合。

dsconf コマンド行ツールがサポートするオプションのリストについては、http://www.oracle.com/technetwork/indexes/documentation/index.html を参照してください。

- プラグインを登録抹消するには、以下のコマンドを使用することができます。

```
dsconf
delete-plugin access-options "IBM DI PassSync"
```

Sun Directory Server のロギングにおけるプラグインのロギングの使用可能化

Sun Directory Server の Password Synchronizer は、Sun Directory Server のエラー・ログにメッセージを記録します。パフォーマンス上の理由から、サーバー・プラグインからのメッセージは、エラー・ログに書き込まれません。

Sun ONE Directory Server 5.2 の使用可能化

手順

1. Directory Server コンソールで「**構成**」タブを選択します。
2. ナビゲーション・ツリーで、「Logs」フォルダーを展開し、「**エラーログ**」アイコンを選択します。
3. ウィンドウの右側にあるペインにエラー・ログの構成属性が表示されます。
4. エラーをログに記録するために「**ロギングを有効にする (Enable Logging)**」を選択します。
5. 「**ログ・レベル**」リスト・ボックスで「**プラグイン**」を選択します。
6. 「**保管**」をクリックします。

Sun Java System Directory Server Enterprise Edition 7.0 の使用可能化

手順

1. Directory Server が実行中であることを確認します。
2. Directory Server の **dsconf** ツールを使用して、以下のコマンドを実行します。

   ```
   dsconf set-log-prop access-options error level:err-plugins
   ```

   access-options について詳しくは、33 ページの『Sun Directory Server への Sun Directory Server 用 Password Synchronizer の登録』トピックを参照してください。

タスクの結果

現在のエラー・ログ・レベルを照会するには、以下のコマンドを実行します。

```
dsconf get-log-prop access-options error level
```

第 6 章 IBM Security Directory Server Password Synchronizer

IBM Security Directory Server Password Synchronizer は、IBM Security Directory Server の LDAP パスワードの変更をインターセプトします。

コンポーネント

IBM Security Directory Server プラグインを使用せずにパスワードを同期するソリューションを作成できます。ソリューションの作成について詳しくは、1 ページの『ソリューションの作成』を参照してください。

IBM Security Directory Integrator Password Synchronizer は、以下のパーツから構成されます。

IBM Security Directory Server プラグイン
このプラグインは、IBM Security Directory Server のプラグイン API を使用するネイティブ・バイナリーです。このプラグインは、IBM Security Directory Server のプロセス内で実行されます。

Java プロキシー
サーバー・プラグインによって開始または停止される別個の Java プロセスです。 このプロセスの主な目的は、パスワード・ストレージ・コンポーネントをホストし、プラグインと通信することです。Java プロキシーの詳細については、5 ページの『パスワード同期のアーキテクチャーおよびワークフロー』を参照してください。

パスワード・ストレージ・コンポーネント
Java プロキシー・プロセス内で実行され、特定のパスワード・ストア (LDAP ディレクトリーやメッセージ・キューなど) にパスワードを保管する Java コンポーネント。パスワード・ストレージ・コンポーネントについて詳しくは、4 ページの『特殊コンポーネント』を参照してください。

IBM Security Directory Server のパスワードは、`userPassword` LDAP 属性に保管されます。Password Synchronizer は、`userPassword` LDAP 属性の更新をインターセプトします。

IBM Security Directory Server Password Synchronizer は、すべてのオブジェクト・クラスのエントリーの `userPassword` 属性に対する変更をインターセプトします。

以下のタイプのエントリー変更におけるパスワード更新がインターセプトされます。

- 新規エントリーがディレクトリーに追加され、そのエントリーに `userPassword` 属性が含まれている。
- 既存のエントリーが変更され、変更された属性の 1 つが `userPassword` 属性である。このエントリーには、以下のケースが含まれます。
  - `userPassword` 属性が追加された。例えば、エントリーに `userPassword` 属性がなかった場合などです。

– userPassword 属性が変更された。例えば、エントリーにこの属性はあったが、その値は今回変更された場合などです。
– userPassword 属性がエントリーから削除された。

注:

1. エントリー (ユーザー) を削除した場合は、そのエントリーに userPassword 属性が含まれていても、IBM Security Directory Server Password Synchronizer によるインターセプトは行われません。
2. IBM Security Directory Server の userPassword 属性は、複数の値を持ちます。ユーザーは複数のパスワードを持つことができます。 IBM Security Directory Server Password Synchronizer は、すべてのパスワード値の変更をインターセプトして報告します。

サポートされるプラットフォーム

IBM Security Directory Server Password Synchronizer は、以下のプラットフォーム上にある、以下のバージョンの IBM Security Directory Server で使用可能です。

- Windows 2008 Standard Edition (x86/x86 – 64)、IBM Security Directory Server 6.1、6.2、および 6.3 (32/64 ビット)
- Windows 2008 Enterprise Edition (x86/x86 – 64)、IBM Security Directory Server 6.1、6.2、および 6.3 (32/64 ビット)
- Windows 2008 Datacenter Edition (x86/x86 – 64)、IBM Security Directory Server 6.1、6.2、および 6.3 (32/64 ビット)
- Windows 2008 R2 Standard Edition (x86/x86 – 64)、IBM Security Directory Server 6.1、6.2、および 6.3 (32/64 ビット)
- Windows 2008 R2 Enterprise Edition (x86/x86 – 64)、IBM Security Directory Server 6.1、6.2、および 6.3 (32/64 ビット)
- Windows 2008 R2 Datacenter Edition (x86/x86 – 64)、IBM Security Directory Server 6.1、6.2、および 6.3 (32/64 ビット)
- AIX® 6.1 (64 ビット)、IBM Security Directory Server 6.0 (64 ビット), IBM Security Directory Server 6.1、6.2、および 6.3 (64 ビット)
- AIX 7.1 (64 ビット)、IBM Security Directory Server 6.0 (64 ビット), IBM Security Directory Server 6.1、6.2、および 6.3 (64 ビット)
- Solaris 10 SPARC (64 ビット)、IBM Security Directory Server 6.1、6.2、および 6.3 (64 ビット)
- Solaris 11 SPARC (64 ビット)、IBM Security Directory Server 6.1、6.2、および 6.3 (64 ビット)
- RHEL ES/AS 5.0 (x86/x86 – 64)、IBM Security Directory Server 6.1、6.2、および 6.3 (32/64 ビット)
- RHEL ES/AS 6.0 (x86/x86 – 64)、IBM Security Directory Server 6.1、6.2、および 6.3 (32/64 ビット)
- SLES 10 (x86/x86 – 64)、IBM Security Directory Server 6.1、6.2、および 6.3 (32/64 ビット)
- SLES 11 (x86/x86 – 64)、IBM Security Directory Server 6.1、6.2、および 6.3 (32/64 ビット)

- RedFlag Data Center 5.0 SP1/Asianix 2.0 SP1、IBM Security Directory Server 6.1、6.2、および 6.3 (32 ビット)

デプロイメントおよび構成

プラグインをデプロイして構成する前に IBM Security Directory Server Password Synchronizer を IBM Security Directory Server に登録する必要があります。

IBM Security Directory Server へのプラグインの登録

プラグインを登録するには、IBM Security Directory Server の *ids_dir*/etc/ibmslapd.conf 構成ファイルを編集します。

注: このファイルを編集する前に、サーバーが実行されていないことを確認してください。

1. dn: cn=Directory, cn=RDBM Backends, cn=IBM Directory, cn=Schemas, cn=Configuration というセクションを検索して、以下の構成の詳細を追加します。

   Win32 ibm-slapdPlugin: preoperation "*TDI_install_dir*¥pwd_plugins¥tds¥idspwsync.dll" PWSyncInit "*TDI_install_dir*¥pwd_plugins¥tds¥pwsync.props"

   AIX64 ibm-slapdPlugin: preoperation "*TDI_install_dir*/pwd_plugins/tds/libidspwsync_64.a.so "PWSyncInit "*TDI_install_dir*/pwd_plugins/tds/pwsync.props"

   Linux32
   ibm-slapdPlugin: preoperation "*TDI_install_dir*/pwd_plugins/tds/libidspwsync.so" PWSyncInit "*TDI_install_dir*/pwd_plugins/tds/pwsync.props"
2. IBM Security Directory Server を再始動します。

IBM Security Directory Server Password Synchronizer の構成

IBM Security Directory Server プラグインのテンプレート構成ファイルは、*TDI_install_dir*/pwd_plugins/tds/pwsync.props にインストールされています。このプラグインが初期化されるとき、構成ファイルは、プラグインの登録行の最後のパラメーターとして設定されます。構成ファイルのいくつかのパラメーターは、プラグインと Java プロキシーで共有されます。サポートされるプロパティーのリストについては、13 ページの『第 3 章 パスワード同期プラグインの共通の構成およびユーティリティー』を参照してください。

syncBase プロパティーは、IBM Security Directory Server Password Synchronizer に固有のものです。

syncBase
このオプションのプロパティーを使用すると、パスワードがインターセプトされるディレクトリー・ツリーの部分を制限できます。指定するストリング値は、エントリーのパスワードがインターセプトされるツリーのルートの LDAP 識別名 (dn) です。例えば、"o=ibm, c=us" を指定したときは、以下のようになります。

- パスワード更新のインターセプト "cn=Kyle Nguyen, ou=Austin, o=IBM, c=US"。
- パスワード更新のスキップ "cn=Henry Nguyen, o=SomeOtherCompany, c=US"。

このプロパティーに値を設定しない場合、ディレクトリー・ツリー全体でパスワード更新がインターセプトされます。

第 7 章 IBM Domino HTTP Password Synchronizer

IBM Domino HTTP Password Synchronizer は、IBM Notes ユーザーのインターネット・パスワード (HTTP パスワードとも呼ばれる) の変更内容をインターセプトします。

概説

IBM Domino HTTP Password Synchronizer を使用すると、以下のタイプのパスワード変更をインターセプトできます。

管理上のパスワードのリセット

必要な権限を備えたユーザー (管理者など) は、古いパスワードの入力を求められることなく、自分のパスワードや他のユーザーのパスワードを変更できます。

HTTP パスワードを変更するには、以下を使用して、ユーザーの個人文書の「**インターネット・パスワード**」フィールドを編集します。

- IBM Domino Administrator クライアント
- Web ブラウザー・インターフェース

通常ユーザーのパスワード変更

ユーザーがパスワードを変更するときは、古いパスワードの入力を求められます。ユーザーは、以下からパスワードを変更できます。

- Web ブラウザー。IBM Domino Web サーバーの構成データベース `domcfg.nsf` からのパスワード変更フォームを使用します。
- IBM iNotes

IBM Domino サーバーでのデプロイメント

IBM Domino HTTP Password Synchronizer は、以下のモードでデプロイできます。

- 管理上のパスワードのリセットと通常ユーザーのパスワード変更の両方をインターセプトする
- 通常ユーザーのパスワード変更のみをインターセプトする
- 管理上のパスワードのリセットのみをインターセプトする

サポートされるプラットフォーム

IBM Domino HTTP Password Synchronizer は以下のプラットフォームでサポートされます。

- Windows Server 2008 Standard Edition (x86/x86-64)、IBM Domino 8.0 および IBM Domino 8.5.x
- Windows Server 2008 Enterprise Edition (x86/x86-64)、IBM Domino 8.0、および IBM Domino 8.5.x
- Windows Server 2008 Datacenter Edition (x86/x86-64)、IBM Domino 8.0、および IBM Domino 8.5.x

- Windows Server 2008 R2 Standard Edition (x86/x86-64)、IBM Domino 8.0、および IBM Domino 8.5.x
- Windows Server 2008 R2 Enterprise Edition (x86/x86-64)、IBM Domino 8.0、および IBM Domino 8.5.x
- Windows Server 2008 R2 Datacenter Edition (x86/x86-64)、IBM Domino 8.0、および IBM Domino 8.5.x
- AIX 6.1 (32/64 bit)、IBM Domino 8.0 および IBM Domino 8.5.x
- AIX 7.1 (PPC_64)、IBM Domino 8.0 および IBM Domino 8.5.x
- Solaris 10 SPARC (32/64 bit)、IBM Domino 8.0 および IBM Domino 8.5.x
- SLES 10 (x86)、IBM Domino 8.0 および IBM Domino 8.5.x
- SLES 10 (x86–64)、IBM Domino 8.0 および IBM Domino 8.5.x
- SLES 11 (x86)、IBM Domino 8.0 および IBM Domino 8.5.x
- SLES 11 (x86–64)、IBM Domino 8.0 および IBM Domino 8.5.x
- RHEL ES/AS 5.0 (x86)、IBM Domino 8.0 および IBM Domino 8.5.x
- RHEL ES/AS 5.0 (x86–64)、IBM Domino 8.0 および IBM Domino 8.5.x
- RHEL ES/AS 6.0 (x86)、IBM Domino 8.0 および IBM Domino 8.5.x
- RHEL ES/AS 6.0 (x86–64)、IBM Domino 8.0 および IBM Domino 8.5.x
- Red Flag Data Center 5.0 SP1 /Asianix 2.0 SP1、IBM Domino 8.0 および IBM Domino 8.5.x

インストールおよび構成ファイル・オプション

IBM Domino HTTP Password Synchronizer は、標準の IBM Security Directory Integrator インストーラー・ウィザードを使用してインストールされます。

構成ファイル・オプション

Domino プラグインのテンプレート構成ファイルは、*TDI_install_dir*/pwd_plugins/domino/pwsync.props にインストールされています。 UNIX の場合、構成ファイルは、IBM Domino サーバー・プラグインの初期化時に *domino_data_dir*/idipwsync/pwsync.props に存在している必要があります。 Windows の場合、構成ファイルは、*domino_program_dir*¥idipwsync¥pwsync.props に存在している必要があります。構成ファイルのいくつかのパラメーターは、プラグインと Java プロキシーで共有されます。サポートされるプロパティーのリストについては、13 ページの『第 3 章 パスワード同期プラグインの共通の構成およびユーティリティー』を参照してください。

IBM Domino Password Synchronizer には、固有のユーザー ID を使用してパスワード変更を同期するオプションがあります。このユーザー ID は、IBM Domino により提供され、対応する IBM Domino サーバー内でユーザーを固有に識別します。

以下の共通のプロパティーは、Domino プラグインで無視されます。

proxyStartExe

IBM Domino サーバーが始動すると、Java プロキシーは、Domino タスクとして始動されます。 IBM Domino サーバーがシャットダウンすると、Java プロキシーは、自動的に停止します。 stopProxy スクリプトを使用し

て、手動でシャットダウンを行うこともできます。 Java プロキシーを始動するために、IBM Domino サーバーは、**com.ibm.di.plugin.domino.ProxyLoader** クラスをインスタンス化します。このクラスは、ネイティブ Domino アドインであり、別個の Domino タスクです。IBM Domino サーバーは、その Domino タスク専用の別の JVM を始動するように構成されます。これは、notes.ini ファイルを編集しているときに runjava 行を追加して構成できます。

logFile Domino プラグインは、1 つではなく 3 つのログ・ファイルを使用するので、このプロパティーは無視されます。

共通の構成プロパティーに加えて、Domino プラグインは、以下のプロパティーを認識します。

admin.logFile
管理エージェントがログインするファイルを設定します。このファイルを設定しない場合、エージェントは、情報を一切ログに記録できません。デフォルト値は、idipwsync/admin.log です。

client.logFile
クライアント・エージェントがログインするファイルを設定します。このファイルを設定しない場合、エージェントは、情報を一切ログに記録できません。デフォルト値は、idipwsync/client.log です。

web.logFile
Web エージェントがログインするファイルを設定します。このファイルを設定しない場合、エージェントは、情報を一切ログに記録できません。デフォルト値は、idipwsync/web.log です。

useUniqueID
固有のユーザー ID をオンまたはオフにします。このプロパティーに true を設定した場合、プラグインは、実際のユーザー名ではなく、固有の ID を送信します。デフォルト値は false です。

ignoreMissingUniqueID
このプロパティーと useUniqueID プロパティーに true を設定した場合、プラグインは、useUniqueID が見つからないユーザーの同期をスキップします。デフォルト値は false です。

usernamePrefix
以下の条件の場合:

- usernamePrefix プロパティーが true に設定されている
- useUniqueID プロパティーが true に設定されている
- ignoreMissingUniqueID プロパティーが false に設定されている

プラグインは、ユーザーの識別名の前に usernamePrefix プロパティーの値を付加します。

インストール後の構成

プラグインのインストール後に、必要な構成ファイルを IBM Domino サーバーのデータ・ディレクトリーにコピーする必要があります。また、Password Synchronizer エージェントの署名者を作成する必要もあります。

以下のファイルを IBM Domino サーバーのデータ・ディレクトリーにコピーします。

- *TDI_install_dir*/pwd_plugins/jars フォルダーのすべてのファイルを、IBM Domino サーバー上の *domino_jvm_directory*/lib/ext フォルダーと、IBM Domino Designer がインストールされているシステム上の Lotus¥Notes¥jvm¥lib¥ext フォルダーにコピーします。
- ファイル idipwsync.nsf および pwsync_install_r8.nsf を、*TDI_install_dir*/pwd_plugins/domino フォルダーから IBM Domino サーバーのデータ・ディレクトリー *domino_data_dir* にコピーします。
- IBM Domino と Java のプロキシー構成ファイルを UNIX 上の *domino_data_directory*/idipwsync/pwsync.props にコピーします。この構成ファイル・テンプレートは、*TDI_install_dir*/pwd_plugins/domino/pwsync.props に含まれています。 Windows では、*domino_program_directory*¥idipwsync¥pwsync.props ファイルにコピーします。

注: Linux および UNIX ベースのプラットフォームでは、Domino ユーザー (デフォルトでは notes) を使用してパスワード・ストアをインストールし、パスワード・ストアを実行するのに必要な特権を Domino JVM に付与します。また、IBM Domino サーバーにコピーされたファイルを読み取るのに必要な特権を Domino ユーザーが持つようにします。

サーバーを再始動して新規ファイルをロードする必要があります。

Password Synchronizer エージェントの署名者

Password Synchronizer エージェントの署名者の作成には、以下のプロセスが必要です。

- エージェント署名者としての個人の作成
- 新たに生成した個人の ID ファイルのダウンロード
- pubnames.ntf および admin4.ntf テンプレートへの管理者アクセス権限の付与
- 署名者に対するメソッドおよび操作を制限なしで署名または実行特権の付与

Password Synchronizer エージェントの署名者の作成

プラグインをデプロイする前に、必要な特権を備えた IBM Security Directory Integrator Domino HTTP Password Synchronizer エージェントの署名者を作成する必要があります。

手順

1. IBM Domino Administrator を開きます。
2. 「**ユーザーとグループ**」タブをクリックします。
3. 右側のパネルで「**ユーザー**」 > 「**登録**」を選択します。
4. 「ユーザーの登録 (Register Person)」ウィザードの「**姓 (Last name)**」フィールドに IIDIPWSyncSigner と入力します。
5. 「**パスワード**」フィールドにパスワードを入力します。
6. 「**メールシステム (Mail system)**」フィールドで「**なし**」を選択します。

7. 「**このユーザーの Notes ID を作成 (Create a Notes ID for this person)**」チェック・ボックスを選択します。エージェントに署名するには、ID ファイルが使用されます。
8. 「**登録**」をクリックします。

次のタスク

『ID ファイルのダウンロード』

ID ファイルのダウンロード

新しく生成されたユーザーの ID ファイルを Domino ディレクトリーの個人文書からダウンロードする必要があります。

手順

1. IBM Domino Administrator を開きます。
2. 「**ユーザーとグループ**」タブをクリックします。
3. 左側のナビゲーション・パネルで、「**ユーザー**」ノードを開きます。
4. IDIPWSyncSigner ユーザーを選択します。
5. 「**ユーザーの編集**」をクリックして、個人文書を開きます。
6. UserID 添付ファイルを右クリックして、「**保存**」をクリックします。 UserID ファイルは、「基本」ウィンドウの左下隅に添付されています。
7. 個人文書を変更せずに閉じる場合は、「**キャンセル**」をクリックします。

次のタスク

『管理者アクセス権限の付与』

管理者アクセス権限の付与

署名者は、pubnames.ntf および admin4.ntf テンプレートへの管理者アクセス権限を持っていなければなりません。

手順

1. IBM Domino Administrator を開きます。
2. 「**ファイル**」タブをクリックします。
3. 「**表示 (Show me)**」から「**テンプレートのみ (Templates only)**」を選択します。
4. テンプレートのリストから「**admin4.ntf**」を選択します。
5. 「**admin4.ntf**」を右クリックし、「**アクセス制御**」 > 「**管理**」を選択します。
6. 「**追加**」をクリックします。
7. 「**IDIPWSyncSigner**」を選択します。
8. 「**種類 (User Type)**」リストから「**個人 (Person)**」を選択します。
9. 「**アクセス権限 (Access)**」リストで、「**管理者 (Manager)**」を選択します。
10. 「**OK**」をクリックして、「アクセスリスト (Access List)」ウィンドウを閉じます。

11. pubnames.ntf テンプレートに対して、ステップ 1 からステップ 10 を実行します。

次のタスク

『署名者に必要な特権の付与』

署名者に必要な特権の付与

メソッドおよび操作を制限なしで署名または実行特権を署名者に与える必要があります。

このタスクについて

注: 複数の IBM Domino サーバーがある場合、各サーバー上で以下のステップを実行する必要があります。

手順

1. IBM Domino Administrator を開きます。
2. 「**構成**」タブをクリックします。
3. 「**サーバー**」 > 「**すべてのサーバー文書 (All Server Documents)**」 を選択します。
4. サーバー文書を選択します。
5. 「**サーバーの編集 (Edit Server)**」 をクリックします。
6. 「**セキュリティー**」タブをクリックします。
7. 「**Programmability の制限 (Programmability Restrictions)**」セクションで、「**メソッドおよび操作を制限なしで署名または実行 (sign or run unrestricted methods and operations)**」フィールドに署名者を追加します。
8. 「**保存して閉じる**」をクリックします。

単一 IBM Domino サーバーでのデプロイメント

単一 IBM Domino サーバーにプラグインをデプロイするには、必要な構成ステップを実行する必要があります。

IBM Domino HTTP Password Synchronizer を IBM Domino にインストールするには、IBM Domino サーバーがインストールされているシステムでインストーラーを実行します。インストールにより適切なディレクトリー構造に必要なすべてのファイルが配置されます。

IBM Domino サーバーのデータ・ディレクトリーのファイル・パスを以下に示します。

- IBM Domino サーバーのプログラム・フォルダーは、*domino_program_directory* です。例えば、Windows プラットフォームの場合は、C:¥Program Files¥IBM¥Lotus¥Domino です。 Linux ベースおよび UNIX ベースのプラットフォームの場合は、/opt/ibm/lotus です。
- IBM Domino サーバーのデータ・フォルダーは、*domino_data_directory* です。例えば、Windows プラットフォームの場合は、C:¥Program

Files¥IBM¥Lotus¥Domino¥Data です。 Linux ベースおよび UNIX ベースのプラットフォームの場合は、/local/notesdata です。

- IBM Domino サーバーの JVM フォルダーは、*domino_jvm_directory* です。例えば、Windows プラットフォームの場合は、C:¥Program Files¥IBM¥Lotus¥Domino¥jvm です。 Linux ベースおよび UNIX ベースのプラットフォームの場合は、/opt/ibm/lotus/notes/80000/linux/jvm です。

注:

1. IBM Domino HTTP Password Synchronizer には、*TDI_install_dir*/pws_plugins/domino/pwsync.props テンプレート構成ファイルが付属しています。このファイルには、必要なすべてのプロパティーがデフォルトで事前設定されており、すぐに使用することが可能です。
2. 付属の pwsync.props ファイルで構成されているデフォルトのパスワード・ストアは、Log パスワード・ストアです。このパスワード・ストアは、取り込んだすべてのパスワードをプロキシーのログ・ファイルに記録します。このパスワード・ストアは、診断の目的でのみ使用してください。

以下の表は、デプロイメント・ステップを示しています。

ステップ	説明
1	インストール後のフェーズでコピーされた新規ファイルが IBM Domino サーバーによって読み取られることを確認します。
2	IBM Security Directory Integrator に付属の外部データベースは、その整合性を保証できるようにするために IBM Domino サーバーが署名する必要があります。 49 ページの『サーバー ID を使用したデータベースの署名』を参照してください。
3	pubnames.ntf テンプレートを編集することにより、names.nsf データベースの動作を変更できます。プレーン・パスワードをインターセプトするためのコードがいくつかの主要な場所に配置されます。パスワードは、取り込まれた後に適切な Java エージェント (IDIPWSyncClientAgent や IDIPWSyncWebAgent など) に渡されます。 49 ページの『pubnames.ntf テンプレート設計の更新』を参照してください。
4	admin4.ntf テンプレートを編集することにより、admin4.nsf データベースの動作を変更できます。コピーされた Java エージェント IDIPWSyncAdminRequestAgent は、各種ユーザーがパスワード変更時に送信する管理要求を定期的に処理します。 53 ページの『admin4.ntf テンプレート設計の更新』を参照してください。
5	エージェントは、エージェントの署名者の権限で実行されます。 Password Synchronizer のエージェントは、ネットワーク・アクセスまたはファイル・システム・アクセスなどの制限付き操作を実行する必要があります。 したがって、このエージェントは、メソッドおよび操作を制限なしで署名または実行 (Sign or run unrestricted methods and operations) 特権を備えたユーザーが署名してください。 54 ページの『署名者を使用したエージェントの署名』を参照してください。

ステップ	説明
6	names.nsf データベースの設計を更新すると、変更されたテンプレートが既存のデータベースに適用されます。 55 ページの『names.nsf データベース設計のリフレッシュ』を参照してください。
7	admin4.nsf データベースの設計を更新すると、変更されたテンプレートが既存のデータベースに適用されます。 56 ページの『admin4.nsf データベースの設計のリフレッシュ』を参照してください。
8	各種の Java エージェントは、さらに処理が必要な文書を保管するために idipwsync.nsf データベースを使用します。このデータベースで文書を保護するために、文書を暗号化する必要があります。このステップで作成される秘密鍵は、データベース暗号化プロセスで使用されます。 56 ページの『秘密鍵暗号化インフラストラクチャーのセットアップ』を参照してください。
9	ポートの暗号化では IBM Domino Administrator と IBM Domino サーバーの間の通信が暗号化されます。これにより、ネットワーク通信がさらに安全になります。 58 ページの『ポート暗号化のセットアップ』を参照してください。
10	Web ブラウザーと IBM Domino HTTP Server 間の通信を保護するためには SSL が必要です。SSL をセットアップしない場合、パスワードはネットワーク上で非暗号化テキストとして送信されます。 59 ページの『IBM Domino HTTP Server の SSL のセットアップ』を参照してください。
11	Java プロキシーは、IBM Domino に付属の JVM で実行されます。 IBM Domino サーバーを始動すると、プロセスがサーバー・タスクとして始動します。 59 ページの『Java プロキシーを自動的に始動および停止するための IBM Domino サーバーの構成』を参照してください。
12	管理パスワードを変更できるように各 IBM Domino Administrator クライアントを構成します。 59 ページの『IBM Domino Administrator クライアントの実行コントロール・リストの構成』を参照してください。
13	IDIPWSync グループには、他のユーザーのパスワードを変更する権限を備えたユーザーのリストが含まれます。通常、このグループには、管理者のみが存在します。通常のユーザーは、このグループに属していなくても、IBM iNotes を通じてパスワードを変更することが可能です。 idipwsync.nsf データベースにアクセスできるのは、このグループのメンバーに限られます。idipwsync.nsf データベースは、Lotus® スクリプトと Password Synchronizer エージェントの間でデータを転送するために使用されます。 Password Synchronizer エージェントが idipwsync.nsf データベースにアクセスできるようにするために、このエージェントの署名者は IDIPWSync グループにも追加する必要があります。エージェントは、エージェントの署名者の権限で実行されます。 60 ページの『アクセス制御リストの構成』を参照してください。

ステップ	説明
14	pwsync_install_r8.nsf データベースは、必要なテンプレート・オブジェクトを配布するためにのみ使用されます。 IBM Domino HTTP プラグインをセットアップする際は、このデータベースは既に不要なため、削除できます。 61 ページの『pwsync_install_r8.nsf データベースの削除』を参照してください。

サーバー ID を使用したデータベースの署名

アクティブ・サーバー ID を使用して、pwsync_install_r8.nsf データベースと idipwsync.nsf データベースに署名する必要があります。

手順

1. IBM Domino Administrator を開始します。
2. 「**ファイル**」をクリックします。
3. pwsync_install_r8 データベースを右クリックし、「**署名**」を選択します。
4. 「**どちらの ID を使用しますか？**」にある「**データベースの署名**」の「**現在のサーバー ID**」を選択します。
5. **IDIPWSync** データベースを右クリックし、「**署名**」を選択します。
6. 「**どちらの ID を使用しますか？**」にある「**データベースの署名**」の「**現在のサーバー ID**」を選択します。
7. 「**OK**」をクリックします。

次のタスク

『pubnames.ntf テンプレート設計の更新』

pubnames.ntf テンプレート設計の更新

names.nsf データベースに必要な変更を加えるには、pubnames.ntf テンプレートを編集する必要があります。

手順

1. IBM Domino Designer を開始します。
2. 以下の項目を開きます。
   a. pwsync_install_r8.nsf データベースを開きます。
   b. pubnames.ntf テンプレートを開きます。
3. エージェントをコピーします。
   a. pwsync_install_r8.nsf データベースで、「**コード/エージェント (Code/Agent)**」を選択します。
   b. IDIPWSyncClientAgent エージェントと IDIPWSyncWebAgent エージェントを選択します。
   c. 選択したエージェントを右クリックして「**コピー**」を選択します。
   d. **pubnames.ntf** で、「**コード/エージェント (Code/Agent)**」を選択します。
   e. 「**編集**」 > 「**貼り付け**」を選択し、2 つのエージェントを貼り付けます。

注: ユーザーがカスタマイズしたロジックを使用して「**ユーザー**」フォームが変更されていない場合は、Password Synchronizer の「**ユーザー**」フォームが使用されます。

4. 以下の手順で、「**ユーザー**」フォームの名前を pubnames.ntf で変更します。
   a. pubnames.ntf データベースで「**フォーム**」を選択します。
   b. 「**ユーザー**」フォームを開きます。
   c. 「**設計**」 > 「**フォームのプロパティー**」を選択します。
   d. 「**名前**」フィールドを編集します。名前を「**original_Person**」に変更するか、「**ユーザー**」以外の任意の名前に変更します。

      注: デフォルトの別名である「ユーザー」の設定を、このフィールドから解除できることを確認してください。
   e. フォームを保管します。
   f. フォームを閉じます。
5. 「**ユーザー**」フォームをコピーします。
   a. pwsync_install_r8.nsf で「**フォーム**」を選択します。
   b. 「**ユーザー**」フォームを右クリックし「**コピー**」を選択します。
   c. pubnames.ntf データベースで「**フォーム**」を選択します。
   d. 「**編集**」 > 「**貼り付け**」を選択してフォームを貼り付けます。
   e. 「**編集**」**->**「**貼り付け**」を選択してフォームを貼り付けます。

      ユーザーがカスタマイズしたロジックを使用して「**ユーザー**」フォームが変更されていて、このロジックを残しておきたい場合は、その「ユーザー」フォームの Password Synchronizer ソース・コードを手動でコピーします。
6. 以下の手順により、「**ユーザー**」フォームのソース・コードをコピーします。
   a. WebQuerySave イベントのコードをコピーします。
      1) pwsync_install_r8.nsf データベースで「**フォーム**」を選択します。
      2) 「**ユーザー**」フォームを開きます。
      3) WebQuerySave イベントを選択します。
      4) 以下のコードで始まり、

         ```
         REM {start of IDI Password Synchronizer code};
         ```

         以下のコードで終わる行をコピーします。

         ```
         REM {end of IDI Password Synchronizer code};
         ```
      5) pubnames.ntf データベースで「**フォーム**」を選択します。
      6) 「**ユーザー**」フォームを開きます。
      7) WebQuerySave イベントを選択します。
      8) コピーしたソース・コードを貼り付けます。このコードは、このイベント内の他のどのコードよりも前の位置に貼り付けてください。
      9) フォームを保管します。
   b. Querysave イベントのコードをコピーします。
      1) pwsync_install_r8.nsf で「**フォーム**」を選択します。
      2) 「**ユーザー**」フォームを開きます。

3) Querysave イベントを選択します。
4) 以下のコードで始まり、

```
'start of Password Synchronizer code
```

以下のコードで終わる行をコピーします。

```
'end of Password Synchronizer code
```

.

5) pubnames.ntf データベースで「**フォーム**」を選択します。
6) 「**ユーザー**」フォームを開きます。
7) Querysave イベントを選択します。
8) コピーしたソース・コードを貼り付けます。このコードは、Querysave プロシージャーの末尾の直前に貼り付けてください。
9) フォームを保管します。

c. SyncPass イベントのコードをコピーします。
1) pwsync_install_r8.nsf データベースで「**フォーム**」を選択します。
2) 「**ユーザー**」フォームを開きます。
3) SyncPass イベントを選択します。
4) **SyncPass** 関数の全コードをコピーします。
5) pubnames.ntf データベースで「**フォーム**」を選択します。
6) 「**ユーザー**」フォームを開きます。
7) Querysave イベントを選択します。
8) コピーしたソース・コードを貼り付けます。このコードは、このイベント内のどのコードよりも後ろの位置に貼り付けてください。SyncPass という新しいイベントが作成され、貼り付けたコードがこのイベントに転送されます。
9) フォームを保管します。

ユーザーがカスタマイズしたロジックを使用して $PersonInheritableSchema サブフォームが変更されていない場合は、Password Synchronizer の $PersonInheritableSchema が使用されます。

7. pubnames.ntf にある $PersonInheritableSchema サブフォームを名前変更します。
a. pubnames.ntf データベースで、「**共有要素/サブフォーム (Shared Elements/Subforms)**」を選択します。
b. 「$PersonInheritableSchema」サブフォームを開きます。
c. 「**設計**」 > 「**サブフォームのプロパティー**」を選択します。
d. 「**名前**」フィールドを編集します。名前を **original_$PersonInheritableSchema** に変更するか、**$PersonInheritableSchema** 以外の任意の名前に変更します。
e. フォームを保管します。
f. フォームを閉じます。
8. $PersonInheritableSchema サブフォームをコピーします。

a. pwsync_install_r8.nsf データベースで、「**共有要素/サブフォーム (Shared Elements/Subforms)**」を選択します。

b. 「$PersonInheritableSchema」フォームを右クリックして「**コピー**」を選択します。

c. pubnames.ntf データベースで「**共有要素/サブフォーム (Shared Elements/Subforms)**」を選択します。

d. 「**編集**」 > 「**貼り付け**」を選択してサブフォームを貼り付けます。

ユーザーがカスタマイズしたロジックを使用して $PersonInheriableSchema サブフォームが変更されていて、このロジックを残しておきたい場合は、Password Synchronizer ソース・コードを手動でコピーする必要があります。

9. 以下のように $PersonInheritableSchema サブフォームのコードをコピーします。

a. 以下の手順により、**HTTPPassword** フィールドのコードをコピーします。

1) pwsync_install_r8.nsf データベースで「**共有要素/サブフォーム (Shared Elements/Subforms)**」を選択します。

2) 「$PersonInheritableSchema」サブフォームを開きます。

3) (フォームの下部にある)「**HTTPPassword**」フィールドを選択します。

4) 「**入力の変換**」 イベントを選択します。

5) 以下のコードで始まり、

```
REM {start of IDI Password Synchronizer code};
```

以下のコードで終わる行をコピーします。

```
REM {end of IDI Password Synchronizer code};
```

6) pubnames.ntf データベースで「**共有要素/サブフォーム (Shared Elements/Subforms)**」を選択します。

7) 「$PersonInheritableSchema」フォームを開きます。

8) 「**HTTPPassword**」フィールドを選択します。

9) 「**入力の変換**」 イベントを選択します。

10) コピーしたソース・コードを貼り付けます。このコードは、このイベント内の他のどのコードよりも前の位置に貼り付けてください。

11) フォームを保管します。

b. 以下の手順により、「パスワードの入力」ボタンのコードをコピーします。

1) pwsync_install_r8.nsf データベースで「**共有要素/サブフォーム (Shared Elements/Subforms)**」を選択します。

2) 「$PersonInheritableSchema」サブフォームを開きます。

3) フォームの末尾付近にある「**パスワードの入力**」を選択します。

4) 「**クリック**」イベントを選択し、「**実行**」フィールドが client に設定されていることを確認します。

5) 以下のコードで始まり、

```
REM {start of IDI Password Synchronizer code};
```

以下のコードで終わる行をコピーします。

```
REM {end of IDI Password Synchronizer code};
```

6) pubnames.ntf データベースで、「**共有要素/サブフォーム (Shared Elements/Subforms)**」を選択します。
7) 「$PersonInheritableSchema」フォームを開きます。
8) 「**パスワードの入力**」を選択します。
9) 「**クリック**」イベントを選択します。右側の「**実行**」フィールドを client に設定します。
10) コピーしたソース・コードを貼り付けます。このコードは、以下の場所に貼り付けてください。
    - 受信したパスワード tmpPassword を検証するコードの後。
    - すべての文書フィールドをリフレッシュするコードの前 (例: @Command([ViewRefreshFields]);)。
11) フォームを保管します。

c. 以下の手順により、**FullName** フィールドのコードをコピーします。
1) pwsync_install_r8.nsf データベースで「**共有要素/サブフォーム (Shared Elements/Subforms)**」を選択します。
2) 「$PersonInheritableSchema」サブフォームを開きます。
3) 「**FullName**」フィールドを選択します。
4) 「**入力の確認**」イベントを選択します。
5) 以下のコードで始まり、

```
REM {start of IDI Password Synchronizer code};
```

以下のコードで終わる行をコピーします。

```
REM {end of IDI Password Synchronizer code};
```

6) pubnames.ntf データベースで「**共有要素/サブフォーム (Shared Elements/Subforms)**」を選択します。
7) 「$PersonInheritableSchema」フォームを開きます。
8) 「**FullName**」フィールドを選択します。
9) 「**入力の確認**」イベントを選択します。
10) コピーしたソース・コードを、このイベントの他のすべてのコードの先頭に貼り付けます。
11) フォームを保管します。

次のタスク

『admin4.ntf テンプレート設計の更新』

admin4.ntf テンプレート設計の更新

admin4.nsf データベースに必要な変更を加えるには、admin4.ntf テンプレートを編集する必要があります。

手順

1. IBM Domino Designer で、admin4.ntf テンプレート・データベースと pwsync_install_r8.nsf データベースを開きます。

2. 以下の手順により、**IDIPWSyncAdminRequestAgent** エージェントをコピーします。
   a. pwsync_install_r8.nsf で「**コード/エージェント (Code/Agents)**」を選択します。
   b. **IDIPWSyncAdminRequestAgent** を選択します。
   c. 選択したエージェントを右クリックして「**コピー**」を選択します。
   d. admin4.ntf で「**コード/エージェント (Code/Agents)**」を選択します。
   e. 「**編集**」 > 「**貼り付け**」を選択し、選択したエージェントを貼り付けます。
3. **IDIPWSyncAdminRequestAgent** を構成します。
   a. **IDIPWSyncAdminRequestAgent** エージェントを開きます。
   b. 「**編集**」 > 「**プロパティー**」を選択します。
   c. エージェント・ダイアログ・ボックスの「ランタイム」セクションの「**設定の編集**」をクリックします。
   d. 「**実行場所 (Run on)**」フィールドで、現在の IBM Domino サーバーの名前を選択します。
   e. 「**OK**」をクリックします。
   f. エージェント・ダイアログ・ボックスを閉じます。
   g. 「**ファイル**」 > 「**保存**」を選択し、新しいエージェントの設定を保存します。

   「あなたはエージェント IDIPWSyncAdminRequestAgent (TDITest/IBM) の実行アクセス権がありません。エージェントは実行されません。」という警告メッセージが表示される場合があります。 IBM Domino Designer で現在使用している Domino アカウントは、IBM Domino Designer 上でメソッドおよび操作を制限なしで署名または実行を行うことはできません。そのため、専用の署名者を使用してエージェントに署名する必要があります。

次のタスク

『署名者を使用したエージェントの署名』

署名者を使用したエージェントの署名

Password Synchronizer のエージェントは、ネットワーク・アクセスまたはファイル・システム・アクセスなどの制限付き操作を実行する必要があります。したがって、エージェントは、「メソッドおよび操作を制限なしで署名または実行 (sign or run unrestricted methods and operations)」特権をもった個人によって署名される必要があります。

手順

1. サーバー文書の「**セキュリティー**」タブ上の「**メソッドおよび操作を制限なしで署名または実行 (Sign or run unrestricted methods and operations)**」フィールドにリストされている署名者の名前を見つけます。サーバー文書にアクセスするには、次のようにします。
   a. IBM Domino Administrator を開始します。
   b. 「**構成**」を選択します。

c. 左のナビゲーション・パネルで、「**サーバー**」 > 「**現在のサーバー文書**」を選択します。

この特権を持った既存のアカウントがない場合、署名者を追加する必要があります。詳しくは、 44 ページの『Password Synchronizer エージェントの署名者の作成』を参照してください。 「メソッドおよび操作を制限なしで署名または実行 (sign or run unrestricted methods and operations)」特権は、信頼できるアカウントにのみ与えます。署名者は、pubnames.ntf および admin4.ntf テンプレートへのマネージャー・アクセス権を持っていなければなりません。

2. IBM Domino Designer をオープンします。
3. 署名者の ID に切り替えるには、「**ファイル**」 > 「**セキュリティー**」 > 「**ID の切り替え**」に進みます。
4. pubnames.ntf テンプレートを開きます。
5. 「**コード (Code)**」 > 「**エージェント (Agents)**」を選択し、すべてのエージェントのリストを開きます。
6. エージェントのリストから、「**IDIPWSyncClientAgent**」を選択します。
7. 「**署名 (Sign)**」をクリックし、現行 ID を使用してエージェントに署名します。
8. エージェントのリストから、「**IDIPWSyncWebAgent**」を選択します。
9. 「**コード (Code)**」 > 「**エージェント (Agents)**」を選択し、すべてのエージェントのリストを開きます。
10. エージェントのリストから、「**IDIPWSyncAdminAgent**」を選択します。
11. 「**署名 (Sign)**」をクリックします。
12. 前に使用していた ID に切り替えるには、「**ファイル**」 > 「**セキュリティー**」 > 「**ID の切り替え**」を選択します。

次のタスク

『names.nsf データベース設計のリフレッシュ』

names.nsf データベース設計のリフレッシュ

変更内容をテンプレートから既存のデータベースに適用するには、names.nsf データベースをリフレッシュする必要があります。

手順

1. IBM Domino Administrator から、「**ファイル**」タブをクリックします。
2. names.nsf データベースを選択します。
3. 「**ファイル**」 > 「**アプリケーション**」 > 「**設計の更新 (Refresh Design)**」に進みます。
4. 「**サーバー**」リストから、ご使用のサーバーの名前を選択します。
5. 「**OK**」をクリックします。
6. 「**はい**」をクリックして続行します。

次のタスク

56 ページの『admin4.nsf データベースの設計のリフレッシュ』

admin4.nsf データベースの設計のリフレッシュ

変更内容をテンプレートから既存のデータベースに適用するには、admin4.nsf データベースをリフレッシュする必要があります。

手順

1. IBM Domino Administrator から、「**ファイル**」タブをクリックします。
2. admin4.nsf データベースを選択します。
3. 「**ファイル**」 > 「**アプリケーション**」 > 「**設計の更新 (Refresh Design)**」を選択します。
4. 「**サーバー**」リストから、ご使用のサーバーの名前を選択します。
5. 「**OK**」をクリックします。
6. 「**はい**」をクリックして先へ進みます。

次のタスク

『秘密鍵暗号化インフラストラクチャーのセットアップ』

秘密鍵暗号化インフラストラクチャーのセットアップ

Java エージェントは idipwsync.nsf データベースを使用して、パスワードをさらに処理するために必要な文書を保管します。このデータベース内のそうした文書を保護するには、文書を暗号化する必要があります。

手順

1. 秘密鍵の生成
   a. IBM Domino Administrator で、「**ファイル**」 > 「**セキュリティ情報**」 > 「**ユーザーセキュリティ**」を選択します。
   b. 左のナビゲーション・パネルから「**Notes データ (Notes Data)**」 > 「**文書**」を選択します。
   c. 「**シークレットキーの作成**」をクリックします。
   d. 秘密鍵の名前として「**IDIPWSync**」を入力し、「**OK**」をクリックします。
   e. 「**その他のアクション (Other Actions)**」をクリックし、「**シークレットキーの書き出し (Export Secret Key)**」を選択します。
   f. エクスポートされた秘密鍵を保護するパスワードを入力します。

      注: このステップはオプションです。
   g. 鍵をファイル idipwsync.key に保管します。
   h. 「**クローズ**」をクリックします。
2. 秘密鍵を IBM Domino サーバー ID ファイルにインポートします。
   a. IBM Domino サーバーを停止します。
   b. IBM Domino Administrator で、「**ファイル**」 > 「**セキュリティー**」 > 「**ID の切り替え**」を選択します。
   c. IBM Domino サーバーの server.id ファイルを開きます。IBM Domino サーバー・システムにインストールされている IBM Domino Administrator を使用するか、または IBM Domino Administrator のインストール先のシステムに

server.id ファイルをコピーする必要があります。server.id ファイルは、*domino_data_directory* に保存します。

d. 「**ファイル**」 > 「**セキュリティ情報**」 > 「**ユーザーセキュリティ**」を選択します。

e. 左のナビゲーション・パネルから「**Notes データ (Notes Data)**」 > 「**文書**」を選択します。

f. 「**その他のアクション (Other Actions)**」をクリックし、「**シークレットキーの呼び出し (Import Secret Key)**」を選択します。

g. idipwsync.key ファイルを開きます。

h. ファイルがパスワードで保護されている場合は、秘密鍵のエクスポート時に作成したパスワードを入力します。パスワードについての詳細は、ステップ 1 のサブステップ f を参照してください。

i. 「**受諾**」をクリックして秘密鍵をインポートします。

j. 「**クローズ**」をクリックします。

k. 「**ファイル**」 > 「**セキュリティー**」 > 「**ID の切り替え**」を選択し、管理者 ID ファイルに切り替えます。

l. server.id ファイルのコピーを編集したら、それで *domino_data_directory* ディレクトリー内の元の server.id ファイルを上書きコピーします。元の server.id をバックアップしてから、そのファイルを新規ファイルで上書きしてください。

m. IBM Domino サーバーを開始します。

3. すべての管理者またはユーザーの ID ファイルに秘密鍵をインポートして、個人文書を編集し、HTTP パスワードを変更します。それらの管理者またはユーザーのそれぞれに対して、以下のステップを実行します。

a. IBM Domino Administrator で、「**ファイル**」 > 「**セキュリティー**」 > 「**ID の切り替え**」を選択します。

b. 管理者またはユーザーの ID ファイルを開きます。

c. 「**ファイル**」 > 「**セキュリティ情報**」 > 「**ユーザーセキュリティ**」を選択します。

d. 左のナビゲーション・パネルから「**Notes データ (Notes Data)**」 > 「**文書**」を選択します。

e. 「**その他のアクション (Other Actions)**」をクリックし、「**シークレットキーの呼び出し (Import Secret Key)**」を選択します。

f. idipwsync.key ファイルを開きます。

g. ファイルがパスワードで保護されている場合は、秘密鍵のエクスポート時に作成したパスワードを入力します。秘密鍵の作成方法については、ステップ 1 を参照してください。

h. 「**受諾**」をクリックして秘密鍵をインポートします。

i. 「**クローズ**」をクリックします。

注: 管理者とユーザーの ID ファイルには、個人文書の「**HTTP パスワード**」フィールドを変更するための秘密暗号鍵を入れないでください。

次のタスク

『ポート暗号化のセットアップ』

ポート暗号化のセットアップ

ポートの暗号化では、IBM Domino Administrator と IBM Domino サーバーの間の通信が暗号化されます。これにより、ネットワーク通信のセキュリティーがさらに強化されます。

このタスクについて

ポート暗号化はオプションです。ポートの暗号化を使用するかどうかに関係なく、パスワードは秘密鍵で暗号化されてからネットワークに送信されます。

選択可能なオプションは以下のとおりです。

- 通信ポートを暗号化するように IBM Domino サーバーをセットアップします。IBM Notes クライアントを使用してセットアップできます。サーバーの設定のみを構成します。ただし、その設定は、正規ユーザーも含めたすべてのクライアントとの通信に影響を与えます。
- 通信ポートを暗号化するように IBM Domino Administrator クライアントをセットアップします。このセットアップには、使用する各 IBM Domino Administrator クライアントの構成が必要です。ただしこの設定は、暗号化が必要でない場合には、他の IBM Notes クライアントには影響を与えません。暗号化を行うには、以下のステップを実行します。

手順

1. IBM Domino サーバーの通信ポートの暗号化
   a. IBM Domino Administrator で、「**構成**」タブを選択します。
   b. 「**サーバー**」 > 「**ポートのセットアップ (Setup Ports)**」を選択します。
   c. 使用中の通信ポートごとに、「**通信ポート**」リストからポートを選択して「**ネットワークデータの暗号化**」を選択します。
   d. 「**OK**」をクリックします。
   e. IBM Domino サーバーを再始動して、変更を有効にします。
2. IBM Domino Administrator 通信ポートを暗号化します。パスワード変更に使用する予定の IBM Domino Administrator クライアントごとに、以下のステップを実行します。
   a. IBM Domino Administrator で、「**ファイル**」 > 「**設定**」 > 「**ユーザー設定**」を選択します。
   b. 左方のナビゲーション・パネルから「**ポート**」を選択します。
   c. 使用中の通信ポートごとに、「**通信ポート**」リストからポートを選択して「**ネットワークデータの暗号化**」を選択します。
   d. 「**OK**」をクリックします。
   e. IBM Domino Administrator を再始動して、変更を有効にします。

次のタスク

59 ページの『IBM Domino HTTP Server の SSL のセットアップ』

IBM Domino HTTP Server の SSL のセットアップ

Web ブラウザーと IBM Domino HTTP Server 間の通信を保護するためには SSL が必要です。SSL をセットアップしない場合、パスワードはネットワーク上で非暗号化テキストとして送信されます。

このタスクについて

SSL のセットアップについての詳細は、IBM Domino Administrator のヘルプ資料を参照してください。

次のタスク

『Java プロキシーを自動的に始動および停止するための IBM Domino サーバーの構成』

Java プロキシーを自動的に始動および停止するための IBM Domino サーバーの構成

Java プロキシーは、IBM Domino に付属の JVM で実行されます。 IBM Domino サーバーを始動すると、プロキシーは、サーバー・タスクとして始動します。

手順

1. *domino_program_directory*/notes.ini ファイルを開き、ServerTasks プロパティーを探します。
2. ServerTasks プロパティーの末尾に次の値を追加します。

   ```
   runjava com.ibm.di.plugin.domino.ProxyLoader
   ```

   notes.ini の ServerTasks プロパティーのサンプルを次に示します。

   ```
   ServerTasks=Update,Replica,Router,AMgr,AdminP,CalConn,Sched,HTTP,runjava
   com.ibm.di.plugin.domino.ProxyLoader
   ```

次のタスク

『IBM Domino Administrator クライアントの実行コントロール・リストの構成』

IBM Domino Administrator クライアントの実行コントロール・リストの構成

管理パスワードを変更できるように各 IBM Domino Administrator クライアントを構成する必要があります。

手順

1. IBM Domino Administrator で、「**ファイル**」 > 「**セキュリティ情報**」 > 「**ユーザーセキュリティ**」を選択します。
2. 左側のナビゲーション・パネルで「**実効制御**」 > 「**ワークステーション**」を選択します。
3. 「**署名者**」リストで、ご使用の IBM Domino サーバーの名前を選択します (serverName や certifierName など)。ご使用の IBM Domino サーバー名がリストに見当たらない場合は、リストに追加してください。
4. 「**アクセスできる操作:**」の下で「**現在のデータベース**」を選択します。

5. 「**実行できる操作:**」の下で「**他データベースの読み込み**」と「**他データベースの変更**」を選択します。
6. 「**OK**」をクリックします。

次のタスク

『アクセス制御リストの構成』

アクセス制御リストの構成

Domino ディレクトリーに IDIPWSync グループを作成し、idipwsync.nsf データベースのアクセス制御リスト (ACL) を更新する必要があります。 idipwsync.nsf データベースにアクセスできるのは、IDIPWSync グループのメンバーに限られます。

手順

1. Domino ディレクトリーに **IDIPWSync** グループを作成します。
   a. IBM Domino Administrator から「**ユーザーとグループ**」タブをクリックします。
   b. 左側のナビゲーション・パネルで、「**Domino ディレクトリ**」/「***your_domain* ディレクトリー**」/「**グループ**」を選択します。ここで、*your_domain* は IBM Domino ドメインの名前です。
   c. 「**グループの追加**」をクリックします。
   d. 「**グループ名**」フィールドに **IDIPWSync** と入力します。
   e. 個人文書を編集してパスワードを変更できるすべての管理者またはユーザーを「**メンバー**」フィールドに追加します。
   f. 「**メンバー**」フィールドで Password Synchronizer のエージェントを署名する署名者を追加します。
2. idipwsync.nsf データベースのアクセス・コントロール・リストを更新します。
   a. IBM Domino Administrator から「**ファイル**」タブをクリックします。
   b. idipwsync.nsf データベースを選択します。
   c. 右側のパネルから「**データベース**」/「**ACL の管理**」を選択します。
   d. 「**追加**」をクリックし、「**IDIPWSync**」 グループを選択します。
   e. 「**アクセス**」リストから「**編集者**」を選択します。
   f. 「**属性**」の下で以下のオプションを設定します。
      1) 「**文書の削除**」チェック・ボックスを選択します。「**文書の作成**」、「**パブリック文書[読者]**」、および「**パブリック文書[作成者]**」の各チェック・ボックスも選択する必要があります。「**編集者**」アクセスが選択されているときは、この選択が自動的に行われます。
      2) 「**個人エージェントの作成**」、「**個人フォルダ/ビューの作成**」、「**共有フォルダ/ビューの作成**」、「**LotusScript/Java エージェントの作成**」、「**文書を複製またはコピー (Replicate or copy documents)**」の各チェック・ボックスをクリアします。
   g. 「**アクセス制御リスト (Access Control List)**」から「**デフォルト**」を選択します。
   h. 「**アクセス**」に「**アクセスなし**」を設定します。

i. 「**OK**」をクリックします。

注: idipwsync.nsf データベースの ACL が変更されると、その ACL を IBM Domino サーバーから変更できなくなります。セキュリティー上の理由から、最も制限の強い設定を使用します。ACL を変更する必要がある場合は、データベースをローカルで開き、要件に従って ACL を変更する必要があります。

次のタスク

『pwsync_install_r8.nsf データベースの削除』

pwsync_install_r8.nsf データベースの削除

pwsync_install_r8.nsf データベースは、必要なテンプレート・オブジェクトを配布するためにのみ使用されます。 IBM Domino HTTP プラグインをセットアップしたときは、このデータベースは不要になり、IBM Domino サーバーから削除できます。

手順

1. IBM Domino Administrator から「**ファイル**」タブをクリックします。
2. pwsync_install_r8 データベースを右クリックして、「**データベースの削除**」を選択します。
3. 「**OK**」をクリックします。

複数の IBM Domino サーバーを含む Domino ドメインへのデプロイ

複数の IBM Domino サーバーが存在する場合、Password Synchronizer は、Domino ドメイン内の 1 次 IBM Domino Directory Server であるすべての IBM Domino サーバーにインストールされます。

このタスクについて

ディレクトリー・サーバーとしてのみ構成されている IBM Domino サーバーには、Password Synchronizer はインストールされません。

手順

1. Domino ディレクトリーの管理サーバーである 1 次 IBM Domino Directory Server で、Password Synchronizer のフルインストールを実行します。インストールの手順については、46 ページの『単一 IBM Domino サーバーでのデプロイメント』を参照してください。
2. 他のすべての 1 次 IBM Domino Directory Server について、以下のステップを実行します。
   a. Password Synchronizer のインストーラーを実行して、必要なファイルをインストールします。
   b. フルセットアップを実行した最初の 1 次 IBM Domino Directory Server からの強制レプリカ生成を実行します。
      1) IBM Domino Administrator から「**サーバー**」タブをクリックします。
      2) 「**状況**」を選択します。

3) 右側のパネルで、「**サーバー**」 > 「**複製**」を選択します。
4) 「**どのサーバーで複製しますか?**」フィールドに、フルセットアップを実行する最初の 1 次 IBM Domino Directory Server の名前を入力します。
5) 「**複製**」をクリックします。
6) 「**完了**」をクリックします。

c. このステップと以降のセットアップ手順については、46 ページの『単一 IBM Domino サーバーでのデプロイメント』のトピックのセットアップ・ステップを参照してください。

ステップ 1、2、3、および 6 はスキップします。Domino ディレクトリー複製により、フルセットアップを実行する最初の 1 次 IBM Domino Directory Server から設計の更新情報が伝搬されます。

d. ステップ 4 および 7 はスキップします。`IDIPWSyncAdminRequestAgent` は、Domino ディレクトリーの管理サーバー上でのみ起動されます。
e. ステップ 8 を実行します。ただし、秘密鍵の作成ステップはスキップします。最初の 1 次 IBM Domino Directory Server 上で Password Synchronizer をセットアップしたときに作成される秘密鍵を使用します。
f. ステップ 9、10、および 11 を実行します。
g. ステップ 12 はスキップします。
h. ステップ 13 を実行します。ただし、**IDIPWSync** グループの作成ステップはスキップします。
i. ステップ 14 を実行します。

Password Synchronizer の部分的なデプロイメント

管理上のパスワードのリセットのインターセプトおよびユーザー・パスワードの変更のインターセプト (これらは互いに独立しています) という、IBM Domino Password Synchronizer の 2 つの機能をインストールできます。

IBM Domino Password Synchronizer は、以下の両方をインターセプトします。

- 管理者がユーザーの個人文書を編集する際の管理上のパスワードのリセット。
- ユーザーが以下のいずれかの方法を使用してパスワードを変更する際の通常のパスワード変更。
  - `domcfg.nsf` ファイルにある「**パスワード変更**」 Web フォームの使用
  - IBM iNotes の使用

Password Synchronizer の部分的なデプロイメントの場合は、次のようにします。

1. 管理上のパスワードのリセットのみをインターセプトする IBM Domino Password Synchronizer をインストールします。それには、IBM Domino Administrator を使用するか、または Web ブラウザー・インターフェースを使用します。

   管理上のパスワードのリセットのみをインターセプトする Password Synchronizer をインストールするには、ステップ 4 および 7 を除いた 46 ページの『単一 IBM Domino サーバーでのデプロイメント』のステップを実行します。

ステップ 5 では、admin4.ntf ファイルを開いて **IDIPWSyncAdminRequestAgent** エージェントに署名するタスクをスキップします。

ステップ 4 およびステップ 7 では、通常のユーザー・パスワード変更をインターセプトするエージェントをインストールします。

複数の IBM Domino サーバーが存在する Domino ドメインにソリューションをインストールする場合、61 ページの『複数の IBM Domino サーバーを含む Domino ドメインへのデプロイ』の説明に従ってください。 Synchronizer を管理サーバーにインストールする場合は、ステップ 4 および 7 をスキップします。

2. 通常ユーザーのパスワード変更のみをインターセプトする IBM Domino Password Synchronizer をインストールします。それには、domcfg.nsf の「**パスワード変更**」 Web フォームを使用するか、または IBM iNotes を使用します。

   通常ユーザーのパスワード変更のみをインターセプトする Password Synchronizer をインストールするには、46 ページの『単一 IBM Domino サーバーでのデプロイメント』のトピックのステップ 1、2、4、5、7、10、11、および 14 を実行します。ステップ 5 では、pubnames.ntf を開いて **IDIPWSyncClientAgent** エージェントおよび **IDIPWSyncWebAgent** エージェントに署名する部分をスキップします。ステップ 3、6、8、9、12、および 13 はスキップします。これらは管理上のパスワードのリセットのインターセプトにのみ必要だからです。

   複数の IBM Domino サーバーが存在する Domino ドメインにソリューションをインストールするには、前述のインストール・ステップと同じステップを、1 次 IBM Domino Directory Server で実行します。1 次の IBM Domino Directory Server は、Domino ディレクトリーの管理サーバーです。Domino ドメイン内の他の IBM Domino サーバーでのインストールは不要です。

専用のエージェント署名者を使用しないデプロイメント手順

IBM Security Directory Integrator 7.1 よりも前のバージョンでは、署名者アカウントは使用できません。その代わりに、メソッドおよび操作を制限なしで署名または実行 (Sign or run unrestricted methods and operations) 特権を IDIPWSync グループに付与する必要があります。

IBM Security Directory Integrator V 7.1 で必要な特権のスコープを最小化するために、専用の署名者アカウントを割り当てるようにデプロイメント手順が変更されました。専用の署名者は、Password Synchronizer のエージェントに署名できます。 V 7.1 より前のデプロイメント手順では、そのような署名者アカウントはありませんでした。 V 7.1 より前のデプロイメント手順は、引き続きサポートされています。

46 ページの『単一 IBM Domino サーバーでのデプロイメント』のデプロイメント手順を以下のように変更する必要があります。

1. ステップ 5 (エージェントに署名するステップ) はスキップします。
2. ステップ 13 の署名者アカウントを IDIPWSync グループに追加するタスクはスキップします。
3. ステップ 13 の後、以下のステップを実行します。

注: マルチサーバー・トポロジーの場合は、Password Synchronizer をデプロイするすべてのサーバーでこれらのステップを適用してください。

a. IBM Domino Administrator から、「**ファイル**」タブをクリックします。

b. 「**無制限メソッドおよび操作の実行**」フィールドに IDIPWSync グループを追加します。

c. 「**保存して閉じる**」をクリックします。

Password Synchronizer の使用法

IBM Domino HTTP Password Synchronizer は、names.nsf データベースおよび admin4.nsf データベースを変更して、パスワードの取得とパスワード変更管理要求を管理します。

IBM Domino HTTP Password Synchronizer は、names.nsf データベースを変更し、カスタム Java エージェントとカスタム・コードを特定のフックに追加します。

フック内のコードは、個人文書が names.nsf に保存されるときに IBM Domino によって実行されます。このコードは、ハッシュされる前の HTTP パスワードを取得し、その値を、カスタム Java コードを使用して Password Synchronizer プロキシー・プロセスに送信します。

IBM Domino HTTP Password Synchronizer は、カスタム Java エージェントを追加して admin4.nsf データベースを変更します。このエージェントは、文書が管理要求データベース admin4.nsf 内で作成または変更された後でトリガーされるようにスケジュールされたエージェントとして構成されています。このエージェントは、admin4.nsf データベース内で文書が作成または変更された直後ではなく、IBM Domino の Agent Manager プロセスの決定に応じて、5 分から 30 分の間隔の後にトリガーされます。エージェントは、トリガーされると、正常に処理された Domino ディレクトリーでの HTTP パスワードの変更管理要求を検索します。エージェントは、新規のパスワードをその要求から取得し、パスワード・データを Password Synchronizer プロキシー・プロセスに送信します。

プロキシー・プロセスはパスワード・ストア・コンポーネントを開始し、そのパスワード・データを暗号化して保管して、IBM Security Directory Integrator がそれを取得できるようにします。

パスワード変更のメカニズム

IBM Domino HTTP Password Synchronizer を使用する場合、次の方法で、以下のパスワード変更メカニズムのみがインターセプトされます。

- IBM Domino Administrator からの個人文書の編集
- Web ブラウザーを介した個人文書の編集
- domcfg.nsf の「パスワード変更」Web フォームの使用
- IBM iNotes の使用

注: 他のインターフェースを通して行われたパスワード変更はどれもインターセプトされません。例えば、Password Synchronization が有効になっている場合に、

LDAP または IBM iNotes を通してパスワードが変更されると、IBM Domino HTTP Password Synchronizer はトリガーされません。また、パスワード変更の同期も行われません。

パスワード転送の保護

セキュア通信を確立するには、パスワード変更用の Web ベース・メカニズムに対して SSL を有効にします。ブラウザーを通して個人文書を編集するには、「パスワード変更」Web フォームまたは IBM iNotes を使用します。

IBM Domino Administrator クライアントを通して個人文書を編集する場合、通信は、IBM Domino においてポート暗号化を有効化することによって保護されます。

IBM Domino のポート暗号化を構成する方法の詳細は、46 ページの『単一 IBM Domino サーバーでのデプロイメント』を参照してください。

ソリューション・ワークフロー

LDAP や JMS などのパスワード・ストアをインスタンス化するようにプロキシー・プロセスを構成する必要があります。これは、ユーザーが IBM Domino サーバーを始動すると開始します。プロキシー・プロセスは、TCP/IP 接続を受け入れ、ユーザー ID とパスワード・データを受信し、データの保管のためにパスワード・ストアを開始します。

IBM Domino Administrator からの個人文書の変更

個人文書には、names.nsf データベース内のカスタム・コードが入っています。個人文書を保存すると、そのコードが IBM Domino Administrator クライアントで実行されます。

HTTP パスワードを変更した場合、以下の一連のアクションが実行されます。

1. ハッシュされる前のパスワードが取得されます。
2. 新規文書が作成され、パスワードがその文書に保管されます。文書は、サーバー上のデータベースに保存されます。
3. エージェントがサーバー上で開始され、新規に作成された文書の ID を渡します。エージェントは、パスワード・データを文書から読み取って、削除します。次に、エージェントはその文書をプロキシー・プロセスに送信します。それから、データはプロキシー・プロセスからパスワード・ストアに送信されます。
4. パスワード・ストアは、正常に保管されなかったパスワードを戻します。パスワードが戻された場合、HTTP パスワード・フィールドの変更も含め、個人文書に加えたすべての変更はリジェクトされます。

IBM Domino Web ブラウザー・インターフェースを使用した個人文書の変更

個人文書には、names.nsf データベース内のカスタム・コードが入っています。個人文書を保存すると、そのコードが IBM Domino サーバーで実行されます。

HTTP パスワードを変更した場合、以下の一連のアクションが実行されます。

1. 個人文書の保存を要求したときに、HTTP パスワード値が変更されると、カスタムの Lotus の式コードによってプレーン・テキストのパスワードがインターセプトされます。そのパスワードは次に、文書内のカスタムの隠しフィールドに保管されます。
2. Lotus の式コードが、文書の保存の直前にエージェントを開始します。
3. エージェントは、隠しフィールドからパスワード値を読み取ります。そして、このフィールドの値を削除し、パスワードをプロキシー・プロセスに送信します。次に、そこから、そのパスワードがパスワード・ストアに送信されます。
4. パスワード・ストアは、正常に保管されなかったパスワードを戻します。パスワードが戻された場合、HTTP パスワード・フィールドの変更も含め、個人文書に加えたすべての変更はリジェクトされます。

注: このシナリオでは、Web フォームの送信時に、ブラウザーから IBM Domino Web サーバーにプレーン・テキストのパスワード値が送信されます。伝送中のパスワードの保護のため、IBM Domino Web サーバーでは SSL が使用可能になっており、ユーザーはブラウザーの HTTPS プロトコルを使用します。

「パスワード変更」Web フォームまたは IBM iNotes を使用するパスワード変更

「パスワード変更」Web フォームまたは IBM iNotes を使用して HTTP パスワードを変更すると、IBM Domino ディレクトリーでの HTTP パスワードの変更管理要求が admin4.nsf データベースにポストされます。管理プロセスはこの要求を処理し、ユーザーの個人文書内のパスワードを変更します。

Password Synchronizer は、カスタム Java エージェントを admin4.nsf データベースに追加します。管理要求文書または管理要求資料への応答が admin4.nsf データベースに追加された後、エージェント・マネージャーによって Java エージェントの開始がスケジュールされます。 Java エージェントは即時開始されるのではなく、エージェント・マネージャーによって選択された構成可能な間隔の後です。通常、その間隔は、文書がポストされてから 5 分から 30 分です。エージェントを実行すると、以下のアクションが行われます。

- すべての管理要求の処理の取得。以下のものがあります。
  - タイプがDomino ディレクトリーでの HTTP パスワードの変更のもの。
  - IBM Domino 管理プロセスによって正常に処理されたもの。パスワードが IBM Domino によって変更されたことを示す応答文書が添付されています。

    パスワード変更要求が未処理の場合や、処理が正常に完了しなかった場合、パスワード変更を適用できません。そのため、Password Synchronizer はそれについての報告を行いません。
  - エージェントの前回の実行時に、エージェントによって正常に処理されたもの。
- パスワード変更の管理要求が正常に処理されるごとにユーザー ID と新規パスワードが取得され、プロキシー・プロセスに送信されます。次に、プロキシー・プロセスはデータをパスワード・ストアに送信します。

  パスワード・ストアが正常に保管されているパスワードを戻した場合、処理済みのマークが管理要求に付けられます。エージェントを次回実行したときに、その

要求がエージェントによって再度処理されることはありません。パスワードが正常に保管されていない場合、処理済みのマークはその文書に付きません。そのため、エージェントは次回の実行時に再度それを処理します。

注: このシナリオでは、Web フォームの送信時に、ブラウザーから IBM Domino Web サーバーにプレーン・テキストのパスワード値が送信されます。送信中のパスワードの保護のため、IBM Domino Web サーバーでは SSL が使用可能になっており、ユーザーはブラウザーの HTTPS プロトコルを使用します。

バージョン 7.1.1 からバージョン 7.2 へのマイグレーション

マイグレーションを行う前に、IBM Domino HTTP Password Synchronizer と IBM Domino サーバーの構成設定を変更する必要があります。

このタスクについて

IBM Security Directory Integrator バージョン 7.1.1 が「メソッドおよび操作を制限なしで署名または実行 (Sign or run unrestricted methods and operations)」特権を備えた専用の署名者と共に構成されている場合は、以下のステップをスキップできます。バージョン 7.2 より前のデプロイメント手順については、 63 ページの『専用のエージェント署名者を使用しないデプロイメント手順』を参照してください。

IBM Security Directory Integrator バージョン 7.2 の場合、Password Synchronizer エージェントは、「メソッドおよび操作を制限なしで署名または実行 (Sign or run unrestricted methods and operations)」特権を備えた専用の署名者によって署名されます。この特権は、IDIPWSync グループがなくても持つことができます。

手順

1. Password Synchronizer のエージェントに署名します。 46 ページの『単一 IBM Domino サーバーでのデプロイメント』トピックのステップ 5 を参照してください。
2. names.nsf と admin4.nsf の設計を更新します。 46 ページの『単一 IBM Domino サーバーでのデプロイメント』トピックのステップ 6 およびステップ 7 を参照してください。
3. エージェントの署名者を IDIPWSync グループに追加します。 46 ページの『単一 IBM Domino サーバーでのデプロイメント』トピックのステップ 13 を参照してください。
4. 「メソッドおよび操作を制限なしで署名または実行 (sign or run unrestricted methods and operations)」特権を IDIPWSync グループから削除します。
   a. IBM Domino Administrator で、「**設定**」タブをクリックします。
   b. 「**サーバー**」 > 「**すべてのサーバー文書**」 を選択します。
   c. サーバーの資料を選択します。 IBM Domino サーバーが複数存在する場合は、それぞれのサーバーに対してすべてのステップを実行する必要があります。
   d. 「**サーバーの編集 (Edit Server)**」 をクリックします。
   e. 「**セキュリティー**」タブをクリックします。

f. 「**Programmability の制限 (Programmability Restrictions)**」セクションで、「**メソッドおよび操作を制限なしで署名または実行 (Sign or run unrestricted methods and operations)**」フィールドから `IDIPWSync` グループを削除します。

g. 「**保存して閉じる**」をクリックします。

第 8 章 UNIX および Linux 用 Password Synchronizer

UNIX および Linux 用の Password Synchronizer は、UNIX および PAM 対応のアプリケーションをベースとするツールで発生したパスワード変更イベントをインターセプトします。

概説

UNIX システム上の PAM (Pluggable Authentication Module) アーキテクチャーは、ユーザー認証に基づくカスタマイズ動作を使用可能にするための拡張可能な設計を備えています。 PAM Password Synchronizer プラグインは、UNIX PAM アーキテクチャーを使用して、パスワード変更通知を IBM Security Directory Integrator プラグインのパスワード・ストアに伝搬できるようにします。

PAM Password Synchronizer プラグインの主な目的は、**passwd** コマンドなどの、UNIX および PAM 対応のアプリケーションをベースとするツールで発生したパスワード変更イベントをインターセプトすることにあります。

サポートされるプラットフォーム

PAM 用 Password Synchronizer が使用可能なプラットフォームは次のとおりです。

- Solaris 10 SPARC (32 ビットおよび 64 ビット)
- Solaris 11 SPARC (32 ビットおよび 64 ビット)
- AIX 6.1 (PPC-64)
- AIX 7.1 (PPC-64)
- RHEL ES/AS 5.0 (x86/x86 - 64)
- RHEL ES/AS 6.0 (x86/x86 – 64)
- SLES 10 (x86/x86 - 64)
- SLES 11 (x86/x86 - 64)
- RedFlag Data Center 5.0 SP1/Asianix 2.0 SP1

注:

1. 64 ビットの x86 Linux では、**prelink** ユーティリティーが **cron** ユーティリティーによって初めて実行される前にプラグインをインストールしようとすると、バンドルされている JRE で問題が発生します。プラグインのインストールに失敗すると、JVM が見つからないというメッセージが表示されます。 `/etc/cron.daily/prelink` スクリプトを実行してこの問題を解決し、プラグインのインストールを開始できるようにします。
2. RHEL 5.0 では、SELinux はデフォルトで有効になっています。 SELinux は、悪意のある攻撃からホストをセキュアに保ちます。ただし、デフォルト設定では、一部のプラグイン・ライブラリーのロードができません。この問題を修正するには、次のコマンドを実行します。

   ```
   find TDI_install_dir/jvm/jre/bin TDI_install_dir/pwd_plugins/PAM -name
   '*.so' -exec chcon -t textrel_shlib_t {} ¥;
   ```

デプロイメントおよび構成

PAM Password Synchronizer を構成するには、TDI_install_dir/pwd_plugins/pam/pwsync.props にあるテンプレート構成ファイルを使用します。

Password Synchronizer をインストールするには、IBM Security Directory Integrator インストーラー・ウィザードを使用します。インストールが完了したら、以下のセクションの指示に従って、PAM Password Synchronizer に必要なデプロイメント・ステップを実行します。

PAM 内の UNIX および Linux プラグインに対する Password Synchronizer の登録

プラグインを登録するには、PAM 構成ファイルを編集します。以下の表は、各種プラットフォーム上の PAM 構成ファイルが配置されている標準的な場所を示しています。個々の PAM 構成により、PAM パスワード・モジュール構成は別々のファイルになります。これらのファイルが存在しない場合、または追加された Password Synchronization モジュールが始動していない場合は、システム管理者に問い合わせてください。

注: UNIX 上の古いバージョンの PAM では、/etc/pam.conf 構成ファイルが使用されています。このファイルは、現在は使用すべきではありません。現在、PAM を利用するモジュールのすべての PAM 構成ファイルは、/etc/pam.d に配置されています。パスワード変更モジュールの PAM 構成ファイルは、このディレクトリーに保管する必要があります。

外部システム構成の基本コンポーネントは PAM 構成ファイルです。プラグインの目的は、パスワード・イベントをインターセプトすることです。そのため、以下の表に示す登録行を PAM 構成ファイルに追加します。 PAM モジュールが他の PAM モジュールと共にスタックされている場合は、セキュリティー・モジュールがスタックの最後のモジュールになります。これにより、PAM がセキュリティー・モジュールを呼び出す前に、前の required モジュールが成功状況を確実に戻すようになります。

オペレーティング・システム	PAM 構成ファイル	PAM プラグイン登録行
AIX 6.1 以降	/etc/pam.conf	passwd パスワードは必須です。 *TDI_Plugin_Root*/pwd_plugins/pam/libpamtivoli.so use_first_pass *TDI_Plugin_Root*/pwd_plugins/pam/pwsync.props
Solaris 10	/etc/pam.conf または /etc/pam.d/system-auth	その他のパスワードは必須です。 *TDI_Plugin_Root*/pwd_plugins/pam/libpamtivoli.so use_first_pass *TDI_Plugin_Root*/pwd_plugins/pam/pwsync.props

オペレーティング・システム	PAM 構成ファイル	PAM プラグイン登録行
Linux	/etc/pam.confor /etc/pam.d/system-auth (RHEL 5) /etc/pam.conf または /etc/pam.d/password (SLES 9) /etc/pam.conf または /etc/pam.d/common-password (SLES 10)	パスワードは必須です。*TDI_Plugin_Root*/pwd_plugins/pam/libpamtivoli.so use_first_pass *TDI_Plugin_Root*/pwd_plugins/pam/pwsync.props

注: システムが 64 ビットであり、PAM を利用するアプリケーション (passwd など) も 64 ビットの場合は、libpamtivoli の代わりに libpamtivoli_64 を使用します。

注: 上記の表では、system-auth は、/etc/pam.d ディレクトリーの PAM 構成ファイルとして示されています。 /etc/pam.d/passwd ファイルは、パスワード設定とパスワード変更を行うメインの構成ファイルです。ほとんどのオペレーティング・システムの場合、標準の PAM インストール済み環境では、/etc/pam.d/system-auth ファイルを使用するように /etc/pam.d/passwd ファイルがセットアップされます。このセットアップでは、パスワード設定とパスワード変更を行う実際の PAM モジュールが定義されます。 RHEL 4 の場合、/etc/pam.d/passwd ファイルの委任を以下の例のようにすることができます。

```
password required pam_stack.so service=system-auth
```

PAM /etc/pam.d/passwd 構成ファイルが system-auth に委任される場合は、構成項目を /etc/pam.d/system-auth ファイルに追加する必要があります。

セキュリティー・モジュールをスタックの最後に配置する場合の例外を以下に示します。

- セキュリティー・モジュールの上にモジュールがあり、sufficient としてマークされている場合、モジュールを required に変更する必要があります。この変更により、セキュリティー・モジュールが確実に呼び出されるようになります。例えば、RHEL 4 Linux の場合、標準インストールでは、pam_unix モジュールが sufficient としてマークされています。 pam_unix モジュールの結果が成功の場合、先行のパスワード・モジュールは始動されません。セキュリティー・モジュールが確実に呼び出されるようにするには、pam_unix を required に変更し、スタック内でそのモジュールをセキュリティー・モジュールの前に配置する必要があります。
- エラー処理専用モジュール (pam_deny など) がある場合、それらのモジュールは、セキュリティー・モジュールの後に配置する必要があります。また、セキュリティー・モジュールは sufficient としてマークする必要があります。

PAM プラグ可能アーキテクチャーでは、モジュールをスタックすることができます。複数の PAM Password Synchronizer を同じシステムにインストールできるカス

タム・ソリューションを作成することが可能です。各 PAM プラグインでは、別個の Java プロキシー・プロセスが必要です。それぞれの Java プロキシーが別々のポートを listen する必要があります。異なる pwsync.props 構成ファイルを使用してください。これらのファイルは、別のフォルダーに配置する必要があります。これは、そのフォルダーで認証が実行されるためです。

PAM Password Synchronizer の構成

PAM プラグインのテンプレート構成ファイルは、*TDI_install_dir*/pwd_plugins/pam/pwsync.props にインストールされています。 PAM プラグインが初期化されるとき、構成ファイルは、プラグインの登録行の最後のパラメーターとして設定されます。構成ファイルのいくつかのパラメーターは、プラグインと Java プロキシーで共有されます。プラグインは、 13 ページの『第 3 章 パスワード同期プラグインの共通の構成およびユーティリティー』トピックで説明されているいくつかのプロパティーを認識します。

syncBase プロパティーと **logFile** プロパティーは、プラグインには無関係であるため、無視されます。 syncBase プロパティーを無視するのは、PAM が到達ユーザーに対して、DN と同様の命名を常に実行できないためです。 **logFile** プロパティーを無視するのは、PAM プラグインがネイティブ UNIX syslog デーモンを使用してログを記録するためです。

syncClass パラメーターに適切なクラス名を設定して、希望するパスワード・ストアを選択します。

第 9 章 LDAP パスワード・ストア

LDAP パスワード・ストアは、インターセプトされたユーザー・パスワードを LDAP ディレクトリー・サーバーに保管します。

サポートされるディレクトリー

LDAP パスワード・ストアは、以下のディレクトリーで使用できます。

- IBM Security Directory Server
- Microsoft Active Directory
- Sun Directory Server

LDAP パスワード・ストアのインストール

IBM Security Directory Integrator LDAP パスワード・ストアは、インターセプトされたユーザー・パスワードを LDAP ディレクトリー・サーバー (リポジトリーまたはデータ・ソース) に保管するために必要な機能を備えています。

LDAP パスワード・ストア・コンポーネントを作成すると、各種の製品またはプラットフォームのパスワード変更をインターセプトする IBM Security Directory Integrator プラグインを多数サポートできます。

ユーザーからのパスワード変更要求をインターセプトするために、以下の Password Synchronizer が提供されています。

Windows 用の IBM Security Directory Integrator Password Synchronizer
Windows のログイン・パスワードの変更をインターセプトします。

Windows、UNIX、および Linux 用の IBM Security Directory Server Password Synchronizer
IBM Security Directory Server のパスワード変更をインターセプトします。

Windows、UNIX、および Linux 用の Sun Directory Server Password Synchronizer
Sun Directory Server のパスワードの変更をインターセプトします。

Windows、UNIX、および Linux 用の IBM Domino Password Synchronizer
IBM Notes ユーザーの HTTP パスワードの変更をインターセプトします。

UNIX および Linux 用の IBM Security Directory Integrator Password Synchronizer
UNIX ユーザーと Linux ユーザーのパスワード変更をインターセプトします。

変更を別の LDAP サーバーに安全に伝搬するために、すべてのプラグインは、LDAP パスワード・ストアの機能を使用します。LDAP サーバーの場合、パスワード変更は、IBM Security Directory Integrator AssemblyLine によって操作されます。

LDAP パスワード・ストアを構成するには、以下のことが可能なプロパティー・ファイルを使用します。

- SSL 接続用の鍵ストア・ファイル、証明書、および資格情報の指定。
- パスワード・データの非対称暗号化。

プロパティー・ファイルは、トレース・ログの制御や、取り込んだパスワードを保管する属性の限定された制御にも対応しています。

前提条件

- LDAP パスワード・ストアでは、JRE 1.5 以上が必要です。IBM Security Directory Integrator には Java 7.0.4 JRE がバンドルされています。
- IBM Security Directory Integrator の製品インストーラーを使用して、パスワード同期プラグインをインストールします。

LDAP サーバーのセットアップ

IBM Security Directory Server を使用してサンプル環境をセットアップできます。セットアップするには、ユーザー ID とパスワードを持つオブジェクト・クラスが置かれているかまたは作成されたコンテナーを特定します。

手順

1. 接尾部を定義します。
   a. 「**スタート**」 > 「**プログラム**」 > 「**IBM Security Directory Server *x.x***」 > 「**ディレクトリーの構成 (Directory Configuration)**」を選択します。
   b. 左側のペインから「**サフィックス管理**」を選択します。
   c. 「**サフィックス DN**」フィールドに、パスワード情報の格納先に使う接尾部を追加します。例えば、`o=ibm,c=us` などです。
   d. 「**追加**」をクリックします。 新規の接尾部が、「**現在のサフィックス DN**」リストに表示されます。
   e. 「**OK**」をクリックします。
   f. 「**ディレクトリーの構成 (Directory Configuration)**」ツールを閉じます。
2. 接尾部データを追加します。
   a. IBM Security Directory Server を再始動します。
   b. 「IBM Security Directory Server Web 管理ツール」から、「**ディレクトリー管理**」 > 「**項目の管理**」を選択します。
   c. 「**追加**」をクリックします。
   d. 構造オブジェクト・クラスのリストから「**組織**」を選択します。
   e. 「**次へ**」をクリックします。
   f. 「補助オブジェクト・クラスの選択」ウィンドウで、「**次へ**」をクリックします。
   g. 「属性の入力」ウィンドウの「**親 DN**」フィールドの値をクリアします。
   h. 「**相対 DN**」フィールドに接尾部名を指定します。例えば、`o=ibm,c=us` などです。
   i. 「**o**」フィールドに組織名を入力します (前の例では **ibm**)。
   j. 「**完了**」をクリックします。
3. ドメイン・オブジェクトを追加します。

a. 「IBM Security Directory Server Web 管理ツール」から、**「ディレクトリー管理」 > 「項目の管理」**を選択します。
b. 前のステップで事前に作成した接尾部 **o=ibm, c=us** を選択します。
c. **「追加」**をクリックします。
d. **構造オブジェクト・クラス**のリストから**ドメイン**を選択します。
e. **「次へ」**をクリックします。
f. 「補助オブジェクト・クラスの選択」ウィンドウで、**「次へ」** をクリックします。
g. **「相対 DN」**フィールドにドメイン名を入力します。例えば、**dc=mydomain** などです。
h. **「dc」**フィールドにドメイン名を入力します (前の例では **mydomain**)。
i. **「完了」**をクリックします。

注: 入力したドメインおよび接尾部は、他の情報とともに `pwsync.props` ファイルにも組み入れる必要があります。構成について詳しくは、76 ページの『LDAP パスワード・ストアの構成』を参照してください。

4. `ibm-diPerson` オブジェクトを定義します。IBM Security Directory Server クライアントを持つシステムで、以下のコマンドを 1 行で *install_directory* から実行します。

```
ldapmodify -c -h LDAP Hostname -D admin DN -w admin PW  -f
TDI_install_dir/pwd_plugins/etc/ibm-diPerson_oc.ldif
```

注: 次のメッセージが表示される場合があります。

- `属性タイプ '1.3.18.0.2.4.155'は既に存在します。追加操作は失敗しました。(Attribute type '1.3.18.0.2.4.155' already exists, add operation failed.)`
- `属性タイプ '0.9.2342.19200300.100.1.1'は既に存在します。追加操作は失敗しました。(Attribute type '0.9.2342.19200300.100.1.1' already exists, add operation failed.)`

これらのメッセージは無視して構いません。これらのメッセージは、`secretKey` 属性および `uid` 属性が既にスキーマ内に定義されていることを示しています。

zLDAP のスキーマの変更

必要な LDIF ファイルを容易にロードできるように z/OS® 上の LDAP サーバーを構成するときは、Technical Database Management (TDBM) サーバーを使用する必要があります。

このタスクについて

注: IBM Security Directory Integrator バージョン 7.2 以降では z/OS オペレーティング・システムはサポートされません。

注: セットアップ手順については、IBM z/OS オンライン製品ライブラリーの「*z/OS Integrated Security Services LDAP サーバー 管理および使用ガイド*」を参照してください。

手順

1. 接尾部の定義では、新しい LDAP 構成ジョブとサーバー JCL ジョブを生成する必要があります。これらのジョブは、LDAP 管理者とシステム・プログラマーが生成を担当します。
2. 接尾部データを追加する必要がない間は、基本スキーマを定義済みの接尾部に追加する必要はありません。 /usr/lpp/ldap/etc ディレクトリーにある 2 つの基本スキーマ LDIF ファイル、schema.IBM.ldif および schema.user.ldif は、ステップ 1 での接尾部を使用してカスタマイズした後、ロードする必要があります。
3. 必要な場合は、ドメインを定義する LDIF ファイルを作成してロードすることにより、ドメインを定義できます。
4. ibm-diPerson_z.ldif ファイルは、LDAP サーバーにロードする前に、ステップ 1 で作成した接尾部が含まれるようにカスタマイズする必要があります。このプロセスでは、接尾部を DN の末尾に追加する必要があります。例えば、接尾部が o=ibm,c=us の場合は、DN の行を dn:cn=schema から dn:cn=schema,o=ibm,c=us に変更します。

Sun Directory Server および Active Directory のスキーマ変更

LDAP パスワード・ストアをインストールする前に、Sun Directory Server と Active Directory のスキーマを、必要な構成を使用して変更する必要があります。

手順

1. Sun Directory Server の LDAP スキーマを変更します。次のコマンドを 1 行に指定して実行します。

   ```
   ldapmodify -c -h LDAP Hostname -D admin DN -w admin PW-f
   TDI_install_dir/pwd_plugins/etc/ibm-diPersonForSunDS.ldif
   ```

2. Active Directory の LDAP スキーマを変更します。
   a. 次の Windows レジストリー・キーを編集して、Active Directory のスキーマを変更できるようにします。

      ```
      HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services¥NTDS¥Parameters
      ```

      Schema Update Allowed という名前の REG_DWORD 値を追加します。値は 1 または 0 よりも大きい任意の値にします。
   b. 次のコマンドを実行して LDAP スキーマを更新します。

      ```
      ldifde -i -f TDI_install_dir/pwd_plugins/etc/ibm-diPersonSchemaForAD.ldif
      ```

   c. Microsoft 管理コンソールを開きます。
   d. 変更されたパスワードを保管する新しい組織単位を作成します。
   e. ldifde.exe、csvde.exe、または dsquery.exe のいずれかのツールを使用して、組織単位の識別名を取得します。この名前は、pwsync.props ファイルで LDAP パスワード・ストアの接尾部を構成するときに使用されます。

LDAP パスワード・ストアの構成

LDAP パスワード・ストアのプロパティーを pwsync.props 構成ファイルに設定する必要があります。

デフォルトでは、プラグインごとに 1 つの構成ファイルが存在します。例えば、IBM Security Directory Server パスワード・プラグインには、*TDI_install_dir*/pwd_plugins/tds/pwsync.props があります。したがって、LDAP パスワード・ストアは、プラグインの pwsync.props ファイルで構成されます。

注: 構成ファイルでは、各パスワード・プロパティーを手動で暗号化する必要があります。暗号化を行うには、encryptPasswd ユーティリティーを使用します。このユーティリティーは、対称アルゴリズムを使用してパスワードを暗号化します。信頼できるシステム・ユーザーのみが pwsync.props ファイルを読み取れるようにしてください。

encryptPasswd ユーティリティーでは、パスワードがパラメーターとして渡される必要があります。暗号化されたパスワードは、標準出力に出力されます。
構成パラメーターとその説明の詳細なリストについては、 13 ページの『第 3 章 パスワード同期プラグインの共通の構成およびユーティリティー』を参照してください。

LDAP パスワード・ストアのクラスは、
com.ibm.di.plugin.pwstore.ldap.LDAPPasswordStore です。

以下の例は、SSL 接続およびパスワード暗号化を行うための完全なプロパティー・ファイルを示しています。

```
#IBM Directory Integrator LDAP Password Store Settings with Encoded Passwords
#Tue Jul 30 08:21:20 EDT 2002
ldap.hostname=gbdthst1
ldap.port=636
ldap.waitForStore=true
ldap.admindn=cn=root
ldap.password=0c0bf0e3146b
ldap.ssl=true
ldap.suffix=dc=carnd11,o=ibm,c=us
encrypt=true
encryptKeyStoreFilePath=c:¥sync¥cryptokeys.jks
encryptKeyStoreFilePassword=0c0bf0e3146b
encryptKeyStoreCertificate=cryptoCertName
encryptKeyPassword=0c0bf0e3146b
```

注:

1. SSL を無効にする場合は、非 SSL ポート (例えば 389) を選択して ssl=false を設定します。
2. 非対称パスワード暗号化を無効にするには、encrypt=false を設定します。encrypt=false が設定されている場合は、encryptKeyStoreFilePath、encryptKeyStoreFilePassword、encryptKeyStoreCertificate、および encryptKeyPassword の値がすべて無視されます。
3. 接尾部キーワードは、ユーザー ID および新規パスワード値を格納したオブジェクトが検出されるコンテナーを識別するために使用されます。
4. デフォルトのオブジェクト・クラスおよび属性定義をオーバーライドするために使用する追加のオプションのキーワードがいくつかあります。 pwsync.props ファイルには、以下のプロパティー名とそれに関連付けられたデフォルト値を追加できます。

   ldap.schemaPersonObjectName
   ibm-diPerson

ldap.schemaUseridAttributeName
ibm-diUserId

ldap.schemaPasswordAttributeName
ibm-diPassword

5. **ldap.waitForStore** プロパティーに false を設定すると、もう 1 つのオプション属性である **ldap.delayMillis** が使用されます。 **ldap.waitForStore=false** を設定したときは、保管する前の遅延時間 (ミリ秒単位) を **ldap.delayMillis** で指定します。以下の場合は、デッドロックが発生することがあります。
   - LDAP パスワード・ストアを使用するように Windows システム用の IBM Security Directory Integrator Password Synchronizer が構成されている場合。
   - Password Synchronizer がインストールされているのと同じシステム上の Active Directory に保管するように LDAP パスワード・ストアが構成されている場合。

   デッドロックを回避するために、この非同期モードの操作を使用します。非同期モード (**ldap.waitForStore=false**) の場合、Windows システムと通信するパスワード取得コードは Windows に制御を戻します。短い遅延時間の後、別のスレッドを実行しているパスワード・ストア・コードは、パスワード更新を Active Directory に保管することを試みます。**ldap.waitForStore=false** の場合に、**ldap.delayMillis** の値が指定されていない場合は、デフォルトの **ldap.delayMillis=2000** が使用されます。この構成では、**logFilePath** プロパティーに指定されたログ・ファイルを使用して、パスワード・ストアの障害がすべて報告されます。

パスワード暗号化

パスワード値の暗号化は、LDAP パスワード・ストアと JMS パスワード・ストアの両方でサポートされます。

デフォルトでは、暗号化は使用不可です。これをオンにするには、**encrypt** プロパティーに true を設定します。

暗号化を使用するときは、**encryptKeyStoreFilePath** プロパティー、**encryptKeyStoreFilePassword** プロパティー、および **encryptKeyStoreCertifcate** プロパティーの値も設定する必要があります。 LDAP パスワード・ストアを使用している場合は、**encryptKeyPassword** プロパティーを設定する必要があります。残りのパスワード・ストアについては、**encryptKeyPassword** プロパティーは無関係です。パスワードの暗号化および暗号化解除の機能では、RSA アルゴリズムが使用されます。以下の例は、暗号化機能の構成プロパティーを示しています。

```
encryptKeyStoreFilePath=path to the key store file
encryptKeyStoreFilePassword=password of the key store file; encoded with
the "encryptPasswd" tool
encryptKeyStoreCertifcate=the alias of the public key certificate in
the key store
encryptKeyPassword=password of the private key; encoded with
the "encryptPasswd" tool
```

鍵ストア・ファイルと公開鍵または秘密鍵は、keytool および iKeyman JRE ユーティリティーを使用して作成および管理できます。

鍵ストアおよび keytool について詳しくは、以下を参照してください。

- 「*インストールと管理*」の『鍵ストアおよびトラストストアの管理 (Keystore and truststore management)』セクション。
- http://www-128.ibm.com/developerworks/websphere/techjournal/0502_benantar/0502_benantar.html#sec2
- http://docs.oracle.com/javase/1.6.0/docs/tooldocs/windows/keytool.html

install_directory/jvm/jre/lib/security ディレクトリーにある java.security ファイルは、セキュリティー・プロバイダー com.ibm.crypto.provider.IBMJCE への参照を含むようにセットアップされています。以下の例は、ファイルの関連する部分を示しています。

```
:
:
:

# List of providers and their preference orders :
#
security.provider.1=sun.security.provider.Sun
security.provider.2=com.ibm.crypto.provider.IBMJCE

:
:
:
```

IBM Security Directory Integrator のインストール済み環境には、取得したパスワードの暗号化解除を説明する AssemblyLine の例が含まれています。 AssemblyLine と Readme ファイルは、*TDI_install_dir*/examples/pwsync_decryption/ ディレクトリーに保管されています。ここで *TDI_install_dir* は、IBM Security Directory Integrator のインストール・ディレクトリーです。

注:

1. RSA は、非対称の暗号化アルゴリズムであり、公開鍵を使用して暗号化を行い、公開鍵に関連付けられた秘密鍵を使用して暗号化解除を行います。暗号化には公開鍵が必要であるため、パスワード・ストアの鍵ストア・ファイルでは公開鍵のみを配布してください。この情報は、LDAP パスワード・ストアには関係ありません。LDAP パスワード・ストアは、既に保管されているパスワード値を暗号化解除して、削除するパスワードを決定するからです。したがって、秘密鍵も必要となります。
2. 鍵ストア・ファイルは、機密データを保持しているため、ファイル・システム許可を使用して適切に保護する必要があります。

パスワード・ストアの使用法

パスワードをインターセプトされる各ユーザーごとに、LDAP パスワード・ストアは、ストレージ LDAP ディレクトリー内の LDAP 項目を保守します。このディレクトリーは、ストレージ項目が追加および変更される場所であるコンテナーであり、LDAP パスワード・ストアの接尾部プロパティーによって指定されます。

ストレージ・ディレクトリー内の項目には常に、ターゲット・システム上の元のユーザーによって現在使用されているパスワードが入っています。 LDAP パスワード・ストアは、パスワードの更新の通知を Password Synchronizer から受信するたびに、ディレクトリー内の項目の状態を更新します。

LDAP パスワード・ストアは、以下のデータを Password Synchronizer から受信します。

- ユーザー ID (ストリング)
- パスワード変更のタイプ
- パスワードの値のリスト

ユーザー ID

ユーザー ID は、LDAP ディレクトリーに保管される項目の相対識別名に使用されます。例えば、ユーザー ID が `john` であって、接尾部プロパティー値が `dc=somedc, o=ibm, c=us` である場合、保管されるその項目の識別名は `ibm-diUserId=john, dc=somedc, o=ibm, c=us` となります。

Password Synchronizer は、パスワードを変更されたユーザーの LDAP 識別名を報告します。例えば、`cn=john, o=somecompany, c=us` となります。 LDAP パスワード・ストアは識別名の最初の要素 `john` を取得して、ストレージ LDAP ディレクトリー上の項目の識別名を作成します。例えば、`ibm-diUserId=john, dc=somedc, o=ibm, c=us` となります。したがって、部門、会社名、および国名などのコンテキスト情報は失われます。同一名であるけれども別々の部門に属する 2 人の人物がターゲット・システム上に存在する場合、パスワード・ストアはそれぞれの名前を区別できません。ただし、パスワード・ストアは、その名前が同一人物を表すものとして機能します。例えば、`cn=Kyle Nguyen, ou=dept_1, o=ibm, c=us` と `cn=Kyle Nguyen, ou=dept_2, o=ibm, c=us` などです。

パスワード変更のタイプおよびパスワード値のリスト

パスワード変更のタイプは、パスワード値の置換、新規の値の追加、または特定の値の削除のどれが行われたかを示します。パスワード・ストアは、この情報と変更内容を表すパスワードのリストを使用して、変更内容をストレージ・ディレクトリー内の項目に複写します。

パスワード変更のタイプが有効であるのは、例えば IBM Security Directory Server または Sun Directory Server などの複数の値をパスワードが持つ場合のみです。ターゲット・システムにおけるパスワードが、例えば Windows のように単一値であれば、パスワード変更のタイプは常に**置換**になります。

パスワードとそのすべての値がターゲット・システムから削除された場合、ストレージ・ディレクトリー内の項目は変更されます。パスワードは、パスワードの保管に使用される LDAP 属性の値を持つことはできません。

IBM Security Directory Integrator から実行できるパスワードの取得

LDAP パスワード・ストアにより LDAP サーバーに保管されたパスワードを取得することができます。 **変更ログ・コネクター**は、ストレージに使用される LDAP ディレクトリーにおける変更を listen するように構成されています。コネクターは、パスワード・ストア・コンテナー内で項目の追加または変更が行われたことを検出するたびに、AssemblyLine を開始します。変更済み項目の ID を渡すことで、AssemblyLine を開始できます。 AssemblyLine は LDAP コネクターを使用して、変

更済み項目の読み取り、更新済みパスワード値の暗号化解除、および同期を必要とするシステムへの値の伝搬を行います。

第 10 章 JMS パスワード・ストア

JMS パスワード・ストアを使用すると、JMS クライアントがパスワードを読み取る JMS キューに、インターセプトされたユーザー・パスワードを保管できます。JMS パスワード・ストアは、以前は IBM WebSphere MQ Everyplace パスワード・ストアと呼ばれていました。

JMS パスワード・ストアは、JMS クライアントがパスワードを読み取ることのできる JMS プロバイダー・キューに、インターセプトされたユーザー・パスワードを保管するために必要な機能を備えています。例えば、IBM Security Directory Integrator などです。

JMS パスワード・ストア・パッケージは、ストレージ・コンポーネントと JMS パスワード・ストア・コネクターから構成されます。JMS パスワード・ストア・コネクターについて詳しくは、「リファレンス」を参照してください。ストレージ・コンポーネントは実質的に、Password Synchronizer により始動されるパスワード・ストアです。 JMS パスワード・ストア・コネクターは、IBM Security Directory Integrator 側の特殊なコネクターであり、構成された JMS プロバイダーが保管したパスワードを取得できます。

このパスワード・ストアのクラスは、
`com.ibm.di.plugin.pwstore.jms.JMSPasswordStore` です。

Apache ActiveMQ ドライバー

ActiveMQ を JMS パスワード・ストア・コンポーネントの JMS プロバイダーとして使用するには、**pwsync.props** の **jmsDriverClass** プロパティーを `com.ibm.di.plugin.pwstore.jms.driver.ActiveMQ` に設定します。 ActiveMQ ドライバーには、次のパラメーターがあります。

`jms.broker` - ActiveMQ サーバーのアドレス (プロトコル、IP アドレス、TCP ポート番号など)。例えば、`tcp://activeMQhost:61616` や `ssl://activeMQhost:61617` (SSL 接続を使用する場合) のように指定します。

IBM WebSphere MQ Everyplace ドライバー

IBM WebSphere MQ Everyplace ドライバーは、IBM WebSphere MQ Everyplace キュー・マネージャーを作成し、必要な接続オブジェクトを取得します。

IBM WebSphere MQ Everyplace を JMS パスワード・ストア・コンポーネントの JMS プロバイダーとして使用するには、`pwsync.props` ファイルの **jmsDriverClass** プロパティーを `com.ibm.di.plugin.pwstore.jms.driver.IBMMQe` に設定する必要があります。

注: IBM WebSphere MQ Everyplace キュー・マネージャーを作成する必要があります。これを作成するには、Password Synchronizer にバンドルされている IBM WebSphere MQ Everyplace 構成ユーティリティーを使用します。IBM WebSphere

MQ Everyplace 構成ユーティリティーについて詳しくは、 90 ページの『MQe キュー・マネージャーのセットアップ』を参照してください。

IBM WebSphere MQ ドライバー

IBM WebSphere MQ ドライバーは、IBM WebSphere MQ JMS プロバイダーとの接続を確立します。 IBM WebSphere MQ を JMS パスワード・ストア・コンポーネントの JMS プロバイダーとして使用するには、`pwsync.props` の **`jmsDriverClass`** プロパティーを `com.ibm.di.plugin.pwstore.jms.driver.IBMMQ` に設定します。

IBM WebSphere MQ ドライバーには、次のパラメーターがあります。

jms.broker
IBM WebSphere MQ サーバーのアドレス (IP アドレス、TCP ポート番号など)。例えば、192.168.113.54:1414 のように指定します。

jms.serverChannel
IBM WebSphere MQ サーバー・インスタンス用に構成されたサーバー・チャネルの名前。

jms.qManager
IBM WebSphere MQ サーバー・インスタンス用に定義されたキュー・マネージャーの名前。

jms.sslCipher
IBM WebSphere MQ サーバー・チャネルの構成時に選択された暗号に対応する暗号スイート名。例えば、SSL_RSA_WITH_RC4128_MD5 のように指定します。

jms.sslUseFlag
IBM WebSphere MQ サーバー・インスタンスへの接続時に SSL を使用するかどうかを指定します。有効な値は `true` および `false` です。

IBM WebSphere MQ ドライバーで SSL を使用する場合は、 13 ページの『第 3 章 パスワード同期プラグインの共通の構成およびユーティリティー』の SSL Java プロパティーの表にあるプロパティーを使用して、JMS パスワード・ストアと IBM WebSphere MQ との間の関係を設定します。

構成情報については、IBM WebSphere MQ サーバーの資料を参照してください。

Microbroker ドライバー

ユーザーが既存の Microbroker インストール済み環境を使用している場合は、Microbroker ドライバーを利用できます。このドライバーは、Microbroker プロバイダーへの接続を確立します。 Microbroker を JMS パスワード・ストア・コンポーネントの JMS プロバイダーとして使用するには、`pwsync.props` ファイルの **`jmsDriverClass`** プロパティーを `com.ibm.di.plugin.pwstore.jms.driver.IBMMB` に設定します。

Microbroker ドライバーには、次のパラメーターがあります。

jms.broker
Microbroker サーバーのアドレス (IP アドレス、TCP ポート番号など)。例えば、9.126.6.120:1883 など。

jms.clientID
必要なクライアント ID。

注: Microbroker を JMS パスワード・ストアとして使用するには、いくつかの Microbroker JAR ファイルが必要です。必要な JAR ファイルのサンプル・リストについては、「リファレンス」の『JMS コネクター』セクションを参照してください。

JMS スクリプト・ドライバー

ユーザー定義の JMS スクリプト・ドライバーは、JMS パスワード・ストアではサポートされません。 JavaScript エンジンは、Password Synchronizer にバンドルされていません。

パスワード・メッセージのセキュリティー

JMS パスワード・ストアと JMS パスワードの間では、パスワードを含むメッセージを、プレーン・テキスト・メッセージ、PKI 暗号化メッセージ、または PKCS7 カプセル化メッセージとして転送することができます。

JMS パスワード・ストアは、パスワードを JMS プロバイダーのキュー上にメッセージとして保管します。パスワードを含むメッセージを次のようにして送信できます。

- プレーン・テキスト・メッセージ

  メッセージは、JMS パスワード・ストアと JMS パスワード・ストア・コネクターとの間でプレーン・テキストとして転送されます。このため、メッセージ・ベースのセキュリティーは適用されません。

- IBM Security Directory Integrator 6.1.1 より前の PKI 暗号化メッセージ

  この機能はオプションです。このオプションが使用されると、以下の操作のために `.jks` ファイルの証明書が使用されます。

  – JMS パスワード・ストアによる受信メッセージの暗号化
  – JMS パスワード・ストア・コネクターによるメッセージの暗号化解除

  注: IBM Security Directory Integrator 6.1.1 以降では、この暗号化は推奨されません。PKCS7 カプセル化ではメッセージをよりセキュアに転送することができ、暗号化も行われるためです。

- PKCS7 カプセル化メッセージ

  IBM Security Directory Integrator 6.1.1 以降では、JMS パスワード・ストアおよび JMS パスワード・ストア・コネクターは、署名と暗号化の両方が組み込まれた PKCS7 をサポートしています。

カプセル化に PKCS7 を使用するかどうかはオプションです。デフォルトでは、オフになっています。PKCS7 を使用する場合、JMS パスワード・ストアと JMS パスワード・ストア・コネクターの両方を、PKCS7 を使用するように構成します。ただし、PKCS7 を使用すると、PKI 暗号化は許可されません。PKCS7 が暗号化をサポートしているためです。

JMS パスワード・ストアの構成

JMS パスワード・ストアのプロパティーを pwsync.props 構成ファイルに設定する必要があります。

JMS パスワード・ストアのプロパティーは、プラグインの汎用構成ファイル pwsync.props に設定されています。デフォルトでは、プラグインごとに 1 つのファイルが存在します (例: *TDI_install_dir*/pwd_plugins/tds/pwsync.props)。

注: 汎用構成ファイルでは、各パスワード・プロパティーを手動で暗号化する必要があります。パスワードを暗号化するには、encryptPasswd ユーティリティーを使用します。このユーティリティーは、対称アルゴリズムを使用してパスワードを暗号化します。信頼できるシステム・ユーザーのみが pwsync.props ファイルを読み取れるようにしてください。

encryptPasswd ユーティリティーでは、パスワードをパラメーターとして渡します。暗号化されたパスワードは、標準出力に出力されます。
構成パラメーターと encryptPasswd ユーティリティーについて詳しくは、13 ページの『第 3 章 パスワード同期プラグインの共通の構成およびユーティリティー』を参照してください。

pwsync.props ファイルで次のようにします。

- プレーン・テキスト・メッセージの場合は、encrypt=false を設定します。
- IBM Security Directory Integrator 6.1.1 PKI より前の暗号化メッセージの場合は、encrypt=true を設定します。
- PKCS7 カプセル化メッセージの場合は、pkcs7=true および encrypt=false を設定します。

  注: encrypt=true および pkcs7=true の設定は無効です。 encrypt または pkcs7 のいずれかを true に設定してください。

パスワード・メッセージ・セキュリティーについて詳しくは、85 ページの『パスワード・メッセージのセキュリティー』を参照してください。

以下の例は、pwsync.props ファイルの JMS パスワード・ストア構成セクションを抽出したものを示しています。

```
#
# This is the configuration file of the Password Synchronizer.
# It is used by all parts of the Password Synchronizer: the Plug-in,
# the Proxy and the Password Store component.
#
# Enter (name)=(value) to set configuration properties.
#
# Follow the Java properties file format. Backslashes must be escaped:
# e.g. instead of 'c:¥myfile.txt' type 'c:¥¥myfile.txt'.
#




# Executable (binary or shell script) used to start the Java Proxy.
# If this property is set, both 'jvmPath' and 'jvmClassPath' will be ignored.
proxyStartExe=C:¥¥Program Files¥¥IBM¥¥TDI¥¥V7.2/pwd_plugins/bin/startProxy.bat

# Port number, on which the Java Proxy listens for commands.
serverPort=18001

# The log file of the Plug-in part of the Password Synchronizer.
# If empty, no logging will be done.
```

```
logFile=C:¥¥Program Files¥¥IBM¥¥TDI¥¥V7.2/pwd_plugins/windows/plugin.log

# Whether to reject password changes if the Password Store is down.
checkRepository=true

# The log file of the Java Proxy part of the Password Synchronizer. If empty,
# no logging will be done.
javaLogFile=C:¥¥Program Files¥¥IBM¥¥TDI¥¥V7.2/pwd_plugins/windows/proxy.log

# Turn on debug logging for all parts of the Password Synchronizer.
debug=true

# Custom data that will be send with each password change.
# This string can be used to uniquely identify the machine or product that generates
# the changes (e.g. machine IP, application name and version).
#customData=machine1



#
# User filtering configuration
#

# A list of Windows groups. If a user is a member of some group on the list,
# the user will be accepted # by the user filter (assuming the user is not
# excluded by some of the exclude lists).
# Group names must be separated by semicolons. Redundant white-spaces are not allowed.
# includeGroups=



# A list of Windows groups. If a user is a member of some group on the list, the user
# will not be accepted
# by the user filter.
# Group names must be separated by semicolons. Redundant white-spaces are not allowed.
# excludeGroups=

# A list of DN suffixes. If a user's Distinguished Name matches some suffix on the list,
# the user will be accepted by the user filter
# (assuming the user is not excluded by some of the exclude lists).
# DN suffixes must be separated by semicolons. Redundant white-spaces are
# not allowed.
# includeDNs=

# A list of DN suffixes. If a user's Distinguished Name matches some suffix on
# the list, the user will not
# be accepted by the user filter.
# DN suffixes must be separated by semicolons. Redundant white-spaces are not allowed.
# excludeDNs=

# Types of the accounts for which password changes will be reported.
# It is a space-delimited list of account types. Recoginzed account types are:
# NORMAL_ACCOUNT
# TEMP_DUPLICATE_ACCOUNT
# INTERDOMAIN_TRUST_ACCOUNT
# WORKSTATION_TRUST_ACCOUNT
# SERVER_TRUST_ACCOUNT
#
# accountTypes=NORMAL_ACCOUNT



#
# The Password Store component
#
# Specify the full name of the Java class.
# Choose one of the following:
# com.ibm.di.plugin.pwstore.log.LogPasswordStore
# com.ibm.di.plugin.pwstore.jms.JMSPasswordStore
# com.ibm.di.plugin.pwstore.ldap.LDAPPasswordStore
#
# LogPasswordStore is for testing purposes only - you should NEVER use it in
# production environment.
#
syncClass=com.ibm.di.plugin.pwstore.log.LogPasswordStore
```

```
#
# Public key encryption of passwords
#
# encrypt=true
# encryptKeyStoreFilePath=
# encryptKeyStoreFilePassword=
# encryptKeyStoreCertificate=

# 'encryptKeyPassword' is required by the LDAP Password Store (the rest do not need it)
# encryptKeyPassword=



#
# PKCS7 encapsulation of passwords
#
# pkcs7=true
# pkcs7KeyStoreFilePath=
# pkcs7KeyStoreFilePassword=
# pkcs7MqeStoreCertificateAlias=
# pkcs7MqeConnectorCertificateAlias=



#
# SSL configuration properties
#
# javax.net.ssl.trustStore=
# javax.net.ssl.trustStorePassword=
# javax.net.ssl.trustStoreType=
# javax.net.ssl.keyStore=
# javax.net.ssl.keyStorePassword=
# javax.net.ssl.keyStoreType=



#
# LDAP Password Store Configuration
#

# LDAP server host
# ldap.hostname=localhost

# LDAP server port
# ldap.port=389

# LDAP bind dn
# ldap.admindn=cn=root

# LDAP bind password
# This field must be encoded. Use the 'encryptPasswd' utility.
# ldap.password=0c0bf0e3146b

# If set to true, password changes will be committed synchronously
# to the Password Store when a password change notification is received.
# The source of the password change will be blocked
# until the password change is written to the Password Store.
#
# If set to false, the commit will be asynchronous.
# Use the 'ldap.delayMillis' property to configure
# the time to wait before committing the password change.
# ldap.waitForStore=true

# Time to wait (in milliseconds), before committing the password change to the
# Password Store. Will be ignored if 'waitForStore' is set to true.
# ldap.delayMillis=2000

# Use SSL for LDAP communication.
# If set to true, JSSE must be configured (set the javax.net.ssl.trustStore and
# javax.net.ssl.keyStore properties).
# ldap.ssl=false

# Location in the LDAP directory tree, where the Password Synchronizer
# will store data.
# ldap.suffix=dc=carnd11,o=ibm,c=us

# Name of an LDAP object class used to hold information for a given user.
```

```
# ldap.schemaPersonObjectName=ibm-diPerson

# Name of an LDAP attribute which represents user identifier.
# This attribute must be a member of the object class specified by the
# 'ldap.schemaPersonObjectName' property.
# ldap.schemaUseridAttributeName=ibm-diUserId

# Name of an LDAP attribute which represents user password.
# This attribute must be a member of the object class specified by
# the 'ldap.schemaPersonObjectName' property.
# ldap.schemaPasswordAttributeName=ibm-diPassword




#
# MQe Password Store Configuration
#

# JMS driver, used to establish connecton to the message broker.
# jmsDriverClass=com.ibm.di.plugin.pwstore.jms.driver.IBMMQe

# The path to the .ini file of the MQe QueueManager.
# mqe.file.ini=

# The TCP/IP port that is used when the MQe Connector sends notifications to the
# Storage Component.
# mqe.notify.port=41002


#
# ActiveMQ Password Store Configuration
#

# JMS driver, used to establish connecton to the message broker.
# jmsDriverClass=com.ibm.di.plugin.pwstore.jms.driver.ActiveMQ

# JMS Server address (jms.broker=tcp://<activeMQhost>:61616 or
# jms.broker=ssl://<activeMQhost>:61617)
# jms.broker=


#
# Websphere MQ Password Store Configuration
#

# JMS driver, used to establish connecton to the message broker.
# jmsDriverClass=com.ibm.di.plugin.pwstore.jms.driver.IBMMQ

# The ID of this client. This value is used when connecting to a broker.
# Most brokers do not allow clients to have the same ID.
# jms.clientId=

# JMS Server address (ip host and tcp port number).
# jms.broker=<host>:<port>
# Login username for the password queue.
# jms.username=

# Login password for password queue.
# This field must be encoded. Use the 'encryptPasswd' utility.
# jms.password=

# MQ Server Channel
# jms.serverChannel=

# Queue Manager Name
# jms.qManager=

# Turn on SSL
# jms.sslUseFlag=false

# SSL cipher suite
# (See the WebSphere MQ documentation for a full list of supported cipher suites).
# jms.sslCipher=SSL_RSA_WITH_RC4_128_MD5




#
# IBM Security Identity Manager Integration
```

```
#
# Passwords will be be verified by an IBM Security Identity Manager Server's
# Password Strength Servlet prior to synchronization.
# To enable TIM integration, set the 'syncClass' property to one of the following:
# com.ibm.di.plugin.pwstore.log.LogPasswordStoreITIMDecorator
# com.ibm.di.plugin.pwstore.jms.JMSPasswordStoreITIMDecorator
# com.ibm.di.plugin.pwstore.ldap.LDAPPasswordStoreITIMDecorator

# URL of the IBM Security Identity Manager hosted Password Strength Servlet.
# Note: If https is used, the javax.net.ssl.trustStore* properties must be set.
# Where the specified truststore contains the IBM Security Identity Manager Server's
# certificate.
# itimPasswordUrl=https://<host>:<port>/passwordsynch/synch

# IBM Security Identity Manager user account permitted to perform a password check.
# itimPrincipalName=

# The password for the IBM Security Identity Manager user acount specified by
# the 'itimPrincipalName' property.
# itimPrincipalPassword=

# The IBM Security Identity Manager service name against which the password check
would be performed.
# itimSourceDN=erservicename=TDIPasswordService, o=IBM, ou=IBM, dc=com
```

注:

mqe.file.ini

IBM WebSphere MQ Everyplace ドライバーを使用している場合にのみ必要です。使用していない場合、このパラメーターは無視され、代わりに **jms.broker** プロパティーが使用されます。

.ini ファイルのパスは、MQe 構成ユーティリティーで生成されます。例えば、C:¥¥Program Files¥¥IBM¥¥TDI¥¥V7.2¥¥pwd_plugins¥¥tds¥¥MQePWStore¥¥pwstore_client.ini のようなパスが生成されます。

mqe.notify.port

IBM WebSphere MQ Everyplace ドライバーを使用している場合にのみ必要です。それ以外の場合、このパラメーターは無視されます。

JMS パスワード・コネクターが JMS パスワード・ストアの代わりに IBM WebSphere MQ Everyplace ドライバーに通知を送信するときに使用される TCP/IP ポート。デフォルト値は 41002 です。

注: このパラメーターについて詳しくは、「リファレンス」の『IBM WebSphere MQ Everyplace での JMS パスワード・ストアからの累積メッセージの強制転送』セクションを参照してください。

MQe キュー・マネージャーのセットアップ

IBM WebSphere MQ Everyplace キュー・マネージャーを自動的に作成して構成するには、*tdi_install_dir*/pwd_plugins/jars ディレクトリーにある IBM WebSphere MQ Everyplace 構成コンポーネント・ユーティリティーを実行する必要があります。

- IBM WebSphere MQ Everyplace 構成コンポーネントを実行する前に、*TDI_install_dir*/pwd_plugins/etc/mqeconfig.props プロパティー・ファイルを開き、以下のプロパティーの値を設定します。

  clientRootFolder

  IBM WebSphere MQ Everyplace キュー・マネージャーを保管するフォル

ダー。例えば、Windows の場合は、C:¥¥Program Files¥¥IBM¥¥TDI¥¥V7.2¥¥pwd_plugins¥¥tds¥¥MQePWStore となります。

注: プロパティー・ファイルで Windows のファイル・パスを指定する場合、ファイル分離文字の円記号 (¥) は、もう一つ円記号を追加して (¥¥) エスケープする必要があります。

serverIP
IBM Security Directory Integrator と JMS パスワード・ストアがデプロイされるシステムの IP アドレス。

communicationPort
2 つの IBM WebSphere MQ Everyplace キュー・マネージャー間で通信を行うために使用される TCP/IP ポート。

clientRegistryType
オプションです。認証済み IBM WebSphere MQ Everyplace アクセスのデプロイメントでのみ必要です。使用する場合は、値を **PrivateRegistry** に設定する必要があります。 **PrivateRegistry** には、IBM WebSphere MQ Everyplace Mini-Certificate サーバーが発行した証明書が保管されます。

clientRegistryPin
オプションです。認証済み IBM WebSphere MQ Everyplace アクセスのデプロイメントでのみ必要です。使用する場合、この値は、PIN アクセス・コードを表します。PIN アクセス・コードは、**PrivateRegistry** にアクセスするために IBM Security Directory Integrator JMS パスワード・ストアによって使用されます。この値は、IBM WebSphere MQ Everyplace .ini ファイルにプレーン・テキストとして保管されます。

clientKeyRingPassword
オプションです。認証済み IBM WebSphere MQ Everyplace アクセスのデプロイメントでのみ必要です。この値は、IBM WebSphere MQ Everyplace Mini-Certificate サーバーからの証明書を要求するときに使用されます。この値は証明書を生成するためのシード値になります。この値は、IBM WebSphere MQ Everyplace .ini ファイルにプレーン・テキストとして保管されます。

certServerReqPin
オプションです。認証済み IBM WebSphere MQ Everyplace アクセスのデプロイメントでのみ必要です。この値は、IBM WebSphere MQ Everyplace Mini-Certificate サーバーから証明書を要求するときにキュー・マネージャーにより 1 回限りの認証 PIN として使用されます。この値は、Mini-Certificate サーバーのセットアップで得られる要求 PIN の値に一致する必要があります。

certServerIPAndPort
オプションです。認証済み IBM WebSphere MQ Everyplace アクセスのデプロイメントでのみ必要です。この値は、IBM WebSphere MQ Everyplace Mini-Certificate サーバーの要求の宛先アドレスとして使用されます。この値の形式は、FastNetwork:*<host>*:*<port>* です。ここで *host* は、IBM WebSphere MQ Everyplace Mini-Certificate サーバーが実行され

ているシステム名または TCP/IP アドレスです。ポート値は、Mini-Certificate サーバーのセットアップで得られる *port* 値に一致する必要があります。

debug `true` または `false` を指定して、デバッグ情報をオンまたはオフにします。

値として `true` を指定すると、IBM WebSphere MQ Everyplace がログに記録したバイナリー・トレース情報が収集されます。このフラグを有効にすると、現行ディレクトリー (ソリューション・ディレクトリー) に単一のトレース・ファイルが生成されます。トレース・ファイルのサイズには制限がありません。このファイルのサイズは、トレース収集が停止するまで、または残りのディスク・スペースがなくなるまで増加し続けます。このファイルの名前は、`mqe0.trc` です。

以下の例は、サンプルの `mqeconfig.props` 構成ファイルを示しています。

```
clientRootFolder=C:¥¥Program Files¥¥IBM¥¥TDI¥¥V7.2¥¥pwd_plugins¥¥tds¥¥MQePWStore
serverIP=127.0.0.1
#clientRegistryType=PrivateRegistry
#clientRegistryPin=<Private client registry access PIN>
#clientKeyRingPassword=<Seed value for certificate generation>


# Properties used for setting up MQe Queue Manager as server

serverRootFolder=C:¥¥Program Files¥IBM¥¥TDI¥¥V7.2¥¥MQePWStore
#serverRegistryType=PrivateRegistry
#serverRegistryPin=<Private client registry access PIN>
#serverKeyRingPassword=<Seed value for certificate generation>

#certServerReqPin=<One time certificate request PIN>
#certServerIPAndPort=FastNetwork:<Mini-Certificate server hostname or IP>:<port>
#certRenewalEntityName=<QueueManager name or QueueManager+Queue name>

communicationPort=41001

#disableQueueRegistry=
debug=true
```

注: プロパティー・ファイルで Windows のファイル・パスを指定する場合、ファイル分離文字の円記号 (¥) は、もう一つ円記号を追加して (¥¥) エスケープする必要があります。

ストレージ・コンポーネントの構成時、`serverRootFolder` プロパティーは使用されません。このプロパティーは、IBM WebSphere MQ Everyplace コネクターで IBM WebSphere MQ Everyplace キュー・マネージャーを構成するために使用され、その値は無視されます。

- ストレージ・コンポーネント用の IBM WebSphere MQ Everyplace キュー・マネージャーを作成し、自動的に構成するには、*TDI_install_dir*`/pwd_plugins/bin` フォルダーでコマンド・プロンプトを開き、以下のコマンドを 1 行で入力します。

  ```
  .¥mqeconfig.bat ..¥etc¥mqeconfig.props create client
  ```

  このコマンドのログがコンソールに表示されます。正常に完了すると、「クライアント MQe 構成が正常に完了しました」というメッセージが表示されます。`mqeconfig.props` ファイルに IBM WebSphere MQ Everyplace 認証済みアクセスに関連するオプション・パラメーターが含まれている場合は、このステップにより、IBM WebSphere MQ Everyplace Mini-Certificate サーバーからの必要な証明書が自動的に要求されます。

ヒント: IBM WebSphere MQ Everyplace 証明書の認証済みアクセスのデプロイメントを実行する場合、証明書は、認証可能なエンティティーごとに 1 回のみ要求されます。構成時に以下の例外メッセージが報告された場合は、Mini-Certificate サーバー GUI を使用して、そのエンティティーの証明書の発行を再度有効にしてください。

```
[MQeConfig] [28/07/05 10:10:01]: Action failed:
Code=351;com.ibm.mqe.MQeException: Registration exception =
com.ibm.mqe.MQeException: certificate request failed[PWStoreClient 4]
 (code=8)[PWStoreClient 8] (code=351) [MQeConfig] [28/07/05 10:10:01]:
Error: Server MQe configiration failed; exception:java.lang.Exception:
Code=351;com.ibm.mqe.MQeException: Registration exception = com.ibm.mqe.
MQeException: certificate request failed[PWStoreClient4] (code=8)
[PWStoreClient 8] (code=351)
```

注: IBM WebSphere MQ Everyplace キュー・マネージャーの構成を変更するために、以下の 2 つのオプションが用意されています。

– ディスクから IBM WebSphere MQ Everyplace キュー・マネージャーを削除し、それを前述の手順に従って作成する。

– IBM WebSphere MQ Everyplace 2.0.1.7 キュー・マネージャーと互換性のある IBM WebSphere MQ Everyplace 管理ツールをインストールし、それを使用してキュー・マネージャーの設定を変更する。例えば、IBM WebSphere MQ Everyplace エクスプローラーなどです。

WebSphere MQ セットアップ

IBM WebSphere MQ を JMS プロバイダーとして使用する場合、インストールされた IBM WebSphere MQ から Password Synchronizer のクラスパスに、JAR ファイルをコピーする必要があります。

以下の JAR ファイルを Password Synchronizer のクラスパスに組み込みます。

IBM WebSphere MQ 6.0 の場合:

- com.ibm.mqjms.jar
- com.ibm.mq.jar
- jms.jar
- connector.jar
- dhbcore.jar
- jta.jar

IBM WebSphere MQ 7.1 の場合:

- com.ibm.mqjms.jar
- com.ibm.mq.jmqi.jar
- jms.jar
- dhbcore.jar

第 11 章 Log パスワード・ストア

Log パスワード・ストアを使用すると、Java プロキシーとネイティブ・プラグイン間の通信を検証できます。

Log パスワード・ストアを使用すると、標準のパスワード・ストアが実行するすべてのアクションをログに記録できます。このパスワード・ストアは、Java プロキシーとネイティブ・プラグインが正常に通信しているかどうかを検証する場合に役立ちます。

注: このパスワード・ストアは、ユーザー名とパスワードを Java プロキシーのログ・ファイルに記録します。このパスワード・ストアは、テストの目的でのみ使用する必要があります。例えば、プラグインの構成時や開発時に使用します。

このパスワード・ストアのクラスは、
`com.ibm.di.plugin.pwstore.log.LogPasswordStore` です。

第 12 章 Password Synchronizer に関する問題のトラブルシューティング

Password Synchronizer に関する問題を診断するには、プラグインと Java プロキシー・コンポーネントのログ・ファイルを確認する必要があります。

プラグインと Java プロキシーの操作中に発生した問題は、すべてエラー・メッセージとしてログに記録されます。エラー・メッセージのタイム・スタンプと重大度レベルを使用して、問題を分析することができます。

プラグインに関する問題のトラブルシューティング

プラグイン・コンポーネントのログ・メッセージは、プラグイン・タイプに応じて、UNIX syslog ファイルまたは LDAP サーバー・ログ・ファイルに書き込まれます。

トラブルシューティングを行うには、以下の詳細事項を確認する必要があります。

- 初期化状況を確認してください。各 Password Synchronizer は、初期化時に状況メッセージをログに記録します。
  - ログが存在するかどうかを確認します。ファイルにログが記録されるプラグインについてのみ、この確認を行ってください。
  - 初期化が成功したことを知らせるメッセージがログに記録されているかどうかを確認します。
  - 初期化メッセージのタイム・スタンプが最近のものかどうかを確認します。以前に実行したプラグインのメッセージがログに残っている場合があります。

  最近の初期化で使用不可の状況がログに記録されている場合、プラグインが実行されていないか、ログへの書き込み前にプラグインの初期化が失敗しています。以下の原因が考えられます。
  - ターゲット・システムにプラグインが正しく登録されていない。 Password Synchronizer の関連セクションを参照して、登録手順を確認してください。
  - プラグインの構成ファイル `pwsync.props` が見つからない。 Password Synchronizer の関連セクションを参照して、プラグインに対して構成ファイルを指定する方法を確認してください。
- 実行エラーが発生していないかどうかを確認してください。

Java プロキシーの問題のトラブルシューティング

Password Synchronizer の Java プロキシー・コンポーネントとパスワード・ストア・コンポーネントは、**`JavaLogFile`** パラメーターで指定されたファイルにメッセージをログ記録します。デフォルト・ログ・ファイルは `proxy.log` です。

`javaLogFile` パラメーターについての詳細は、『javaLogFile 構成パラメーター』を参照してください。

- 初期化状況を検査してください。

プラグインは、初期化時に Java プロキシーを開始します。 Java プロキシーは、開始すると、状況メッセージをログ記録します。

– ログ・ファイル proxy.log が存在するかどうかの検証。
– 初期化が成功したことを知らせるメッセージがログに記録されているかどうかを確認します。
– 初期化メッセージのタイム・スタンプが最近のものかどうかを確認します。プロキシーの前回の実行時のメッセージがログに残っていることがあります。
–

最近の初期化で非可用性の状況がログに記録されている場合、プロキシーが実行中でないか、あるいはログへの書き込みの前に初期化に失敗したことを示します。 Java プロキシーの一般的な標準ログまたはエラー・ログは、*authentication_folder*/proxy.stdout.log ファイルに用意されています。*authentication_folder* は、プラグイン構成ファイル pwsync.props を格納するフォルダーです。ログ・ファイルに java.lang.NoClassDefFoundException といったメッセージがある場合、考えうる理由は次のものです。

– プロキシーのクラスパスが不完全です。

  パスワード・ストアを実行するのに必要なサード・パーティー・ライブラリーがすべて、プラグインの jars フォルダーに追加されているかどうかを検証します。デフォルト・パスは *TDI_install_dir*/pwd_plugins/jars/ です。startProxy スクリプトによって生成されたクラスパスが、ご使用のオペレーティング・システムで許可されているシェル・コマンドの長さより長い場合、JavaProxy を実行できないことがあります。
– startProxy.bat または startProxy.sh を手動で実行する場合に発生するエラーの場合、次のようにします。

  startProxy スクリプトをコマンド・プロンプトから正しく実行できるかどうかを検証します。

  Linux または UNIX では、スクリプト・パスの構成が、ご自分のオペレーティング・システム環境で有効であることを確かめます。

  Windows では、プラグインの始動スクリプトは JScript を使用してクラスパスを収集します。 Windows Script Host (WSH) が有効になっていることを確かめます。ご使用のシステムで WSH が無効になっている場合、次のようなメッセージが表示されます。

  ```
  Windows Script Host access is disabled on this machine.
  Contact your administrator for details.
  ```

  このメッセージは、*TDI_install_dir*/pwd_plugins/bin/worker.js ファイルをダブルクリックすると表示されます。
– 初期化時に想定外のエラーが起きた場合、次のようにします。

  Java プロキシー・プロセスの始動に関連したエラー・メッセージをプラグインのログ・ファイルでチェックします。

プラグイン・ログで、プラグインが Java プロキシーを開始するのに使用するコマンド・ストリングを見つけ出して、それをコマンド・シェルで実行します。

- 実行エラーが発生していないかどうかを確認してください。

IBM Security Identity Manager と統合した PAM パスワード・プラグインの問題のトラブルシューティング

IBM Security Identity Manager および PAM パスワード・プラグインによって拒否される場合でもユーザー・パスワードが変更されてしまうときの問題のトラブルシューティングを行うには、以下の説明を参照してください。

問題

PAM パスワード・プラグインを IBM Security Identity Manager と統合してパスワード・ポリシーの検証を行っています。ユーザーがパスワードを変更しようとしたときに、以下の問題が発生します。

1. 新しいパスワードが IBM Security Identity Manager のパスワード・ポリシーでの要件を満たしていない場合に、以下のエラーがコマンド行に出力される。

```
testuser1@iapp2 ~]$ passwd
Changing password for user testuser1.
Changing password for testuser1.
(current) UNIX password:
New password:
Retype new password:
passwd: Authentication token manipulation error
```

2. パスワードがパスワード・ルールを満たしていないため、IBM Security Identity Manager によって拒否されていることが `proxy.log` に示される。構成されているパスワード・ストアにパスワードの変更を保管するための IBM Security Directory Integrator の Java プロキシーもこのパスワードを拒否する。

```
[6/18/13 9:55 AM] {Proxy} DEBUG:
                  CTGDKN026I Received operational code: '2'.
[6/18/13 9:55 AM] {LDAPStore} WARN:
                  CTGIME012E  The password does not meet
                  the requirements of the password rule.
                  The following error occurred.
                  Error: CTGIMH023E A user name cannot be
                  part of a password.
[6/18/13 9:55 AM] {Proxy} WARN:
                  CTGDKN028I Rejecting operation.
```

3. それにもかかわらず、ユーザー・パスワードが変更されてしまう (この事態が発生してはならない)。変更したパスワードを使用してユーザーがログインできる。

解決策

ここに示すように `/etc/pam.d/system-auth` の設定を更新してください。

IBM Security Directory Integrator プラグインのモジュールおよびオペレーティング・システム・プラグインのモジュールに `requisite` のマークを付けます。この設定により、先行するプラグイン・モジュールによって返されたエラーが無視されなくなります。

```
password    requisite    pam_cracklib.so try_first_pass retry=3 type=
password    requisite    /opt/IBM/TDI/V7.2/pwd_plugins/pam/libpamtivoli_64.so
                         use_first_pass
                         /opt/IBM/TDI/V7.2/pwd_plugins/pam/pwsync_ioc.props
password    requisite     pam_unix.so md5 shadow use_authtok
```

また、/etc/pam.d/passwd の設定も調べてください。パスワード・モジュールに substack のマークが付いていることを確認します。

```
#%PAM-1.0
auth       include      system-auth
account    include      system-auth
password   substack     system-auth
```

パスワード・プラグインの機能拡張

このセクションでは、パスワード・プラグインの機能拡張について説明します。

プラグインの機能拡張

IBM Security Directory Integrator のパスワード・プラグインでは、次の機能拡張が行われました。

パスワード同期メッセージ内のカスタム属性のプロビジョニングをサポートする拡張 Java プロキシー

通常、同期データには、ユーザー名、パスワード値、およびパスワード変更のタイプ (追加、削除、更新など) のみが含まれます。カスタム属性の内容として使用可能なオプションには、ハードコーディングされたストリング、Password Synchronizer がデプロイされているシステムのホスト名または IP アドレス、Java プロキシーが通知を受信した時点のタイム・スタンプなどがあります。Java プロキシーは、パスワード同期データ内のカスタム属性をサポートするように機能拡張されています。

第 13 章 IBM Security Identity Manager の統合

Password Synchronizer 用の IBM Security Identity Manager の統合により、IBM Security Identity Manager Server のパスワード・ストレングス・サーブレットを使用した同期済みパスワードの検証が可能になります。

概説

Password Synchronization には、IBM Security Identity Manager パスワード・ポリシーを使用したパスワード強度検査機能が組み込まれています。以下の IBM Security Identity Manager のデコレーター Password Synchronizer クラスのいずれかを使用して、IBM Security Identity Manager の統合を有効にすることができます。

- `com.ibm.di.plugin.pwstore.ldap.LDAPPasswordSynchronizerITIMDecorator`
- `com.ibm.di.plugin.pwstore.jms.MQePasswordStoreITIMDecorator`
- `com.ibm.di.plugin.pwstore.log.LogPasswordStoreITIMDecorator`

  注: `com.ibm.di.plugin.pwstore.log.LogPasswordStoreITIMDecorator` パスワード・ストアは、ユーザー名とパスワードを Java プロキシーのログ・ファイルに記録します。このパスワード・ストアは、テスト目的のみで使用してください。例えば、プラグインのデプロイメント・テストなどで使用してください。

サポートされているシンクロナイザー

IBM Security Identity Manager 用の Password Synchronizer のデコレーター・クラスは、以下の Password Synchronizer でサポートされます。

- Windows 用 Password Synchronizer
- IBM Security Directory Server Synchronizer 用の Password Synchronizer
- Sun Directory Server 用 Password Synchronizer
- UNIX および Linux 用 Password Synchronizer

注: IBM Domino HTTP Password Synchronizer は IBM Security Identity Manager との統合をサポートしていません。IBM Domino サーバー上でカスタムのパスワード・ポリシーを作成することができます。これらのパスワード・ポリシーを使用して、保管前のパスワードを検証することができます。

IBM Security Identity Manager のパスワード・ストレングスの検証通信

外部のアプリケーションは、パスワード・ストレングスの検証を求める XML 要求を IBM Security Identity Manager サーバーから作成する必要があります。この要求は、IBM Security Identity Manager サーバーによってホストされるサーブレットに HTTPS 経由で送信されます。以下のサンプルは、パスワード・ストレングスの検証を求める XML 要求を示しています。

```
<PSWD_REQ_MSG>
 <CREDENTIALS principal="",pswd="" />
 <REQUEST op="check", srcDN="", userDN="", pswd="" />
</PSWD_REQ_MSG>
```

資格情報タグ

資格情報は、IBM Security Identity Manager プリンシパルのユーザー名とパスワードを表します。プリンシパルとパスワードの値を使用してクライアント (つまりパスワード・ストア・デコレーター) が使用可能になり、IBM Security Identity Manager サーバーが認証されます。 IBM Security Identity Manager プリンシパルは、IBM Security Identity Manager サーバー上に存在してパスワード検査の実行権限を与えられている必要があります。これらの資格情報の値は、構成プロパティーを介して IBM Security Directory Integrator クライアント・コンポーネントに渡されます。

要求タグ

エレメント属性は以下のとおりです。

- op – 実行される操作。デフォルト値は check です。ただし、値 synch を使用して、IBM Security Identity Manager とのパスワードの同期を行うことができます。
- srcDN - パスワード・ストレングス検査のソースであるサービス (リソース) の疑似識別名が格納されます。この識別名は、&<service RDN®>,<bu RDN>,<org RDN>,<tenant DN> という形式になります。 RDN は、attribute=value という形式になります。 service RDN は、組織図のセクション内のサービスを一意的に識別します。 bu RDN は、組織図の別のセクション内で、組織図内のコンテナーを一意的に識別します。組織図の構造に応じて、bu RDN の数がゼロになる場合もあれば、複数になる場合もあります。 org RDN は、テナント内の組織を一意的に識別します。 tenant DN は、テナントの物理的な識別名です。以下の識別名は、Acme 組織の IT 組織単位内の Test という名前のサービスを表します。

  ```
  erservicename=Test,ou=IT,o=Acme,ou=Acme,dc=com
  ```

  ou=Acme, dc=com は、テナントの物理的な DN、つまり単一のテナント・デプロイメント内の Directory Server のルート・セクションです。
- userDN – ソース・サービスの範囲内のユーザー・アカウントの識別名が格納されます。例えば、jdoe というユーザー ID を持つ UNIX ユーザーの識別名は eruid=jdoe となります。
- pswd – パスワード・ストレングスの検査対象となるパスワードの値が格納されます。

IBM Security Identity Manager と統合するための Password Synchronizer の構成

IBM Security Identity Manager と統合するように Password Synchronizer を構成するには、pwsync.props 構成ファイルに syncClass プロパティー値を設定する必要があります。

IBM Security Identity Manager のデコレーターを使用するように Password Synchronizer を構成します。以下のリストに示すデコレーター・クラス名のいずれかを使用します。

- com.ibm.di.plugin.pwstore.ldap.LDAPPasswordStoreITIMDecorator
- com.ibm.di.plugin.pwstore.ldap.JMSPasswordStoreITIMDecorator

- `com.ibm.di.plugin.pwstore.log.LogPasswordStoreITIMDecorator`

IBM Security Identity Manager と統合するように構成を行うには、`pwsync.props` 構成ファイルに以下の必須プロパティーを指定します。

注: プロパティー名では大/小文字が区別されます。

itimPasswordUrl
IBM Security Identity Manager でホストされるパスワード・ストレングス・サーブレットの URL。例を示します。

```
https://host:port/passwordsynch/synch
```

itimPrincipalName
パスワード検査を実行する IBM Security Identity Manager ユーザー名。

itimPrincipalPassword
`itimPrincipalName` プロパティーに指定された IBM Security Identity Manager ユーザー名のパスワード。

itimSourceDN
パスワード検査を実行する必要のある IBM Security Identity Manager サービス名。例を示します。

```
erservicename=TDIPasswordService, o=IBM, ou=IBM, dc=com
```

注: IBM Security Identity Manager の統合が可能なときは、Password Synchronizer の構成ファイルで **`checkRepository`** プロパティーに `true` を設定します。

付録. IBM ソフトウェア・サポート

IBM ソフトウェア・サポートでは、製品の問題点に関するサポートを提供します。

IBM ソフトウェア・サポートに連絡する前に、貴社が有効な IBM ソフトウェア保守契約を保持しており、IBM への問題の送信が許可されていることを確認してください。必要なソフトウェア保守契約は、ご使用の製品に応じて異なります。

- IBM 分散ソフトウェア製品 (Tivoli、Lotus、Rational® 製品のほか、Windows または UNIX オペレーティング・システムで稼働している DB2® および WebSphere 製品を含みますが、これだけに限定されません) の場合には、以下のいずれかの方法で、パスポート・アドバンテージに登録してください。
  - **オンライン**: 次のパスポート・アドバンテージ Web ページにアクセスして、「**How to Enroll**」をクリックします。

    http://www.lotus.com/services/passport.nsf/WebDocs/ Passport_Advantage_Home

    (URL の参照先は英語のみの対応となります)
  - **電話**: お客様の国での連絡先の電話番号を調べるには、IBM ソフトウェア・サポート Web サイト (http://techsupport.services.ibm.com/guides/contacts.html) にアクセスし、お客様の地域名をクリックしてください。
- IBM eServer™ ソフトウェア製品 (zSeries、pSeries、および iSeries® 環境で実行されている DB2 および WebSphere 製品を含みますが、これだけに限定されません) の場合は、IBM 営業担当員または IBM ビジネス・パートナーに直接ご相談いただくことによって、ソフトウェア保守契約を購入することができます。eServer ソフトウェア製品のサポートについての詳細は、IBM Technical Support Advantage Web ページ (http://www.ibm.com/servers/eserver/techsupport.html) にアクセスしてください。

どのタイプのソフトウェア保守契約が必要かわからない場合は、米国内では 1-800-IBMSERV (1-800-426-7378) に電話してください。その他の国では、Web 上の「IBM Software Support Handbook」(http://techsupport.services.ibm.com/guides/contacts.html) の連絡先のページにアクセスし、お客様の地域名をクリックして、その地域のサポート担当者の電話番号を調べてください。

以下のステップに従って、IBM ソフトウェア・サポートにお問い合わせください。

1. 106 ページの『お客様の問題点のビジネス・インパクトの判別』
2. 106 ページの『問題点の記述と背景情報の収集』
3. 106 ページの『IBM ソフトウェア・サポートへの問題の提出』

お客様の問題点のビジネス・インパクトの判別

IBM では、お客様が報告された問題の重大度レベルをお尋ねします。したがって、報告する問題のビジネス・インパクトを理解および評価する必要があります。以下の基準を使用してください。

重大度 1	**クリティカルな**ビジネス・インパクト: プログラムを使用できないため、業務に重大な影響があります。この状態の即時解決が必要です。
重大度 2	**重大な**ビジネス・インパクト: プログラムは使用できますが、極めて限定的です。
重大度 3	**一定の**ビジネス・インパクト: プログラムは重大な機能をほぼすべて使用できる状態で (業務に重大な影響なしに) 使用できます。
重大度 4	**最小限の**ビジネス・インパクト: 問題による業務への影響がほとんどないか、問題に対する適切な次善策が導入されています。

問題点の記述と背景情報の収集

IBM では、問題をできるだけ具体的に記述してくださるようお願いしています。IBM ソフトウェア・サポートのスペシャリストが問題の解決を効率的に支援できるよう、関連するすべての背景情報を含めてください。時間を節約するために、以下の質問への回答をご用意ください。

- 問題発生時に実行されていたソフトウェアのバージョン。
- 問題の症状に関連するログ、トレース、およびメッセージの有無。 IBM ソフトウェア・サポートは、以下の情報の提供をお願いすることがあります。
- 問題の再現可能性。再現可能な場合は、再現させるための手順。
- システムに対する変更の有無。(例えば、ハードウェア、オペレーティング・システム、ネットワーキング・ソフトウェアなど。)
- 問題に対する現時点における次善策の実施有無。実施している場合は、問題の報告時に説明できるようにご準備ください。

IBM ソフトウェア・サポートへの問題の提出

以下のいずれかの方法で問題をサブミットできます。

- **オンライン**: IBM ソフトウェア・サポート・サイト (http://www.ibm.com/software/support/probsub.html) の「Submit and track problems」ページにアクセスします。適切な問題サブミット・ツールに情報を入力します。
- **電話**: お客様の国での連絡先の電話番号を調べるには、IBM Software Support Handbook (http://techsupport.services.ibm.com/guides/contacts.html) の contacts (連絡先) ページにアクセスしてください。お客様の地域名をクリックしてください。

送信した問題が、ソフトウェアの障害に関するものか、資料の欠落や不正確な記述によるものである場合は、IBM ソフトウェア・サポートはプログラム診断依頼書 (APAR) を作成します。APAR には、問題が詳細に記述されます。IBM ソフトウェア・サポートでは、APAR が解決されフィックスが配布されるまでの間、お客様が

実行できる次善策を可能な限り提供します。 IBM は、解決された APAR を IBM 製品サポート Web ページに毎日公開し、同じ問題に遭遇した他のユーザーが同じ解決方法を利用できるようにしています。

問題解決の詳細については、『知識ベースの検索』および『フィックスの入手』を参照してください。

知識ベースの検索

IBM ソフトウェアの使用における問題の早期解決を図ります。まず、使用可能な知識ベースを検索して、問題に対する解決策が既に文書化されているかどうかを判別してください。

ローカル・システムまたはネットワーク上の製品資料の検索

IBM では、ローカル・システム、またはイントラネットのサーバーにインストールできる多数の文書を提供しています。この製品資料の検索機能を使用すると、概念に関する情報、タスクを完了するための説明、参照情報、およびサポート資料を照会できます。

インターネットの検索

以下は英語のみの対応となります。製品資料で問題に対する回答を検索できない場合は、問題解決に役立つ最新の、最も完全な情報をインターネットで検索します。ご使用の製品について複数のインターネット・リソースを検索するには、ナビゲーション・フレームにある製品のフォルダーを左に展開して、「**詳細情報**」を選択してください。次のようなさまざまなリソースを検索できます。

- IBM 技術情報
- IBM ダウンロード
- IBM Redbooks®
- IBM DeveloperWorks
- フォーラムおよびニュースグループ
- Google

フィックスの入手

このタスクについて

以下は英語のみの対応となります。お客様の問題の解決に、プロダクトのフィックスが有効な場合があります。ご使用の IBM ソフトウェア・プロダクトで選択可能なフィックスを判別するには、次のようにして製品サポートの Web サイトを調べてください。

1. IBM Software Support Web サイト (http://www.ibm.com/software/support) にアクセスします。
2. 「**All IBM software (A-Z)**」 をクリックして『Software A to Z』ページを開き、商品名を選択してその製品に固有のサポート・サイトを開きます。

3. 「**Self help**」で「**All Updates**」のリンクに進むと、ご使用の製品に関するフィックスのリスト、フィックスパック、および他のサービスの更新情報を確認することができます。検索対象を絞り込むためのヒントについては、「**Search tips**」をクリックします。
4. フィックスの名前をクリックして説明を読み、必要に応じてそのフィックスをダウンロードします。

フィックスや IBM 製品に関するその他のニュースについての通知を週ごとに E メールで受信するには、以下の手順に従ってください。

1. 任意の IBM プロダクトのサポート・ページで、右上隅にある「**My support** 」をクリックします。
2. 既に登録済みの場合は、スキップして次のステップに進みます。まだ登録がお済みでない場合は、サポート・ページ右上の「Register」をクリックして、ユーザー ID とパスワードを設定します。
3. 「**My support**」にサインインします。
4. 「My support」ページで、左のナビゲーション・ペインにある「**Edit profiles**」をクリックし、「**Select Mail Preferences**」までスクロールします。プロダクト・ファミリーを選択し、必要な情報の種類に対応するボックスにチェック・マークを付けます。
5. **Submit**をクリックします。
6. 他の製品に関する E メール通知をご希望の場合は、ステップ 4 および 5 を繰り返します。

フィックスのタイプの詳細については、「ソフトウェア・サポート・ハンドブック」(http://www-06.ibm.com/software/jp/supportguide/handbook/home.html) を参照してください。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。

国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラット

フォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。お客様は、IBM のアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、 IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年). このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。© Copyright IBM Corp. _年を入れる_. All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

IBM、IBM ロゴおよび ibm.com® は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

Adobe、PostScript は、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

IT Infrastructure Library は英国 Office of Government Commerce の一部である the Central Computer and Telecommunications Agency の登録商標です。

インテル、Intel、Intel ロゴ、Intel Inside、Intel Inside ロゴ、Centrino、Intel Centrino ロゴ、Celeron、Xeon、Intel SpeedStep、Itanium、Pentium は、Intel Corporation または子会社の米国およびその他の国における商標または登録商標です。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

ITIL は英国 The Minister for the Cabinet Office の登録商標および共同体登録商標であって、米国特許商標庁にて登録されています。

UNIX は The Open Group の米国およびその他の国における登録商標です。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

Cell Broadband Engine は、Sony Computer Entertainment, Inc. の米国およびその他の国における商標であり、同社の許諾を受けて使用しています。

Linear Tape-Open、LTO、LTO ロゴ、Ultrium、および Ultrium ロゴは、HP、IBM Corp. および Quantum の米国およびその他の国における商標です。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

[サ行]

[タ行]

[ハ行]

[マ行]

[ラ行]

A

I

J

L

M

N

P

S

W

Z

Printed in Japan

SA88-7241-03

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21