IBM Security Identity Manager
バージョン 6.0

インストール・ガイド

GA88-4860-00
(英文原典：GC14-7695-00)

IBM Security Identity Manager
バージョン 6.0

インストール・ガイド

GA88-4860-00
(英文原典：GC14-7695-00)

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、 315 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。

本書は、IBM Security Identity Manager バージョン 6.0 (製品番号 5724-C34)、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： GC14-7695-00
IBM Security Identity Manager
Version 6.0
Installation Guide

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

表リスト

本書について

「IBM® Security Identity Manager *インストール・ガイド*」では、IBM Security Identity Manager バージョン 6.0 のインストールおよび構成について説明します。また、以下に示すその各種コンポーネントのインストールおよび構成についても説明します。

WebSphere®

データベース・サーバー (IBM DB2®、Oracle、および MS SQL)

ディレクトリー・サーバー (IBM Tivoli® Directory Server および Sun Enterprise Directory Server)

IBM Tivoli Directory Integrator

IBM Security Identity Manager アダプター

資料および用語集へのアクセス

このセクションでは、以下について述べます。

- IBM Security Identity Manager ライブラリーの資料リスト。
- 『オンライン資料』へのリンク。
- x ページの『IBM Terminology Web サイト』へのリンク。

IBM Security Identity Manager ライブラリー

IBM Security Identity Manager ライブラリーには、以下の資料があります。

- *IBM Security Identity Manager Quick Start Guide* (CF3L2ML)
- *IBM Security Identity Manager 製品概要* (GA88-4857)
- *IBM Security Identity Manager シナリオ* (SA88-4858)
- *IBM Security Identity Manager 計画* (GA88-4859)
- *IBM Security Identity Manager インストール・ガイド* (GA88-4860)
- *IBM Security Identity Manager 構成ガイド* (SA88-4862)
- *IBM Security Identity Manager Security Guide* (SC14-7699)
- *IBM Security Identity Manager 管理ガイド* (SA88-4863)
- *IBM Security Identity Manager トラブル・シューティング・ガイド* (GA88-4864)
- *IBM Security Identity Manager Error メッセージ・リファレンス* (GA88-4865)
- *IBM Security Identity Manager リファレンス・ガイド* (SA88-4866)
- *IBM Security Identity Manager Database and Schema リファレンス・ガイド* (SA88-4867)
- *IBM Security Identity Manager Glossary* (SC14-7397)

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 Identity Manager インフォメーション・センター
このサイト (http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0/ic-homepage.htm) には、この製品のインフォメーション・センターのウェルカム・ページが表示されます。

IBM Security インフォメーション・センター
このサイト (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp)には、すべての IBM Security 製品資料のアルファベット順リストと一般情報が掲載されています。

IBM Publications Center
このサイト (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。

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 つのロケーションに統合したものです。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出力してナビゲートする支援技術を利用できます。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。

詳しくは、「*IBM Security Identity Manager リファレンス・ガイド*」のトピック『IBM Security Identity Manager のアクセシビリティー機能』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、IBM Education Web サイト (http://www.ibm.com/software/tivoli/education) を参照してください。

サポート情報

IBM サポートは、コード関連の問題、およびインストールまたは使用方法に関する短時間の定型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 から直接アクセスできます。

「*IBM Security Identity Manager トラブル・シューティング・ガイド*」では、以下に関する詳細が説明されています。

- IBM サポートに連絡する前に収集する情報。
- IBM サポートに連絡する際の各種の方法。
- IBM Support Assistant の使用方法。

- 問題を自分自身で切り分けて修正するための指示および問題判別リソース。

注: 製品のインフォメーション・センターの「**コミュニティーおよびサポート**」タブには、その他のサポート・リソースが用意されています。

第 1 部 インストール

IBM Security Identity Manager をインストールするには、このパートの指示に従ってください。

第 1 章 IBM Security Identity Manager コンポーネント

この章では、IBM Security Identity Manager 用にインストールして構成する必要のあるコンポーネントの概要を説明します。

サポートされるリリース・レベル、およびフィックスパックの指定を確認するには、IBM Security Identity Manager インフォメーション・センターの『ソフトウェア*前提条件*』を参照してください。オペレーティング・システムとコンポーネントに関する指定が提供されています。

IBM Security Identity Manager では、通信用のアダプターを使用して、リモート・リソース上のユーザー・アカウントのライフサイクルを管理できます。

IBM Security Identity Manager 製品は、以下を実行します。

- IBM Security Identity Manager アダプターが接続されている 1 つ以上のリソース上で、許可されるユーザーにユーザー・アカウントを提供します。
- WebSphere Application Server 環境 (単一サーバー構成またはクラスター構成のいずれか) で実行されます。
- データベース・サーバーにヒストリカル・データおよびペンディング・データを保管します。
- LDAP ディレクトリー・サーバーにユーザー・アカウントおよび組織データを保管します。
- 監査およびレポート作成用の IBM Security Identity Manager 情報をデータベースに保管します。
- Web ブラウザーのクライアント・インターフェースから管理を行います。このインターフェースは、HTTP サーバーおよび WebSphere Web サーバー・プラグイン、または WebSphere Application Server 内蔵 HTTP トランスポート経由で通信を行います。

IBM Security Identity Manager では、次のセクションで説明するコンポーネントをインストールして構成する必要があります。

データベース・サーバー製品

IBM Security Identity Manager は、データベース・サーバーにトランザクション・データおよびヒストリカル・データを保管します。例えば、IBM Security Identity Manager プロビジョニング・プロセスは、リレーショナル・データベースを使用して、現在の状況およびそのヒストリーを保守します。

データベースと通信するコンピューターは、Java™ Database Connectivity ドライバー (JDBC ドライバー) を必要とします。例えば、JDBC ドライバーを使用すると、IBM Security Identity Manager サーバーはデータ・ソースと通信可能になります。IBM Security Identity Manager は、Java ベースのアプリケーションからデータベースへの接続に JDBC タイプ 4 ドライバーをサポートします。

サポートされるデータベース製品は、IBM DB2、Oracle データベース、および MS SQL Server データベースです。

サポートされるデータベース・サーバー製品について詳しくは、IBM Security Identity Manager インフォメーション・センターの『データベース・サーバー要件』を参照してください。

ディレクトリー・サーバー製品

IBM Security Identity Manager は、管理対象の ID の現在の状態を LDAP ディレクトリーに保管します。これには、ユーザー・アカウントおよび組織データも含まれます。

IBM Security Identity Manager は、以下の製品をサポートします。

- IBM Tivoli Directory Server
- Oracle Directory Server Enterprise Edition

サポートされるディレクトリー・サーバー製品について詳しくは、IBM Security Identity Manager インフォメーション・センターの『ディレクトリー・サーバーの要件』を参照してください。

IBM Tivoli Directory Integrator

IBM Tivoli Directory Integrator は、異なるディレクトリー、データベース、およびアプリケーション内の ID データを同期化する、オプションのインストール・コンポーネントです。

IBM Tivoli Directory Integrator は、アプリケーション間またはディレクトリー・ソース間の情報交換を同期化および管理します。

IBM Tivoli Directory Integrator について詳しくは、IBM Security Identity Manager インフォメーション・センターの『*Directory Integrator 要件*』を参照してください。

WebSphere Application Server

WebSphere Application Server は、IBM Security Identity Manager 環境の主要なコンポーネントです。WebSphere Application Server は、エンタープライズ・アプリケーション・コードのランタイム環境を提供して、Java 仮想マシンを実行します。

アプリケーション・サーバーにより、特定の Java アプリケーション・コンポーネントの実行を専門に扱うコンテナーが提供されます。

HTTP サーバーおよび WebSphere Web サーバー・プラグイン

HTTP サーバーは、Web ブラウザーのクライアント・インターフェースを介した IBM Security Identity Manager の管理を可能にするオプションのコンポーネントです。

IBM Security Identity Manager では、HTTP サーバーとともに WebSphere Web サーバー・プラグインをインストールする必要があります。WebSphere Application Server は、IBM HTTP Server および WebSphere Web サーバー・プラグインをインストールするための別のインストーラーを提供しています。これらのコンポーネントは、WebSphere Application Server とともにインストールすることも、別のコンピューターにインストールすることもできます。

注: HTTP サーバーを使用する場合、IBM Security Identity Manager アプリケーションを HTTP Web サーバー名にマップする必要があります。WebSphere Application Server 管理コンソールを使用して、マップします。アプリケーションのマッピングについて詳しくは、 139 ページの『IBM Security Identity Manager アプリケーションのマッピング』 を参照してください。

IBM Security Identity Manager サーバー

IBM Security Identity Manager サーバーとそのアダプターは、ID を一連の異機種のリソースにプロビジョンします。

これらのリソースとしては、オペレーティング・システム、データ・ストア、その他のアプリケーションなどがあります。

IBM Security Identity Manager アダプター

IBM Security Identity Manager アダプターにより、IBM Security Identity Manager サーバーは、一連の異機種のリソースに接続できます。 ID をプロビジョンできるのは、オペレーティング・システムやデータ・ストア、その他のアプリケーションなどのリソースです。

第 2 章 デプロイメントのためのインストール計画

初期のデプロイメント問題を回避するために、サイトに応じて以下の計画アクティビティーのバリエーションを用意することを検討してください。 IBM Security Identity Manager および後続のフィックスパックをインストールする前に計画を立ててください。

- ミドルウェアをインストールするスペシャリストのすべてに IBM Security Identity Manager の包括的な関連情報を提供する作業方法を確立する。例えば、チームが定期的に会議を開き、問題を出し合って解決策を共有するなど。
- 調整を確実に行うために、1 名の担当者を企業のフォーカル・ポイント (サイトと IBM お客様サポート・スペシャリストとの間の橋渡しを担当する) として指定する。
- 可能であれば、アプリケーションをインストールおよび構成するスペシャリストの数を削減する。以下のようにして、スペシャリスト間のコミュニケーション・フローを増やします。
  - FTP サーバーおよび Web サイトの包括的なライブラリーまたはリストを、前提条件となるインストールおよび構成情報に対して提供する。
  - IBM Security Identity Manager をインストールするスペシャリストが、ミドルウェア・サーバー上で前提条件のミドルウェアに対する root 権限またはアドミニストレーター権限を持つことを確認する。
  - システムまたは解決方法のすべての要素がアカウントを提供するために十分な特権を持っていることを確認する。
  - トラブルシューティングのアクションを識別し、集中的な問題および解決方法のデータベースをサポートして、アクションの所有者を割り当てる。
  - 開始プロセスを自動化するスクリプトの共通ライブラリーを保守する。
  - すべてのカスタマイズ・アクティビティーを調整する変更コントロール・データベースを作成する。
  - この資料で提供するものに類似の、スペシャリストが重要な構成パラメーターの値の記録を提供する作業方法を決定する。すべてのスペシャリストが、情報の集中化を行う共通ワークシートにアクセス権を持ち、使用できるようにします。

    例えば、このマニュアルの各インストールの章では、インストールを開始する前にインストール、構成、および実行する必要のある前提条件のチェックリストを提供しています。また、 150 ページの『ディレクトリー・サーバーのセキュリティー構成』では、ユーザー ID、パスワード、およびセキュリティー設定などの重要な値の集中収集ポイントを提供しています。前提条件のレベルおよびフィックスパックまたはパッチについて詳しくは、IBM Security Identity Manager インフォメーション・センターの『ソフトウェア*前提条件*』を参照してください。

WebSphere セキュリティー構成

IBM Security Identity Manager では、WebSphere Application Server 管理セキュリティーおよびアプリケーション・セキュリティーを有効にする必要があります。

管理セキュリティー

WebSphere Application Server のデフォルトのインストール済み環境では、管理セキュリティーがグローバル・セキュリティーの一部として構成されています。新しい WebSphere サーバーをインストールする場合は、デフォルト設定を受け入れて、管理セキュリティーを有効にします。管理セキュリティーがオフになっている既存の WebSphere Application Server を使用する予定の場合は、IBM Security Identity Manager をインストールする前に、管理セキュリティーを有効にする必要があります。 IBM Security Identity Manager インストール・プログラムは、管理セキュリティーがオンであるかどうかを検証します。

アプリケーション・セキュリティー

IBM Security Identity Manager がデプロイされるアプリケーション・サーバーでは、アプリケーション・セキュリティーをオンにする必要があります。 IBM Security Identity Manager をホストするアプリケーション・サーバーのアプリケーション・セキュリティーを有効にするには、セキュリティー・ドメインを構成したかどうかに応じて、さまざまな方法があります。

IBM Security Identity Manager 用にセキュリティー・ドメインが構成されていない場合は、グローバル・セキュリティーのアプリケーション・セキュリティーをオンにする必要があります。

IBM Security Identity Manager 用にセキュリティー・ドメインが構成されている 場合は、以下のようになります。

- グローバル・セキュリティーのアプリケーション・セキュリティー設定がオフ の場合は、セキュリティー・ドメインのアプリケーション・セキュリティーをオンにする必要があります。
- グローバル・セキュリティーのアプリケーション・セキュリティー設定がオン の場合は、グローバル・セキュリティーからアプリケーション・セキュリティー設定を使用できます。必要な場合は、セキュリティー・ドメインのアプリケーション・セキュリティーをオンにすることもできます。

Java 2 セキュリティー

IBM Security Identity Manager は、IBM Security Identity Manager セキュリティー・ドメインを構成するインストーラーを備えています。このインストーラーでは、WebSphere グローバル・セキュリティー設定で Java 2 セキュリティーを無効にすることが必要です。他の要件を満たすために Java 2 セキュリティーを有効にする必要がある場合は、`server.policy` ファイルを変更し、IBM Security Identity Manager JAR ファイルの許可を `WAS_PROFILE_HOME/classes` に付与する必要があります。

許可を付与するには、単一サーバー、またはクラスター・セットアップ・ノード上で `WAS_PROFILE_HOME/properties/server.policy` を開き、次のステートメントを追加します。

```
grant codeBase "file:${user.install.root}/classes/-" {
      permission java.security.AllPermission;
    };
```

注: IBM Security Identity Manager のインストールが完了したら、server.policy ファイルに対する変更を除去する必要があります。

カスタム・レジストリー

IBM Security Identity Manager は、デフォルトのカスタム・レジストリー を備えています。このレジストリーを認証に使用する必要はありません。*外部レジストリー*を使用することを選択できます。外部ユーザー・レジストリーとは、WebSphere Application Server と共に構成できる他の任意のレジストリーです。既存のレジストリーを使用することも、新規のレジストリーを構成することもできます。

IBM Security Identity Manager インストール・プログラムは、カスタム・レジストリーを使用するかどうかを尋ねるプロンプトを表示します。

- カスタム・レジストリーを使用する場合、IBM Security Identity Manager インストール・プログラムは、プログラマチックにセキュリティー・ドメインを作成し、アプリケーション・セキュリティーを有効にして、それを IBM Security Identity Manager カスタム・レジストリーに対して構成します。
- 外部レジストリーを使用する場合は、アプリケーション・セキュリティーを手動で構成する必要があります。このインストール・ガイドでは、構成を完了する方法について説明します。外部レジストリーを使用する場合は、以下の作業を行います。
  1. IBM Security Identity Manager をインストールする前に、 69 ページの『外部ユーザー・レジストリーを使用した認証のためのインストール前の構成』に記載されている手順を完了します。
  2. IBM Security Identity Manager のインストール時に、カスタム・レジストリーを使用しない ことを選択します。
  3. IBM Security Identity Manager をインストールした後、 166 ページの『認証用の外部ユーザー・レジストリーに対するインストール後の構成』に記載されている手順を完了します。

構成オプション

IBM Security Identity Manager は、単一サーバー環境とクラスター環境のどちらでも構成することが可能です。

IBM Security Identity Manager をインストールする前に、単一サーバー構成またはクラスター構成で WebSphere Application Server を構成する方法を決定する必要があります。

単一サーバー構成

単一サーバー構成では、WebSphere Application Server ベース・サーバーと IBM Security Identity Manager が 1 つのコンピューター上に含まれます。その他の必要なアプリケーションは、同じコンピューター上でも別のコンピューター上でも実行できます。コンピューターに、ワークロードに応じた必要なメモリー、速度、および使用可能ディスク・スペースがあることを確認してください。

単一サーバー構成では、以下のコンポーネントおよび製品を必要とします。

- データベース・サーバー
- ディレクトリー・サーバー
- IBM Tivoli Directory Integrator (オプション)
- WebSphere Application Server Base サーバー
- IBM Security Identity Manager サーバー
- IBM Security Identity Manager アダプター

クラスター構成

クラスター構成には、コンピューター上の 1 つ以上のアプリケーション・サーバーの論理グループである WebSphere Application Server のプロファイルが含まれます。プロファイルはセルと呼ばれる管理可能ドメイン内にあり、セルはデプロイメント・マネージャーが管理します。プロファイル・エージェントは、デプロイメント・マネージャーと通信することでプロファイル上のすべての管理対象プロセスを管理し、構成を調整および同期化します。デプロイメント・マネージャーは、セルのすべてのエレメントに集中管理ビューとコントロール (クラスターの管理を含む) を提供する管理プロセスです。

IBM Security Identity Manager では、各クラスター・メンバーのオペレーティング・システムが同じであると想定します。

例えば、IBM Security Identity Manager クラスター・メンバーは、IBM AIX® オペレーティング・システム上で稼働します。ID フィードの問題を避けるために、IBM Security Identity Manager のクラスター内では複数タイプのオペレーティング・システムを使用しないでください。

IBM Security Identity Manager は、各クラスター・ノードが 1 つ以上のアプリケーション・サーバーをホストする、水平クラスター構成と垂直クラスター構成の両方をサポートします。各ノードは、1 つのコンピューターから構成され、別個のサーバー上のデプロイメント・マネージャーで制御されます。残りのアプリケーションは、追加のコンピューターに構成されます。

例

以下に、クラスター構成の例を示します。

- デプロイメント・マネージャーをインストールするコンピューター上で、以下のコンポーネントおよび製品をインストールします。
  - WebSphere Application Server デプロイメント・マネージャー
  - 必要な場合、JDBC ドライバー
  - IBM Security Identity Manager サーバー
- クラスター・メンバーは、WebSphere Application Server クラスターの 1 つのインスタンスです。各 クラスター・メンバーで、以下のコンポーネントおよび製品をインストールします。
  - WebSphere Application Server Base サーバー
  - IBM Security Identity Manager サーバー
  - 必要な場合、JDBC ドライバー

- 1 台以上の追加コンピューター (クラスター内でもクラスター外でもよい) で、以下のコンポーネントおよび製品をインストールします。
  - データベース・サーバー
  - ディレクトリー・サーバー
  - IBM Tivoli Directory Integrator (オプション)
  - IBM HTTP Server および WebSphere Application Server プラグイン (オプション)

これは単なる構成例です。接続形態では、すべてクラスター内にあるコンピューター上にこれらのコンポーネントを構成する可能性があります。デプロイメント・マネージャーは、WebSphere Application Server ベース・サーバーと同じコンピューターにインストールできます。コンピューターに、追加の負荷に対応できる必要なメモリー、速度、および使用可能スペースがあることを確認してください。

第 3 章 インストールの準備

インストール・プロセスには、IBM Security Identity Manager の各コンポーネントを連続してインストールおよび構成する作業が含まれます。 IBM Security Identity Manager サーバーをインストールする前に、前提コンポーネントが既にインストールおよび構成されている必要があります。

IBM Security Identity Manager サーバーには、以下のコンポーネントが必要です。

- データベース
- ディレクトリー・サーバー
- Tivoli Directory Integrator (オプション)
- WebSphere Application Server

次のセクションの手順に従って、インストール要件がすべて満たされていることを確認します。

プリインストール・ロードマップ

プリインストールは、IBM Security Identity Manager のインストールに必要なコンポーネントをインストールおよび構成する一連のアクティビティーから構成されます。

IBM Security Identity Manager のプリインストールおよびテストのための主要なタスクを以下に示します。

1. IBM Security Identity Manager サーバーのトポロジーを決定します。本章の情報では、主な構成の選択について説明します。
2. 各物理サーバーのオペレーティング・システムが、IBM Security Identity Manager が必要とするレベルにあることを確認します。ソフトウェア要件とハードウェア要件について詳しくは、IBM Security Identity Manager インフォメーション・センターの『*ハードウェア要件およびソフトウェア要件*』を参照してください。
3. データベース・サーバーがインストール済みであり、事前構成されていることを確認します。データベースを準備するステップについては、 18 ページの『データベースのインストールと構成』を参照してください。
4. ディレクトリー・サーバーがインストール済みであり、事前構成されていることを確認します。ディレクトリー・サーバーを準備するステップについては、 43 ページの『ディレクトリー・サーバーのインストールおよび構成』を参照してください。
5. IBM Tivoli Directory Integrator を使用することを決定した場合は、それがインストールおよび事前構成されていることを確認します。IBM Tivoli Directory Integrator を準備するステップについては、 54 ページの『IBM Tivoli Directory Integrator のインストール (オプション)』を参照してください。

6. WebSphere Application Server の準備が整っていることを確認します。単一クラスター構成またはクラスター構成で WebSphere Application Server を準備するステップについては、 58 ページの『WebSphere Application Server のインストールおよび構成』を参照してください。

IBM Security Identity Manager のダウンロード

IBM Security Identity Manager は IBM パスポート・アドバンテージからダウンロードできます。

始める前に

IBM パスポート・アドバンテージのお客様番号およびパスワードを持っていることを確認してください。

このタスクについて

以下の IBM Security Identity Manager ダウンロード・ページに移動します。

http://www.ibm.com/support/docview.wss?uid=swg24023254

手順

1. ご使用のオペレーティング・システムのタブをクリックします。
2. パッケージを確認した後で、「Download package」という表までスクロールダウンします。
3. ダウンロード・オプションをクリックします。 これで、IBM Passport Advantage ページに移動します。
4. ログインして、指示に従ってください。

次のタスク

前提条件のコンポーネントをインストールして構成します。

フィックスパックの入手

フィックスパックは、IBM Security Identity Manager サポート Web サイトからダウンロードできます。

IBM Security Identity Manager フィックス、およびフィックスパックのインストールに関する情報は、Web サイト『ダウンロード』で入手できます。

フィックスパックをインストールする前の SOAP タイムアウト間隔の設定

フィックスパックのインストールには、タイムアウト例外の発生を防ぐために十分な時間間隔が必要です。

始める前に

フィックスパックのインストール中にタイムアウト例外エラーが発生するのを防ぐために、各フィックスパックのインストールの前に、SOAP タイムアウト間隔を少なくとも 15 分 (900 秒) に設定します。

手順

1. soap.client.props ファイルを編集します。 このファイルは、*WAS_HOME*¥profiles¥*profile_name*¥properties ディレクトリーにあります。
2. com.ibm.SOAP.requestTimeout プロパティーを 900 に設定します。 例えば、次のように設定します。

   ```
   com.ibm.SOAP.requestTimeout=900
   ```

3. 変更をファイルに保存します。

次のタスク

フィックスパックをインストールします (該当する場合)。

第 4 章 前提コンポーネントのインストール

この章では、IBM Security Identity Manager サーバーをインストールする前に前提コンポーネントをインストールして構成する手順について説明します。

Red Hat Linux サーバーの構成

Red Hat Linux Enterprise 6.0 上にインストールする場合は、IBM Security Identity Manager をインストールする前に構成タスクを完了する必要があります。

このタスクについて

IBM Security Identity Manager をインストールする前に、必ず Security Enhanced Linux (SEL) を無効にしてください。SEL のデフォルト・ポリシー制約により、インストーラーが失敗する場合があります。また、適切な Linux パッケージがインストールされていることを確認してください。

手順

1. Security Enhanced Linux がインストールされており、制約モードで実行されているかどうかを確認するには、**sestatus** コマンドを実行するか、/etc/sysconfig/selinux ファイルを確認します。SEL を無効にするには、以下のいずれかのアクションを実行します。
   - SEL を許容モードに設定し、スーパーユーザーとして **setenforce 0** コマンドを実行します。
   - /etc/sysconfig/selinux ファイルを変更し、コンピューターをリブートします。
2. 以下の各パッケージについて **rpm -qa | grep** *package_name* コマンドを実行し、これらがインストールされているかどうか確認します。

   注: IBM Security Identity Manager とその前提条件ミドルウェアを正常にインストールするためには、以下のパッケージがシステム上に存在する必要があります。

   compat-libstdc++-33-3.2.3-69

   compat-db-4.6.21-15

   libXp-1.0.0-15.1

   libXmu-1.0.5-1

   libXtst-1.0.99.2-3

   pam-1.1.1-4

   libXft-2.1.13-4.1

   gtk2-2.18.9-4

   gtk2-engines-2.18.4-5

   Red Hat Linux Enterprise 5.0 上にインストールする場合は、以下の各パッケージについて **rpm -qa | grep***package_name* コマンドを実行し、これらがインストールされているかどうか確認します。 32 ビット・アプリケーションと 64 ビッ

ト・アプリケーションの両方をサポートするプラットフォームでは、以下のパッケージの 32 ビット版と 64 ビット版の両方が必要です。

compat-libstdc++-33-3.2.3-61

compat-db-4.2.52-5.1

libXp-1.0.0-8

libXmu-1.0.2-5

libXtst-1.0.1-3.1

pam-0.99.6.2-3.26.el5

libXft-2.1.10-1.1

Red Hat Linux Enterprise 5.0 について詳しくは、WebSphere Application Server バージョン 7.0 インフォメーション・センターの『*Linux システムのインストール準備*』を参照してください。

データベースのインストールと構成

IBM Security Identity Manager は、スケジュールや監査データを含むトランザクション・データおよびヒストリカル・データをデータベースに保管します。 IBM Security Identity Manager サーバーをインストールする前に、データベースをインストールして構成する必要があります。

以下のいずれかのデータベースをインストールして構成することを選択できます。

- IBM DB2 データベース
- Oracle データベース
- Microsoft SQL Server 2008

サポートされるデータベース・リリース、および必要なフィックスパックについて詳しくは、IBM Security Identity Manager インフォメーション・センターの『*製品概要*』に記載されている『*データベース・サーバー要件*』を参照してください。

このセクションの情報は、データベース製品によって提供される、より広範囲な前提条件の資料に代わるものではありません。データベースについて詳しくは、製品関連の Web サイトから以下のソースを参照してください。

- IBM DB2 データベース
- Oracle データベース
- Microsoft SQL Server 2008

ワークシート

このワークシートには、データベースのインストールと構成に必要な一般的な情報が示されています。インストールするデータベースに応じて、追加の情報が必要になる場合があります。

表 1. 一般的なデータベース・ワークシート

フィールド名	説明	デフォルトまたは例の値	ご使用の値
Host name (ホスト名)	データベースをホストするコンピューターの名前。		
ポート番号	データベース・サービス Listen ポート。	例: 50000、50002、または 60000	
データベース名	IBM Security Identity Manager データベースの名前。	例: **itimdb**	
管理者 ID	データベース管理者ユーザー ID。	例: **db2admin** **注:** ミドルウェア構成ユーティリティーを使用しない場合、この値は UNIX システムではデフォルトで *db2inst1* です。	
Admin password (管理者パスワード)	データベース管理者ユーザー ID のパスワード。		
Database user ID (データベース・ユーザー ID)	データベースへのログオンで IBM Security Identity Manager が使用するアカウント。	例: **itimuser**	
Database password (データベース・パスワード)	**itimuser** ユーザー ID のパスワード。		

データベース製品をインストールする前に

データベース製品をインストールする前に、以下を実行する必要があります。

- データベース製品により提供されるインストール情報を読むこと。
- 環境がハードウェアおよびソフトウェア要件に適合していることの確認。
- 必要なオペレーティング・システムのパッチがすべて適用されていることの検証。
- Solaris および Linux オペレーティング・システムなどの一部のオペレーティング・システムに対してカーネル設定が適正であることの確認。それぞれのデータベース・アプリケーションは、追加のオペレーティング・システムの値など独自の要件を指定します。アプリケーションのインストールの前に、これらの追加の設定の資料をお読みください。例えば、DB2 で必要なカーネルの設定については、IBM Web サイトを参照してください。
  - AIX

    必要ありません。
  - Solaris
  - Linux (Red Hat および SUSE)
  - Windows

必要ありません。

IBM DB2 データベースのインストールおよび構成

ここでは、IBM DB2 Universal Database™ (DB2) のインストールと構成について説明します。このセクションの構成ステップでは、後で IBM Security Identity Manager サーバーのインストール・プログラムが使用するデータベースを作成します。インストール・プログラムによって、データベースにデータ・オブジェクトが追加されます。

DB2 は、IBM Security Identity Manager と同じコンピューターにインストールすることも、別のコンピューターにインストールもできます。DB2 を同じコンピューターにインストールするためには、Java Database Connectivity ドライバー (JDBC ドライバー、タイプ 4) のインストールが必要です。 JDBC ドライバーによって、IBM Security Identity Manager は、データ・ソースと通信できるようになります。DB2 をインストールすると、タイプ 4 JDBC ドライバーが自動的にインストールされます。

DB2 インストール

IBM Security Identity Manager では、必要なレベルの DB2 フィックスパックを適用して DB2 を実行する必要があります。 DB2 およびフィックスパックのインストールについて詳しくは、IBM Security Identity Manager インフォメーション・センターを参照し、データベース製品で提供される資料を調べてください。

ユーザー・データ

DB2 のインストールでは、DB2 管理者のユーザー ID およびパスワードなど、いくつかのシステム・データを指定する必要があります。インストール・ウィザードでは、状況報告および初期確認アクティビティーが提供されます。

UNIX システムおよび Linux システムにおけるユーザー名およびパスワード

次の表は、UNIX システムおよび Linux システム上に作成されるデフォルト値を示します。この情報を記録してください。この情報は、IBM Security Identity Manager が使用する DB2 データベースの構成に必要です。ミドルウェア構成ユーティリティーを使用して DB2 インスタンスを作成しない場合は、DB2 のインストールでデフォルトの DB2 インスタンスを作成できます。

表 2. UNIX システムおよび Linux システム上の DB2 データベース標準構成パラメーター。

UNIX および Linux システム	**説明**	**値**
DB2 管理者ユーザー ID およびインスタンス名	DB2 管理者およびインスタンス所有者として DB2 に接続するために使用するユーザー ID。	`db2admin` **注:** ミドルウェア構成ユーティリティーを使用しない場合、この値はデフォルトで `db2inst1` です。
DB2 インスタンスのパスワード	管理者ユーザー ID のパスワード。	ユーザー定義の値。

表 2. UNIX システムおよび Linux システム上の DB2 データベース標準構成パラメーター。(続き)

UNIX および Linux システム	説明	値
DB2 インスタンスのホーム・ディレクトリー	DB2 管理者およびインスタンス所有者のホーム・ディレクトリー。	• AIX: /home/db2admin • Linux: /home/db2admin • Linux for System p®: /home/db2admin • Linux for System z®: /home/db2admin • Solaris: /export/home/db2admin

Windows システムにおけるユーザー名およびパスワード

次の表は、Windows システム上に作成されるデフォルト値を示します。ミドルウェア構成ユーティリティーを使用して DB2 インスタンスを作成しない場合は、DB2 のインストールでもデフォルトの DB2 インスタンスを作成できます。ミドルウェア構成ユーティリティーの使用法について詳しくは、23 ページの『ミドルウェア構成ユーティリティーの実行』を参照してください。

表 3. Windows システム上の DB2 データベース標準構成パラメーター。

Windows システム	説明	値
DB2 インスタンス名	DB2 インスタンスの名前。	db2admin **注:** DB2 のデフォルトは、DB2 のインスタンス値です。
管理ユーザー ID	DB2 管理者およびインスタンス所有者として DB2 に接続するために使用するユーザー ID。	db2admin
パスワード	管理者ユーザー ID のパスワード。	ユーザー定義の値。
DB2 インスタンスのホーム・ディレクトリー	DB2 管理者およびインスタンス所有者のホーム・ディレクトリー。	*ドライブ* 例えば、C: です。

必要なフィックスパックのインストール

DB2 のバージョンによっては、フィックスパックが必要なものがあります。フィックスパックが必要であるかどうかを確認し、必要な場合は DB2 サポート Web サイトから入手してください。

DB2 のフィックスパックをインストールするコマンドは、オペレーティング・システムによっても、インストール時にインスタンスを作成したかどうかによっても異なります。

インストール時に DB2 インスタンスを作成したか	Windows オペレーティング・システム	UNIX および Linux オペレーティング・システム

はい	DB2 コマンド・ウィンドウで、**db2level** コマンドを入力します。
	`db2level`
		DB2 インスタンスのユーザー ID を指定してログオンし、**db2level** コマンドを入力します。
		`su - DB2_instance_ID`
		`db2level`

いいえ	regedit コマンドを実行して、`HKEY_LOCAL_MACHINE¥SOFTWARE¥IBM¥DB2¥InstalledCopies¥ db2_name¥CurrentVersion` 内の情報を探します。	db2ls コマンドを入力します。
		`DB_HOME/install/db2ls`
		または
		`/usr/local/bin/db2ls`

詳しくは、IBM Security Identity Manager インフォメーション・センターの『データベース・サーバー要件』、および DB2 フィックスパックで提供される資料を参照してください。

DB2 インストールを検証してください。

インストール済み環境の検査

インストールが完了すると、インストール・ウィザードにより状況報告が提供されます。さらに、DB2 ファースト・ステップ操作を実行して、インストールが成功したことを検証します。

始める前に

DB2 のインストールの検証について詳しくは、以下の Web サイトにアクセスしてください。http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp?topic=/com.ibm.db2.udb.uprun.doc/doc/t0006838.htm

手順

1. DB2 ファースト・ステップ操作を実行するには、まず、ご使用のオペレーティング・システムを選択します。
   - UNIX または Linux オペレーティング・システム
   - Windows オペレーティング・システム
2. オペレーション・システムに応じて、以下のステップを実行します。
   - UNIX または Linux オペレーティング・システムの場合:

     コマンド *DB_INSTANCE_HOME*/sqllib/bin/db2fs を入力します。
   - Windows オペレーティング・システムの場合:

     「**スタート**」 > 「**すべてのプログラム**」 > 「**IBM DB2**」 > ***DB2 コピー名*** > 「**セットアップ・ツール**」 > 「**ファースト・ステップ**」をクリックします。

IBM DB2 データベース構成

IBM Security Identity Manager インストール製品には、データベース・インスタンスとユーザー ID を作成する、ミドルウェア構成ユーティリティーが含まれています。このユーティリティーでは、DB2 および IBM Tivoli Directory Server のパラメーターを構成することもできます。

標準パラメーターの多くと、すべての拡張パラメーターに、デフォルト値が提供されています。入力されたパラメーター (DB2 インスタンス ID など) が存在する場合は、ミドルウェア構成ユーティリティーは作成タスクをスキップします。これらの値をそのまま使用するか、独自の値を入力するかを選択することができます。必須フィールドは、アスタリスク (*) でマークされています。所望のパネルに達するまで「**戻る**」をクリックして、デプロイメント・ウィザードの任意のパネルに戻ることができます。

ミドルウェア構成ユーティリティーは、以下を実行します。

- 必要な場合、ユーザー ID の作成
- 必要な場合、DB2 インスタンスの作成
- 必要な場合、データベースの作成
- DB2 の調整 (バッファー・プール、ログ調整)
- DB2 設定値の構成 (DB2ENVLIST=EXTSHM、DB2COMM=tcpip)

ミドルウェア構成ユーティリティーは、手動でもサイレント・モードでも実行できます。サイレント・モードでの構成について詳しくは、26 ページの『DB2 のサイレント構成』を参照してください。

注: ミドルウェア構成ユーティリティーは、デフォルトで、システム一時ディレクトリー (例えば `/tmp` ディレクトリー) にある `db2ldap.rsp` という応答ファイルに指定した入力をすべて保管します。このファイルは、通常はユーティリティー完了後にクリーンアップされます。ユーティリティーが完了する前にキャンセルすると、このファイルが消去されない場合があります。

ミドルウェア構成ユーティリティーの実行:

ミドルウェア構成ユーティリティーを実行して、後で IBM Security Identity Manager デプロイメントで使用する DB2 パラメーターを設定できます。

始める前に

Windows オペレーティング・システムの場合は、管理者であるか、管理者権限を持っている必要があります。

UNIX および Linux オペレーティング・システムの場合は、root ユーザーである必要があります。また、umask 設定が 022 であることが必要です。umask 設定を確認するためにコマンド **umask** を発行し、umask 値を 022 に設定します。

```
umask 022
```

注: 後で IBM Security Identity Manager サーバーのインストール時に DBConfig および ldapConfig ユーティリティーで使用できるように、ミドルウェア構成ユーティリティーで指定する値を記録してください。

以下と共に Tivoli Identity Manager バージョン 5.1 の新規インストールを行う準備ができたら、ミドルウェア構成ユーティリティーを実行する前に、IBM サポートに連絡して支援を受けてください。

- 現在サポートされている IBM DB2 バージョン 9.7
- および IBM Tivoli Directory Server バージョン 6.3

連絡先情報:

- Tivoli ソフトウェア・サポート
- 地域の連絡窓口

手順

1. DB2 がインストールされているコンピューター上にシステム管理特権を持つアカウントにログオンします。
2. 日本語、韓国語、中国語 (簡体字)、または中国語 (繁体字) の AIX にインストールする場合は、以下の手順を実行してください。

   注: これらの言語のいずれの AIX にもインストールしない場合は、以下の作業をスキップして、次のステップに進んでください。

   a. ミドルウェア構成ユーティリティーの圧縮ファイルから、`cfg_itim_mw.jar` ファイルを見つけます。ミドルウェア構成ユーティリティーの圧縮ファイルは、製品 DVD またはダウンロード・ディレクトリーにあります。

   b. コマンド `java -jar cfg_itim_mw.jar` を実行します。

   このコマンドは、ミドルウェア構成ユーティリティー用のグラフィカル・ユーザー・インターフェースが、ミドルウェアの構成中に構成パネルを正しく表示するように構成します。ミドルウェア構成ユーティリティーを開始する前にこのコマンドを実行しないと、言語選択パネルで表示上の問題が発生します。
3. DVD のベース・ディレクトリーまたはダウンロード・ディレクトリーで、ミドルウェア構成ユーティリティーを開始します。
   - **AIX オペレーティング・システム**: cfg_itim_mw_aix プログラムを実行してミドルウェア構成ユーティリティーを開始します。
   - **Solaris オペレーティング・システム**: cfg_itim_mw_solaris プログラムを実行してミドルウェア構成ユーティリティーを開始します。
   - **Linux for xSeries® オペレーティング・システム**: cfg_itim_mw_xLinux プログラムを実行してミドルウェア構成ユーティリティーを開始します。
   - **Linux for pSeries® オペレーティング・システム**: cfg_itim_mw_pLinux プログラムを実行してミドルウェア構成ユーティリティーを開始します。
   - **Linux for zSeries® オペレーティング・システム**: cfg_itim_mw_zLinux プログラムを実行してミドルウェア構成ユーティリティーを開始します。
   - **Windows オペレーティング・システム:** Windows の自動実行機能が使用不可の場合は、cfg_itim_mw.exe プログラムを使用してミドルウェア構成ユーティリティーを開始します。

   ネイティブ・プログラムとともに実行するために、各プラットフォームは `cfg_itim_mw.jar` というファイルを必要とします。JAR ファイルとネイティブ・プログラムは、同じディレクトリー位置にある必要があります。

4. 言語を選択し、「**OK**」をクリックします。
5. 「製品の構成」パネルで、「**IBM DB2 Universal Database の構成**」のみにチェック・マークを付け、「**次へ**」をクリックします。 DB2 が正しいレベルでない場合、またはインストールされていない場合は、警告を受け取る可能性があります。DB2 が正しいレベルであることを確認する必要があります。この警告をバイパスするには、「**次へ**」をクリックします。
6. 「**IBM DB2 データベース構成オプション**」パネルで以下の情報を入力し、「**次へ**」 をクリックします。
   - DB2 管理者 ID またはインスタンス名

     DB2 管理者として DB2 データベースに接続するために使用するユーザー ID を指定します。例: `db2admin`。この値が新規値の場合、ユーティリティーはユーザー ID およびインスタンス名を作成します。既存のユーザー ID およびインスタンス名を指定すると、新規ユーザー ID およびインスタンス名は作成されません。
   - DB2 管理者パスワード

     DB2 データベース管理者アカウントに設定したパスワードを入力します。
   - パスワードの確認

     再度パスワードを入力します。
   - DB2 サーバー・データベース・ホーム

     DB2 インスタンスが入っているディレクトリーを指定します。例えば、C: または `/home/dbinstancename` です。
   - DB2 データベース名

     作成するデータベースの名前を指定します。例: `itimdb`
   - IBM Security Identity Manager データベース・ユーザー ID

     作成するデータベースのユーザー ID を指定します。例えば、`itimuser` です。

     注: Windows システムの場合、ユーティリティーの実行後、このユーザー・アカウントのパスワードの有効期限を無効にします。
   - IBM Security Identity Manager データベース・ユーザー ID のパスワード:

     データベース・ユーザー ID のパスワードを指定します。
   - パスワードの確認

     再度パスワードを入力します。
   - DB2 管理者のグループ

     有効なグループ (root がそのグループのメンバー) を選択し、DB2 管理者 ID インスタンス名を関連付けます。例えば、`bin` です。この値は、UNIX または Linux オペレーティング・システムの場合にのみ選択可能です。

注: ドル記号 ($) は、ミドルウェア構成ユーティリティーによって使用されるインストーラー・フレームワークにおいて特別な意味を持っています。フィールド

値で $ を使用しないでください。インストーラー・フレームワークまたはオペレーティング・システム・プラットフォームが値の変数置換を実行する可能性があります。

7. デフォルトの DB2 インスタンス名が変更されているか、またはその名前の DB2 インスタンスが存在する場合は、警告メッセージのプロンプトが出されます。その DB2 インスタンスを IBM Security Identity Manager でのみ使用する場合は、「**はい**」をクリックします。インスタンスを別のプログラムと共有しないでください。
8. 構成オプションを確認してから、「**次へ**」をクリックして構成プロセスを開始します。
9. 構成が完了するまで数分かかる可能性があります。構成が正常に完了したら、「**完了**」をクリックしてデプロイメント・ウィザードを終了します。このステップで、DB2 データベースのミドルウェア構成プロセスは終了しました。

次のタスク

ミドルウェア構成ユーティリティーが DB2 についてエラーなしで完了したことを検証し、システム一時ディレクトリーの `cfg_itim_mw.log` を確認してください。

DB2 のサイレント構成:

以下の手順を使用して、ミドルウェア構成ユーティリティーをサイレントに開始します。

始める前に

DB2 データベースが正しくインストールされていることを確認します。

手順

1. サンプルである `cfg_itim_mw.rsp` 応答ファイル (または、Windows システムの場合は `cfg_itim_mw_windows.rsp`) をターゲット・コンピューター上のディレクトリーにコピーします。
2. 応答ファイルを正しい値で更新します。configureDB2 値が `yes` に設定されていることを確認します。同時にディレクトリー・サーバーを構成しない場合は、configureLDAP 値が `no` に設定されていることを確認します。
3. コマンド・ウィンドウから、次のコマンドを実行します。

   ```
   cfg_itim_mw –W ITIM.responseFile=cfg_itim_mw.rsp –silent
   ```

   ここで、`cfg_itim_mw` は以下のとおりです。
   - **AIX オペレーティング・システム**: `cfg_itim_mw_aix`
   - **Solaris オペレーティング・システム**: `cfg_itim_mw_solaris`
   - **Linux for xSeries オペレーティング・システム**: `cfg_itim_mw_xLinux`
   - **Linux for pSeries オペレーティング・システム**: `cfg_itim_mw_pLinux`
   - **Linux for zSeries オペレーティング・システム**: `cfg_itim_mw_zLinux`
   - **Windows オペレーティング・システム**: `cfg_itim_mw_windows`

   注: サイレント・モードでミドルウェア構成ユーティリティーを実行すると、構成プロセス中に応答ファイルが更新されます。

次のタスク

サービス Listen ポートおよびサービス名を確認します。

手動での DB2 サーバーの構成:

DB2 サーバーを手動で構成できます。ここで説明する DB2 設定は、ランタイム調整が必要な初期設定です。

DB2 サーバーの構成には、以下のステップが必要です。

1. オペレーティング・システムでユーザーを作成します。
2. IBM Security Identity Manager データベースを作成します。
3. TCP/IP 通信が指定されていることを確認します。

詳しくは、技術的な補足情報である「*IBM Security Identity Manager Performance Tuning Guide*」を参照してください。

Windows および UNIX システムにおけるユーザーの作成:

以下の手順を使用して、DB2 サーバーがインストールされているコンピューターに、itimuser という名前のオペレーティング・システム・ユーザーを作成します。

始める前に

このユーザーには特別な権限は必要ありません。次回ログオン時にパスワードの変更が必要ではなく、パスワードは無期限であることを確実に確認してください。

このタスクについて

IBM Security Identity Manager サーバーは、デフォルトのユーザー ID である itimuser を使用してデータベースにアクセスします。デフォルトのユーザー ID 以外のユーザー ID を作成することも、既存のユーザー ID を使用することもできます。

ユーザーを作成するには、以下の手順を実行します。

手順

1. root またはアドミニストレーターとして、オペレーティング・システムのシステム管理ツールを開始します。
   - AIX オペレーティング・システム: SMIT または SMITTY
   - Solaris: システム管理コンソール (SMC)
   - Windows: 「**スタート**」 > 「**管理ツール**」 > 「**コンピューターの管理**」 > 「**ローカル ユーザーとグループ**」 > 「**ユーザー**」をクリックします。
2. ユーザー itimuser を追加し、ユーザー・パスワードを設定します。
3. システム管理ツールを終了します。

次のタスク

ユーザー・アクセスをテストします。パスワードのリセットが発生することなく、ユーザー ID itimuser でログオンできることを確認します。

IBM Security Identity Manager データベースを作成します。

Linux システムにおけるユーザーの作成:

DB2 サーバーがインストールされているコンピューター上に itimuser という名前のユーザーを作成するには、コンソール・コマンド・インターフェースまたは GUI ユーティリティーを使用することができます。

始める前に

このユーザーには特別な権限は必要ありません。次回ログオン時にパスワードの変更が必要ではなく、パスワードは無期限であることを確実に確認してください。

このタスクについて

IBM Security Identity Manager サーバーは、デフォルトのユーザー ID である itimuser を使用してデータベースにアクセスします。独自のユーザー ID を作成することもできます。

手順

Linux システムでユーザーを作成するには、以下の 2 つの方法があります。

- コンソール・コマンド・インターフェースを使用して、以下のコマンドを入力する。

  ```
  useradd -d /home/itimuser -p password itimuser
  ```

  -d スイッチは、ホーム・ディレクトリーを指定します。項目 itimuser は、作成されるユーザー ID を指定します。
- グラフィカル・ユーザー・マネージャー・アプリケーションを使用して、Red Hat Enterprise Linux システムでユーザーを作成する。
  1. 以下のいずれかの方式を使用して、ユーザーを作成します。
     - グラフィカル・ユーザー・マネージャー・アプリケーションから、「**アプリケーション**」 > 「**システム設定**」 > 「**ユーザーおよびグループ**」を選択します。または、
     - シェル・プロンプトに redhat-config-users と入力して、グラフィカル・ユーザー・マネージャーを開始します。

     「ユーザーの追加」ウィンドウが開きます。
  2. 「**ユーザーの追加**」をクリックします。
  3. 「新規ユーザーの作成」ダイアログ・ボックスで、username (このアカウントの作成対象のユーザーのフルネーム) とパスワードを入力します。
  4. 「**OK**」をクリックします。

次のタスク

ユーザー・アクセスをテストします。パスワードのリセットが発生することなく、ユーザー ID itimuser でログオンできることを確認します。

IBM Security Identity Manager データベースを作成します。

IBM Security Identity Manager データベースの作成:

IBM Security Identity Manager データベースに任意の名前を指定できます。itimdb など。

始める前に

ご使用のシステムに IBM DB2 データベースをインストールして構成しておく必要があります。

手順

1. DB2 コマンド・ウィンドウで、以下のコマンドを入力して、データベースを作成します。

   ```
   db2 create database itim_dbname using codeset UTF-8 territory us
   db2 connect to itim_dbname user itim_dbadmin_name using itim_dbadmin_password
   db2 create bufferpool ENROLEBP size automatic pagesize 32k
   db2 update db cfg for itim_dbname using logsecond 12
   db2 update db cfg for itim_dbname using logfilsiz 10000
   db2 update db cfg for itim_dbname using auto_runstats off
   db2 disconnect current
   ```

   itim_dbname の値は、itimdb などの名前です。 DB2 のパフォーマンス・パラメーターの調整について詳しくは、「*IBM Security Identity Manager Performance Tuning Guide*」を参照してください。
2. DB2 サーバーを停止および開始して、構成をリセットします。

   IBM Security Identity Manager データベースの作成および構成が済んだら、DB2 サーバーを停止および開始して、変更を有効にします。次のコマンドを入力します。

   a. db2stop 入力 db2stop が失敗し、データベースがアクティブのままの場合、db2 force application all と入力して、データベースを非アクティブ化します。再度、db2stop を入力します。

   b. db2start

次のタスク

TCP/IP 通信が指定されていることを確認します。

TCP/IP 通信が指定されていることの確認:

DB2 をインストールするとデフォルトで TCP/IP 通信が指定されます。ただし、DB2 サーバーおよび DB2 クライアントで TCP/IP 通信が指定されていることを確認する必要があります。

始める前に

ご使用のシステムに IBM DB2 データベースをインストールして構成しておく必要があります。

手順

次のコマンドを入力します。

```
db2set -all DB2COMM
```

値のリストが返されます。

- 返されたリストに tcpip 項目がない場合は、以下のコマンドを入力します。tcpip、および コマンドによって提供されたリストに返されたその他のすべての値を含めてください。

  ```
  db2set DB2COMM=tcpip,values_from_db2set_command
  ```

  例えば、db2set -all DB2COMM コマンドが npipe および ipxspx といった値をリストに戻した場合、2 回目に db2set コマンドを入力するときにこれらの値を再び指定します。

  ```
  db2set DB2COMM=tcpip,npipe,ipxspx
  ```

tcpip を含む値のリストが返されます。

次のタスク

他のコンポーネントをインストールして構成します。

正しいサービス Listen ポートおよびサービス名の決定:

ミドルウェア構成ユーティリティーを実行すると、サービス Listen ポート番号およびデータベース・サービス名が構成されます。ただし、正しいサービス名と Listen ポートが指定されていることを確認する必要があります。

始める前に

ご使用のシステムに IBM DB2 データベースをインストールして構成しておく必要があります。

このタスクについて

サービス Listen ポートは、各 DB2 インスタンスに関連付けられています。このポートは、DB2 アプリケーションからインスタンスが所有するデータベースへの DB2 接続の確立に使用されます。

DB2 デフォルト・インスタンスは、ご使用のオペレーティング・システムによって異なります。

- Windows オペレーティング・システムの場合: DB2
- UNIX および Linux オペレーティング・システムの場合: db2inst1

DB2 サーバーのインストール時に作成される DB2 デフォルト・インスタンスのデフォルトのサービス・ポート番号は、50000 です。ミドルウェア構成ユーティリティーを実行して DB2 インスタンスを作成した場合は、インスタンスのデフォルトのサービス・ポート番号は 50002 です。DB2 8.2 を DB2 9.5 または DB2 9.7 にマイグレーションした場合は、DB2 マイグレーション・ユーティリティーによって DB2 インスタンスがリセットされます。DB2 マイグレーション・ユーティリティーで、インスタンスのサービス・ポートも 60000 にリセットされる場合があります。

手順

1. 正しいサービス名またはサービス Listen ポートが定義されているかどうかを判別するには、 次のコマンドを入力します。

```
db2 connect to itim_dbname user itim_dbadmin_id using itim_dbadmin_password
db2 get dbm cfg
```

SVCENAME 属性を検索して、サービス名を見つけます。

2. DB2 サーバーが配置されているコンピューターのサービス・ファイルで、現在のポート番号を指定しているステートメントを見つけます。

   サービス・ファイルのパスは以下のとおりです。

   - Windows オペレーティング・システム: %SYSTEMROOT %¥system32¥drivers¥etc¥services
   - UNIX または Linux オペレーティング・システム: /etc/services

DB2 データベースのパフォーマンス調整タスク

DB2 の初期構成後にパフォーマンス問題が発生することがあります。このタスクでは、DB2 を正常に稼働させるために実行するアクションについて説明します。

TCP KeepAlive 設定値の構成:

メッセージング・エンジンのフェイルオーバー設計は、メッセージング・エンジンのインスタンスに障害が発生したときに切断されるデータベース接続に依存しています。高可用性環境でフェイルオーバーが発生するためには、システムが、切断された接続のタイムリーな認識とデータベース・ロックの解放を確実に行うようにします。この作業は、TCP KeepAlive 設定値を構成することにより行うことができます。

始める前に

ご使用のシステムに DB2 データベースをインストールして構成しておく必要があります。

手順

1. システム管理者としてログインします。
2. DB2 サーバーがあるコンピューター上で、以下のコマンドを実行します。
   - Linux オペレーティング・システムの場合、以下のコマンドを入力します。

     ```
     echo 30 >  /proc/sys/net/ipv4/tcp_keepalive_intvl
     echo 30 > /proc/sys/net/ipv4/tcp_keepalive_time
     ```

     注: これらの設定値は、IPv6 インプリメンテーションによっても使用されます。
   - Windows オペレーティング・システムの場合、以下のステップを実行します。

     regedit を実行して、HKEY_LOCAL_MACHINE¥System¥CurrentControlSet¥Services¥Tcpip¥Parameters ディレクトリー内の Windows レジストリー・キーを編集します。
3. 変更を有効にするために、コンピューターを再起動します。 Linux オペレーティング・システムの場合、以下のコマンドを実行します。

   ```
   # /etc/init.d/network restart
   ```

次のタスク

変更を有効にするために、コンピューターを再始動します。

DB2 アプリケーション・ヒープ・サイズの変更:

多数のユーザーをロードすると、パフォーマンス問題が発生することがあります。

次のようなメッセージが表示されます。

```
Not enough storage available for processing the sql statements.
```

追加のストレージ・スペースを提供するには、DB2 アプリケーション・ヒープ・サイズを、次のようにより大きい値に変更します。実稼働環境とテスト環境の両方ですべてのシステム用に DB2 を調整するには、「*IBM Security Identity Manager Performance Tuning Guide*」を参照してください。

Oracle データベースのインストールおよび構成

ここでは、Oracle データベースを IBM Security Identity Manager 用にインストールおよび構成する方法について説明します。

詳細な情報が必用な場合は、必ず Oracle が提供しているインストールおよびマイグレーションのガイドを参照してください。

データベース作成タスク

この一連のタスクを使用して、IBM Security Identity Manager と共に使用する Oracle データベースを作成します。

注: IBM Security Identity Manager の複数のインスタンスを同一の Oracle データベース・サーバーと共に使用するには、追加のタスクが必要です。データベースを作成する前に、『1 つの Oracle データベース・サーバーと IBM Security Identity Manager の複数インスタンス』を参照してください。

IBM Security Identity Manager 用の Oracle データベースを作成するには、以下のステップを実行します。

1. 既存のデータベースをバックアップします。
2. Oracle データベース・サーバーをインストールします。
3. init.ora ファイルを構成します。
4. 環境変数を設定します。
5. Oracle JDBC ドライバーをインストールします。

1 つの Oracle データベース・サーバーと IBM Security Identity Manager の複数インスタンス:

IBM Security Identity Manager の複数のインスタンスが同一の Oracle サーバー上の複数のデータベースを指すようにするには、`$ISIM_home/config/rdbms/oracle/enrole_admin.sql` ファイルをコピーしてから変更します。

`$ISIM_home/config/rdbms/oracle/enrole_admin.sql` ファイルにある以下のコード例をコピーして変更する必要があります。

この例では、値 enrole1_data_001.dbf は enrole1_data_002.dbf に変更されています。この値は、コードの各コピーで増分的に変更します。このタスクは、同一の Oracle サーバー上で使用される追加の IBM Security Identity Manager インスタンスごとに行います。

注: コード内で**太字**で強調表示しているのが、変更が必要な 2 行です。

例

```
# pwd
/u02/enrole/config/rdbms/oracle
# more enrole_admin.sql
CREATE TABLESPACE enrole_data
DATAFILE 'enrole1_data_002.dbf'
SIZE 160M
AUTOEXTEND ON
NEXT 20M
MAXSIZE 1024M
DEFAULT STORAGE (INITIAL 10M
NEXT 1M
PCTINCREASE 10)
PERMANENT
ONLINE
LOGGING;

CREATE TABLESPACE enrole_indexes
DATAFILE 'enrole1_idx_002.dbf'
SIZE 160M
AUTOEXTEND ON
NEXT 20M
MAXSIZE 1024M
DEFAULT STORAGE (INITIAL 10M
NEXT 1M
PCTINCREASE 10)
PERMANENT
ONLINE
LOGGING;

CREATE USER enrole IDENTIFIED BY enrole
DEFAULT TABLESPACE enrole_data
QUOTA UNLIMITED ON enrole_data
QUOTA UNLIMITED ON enrole_indexes;
GRANT CREATE SESSION TO enrole;
GRANT CREATE TABLE to enrole;
#
```

既存のデータベースのバックアップ:

Oracle 製品のインストール、または既存のデータベースのアップグレードを開始する前に、既存のすべてのデータベースのフルバックアップを作成します。

Oracle Corporation の資料に記載されている準備ステップを確認して、Oracle データベースをアップグレードします。

Oracle データベース・サーバーのインストール:

Oracle データベース・サーバーは、IBM Security Identity Manager と同一のコンピューターにインストールする場合も、別のコンピューターにインストールする場合もあります。

Oracle データベース・サーバーのインストールについては、Oracle 公式 Web サイトで提供されている資料を参照してください。

注: IBM Security Identity Manager 用の Oracle データベースを手動で作成する場合は、JVM 機能を手動でインストールする必要があります。そうしないと、IBM Security Identity Manager からのトランザクションが後ですべて失敗する場合があります。データベースを手動で作成して JVM 機能をインストールする必要はありません。Oracle データベース構成アシスタント・ウィザードを使用して、データベースの作成および JVM 機能のインストールを行うことができます。

init.ora ファイルの構成:

Oracle データベース・サーバーをインストールした後で、init.ora ファイルを IBM Security Identity Manager データベース用に構成する必要があります。

始める前に

Oracle データベース・サーバーがインストールされている必要があります。

手順

1. init.ora ファイルをコピーします。
   - Windows オペレーティング・システム:
     a. *ORACLE_HOME*¥admin¥ ディレクトリーの下に、*db_name*¥pfile という名前のディレクトリーを作成します。*db_name* の値は *itimdb* にすることができます。
     b. サンプル initsmpl.ora ファイルを *ORACLE_HOME*¥db_1¥admin¥sample¥pfile¥ ディレクトリーから *ORACLE_HOME*¥admin¥db_name¥pfile ディレクトリーにコピーします。
     c. 新規の init.ora ファイルの名前を init*db_name*.ora という値に変更します。
   - UNIX または Linux オペレーティング・システム:

     ORACLE_HOME/product/<*version number*>/dbhome_1/dbs/init.ora ファイルを、新規の *ORACLE_HOME*/dbs/init*db_name*.ora ファイルにコピーします。
2. 環境要件に基づいて、init*db_name*.ora ファイル内の以下のパラメーターの値を調整します。

   ```
   db_name=itimdb
   compatible=<version number>
   processes=150
   shared_pool_size=50000000
   ```

   さらに、IBM Security Identity Manager データベースに 3 つの制御ファイルを定義します。このサンプル・ステートメントは、UNIX オペレーティング・システム用の制御ファイルを定義します。

   ```
   control_files=(ORACLE_HOME/oradata/db_name/control01.ctl,
   ORACLE_HOME/oradata/db_name/control02.ctl,
   ORACLE_HOME/oradata/db_name/control03.ctl)
   ```

「*IBM Security Identity Manager Performance Tuning Guide*」を使用して、すべてのシステムの実稼働環境とテスト環境の両方について、Oracle データベースを調整します。

3. `init db_name.ora` ファイルで定義されているすべてのディレクトリーを手動で作成します。

次のタスク

環境変数を設定します。

環境変数の設定:

`.profile` ファイルを編集して、Oracle の環境変数を設定します。

必要な環境変数には、以下のものがあります。

- ORACLE_SID=itimdb
- ORACLE_BASE=/home/oracle/app/oracle
- ORACLE_HOME=$ORACLE_BASE/product/11.2.0/dbhome_1
- PATH=$ORACLE_HOME/bin;$PATH

現行セッションで環境変数を更新する、UNIX オペレーティング・システムのプロファイルを入手します。このタスクにより、IBM Security Identity Manager はデータベースと確実に通信できるようになります。このプロファイルを入手するには、以下のコマンドを入力します。

```
# . /.profile
```

詳しくは、Oracle 公式 Web サイトを参照してください。

Oracle JDBC ドライバーのインストール:

Oracle 10g または 11g データベースをご使用の場合、IBM Security Identity Manager バージョン 6.0 では Oracle 11g Release 1 (11.1.0.7.0) JDBC ドライバーが必要です。

Oracle サーバー・ディレクトリーにある Oracle JDBC ドライバーを IBM Security Identity Manager のインストール先のコンピューターのディレクトリーにコピーします。例えば、Windows オペレーティング・システムの場合は、`C:¥isim_jdbcdriver` というディレクトリーを作成します。 UNIX または Linux オペレーティング・システムの場合は、 `/isim_jdbcdriver` というディレクトリーを作成します。 JDBC ドライバー・ファイルをこのディレクトリーにコピーしてから、インストール時にこのディレクトリーを指すようにします。

また、Oracle Web サイトからもドライバーをダウンロードできます。インストール・プログラムが、JDBC ドライバーおよびドライバー名を含むディレクトリーを要求するプロンプトを出します。クラスター構成では、デプロイメント・マネージャーがあるコンピューター、および各クラスター・メンバー・コンピューターに、JDBC ドライバーが必要です。

IBM Security Identity Manager データベースの作成

IBM Security Identity Manager データベースの作成に Oracle データベース・コンフィギュレーション・アシスタント・ウィザードを使用しない場合にのみ、このステップが必要です。Oracle データベース・コンフィギュレーション・アシスタント・ウィザードを使用してデータベースを作成する場合は、Oracle 社の公式 Web サイトの「*DBCA を使用したデータベースの作成*」を参照してください。

始める前に

Oracle データベースのインストールを完了している必要があります。

手順

1. IBM Security Identity Manager データベースを手動で作成します。
   - Windows オペレーティング・システム:
     a. 以下のコマンド (1 行で入力します) を使用して、インスタンスを作成します。

        ```
        # oradim -new -sid db_name -pfile ORACLE_HOME¥admin¥db_name¥pfile¥
        initdb_name.ora
        ```

        -sid パラメーターの値は、データベース・インスタンス名を指定します。例えば、*db_name* の値は itimdb にすることができます。**-pfile** パラメーターの値は、34 ページの『init.ora ファイルの構成』で以前に構成したファイルを指定します。

     b. 以下のコマンドを使用して、データベース・インスタンスを開始します。

        ```
        # sqlplus "/ as sysdba"
        SQL> startup nomount pfile=ORACLE_HOME¥admin¥db_name¥pfile¥initdb_name.ora
        ```

     c. Windows サービス OracleService*db_name* が開始済みであることを確認します。
   - UNIX または Linux オペレーティング・システム:

     以下のコマンドを使用して、データベース・インスタンスを開始します。

     ```
     # ./sqlplus "/ as sysdba"
     SQL> startup nomount pfile= ORACLE_HOME/dbs/initdb_name.ora
     ```

2. 以下の例に類似した SQL スクリプトを使用して、データベースを作成します。このスクリプト内の値を、サイトの要件に一致するように変更します。この例では、*db_name* の値は、itimdb などのインスタンス名です。

   ```
   --  Create database
   CREATE DATABASE db_name
       CONTROLFILE REUSE
       LOGFILE '/u01/oracle/db_name/redo01.log' SIZE 1M REUSE,
               '/u01/oracle/db_name/redo02.log' SIZE 1M REUSE,
               '/u01/oracle/db_name/redo03.log' SIZE 1M REUSE,
               '/u01/oracle/db_name/redo04.log' SIZE 1M REUSE
       DATAFILE '/u01/oracle/db_name/system01.dbf' SIZE 10M REUSE
         AUTOEXTEND ON
         NEXT 10M MAXSIZE 200M
       CHARACTER SET UTF8;

   -- Create another (temporary) system tablespace
   CREATE ROLLBACK SEGMENT rb_temp STORAGE (INITIAL 100 k NEXT 250 k);

   -- Alter temporary system tablespace online before proceeding
   ALTER ROLLBACK SEGMENT rb_temp ONLINE;
   ```

```
-- Create additional tablespaces ...
-- RBS: For rollback segments
-- USERs: Create user sets this as the default tablespace
-- TEMP: Create user sets this as the temporary tablespace
CREATE TABLESPACE rbs
    DATAFILE '/u01/oracle/db_name/db_name.dbf' SIZE 5M REUSE AUTOEXTEND ON
      NEXT 5M MAXSIZE 150M;
CREATE TABLESPACE users
    DATAFILE '/u01/oracle/db_name/users01.dbf' SIZE 3M REUSE AUTOEXTEND ON
      NEXT 5M MAXSIZE 150M;
CREATE TABLESPACE temp
    DATAFILE '/u01/oracle/db_name/temp01.dbf' SIZE 2M REUSE AUTOEXTEND ON
      NEXT 5M MAXSIZE 150M;

-- Create rollback segments.
CREATE ROLLBACK SEGMENT rb1 STORAGE(INITIAL 50K NEXT 250K)
  tablespace rbs;
CREATE ROLLBACK SEGMENT rb2 STORAGE(INITIAL 50K NEXT 250K)
  tablespace rbs;
CREATE ROLLBACK SEGMENT rb3 STORAGE(INITIAL 50K NEXT 250K)
  tablespace rbs;
CREATE ROLLBACK SEGMENT rb4 STORAGE(INITIAL 50K NEXT 250K)
  tablespace rbs;

-- Bring new rollback segments online and drop the temporary system one
ALTER ROLLBACK SEGMENT rb1 ONLINE;
ALTER ROLLBACK SEGMENT rb2 ONLINE;
ALTER ROLLBACK SEGMENT rb3 ONLINE;
ALTER ROLLBACK SEGMENT rb4 ONLINE;

ALTER ROLLBACK SEGMENT rb_temp OFFLINE;
DROP ROLLBACK SEGMENT rb_temp ;
```

注: 「*IBM Security Identity Manager Performance Tuning Guide*」を使用して、すべてのシステムの実稼働環境とテスト環境の両方について、Oracle データベースを調整します。

3. このデータベース用に JVM をインストールします。 以下のコマンドを使用してください。

```
# sqlplus "/ as sysdba"

SQL> @$ORACLE_HOME/rdbms/admin/catalog.sql
SQL> @$ORACLE_HOME/rdbms/admin/catproc.sql
SQL> @?/javavm/install/initjvm.sql
SQL> @?/xdk/admin/initxml.sql
SQL> @?/xdk/admin/xmlja.sql
SQL> @?/rdbms/admin/catjava.sql

SQL> connect system/manager
SQL> @$ORACLE_HOME/sqlplus/admin/pupbld.sql
```

manager パラメーターの値は、システム・ユーザー・アカウントのパスワードです。

次のタスク

データベースのパフォーマンスを調整します。

Oracle データベース・パフォーマンス・チューニング

ここでは、Oracle データベースが適切に機能するようにするために必要なアクションについて説明します。

XA リカバリー操作の有効化:

Oracle では、XA リカバリー操作を有効にするために、特別な権限を付与する必要があります。

始める前に

データベース管理者権限があることを確認します。

このタスクについて

XA リカバリーの有効化に失敗すると、次のエラーが発生します。

```
WTRN0037: トランザクション・サービスでは xa_recover 操作中にエラーが発生しました。
(WTRN0037: The transaction service encountered an error on an xa_recover operation.)
```

手順

1. データベース管理者として、コマンド **sqlplus /AS SYSDBA** を発行してデータベースに接続します。
2. 次のコマンドを実行します。

   ```
   grant select on pending_trans$ to public;
   grant select on dba_2pc_pending to public;
   grant select on dba_pending_transactions to public;
   grant execute on dbms_system to itim_db_user;
   ```

   ここで、*itim_db_user* は、itimuser などの IBM Security Identity Manager データベースを所有しているユーザーです。
3. これらの変更内容を有効にするために、データベース・インスタンスを停止してから再始動します。
   - 以下のコマンドを使用して、データベース・インスタンスを開始します。

     ```
     # ./sqlplus "/ as sysdba"
     SQL> startup nomount pfile= ORACLE_HOME/dbs/initdb_name.ora
     ```
   - 以下のコマンドを使用して、データベース・インスタンスを停止します。

     ```
     SQL> SHUTDOWN [mode]
     ```

     ここで、*mode* は *normal*、*immediate*、または *abort* です。

次のタスク

追加設定を調整します。

TCP KeepAlive 設定値の構成:

メッセージング・エンジンのフェイルオーバー設計は、メッセージング・エンジンのインスタンスに障害が発生したときに切断されるデータベース接続に依存しています。高可用性環境でフェイルオーバーが発生するためには、RDBMS が、切断された接続のタイムリーな検出とデータベース・ロックの解放を確実に行うようにします。この作業は、TCP KeepAlive 設定値を構成することにより行うことができます。

始める前に

ご使用のシステムに Oracle データベースをインストールして構成しておく必要があります。

手順

1. システム管理者としてログインします。
2. 左側のペインで、次のパスを選択します。

   ```
   My Computer¥HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥
   Services¥Tcpip¥Parameters
   ```

3. 右側のペインを右クリックし、「**新規**」 > 「**DWORD 値 (DWORD Value)**」を選択します。
4. 新規パラメーターの名前を「KeepAliveInterval」と入力します。
5. この新規パラメーターを右クリックし、「**変更**」を選択します。
6. 「**10 進ベース (Base as Decimal)**」を選択し、値を 30000 (30000 ms (ミリ秒) = 30 秒) と入力します。
7. 同様に、名前 KeepAliveTime を持つ別の DWORD 値を追加し、値を 30000 に設定します。

次のタスク

変更を有効にするために、コンピューターを再始動します。

Oracle 製品およびリスナー・サービスの開始

IBM Security Identity Manager で Oracle データベースを使用するには、製品サービスとリスナー・サービスの両方を開始する必要があります。

始める前に

Oracle データベースをインストールしておく必要があります。

手順

1. Oracle データベースを始動します。
   - Windows オペレーティング・システム:

     「サービス」メニューを使用して、OracleService*db_name* という名前の Oracle データベース・サービスを開始します。
   - UNIX および Linux オペレーティング・システム:

     以下のコマンドを入力します。

     ```
     # su - oracle
     # ./sqlplus "/ as sysdba"
     # SQL> startup
     ```

2. Oracle リスナー・サービスを開始します。
   - Windows オペレーティング・システム:

「サービス」メニューを使用して、OracleOraDb10_home1TNSListener という名前の Oracle TNS リスナーを開始します。Oracle リスナー・サービスがアイドルになっている場合は、リスナーを開始します。

- UNIX および Linux オペレーティング・システム:

  以下のコマンドを入力します。

  ```
  # su - oracle
  # ./lsnrctl start
  ```

  Oracle プロセスが開始済みであることを確認するには、以下のコマンドを入力します。

  ```
  ps -ef | grep ora
  ```

  リスナーが実行されていることを確認するには、以下のコマンドを入力します。

  ```
  # ./lsnrctl status
  ```

次のタスク

追加のコンポーネントをインストールして構成します。

Windows オペレーティング・システム上での SQL Server 2008 のインストールおよび構成

ここでは、SQL Server 2008 データベースのインストールおよび構成の方法について説明します。

SQL Server 2008 のインストール

このセクションでは、SQL Server 2008 の準備とインストールに役立つ情報を説明します。

Windows システムに SQL Server 2008 をインストールする前に、以下の手順を実行します。

1. 最新の SQL Server 2008 サービス・パックを入手します。
2. SQL Server 2008 のインストールを開始する前に、管理者アカウントで Windows システムにログオンします。

サーバーのインストール

SQL Server 2008 は、IBM Security Identity Manager と同一のコンピューターにインストールする場合も、別のコンピューターにインストールする場合もあります。SQL Server 2008 をインストールした後、最新の SQL Server 2008 サービス・パックをインストールします。 SQL Server 2008 のインストールについて詳しくは、SQL Server 公式 Web サイトで提供されている資料を参照してください。

注: SQL Server 2008 をインストールするときは、データベースのコード・ページの大/小文字を区別しないように (CI として) 設定する必要があります。

SQL Server 2008 の構成

IBM Security Identity Manager 用に SQL Server 2008 を構成するには、いくつかのポストインストール・タスクを実行する必要があります。

ポストインストール・タスクには、以下のものが含まれます。

- SQL Server JDBC ドライバーのインストール
- XA トランザクションのための SQL Server 2008 の構成
- SQL Server 2008 のセキュリティー構成の検証

SQL Server JDBC ドライバーのインストール:

IBM Security Identity Manager バージョン 6.0 では、SQL Server 2008 JDBC ドライバー 3.0 が必要です。

SQL Server 2008 の SQL Server JDBC ドライバーを IBM Security Identity Manager のインストール先のコンピューターのディレクトリーにコピーします。また、Microsoft Web サイトからもドライバーをダウンロードできます。IBM Security Identity Manager インストール・プログラムが、JDBC ドライバーおよびドライバー名を含むディレクトリーを要求するプロンプトを出します。クラスター構成では、デプロイメント・マネージャーがあるコンピューター、および各クラスター・メンバー・コンピューターに、JDBC ドライバーが必要です。

例えば、IBM Security Identity Manager をインストールするコンピューター上で、以下の作業を行う必要があります。

1. ディレクトリー `C:¥itim_jdbcdriver¥` を作成します。
2. このディレクトリーに JDBC ドライバー・ファイルをコピーします。
3. インストール時にこのディレクトリーを指すようにします。

XA トランザクションのための SQL Server 2008 の構成:

MS DTC サービスを実行し、JDBC 分散トランザクション・コンポーネントを SQL サーバー用に構成する必要があります。

始める前に

JDBC ドライバーを、以下の Web サイトからダウンロードして解凍しておきます。http://msdn.microsoft.com/en-us/data/aa937724.aspx

手順

MS SQL Server 2008 JDBC ドライバー 3.0 を *JDBC_DRIVER_INSTALL_DIR* にインストールした場合は、JDBC_DRIVER_INSTALL_DIR¥help¥html¥574e326f-0520-4003-bdf1-62d92c3db457.htm ファイルを開きます。『*Understanding XA Transactions*』内の、以下のセクションの指示に従ってください。

1. Running the MS DTC Service
2. Configuring the JDBC Distributed Transaction Components

注: 『*Configuring the User-Defined Roles*』というタイトルのセクションを実行する必要はありません。IBM Security Identity Manager によって、必要な ID と、SqlJDBCXAUser 役割との関連付けが作成されます。

SQL Server 2008 のセキュリティー構成の検証:

SQL Server Management Studio を使用して、SQL Server 2008 のセキュリティー構成を検証します。

始める前に

SQL Server 2008 のダウンロードとインストールを完了している必要があります。

手順

1. Microsoft SQL Server Management Studio を開始します。
2. SQL Server ルート・ノードを右クリックし、「**プロパティ**」をクリックします。
3. 「ページの選択」パネルから「**セキュリティ**」を選択します。
4. 「**SQL Server 認証モードと Windows 認証モード**」が選択されていることを確認します。
5. 「**OK**」をクリックします。

次のタスク

IBM Security Identity Manager データベースを作成します。

IBM Security Identity Manager データベースの作成

IBM Security Identity Manager データベースを作成するには、いくつかのポストインストール・タスクを実行する必要があります。

始める前に

SQL Server 2008 がインストールされ、構成されていることを確認してください。

手順

1. Microsoft SQL Server Management Studio を開始します。
2. ツリーを選択し、「**データベース**」ノードを右クリックして、「**新規データベース**」を選択します。
3. データベース名の下に、`itimdb` などのデータベース名を入力し、「**OK**」をクリックします。
4. データ・ファイルおよびトランザクション・ログには、以下の値を入力します。
   - ファイルの初期サイズ: 20 MB
   - ファイルを自動的に大きくする
   - ファイルを無制限に大きくすることを許可する

   注: SQL Server が混合認証モードであることを確認してください。

次のタスク

追加のコンポーネントをインストールして構成します。

ディレクトリー・サーバーのインストールおよび構成

IBM Security Identity Manager は、ディレクトリー・サーバーにユーザー・アカウントおよび組織データ (ただし、スケジューリング・データと監査データは除く) を保管します。このセクションでは、IBM Security Identity Manager で使用するディレクトリー・サーバーの構成について説明します。

サポートされるディレクトリー・サーバーの組み合わせ、および必要なフィックスパックについては、IBM Security Identity Manager インフォメーション・センターの『データベース・サーバー要件』を参照してください。

このセクションの情報は、ディレクトリー・サーバー製品そのものによって提供されるより広範囲な前提条件の資料に代わるものではありません。詳しくは、IBM Security Identity Manager インフォメーション・センターの『ハードウェア要件およびソフトウェア要件』を参照してください。フィックスおよびダウンロードについては、IBM ソフトウェア製品のサポート Web サイトを参照してください。

ディレクトリー・サーバー製品をインストールする前に

ディレクトリー・サーバー製品をインストールする前に、以下を実行する必要があります。

- ディレクトリー・サーバー製品により提供されるインストール・ガイドを読むこと。
- インストールがディレクトリー・サーバーのハードウェアおよびソフトウェア要件に適合していることの確認。

IBM Directory Server のインストールおよび構成

IBM Tivoli Directory Server は、IBM Security Identity Manager と同じコンピューターにも別のコンピューターにもインストールできます。サポートされるバージョンの IBM Tivoli Directory Server は、IBM Security Identity Manager でサポートされるオペレーティング・システム・リリースに対応しています。詳しくは、IBM Security Identity Manager インフォメーション・センターの『ソフトウェア要件』の『オペレーティング・システムのサポート』を参照してください。

IBM Tivoli Directory Server は、データ・ストアとして DB2 データベース、Web 管理ツールとして WebSphere Application Server を使用します。

IBM Tivoli Directory Server のインストール

以下の手順では、IBM Security Identity Manager 製品に付属の DVD を使用して IBM Tivoli Directory Server をインストールする方法について説明します。これらの DVD には、DB2 および WebSphere Application Server の組み込みミドルウェアは含まれていません。組み込みミドルウェアが含まれたインストール DVD の場合、オプションで、IBM Tivoli Directory Server 用の組み込みの DB2 および WebSphere Application Server をインストールできます。インストール・プロセスは異なる可能性があります。

始める前に

ディレクトリー・サーバーのインストールについて詳しくは、ディレクトリー・サーバー製品が提供する資料を参照してください。例えば、次の Web サイトにアクセスします (日本では異なる場合があります。日本における情報については営業担当員にお問い合わせください)。http://www.ibm.com/software/sysmgmt/products/support/IBMDirectoryServer.html

このタスクについて

組み込み DB2は、IBM Security Identity Manager データベースと組み込み WebSphere Application Server のいずれにも使用することはできません。

IBM Tivoli Directory Server をインストールするには、以下の手順を実行します。

手順

1. まだ DB2 がインストールされていない場合は、IBM Security Identity Manager 製品とともに提供される DVD から DB2 をインストールします。
2. オプション。このステップは、IBM Tivoli Directory Server に WebSphere Application Server アプリケーション・クライアントを使用する場合にのみ必要です。 IBM Security Identity Manager 製品とともに提供される DVD から WebSphere Application Server をインストールします。IBM Tivoli Directory Server と同じコンピューターに IBM Security Identity Manager をインストールする場合は、最初に WebSphere Application Server インストールを完了する必要があります。詳しくは、 58 ページの『単一サーバー環境への WebSphere Application Server のインストール』を参照してください。
3. IBM Security Identity Manager 製品とともに提供される DVD から IBM Tivoli Directory Server をインストールします。
4. IBM Tivoli Directory Server のインストール中に、インストール・タイプとして「**カスタム**」を選択する必要があります。「**次へ**」をクリックします。
5. 次のパネルでは、DB2 データベースも組み込み WebSphere Application Server も選択しないでください。サポートされている IBM Tivoli Directory Server を選択する必要があります。その他の機能はオプションです。「**次へ**」をクリックします。
6. 次のパネルでは、インストーラーはご使用の WebSphere Application Server を検出します。WebSphere Application Server インストール・パスのカスタム・ロケーションを選択するように求めるプロンプトが出される場合があります。 Web Administration Tools のデプロイメントをスキップすることもできます。「**次へ**」をクリックします。
7. 要約を確認し、「**インストール**」をクリックして IBM Tivoli Directory Server をインストールします。

   ディレクトリー・サーバーのインストールについて詳しくは、ディレクトリー・サーバー製品が提供する資料を参照してください。

次のタスク

必要なフィックスパックをインストールします。

必須フィックスパックのインストール

ご使用のバージョンの IBM Tivoli Directory Server でフィックスパックが必要な場合、そのフィックスを取得してインストールします。

フィックスパックについては、「ディレクトリー・サーバーのサポート」Web サイトを参照してください。

正しいフィックスパックがインストールされていることを検証します。

IBM Tivoli Directory Server に正しいフィックスパックがインストールされていることを検証するには、以下のコマンドを発行します。

- AIX: `lslpp -l 'idsldap*'`
- Linux: `rpm -qa | grep idsldap`
- Solaris:
  1. 特定パッケージのバージョンを照会するには、`pkginfo | grep IDSl` と入力します。
  2. 各インストール済みパッケージについては、`pkgparam` *`package_name`* `VERSION` と入力します。例えば、IBM Tivoli Directory Server でサポートされるバージョンの場合は、`pkgparam IDSl64s<`*`version number`*`> VERSION` のようになります。
- Windows:
  1. コマンド・プロンプトから、`<IDS_HOME>¥bin` に進みます。
  2. 以下のコマンドを実行します。

     ```
     idsversion.cmd
     ```

詳しくは、IBM Security Identity Manager インフォメーション・センターの『ソフトウェア要件』と、IBM Tivoli Directory Server フィックスパックで提供される資料を参照してください。

IBM Tivoli Directory Server 構成

IBM Tivoli Directory Server の設定を行うには、IBM Security Identity Manager サーバーをインストールする前に、組織の LDAP サフィックスを作成する必要があります。また、IBM Tivoli Directory Server の設定には、IBM Security Identity Manager の参照整合性ファイルの構成も必要です。LDAP サフィックス (命名コンテキストとも呼ばれる) は、ローカルに保持されたディレクトリー階層の最上部のエントリーを識別する識別名 (DN) です。

IBM Security Identity Manager インストール製品には、ミドルウェア構成ユーティリティーが含まれています。このユーティリティーでは、データベース・インスタンスとユーザー ID を作成できます。また、DB2 と IBM Tivoli Directory Server の参照整合性およびパラメーターを構成できます。標準パラメーターの多くと、すべての拡張パラメーターに、デフォルト値が提供されています。入力されたパラメーター (ディレクトリー・サーバー管理者 ID など) が存在する場合は、ミドルウェア構成ユーティリティーは作成タスクをスキップします。これらの値をそのまま使用するか、独自の値を入力するかを選択することができます。必須フィールドは、アスタリスク (*) でマークされています。所望のパネルに達するまで「**戻る**」をクリックして、デプロイメント・ウィザードの任意のパネルに戻ることができます。

注: ミドルウェア構成ユーティリティーは、デフォルトで、システム一時ディレクトリー (例えば `/tmp` ディレクトリー) にある `db2ldap.rsp` という応答ファイルに指定した入力をすべて保管します。このファイルは、通常はユーティリティー完了後にクリーンアップされます。ユーティリティーが完了する前にキャンセルすると、このファイルが消去されない場合があります。

ミドルウェア構成ユーティリティーの実行:

ミドルウェア構成ユーティリティーを実行して、後で IBM Security Identity Manager デプロイメントで使用する IBM Tivoli Directory Server パラメーターを設定できます。

始める前に

Windows オペレーティング・システムの場合は、管理者であるか、管理者権限を持っている必要があります。

UNIX および Linux オペレーティング・システムの場合は、root ユーザーである必要があります。また、umask 設定が 022 であることが必要です。 umask 設定を確認するには、コマンド **umask** を発行します。

umask 値を 022 に設定するには、以下のコマンドを発行します。

```
umask 022
```

現在サポートされている IBM DB2 バージョン 9.7 および IBM Tivoli Directory Server バージョン 6.3 を使用して Tivoli Identity Manager バージョン 5.1 の新規インストールを行う準備ができたら、ミドルウェア構成ユーティリティーを実行する前に、IBM サポートに連絡して支援を受けてください。

- Tivoli ソフトウェア・サポート
- 地域の連絡窓口

このタスクについて

ミドルウェア構成ユーティリティーは、以下を実行します。

- 必要な場合、ユーザー ID の作成
- 必要な場合、IBM Tivoli Directory Server インスタンスの作成
- 必要な場合、ディレクトリー・サーバー・データベースの作成
- LDAP の調整 (バッファー・プール、ログ調整)
- LDAP サフィックスの追加
- 非 SSL ポートの構成
- IBM Tivoli Directory Server のサポートされているバージョンでは、IBM Security Identity Manager 用の参照整合性プラグインを構成します。

ミドルウェア構成ユーティリティーは、手動でもサイレント・モードでも実行できます。サイレント・モードでの構成について詳しくは、49 ページの『IBM Tivoli Directory Server のサイレント構成』を参照してください。

IBM Tivoli Directory Server のミドルウェア構成ユーティリティーを手動で開始するには、以下のようにします。

手順

1. IBM Tivoli Directory Server がインストールされているコンピューター上にシステム管理特権を持つアカウントにログオンします。
2. 日本語、韓国語、中国語 (簡体字)、または中国語 (繁体字) の AIX にインストールする場合は、以下の手順を実行してください。

   注: これらの言語のいずれの AIX にもインストールしない場合は、以下の作業をスキップして、次のステップに進んでください。

   a. ミドルウェア構成ユーティリティーの圧縮ファイルから、`cfg_itim_mw.jar` ファイルを見つけます。ミドルウェア構成ユーティリティー圧縮ファイルは、製品 DVD またはダウンロード・ディレクトリーのベース・ディレクトリーにあります。

   b. コマンド `java -jar cfg_itim_mw.jar` を実行します。

   このコマンドは、ミドルウェア構成ユーティリティー用のグラフィカル・ユーザー・インターフェースが、ミドルウェアの構成中に構成パネルを正しく表示するように構成します。ミドルウェア構成ユーティリティーを開始する前にこのコマンドを実行しないと、言語選択パネルで表示上の問題が発生します。
3. DVD のベース・ディレクトリーまたはダウンロード・ディレクトリーで、ミドルウェア構成ユーティリティーを開始します。
   - AIX オペレーティング・システム: `cfg_itim_mw_aix` プログラムを実行してミドルウェア構成ユーティリティーを開始します。
   - Solaris オペレーティング・システム: `cfg_itim_mw_solaris` プログラムを実行してミドルウェア構成ユーティリティーを開始します。
   - Linux for xSeries オペレーティング・システム: `cfg_itim_mw_xLinux` プログラムを実行してミドルウェア構成ユーティリティーを開始します。
   - Linux for pSeries オペレーティング・システム: `cfg_itim_mw_pLinux` プログラムを実行してミドルウェア構成ユーティリティーを開始します。
   - Linux for zSeries オペレーティング・システム: `cfg_itim_mw_zLinux` プログラムを実行してミドルウェア構成ユーティリティーを開始します。
   - Windows オペレーティング・システム: Windows の自動実行機能が使用不可の場合は、`cfg_itim_mw.exe` プログラムを使用してミドルウェア構成ユーティリティーを開始します。

   ネイティブ・プログラムとともに実行するために、各プラットフォームは `cfg_itim_mw.jar` というファイルを必要とします。JAR ファイルとネイティブ・プログラムは、同じディレクトリー位置にある必要があります。
4. 言語を選択し、「**OK**」をクリックします。
5. 「製品の構成」パネルで、「**IBM Tivoli Directory Server の構成**」のみにチェック・マークを付け、「**次へ**」をクリックします。
6. IBM Tivoli Directory Server が正しいレベルでない場合、またはインストールされていない場合は、警告を受け取る可能性があります。IBM Tivoli Directory Server を正しいレベルにするためのアクションが必要な場合があります。この警告をバイパスするには、「**次へ**」をクリックします。
7. 「IBM Tivoli Directory Server 構成オプション」パネルから、以下の情報を入力し、「**次へ**」をクリックします。

- ディレクトリー・サーバー管理者 ID およびインスタンス名

  ディレクトリー・サーバー管理者として IBM Tivoli Directory Server に接続するために使用するユーザー ID を指定します。例えば、`itimldap` です。

  注: Windows システムの場合、ユーティリティーの実行後、このユーザー・アカウントのパスワードの有効期限を無効にします。
- ディレクトリー・サーバー管理者パスワード

  IBM Tivoli Directory Server 管理者アカウントに設定したパスワードを入力します。
- パスワードの確認

  再度パスワードを入力します。
- DB2 管理者のグループ

  リストから有効なグループ (その root がメンバー) を選択し、DB2 管理者 ID を関連付けます。例えば、`bin` です。この値は、UNIX または Linux オペレーティング・システムの場合にのみ選択可能です。
- ディレクトリー・サーバー・データベース・ホーム

  ディレクトリー・サーバーの DB2 インスタンスが入っているディレクトリーを指定します。例えば、C: または `/home/`*`directory_server_instancename`* です。
- ディレクトリー・サーバー・データベース名

  作成するデータベースの名前を指定します。例えば、`ldapdb2` です。
- 暗号化シード

  暗号鍵を指定します。これには、任意の語または句を使用できます。鍵は、Tivoli Identity Manager のパスワードおよびその他の機密テキストの暗号化に使用します。暗号化シードは、12 文字以上の長さにする必要があります。

注: ドル記号 ($) は、ミドルウェア構成ユーティリティーによって使用されるインストーラー・フレームワークにおいて特別な意味を持っています。フィールド値で $ を使用しないでください。インストーラー・フレームワークまたはオペレーティング・システム・プラットフォームが値の変数置換を実行する可能性があります。

8. 以下の LDAP 情報を指定し、「**次へ**」をクリックします。
   - 管理者 DN

     基本識別名 (DN) を表すユーザー ID。この DN は、Tivoli Identity Manager の root サフィックスです。例えば、`cn=root` です。
   - 管理者 DN パスワード

     基本識別名 (DN) を表すユーザー ID のパスワード。例えば、`secret` です。
   - パスワードの確認

     再度パスワードを入力します。

- ユーザー定義サフィックス

  LDAP サフィックスを指定します。このサフィックスには、任意の有効なサフィックスを指定することができ、IBM Security Identity Manager 情報が配置されるコンテキスト・ルートとして使用されます。例えば、`dc=com` を選択します。

- 非 SSL ポート

  ディレクトリー・サーバーが listen するポート。デフォルト・ポートは 389 です。

  注: このデフォルト・ポートがその他のサービスと競合する可能性があります。例えば、Windows サーバーが Windows Active Directory サービスを実行する可能性があります。このサービスはデフォルト・ポート 389 を使用します。

9. 構成オプションを確認してから、「**次へ**」をクリックして構成プロセスを開始します。
10. 構成が完了するまで数分かかる可能性があります。構成が正常に完了したら、「**完了**」をクリックしてデプロイメント・ウィザードを終了します。

次のタスク

この作業で、IBM Tivoli Directory Server のミドルウェア構成プロセスは終了しました。IBM Tivoli Directory Server のミドルウェア構成ユーティリティーがエラーなしで完了したことを検証するには、システム一時ディレクトリーの `cfg_itim_mw.log` を確認します。

IBM Tivoli Directory Server のサイレント構成:

ミドルウェア構成ユーティリティーを実行して、後で IBM Security Identity Manager デプロイメントで使用する IBM Tivoli Directory Server パラメーターを設定できます。

始める前に

Windows オペレーティング・システムの場合は、管理者であるか、管理者権限を持っている必要があります。

UNIX および Linux オペレーティング・システムの場合は、root ユーザーである必要があります。また、umask 設定が 022 であることが必要です。umask 設定を確認するには、コマンド **umask** を発行します。

umask 値を 022 に設定するには、以下のコマンドを発行します。

```
umask 022
```

このタスクについて

ミドルウェア構成ユーティリティーは、以下を実行します。

- 必要な場合、ユーザー ID の作成
- 必要な場合、IBM Tivoli Directory Server インスタンスの作成

- 必要な場合、ディレクトリー・サーバー・データベースの作成
- LDAP の調整 (バッファー・プール、ログ調整)
- LDAP サフィックスの追加
- 非 SSL ポートの構成
- IBM Tivoli Directory Server のサポートされているバージョンでは、IBM Security Identity Manager 用の参照整合性プラグインを構成します。

ミドルウェア構成ユーティリティーをサイレントに開始するには、以下のようにします。

手順

1. サンプル応答ファイル `cfg_itim_mw.rsp` (または、Windows システムの場合は `cfg_itim_mw_windows.rsp`) をターゲット・コンピューター上のディレクトリーにコピーします。
2. 応答ファイルを正しい値で更新します。`configureLDAP` 値が `yes` に設定されていることを確認します。同時にデータベース・サーバーを構成しない場合は、`configureDB2` 値が `no` に設定されていることを確認します。
3. コマンド・ウィンドウから、次のコマンドを実行します。

   ```
   cfg_itim_mw –W ITIM.responseFile=cfg_itim_mw.rsp –silent
   ```

   ここで、*cfg_itim_mw* は以下のとおりです。
   - AIX オペレーティング・システム: **cfg_itim_mw_aix**
   - Solaris オペレーティング・システム: **cfg_itim_mw_solaris** プログラム
   - Linux for xSeries オペレーティング・システム: **cfg_itim_mw_xLinux** プログラム
   - Linux for pSeries オペレーティング・システム: **cfg_itim_mw_pLinux** プログラム
   - Linux for zSeries オペレーティング・システム: **cfg_itim_mw_zLinux** プログラム
   - Windows オペレーティング・システム: **cfg_itim_mw_windows**

   注: サイレント・モードでミドルウェア構成ユーティリティーを実行すると、構成プロセス中に応答ファイルが更新されます。

次のタスク

この作業で、IBM Tivoli Directory Server のミドルウェア構成プロセスは終了しました。IBM Tivoli Directory Server のミドルウェア構成ユーティリティーがエラーなしで完了したことを検証するには、システム一時ディレクトリーの `cfg_itim_mw.log` を確認します。

正常なサフィックス・オブジェクト構成の検証:

ミドルウェア構成ユーティリティーを実行した後、LDAP サフィックスが正常に追加されたことを確認する必要があります。

サフィックス・オブジェクト構成を検証するには、以下のコマンドを入力します。

- Windows オペレーティング・システム: *ITDS_HOME*¥bin¥ldapsearch.cmd -h localhost -b dc=com "(objectclass=domain)"
- UNIX または Linux オペレーティング・システム: *ITDS_HOME*/bin/ldapsearch.sh -h localhost -b dc=com "(objectclass=domain)"

オプションは次の通りです。

-h LDAP サーバーが稼働しているホストを指定します。

-b デフォルトの代わりに、初期検索の検索ベースを指定します。

出力は、dc=com の許可を構成したこと、データでサフィックスを初期化したことを確認します。

```
dc=com
objectclass=domain
objectclass=top
dc=com
```

手動による IBM Tivoli Directory Server データベースの調整:

IBM Tivoli Directory Server が使用する DB2 インスタンスのパフォーマンスを手動で調整できます。

始める前に

ご使用のシステムに DB2 データベースがインストールされ、構成されていることを確認します。

手順

1. DB2 コマンド・ウィンドウを開きます。
2. DB2 コマンド・ウィンドウで、以下のコマンドを入力して、IBM Tivoli Directory Server データベース・インスタンスを調整します。

   ```
   db2 connect to itds_dbname user itds_dbadmin_name using itds_dbadmin_password
   db2 alter bufferpool IBMDEFAULTBP size automatic
   db2 alter bufferpool ldapbp size automatic
   db2 update db cfg for itds_dbname using logsecond 12
   db2 update db cfg for itds_dbname using logfilsiz 10000
   db2 update db cfg for itds_dbname using database_memory itds_dbmemory
   db2 disconnect current
   ```

   itim_dbname の値は、itimdb などの名前です。 *itim_dbmemory* の値は、単一サーバー・インストールの場合は 40000、AIX および Windows 以外のすべてのプラットフォームの場合は COMPUTED です。AIX および Windows の場合、値は AUTOMATIC です。DB2 のパフォーマンス・パラメーターの調整について詳しくは、「*IBM Security Identity Manager Performance Tuning Guide*」を参照してください。
3. DB2 サーバーを停止および開始して、構成をリセットします。 構成をリセットしたら、DB2 サーバーを停止および開始して、変更を有効にします。次のコマンドを入力します。

   ```
   db2stop
   db2start
   ```

入力 db2stop が失敗し、データベースがアクティブのままの場合、db2 force application all と入力して、データベースを非アクティブ化します。再度、db2stop を入力します。

次のタスク

他のコンポーネントをインストールして構成します。

Oracle Directory Server Enterprise Edition のインストールおよび構成

このセクションでは、Oracle Directory Server Enterprise Edition のインストールと構成の方法について説明します。

Oracle Directory Server Enterprise Edition のインストール

Oracle Directory Server Enterprise Edition のインストールに関する説明と詳細については、Oracle 公式 Web サイトを参照してください。

Oracle Directory Server Enterprise Edition の構成

Oracle Directory Server Enterprise Edition をインストールした後で、それを IBM Security Identity Manager で使用するために構成します。

始める前に

Oracle Directory Server Enterprise Edition をダウンロードおよびインストール済みであることを確認してください。

手順

1. IBM Security Identity Manager LDAP サーバー・インスタンスを作成します。以下のコマンドを入力します。

   ```
   ./dsadm create -p portnumber -P SSL-port instance-path
   ```

   ここで、*portnumber* は Oracle Directory Server Enterprise Edition のポート番号で、*SSL-port* は Oracle Directory Server Enterprise Edition の SSL ポート番号です。以下に例を示します。

   - UNIX または Linux オペレーティング・システムの場合:

     ```
     ./dsadm create –p 1389 –P 1363 /local/itimldap
     ```

   - Windows オペレーティング・システムの場合:

     ```
     dsadm.exe create –p 1389 –P 1363 C:¥itimldap
     ```

2. IBM Security Identity Manager LDAP サーバーを起動します。 以下のコマンドを入力します。

   ```
   ./dsadm start instance-path
   ```

   以下に例を示します。

   - UNIX または Linux オペレーティング・システムの場合:

     ```
     ./dsadm start /local/itimldap
     ```

   - Windows オペレーティング・システムの場合:

     ```
     dsadm.exe start ¥local¥itimldap
     ```

3. ルート・サフィックスを作成します。 以下のコマンドを入力します。

   ```
   ./dsconf create-suffix –h host –p portnumber rootsuffix
   ```

   以下に例を示します。

   - UNIX または Linux オペレーティング・システムの場合:

     ```
     ./dsconf create-suffix –h localhost –p 1389 dc=com
     ```

   - Windows オペレーティング・システムの場合:

     ```
     dsconf.exe create-suffix –h localhost –p 1389 dc=com
     ```

   このコマンドにより、 LDAP サーバー上にルート・サフィックス dc=com が作成されます。

   以下のメッセージを受け取った場合は、**--unsecured** パラメーターを使用してください。

   host:*portNumber* 上で安全にバインドできませんでした
   (Unable to bind securely on *host*:*portNumber*)

   以下に例を示します。

   - UNIX または Linux オペレーティング・システムの場合:

     ```
     ./dsconf create-suffix ––unsecured –h localhost –p 1389 dc=com
     ```

   - Windows オペレーティング・システムの場合:

     ```
     dsconf.exe create-suffix ––unsecured –h localhost –p 1389 dc=com
     ```

4. 以下の内容で、dcequalscom.ldif という名前のファイルを作成して保存します。

   ```
   dn:dc=com
   dc:com
   objectclass:top
   objectclass:domain
   ```

5. dcequalscom.ldif ファイルを dc=com ルート・サフィックスにインポートします。 以下のコマンドを入力します。

   ```
   ./dsconf import -p portnumber -e path/dcequalscom.ldif rootsuffix
   ```

   以下に例を示します。

   - UNIX または Linux オペレーティング・システムの場合:

     ```
     ./dsconf import -p 1389 -e /temp/dcequalscom.ldif dc=com
     ```

   - Windows オペレーティング・システムの場合:

     ```
     dsconf.exe import -p 1389 -e ¥temp¥dcequalscom.ldif dc=com
     ```

   以下のメッセージを受け取った場合は、**--unsecured** パラメーターを使用してください。

   host:*portNumber* 上で安全にバインドできませんでした
   (Unable to bind securely on *host*:*portNumber*)

   - UNIX または Linux オペレーティング・システムの場合:

     ```
     ./dsconf import --unsecured -p 1389 -e /temp/dcequalscom.ldif dc=com
     ```

   - Windows オペレーティング・システムの場合:

     ```
     dsconf.exe import --unsecured -p 1389 -e ¥temp¥dcequalscom.ldif dc=com
     ```

6. ディレクトリー・サーバーを再始動します。

次のタスク

Oracle Directory Server Enterprise Edition のアクセス・コントロール命令により、匿名読み取りアクセスがアクティブになる場合があります。より安全なデータを提供するには、匿名読み取りアクセスを使用不可にするよう、デフォルトのアクセス・コントロール命令を変更します。詳しくは、Oracle Directory Server Enterprise Edition の資料を参照してください。

他のコンポーネントをインストールして構成します。

IBM Tivoli Directory Integrator のインストール (オプション)

IBM Tivoli Directory Integrator は、アプリケーション間またはディレクトリー・ソース間の情報交換を同期化および管理します。このセクションでは、IBM Security Identity Manager での使用を目的とした IBM Tivoli Directory Integrator のインストールについて説明します。

始める前に

IBM Tivoli Directory Integrator をインストールする前に、以下のステップを完了してください。

- Directory Integrator 製品により提供されるインストール・ガイドを読みます。
- インストールが Directory Integrator のハードウェア要件とソフトウェア要件を満たしていることを確認します。
  - ハードウェア要件とソフトウェア要件、および文書

    http://www.ibm.com/software/sysmgmt/products/support/J958636N88774A05-doc.html
  - フィックス

    http://www.ibm.com/software/sysmgmt/products/support/IBMDirectoryIntegrator.html

このタスクについて

この章の情報は、Directory Integrator 製品そのものによって提供されるより広範囲な前提条件の資料に代わるものではありません。

IBM Tivoli Directory Integrator は、IBM Security Identity Manager と同じコンピューターにも別のコンピューターにもインストールできます。

手順

1. 必要なフィックスパックをインストールします。 ご使用になるバージョンの IBM Tivoli Directory Integrator でフィックスパックが必要な場合は、そのフィックスを取得してインストールします。詳しくは、サポート Web サイトを参照してください。
   - サポート

     http://www.ibm.com/software/sysmgmt/products/support/IBMDirectoryIntegrator.html
   - インフォメーション・センター

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDI.doc/toc.xml

2. エージェントレス・アダプターをインストールします。

   アダプターは、IBM Security Identity Manager と連携してリソースを管理します。エージェント・ベースのアダプターは、管理対象リソースへのアダプターのインストール、および IBM Security Identity Manager サーバーへのアダプター・プロファイルのインストールを必要とします。エージェントレス・アダプターを使用するには、IBM Tivoli Directory Integrator をホストするコンピューターにアダプターをインストールする必要があります。また、IBM Security Identity Manager サーバーにアダプター・プロファイルをインストールする必要があります。

   IBM Tivoli Directory Integrator は、IBM Security Identity Manager と同じコンピューターにインストールすることも、リモート側でインストールすることもできます。IBM Security Identity Manager をローカル側でインストールする場合は、インストール・プログラムによって自動的にエージェントレス・アダプターがインストールされます。エージェントレス・アダプター・プロファイルの自動インストールを選択することもできます。IBM Security Identity Manager をリモート側でインストールする場合は、IBM Tivoli Directory Integrator をホストするコンピューターにエージェントレス・アダプターを手動でインストールする必要があります。エージェントレス・アダプター・プロファイルは、IBM Security Identity Manager をホストするコンピューターに手動でインストールする必要があります。

   注: エージェントレス・アダプターおよびアダプター・プロファイルを*手動で*インストールするには、その前に、IBM Security Identity Manager のインストールが完了するまで待機する必要があります。

次のタスク

エージェントレス・アダプターおよびアダプター・プロファイルをリモート・システムに手動でインストールします。『エージェントレス・アダプターのインストール』および 57 ページの『エージェントレス・アダプター・プロファイルのインストール』を参照してください。

その他のコンポーネントをインストールして構成します。

エージェントレス・アダプターのインストール

IBM Security Identity Manager バージョン 6.0 は Tivoli Directory Integrator バージョン 7.1 をサポートしています。Tivoli Directory Integrator 用のエージェントレス・アダプターは、対話式でもサイレント・モードでもインストールできます。

始める前に

アダプターが正常に機能するためには、以下のコンポーネントをインストールする必要があります。

1. RMI ディスパッチャー
2. POSIX アダプター、UNIX アダプター、または Linux アダプター

このタスクについて

RMI ディスパッチャーと、POSIX アダプター、UNIX アダプター、Linux アダプターの 3 つのうちの 1 つのアダプターは、対話式にインストールすることも、サイレントにインストールすることもできます。POSIX アダプター、UNIX アダプター、または Linux アダプターをインストールする前に、RMI ディスパッチャーを Tivoli Directory Integrator にインストールしておく必要があります。

手順

1. RMI ディスパッチャーを対話式にインストールするには、以下のコマンドを実行します。
   a. Windows オペレーティング・システムの場合は、以下を入力します。

      ```
      cd ISIM_HOME¥config¥adapters
      ```

      その後、以下のテキストを 1 つのコマンドとして入力します。

      ```
      WAS_HOME¥java¥bin¥java.exe -jar DispatcherInstall_70.jar
      ```

   b. UNIX および Linux オペレーティング・システムの場合は、以下を入力します。

      ```
      cd ISIM_HOME/config/adapters
      ```

      その後、以下のテキストを 1 つのコマンドとして入力します。

      ```
      WAS_HOME/java/bin/java -jar DispatcherInstall_70.jar
      ```

2. RMI ディスパッチャーをサイレント・インストールするには、以下のコマンドを実行します。
   a. Windows オペレーティング・システムの場合は、以下を入力します。

      ```
      cd ISIM_HOME¥config¥adapters
      ```

      その後、以下のテキストを 1 つのコマンドとして入力します。

      ```
      "WAS_HOME¥java¥bin¥java.exe" -cp DispatcherInstall_70.jar -i silent
       -DLICENSE_ACCEPTED=TRUE -DUSER_INSTALL_DIR=ITDI_HOME
       -DUSER_SELECTED_SOLDIR=ITDI_HOME¥timsol
       -DUSER_DISPATCHER_SERVICE_NAME="ISIM Adapters"
       -DUSER_INPUT_RMI_PORTNUMBER=1099
       -DUSER_INPUT_WS_PORTNUMBER=8081
      ```

      ここで、1099 および 8081 は、RMI ディスパッチャーが listen しているポートです。

   b. UNIX および Linux オペレーティング・システムの場合は、以下を入力します。

      ```
      cd ISIM_HOME/config/adapters
      ```

      その後、以下のテキストを 1 つのコマンドとして入力します。

      ```
      "WAS_HOME/java/bin/java" -cp DispatcherInstall_70.jar -i silent
       -DLICENSE_ACCEPTED=TRUE -DUSER_INSTALL_DIR=ITDI_HOME
       -DUSER_SELECTED_SOLDIR=ITDI_HOME/timsol
       -DUSER_INPUT_RMI_PORTNUMBER=1099
       -DUSER_INPUT_WS_PORTNUMBER=8081
      ```

      ここで、1099 および 8081 は、RMI ディスパッチャーが listen しているポートです。

3. POSIX アダプター、UNIX アダプター、または Linux アダプターを対話式にインストールするには、以下のコマンドを実行します。
   a. Windows オペレーティング・システムの場合は、以下を入力します。

      ```
      cd ISIM_HOME¥config¥adapters
      ```

      その後、以下のテキストを 1 つのコマンドとして入力します。

      ```
      WAS_HOME¥java¥bin¥java.exe -jar PosixAdapterInstall_70.jar
      ```

   b. UNIX および Linux オペレーティング・システムの場合は、以下を入力します。

      ```
      cd ISIM_HOME/config/adapters
      ```

      その後、以下のテキストを 1 つのコマンドとして入力します。

      ```
      WAS_HOME/java/bin/java -jar PosixAdapterInstall_70.jar
      ```

4. POSIX アダプター、UNIX アダプター、または Linux アダプターをサイレント・インストールするには、以下のコマンドを入力します。
   a. Windows オペレーティング・システムの場合は、以下を入力します。

      ```
      cd ISIM_HOME¥config¥adapters
      ```

      その後、以下のテキストを 1 つのコマンドとして入力します。

      ```
      "WAS_HOME¥java¥bin¥java.exe" -cp PosixAdapterInstall_70.jar -i silent
       -DLICENSE_ACCEPTED=TRUE -DUSER_INSTALL_DIR=ITDI_HOME
      ```

   b. UNIX および Linux オペレーティング・システムの場合は、以下を入力します。

      ```
      cd ISIM_HOME/config/adapters
      ```

      その後、以下のテキストを 1 つのコマンドとして入力します。

      ```
      "WAS_HOME/java/bin/java" -cp PosixAdapterInstall_70.jar -i silent
       -DLICENSE_ACCEPTED=TRUE -DUSER_INSTALL_DIR=ITDI_HOME
      ```

エージェントレス・アダプター・プロファイルのインストール

以下の手順を使用して、エージェントレス・アダプター・プロファイルをインストールします。常にアダプター・ダウンロード・サイトから最新の POSIX アダプターをダウンロードすることをお勧めします。

このタスクについて

エージェントレス・アダプター・プロファイルをインストールするには、Windows、UNIX、または Linux のすべてのオペレーティング・システムでコマンド行を実行します。IBM Security Identity Manager コンソール・ユーザー・インターフェースから「**システムの構成**」 > 「**サービス・タイプの管理**」 > 「**インポート**」を選択することにより、それらをインストールすることもできます。

手順

1. Windows オペレーティング・システムの場合は、以下のコマンドを実行します。

   ```
   cd ISIM_HOME¥config¥adapters "ISIM_HOME/bin/win/config_remote_services.cmd"
    -profile LdapProfile -jar LdapProfile.jar

   "ISIM_HOME/bin/win/config_remote_services.cmd" -profile PosixSolarisProfile -jar
   ```

```
PosixSolarisProfile.jar

"ISIM_HOME/bin/win/config_remote_services.cmd" -profile PosixLinuxProfile -jar
PosixLinuxProfile.jar

"ISIM_HOME/bin/win/config_remote_services.cmd" -profile PosixHpuxProfile -jar
PosixHpuxProfile.jar

"ISIM_HOME/bin/win/config_remote_services.cmd" -profile PosixAixProfile -jar
PosixAixProfile.jar
```

2. UNIX または Linux オペレーティング・システムの場合は、以下のコマンドを実行します。

```
-bash-3.00# cd ISIM_HOME/bin/unix
-bash-3.00# ./config_remote_services.sh -profile LdapProfile -jar /opt/IBM/isim
/config/adapters/LdapProfile.jar

-bash-3.00# ./config_remote_services.sh -profile PosixSolarisProfile -jar /opt
/IBM/isim/config/adapters/PosixSolarisProfile.jar

-bash-3.00# ./config_remote_services.sh -profile PosixLinuxProfile -jar /opt
/IBM/isim/config/adapters/PosixLinuxProfile.jar

-bash-3.00# ./config_remote_services.sh -profile PosixHpuxProfile -jar /opt
/IBM/isim/config/adapters/PosixHpuxProfile.jar

-bash-3.00# ./config_remote_services.sh -profile PosixAixProfile -jar /opt
/IBM/isim/config/adapters/PosixAixProfile.jar
```

WebSphere Application Server のインストールおよび構成

WebSphere Application Server は、セキュアでスケーラブルなアプリケーション・インフラストラクチャーを IBM Security Identity Manager サーバーに提供します。WebSphere Application Server は、単一サーバー環境でもクラスター・サーバー環境でも実行できます。

このセクションでは、IBM Security Identity Manager サーバーをインストールする前に WebSphere Application Server 環境を作成するための一般的なステップについて説明します。これらのステップは、単一サーバー構成とクラスター構成のいずれにも適用されます。 WebSphere Application Server のサポートされるリリースと必要なフィックスパックについては、IBM Security Identity Manager インフォメーション・センターの『*WebSphere Application Server の要件*』を参照してください。

単一サーバー環境への WebSphere Application Server のインストール

WebSphere Application Server バージョン 7 のインストールは、2 段階のプロセスです。

始める前に

WebSphere Application Server をインストールする前に、以下のことを行ってください。

- WebSphere Application Server インストール・ガイドを読みます。
- WebSphere Application Server を単一サーバー環境またはクラスター環境のどちらにインストールするかを決定します。

- システムが製品のハードウェアおよびソフトウェア要件を満たしていることを確認します。
- オペレーティング・システムに必要なフィックスパックがすべて適用されていることを確認します。WebSphere Application Server 向けにオペレーティング・システムを調整する方法について詳しくは、Web サイト『オペレーティング・システムの調整』を参照してください。

WebSphere Application Server のインストールについて詳しくは、以下の Web サイトを参照してください。

- ハードウェアおよびソフトウェア要件:

  ハードウェア要件およびソフトウェア要件
- サポート:

  製品サポート
- インフォメーション・センター:

  WebSphere Application Server バージョン 7.0 インフォメーション・センター

このタスクについて

インストール・プロセスの 2 つのステップは、以下のとおりです。

1. WebSphere Application Server インストール製品を使用して、コア・プロダクト・ファイルの共用セットをインストールします。
2. プロファイルを使用して、複数のアプリケーション・サーバー・ランタイム環境を定義します。これらのプロファイルには、それぞれにコア・ファイルを共有する独自の管理インターフェースがあります。プロファイルは、環境が機能するために必要です。作成できるプロファイルのタイプは以下の 3 つです。

   アプリケーション・サーバー・プロファイル
   このプロファイルは、スタンドアロン・ノードとして、またはデプロイメント・マネージャー・セルの一部として実行できます。

   デプロイメント・マネージャー・プロファイル
   このプロファイルは、アプリケーション・サーバーを集中管理できるようにします。

   カスタム・プロファイル
   このプロファイルは、デプロイメント・マネージャーを使用して、統合してからカスタマイズする必要があります。カスタム・プロファイルは独自の管理コンソールを持っていません。デプロイメント・マネージャー・ノードで管理されます。

   例えば、コア・ファイルがインストールされた後に、1 つ以上のデプロイメント・マネージャー・プロファイル、アプリケーション・サーバー・プロファイル、またはカスタム・プロファイルを作成します。プロファイルは、インストール後に、プロファイル作成ウィザード GUI または **manageprofiles** コマンドを使用していつでも作成できます。

IBM HTTP Server および WebSphere Web サーバー・プラグインをインストールする場合は、追加の構成ステップが必要です。67 ページの『IBM HTTP Server およ

び WebSphere Web サーバー・プラグインのインストールおよび構成 (オプション)』を参照してください。

手順

1. UNIX システムの場合は root ユーザーとして、Windows オペレーティング・システムの場合はアドミニストレーター権限を持つユーザーとして、WebSphere 製品をインストールします。
2. WebSphere Application Server インストール・プログラムを開始します。
3. 「**アプリケーション・サーバー**」プロファイルを選択します。 デフォルトでは、管理セキュリティーがアクティブになっています。管理セキュリティーによって、許可のないユーザーからサーバーが保護されます。
4. WebSphere インストール・プログラムが必要とする追加の値を入力します。
5. インストールが完了したら、製品サポート Web サイト「 サポート・ホーム」から Update Installer for WebSphere Application Server をダウンロードしてインストールします。
6. Update Installer を使用して、サポートされる WebSphere Application Server バージョンを含むサービス・パックをインストールします。IBM Security Identity Manager インフォメーション・センターの『*WebSphere Application Server の要件*』を参照してください。インストールに使用したアカウントと同じオペレーティング・システム管理者アカウントを使用してください。
7. Java Runtime Environment (JRE) バージョン 1.6 SR10 フィックスパック 1 を使用していることを確認します。 WebSphere Application Server フィックスパックの Web サイト「ダウンロード」で、このサービス・リリースをダウンロードし、指示に従って修正を適用できます。
8. WebSphere Application Server フィックスパックを適用したら、WebSphere Application Server を開始します。 以下のいずれかのコマンドを使用します。
   - Windows オペレーティング・システム:

     WAS_PROFILE_HOME¥bin¥startServer.bat *server_name*
   - UNIX または Linux オペレーティング・システム:

     WAS_PROFILE_HOME/bin/startServer.sh *server_name*

   server_name は、WebSphere Application Server の名前です。例えば、server1 です。
9. WebSphere Application Server の「ファースト・ステップ」パネルを開き、「**インストールの検査**」をクリックして、インストールに問題がないことを確認します。 ファースト・ステップを実行するには、以下のいずれかのコマンドを使用します。
   - Windows オペレーティング・システム:

     WAS_PROFILE_HOME¥firststeps¥firststeps.bat
   - UNIX または Linux オペレーティング・システム:

     WAS_PROFILE_HOME/firststeps/firststeps.sh
10. WebSphere Application Server フィックスパックが、正しいレベルであることを確認してください。 以下のいずれかのコマンドを使用します。
    - Windows オペレーティング・システム:

      WAS_PROFILE_HOME¥bin¥versionInfo.bat

- UNIX または Linux オペレーティング・システム:

  WAS_PROFILE_HOME/bin/versionInfo.sh

例えば、WebSphere Application Server ベースのバージョン出力は以下のようになります。

```
Installed Product
-------------------------------------------
Name     IBM WebSphere Application Server
Version  7.0.0.23
ID       BASE
```

11. 以下の Web アドレスを使用して、管理コンソールにアクセスします。

    http://*hostname*:*port*/ibm/console

    hostname の値は、WebSphere Application Server ベース製品をインストールしたコンピューターの完全修飾ホスト名または IP アドレスです。*port* の値は、WebSphere 管理 HTTP トランスポートのポート番号です。デフォルト値は 9060 です。コンピューター上に WebSphere Application Server の別のインスタンスがある場合は、ポート番号は 9060 ではない可能性があります。

12. *WAS_PROFILE_HOME*¥logs¥*server_name* 内の SystemOut.log ファイルと SystemErr.log ファイルを調べて、他に問題がないことを確認します。 詳しくは、 188 ページの『ログ・ファイル』を参照してください。

次のタスク

IBM Security Identity Manager サーバーをインストールします。

クラスター環境への WebSphere Application Server のインストール

クラスター内の各コンピューターに WebSphere Application Server をインストールする必要があります。また、デプロイメント・マネージャーを作成する必要があります。

手順

1. WebSphere Application Server パッケージをインストールします。
2. デプロイメント・マネージャー・プロファイルを作成します。
3. クラスター内の各コンピューターで、以下を実行します。
   a. WebSphere Application Server パッケージをインストールします。
   b. カスタム・プロファイルを作成します。
   c. デプロイメント・マネージャーによって管理されるセルにノードを統合します。

IBM HTTP Server および WebSphere Web サーバー・プラグインをインストールする場合は、追加の構成ステップが必要です。 67 ページの『IBM HTTP Server および WebSphere Web サーバー・プラグインのインストールおよび構成 (オプション)』を参照してください。

WebSphere Application Server デプロイメント・マネージャーのインストール

デプロイメント・マネージャーは、アプリケーション・サーバーを集中管理できるようにします。

手順

1. UNIX システムの場合は root ユーザーとして、Windows オペレーティング・システムの場合はアドミニストレーター権限を持つユーザーとして、WebSphere 製品をインストールします。
2. WebSphere Application Server インストール・プログラムを開始します。
3. 「**デプロイメント・マネージャー**」プロファイルを選択します。 デフォルトでは、管理セキュリティーがアクティブになっています。管理セキュリティーによって、許可のないユーザーからサーバーが保護されます。
4. WebSphere インストール・プログラムが必要とする追加の値を入力します。
5. インストールが完了すると、「ファースト・ステップ」パネルが開きます。「**インストール検査**」をクリックして、インストールに問題がないかどうかを確認します。
   - Windows オペレーティング・システム:

     ```
     WAS_NDM_PROFILE_HOME¥firststeps¥firststeps.bat
     ```
   - UNIX または Linux オペレーティング・システム:

     ```
     WAS_NDM_PROFILE_HOME/firststeps/firststeps.sh
     ```
6. 製品サポート Web サイトから Update Installer for WebSphere Application Server をダウンロードしてインストールします。
7. Update Installer を使用して、サポートされる WebSphere Application Server バージョンを含むサービス・パックをインストールします。IBM Security Identity Manager インフォメーション・センターの『WebSphere Application Server の要件』を参照してください。インストールに使用したアカウントと同じオペレーティング・システム管理者アカウントを使用してください。
8. IBM Java 2 Platform Standard Edition Development Kit 1.5 Service Release 6 以降を使用していることを確認してください。IBM Java のサービス・リリース・レベルを確認するには、以下のコマンドを実行します。
   - Windows オペレーティング・システム:

     ```
     <WAS_NDM_PROFILE_HOME>¥java¥bin¥java.exe -version
     ```
   - UNIX または Linux オペレーティング・システム:

     ```
     <WAS_NDM_PROFILE_HOME>/java/bin/java -version
     ```

   Java 2 セキュリティーをアクティブにする場合は、Service Release 6 が必要です。WebSphere Application Server フィックスパックの Web サイト「ダウンロード」で、このサービス・リリースをダウンロードし、指示に従って修正を適用できます。
9. WebSphere Application Server フィックスパックを適用したら、デプロイメント・マネージャーを開始します。 以下のいずれかのコマンドを使用します。
   - Windows オペレーティング・システム

     ```
     WAS_NDM_PROFILE_HOME¥bin¥startManager.bat
     ```
   - UNIX または Linux オペレーティング・システム

WAS_NDM_PROFILE_HOME/bin/startManager.sh

10. WebSphere Application Server フィックスパックが、正しいレベルであることを確認してください。 以下のいずれかのコマンドを使用します。
    - Windows オペレーティング・システム
      - クラスター・メンバー

        WAS_PROFILE_HOME¥bin¥versionInfo.bat
      - デプロイメント・マネージャー

        WAS_NDM_PROFILE_HOME¥bin¥versionInfo.bat
    - UNIX または Linux オペレーティング・システム
      - クラスター・メンバー

        WAS_PROFILE_HOME/bin/versionInfo.sh
      - デプロイメント・マネージャー

        WAS_NDM_PROFILE_HOME/bin/versionInfo.sh

    例えば、WebSphere Application Server ベースのバージョン出力は以下のようになります。
    - WebSphere Application Server ベース

      ```
      Installed Product
      ------------------------------------------------
      Name     IBM WebSphere Application Server
      Version  7.0.0.23
      ID       BASE
      ```
    - デプロイメント・マネージャー

      ```
      Installed Product
      ------------------------------------------------
      Name     IBM WebSphere Application Server Deployment Manager
      Version  7.0.0.23
      ID       ND
      ```
11. 以下の Web アドレスを使用して、管理コンソールにアクセスします。

    http://*hostname*:*port*/ibm/console

    hostname の値は、WebSphere Application Server ベース製品をインストールしたコンピューターの完全修飾ホスト名または IP アドレスです。*port* の値は、WebSphere 管理 HTTP トランスポートのポート番号です。デフォルト値は 9060 です。コンピューター上に WebSphere Application Server の別のインスタンスがある場合は、ポート番号は 9060 ではない可能性があります。
12. *WAS_NDM_PROFILE_HOME*¥logs¥*dm_server_name* ディレクトリーの SystemOut.log and SystemErr.log ファイルおよび SystemErr.log ファイルを調べ、他に問題がないことを確認します。

次のタスク

各ノード・メンバーに WebSphere Application Server をインストールします。

各ノード・メンバーへの WebSphere Application Server 製品のインストール

各クラスター・メンバー・ホストに WebSphere Application Server をインストールし、各ノード・メンバーをセルに統合します。

手順

1. UNIX システムの場合は root ユーザーとして、Windows オペレーティング・システムの場合はアドミニストレーター権限を持つユーザーとして、WebSphere 製品をインストールします。
2. WebSphere Application Server インストール・プログラムを開始します。
3. 「**カスタム**」プロファイルを選択します。
4. 「**統合**」パネルで、以下のフィールドに入力します。
   a. デプロイメント・マネージャーのホスト名または IP アドレスを入力します。
   b. デプロイメント・マネージャーの SOAP ポートを入力するか、またはデフォルト・ポートを受け入れます。
   c. 管理セキュリティーが使用可能である場合は、デプロイメント・マネージャー管理ユーザー名およびパスワードを入力します。
5. インストールが完了したら、製品サポート Web サイトから Update Installer for WebSphere Application Server をダウンロードしてインストールします。
6. Update Installer を使用して、サポートされる WebSphere Application Server バージョンを含むサービス・パックをインストールします。IBM Security Identity Manager インフォメーション・センターの『ソフトウェア*前提条件*』を参照してください。インストールに使用したアカウントと同じオペレーティング・システム管理者アカウントを使用してください。
7. IBM Java 2 Platform Standard Edition Development Kit 1.5 Service Release 6 以降を使用していることを確認してください。IBM Java のサービス・リリース・レベルを確認するには、以下のコマンドを実行します。
   - Windows オペレーティング・システム:

     ```
     <WAS_NDM_PROFILE_HOME>¥java¥bin¥java.exe -version
     ```
   - UNIX または Linux オペレーティング・システム:

     ```
     <WAS_NDM_PROFILE_HOME>/java/bin/java -version
     ```

   Java 2 セキュリティーを使用可能にする場合は、Service Release 6 が必要です。WebSphere Application Server フィックスパックの Web サイト「ダウンロード」で、このサービス・リリースをダウンロードし、指示に従って修正を適用できます。
8. WebSphere Application Server フィックスパックを適用したら、WebSphere Application Server を開始します。 以下のいずれかのコマンドを使用します。
   - Windows オペレーティング・システム:

     ```
     WAS_PROFILE_HOME¥bin¥startServer.bat
     ```
   - UNIX または Linux オペレーティング・システム:

     ```
     WAS_PROFILE_HOME/bin/startServer.sh
     ```
9. WebSphere Application Server の「ファースト・ステップ」パネルを開き、「**インストールの検査**」をクリックして、インストールに問題がないことを確認します。 ファースト・ステップを実行するには、以下のいずれかのコマンドを使用します。
   - Windows オペレーティング・システム:

     ```
     WAS_PROFILE_HOME¥firststeps¥firststeps.bat
     ```

- UNIX または Linux オペレーティング・システム:

  WAS_PROFILE_HOME/firststeps/firststeps.sh

次のタスク

セル内のノードの統合を検証します。

WebSphere Application Server ノード・メンバーの手動での統合

インストール時に、カスタム・プロファイルを使用したがノードをセルに統合しなかった場合、またはノード・メンバーが統合されないベース WebSphere Application Server プロファイルを作成した場合は、このステップをオプションで実行します。

始める前に

クラスター内の各コンピューターで、デプロイメント・マネージャーの作成と WebSphere Application Server のインストールが終了していることを確認してください。

手順

addnode コマンドで、パラメーター **username dmgr_admin_user_id** および **password dmgr_admin_user_id** を追加します。以下のいずれかのコマンドを実行します。

- Windows オペレーティング・システム:

  WAS_HOME¥bin¥addNode.bat *dmgr_host portnumber* -profileName *profile_name* -username *dmgr_admin_user_id* -password *dmgr_admin_user_id*

- UNIX または Linux オペレーティング・システム:

  WAS_HOME/bin/addNode.sh *dmgr_host portnumber* -profileName *profile_name* -username *dmgr_admin_user_id* -password *dmgr_admin_user_id*

WAS_HOME の値は、WebSphere Application Server コア・ファイルがインストールされている WebSphere Application Server ホーム・ディレクトリーの場所です。*dmgr_host* パラメーターは、デプロイメント・マネージャーがインストールされているコンピューターのホスト名です。*portnumber* パラメーターは、デプロイメント・マネージャーに割り当てられている SOAP ポート番号を指定します。デフォルトのポート番号は 8887 です。
ノードがセルに正常に追加された後にノード・エージェントが作成され、開始します。

次のタスク

セル内のノードの統合を検証します。

セル内のノードの統合の検証

セル内でノード・メンバーを統合した後に、ノードが正しく実行されていることを検証する必要があります。

始める前に

ノード・メンバーを統合するために必要なステップが完了していることを確認してください。

手順

1. 以下の Web アドレスを使用して、管理コンソールにアクセスします。

   `http://hostname:port/ibm/console`

   hostname の値は、WebSphere Application Server デプロイメント・マネージャーの完全修飾ホスト名または IP アドレスのいずれかです。*port* の値は、WebSphere 管理 HTTP トランスポートのポート番号です。デフォルト値は 9060 です。コンピューター上に WebSphere Application Server の別のインスタンスがある場合は、ポート番号は 9060 ではない可能性があります。
2. Integrated Solutions Console のルート構造から「**システム管理**」をクリックします。
3. 「ノード」をクリックします。 マネージャー・ノードおよび統合されたノードがリストされていて、使用可能であることを確認します。「**Nodeagent**」をクリックして、すべてのノード・エージェントの状況を確認することもできます。

次のタスク

IBM Security Identity Manager の WebSphere クラスターを作成します。

IBM Security Identity Manager アプリケーション用の WebSphere クラスターの作成

WebSphere Application Server 環境に 2 つのサーバー・クラスターを作成する必要があります。1 つのクラスターは、IBM Security Identity Manager アプリケーションをホストします。もう 1 つのクラスターは、メッセージング・サービスとして使用されます。

始める前に

クラスターを作成する前に、すべてのノード・エージェントが実行中であることを確認してください。

手順

1. 以下の Web アドレスを使用して、管理コンソールにアクセスします。

   `http://hostname:port/ibm/console`

   hostname の値は、WebSphere Application Server デプロイメント・マネージャーの完全修飾ホスト名または IP アドレスのいずれかです。*port* の値は、WebSphere 管理 HTTP トランスポートのポート番号です。デフォルト値は 9060 です。コンピューター上に WebSphere Application Server の別のインスタンスがある場合は、ポート番号は 9060 ではない可能性があります。
2. Integrated Solutions Console のルート構造から「**サーバー**」をクリックします。
3. 「**クラスター**」 > 「**WebSphere Application Server クラスター**」をクリックします。
4. ホスト・アプリケーション・クラスターの名前を指定します。 例えば、`ITIM_Application_Cluster` です。クラスター名は、セル内で固有でなければなりません。
5. デフォルトのチェック・ボックス設定値を使用し、「**次へ**」をクリックします。

6. 最初のクラスター・メンバーのメンバー名を指定します。
7. 最初のクラスター・メンバーをホストするために使用するノードを指定します。
8. 「**アプリケーション・サーバー・テンプレートを使用してメンバーを作成します**」をクリックし、「**デフォルト**」を選択します。
9. その他のデフォルト設定はすべて変更せずに「**次へ**」をクリックします。
10. トポロジー内のサーバーごとにクラスター・メンバーを作成します。`ITIM_Application_Cluster` に対して、各ノードに少なくとも 1 つのサーバーを作成する必要があります。使用可能なリソースがあり、かつ垂直クラスター・トポロジーを使用したい場合は、各ノードに複数のサーバーを定義できます。
    a. メンバー名を指定し、ノードを選択します。
    b. 「**メンバーの追加**」をクリックします。
    c. クラスター・メンバーの追加が終了したら、「**次へ**」をクリックします。
11. 情報の要約を確認し、「**完了**」をクリックします。
12. メッセージング・クラスターに対してこのプロセスを繰り返します。メッセージング・クラスターおよびクラスター・メンバーには、`ITIM_Messaging_Cluster` など、固有の名前を指定します。少なくとも 2 つのアプリケーション・サーバーを別々のノードに定義します。
13. 2 番目のクラスターの作成が終了したら、Integrated Solutions Console のルート構造から「**サーバー**」をクリックします。
14. 「**クラスター**」をクリックして、ご使用のクラスターが表示されることを確認します。
15. 各クラスターの名前をクリックし、「**クラスター・メンバー**」をクリックして各クラスター・メンバーに関する詳細情報を表示します。

次のタスク

IBM Security Identity Manager Server をインストールします。

IBM HTTP Server および WebSphere Web サーバー・プラグインのインストールおよび構成 (オプション)

デプロイメント・マネージャーを備えた同一のコンピューターに IBM HTTP Server と WebSphere Web サーバー・プラグインをインストールすることが可能です。ただし、セキュリティーの向上およびロード・バランシングのために、IBM HTTP Server と WebSphere Web サーバー・プラグインは、別々のコンピューターにインストールするのがよいでしょう。

IBM HTTP Server

IBM HTTP Server のインストールについては、IBM HTTP Server for WebSphere Application Server の製品資料を IBM WebSphere Application Server インフォメーション・センターで参照してください。

WebSphere Web Server プラグイン

WebSphere Web サーバー・プラグインのインストールについては、WebSphere Application Server Network Deployment バージョン 7.0 インフォメーション・センターの『*Web サーバー・プラグインのインストール (Installing Web server plug-ins)*』を参照してください。

HTTP サーバーを使用する場合、管理コンソールを使用して、IBM Security Identity Manager アプリケーションを HTTP Web サーバー名にマップする必要があります。マッピング手順については、139 ページの『IBM Security Identity Manager アプリケーションのマッピング』を参照してください。

WebSphere Application Server のパフォーマンス調整タスク

最初に WebSphere Application Server を構成した後にパフォーマンスの問題が発生する場合があります。以下のタスクでは、WebSphere Application Server を正常に稼働させるために実行するアクションについて説明します。

Performance Monitoring Infrastructure (PMI) トラッキングを使用不可にする

WebSphere Application Server では、デフォルトで Performance Monitoring Infrastructure (PMI) が使用可能となり、基本レベルに設定されます。このレベルでは、URIRequestCount モニターおよび URIServiceTime monitoring モニターが使用可能です。これらが使用可能になっていると、Console GUI を使用するときに、そのインターフェース用に固有の URL が生成されるため、パフォーマンス上の問題が発生します。

始める前に

WebSphere Application Server がシステムに正しくインストールされていることを確認してください。

このタスクについて

パフォーマンスの低下を防ぐには、PMI を完全に使用不可にするか、または以下の特定の PMI フラグを使用不可にします。

手順

1. 管理コンソールにログオンします。
2. 左のナビゲーション・ペインから、「**モニターおよびチューニング**」 > 「**Performance Monitoring Infrastructure (PMI)**」をクリックします。
3. 管理するサーバーの名前をクリックします。
4. 「**カスタム**」を選択し、「**カスタム**」リンクをクリックします。
5. ツリー・リストから「**Web アプリケーション**」を選択します。
6. 「**URIConcurrentRequests**」を選択します。
7. 「**URIRequestCount**」を選択します。
8. 「**URIServiceTime**」を選択します。
9. ペインの上部で、「**使用不可にする**」をクリックします。

10. 「**保存**」をクリックして構成を保存します。
11. IBM Security Identity Manager を実行する各アプリケーション・サーバーに対してこの手順を繰り返します。
12. すべてのアプリケーション・サーバーを再始動し、変更を有効にします。

次のタスク

追加の調整を行います。

WebSphere Application Server での TCP KeepAlive 設定値の変更

メッセージング・エンジンのフェイルオーバー設計は、メッセージング・エンジンのインスタンスに障害が発生したときにデータベース接続が切断されることに依存しています。高可用性環境でフェイルオーバーが発生するためには、システムが、切断された接続のタイムリーな認識とデータベース・ロックの解放を確実に行うようにします。この作業は、TCP KeepAlive 設定値を構成することにより行うことができます。

始める前に

WebSphere Application Server をご使用のシステムに正しくインストールする必要があります。

手順

1. システム管理者としてログインします。
2. 以下のコマンドを実行します。

   ```
   echo 30 >  /proc/sys/net/ipv4/tcp_keepalive_intvl
   ```

   注: これらの設定値は、IPv6 インプリメンテーションによっても使用されます。
3. `tcp_keepalive_intvl` ファイルで値が 30 になっているかを調べて、更新を確認します。

次のタスク

追加の調整を行います。

外部ユーザー・レジストリーを使用した認証のためのインストール前の構成

IBM Security Identity Manager は、外部ユーザー・レジストリーを使用した認証をサポートしています。製品をインストールする前に、レジストリーを構成する必要があります。

WebSphere Application Server ユーザー・レルムとして構成可能なすべてのユーザー・レジストリーは、IBM Security Identity Manager の認証ユーザー・レジストリーとして使用できます。 WebSphere Application Server でサポートされるユーザー・レルムのタイプは、フェデレーテッド・リポジトリー、ローカル・オペレーティング・システム、スタンドアロン LDAP レジストリー、およびカスタム LDAP

レジストリーの 4 つです。この資料で説明する構成例では、スタンドアロン LDAP ユーザー・レジストリーを使用しています。

注: WebSphere Application Server ユーザー・レルムについて詳しくは、WebSphere Application Server インフォメーション・センターを参照してください。

外部ユーザー・レジストリーを IBM Security Identity Manager の認証レジストリーとして使用するには、以下のタスクを実行します。

1. 外部ユーザー・レジストリーから情報を収集します。
2. 必要なユーザーを外部ユーザー・レジストリーに追加します。
3. WebSphere セキュリティー・ドメインを構成します。

外部ユーザー・レジストリーからの情報の収集

必須ユーザーを追加してセキュリティー・ドメインを構成する場合に使用する構成設定を、外部ユーザー・レジストリーから収集する必要があります。

手順

1. まだユーザー・レジストリーをインストールしていない場合は、インストールおよび構成を完了してください。

   インストールおよび構成の正確な手順は、ユーザー・レジストリー製品ごとに固有です。例えば、LDAP レジストリーの場合は、接尾部、ドメイン、ユーザー・テンプレート、およびユーザー・レルムを作成する必要があります。IBM Tivoli Directory Server ユーザー・レジストリーの例については、305 ページの『付録 A. 外部ユーザー・レジストリーとしてのユーザー・レジストリーの構成』を参照してください。
2. WebSphere セキュリティー・ドメインの構成に必要な情報を収集します。

   例えば、LDAP ユーザー・レジストリーの場合は、以下のようにします。

表 4. WebSphere セキュリティー・ドメインの構成に必要なユーザー・レジストリー構成の設定

設定	例
LDAP サーバー・ホストの IP アドレス	ご使用のホストの IP アドレス
LDAP サーバーのポート・アドレス	ご使用の LDAP サーバー・ポート
バインド・ユーザー名およびパスワード	cn=root / secret
ユーザー・リポジトリーの基本 DN	dc=mycorp
ユーザーのオブジェクト・クラス名	InetOrgPerson
ユーザーの相対名前属性	uid
グループのオブジェクト・クラス名	groupOfNames および groupOfUniqueNames
グループ・メンバーシップの属性名	member および uniqueMember

外部ユーザー・レジストリーへの必要なユーザーの追加

必要なユーザーを外部ユーザー・レジストリーに追加する必要があります。

このタスクについて

IBM Security Identity Manager では、2 つのアカウントが存在する必要があります。

表 5. 必要なユーザーのデフォルトのアカウント名

アカウント使用	デフォルトのアカウント名
デフォルトの管理ユーザー	ITIM Manager
デフォルトのシステム・ユーザー	isimsystem

アカウントごとに異なるアカウント名を使用することを選択できます。既存の外部ユーザー・レジストリーで管理ユーザー・アカウント名またはシステム・ユーザー・アカウント名を既に使用している場合は、異なるアカウント名を使用するのがよいでしょう。アカウント名のスペースがオペレーティング・システムでサポートされていない場合は、管理ユーザーに異なるアカウント名を使用するのがよいでしょう。例えば、ユーザー・レジストリーが Linux システム上にある場合は、ITIM Manager ではなく、itimManager というアカウント名を指定するのがよいでしょう。

ユーザーを作成する正確なステップは、ユーザー・レジストリーのタイプに応じて異なります。必要なユーザーを IBM Tivoli Directory Server レジストリーに追加するには、**ldapadd** コマンドを使用します。

コマンド行を使用して、以下のコマンドを発行します。

```
ldapadd -D Bind DN -w Bind PW -p Port -f filename
```

例:

```
ldapadd -D cn=root -w root -p 389 -f filename
```

ここで、*filename* には、以下の詳細情報が含まれます。

```
dn:cn=ITIM Manager,dc=com
objectclass:person
objectclass:inetOrgPerson
cn:System Administrator
sn:Administrator
uid:ITIM Manager
userpassword:secret

dn:cn=isimsystem,dc=com
objectclass:person
objectclass:inetOrgPerson
cn:isimsystem
sn:isimsystem
uid:isimsystem
userpassword:isimsystem
```

別の方法として、IBM Tivoli Directory Server Web 管理ツールを使用して必要なユーザーを追加する方法を以下の手順で説明します。

手順

1. IBM Tivoli Directory Server Web 管理ツールにログオンします。

2. ナビゲーション・ツリーから「**ディレクトリー管理**」>「**項目の追加**」をクリックして、「項目の追加」ページの「オブジェクト・クラスの選択」タブを開きます。
3. 「**構造オブジェクト・クラス**」リストから「**inetOrgPerson**」を選択します。
4. 「**次へ**」をクリックして、「補助オブジェクト・クラスの選択」タブを開きます。
5. 「補助オブジェクト・クラスの選択」タブで「**次へ**」をクリックして、「必要な属性」タブを開きます。
6. 以下の属性の値を「必要な属性」タブで指定します。
   - **相対 DN**
   - **親 DN**
   - **cn**
   - **sn**

   デフォルトの管理ユーザー ID (uid) ITIM Manager とデフォルトのシステム・ユーザー ID (uid) isimsystem を使用することも、別の uid を指定することもできます。以下の表は、デフォルトの管理ユーザー ID、またはデフォルトのシステム・ユーザー ID を使用するときの、必要な属性のエントリーの例を示しています。

表 6. デフォルトの管理ユーザーおよびデフォルトのシステム・ユーザーのアカウントに必要な名前属性のエントリーの例

属性	デフォルトの管理ユーザーの値の例	デフォルトのシステム・ユーザーの値の例
相対 DN	cn=ITIM Manager	cn=isimsystem
親 DN	dc=com	dc=com
cn	システム管理者	isimsystem
sn	Administrator	isimsystem

7. 「**次へ**」をクリックして、「オプションの属性」タブを開きます。
8. 以下の属性の値を「オプションの属性」タブで指定します。
   - **uid**
   - **userPassword**

   例えば、以下の表に示すオプションの属性値を指定します。

表 7. デフォルトの管理ユーザーおよびデフォルトのシステム・ユーザーのアカウントのオプションの属性値

属性	デフォルトの管理ユーザーの値の例	デフォルトのシステム・ユーザーの値の例
uid	ITIM Manager	isimsystem
userPassword	ITIM Manager アカウントのデフォルトのパスワードは、 secret です。任意のパスワードを指定できます。	isimsystem アカウントのデフォルトのパスワードは、 secret です。任意のパスワードを指定できます。

9. 「**終了**」をクリックします。

次のタスク

『WebSphere セキュリティー・ドメインの構成』に進みます。

WebSphere セキュリティー・ドメインの構成

WebSphere Application Server は、さまざまなセキュリティー構成を使用する柔軟性を有するセキュリティー・ドメインをサポートします。

このタスクについて

異なるアプリケーションに対して異なるセキュリティー属性 (例えば、UserRegistry) を使用するように、WebSphere Application Server を構成できます。この構成例では、スタンドアロン LDAP ユーザー・レジストリーを使用して IBM Security Identity Manager のセキュリティー・ドメインを作成します。

以下のいずれかの条件が適用される場合は、次の手順をスキップできます。

- WebSphere Application Server グローバル・セキュリティーを、IBM Security Identity Manager 認証に使用するユーザー・レジストリーを指定して既に構成済みである。
- WebSphere Application Server のセキュリティー・ドメインを、IBM Security Identity Manager 認証に使用するユーザー・レジストリーを指定して既に構成済みである。

注: IBM Security Identity Manager のインストール中に、アプリケーション・サーバー用の既存のレルムを使用することを選択できます。

手順

1. 管理者として管理コンソールにログオンします。
2. 「**セキュリティー**」>「**セキュリティー**」ドメインに進みます。「**新規**」をクリックして、IBM Security Identity Manager のセキュリティー・ドメインを作成します。
3. 「**名前**」フィールドに、使用したい名前を入力します。「**OK**」をクリックして、変更を保存します。
4. 新規セキュリティー・ドメインが作成された後で、セキュリティー・ドメイン名をクリックしてドメインのセキュリティー属性を構成します。
5. セキュリティー・ドメイン名をクリックすると、「セキュリティー・ドメイン」ページが表示されます。複数の設定値を構成する必要があります。「割り当て済み有効範囲」セクションで、IBM Security Identity Managerのインストール先の WebSphere アプリケーション・サーバーを選択します。
6. 「セキュリティー属性」セクションで以下を実行します。
   a. 「アプリケーション・セキュリティー」で、「**アプリケーション・セキュリティーを有効にする**」をクリックします。
   b. Java 2 セキュリティーについては、パフォーマンスを最適化するためにデフォルトの「**使用不可**」を受け入れます。
   c. 「ユーザー・レルム」で、「**スタンドアロン LDAP レジストリー**」を選択して「**構成...**」をクリックします。

7. 「スタンドアロン LDAP レジストリー」ページで、以下の表に示した値を指定します。

表 8. スタンドアロン LDAP レジストリーのセキュリティー・ドメイン構成

フィールド	説明
レルム名	使用したいレルム名を指定します。
LDAP サーバーのタイプ:	この例では、IBM Tivoli Directory Server
ホスト	IBM Tivoli Directory Server のホスト名または IP アドレス
ポート	IBM Tivoli Directory Server の LDAP サーバー・ポート
基本 DN	LDAP レジストリーの基本 DN
バインド DN	LDAP レジストリーにバインドするユーザー DN
バインド・パスワード	バインド・ユーザーのパスワード。

8. **「接続のテスト」**をクリックして、WebSphere が LDAP レジストリーと通信可能であることを確認します。
9. 接続テストが正常に行われたら、**「OK」**をクリックして変更を保存します。
10. ユーザー・レルムの基本セキュリティー属性が構成されたら、このユーザー・レルムの拡張 LDAP 設定値を設定します。
    a. セキュリティー・ドメイン名をクリックします。
    b. **「構成」** (レルム名の横にある) をクリックします。
    c. 「スタンドアロン LDAP レジストリー属性の設定 (Set Advanced Lightweight Directory Access Protocal (LDAP) user registry setting)」ページの**「拡張 Lightweight Directory Access Protocal (LDAP) ユーザー・レジストリー設定値の設定 (Set Advanced Lightweight Directory Access Protocal (LDAP) user registry setting)」**リンクを選択します。
11. **「OK」**をクリックして、変更を保存します。「スタンドアロン LDAP レジストリー」ページから、**「OK」**をクリックして変更を保存します。
12. 変更を保存すると、ドメインのリスト・ページにリダイレクトされます。このドメインの残りのセキュリティー属性の構成を続行するには、ドメイン名を選択します。

    デフォルトの設定値を確認し、ご使用のデプロイメントに適用する設定を変更します。
13. **「OK」**をクリックして、変更を保存します。
14. WebSphere Application Server を再始動します。

タスクの結果

WebSphere セキュリティー・ドメインの構成が完了しました。これで、 IBM Security Identity Manager をインストールすることができます。

第 5 章 IBM Security Identity Manager サーバーのインストール

IBM Security Identity Manager サーバーは、単一サーバー環境とクラスター環境のどちらでもインストールおよび構成することが可能です。

それをサイレント・モードでインストールおよび構成することもできます。詳しくは、111 ページの『第 6 章 サイレント・インストールとサイレント構成』を参照してください。

プリインストール・ワークシート

以下の表は、一般的なプリインストール構成パラメーターを示しています。

表 9. プリインストール・ワークシート

フィールド名	説明	デフォルトまたは例の値	ご使用の値
ISIM_HOME	IBM Security Identity Manager サーバーのインストール・ディレクトリー	**Windows オペレーティング・システム:** *path*¥IBM¥isim **UNIX または Linux オペレーティング・システム:** *path*/IBM/isim	
WAS_HOME	WebSphere Application Server サーバーのインストール・ディレクトリー	**Windows オペレーティング・システム:** *path*¥IBM¥WebSphere¥AppServer **UNIX または Linux オペレーティング・システム:** *path*/IBM/WebSphere/AppServer	
WebSphere Application Server プロファイル名	WebSphere Application Server プロファイルの名前。	**単一サーバー:** AppSrv01 **デプロイメント・マネージャー:** Dmgr01 **クラスター・メンバー:** Custom01	
WebSphere Application Server サーバー名	WebSphere Application Server の名前。	**例:** server1	
Computer host name (コンピューター・ホスト名)	コンピューターのホスト名。		

表 9. プリインストール・ワークシート (続き)

フィールド名	説明	デフォルトまたは例の値	ご使用の値
WebSphere Application Server 管理者ユーザー ID	WebSphere Application Server の管理に使用されるユーザー名。WebSphere Application Server を再始動するために使用されます。このフィールドはオプションです。	**例:** `wsadmin`	
WebSphere Application Server 管理者パスワード	WebSphere ユーザー名で使用されるパスワード。このフィールドはオプションです。		
鍵ストア・パスワード	IBM Security Identity Manager 機密データの暗号化に使用される暗号鍵を保管する IBM Security Identity Manager 鍵ストア・ファイルのアンロックに使用されます。		
ITDI_HOME	IBM Tivoli Directory Integrator サーバーのコードが保管され、アダプターがインストールされるディレクトリー。このフィールドは、IBM Tivoli Directory Integrator を使用しているかに応じて、任意指定です。	**Windows オペレーティング・システム:** *path*¥IBM¥TDI¥V7.1 **UNIX または Linux オペレーティング・システム:** *path*/IBM/TDI/V7.1	
TIVOLI_COMMON_DIRECTORY	すべての保守関連ファイル (ログ、初期エラー・キャプチャー・データなど) の中央保管場所。	**Windows オペレーティング・システム:** *path*¥IBM¥tivoli¥common **UNIX または Linux オペレーティング・システム:** *path*/IBM/tivoli/common	

表 9. プリインストール・ワークシート (続き)

フィールド名	説明	デフォルトまたは例の値	ご使用の値
アプリケーション・クラスター名	ターゲットの WebSphere Application Server セルで定義されたアプリケーション・クラスター名。	*isim_application_cluster*	
メッセージング・クラスター名	ターゲットの WebSphere Application Server セルで定義されたメッセージング・クラスター名。	*isim_messaging_cluster*	

注: IBM Security Identity Manager を Red Hat Linux サーバーにインストールする場合は、以下のステップを実行します。

1. インストールの前に Security Enhanced Linux (SEL) が無効になっていることを確認します。SEL のデフォルト・ポリシー制約により、インストーラーが失敗する場合があります。
   - Security Enhanced Linux がインストールされており、制約モードで実行されているかどうかを確認するには、**sestatus** コマンドを実行するか、`/etc/sysconfig/selinux` ファイルを確認します。
   - SEL を無効にするには、SEL を許可モードに設定し、スーパーユーザーとして **setenforce 0** コマンドを実行するか、`/etc/sysconfig/selinux` ファイルを変更してシステムをリブートします。
2. インストールの前に、必要なパッケージがシステムにインストールされていることを確認します。以下のそれぞれのパッケージについて `rpm -qa | grep` *package_name* コマンドを実行して、これらが適切にインストールされていることを確認します。IBM Security Identity Manager とその前提条件ミドルウェアを正常にインストールするためには、これらのパッケージがシステム上に存在する必要があります。

   Red Hat Enterprise Linux 6 の場合:

   compat-libstdc++-33-3.2.3-69

   compat-db-4.6.21-15

   libXp-1.0.0-15.1

   libXmu-1.0.5-1

   libXtst-1.0.99.2-3

   pam-1.1.1-4

   libXft-2.1.13-4.1

   gtk2-2.18.9-4

   gtk2-engines-2.18.4-5

インストール・ロードマップ

インストール・プロセスは、IBM Security Identity Manager サーバーのインストール、構成、および検証という各アクティビティーから構成されます。

IBM Security Identity Manager サーバーをインストールしてテストするタスクには、以下の作業が含まれます。

1. 以下のいずれかの構成に基づく IBM Security Identity Manager サーバーのインストール。
   - 単一サーバー・インストール。IBM Security Identity Manager は、通常のインストールとサイレント・インストールの両方をサポートします。単一サーバー・インストールについて詳しくは、 80 ページの『単一サーバー環境への IBM Security Identity Manager サーバーのインストール』を参照してください。
   - クラスター・インストール。IBM Security Identity Manager は、通常のインストールとサイレント・インストールの両方をサポートします。クラスター・インストールについて詳しくは、 94 ページの『クラスター環境への IBM Security Identity Manager のインストール』を参照してください。

   注: IBM Security Identity Manager の既存のインストールをアップグレードするステップについては、 237 ページの『第 15 章 IBM Security Identity Manager のアップグレード』を参照してください。

   IBM Security Identity Manager のサイレント・インストールのステップについては、 111 ページの『第 6 章 サイレント・インストールとサイレント構成』を参照してください。
2. IBM Security Identity Manager サーバーとそのコンポーネントが正しくインストールされているかどうかの検証。 121 ページの『第 7 章 インストールの検証』を参照してください。
3. IBM Security Identity Manager の構成。 135 ページの『第 9 章 IBM Security Identity Manager サーバーの構成』を参照してください。
4. インストールおよび始動時に問題が発生した場合は、そのトラブルシューティング。詳しくは、 173 ページの『第 10 章 トラブルシューティング』を参照してください。

ワークシート

以下の表は、一般的なシステム構成パラメーターを示しています。

インストール・ワークシート

フィールド名	説明	デフォルトまたは例の値	ご使用の値
Heart beat (seconds) (ハートビート (秒数))	処理するイベント (ハートビート) についてスケジューリング・スレッドが予定メッセージ・ストアに照会する頻度を定義します。	30	

フィールド名	説明	デフォルトまたは例の値	ご使用の値
Recycle bin age limit (days) (リサイクル・ビン経過日数限界 (日数))	クリーンアップ・スクリプトによってオブジェクトを削除できるようになるまで、システムのリサイクル・ビンに保持しておく日数を指定します。	62	
Maximum pool size (最大プール・サイズ)	LDAP 接続プールが任意の時点で持つことができる接続の最大数を指定します。	100	
Initial pool size (初期プール・サイズ)	LDAP 接続プール用に作成される接続の数の初期値を指定します。	50	
Increment count (増分カウント)	すべての接続が使用中になっているときに接続が要求される場合の、LDAP 接続プールに追加される接続数を指定します。	3	
Database pool initial capacity (データベース・プール初期容量)	JDBC 接続の数の初期値を指定します。	5	
Database pool maximum capacity (データベース・プール最大容量)	IBM Security Identity Manager サーバーが任意の時点で開くことができる、データベースへの JDBC 接続の最大数を指定します。	50	
Logging trace level (ロギング・トレース・レベル)	ログ・ファイルに書き込まれる情報量を指定します。	MIN	
IBM Security Identity Manager ベース・サーバーの URL	IBM Security Identity Manager サーバーの公開済みログイン Universal Resource Locator (URL) を指定します。これは、実行時にメール・メッセージの受信側に送信される URL の最初の部分です。	例: `http://hostname:9080/itim/console`	
メール発信元	サイトの IBM Security Identity Manager システム管理者の電子メール・アドレスを指定します。	例: `admin@mysite.com`	
Mail server name (メール・サーバー名)	電子メール通知を送信しメール・ゲートウェイとして機能する SMTP メール・ホストを指定します。	例: `smtp.mysite.com`	

インストール・ワークシート

フィールド名	説明	デフォルトまたは例の値	ご使用の値
Customer logo (カスタマー・ロゴ)	ロゴ・グラフィックのパスとファイル名を指定します。	ibm_banner.gif	
Customer logo link (カスタマー・ロゴ・リンク)	ロゴ・イメージをクリックすることによって、活動化されるオプションの URL リンクを指定します。	www.ibm.com	
List page size (リストのページ・サイズ)	ディレクトリー内の検索を必要とする項目のうち、ユーザー・インターフェース全体にわたってリストに表示する項目の数を指定します。	50	
暗号化	データベースおよびディレクトリー・サーバーへの接続に使用されるパスワードと、システム認証に使用される IBM Security Identity Manager システム・ユーザーのパスワードを暗号化するオプション。	True (On)	
WebSphere 管理者	WebSphere 管理者、および WebSphere 管理者パスワードを指定します。		
WebSphere 管理者パスワード	WebSphere 管理者パスワードを指定します。		
IBM Security Identity Manager システム・ユーザー	IBM Security Identity Manager システム・ユーザー ID を指定します。		
IBM Security Identity Manager システム・ユーザー・パスワード	Specifies the IBM Security Identity Manager システム・ユーザー・パスワード **注:** IBM Security Identity Manager システム・ユーザーのパスワードは、最大 12 文字です。		

単一サーバー環境への IBM Security Identity Manager サーバーのインストール

このセクションでは、IBM Security Identity Manager サーバーを単一サーバー環境においてインストールおよび構成する作業について説明します。

始める前に

IBM Security Identity Manager サーバーを単一サーバー環境においてインストールする前に、以下の作業を完了します。

- IBM Security Identity Manager をインストールするシステムが、インストール処理中に確実に保護されるようにします。
- IBM Security Identity Manager のインストールに必要な製品 DVD を判別します。DVD の内容の明細については、DVD イメージと一緒に提供される `itim-6.0-dvd-images-operatingsystem.txt` などのテキスト・ファイルを参照してください。これらのイメージ・ファイルの完全なリストについては、 14 ページの『IBM Security Identity Manager のダウンロード』を参照してください。
- フリー・ディスク・スペースおよびメモリー要件に適合していることを確認します。また、システムの temp ディレクトリーおよび *WAS_PROFILE_HOME* ディレクトリーに、十分なフリー・ディスク・スペースがあることを確認します。ターゲット・コンピューターは、IBM Security Identity Manager インフォメーション・センターの『ハードウェアおよびソフトウェア要件』に記載されたコンピューター要件を満たしている必要があります。
- 必要な管理権限を持っていることを確認します。Windows システムでは、ログオン・ユーザー ID は Administrators グループに属する必要があります。UNIX システムでは、ログオン・ユーザー ID は root である必要があります。
- IBM Security Identity Manager サーバーをインストールすると、IBM Security Identity Manager データベースにデータが書き込まれます。
- 前提アプリケーションがインストールされ実行されていることを確認します。

前提条件	**詳細情報の参照先**
データベース	18 ページの『データベースのインストールと構成』
ディレクトリー・サーバー	43 ページの『ディレクトリー・サーバーのインストールおよび構成』
Directory Integrator (オプション)	54 ページの『IBM Tivoli Directory Integrator のインストール (オプション)』
WebSphere Application Server	58 ページの『WebSphere Application Server のインストールおよび構成』

  IBM Security Identity Manager および WebSphere Application Server のみが、同じコンピューター上へのインストールを必要とします。その他のアプリケーションはすべて、ローカル側でも、Tivoli Identity Manager がインストールされているコンピューターのリモート側でも実行できます。IBM Tivoli Directory Integrator は、オプションのコンポーネントです。
- IBM Security Identity Manager インストーラーの実行時は、必ず IBM Security Identity Manager Java 2 セキュリティーを無効にします。 8 ページの『WebSphere セキュリティー構成』を参照してください。
- IBM Security Identity Manager で外部ユーザー・レジストリーを使用して認証を行う場合は、 69 ページの『外部ユーザー・レジストリーを使用した認証のためのインストール前の構成』に記載されたステップを完了します。
- IBM Security Identity Manager サーバーをインストールする前に、WebSphere Application Server を停止および開始できることを確認します。確認するために、WebSphere Application Server を停止および開始します。これらの手順について詳しくは、 58 ページの『WebSphere Application Server のインストールおよび構成』を参照してください。

- ご使用の構成の詳細を収集します。構成パラメーターの詳細なリストについては、17 ページの『第 4 章 前提コンポーネントのインストール』の『プリインストール・ワークシート』を参照してください。
- 既にコンピューターにインストールされている IBM Security Identity Manager のバージョンをアップグレードする場合は、237 ページの『第 15 章 IBM Security Identity Manager のアップグレード』を参照してください。このトピックには、IBM Security Identity Manager のカスタマイズおよびデータの保護について、より詳しい説明が記載されています。

手順

1. インストール・ウィザードを開始します。
2. インストール・ウィザード・ページを完了します。
3. 主要なインストール・アクションに応答します。

インストール・ウィザードの開始

インストール・ウィザードを使用して、単一サーバー環境に IBM Security Identity Manager サーバーをインストールします。他のすべてのコンポーネントは既にインストールされている必要があります。

始める前に

80 ページの『単一サーバー環境への IBM Security Identity Manager サーバーのインストール』で指定されたすべての前提条件タスクが完了していることを確認します。

手順

1. IBM Security Identity Manager サーバーをインストールするコンピューターで、システム管理特権を使用してアカウントにログオンします。
2. インストール・プログラムを開始するか、または DVD ドライブに 製品 DVD を挿入します。ユーザーの環境に応じた正しい DVD を見つけるには、14 ページの『IBM Security Identity Manager のダウンロード』を参照してください。
3. インストール・プログラムを実行します。
   - Windows オペレーティング・システムの場合:
     a. **「スタート」 > 「ファイル名を指定して実行」**をクリックします。
     b. インストール・プログラムが置かれているドライブおよびパスを入力してから、次のコマンドを入力します。

        ```
        instwin.exe
        ```

        「ようこそ」ウィンドウが開きます。
   - UNIX または Linux オペレーティング・システムの場合:

     注: UNIX または Linux システムでは、インストール・プログラムを実行するために、`/tmp` ディレクトリーに 150 MB 以上のフリー・スペースが必要です。ご使用のシステムに十分なスペースがない場合は、*IATEMPDIR* 環境変数を、十分な空きディスク・スペースのあるディスク区分上のディレクトリーに設定します。

変数を設定するためには、次に示すコマンドのうちの 1 つをコマンド行プロンプトに入力し、それからインストール・プログラムを再実行します。

– Bourne shell (sh)、ksh、bash、および zsh:

```
$ IATEMPDIR=temp_dir
$ export IATEMPDIR
```

– C shell (csh) および tcsh:

```
$ setenv IATEMPDIR temp_dir
```

ここで *temp_dir* はディレクトリーへのパスで、例えば、`/your/free/directory` の場合、 使用可能なフリー・ディスク・スペースがあります。

a. コマンド・シェル・プロンプト・ウィンドウを開き、インストール・プログラムのあるディレクトリーを選択します。

b. 以下のいずれかのコマンドを入力して、IBM Security Identity Manager インストール・プログラムを実行します。

   – AIX オペレーティング・システム:

     `instaix.bin`

   – Linux オペレーティング・システム:

     `instlinux.bin`

   – Linux for pSeries オペレーティング・システム:

     `instplinux.bin`

   – Linux for zSeries オペレーティング・システム:

     `instzlinux.bin`

   – Solaris オペレーティング・システム:

     `instsol.bin`

インストール・プログラムが開始し、「ようこそ」ウィンドウが開きます。

次のタスク

インストール・ウィザード・ページを完了します。

インストール・ウィザード・ページの完了

最初のインストール・ウィザード・ページを使用して、インストールをセットアップします。

始める前に

インストール・ウィザードが開始されていることを確認します。

このタスクについて

ドル記号 ($) は、Install Anywhere が使用するインストーラー・フレームワークにおいて特別な意味を持っています。フィールド値で $ を使用しないでください。インストール・プログラム・フレームワークまたはオペレーティング・システム・プラットフォームが、値を変数に置換する可能性があります。

以下の手順に従って、インストール・ウィザード・ページを完了します。

手順

1. インストール・ウィザード・ページで使用する言語を変更するには、リストから別の言語を選択し、「**OK**」をクリックします。 この選択が影響するのはインストール・ウィザードのみであり、インストールする IBM Security Identity Manager の言語バージョンには影響しません。

   注: ライセンスは、選択したインストール言語ではなく、常にシステム・ロケールで表示されます。
2. 著作権および特記事項を確認し、「**次へ**」をクリックします。

   注: IBM Security Identity Manager を AIX システムにインストールし、著作権のテキストを表示できない場合は、システムの色のコントラストの設定を調整する必要があります。コントラスト色の設定を High から Low に変更します。
3. 「ご使用条件」ウィンドウで、使用条件を読み、その条項に同意するかどうか決定します。条項に同意してインストールを続行する場合は、「**同意する**」を選択して、「**次へ**」をクリックします。 必要に応じ、「**印刷**」をクリックしてご使用条件を印刷します。
4. インストール・ディレクトリーを指定し、「**次へ**」をクリックします。
   - デフォルトのインストール・ディレクトリーである *ISIM_HOME* をそのまま使用します。または、
   - 別のディレクトリーを選択するには、「**選択**」をクリックします。
5. 「インストール・タイプ」ウィンドウで、「**単一 WebSphere Application Server**」を選択します。次に、「**次へ**」をクリックします。 「WebSphere Application Server のインストール・ディレクトリー」ウィンドウが開き、WebSphere Application Server のインストール・ディレクトリー (*WAS_HOME* ディレクトリー) の値が表示されます。

   注: コンピューターに複数の WebSphere Application Server がインストールされている場合があります。ディレクトリーが IBM Security Identity Manager サーバーをインストールするディレクトリーではない場合は、「**選択**」をクリックします。正しいディレクトリーの値を入力し、「**次へ**」をクリックします。
6. 「WebSphere プロファイルの選択」パネルで、IBM Security Identity Manager のインストール先となる WebSphere Application Server のプロファイル名をリストから選択します。「**次へ**」をクリックします。
7. WebSphere Application Server に関する以下のデータを検証し、「**次へ**」をクリックします。
   - IBM Security Identity Manager サーバーのデプロイ先となる WebSphere Application Server の名前 (デフォルトでは *server1*)。
   - コンピューターのホスト名。コンピューターに複数のホスト名が付けられておらず、WebSphere Application Server が表示された値以外のホスト名でインストールされていない限り、表示された値をそのまま使用します。
8. WebSphere Application Server 管理セキュリティーが有効になっている場合は、管理者ユーザー ID およびパスワードを指定する必要があります。「**次へ**」をクリックします。

9. WebSphere アプリケーション構成のセキュリティー・ドメイン・ウィンドウのタイプを選択し、「**次へ**」をクリックします。
   - IBM Security Identity Manager のカスタム・レジストリーを使用する場合は「**はい**」を選択します。
   - 既存のセキュリティー・ドメインとレジストリーを使用する場合は「**いいえ**」を選択します。

   注: 「**はい**」を選択した場合は、新しいセキュリティー・ドメインが作成され、IBM Security Identity Manager で提供されるカスタム・レジストリーを使用して構成されます。 IBM Security Identity Manager は、このカスタム・レジストリーを認証の決定に使用します。「**いいえ**」を選択した場合
   - IBM Security Identity Manager は、アプリケーション・サーバー用に構成されている現行のセキュリティー・ドメインを使用します。外部ユーザー・レジストリーの構成方法に関するインストール前の指示を確認するには、 69 ページの『外部ユーザー・レジストリーを使用した認証のためのインストール前の構成』を参照してください。
   - インストール・ウィザードが完了したら、インストール後の構成ステップを完了する必要があります。 166 ページの『認証用の外部ユーザー・レジストリーに対するインストール後の構成』を参照してください。
10. システム・ユーザーの名前とパスワードを入力し、「**次へ**」をクリックします。 前の手順でセキュリティー・ドメインを作成することを選択している場合は、デフォルトのシステム・ユーザーおよびパスワードとして `isimsystem` および `secret` が入力されます。
11. 「データベース・タイプ」ウィンドウで、以下のデータベース・タイプの 1 つを選択し、「**次へ**」をクリックします。
    - IBM DB2 Universal Database
    - Oracle データベース
    - Microsoft SQL Server (Windows オペレーティング・システムの場合のみ選択可能)

    以下の条件が当てはまることを確認するための「注意」ウィンドウが開きます。
    - DB2 が選択されている場合、「**続行**」をクリックします。
    - Oracle データベースまたは Microsoft SQL Server が選択されている場合は、JDBC ドライバーのロケーションおよび名前を入力する必要があります。「**次へ**」をクリックします。詳しくは、 35 ページの『Oracle JDBC ドライバーのインストール』 および 41 ページの『SQL Server JDBC ドライバーのインストール』を参照してください。
    - ディレクトリー・サーバー・バージョンは正しいレベルでなければなりません。バージョンが正しいことを確認し、「**続行**」をクリックします。
12. 「ディレクトリー・サーバー情報」ウィンドウで、LDAP サーバー情報を入力します。「**テスト**」をクリックします。
13. 接続テストが成功した場合は、組織データを入力します。「**次へ**」をクリックします。
14. 「鍵ストアのパスワード」ウィンドウで、鍵ストアのパスワードを指定します。ここに入力される鍵ストアのパスワードは、IBM Security Identity Manager

鍵ストア・ファイルのアンロックに使用されます。このファイルは、IBM Security Identity Manager の機密データの暗号化に使用される暗号鍵を保管します。「**次へ**」をクリックします。

15. IBM Tivoli Directory Integrator にエージェントレス・アダプターをインストールするかどうかを選択し、「**次へ**」をクリックします。

    インストール・プログラムは、以下の管理対象リソースに対してこれらの POSIX アダプターをインストールします。

    - AIX
    - HP-UX
    - LDAP
    - Linux
    - Solaris

    エージェントレス・アダプター用のインストール・プログラムは、*ISIM_HOME*¥config¥adapters ディレクトリーにあります。アダプターは、後から必要に応じて再インストールできます。IBM Security Identity Manager インストール・プログラムでは、POSIX アダプターがインストールされます。しかし、最新のアダプター・プロファイルをインストールすることをお勧めします。手動でのアダプター・インストールについて詳しくは、55 ページの『エージェントレス・アダプターのインストール』および 57 ページの『エージェントレス・アダプター・プロファイルのインストール』を参照してください。

16. IBM Tivoli Directory Integrator ウィンドウの「ロケーション」の「Directory Integrator のホーム・ディレクトリー」フィールドで、正しいディレクトリー値を入力するか、正しいディレクトリー値であることを確認し、「**次へ**」をクリックします。 必要に応じ、「**選択**」をクリックして別のロケーションを選択します。

17. 「共有アクセス・モジュールをインストールしますか」ウィンドウで、以下の基準に従って、共有アクセス・モジュールをインストールするかどうかを決定します。

    - 共有アクセス・モジュールが必要で、購入済みである場合は「**はい**」を選択します。インストール・プログラムによって、IBM Security Identity Manager が共有アクセス・モジュール・コンポーネント共にインストールされます。
    - 共有アクセス・モジュールを購入していない場合は、「**いいえ**」を選択します。インストール・プログラムでは、IBM Security Identity Manager サーバーのみインストールされます。共有アクセス・モジュールは、後で必要になったときに、いつでも個別にインストールできます。

    「**次へ**」をクリックします。

18. TivoliCommon Directory ウィンドウで、インストール・プログラムで定義したデフォルトのディレクトリーを受け入れるか、新規のディレクトリーを選択します。「**次へ**」をクリックします。 ディレクトリーに 25 MB 以上のフリー・スペースがあることを確認してください。Tivoli Common Directory は、ログ、First Failure Data Capture データなどのすべての保守関連ファイルのためのセントラル・ロケーションです。

19. 「単一サーバーのプリインストール要約」ウィンドウで、以下の情報を確認します。すべてが受け入れ可能な場合、「**インストール**」をクリックします。
    - 製品名。
    - IBM Security Identity Manager のインストール・ディレクトリー。
    - エージェントレス・アダプターをインストールするかどうかの選択。
    - WebSphere Application Server のインストール・ディレクトリー。
    - 必要な空きディスク・スペースと使用可能な空きディスク・スペース。

    注: 「**インストール**」をクリックしてから、「**キャンセル**」をクリックしてインストールを取り消すと、IBM Security Identity Manager がインストールされないことを示すメッセージが表示されます。ただし、このアクションではファイルは自動的にはクリーンアップされず、この状態では結果的に部分インストールになる可能性があります。再度「**インストール**」を実行する前に、手動で部分インストールをすべてクリーンアップします。
20. インストールが完了したら、「**完了**」をクリックします。 インストール・プログラムによって、IBM Security Identity Manager ファイルが *ISIM_HOME* ディレクトリーへコピーされます。

次のタスク

Microsoft SQL Server 2008 を使用している場合は、*lockTimeout* 値を変更する必要があります。この変更は、IBM Security Identity Manager のインストールが完了した後に、WebSphere Application Server でデータ・ソースが既にセットアップされた状態で行う必要があります。*lockTimeout* 値を変更するには、以下の手順を実行します。

1. WebSphere Application Server 管理コンソールにログオンします。
2. 「**リソース**」 > 「**JDBC**」 > 「**データ・ソース**」 > 「**ITIM データ・ソース**」 > 「**カスタム・プロパティー**」 > 「**lockTimeout**」を選択します。
3. *locktimeout* 値を -1 に設定します。
4. 「**OK**」をクリックします。
5. 変更を保存します。

主なインストール・エラーへの対処

インストール・プログラムにより、IBM Security Identity Manager ファイルが *ISIM_HOME* ディレクトリーへコピーされます。追加の主要なインストール・セットアップおよび構成用の一連の進行ウィンドウが開きます。このセクションでは、このセットアップ時に発生するエラーについて説明します。

詳しくは、 125 ページの『IBM Security Identity Manager サーバーが単一サーバー環境で作動可能であるかどうかの検証』を参照してください。

WebSphere Application Server の始動エラーの修正

WebSphere Application Server は実行中であり、IBM Security Identity Manager デプロイメントおよび構成が許可される必要があります。IBM Security Identity Manager インストール・プログラムにより、WebSphere Application Server の状況が確認され

ます。WebSphere Application Server が実行されていない場合、インストール・プログラムにより、WebSphere Application Server の開始が試行されます。

始める前に

WebSphere Application Server が正しくインストールされていることを確認してください。

このタスクについて

IBM Security Identity Manager インストール・プログラムによる WebSphere Application Server の始動が失敗すると、エラー・メッセージが表示されます。

エラーが発生した場合、次のようにします。

手順

以下の手順のいずれかを実行します。

- インストール・プログラムを終了し、以下のステップを完了します。
  1. WebSphere Application Server が開始されない問題を解決します。
  2. 手動で *ISIM_HOME* ディレクトリーのファイルをすべて削除します。
  3. インストール・プログラムを再度実行します。
- 手動で WebSphere Application Server を開始および停止でき、エラーが表示されないことを確認した後、インストール・プログラムを続行します。以下の手順を実行します。
  1. WebSphere Application Server を停止します。
     - Windows オペレーティング・システム

       WAS_PROFILE_HOME¥bin¥stopServer.bat *servername*
     - UNIX または Linux オペレーティング・システム

       WAS_PROFILE_HOME/bin/stopServer.sh *servername*
  2. WebSphere Application Server を始動するには、次のようにします。
     - Windows オペレーティング・システム

       WAS_PROFILE_HOME¥bin¥startServer.bat *servername*
     - UNIX または Linux オペレーティング・システム

       WAS_PROFILE_HOME/bin/startServer.sh *servername*

データベースのデータの収集およびデータベースの構成

このステップでは、IBM Security Identity Manager インストール・プログラムは IBM Security Identity Manager データベースをセットアップします。

始める前に

データベースが正しくインストールされていることを確認します。

このタスクについて

エラーが発生した場合、エラーを調査し、修正アクションを実行します。
ISIM_HOME¥install_logs¥dbConfig.stdout ログ・ファイルに、より詳しい情報があります。データベース製品に付属の資料を参照してください。

インストール・プログラムを続行します。インストールが完了したら、以下のステップを実行します。

手順

1. *ISIM_HOME*¥install_logs¥dbConfig.stdout ログ・ファイルの名前を変更することにより、現在のログ・データを保存します。
2. IBM Security Identity Manager メッセージング・エンジンが実行されていないことを確認します。 WebSphere 管理コンソールにログインして、以下のステップを実行します。
   a. 「**サービス統合**」 > 「**バス**」をクリックします。
   b. 「**itim_bus**」をクリックします (存在する場合)。
   c. 「トポロジー」セクションで、「**メッセージング・エンジン**」をクリックします。

      単一サーバー・インストールの場合、*nodename.servername*-itim_bus という名前のエンジンが表示されます。

      クラスター・インストールの場合、*n*+1 個のメッセージング・エンジンが表示されます。*n* はクラスター・メンバーの数です。追加のメッセージング・エンジンが メッセージング・クラスター用に使用されています。
   d. 1 つ以上のメッセージング・エンジンを選択し、「**停止**」をクリックします。
3. 修正が完了した後、以下のコマンドを使用して、IBM Security Identity Manager データベースを構成します。
   - Windows オペレーティング・システム:

     ISIM_HOME¥bin¥DBConfig.exe
   - UNIX または Linux オペレーティング・システム:

     ISIM_HOME/bin/DBConfig

   新規のログ・データは、ログ・ファイル
   ISIM_HOME¥install_logs¥dbConfig.stdout に記録されます。

次のタスク

DBConfig コマンドは、IBM Security Identity Manager が必要とするデータベース・テーブル定義を作成します。インストール中にコマンドがデータベースの構成に失敗した場合のみ、このコマンドを実行してください。データベース・テーブルがあらかじめ設定されている状態で **DBConfig** コマンドを実行すると、最初に、既存のすべてのデータベース・テーブルが除去されます。詳しくは、 135 ページの『手動による DBConfig データベース構成ツールの開始』を参照してください。

インストール・プログラムの次のステップへ進みます。

ディレクトリー・サーバーに関するデータの収集とディレクトリー・サーバーの構成

このステップでは、IBM Security Identity Manager インストール・プログラムにより、LDAP スキーマと IBM Security Identity Manager のデフォルトのデータ入力項目がセットアップされます。

始める前に

ディレクトリー・サーバーが正しくインストールされていることを確認します。

このタスクについて

エラーが発生した場合、エラー・メッセージを記録してください。このメッセージには、ディレクトリー・サーバーへの LDAP スキーマのセットアップ時またはデータ構成作成時の問題について説明されている場合があります。

インストール・プログラムを続行します。インストールが完了したら、以下のステップを実行します。

手順

1. エラーを調査し、修正アクションを実行します。
   ISIM_HOME¥install_logs¥ldapConfig.stdout ログ・ファイルに、より詳しい情報があります。ディレクトリー・サーバー製品に付属の資料を参照してください。
2. *ISIM_HOME*¥install_logs¥ldapConfig.stdout ログ・ファイルの名前を変更することにより、現在のログ・データを保存します。
3. 修正が完了した後、以下のコマンドを使用してディレクトリー・サーバーを構成します。
   - Windows オペレーティング・システム:

     ISIM_HOME¥bin¥ldapConfig.exe
   - UNIX または Linux オペレーティング・システム:

     ISIM_HOME/bin/ldapConfig

   新規のログ・データは、ログ・ファイル *ISIM_HOME*¥install_logs¥ldapConfig.stdout に記録されます。

次のタスク

ldapConfig コマンドを実行すると、IBM Security Identity Manager が使用するデフォルト値が復元されます。itim manager というユーザー ID のパスワードなど、これらの属性のいずれかの値を変更した場合には、値は上書きされます。LDAP 構成が IBM Security Identity Manager サーバーのインストール・プロセス中に失敗した場合を除き、**ldapConfig** コマンドを 2 回実行しないでください。詳しくは、137 ページの『ディレクトリー・サーバーの構成』を参照してください。

インストール・プログラムの次のステップへ進みます。

IBM Security Identity Manager に関するデータの収集と IBM Security Identity Manager サーバーの構成

IBM Security Identity Manager インストール・プログラムにより、プロパティー・ファイルのセットが *ISIM_HOME*¥data ディレクトリーへコピーされます。このステップでは、GUI を使用して、 プロパティーを変更できます。

始める前に

インストール・プログラムにより、IBM Security Identity Manager サーバーに必要な WebSphere 環境設定も構成されます。このステップが完了するまでに数分かかります。

このタスクについて

エラーが発生した場合、エラー・メッセージを記録してください。このメッセージには、IBM Security Identity Manager サーバーに必要な WebSphere 環境設定の構成時の問題について説明されている場合があります。

インストール・プログラムを続行します。インストールが完了したら、以下のステップを実行します。

手順

1. エラーを調査し、修正アクションを実行します。
   ISIM_HOME¥install_logs¥runConfigFirstTime.stdout ログ・ファイルに、より詳しい情報があります。WebSphere 製品に付属の資料を参照してください。
2. 修正が完了したら、以下のコマンドを使用して、よく使用されるプロパティーを更新します。
   - Windows オペレーティング・システム:

     ISIM_HOME¥bin¥runConfig.exe
   - UNIX または Linux オペレーティング・システム:

     ISIM_HOME/bin/runConfig

   runConfig ユーティリティーは、**install** パラメーターも受け入れます。インストール中に **runConfig** での問題が報告された場合は、**install** パラメーターを持つ **runConfig** を使用します。**install** オプションを使用すると、システム構成が完了するまで数分かかります。
   - Windows オペレーティング・システム:

     ISIM_HOME¥bin¥runConfig.exe install
   - UNIX または Linux オペレーティング・システム:

     ISIM_HOME/bin/runConfig install

   新規のログ・データは、ログ・ファイル *ISIM_HOME*¥install_logs¥runConfig.stdout に記録されます。

次のタスク

詳しくは、 140 ページの『一般に使用されるシステム・プロパティーの構成』を参照してください。

インストール・プログラムの次のステップへ進みます。

デプロイメント・エラーの修正

IBM Security Identity Manager アプリケーションは、WebSphere Application Server 内で、エンタープライズ・アプリケーションとして稼働します。IBM Security Identity Manager インストール・プログラムでは、WebSphere コマンド行インターフェース (wsadmin) を使用し、IBM Security Identity Manager アプリケーションを WebSphere Application Server にデプロイします。

始める前に

WebSphere Application Server が正しくインストールされていることを確認してください。

このタスクについて

IBM Security Identity Manager アプリケーションをデプロイすると、WebSphere Application Server で特定の構成ステップも実行されます。このステップが完了するまでに数分必要です。

デプロイメントが完了した時点で、IBM Security Identity Manager ファイルは以下のディレクトリーに格納されています。

- *WAS_PROFILE_HOME*¥installedApps¥*cellname*¥ITIM.ear
- *WAS_PROFILE_HOME*¥config¥cells¥*cellname*applications¥ITIM.ear

注: デプロイメント・マネージャー・ノードの場合、これらのファイルは *WAS_NDM_PROFILE_HOME*¥config¥cells¥*cellname*¥applications¥ITIM.ear ディレクトリーにのみあります。

デプロイメントの実行中にエラー・メッセージが表示された場合は、以下のステップを実行します。

手順

1. エラーを訂正してください。
   - ログ・データに以下の事象が記録されている場合:
     - WebSphere Application Server 構成マネージャーとの SOAP 接続確立の失敗。
     - 何らかのタイプの WebSphere Application Server スクリプト・エラー。
     a. インストール・プログラムを終了します。
     b. WebSphere Application Server へ接続できない問題、またはスクリプト・エラーとして説明されている問題を解決します。詳しくは、WebSphere の資料を参照してください。
     c. 手動で *ISIM_HOME* ディレクトリーのファイルをすべて削除します。
     d. インストール・プログラムを再度実行します。
   - ログ・データに失敗の原因がタイムアウトであることが示されている場合:
     - インストール・プログラムを続行します。
     - インストール・プログラムが完了した時点で、以下のディレクトリーが存在している場合は、これらを削除します。

- *WAS_PROFILE_HOME*¥installedApps¥*cellname*¥ITIM.ear
- *WAS_PROFILE_HOME*¥config¥cells¥*cellname*applications¥ITIM.ear

2. 以下のいずれかのコマンドを実行して、IBM Security Identity Manager サーバーを WebSphere Application Server にデプロイします。
   - WebSphere の管理セキュリティーおよびアプリケーション・セキュリティーが有効になっている場合は、以下のいずれかのコマンドを入力します。
     – Windows オペレーティング・システム

       ```
       ISIM_HOME¥bin¥setupEnrole.exe install server:server_name user:user_id
       password:pwd ejbuser:ejb_user_id ejbpassword:ejbpassword
       ```

     – UNIX または Linux オペレーティング・システム

       ```
       ISIM_HOME¥bin¥setupEnrole.sh install server:server_name user:user_id
       password:pwd ejbuser:ejb_user_id ejbpassword:ejbpassword
       ```

     server_name の値は、IBM Security Identity Manager アプリケーションのデプロイ先である WebSphere Application Server の名前です。*user_id* の値は、*wsadmin* などの WebSphere アドミニストレーター・ユーザー ID です。*pwd* の値は、*secret* などの WebSphere アドミニストレーター・ユーザー ID のパスワードです。 *ejb_user_id* の値は、IBM Security Identity Manager のシステム・ユーザー ID です。デフォルトでは、WebSphere Application Server の管理者ユーザー ID が使用されます。

     注: EJBUser ID に、スペースがある値 (*Bob Smith* など) が含まれている場合は、その値を引用符で囲む必要があります。例えば、コマンドは以下のように入力する必要があります。

     ```
     SetupEnrole.exe install server:server1 user:wsadmin password:secret
     ejbuser:"Bob Smith" ejbpassword:secret
     ```

   - WebSphere の管理セキュリティーおよびアプリケーション・セキュリティーが無効になっている場合は、以下のいずれかのコマンドを入力します。
     – Windows オペレーティング・システム

       ```
       ISIM_HOME¥bin¥setupEnrole.exe install server:server_name
       ```

     – UNIX または Linux オペレーティング・システム

       ```
       ISIM_HOME¥bin¥setupEnrole.exe install server:server_name
       ```

     server_name のデフォルトは、server1 です。

WebSphere Application Server の再始動

エラー・メッセージに、WebSphere Application Server の再始動が失敗することが示されている場合、インストールを完了し、WebSphere Application Server の再始動を試行します。

始める前に

WebSphere Application Server が正しくインストールされていることを確認してください。

手順

1. WebSphere Application Server を停止します。
   - Windows オペレーティング・システム

WAS_PROFILE_HOME¥bin¥stopServer.bat *servername -user userid -password userpassword*

- UNIX または Linux オペレーティング・システム

  WAS_PROFILE_HOME/bin/stopServer.sh *servername -user userid -password userpassword*

2. WebSphere Application Server を開始します。
   - Windows オペレーティング・システム

     WAS_PROFILE_HOME¥bin¥startServer.bat *servername*

   - UNIX または Linux オペレーティング・システム

     WAS_PROFILE_HOME/bin/startServer.sh *servername*

次のタスク

インストールを検証します。 121 ページの『第 7 章 インストールの検証』を参照してください。

クラスター環境への IBM Security Identity Manager のインストール

このセクションでは、クラスター環境における IBM Security Identity Manager サーバーのインストールおよび構成について説明します。インストール・プログラムでは、IBM Security Identity Manager サーバーのみインストールされます。

始める前に

9 ページの『構成オプション』をお読みください。

以下のタスクを完了します。

- IBM Security Identity Manager をインストールするシステムが、インストール処理中に確実に保護されるようにします。
- IBM Security Identity Manager のインストールに必要な製品 DVD を判別します。DVD の内容の明細については、DVD イメージと一緒に提供される itim-6.0-dvd-images-*operatingsystem*.txt などのテキスト・ファイルを参照してください。これらのイメージ・ファイルの完全なリストについては、 14 ページの『IBM Security Identity Manager のダウンロード』を参照してください。
- クラスター内のすべてのコンピューターがフリー・ディスク・スペースおよびメモリーの要件を満たしていることを確認します。システム一時ディレクトリーおよび *WAS_PROFILE_HOME* ディレクトリーと *WAS_NDM_PROFILE_HOME* ディレクトリーに、十分なフリー・ディスク・スペースがあることを確認します。ターゲット・コンピューターが、IBM Security Identity Manager インフォメーション・センターの「*製品概要*」にある『*ハードウェア要件およびソフトウェア要件*』に記載されているコンピューター要件を満たしている必要があります。
- 必要な管理権限を持っていることを確認します。Windows システムでは、ログオン・ユーザー ID は Administrators グループに属する必要があります。UNIX システムでは、ログオン・ユーザー ID は root である必要があります。
- IBM Security Identity Manager サーバーをインストールすると、IBM Security Identity Manager データベースにデータが書き込まれます。このデータベースがインストール済みであることを確認します。DB2 を使用する場合は、必要なフィックスパックがインストール済みであることと、ミドルウェア構成ユーティリティ

ーを実行していることを確認します。詳しくは、 18 ページの『データベースのインストールと構成』を参照してください。

- クラスターでは、IBM Security Identity Manager インストール・ディレクトリーの名前は、すべてのクラスター・メンバーで同じでなければなりません。後で別のクラスター・メンバー・コンピューターでの ID フィード・アクティビティーでランタイム障害が発生しないようにするために、同じディレクトリーを指定してください。
- 前提アプリケーションがインストールされ実行されていることを確認します。

前提条件	詳細情報の参照先
データベース	18 ページの『データベースのインストールと構成』
ディレクトリー・サーバー	43 ページの『ディレクトリー・サーバーのインストールおよび構成』
Directory Integrator (オプション)	54 ページの『IBM Tivoli Directory Integrator のインストール (オプション)』
WebSphere Application Server	61 ページの『クラスター環境への WebSphere Application Server のインストール』

IBM Security Identity Manager および WebSphere Application Server のみが、同じコンピューター上へのインストールを必要とします。その他のアプリケーションはすべて、ローカル側でも、IBM Security Identity Manager がインストールされているコンピューターのリモート側でも実行できます。IBM Tivoli Directory Integrator は、オプションのコンポーネントです。

- IBM Security Identity Manager インストーラーの実行時は、必ず IBM Security Identity Manager Java 2 セキュリティーを無効にします。 8 ページの『WebSphere セキュリティー構成』を参照してください。
- IBM Security Identity Manager で外部ユーザー・レジストリーを使用して認証を行う場合は、 69 ページの『外部ユーザー・レジストリーを使用した認証のためのインストール前の構成』に記載されたステップを完了します。
- WebSphere Application Server のセルおよびクラスターによる IBM Security Identity Manager のインストールの準備ができていることの判別。 58 ページの『WebSphere Application Server のインストールおよび構成』 で説明するステップを完了して、WebSphere Application Server のセルおよびクラスターを構成します。

  以下のプロセスは、IBM Security Identity Manager サーバーのインストール前およびインストール後に実行中である必要があります。

  – デプロイメント・マネージャー

  – WebSphere Application Server ノード・エージェント
- ご使用の構成の詳細を収集します。構成パラメーターの詳細なリストについては、 75 ページの『第 5 章 IBM Security Identity Manager サーバーのインストール』の『プリインストール・ワークシート』を参照してください。
- 既にコンピューターにインストールされている IBM Security Identity Manager のバージョンをアップグレードする場合は、 237 ページの『第 15 章 IBM Security

Identity Manager のアップグレード』を参照してください。このトピックでは、IBM Security Identity Manager のカスタマイズとデータの保護について詳しく説明されています。

このタスクについて

クラスター構成でのインストールでは、以下のコンピューターに IBM Security Identity Manager サーバーをインストールする必要があります。

- デプロイメント・マネージャー

  クラスター・ノードに IBM Security Identity Manager サーバーをインストールする*前* に、デプロイメント・マネージャーがインストールされているコンピューターに IBM Security Identity Manager サーバーをインストールします。このインストール中に、IBM Security Identity Manager アプリケーションのデプロイメントおよび IBM Security Identity Manager のデータベースとディレクトリー・サーバーの構成が行われます。デプロイメント・マネージャーは、IBM Security Identity Manager アプリケーションをすべてのクラスター・メンバー・コンピューターに配布して展開します。
- クラスター・メンバー

  この章のステップを繰り返して、クラスター・メンバーである各コンピューターに IBM Security Identity Manager サーバーをインストールします。インストール・プログラムは、以下のタスクを実行します。

  – IBM Security Identity Manager ファイルをターゲット・コンピューターにコピーする。
  – クラスター・メンバーをホストする WebSphere Application Server を構成する。

  クラスターの IBM Security Identity Manager サーバーのインストールは、一度に 1 台のコンピューター単位で、順次実行する必要があります。IBM Security Identity Manager のインストール・プログラムを複数のコンピューター上で同時に実行すると、WebSphere のマスター構成ファイルとの同期問題が発生する可能性があります。

注: 同じコンピューターにデプロイメント・マネージャーと IBM Security Identity Manager クラスター・メンバーの両方がインストールされている場合は、インストール・プログラムを実行するときに両方のノード・タイプを選択する必要があります。

クラスター環境に IBM Security Identity Manager サーバーをインストールするには、以下の手順を実行します。

手順

1. インストール・ウィザードを開始します。
2. インストール・ウィザード・ページを完了します。
3. 主要なインストール・アクションに応答します。

インストール・ウィザードの開始

インストール・ウィザードを使用して、クラスター環境で IBM Security Identity Manager サーバーをインストールします。他のすべてのコンポーネントは既にインストールされている必要があります。

始める前に

94 ページの『クラスター環境への IBM Security Identity Manager のインストール』で指定されたすべての前提条件タスクが完了していることを確認します。

手順

1. IBM Security Identity Manager サーバーをインストールするコンピューターで、システム管理特権を使用してアカウントにログオンします。
2. インストール・プログラムをインストールするか、または DVD ドライブに IBM Security Identity Manager 製品 DVD を挿入します。ユーザーの環境に応じた正しい DVD を見つけるには、14 ページの『IBM Security Identity Manager のダウンロード』を参照してください。
3. インストール・プログラムを実行します。
   - Windows オペレーティング・システム:
     a. **「スタート」 > 「ファイル名を指定して実行」**をクリックします。
     b. インストール・プログラムがあるドライブおよびパスを入力してから、次のコマンドを入力します。

        ```
        instwin.exe
        ```

        「ようこそ」ウィンドウが開きます。
   - UNIX または Linux オペレーティング・システム:

     UNIX または Linux システムでは、インストール・プログラムを実行するために、`/tmp` ディレクトリーに 150 MB 以上のフリー・スペースが必要です。ご使用のシステムに十分なスペースがない場合は、*IATEMPDIR* 環境変数を、十分な空きディスク・スペースのあるディスク区分上のディレクトリーに設定します。

     変数を設定するためには、次に示すコマンドのうちの 1 つを入力し、それからインストール・プログラムを再実行します。

     – Bourne shell (sh)、ksh、bash、および zsh:

       ```
       $ IATEMPDIR=temp_dir
       $ export IATEMPDIR
       ```

     – C shell (csh) および tcsh:

       ```
       $ setenv IATEMPDIR temp_dir
       ```

     ここで *temp_dir* はディレクトリーへのパスで、例えば、`/your/free/directory` の場合、 使用可能なフリー・ディスク・スペースがあります。

     a. コマンド・シェル・プロンプト・ウィンドウを開き、インストール・プログラムのあるディレクトリーを選択します。
     b. 以下のいずれかのコマンドを入力して、インストール・プログラムを実行します。

– AIX オペレーティング・システム:
  `instaix.bin`
– Linux オペレーティング・システム:
  `instlinux.bin`
– Linux for pSeries オペレーティング・システム:
  `instplinux.bin`
– Linux for zSeries オペレーティング・システム:
  `instzlinux.bin`
– Solaris オペレーティング・システム:
  `instsol.bin`

インストール・プログラムが開始し、「ようこそ」ウィンドウが開きます。

次のタスク

インストール・ウィザード・ページを完了します。

インストール・ウィザード・ページの完了

最初のインストール・ウィザード・ページを使用して、インストールをセットアップします。

始める前に

インストール・ウィザードが開始されていることを確認します。

このタスクについて

ドル記号 ($) は、Install Anywhere が使用するインストール・プログラム・フレームワークにおいて特別な意味を持っています。フィールド値で $ を使用しないでください。インストール・プログラム・フレームワークまたはオペレーティング・システム・プラットフォームが、値を変数に置換する可能性があります。

以下の手順に従って、インストール・ウィザード・ページを完了します。

手順

1. インストール・ウィザード・ページの言語を変更するには、リストから別の言語を選択し、「**OK**」をクリックします。 この選択が影響するのはインストール・ウィザードのみであり、インストールする IBM Security Identity Manager サーバーの言語バージョンには影響しません。

   注: ライセンスは、選択したインストール言語ではなく、システム・ロケールの言語で常に表示されます。
2. 著作権および特記事項を確認し、「**次へ**」をクリックします。

   注: IBM Security Identity Manager を AIX システムにインストールし、著作権のテキストを表示できない場合は、システムの色のコントラストの設定を調整する必要があります。コントラスト色の設定を High から Low に変更します。

3. 「ご使用条件」ウィンドウで、使用条件を読み、その条項に同意するかどうか決定します。条項に同意してインストールを続行する場合は、「**同意する**」を選択して、「**次へ**」をクリックします。 必要に応じ、「**印刷**」をクリックしてご使用条件を印刷します。
4. 「インストール・ディレクトリー」ウィンドウで、インストール・ディレクトリーを指定して、「**次へ**」をクリックします。
   - デフォルトのインストール・ディレクトリーである *ISIM_HOME* をそのまま使用します。
   - 「**選択**」を選択して別のディレクトリーを選択します。
5. 「インストール・タイプ」ウィンドウで、「**WebSphere クラスター**」を選択します。「**次へ**」をクリックします。
6. 「クラスター環境に IBM Security Identity Manager をインストールします」ウィンドウで、クラスター環境に適用される条件を確認します。「**次へ**」をクリックします。 続行する前に、環境の構成に必要なその他の変更をこれらの条件に適用します。例えば、デプロイメント・マネージャーおよびすべての WebSphere ノード・エージェントが実行中であることを確認します。詳しくは、 65 ページの『セル内のノードの統合の検証』を参照してください。
7. 「クラスター・ノード・タイプの選択 (Choose Cluster Node Type)」ウィンドウで、以下のノード・タイプの 1 つまたは両方を選択します。
   - デプロイメント・マネージャー

     まず最初に、IBM Security Identity Manager をデプロイメント・マネージャーがインストールされているコンピューターにインストールします。
   - クラスター・メンバー

     デプロイメント・マネージャーが同じコンピューターにインストールされていないすべてのクラスター・メンバーに、IBM Security Identity Manager をインストールします。同じコンピューター上にデプロイメント・マネージャーおよび IBM Security Identity Manager クラスター・メンバーがある場合、両方のノード・タイプを選択する必要があります。

   「WebSphere Application Server のインストール・ディレクトリー」ウィンドウが開き、WebSphere Application Server のインストール・ディレクトリーの値 (*WAS_HOME* ディレクトリー) が表示されます。

   注: コンピューターに複数の WebSphere Application Server がインストールされている場合があります。ディレクトリーが IBM Security Identity Manager サーバーをインストールするディレクトリーではない場合は、「**選択**」をクリックします。正しいディレクトリーの値を入力し、「**次へ**」をクリックします。
8. WebSphere プロファイル名を選択し、「**次へ**」をクリックします。
   - IBM Security Identity Manager インストールにクラスター・メンバーを選択した場合は、そのクラスター・メンバーをホストする WebSphere Application Server プロファイルを選択します。
   - IBM Security Identity Manager のインストール先としてデプロイメント・マネージャーを選択した場合は、リストから WebSphere Application Server プロファイル名を選択します。このプロファイル名は、IBM Security Identity Manager のインストール先となる Network Deployment Manager です。

IBM Security Identity Manager のインストール先としてデプロイメント・マネージャーを選択した場合は、注意ウィンドウが開きます。これらのウィンドウは、ディレクトリー・サーバーのバージョンが正しいレベルであることを確認するものです。バージョンが正しいことを確認し、「**続行**」をクリックします。

9. クラスター名を要求するデータ・ウィンドウで、IBM Security Identity Manager アプリケーション・クラスターと作成したメッセージング・クラスターの両方の名前を入力します。次に、「**次へ**」をクリックします。
10. コンピューターのホスト名を検証して、「**次へ**」をクリックします。 コンピューターに複数のホスト名が付けられておらず、デプロイメント・マネージャーまたは WebSphere Application Server が他のホスト名でインストールされていない場合は、表示された値をそのまま使用します。
11. WebSphere Application Server 管理セキュリティーが有効になっている場合は、管理者ユーザー ID とパスワードを指定し、「**次へ**」をクリックします。
12. このステップは、デプロイメント・マネージャーがインストールされているシステムにインストールする場合にのみ実行します。WebSphere Application Server 構成のセキュリティー・ドメイン・ウィンドウのタイプを選択し、「**次へ**」をクリックします。
    - IBM Security Identity Manager のカスタム・レジストリーを使用する場合は「**はい**」を選択します。
    - 既存のセキュリティー・ドメインとレジストリーを使用する場合は「**いいえ**」を選択します。

    注: 「**はい**」を選択した場合は、新しいセキュリティー・ドメインが作成され、IBM Security Identity Manager で提供されるカスタム・レジストリーを使用して構成されます。 IBM Security Identity Manager は、このカスタム・レジストリーを認証の決定に使用します。「**いいえ**」を選択した場合
    - IBM Security Identity Manager は、アプリケーション・サーバー用に構成されている現行のセキュリティー・ドメインを使用します。外部ユーザー・レジストリーの構成方法に関するインストール前の指示を確認するには、 69 ページの『外部ユーザー・レジストリーを使用した認証のためのインストール前の構成』を参照してください。
    - インストール・ウィザードが完了したら、インストール後の構成ステップを完了する必要があります。 166 ページの『認証用の外部ユーザー・レジストリーに対するインストール後の構成』を参照してください。
13. このステップは、デプロイメント・マネージャーがインストールされているシステムにインストールする場合にのみ実行します。IBM Security Identity Manager システム・ユーザーの名前とパスワードを入力し、「**次へ**」をクリックします。 前の手順でセキュリティー・ドメインを作成することを選択している場合は、デフォルトの IBM Security Identity Manager システム・ユーザーとして `isimsystem` が入力されます。
14. 「データベース・タイプ」ウィンドウで、以下のデータベース・タイプの 1 つを選択し、「**次へ**」をクリックします。
    - DB2 データベース
    - Oracle データベース

- Microsoft SQL Server (Windows オペレーティング・システムの場合のみ選択可能)

「注意」ウィンドウが開き、以下の条件を満たしているかどうかを確認するプロンプトが出されます。

- DB2 が選択されている場合、「**続行**」をクリックします。
- Oracle データベースまたは Microsoft SQL サーバーが選択されている場合、JDBC ドライバーのロケーションおよび名前の入力を促すウィンドウが表示されます。ロケーションおよび名前を入力し、「**次へ**」をクリックします。詳しくは、『*Oracle JDBC ドライバーのインストール*』および『*SQL Server JDBC ドライバーのインストール*』を参照してください。

15. クラスター・メンバーで IBM Security Identity Manager をインストールしている場合、「ディレクトリー・サーバー情報」ウィンドウが開きます。フィールドに値を入力し、「**次へ**」をクリックします。

    クラスター・メンバーでは、LDAP に関するフィールドがあるウィンドウに情報を入力します。デプロイメント・マネージャーがインストールされているコンピューターに IBM Security Identity Manager をインストールするときは、このウィンドウは開きません。

    ウィンドウ内のフィールドに組織データを入力します。各クラスター・メンバーに対して、この情報は同一でなければなりません。デプロイメント・マネージャーでの IBM Security Identity Manager のインストール中に入力した LDAP 仕様に一致している必要があります。

16. 「鍵ストアのパスワード」ウィンドウで、鍵ストアのパスワードを指定します。ここに入力される鍵ストアのパスワードは、IBM Security Identity Manager 鍵ストア・ファイルのアンロックに使用されます。このファイルは、IBM Security Identity Manager 機密データの暗号化に使用される暗号鍵を保管します。「**次へ**」をクリックします。

    IBM Security Identity Manager は、*WAS_NDM_PROFILE*¥config¥cells¥*cell_name*¥isim ディレクトリーの下のデプロイメント・マネージャー・ノードに鍵ストア・ファイル itim_keystore.jceks を作成します。次に、このファイルは *WAS_PROFILE_HOME*¥config¥cells¥*cell_name*¥isim ディレクトリーのすべてのクラスター・メンバー・ノードに伝搬されます。インストーラーは、クラスター・メンバー・ノードでの IBM Security Identity Manager のインストール時に鍵ストアを開いてみることにより、鍵ストアのパスワードを検査します。デプロイメント・マネージャー・ノードとクラスター・メンバー・ノードが同じコンピューター上にある場合、これは行われません。パスワードが正しくない場合、または鍵ストア・ファイルが存在しない場合は、エラー・メッセージが表示されます。鍵ストア・ファイルが存在しない場合は、デプロイメント・マネージャー・ノードからクラスター・メンバー・ノードにファイルをコピーし、再度「**次へ**」をクリックします。

17. IBM Tivoli Directory Integrator にエージェントレス・アダプターをインストールするかどうかを選択し、「**次へ**」をクリックします。

    IBM Security Identity Manager インストール・プログラムは、以下の管理対象リソースに対してこれらの POSIX アダプターをインストールします。

- AIX
- HP-UX
- LDAP
- Linux
- Solaris

IBM Security Identity Manager インストール・プログラムによってインストールされたエージェントレス・アダプター用のインストール・プログラムは *ISIM_HOME*¥config¥adapters ディレクトリーにあります。アダプターは、後から必要に応じて再インストールできます。IBM Security Identity Manager インストール・プログラムでは、POSIX アダプターがインストールされます。しかし、最新のアダプター・プロファイルをインストールすることをお勧めします。手動でのアダプター・インストールについて詳しくは、55 ページの『エージェントレス・アダプターのインストール』および 57 ページの『エージェントレス・アダプター・プロファイルのインストール』を参照してください。

注: IBM Tivoli Directory Integrator がリモート側でインストールされる場合、「**エージェントレス・アダプターをインストールしない**」を選択します。

18. IBM Tivoli Directory Integrator ウィンドウの「ロケーション」で、正しいディレクトリー値を入力するか、正しいディレクトリー値であることを確認し、「**次へ**」をクリックします。 必要に応じ、「**選択**」をクリックして別のロケーションを入力します。
19. 「共有アクセス・モジュールをインストールしますか」ウィンドウで、以下の基準に従って、共有アクセス・モジュールをインストールするかどうかを決定します。
    - 共有アクセス・モジュールが必要で、購入済みである場合は「**はい**」を選択します。インストーラーによって、IBM Security Identity Manager が共有アクセス・モジュール・コンポーネントと共にインストールされます。
    - 共有アクセス・モジュールをインストールしない場合は、「**いいえ**」を選択します。インストーラーによって IBM Security Identity Manager のみがインストールされます。共有アクセス・モジュールは、後で必要になったときに、いつでも個別にインストールできます。
20. TivoliCommon Directory ウィンドウで、IBM Security Identity Manager インストール・プログラムで定義したデフォルトのディレクトリーを受け入れるか、新規のディレクトリーを選択します。「**次へ**」をクリックします。 ディレクトリーに 25 MB 以上のフリー・スペースがあることを確認してください。Tivoli Common Directory は、ログ、First Failure Data Capture データなどのすべての保守関連ファイルのためのセントラル・ロケーションです。
21. 「プリインストールの要約」ウィンドウで、以下の情報を確認します。すべてが受け入れ可能な場合、「**インストール**」をクリックします。
    - 製品名。
    - IBM Security Identity Manager のインストール・ディレクトリー。
    - エージェントレス・アダプターをインストールするかどうかの選択。
    - WebSphere Application Server のインストール・ディレクトリー。
    - 必要な空きディスク・スペースと使用可能な空きディスク・スペース。

- 共有アクセス・モジュールをインストールするかどうかの選択。

注: 「**インストール**」をクリックしてから、「**キャンセル**」をクリックしてインストールを取り消すと、IBM Security Identity Manager がインストールされないことを示すメッセージが表示されます。ただし、このアクションではファイルは自動的にはクリーンアップされず、この状態では結果的に部分インストールになる可能性があります。再度「**インストール**」を実行する前に、手動で部分インストールをすべてクリーンアップします。

22. インストールの進行中に、「データベース構成」ウィンドウが表示されます。「ホスト名」、「ポート番号」、「データベース名」、「管理者 ID」、および「管理者パスワード」の各フィールドに値を入力します。「**テスト**」をクリックして、データベース接続をテストします。 データベースが接続されたら、「**OK**」をクリックします。
23. 「データベース構成」ウィンドウが開きます。ここで、IBM Security Identity Manager のユーザー ID とユーザー・パスワードを入力します。その後、「**続行**」をクリックします。
24. 「ディレクトリー構成」ウィンドウが開きます。「基本 DN」、「パスワード」、「ホスト名」、および「ポート」の各フィールドに情報を入力します。「テスト」をクリックして、ディレクトリー接続をテストします。 ディレクトリーが接続されたら、「**OK**」をクリックします。

    注: 接続のテストは必須です。ディレクトリーが接続されていなければ、ディレクトリーの構成を続行できません。
25. 「ディレクトリー構成」ウィンドウが開きます。ここで、さらに詳しい情報を入力します。

    注: これらのフィールドに入力した情報は覚えておく必要があります。後から各クラスター・メンバーに製品をインストールするときに、同じ情報を入力する必要があります。
    「**続行**」をクリックします。
26. 「システム構成」ウィンドウが開きます。「メール」タブで、各フィールドに情報を入力し、「**OK**」をクリックします。
27. インストールが完了したら、「**完了**」をクリックします。 インストール・プログラムにより、IBM Security Identity Manager ファイルが *ISIM_HOME* ディレクトリーへコピーされます。
28. 各クラスター・メンバーに対するインストールで、ステップ 1 からステップ 21 までを繰り返します。インストールの進行中に、「システム構成」ウィンドウが開きます。ここでは、以下の手順に従って情報を検証し、接続をテストします。
    a. 「メール」タブで、表示された情報が最初のインストールと一致していることを確認します。
    b. 「一般」タブで、表示された情報が最初のインストールと一致していることを確認します。
    c. 「ディレクトリー」タブで、パスワードとホスト名を入力し、このタブの他の情報を検証します。「**テスト**」をクリックして、接続をテストします。
    d. 「データベース」タブで、パスワードを入力し、このタブの他の情報を検証します。「**テスト**」をクリックして、データベース接続をテストします。

e. 「ロギング」タブで、表示された情報を検証し、最初のインストールと一致していることを確認します。

f. 「UI」タブの情報を検証して更新します。この情報が最初のインストールと一致していることを確認します。

g. 「セキュリティー」タブで、最初のインストールに使用した IBM Security Identity Manager のユーザー ID とパスワードを入力します。

h. 各タブのすべての情報を検証したら、「**OK**」をクリックします。

29. インストールが完了したら、「**完了**」をクリックします。

次のタスク

Microsoft SQL Server 2008 を使用している場合は、*lockTimeout* 値を変更する必要があります。この変更は、IBM Security Identity Manager のインストールが完了した後に、WebSphere Application Server でデータ・ソースが既にセットアップされた状態で行う必要があります。*lockTimeout* 値を変更するには、以下の手順を実行します。

1. WebSphere Application Server 管理コンソールにログオンします。
2. 「**リソース**」 > 「**JDBC**」 > 「**データ・ソース**」 > 「**ITIM データ・ソース**」 > 「**カスタム・プロパティー**」 > 「**lockTimeout**」を選択します。
3. *lockTimeout* 値を -1 に設定します。
4. 「**OK**」をクリックします。
5. 変更を保存します。

インストールが正常に完了したら、次のステップ 109 ページの『クラスターの開始』に進みます。インストール中にエラーが発生した場合は、『主なインストール・エラーへの対処』を参照してエラーを修正してください。

主なインストール・エラーへの対処

IBM Security Identity Manager インストール・プログラムでは、追加の主要インストールのセットアップ用および構成用に、一連の進行ウィンドウが開きます。このセクションでは、このセットアップ時に発生するエラーについて説明します。

ターゲット・コンピューターにコピーされる IBM Security Identity Manager ファイル

インストール・プログラムにより、IBM Security Identity Manager ファイルが *ISIM_HOME* ディレクトリーへコピーされます。

デプロイメント・マネージャーでインストールを実行している場合、次のステップの内容は、データベースのデータを収集して、データベースを構成することです。

データベース・セットアップ・エラーの修正

データベースをセットアップする際にエラーが発生した場合は、*ISIM_HOME*¥install_logs¥dbConfig.stdout ログ・ファイルの情報を調べます。また、データベース製品付属の資料を参照してください。

始める前に

データベースが正しくインストールされていることを確認します。

手順

1. *ISIM_HOME*¥install_logs¥dbConfig.stdout ログ・ファイルの名前を変更することにより、現在のログ・データを保存します。
2. IBM Security Identity Manager メッセージング・エンジンが実行されていないことを確認します。 WebSphere 管理コンソールにログオンし、以下のステップを実行します。
   a. 「**サービス統合**」 > 「**バス**」をクリックします。
   b. 「**itim_bus**」をクリックします (存在する場合)。
   c. 「トポロジー」セクションで、「**メッセージング・エンジン**」をクリックします。

      単一サーバー・インストールの場合、*nodename.servername*-itim_bus という名前のエンジンが表示されます。

      クラスター・インストールの場合、*n*+1 個のメッセージング・エンジンが表示されます。*n* は IBM Security Identity Manager クラスター・メンバーの数です。追加のメッセージング・エンジンが IBM Security Identity Manager メッセージング・クラスター用に使用されています。
   d. 1 つ以上のメッセージング・エンジンを選択し、「**停止**」をクリックします。
3. 以下のコマンドを使用して IBM Security Identity Manager データベースを構成します。
   - Windows オペレーティング・システム

     ISIM_HOME¥bin¥DBConfig.exe
   - UNIX または Linux オペレーティング・システム

     ISIM_HOME/bin/DBConfig

   新規のログ・データは、ログ・ファイル *ISIM_HOME*¥install_logs¥dbConfig.stdout に記録されます。

   注: DBConfig コマンドは、IBM Security Identity Manager が必要とするデータベース・テーブル定義を作成します。インストール中にコマンドがデータベースの構成に失敗した場合のみ、このコマンドを実行してください。IBM Security Identity Manager データベース・テーブルが既に設定されている状態で **DBConfig** コマンドを実行すると、最初に既存の IBM Security Identity Manager テーブルがすべてドロップされます。詳しくは、135 ページの『手動による DBConfig データベース構成ツールの開始』を参照してください。

ディレクトリー・サーバー・セットアップ・エラーの修正

ディレクトリー・サーバーで LDAP スキーマのセットアップとデータの構成を行う際にエラーが発生した場合は、エラー・メッセージを記録しておきます。

始める前に

ディレクトリー・サーバーが正しくインストールされていることを確認します。

手順

1. インストールが完了したら、エラーを調査し、修正アクションを実行します。*ISIM_HOME*¥install_logs¥ldapConfig.stdout ログ・ファイルに、より詳しい情報があります。ディレクトリー・サーバー製品で提供される資料の参照が必要な場合もあります。
2. *ISIM_HOME*¥install_logs¥ldapConfig.stdout ログ・ファイルの名前を変更することにより、現在のログ・データを保存します。
3. 修正が完了した後、以下のコマンドを使用してディレクトリー・サーバーを構成します。
   - Windows オペレーティング・システム

     ISIM_HOME¥bin¥ldapConfig.exe
   - UNIX または Linux オペレーティング・システム

     ISIM_HOME/bin/ldapConfig

   新規のログ・データは、ログ・ファイル *ISIM_HOME*¥install_logs¥ldapConfig.stdout に記録されます。

   注: ldapConfig コマンドを実行すると、IBM Security Identity Manager が使用するデフォルト値が復元されます。itim manager というユーザー ID のパスワードなど、これら IBM Security Identity Manager 属性のいずれかの値を変更した場合には、値は上書きされます。LDAP 構成が IBM Security Identity Manager サーバーのインストール処理中に失敗した場合を除き、**ldapConfig** コマンドは、2 回実行しないでください。

次のタスク

詳しくは、 137 ページの『ディレクトリー・サーバーの構成』を参照してください。

IBM Security Identity Manager サーバー・セットアップ・エラーの修正

IBM Security Identity Manager インストール・プログラムにより、IBM Security Identity Manager サーバーに必要な WebSphere 環境設定も構成されます。このステップが完了するまでに数分かかります。エラーが発生した場合、エラー・メッセージを記録してください。このメッセージには、IBM Security Identity Manager サーバーに必要な WebSphere 環境設定の構成時の問題について説明されている場合があります。

始める前に

IBM Security Identity Manager インストール・プログラムにより、プロパティー・ファイルのセットが *ISIM_HOME*¥data ディレクトリーへコピーされます。このステップでは、GUI を使用して、IBM Security Identity Manager プロパティーを変更できます。

インストールをクラスター・メンバーで行う場合は、「ディレクトリー」タブおよび「データベース」タブで入力するディレクトリーとデータベースの接続情報が、デプロイメント・マネージャーを構成するときに指定する情報と一致していることを確認します。デフォルトのデータベースのユーザー ID は、isimuser です。ユーザー・パスワードは、デプロイメント・マネージャーの設定中にユーザー ID isimuser に対して使用されるパスワードです。クラスター・メンバーに使用されるユーザー ID およびパスワードは、デプロイメント・マネージャーで使用されるユーザー ID およびパスワードと同じでなければなりません。ユーザー情報が間違っていると、IBM Security Identity Manager は適切に機能しません。

手順

1. エラーを調査し、*ISIM_HOME*¥install_logs¥runConfigFirstTime.stdout ログ・ファイルを調べます。 ログ・ファイルには、問題の解決に役立つ詳細な情報が記録されています。WebSphere 製品で提供される資料の参照が必要な場合もあります。
2. 修正が完了したら、以下のコマンドを使用して、一般に使用される IBM Security Identity Manager プロパティーを更新します。
   - Windows オペレーティング・システム

     ISIM_HOME¥bin¥runConfig.exe
   - UNIX または Linux オペレーティング・システム

     ISIM_HOME/bin/runConfig

   runConfig ユーティリティーは、**install** パラメーターも受け入れます。IBM Security Identity Manager のインストール中に runConfig での問題が報告された場合は、**install** パラメーターを持つ runConfig を使用します。**install** オプションを使用すると、システム構成が完了するまで数分かかります。
   - Windows オペレーティング・システム

     ISIM_HOME¥bin¥runConfig.exe install
   - UNIX または Linux オペレーティング・システム

     ISIM_HOME/bin/runConfig install

   新規のログ・データは、ログ・ファイル *ISIM_HOME*¥install_logs¥runConfig.stdout に記録されます。

   詳しくは、 140 ページの『一般に使用されるシステム・プロパティーの構成』を参照してください。

デプロイメント・エラーの修正

IBM Security Identity Manager アプリケーションは、WebSphere Application Server 内で、エンタープライズ・アプリケーションとして稼働します。IBM Security Identity Manager インストール・プログラムでは、WebSphere コマンド行インターフェース (wsadmin) を使用し、IBM Security Identity Manager アプリケーションを WebSphere Application Server にデプロイします。デプロイメントが失敗した場合、エラー・メッセージ内で、setupEnrole.stdout ログ・ファイルの場所が表示されます。

始める前に

WebSphere Application Server が正しくインストールされていることを確認してください。

このタスクについて

デプロイメントが完了すると、IBM Security Identity Manager のファイルは *WAS_NDM_PROFILE_HOME*¥config¥cells¥*cellname*applications¥ITIM.ear ディレクトリーに格納されます。

setupEnrole.stdout ログ・ファイル内でエラーを調査します。次に、以下のタスクを完了します。

手順

1. ログ・データが次のエラーを示している場合は、下記のステップを実行します。
   - WebSphere Application Server 構成マネージャーとの SOAP 接続確立の失敗。
   - 何らかのタイプの WebSphere Application Server スクリプト・エラー。

   a. IBM Security Identity Manager インストール・プログラムを終了します。
   b. WebSphere Application Server へ接続できない問題、またはスクリプト・エラーとして説明されている問題を解決します。詳しくは、WebSphere の資料を参照してください。
   c. 手動で *ISIM_HOME* ディレクトリーのファイルをすべて削除します。
   d. IBM Security Identity Manager インストール・プログラムを再度実行します。
2. 失敗の原因がタイムアウトであることをログ・データが示している場合は、以下のステップを実行します。
   a. IBM Security Identity Manager インストール・プログラムを続行します。
   b. IBM Security Identity Manager インストール・プログラムが完了したら、次のディレクトリーを削除します (存在する場合)。
      WAS_NDM_PROFILE_HOME¥config¥cells¥*cellname*¥applications¥ITIM.ear
   c. 以下のいずれかのコマンドを実行して、IBM Security Identity Manager サーバーを WebSphere Application Server にデプロイします。
      - WebSphere の管理セキュリティーおよびアプリケーション・セキュリティーが有効になっている場合は、以下のいずれかのコマンドを入力します。
        – Windows オペレーティング・システム

          ISIM_HOME¥bin¥setupEnrole.exe install server:*server_name* user:*user_id* password:*pwd* ejbuser:*ejb_user_id* ejbpassword:*ejbpassword*

        – UNIX または Linux オペレーティング・システム

          ISIM_HOME¥bin¥setupEnrole.sh install server:*server_name* user:*user_id* password:*pwd* ejbuser:*ejb_user_id* ejbpassword:*ejbpassword*

          user_id の値は、*wsadmin* などの WebSphere アドミニストレーター・ユーザー ID です。*pwd* の値は、*secret* などの WebSphere アドミニストレーター・ユーザー ID のパスワードです。 *ejb_user_id* の値は、IBM Security Identity Manager EJB ユーザー ID です。これは、デフォルトで WebSphere 管理者ユーザー ID を使用します。

注: EJBUser ID に、スペースがある値 (*Bob Smith* など) が含まれている場合は、その値を引用符で囲む必要があります。例えば、コマンドは以下のように入力する必要があります。

```
SetupEnrole.exe install server:server1 user:wsadmin password:secret
ejbuser:"Bob Smith" ejbpassword:secret
```

- WebSphere の管理セキュリティーおよびアプリケーション・セキュリティーが無効になっている場合は、以下のいずれかのコマンドを入力します。
  - Windows オペレーティング・システム

    ```
    ISIM_HOME¥bin¥setupEnrole.exe install server:server_name
    ```

  - UNIX または Linux オペレーティング・システム

    ```
    ISIM_HOME¥bin¥setupEnrole.exe install server:server_name
    ```

    server_name のデフォルトは、server1 です。

クラスターの開始

クラスターを開始する前に、クラスター・メンバーが実行されているすべてのノード・エージェントを再始動する必要があります。

始める前に

IBM Security Identity Manager のインストールが完了していることを確認します。すべての構成上およびセキュリティー上の変更が完了していることを確認します。

手順

1. IBM Security Identity Manager アプリケーションと IBM Security Identity Manager メッセージング・クラスターの両方を開始します。
   a. 「**サーバー**」 > 「**クラスター**」をクリックします。
   b. IBM Security Identity Manager クラスターを選択します。
   c. 「**開始**」をクリックします。クラスターが開始すると、 IBM Security Identity Manager アプリケーションが開始します。
2. すべての必要なクラスター・メンバーが開始されていることを確認します。
   a. 「**アプリケーション**」 > 「**エンタープライズ・アプリケーション**」をクリックします。 IBM Security Identity Manager アプリケーションの状況を調査します。
   b. 「**サーバー**」 > 「**アプリケーション・サーバー**」をクリックします。 クラスター・メンバーの状況を調査します。
   c. その他の問題のログ・ファイルを調査します。 詳しくは、 188 ページの『ログ・ファイル』を参照してください。
3. IBM Security Identity Manager アプリケーションの状況が部分始動を示す場合、以下のステップを実行します。
   a. 始動に失敗したクラスター・メンバーのあるコンピューターを見つけます。
   b. クラスター・メンバーが存在するコンピューターの以下のログ・ファイルを調べて、IBM Security Identity Manager サーバーが正常に開始されたかどうかを確認します。
      - WAS_PROFILE_HOME¥logs¥server_name¥SystemOut.log
      - TIVOLI_COMMON_DIRECTORY¥CTGIM¥logs¥trace.log

c. 問題を修正します。次に、WebSphere 管理コンソールを使用してクラスター・メンバーを開始します。

次のタスク

インストールを検証します。 121 ページの『第 7 章 インストールの検証』を参照してください。

第 6 章 サイレント・インストールとサイレント構成

IBM Security Identity Manager はサイレント・モードでインストールすることができます。サイレント・モードで読み取る応答ファイルには、ディレクトリー・サーバー、データベース・サーバー、WebSphere Application Server、および IBM Security Identity Manager を構成するための値が含まれています。サイレント・インストールは、単一サーバー環境とクラスター環境の両方で、クリーン・インストールおよびアップグレードに対してサポートされています。

インストール・プログラムは、`installvariables.properties` および `configResponse.properties` という 2 つの応答ファイルからデータを受け取ります。 `installvariables.properties` ファイルには、インストール・ディレクトリー、データベース・タイプ、ディレクトリー・サーバー・タイプなど、インストーラー関連の値があります。 `configResponse.properties` ファイルには、データベース構成プログラム、LDAP 構成プログラム、およびシステム構成プログラムに必要なプロパティーがあり、以下のように、構成プログラムごとに異なる接頭部が付いています。

データベース構成

`dbConfigResponse.`*propertyName*`=`*value*

LDAP 構成

`ldapConfigResponse.`*propertyName*`=`*value*

システム構成

`sysConfigResponse.`*propertyFileName.propertyName*`=`*value*

アップグレード・シナリオには異なるファイル名があります。クリーン・インストールおよびアップグレードを行うには、アプリケーション・サーバーのタイプに応じて、以下の一連の応答ファイルが必要です。

クリーン・インストール

- 単一サーバーまたはデプロイメント・マネージャーの場合:

  `installvariables.properties、configResponse.properties`
- クラスター・メンバーの場合:

  `installvariables.properties、configResponseCM.properties`

アップグレード

- 単一サーバーまたはデプロイメント・マネージャーの場合:

  ```
  installvariablesUpgrade.properties,
  configResponseUpgrade.properties
  ```
- クラスター・メンバーの場合:

  ```
  installvariablesUpgrade.properties,
  configResponseCMUpgrade.properties
  ```

インストール応答ファイルには、別のファイル名を使用できます (installvariablesUpgrade.properties など)。このファイルは、**-f** フラグを指定することにより、インストーラーに渡すことができます。ただし、構成応答ファイルの名前は、常に configResponse.properties にする必要があります。

システム構成プログラムの場合、configResponse.properties テンプレートまたは configResponseUpgrade.properties テンプレートには、接頭部が sysConfigResponse の必要最小限のシステム・プロパティー・セットしか含まれていません。必要により、追加のシステムプロパティーをファイルへ追加します。以下の規則を使用します。

```
sysConfigResponse.propertyFileName.propertyName=value
```

例えば、IBM Tivoli Directory Server 構成の許可 ID が *cn=root* の場合は、以下のようになります。

```
sysConfigResponse.enRoleLDAPConnection.java.naming.provider.url=ldap:
//hostname:389
sysConfigResponse.enRoleLDAPConnection.java.naming.security.principal=cn=root
sysConfigResponse.enRoleLDAPConnection.java.naming.security.credentials=xxxxxx
```

サイレント・モード実行時、システム構成プログラムは、enRoleLDAPConnection.properties ファイルにリストされているプロパティーの値を設定します。

サイレント・インストーラーは、configResponse.properties ファイルの値を読み取り、IBM Security Identity Manager コンポーネントを構成します。特定のコンポーネントの構成が失敗した場合、そのユーティリティーおよび関連付けられた .lax ファイルは *ISIM_HOME*¥bin にあります。インストールの各コンポーネントは、そのコンポーネントの .lax ファイル内の IS_SILENT=<true/false> プロパティーを変更することによって、サイレント・モードで実行できます。

応答ファイルの例

ベース DVD の response_files ディレクトリーに、サンプル応答ファイルがあります。

単一サーバー環境でのサイレント・インストールの実行

単一サーバー環境でクリーン・サイレント・インストールまたはアップグレード・サイレント・インストールを実行するには、以下のステップを実行します。

始める前に

サイレント・インストールを実行する前に、ディレクトリー・サーバー、データベース・サーバー、Directory Integrator、アプリケーション・サーバーなど、必要なミドルウェアをインストールおよび構成する必要があります。また、これらのすべてのコンポーネントが正しく動作しており、正しいデータが入力されていることを確認します。システムのセットアップに誤りがあると、サイレント・インストールが失敗する可能性があります。

手順

1. クリーン・インストールの場合:

a. 応答ファイル `installvariables.properties` および `configResponse.properties` をターゲット・コンピューター上のディレクトリーにコピーします。
b. 応答ファイルを正しい値で更新します。
c. インストーラーと応答ファイルが同じディレクトリーにある場合は、`inst`*`platform`* `-i silent -f installvariables.properties` を実行します。システム・プラットフォームのインストーラー・プログラムの名前は以下のとおりです。
   - Windows オペレーティング・システム: instwin.exe
   - AIX オペレーティング・システム: instaix.bin
   - Linux オペレーティング・システム: instlinux.bin
   - Linux for System p オペレーティング・システム: instplinux.bin
   - Linux for System z オペレーティング・システム: instzlinux.bin
   - Solaris オペレーティング・システム: instsol.bin

   注: インストーラーと応答ファイルが異なるディレクトリーまたは異なるドライブにある場合は、`installvariables.properties` ファイルの相対パスまたは絶対パスを使用します。`configResponse.properties` ファイルの場合も絶対パスを使用する必要があります。例えば、応答ファイルが Windows システム上の `C:¥temp` ディレクトリーにある場合は、次のコマンドを使用します。

   ```
   instwin.exe -i silent -f C:¥temp¥installvariables.properties
   -DITIM_CFG_RESP_FILE_DIR=C:/temp
   ```

   UNIX システムでは、異なるインストーラー・コマンド (AIX の場合の **instaix.bin** など) と異なるパスが使用されます。

2. アップグレード・インストールの場合:
   a. 応答ファイル `installvariablesUpgrade.properties` および `configResponseUpgrade.properties` をターゲット・コンピューター上のディレクトリーにコピーします。
   b. `configResponseUpgrade.properties` ファイルを `configResponse.properties` と名前変更します。
   c. 応答ファイルを正しい値で更新します。
   d. インストーラーと応答ファイルが同じディレクトリーにある場合は、`inst`*`platform`* `-i silent -f installvariablesUpgrade.properties` を実行します。 システム・プラットフォームのインストーラー・プログラムの名前は以下のとおりです。
      - Windows オペレーティング・システム: instwin.exe
      - AIX オペレーティング・システム: instaix.bin
      - Linux オペレーティング・システム: instlinux.bin
      - Linux for System p オペレーティング・システム: instplinux.bin
      - Linux for System z オペレーティング・システム: instzlinux.bin
      - Solaris オペレーティング・システム: instsol.bin

      注: インストーラーと応答ファイルが異なるディレクトリーまたは異なるドライブにある場合は、`installvariablesUpgrade.properties` ファイルの相対

パスまたは絶対パスを使用します。configResponse.properties ファイルの場合も絶対パスを使用する必要があります。例えば、応答ファイルが Windows システム上の C:¥temp ディレクトリーにある場合は、次のコマンドを使用します。

```
instwin.exe -i silent -f C:¥temp¥installvariables.properties
-DITIM_CFG_RESP_FILE_DIR=C:/temp
```

UNIX システムでは、異なるインストーラー・コマンド (AIX の場合の **instaix.bin** など) と異なるパスが使用されます。

次のタスク

サイレント・インストールが完了するまでしばらくかかります。インストールの進行状況を確認するには、itim_install_activity.log ファイルを確認します。このファイルは *ISIM_HOME*¥install_logs ディレクトリーにあります。

インストールを検証して、インストールおよび始動中に発生した問題を解決します。詳しくは、『*インストールの検査*』を参照してください。

共有アクセス・モジュールの別個のインストール

共有アクセス・モジュールの使用可能化ツールは、ターゲット・システム上での共有アクセス・モジュールのサイレント・インストールおよび構成をサポートしています。

インストール時に共有アクセス・モジュールを使用可能にする場合は、installvariables.properties サイレント・インストール応答ファイルで *INSTALL_PIM=1* を変数として設定する必要があります。

クラスター環境でのサイレント・インストールの実行

クラスター環境でクリーン・サイレント・インストールまたはアップグレード・サイレント・インストールを実行するには、以下のステップを実行します。

始める前に

サイレント・インストールを実行する前に、ディレクトリー・サーバー、データベース・サーバー、Directory Integrator、アプリケーション・サーバーなど、必要なミドルウェアをインストールおよび構成する必要があります。また、これらのすべてのコンポーネントが正しく動作しており、正しいデータが入力されていることを確認します。システムのセットアップに誤りがあると、サイレント・インストールが失敗する可能性があります。

手順

1. クリーン・インストールの場合:
   a. デプロイメント・マネージャーで、応答ファイル installvariables.properties および configResponse.properties をターゲット・コンピューター上のディレクトリーにコピーします。
   b. 応答ファイルを正しい値で更新します。

c. インストーラーと応答ファイルが同じディレクトリーにある場合は、inst*platform* -i silent -f installvariables.properties を実行します。システム・プラットフォームのインストーラー・プログラムの名前は以下のとおりです。

- Windows オペレーティング・システム: instwin.exe
- AIX オペレーティング・システム: instaix.bin
- Linux オペレーティング・システム: instlinux.bin
- Linux for System p オペレーティング・システム: instplinux.bin
- Linux for System z オペレーティング・システム: instzlinux.bin
- Solaris オペレーティング・システム: instsol.bin

注: インストーラーと応答ファイルが異なるディレクトリーまたは異なるドライブにある場合は、installvariables.properties ファイルの相対パスまたは絶対パスを使用します。configResponse.properties ファイルの場合も絶対パスを使用する必要があります。例えば、応答ファイルが Windows システム上の C:¥temp ディレクトリーにある場合は、次のコマンドを使用します。

```
instwin.exe -i silent -f C:¥temp¥installvariables.properties
-DITIM_CFG_RESP_FILE_DIR=C:/temp
```

UNIX システムでは、異なるインストーラー・コマンド (AIX の場合の **instaix.bin** など) と異なるパスが使用されます。

d. クラスター・メンバーで、応答ファイル installvariables.properties および configResponseCM.properties をターゲット・コンピューター上のディレクトリーにコピーします。

e. configResponseCM.properties ファイルを configResponse.properties と名前変更します。

f. 応答ファイルを正しい値で更新します。

g. インストーラーと応答ファイルが同じディレクトリーにある場合は、inst*platform* -i silent -f installvariables.properties を実行します。システム・プラットフォームのインストーラー・プログラムの名前は以下のとおりです。

- Windows オペレーティング・システム: instwin.exe
- AIX オペレーティング・システム: instaix.bin
- Linux オペレーティング・システム: instlinux.bin
- Linux for System p オペレーティング・システム: instplinux.bin
- Linux for System z オペレーティング・システム: instzlinux.bin
- Solaris オペレーティング・システム: instsol.bin

注: インストーラーと応答ファイルが異なるディレクトリーまたは異なるドライブにある場合は、installvariables.properties ファイルの相対パスまたは絶対パスを使用します。configResponse.properties ファイルの場合も絶対パスを使用する必要があります。例えば、応答ファイルが Windows システム上の C:¥temp ディレクトリーにある場合は、次のコマンドを使用します。

```
instwin.exe -i silent -f C:¥temp¥installvariables.properties
-DITIM_CFG_RESP_FILE_DIR=C:/temp
```

UNIX システムでは、異なるインストーラー・コマンド (AIX の場合の **instaix.bin** など) と異なるパスが使用されます。

2. アップグレード・インストールの場合:
   a. デプロイメント・マネージャーで、応答ファイル `installvariablesUpgrade.properties` および `configResponseUpgrade.properties` をターゲット・コンピューター上のディレクトリーにコピーします。
   b. `configResponseUpgrade.properties` ファイルを `configResponse.properties` と名前変更します。
   c. 応答ファイルを正しい値で更新します。
   d. インストーラーと応答ファイルが同じディレクトリーにある場合は、`inst`*`platform`* `-i silent -f installvariablesUpgrade.properties` を実行します。 システム・プラットフォームのインストーラー・プログラムの名前は以下のとおりです。
      - Windows オペレーティング・システム: instwin.exe
      - AIX オペレーティング・システム: instaix.bin
      - Linux オペレーティング・システム: instlinux.bin
      - Linux for System p オペレーティング・システム: instplinux.bin
      - Linux for System z オペレーティング・システム: instzlinux.bin
      - Solaris オペレーティング・システム: instsol.bin

      注: インストーラーと応答ファイルが異なるディレクトリーまたは異なるドライブにある場合は、`installvariablesUpgrade.properties` ファイルの相対パスまたは絶対パスを使用します。 `configResponse.properties` ファイルの場合も絶対パスを使用する必要があります。例えば、応答ファイルが Windows システム上の `C:¥temp` ディレクトリーにある場合は、次のコマンドを使用します。

      ```
      instwin.exe -i silent -f C:¥temp¥installvariables.properties
      -DITIM_CFG_RESP_FILE_DIR=C:/temp
      ```

      UNIX システムでは、異なるインストーラー・コマンド (AIX の場合の **instaix.bin** など) と異なるパスが使用されます。
   e. クラスター・メンバーで、応答ファイル `installvariablesUpgrade.properties` および `configResponseCMUpgrade.properties` をターゲット・コンピューター上のディレクトリーにコピーします。
   f. `configResponseCMUpgrade.properties` ファイルを `configResponse.properties` と名前変更します。
   g. 応答ファイルを正しい値で更新します。
   h. インストーラーと応答ファイルが同じディレクトリーにある場合は、`inst`*`platform`* `-i silent -f installvariablesUpgrade.properties` を実行します。 システム・プラットフォームのインストーラー・プログラムの名前は以下のとおりです。
      - Windows オペレーティング・システム: instwin.exe
      - AIX オペレーティング・システム: instaix.bin

- Linux オペレーティング・システム: instlinux.bin
- Linux for System p オペレーティング・システム: instplinux.bin
- Linux for System z オペレーティング・システム: instzlinux.bin
- Solaris オペレーティング・システム: instsol.bin

注: インストーラーと応答ファイルが異なるディレクトリーまたは異なるドライブにある場合は、`installvariablesUpgrade.properties` ファイルの相対パスまたは絶対パスを使用します。 `configResponse.properties` ファイルの場合も絶対パスを使用する必要があります。例えば、応答ファイルが Windows システム上の `C:¥temp` ディレクトリーにある場合は、次のコマンドを使用します。

```
instwin.exe -i silent -f C:¥temp¥installvariables.properties
-DITIM_CFG_RESP_FILE_DIR=C:/temp
```

UNIX システムでは、異なるインストーラー・コマンド (AIX の場合の `instaix.bin` など) と異なるパスが使用されます。

次のタスク

サイレント・インストールが完了するまでしばらくかかります。インストールの進行状況を確認するには、`itim_install_activity.log` ファイルを確認します。このファイルは *ISIM_HOME*`¥install_logs` ディレクトリーにあります。

インストールを検証して、インストールおよび始動中に発生した問題を解決します。詳しくは、『*インストールの検査*』を参照してください。

共有アクセス・モジュールの別個のインストール

共有アクセス・モジュールの使用可能化ツールは、ターゲット・システム上での共有アクセス・モジュールのサイレント・インストールおよび構成をサポートしています。

インストール時に共有アクセス・モジュールを使用可能にする場合は、`installvariables.properties` サイレント・インストール応答ファイルで *INSTALL_PIM=1* を変数として設定する必要があります。

サイレント・インストール応答ファイル

ベース DVD の `response_files` ディレクトリーに、サンプル応答ファイルが提供されています。

サイレント・モードによるデータベースの構成

サイレント・インストール中にデータベース構成が失敗した場合、`configResponse.properties` ファイル内の情報を訂正してから、サイレント・データベース構成を開始することができます。

始める前に

応答ファイル用の正しいデータベース情報を取得します。

手順

1. configResponse.properties ファイルをターゲット・コンピューター上のディレクトリーにコピーします。
2. 正しいデータベース情報で configResponse.properties ファイルを更新します。
3. *ISIM_HOME*/bin/DBConfig.lax ファイルを編集し、以下のプロパティーに値を設定します。

   ```
   IS_SILENT=true
   RESPONSE_FILE=full path to the configResponse.properties file
   ```

4. 以下のコマンドを実行し、データベース構成プログラムを開始します。

   ```
   ISIM_HOME/bin/DBConfig
   ```

例

ベース DVD の response_files ディレクトリーに、サンプル応答ファイルがあります。

次のタスク

データベース構成が完了するまで数分かかります。構成の進行状況をモニターするには、*ISIM_HOME*/install_logs ディレクトリーの dbConfig.stdout ファイルを表示します。

サイレント・モードによるディレクトリー・サーバーの構成

サイレント・インストール中にディレクトリー・サーバーの構成が失敗した場合は、以下の手順に従ってディレクトリー・サーバーのサイレント構成を行ってください。

始める前に

応答ファイル用の正しいディレクトリー・サーバー情報を取得します。

手順

1. configResponse.properties ファイルをターゲット・コンピューター上のディレクトリーにコピーします。
2. 正しいデータベース情報で configResponse.properties ファイルを更新します。
3. *ISIM_HOME*/bin/ldapConfig.lax ファイルを編集し、以下のプロパティーに値を設定します。

   ```
   IS_SILENT=true
   RESPONSE_FILE=full path to the configResponse.properties file
   ```

4. 以下のコマンドを実行し、LDAP 構成プログラムを開始します。

   ```
   ISIM_HOME/bin/ldapConfig
   ```

例

ベース DVD の response_files ディレクトリーに、サンプル応答ファイルが提供されています。

次のタスク

ディレクトリー・サーバー構成が完了するまで数分かかります。構成の進行状況をモニターするには、*ISIM_HOME*/install_logs ディレクトリーの ldapConfig.stdout ファイルを表示します。

単一サーバー環境でのサイレント・モードによるシステムの構成

サイレント・インストール中にデータベースの構成が失敗した場合は、以下の手順に従ってシステムをサイレント・モードで構成します。

始める前に

応答ファイル用の正しいシステム情報を取得します。

手順

1. configResponse.properties ファイルをターゲット・コンピューター上のディレクトリーにコピーします。
2. 正しいシステム情報で configResponse.properties ファイルを更新します。
3. *IISIM_HOME*/bin/DBConfig.lax ファイルを編集し、以下のプロパティーに値を設定します。

   ```
   IS_SILENT=true
   RESPONSE_FILE=full path to the configResponse.properties file
   ```

4. WebSphere Application Server を開始します。
5. 以下のコマンドを実行し、サーバー構成プログラムを開始します。

   ```
   ISIM_HOME/bin/runConfig -install
   ```

例

ベース DVD の response_files ディレクトリーに、サンプル応答ファイルが提供されています。

次のタスク

システム構成が完了するまで数分かかります。構成の進行状況をモニターするには、*ISIM_HOME*/install_logs ディレクトリーの runConfig.stdout ファイルを表示します。

クラスター環境でのサイレント・モードによるシステムの構成

サイレント・インストール中にシステムの構成が失敗した場合は、以下の手順に従って、再度、システムをサイレント・モードで構成します。

始める前に

応答ファイル用の正しいシステム情報を取得します。

手順

1. デプロイメント・マネージャー上で、configResponse.properties ファイルをターゲット・コンピューター上のディレクトリーにコピーします。

2. クラスター・メンバー・システム上で、configResponseCM.properties ファイルをターゲット・コンピューター上のディレクトリーにコピーし、ファイル名を configResponse.properties に変更します。
3. 正しいシステム情報で configResponse.properties ファイルを更新します。
4. *ISIM_HOME*/bin/DBConfig.lax ファイルを編集し、以下のプロパティーに値を設定します。

   ```
   IS_SILENT=true
   RESPONSE_FILE=full path to the configResponse.properties file
   ```

5. WebSphere デプロイメント・マネージャーおよびすべてのノード・エージェントを開始します。
6. 以下のコマンドを実行し、サーバー構成プログラムを開始します。

   ```
   ISIM_HOME/bin/runConfig -install
   ```

例

ベース DVD の response_files ディレクトリーに、サンプル応答ファイルが提供されています。

次のタスク

システム構成が完了するまで数分かかります。構成の進行状況をモニターするには、*ISIM_HOME*/install_logs ディレクトリーの runConfig.stdout ファイルを表示します。

第 7 章 インストールの検証

このセクションでは、IBM Security Identity Manager サーバーが使用するデータベース、ディレクトリー・サーバー、およびその他のプログラムが正常に構成されているかどうかを検証する方法について説明します。これらは、IBM Security Identity Manager サーバーと完全に通信できる必要もあります。

WebSphere Application Server が実行中であることの検証

IBM Security Identity Manager アプリケーションをデプロイする WebSphere Application Server が実行されている必要があります。

始める前に

IBM Security Identity Manager およびそのコンポーネントのインストールおよび構成タスクがすべて完了していることを確認します。

手順

次のコマンドのいずれかを入力します。

- Windows オペレーティング・システム

  WAS_PROFILE_HOME¥bin¥serverStatus.bat -all
- UNIX または Linux オペレーティング・システム

  WAS_PROFILE_HOME/bin/serverStatus.sh -all

注: プロセスが実行されていない場合は、以下のいずれかのコマンドを実行してサーバーを始動します。

- Windows オペレーティング・システム
  - *WAS_PROFILE_HOME*¥bin¥startServer.bat *server_name*
- UNIX または Linux オペレーティング・システム -
  - *WAS_PROFILE_HOME*/bin/startServer.sh *server_name*

  server_name の値は、WebSphere Application Server の名前です。例えば、server1 です。

次のタスク

さらに、logs ディレクトリーのログ・ファイルに、server1 の状況を示す項目があるかどうか調べてください。例えば、*WAS_PROFILE_HOME*¥logs¥server1 ディレクトリー内のログ・ファイルを調べます。

サーバーを始動できない場合は、 173 ページの『第 10 章 トラブルシューティング』を参照してください。

WebSphere 管理コンソールを開始して追加の検証タスクを実行します。

WebSphere Application Server 管理コンソールの開始

IBM Security Identity Manager のコンポーネントが正しく実行されていることを確認できるようにするために、WebSphere Application Server 管理コンソールを実行しておく必要があります。

始める前に

WebSphere Application Server のユーザー ID を保持している必要があります。セキュリティーが有効になっている場合は、パスワードも必要です。

手順

1. Web ブラウザーで次のアドレスを入力します。

   ```
   http://hostname:port/ibm/console
   ```

   hostname の値は、WebSphere Application Server が実行されているコンピューターの完全修飾ホスト名または IP アドレスです。*port* の値は、WebSphere 管理 HTTP トランスポートのポート番号です。デフォルト値は 9060 です。
2. ユーザー ID、および必要に応じてパスワードを入力します。
3. 「**OK**」をクリックします。

次のタスク

さまざまな管理タスクを引き続き実行して IBM Security Identity Manager のインストールを検証できます。

データベース接続の検証

IBM Security Identity Manager サーバーを開始する前に、管理コンソールを使用してデータベース接続をテストします。

始める前に

データベースがインストールされており、実行中であることを確認します。

WebSphere Application Server が実行されており、WebSphere 管理コンソールが開始されていることを確認します。

手順

1. WebSphere 管理コンソールにログオンします。
2. 「**リソース**」 > 「**JDBC**」 > 「**データ・ソース**」を選択します。
3. 「**ITIM データ・ソース**」を選択します。
4. 「**接続のテスト**」をクリックします。 テスト結果を示すメッセージが開きます。
5. 以下に対して上記のステップを繰り返します。
   - **ITIM バスのデータ・ソース**
   - クラスターの場合のみ追加で **ITIM バスの共有データ・ソース**

次のタスク

機能しない接続がある場合は、173 ページの『第 10 章 トラブルシューティング』を参照してください。

その他の検証タスクを実行します。

ディレクトリー・サーバーが正常に実行されていることの検証

この情報では、IBM Security Identity Manager 用のインストール済みディレクトリー・サーバーが実行中であることを確認するためのステップについて説明します。

始める前に

ディレクトリー・サーバーがインストールされていることを確認します。

手順

1. IBM Tivoli Directory Server が実行中であるかどうか判断します。
   - Windows オペレーティング・システム:
     a. 「**スタート**」 > 「**プログラム**」 > 「**管理ツール**」 > 「**サービス**」をクリックします。
     b. ディレクトリー・サーバー項目 (サポート対象の IBM Tivoli Directory Server インスタンスの場合は ldapdb2 など) を特定します。
     c. ディレクトリー・サーバー・サービスが開始済みであることを確認します。

        サービスが開始されていない場合は、サービスを選択し、「サービス」ウィンドウのメインメニューから「**アクション**」 > 「**開始**」を選択します。
   - UNIX または Linux オペレーティング・システム:

     ibmslapd プロセスが実行中であることを確認します。次のコマンドを入力します。

     ```
     ps -ef | grep ibmslapd
     ```

     IBM Tivoli Directory Server が実行中の場合は、プロセス ID ID (PID) 番号が戻されます。PID 番号が戻されない場合は、サーバーを再始動する必要があります。

     a. サーバーを停止します。

        ```
        ibmslapd -I instancename -k
        ```

     b. サーバーを始動します。

        ```
        ibmslapd -I instancename
        ```

2. IBM Tivoli Directory Server が実行中である場合は、IBM Tivoli Directory Server が構成モードのみではないことを確認します。 次のコマンドを入力します。

   ```
   ldapsearch -s base -b " " objectclass=* ibm-slapdisconfigurationmode
   ```

   IBM Tivoli Directory Server が構成モードになっていない場合、ibm-slapdisconfigurationmode パラメーターの値は FALSE です。**ldapsearch** コマンドは、LDAP サーバーへの接続を開いてバインドし、検索を開始します。 -s

パラメーターは、base、one、または sub という検索の有効範囲を指定します。これらはそれぞれ、基本オブジェクト、1 つのレベル、またはサブツリーを検索します。-b パラメーターは、検索の開始点として、デフォルトではなく *searchbase* を使用します。

次のタスク

追加の検証タスクを実行します。

IBM Security Identity Manager バスおよびメッセージング・エンジンの確認

IBM Security Identity Manager サーバーを開始する前に、WebSphere 管理コンソールを使用してバスおよびメッセージング・エンジンの状況を確認します。

始める前に

WebSphere Application Server が実行されており、WebSphere 管理コンソールが開始されていることを確認します。

手順

1. WebSphere 管理コンソールにログオンします。
2. 「**サービス統合**」 > 「**バス**」を選択します。
3. 「**itim_bus**」をクリックします (存在する場合)。
4. 「トポロジー」セクションで、「**メッセージング・エンジン**」をクリックします。
5. エンジン名と状況を確認します。
   - 単一サーバー・インストールの場合、*nodename.servername*-itim_bus という名前のエンジンが表示されます。
   - クラスター・インストールの場合、*n*+1 個のメッセージング・エンジンが表示されます。*n* は IBM Security Identity Manager クラスター・メンバーの数です。追加のメッセージング・エンジンが IBM Security Identity Manager メッセージング・クラスター用に使用されています。これらのメッセージング・エンジンをすべて開始します。

   メッセージング・エンジンが開始されていない場合は、メッセージング・エンジン名をクリックして「**開始**」をクリックします。

次のタスク

メッセージング・エンジンを開始できない場合は、 173 ページの『第 10 章 トラブルシューティング』を参照してください。

その他の検証タスクを実行します。

IBM Security Identity Manager サーバーの検証

インストールしたコンポーネントがすべて稼働していることを確認したら、IBM Security Identity Manager サーバーが正常に稼働していることを確認します。

IBM Security Identity Manager は、以下のいずれかの環境にインストールします。

- 単一サーバー
- クラスター

適切な方法を選択して、IBM Security Identity Manager サーバーが正常に稼働していることを確認します。

IBM Security Identity Manager サーバーが単一サーバー環境で作動可能であるかどうかの検証

インストール後のタスクまたは構成タスクを続行する前に、WebSphere 管理コンソールを通じて IBM Security Identity Manager にログオンできることを検証する必要があります。

始める前に

IBM Security Identity Manager のすべてのインストール・タスクが完了しており、すべての必須コンポーネントが実行中であることを確認します。

WebSphere Application Server が実行中であり、管理コンソールが開始されていることを確認します。

手順

1. WebSphere 管理コンソールにログオンします。
2. 管理コンソールで、「**アプリケーション**」 > 「**エンタープライズ・アプリケーション**」をクリックし、IBM Security Identity Manager サーバーが実行中であることを確認します。IBM Security Identity Manager サーバーおよび他のプロセスが実行中であることを検証する追加ステップについては、 121 ページの『第 7 章 インストールの検証』を参照してください。
3. WebSphere 内蔵 HTTP トランスポートを通じて IBM Security Identity Manager サーバーにログオンします。 次の Web アドレスをブラウザーに入力します。

   ```
   http://hostname:port/itim/console
   ```

   hostname の値は、WebSphere Application Server のホスト名です。 *port* の値は、WebSphere 仮想ホストのデフォルトのポート番号です。デフォルトのポート番号は 9080 です。同一のシステムに WebSphere Application Server の複数のインストール済み環境が存在する場合、このポート番号は 9081 など別の値である場合があります。フロントエンド・プロキシーとして HTTP サーバーを使用する場合は、ポート番号を除去できます。 ブラウザーに、IBM Security Identity Manager のログオン・ウィンドウが表示されます。
4. 管理者ユーザー ID (`itim manager`) とパスワード (`secret`) を入力します。

注: バックアップ用の管理者ユーザー ID を作成しておくことをお勧めします。この ID は、`itim manager` ユーザー ID と同じアクセス権限を保持している必要があります。

5. パスワードを変更します。 最初にログオンに成功した直後に、ログオン・ウィンドウで、アドミニストレーター・パスワードを変更するように促すプロンプトが出されます。パスワードが正常に変更されたことを確認します。パスワードを変更した後、組織のオブジェクトおよび ITIM ユーザーと呼ばれるユーザーを作成できます。
6. 内蔵 HTTP トランスポートを通じて正常にログオンできたら、IBM HTTP Server を通じて IBM Security Identity Manager サーバーにログオンします。このログオン操作は、IBM HTTP Server と WebSphere Web サーバー・プラグインがインストールおよび構成されている場合にのみ実行します。 次の Web アドレスをブラウザーに入力します。

   `http://`*`hostname`*`:`*`port`*`/itim/console`

   hostname の値は、IBM HTTP Server のホスト名です。*port* の値は、WebSphere 仮想ホストのポート番号です。デフォルトのポート番号は 9080 です。フロントエンド・プロキシーとして HTTP サーバーを使用する場合は、ポート番号を除去できます。

次のタスク

IBM Security Identity Manager の始動およびログオンができない場合、 173 ページの『第 10 章 トラブルシューティング』を参照してください。

オプションのポストインストール・タスクまたは構成タスクを実行します。 135 ページの『第 9 章 IBM Security Identity Manager サーバーの構成』を参照してください。

IBM Security Identity Manager サーバーがクラスター環境で作動可能であることの検証

インストール後のタスクまたは構成タスクを続行する前に、WebSphere 管理コンソールを通じて IBM Security Identity Manager にログオンできることを検証する必要があります。

始める前に

IBM Security Identity Manager のすべてのインストール・タスクが完了していることを確認します。すべての必須コンポーネントが実行中であることを確認します。

WebSphere Application Server が実行されており、WebSphere 管理コンソールが開始されていることを確認します。

手順

1. WebSphere 管理コンソールにログオンします。
2. IBM Security Identity Manager アプリケーションと IBM Security Identity Manager メッセージング・クラスターの両方を開始します。
   a. 「**サーバー**」 > 「**クラスター**」をクリックします。

b. IBM Security Identity Manager クラスターを選択します。

c. 「**開始**」をクリックします。 クラスターが開始すると、 IBM Security Identity Manager アプリケーションが開始します。

3. WebSphere 内蔵 HTTP 転送を使用して、IBM Security Identity Manager サーバーにログオンします。 ブラウザー・ウィンドウで、以下のコマンドを入力します。

   `http://hostname:port/itim/console/`

   hostname の値は、WebSphere Application Server クラスター・メンバーおよび IBM Security Identity Manager サーバー・アプリケーションをホストしているコンピューターの完全修飾名または IP アドレスです。 port の値は、WebSphere 仮想ホストのポート番号です。デフォルトのポート番号は 9080 です。同一のコンピューター上に WebSphere Application Server の複数インスタンスが存在する場合は、ポート番号は 9081 などの別の値になっていることがあります。フロントエンド・プロキシーとして HTTP サーバーを使用する場合は、ポート番号を除去できます。詳しくは、 186 ページの『デフォルト・ホストのポート番号の判別』を参照してください。 ブラウザーに、IBM Security Identity Manager のログオン・ウィンドウが表示されます。

4. IBM Security Identity Manager サーバーの管理者ユーザー ID (`itim manager`) とパスワードを入力します。 インストール直後のパスワードの値は `secret` です。

   注: バックアップ用の管理者ユーザー ID を作成しておくことをお勧めします。この ID は、`itim manager` ユーザー ID と同じアクセス権限を保持している必要があります。

5. パスワードを変更します。 最初にログオンに成功した直後に、ログオン・ウィンドウで、アドミニストレーター・パスワードを変更するように促すプロンプトが出されます。パスワードが正常に変更されたことを確認します。パスワードを変更した後、組織のオブジェクトおよび ITIM ユーザーと呼ばれるユーザーを作成できます。

次のタスク

IBM Security Identity Manager の始動およびログオンができない場合、 173 ページの『第 10 章 トラブルシューティング』を参照してください。

オプションのポストインストール・タスクまたは構成タスクを実行します。 135 ページの『第 9 章 IBM Security Identity Manager サーバーの構成』を参照してください。

第 8 章 共有アクセス・モジュールの構成

シナリオによっては、手動ステップを実行して、共有アクセス・モジュールを構成する必要があります。

初期構成

初期構成のシナリオは、IBM Security Identity Manager の初期インストールと、IBM Tivoli Identity Manager の前のバージョンからのアップグレードの両方に適用されます。

初期構成のタスクは、初期インストール時に共有アクセス・モジュールを選択したかどうかと、IBM Security Identity Manager を WebSphere 単一サーバーと WebSphere クラスターのどちらにデプロイするかによって異なります。

注: 初期インストール時に共有アクセス・モジュールをインストールしなかった 場合、IBM Security Identity Manager を再インストールする必要はありませんが、共有アクセス・モジュールを構成する必要があります。また、共有アクセス・モジュールを使用するためには、IBM Security Privileged Identity Manager ライセンスも必要です。

表 10 で、ご使用のデプロイメントに合った指示を参照してください。

表 10. 共有アクセス・モジュールの初期構成シナリオ

シナリオ	構成は必要か
• IBM Security Identity Manager を WebSphere 単一サーバー にインストールした • 共有アクセス・モジュールをインストールした	共有アクセス・モジュールに対して構成タスクを実行する必要はありません。
• IBM Security Identity Manager を WebSphere 単一サーバー にインストールした • 共有アクセス・モジュールをインストールしなかった • 今、共有アクセス・モジュールを使用したい	共有アクセス・モジュールによって使用されるデータおよびプロパティーを構成する必要があります。 130 ページの『WebSphere 単一サーバーでの共有アクセス・モジュールの構成』を参照してください。
• IBM Security Identity Manager を WebSphere クラスター にインストールした • 共有アクセス・モジュールをインストールした	すべてのクラスター・メンバーによって使用されるクレデンシャル・ボールト・サーバーの設定を構成する必要があります。 131 ページの『WebSphere クラスターでの共有アクセス・モジュールの構成』を参照してください。

表 10. 共有アクセス・モジュールの初期構成シナリオ (続き)

シナリオ	構成は必要か
• IBM Security Identity Manager を WebSphere クラスター にインストールした • 共有アクセス・モジュールをインストールしなかった • 今、共有アクセス・モジュールを使用したい	以下を構成する必要があります。 • 共有アクセス・モジュールによって使用されるデータおよびプロパティー。 • すべてのクラスター・メンバーによって使用されるクレデンシャル・ボールト・サーバーの設定。 131 ページの『WebSphere クラスターでの共有アクセス・モジュールの構成』を参照してください。

再構成

共有アクセス・モジュールの初期構成が完了した後、ディレクトリー・サーバーまたはデータベースを再構成する場合は、共有アクセス・モジュールを再構成する必要があります。

データベースを再構成した場合に、デプロイメントが WebSphere クラスター内であるときは、クレデンシャル・ボールト・サーバー用の鍵ファイルを再生成する必要もあります。

詳しくは、 309 ページの『付録 B. 共有アクセスの再構成』を参照してください。

WebSphere 単一サーバーでの共有アクセス・モジュールの構成

WebSphere 単一サーバーで使用する共有アクセス・モジュールを構成するには、**SAConfig** ユーティリティーを使用します。

このタスクについて

IBM Security Identity Manager の初期インストール時に共有アクセス・モジュールをインストールしないことを選択した場合は、**SAConfig** ユーティリティーを実行してその構成を行う必要があります。

手順

1. IBM Security Identity Manager のデータベースが構成されていることを確認します。

   データベースを構成していなかった場合は、**DBConfig** コマンドを使用します。135 ページの『手動による DBConfig データベース構成ツールの開始』に記載されている手順を完了します

2. IBM Security Identity Manager のディレクトリー・サーバーが構成されていることを確認します。

   ディレクトリー・サーバーを構成していなかった場合は、**ldapConfig** コマンドを使用します。137 ページの『手動による ldapConfig 構成ツールの実行』に記載されている手順を完了します。

3. IBM Security Identity Manager のインストール・ロケーション内の bin ディレクトリーに移動し、ユーティリティーを実行します。

   以下に例を示します。

表 11. SAConfig の実行

オペレーティング・システム	コマンド
Windows	C:¥Program Files¥IBM¥isim¥bin で、「SAConfig」をクリックするか、コマンド・ウィンドウを開いて **SAConfig** と入力します。
UNIX または Linux	/opt/IBM/isim/bin で、**./SAConfig** と入力します。

4. WebSphere Application Server を再始動します。

WebSphere クラスターでの共有アクセス・モジュールの構成

WebSphere クラスターで共有アクセス・モジュールを構成することができます。

始める前に

IBM Security Identity Manager を WebSphere クラスターに正常にインストールしました。

このタスクについて

また、クレデンシャル・ボールト・サーバーの鍵ストア・ファイルの再構成も行う必要があります。

IBM Security Identity Manager のインストール時に共有アクセス・モジュールをインストールしなかった場合は、**SAConfig** ユーティリティーを実行してその構成を行う必要があります。

手順

1. IBM Security Identity Manager のデータベースが構成されていることを確認します。

   データベースを構成していなかった場合は、**DBConfig** コマンドを使用します。135 ページの『手動による DBConfig データベース構成ツールの開始』に記載されている手順を完了します。

2. IBM Security Identity Manager のディレクトリー・サーバーが構成されていることを確認します。

   ディレクトリー・サーバーを構成していなかった場合は、**ldapConfig** コマンドを使用します。137 ページの『手動による ldapConfig 構成ツールの実行』に記載されている手順を完了します。

3. IBM Security Identity Manager のインストール時に共有アクセス・モジュールをインストールしなかった場合は、**SAConfig** ユーティリティーを実行してその構成を行う必要があります。

   IBM Security Identity Manager のインストール・ロケーション内の bin ディレクトリーに移動し、ユーティリティーを実行します。

注: このコマンドは、デプロイメント・マネージャーおよび各クラスター・メンバー上で実行する必要があります。

以下に例を示します。

表 12. SAConfig の実行

オペレーティング・システム	コマンド
Windows	C:¥Program Files¥IBM¥isim¥bin で、「SAConfig」をクリックするか、コマンド・ウィンドウを開いて **SAConfig** と入力します。
UNIX または Linux	/opt/IBM/isim/bin で、**./SAConfig** と入力します。

4. ISIM_HOME/data/KMIPServer.properties ファイルの clipassword プロパティーを更新します。

   どのようなストリング値でも指定できます。以下に例を示します。

   ```
   clipassword=test
   ```

   注: このファイルは、デプロイメント・マネージャー上でのみ編集してください。
5. クレデンシャル・ボールト・サーバーの鍵ストア・ファイルを構成します。

   注: このステップは、デプロイメント・マネージャーでのみ実行します。クラスター・メンバーでは、このステップは実行する必要はありません。

   次のコマンドで、-p パラメーターの値が、ISIM_HOME/data/KMIPServer.properties ファイルの clipassword に指定した値と同じであることを確認します。

   以下のとおり、ご使用のオペレーティング・システム用のコマンドを使用します。

   - Windows オペレーティング・システムの場合、次のように入力します。

     ```
     cd /d "ISIM_HOME¥lib"
     ```

     ISIM_HOME¥lib ディレクトリーから次のコマンドを実行します。

     ```
     "ISIM_HOME¥jre¥jre¥bin¥java"-cp
     com.ibm.sec.authz.jaccplus_7.3.1.jar;
     com.ibm.sec.authz.xacml4j_7.3.1.jar;
     j2ee.jar;
     ojdbc.jar;
     db2jcc.jar;
     db2jcc_license_cu.jar;
     sqljdbc.jar;
     com.ibm.tklm.kmip.jar;
     CVCommon.jar;
     CVCore.jar;
     CVCli.jar;
     com.ibm.tklm.credvault.common.jar;
     commons-cli.jar;
     com.ibm.cv.kmip.ext.jar
     -DKMIPConfigProperties="$USER_INSTALL_DIR$$¥$data$¥$KMIPServer.properties"
     -Djava.security.auth.login.config==login.config
     -Djava.security.auth.policy==jaas.policy
     com.ibm.cv.cli.CVShell -u test -p test
     ```

- UNIX または Linux オペレーティング・システムの場合、次のように入力します。

  ```
  cd "ISIM_HOME/lib"
  ```

  ISIM_HOME¥lib ディレクトリーから次のコマンドを実行します。

  ```
  "ISIM_HOME/jre/jre/bin/java"-cp
  com.ibm.sec.authz.jaccplus_7.3.1.jar:
  com.ibm.sec.authz.xacml4j_7.3.1.jar:
  j2ee.jar:
  ojdbc.jar:
  db2jcc.jar:
  db2jcc_license_cu.jar:
  sqljdbc.jar:
  com.ibm.tklm.kmip.jar:
  CVCommon.jar:
  CVCore.jar:
  CVCli.jar:
  com.ibm.tklm.credvault.common.jar:
  commons-cli.jar:
  com.ibm.cv.kmip.ext.jar:
  -DKMIPConfigProperties="$USER_INSTALL_DIR$$/$data$/$KMIPServer.properties"
  -Djava.security.auth.login.config==login.config
  -Djava.security.auth.policy==jaas.policy
  com.ibm.cv.cli.CVShell -u test -p test
  ```

  このコマンドにより、cvKeystore.jceks および pwdEncKeystore.jceks という 2 つのクレデンシャル・ボールト鍵ストア・ファイルが *ISIM_HOME*/data/keystore ディレクトリーの下に生成されます。また、*ISIM_HOME*/data/KMIPServer.properties 内の暗号鍵、およびクレデンシャル・ボールト・データベースのデータ・エントリーが更新されます。

6. 生成された鍵ストア・ファイルと KMIPServer.properties を WAS_DM_profile_path/config/cells/*cellName*/itim ディレクトリーにコピーします。

   注: このステップは、デプロイメント・マネージャーでのみ実行します。クラスター・メンバーでは、このステップは実行する必要はありません。

7. WebSphere Application Server デプロイメント・マネージャー・コンソールから手動でノードを同期化します。
8. 各クラスター・メンバー上で、WebSphere プロファイル・ディレクトリー階層にある次のクレデンシャル・ボールト・ファイルを IBM Security Identity Manager データ・ディレクトリー階層にコピーします。

表 13. コピーするクレデンシャル・ボールト・サーバー・ファイル

コピーするファイル	コピー先
WAS_PROFILE_PATH/config/cells/*cellName*/itim/cvKeystore.jceks	*ISIM_HOME*/data/keystore/cvKeystore.jceks
WAS_PROFILE_PATH/config/cells/*cellName*/itim/pwdEncKeystore.jceks	*ISIM_HOME*/data/keystore/pwdEncKeystore.jceks
WAS_PROFILE_PATH/config/cells/*cellName*/itim/KMIPServer.properties	*ISIM_HOME*/data/KMIPServer.properties

9. WebSphere Application Server クラスターを再始動します。

第 9 章 IBM Security Identity Manager サーバーの構成

インストールを検証した後、各種のインストール後のタスク (オプション) を完了したり、構成エラーを修正したり、構成設定を変更したりできます。

IBM Security Identity Manager のインストール・プロセスでは、DBConfig や ldapConfig などの各種の構成ツールが自動的に実行されます。インストール時に問題が発生した場合や、インストール時に構成ツールを実行しないことを選択した場合は、手動でプロセスを実行できます。これらの手動プロセスを使用して構成を変更することも可能です。

IBM Security Identity Manager データベースの構成

IBM Security Identity Manager インストール・プログラムは、DBConfig データベース構成ツールを自動的に使用して、IBM Security Identity Manager と共に機能するようにデータベースをセットアップします。この構成は、シングル・サーバー・インストール時、またはデプロイメント・マネージャー上でのクラスター・インストール時に実行されます。

データベースの初期インストールおよび構成について詳しくは、18 ページの『データベースのインストールと構成』を参照してください。

手動による DBConfig データベース構成ツールの開始

DBConfig コマンドは、IBM Security Identity Manager が必要とするデータベース・テーブル定義を作成します。インストール中にコマンドがデータベースの構成に失敗した場合のみ、このコマンドを実行してください。データベース・テーブルがあらかじめ設定されている状態で **DBConfig** コマンドを実行すると、最初に、既存のすべてのデータベース・テーブルが除去されます。データベース・テーブルの除去をキャンセルした場合、データベースの構成が失敗する可能性があるため、手動で **DBConfig** コマンドを実行する必要があります。

始める前に

インストール後にこのコマンドを実行する場合は、**DBConfig** を実行する前に、WebSphere Application Server 管理コンソールから、サービス統合バス (itim_bus) のもとにあるメッセージング・エンジンが停止されていることを確認してください。サービス統合バスを停止するには、WebSphere 管理コンソールにログオンして、以下のステップを実行します。

1. 「**サービス統合**」 > 「**バス**」をクリックします。
2. 「**itim_bus**」をクリックします (存在する場合)。
3. 「トポロジー」セクションで、「**メッセージング・エンジン**」をクリックします。

   単一サーバー・インストールの場合、*nodename.servername*-itim_bus という名前のエンジンが表示されます。

クラスター・インストールの場合、*n*+1 個のメッセージング・エンジンが表示されます。*n* は IBM Security Identity Manager クラスター・メンバーの数です。追加のメッセージング・エンジンが IBM Security Identity Manager メッセージング・クラスター用に使用されています。

4. 1 つ以上のメッセージング・エンジンを選択し、「**停止**」をクリックします。

このタスクについて

データベース構成ツールを実行すると *ISIM_HOME*¥install_logs¥dbConfig.stdout ログ・ファイルにデータが書き込まれます。元のファイルを保存する場合は、コマンドを実行する前にこのファイルをバックアップしてください。データベース構成が完了するまで数分かかります。

注: データベース変更が更新されていることを確認するために、**DBConfig** の実行後に **runConfig** コマンドを実行する必要があります。

データベース構成ツール **DBConfig** を手動で開始するには、以下を実行します。

手順

1. *ISIM_HOME*¥install_logs¥dbConfig.stdout をバックアップします。
2. 以下のいずれかのコマンドを実行します。
   - Windows オペレーティング・システム:

     ISIM_HOME¥bin¥DBConfig.exe
   - UNIX または Linux オペレーティング・システム:

     ISIM_HOME/bin/DBConfig

   データベースのプロパティー・ファイルを構成して、IBM Security Identity Manager データベースにテーブルをセットアップするための、データベース構成ウィンドウが開きます。ウィンドウのフィールドは、使用するデータベースに応じて異なることがあります。
3. 「データベース情報」フィールドに入力します。 データは、 データベースを構成して接続するために必要です。
   - ホスト名

     データベース・ホストの名前を指定します。
   - ポート番号

     データベース・インスタンスのポート番号を指定します。
   - データベース名

     DB2 または Microsoft SQL データベースの場合:
     データベース名を指定します。

     Oracle データベースの場合:
     a. 「**SID**」または「**サービス名**」をクリックします。
     b. 選択に基づいて、Oracle システム ID (SID) またはサービス名を指定します。
   - 管理者 ID

データベース・ホストの管理者 ID を指定します。管理者 ID に、テーブル・スペースを作成し、データベースを停止および開始する権利があることを確認してください。

- 管理者パスワード

  管理者 ID のパスワードを指定します。

4. 「**テスト**」をクリックして、データベースへの接続がアクティブになっていることを確認します。 データベース接続テストが成功すると、「ユーザー・パスワード」フィールドがアクティブになり、「**テスト**」ボタンが「**続行**」に変わります。「ユーザー ID」フィールドにはデフォルト値 `itimuser` が表示されますが、このユーザー ID は変更可能です。DB2 データベースの場合は、次のステップに進む前に、ユーザー ID `itimuser` が存在していることを確認します。
5. `itimuser` という名前の既存データベース・ユーザー ID の正しいパスワードを入力し、「**続行**」をクリックします。 データベース構成が完了するまで数分かかります。
6. インストール中に初期 DBConfig がキャンセルされた場合またはエラーで終了した場合は、以下のいずれかのコマンドを実行して変更を更新する必要があります。
   - Windows オペレーティング・システム:

     ISIM_HOME¥bin¥runConfig.exe install
   - UNIX または Linux オペレーティング・システム:

     ISIM_HOME/bin/runConfig install
7. デプロイメントに共有アクセス・モジュールが含まれている場合は、ここで共有アクセス・モジュールを再構成する必要があります。

129 ページの『第 8 章 共有アクセス・モジュールの構成』に進みます。

次のタスク

手動による追加構成タスクを実行します。

ディレクトリー・サーバーの構成

IBM Security Identity Manager インストール・プログラムは、`ldapConfig` データベース構成ツールを自動的に使用して、IBM Security Identity Manager と共に機能するようにディレクトリー・サーバーをセットアップします。この構成は、シングル・サーバー・インストール時、またはデプロイメント・マネージャー上でのクラスター・インストール時に実行されます。

ディレクトリー・サーバーの初期インストールおよび構成について詳しくは、 43 ページの『ディレクトリー・サーバーのインストールおよび構成』を参照してください。

手動による ldapConfig 構成ツールの実行

既存のディレクトリー・サーバーのデータが失われることがないようにするために、インストール中にディレクトリー・サーバーの構成に問題が発生しない限り、このツールを手動で実行しないでください。

始める前に

ディレクトリー・サーバー構成ツールを実行すると *ISIM_HOME*¥install_logs¥ldapConfig.stdout ログ・ファイルにデータが書き込まれます。元のファイルを保存する場合は、コマンドを実行する前にこのファイルをバックアップしてください。

このタスクについて

ldapConfig コマンドを実行すると、IBM Security Identity Manager が使用するデフォルト値が復元されます。itim manager というユーザー ID のパスワードなど、これら IBM Security Identity Manager 属性のいずれかの値を変更した場合には、値は上書きされます。LDAP 構成が IBM Security Identity Manager サーバーのインストール処理中に失敗した場合を除き、**ldapConfig** コマンドは、2 回実行しないでください。

データベース構成が完了するまで数分かかります。

手順

1. *ISIM_HOME*¥install_logs¥ldapConfig.stdout をバックアップします。
2. 以下のいずれかのコマンドを実行します。
   - Windows オペレーティング・システム -

     ISIM_HOME¥bin¥ldapConfig.exe
   - UNIX または Linux オペレーティング・システム -

     ISIM_HOME/bin/ldapConfig
3. 「LDAP サーバー情報」のフィールド (「基本 DN」、「パスワード」、「ホスト名」、「ポート」) に値を入力して、ディレクトリー・サーバーへの接続をセットアップします。 例えば、「**ホスト名**」フィールドの値は、ディレクトリー・サーバーが稼働しているコンピューターの完全修飾ホスト名です。
4. 「**テスト**」をクリックして、ディレクトリー・サーバーへの接続を確立できることを確認します。 ディレクトリー・サーバーへの接続テストに成功すると、「IBM Security Identity Manager ディレクトリー情報」セクションがアクティブになります。
5. 「IBM Security Identity Manager ディレクトリー情報」のフィールドに値を入力します。 以下のフィールドを構成できます。

   ハッシュ・バケット数
   ハッシュ・バケット数を指定します。

   組織名を指定します。
   組織名を指定します。例えば、「**ユーザー組織**」です。

   デフォルトの組織短縮名
   組織の短縮名を指定します。例えば、myorg です。

   Identity Manager DN ロケーション
   IBM Security Identity Manager サフィックスを指定します。例: dc=com
6. 完了したら、「**続行**」をクリックします。
7. デプロイメントに共有アクセス・モジュールが含まれている場合は、ここで共有アクセス・モジュールを再構成する必要があります。

129 ページの『第 8 章 共有アクセス・モジュールの構成』に進みます。

次のタスク

手動による追加構成タスクを実行します。

IBM Security Identity Manager アプリケーションのマッピング

HTTP サーバーを使用する場合は、管理コンソールを使用して IBM Security Identity Manager アプリケーションを IBM HTTP Web サーバーにマップします。

始める前に

WebSphere Application Server がインストールされていること、および管理コンソールが実行中であることを確認してください。管理特権を持っている必要があります。

手順

1. IBM Security Identity Manager クラスターの WebSphere Application Server Network Deployment Manager で、管理コンソールにログオンします。WebSphere Application Server の管理者資格情報を使用してログインします。
2. タスク・メニューで、「**アプリケーション**」 > 「**アプリケーション・タイプ**」 > 「**WebSphere エンタープライズ・アプリケーション**」をクリックします。
3. エンタープライズ・アプリケーション・リストの 「**ITIM**」をクリックします。
4. 「**モジュールの管理**」をクリックします。
5. ITIM アプリケーション・クラスター名 (JMS クラスター名ではありません) を選択し、以下のモジュールのチェック・ボックスを選択します。
   - PasswordSynch
   - ITIM_Console
   - EnRole
   - ITIM_Self_Service
   - ITIM_Self_Service_Help
   - ITIM_Console_Help
   - ITIM_Message_Help
   - EHS3.01
   - PasswordReset
   - ITIM Web サービス (ITIM Web Services)
   - クレデンシャル・ボールト (Credential Vault)
6. 「**適用**」をクリックします (「クラスターおよびサーバー」フィールドの横にあります)。
7. 「**OK**」をクリックします。
8. メッセージ・ボックスの「**構成の保存**」をクリックします。

一般に使用されるシステム・プロパティーの構成

IBM Security Identity Manager サーバーを構成するには、システム・プロパティーを管理します。例えば、システム・プロパティーは、ユーザー確認のための質問が正しく完了したときに、サーバーがどのように応答するかを決定します。システム・プロパティーはいつでも変更可能です。

サーバーのスタートアップ・モジュールなど、いくつかのシステム・プロパティーに変更を加えた場合、IBM Security Identity Manager サーバーを再始動する必要が生じることがあります。これらのプロパティーは、サーバーを再始動しない限り認識されません。システム構成ツールでプロパティーを変更した後は、IBM Security Identity Manager サーバーを再始動してください。他のシステム・プロパティーに加えられた変更は、30 秒以内に認識できます。ロギング・プロパティーはサーバーを再始動しなくても変更でき、変更は 5 分以内に有効になります。

システム・プロパティーを変更するには、次の方法を使用します。

手動による runConfig システム構成ツールの実行

IBM Security Identity Manager インストール・プログラムは、自動的に runConfig システム構成ツールを実行します。ただし、runConfig ユーティリティーを使用して、インストール時に設定したプロパティーを変更することもできます。インストール時に発生したシステム構成エラーを訂正することもできます。

始める前に

システム構成ツールを実行すると、*ISIM_HOME*¥ install_logs¥runConfig.stdout ログ・ファイルにログ・データが書き込まれます。元のファイルを保存する場合は、コマンドを実行する前にこのファイルをバックアップしてください。

このタスクについて

IBM Security Identity Manager サーバー用のよく使用されるシステム・プロパティーを編集することに加えて、IBM Security Identity Manager アプリケーション用に WebSphere Application Server 設定を構成することもできます。

システム構成ツールは、シングル・サーバー構成とクラスター構成の両方に使用できます。クラスター構成には、デプロイメント・マネージャーとクラスター・メンバーが含まれます。

よく使用される IBM Security Identity Manager プロパティーを更新するには、以下のようにします。

手順

1. 以下のいずれかのコマンドを実行します。
   - Windows オペレーティング・システム:

     ISIM_HOME¥bin¥runConfig.exe
   - UNIX または Linux オペレーティング・システム:

     ISIM_HOME/bin/runConfig

注: runConfig ユーティリティーは、**install** パラメーターも受け入れます。IBM Security Identity Manager のインストール中に runConfig での問題が報告された場合は、**install** パラメーターを持つ runConfig を使用します。

- Windows オペレーティング・システム:

  ISIM_HOME¥bin¥runConfig.exe install

- UNIX または Linux オペレーティング・システム:

  ISIM_HOME/bin/runConfig install

install オプションを使用すると、システム構成が完了するまで数分かかります。

2. 「**メール**」タブをクリックします。

   システム構成ツールの「**メール**」タブには、メール通知およびゲートウェイ・パラメーターが表示されます。

   - **IBM Security Identity Manager のベース URL** フィールドで、IBM Security Identity Manager サーバーのログイン Universal Resource Locator (URL) を指定します。このアドレスは、実行時にメール・メッセージの受信側に送信される URL の最初の部分です。この URL は、IBM Security Identity Manager 管理コンソールのログイン・ページも指します。

     この値は、プロキシー・サーバー (例えば、IBM HTTP Server) の URL です。ホスト名 (または IP アドレス) およびポートをベース URL に指定します。この値が、IBM Security Identity Manager システムにパブリッシュされているログイン URL に一致していることを確認してください。

     – 単一サーバー構成

       ベース URL は、デフォルトでポート 80 を使用する Web サーバー (例えば、IBM HTTP Server) のアドレスです。

     – クラスター構成

       ベース URL は、特定のアプリケーション・サーバー・インスタンスではなく、クラスター内のすべてのアプリケーション・サーバー・インスタンスとロード・バランスを取る Web サーバーのアドレスです。

     IPv6 の場合、リテラル・アドレスは大括弧で囲む必要があります。次に例を示します。

     ```
     jdbc:db2://[abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd]:50002/itimdb
     ```

     ここで、abcd は 0000 から FFFF までの 16 進数です。

   - 「**メール発信元**」フィールドで、サイトの IBM Security Identity Manager システム管理者の電子メール・アドレスへのアドレスを指定します。すべての電子メールは、「**メール発信元**」パラメーターから配布されます。このアドレスを変更しないと、リストされた電子メール・アドレスにスパム・メールを送信することになります。
   - 「**メール・サーバー名**」フィールドで、電子メール通知を送信する SMTP メール・ホストを指定します。SMTP メール・サーバーがサポートされています。SMTP ホストはメール・ゲートウェイです。例えば、swiftcreek.mycity.ibm.com などのホスト名を入力します。

3. 「**一般**」タブをクリックします。 システム構成ツールの「**一般**」タブで、IBM Security Identity Manager Server に関する一般情報を構成します。

   「**一般**」タブの以下のフィールド値は、インストール・プログラムによって事前に入力されています。

   - **ハートビート** (秒数)

     「**スケジューリング情報**」フィールドには、スケジューリング・スレッドが、処理するイベント (ハートビート) について予定メッセージ・ストアに照会する頻度に関する情報が表示されます。さらに頻繁にハートビートを処理できるようにする前に、パフォーマンスの問題を考慮してください。ハートビート (秒で測定されます) を変更できるのは、システム管理者だけです。

   - **リサイクル・ビン経過日数限界** (日数)

     IBM Security Identity Manager オブジェクト (組織単位、個人、アカウントなど) を削除しても、そのオブジェクトは即時にシステムから除去されるわけではありません。削除されたオブジェクトは、リサイクル・ビン・コンテナーに移されます。リサイクル・ビンを空にするプロセスは、クリーンアップ・スクリプトの実行を含む、独立した削除プロセスです。

     リサイクル・ビンはデフォルトで使用不可ですが、*ISIM_HOME*¥data ディレクトリーの enRole.properties ファイルを編集することにより使用可能にできます。

     例えば、古いユーザーID を新規ユーザーに割り当てないようにするには、割り当てプロセスでリサイクル・ビンをチェックして、古いユーザー ID が存在しているかどうかを判別します。リサイクル・ビンの間隔の値は、古いユーザー ID の保持時間を決定する間隔に設定することもできます。

     「リサイクル・ビン経過日数限界」フィールドは、オブジェクトを削除できるようになるまで、リサイクル・ビンに保持しておく日数を指定します。このクリーンアップ・スクリプトが除去できるのは、経過日数限界の設定値よりも古いオブジェクトだけです。例えば、経過日数限界の設定値が 62 日 (デフォルト値) の場合、62 日を超えたオブジェクトのみを削除できます。

     以下のスクリプトを使用すると、経過日数限界を過ぎたリサイクル・ビン項目を手動で除去することも、定期的にクリーンアップするようスケジュールすることもできます。

     – Windows オペレーティング・システム:

       ISIM_HOME¥bin¥win¥ldapClean.cmd

     – UNIX または Linux オペレーティング・システム:

       ISIM_HOME/bin/unix/ldapClean.sh

       定期的なクリーンアップをスケジュールするには、以下の例のような UNIX cron ジョブを作成します。

       ISIM_HOME/bin/unix/schedule_garbage.cron

4. 「**データベース**」タブをクリックします。 「**データベース**」タブには、一般的なデータベース情報およびデータベース・プール情報が表示されます。このタブには、データベースとの接続をテストするための「**テスト**」ボタンもあります。

このタブのいずれかのフィールドを更新する場合は、「**テスト**」をクリックして、接続が動作していることを確認します。システムのセットアップ後にこの構成を変更すると、有害な結果が生じることがあります。

使用されている接続のタイプに応じて、データベース・プロパティーの構成時に、いくつかあるウィンドウの内の 1 つが表示されます。IBM Security Identity Manager が Oracle データベースとの接続に Oracle クライアントを使用していない場合は、この例のウィンドウに「**データベース**」タブが表示されます。

このインストールをクラスター・メンバーに行う場合、これらの情報は前もってデプロイメント・マネージャー用に作成されたデータベース指定と一致させる必要があります。

- 「**JDBC URL**」フィールドで、タイプ 4 JDBC ドライバーの URL 形式で URL 値を指定します。

  IPv6 の場合、リテラル・アドレスは大括弧で囲む必要があります。次に例を示します。

  ```
  jdbc:db2://[abcd:abcd:abcd:abcd:abcd:abcd:abcd:abcd]:50002/itimdb
  ```

  ここで、*abcd* は `0000` から `FFFF` までの 16 進数です。
- 「**データベース・ユーザー**」フィールドおよび「**ユーザー・パスワード**」フィールドで、IBM Security Identity Manager がデータベースへのログオンに使用するデータベース・アカウントおよびパスワードを指定します。デフォルトのユーザー ID は `itimuser` です。これは、IBM Security Identity Manager データベース構成プログラム (DBConfig) によって作成されます。アカウントは、有効なユーザー・パスワードを所有している必要があります。
- データベース・プール情報は、JDBC 接続の数を決定します。サポートされている JDBC ドライバーについて詳しくは、3 ページの『データベース・サーバー製品』を参照してください。
  - 「**初期容量**」フィールドで、JDBC 接続の数の初期値を指定します。
  - 「**最大容量**」フィールドで、IBM Security Identity Manager サーバーが一度にデータベースに対して開いておくことのできる JDBC 接続の最大数を指定します。

5. 「**ディレクトリー**」タブをクリックします。 システム構成ツールの「**ディレクトリー**」タブには、ディレクトリー接続情報および LDAP 接続プール情報が表示されます。このタブには、ディレクトリー・サーバーとの接続をテストするための「**テスト**」ボタンもあります。このタブのいずれかのフィールドを更新する場合は、「**テスト**」をクリックして、接続が動作していることを確認します。

   この情報は、デプロイメント・マネージャーの場合は事前に入力されていますが、WebSphere アプリケーション・サーバーの場合は事前に入力されていません。必要であれば、ディレクトリー・サーバーに関する以下の情報を変更してください。

   - ディレクトリー・サーバーにログオンするために IBM Security Identity Manager サーバーが使用するプリンシパル DN およびパスワード。
   - ディレクトリー・サーバーのホスト名または IP アドレス。

IPv6 の場合、リテラル・アドレスは大括弧で囲む必要があります。次に例を示します。

[*abcd*:*abcd*:*abcd*:*abcd*:*abcd*:*abcd*:*abcd*:*abcd*]

ここで、*abcd* は 0000 から FFFF までの 16 進数です。

- ディレクトリー・サーバーのポート番号。
- LDAP 接続プール情報は、IBM Security Identity Manager サーバーがアクセス可能な LDAP 接続のプールを定義します。接続が確立し、データが LDAP ディレクトリー・サーバーに保管されている場合に、ホスト名またはポート番号を変更すると、有害な影響をもたらすことがあります。
  - 「**最大プール・サイズ**」フィールドで、LDAP 接続プールが任意の時点で持つことができる接続の最大数を指定します。
  - 「**初期プール・サイズ**」フィールドで、LDAP 接続プール用に作成される接続の数の初期値を指定します。
  - 「**増分カウント**」フィールドで、LDAP 接続プールに追加する接続の数を指定します。この増分は、すべての接続が使用中になった後で接続が要求されるたびに行われます。

6. 「**ロギング**」タブをクリックします。 システム構成ツールの「**ロギング**」タブを使用して、トレースのレベルを設定できます。以下の値の内のいずれか 1 つを選択してください。

   MIN わずかな情報をログ・ファイルに書き込みます。最も優れたパフォーマンスを得るには、この設定を使用します。

   MID さらに多くの情報量をログ・ファイルに書き込みます。

   MAX 最大情報量をログ・ファイルに書き込みます。ロギング・アクティビティーの量が増加すると、パフォーマンスに影響が出る可能性があります。この設定は、ほぼ VERBOSE と等価です。

7. 「**UI**」タブをクリックします。

   システム構成ツールの「**UI**」タブには、IBM Security Identity Manager Server GUI をカスタマイズするための情報が表示されます。

   - 「**カスタマー・ロゴ**」フィールドで、以下を実行します。
     - ロゴ・グラフィックのファイル名を指定します。このファイルはデフォルトのディレクトリー内になければならないため、ファイルをその場所にコピーする必要があります。
     - ロゴ・イメージをクリックすることによって、活動化されるオプションの URL リンクを指定します。リンクには任意の URL を使用できます。システム管理者は、これら 2 つの変数を指定して、IBM Security Identity Manager システム全体で使用されている IBM ロゴを自社のロゴに置き換えることができます。デフォルトの IBM ロゴ・ファイルは `ibm_banner.gif` ファイルです。このファイルは、*WAS_PROFILE_HOME*¥installedApps¥*cellname*¥ITIM.ear¥itim_console.war¥html¥images ディレクトリーにあります。クラスター構成では、このデフォルトのロゴは、デプロイメント・マネージャー・ワークステーション上ではなく、ノード・メンバー・ワークステーション内にあります。

- 「**ページ・サイズのリスト**」フィールドで、ディレクトリー内の検索を必要とする項目のうち、ユーザー・インターフェース全体にわたってリストに表示する項目の数を指定します。項目の合計数が、設定されているページ・サイズのリストを超えている場合、リストは複数ページにわたって表示されます。例えば、この値は、IBM Security Identity Manager GUI の「**ユーザー組織**」 > 「**ユーザーの管理**」タブを表示すると開く、名前リストのサイズを制御します。

8. 「**セキュリティー**」タブをクリックします。 「**セキュリティー**」タブには、プロパティー・ファイルに保管されている、データベース、LDAP、およびアプリケーション・サーバーのユーザー ID とパスワードをそれぞれ管理するための情報が表示されます。このタブには、IBM Security Identity Manager 内の暗号化の設定値およびアプリケーション・サーバーのユーザー管理設定が表示されます。

   デフォルトでは、IBM Security Identity Manager プロパティー・ファイル内のパスワードは暗号化されています。

   - 「**暗号化**」ボックスで、データベースおよびディレクトリー・サーバーの接続用のパスワード、およびシステム認証用のシステム・ユーザーのパスワードを暗号化するためのチェック・ボックスにチェック・マークを付けます。暗号化フラグが true に設定されます。このボックスのチェック・マークを外すと、パスワードが暗号化解除され、フラグは false に設定されます。フラグは、`enRole.properties` ファイル内の以下のプロパティーで表されます。

     ```
     enrole.password.database.encrypted
     enrole.password.ldap.encrypted
     enrole.password.appServer.encrypted
     ```

   - 「**WebSphere 管理者**」フィールドおよび「**WebSphere 管理者パスワード**」フィールドに、WebSphere 管理者および WebSphere 管理者パスワードを指定します。WebSphere の管理セキュリティーおよびアプリケーション・セキュリティーが有効になっており、管理者のユーザー ID およびパスワードが入力されている場合、上記のフィールドは事前に入力されています。WebSphere の管理セキュリティーおよびアプリケーション・セキュリティーが有効になっていない場合、これらのフィールドは空です。

   - 「**Identity Manager システム・ユーザー**」フィールドおよび「**Identity Manager システム・ユーザー・パスワード**」フィールドで、システム・ユーザーおよびユーザー・パスワードを指定します。これらのフィールドには、最初は「WebSphere 管理者」フィールドおよび「パスワード」フィールドの値が入っています。

     インストール時に、WebSphere 管理者とは異なる、独自のシステム・ユーザーを定義している場合は、「**Identity Manager システム・ユーザー**」フィールドおよび「**Identity Manager システム・ユーザー・パスワード**」フィールドの変更が必要となることがあります。このシステム構成の「セキュリティー」ウィンドウでシステム・ユーザー ID またはユーザー・パスワードの値を変更し、スタンドアロン・コマンドとして `runConfig` を実行すると、追加の手動ステップが必要になります。このステップは、IBM Security Identity Manager のインストール後に、IBM Security Identity Manager を開始するように IBM Security Identity Manager ユーザーにセキュリティー役割をマップするために必要です。詳しくは、 157 ページの『管理ユーザーと役割の間のマッピング』を参照してください。

次のタスク

手動による追加構成タスクを実行します。

システム・プロパティーの手動による変更

もう 1 つの方法として、該当するプロパティー・ファイルを編集して、システム・プロパティーを手動で変更することもできます。

システムおよび補足プロパティー・ファイルは、IBM Security Identity Manager サーバーの *ISIM_HOME*¥data ディレクトリーにあります。これらのファイルには、サーバーが使用するすべてのシステムおよび補足プロパティーが含まれています。enRole.properties ファイルのシステム・プロパティーについて詳しくは、IBM Security Identity Manager インフォメーション・センターの『*enRole.properties* でのシステム・プロパティー構成』を参照してください。

IBM Security Identity Manager グラフィカル・ユーザー・インターフェースを使用したシステム・プロパティーの変更

いくつかのシステム・プロパティーは、IBM Security Identity Manager Server グラフィカル・ユーザー・インターフェース (GUI) 内のメインメニューのナビゲーション・バーの「構成」セクション内から変更することもできます。

「システム・セキュリティーの設定」 > 「セキュリティー・プロパティーの設定」から、以下のセキュリティー・プロパティーを変更できます。

- パスワード設定
- IBM Security Identity Manager ログイン・アカウント設定
- グループ設定

「システム・セキュリティーの設定」 > 「パスワードを忘れた場合の設定の構成」から、以下のプロパティーを変更できます。

- パスワードを忘れた場合の認証を使用可能にする
- ログイン動作
- ユーザー確認の質問の動作の設定

セキュリティーのプロパティー

「システム・セキュリティーの設定」 > 「セキュリティー・プロパティーの設定」から、以下のセキュリティー・プロパティーを変更できます。

パスワード設定:

以下のパスワード・プロパティーを変更するには、**「システム・セキュリティーの設定」 > 「セキュリティー・プロパティーの設定」**をクリックします。

パスワード編集を使用可能にする

ユーザーが自分自身のパスワードを変更するときに値を入力できるようにするには、このチェック・ボックスを選択します。さらに、ヘルプ・デスク・アシスタント、サービス所有者、および管理者は、自分自身のパスワードのほか、他のユーザーのパスワードを変更する場合も値を入力できます。チェ

ック・ボックスを選択するには、タブ・キーを使用してチェック・ボックスにフォーカスを合わせてからスペース・バーを押す方法もあります。

他のユーザーの生成済みパスワードを非表示にする
他のユーザーの生成済みパスワードを非表示にするには、このチェック・ボックスをクリックします。パスワードの編集が使用可能である場合は、このチェック・ボックスは選択できません。

パスワード同期を使用可能にする
ユーザーのすべてのアカウントにおける以降のパスワード変更を同期するには、このチェック・ボックスを選択します。このチェック・ボックスを選択すると、1 つのパスワード変更が、そのユーザーのすべてのアカウントで同期されます。このチェック・ボックスをクリアした場合、ユーザーは各アカウントを選択し、個々のパスワードを変更する必要があります。

ユーザーのパスワードはユーザーの作成時に設定
ユーザーを作成するときにユーザーのパスワードを設定するには、このチェック・ボックスを選択します。

パスワード検索有効期限 (時間数)
パスワードの期限が切れる前にユーザーがパスワードを検索する必要がある間隔を、時間単位で入力します。新規のアカウントが作成されると、ユーザーは、パスワードを提供する URL リンクを含む電子メールを受け取ります。ユーザーは、パスワード取り出し有効期限が切れる前にこのパスワードを取得する必要があります。

新しい値を有効にするには、ログアウトし、再度ログインする必要があります。

IBM Security Identity Manager ログイン・アカウント設定:

以下のログイン・プロパティーを変更するには、「**システム・セキュリティーの設定**」 > 「**セキュリティー・プロパティーの設定**」をクリックします。

識別アカウント・パスワード有効期限 (日数)
このプロパティーは、IBM Security Identity Manager サーバー・アカウントのためだけのものです。 IBM Security Identity Manager アカウントのパスワードの有効期限が切れるまでの間隔を日数で入力します。ユーザーは、この期間に達する前に、パスワードを変更する必要があります。新規のパスワードが IBM Security Identity Manager サーバー・アカウントに設定された場合は、常にその時点からパスワードの有効期限が影響を受けます。この値をゼロに設定することによって、パスワードの有効期限を無効にできます。デフォルト値は 0 で、アカウント・パスワードが無期限であることを表します。

最大無効ログイン試行回数
IBM Security Identity Manager アカウントがサスペンドされるまでに許容される、無効ログイン試行回数を入力します。デフォルト値は 0 で、制限がないことを表します。

新しい値を有効にするには、ログアウトし、再度ログインする必要があります。

グループ設定:

グループ・プロパティーを変更するには、「**システム・セキュリティーの設定**」 > 「**セキュリティー・プロパティーの設定**」をクリックします。

自動的に IBM Security Identity Manager グループに取り込む

新規に指名したサービス所有者の IBM Security Identity Manager アカウントをデフォルトのサービス所有者グループに自動的に書き込む場合は、このチェック・ボックスを選択します。自動操作の使用可能/使用不可の切り替えは、即座に行われます。 IBM Security Identity Manager を再始動する必要はありません。例えば、グループのメンバーシップは、サービスを作成または変更して、サービス所有者を指定すると有効になります。

さらに、新規に指名した管理者の IBM Security Identity Manager アカウントは、デフォルトの管理者グループに自動的に書き込まれます。例えば、この動作が実行されるのは、従属ユーザーを作成または変更して、そのユーザーの管理者を指定した場合です。

サービス所有者が役割となっている場合、自動グループ・メンバーシップはサポートされません。

新しい値を有効にするには、ログアウトし、再度ログインする必要があります。

パスワードを忘れた場合の設定

「**システム・セキュリティーの設定**」 > 「**パスワードを忘れた場合の設定の構成**」から、以下のプロパティーを変更できます。

パスワードを忘れた場合の認証:

「**システム・セキュリティーの設定**」 > 「**パスワードを忘れた場合の設定の構成**」をクリックし、パスワードを忘れた場合の認証を変更します。

パスワードを忘れた場合の認証をアクティブにするには、このチェック・ボックスを選択します。この認証をアクティブにすると、ユーザーがパスワードを忘れた場合、ログイン・ページで「**パスワードを忘れましたか?**」というプロンプトが開きます。質問に正しく回答したユーザーは、新規の自動生成パスワードを受け取ります。このチェック・ボックスをクリアすると、ログイン・ページにプロンプトが表示されません。ユーザーはヘルプ・デスク・アシスタントまたはシステム管理者に連絡して、パスワードを再設定してもらう必要があります。

新しい値を有効にするには、ログアウトし、再度ログインする必要があります。

ログイン動作:

ログイン・プロパティーを変更するには、「**システム・セキュリティーの設定**」 > 「**パスワードを忘れた場合の設定の構成**」をクリックします。

ユーザーが質問に正しく回答した場合
ログイン動作を選択します。

パスワードを変更してシステムにログインする
ユーザーをシステムにログインさせるときに、パスワード変更を要求します。

パスワードを再設定し、電子メールで送信
パスワードを再設定し、ユーザーの電子メール・アドレスに新規パスワードを送信します。

正しく回答しなかった場合にアカウントをサスペンドするメッセージ
正しい回答を入力できなかった場合にユーザーが受け取るメッセージを入力します。

電子メール・アドレスにメッセージを送信
メッセージを受け取る電子メール・アドレスを入力します。

新しい値を有効にするには、ログアウトし、再度ログインする必要があります。

ユーザー確認の質問の動作:

「システム・セキュリティーの設定」 > 「パスワードを忘れた場合の設定の構成」をクリックし、ユーザー確認のための質問のプロパティーを変更します。

ユーザー確認のための質問を、ユーザーと管理者のどちらが定義するかを選択します。

ユーザーが独自の質問を定義する

ユーザーが質問を定義する場合は、このオプションを選択します。

ユーザーがセットアップする質問の数
ユーザーが設定する必要のある質問の数を入力します。

ユーザーが入力する必要のある正しい回答の数
システムにアクセスするためにユーザーが正しく答える必要がある回答の数を入力します。

管理者が事前定義の質問を提供する

ユーザーが回答する必要がある質問のセット、および使用する質問の言語を定義する場合は、このオプションを選択します。このオプションを選択した場合は、「パスワードを忘れた場合の質問の指定」セクションが開きます。

パスワードを忘れた場合の質問の指定
ユーザーに回答させる質問を指定するには、このセクションをクリックして展開します。

新規のユーザー確認用の質問
ユーザーに回答させる質問を入力し、「**追加**」をクリックします。

ロケール
使用する質問の言語を選択し、「**追加**」をクリックします。

ユーザー確認のための質問のテーブル
ユーザー確認のための質問のテーブルには、ユーザーに回答させる質問を選択元になる、追加済みの質問のリストが含まれます。テーブルを特定の列でソートするには、その列見出しにある矢印をクリックします。 テーブルには以下の列が含まれています。

選択 既存の質問を選択するには、このチェック・ボックスを選択します。

ロケール
質問で使用される言語を表示します。

質問　質問テキストが表示されます。

「**除去**」をクリックして、選択した質問を除去します。

テーブルに複数のページが含まれている場合、以下の処理を行うことができます。

- 矢印をクリックして次のページに進む。
- 表示するページの番号を入力してから「**実行**」をクリックする。

事前定義の質問をユーザーが選択できるか?

いいえ、すべての質問に答えます
ユーザーが正しく答える必要のある、事前定義された質問をすべて表示します。

はい、回答する質問をユーザーが選択します
ユーザーが選択し、パスワードを忘れたときに正しく答える必要がある質問の数を表示します。ユーザーが選択する質問の数を入力します。

いいえ、システムが提供する質問の一部に答えます
パスワードを忘れたときにユーザーが正しく答える必要のある、事前定義された質問のランダムなサブセットを表示します。

ユーザーがセットアップする質問の数
ユーザーが構成する質問の数を入力します。

ユーザーが入力する必要のある正しい回答の数
ユーザーが正しく答える必要がある質問の数を入力します。このフィールドは、システムが提供する質問のサブセットにユーザーが答える必要がある場合に使用可能になります。

新しい値を有効にするには、ログアウトし、再度ログインする必要があります。

セキュリティー構成

このセクションでは、IBM Security Identity Manager およびミドルウェア・コンポーネントのセキュリティーの構成方法を説明します。

セキュリティーについて詳しくは、IBM Security Identity Manager インフォメーション・センターの『セキュリティー』を参照してください。

ディレクトリー・サーバーのセキュリティー構成

通信を保護するために、LDAP サーバーと IBM Security Identity Manager との間で Secure Sockets Layer (SSL) 通信が使用されます。通信を保護するには、SSL を使用するように LDAP サーバーを構成する必要があります。

IBM Tivoli Directory Server または Oracle Directory Server Enterprise Edition を使用して IBM Security Identity Manager 情報を保管している場合は、SSL を使用するようにサーバーを設定する必要があります。次に、使用する SSL 証明書を構成する必要があります。

このタスクは、IBM Security Identity Manager をインストールした後にのみ実行できます。SSL 接続のみを使用して LDAP を構成する場合は、インストール中の LDAP 構成をスキップし、インストール完了後に **ldapConfig** を実行します。

IBM Tivoli Directory Server に対する SSL の構成

IBM Tivoli Directory Server と IBM Security Identity Manager との間で Secure Sockets Layer (SSL) 通信を行うには、定義済みの証明書を持つポートを listen するように IBM Tivoli Directory Server を構成する必要があります。認証局 (CA) が SSL クライアントの署名者証明書データベースになければなりません。

GSKit を使用して、鍵データベース・ファイルおよび証明書を作成します。 クライアントが使用するサーバーの証明書 (LDAP サーバー用に作成された証明書) を必ず抽出してください。IBM Security Identity Manager が実行されているシステムに証明書をコピーする必要があります。サーバーの証明書の場所は、後のタスクで IBM Security Identity Manager の信頼される証明書をセットアップするために必要です。

IBM Tivoli Directory Server 用に LDAP で SSL をアクティブにする方法について詳しくは、IBM Tivoli Directory Server インフォメーション・センターで提供されている資料を参照してください。

Oracle Directory Server Enterprise Edition に対する SSL の構成

IBM Security Identity Manager は、Oracle Directory Server Enterprise Edition との SSL 通信をサポートしています。 Oracle Directory Server は、SSL が事前構成された状態で出荷されています。

Oracle Directory Server と通信するようにクライアントを構成する方法について詳しくは、Oracle 公式 Web サイトで提供されている資料を参照してください。

LDAP サーバー証明書を信頼するように SSL クライアントを構成する

IBM Security Identity Manager サーバーは、WebSphere Application Server に組み込まれた一部分としては機能しません。これは Java アプリケーションとして作動し、Java Secure Socket Extension (JSSE) を使用して、SSL サポートをインプリメントします。

SSL 証明書および CA 証明書は標準形式の Java トラストストアまたは鍵ストアから取り出されます。トラストストアおよび鍵ストアは、Java 仮想マシン (JVM) および WebSphere Application Server がその他の証明書構成に対して使用するものと同じファイル・フォーマットを使用します。IBM 鍵管理ツールや Java keytool コマンド行ユーティリティーなど、標準 Java ツールを使用してトラストストアおよび鍵ストアを管理できます。

IBM Security Identity Manager サーバーと LDAP サーバーとの間で SSL 接続を構成するには、LDAP サーバー用に作成された CA 証明書、または自己署名証明書をトラストストアにインポートする必要があります。このトラストストアは、WebSphere Application Server の一部である IBM JSSE によって使用されます。さらに、最初に、LDAP サーバーと通信するときに SSL を使用するように IBM Security Identity Manager を構成する必要があります。 `ldap` プロトコルではなく、`ldaps` プロトコルを使用するように IBM Security Identity Manager を構成します。

JSSE トラストストアへの自己署名証明書のインストール:

以下の手順を使用して、自己署名証明書をインストールし、それを証明書ストアに追加します。

始める前に

このタスクには、WebSphere Application Server の JRE に存在するデフォルトのトラストストアが使用されます。また、証明書を構成するために *ikeyman* ユーティリティーが使用されます。

手順

1. *ikeyman* ユーティリティーを開始します。 ユーティリティー (ikeyman.bat または ikeyman.sh) は、*WAS_HOME*¥bin にあります。
2. 「鍵データベース・ファイル」メニューから、「**開く**」を選択します。
3. 「鍵データベース・タイプ」で、「**JKS**」を選択します。
4. 「ファイル名」フィールドに、cacerts と入力します。
5. 「ロケーション」フィールドに、WAS_HOME¥java¥jre¥lib¥security¥ と入力します。
6. パスワード・プロンプト・ウィンドウで、「パスワード」および「パスワードの確認」ウィンドウに鍵ストアのパスワードを入力します。 デフォルトのパスワードは changeit です。
7. 「**OK**」をクリックします。
8. LDAP サーバー用に作成した証明書をこの証明書ストアに追加します。
   a. メイン・ウィンドウの、「鍵データベースの内容」領域で、リストから「**署名者証明書**」を選択します。
   b. 「**追加**」をクリックします。
   c. 「証明書ファイル名」フィールドで、LDAP サーバー用に作成されたサーバー証明書ファイル (「**バイナリー DER データ**」内のファイル) を参照して位置を指定します。「ロケーション」フィールドに適切なディレクトリーが表示されていることを検証します。
   d. 「**OK**」をクリックします。
   e. プロンプトに、この証明書のラベルを入力します。 例えば、LDAPCA と入力します。
   f. 「**OK**」をクリックします。

   注: 前述のサーバー証明書ファイルが見つからない場合は、以下の手順に従って、サーバー証明書ストアから証明書を取り出します。

   - IBM Tivoli Directory Server の場合は、*ikeyman* ユーティリティーを使用して証明書を取り出します。
   - Oracle Directory Server の場合は、以下の手順に従ってサーバー証明書を取り出します。
     a. 証明書の別名を検索します。ODSEE-install/bin ディレクトリーから以下を実行します。

        ```
        ./dsadm list-certs <instance-home-dir-path>
        ```

b. 証明書を表示して、出力を Binary Der ファイルにリダイレクトします。証明書の別名は *defaultCert* であると仮定します。

```
./dsadm show-cert -F der -o cert.der <instance-home-dir-path> defaultCert
```

cert.der は、必要なサーバー証明書ファイルです。
証明書が LDAP サーバー用に追加されます。これで、*ikeyman* ユーティリティーを終了できます。

次のタスク

LDAP サーバーと通信するときに SSL を使用するように IBM Security Identity Manager を構成します。

LDAP サーバーと通信するときに SSL を使用するように IBM Security Identity Manager を構成する:

LDAP 自己署名証明書のインポート後に、SSL 接続を完了するように IBM Security Identity Manager Server を構成する必要があります。

始める前に

LDAP サーバーの自己署名証明書の JSSE トラストストアへのインストールを完了する必要があります。

手順

1. enRoleLDAPConnection.properties ファイルを編集します。 このファイルは *ISIM_HOME*¥data ディレクトリーにあります。
   a. java.naming.provider.url プロパティーのポート値を、ディレクトリー・サーバー [LDAP] に対して構成されている SSL ポート番号に設定します。 例えば、次のように設定します。

      ```
      java.naming.provider.url=ldaps://localhost:636
      ```

   b. java.naming.security.protocol プロパティーの値を ssl に設定します。この設定は、IBM Security Identity Manager Server に SSL を使用して LDAP と通信するように指示します。 または、java.naming.provider.url のプロトコルを ldap から ldaps に変更します。例えば、次のように設定します。

      ```
      java.naming.security.protocol=ssl
      ```

2. 変更を保存します。

次のタスク

その他のセキュリティー関連タスクを実行します。

JVM でのトラストストアおよびパスワードのカスタム・プロパティーとしての定義:

IBM Security Identity Manager サーバーでは、WebSphere 管理コンソールの「**セキュリティー | SSL**」タブの WebSphere Application Server SSL 構成リポジトリーの設定値を使用しません。代わりに、SSL 設定値を構成し、javax プロパティーを指定する必要があります。

始める前に

WebSphere Application Server が稼働中であり、WebSphere 管理コンソールが開始されていることを確認します。また、WebSphere Application Server 管理ユーザー ID とパスワードが必要です。

手順

1. **「サーバー」** > **「アプリケーション・サーバー」** > 「*server_name*」 > **「プロセス定義」** > **「Java 仮想マシン」** > **「カスタム・プロパティー」** > **「新規」** を選択します。
2. **ikeyman** 鍵管理ツールを使用して変更した javax プロパティーの名前を定義します。 152 ページの『JSSE トラストストアへの自己署名証明書のインストール』で、WebSphere Application Server が使用する JVM のトラストストアに証明書をインストールしました。または、独自の証明書ストア・ロケーションを作成できます。それに対して、追加のプロパティーを定義する必要があります。

   以下の表に、定義する必要がある javax プロパティーに関する情報を示します。

表 14. トラストストア javax プロパティー

プロパティー名	説明	デフォルト値
javax.net.ssl.trustStore	トラストストア・ファイルのファイル・パス。クライアント証明書の指定に javax.net.ssl.keyStore を使用しない場合は、トラストストアを使用して CA 証明書およびクライアント証明書をインストールできます。	*jre_install_dir*¥lib¥security¥cacerts 例: C:¥Program Files¥WebSphere¥AppServer¥java¥jre¥lib¥security¥cacerts
javax.net.ssl.trustStorePassword	トラストストアを保護するパスワード。	changeit
javax.net.ssl.trustStoreType	鍵データベース・タイプ。このプロパティーは、トラストストアに必要です。この値は、自己署名証明書の作成時に指定されます。	jks

次のタスク

その他のセキュリティー関連タスクを実行します。

SSL を使用した ldapConfig の実行:

LDAP が SSL のみを使用するように構成されている場合、**ldapConfig** ユーティリティーは新規 IBM Security Identity Manager のインストール中動作しません。インストール・プロセス中は **ldapConfig** をスキップします。

始める前に

IBM Security Identity Manager のインストール・プロセスが完了していることを確認してください。

このタスクについて

以下の手順を完了した後で **ldapConfig** を実行します。

手順

1. enRoleLDAPConnections.properties の java.naming.security.protocol が **ssl** に設定されていることを検証します。
2. *ISIM_HOME*¥bin¥ldapConfig.lax ファイルを編集します。

   注: CA 証明書は、LDAP サーバー証明書を発行した当局の認証性の検証に必要です。**ldapConfig** によって使用される JVM のトラストストアに CA 証明書がインストールされている場合は、このステップをスキップします。

   以下のプロパティーを 1 行で追加します。

   ```
   lax.nl.java.option.additional=-Djavax.net.ssl.
   trustStoreType=jks
   -Djavax.net.ssl.trustStore=/opt/IBM/WebSphere/AppServer/java/
   jre/lib/security/cacerts -Djavax.net.ssl.trustStorePassword
   =changeit -Djava.ext.dirs=/opt/IBM/WebSphere/AppServer/java/
   jre/lib/ext:/opt/IBM/WebSphere/AppServer/plugins:/opt/IBM/
   WebSphere/AppServer/lib:/opt/IBM/WebSphere/AppServer/lib/ext
   ```

次のタスク

ldapConfig ユーティリティーを実行します。

その他のセキュリティー関連タスクを実行します。

ldapUpgrade の実行:

LDAP が IBM Security Identity Manager との通信に SSL のみを使用するように構成されている場合は、以下の手順に従って、フィックスパックのインストール時に ldapUpgrade ユーティリティーを実行してください。

始める前に

IBM Security Identity Manager がインストールされていて、フィックスパックがダウンロードされている必要があります。

手順

1. ldapUpgrade ユーティリティーを実行する前に、enRoleLDAPConnections.properties の java.naming.security.protocol が **ssl** に設定されていることを検証します。
2. *ISIM_HOME*¥bin¥ldapUpgrade.lax ファイルを編集します。

   以下のプロパティーを 1 行で追加します。

   ```
   lax.nl.java.option.additional=-Djavax.net.ssl.
   trustStoreType=jks
   -Djavax.net.ssl.trustStore=/opt/IBM/WebSphere/AppServer/java/
   jre/lib/security/cacerts -Djavax.net.ssl.trustStorePassword
   =changeit -Djava.ext.dirs=/opt/IBM/WebSphere/AppServer/java/
   jre/lib/ext:/opt/IBM/WebSphere/AppServer/plugins:/opt/IBM/
   WebSphere/AppServer/lib:/opt/IBM/WebSphere/AppServer/lib/ext
   ```

   例えば Windows オペレーティング・システムの場合:

   ```
   lax.nl.java.option.additional=-Djavax.net.ssl.trustStoreType=jks
   -Djavax.net.ssl.trustStore=
   C:¥Progra~1¥IBM¥WebSphere¥AppServer¥java¥jre¥lib¥security¥cacerts
   -Djavax.net.ssl.trustStorePassword=changeit
   ```

```
-Djava.ext.dirs= C:¥Progra~1¥IBM¥WebSphere¥AppServer¥java¥jre¥lib¥ext;
C:¥Progra~1¥IBM¥WebSphere¥AppServer¥plugins;
C:¥Progra~1¥IBM¥WebSphere¥AppServer¥lib;
C:¥Progra~1¥IBM¥WebSphere¥AppServer¥lib¥ext
```

注: UNIX システムでは、java.ext.dirs にあるディレクトリーのリストの区切り文字はコロンにする必要があります。Windows システムでは、これらのディレクトリーの区切り文字はセミコロンにする必要があります。また、Windows システムではリストにスペースを使用できないため、ディレクトリー名に 8.3 形式の表記を使用します。

3. このプロパティーが正しく設定されているかどうかをテストします。
   a. プロパティーを *ISIM_HOME*¥bin¥ldapConfig.lax ファイルにコピーします。
   b. ldapConfig 画面で「**テスト**」をクリックします。 テスト成功のメッセージが戻ってきた場合は、プロパティーは正しく設定されています。

      注: ldapConfig 画面で「**続行**」をクリックしないでください。「**キャンセル**」 をクリックして終了します。

次のタスク

ldapUpgrade ユーティリティーを実行します。

その他のセキュリティー関連タスクを実行します。

SSL を使用した LDAP サーバーにアクセスするユーティリティーの実行:

SSL を使用して LDAP サーバーにアクセスするユーティリティーに、Java ランタイム・プロパティーを追加する必要があります。

始める前に

IBM Security Identity Manager のインストールが完了していることを確認してください。

このタスクについて

ISIM_HOME¥bin¥platform ディレクトリーに存在している以下のユーティリティーを正常に実行するには:

- addindex
- addintegrity
- config_remote_services
- createLinks
- ldapClean
- remove_service_profiles
- loadDSMLSchema
- serviceability

SSL の構成時に以下の手順を実行する必要があります。

手順

1. enRoleLDAPConnections.properties の java.naming.security.protocol が **ssl** に設定されていることを検証します。
2. テキスト・エディターでユーティリティー・ファイル (例えば、addindex.sh や addindex.cmd など) を開きます。
3. 以下のプロパティーを Java ランタイム・プロパティーとして追加します。 プロパティーは 1 行に入力します。

   ```
   -Djavax.net.ssl.trustStoreType=type_of_truststore
   -Djavax.net.ssl.trustStore=truststore_location -Djavax.net.ssl.
   trustStorePassword=truststore_password -Djava.ext.dirs=WAS_HOME
   ¥java¥jre¥lib¥ext:WAS_HOME¥plugins:WAS_HOME¥lib:WAS_HOME¥lib¥ext
   ```

   例えば、SSL 用に変更された ldapClean.sh は、以下の例のようになります。

   ```
   $JAVA -Djavax.net.ssl.trustStoreType=jks -Djavax.net.ssl.trustStore=
   /opt/ibm/cacerts -Djavax.net.ssl.trustStorePassword=changeit -Djava.ext.
   dirs=/opt/IBM/WebSphere70/AppServer/java/jre/lib/ext:
   /opt/IBM/WebSphere70/AppServer/plugins:/opt/IBM/WebSphere61/
   AppServer/lib:/opt/IBM/WebSphere70/AppServer/lib/ext -cp $CLASSPATH
   com.ibm.itim.systemConfig.LdapSweeper
   ```

4. 変更をユーティリティー・ファイルに保存します。

次のタスク

ユーティリティーを使用します。

その他のセキュリティー関連タスクを実行します。

WebSphere Application Server のセキュリティー構成

WebSphere Application Server で管理セキュリティーとアプリケーション・セキュリティーをアクティブにすることを選択した場合は、追加のセキュリティー構成が必要になる場合があります。

これらの各セキュリティー・タスクは、単一ノード・デプロイメントとマルチノード・デプロイメントの両方に適用されます。以下の追加セキュリティー・タスクを実行することができます。

- itimadmin 管理ユーザーを ITIM_SYSTEM 役割にマップして、アクセスをさらに制限します。
- IBM Security Identity Manager の外部で WebSphere 管理者または IBM Security Identity Manager システム・ユーザーを変更した場合は、 **runConfig** コマンドを実行して IBM Security Identity Manager 構成を更新します。
- Java 2 セキュリティーもアクティブにした場合は、library.policy ファイルを変更し、was.policy ファイルが存在することを確認します。
- トークンの有効期限を変更し、クラスター構成で不測のタイムアウトが発生しないようにします。
- WebSphere Application Server の FIPS 準拠をアクティブにします。

管理ユーザーと役割の間のマッピング

管理ユーザーを IBM Security Identity Manager 役割にマップできます。通常は、インストール・プロセス中にインストーラーがマップします。ただし、IBM Security

Identity Manager をインストールした後で IBM Security Identity Manager システム・ユーザー ID を変更した場合は、このタスクが必要です。

始める前に

WebSphere Application Server が実行されており、WebSphere 管理コンソールが開始されていることを確認します。

手順

1. WebSphere 管理コンソールで、「**アプリケーション**」 > 「**エンタープライズ・アプリケーション**」をクリックします。
2. 「**ITIM**」をクリックします。
3. 「詳細プロパティー」で、スクロールダウンして、「**ユーザー/グループへのセキュリティー・ロールのマッピング**」をクリックします。
4. **ITIM_SYSTEM** のチェック・ボックスを選択します。
5. 「**ユーザー検索 (Lookup users)**」をクリックします。
6. 「**検索**」をクリックします。
7. リストから IBM Security Identity Manager システム・ユーザー (例えば、`wasadmin`) を選択します。
8. 「**OK**」をクリックします。
9. 無許可アクセスを防止するために、「**全員?**」または「**全認証者?**」チェック・ボックスをクリアします。
10. 構成変更を保存します。

次のタスク

その他のセキュリティー関連タスクに進みます。

WebSphere 管理者および IBM Security Identity Manager のシステム・ユーザーの更新

WebSphere 管理者または IBM Security Identity Manager のシステム・ユーザーのフィールドを変更した場合は、新規の値を使用して IBM Security Identity Manager の構成を更新する必要があります。

始める前に

IBM Security Identity Manager のインストール・プロセスが完了していることを確認してください。

手順

1. システム構成ツールを開始します。 以下のいずれかのコマンドを発行します。
   - Windows オペレーティング・システムの場合 -
     ISIM_HOME¥bin¥runConfig
   - UNIX または Linux オペレーティング・システムの場合 -
     ISIM_HOME/bin/runConfig.sh
2. 「**セキュリティー**」タブを選択します。

a. ローカルの OS レジストリーに作成した wasadmin ユーザー ID を使用して、「**WebSphere 管理者**」フィールドおよびそのパスワードを更新します。
b. ローカルのオペレーティング・システム・レジストリーに作成した itimadmin ユーザー ID を使用して、「**Identity Manager システム・ユーザー**」フィールドおよびそのパスワードを更新します。

3. 「**OK**」をクリックします。

次のタスク

その他のセキュリティー関連タスクを実行します。

ポリシー・ファイルの作成と変更による Java 2 セキュリティーのアクティブ化

Java 2 セキュリティーをオンにする場合は、library.policy ファイルを作成する必要があります。また、必要なリソースにアクセスする権限を追加するために、was.policy ファイルを変更する必要もあります。

始める前に

Java 2 セキュリティーをアクティブ化する予定の場合は、IBM Java 2 Platform Standard Edition Development Kit 1.5 Service Release 6 以降のバージョンを使用してください。このサービス・リリースは、ダウンロードできます。WebSphere Application Server フィックスパックの Web サイトの説明に従って、フィックスを適用します。

このタスクについて

IBM Security Identity Manager の Java 2 セキュリティーをアクティブにすると、WebSphere Application Server で稼働するすべてのアプリケーションに対して Java 2 セキュリティーが適用されます。IBM Security Identity Manager アプリケーションの Java 2 セキュリティーをアクティブにする場合は、WebSphere Application Server で実行するその他のすべてのアプリケーションを構成してください。

手順

1. 必要なリソースにアクセスする許可を追加するために、library.policy ファイルを作成します。
   a. 次のディレクトリー位置に library.policy ファイルを作成します。
      WAS_PROFILE_HOME/config/cell/*cellname*/nodes/*nodename*
   b. library.policy ファイルを編集します。次のステートメントを追加します。

      ```
      grant {
      permission java.security.AllPermission;
      }
      ```

      注: このサンプル・ポリシー・ファイルは、IBM Security Identity Manager 共有ライブラリーへのブランケット・アクセスを提供します。追加のセキュリティーは提供しません。このファイルを正しく構成することにより、セキュリティー要件に従ってポリシー・ファイルを設定します。
2. was.policy ファイルが存在していることを確認してください。 IBM Security Identity Manager インストール・プログラムは、自動的にサンプルの was.policy

ファイルを作成します。このファイルには、IBM Security Identity Manager アプリケーションが Java 2 セキュリティーを使用して実行する権限がすべて含まれています。このファイルが存在しない場合は、以下を実行する必要があります。

a. ノード上の以下のディレクトリー内に、ファイルを作成します。
WAS_PROFILE_HOME/config/cells/*cellname*/applications/ITIM.ear/deployments/*application_name*/META-INF

b. was.policy ファイルを編集します。次のステートメントを追加します。

```
grant codeBase "file::${application}" {
permission java.security.AllPermission;
};
```

注: このサンプル・ポリシー・ファイルは、IBM Security Identity Manager へのブランケット・アクセスを提供します。追加のセキュリティーは提供しません。このファイルを正しく構成することにより、セキュリティー要件に従ってポリシー・ファイルを設定します。

次のタスク

Java 2 セキュリティーを実行します。

単一ノード・デプロイメントでの Java 2 セキュリティーの実行:

Java 2 セキュリティーを実行するには、IBM Security Identity Manager を再始動する必要があります。

始める前に

Java 2 セキュリティーが使用可能になっていて、IBM Security Identity Manager が単一ノード・デプロイメントにインストールされていることを確認します。

WebSphere Application Server が実行されており、WebSphere 管理コンソールが開始されていることを確認します。

手順

1. WebSphere 管理コンソールにログオンします。
2. 「**アプリケーション**」 > 「**エンタープライズ・アプリケーション**」をクリックします。
3. 「**ITIM**」のチェック・ボックスを選択し、「**停止**」をクリックします。 IBM Security Identity Manager アプリケーションが停止するまで待機します。
4. 「**開始**」をクリックします。

次のタスク

その他のセキュリティー関連タスクを実行します。

マルチノード・デプロイメントでの Java 2 セキュリティーの実行:

Java 2 セキュリティー・コンポーネントを実行するには、セル内のノードを同期化する必要があります。

始める前に

Java 2 セキュリティーが使用可能で、IBM Security Identity Manager がマルチノード (クラスター化) デプロイメントにインストールされていることを確認します。

WebSphere Application Server が実行されており、WebSphere 管理コンソールが開始されていることを確認します。

手順

1. WebSphere 管理コンソールにログオンします。
2. 「**サーバー**」 > 「**クラスター**」をクリックします。
3. クラスター名の横にあるチェック・ボックスを選択し、「**停止**」をクリックします。 クラスターが停止するまで待機します。
4. 「**開始**」をクリックします。

次のタスク

その他のセキュリティー関連タスクを実行します。

タイムアウト間隔の増加

セキュリティーは、システムがある期間非アクティブになった後に期限切れとなる Lightweight Third Party Authentication (LTPA) トークンを使用します。クラスター構成で不測のタイムアウトが発生しないようにするために、トークンの有効期限値が十分な長さであることを確認する必要があります。

始める前に

WebSphere Application Server が実行されており、WebSphere 管理コンソールが開始されていることを確認します。

このタスクについて

トークンのデフォルトの有効期限値は 120 分ですが、これは IBM Security Identity Manager で使用するのに十分な長さではない場合があります。一部のシステムでは、実際のタイムアウト・インターバルは指定した値よりも短いことがあります。タイムアウトによりログオンできないことも生じます。タイムアウトが発生した場合、デプロイメント・マネージャー、クラスター、およびすべてのノード・エージェントをリサイクルする必要があります。

手順

1. WebSphere 管理コンソールにログオンします。
2. 「**セキュリティー**」 > 「**管理、アプリケーション、インフラストラクチャーの保護**」 > 「**認証メカニズムおよび有効期限**」 > 「**認証の有効期限**」をクリックします。
3. トークンの有効期限を、サイトで予想されているシステムの最も長い非アクティブ間隔を超える値に設定します。

次のタスク

その他のセキュリティー関連タスクを実行します。

WebSphere Application Server の FIPS 準拠

連邦情報処理標準 (FIPS) は、ソフトウェアおよびハードウェアのコンピューター・セキュリティー製品を設定するガイドラインです。FIPS 標準をサポートする製品は、製品が FIPS 承認アルゴリズムおよびメソッドのみを使用するモードに設定できます。

セキュリティー・ツールキットは、通常、FIPS 承認機能と非 FIPS 承認機能の両方をサポートします。FIPS モードでは、製品は非 FIPS 承認メソッドを使用できません。

Java において、以下の IBM 暗号プロバイダーがすべての暗号機能に確実に使用されるようにする必要があります。 *WAS_HOME*¥java¥jre¥lib¥security ディレクトリー内にある java.security ファイルの暗号プロバイダー・リストに以下のエントリーが存在するかどうかを確認します。存在しない場合は、これらのエントリーをリストに追加します。

```
security.provider.1=com.ibm.crypto.fips.provider.IBMJSSE2
security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
```

注: セキュリティー・プロバイダーを指定する順序は重要です。セキュリティー・プロバイダーは、数値順に処理されます。要求されている暗号化方式をサポートする最初のセキュリティー・プロバイダーが使用されます。Solaris システムの場合、最初のプロバイダーは必ず sun.security.provider.Sun でなければなりません。

WebSphere Application Server での FIPS 準拠のアクティブ化:

FIPS を使用するには、暗号プロバイダー・リストの設定後に、WebSphere Application Server を開始する必要があります。また、IBMJSSE2 プロバイダーを FIPS 準拠アルゴリズムに制限するように環境変数を設定する必要もあります。

始める前に

IBM 暗号プロバイダーは、java.security ファイル内に存在する必要があります。

WebSphere Application Server が実行中であり、管理コンソールが開始されていることを確認します。

WebSphere Application Server での FIPS のアクティブ化について詳しくは、WebSphere Application Server インフォメーション・センターで利用可能な資料を参照してください。

手順

1. 管理コンソールにログオンします。
2. WebSphere Application Server の FIPS をアクティブ化します。
   a. 「**セキュリティー**」 > 「**SSL 証明書と鍵の管理**」をクリックします。
   b. 「**米国連邦情報処理標準 (FIPS) アルゴリズムを使用する**」の横にあるチェック・ボックスを選択します。
   c. 「**適用**」をクリックします。
   d. 構成変更を保存します。

3. IBMJSSE2 プロバイダーを FIPS 準拠アルゴリズムに制限するように環境変数を設定します。
   a. 「**サーバー**」 > 「**アプリケーション・サーバー**」をクリックします。
   b. サーバー (server1 など) をクリックします。
   c. 「**サーバー・インフラストラクチャー**」フィールドで、「**Java およびプロセス管理**」 > 「**プロセス定義**」のリンクをクリックします。
   d. 「**追加プロパティー**」フィールドで、「**Java 仮想マシン**」のリンクをクリックします。
   e. 「**汎用 JVM 引数**」フィールドで、次のステートメントを追加することにより環境変数を設定します。

      ```
      -Dcom.ibm.jsse2.JSSEFIPS=true
      ```
4. 変更を保存します。

次のタスク

暗号マイグレーション・ツールを実行します。

暗号マイグレーション・ツール:

暗号鍵の変更、および非準拠 FIPS アルゴリズムから FIPS 準拠アルゴリズムおよび鍵への遷移のために、暗号マイグレーション・ユーティリティー changeCipher が提供されています。新規暗号鍵を使用して、マイグレーション・ユーティリティーはプロパティー・ファイルおよび LDAP 内のすべてのデータを再暗号化します。

このユーティリティーは、以下の場所にあります。

- Windows オペレーティング・システムの場合:

  ISIM_HOME¥bin¥win¥changeCipher.cmd
- UNIX または Linux オペレーティング・システムの場合:

  ISIM_HOME/bin/unix/changeCipher.sh

単一サーバー上またはデプロイメント・マネージャーでこのユーティリティーを実行し、LDAP リポジトリーおよびプロパティー・ファイル内のデータをマイグレーションします。また、各管理対象ノード (クラスター環境内) でこのユーティリティーを実行し、そのノードのプロパティー・ファイルをマイグレーションします。

以下の例に、changeCipher コマンドでサポートされる使用法およびコマンド行パラメーターを示します。

```
changekey     {keystore_name} {keystore_password}
                    [-algorithm AES] [-keysize 128 | 192 | 256]
                    [-skiperrors]
resume        [-skiperrors]
```

例えば、PBEWithMD5AndDES から AES に暗号設定をマイグレーションするには、次のコマンドを実行します。

```
changeCipher changekey itimKeystore2.jceks sunshine
```

このコマンドにより実行されるタスクを以下に示します。

- 128 ビット AES 鍵を生成し、指定された鍵ストアに書き込みます。

- LDAP リポジトリー内の暗号化データを新規暗号にマイグレーションします。

  注: 新規暗号化データは長くなります。LDAP の属性長が小さすぎる場合は、オブジェクト・クラス違反が発生し、スクリプトは終了します。
- プロパティー・ファイル内の暗号化データを新規暗号にマイグレーションします。
- `enrole.properties` に新規暗号設定値を設定します。

実行中、このツールは現在の状態情報を含むファイルを作成して維持します。このファイルは、*ISIM_HOME*¥temp¥CipherMigrator.properties に書き込まれます。マイグレーション中にエラーが発生した場合 (例えば、LDAP サーバーのシャットダウン)、問題を修正し、**resume** パラメーターを使用してツールを開始します。このパラメーターは、エラー発生前にユーティリティーが処理を中止した個所から再開するようにユーティリティーに指示します。

オプションの **-skiperrors** パラメーターは、旧暗号を使用して暗号化解除できないデータを検出した場合にも実行し続けるようにツールに指示します。指定された場合、暗号化解除できない LDAP データがあってもツールは失敗しません。

ツールを実行する前に、すべての LDAP データをバックアップします。LDAP データをマイグレーションするときは、不具合が発生する可能性のあるいくつかの状況があります。例えば、LDAP マイグレーション完了前に誤って鍵ストア・ファイルが削除された場合、一部の暗号化 LDAP データにアクセスできなくなります。LDAP データを現行の鍵ストアとともにバックアップすることにより、確実に安全な状態に戻ることができます。

ツールを実行する前に、Tivoli Identity Manager サーバーを停止します。データベース内の暗号化データはマイグレーションされないため、データベース内に保留トランザクションがないことを確認します。

各 LDAP オブジェクトに対して、暗号マイグレーション・ユーティリティーは、旧暗号を使用して属性を暗号化解除し、新規暗号を使用して属性を再暗号化します。ハッシュされている属性に対する変更は行われません。

デフォルトでは、Java Cryptography Extension (JCE) は、制限付きまたは強度制限がある暗号とともに出荷されます。192 ビットまたは 256 ビットの Advanced Encryption Standard (AES) 暗号化アルゴリズムを使用するためには、無制限準拠ポリシー・ファイルを適用する必要があります。詳しくは、Web サイト http://www.ibm.com/developerworks/java/jdk/security/index.html を参照してください。

非 root プロセスとして実行する IBM Security Identity Manager 構成

システム・セキュリティーのために、プロファイル・ディレクトリーとログ・ディレクトリーの所有権を非 root ユーザーに割り当てることができます。

1. WebSphere プロファイルを作成して、非 root ユーザーに所有権を割り当てます。WebSphere Application Server インフォメーション・センターの『*インストーラーとしてのプロファイルの作成、および非 root ユーザーへの所有権の割り当て (Creating a profile as an installer and assigning ownership to a non-root user)*』を参照してください。

2. 非 root ユーザーが以下を所有していることを確認してください。
   - *ISIM_HOME*/dirs ディレクトリー内のファイルへの読み取りアクセス権。
   - IBM Security Identity Manager ログ・ファイルへの読み取りおよび書き込みアクセス権。例: /opt/IBM/tivo../../common/CTGIM/logs/

     注: 非 root ユーザーが WebSphere および IBM Security Identity Manager のログ・ファイルに対するアクセス権を所有していることを確認します。 root が所有するログが存在する場合は、除去するか、またはログのアクセス権を変更します。
     WebSphere Application Server インフォメーション・センターの『*プロファイル作成のためにファイルおよびディレクトリーの書き込みアクセス権を非 root ユーザーに付与 (Granting write permissions of files and directories to a non-root user for profile creation)*』の説明を参照してください。

Java プラグインのインストール

Java プラグインがシステムにインストールされていないか、サポートされたレベルでない場合、ブラウザーは、プラグインのインストールを促すプロンプトを出します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権限を取得するか、代わりのユーザーにこのタスクを実行してもらうには、システム管理者に連絡してください。

このタスクについて

Java プラグインにより、ブラウザーと Java プラットフォーム間の接続、およびブラウザー内でのIBM Security Identity Manager アプレットの実行が可能になります。

IBM Security Identity Manager では、管理者が Java プラグインの静的なバージョン管理と動的なバージョン管理のいずれかを選択できます。デフォルトでは、IBM Security Identity Managerは動的なバージョン管理を使用して、1.5.x バージョンが 1.5.0 に優先して動作するようにします。あるいは、IBM Security Identity Manager は、バージョン 1.5.0_02 など、Java プラグインの静的なバージョン管理を使用できます。

プラグインを提供する外部 Web サイトは変更されることがあります。管理者は、Java プラグインをダウンロードするための内部 Web サイトを作成することもできます。静的なバージョン管理と動的なバージョン管理の選択や、ダウンロード場所の定義について詳しくは、*ISIM_HOME*¥data¥ui.properties ファイルを参照してください。

プラグインをインストールするには、以下の手順を実行します。

手順

- Windows システムでは、Internet Explorer または Mozilla Firefox ブラウザーから、Java プラグインをインストールしてブラウザーに自動的に登録することを求めるプロンプトが出されます。

  ブラウザーから Java プラグインに関するプロンプトが出されない場合は、Oracle Web サイトの Java SE ページから Java プラグインを入手できます。
- UNIX システムと Linux システムでは、以下の手動のステップを実行して、Java プラグインのインストールと登録を行う必要があります。
  1. 以下のいずれかの Web サイトから、Java プラグインを入手します。
     - Solaris または Linux システム: Oracle Web サイトの *Java SE* ページ
     - AIX システム: IBM developerWorks® Web サイトの「*AIX Download and service information*」
  2. Java プラグインをブラウザーに登録します。

認証用の外部ユーザー・レジストリーに対するインストール後の構成

認証用に外部ユーザー・レジストリーを使用するように IBM Security Identity Manager をインストールした場合は、インストール後の構成ステップを実行する必要があります。

インストール後の構成ステップを以下に示します。

1. パスワード変更要求を除去します。
2. 外部ユーザー・レジストリーの管理者アカウントを構成します。
3. 管理者アカウントのアクセス権限を検証します。
4. WebSphere アカウント・リポジトリー設定を構成します。

『パスワード変更要求の除去』に進みます。

パスワード変更要求の除去

管理コンソールにログオンしたときにパスワードの変更を要求されないように、構成を変更します。

デフォルトの管理アカウントについて、「**次回のログオン時にパスワードを変更する**」属性が無効になるように構成を変更します。「**ITIM Manager**」の `erChangePswdRequired` 属性に `false` を設定します。

ユーザー・レジストリーの構成ユーティリティーを使用してください。以下のトピックでは、IBM Tivoli Directory Server の構成の変更方法について説明します。一方のトピックでは、グラフィカル管理ユーティリティーの使用方法について説明します。もう一方のトピックでは、コマンド行ユーティリティーの使用方法について説明します。

以下のいずれかのトピックアクションに進みます。

- 167 ページの『コマンド行ユーティリティーを使用したパスワードの変更属性の無効化』

- 168 ページの『Web 管理ユーティリティーを使用したパスワード変更属性の無効化』

コマンド行ユーティリティーを使用したパスワードの変更属性の無効化

管理コンソールにログオンしたときにパスワードの変更を要求されないように、構成を変更します。

このタスクについて

属性を構成するには、コマンド行ユーティリティーを使用します。グラフィカル管理ユーティリティーを使用する場合は、以下の手順を実行しないでください。代わりに、 168 ページの『Web 管理ユーティリティーを使用したパスワード変更属性の無効化』を参照してください。

手順

1. デフォルトの管理アカウントの属性を表示します。

   例えば、デフォルトの管理アカウントが ITIM Manager の場合は以下のようにします。

   ```
   ldapsearch -D "cn=root" -w mypassword -L -b "dc=com" "eruid=ITIM Manager"
   ```

   検索結果の例を以下に示します。

   ```
   eruid=ITIM Manager,uo=systemUser,ou=itim,ou=org,dc=com
   eruid=ITIM Manager
   erpswdlastchanged=201204221506Z
   erchangepwrequired=true
   ```

2. 属性をファイルに保存します。

   以下に例を示します。

   ```
   ldapsearch -D "cn=root" -w mypassword -L -b "dc=com"
       "eruid=ITIM Manager"
   > myfile
   ```

3. エディターを使用して、erchangepwrequired=false を設定します。
4. LDAP コマンドを実行して、属性 erchangepwrequired=false を指定したファイルをロードします。

   以下に例を示します。

   ```
   ./ldapmodify -D "cn=root" -w mypassword -f myfile
   ```

   出力例:

   ```
   Operation 0 modifying entry eruid=ITIM Manager,ou=systemUser,
      ou=tim,ou=org,
   dc=com
   ```

5. 構成が正常に完了したことを確認します。

   以下に例を示します。

   ```
   ldapsearch -D "cn=root" -w mypassword -L -b "dc=com" "eruid=ITIM Manager"
   ```

   検索結果の例を以下に示します。

```
eruid=ITIM Manager,uo=systemUser,ou=itim,ou=org,dc=com
eruid=ITIM Manager
erpswdlastchanged=201204221506Z
erchangepwrequired=false
```

次のタスク

『外部ユーザー・レジストリーの管理者アカウントの構成』に進みます。

Web 管理ユーティリティーを使用したパスワード変更属性の無効化

管理コンソールにログオンしたときにパスワードの変更を要求されないように、構成を変更します。

このタスクについて

ディレクトリー・サーバーの管理ユーティリティーを使用できます。以下の手順では、IBM Tivoli Directory Server Web 管理ツールの使用方法を説明します。

コマンド行ユーティリティーを使用する場合は、この手順を使用しないでください。代わりに、167 ページの『コマンド行ユーティリティーを使用したパスワードの変更属性の無効化』を参照してください。

手順

1. 管理者として、IBM Tivoli Directory Server Web 管理ツールにログオンします。
2. 「**ディレクトリー管理**」>「**項目の管理**」に移動します。 ITIM Manager という項目を見つけます。

   ITIM Manager は、デフォルトの管理者アカウントです。
3. eruid=ITIM Manager をクリックし、「**次へ**」をクリックします。

   注: デフォルトの管理者に別のアカウントを指定した場合は、ITIM Manager の代わりにそのアカウントを変更してください。例えば、UNIX オペレーティング・システムではスペースを含むアカウント名を作成できません。この場合、管理者によっては別のアカウント名 (itimManager など) を作成している場合があります。
4. 「項目の編集」ページで、「**オプションの属性**」を選択します。
5. erChangePswdRequired 属性までスクロールダウンし、値を **False** に変更します。
6. 「**終了**」をクリックして、変更を保存します。

次のタスク

『外部ユーザー・レジストリーの管理者アカウントの構成』に進みます。

外部ユーザー・レジストリーの管理者アカウントの構成

外部ユーザー・レジストリーを使用するときに、デフォルトの管理者 ID を ITIM Manager 以外の値に設定する場合は、デフォルトの管理者アカウントを構成する必要があります。

このタスクについて

デフォルトの IBM Security Identity Manager インストールでは、ITIM Manager という管理者アカウントが作成されます。オプションで、別の管理者アカウント名の使用を選択できます。IBM Security Identity Manager をインストールする環境に、外部ユーザー・レジストリーを使用する WebSphere セキュリティー・ドメインが既に存在している場合、このオプションは便利です。

以下の手順では、デフォルトの管理者アカウントを ITIM Manager から itimManager に変更する方法の例を示します。この手順では、IBM Tivoli Directory Server LDAP ディレクトリー・サーバーを、最初のステップに示す組織単位で使用するものと仮定します。

手順

1. 以下の内容を含むテキスト・ファイルを作成します。

```
dn: eruid=ITIM Manager,ou=systemUser,ou=itim,ou=org,dc=com
changetype: modrdn
newrdn: eruid=itimManager
deleteoldrdn: 1
```

2. 作成したテキスト・ファイルを使用する **ldapmodify** コマンドを実行します。

   コマンド構文:

```
ldapmodify -h hostIP -D adminDN -w adminPassword  -i filePath
```

表 15. 管理者アカウントを変更するサンプル **ldapmodify** *コマンド*

項目	説明
ldapmodify	このコマンドは、*TDS_HOME*/bin ディレクトリーにあります。以下に例を示します。 **Windows** C:¥Program Files¥LDAP¥V6.3¥bin **UNIX または Linux** *TDS_HOME*/bin
hostIP	IBM Security Identity Manager LDAP データが保管されている IBM Tivoli Directory Server の IP アドレス。
adminDN	管理者の DN。例えば、cn=root です。
adminPassword	管理者パスワード
filePath	前のステップで作成したファイルへのパス。

3. 新しいデフォルトの管理者 ID を使用して、IBM Security Identity Manager プロパティー・ファイル ISIM_HOME/data/enRole.properties を更新します。

   エントリーの例は、以下のとおりです。

```
enrole.defaultadmin.id=itimManager
```

4. WebSphere アプリケーション・サーバーを再始動して、プロパティー・ファイルから更新済みの値をロードします。

次のタスク

170 ページの『管理者アカウントのアクセス権限の検証』に進みます。

管理者アカウントのアクセス権限の検証

管理者アカウントが正しく構成されていることを検証します。

このタスクについて

IBM Security Identity Manager 管理者が、外部ユーザー・レジストリーを使用した認証によって正常にログインできることを確認します。

手順

1. IBM Security Identity Manager 管理コンソールにログオンします。

   デフォルト URL にアクセスします。ここで、`hostIP` は IBM Security Identity Manager を実行するサーバーの IP アドレスまたは完全修飾ドメイン名です。

   `http://hostIP:9080/itim/console`

2. IBM Security Identity Manager のインストール時に指定した管理者名を使用してください。

   デフォルトの管理者アカウントは `ITIM Manager` です。ただし、オプションで別の名前を指定できます。

3. 管理者アカウント用に指定したパスワードを入力します。

   デフォルト・パスワードは `secret` です。

タスクの結果

デフォルトの管理者ユーザー用に使用したパスワードを指定して正常にログインできる場合は、LDAP ユーザー・レジストリーが IBM Security Identity Manager の外部認証ユーザー・レジストリーとして正常に構成されています。

次のタスク

『WebSphere アカウント・リポジトリー設定の構成』に進みます。

WebSphere アカウント・リポジトリー設定の構成

WebSphere アカウント・リポジトリー属性のデフォルト値を除去するには、管理コンソールを使用します。

このタスクについて

管理コンソールを使用してサービスを管理できます。コンソールで「**サービスの管理**」を選択すると、サービスを選択して「サービス情報」ページにアクセスできます。このページを使用して、サービスの属性値を更新できます。

外部ユーザー・レジストリーの構成を完了するには、ITIM サービスの「サービス情報」ページで「**WebSphere アカウント・リポジトリー**」属性の値を変更する必要があります。このフィールドの値で、IBM Security Identity Manager が認証のために使用するアカウント・リポジトリー・サービスが指定されます。デフォルトでは、このフィールドは、IBM Security Identity Manager *カスタム・レジストリー* をサポートする `ITIM Service` に設定されます。

カスタム・レジストリーではなく*外部レジストリー* の使用を選択済みです。外部レジストリーの構成を完了するには、フィールドからデフォルト値を除去する必要があります。

手順

1. 現在 IBM Security Identity Manager 管理コンソールにログオンしていない場合は、ここで管理者としてログインしてください。

   ログインの説明については、170 ページの『管理者アカウントのアクセス権限の検証』を参照してください。
2. 「**サービスの管理**」をクリックします。
3. 「サービスの選択」ページで「**検索**」をクリックします。

   検索結果に、構成済みの各サービスの項目を示すテーブルが表示されます。
4. そのテーブルで、「**ITIM サービス**」のチェック・ボックスを選択します。
5. 「**変更**」をクリックします。
6. 「サービス情報」ページで、「**WebSphere アカウント・リポジトリー**」フィールドを見つけます。このフィールドの値は、`ITIM Service` です。「**クリア**」をクリックします。

   これで、「**WebSphere アカウント・リポジトリー**」フィールドが空になります。

   詳しくは、オンライン・ヘルプを参照してください。オンライン・ヘルプを表示するには、「**?**」アイコンをクリックします。ブラウザーの新規ブラウザー・ウィンドウに「サービスの変更」ヘルプ・ファイルが表示されます。「**サービス情報**」をクリックします。「サービス情報」ヘルプ・ページで、「**ITIM サービス**」をクリックします。このページの内容を確認します。
7. 「**OK**」をクリックします。

タスクの結果

これで、認証用の外部ユーザー・レジストリーの構成は完了です。

外部レジストリーの使用方法について詳しくは、『*外部ユーザー・レジストリーを使用した IBM Security Identity Manager の構成と使用 (Configuring and using IBM Security Identity Manager with an external user registry)*』のチュートリアル例を参照してください。この文書は、ご使用のコードがインストールされたファイル・システムにあります。*ISIM_HOME*/extensions/6.0/doc/authentication/Using_an_External_User_Registry.odt を参照してください。

第 10 章 トラブルシューティング

このセクションでは、IBM Security Identity Manager のインストールの問題を修正する方法について説明します。

IBM Security Identity Manager サーバーの問題

ここでは、IBM Security Identity Manager サーバーのインストール時に発生することのある、一般的な問題を解決するのに役立つ情報を説明します。

インストール・プログラムの開始時の問題

IBM Security Identity Manager インストール・プログラムを開始できない場合は、以下の要件を確認してください。

- インストール・プログラムを実行するのに十分な実メモリーが使用可能になっていますか。詳しくは、IBM Security Identity Manager インフォメーション・センターの『*ハードウェア要件およびソフトウェア要件*』を参照してください。
- 正しいオペレーティング・システム・レベル、パッチ、およびスペース要件が、ハードウェアおよびソフトウェア前提条件に与えられていますか。詳しくは、IBM Security Identity Manager インフォメーション・センターの『*ハードウェア要件およびソフトウェア要件*』を参照してください。
- インストール・プログラムが、実行に必要な正しいファイル・アクセス権を所有していますか。管理特権が必要です。
- ファイアウォールによって、インストール中にアクティブなプロセスが、外部リソースにアクセスできないようになっていますか。例えば、ファイアウォールのために **ldapsearch** がディレクトリー・サーバーに接続できない場合、IBM Security Identity Manager のインストールは失敗します。
- UNIX システムまたは Linux システムにインストールする場合は、正しいアクセス権および表示変数セットを所有していますか。

  よくある間違いは、デスクトップにログオンして、アクセス・コントロールの使用不可化を省略することです。その後に Telnet または SSH を使用して、IBM Security Identity Manager サーバーをインストールするリモート・ホストに接続します。この問題を訂正するには、以下のようにします。

  1. デスクトップのコマンド・シェルで以下のコマンドを実行し、X サーバーのアクセス・コントロールを使用不可にします。

     ```
     xhost +
     ```

  2. Telnet または SSH を使用して、リモート・ホストに接続します。次のコマンドを実行して、DISPLAY 環境変数を設定します。

     ```
     export DISPLAY=hostname:0.0
     ```

     hostname の値は、ローカル・デスクトップ・コンピューターのホスト名または IP アドレスです。

IBM Security Identity Manager 構成エラー

IBM Security Identity Manager アクティビティー要約ログ・ファイル (itim_install_activity.log) をチェックします。致命的でないエラーが報告され、DBConfig、ldapConfig、またはシステム構成が関わる場合は、スタンドアロンの IBM Security Identity Manager 構成ユーティリティーを使用してリカバリーすることができます。

IBM Security Identity Manager サーバーが始動しない

IBM Security Identity Manager サーバーが開始しない場合は、以下のログ・ファイルを調べてください。記録されたエラーを修正してください。

- *WAS_PROFILE_HOME*¥logs¥*server_name*¥SystemOut.log

  PROFILE の値は、IBM Security Identity Manager を実行する WebSphere Application Server プロファイルの名前です。

  server_name の値は、単一サーバー環境の場合は通常 server1 です。

- *TIVOLI_COMMON_DIRECTORY*¥CTGIM¥logs¥trace.log

  このディレクトリーでは、msg.log ファイルも調べてください。IBM Security Identity Manager サーバーをインストールすると、*TIVOLI_COMMON_DIRECTORY* の値が定義されます。

IBM Security Identity Manager にログオンできない

連続して IBM Security Identity Manager へのログオンに失敗する場合は、SystemOut.log ファイルに IBM Security Identity Manager プロパティー・ファイルの参照に関するエラーが含まれていないかどうかを判別してください。

始める前に

WebSphere Application Server が実行されており、WebSphere 管理コンソールが開始されていることを確認します。

ISIM_HOME¥data ディレクトリーにプロパティー・ファイルが含まれていることを確認します。

手順

1. WebSphere Application Server が *ISIM_HOME*¥data ディレクトリーを参照していることを検証するには、WebSphere 管理コンソールにログオンします。
2. 「**サーバー**」 > 「**アプリケーション・サーバー**」をクリックします。
3. 「**サーバー・インフラストラクチャー**」 > 「**Java およびプロセス管理**」の下で server1 などのサーバーを選択し、「**プロセス定義**」をクリックします。
4. 「プロセス定義」で、「**Java 仮想マシン**」をクリックします。
5. 「クラスパス」フィールドで *ISIM_HOME*¥data ディレクトリーが指定されていることを確認します。

次のタスク

連続して試行が失敗した場合は、IBM Security Identity Manager ミドルウェアの状況を調べてください。

- を参照してください。 122 ページの『データベース接続の検証』
- 123 ページの『ディレクトリー・サーバーが正常に実行されていることの検証』

メッセージング・エンジンが始動しない

メッセージング・エンジンが始動しない場合は、データ・ソース接続を確認する必要があります。

始める前に

WebSphere Application Server が実行されており、WebSphere 管理コンソールが開始されていることを確認します。

手順

1. WebSphere 管理コンソールにログインします。
2. 「**サービス統合**」 > 「**バス**」を選択します。
3. 「**itim_bus**」をクリックします (存在する場合)。
4. 「トポロジー」セクションで、「**メッセージング・エンジン**」をクリックします。
5. メッセージング・エンジン名をクリックします。
6. 「追加プロパティー」セクションで、「**メッセージ・ストア**」をクリックして、データ・ソースの JNDI 名を確認します。
7. この JNDI 名から、「リソース」セクションで定義された IBM Security Identity Manager データ・ソースにリンクします。
8. データ・ソース接続をテストします。 122 ページの『データベース接続の検証』を参照してください。
   - データ・ソースの接続テストが失敗する場合は、 176 ページの『データベース接続の失敗』を参照してください。
   - 接続テストが成功する場合は *WAS_PROFILE_HOME*¥logs¥server_name¥SystemOut.log ファイルを調べて、メッセージング・エンジンを開始できない理由を判別してください。

次のタスク

その他のトラブルシューティングを実行するか、検証タスクに戻ります。

データベースの問題

ここでは、IBM Security Identity Manager サーバーのインストール時に発生することのある、データベースに関する一般的な問題のいくつかを解決するのに役立つ情報を説明します。

データベース接続の失敗

データベース接続の検証時に動作しなかった接続を修正するには、以下のタスクを実行します。

始める前に

WebSphere Application Server が実行されており、WebSphere 管理コンソールが開始されていることを確認します。

このタスクについて

このタスクでは、IBM DB2 で使用する値を示します。Microsoft SQL Server または Oracle データベースを使用している場合は、適切な値を使用して同様のステップを実行してください。詳しくは、ご使用のデータベース製品の資料を参照してください。

手順

1. CLASSPATH 値が正しいことを確認してください。 JDBC プロバイダーの CLASSPATH 定義は、IBM Security Identity Manager のインストール時にセットアップされます。
   a. WebSphere 管理コンソールにログオンします。
   b. 「**リソース**」 > 「**JDBC**」 > 「**JDBC プロバイダー**」 > 「**ITIM XA DB2 JDBC Provider**」をクリックします。
   c. プロパティーを調べて、CLASSPATH 値が正しいことを確認します。 例えば、DB2 の場合、その値は以下のような値になります。

      ```
      $ITIM_DB_JDBC_DRIVER_PATH¥db2jcc.jar
      $ITIM_DB_JDBC_DRIVER_PATH¥db2jcc_license_cisuz.jar
      $ITIM_DB_JDBC_DRIVER_PATH¥db2jcc_license_cu.jar
      ```

   d. $ITIM_DB_JDBC_DRIVER_PATH の値を判別するには、「**環境**」 > 「**WebSphere 変数**」をクリックします。 リストをスクロールしてこの変数を見つけ、それが正しいことを確認します。
2. DB2 ユーザー ID およびパスワードが正しいことを確認します。
   a. WebSphere 管理コンソールにログオンします。
   b. 「**リソース**」 > 「**JDBC**」 > 「**データ・ソース**」 > 「**ITIM データ・ソース**」をクリックします。
   c. 以下のフィールドを調べ、値が正しいことを確認します。
      - コンポーネント管理認証別名

        この値は `itim-init` です。
      - コンテナー管理認証別名

        この値は `itim-init` です。
3. 「関連項目」カテゴリーの「**JAAS - J2C 認証データ**」をクリックし、「別名」リストを調べて、「itim-init」項目が存在していることを確認します。
   a. 「**itim-init**」をクリックします。

b. 「ユーザー ID」フィールドの値が、*ISIM_HOME*¥data¥enRole.properties ファイルで指定された Tivoli Identity Manager データベース・ユーザー (例えば、itimuser) と一致していることを確認します。この値は変更しないでください。

c. パスワード・フィールドに注意してください。このフィールドを使用してパスワードをリセットした場合は、入力するパスワード値が、*ISIM_HOME*¥data¥enRoleDatabase.properties ファイルで定義されている値に等しいことを確認してください。

4. 他のデータベース設定が正しいことを確認します。 netstat などのユーティリティーを使用して、DB2 のサービス Listen ポート (通常は 50000、50002、または 60000) の状況を確認します。システムの etc ディレクトリーには、使用される実際のポート番号が含まれている services というファイルがあります。詳しくは、『*正しいサービス Listen ポートおよびサービス名の決定*』を参照してください。

5. DB2 がそのポートで listen しておらず、IPv6 と UNIX/Linux を使用して DB2 に接続している場合は、/etc/hosts ファイルを変更します。

a. IPv6 を実行しているワークステーションで、以下の 2 行を /etc/hosts ファイルに追加します。

```
IPv4_address hostname
IPv6_address hostname
```

例えば、ホスト名が myhost、IPv6_address が 0000:ffff:ffff:0000:20e:cff:fe50:39c8、IPv4_address が 192.168.4.4 である場合は、/etc/hosts ファイルに以下の 2 行を追加します。

```
192.168.4.4 myhost
0000:ffff:ffff:0000:20e:cff:fe50:39c8 myhost
```

b. DB2 インスタンス所有者としてログインし、以下のコマンドを実行することにより DB2 サーバーを再始動します。

```
db2stop
db2start
```

a. 以下のコマンドを実行することにより、DB2 が IPv6 アドレスで実行されていることを確認します。

```
netstat -an | grep db2port
```

例えば、DB2 がポート 50000 で実行されている場合、出力として以下の行が表示されます。

```
tcp        0      0 :::50000                :::*                    LISTEN
```

次のタスク

その他のトラブルシューティングを実行するか、検証タスクに戻ります。

SQL Server でパスワード変更のプロンプトが出されない

itim manager アカウントが初めてログインすると、通常はパスワードを変更するように求めるプロンプトがそのユーザーに出されます。SQL Server 2008 を使用している場合は、このプロンプトが出されないことがあります。

始める前に

IBM Security Identity Manager と Microsoft SQL Server がインストールされている必要があります。

手順

1. パスワード・プロンプトに関する問題を解決するには、SQL Server 2008 のホスト・コンピューターにログオンします。
2. Microsoft SQL Server Management Studio を開始します。
3. オブジェクト・エクスプローラーで SQL Server を展開します。
4. 「**データベース**」を展開し、マスター・データベースに移動します。
5. 「**セキュリティ**」 > 「**スキーマ**」を展開します。
6. 「**DBO**」を右クリックし、「**プロパティ**」をクリックします。
7. 「**権限**」、「**追加**」の順にクリックして、参照により必要なユーザーを追加します。
8. これらの必要なユーザーにすべての権限を付与し、「**OK**」をクリックします。
9. サーバーを再始動し、切断後、混合認証モードでユーザー `sa` を使用して再接続します。

次のタスク

その他のトラブルシューティングを実行するか、検証タスクに戻ります。

データベース構成が SQL Server に対して厳しすぎる

IBM Security Identity Manager では、Microsoft SQL Server 2008 が IBM Security Identity Manager データベースとして構成されます。 `trace.log` ファイルに、アクセス権が拒否されたことを示すメッセージが記録される場合があります。

始める前に

IBM Security Identity Manager と Microsoft SQL Server がインストールされている必要があります。

このタスクについて

このエラー・メッセージは、DBConfig を実行した後で IBM Security Identity Manager サーバーに初めてアクセスしたときに発生する可能性があります。

```
javax.transaction.xa.XAException: java.sql.SQLException:
Failed to create the XA control connection.
Error: EXECUTE permission denied on object 'xp_sqljdbc_xa_init',
database 'master', schema 'dbo'.
```

この問題を解決するには、以下のステップを実行します。

注: 以下のタスクでは、*itimuser* は IBM Security Identity Manager データベース用に構成されたデータベース・ユーザーで、*itimdb* は IBM Security Identity Manager 用に構成されたデータベース名です。

手順

1. アプリケーション・サーバーを停止します。
2. Microsoft SQL Server Management Studio を開始します。
3. オブジェクト・エクスプローラーで SQL Server を展開します。
4. 「**データベース**」を展開し、*itimdb* を削除します。
5. マスター・データベースから *itimuser* スキーマを削除します。
   a. 「**データベース**」「**システム データベース**」「**master**」「**セキュリティ**」「**スキーマ**」を展開します。
   b. itimuser を削除します。
6. itimuser、ITIML000、ITIML001 などを削除し、「**セキュリティ**」「**ログイン**」からログインします。
7. データベースを作成します。
8. dbConfig 操作を実行します。
9. アプリケーション・サーバーを開始します。

注: データベースの名前またはデータベース・ユーザーを変更した場合は、runConfig ユーティリティーを実行し、アプリケーション・サーバーを再始動します。

次のタスク

その他のトラブルシューティングを実行するか、検証タスクに戻ります。

オブジェクト名が無効な場合のデータ複製エラーの修正

共有アクセス構成ユーティリティーを実行しなかった場合は、クラスター環境でデータ複製エラーが発生することがあります。

このタスクについて

IBM Security Identity Manager をクラスター環境にデプロイして、共有アクセスを構成すると、データ複製でエラーが報告される場合があります。このエラーは、無効なオブジェクト名が見つかったことを示します。エラーのパターンは以下のとおりです。

```
Invalid object name itimuser.isim_object_name
```

以下に例を示します。

```
Invalid object name 'itimuser.erAccountItem'
Invalid object name 'itimuser.erServiceItem'
Invalid object name 'itimuser.erSystemUser'
```

この場合、データ複製が失敗するのは、**DBConfig** を実行してデータベース・テーブルをすべて除去したが、**SAConfig** を実行して共有アクセス・モジュールに固有のテーブルを再設定しなかった場合です。

ファイル *ISIM_HOME*/data/dataSynchronization.properties には、複製するように構成されたエントリーが含まれています (erAccountItem や erServiceItem など)。

ただし、複製コンポーネントでは、DB_REPLICATION_CONFIG で指定されたターゲット複製テーブルを見つけることはできません。この場合、このコンポーネントがデフォルトのクラス名になります。

この問題を解決するには、以下の手順の各ステップを実行します。

手順

1. デプロイメント・マネージャー上で、IBM Security Identity Manager インストール・ロケーション内の bin ディレクトリーに切り替えて、**SAConfig** ユーティリティーを実行します。

   以下に例を示します。

   表 16. SAConfig の実行

オペレーティング・システム	コマンド
Windows	C:¥Program Files¥IBM¥isim¥bin で、「SAConfig」をクリックするか、コマンド・ウィンドウを開いて **SAConfig** と入力します。
UNIX または Linux	/opt/IBM/isim/bin で、**./SAConfig** と入力します。

2. ISIM_HOME/data/KMIPServer.properties ファイルの clipassword プロパティーを更新します。

   どのようなストリング値でも指定できます。以下に例を示します。

   ```
   clipassword=test
   ```

   注: このファイルは、デプロイメント・マネージャー上でのみ編集してください。

3. クレデンシャル・ボールト・サーバーの鍵ストア・ファイルを構成します。

   注: このステップは、デプロイメント・マネージャーでのみ実行します。クラスター・メンバーでは、このステップは実行する必要はありません。

   次のコマンドで、-p パラメーターの値が、ISIM_HOME/data/KMIPServer.properties ファイルの clipassword に指定した値と同じであることを確認します。

   以下のとおり、ご使用のオペレーティング・システム用のコマンドを使用します。

   - Windows オペレーティング・システムの場合、次のように入力します。

     ```
     cd /d "ISIM_HOME¥lib"
     ```

     ISIM_HOME¥lib ディレクトリーから次のコマンドを実行します。

     ```
     "ISIM_HOME¥jre¥jre¥bin¥java"-cp
     com.ibm.sec.authz.jaccplus_7.3.1.jar;
     com.ibm.sec.authz.xacml4j_7.3.1.jar;
     j2ee.jar;
     ojdbc.jar;
     db2jcc.jar;
     db2jcc_license_cu.jar;
     sqljdbc.jar;
     com.ibm.tklm.kmip.jar;
     ```

```
CVCommon.jar;
CVCore.jar;
CVCli.jar;
com.ibm.tklm.credvault.common.jar;
commons-cli.jar;
com.ibm.cv.kmip.ext.jar
-DKMIPConfigProperties="$USER_INSTALL_DIR$$¥$data$¥$KMIPServer.properties"
-Djava.security.auth.login.config==login.config
-Djava.security.auth.policy==jaas.policy
com.ibm.cv.cli.CVShell -u test -p test
```

- UNIX または Linux オペレーティング・システムの場合、次のように入力します。

  ```
  cd "ISIM_HOME/lib"
  ```

  ISIM_HOME¥lib ディレクトリーから次のコマンドを実行します。

  ```
  "ISIM_HOME/jre/jre/bin/java"-cp
  com.ibm.sec.authz.jaccplus_7.3.1.jar:
  com.ibm.sec.authz.xacml4j_7.3.1.jar:
  j2ee.jar:
  ojdbc.jar:
  db2jcc.jar:
  db2jcc_license_cu.jar:
  sqljdbc.jar:
  com.ibm.tklm.kmip.jar:
  CVCommon.jar:
  CVCore.jar:
  CVCli.jar:
  com.ibm.tklm.credvault.common.jar:
  commons-cli.jar:
  com.ibm.cv.kmip.ext.jar:
  -DKMIPConfigProperties="$USER_INSTALL_DIR$$/$data$/$KMIPServer.properties"
  -Djava.security.auth.login.config==login.config
  -Djava.security.auth.policy==jaas.policy
  com.ibm.cv.cli.CVShell -u test -p test
  ```

  このコマンドにより、cvKeystore.jceks および pwdEncKeystore.jceks という 2 つのクレデンシャル・ボールト鍵ストア・ファイルが *ISIM_HOME*/data/keystore ディレクトリーの下に生成されます。また、*ISIM_HOME*/data/KMIPServer.properties 内の暗号鍵、およびクレデンシャル・ボールト・データベースのデータ・エントリーが更新されます。

4. 生成された鍵ストア・ファイルと KMIPServer.properties を WAS_DM_profile_path/config/cells/*cellName*/itim ディレクトリーにコピーします。

   注: このステップは、デプロイメント・マネージャーでのみ実行します。クラスター・メンバーでは、このステップは実行する必要はありません。

5. WebSphere Application Server デプロイメント・マネージャー・コンソールから手動でノードを同期化します。
6. 各クラスター・メンバー上で、WebSphere プロファイル・ディレクトリー階層にある次のクレデンシャル・ボールト・ファイルを IBM Security Identity Manager データ・ディレクトリー階層にコピーします。

表 17. コピーするクレデンシャル・ボールト・サーバー・ファイル

コピーするファイル	コピー先
WAS_PROFILE_PATH/config/cells/*cellName*/itim/cvKeystore.jceks	*ISIM_HOME*/data/keystore/cvKeystore.jceks

表 17. コピーするクレデンシャル・ボールト・サーバー・ファイル (続き)

コピーするファイル	コピー先
WAS_PROFILE_PATH/config/cells/*cellName*/itim/pwdEncKeystore.jceks	*ISIM_HOME*/data/keystore/pwdEncKeystore.jceks
WAS_PROFILE_PATH/config/cells/*cellName*/itim/KMIPServer.properties	*ISIM_HOME*/data/KMIPServer.properties

7. WebSphere Application Server クラスターを再始動します。

ディレクトリー・サーバーの問題

ここでは、IBM Security Identity Manager サーバーのインストール時に発生することのある、ディレクトリー・サーバーに関する一般的な問題を解決するのに役立つ情報を説明します。

ディレクトリー・サーバーが始動しない

再始動を試みてもディレクトリー・サーバーが始動しない場合は、ibmslapd.log ファイルを確認します。

ibmslapd.log ファイルを調べて、ディレクトリー・サーバーが完全に始動したのか、それとも部分的に始動したのかを示すメッセージがないかどうかを確認します。修正アクションを実行します。

このログ・ファイルのロケーションは、次のように IBM Tivoli Directory Server のバージョンによって異なります。

- Windows オペレーティング・システム:

  ITDS_INSTANCE_HOME¥logs¥ibmslapd.log。例えば、このファイルは C:¥idsslapd-ldapdb2¥logs ディレクトリーにあります。
- UNIX または Linux オペレーティング・システム:

  ITDS_INSTANCE_HOME/etc/ibmslapd.log。例えば Linux では、このファイルは /home/ldapdb2/idsslapd-ldapdb2/etc/logs ディレクトリーにあります。

Tivoli Directory Integrator の問題

ここでは、IBM Tivoli Directory Integrator バージョン 7.1 を Red Hat Linux Enterprise 6.0 にインストールするときの問題を解決するのに役立つ情報を説明します。

launchpad.sh で IBM Tivoli Directory Integrator のインストールを開始できない

Red Hat Linux Enterprise 6.0 上で launchpad.sh を使用して IBM Tivoli Directory Integrator バージョン 7.1 のインストール・ランチパッドを開始できない場合は、代わりに install_tdi71_linux_x86.bin を使用します。

Web ブラウザーの問題

ここでは、IBM Security Identity Manager サーバーのインストール時に発生することのある、Web ブラウザーに関する一般的な問題を解決するのに役立つ情報を説明します。

IBM Security Identity Manager ログオン障害

さまざまな理由から、IBM Security Identity Manager にログオンできない場合があります。例えば、サポートされていない Web ブラウザーを使用している可能性がある場合などです。

サポートされるブラウザーのリストについては、IBM Security Identity Manager インフォメーション・センターの『*クライアント接続のためのブラウザー要件*』を参照してください。

ブラウザーに Java プラグインが登録されていることの確認

IBM Security Identity Manager は、Java 2 Runtime Environment、Standard Edition (JRE) が提供している Java プラグインを必要とするアプレットを使用します。Java プラグインにより、ブラウザーと Java プラットフォーム間の接続、およびブラウザー内でのアプレットの実行が可能になります。 IBM Security Identity Manager でサポートされる Java プラグインのバージョンについて詳しくは、IBM Security Identity Manager インフォメーション・センターの『*ソフトウェア前提条件*』を参照してください。

Java プラグインがシステムにインストールされていないか、サポートされたレベルでない場合、ブラウザーは、プラグインのインストールを促すプロンプトを出します。これらのステップについて詳しくは、IBM Security Identity Manager インフォメーション・センターの『*Java プラグインのインストール*』を参照してください。

同一コンピューター上での 2 つの Web ブラウザー・セッションの回避

同一のクライアント・コンピューターから、2 つの別々のブラウザー・セッションを開始しないでください。 2 つのセッションは 1 つのセッション ID とみなされ、結果としてデータに関連する問題が発生します。

Microsoft Internet Explorer でのアクティブ・スクリプトの有効化

Microsoft Internet Explorer については、「インターネット オプション」の「スクリプト」セクションで「アクティブ スクリプト」項目が使用可能になっていることを確認してください。

始める前に

サポートされているバージョンの Internet Explorer がインストールされている必要があります。

手順

1. Internet Explorer を開始します。

2. メインメニューで、「**ツール**」 > 「**インターネット オプション**」をクリックします。
3. 「セキュリティ」タブで「**インターネット**」アイコンをクリックし、「**レベルのカスタマイズ**」をクリックします。
4. 「スクリプト」の「アクティブ スクリプト」エリアで、「**有効にする**」を選択します。
5. 「**OK**」をクリックします。
6. 「インターネット オプション」ウィンドウで、「**OK**」をクリックします。

次のタスク

その他のトラブルシューティングを実行するか、検証タスクに戻ります。

WebSphere Application Server の問題

ここでは、IBM Security Identity Manager サーバーのインストール時に発生することのある、WebSphere Application Server に関する一般的な問題を解決するのに役立つ情報を説明します。

IBM Security Identity Manager アプリケーションは、WebSphere Application Server 内で、エンタープライズ・アプリケーションとして稼働します。IBM Security Identity Manager インストール・プログラムでは、WebSphere コマンド行インターフェース (`wsadmin`) を使用し、IBM Security Identity Manager アプリケーションを WebSphere Application Server にデプロイします。IBM Security Identity Manager アプリケーションをデプロイすると、WebSphere Application Server で特定の構成ステップも実行されます。

デプロイメントが完了すると、IBM Security Identity Manager ファイルは以下のディレクトリーに格納されます。

- *WAS_PROFILE_HOME*¥installedApps¥*cellname*¥ITIM.ear
- *WAS_PROFILE_HOME*¥config¥cells¥*cellname*¥applications¥ITIM.ear

デプロイメントが失敗した場合は、*ISIM_HOME*¥`install_logs¥` ディレクトリーの下にあるインストール・ログ・ファイルを確認します。 itim_install_activity.log ファイルから始めます。また、setupEnrole.stdout ログ・ファイルも調べます。

接続スクリプト・エラーの訂正

このタスクは、WebSphere Application Server 構成マネージャーへの SOAP 接続の確立に失敗したことがログ・データで示されている場合に使用します。このタスクは、WebSphere Application Server のスクリプト・エラーが発生した場合にも使用できます。

始める前に

WebSphere Application Server と IBM Security Identity Manager がインストールされていることを確認します。

手順

1. WebSphere Application Server へ接続できない問題、またはスクリプト・エラーとして説明されている問題を解決します。詳しくは、WebSphere の資料を参照してください。
2. 以下のいずれかのコマンドを実行して、IBM Security Identity Manager サーバーを WebSphere Application Server にデプロイします。
   - WebSphere の管理セキュリティーおよびアプリケーション・セキュリティーが有効になっている場合は、以下のいずれかのコマンドを入力します。
     - Windows オペレーティング・システム:

       ```
       ISIM_HOME¥bin¥setupEnrole.exe install server:server_name user:user_id
       password:pwd ejbuser:ejb_user_id ejbpassword:ejbpassword
       ```

     - UNIX または Linux オペレーティング・システム:

       ```
       ISIM_HOME¥bin¥setupEnrole.sh install server:server_name user:user_id
       password:pwd ejbuser:ejb_user_id ejbpassword:ejbpassword
       ```

     server_name の値は、IBM Security Identity Manager アプリケーションのデプロイ先である WebSphere Application Server の名前です。*user_id* の値は、*wsadmin* などの WebSphere アドミニストレーター・ユーザー ID です。*pwd* の値は、*secret* などの WebSphere アドミニストレーター・ユーザー ID のパスワードです。 *ejb_user_id* の値は、Identity Manager System ユーザー ID です。これは、デフォルトで WebSphere 管理者ユーザー ID を使用します。

     注: Identity Manager のシステム・ユーザー ID に、*Bob Smith* など間にスペースがある値を指定する場合は、この値に引用符を追加する必要があります。例えば、コマンドは以下のように入力する必要があります。

     ```
     SetupEnrole.exe install server:server1 user:wsadmin password:secret
     ejbuser:"Bob Smith" ejbpassword:secret
     ```

   - WebSphere の管理セキュリティーおよびアプリケーション・セキュリティーが無効になっている場合は、以下のいずれかのコマンドを入力します。
     - Windows オペレーティング・システム:

       ```
       ISIM_HOME¥bin¥setupEnrole.exe install server:server_name
       ```

     - UNIX または Linux オペレーティング・システム:

       ```
       ISIM_HOME¥bin¥setupEnrole.exe install server:server_name
       ```

     server_name のデフォルトは、server1 です。

次のタスク

その他のトラブルシューティングを実行するか、検証タスクに戻ります。

タイムアウト・エラーの訂正

失敗の原因がタイムアウト・エラーであることがログ・データで示されている場合は、IBM Security Identity Manager のインストール・プロセスを続行します。

始める前に

IBM Security Identity Manager のインストール・プロセスが完了していることを確認します。

手順

1. 以下のディレクトリーがある場合は、これらを削除します。
   - *WAS_PROFILE_HOME*¥installedApps¥*cellname*¥ITIM.ear
   - *WAS_PROFILE_HOME*¥config¥cells¥*cellname*¥applications¥ITIM.ear
2. 以下のいずれかのコマンドを実行して、IBM Security Identity Manager サーバーを WebSphere Application Server にデプロイします。
   - WebSphere の管理セキュリティーおよびアプリケーション・セキュリティーが有効になっている場合は、以下のいずれかのコマンドを入力します。
     – Windows オペレーティング・システム:

     ```
     ISIM_HOME¥bin¥setupEnrole.exe install server:server_name user:user_id
     password:pwd ejbuser:ejb_user_id ejbpassword:ejbpassword
     ```

     – UNIX または Linux オペレーティング・システム:

     ```
     ISIM_HOME¥bin¥setupEnrole.sh install server:server_name user:user_id
     password:pwd ejbuser:ejb_user_id ejbpassword:ejbpassword
     ```

     server_name の値は、IBM Security Identity Manager アプリケーションのデプロイ先である WebSphere Application Server の名前です。*user_id* の値は、*wsadmin* などの WebSphere アドミニストレーター・ユーザー ID です。*pwd* の値は、*secret* などの WebSphere アドミニストレーター・ユーザー ID のパスワードです。 *ejb_user_id* の値は、システム・ユーザー ID です。これは、デフォルトで WebSphere Application Server 管理者ユーザー ID を使用します。

     注: システム・ユーザー ID に、*Bob Smith* などの間にスペースがある値を指定する場合は、この値に引用符を追加する必要があります。例えば、コマンドは以下のように入力する必要があります。

     ```
     SetupEnrole.exe install server:server1 user:wsadmin password:secret
     ejbuser:"Bob Smith" ejbpassword:secret
     ```

   - WebSphere の管理セキュリティーおよびアプリケーション・セキュリティーが無効になっている場合は、以下のいずれかのコマンドを入力します。
     – Windows オペレーティング・システム:

     ```
     ISIM_HOME¥bin¥setupEnrole.exe install server:server_name
     ```

     – UNIX または Linux オペレーティング・システム:

     ```
     ISIM_HOME¥bin¥setupEnrole.exe install server:server_name
     ```

     server_name のデフォルトは、server1 です。

次のタスク

その他のトラブルシューティングを実行するか、検証タスクに戻ります。

デフォルト・ホストのポート番号の判別

同一のコンピューター上で WebSphere Application Server の複数インスタンスが実行されている場合は、ポート番号が別の値になっていることがあります。

始める前に

WebSphere Application Server が実行されており、WebSphere 管理コンソールが開始されていることを確認します。

手順

1. WebSphere 管理コンソールにログオンします。
2. 「**サーバー**」 > 「**アプリケーション・サーバー**」を選択します。
3. IBM Security Identity Manager アプリケーション・クラスター・メンバーをホストするサーバーをクリックします。
4. 「通信」セクションで、「**ポート**」リンクをクリックします。
5. WC_defaulthost ポート名の横にポート番号がリストされています。 このポート番号は、IBM Security Identity Manager との接続に使用されています。

次のタスク

その他のトラブルシューティングを実行するか、検証タスクに戻ります。

WSSession のキャッシュ・サイズの変更

WSSession キャッシュのキャッシュ制限は、WebSphere Application Server 管理コンソールで手動で変更できます。

手順

1. 管理コンソールから、「**リソース**」 > 「**オブジェクト・キャッシュ・インスタンス**」タブに移動します。
2. WSSession_cache のキャッシュ・サイズを変更します。

IIA:Runconfig updateRealmName.py が失敗する

お客様のセキュリティー・ドメイン・ユーザー・レルムがグローバル・セキュリティーを使用するように構成されている場合に、IIA:Runconfig updateRealmName.py が失敗します。

始める前に

WebSphere Application Server が実行されており、WebSphere 管理コンソールが開始されていることを確認します。

このタスクについて

このエラーは、指定されたユーザー・レジストリーが構成に含まれていないことが原因で発生します。セキュリティー・ドメインに対して、レルムが適切に構成されていません。グローバル・セキュリティーでフェデレーテッド・リポジトリーを使用するように構成するときに、このエラーを防止するには、以下の手順を実行します。

手順

1. 「セキュリティー・ドメイン」ページで、「**ユーザー・レルム (User Realm)**」を展開します。

2. 「**このドメイン用にカスタマイズする (Customize for this domain)**」をクリックします。
3. 「**レルム・タイプ**」フィールドで、「グローバル・セキュリティー」ページのレルム設定と一致する設定を選択します。
4. 構成プロセスを続行します。

ログ・ファイル

システム構成が完了すると、ログ・ファイルは以下のロケーションで見つけることができます。

ファイル名	説明およびロケーション
log.txt	WebSphere Application Server のインストール・ログ・ファイル。 システムの一時ディレクトリー内。
• isim_install.stdout • isim_install.stderr	IBM Security Identity Manager の標準出力およびエラー・ログ・ファイル。 システムのルート・ディレクトリー内。
• dbConfig.stdout • ldapConfig.stdout • dbUpgrade.stdout • ldapUpgrade.stdout • itim_installer_debug.txt • runConfigFirstTime.stdout • runConfig.stdout • setupEnrole.stdout • StartStopWas.stdout • itim_install_activity.log	ISIM_HOME¥install_logs ディレクトリーにあります。
• trace.log • msg.log	TIVOLI_COMMON_DIRECTORY¥CTGIM¥logs¥ ディレクトリーにあります。 Tivoli Common Directory は、ログ・ファイル、First Failure Data Capture データなどのすべての保守関連ファイルのためのセントラル・ロケーションです。
cfg_itim_mw.log	ミドルウェア構成ユーティリティー・ログ・ファイル。 システムの %TEMP% ディレクトリーにあります。

第 11 章 IBM Security Identity Manager のアンインストール

アンインストール・プログラムを使用して、IBM Security Identity Manager を削除します。

IBM Security Identity Manager アンインストール・プログラムは、以下のタスクを実行します。

- IBM Security Identity Manager インストール・プログラムが作成した *ISIM_HOME* ディレクトリー内のファイルをすべて除去します。 *ISIM_HOME*¥cert ディレクトリー内の証明書、および *ISIM_HOME*¥config¥keystore ディレクトリー内の itimKeystore.jceks 鍵ストア・ファイルを除去します。
- WebSphere Application Server 上の IBM Security Identity Manager サーバー用に作成されたすべての構成設定を消去します。
- 以下のコンピューターから IBM Security Identity Manager サーバーを除去します。

  単一サーバー構成:

  WebSphere Application Server がインストールされているコンピューター。

  クラスター構成:

  デプロイメント・マネージャーがインストールされているコンピューター。

  デプロイメント・マネージャーからアンインストールを行うことにより、クラスターは、IBM Security Identity Manager サーバーを使用できなくなります。デプロイされた IBM Security Identity Manager アプリケーション・ファイルは、IBM Security Identity Manager クラスター・メンバーから自動的に除去されます。

アンインストール・プロセスで除去されなかった残余 IBM Security Identity Manager ファイルをクリーンアップするために、アンインストール後に Windows オペレーティング・システムをリブートします。

除去されないもの

IBM Security Identity Manager サーバーのアンインストールでは、既存データベース・テーブルやディレクトリー・サーバー・スキーマおよびデータは変更されません。IBM Security Identity Manager ログ・ファイルは除去されません。

データベース・テーブル、ディレクトリー・サーバー・スキーマ、およびログ・ファイルの手動除去について詳しくは、『コンポーネントの手動除去』を参照してください。

サーバーのアンインストール

UNIX、Linux、または Windows の各オペレーティング・システムから IBM Security Identity Manager をアンインストールするには、IBM Security Identity Manager のアンインストール・プログラムを使用します。Windows オペレーティング・システムでは、Windows のコントロール・パネルから「プログラムの追加と削除」を使用することもできます。

始める前に

IBM Security Identity Manager サーバーをアンインストールする前に、以下のタスクを完了してください。

- 単一サーバー構成:
  - *ISIM_HOME*¥cert ディレクトリー内の証明書、および *ISIM_HOME*¥config¥keystore ディレクトリー内の itimKeystore.jceks 鍵ストア・ファイルをバックアップします。
  - WebSphere Application Server が実行中であることを確認します。
- クラスター構成:
  - *ISIM_HOME*¥cert ディレクトリー内の証明書、および *ISIM_HOME*¥config¥keystore ディレクトリー内の itimKeystore.jceks 鍵ストア・ファイルをバックアップします。
  - ノード・エージェントが実行されていること、およびデプロイメント・マネージャーも実行されていることを確認します。

このタスクについて

IBM Security Identity Manager の再インストールを予定している場合は、IBM Security Identity Manager アンインストール・プログラムを使用します。

- 単一サーバー構成:

  IBM Security Identity Manager サーバーがインストールされているコンピューターでコマンドを実行します。
- クラスター構成:

  最初に各クラスター・メンバーでコマンドを実行し、次にデプロイメント・マネージャーがインストールされているコンピューターでコマンドを実行します。

手順

1. 以下のコマンドを入力して、IBM Security Identity Manager をアンインストールします。 *ISIM_HOME*¥itimUninstallerData¥Uninstall_ITIM
2. アンインストール・ウィザードのパネルに情報を入力し、IBM Security Identity Manager サーバーをアンインストールすることを確認します。
3. アンインストール中に除去できなかった残余 IBM Security Identity Manager ファイルをクリーンアップするために、アンインストール後に Windows システムをリブートします。

次のタスク

- IBM Security Identity Manager サーバーが除去されていることを検証します。
- その他のコンポーネントを手動で除去します。

IBM Security Identity Manager サーバーがアンインストールされたことの検証

コンポーネントを除去する前に、IBM Security Identity Manager が除去されたことを検証する必要があります。

始める前に

アンインストール・ユーティリティーの実行が終了したことを確認します。

手順

1. *ISIM_HOME* ディレクトリーを調査して、すべての残りの IBM Security Identity Manager ディレクトリー、構成ファイル、およびログ・ファイルを除去します。
2. WebSphere 管理コンソールを開始してログインします。
3. ナビゲーション・ツリーから、ターゲット・ノードを特定し、「**アプリケーション**」>「**エンタープライズ・アプリケーション**」リンクをクリックします。

   アプリケーション・サーバーにインストールされているエンタープライズ・アプリケーションに関するリストが表示されます。

   ITIM という名前のアプリケーションがリストされている場合は、アンインストール・プロセスによって IBM Security Identity Manager サーバーが WebSphere Application Server から自動的に除去されていません。アプリケーションは手動で除去します。詳しくは、『WebSphere Application Server からの IBM Security Identity Manager サーバーの手動による除去』を参照してください。

次のタスク

その他のコンポーネントを手動で除去します。

コンポーネントの手動除去

アンインストール・ユーティリティーを実行した後、追加のコンポーネントを手動で停止または除去する必要があります。

WebSphere Application Server からの IBM Security Identity Manager サーバーの手動による除去

アンインストール・ユーティリティーによって IBM Security Identity Manager サーバーが除去されなかった場合は、手動で除去する必要があります。

始める前に

WebSphere 管理コンソールにログオンしていることを確認します。

手順

1. 単一サーバー構成またはクラスター構成で IBM Security Identity Manager・サーバーをアンインストールするには、「**アプリケーション**」>「**エンタープライズ・アプリケーション**」を選択します。
2. **ITIM** アプリケーションを選択します。
3. 「**停止**」をクリックします。
4. Tivoli Identity Manager アプリケーションが停止したら、再度 **ITIM** アプリケーションを選択します。
5. 「**アンインストール**」をクリックします。
6. ITIM.ear ディレクトリーが除去されたことを手動で確認します。
   a. 以下のアプリケーション・ディレクトリーをオープンします。
      - 単一サーバーおよびそれぞれのクラスター・メンバー

        WAS_PROFILE_HOME¥config¥cells¥*cellname*¥applications

        注:

        1) .ear ファイルが既に除去されている場合は、クラスター・メンバーにアプリケーション・ディレクトリーはありません。
        2) .ear ファイルも *WAS_PROFILE_HOME*¥config¥cells¥*cellname*¥installedApps¥ITIM.ear ディレクトリーから除去する必要があります。
      - デプロイメント・マネージャー

        WAS_NDM_PROFILE_HOME¥config¥cells¥*cellname*¥applications
   b. ITIM.ear ディレクトリーが存在する場合は、そのディレクトリーを除去します。

次のタスク

その他のコンポーネントを除去します。

IBM Security Identity Manager メッセージング・エンジンの停止および除去

IBM Security Identity Manager を完全にアンインストールするには、メッセージング・エンジンもアンインストールする必要があります。

始める前に

WebSphere 管理コンソールにログオンしていることを確認します。

手順

1. 単一サーバー構成またはクラスター構成で IBM Security Identity Manager サーバーのメッセージング・エンジンを停止して除去するには、「**サービス統合**」>「**バス**」を選択します。
2. 「**itim_bus**」をクリックします。

3. 「トポロジー」セクションで、「**メッセージング・エンジン**」をクリックします。

   単一サーバー・インストールの場合、 *nodename.servername*-itim_bus という名前のエンジンが表示されます。

   クラスター・インストールの場合、n+1 個のメッセージング・エンジンが表示されます。n は IBM Security Identity Manager クラスター・メンバーの数です。追加のメッセージング・エンジンが IBM Security Identity Manager メッセージング・クラスター用に使用されています。
4. 1 つ以上のメッセージング・エンジンを選択し、「**停止**」をクリックします。
5. WebSphere 管理コンソールから itim_bus 構成を除去します。
6. IBM Security Identity Manager データベースで、メッセージング・エンジンが使用するテーブルとスキーマを除去します。適合するコマンドについては、ご使用のデータベース・システムの資料を参照してください。

例

ファイル (*ISIM_HOME*/config/rdbms/dbtype/drop_itim_sib.ddl) に例があります。

次のタスク

追加のコンポーネントを除去します。

WebSphere Application Server からのその他の IBM Security Identity Manager 構成設定の除去

アンインストールを完了するには、WebSphere Application Server から他の IBM Security Identity Manager 構成設定を手動で除去する必要があります。

WebSphere 管理コンソールで次のタスクを実行します。

JDBC プロバイダーおよびデータ・ソースの除去

アンインストールを完了するには、WebSphere Application Server から JDBC プロバイダー構成の設定を手動で削除する必要があります。

始める前に

WebSphere 管理コンソールにログオンしていることを確認します。

手順

1. WebSphere 管理コンソールで、「**リソース**」 > 「**JDBC**」 > 「**JDBC プロバイダー**」をクリックします。
2. 有効範囲レベルとして、「**すべての有効範囲**」を選択します。
3. 名前が「ITIM XA」または「ITIM non-XA」で始まる JDBC プロバイダーを選択します。
4. 「**削除**」をクリックします。JDBC プロバイダー、およびそれらに関連付けられたデータ・ソースの両方が除去されます。
5. 「**保存**」をクリックして構成を保存します。

次のタスク

WebSphere Application Server から、追加の IBM Security Identity Manager 構成の設定を除去します。

JMS キュー接続ファクトリー、キュー、およびアクティベーション・スペックの除去

アンインストールを完了するには、WebSphere Application Server から JMS 構成の設定を手動で削除する必要があります。

WebSphere 管理コンソールを使用して、以下のタスクを実行します。

JMS キュー接続ファクトリーの除去:

アンインストールを完了するには、WebSphere Application Server から JMS キュー接続ファクトリー構成の設定を手動で削除する必要があります。

始める前に

WebSphere 管理コンソールにログオンしていることを確認します。

手順

1. 「**リソース**」 > 「**JMS**」 > 「**キュー接続ファクトリー**」をクリックします。
2. 有効範囲レベルとして、「**すべての有効範囲**」を選択します。
3. 「**ITIM キュー接続ファクトリー**」および「**ITIM 共有キュー接続ファクトリー**」を選択します。
4. 「**削除**」をクリックします。
5. 「**保存**」をクリックして構成を保存します。

次のタスク

以下に関する JMS 構成の設定を除去します。

- キュー
- アクティベーション・スペック

JMS キューの除去:

アンインストールを完了するには、WebSphere Application Server から JMS キュー構成の設定を手動で削除する必要があります。

始める前に

WebSphere 管理コンソールにログオンしていることを確認します。

手順

1. 「**リソース**」 > 「**JMS**」 > 「**キュー**」をクリックします。
2. 有効範囲レベルとして、「**すべての有効範囲**」を選択します。
3. 名前が「itim」で始まるキューをすべて選択します。
4. 「**削除**」をクリックします。

5. 「**保存**」をクリックして構成を保存します。

次のタスク

以下に関する JMS 構成の設定を除去します。

- キュー接続ファクトリー
- アクティベーション・スペック

JMS アクティベーション・スペックの除去:

アンインストールを完了するには、WebSphere Application Server から JMS アクティベーション・スペック構成の設定を手動で削除する必要があります。

始める前に

WebSphere 管理コンソールにログオンしていることを確認します。

手順

1. 「**リソース**」 > 「**JMS**」 > 「**アクティベーション・スペック**」をクリックします。
2. 有効範囲レベルとして、「**すべての有効範囲**」を選択します。
3. 名前が「itim」で始まるスペックをすべて選択します。
4. 「**削除**」をクリックします。
5. 「**保存**」をクリックして構成を保存します。

次のタスク

以下に関する JMS 構成の設定を除去します。

- キュー接続ファクトリー
- キュー

オブジェクト・キャッシュ・インスタンスの除去

アンインストールを完了するには、WebSphere Application Server からオブジェクト・キャッシュ・インスタンスを手動で削除する必要があります。

始める前に

WebSphere 管理コンソールにログオンしていることを確認します。

手順

1. 「**リソース**」 > 「**キャッシュ・インスタンス**」 > 「**オブジェクト・キャッシュ・インスタンス (Object cache instance)**」をクリックします。
2. 有効範囲レベルとして、「**すべての有効範囲**」を選択します。
3. 「**LdapCache**」および「**SecondaryLdapCache**」を選択します。
4. 「**削除**」をクリックします。
5. 「**保存**」をクリックして構成を保存します。

次のタスク

WebSphere Application Server から、追加の IBM Security Identity Manager 構成の設定を除去します。

セキュリティー設定の除去

アンインストールを完了するには、WebSphere Application Server からセキュリティー設定を手動で削除する必要があります。

始める前に

WebSphere 管理コンソールにログオンします。

手順

1. 「**グローバル・セキュリティー**」 > 「**Java 認証・承認 (Java Authentication and Authorizations)**」 > 「**J2C 認証データ**」をクリックします。
2. 「**itim_init**」 および 「**itim_jms**」 をクリックします。
3. 「**削除**」をクリックします。
4. 「**保存**」をクリックして構成を保存します。
5. 「**グローバル・セキュリティー**」 > 「**Java 認証・承認 (Java Authentication and Authorizations)**」 > 「**アプリケーション・ログイン**」をクリックします。
6. 「**ITIM**」 および 「**serviceLoginContext**」を選択します。
7. 「**削除**」をクリックします。
8. 「**保存**」をクリックして構成を保存します。

次のタスク

WebSphere Application Server から、追加の IBM Security Identity Manager 構成の設定を除去します。

コア・グループ・ポリシーの除去 (クラスター環境のみ)

このタスクはクラスター環境にのみ適用されます。アンインストールを完了するには、WebSphere Application Server からコア・グループ・ポリシーを手動で削除する必要があります。

始める前に

WebSphere 管理コンソールにログオンしていることを確認します。

手順

1. 「**サーバー**」 > 「**コア・グループ設定**」をクリックします。
2. 「**DefaultCoreGroup**」をクリックします。
3. 「**ポリシー**」をクリックします。
4. 名前が「itim_bus」で始まるすべてのポリシーを選択します。
5. 「**削除**」をクリックします。
6. 「**保存**」をクリックして構成を保存します。

次のタスク

WebSphere Application Server から、追加の IBM Security Identity Manager 構成の設定を除去します。

共用ライブラリーの除去

アンインストールを完了するには、WebSphere Application Server から共有ライブラリーを手動で削除する必要があります。

始める前に

WebSphere 管理コンソールにログオンしていることを確認します。

手順

1. 「**環境**」 > 「**共用ライブラリー**」をクリックします。
2. 有効範囲レベルとして、「**すべての有効範囲**」を選択します。
3. 「**ITIM_LIB**」を選択します。
4. 「**削除**」をクリックします。
5. 「**保存**」をクリックして構成を保存します。

次のタスク

WebSphere Application Server から、追加の IBM Security Identity Manager 構成の設定を除去します。

JVM クラスパスの除去

アンインストールを完了するには、WebSphere Application Server から JVM クラスパスを手動で削除する必要があります。

始める前に

WebSphere 管理コンソールにログオンしていることを確認します。

手順

1. 「**サーバー**」 > 「**WebSphere Application Server**」 > 「**サーバー名**」 > 「**Java およびプロセス管理**」 > 「**プロセス定義**」 > 「**Java 仮想マシン**」をクリックします。
2. クラスパス・フィールドから「***{ISIM_HOME}*/data**」を除去します。
3. 「**保存**」をクリックして構成を保存します。

次のタスク

WebSphere Application Server から、追加の IBM Security Identity Manager 構成の設定を除去します。

WebSphere 変数の除去

アンインストールを完了するには、WebSphere Application Server から WebSphere 変数を手動で削除する必要があります。

始める前に

WebSphere 管理コンソールにログオンしていることを確認します。

手順

1. 「**環境**」 > 「**共用ライブラリー**」をクリックします。
2. 有効範囲レベルとして、「**すべての有効範囲**」を選択します。
3. 「*ISIM_HOME*」および「ITIM_DB_JDBC_DRIVER_PATH」という名前を持つ変数すべてを選択します。
4. 「**削除**」をクリックします。
5. 「**保存**」をクリックして構成を保存します。

次のタスク

WebSphere Application Server から、追加の IBM Security Identity Manager 構成の設定を除去します。

その他のファイルまたはディレクトリーの手動除去

アンインストールを完了するには、残っている IBM Security Identity Manager ファイルを手動で削除する必要があります。

始める前に

アンインストール・ユーティリティーを実行して、すべてのコンポーネントを除去していることを確認します。

手順

1. アンインストール後にオペレーティング・システムを再始動します。
2. *ISIM_HOME* ディレクトリーを調べます。
3. 以下のファイルが残っている場合は除去します。
   - IBM Security Identity Manager ディレクトリー
   - 構成ファイル
   - ログ・ファイル
   - .dll ファイル
   - .so ファイル
   - .a ファイル
   - .jar ファイル
4. オペレーティング・システムを再始動します。

次のタスク

IBM Security Identity Manager を再インストールします。

第 12 章 IBM Security Identity Manager の再インストール

よりクリーンなインストールを行うために、再度 IBM Security Identity Manager インストール・プログラムを実行する前にデータベースおよび LDAP サーバーをクリーンアップできます。IBM Security Identity Manager メッセージング・エンジンが実行されていないことを確認します。アンインストールを行った後、再インストールを試みる前に Windows システムをリブートしてください。

IBM Security Identity Manager オブジェクトが Oracle Directory Server Enterprise Edition から除去されたことの確認

IBM Security Identity Manager を再インストールする前に、IBM Security Identity Manager の以前のスキーマ・オブジェクト、オブジェクト・クラス、およびその他の属性が、Oracle Directory Server Enterprise Edition から除去されていることを確認します。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権限を取得するか、代わりのユーザーにこのタスクを実行してもらうには、システム管理者に連絡してください。

手順

1. Oracle Directory Server Enterprise Edition の管理コンソールを開始します。
2. 「構成」タブで、IBM Security Identity Manager サフィックスを除去します。
3. 「ディレクトリー」タブで、以下のステップを実行します。
   a. IBM Security Identity Manager ドメインを除去します。
   b. 「**構成**」 > 「**プラグイン**」をクリックします。次に、参照整合性ポスト操作項目のプロパティーをオープンし、文字 `er` で始まるすべての属性を削除します。
4. ディレクトリー・サーバーを停止します。
5. *ldapServerInstance*¥config¥schema¥99user.ldif ファイルを開きます。次に、すべての IBM Security Identity Manager オブジェクト・クラス、および文字 `er` で始まる属性タイプを除去します。
6. ディレクトリー・サーバーを開始します。

次のタスク

次に、IBM Security Identity Manager をインストールすることができます。

第 2 部 オプション構成

ご使用のデプロイメントで、必要に応じて、オプションの構成タスクを実行できます。

第 13 章 オプションのポストインストール・タスク

IBM Security Identity Manager をインストールした後、必要に応じて、言語パックやアダプター・プロファイルをインストールしたり、クラスター構成を変更したりできます。

言語パックのインストール

IBM Security Identity Manager のインストール後、英語以外の言語をサポートする言語パックをインストールできます。

始める前に

IBM Security Identity Manager サーバーと関連プロセスが実行中であることの検証が完了していることを確認します。

IBM Security Identity Manager 言語パックのセットアップ・プログラムを実行する前に、IBM Security Identity Manager が必要とする Java ランタイム環境のバージョンにコマンド行からアクセスできることを確認します。

例えば、WebSphere Application Server に付属している Java のバージョンを使用できます。 次のコマンドを入力します。

```
WAS_HOME¥java¥bin¥java -fullversion
```

次の例のような応答を受け取ります。

```
java full version "1.5.0 IBM Windows 32 build pwi32devifx-20061107
(iFix 111765 SR3 + 111700)"
```

手順

1. 言語パック・インストーラー JAR ファイルをダウンロードします。
2. コマンド行モードを使用して、itimlp_setup.jar ファイルを使用して言語パックをインストールします。 例えば、コマンド・プロンプトで以下の言語パック・コマンドを入力します。

   ```
   WAS_HOME¥java¥bin¥java –jar itimlp_setup.jar
   ```

   注: Linux の場合は、必ず WebSphere Application Server と共に *WAS_HOME*/java/bin にインストールされる Java のバージョンを使用して、言語パックをインストールしてください。
   IBM Security Identity Manager 言語パックのセットアップ・プログラムが開始します。
3. 言語パックのインストールを完了するには、セットアップ・プログラム・ウィンドウに表示される指示に従います。
4. WebSphere Application Server を再始動して、上記の変更をアクティブ化します。

   a. WebSphere Application Server を停止します。

- Windows オペレーティング・システムでは、以下のコマンドを実行します。
  - *WAS_HOME*¥bin¥stopServer.bat *server_name*
- UNIX または Linux オペレーティング・システムでは、以下のコマンドを実行します。
  - *WAS_HOME*/bin/stopServer.sh *server_name*

  server_name の値は、WebSphere Application Server の名前です。例えば、server1 です。

b. WebSphere Application Server を始動するには、次のようにします。
- Windows オペレーティング・システムでは、以下のコマンドを実行します。
  - *WAS_HOME*¥bin¥startServer.bat *server_name*
- UNIX または Linux オペレーティング・システムでは、以下のコマンドを実行します。
  - *WAS_HOME*/bin/startServer.sh *server_name*

  server_name の値は、WebSphere Application Server の名前です。例えば、server1 です。

次のタスク

ブラウザーの言語を変更します。

注: システムから言語パックをアンインストールするには、*ISIM_HOME*¥timlp ディレクトリーに移動し、コマンド・プロンプトで次の言語パック・コマンドを入力します。

```
java –jar timlp_uninstall.jar
```

ブラウザーの言語表示の変更

言語パックが正常にインストールされたら、IBM Security Identity Manager インターフェースに表示される言語を変更できます。インターフェース言語を変更するには、ブラウザーの言語設定を変更します。

Internet Explorer の言語表示の変更

Internet Explorer バージョン 7.0 の言語設定を変更することで、IBM Security Identity Manager インターフェースに表示される言語を変更できます。

始める前に

適切な言語パックがインストールされていることを確認します。言語設定の変更は、IBM Security Identity Manager にログインする前に行います。

手順

1. 「**ツール**」 > 「**インターネット・オプション**」を選択します。
2. 「全般」タブで、「**言語**」をクリックします。
3. 「**追加**」をクリックします。

a. 追加する言語を選択します。

b. 「**OK**」をクリックします。

4. 言語を選択し、言語優先順位を設定します。 優先順位を上下に移動するには、ボタンを使用します。
5. 「**OK**」をクリックします。
6. 再度「**OK**」をクリックして、変更を保存します。

次のタスク

その他のポストインストール・タスクを実行します。

IBM Security Identity Manager を構成します。

Mozilla Firefox の言語表示の変更

Mozilla Firefox の言語設定を変更することで、IBM Security Identity Manager インターフェースに表示される言語を変更できます。

始める前に

適切な言語パックがインストールされていることを確認します。言語設定の変更は、IBM Security Identity Manager にログインする前に行います。

手順

1. 「**ツール**」 > 「**オプション**」を選択します。
2. 「コンテンツ」タブの「言語」セクションで、「**選択**」をクリックします。
3. 「追加する言語を選択」メニューで、言語を選択します。「**追加**」をクリックします。
4. 言語設定を設定します。 設定を上下に移動するには、ボタンを使用します。
5. 「**OK**」をクリックします。

次のタスク

その他のポストインストール・タスクを実行します。

アダプターおよびプロファイルのインストール

アダプターのインストールは、アダプター・プロファイル (サービス・タイプ) のインポートとアダプター・インストーラーの実行の 2 つのステップから構成されます。

IBM Security Identity Manager アダプターを使用すると、IBM Security Identity Manager を一連の異機種のリソースに接続できます。 ID をプロビジョニングできるのは、オペレーティング・システムやデータ・ストア、その他のアプリケーションなどのリソースです。

アダプターは、管理対象リソースと IBM Security Identity Manager サーバーの間のインターフェースを提供するプログラムです。アダプターは、アカウント管理のターゲット・プラットフォームでトラステッド仮想アドミニストレーターとして機能

します。例えば、アダプターは、アカウントを作成したり、アカウントを使用停止にしたり、アカウントの属性を変更したりできます。

IBM Security Identity Manager アダプターは、エージェント・ベースにすることも、エージェントレスにすることもできます。

エージェント・ベース・アダプター
管理対象リソースにインストールされるエージェント・アダプター・コードと、IBM Security Identity Manager サーバー・サイドにインストールされるプロファイルで構成されます。

エージェントレス・アダプター
IBM Tivoli Directory Integrator をホストしているシステムにインストールされたエージェントレス・アダプター・コードと IBM Security Identity Managerにインストールされたプロファイルで構成されます。アダプター・コードは、通信用に設計された管理対象リソースとは分離しています。

注: エージェントレス・アダプターの場合は、管理対象リソース上で SSH プロセスまたはデーモンがアクティブでなければなりません。

IBM Security Identity ManagerIBM Security Identity Manager インストール・プログラムは、常に次のエージェントレス・アダプター・サービス・タイプをインストールします。

- AIX プロファイル (UNIX アダプター)
- Solaris プロファイル (UNIX アダプター)
- HP-UX プロファイル (UNIX アダプター)
- Linux プロファイル (Linux アダプター)
- LDAP プロファイル (LDAP アダプター)

IBM Security Identity Manager インストール・プログラムは、リストされたサービス・タイプに対するアダプターをオプションでインストールします。 IBM Security Identity Manager のインストールの際にアダプターをインストールしないよう選択した場合や、アダプターが IBM Security Identity Managerにサービス・タイプとしてインストールされていない場合は、アダプターをインストールする追加のステップを実行する必要があります。

注: IBM Security Identity Manager インストール・プログラムによってインストールされた場合であっても、最新のアダプターおよびそのプロファイルをダウンロードおよびインストールしてください。

アダプターは次の場所で入手可能です (日本では異なる場合があります。日本における情報については営業担当員にお問い合わせください)。

- IBM パスポート・アドバンテージ Web サイト:

  http://www.ibm.com/software/sw-lotus/services/cwepassport.nsf/wdocs/passporthome

アダプターは圧縮ファイルとしてパッケージされています。この圧縮ファイルには、以下の共通エレメントが含まれています。

- サービス定義ファイル (アダプター・プロファイル)。これは、`WinLocalProfile.jar` などのプロファイルを含むアーカイブ Java (JAR) ファイルです。
- アダプターをインストールするための実行可能インストール・プログラム。
- リリース情報およびインストールと構成のガイドを含む PDF (Portable Document Format) 形式の資料。

アダプターのインストール

アダプター・インストーラーを開始する必要があります。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権限を取得するか、代わりのユーザーにこのタスクを実行してもらうには、システム管理者に連絡してください。

手順

1. 圧縮したアダプター・ファイルを開きます。
2. 「インストールと構成のガイド」を含む pdf ファイルを開きます。
3. インストールと構成のガイドに記載されているステップに従って、アダプターをインストールして構成します。

アダプター・プロファイルのインストール

IBM Security Identity Manager インストール・プロセス中にインストールしなかったアダプター・プロファイルをインストールおよびインポートできます。

始める前に

IBM Security Identity Manager サーバーと関連プロセスが実行中であることの検証が完了していることを確認します。

このタスクについて

注: Tivoli Identity Manager バージョン 5.0 からアップグレードしたが、Tivoli Identity Manager 5.0 プロファイルを使用して作成されたサービス・インスタンスを使用している場合は、サービスでグループを作成する前に、6.0 アダプターにアップグレードする必要があります。Tivoli Identity Manager 5.0 用のアダプターでは、グループ管理はサポートされません。

アダプターの役割について詳しくは、『*IBM Security Identity Manager アダプター*』を参照してください。

アダプター・プロファイルをインストールおよびインポートするには、次のようにします。

手順

1. 圧縮されたアダプター・ファイルを開いて解凍します。

2. アダプター・プロファイルを含む JAR ファイルを、IBM Security Identity Manager を実行しているコンピューター上の一時ディレクトリーに配置します。
3. 管理者として、Tivoli Identity Manager ユーザー・インターフェースを開きます。
4. 「**システムの構成**」 > 「**サービス・タイプの管理**」をクリックします。
5. 「サービス・タイプの管理」ウィンドウで、「**インポート**」をクリックします。
6. 「**サービス定義ファイル**」フィールドで、「**参照**」をクリックします。
7. アダプター・プロファイルを含む JAR ファイルを見つけて選択します。次に、「**開く**」をクリックします。
8. 「**OK**」をクリックします。
9. 「成功」ページで、「**クローズ**」をクリックします。

次のタスク

その他のポストインストール・タスクを実行します。

アダプター・ラベルの言語の変更

デフォルト言語が英語ではなく、アダプター・ラベルが英語で表示される場合は、ラベルの言語を変更できます。

始める前に

IBM Security Identity Manager と適切な言語パックがインストールされていることを確認します。

手順

1. 管理者として、IBM Security Identity Manager ユーザー・インターフェースを開きます。
2. 「**システムの構成**」 > 「**サービス・タイプの管理**」をクリックします。
3. 「サービス・タイプ」テーブルで「**インポート**」をクリックします。
4. 「**サービス定義ファイル**」フィールドで、「**参照**」をクリックします。
5. *ISIM_HOME*¥timlp ディレクトリーにある timx_agents.jar ファイルを特定し、「**開く**」をクリックします。
6. 「**OK**」をクリックします。
7. 「成功」ページで、「**クローズ**」をクリックします。

IBM Security Identity Manager のインストール後のクラスター構成の変更

ここでは、パフォーマンス上の理由から、IBM Security Identity Manager のインストール後にクラスターのメンバー数を拡張または縮小する方法について説明します。

クラスターの水平方向への拡張

既存のクラスターにメンバーを追加できます。

始める前に

クラスター構成に IBM Security Identity Manager がインストールされていることを確認します。

手順

1. 新規コンピューター上にプロファイルを作成し、新規ノードをセルに統合します。
   - カスタム・プロファイルを作成します。

     新規コンピューター上にカスタム・プロファイルを作成し、そのプロファイルをデプロイメント・マネージャー・セルに統合します。
   - 基本プロファイルを作成します。

     新規コンピューター上にベース・プロファイルを作成し、addNode コマンドを実行して、新規ノードをセルに統合します。詳しくは、『*WebSphere Application Server ノード・メンバーの手動での統合*』を参照してください。
2. 新規ノードに、IBM Security Identity Manager のクラスター・メンバーを作成します。 アプリケーション・クラスターとメッセージング・エンジン・クラスターの両方にクラスター・メンバーを作成するために、この手順を繰り返します。WebSphere 管理コンソールで、以下のステップを実行します。
   a. 「**サーバー**」 > 「**クラスター**」をクリックします。
   b. 次のウィンドウで、IBM Security Identity Manager のクラスター名をクリックします。
   c. 「**クラスター・メンバー**」をクリックし、「**新規**」をクリックします。
   d. セルに追加したノードのノード名を選択します。ノード名を入力します。「**次へ**」をクリックします。
   e. 「要約」ウィンドウを検証して、「**完了**」をクリックします。
   f. 変更を保存します。
3. クラスター・メンバーのインストールを選択し、新規コンピューター上で、IBM Security Identity Manager インストール・プログラムを実行します。
4. メッセージング・エンジンとクラスター・メンバーの関連付けに関するポリシーを設定します。 デプロイメント・マネージャー・ノードで以下のコマンドを実行します。
   - Windows オペレーティング・システムでは、以下のように入力します。

     ```
     ISIM_HOME¥bin¥runConfig.exe install
     ```
   - UNIX または Linux オペレーティング・システムでは、以下のように入力します。

     ```
     ISIM_HOME/bin/runConfig install
     ```
5. 新規クラスター・メンバーを開始します。
   a. 「**サーバー**」 > 「**クラスター**」をクリックします。
   b. クラスターを選択します。
   c. 「**クラスター・メンバー**」をクリックします。
   d. 新規メンバーを選択して、「**開始**」をクリックします。

次のタスク

その他のポストインストール・タスクを実行します。

クラスターの垂直方向への拡張

既存のクラスターの任意の場所にある既存のノードに、サーバーを追加できます。

始める前に

クラスター構成に IBM Security Identity Manager がインストールされていることを確認します。

このタスクについて

WebSphere Application Server を実行している物理コンピューターに、十分に活用されていないプロセッサー容量やメモリー容量がある場合は、既存のクラスターを垂直方向に拡張できます。

手順

1. クラスターが実行中であることを確認します。
2. WebSphere コンソールを使用して、既存の IBM Security Identity Manager アプリケーション用に定義されているクラスターにサーバーを追加します。
   WebSphere 管理コンソールで、以下のステップを実行します。
   a. 「**サーバー**」>「**クラスター**」>「**WebSphere Application Server クラスター**」をクリックします。
   b. 他のサーバーを追加するクラスターの名前をクリックします。アプリケーション・クラスターとメッセージング・クラスターのどちらでもかまいません。

      例えば、`ITIM Application Cluster`、`ITIM Messaging Cluster` などを選択します。
   c. 「構成」タブの「追加プロパティー」セクションで、「**クラスター・メンバー**」をクリックします。
   d. 「クラスター・メンバー」ページで、「**新規**」をクリックします。
   e. 以下のように必要な情報を指定して、新規サーバーを定義します。
      1) 「**メンバー名**」フィールドに名前を入力します。
      2) サーバーが稼働するノードを選択します。
      3) 「**重み**」フィールドに値を指定します。
      4) 「**固有の HTTP ポートを生成する**」チェック・ボックスが選択されていることを確認します。
      5) 「**メンバーの追加**」をクリックします。

      必要に応じ、別の名前とノードを使用して上記のステップを繰り返すことで、さらにサーバーを追加できます。
   f. ページ下部の表に、新規メンバーがリストされていることを確認します。「**次へ**」をクリックします。

g. 要約情報を確認し、「**完了**」をクリックします。 クラスター・メンバーの表に、新規メンバーがリストされていることを確認します。

h. WebSphere 構成を保存します。

WebSphere での変更をすべて実行したら、次のステップに進みます。

3. デプロイメント・マネージャー・ノードで以下のコマンドを実行します。

注: IBM Security Identity Manager を再始動する必要はありません。

- Windows オペレーティング・システムでは、以下のように入力します。

  ISIM_HOME¥bin¥runConfig.exe install

- UNIX または Linux オペレーティング・システムでは、以下のように入力します。

  ISIM_HOME/bin/runConfig install

4. WebSphere コンソールから、クラスター内のサーバーを始動できるようになりました。これらのサーバーは直ちに使用できます。

クラスターの縮小

既存のクラスターからクラスター・メンバーを除去できます。

始める前に

クラスター構成に IBM Security Identity Manager がインストールされていることを確認します。

手順

1. 除去するクラスター・メンバーのあるコンピューター上で IBM Security Identity Manager アンインストール・プログラムを実行します。 詳しくは、 189 ページの『第 11 章 IBM Security Identity Manager のアンインストール』を参照してください。
2. WebSphere 管理コンソールで、両方の IBM Security Identity Manager クラスターからクラスター・メンバーを削除します。

次のタスク

その他のポストインストール・タスクを実行します。

IBM Security Identity Manager を構成します。

インフォメーション・センターのファイルのダウンロードとインストール

IBM Security Identity Manager インフォメーション・センターは Web でインストールしますが、ダウンロードしてローカルで IBM Security Identity Manager サーバーにインストールすることもできます。

始める前に

Web で IBM Security Identity Managerを表示するには、以下のサイトにアクセスしてください。

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itim.doc/welcome.htm

手順

1. 以下の説明を印刷します。
2. インフォメーション・センターのこのインスタンスをクローズします。
3. 以下の Web サイトにアクセスします。

   http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0/isim60_infoctr.zip
4. com.ibm.isim.doc_6.0.zip ファイルをダウンロードします。このファイルに IBM Security Identity Manager インフォメーション・センターが含まれています。
5. com.ibm.isim.doc_6.0.zip ファイルを以下のディレクトリーに解凍します。

   WAS_HOME¥profiles¥*profilename*¥installedApps¥*cellname*¥ITIM.ear¥itim_iehs_help.war¥WEB-INF¥lib¥eclipse¥plugins
6. plugins ディレクトリーに以下のディレクトリーが追加されていることを確認します。

   com.ibm.isim.doc_6.0
7. WebSphere Application Server を再始動します。
8. インフォメーション・センターを開くには、以下の手順を実行します。
   a. IBM Security Identity Manager サーバーを再始動します。
   b. システム管理者 *isim manager* としてログインします。
   c. ブラウザーの「**アドレス**」フィールドに、以下のアドレスを 1 行で入力します。

      http://*hostname*:9080/itim/concepthelp/topic/com.ibm.itim.doc_6.0/ic-homepage.htm

      hostname の値は、IBM Security Identity Manager サーバーが実行されるコンピューターのホスト名です。
9. IBM Security Identity Manager インフォメーション・センターが開いたら、ブラウザーの「**ツール**」メニューを使用して、将来の利用のためにこのアドレスにブックマークを付けます。

次のタスク

インフォメーション・センターのみを再起動するには、以下の手順を実行します。

1. WebSphere Application Server で、「**アプリケーション**」 > 「**エンタープライズ・アプリケーション**」をクリックします。
2. インフォメーション・センター・アプリケーションを停止してから開始します。
3. IBM Security Identity Manager インフォメーション・センターのブラウザー・セッションをリフレッシュします。

Incremental Data Synchronizer のインストール

Incremental Data Synchronizer は別途インストールされるユーティリティーで、IBM Security Identity Manager が使用するディレクトリー・サーバーと IBM Security Identity Manager データベースとの間でデータおよびアクセス・コントロール項目を高速に同期化します。

Incremental Data Synchronizer は、IBM Security Identity Manager サーバーと同じコンピューターにインストールすることができますし、別のコンピューターにインストールすることもできます。パフォーマンス上の理由から、Incremental Data Synchronizer は、別個のコンピューターにインストールすることをお勧めします。

別のシステムへの Incremental Data Synchronizer のインストール

IBM Security Identity Manager サーバー がインストールされているコンピューター以外の別個のコンピューター上で Incremental Data Synchronizer をインストールおよび構成することが可能です。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権限を取得するか、代わりのユーザーにこのタスクを実行してもらうには、システム管理者に連絡してください。

新しいバージョンの IBM Security Identity Manager をインストールする場合は、このセクションの手順を実行して、両方のシステム上のファイルが確実に互換性を持つようにする必要があります。この場合は、プロパティー・ファイルをコピーした後に編集して、正しい値が確実に設定されるようにします。

IBM Security Identity Manager がインストールされているシステム上で WebSphere Application Server をアップグレードする場合は、Incremental Data Synchronizer がインストールされているシステムに新しい `JAR` ファイルをコピーする必要があります。または、Incremental Data Synchronizer がインストールされているシステムに新しい WebSphere Application Server シン・クライアント・ファイルをインストールする必要があります。

IBM Security Identity Managerがインストールされたシステム上で DB2 をアップグレードする場合は、Incremental Data Synchronizer がインストールされたシステムに新規の DB2 クライアントをインストールします。

このタスクについて

値 *synchronizer_computer* は、Incremental Data Synchronizer がインストールされているコンピューターです。

itim_computer は、IBM Security Identity Manager がインストールされているコンピューターです。この値は、IBM Security Identity Manager のインストール時に指定されます。この名前は `itim.ear` ファイルが存在する WebSphere Application Server インストール・ディレクトリーのディレクトリー・パスにあります。

手順

1. *ISIM_HOME* ディレクトリーを *itim_computer* から *synchronizer_computer* にコピーします。
2. WebSphere Application Server アプリケーション・クライアントを *synchronizer_computer* の *WAS_CLIENT_HOME* ディレクトリーにインストールします。
3. *synchronizer_computer* のオペレーティング・システムに対応する適切なクライアント・インストーラーを使用してください。アプリケーション・クライアントは、Incremental Data Synchronizer が WebSphere Application Server と通信できるようにするクライアント・ランタイムを提供します。 Incremental Data Synchronizer では、J2EE およびシン・クライアントのみが必要です。したがって、アプリケーション・クライアントのインストール時は、そのオプションのみを選択します。
4. app_ejb.jar、api_ejb.jar、および wf_ejb.jar ファイルを *itim_computer* の *WAS_HOME*/profiles/*profile_name*/installedApps/*cell_name*/itim.ear ディレクトリーから、*synchronizer_computer* の *ISIM_HOME*/lib ディレクトリーにコピーします。
5. *itim_computer* 上の *ISIM_HOME*/extensions/examples/apps/bin ディレクトリー内にある jaas_login_was.conf ファイルを *synchronizer_computer* 上の *ISIM_HOME*/data ディレクトリーにコピーします。
6. *synchronizer_computer* の *ISIM_HOME* ディレクトリーに logs という名前のディレクトリーを作成します。trace.log、trace1.log などのトレース・ログ・ファイルは、このディレクトリーに生成されます。
7. *synchronizer_computer* 上の *ISIM_HOME*/data/enroleLogging.properties ファイルを以下のように変更します。
   a. *ISIM_HOME*/logs ディレクトリーを指すよう handler.file.fileDir プロパティーを設定します。
   b. *ISIM_HOME*/logs ディレクトリーを指すよう handler.file.security.fileDir プロパティーを設定します。
8. ディレクトリー・サーバー・インスタンスでの *changelog* 機能を有効にします。 例えば、以下のとおりです。
   - IBM Tivoli Directory Server の場合は、インスタンス構成ツール (LDAP/sbin/idsxcfg) を使用して、ディレクトリー・インスタンスの *changelog* を構成します。
   - Sun Directory Server Enterprise Edition のディレクトリー管理コンソールの場合は、ディレクトリー・サーバー・インスタンスを開き、「**プラグイン**」セクションにある「**retro changelog plug-in**」を有効にします。これにより、Sun Directory Server Enterprise Edition ディレクトリー・サーバーの *changelog* 機能が有効になります。

     コマンドを使用して *changelog* 機能を有効にするには、次のように入力します。

     ```
     dsconf set-server-prop -h host -p port retro-cl-enabled:on
     ```
9. *itim_computer* での *changelog* 処理を有効にします。

a. *ISIM_HOME*/data ディレクトリー内の adhocreporting.properties ファイルを開きます。

b. 以下のオプションを設定します。

- changelogEnabled=true
- changelogBaseDN=*changelog_base_dn*

changelog_base_dn は、*changelog* エントリーをディレクトリー・サーバーに保持する基本 DN です。以下に例を示します。

```
changelogBaseDN=cn=changelog
```

10. オプション: *itim_computer* 上の *ISIM_HOME*/data/adhocreporting.properties ファイルでスキーマの制約を使用可能にするには、次のように入力します。

```
enableDeltaSchemaEnforcer=true
```

11. オプション: *ISIM_HOME*/data/adhocreporting.properties ファイルを変更して、*changelog* のプルーニングを有効にします。既に処理された *changelog* エントリーを除去する場合は、次のプロパティーを設定します。このプロパティーは、Sun Directory Server Enterprise Edition ディレクトリー・サーバーに固有のものです。 例えば、以下のとおりです。

```
enableChangelogPruning=true
```

12. *synchronizer_computer* の *ISIM_HOME*/data/enrole.properties ファイルを変更して、 *itim_computer* の WebSphere Application Server ブートストラップ・ポートを指すようにします。

```
Set enrole.appServer.url=iiop://itim_computer:2809
```

13. オプション: *synchronizer_computer* の *ISIM_HOME*/data/enRole.properties ファイルを変更して Incremental Data Synchronizer を調整します。*itim_computer* についても同じ値の変更が検討可能です。 これらのプロパティーについて詳しくは、*IBM Security Identity Manager パフォーマンス・チューニング・ガイド*を参照してください。

- enroleconnectionpool.initialpoolsize
- enroleconnectionpool.maxpoolsize
- enroleconnectionpool.prefsize
- enroleconnectionpool.incrementcount

14. データベースが DB2 であり、*itim_computer* 上にある場合は、 db2jcc.jar ファイルおよび db2jcc_license_cu.zip ファイルを *itim_computer* から *synchronizer_computer* 上の *ISIM_HOME*/lib ディレクトリーにコピーします。

注: これらの 2 つのファイルは、デフォルトで *synchronizer_computer* 上の *ISIM_HOME*/lib ディレクトリーに既に存在している場合があります。これらのファイルは、*itim_computer* からコピーできます。

15. オプション: 使用するデータベースが Oracle であり、*synchronizer_computer* 上にない場合は、*itim_computer* が使用する Oracle データベースに接続するために Oracle クライアントを *synchronizer_computer* にインストールします。

16. ojdbc14.jar ファイルが *synchronizer_computer* の *ISIM_HOME*/lib ディレクトリー内にあることを確認してください。

17. *synchronizer_computer* 上の *ISIM_HOME*/data ディレクトリー内にある enRoleDatabase.properties ファイルと enRoleLDAPConnection.properties フ

ファイルを変更し、IBM Security Identity Manager データベースおよびディレクトリー・サーバーの詳細を含めます。これらのファイルは、*itim_computer* からコピーできます。

18. sas.client.props ファイルを、 *synchronizer_computer* の *WAS_CLIENT_HOME*/properties ディレクトリーから *synchronizer_computer* の *ISIM_HOME*/data ディレクトリーにコピーします。sas.client.props ファイルは、 CSIv2 プロパティー・ファイルであり、Incremental Data Synchronizer が IBM Security Identity Manager に対する認証を保護するために必要です。
19. IBM Security Identity Manager で SSL がサポートされていない場合、または使用されていない場合は、*synchronizer_computer* 上にある *ISIM_HOME*/data/sas.client.props ファイル内の com.ibm.CSI.performTransportAssocSSLTLSSupported プロパティーに false が設定されていることを確認します。
20. 以下に示すように、*ISIM_HOME* ディレクトリーと *WAS_CLIENT_HOME* ディレクトリーを指すように *ISIM_HOME* および *WAS_HOME* スクリプト変数を設定します。
    a. *synchronizer_computer* 上の *ISIM_HOME*/bin/[*win*|*unix*] ディレクトリー内にある以下の 2 つのスクリプト・ファイルを編集します。これらのファイルのロケーションは、ご使用のオペレーティング・システムによって異なります。

       Microsoft Windows オペレーティング・システム

       - startIncrementalSynchronizerCMD_WAS.bat
       - startIncrementalSynchronizerUI_WAS.bat

       UNIX オペレーティング・システム

       - startIncrementalSynchronizerCMD_WAS.sh
       - startIncrementalSynchronizerUI_WAS.sh

    b. ユーザー・インターフェース・スクリプトを使用して、シンプルな Java Swing ユーザー・インターフェースを通じて増分同期を実行します。
    c. WebSphere Application Server で管理セキュリティーが使用不可に設定されている場合は、アンコメントし、スクリプトに記述されている適切な Java コマンドを使用してください。

同じシステムへの Incremental Data Synchronizer のインストール

IBM Security Identity Manager サーバー がインストールされている同一のコンピューター上で Incremental Data Synchronizer をインストールおよび構成することが可能です。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権限を取得するか、代わりのユーザーにこのタスクを実行してもらうには、システム管理者に連絡してください。

手順

1. *WAS_HOME*/*profile_name*/installedApps/*cell_name*/ITIM.ear 内にある app_ejb.jar、api_ejb.jar ファイルと wf_ejb.jar ファイルを *ISIM_HOME*/lib ディレクトリーにコピーします。
2. jaas_login_was.conf ファイルを *ISIM_HOME*/extensions/*version number*/examples/apps/bin ディレクトリーから *ISIM_HOME*/data ディレクトリーにコピーします。
3. ディレクトリー・サーバー・インスタンスでの *changelog* 機能を有効にします。 例えば、以下のとおりです。
   - IBM Tivoli Directory Server の場合は、インスタンス構成ツール (LDAP/sbin/idsxcfg) を使用して、ディレクトリー・インスタンスの *changelog* を構成します。
   - Sun Directory Server Enterprise Edition のディレクトリー管理コンソールから、ディレクトリー・サーバー・インスタンスを開き、「**プラグイン**」セクションにある「**retro changelog plugin**」を有効にします。このアクションにより、Sun One Directory Server の *changelog* 機能が有効になります。

     コマンドを使用して *changelog* 機能を有効にするには、次のように入力します。

     ```
     dsconf set-server-prop -h host -p port retro-cl-enabled:on
     ```
4. *itim_computer* での *changelog* 処理を有効にします。 *ISIM_HOME*/data ディレクトリー内の adhocreporting.properties ファイルを編集して、以下のオプションを設定します。
   - changelogEnabled=true
   - changelogBaseDN=*changelog_base_dn*

   changelog_base_dn は、*changelog* エントリーをディレクトリー・サーバーに保持する基本 DN です。以下に例を示します。

   ```
   changelogBaseDN=cn=changelog
   ```
5. オプション: 次の操作を行い、*itim_computer* の *ISIM_HOME*/data/adhocreporting.properties ファイルでスキーマの制約を可能にします。

   ```
   enableDeltaSchemaEnforcer=true
   ```
6. オプション: *ISIM_HOME*/data/adhocreporting.properties ファイルを変更して、*changelog* のプルーニングを有効にします。既に処理された *changelog* エントリーを除去する場合は、次のプロパティーを設定します。このプロパティーは、Sun Directory Server Enterprise Edition ディレクトリー・サーバーに固有のものです。 例えば、以下のとおりです。

   ```
   enableChangelogPruning=true
   ```
7. IBM Security Identity Manager によってどのデータベースが使用されるかに応じて、以下のいずれかのアクションを実行します。
   - DB2

     DB2 が itim_computer にある場合、 db2jcc.jar ファイルおよび db2jcc_license_cu.zip ファイルを SQLLIB/java ディレクトリーから

ISIM_HOME/lib ディレクトリーにコピーします。これら 2 つのファイルは、デフォルトで ISIM_HOME/lib ディレクトリーに既に存在している場合があります。

- Oracle

  ojdbc14.jar ファイルが *ISIM_HOME*/lib ディレクトリーに存在することを確認してください。

- Microsoft SQL Server

  sqljdbc.jar ファイルが *ISIM_HOME*/lib ディレクトリーに存在することを確認してください。

8. sas.client.props ファイルを *WAS_HOME* /profiles/*profile_name*/properties ディレクトリーから *ISIM_HOME*/data ディレクトリーにコピーします。*WAS_HOME* は、WebSphere Application Server がインストールされているディレクトリーです。sas.client.props ファイルは、 CSIv2 プロパティー・ファイルであり、Incremental Data Synchronizer が IBM Security Identity Manager に対する認証を保護するために必要です。
9. IBM Security Identity Manager で SSL がサポートされていない場合、*ISIM_HOME*/data/sas.client.props ファイルで com.ibm.CSI.performTransportAssocSSLTLSSupported プロパティーが false に設定されていることを確認します。
10. Incremental Data Synchronizer を実行するノードの ISIM_HOME/data/sas.client.props ファイル内のホスト名とブートストラップ・ポートの詳細を更新します。 例えば、以下のとおりです。

    ```
    com.ibm.CORBA.securityServerHost=localhost
    com.ibm.CORBA.securityServerPort=2809
    ```

    注: クラスター・セットアップを構成した場合のみ、sas.client.props ファイルを更新します。
11. Security Identity Manager サーバー と WebSphere Application Server のインストール済み環境を指すように *ISIM_HOME* および *WAS_HOME* スクリプト変数を設定します。
    a. *ISIM_HOME*/bin/[*win*|*unix*] ディレクトリー内にある以下の 2 つのスクリプト・ファイルを編集します。これらのファイルのロケーションは、ご使用のオペレーティング・システムによって異なります。

       Microsoft Windows オペレーティング・システム

       - startIncrementalSynchronizerCMD_WAS.bat
       - startIncrementalSynchronizerUI_WAS.bat

       UNIX オペレーティング・システム

       - startIncrementalSynchronizerCMD_WAS.sh
       - startIncrementalSynchronizerUI_WAS.sh

    b. ユーザー・インターフェース・スクリプトを使用して、シンプルな Java Swing ユーザー・インターフェースを通じて増分同期を実行します。
    c. WebSphere Application Server で管理セキュリティーが使用不可に設定されている場合は、それをアンコメントし、スクリプトに記述されている適切な Java コマンドを使用してください。

外部レポート・データを同期化するためのユーティリティー

レポート・データ同期化ユーティリティーは、ディレクトリー・サーバーと IBM Security Identity Manager データベース間でデータおよびアクセス・コントロール項目を同期化するユーティリティーです。このユーティリティーは、別個にインストールされます。同期化されたデータは、レポートの実行に使用されます。

このユーティリティーは、IBM Security Identity Manager と同じコンピューター上でも、別のコンピューター上でもインストール、構成、および実行することが可能です。このユーティリティーを別のコンピューターにインストールする場合、そのコンピューターには、WebSphere Application Server やディレクトリー・サーバー、データベースをインストールする必要はありません。

システム要件

レポート・データ同期化ユーティリティーには、次のシステム要件があります。

表 18. レポート・データ同期化ユーティリティーのシステム要件

オペレーティング・システム要件	プラットフォーム	パッチ、または保守の要件
Microsoft Windows Server 2008 Enterprise Edition	x86-64	Service Pack 1
Microsoft Windows Server 2008 Enterprise Edition	x86-32	Service Pack 1
Microsoft Windows Server 2008 Release 2 Enterprise Edition	x86-64	なし
Microsoft Windows Server 2003 Enterprise Edition	x86-32	Service Pack 2
Microsoft Windows Server 2003 Release 2 Enterprise Edition	x86-32	Service Pack 2
SUSE Linux Enterprise Server 11.0	x86-64	Service Pack 1
SUSE Linux Enterprise Server 11.0	x86-32	なし
Red Hat Enterprise Linux AS Version 4	x86-32	Update 6
Oracle Solaris 10	SPARC 64 ビット	なし
AIX バージョン 6.1	System P 64 ビット	Technology level 7、Service Pack 1

Java ランタイム環境 (JRE) の要件

レポート・データ同期化ユーティリティーは、IBM JRE または WebSphere JRE のいずれかを必要とします。以下の表は、JRE 要件およびサポートされるオペレーティング・システム間の関係を示しています。

表 19. レポート・データ同期化ユーティリティーの JRE 要件

オペレーティング・システム	32 ビット IBM JRE 1.6.0	32 ビット WebSphere 7.0 の JRE	64 ビット WebSphere 7.0 の JRE
Microsoft Windows Server 2008 Enterprise Edition Service Pack 1 x86-64			✓
Microsoft Windows 2008 Enterprise Edition Service Pack 1 x86-32		✓	

表 19. レポート・データ同期化ユーティリティーの JRE 要件 (続き)

オペレーティング・システム	32 ビット IBM JRE 1.6.0	32 ビット WebSphere 7.0 の JRE	64 ビット WebSphere 7.0 の JRE
Microsoft Windows Server 2008 Release 2 Enterprise Edition x86-64			✓
Microsoft Windows Server 2003 Service Pack 2 Enterprise Edition x86-32		✓	
Microsoft Windows Server 2003 Release 2 Service Pack 2 Enterprise Edition x86-32		✓	
SUSE Linux Enterprise Server 11.0 Service Pack 1 x86-64	✓		✓
SUSE Linux Enterprise Server 11.0 x86-32	✓	✓	
Red Hat Enterprise Linux AS Version 4 (Update 6、32 ビット)		✓	
Oracle Solaris 10 64 ビット			✓
AIX バージョン 6.1 Technology level 7、Service Pack 1、64 ビット	✓		✓

ハードウェア要件

レポート・データ同期化ユーティリティーには、次のハードウェア要件があります。

表 20. レポート・データ同期化ユーティリティーのハードウェア要件

システム・コンポーネント	最小値 *	推奨値 **
システム・メモリー (RAM)	2 ギガバイト	4 ギガバイト
プロセッサー速度	シングル 2.0 ギガヘルツの Intel または pSeries プロセッサー	デュアル 3.2 ギガヘルツの Intel または pSeries プロセッサー
ユーティリティーおよびログ・ファイル用のディスク・スペース	50 メガバイト	250 メガバイト
* 最小値: これらの値では、IBM Security Identity Manager の基本使用が可能になります。 ** 推奨値: 実稼働環境に適したさらに大きい値を使用する必要がある場合があります。		

レポート・データ同期化ユーティリティーのインストール

このセクションでは、ユーティリティーをインストールする方法を説明します。

始める前に

お客様の環境がシステム要件を満たしていることを確認します。

このタスクについて

レポート・データ同期化ユーティリティーをインストールするには、以下のステップを実行します。

手順

1. *ISIM_HOME*/bin ディレクトリーで isim_report_data_sync_utility.zip ファイルを見つけます。*ISIM_HOME* は IBM Security Identity Manager がインストールされているディレクトリーです。
2. *拡張暗号化標準* (AES) 暗号化アルゴリズムを使用する場合は、*ISIM_HOME*/data/keystore ディレクトリーで鍵ストア・ファイルを見つけます。
3. AES を使用する場合は、ユーティリティーのインストール、構成、実行を行う予定のコンピューターに圧縮ファイルと鍵ストア・ファイルをコピーします。
4. isim_report_data_sync_utility.zip ファイルを解凍します。
5. AES 暗号化アルゴリズムを使用する場合は、ユーティリティーを解凍したディレクトリーにアクセスし、解凍された data/keystore ディレクトリーに鍵ストア・ファイルをコピーします。
6. 必須: UNIX または Linux プラットフォームにユーティリティーをインストールする場合は、**SyncData.sh** ファイルに実行権限があることを確認します。以下のコマンドを実行します。

   ```
   chmod +x SyncData.sh
   ```

次のタスク

『レポート・データ同期化ユーティリティーの構成』を参照してください。

レポート・データ同期化ユーティリティーの構成

データ同期化ユーティリティーのインストール後に、このユーティリティーを構成する必要があります。

始める前に

- ユーティリティーを解凍したディレクトリーの下に、data ディレクトリーが存在することを確認します。すべてのプロパティー・ファイルは data ディレクトリー内にあります。
- IBM Security Identity Manager のインストール時に作成したデータベース・サーバーおよびディレクトリー・サーバーの資格情報を確認します。

手順

1. 220 ページの『レポート・データ同期化ユーティリティーのインストール』でユーティリティーを解凍したディレクトリーにアクセスします。
2. data ディレクトリーに移動します。
3. プロパティー・ファイルを変更します。 222 ページの表 21を参照してください。

表 21. 変更するプロパティー・ファイル

プロパティー・ファイル名	アクション
encryptionKey.properties	encryption.password プロパティーに適切な値を指定します。
enRole.properties	• 以下のプロパティーに適切な値を指定します。 – enrole.password.database.encrypted – enrole.password.ldap.encrypted – enrole.encryption.password.encoded • *Lightweight Directory Access Protocol* (LDAP) のデフォルトのテナント ID である enrole.defaulttenant.id を指定します。 • LDAP サーバー情報を以下のように指定します。 – enrole.ldapserver.root – enrole.ldapserver.home • 以下の暗号化プロパティーに適切な値を指定します。 – enrole.encryption.algorithm – enrole.encryption.passwordDigest • *Advanced Encryption Standard* (AES) 暗号化アルゴリズムを使用する場合は、enrole.encryption.keystore プロパティーの値を設定します。この値は、インストール手順の実行中に data/keystore ディレクトリーにコピーしたファイルの名前に設定してください。
enRoleDatabase.properties	以下のプロパティーに適切な値を指定します。 • database.db.type • database.db.owner • database.db.user • database.db.password • database.jdbc.driverUrl • database.jdbc.driver
enRoleLDAPConnection.properties	以下のプロパティーに適切な値を指定します。 • java.naming.provider.url • java.naming.security.principal • java.naming.security.credentials
enRoleLogging.properties	• トレース・ファイルおよびログ・ファイルの生成先のディレクトリーを指定します。 – handler.file.fileDir – handler.file.security.fileDir – handler.ffdc.baseDir – handler.ffdc.fileCopy.filesToCopy
ReportDataSynchronization.properties	以下のプロパティーに適切な値を指定します。 • report.data.synchronization.utility.server.name **注:** このプロパティーに値を指定しない場合、ホスト名がサーバー名として使用されます。 • report.data.synchronization.utility.user.name

4. オプション: データ同期化に関連する追加プロパティーの変更を検討し、デプロイされた IBM Security Identity Manager 環境に指定する値と類似した値を指定してください。
5. オプション: -JAVA_HOME オペレーティング・システム環境変数を、Java ランタイム環境のロケーションに設定します。

次のタスク

レポート・データ同期化ユーティリティーを実行します。*IBM Security Identity Manager* インフォメーション・センター の「管理」>「レポート管理」>「データ同期化」>「外部レポート・データの同期化のユーティリティー」>「レポート・データ同期ユーティリティーの実行」を参照してください。

第 14 章 外部ユーザー・レジストリーを使用した認証のための再構成

外部ユーザー・レジストリーを使用した認証をサポートするようにミドルウェアを再構成することが可能です。

IBM Security Identity Manager は、2 つの異なるデプロイメント構成を通じた認証をサポートしています。デフォルトの構成では、IBM Security Identity Manager が提供するカスタム・ユーザー・レジストリーが使用されます。 IBM Security Identity Manager で提供されないユーザー・レジストリーを使用するようにデプロイメントを構成することも可能です。 IBM Security Identity Manager で提供されないユーザー・レジストリーは、*外部ユーザー・レジストリー* と呼ばれます。

このセクションでは、外部ユーザー・レジストリーをサポートするように、IBM Security Identity Manager で使用されるミドルウェアを再構成する方法について説明します。

注: このセクションを利用するのは、デフォルトのカスタム・レジストリーを使用するように IBM Security Identity Manager をインストールしたが、外部ユーザー・レジストリーに切り替える場合のみにしてください。外部ユーザー・レジストリーを使用するように IBM Security Identity Manager をインストールしたが、インストール後の構成を完了していない場合は、このセクションを利用しないでください。その代わりに、 166 ページの『認証用の外部ユーザー・レジストリーに対するインストール後の構成』のインストール後のタスクを実行してください。

IBM Security Identity Manager が WebSphere Application Server セキュリティーを使用する方法を確認するには、 8 ページの『WebSphere セキュリティー構成』を参照してください。

再構成タスクを以下に示します。

1. 必要なユーザーをユーザー・レジストリーに追加します。
2. WebSphere セキュリティー・ドメインを再構成します。
3. 管理者アカウントのアクセス権限を検証します。

再構成タスクを実行するには、『外部ユーザー・レジストリーへの必要なユーザーの追加』に進んでください。

外部ユーザー・レジストリーへの必要なユーザーの追加

必要なユーザーを外部ユーザー・レジストリーに追加する必要があります。

このタスクについて

IBM Security Identity Manager では、2 つのアカウントが存在する必要があります。

表 22. 必要なユーザーのデフォルトのアカウント名

アカウント使用	デフォルトのアカウント名
デフォルトの管理ユーザー	ITIM Manager
デフォルトのシステム・ユーザー	isimsystem

アカウントごとに異なるアカウント名を使用することを選択できます。既存の外部ユーザー・レジストリーで管理ユーザー・アカウント名またはシステム・ユーザー・アカウント名を既に使用している場合は、異なるアカウント名を使用するのがよいでしょう。アカウント名のスペースがオペレーティング・システムでサポートされていない場合は、管理ユーザーに異なるアカウント名を使用するのがよいでしょう。例えば、ユーザー・レジストリーが Linux システム上にある場合は、ITIM Manager ではなく、itimManager というアカウント名を指定するのがよいでしょう。

ユーザーを作成する正確なステップは、ユーザー・レジストリーのタイプに応じて異なります。必要なユーザーを IBM Tivoli Directory Server レジストリーに追加するには、**ldapadd** コマンドを使用します。

コマンド行を使用して、以下のコマンドを発行します。

```
ldapadd -D Bind DN -w Bind PW -p Port -f filename
```

例:

```
ldapadd -D cn=root -w root -p 389 -f filename
```

ここで、*filename* には、以下の詳細情報が含まれます。

```
dn:cn=ITIM Manager,dc=com
objectclass:person
objectclass:inetOrgPerson
cn:System Administrator
sn:Administrator
uid:ITIM Manager
userpassword:secret

dn:cn=isimsystem,dc=com
objectclass:person
objectclass:inetOrgPerson
cn:isimsystem
sn:isimsystem
uid:isimsystem
userpassword:isimsystem
```

別の方法として、IBM Tivoli Directory Server Web 管理ツールを使用して必要なユーザーを追加する方法を以下の手順で説明します。

手順

1. IBM Tivoli Directory Server Web 管理ツールにログオンします。
2. ナビゲーション・ツリーから「**ディレクトリー管理**」>「**項目の追加**」をクリックして、「項目の追加」ページの「オブジェクト・クラスの選択」タブを開きます。
3. 「**構造オブジェクト・クラス**」リストから「**inetOrgPerson**」を選択します。

4. 「**次へ**」をクリックして、「補助オブジェクト・クラスの選択」タブを開きます。
5. 「補助オブジェクト・クラスの選択」タブで「**次へ**」をクリックして、「必要な属性」タブを開きます。
6. 以下の属性の値を「必要な属性」タブで指定します。
   - **相対 DN**
   - **親 DN**
   - **cn**
   - **sn**

   デフォルトの管理ユーザー ID (uid) ITIM Manager とデフォルトのシステム・ユーザー ID (uid) isimsystem を使用することも、別の uid を指定することもできます。以下の表は、デフォルトの管理ユーザー ID、またはデフォルトのシステム・ユーザー ID を使用するときの、必要な属性のエントリーの例を示しています。

表 23. デフォルトの管理ユーザーおよびデフォルトのシステム・ユーザーのアカウントに必要な名前属性のエントリーの例

属性	デフォルトの管理ユーザーの値の例	デフォルトのシステム・ユーザーの値の例
相対 DN	cn=ITIM Manager	cn=isimsystem
親 DN	dc=com	dc=com
cn	システム管理者	isimsystem
sn	Administrator	isimsystem

7. 「**次へ**」をクリックして、「オプションの属性」タブを開きます。
8. 以下の属性の値を「オプションの属性」タブで指定します。
   - **uid**
   - **userPassword**

   例えば、以下の表に示すオプションの属性値を指定します。

表 24. デフォルトの管理ユーザーおよびデフォルトのシステム・ユーザーのアカウントのオプションの属性値

属性	デフォルトの管理ユーザーの値の例	デフォルトのシステム・ユーザーの値の例
uid	ITIM Manager	isimsystem
userPassword	ITIM Manager アカウントのデフォルトのパスワードは、 secret です。任意のパスワードを指定できます。	isimsystem アカウントのデフォルトのパスワードは、 secret です。任意のパスワードを指定できます。

9. 「**終了**」をクリックします。

タスクの結果

項目が LDAP サーバーに追加されます。

次のタスク

『WebSphere セキュリティー・ドメインの再構成』に進みます。

WebSphere セキュリティー・ドメインの再構成

WebSphere セキュリティー・ドメインを IBM Security Identity Manager 用に再構成する必要があります。

以下の構成タスクを実行します。

1. 『WebSphere ユーザー・レルム・タイプの再構成』
2. 230 ページの『プロパティー・ファイルの更新』
3. 231 ページの『システム・ユーザーの役割のマップ解除』
4. 232 ページの『システム・ユーザーの役割の再マップ』
5. 233 ページの『システム・ユーザーのサービス・バス・ユーザー役割の再マップ』
6. 234 ページの『管理者アカウントのアクセス権限の検証』

『WebSphere ユーザー・レルム・タイプの再構成』に進みます。

WebSphere ユーザー・レルム・タイプの再構成

WebSphere セキュリティー・ドメインのユーザー・レルム・タイプを再構成する必要があります。

始める前に

IBM Security Identity Manager のインストール時に、インストール・ウィザードによって `ISIMSecurityDomain` と呼ばれるデフォルトの WebSphere セキュリティー・ドメインが作成されています。カスタム・レジストリーからスタンドアロン LDAP レジストリーに切り替えるには、このドメインの構成設定を変更する必要があります。

手順

1. スタンドアロン LDAP レジストリーを使用するように `ISIMSecurityDomain` を変更するには、WebSphere Application Server 管理コンソール にログオンします。
2. ISIM エンタープライズ・アプリケーションを停止します。
3. 「**セキュリティー**」>「**セキュリティー・ドメイン**」をクリックします。
4. 「**ISIMSecurityDomain**」リンクをクリックします。
5. 「ISIMSecurityDomain」ページの「**セキュリティー属性**」セクションで、「**ユーザー・レルム**」を展開します。
6. 「**このドメイン用にカスタマイズする (Customize for this domain)**」が選択されていることを確認します。
7. 「**レルム・タイプ**」リストから「**スタンドアロン LDAP レジストリー**」を選択します。

8. 「**構成**」をクリックして「スタンドアロン LDAP レジストリー」ページを開きます。
9. 「**レルム名を指定 (Provide a realm name)**」を選択して、レルム名を入力します。例えば、`newRealm` です。
10. 「**LDAP サーバーのタイプ**」リストから LDAP サーバーを選択します。例えば、**IBM Tivoli Directory Server** です。
11. 以下のフィールドに LDAP 構成プロパティーの値を指定します。
    - **ホスト**
    - **ポート**
    - **基本識別名 (DN)**
    - **バインド識別名 (DN)**
    - **バインド・パスワード**

    例えば、以下の表から IBM Tivoli Directory Server のプロパティー値を指定します。

表 25. IBM Tivoli Directory Server の LDAP 構成

構成プロパティー	サンプル値
ホスト	*your_host_name*
ポート	389 (または、ご使用のディレクトリー・サーバーが listen しているポート)
基本識別名 (DN)	*c=us*
バインド識別名 (DN)	*cn=root*
バインド・パスワード	*your_current_password*

12. 「**接続のテスト**」をクリックして接続情報を検査します。
13. 「スタンドアロン LDAP レジストリー」ページの「**追加プロパティー**」セクションで、「**拡張 Lightweight Directory Protocol (LDAP) ユーザー・レジストリーの設定 (Advanced Lightweight Directory Protocol (LDAP) user registry settings)**」リンクをクリックします。
14. 「拡張 Lightweight Directory Protocol (LDAP) ユーザー・レジストリーの設定 (Advanced Lightweight Directory Access Protocol (LDAP) user registry settings)」ページの「**一般プロパティー**」セクションで、「**ユーザー・フィルター**」フィールドの既存の値を `(&(uid=%v)(objectclass=inetOrgPerson))` に置き換えます。
15. 「**OK**」をクリックし、「**保存**」をクリックして変更を保存します。
16. 必要に応じて (ログインまたはパスワードを変更した場合)、Java 2 Connector (J2C) グローバル別名定義を「**isimsystem**」ユーザーの「**リソース**」>「**リソース・アダプター**」から更新してください。
17. WebSphere Application Server を停止します。

次のタスク

230 ページの『プロパティー・ファイルの更新』に進みます。

プロパティー・ファイルの更新

新規レルム・タイプとすべての変更をシステム・ユーザー構成に反映させるには、IBM Security Identity Manager のプロパティー・ファイルを更新します。

このタスクについて

WebSphere セキュリティー・ドメインの再構成時に、新規レルム名を指定しました。その新規レルム名で IBM Security Identity Manager のプロパティー・ファイルを更新する必要があります。

必須ユーザーを外部ユーザー・レジストリーに追加した際に、IBM Security Identity Manager システム・ユーザーのアカウント名またはパスワードを指定しました。必要に応じて、以前にカスタム・レジストリーで使用した別の値を指定することもできます。この場合は、IBM Security Identity Manager 構成ユーティリティーを実行する必要があります。

手順

1. ユーザーの追加時にシステム・ユーザーのアカウント名またはパスワードを変更した場合は、構成を更新してください。

   注: アカウント名もパスワードを変更しなかった 場合は、このステップをスキップしてください。

   a. 以下のとおり、ご使用のオペレーティング・システム用のコマンドを使用します。
      - Windows オペレーティング・システム:

        ISIM_HOME¥bin¥runConfig.exe
      - UNIX または Linux オペレーティング・システム:

        ISIM_HOME/bin/runConfig

   b. 「セキュリティー」タブをクリックします。

   c. 「Identity Manager システム・ユーザー」フィールドおよび「Identity Manager システム・ユーザー・パスワード」フィールドで、IBM Security Identity Manager システム・ユーザーおよびシステム・ユーザー・パスワードの新規の値を指定します。

   注: WebSphere に接続できないことを示す **runConfig** の警告は無視してください。WebSphere が停止しているため、この警告は予想されています。

2. ご使用の IBM Security Identity Manager 環境で、enRole.properties ファイルを編集のために開きます。

   例えば、UNIX システムまたは Linux システムでは、ファイル・パスは /opt/IBM/isim/data/enRole.properties です。

3. デフォルトのレルム名をリセットして、スタンドアロン LDAP レジストリー用に指定したレルム名と一致するようにします。

   設定例:

表 26. enRole.properties でのレルム名の設定例

元の設定	enrole.appServer.realm=itimCustomRealm

表 26. enRole.properties でのレルム名の設定例 (続き)

新しい設定	enrole.appServer.realm=*your_realm_name* 以下に例を示します。enrole.appServer.realm=newRealm

4. ファイルを保存します。
5. WebSphere Application Server を始動します。

次のタスク

『システム・ユーザーの役割のマップ解除』に進みます。

システム・ユーザーの役割のマップ解除

システム・ユーザーの役割の WebSphere マップを除去します。

このタスクについて

IBM Security Identity Manager は、WebSphere では ITIM と呼ばれるエンタープライズ・アプリケーションとして稼働します。ITIM アプリケーションの構成には、IBM Security Identity Manager システム・ユーザーが使用する役割のマッピングが含まれます。ミドルウェアで外部ユーザー・レジストリーをサポートするための再構成の一部として、役割を再マップする必要があります。このタスクでは、既存の役割をマップ解除する必要があります。

デフォルトの IBM Security Identity Manager システム・ユーザーは isimsystem です。ご使用のデプロイメントでは、初期インストール時に指定した名前によっては、別の名前を使用している場合があります。

手順

1. WebSphere 管理コンソールにログオンします。
2. 「**アプリケーション**」 > 「**アプリケーション・タイプ**」 > 「**WebSphere Enterprise Application**」 > 「**ITIM**」を選択します。
3. 「構成」タブの「詳細プロパティー」セクションに進み、「**ユーザー RunAs ロール**」をクリックします。
4. 「ユーザー RunAs ロール」パネルで、「**ITIM_SYSTEM**」チェック・ボックスを選択して「**除去**」をクリックします。

   このアクションで、システム・ユーザー名が ITIM_SYSTEM 役割から除去されます。
5. 「**OK**」をクリックしてから「**保存**」をクリックします。
6. 「**アプリケーション**」 > 「**アプリケーション・タイプ**」 > 「**WebSphere Enterprise Applications**」 > 「**ITIM**」の順でページに戻ります。
7. 「構成」タブの「詳細プロパティー」セクションに進み、「**ユーザー/グループへのセキュリティー・ロールのマッピング**」をクリックします。
8. 「**ITIM_SYSTEM**」チェック・ボックスを選択して「**ユーザーのマップ**」をクリックします。

9. 「ユーザー/グループのマップ (Map users/groups)」ウィンドウの「**選択**」リストからシステム・ユーザー名を選択します。「**除去**」をクリックして、システム・ユーザー名を「**使用可能**」リストに移動します。

   デフォルトのシステム・ユーザー名は `isimsystem` です。
10. 「**OK**」を 2 回クリックして、まず「ユーザー/グループのマップ (Map users/groups)」ウィンドウを閉じ、次に「ユーザー/グループへのセキュリティー・ロールのマッピング」ウィンドウを閉じます。変更をマスター構成に保存します。

次のタスク

『システム・ユーザーの役割の再マップ』に進みます。

システム・ユーザーの役割の再マップ

システム・ユーザーの役割の WebSphere マップを除去します。

手順

1. WebSphere 管理コンソールにログインします。
2. 「**アプリケーション**」 > 「**アプリケーション・タイプ**」 > 「**WebSphere Enterprise Application**」 > 「**ITIM**」を選択します。
3. 「構成」タブに進んで、「詳細プロパティー」セクションに進み、「**ユーザー/グループへのセキュリティー・ロールのマッピング**」をクリックします。
4. 「**ITIM_SYSTEM**」チェック・ボックスを選択して「**ユーザーのマップ**」をクリックします。
5. 「ユーザー/グループのマップ (Map users/groups)」ウィンドウで「**検索ストリング**」フィールドに進み、ご使用のシステム・ユーザーのレジストリー項目を検索するストリング **isimsystem** を入力し、「**検索**」をクリックします。

   例えば、ご使用のシステム・ユーザーがデフォルトの `isimsystem` である場合は、`*isimsystem*` というストリングを入力します。

   検索結果は、*isimsystem* ユーザー項目の構文、またはご使用のスタンドアロン LDAP レジストリーの DN の構文を反映したものでなければなりません。例えば、結果は *cn=isimsystem, c=us* などです。
6. 検索結果は「**使用可能**」リストに表示されます。項目 (この例では、*cn=isimsystem, c=us*) を選択します。「**追加**」の矢印ボタンをクリックして、ユーザーを「**選択**」リストに移動します。
7. 「**OK**」を 2 回クリックして、まず「ユーザー/グループのマップ (Map users/groups)」ウィンドウを閉じ、次に「ユーザー/グループへのセキュリティー・ロールのマッピング」ウィンドウを閉じます。変更をマスター構成に保存します。
8. 「**アプリケーション**」 > 「**アプリケーション・タイプ**」 > 「**WebSphere Enterprise Applications**」 > 「**ITIM**」の順に戻ります。
9. 「構成」タブの「詳細プロパティー」セクションに進み、「**ユーザー RunAs ロール**」をクリックします。

10. 「ユーザー RunAs ロール」ウィンドウで、「**ユーザー名**」フィールドにシステム・ユーザー名を入力し、「**パスワード**」フィールドにシステム・ユーザー・パスワードを入力します。

    ユーザー ID は、前に使用した短縮名 (例えば、*cn=isimsystem, c=us*) にする必要があります。この場合は、ユーザー名は isimsystem です。
11. 「**ITIM_SYSTEM**」チェック・ボックスを選択して、「**適用**」をクリックします。
12. ユーザー名 *isimsystem* が、「**ITIM_SYSTEM**」の「役割」項目の「**ユーザー名**」列に現在リストされていることを確認します。
13. 「**OK**」クリックし、「**保存**」をクリックします。

次のタスク

『システム・ユーザーのサービス・バス・ユーザー役割の再マップ』に進みます。

システム・ユーザーのサービス・バス・ユーザー役割の再マップ

サービス・バス・ユーザー役割の WebSphere 役割構成を再マップします。

手順

1. 「**サービス統合**」>「**バス**」で、itim_bus リソースの「**セキュリティー**」列にある「**使用可能**」リンクをクリックします。
2. 「**バス itim_bus のセキュリティー**」ページの「**許可ポリシー**」で、「**バス・コネクター役割を持つユーザーおよびグループ (Users and groups in the bus connector role)**」をクリックします。
3. 「**バス・コネクター・ロールを持つユーザーおよびグループ**」ページで、システム・ユーザーを除去します。例えば、isimsystem です。
4. 同じページで、「**新規**」をクリックして、外部ユーザー・レジストリー・リポジトリーからシステム・ユーザー (例えば、isimsystem) を追加します。
5. 「SIB セキュリティー・リソース」ウィザードで以下を実行します。
   a. 「ユーザーまたはグループの検索」ページで、「**検索パターン**」フィールドにアスタリスク「*」を入力して、「**次へ**」をクリックします。
   b. 「ユーザーおよびグループの選択」ページで、システム・ユーザーを選択します。例えば、isimsystem です。「**次へ**」をクリックします。
   c. 「要約」ページで、構成を確認して「**完了**」をクリックします。
6. 「**バス itim_bus のセキュリティー**」に戻り、「**許可ポリシー**」で「**デフォルトのアクセス役割の管理 (Manage default access roles)**」をクリックします。
7. 「**デフォルトのアクセス役割 (Default access roles)**」ページで、「**デフォルト・アクセス**」を展開してシステム・ユーザー (isimsystem) を選択し、「**除去**」をクリックします。
8. 「**バス itim_bus のセキュリティー**」ページで、「**追加**」をクリックします。
9. 外部ユーザー・レジストリー・リポジトリーからシステム・ユーザーを追加します。「SIB セキュリティー・リソース」ウィザードで以下を実行します。

a. 「ユーザーまたはグループの検索」ページで、「**検索パターン**」フィールドにアスタリスク「*」を入力して、「**次へ**」をクリックします。
b. 「ユーザーおよびグループの選択」ページで、システム・ユーザーを選択します。例えば、`isimsystem` です。「**次へ**」をクリックします。
c. 「役割タイプの選択 (Select Role Types)」ページで、「**送信者**」、「**ブラウザー**」、「**受信側**」、および「**作成者**」を選択します。
d. 「要約」ページで、構成を確認して「**完了**」をクリックします。

10. IBM Security Identity Manager アプリケーションのターゲット・デプロイメントの状況を「**開始**」に設定します。
11. 変更を保存します。
12. IBM Security Identity Manager アプリケーションを開始します。

タスクの結果

『管理者アカウントのアクセス権限の検証』に進みます。

管理者アカウントのアクセス権限の検証

管理者アカウントが正しく構成されていることを検証します。

このタスクについて

IBM Security Identity Manager 管理者が、外部ユーザー・レジストリーを使用した認証によって正常にログインできることを確認します。

手順

1. IBM Security Identity Manager 管理コンソールにログオンします。

   デフォルト URL にアクセスします。ここで、`hostIP` は IBM Security Identity Manager を実行するサーバーの IP アドレスまたは完全修飾ドメイン名です。

   `http://hostIP:9080/itim/console`
2. 外部ユーザー・レジストリーに必須ユーザーを追加したときに指定した管理者名を使用してください。

   デフォルトの管理者アカウントは `ITIM Manager` です。
3. 管理者アカウント用に指定したパスワードを入力します。

   デフォルト・パスワードは、`secret` です。

タスクの結果

管理者ユーザー用に使用したパスワードを指定して正常にログインできる場合は、LDAP ユーザー・レジストリーが IBM Security Identity Manager の外部認証ユーザー・レジストリーとして正常に構成されています。

第 3 部 アップグレード

IBM Security Identity Manager は、データ・マイグレーションと共にインプレース・アップグレードおよび別個のシステム・アップグレードを行うことをサポートしています。

第 15 章 IBM Security Identity Manager のアップグレード

IBM Security Identity Manager インストール・プログラムは、以前のバージョンの Tivoli Identity Manager がインストールされているコンピューターをアップグレードします。設定を保存または再カスタマイズするには、いくつかの手動ステップが必要です。この節では、単一サーバーおよびクラスターの構成の両方のアップグレードについて説明します。

IBM Security Identity Manager インストール・プログラムは、以下からのアップグレードをサポートしています。

- Tivoli Identity Manager バージョン 5.0
- Tivoli Identity Manager バージョン 5.1

アップグレード・プロセスの説明

アップグレード・プロセスの主要なタスクは、以下のとおりです。

1. オペレーティング・システムをこのリリースの IBM Security Identity Manager がサポートするレベルにマイグレーションします。システムに必要なフィックスパックまたはパッチがインストールされていることを確認します。オペレーティング・システム要件について詳しくは、IBM Security Identity Manager インフォメーション・センターの『ハードウェア要件およびソフトウェア要件』を参照してください。

   注: Linux SUSE 9 から SUSE 10.0 および 11.0 にアップグレードする場合は、アップグレードの前に必ず既存の `/etc/services` ファイルをバックアップしてください。アップグレード後に `/etc` ディレクトリーにファイルをコピーして戻してください。
2. データベースをサポートされるバージョンにマイグレーションし、データベースのコマンドを確実に実行するようにします。
3. ディレクトリー・サーバーをサポートされるバージョンにマイグレーションし、ディレクトリー・サーバーのコマンドを確実に実行するようにします。
4. IBM Tivoli Directory Integrator を使用している場合、サポートされるバージョンにマイグレーションします。
5. Tivoli Identity Manager サーバーをアップグレードして、IBM Security Identity Manager バージョン 6.0 インストール・プログラムを使用します。

   インストール・プログラムによって、以下のアップグレードが行われます。
   - データベースのスキーマおよびデータ
   - ディレクトリー・サーバーのスキーマおよびデータ
   - IBM Security Identity Manager 用の WebSphere Application Server 構成
   - IBM Security Identity Manager プロパティー・ファイル
   - その他の IBM Security Identity Manager ファイル

アップグレード・プロセス中、*ITIM_HOME*¥data ディレクトリーが *ITIM_HOME*¥data¥backup ディレクトリーにバックアップされ、必要な場合は後でリカバリーできます。

アップグレードでは、IBM Tivoli Identity Manager サーバーのみをアップグレードします。アダプターのアップグレードは、このサーバーのアップグレードが完了して安定状態に入るまでは行いません。アダプターのアップグレードについて詳しくは、IBM Security Identity Manager インフォメーション・センターのアダプターの資料を参照してください。

注: アップグレードを行うには、現在の *ITIM_HOME* ディレクトリーを IBM Security Identity Manager バージョン 6.0 のインストール・ロケーションとして選択する必要があります。アップグレードの実行後、*ITIM_HOME*¥data ディレクトリーの Messages.properties ファイルのヘッダーの著作権表示を調べることで現在のバージョンを検証できます。

6. WebSphere Application Server バージョン 7.0 が既にインストールされている場合は、必要なフィックスパックがインストールされていることを確認します。現在実行中の WebSphere Application Server のバージョンが 6.1 の場合は、WebSphere Application Server バージョン 7.0 を別途インストールして IBM Security Identity Manager をアップグレードしてから、必要なフィックスパックをすべてインストールする必要があります。
7. IBM Tivoli Identity Manager サーバーのアップグレードが完了したら、それらのアダプターを IBM Security Identity Manager バージョン 6.0 のアダプターにアップグレードします。詳しくは、260 ページの『アダプターのアップグレード』を参照してください。

アップグレード・プロセスが保持するプロセスおよび設定

アップグレード・プロセスは、承認や、パスワード変更などの他の関連アクションのために保留している実行中ワークフロー・プロセスを保存します。

アップグレード・プロセスでは、以下の設定が保存されます。

- 認証局 (CA) 証明書。IBM Security Identity Manager のデモンストレーション証明書は更新されます。
- 以下のファイルで定義された IBM Security Identity Manager のプロパティー
  - enRole.properties
  - enRoleAuthentication.properties
  - enRoleDatabase.properties
  - enRoleLDAPConnection properties
  - enRoleMail.properties
  - enRoleLogging.properties
  - enroleAuditing.properties
  - enroleworkflow.properties
  - ui.properties
  - CustomLabels.properties
  - CustomLabels_en.properties

- adhocreporting.properties
- SelfServiceScreenText.properties
- SelfServiceScreenText_en.properties
- SelfServiceHelp.properties
- SelfServiceUI.properties
- SelfServiceHomePage.properties
- scriptframework.properties

- data¥workflow_systemprocess ディレクトリーの以下のワークフロー・システム・ファイル。
  - notifytemplate.html

    注: 通知テンプレートは、Tivoli Identity Manager バージョン 5.0 以降に変更されました。新規テンプレートを使用するには、notifytemplate.html.5.0 を元の notifytemplate.html に名前変更します。通知テンプレートのマイグレーションについて詳しくは、255 ページの『通知テンプレートのマイグレーション』を参照してください。
  - multiaccountdelete.xml
  - multiaccountrestore.xml
  - multiaccountsuspend.xml
- LDAP に保管されているすべてのデフォルトの通知テンプレート。

保存されない、または手動アップグレードが必要なプロセスおよび設定

アップグレード・プロセスは、以下のワークフロー・プロセスを保存しません。これらは、IBM Security Identity Manager をアップグレードする前に完了を停止するか、許可する必要があります。

- プロビジョニング・ポリシーの追加/変更/除去
- 動的役割の追加/変更/除去
- 調整
- ID フィード

その他のカスタマイズ・データおよび設定は、アップグレード・プロセスの後に失われます。詳しくは、254 ページの『カスタマイズ・データの手動保存』を参照してください。

以下のユーザー・カスタマイズは保存されません。

- ウェルカム・ページおよび XLS スタイル・シートで使用されたカスタム・ロゴ。ウェルカム・ページを変更した場合、Styles.css ファイルを再インプリメントする必要があります。
- カスタマイズされた WebSphere Application Server 構成。例を以下に示します。
  - ITIM_CLIENT 役割マッピング (再マップが必要)。
  - Tivoli Identity Manager が WebSphere Application Server 共有ライブラリー定義を通じて使用する共有ライブラリー。

また、以下のコンポーネントを手動でアップグレードする必要があります。

- IBM Security Identity Manager クライアント・アプリケーションが使用する IBM Security Identity Manager JAR ファイル。

  IBM Security Identity Manager クライアント・アプリケーションは、現行の itim_api.jar、api_ejb.jar、itim_server_api.jar、および jlog.jar ファイルを、IBM Security Identity Manager バージョン 6.0 のファイルと置き換える必要があります。

  クライアント・サイドにプロパティー・ファイルの重複コピーがあるすべての IBM Security Identity Manager クライアント・アプリケーションに対して、以下のステップを実行します。

  1. クライアント・アプリケーション上の重複プロパティー・ファイルの名前を変更して、実行したすべての手動変更を保存します。
  2. IBM Security Identity Manager サーバーからクライアント・アプリケーション上の重複コピーにプロパティー・ファイルをコピーします。
  3. 以前に重複プロパティー・ファイルを手動で変更した場合は、再度手動で変更を適用します。
- Tivoli Identity Manager 5.1 の HR フィード・サービス・フォームでは、職務分離ポリシーを評価するためのチェック・ボックスが追加されています。この機能を使用可能にするには、「**システムの構成**」 -> 「**フォームの設計**」を使用し、新しい属性 **erevaluatesod** を HR フィード・サービス定義フォームに組み込みます。**erevaluatesod** 属性は、ブール値型で、フォーム上のチェック・ボックスとして組み込む必要があります。
- IBM Security Identity Manager バージョン 6.0 では、新しい属性 errepositoryservice が ITIM サービス・フォームに追加されています。「サービス情報」ページでは、この属性に「**WebSphere アカウント・リポジトリー**」というラベルが付いています。 Tivoli Identity Manager 5.0 または 5.1 からアップグレードした後、デフォルトの ITIM サービス DN 値が ITIM サービス・インスタンスに設定されます。ただし、ITIM サービス・フォームは、自動的にこの属性が付いてアップグレードされるわけではありません。なぜなら、ユーザーによっては、カスタマイズ済みの ITIM サービス・フォームを持っている場合があるからです。この属性値を表示または更新するには、Form Designer アプレットを使用して、この属性を手動で ITIM サービス・フォームに追加する必要があります。アップグレード後に、認証ユーザー・レジストリーとして外部ユーザー・レジストリーを使用する場合は、このステップが必要です。 Form Designer アプレットを使用してこの属性を追加するには、以下のステップを実行します。

  1. IBM Security Identity Manager 管理コンソールから、「**システムの構成**」 > 「**フォームの設計**」を選択します。
  2. 「フォームの設計」パネルで、「**サービス**」 > 「**ITIM**」をダブルクリックします。
  3. 右側のパネルの属性リストの下で、「**errepositoryservice**」をダブルクリックします。 errepositoryservice 属性が ITIM サービスに追加されます。
  4. 「**$errepositoryservice**」の隣にある **[TextField]** を右クリックして、「**変更先**」 > 「**検索コントロール**」を選択します。「検索コントロール・エディター」ウィンドウが開きます。
  5. 「カテゴリー」リストから、「**サービス**」を選択します。

6. 「タイプ」リストから「**単一値**」を選択します。
7. 「**組織全体の検索 (チェックされない場合は現行コンテナーのみ)**」ボックスを選択します。
8. 「**OK**」をクリックして、ウィンドウを閉じます。
9. フォームを保存します。

- アクセス・コントロール項目を手動でアップグレードします。詳しくは、259 ページの『アクセス・コントロール項目の手動アップグレード』を参照してください。

IBM Security Identity Manager のアップグレードの準備

IBM Security Identity Manager をアップグレードする前に、いくつかのシステム・タスクを完了する必要があります。

手順

1. アップグレード・プロセスの開始前にシステム・アクティビティーを削減します。 IBM Security Identity Manager をアップグレードする前に、ポリシー実行または調整要求を開始しないでください。 IBM Security Identity Manager データベースの SCHEDULED_MESSAGES テーブルから直接エントリーを削除しないでください。
2. 以下のワークフロー・プロセスを完了または停止します。これらはアップグレード中に保存されません。
   - プロビジョニング・ポリシーの追加/変更/除去
   - 動的役割の追加/変更/除去
   - 調整
   - ID フィード
3. API クライアントをシャットダウンし、IBM Security Identity Manager アプリケーションへの Web アクセスをオフにします。 これらの処置により、アップグレード・プロセスの前に新規ワークフロー要求の実行依頼が行われなくなります。
4. IBM Security Identity Manager データベースをバックアップし、データベース・サーバーが実行中であることを確認します。次に、データベース・サーバーをサポートされるバージョンにマイグレーションします。
   - DB2 データベース

     DB2 データベースのアップグレードについて詳しくは、Web サイト http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/topic/com.ibm.db2.luw.doc/welcome.html を参照してください。

     注: DB2 データベースをアップグレードすると、ポート番号が変更される場合があります。ご使用のポート番号を検証してください。詳しくは、30 ページの『正しいサービス Listen ポートおよびサービス名の決定』を参照してください。
   - Oracle

Oracle のアップグレードについて詳しくは、Oracle Web サイトの資料を参照してください。

- SQL Server 2008

  SQL Server 2008 のアップグレードについて詳しくは、Microsoft SQL Server Web サイトの資料を参照してください。

  SQL Server 2008 の構成について詳しくは、41 ページの『SQL Server 2008 の構成』を参照してください。

5. ディレクトリー・サーバーをサポートされるバージョンにマイグレーションします。次に IBM Security Identity Manager スキーマおよびデータをバックアップして、ディレクトリー・サーバーが実行中であることを確認します。 Tivoli Identity Manager バージョン 5.0 または 5.1 をリカバリーする場合は、Tivoli Identity Manager LDAP ディレクトリーを LDIF ファイルにエクスポートします。

   注: 現在サポートされている IBM Tivoli Directory Server または Sun Directory Server Enterprise Edition 6.3 を使用している場合は、マイグレーションは不要です。これらはサポート対象のディレクトリー・サーバーです。

   IBM Tivoli Directory Server を新しい LDAP インスタンスにマイグレーションする場合は、システム構成ツール `runConfig` を実行して、関連するプロパティー・ファイルを新しい LDAP インスタンスのデータに更新します。

   Windows オペレーティング・システムの場合は、以下のコマンドを実行します。

   ```
   runConfig.exe
   ```

   UNIX または Linux オペレーティング・システムの場合は、以下のコマンドを実行します。

   ```
   ./runConfig
   ```

6. 現在 WebSphere Application Server バージョン 6.1 を実行している場合は、WebSphere Application Server バージョン 7.0 にマイグレーションすることはできません。 WebSphere Application Server バージョン 7.0 の別のインストール済み環境を使用して、IBM Security Identity Manager をアップグレードする必要があります。また、以下の手順も実行する必要があります。
   - 単一サーバー: 必要なフィックスパックをインストールします。
   - クラスター: 必要なフィックスパックをインストールします。
7. 単一サーバー構成およびクラスター構成の各クラスター・メンバーでは、以下のステップを完了します。
   a. *itim* ディレクトリーをバックアップします。
   b. Tivoli Identity Manager 5.0 または 5.1 からアップグレードしている場合、*WAS_HOME*¥installedApps¥*cellname*¥ITIM.ear ディレクトリーにアクセスし、カスタマイズされているファイルを一時保持領域に保管します。
8. WebSphere 環境で該当するサーバーが実行中であることを確認します。次のステップを実行します。
   - 単一サーバー構成:

インストールした最新のフィックスパックが適用された WebSphere Application Server を開始します。最新のフィックス・パックおよび使用可能な APAR については、IBM Security Identity Manager インフォメーション・センターを参照してください。

- クラスター構成:

  管理コンソールを使用して、デプロイメント・マネージャーとすべてのノードが統合されていることを確認します。また、ノード・エージェントが実行されていること、および最新のフィックスパックが適用されていることも確認します。最新のフィックス・パックおよび使用可能な APAR については、IBM Security Identity Manager インフォメーション・センターを参照してください。

9. IBM Tivoli Identity Manager アプリケーションと WebSphere サーバーを停止します。
   - 単一サーバー構成:

     IBM Tivoli Identity Manager アプリケーションと、IBM Tivoli Identity Manager が実行されている WebSphere サーバーを停止します。
   - クラスター構成:

     IBM Tivoli Identity Manager アプリケーションと、IBM Tivoli Identity Manager アプリケーションが実行されている WebSphere クラスターを停止します。

サービス統合バスの消去

Tivoli Identity Manager 5.0 または 5.1 から IBM Security Identity Manager バージョン 6.0 にアップグレードする前に、復元したデータベースからサービス統合バス (SIB) データを消去する必要があります。

始める前に

フリー・ディスク・スペースおよび仮想メモリー要件に適合していることを確認します。また、システムの temp ディレクトリーに、十分なフリー・ディスク・スペースがあることを確認します。ターゲット・システムは、IBM Security Identity Manager インフォメーション・センターの『*ハードウェア要件およびソフトウェア要件*』に記載されているハードウェアとソフトウェアの要件を満たしている必要があります。

必要な管理権限を持っていることを確認します。Windows システムでは、ログイン・ユーザー ID は Administrators グループに属する必要があります。DB2 または Oracle を使用する場合、Linux システムでは、ログイン・ユーザー ID が root でなければなりません。

IBM Security Identity Manager データベースが稼働していることを確認します。

手順

1. ターゲットの IBM Security Identity Manager バージョン 6.0 サーバーで、データベースを開始します。ご使用のデータベースのタイプに応じて、以下に示す手順を実行します。

- DB2
  a. DB2 コマンド・ウィンドウを開きます。
  b. UNIX または Linux: DB2 インスタンス所有者としてログオンして db2 と入力し、DB2 コマンド・ウィンドウを開きます。

     Windows: 「**スタート**」 > 「**ファイル名を指定して実行**」をクリックし、db2cmd と入力します。DB2 コマンド・ウィンドウが開いたら、db2 と入力します。
  c. 以下のコマンドを使用して、DB2 インスタンス所有者としてデータベースに接続します。

     ```
     connect to itimdb user instance_owner using instance_owner_password
     ```

     各ディレクトリーの説明を以下に示します。
     – *itimdb* は IBM Security Identity Manager データベース名です。
     – *instance_owner* は DB2 インスタンスの所有者です。
     – *instance_owner_password* は DB2 インスタンスの所有者のパスワードです。
- Oracle

  Oracle データベースを始動します。
- Microsoft SQL
  a. Microsoft SQL Server Management Studio を開始します。
  b. IBM Security Identity Manager バージョン 6.0 で使用されるデータベースに移動します。
  c. データベースを右クリックして、「**新しいクエリ**」をクリックします。

2. SIB スキーマのテーブルからデータをすべて削除するために必要な DELETE SQL ステートメントを入力します。

   ```
   delete from schema_name.SIB000
   delete from schema_name.SIB001
   delete from schema_name.SIB002
   delete from schema_name.SIBCLASSMAP
   delete from schema_name.SIBKEYS
   delete from schema_name.SIBLISTING
   delete from schema_name.SIBXACTS
   delete from schema_name.SIBOWNER
   delete from schema_name.SIBOWNERO
   ```

   SIB スキーマ *schema_name* は、以下のとおりです。

表 27. サービス統合バス・スキーマ名

Tivoli Identity Manager 環境	スキーマ名
単一サーバー	ITIML000
クラスター	ITIML000、ITIML001、ITIML002、ITIML003、および ITIMS000

注: SIBOWNERO は、すべての Tivoli Identity Manager 環境に存在しない可能性があります。これが存在しない場合に delete ステートメントが失敗したときは、失敗を無視できます。

単一サーバーの Tivoli Identity Manager バージョン 5.0 または 5.1 から IBM Security Identity Manager バージョン 6.0 へのアップグレード

この手順は、ご使用の単一サーバー構成を、以前のバージョンの Tivoli Identity Manager から現在のバージョンの IBM Security Identity Manager にマイグレーションする場合に使用します。

始める前に

241 ページの『IBM Security Identity Manager のアップグレードの準備』に記載されたステップが完了していることを確認します。また、以下のものも必要です。

- データベース管理ユーザー ID とパスワード
- WebSphere Application Server の管理ユーザー ID とパスワード
- /tmp ディレクトリーに 150 MB 以上のフリー・スペース

このタスクについて

アップグレード・プロセスは、単一サーバー構成で以下のタスクを実行します。

1. *ITIM_HOME*¥data ディレクトリーのファイルをバックアップします。
2. *ITIM_HOME* ディレクトリーのファイルを置換します。
3. WebSphere Application Server のバージョン状況を確認し、WebSphere Application Server が実行されていない場合は、その開始を試みます。 241 ページの『IBM Security Identity Manager のアップグレードの準備』のステップ 8 を参照してください。
4. システム構成ツール (**runConfig**) を開始して、ユーザーに現在のシステム構成の値を確認するためのプロンプトを出します。
5. 複数のプロパティー・ファイルを更新します。詳しくは、 238 ページの『アップグレード・プロセスが保持するプロセスおよび設定』を参照してください。
6. WebSphere Application Server を IBM Security Identity Manager バージョン 6.0 用に構成します。
7. IBM Security Identity Manager データベースのスキーマおよびデータをアップグレードします。
8. IBM Security Identity Manager ディレクトリー・サーバーのスキーマおよびデータをアップグレードします。
9. IBM Security Identity Manager アプリケーション (ITIM.ear) を WebSphere Application Server にデプロイします。
10. WebSphere Application Server と IBM Security Identity Manager アプリケーションを停止および開始します。

手順

1. インストール・プログラムを実行します。
   - Windows オペレーティング・システムの場合:
     a. 「**スタート**」 > 「**ファイル名を指定して実行**」をクリックします。
     b. インストール・プログラムがあるドライブおよびパスを入力してから、コマンド instwin.exe を入力します。

「ようこそ」ウィンドウが開きます。

- UNIX または Linux オペレーティング・システムの場合:
  a. コマンド・シェル・プロンプト・ウィンドウを開き、インストール・プログラムのあるディレクトリーを特定します。
  b. IBM Security Identity Manager インストール・プログラムで、次のコマンドを入力します。
     - AIX オペレーティング・システム: `instaix.bin`
     - Linux オペレーティング・システム: `instlinux.bin`
     - Linux for System p オペレーティング・システム: `instplinux.bin`
     - Linux for System z オペレーティング・システム: `instzlinux.bin`
     - Solaris オペレーティング・システム: `instsol.bin`

  インストール・プログラムが開始し、「ようこそ」ウィンドウが開きます。

  UNIX または Linux システムでは、インストール・プログラムを実行するために、`/tmp` ディレクトリーに 150 MB 以上のフリー・スペースが必要です。十分なスペースがない場合は、*IATEMPDIR* 環境変数を、十分な空きディスク・スペースのあるディスク区分上のディレクトリーに設定します。変数を設定するためには、次に示すコマンドのうちの 1 つをコマンド行プロンプトに入力し、それからインストール・プログラムを再実行します。

  - Bourne shell (sh)、ksh、bash、および zsh:

    ```
    $ IATEMPDIR=temp_dir
    $ export IATEMPDIR
    ```

  - C shell (csh) および tcsh:

    ```
    $ setenv IATEMPDIR temp_dir
    ```

  ここで *temp_dir* はディレクトリーへのパスで、例えば、`/your/free/directory` の場合、 使用可能なフリー・ディスク・スペースがあります。

2. 適合する言語を選択し、「**OK**」をクリックします。
3. 著作権および特記事項を確認し、「**次へ**」をクリックします。

   注: IBM Security Identity Manager を AIX システムにインストールし、著作権のテキストを表示できない場合は、システムの色のコントラストの設定を調整する必要があります。コントラスト色の設定を High から Low に変更します。
4. 「ご使用条件」ウィンドウで、使用条件を読み、その条項に同意するかどうか決定します。同意する場合は、以下の手順を実行します。
   a. 「**同意する**」を選択します。
   b. 「**次へ**」をクリックします。
5. 「インストール・ディレクトリーの選択 (Choose Install Directory)」ウィンドウで、アップグレードする既存の Tivoli Identity Manager のホーム・ディレクトリーを選択する必要があります。
   - 既存のディレクトリーをそのまま使用します。または、
   - 「**選択**」をクリックして、該当するディレクトリーを選択します。

   a. 「**次へ**」をクリックします。

6. 「IBM Security Identity Manager のアップグレード」ウィンドウで、**「次に進む」**をクリックしてアップグレードを開始します。
7. 「注意」ウィンドウを読んで、前提条件のアプリケーションが IBM Security Identity Manager がサポートする要件に適合していることを確認します。**「次へ」**をクリックします。
8. 「WebSphere Application Server インストール・ディレクトリー (installation directory)」ウィンドウで、WebSphere Application Server の場所を指定します。**「次へ」**をクリックします。 コンピューター上に WebSphere Application Server の複数インスタンスを存在させることができます。
9. IBM Security Identity Manager のデプロイ先となる WebSphere Application Server 基本プロファイルを選択します。**「次へ」**をクリックします。
10. WebSphere Application Server 管理セキュリティーが有効になっている場合は、WebSphere Application Server のユーザー ID およびパスワードのウィンドウが開きます。ユーザー ID とパスワードを入力し、**「次へ」**をクリックします。
11. WebSphere アプリケーション構成のセキュリティー・ドメイン・ウィンドウのタイプを選択し、**「次へ」**をクリックします。
    - IBM Security Identity Manager のカスタム・レジストリーを使用する場合は**「はい」**を選択します。
    - 既存のセキュリティー・ドメインとレジストリーを使用する場合は**「いいえ」**を選択します。

    注: **「はい」**を選択すると、IBM Security Identity Manager に付属のカスタム・レジストリーが認証の判定に使用されます。**「いいえ」**を選択すると、WebSphere セキュリティー・ドメインの既存のユーザー・レジストリーが認証の判定に使用されます。**「いいえ」**を選択した場合は、インストール・ウィザードの完了後にインストール後の構成ステップを実行する必要があります。166 ページの『認証用の外部ユーザー・レジストリーに対するインストール後の構成』を参照してください。
12. IBM Security Identity Manager システム・ユーザーの名前とパスワードを入力し、**「次へ」**をクリックします。 前の手順でセキュリティー・ドメインを作成することを選択している場合は、デフォルトの IBM Security Identity Manager システム・ユーザーとして `isimsystem` が入力されます。
13. 「Java ホーム (Java home)」ウィンドウで、IBM Security Identity Manager バージョン 6.0 が現在指しているディレクトリーを記録します。前のディレクトリーを参照するファイルを手動でマイグレーションして、現行ディレクトリーを参照することが必要な場合があります。**「OK」**をクリックします。
14. Oracle データベースまたは Microsoft SQL Server を使用する場合は、「Microsoft SQL Server JDBC ドライバーの場所」ウィンドウが表示されます。JDBC ドライバーとロケーション名を指定します。 **「次へ」**をクリックします。 詳しくは、35 ページの『Oracle JDBC ドライバーのインストール』 および 41 ページの『SQL Server JDBC ドライバーのインストール』を参照してください。

    注: WebSphere Application Server 6.1.1 上の Tivoli Identity Manager 5.1 から WebSphere Application Server 7.0 上の IBM Security Identity Manager 6.0 にア

ップグレードする場合は、JDBC ドライバーのセットアップ用パネルは開きません。Oracle データベースの場合は、追加の手動ステップが必要です。

a. IBM Security Identity Manager 6.0 を WebSphere Application Server 7.0 フィックスパック 5 にデプロイしたら、`ojdbc.jar` ファイルを `ISIM_HOME/lib` から削除し、`ojdbc6.jar` に置き換えます。次に、`ojdbc6.jar` の名前を `ojdbc.jar` に変更します。 WebSphere Application Server 7.0 では JDK1.6 が使用されるため、この操作は必要です。

b. サービス統合バスを消去します。この章の 269 ページの『サービス統合バスの消去』を参照してください。

15. 「Tivoli Common Directory」ウィンドウで、Tivoli Common Directory のデフォルトのディレクトリーをそのまま使用するか、別のディレクトリーを指定します。「**次へ**」をクリックします。 IBM Security Identity Manager インストール・プログラムは、CTGIM サブディレクトリーを作成して、IBM Security Identity Manager の保守関連ファイルを保管します。ディレクトリーに 25 MB 以上のフリー・スペースがあることを確認してください。

16. 「プリインストールの要約 (Pre-install Summary)」ウィンドウで、「**インストール**」をクリックします。 インストール・プログラムによってシステム構成ツール `runConfig` が開始されます。これにより、ユーザーは必要に応じて構成設定値を変更できます。**runConfig** について詳しくは、140 ページの『一般に使用されるシステム・プロパティーの構成』を参照してください。

    a. 「システム構成ツール」ウィンドウで、すべてのパラメーターの値を確認します。これらは、以前のバージョンの Tivoli Identity Manager から保持されています。

    b. 「データベース」タブで、JDBC URL が正しいタイプ 4 JDBC ドライバー URL 形式であることを検証し、「**テスト**」をクリックしてデータベース接続をテストします。

    c. 「**セキュリティー**」タブの IBM Security Identity Manager のシステム・ユーザー ID とパスワードが、WebSphere Application Server の管理ユーザー ID およびパスワードと異なっている場合は、システム・ユーザー ID とパスワードを変更します。

    d. 値を検証して、「**OK**」をクリックします。 システム構成には数分を要します。

    インストーラーによってデータベースのアップグレード・プログラムが開始され、データベース・スキーマとデータがアップグレードされます。

17. データベースの管理ユーザー ID とパスワードを指定して、メッセージング・エンジンに必要なデータベース・スキーマを作成またはアップグレードします。 管理ユーザー ID にデータベース・スキーマを作成するための特権がない場合は、アップグレード中にエラー・メッセージが生成されます。アップグレード完了後に *ISIM_HOME*¥bin¥DBUpgrade プログラムを実行し、正しいデータベース管理 ID を入力します。このプログラムにより、メッセージング・エンジンのデータベース・スキーマおよびテーブルが確実に作成されるようになります。 インストーラーによって LDAP のアップグレード・プログラムが開始され、LDAP スキーマとデータが自動的にアップグレードされます。

注: Oracle Enterprise Directory Server Enterprise を使用する場合に、アップグレードによって新しい索引が追加される場合は、アップグレードの完了後に、再度データに索引付けを行う必要があります。

次のタスク

インストールの完了後、アップグレード・プロセス中に保存されなかったカスタマイズを手動で更新する必要があります。詳しくは、254 ページの『カスタマイズ・データの手動保存』を参照してください。

Tivoli Identity Manager バージョン 5.0 または 5.1 クラスター構成から IBM Security Identity Manager バージョン 6.0 へのアップグレード

この手順は、ご使用のクラスター構成を、以前のバージョンの IBM Tivoli Identity Manager から現在のバージョンにマイグレーションする場合に使用します。

始める前に

241 ページの『IBM Security Identity Manager のアップグレードの準備』に記載されたステップが完了していることを確認します。また、以下のものも必要です。

- データベース管理ユーザー ID とパスワード
- WebSphere Application Server 管理ユーザー ID とパスワード
- UNIX または Linux オペレーティング・システムの場合は、`/tmp` ディレクトリーに 150 MB 以上のフリー・スペース

このタスクについて

クラスター構成のアップグレード・プロセスでは、以下のタスクを実行します。

1. *ITIM_HOME*¥data ディレクトリーのファイルをバックアップします。
2. *ITIM_HOME* ディレクトリーのファイルを置換します。
3. デプロイメント・マネージャーがインストールされているコンピューターで、以下のタスクを実行します。
   a. システム構成ツール (**runConfig**) を開始して、ユーザーが現在のシステム構成の値を確認できるようにします。
   b. 複数のプロパティー・ファイルを更新します。詳しくは、238 ページの『アップグレード・プロセスが保持するプロセスおよび設定』を参照してください。
   c. WebSphere Application Server を IBM Security Identity Manager バージョン 6.0 用に構成します。
   d. IBM Security Identity Manager データベースのスキーマおよびデータをアップグレードします。
   e. IBM Security Identity Manager ディレクトリー・サーバーのスキーマおよびデータをアップグレードします。
4. クラスター・メンバーがインストールされている各コンピューターで、システム構成ツール **runConfig** を開始します。このツールは、以下のことを行います。
   - ユーザーに対して現在のシステム構成の値を確認するように要求します。
   - 複数のプロパティー・ファイルを更新します。

- WebSphere Application Server を IBM Security Identity Manager 用に構成します。

詳しくは、238 ページの『アップグレード・プロセスが保持するプロセスおよび設定』を参照してください。

手順

1. デプロイメント・マネージャーと各クラスター・メンバー・コンピューターでインストール・プログラムを実行します。
   - Windows オペレーティング・システムの場合:
     a. 「**スタート**」 > 「**ファイル名を指定して実行**」をクリックします。
     b. インストール・プログラムがあるドライブおよびパスを入力してから、コマンド `instwin.exe` を入力します。

     「ようこそ」ウィンドウが開きます。
   - UNIX または Linux オペレーティング・システムの場合:
     a. コマンド・シェル・プロンプト・ウィンドウを開き、インストール・プログラムのあるディレクトリーを特定します。
     b. IBM Security Identity Manager インストール・プログラムで、次のコマンドを入力します。
        - AIX オペレーティング・システム: `instaix.bin`
        - Linux オペレーティング・システム: `instlinux.bin`
        - Linux for System p オペレーティング・システム: `instplinux.bin`
        - Linux for System z オペレーティング・システム: `instzlinux.bin`
        - Solaris オペレーティング・システム: `instsol.bin`

     インストール・プログラムが開始し、「ようこそ」ウィンドウが開きます。

     UNIX または Linux システムでは、インストール・プログラムを実行するために、`/tmp` ディレクトリーに 150 MB 以上のフリー・スペースが必要です。十分なスペースがない場合は、*IATEMPDIR* 環境変数を、十分な空きディスク・スペースのあるディスク区分上のディレクトリーに設定します。変数を設定するためには、次に示すコマンドのうちの 1 つをコマンド行プロンプトに入力し、それからインストール・プログラムを再実行します。
     - Bourne shell (sh)、ksh、bash、および zsh:

       ```
       $ IATEMPDIR=temp_dir
       $ export IATEMPDIR
       ```

     - C shell (csh) および tcsh:

       ```
       $ setenv IATEMPDIR temp_dir
       ```

     ここで *temp_dir* はディレクトリーへのパスで、例えば、`/your/free/directory`の場合、 使用可能なフリー・ディスク・スペースがあります。
2. 適合する言語を選択し、「**OK**」をクリックします。
3. 著作権および特記事項を確認し、「**次へ**」をクリックします。

注: IBM Security Identity Manager を AIX システムにインストールし、著作権のテキストを表示できない場合は、システムの色のコントラストの設定を調整する必要があります。コントラスト色の設定を High から Low に変更します。

4. 「ご使用条件」ウィンドウで、使用条件を読み、その条項に同意するかどうか決定します。同意する場合は、以下の手順を実行します。
   a. 「**同意する**」を選択します。
   b. 「**次へ**」をクリックします。
5. 「IBM Security Identity Manager インストール・ディレクトリー」ウィンドウでは、アップグレード対象として、既存の Tivoli Identity Manager ホーム・ディレクトリーを選択する必要があります。
   - 既存のディレクトリーをそのまま使用します。または、
   - 「**選択**」をクリックして、該当するディレクトリーを選択します。
6. 「**次へ**」をクリックして、次のステップに進みます。
7. 「IBM Security Identity Manager のアップグレード」ウィンドウで、「**次に進む**」をクリックしてアップグレードを開始します。
8. IBM Security Identity Manager 6.0 にアップグレードするかどうかを確認するための警告ウィンドウが開きます。「**次に進む**」をクリックしてアップグレードに進みます。
9. IBM Security Identity Manager が 2 つのバージョンの WebSphere Application Server 内で共存できないことを示す警告ウィンドウが開きます。「**OK**」をクリックします。
10. 「注意」ウィンドウを読んで、前提条件のアプリケーションが IBM Security Identity Manager がサポートする要件に適合していることを確認します。次に、「**OK**」をクリックします。
11. IBM Security Identity Manager クラスター・メンバーがコンピューター上にインストールされている場合は、WebSphere Application Server のインストール・ディレクトリーを指定し、「**次へ**」をクリックします。WebSphere プロファイル名を選択し、「**次へ**」をクリックします。
12. デプロイメント・マネージャーがコンピューター上にインストールされている場合は、デプロイメント・マネージャーのインストール・ディレクトリーを指定し、「**次へ**」をクリックします。WebSphere Deployment Manager プロファイル名を選択し、「**次へ**」をクリックします。
13. WebSphere Application Server 管理セキュリティーが有効になっている場合は、WebSphere Application Server の管理者クリデンシャル」ウィンドウが表示されます。管理者ユーザー ID とパスワードを入力し、「**次へ**」をクリックします。
14. IBM Security Identity Manager システム・ユーザーの名前とパスワードを入力し、「**次へ**」をクリックします。 前の手順でセキュリティー・ドメインを作成することを選択している場合は、デフォルトのシステム・ユーザーとして `isimsystem` が入力されます。
15. Oracle データベースまたは Microsoft SQL Server を使用する場合は、「Microsoft SQL Server JDBC ドライバーの場所」ウィンドウが開きます。JDBC ドライバーとロケーション名を指定します。 「**次へ**」をクリックしま

す。 詳しくは、 35 ページの『Oracle JDBC ドライバーのインストール』 および 41 ページの『SQL Server JDBC ドライバーのインストール』を参照してください。

16. 「ディレクトリー・サーバーのサポートされるバージョンが必要です」ウィンドウが開き、ディレクトリー・サーバーがインストールされることが示されます。「**続行**」をクリックします。
17. 「新規の Java Home」ウィンドウで、IBM Security Identity Manager バージョン 6.0 が現在指しているディレクトリーを確認します。前のディレクトリーを参照するファイルを現行ディレクトリーに手動でマイグレーションすることが必要な場合があります。「**OK**」をクリックします。
18. 「**次へ**」をクリックして、「エージェントレス・アダプターは別途アップグレードしてください」ウィンドウの次まで進みます。
19. 「共有アクセス・モジュールをインストールしますか」ウィンドウで、以下の基準に従って、共有アクセス・モジュールをインストールするかどうかを決定します。
    - 共有アクセス・モジュールが必要で、購入済みである場合は「**はい**」を選択します。インストーラーによって、IBM Security Identity Manager が共有アクセス・モジュール・コンポーネントと共にインストールされます。
    - 共有アクセス・モジュールを購入していない場合は、「**いいえ**」を選択します。共有アクセス・モジュールは、後で必要になったときに、いつでも個別にインストールできます。
20. 「Tivoli Common Directory」ウィンドウで、Tivoli Common Directory のデフォルトのディレクトリーをそのまま使用するか、別のディレクトリーを指定します。「**次へ**」をクリックします。 インストール・プログラムは、CTGIM サブディレクトリーを作成して、IBM Security Identity Manager の保守関連ファイルを保管します。ディレクトリーに 25 MB 以上のフリー・スペースがあることを確認してください。
21. 「プリインストールの要約 (Pre-install Summary)」ウィンドウで、「**インストール**」をクリックします。 インストール・プログラムによってシステム構成ツール `runConfig` が開始されます。これにより、ユーザーは必要に応じて構成設定値を変更できます。このツールについて詳しくは、 140 ページの『一般に使用されるシステム・プロパティーの構成』を参照してください。
    a. 「システム構成ツール」ウィンドウで、すべてのパラメーターの値を確認します。これらは、以前のバージョンの Tivoli Identity Manager から保持されています。
    b. 「ディレクトリー」タブで値を確認し、「**テスト**」をクリックしてディレクトリー・サーバーの接続をテストします。
    c. 「データベース」タブで、JDBC URL が正しいタイプ 4 JDBC ドライバー URL 形式であることを検証します。「**テスト**」をクリックして、データベース接続をテストします。
    d. ユーザー ID とパスワードが WebSphere Application Server の管理ユーザー ID およびパスワードと異なる場合は、「**セキュリティー**」タブで EJB ユーザー ID とパスワードを変更します。EJB ユーザー ID とパスワードは、ステップ 14 で指定した IBM Security Identity Manager のシステム・ユーザー名とパスワードです。

e. 値を検証して、「**OK**」をクリックします。 システム構成には数分を要します。

最初のインストール後、クラスター・メンバーのインストール時にのみ「システム構成」パネルが表示されます。ここで、ユーザーは情報を確認して接続テストできます。

a. 「メール」タブで、表示された情報が最初のインストールと一致していることを確認します。
b. 「一般」タブで、表示された情報が最初のインストールと一致していることを確認します。
c. 「ディレクトリー」タブで、パスワードとホスト名を入力し、このタブの他の情報を検証します。「**テスト**」をクリックして、接続をテストします。
d. 「データベース」タブで、パスワードを入力し、このタブの他の情報を検証します。「**テスト**」をクリックして、データベース接続をテストします。
e. 「ロギング」タブで、表示された情報を検証し、最初のインストールと一致していることを確認します。
f. 「UI」タブの情報を検証して更新します。この情報が最初のインストールと一致していることを確認します。
g. 「**セキュリティー**」タブで、最初のインストールに使用した IBM Security Identity Manager のユーザー ID とパスワードを入力します。デフォルトのユーザー ID は `isimsystem` です。
h. 各タブのすべての情報を検証したら、「**OK**」をクリックします。

注: このシステム構成パネルは、デプロイメント・マネージャーとクラスター・メンバーがインストールされているシステムで使用できます。クラスター・メンバーのアップグレードのみを実行するシステムでは表示されません。デプロイメント・マネージャーで、インストーラーによってデータベース・アップグレード・プログラムが開始され、データベース・スキーマおよびデータがアップグレードされます。

22. データベースの管理ユーザー ID とパスワードを指定して、メッセージング・エンジンに必要なデータベース・スキーマを作成またはアップグレードします。

管理ユーザー ID にデータベース・スキーマを作成するための特権がない場合は、アップグレード中にエラー・メッセージが生成されます。アップグレード完了後に *ISIM_HOME*¥bin¥DBUpgrade プログラムを実行し、正しいデータベース管理 ID を入力します。このプログラムにより、メッセージング・エンジンのデータベース・スキーマおよびテーブルが確実に作成されるようになります。

DBUpgrade の実行後、インストール・プログラムによって LDAP アップグレード・プログラムが開始され、LDAP スキーマとデータが自動的にアップグレードされます。

注: Sun Enterprise Directory Server 6.3 を使用する場合に、アップグレードによって新しい索引が追加される場合は、IBM Security Identity Manager バージョン 6.0 へのアップグレードが完了した後に、再度データに索引付けを行う必要があります。

23. 「**完了**」をクリックして、インストールを終了します。

次のタスク

インストールの完了後、アップグレード・プロセス中に保存されなかったカスタマイズを手動で更新する必要があります。詳しくは、『カスタマイズ・データの手動保存』を参照してください。このアップグレード手順は、各クラスター・メンバーについても実行する必要があります。

カスタマイズ・データの手動保存

アップグレード・プロセスにより保存されないカスタマイズ・データを保存するには、適用可能である場合は以下の手動タスクを実行します。

保存されないプロセスについて詳しくは、 239 ページの『保存されない、または手動アップグレードが必要なプロセスおよび設定』を参照してください。

Java セキュリティーの手動での適用

以前の IBM Development Kit for Java 用に行った変更を新しい IBM Development Kit for Java に手動で適用します。

ロゴおよびスタイル・シートのカスタマイズ

カスタマイズしたロゴおよびスタイル・シートを *WAS_HOME*¥*cellname*¥ITIM.ear ディレクトリーに挿入する必要がある場合、これらのファイルをバックアップ・ロケーションから復元します。

WebSphere Application Server のカスタマイズの保存

WebSphere Application Server 共用ライブラリーの設定値を使用する特定の JAR ファイルなど、WebSphere のカスタマイズを保存できます。

始める前に

システム管理者によるシステムのカスタマイズ方法によっては、このタスクへのアクセス権が付与されていない場合があります。このタスクへのアクセス権限を取得するか、代わりのユーザーにこのタスクを実行してもらうには、システム管理者に連絡してください。

このタスクについて

共用ライブラリーの場合、新規にデプロイされた IBM Security Identity Manager バージョン 6.0 に共用ライブラリーの名前を定義する必要があります。例えば、Tivoli Identity Manager バージョン 5.0 または 5.1 は、user_shared_library などの名前を指定された共用ライブラリーをロードする必要があります。

WebSphere 管理コンソール上で以下のタスクを実行し、前に定義した共用ライブラリーを IBM Security Identity Manager バージョン 6.0 に関連付けます。

手順

1. 「**アプリケーション**」 > 「**エンタープライズ・アプリケーション**」 >「**ITIM**」をクリックします。
2. 「**共用ライブラリー参照**」をクリックします。
   a. 共有ライブラリーを選択します。
   b. 「**OK**」をクリックします。
3. 「**適用**」をクリックして、変更を適用します。
4. 構成を保存します。
5. WebSphere Application Server を再始動して変更を有効化します。

次のタスク

その他のカスタマイズを保存できます。

レポート・テーブルの更新

IBM Security Identity Manager バージョン 6.0 へのアップグレード後は、レポート・データを格納するテーブルのデータがすべて失われます。データを再取得するために、データ同期化を実行する必要があります。

手順

1. IBM Security Identity Manager 管理コンソールにログオンします。
2. 「**レポート**」 > 「**データ同期化**」に移動します。
3. 「**今すぐ同期化を実行**」をクリックします。 テーブルが有効なレポート・データを使用して更新されます。

通知テンプレートのマイグレーション

Tivoli Identity Manager 5.0 または 5.1 環境でデフォルト・テンプレートを更新しても、通知テンプレートはアップグレードされません。 IBM Security Identity Manager アップグレード・プログラムによって上書き (アップグレード) される通知テンプレートはありません。

古い通知テンプレートを IBM Security Identity Manager の通知テンプレートと一致するようにマイグレーションするには、XML Text Template Language (XTTL) コンテンツおよびスタイルの両方を手動で更新する必要があります。

次の表に、IBM Security Identity Manager 構成ファイル「`tenant.tmpl`」内に含まれているテンプレートとそれぞれの場所をリストします。このリストは、アップデートしたデフォルトの通知テンプレートのコンテンツに対するリファレンスとして使用してください。

表 28. tenant.tmpl に含まれているテンプレート

テンプレート名	テンプレート DN
Todo Item Reminder Notification	`cn=Reminder,erglobalid=<%config.workflow%>,ou=config,ou=itim, <%tenant.dn%>`
Default Compliance Alert Notification	`cn=Compliance,erglobalid=<%config.workflow%>,ou=config,ou=itim, <%tenant.dn%>`

表 28. *tenant.tmpl* に含まれているテンプレート (続き)

テンプレート名	テンプレート DN
Default New Account Notification	cn=NewAccount,erglobalid=<%config.workflow%>,ou=config,ou=itim,<%tenant.dn%>
Default New Password Account Notification	cn=NewPassword,erglobalid=<%config.workflow%>,ou=config,ou=itim,<%tenant.dn%>
Default Change Account Notification	cn=ChangeAccount,erglobalid=<%config.workflow%>,ou=config,ou=itim,<%tenant.dn%>
Default Restore Account Notification	cn=RestoreAccount,erglobalid=<%config.workflow%>,ou=config,ou=itim,<%tenant.dn%>
Default Suspended Account Notification	cn=SuspendedAccount,erglobalid=<%config.workflow%>, ou=config,ou=itim,<%tenant.dn%>
Default Deprovision Account Notification	cn=Deprovision,erglobalid=<%config.workflow%>,ou=config,ou=itim,<%tenant.dn%>
Default Activity Timeout Notification	cn=ActivityTimeout,erglobalid=<%config.workflow%>,ou=config,ou=itim,<%tenant.dn%>
Default Process Timeout Notification	cn=ProcessTimeout,erglobalid=<%config.workflow%>,ou=config,ou=itim,<%tenant.dn%>
Default Process Completion Notification	cn=ProcessCompletion,erglobalid=<%config.workflow%>, ou=config,ou=itim,<%tenant.dn%>
Default ManualActivity Notification	cn=ManualActivityApproval,erglobalid=<%config.workflow%>,ou=config,ou=itim,<%tenant.dn%>
Default ManualActivityRFI Notification	cn=ManualActivityRFI,erglobalid=<%config.workflow%>, ou=config,ou=itim,<%tenant.dn%>
Default ManualActivityWorkOrder Notification	cn=ManualActivityWorkOrder,erglobalid=<%config.workflow%>, ou=config,ou=itim,<%tenant.dn%>

XML Text Template Language (XTTL) コンテンツ

Tivoli Identity Manager 5.0 から IBM Security Identity Manager バージョン 6.0 にアップグレードするには、新しい XTTL コンテンツがデフォルトのワークフロー通知テンプレートに必要です。

Tivoli Identity Manager バージョン 5.0 からアップグレードしている場合、以下の XTTL コンテンツがデフォルトのワークフロー通知テンプレートに必要です。

Todo Item Reminder Notification

以下を削除します。

```
<RE key="escalation_note"/> <escalationTime/>
```

以下を追加します。

```
<RE><KEY><JS>  var currentDate = new Date();
var currentTime = currentDate.getTime();
if (currentTime < reminderCtx.getEscalationDate().getTime())
{
   return "workitem_due_note";
}
else
{
  return "workitem_overdue_note";
}
</JS></KEY>
<PARM><escalationTime/></PARM>
</RE>
```

XML Text Template Language (XTTL) コンテンツの更新

この手順は、デフォルトのワークフロー通知テンプレートの XTTL コンテンツを追加または変更する場合に使用します。

始める前に

デフォルトのワークフロー通知テンプレートのコンテンツを変更するには、管理権限を使用して IBM Security Identity Manager バージョン 6.0 GUI 管理コンソールにログオンします。

このタスクについて

この手順を使用して、現在のレベルの IBM Security Identity Manager へのアップグレードに必要なデフォルトのワークフロー通知テンプレートを変更します。XTTL コンテンツの追加、削除、または変更を行うことができます。

手順

1. 「**システムの構成**」 > 「**ワークフロー通知プロパティー**」に移動します。
2. 変更するテンプレートを選択して、「**変更**」をクリックします。
3. 「通知テンプレート」ページで、通知テンプレートの該当セクションを変更します。
4. 「**OK**」をクリックします。

次のタスク

追加のワークフロー・テンプレートの XTTL コンテンツを変更します。

通知テンプレートのスタイルを更新します。

通知テンプレートのスタイル

電子メール通知 (XHTML テンプレート) を設計するには、以下のテンプレートを使用します。

XHTML テンプレートを設計するには、以下のカスケーディング・スタイル・シート (CSS) ファイルおよびイメージを使用します。

- Imperative スタイル・シート

  BASE_URL/console/css/imperative.css
- イメージ
  - Tivoli ロゴ

    BASE_URL/console/html/images/left-tiv-1.gif
  - IBM バナー

    BASE_URL/console/html/images/ibm_banner.gif
  - 背景イメージ

    BASE_URL/console/html/images/mid-part-1.gif
  - テンプレート本体

    BASE_URL/console/html/images/portfolio_background.gif

  注: *BASE_URL* の値は、http://*servername*:*port*/itim です。

背景色

背景のフォーマット設定には以下のカラーが使用されます。

- タイトル・バー: `#a8a8a8`
- 値を含むテーブル: `gray` と `EBEDF3`
- 著作権テーブル: `#a8a8a8`

スタイル・シート

スタイル・シートを適用するには、次のようにしてスタイル・シートをリンクします。

```
<link type="text/css" title="Styles" rel="stylesheet"
href="BASE_URL/console/css/imperative.css" />
```

注: *BASE_URL* の値は、http://*servername*:*port*/itim です。

上記 CSS の text-description クラスは、電子メール通知内のテキストのフォーマット設定に使用されます。例えば、タイトルをフォーマットするには、次のコードを使用します。

```
<!-- Title Bar -->
<table width="100%" border="0" cellpadding="0" cellspacing="0">
 <tbody>
 <tr bgcolor="#a8a8a8">
  <td height="20" width="8"></td>
  <!-- ITIM Notification Label -->
      <td height="20" class="text-description" width="979"
      valign="middle">$TITLE</td>
      <td height="20" width="5"></td>

 </tr>
 </tbody>
</table>
```

通知テンプレート・スタイルの更新

この手順は、デフォルトのワークフロー通知テンプレートのスタイルを追加または変更する場合に使用します。

始める前に

デフォルトのワークフロー通知テンプレートのスタイルを変更するには、管理権限を使用して IBM Security Identity Manager バージョン 6.0 GUI 管理コンソールにログオンします。

手順

1. 「**システムの構成**」 > 「**ワークフロー通知プロパティー**」に移動します。
2. 変更するテンプレートを選択して、「**変更**」をクリックします。
3. 「通知テンプレート」ページで、通知テンプレートの該当セクションを変更します。
4. 「**OK**」をクリックします。

次のタスク

ワークフロー・テンプレートの XTTL コンテンツを変更します。

アクセス・コントロール項目の手動アップグレード

既存の組織のアクセス・コントロール項目は、アップグレード・プロセスによる変更は受けません。IBM Security Identity Manager は、ユーザーおよび他のグループ内のメンバーに対して権限を定義するデフォルト・アクセス・コントロール項目を提供します。ただし、対象とする個人の特定の操作および許可を指定するには、アクセス・コントロール項目を手動で作成する必要があります。

IBM Tivoli Identity Manager 5.0 および 5.1 から IBM Security Identity Manager 6.0 にアップグレードすると、カスタマイズされたアクセス・コントロール項目を手動で作成するための以下の新しい操作が使用可能になります。

- サービス用の新しい操作:
  - アカウント・フォームのカスタマイズ
  - ポリシーの実行
  - ブロックされた要求の再試行
- ITIM サービス用の新しい操作:
  - ポリシーの実行

バージョン 5.0 からバージョン 6.0 にアップグレードした場合は、以下に示す 3 つの新しいデフォルトのアクセス・コントロール項目が導入されます。

- 職務分離ポリシーのデフォルトのアクセス・コントロール項目: 所有者に「すべて」を許可
- 職務分離ポリシーのデフォルト ACI: 監査員グループに「検索」を許可
- サービス・グループのデフォルト ACI: アクセス権の所有者に「すべて」(「追加」操作を除く) を許可

共有アクセス・モジュールの場合、共有アクセス使用可能化ツールの SAConfig が新しいアクセス・コントロール項目を作成します。

デフォルトのアクセス・コントロール項目 (共有アクセス・モジュールの項目を含む) を表示するには、「IBM Security Identity Manager 管理ガイド」のトピック『デフォルトのアクセス・コントロール項目』を参照してください。アクセス・コントロール項目の作成方法については、「*IBM Security Identity Manager 管理ガイド*」の『アクセス・コントロール項目の作成』を参照してください。

アダプターのアップグレード

IBM Security Identity Manager のアップグレード時、IBM Security Identity Manager バージョン 5.0 および 5.1 のアダプターとプロファイルは、IBM Security Identity Manager バージョン 6.0 でサポートされます。アップグレードが完了したら、アダプターを IBM Security Identity Manager バージョン 6.0 にアップグレードする必要があります。

各アダプターには、IBM Security Identity Manager バージョン 6.0 にアップグレードするための特別な手順が存在する場合があります。詳しくは、そのアダプターの資料およびパッケージを参照してください。

以下の要件は、すべてのアダプターのアップグレードに適用されます。

- IBM Security Identity Manager バージョン 6.0 のアダプターは、アダプターのプロファイル・バージョン 6.0 と共に使用する必要があります。
- Tivoli Directory Integrator 上で実行されるすべてのバージョン 6.0 アダプターについて、ディスパッチャー・バージョン 6.0 が必要です。
- ディスパッチャー・バージョン 6.0 は、バージョン 6.0 のアダプターおよびプロファイルと共にしか使用できません。
- Tivoli Directory Integrator を必要としないすべてのアダプター (ADK ベースのアダプター) の場合、これらのアダプターは、バージョン 6.0 より前のアダプターがインストールされている Windows サーバーにインストールしてはなりません。すべてのアダプターは、DLL を共有しているため、同一のサーバー上で同時にアップグレードする必要があります。

第 16 章 別個のシステムのアップグレードおよびデータ・マイグレーション

既存の Tivoli Identity Manager から、IBM Security Identity Manager バージョン 6.0 が稼働している別個の環境にデータベースおよびディレクトリー・データをマイグレーションするには、以下のタスクを使用します。

これらのタスクでは、ミドルウェアのインストールと、IBM Security Identity Manager バージョン 6.0 へのアップグレードやインストールが必要です。これらのトピックでは、実稼働環境からアップグレードとマイグレーションを行う際のベスト・プラクティスについても説明します。

サポートされるアップグレード・パス

表 29. IBM Security Identity Manager バージョン 6.0 へのアップグレード・パス

開始	終了
WebSphere Application Server 6.1 にデプロイされた Tivoli Identity Manager バージョン 5.0	WebSphere Application Server 7.0 にデプロイされた IBM Security Identity Manager バージョン 6.0
WebSphere Application Server 6.1 または WebSphere Application Server 7.0 にデプロイされた Tivoli Identity Manager バージョン 5.1	WebSphere Application Server 7.0 にデプロイされた IBM Security Identity Manager バージョン 6.0

IBM Security Identity Manager バージョン 6.0 では、サポートされる UNIX ベースのオペレーティング・システム間でのデータ・マイグレーションがサポートされます。HP_UX 環境にあるデータは、サポートされる UNIX 環境のいずれにもマイグレーションできます。 Windows オペレーティング・システム間でもデータをマイグレーションすることができます。ただし、UNIX 環境から Windows 環境へ、または Windows 環境から UNIX 環境へとデータをマイグレーションすることはできません。

データをマイグレーションするには、以前のバージョンの Tivoli Identity Manager に対して最低限のフィックスパックと暫定修正がインストールされている必要があります。

IBM Security Identity Manager インフォメーション・センターを参照して、以下を確認してください。

- サポートされるオペレーティング・システムのサポートされるリリース・レベルおよびフィックスパックの指定。
- アダプターをマイグレーションする場合の手順。

データのマイグレーションに関する既知の問題については、300 ページの『マイグレーション後のトラブルシューティングおよび既知の問題』を参照してください。

マイグレーション・プロセスの概要

データ・マイグレーションは、単一サーバー環境、または複数のコンピューターから構成されるクラスター環境のいずれでも実行できます。ミドルウェアは、どちらの環境でも 1 つ以上のコンピューターにインストールできます。データ・マイグレーションには、さまざまなアクティビティーが含まれます。

Tivoli Identity Manager とそれに関連する前提ミドルウェア・サーバーをマイグレーションするための主なステップを以下に示します。

- Tivoli Identity Manager バージョン 5.0 または 5.1 サーバー環境:
  1. WebSphere Application Server、および Tivoli Identity Manager データベースへの接続を必要に応じて停止します。
  2. 以下のデータをバックアップして、ミドルウェア・サーバーから一時ファイル・ディレクトリーにエクスポートします。
     - データベース・サーバー・コンポーネント
     - ディレクトリー・サーバー・コンポーネント

  注: バックアップとエクスポートが完了すると、Tivoli Identity Manager バージョン 5.0 または 5.1 サーバー環境を実動に戻すことができます。実動データは、後日、新しい IBM Security Identity Manager バージョン 6.0 システムにロードできます。データをテスト環境にマイグレーションしてから、新しいシステムへの実動サービスインを行うことが可能です。新しいシステム上の IBM Security Identity Manager データに対する変更は、Tivoli Identity Manager バージョン 5.0 または 5.1 実動データを最終的なサービスインで再インポートするときに上書きされます。
- IBM Security Identity Manager バージョン 6.0 サーバー環境で以下のステップを実行します。
  1. (必要なリリース・レベルおよびフィックスパック・レベルの) 必須ミドルウェアをインストールします。
  2. 必要に応じて、DB2 Universal Database および IBM Tivoli Directory Server のミドルウェア構成ユーティリティーを実行します。

データベースのマイグレーション

IBM Security Identity Manager バージョン 6.0 では、 Tivoli Identity Manager バージョン 5.0 または 5.1 でサポートされる大半のデータベースからのデータ・マイグレーションがサポートされます。

サポートされるデータベースのリリース・レベルを確認するには、IBM Security Identity Manager インフォメーション・センターの『*データベース・サーバー要件*』を参照してください。

DB2 Universal Database のマイグレーション

DB2 Universal Database データを IBM Security Identity Manager バージョン 6.0 でサポートされるバージョンにマイグレーションするには、以下のタスクを使用します。

DB2 Universal Database データのバックアップ

DB2 Universal Database には、バックアップと復元のコマンドが用意されています。アップグレードの前に、これらのコマンドを使用して、5.0 または 5.1 システムから 6.0 システムにデータを移動します。

始める前に

フリー・ディスク・スペースおよび仮想メモリー要件に適合していることを確認します。また、システムの temp ディレクトリーに、十分なフリー・ディスク・スペースがあることを確認します。ターゲット・システムは、IBM Security Identity Manager インフォメーション・センターに記載されているハードウェアとソフトウェアの要件を満たしている必要があります。

必要な管理権限を持っていることを確認します。Windows システムでは、ログイン・ユーザー ID は Administrators グループに属する必要があります。Linux システムでは、ログイン・ユーザー ID は root である必要があります。

手順

1. DB2 コマンド・ウィンドウを開きます。
   - UNIX および Linux: DB2 インスタンス所有者としてログオンして db2 と入力し、DB2 コマンド・ウィンドウを開きます。
   - Windows: 「**スタート**」 > 「**ファイル名を指定して実行**」をクリックし、db2cmd と入力します。DB2 コマンド・ウィンドウが開いたら、db2 と入力します。
2. Tivoli Identity Manager データベースへの接続をすべて閉じます (WebSphere とその他のすべてのツールを停止します)。
   - 単一の WebSphere サーバーでアップグレードを行う場合は、Tivoli Identity Manager アプリケーション、および Tivoli Identity Manager アプリケーションを実行している WebSphere サーバーを停止します。
   - WebSphere クラスターでアップグレードを行う場合は、Tivoli Identity Manager アプリケーション、および Tivoli Identity Manager アプリケーションを実行している WebSphere クラスターを停止します。
   - 必要な場合は、以下のコマンドを実行して、すべての接続を強制的に閉じます。

     ```
     force application all
     ```
3. Tivoli Identity Manager データベースをバックアップします。

   以下のコマンドを発行します。

   ```
   backup database ITIM_DB to OLD_DB2_BACKUP_DIR
   ```

   ITIM_DB は、Tivoli Identity Manager データベースの名前です。例: itimdb。*OLD_DB2_BACKUP_DIR* は、バックアップを格納するディレクトリー・パスです。例えば、/51data/db2 (Linux または UNIX システムの場合) や C:¥temp¥51data¥db2 (Windows システムの場合) を指定します。

   注: db2admin アカウントがその他のファイル・システム・ロケーションへのアクセス権を持たない場合があります。例えば、UNIX または Linux システムで /home/db2admin の使用が必要になる場合があります。

次のタスク

新しいバージョンの DB2 Universal Database をインストールします。

DB2 Universal Database のインストール、およびターゲット・サーバー環境へのデータのコピー

データをバックアップしたら、このタスクを使用して DB2 データベースを必要なレベルに更新します。

始める前に

必要な管理権限を持っていることを確認します。Windows システムでは、ログイン・ユーザー ID は Administrators グループに属する必要があります。UNIX または Linux システムでは、ログイン・ユーザー ID は root である必要があります。

手順

1. ターゲット・データベース・サーバーで、新しいバージョンの DB2 Universal Database をインストールします。

   IBM Security Identity Manager インフォメーション・センターで、「*IBM Security Identity Manager インストール・ガイド*」の『*IBM DB2 データベースのインストールおよび構成*』を参照してください。この操作はマイグレーションであるため、同じ 5.0 または 5.1 データベース・システム・ユーザー (`enrole` など) を作成するようにしてください。このユーザーには、古いシステムで割り当てられていた権限と特権を割り当てる必要があります。
2. ミドルウェア構成ツールを実行して、DB2 インスタンスを作成します。

   23 ページの『ミドルウェア構成ユーティリティーの実行』を参照してください。ミドルウェア構成ツールを実行して DB2 Universal Database を構成すると、データベース・ユーザー・フィールドがデフォルト値の `itimuser` に設定されます。データベース・ユーザー・フィールドを、前の Tivoli Identity Manager データベースで使用していたデータベース・ユーザーに変更します。データベース・ユーザー名とパスワードは、Tivoli Identity Manager バージョン 5.0 または 5.1 で使用されているものを使用してください。この名前はスキーマ名であり、パスワードは*OLD_ITIM_HOME*¥`data` ディレクトリー内のプロパティー・ファイルに既に保存されています。アップグレード時にこれらの値を変更することはできません。
3. Tivoli Identity Manager データベース・バックアップ・ディレクトリーの内容をターゲット・サーバー (`/60data/db2` など) にコピーします。 作成したデータベース・インスタンス所有者に、ターゲット・ディレクトリーとサブファイルを読み取る権限があることを確認します。

次のタスク

新しいバージョンの DB2 Universal Database にデータを復元します。

DB2 Universal Database データの復元

DB2 Universal Database には、復元コマンドが用意されています。アップグレードの後に、このコマンドを使用して、5.0 または 5.1 システムから 6.0 システムに保存データを復元します。

始める前に

必要な管理権限を持っていることを確認します。Windows システムでは、ログイン・ユーザー ID は Administrators グループに属する必要があります。UNIX または Linux システムでは、ログイン・ユーザー ID は root である必要があります。

このタスクについて

DB2 Universal Database には、バックアップと復元のコマンドが用意されています。アップグレードの前に、これらのコマンドを使用して、5.0 または 5.1 システムから 6.0 システムにデータを移動します。

手順

1. DB2 コマンド・ウィンドウを開きます。
   - UNIX および Linux: DB2 インスタンス所有者としてログオンして `db2` と入力し、DB2 コマンド・ウィンドウを開きます。
   - Windows: 「**スタート**」 > 「**ファイル名を指定して実行**」をクリックし、`db2cmd` と入力します。DB2 コマンド・ウィンドウが開いたら、`db2` と入力します。
2. DB2 コマンド・ウィンドウで、以下のコマンドを入力して、保存された DB2 データを使用してデータベースを復元します。

   ```
   restore db itimdb from OLD_DB2_TEMP_DATA
   ```

   itimdb は、IBM Security Identity Manager データベースの名前です。*OLD_DB2_TEMP_DATA* は、前のバージョンからコピーした DB2 データの場所です (`C:¥temp¥50data¥db2` など)。
3. DB2 サーバーを停止および開始して、構成をリセットします。 次のコマンドを入力します。

   ```
   db2stop
   db2start
   ```

   `db2stop` が失敗してデータベースがアクティブなままである場合は、以下のコマンドを入力します。

   a. `force application all`

      このコマンドによってデータベースは非アクティブになります。

   b. `db2start`.

次のタスク

最新の調整設定を適用して、最適なパフォーマンスが得られるようにデータベースを調整します。IBM Security Identity Manager インフォメーション・センターの「Performance」トピックで、『*Tuning IBM DB2*』を参照してください。

DB2 Universal Database のバックアップと復元については、DB2 インフォメーション・センターを参照してください。

サービス統合バスの消去

WebSphere Application Server 6.1 上で稼働する Tivoli Identity Manager 5.0 または 5.1 を、WebSphere Application Server 7 で稼働する IBM Security Identity Manager バージョン 6.0 にアップグレードする場合は、復元したデータベースからサービス統合バス (SIB) データを消去する必要があります。

始める前に

必要な管理権限を持っていることを確認します。Windows システムでは、ログイン・ユーザー ID は Administrators グループに属する必要があります。UNIX または Linux システムでは、ログイン・ユーザー ID は root である必要があります。

IBM Security Identity Manager データベースが稼働していることを確認します。

手順

1. DB2 コマンド・ウィンドウを開きます。
   - UNIX または Linux: DB2 インスタンス所有者としてログオンして `db2` と入力し、DB2 コマンド・ウィンドウを開きます。
   - Windows: 「**スタート**」 > 「**ファイル名を指定して実行**」をクリックし、`db2cmd` と入力します。DB2 コマンド・ウィンドウが開いたら、`db2` と入力します。
2. 以下のコマンドを使用して、DB2 インスタンス所有者としてデータベースに接続します。

   ```
   connect to itimdb user instance_owner using instance_owner_password
   ```

   各ディレクトリーの説明を以下に示します。
   - *itimdb* は IBM Security Identity Manager データベース名です。
   - *instance_owner* は DB2 インスタンスの所有者です。
   - *instance_password* は DB2 インスタンスの所有者のパスワードです。
3. SIB スキーマのテーブルからすべてのデータを削除するために必要な DELETE SQL ステートメントを DB2 コマンド・ウィンドウに入力します。

   環境の SIB スキーマごとに以下のコマンドを発行します。

   ```
   delete from schema_name.SIB000
   delete from schema_name.SIB001
   delete from schema_name.SIB002
   delete from schema_name.SIBCLASSMAP
   delete from schema_name.SIBKEYS
   delete from schema_name.SIBLISTING
   delete from schema_name.SIBXACTS
   delete from schema_name.SIBOWNER
   delete from schema_name.SIBOWNERO
   ```

   SIB スキーマ *schema_name* は、以下のとおりです。

表 30. サービス統合バス・スキーマ名

Tivoli Identity Manager 環境	スキーマ名
単一サーバー	ITIML000
クラスター	ITIML000、ITIML001、ITIML002、ITIML003、および ITIMS000

注: SIBOWNERO は、すべての Tivoli Identity Manager 環境に存在しない可能性があります。これが存在しない場合に delete ステートメントが失敗したときは、失敗を無視できます。

Oracle データベースのマイグレーション

Oracle データベース・データを IBM Security Identity Manager バージョン 6.0 でサポートされる Oracle データベースのシステムおよびバージョンにマイグレーションおよびインポートするには、以下のタスクを使用します。

Oracle データのエクスポート

論理データベースのバックアップと復元には、Oracle データベース・エクスポート (EXP) およびインポート (IMP) ユーティリティーを使用します。これらのユーティリティーは、あるサーバー、データベース、またはスキーマから別のサーバー、データベース、またはスキーマに Oracle データをマイグレーションするときにも使用されます。

始める前に

必要な管理権限を持っていることを確認します。Windows システムでは、ログイン・ユーザー ID は Administrators グループに属する必要があります。UNIX または Linux システムでは、ログイン・ユーザー ID は root である必要があります。

手順

1. Tivoli Identity Manager バージョン 5.0 または 5.1 用に Oracle データベースを実行しているサーバーで、Oracle データベース・インスタンス所有者としてログインします。
2. 環境変数 *ORACLE_HOME* および *ORACLE_SID* が正しく設定されていることを確認します。 *ORACLE_HOME* は、Oracle のデフォルトのインストール・ディレクトリーです。*ORACLE_SID* は、Tivoli Identity Manager データベース・インスタンスです。
   a. 環境変数のエントリーが以下のように指定されていることを確認します。 この例は、Windows ホーム・ディレクトリーの場合です。

      ```
      ORACLE_HOME=c: ¥oracle¥ora92
      ORACLE_SID=itim
      ```
3. Oracle データベースのダンプ・ファイルとログ・ファイルをエクスポートします。以下のコマンドを 1 行で指定して発行します。

   ```
   exp system/system_pwd file=path¥itim51.dmp log=path¥itim51exp.log
   owner=itim_username
   ```

   system_pwd は、システム・ユーザーのパスワードです。*path* はファイルのパスです (`C:¥51data¥oracle` や `/opt/51data/oracle` など)。*itim_username* は、Tivoli Identity Manager バージョン 5.0 または 5.1 データベースのユーザーです (`enrole` や `itimuser` など)。

4. エクスポートしたディレクトリーの内容をターゲット・サーバー (/61data/oracle など) にコピーします。 作成したデータベース・インスタンス所有者 enrole に、ターゲット・ディレクトリーとサブファイルを読み取る権限があることを確認します。

次のタスク

新しいバージョンの Oracle データベースをインストールします。

Oracle データベースのインストールおよびデータのインポート

データをエクスポートしたら、このタスクを使用して Oracle データベースを必要なレベルに更新します。

始める前に

必要な管理権限を持っていることを確認します。Windows システムでは、ログイン・ユーザー ID は Administrators グループに属する必要があります。UNIX または Linux システムでは、ログイン・ユーザー ID は root である必要があります。

手順

1. ターゲットの IBM Security Identity Manager バージョン 6.0 サーバーで、サポートされるバージョンの Oracle データベースをインストールします。IBM Security Identity Manager インフォメーション・センターで、「*IBM Security Identity Manager インストール・ガイド*」の 32 ページの『Oracle データベースのインストールおよび構成』を参照してください。
2. Oracle データベース・インスタンスを構成します。 以下の enrole_admin.sql ファイルを使用すると、新しい Oracle データベース・インスタンスをマイグレーション用に簡単に構成できます。 *itimuserTag* を Tivoli Identity Manager バージョン 5.0 または 5.1 データベース・ユーザー (enrole など) で置き換えてください。*itimuserPwdtag* を Tivoli Identity Manager バージョン 5.0 または 5.1 データベース・ユーザーのパスワードで置き換えてください。データベース・ユーザー ID およびパスワードが前のバージョンと同じでないと、IBM Security Identity Manager のアップグレードは失敗します。

```
CREATE TABLESPACE enrole_data
DATAFILE 'enrole1_data_001.dbf'
SIZE 64M
AUTOEXTEND ON
NEXT 64M
MAXSIZE unlimited
DEFAULT STORAGE (INITIAL 10M
                                 NEXT 1M
                                 PCTINCREASE 10)
PERMANENT
ONLINE
LOGGING;

CREATE TABLESPACE enrole_indexes
DATAFILE 'enrole1_idx_001.dbf'
SIZE 32M
AUTOEXTEND ON
NEXT 32M
MAXSIZE unlimited
DEFAULT STORAGE (INITIAL 10M
                                 NEXT 1M
                                 PCTINCREASE 10)
```

```
PERMANENT
ONLINE
LOGGING;
CREATE USER itimuserTag IDENTIFIED BY itimuserPwdtag
  DEFAULT TABLESPACE enrole_data
  QUOTA UNLIMITED ON enrole_data
  QUOTA UNLIMITED ON enrole_indexes;
GRANT CREATE SESSION TO itimuserTag;
GRANT CREATE TABLE to itimuserTag;
GRANT CREATE ANY PROCEDURE to itimuserTag;
GRANT CREATE VIEW to itimuserTag;
```

3. 環境変数 *ORACLE_HOME* および *ORACLE_SID* が正しく設定されていることを確認します。 *ORACLE_HOME* は、Oracle のデフォルトのインストール・ディレクトリーです。*ORACLE_SID* は、Tivoli Identity Manager データベース・インスタンスです。
4. **sqlplus** ユーティリティーを使用して、上記の enrole_admin.sql ファイルを実行します。

   ```
   sqlplus system/system_pwd @path¥enrole_admin.sql
   ```

   system_pwd は、システム・ユーザーのパスワードです。*path* はファイルのパスです。このスクリプト・ファイルを実行すると、必要な IBM Security Identity Manager テーブル・スペースが作成され、必要な権限を持つ (itimuserTag で指定された) データベース・ユーザーが作成されます。
5. テーブル・スペースを作成したら、以下のコマンドを 1 行で入力して、 Tivoli Identity Manager バージョン 5.0 または 5.1 のエクスポート・データをインポートします。

   ```
   imp system/system_pwd file=path¥itim51.dmp log=path¥itim516exp.log
    fromuser=itim_username
   ```

   system_pwd は、システム・ユーザーのパスワードです。*path* はファイルのパスです (C:¥51data¥oracle や /opt/51data/oracle など)。*itim_username* は、Tivoli Identity Manager バージョン 5.0 または 5.1 データベースのユーザーです (enrole や itimuser など)。

次のタスク

アップグレードとインストールが完了したら、最新の調整設定を適用して、最適なパフォーマンスが得られるようにデータベースを調整する必要があります。 IBM Security Identity Manager インフォメーション・センターの「*Performance*」トピックで、『*Tuning Oracle*』を参照してください。

サービス統合バスの消去

Tivoli Identity Manager 5.0 または 5.1 から IBM Security Identity Manager バージョン 6.0 への個別システム・アップグレードを行う場合は、復元したデータベースからサービス統合バス (SIB) データを消去する必要があります。

始める前に

フリー・ディスク・スペースおよび仮想メモリー要件に適合していることを確認します。また、システムの temp ディレクトリーに、十分なフリー・ディスク・スペースがあることを確認します。ターゲット・システムは、IBM Security Identity

Manager インフォメーション・センターの『*ハードウェア要件およびソフトウェア要件*』に記載されているハードウェアとソフトウェアの要件を満たしている必要があります。

必要な管理権限を持っていることを確認します。Windows システムでは、ログイン・ユーザー ID は Administrators グループに属する必要があります。Linux システムでは、ログイン・ユーザー ID は root である必要があります。

IBM Security Identity Manager データベースが稼働していることを確認します。

手順

1. ターゲットの IBM Security Identity Manager バージョン 6.0 Oracle サーバーで、Oracle データベースを開始します。
2. 環境の SIB スキーマごとに以下のコマンドを発行します。

```
delete from schema_name.SIB000
delete from schema_name.SIB001
delete from schema_name.SIB002
delete from schema_name.SIBCLASSMAP
delete from schema_name.SIBKEYS
delete from schema_name.SIBLISTING
delete from schema_name.SIBXACTS
delete from schema_name.SIBOWNER
delete from schema_name.SIBOWNERO
```

SIB スキーマ *schema_name* は、以下のとおりです。

表 31. サービス統合バス・スキーマ名

Tivoli Identity Manager 環境	スキーマ名
単一サーバー	ITIML000
クラスター	ITIML000、ITIML001、ITIML002、ITIML003、および ITIMS000

注: SIBOWNERO は、すべての Tivoli Identity Manager 環境に存在しない可能性があります。これが存在しない場合に delete ステートメントが失敗したときは、失敗を無視できます。

次のタスク

ディレクトリー・サーバーをマイグレーションします。

SQL Server のマイグレーション

Microsoft SQL Server データを IBM Security Identity Manager バージョン 6.0 でサポートされる SQL Server のシステムおよびバージョンにインポートするには、以下のタスクを使用します。

SQL Server データのバックアップ

サーバー、データベース、またはスキーマ間で SQL Server データを移動するには、Microsoft SQL Server のバックアップおよび復元ユーティリティーを使用します。アップグレードの前に、5.0 または 5.1 システムから 6.0 システムにデータを移動します。

始める前に

必要な管理権限を持っていることを確認します。Windows システムでは、ログイン・ユーザー ID は Administrators グループに属する必要があります。

手順

1. Tivoli Identity Manager バージョン 5.0 または 5.1 用の SQL Server を実行しているサーバーで、Microsoft SQL Server Management Studio を開始し、Tivoli Identity Manager データベースに移動します。
2. Tivoli Identity Manager データベース (itimdb) を右クリックし、「**タスク**」 > 「**バックアップ**」を選択します。
3. 「**追加**」をクリックして、ファイル名を指定します (itimdb.bak など)。
4. その他のオプションについてはデフォルト値を受け入れて、「**OK**」をクリックします。

次のタスク

『SQL Server のインストールとデータのインポート』に進みます。

SQL Server のインストールとデータのインポート

必要なレベルの Microsoft SQL Server をインストールします。

始める前に

必要な管理権限を持っていることを確認します。Windows システムでは、ログイン・ユーザー ID は Administrators グループに属する必要があります。

手順

1. IBM Security Identity Manager 用の SQL Server を実行しているサーバーに、SQL Server 2008 をインストールします。

   新しいシステムでは、Tivoli Identity Manager バージョン 5.0 または 5.1 と同じデータベース・システム・ユーザーを使用してください。
2. IBM Security Identity Manager バージョン 6.0 データベースを作成したら、データベースを右クリックして、「**タスク**」 > 「**復元**」 > 「**データベース**」をクリックします。
3. 「データベースの復元」ウィンドウの「全般」ページで、以下の手順を実行します。
   a. 復元オプションとして、「**デバイスから**」ソースを選択します。
   b. 省略符号 (**...**) をクリックします。
   c. 「**追加**」をクリックします。
   d. Tivoli Identity Manager バージョン 5.0 または 5.1 データベースのバックアップ・ファイル名 (itimdb.bak) に対して、「**復元**」チェック・ボックスを選択します。
4. 「オプション」ページで以下の手順を実行します。
   a. 「**既存のデータベースを上書きする**」を選択します。
   b. 「**OK**」をクリックします。

5. IBM Security Identity Manager バージョン 6.0 用に SQL Server データベースを構成します。
   a. SQL Server Enterprise Manager を始動します。
   b. IBM Security Identity Manager バージョン 6.0 で使用されるデータベースに移動します。
   c. データベースを右クリックして、「**新しいクエリ**」をクリックします。
   d. 以下のユーザー・スクリプトを入力して SQL を構成します。

```
sp_addlogin itimuserTag, itimuserPwdTag;
sp_adduser itimuserTag, itimuserTag, db_owner;
use master;
sp_grantdbaccess itimuserTag, itimuserTag;
sp_addrolemember [SqlJDBCXAUser], itimuserTag;
use itimdbTag;
sp_change_users_login  'Update_One', 'itimuserTag', 'itimuserTag'
```

   - *itimuserTag* を Tivoli Identity Manager バージョン 5.0 または 5.1 データベース・ユーザーで置き換えてください。例えば enrole などです。
   - *itimuserPwdTag* を Tivoli Identity Manager バージョン 5.0 または 5.1 データベース・ユーザーのパスワードで置き換えてください。
   - *itimdbTag* をデータベース・インスタンス名で置き換えてください。

   注: *itimuserTag* データベースは、*itimdbTag* データベースを使用して既に復元されている場合があります。既に復元されているためにユーザー・スクリプトが失敗した場合、その失敗は無視してかまいません。
6. SQL Server 2008 を再始動します。

次のタスク

『サービス統合バスの消去』に進みます。

サービス統合バスの消去

復元したデータベースからサービス統合バス (SIB) データを消去します。

始める前に

必要な管理権限を持っていることを確認します。Windows システムでは、ログイン・ユーザー ID は Administrators グループに属する必要があります。

IBM Security Identity Manager データベースが稼働していることを確認します。

手順

1. IBM Security Identity Manager バージョン 6.0 用の SQL Server を実行しているサーバーで、Microsoft SQL Server Management Studio を開始します。
2. IBM Security Identity Manager バージョン 6.0 で使用されるデータベースに移動します。
3. データベースを右クリックして、「**新しいクエリ**」をクリックします。
4. SIB スキーマのテーブルからデータをすべて削除するために必要な DELETE SQL ステートメントを入力します。

   環境の SIB スキーマごとに以下のコマンドを発行します。

```
delete from schema_name.SIB000
delete from schema_name.SIB001
delete from schema_name.SIB002
delete from schema_name.SIBCLASSMAP
delete from schema_name.SIBKEYS
delete from schema_name.SIBLISTING
delete from schema_name.SIBXACTS
delete from schema_name.SIBOWNER
delete from schema_name.SIBOWNERO
```

SIB スキーマ *schema_name* は、以下のとおりです。

表 32. サービス統合バス・スキーマ名

Tivoli Identity Manager 環境	スキーマ名
単一サーバー	ITIML000
クラスター	ITIML000、ITIML001、ITIML002、ITIML003、および ITIMS000

注: SIBOWNERO は、すべての Tivoli Identity Manager 環境に存在しない可能性があります。これが存在しない場合に delete ステートメントが失敗したときは、失敗を無視できます。

次のタスク

ディレクトリー・サーバーをアップグレードします。

ディレクトリー・サーバーのマイグレーション

IBM Security Identity Manager バージョン 6.0 では、 Tivoli Identity Manager バージョン 5.0 または 5.1 でサポートされる大半のディレクトリー・サーバーからのデータ・マイグレーションがサポートされます。

IBM Security Identity Manager インフォメーション・センターの「*IBM Security Identity Manager 製品概要*」に記載されている『ディレクトリー・サーバーの要件』を参照してください。

Tivoli Directory Server のマイグレーション

Tivoli Directory Server データを IBM Security Identity Manager バージョン 6.0 でサポートされるバージョンにマイグレーションするには、以下のタスクを使用します。

Tivoli Identity Manager バージョン 5.0 は、IBM Tivoli Directory Server バージョン 6.0、6.1、および 6.2 をサポートしています。Tivoli Identity Manager バージョン 5.1 は、IBM Tivoli Directory Server バージョン 6.1、6.2、および 6.3 をサポートしています。ディレクトリー・サーバー・データを IBM Security Identity Manager バージョン 6.0 でサポートされるバージョンにマイグレーションする必要があります。

IBM Security Identity Manager インフォメーション・センターの「*IBM Security Identity Manager 製品概要*」に記載されている『ディレクトリー・サーバーの要件』を参照してください。

ディレクトリー・サーバー・データのバックアップ

IBM Security Identity Manager バージョン 6.0 でサポートされるディレクトリー・サーバー・バージョンに移行する前に、ディレクトリー・サーバー・データをファイルにエクスポートします。

手順

1. root 特権を持つ管理者としてログインします。

   注: LDAP サーバーを停止する必要はありません。
2. コマンド・ウィンドウを開きます。
3. *<TDS_HOME>*/sbin ディレクトリーに移動し、以下のコマンドを入力します。

   ```
   db2ldif -s ldap_suffix -o ldap_output_file -I ldap_instance_name
   ```

   各ディレクトリーの説明を以下に示します。
   - *ldap_suffix* は、Tivoli Identity Manager の構成が行われるサフィックスの名前です。例: dc=com
   - *ldap_output_file* は、ldif 出力ファイルの名前です。例えば、old_ldif_data.ldif です。
   - *ldap_instance_name* は、LDAP サーバー・インスタンスの名前です。この名前は、IBM Tivoli Directory Server インスタンス管理ツールで確認できます。

次のタスク

『ターゲット・サーバーへの Tivoli Directory Server のインストール』に進みます。

ターゲット・サーバーへの Tivoli Directory Server のインストール

IBM Security Identity Manager バージョン 6.0 でサポートされるバージョンの IBM Tivoli Directory Server をインストールします。

始める前に

ディレクトリー・サーバー・データがバックアップされていることを確認してください。

手順

1. ターゲットの IBM Security Identity Manager バージョン 6.0 サーバーで、root 特権を持つ管理者としてログオンします。
2. サポートされるバージョンの IBM Tivoli Directory Server をインストールします。

   を参照してください。
3. ミドルウェア構成ツールを実行して、IBM Tivoli Directory Server インスタンスを作成します。

   23 ページの『ミドルウェア構成ユーティリティーの実行』を参照してください。

- Tivoli Identity Manager バージョン 5.0 または 5.1 と同じ root サフィックスが作成され、使用されることを確認してください。
- 暗号化シード値は、古い Tivoli Directory Server インスタンスと同じものを使用してください。そうしないと、新しい Tivoli Directory Server インスタンスからシードおよびソルト・キーを使用する際に、古いインスタンスからデータをエクスポートしなければなりません。

4. Tivoli Identity Manager バージョン 5.*x* サーバーで使用されている Tivoli Directory Server インスタンス・ホーム・ディレクトリーの *OLD_ITDS_INSTANCE_HOME*¥etc ディレクトリーから、スキーマ・ファイル V3.modifiedschema をコピーします。このファイルを、IBM Security Identity Manager バージョン 6.0 サーバーで使用される Tivoli Directory Server インスタンスの *NEW_ITDS_INSTANCE_HOME*¥etc ディレクトリーに貼り付けます。

   注: スキーマ・ファイルをカスタマイズまたは変更した場合は、変更内容を新しいスキーマ・ファイルに手動でマージしてください。
5. 変更を有効にするために、Tivoli Directory Server を停止し、再び開始します。

次のタスク

『ディレクトリー・サーバー・データのインポート』に進みます。

ディレクトリー・サーバー・データのインポート

アップグレード・プロセス中に、前のステップで保存したディレクトリー・サーバー・データをインポートします。

手順

1. root 特権を持つ管理者としてログインします。
2. LDAP サーバーを停止します。
3. *TDS_HOME*/sbin から以下のコマンドを実行します。

   ```
   bulkload -i OLD_ITDS_TEMP_DATA¥ldif_output_file -I ldap_instance_name
   ```

   ここで、
   - *OLD_ITDS_TEMP_DATA* は、前のバージョンからコピーした Tivoli Directory Server データの一時ディレクトリーの場所です (例えば C:¥temp¥51data¥ids¥)。
   - *ldif_output_file* は、前のタスクでエクスポートしたファイルの名前です (例えば old_ldif_data.ldif)。
   - *ldap_instance_name* は、LDAP サーバー・インスタンスの名前です。例えば、itimldap です。インスタンス名は、Tivoli Directory Server インスタンス管理ツールを使用して確認できます。

タスクの結果

bulkload コマンドの実行中に、以下のエラーが発生することがあります。

- 入力 LDIF ファイルのいずれかのエントリーが LDAP に存在する場合は、bulkload ユーティリティーが失敗します。このエラーは、定義したサフィックスがディレクトリー・サーバーのエントリーとして存在する場合に発生することがあります。場合によっては、このコマンドを実行する前に、LDAP からサフィッ

クス内のすべてのエントリーを削除する必要があります (ただしサフィックス自体は残します)。エントリーの有無を確認するには **ldapsearch** コマンドを使用し、エントリーの削除には **ldapdelete** コマンドを使用できます。

- エラー・コード:

```
GLPCRY007E The directory key stash file is inconsistent with the
           associated encrypted data.

GLPBLK071E Bulkload is unable to run because of an initialization error.

GLPBLK030E Run DB2CMD.EXE first, and then run bulkload within the "DB2 CMD"
command interpreter.
```

これらのエラーを修正するには、ターゲット・インスタンスの暗号化シード値およびソルト値を調べる必要があります。ターゲット・インスタンスとは、bulkload の実行場所であるディレクトリー・サーバー・インスタンスです。

1. ターゲット・インスタンスのソルト値を確認するには、*TDS_HOME*/bin から以下のコマンドを実行します。

   ```
   ldapsearch -D bind DN  -w password -h hostname  -p port
    -s base -b cn=crypto,cn=localhost cn=*
   ```

   ここで、

   – *bind DN* は、ディレクトリー・サーバーの識別名 (DN) です。
   – *password* は、DN のパスワードです。
   – *hostname* は、Tivoli Directory Server がインストールされているコンピューターの名前です。
   – *port* は、Tivoli Directory Server が listen しているポート番号です。

2. *ibm-slapdCryptoSync* の値 *ibm-slapdCryptoSalt* を、**ldapsearch** コマンドから *ldap_output_file* ファイルに返された値で置き換えます。このファイルは、**db2ldif** コマンドの出力として生成されます (*old_ldif_data.ldif* など)。
3. **bulkload** コマンドを再度実行します。

   ヒント: **bulkload** コマンドで「-W OUT_FILE_NAME」オプションを使用することができます。このオプションを指定すると、コマンドからの出力が指定したファイルに書き込まれます。**bulkload** コマンドでは、DB2 コマンドの複数のインスタンスを実行してデータがロードされます。インスタンスごとに、成功、エラー、または警告のメッセージが発生します。-W オプションを指定して出力を保存しないと、結果を調べることが困難になります。

次のタスク

最新の調整設定を適用して、最適なパフォーマンスが得られるように LDAP を調整します。詳しくは、「*IBM Security Identity Manager Performance Tuning Guide*」の『*Tuning Tivoli Directory Server*』を参照してください。

Oracle Directory Server データのマイグレーション

Oracle (旧称 Sun) Directory Server データを IBM Security Identity Manager バージョン 6.0 でサポートされるバージョンにマイグレーションするには、以下のタスクを使用します。

IBM Security Identity Manager インフォメーション・センターの「*IBM Security Identity Manager 製品概要*」に記載されている『ディレクトリー・サーバーのサポート』を参照してください。

Oracle Directory Server を Oracle Directory Server Enterprise Edition 6.3.1、7.0、または 11.1.1 にマイグレーションする方法について詳しくは、Oracle Web サイト (http://www.oracle.com) を参照してください。

同じシステムでの Sun Directory Server Enterprise Edition のインストールとデータのインポート

ディレクトリー・サーバー・データをバックアップしたら、IBM Security Identity Manager バージョン 6.0 でサポートされるバージョンの Sun Directory Server Enterprise Edition をインストールします。

始める前に

IBM Security Identity Manager インフォメーション・センターで、「*製品概要*」の『ディレクトリー・サーバーのサポート』を参照してください。

ディレクトリー・サーバー・データを必ずバックアップするようにしてください。

root 特権を持つ管理者としてログインする必要があります。

手順

1. サポートされるバージョンの Directory Server Enterprise Edition を (同じシステムに) インストールし、LDAP インスタンスを作成します。 以下に例を示します。

   ```
   DSEE7.0_HOME/bin/dsadm create -p 389 -P 636 /export/home/itimldap
   ```

2. 以前のバージョンの Sun ONE Directory Server と同じ root サフィックスを作成します。 以下に例を示します。

   ```
   DSEE7.0_HOME/bin/dsconf create-suffix -h localhost -p 389 -e dc=com
   ```

3. **dsmig** コマンドを使用して、同じシステム上のスキーマ、構成、およびデータをマイグレーションします。 以下に例を示します。

   ```
   DSEE7.0_HOME/bin/dsmig migrate-schema old-instance-path new-instance-path
   DSEE7.0_HOME/bin/dsmig migrate-config old-instance-path new-instance-path
   DSEE7.0_HOME/bin/dsmig migrate-data old-instance-path new-instance-path
   ```

   1 つのコマンドで、同じシステム上のスキーマ、構成、およびデータをマイグレーションすることもできます。 以下に例を示します。

   ```
   DSEE7.0_HOME/bin/dsmig migrate-all old-instance-path new-instance-path
   ```

次のタスク

IBM Security Identity Manager のアップグレードとインストールが完了したら、最新の調整設定を適用して最適なパフォーマンスが得られるように LDAP を調整します。IBM Security Identity Manager インフォメーション・センターの「*Performance*」トピックで、『*Tuning Sun Enterprise Directory Server*』を参照してください。

IBM Security Identity Manager 6.0 へのアップグレード

このトピックでは、シングル・サーバー環境とクラスター環境の両方で IBM Security Identity Manager バージョン 6.0 にアップグレードする方法について説明します。

サポートされるアップグレード・パスは以下のとおりです。

表 33. IBM Security Identity Manager バージョン 6.0 へのアップグレード・パス

開始	終了
WebSphere Application Server 6.1 にデプロイされた Tivoli Identity Manager バージョン 5.0	WebSphere Application Server 7.0 にデプロイされた IBM Security Identity Manager バージョン 6.0
WebSphere Application Server 6.1 または WebSphere Application Server 7.0 にデプロイされた Tivoli Identity Manager バージョン 5.1	WebSphere Application Server 7.0 にデプロイされた IBM Security Identity Manager バージョン 6.0

既存の Tivoli Identity Manager バージョン・ホーム・ディレクトリーのターゲット環境へのコピー

インストール・プログラムを実行して IBM Security Identity Manager バージョン 6.0 にアップグレードするには、既存の Tivoli Identity Manager ホーム・ディレクトリーをターゲット環境にコピーします。

始める前に

必要な管理権限を持っていることを確認します。Windows システムでは、ログイン・ユーザー ID は Administrators グループに属する必要があります。

このタスクについて

ホーム・ディレクトリーをコピーするときは、前のバージョンの Tivoli Identity Manager の *OLD_ITIM_HOME* ロケーションを保持します。例えば、*OLD_ITIM_HOME* ディレクトリーが `C:¥itim51 (Windows)` または `/opt/IBM/itim51 (UNIX または Linux)` だった場合は、インストール・プログラムを実行する前に、新しいサーバー上の同じパスにこのディレクトリーをコピーします

手順

ディレクトリーをコピーします。

- UNIX システムまたは Linux システムの場合
  1. UNIX または Linux のルート・ディレクトリーに移動します。
  2. *OLD_ITIM_HOME* の絶対パスを入力して、tar ファイルを作成します。次に例を示します。

     ```
     tar –cvf itim.tar OLD_ITIM_HOME
     ```

IBM Security Identity Manager をクラスター環境で稼働している場合は、デプロイメント・マネージャーとクラスター・メンバー用に tar ファイルを別々に作成します。

3. tar ファイル itim.tar をターゲット・サーバーの root ディレクトリーにコピーします。クラスター環境の場合は、tar ファイルを、古いデプロイメント・マネージャーから新しいデプロイメント・マネージャーへと、また古いクラスター・メンバーから新しいクラスター・メンバーへとコピーします。
4. 以下のコマンドを使用して、1 つ以上のサーバーで *OLD_ITIM_HOME* ディレクトリーを抽出します。

   ```
   tar –xvf itim.tar
   ```

- Windows システムの場合
  1. *OLD_ITIM_HOME* ディレクトリーの圧縮ファイルを作成します。クラスター環境の場合は、デプロイメント・マネージャー用とクラスター・メンバー用に別々の圧縮ファイルを作成します。
  2. 圧縮ファイルをターゲット・サーバーにコピーします。クラスター環境の場合は、圧縮ファイルを古いデプロイメント・マネージャーから新しいデプロイメント・マネージャーへと、また古いクラスター・メンバーから新しいクラスター・メンバーへとコピーします。
  3. 1 つ以上のサーバーで *OLD_ITIM_HOME* ディレクトリーを IBM Security Identity Manager がインストールされているドライブ・ロケーションに抽出します。

次のタスク

IBM Security Identity Manager インストール・プログラムを実行します。

IBM Security Identity Manager インストール・プログラムの実行

既存のデータのコピーとバックアップが完了したら、IBM Security Identity Manager サーバーをインストールする必要があります。

始める前に

IBM Security Identity Manager バージョン 6.0 のインストール・プログラムを実行する前に、それぞれのディレクトリー・サーバーとデータベース・サーバーにコピーしたディレクトリー・データとデータベース・データをインポートまたは復元したことを確認します。また、以下のミドルウェアが、サポートされるリリース・レベルおよびフィックスパックで稼働していることを確認します。

- WebSphere Application Server
- DB2 Universal Database またはその他のサポートされるミドルウェア
- IBM Tivoli Directory Server またはその他のサポートされるミドルウェア

IBM Security Identity Manager インフォメーション・センターの「*製品概要*」で、『*ハードウェア要件およびソフトウェア要件*』を参照してください。上記のミドルウェア製品のインストールと構成の手順については、IBM Security Identity Manager インフォメーション・センターの 17 ページの『第 4 章 前提コンポーネントのインストール』を参照してください。

このタスクについて

IBM Security Identity Manager をクラスター環境にインストールする場合は、IBM Security Identity Manager をクラスター・メンバーにインストールする前に、IBM Security Identity Managerをデプロイメント・マネージャーにインストールしてデータベースおよびディレクトリー・サーバーをアップグレードする必要があります。

IBM Security Identity Manager バージョン 6.0 にアップグレードするには、以下の手順を実行します。

手順

1. IBM Security Identity Manager をインストールするコンピューターで、システム管理特権を持つアカウントにログオンします。 Windows システムでは、ログイン・ユーザー ID は Administrators グループに属する必要があります。Linux システムでは、ログイン・ユーザー ID は root である必要があります。
2. インストール・プログラムをダウンロードするか、または DVD ドライブに IBM Security Identity Manager 製品 DVD を挿入します。
3. インストール・プログラムを実行します。
   - Windows システムの場合
     a. 「**スタート**」 > 「**ファイル名を指定して実行**」をクリックします。
     b. インストール・プログラムが置かれているドライブおよびパスを入力してから、コマンドを入力します。

     ```
     instwin.exe
     ```
   - UNIX システムまたは Linux システムの場合
     a. コマンド・シェル・プロンプト・ウィンドウを開き、インストール・プログラムのあるディレクトリーに移動します。
     b. インストール・プログラムを実行するコマンドとして以下のいずれかを入力します。

     AIX システム
     ```
     instaix.bin
     ```

     Linux システム
     ```
     instlinux.bin
     ```

     pLinux システム
     ```
     instplinux.bin
     ```

     zLinux システム
     ```
     instzlinux.bin
     ```

     Solaris システム
     ```
     instsol.bin
     ```

     注: UNIX または Linux システムでインストール・プログラムを実行する場合は、/tmp ディレクトリーに少なくとも 150 MB のフリー・スペースが必要です。十分なスペースがない場合は、十分なフリー・ディスク・スペースがあるディスク・パーティション上のディレクトリーに IATEMPDIR 環境変数を設定する必要があります。変数を設定するためには、次に示すコマンドのうちの 1 つをコマンド行プロンプトに入力し、それからインストール・プログラムを再実行します。

Bourne shell (sh)、ksh、bash、および zsh

```
$ IATEMPDIR=temp_dir
$ export IATEMPDIR
```

C shell (csh) および tcsh

```
$ setenv IATEMPDIR temp_dir
```

temp_dir はディレクトリーのパスで、例えば、/your/free/directory の場合、使用可能なフリー・ディスク・スペースがあります。

「ようこそ」ウィンドウが開きます。

4. 言語を選択し、「**OK**」をクリックします。
5. 条件に同意する場合は、使用許諾契約書を受け入れて、「**次へ**」をクリックします。
6. 「インストール・ディレクトリーの選択 (Choose Install Directory)」ウィンドウで、アップグレードする既存の Tivoli Identity Manager のホーム・ディレクトリーを選択する必要があります。デフォルトのディレクトリーを受け入れるか、または「**選択**」をクリックして該当のディレクトリーを選択します。「**次へ**」をクリックします。
7. 「IBM Security Identity Manager のアップグレード」ウィンドウで、「**次に進む**」をクリックしてアップグレードを開始します。
8. 「注意」ウィンドウを読んで、前提条件のアプリケーションが IBM Security Identity Manager がサポートする要件に適合していることを確認します。「**次へ**」をクリックします。
9. 「WebSphere Application Server」ウィンドウの「インストール・ディレクトリー」で WebSphere Application Server ディレクトリーを確認して、「次へ」をクリックします。
10. 「WebSphere プロファイルの選択」ウィンドウで WebSphere Application Server プロファイル名を選択して、「**次へ**」をクリックします。
11. IBM Security Identity Manager をクラスター環境で稼働している場合は、アプリケーション名とメッセージング・クラスター名を入力して、「**次へ**」をクリックします。

    注: 入力するクラスター名は、前のバージョンの Tivoli Identity Manager と一致していなくてもかまいませんが、WebSphere Application Server の構成に存在している必要があります。WebSphere Application Server を IBM Security Identity Manager 用に構成する方法について詳しくは、IBM Security Identity Manager インフォメーション・センターの 58 ページの『WebSphere Application Server のインストールおよび構成』を参照してください。
12. WebSphere Application Server の「データ」ウィンドウで、アプリケーション・サーバー名を入力するか受け入れます。新しいコンピューターのホスト名が正しく表示されることを確認して、「**次へ**」をクリックします。
13. IBM Security Identity Manager をクラスター環境で実行している場合は、WebSphere Application Server と IBM Security Identity Manager をインストールするシステムのホスト名を確認します。「**次へ**」をクリックします。
14. WebSphere の管理セキュリティーとアプリケーション・セキュリティーが有効になっている場合は、「WebSphere Application Server の管理者クリデンシャ

ル」ウィンドウで WebSphere Application Server 管理者のユーザー ID とパスワードを入力して、「**次へ**」をクリックします。

15. Java Database Connectivity (JDBC) ドライバーの入力を要求された場合は、JDBC ドライバーのディレクトリー・ロケーションとドライバー名を入力して、「**次へ**」をクリックします。

    注: WebSphere Application Server 7.0 で Tivoli Identity Manager 5.0 から Tivoli Identity Manager 5.1 にアップグレードする場合は、JDBC ドライバー・セットアップ・パネルが表示されません。Oracle データベースの場合は、追加の手動ステップが必要です。

    a. WebSphere Application Server 7.0 フィックスパック 5 上で Tivoli Identity Manager 5.1 をデプロイした後に、ojdbc.jar ファイルを *ISIM_HOME*/lib から削除し、ojdbc6.jar で置き換えます。次に、ojdbc6.jar の名前を ojdbc.jar に変更します。この名前変更が必要なのは、WebSphere Application Server 7.0 が JDK1.6 を使用するためです。

16. 「Tivoli Common Directory」ウィンドウで Tivoli Common Directory または別のディレクトリーのロケーションを選択して、「**次へ**」をクリックします。選択したディレクトリーは、ログや First Failure Capture データなどのすべての保守関連ファイルのセントラル・ロケーションになります。

17. 「プリインストールの要約 (Pre-Installation Summary)」ウィンドウで情報が正しいことを確認して、「**インストール**」をクリックします。

18. 「システム構成ツール (System Configuration tool)」ウィンドウが画面に表示されたら、 IBM Security Identity Manager バージョン 6.0 の値を正しく入力します。各タブで、以下のディレクトリー、データベース、およびメール・サーバーの各フィールドの値が正しいことを確認するか、または値を更新します。これらの値は、以前のバージョンの Tivoli Identity Manager で使用されていた古い情報から変更する必要があります。

    - データベース
      - JDBC URL

        JDBC URL を入力します。この URL には、IBM Security Identity Manager バージョン 6.0 のデータベース・ホスト名、ポート番号、およびデータベース名が正しく指定されている必要があります。例えば、DB2 データベース「itimdb」をポート 50000 上のホスト 10.1.1.1 で実行している場合は、jdbc:db2://10.1.1.1:50000/itimdb と入力します。

        注: ホスト名は、完全修飾ドメイン名、IPv4 または [IPv6] アドレスにすることができます。 IPv6 アドレスは、大括弧で囲む必要があります。

      情報を入力したら、「**テスト**」をクリックして接続をテストします。

      注: 「データベース・ユーザー」フィールドと「ユーザー・パスワード」フィールドは、使用不可になっています。 IBM Security Identity Manager バージョン 6.0 のデータベース・ユーザーを作成するときは、以前の Tivoli Identity Manager サーバーで使用したのと同じデータベース・ユーザー ID とパスワードを必ず使用してください。

    - ディレクトリー
      - 基本 DN

- パスワード
- ホスト名
- ポート

情報を入力したら、「**テスト**」をクリックして接続をテストします。

- メール
  - Identity Manager サーバーのベース URL

19. すべてのタブですべてのフィールドを変更または確認したら、「**OK**」をクリックします。 データベース・アップグレード・プログラムが開始されて、データベース・スキーマおよびデータがアップグレードされます。データベースのアップグレードが完了するまでには、かなり時間がかかる場合があり、その進行状況は表示されません。このアップグレードが完了すると、LDAP アップグレード・プログラムが開始されて、 LDAP スキーマおよびデータがアップグレードされます。このアップグレードにもある程度の時間がかかる場合があります。 *ISIM_HOME*¥install_logs ディレクトリー内のログ・ファイルを調べると、アップグレードの進行状況を確認することができます。特に、以下のログ・ファイルを調べてください。
    - itim_install_activity.log
    - dbUpgrade.stdout
    - ldapUpgrade.stdout
    - runConfigFirstTime.stdout
20. インストール・プログラムが終了したら、「**完了**」をクリックします。

次のタスク

IBM Security Identity Manager バージョン 6.0 システムにログオンできることを確認します。ログオンには、前のバージョンの Tivoli Identity Manager で使用していたユーザー ID とパスワードを使用します。

インストール後のタスク

IBM Security Identity Manager バージョン 6.0 にマイグレーションした後、以下のタスクを実行します。

Sun Enterprise Directory Server バージョン 6.3 の再始動および再索引付け

このタスクは、IBM Security Identity Manager バージョン 6.0 を Sun Enterprise Directory Server に接続できるようにする場合に使用します。

始める前に

IBM Security Identity Manager バージョン 6.0 がインストールされている必要があります。

このタスクについて

Sun ONE Directory Server からデータをマイグレーションした場合は、 IBM Security Identity Manager バージョン 6.0 のインストールが完了した後に IBM Security Identity Manager を停止する必要があります。その後にディレクトリー・サ

ーバーを始動し、ディレクトリー・サーバーに再索引付けを行います。そうしないと、IBM Security Identity Manager をディレクトリー・サーバーに接続できません。

Sun Enterprise Directory Server に再索引付けを行うには、以下の手順を実行します。

手順

1. Sun Enterprise Directory Server コンソールから、「**構成**」タブをクリックします。
2. ディレクトリー・サーバーに再索引付けを行います。
   a. ディレクトリー・サーバーを選択します。
   b. **データ**・ツリーを開きます。
   c. エクスポートされた root サフィックスをクリックします。
   d. 「**再索引 (Reindex)**」を選択します。
3. 「**すべてチェック (Check All)**」を選択します。
4. 「**OK**」をクリックします。

WebSphere Application Server のデフォルトの listen ポートの更新 (クラスターのみ)

このタスクは、クラスター環境でのインストール後に WebSphere Application Server のデフォルトのホスト・ポートを更新する場合に使用します。

このタスクについて

インストールが完了したら、各アプリケーション・クラスター・メンバーのデフォルトのホスト・ポートが **default_host** のホスト別名に含まれているかどうかを確認します。含まれていない場合は、ポートの新しいホスト別名を手動で入力して、WebSphere Application Server のデフォルト listen ポートを更新しなければならない場合があります。以下のステップを実行します。

手順

1. 管理コンソールで、「**環境**」 > 「**仮想ホスト**」 > 「**default_host**」 > 「**ホスト別名**」の順にクリックします。
2. 「ホスト別名」で「**新規**」をクリックして、別名を作成します。
3. 「**ホスト名**」フィールドに * を入力して、「**ポート**」フィールドにポート番号を入力した後、「**OK**」をクリックします。

   注: デフォルトのホスト・ポートを確認するには、「**サーバー**」 > 「**アプリケーション・サーバー**」 > 「**ServerName**」 > 「**ポート**」をクリックします。WC_defaulthost と WC_defaulthost_secure の値を探します。ここで、serverName は、IBM Security Identity Manager がデプロイされているアプリケーション・クラスター・メンバーのサーバー名です。
4. 構成変更を保存します。
5. WebSphere Application Server ノードの完全同期を実行します。

カスタム・ロゴの保持

UI で使用されるカスタム・ロゴは、アップグレード後は保持されません。`ui.properties` ファイルを変更する必要があります。

`enrole.ui.customerLogo.image` という名前の `ui.properties` ファイルのプロパティーは、依然として 5.0 または 5.1 で指定されたロケーションを指しています。ただし、このポインターは、`enrole.ear` または `ITIM.ear` ディレクトリー内のパスにデフォルト設定されます。イメージ・ファイルは、古いロケーションから新しいロケーションにコピーする必要があります。

ロゴおよびスタイル・シートのカスタマイズについては、IBM Security Identity Manager インフォメーション・センターの 254 ページの『カスタマイズ・データの手動保存』を参照してください。

インストールの検証

インストールが完了したら、IBM Security Identity Manager バージョン 6.0 システムにログオンできることを確認します。

IBM Security Identity Manager バージョン 6.0 にログオンします。以前のバージョンの Tivoli Identity Manager で使用していた管理者ユーザー ID およびパスワードを使用します。

IBM Security Identity Manager バージョン 6.0 のインストールの検証について詳しくは、 22 ページの『インストール済み環境の検査』 を参照してください。

パフォーマンスの調整

新しいシステムの検証が完了したら、パフォーマンス調整の設定を適用して、新しいシステムがパフォーマンス要件を満たすことを確認します。

例えば、DB2 Universal Database が稼働しているシステムでは、テーブル・スペースの自動サイズ変更を使用可能にすると利点が得られる場合があります。自動サイズ変更は、デフォルトで使用可能に設定されますが、使用可能になっていることを確認してください。以下のコマンドを発行します。

```
db2 get snapshot for tablespaces on itimdb
```

出力に「Auto-resize enabled」行がないか探します。

パフォーマンス調整の設定について詳しくは、IBM Security Identity Manager インフォメーション・センターの『パフォーマンス』トピックを参照してください。

アップグレード後の実動サービスイン

このセクションでは、アップグレード後の実動サービスインの実行方法について説明します。

アップグレード・プロセスを実行して、新しい実動システムをテストしている間にも、古い実動システムは、実動中に行われた変更を収集し続けます。IBM Security Identity Manager のアップグレードでは、これらの変更を収集して、バージョン 6.0 を稼働しているアップグレード・システムにインポートするメカニズムは提供されません。IBM Security Identity Manager は、完全に新規の IBM Security Identity

Manager バージョン 6.0 環境をインストールしなくても、古い実動システムから現在のデータを収集して、新しい環境にインポートする機能を備えています。

以下のデータと設定は、新しい実動システムから保持されます。

- WebSphere Application Server 構成設定 (パフォーマンスの調整を含む)
- プロパティー・ファイルに保管された Tivoli Identity Manager 構成設定

以下のデータと設定は、新しい実動システムから保持されません。

- すべてのデータベース・サーバー・データ
- すべてのディレクトリー・サーバー・データ
- 設定 (DB2 Universal Database や IBM Tivoli Directory Server の設定など) を調整するすべてのミドルウェア。

実動サービスインのロードマップ

現在の実稼働環境から新しい環境に移行するには、以下のロードマップに従います。

実稼働環境のサービスインは、以下のステップから構成されます。

1. 新しい実稼働環境で WebSphere Application Server をシャットダウンします。
2. 以下の新しい実動サーバーをデータ・インポート用に準備します。
   - ディレクトリー・サーバー
   - データベース・サーバー (DB2 Universal Database または SQL Server の場合は、データの準備は不要です)
3. 古い実稼働環境で WebSphere Application Server をシャットダウンします。
4. 以下の古い実動サーバーからデータを収集します。
   - ディレクトリー・サーバー
   - データベース・サーバー
5. 古い実稼働環境から新しい環境に Tivoli Identity Manager ディレクトリー・データをインポートします。
6. 古い実稼働環境から新しい環境に Tivoli Identity Manager データベース・データをインポートします。
7. LDAP アップグレード・ツールを実行して、ディレクトリー・サーバー・データを IBM Security Identity Manager バージョン 6.0 にマイグレーションします。
8. データベース・アップグレード・ツールを実行して、データベース・サーバー・データを IBM Security Identity Manager バージョン 6.0 にマイグレーションします。
9. 新しい実稼働環境で WebSphere Application Server を始動します。
10. パフォーマンスの調整設定をディレクトリー・サーバーとデータベース・サーバーに適用します。

新しい実稼働環境で WebSphere Application Server を停止する

新しい実稼働環境で WebSphere Application Server を停止します。

アプリケーション・サーバーとメッセージ・サーバーの両方を停止します。WebSphere クラスター環境にデプロイする場合は、すべてのクラスター・メンバー上でアプリケーション・サーバーとメッセージ・サーバーを停止する必要があります。

サーバーを停止するには、WebSphere コンソールを使用するか、またはコマンド行からコマンドを使用します。 WebSphere クラスターで作業している場合は、WebSphere コンソールを使用してアプリケーション・サーバーとメッセージ・サーバーを停止した方が簡単です。

注: オプション: デプロイメントに HTTP サーバーが含まれている場合は、HTTP サーバーを停止します。

WebSphere コマンド行のコマンド

- Windows

  WAS_PROFILE_HOME¥bin¥stopServer.bat *servername*

- UNIX または Linux

  WAS_PROFILE_HOME/bin/stopServer.sh *servername*

注: WebSphere 管理セキュリティーが有効の場合は、前のコマンドの最後に以下のフラグを付加します。

-user *WAS_username* - password *WAS_user_password*

ここで、*WAS_username* は、WebSphere Application Server 管理ユーザー名、*WAS_user_password* は、管理ユーザーのパスワードです。

新しい実稼働環境のディレクトリー・サーバーとデータベース・サーバーをデータ・インポートに備えて準備する

データベースおよびディレクトリー・サーバーのデータ・インポートに備えて、新しい実稼働環境を準備する必要があります。新しい実稼働環境では、最初に WebSphere Application Server を確実に停止してください。

注: DB2 または SQL Server のデータは、準備することも再構成することもしないでください。なぜなら、データベースの復元プロセスにより、すべての構成が上書きされるからです。

IBM Security Directory Server インスタンスの再構成

IBM Security Identity Manager バージョン 6 の環境で実行できるようにディレクトリー・サーバー・インスタンスを構成する必要があります。

始める前に

新しい実稼働環境で WebSphere Application Server を停止する必要があります。

手順

1. IBM Tivoli Directory Server を停止します。

   次のコマンドを発行します。

   ibmslapd -I *ldap_instance_name* -k

2. IBM Tivoli Directory Server インスタンス管理ツールを開始します。

   ITDS_HOME¥sbin ディレクトリーにある以下のコマンドを実行します。

   ```
   idsxinst
   ```

3. インスタンス管理ツール (idsxinst) を使用して、現在の IBM Security Identity Manager LDAP インスタンスを削除します。

   また、データベースの削除を選択します。

4. IBM Security Identity Manager ミドルウェア構成ユーティリティーを実行して、IBM Security Identity Manager LDAP インスタンスを作成します。

   インスタンス名とパスワードは、以前に作成したインスタンスと同じにしてください。LDAP インスタンスの作成について詳しくは、274 ページの『ターゲット・サーバーへの Tivoli Directory Server のインストール』 を参照してください。

   注: LDAP インスタンスを破棄せずにミドルウェア構成ユーティリティーを再実行する場合は、データベースを再構成できます。 **idsxcfg** または **idsucfgdb** と **idscfgdb** コマンドを使用します。データベースを再構成する場合に、ミドルウェア構成ユーティリティーによって LDAP インスタンスに適用された調整設定は保存されません。その調整設定でデータベースを更新する必要があります。IBM Security Identity Manager インフォメーション・センターの「*Performance*」トピックで、を参照してください。

次のタスク

データベース・インスタンスを再構成します。

Sun Enterprise ディレクトリー・サーバー・インスタンスの再構成

IBM Security Identity Manager バージョン 6 の環境で実行できるようにディレクトリー・サーバー・インスタンスを構成する必要があります。

始める前に

新しい実稼働環境で WebSphere Application Server を停止する必要があります。

手順

1. Sun Enterprise Directory Server コンソールをロードして、管理者としてログインします。
2. マイグレーションした LDAP サーバーを選択して「**開く**」をクリックし、サーバーの管理コンソールを開きます。
3. 「**構成**」タブをクリックして、「**データ**」サブツリーを展開します。
4. 現在の IBM Security Identity Manager データを収容するサフィックスを探し、そのサフィックスを右クリックして「**削除**」を選択します。
5. サフィックスが削除されたら、「**データ**」サブツリーを右クリックして、「**新規サフィックス**」をクリックします。次に、前と同じサフィックスを再作成します。
6. LDAP サーバーを停止します。

次のタスク

データベース・インスタンスを再構成します。

Oracle データベース・インスタンスの再構成

IBM Security Identity Manager バージョン 6 の環境で実行できるようにデータベース・インスタンスを構成する必要があります。

始める前に

新しい実稼働環境で WebSphere Application Server を停止する必要があります。

手順

1. **dbca** コマンドまたはその他のツールを使用して、テスト環境用に作成された IBM Security Identity Manager データベースおよびインスタンスを除去します。
2. データベースが除去されたら、以前提供されたマイグレーション・コマンドを使用して、同じ名前のデータベースを作成します。詳しくは、267 ページの『Oracle データベースのマイグレーション』を参照してください。
3. Oracle データベース・インスタンスを構成します。

   以下の enrole_admin.sql ファイルを使用すると、新しい Oracle 10g または 11g データベース・インスタンスをマイグレーション用に簡単に構成できます。

   a. このファイルを編集します。

      注: データベース・ユーザー ID およびパスワードが前のバージョンと同じでないと、IBM Security Identity Manager のアップグレードは失敗します。

   b. *itimuserTag* は、IBM Security Identity Manager データベース・ユーザーで置き換えます。例えば enrole などです。

   c. *itimuserPwdtag* は、IBM Security Identity Manager データベース・ユーザーのパスワードで置き換えます。

```
CREATE TABLESPACE enrole_data
DATAFILE 'enrole1_data_001.dbf'
SIZE 64M
AUTOEXTEND ON
NEXT 64M
MAXSIZE unlimited
DEFAULT STORAGE (INITIAL 10M
                                 NEXT 1M
                                 PCTINCREASE 10)
PERMANENT
ONLINE
LOGGING;

CREATE TABLESPACE enrole_indexes
DATAFILE 'enrole1_idx_001.dbf'
SIZE 32M
AUTOEXTEND ON
NEXT 32M
MAXSIZE unlimited
DEFAULT STORAGE (INITIAL 10M
                                 NEXT 1M
                                 PCTINCREASE 10)
PERMANENT
ONLINE
LOGGING;
```

```
CREATE USER itimuserTag IDENTIFIED BY itimuserPwdtag
  DEFAULT TABLESPACE enrole_data
  QUOTA UNLIMITED ON enrole_data
  QUOTA UNLIMITED ON enrole_indexes;
GRANT CREATE SESSION TO itimuserTag;
GRANT CREATE TABLE to itimuserTag;
GRANT CREATE ANY PROCEDURE to itimuserTag;
GRANT CREATE VIEW to itimuserTag;
```

4. 前のステップで **sqlplus** ユーティリティーを使用して編集した enrole_admin.sql ファイルを実行します。 sqlplus system/*system_pwd* @*path*¥enrole_admin.sql system_pwd は、システム・ユーザーのパスワードです。*path* はファイルのパスです。このスクリプト・ファイルを実行すると、必要な IBM Security Identity Manager テーブル・スペースが作成され、必要な権限を持つデータベース・ユーザー (enrole) が作成されます。

次のタスク

古い実動サーバー・データを収集してインポートします。

実動サーバー・データの収集およびインポート

Tivoli Identity Manager 5.0 または 5.1 の実動サーバー・データを新しい実稼働環境に転送するには、以下のタスクを使用します。

新しい実稼働環境を準備した後、以下のタスクを実行して、古い環境からディレクトリー・サーバーとデータベースの情報をインポートします。

Tivoli Directory Server 実動サーバー・データの内容の収集およびインポート

新しい実動サーバーでデータをインポートする準備が完了したら、このタスクを使用して Tivoli Directory Server 実動サーバー・データを新しい実稼働環境に転送します。

手順

1. 古い実動サーバーでディレクトリー・サーバー・データをエクスポートします。

   詳しくは、 274 ページの『ディレクトリー・サーバー・データのバックアップ』を参照してください。

2. Tivoli Identity Manager バージョン 5.0 または 5.1 サーバーで使用されている IBM Tivoli Directory Server の *OLD_ITDS_HOME*¥etc ディレクトリーから、スキーマ・ファイル V3.modifiedschema をコピーします。
3. スキーマ・ファイル V3.modifiedschema を、IBM Security Identity Manager バージョン 6.0 サーバーで使用されている IBM Tivoli Directory Server の *NEW_ITDS_HOME*¥etc ディレクトリーに貼り付けます。
4. ディレクトリー・サーバー・データをインポートします。

   詳しくは、 275 ページの『ディレクトリー・サーバー・データのインポート』を参照してください。

次のタスク

データベース情報を収集してインポートします。

Sun Enterprise Directory Server 実動サーバー・データの内容の収集およびインポート

このタスクは、Sun Enterprise Directory Server 実動サーバー・データを新しい実稼働環境に転送する場合に使用します。

手順

1. 古い実動サーバーでディレクトリー・サーバー・データをエクスポートします。
2. *path*/slapd-serverID/config/schema ディレクトリーから IBM Security Identity Manager バージョン 6.0 サーバー・ディレクトリー内のサーバー・スキーマ・ディレクトリーに、99user.ldif スキーマ・ファイルをコピーします。
3. LDAP サーバーを停止します。
4. 以下のコマンドを実行してデータをインポートします。

   ```
   ldif2db -n instance_name -i ldif_output_file
   ```

   instance_name は、古いインスタンスの名前です。*ldif_output_file* は、前のバージョンの Sun Enterprise Directory Server からエクスポートしたファイルの名前です。

次のタスク

データベース情報を収集してインポートします。

DB2 データベース実動サーバー・データの内容の収集およびインポート

このタスクは、DB2 データベース実動サーバー・データを新しい実稼働環境に転送する場合に使用します。

手順

1. DB2 Universal Database のデータをバックアップします。

   詳しくは、 263 ページの『DB2 Universal Database データのバックアップ』を参照してください。

2. Tivoli Identity Manager データベース・バックアップ・ディレクトリーの内容をターゲット・サーバーにコピーします。例えば /51data/db2 にコピーします。

   以前に作成したデータベース・インスタンス所有者 enrole に、ターゲット・ディレクトリーとその中のファイルを読み取る権限があることを確認します。

3. データベース・データを復元します。詳細情報。

   詳しくは、 264 ページの『DB2 Universal Database データの復元』を参照してください。

次のタスク

サービス統合バスを消去します。

Oracle データベース実動サーバー・データの内容の収集およびインポート

このタスクは、Oracle データベース実動サーバー・データを新しい実稼働環境に転送する場合に使用します。

手順

1. Oracle データベース・データをエクスポートします。詳細情報。 詳しくは、267 ページの『Oracle データのエクスポート』を参照してください。
2. 以下のコマンドを 1 行で入力して、Tivoli Identity Manager バージョン 5.0 または 5.1 のエクスポート・データをインポートします。

   ```
   imp system/system_pwd file=path¥itimxx.dmp log=path¥itimxxexp.log
   fromuser=itim_username
   ```

   system_pwd は、システム・ユーザーのパスワードです。*path* はコピーしたファイルのパスです (例えば C:¥*xx*data¥oracle や /opt/*xx*data/oracle)。*xx* は、前に使用していたバージョンの Tivoli Identity Manager のバージョン番号です (5.0 または 5.1)。*itim_username* は、Tivoli Identity Manager (5.0 または 5.1) データベース・ユーザーの名前です (`enrole` など)。

次のタスク

アップグレード・コマンドを実行します。

Microsoft SQL データベース実動サーバー・データの内容の収集およびインポート

このタスクは、Microsoft SQL データベース実動サーバー・データを新しい実稼働環境に転送する場合に使用します。

手順

1. SQL Server データベースをエクスポートします。

   詳しくは、270 ページの『SQL Server データのバックアップ』を参照してください。
2. 新しい実動サーバー・データベースでデータベースを右クリックして、「**タスク**」 > 「**復元**」 > 「**データベース**」を選択します。
3. 「データベースの復元」で「全般」ページを選択します。Tivoli Identity Manager バージョン 4.6 データベース・バックアップ・ファイルの名前 (`itimdb.bak`) を指定します。
   a. 復元オプションとして、「**デバイスから**」ソースを選択します。
   b. **省略符号 (...)** をクリックします。
   c. Tivoli Identity Manager バージョン 5.*X* データベース・バックアップ・ファイルの名前 (itimdb.bak) を指定します。
4. バックアップ・ファイルをリストに追加したら、チェック・ボックスをオンにしてファイルを選択し、左側のペインで「**オプション**」をクリックします。
5. 「オプション」ページで「**既存のデータベースを上書きする**」オプションを選択して、「**OK**」をクリックします。
6. 以下のユーザー・スクリプトを使用して SQL を構成します。

```
sp_addlogin itimuserTag, itimuserPwdTag;
sp_adduser itimuserTag, itimuserTag, db_owner;
use master;
sp_grantdbaccess itimuserTag, itimuserTag;
sp_addrolemember [SqlJDBCXAUser], itimuserTag;
use itimdbTag;
```

itimuserTag は、Tivoli Identity Manager バージョン 5.*X* データベース・ユーザー (enrole など) で置き換えます。*itimuserPwdTag* は、Tivoli Identity Manager Version 5.*X* データベース・ユーザーのパスワードで置き換えます。*itimdbTag* は、データベース・インスタンス名で置き換えます。

7. 以下のスクリプトを使用して SQL を構成します。

```
sp_change_users_login  'Update_One', 'itimuserTag', 'itimuserTag'
```

itimuserTag は、Tivoli Identity Manager バージョン 5.*X* データベース・ユーザー (enrole など) で置き換えます。

8. SQL Server 2008 を再始動します。

次のタスク

サービス統合バスを消去します。

サービス統合バスの消去

このタスクは、DB2 データベースまたは Microsoft SQL データベースを使用している場合に限って適用されます。

Tivoli Identity Manager 5.*X* から IBM Security Identity Manager 6.0 サーバーへと個別システム・アップグレードを行う場合は、復元したデータベースからサービス統合バス (SIB) データを除去する必要があります。

- DB2 サーバーについては、266 ページの『サービス統合バスの消去』を参照してください。
- Microsoft SQL Server については、272 ページの『サービス統合バスの消去』を参照してください。

ディレクトリーおよびデータベース・データをマイグレーションするコマンド

インポートしたデータを IBM Security Identity Manager バージョン 6.0 レベルにアップグレードするには、以下のコマンドを使用します。

新しい実稼働環境でディレクトリーおよびデータベース・データをインポートしたら、 **ldapUpgrade** および **DBUpgrade** ユーティリティーを実行します。これらのユーティリティーを実行すると、インポートしたデータが IBM Security Identity Manager バージョン 6.0 レベルにアップグレードされます。データ・プールのサイズによっては、このプロセスに時間がかかる場合があります。アップグレードが完了したかどうかを確認するには、*NEW_ISIM_HOME*¥install_logs ディレクトリーにあるログ・ファイル DBUpgrade.stdout および ldapUpgrade.stdout を調べます。

アップグレード時に共有アクセス・モジュールをインストールした場合は、データのインポート後に共有アクセス・モジュールを再構成する必要があります。

『ldapUpgrade および DBUpgrade の実行』に進みます。

ldapUpgrade および DBUpgrade の実行

ldapUpgrade および **DBUpgrade** を実行して、IBM Security Identity Manager にデータをインポートします。

このタスクについて

IBM Security Identity Manager をクラスター環境で実行している場合は、Network Deployment Manager が配置されているシステムで **ldapUpgrade** および **DBUpgrade** コマンドを実行します。

手順

1. **ldapUpgrade** コマンドを実行します。

   Windows オペレーティング・システム

   NEW_ITIM_HOME¥bin¥ldapUpgrade

   UNIX または Linux オペレーティング・システム

   NEW_ITIM_HOME/bin/ldapUpgrade

   注: Oracle Enterprise Directory Server が使用されている場合は、ディレクトリー・サーバーに再索引付けを行う必要があります。詳しくは、283 ページの『Sun Enterprise Directory Server バージョン 6.3 の再始動および再索引付け』を参照してください。

2. **DBUpgrade** コマンドを実行して IBM Security Identity Manager データベースをアップグレードします。

   Windows

   NEW_ITIM_HOME¥bin¥DBUpgrade

   UNIX または Linux

   NEW_ITIM_HOME/bin/DBUpgrade

3. 以下のいずれかのオプションを選択します。
   - アップグレード・インストール時に共有アクセスのインストールを選択しなかった場合は、ここでタスクが完了です。
   - アップグレード・インストール時に共有アクセスのインストールを選択した場合は、**ldapUpgrade** コマンドと **DBUpgrade** コマンドの完了後に手動で共有アクセスを再構成する必要があります。295 ページの『アップグレード時の WebSphere クラスター上での共有アクセスの構成』に進みます。

アップグレード時の WebSphere 単一サーバーでの共有アクセス・モジュールの構成

アップグレード時、共有アクセス・モジュールを構成する必要があります。

始める前に

ldapUpgrade コマンドと **DBUpgrade** コマンドを実行したことを確認します。詳しくは、『ldapUpgrade および DBUpgrade の実行』を参照してください。

このタスクについて

実動サービスインにより、データベースおよびディレクトリー・サーバーの既存のデータが除去され、IBM Tivoli Identity Manager 5.0 または 5.1 システムからデータがロードされます。このプロセスで共有アクセスの構成は除去されます。ここで、共有アクセスを再構成する必要があります。

注: デプロイメントで WebSphere クラスターを使用する場合は、以下の指示に従わないでください。 『アップグレード時の WebSphere クラスター上での共有アクセスの構成』を参照してください。

手順

1. IBM Security Identity Manager のインストール・ロケーション内の bin ディレクトリーに移動し、ユーティリティーを実行します。

   以下に例を示します。

表 34. SAConfig の実行

オペレーティング・システム	コマンド
Windows	C:¥Program Files¥IBM¥isim¥bin で、「SAConfig」をクリックするか、コマンド・ウィンドウを開いて **SAConfig** と入力します。
UNIX または Linux	/opt/IBM/isim/bin で、**./SAConfig** と入力します。

2. WebSphere Application Server を再始動します。

アップグレード時の WebSphere クラスター上での共有アクセスの構成

ディレクトリー・サーバーおよびデータベース・ファイルをアップグレードした後に WebSphere クラスター上で共有アクセス・モジュールを構成するには、以下の手順を使用します。

始める前に

ldapUpgrade コマンドと **DBUpgrade** コマンドを実行したことを確認します。詳しくは、 294 ページの『ldapUpgrade および DBUpgrade の実行』を参照してください。

このタスクについて

実動サービスインにより、データベースおよびディレクトリー・サーバーの既存のデータが除去され、IBM Tivoli Identity Manager 5.0 または 5.1 システムからデータがロードされます。このプロセスで共有アクセスの構成は除去されます。ここで、共有アクセスを再構成する必要があります。

手順

1. IBM Security Identity Manager のインストール・ロケーション内の bin ディレクトリーに移動し、ユーティリティーを実行します。

   以下に例を示します。

表 35. SAConfig の実行

オペレーティング・システム	コマンド
Windows	C:¥Program Files¥IBM¥isim¥bin で、「SAConfig」をクリックするか、コマンド・ウィンドウを開いて **SAConfig** と入力します。
UNIX または Linux	/opt/IBM/isim/bin で、**./SAConfig** と入力します。

2. クレデンシャル・ボールト・サーバーの既存の証明書ファイルを除去します。

   ISIM_HOME/data/keystore/cvystore.jceks
   ISIM_HOME/data/keystore/pwdEncKeystore.jceks

3. *ISIM_HOME*/data/KMIPServer.properties ファイルを編集して、パスワードを指定します。
   - プロパティー・ファイルにプロパティー cv.encryption.password を指定する必要がありますが、その値はブランクにしなければなりません。
   - データベースのパスワードは、平文にする必要があります。このパスワードは、データベースに接続する際に使用され、その呼び出し元のコマンドによって暗号化されます。

   以下の手順を実行します。

   a. cv.encryption.password を空に設定します。
   b. dbpassword を変更して、データベース・パスワードに既存の平文のパスワードを設定します。
   c. clipassword プロパティーを更新します。

      どのようなストリング値でも指定できます。以下に例を示します。

      clipassword=test

4. クレデンシャル・ボールト・サーバーの鍵ストア・ファイルを構成します。

   注: このステップは、デプロイメント・マネージャーでのみ実行します。クラスター・メンバーでは、このステップは実行する必要はありません。

   次のコマンドで、-p パラメーターの値が、ISIM_HOME/data/KMIPServer.properties ファイルの clipassword に指定した値と同じであることを確認します。

   以下のとおり、ご使用のオペレーティング・システム用のコマンドを使用します。

   - Windows オペレーティング・システムの場合、次のように入力します。

     cd /d "*ISIM_HOME*¥lib"

     ISIM_HOME¥lib ディレクトリーから次のコマンドを実行します。

     "*ISIM_HOME*¥jre¥jre¥bin¥java"-cp
     com.ibm.sec.authz.jaccplus_7.3.1.jar;
     com.ibm.sec.authz.xacml4j_7.3.1.jar;
     j2ee.jar;
     ojdbc.jar;
     db2jcc.jar;
     db2jcc_license_cu.jar;
     sqljdbc.jar;
     com.ibm.tklm.kmip.jar;

```
CVCommon.jar;
CVCore.jar;
CVCli.jar;
com.ibm.tklm.credvault.common.jar;
commons-cli.jar;
com.ibm.cv.kmip.ext.jar
-DKMIPConfigProperties="$USER_INSTALL_DIR$$¥$data$¥$KMIPServer.properties"
-Djava.security.auth.login.config==login.config
-Djava.security.auth.policy==jaas.policy
com.ibm.cv.cli.CVShell -u test -p test
```

- UNIX または Linux オペレーティング・システムの場合、次のように入力します。

  ```
  cd "ISIM_HOME/lib"
  ```

  ISIM_HOME¥lib ディレクトリーから次のコマンドを実行します。

  ```
  "ISIM_HOME/jre/jre/bin/java"-cp
  com.ibm.sec.authz.jaccplus_7.3.1.jar:
  com.ibm.sec.authz.xacml4j_7.3.1.jar:
  j2ee.jar:
  ojdbc.jar:
  db2jcc.jar:
  db2jcc_license_cu.jar:
  sqljdbc.jar:
  com.ibm.tklm.kmip.jar:
  CVCommon.jar:
  CVCore.jar:
  CVCli.jar:
  com.ibm.tklm.credvault.common.jar:
  commons-cli.jar:
  com.ibm.cv.kmip.ext.jar:
  -DKMIPConfigProperties="$USER_INSTALL_DIR$$/$data$/$KMIPServer.properties"
  -Djava.security.auth.login.config==login.config
  -Djava.security.auth.policy==jaas.policy
  com.ibm.cv.cli.CVShell -u test -p test
  ```

  このコマンドにより、cvKeystore.jceks および pwdEncKeystore.jceks という 2 つのクレデンシャル・ボールト鍵ストア・ファイルが *ISIM_HOME*/data/keystore ディレクトリーの下に生成されます。また、*ISIM_HOME*/data/KMIPServer.properties 内の暗号鍵、およびクレデンシャル・ボールト・データベースのデータ・エントリーが更新されます。

5. 生成された鍵ストア・ファイルと KMIPServer.properties を WAS_DM_profile_path/config/cells/*cellName*/itim ディレクトリーにコピーします。

   注: このステップは、デプロイメント・マネージャーでのみ実行します。クラスター・メンバーでは、このステップは実行する必要はありません。

6. WebSphere Application Server デプロイメント・マネージャー・コンソールから手動でノードを同期化します。
7. 各クラスター・メンバー上で、WebSphere プロファイル・ディレクトリー階層にある次のクレデンシャル・ボールト・ファイルを IBM Security Identity Manager データ・ディレクトリー階層にコピーします。

表 36. コピーするクレデンシャル・ボールト・サーバー・ファイル

コピーするファイル	コピー先
WAS_PROFILE_PATH/config/cells/*cellName*/itim/cvKeystore.jceks	*ISIM_HOME*/data/keystore/cvKeystore.jceks

表 36. コピーするクレデンシャル・ボールト・サーバー・ファイル (続き)

コピーするファイル	コピー先
WAS_PROFILE_PATH/config/cells/*cellName*/itim/pwdEncKeystore.jceks	*ISIM_HOME*/data/keystore/pwdEncKeystore.jceks
WAS_PROFILE_PATH/config/cells/*cellName*/itim/KMIPServer.properties	*ISIM_HOME*/data/KMIPServer.properties

8. WebSphere Application Server クラスターを再始動します。

WebSphere Application Server の開始

WebSphere Application Server を開始して実働サービスインを完了します。

このタスクについて

インポート・データを使用した **ldapUpgrade** と **DBUpgrade** の実行が完了したら、新しい実稼働環境で WebSphere Application Server とメッセージ・サーバーを開始します。

WebSphere コンソールまたはコマンド行を使用できます。クラスター・デプロイメントの場合は、WebSphere コンソールを使用する方が簡単です。

HTTP サーバーを停止していた場合は、WebSphere サーバーを開始した後に開始します。

手順

コマンド行を使用する場合は、ご使用のオペレーティング・システムに応じて以下のコマンドを入力します。

- Windows

  WAS_PROFILE_HOME¥bin¥startServer.bat *servername*
- UNIX または Linux

  WAS_PROFILE_HOME/bin/startServer.sh *servername*

注: WebSphere 管理セキュリティーが有効の場合は、前のコマンドの最後に以下のフラグを付加します。

-user *WAS_username* - password *WAS_user_password*

ここで、*WAS_username* は、WebSphere Application Server 管理ユーザー名、*WAS_user_password* は、管理ユーザーのパスワードです。

次のタスク

新しい実稼働環境のサービスイン後のタスクを実行します。

新しい実稼働環境のサービスイン後のタスク

実働サービスインが完了したら、サービスイン後のタスクをいくつか実行する必要があります。

Sun Enterprise Directory Server バージョン 6.3 の再始動および再索引付け

このタスクは、IBM Security Identity Manager バージョン 6.0 を Sun Enterprise Directory Server に接続できるようにする場合に使用します。

始める前に

IBM Security Identity Manager バージョン 6.0 がインストールされている必要があります。

このタスクについて

Sun ONE Directory Server からデータをマイグレーションした場合は、 IBM Security Identity Manager バージョン 6.0 のインストールが完了した後に IBM Security Identity Manager を停止する必要があります。その後にディレクトリー・サーバーを始動し、ディレクトリー・サーバーに再索引付けを行います。そうしないと、IBM Security Identity Manager をディレクトリー・サーバーに接続できません。

Sun Enterprise Directory Server に再索引付けを行うには、以下の手順を実行します。

手順

1. Sun Enterprise Directory Server コンソールから、「**構成**」タブをクリックします。
2. ディレクトリー・サーバーに再索引付けを行います。
   a. ディレクトリー・サーバーを選択します。
   b. **データ**・ツリーを開きます。
   c. エクスポートされた root サフィックスをクリックします。
   d. 「**再索引 (Reindex)**」を選択します。
3. 「**すべてチェック (Check All)**」を選択します。
4. 「**OK**」をクリックします。

LDAP リサイクル・ビンのクリーンアップ

`enRole.properties` の `enrole.recyclebin.enable` プロパティーに `false` が設定されている場合は、 LDAP のリサイクル・ビンが空であることを確認してください。そうしないと、以前削除したエンティティーが検索で返される場合があります。

`enrole.recyclebin.enable` に `false` が設定されている場合、LDAP リサイクル・ビンには、アップグレード後に削除したエントリーが含まれている場合があります。これらのエントリーは、以前のバージョンの Tivoli Identity Manager から削除されたものです。これらは、エントリーの検索時に IBM Security Identity Manager ユーザー・インターフェースによって返される場合があります。この問題が存在する場合は、LDAP サーバーのリサイクル・ビンからエントリーをすべて削除するか、このプロパティーに `true` を設定する必要があります。

リサイクル・ビンを空にする方法について詳しくは、IBM Security Identity Manager インフォメーション・センターの『パフォーマンス』トピックに記載されている『リサイクル・ビンを空にする *(Emptying the recycle bin)*』を参照してください。

インストールの検証

インストールが完了したら、IBM Security Identity Manager バージョン 6.0 システムにログオンできることを確認します。

IBM Security Identity Manager バージョン 6.0 にログオンします。以前のバージョンの Tivoli Identity Manager で使用していた管理者ユーザー ID およびパスワードを使用します。

IBM Security Identity Manager バージョン 6.0 のインストールの検証について詳しくは、22 ページの『インストール済み環境の検査』 を参照してください。

パフォーマンスの調整

新しいシステムの検証が完了したら、パフォーマンス調整の設定を適用して、新しいシステムがパフォーマンス要件を満たすことを確認します。

例えば、DB2 Universal Database が稼働しているシステムでは、テーブル・スペースの自動サイズ変更を使用可能にすると利点が得られる場合があります。自動サイズ変更は、デフォルトで使用可能に設定されますが、使用可能になっていることを確認してください。以下のコマンドを発行します。

```
db2 get snapshot for tablespaces on itimdb
```

出力に「Auto-resize enabled」行がないか探します。

パフォーマンス調整の設定について詳しくは、IBM Security Identity Manager インフォメーション・センターの『パフォーマンス』トピックを参照してください。

マイグレーション後のトラブルシューティングおよび既知の問題

このセクションでは、マイグレーションが完了したときの既知の問題に関する情報と、トラブルシューティングのヒントについて説明します。

IBM Security Identity Manager バージョン 6.0 へアップグレードすると、以下の問題が発生することがわかっています。

デフォルト・データがロードされない

IBM Security Identity Manager に固有のデフォルト・データのいくつかがアップグレード時にロードされません。

例えば、デフォルトのアクセス・コントロール項目 (ACI) は、ロードされません。以前のバージョンの ACI との干渉を防止するために、これらの項目はコピーされません。

サービス用にコピーされる追加のファイル

サービスが ID フィードなどのファイル・システム上のファイルを指している場合は、指定のファイルを新しい IBM Security Identity Manager バージョン 6.0 サーバ

ーにコピーします。また、IBM Security Identity Manager バージョン 6.0 サーバー上の新しいファイル・ロケーションを指すようにサービスを更新する必要もあります。この資料では、*OLD_ITIM_HOME* ディレクトリーの内容をコピーすることだけを説明しています。

GetDN は erPolicyMembership または erPolicyTarget でのみサポートされる

アップグレード前に、プロビジョニング・ポリシー属性 erPolicyMembership または erPolicyTarget を除き、レポートのどの属性でも GetDN 関数が使用されていないことを確認します。

このデータベース関数は、これらの 2 つの属性でのみ使用することを目的としています。 IBM Security Identity Manager バージョン 6.0 では、GetDN 関数は不要になっています。この関数は、他の属性では機能しません。レポートは無効であり、正常に構文解析されません。 この問題は、カスタム・レポートでも発生します。

DB2 復元エラー

Windows オペレーティング・システムで DB2 Universal Database を使用している場合は、以下のエラーが発生することがあります。

次のエラーが発生した場合は、以下のコマンドを使用します。

SQL2519N データベースがリストアされましたが、リストアされたデータベースは現行リリースに移行されませんでした。エラー "-1704"、トークン "3" が戻されました。

この問題が発生する場合は、以下のコマンドを実行して問題を修正します。

```
update db cfg for itimdb using LOGFILSIZ 1000
update db cfg for itimdb using LOGPRIMARY 30
update db cfg for itimdb using LOGSECOND 20
migrate db itimdb
```

itimdb は、 IBM Security Identity Manager のデータベース名です。このエラーについて詳しくは、DB2 インフォメーション・センターを参照してください。

http://publib.boulder.ibm.com/infocenter/db2luw/v9/index.jsp.

以前のバージョンからの JavaScript が空を返す

FESI と IBM JavaScript Engine の違いのため、マイグレーションした JavaScript が、アップグレード後に機能しなくなる場合があります。

IBM JavaScript Engine では、明示的な戻りステートメントが必要です。詳しくは、IBM Security Identity Manager インフォメーション・センターの『リファレンス』セクションに記載されている『*IBM(r) JSEngine へのカスタム FESI 拡張機能のマイグレーション*』を参照してください。

コンパイルの失敗

アップグレードの完了時、拡張ディレクトリーからの一部のサンプル・クラスがコンパイルされません。

この失敗は、クラスおよびパッケージの名前を変更することによって発生します。

クラスター・インストールのエラー

クラスター環境でインストールを行う場合は、インストール・プロセスでエラー・メッセージが返される場合があります。

ISIM_HOME¥install_logs¥runConfig.stdout ディレクトリーを確認します。次のメッセージが表示された場合は、WebSphere Application Server の環境変数が正しく定義されているかどうかを確認します。

```
WASX7017E: Exception received while running file
   "C:¥Program Files¥IBM¥itim¥config¥was¥setEVCluster.jacl";exception information:
    com.ibm.websphere.management.exception.ConfigServiceException
    java.lang.reflect.UndeclaredThrowableException:
    java.lang.reflect.UndeclaredThrowableException
```

WebSphere Application Server の環境変数がクラスター・メンバーに対して正しく定義されていることを確認するには、以下のステップを実行します。

1. ノード・エージェントとデプロイメント・マネージャーが稼働していることを確認します。
2. 各 WebSphere Application Server ノードが同期されていることを確認します。
3. クラスター・メンバーに対して *ISIM_HOME*¥bin¥runConfig -install プログラムを実行します。

第 4 部 付録

付録 A. 外部ユーザー・レジストリーとしてのユーザー・レジストリーの構成

認証用に外部ユーザー・レジストリーを使用する場合に、レジストリーがまだ存在しないときは、レジストリー項目を作成する必要があります。

トピック 69 ページの『外部ユーザー・レジストリーを使用した認証のためのインストール前の構成』では、認証用の外部ユーザー・レジストリーとして使用するように既存のユーザー・レジストリーを準備する方法について説明しています。ただし、既存のユーザー・レジストリーが存在しない場合は、最初にユーザー・レジストリーを作成する必要があります。ここでは、認証用の外部ユーザー・レジストリーとして使用できるように新しいユーザー・レジストリーを構成する方法について説明します。

この説明では、IBM Tivoli Directory Server のグラフィカル管理ツールを使用してユーザー・レジストリーを構成する方法の例を 1 つ取り上げます。別の方法として、**ldapadd** などのコマンド行ユーティリティーを使用することもできます。他のユーザー・レジストリー製品を使用している場合は、構成ステップが異なる場合があります。

タスク・シーケンスは次のようになります。

1. サフィックスを作成します。

   この例では、サフィックスとして `dc=mycorp` を使用します。
2. ドメインを作成します。

   この例では、ドメインとして `dc=mycorp` を使用します。
3. ユーザー・テンプレートを作成します。
4. ユーザー・レルムを作成します。

   この例では、レルムとして `dc=mycorp` を使用します。 IBM Security Identity Manager では、レルム内に 2 つのユーザー・アカウントが必要です。ユーザー・アカウントは、管理者ユーザーとシステム・ユーザーです。管理者ユーザーには、`ITIM Manager` を使用します。システム・ユーザーには、`isimsystem` を使用します。

この例では、サフィックスとして `dc=mycorp` を作成します。

構成を開始するには、『サフィックスの作成』を参照してください。

サフィックスの作成

IBM Tivoli Directory Server インスタンス管理ユーティリティーを使用して、サフィックスを作成することが可能です。

手順

1. IBM Tivoli Directory Server インスタンス管理ツールを開始します。
2. インスタンス管理ツールでインスタンスを選択した後、サーバーを停止するために「**開始/停止...**」をクリックします。サフィックスを作成するには、サーバーを停止する必要があります。
3. 「**サーバーの停止**」をクリックして、サーバーを停止します。「**閉じる**」をクリックして、「サーバー状態の管理」ウィンドウを閉じます。
4. インスタンス管理ツールで、「**管理...**」をクリックします。
5. IBM Tivoli Directory Server 構成ツールで、「**サフィックス管理**」に移動します。「サフィックス DN」フィールドにサフィックス名 `dc=mycorp` を入力します。「**追加**」をクリックし、「**OK**」をクリックします。
6. `dc=mycorp` サフィックスが追加されたら、IBM Tivoli Directory Server サーバーを始動します。

次のタスク

『*ドメイン、ユーザー・テンプレート、およびユーザー・レルムの作成*』の手順に進みます。

ドメイン、ユーザー・テンプレート、およびユーザー・レルムの作成

IBM Tivoli Directory Server Web 管理ツールを使用して、ドメイン、ユーザー・テンプレート、およびユーザー・レルムを作成することが可能です。

このタスクについて

このタスクは、グラフィカル・ユーザー・インターフェースの使用方法を示しています。

Web 管理ツールがインストールされていない場合は、IBM Tivoli Directory Server の資料 (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.IBMDS.doc%2Fwelcome.htm) でインストールの手順を参照してください。

注: あるいは、**ldapadd** コマンドを使用することもできます。

手順

1. IBM Tivoli Directory Server Web 管理ツールを開始して、管理者として LDAP サーバーにログオンします。
2. 「**ディレクトリー管理**」 > 「**項目の管理**」を選択した後、「**追加...**」をクリックしてドメインを作成します。
3. 「構造化オブジェクト・クラス」フィールドで「**ドメイン**」を選択して、「**次へ**」をクリックします。
4. 「補助オブジェクト・クラスの選択」パネルでは、設定を指定する必要はありません。「**次へ**」をクリックします。
5. 「必要な属性」パネルの「**相対 DN**」フィールドに `dc=mycorp` と入力します。「必要な属性」セクションの「**dc**」フィールドに `mycorp` と入力します。「**次へ**」をクリックします。

6. 「オプション属性」ページで値を設定する必要はありません。パネル下部までスクロールして、「**終了**」をクリックします。
7. 確認ページが表示され、同様のエントリーを追加するかどうかが尋ねられます。「**いいえ**」をクリックして、「項目の管理」ページに戻ります。
8. 「項目の管理」ページで、dc=mycorp ドメインが作成されており、「RDN」列にリストされていることを確認します。
9. 必要な場合は、ユーザー・テンプレートを作成できます。ユーザー・テンプレートが不要の場合は、次のステップに進み、ユーザー・ドメインを作成します。ユーザー・テンプレートを作成するには、以下のステップを実行します。
   a. 「**レルムとテンプレート**」-->「**ユーザー・テンプレートの管理**」ページに移動して、「**追加...**」をクリックします。
   b. 「ユーザー・テンプレートの追加」ページで、「**ユーザー・テンプレート名**」フィールドに名前を入力し、「**親 DN**」フィールドに値を入力します。「**次へ**」をクリックします。

      この例では、「**ユーザー・テンプレート名**」は mycorpUserTempl、「**親 DN**」 は dc=mycorp です。
   c. このユーザー・テンプレートの「**構造化オブジェクト・クラス**」の値を選択します。この例では、メニュー項目の「**inetOrgPerson**」を選択します。「**次へ**」をクリックします。
   d. 「**名前属性**」フィールドに値を入力します。この例では、uid と入力します。「**編集...**」をクリックして、「必要な属性」タブにパスワード・フィールドを追加します。
   e. 「編集」タブ・ページで「**userPassword**」属性を選択して、「**追加**」をクリックします。
   f. 「**userPassword**」が追加されたら、「**選択された属性**」フィールドに移動して、「**userPassword**」を下部に移動します。「**OK**」をクリックします。
   g. 「**終了**」をクリックして、ユーザー・テンプレートを作成します。
   h. ユーザー・テンプレート mycorpUserTempl が作成されたことを確認します。

      「ユーザー・テンプレートの管理」ページで、エントリー cn=mycorpusertempl,dc=mycorp が存在することを確認します。
10. 「**レルムとテンプレート**」-->「**レルムの管理**」ページで「**追加...**」をクリックして、作成したユーザー・テンプレートのユーザー・レルムを作成します。
11. 「レルムの追加」ページで、「**レルム名**」フィールドと「**親 DN**」フィールドに値を入力して、「**次へ**」をクリックします。

    例えば、「**レルム名**」に mycorpUserRealm、「**親 DN**」に dc=mycorp と入力します。
12. 「レルムの追加」ページで、「**ユーザー・テンプレート**」メニューに移動して、作成したユーザー・テンプレートを選択します。「**編集...**」をクリックします。

    この例では、「ユーザー・テンプレート」フィールドの値は cn=mycorpusertempl,dc=mycorp となります。

13. 「検索フィルター」ページで、デフォルト設定を受け入れて、「**OK**」をクリックします。
14. 「**終了**」をクリックして、ユーザー・レルムの作成を完了します。
15. 「**レルムとテンプレート**」>「**レルムの管理**」を選択します。新しいレルムがリストされることを確認します。

    この例では、エントリー `cn=mycorpuserrealm,dc=mycorp` が存在することを確認します。

タスクの結果

これで、ユーザー・レジストリーが構成されました。

付録 B. 共有アクセスの再構成

ディレクトリー・サーバーまたはデータベースを再構成したら、共有アクセスを再構成する必要があります。

共有アクセスの初期構成は、2 つの異なる方法で実行できます。初期インストール時に共有アクセス・モジュールを選択した場合、インストール・ユーティリティーは、共有アクセス・モジュールを自動的に構成しています。インストール時に共有アクセス・モジュールを選択しなかった場合は、**SAConfig** ユーティリティーを使用して、手動で共有アクセス・モジュールを構成します。

注: 共有アクセスの初期構成を実行しなかった場合は、このトピックを参照しないでください。 129 ページの『第 8 章 共有アクセス・モジュールの構成』を参照してください。

共有アクセスの初期構成を実行した後、以下の 2 つのシナリオで共有アクセスの再構成が必要となります。

- IBM Security Identity Manager が使用するディレクトリー・サーバーを再構成した場合
- IBM Security Identity Manager データベースを再構成した場合

ディレクトリー・サーバーまたはデータベースを再構成した場合は、該当するタスクを実行します。

- 『インストール後に LDAP を再構成したときの共有アクセスの再構成』
- 310 ページの『インストール後にデータベースを再構成したときの共有アクセスの再構成』

インストール後に LDAP を再構成したときの共有アクセスの再構成

IBM Security Identity Manager のインストール後に LDAP を再構成した場合は、**SAConfig** ユーティリティーを実行する必要があります。

IBM Security Identity Manager のインストールが完了した後に LDAP を再び再構成すると、共有アクセス・モジュールのデフォルト・データがすべて失われます。

共有アクセスを再構成するには、**SAConfig** ユーティリティーを実行します。このユーティリティーは、共有アクセス・モジュールのデフォルト・データを再設定します。

このステップは、WebSphere 単一サーバー上でデプロイメントを行うのか、それとも WebSphere クラスター上でデプロイメントを行うのかによって異なります。ご自分のデプロイメントに合った指示を参照してください。

- 310 ページの『LDAP 再構成後の WebSphere 単一サーバーでの共有アクセスの構成』
- 310 ページの『LDAP 再構成後の WebSphere クラスターでの共有アクセスの構成』

LDAP 再構成後の WebSphere 単一サーバーでの共有アクセスの構成

IBM Security Identity Manager をインストールした後に LDAP を再構成したときは、**SAConfig** ユーティリティーを再実行する必要があります。

手順

1. IBM Security Identity Manager のインストール・ロケーション内の bin ディレクトリーに移動し、ユーティリティーを実行します。

   以下に例を示します。

表 37. SAConfig の実行

オペレーティング・システム	コマンド
Windows	C:¥Program Files¥IBM¥isim¥bin で、「SAConfig」をクリックするか、コマンド・ウィンドウを開いて **SAConfig** と入力します。
UNIX または Linux	/opt/IBM/isim/bin で、**./SAConfig** と入力します。

2. WebSphere Application Server を再始動します。

LDAP 再構成後の WebSphere クラスターでの共有アクセスの構成

IBM Security Identity Manager をインストールした後に LDAP を再構成したときは、**SAConfig** ユーティリティーを再実行する必要があります。

手順

1. WebSphere デプロイメント・マネージャー上で、IBM Security Identity Manager インストール・ロケーション内の bin ディレクトリーに切り替えて、このユーティリティーを実行します。

   以下に例を示します。

表 38. SAConfig の実行

オペレーティング・システム	コマンド
Windows	C:¥Program Files¥IBM¥isim¥bin で、「SAConfig」をクリックするか、コマンド・ウィンドウを開いて **SAConfig** と入力します。
UNIX または Linux	/opt/IBM/isim/bin で、**./SAConfig** と入力します。

2. WebSphere Application Server クラスターを再始動します。

インストール後にデータベースを再構成したときの共有アクセスの再構成

IBM Security Identity Manager のインストール後に IBM Security Identity Manager データベースを再構成した場合は、**SAConfig** ユーティリティーを実行する必要があります。

IBM Security Identity Manager のインストールが完了した後にデータベースを再び再構成すると、共有アクセス・モジュールのデフォルト・データがすべて失われます。

共有アクセスを再構成するには、**SAConfig** ユーティリティーを実行します。このユーティリティーは、共有アクセス・モジュールのデフォルト・データを再設定します。

このステップは、WebSphere 単一サーバー上でデプロイメントを行うのか、それとも WebSphere クラスター上でデプロイメントを行うのかによって異なります。ご自分のデプロイメントに合った指示を参照してください。

- 『データベース再構成後の WebSphere 単一サーバーでの共有アクセスの構成』
- 312 ページの『データベース再構成後の WebSphere クラスターでの共有アクセスの構成』

データベース再構成後の WebSphere 単一サーバーでの共有アクセスの構成

IBM Security Identity Manager をインストールした後にデータベースを再構成したときは、**SAConfig** ユーティリティーを再実行する必要があります。

手順

1. IBM Security Identity Manager のインストール・ロケーション内の bin ディレクトリーに移動し、ユーティリティーを実行します。

   以下に例を示します。

   表 39. SAConfig の実行

オペレーティング・システム	コマンド
Windows	C:¥Program Files¥IBM¥isim¥bin で、「SAConfig」をクリックするか、コマンド・ウィンドウを開いて **SAConfig** と入力します。
UNIX または Linux	/opt/IBM/isim/bin で、**./SAConfig** と入力します。

2. *ISIM_HOME*/data/keystore ディレクトリーから以下のファイルを除去します。

   ```
   cvKeystore.jceks
   pwdEncKeystore.jceks
   ```

   ここで、*ISIM_HOME* は IBM Security Identity Manager のインストール・ディレクトリーです。

3. *ISIM_HOME*/data/KMIPServer.properties ファイルから cv.encryption.password プロパティーを除去します。
4. WebSphere Application Server を再始動します。

データベース再構成後の WebSphere クラスターでの共有アクセスの構成

IBM Security Identity Manager をインストールした後にデータベースを再構成したときは、**SAConfig** ユーティリティーを再実行する必要があります。

手順

1. IBM Security Identity Manager のインストール・ロケーション内の bin ディレクトリーに移動し、ユーティリティーを実行します。

   注: このコマンドは、デプロイメント・マネージャーおよび各クラスター・メンバー上で実行する必要があります。

   以下に例を示します。

   表 40. SAConfig の実行

オペレーティング・システム	コマンド
Windows	C:¥Program Files¥IBM¥isim¥bin で、「SAConfig」をクリックするか、コマンド・ウィンドウを開いて **SAConfig** と入力します。
UNIX または Linux	/opt/IBM/isim/bin で、**./SAConfig** と入力します。

2. *ISIM_HOME*/data/keystore ディレクトリーから以下のファイルを除去します。

   ```
   cvKeystore.jceks
   pwdEncKeystore.jceks
   ```

   ここで、*ISIM_HOME* は IBM Security Identity Manager のインストール・ディレクトリーです。

3. *ISIM_HOME*/data/KMIPServer.properties ファイルから cv.encryption.password プロパティーを除去します。
4. ISIM_HOME/data/KMIPServer.properties ファイルの clipassword プロパティーを更新します。

   どのようなストリング値でも指定できます。以下に例を示します。

   ```
   clipassword=test
   ```

   注: このファイルは、デプロイメント・マネージャー上でのみ編集してください。
5. クレデンシャル・ボールト・サーバーの鍵ストア・ファイルを構成します。

   注: このステップは、デプロイメント・マネージャーでのみ実行します。クラスター・メンバーでは、このステップは実行する必要はありません。

   次のコマンドで、-p パラメーターの値が、ISIM_HOME/data/KMIPServer.properties ファイルの clipassword に指定した値と同じであることを確認します。

   以下のとおり、ご使用のオペレーティング・システム用のコマンドを使用します。

   - Windows オペレーティング・システムの場合、次のように入力します。

```
cd /d "ISIM_HOME¥lib"
```

ISIM_HOME¥lib ディレクトリーから次のコマンドを実行します。

```
"ISIM_HOME¥jre¥jre¥bin¥java"-cp
com.ibm.sec.authz.jaccplus_7.3.1.jar;
com.ibm.sec.authz.xacml4j_7.3.1.jar;
j2ee.jar;
ojdbc.jar;
db2jcc.jar;
db2jcc_license_cu.jar;
sqljdbc.jar;
com.ibm.tklm.kmip.jar;
CVCommon.jar;
CVCore.jar;
CVCli.jar;
com.ibm.tklm.credvault.common.jar;
commons-cli.jar;
com.ibm.cv.kmip.ext.jar
-DKMIPConfigProperties="$USER_INSTALL_DIR$$¥$data$¥$KMIPServer.properties"
-Djava.security.auth.login.config==login.config
-Djava.security.auth.policy==jaas.policy
com.ibm.cv.cli.CVShell -u test -p test
```

- UNIX または Linux オペレーティング・システムの場合、次のように入力します。

```
cd "ISIM_HOME/lib"
```

ISIM_HOME¥lib ディレクトリーから次のコマンドを実行します。

```
"ISIM_HOME/jre/jre/bin/java"-cp
com.ibm.sec.authz.jaccplus_7.3.1.jar:
com.ibm.sec.authz.xacml4j_7.3.1.jar:
j2ee.jar:
ojdbc.jar:
db2jcc.jar:
db2jcc_license_cu.jar:
sqljdbc.jar:
com.ibm.tklm.kmip.jar:
CVCommon.jar:
CVCore.jar:
CVCli.jar:
com.ibm.tklm.credvault.common.jar:
commons-cli.jar:
com.ibm.cv.kmip.ext.jar:
-DKMIPConfigProperties="$USER_INSTALL_DIR$$/$data$/$KMIPServer.properties"
-Djava.security.auth.login.config==login.config
-Djava.security.auth.policy==jaas.policy
com.ibm.cv.cli.CVShell -u test -p test
```

このコマンドにより、cvKeystore.jceks および pwdEncKeystore.jceks という 2 つのクレデンシャル・ボールト鍵ストア・ファイルが *ISIM_HOME*/data/keystore ディレクトリーの下に生成されます。また、*ISIM_HOME*/data/KMIPServer.properties 内の暗号鍵、およびクレデンシャル・ボールト・データベースのデータ・エントリーが更新されます。

6. 生成された鍵ストア・ファイルと KMIPServer.properties を WAS_DM_profile_path/config/cells/*cellName*/itim ディレクトリーにコピーします。

注: このステップは、デプロイメント・マネージャーでのみ実行します。クラスター・メンバーでは、このステップは実行する必要はありません。

7. WebSphere Application Server デプロイメント・マネージャー・コンソールから手動でノードを同期化します。
8. 各クラスター・メンバー上で、WebSphere プロファイル・ディレクトリー階層にある次のクレデンシャル・ボールト・ファイルを IBM Security Identity Manager データ・ディレクトリー階層にコピーします。

表 41. コピーするクレデンシャル・ボールト・サーバー・ファイル

コピーするファイル	コピー先
WAS_PROFILE_PATH/config/cells/*cellName*/itim/cvKeystore.jceks	*ISIM_HOME*/data/keystore/cvKeystore.jceks
WAS_PROFILE_PATH/config/cells/*cellName*/itim/pwdEncKeystore.jceks	*ISIM_HOME*/data/keystore/pwdEncKeystore.jceks
WAS_PROFILE_PATH/config/cells/*cellName*/itim/KMIPServer.properties	*ISIM_HOME*/data/KMIPServer.properties

9. WebSphere Application Server クラスターを再始動します。

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
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
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 の将来の方向性および指針に関するすべての記述は、予告なく変更または撤回される場合があります。これらは目標および目的を提示するものにすぎません。

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。これらのサンプル・プログラムは特定物として現存するままの状態で提供されるものであり、いかなる保証も提供されません。 IBM は、お客様の当該サンプル・プログラムの使用から生ずるいかなる損害に対しても一切の責任を負いません。

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した創作物にも、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. 2004, 2012. 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。

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。

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。

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、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。

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。

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]

[ナ行]

[ハ行]

[マ行]

[ヤ行]

[ラ行]

[ワ行]

D

F

T

U

W

X

Printed in Japan

GA88-4860-00

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