IBM Security Directory Integrator
バージョン 7.2.0.1

Federated Directory Server 管理ガイド

SA88-7236-01
(英文原典：SC27-6211-01)

IBM Security Directory Integrator
バージョン 7.2.0.1

Federated Directory Server 管理ガイド

SA88-7236-01
(英文原典：SC27-6211-01)

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、 107 ページの『特記事項』に記載されている情報をお読みください。

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

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

原典： SC27-6211-01
IBM Security Directory Integrator
Version 7.2.0.1
Federated Directory Server
Administration 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

図

本書について

IBM® Security Directory Integrator は、汎用的、多形式、多方向のリアルタイムでのデータの移動、同期、変換を行うための統合開発環境およびランタイム・サービスです。

「*IBM Security Directory Integrator バージョン 7.2.0.1 Federated Directory Integrator 管理ガイド*」には、Federated Directory Server コンソールを使用したデータ統合ソリューションの設計、実装、管理に関する情報が記載されています。

また、System for Cross-Domain Identity Management (SCIM) プロトコルとインターフェースを使用して ID を管理する方法についても記載されています。

資料および用語集へのアクセス

以下は英語のみの対応となります。オンラインでアクセス可能な IBM Security Directory Integrator バージョン 7.2.0.1 ライブラリーおよび関連資料の説明をお読みください。

このセクションの内容は以下のとおりです。

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

IBM Security Directory Integrator ライブラリー

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

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

  Federated Directory Server コンソールを使用して、データ統合ソリューションの設計、インプリメント、管理を行う方法について記載されています。また、System for Cross-Domain Identity Management (SCIM) プロトコルとインターフェースを使用して ID を管理する方法についても記載されています。

- *IBM Security Directory Integrator バージョン 7.2.0.1 スタートアップ・ガイド*

  IBM Security Directory Integrator の解説および概要です。対話の作成の例と、IBM Security Directory Integrator の実践学習を含んでいます。

- *IBM Security Directory Integrator バージョン 7.2.0.1 ユーザーズ・ガイド*

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

- *IBM Security Directory Integrator バージョン 7.2.0.1 インストールおよび管理者ガイド*

  インストール、旧バージョンからのマイグレーション、ロギング機能の構成、および IBM Security Directory Integrator のリモート・サーバー API の基礎となるセキュリティー・モデルについて記載されています。ソリューションのデプロイおよび管理の方法についての情報が記載されています。

- *IBM Security Directory Integrator バージョン 7.2.0.1 リファレンス・ガイド*

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

- *IBM Security Directory Integrator バージョン 7.2.0.1 Problem Determination Guide*

  問題の識別および解決を支援する IBM Security Directory Integrator のツール、リソース、および技法に関する情報が記載されています。

- *IBM Security Directory Integrator バージョン 7.2.0.1 Message Guide*

  IBM Security Directory Integrator に関連付けられたすべての情報、警告、およびエラー・メッセージのリストが記載されています。

- *IBM Security Directory Integrator バージョン 7.2.0.1 パスワード同期プラグイン*

  5 つの IBM Password Synchronization Plug-ins (Windows 用 Password Synchronizer、Sun Directory Server 用 Password Synchronizer、IBM Security Directory Server 用 Password Synchronizer、Domino® 用 Password Synchronizer、UNIX および Linux 用 Password Synchronizer) それぞれのインストールおよび構成について詳細に説明されています。また、LDAP パスワード・ストアと JMS パスワード・ストアの構成手順についても説明します。

- *IBM Security Directory Integrator バージョン 7.2.0.1 リリース・ノート*

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

オンライン資料

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

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

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

IBM Publications Center
IBM Publications Center サイト (http://www-05.ibm.com/e-business/linkweb/

publications/servlet/pbi.wss) には、必要なすべての IBM 資料を探す場合に役立つカスタマイズ検索機能が用意されています。

関連情報

IBM Security Directory Integrator に関連する情報は、以下の場所で参照することができます。

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

IBM Terminology Web サイト

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

アクセシビリティー

アクセシビリティー機能は、運動障害または視覚障害など身体に障害を持つユーザーがソフトウェア・プロダクトを快適に使用できるようにサポートします。この製品では、インターフェースの読み上げおよびナビゲートを行うための支援技術を使用できます。また、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できます。

詳しくは、「*Directory Integrator の構成*」のアクセシビリティーに関する付録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。

トラブルシューティング では、以下が詳細に説明されています。

- IBM サポートに問い合わせる前に収集しておくべき情報。
- IBM サポートへの各種の問い合わせ方法。
- IBM Support Assistant の使用方法。
- 問題を自分自身で特定して解決するための手順と問題判別のためのリソース。

適切なセキュリティーの実践に関する注意事項

IT システムのセキュリティーでは、企業内および企業外からの不適切なアクセスの防止、検出、およびそれらのアクセスへの対応により、システムおよび情報を保護する必要があります。不適切なアクセスにより、情報が改ざん、破壊、盗用、または悪用されたり、ご使用のシステムの損傷または他のシステムへの攻撃のための利用を含む悪用につながる可能性があります。完全に安全と見なすことができる IT システムまたは IT 製品は存在せず、また単一の製品、サービス、またはセキュリティー対策が、不適切な使用またはアクセスを防止する上で、完全に有効となることもありません。 IBM のシステム、製品およびサービスは、包括的なセキュリティーの取り組みの一部となるように設計されており、これらには必ず追加の運用手順が伴います。また、最高の効果を得るために、他のシステム、製品、またはサービスを必要とする場合があります。IBM は、何者かの悪意のある行為または違法行為によって、システム、製品、またはサービスのいずれも影響を受けないこと、またはお客様の企業がそれらの行為によって影響を受けないことを保証するものではありません。

第 1 章 Federated Directory Server

Federated Directory Server により、ディレクトリーおよびその他のデータ・ソースの集合を結合して、単一の階層ディレクトリーとして扱うことができます。Federated Directory Server コンソールは、このディレクトリー統合を実装する、すぐに利用可能なアプリケーションです。

概説

IBM Security Directory Integrator には、複雑なデータ統合ソリューションを開発するための豊富な機能が用意されています。 Federated Directory Server コンソールは、これらの機能をベースに構築されており、各種ソースからのデータの接続と同期を行うための迅速で使いやすいソリューションを提供します。

IBM Security Directory Server は、Federated Directory Server 向けの一元化されたデフォルトのコア・リポジトリーです。Federated Directory Server コンソールは、1 つ以上のソース・システム (Active Directory や Sun Directory など) からターゲット・ディレクトリーへの同期サービスを提供します。

Federated Directory Server コンソールには、以下の利点があります。

- すぐに使用可能な高品質のアプリケーションであるため、カスタムビルト・ソリューションと比べて、実装にかかる時間や労力が少なくて済みます。
- IBM Security Directory Integrator に関する詳細な知識は必要ないため、簡単にデプロイして使用することができます。
- 既存のシステムに影響を与えることなく、ディレクトリー、データベース、レガシー・データ、フラット・ファイルなどの各種データ・ソースを統合することができます。
- 単一のアクセス・ポイントを通じて、ID 管理アプリケーションとアクセス管理アプリケーションを迅速にデプロイすることができます。
- 高速な処理、拡張が容易なパフォーマンス、優れたセキュリティーを実現します。

機能

Federated Directory Server には、ディレクトリー統合ソリューションを迅速かつ簡単に実装するための機能がいくつか組み込まれています。

- 既存のレガシー・データを変更することなく、ディレクトリーを統合することができます。
- データが自動的に IBM Security Directory Server に格納されます。
- すべての関係に拡張マッピングとデータ変換を含めることができます。
- ユーザーとグループの両方を統合することができます。
- ディレクトリー階層を維持することも、フラット化することもできます。
- 複数のソースにまたがる Federated Directory Server 実装で、グループ (動的グループを含む) を作成することができます。

- 複数のソースからのリンク・データや拡張データを使用して、ユーザーに関する豊富なデータを作成することができます。
- ユーザー認証を既存のバックエンド・ローカル・システムに直接渡すように Federated Directory Server を構成することができます。主要なコスト要因となるパスワード複製を行う必要はありません。
- 既存のディレクトリーとデータ・インフラストラクチャー内のすべてのコンテンツを検索することができます。
- ユーザーは、固有の属性 (E メールや従業員 ID など) を使用して、エンタープライズ・ディレクトリーにログインすることができます。
- 使いやすいインターフェースにより、レガシー・データと、属性のカスタム・マッピングを管理することができます。
- 書き戻しを有効にして元のソースを更新することができます。

ビジネス・シナリオ

Federated Directory Server は、さまざまなビジネス・シナリオでのディレクトリー・サービスのセキュリティー要件およびコラボレーション要件に対応するハイブリッド・アプローチです。

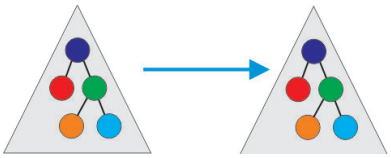
以下の例は、Federated Directory Server の機能で対応可能なビジネス・ニーズの一部です。

- 中央認証サービスを使用可能にする。しかし、パスワードを元のソース・ディレクトリーに残す必要がある。
- エンタープライズ・メッセージングやアクセス制御などのサービスをサポートするために、複数のディレクトリーにわたるグループを管理する必要がある。
- 中央の LDAP ディレクトリーがアプリケーションおよびサービスに固有のニーズをサポートできるように、ID 情報を増加する必要がある。

デフォルトでは、IBM Security Directory Server は集中型のコア・バックエンド・ディレクトリー・サーバーです。管理者は、パススルー認証や書き戻しなどの必要なサービス・レベルを選択できます。さらに、必要に応じて別のシステムを中央 ID リポジトリーとして使用できます。

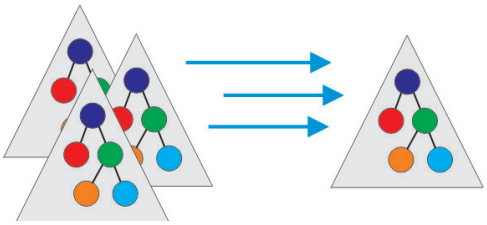
お客様に固有のニーズは、図示されている以下のシナリオに分類できます。

ディレクトリーのマイグレーションまたは共存



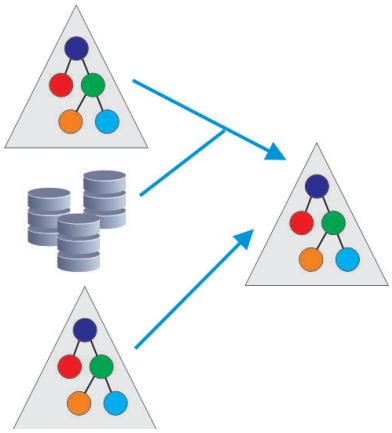
マイグレーションする必要があるスキーマと情報量を定義できます。例えば、元のデータ・ソースのスキーマを拡張する必要なしに、Federated Directory Server にマイグレーションすることによってデータ・ソースのスケーラビリティーと柔軟性を高めることができます。

複数のデータ・ソースまたはディレクトリーのマージ



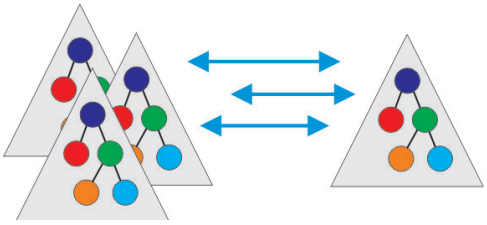
さまざまなデータ・ソースからデータをマイグレーションまたはマージする場合、その関係に高度なマッピングおよびデータ変換が含まれている可能性があります。例えば、Federated Directory Server 内に、ユーザーおよびグループを統合したり、ディレクトリー階層を維持またはフラット化したり、複数のデータ・ソースにまたがる動的なグループを作成したりできます。

他のソースからのデータによるデータの品質向上および増加



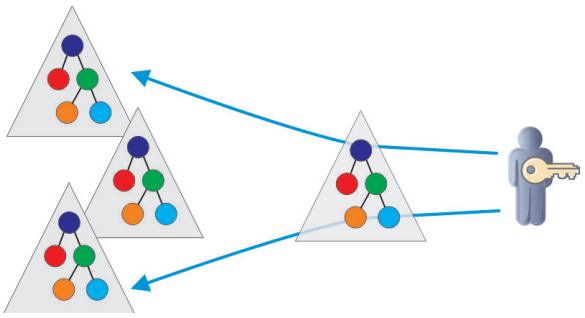
エンドポイントとの結合をセットアップすることにより、別のデータ・ソースから特定の条件でデータを選択的に追加することができます。

元のソースへの変更の選択的な書き戻し



ターゲット・ディレクトリー・サーバーで情報が変更された場合、それをエンドポイントに書き戻すことができます。ただし、お客様によってはエンドポイントの元データを保持するバリアを必要とすることがあるため、書き戻しは選択的です。

元のソースへの認証の統合



Federated Directory Server は、認証プロセスがエンドポイントで行われるように、資格情報が保管されている元のエンドポイントに認証要求を送信できます。希望する場合を除き、資格情報を Federated Directory Server に保管する必要はありません。

例えば、Federated Directory Server のさまざまな機能を結合して、要件に合ったカスタム・ソリューションを作成することができます。Active Directory をシングル・サインオンに使用するとします。ソーシャル・ネットワーキングなど、さらに多くの用途に使用できるようにスケーラビリティーを高める必要がありますが、スキーマは拡張しないとします。その場合は、データを選択的に、例えば、ユーザーの E メール・アドレスのみをマイグレーションすることができます。また、Federated Directory Server は、ソース・ディレクトリーから識別名 (DN) をプルします。Federated Directory Server のパススルー認証機能を使用して、パスワード資格情報をターゲット・ディレクトリーにプルすることなく、ソース・ディレクトリー自体に保持することができます。ユーザーは、固有の属性 (この場合は E メール・アドレス) を使用して、IBM Security Directory Server にログインできます。IBM Security Directory Server は、ユーザーのアクセス元の Active Directory への DN のバインドを実行します。正常な応答が返された場合、ユーザーは認証されます。

機能の概要

ここでは、Federated Directory Server の主要な概念、コンポーネント、アーキテクチャーについて説明します。

次の図に、Federated Directory Server の各種のコンポーネントを示します。

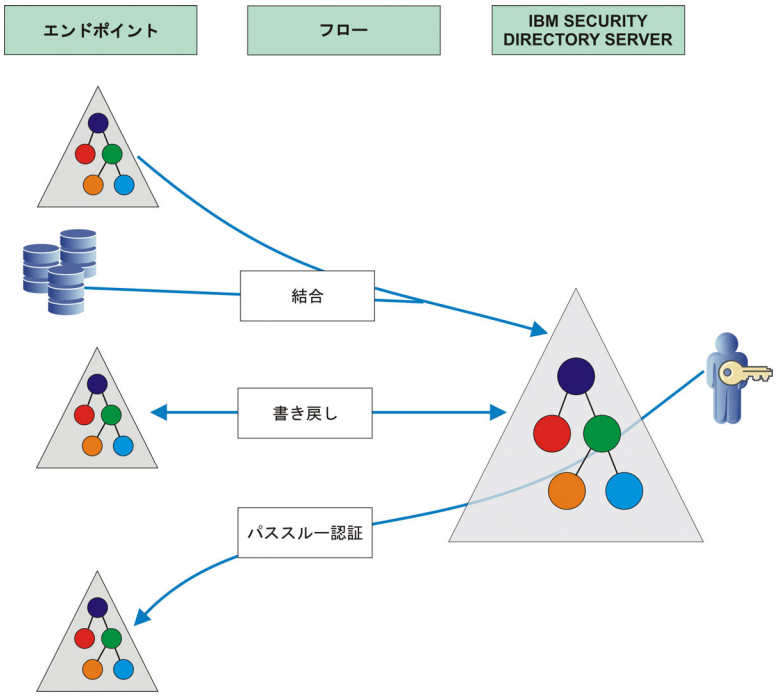


図 1. Federated Directory Server のコンポーネント

ディレクトリー・サーバー
プロジェクトのすべてのフローのターゲットである IBM Security Directory Server。

エンドポイント
フローのデータを提供できる構成済みのソース・システム。現在使用できるエンドポイント・タイプは、Active Directory、カスタム AssemblyLine、ファイル、JDBC、LDAP、IBM Security Directory Server、Sun Directory です。

フロー エンドポイントとターゲットの IBM Security Directory Server との間の関係を定義する構成。フローを作成する前に、ターゲットの Directory Server の接続設定を構成し、1 つ以上のエンドポイントを追加する必要があります。

属性マップ
ソース・スキーマの属性をターゲット・スキーマの対応する属性に変換するために使用されるマップ。Federated Directory Server では、すぐに使用可能ないずれかの属性マップ、またはカスタマイズされた属性マップを、フロー操作に適用することができます。

結合 エンドポイントからのデータを拡張して強化するためのデータを提供する構成済みのソース・システム。フローを構成してエンドポイントとの結合を指定した場合、項目は以下の方法で処理されます。

1. 項目がエンドポイントから読み取られます。
2. フローにより、結合データ・ソース上でその項目が検索されます。
3. 項目がエンドポイントのデータとマージされます。
4. マージされたデータがターゲット・ディレクトリー・サーバーに追加されます。

パススルー認証

認証を別の LDAP サーバーに委任することによってユーザーを認証する IBM Security Directory Server の機能。フローに対してパススルー認証を使用可能にすると、そのフローからのユーザーを認証する際に、エンドポイントに保管されている資格情報を使用するように IBM Security Directory Server が構成されます。

作業を開始するためのロードマップ

Federated Directory Server 構成をセットアップするための主要なタスクを理解し、同期操作を実行するには、以下のロードマップを参照してください。

表 1. Federated Directory Server で作業を開始するためのロードマップ

主要なステップ	オプション・タスクまたは拡張タスク
主要な概念、コンポーネント、アーキテクチャーを理解する。	
Federated Directory Server コンソールにアクセスする。	コンソールにアクセスするためのセキュリティー設定を構成する。
ターゲット・ディレクトリー・サーバーに接続する。	ソース・エンドポイントとターゲット・ディレクトリー・サーバー間のカスタム属性マッピングを定義する。 ディレクトリー・サーバーのログ設定を指定する。
エンドポイントを追加して、以下の 1 つ以上のデータ・ソース用に構成する。 • LDAP • Active Directory • IBM Security Directory Server • Sun Directory • JDBC • ファイルとファイル・パーサー • カスタム AssemblyLine (AL)	パススルー認証を構成し、認証をエンドポイントに委任する。
フローを作成して、エンドポイントとターゲット・ディレクトリー間の関係を定義する。	
フロー設定を定義する。	カスタム属性マップを特定のフロー用に拡張する。 結合を構成し、別のデータ・ソースからのデータを選択的に拡張する。 書き戻し機能を使用可能にして、ターゲット・ディレクトリー・サーバーで行われた変更をエンドポイントに伝搬する。
同期操作のシミュレーションを実行して、フロー構成を検証する。	
初期同期を実行して、データをターゲット・ディレクトリーにマイグレーションする。	

表 1. Federated Directory Server で作業を開始するためのロードマップ (続き)

主要なステップ	オプション・タスクまたは拡張タスク
定期的な増分同期をスケジュールする。	同期操作を手動で実行する。
フローのモニターを有効にして構成する。	
ログとレポートを使用して、フロー構成と同期操作に関する問題のトラブルシューティングを行う。	既知の問題と制限を確認して、特定の問題を解決する。

Federated Directory Server コンソールへのアクセス

ブラウザーで Web ベースの Federated Directory Server コンソール・アプリケーションにアクセスできます。

始める前に

IBM Security Directory Integrator バージョン 7.2 をインストールして最新のフィックスパックを適用します。

このタスクについて

- IBM Security Directory Integrator をインストールすると、Federated Directory Server の成果物と構成ファイルは *tdi_install_dir*/LDAPSync ディレクトリーにインストールされます。
- Federated Directory Server コンソールを初めて開始するとき、次のことが実行されます。
  1. *sdi_solution_dir*/LDAPSync ディレクトリーにデータが取り込まれます。
  2. デフォルト構成ファイル LDAPSync.xml が *sdi_solution_dir*/configs フォルダーにコピーされます。
- 将来の更新に備えて、LDAPSync.xml 構成ファイルを *sdi_solution_dir*/LDAPSync から *sdi_solution_dir*/configs に手動でコピーする必要があります。

手順

1. ご使用のシステムの起動インターフェースから、あるいはコマンド行から **ibmditk** または **ibmdisrv** コマンドを使用して、IBM Security Directory Integrator を開始します。

   注:

   - 先へ進む前に IBM Security Directory Integrator サーバー (ibmdisrv) をアクティブにしておく必要があります。IBM Security Directory Integrator サーバーを開始しないよう構成エディターのデフォルト・プロパティーを変更した場合、次のステップは失敗します。
2. Federated Directory Server コンソールを開きます。
   - ローカル・システムから Federated Directory Server にアクセスしている場合は、「**スタート**」 > 「**プログラム**」 > 「**IBM Security Directory Integrator 7.2**」 > 「**Federated Directory Server コンソール**」をクリックします。
   - リモート・システムから Federated Directory Server にアクセスしている場合は、ブラウザーで次のリンクを開きます。

```
https://hostname:1098/fds
```

注: デフォルトのポート番号は 1098 ですが、IBM Security Directory Integrator のインストール中に「**REST API ポート**」フィールドに入力した値を使用する必要があります。

3. Federated Directory Server コンソールへのアクセス時に、セキュリティー設定により認証が必要であることが示されている場合、ログイン画面が表示されます。
   - localhost からアクセスしている場合は、ユーザー名として admin、パスワードとして admin を指定し (いずれもデフォルト)、「**ログイン**」をクリックします。
   - デフォルトでは、リモート・アクセスは拒否されます。リモート・システムからアクセスできるようにしたい場合は、管理者によって指定されているセキュリティー設定に従って適切な認証資格情報を指定する必要があります。詳しくは、『セキュリティー設定』を参照してください。

次のタスク

Federated Directory Server に対して以下のステップを実行します。

1. ターゲット・ディレクトリー・サーバーに接続します。
2. 1 つ以上のエンドポイントを構成します。
3. フロー設定を定義します。

注: コンソールで Federated Directory Server の各種機能を構成すると、デフォルトでは変更内容が自動的に保存されます。コンソールの自動保存設定と最新表示のデフォルト設定を変更するには、以下のようにします。

1. Federated Directory Server コンソールのメニュー・バーで、「**オプション**」をクリックします。
2. コンソールで行った構成変更を手動で保存するには、「**自動保存を使用可能にする**」チェック・ボックスをクリアします。
3. 構成変更を自動的に再ロードしないようにするには、「**構成を保存するときに自動的に FDS を更新します**」チェック・ボックスをクリアします。
4. 現行構成のスナップショットを作成するには、「**スナップショットの説明**」を指定してから、「**スナップショットの作成**」をクリックします。
5. 後で、スナップショット作成時のレベルに変更をロールバックすることができます。「**スナップショットのロード**」からスナップショットを選択して、「**ロード**」をクリックします。

セキュリティー設定

Federated Directory Server コンソールへのアクセスは、セキュリティー設定を指定する一連のプロパティーによって制御されます。

セキュリティー設定は、IBM Security Directory Integrator ソリューション・ディレクトリーの solution.properties ファイルで指定する必要があります。これらのプロパティーが、すべての IBM Security Directory Integrator Web アプリケーション (ダッシュボード、REST API、および Federated Directory Server コンソールなど) へのアクセスを制御します。

ローカル・ユーザーとリモート・ユーザーは、着信アクセス要求のクライアント IP アドレスで区別されます。

- IP アドレスが IBM Security Directory Integrator が実行されているシステム上のいずれかのネットワーク・カードに属している場合、その IP アドレスは localhost ユーザーとして見なされます。
- その他すべての IP アドレスはリモート・ユーザーとして見なされます。

localhost ユーザーのアクセス許可は、以下の資格情報で組み込まれています。

ユーザー名: admin

パスワード: admin

アクセス制御および許可を指定するために、以下の認証プロパティーを設定または変更することができます。

dashboard.auth=true

ユーザーの認証が必要であるかどうかを示します。

有効な値は、ユーザーの認証が必要な場合の true、または認証が不要な場合の false です。

dashboard.auth.localhost

localhost からの接続で使用する必要がある認証のタイプを示します。

有効値は以下のとおりです。

- プロパティー・ベースの認証を使用する必要があることを指定する properties。
- 認証が不要であることを指定する none。
- localhost からのすべての接続を拒否することを指定する deny。
- LDAP サーバーにログインして、オプションでグループ・メンバーシップを検証することによって認証することを指定する ldap。

dashboard.auth.remote

リモート接続で使用する必要がある認証のタイプを示します。

有効値は以下のとおりです。

- プロパティー・ベースの認証を使用する必要があることを指定する properties。
- 認証が不要であることを指定する none。
- deny は、すべてのリモート接続 (localhost 以外からのすべての接続) のアクセスを拒否することを指定します。
- LDAP サーバーにログインして、オプションでグループ・メンバーシップを検証することによって認証することを指定する ldap。

{protect}-dashboard.auth.user.*username*=*password*

リモート・アクセス用のユーザー資格情報を指定します。

デフォルトのユーザー名は admin でパスワードは admin です。

```
{protect}-dashboard.auth.user.admin=admin
```

複数の Federated Directory Server ユーザー・ログイン・アカウントを指定するには、以下の例を参照してください。

```
{protect}-dashboard.auth.user.admin=admin
{protect}-dashboard.auth.user.user1=user1passwd
{protect}-dashboard.auth.user.user2=user2passwd
```

dashboard.auth.ldap.url
ユーザーの認証に使用する LDAP サーバーのアドレスを指定します。このプロパティーは、認証メカニズムとして ldap を指定した場合にのみ使用されます。

LDAP ホスト名、ポート番号、およびオプションの検索ベースを次の形式で入力します。

`ldap://host:port [/search-base]`

例を示します。

```
ldap://localhost:10389/ou=system
```

ユーザーがユーザー名入力フィールドに E メール・アドレスを指定した場合、IBM Security Directory Integrator は最初に、識別名 (DN) を抽出する LDAP サーバー内の固有の項目を検索します。それ以外の場合は、指定されている値が LDAP サーバーに受け入れられることが予期されます。IBM Security Directory Integrator は、ユーザー名を表す DN、およびユーザーのパスワードを取得した後、その DN およびパスワードを使用して LDAP 基本認証を実行します。

dashboard.auth.ldap.url.group
認証後にユーザーのグループ・メンバーシップを検証するために使用する LDAP サーバーのアドレスを指定します。このプロパティーは、認証メカニズムとして ldap を指定した場合にのみ使用されます。

LDAP ホスト名、ポート番号、およびオプションの検索ベースを次の形式で入力します。

`ldap://host:port [/search-base]`

例を示します。

```
ldap://localhost:389/cn=group1,ou=groups,ou=system
```

このプロパティーを指定した場合、LDAP リポジトリーに対してユーザーの資格情報が認証された後に追加の認証ステップが実行されます。認証されたユーザーが、指定されたグループのメンバーでもあるかどうかを確認した後、アクセスが許可されます。

これらのプロパティーは、IBM Security Directory Integrator ダッシュボードのグラフィカル・ユーザー・インターフェースでも構成できます。「ダッシュボード」ウィンドウで、「**アクション**」 > 「**サーバー詳細の表示**」 > 「**セキュリティーおよび接続**」をクリックします。詳しくは、IBM Security Directory Integrator の資料を参照して、『ダッシュボード・セキュリティー設定の構成』を検索してください。

リモート・アクセス用の Internet Explorer 設定

Internet Explorer Enhanced Security Configuration (IE ESC) が有効な場合、Internet Explorer ブラウザー内でリモート・システムから Federated Directory Server コンソールにアクセスするために必要な構成設定を追加します。

デフォルトでは、IE ESC は Web ページ上で実行するすべてのスクリプトをブロックします。Federated Directory Server は何らかの情報をコンソールに表示する前に、いくつかのスクリプトをロードします。したがって、ユーザーがコンソールを

開くと、IESC に対応した Internet Explorer ブラウザーはブランク・ページを表示します。ページにアクセスするには、Federated Directory Server をホストするサイトを、Internet Explorer の安全なリストに追加する必要があります。

1. **Internet Explorer** のメニューで、「**ツール**」 > 「**インターネット オプション**」をクリックします。
2. 「**セキュリティ**」タブをクリックします。
3. 「**信頼済みサイト**」をクリックします。
4. 「**サイト**」をクリックします。
5. 「**この Web サイトをゾーンに追加する**」フィールドに、Federated Directory Server コンソールの URL を入力します。例えば、`https://myfds.com/fds/*` などです。
6. 「**追加 (Add)**」をクリックします。
7. 「**閉じる**」、「**OK**」の順にクリックしてページを閉じ、設定を保存します。
8. Internet Explorer ブラウザーを再始動します。
9. Internet Explorer ブラウザーの Federated Directory Server コンソールにアクセスします。

IBM Security Directory Server への接続

IBM Security Directory Server は、Federated Directory Server 向けの一元化されたデフォルトのコア・リポジトリーです。1 つ以上のソース・システムからターゲット・ディレクトリー・サーバーへの同期サービスを使用するには、Federated Directory Server コンソールでターゲットの IBM Security Directory Server の接続パラメーターを定義する必要があります。

手順

1. Federated Directory Server コンソールのナビゲーション・ペインで、「**ディレクトリー・サーバー**」の下の「**接続設定**」をクリックします。
2. 「**接続設定**」ページの「**LDAP URL**」で、ターゲット IBM Security Directory Server の「**ホスト名**」と「**ポート**」を入力します。
3. セキュア接続の場合は「**SSL**」を選択します。
4. 「**ユーザー・ログイン**」および「**パスワード**」の各フィールドに、IBM Security Directory Server への認証用の識別名と資格情報を入力します。
5. 「**デフォルトのターゲット・コンテナー**」で、同期されたデータを保管するために使用される、ターゲットの IBM Security Directory Server のコンテナーを指定します。後でフローを作成する時に、各シナリオに異なるターゲット・コンテナーを指定することができます。
6. 次のフィールドでは、バイナリーとして扱う必要がある属性 (例えば、**jpegPhoto**) のリストを指定できます。 1 行に 1 つずつ属性を入力してください。
7. 接続が正常に行われているようにします。「**テスト接続**」をクリックします。エンドポイント名の横に緑色のチェック・マークが表示されている場合は、正常に接続されていることを示します。

8. ターゲット・ディレクトリー・サーバー内の項目を確認するには、「**データのブラウズ**」をクリックします。この機能を使用してディレクトリー項目全体をブラウズし、項目を追加、削除、変更することができます。

次のタスク

『ディレクトリー項目のブラウズ』を参照してください。

関連情報:

Secure Sockets Layer (SSL) サポート

ディレクトリー項目のブラウズ

ディレクトリー・ブラウザーを使用して、ターゲットの IBM Security Directory Server のディレクトリー階層と、ユーザー、グループ、およびコンテナーのタイプを表示します。また、データが正常に転送されたかの確認と、項目の追加、変更、削除もできます。

始める前に

Federated Directory Server から ターゲット IBM Security Directory Server に正常に接続できることを確認します。「**接続設定**」リンクの横に緑色のチェック・マークが表示されている場合は、正常に接続されていることを示します。正常に接続されていない場合、「**ディレクトリーのブラウズ**」リンクは無効になります。

手順

1. Federated Directory Server コンソールの「**Directory Server**」で、「**ディレクトリーのブラウズ**」をクリックします。ディレクトリー・サーバーの「接続設定」ページからも、同じブラウザーにアクセスできます。
2. 指定の「**検索ベース**」の下で、入力した「**検索テキスト**」を検索するには、「**検索**」をクリックします。
3. 「**アクション**」をクリックして、以下のいずれかのオプションを選択します。
   - ディレクトリー・サーバー・ツリーのルートからブラウズするには、「**ルートからブラウズ**」を選択します。
   - 接続設定で指定したデフォルトのターゲット・コンテナーからブラウズするには、「**エンドポイント検索ベースのブラウズ**」をクリックします。
4. 項目をクリックして、その属性を表示します。 値が取り込まれた属性のみが表示されます。
5. 値が設定されているかどうかにかかわらず、項目のオブジェクト・クラスに該当する属性をすべて表示するには、「**すべての属性を表示**」を選択します。 これらは「**必須属性**」と「**オプション属性**」の 2 つのセクションに表示されます。
6. 項目を追加、変更、または削除することができます。

   IBM Telephone Directory V5.2 アプリケーションを使用したエントリーの追加

   「**アクション**」 > 「**追加**」をクリックします。

   表示されたリストから、エンティティー・タイプを選択します。

   「**OK**」をクリックします。

属性の値の変更

ディレクトリー・ツリーのナビゲーション・ペインから項目をクリックします。

表示される属性と値の表で、値をダブルクリックして編集します。

「**保存**」をクリックします。ペインのヘッダーに「**項目が変更されました**」というメッセージが表示されます。

項目の削除

ディレクトリー・ツリーのナビゲーション・ペインから項目をクリックします。

「**削除**」をクリックします。

「**OK**」をクリックします。

7. オプション: ディレクトリー・サーバーへのアクセスをテストします。
   a. 「**ログイン・テスト**」をクリックします。
   b. 資格情報を確認するためのパスワードを入力します。

グローバル書き戻しを使用可能または使用不可にする

グローバル書き戻しオプションを使用して、ターゲット・ディレクトリー・サーバーで行われた変更をソース・エンドポイントに反映させる必要があるかどうかを指定します。

このタスクについて

グローバル書き戻しオプションは、すべてのフローについて書き戻しをオフにできる安全機能です。ただし、特定のフローについて書き戻しを選択的に使用可能にするには、このグローバル書き戻しオプションを使用可能にしておく必要があります。次に、各フロー構成内の書き戻しオプションを使用して、特定のフローについて書き戻しを使用可能にするか使用不可にするかを指定します。40 ページの『フローに対して書き戻し機能を使用可能にする』を参照してください。

手順

1. グローバル書き戻し機能を使用可能にするには、「Directory Server」の下で、「**書き戻し**」をクリックして「**書き戻しが使用可能**」を選択します。「**書き戻し**」の隣に緑の目盛りマークが表示されます。
2. IBM Security Directory Server の接続設定内に指定されているユーザーが変更した項目が書き戻し操作の処理を受けないよう指定するには、「**FDS による変更を無視**」を選択します。

   例:

   `cn=root` が、接続設定内に指定されているユーザーであるとします。

   「**FDS による変更を無視**」を選択しない場合、ユーザー `cn=root` によって行われたすべての変更は、ソース・エンドポイントに対して書き戻しされます。これには、Federated Directory Server のフロー操作によって行われる変更は含まれません。

タスクの結果

書き戻し操作が実行されると、エンドポイントに対して書き戻された内容の要約が表示されます。この要約には、フロー名、変更された属性、ディレクトリー・サーバーとエンドポイントの DN などの詳細情報が含まれます。「**フィルター**」フィールドを使用して、書き戻しの要約を検索することができます。

パススルー認証の構成

認証資格情報がターゲットの IBM Security Directory Server にない場合、パススルー認証を使用して認証をエンドポイントに委任します。

始める前に

- IBM Security Directory Server をパススルー認証用に構成します。IBM Security Directory Serverの資料を参照してください。
- Federated Directory Server からターゲット IBM Security Directory Server への接続を確認します。「**Directory Server**」の下の「**接続設定**」リンクの横に緑色のチェック・マークがある場合は、接続が正常であることを示します。正常に接続されていない場合、「**パススルー認証**」リンクは使用不可です。

このタスクについて

パススルー認証は、ユーザー認証を別の LDAP サーバーに委任する IBM Security Directory Server のオプション機能です。認証資格情報をエンドポイントにのみ保持し、ターゲットの IBM Security Directory Server に保持しない場合にこの機能を使用します。パススルー認証を構成すると、IBM Security Directory Server は、クライアントに代わって、外部の LDAP ディレクトリー・サーバーからの資格情報を検査します。

手順

1. ナビゲーション・ペインの「**Directory Server**」の下の「**パススルー認証**」をクリックします。
2. 「**追加**」をクリックして、構成を識別するための「**名前**」を指定します。
3. 「**ターゲット・サブツリー**」フィールドで、IBM Security Directory Server ターゲット・サブツリーを指定します。ターゲット・サブツリーのコンテナー内のユーザーについてのみ、パススルー認証が使用可能になります。
   - 「**選択**」をクリックすると、サブツリーを表示してコンテナーを指定できます。
   - 「**データのブラウズ**」をクリックすると、ターゲット・ディレクトリー・サーバー内の項目を表示、追加、削除、または変更できます。
4. 「**接続詳細のコピー元エンドポイントを選択**」リストから、エンドポイントを選択します。この詳細は、エンドポイントの作成時に指定した接続パラメーターに基づいて、自動的に入力されます。
5. オプション: 「**ホスト名**」、「**ポート**」、「**検索ベース**」、「**ユーザー名**」、「**パスワード**」フィールドを必要に応じて編集します。
6. 「**テスト接続**」をクリックして、パススルー認証の接続設定を検査します。
7. 以下のいずれかのアクションを実行します。

- この構成の影響を受けるフローに対してパススルー認証メカニズムを使用可能にする場合は、「**保存**」をクリックします。影響を受けるフローは、ターゲット検索ベースが一致するか、パススルー認証構成で指定した検索ベースのコンテナー階層の下に存在する、1 つ以上のフローです。
- 影響を受けるフローのパススルー認証を使用可能にしない場合は「**削除**」をクリックします。

8. IBM Security Directory Server を手動で再始動して、変更内容を有効にし、影響を受けるフローについてのパススルー認証を使用可能にします。

関連タスク:

12 ページの『ディレクトリー項目のブラウズ』
ディレクトリー・ブラウザーを使用して、ターゲットの IBM Security Directory Server のディレクトリー階層と、ユーザー、グループ、およびコンテナーのタイプを表示します。また、データが正常に転送されたかの確認と、項目の追加、変更、削除もできます。

ログ設定の指定

IBM Security Directory Server の接続設定を構成してから、ログ・ファイルのパスおよびログ設定を指定します。

手順

1. ナビゲーション・ペインで、「**共通設定**」の下の「**ログ設定**」をクリックします。
2. 「**ログ・ディレクトリー**」フィールドに、ログ・ファイルのパスを指定します。デフォルト・パスは `LDAPSync/logs` です。

   注:

   - IBM Security Directory Integrator のソリューション・ディレクトリーまたは現行作業ディレクトリーに対する相対パスを指定できます。
   - Windows と UNIX の両方のシステムに適用できるように、スラッシュを使用できます。

3. 「**ログ・ファイル履歴**」フィールドに、保持する必要がある以前のログ・ファイルの数を指定します。デフォルト値は `20` です。

次のタスク

1 つ以上のデータ・リソースをエンドポイントとして構成します。さまざまなタイプのエンドポイントを構成するためのステップについては、下記のトピックを参照してください。

属性マップのカスタマイズ

複数のソースからデータが統合される場合、属性は、単一のターゲット・ディレクトリーと同期されるときに正しくマップされる必要があります。属性のカスタム・マップを定義することにより、ソース・エンドポイント・スキーマからターゲット・スキーマに属性を変換する方法を指定できます。

このタスクについて

Active Directory および Sun Directory などの標準スキーマの属性マッピングは組み込まれています。さらに、Federated Directory Server には、すぐに利用可能なカスタム・マップがいくつか用意されています。ただし、一部のシナリオでは、これらの属性マップを変更または拡張するか、新規カスタム・マップを作成することが必要になる場合があります。例えば、データベースまたはファイルをエンドポイントとして使用する場合にカスタム・マップが必要になります。

手順

1. ナビゲーション・ペイン内の「**共通設定**」の下で、「**属性マップ**」をクリックします。 「属性マップ」ページには、個人、グループ、およびコンテナーのオブジェクト用のさまざまな属性マップが表示されます。これらのマップは、*sdi_solution_dir*/LDAPSync ディレクトリー内にあるすぐに利用可能なマップ・ファイルです。
2. カスタマイズする属性マップのタイプをリストから選択します。 属性マップ・テーブルが表示されます。
3. 以下のいずれのアクションも実行できます。

   属性マッピングを作成する

   a. 「**属性の追加**」をクリックします。

   b. ターゲット・ディレクトリー・サーバーの属性リストから属性を選択します。「**Directory Server 属性**」の下に、選択した属性名を示す新しい行が表示されます。

      注: ターゲット・ディレクトリーからの属性のリストが「属性の追加」ウィンドウに表示されない場合、以下のアクションを実行します。

      1) ナビゲーション・ペインの「**Directory Server**」で、「**接続設定**」に移動します。

      2) 「**テスト接続**」をクリックします。エンドポイントの名前の横に緑色のチェック・マークが表示されていることを確認します。これは、正常に接続されていることを示します。このアクションにより、ターゲット・ディレクトリー属性を参照するフィールドにデータが取り込まれます。

   c. 「**エンドポイント属性/割り当て**」の下で、マッピングを変更するためにデフォルト値をダブルクリックして、属性マッピングの詳細設定を指定します。

   d. この属性マッピングをエンドポイントに対して使用するには、「**使用可能**」を選択します。

   e. マッピングのタイプを指定するには、「**単純な割り当て**」または「**スクリプト化された割り当て**」をクリックします。

      注: 「**スクリプト化された割り当て**」を選択した場合、JavaScript コードを作成するか、*sdi_solution_dir*¥LDAPSync¥customScript.js ファイルで関数を呼び出すことにより、割り当てを定義することができ

ます。詳しくは、IBM Security Directory Integrator の資料を参照して、『*IBM Security Directory Integrator のスクリプト*』を検索してください。

f. 「**マップするタイミング**」の下で、このマッピングをすべての操作で使用するか、または項目を変更あるいは作成するときにのみ使用するかを指定します。

g. 「**属性の選択**」フィールドで、ターゲット属性にマップする必要があるソース・エンドポイントの属性名を指定します。

特定の属性のマッピングを削除する

a. 対象とする属性の横にあるチェック・ボックスを選択します。

b. 「**属性の除去**」をクリックします。

c. 「**OK**」をクリックします。

マップを複写してカスタム属性マッピングで拡張する

a. 「**マップの複写**」をクリックします。

b. 新規マップ・ファイルの名前を入力します。

c. 「**OK**」をクリックします。

ソース・マップの属性マッピング項目がすべて入った新規属性マップが作成されます。

属性マップとそのすべての項目を削除する

a. 「**マップの削除**」をクリックします。

b. 「**OK**」をクリックします。

4. 「**保存**」をクリックします。編集した各マップを保存しない限り、変更は失われます。

タスクの結果

すべての属性マップは、*sdi_solution_dir*¥LDAPSync ディレクトリーに格納されます。

次のタスク

フローの指定を定義するときに、フロー操作のためのこのカスタム属性マップを選択することができます。

エンドポイントの構成

ターゲットの IBM Security Directory Server と同期するためのエンドポイントを指定する必要があります。 Federated Directory Server コンソールで、複数の LDAP ディレクトリー、データベース、ファイル、およびサブツリーをエンドポイントとして構成できます。

始める前に

ターゲット IBM Security Directory Server の接続設定を指定していることを確認してください。 11 ページの『IBM Security Directory Server への接続』を参照してください。

手順

1. 新規エンドポイントを指定するには、ナビゲーション・ペインの「エンドポイント」セクションで、「**追加**」をクリックします。 「**エンドポイントの追加**」ウィンドウが表示されます。
2. 「**名前**」フィールドに、エンドポイントを識別するための名前を入力します。
3. 「**エンドポイント・タイプの選択**」リストから、エンドポイントの適切なタイプを選択します。 以下のエンドポイントのタイプが使用可能です。
   - Active Directory
   - カスタム AssemblyLine
   - ファイル
   - JDBC
   - LDAP
   - Sun Directory
   - Security Directory Server

   注: 特定タイプのエンドポイント用に構成ページを作成すると、後で変更することはできません。エンドポイントを削除してから、構成するエンドポイントのタイプ用にエンドポイントを再び作成する必要があります。

タスクの結果

エンドポイント・パラメーターを示す構成ページが表示されます。このページは、エンドポイント・タイプごとに異なります。

ナビゲーション・ペインで、各エンドポイントの隣に状況アイコンが表示されます。「**リフレッシュ**」をクリックして、最新の状況を表示できます。

- エンドポイントを作成した直後に緑色のドットが表示され、エンドポイントの「**テスト接続**」をクリックするまで表示されたままになります。
- 接続が正常に行われることをテストした後、緑色のドットは緑色の目盛りマークに置き換えられます。
- 接続が失敗すると、赤色のクロス・マークが表示されます。

次のタスク

エンドポイントのパラメーターを構成します。さまざまなエンドポイント・タイプについては、下記のトピックを参照してください。

作成および構成したエンドポイントを削除するには、以下のステップを実行します。

1. ナビゲーション・ペインの「**エンドポイント**」セクションで、削除するエンドポイントの名前を右クリックして、「**削除**」をクリックします。
2. 確認メッセージが表示されたら「**OK**」をクリックします。

注: エンドポイントを削除すると、エンドポイントに基づくフローも自動的に削除されます。

Active Directory エンドポイントの構成

Active Directory をエンドポイントとして構成するには、LDAP URL、ログイン名と資格情報、検索ベース、およびルート接尾部を指定する必要があります。

始める前に

エンドポイントを作成していて、タイプを「**Active Directory**」と指定していることを確認してください。 17 ページの『エンドポイントの構成』を参照してください。

手順

1. 「Active Directory」エンドポイント構成ページの「**LDAP URL**」で、アクセスする Active Directory の「**ホスト名**」と「**ポート**」を入力します。デフォルトの LDAP ポート番号は 389 です。SSL を使用している場合は、デフォルトの LDAP ポート番号は 636 です。 Active Directory 接続のための SSL のセットアップについて詳しくは、IBM Security Directory Integrator の資料を参照して、「*Microsoft Active Directory SSL の構成*」を検索してください。
2. セキュア接続の場合は「**SSL**」を選択します。
3. 「**ユーザー・ログイン**」および「**パスワード**」の各フィールドに、サービスへの認証用の識別名と資格情報を入力します。

   例: `cn=administrator,cn=users,dc=your_domain,dc=com`
4. 「**以下のコンテナーから項目を組み込みます**」フィールドに、同期のために項目が読み取られるソース・ディレクトリーの検索ベースを入力します。あるいは、「**コンテキスト**」をクリックして、「**LDAP 検索ベース**」リストから選択し、「**OK**」をクリックします。

   例: `dc=your_domain,dc=com`

   注: Active Directory の場合、この値をドメイン・コントローラーのルート接尾部に設定する必要があります。そうでない場合、削除変更は検出されません。
5. Active Directory 接続設定を検査するために、「**テスト接続**」をクリックします。 エンドポイント名の横に緑色のチェック・マークが表示されている場合は、正常に接続されていることを示します。接続が正常に行われた場合、エンドポイントの属性が別のペインに表示されます。「**フィルター**」フィールドを使用して、属性を検索できます。
6. エンドポイントを構成してから、ディレクトリー内のデータに簡単にアクセスするには、「**データのブラウズ**」をクリックします。LDAP ブラウザーを使用して、ディレクトリー階層と、ユーザー、グループ、およびコンテナーのタイプを表示できます。また、ディレクトリー内の項目の追加、変更、削除もできます。LDAP ブラウザーについて詳しくは、 28 ページの『LDAP ディレクトリー内の項目のブラウズ』を参照してください。
7. オプション: 以下の詳細パラメーターを構成することもできます。「**拡張**」セクションを展開して、以下のパラメーターを表示します。

   ページ・サイズ

   要求によって返される必要がある、ページ当たりの項目数を指定します。デフォルト値は 500 です。

タイムアウトまでの秒数
変更された次の Active Directory オブジェクトを待機する最大秒数を指定します。デフォルト値は 0 です。

ポーリング間の秒数
連続したポーリング間でスリープする秒数を指定します。デフォルト値は 60 です。

変更状態キー
変更検出イテレーター状態を保管するキーまたはパラメーターの名前を指定します。状態キーは、処理された最後の変更を記憶しておくために実行間に使用されます。何らかの理由で同期が停止された場合、再開時に、停止した時点から開始できます。

このキーの値はエンドポイントごとに固有でなければなりません。このパラメーターを設定しない場合、値は、固有性を確保するために自動的に計算されます。

バイナリー属性
ストリングではなくバイナリー値として解釈される必要がある属性のリストを指定します。このフィールドに属性名を入力する場合、1 行につき 1 つの属性を入力して、分離文字を使用しないでください。

次のタスク

エンドポイントを構成した後、フローを作成して、エンドポイントとターゲット・ディレクトリー・サーバーの間の関係を定義できます。

カスタム AssemblyLine エンドポイントの構成

以前に構成エディターで作成した AssemblyLine を Federated Directory Server のエンドポイントとして指定できます。

始める前に

- 構成エディターを使用して AssemblyLine を作成します。AssemblyLine プロジェクト用の構成 XML ファイルが *sdi_solution_dir*/configs にコピーされていることを確認してください。詳しくは、IBM Security Directory Integrator の資料で『構成エディター』を検索してください。
- Federated Directory Server コンソールで、エンドポイントを作成していて、タイプとして「**カスタム AssemblyLine**」を指定していることを確認してください。17 ページの『エンドポイントの構成』を参照してください。

手順

1. 「カスタム AssemblyLine」エンドポイント構成ページで、「**SDI プロジェクト構成名**」フィールドに、AssemblyLine が含まれているプロジェクト用に定義されているソリューション・インスタンスの名前を入力します。デフォルトでは、ソリューション・インスタンス名はプロジェクト名自体と同じです。
2. 以下のフィールドで、各タイプの項目の処理に使用する必要がある AssemblyLine を指定します。
   - **個人項目を読み取る AL**
   - **グループ項目を読み取る AL**

- **コンテナー項目を読み取る AL**

  構成エディターで作成した AssemblyLine プロジェクトの以下の詳細を入力する必要があります。

  - AssemblyLine が含まれている IBM Security Directory Integrator プロジェクトの名前
  - AssemblyLine の名前

  以下の形式を使用します。

  Project Name:/AssemblyLines/*AssemblyLine Name*

  例えば、プロジェクトの名前が OS400 で、このプロジェクトに ReadUsers という AssemblyLine が含まれている場合は、以下のように入力します。

  OS400:/AssemblyLines/ReadUsers

3. カスタム AssemblyLine エンドポイント接続設定を検査するために、「**テスト接続**」をクリックします。 エンドポイント名の横に緑色のチェック・マークが表示されている場合は、正常に接続されていることを示します。接続が正常に行われた場合、エンドポイントの属性が別のペインに表示されます。「**フィルター**」フィールドを使用して、属性を検索できます。

次のタスク

エンドポイントを構成した後、フローを作成して、エンドポイントとターゲット・ディレクトリー・サーバーの間の関係を定義できます。

ファイル・エンドポイントの構成

ファイルをエンドポイントとして構成するには、ファイル・パス、項目のタイプ、およびファイル・パーサーを指定する必要があります。

始める前に

エンドポイントを作成していて、タイプとして「**ファイル**」を指定していることを確認してください。 17 ページの『エンドポイントの構成』を参照してください。

手順

1. 「ファイル」エンドポイント構成ページで、「**ファイル・パス**」フィールドに、アクセスするファイルのパスを入力します。
2. 「**項目のタイプ**」リストから、person、group、または container を選択します。
3. ファイル接続設定を検査するために、「**テスト接続**」をクリックします。 エンドポイント名の横に緑色のチェック・マークが表示されている場合は、正常に接続されていることを示します。接続が正常に行われた場合、エンドポイントの属性が別のペインに表示されます。「**フィルター**」フィールドを使用して、属性を検索できます。
4. オプション: 以下の詳細パラメーターを構成することもできます。「**拡張**」セクションを展開して、以下のパラメーターを表示します。

タイムアウト (秒単位)

タイムアウトになるまでに操作と操作の間に待機する秒数を示す正数を指定します。

無期限に待機する場合は 0 (ゼロ) を指定します。

「**ファイルのロック**」オプションを選択する場合は、「**タイムアウト**」値は、ロックを獲得するまで待機する時間を指定します。

ファイルのロック

ファイルに書き込むために排他ロックを獲得することを指定するには、このオプションを選択します。このロックは、ロックが解除されるまで、Federated Directory Server の別のインスタンスまたは他のプログラムによってファイルが書き込みのために開かれないようにします。

5. 「**パーサー**」リストから、ファイルにアクセスするために必要なパーサーの名前を選択します。

次のタスク

エンドポイントを構成した後、フローを作成して、エンドポイントとターゲット・ディレクトリー・サーバーの間の関係を定義できます。

関連概念:

50 ページの『ファイル・パーサー』

Federated Directory Server コンソール のファイル・エンドポイント構成ページのリストから、適切なファイル・パーサーを選択して構成することができます。

JDBC エンドポイントの構成

JDBC 接続をエンドポイントとして構成するには、JDBC URL、ユーザー名とパスワード、スキーマ、テーブル名、および項目のタイプを指定する必要があります。

始める前に

エンドポイントを作成していて、タイプとして「**JDBC**」を指定していることを確認してください。 17 ページの『エンドポイントの構成』を参照してください。

手順

1. JDBC エンドポイント構成ページの「**JDBC URL**」で、「**タイプ**」リストからデータベースのタイプを選択します。以下のようなオプションがあります。
   - よく使用されるデータベースを選択します。
     a. DB2、Derby、組み込み Derby、solidDB、Microsoft SQL、または Oracle のいずれかのデータベースをリストから選択します。
     b. 必要に応じて「**ホスト名**」、「**ポート**」、および「**データベース**」の名前を選択します。
   - 汎用データベースを選択します。
     a. 「JDBC の詳細」を選択します。
     b. 「**JDBC URL**」フィールドに、アクセスするデータベースの JDBC 接続 URL を入力します。以下の例は、さまざまな JDBC プロバイダーの標準的な URL です。

Informix®

```
jdbc:informix-sqli://hostname:port/
dbname:informixserver=Informix Server Name
```

Sybase `jdbc:sybase:Tds:hostname:port/`

c. 「**JDBC ドライバー**」フィールドに、JDBC ドライバーのインプリメンテーション・クラス名を入力します。以下の例は、さまざまな JDBC プロバイダーの標準的なドライバーのインプリメンテーション・クラス名です。

Informix

```
com.informix.jdbc.IfxDriver
```

Sybase `com.sybase.jdbc3.jdbc.SybDriver`

JDBC ドライバーについて詳しくは、IBM Security Directory Integrator の資料を参照して、「*JDBC ドライバーについて*」を検索してください。

2. 「**ユーザー名**」および「**パスワード**」の各フィールドに、指定されたデータベースにアクセスするためのログイン名と資格情報を入力します。
3. 「**テーブル名**」リストから、操作用のテーブルまたはビューを選択します。指定されたデータベース内のテーブルがリストに表示されます。
4. 「**項目のタイプ**」リストから、`person`、`group`、または `container` を選択します。
5. JDBC 接続設定を検査するために、「**テスト接続**」をクリックします。

   エンドポイント名の横に緑色のチェック・マークが表示されている場合は、正常に接続されていることを示します。接続が正常に行われた場合、エンドポイントの属性が別のペインに表示されます。このペインを使用してレコードをブラウズし、属性名で「**フィルター**」の処理を実行することができます。
6. オプション: 操作用の項目を指定するために、カスタムの `SELECT` ステートメントを指定することもできます。
   a. 「**拡張**」セクションを展開します。
   b. 「**カスタム選択**」フィールドにステートメントを入力します。
7. オプション: 「**追加のプロバイダー・パラメーター**」フィールドに、JDBC プロバイダーによってサポートされている、他のパラメーターを入力します。
   a. `name:value` という形式を使用し、各行にパラメーターを 1 つずつ入力してください。
   b. サポートされるパラメーターについては、ドライバーの資料を確認してください。
   c. 例えば、以下の追加のパラメーターは DB2 に固有のものです。

```
securityMechanism:KERBEROS_SECURITY
loginTimeout:20
readOnly:true
```

次のタスク

エンドポイントを構成した後、フローを作成して、エンドポイントとターゲット・ディレクトリー・サーバーの間の関係を定義できます。

LDAP エンドポイントの構成

LDAP ディレクトリーをエンドポイントとして構成するには、LDAP URL、ログイン名と資格情報、検索ベース、およびルート接尾部を指定する必要があります。

始める前に

エンドポイントを作成していて、タイプとして「**LDAP**」を指定していることを確認してください。 17 ページの『エンドポイントの構成』を参照してください。

手順

1. LDAP エンドポイント構成ページの「**LDAP URL**」で、アクセスする LDAP ディレクトリーの「**ホスト名**」と「**ポート**」を入力します。デフォルトの LDAP ポート番号は 389 です。SSL を使用している場合は、デフォルトの LDAP ポート番号は 636 です。
2. セキュア接続の場合は「**SSL**」を選択します。
3. 「**ユーザー・ログイン**」および「**パスワード**」の各フィールドに、サービスへの認証用の識別名と資格情報を入力します。

   例: `cn=administrator,cn=users,dc=your_domain,dc=com`
4. 「**以下のコンテナーから項目を組み込みます**」フィールドに、変更のためにポーリングされる LDAP ディレクトリーの検索ベースを入力します。あるいは、「**コンテキスト**」をクリックして、「**LDAP 検索ベース**」 リストから選択し、「**OK**」をクリックします。

   例: `dc=your_domain,dc=com`
5. LDAP ディレクトリー接続設定を検査するために、「**テスト接続**」をクリックします。 エンドポイント名の横に緑色のチェック・マークが表示されている場合は、正常に接続されていることを示します。接続が正常に行われた場合、エンドポイントの属性が別のペインに表示されます。「**フィルター**」フィールドを使用して、属性を検索できます。
6. エンドポイントを構成してから、ディレクトリー内のデータに簡単にアクセスするには、「**データのブラウズ**」をクリックします。LDAP ブラウザーを使用して、ディレクトリー階層と、ユーザー、グループ、およびコンテナーのタイプを表示できます。また、ディレクトリー内の項目の追加、変更、削除もできます。
7. オプション: 以下の詳細パラメーターを構成することもできます。「**拡張**」セクションを展開して、以下のパラメーターを表示します。

   バイナリー属性
   ストリングではなくバイナリー値として解釈される必要がある属性のリストを指定します。このフィールドに属性名を入力する場合、1 行につき 1 つの属性を入力して、分離文字を使用しないでください。

   ページ・サイズ
   要求によって返される必要がある、ページ当たりの項目数を指定します。デフォルト値は 500 です。

次のタスク

エンドポイントを構成した後、フローを作成して、エンドポイントとターゲット・ディレクトリー・サーバーの間の関係を定義できます。

関連情報:

28 ページの『LDAP ディレクトリー内の項目のブラウズ』
ディレクトリー・ブラウザーを使用して、エンドポイントのディレクトリー階層と、ユーザー、グループ、およびコンテナーのタイプを表示します。また、データが正常に転送されたかの確認と、項目の追加、変更、削除もできます。

Sun Directory エンドポイントの構成

Sun Directory をエンドポイントとして構成するには、LDAP URL、ログイン名と資格情報、検索ベース、およびルート接尾部を指定する必要があります。

始める前に

エンドポイントを作成していて、タイプとして「**Sun Directory**」を指定していることを確認してください。 17 ページの『エンドポイントの構成』を参照してください。

手順

1. Sun Directory エンドポイント構成ページの「**LDAP URL**」で、アクセスする Sun Directory サービスの「**ホスト名**」と「**ポート**」を入力します。デフォルトの LDAP ポート番号は 389 です。SSL を使用している場合は、デフォルトの LDAP ポート番号は 636 です。
2. セキュア接続の場合は「**SSL**」を選択します。
3. 「**ユーザー・ログイン**」および「**パスワード**」の各フィールドに、サービスへの認証用の識別名と資格情報を入力します。

   例: `cn=administrator,cn=users,dc=your_domain,dc=com`
4. 「**以下のコンテナーから項目を組み込みます**」フィールドに、変更のためにポーリングされる Sun Directory の検索ベースを入力します。あるいは、「**コンテキスト**」をクリックして、「**LDAP 検索ベース**」 リストから選択し、「**OK**」をクリックします。

   例: `dc=your_domain,dc=com`
5. Sun Directory 接続設定を検査するために、「**テスト接続**」をクリックします。エンドポイント名の横に緑色のチェック・マークが表示されている場合は、正常に接続されていることを示します。接続が正常に行われた場合、エンドポイントの属性が別のペインに表示されます。「**フィルター**」フィールドを使用して、属性を検索できます。
6. エンドポイントを構成してから、ディレクトリー内のデータに簡単にアクセスするには、「**データのブラウズ**」をクリックします。LDAP ブラウザーを使用して、ディレクトリー階層と、ユーザー、グループ、およびコンテナーのタイプを表示できます。また、ディレクトリー内の項目の追加、変更、削除もできます。
7. オプション: 以下の詳細パラメーターを構成することもできます。「**拡張**」セクションを展開して、以下のパラメーターを表示します。

タイムアウトまでの秒数
変更された次の Sun Directory オブジェクトを待機する最大秒数を指定します。デフォルト値は 0 です。

ポーリング間の秒数
コネクターが連続したポーリング間でスリープする秒数を指定します。デフォルト値は 60 です。

変更状態キー
変更検出イテレーター状態を保管するキーまたはパラメーターの名前を指定します。状態キーは、処理された最後の変更を記憶しておくために実行間に使用されます。何らかの理由で同期が停止された場合、再開時に、停止した時点から開始できます。

このキーの値はエンドポイントごとに固有でなければなりません。このパラメーターを設定しない場合、値は、固有性を確保するために自動的に計算されます。

バイナリー属性
ストリングではなくバイナリー値として解釈される必要がある属性のリストを指定します。このフィールドに属性名を入力する場合、1 行につき 1 つの属性を入力して、分離文字を使用しないでください。

ページ・サイズ
要求によって返される必要がある、ページ当たりの項目数を指定します。

次のタスク

エンドポイントを構成した後、フローを作成して、エンドポイントとターゲット・ディレクトリー・サーバーの間の関係を定義できます。

関連情報:

28 ページの『LDAP ディレクトリー内の項目のブラウズ』
ディレクトリー・ブラウザーを使用して、エンドポイントのディレクトリー階層と、ユーザー、グループ、およびコンテナーのタイプを表示します。また、データが正常に転送されたかの確認と、項目の追加、変更、削除もできます。

IBM Security Directory Server ソース・エンドポイントの構成

IBM Security Directory Server をエンドポイントとして構成するには、LDAP URL、ログイン名と資格情報、検索ベース、およびルート接尾部を指定する必要があります。

始める前に

エンドポイントを作成していて、タイプとして「**IBM Security Directory Server**」を指定していることを確認してください。 17 ページの『エンドポイントの構成』を参照してください。

手順

1. IBM Security Directory Server ソース・エンドポイント構成ページの「**LDAP URL**」で、アクセスする IBM Security Directory Server の「**ホスト名**」と「**ポー**

ト」を入力します。デフォルトの LDAP ポート番号は 389 です。SSL を使用している場合は、デフォルトの LDAP ポート番号は 636 です。

2. セキュア接続の場合は「**SSL**」を選択します。
3. 「**ユーザー・ログイン**」および「**パスワード**」の各フィールドに、サーバーへの認証用の識別名と資格情報を入力します。

   例: `cn=root`
4. 「**以下のコンテナーから項目を組み込みます**」フィールドに、変更のためにポーリングされるディレクトリー・サーバーの検索ベースを入力します。あるいは、「**コンテキスト**」をクリックして、「**LDAP 検索ベース**」 リストから選択し、「**OK**」をクリックします。

   例: `o=sample`
5. IBM Security Directory Server 接続設定を検査するために、「**テスト接続**」をクリックします。 エンドポイント名の横に緑色のチェック・マークが表示されている場合は、正常に接続されていることを示します。接続が正常に行われた場合、エンドポイントの属性が別のペインに表示されます。「**フィルター**」フィールドを使用して、属性を検索できます。
6. エンドポイントを構成してから、ディレクトリー内のデータに簡単にアクセスするには、「**データのブラウズ**」をクリックします。LDAP ブラウザーを使用して、ディレクトリー階層と、ユーザー、グループ、およびコンテナーのタイプを表示できます。また、ディレクトリー内の項目の追加、変更、削除もできます。
7. オプション: 以下の詳細パラメーターを構成することもできます。「**拡張**」セクションを展開して、以下のパラメーターを表示します。

   タイムアウトまでの秒数
   変更された次のディレクトリー・サーバー・オブジェクトを待機する最大秒数を指定します。デフォルト値は 0 です。

   ポーリング間の秒数
   連続したポーリング間でスリープする秒数を指定します。デフォルト値は 60 です。

   変更状態キー
   変更検出イテレーター状態を保管するキーまたはパラメーターの名前を指定します。状態キーは、処理された最後の変更を記憶しておくために実行間に使用されます。何らかの理由で同期が停止された場合、再開時に、停止した時点から開始できます。

   このキーの値はエンドポイントごとに固有でなければなりません。このパラメーターを設定しない場合、値は、固有性を確保するために自動的に計算されます。

   バイナリー属性
   ストリングではなくバイナリー値として解釈される必要がある属性のリストを指定します。このフィールドに属性名を入力する場合、1 行につき 1 つの属性を入力して、分離文字を使用しないでください。

   ページ・サイズ
   要求によって返される必要がある、ページ当たりの項目数を指定します。

次のタスク

エンドポイントを構成した後、フローを作成して、エンドポイントとターゲット・ディレクトリー・サーバーの間の関係を定義できます。

関連情報:

『LDAP ディレクトリー内の項目のブラウズ』
ディレクトリー・ブラウザーを使用して、エンドポイントのディレクトリー階層と、ユーザー、グループ、およびコンテナーのタイプを表示します。また、データが正常に転送されたかの確認と、項目の追加、変更、削除もできます。

LDAP ディレクトリー内の項目のブラウズ

ディレクトリー・ブラウザーを使用して、エンドポイントのディレクトリー階層と、ユーザー、グループ、およびコンテナーのタイプを表示します。また、データが正常に転送されたかの確認と、項目の追加、変更、削除もできます。

始める前に

Federated Directory Server からエンドポイント・ディレクトリーに正常に接続できることを確認します。「**エンドポイント**」の下のエンドポイント名の横に緑色のチェック・マークが表示されている場合は、正常に接続されていることを示します。正常に接続されていない場合は、データをブラウズしようとするとエラーが表示されます。

このタスクについて

この機能は LDAP ディレクトリーのみで使用可能です。Federated Directory Server で構成できる LDAP エンドポイントは、Active Directory、LDAP、Sun Directory、および IBM Security Directory Server です。

手順

1. エンドポイントの構成画面で「**データのブラウズ**」をクリックします。
2. 指定の「**検索ベース**」の下で、入力した「**検索テキスト**」を検索するには、「**検索**」をクリックします。
3. 「**アクション**」をクリックして、以下のいずれかのオプションを選択します。
   - ディレクトリー・ツリーのルートからブラウズするには、「**ルートからブラウズ**」を選択します。
   - エンドポイント構成で指定した検索ベースからブラウズするには、「**エンドポイント検索ベースのブラウズ**」をクリックします。
4. 項目をクリックして、その属性を表示します。 値が取り込まれた属性のみが表示されます。
5. 値が設定されているかどうかにかかわらず、項目のオブジェクト・クラスに該当する属性をすべて表示するには、「**すべての属性を表示**」を選択します。 これらは「**必須属性**」と「**オプション属性**」の 2 つのセクションに表示されます。
6. 項目を追加、変更、または削除することができます。

   IBM Telephone Directory V5.2 アプリケーションを使用したエントリーの追加
   「**アクション**」 > 「**追加**」をクリックします。

   表示されたリストから、エンティティー・タイプを選択します。

「**OK**」をクリックします。

属性の値の変更

ディレクトリー・ツリーのナビゲーション・ペインから項目をクリックします。

表示される属性と値の表で、値をダブルクリックして編集します。

「**保存**」をクリックします。ペインのヘッダーに「**項目が変更されました**」というメッセージが表示されます。

項目の削除

ディレクトリー・ツリーのナビゲーション・ペインから項目をクリックします。

「**削除**」をクリックします。

「**OK**」をクリックします。

7. オプション: ディレクトリー・サーバーへのアクセスをテストします。
   a. 「**ログイン・テスト**」をクリックします。
   b. 資格情報を確認するためのパスワードを入力します。

フローの作成

エンドポイントとターゲット IBM Security Directory Server との間の関係を定義するフローを作成します。

始める前に

- ターゲット・ディレクトリー・サーバーに接続します。
- 1 つ以上のエンドポイントを構成します。

手順

1. 「**フロー**」タブをクリックして「フロー」ページを表示します。
2. 「フロー」ページで「**追加**」をクリックします。
3. 「フローの追加」ウィンドウで、フローの**名前**を指定します。
4. 「**エンドポイントの選択**」リストで、フロー用のデータを提供するための、いずれかの構成済みエンドポイントを選択します。
5. 「**OK**」をクリックしてフローを作成します。

次のタスク

フローを編集してフロー設定を定義します。

フロー設定の定義

フローを作成したら、そのフローを編集して特定の設定を定義することも、多くの設定用に用意されているデフォルト値を使用することもできます。

始める前に

フローを作成します。

手順

1. フローの設定を指定または変更するには、「**フロー**」ページでフローの名前をクリックして「**編集**」をクリックします。 選択したフローの構成ページが開きます。「**ソース**」タブで、フロー設定の表示と編集を行うことができます。
2. エンドポイントを変更するには、「**ソース**」リストから、フロー用のデータを提供するためのいずれかの構成済みエンドポイントを選択します。
3. 指定できるフロー設定は、以下のカテゴリーにグループ化されています。

   一般設定

   処理する項目のタイプ
   フロー操作で考慮する必要がある項目のタイプを選択します。

   デフォルトでは、「**個人項目の処理**」オプションと「**グループ項目の処理**」オプションが両方とも選択されています。

   ソース階層を Directory Server にミラーリングします
   同期時の階層の処理方法を指定します。

   このチェック・ボックスを選択すると、コンテナーが保持され、ディレクトリー情報のツリー構造がエンドポイントからターゲット・ディレクトリー・サーバーにコピーされます。

   このチェック・ボックスをクリアすると、エンドポイントの複数のコンテナー内のすべての項目が、ターゲット・ディレクトリー内の指定された 1 つのコンテナーに格納され、階層がフラット化されます。

   Directory Server 内のターゲット・コンテナー
   ターゲット・ディレクトリー・サーバーの検索ベースを指定します。

   このフィールドは、ソース階層をミラーリングするオプションが選択されている場合にのみ表示されます。

   この値は、ソース階層をミラーリングする際にルートとして使用されます。

   ユーザーのターゲット・コンテナー
   個人項目を書き込むコンテナーを指定します。

   このフィールドは、ソース階層をミラーリングするオプションが選択されていない場合にのみ表示されます。

   この値は、ソース階層をフラット化する場合にのみ使用されます。

   グループのターゲット・コンテナー
   グループ項目を書き込むコンテナーを指定します。

   このフィールドは、ソース階層をミラーリングするオプションが選択されていない場合にのみ表示されます。

   この値は、ソース階層をフラット化する場合にのみ使用されます。

デバッグ・ログ出力

このチェック・ボックスを選択すると、追加情報 (処理も同期もされなかった項目に関するエラー情報など) を含む詳細なログ・メッセージが生成されます。

フィルタリングの詳細

同期時に項目を含めるため、または除外するためのフィルター基準を指定します。以下のフィールドで各行に 1 つの基準を入力します。項目は、完全な DN でも、部分的なテキストでもかまいません。

次を含める

同期したいエンドポイントのノードのリストを指定します。

これらの値を使用して、返された項目 DN でサブストリングが検索されます。

次を除外する

同期時に除外したいエンドポイントのノードのリストを指定します。

ユーザー/個人設定

フロー用に選択したエンドポイントのタイプに従い、以下の設定用の一般的なデフォルト値が用意されています。

ソースの個人項目のオブジェクト・クラス

エンドポイントの個人項目のオブジェクト・クラスを指定します。

ターゲットの個人項目のオブジェクト・クラス

ターゲット・ディレクトリーに個人項目を作成するために使用する必要がある項目を指定します。

ソースのユーザー RDN 属性

個人項目の DN の相対 DN として使用される属性を指定します。

ターゲットのユーザー RDN 属性

SDS に書き込まれる項目の RDN として使用される属性を指定します。

グループ設定

フロー用に選択したエンドポイントのタイプに従い、以下の設定用の一般的なデフォルト値が用意されています。

ソースのグループ項目のオブジェクト・クラス

エンドポイントのグループ項目のオブジェクト・クラスを指定します。

ターゲットのグループ項目のオブジェクト・クラス

ターゲット・ディレクトリーにグループ項目を作成するために使用する必要がある項目を指定します。

ターゲットのグループ・メンバーシップ属性
ターゲット・ディレクトリーのグループ・メンバーシップを保持するための属性を指定します。

フロー・フック
オプションで、さまざまなタイプのフロー操作の前後で呼び出す必要がある AssemblyLine を指定できます。

『フロー・フックを使用したフローのカスタマイズ』を参照してください。

拡張設定
必要な場合は、Federated Directory Server コンソールで指定された設定をオーバーライドするためのカスタム・プロパティーを指定することができます。

34 ページの『カスタム・プロパティーの構成』を参照してください。

次のタスク

不要なフローを削除する場合は、そのフローの構成ページを閉じます。「**フロー**」ページでフローの名前をクリックし、「**フローの削除**」をクリックします。確認メッセージが表示されたら「**OK**」をクリックします。

1. フローの機能拡張を構成することができるのは、以下のとおりです。
   - 属性マップをカスタマイズする
   - 結合を定義する
   - 書き戻しを有効にする
2. フロー設定の定義がすべて完了したら、初期同期操作を実行します。
3. 次に、増分同期を手動で実行するか、定期的な同期のスケジューリングを行います。

フロー・フックを使用したフローのカスタマイズ

フロー・フックを使用して、さまざまなタイプのフロー操作の前後で呼び出す必要がある AssemblyLine を指定することによって、フローをカスタマイズすることができます。また、Federated Directory Server コンソールの設定をオーバーライドするカスタム・プロパティーを指定することもできます。

始める前に

1. 構成エディターを使用して AssemblyLine を作成します。
2. AssemblyLine プロジェクト用の構成 XML ファイルを *sdi_solution_dir*/configs フォルダーにコピーします。

IBM Security Directory Integrator の資料の『構成エディター』のセクションを参照してください。

このタスクについて

フロー・フックは、フローの操作の中でカスタム AssemblyLine を呼び出してさまざまな処理を実行できるポイントです。例えば、項目および属性のフィルター処理、監査、アラート生成、およびイベント生成のための AssemblyLine を呼び出す

ことができます。ファイルの移動や名前変更など、フロー前およびフロー後の処理のための AssemblyLine を呼び出すこともできます。

以下の例は、フロー・フックを使用することが推奨される典型的なシナリオです。

- 各書き込み操作の前に項目または特定の属性でプライバシー・コントロールを実行する場合。
- 書き込み操作をした後に、他のシステム (IBM Security Access Manager など) をプロビジョニングする場合。ターゲット・ディレクトリー・サーバーに書き込まれた項目は、`afterwrite` フックの AssemblyLine にも渡されます。この情報を他のシステムと同期できるほか、監査イベントを送信することもできます。

手順

1. 「**フロー**」ページで、フローの名前をクリックしてから「**編集**」をクリックします。
2. 「**ソース**」タブで、「**フロー・フック**」をクリックします。
3. 「**フックの使用可能化**」を選択してフロー・フックを使用可能にします。すべてのフロー・フックを使用不可にするには、このチェック・ボックスをクリアします。このオプションは、個々の設定をオーバーライドして、各操作の個々のフロー・フックを使用可能にします。
4. アクティブにするフックの横にある「**使用可能**」チェック・ボックスをクリックします。このオプションは、すべてのフロー・フックに対するグローバルな「**フックの使用可能化**」オプションが選択されている場合にのみ機能します。
5. AssemblyLine を指定するために、使用可能化されたフックを展開して「**ブラウズ**」をクリックします。 *sdi_solution_dir*`/configs` フォルダー内の使用可能な AssemblyLine が表示されます。
6. フロー・フック用に呼び出す AssemblyLine を選択します。

   以下のフックは Federated Directory Server コンソールで構成できます。

   フロー開始時

   フロー操作の開始時に、指定した AssemblyLine が呼び出されます。このフックは、プロパティーが検査されて処理された後、かつエンドポイントやターゲット・ディレクトリー・サーバーへの接続が行われる前に実行されます。

   このフックを使用して、接続および処理の準備を行うコマンドを実行します。

   例えば、ファイルのスキャンや移動を行ったり、ファイル・エンドポイント・ソース用の情報をダンプするコマンドを実行したりするために使用します。

   プロパティー名は、`hook.prolog` です。

   書き込み前

   現在の項目がソース・エンドポイントから読み取られ、オプションの結合操作が実行されてから、指定した AssemblyLine が呼び出されます。データがターゲット・ディレクトリー・サーバーに書き込まれる前に呼び出されます。

このフックを使用して、項目と属性、またはそれらの値でフィルターを掛けることができます。

プロパティー名は、hook.beforewrite です。

ユーザーの追加/変更/削除
ターゲット・ディレクトリー・サーバーで個人項目を追加、変更、または削除する書き込み操作の後に、指定した AssemblyLine が呼び出されます。

このフロー・フックを使用して、IBM Security Access Manager をプロビジョンする AssemblyLine を呼び出すこともできます。

グループの追加/変更/削除
ターゲット・ディレクトリー・サーバーでグループ項目を追加、変更、または削除する書き込み操作の後に、指定した AssemblyLine が呼び出されます。

このフロー・フックを使用して、IBM Security Access Manager をプロビジョンする AssemblyLine を呼び出すこともできます。

ユーザー・オブジェクトと同じ AssemblyLine を使用します
「**ユーザーの追加/変更/削除**」フックに指定したものと同じプロパティーを「**グループの追加/変更/削除**」フックにも使用する場合にこのチェック・ボックスを選択します。「**グループの追加/変更/削除**」フックに別のプロパティーを指定するには、このチェック・ボックスをクリアします。

フロー・エラー
フロー操作でエラーが発生するたびに、指定した AssemblyLine が呼び出されます。

フロー終了時
フローがソース・エンドポイントから入力項目を経由するサイクルを終了するとき (フロー操作の完了時およびシャットダウン時) に、指定した AssemblyLine が呼び出されます。

関連概念:

71 ページの『第 2 章 Federated Directory Server Plug-in for IBM Security Access Manager』
1 つ以上のディレクトリーを IBM Security Access Manager 用の認証ソ ースとして使用するには、このプラグインを構成します。例えば、Active Directory と Sun Directory Server を認証ソースとして使用できます。ユーザー管理とパスワードは個々の ID ストアに配置したままです。

カスタム・プロパティーの構成

Federated Directory Server コンソールで指定された設定をオーバーライドするためのカスタム・プロパティーを指定することができます。

このタスクについて

カスタム・プロパティーを使用して、Federated Directory Server コンソールでエンドポイント、ターゲット・ディレクトリー・サーバー接続、またはフローに対して指定された設定をオーバーライドすることができます。また、カスタム・プロパテ

ィーを使用して、コンソールで使用できない設定を構成することもできます。

手順

1. カスタム・プロパティーを指定するには、「**フロー**」ページでフローの名前をクリックしてから「**編集**」をクリックします。
2. 「**ソース**」タブで「**詳細設定**」をクリックします。
3. 「**カスタム・プロパティー**」フィールドで、構成するカスタム・プロパティーをそれぞれ別の行に入力します。

   各設定のカスタム・プロパティー名は、以下の手順により、IBM Security Directory Integrator 構成エディターで探すことができます。

   a. コネクターの構成ページで「**接続**」タブをクリックします。
   b. フィールドの隣にある編集アイコンをクリックして式エディターを開きます。
   c. 表示される「**内部名**」が、カスタム・プロパティー名です。

   以下のフロー・フックはコンソールで使用できませんが、カスタム・プロパティーとして構成することができます。

   hook.onsuccess
   このフックは、フローが正常に完了するときに呼び出されます。

   hook.onfailure
   このフックは、エラーが原因でフローが停止するときに呼び出されます。

   hook.onshutdownrequest
   このフックは、シャットダウン要求がフローに送信されたときに呼び出されます。

   hook.afterwrite
   コンソールから構成できる `afterwrite` フックは、書き込み操作に成功して項目が変更された場合のみを対象としています。しかし、カスタム・プロパティーでは、書き込み状況が成功、失敗、またはスキップの場合に呼び出される限定なしの `afterwrite` フックを構成できます。これは、操作の結果として項目が変更されなかった場合にも呼び出すことができます。

例

カスタム・プロパティーの使用法を以下の例に示します。

カスタム・プロパティーの指定によるコンソール設定のオーバーライド
「**一般設定**」ページで「**デバッグ・ログ出力**」を有効にすると、詳細なログを生成できます。この設定をオーバーライドするには、カスタム・プロパティー設定の `global.debug=true` を入力します。この設定は、IBM Security Directory Integrator ソリューションに渡されます。

コンソールで使用できないカスタム・プロパティーの指定
`onfailure` フロー・フックは Federated Directory Server コンソールで使用できません。このフロー・フックを使用すると、エラーが原因でフローが停止するときに AssemblyLine を呼び出すことができます。このフロー・フックを有効にするには、以下のカスタム・プロパティーを使用します。

```
hook.onfailure.AL=hookProject:/AssemblyLines/FlowFailure
hook.onfailure.enabled=true
```

属性マップをフロー用に拡張する

フローのすべての関係に、拡張マッピングとデータ変換を含めることができます。フローをセットアップすると、フロー操作の実行時に適用する必要のあるカスタム属性マップを指定することができます。ユーザーとグループ用に定義されている属性マップからマップを選択し、それらのマップを特定のフロー用に拡張することができます。

始める前に

属性マップをカスタマイズします。

このタスクについて

カスタム属性マップを使用して、ソース・エンドポイント・スキーマの属性がターゲット・スキーマの対応する属性に変換されます。

手順

1. 「**フロー**」タブでフローの名前をクリックし、「**編集**」をクリックしてフロー構成ページを開きます (まだ開いていない場合)。
2. フロー構成ページで「**属性マップ**」タブをクリックし、「**個人オブジェクト**」または「**グループ・オブジェクト**」をクリックして、ユーザーまたはグループのカスタム・マッピングを表示します。
3. 「**個人オブジェクト用マップの選択**」リストまたは「**グループ・オブジェクト用マップの選択**」リストで、フロー操作に適用するマップを指定します。

   個人オブジェクトの場合のデフォルトは `person.map`、グループ・オブジェクトの場合のデフォルトは `group.map` です。

   リストから、別のマップを選択することもできます。このリストには、Federated Directory Server に付属している、すぐに使用できるカスタム属性マップと、以前にカスタマイズされたマップの両方が表示されます。
4. 属性マッピングを拡張するには、以下のいずれかのアクションを実行します。

   属性マッピングを作成する

   a. 「**属性の追加**」をクリックします。
   b. ターゲット・ディレクトリー・サーバーの属性リストから属性を選択します。「**Directory Server 属性**」の下に、選択した属性名を示す新しい行が表示されます。

      注: ターゲット・ディレクトリーからの属性のリストが「属性の追加」ウィンドウに表示されない場合、以下のアクションを実行します。

      1) ナビゲーション・ペインの「**Directory Server**」で、「**接続設定**」に移動します。
      2) 「**テスト接続**」をクリックします。エンドポイントの名前の横に緑色のチェック・マークが表示されていることを確認します。こ

れは、正常に接続されていることを示します。このアクションにより、ターゲット・ディレクトリー属性を参照するフィールドにデータが取り込まれます。

c. 「**エンドポイント属性/割り当て**」の下で、マッピングを変更するためにデフォルト値をダブルクリックして、属性マッピングの詳細設定を指定します。

d. この属性マッピングをエンドポイントに対して使用するには、「**使用可能**」を選択します。

e. マッピングのタイプを指定するには、「**単純な割り当て**」または「**スクリプト化された割り当て**」をクリックします。

注: 「**スクリプト化された割り当て**」を選択した場合、JavaScript コードを作成するか、*sdi_solution_dir*¥LDAPSync¥customScript.js ファイルで関数を呼び出すことにより、割り当てを定義することができます。詳しくは、IBM Security Directory Integrator の資料を参照して、『*IBM Security Directory Integrator のスクリプト*』を検索してください。

f. 「**マップするタイミング**」の下で、このマッピングをすべての操作で使用するか、または項目を変更あるいは作成するときにのみ使用するかを指定します。

g. 「**属性の選択**」フィールドで、ターゲット属性にマップする必要があるソース・エンドポイントの属性名を指定します。

特定の属性のマッピングを削除する

a. 属性行のチェック・ボックスを選択します。

b. 「**属性の除去**」をクリックします。

c. 「**OK**」をクリックします。

5. 「**保存**」をクリックします。編集した各マップを保存しない限り、変更は失われます。

タスクの結果

カスタム属性マップを拡張すると、予防策として、元の属性マップ・ファイルのコピーが変更されます。この新規ファイルは、このフロー固有のファイルです。このファイル名には、接頭部として Flow_*flow_name* が付けられます。例: Flow_ADFlow_person.map。

すべての属性マップは、*sdi_solution_dir*¥LDAPSync ディレクトリーに格納されます。

結合の構成

エンドポイントからのデータを拡張して強化するには、フローを構成して、別のデータ・ソースからの選択的な結合を指定します。

このタスクについて

フローは、あるエンドポイントのデータを別のエンドポイントのデータと結合することができます。例えば、LDAP ディレクトリーでは使用できないユーザー情報が

データベースに格納されている場合があります。そのデータベースに LDAP ディレクトリーを結合すると、そのユーザーに関するより豊富なデータを Federated Directory Server で表示できるようになります。

エンドポイントから項目が渡されるたびに、フローはその項目を結合データ・ソースで検索し、エンドポイントからのデータとマージして、ターゲットの IBM Security Directory Server に追加します。

注: 検索をサポートしているエンドポイントのみ、結合で使用することができます。例えば LDAP などエンドポイントは、特定の基準を使用する検索をサポートしているため、結合で使用することができます。一方、ファイル・ベースのエンドポイントは検索をサポートしていないため、結合で使用することはできません。

手順

1. 「**フロー**」タブでフローの名前をクリックし、「**編集**」をクリックしてフロー構成ページを開きます (まだ開いていない場合)。
2. 「**結合**」タブをクリックし、結合用のディレクトリーまたはデータ・ソースのプロパティーを表示して編集します。
3. 「**使用可能**」を選択して、このフローに結合を適用します。
4. 「**エンドポイントの選択**」リストから、結合で使用するエンドポイントを選択します。「**エンドポイントの選択**」リストには、Federated Directory Server で構成したエンドポイントがすべて表示されます。「**使用可能**」チェック・ボックスをクリアすると、「**エンドポイントの選択**」フィールドが使用不可になります。以前に入力した設定は保持されますが、フロー操作の実行時には適用されません。
5. フロー操作の実行時に結合が原因で項目に関するエラーや障害が発生した場合に実行する必要のあるアクションを指定します。「**結合で障害が発生しました**」リストから、以下のいずれかのオプションを選択します。
   - **エラーを無視して続行します**: このオプションを選択した場合、エラーが無視され、項目が追加、変更、または削除されます。フロー操作は、次の項目の処理に進みます。
   - **現在の項目をスキップして続行します**: このオプションを選択した場合、エラーの原因となった項目がスキップされ、フロー操作が続行されます。
   - **フローを中止して終了します**: このオプションを選択した場合は、フロー操作がこの項目で終了します。

   「**ソース**」タブの「**一般設定**」の「**デバッグ・ログ出力**」を有効にすると、エラーの原因となった項目に関する詳細を表示することができます。
6. ステートメントを使用して、単純な基準を指定したり、拡張基準用のスクリプトを指定することができます。
   - 単純な基準を指定して、結合内で一致する項目を検索するには、「**スクリプト化されている基準**」チェック・ボックスをクリアしたまま、基準ステートメントを指定します。
     - 結合エンドポイントの属性を「**属性**」フィールドに入力します。
     - 「**演算子**」リストで、そのステートメント用の適切な演算子を選択します。
     - メイン・エンドポイントの対応する属性を「**値**」フィールドに入力します。

- スクリプトを使用して拡張基準を指定するには、「**スクリプト化されている基準**」を選択します。拡張基準用のスクリプトを記述するためのフィールドが表示されます。詳しくは、IBM Security Directory Integrator の資料を参照して、『*IBM Security Directory Integrator* のスクリプト』を検索してください。

7. 「**属性マップ**」の下で、結合用の属性マッピングの追加、削除、変更を行うことができます。
   a. 「**属性の追加**」をクリックし、ターゲット・ディレクトリー・サーバーの属性リストから属性を選択します。 「**Directory Server 属性**」列の下に、選択した属性名を示す新しい行が表示されます。
   b. 「**エンドポイント属性/割り当て**」の下で、ターゲット属性にマップする必要があるエンドポイントの属性名を指定します。
   c. エンドポイント属性の名前をダブルクリックして、属性マッピングの詳細設定を指定します。
      - この属性マッピングをエンドポイントに対して使用するには、「**使用可能**」を選択します。
      - マッピングのタイプを指定するには、「**単純な割り当て**」または「**スクリプト化された割り当て**」をクリックします。「**スクリプト化された割り当て**」を選択した場合、JavaScript コードを作成するか、*sdi_solution_dir*¥LDAPSync¥customScript.js ファイルで関数を呼び出すことにより、割り当てを定義することができます。詳しくは、IBM Security Directory Integrator の資料を参照して、『*IBM Security Directory Integrator* のスクリプト』を検索してください。
      - このマッピングをすべての操作で使用するか、項目の変更時または作成時にのみ使用するかを指定します。
   d. 特定の属性のマッピングを削除するには、その行のチェック・ボックスをクリックします。次に「**属性の除去**」をクリックし、確認メッセージが表示されたら「**OK**」をクリックします。
8. エンドポイントの代わりに独自の AssemblyLine を指定して、結合操作を定義することもできます。その場合は、「**ルックアップ/結合 AssemblyLine のカスタマイズ**」セクションを展開し、「**個人オブジェクト**」、「**グループ・オブジェクト**」、および「**コンテナー・オブジェクト**」を指定します。

   これらのフィールドを使用するには、構成エディターを使用して AssemblyLine を作成する必要があります。AssemblyLine プロジェクト用の構成 XML ファイルが *sdi_solution_dir*/configs フォルダーにコピーされていることを確認してください。詳しくは、IBM Security Directory Integrator の資料で『構成エディター』を検索してください。

   構成エディターで作成した AssemblyLine プロジェクトに関する以下の詳細情報を「**ルックアップ/結合 AssemblyLine のカスタマイズ**」フィールドに入力します。

   - AssemblyLine が含まれている IBM Security Directory Integrator プロジェクトの名前
   - AssemblyLine の名前

   これらのフィールドに名前を入力する場合は、以下の形式で入力してください。

Project Name:/AssemblyLines/*AssemblyLine Name*

例えば、プロジェクトの名前が OS400 で、このプロジェクトに ReadUsers という AssemblyLine が含まれている場合は、以下のように入力します。

```
OS400:/AssemblyLines/ReadUsers
```

フローに対して書き戻し機能を使用可能にする

選択された属性に対する書き戻し機能をフローに対して使用可能にすることにより、ターゲット・ディレクトリー・サーバーで行われた変更をエンドポイントに伝搬することができます。

始める前に

グローバル書き戻しオプションは、すべてのフローについて書き戻し機能をオフにできる安全機能として用意されています。ただし、書き戻し機能をグローバルにオフにすると、書き戻し機能を使用可能にする必要がある特定のフローを含むすべてのフローについて、書き戻しが禁止されます。そのため、最初にすべてのフローについて、書き戻し機能をグローバル・レベルで使用可能にする必要があります。13 ページの『グローバル書き戻しを使用可能または使用不可にする』を参照してください。

グローバル書き戻し機能を使用可能にしたら、以下の手順を実行して、特定のフローについて書き戻し機能を使用可能にする必要があります。

このタスクについて

このフローのターゲットである個人項目に対する変更だけが、書き戻し操作の候補になります。

次のステップに記載されている選択された属性のみが、書き戻し操作によって処理されます。

手順

1. 特定のフローについて書き戻し機能を使用可能にするには、「**フロー**」タブでフローの名前をクリックし、「**編集**」をクリックします。 フローの構成ページが開きます。
2. 「**書き戻し**」タブをクリックします。
3. 「**使用可能**」を選択して、このフローに対する書き戻しオプションを使用可能にします。
4. 書き戻し操作を起動する必要があるディレクトリー・サーバーの属性を指定し、それをエンドポイントの属性にマップします。
   a. 「**属性の追加**」をクリックして、エンドポイントの属性リストから属性を選択します。 「**エンドポイント属性**」列の下に、選択した属性名を示す新しい行が表示されます。
   b. 「**Directory Server 属性/割り当て**」の下で、エンドポイント属性にマップする必要があるディレクトリー・サーバーの属性名を指定します。
   c. ディレクトリー・サーバーの属性名をダブルクリックして、属性マッピングの詳細設定を指定します。

- この属性マッピングを書き戻し操作で使用する場合は、「**使用可能**」を選択します。
- マッピングのタイプを指定するには、「**単純な割り当て**」または「**スクリプト化された割り当て**」をクリックします。「**スクリプト化された割り当て**」を選択した場合、JavaScript コードを作成するか、*sdi_solution_dir*¥LDAPSync¥customScript.js ファイルで関数を呼び出すことにより、割り当てを定義することができます。詳しくは、IBM Security Directory Integrator の資料を参照して、『*IBM Security Directory Integrator* のスクリプト』を検索してください。

d. 特定の属性のマッピングを削除するには、その行のチェック・ボックスをクリックします。次に「**属性の除去**」をクリックし、確認メッセージが表示されたら「**OK**」をクリックします。

タスクの結果

書き戻し操作が実行されると、エンドポイントに対して書き戻された内容の要約が表示されます。この要約には、フロー名、変更された属性、ディレクトリー・サーバーとエンドポイントの DN などの詳細情報が表示されます。「**フィルター**」フィールドを使用して、書き戻しの要約を検索することができます。

フロー構成の検証

フローを構成してフロー操作の基準を指定したら、同期のシミュレーションを実行してフローを検証することができます。

始める前に

フローが作成されて定義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

同期のシミュレーションでは、初期同期と同じ操作が実行されますが、ディレクトリー・サーバーには何も書き込まれません。この機能は、計画の初期段階で、フローがエンドポイントの正しいデータ・サブセットを選択できるかどうかを確認する場合に役立ちます。

手順

1. 「**フロー**」ページで、フローの名前をクリックして「**同期化の実行**」をクリックします。
2. 「同期化の実行」ウィンドウで、「**シミュレート**」を選択します。

タスクの結果

フロー用に指定された基準に従って、ソース・システムからの完全な同期がシミュレーションされます。

「**最後のアクティビティー**」列の下に、進行状況を示すバーが表示されます。状況とログは、フローの下に表示されます。

次のタスク

進行中のシミュレーション操作を停止する場合は、フローの名前をクリックして「**終了**」をクリックします。確認メッセージが表示されたら「**OK**」をクリックします。

操作が完了すると、シミュレーションの詳細 (日付、操作、変更された属性など) が新しいタブに表示されます。「**フィルター**」フィールドを使用して、テーブルを検索することができます。

状況とログを参照して、同期のシミュレーションが成功したかどうかを確認したり、エラーをデバッグしたりすることができます。

同期のシミュレーションを実行してフローを検証したら、初期同期を実行して、データをディレクトリー・サーバーにマイグレーションします。

ターゲット・ディレクトリーのデータの同期

フロー設定を定義したら、エンドポイントのデータをターゲットの IBM Security Directory Server に同期することができます。この処理は、手動で行うことも、定期的な間隔で実行される自動同期のスケジュールをセットアップして行うこともできます。

初期同期の実行

フロー設定を定義したら、初期同期を実行して、データをエンドポイントからターゲットの IBM Security Directory Server にマイグレーションすることができます。

始める前に

フローが作成されて定義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

フローの初期同期は、一回限りの操作です。初期同期では、エンドポイントの項目のうち、フロー基準に一致するすべての項目が選択され、ディレクトリー・サーバーが更新されます。

手順

1. 「**フロー**」ページで、フローの名前をクリックして「**同期化の実行**」をクリックします。
2. 「同期化の実行」ウィンドウで、「**イニシャル同期**」を選択します。

タスクの結果

フロー用に指定された基準に従って、ソース・システムからの完全な同期が開始されます。現在の同期状態データはすべてリセットされます。

「**最後のアクティビティー**」列の下に、進行状況を示すバーが表示されます。状況とログは、フローの下に表示されます。

次のタスク

進行中の同期操作を停止する場合は、フローの名前をクリックして「**終了**」をクリックします。確認メッセージが表示されたら「**OK**」をクリックします。フロー操作を途中で終了すると、フロー操作が部分的に同期された状態になるため、注意が必要です。

操作が完了したら、状況とログを調べて、同期が正常に終了したかどうかを確認します。エラーがある場合は、そのエラーをデバッグします。

初期同期が正常に完了したことを確認したら、特定の間隔で同期のスケジュールをセットアップすることができます。

増分同期の実行

初期同期を実行したら、エンドポイントで行われた変更に基づいて、ターゲットの IBM Security Directory Server データの増分同期を実行することができます。手動で同期を実行することも、定期的な間隔で実行される自動同期のスケジュールをセットアップすることもできます。

始める前に

- フローの作成と定義を行います。
- フローの初期同期を実行します。

手順

1. 「**フロー**」ページで、フローの名前をクリックして「**同期化の実行**」をクリックします。
2. 「同期化の実行」ウィンドウで、「**増分同期**」を選択します。

タスクの結果

同期操作が開始され、「**最後のアクティビティー**」列の下に、進行状況を示すバーが表示されます。

次のタスク

進行中の同期操作を停止する場合は、フローの名前をクリックして「**終了**」をクリックします。確認メッセージが表示されたら「**OK**」をクリックします。フロー操作を途中で終了すると、フロー操作が部分的に同期された状態になるため、注意が必要です。

操作が完了したら、状況とログを調べて、同期が正常に終了したかどうかを確認します。エラーがある場合は、そのエラーをデバッグします。

同期を一定間隔で自動的に実行するには、特定の間隔で実行される同期のスケジュールをセットアップします。

同期のスケジューリング

スケジュールを指定して、フローでの増分同期操作を一定の間隔で自動的に実行することができます。

始める前に

- フローの作成と定義を行います。
- フローの初期同期を実行します。

手順

1. 初めてフロー操作のスケジュールを作成する場合は、「**フロー**」ページのフロー名の下で「**スケジュールなし**」をクリックします。既に作成されているスケジュールを編集する場合は、フローの下に表示されている、次回スケジュールされている操作の日時をクリックします。
2. 「スケジュール」ウィンドウで「**使用可能**」をクリックして、スケジューラーをアクティブにします。
3. スケジュールのタイプを選択します。
   - 「**タイマー**」を選択した場合は、スケジュールに指定された間隔で同期が実行されます。
   - 「**キープアライブ**」を選択した場合は、エンドポイントでタイムアウト値が指定されていても、継続して同期が実行されます。
4. フロー操作の頻度として、「**毎月**」または「**選択された月**」を選択します。「**選択された月**」を選択した場合は、月名が表示されます。1 つ以上の月を選択する必要があります。
5. フロー操作を実行する日を、「**毎日**」、「**平日**」 (曜日を指定)、「**選択された日**」 (月の日を指定) の各オプションから選択します。
6. 「**時/分/秒**」セクションで、フロー操作を開始する時刻を入力します。ワイルドカードの「*」(アスタリスク)、コンマ区切りリスト、または数字の範囲を入力して、時、分、秒を指定することもできます。

   例を示します。
   - 毎正時に同期を実行する場合は、「**時**」フィールドに `*` を入力し、「**分**」フィールドと「**秒**」フィールドの両方のに `0` を入力します。
   - 15 分ごとに同期を実行する場合は、「**時**」フィールドに `*`、「**分**」フィールドに `0,15,30,45`、「**秒**」フィールドに `0` をそれぞれ入力します。
7. 「**使用可能**」を選択します。
8. 次の操作が開始されるまでにフロー操作が完了しない可能性がある場合は、「**既に実行中の場合は開始しない**」を選択します。このオプションを選択すると、同じ操作の 2 つのインスタンスが同時に実行されることがなくなるため、長時間にわたる操作の場合に役立ちます。
9. 障害が発生した場合にフロー操作を停止する場合は、「**AssemblyLine が失敗した場合にスケジュールを強制終了する**」を選択します。 例えば、このオプションを有効にすると、失敗した同期が自動的に繰り返し実行される前に、ログ・ファイルに記録されているエラーを修正することができます。
10. 「**クローズ**」をクリックして、スケジュールを保存します。

タスクの結果

次にスケジュールされているフロー操作の日時がフローの下に表示されます。

次のタスク

今後スケジューラーを使用しない場合は、「スケジュール」ウィンドウの「**使用可能**」チェック・ボックスをクリアします。

ログとレポートの表示

同期アクティビティーが完了したら、ログを表示して同期が成功したかどうかを確認することができます。

このタスクについて

「**フロー**」ページの各フローの下に、フロー操作の要約が表示されます。以下の情報が表示されます。

- 追加、変更、削除されたユーザーの数
- 追加、変更、削除されたグループの数
- このフローで最後に実行されたアクティビティー
- 処理されたユーザーとグループの総数

フローの一般設定を定義する際に「**デバッグ・ログ出力**」オプションを選択した場合は、デバッグ用の詳細情報が記録されたログが生成されます。

手順

1. 詳細ログを表示するには、「**ログを表示**」リストから操作を選択します。最後の操作がデフォルトで表示されます。リストされている以前のログのうち、任意のログを選択することができます。

   注: 保管する必要がある履歴ログ・ファイルの数を変更する方法については、15 ページの『ログ設定の指定』を参照してください。
2. ログ内の以下のいずれかのセクションをクリックすると、詳細レポートが表示されます。

   要約 以下の要約が表示されます。
   - 処理されたユーザー項目、グループ項目、コンテナー項目の数
   - エラーと警告の数
   - スキップされ、ターゲット・ディレクトリーに正常に書き込まれなかった項目の数

   エラー・ログ
   すべてのエラーと警告が表示されます。詳細情報を参照することにより、同期におけるすべての失敗について、トラブルシューティングを行うことができます。

   マイグレーション・ログまたは同期ログ
   初期同期のログを表示している場合は、マイグレーション・ログが表示されます。それ以外の場合は、同期操作のログが表示されます。このログには、フロー操作全体の詳細情報が含まれています。

モニター

Federated Directory Server コンソールには、フローの動作および正常性をモニターするためのオプションが用意されています。

モニターには以下のオプションを使用できます。

- セキュリティー・イベントは Syslog 経由で QRadar に送信できます。セキュリティー・イベントは、ターゲット・ディレクトリー・サーバーに対する項目の追加、変更、または削除のときに定義されます。
- エラー・イベントは、エラーが発生してログに記録されたときに SNMP トラップとして発行できます。
- カスタム・モニターを有効にすると、他のフック (標準のものとモニター (QRadar と SNMP) の両方を含みます) がアクティブ化される前にただちに開始されます。

モニターの設定を構成するには、Federated Directory Server のナビゲーション・ペインの「**共通設定**」で「**モニター**」をクリックします。

QRadar モニターの構成

ターゲットの IBM Security Directory Server で項目の追加、変更、または削除が行われるときに発生するセキュリティー・イベントを追跡するには、QRadar モニターを構成します。

手順

1. ナビゲーション・ペインで、「**共通設定**」の下の「**モニター**」をクリックします。
2. 「モニター」ページで「**QRadar**」タブをクリックします。
3. 「QRadar」ページで「**使用可能**」を選択し、セキュリティー・イベントをモニターすることを指定します。
4. 「**ホスト名**」フィールドに、セキュリティー・イベントを受信すべき QRadar サーバーのホスト名または IP アドレスを入力します。
5. 「**ポート**」フィールドに、QRadar サーバーが Syslog イベントを受信すべきポートの番号を入力します。
6. 「**重大度**」リストから、Syslog イベントの重大度の値を選択します。
7. 「**機能**」フィールドで、Syslog イベントの機能の値を選択します。
8. 「**マップ・ファイル**」フィールドに、イベントの各種の QRadar LEEF 属性をセットアップするために使用するマップ・ファイルのパスおよびファイル名を指定します。
9. 「**選択...**」をクリックしてマップ・ファイルを参照します。デフォルト値は `LDAPSync/QRadar.map` ファイルを指します。
10. オプション: 「**日付形式マスク**」フィールドで、マップ対象の LEEF 属性に書き込まれる日付値に対する標準の Java `SimpleDateFormat` マスクを指定します。

この値は、**devTimeFormat** 属性の値と、イベントの日付値の形式の両方を制御します。デフォルト値は ISO 8601 規格のマスク MMM dd yy HH:mm:ss であり、Oct 16 12 15:15:57 などのストリングを生成します。

SNMP モニターの構成

フロー操作中にエラーがログに記録されるたびに発生するエラー・イベントを追跡するには、SNMP モニターを構成します。

手順

1. ナビゲーション・ペインで、「**共通設定**」の下の「**モニター**」をクリックします。
2. 「モニター」ページで「**SNMP**」タブをクリックします。
3. 「SNMP」ページで「**使用可能**」を選択し、エラー・イベントをモニターすることを指定します。
4. 「**ホスト名**」フィールドに、エラー・イベントを受信すべき SNMP モニターのホスト名または IP アドレスを入力します。
5. 「**トラップ・ポート**」フィールドに、SNMP がトラップを listen するポートの番号を入力します。
6. 「**コミュニティー・ストリング**」フィールドに、出力された SNMP トラップに使用するコミュニティー・ストリングを指定します。

   正しいコミュニティー名を認識していないデバイスは SNMP 操作から除外されるため、SNMP コミュニティー名は、弱い認証として機能します。このコミュニティー・ストリングに一致しないメッセージは、すべて破棄されます。

   ブランクにしておくと、すべてのコミュニティー・ストリングが受け入れられます。デフォルト値は public です。
7. 「**マップ・ファイル**」フィールドで、出力される SNMP トラップに渡される各種のオブジェクト ID (OID) をセットアップするマップ・ファイルのパスとファイル名を指定します。デフォルト値は LDAPSync/SNMP.map です。

タスクの結果

使用可能にした場合は、SNMP モニター機能がエラー・メッセージおよびエラー・レベル (ERROR、WARN、または FATAL) を渡します。

次のタスク

sdi_solution_dir/LDAPSync から SNMP サーバーの MIB リポジトリーに IBM-FDS-MIB.txt をコピーして、Federated Directory Server から送信された SNMP メッセージを SNMP サーバーが正しく解釈できるようにすることができます。SNMP デバイスが Federated Directory Server の MIB ファイルを使用するための構成については、SNMP サーバー管理者にお問い合わせください。

カスタム・モニターの構成

カスタム・モニター・オプションは、フロー操作中の各アクティブ・フック・ポイントで任意の数のアクションを実行するために使用します。

このタスクについて

カスタム・モニターを構成すると、指定した AssemblyLine がフロー操作のすべての標準のフック・ポイントで呼び出されます。呼び出しは、実際のフロー・フックが使用不可になっていても、そのフックの AssemblyLine が開始される前に行われます。

手順

1. ナビゲーション・ペインで、「**共通設定**」の下の「**モニター**」をクリックします。
2. 「モニター」ページで「**カスタム**」タブをクリックします。
3. 「カスタム」ページで「**使用可能**」を選択し、カスタム AssemblyLine の呼び出しによってフロー・イベントをモニターすることを指定します。
4. 「**カスタム AssemblyLine**」フィールドに、カスタム・モニターに使用する AssemblyLine を指定します。

タスクの結果

カスタム・モニターは、他のフロー・フックをアクティブ化する直前に開始されます。

カスタム・ターゲット構成

デフォルトでは、Federated Directory Server ターゲットは IBM Security Directory Server インスタンスであり、これはコンソールの「**接続設定**」で構成できます。IBM Security Directory Server 以外のターゲットを構成するには、ターゲットへの接続設定および同期を処理するカスタム・コネクターおよびカスタム AssemblyLine を定義する必要があります。

構成の説明および例については、技術文書、「Federated Directory Server custom target configuration」を参照してください。

既知の問題、制限、および回避策

Federated Directory Server の使用時に発生する可能性のある問題を解決するには、提供されている問題の説明とその解決策を参照してください。

ネストされたグループ・メンバーシップが初期同期中に失われる

問題 初期同期中に、まだ同期されていないメンバー・グループを含んだグループが処理されると、このメンバーが欠落しているとみなされます。

解決策 ネストされたメンバーシップがすべて処理されるようにするには、初期同期後に再度フローを使用して、欠落メンバーがあるすべてのグループを再実行します。また、「メンバーの欠落」を通知するすべてのエラー・メッセージの表示を、グループ処理のこの最終ラウンドまで遅らせます。

ページ・サイズ値を取得した後に初期同期が失敗する

問題 Windows Server 2008 R2 システムで、「ページ・サイズ」で設定された値を取得した後に初期同期が失敗する。

これは、Active Directory を使用する操作特有の問題です。

説明 この問題は、以下のシナリオで発生します。

- Windows Server 2008 R2 システム上に存在する Active Directory のユーザー数とグループ数が多い (10,000 ユーザー、10,000 グループなど)。
- Active Directory エンドポイントのページ・サイズが、デフォルト値の 500 に設定されている。
- これらの項目を IBM Security Directory Server にマイグレーションするようにフローが定義されている。

上記のシナリオで初期同期操作を実行すると、500 ユーザーがマイグレーションされ、エラーが発生します。次に 500 グループがマイグレーションされ、エラーが発生します。ここで操作が終了し、以下のエラーのような OperationNotSupportedException が発行されます。

```
2013-06-12 16:37:31,250 ERROR [AssemblyLine.Flow_ADFlow1_ReadGroups_group.7]
     - [Flow_ADFlow1_ReadGroups_group/Read Groups/Default On Error]
     - [Flow_ADFlow1_ReadGroups_group/Read Groups/Default On Error]
     - javax.naming.OperationNotSupportedException: [LDAP: error code 12
     - 00002040: SvcErr: DSID-031401E7, problem 5010 (UNAVAIL_EXTENSION), data 0
]; remaining name 'ou=set1,dc=adsync,dc=tditest,dc=internal'
     - [LDAP: error code 12 - 00002040: SvcErr: DSID-031401E7,
     problem 5010 (UNAVAIL_EXTENSION), data 0
]
Stacktrace (for support):
javax.naming.OperationNotSupportedException: [LDAP: error code 12
     - 00002040: SvcErr: DSID-031401E7, problem 5010 (UNAVAIL_EXTENSION), data 0
]; remaining name 'ou=set1,dc=adsync,dc=tditest,dc=internal'
 at com.sun.jndi.ldap.LdapCtx.mapErrorCode(LdapCtx.java:3159)
 at com.sun.jndi.ldap.LdapCtx.processReturnCode(LdapCtx.java:3045)
 at com.sun.jndi.ldap.LdapCtx.processReturnCode(LdapCtx.java:2852)
 at com.sun.jndi.ldap.LdapCtx.searchAux(LdapCtx.java:1861)
 at com.sun.jndi.ldap.LdapCtx.c_search(LdapCtx.java:1784)
 at com.sun.jndi.toolkit.ctx.ComponentDirContext.p_search(ComponentDirContext.java:398)
 at com.sun.jndi.toolkit.ctx.PartialCompositeDirContext.search(PartialCompositeDirContext.java:368)
 at javax.naming.directory.InitialDirContext.search(InitialDirContext.java:287)
 at com.ibm.di.connector.LDAPConnector.getNextEntry(LDAPConnector.java:750)
 at com.ibm.di.server.AssemblyLineComponent.executeOperation(AssemblyLineComponent.java:3355)
 at com.ibm.di.server.AssemblyLineComponent.getnext(AssemblyLineComponent.java:932)
 at com.ibm.di.server.AssemblyLine.msGetNextIteratorEntry(AssemblyLine.java:3666)
 at com.ibm.di.server.AssemblyLine.executeMainStep(AssemblyLine.java:3375)
 at com.ibm.di.server.AssemblyLine.executeCycle(AssemblyLine.java:3151)
 at com.ibm.di.server.AssemblyLine.executeCycle(AssemblyLine.java:3091)
 at com.ibm.di.fc.AssemblyLineFC.executeCycle(AssemblyLineFC.java:451)
 at com.ibm.di.fc.AssemblyLineFC.perform(AssemblyLineFC.java:272)
 at sun.reflect.GeneratedMethodAccessor77.invoke(Unknown Source)
 at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:55)
 at java.lang.reflect.Method.invoke(Method.java:613)
 at com.ibm.jscript.types.JavaAccessObject.call(JavaAccessObject.java:321)
 at com.ibm.jscript.types.FBSObject.call(FBSObject.java:161)
 at com.ibm.jscript.ASTTree.ASTCall.interpret(ASTCall.java:175)
 at com.ibm.jscript.ASTTree.ASTAssign.interpret(ASTAssign.java:91)
 at com.ibm.jscript.ASTTree.ASTProgram.interpret(ASTProgram.java:119)
 at com.ibm.jscript.ASTTree.ASTProgram.interpretEx(ASTProgram.java:139)
 at com.ibm.jscript.JSExpression._interpretExpression(JSExpression.java:435)
 at com.ibm.jscript.JSExpression.interpretExpression(JSExpression.java:421)
 at com.ibm.jscript.JSExpression.evaluateValue(JSExpression.java:251)
 at com.ibm.jscript.JSExpression.evaluateValue(JSExpression.java:238)
 at com.ibm.jscript.JSExpression.evaluateValue(JSExpression.java:241)
 at com.ibm.jscript.JSInterpreter.interpret(JSInterpreter.java:57)
 at com.ibm.di.script.ScriptEngine.interpret(ScriptEngine.java:940)
 at com.ibm.di.script.ScriptEngine.interpret(ScriptEngine.java:925)
 at com.ibm.di.server.ScriptComponent.add1(ScriptComponent.java:244)
 at com.ibm.di.server.ScriptComponent.add(ScriptComponent.java:210)
 at com.ibm.di.server.AssemblyLine.msExecuteNextConnector(AssemblyLine.java:3759)
 at com.ibm.di.server.AssemblyLine.executeMainStep(AssemblyLine.java:3379)
 at com.ibm.di.server.AssemblyLine.executeMainLoop(AssemblyLine.java:2988)
 at com.ibm.di.server.AssemblyLine.executeMainLoop(AssemblyLine.java:2971)
 at com.ibm.di.server.AssemblyLine.executeAL(AssemblyLine.java:2940)
 at com.ibm.di.server.AssemblyLine.run(AssemblyLine.java:1319)

2013-06-12 16:37:31,250 ERROR [AssemblyLine.Flow_ADFlow1_ReadGroups_group.7]
     - [Flow_ADFlow1_ReadGroups_group/Read Groups/Default On Error]
     - Make sure that the search base is visible in the source system,
     for example from an LDAP browser.
Also ensure that the credentials defined for the Source connection are
     authorized to see entries in this container.
***** Start dumping: ERROR *****
                    class: 'javax.naming.OperationNotSupportedException'
             connectorname: 'Read Groups'
                 exception: 'javax.naming.OperationNotSupportedException:
     [LDAP: error code 12 - 00002040: SvcErr: DSID-031401E7,
     problem 5010 (UNAVAIL_EXTENSION), data 0
]; remaining name 'ou=set1,dc=adsync,dc=tditest,dc=internal''
                  message: '[LDAP: error code 12 - 00002040: SvcErr: DSID-031401E7,
     problem 5010 (UNAVAIL_EXTENSION), data 0
]'
```

```
                operation: 'get'
                   status: 'fail'
***** End dumping: ERROR *****
***** Connector parameters: Read Groups *****
    ldapUrl: ldap://9.120.98.148:389
    ldapUsername: Administrator@adsync.tditest.internal
    ldapSearchBase: ou=set1,dc=adsync,dc=tditest,dc=internal
    ldapSearchFilter: objectClass=groupofuniquenames
    ldapSearchScope: subtree
    ldapSizeLimit: 0
    ldapPageSize: 500
    jndiExtraProviderParams: null
```

解決策 この問題を回避するには、以下のステップを実行します。

1. Windows Server 2008 R2 Active Directory で、Microsoft サポート技術情報 Web サイト (http://support.microsoft.com/kb/977180) に掲載されている解決策を適用します。
2. Windows レジストリーをバックアップします。
3. レジストリー設定 `HKLM¥System¥CurrentControlSet¥Services¥NTDS¥Parameters` にストリング値 `DSA Heuristics` を追加します。
4. 値を `000000000001` に設定します。
5. システムを再起動します。

リファレンス

Federated Directory Server コンソールの機能やコンポーネントの詳細について理解するには、リファレンス情報を参照してください。

ファイル・パーサー

Federated Directory Server コンソール のファイル・エンドポイント構成ページのリストから、適切なファイル・パーサーを選択して構成することができます。

ファイル・エンドポイント用の CBE パーサー

入力ストリームから XML を読み取り、この XML を Common Base Event (CBE) オブジェクトに変換するには、CBE パーサーを使用します。CBE パーサーは、XML から読み取ると、すべての標準 CBE 属性および CBE オブジェクトを入力マップの属性として返します。

CBE パーサー構成パラメーターにアクセスするには、次のようにします。

1. ファイル・エンドポイントを追加します。
2. 「ファイル」エンドポイント構成ページで、「**パーサー**」をクリックして、リストから「**CBE パーサー**」を選択します。
3. 「**パーサー**」セクションを展開して、パラメーターを表示します。

パラメーター

コメント

このフィールドを使用して、コメントを追加します。データの構文解析時には、このコメントは無視されます。

詳細ログ

追加情報が入った詳細なログ・メッセージを生成するには、このチェック・ボックスを選択します。

以下の詳細パラメーターを構成することもできます。「**パーサー**」セクションで、「**拡張**」を展開して以下のパラメーターを表示します。

文字エンコード
読み取りまたは書き込み時に使用される文字エンコードを指定します。デフォルト値は UTF-8 です。パーサーが XML から読み取るときに、入力ソースにまだエンコードが定義されていない場合にのみ、このパラメーターが使用されます。

CBE パーサーは XML パーサーを拡張したものであるため、同じ文字エンコードのルールが適用されます。詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*XML パーサーにおける文字エンコード*」を検索してください。

XML の妥当性検査
パーサーが指定から要求される XSD スキーマで XML を検査する必要があることを指定するには、このチェック・ボックスを選択します。

XML 宣言の省略
パーサーが出力ストリームで XML 宣言ヘッダーを省略する必要があることを指定するには、このチェック・ボックスを選択します。

CBE パーサーおよびその入出力マップ属性について詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*CBE パーサー*」を検索してください。

ファイル・エンドポイント用の CSV パーサー

コンマ区切り値 (CSV) 形式でデータの読み取りおよび書き込みを行うには、CSV パーサーを使用します。

CSV パーサー構成パラメーターにアクセスするには、次のようにします。

1. ファイル・エンドポイントを追加します。
2. 「ファイル」エンドポイント構成ページで、「**パーサー**」をクリックして、リストから「**CSV パーサー**」を選択します。
3. 「**パーサー**」セクションを展開して、パラメーターを表示します。

パラメーター

フィールド分離文字
各列を分離するために使用する文字 (通常はコンマまたはセミコロン) を指定します。デフォルト値はセミコロン (**;**) です。

フィールドのソート
ヘッダー・フィールドをアルファベット順 (昇順) に書き込むには、このチェック・ボックスを選択します。デフォルト値は false です。

コメント
このフィールドを使用して、コメントを追加します。データの構文解析時には、このコメントは無視されます。

詳細ログ
追加情報が入った詳細なログ・メッセージを生成するには、このチェック・ボックスを選択します。

以下の詳細パラメーターを構成することもできます。「**パーサー**」セクションで、「**拡張**」を展開して以下のパラメーターを表示します。

フィールド名
パーサーが読み取りまたは書き込みを行う必要がある各列の名前を指定します。フィールド名の間に「**フィールド分離文字**」を使用することも、別個の行にそれぞれの名前を指定することもできます。

列名を指定する順序により、列が出力ファイルに書き込まれる順序が制御されます。

引用符の使用可能
書き込み操作時に引用符を使用して出力するには、このチェック・ボックスを選択します。デフォルトでは、このオプションは選択されています。

このチェック・ボックスをクリアすると、フィールドはそのまま出力され、問題が発生する場合があります。「**引用符の使用**」チェック・ボックスが選択されている場合、読み取り時に、フィールドを囲む引用符は取り除かれます。パーサーは、列分離文字を含む、引用符で囲まれた属性を読み取ることもできます。「**引用符の使用**」チェック・ボックスがクリアされている場合、引用符で区切られたフィールドが入力に含まれていると、パーサーによって予期しない値が返されます。

すべてのフィールドを引用符で囲む
フィールドに引用符、分離文字、または改行が含まれている場合に、すべてのフィールドを個別に引用符で囲んで出力するには、このチェック・ボックスを選択します。

ヘッダーの書き込み
列分離文字で区切られたすべてのフィールド名を最初の行に出力するには、このチェック・ボックスを選択します。デフォルトでは、このオプションは選択されています。

BOM の書き込み
バイト・オーダー・マーク (BOM) をファイルに書き込むには、このチェック・ボックスを選択します。このオプションを有効にするには、「**ヘッダーの書き込み**」も選択する必要があります。

長い行のログ
1 行の最大バイト数を指定します。この最大数より長い行の行番号がログに記録されます。

余りを最後のフィールドに結合
行にある定義フィールド数を超えるすべての余分のフィールドを新しい「**余り**」フィールドに結合するには、このチェック・ボックスを選択します。これらのフィールド、および暗黙的にそのフィールド数は、「**フィールド名**」によって、または存在しない場合にはファイルの最初の行によって定義されます。

文字エンコード
読み取りまたは書き込み時に使用される文字エンコードを指定します。

詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*文字エンコード変換*」を検索してください。

CSV パーサーおよびそのスキーマについて詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*CSV パーサー*」を検索してください。

ファイル・エンドポイント用の DSMLv1 パーサー

XML 文書の読み取りおよび書き込みを行うには、DSMLv1 パーサーを使用します。 Directory Services Markup Language v1.0 (DSMLv1) を使用すると、ディレクトリー構造情報を XML 文書として表現できます。このパーサーは、スキーマ項目を警告なしに無視します。

DSMLv1 パーサー構成パラメーターにアクセスするには、次のようにします。

1. ファイル・エンドポイントを追加します。
2. 「ファイル」エンドポイント構成ページで、「**パーサー**」 をクリックして、リストから「**DSMLv1 パーサー**」を選択します。
3. 「**パーサー**」セクションを展開して、パラメーターを表示します。

パラメーター

コメント
このフィールドを使用して、コメントを追加します。データの構文解析時には、このコメントは無視されます。

詳細ログ
詳細なデバッグ情報が入ったログ・メッセージを生成するには、このチェック・ボックスを選択します。

以下の詳細パラメーターを構成することもできます。「**パーサー**」セクションで、「**拡張**」を展開して以下のパラメーターを表示します。

DN 属性
識別名 DSML 属性に使用する属性を指定します。デフォルト値は `$dn` です。

DSML 接頭部
XML エレメントが DSML ネーム・スペースに属することを指示する接頭部を指定します。デフォルト値は `dsml` です。

DSML ネーム・スペース URI
このネーム・スペースを識別する URI を指定します。デフォルト値は `http://www.dsml.org/DSML` です。

XML 宣言の省略
パーサーが出力ストリームで XML 宣言ヘッダーを省略する必要があることを指定するには、このチェック・ボックスを選択します。

文書の妥当性検査
指定した DTD またはスキーマに基づくファイルの妥当性検査を要求するには、このチェック・ボックスを選択します。

ネーム・スペースを意識
パーサーがネーム・スペース認識パーサーを要求する必要があることを指定するには、このチェック・ボックスを選択します。

文字エンコード

読み取りまたは書き込み時に使用される文字エンコードを指定します。デフォルト値は UTF-8 です。

DSMLv1 パーサーは単純 XML パーサーを拡張したものであるため、同じ文字エンコードのルールが適用されます。詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*単純 XML パーサーにおける文字エンコード*」を検索してください。

DSMLv1 パーサーおよび使用例について詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*DSMLv1 パーサー*」を検索してください。

ファイル・エンドポイント用の DSMLv2 パーサー

DSMLv2 の要求メッセージおよび応答メッセージを解析して作成するには、DSMLv2 パーサーを使用します。Directory Services Markup Language v2.0 (DSMLv2) は、ディレクトリーの照会や更新、およびこれらの操作の結果を XML 文書として表現するメソッドを提供します。

DSMLv2 パーサー構成パラメーターにアクセスするには、次のようにします。

1. ファイル・エンドポイントを追加します。
2. 「ファイル」エンドポイント構成ページで、「**パーサー**」をクリックして、リストから「**DSMLv2 パーサー**」を選択します。
3. 「**パーサー**」セクションを展開して、パラメーターを表示します。

パラメーター

モード パーサーが「**サーバー**」または「**クライアント**」のどちらのモードで動作するかを指定します。**サーバー**・モードでは、要求が読み取られ、応答が書き込まれます。**クライアント**・モードでは、要求が書き込まれ、応答が読み取られます。

コメント

このフィールドを使用して、コメントを追加します。データの構文解析時には、このコメントは無視されます。

詳細ログ

追加情報が入った詳細なログ・メッセージを生成するには、このチェック・ボックスを選択します。

以下の詳細パラメーターを構成することもできます。「**パーサー**」セクションで、「**拡張**」を展開して以下のパラメーターを表示します。

文字エンコード

読み取りまたは書き込み時に使用される文字エンコードを指定します。デフォルト値は UTF-8 です。

DSMLv2 パーサーは単純 XML パーサーを拡張したものであるため、同じ文字エンコードのルールが適用されます。詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*単純 XML パーサーにおける文字エンコード*」を検索してください。

バイナリー属性
パーサーによってバイナリー属性として処理される必要がある属性を、コンマで区切ったリストとして指定します。属性のリストはデフォルトで提供されており、変更可能です。

On Error
バッチ要求エレメントの処理中の障害に対するサーバーの対応を指定します。有効な値は、**終了** および **再開** です。デフォルト値は「**終了**」です。

処理 バッチ要求の **processing** DSML 属性の値を指定します。有効な値は、**順次** および **並列** です。デフォルト値は「**順次**」です。

応答順序
サーバーによるバッチ応答内の個々の応答の順序付け方法を指定します。有効な値は、**順次** および **順不同** です。デフォルト値は「**順次**」です。「**順次**」を選択する場合、サーバーは、個々の応答がそれぞれの要求に対応した順序になっているバッチ応答を返す必要があります。

XML 宣言の省略
パーサーが出力ストリームで XML 宣言ヘッダーを省略する必要があることを指定するには、このチェック・ボックスを選択します。

インデント出力
このチェック・ボックスが選択されている場合は、ステートメント行の深さに基づいて出力がインデントされます。結果は形式的なもののみであり、出力ファイルの内容のセマンティックには影響しません。

SOAP バインディング
SOAP DSML メッセージを作成するには、このチェック・ボックスを選択します。それ以外の場合は、DSML メッセージは SOAP によりラップされません。

DSMLv2 パーサー、その操作、属性、および例について詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*DSMLv2 パーサー*」を検索してください。

ファイル・エンドポイント用の固定レコード・パーサー

固定長のテキスト・レコードの読み取りおよび書き込みを行うには、固定レコード・パーサーを使用します。

固定レコード・パーサー構成パラメーターにアクセスするには、次のようにします。

1. ファイル・エンドポイントを追加します。
2. 「ファイル」エンドポイント構成ページで、「**パーサー**」をクリックして、リストから「**固定レコード・パーサー**」を選択します。
3. 「**パーサー**」セクションを展開して、パラメーターを表示します。

パラメーター

列記述 各列記述をコンマで区切られたフィールド名、オフセット、および長さとして指定します。このフィールドは複数行フィールドです。1 行につき 1 つの列記述を指定する必要があります。

例を示します。

```
field1, 1, 12
field2, 13, 4
field3, 17, 3
```

フィールド名は、スキーマ・ディスカバリー時に表示されます。オフセットは 1 で開始されます。0 などの無効な値は例外を引き起こす場合があります。

コメント
このフィールドを使用して、コメントを追加します。データの構文解析時には、このコメントは無視されます。

詳細ログ
追加情報が入った詳細なログ・メッセージを生成するには、このチェック・ボックスを選択します。

以下の詳細パラメーターを構成することもできます。「**パーサー**」セクションで、「**拡張**」を展開して以下のパラメーターを表示します。

値のトリム
読み取り操作時にフィールドから先頭および末尾のスペースを削除するには、このチェック・ボックスを選択します。

文字エンコード
読み取りまたは書き込み時に使用される文字エンコードを指定します。

詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*文字エンコード変換*」を検索してください。

ファイル・エンドポイント用の HTTP パーサー

HTTP 仕様に従ってバイト・ストリームを解釈するには、HTTP パーサーを使用します。

HTTP パーサー構成パラメーターにアクセスするには、次のようにします。

1. ファイル・エンドポイントを追加します。
2. 「ファイル」エンドポイント構成ページで、「**パーサー**」をクリックして、リストから「**HTTP パーサー**」を選択します。
3. 「**パーサー**」セクションを展開して、パラメーターを表示します。

パラメーター

クライアント・モード
パーサーがクライアント HTTP 応答モードで動作する必要があることを指定するには、このチェック・ボックスを選択します。「**クライアント・モード**」チェック・ボックスがクリアされている場合、パーサーはサーバー・モードで動作します。この操作は、パーサーが出力ストリームを書き込む場合にのみ有用です。

コメント
このフィールドを使用して、コメントを追加します。データの構文解析時には、このコメントは無視されます。

詳細ログ

追加情報が入った詳細なログ・メッセージを生成するには、このチェック・ボックスを選択します。

以下の詳細パラメーターを構成することもできます。「**パーサー**」セクションで、「**拡張**」を展開して以下のパラメーターを表示します。

プロパティーとしてのヘッダー

ヘッダー値をプロパティーとして取得および設定するには、このチェック・ボックスを選択します。このチェック・ボックスがクリアされている場合、ヘッダー値は属性として読み取られ、属性として返されます。

文字エンコード

読み取りまたは書き込み時に使用される文字エンコードを指定します。

詳しくは、IBM Security Directory Integrator の資料にアクセスして、「文字セット/エンコード」を検索してください。

HTTP パーサー、そのスキーマ、およびヘッダー・フィールドについて詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*HTTP パーサー*」を検索してください。

ファイル・エンドポイント用の IdML パーサー

IdML (Identity Markup Language) ファイルの内容を解析するには、IdML パーサーを使用します。これは、IdML 文書の読み取りにのみ使用できます。 IdML ファイルおよびスニペットの処理には、XML パーサーを使用します。

IdML パーサー構成パラメーターにアクセスするには、次のようにします。

1. ファイル・エンドポイントを追加します。
2. 「ファイル」エンドポイント構成ページで、「**パーサー**」をクリックして、リストから「**IdML パーサー**」を選択します。
3. 「**パーサー**」セクションを展開して、パラメーターを表示します。

パラメーター

コメント

このフィールドを使用して、コメントを追加します。データの構文解析時には、このコメントは無視されます。

詳細ログ

詳細なデバッグ情報が入ったログ・メッセージを生成するには、このチェック・ボックスを選択します。

以下の詳細パラメーターを構成することもできます。「**パーサー**」セクションで、「**拡張**」を展開して以下のパラメーターを表示します。

文字エンコード

読み取りまたは書き込み時に使用される文字エンコードを指定します。

IdML パーサーおよびそのスキーマについて詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*IdML パーサー*」を検索してください。

ファイル・エンドポイント用の JSON パーサー

JavaScript Object Notation (JSON) フォーマットで項目の読み取りおよび書き込みを行うには、JSON パーサーを使用します。JSON は、軽量のデータ交換フォーマットであり、JavaScript プログラミング言語のサブセットです。 JSON は、値の番号付きリスト (配列) および名前値ペアのコレクション (オブジェクト) という 2 つの構造で作成されます。

JSON パーサー構成パラメーターにアクセスするには、次のようにします。

1. ファイル・エンドポイントを追加します。
2. 「ファイル」エンドポイント構成ページで、「**パーサー**」をクリックして、リストから「**JSON パーサー**」を選択します。
3. 「**パーサー**」セクションを展開して、パラメーターを表示します。

パラメーター

圧縮出力
このチェック・ボックスを選択して、圧縮モードでデータを表示します。圧縮モードの場合、フォーマットされていない単一行に JSON データが書き込まれます。これは、デフォルト・モードです。

文字エンコード
データの読み取りまたは書き込みに使用する文字エンコードを指定します。

コメント
このフィールドを使用して、コメントを追加します。データの構文解析時には、このコメントは無視されます。

詳細ログ
詳細なデバッグ情報が入ったログ・メッセージを生成するには、このチェック・ボックスを選択します。

JSON パーサー、そのオブジェクトと属性、および使用例について詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*JSON パーサー*」を検索してください。

ファイル・エンドポイント用の LDIF パーサー

LDAP Data Interchange Format (LDIF) のデータの読み取りおよび書き込みを行うには、LDIF パーサーを使用します。LDIF フォーマットは、一連のディレクトリー項目、またはディレクトリー項目に適用された一連の変更を指定するために使用されますが、両方は指定しません。LDIF ファイルは、行の分離文字で区切られた一連のレコードで構成されています。

LDIF パーサー構成パラメーターにアクセスするには、次のようにします。

1. ファイル・エンドポイントを追加します。
2. 「ファイル」エンドポイント構成ページで、「**パーサー**」をクリックして、リストから「**LDIF パーサー**」を選択します。
3. 「**パーサー**」セクションを展開して、パラメーターを表示します。

パラメーター

DN 属性名
LDIF dn 行に使用する属性名を指定します。デフォルト値は $dn です。

バージョン番号
このチェック・ボックスを選択すると、RFC 2849 で規定されているように、出力の始めにバージョン属性が表示されます。デフォルトでは、このチェック・ボックスは選択されています。

コメント
このフィールドを使用して、コメントを追加します。データの構文解析時には、このコメントは無視されます。

詳細ログ
詳細なデバッグ情報が入ったログ・メッセージを生成するには、このチェック・ボックスを選択します。

以下の詳細パラメーターを構成することもできます。「**パーサー**」セクションで、「**拡張**」を展開して以下のパラメーターを表示します。

バイナリー属性
パーサーによってバイナリー属性として処理される必要がある属性を、コンマで区切ったリストとして指定します。

文字エンコード
読み取りまたは書き込み時に使用される文字エンコードを指定します。デフォルト値は UTF-8 です。

詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*文字エンコード変換*」を検索してください。

注: 準拠する LDIF ファイルは、常に**文字エンコード**が UTF-8 に設定されていることが必要です。「**文字エンコード**」は、BASE64 エンコード・ストリングをエンコードまたはデコードする場合にも適用されます。BASE64 エンコードは、デコードの方法を知らない限り、文字化けしたテキストのように見えます。

記述レコードのみ
このチェック・ボックスを選択して、記述レコードのみが書き込まれます。LDIF ファイルには、変更レコードまたは記述レコードが含まれる場合があります。変更レコードには、項目に必要な変更が記述されています。このレコードは、dn 行の直後にある 2 番目の行である changetype 行で識別されます。記述レコードでは、項目が記述されています。正しい LDIF ファイルには、変更レコードのみが含まれるか、または記述レコードのみが含まれています。

デフォルトでは、このチェック・ボックスは選択されていません。

言語タグのサポート
パーサーで言語タグをサポートするには、このボックスを選択します。情報が複数の言語で表現されている場合、サーバーは言語タグを属性値に関連付けます。

LDIF パーサーについて詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*LDIF パーサー*」を検索してください。

ファイル・エンドポイント用の行リーダー・パーサー

ファイルから単一行のデータを読み取るには、行リーダー・パーサーを使用します。読み取られた行は単一の属性として戻されます。 `linenumber` という属性には、1 から始まる行番号が入っています。

行リーダー・パーサーは、バイナリー・ファイルではなく、テキスト・ファイルのみを読み取るために使用します。バイナリー・ファイルをコピーする場合は、スクリプト記述可能な FTP オブジェクトを使用できます。FTP オブジェクトの詳細および例については、IBM Security Directory Integrator の資料にアクセスして、「*FTP オブジェクト*」を検索してください。

行リーダー・パーサー構成パラメーターにアクセスするには、次のようにします。

1. ファイル・エンドポイントを追加します。
2. 「ファイル」エンドポイント構成ページで、「**パーサー**」をクリックして、リストから「**行リーダー・パーサー**」を選択します。
3. 「**パーサー**」セクションを展開して、パラメーターを表示します。

パラメーター

属性名 直前に読み取ったか、書き込もうとしているテキストの行を含む属性の名前を指定します。デフォルト値は `line` です。

コメント
このフィールドを使用して、コメントを追加します。データの構文解析時には、このコメントは無視されます。

詳細ログ
詳細なデバッグ情報が入ったログ・メッセージを生成するには、このチェック・ボックスを選択します。

以下の詳細パラメーターを構成することもできます。「**パーサー**」セクションで、「**拡張**」を展開して以下のパラメーターを表示します。

文字エンコード
読み取りまたは書き込み時に使用される文字エンコードを指定します。

詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*文字エンコード変換*」を検索してください。

ファイル・エンドポイント用のスクリプト・パーサー

JavaScript を使用して独自のパーサーを作成するには、スクリプト・パーサーを使用します。

スクリプト・パーサー構成パラメーターにアクセスするには、次のようにします。

1. ファイル・エンドポイントを追加します。
2. 「ファイル」エンドポイント構成ページで、「**パーサー**」をクリックして、リストから「**スクリプト・パーサー**」を選択します。
3. 「**パーサー**」セクションを展開して、パラメーターを表示します。

パラメーター

スクリプト
実行されるユーザー定義のスクリプトを作成するには、このフィールドを使用します。デフォルトでサンプル・スクリプトが提供されています。スクリプトで使用できるオブジェクトおよび関数について詳しくは、IBM Security Directory Integrator の資料にアクセスして、「スクリプト・パーサー」を検索してください。

以下の詳細パラメーターを構成することもできます。「**パーサー**」セクションで、「**拡張**」を展開して以下のパラメーターを表示します。

外部ファイル
実行時に外部スクリプト・ファイルを組み込む場合は、それらのファイルを指定します。ファイルは 1 行に 1 つずつ指定してください。これらのファイルは、スクリプトの前に実行されます。

グローバル・スクリプトの組み込み
スクリプト・ライブラリーからスクリプトを組み込むには、これを選択します。

文字エンコード
読み取りまたは書き込み時に使用される文字エンコードを指定します。

詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*文字エンコード変換*」を検索してください。

コメント
このフィールドを使用して、コメントを追加します。データの構文解析時には、このコメントは無視されます。

詳細ログ
詳細なデバッグ情報が入ったログ・メッセージを生成するには、このチェック・ボックスを選択します。

スクリプト・パーサー、そのオブジェクト、メソッド、およびスキーマについて詳しくは、IBM Security Directory Integrator の資料にアクセスして、「スクリプト・パーサー」を検索してください。

ファイル・エンドポイント用の単純なパーサー

属性名と値のペアで構成される項目の読み取りおよび書き込みを行うには、単純なパーサーを使用します。

項目は次の形式になっています。

- 各行に 1 つの `attributename:value` ペアがあります。
- 多値属性には複数の行を使用します。
- 単一のピリオドがある行は項目の終わりを示します。
- 値の **¥r** および **¥n** は、`CR` および `LF` の改行のエンコードです。

単純なパーサー構成パラメーターにアクセスするには、次のようにします。

1. ファイル・エンドポイントを追加します。

2. 「ファイル」エンドポイント構成ページで、「**パーサー**」をクリックして、リストから「**単純なパーサー**」を選択します。
3. 「**パーサー**」セクションを展開して、パラメーターを表示します。

パラメーター

コメント
このフィールドを使用して、コメントを追加します。データの構文解析時には、このコメントは無視されます。

詳細ログ
詳細なデバッグ情報が入ったログ・メッセージを生成するには、このチェック・ボックスを選択します。

以下の詳細パラメーターを構成することもできます。「**パーサー**」セクションで、「**拡張**」を展開して以下のパラメーターを表示します。

文字エンコード
読み取りまたは書き込み時に使用される文字エンコードを指定します。

詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*文字エンコード変換*」を検索してください。

ファイル・エンドポイント用の単純 XML パーサー

XML 文書の読み取りおよび書き込みを行うには、単純 XML パーサーを使用します。このパーサーは、深くても 2 レベルまでの深度の XML データを扱います。

単純 XML パーサーは、Apache の Xerces および Xalan ライブラリーを使用します。このパーサーでは、`xmldom` というスクリプト・オブジェクトを使用して XML 文書にアクセスできます。`xmldom` は、`org.w3c.dom.Document` インターフェースのインスタンスです。

注: 65 ページの『ファイル・エンドポイント用の XML パーサー』は、改善された拡張版の XML パーサーです。

単純 XML パーサー構成パラメーターにアクセスするには、次のようにします。

1. ファイル・エンドポイントを追加します。
2. 「ファイル」エンドポイント構成ページで、「**パーサー**」をクリックして、リストから「**単純 XML パーサー**」を選択します。
3. 「**パーサー**」セクションを展開して、パラメーターを表示します。

パラメーター

ルート・タグ
項目を囲むルート・タグを指定します。デフォルト値は `DocRoot` です。

項目タグ
パーサーに渡される項目のエレメントの名前を指定します。デフォルト値は `Entry` です。

値タグ パーサーに渡される属性値のエレメントの名前を指定します。デフォルト値は `ValueTag` です。

コメント
このフィールドを使用して、コメントを追加します。データの構文解析時には、このコメントは無視されます。

詳細ログ
詳細なデバッグ情報が入ったログ・メッセージを生成するには、このチェック・ボックスを選択します。

以下の詳細パラメーターを構成することもできます。「**パーサー**」セクションで、「**拡張**」を展開して以下のパラメーターを表示します。

XML 宣言の省略
パーサーが出力ストリームで XML 宣言ヘッダーを省略する必要があることを指定するには、このチェック・ボックスを選択します。

文書の妥当性検査
指定した DTD またはスキーマに基づくファイルの妥当性検査を要求するには、このチェック・ボックスを選択します。

ネーム・スペースを意識
パーサーがネーム・スペース認識パーサーを要求する必要があることを指定するには、このチェック・ボックスを選択します。

文字エンコード
読み取りまたは書き込み時に使用される文字エンコードを指定します。デフォルト値は `UTF-8` です。

詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*単純 XML パーサーにおける文字エンコード*」を検索してください。

インデント出力
このチェック・ボックスが選択されている場合は、ステートメント行の深さに基づいて出力がインデントされます。結果は形式的なもののみであり、出力ファイルの内容のセマンティックには影響しません。

単純 XML パーサーおよび使用例について詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*単純 XML パーサー*」を検索してください。

関連情報:

http://www.w3schools.com にある W3C の資料

http://docs.oracle.com にある Oracle Java API の資料

ファイル・エンドポイント用の SOAP パーサー

SOAP XML 文書の読み取りおよび書き込みを行うには、SOAP パーサーを使用します。

SOAP パーサーは、以下の方法で SOAP XML 文書を項目オブジェクトに、そして項目オブジェクトを SOAP XML 文書に変換します。

- パーサーが XML 文書に書き込む場合、項目からの属性を使用して文書を作成します。**`SOAP_CALL`** 属性には、SOAP 呼び出しの値が含まれます。

- パーサーが XML 文書から読み取る場合、**SOAP_CALL** 属性は、SOAP-ENV:Body タグの後の最初のタグを反映するように設定されます。項目内の各属性について、その名前と値を持つタグが作成されます。SOAP_CALL タグの下の各タグは項目オブジェクト内の属性に変換されます。

SOAP パーサー構成パラメーターにアクセスするには、次のようにします。

1. ファイル・エンドポイントを追加します。
2. 「ファイル」エンドポイント構成ページで、「**パーサー**」をクリックして、リストから「**SOAP パーサー**」を選択します。
3. 「**パーサー**」セクションを展開して、パラメーターを表示します。

パラメーター

コメント
このフィールドを使用して、コメントを追加します。データの構文解析時には、このコメントは無視されます。

詳細ログ
詳細なデバッグ情報が入ったログ・メッセージを生成するには、このチェック・ボックスを選択します。

以下の詳細パラメーターを構成することもできます。「**パーサー**」セクションで、「**拡張**」を展開して以下のパラメーターを表示します。

XML 宣言の省略
パーサーが出力ストリームで XML 宣言ヘッダーを省略する必要があることを指定するには、このチェック・ボックスを選択します。

文書の妥当性検査
指定した DTD またはスキーマに基づくファイルの妥当性検査を要求するには、このチェック・ボックスを選択します。

ネーム・スペースを意識
パーサーがネーム・スペース認識パーサーを要求する必要があることを指定するには、このチェック・ボックスを選択します。

文字エンコード
読み取りまたは書き込み時に使用される文字エンコードを指定します。デフォルト値は UTF-8 です。

詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*文字エンコード変換*」を検索してください。

SOAP パーサーおよび使用例について詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*SOAP パーサー*」を検索してください。

ファイル・エンドポイント用の SPMLv2 パーサー

SPML バージョン 2 (SPMLv2) メッセージの解析または書き込みを行うには、SPMLv2 パーサーを使用します。これらのメッセージは、個々の SPMLv2 要求と応答です。

SPMLv2 は、実際のプロビジョニング・データを定義するためにさまざまなデータ・モデルを使用できるコア・プロトコルを定義します。データ・モデルと SPML

コア仕様の組み合わせは、プロファイルと呼ばれます。SPML を使用するには、特定のプロファイルを使用する必要があります。 Federated Directory Server コンソールで提供されているこの SPMLv2 パーサーは、SPMLv2 DSMLv2 プロファイルをサポートしています。

SPMLv2 パーサー構成パラメーターにアクセスするには、次のようにします。

1. ファイル・エンドポイントを追加します。
2. 「ファイル」エンドポイント構成ページで、「**パーサー**」をクリックして、リストから「**SPMLv2 パーサー**」を選択します。
3. 「**パーサー**」セクションを展開して、パラメーターを表示します。

パラメーター

コメント
このフィールドを使用して、コメントを追加します。データの構文解析時には、このコメントは無視されます。

詳細ログ
詳細なデバッグ情報が入ったログ・メッセージを生成するには、このチェック・ボックスを選択します。

以下の詳細パラメーターを構成することもできます。「**パーサー**」セクションで、「**拡張**」を展開して以下のパラメーターを表示します。

バイナリー属性
パーサーによってバイナリー属性として処理される必要がある属性を、コンマで区切ったリストとして指定します。属性のリストはデフォルトで提供されており、変更可能です。

文字エンコード
読み取りまたは書き込み時に使用される文字エンコードを指定します。デフォルト値は `UTF-8` です。

SPMLv2 パーサーは XML パーサーを拡張したものであるため、同じ文字エンコードのルールが適用されます。詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*XML パーサーにおける文字エンコード*」を検索してください。

SPMLv2 パーサー、その操作と属性、および使用例について詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*SPMLv2 パーサー*」を検索してください。

ファイル・エンドポイント用の XML パーサー

XML 文書の読み取りおよび書き込みを行うには、XML パーサーを使用します。XML パーサーは StAX (JSR-173) 仕様の XLXP インプリメンテーションを使用します。 StAX は、XML の読み取りと書き込みの両方を実行できるカーソル・ベースの XML パーサーです。

この XML パーサーは、DOM のように XML 構造全体をメモリーにロードする必要がないため、従来の DOM ベースの単純 XML パーサーよりもはるかに高速です。

XML パーサー構成パラメーターにアクセスするには、次のようにします。

1. ファイル・エンドポイントを追加します。
2. 「ファイル」エンドポイント構成ページで、「**パーサー**」をクリックして、リストから「**XML パーサー**」を選択します。
3. 「**パーサー**」セクションを展開して、パラメーターを表示します。

パラメーター

単純 XPath
エレメントを検出してそれらを項目として解釈するために使用される値 (XPath に類似した式) を指定します。このパラメーターは、書き込まれる XML 文書の構造を表示する場合にも使用されます。

項目タグ
XML パーサーに渡された各項目を保持するエレメントの名前を指定します。

値タグ XML パーサーに渡された各属性値を保持するエレメントの名前を指定します。

コメント
このフィールドを使用して、コメントを追加します。データの構文解析時には、このコメントは無視されます。

詳細ログ
詳細なデバッグ情報が入ったログ・メッセージを生成するには、このチェック・ボックスを選択します。

以下の詳細パラメーターを構成することもできます。「**パーサー**」セクションで、「**拡張**」を展開して以下のパラメーターを表示します。

ネーム・スペース・マップの接頭部
接頭部とネーム・スペースの間のマッピングのリストを *prefix=namespace* の形式で指定します。

各マッピングを縦棒 (|) で区切ります。

接頭部が `$` で始まっている場合、その接頭部はデフォルトのネーム・スペース宣言と見なされます。

デフォルト値は `prefix=namespace` です。

XSD スキーマ・ロケーション
表示のみを目的として使用されるスキーマ・ロケーションを指定します。

文字エンコード
読み取りまたは書き込み時に使用される文字エンコードを指定します。デフォルト値は `UTF-8` です。

詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*XML パーサーにおける文字エンコード*」を検索してください。

静的属性宣言
属性および接頭部の宣言を指定します。これらは、「**単純 XPath**」フィールドで指定される静的エレメントと共に書き込まれます。

デフォルトでは、このフィールドに次のテキストが入力されています。

```
<!-- this is an example for statically declared XML attributes/namespaces -->
<!-- DocRoot xmlns="defaultNS" attr1="val2">
<Entry xmlns:p1="p1NS" p1:attr2="val2" />
</DocRoot-->
```

読み取り中に反復 XML 宣言を無視
常に最初の XML 宣言を認知して、これより後の宣言を無視するには、このチェック・ボックスを選択します。

合体 隣接する文字データ・セクションを合体させるには、このチェック・ボックスを選択します。

書き込み時に XML 宣言を省略
出力に XML 宣言を書き込まない場合は、これにチェック・ボックスを選択します。このオプションは、既存の XML ファイルに付加する場合に役立ちます。

複数ルート文書
各項目をスタンドアロン・エレメントとして出力するには、このチェック・ボックスを選択します。これにより、複数ルート文書が作成されます。

インデント出力
このチェック・ボックスが選択されている場合は、ステートメント行の深さに基づいて出力がインデントされます。結果は形式的なもののみであり、出力ファイルの内容のセマンティックには影響しません。

書き込み時に無効な XML 文字を許可
無効な XML 文字を XML タグに組み込むには、このチェック・ボックスを選択します。このチェック・ボックスが選択されない場合、XML 文書での書き込み操作時に例外が発生します。

XML パーサーおよび使用例について詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*XML パーサー*」を検索してください。

ファイル・エンドポイント用の XML SAX パーサー

DOM ベースの XML パーサーがメモリーの制約により処理できない大容量の XML 文書を読み取るには、XML SAX パーサーを使用します。 XML SAX パーサーは、Apache Xerces ライブラリーを基にしています。

XML SAX パーサーは、構成で指定された「**グループ・タグ**」で囲まれているデータを抽出します。このパーサーは、データにある属性を使用して項目を作成します。

XML SAX パーサー構成パラメーターにアクセスするには、次のようにします。

1. ファイル・エンドポイントを追加します。
2. 「ファイル」エンドポイント構成ページで、「**パーサー**」をクリックして、リストから「**XML SAX パーサー**」を選択します。
3. 「**パーサー**」セクションを展開して、パラメーターを表示します。

パラメーター

グループ・タグ
項目を囲む 1 つ以上の XML グループ・タグの名前を指定します。複数の

タグを指定する場合は、各タグ名をコンマで区切ります。値を指定しない場合、ルート・タグが使用され、XML 文書全体が単一の項目として返されます。

コメント
このフィールドを使用して、コメントを追加します。データの構文解析時には、このコメントは無視されます。

詳細ログ
詳細なデバッグ情報が入ったログ・メッセージを生成するには、このチェック・ボックスを選択します。

以下の詳細パラメーターを構成することもできます。「**パーサー**」セクションで、「**拡張**」を展開して以下のパラメーターを表示します。

接頭部の除去
属性名から除去する接頭部を指定します。

属性無視
グループ・タグとその子の属性を無視するには、このチェック・ボックスを選択します。

文字エンコード
読み取りまたは書き込み時に使用される文字エンコードを指定します。デフォルト値は UTF-8 です。

文書の妥当性検査
指定した DTD またはスキーマに基づくファイルの妥当性検査を要求するには、このチェック・ボックスを選択します。

XSD 検証の使用
XML ファイルの検証に DTD ではなく XSD を使用するには、このチェック・ボックスを選択します。

ネーム・スペースを意識
パーサーがネーム・スペース認識パーサーを要求する必要があることを指定するには、このチェック・ボックスを選択します。

読み取りタイムアウト
データを何も受け取らない場合にパーサーが停止するまでの秒数を指定します。

XML SAX パーサーおよび使用例について詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*XML SAX パーサー*」を検索してください。

ファイル・エンドポイント用の XSL ベース XML パーサー

指定する XSL を使用して任意のフォーマットの XML 文書を解析するには、XSL ベース XML パーサーを使用します。XML 文書は属性値ペアに解析され、項目オブジェクトに保管されます。

XSL ベース XML パーサー構成パラメーターにアクセスするには、次のようにします。

1. ファイル・エンドポイントを追加します。

2. 「ファイル」エンドポイント構成ページで、「**パーサー**」をクリックして、リストから「**XSL ベース XML パーサー**」を選択します。
3. 「**パーサー**」セクションを展開して、パラメーターを表示します。

パラメーター

コメント

このフィールドを使用して、コメントを追加します。データの構文解析時には、このコメントは無視されます。

詳細ログ

詳細なデバッグ情報が入ったログ・メッセージを生成するには、このチェック・ボックスを選択します。

以下の詳細パラメーターを構成することもできます。「**パーサー**」セクションで、「**拡張**」を展開して以下のパラメーターを表示します。

文字エンコード

読み取りまたは書き込み時に使用される文字エンコードを指定します。デフォルト値は UTF-8 です。

XSL ベース XML パーサーは単純 XML パーサーを拡張したものであるため、同じ文字エンコードのルールが適用されます。詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*単純 XML パーサーにおける文字エンコード*」を検索してください。

インデント出力

このチェック・ボックスが選択されている場合は、ステートメント行の深さに基づいて出力がインデントされます。結果は形式的なもののみであり、出力ファイルの内容のセマンティックには影響しません。

XML 宣言の省略

パーサーが出力ストリームで XML 宣言ヘッダーを省略する必要があることを指定するには、このチェック・ボックスを選択します。

文書の妥当性検査

指定した DTD またはスキーマに基づくファイルの妥当性検査を要求するには、このチェック・ボックスを選択します。

ネーム・スペースを意識

パーサーがネーム・スペース認識パーサーを要求する必要があることを指定するには、このチェック・ボックスを選択します。

入力パラメーターを構成するには、「**パーサー**」セクションで「**入力**」を展開します。

入力 XSL ファイルを使用

このチェック・ボックスを選択して、入力 XSL ファイルを使用します。このチェック・ボックスを選択する場合、「**入力 XSL**」フィールドの内容は無視されます。

入力 XSL ファイル名

ユーザー XML を IBM Security Directory Integrator 内部フォーマットに変換するための突き合わせ規則が指定された入力 XSL ファイルのパスとファイル名を指定します。

入力 XSL

入力 XSL 全体を入力するか、貼り付けるには、この編集可能な領域を使用します。

出力パラメーターを構成するには、「**パーサー**」セクションで「**出力**」を展開します。

出力 XSL ファイルを使用

このチェック・ボックスを選択して、出力 XSL ファイルを使用します。このチェック・ボックスを選択する場合、「**出力 XSL**」フィールドの内容は無視されます。

出力 XSL ファイル名

IBM Security Directory Integrator 内部フォーマットをユーザー XML に変換するための突き合わせ規則が指定された出力 XSL ファイルのパスとファイル名を指定します。

出力 XSL

出力 XSL 全体を入力するか、貼り付けるには、この編集可能な領域を使用します。

XSL ベース XML パーサーおよび使用例について詳しくは、IBM Security Directory Integrator の資料にアクセスして、「*XSL ベース XML パーサー*」を検索してください。

第 2 章 Federated Directory Server Plug-in for IBM Security Access Manager

1 つ以上のディレクトリーを IBM Security Access Manager 用の認証ソースとして使用するには、このプラグインを構成します。例えば、Active Directory と Sun Directory Server を認証ソースとして使用できます。ユーザー管理とパスワードは個々の ID ストアに配置したままです。

このプラグインは、Federated Directory Server で提供される同期サービスおよび IBM Security Directory Server のパススルー認証機能に基づいています。 Federated Directory Server では、すぐに使用できるブラウザー・インターフェースから、複数の ID ストアと中央の IBM Security Directory Server インスタンスの同期を構成することができます。Federated Directory Server ブラウザー・コンソールを使用して、IBM Security Directory Server のパススルー認証を構成することもできます。

Federated Directory Server では、フローによる特定のディレクトリーとの同期が処理されます。各項目が処理されて IBM Security Directory Server に書き込まれた後に呼び出しを行うようにフローを構成できます。このポストオペレーション機能では、Federated Directory Server Plug-in for IBM Security Access Manager は必要とされるフローに接続されます。ターゲット・ディレクトリーで個人項目またはグループ項目が追加、変更、または削除されると、必ずプラグインが呼び出されます。

プラグインが呼び出されると、Federated Directory Server コンソールで設定された構成パラメーターがプラグインに渡されます。次に、フロー操作の一環として、ID 情報の変更がプラグインから IBM Security Access Manager に伝搬されます。

IBM Security Directory Integrator は、Federated Directory Server のサーバー・サイドの機能を強化するシステムです。IBM Security Directory Integrator での作業経験は必要ありませんが、このツールを理解していると、Federated Directory Server ソリューションのデプロイと管理が容易になります。これは、Federated Directory Server 内のフックを使用して、独自のビジネス・ロジックを、実行中のさまざまなバックグラウンド統合プロセスに関連付けるのに役立ちます。

注: Federated Directory Server Plug-in for IBM Security Access Manager は、LDAP エンドポイントでのみサポートされます。非 LDAP エンドポイントはサポートされません。

関連情報:

 Getting started with IBM Security Directory Integrator

 IBM Security Access Manager v2 コネクター

プラグインのセットアップのロードマップ

プラグインをセットアップするためには、IBM Security Access Manager API、IBM Security Directory Server、および Federated Directory Server で必要な設定を構成する必要があります。

Federated Directory Server は、ID 統合サービスを提供します。1 つ以上の数の ID ストアを中央の IBM Security Directory Server インスタンスと同期させた状態に保持します。

IBM Security Directory Server は、Federated Directory Server を使用して構成可能なパススルー認証機能を提供します。

Federated Directory Server Plug-in for IBM Security Access Manager は、このソリューションを拡張します。ユーザー・アカウントおよびグループを IBM Security Access Manager と同期させます。

以下のロードマップは、プラグインをセットアップするためのエンドツーエンド・シナリオのステップを示しています。

表 2. Federated Directory Server Plug-in for IBM Security Access Manager のセットアップのロードマップ

主要なステップ	**詳細情報**
プラグイン・パッケージのインストール。	73 ページの『プラグインのインストール』
IBM Security Access Manager API プロパティー・ファイルの生成およびプロパティー値の指定。	74 ページの『プラグイン API プロパティー・ファイル』
Federated Directory Server コンソールへのログオン。	7 ページの『Federated Directory Server コンソールへのアクセス』
Federated Directory Server から IBM Security Directory Server への接続。	11 ページの『IBM Security Directory Server への接続』
IBM Security Directory Server との同期のためのソース・エンドポイントの構成。 **注:** Federated Directory Server Plug-in for IBM Security Access Manager は、LDAP エンドポイントでのみサポートされます。非 LDAP エンドポイントはサポートされません。	17 ページの『エンドポイントの構成』
IBM Security Directory Server でのパススルー認証の有効化。	パススルー認証
Federated Directory Server でのパススルー認証の構成。	14 ページの『パススルー認証の構成』
Federated Directory Server でのフローの作成およびフロー設定の定義。	29 ページの『フローの作成』 29 ページの『フロー設定の定義』
Federated Directory Server でのフローへのプラグインの接続およびプラグイン・プロパティーの構成。	75 ページの『プラグイン・プロパティーの構成』

表 2. Federated Directory Server Plug-in for IBM Security Access Manager のセットアップのロードマップ (続き)

主要なステップ	詳細情報
ソース・エンドポイント属性を IBM Security Access Manager のユーザーおよびグループ項目にマップします。	77 ページの『属性のマッピング』
シミュレートされた同期の実行によるフローのテスト。	41 ページの『フロー構成の検証』
イニシャル同期を実行してエンドポイントからターゲット IBM Security Directory Server へとデータを移行。	42 ページの『初期同期の実行』
IBM Security Access Manager 認証が要件どおりに動作することをテスト。	79 ページの『プラグインのセットアップの検証』
増分同期を時間間隔で自動的に実行するスケジュールの作成。	43 ページの『同期のスケジューリング』

プラグインのインストール

IBM Security Access Manager API は、IBM Security Directory Integrator で使用できるようにする必要があります。

始める前に

以下の製品をインストールします。

- 最新のフィックスパックが適用された IBM Security Directory Integrator バージョン 7.2。このプラグインは、バージョン 7.2.0.1 以降で提供されます。
- IBM Security Access Manager バージョン 6.1.1 以降。

また、Federated Directory Server のターゲット・ディレクトリーと IBM Security Access Manager で使用されるディレクトリーが、同じ IBM Security Directory Server インスタンスであることを確認します。そうでない場合、IBM Security Directory Server の手動構成が必要になります。IBM Security Directory Server 内の IBM Security Access Manager スキーマに拡張属性を追加した場合は、`FDS_ISAM_Plugin.map` マッピング・ファイルに割り当てを追加する必要があります。

このタスクについて

`sdi_solution_dir` は、IBM Security Directory Integrator のソリューション・ディレクトリーです。これはインストール中に選択され、 *`tdi_install_dir`*`/bin/defaultSolDir` スクリプトに入れられます。

`tdi_install_dir` は、IBM Security Directory のインストール・ディレクトリーです。

プラグイン用の以下のファイルがインストールされます。

FDS_ISAM_Plugin.xml

IBM Security Access Manager との同期を処理する AssemblyLine を提供する IBM Security Directory Integrator の構成 XML ファイル。

Federated Directory Server コンソールに初めてアクセスしたときに、このファイルが *sdi_solution_dir*/configs ディレクトリーにコピーされます。

それ以降に更新があった場合は、このファイルを *sdi_solution_dir*/LDAPSync から *sdi_solution_dir*/configs に手動でコピーする必要があります。

FDS_ISAM_Plugin.map

ソース・エンドポイント属性と IBM Security Access Manager ユーザー項目とのマッピング方法を制御します。

このファイルは *sdi_solution_dir*/LDAPSync ディレクトリーにあります。

手順

以下のいずれかの方法で、IBM Security Directory Integrator が IBM Security Access Manager API を使用できるようにします。

- *ISAM_install_dir*/java/export/rgy ディレクトリーから com.tivoli.pd.rgy.jar ファイルを *tdi_install_dir*/jars ディレクトリーにコピーします。
- *ISAM_install_dir*/java/export/rgy を *sdi_solution_dir*/solution.properties ファイルの **com.ibm.di.userjars** プロパティーに追加します。

次のタスク

IBM Security Access Manager API の接続詳細が含まれた構成ファイルを生成する必要があります。『プラグイン API プロパティー・ファイル』を参照してください。

プラグイン API プロパティー・ファイル

IBM Java ランタイム環境で、**com.tivoli.pd.rgy.until.RgyConfig** ツールを実行し、プラグイン用の API プロパティー・ファイルを作成してセットアップします。

注: IBM Java ランタイム環境は、*tdi_install_dir*/jvm/jre/bin フォルダー内にあります。

構文

```
java com.tivoli.pd.rgy.util.RgyConfig properties_file_destination
  create Default Default "ldaphostname:389:readwrite:5" "DN" DN_password
```

パラメーター

properties_file_destination

このコマンドを実行すると作成されるファイルの絶対パスを指定します。

デフォルト値は相対パス LDAPSync/ISAM_API.properties です。

ldaphostname:*port*:*settings*

以下の詳細を指定します。

- IBM Security Access Manager の構成に使用する LDAP サーバーのホスト名。LDAP サーバーのホスト名は、Security Access Manager のランタイム構成ファイル内に指定されています。
- LDAP サーバーのポート番号。デフォルト値は 389 です。この値は変更可能です。
- 設定値 :readwrite:5。

値全体 (*ldaphostname*:*port*:*settings*) を二重引用符で囲んでください。

DN IBM Security Access Manager に対する認証用の LDAP 識別名 (DN) を指定します。値は、二重引用符で囲んでください。

DN_password
DN の対応するパスワードを指定します。

例

```
java com.tivoli.pd.rgy.util.RgyConfig
     sdi_solution_dir/LDAPSync/ISAM_API.properties
     create Default Default "9.118.51.177:389:readwrite:5"  "cn=root" cnrootpassword
```

コマンド・ステートメント内の Default は、統合対象の IBM Security Access Manager ドメインおよび IBM Security Access Manager プラグインの AssemblyLine パラメーターで設定されている値に対応しています。

結果は以下のようなプロパティー・ファイルになります。ここでは、**RgyConfig** ツールの実行時に指定された値がプロパティー設定に反映されています。

```
#IBM Tivoli Access Manager
#Mon Dec 03 10:40:06 MHT 2013
ldap.ssl-enable=false
ldap.bind-pwd={obf2}dwTRqM+riTiJyfwSscdYIsiAAb2aAXkqmJrtiJm2Hp4¥=
ldap.bind-dn=cn¥=root
ldap.mgmt-version=6.1.1
ldap.svrs=9.118.51.177 ¥1:389¥:readwrite¥:5;
local_domain=Default
ldap.mgmt=true
mgmt_domain=Default
delFromRegistry=true
```

構成を反映するには、以下の手順を実行します。

1. 新規に作成された ISAM_API.properties ファイルを *sdi_solution_dir*/LDAPSync ディレクトリーにコピーします。
2. IBM Security Directory Integrator を再始動します。

プラグイン・プロパティーの構成

プラグインを Federated Directory Server 内のフローに接続し、プラグインの構成プロパティーの値を指定します。

始める前に

72 ページの『プラグインのセットアップのロードマップ』に記載されているステップ 1 から 8 までを実行します。

手順

1. Federated Directory Server コンソールの「**フロー**」ページで、フローの名前をクリックし、「**編集**」をクリックします。
2. 「**ソース**」タブで、「**フロー・フック**」をクリックします。
3. 「**使用可能**」を選択して、AssemblyLine をフローに接続する機能を使用可能にします。
4. 「**ユーザーの追加/変更/削除**」を展開して「**使用可能**」を選択し、各ユーザーが追加、変更、または削除された後でこの特定のフロー・フックで AssemblyLine を呼び出す必要があることを示します。
5. 「**AssemblyLine**」の横の「**参照**」をクリックします。
6. 参照メニューで FDS_ISAM_Plugin を展開し、ProvisionISAM を選択して「**OK**」をクリックします。
7. 以下のプロパティーを指定してプラグインを構成します。

   isam.api.properties.filepath
   IBM Security Access Manager API プロパティー・ファイルのパスを指定します。

   デフォルト値は LDAPSync/ISAM_API.properties です。

   isam.domain
   統合対象の IBM Security Access Manager ドメインを指定します。

   このドメイン名は、IBM Security Access Manager API プロパティー・ファイルの作成に使用されるドメインと同じである必要があります。

   デフォルト値は Default です。

   isam.map.principalName
   同期中である現在の個人に対応する IBM Security Access Manager 項目の principalName についてマッピング指示を指定します。

   以下の特殊値のいずれかを使用できます。

   - targetRDN は、ターゲットの個人 RDN を指定します。
   - sourceRDN は、ソースの個人 RDN を指定します。

   それ以外の場合、このプロパティーの値は、ソース・エンドポイントから読み取られる項目内にある属性の名前である必要があります。

   デフォルト値は targetRDN です。

   注: このソリューションのセットアップでは、Federated Directory Server と IBM Security Access Manager が同じ IBM Security Directory Server インスタンスを共有している必要があります。このシナリオでは、値として targetRDN を指定する必要があります。

   isam.map.secDN
   同期中である現在の個人に対応する IBM Security Access Manager 項目の secDN についてマッピング指示を指定します。

   以下の特殊値のいずれかを使用できます。

   - targetDN は、ターゲットの個人 DN を指定します。
   - sourceDN は、ソースの個人 DN を指定します。

- mapFile は、マップ・ファイルにより secDN が処理されることを指定します。

それ以外の場合、このプロパティーの値は、ソース・エンドポイントから読み取られる項目で使用可能な属性の名前である必要があります。

デフォルト値は targetRDN です。

注: このソリューションのセットアップでは、Federated Directory Server と IBM Security Access Manager が同じ IBM Security Directory Server インスタンスを共有している必要があります。このシナリオでは、値として targetRDN を指定する必要があります。

isam.mapFile

使用するマップ・ファイルのパスおよびファイル名を指定するオプションのプロパティー。

ソリューション・ディレクトリーは常に IBM Security Directory Integrator の現行作業ディレクトリーであるため、相対パス (LDAPSync/FDS_ISAM_Plugin.map など) を使用できます。

デフォルト値は LDAPSync/FDS_ISAM_Plugin.map です。

属性のマッピング

ソース・エンドポイント属性を IBM Security Access Manager のユーザーおよびグループ項目にマップします。

このタスクについて

Federated Directory Server コンソールでは、フロー構成で属性をマップすることができます。ただし、フロー構成の「**属性マップ**」タブで FDS_ISAM_Plugin.map を変更しようとすると、必要な結果が得られない可能性があります。行った変更は FDS_ISAM_Plugin.map ファイルに保存されません。代わりに、変更内容は FDS_ISAM_Plugin.map のコピーに保存され、フローの名前に対応する別のファイル名が付けられます。これは、「フロー・フック」ページの **isam.mapFile** プロパティーの値の構成 (通常は FDS_ISAM_Plugin.map) と矛盾する可能性があります。

手順

1. Federated Directory Server コンソールの「**共通設定**」で、「**属性マップ**」をクリックします。 *sdi_solution_dir*/LDAPSync ディレクトリー内の属性マップがリストされます。
2. 「**FDS_ISAM_Plugin.map**」を選択します。プラグイン用の属性マッピング・テーブルが、デフォルトのマッピングとともに表示されます。
3. FDS_ISAM_Plugin.map の属性マッピングを構成します。 15 ページの『属性マップのカスタマイズ』の手順に従って操作します。最小限必要なマッピングは、対応する IBM Security Access Manager ユーザーの principalName に使用されるソースの Person 属性です。デフォルトでは、この値はソース項目の UID 値に設定されています。ソース項目に UID が見つからない場合、プラグインは sAMAccountName に employeeCode を付加したものを使用します。

以下の属性がデフォルトの FDS_ISAM_Plugin.map 内に存在します。

cn ユーザーまたはグループの共通名。

description
ユーザーまたはグループの説明。

secAcctValid
IBM Security Access Manager ユーザー・アカウントを使用可能または使用不可にするユーザー項目フラグ。

- `true` は、アカウントが使用不可であることを指定します。デフォルト値は `true` です。この値は、プロビジョンされた IBM Security Access Manager ユーザー・アカウントに対してパススルー認証が動作するようにするためには `true` に設定する必要があります。
- `false` は、アカウントが使用不可ではないことを指定します。

secPwdValid
IBM Security Access Manager ユーザーの **userPassword** 属性が有効かどうかを示すユーザー項目フラグ。

- `true` は、アカウントが使用不可であることを指定します。デフォルト値は `true` です。この値は、プロビジョンされた IBM Security Access Manager ユーザー・アカウントに対してパススルー認証が動作するようにするためには `true` に設定する必要があります。
- `false` は、アカウントが使用不可ではないことを指定します。

sn ユーザーの姓。

デフォルトの `FDS_ISAM_Plugin.map` ファイルには、必ずしもすべての属性が存在しない場合があります。例えば、パスワードは同期化されないため、**userPassword** は不要です。代わりに、IBM Security Access Manager からの認証要求は、IBM Security Directory Server のパススルー認証機能によりソース・エンドポイントにパススルーされます。一部の属性について以下で説明します。

secDN
ユーザー項目およびグループ項目両方のための IBM Security Access Manager ディレクトリー内の項目の DN。**isam.map.secDN** プロパティーによりこの属性のマップ方法が記述されます。マップ・ファイルの項目が使用されるのは、このプロパティーの値が `mapFile` に設定されている場合のみです。

member
uniqueMember
IBM Security Access Manager ユーザーのプリンシパル名またはその `secDN` 値のいずれかのオプションのリストを指定するために、ユーザー項目用に提供される属性。これらのユーザーは、ユーザー項目として存在する場合、IBM Security Access Manager のセキュリティー・グループに追加されます。

値が `secDN` 値であると判別される場合、DN の RDN は、ユーザーのプリンシパル名であると想定されます。デルタ操作タグが設定されている場合、`delete` のタグが付けられた値はすべてグループ・メンバーシップから削除されます。

memberOf
ユーザー項目がメンバーとなっている IBM Security Access Manager セキュリティー・グループ名のオプションのリストを指定するグループ項目の属性。

この機能は便宜上提供されています。ただし、グループ・メンバーシップは通常、ユーザー項目の member 属性をマッピングすることにより処理されます。

userPassword
IBM Security Access Manager ユーザー用のオプションのパスワード。

タスクの結果

属性マッピングは、*sdi_solution_dir*/LDAPSync ディレクトリー内の FDS_ISAM_Plugin.map ファイルに保存されます。

プラグインのセットアップの検証

プラグインが正常に機能していることをテストするには、ターゲット IBM Security Directory Server 内の同期されている項目を検証する必要があります。

このタスクについて

Federated Directory Server コンソールで LDAP ブラウザーを使用して、ターゲット IBM Security Directory Server 内の項目を検証できます。詳しくは、 12 ページの『ディレクトリー項目のブラウズ』を参照してください。

手順

1. IBM Security Access Manager ユーザーがプラグインによって追加されたことを検証します。これらのユーザー項目が IBM Security Directory Server の SECAUTHORITY=instance name,cn=Users コンテナーの下に表示されていなければなりません。
2. IBM Security Access Manager インスタンスとして Default を使用した場合は、cn=Users,SECAUTHORITY=DEFAULT 検索ベースの下を確認して、principalname=* をフィルターとして使用して検索します。 IBM Security Directory Server に同期されている各 LDAP 個人項目が IBM Security Access Manager ユーザーとしても表示されていることを確認します。ユーザーの secDN が、対応する LDAP 項目を指していることが必要です。
3. IBM Security Directory Server に同期されていたユーザーの資格情報を使用します。ただし、そのユーザーの元のパスワードはソース・ディレクトリーに存在します。正常にログインできれば、パススルー認証も正常に機能しています。

トラブルシューティング

制限事項、ログ・ファイル、および一般的なエラーの説明を理解しておくと、Federated Directory Server Plug-in for IBM Security Access Manager のトラブルシューティングに役立ちます。

既知の制限

このソリューションでは、IBM Security Access Manager Registry Direct API を使用します。グローバル・サインオン (GSO) ユーザーの追加、変更、削除はサポートされません。

ログ・ファイル

IBM Security Access Manager の同期プロセスでは、ログ・ファイル *sdi_solution_dir* /LDAPSync/logs/*flow*-ProvisionISAM.log が作成されます。ここで、*flow* は、IBM Security Access Manager をプロビジョンするためのプラグインを呼び出す同期フローの名前です。50 個の過去のログの履歴も維持されます。このログには通常、問題の詳細 (同期中の項目の principalName や secDN など) が記録されています。

IBM Security Access Manager のプロビジョニング・プロセスにより報告されるエラーは、Federated Directory Server に表示されます。このログに記録されるメッセージには、通常 *afterwrite* または *post-write* というテキストが含まれています。ログに記録されるメッセージは通常 2 つの部分で構成されており、最初に Federated Directory Server のエラーが出力され、エラーの根本原因を示す 2 番目のメッセージが続きます。

例えば、書き込み操作の後に以下のようなエラーが発生する場合があります。

```
CTGDII761E Error invoking afterwrite Hook
```

場合によっては、最初のメッセージに構成および AssemblyLine の名前も含まれています。これは、デフォルトでは FDS_ISAM_Plugin:/AssemblyLines/ProvisionISAM です。

各エラー・レポートの最後の部分に、問題を修正するための洞察が提供されます。

出力マップに必須属性が欠落している
: このエラー・メッセージには、IBM Security Access Manager で必須の属性の名前も含まれています。マップ・ファイルを更新して、この値が返されるようにする必要があります。

CTGDIS047W 項目が見つかりません
: このエラーは、増分同期中に、IBM Security Access Manager からユーザーを削除するときにのみ発生します。これは、このユーザーが IBM Security Access Manager レジストリー内に見つからなかったことを示しています。

CTGDKD262E 構成インスタンスを開始できませんでした
: このエラーは、IBM Security Access Manager Provisioning AssemblyLine を含む構成 XML ファイルが *sdi_solution_dir*/configs フォルダー内に見つからない場合に発生します。デフォルトでは、このファイルは FDS_ISAM_Plugin.xml です。構成ファイルがこのフォルダーにコピーされていることを確認し、再試行してください。

HPDAA0321E この識別名は、レジストリー内の既存のエントリーにマップされていません。
HPDAA0320E 指定された識別名に、無効な構文があります。
: これらのエラーは、secDN 属性値が無効であることを示しています。

isam.map.secDN プロパティーを compute に設定した場合は、**isam.user.container** プロパティーの値を確認してください。このプロパティーには、ユーザー項目が書き込まれる IBM Security Access Manager ディレクトリー内の既存のコンテナーの DN が含まれています。また、**isam.map.secDN.type** プロパティーが CN または UID のいずれかに設定されていることも確認してください。

isam.map.secDN プロパティーが mapFile に設定されている場合は、マップ・ファイルに secDN 属性が含まれているようにしてください。マッピング割り当てでは、構文の正しい DN 値を生成する必要があります。また、DN のサフィックスは、IBM Security Access Manager ディレクトリー内の既存のコンテナーを参照している必要があります。

第 3 章 System for Cross-Domain Identity Management

System for Cross-Domain Identity Management (SCIM) は、ID 管理用のスキーマとプロトコルを定義する標準です。 IBM Security Directory Integrator に付属している SCIM サービスは、バックエンド・ディレクトリーとして IBM Security Directory Server と共に使用することができます。また、IBM Security Directory Integrator ソリューション SCIM コネクターを使用すると、SCIM プロトコルをサポートするサーバーに対して読み取りと書き込みを行うことができます。

概説

SCIM は、ユーザーとグループを管理するための標準として開発され、多くの場合、従来の LDAP プロトコルの代わりに使用されます。SCIM は、HTTP REST のデプロイメント、企業間デプロイメント、クラウド・アプリケーション・デプロイメントで必要となる柔軟性を提供します。多くのクラウド・サービスには、LDAP インターフェースが用意されていません。そのため、基盤となるプロトコルとは関係なく、SCIM を使用することができます。

SCIM プロトコルは、Web 上の ID データのプロビジョニングと管理を行うためのアプリケーション・レベルの REST プロトコルです。このプロトコルは、核となる ID リソース (ユーザーとグループ) とカスタム・リソース拡張の作成、変更、取得、ディスカバリーをサポートします。

機能

SCIM の仕様は、クラウド・ベースのアプリケーションとサービスで、ユーザー ID の管理を迅速に、簡単に、低コストで行うことができるように設計されています。

SCIM には、以下の特徴があります。

- 従来のスキーマとデプロイメントに関する経験に基づいて構築されています。
- 開発と統合の簡素化に重点を置いています。
- 既存の認証、許可、プライバシー・モデルを適用します。

共通のユーザー・スキーマと拡張モデルを提供することにより、ユーザー管理操作のコストと複雑さを軽減します。また、標準プロトコルを使用して、このスキーマを交換するためのパターンを提供する文書がバインドされています。

詳しくは、SCIM の Web サイト (http://www.simplecloud.info/) を参照してください。

ビジネス・シナリオ

SCIM プロトコルは、多くの場合、LDAP 以外のシステム上でユーザーとグループを管理する目的で使用されます。新しいアプリケーションは、企業内のシナリオとクラウドに関連するシナリオのどちらにおいても、HTTP REST を使用して、基盤となるテクノロジーを抽象化することができます。

SCIM は、以下のシナリオで正常に使用することができます。

- 新しい ID サービスを SCIM と共にプロビジョニング・プロトコルとして内部的にデプロイして、将来長期にわたって使用する。
- LDAP がプロトコルとして許可されない内部クラウドまたは外部クラウド。
- ユーザー管理インターフェースとして SCIM を持つ SaaS アプリケーションへのプロビジョニング。

詳しくは、SCIM の Web サイト (http://www.simplecloud.info/) で『*SCIM scenarios*』を検索してください。

IBM Security Directory Integrator の SCIM サービス

IBM Security Directory Integrator の SCIM サービスは、IBM Security Directory Server に対する SCIM インターフェースと、SCIM プロトコルを使用するサーバー用の SCIM コネクターを提供します。

SCIM サービスは、IBM Security Directory Integrator 自体を使用して構築されています。このサービスは、実際には、サーバーとして機能する IBM Security Directory Integrator のアセンブリー・ラインです。SCIM サーバーのバックエンドは、ID データを持つ IBM Security Directory Server でなければなりません。SCIM サーバーは、SCIM 要求を受信すると、IBM Security Directory Server に内部的に接続してデータにアクセスし、要求を処理します。

SCIM コネクターは、JavaScript と HTTP クライアント・コネクターを使用して SCIM プロトコルを実装します。

サポートされるソフトウェア

IBM Security Directory Integrator バージョン 7.2 以降に付属している SCIM サービスは、IBM Security Directory Server バージョン 6.3.1 をサポートします。

IBM Security Directory Integrator に実装される SCIM サービスは、SCIM 1.1 仕様に準拠しています。詳しくは、SCIM の Web サイト (http://www.simplecloud.info/) で『*Specifications*』を検索してください。

サポートされる機能

バージョン 2.0 での変更に適切に対応することにより、IBM Security Directory Integrator の SCIM サービスは、SCIM バージョン 1.1 の大部分の操作をサポートしています。

現行バージョンの SCIM サービスでは、以下の機能がサポートされています。

- IBM Security Directory Server をバックエンド・ディレクトリーとして使用したユーザーとグループの管理
- スキーマ: エンタープライズ・ユーザーのスキーマ拡張
- JSON データ・タイプ
- GET/PUT/POST/DELETE 要求
- PATCH: PATCH (HTTP) 要求を使用した変更により、コンシューマーは、変更が必要な属性だけを送信することができます。

- ページ編集
- 認証方式: HTTP 基本認証
- フィルタリングにより、コンシューマーは、**filter** 照会パラメーターを使用して、リソースのサブセットを要求することができます。
- 部分的なリソースにより、コンシューマーは、**attributes** 照会パラメーターを使用して、リソース表記で返す必要がある属性を指定することができます。
- ソートにより、コンシューマーは、リソースを返す順序を指定することができます。

現行バージョンの SCIM サーバーでは、以下の機能はサポートされていません。

- OAuth 認証
- 一括更新
- 返されるリソース数の自動制限。

注: SCIM パラメーターの **active** を正常に機能させるには、IBM Security Directory Server でパスワード・ポリシーをオンにする必要があります。パスワード・ポリシーをオンにするには、`cn=pwdpolicy,cn=ibmpolicies` の下で **ibm-pwdPolicy** を `true` に設定します。この設定により、SCIM は、IBM Security Directory Server から **ibm-pwdAccountLocked** の設定を読み取ることができるようになります。パスワード・ポリシーの設定について詳しくは、IBM Security Directory Server の資料で『パスワード・ポリシーの設定』を検索してください。

構成ファイル

SCIM サービスをデプロイする前に、構成ファイルを変更して、接続設定、ユーザーとグループのマッピング、スキーマを指定する必要があります。

IBM Security Directory Integrator をインストールすると、`SCIM` という名前のフォルダーが *tdi_install_dir* に作成されます。ソリューション・ディレクトリーを手動で作成するか、サーバーの始動時に作成すると、`SCIM` フォルダーがソリューション・ディレクトリーに自動的にコピーされます。`SCIM` フォルダーは、手動でソリューション・ディレクトリーにコピーすることもできます。

`SCIM` フォルダーには、セットアップを構成するために変更可能な構成ファイルなど、以下に示す一連のファイルが格納されています。ほとんどの場合、更新する必要があるのは、`SCIM.properties` ファイルだけです。他のファイルは、ほとんどの場合、変更する必要はありません。

SCIM.properties

`SCIM.properties` ファイルには、バックエンド IBM Security Directory Server の詳細など、以下に示すサーバー・システム固有のプロパティーが含まれています。

Location
SCIM サービスの、外部からアクセス可能な URL。これは、SCIM 応答内のロケーション・ヘッダーにのみ影響します。

httpPort
SCIM サービスが listen 用に使用するポート。SCIM サービスは、常に SSL を使用します。

LDAP.LookupLimit
SCIM サービスで検索できるリソースの最大数。メモリー・オーバーフローを回避するため、デフォルト値は 20000 に設定されています。

LDAPServer
ユーザー・データを格納する IBM Security Directory Server の URL。

userSearchBase
IBM Security Directory Server のユーザーの検索ベース。

groupSearchBase
IBM Security Directory Server のグループの検索ベース。

userObjectClass
IBM Security Directory Server でユーザーを作成する場合に使用されるオブジェクト・クラスのリスト。

groupObjectClass
IBM Security Directory Server でグループを作成する場合に使用されるオブジェクト・クラスのリスト。

userSearchFilter
userSearchBase のすべてのユーザーを検索する場合に使用されます。

groupSearchFilter
groupSearchBase のすべてのグループを検索する場合に使用されます。

dummyGroupMember
新しいグループの作成時にグループ内にメンバーが存在しない場合は、オブジェクト違反エラーを回避するために **dummyGroupMember** の値が追加されます (この値が設定されている場合)。

audit.log
監査ログを作成するには、このパラメーターに `true` を設定します。

audit.logFile
監査ログ・ファイルの名前。

audit.logFileDatePattern
この日付パターンは、ログ・ファイルをバックアップ・ファイルにロールオーバーする頻度を指定します。また、以前のログを保管するバックアップ・ファイルのログ・ファイル名に日付を付加する方法も指定します。

audit.syslog
QRadar® に対する syslog を有効にするかどうかを指定します。有効にするには、この値を `true` に設定します。

audit.QRadarHost
QRadar が配置されているホスト。

audit.QRadarPort
QRadar のポート番号。

audit.facility
監査メッセージの機能。

audit.eventID
監査ログで使用するイベント ID。

audit.devTimeFormat
監査ログで使用する日付形式。

mapTenantNames
SCIM 認証の実行方法を変更する場合は、このプロパティーを true に設定します。詳細情報およびこのプロパティーを true に設定した場合に使用できるプロパティーのリストについては、102 ページの『SCIM 要求の認証』を参照してください。

AuthenticationRealm
認証の要求時にユーザーに提示されるレルム。

authenticationEndpoint
このプロパティーを true に設定すると、認証エンドポイントが使用可能になります。デフォルト値は false です。

UserMapping.json と GroupMapping.json

UserMapping.json ファイルと GroupMapping.json ファイルは、SCIM 属性と IBM Security Directory Server のユーザー属性またはグループ属性との間のマッピングを指定します。これらのファイルの各項目には、SCIM 属性名と LDAP 属性名が含まれています。各項目には、以下の追加属性が含まれている場合もあります。

ReadOnly
値が LDAP から SCIM にのみマッピングされ、他の方法ではマッピングされないことを指定します。

WriteOnly
値が SCIM から LDAP にのみマッピングされ、他の方法ではマッピングされないことを指定します。この項目は、パスワードで使用する必要があります。

CreateDN
この値に userSearchBase を付加することにより、この値が IBM Security Directory Server の識別名 (DN) の作成にも使用されることを指定します。新しいリソースを作成できるようにするには、常に指定される SCIM 属性名を使用する、**CreateDN** 属性を持つ項目が 1 つ存在する必要があります。

Type
多値属性の正規タイプを指定します。

Conversion
属性値の変換を指定します。変換属性には、以下のいずれかの値を設定することができます。

- **DateTime**: 値を LDAP 日付形式から SCIM 日付形式に変換します。
- **Group**: 値を LDAP グループから SCIM グループに変換します。
- **NewLines**: SCIM 値の改行を LDAP 値の $ に変換します (その逆も同様)。

注:

- 項目が固有の **Type** を持っている場合を除き、SCIM 名ごとにマップ項目が 1 つだけ存在している必要があります。
- 項目が **ReadOnly** の場合を除き、LDAP 名ごとに項目が 1 つだけ存在している必要があります。

UserSchema.json と GroupSchema.json

UserSchema.json ファイルと GroupSchema.json ファイルは、SCIM の仕様に従い、ユーザーまたはグループのスキーマを定義します。指定する属性は、UserMapping.json ファイルと GroupMapping.json ファイルで定義された属性に一致する必要があります。

ServiceProviderConfig.json
仕様への準拠性、サポートされるデータ・モデル、認証方式などを定義します。

SCIM.xml
SCIM サービスを実装する構成ファイル。

QRadarLogging.map

QRadarLogging.map ファイルは、QRadar syslog が有効になっている場合に QRadar システムに送信される属性の値を指定します。

詳しくは、IBM Security Directory Integrator インストール済み環境の *sdi_solution_dir* にある SCIM フォルダー内の Readme.txt ファイルを参照してください。

SCIM サービスの開始

SCIM サービスを開始するには、**ibmdisrv** コマンドを使用します。

始める前に

- SCIM 構成ファイルを必要に応じて変更します。

手順

次のコマンドを実行します。

```
ibmdisrv -c SCIM/SCIM.xml -r SCIM_Service -w
```

タスクの結果

SCIM サービスを開始すると IBM Security Directory Server に対する匿名バインドが試行されます。この処理が失敗した場合、SCIM サービスが停止し、「CTGDIS1930E LDAP サーバーに接続できません」というメッセージが ibmdi.log ファイルに表示されます。

SCIM コネクター

IBM Security Directory Integrator の SCIM コネクターを使用すると、SCIM プロトコルをサポートするサーバーに対して、読み取り操作と書き込み操作を行うことができます。

SCIM コネクターは、他の IBM Security Directory Integrator コネクターと同じように機能しますが、内部的には、REST 呼び出しを渡して SCIM 操作を使用します。

SCIM コネクターの構成方法と使用方法については、IBM Security Directory Integrator の資料 で『*SCIM コネクター*』を検索してください。

ロギングとトレース

SCIM のロギングとトレースの機能は、問題の原因を特定して解決する場合に役立ちます。

SCIM.properties ファイルの **debug** パラメーターに true を設定すると、ログ・ファイルに記録されるデータ量を増やすことができます。

監査ロギングを構成するには、SCIM.properties ファイルで以下のプロパティーを設定します。

audit.log
ロギングをオンにするかどうかを指定します。この値に true を設定すると、ロギングがオンになります。

auditLogFile
日次ロギングを実行するファイル名を指定します。

audit.logFileDatePattern
ログ・ファイルを新しいファイルにロールオーバーする頻度を指定します。デフォルト値は、daily です。ロールオーバーは、最初のメッセージが新しい日付に記録されたときだけ実行されます。ロギングは、log4j DailyRollingFileAppender を使用して実行されます。

ロギングは、JSON 形式で実行されます。JSON 形式では、以下の例のように、各行が 1 つの JSON オブジェクトになります。

```
{"url":"¥/Users", "date":"2013-08-03 14:19:25,234","host":"127.0.0.1",
     "method":"POST","user":"cn=root",
     "resourceID":"cn=John Doe,ou=People,DC=EXAMPLE,DC=COM",
     "date":"2013-08-03 14:19:25,296","user":"cn=root","status":"201 Created"}
```

JSON オブジェクトには、以下の属性があります。

user
要求を許可するユーザー名。

date
要求を受信した日時。

remoteHost
要求の受信元ホストの IP アドレス。

remotePort
要求の送信元ポート。

localHost
ローカル IP アドレス。

localPort
ローカル・ポート。

method
要求内のメソッド。

url
要求内の URL。

userAgent
要求の送信元ブラウザーの名前 (使用可能な場合)。

resourceID
要求によって作成または返されたリソース ID。

status
返された HTTP 状況。

SCIM オブジェクト・モデル

SCIM は、*Resource* を共通の特徴として持つオブジェクト・モデルに基づいて構築されています。すべての SCIM オブジェクトが、このオブジェクト・モデルから派生します。

現在、SCIM には、Resource オブジェクトから直接継承された 3 つのオブジェクトがあります。`ServiceProviderConfiguration` オブジェクトと `Schema` オブジェクトはディスカバリーで使用され、ユーザー情報は含まれていません。`CoreResource` オブジェクトには、2 つの子リソース (User と Group) 内のユーザー・データとグループ・データが含まれています。

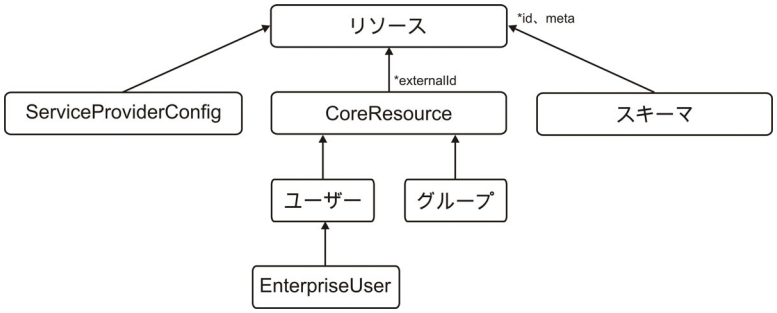


図 2. SCIM オブジェクト・モデル

操作

SCIM は、豊富でシンプルな一連の操作を備えた REST API を提供します。これらの操作を使用して、リソースを管理することができます。

SCIM 操作は、特定のユーザーの特定の属性のパッチ適用から、大量の一括更新の実行まで、すべての操作をサポートしています。

作成 `POST https://example.com/{v}/{resource}`

読み取り
`GET https://example.com/{v}/{resource}/{id}`

置換 `PUT https://example.com/{v}/{resource}/{id}`

削除 `DELETE https://example.com/{v}/{resource}/{id}`

更新 `PATCH https://example.com/{v}/{resource}/{id}`

検索

```
GET https://example.com/{v}/{resource}?filter={attribute}{op}{value}
     &sortBy={attributeName}&sortOrder={ascending|descending}
```

一括 `POST https://example.com/{v}/Bulk`

ディスカバリー操作

インターオペラビリティーを簡素化するために、SCIM には、サポートされる機能と特定の属性の詳細をディスカバーするためのエンドポイントが 2 つ用意されています。

GET /ServiceProviderConfigs

仕様への準拠性、認証方式、データ・モデルをディスカバーします。

GET /Schemas

- GET /Schemas/User
- GET /Schemas/Group

リソースと属性拡張をイントロスペクトします。

SCIM 操作の例

SCIM 操作を使用すると、さまざまなシナリオで、ユーザーとグループの検索、作成、変更、削除を行うことができます。

例 1

すべてのユーザーのリストを取得するには、以下の要求を送信します。

```
GET /users
```

例 2

以下の例は、すべてのユーザーのリストを取得する方法を示しています。ただし、表示されるのは **displayName** 属性と **id** 属性だけです。また、結果は、番号が 11 から 20 までのユーザーに制限されています。

要求:

```
GET /users?attributes=displayName,id&count=10&startIndex=11
```

結果:

```
{
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]
,
  "Resources":  [
        {
      "id":"7b401115-35f2-4a74-8384-a684cb4f31a1",
      "displayName":"Alexander Shelton"
    }
,
        {
      "id":"44216fbe-36a1-4215-b6f7-032775bc5e07",
      "displayName":"Andy Walker"
    }
,
        {
```

```
      "id":"c5292b7e-ffeb-4855-a086-7289d3445bd6",
      "displayName":"Alan White"
    }
,
        {
      "id":"5ad2d53c-9844-48ca-8460-c0d80fec5972",
      "displayName":"Alan Worrell"
    }
,
        {
      "id":"2b62e6a0-a698-4ffb-a107-1078b2d56437",
      "displayName":"Barbara Francis"
    }
,
        {
      "id":"3904d440-3f54-46cf-b63a-aacab03ac767",
      "displayName":"Bjorn Free"
    }
,
        {
      "id":"abb9526e-dfa8-452a-9d88-9eff3d79da90",
      "displayName":"Barbara Hall"
    }
,
        {
      "id":"d7df93df-d0bd-4c60-ad52-ec2bf8917fbc",
      "displayName":"Benjamin Hall"
    }
,
        {
      "id":"f98c9470-d7fe-490f-ab71-e84c9d3e9448",
      "displayName":"Barbara Jablonski"
    }
,
        {
      "id":"87fd1385-7d13-4423-851a-fb1d047bc2f0",
      "displayName":"Bjorn Jensen"
    }

  ]
,
  "totalResults":"163",
  "startIndex":"11",
  "itemsPerPage":"10"
}
```

例 3

以下の例は、**familyName** が「k」で始まるすべてのユーザーのリストを取得する方法を示しています。

要求:

```
GET /users?filter=name.familyName sw "k"
```

結果:

```
{
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]
,
  "Resources":  [
        {
      "id":"6f0fa17b-d988-4f95-98c0-095a545cc44e",
      "externalID":"aknutson",
```

```
      "meta":      {
        "created":"2013-04-16T09:14:02Z",
        "modified":"2013-04-16T09:14:02Z"
      }
,
      "userName":"uid=aknutson,ou=People,DC=EXAMPLE,DC=COM",
      "displayName":"Ashley Knutson",
      "name":      {
        "givenName":"Ashley",
        "familyName":"Knutson"
      }
,
      "phoneNumbers":      [
                {
          "type":"work",
          "value":"+1 408 555 2169"
        }
,
                {
          "type":"fax",
          "value":"+1 408 555 4774"
        }

      ]
,
      "emails":      [
                {
          "type":"work",
          "value":"aknutson@example.com"
        }

      ]

    }
,
        {
      "id":"6f7a3e28-db6c-4846-ae78-2346f39f65ee",
      "externalID":"ekohler",
      "meta":      {
        "created":"2013-04-16T09:14:02Z",
        "modified":"2013-04-16T09:14:02Z"
      }
,
      "userName":"uid=ekohler,ou=People,DC=EXAMPLE,DC=COM",
      "displayName":"Elba Kohler",
      "name":      {
        "givenName":"Elba",
        "familyName":"Kohler"
      }
,
      "phoneNumbers":      [
                {
          "type":"work",
          "value":"+1 408 555 1926"
        }
,
                {
          "type":"fax",
          "value":"+1 408 555 9332"
        }

      ]
,
      "emails":      [
                {
          "type":"work",
          "value":"ekohler@example.com"
```

```
        }

      ]

    }
,
      {
    "id":"e5318e13-1534-4eb9-9237-e1367a2744e1",
    "externalID":"skellehe",
    "meta":      {
      "created":"2013-04-16T09:14:02Z",
      "modified":"2013-04-16T09:14:02Z"
    }
,
    "userName":"uid=skellehe,ou=People,DC=EXAMPLE,DC=COM",
    "displayName":"Sue Kelleher",
    "name":      {
      "givenName":"Sue",
      "familyName":"Kelleher"
    }
,
    "phoneNumbers":      [
            {
       "type":"work",
       "value":"+1 408 555 3480"
      }
,
            {
       "type":"fax",
       "value":"+1 408 555 8721"
      }

    ]
,
    "emails":      [
            {
       "type":"work",
       "value":"skellehe@example.com"
      }

    ]

  }
,
      {
    "id":"3bac3d16-33ee-4a39-a6d1-063c5537530a",
    "externalID":"tkelly",
    "meta":      {
      "created":"2013-04-16T09:14:02Z",
      "modified":"2013-04-16T09:14:02Z"
    }
,
    "userName":"uid=tkelly,ou=People,DC=EXAMPLE,DC=COM",
    "displayName":"Timothy Kelly",
    "name":      {
      "givenName":"Timothy",
      "familyName":"Kelly"
    }
,
    "phoneNumbers":      [
            {
       "type":"work",
       "value":"+1 408 555 4295"
      }
,
            {
       "type":"fax",
```

```
          "value":"+1 408 555 1992"
        }

      ]
,
      "emails":      [
                {
          "type":"work",
          "value":"tkelly@example.com"
        }

      ]

    }

  ]
,
  "totalResults":"4"
}
```

例 4

以下の例は、**id** が 2064f364-260b-4c29-8c28-b12583486ca3 のユーザーを検索する方法を示しています。

要求:

```
GET /users/2064f364-260b-4c29-8c28-b12583486ca3
```

結果:

```
{
  "id":"2064f364-260b-4c29-8c28-b12583486ca3",
  "externalID":"abergin",
  "meta":  {
    "created":"2013-04-16T09:14:02Z",
    "modified":"2013-04-16T09:14:02Z"
  }
,
  "userName":"uid=abergin,ou=People,DC=EXAMPLE,DC=COM",
  "displayName":"Andy Bergin",
  "name":  {
    "givenName":"Andy",
    "familyName":"Bergin"
  }
,
  "phoneNumbers":  [
        {
      "type":"work",
      "value":"+1 408 555 8585"
    }
,
        {
      "type":"fax",
      "value":"+1 408 555 7472"
    }

  ]
,
  "emails":  [
        {
      "type":"work",
      "value":"abergin@example.com"
    }

  ]
```

```
,
  "groups":  [
        {
      "value":"57a96228-48a6-4f29-a8ad-345828fccd6a",
      "display":"QA Managers"
    }

  ]
,
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]

}
```

例 5

以下の例は、指定された日付以降に作成されたすべてのユーザーのリストを取得する方法を示しています。

要求:

```
 GET /users?filter=meta.created gt "2013-05-17T00:00:00Z"
```

結果:

```
{
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]
,
  "Resources":  [
        {
      "id":"78a13de7-0ef9-42ae-ba7c-b9c64a2050aa",
      "externalID":"wlutz2",
      "meta":      {
        "created":"2013-05-21T11:39:48Z",
        "modified":"2013-05-21T11:53:30Z"
      }
,
      "userName":"uid=wlutz2,ou=People,DC=EXAMPLE,DC=COM",
      "displayName":"Wendy Lutz",
      "name":      {
        "givenName":"Wendy",
        "familyName":"Lutz"
      }
,
      "phoneNumbers":      [
              {
          "type":"work",
          "value":"+1 408 555 3358"
        }
,
              {
          "type":"fax",
          "value":"+1 408 555 9332"
        }

      ]
,
      "emails":      [
              {
          "type":"work",
          "value":"wlutz@example.com"
        }
```

```
      ]

    }
,
      {
    "id":"a4cc7512-1530-4adc-952b-cd752aa79828",
    "externalID":"wlutz4",
    "meta":      {
      "created":"2013-05-21T11:54:12Z",
      "modified":"2013-05-21T11:54:12Z"
    }
,
    "userName":"uid=wlutz4,ou=People,DC=EXAMPLE,DC=COM",
    "displayName":"Wendy Lutz",
    "name":      {
      "givenName":"Wendy",
      "familyName":"Lutz"
    }
,
    "phoneNumbers":      [
            {
       "type":"work",
       "value":"+1 408 555 3358"
      }
,
            {
       "type":"fax",
       "value":"+1 408 555 9332"
      }

    ]
,
    "emails":      [
            {
       "type":"work",
       "value":"wlutz@example.com"
      }

    ]

    }
,
      {
    "id":"9be8c033-cf93-448e-a96b-d1290ff6d445",
    "externalID":"abergin2",
    "meta":      {
      "created":"2013-05-24T11:29:51Z",
      "modified":"2013-05-24T11:51:09Z"
    }
,
    "userName":"uid=abergin2,ou=People,DC=EXAMPLE,DC=COM",
    "displayName":"Andy Bergin Jr",
    "name":      {
      "givenName":"Andy",
      "familyName":"Bergin"
    }
,
    "phoneNumbers":      [
            {
       "type":"work",
       "value":"+1 408 555 8585"
      }
,
            {
       "type":"fax",
       "value":"+1 408 555 7472"
      }
```

```
      ]
,
      "emails":      [
                {
           "type":"work",
           "value":"abergin@example.com"
         }

      ]

    }

  ]
,
  "totalResults":"3"
}
```

例 6

ユーザーを作成するには、以下の要求を送信します。

```
 POST /users
```

以下の例のように、本文には、新規ユーザーに関する情報を JSON 形式で指定する必要があります。

```
{
      "externalID":"abergin2",
      "displayName":"Andy Bergin",
      "name":      {
        "givenName":"Andy",
        "familyName":"Bergin"
      }
,
      "phoneNumbers":      [
                {
           "type":"work",
           "value":"+1 408 555 8585"
         }
,
                {
           "type":"fax",
           "value":"+1 408 555 7472"
         }

      ]
,
      "emails":      [
                {
           "type":"work",
           "value":"abergin@example.com"
         }

      ]
}
```

結果:

```
200 OK
{
  "id":"9be8c033-cf93-448e-a96b-d1290ff6d445",
  "externalID":"abergin2",
  "meta":  {
    "created":"2013-05-24T11:29:51Z",
    "modified":"2013-05-24T11:51:09Z"
```

```
  }
,
  "userName":"uid=abergin2,ou=People,DC=EXAMPLE,DC=COM",
  "displayName":"Andy Bergin",
  "name":  {
    "givenName":"Andy",
    "familyName":"Bergin"
  }
,
  "phoneNumbers":  [
        {
      "type":"work",
      "value":"+1 408 555 8585"
    }
,
        {
      "type":"fax",
      "value":"+1 408 555 7472"
    }

  ]
,
  "emails":  [
        {
      "type":"work",
      "value":"abergin@example.com"
    }

  ]
,
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]

}
```

例 7

以下の例は、ユーザーを変更する方法を示しています。前の例で id が b9be8c033-cf93-448e-a96b-d1290ff6d445 として作成されたユーザーの **displayName** だけが変更されます。

要求:

```
PATCH /users/b9be8c033-cf93-448e-a96b-d1290ff6d445
```

HTTP 本文には、以下の情報を指定する必要があります。

```
{
 "displayName":"Andy Bergin Jr"
}
```

結果:

```
{
  "id":"9be8c033-cf93-448e-a96b-d1290ff6d445",
  "externalID":"abergin2",
  "meta":  {
    "created":"2013-05-24T11:29:51Z",
    "modified":"2013-05-24T11:51:09Z"
  }
,
  "userName":"uid=abergin2,ou=People,DC=EXAMPLE,DC=COM",
  "displayName":"Andy Bergin Jr",
  "name":  {
    "givenName":"Andy",
```

```
    "familyName":"Bergin"
  }
,
  "phoneNumbers":  [
        {
      "type":"work",
      "value":"+1 408 555 8585"
    }
,
        {
      "type":"fax",
      "value":"+1 408 555 7472"
    }

  ]
,
  "emails":  [
        {
      "type":"work",
      "value":"abergin@example.com"
    }

  ]
,
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]

}
```

注: PATCH コマンドがないブラウザーで操作をテストするには、HTTP ヘッダーの X-HTTP-Method-Override の値を PATCH に設定します。この設定を使用すると、特定の HTTP メソッドをブロックするファイアウォールを回避することもできます。

例 8

以下の例は、**id** が 2064f364-260b-4c29-8c28-b12583486ca3 のユーザーを削除する方法を示しています。

要求:

```
DELETE /users/2064f364-260b-4c29-8c28-b12583486ca3
```

結果:

```
200 OK
```

例 9

すべてのグループのリストを取得するには、以下の要求を使用します。

```
GET /groups
```

例 10

以下の例は、グループの **id** を使用して特定のグループを検索する方法を示しています。

要求:

```
GET /groups/5653c887-1d5a-42cf-a470-6a2fe2608730
```

結果:

```
{
  "id":"5653c887-1d5a-42cf-a470-6a2fe2608730",
  "externalID":"Accounting Managers",
  "meta":  {
    "created":"2013-04-16T09:10:45Z",
    "modified":"2013-04-16T09:10:45Z"
  }
,
  "displayName":"Accounting Managers",
  "members":  [
        {
      "value":"71e064d4-3791-4ac8-b7c6-62686ce710cd",
      "display":"Sam Carter"
    }
,
        {
      "value":"6ba0ff5b-98b4-41c8-be28-331b99d94bde",
      "display":"Ted Morris"
    }

  ]
,
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]

}
```

例 11

以下の例は、グループの **displayName** を使用して特定のグループを検索する方法を示しています。

要求:

```
 GET /groups?filter=displayName eq "Accounting Managers"
```

結果:

```
{
  "id":"5653c887-1d5a-42cf-a470-6a2fe2608730",
  "externalID":"Accounting Managers",
  "meta":  {
     "created":"2013-04-16T09:10:45Z",
    "modified":"2013-04-16T09:10:45Z"
  }
,
  "displayName":"Accounting Managers",
  "members":  [
        {
      "value":"71e064d4-3791-4ac8-b7c6-62686ce710cd",
      "display":"Sam Carter"
    }
,
        {
      "value":"6ba0ff5b-98b4-41c8-be28-331b99d94bde",
      "display":"Ted Morris"
    }

  ]
,
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]

}
```

例 12

以下の例は、グループを作成する方法を示しています。

要求:

```
POST /groups
```

本文には、新しいグループに関する情報を指定する必要があります。

```
{
       "externalID":"Test Group",
       "displayName":"Test Group",
      "members":      [
     "5156d423-3c74-415b-844f-606a2aabafcc",
     "900faa78-d7c6-421c-9181-313134d17dd0"
      ]
    }
```

結果:

```
201 Created
{
  "id":"7e15ce9e-2fe7-4624-b5d5-adedc242e07a",
  "externalID":"Test Group",
  "meta":  {
    "created":"2013-05-27T02:37:38Z",
    "modified":"2013-05-27T02:37:38Z"
  }
,
  "displayName":"Test Group",
  "members":  [
        {
      "value":"5156d423-3c74-415b-844f-606a2aabafcc",
      "display":"Kirsten Vaughan"
    }
,
        {
      "value":"900faa78-d7c6-421c-9181-313134d17dd0",
      "display":"Robert Daugherty"
    }

  ]
,
  "schemas":  [
    "urn:scim:schemas:core:1.0"
  ]

}
```

SCIM 要求の認証

SCIM 認証サービスは、SCIM 標準を拡張して、認証呼び出しとユーザーおよびグループの管理を可能にします。

SCIM 要求は、Schema オブジェクトまたは ServiceProviderConfig オブジェクトに対する要求でない限り、すべて認証を必要とします。要求が認証されていない場合は、メッセージ「401 Unauthorized」が返されます。

認証では、ユーザー名とパスワードの Base64 エンコードを含む標準的な HTTP 基本許可ヘッダーが使用されます。このメカニズムは、大半のブラウザーによって使用されるプロセスと同じです。

資格情報の認証には以下の 2 つのシナリオがあります。

- SCIM.properties ファイルで、プロパティー **mapTenantNames** の値を true に指定しない場合。この場合、ユーザー名は、SCIM サービス AssemblyLine のバックエンド・サーバーである LDAP サーバーに認識されている LDAP 名であることが必要です。ユーザー名とそれに対応するパスワードが、検証のために LDAP サーバーに送信されます。
- SCIM.properties ファイルで、プロパティー **mapTenantNames** の値を true に指定する場合。この場合、SCIM.properties ファイルで、このユーザー名を定義するいくつかのプロパティーをさらに指定する必要があります。例えば、ユーザー名が domain の場合、domain.ldapName=cn=root と指定できます。これは、HTTP ユーザー名 domain からの要求が、ユーザー名 cn=root で LDAP サーバーにバインドされることを示します。パスワードについては、domain.password=Secret および domain.ldapPassword=VerySecret を指定した場合、HTTP 要求パスワードは Secret である必要があります。そうでないと認証は失敗します。LDAP サーバーに送信されるパスワードは VerySecret です。これらの 2 つのプロパティーが存在しない場合、パスワードは直接 LDAP サーバーに送信されます。

ユーザー domain にアクセス制限がある場合にも、要求の許可が失敗する可能性があります。プロパティー **domain.access** が存在しない場合、またはリソースとメソッドに適合しない場合は、要求が許可されません。**mapTenantNames** を true に設定した場合、この設定によっても、すべてのユーザーに対してアクセス権プロパティーを使用可能にします。

アクセス権の検証

また、**mapTenantNames** プロパティーを true に設定した場合、すべての要求でユーザーのアクセス権が検証されます。許可を求める要求に対して、要求対象のリソースおよびメソッドに一致する値を指定して **domain.access** プロパティーを指定する必要があります。**domin.access** プロパティーの値は、キーワードをコンマで区切ったストリングである必要があります。デフォルトはアクセス権なしです。以下のキーワードを使用できます。

all　すべてのアクセス権が許可されます。

createUser
ユーザーを POST します。

createGroup
グループを POST します。

modifyUser
ユーザーを PATCH または PUT します。

modifyGroup
グループを PATCH または PUT します。

deleteUser
ユーザーを DELETE します。

deleteGroup
グループを DELETE します。

readUser
1 人以上のユーザーに対して GET を実行します。

readGroup
1 つ以上のグループに対して GET を実行します。

auth 非標準のエンドポイントまたは認証によってユーザーを認証します。

セキュリティー上の理由から、このアクセス制御は、要求されたリソースの LDAP DN が LDAP 検索ベースに一致することも検証します。

認証エンドポイント

SCIM.properties ファイルでプロパティー authenticationEndpoint=true を設定すると、SCIM プロトコルへのローカル拡張が有効になり、ユーザー名の認証が可能になります。

認証エンドポイントの使用も許可を必要とします。「許可」ヘッダーには、他の SCIM 要求と同様、ユーザー名とパスワードが含まれている必要があります。このユーザー名とパスワードについては、前のセクションで説明しています。この許可資格情報は認証対象のユーザーに直接には関係していません。認証対象のユーザーは、例えば userName sw "Je" (sw は starts with (で始まる) の意味) のようなフィルターを使用して指定します。認証サービスは、許可資格情報を手掛かりにしてこのユーザーを検索します。フィルター基準には 1 人のユーザーのみが一致することが必要です。次にサービスは、このユーザーの DN と「認証パスワード」ヘッダーに指定されたパスワードを使用して、LDAP サーバーへのバインドを試みます。この試行の結果は以下のいずれかになります。

- バインドが成功した場合は、「204 No Content」応答が返されます。
- ユーザーが存在しないか、パスワードが一致しないために、認証が失敗した場合は、「403 Forbidden」応答が返されます。
- 「認証パスワード」ヘッダーが存在しない場合は、「403 No Password」応答が返されます。

認証エンドポイントには、以下の要求の例のように、エンドポイント名 authentication を指定してアクセスします。

```
GET /authentication?filter=userName eq "Some User"
Authorization: Basic  QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Authentication-Password: secret
```

HTTP 応答コード

ここでは、操作の正常終了およびエラーの場合に返される HTTP 応答コードについて説明します。

正常に行われた操作

200 OK
操作が正常に完了しました。

201 Created
ユーザーまたはグループは正常が作成されました。

204 No Content
認証要求が正常に行われました。

エラー

400 Bad Request

URL にはパス・コンポーネントが必要です。

不変なエンドポイント (スキーマなど) を変更しようとしました。

エンドポイントが不明です。

外部 ID なしの POST 要求 (ユーザーまたはグループの作成) が行われました。

変更 (PUT、PATCH、または DELETE) 要求で ID が指定されませんでした。

要求の構文解析中に例外が発生しました。

変更 (PUT または PATCH) 要求に HTTP 本文が含まれていませんでした。

変更 (PUT または PATCH) 要求で HTTP 本文を JSON として構文解析できませんでした。

グループ・メンバー属性で指定された ID を LDAP DN に変換できませんでした。

検索フィルターを正常に構文解析できませんでした。

401 Unauthorized

資格情報が指定されませんでした。

資格情報 (ユーザー名またはパスワード) が誤っていました。

このユーザー名の有効範囲から外れたユーザーを変更しようとしました。

このユーザーはアクセス権限を持っていません。

このユーザーは、試行された操作を実行できません。

403 Forbidden

存在しないユーザーを認証しようとしました。

ユーザーの認証のために指定されたパスワードが誤っていました。

403 No Password

ユーザーを認証しようとしましたが、「Authentication-Password」 HTTP ヘッダーでパスワードが指定されませんでした。

404 Not Found

不明なスキーマに対する要求が行われました。

見つからないユーザーまたはグループを変更 (PUT、PATCH、または DELETE) しようとしました。

見つからないユーザーまたはグループを検索 (GET) しようとしました。

409 Conflict

存在するユーザーまたはグループを作成しようとしました。

409 Duplicate

AUTHENTICATE 要求で 2 人以上のユーザーがフィルターに一致しました。

500 Internal server error

ユーザーまたはグループが、作成後に見つかりませんでした。

要求を処理しようとしたときに例外が発生しました。

スキーマ・ファイルが見つかりませんでした。

ユーザーまたはグループのマッピング・ファイルが見つかりませんでした。

ユーザーまたはグループのマッピング・ファイルを構文解析できませんでした。

ユーザーまたはグループのマッピングで DN の作成方法が指定されませんでした。

501 Not Implemented

XML エンコードされた情報を送信または受信しようとしました。

HTML 操作が認識されませんでした。

503 Service Unavailable

バックエンド LDAP サーバーに接続できません。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。

国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向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。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラット

フォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。お客様は、IBM のアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年). このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。© Copyright IBM Corp. _年を入れる_. All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

IBM、IBM ロゴおよび ibm.com® は、世界の多くの国で登録された International Business Machines Corporation の商標です。 他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

Adobe、PostScript は、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

IT Infrastructure Library は英国 Office of Government Commerce の一部である the Central Computer and Telecommunications Agency の登録商標です。

インテル、Intel、Intel ロゴ、Intel Inside、Intel Inside ロゴ、Centrino、Intel Centrino ロゴ、Celeron、Xeon、Intel SpeedStep、Itanium、および Pentium は、Intel Corporation または子会社の米国およびその他の国における商標または登録商標です。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

ITIL は英国 The Minister for the Cabinet Office の登録商標および共同体登録商標であって、米国特許商標庁にて登録されています。

UNIX は The Open Group の米国およびその他の国における登録商標です。

Java™ およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

Cell Broadband Engine は、Sony Computer Entertainment, Inc.の米国およびその他の国における商標であり、同社の許諾を受けて使用しています。

Linear Tape-Open、LTO、LTO ロゴ、Ultrium、および Ultrium ロゴは、HP、IBM Corp. および Quantum の米国およびその他の国における商標です。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

[サ行]

[タ行]

[ハ行]

[マ行]

[ラ行]

A

D

E

F

H

I

J

L

P

Q

S

Printed in Japan

SA88-7236-01

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