Novell LDAP 用 Identity Manager ドライバ

1.9.2

www.novell.com

実装ガイド

2006 年 5 月 25 日

Novell®

保証と著作権

米国 Novell, Inc. およびノベル株式会社は、本書の内容または本書に起因する結果に関して、いかなる責任も負いません。また、本書の商品性、および特定用途への適合性について、いかなる黙示の保証も否認し、排除します。米国 Novell, Inc. およびノベル株式会社は、本書の内容を改訂または変更する権利を常に留保します。米国 Novell, Inc. およびノベル株式会社は、このような改訂または変更を個人または事業体に通知する義務を負いません。

米国 Novell, Inc. およびノベル株式会社は、ノベル製ソフトウェアの使用に起因する結果に関して、いかなる表示も行いません。また、商品性、および特定目的への適合性について、いかなる黙示の保証も行いません。米国 Novell, Inc. およびノベル株式会社は、ノベル製ソフトウェアの内容を変更する権利を常に留保します。米国 Novell, Inc. およびノベル株式会社は、このような変更を個人または事業体に通知する義務を負いません。

本契約の締結に基づいて提供されるすべての製品または技術情報には、米国の輸出管理規定およびその他の国の貿易関連法規が適用されます。お客様は、取引対象製品の輸出、再輸出または輸入に関し、国内外の輸出管理規定に従うこと、および必要な許可、または分類に従うものとします。お客様は、現在の米国の輸出除外リストに記載されている企業、および米国の輸出管理規定で指定された輸出禁止国またはテロリスト国に本製品を輸出または再輸出しないものとします。お客様は、取引対象製品を、禁止されている核兵器、ミサイル、または生物化学兵器を最終目的として使用しないものとします。本ソフトウェアの輸出については、www.novell.co.jp/info/exports/expmtx.html または www.novell.com/ja-jp/company/exports/ もあわせてご参照ください。弊社は、お客様が必要な輸出承認を取得しなかったことに対し如何なる責任も負わないものとします。

米国 Novell, Inc. は、本ドキュメントで説明されている製品に組み込まれた技術に関する知的財産権を有します。これらの知的所有権は、http://www.novell.com/company/legal/patents/ に記載されている 1 つ以上の米国特許、および米国ならびにその他の国における 1 つ以上の特許または出願中の特許を含む場合があります。

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

オンラインマニュアル : 本製品とその他の Novell 製品のオンラインマニュアルにアクセスする場合や、アップデート版を入手する場合は、www.novell.com/ja-jp/documentation をご覧ください。

Novell の商標

Novell の商標については、商標とサービスマークの一覧 (http://www.novell.com/company/legal/trademarks/tmlist.html) を参照してください。

第三者の商標

第三者の商標は、それぞれの所有者に属します。

目次

このガイドについて

このガイドでは、LDAP 用の Identity Manager ドライバのインストール方法および設定方法について説明します。

対象読者

このガイドは、LDAP 用 Identity Manager ドライバを使用する Novell® eDirectory™ および Identity Manager の管理者を対象にしています。

ご意見やご要望

このマニュアルおよび本製品に含まれるその他のマニュアルに関するご意見やご要望をお聞かせください。オンラインヘルプの各ページの下部にあるユーザコメント機能を使用するか、または www.novell.com/documentation/feedback.html にアクセスして、ご意見をお寄せください。

最新のマニュアル

このマニュアルの最新バージョンについては、Novell マニュアルの Web サイト (http://www.novell.com/ja-jp/documentation) の Identity Manager ドライバのセクションで LDAP 用の Identity Manager ドライバを参照してください。

その他のマニュアル

Identity Manager および Identity Manager の他のドライバについては、Novell マニュアルの Web サイト (http://www.novell.com/ja-jp/documentation) を参照してください。

表記規則

本マニュアルでは、手順に含まれる複数の操作および相互参照パス内の項目を分けるために、大なり記号 (>) を使用しています。

商標記号 (®、™ など) は、Novell の商標を示します。アスタリスク (*) は第三者の商標を示します。

LDAP 用 Identity Manager ドライバの概要

1

1.1 新機能

表 *1-1* リリースされた機能の概要

機能	LDAP ドライバのバージョン	説明
PasswordModify 拡張操作のサポート	1.9	LDAP 用 Identity Manager ドライバは、RFC 3062 で定義されている PasswordModify 拡張操作をサポートします。 PasswordModify 拡張操作をサポートする LDAP ディレクトリ (OpenLDAP など) を使用している場合、LDAP 用ドライバでは、購読者チャネルでのパスワードの設定時または変更時に拡張操作が使用されます。 LDAP ディレクトリが PasswordModify 拡張操作をサポートしていない場合、LDAP 用ドライバでは、以前のドライババージョンと同様に UserPassword 属性の値が設定されます。この値は、ハッシュされて安全に保存されます。 この機能には、特別な設定は不要です。ドライバには LDAP サーバがこの操作をサポートしているかどうかを判別する機能があります。
バイナリオプションを属性名に追加するかどうかを制御する	1.9.2	購読者チャネルのパラメータは、値のエンコード時にバイナリオプションを属性名に追加するかどうかを制御します。29 ページの 「LDAP 購読者設定」を参照してください。
最初の検索結果を同期するかどうかを制御する	1.9.2	LDAP 検索で用いられる発行方法のパラメータは、最初の検索結果を同期するか、その後の変更だけを同期するかを制御します。33 ページの 「LDAP 発行者設定 : LDAP 検索方式のみ」を参照してください。

1.2 今後の更新に関する情報

今後の更新では、次の機能拡張が予定されています。

- 発行者チャネルの移動イベントのサポート

- LDAP サーバが Sun* のディレクトリである場合の、発行者チャネルパスワード同期のサポート。

  これらは更新されたドライバと Sun ディレクトリのプラグインによりサポートされます。Sun ディレクトリにプラグインをインストールして設定します。

1.3 用語の変更

次の用語が、旧リリースから変わりました。

表 *1-2* 用語の変更

旧用語	新用語
DirXML®	Identity Manager
DirXML サーバ	メタディレクトリサーバ
DirXML エンジン	メタディレクトリエンジン
eDirectory™	アイデンティティボールト (eDirectory 属性またはクラスを参照する場合は除く)

1.4 ドライバの概要

LDAP 用 Identity Manager ドライバは、アイデンティティボールトと LDAP 準拠のディレクトリの間でデータを同期します。このドライバは、Windows*、NetWare®、Linux*、Solaris*、および AIX* をはじめとする、アイデンティティボールトが実行するすべてのプラットフォームで動作し、メタディレクトリサーバまたは Identity Manager リモートローダが実行している場所で実行できます。

このドライバは、軽量ディレクトリアクセスプロトコル (LDAP) を使用して、LDAP 準拠の接続ディレクトリとアイデンティティボールトの間の変更を双方向に同期します。

通信向けの柔軟性の高いモデルであることから、このドライバはアイデンティティボールトでサポートされていないプラットフォーム (HP-UX*、OS/400、OS/390 など) で実行する LDAP 準拠のディレクトリとの同期が可能です。

このドライバでは、次のいずれかの発行方法に従ってデータ変更を認識し、そうした変更を Identity Manager を介してアイデンティティボールトに通知できます。

- 変更ログ方式

  この方式は、変更ログが使用可能な場合に優先されます。変更ログは次の場所にあります。

  - Netscape* Directory Server
  - iPlanet* Directory Server
  - IBM* SecureWay Directory
  - Critical Path* InJoin* Directory
  - Oracle* Internet Directory

30 ページのセクション 4.1.3「LDAP 発行者設定 : 変更ログと LDAP 検索方式」および 31 ページのセクション 4.1.4「LDAP 発行者設定 : 変更ログ方式のみ」を参照してください。

- LDAP 検索方式

  一部のサーバでは、変更ログメカニズムを採用していません。LDAP 検索方式を利用すると、LDAP ドライバで LDAP サーバに関するデータをアイデンティティボールトに発行できます。

  追加ソフトウェアや LDAP 準拠のディレクトリの変更は必要ありません。

  33 ページのセクション 4.1.5「LDAP 発行者設定 : LDAP 検索方式のみ」を参照してください。

Identity Manager の新機能については、『Identity Manager 3.0 インストールガイド』の「Identity Manager 3 の新機能」を参照してください。

1.5 デフォルトのドライバ環境設定

この節では、このドライバ固有の実装、追加、または例外について説明します。Identity Manager の基礎については、『Novell Identity Manager 3.0 管理ガイド』を参照してください。

1.5.1 データフロー

この節では、データフローを制御するチャネル、フィルタ、およびポリシーについて解説します。

発行者チャネルと購読者チャネル

このドライバは、次に示すように発行者チャネルと購読者チャネルをサポートします。

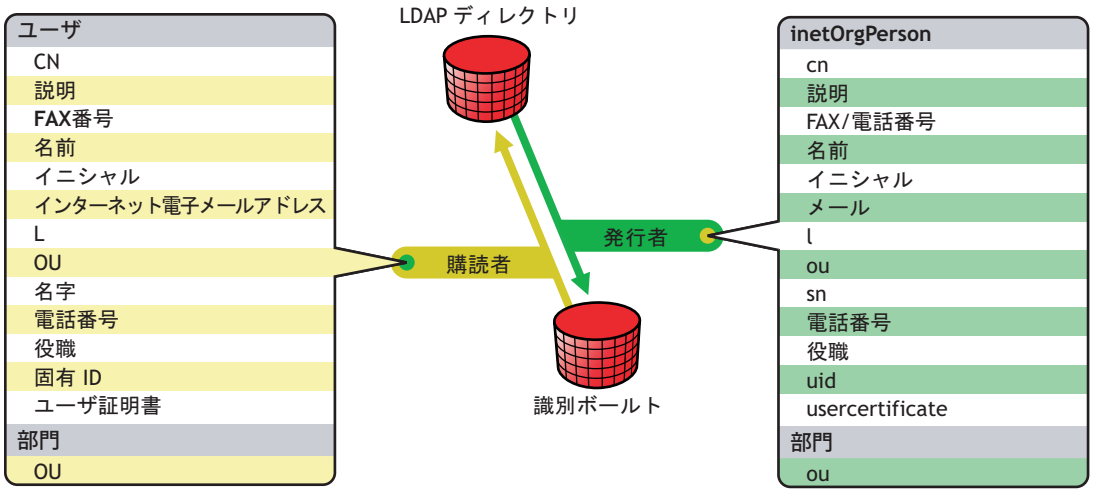
- 発行者チャネルでは、LDAP ディレクトリ変更ログまたは LDAP 検索からの情報が読み込まれ、その情報がメタディレクトリエンジンを介してアイデンティティボールトに送信されます。

  デフォルトでは、発行者チャネルにより 20 秒ごとにログがチェックされ、未処理の最初のエントリから始めて、一度に最大 1000 エントリが処理されます。
- 購読者チャネルでは、アイデンティティボールトブジェクトへの追加や変更が監視され、LDAP ディレクトリに変更を加える LDAP コマンドが発行されます。

フィルタ

Identity Manager では、フィルタを使用して、共有されるオブジェクトや属性を制御します。次の図に示すように、LDAP ドライバのフィルタは、デフォルトでオブジェクトや属性を共有できる設定になっています。

図 *1-1* *LDAP ドライバのフィルタ*



ポリシー

ポリシーは、ドライバとアイデンティティボールトの間のデータ同期を制御するために使用されます。LDAP ドライバには、ポリシーを設定する 2 つの設定済みのオプションが付属しています。

- 平面オプションでは、両方のディレクトリにユーザの平面構造が実装されます。

  この環境設定では、一方のディレクトリに作成されたユーザオブジェクトは、ドライバの設定中に他方のディレクトリに指定したコンテナのルートに格納されます (コンテナは、アイデンティティボールトと LDAP ディレクトリの両方で同じ名前にする必要はありません)。既存のオブジェクトが更新されても、そのコンテキストは保持されます。

- ミラー側オプションは、ディレクトリ内の階層構造を一致させます。

  この環境設定では、一方のディレクトリに新規ユーザオブジェクトが作成されると、そのオブジェクトは、他方のディレクトリ内の一致する階層レベルのミラーコンテナに格納されます。既存のオブジェクトが更新されても、そのコンテキストは保持されます。

平面環境設定では部門オブジェクトが同期されない点と、配置ポリシーを除き、これらのオプションのポリシー設定は同一です。

次の表は、デフォルトのポリシーに関する情報を示しています。これらのポリシーとそこに含まれている個々のルールは、27 ページの第 4 章「LDAP ドライバのカスタマイズ」で説明されているように、Novell iManager によってカスタマイズできます。

表 *1-3* デフォルトのポリシー

ポリシー	説明
マッピング	アイデンティティボールトユーザオブジェクトと選択したプロパティを LDAP の inetOrgPerson にマップします。 アイデンティティボールトの部門を LDAP の organizationalUnit にマップします。 デフォルトでは、十数個の標準のプロパティがマップされます。
発行者の作成	アイデンティティボールトにユーザを作成するために、cn、sn、mail の各属性を定義する必要があることを指定します。部門を作成するために、ou 属性を定義する必要があります。
発行者の配置	単純配置オプションでは、LDAP ディレクトリに作成される新規ユーザオブジェクトは、ドライバ環境設定のインポート時に指定するアイデンティティボールト内のコンテナに格納されます。ユーザオブジェクトには、cn の値で名前が付けられます。 ミラー配置オプションでは、LDAP ディレクトリに作成される新規ユーザオブジェクトは、オブジェクトの LDAP コンテナをミラーリングするアイデンティティボールトコンテナに格納されます。
一致	電子メール属性が一致する場合にアイデンティティボールト内のユーザオブジェクトが LDAP ディレクトリの inetOrgPerson と同じオブジェクトであることを指定します。
購読者の作成	LDAP ディレクトリにユーザを作成するために、CN、名字、インターネット電子メールアドレスの各属性を定義する必要があることを指定します。部門を作成するために、OU 属性を定義する必要があります。
購読者の配置	ドライバ環境設定のインポート中に［平面］配置オプションを選択すると、アイデンティティボールトに作成される新規ユーザオブジェクトは、インポート中に指定した値を基にします。 ドライバ環境設定のインポート中に［ミラーリング済み］配置を選択すると、アイデンティティボールトに作成される新規ユーザオブジェクトは、オブジェクトのアイデンティティボールトコンテナをミラーリングする LDAP ディレクトリコンテナに格納されます。

アップグレード

2

2.1 ドライバシムのアップグレード

アップグレードにより、既存のドライバシムが新しいドライバシムで置き換えられますが、旧ドライバの環境設定はそのまま使用できます。新しいドライバシムで DirXML® 1.*x* の環境設定を実行する場合、変更は必要ありません。

ドライバシムをアップグレードするには、次を実行します。

1. 現在実行中のバージョンに対するパッチをすべて適用してドライバを更新していることを確認します。

   ドライバシムおよび環境設定に最新の修正が適用されていれば、通常は、既存のドライバ環境設定を変更しなくても新しいドライバシムが機能するようになっています。使用中のドライバのバージョンについて、すべての TID および製品の更新を確認します。

   アップグレードの問題を最小限にするために、この手順をすべてのドライバで実行することをお勧めします。

2. 新しいドライバシムをインストールします。

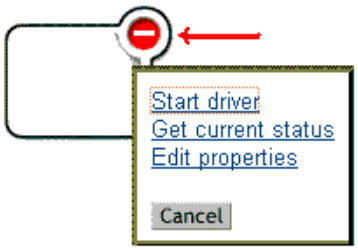
   これは、メタディレクトリエンジンのインストールと同時に、またはその後に実行できます。13 ページの第 3 章「LDAP ドライバのインストール」を参照してください。

3. シムのインストール後に、ドライバを再起動します。

   3a iManager で、［Identity Manager］>［Identity Manager の概要］の順に選択します。

   3b ドライバが存在するドライバセットを参照します。

   3c 再起動するドライバを選択し、ステータスアイコンをクリックして、［ドライバの起動］を選択します。



4. Identity Manager のアクティベーションキーを使用してドライバシムをアクティブにします。

   アクティブ化の方法については、『Identity Manager 3.0 インストールガイド』の「Novell Identity Manager 製品のアクティベーション」を参照してください。

ドライバシムをインストールしたら、ドライバ環境設定をアップグレードします。12 ページのセクション 2.2「ドライバ環境設定のアップグレード」を参照してください。

2.2 ドライバ環境設定のアップグレード

ドライバシムをインストールしても、既存の環境設定は変更されません。既存の環境設定は、新しいドライバシムでも変更なしで引き続き使用できます。

ただし、新機能を利用するには、ドライバ環境設定をアップグレードする必要があります。ドライバ環境設定は、既存のドライバ環境設定を新しいサンプル環境設定で置き換えるか、または既存の環境設定を Identity Manager 形式に変換してポリシーを追加するかのいずれかの方法でアップグレードします。

- 既存の環境設定を置き換えるには、既存のドライバオブジェクトの新しいサンプル環境設定をインポートします。
- 新しいIdentity Managerプラグインで編集できるように既存のドライバ環境設定を変換する方法については、『Novell Identity Manager 3.0 管理ガイド』の「DirXML 1.1a から Identity Manager 形式へのドライバ環境設定のアップグレード」を参照してください。
- Identity Manager のパスワード同期機能を既存のドライバ環境設定に追加するには、『Novell Identity Manager 3.0 管理ガイド』の「パスワード同期をサポートするための、既存のドライバ設定のアップグレード」を参照してください。

LDAP ドライバのインストール

3

3.1 計画段階の考慮事項

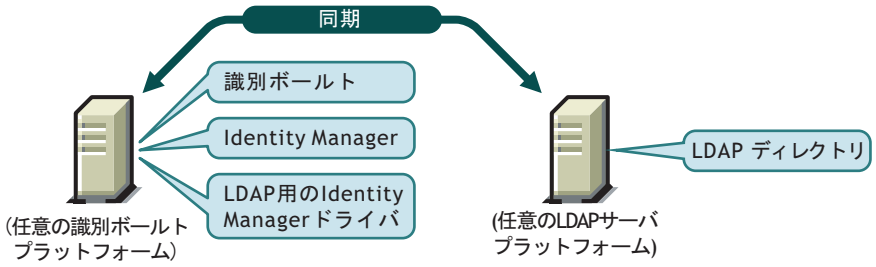
Identity Manager 対応の LDAP ドライバは、LDAP v3 互換のほとんどの LDAP サーバで機能します。このドライバは、LDAP の RFC 2251 仕様に従って作成されています。互換性の問題については、46 ページのセクション 5.3「LDAP v3 の互換性」を参照してください。

3.1.1 LDAP ドライバをインストールする場所

Identity Manager ドライバは、アイデンティティボールトとメタディレクトリエンジンがインストールされている同一コンピュータ上にインストールできます。このインストールは、ローカル構成と呼ばれます。

ローカル構成では、次の図に示すように、LDAP ドライバをアイデンティティボールトとメタディレクトリエンジンがインストールされているコンピュータにインストールします。

図 *3-1* ローカル構成



プラットフォームまたはポリシーの制約のためにローカル構成が困難な場合は、ターゲットアプリケーションをホストしているコンピュータに Identity Manager ドライバをインストールできます。このインストールは、リモート構成と呼ばれます。

リモート構成で LDAP ドライバをインストールすることは可能ですが、次の理由から、柔軟性はあまり高くはなりません。

- ドライバは任意のアイデンティティボールトプラットフォームで実行できる。
- ドライバは LDAP プロトコルを介して任意のプラットフォームの LDAP サーバと通信する。

3.1.2 Identity Manager 3 へのアップグレード

Identity Manager のインストール中に、メタディレクトリエンジンをインストールすると同時に、LDAP 用ドライバを (他の Identity Manager ドライバとともに) インストールできます。『Identity Manager 3.0 インストールガイド』を参照してください。DirXML 1.1a または Identity Manager 2 から Identity Manager 3 にアップグレードできます。

3.1.3 収集する情報

インストール中やセットアップ中に、次のような情報を要求するメッセージが表示されます。

- 階層構造の同期に平面またはミラー側のどちらのオプションを使用するか。8 ページの 「ポリシー」を参照してください。
- 同期されたオブジェクトを保持するアイデンティティボールトコンテナと LDAP ディレクトリコンテナ。
- ドライバの同等セキュリティとして割り当てるアイデンティティボールトのユーザオブジェクトと同期から除外するオブジェクト。
- ドライバによる LDAP ディレクトリへのアクセスに使用される LDAP オブジェクトとパスワード。

23 ページの 「サンプルのドライバ環境設定ファイルのインポート」の表を参照してください。

3.1.4 LDAP データソースに関する前提

発行者チャネルを使用して LDAP ディレクトリでの変更に関するデータをアイデンティティボールトに送信する場合は、データを発行するためにドライバで使用される次の 2 つの方式を理解する必要があります。

- 変更ログ方式

  変更ログは、LDAP ディレクトリにおけるメカニズムです。変更ログからドライバの LDAP イベント情報を取得できます。この方式は、変更ログが使用可能な場合に優先されます。

- LDAP 検索方式

  この方式を利用すると、LDAP ドライバで、変更ログを使用しない LDAP サーバに関するデータをアイデンティティボールトに発行できるようになります。

3.2 システムの前提条件

- ❑ Novell® Identity Manager
- ❑ Identity Manager 以降のシステム要件
- ❑ 変更ログ方式を使用している場合は、次のいずれかの LDAP ディレクトリが必要です。
  - Netscape Directory Server 4.*x* または 6
  - iPlanet Directory Server 5.0 以降
  - IBM SecureWay Directory 3.2、4.1.1、または 5.1

- Critical Path InJoin Directory 3.1
- Oracle Internet Directory 2.1.1 以降
- Sun ONE* 5.2
- LDAP バージョン 3 準拠のディレクトリ

3.3 インストール

- 15 ページの 「LDAP ドライバのインストール」
- 20 ページの 「ドライバの設定」

3.3.1 LDAP ドライバのインストール

メタディレクトリエンジンをインストールした後で、ドライバを別途インストールできます。

- 15 ページの 「Windows でのインストール」
- 17 ページの 「NetWare でのインストール」
- 18 ページの 「Linux、Solaris、または AIX でのインストール」

Windows でのインストール

Windows NT* 2003 サーバ、または Support Pack 2 を適用した Windows NT 2000 に LDAP 用 Identity Manager ドライバをインストールします。

1. Identity Manager 2.0 の CD またはダウンロードイメージからインストールプログラムを実行します。

   ダウンロードイメージは、ノベル用ダウンロード (http://download.novell.com/index.jsp) から入手できます。

   インストールプログラムが自動的に起動されない場合は、\nt\install.exe を実行できます。
2. ［ようこそ］ダイアログボックスで、［次へ］をクリックして、使用許諾契約書に同意します。
3. 最初の［Identity Manager の概要］ダイアログボックスで、情報を確認して、［次へ］をクリックします。

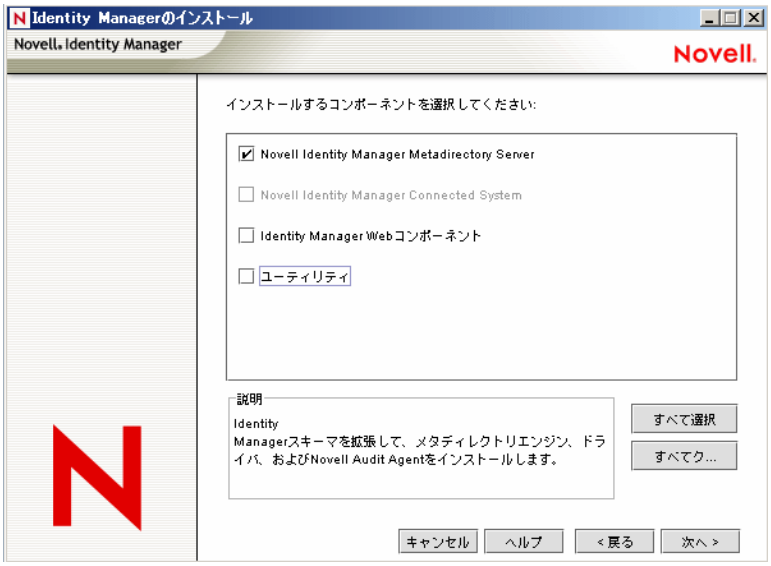
   このダイアログボックスには、次の情報が表示されます。

   - メタディレクトリサーバ
   - Identity Manager 接続サーバシステム
4. 2 番目の［Identity Manager の概要］ダイアログボックスで、情報を確認して、［次へ］をクリックします。

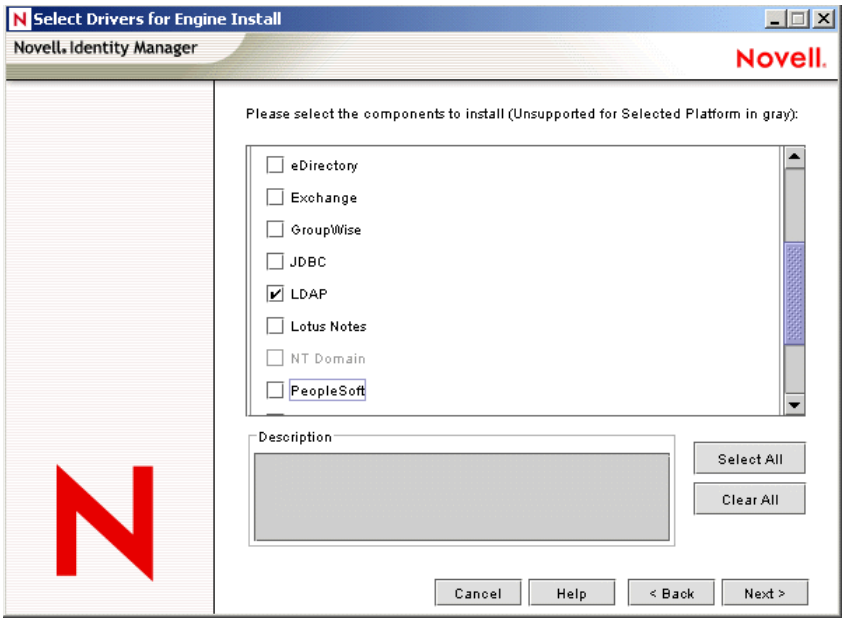
   このダイアログボックスには、次の情報が表示されます。

   - Web ベースの管理サーバ
   - Identity Manager ユーティリティ

5 ［インストールするコンポーネントを選択してください］のダイアログボックスで、［メタディレクトリサーバ］だけを選択し、［次へ］をクリックします。



6 エンジンインストールのドライバを選択するダイアログボックスで、［LDAP］だけを選択し、［次へ］をクリックします。



7 ［Identity Manager アップグレードの警告］ダイアログボックスで、［OK］をクリックします。

8 ［スキーマ拡張］ダイアログボックスで、ユーザ名とパスワードを入力して、［次へ］をクリックします。

パスワードを有効にするために、ルートの権限が必要です。

9 ［概要］ダイアログボックスで、選択したオプションを確認して、［終了］をクリックします。

10 ［インストールが完了しました］ダイアログボックスで、［閉じる］をクリックします。

インストール後、20 ページの 「ドライバの設定」にある説明に従ってドライバを設定します。

NetWare でのインストール

1 NetWare® サーバで、Identity Manager 3 の CD をドライブに挿入して、CD をボリュームとしてマウントします。

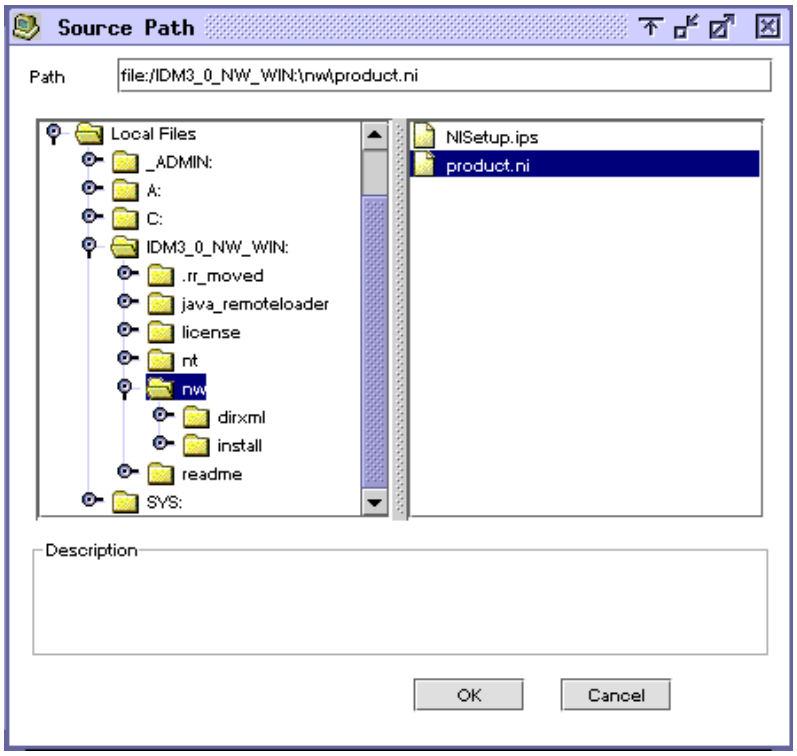
CD をマウントするには、「m cdrom」と入力します。

2 (条件付き) グラフィカルユーティリティがロードされない場合は、「startx」と入力してユーティリティをロードします。

3 グラフィカルユーティリティで、［Novell］アイコンをクリックして、［インストール］をクリックします。

4 ［インストール済みの製品］ダイアログボックスで、［追加］をクリックします。

5 ［ソースパス］ダイアログボックスで、product.ni ファイルを参照して選択します。



5a 以前にマウントした CD ボリュームを参照して展開します。

5b nw ディレクトリを展開し、product.ni を選択して、［OK］を 2 回クリックします。

6 ［ようこそ］ダイアログボックスで、［次へ］をクリックして、使用許諾契約書に同意します。

7 ［Identity Manager のインストール］ダイアログボックスで、［メタディレクトリサーバ］だけを選択します。

次の項目を選択解除します。

- Identity Manager Web コンポーネント
- ユーティリティ

8 エンジンインストールのドライバを選択するダイアログボックスで、［区切りテキスト］だけを選択します。

次の項目を選択解除します。

- メタディレクトリエンジン
- LDAP 以外のすべてのドライバ

9 ［次へ］をクリックします。

10 ［Identity Manager アップグレードの警告］ダイアログボックスで、［OK］をクリックします。

このダイアログボックスに、90 日以内にドライバのライセンスを有効にするよう促すメッセージが表示されます。

11 ［スキーマ拡張］ダイアログボックスで、ユーザ名とパスワードを入力して、［次へ］をクリックします。

12 ［概要］ページで、選択したオプションを確認して、［終了］をクリックします。

13 ［閉じる］をクリックします。

インストール後、20 ページの 「ドライバの設定」にある説明に従ってドライバを設定します。

Linux、Solaris、または AIX でのインストール

デフォルトでは、LDAP 用 Identity Manager ドライバは、メタディレクトリエンジンをインストールするときにインストールされます。この節では、メタディレクトリエンジンのインストール時にドライバがインストールされなかった場合のドライバのインストール方法についても記載しています。

インストールプログラムに従って進むときに、「previous」と入力すれば前のセクション (画面) に戻ることができます。

1 端末のセッションで、root としてログインします。

2 Identity Manager 3.0 の CD をドライブに挿入してマウントします。

通常、CD は自動的にマウントされます。CD を手動でマウントすることもできます。たとえば、SUSE® の場合は、「mount /media/cdrom」と入力します。

3 setup ディレクトリに移動します。

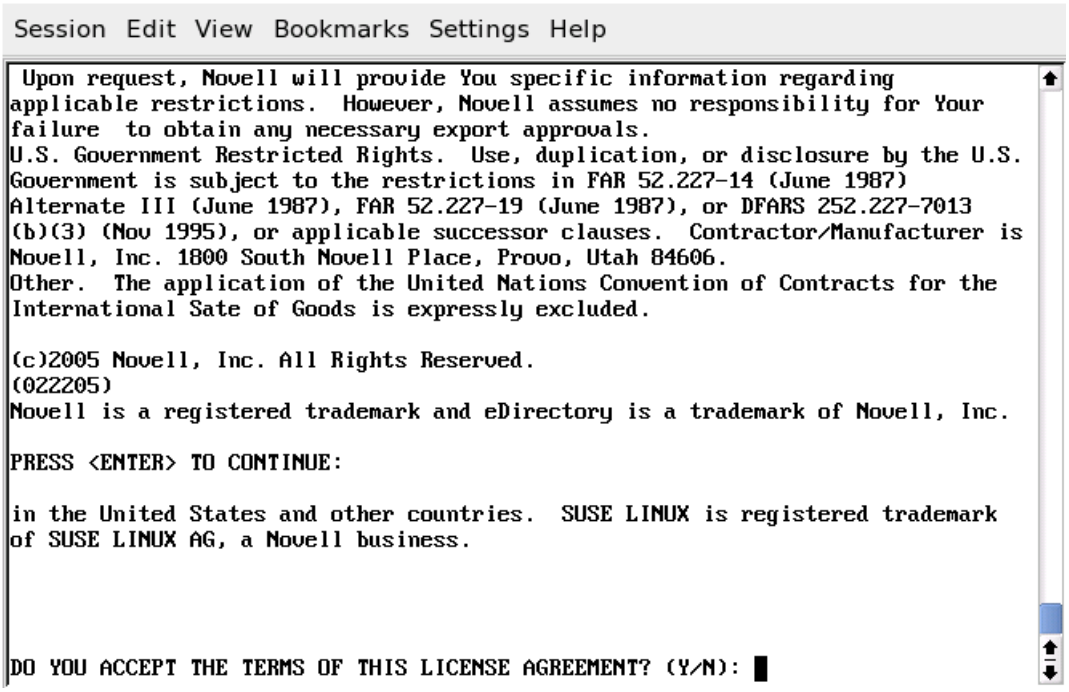
プラットフォーム	パス
Red Hat	/mnt/cdrom/linux/setup/
SUSE	/media/cdrom/linux/setup/
Solaris	/cdrom/solaris/_idm_2/setup/
AIX	/media/cdrom/aix/setup/

4 インストールプログラムを実行します。

たとえば、SUSE の場合は、./dirxml_linux.bin を実行します。

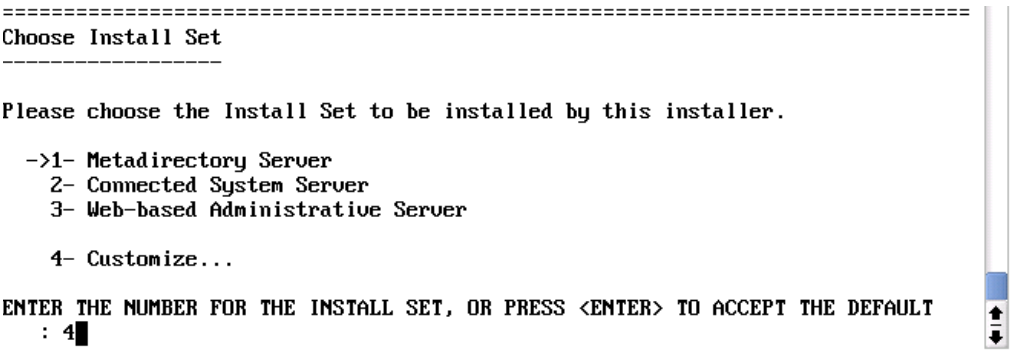
5 ［イントロダクション］セクションで、<Enter> キーを押します。

6 ［DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT (この使用許諾契約書の条項に同意しますか ?)］が表示されるまで <Enter> キーを押し、使用許諾契約書に同意するために「y」と入力して、<Enter> キーを押します。



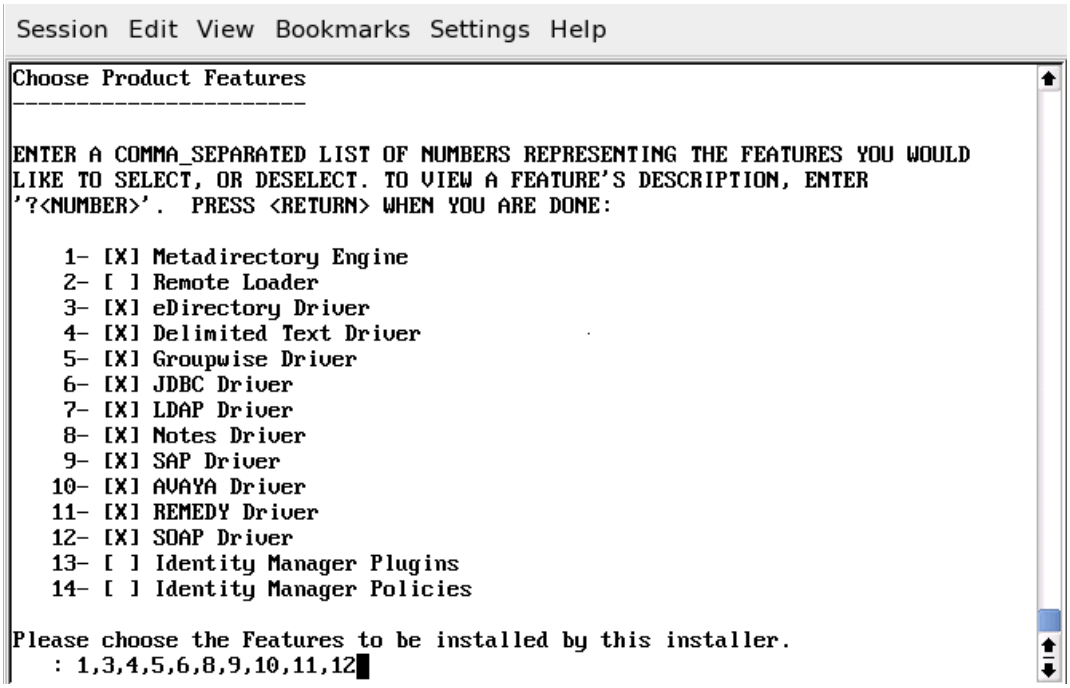
7 ［インストールセットの選択］セクションで、［カスタマイズ］オプションを選択します。

「4」と入力して、<Enter> キーを押します。

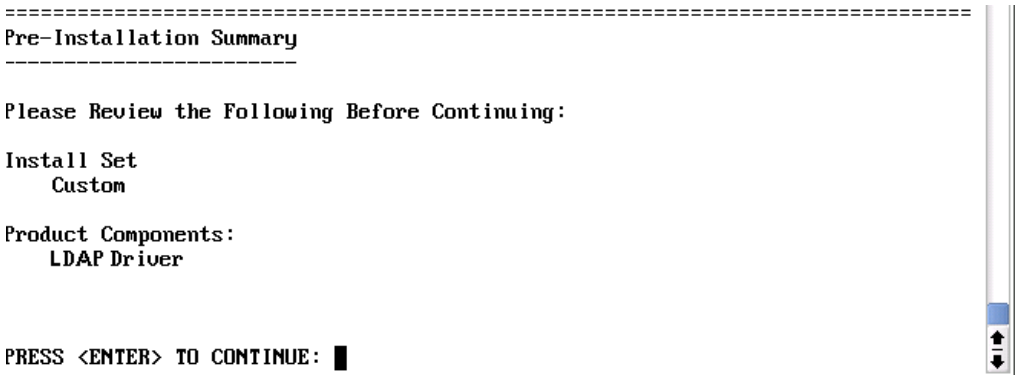


8 ［Choose Product Features (製品の機能の選択)］セクションで、［LDAP］を除くすべての機能を選択解除して、<Enter> キーを押します。

機能を選択解除するには、その番号を入力します。複数の機能を選択解除するには、各機能の間にカンマを入力します。



9 ［インストール前の概要］セクションで、オプションを確認します。



前のセクションに戻るには、「previous」と入力して、<Enter> キーを押します。

続行するには、<Enter> キーを押します。

10 インストールが完了したら、<Enter> キーを押してインストールを終了します。

インストール後、20 ページの 「ドライバの設定」にある説明に従ってドライバを設定します。

3.3.2 ドライバの設定

既存のドライバをアップグレードしている場合、セットアップは不要です。

LDAP ドライバを初めて使用した場合は、これ以降の節に記載されているセットアップタスクを実行します。

- 21 ページの 「LDAP サーバの準備」
- 23 ページの 「サンプルのドライバ環境設定ファイルのインポート」
- 25 ページの 「ドライバの起動」
- 26 ページの 「データの移行と再同期化」
- 26 ページの 「ドライバの有効化」

LDAP サーバの準備

アイデンティティボールトから LDAP サーバ (購読者チャネルで) へのデータの同期のみにこのドライバを使用するのであれば、ほとんどの LDAP サーバやアプリケーションは追加設定なしで機能します。

常に必要な権限を持つユーザオブジェクトを作成し、ドライバが LDAP サーバに対して認証できるようにしてください。

ただし、LDAP サーバのエントリに加えた変更を (発行者チャネルで) アイデンティティボールトに同期させる必要があり、その際に変更ログ方式を採用する場合は、LDAP サーバで別の設定タスクを少なくとも 1 つ実行してからでなければ、ドライバを実行することができません。LDAP サーバの変更ログメカニズムが有効になっていることを確認してください。

重要 **:** LDAP サーバに変更ログメカニズムがない場合は、LDAP 検索方式を使用します。そうしなければ、ドライバからそのサーバのイベントを発行できません。

認証権限を備えた LDAP ユーザオブジェクトの作成

購読者チャネルで発生するイベントは発行者チャネルのメタディレクトリエンジンに返送されますが、変更ログ発行方式を採用することで、ドライバはこうしたループバックの発生を回避しようとします。ただし、LDAP 検索方式では、ループバックを防止するために、メタディレクトリエンジンが利用されます。

変更ログ方式では、ドライバによるループバックの発生を防止する 1 つの方法として、変更ログを調べて変更したユーザを確認します。変更を行ったユーザが、ドライバで認証に使用されるユーザと同じ場合、発行者は、ドライバの購読者チャネルにより変更が行われたと仮定します。

注 **:** Critical Path InJoin Server を使用する場合、変更を開始したオブジェクトの DN は提供されないため、該当するサーバでの変更ログの実装は一部制限されます。したがって、作成者 / 変更者 DN を使用して、変更がアイデンティティボールトから生じたかどうかを決定することはできません。

その場合、変更ログで検出されるすべての変更は、発行者によってメタディレクトリエンジンに送信され、最適化または変更により、不要な変更や繰り返しの変更は破棄されます。

発行者チャネルでの正当な変更を破棄させないようにするために、ドライバでの認証に使用するユーザオブジェクトが他の目的に使用されていないことを確認します。

たとえば、Netscape Directory Server を使用しており、管理者アカウント CN=Directory Manager を使用するようドライバを設定しているとします。Netscape Directory Server に手動で変更を加えて、その変更を同期させた場合は、CN=Directory Manager でログインおよび変更が実行できなくなります。このような場合には別のアカウントを使用しなければなりません。

この問題を回避するには、次のようにします。

1. ドライバで排他的に使用されるユーザアカウントを作成します。
2. そのユーザアカウントに、変更ログを確認する権限と、ドライバで変更を加えるために必要な権限を割り当てます。

   たとえば、VMP 社で、uid=ldriver,ou=Directory Administrators,o=lansing.vmp.com というドライバのユーザアカウントを作成するとします。次に、そのユーザアカウントに適切な権限を割り当てるために、LDAPModify ツールまたは Novell インポート / エクスポート変換ユーティリティを使用して、次の LDIF をサーバに適用します。

```
# give the new user rights to read and search the changelog


dn: cn=changelog


changetype: modify


add: aci


aci: (targetattr = "*")(version 3.0; acl "LDAP DirXML Driver";
allow (compare,read,search) userdn = "ldap:///
uid=ldriver,ou=Directory Administrators,o=lansing.vmp.com"; )


-


# give the new user rights to change anything in the
o=lansing.vmp.com container


dn: o=lansing.vmp.com


changetype: modify


add: aci


aci: (targetattr = "*")(version 3.0; acl "LDAP DirXML Driver";
allow (all) userdn = "ldap:///uid=ldriver,ou=Directory
```

```
Administrators,o=lansing.vmp.com"; )


-
```

変更ログの有効化

変更ログは LDAP サーバの一部であり、このログにより、LDAP ディレクトリからアイデンティティボールトに発行する必要がある変更をドライバで認識できます。このドライバでサポートされている LDAP ディレクトリは、変更ログメカニズムをサポートしています。

Critical Path InJoin および Oracle Internet Directory は、デフォルトで変更ログが有効になっています。変更ログを無効にしない限り、さらに手順を実行して変更ログを有効にする必要はありません。

IBM SecureWay、Netscape Directory Server、および iPlanet Directory Server では、インストール後に変更ログを有効にする必要があります。変更ログを有効にする方法の詳細については、LDAP ディレクトリをサポートしている製品のマニュアルを参照してください。

ヒント **:** iPlanet の変更ログでは、Retro Changelog プラグインを有効にする必要があります。

サンプルのドライバ環境設定ファイルのインポート

- 23 ページの 「iManager を使用したインポート」
- 25 ページの 「Identity Manager の Designer を使用したインポート」

iManager を使用したインポート

LDAP ドライバ環境設定をインポートするには、『Novell Identity Manager 3.0 管理ガイド』の「ドライバの作成と設定」に記載されているドライバのインポート手順に従います。

インポート中に、ドライバ環境設定の次の情報を指定します。

表 *3-1* *LDAP* ドライバの設定

フィールド	説明
ドライバ名	このドライバに割り当てられるアイデンティティボールトブジェクト名、または環境設定を更新する既存のドライバ。
配置タイプ	単純配置オプションでは、LDAP ディレクトリに作成される新規ユーザオブジェクトは、ドライバ環境設定のインポート時に指定するアイデンティティボールト内のコンテナに格納されます。ユーザオブジェクトには、cn の値で名前が付けられます。 ミラー配置オプションでは、LDAP ディレクトリに作成される新規ユーザオブジェクトは、オブジェクトの LDAP コンテナをミラーリングするアイデンティティボールトコンテナに格納されます。

フィールド	説明
eDirectory コンテナ	新規ユーザを作成する必要があるアイデンティティボールト内のコンテナ。 このコンテナが存在しない場合は、コンテナを作成してから、ドライバを起動する必要があります。 LDAPMirrorSample.xml の環境設定の場合、このディレクトリは、ドライバの配置ポリシーの起点となります。サブオーディネイトコンテナには、LDAP ミラーコンテナ内のサブオーディネイトコンテナと同じ名前を付ける必要があります。 平面環境設定の場合、このコンテナにはすべてのユーザオブジェクトが収容されます。
LDAP コンテナ	新しいユーザを作成する必要がある LDAP ディレクトリ内のコンテナ。 このコンテナが存在しない場合は、コンテナを作成してから、ドライバを起動する必要があります。 平面環境設定の場合、このディレクトリは、ドライバの配置ポリシーの起点となります。 LDAPSimplePlacementSample.xml の環境設定の場合、このコンテナにはすべてのユーザオブジェクトが収容されます。
LDAP サーバ	LDAP サーバのホスト名または IP アドレスおよびポート。
LDAP 認証 DN	LDAP ドライバ用に作成された管理者アカウントの LDAP DN を指定します。
LDAP 認証パスワード	LDAP ドライバ管理者アカウントのパスワード。隣のフィールドにパスワードを再入力して、パスワードを確認します。 これは、認証ユーザに必要なパスワードです。 LDAP ドライバがディレクトリマネージャを排他的に使用する場合は、デフォルトの認証ユーザが適しています。ただし、このユーザを他の目的に使用するには、場合によって、ドライバの起動後にデフォルトを変更する必要があります。21 ページの 「認証権限を備えた LDAP ユーザオブジェクトの作成」を参照してください。
SSL	LDAP プロトコルの通信を暗号化します。
データフローの設定	◆ 双方向は、LDAP とアイデンティティボールトの両方が、両者間で同期されるデータの信頼されるソースであることを示します。 ◆ LDAP to eDirectory (LDAP から eDirectory へ) は、LDAP が信頼されるソースであることを示します。 ◆ eDirectory to LDAP (eDirectory から LDAP へ) は、アイデンティティボールトが信頼されるソースであることを示します。
リモート / ローカルとしてのドライバのインストール	［リモート］を選択してリモートローダサービス用にドライバを設定するか、または［ローカル］を選択して、ローカル用にドライバを設定します。
リモートホスト名とポート	リモートローダサービスがインストールされてこのドライバ用に実行しているホストの名前または IP アドレスとポート番号を指定します。デフォルトのポートは 8090 です。
ドライバパスワード	ドライバオブジェクトパスワードは、リモートローダがメタディレクトリサーバに対して自身の認証を求めるときに使用されます。ドライバオブジェクトパスワードには、Identity Manager リモートローダのドライバオブジェクトパスワードと同じパスワードを指定する必要があります。

フィールド	説明
リモートパスワード	このパスワードは、リモートローダ環境設定でのみ使用されます。このパスワードを使用することで、リモートローダがメタディレクトリエンジンに対して自身を認証できるようになります。 リモートローダインスタンスへのアクセスを制御するために、リモートローダのパスワードが使用されます。リモートローダパスワードには、Identity Manager リモートローダのリモートローダパスワードと同じパスワードを指定する必要があります。
パスワードの障害を通知するユーザ	パスワードのエラー時に、指定したサーバに電子メール通知を送信します。
エンタイトルメントの有効化	[はい] または [いいえ] を選択します。これは設計段階で決定しなければならないため、エンタイトルメントを十分に理解した上で使用するかどうかを選択する必要があります。 エンタイトルメントについては、『Novell Identity Manager 3.0 管理ガイド』の「エンタイトルメントの作成と使用」を参照してください。

Identity Manager の Designer を使用したインポート

LDAP ドライバの基本的なドライバ環境設定ファイルをインポートするには、Identity Manager の Designer を使用できます。この基本的なファイルを使用して、ドライバを正しく機能させるために必要なオブジェクトやポリシーを作成および設定します。

次の手順は、サンプル環境設定ファイルをインポートする方法の 1 つを示しています。

1. Designer でプロジェクトを開きます。
2. モデラーで、[ドライバセット] オブジェクトを右クリックして、[Add Connected Application (接続アプリケーションの追加)] を選択します。
3. ドロップダウンリストから、[LDAP.xml] を選択して、[実行] をクリックします。
4. [Perform Prompt Validation (プロンプト検証の実行)] ウィンドウで、[はい] をクリックします。
5. フィールドに入力してドライバを設定します。

   環境に特有の情報を指定します。設定については、23 ページの 「iManager を使用したインポート」の表を参照してください。
6. パラメータを指定したら、[OK] をクリックしてドライバをインポートします。
7. ドライバをカスタマイズおよびテストします。
8. アイデンティティボールトにドライバを展開します。

   『Designer for Identity Manager 3: Administration Guide』の「Deploying a Project to an Identity Vault」を参照してください。

ドライバの起動

環境設定中にデフォルトのデータの場所を変更した場合は、新しい場所が存在することを確認してからドライバを起動します。

1. iManager で、[Identity Manager] > [Identity Manager の概要] の順に選択します。
2. ドライバセット内でドライバを検索します。

3 ドライバアイコンの右上隅にあるドライバステータスインジケータをクリックして、［ドライバの起動］をクリックします。

変更ログが使用可能な場合は、ドライバにより変更ログ内のすべての変更が処理されます。最初の同期を強制的に実行するには、26 ページの 「データの移行と再同期化」を参照してください。

データの移行と再同期化

Identity Manager では、データが変化するとデータの同期を行います。すべてのデータを即時に同期する場合は、次のオプションから選択できます。

- **eDirectory** からのデータの移行 **:** アイデンティティボールトから LDAP サーバに移行するコンテナまたはオブジェクトを選択できます。オブジェクトを移行すると、メタディレクトリエンジンによって、一致、配置、および作成のすべてのポリシーと、購読者フィルタがそのオブジェクトに適用されます。

  注 **:** データをアイデンティティボールトから LDAP ディレクトリに移行する場合は、多量のオブジェクトを移動できるように LDAP サーバの設定変更が必要になる可能性があります。45 ページのセクション 5.1「アイデンティティボールトへのユーザの移行」を参照してください。

- **eDirectory** へのデータの移行 **:** LDAP サーバからアイデンティティボールトにオブジェクトを移行する際に Identity Manager が使用する条件を定義できます。オブジェクトを移行すると、メタディレクトリエンジンによって、一致、配置、および作成のすべてのポリシーと、購読者フィルタがそのオブジェクトに適用されます。オブジェクトは、クラス一覧で指定した順序で、アイデンティティボールトに移行されます。
- 同期 **:** Identity Manager では、購読者クラスフィルタが調べられ、そうしたクラスのすべてのオブジェクトが処理されます。関連付けられたオブジェクトはマージされます。関連付けられていないオブジェクトは追加イベントとして処理されます。

次のオプションのいずれかを使用します。

1 iManager で、［Identity Manager］>［Identity Manager の概要］の順に選択します。
2 LDAP 用 Identity Manager ドライバを含むドライバセットを探し、ドライバのアイコンをダブルクリックします。
3 適切なマイグレーションボタンをクリックします。

ドライバの有効化

インストール後 90 日以内にドライバを有効化 (アクティベーション) します。そうしなければ、ドライバは機能しません。

有効にする方法については、『Identity Manager 3.0 インストールガイド』の「Novell Identity Manager 製品を有効にする」を参照してください。

LDAP ドライバのカスタマイズ

4

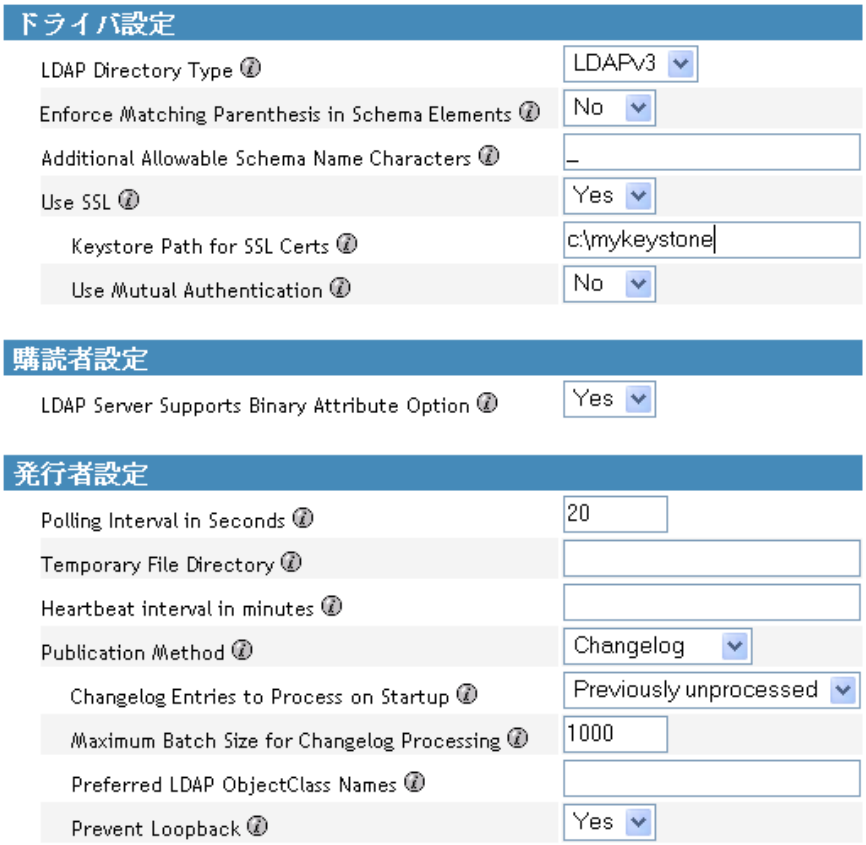
LDAP ドライバには、展開の出発点として使用できるサンプル環境設定が用意されています。ただし、通常、Identity Manager を展開する場合には、これらのサンプルを変更する必要があります。

この節では、次の項目について説明します。

注 **:** データ同期をカスタマイズする場合は、同期対象のオペレーティングシステムおよびアカウントでサポートされている標準や規則の範囲で作業する必要があります。1 つの環境では有効でも、別の環境では無効な文字が含まれているデータは、エラーになります。

4.1 LDAP ディレクトリからアイデンティティボールトへのデータフローの制御

図 *4-1* サンプル環境設定ファイル内の設定

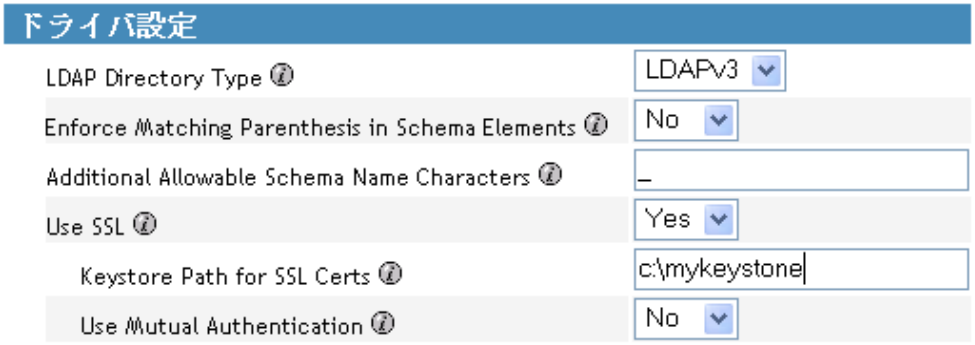


ドライバの動作パラメータを調整することで、ネットワーク環境と協調するようにドライバの動作を調整できます。たとえば、デフォルトの発行者チャネルポーリング間隔が同期に必要な間隔より短いことが判明したとします。この間隔を長くすることで、適切な同期を維持しながら、ネットワークパフォーマンスを改善できる場合があります。

LDAP サーバに変更ログがある場合は、変更ログ発行方式を採用することをお勧めします。変更ログを利用できない場合は、LDAP 検索発行方式を採用します。変更ログ方式が、優先される方式です。

4.1.1 LDAP ドライバ設定

図 *4-2* *LDAP* ドライバ設定

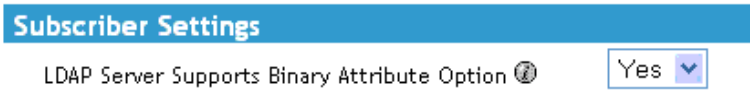


1. iManager で、［Identity Manager］>［Identity Manager の概要］の順にクリックし、ドライバセットを検索します。
2. ドライバセットで、LDAP ドライバアイコンをクリックします。
3. ［ドライバ］ビューで、もう一度 LDAP ドライバアイコンをクリックします。
4. ［ドライバパラメータ］までスクロールします。
5. ［ドライバ設定］セクションで、目的のオプションを選択します。

   設定については、情報アイコン をクリックします。

4.1.2 LDAP 購読者設定

図 *4-3* *LDAP* 購読者設定



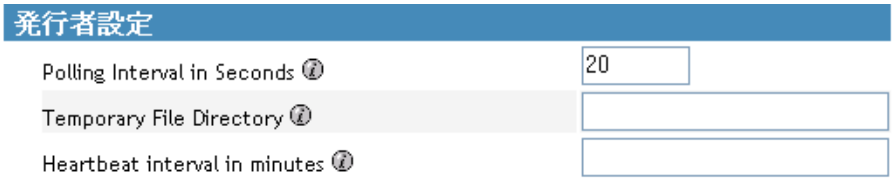
サンプル環境設定ファイルをインポートする場合は、この設定の入力を要求するメッセージは表示されません。ただし、ファイルをインポートした後に設定を変更できます。［購読者設定］セクションで、目的のオプションを選択します。

デフォルトの設定は［はい］です。ほとんどの LDAP サーバでは、RFC 2251 のセクション 4.1.5.1 で定義されているバイナリ属性オプションを使用できます。

このドライバの接続先 LDAP サーバがバイナリ属性オプションをサポートしているかわからない場合は、［はい］を選択します。

4.1.3 LDAP 発行者設定 : 変更ログと LDAP 検索方式

図 *4-4* *LDAP* の共通発行者設定



一部の設定は、変更ログ発行方式と LDAP 検索発行方式の両方に適用されます。また、変更ログ発行方式のみに適用される設定もあります。それ以外の設定は、LDAP 検索発行方式だけに適用されます。

ポーリング間隔 (秒)

ドライバが LDAP サーバの変更ログまたは LDAP 検索方式をチェックする間隔。新たな変更が検出されると、変更はアイデンティティボールトに適用されます。

推奨ポーリング間隔は 120 秒です。

一時ファイルディレクトリ

一時的な状態のファイルを書き込めるローカルファイルシステム (ドライバが実行しているファイルシステム) のディレクトリに値を設定します。パスを指定していない場合、ドライバではデフォルトのドライバパスが使用されます。

表 *4-1* 一時ファイルディレクトリ

プラットフォームまたは環境	デフォルトのディレクトリ
eDirectory	DIB ファイルのディレクトリ
リモートローダ	リモートローダのルートディレクトリ

これらのファイルは、次のような場合に役立ちます。

- ドライバがシャットダウン中でもドライバの整合性を維持する
- 検索対象のデータが広範な場合のメモリ不足を防ぐ

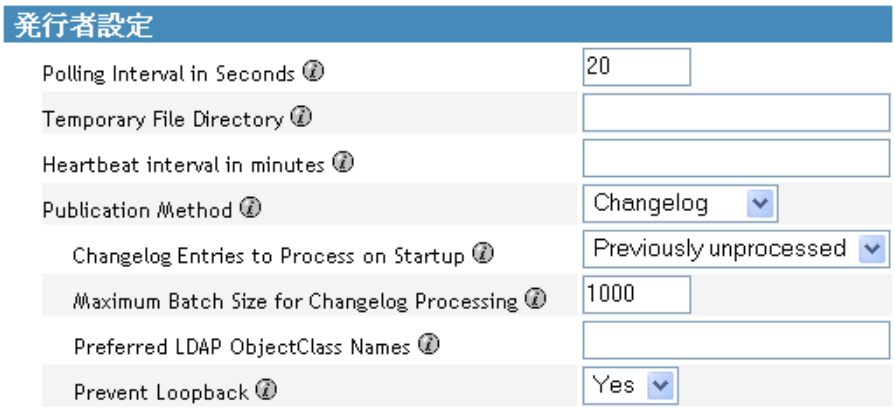
ハートビート間隔 (分)

ハートビートをオンにするには、値を入力します。ハートビートをオフにするには、このフィールドを空白のままにします。

ドライバのハートビートについては、『Novell Identity Manager 3.0 管理ガイド』の「ドライバのハートビートの追加」を参照してください。

4.1.4 LDAP 発行者設定：変更ログ方式のみ

図 *4-5* *LDAP* 発行者チャネルでの変更ログ設定



起動時に処理する変更ログエントリ

このパラメータでは、起動時に処理するエントリを指定します。

- すべて : 変更ログで検出されたすべての変更が、発行者の処理対象になります。この操作は、すべての変更が処理されるまで続行されます。ポーリング間隔に応じて、新たな変更は発行者により処理されます。
- なし : ドライバの実行開始時点で既存のエントリは、発行者の処理対象外になります。ポーリング間隔に応じて、新たな変更は発行者により処理されます。
- 前回は未処理 : この設定はデフォルトです。初めてドライバが実行された場合、ドライバは、新たなすべての変更を処理するために、初回実行時の「すべて」のように動作します。

  ドライバが前に実行されたことがある場合は、この設定では、最後にドライバが実行したとき以降の新たな変更だけが、発行者により処理されます。その後は、ドライバによって、ポーリング間隔に従って新たな変更が処理されます。

変更ログ方式を利用する場合は、ドライバでバッチサイズとループバックの回避の設定が検索されます。

変更ログ処理の最大バッチサイズ

発行者チャネルで LDAP 変更ログの新しいエントリを処理する場合は、このサイズのバッチのエントリが発行者から要求されます。変更ログのエントリ数がこの値より少ない場合は、そのすべてが直ちに処理されます。変更ログのエントリ数がこの値より多い場合は、エントリはこのサイズのバッチで順次処理されます。

優先される LDAP オブジェクトクラス名

［優先される LDAP オブジェクトクラス名］の設定は、発行者チャネルでの優先オブジェクトクラスを指定できるオプションのドライバパラメータです。

Identity Manager では、1 つのオブジェクトクラスを使用して該当するオブジェクトを指定する必要があります。ただし、多くの LDAP サーバとアプリケーションでは、1 つのオブ

ジェクトに対し、複数のオブジェクトクラスを一覧表示できます。デフォルトでは、LDAP 用 Identity Manager ドライバは、LDAP サーバまたはアプリケーションで追加、削除、または変更されたオブジェクトを検出すると、イベントをメタディレクトリエンジンに送信し、スキーマ定義の最も多くのレベルを継承したオブジェクトクラスを使用してそのイベントを特定します。

たとえば、inetorgperson、organizationalperson、person、および top の各オブジェクトクラスで特定されるユーザオブジェクトが LDAP に存在します。inetorgperson は、スキーマの最も多くのレベルを継承しています (top、person、organizationalperson の順で段階的に継承します)。デフォルトでは、ドライバはメタディレクトリエンジンにレポートするオブジェクトクラスとして inetorgperson を使用します。

ドライバのデフォルトの動作を変更する場合は、preferredObjectClasses という名前のオプションのドライバ発行者パラメータを追加できます。このパラメータの値には、1 つの LDAP オブジェクトクラスまたは複数の LDAP オブジェクトクラスをスペースで区切ったリストのいずれかを指定できます。

このパラメータが存在する場合は、LDAP 用 Identity Manager ドライバにより、発行者チャネルに存在する各オブジェクトが調べられ、リスト内にいずれかのオブジェクトクラスが含まれているかどうか確認されます。オブジェクトクラスは、preferredObjectClasses パラメータに記載されている順に検索されます。一覧表示されたオブジェクトクラスのいずれかが、LDAP オブジェクトの objectclass 属性のいずれかの値と一致すると、そのクラスはメタディレクトリエンジンにレポートするクラスとしてこのドライバで使用されます。オブジェクトクラスのいずれとも一致しない場合、このドライバがプライマリオブジェクトクラスをレポートするためのデフォルトの動作になります。

ループバックの回避

［ループバックの回避］のパラメータは、変更ログ発行方式でのみ使用されます。LDAP 検索方式では、メタディレクトリエンジンに組み込まれているループバック回避しか行われません。

発行者チャネルのデフォルトの動作では、購読者チャネルで加える変更の送信が回避されます。発行者チャネルでは購読者チャネルの変更を検出するために、creatorsName 属性または modifiersName 属性で LDAP 変更ログが調べられ、変更を加えた認証済みエントリがこのドライバの LDAP サーバに対する認証に使用されるエントリと同じかどうかを確認します。エントリが同じ場合、発行者チャネルでは、この変更がドライバの購読者チャネルで行われたと見なされ、変更は同期されません。

サンプルシナリオとして、購読者チャネルがこのドライバ向けに設定されていなくても、変更を行う他のプロセスと同じ DN およびパスワードを使用できるようにします。

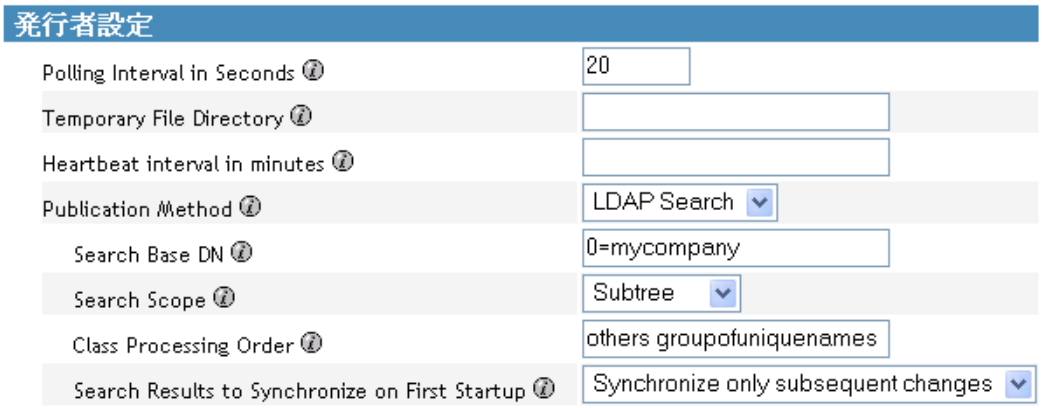
このタイプのループバックを確実に発生させるには、ドライバパラメータを次のように編集します。

1. iManager で、［Identity Manager 管理］>［Identity Manager の概要］の順に選択します。
2. ドライバセット内でドライバを検索します。
3. ドライバをクリックしてドライバの概要ページを開き、もう一度ドライバをクリックして［オブジェクトの変更］ページを開きます。
4. ［発行者設定］セクションまでスクロールし、［ループバックの回避］を［いいえ］に設定します。

5 ［OK］をクリックし、［適用］をクリックして、このパラメータが有効になるようにドライバを再起動します。

4.1.5 LDAP 発行者設定 : LDAP 検索方式のみ

図 *4-6* *LDAP* 発行者チャネルでの *LDAP* 検索の設定



従来、LDAP ドライバでは、変更ログを読み込むだけで LDAP サーバでの変更を検出できていました。ただし、変更ログは実際のところ LDAP 標準ではないため、一部のサーバでは変更ログメカニズムが採用されていません。変更ログが存在しない場合、従来の LDAP ドライバではこのような LDAP サーバに関するデータをアイデンティティボールトに発行できませんでした。

しかし、LDAP 検索発行方式では変更ログを必要としません。この方式では、標準の LDAP 検索を使用した上で、ある検索間隔から次の間隔までの結果を比較し、変更を検出します。

LDAP 検索発行方式は、従来の変更ログ発行方式の代替方式として利用できます。LDAP 用 Identity Manager ドライバは、どちらの方式もサポートしています。ただし、変更ログ方式はパフォーマンスの面で優れており、変更ログが使用可能な場合は優先される方式です。

変更ログを使用できない場合は、次のパラメータを設定します。

- 33 ページの 「ベース DN の検索」
- 34 ページの 「検索スコープ (1- サブツリー、2- レベル、3- ベース)」
- 34 ページの 「クラスの処理順序」
- 34 ページの 「初回起動時の検索結果の同期」

ベース DN の検索

変更ログが使用できない環境で発行者チャネルを使用する場合に必要なパラメータ。このパラメータにはポーリング検索を開始するコンテナの LDAP 識別名 (DN) (ou=people、o=company など) を設定します。

変更ログを使用するには、このパラメータを空白のままにします。

検索スコープ (1- サブツリー、2- レベル、3- ベース)

ポーリング検索の深さを指定します。このパラメータのデフォルトでは、検索ベース DN で指定したサブツリー全体が検索対象になります。

変更ログが使用可能でない場合にこのパラメータを設定します。

クラスの処理順序

参照属性に問題がある場合に特定のイベントを並び替えるために発行者チャネルで使用されるオプションのパラメータ。このパラメータの値は、LDAP サーバからのクラス名をスペースで区切った形式のリストです。たとえば、確実に新規ユーザを作成してからグループに追加するには、interorgperson を必ず groupofuniquenames より前に指定します。

LDAP 用 Identity Manager ドライバでは、明示的に示されたクラス以外のすべてのクラスを表す特別なクラス名「others」が定義されています。

このパラメータのデフォルト値は「other groupofuniquenames」です。

変更ログを使用できない場合にこのパラメータを使用します。

初回起動時の検索結果の同期

LDAP ドライバが初めて起動したときに、定義済みの LDAP 検索が実行されます。［初回起動時に検索結果を同期］設定で、最初の検索結果を同期するか、それ以降の変更だけを同期するかを定義します。

［初回起動時に検索結果を同期］オプションは、［発行方法］パラメータが［LDAP 検索］に設定されている場合にのみ表示されます。環境設定ファイルをインポートする場合は、この設定の入力を促すメッセージは表示されません。ただし、ファイルをインポートした後に設定を変更できます。

1. iManager で、［Identity Manager］>［Identity Manager の概要］の順にクリックし、ドライバセットを検索します。
2. ドライバセットで、LDAP ドライバアイコンをクリックします。
3. ドライバビューで、もう一度 LDAP ドライバアイコンをクリックします。
4. ［ドライバパラメータ］までスクロールします。
5. ［発行者設定］セクションで、目的のオプションを選択します。

   デフォルトの設定は、［この後の変更分のみを同期する］です。

4.2 データ同期の設定

4.2.1 同期されるオブジェクトの決定

Identity Manager では、発行者チャネルと購読者チャネルのフィルタを使用して、同期されるオブジェクトの制御および、オブジェクトの信頼されるデータソースの定義が行われます。

8 ページの 「フィルタ」ではデフォルトのフィルタを参照できます。デフォルトを変更するには、次の手順に従ってください。

発行者フィルタと購読者フィルタの編集

1. iManager で、［Identity Manager］>［Identity Manager の概要］の順に選択します。
2. ドライバセットからドライバを選択します。
3. ドライバをクリックして［Identity Manager ドライバの概要］ページを開きます。
4. 発行者フィルタまたは購読者フィルタのアイコンをクリックして、適切に変更します。

   発行者フィルタには、アイデンティティボールトの必須属性を含める必要があります。購読者フィルタには、LDAP サーバの必須属性を含める必要があります。

   フィルタで選択したすべてのオブジェクトおよび属性に対し、マッピングポリシーでは対応するエントリが必要です。ただし、クラス名または属性名が両方のディレクトリで同じ場合は除きます。属性をマッピングする前に、対応する属性が実際にターゲットディレクトリに存在していることを確認してください。

4.2.2 スキーママッピングの定義

LDAP サーバごとに、用意されているスキーマは異なります。ドライバは初めて起動されたときに特定のスキーマのサーバを照会します。

管理者は、eDirectory 属性と LDAP サーバ属性の特性に精通している必要があります。このドライバでは、すべての LDAP 属性タイプ (cis、ces、tel、dn、int、bin) が処理されます。また、eDirectory の Fax 番号も処理されます。

属性をマッピングする場合は、次のガイドラインに従ってください。

- クラス名または属性名が両方のディレクトリで同じ場合を除き、購読者ポリシーと発行者ポリシーで指定したすべてのクラスと属性がマッピングポリシーでマッピングされていることを確認してください。
- eDirectory™ の属性を LDAP サーバ属性にマッピングする前に、LDAP サーバ属性が実際に存在していることを確認してください。たとえば、ユーザオブジェクトのフルネーム属性がアイデンティティボールトに定義されていても、Netscape の inetOrgPerson オブジェクトに fullname は存在しません。
- 属性は常に同じタイプの属性にマッピングしてください。たとえば、文字列属性は文字列属性に、オクテット属性はバイナリ属性に、電話番号属性は電話番号属性にマッピングします。
- 複数値属性には複数値属性をマッピングしてください。

このドライバでは、さまざまな属性タイプ間のデータ変換や複数値から単一値属性への変換は行われません。また、このドライバでは、Fax 番号と住所以外の構造属性も認識されません。

Identity Manager は、発行者からの入力を受け入れる次のような柔軟性の高い構文をサポートしています。

- 非構造 / 非オクテット構文の受け入れ . Identity Manager では、実際のデータを強制的に適切なタイプにすることができる限り、他の非構造 / 非オクテット構文向けのあらゆる非構造 / 非オクテット構文を受け入れます。つまり、アイデンティティボールトで数値が検索される場合、実際のデータは数値でなければなりません。
- データの強制オクテット変換 . Identity Manager でオクテットデータを想定していたときに別の非オクテット / 非構造タイプが得られた場合、Identity Manager では、データを強制的にオクテットにするために文字列値が UTF-8 に直列化されます。
- データの強制文字列変換 . Identity Manager にオクテットデータが渡されたときに別の非構造タイプが想定されていた場合、Identity Manager では、データを強制的に文字列にするために Base64 データがデコードされます。次に Identity Manager では、その結果が UTF-8 エンコード文字列 (有効な UTF-8 文字列でない場合は、プラットフォームのデフォルトの文字エンコード) と解釈され、「非構造 / 非オクテット構文の受け入れ」と同じルールが適用されます。
- **faxNumber** . faxNumber の場合は、非構造タイプが渡されると、ファックス番号の電話番号部分を取得するために「非構造 / 非オクテット構文の受け入れ」や「データの強制文字列変換」がデータに適用されます。その他のフィールドは、デフォルトに設定されます。
- 状態。状態。状態の場合、False、No、F、N (大文字または小文字)、0、および "" (空の文字列) は False と解釈され、それ以外の値は True と解釈されます。

スキーママッピングポリシーを設定する

1. iManager で、［Identity Manager］>［Identity Manager の概要］の順にクリックします。
2. ドライバセットからドライバを選択します。
3. ドライバをクリックして［Identity Manager ドライバの概要］ページを開きます。
4. 発行者チャネルまたは購読者チャネルのスキーママッピングアイコンをクリックします。
5. 設定に合わせてポリシーを編集します。

4.2.3 Netscape でのオブジェクト配置の定義

Netscape Directory Server のオブジェクトについては、Netscape の命名ルールに従うことをお勧めします。ここで命名ルールについて簡単に説明します。

このディレクトリには、人物を表すエントリが格納されます。この人物を表すエントリには、名前を付ける必要があります。つまり、これらのエントリごとに相対識別名 (RDN) を決定する必要があります。DN には、固有で容易に認識できる変わらない値を指定してください。uid 属性を使用して、人物に関連付ける固有の値を指定することをお勧めします。人物エントリの DN の例は、次のとおりです。

uid=jsmith,o=novell

このディレクトリには、人物以外の多くのオブジェクト (グループ、デバイス、サーバ、ネットワーク情報、その他のデータなど) を表すエントリも格納されます。RDN で cn 属性を使用することをお勧めします。したがって、グループエントリに名前を付ける場合は、次のようにします。

cn=administrators,ou=groups,o=novell

このディレクトリには、分岐点やコンテナも格納されます。分岐点を指定するために使用する属性を決定する必要があります。属性名は意味を表すため、エントリのタイプを表す属性名を使用してください。Netscape では属性を次のように定義するよう推奨しています。

表 *4-2* *Netscape* 推奨の属性

属性名	定義
c	国名
o	組織名
ou	部門
st	状態
l	地域
dc	ドメインコンポーネント

購読者配置ポリシーでクラス名の名前付け属性を指定します。次に示すのは、User クラス名の例です。<placement> ステートメントは、uid を名前付け属性として使用することを指定しています。

```
<placement-rule> <match-class class-name="User"/> <match-path
prefix="\Novell-Tree\Novell\Users"/> <placement>uid=<copy-name/
>,ou=People,o=Netscape</ placement> </placement-rule>
```

次の購読者配置では、ou をクラス名 Organizational Unit の名前付け属性として使用することを指定しています。

```
<placement-rule> <match-class class-name="Organizational Unit"/>
<match-path prefix="\Novell-Tree\Novell\Users"/> <placement>ou=<copy-
name/>,ou=People,o=Netscape</placement> </placement-rule>
```

配置ポリシーの設定

1. iManager で、［Identity Manager］>［Identity Manager の概要］の順にクリックします。
2. ドライバセットからドライバを選択します。
3. ドライバをクリックして［Identity Manager ドライバの概要］ページを開きます。
4. 発行者配置ポリシーまたは購読者配置ポリシーのアイコンをクリックして、適宜、変更します。

4.2.4 eDirectory グループと Netscape の連携

グループ属性はアイデンティティボールトと Netscape Directory Server では異なるため、このドライバの特別な処理が必要です。発行者チャネルでの特別な処理は、ドライバでクラス名 *groupofuniquenames* の属性 *uniquemember* を参照する際に行われます。

このドライバで、eDirectory グループに同等権利保有者属性も設定されます。同等権利保有者属性は、発行者フィルタに含まれている必要があります。eDirectory 属性名が使用されるため、スキーママッピングポリシーに同等権利保有者属性含んでいる必要はありません。Netscape Directory Server には、同等の属性名はありません。購読者チャネルでは、特別な処理は不要です。

4.3 SSL 接続の設定

このドライバは、LDAP プロトコルを使用して LDAP サーバと通信します。ほとんどの LDAP サーバでは、暗号化されていない (クリアテキスト) 接続を許可しています。正しく設定されていれば、一部の LDAP サーバでは SSL 暗号化接続が許可されます。SSL 接続では、公開鍵と秘密鍵のペアを使用して TCP/IP ソケットのすべてのトラフィックが暗号化されます。実際の LDAP プロトコルは変わりませんが、通信チャネルでは暗号化が実行されます。

SSL 接続を有効にする手順は、LDAP サーバによってわずかに異なります。このドキュメントでは、Netscape Directory Server 4.12 を使用している場合の SSL 接続を有効にするプロセスについて説明します。

- 38 ページの 「ステップ 1: サーバ証明書の生成」
- 39 ページの 「ステップ 2: 証明書要求の送信」
- 40 ページの 「ステップ 3: 証明書のインストール」
- 40 ページの 「ステップ 4: Netscape Directory Server 4.12 での SSL の有効化」
- 41 ページの 「ステップ 5: eDirectory ツリーからのルート認証局証明書のエクスポート」
- 41 ページの 「ステップ 6: ルート認証局証明書のインポート」
- 42 ページの 「ステップ 7: ドライバ設定の調整」

別の LDAP サーバを使用している場合でも、手順は同様です。

4.3.1 ステップ 1: サーバ証明書の生成

最初にサーバ証明書をインストールする必要があります。LDAP サーバ自体で証明書を生成できますが、証明書には、サーバが信頼する CA の署名が必要です。証明書の署名を取得する 1 つの方法として、アイデンティティボールトに付属する CA を使用する方法があります。

証明書要求を生成するには、次のようにします。

1. Netscape Console のナビゲーションツリーで、このドライバの通信先サーバを選択します。
2. ［Open Server (サーバを開く)］をクリックします。
3. ［Tasks (タスク)］>［Certificate Setup Wizard (証明書セットアップウィザード)］の順にクリックします。
4. 証明書を要求するための情報を設定します。

   ホストシステムにすでにインストールされている証明書またはトークンに応じて、次のフィールドの一部または全部が表示されます。

Select a Token (Cryptographic Device) (トークンの選択 **(** 暗号化デバイス **)):**［Internal (Software) (内部 (ソフトウェア))］を選択します。

［**Is the Server Certificate Already Requested and Ready to Install? (** サーバ証明書をすでに要求し、インストールの準備は整っていますか **?)**］［No（いいえ）］を選択します。

このホストの信頼できるデータベースが存在していない場合は、データベースが生成されます。

信頼できるデータベースとは、ローカルホストにインストールされた鍵ペアと証明書データベースのことです。内部のトークンを使用する場合の信頼できるデータベースとは、鍵と証明書をインストールするデータベースのことです。

5 パスワードを入力して確認します。

パスワードは 8 文字以上で、少なくとも 1 文字は数値にする必要があります。このパスワードにより、作成している新規鍵データベースに安全にアクセスできるようになります。

6 引き続き要求されるとおりに情報を設定して、［Next (次へ)］をクリックします。

7 信頼できるデータベースが作成されたら、［Next (次へ)］をクリックします。

8 要求された情報を入力して、［Next (次へ)］をクリックします。

9 以前に選択したトークンのパスワードを入力して、［Next (次へ)］をクリックします。

証明書セットアップウィザードで、サーバの証明書要求が生成されます。要求ページが表示されたら、証明書要求を認証局に送信できます。

4.3.2 ステップ 2: 証明書要求の送信

1 サーバ証明書要求をメモ帳または別のテキストエディタにコピーします。

2 ファイルを csr.txt として保存します。

証明書要求の電子メールは、次のような形式になるはずです。

```
-----BEGIN NEW CERTIFICATE REQUEST-----

        .

        .

        . -----END NEW CERTIFICATE REQUEST----
```

3 iManager で、［Novell 証明書サーバ］>［証明書の発行］の順にクリックします。

4 ［ファイル名］フィールドで、csr.txt を参照して、［次へ］をクリックします。

5 ［Organizational Certificate Authority (組織の認証局)］を選択します。

6 キータイプとして SSL を指定し、［次へ］をクリックします。

7 証明書パラメータを指定し、［次へ］をクリックして、［終了］をクリックします。

8 ローカルディスクまたはフロッピーディスクに Base64 形式の証明書を cert.b64 という名前で保存します。

4.3.3 ステップ 3: 証明書のインストール

1. Netscape Console のナビゲーションツリーで、このドライバの接続先サーバを選択します。
2. ［Open (開く)］をクリックします。
3. ［Tasks (タスク)］>［Certificate Setup Wizard (証明書セットアップウィザード)］の順にクリックします。
4. ウィザードを起動して、証明書をインストールする準備ができたことを示します。
5. メッセージが表示されたら、次の情報を指定します。

   Select a Token (Cryptographic Device) (トークンの選択 **(** 暗号化デバイス **)):**［Internal (Software) (内部 (ソフトウェア))］を選択します。

   ［**Is the Server Certificate Already Requested and Ready to Install? (** サーバ証明書をすでに要求し、インストールの準備は整っていますか **?)**］［Yes (はい)］を選択します。
6. ［Next (次へ)］をクリックします。
7. ［Install Certificate For (証明書のインストール先)］フィールドで、［This Server (このサーバ)］を選択します。
8. ［Password (パスワード)］フィールドで、信頼できるデータベースの設定に使用するパスワードを入力して、［Next (次へ)］をクリックします。
9. ［Certificate Is Located in This File (証明書を含むファイル)］フィールドで、証明書への絶対パス (A:\CERT.B64 など) を入力します。
10. 証明書が生成されたら、［Add (追加)］をクリックします。
11. 証明書が正しくインストールされたら、［Done (完了)］をクリックします。

4.3.4 ステップ 4: Netscape Directory Server 4.12 での SSL の有効化

証明書をインストールした後に、次の操作を実行して SSL を有効にします。

1. Netscape Console のナビゲーションツリーで、SSL 暗号化を使用するサーバを選択します。
2. ［Open (開く)］>［Configuration (構成)］>［Encryption (暗号化)］の順にクリックします。
3. 次の情報を入力します。

   Enable SSL (SSL の有効化 **):** このオプションを選択します。

   Cipher Family (暗号ファミリー **):**［RSA］を選択します。

   Token to Use (使用するトークン **):**［Internal (Software) (内部 (ソフトウェア))］を選択します。

   Certificate to Use (使用する証明書 **):**［Server-Cert］を選択します。

   Client Authentication (クライアント認証 **):** このドライバではクライアント認証をサポートしていないため、［Allow Client Authentication (クライアント認証を許可する)］を選択します。
4. ［Save (保存)］をクリックします。
5. ［Tasks (タスク)］をクリックし、サーバを再起動して変更を有効にします。

4.3.5 ステップ 5: eDirectory ツリーからのルート認証局証明書のエクスポート

1 iManager で、［eDirectory 管理］>［オブジェクトの変更］の順に選択します。
2 認証局 (CA) オブジェクトを参照して、［OK］をクリックします。
3 ドロップダウンリストから［証明書］を選択します。
4 ［エクスポート］をクリックします。
5 「Do you want to export the private key with the certificate? (証明書付きプライベートキーをエクスポートしますか ?)」というメッセージが表示されたら、［いいえ］をクリックします。
6 ［次へ］をクリックします。
7 ［ファイル名］フィールドは、ファイル名 (PublicKeyCert など) を入力して、形式として［Base64］を選択します。
8 ［エクスポート］をクリックします。

4.3.6 ステップ 6: ルート認証局証明書のインポート

LDAP サーバの信頼できるデータベースおよびクライアントの証明書ストアに、ルート認証局証明書をインポートする必要があります。

LDAP サーバの信頼できるデータベースのインポート

LDAP サーバの信頼できるデータベースに、ルート認証局証明書をインポートする必要があります。サーバ証明書はアイデンティティボールトの CA によって署名されているため、アイデンティティボールト CA を信頼するよう信頼できるデータベースを設定する必要があります。

1 Netscape Console で、［Tasks (タスク)］>［Certificate Setup Wizard (証明書セットアップウィザード)］>［Next (次へ)］の順にクリックします。
2 ［Select a Token (トークンの選択)］で、デフォルトの［Internal (Software) (内部 (ソフトウェア))］をそのまま使用します。
3 ［Is the Server Certificate Already Requested and Ready to Install? (サーバ証明書をすでに要求し、インストールの準備は整っていますか ?)］で、［Yes (はい)］を選択します。
4 ［Next (次へ)］を 2 回クリックします。
5 ［Install Certificate For (証明書のインストール先)］ダイアログボックスで、［Trusted Certificate Authority (信頼された認証局)］を選択します。
6 ［Next (次へ)］をクリックします。
7 ［Certificate Is Located in This File (証明書を含むファイル)］を選択して、ルート認証局証明書が含まれている .b64 ファイルへのフルパスを入力します。
8 ［Next (次へ)］をクリックします。
9 画面に表示される情報を確認して、［Add (追加)］をクリックします。
10 ［Done (完了)］をクリックします。

クライアントの証明書ストアへのインポート

このドライバで使用できる証明書ストア (別名 : キーストア) にルート認証局証明書をインポートする必要があります。

1 rt.jar にある KeyTool クラスを使用します。

公開鍵証明書がフロッピーディスクに PublicKeyCert.b64 として保存されており、それを現在のディレクトリの .keystore という名前の新しい証明書ストアファイルにインポートする場合は、コマンドラインで次のように入力します。

```
java sun.security.tools.KeyTool -import -alias TrustedRoot -file
a:\PublicKeyCert.b64

-keystore .keystore -storepass keystorepass
```

2 この証明書を信頼するよう促すメッセージが表示された場合は、［はい］を選択して、［Enter (入力)］をクリックします。

3 アイデンティティボールトファイルを格納しているファイルシステムの任意のディレクトリに .keystore ファイルをコピーします。

4 iManager で、［Identity Manager］>［Identity Manager の概要］の順に選択します。

5 ドライバを検索します。

6 LDAP ドライバオブジェクトをクリックし、［Identity Manager ドライバの概要］ページでもう一度そのオブジェクトをクリックします。

7 ［キーストアパス］パラメータで、.keystore ファイルへの完全なパスを入力します。

4.3.7 ステップ 7: ドライバ設定の調整

次の表は、サンプル環境設定でのドライバの設定とそのデフォルト値を示しています。

表 *4-3* ドライバ設定とデフォルト値

パラメータ	サンプルの環境設定値	説明
Use SSL for LDAP Connections (LDAP 接続に SSL を使用)	いいえ	このパラメータの値には、［はい］または［いいえ］を指定します。このパラメータは、LDAP サーバとの通信時に SSL 接続を使用するかどうかを表示します。SSL を使用するには、LDAP サーバも正しく設定する必要があります。 詳細については、38 ページの 「SSL 接続の設定」を参照してください。
SSL ポート	636	このパラメータは、［Use SSL for LDAP Connections (LDAP 接続に SSL を使用)］が［はい］に設定されていない限り無視されます。このパラメータでは、LDAP サーバがセキュリティ保護された接続に使用するポートを指定します。

パラメータ	サンプルの環境設定値	説明
SSL 証明書用のキーストアパス	[空白]	［Use SSL for LDAP Connections (LDAP 接続に SSL を使用)］が［はい］に設定されている場合、このパラメータ値には、サーバ証明書に署名した認証局 (CA) のルート認証局証明書が格納されているキーストアファイルへの完全なパスを指定する必要があります。 キーストアファイルの作成に関する詳細については、42 ページの 「クライアントの証明書ストアへのインポート」を参照してください。

トラブルシューティング

5

5.1 アイデンティティボールトへのユーザの移行

一部の LDAP サーバには、LDAP クエリが返せるエントリ数を制限する設定があります。たとえば、iPlanet Directory Server 5.1 のデフォルトの制限は、2000 オブジェクトです。

LDAP からアイデンティティボールトにユーザデータを移行する場合は、ドライバでサーバへの LDAP クエリが作成され、条件 (objectclass=User など) に一致するオブジェクトが返されます。

LDAP クエリに対し、返せるエントリ数の上限を設定すると、Identity Manager ドライバで他の機能が正常に実行していても、移行が完了する前に停止する原因になる可能性があります。

この問題を解決するには、制限を変更します。たとえば、iPlanet で次の操作を実行します。

1 ［Configuration (構成)］タブを開いて、［Database (データベース)］の設定を選択します。

2 LDBM プラグインタブのルックスルー制限をデフォルトの 5000 から適切な数にします。

この値は、クエリの実行中にクエリで参照できるレコード数です。

3 ［Configuration (構成)］タブを開いて、［Directory Server Settings (ディレクトリサーバの設定)］を選択します。次に、［Performance (パフォーマンス)］タブを選択して、移行に必要なユーザアカウント数に従ってサイズ制限を大きくします。

この値は、クエリが返せる実際のレコード数です。

これらの設定を調整すれば、移行は正しく完了するはずです。

5.2 OutOfMemoryError

LDAP 検索方式で、このドライバが java.lang.OutOfMemoryError でシャットダウンする場合は、次のようにしてください。

1 DHOST_JVM_INITIAL_HEAP と DHOST_JVM_MAX_HEAP の環境変数を設定するか、その値よりも大きくします。

2 ドライバを再起動します。

3 これらの変数により十分なメモリが確実に提供されるように、ドライバを監視します。

詳細については、TID 10062098 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10062098.htm) を参照してください。

5.3 LDAP v3 の互換性

Identity Manager 対応の LDAP ドライバは、LDAP v3 互換のほとんどの LDAP サーバで機能します。このドライバは、LDAP の RFC 2251 仕様に従って作成されています。RFC 2251 の要件を満たしていない一部の LDAP サーバとの互換性を高めるため、LDAP ドライバに対応策を施しました。

互換性の問題として、サーバで最大 2,147,483,647(4 バイトを使用した整数値) のメッセージ ID 値を許可する、RFC 2251 の要件があります。この問題は無視できません。また、対応策を施すこともできません。

Oracle Internet Directory version 2.1.1.0.0 (Oracle 8i の一部) では、最大 32,767 (2 バイトを使用した整数値) のメッセージ ID 値しか許可されません。したがって、このディレクトリは、Identity Manager 対応の LDAP ドライバでは正しく機能できません。

Oracle Internet Directory との互換性が必要場合は、バージョン 9.2.0.1.0 (Oracle 9i に付属) にアップグレードすることをお勧めします。

5.4 よくある質問とその回答

質問 : LDAP 検索方式では、毎回すべてを取得しますか ? または、最後のポーリング以降の更新だけを取得しますか ?

回答 : LDAP 検索方式では、あるポーリングから次のポーリングまでの更新が同期されます。

質問 : LDAP 検索方式を使用するか、変更ログ方式を使用するかを選択できる場合は、LDAP 検索方式を使用した方がよいのでしょうか ?

回答 : 変更ログ方式の長所は、そのパフォーマンスにあります。変更ログ方式を採用してください。変更ログ方式が、優先される方式です。

最新のマニュアル

A

この節には、LDAP 用 Identity Manager ドライバについての新規および更新情報が含まれています。

マニュアルは、Web 上に HTML と PDF の 2 つの形式で用意されています。HTML および PDF のマニュアルはいずれもこの節に挙げるマニュアルの変更を反映した最新の状態になっています。

使用中の PDF マニュアルが最新かどうかを確認する必要がある場合は、PDF ファイルの発行日を確認します。日付はタイトルページの次の「保証と著作権」の節にあります。

新規マニュアルまたは更新されたマニュアルは、次の日付に発行されました。

- 47 ページのセクション A.1「2006 年 5 月 25 日」

A.1 2006 年 5 月 25 日

表 *A-1* *2006 年 5 月 8 日に行われた変更*

場所	変更内容
5 ページのセクション 1.1「新機能」	このトピックに 2 つの項目を追加しました。
5 ページのセクション 1.2「今後の更新に関する情報」	このトピックを追加しました。
13 ページのセクション 3.1「計画段階の考慮事項」	LDAP v3 の互換性の問題と RFC 2251 の仕様に関する段落を追加しました。
28 ページのセクション 4.1「LDAP ディレクトリからアイデンティティボールトへのデータフローの制御」	変更ログ方式と LDAP 検索方式を簡単に実装できるように、この節を再構成しました。
29 ページの 「LDAP 購読者設定」	新しい購読者パラメータに関する情報を追加しました。
34 ページの 「初回起動時の検索結果の同期」	この新しい発行者パラメータに関する情報を追加しました。
46 ページのセクション 5.3「LDAP v3 の互換性」	この節を追加しました。
46 ページのセクション 5.4「よくある質問とその回答」	この節を追加しました。