Novell Active Directory* 用の Identity Manager ドライバ

3.1

www.novell.com

実装ガイド

2006 年 4 月 28 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、いかなる表示も行いません。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行いません。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掲載されている企業、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

ConsoleOne は、米国 Novell, Inc. の米国およびその他の国々における登録商標です。

DirXML は、米国 Novell, Inc. の米国およびその他の国々における登録商標です。

eDirectory は、米国 Novell, Inc. の商標です。

NCP および NetWare Core Protocol は、米国 Novell, Inc. の登録商標です。

NDS および Novell Directory Services は、米国 Novell, Inc. の米国およびその他の国々における登録商標です。

NetWare は、米国 Novell, Inc. の米国およびその他の国々における登録商標です。

Novell は、米国 Novell, Inc. の米国およびその他の国々における登録商標です。

Novell Certificate Server は、米国 Novell, Inc. の商標です。

Novell Client は、米国 Novell, Inc. の登録商標です。

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、Active Directory 用の Identity Manager ドライバのインストール、設定、および管理の方法について説明します。

対象読者

このガイドは、NT ドメイン用の Identity Manager ドライバを実装する Active Directory 管理者、Novell® eDirectory™ 管理者など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のバージョンについては、ドライバのマニュアルの Web サイト (http://www.novell.com/documentation/lg/dirxmldrivers) を参照してください。

その他のマニュアル

Identity Manager および他の Identity Manager ドライバの使用に関するマニュアルについては、Identity Manager のマニュアルの Web サイト (http://www.novell.com/documentation/lg/dirxml20) を参照してください。

マニュアル表記規則

Novell のマニュアルでは、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。

概要

1

1.1 主要な用語

1.1.1 Identity Manager

Novell® Identity Manager は、設定可能で堅牢なポリシーセットを使用して接続システムのサーバ間でデータを同期するサービスです。Identity Manager では、アイデンティティボールトを使用して共有情報が格納され、その情報がボールトまたは接続システムで変更されると、メタディレクトリエンジンを使用してポリシーベースの情報管理が行われます。Identity Manager 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配置されているサーバで実行します。

1.1.2 接続システム

接続システムとは、ドライバを介して Identity Manager とデータを共有できるシステムのことです。Active Directory は接続システムです。

1.1.3 アイデンティティボールト

アイデンティティボールトは、eDirectory™ で動作する永続的なデータベースであり、接続システムとのデータの同期を維持するために Identity Manager で使用されます。ボールトは、狭義には Identity Manager のプライベートデータストア、また広義には企業規模のデータを保持するメタディレクトリと見なすことができます。ボールトのデータは、NCP™ (ConsoleOne® や iManager のようなユーティリティで使用される従来のプロトコル)、LDAP、および DSML をはじめとする、eDirectory でサポートされているプロトコルで使用できます。

ボールトは eDirectory で動作するため、既存のディレクトリツリーをボールトとして使用すれば、Identity Manager を企業のディレクトリインフラストラクチャに容易に組み込むことができます。

1.1.4 メタディレクトリエンジン

メタディレクトリエンジンは、Identity Manager のイベント管理およびポリシーを実装するコアサーバです。このエンジンは、eDirectory の Java* 仮想マシンで実行します。

1.1.5 Active Directory ドライバ

ドライバには、接続システムのデータ共有ポリシーが実装されます。管理者は、iManager を使用してフィルタやポリシーを定義し、ドライバのアクションを制御します。Active Directory の場合、ドライバには 1 つのドメインのポリシーが実装されます。

1.1.6 ドライバシム

ドライバシムとは、XML ベースの Identity Manager コマンドやイベント言語 (XDS) を、接続システムとのやりとりに必要なプロトコルや API コールに変換する、ドライバのコンポーネントのことです。シムは、出力変換が実行された後に接続システム上でコマンドを実行するために呼び出されます。通常、コマンドは、購読者チャネルで生成されますが、発行者チャネルではコマンドライトバックによって生成できます。

シムで、入力変換ポリシー用の接続システムからのイベントも生成されます。ドライバシムは、Java クラス内に、またはネイティブの Windows DLL ファイルとして実装できます。Active Directory 用のシムには、ADDriver.dll があります。

ADDriver.dll は、ネイティブの Windows DLL ファイルとして実装されます。ADDriver は、さまざまな Windows API を使用して Active Directory と統合されます。一般に、これらの API では、何らかの種類のログインと認証が成功する必要があります。また、こうした API では、ログインアカウントに Active Directory 内および ADDriver.dll が実行するコンピュータでの特定の権限や特権が必要になる場合もあります。

リモートローダを使用する場合、ADDriver.dll は、リモートローダを実行しているサーバ上で実行します。それ以外の場合、このシムは、メタディレクトリエンジンを実行しているサーバ上で実行します。

1.1.7 リモートローダ

リモートローダにより、ドライバシムは、メタディレクトリエンジンの外で (おそらく別のコンピュータ上でリモートに) 実行できます。一般に、リモートローダは、ドライバシムの要件が Identity Manager サーバで満たされない場合に使用されます。たとえば、メタディレクトリエンジンを Linux* 上で実行している場合、リモートローダは、Windows サーバ上で Active Directory ドライバシムを実行するために使用されます。

リモートローダは、ドライバシムを実行してシムとメタディレクトリエンジンの間で情報を受け渡すサービスです。リモートローダを使用する場合は、メタディレクトリエンジンを実行しているサーバではなく、リモートローダを実行しているサーバにドライバシムをインストールします。SSL を使用して、メタディレクトリエンジンとリモートローダの間の接続を暗号化することもできます。

リモートローダを Active Directory ドライバシムとともに使用する場合は、次の 2 つのネットワーク接続が存在します。

- ドメインコントローラとリモートローダの間
- Active Directory と Active Directory ドライバシムの間

1.2 新機能

1.2.1 ドライバの機能

- [Platform Logon (プラットフォームログオン)] はドライバシム環境設定パラメータです。このパラメータにより、シムのローカルログオンが有効になります。ローカルログオンを有効にすると、購読者チャネルのパスワードの設定やパスワードの変更では、SSL 暗号化 LDAP セッションを必要としないプラットフォームパスワード管理 API が使用されます。

  CDOEXM を使用した Exchange 操作では、認証にスレッド ID が使用され、LDAP チャネル外での操作の失敗の可能性が低減します。詳細については、39 ページの第 4 章「Active Directory ドライバの設定」を参照してください。
- ドライバシム環境設定パラメータが更新されています。ドライバパラメータには、パラメータの優れた分類とパラメータに格納される値の効率的な管理を行うことができる、柔軟性の高いプロンプト表示が採用されています。既知の値セットに制約されているパラメータはドロップダウンリストで制御され、整数値を必要とするパラメータは無効な文字がないか確認されます。
- 2 つのドライバシム環境設定パラメータが、Microsoft Exchange メールボックスの移動や削除を制御するために追加されています。CDOEXM と Exchange メールボックスの移動が有効にされている場合に、すでに Exchange メールボックスを保持しているユーザオブジェクトの homeMDB 属性の値を設定すると、そのメールボックスは、新しい Exchange メッセージデータベースに移動されます。シムは、ドメイン内の移動だけをサポートします。したがって、新しいメッセージデータベースをホストする Exchange サーバは、シムで管理されるドメイン内に存在する必要があります。
- ユーザアプリケーションまたはポリシーを介した役割ベースエンタイトルメントのサポートが拡大されました。『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。
- ドライバシムは、拡張クエリ (query-ex) をサポートします。拡張クエリでは、LDAP 検索のページ区切りの結果が有効になります。この機能により、シムでは大規模なデータセットを Active Directory からアイデンティティボールトに移行できます。Active Directory からの移行の詳細については、89 ページの第 8 章「トラブルシューティング」を参照してください。

1.2.2 Identity Manager の機能

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。

1.3 システム間のデータ転送

この節では、Active Directory とアイデンティティボールトの間のデータフローについて説明します。

1.3.1 発行者チャネルと購読者チャネル

Active Directory ドライバは、発行者チャネルと購読者チャネルをサポートします。

発行者チャネルの機能は、次のとおりです。

- ドライバシムの接続先サーバでホストされているドメインの Active Directory からイベントを読み込む。
- 該当する情報をアイデンティティボールトに送信する。

購読者チャネルの機能は、次のとおりです。

- アイデンティティボールトブジェクトに対する追加や変更を監視する。
- 対象となる Active Directory に変更を加える。

ドライバを設定すると、Active Directory とアイデンティティボールトのどちらについても特定の属性を更新できるようになります。この環境設定では、最新の変更により属性値が決定されます。ただし、マージ操作がフィルタとマージ権限で制御されている場合は除きます。

1.4 デフォルトのドライバ環境設定

Active Directory ドライバは、ActiveDirectory.xml というデフォルトの環境設定ファイルに付属しています。デザイナまたは iManager でインポートされると、この環境設定ファイルにより、Active Directory との同期に適したルールセットとポリシーでドライバが作成されます。ドライバの要件がデフォルトのポリシーと異なる場合は、適切なポリシーを実施するようポリシーを変更する必要があります。デフォルトの一致ポリシーに細心の注意を払ってください。通常、ユーザを表し信頼するデータは、デフォルトとは異なります。ポリシー自体には注釈が付いているので、テストドライバをインポートしてデザイナまたは iManager でポリシーを確認すれば、ポリシーの機能を十分に理解できます。

1.4.1 ユーザオブジェクト名マッピング

iManager や ConsoleOne のようなアイデンティティボールトの管理ユーティリティには、通常、Microsoft* 管理コンソール (MMC) の「ユーザとコンピュータスナップイン」とは異なるユーザオブジェクトの名前が付けられます。使用する一致ポリシーと任意の変換ポリシーが正しく実装されるように、相違点を確実に理解してください。

1.4.2 データフロー

データは、Active Directory とアイデンティティボールトの間で受け渡しできます。データフローは、Active Directory ドライバのために用意されているポリシーによって制御されます。

ポリシー

ポリシーは、Active Directory とアイデンティティボールトの間のデータ同期を制御します。

ドライバの環境設定中に、Active Directory 環境設定ファイルによって作成したデフォルトのポリシーとフィルタに作用するオプションをいくつか選択できます。11 ページの 表 1-1 は、こうしたオプションおよび作成したポリシーやフィルタへの作用を示しています。

表 *1-1* データフローオプション

オプション	説明
ボールトからADへ	［データフローの設定］では、同期される属性およびクラスを制御する最初のドライバフィルタを確立します。このオプションの目的は、一般的なデータフローポリシーを最もよく表すようにドライバを設定することです。特定の要件を反映するように、このオプションをインポート後に変更できます。 ［Bidirectional (双方向)］では、発行者チャネルと購読者チャネルの両方で同期するようにクラスと属性を設定します。アイデンティティボールトまたは Active Directory での変更は相手側に反映されます。両方を信頼されるデータソースにしたい場合に、このオプションを使用します。 ［AD からボールトへ］では、発行者チャネルだけで同期するようにクラスと属性を設定します。Active Directory での変更はアイデンティティボールトに反映されますが、アイデンティティボールトでの変更は無視されます。Active Directory を信頼されるデータソースにしたい場合に、このオプションを使用します。 ［ボールトから AD へ］では、購読者チャネルだけで同期するようにクラスと属性を設定します。アイデンティティボールトでの変更は Active Directory に反映されますが、Active Directory での変更は無視されます。ボールトを信頼されるデータソースにしたい場合に、このオプションを使用します。
平面	［発行者の配置］では、アイデンティティボールトでのオブジェクトの作成場所を制御します。 ［ミラーリング済み］では、オブジェクトを Active Directory の場合と同じ階層でアイデンティティボールトに格納します。 ［平面］では、環境設定中に指定したアイデンティティボールト内のベースコンテナにすべてのオブジェクトを格納します。
平面	［Subscriber Placement (購読者の配置)］では、Active Directory でのオブジェクトの配置方法を制御します。 ［ミラーリング済み］では、オブジェクトをアイデンティティボールトの場合と同じ階層で Active Directory に格納します。 ［平面］では、環境設定中に指定した Active Directory 内のベースコンテナにすべてのオブジェクトを格納します。

12 ページの 表 1-2 は、デフォルトのポリシーを示し、環境設定中に選択した設定内容がどのようにポリシーに作用するかについて説明しています。

表 *1-2* デフォルトのポリシー

ポリシー	説明
作成	ミラーリング済み階層または平面階層では、フルネームを定義して、Active Directory ユーザをアイデンティティボールトのユーザとして作成する必要があります。
一致	ミラーリング済み階層では、一致ポリシーは、階層内の同じ位置でオブジェクトを検出しようとします。 平面階層では、一致ポリシーは、指定するベースコンテナの同じフルネームを持つオブジェクトと一致するユーザを検出しようとします。
配置	ミラーリング済み階層では、配置ポリシーは、操作を送信するデータストアの階層を反映する階層内にすべてのオブジェクトを格納します。 平面階層では、配置ポリシーは、指定するベースコンテナにすべてのオブジェクトを格納します。

スキーママッピング

次のアイデンティティボールトのユーザ、グループ、および部門の属性は、Active Directory ユーザおよびグループ属性にマップされます。

表に示すマッピングは、デフォルトのマッピングです。同じタイプの属性を再マップできます。

表 *1-3* すべてのクラス向けにマップされる属性

eDirectory	Active Directory
CN	cn
説明	description
Fax 番号	facsimiletelephoneNumber
フルネーム	displayName
名前	givenName
イニシャル	initials
インターネット電子メールアドレス	mail
L	physicalDeliveryOfficeName
地域	locality
ログインの無効化	dirxml-uACAccountDisabled
アカウントの有効期限	accountExpires
物理配信局名	l
郵便番号	PostalCode
私書箱	postOfficeBox

eDirectory	Active Directory
S	st
SA	streetAddress
関連項目	seeAlso
名字	sn
電話番号	telephoneNumber
役職	title

eDirectory の L 属性は Active Directory の physicalDeliveryOfficeName 属性にマップされ、eDirectory の Physical Delivery Office Name (物理配信局名) 属性は Active Directory の L 属性にマップされます。同じような名前のフィールドに同じ値が設定されているため、このように属性をマップすると、属性が ConsoleOne や Microsoft 管理コンソールで有効に機能できます。

表 *1-4* ユーザ向けにマップされる属性

eDirectory	Active Directory
CN	userPrincipalName
DirXML-ADAliasName	sAMAccountName
Login Allowed Time Map (ログイン許容時間マップ)	logonHours

表 *1-5* マップされる部門属性

eDirectory	Active Directory
部門	organizationalUnit
OU	ou

ネームマッピングポリシー

デフォルトの環境設定には、連携する 2 つのネームマッピングポリシーが用意されています。これらのポリシーにより、アイデンティティボールトと Active Directory の間の異なるネーミングポリシーを調整できます。「Active Directory ユーザとコンピュータ」ツール (Microsoft 管理コンソールのスナップイン、このマニュアルでの略称 : MMC) でユーザを作成すると、ユーザフルネームがそのオブジェクト名として使用されることがわかります。ユーザオブジェクトの属性では、Windows 2000 以前のログオン名 (別名 : NT ログオン名または sAMAccountName) および Windows 2000 ログオン名 (別名 : userPrincipalName) が定義されます。iManager または ConsoleOne でアイデンティティボールトにユーザを作成すると、オブジェクト名とユーザログオン名は同じになります。

MMC を使用して Active Directory に一部のユーザを作成し、アイデンティティボールトまたはアイデンティティボールトと同期する別の接続システムにその他のオブジェクトを作

成すると、相手側のコンソールではオブジェクトが正しく表示されないことがあり、相手側のシステムでオブジェクトを作成できない場合があります。

The Full Name Mapping Policy is used to manage objects in Active Directory using the MMC conventions. このポリシーが有効にされると、アイデンティティボールト内のフルネーム属性は Active Directory 内のオブジェクト名と同期されます。

NT ログオン名マッピングポリシーは、アイデンティティボールトの規則に従って Active Directory 内のオブジェクトを管理するために使用されます。このポリシーが有効にされると、アイデンティティボールト内のオブジェクト名は、Active Directory 内のオブジェクト名および NT ログオン名の両方と同期するために使用されます。Active Directory 内のオブジェクトはアイデンティティボールトと同じ名前が付けられ、NT ログオン名はアイデンティティボールトのログオン名と一致します。

両方のポリシーが同時に有効にされると、Active Directory オブジェクト名はアイデンティティボールトのフルネームになりますが、NT ログオン名はアイデンティティボールトのログオン名と一致します。

両方のポリシーが無効にされると、特別なマッピングは作成されません。オブジェクト名は同期されますが、NT ログオン名を作成するための特別なルールはありません。NT ログオン名は Active Directory の必須属性であるため、追加操作中に NT ログオン名を生成する何らかの方式が必要です。NT ログオン名 (sAMAccountName) はアイデンティティボールト内の DirMXL-ADAliassName にマップされるので、その属性を使用して Active Directory 内の NT ログオン名を制御するか、または購読者作成ポリシーに独自のポリシーを構築して NT ログオン名を生成することができます。このようなポリシー選択によって、MMC で作成されたユーザは、オブジェクト名としてアイデンティティボールト内の、MMC で生成されたオブジェクト名を使用します。この名前は、ボールトへのログインには使用できない場合があります。

Windows 2000 ログオン名ポリシー

Windows 2000 ログオン名 (別名 : userPrincipalName または UPN) に直接対応する名前は、アイデンティティボールトにはありません。UPN は、電子メールアドレス (user@mycompany.com) のように見え、実際にユーザの電子メール名である場合があります。UPN で作業する際には、ドメインを正しく使用する目的で設定されているドメイン名 (@ 記号の後の部分) を使用する必要があることを覚えておいてください。MMC を使用してユーザを作成し、UPN を追加するときにドメイン名のドロップダウンボックスを調べると、どのドメイン名が許可されているかがわかります。

デフォルトの環境設定には、userPrincipalName を管理するための選択肢がいくつか用意されています。ユーザの電子メールアドレスを userPrincipalName として使用できるようにドメインを設定する場合は、ユーザの電子メールアドレスを追跡するオプションのいずれかが適しています。アイデンティティボールトまたは Active Directory の電子メールアドレスに従って userPrincipalName を設定できます。従うアドレスは、どちらの電子メールが信頼できるかによって異なります。ユーザ電子メールアドレスが適切でない場合は、userPrincipalName をユーザログオン名とあらかじめ準備されているドメイン名から作成できます。複数の名前を使用できる場合は、インポート後にポリシーを更新して選択します。こうしたオプションのどれも適切でない場合は、デフォルトのポリシーを無効にして独自のポリシーを作成できます。

エンタイトルメント

エンタイトルメントにより、Identity Manager を eDirectory の Identity Manager ユーザアプリケーションや役割ベースのサービスと簡単に統合できます。ユーザアプリケーションを使用すると、Active Directory 内のアカウントの提供のようなアクションは、正当な承認が得られるまで遅延されます。役割ベースのサービスを使用すると、正規のグループメンバーシップではなく、ユーザオブジェクトの属性に基づいて権限が割り当てられます。このどちらのサービスでも課題が生じます。その理由は、オブジェクトの属性からでは、承認が与えられているか、またはユーザが役割に適合するかが明らかにならないためです。

エンタイトルメントにより、アイデンティティボールト内のオブジェクトに関するこの情報を記録する方式が標準化されます。ドライバの観点からは、エンタイトルメントにより、Active Directory 内の何らかの項目に権限が与えられたり取り消されたりします。エンタイトルメントを使用すると、Active Directory 内のアカウントへの権限の付与、グループメンバーシップの制御、および Exchange メールボックスの提供を行うことができます。ドライバでは、ユーザアプリケーションや役割ベースのエンタイトルメントは意識されません。独自のルールに基づく、ユーザのエンタイトルメントの付与または取り消しは、ユーザアプリケーションサーバまたはエンタイトルメントドライバに依存します。

ドライバでユーザアプリケーションまたは役割ベースエンタイトルメントを使用する場合に限り、ドライバのエンタイトルメントを有効にしてください。

Active Directory の準備

2

この節では、次の項目について説明します。

2.1 Active Directory の前提条件

- ❑ Novell® Identity Manager 3.0 とその前提条件。『Identity Manager 3.0 インストールガイド』の「Identity Manager 3 のインストール」を参照。
- ❑ Windows 2003 Server、または Service Pack 2 以降を適用した Windows 2000 Server。
- ❑ Active Directory (AD) ドライバを実行しているサーバ上およびターゲットドメインコントローラ上の Internet Explorer 5.5 以降。
- ❑ Active DirectoryドメインコントローラDNS名またはIPアドレス(認証方式によって異なる)。

また、Active Directory ドライバをホストするサーバを Active Directory ドメインのメンバーにすることもお勧めします。これは、Exchange メールボックスを提供してパスワードを同期するために必要です。こうした機能が必要ない場合は、［シンプル］(単純なバインド) 認証モードを使用すれば、サーバを任意のドメインのメンバーにすることができます。双方向のパスワード同期機能を設定するには、［ネゴシエーション］認証オプションを選択する必要があります。

2.2 インストールの計画

Active Directory ドライバをドメインコントローラまたはメンバーサーバにインストールできます。ドライバのインストールを開始する前に、次の項目を検討し、決定してください。

- Active Directory ドライバシムをインストールする場所
- セキュリティの問題に対処する方法

2.2.1 Active Directory ドライバおよびシムをインストールする場所

Active Directory ドライバシムは、サポートされているいずれかの Windows プラットフォームで実行する必要があります。ただし、この同じコンピュータにメタディレクトリエンジンをインストールする必要はありません。リモートローダを使用すると、エンジンとドライバシムを分離できます。それにより、さまざまなコンピュータの負荷を分散したり、会社の指示に対応することができます。

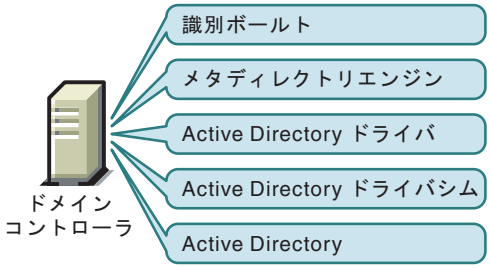
選択するインストールシナリオに応じてドライバシムのインストール方法が決定されます。ドライバシムを Identity Manager と同じコンピュータ (メタディレクトリエンジンとアイデンティティボールトが格納されている場所) にインストールすると、ドライバシムは Identity Manager から直接呼び出されます。ドライバシムを別のコンピュータにインストールする場合は、リモートローダを使用する必要があります。

ドライバ自体は、各シナリオで同じようにインストールされます。39 ページの第 4 章「Active Directory ドライバの設定」を参照してください。

ローカルインストール

1 つの Windows ドメインコントローラで、アイデンティティボールト、メタディレクトリエンジン、およびドライバをホストできます。

図 2-1 シナリオ *1* - すべてのコンポーネントが *1* つのサーバ上にある



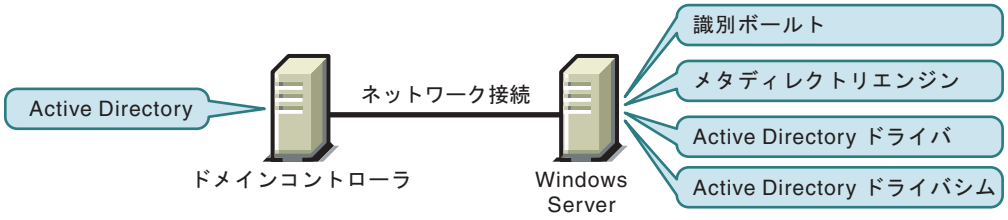
この環境設定は、ハードウェアコストの節減を求める組織に適しています。また、この環境設定は、Identity Manager と Active Directory の間にネットワークトラフィックがないため、最も高性能な環境設定となります。

ただし、ドメインコントローラで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をホストすると、コントローラの全体的な負荷が増大し、コントローラに障害が発生する危険性が高まります。ドメインコントローラは、Microsoft ネットワーキングにおいて重要な役割を果たすため、多くの組織では、追加ハードウェアのコストよりも、ドメイン認証の速度やドメインコントローラの障害に関する危険性の方を懸念しています。

Windows Server だけでのリモートインストール

Active Directory ドメインコントローラとは別のコンピュータにアイデンティティボールト、メタディレクトリエンジン、およびドライバをインストールできます。この環境設定では、ドメインコントローラがあらゆる Identity Manager ソフトウェアと無関係になります。

図 2-2 シナリオ *2* - 別々のサーバ上の *Active Directory* およびドライバシム

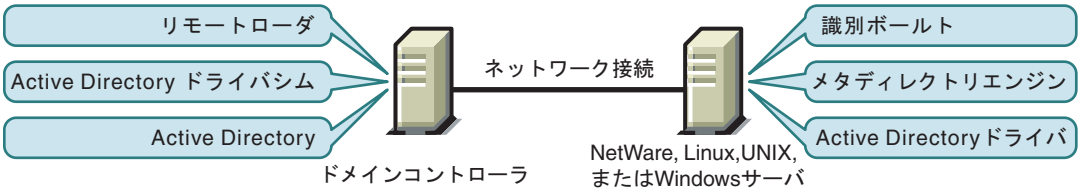


会社の方針として、ドメインコントローラとして稼働しているコンピュータで同時にドライバを稼働させてはならない場合は、この環境設定が適しています

Windows および他のプラットフォームでのリモートインストール

リモートローダとドライバシムを Active Directory ドメインコントローラのコンピュータにインストールし、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は別のサーバにインストールする、という構成が可能です。

図 2-3 シナリオ *3* - 1 つのサーバ上の *Active Directory*、リモートローダ、およびドライバシム



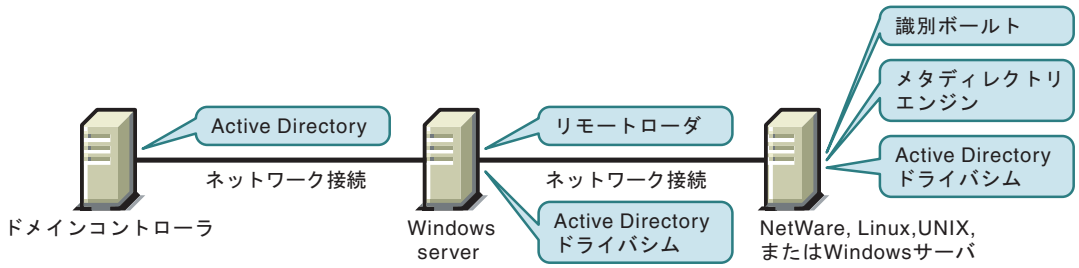
この環境設定は、アイデンティティボールトとメタディレクトリエンジン (Identity Manager) が、サポートされている Windows バージョン以外のプラットフォームにインストールされている場合に便利です。

シナリオ 2 とシナリオ 3 の環境設定では、ドメインコントローラで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をホストする際のパフォーマンスへの影響が排除されます。

Windows メンバーサーバでのリモートインストール

プラットフォームの要件とドメインコントローラの制約が設定されている場合は、3 サーバ環境設定を使用できます。

図 2-4 シナリオ *4* - *3* サーバ環境設定



この環境設定は、設定するのは複雑ですが、一部の組織の制約に適応します。この図では、2 つの Windows サーバはドメインのメンバーサーバです。

2.3 セキュリティ問題の対処

主要なセキュリティの問題として、認証、暗号化、およびリモートローダの使用を考慮する必要があります。Windows 2003 または Windows 2000 SP3 以降がある場合は、署名というセキュリティオプションを考慮します。59 ページの 「セキュリティパラメータ」の「署名を使用する」を参照してください。

Windows で使用可能なセキュリティプロファイルはサーバのサービスパック、DNS サーバインフラストラクチャ、ドメインポリシー、およびサーバのローカルポリシー設定によって異なるため、セキュリティ管理の簡単な処方は考えられません。以降の節では、セキュリティの選択肢について説明し、推奨の環境設定を提示します。ドライバの実装時お

よびコンポーネントのアップグレード時には、セキュリティに細心の注意を払ってください。

2.3.1 認証方式

認証により、ドライバシムは Active Directory に、および場合によってはローカルコンピュータに認識されます。Active Directory の認証を受けるには、［ネゴシエーション］方式または［シンプル］(単純なバインド) 方式を使用できます。

表 *2-1* 認証方式

認証方式	説明	長所	短所
ネゴシエーション	優先の方式。 Kerberos*、NTLM、またはプラグ可能な認証スキーマがインストールされている場合は、それを使用します。	ドライバは、ドメイン内の任意のサーバにインストールできます。	ドライバをホストするサーバは、ドメインのメンバーである必要があります。
シンプル	ドライバシムをホストするサーバがドメインのメンバーでない場合に使用されます。	ドライバは、ドメインのメンバーでないサーバにインストールできます。	Exchange メールボックスプロビジョニングやパスワード同期のような、一部のプロビジョニングサービスは利用できません。

2.3.2 暗号化

SSL でデータを暗号化します。環境設定に基づいて、SSL を次の 2 箇所で使用できます。

- Active Directory ドライバとドメインコントローラの間
- アイデンティティボールトと Active Directory ドライバを実行するリモートローダの間

Active Directory とアイデンティティボールト (eDirectory) の間では、パスワード同期が行われます。ネットワークを介する通信では、必ず SSL を使用する必要があります。

メタディレクトリエンジン、アイデンティティボールト、Active Directory ドライバ、および Active Directory が同じコンピュータ上にある場合、SSL は不要です。通信は、ネットワークを横断しません。

ただし、メンバーサーバの Active Directory ドライバシムを使用して Active Directory にリモートでアクセスする場合は、Active Directory ドライバシムと Active Directory の間に SSL を設定する必要があります。この操作を行うには、ドライバ環境設定の SSL パラメータを［はい］に設定します。24 ページのセクション 2.3.3「リモートローダと Identity Manager の間の SSL 接続」の 23 ページのステップ 5 を参照してください。

ドメインコントローラのリモートローダを使用している場合は、メタディレクトリエンジンとリモートローダの間に SSL を設定できます。SSL とリモートローダの詳細については、『Novell Identity Manager 3.0 管理ガイド』の「接続システムの設定」を参照してください。

次の表は、17 ページのセクション 2.2「インストールの計画」で説明したシナリオごとに SSL 接続を使用できる場所について説明しています。

表 2-2 *SSL 接続*

環境設定	使用可能な SSL 接続
1 つのサーバ	SSL 接続は必要ありません。
2 つのサーバ : Identity Manager と Active Directory ドライバが同じサーバ上にある	Active Directory ドライバとドメインコントローラの間で SSL 接続を確立できます。
デュアルサーバ : Identity Manager と Active Directory ドライバが別々のサーバ上にある	Identity Manager と Active Directory ドライバを実行するリモートローダの間で SSL 接続を確立できます。
3 つのサーバ	Active Directory ドライバとドメインコントローラの間で SSL 接続を確立できます。 Identity Manager と Active Directory ドライバを実行するリモートローダの間でも SSL 接続を確立できます。

Active Directory ドライバとドメインコントローラの間の SSL 接続

Active Directory ドメインコントローラへの SSL 接続を作成するには、SSL を使用するよう設定する必要があります。この作業には、認証局の設定、必要な証明書の作成、エクスポート、およびインポートが必要です。

認証局の設定

大半の組織には、すでに認証局が用意されています。このような場合には、有効な証明書をエクスポートした後、それをドメインコントローラの証明書ストアにインポートする必要があります。ドライバシムをホストするサーバは、この証明書の発行元認証局が連鎖しているルート認証局を信頼する必要があります。

組織に認証局が用意されていない場合は、認証局を確立する必要があります。Novell、Microsoft、および他のいくつかのサードパーティでは、認証局を確立するために必要なツールを提供しています。認証局を確立する方法については、このガイドでは説明していません。詳細については、次の資料を参照してください。

- Novell Certificate Server™ 2.5 Administration Guide (http://www.novell.com/documentation/lg/crt252/index.html)
- Microsoft Step-by-Step Guide to Setting up a Certificate Authority (http://http://www.microsoft.com/japan/technet/prodtechnol/windows2000serv/deploy/confeat/default.mspx)

証明書の作成、エクスポート、およびインポート

認証局を用意できたら、LDAP SSL が正常に機能するように、LDAP サーバに適切なサーバ認証証明書をインストールする必要があります。また、ドライバシムをホストするサー

バは、そのような証明書を発行した認証局を信頼する必要があります。サーバとクライアントのどちらも 128 ビット暗号化をサポートする必要があります。

1 次の Active Directory LDAP サービス要件を満たす証明書を生成します。

- LDAPS 証明書が、ローカルコンピュータの個人証明書ストア (プログラム的にはコンピュータの MY 証明書ストアと呼ばれる) に存在する。
- 証明書と一致する秘密鍵が、ローカルコンピュータのストアに存在し、正しく証明書に関連付けられている。

  秘密鍵に対して強固な秘密鍵保護を有効にしないでください。
- 拡張キー使用法に、サーバ認証 (1.3.6.1.5.5.7.3.1) オブジェクト ID (OID) が含まれている。
- ドメインコントローラの Active Directory での完全修飾ドメイン名 (DC01.DOMAIN.COM など) が次のいずれかの場所に存在する。
  - ［サブジェクト］フィールドの共通名 (CN)。
  - ［サブジェクトの別名］拡張の DNS エントリ。
- 証明書が、ドメインコントローラおよび LDAPS クライアントが信頼する CA によって発行されている。

  信頼は、発行元 CA が連鎖しているルート CA を信頼するようクライアントとサーバを設定することによって確立されます。

この証明書により、ドメインコントローラの LDAP サービスで、LDAP とグローバルカタログトラフィックをリスンして自動的に両方の SSL 接続を受け入れることができるようになります。

注 **:** この情報については、Microsoft サポート技術情報の文書番号 321051「SSL でどのようにサードパーティ証明機関と LDAP を有効にするには。(http://support.microsoft.com/kb/321051/ja)」を参照してください。このドキュメントで最新の要件と追加情報を調べてください。

---

2 Windows 2000 によってサポートされている次の標準の証明書ファイル形式のいずれかでこの証明書をエクスポートします。

- 個人情報交換 (PFX または PKCS #12)
- 暗号化メッセージシンタックス標準 (PKCS #7)
- DER (Distinguished Encoding Rules) エンコードのバイナリの X.509
- Base64 エンコードの X.509

3 この証明書をドメインコントローラにインストールします。

次のリンクには、サポートされているプラットフォームごとの手順が記載されています。

- インポートした証明書を Windows Server 2003 の Web サーバーにインストールする方法 (http://support.microsoft.com/kb/816794/ja)
- インポートした証明書の Web サーバーへのインストール (http://support.microsoft.com/kb/310178/ja)

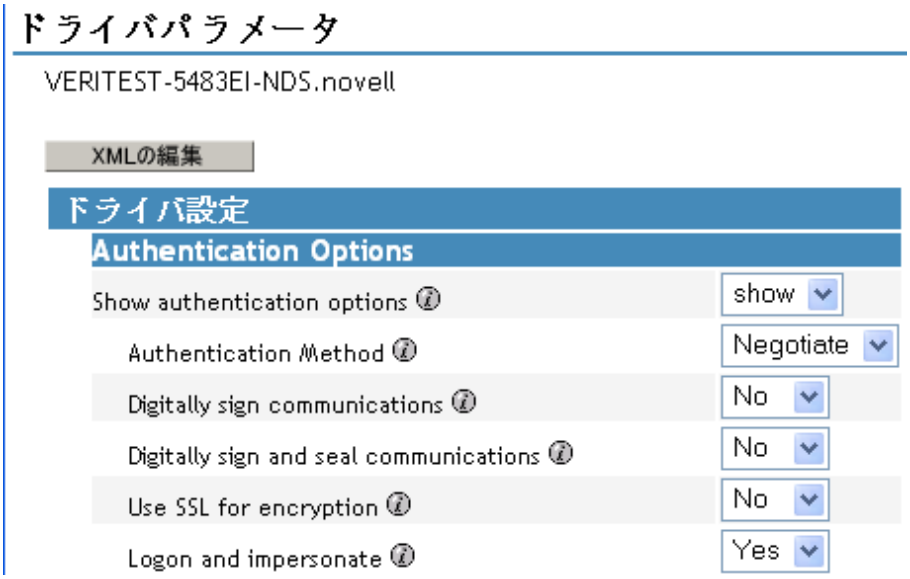
「ローカル コンピュータ ストアへの証明書のインポート」で表示される手順に従ってください。

4 ドライバシムをホストするサーバと証明書を発行したルート認証局の間で信頼関係が確立されていることを確認します。

ドライバシムをホストするサーバは、発行元認証局が連鎖しているルート認証局を信頼する必要があります。

証明書の信頼を確立する方法の詳細については、Windows 2000 Server のヘルプの「ルート証明機関の信頼を確立するポリシー」を参照してください。

5 iManager で、ドライバのプロパティを編集して、［Use SSL (yes/no) (SSL を使用 (はい / いいえ))］オプションを［はい］に変更します。



6 ドライバを再起動します。

ドライバが再起動すると、SSL 接続は、ドメインコントローラと Active Directory ドライバシムを実行するサーバの間でネゴシエートされます。

証明書の確認

証明書を確認するには、SSL を介して AD を認証します。Windows サーバにある ldifde コマンドラインユーティリティを使用します。ldifde コマンドを使用する

1 コマンドラインプロンプトを開きます。

2 「ldifde -f output/input file -t 636 -b administrator domain password -s computerFullName」と入力します。

サーバがポート 636 に対して設定されている場合は、次のように入力します。

ldife -f out.txt -t 636 -b administrator dxad.novell.com novell -s parent1.dxad3.lab.novell

出力は out.txt ファイルに送出されます。このファイルを開いて Active Directory 内のオブジェクトの一覧を表示すると、Active Directory への SSL 接続が正しく作成され、証明書が有効になっていることがわかります。

2.3.3 リモートローダと Identity Manager の間の SSL 接続

リモートローダを使用している場合は、メタディレクトリエンジンとリモートローダの間およびドライバと Active Directory の間で SSL を設定する必要があります。

リモートローダと Identity Manager の間で SSL 接続を確立する方法の詳細については、『Novell Identity Manager 3.0 管理ガイド』の「“ リモートローダの設定 ”」を参照してください。

2.4 管理用アカウントの作成

テスト環境では、Active Directory ドライバが正しく機能するまでは管理者アカウントを使用します。その後、適切な権限 (制限された権限を含む) を持つ管理用アカウントを作成します。このアカウントは、Active Directory を認証するために Active Directory ドライバで排他的に使用できます。

このようにすると、Identity Manager 管理用アカウントが他の管理用アカウントの変更の影響を受けないようにすることができます。この設計の長所は、次のとおりです。

- Active Directory の監査を利用して Active Directory ドライバのアクティビティを追跡できます。
- 他のアカウントと同様にパスワード変更ポリシーを実装した後、ドライバ環境設定に必要な更新を加えることができます。

このアカウント名とパスワードは、ドライバ環境設定に保存されます。したがって、アカウントパスワードが変更されるたびにこのパスワードを変更する必要があります。ドライバ環境設定を更新せずにアカウントパスワードを変更すると、次回ドライバが再起動されたときに認証は失敗します。

少なくとも、このアカウントには、操作する発行者チャネル用のドメインのルートでの読み込み権とディレクトリの変更の複製権が必要です。購読者チャネルで変更されるオブジェクトへの書き込み権も必要です。書き込み権は、購読者チャネルから書き込まれるコンテナと属性に制限することができます。

Exchange メールボックスを装備するために、Identity Manager アカウントには、ログオンアカウントに対する「オペレーティングシステムの一部として動作する」権限が必要です。

Windows 2003 では、削除されたオブジェクトを確認するためにさらに権限が必要です。97 ページの付録 A「CN=Deleted Objects コンテナの許可の変更」を参照してください。

2.5 ドライバの機能の理解

この節では、Active Directory ドライバを展開する前に精通する必要があるドライバの機能について説明します。

- 27ページのセクション2.5.5「Active Directoryオブジェクトを復元する場合のeDirectoryオブジェクトの保持」

2.5.1 複数値属性

Active Directory ドライバでの複数値属性の処理方法は、バージョン 2 とは変わりました。

バージョン 2 では複数値属性を購読者チャネルの単一値属性として処理するために、追加操作または変更操作で最初に変更した値以外はすべて無視していました。Active Directory ドライバのバージョン 3 では、複数値属性を完全にサポートしています。

ただし、Active Directory ドライバでは、複数値属性を単一値属性と同期する場合に複数値属性は単一値属性として処理されます。たとえば、［電話番号］属性は、Active Directory では単一値属性であり、アイデンティティボールトでは複数値属性です。この属性が Active Directory から同期されると、1 つの値だけがアイデンティティボールトに保存されます。

これにより、2 つの属性間で正確に同期され、正しいマッピングが作成されますが、単一値属性にマップされる属性に複数の値が設定されている場合は、データが失われるおそれがあります。ほとんどの場合、使用する環境に必要であれば、特別な値は別の場所に保持するようポリシーを実装できます。

2.5.2 カスタムブール型属性を使用したアカウント設定の管理

Active Directory 属性 userAccountControl は整数の値であり、そのビットでログオンの許可、パスワードの要求、アカウントのロックなどのログオンアカウントプロパティを制御します。個々のプロパティを表すブール値は整数値の中に隠れているため、プロパティを個別に同期することは、簡単ではありません。

バージョン 2 の Active Directory ドライバでは、userAccountControl を eDirectory の［ログインの無効化］属性にマップできていましたが、属性内の他のプロパティビットはマップできていませんでした。

バージョン 3 では、userAccountControl 属性内の各ビットをブール値として個々に参照するか、または userAccountControl を整数として全体で管理することができます。ドライバでは、userAccountControl 内の各ビットのブール型の別名を認識します。こうした別名の値は、userAccountControl を含む任意のクラスのスキーマに反映されます。別名の値は、購読者チャネルで受け入れられ、発行者チャネルで提示されます。

この機能の長所は、各ビットをブール型として使用できるため、ビットを発行者フィルタで個々に有効にしたり、容易にアクセスできる点にあります。また、userAccountControl を発行者フィルタに挿入して、変更通知を整数で受け取ることもできます。

userAccountControl の整数と別名のバージョンを 1 つの環境設定に混在させないでください。

次の表は、使用可能な別名と 16 進の値を示しています。「読み込み専用」の属性を購読者チャネルで設定することはできません。

表 *2-3* 別名と *16* 進の値

別名	16 進の値	メモ
dirxml-uACDontExpirePassword	0x10000	読み書き可能
dirxml-uACHomedirRequired	0x0008	読み書き可能
dirxml-uACInterdomainTrustAccount	0x0800	読み込み専用
dirxml-uACNormalAccount	0x0200	読み込み専用
dirxml-uACServerTrustAccount	0x2000	読み込み専用
dirxml-uACWorkstationTrustAccount	0x1000	読み込み専用
dirxml-uACAccountDisable	0x0002	読み書き可能
dirxml-uACPasswordNotRequired	0x0020	読み書き可能

userAccountControl 属性に関するトラブルシューティングのヒントについては、92 ページのセクション 8.9「購読者チャネルでユーザが追加した後に無効にされた Active Directory アカウント」を参照してください。

2.5.3 homeMDB 属性を使用した Exchange メールボックスの提供

Exchange 2000 と Exchange 2003 のメールボックスを提供するためのオプションが、バージョン 2 とは変わりました。

バージョン 2 では、Exchange プロビジョニングはユーザオブジェクトで属性を設定することによって実現されていました。Microsoft プログラム (受信者更新サービス) では、この情報を使用して Exchange データベースが提供されていました。

この方式は Active Directory ドライバのバージョン 3 でも機能しますが、新しい方式 (CDOEXM) が追加されました。CDOEXM を有効にすると、Exchange メールボックスは、homeMDB 属性の設定によって提供されます。homeMDB 属性が設定されると、必要なすべての属性が、ドライバにより自動的に設定されます。

homeMDB 属性は最初の環境設定中に設定されますが、ドライバポリシーを変更すれば設定を変更できます。このパラメータについては、40 ページのセクション 4.3「環境設定パラメータ」を参照してください。

2.5.4 Active Directory でのアカウントの期限切れ

［アカウントの有効期限］という eDirectory 属性を accountExpires という Active Directory 属性にマップすると、Active Directory 内のアカウントは、eDirectory で設定された時間より 1 日早く期限切れになります。

このようになる理由は、Active Directory では、accountExpires 属性の値が 1 日単位の増分で設定されるためです。［アカウントの有効期限］という eDirectory 属性では、特定の日時を使用してアカウントを期限切れにします。

たとえば、2006 年 7 月 15 日午後 5 時 00 分に期限切れになるように eDirectory でアカウントを設定すると、このアカウントは、7 月 14 日までは全日 Active Directory で有効です。

2006 年 7 月 15 日に期限切れになるように Microsoft 管理コンソールでアカウントを設定すると、［アカウントの有効期限］という eDirectory 属性は、2006 年 7 月 16 日午前 12 時 00 分に期限切れになるように設定されます。Microsoft 管理コンソールでは時刻の値を設定できないため、デフォルトは午前 12 時 00 分になります。

ドライバでは、最も制限の厳しい設定が使用されます。要件によっては、Microsoft での有効期限を 1 日追加できます。

2.5.5 Active Directory オブジェクトを復元する場合の eDirectory オブジェクトの保持

Active Directory ツールで Active Directory オブジェクトを復元すると、オブジェクトを同期するときに、関連付けられた eDirectory オブジェクトが削除されます。Active Directory ドライバで、Active Directory オブジェクトの isDeleted 属性の変更が検索されます。ドライバでこの属性の変更が検出されると、Active Directory オブジェクトに関連付けられているオブジェクトのドライバによって削除イベントが発行されます。

eDirectory オブジェクトを削除しない場合は、Active Directory ドライバにさらにポリシーを追加する必要があります。Identity Manager 3.0 には、すべての「削除」イベントを「関連付けを削除」イベントに変更する事前定義されたルールが付属しています。詳細については、『Policy Builder and Driver Customization Guide』の「Command Transformation - Publisher Delete to Disable」を参照してください。

Active Directory ドライバのインストール

3

3.1 基本手順

次の図は、Identity Manager をインストールするときに選択できるオプションを示しています。

図 3-1 *Identity Manager* インストールオプション

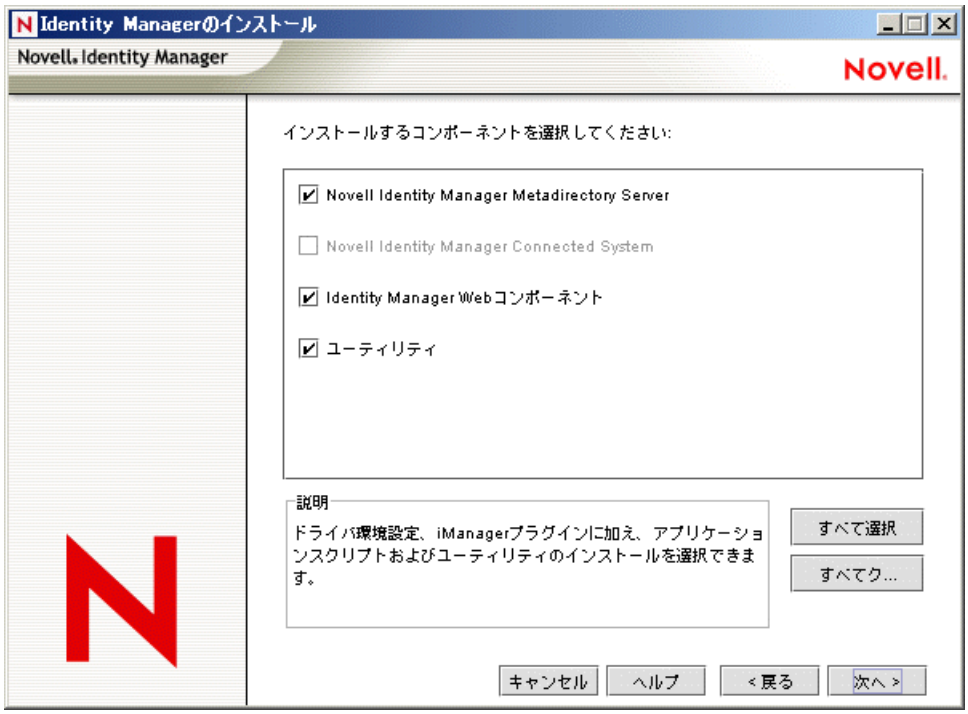


表 3-1 *Identity Manager* インストールオプション

オプション	説明
メタディレクトリサーバ	メタディレクトリエンジンと Identity Manager がインストールされます
接続システム	リモートローダがインストールされます

オプション	説明
Identity Manager Web コンポーネント	設定済みの (サンプル) ドライバ環境設定ファイルがインストールされます
ユーティリティ	Active Directory ディスカバリツールがインストールされます

Active Directory ドライバシムのインストールには、次の 3 つの基本手順が必要です。

表 *3-2* インストール手順

ステップ	インストール時の選択項目
1. Active Directory ドライバシムをメタディレクトリエンジンサーバまたはリモートローダサーバにインストールします。	[メタディレクトリサーバ] または [Novell Identity Manager Connected System] を選択します。30 ページのセクション 3.2「Active Directory ドライバシムのインストール」を参照してください。
2. iManager サーバに Active Directory の設定済みのインポートファイルをインストールします。	[Identity Manager Web コンポーネント] オプションを選択します。35 ページのセクション 3.3「設定済みのインポートファイルのインストール」を参照してください。
3. Identity Manager の設定に使用するワークステーションに Active Directory ディスカバリツールをインストールします。	[ユーティリティ] オプションを選択します。37 ページのセクション 3.4「Active Directory ディスカバリツールのインストール」を参照してください。

通常は、メタディレクトリサーバ (またはリモートローダ) と Web コンポーネントをインストールするときに、Active Directory ドライバコンポーネントをインストールします。ただし、Active Directory ドライバコンポーネントは後でインストールしてもかまいません。

3.2 Active Directory ドライバシムのインストール

3.2.1 メタディレクトリサーバへのシムのインストール

1. 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実行しているサーバで、Identity Manager のインストールを開始します。

   Identity Manager 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。
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

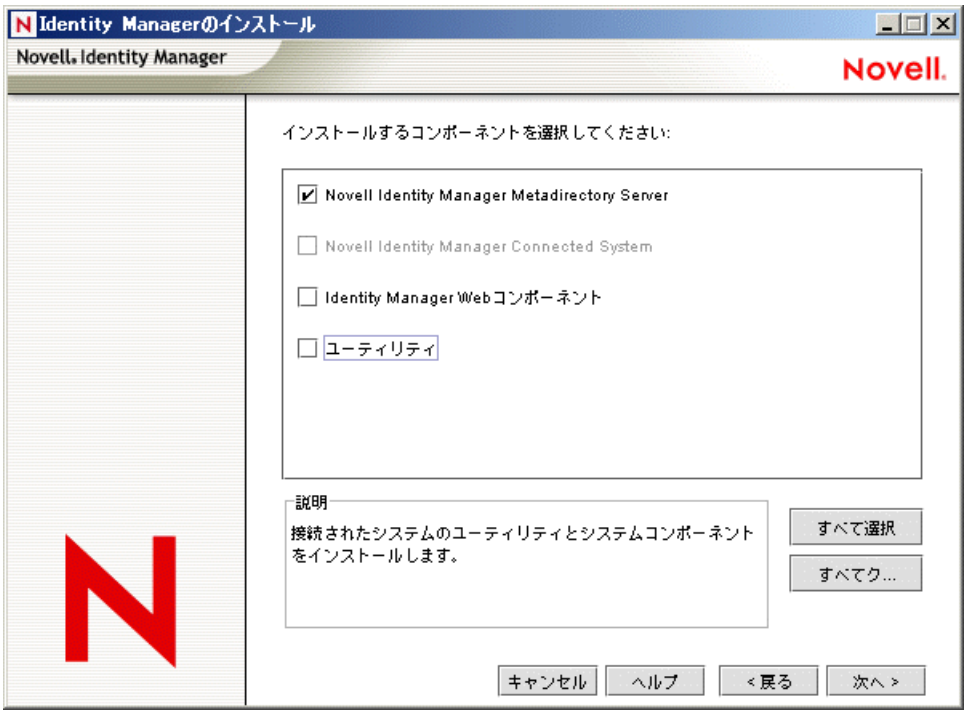
- 接続システムサーバ

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
- ユーティリティ

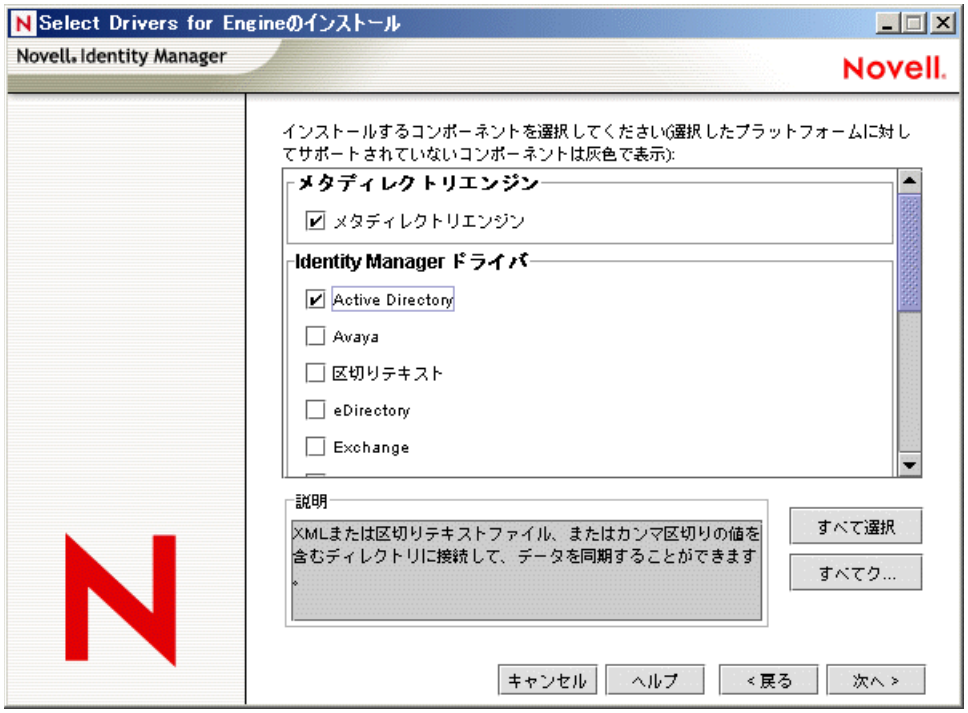
5 ［インストールするコンポーネントを選択してください］ダイアログボックスで、［メタディレクトリサーバ］を選択し、［次へ］をクリックします。



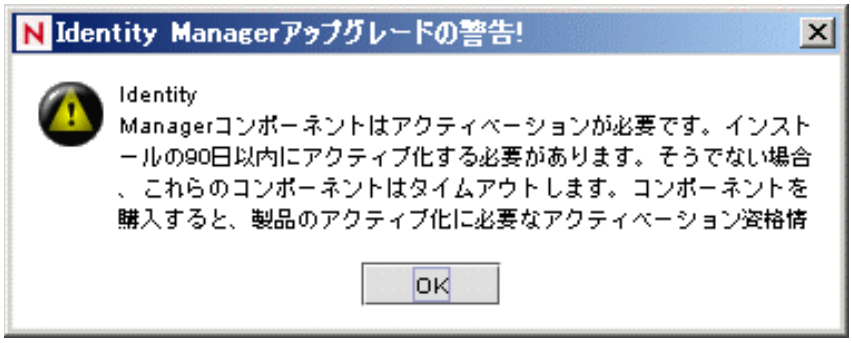
iManager がこのコンピュータにすでにインストールされており、このときに iManager プラグインと環境設定ファイルをインストールする場合は、［Identity Manager Web コンポーネント］も選択します。

このときに Active Directory 管理ツールをインストールする場合は、［ユーティリティ］も選択します。

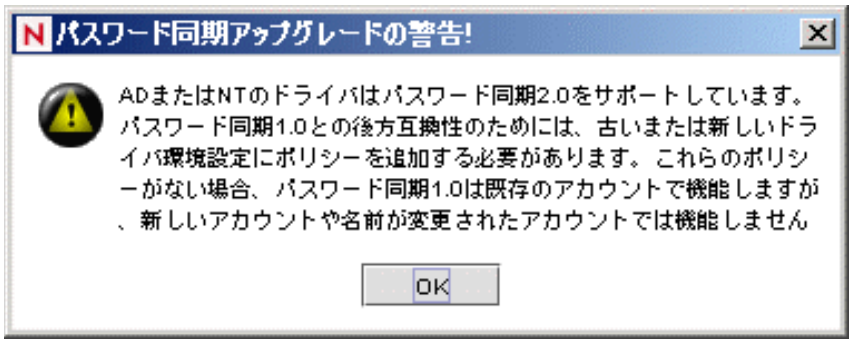
6 エンジンインストールのドライバを選択するダイアログボックスで、［メタディレクトリエンジン］を選択し、［Active Directory］を選択して、［次へ］をクリックします。



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 ［パスワード同期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。



9 ［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。

10 選択したオプションを確認して、［完了］をクリックします。

3.2.2 リモートローダへのシムのインストール

このオプションを使用すると、メタディレクトリエンジンを実行するサーバとは別のサーバで実行する Active Directory ドライバシムをインストールできます。

1 リモートローダが実行しているサーバで Identity Manager のインストールを開始します。

Identity Manager 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。

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。

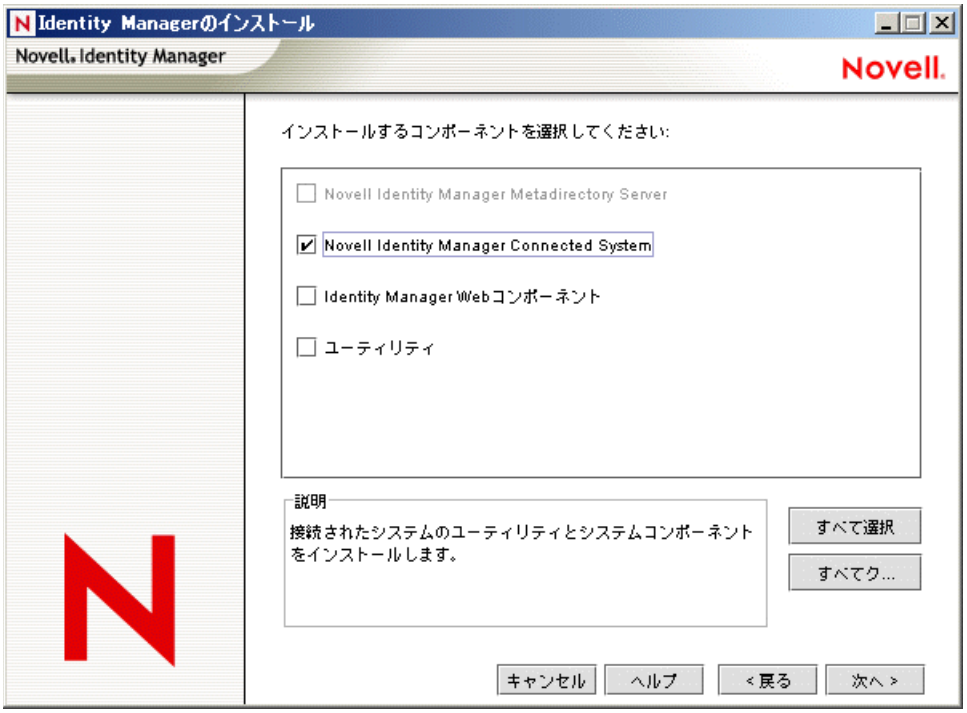
- メタディレクトリサーバ
- 接続システムサーバ

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。

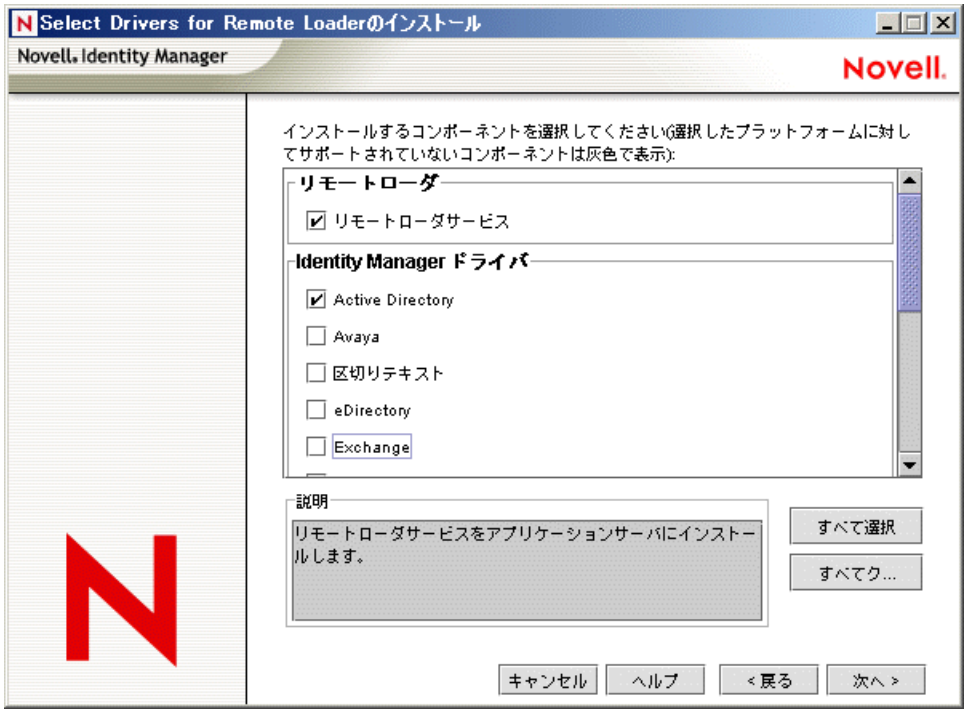
- Web ベースの管理サーバ
- ユーティリティ

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］ダイアログボックスで、［メタディレクトリサーバ］およびその他のオプションを選択解除し、［Novell Identity Manager Connected System］を選択して、［次へ］をクリックします。

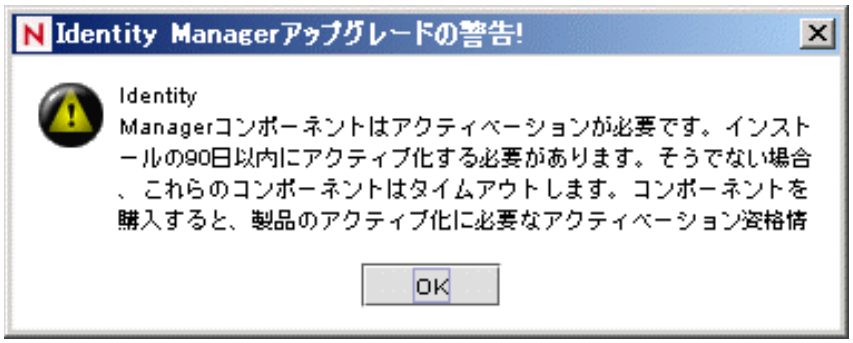


6 インストールパスを指定して、［OK］をクリックします。

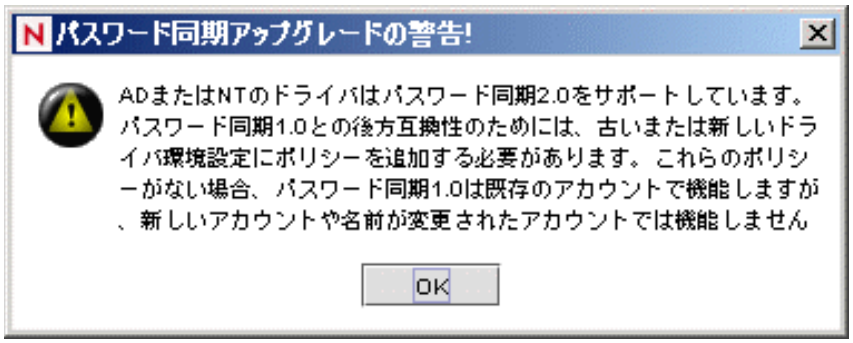
7 エンジンインストールのドライバを選択するダイアログボックスで、［リモートローダサービス］を選択し、［Active Directory］を選択して、［次へ］をクリックします。



8 ［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。



9 ［パスワード同期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。



10 選択したオプションを確認して、［終了］をクリックします。

3.3 設定済みのインポートファイルのインストール

このオプションでは、Identity Manager のプラグインと設定済みの (サンプル) ドライバ環境設定がインストールされます。ファイルをインストールしたら、iManager を使用して Active Directory の設定済みのファイルをドライバセットにインポートして、ドライバを設定します。

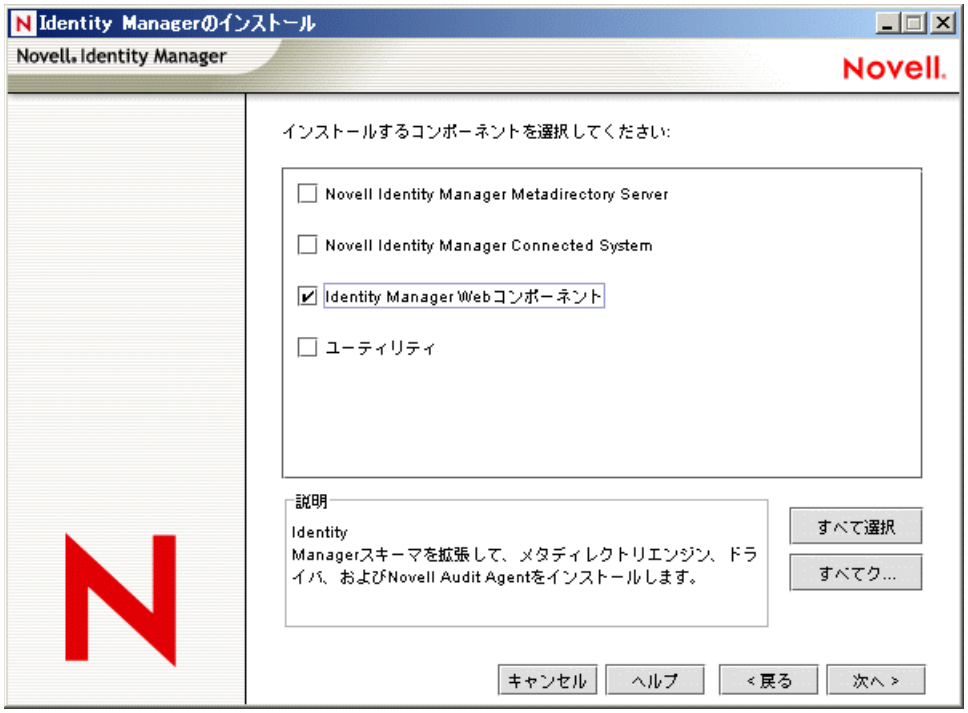
これらのファイルは、メタディレクトリエンジンまたはリモートローダをインストールした時点ですでにインストールされている場合があります。こうしたファイルを別にインストールする

1 iManager がインストールされているサーバで、Identity Manager のインストールを開始します。

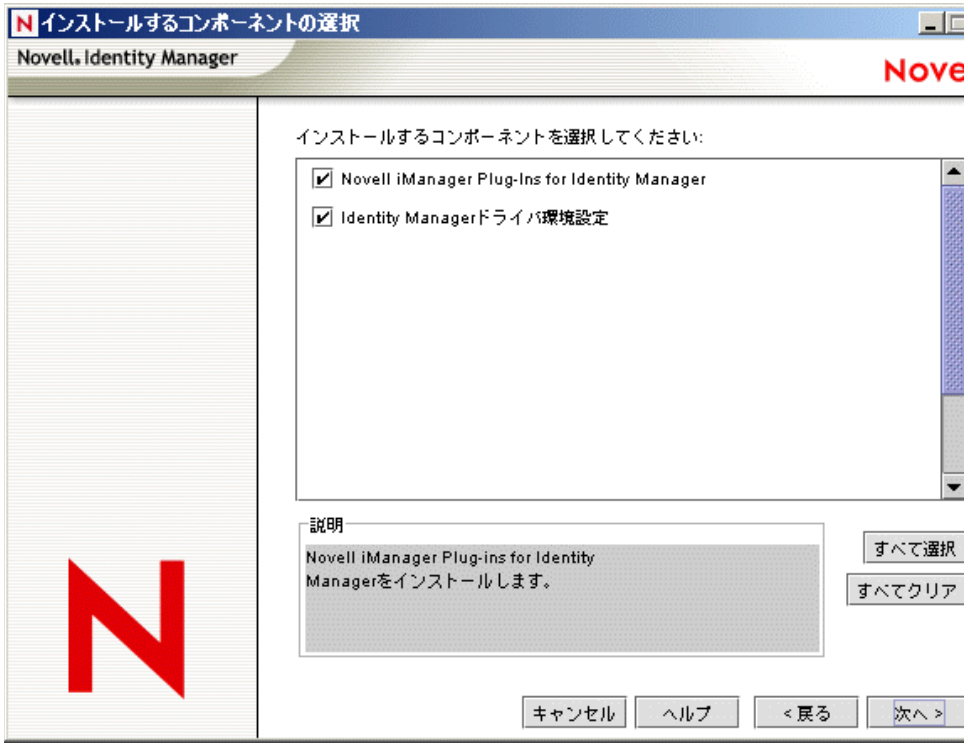
2 ［ようこそ］ダイアログボックスで、［次へ］をクリックして、使用許諾契約に同意します。

3 2 つの［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。

4 ［インストールするコンポーネントを選択してください］ダイアログボックスで、［Identity Manager Web コンポーネント］以外のすべてのオプションを選択解除して、［次へ］をクリックします。



5 ［Identity Manager ドライバ環境設定］を選択して、［次へ］をクリックします。



Novell iManager プラグインをインストールするときにドライバ環境設定ファイルをインストールできます。あるいは、環境設定ファイルを別途インストールできます。

6 選択したオプションを確認して、［完了］をクリックします。

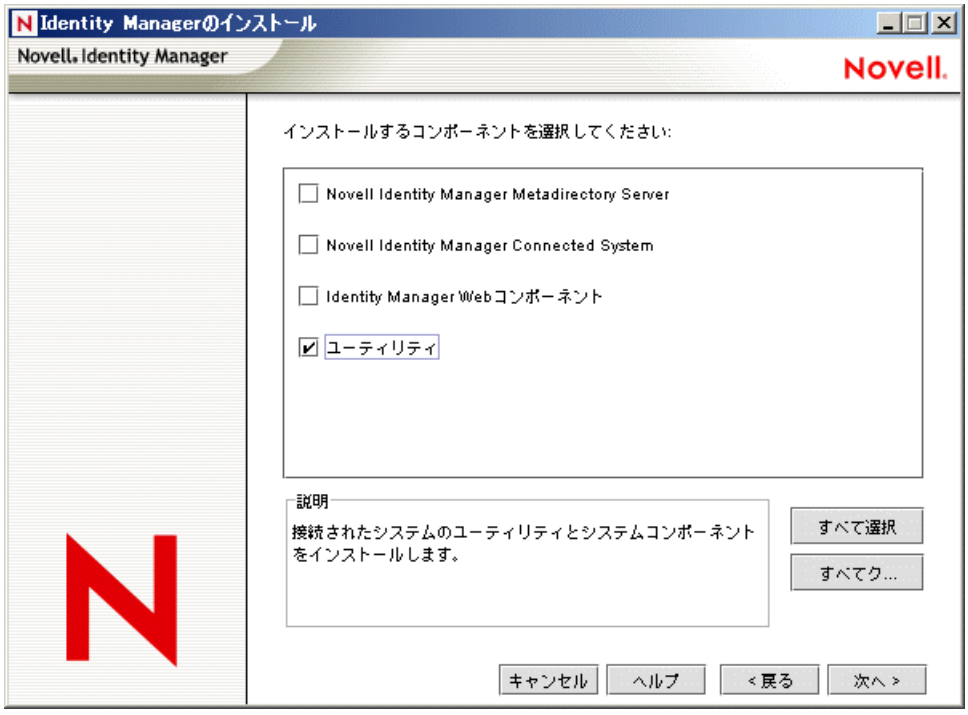
3.4 Active Directory ディスカバリツールのインストール

1 Active Directory の設定に使用するワークステーションで、Identity Manager のインストールを開始します。

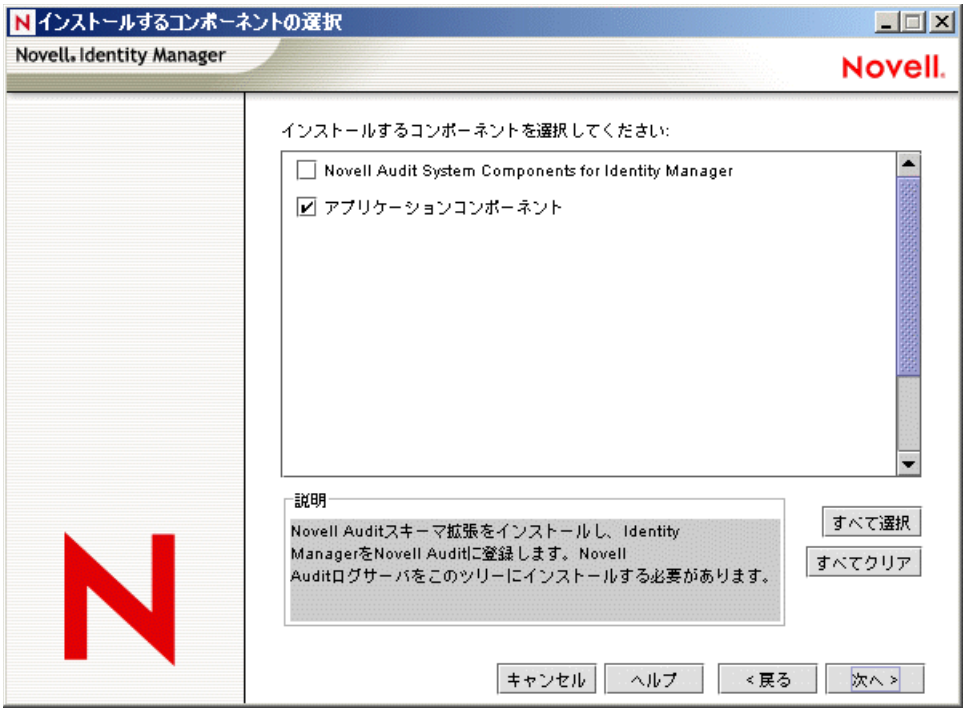
2 ［ようこそ］ダイアログボックスで、［次へ］をクリックして、使用許諾契約に同意します。

3 2 つの［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。

4 ［インストールするコンポーネントを選択してください］ダイアログボックスで、［ユーティリティ］以外のすべてのオプションを選択解除して、［次へ］をクリックします。



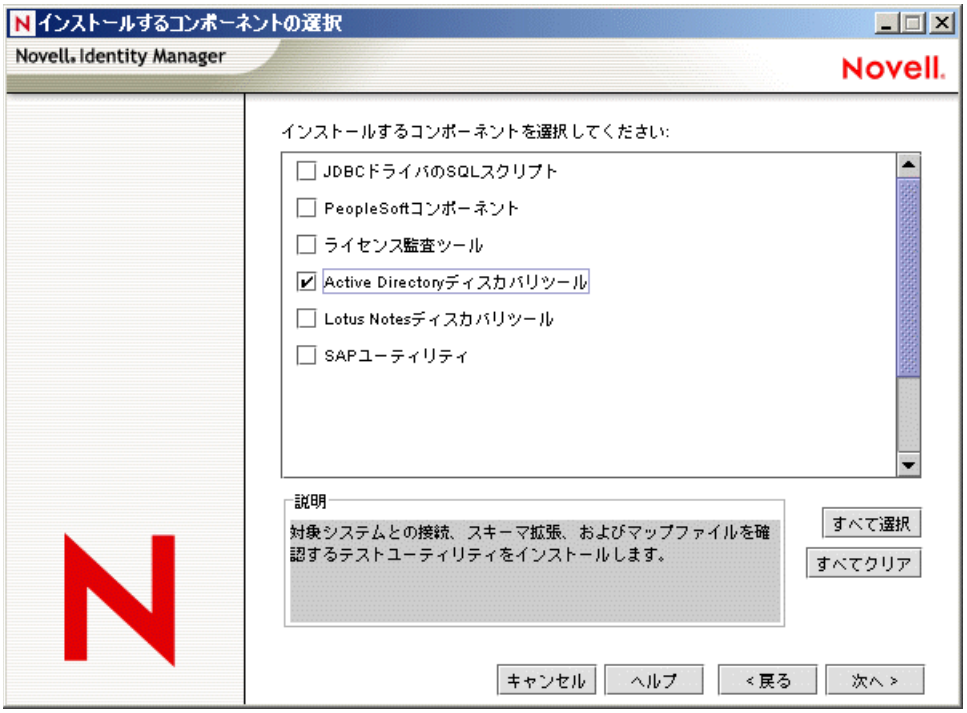
5 ［アプリケーションコンポーネント］を選択して、［次へ］をクリックします。



［Novell Audit System Components for Identity Manager］を選択解除します。

6 インストールパスを指定して、［OK］をクリックします。

7 ［Active Directory ディスカバリツール］だけを選択して、［次へ］をクリックします。



8 選択したオプションを確認して、［完了］をクリックします。

Active Directory ドライバの設定

4

Novell® iManager では、ドライバ作成ウィザードで Active Directory の基本的なドライバ環境設定をインポートできます。このウィザードで、ドライバを正常に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。このウィザードの使用に関する詳細については、『Novell Identity Manager 3.0 管理ガイド』の「ドライバの作成と設定」を参照してください。

この節では、次の項目について説明します。

4.1 Designer でのドライバ環境設定ファイルのインポート

Designer を使用すると、Active Directory の基本的なドライバ環境設定ファイルをインポートできます。このファイルを使用して、ドライバを正常に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、ドライバを作成してドライバの環境設定をインポートする方法を示しています。

ドライバ環境設定ファイルをインポートする方法には、さまざまなものがあります。この手順は、1 つの方法だけを示しています。

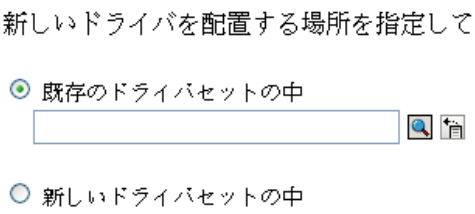
1. Designer およびモデラーで、［ドライバセット］オブジェクトを右クリックして、［Add Connected Application (接続アプリケーションの追加)］を選択します。
2. ドロップダウンリストから、［ActiveDirectory.xml］を選択して、［実行］をクリックします。
3. ［Perform Prompt Validation (プロンプト検証の実行)］ウィンドウで、［はい］をクリックします。この操作により、Active Directory ドライバを正しく設定するためにすべてのフィールドに入力できるようになります。
4. フィールドに入力してドライバを設定します。環境に特有の情報を指定します。設定の詳細については、40 ページのセクション 4.3「環境設定パラメータ」を参照してください。
5. 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。
6. ドライバがインポートされたら、ドライバをカスタマイズしてテストします。
7. ドライバを十分にテストしたら、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 Driver to an Identity Vault」を参照してください。

4.2 iManager でのドライバ環境設定ファイルのインポート

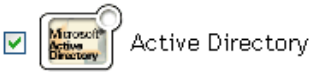
Active Directory の設定済みの環境設定ファイルはサンプル環境設定ファイルです。このファイルは、iManager サーバに Identity Manager Web コンポーネントをインストールした

ときにインストールされます。設定済みの環境設定ファイルは、インポートして各自の環境に合わせてカスタマイズまたは設定するテンプレートと考えてください。

1. iManager で、［Identity Manager ユーティリティ］>［ドライバのインポート］の順に選択します。
2. ドライバセットを選択し、［次へ］をクリックします。

   このドライバを新しいドライバセットに配置する場合は、ドライバセット名、コンテキスト、および関連サーバを指定する必要があります。
3. ［Active Directory］ドライバを選択して、［次へ］をクリックします。

4. 環境設定パラメータを入力してドライバを設定します。設定の詳細については、40 ページのセクション 4.3「環境設定パラメータ」を参照してください。
5. ドライバに必要なサーバ上の権限を備えたユーザオブジェクトを使用して同等セキュリティを定義します。

   この作業では、Admin ユーザオブジェクトを使用する傾向が見られます。しかし、たとえば DriversUser を作成して、そのユーザに同等セキュリティを割り当てた方がよい場合があります。ドライバに必要なサーバ上の権限が何であっても、DriversUser オブジェクトには同じセキュリティ権限が必要です。
6. 管理の役割を表すすべてのオブジェクトを指定して、それらをレプリケーションから除外します。

   ステップ 2 で指定した同等セキュリティオブジェクト (DriversUser など) を除外します。同等セキュリティオブジェクトを削除すると、ドライバから権限が削除されます。したがって、ドライバで Identity Manager に変更を加えることができません。
7. ［終了］をクリックします。

4.3 環境設定パラメータ

次の表は、最初のドライバ環境設定時に指定する必要があるパラメータを示しています。

注 **:** パラメータは複数の画面で提示されますが、前のプロンプトに対する回答で、ポリシーを正しく設定するために詳細な情報が必要な場合は、一部のパラメータのみが表示されます。

表 *4-1* 環境設定パラメータ

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 eDirectory™ オブジェクト名。 各 Active Directory ドメインには個別のドライバが必要となるため、ドライバ名にドメイン名を含める必要があります。ドライバを調べると、それがどのドメインに関連付けられているかがわかります。
認証方式	Active Directory で認証する方式。 ［ネゴシエーション］が、優先される方式です。Microsoft セキュリティパッケージを使用して認証をネゴシエートする場合に［ネゴシエーション］を選択しします。［ネゴシエーション］を使用するには、ドライバをホストするサーバがドメインのメンバーである必要があります。 パスワード同期を使用してメンバーサーバで実行している場合は、SSL が必要です。 ［シンプル］では、LDAP の単純なバインドを使用します。［シンプル］を選択する場合は、SSL をお勧めします。 **重要 :** ［シンプル］バインドでは、パスワード同期および Exchange プロビジョニングをサポートしていません。
認証 ID	Identity Manager で使用される管理者特権を備えた Active Directory アカウント。使用される名前形式は、選択した認証メカニズムによって異なります。 ［ネゴシエーション］の場合は、Active Directory 認証メカニズムで必要な名前形式を指定します。次に例を示します。 ◆ 管理者 - AD ログオン名 ◆ ドメイン / 管理者 - ドメイン修飾 AD ログオン名 ［シンプル］の場合は、LDAP ID を指定します。次に例を示します。 ◆ cn=DirXML,cn=Users,DC=domain,dc=com
認証パスワード	認証 ID で指定したユーザアカウントのパスワード。
認証コンテキスト	同期に使用する Active Directory ドメインコントローラの名前。 たとえば、［ネゴシエーション］認証方式の場合は、DNS 名 mycontroller.domain.com を使用します。［シンプル］認証方式の場合は、サーバの IP アドレス (10.10.128.23 または DNS 名) を使用できます。 値を指定しない場合は、localhost が使用されます。 **注 :** この値は、認証コンテキスト属性に保存されます。最初の環境設定後にこの値を変更するには、59 ページの 「セキュリティパラメータ」にある説明に従ってこの属性を変更します。
ドメイン名	このドライバで管理される Active Directory ドメイン。 ドライバでは、LDAP 形式のドメイン名 dc=domain,dc=com が必要です。

フィールド	説明
ドメイン DNS 名	このドライバで管理される Active Directory ドメインの DNS 名。 ドライバでは、DNS 形式のドメイン名 domain.com が必要です。
ドライバのポーリング間隔	アイデンティティボールトから Active Directory に変更がそのまま送信されます。ただし、Active Directory に対する変更は、設定されたポーリング間隔と同じ頻度でのみアイデンティティボールトに送信されます。デフォルトは 1 分です。 **重要 :** このポーリング間隔は、システム パフォーマンスに影響します。ポーリング間隔が短いと、データが頻繁に検索され、早く更新されます。ポーリング間隔が長いと、トラフィックが周期的に増大します。ポーリング間隔の短い方が全体的なコストは大きくなりますが、コストは時間の経過とともに均一になります。 ポーリング間隔を 0 (ゼロ) に設定すると、10 秒間隔になります。
パスワード同期のタイムアウト (分)	ドライバがパスワードの同期を試みる時間 (分)。 どんなパスワードの一時的なバックログでも処理できる十分に大きい値を設定します。一括変更する場合は、すべての変更を処理できるようにタイムアウトを大きく設定します。経験的には、パスワードあたりに 1 秒を考慮します。たとえば、18,000 のパスワードを同期するには、300 分 (18,000 パスワード /60 秒) を考慮します。 -1 を設定すると無期限になります。この設定で一括変更を処理できますが、問題が生じる場合があります。たとえば、アカウントが関連付けられていないため、パスワードを同期できないことがあります。したがって、そのようなパスワードは永久にシステムに残ります。同様の状況が数多い場合、同期されていない大量のパスワードはシステムで保持することになります。 パスワード同期のタイムアウトを少なくともポーリング間隔の 3 倍に設定する必要があります。
ドライバの選択 (ローカル / リモート)	[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] オプションのみ。 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。デフォルトのポートは 8090 です。 この設定は、[ドライバの選択 (ローカル / リモート)] を [リモート] に設定した場合にのみ表示されます。
ドライバパスワード	[リモート] オプションのみ。 ドライバオブジェクトパスワードは、リモートローダが Identity Manager 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。このパスワードには、リモートローダ上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。 この設定は、[ドライバの選択 (ローカル / リモート)] を [リモート] に設定した場合にのみ表示されます。

フィールド	説明
リモートパスワード	［リモート］オプションのみ。 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。このパスワードには、リモートローダ上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。 この設定は、［ドライバの選択 (ローカル / リモート)］を［リモート］に設定した場合にのみ表示されます。
インポート作業は、ドライバポリシーの選択に進みます	［リモート］オプションのみ。 ［OK］をクリックすると、ドライバウィザードがドライバのポリシーの環境設定を続行します。
eDirectory のベースコンテナ	同期に備えてアイデンティティボールトのベースコンテナを指定します。このコンテナは、アイデンティティボールトブジェクトの同期を制限する購読者一致ポリシー、およびアイデンティティボールトにオブジェクトを追加するときの発行者配置ポリシーで使用されます。 新規ユーザは、デフォルトではこのコンテナに格納されます。ドット形式を使用してください。例 : users.myorg コンテナが存在しない場合は、それを作成し、Active Directory ベースコンテナに関連付けられていることを確認してから、このコンテナにユーザを追加する必要があります。
発行者の配置	［ミラーリング済み］では、オブジェクトがベースコンテナ内に階層的に配置されます。 ［平面］では、オブジェクトがベースコンテナ内に階層なしで完全に配置されます。 この選択により、デフォルトの発行者配置ポリシーが構築されます。 **注 :** ［ミラーリング済み］を選択した場合、ドライバでは、eDirectory データベースの構造が eDirectory ベースコンテナの Active Directory での構造と同じであると見なします。構造が同じでない場合、オブジェクトは正しく配置されません。eDirectory 内の構造と同じ構造を Active Directory で作成するか、または eDirectory コンテナを移行してからユーザオブジェクトを移行します。
Active Directory のベースコンテナ	Active Directory のベースコンテナを LDAP 形式で指定します。新規ユーザは、デフォルトではこのコンテナに格納されます。例 : CN=Users,DC=MyDomain,DC=com ターゲットコンテナが存在しない場合は、それを作成し、eDirectory ベースコンテナに関連付けられていることを確認してから、このコンテナにユーザを追加する必要があります。 Active Directory のユーザ以外のコンテナを作成または使用している場合、コンテナは CN ではなく OU です。例 : OU=Sales,OU=South,DC=MyDomain,DC=com

フィールド	説明
Active Directory の配置	［ミラーリング済み］では、オブジェクトがベースコンテナ内に階層的に配置されます。 ［平面］では、オブジェクトがベースコンテナ内に階層なしで完全に配置されます。 この選択により、デフォルトの購読者配置ポリシーが構築されます。 **注 :** ［ミラーリング済み］を選択した場合、ドライバでは、Active Directory データベースの構造が Active Directory ベースコンテナの eDirectory での構造と同じであると見なします。構造が同じでない場合、オブジェクトは正しく配置されません。Active Directory 内の構造と同じ構造を eDirectory で作成するか、または Active Directory コンテナを移行してからユーザオブジェクトを移行します。
データフローの設定	［データフローの設定］では、同期される属性およびクラスを制御する最初のドライバフィルタを確立します。このオプションの目的は、一般的なデータフローポリシーを最もよく表すようにドライバを設定することです。特定の要件を反映するように、このオプションをインポート後に変更できます。 ［Bidirectional (双方向)］では、発行者チャネルと購読者チャネルの両方で同期するようにクラスと属性を設定します。アイデンティティボールトまたは Active Directory での変更は相手側に反映されます。両方を信頼されるデータソースにしたい場合に、このオプションを使用します。 ［AD からボールトへ］では、発行者チャネルだけで同期するようにクラスと属性を設定します。Active Directory での変更はアイデンティティボールトに反映されますが、アイデンティティボールトでの変更は無視されます。Active Directory を信頼されるデータソースにしたい場合に、このオプションを使用します。 ［ボールトから AD へ］では、購読者チャネルだけで同期するようにクラスと属性を設定します。アイデンティティボールトでの変更は Active Directory に反映されますが、Active Directory での変更は無視されます。ボールトを信頼されるデータソースにしたい場合に、このオプションを使用します。 **警告 :** 削除。「移動」イベントと「リネーム」イベントはフィルタとは無関係です。どのオプションを選択するかにかかわらず、これらのイベントはドライバで処理されます。これらのイベントを同期させない場合は、ドライバのデフォルトの環境設定を変更する必要があります。 Identity Manager 3.0 に付属している定義済みのポリシーのいずれかを使用して、「削除」イベントを「関連付けを削除」イベントに変更できます。詳細については、『Policy Builder and Driver Customization Guide』の「Command Transformation - Publisher Delete to Disable」を参照してください。 「移動」イベントと「リネーム」イベントをブロックするには、ドライバをカスタマイズ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	パスワード同期のポリシーは、パスワードの更新に失敗したときに電子メール通知を関連ユーザに送信するように設定されています。選択によって通知電子メールのコピーを別のユーザ (セキュリティ管理者など) に送信できます。コピーを送信する場合は、そのユーザの DN を入力または参照します。送信しない場合は、このフィールドを空白のままにします。

フィールド	説明
エンタイトルメントの設定	ドライバを設定すれば、エンタイトルメントを使用して Active Directory のユーザアカウントやグループメンバーシップを管理したり、Exchange メールボックスをプロビジョニングすることができます。エンタイトルメントを使用すると、ドライバは、Identity Manager ユーザアプリケーションまたは役割ベースエンタイトルメントなどの外部サービスと連動して、これらの機能を Active Directory でプロビジョニング / プロビジョニング解除する条件を制御します。詳細については、15 ページの 「エンタイトルメント」を参照してください。 このいずれかの外部サービスを利用して Active Directory へのプロビジョニングを制御する場合は、［はい］を選択します。 Identity Manager ユーザアプリケーションの使用および Exchange メールボックスのプロビジョニングを行わない場合は、［いいえ］を選択します。
ユーザアカウントポリシー	［要素］オプションだけを設定します。 Active Directory でのユーザアカウントは、ワークフローサービスや役割ベースエンタイトルメントとエンタイトルメントの併用、または同期により制御できます。 ［エンタイトルメント］により、アイデンティティボールト内のエンタイトルメントに対する Active Directory のアカウントの有効化を制御できます。 ［ポリシーで実装する］では、エンタイトルメントの代わりにドライバでポリシーを使用します。
Exchange ポリシー	［要素］オプションだけを設定します。 Exchange プロビジョニングは、ドライバポリシーまたはエンタイトルメントで処理するか、あるいはすべてスキップすることができます。ユーザ (メールボックスが有効なユーザ) に Exchange のメールボックスを割り当てるか、またはユーザ (メールボックスが有効なユーザ) が外部メールボックスに関する情報をアイデンティティボールトレコードに格納させることができます。ドライバポリシーを使用する場合は、ユーザに対してメールボックスまたはメールのどちらを有効にするかの決定、およびアカウントが存在する Exchange メッセージデータベースは、ポリシーで完全に制御されます。 ［エンタイトルメント］を使用すると、ワークフローサービスや役割ベースエンタイトルメントのような外部サービスでこうした決定が行われ、ドライバポリシーはそれらに適用されるだけです。 ［ポリシーで実装する］では、エンタイトルメントの代わりにドライバでポリシーを使用して Exchange メールボックスが割り当てられます。 ［なし］が選択されると、デフォルトの環境設定では Exchange メールボックスは作成されず、Active Directory メール属性でアイデンティティボールトインターネット電子メールアドレスが同期されます。

フィールド	説明
グループメンバーシップポリシー	［要素］オプションだけを設定します。 Active Directory でのグループメンバーシップは、メンバーシップリストを同期するか、エンタイトルメントを使用して制御できます。 ［エンタイトルメント］では、ワークフローサービスまたは役割ベースエンタイトルメントを使用してグループメンバーシップが割り当てられます。 ［同期］では、ポリシーを使用してグループメンバーシップリストが同期されます。 ［なし］では、グループメンバーシップ情報が同期されません。
CDOEXM for Exchange を使用する (はい / いいえ)	［Exchange ポリシー］オプションのみ。 Exchange メールボックスは、正規の属性同期ではなく Microsoft Exchange 管理システムの呼び出しによって制御できます。有効にすると、ドライバシムは Active Directory の homeMDB 属性への変更を行わずに、CDOEXM (Collaboration Data Objects for Exchange Management) サブシステムを呼び出します。 ここで選択した値は、ドライバシムの環境設定に記録されます。 ［はい］では、Exchange メールボックスが同期されます。 ［いいえ］では、Exchange メールボックスが同期されません。
CDOEXM で Exchange メールボックスを移動できるようにする (はい / いいえ)	［Exchange ポリシー］オプションのみ。 有効にすると、ドライバシムは Active Directory の homeMDB 属性を変更せずに、CDOEXM を呼び出すことでメールボックスを新しいメッセージデータストアに移動します。 ［はい］では、Exchange メールボックスが移動されます。 ［いいえ］では、Exchange メールボックスが移動されません。
CDOEXM で Exchange メールボックスを削除できるようにする (はい / いいえ)	［Exchange ポリシー］オプションのみ。 有効にすると、ドライバシムは Active Directory の homeMDB 属性を削除せずに、CDOEXM を呼び出すことでメールボックスを削除します。 ［はい］では、Exchange メールボックスを削除できます。 ［いいえ］では、Exchange メールボックスを削除できません。
デフォルトの Exchange MDB	［Exchange ポリシー］> ［ポリシーで実装する］オプションのみ。 デフォルトの Exchange メッセージデータベース (MDB) を入力します。例 : [CN=Mailbox Store (CONTROLLER),CN=First Storage Group,CN=InformationStore,CN=CONTROLLER,CN=Servers,CN=First Administrative Group,CN=Administrative Groups,CN=Domain,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=Domain,DC=com] インポートが完了したら、追加 MDB を管理するためにドライバを更新できます。

フィールド	説明
アカウントのエンタイトルメントが取り消された場合	［Exchange ポリシー］オプションのみ。 エンタイトルメントでユーザアカウントを削除するときに実行するアクションを選択できます。 *アカウントを無効にする* *アカウントを削除する*
ネームマッピングポリシーの選択 >	ドライバにより、アイデンティティボールトのフルネーム属性が Active Directory のオブジェクト名にマップされ、Active Directory の旧 Windows 2000 ログオン名がアイデンティティボールトユーザ名にマップされます。 ポリシーのフル機能を受諾することも、ポリシーの一部を手動選択することもできます。ポリシーがニーズを満たしていない場合は、インポート完了後に購読者および発行者のコマンド変換ポリシーの NameMap ポリシーを編集することで、ポリシーを変更できます。 ［受諾］では、ポリシーのフル機能が使用されます。 ［手動］では、ポリシーの一部を使用できます。
フルネームでマッピング	［ネームマッピングポリシーの選択］>［手動］オプションのみ。 ［はい］では、ドライバで、アイデンティティボールトの［フルネーム］属性と Active Directory のオブジェクト名および表示名との同期を維持できます。 ［いいえ］では、ドライバで、アイデンティティボールトの［フルネーム］属性と Active Directory のオブジェクト名および表示名との同期は維持されません。 このポリシーは、Microsoft 管理コンソールの「ユーザとコンピュータ」スナップインを使用して、ユーザアカウントを Active Directory 内に作成するときに役立ちます。
ログオン名でマッピング	［ネームマッピングポリシーの選択］>［手動］オプションのみ。 ［はい］では、ドライバで、アイデンティティボールトのオブジェクト名と Active Directory の旧 Windows 2000 ログオン名 (別名 : NT ログオン名および sAMAccountName) との同期を維持できます。 ［いいえ］では、ドライバで、アイデンティティボールトのオブジェクト名と Active Directory の旧 Windows 2000 ログオン名との同期は維持されません。
Import will proceed to Windows 2000 logon name policy selections (インポート作業は Windows 2000 ログオン名ポリシーの選択に進みます)	［ネームマッピングポリシーの選択］>［手動］オプションのみ。 *OK*

フィールド	説明
ユーザプリンシパル名のマッピング	Active Directory の Windows 2000 ログオン名 (別名 : userPrincipalName) の管理方法を選択できます。userPrincipalName は、「usere@domain.com」のような電子メールアドレス形式にします。シムでは、userPrincipalName に任意の値を配置できますが、名前を使用したドメイン名を受け付けるようにドメインが設定されていないと、ログオン名としては使い勝手が悪くなります。 ［Active Directory の電子メールアドレスに従う］では、userPrincipalName が Active Directory のメール属性値に設定されます。このオプションは、認証にユーザの電子メールアドレスを使用する場合や、Active Directory で電子メールアドレスが信頼される場合に役立ちます。 ［アイデンティティボールトの電子メールアドレスに従う］では、userPrincipalName がアイデンティティボールトの電子メールアドレス属性値に設定されます。このオプションは、認証にユーザの電子メールアドレスを使用する場合や、アイデンティティボールトで電子メールアドレスが信頼される場合に役立ちます。 ［アイデンティティボールト名に従う］は、ユーザログオン名とポリシーに定義されたハードコード文字列から userPrincipalName を生成する場合に役立ちます。 ［なし］は、userPrincipalName を制御しない場合や独自のポリシーを実装する場合に役立ちます。

Active Directory ドライバのアップグレード

5

5.1 アップグレード用のチェックリスト

Active Directory ドライバをアップグレードするには、次のチェックリストを使用します。Identity Manager に詳しくない場合は、有能なコンサルタントを雇った方がよい場合があります。

- ❑ Password Synchronization 2.0, を使用するには、ドライバマニフェストとパスワードポリシーを追加します。

  「Upgrading an Existing Driver Configuration to Support Identity Manager Password Synchronization (http://www.novell.com/documentation/dirxml20/index.html?page=/documentation/dirxml20/admin/data/bo16oyy.html)」を参照してください。
- ❑ Password Synchronization 1.0 を引き続き使用する場合は、既存のドライバ環境設定に従来のポリシーを追加します。

  「Upgrading Password Synchronization 1.0 to Password Synchronization Provided with Identity Manager (http://www.novell.com/documentation/dirxmldrivers/index.html?page=/documentation/dirxmldrivers/ad/data/bnwjt02.html)」を参照してください。
- ❑ 既存のドライバのスタイルシートにある構造化された形式の sAMAccountName を削除します。

  sAMAccountName は、DirXML® 1.1a の Active Directory 2.0 ドライバにおける構造化された属性でした。新しい Active Directory 3.0 ドライバでは、この属性は文字列です。

  古い形式

  ```
  <value type="structured"> <component name="nameSpace">0</
  component> <component association-
  ref="XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX" name="volume"/> <component
  name="path">jsmith</component> </value>
  ```

  新しい形式

  ```
  <add-attr attr-name="sAMAccountName"> <value
  type="string">jsmith</value> </add-attr>
  ```

- ❑ ドライバ環境設定パラメータをアップグレードします。

  次の設定をデフォルトで使用することをお勧めします。

  ```
  <?xml version="1.0"?> <driver-config name="Active Directory
  ```

```
Driver"> <driver-options> <pollingInterval display-name="Polling
Interval (min.)"> 1</pollingInterval> <auth-method display-
name="Authentication Method"> Negotiate</auth-method> <signing
display-name="Use Signing (yes/no)" id="> no</signing> <sealing
display-name="Use Sealing (yes/no)"> no</sealing> <use-ssl display-
name="Use SSL (yes/no)"> no</use-ssl> <pub-heartbeat-interval
display-name="Heart Beat"> 0</pub-heartbeat-interval> <pub-
password-expire-time display-name="Password Sync Timeout
(minutes):">60</pub-password-expire-time> <use-CDOEXM display-
name="Use CDOEXM for Exchange (yes/no)"> no</use-CDOEXM> <cdoexm-
move display-name="Allow CDOEXM Exchange mailbox move (yes/
no)">yes</cdoexm-move> <cdoexm-delete display-name="Allow CDOEXM
Exchange mailbox delete (yes/no)">yes</cdoexm-delete> </driver-
options> </driver-config>
```

- 認証IDをSamアカウント名(jsmithなど)またはドメイン名/アカウント名形式(ドメイン/jsmith など) に変換します。
- 「ログインの無効化」属性のマッピングを userAccountControl から dirxml-uACAccountDisable に変更します。
- Exchange アカウントをプロビジョニングしている場合は、CDOEXM のドライバパラメータを［はい］に変更して、既存のドライバ環境設定から次の 4 つのハードコードされた属性を削除します。
  - msExchHomeServerName
  - legacyExchangeDN
  - homeMTA
  - msExchMailboxSecurityDescriptor
- Identity Manager 2.x からアップグレードしている場合は、Exchange プロビジョニングを有効にして、オーバレイをドライバに適用する必要があります。Identity Manager 3.0 で、Exchange メールボックスによる移動と削除を制御します。この機能がアップグレードされたドライバで動作するように、オーバレイを適用する必要があります。オーバレイを適用する方法の詳細については、52 ページのセクション 5.5「Exchange メールボックスのオーバレイの適用」を参照してください。

5.2 ログインの無効化の値の対処

eDirectory™ では、ログインの無効化 = true がない場合は、ログインの無効化 = false と同じに処理されます。したがって、バージョン 3 の Active Directory ドライバをアップグレードではなく新規インストールとしてインストールし、ログインの無効化 = false という値が指定されていない場合は、作成ルールのデフォルトのポリシーでその値が合成されます。

バージョン 2 のドライバからバージョン 3 のドライバにアップグレードする場合、デフォルトではこのポリシーは取得されません。

5.3 DirXML 1.1a からのドライバシムのアップグレード

アップグレードすると、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、前のドライバの環境設定はそのまま使用されます。新しいドライバシムは、変更なしで DirXML 1.1a 環境設定を実行できます (ただし、Password Synchronization 1.0 を使用している場合は除きます)。

Password Synchronization 1.0 を引き続き使用する場合は、ドライバシムをアップグレードする必要はありません。DirXML 1.1a ドライバシムは Identity Manager 3.0 エンジンで実行しますが、Identity Manager 3.0 ドライバシムは DirXML1.1a エンジンでは実行できません。

ドライバシムをアップグレードしない場合は、Identity Manager 3.0 エンジンのインストール時に、Active Directory ドライバが選択解除されていることを確認します。Active Directory ドライバが選択されている場合、ドライバシムはアップグレードされます。

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。

   アップグレードの問題を最小限にするために、すべてのドライバにこの手順をお勧めします。

2. Identity Manager 3.0 ドライバシムをインストールします。この操作は、Identity Manager 3.0 エンジンのインストールと同時に実行できます。

   『Identity Manager 3.0 インストールガイド』の「Identity Manager のインストール」の節の手順に従ってください。

   警告 : Password Synchronization 1.0 を使用している場合は、67 ページのセクション 7.2「Identity Manager に付属のパスワード同期への Password Synchronization 1.0 のアップグレード」を読み、Password Synchronization 1.0 との後方互換性を保つためにドライバ環境設定にポリシーを追加する準備ができるまでは、Active Directory 用の Identity Manager ドライバをインストールしないでください。

   Identity Manager2.0 または 3.0 のドライバシムとドライバ環境設定を DirXML 1.1a エンジンで実行することはできません。

3. シムをインストールしたら、Novell eDirectory とドライバを再起動する必要があります。

   3a iManager で、［Identity Manager］>［Identity Manager の概要］の順にクリックします。

   3b ドライバが存在するドライバセットを参照し、［検索］をクリックします。

   3c ドライバアイコンの右上隅をクリックし、［ドライバの再起動］をクリックします。

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。

   63 ページのセクション 6.4「ドライバを有効にする」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、39 ページの第 4 章「Active Directory ドライバの設定」に進みます。

5.4 IDM 2.*x* からのドライバシムのアップグレード

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。

アップグレードの問題を最小限にするために、すべてのドライバにこの手順をお勧めします。

2 Identity Manager 3.0 ドライバシムをインストールします。この操作は、Identity Manager 3.0 エンジンのインストールと同時に実行できます。

『Identity Manager 3.0 インストールガイド』の「Identity Manager のインストール」の節の手順に従ってください。

警告 **:** Password Synchronization 1.0 を使用している場合は、67 ページのセクション 7.2「Identity Manager に付属のパスワード同期への Password Synchronization 1.0 のアップグレード」を読み、Password Synchronization 1.0 との後方互換性を保つためにドライバ環境設定にポリシーを追加する準備ができるまでは、Active Directory 用の Identity Manager ドライバをインストールしないでください。

Identity Manager ドライバシムとドライバ環境設定を DirXML 1.1a エンジンで実行することはできません。

3 シムをインストールしたら、Novell eDirectory とドライバを再起動する必要があります。『Novell Identity Manager 3.0 管理ガイド』の「ドライバの起動、停止、または再起動」の手順に従ってください。

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。

63 ページのセクション 6.4「ドライバを有効にする」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、39 ページの第 4 章「Active Directory ドライバの設定」に進みます。

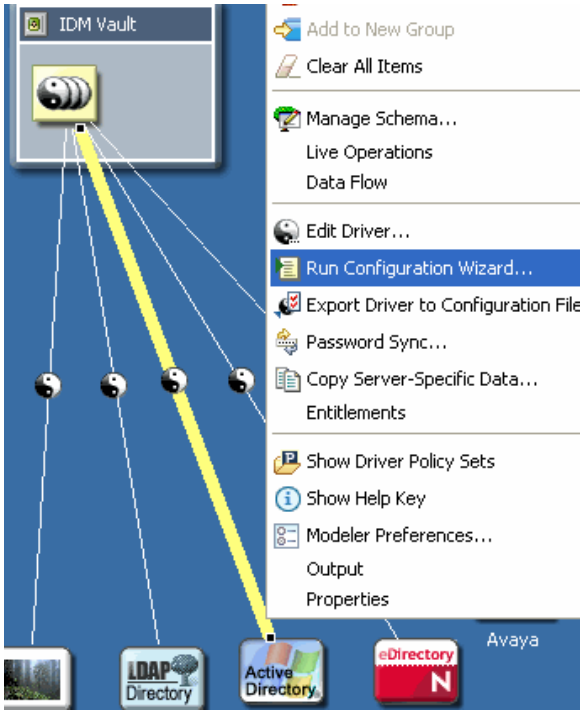
5.5 Exchange メールボックスのオーバレイの適用

Identity Manager 2.x から Identity Manager 3.0 にアップグレードした場合は、ドライバで Exchange プロビジョニングを有効にする際に AD ドライバオーバレイを適用する必要があります。オーバレイを使用すると、ドライバで Exchange メールボックスによる削除と移動を制御できます。

- 53 ページのセクション 5.5.1「Designer でのオーバレイの適用」
- 56 ページのセクション 5.5.2「iManager でのオーバレイの適用」

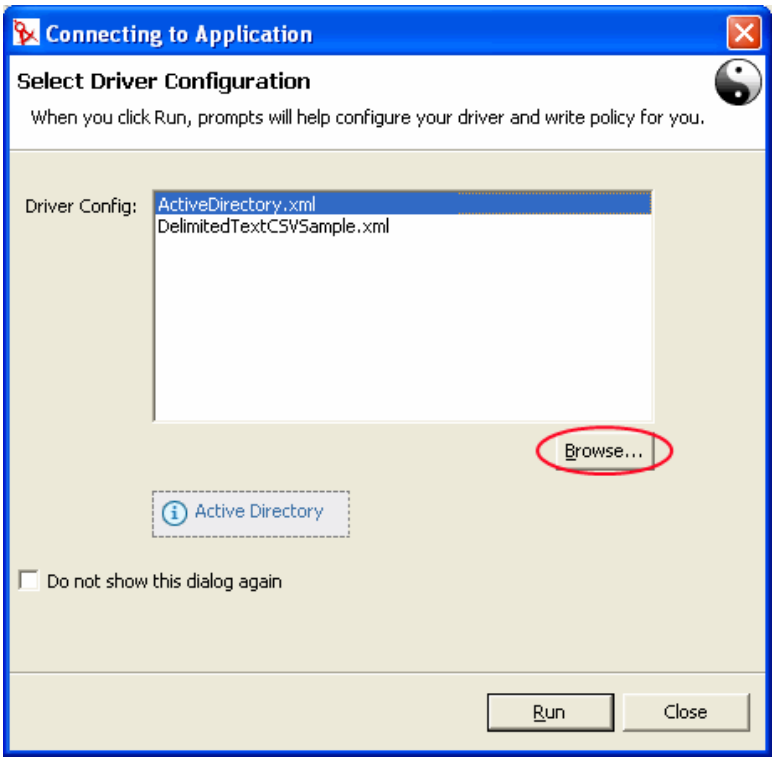
5.5.1 Designer でのオーバレイの適用

1 モデラーで、AD ドライバコネクタアイコンを右クリックして、[Run Configuration Wizard (環境設定ウィザードの実行)] をクリックします。



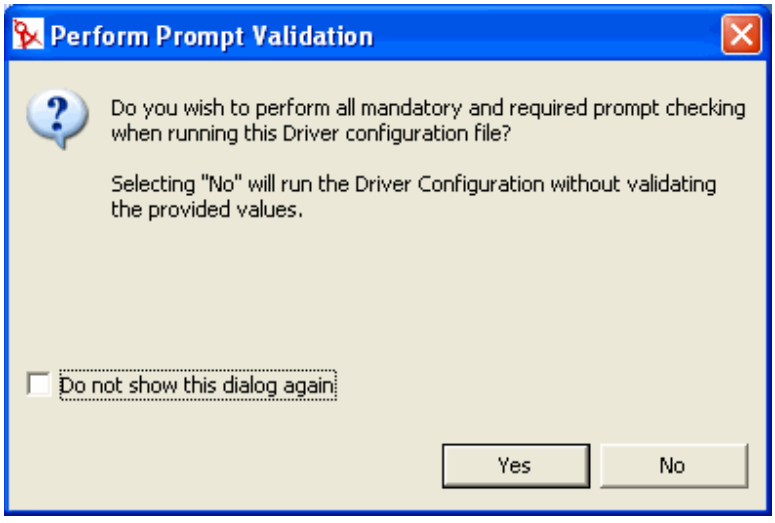
2 [参照] を選択してファイル ActiveDirectoryUpdate.xml を参照し、[開く] をクリックします。

このファイルは、次のプラグイン eclipse\plugins\com.novell.designer.idm_*x.x.x*\defs\ActiveDirect oryUpdate.xml にあります。



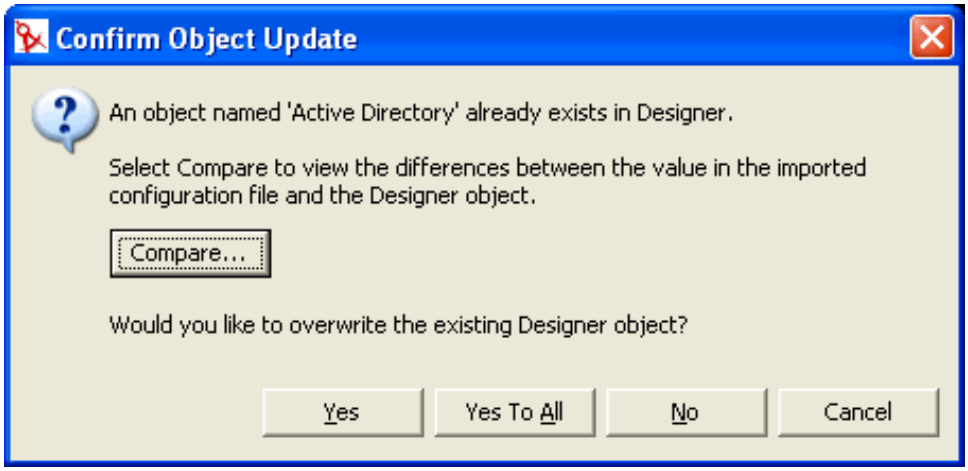
3 ［ActiveDirectoryUpdate.xml］を選択して、［実行］をクリックします。

4 ［はい］を選択するか、またはプロンプトで入力した情報を Designer で検証する場合は［いいえ］を選択します。



5 各自の環境に特有の情報を入力して、［OK］をクリックします。フィールドの説明については、55 ページの 表 5-1 を参照してください。

6 ［Confirm Object Update (オブジェクトの更新の確認)］ウィンドウで、インポートされた環境設定ファイルの値と Designer オブジェクトの値の違いを表示するために［比較］を選択して、［閉じる］をクリックします。



7 変更が正しい場合は、［はい］を選択すると、既存の Designer オブジェクトが上書きされます。ドライバを更新しない場合は、［いいえ］を選択します。

表 5-1 *Designer* でのオーバレイ環境設定パラメータ

パラメータ	説明
ドライバ名	このパラメータは、新しいパラメータで更新する必要があるドライバです。ドライバ名を入力するか、またはドライバを参照して選択します。
ドライバの更新	このパラメータを使用すると、他のパラメータでドライバが更新されます。ドライバを更新する場合は、［はい］**を選択します。ドライバを更新しない場合は、**［**いいえ**］を選択します。
Exchange の移動を制御する homeMDB	ユーザの homeMDB 属性を変更すると、CDOEXM の使用時にユーザの Exchange メールボックスを移動できます。ユーザのメールボックスの移動先の Exchange メッセージデータベースは、古い Exchange メッセージデータベースと同じドメインに存在する必要があります。 ［はい］を選択した場合は、ユーザオブジェクトが eDirectory に移動されると、その移動が Active Directory と Exchange にも反映されます。 ［いいえ］を選択した場合は、ユーザオブジェクトが eDirectory に移動されると、その移動が Active Directory には反映されますが、Exchange には反映されません。

パラメータ	説明
Exchange の削除を制御する homeMDB	ユーザの homeMDB 属性を削除すると、CDOEXM の使用時にユーザの Exchange メールボックスを削除できます。 ［はい］を選択した場合は、eDirectory のユーザオブジェクトが削除されると、関連する Active Directory ユーザオブジェクトと Exchange アカウントも削除されます。 ［いいえ］を選択した場合は、eDirectory のユーザオブジェクトが削除されると、関連する Active Directory ユーザオブジェクトは削除されますが、Exchange アカウントはそのまま残されます。
ログオンと偽装	CDOEXM 用およびパスワードの設定サポート用のドライバ認証アカウントがさまざまな方式でログオンできます。 ［いいえ］を選択すると、ドライバでネットワークログオンだけが実行されます。 ［はい］を選択すると、ドライバでローカルログオンが実行されます。認証アカウントは、管理者特権を備えた Active Directory アカウントである必要があります。

5.5.2 iManager でのオーバレイの適用

iManager を介してドライバを更新する場合は、2 通りの方法があります。ドライバは、［Identity Manager の概要］または［Identity Manager ユーティリティ］で更新できます。

Identity Manager の概要

1. iManager で、［Identity Manager］>［Identity Manager の概要］の順に選択します。
2. ［検索］を選択して、Active Directory ドライバを保存するドライバセットオブジェクトを検索します。
3. ［Identity Manager の概要］画面で［ドライバの追加］を選択します。
4. Active Directory ドライバを保存するドライバセットオブジェクトを参照して選択し、［次へ］をクリックします。
5. ［サーバからのドライバ環境設定のインポート (.XML ファイル)］を選択します。
6. ドロップダウンメニューから、［ActiveDirectoryUpdate.xml］を選択して、［次へ］をクリックします。
7. 各自の環境に特有の情報を入力して、［次へ］をクリックします。フィールドの説明については、57 ページの 表 5-2 を参照してください。
8. ［該当ドライバの更新 (ドライバのイメージを含める)］を選択するか、［異なるドライバの選択］を選択して、［次へ］をクリックします。
9. 変更の要約を表示して、［終了］をクリックします。

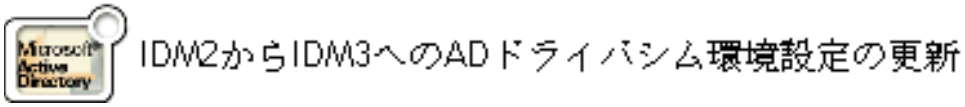
表 **5-2** *iManager* でのオーバレイ環境設定パラメータ

パラメータ	説明
ドライバ名	このパラメータは、新しいパラメータで更新する必要があるドライバです。
既存のドライバ	ドロップダウンメニューから、Exchange プロビジョニングを有効にした更新済み AD ドライバの名前を選択します。ドライバ名を選択すると、［ドライブ名］フィールドが自動的に作成されます。
ドライバの更新	このパラメータを使用すると、他のパラメータでドライバが更新されます。ドライバを更新する場合は、［はい］を選択します。ドライバを更新しない場合は、［いいえ］を選択します。
Exchange の移動を制御する homeMDB	ユーザの homeMDB 属性を変更すると、CDOEXM の使用時にユーザの Exchange メールボックスを移動できます。ユーザのメールボックスの移動先の Exchange メッセージデータベースは、古い Exchange メッセージデータベースと同じドメインに存在する必要があります。 ［はい］を選択した場合は、ユーザオブジェクトが eDirectory に移動されると、その移動が Active Directory と Exchange にも反映されます。 ［いいえ］を選択した場合は、ユーザオブジェクトが eDirectory に移動されると、その移動が Active Directory には反映されますが、Exchange には反映されません。
Exchange の削除を制御する homeMDB	ユーザの homeMDB 属性を削除すると、CDOEXM の使用時にユーザの Exchange メールボックスを削除できます。 ［はい］を選択した場合は、eDirectory のユーザオブジェクトが削除されると、関連する Active Directory ユーザオブジェクトと Exchange アカウントも削除されます。 ［いいえ］を選択した場合は、eDirectory のユーザオブジェクトが削除されると、関連する Active Directory ユーザオブジェクトは削除されますが、Exchange アカウントはそのまま残されます。
ログオンと偽装	CDOEXM 用およびパスワードの設定サポート用のドライバ認証アカウントがさまざまな方式でログオンできます。 ［いいえ］を選択すると、ドライバでネットワークログオンだけが実行されます。 ［はい］を選択すると、ドライバでローカルログオンが実行されます。認証アカウントは、管理者特権を備えた Active Directory アカウントである必要があります。

Identity Manager ユーティリティ

1. iManager で、［Identity Manager ユーティリティ］>［ドライバのインポート］の順に選択します。
2. Active Directory ドライバを保存するドライバセットオブジェクトを参照して選択し、［次へ］をクリックします。

3 ［その他のポリシー］で、［IDM2 から IDM3 への AD ドライバシム環境設定の更新］を選択して、［次へ］をクリックします。



4 各自の環境に特有の情報を入力して、［次へ］をクリックします。フィールドの説明については、57 ページの 表 5-2 を参照してください。

5 ［該当ドライバの更新 (ドライバのイメージを含める)］を選択するか、［異なるドライバの選択］を選択して、［次へ］をクリックします。

6 変更の要約を表示して、［終了］をクリックします。

Active Directory ドライバの管理

6

6.1 セキュリティパラメータ

インストール時に、ドライバで必要な情報が収集され、デフォルトのセキュリティポリシーとパラメータが作成されます。Active Directory ドライバをカスタマイズするには、次のことに精通している必要があります。

- デフォルトのポリシーとパラメータ
- 89 ページの第 8 章「トラブルシューティング」で説明されているトピック。それにより、こうした問題のいずれかが各自の環境に当てはまるかどうかを決定できます。

パラメータの連携やオペレーティングシステムとの連動を理解すると、Identity Manager データ同期のセキュリティへのアプローチを定義できるようになります。

- 認証 **ID:** ドメインデータにアクセスするためにドライバで使用されるアカウント。

表 *6-1* 認証 *ID*

形式	ユーザ名	方式
ドメイン名	ユーザ	ネゴシエーション
完全修飾ドメイン名	ドメイン\ユーザ	ネゴシエーション
識別名	cn=DirXML,cn=Users,DC=domain,dc=com	シンプル

- 認証コンテキスト **:** ドメインデータのアクセスに使用されるコンテキスト。

表 *6-2* 認証コンテキスト

形式	例	方式
アクティブなドメインコントローラの DNS 名	mycontroller.mydomain.com	ネゴシエーション
アクティブなドメインコントローラの DNS 名、または使用する LDAP サーバの IP アドレス	mycontroller.mydomain.com 137.65.134.83	シンプル

- アプリケーションのパスワード **:** 認証 ID アカウントのパスワード。

- 署名を使用する **:** このパラメータは、Active Directory ドライバと Active Directory の間で使用されますが、メタディレクトリエンジンとリモートローダの間では使用されません。署名により、悪質なコンピュータにデータが傍受されていないことが保障されます。LDAP SSL ポートを使用していない場合は、このフラグで Active Directory 接続の署名を有効にします。

  この設定には、最新のサポートパックを適用した Windows 2003 または Windows 2000、および両方のサーバ上に Internet Explorer 5.5 SP2 以降が必要です。この設定により、Kerberos または NTLM v2 の認証された接続での署名が有効になります。

  SSL と同様に、このパラメータは最初のインポート時には使用できません。インストールの完了後に、［ドライバパラメータ］ページでこのパラメータを設定します。

- 封印を使用する **:** このパラメータは、Active Directory ドライバと Active Directory の間で使用されますが、メタディレクトリエンジンとリモートローダの間では使用されません。封印すると、ネットワークモニタで表示できないようにデータが暗号化されます。LDAP SSL ポートを使用していない場合は、このフラグで Active Directory 接続の封印を有効にします。

  この設定には、最新のサポートパックを適用した Windows 2003 または Windows 2000、および両方のサーバ上に Internet Explorer 5.5 SP2 以降が必要です。この設定により、Kerberos または NTLM v2 の認証された接続での暗号化が有効になります。

  SSL と同様に、このパラメータは最初のインポート時には使用できません。インストールの完了後に、［ドライバパラメータ］ページでこのパラメータを設定します。

- **SSL** の使用 **:** このパラメータは、Active Directory ドライバと Active Directory の間で使用されます。LDAP SSL ポートを使用して Active Directory に接続する場合は、このパラメータで暗号化を制御します。このパラメータは、［ネゴシエーション］と［シンプル］の両方の認証方式に適用されます。

  デフォルトでは、パラメータは［いいえ］に設定されます。この値を［はい］に設定すると、やりとり全体の SSL パイプが暗号化されます。通常はドライバで機密情報を同期するため、暗号化されたパイプが優先されます。ただし、暗号化するとサーバの全般的なパフォーマンスが低下します。

  このパラメータは、ドライバがインポートされた後に［ドライバパラメータ］ページで設定できます。

6.1.1 推奨されるセキュリティ設定

Identity Manager リモートローダの使用

表 *6-3* 推奨される設定

パラメータ	説明
認証 ID	ドメインログオン名 (Administrator など)。
認証コンテキスト	ドメインコントローラの DNS 名。 Active Directory ドメインコントローラでドライバを実行しない場合、［ネゴシエーション］方式では*ホスト名*を使用しますが、［シンプル］方式では*ホスト名*または IP アドレスを使用します。
アプリケーションパスワード	認証アカウント用のパスワード。

パラメータ	説明
リモートローダパスワード	リモートローダサービスのパスワード。
認証方式	ネゴシエーション。
署名を使用する	いいえ。最新のサポートパックを適用した Windows 2003 または Windows 2000、および両方のサーバ上に Internet Explorer 5.5 SP2 以降が必要です。
封印を使用する	いいえ。最新のサポートパックを適用した Windows 2003 または Windows 2000、および両方のサーバ上に Internet Explorer 5.5 SP2 以降が必要です。
SSL の使用	はい。ドライバシムがドメインコントローラで実行していないときに購読者パスワードのチェック、設定、および変更を実行するために、SSL が必要です。

SSL の使用

［シンプル］認証ではパスワードがクリアテキストで渡されるため、［シンプル］認証メカニズムを選択した場合は、SSL を使用することをお勧めします。

表 *6-4* *SSL パラメータ*

パラメータ	説明
認証 ID	LDAP 形式の認証 ID
認証コンテキスト	ドメインコントローラの IP アドレス
パスワード	指定した認証 ID のパスワード
署名を使用する	いいえ
封印を使用する	いいえ
SSL の使用	はい

6.2 グループの管理

Active Directory グループクラスでは、2 種類のグループおよびグループ内のメンバーシップの 3 つのスコープを定義します。タイプおよびスコープは、groupType 属性で制御されます。この属性は、グループが Active Directory で作成された場合や属性の修正により変更された場合に、Identity Manager ポリシーを介して設定できます。

グループでは、オブジェクト参照のコレクションが保持されます。配布グループタイプでは、そのメンバーに特別な権限や特権が設定されないので、一般に Exchange の配布リストとして使用されます。セキュリティグループタイプは、セキュリティプリンシパルです。そのメンバーには、グループの権限および特権が与えられます。セキュリティグループには、旧 Windows 2000 のログオン名 (samAccountName) とセキュリティ ID (SID) が設定されます。この SID を他のオブジェクトのセキュリティ記述子 (SD) アクセス制御リスト (ACL) で使用すると、そのメンバーへの権限や特権を付与または拒否できます。

グループスコープでは、外部ドメインからのオブジェクトをグループのメンバーにすることができるかどうか、また、グループ自体を別のグループのメンバーにすることができる

かどうかを制御します。3 つのスコープとして、ドメインローカル、グローバル、およびユニバーサルがあります。これらのスコープの動作、つまりスコープが有効であるかどうかは、Active Directory が Windows 2000 混在モード、Windows 2000 ネイティブモード、または Windows 2003 モードのどれで動作しているかによって異なります。

一般に、ドメインローカルグループではフォレスト内のどこででもオブジェクトの参照を保持できますが、このグループにはドメイン内でのみ許可を割り当てることができます。グローバルグループはその逆です。グローバルグループではドメイン内でのみオブジェクトの参照を保持できますが、このグループにはフォレスト内のどこででも許可を割り当てることができます。ユニバーサルグループの場合は、フォレスト内のどこででもオブジェクトの参照を保持し、許可を割り当てることができます。しかし、ユニバーサルグループでは、独自の制限とパフォーマンスの問題が生じます。グループは、Microsoft の推奨事項に基づいて作成および使用する必要があります。

groupType 属性は 32 ビットの整数であり、ビット列でタイプとスコープが定義されています。グループには、常に 1 つのスコープだけを設定できます。

表 *6-5* *groupType* 属性

groupType 属性	スコープ	タイプとスコープを定義するビット列
GROUP_TYPE_GLOBAL_GROUP	配布	0x00000002
GROUP_TYPE_DOMAIN_LOCAL_GROUP	配布	0x00000004
GROUP_TYPE_UNIVERSAL_GROUP	配布	0x00000008
GROUP_TYPE_SECURITY_ENABLED	セキュリティ	0x80000000

6.3 Microsoft Exchange メールボックスの管理

Active Directory ドライバを設定すれば、Active Directory のユーザ向けに Microsoft Exchange メールボックスの作成、移動、および削除を行うことができます。メールボックスを管理するには、ユーザオブジェクトの homeMDB 属性の値を設定および削除します。この属性では、メールボックスが存在する Exchange のプライベートメッセージデータベース (MDB) の識別名が保持されます。ドライバと同じドメインにある Exchange サーバのメールボックスは、ドライバで管理されます。

Exchange メールボックスを管理する方法は、何種類かあります。デフォルトの環境設定では、購読者コマンド変換ポリシーでのポリシー決定を介してメールボックスが管理されます。ユーザが特定の条件を満たす場合に、メールボックスは作成、移動、または削除されます。インポートファイルでは、メールボックスの管理方法として次の 3 つから選択できます。

- エンタイトルメント
- ポリシー
- Exchange メールボックスを管理しない

プロビジョニングにエンタイトルメント方式を採用すると、ユーザは、アイデンティティボールトでそのユーザに対して設定されているエンタイトルメントに基づいてメールボックスが許可または拒否されます。エンタイトルメントでは、MDB の識別名、およびエンタイトルメントの許可または取り消しをドライバに示す状態値が保持されます。エンタイ

トルメント自体は、ユーザアプリケーションまたは役割ベースのエンタイトルメントドライバで管理されます。どちらの場合も、外部ツールでメールボックスに権限が付与され (または取り消され)、購読者コマンド変換ポリシーでその権限が homeMDB 属性の「add-value(値の追加)」または「remove-value(値の削除)」に変換されます。また、ドライバシムで、homeMDB の変更が適切な Exchange 管理システムの呼び出しに変換されます。

エンタイトルメントを使用している状態で組織に複数の MDB がある場合は、ユーザアプリケーションを使用して、特定のユーザに割り当てる MDB を決定します。複数の MDB の設定方法については、『Identity Manager Accessory Portlet Reference Guide (http://www.novell.com/documentation/idm)』を参照してください。Identity Manager ドライバの役割は、ユーザオブジェクトに配置されたエンタイトルメントに応答することであり、エンタイトルメントをユーザオブジェクトに配置することではありません。ユーザアプリケーションを使用している場合は、ワークフロー項目が承認プロセスに渡るときに選択元の Exchange MDB のリストが得られます。役割ベースエンタイトルメントを使用している場合は、ユーザの役割を保持するグループに MDB が割り当てられます。

プロビジョニングに備えてポリシーベースの方式を採用する場合は、購読者コマンド変換ポリシーで、アイデンティティボールト内のユーザオブジェクトの状態に関する情報を使用して MDB が割り当てられます。ドライバシムでは、変更が Exchange 管理システムへの適切な呼び出しに変換されます。デフォルトのポリシーでは、メールボックスを割り当てるための単純なルールが使用されます。このポリシーでは、MDB が 1 つしかないこと、およびポリシーチェーンを介してここまで行ってきたすべてのユーザをその MDB に割り当てる必要があることを想定しています。さまざまな MDB を割り当てるためのルールは会社によって大きく異なるため、デフォルトの環境設定では、割り当ての「正しい方法」を確立しようとはしていません。独自のポリシーを実装するには、デフォルトの割り当てルールを変更するだけです。DirXML スクリプトの if ステートメントを使用して、メールボックス割り当ての条件および homeMDB 属性の do-set-dest-attribute コマンドを定義し、変更を有効にします。ADManager.exe ツールを使用するか、または独自の方法で Exchange MDB のリストを取得できます。

Exchange メールボックスを管理しない場合は、ドライバでユーザの電子メールアドレスとメールニックネームが同期されます。

ほかにも Exchange メールボックスを管理する方法があります。たとえば、homeMDB 情報を保持するためにアイデンティティボールトのスキーマを拡張し、基本的なデータ同期を利用して Active Directory のユーザにメールボックスを割り当てることができます。このような場合は、独自のツールを使用してアイデンティティボールトに割り当てを作成します。

デフォルトのポリシーは、1 つの MDB に単純なメールボックスを割り当てるのに適しています。ポリシーにより、各自の環境で要求される複雑なルールを反映させる場合は、ポリシーを変更する必要があります。

6.4 ドライバを有効にする

インストール後 90 日以内にドライバを有効にします。90 日の試用期間が期限切れになると、ドライバは適切なアクティベーションキーがなければ起動しません。ドライバが有効にされない場合に発生するイベントは、ドライバのアクティベーション時および以降の起動時に処理されます。

有効にする方法の詳細については、『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。

パスワード同期

7

この節は、『Novell Identity Manager 3.0 管理ガイド』の「接続システム間のパスワード同期」に記載されている情報に精通していることを前提としています。この節の情報は、このドライバに特有のものです。

重要 : 以前に Password Synchronization 1.0 を使用していた場合は、67 ページの 「Identity Manager に付属のパスワード同期への Password Synchronization 1.0 のアップグレード」を読んで影響を理解するまでは、新しいドライバシムをインストールしないでください。ドライバシムをインストールする場合は、Identity Manager に付属のパスワード同期をすぐに利用しなくても、同時にドライバポリシーに Password Synchronization 1.0 との後方互換性を追加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。

パスワード同期のトラブルシューティングについては、91 ページの 「パスワード同期のヒント」を参照してください。

7.1 Password Synchronization 1.0 と Identity Manager に付属のパスワード同期との比較

表 *7-1* パスワード同期のさまざまなバージョンでの相違点

機能	Password Synchronization 1.0	Identity Manager に付属のパスワード同期
製品の提供	Identity Manager とは別の製品です。	Identity Manager に含まれており、別製品として販売されていません。

機能	Password Synchronization 1.0	Identity Manager に付属のパスワード同期
プラットフォーム	◆ Active Directory ◆ NT ドメイン	次のプラットフォームでは完全な双方向パスワード同期がサポートされています。 ◆ Active Directory ◆ eDirectory™ ◆ NIS ◆ NT ドメイン これらの接続システムは、Identity Manager へのユーザパスワードの発行をサポートしています。ユニバーサルパスワード (および配布パスワード) は逆方向に同期できるため、Identity Manager はパスワードを接続システムに配布できます。 購読者パスワード要素をサポートする接続システムは、パスワードを Identity Manager から受信できます。 『Novell Identity Manager 3.0 管理ガイド』の「接続システム間のパスワード同期」を参照してください。
eDirectory で使用されるパスワード	eDirectory パスワード (逆方向は不可能)	ユニバーサルパスワード (逆方向の同期が可能)、または配布パスワード (同様に逆方向の同期が可能)。また、必要に応じて eDirectory パスワードの同期を維持することもできます。シナリオの例については、『Novell Identity Manager 3.0 管理ガイド』の「パスワード同期の実装」を参照してください。
Windows 接続システムの主な機能	eDirectory パスワードが Windows のパスワードと同期されるように、双方向のパスワード同期を提供する場合。ただし、各ワークステーションには Novell® Client™ が必要です。	双方向パスワード同期を提供する場合。ユニバーサルパスワード (および配布パスワード) は逆方向に同期できるため、パスワードは両方のディレクトリで同期できます。iManager の発行者チャネルおよび購読者チャネル内で実現されます。
LDAP パスワードの変更	サポートされていません。	サポートされています。
Novell Client	必須。	不要。
nadLoginName 属性	パスワードの更新を保つために使用されます。	使用されません。

機能	Password Synchronization 1.0	Identity Manager に付属のパスワード同期
パスワード同期機能を含むコンポーネント	nadLoginName を更新するための機能は Identity Manager ドライバに含まれていました。	ドライバ環境設定のポリシーでパスワード同期機能が提供されます。ドライバは単に、ポリシー内のロジックから発生する、メタディレクトリエンジンによって与えられるタスクを実行します。 ドライバマニフェスト、グローバル構成値、およびドライバフィルタ設定もパスワード同期をサポートする必要があります。これは、サンプルドライバ環境設定に含まれており、既存のドライバに追加できます。74 ページのセクション 7.4「Identity Manager 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。
エージェント	別個のソフトウェア。	エージェントはインストールされません。この機能はドライバの一部になりました。

7.2 Identity Manager に付属のパスワード同期への Password Synchronization 1.0 のアップグレード

現在 Password Synchronization 1.0 を使用している場合は、この節の手順を実行してアップグレードします。

重要 : こうした手順を確認するまでは、Identity Manager ドライバシムをインストールしないでください。

Password Synchronization 1.0 から Identity Manager に付属のパスワード同期へアップグレードする

1 現在の環境でユニバーサルパスワードを使用する準備ができていることを確認します。

『Novell Identity Manager 3.0 管理ガイド』の「Identity Manager パスワード同期およびユニバーサルパスワードを使用するための準備作業」を参照してください。

ユニバーサルパスワードを有効にしても、両方のシステムで自動的にパスワードが変更されるわけではありません。ユーザがパスワードを変更した後にのみユニバーサルパスワード同期が機能し始めます。

シナリオ : ユニバーサルパスワード。DigitalAirlines において、ネットワーク管理者 Sandy がユニバーサルパスワードを有効にします。ユーザ Markus がログインして自分のパスワードを変更します。Markus のユニバーサルパスワードは、両方のシステムで設定されています。しかし、ユーザ Marie はログインしますが、自分のパスワードを変更しません。彼女は、未変更のパスワードを使用して引き続きログインします。Marie のユニバーサルパスワード機能は、彼女が自分のパスワードを変更するまでは設定されません。

2 Identity Manager 3 ドライバシムをインストールし、DirXML® 1.1a ドライバシムを置き換えて、すぐにステップ 3 を実行します。

注 **:** Identity Manager 2.0 を実行しており、ユニバーサルパスワードを使用している場合は、パスワード同期はアップグレードされません。

『Identity Manager 3.0 インストールガイド』の「Identity Manager のインストール」の章にある説明に従って、インストールプログラムを使用し、Active Directory 用の Identity Manager ドライバだけを選択します。

3 Password Synchronization 1.0 との後方互換性を保つために、70 ページの 「ポリシーの追加による Password Synchronization 1.0 との後方互換性の維持」にある説明に従ってドライバ環境設定に新しいポリシーを追加します。

DirXML 1.1a ドライバシムでは nadLoginName 属性は更新されますが、Identity Manager ドライバシムでは更新されません。したがって、ドライバ環境設定にポリシーを追加して nadLoginName を更新する必要があります。これにより、ドライバシムをインストールすると Password Synchronization 1.0 が通常通り機能できるので、Identity Manager パスワード同期の展開を終了するときのパスワードの変更は免れません。

重要 **:** 後方互換性を保たない場合は、Password Synchronization 1.0 で引き続き既存のユーザが更新されますが、Identity Manager パスワード同期を展開するまで新規ユーザおよびリネームされたユーザを同期することはできません。

このステップを完了したら、Identity Manager 3.0 のドライバシムおよび後方互換性を保つためのポリシーが得られます。したがって、使用するドライバは Password Synchronization 1.0 をサポートしています。

この手順の残りをすぐに完了できない場合は、Identity Manager パスワード同期の展開を終了する準備ができるまで、引き続き Password Synchronization 1.0 を使用できます。

4 パスワード同期に使用する各ドライバに Identity Manager パスワード同期のサポートを追加します。

既存の環境設定をアップグレードするか、既存の環境設定を置き換えます。

既存の環境設定をアップグレード **:** 既存の DirXML 1.1a ドライバ環境設定をアップグレードするには、それを Identity Manager 形式に変換して、Identity Manager パスワード同期に必要なポリシーを追加します。

- ウィザードを使用してドライバを Identity Manager 形式に変換します。『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。
- Identity Manager パスワード同期をサポートするポリシーを追加します。「オーバーレイ」設定ファイルを使用すると、ポリシー、ドライバマニフェスト、および GCV を一度に追加できます。フィルタにも属性を追加する必要があります。手順については、『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。

既存の環境設定を **Identity Manager** 環境設定に置き換えて、もう一度後方互換性を追加 **:** Identity Manager サンプルドライバ環境設定には、Identity Manager パスワード同期をサポートするポリシー、ドライバマニフェスト、GCV、およびフィルタ設定が含まれています。新しいドライバ環境設定のインポートに関については、このドラ

イバガイドの 39 ページの第 4 章「Active Directory ドライバの設定」の手順を参照してください。

- 既存の環境設定を置き換えることにする場合は、70 ページの 「ポリシーの追加による Password Synchronization 1.0 との後方互換性の維持」にある説明に従って、必ずもう一度後方互換性を追加します。Identity Manager サンプルドライバ環境設定には、そうしたポリシーは含まれていません。
- nadLoginName 属性は、以前のドライバ環境設定にあったので、その属性が［発行］に設定されていることを確認します。

5 新しいパスワード同期フィルタをインストールし、接続システムで Identity Manager へのユーザパスワードを設定する場合は、それらのフィルタを設定します。

77 ページのセクション 7.5「パスワード同期のフィルタの設定」を参照してください。

6 必要に応じて SSL を設定します。

手順については、19 ページのセクション 2.3「セキュリティ問題の対処」を参照してください。

Active Directory (購読者チャネル) でパスワードを設定するドライバの機能には、次のいずれかの条件に基づいて提供される安全な接続が必要です。

- ドライバを実行するコンピュータがドメインコントローラと同じコンピュータである。
- ドライバを実行するコンピュータがドメインコントローラと同じドメインにある。
- 同じドメインにないコンピュータの場合は、そのコンピュータとドメインコントローラの間で［シンプル］方式および SSL を設定する必要があります。双方向のパスワード同期機能は、［ネゴシエーション］認証メカニズムを採用する場合に限り使用できます。

  手順については、Microsoft のマニュアル (『Configuring Digital Certificates on Domain Controllers (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/secwin2k/a0701.asp)』など) を参照してください。

7 アイデンティティボールトユーザアカウントのユニバーサルパスワードをオンにするには、ユニバーサルパスワードが有効なパスワードポリシーを作成します。

『Novell Identity Manager 3.0 管理ガイド』の「パスワード同期の管理」を参照してください。

管理を簡素化するには、パスワードポリシーをツリーのできるだけ上位のレベルに割り当てることをお勧めします。

8 ドライバ向けのパスワードポリシーとパスワード同期の設定を使用して、パスワード同期に使用するシナリオを準備します。

『Novell Identity Manager 3.0 管理ガイド』の「パスワード同期の実装」を参照してください。

9 パスワード同期をテストします。

10 Identity Manager パスワード同期が正常に機能したら、Password Synchronization 1.0 を削除します。

10a ［プログラムの追加と削除］を使用して、エージェントを削除すると、Password Synchronization 1.0 が無効になります。

10b ドライバのフィルタで、nadLoginName 属性を［無視］に変更します。

10c ドライバ環境設定の nadLoginName を更新している後方互換性ポリシーを削除します。

10d Identity Manager パスワード同期が正常に機能したら、nadLoginName 属性は不要になるため、必要に応じてユーザからこの属性を削除することもできます。

7.2.1 ポリシーの追加による Password Synchronization 1.0 との後方互換性の維持

Password Synchronization 1.0 では、nadLoginName という名前の属性を更新するドライバシムを利用しています。この属性は、ユーザのパスワードを同期する必要があるかどうかを示します。新規ユーザが追加された場合やユーザの名前が変更された場合、nadLoginName 属性は追加されるか、一致するよう更新されていました。

Identity Manager のドライバシムでは、この属性が Identity Manager パスワード同期に不要なため、この属性は更新されなくなりました。したがって、新しいドライバシムをインストールしても、nadLoginName 属性は更新されていません。つまり、Password Synchronization 1.0 では、新規ユーザまたは名前が変更されたユーザの通知を受け取らなくなったということです。ただし、現在のドライバ環境設定に後方互換性を追加する場合は除きます。

Password Synchronization 1.0 から Identity Manager パスワード同期へスムーズに移行するために、Password Synchronization 1.0 との後方互換性が必要です。

Password Synchronization 1.0 との後方互換性を維持するには、nadLoginName 属性を更新するポリシーを追加する必要があります。

既存のドライバ環境設定を更新しているか、そうした設定を Identity Manager に付属の新しい環境設定に置き換えているかにかかわらず、こうしたポリシーを追加する必要があります。Active Directory の Identity Manager サンプルドライバ環境設定には、デフォルトではポリシーが含まれていません。

購読者出力変換、発行者入力変換、および発行者コマンド変換にそれぞれ 1 つずつ、3 つのポリシーが必要です。これらのポリシーは、Password Synchronization 1.0 Policies for Active Directory という名前の環境設定ファイルで、Identity Manager に付属しています。次の手順は、新しいポリシーをインポートしてそれをドライバ環境設定に追加する方法を示しています。

1 iManager で、［Identity Manager ユーティリティ］>［ドライバのインポート］の順にクリックします。

ドライバインポートウィザードが開きます。

2 既存の Active Directory ドライバの存在するドライバセットを選択し、［次へ］をクリックします。

3 表示されるドライバ環境設定のリストで、［その他のポリシー］セクションまでスクロールし、［レガシパスワード同期 1.0 のポリシー : AD および NT の下位互換性］を選択して、［次へ］をクリックします。

4 インポートプロンプトに対して次の操作を実行します。

4a 既存の Active Directory ドライバを選択します。

既存のドライバを選択すると、必要な 3 つのポリシーを追加できます。インポートプロセスでは、3 つの新しいポリシーオブジェクトが作成されます。次に、それらをドライバ環境設定の適切な場所に挿入する必要があります。

4b ドライバが Active Directory ドライバであるかどうか指定します。

インポートされるポリシーは、選択されるシステムによって少し異なります。

4c 更新するドライバに関連付けられている nadDomain オブジェクトを参照して選択します。

このオブジェクトは、通常ドライバオブジェクトの下にあります。

4d (Active Directory のみ) Active Directory 属性 sAMAccountName にマッピングされる eDirectory™ 属性の名前を指定します。

この情報は、ドライバ環境設定内のスキーママッピングポリシーにあります。

注 **:** sAMAccountName が eDirectory 属性にマッピングされていない場合は、sAMAccountName を DirXML-ADAlias 名にマッピングします。

---

5 ［次へ］をクリックします。

既存のドライバを選択したため、ドライバの更新方法を決定するよう要求するページが表示されます。この場合は、選択したポリシーの更新を求めるだけです。

6 ［該当ドライバで選択したポリシーのみを更新］を選択して、表示される 3 つのポリシーすべてのチェックボックスをオンにします。

7 ［次へ］をクリックし、［終了］をクリックしてウィザードを完了します。

この時点では、新しい 3 つのポリシーはドライバオブジェクトの下のポリシーオブジェクトとして作成されていますが、ドライバ環境設定の一部にはなっていません。環境設定にリンクさせるには、発行者および購読者チャネルのドライバ環境設定の右側のポイントに、各ポリシーを手動で挿入する必要があります。

8 新しい 3 つのポリシーをそれぞれ既存のドライバ環境設定の正しい場所に挿入します。

ドライバ環境設定のこのいずれかの部分に複数のポリシーがある場合、これらの新しいポリシーが最後に表示されるようにしてください。

表 *7-2* ポリシー

ポリシーオブジェクト名	挿入場所
PassSync(Pub)- コマンド変換ポリシー	発行者チャネルでのコマンド変換ポリシー
PassSync(Pub)- 入力変換ポリシー	発行者チャネルでの入力変換ポリシー
PassSync(Sub)- 出力変換ポリシー	購読者チャネルでの出力変換ポリシー 

ポリシーごとに、ステップ 8a ～ 8f を繰り返します。

8a ［Identity Manager］>［Identity Manager の概要］の順にクリックします。

8b 更新しているドライバのドライバセットを選択します。

8c 更新したドライバをクリックします。

ページが開いて、ドライバ環境設定がグラフィカル表示されます。

8d 新しい 3 つのポリシーのいずれかを追加する必要がある場所のアイコンをクリックします。

8e ［挿入］をクリックし、新しいポリシーを追加します。

表示される［挿入］ページで、［既存のポリシーを使用する］をクリックし、新しいポリシーオブジェクトを参照して、［OK］をクリックします。

8f 新しい 3 つのポリシーのいずれかのリストに複数のポリシーがある場合は、矢印ボタン を使用して、新しいポリシーをリストの最後になるように下に移動します。

9 Active Directory ドライバのすべてに対してステップ 1 ～ 9 を繰り返します。

sAMAccountName を発行者チャネルスキーママッピングポリシーの DirXML-ADAliasName にマッピングする必要がある場合は、この手順に従ってください。

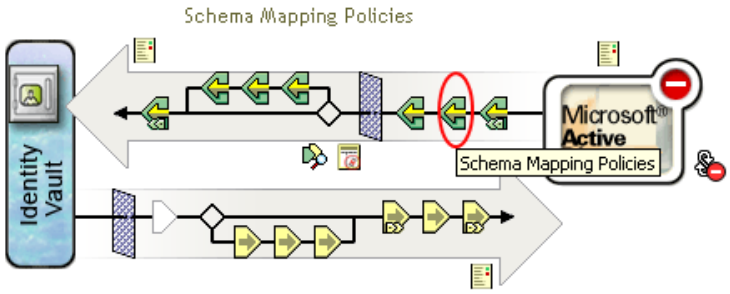
警告 **:** sAMAccountName が別の属性にマッピングされている場合、この手順に従うと、現在のポリシーが無効になります。ポリシーによるパスワードの同期が中止されます。71 ページのステップ 4d で適切な属性を確実に入力してください。

---

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

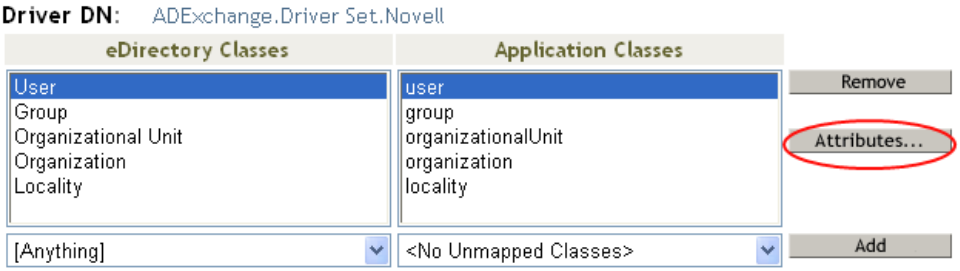
2 Active Directory ドライバを含むドライバセットオブジェクトを参照して選択し、［検索］をクリックします。

3 ドライバアイコンをクリックして、発行者チャネルの［スキーママッピングポリシー］アイコンをクリックします。



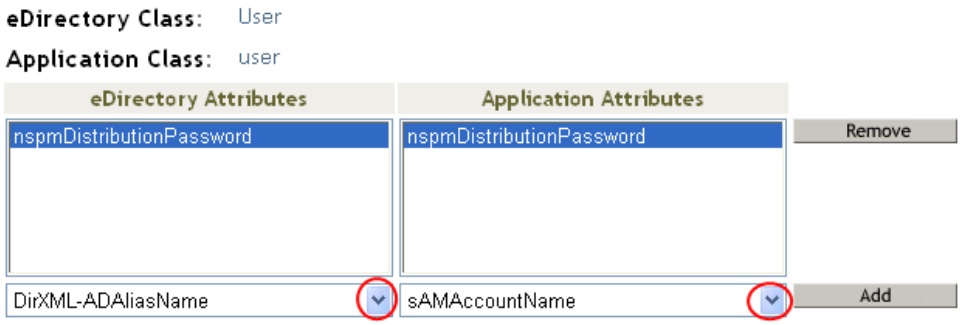
4 ［編集］をクリックします。

5 ユーザクラスを選択して、［属性］をクリックします。



6 ［eDirectory 属性］の下のドロップダウンリストをクリックし、DirXML-ADAliasName を参照して選択します。

7 ［アプリケーション属性］の下のドロップダウンリストをクリックし、sAMAccountName を参照して選択します。



8 ［追加］をクリックし、［OK］をクリックします。

9 グループクラスを選択して、［属性］をクリックします。

10 グループクラスに対してステップ 6 ～ 8 を繰り返します。

11 ［OK］を 2 回クリックします。

この手順を完了すると、Active Directory ドライバのドライバ環境設定の Password Synchronization 1.0 との後方互換性が保たれます。つまり、引き続きパスワード同期が以前と同様に機能するため、都合のよいときに Identity Manager パスワード同期にアップグレードできるということです。

7.3 新しいドライバ環境設定と Identity Manager のパスワード同期

Password Synchronization 1.0 を使用しておらず、新しいドライバを作成している場合、または既存のドライバの環境設定を Identity Manager 環境設定に置き換えている場合は、『Novell Identity Manager 3.0 管理ガイド』の「新しいドライバ環境設定と Identity Manager のパスワード同期」の手順に従ってください。

さらに、次の作業を行います。

- 必要に応じて SSL を設定します。19 ページのセクション 2.3「セキュリティ問題の対処」を参照してください。

  Active Directory (購読者チャネル) でパスワードを設定するドライバの機能には、次のいずれかの条件に基づいて提供される安全な接続が必要です。

  - ドライバを実行するコンピュータがドメインコントローラと同じコンピュータである。
  - ドライバを実行するコンピュータがドメインコントローラと同じドメインにある。
  - 同じドメインにないコンピュータの場合は、そのコンピュータとドメインコントローラの間で［シンプル］方式および SSL を設定する必要があります。双方向のパスワード同期機能は、［ネゴシエーション］認証メカニズムを採用する場合に限り使用できます。

    手順については、Microsoft のマニュアル (『Enabling Secure Sockets Layer for SharePoint Portal Server 2003 (http://office.microsoft.com/en-us/assistance/HA011648191033.aspx)』など) を参照してください。

- 新しいパスワード同期フィルタをインストールし、接続システムで Identity Manager へのユーザパスワードを設定する場合は、それらのフィルタを設定します。77 ページのセクション 7.5「パスワード同期のフィルタの設定」を参照してください。
- ドライバ向けのパスワードポリシーとパスワード同期の設定を使用して、使用するパスワード同期のシナリオを準備します。『Novell Identity Manager 3.0 管理ガイド』の「パスワード同期の実装」を参照してください。

7.4 Identity Manager 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

重要 : ドライバが Password Synchronization 1.0 で使用されている場合は、単独ではなく、67 ページのセクション 7.2「Identity Manager に付属のパスワード同期への Password Synchronization 1.0 のアップグレード」の一部としてこのセクションだけを実行する必要があります。

次に示すのは、このセクションの手順に従って実行する必要があるタスクの概要です。

- ドライバマニフェスト、グローバル環境設定値、およびパスワード同期ポリシーをドライバ環境設定に追加します。追加するポリシーのリストについては、『Novell Identity Manager 3.0 管理ガイド』の「ドライバ設定で必要なポリシー」を参照してください。
- フィルタを変更すると、nspmDistributionPassword 属性を購読者は通知し、発行者は無視することができます。

前提条件

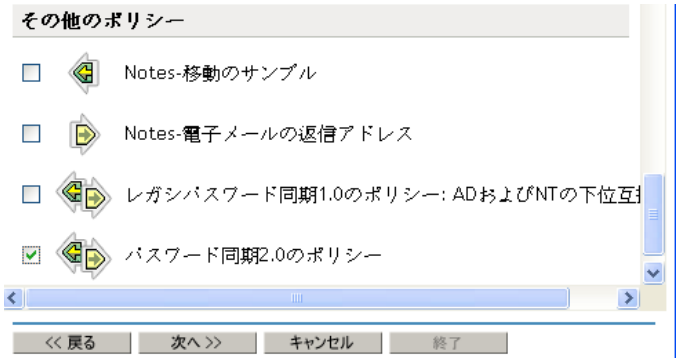
- ❑ 『Novell Identity Manager 3.0 管理ガイド』で「DirXML 1.1a から Identity Manager 形式へのドライバ環境設定のアップグレード」にある説明に従って、既存のドライバを Identity Manager 形式に変換したことを確認します。
- ❑ ドライバエクスポートウィザードを使用し、既存のドライバのバックアップを作成します。
- ❑ 新しいドライバシムがインストール済みであることを確認します。［パスワードステータスの確認］など、パスワード同期の機能の中には、Identity Manager のドライバシムがないと機能しないものもあります。

手順

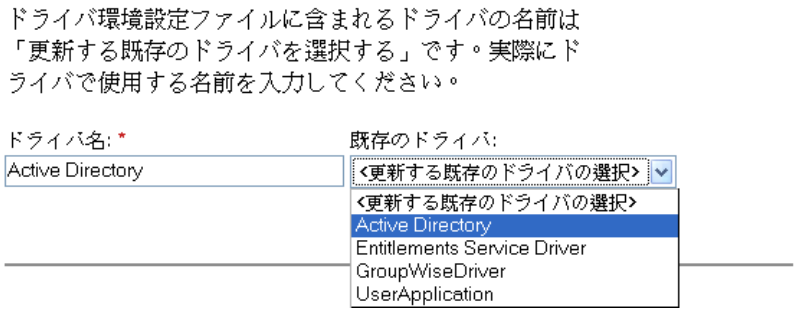
1 iManager で、［Identity Manager ユーティリティ］>［ドライバのインポート］の順にクリックします。

ドライバインポートウィザードが開きます。

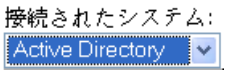
2 既存のドライバの存在するドライバセットを選択し、［次へ］をクリックします。



3 表示されるドライバ環境設定のリストで、［パスワード同期 2.0 のポリシー］を選択して、［次へ］をクリックします。



4 ドロップダウンリストから［Active Directory］を選択します。



5 接続システムとして［Active Directory］を選択し、［次へ］をクリックします。

6 ドライバの機能と接続システムに関する 3 つのプロンプトに［はい］と回答します。

- 接続システムが Identity Manager にパスワードを提供できるかどうか。
- 接続システムがIdentity Managerからのパスワードを受け入れることができるかどうか。
- パスワードが Identity Manager のパスワードに一致しているかを、接続システムが確認できるかどうか。

7 ［次へ］をクリックして、ドライバに関するすべてを更新するように選択します。

このオプションでは、パスワード同期に必要なドライバマニフェスト、グローバル環境設定値 (GCV)、およびパスワードポリシーを指定します。

ドライバマニフェストと GCV により既存の値が上書きされますが、Identity Manager にはほかにこのようなドライバパラメータがなかったため、上書きする既存の値はありません。

パスワードポリシーでは、既存のポリシーオブジェクトは上書きされません。単にドライバオブジェクトに追加されます。

保存するドライバマニフェストまたは GCV がある場合は、そのドライバの［該当ドライバで選択したポリシーのみを更新］という名前のオプションを選択し、すべてのポリシーのチェックボックスをオンにします。このオプションは、パスワードポリシーをインポートしますが、ドライバマニフェストまたは GCV は変更しません。

8 ［次へ］をクリックし、［終了］をクリックしてウィザードを完了します。

この時点では、新しいポリシーはドライバオブジェクトの下のポリシーオブジェクトとして作成されています。ただし、新しいポリシーはドライバ環境設定の一部になっていません。環境設定にリンクさせるには、発行者および購読者チャネルのドライバ環境設定の右側のポイントに、各ポリシーを手動で挿入する必要があります。

9 新しい各ポリシーを既存のドライバ環境設定の正しい場所に挿入します。

ポリシーセットに複数のポリシーがある場合は、これらのパスワード同期のポリシーが最後に表示されるようにしてください。

ポリシーのリストと挿入場所については、『Novell Identity Manager 3.0 管理ガイド』の「ドライバ設定で必要なポリシー」を参照してください。

ポリシーごとに、ステップ 9a ～ 9e を繰り返します。

9a ［Identity Manager］>［Identity Manager の概要］の順に選択し、更新するドライバが含まれているドライバセットを選択します。

9b 更新したドライバをクリックします。

ページが開いて、ドライバ環境設定がグラフィカル表示されます。

9c 新しいポリシーのいずれかを追加する必要がある場所のアイコンをクリックします。

9d ［挿入］をクリックし、新しいポリシーを追加します。

表示される［挿入］ページで、［既存のポリシーを使用する］をクリックし、新しいポリシーオブジェクトを参照して、［OK］をクリックします。

9e 新しいポリシーのいずれかのリストに複数のポリシーがある場合は、矢印ボタン を使用して、新しいポリシーをリスト内の正しい場所に移動します。

ポリシーが『Novell Identity Manager 3.0 管理ガイド』の「ドライバ設定で必要なポリシー」に示す順になっていることを確認してください。

10 nspmDistributionPassword 属性を同期できるようにドライバのフィルタを変更します。

購読者チャネルでのみ通知を有効にします。発行者チャネルを［無視］に設定します。

11 必要に応じて SSL を設定します。

手順については、19 ページのセクション 2.3「セキュリティ問題の対処」を参照してください。

Active Directory (購読者チャネル) でパスワードを設定するドライバの機能には、次のいずれかの条件に基づいて提供される安全な接続が必要です。

- ドライバを実行するコンピュータがドメインコントローラと同じコンピュータである。
- ドライバを実行するコンピュータがドメインコントローラと同じドメインにある。
- 同じドメインにないコンピュータの場合は、そのコンピュータとドメインコントローラの間で［シンプル］方式および SSL を設定する必要があります。双方向のパスワード同期機能は、［ネゴシエーション］認証メカニズムを採用する場合に限り使用できます。

手順については、Microsoft のマニュアル (『Configuring Digital Certificates on Domain Controllers (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/secwin2k/a0701.asp)』など) を参照してください。

12 新しいパスワード同期フィルタをインストールし、接続システムで Identity Manager へのユーザパスワードを設定する場合は、それらのフィルタを設定します。77 ページのセクション 7.5「パスワード同期のフィルタの設定」を参照してください。

この時点で、ドライバには、パスワード同期をサポートするために必要な新しいドライバシム、Identity Manager 形式、およびその他の要素 (ドライバマニフェスト、GCV、パスワード同期化ポリシー、フィルタなど) が設定されます。これで、iManager のパスワード同期インタフェースを使用して、接続システムとパスワードをやりとりする方法を指定できます。

13 ドライバ向けのパスワードポリシーとパスワード同期の設定を使用して、使用するパスワード同期のシナリオを準備します。

『Novell Identity Manager 3.0 管理ガイド』の「パスワード同期の実装」を参照してください。

14 パスワード同期に使用するすべてのドライバに対してステップ 1 ～ 14 を繰り返します。

7.5 パスワード同期のフィルタの設定

ドライバは、1 台の Windows コンピュータだけで実行するよう設定する必要があります。

ただし、ドライバをインストールして設定したら、その他の各ドメインコントローラで次の作業を行います。

1 パスワードフィルタ (pwfilter.dll ファイル) をインストールします。

2 パスワードをキャプチャするようレジストリを設定して、パスワードを Identity Manager に送信できるようにします。

パスワードフィルタは、ドメインコントローラが起動されると自動的に開始されます。このフィルタでは、ユーザが Windows クライアントを使用して行ったパスワード変更のキャプチャ、変更の暗号化、および Identity Manager データストアを更新するためのドライバへの変更の送信が行われます。

注 : パスワード同期の設定については、『Novell Identity Manager 3.0 管理ガイド』の「パスワード同期の実装」を参照してください。

パスワードフィルタの設定と管理を容易にするには、ドライバのインストール時に Identity Manager PassSync ユーティリティをコントロールパネルに追加します。このユーティリティでは、使用するドメインコントローラのレジストリへのリモートアクセスを許可するかどうかに応じて、パスワードフィルタを設定する場合に次のどちらかを選択できます。

- レジストリへのリモートアクセスを許可する場合 : ドライバを実行する予定の 1 台のコンピュータから、Identity Manager PassSync ユーティリティを使用して、すべてのドメインコントローラのパスワードフィルタを設定します。

  この方法では、1 箇所からすべてのドメインコントローラを設定できます。

1 台のコンピュータからすべてのドメインコントローラを設定する場合、Identity Manager PassSync ユーティリティで、設定に役立つ次の機能が提供されます。

- パスワード同期に使用するドメインを指定できる。
- ドメインのすべてのドメインコントローラを自動的に検出する。
- 各ドメインコントローラに pwfilter.dll をリモートでインストールできる。
- ドライバが実行しているコンピュータ上および各ドメインコントローラ上のレジストリを自動的に更新する。
- 各ドメインコントローラのフィルタのステータスを表示できる。
- ドメインコントローラをリモートで再起動できる。

  この機能は、パスワード同期に備えて初めてドメインを追加する場合に必要です。この理由は、パスワード変更をキャプチャするフィルタが DLL ファイルで、ドメインコントローラの起動時に開始されるためです。

78 ページのセクション 7.5.1「1 台のコンピュータによるすべてのドメインコントローラのパスワードフィルタの設定」を参照してください。

- レジストリへのリモートアクセスを許可しない場合 : 各ドメインコントローラで個別にパスワードフィルタを設定します。この操作を行うには、各ドメインコントローラで、ドライバファイルをインストールして Identity Manager PassSync ユーティリティを用意します。次に、各コンピュータでこのユーティリティを使用してパスワードフィルタをインストールし、レジストリを更新します。

  82 ページのセクション 7.5.2「各ドメインコントローラのパスワードフィルタの個別設定」を参照してください。

7.5.1 1 台のコンピュータによるすべてのドメインコントローラのパスワードフィルタの設定

この手順では、各ドメインコントローラにパスワードフィルタをインストールして設定する方法について説明します。操作はすべて、ドライバを実行している同じコンピュータから行います。

レジストリへのリモートアクセスを許可する場合は、この方法を採用してください。

フィルタを設定するには、ドメインコントローラを再起動する必要があるため、後でこの手順を実行するか、またはドメインコントローラを 1 つずつ再起動した方がよい場合があります。ドメインに複数のドメインコントローラがある場合は、パスワード同期を機能させる各ドメインコントローラにフィルタをインストールして再起動する必要がある点に留意してください。

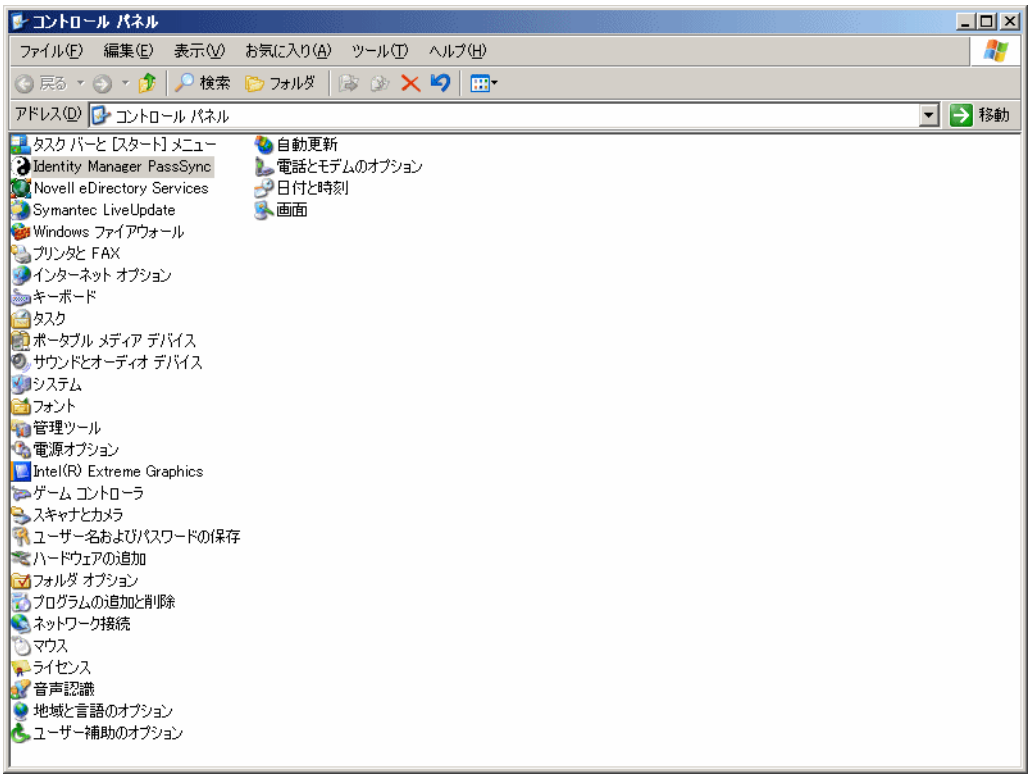
1 ドメインコントローラ上および Active Directory 用の Identity Manager ドライバが実行するように設定されるコンピュータ上のポート 135 (RPC エンドポイントマッパー) にアクセスできることを確認します。

  NetBIOS over TCP を使用している場合は、次のポートも必要です。

  - 137: NetBIOS ネームサービス
  - 138: NetBIOS データグラムサービス
  - 139: NetBIOS セッションサービス

ファイアウォールを使用すると、リモートからこれらのポートにアクセスできないようにすることができます。

2 ドライバをインストールするコンピュータで、［スタート］>［設定］>［コントロールパネル］をクリックします。



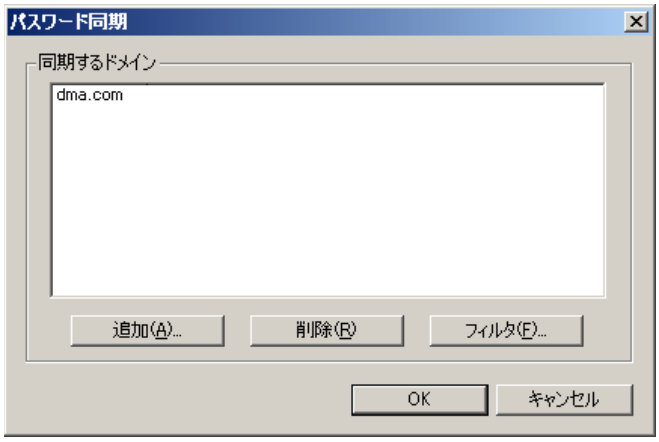
3 ［Identity Manager PassSync］をダブルクリックします。

このユーティリティを初めて開くと、このコンピュータが Identity Manager ドライバのインストール先であるかどうかが尋ねられます。

環境設定を完了したら、リストからこのドメインを削除しない限り再びこのプロンプトは表示されません。

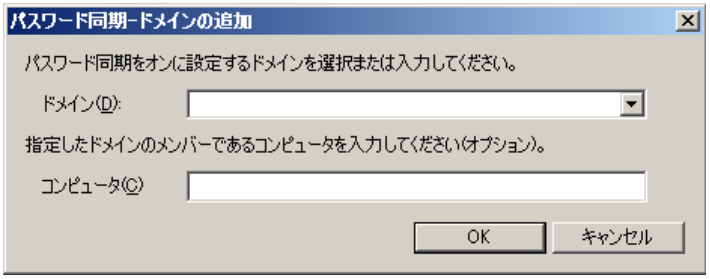
4 ［はい］をクリックします。

［同期するドメイン］というラベルのリストが表示されます。



5 パスワード同期に使用するドメインを追加するには、［追加］をクリックします。

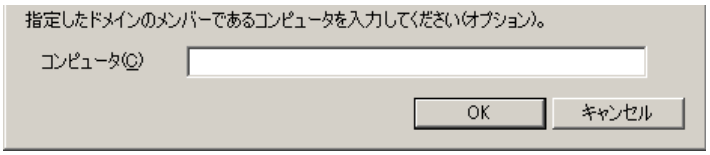
［ドメインの追加］ダイアログボックスが表示されます。



6 追加するドメイン名を指定または選択します。

ドロップダウンリストに既知のドメインが表示されます。

7 (オプション) ドメイン内のコンピュータを指定します。



［コンピュータ］編集ボックスを空白のままにすると、ローカルコンピュータが自動的に照会されます。したがって、ドメインコントローラで PassSync を実行している場合は、名前を入力する必要はありません。PassSync で、ローカルコンピュータ (この場合はドメインコントローラ) が照会され、ドメイン内のすべてのドメインコントローラのリストが (データベースから) 取得されます。

ドメインコントローラにインストールしていない場合は、ドメイン内にあってドメインコントローラに到達できるコンピュータの名前を入力します。

PassSync でドメインが見つからないことを示すエラーメッセージが表示される場合は、別の名前を入力します。

8 ドメインの DNS 名を使用するかどうかを決定します。

DNS 名により、高度な認証および大規模なインストール環境でドメインをより確実に検出するための機能が提供されます。ただし、選択肢は各自の環境によって異なります。

9 管理者権限でログインします。

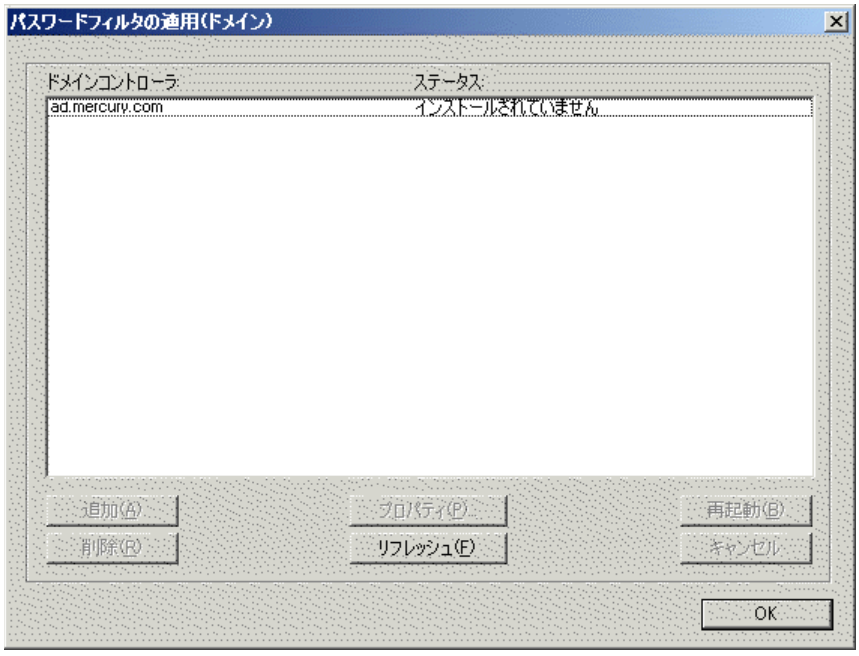
Identity Manager PassSync ユーティリティで、該当するドメインのすべてのドメインコントローラが検出され、各ドメインコントローラに pwfilter.dll がインストールされます。また、ドライバを実行しているコンピュータ上および各ドメインコントローラ上のレジストリも自動的に更新されます。この操作には、数分かかる場合があります。

pwfilter.dll では、ドメインコントローラが再起動されるまでパスワードの変更がキャプチャされません。Identity Manager PassSync ユーティリティを使用すると、すべてのドメインコントローラのリストおよびドメインコントローラのフィルタのステータスを参照できます。また、このユーティリティからドメインコントローラを再起動することもできます。

10 リスト内のドメインの名前をクリックして、[フィルタ] をクリックします。

このユーティリティで、すべてのドメインコントローラの名前およびそれぞれのフィルタのステータスが表示されます。

各ドメインコントローラのステータスには、再起動を必要とすることが示されます。ただし、ユーティリティでその自動タスクを完了するのに数分かかるので、その間はステータスが [不明] と表示される場合があります。



11 各ドメインコントローラを再起動します。

各自の環境でつじつまが合うようにドメインコントローラを一度に再起動してもかまいません。パスワード同期は、あらゆるドメインコントローラが再起動されるまでは完全に機能しないことに留意してください。

12 すべてのドメインコントローラのステータスが［稼動中］になっている場合は、パスワード同期をテストしてそれが機能していることを確認します。

13 さらにドメインを追加するには、［OK］をクリックしてドメインのリストに戻り、ステップ 6 ～ステップ 12 を繰り返します。

7.5.2 各ドメインコントローラのパスワードフィルタの個別設定

この節に記載している手順では、各ドメインコントローラでパスワードフィルタをインストールおよび設定する方法を 1 つずつ説明します。

レジストリへのリモートアクセスを許可しない場合は、この方法を採用してください。

この手順では、ドライバをインストールして Identity Manager PassSync ユーティリティを用意します。次に、このユーティリティを使用して pwfilter.dll ファイルをインストールし、使用するポートを指定して、Active Directory 用の Identity Manager ドライバを実行しているホストコンピュータを指定します。

フィルタを設定するには、ドメインコントローラを再起動する必要があるため、後でこの手順を実行するか、またはドメインコントローラを 1 つずつ再起動した方がよい場合があります。ドメインに複数のドメインコントローラがある場合は、パスワード同期を機能させる各ドメインコントローラにフィルタをインストールして再起動する必要がある点に留意してください。

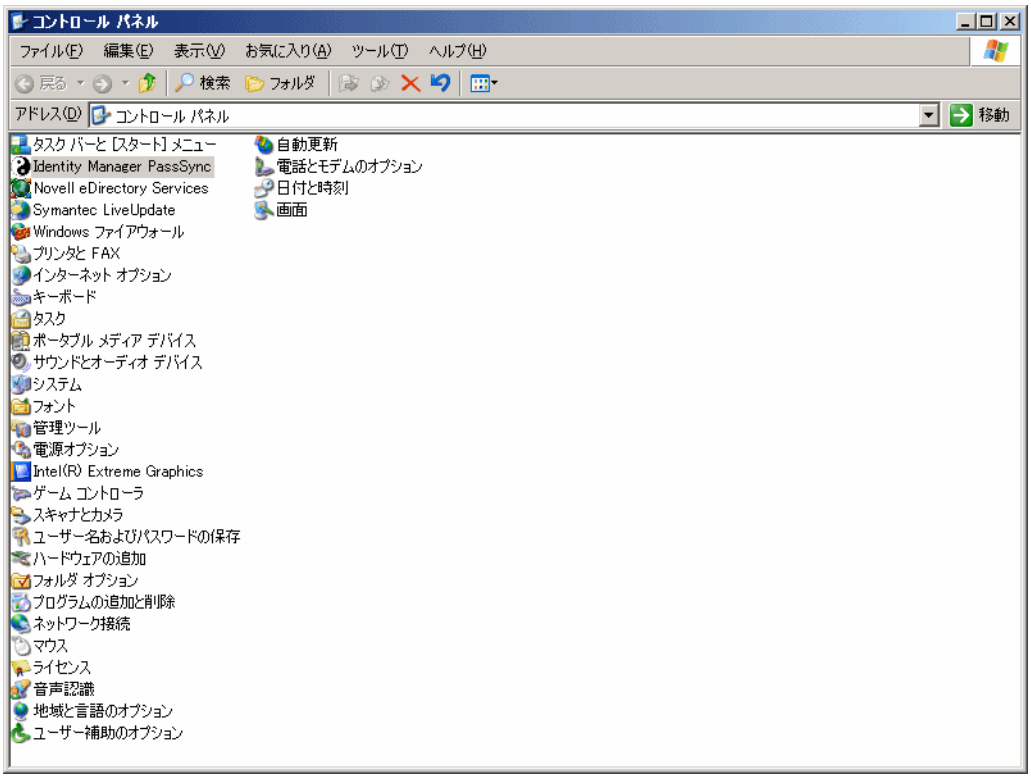
1 ドメインコントローラおよび Active Directory 用の Identity Manager ドライバが実行するよう設定されているコンピュータの両方で使用可能なポートを確認します。

- 135: RPC エンドポイントマッパー
- 137: NetBIOS ネームサービス
- 138: NetBIOS データグラムサービス
- 139: NetBIOS セッションサービス

2 ドメインコントローラで、Identity Manager のインストールを利用して、Active Directory 用の Identity Manager ドライバだけをインストールします。

ドライバをインストールすると、Identity Manager PassSync ユーティリティがインストールされます。

3 ［スタート］>［設定］>［コントロールパネル］の順にクリックして、Identity Manager PassSync ユーティリティを検索します。



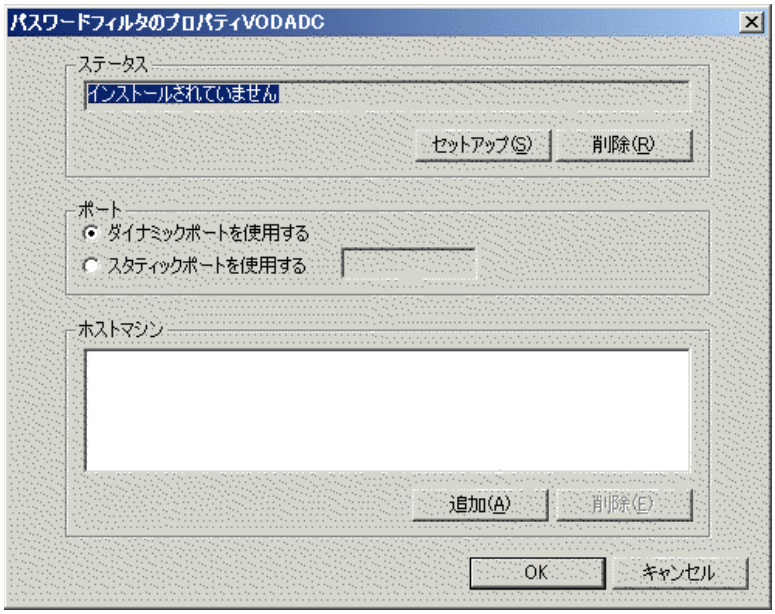
4 ［Identity Manager PassSync］をダブルクリックします。

このユーティリティを初めて開くと、このコンピュータが Identity Manager ドライバのインストール先であるかどうかが尋ねられます。

5 ［いいえ］をクリックします。

環境設定を完了したら、［Password Filter Properties (パスワードフィルタのプロパティ)］ダイアログボックスで、［削除］ボタンを使用してパスワードフィルタを削除しない限り再びこのプロンプトは表示されません。

［いいえ］をクリックすると、［Password Filter Properties (パスワードフィルタのプロパティ)］ダイアログボックスが開かれ、このドメインコントローラのパスワードフィルタが設定されていないことを示すステータスメッセージが表示されます。



6 ［セットアップ］ボタンをクリックして、パスワードフィルタ pwfilter.dll をインストールします。

7 ［ポート］設定では、ダイナミックポートまたはスタティックポートを使用するかどうかを指定します。

ドメインコントローラのリモートプロシージャコール (RPC) をデフォルトと異なる設定にする場合に限り、スタティックポートオプションを使用します。

8 Identity Manager ドライバの場所を指定して、［追加］ボタンをクリックします。次に、［パスワード同期フィルタ - ホストの追加］ダイアログボックスで Identity Manager ドライバを実行しているコンピュータのホスト名を指定して、［OK］をクリックします。

このステップは、パスワードフィルタにパスワード変更の送信先をわからせるために必要です。パスワードフィルタで、パスワード変更をキャプチャして、Identity Manager データストアを更新するためにそうした変更を Identity Manager ドライバに送信する必要があります。

9 ［Password Filter Proper (パスワードフィルタのプロパティ)］ダイアログボックスで、［OK］をクリックします。

10 ドメインコントローラを再起動して、パスワードフィルタのインストールを完了します。

各自の環境でつじつまが合うようにドメインコントローラを一度に再起動してもかまいません。パスワード同期は、あらゆるドメインコントローラがパスワードフィルタのインストール後に再起動されるまでは完全に機能しないことに留意してください。

インストールが完了してドメインコントローラが再起動されたら、ドメインコントローラの起動時に毎回パスワードフィルタが自動的にロードされます。

11 パスワードフィルタのステータスをもう一度チェックするには、［スタート］>［設定］>［コントロールパネル］をクリックして、［Identity Manager PassSync］ユーティリティをダブルクリックします。

ステータスが［稼動中］になっていることを確認します。

12 パスワード同期に使用するドメインコントローラごとにステップ 2 ～ステップ 11 を繰り返します。

13 すべてのドメインコントローラのステータスが［稼動中］になっている場合は、パスワード同期をテストしてそれが機能していることを確認します。

7.6 障害発生後の同期の再試行

ドライバおよびパスワードフィルタは、障害発生後にパスワード同期を再試行する動作を改善するために機能強化されました。

7.6.1 「追加」イベントまたは「変更」イベント後の再試行

Active Directory から送信されたパスワード変更がアイデンティティボールトで正常に完了されない場合は、ドライバによりパスワードがキャッシュに格納されます。パスワードの所有ユーザの「追加」イベントまたは「変更」イベントが発生するまで、パスワード変更の再試行は行われません。(以前は、このような保存されたパスワードがポーリング間隔で毎回再試行されていました)。

ドライバで Active Directory での変更をポーリングすると、そのドライバがユーザの「追加」イベントまたは「変更」イベントを受信します。ドライバでは、ユーザの「追加」イベントまたは「変更」イベントごとに、この新規ユーザ向けの保存されたパスワードがあるかどうかが確認されます。パスワードがある場合は、そのパスワードが変更ユーザイベントとしてアイデンティティボールトに送信されます。

パスワード同期が失敗したときにユーザに電子メールメッセージを送信するようパスワード同期を設定した場合は、この機能拡張により、ユーザが受信する電子メールの数は最小限に抑えられます。

7.6.2 パスワード期限の時刻

［パスワード期限の時刻］という名前のパラメータが追加されました。このパラメータでは、同期が最初の試行で正常に終了していない場合に特定のユーザのパスワードを保存する期間を決定できます。パスワードがアイデンティティボールトで正常に変更されるまで、または［パスワード期限の時刻］を経過するまで、ドライバによりパスワードが保存されます。

サンプルドライバ環境設定ファイルをインポートする場合は、有効期限の指定を要求するメッセージが表示されます。期限を指定しない場合、または期限 (間隔フィールド) に無

効な文字が含まれている場合、デフォルトの設定は 60 分です。指定した期限が、指定したポーリング間隔の 3 倍より短い場合は、ポーリング間隔の 3 倍になるようにドライバで期限が変更されます。

どんなパスワードの一時的なバックログでも処理できる十分に大きい値を設定します。一括変更する場合は、すべての変更を処理できるようにタイムアウトを大きく設定します。経験的には、パスワードあたりに 1 秒を考慮します。たとえば、18,000 のパスワードを同期するには、300 分 (18,000 パスワード /60 秒) を考慮します。

-1 を設定すると無期限になります。この設定で一括変更を処理できますが、問題が生じる場合があります。たとえば、アカウントが関連付けられていないため、パスワードが同期されないことがあります。したがって、そのようなパスワードは永久にシステムに残ります。同様の状況が数多い場合、同期されていない大量のパスワードはシステムで保持することになります。

［パスワード期限の時刻］に関するシナリオ

発行者チャネルでは、パスワード同期が「追加」イベントより先に発生する場合があります。その場合は、ドライバで「追加」イベントの直後に再試行されます。

シナリオ : 影響なし

新規ユーザとパスワードを Active Directory で作成します。フィルタにより、直ちに新しいパスワードがドライバに送信されます。ただし、ポーリングの間にイベントが発生したため、ユーザの「追加」イベントはドライバで受信されていません。また、ドライバでアイデンティティボールトにユーザが作成されていないため、パスワード同期は、この最初に試行した時点で正常に終了していません。ドライバにより、このパスワードがキャッシュに格納されます。

次のポーリング間隔で、新規ユーザの「追加」ユーザイベントがドライバで受信されます。ドライバでは、この新規ユーザ向けのキャッシュされたパスワードがあるかどうかも確認されます。ドライバで「追加」ユーザイベントがアイデンティティボールトに送信され、パスワードを同期するために「変更」ユーザイベントも送信されます。

この場合、パスワード同期は 1 回のポーリング間隔だけ遅延されます。

この状況では、［パスワード期限の時刻］パラメータに影響はありません。

シナリオ : 有効期限の延長

新規ユーザとパスワードを Active Directory で作成します。ただし、ユーザ情報が Active Directory ドライバの作成ポリシーの要件を満たしていません。

たとえば、作成ルールではフルネームを必要としますが、必要な情報がないとします。「影響なし」の例と同様に、フィルタにより、パスワード変更が直ちにドライバに送信されます。しかし、ユーザが存在しないため、最初に試行した時点でパスワード変更がアイデンティティボールトにおいて正常に終了していません。ドライバにより、このパスワードがキャッシュに格納されます。

ただし、この場合、ドライバで Active Directory での変更のポーリングおよび新規ユーザの検出が行われても、ユーザ情報が作成ポリシーの要件を満たしていないため、新しいユーザを作成できません。

新規ユーザの作成およびパスワードの同期は、作成ポリシーを満たすために Active Directory ですべてのユーザ情報が追加されるまで遅延されます。次に、アイデンティ

ティボールトで新規ユーザが追加され、この新規ユーザ向けのパスワードがキャッシュに格納されているかどうかが確認され、パスワードを同期するために「変更」ユーザイベントが送信されます。

［パスワード期限の時刻］パラメータは、Active Directory でのユーザ情報が作成ポリシーの要件を満たすのに時間がかかる場合に限り、このシナリオに影響します。パスワードが期限切れになった後に「追加」イベントが発生し、該当ユーザのパスワードがキャッシュに格納されていない場合、同期は行われません。キャッシュに格納されたパスワードがないため、ドライバではパスワードポリシーのデフォルトのパスワードが使用されます。

ユーザが Active Directory またはアイデンティティボールトでパスワードを変更したら、パスワードは同期されます。

パスワードの双方向フローに備えてパスワード同期が設定されている場合は、アイデンティティボールトでパスワード変更が行われたときにアイデンティティボールトから Active Directory に対してパスワードを同期することもできます。

作成ポリシーの制限が厳しく、一般に Active Directory で新規ユーザの情報すべてを入力するのに 2 日以上かかる場合は、適宜［パスワード期限の時刻］パラメータ間隔を長くすることができます。次に、最終的にユーザがアイデンティティボールトで作成されるまでパスワードをキャッシュに格納できます。

シナリオ : 要件の不適合

ユーザとパスワードを Active Directory で作成します。ただし、このユーザは、Active Directory ドライバの作成ポリシーの条件を満たしていません。

たとえば、Active Directory の新規ユーザには、ユーザが契約社員であることを示す説明があり、ビジネスポリシーにより、契約社員にはアイデンティティボールトに対応するユーザアカウントを設定しないようにしているため、作成ポリシーで契約社員のユーザオブジェクトが作成されないようになっているとします。前の例と同様に、パスワード変更はフィルタで直ちに送信されますが、パスワード同期は最初の試行時に正常に終了していません。ドライバにより、このパスワードがキャッシュに格納されます。

この場合、対応するユーザアカウントはアイデンティティボールトで作成されません。したがって、キャッシュされたパスワードは同期されません。［パスワード期限の時刻］が経過したら、そのキャッシュからユーザパスワードが削除されます。

シナリオ : 電子メール通知

Markus には、Active Directory アカウントおよび対応するアイデンティティボールトアカウントがあります。彼は、自分の Active Directory パスワードを変更します。このパスワードは 6 文字です。しかし、このパスワードは、管理者が eDirectory で作成したパスワードポリシーに規定されている最低 8 文字を満たしていません。パスワード同期は、ポリシーを満たさないパスワードを拒否してパスワード同期に失敗したことを示す通知電子メールを Markus に送信するよう設定されています。このパスワードはキャッシュに格納され、Active Directory でユーザオブジェクトを変更する場合に限りこのパスワードが再試行されます。

この場合、Markus は、パスワードを変更した直後にパスワード同期が正常に終了していないことを示す電子メールを受信します。Markus は、パスワードの再試行のたびに同じ電子メールメッセージを受信します。

Markus が、Active Directory でのパスワードを、パスワードポリシーに従ったパスワードに変更すると、アイデンティティボールトに対する新しいパスワードがドライバで正常に同期されます。

Markus が、ポリシーに従ったパスワードに変更しなかった場合、パスワード同期は正常に終了しません。［パスワード期限の時刻］が経過すると、キャッシュされたパスワードが削除され、再試行されなくなります。

トラブルシューティング 8

8.1 発行者または購読者からの変更が同期していない

Active Directory での変更を同期するには、Identity Manager ドライバで使用されるアカウントに適切な権限を設定する必要があります。必要な権限については、24 ページのセクション 2.4「管理用アカウントの作成」を参照してください。

デフォルトのポリシーを使用する場合は、作成、一致、配置の各ポリシーの要件も満たす必要があります。デフォルトのポリシーの要件については、10 ページの 「ポリシー」を参照してください。

属性 dirxml-uACLockout は、発行者チャネルでは同期されません。

8.2 NT ログオン名として有効でない文字の使用

デフォルトの購読者作成ポリシーでは、アイデンティティボールトでのアカウントの相対識別名に基づいて NT ログオン名 (別名 : sAMAccountName および旧 Windows 2000 ログオン名) が生成されます。NT ログオン名には、ASCII 文字セットのサブセットが使用されます。デフォルトのポリシーでは、有効でない文字を除去した後に Active Directory でオブジェクトが作成されます。

このポリシーが自社のビジネスルールを満たさない場合は、インポート後にポリシーを変更できます。従来の ASCII 文字セット以外のアイデンティティボールトアカウント名を使用するビジネスでは、このポリシーに対して特に注意を払う必要があります。

8.3 c、co、countryCode の各属性の同期

Active Directory 管理コンソールを使用してユーザの国を選択する場合は、次の 3 つの属性が設定されます。

表 *8-1* 国の属性

属性	説明
c	ISO で定義された 2 文字の国コードが含まれます。
co	国名が含まれます。
countryCode	国を表す数値 (ISO でも定義済み) が含まれます。

ISO 定義による数値の国コードは、英字を処理できないアプリケーション用になっているため、デフォルトでは、アイデンティティボールトでのスキーマに c と co は含まれますが、countryCode は含まれません。

Identity Manager では、c と co をマッピングできます。また、同様の属性を eDirectory スキーマに追加すれば、countryCode をマッピングすることもできます。

Active Directory の管理コンソールでは、この 3 つの属性の同期を維持させようとします。そのため、コンソールで国を設定すると、3 つの属性すべてに適切な値が設定されます。一部の管理者は、Identity Manager を介して属性が設定されるときに同様の動作を必要とする場合があります。たとえば、フィルタに c しかなくても、購読者チャネルで c の変更が送信されたときに co と countryCode も設定されるようにドライバを設定できます。

8.4 オペレーショナル属性の同期

オペレーショナル属性とは、LDAP サーバで保持される、特別な操作情報を含む属性のことです。オペレーショナル属性は読み込み専用です。この属性を同期および変更することはできません。

8.5 Windows 2003 のパスワードの複雑さ

パスワードは、パスワードポリシーで指定された条件を満たす必要があります。

Windows 2000/2003 のパスワードポリシーの複雑さと要件は、eDirectory での複雑さと要件とは異なります。

パスワード同期を利用する場合は、Active Directory と eDirectory™ の両方の複雑なルールに適合するパスワードを作成および使用します。適合しない場合、パスワードはエラーになります。

ヒント **:** 両方のシステムのパスワードポリシーをできるだけ互いに類似させてください。テスト環境では、Windows 2003 サーバの強力なパスワード機能を無効にしてから、Active Directory ドライバをインストールします。Active Directory ドライバが正常に機能したら、eDirectory と Active Directory で使用されるパスワードが両方のシステムの複雑なルールを満たしていることを確認してください。次に、Windows 2003 サーバの強力なパスワード機能をもう一度有効にします。

トラブルシューティングのヒントについては、TID 10083320 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10083320.htm) を参照してください。

8.6 エラーメッセージ LDAP_SERVER_DOWN

通常、エラーコード LDAP_SERVER_DOWN は、同期用に設定された Active Directory ドメインコントローラの LDAP ポートをドライバで開くことができないことを示します。このようになる理由はいくつかあります。

- ドライバ認証コンテキストで指定されているサーバが正しくありません。認証コンテキストでは、同期用のドメインコントローラの DNS 名または IP アドレスを保持する必要があります。パラメータを空のままにすると、ドライバシムを実行しているコンピュータ (IDM を実行している同じサーバまたはリモートローダをホストしているサーバ) への接続が試行されます。
- 認証コンテキストの IP アドレスを使用しているので、Active Directory に対する Kerberos 以外の認証を無効にしたことになっています。Kerberos では、認証コンテキストの DNS 名が必要です。

  ドライバシムでは、旧 Windows 2000 ログオン方式または単純なバインドを使用してのみ認証できます。ネットワーク上の NTLM、NTLM2、および単純なバインドを無効にした場合は、LDAP_SERVER_DOWN メッセージが表示される可能性があります。
- Active Directory への SSL 接続を使用するようにドライバが設定されています。このメッセージは、ドライバシムサーバにインポートした証明書に何らかの誤りがある (または証明書がインポートされていない) ことを示しています。

8.7 パスワード同期のヒント

パスワードを同期している場合は、安全な接続を使用することをお勧めします。次のそれぞれの間の接続は脆弱です。

- メタディレクトリエンジンとリモートローダ
- リモートローダと Active Directory

  この脆弱性は、接続先のドメインコントローラからリモートでリモートローダを実行する場合に限ります。
- リモートローダを使用していない場合のメタディレクトリエンジンと Active Directory

  この脆弱性は、ドメインコントローラがこのコンピュータに対してローカルでない場合に限ります。

安全な接続を作成するには、次の操作を 1 つ以上実行します。

- メタディレクトリエンジンとリモートローダの間で SSL を設定する
- ドメインコントローラでリモートローダを実行する
- ドライバシムと Active Directory の間で SSL を設定する

  接続先のドメインコントローラでドライバを実行している場合は、これには該当しません。

ドライバシムがドメインコントローラで実行していなくてもパスワード同期が機能するように、SSL を設定する必要があります。

8.7.1 初期パスワードの設定

ユーザを最初に作成したときにパスワードが準拠していないというエラーが表示された場合は、パスワードポリシーを確認する必要があります。

たとえば、Active Directory ドライバによりアイデンティティボールトで新しいユーザオブジェクトを作成するときに、Active Directory ドライバにユーザの初期パスワードを設定させるとします。ユーザを作成すると、ドライバシムでユーザが作成された後、パスワードが設定されます。

ユーザの追加とパスワードの設定は別々に行われるため、新規ユーザは一時的のみであってもデフォルトのパスワードを受信します。ユーザを追加した直後に Active Directory ドライバでパスワードが送信されるため、パスワードはすぐに更新されます。

デフォルトのパスワードがユーザの eDirectory のパスワードポリシーに従っていない場合は、エラーが表示されます。たとえば、ユーザの名字を使用して作成されたデフォルトのパスワードが短すぎてパスワードポリシーに準拠できない場合は、パスワードが短すぎることを示す -216 エラーが表示されます。ただし、その後 Active Directory ドライバでポリシーに準拠する初期パスワードが送信されると、この状況はすぐに解決されます。

使用しているドライバにかかわらず、ユーザオブジェクトを作成する接続システムで初期パスワードを設定するようにするには、次のいずれかを行うことを検討します。

- 組織向けにアイデンティティボールトで定義されたパスワードポリシー (パスワードの管理の［Manage Password Policies (パスワードポリシーの管理)］オプションを使用して作成) にデフォルトのパスワードが準拠するように、デフォルトのパスワードを作成する発行者チャネルのポリシーを変更します。初期パスワードが信頼されるアプリケーションで設定されると、デフォルトのパスワードが上書きされます。

  このオプションが優先されます。システム内で高レベルのセキュリティを維持するために、デフォルトのパスワードポリシーを用意することをお勧めします。
- デフォルトのパスワードを作成する、発行者チャネルのポリシーを削除します。サンプルの環境設定では、このポリシーはコマンド変換ポリシーセットにより提供されます。eDirectory では、パスワードのないユーザも追加できます。このオプションは、新しく作成されたユーザオブジェクトのパスワードが最終的に購読者チャネルから提供されることを想定しているので、ユーザオブジェクトは一時的にパスワードなしの状態になります。

これらの方法は、初期パスワードが「追加」イベントで提供されなくても、それ以降のイベントとして提供される場合には、特に重要です。

8.8 SSL パラメータを設定する場所

ドライバ環境設定の SSL パラメータは、Active Directory ドライバと Active Directory の間の SSL 用です。このパラメータは、メタディレクトリエンジンとリモートローダの間の SSL 用ではありません。20 ページの 「暗号化」を参照してください。

8.9 購読者チャネルでユーザが追加した後に無効にされた Active Directory アカウント

デフォルトの環境設定では、アイデンティティボールトの「ログインの無効化」属性を Active Directory での userAccountControl 属性の dirxml-uACAccountDisable ビットにマッピ

ングします。購読者追加操作では、「ログインの無効化」を false (アカウントが有効) に設定できますが、追加操作の発行者ループバックでは、「ログインの無効化」が true (アカウントが無効) であるとレポートされます。

さらに、Active Directory 内のオブジェクトを調べると、アカウントが無効にされていることを示す場合があります。このようになる理由には、ドライバで Active Directory のオブジェクトを作成する方法や、ドライバと Active Directory 自体の間のポリシーなどがあります。

8.9.1 ［Active Directory ユーザーとコンピュータ］で無効にされたアカウント

プロビジョニングサイクルが完了した後に Active Directory でアカウントが無効にされたままの場合は、Active Directory により実行されるドライバやポリシー向けに設定されたポリシー間に不一致が生じることがあります。

たとえば、パスワード要求ポリシーを考えてみます。ユーザ追加操作に無効なパスワードが含まれている (またはパスワードがない) 場合は、Active Directory で作成されたアカウントを無効にする必要があります。しかし、Active Directory では、ドライバの知識がなくても userAccountControl の dirxml-uACPasswordNotRequired ビットを設定できます。

このような操作を行うと、追加操作に dirxml-uACPasswordNotRequired のポリシーが含まれていない場合は、追加操作のログオン有効化アクションが失敗します。したがって、アカウントは無効のままになります。

後ほど (マージ操作のためほぼ直後)、ドライバで「ログインの無効化」を false に設定して、もう一度アカウントを有効にすることができます。Active Directory ポリシーを上書きしてアカウントのパスワードが常に要求されるようにする場合は、購読者チャネルで「ログインの無効化」が変更されるたびに dirxml-uACPasswordNotRequired を false に設定する必要があります。

8.10 子ドメインへの親メールボックスの移動

ユーザの homeMDB 属性を変更して親メールボックスを子ドメインのメールボックスストアに移動しても、移動は失敗します。エラーコード 0x80072030 が返されます。

このエラーは、ドメイン間の移動時に発生します。Exchange 親メールボックスを子ドメインへ移動することはできません。

8.11 Active Directory の復元

Active Directory の一部または全部を復元する必要がある場合は、一時的なイベントが取得され、アイデンティティボールトでの不必要なアクションが実行されることがあります。問題なく復元するには、復元操作中にドライバを一時的に使用不可にして、アイデンティティボールトを Active Directory と同期した状態に戻します。

1. ドライバを使用不可にします。
2. アイデンティティボールト内のドライバオブジェクトの Dirxml-DriverStorage 属性を削除します。
3. Active Directory を復元します。
4. Active Directory ドライバを［手動］または［自動］起動に設定します。

5 ドライバを起動します。

6 関連しないオブジェクトを検出するために再移行します。

8.12 別のドメインコントローラへのドライバの移動

別のドメインコントローラに対して同期するようドライバを設定するには、ドライバの［認証コンテキスト］パラメータを変更します。ドライバを再起動しても、Active Directory での変更を追跡するためにドライバで使用される状態情報が無効なので、Active Directory では、多数の古いイベントの再生により現時点の状態に戻される場合があります。

このような再生を防ぐには、次のように認証コンテキストの更新中にドライバの状態情報を削除します。

1 ドライバを停止します。

2 アイデンティティボールト内のドライバオブジェクトの Dirxml-DriverStorage 属性を削除します。

3［認証コンテキスト］パラメータを更新します。

4 ドライバを起動します。

この操作により、アイデンティティボールト内の関連付けられたオブジェクトの再同期が行われます。

5 Active Directory 内の関連しないオブジェクトを検出するために再移行します。

8.13 Active Directory からの移行

Active Directory からアイデンティティボールトに移行する場合は、Active Directory サーバでのオブジェクトの包含、DN 参照、および検索制限に注意する必要があります。包含を処理する一般的な方針では、最初にコンテナを移行し、次にグループのメンバーと考えられるオブジェクト (ユーザオブジェクトを含む) を移行して、最後にグループを移行します。ある程度の数のオブジェクトを移行する場合は、Active Directory サーバで設定されている LDAP 検索制約を処理するよう現在の方針を調整する必要があります。LDAP サーバの制約を変更するか、または毎回オブジェクトのサブセットだけを取得するよう移行を調整することができます (たとえば、コンテナ単位の移行や「A」、「B」などで始まるオブジェクトの移行を行うことができます)。

8.14 LDAP サーバの検索制約の設定

次に示すのは、NTDSUTIL.EXE を使用してドメインコントローラの LDAP 検索パラメータを変更する方法を示す端末セッションです。移行中の IDM 同期に使用されているドメインコントローラでこうした設定を変更するだけです。現在の環境設定の値を記録して、移行の完了後に NTDSUTIL.EXE を実行して元の値に戻します。NTDSUTIL.EXE は、任意のメンバーサーバ上で実行できます。

1 コマンドプロンプトで「ntdsutil」と入力します。

2「LDAP Policies」と入力して、<Enter> キーを押します。

3「Connections」と入力して、<Enter> キーを押します。

4「Connect to domain ドメイン名」と入力して、<Enter> キーを押します。

5「Connect to server サーバ名」と入力して、<Enter> キーを押します。

6「Quit」と入力して、<Enter> キーを押します。

7「Show Values」と入力して、<Enter> キーを押します。

```
C:\>ntdsutil ntdsutil: LDAP Policies ldap policy: Connections server
connections: Connect to domain raptor Binding to \\raptor1.raptor.lab
... Connected to \\raptor1.raptor.lab using credentials of locally
logged on user. server connections: Connect to server raptor1
Disconnecting from \\raptor1.raptor.lab... Binding to raptor1 ...
Connected to raptor1 using credentials of locally logged on user.
server connections: Quit ldap policy: Show Values

Policy                       Current(New) MaxPoolThreads
4 MaxDatagramRecv                  4096 MaxReceiveBuffer
10485760 InitRecvTimeout              120 MaxConnections
5000 MaxConnIdleTime                  900 MaxPageSize
1000 MaxQueryDuration                 120 MaxTempTableSize
10000 MaxResultSetSize                262144 MaxNotificationPerConn
5 MaxValRange                        1500ldap policy: set MaxQueryDuration
to 1200 ldap policy: set MaxResultSetSize to 6000000 ldap policy:
Commit Changes ldap policy: Quit ntdsutil: Quit Disconnecting from
raptor1...C:\>
```

CN=Deleted Objects コンテナの許可の変更

A

Active Directory オブジェクトが削除されると、変更を複製している他のドメインコントローラが削除に気付くように、オブジェクトの一部が、指定した時間だけそのまま残されます。デフォルトでは、System アカウントと Administrators グループのメンバーだけが、このコンテナの内容を表示できます。この節では、CN=Deleted Objects コンテナの許可を変更する方法について説明します。

System 以外または Admin 以外のアカウントで Active Directory へのバインドおよびディレクトリ変更のポーリングを行うエンタープライズアプリケーションまたはエンタープライズサービスがある場合は、Deleted Objects コンテナの許可の変更を必要とすることがあります。

このプロセスには、Active Directory Application Mode (ADAM) パッケージの dscals.exe が必要です。このバージョンは、Windows Server 2003 Support Tools 内のそのファイルのアップグレードであり、現在は必要な機能をサポートしています。ADAM 管理ツールは、Windows XP Professional、Windows Server 2003 Standard Edition、Windows Server 2003 Enterprise Edition、および Windows Server 2003 Datacenter Edition でサポートされています。

ADAM 管理ツールを取得してインストールする

1. ADAM Web ページ (http://www.microsoft.com/downloads/details.aspx?FamilyId=9688F8B9-1034-4EF6-A3E5-2A2A57B5C8E4&displaylang=en) から、ADAM リテールパッケージをダウンロードします。
2. ダウンロードしたファイルをダブルクリックして、アーカイブを抽出するディレクトリを指定します。
3. adamsetup.exe をダブルクリックして Active Directory Application Mode セットアップウィザードを起動し、［次へ］をクリックします。
4. 使用許諾契約書の条項を確認して同意し、［次へ］をクリックします。
5. ADAM 管理ツールだけを選択して、［次へ］をクリックします。
6. 選択した内容を確認して、［次へ］をクリックします。
7. セットアップが完了したら、［終了］をクリックします。

ADAM 管理ツールのインストール後に、次のように CN=Deleted Objects コンテナの許可を変更します。

1. Domain Admins グループのメンバーであるユーザアカウントでログインします。
2. ［スタート］>［すべてのプログラム］>［ADAM］>［ADAM Tools Command Prompt (ADAM ツールコマンドプロンプト)］の順にクリックします。
3. コマンドプロンプトで、次のコマンドを入力します。

   ```
   dsacls "CN=Deleted Objects,DC=Contoso,DC=com" /takeownership
   ```

   自分自身のドメインを Deleted Objects コンテナの識別名に置き換えます。

   フォレストの各ドメインには、独自の Deleted Objects コンテナがあります。

次の出力が表示されます。

```
Owner: Contoso\Domain Admins Group: NT AUTHORITY\SYSTEM Access
list: {This object is protected from inheriting permissions from
the parent} Allow BUILTIN\Administrators  SPECIAL ACCESS LIST
CONTENTS READ PROPERTY Allow NT AUTHORITY\SYSTEM    SPECIAL ACCESS
DELETE READ PERMISSONS WRITE PERMISSIONS CHANGE OWNERSHIP CREATE
CHILD DELETE CHILD LIST CONTENTS WRITE SELF WRITE PROPERTY READ
PROPERTY The command completed successfully
```

4 CN=Deleted Objects コンテナ内のオブジェクトを表示するためにセキュリティプリンシパルの許可を付与するには、次のコマンドを入力します。

```
dsacls "CN=Deleted Objects,DC=Contoso,DC=com" /g
CONTOSO\JaneDoe:LCRP
```

この例では、ユーザ CONTOSO\JaneDoe が、コンテナの内容の表示とプロパティの読み込みの許可が付与されています。ユーザが Deleted Objects コンテナの内容を表示するには、これらの許可で十分です。ただし、こうした許可では、ユーザが該当するオブジェクトに変更を加えることはできません。これらの許可は、Administrators グループに付与されているデフォルトのアクセス許可と同等です。デフォルトでは、System アカウントだけが、Deleted Objects コンテナ内のオブジェクトを変更できます。

次の出力が表示されます。

```
      Owner: CONTOSO\Domain Admins Group: NT AUTHORITY\SYSTEM
Access list: {This object is protected from inheriting permissions
from the parent} Allow BUILTIN\Administrators  SPECIAL ACCESS LIST
CONTENTS READ PROPERTY Allow NT AUTHORITY\SYSTEM    SPECIAL ACCESS
DELETE READ PERMISSONS WRITE PERMISSIONS CHANGE OWNERSHIP CREATE
CHILD DELETE CHILD LIST CONTENTS WRITE SELF WRITE PROPERTY READ
PROPERTY Allow CONTOSO\JaneDoe        SPECIAL ACCESS LIST CONTENTS
READ PROPERTY The command completed successfully.
```

これで、ユーザ CONTOSO\JaneDoe は、CONTOSO ドメイン内の削除されたオブジェクトを表示できます。