Novell Identity Manager

3.0

www.novell.com

管理ガイド

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

米国 Novell, Inc. およびノベル株式会社は、ソフトウェアの使用に起因する結果に関して、いかなる責任も負いません。また、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否認し、排除します。米国 Novell, Inc. およびノベル株式会社は、ノベル製ソフトウェアの内容を変更する権利を常に留保します。米国 Novell, Inc. およびノベル株式会社は、このような変更を個人または事業体に通知する義務を負いません。

本契約の締結に基づいて提供されるすべての製品または技術情報には、米国の輸出管理規定およびその他の国の貿易関連法規が適用されます。お客様は、取引対象製品の輸出、再輸出または輸入に関し、国内外の輸出管理規定に従うこと、および必要な許可、または分類に従うものとします。お客様は、現在の米国の輸出除外リストに記載されている企業、および米国の輸出管理規定で指定された輸出禁止国またはテロリスト国に本製品を輸出または再輸出しないものとします。お客様は、取引対象製品を、禁止されている核兵器、ミサイル、または生物化学兵器を最終目的として使用しないものとします。本ソフトウェアの輸出については、www.novell.com/info/exports/ もあわせてご参照ください。弊社は、必要な輸出認可が取得されなかった場合、一切の責任または義務を負いません。

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

オンラインヘルプ: 本製品とその他の Novell 製品のオンラインヘルプ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/documentation をご覧ください。

Novell の商標

eDirectory は、米国 Novell, Inc. の商標です。
exteNd は、米国 Novell, Inc. の商標です。
exteNd Director は、米国 Novell, Inc. の商標です。
GroupWise 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。
NDS 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。
NMAS は、米国 Novell, Inc. の商標です。
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. の商標です。
SUSE 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。

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

DirXML® の後継製品である Novell® Identity Manager 3 は、アプリケーション、ディレクトリ、およびデータベース間で情報を共有するためのデータ共有および同期サービスです。このサービスは、分散された情報をリンクし、ユーザは識別情報の変更時に指定システムを自動的に更新するポリシーを設定できます。Identify Manager は、アカウントプロビジョニング、セキュリティ、ユーザセルフサービス、認証、認可、自動化されたワークフロー、および Web サービスの基盤になります。Identify Manager を使用すると、分散された識別情報を統合、管理、および制御できるため、適切なユーザに適切なリソースを安全に提供できます。

このガイドでは、Identity Manager の技術の概要と、管理および設定の機能について説明します。

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［User Comments］機能を使用するか、または http://www.novell.com/documentation/feedback.html にアクセスし、コメントを入力してください。

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、Identity Manager のマニュアルの Web サイト (http://www.novell.com/documentation) を参照してください。

その他のマニュアル

Identity Manager のインストールおよびアップグレードに関するマニュアルについては、『*Identity Manager 3.0 インストールガイド*』を参照してください。

Identity Manager のポリシーとフィルタに関するマニュアルについては、『*Policy Builder and Driver Customization Guide*』を参照してください。

設計と展開の実践に関するマニュアルについては、『*Designer for Identity Manager 3: Administration Guide* (http://www.novell.com/documentation/designer)』を参照してください。

パスワードポリシー、パスワードセルフサービス、およびパスワードの管理に関するマニュアルについては、『Password Management Administration Guide (http://www.novell.com/documentation)』を参照してください。

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 Driver のマニュアルの Web サイト (http://www.novell.com/documentation/idmdrivers/index.html) を参照してください。

マニュアル表記規則

本マニュアルでは、手順に含まれる複数の操作および相互参照パス内の項目を分けるために、左向きの不等号 (>) 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。

Identity Manager 3.0 アーキテクチャの概要

1

Identity Manager には、次の 3 つの主なコンポーネントがあります。

1.1 以前のバージョンからの用語の変更

DirXML® 1.1a または Identity Manager 2.0 を使用したことがない場合は、この節を読む必要はありません。

DirXML 1.1a では、「ルール」という用語は、文脈に応じて、一連のルール、セットに含まれる個々のルール、および個々のルールに含まれる条件やアクションを指すために使用されていました。このように同じ用語が違う意味で使われると、文脈が不明瞭な場合には混乱を招きます。

Identity Manager 2 では、記述されている高レベルな変換を説明する場合、「ルール」という用語の代わりに「ポリシー」という用語を使用します。各ポリシーに 1 つ以上のルールが含まれている、一連のポリシーを定義します。「ルール」という用語は、複数の条件とアクションからなる個々のセットのみを指すようになりました。

次の表は、DirXML 1.1a から Identity Manager 2.x への用語の変更を示しています。

表 *1-1* *DirXML 1.1a から Identity Manager 2.x への用語の変更*

意味する内容	DirXML 1.1a の用語	Identity Manager 2.x の用語
変換セット	ルール	ポリシーセット
セットに含まれる個々の変換	ルール	“ポリシー”
個々の変換に含まれる条件とアクション	ルール	ルール

次の表は、Identity Manager 2.x から Identity Manager 3.0 への用語の変更を示しています。

表 *1-2* *Identity Manager 2.x から Identity Manager 3.0 への用語の変更*

意味する内容	Identity Manager 2.x の用語	Identity Manager 3 の用語
製品	DirXML	Identity Manager
製品がインストールされているサーバ	DirXML サーバ	メタディレクトリサーバ

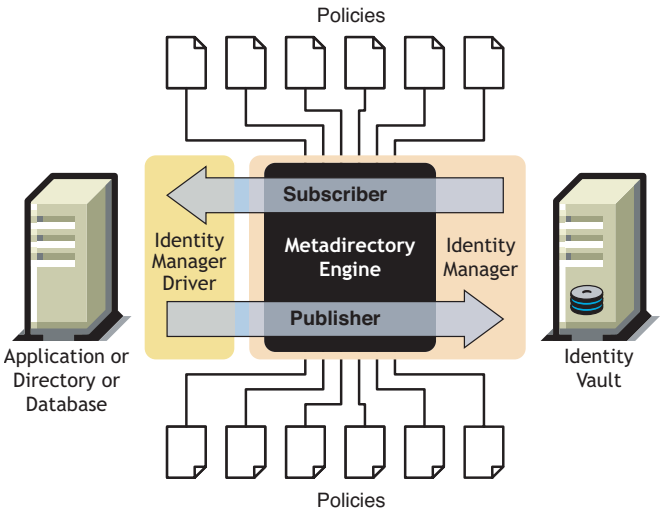
意味する内容	Identity Manager 2.x の用語	Identity Manager 3 の用語
データの同期先のアプリケーションまたはデータベースのサーバ	DirXML 接続システムサーバ	接続システムサーバ
オブジェクトが保存される場所	eDirectory™	アイデンティティボールト
処理コンポーネント	DirXML エンジン	メタディレクトリエンジン

1.2 Identity Manager

Identity Manager は、アイデンティティボールトと接続システム間におけるデータの同期機能を提供します。接続システムは、アプリケーション、ディレクトリ、データベース、またはファイルで構成されます。

Identity Manager には、いくつかのコンポーネントが含まれています。次の図は、基本コンポーネントとそれらの関係を示します。

図 *1-1* *Identity Manager* のコンポーネント



メタディレクトリエンジンは Identity Manager アーキテクチャの重要なモジュールです。このエンジンは、Identity Manager ドライバがアイデンティティボールト情報と同期する際のインタフェースとして機能し、異なるデータシステムでも接続してデータを共有できるようにします。

メタディレクトリエンジンは、XML 形式を使用してアイデンティティボールトデータおよびアイデンティティボールトイベントを処理します。ルールプロセッサとデータ変換エンジンを採用して、2 つのシステム間のデータフローを操作します。

1. すべての Identity Manager ドライバのフィルタを読み込みます。
2. 適切なアイデンティティボールトイベントのドライバを登録します。
3. 各ドライバの指定に従ってデータをフィルタ処理します。
4. 各ドライバに渡されるアイデンティティボールトイベントのキャッシュを設定します。

アイデンティティボールトは、初期化時に次の処理を実行します。

- イベントがキャッシュされると、そのキャッシュを所有するドライバがイベントを読み込みます。
- ドライバはアイデンティティボールトデータをeDirectoryのネイティブ形式で受信し、これを XDS 形式 (Identity Manager で使用される XML ボキャブラリで、ポリシーによって変換できます) に変換した後、イベントをメタディレクトリエンジンに送信します。このエンジンが接続システムドライバ内のすべてのポリシーを読み込み、ポリシーに従って XML 形式のデータを作成して、接続システムドライバにデータを送信します。続いて、接続システムにデータを送信します。ポリシーの詳細については、『*Policy Builder and Driver Customization Guide*』の「Introduction to Policies」を参照してください。
- ドライバの発行者部分は、接続システムの更新情報の収集と、それらの情報のアイデンティティボールトへの送信を担当します。2 つのシステム間で共有している情報の変更が接続システムドライバに通知されると、接続システムドライバはそれらの情報を収集し、適切なデータセットにフィルタされているかどうかを確認した後 XDS 形式に変換してエンジンに送信します。

1.2.1 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、eDirectory インタフェースと同期エンジンの 2 つのコンポーネントに分けることができます。

eDirectory インタフェース

メタディレクトリエンジンに組み込まれた eDirectory インタフェースは、eDirectory で発生するイベントを検出するために使用されます。このインタフェースは、イベントキャッシュを使用することで、Identity Manager に確実にイベントを送信できるようにしています。eDirectory インタフェースは複数のドライバをロードできます。つまり、その eDirectory サーバ用に実行されている Identity Manager のインスタンスは 1 つだけですが、複数の接続システムと通信できます。アイデンティティボールトと接続システムの間でイベントループが発生しないように、このインタフェースにはループバック検出機能が組み込まれています。このインタフェースにはループバック保護機能が含まれていますが、個々の接続システムドライバにループバック検出機能を組み込むことをお勧めします。

同期エンジン

同期エンジンは、Identity Manager ポリシーを各イベントに適用します。ポリシーは、DirXML スクリプトを使用してポリシービルダで作成します。ポリシービルダを使用すると、XML ドキュメントまたは XSLT で記述されたスタイルシートを使用する代わりに、GUI インタフェースを使ってポリシーを作成できます。スタイルシートも使用できますが、使いやすさではポリシービルダの方が優れています。ポリシービルダまたは DirXML スクリプトの詳細については、『*Policy Builder and Driver Customization Guide*』を参照してください。

同期エンジンは各タイプのポリシーをソースドキュメントに適用します。これらの変換を完了する機能は、Identity Manager の最も強力な機能の 1 つです。アイデンティティボールトと接続システムとの間で共有されるときに、データはリアルタイムで変換されます。

1.2.2 ドライバ環境設定ファイル

ドライバ環境設定は、Identity Manager に含まれる事前設定済みの XML ファイルです。これらの環境設定ファイルを、iManager および Designer のウィザードを使用してインポートできます。

ドライバ環境設定にはサンプルポリシーが含まれます。運用環境での使用を目的としたものではなく、ユーザが変更して使用できるテンプレートとして提供されています。

1.2.3 Identity Manager のイベントキャッシュ

eDirectory から生成されるすべてのイベントは、正常に処理されるまでイベントキャッシュに格納されています。これによって、接続不良、システムリソースの損失、ドライバの入手不能、またはその他のネットワーク障害によってデータが失われることを防ぎます。

1.2.4 ドライバシム

ドライバシムは、接続システムとアイデンティティボールトとの間における情報の管路として機能します。シムは Java、C、または C++ のいずれかで記述されます。

メタディレクトリエンジンとドライバシムの間の通信は、イベント、クエリ、および結果を記述した XML ドキュメントの形式で行われます。ドライバシムは一般的にはドライバと呼ばれます。これは、アイデンティティボールトと接続システムとの間で情報が転送される管路です。

シムでサポートされているオブジェクトイベントは次のとおりです。

- 追加 (作成)
- 変更
- 削除
- 名前変更
- 移動
- クエリ

また、Identity Manager が接続システムを照会できるように、シムは定義済みクエリの機能をサポートしている必要があります。

接続システムでアクションを引き起こすイベントがアイデンティティボールトで発生すると、Identity Manager は、そのアイデンティティボールトイベントを記述する XML ドキュメントを作成し、購読者チャネルを介してドライバシムに送信します。

接続システムでイベントが発生すると、接続システムイベントを記述する XML ドキュメントがドライバシムによって生成されます。続いて、ドライバシムが発行者チャネルを使用してその XML ドキュメントを Identity Manager に送信します。Identity Manager は、発行者ポリシーを使用してイベントを処理した後、適切なアクションを実行するようアイデンティティボールトに指示します。

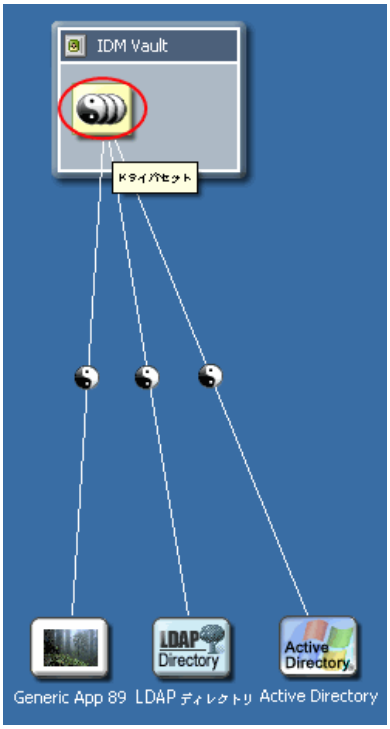
1.2.5 ドライバセット

ドライバセットは、複数の Identity Manager ドライバを格納するコンテナオブジェクトです。一度に 1 つのドライバセットを 1 つのサーバに関連付けることができます。このため、実行中のドライバはすべて同じドライバセットにグループ化する必要があります。

ドライバセットオブジェクトは、そのオブジェクトを使用しているサーバ上にある、完全な読み書き可能レプリカに存在しなければならないため、ドライバセットをパーティションに分割することをお勧めします。ユーザのレプリカが別のサーバに移動された場合に、ドライバオブジェクトも移動されないようにするためです。

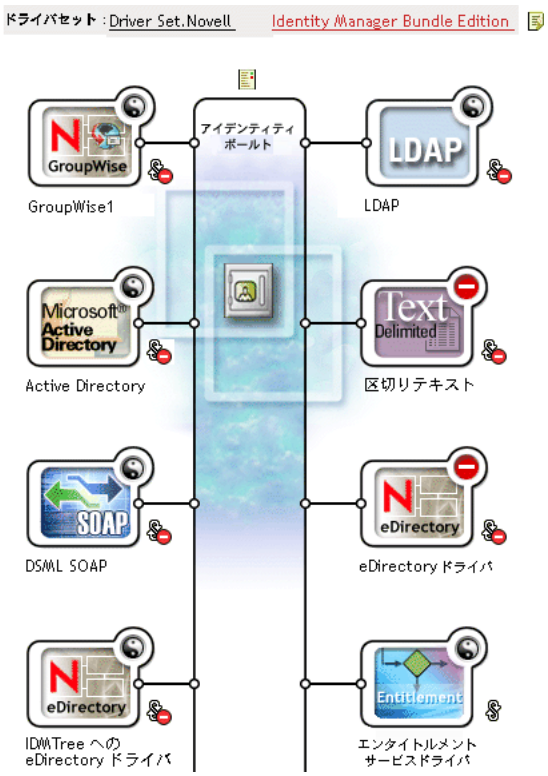
次の図は、Designer でドライバセットがどのように表示されるのかを示します。

図 *1-2* *Designer* でのドライバセット



次の図は、iManager でドライバセットがどのように表示されるのかを示します。

図 *1-3* *iManager* でのドライバセット



Designer の Modeler13 ページの 図 1-2 または iManager の概要ページ 14 ページの 図 1-3 から、次の処理を実行できます。

- ドライバセットとそのプロパティを表示および変更する
- ドライバセット内のドライバを表示する
- ドライバのステータスを変更する
- ドライバセットをサーバに関連付ける
- ドライバを追加または削除する
- ドライバセットの起動情報を表示する
- ドライバセットのステータスログを表示する

1.2.6 ドライバオブジェクト

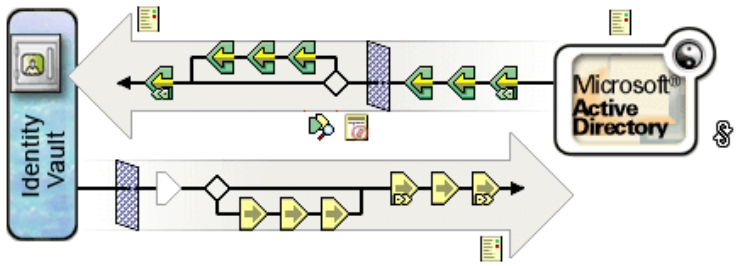
ドライバオブジェクトは、アイデンティティボールトと統合されている接続システムに接続されているドライバを表します。ドライバオブジェクトとその環境設定パラメータは、次のコンポーネントで構成されています。

- ドライバセットオブジェクトに含まれる eDirectory ツリーのドライバオブジェクト。
- ドライバオブジェクトに含まれる購読者チャネルオブジェクト。
- ドライバオブジェクトに含まれる発行者オブジェクト。

- ドライバオブジェクト、購読者オブジェクト、および発行者オブジェクトによって参照される複数のポリシーオブジェクト。
- ドライバオブジェクトによって参照される実行可能ドライバシム。
- 管理者によって設定されるシム固有のパラメータ。
- ドライバオブジェクトの eDirectory パスワード。このパスワードをシムで使用して、シムのリモート部分を認証できます。
- 接続システムに接続し、認証するために使用する認証パラメータ。
- エンタイトルメント。すべてのドライバに不可欠なものではありません。エンタイトルメントは、ドライバの作成時に有効にしたり、または後で追加したりできます。
- 次を含む、ドライバの起動オプション。
  - 使用不可 - ドライバは実行されません。
  - 手動 - ドライバは、iManager を使用して手動で起動する必要があります。
  - 自動スタート - アイデンティティボールトが起動すると、ドライバが自動的に起動します。
- スキーママッピングポリシーの参照。
- 接続システムのスキーマを XML で表したもの。通常、シムを使用して接続システムから自動的に取得されます。

iManager では、［Identity Manager ドライバの概要］にアクセスして、既存のドライバのパラメータ、ポリシー、スタイルシート、およびエンタイトルメントを変更できます。Identity Manager ドライバの概要を次に示します。

図 *1-4* *Identity Manager* ドライバの概要



ドライバオブジェクトは、eDirectory の権利の確認にも使用されます。ドライバオブジェクトには、読み込みまたは書き込みを行うオブジェクトに対して、必要な eDirectory 権利を付与する必要があります。そのためには、ドライバオブジェクトを、ドライバの同期先 eDirectory オブジェクトのトラスティにするか、ドライバオブジェクトに同等セキュリティを付与します。

権利の割り当ての詳細については、『*Novell eDirectory 8.8* 管理ガイド』の「eDirectory での権利 (http://www.novell.com/documentation/edir88/index.html?page=/documentation/edir88/edir88/data/fbachifb.html)」を参照してください。

1.2.7 発行者チャネルと購読者チャネル

Identity Manager ドライバには、データを処理するために、発行者チャネルおよび購読者チャネルという 2 つのチャネルがあります。発行者チャネルは、接続システムからアイデンティティボールトにイベントを送信します。購読者チャネルは、アイデンティティボールトから接続システムにイベントを送信します。各チャネルには、データの処理と変換の方法を定義する独自のポリシーが含まれています。

図 *1-5* *Designer* の発行者チャネルおよび購読者チャネル

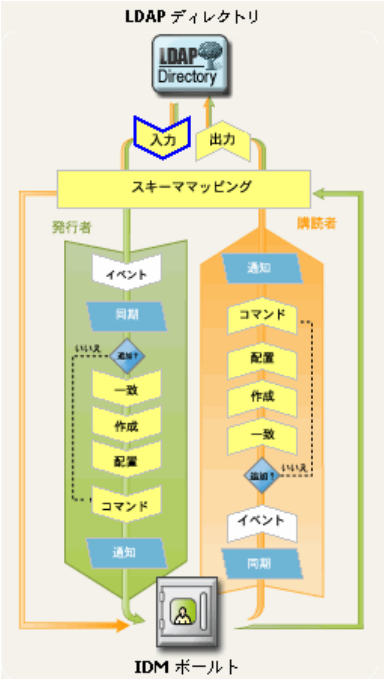
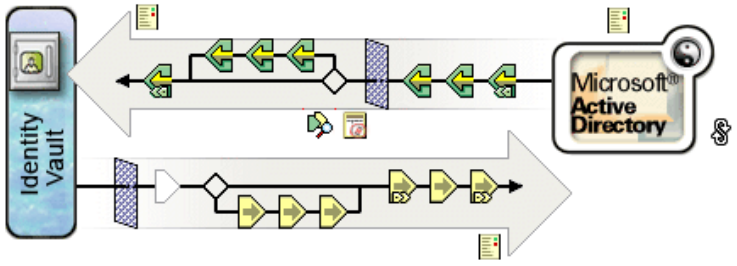


図 *1-6* *iManager* の発行者チャネルおよび購読者チャネル

ドライバ： Active Directory.DriverSet.South.Novell



1.2.8 イベントとコマンド

Identity Manager のイベントとコマンドの違いは重要です。イベントがドライバに送信される場合、そのイベントはコマンドです。イベントが Identity Manager に送信される場合、そのイベントは通知です。ドライバは、Identity Manager にイベント通知を送信する際に、接続システムで発生した変更を Identity Manager に通知します。メタディレクトリエンジ

ンは、設定可能なルールに基づいて、アイデンティティボールトに送信する必要があるコマンドを決定します (該当する場合)。

Identity Manager は、ドライバにコマンドを送信する時点において、すでにアイデンティティボールトイベントを入力として受け付けて適切なポリシーを適用し、コマンドが表す接続システム内の変更が必要であると判断しています。

1.2.9 ポリシーとフィルタ

ポリシーとフィルタによって、システム間のデータフローを制御できます。接続システムで使用するために、管理側のアイデンティティボールトのクラス、属性、およびイベントをどのように変換するのかを定義したポリシー内のルールを使用しています。ポリシーとフィルタの詳細については、『*Policy Builder and Driver Customization Guide*』を参照してください。

1.2.10 関連付け

大部分の識別情報管理製品では、接続システムからディレクトリにオブジェクトをマップするために、接続システムに何らかの識別子を格納する必要があります。Identity Manager では、接続システムを変更する必要はありません。アイデンティティボールトの各オブジェクトには、アイデンティティボールトブジェクトを接続システム内の一意の識別子にマップする関連付けテーブルが含まれています。このテーブルはリバースインデックス形式なので、接続システムは、アイデンティティボールトの更新時にアイデンティティボールト識別子 (識別名など) をドライバに提供する必要がありません。

2 つのオブジェクト間の関連付けは、アイデンティティボールト内の別のオブジェクトとまだ関連付けられていないオブジェクトでイベントが発生したときに作成されます。関連付けを作成するためには、定義可能な条件の最低限のセットが各オブジェクトで一致している必要があります。たとえば、4 つの属性のうち 2 つ (フルネーム、電話番号、従業員 ID、電子メールアドレス) が 90% 以上一致する場合にオブジェクトを関連付けるポリシーを作成できます。

2 つのオブジェクトが同じかどうかを判断するための条件は、一致ポリシーで定義します。変更されたオブジェクトに対して一致するオブジェクトが見つからない場合は、新しいオブジェクトが作成されます。そのためには、最低限の作成条件すべてに一致していなければなりません。条件は、ポリシーを作成することで定義されます。最後に、新しいオブジェクトをネーミング階層の中のどの位置に作成するかが配置ポリシーによって定義されます。

関連付けは次の 2 つの方法で作成できます。

- オブジェクト間の一致によって作成
- 特定場所内の新しいオブジェクトの作成によって作成

形成されたオブジェクト間の関連付けは、その後、管理者がオブジェクトを削除するか、または関連付けを削除するまで有効です。

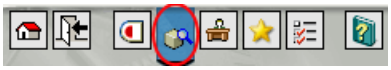
関連付けテーブル

Identity Manager では、関連付けとは eDirectory 内のオブジェクトを、接続システムに存在するオブジェクトと一致させることを指します。Identity Manager を初回にインストールしたときに、eDirectory スキーマが拡張されます。この拡張には、すべての eDirectory オブジェクトのベースクラスに結び付けられた新しい属性が含まれます。新しい属性が、関

連付けテーブルです。関連付けテーブルは、eDirectory オブジェクトをリンク先とするすべての接続システムオブジェクトを追跡します。このテーブルは自動的に作成および保守されるため、情報を手動で編集する必要はほとんどありません。ただし、表示して内容を確認したいことはよくあります。

オブジェクト上の関連付け属性は iManager で表示できます。

1 iManager で、ツールバーの［オブジェクトの表示］アイコンを選択します。



2 ブラウズしてオブジェクトを選択し、［オブジェクトの変更］を選択します。

3 ［Identity Manager］タブを選択します。

［Identity Manager］タブに関連付け属性が表示されます。

1.3 ユーザアプリケーション

ユーザアプリケーションはプロビジョニングソリューションです。これは Identity Manager 3 のアドオン製品です。ユーザアプリケーションにより、強力な承認ワークフローが Identity Manager に統合されます。組織は、人が介入する必要のない自動ルールに加えて、人の決定による手動入力に基づいてプロビジョニングを決定できます。詳細については、ユーザアプリケーションのドキュメント (http://www.novell.com/documentation/idm) を参照してください。

1.4 Designer

Designer は、スタンドアロンのクライアントアプリケーションです。Modeler スペース、Palette、ビュー、ポリシービルダ、ドキュメントジェネレータなどの機能で構成されており、生産性の高い環境で Identity Manager ベースのソリューションを設計、テスト、ドキュメント化、および展開できます。Designer の詳細については、『*Designer for Identity Manager 3:Administration Guide (http://www.novell.com/documentation/designer)*』を参照してください。

Identity Manager ドライバの管理

2

この節では、Identity Manager ドライバの作成と管理に役立つ情報について説明します。主なトピックは次のとおりです。

2.1 ドライバの作成と設定

使用する各 Identity Manager ドライバに対して、ドライバオブジェクトを作成し、ドライバ環境設定をインポートする必要があります。ドライバオブジェクトには、環境設定パラメータとそのドライバのポリシーが含まれます。ドライバオブジェクトの作成時に、ドライバ固有の環境設定ファイルをインポートします。ドライバ環境設定には、デフォルトのポリシーセットが含まれています。これらのポリシーは、データ共有モデルを簡単に実装できるようにすることを目的としています。ほとんどの場合は、出荷時のデフォルト設定を使用してドライバを設定してから、環境の要件に応じてドライバの設定を変更します。

ドライバオブジェクトを作成するには、次の 2 つの方法があります。

- ［ドライバの作成］タスク - 1 つのドライバを作成して、ドライバ環境設定をインポートできます。詳細については、19 ページの 「ドライバオブジェクトの作成」を参照してください。
- ［ドライバのインポート］タスク - 複数のドライバを同時に作成して、それらの環境設定をインポートできます。詳細については、20 ページのセクション 2.1.2「複数のドライバの作成」を参照してください。

2.1.1 ドライバオブジェクトの作成

ドライバ環境設定 (XML) ファイルを使用して、ドライバが適切に動作するために必要なオブジェクトを作成および設定します。また、ドライバ環境設定ファイルには、実装に合わせて変更できるポリシーの例も含まれています。

1 iManager で、［Identity Manager ユーティリティ］>［新規ドライバ］の順に選択します。

2 ドライバを作成する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 ［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)］にチェックマークを付け、.xml ファイルを選択し、［次へ］をクリックします。

ドライバ環境設定ファイルは、iManager の設定時に Web サーバにインストールされます。

4 表示される指示に従ってドライバ環境設定のインポートを完了します。

必要な Identity Manager オブジェクトが作成されます。インポート中に同等セキュリティの定義や管理ユーザの除外を実行しなかった場合、これらの作業は、ドライバオブジェクトのプロパティを変更することによって完了できます。

注 **:** インポート処理中にエンタイトルメントを有効にしないと、エンタイトルメントポリシーは作成されません。後でエンタイトルメントを使用するには、エンタイトルメントを有効にした新しいドライバを作成する必要があります。

2.1.2 複数のドライバの作成

Identity Manager は、複数のドライバを一度に作成する機能を備えています。このプロセスは、ドライバが適切に動作するためには必要なオブジェクトをドライバ環境設定 (XML) ファイルで作成および設定するという点で、単一のドライバを作成するプロセスとほぼ同じです。

複数のドライバを同時にインポートする

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 新しいドライバを作成するドライバセットを選択し、［次へ］をクリックします。

これら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 ドライバセットに追加するアプリケーション環境設定を選択し、［次へ］をクリックします。

4 表示される指示に従って要求されたデータを指定し、［次へ］をクリックします。

同時にインポートする環境設定を複数選択した場合、アプリケーションの環境設定ページが 1 つずつ表示されます。

ドライバごとに必要な Identity Manager オブジェクトが作成されます。インポート中に同等セキュリティの定義や管理ユーザの除外を実行しなかった場合、これらの作業は、ドライバオブジェクトのプロパティを変更することによって完了できます。

2.2 Identity Manager 環境での DirXML 1.1a ドライバの管理

DirXML 1.1a 用に作成された既存のドライバは、Identity Manager でも引き続き動作します。

Identity Manager 3.0 に付属のメタディレクトリエンジンは、古いドライバとの後方互換性を備えています (古いドライバシムと環境設定が最新の製品アップデートとパッチで更新されている必要があります)。そのため、必要に応じて、変更を加えずに Identity Manager サーバ上で DirXML 1.1a ドライバを実行できます。

ただし、iManager プラグインの後方互換性には制限があります。旧ドライバは［ドライバセットの概要］に表示できますが、ドライバを変換しなければドライバ環境設定を表示または編集できません。［ドライバセットの概要］で DirXML 1.1a ドライバをクリックすると、ドライバが DirXML 1.1a 形式であることが Identity Manager プラグインによって検出され、ウィザードを使用してドライバを 3.0 形式に変換するよう要求されます。

既存のドライバセットを変更しない場合は、ウィザードをキャンセルできます。

1.1a 形式の 1.1a ドライバを編集するには、DirXML 1.1a プラグインを使用する必要があります。これを実行するには、1.1a プラグインがインストールされた別の iManager Web サーバを使用する必要があります。Identity Manager に付属の Identity Manager プラグインを使用する場合、ドライバを Identity Manager 3.0 形式に変換せずにドライバ環境設定を編集することはできません。

2.3 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

DirXML 1.1a からアップグレードするには、Identity Manager 3 をインストールする必要があります。Identity Manager 3 のインストールによって新しいドライバシムがインストールされますが、既存のドライバオブジェクトまたはドライバ環境設定は変更されません。

DirXML 1.1a 用に作成された既存のドライバ環境設定は、Identity Manager で引き続き動作します。ただし、Identity Manager プラグインで編集できるのは、Identity Manager 形式のドライバのみです。

重要 **:** 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。

DirXML 1.1a ドライバを Identity Manager 形式に変換する場合に役立つウィザードが用意されています。

ウィザードを起動する

1. iManager で、［Identity Manager］>［Identity Manager の概要］の順にクリックします。
2. 変換するドライバを含むドライバセットを選択し、［検索］をクリックします。
3. 変換するドライバのアイコンをクリックします。
   ドライバを新しい形式に変換するように要求するメッセージが表示されます。
4. ウィザードの手順に従って変換を完了します。

2.4 ドライバの起動、停止、または再起動

1. iManager で、［Identity Manager］>［Identity Manager の概要］の順にクリックします。
2. ドライバ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。

3 ステータスを変更するドライバアイコンの右上隅をクリックし、ドライバが停止している場合は［ドライバの起動］をクリックし、ドライバが実行中の場合は［ドライバの停止］をクリックします。

2.5 ドライバパラメータ

各ドライバのプロパティには、ドライバパラメータがあります。パラメータには、ドライバ固有の情報が保存されます。SSL の使用有無、ドライバのハートビート設定、ポーリング間隔、認証方法などの情報がパラメータに保存されます。

2.6 グローバル構成値の使用

グローバル構成値 (GCV) は、ドライバパラメータに似た設定です。グローバル構成値は、ドライバセットに対しても、個々のドライバに対しても指定できます。ドライバに GCV 値がない場合、ドライバはドライバセットからその GCV の値を継承します。

GCV によって、パスワード同期やドライバハートビートなどの Identity Manager 機能の設定、および個々のドライバ環境設定の機能に固有の設定を指定できます。一部の GCV はドライバに付属していますが、ユーザが独自の GCV を追加することもできます。ポリシーでこれらの値を参照すると、ドライバ環境設定を容易にカスタマイズできます。

重要 **:** パスワード同期の設定は GCV ですが、これらを編集する場合は、［GCV (GCV)］ページではなく、ドライバの［サーバ変数］ページで利用できるグラフィカルインタフェースを使用することをお勧めします。パスワード同期の設定が表示される［サーバ変数］ページには、その他のドライバパラメータと同様のタブとしてアクセスできます。または、［パスワードの管理］>［パスワード同期］の順にクリックしてドライバを検索し、ドライバ名をクリックすることでアクセスできます。このページには、パスワード同期の各設定のオンラインヘルプがあります。

Identity Manager のパスワード同期に関連しない GCV を追加、削除、または編集する

1 iManager で、［Identity Manager］>［Identity Manager の概要］の順にクリックします。
2 ドライバセットまたはドライバオブジェクトを参照してクリックし、［検索］をクリックします。
3 ドライバの右上隅をクリックし、［プロパティの編集］をクリックします。
4 ［グローバル構成値］を選択します。
5 ドライバ作成時に設定されたデフォルト値を変更します。
6 他の情報を追加するには、［XML の編集］をクリックします。
7 ［XML 編集の有効化］をクリックします。
8 XML を追加、削除、または編集し、［OK］をクリックして変更を適用します。

2.7 DirXML コマンドラインユーティリティの使用

DirXML コマンドラインユーティリティにより、Identity Manager の特定の eDirectory の verb にアクセスできます。このユーティリティは、iManager または Designer の代わりにはなりません。このユーティリティの主な使用目的はスクリプトの作成です。DirXML コマンドラインユーティリティの詳細については、249 ページの付録 A「DirXML コマンド

ラインユーティリティ」を参照してください。日常のタスクには、iManager または Designer を使用します。

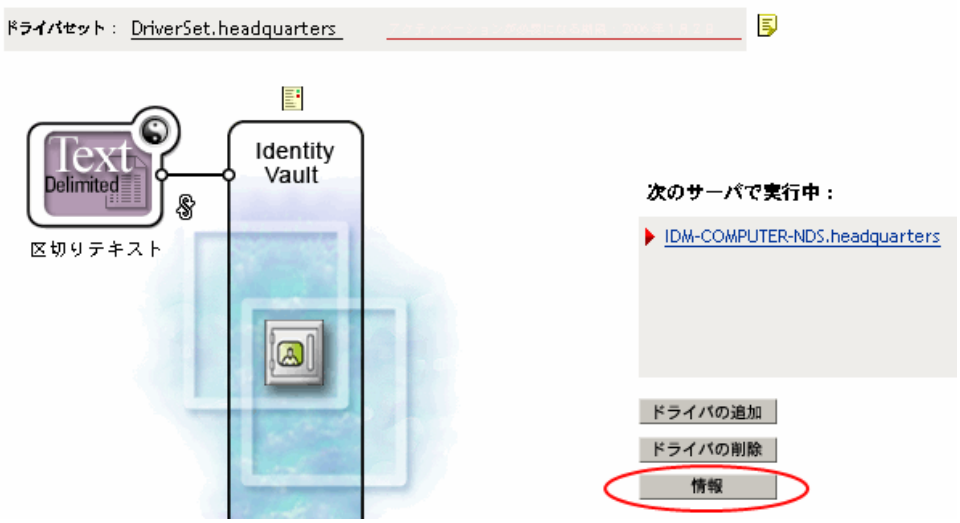
2.8 バージョン情報の表示

バージョン検出ツールで実行できる作業は、次のとおりです。

- 23 ページのセクション 2.8.1「階層構造でのバージョン情報の表示」
- 25 ページのセクション 2.8.2「テキストファイルでのバージョン情報の表示」
- 26 ページのセクション 2.8.3「バージョン情報の保存」

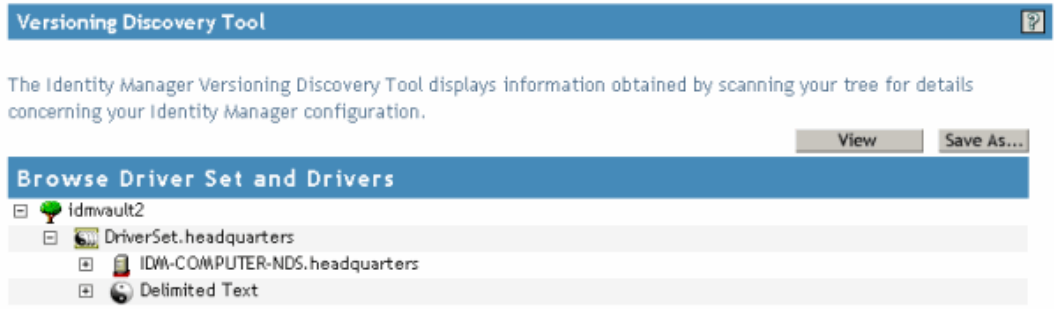
2.8.1 階層構造でのバージョン情報の表示

1. iManager で、[Identity Manager] > [Identity Manager の概要] の順にクリックし、[検索] をクリックしてドライバセットを検索します。
2. [Identity Manager の概要] 画面で [情報] をクリックします。



また、[Identity Manager ユーティリティ] > [バージョン検出] の順に選択し、ドライバセットを参照して選択して [OK] をクリックすることもできます。

3. トップレベルまたは展開していない階層ビューにバージョン情報を表示します。

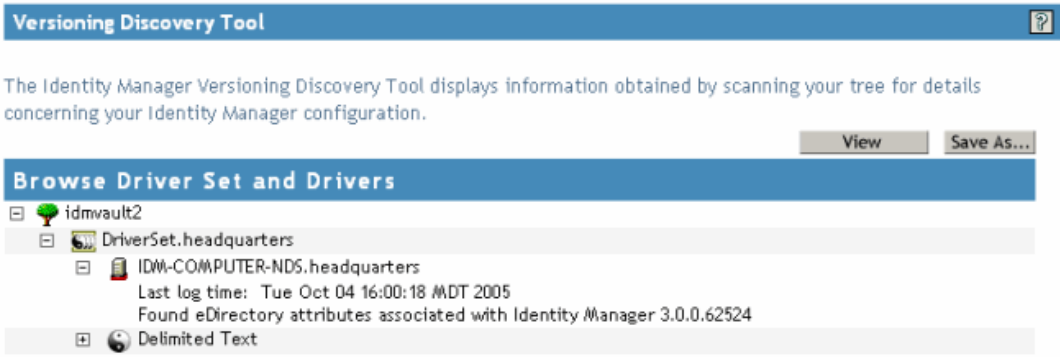


展開していない階層ビューには、次が表示されます。

- 認証されている eDirectory ツリー
- 選択したドライバセット
- ドライバセットに関連付けられているサーバ

  ドライバセットが 2 つ以上のサーバに関連付けられている場合、各サーバの Identity Manager 情報を表示できます。
- ドライバ

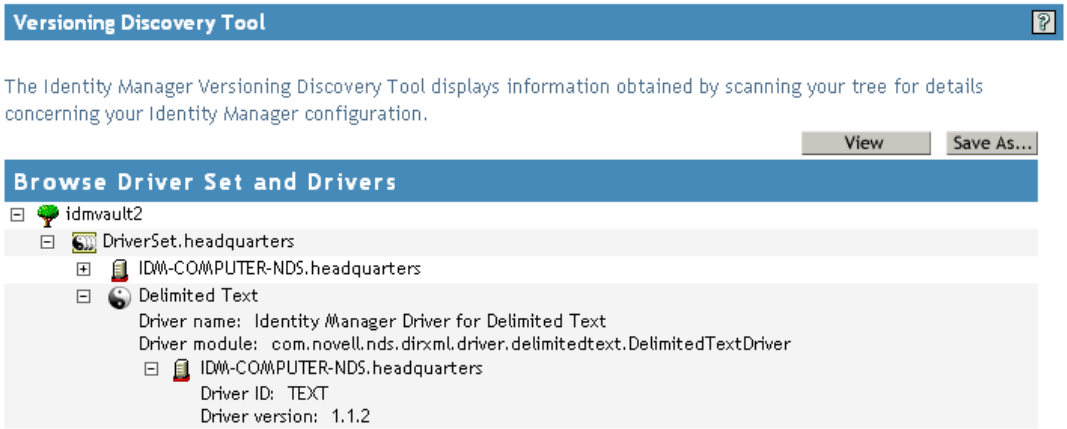
4 サーバアイコンを展開して、サーバに関連するバージョン情報を表示します。



トップレベルのサーバアイコンの展開ビューでは、次が表示されます。

- 前回のログ時間
- サーバ上で実行中の Identity Manager のバージョン

5 ドライバアイコンを展開して、ドライバに関連するバージョン情報を表示します。



トップレベルのドライバアイコンの展開ビューには、次が表示されます。

- ドライバ名
- ドライバモジュール (com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver など)

ドライバアイコンの下位にあるサーバの展開ビューには、次が表示されます。

- ドライバ ID

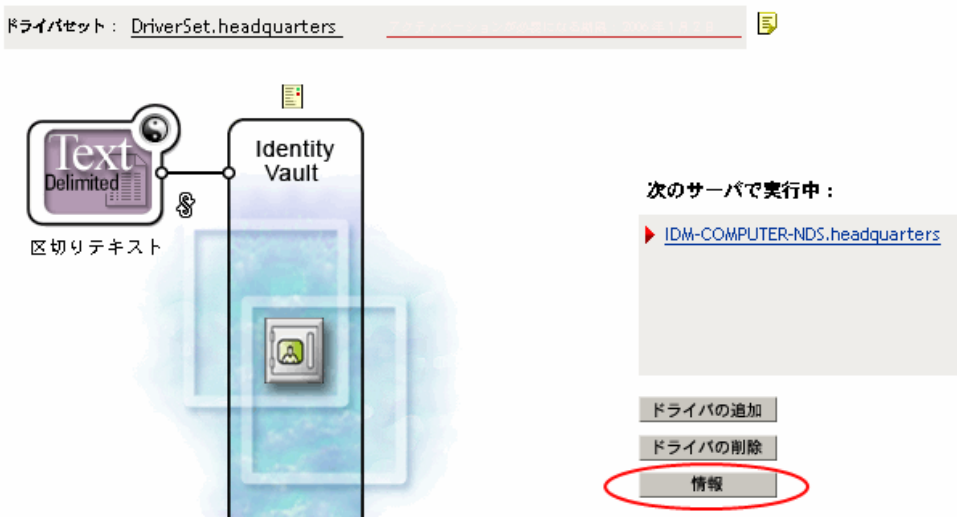
- サーバ上で実行されているドライバのインスタンスのバージョン

2.8.2 テキストファイルでのバージョン情報の表示

Identity Manager を使用して、バージョン情報をファイルに発行できます。テキスト形式で保存されたこの情報を表示できます。テキスト形式で表示される情報は、階層ビューの情報と同じです。

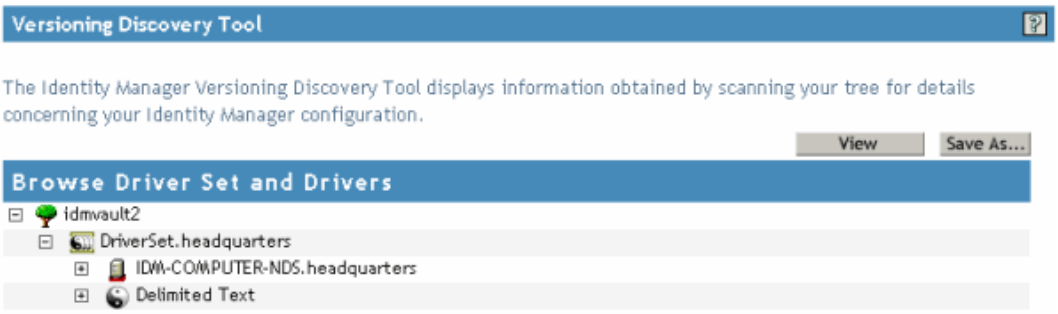
1 iManager で、［Identity Manager］>［Identity Manager の概要］の順にクリックし、［検索］をクリックしてドライバセットを検索します。

2 ［Identity Manager の概要］画面で［情報］をクリックします。

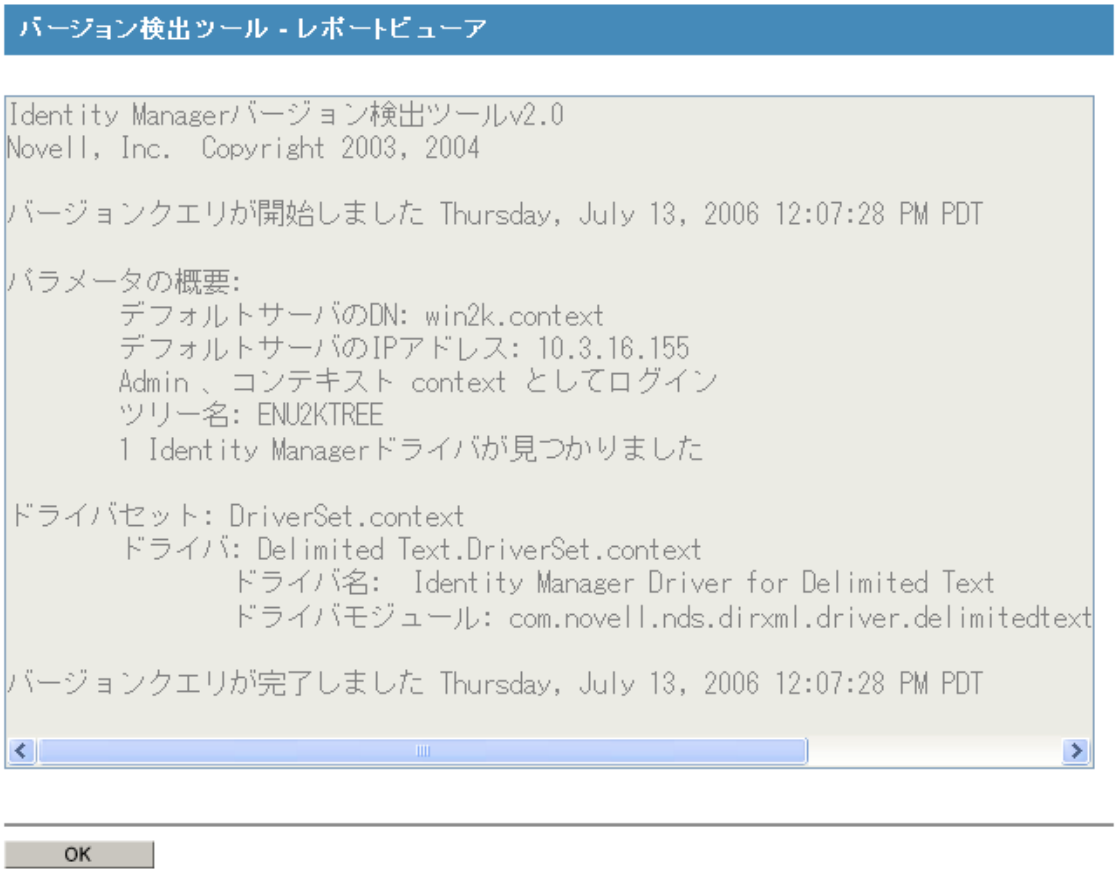


また、［Identity Manager ユーティリティ］>［バージョン検出］の順に選択し、ドライバセットを参照して選択して［情報］をクリックすることもできます。

3 ［バージョン検出ツール］ダイアログボックスで、［表示］をクリックします。



情報が［レポートビューア］ウィンドウにテキストファイルとして表示されます。

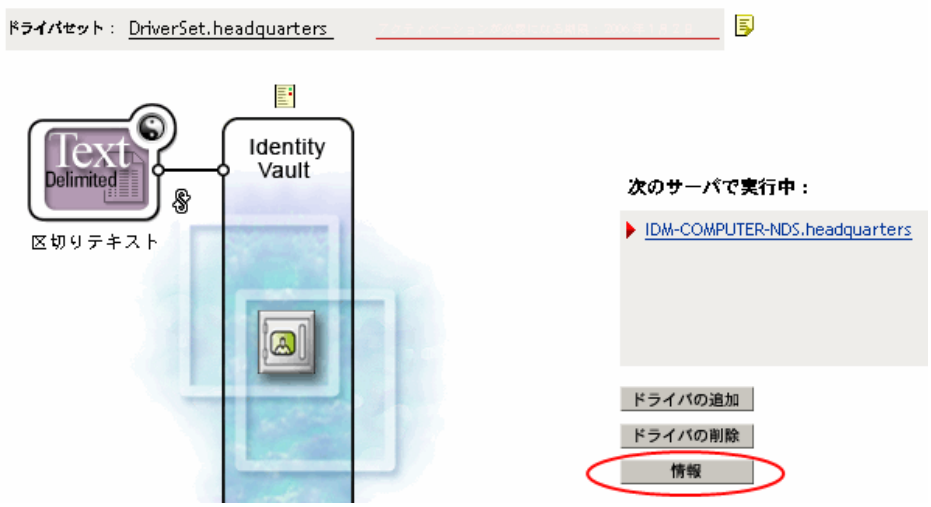


2.8.3 バージョン情報の保存

バージョン情報は、ローカルドライブまたはネットワークドライブにテキストファイルとして保存できます。

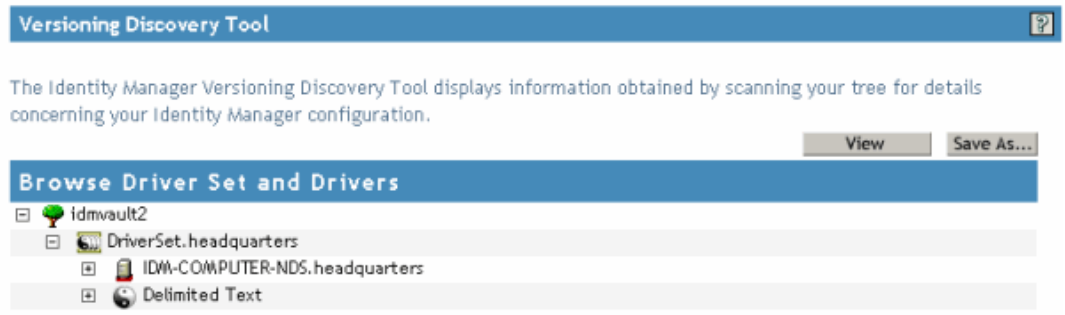
1 iManager で、［Identity Manager］>［Identity Manager の概要］の順にクリックし、［検索］をクリックしてドライバセットを検索します。

2 ［Identity Manager の概要］画面で［情報］をクリックします。



また、［Identity Manager ユーティリティ］>［バージョン検出］の順に選択し、ドライバセットを参照して選択して［情報］をクリックすることもできます。

3 ［バージョン検出ツール］ダイアログボックスで、［名前を付けて保存］をクリックします。



4 ［File Download (ファイルのダウンロード)］ダイアログボックスで、［保存］をクリックします。

5 目的のディレクトリに移動し、ファイル名を入力して［保存］をクリックします。

Identity Manager によってデータがテキストファイルに保存されます。

2.9 名前付きパスワードの使用

Identity Manager では、特定のドライバで使用される複数のパスワードを安全に保存できます。この機能は、「名前付きパスワード」と呼ばれます。各パスワードには、キー、つまり名前でアクセスします。

また、名前付きパスワード機能を使用して、ユーザ名などの情報を安全に保存することもできます。

ドライバポリシーで名前付きパスワードを使用するには、実際のパスワードではなくパスワードの名前を使用してパスワードを参照します。その後、メタディレクトリエンジンか

らドライバにパスワードが送信されます。この節で説明する名前付きパスワードの保存と取得の方法は、ドライバシムを変更することなく、どのドライバでも使用できます。

注 **:** Lotus Notes 用 Identity Manager ドライバで提供されているサンプル設定には、この方法で名前付きパスワードを使用する例が含まれています。Notes ドライバシムは、名前付きパスワードを使用する他の方法をサポートするようにカスタマイズされており、それらの方法の例も含まれています。詳細については、『*Identity Manager Driver for Lotus Notes:Implementation Guide*』の「Named Passwords」のセクションを参照してください。

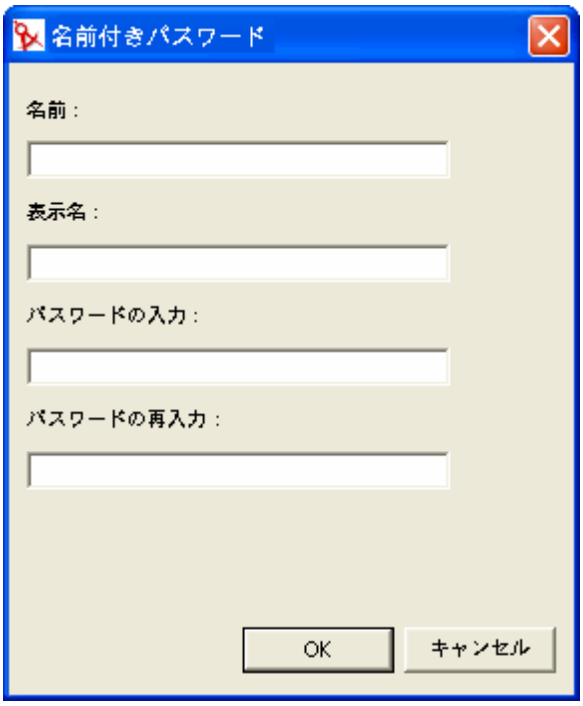
この節では、次の項目について説明します。

- 28 ページのセクション 2.9.1「Designer を使用した名前付きパスワードの設定」
- 29 ページのセクション 2.9.2「iManager を使用した名前付きパスワードの設定」
- 30 ページのセクション 2.9.3「ドライバポリシーでの名前付きパスワードの使用」
- 31 ページのセクション 2.9.4「DirXML コマンドラインユーティリティを使用した名前付きパスワードの設定」

2.9.1 Designer を使用した名前付きパスワードの設定

1 ドライバオブジェクトを選択し、右クリックして［プロパティ］を選択します。

2 ［名前付きパスワード］を選択し、［新規］をクリックします。



3 名前付きパスワードの名前を指定します。

4 名前付きパスワードの表示名を指定します。

5 名前付きパスワードを指定し、パスワードを再入力します。

6 ［OK］を 2 回クリックします。

2.9.2 iManager を使用した名前付きパスワードの設定

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

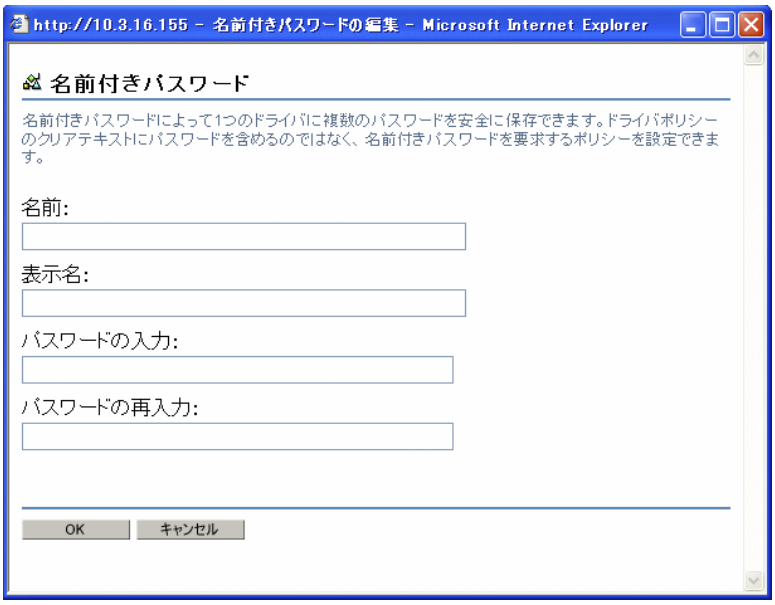
2 ドライバセットを検索するか、対象のドライバセットを含むコンテナを参照して選択します。ドライバセットがグラフィカルに表示されます。

3 ［Identity Manager の概要］画面で、ドライバアイコンの右上隅をクリックし、［プロパティの編集］をクリックします。

4 ［Identity Manager］タブの［オブジェクトの変更］ページで、［名前付きパスワード］をクリックします。

このドライバの現在の名前付きパスワードを一覧表示する［名前付きパスワード］ページが表示されます。名前付きパスワードを設定していない場合、このリストは空です。

5 名前付きパスワードを追加するには、［追加］をクリックしてフィールドに入力し、［OK］をクリックします。



6 名前、表示名、およびパスワードを指定し、［OK］を 2 回クリックします。

この機能を使用して、ユーザ名などの情報を安全に保存することもできます。

7 「ドライバを再起動して変更を有効にしますか？(OK= はい、キャンセル = いいえ)」というメッセージが表示されます。［OK］をクリックします。

8 名前付きパスワードを削除するには、［削除］をクリックします。パスワードが削除されます。削除の確認を求めるメッセージは表示されません。

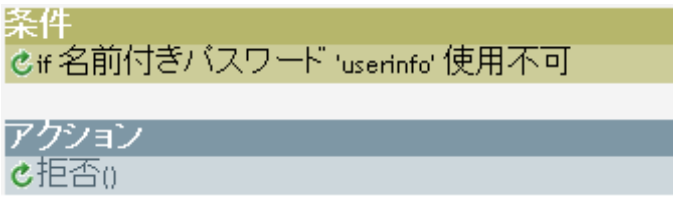
2.9.3 ドライバポリシーでの名前付きパスワードの使用

- 30 ページの 「ポリシービルダの使用」
- 31 ページの 「XSLT の使用」

ポリシービルダの使用

ポリシービルダを使用すると、名前付きパスワードを呼び出すことができます。新しいルールを作成し、条件として名前付きパスワードを選択します。名前付きパスワードが使用可能か、使用不可かに応じてアクションを設定します。次に、名前付きパスワードのユーザ情報が使用不可である場合に、イベントが拒否される例を示します。

図 *2-1* 名前付きパスワードを使用したポリシー



XSLT の使用

次のサンプルは、名前付きパスワードが、XSLT における購読者チャネルのドライバポリシーに参照される方法を示しています。

```
<xsl:value-of
select="query:getNamedPassword($srcQueryProcessor,'mynamedpassword')"
xmlns:query="http://www.novell.com/java/
com.novell.nds.dirxml.driver.XdsQueryProcessor/>
```

2.9.4 DirXML コマンドラインユーティリティを使用した名前付きパスワードの設定

- 31 ページの 「DirXML コマンドラインユーティリティでの名前付きパスワードの作成」
- 32 ページの 「DirXML コマンドラインユーティリティでの名前付きパスワードの削除」

DirXML コマンドラインユーティリティでの名前付きパスワードの作成

1 DirXML コマンドラインユーティリティを実行します。

詳細については、249 ページの付録 A「DirXML コマンドラインユーティリティ」を参照してください。

2 ユーザ名とパスワードを入力します。

次のオプションリストが表示されます。

```
DirXML commands


 1: Start driver 2:Stop driver 3:Driver operations...4: Driver set
operations...5: Log events operations...6: Get DirXML version
99:Quit


Enter choice:
```

3 「3」を入力して、ドライバの操作を選択します。

ドライバの番号付きリストが表示されます。

4 名前付きパスワードを追加するドライバの番号を入力します。

次のオプションリストが表示されます。

```
Select a driver operation for:driver_name


 1: Start driver 2:Stop driver 3:Get driver state 4:Get driver
start option 5:Set driver start option 6:Resync driver 7:Migrate
from application into DirXML 8:Submit XDS command document to
```

```
driver 9:Check object password 10:Initialize new driver object
11:Passwords operations 12:Cache operations 99:Exit


Enter choice:
```

5 「11」を入力して、パスワードの操作を選択します。

次のオプションリストが表示されます。

```
Select a password operation


 1: Set shim password 2:Reset shim password 3:Set named password
4:Clear named password(s) 5:List named passwords 99:Exit


Enter choice:
```

6 「3」を入力して、新しい名前付きパスワードを設定します。

次のプロンプトが表示されます。

```
Enter password name:
```

7 名前付きパスワードの参照に使用する名前を入力します。

8 次のプロンプトが表示されたら、セキュリティで保護する実際のパスワードを入力します。

```
Enter password:
```

パスワードに入力する文字は表示されません。

9 次のプロンプトが表示されたら、パスワードをもう一度入力して確認します。

```
Confirm password:
```

10 パスワードを入力して確認すると、パスワードの操作メニューに戻ります。

このステップが終わったら、オプション 99 を 2 回使用してメニューを終了し、DirXML コマンドラインユーティリティを終了します。

DirXML コマンドラインユーティリティでの名前付きパスワードの削除

このオプションは、以前に作成した名前付きパスワードが不要になった場合に便利です。

1 DirXML コマンドラインユーティリティを実行します。

詳細については、249 ページの付録 A「DirXML コマンドラインユーティリティ」を参照してください。

2 ユーザ名とパスワードを入力します。

次のオプションリストが表示されます。

```
DirXML commands


 1: Start driver 2:Stop driver 3:Driver operations...4: Driver set
operations...5: Log events operations...6: Get DirXML version
99:Quit


Enter choice:
```

3 「3」を入力して、ドライバの操作を選択します。
ドライバの番号付きリストが表示されます。

4 名前付きパスワードを削除するドライバの番号を入力します。
次のオプションリストが表示されます。

```
Select a driver operation for:driver_name


 1: Start driver 2:Stop driver 3:Get driver state 4:Get driver
start option 5:Set driver start option 6:Resync driver 7:Migrate
from application into DirXML 8:Submit XDS command document to
driver 9:Check object password 10:Initialize new driver object
11:Passwords operations 12:Cache operations 99:Exit


ëIëšéàÇšì¸óÕÇµÇƒÇ¦ÇæÇŠÇ¢:
```

5 「11」を入力して、パスワードの操作を選択します。
次のオプションリストが表示されます。

```
Select a password operation


 1: Set shim password 2:Reset shim password 3:Set named password
4:Clear named password(s) 5:List named passwords 99:Exit


Enter choice:
```

6 (オプション) 「5」を入力して、既存の名前付きパスワードのリストを参照します。
既存の名前付きパスワードのリストが表示されます。
このステップによって、削除するパスワードが正しいことを確認できます。

7 「4」を入力して、1 つまたは複数の名前付きパスワードを削除します。

8 次のプロンプトが表示されたら、「No」を入力して、1 つの名前付きパスワードを削除します。

```
Do you want to clear all named passwords?(yes/no):
```

9 次のプロンプトが表示されたら、削除する名前付きパスワードの名前を入力します。

```
Enter password name:
```

削除する名前付きパスワードの名前を入力すると、次のパスワード操作メニューに戻ります。

```
Select a password operation


 1: Set shim password 2:Reset shim password 3:Set named password
4:Clear named password(s) 5:List named passwords 99:Exit


Enter choice:
```

10 (オプション)「5」を入力して、既存の名前付きパスワードのリストを参照します。

既存の名前付きパスワードのリストが表示されます。

このステップによって、削除したパスワードが正しいことを確認できます。

このステップが終わったら、オプション 99 を 2 回使用してメニューを終了し、DirXML コマンドラインユーティリティを終了します。

2.10 ドライバオブジェクトとサーバの再関連付け

ドライバオブジェクトはサーバに関連付けられています。

何らかの理由で関連付けが無効になった場合、次のいずれかで示されます。

- Identity Manager サーバ上の eDirectory をアップグレードしたときに、「UniqueSPIException error -783.」というエラーメッセージが表示される。
- ［Identity Manager の概要］画面のドライバの横にサーバのリストが表示されない。
- ［Identity Manager の概要］画面のドライバの横にサーバのリストが表示されるが、名前が文字化けしている。

この問題を解決するには、ドライバオブジェクトとサーバの関連付けを解除したうえで、再度関連付ける必要があります。

iManager にログインし、［Identity Manager の概要］画面のドライバオブジェクトに移動します。アイコンを使用して削除し、ドライバアイコンの横にあるサーバ名リストにサーバを追加します。削除してから追加することで、サーバがドライバオブジェクトに再度関連付けられます。

2.11 ドライバハートビートの追加

ドライバハートビートは、Identity Manager 2 以降に付属の Identity Manager ドライバの機能です。この使用は必須ではありません。ドライバハートビートは、ドライバパラメータ

と指定した間隔を使用して設定します。ハートビートパラメータが存在し、間隔値が 0 以外の場合、指定された間隔内に発行者チャネル上で通信が行われていなければ、ドライバはハートビートドキュメントをメタディレクトリエンジンに送信します。

ドライバハートビートの目的は、ドライバによる発行者チャネルでの通信が、望ましい頻度で発生していない場合に、一定間隔でアクションを開始できるトリガを提供することです。ハートビートを利用する場合は、ドライバ設定などのツールをカスタマイズする必要があります。メタディレクトリエンジンは、ハートビートドキュメントを受け付けますが、それによってアクションを実行することはありません。

ほとんどのドライバでは、ハートビートのドライバパラメータはサンプル設定では使用されていませんが、このパラメータを追加できます。

Identity Manager に付属しないカスタムドライバであっても、ドライバの開発者がハートビートドキュメントをサポートするようドライバを作成していれば、ハートビートドキュメントを提供できます。

ハートビートを設定するには、次の操作を行います。

1. iManager で、［Identity Manager］>［Identity Manager の概要］の順にクリックします。
2. ドライバセットを参照して選択し、［検索］をクリックします。
3. ［Identity Manager の概要］画面で、ドライバアイコンの右上隅をクリックし、［プロパティの編集］をクリックします。
4. ［Identity Manager］タブで、［ドライバ環境設定］をクリックし、［ドライバパラメータ］までスクロールして［Heart Beat (ハートビート)］または同様の表示名を探します。

   ハートビートのドライバパラメータがすでに存在する場合は、その間隔を変更して変更を保存すると、設定が完了します。

   間隔に 1 未満の値を設定できません。値 0 は、この機能がオフになっていることを意味します。

   通常、時間の単位は分ですが、ドライバの中には秒を使用するなど、分以外を実装しているものもあります。
5. ハートビートのドライバパラメータが存在しない場合は、［XML の編集］をクリックします。
6. 次の例のようなドライバパラメータのエントリを、<publisher-options> の子エントリとして追加します (AD ドライバでは、これを <driver-options> の子エントリにします)。

   ```
   <pub-heartbeat-interval display-name="Heart Beat">10</pub-
   heartbeat-interval>
   ```

   ヒント **:** ドライバを再起動してもハートビートドキュメントが生成されない場合は、XML 内のドライバパラメータの場所を確認してください。

   ---
7. 変更を保存し、ドライバが停止および再起動されることを確認します。

ドライバパラメータを追加した後で、グラフィカルビューを使用して間隔を編集できます。もう 1 つの方法は、間隔のグローバル構成値 (GCV) への参照を作成する方法です。他のグローバル構成値と同様に、ドライバハートビートは、各ドライバオブジェクトのレベルではなくドライバセットレベルで設定できます。ドライバに特定のグローバル構成値

がなく、ドライバセットにグローバル構成値がある場合、ドライバはドライバセットの値を継承します。

次に、Notes ドライバによって送信されたハートビートのステータスドキュメントの例を示します。

```
<nds dtdversion="2.0" ndsversion="8.x"> <source> <product
build="20031112_1037" instance="blackcap" version="2.0">DirXML Driver
for Lotus Notes</product> <contact>Novell, Inc.</contact> </source>
<input> <status level="success" type="heartbeat"/> </input> </nds>
```

2.12 Identity Manager のプロセスの表示

Identity Manage のプロセスイベントを表示するには、DSTRACE を使用します。これは、Identity Manager をテストおよびトラブルシューティングする場合にのみ使用してください。ドライバの運用中に DSTRACE を実行すると、Identity Manager サーバ上の使用率が増加して、イベントの処理速度が非常に遅くなる場合があります。

DSTRACE で Identity Manager のプロセスを調べるには、ドライバセットおよびドライブのオブジェクトに値を追加します。これは、Designer および iManager で実行できます。

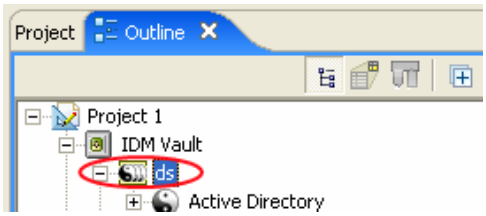
- 36 ページのセクション 2.12.1「Designer でのトレースレベルの追加」
- 38 ページのセクション 2.12.2「iManager でのトレースレベルの追加」
- 39 ページのセクション 2.12.3「ファイルへの Identity Manager のプロセスのキャプチャ」

2.12.1 Designer でのトレースレベルの追加

ドライバセットオブジェクトまたは各ドライバオブジェクトにトレースレベルを追加できます。

ドライバセット

1 Designer 内で開いているプロジェクトの［Outline (アウトライン)］ビューで、ドライバセットオブジェクトを選択します。



2 右クリックして［プロパティ］を選択し、［5. Trace (5. トレース)］をクリックします。

3 トレースパラメータを設定し、［OK］をクリックします。ドライバセットのトレースパラメータの詳細については、37 ページの 表 2-1 を参照してください。

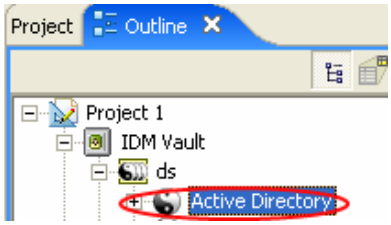
ドライバセットオブジェクトのトレースレベルを設定すると、すべてのドライバが DSTRACE ログに記述されます。

表 *2-1* ドライバセットのトレースパラメータ

パラメータ	説明
ドライバトレースレベル	ドライバオブジェクトのトレースレベルを上げると、DSTRACE に表示される情報量が増えます。 トレースレベル 1 はエラーを示しますが、エラーの原因は示しません。パスワード同期の情報を表示するには、トレースレベルを 5 に設定します。
XSL トレースレベル	DSTRACE では、XSL イベントが表示されます。このトレースレベルは、XSL スタイルシートのトラブルシューティング時にのみ設定します。XSL 情報を表示しない場合は、レベルをゼロに設定します。
Java デバッグポート	開発者は Java デバッガをアタッチできます。
Java トレースファイル	このフィールドの値が設定されている場合、ドライバセットオブジェクトのすべての Java 情報がファイルに書き込まれます。このフィールドの値は、そのファイルのパッチです。 ファイルを指定すると、Java 情報がこのファイルに書き込まれます。Java をデバッグする必要がない場合、このフィールドを空白のままにします。
トレースファイルのサイズ制限	Java トレースファイルの制限を設定できます。ファイルサイズを無制限に設定した場合、ディスクスペースがなくなるまでファイルサイズが増加します。

ドライバ

1 Designer 内で開いているプロジェクトの［Outline (アウトライン)］ビューで、ドライバオブジェクトを選択します。



2 右クリックして［プロパティ］を選択し、［8. Trace (8. トレース)］をクリックします。

3 トレースパラメータを設定し、［OK］をクリックします。これらのパラメータの詳細については、38 ページの 表 2-2 を参照してください。

ドライバオブジェクトのパラメータのみを設定した場合、そのドライバの情報のみが DSTRACE ログに記述されます。

表 *2-2* ドライバのトレースパラメータ

パラメータ	説明
トレースレベル	ドライバオブジェクトのトレースレベルを上げると、DSTRACE に表示される情報量が増えます。 トレースレベル 1 はエラーを示しますが、エラーの原因は示しません。パスワード同期の情報を表示するには、トレースレベルを 5 に設定します。 ［Use setting from Driver Set (ドライバセットの設定を使用する)］を選択した場合、値はドライバセットオブジェクトから取得されます。
トレースファイル	選択したドライバに対して、ファイル名および Identity Manager 情報を書き込む場所を指定します。 ［Use setting from Driver Set (ドライバセットの設定を使用する)］を選択した場合、値はドライバセットオブジェクトから取得されます。
トレースファイルのサイズ制限	Java トレースファイルの制限を設定できます。ファイルサイズを無制限に設定した場合、ディスクスペースがなくなるまでファイルサイズは増加します。 ［Use setting from Driver Set (ドライバセットの設定を使用する)］を選択した場合、値はドライバセットオブジェクトから取得されます。
トレース名	ドライバトレースメッセージの前に、ドライバ名の代わりに入力した値が付きます。ドライバ名が長い場合に使用します。

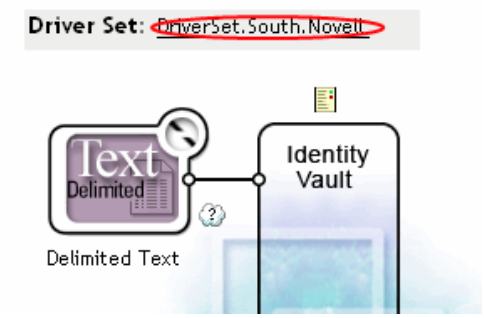
2.12.2 iManager でのトレースレベルの追加

ドライバセットオブジェクトまたは各ドライバオブジェクトにトレースレベルを追加できます。

ドライバセット

1. iManager で、［Identity Manager］>［Identity Manager の概要］の順に選択します。
2. ドライバセットオブジェクトを参照し、［検索］をクリックします。

3 ドライバセット名をクリックします。



4 ドライバセットオブジェクトの［その他］タブを選択します。

5 トレースパラメータを設定し、［OK］をクリックします。これらのパラメータの詳細については、37 ページの 表 2-1 を参照してください。

ドライバ

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

2 ドライバオブジェクトがあるドライバセットオブジェクトを参照し、［検索］をクリックします。

3 ドライバオブジェクトの右上隅をクリックし、［プロパティの編集］をクリックします。

4 ドライバオブジェクトの［その他］タブを選択します。

5 トレースパラメータを設定し、［OK］をクリックします。詳細については、38 ページの 表 2-2 を参照してください。

注 : ［Use setting from Driver Set (ドライバセットの設定を使用する)］のオプションは、iManager には存在しません。

2.12.3 ファイルへの Identity Manager のプロセスのキャプチャ

Identity Manager のプロセスをファイルに保存する場合、ドライバオブジェクトのパラメータ、または DSTRACE を使用して保存します。ドライバオブジェクトのパラメータは、［トレースファイル］パラメータです。

次の方法は、異なる OS プラットフォーム上で DSTRACE を使用して、Identity Manager のプロセスをキャプチャおよび保存する場合に役立ちます。

NetWare

システムコンソールにトレースメッセージを表示したり、ファイル (SYS:\SYSTEM\DSTRACE.LOG) にトレースメッセージを出力したりするには、DSTRACE.NLM を使用します。DSTRACE.NLM により、［DSTRACE Console (DSTRACE コンソール)］画面にトレースメッセージが表示されます。

1 サーバコンソールで「DSTRACE.NLM」と入力します。

これにより、メモリに DSTRACE.NLM がロードされます。

2 サーバコンソールで「DSTRACE SCREEN ON」と入力します。

［DSTRACE Console (DSTRACE コンソール)］画面にトレースメッセージが表示されます。

3 サーバコンソールで「DSTRACE FILE ON」と入力します。

これにより、［DSTRACE Console (DSTRACE コンソール)］に送信されたトレースメッセージが DSTRACE.LOG にキャプチャされます。

4 サーバコンソールで「DSTRACE -ALL」と入力します。

すべてのトレースのフラグがオフになります。

5 サーバコンソールで「DSTRACE +DXML DSTRACE +DVRS」と入力します。

Identity Manager イベントが表示されます。

6 サーバコンソールで「DSTRACE +TAGS DSTRACE +TIME」と入力します。

メッセージタグおよびタイムスタンプが表示されます。

7 ［DSTRACE Console (DSTRACE コンソール)］画面に切り替え、渡されるイベントを確認します。

8 サーバコンソールに再度切り替えます。

9 サーバコンソールで「DSTRACE FILE OFF」と入力します。

ログファイルへのトレースメッセージのキャプチャが停止されます。ファイルへの情報のログも停止されます。

10 テキストエディタで DSTRACE.LOG を開き、変更したイベントまたはオブジェクトを検索します。

Windows

1 ［コントロールパネル］>［NDS Services (NDS サービス)］>［dstrace.dlm］の順に開き、［開始］をクリックします。

［NDS Server Trace Utility (NDS サーバトレースユーティリティ)］という名前のウィンドウが開きます。

2 ［編集］>［オプション］の順に選択し、［すべてクリア］をクリックします。

これにより、すべてのデフォルトのフラグがクリアされます。

3 ［DirXML］>［DirXML ドライバ］の順に選択します。

4 ［OK］をクリックします。

5 ［ファイル］>［新規］の順に選択します。

6 ファイル名および DSTRACE 情報を保存する場所を指定し、［開く］をクリックします。

7 イベントが発生するのを待機します。

8 ［ファイル］>［閉じる］の順に選択します。

これにより、ログファイルへの情報の書き込みが停止されます。

9 テキストエディタでファイルを開き、変更したイベントまたはオブジェクトを検索します。

UNIX

1 「ndstrace」と入力し、ndstrace ユーティリティを起動します。

2 「set ndstrace=nodebug」と入力します。

現在設定されているすべてのトレースのフラグがオフになります。

3 「set ndstrace on」と入力します。

トレースメッセージがコンソールに表示されます。

4 「set ndstrace file on」と入力します。

eDirectory がインストールされたディレクトリにある ndstrace.log ファイルに、トレースメッセージがキャプチャされます。デフォルトでは、/var/nds です。

5 「set ndstrace=+dxml」と入力します。

Identity Manager イベントが表示されます。

6 「set ndstrace=+dvrs」と入力します。

Identity Manager ドライバイベントが表示されます。

7 イベントが発生するのを待機します。

8 「set ndstrace file off」と入力します。

これにより、ファイルへの情報のログが停止されます。

9 「exit」と入力し、ndstrace ユーティリティを終了します。

10 ファイルをテキストエディタで開きます。変更されたイベントまたはオブジェクトを検索します。

iMonitor

iMonitor を使用すると、Web ブラウザから DSTRACE 情報を参照できます。Identity Manager が実行されている場所は関係ありません。iMonitor を実行するファイルは、次のとおりです。

- NDSIMON.NLM - NetWare で動作します。
- NDSIMON.DLM - Windows で動作します。
- ndsimonitor - UNIX で動作します。

1 http://*server_ip*:8008/nds から iMonitor にアクセスします。

ポート 8008 はデフォルトのポートです。

2 管理者権限を使用してユーザ名およびパスワードを入力し、［ログイン］をクリックします。

3 左側の［トレースの環境設定］を選択します。

4 ［すべてクリア］をクリックします。

5 ［DirXML］>［DirXML ドライバ］の順に選択します。

6 ［オン］をクリックします。

7 左側の［トレース履歴］を選択します。

8 ドキュメントの［Modification Time of Current (現在の変更時刻)］をクリックし、ライブトレースを表示します。

9 より頻繁に情報を表示するには、［リフレッシュ間隔］を変更します。

10 左側の［トレースの環境設定］を選択し、［オフ］をクリックしてトレースをオフにします。

11 ［トレース履歴］を選択すると、トレースの履歴を表示できます。ファイルはタイムスタンプで区別されます。

HTML ファイルのコピーが必要な場合、デフォルトの場所は次のとおりです。

- NetWare: SYS:\SYSTEM\ndsimon\DSTRACE*.htm
- Windows: *Drive_letter*:\Novell\NDS\ndsimon\dstrace*.htm
- UNIX: /var/nds/dstrace/*.htm

接続システムの設定

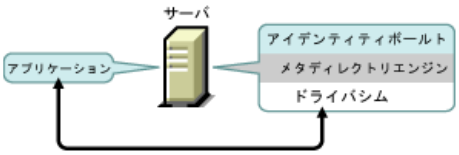
3

ここでは、次の各項目について説明します。

3.1 概要

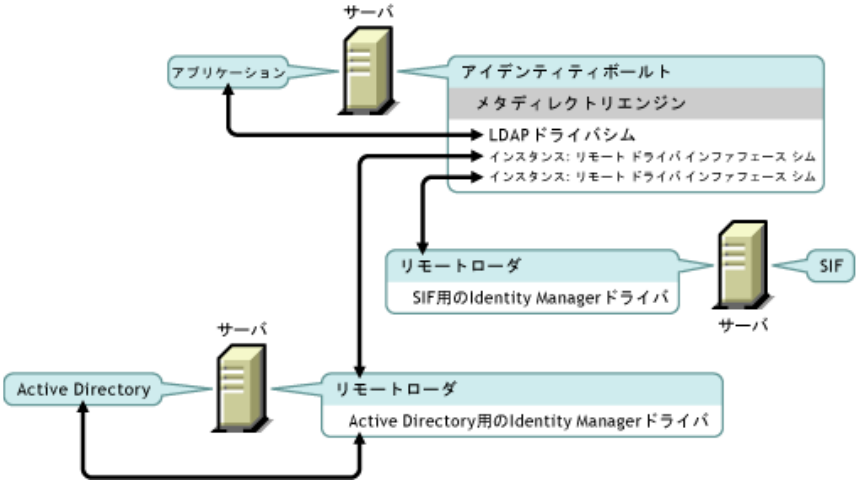
次の図に示すように、メタディレクトリエンジンは eDirectory の一部としてサーバ上で実行されます。Identity Manager ドライバシムとその設定済みドライバは、アプリケーションおよびメタディレクトリエンジンと通信します。

図 3-1 *eDirectory* の下で実行しているメタディレクトリエンジン



次の図に示すように、接続システムにより、アプリケーション間で Identity Manager の機能が拡張されます。

図 3-2 リモートローダを含む接続システム



接続システムにはリモートローダが必要です。このサービスにより、メタディレクトリエンジンは、次のように、異なるプロセスとして異なる場所で実行している Identity Manager ドライバとデータを交換できます。

- メタディレクトリエンジンを実行しているサーバ上の別のプロセスとして実行する

メタディレクトリエンジンは eDirectory プロセスの一部として実行されます。Identity Manager ドライバは、メタディレクトリエンジンを実行しているサーバで実行できます。実際に、これらはメタディレクトリエンジンと同じプロセスの一部として実行できます。

効率化の観点から、Identity Manager ドライバをサーバ上の別のプロセスとして実行できますが、通常、Identity Manager ドライバは別のサーバで実行します。

ドライバを別のプロセスとして実行する場合、リモートローダにより、メタディレクトリエンジンとドライバ間の通信チャネルが提供されます。

- メタディレクトリエンジンを実行しているサーバ以外のサーバで実行する

  一部の Identity Manager ドライバは、メタディレクトリエンジンを実行している場所では実行できません。リモートローダを使用すると、メタディレクトリエンジンを特定の環境で実行しつつ、Identity Manager ドライバを別の環境のサーバで実行できます。たとえば、NetWare サーバ上で Active Directory ドライバを実行できません。メタディレクトリエンジンは、NetWare サーバで実行でき、リモートローダは Active Directory サーバで実行します。

  シナリオ **:** 別のサーバ。メタディレクトリエンジンは NewWare サーバ上で実行します。Active Directory 用の Identity Manager ドライバを実行する必要があります。このドライバは、Active Directory 環境で実行する必要があるため、NetWare サーバ上では実行できません。Windows 2003 サーバ上にリモートローダをインストールして実行してください。リモートローダは、Active Directory ドライバとメタディレクトリエンジンの間の通信チャネルになります。

  シナリオ **:** ホスト以外。メタディレクトリエンジンは Solaris 上で実行します。ユーザアカウントのプロビジョニングを行う NIS システムと通信する必要があります。通常、NIS システムはメタディレクトリエンジンをホストしません。NIS システム上にリモートローダと NIS 用の Identity Manager ドライバをインストールしてください。NIS システム上のリモートロードが NIS ドライバを実行して、メタディレクトリエンジンと NIS ドライバがデータを交換できるようにします。

Identity Manager 3 では、dirxml_remote、rdxml、または dirxml_jremote を使用してリモートローダの機能が提供されます。

Dirxml_remote

Dirxml_remote は、Windows 上で実行している Identity Manager ドライバとメタディレクトリエンジンを通信できるようにする実行可能ファイルです。

リモートローダコンソールでは、dirxml_remote.exe が使用されます。コマンドラインでパラメータを付けずに dirxml_remote.exe を指定した場合、リモートローダアプリケーションウィザードが起動します。「dirxml_remote.exe」と入力してパラメータを渡すと、リモートローダが起動します。

Rdxml

Rdxml は、Solaris、Linux、または AIX 環境で実行している Identity Manager ドライバとメタディレクトリエンジンを通信できるようにする実行可能ファイルです。

Rdxml は、ネイティブドライバと Java ドライバの両方をサポートしています。

Dirxml_jremote

Dirxml_jremote は、純粋な Java リモートローダです。1 つのサーバで実行しているメタディレクトリエンジンと、rdxml または Dirxml_jremote を実行していない場所で実行して

いる Identity Manager ドライバとの間で、データを交換するために使用されます。互換性がある JRE (最低でも 1.4.0、1.4.2 以降を推奨) および Java Sockets がインストールされていればどのシステムでも動作しますが、正式にサポートされているのは次のとおりです。

- HP-UX
- AS/400
- OS/390
- z/OS

概要 **:** 主な作業

リモートローダを使用するには、次の作業を行う必要があります。

- SSL (セキュアソケットレイヤ) を使用する場合、安全なデータ転送のために証明書を指定します。
- リモートローダをインストール、設定、および実行します。
- Identity Manager ドライバをインポート、設定、および起動します。

管理者によっては、リモートローダを設定する前に Identity Manager ドライバをインポートおよび設定する場合があります。ドライバをすでに実行中であるが、リモートでも実行できるようにしたい場合などです。

一方、リモートローダを実行中でも、ドライバをインポート、設定、および起動して、メタディレクトリエンジン、リモートローダ、および Identity Manager ドライバの間で適切な通信が行われているかどうかをすぐに確認できます。

3.2 安全なデータ転送の提供

SSL (セキュアソケットレイヤ) を使用して安全なデータ転送を提供する場合は、次の作業を完了します。

1. サーバ証明書を作成する。

   証明書が認識されない場合、新しい証明書を作成します。

   ただし、SSL サーバ証明書がすでに存在し、SSL 証明書を使用したことがある場合は、新しい証明書を作成して使用しなくても、既存の証明書を使用できます。

   サーバがツリーに追加されると、eDirectory によって次のデフォルトの証明書が作成されます。

   - SSL CertificateIP
   - SSL CertificateDNS
2. 自己署名証明書をエクスポートする。

3.2.1 サーバ証明書の作成

1 Novell iManager で、［Novell Certificate Server］>［サーバ証明書の作成］の順にクリックします。

2 証明書を所有するサーバを選択し、証明書のニックネーム (remotecert など) を付けます。

重要 : 証明書のニックネームにはスペースを使用しないことをお勧めします。たとえば、「remote cert」ではなく、「remotecert」を使用します。

また、証明書のニックネームは忘れないよう書き留めておいてください。このニックネームは、ドライバのリモート接続パラメータの KMO 名に使用します。

---

3 ［作成方法］は［標準］のままにし、［次へ］をクリックします。

4 ［概要］の画面を確認し、［終了］をクリックして［閉じる］をクリックします。

これでサーバ証明書が作成されました。続いて、46 ページのセクション 3.2.2「自己署名証明書のエクスポート」に進みます。

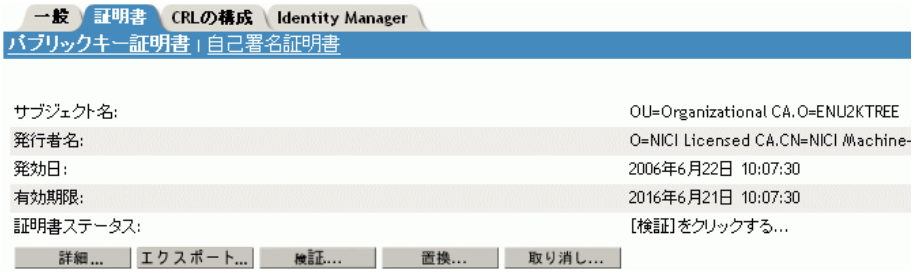
3.2.2 自己署名証明書のエクスポート

1 iManager で、［eDirectory 管理］>［オブジェクトの変更］の順にクリックします。

2 セキュリティコンテナの認証局を参照して選択し、［OK］をクリックします。

CA (認証局) にはツリー名に基づいた名前 (Treename-CA.Security) が付けられます。

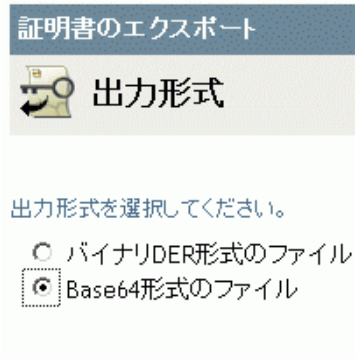
3 ［証明書］タブをクリックして［自己署名証明書］、［エクスポート］の順にクリックします。



4 証明書のエクスポートウィザードで、［いいえ］を選択して［次へ］をクリックします。

秘密鍵は、証明書と一緒にエクスポートしないようにします。

5 ［Base64 形式のファイル］を選択し (akranes-tree CA.b64 など)、［次へ］をクリックします。



6 ［エクスポートされた証明書をファイルに保存してください。］へのリンクをクリックし、ファイル名を指定して、場所を指定してから［保存］をクリックします。

ルートファイル名には、拡張子 .pem が必要です。

7 ［名前を付けて保存］ダイアログボックスで、このファイルをローカルディレクトリにコピーします。

8 ［閉じる］をクリックします。

3.3 リモートローダの設定

ここでは、次の各項目について説明します。

- 48 ページのセクション 3.3.1「リモートローダのインストール」
- 50 ページのセクション 3.3.2「リモートローダの設定」
- 61 ページのセクション「Solaris、Linux、または AIX での環境変数の設定」
- 62 ページのセクション「リモートローダの起動」64 ページのセクション「リモートローダの停止」
- 64 ページのセクション「リモートローダの停止」

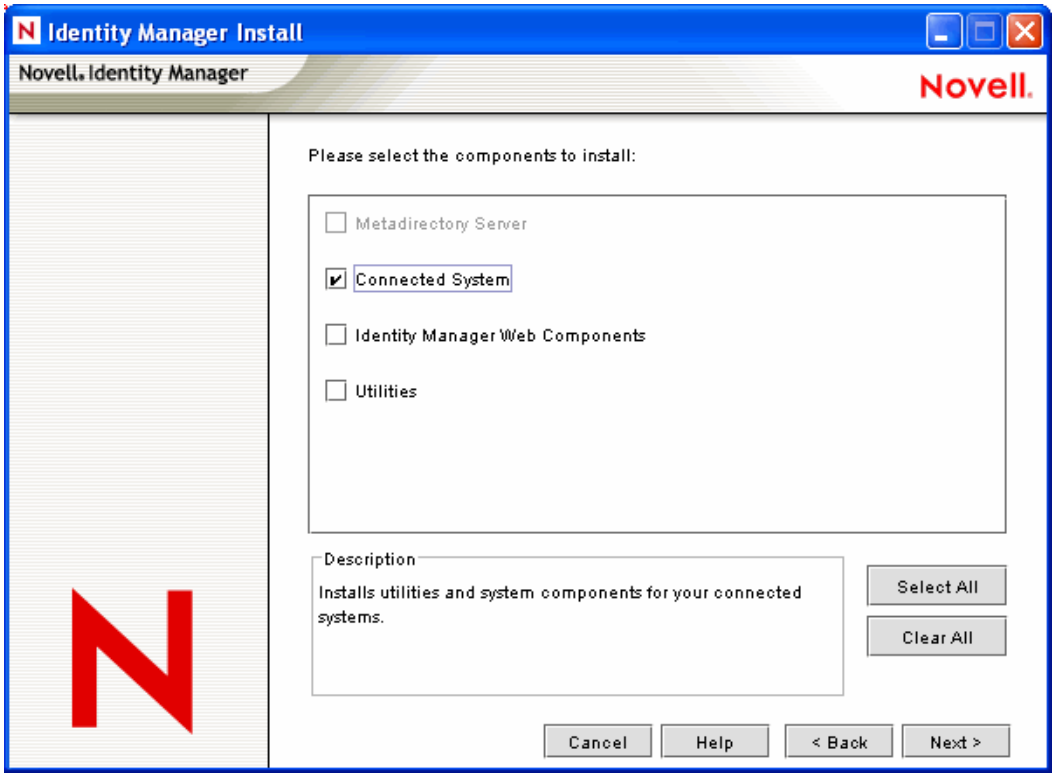
3.3.1 リモートローダのインストール

ここでは、次の各項目について説明します。

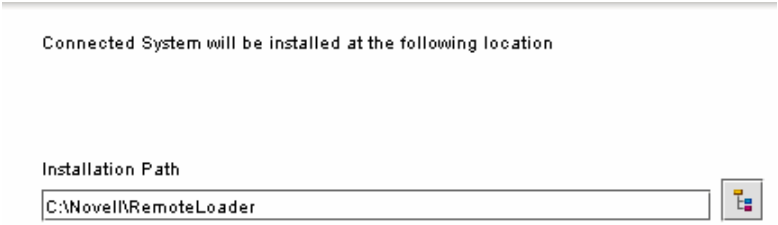
- 48 ページの 「Windows サーバへのリモートローダのインストール」
- 49 ページの 「Solaris、Linux、または AIX へのリモートローダのインストール」
- 50 ページの 「HR-UX、AS/400、OS/390、または z/OS へのリモートローダのインストール」

Windows サーバへのリモートローダのインストール

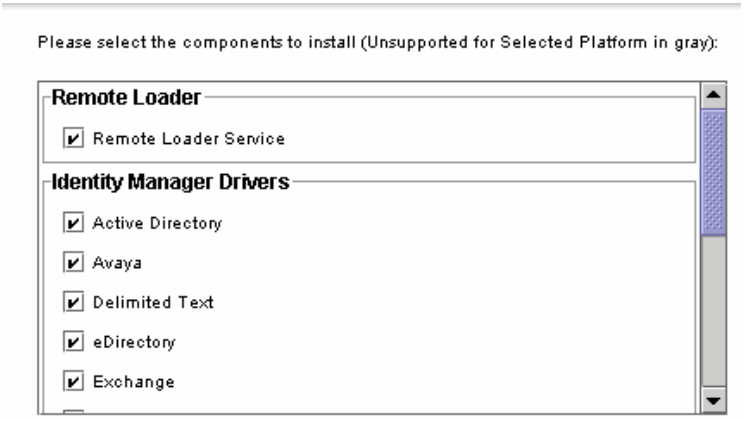
1. Identity Manager 3 インストールプログラム (\nt\install.exe など) を実行します。
2. 最初の画面を確認して、使用許諾契約に同意し、2 つの概要ページを表示します。
3. ［Identity Manager のインストール］ダイアログボックスで、［接続システム］以外のすべてのコンポーネントを選択解除して、［次へ］をクリックします。



4. 接続システム (リモートローダとリモートドライバシム) の場所を選択し、［次へ］をクリックします。



5 ［リモートローダサービス］とリモートドライバシム (ドライバ) を選択し、［次へ］をクリックします。



6 アクティベーション要件を確認して、インストールする製品を表示し、［終了］をクリックします。

7 デスクトップに［リモートローダコンソール］アイコンを作成するかどうかを選択します。

Solaris、Linux、または AIX へのリモートローダのインストール

このセクションは、Identity Manager 3 をダウンロードして展開してあることを前提として説明しています。Identity Manager をダウンロードする必要がある場合、Novell のダウンロード Web サイト (http://download.novell.com) にアクセスしてください。

Novell Web サイトからダウンロードした Identity Manager 3 ファイルを展開した後で、次のステップを実行します。

1 プラットフォームに応じて、次のインストールファイルの 1 つを実行します。

- dirxml_solaris.bin
- dirxml_linux.bin
- dirxml_aix.bin

2 使用許諾契約に同意した後で、<Enter> キーを押し、次の［インストールセットの選択］ページを表示します。

```
===============================================================================
Choose Install Set
------------------

Please choose the Install Set to be installed by this installer.

  ->1- Metadirectory Server
    2- Connected System Server
    3- Web-based Administrative Server

    4- Customize...

ENTER THE NUMBER FOR THE INSTALL SET, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
   :
```

3 「2」と入力して［Connected System Server］を選択し、<Enter> キーを押します。

4 ［インストール前の概要］画面で、インストールするよう選択したコンポーネントを確認し、<Enter> キーを押します。

```
================================================================================
Pre-Installation Summary
------------------------

Please Review the Following Before Continuing:

Install Set
    Connected System Server

Product Components:
    LDAP Driver,
    SAP Driver,
    JDBC Driver,
    Delimited Text Driver,
    Notes Driver,
    Remote Loader,
    Groupwise Driver,
    AVAYA Driver,
    SOAP Driver,
    REMEDY Driver


PRESS <ENTER> TO CONTINUE:
```

HR-UX、AS/400、OS/390、または z/OS へのリモートローダのインストール

HP-UX、AS/400、OS/390、および z/OS のプラットフォームには、Java リモートローダが必要です。

1 Java リモートローダを実行するターゲットシステムにディレクトリを作成します。

2 ステップ 1 で作成したディレクトリに、Identity Manager 3 CD またはダウンロードイメージから /java_remoteloader ディレクトリ内の適切なファイルをコピーします。

プラットフォーム	ファイル
HP-UX AS/400	dirxml_jremote.tar.gz dirxml_jremote.tar.gz dirxml_jremote_mvs.tar
z/OS OS/390	dirxml_jremote_mvs.tar

3 HP-UX、AS/400、または z/OS では、dirxml_jremote ファイルを圧縮解除します。

4 コピーした tar 形式ファイルを解凍 (untar) します。

これで Java リモートローダを設定する準備ができました。tar ファイルにはドライバが含まれていないため、ドライバを手動で lib ディレクトリにコピーする必要があります。lib ディレクトリは、解凍を行ったディレクトリの下にあります。

MVS の詳細については、dirxml_jremote_mvs.tar ファイルを解凍して、usage.html ドキュメントを参照してください。

3.3.2 リモートローダの設定

リモートローダは、.dll、.so、または .jar ファイルに含まれる Identity Manager アプリケーションシムをホストできます。Java リモートローダは Java ドライバシムのみをホストし、ネイティブ (C++) ドライバシムはロードまたはホストしません。

- 51 ページの 「Windows でのリモートローダの設定」

- 56 ページの 「コマンドラインオプションを使用したリモートローダの設定」
- 62 ページの 「リモートローダの起動」
- 64 ページの 「リモートローダの停止」

Windows でのリモートローダの設定

- 51 ページの 「リモートローダコンソールユーティリティの使用」
- 52 ページの 「リモートローダインスタンスの追加」
- 56 ページの 「リモートローダインスタンスの編集」

リモートローダコンソールユーティリティの使用

リモートローダコンソールは、Windows でのみ実行できます。コンソールを使用すると、そのコンピュータのリモートローダで実行しているすべての Identity Manager ドライバを管理できます。

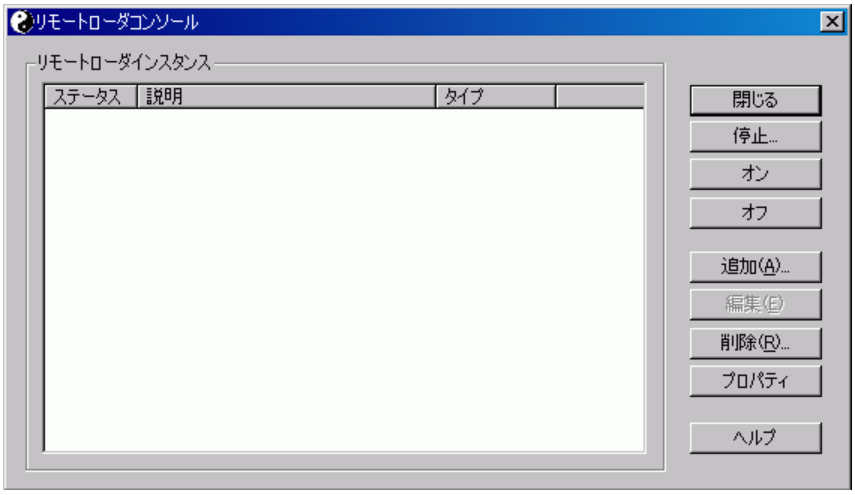
Identity Manager 3 にアップグレードすると、コンソールはリモートローダの既存のインスタンスを検出し、インポートします (自動的にインポートするには、ドライバ環境設定をリモートローダのディレクトリ (通常は c:\novell\remoteloader) に保存する必要があります)。その後、コンソールを使用してリモートドライバを管理できます。

リモートローダコンソールを起動するには、デスクトップ上の［リモートローダコンソール］アイコンをクリックします。

図 *3-3* ［リモートローダコンソール］アイコン

リモートローダコンソールを使用すると、リモートローダサービスの各インスタンスを起動、停止、追加、削除、および編集できます。

図 *3-4* リモートローダコンソール



コマンドラインでパラメータを付けずに「dirxml_remote.exe」と入力すると、リモートローダアプリケーションウィザードが起動します。

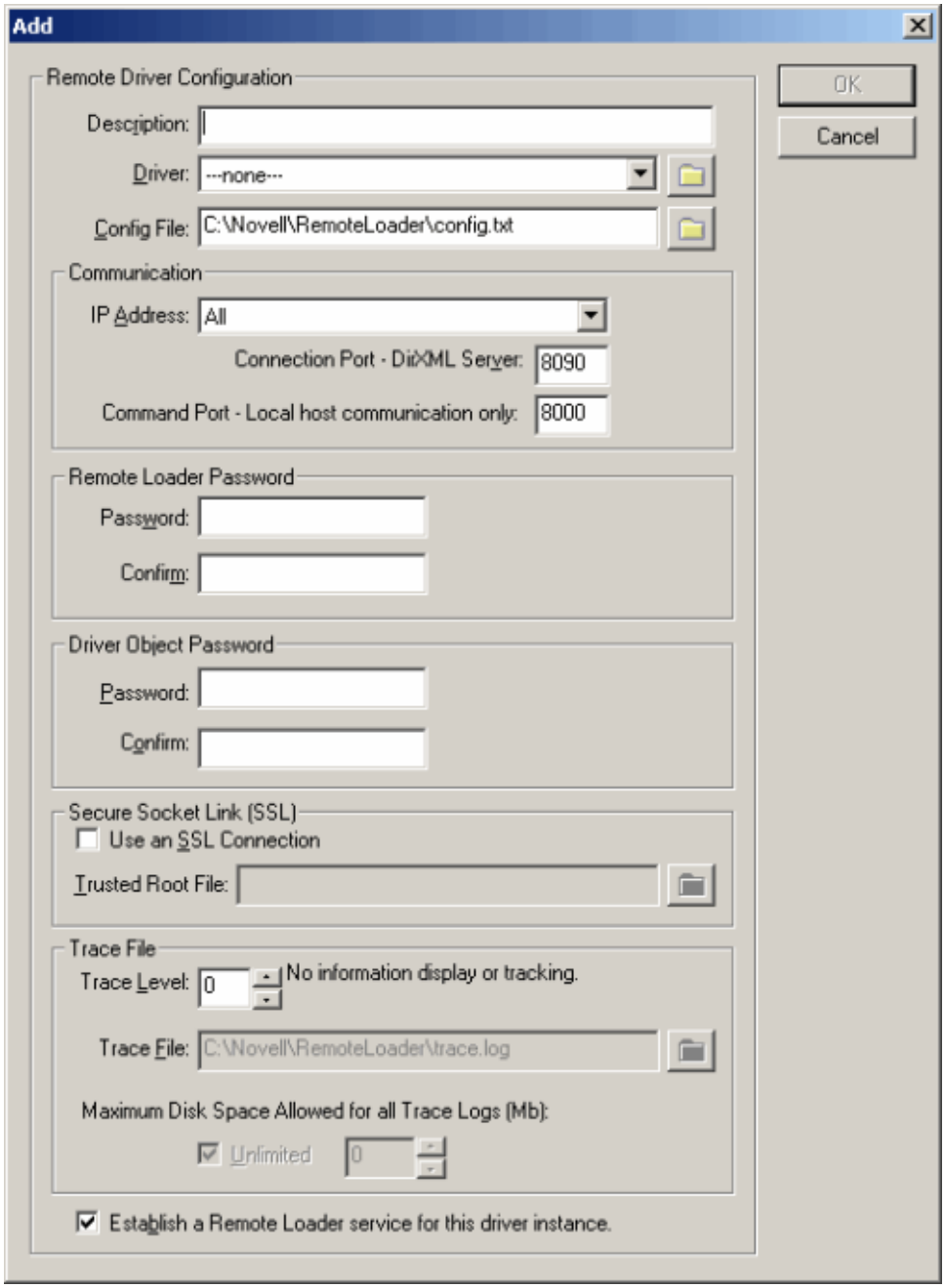
注 : ウィザードとコンソールを併用すると、予期しない動作が起こることがあります。そのため、以降はリモートローダコンソールを使用して、既存の設定をコンソールにアップグレードすることをお勧めします。

リモートローダインスタンスの追加

リモートローダインスタンスを追加するには、[追加] をクリックして次の情報を指定します。

- 53 ページの 「リモートドライバ環境設定」
- 54 ページの 「通信パラメータ」
- 54 ページの 「リモートローダパスワード」
- 55 ページの 「ドライバオブジェクトパスワード」
- 55 ページの 「Secure Socket Link (SSL)」
- 55 ページの 「トレースファイル」
- 56 ページの 「Establish a Remote Loader Service for this Drive Instance (このドライバインスタンスのリモートローダサービスを設定する)」

図 *3-5* リモートローダの環境設定パラメータ



リモートドライバ環境設定

図 *3-6* リモートドライバ環境設定

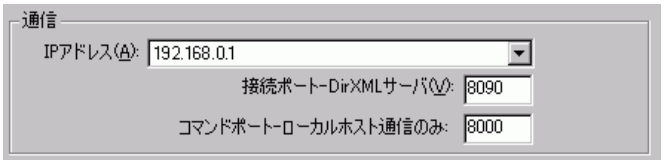
- 説明 : リモートローダインスタンスを識別する説明を指定します。

- ドライバ : ドライバに適したシムを参照して選択します。
- 環境設定ファイル : 環境設定ファイルの名前を指定します。

  リモートローダコンソールは、環境設定パラメータをこのテキストファイルに保存し、実行時にこれらのパラメータを使用します。

通信パラメータ

図 *3-7* 通信パラメータ



- IP アドレス : リモートローダがメタディレクトリサーバからの接続をリッスンする IP アドレスを指定します。
- Connection Port - metadirectory server (接続ポート - メタディレクトリサーバ): リモートローダがメタディレクトリサーバからの接続をリッスンする TCP ポートを指定します。

  この接続のデフォルトの TCP/IP ポートは 8090 です。新しいインスタンスを作成するたびに、デフォルトのポート番号が自動的に 1 つずつ増えます。
- コマンドポート-ローカルホスト通信のみ: リモートローダがStopやChange Trace Levelなどのコマンドをリッスンする TCP ポート番号を指定します。

  特定のコンピュータ上で実行されるリモートローダの各インスタンスには、異なるコマンドポート番号を設定する必要があります。デフォルトのコマンドポートは 8000 です。新しいインスタンスを作成するたびに、デフォルトのポート番号が自動的に 1 つずつ増えます。

注 **:** 接続ポートとコマンドポートを別個に指定することによって、複数のドライバインスタンスをホストする同一のサーバから、リモートローダの複数のインスタンスを実行できます。

リモートローダパスワード

図 *3-8* リモートローダパスワード

- パスワード : このパスワードは、ドライバの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使用します。

  パスワードは、ドライバを設定したときに［Identity Manager Configuration (Identity Manager 設定)］ページの［認証］セクションの［リモートローダパスワードの入力］編集ボックスに入力したパスワードと大文字小文字まで同じである必要があります。
- 確認 : パスワードを再入力します。

ドライバオブジェクトパスワード

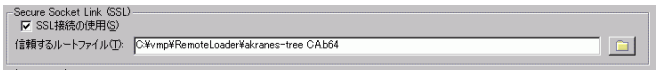
図 3-9 ドライバオブジェクトパスワード

- パスワード : リモートローダは、このパスワードを使用してメタディレクトリサーバに対して自身を認証します。

  このパスワードは、ドライバを設定したときに、［ドライバ環境設定］ページの［ドライバオブジェクトパスワード］編集ボックスに入力したパスワードと同じパスワードを設定する必要があります。
- 確認 : パスワードを再入力します。

Secure Socket Link (SSL)

図 3-10 *Secure Socket Link (SSL)*

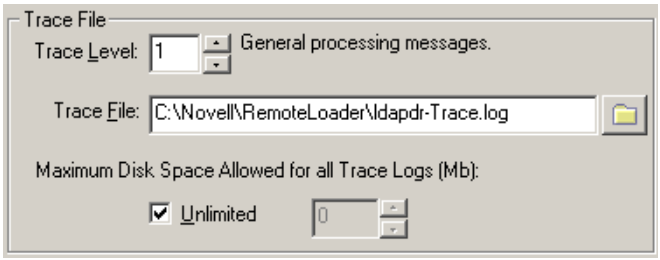


- SSL 接続の使用 : SSL 接続を指定する場合は、このオプションを選択します。
- ルート認証局ファイル : ルート認証局ファイルを参照して選択します。

  これは、eDirectory ツリーの組織認証局からエクスポートされた自己署名証明書です。46 ページのセクション 3.2.2「自己署名証明書のエクスポート」を参照してください。

トレースファイル

図 3-11 トレースファイル



- トレースレベル : リモートローダインスタンスがリモートローダとドライバの両方からの情報メッセージを含むトレースウィンドウを表示するには、ゼロよりも大きいトレースレベルを設定します。最も一般的な設定は、トレースレベル 3 です。

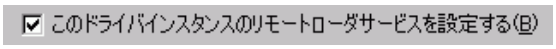
  トレースレベルを 0 に設定すると、トレースウィンドウが表示されないか、またはトレースウィンドウにメッセージが表示されません。
- ［トレースファイル］で、トレースメッセージを書き込むトレースファイル名を指定します。

特定のマシンで実行しているリモートローダの各インスタンスには、個別のトレースファイルを使用する必要があります。トレースメッセージは、トレースレベルがゼロよりも大きい場合にだけトレースファイルに書き込まれます。

- すべてのトレースログに許される最大ディスク領域 (MB): ディスク上で、このインスタンスのトレースファイルデータに使用できる最大サイズを指定します。

Establish a Remote Loader Service for this Drive Instance (このドライバインスタンスのリモートローダサービスを設定する)

図 3-12 *Establish a Remote Loader Service for this Drive Instance (* このドライバインスタンスのリモートローダサービスを設定する *)*



- リモートローダインスタンスをサービスとして設定するには、このオプションを選択します。このオプションを有効にすると、オペレーティングシステムはコンピュータの起動時に自動的にリモートローダを起動します。

リモートローダインスタンスの編集

1. ［説明］カラムから［リモートローダインスタンス］を選択します。
2. ［停止］をクリックしてリモートローダのパスワードを入力し、［OK］をクリックします。
3. ［編集］をクリックし、環境設定情報を変更します。リモートローダインスタンスを追加するときと同じフィールドを使用します。

コマンドラインオプションを使用したリモートローダの設定

リモートローダを実行するために、すべてのプラットフォームで環境設定ファイル (LDAPShim.txt など) が使用されます。コマンドラインのオプションを使用して、環境設定ファイルを作成または編集できます。次の手順に従って、環境設定ファイルの基本的なパラメータを設定します。その他のパラメータの詳細については、261 ページの付録 B「リモートローダの設定オプション」を参照してください。

1. テキストエディタを開きます。
2. (オプション) -description オプションを使用して、説明を加えます。

オプション	2 次名	パラメータ	説明
-description	-desc	短い説明	トレースウィンドウのタイトルと Nsure Audit のログに使用される短い説明の文字列 (SAP など) を指定します。 例 : -description SAP -desc SAP 環境設定ファイルには、リモートローダコンソールによって長い形式が配置されます。長い形式 (たとえば -description) または短い形式 (たとえば -desc) のいずれかを使用できます。

3 -commandport オプションを使用して、リモートローダインスタンスによって使用される TCP/IP ポートを指定します。

オプション	2 次名	パラメータ	説明
-commandport	-cp	ポート番号	リモートローダインスタンスが制御目的で使用する TCP/IP ポートを指定します。リモートローダインスタンスがアプリケーションシムをホストしている場合、コマンドポートには、別のリモートローダインスタンスが、シムをホストしているインスタンスと通信するポートが指定されます。リモートローダインスタンスが、アプリケーションシムをホストしているインスタンスにコマンドを送信する場合、コマンドポートは管理インスタンスがリッスンしているポートが指定されます。コマンドポートが指定されていない場合のデフォルトポートは 8000 です。複数の接続ポートとコマンドポートを指定することで、異なるドライバインスタンスをホストしている同じサーバ上でリモートローダの複数のインスタンスを実行できます。 例 : -commandport 8001 -cp 8001

4 -connection オプションを使用して、Identity Manager のリモートインタフェースシムで実行しているメタディレクトリサーバに接続するためのパラメータを指定します。

「-connection " パラメータ [パラメータ] [パラメータ]"」と入力します。

たとえば、次のいずれかを入力します。

```
-connection "port=8091 rootfile=server1.pem" -conn "port=8091
rootfile=server1.pem"
```

パラメータはすべて二重引用符で囲む必要があります。パラメータには、次のようなものがあります。

オプション	2 次名	パラメータ	説明
-connection	-conn	接続設定文字列	Identity Manager リモートインタフェースシムを実行しているメタディレクトリサーバに接続するための接続パラメータを指定します。リモートローダのデフォルトの接続方法は、SSL を使用した TCP/IP です。この接続のデフォルトの TCP/IP ポートは 8090 です。リモートローダの複数のインスタンスを同じサーバ上で実行できます。リモートローダの各インスタンスは個別の Identity Manager アプリケーションシムインスタンスをホストします。リモートローダの各インスタンスに個別の接続ポートとコマンドポートを指定することによって、リモートローダの複数のインスタンスを区別します。 例 : -connection "port=8091 rootfile=server1.pem" -conn "port=8091 rootfile=server1.pem"
port		10 進数のポート番号	必須パラメータ。リモートローダがリモートインタフェースシムからの接続をリッスンする TCP/IP ポートを指定します。 例 : port=8090
address		IP アドレス	オプションのパラメータ。リモートローダが特定のローカル IP アドレスをリッスンするよう指定します。リモートローダをホストするサーバが複数の IP アドレスを持ち、リモートローダは 1 つのアドレスのみをリッスンしなければならない場合などに便利です。 次の 3 つの方法があります。address= *アドレス番号* address='localhost' このパラメータを使用しない -address を使用しない場合、リモートローダはすべてのローカル IP アドレスをリッスンします。 例 : address=137.65.134.83
rootfile			条件付きパラメータ。SSL を実行していて、リモートローダがネイティブドライバと通信する必要がある場合、次を入力します。 rootfile='*trusted certname*'

オプション	2 次名	パラメータ	説明
keystore			条件付きパラメータ。.jar ファイルに含まれる Identity Manager アプリケーションシムにのみ使用します。 リモートインタフェースシムによって使用される証明書の発行者のルート認証局証明書を含む、Java キーストアのファイル名を指定します。通常、これはリモートインタフェースシムをホストしている eDirectory ツリーの認証局です。 SSL を実行していて、リモートローダが Java ドライバと通信する必要がある場合、次の key-value ペアを入力します。 keystore='*keystorename*' storepass='*password*'
-storepass		キーストアのパスワード	.jar ファイルに含まれる Identity Manager アプリケーションシムにのみ使用します。keystore パラメータで指定した Java キーストアのパスワードを指定します。 例 : storepass=mypassword このオプションは Java リモートローダにのみ適用されます。

5 (オプション) -trace オプションを使用して、トレースパラメータを指定します。

オプション	2 次名	パラメータ	説明
-trace	-t	整数	トレースレベルを指定します。これはアプリケーションシムをホストする場合にのみ使用できます。トレースレベルはメタディレクトリサーバで使用されているレベルと同じです。 例 : -trace 3 -t 3

6 (オプション) -tracefile オプションを使用して、トレースファイルを指定します。

オプション	2 次名	パラメータ	説明
-tracefile	-tf	ファイル名	トレースメッセージを書き込むファイルを指定します。トレースメッセージは、トレースレベルがゼロよりも大きい場合にファイルに書き込まれます。トレースメッセージは、トレースウィンドウが開いていなくてもファイルに書き込まれます。 例 : -tracefile c:\temp\trace.txt -tf c:\temp\trace.txt

7 (オプション) -tracefilemax オプションを使用して、トレースファイルのサイズを制限します。

たとえば、次のいずれかを入力します。

```
-tracefilemax 1000M -tfm 1000M
```

この例では、トレースファイルは 1GB までです。

オプション	2 次名	パラメータ	説明
-tracefilemax	-tfm	サイズ	ディスク上でトレースファイルデータに使用できる最大サイズを指定します。このオプションを指定すると、tracefile オプションを使用して指定した名前の付いたトレースファイルと、最大 9 個の追加ロールオーバファイルが生成されます。ロールオーバファイルには、メインのトレースファイル名と「*_n*」に基づいた名前が付けられます。「n」は 1 ～ 9 の値になります。 サイズのパラメータはバイト数です。K (キロバイト)、M (メガバイト)、または G (ギガバイト) のサフィックスを使用してサイズを指定します。 リモートローダの起動時に、トレースファイルのデータが指定した最大サイズよりも大きいと、10 ファイルすべてのロールオーバが完了するまで、トレースファイルのデータは指定した最大値よりも大きいままになります。 例 : -tracefilemax 1000M -tfm 1000M この例では、トレースファイルは 1GB までです。

8 -class オプションを使用してクラスを指定するか、-module オプションを使用してモジュールを指定します。

オプション	2 次名	パラメータ	説明
-class	-cl	Java クラス名	ホストする Identity Manager アプリケーションシムの Java クラス名を指定します。 たとえば、Java ドライバに対しては次のいずれかを入力します。 -class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim -cl com.novell.nds.dirxml.driver.ldap.LDAPDriverShim Java では、キーストアを使用して証明書を読み取ります。-class オプションと -module オプションは排他的で、どちらか一方を使用できます。 Java クラス名のリストを参照するには、261 ページの付録 B「リモートローダの設定オプション」の 268 ページの 表 B-2 を参照してください。

オプション	2 次名	パラメータ	説明
-module	-m	モジュール名	ホストする Identity Manager アプリケーションシムを含むモジュールを指定します。 たとえば、ネイティブドライバに対しては次のいずれかを入力します。 -module "c:\Novell\RemoteLoader\Exchange5Shim.dll" -m "c:\Novell\RemoteLoader\Exchange5Shim.dll" または、 -module "usr/lib/dirxml/NISDriverShim.so" -m "usr/lib/dirxml/NISDriverShim.so" -module オプションでは、ルートファイル証明書が使用されます。-module オプションと -class オプションは排他的で、どちらか一方を使用できます。

9 ファイルに名前を付けて保存します。

リモートローダの実行中に一部の設定を変更できます。これらの設定の詳細については、261 ページの付録 B「リモートローダの設定オプション」を参照してください。

パラメータ	説明
-commandport	リモートローダのインスタンスを指定します。
-config	環境設定ファイルを指定します。
-javadebugport	指定されたポートでリモートローダインスタンスが Java デバッグを有効にするよう指定します。
-password	コマンドで送信できるようになります。
-service	インスタンスをサービスとしてインストールします (Windows のみ)。
-tracechange	トレースレベルを変更します。
-tracefilechange	書き込み先のトレースファイルの名前を変更します。
-unload	リモートローダインスタンスをアンロードします。
-window	リモートローダインスタンスでトレースウィンドウのオン / オフを切り替えます (Windows のみ)。

Solaris、Linux、または AIX での環境変数の設定

リモートローダをインストールした後で、rdxml の現在のディレクトリを変更する環境変数 RDXML_PATH を設定できます。設定後、このディレクトリは、以降に作成するファ

イルの基本パスになります。RDXML_PATH 変数の値を設定するには、次のコマンドを入力します。

- set RDXML_PATH=*path*
- export RDXML_PATH

リモートローダの起動

- 62 ページの 「Windows でのリモートローダの起動」
- 63 ページの 「コマンドラインからのリモートローダの起動」

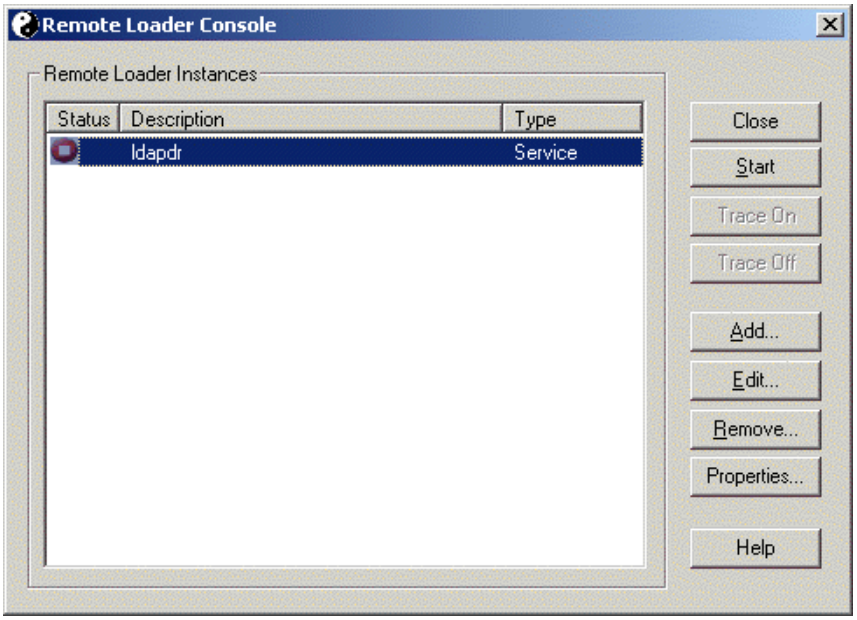
Windows でのリモートローダの起動

Windows でリモートローダを実行する

図 *3-13* ［リモートローダコンソール］アイコン

1 デスクトップ上の［リモートローダコンソール］アイコンをクリックします。

図 *3-14* リモートローダコンソール



2 ドライバインスタンスを選択し、［開始］をクリックします。

コマンドラインからのリモートローダの起動

Solaris、Linux、または AIX では、バイナリコンポーネント rdxml によってリモートローダの機能が提供されます。このコンポーネントは /usr/bin/ ディレクトリにあります。Windows では、デフォルトは c:\novell\RemoteLoader です。

リモートローダを実行する

1 パスワードを設定します。

プラットフォーム	コマンド
Windows	dirxml_remote -config *path_to_config_file* -sp *password password*
Solaris LInux AIX	rdxml -config *path_to_config_file* -sp *password password*
HP-UX AS/400 OS/390 z/OS	dirxml_jremote -config *path_to_config_file* -sp *password password*

オプション	2 次名	パラメータ	説明
-password	-p	パスワード	コマンド認証のパスワードを指定します。このパスワードは、コマンドの発行先のローダインスタンスの **setpasswords** で指定した最初のパスワードと同じパスワードにする必要があります。コマンドオプション (unload や tracechange など) を指定して、**password** オプションを指定しなければ、コマンドの対象となるローダのパスワードを入力するよう要求するメッセージが表示されます。 例 : -password novell4 -p novell4
-setpasswords	-sp	パスワード パスワード	リモートローダインスタンスのパスワード、およびリモートローダが通信するリモートインタフェースシムの Identity Manager ドライバオブジェクトのパスワードを指定します。引数の最初のパスワードは、リモートローダのパスワードです。オプション引数の 2 番目のパスワードは、メタディレクトリサーバのリモートインタフェースシムに関連付けられた Identity Manage ドライバオブジェクトのパスワードです。どちらのパスワードも指定しないか、または両方のパスワードを指定する必要があります。パスワードを指定しないと、リモートローダはパスワードを要求するメッセージを表示します。これは環境設定オプションです。このオプションを使用すると、指定したパスワードがリモートローダインスタンスに設定されます。ただし、このオプションを指定しても、Identity Manager アプリケーションシムはロードされず、ローダの別のインスタンスとも通信しません。 例 : -setpasswords novell4 staccato3 -sp novell4 staccato3

2 リモートローダを起動します。

プラットフォーム	コマンド
Windows	dirxml_remote -config *path_to_config_file*
Solaris LInux AIX	rdxml -config *path_to_config_file*
HP-UX AS/400 OS/390 z/OS	dirxml_jremote -config *path_to_config_file*

3 iManager を使用してドライバを起動します。

4 リモートローダが適切に動作していることを確認します。

リモートローダは、リモートローダがメタディレクトリサーバ上のリモートインタフェースシムと通信している場合にのみ、Identity Manager アプリケーションシムをロードします。たとえば、リモートローダがメタディレクトリサーバとの通信を終了すると、アプリケーションシムはシャットダウンされます。

Linux、Solaris、または AIX では、ps コマンドまたはトレースファイルを使用して、コマンドおよび接続ポートがリッスンしているかどうかを調べます。

HP-UX などのプラットフォームでは、トレースファイル上で tail コマンドを使用して Java リモートローダを監視します。

```
tail -f trace filename
```

ログの最終行に次の情報が表示される場合、ローダは正常に実行しており、Identity Manager リモートインタフェースシムからの接続を待機しています。

```
TRACE: Remote Loader: Entering listener accept()
```

UNIX で自動的に起動するようにリモートローダ (rdxml) を設定するには、TID 10097249 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10097249.htm) を参照してください。

リモートローダの停止

プラットフォーム	コマンド
Windows	リモートローダコンソールを使用して、ドライバインスタンスを停止します。
Solaris LInux AIX	rdxml -config *path_to_config_file* -u
HP-UX AS/400 OS/390 z/OS	dirxml_jremote -config *path_to_config_file* -u

コンピュータでリモートローダの複数のインスタンスが実行されている場合は、リモートローダが適切なインスタンスを停止できるように -cp *command port* オプションを渡します。

リモートローダを停止する場合、十分な権利を持っているか、リモートローダのパスワードを入力する必要があります。

シナリオ : 十分な権利。リモートローダが Windows サービスとして実行されています。リモートローダを停止するための十分な権限を持っています。パスワードを入力しますが、パスワードが正しくないことに気付きます。リモートローダが停止します。

リモートローダはパスワードを受け入れません。この場合パスワードが冗長であるため、パスワードは無視されます。サービスではなくアプリケーションとしてリモートローダを実行している場合は、パスワードが使用されます。

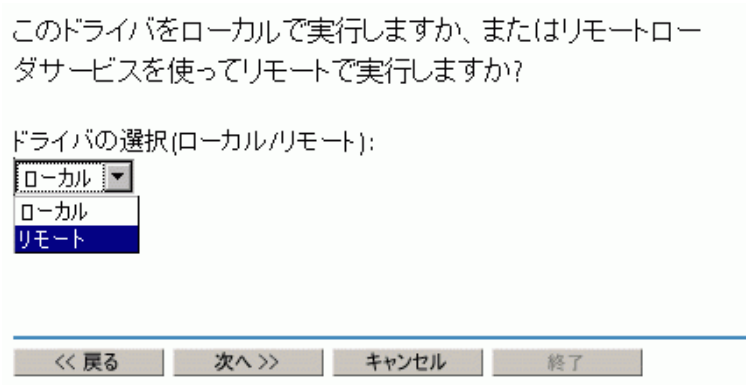
3.4 リモートローダを使用するための、Identity Manager ドライバの設定

新しいドライバを設定するか、または既存のドライバを有効にして、リモートローダと通信できます。このセクションでは、リモートローダと通信するためのドライバの設定に関する一般的な情報について説明します。追加情報およびドライバ固有の情報については、関連するドライバの実装ガイドを参照してください。

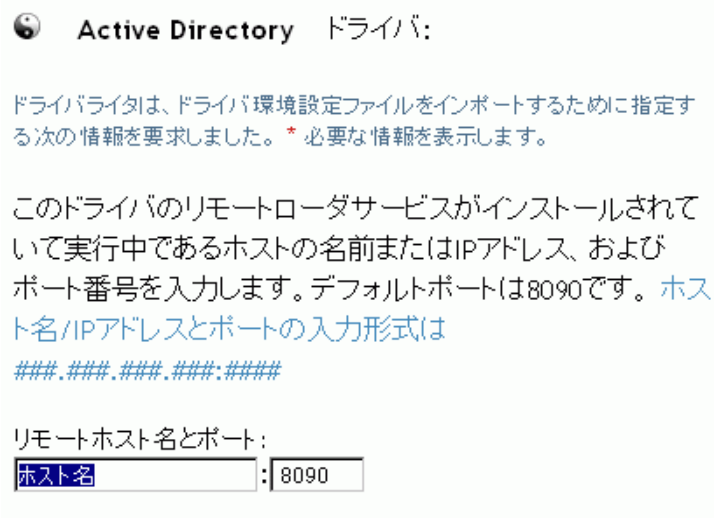
- 65 ページのセクション 3.4.1「新しいドライバのインポートおよび設定」
- 67 ページのセクション 3.4.2「既存のドライバの設定」
- 68 ページのセクション 3.4.3「キーストアの作成」

3.4.1 新しいドライバのインポートおよび設定

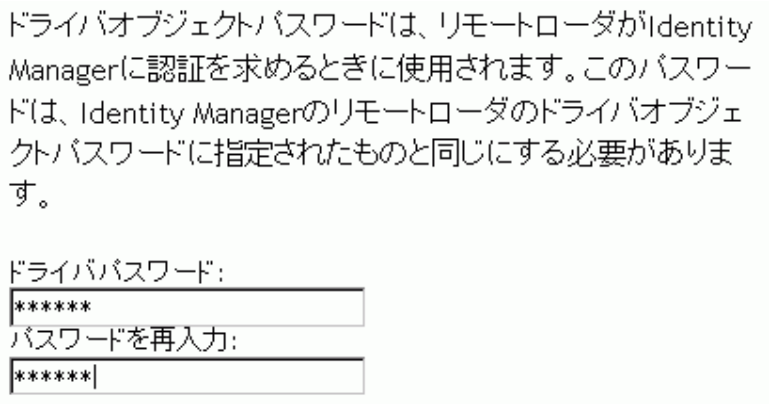
1. Novell iManager で、新しいドライバをインポートまたは作成して設定します。
2. 環境設定オプションの下部までスクロールして、ドロップダウンリストから［リモート］を選択し、［次へ］をクリックします。



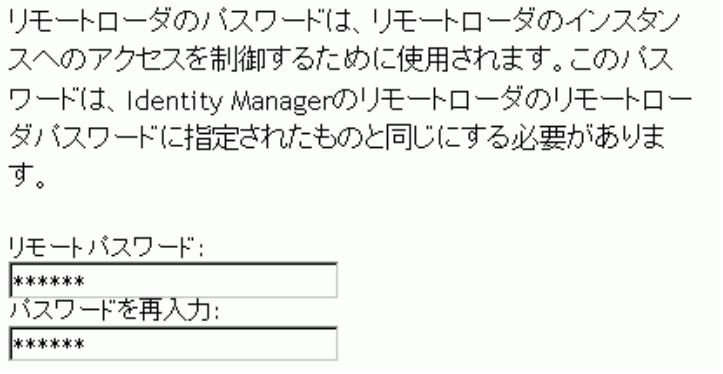
3 リモートのホスト名およびポートを入力します。



4 ドライバオブジェクトのパスワードを入力して再入力します。



5 リモートローダのパスワードを入力して再入力し、［次へ］をクリックします。



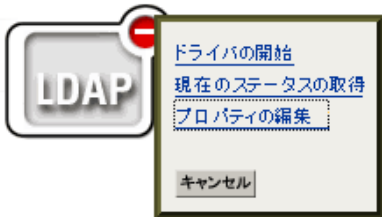
6 セキュリティが同等なユーザを定義し、［次へ］をクリックし、［終了］をクリックします。

3.4.2 既存のドライバの設定

リモートローダに接続するための、ドライバオブジェクトのパラメータを指定します。

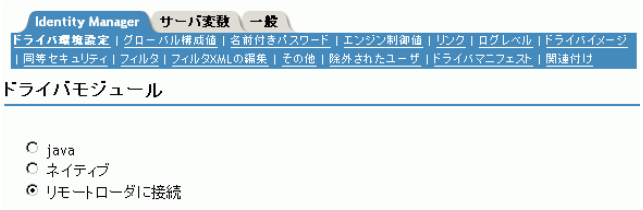
1 Novell iManager で、［Identity Manager］>［Identity Manager の概要］の順にクリックします。

2 変更するドライバを参照して選択します。

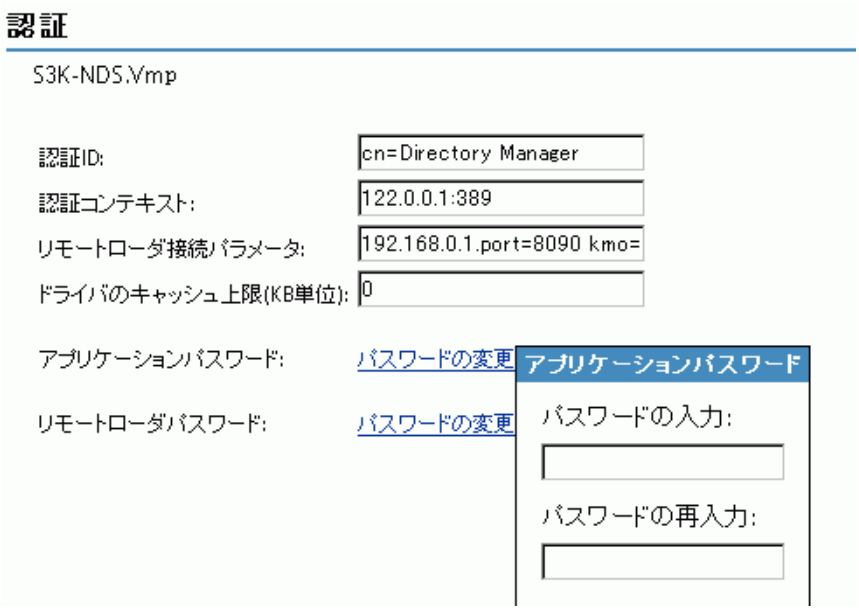


3 ドライバのステータスアイコンをクリックし、［プロパティの編集］をクリックします。

4 ［ドライバモジュール］セクションで、［リモートローダに接続］を選択します。



5 ［認証］セクションで、リモートローダのパラメータを入力します。



- リモートローダ接続パラメータ

以前は、自己署名証明書をエクスポートしていました (46 ページのセクション 3.2.2「自己署名証明書のエクスポート」を参照)。SSL では、自己署名証明書のニックネームが必要です。

［リモートローダ接続パラメータ］編集ボックスで、鍵と値のペアのパラメータを入力します。たとえば、次のように入力します。

```
hostname=192.168.0.1 port=8090 kmo=remotecert
hostname=192.168.0.1 port=8090 kmo='remote cert'
```

- hostname

  ホスト名または IP アドレス (190.162.0.1 など)。リモートローダを実行しているコンピュータのアドレスまたは名前を指定します。IP アドレスまたはサーバ名を指定しない場合、この値がローカルホストのデフォルトになります。

- port

  リモートローダが、リモートインタフェースシムからの接続を受け入れる場所です。この通信パラメータを指定しない場合、値はデフォルトで 8090 に設定されます。

- kmo

  SSL に使用する鍵と証明書を含む暗号化キーオブジェクト (KMO) のキー名 (kmo=remotecert など) を指定します。

  証明書の名前にスペースを使用した場合は、KMO オブジェクトのニックネームを一重引用符で囲む必要があります。

  ヒント : KMO オブジェクト名は、46 ページのセクション 3.2.1「サーバ証明書の作成」のステップ 2 で指定したニックネーム値です。

- アプリケーションのパスワードを入力

  アプリケーションユーザ ID のパスワードを指定します。通常はドライバがアプリケーションに接続するために、ドライバシムはこのパスワードを必要とします。

- リモートローダパスワードの入力

  リモートローダのパスワードを指定します。リモートインタフェースシムは、このパスワードを使用してリモートローダに対して自身を認証します。

  注 : アプリケーションのパスワードとリモートローダのパスワードは、両方を同時に設定するか、または両方を同時にリセットしてください。

  ---

6 ［OK］をクリックします。

3.4.3 キーストアの作成

キーストアは、暗号化キーおよび証明書 (オプション) を含む Java ファイルです。リモートローダとメタディレクトリエンジンの間で SSL を使用する必要があり、Java シムを使用する場合は、キーストアファイルを作成する必要があります。

- 69 ページの 「Windows でのキーストア」
- 69 ページの 「Solaris、Linux、または AIX でのキーストア」

- 69 ページの 「すべてのプラットフォームでのキーストア」

Windows でのキーストア

Windows で Keytool ユーティリティを実行します。これは通常、c:\novell\remoteloader\jre\bin ディレクトリにあります。

Solaris、Linux、または AIX でのキーストア

Solaris、Linux、または AIX の環境では、create_keystore ファイルを使用します。create_keystore は rdxml とともにインストールされます。また、\dirxml\java_remoteloader ディレクトリにある dirxml_jremote.tar.gz ファイルにも含まれています。create_keystore ファイルは、Keytool ユーティリティを呼び出すシェルスクリプトです。

UNIX では、自己署名証明書を使用してキーストアが作成されると、Base64 またはバイナリの .der 形式で証明書をエクスポートできます。

コマンドラインで次を入力します。

create_keystore *self-signed_certificate_name keystorename*

たとえば、次のいずれかを入力します。

```
create_keystore tree-root.b64 mystore create_keystore tree-root.der
mystore
```

create_keystore スクリプトにより、キーストアパスワード用にハードコードされている “dirxml” のパスワードが指定されます。キーストアにはパブリック証明書と公開鍵のみが保存されるため、セキュリティリスクはありません。

すべてのプラットフォームでのキーストア

任意のプラットフォームでキーストアを作成するには、コマンドラインで次を入力します。

keytool -import -alias trustedroot -file *self-signed_certificate_name* -keystore *filename* -storepass

filename には、どのような名前でも指定できます (rdev_keystore など)。

ポリシーの作成

4

ポリシーにより、アイデンティティボールトに対する情報フローを特定の環境に合わせてカスタマイズできます。

たとえば、ある会社ではメインのユーザクラスとして inetorgperson を使用していて、別の会社では User を使用しているとします。これを処理するために、各システムで呼び出すユーザをメタディレクトリエンジンに指示するポリシーが作成されています。接続システム間でユーザに影響する操作をやり取りする場合、Identity Manager は、この変更を行うポリシーを適用します。

また、ポリシーは、新しいオブジェクトの作成、属性値の更新、スキーマ変換の実行、一致条件の定義、Identity Manager の関連付けの維持など、多くのタスクを実行します。

ポリシーに関する詳しいガイドは、『*Policy Builder and Driver Customization Guide*』に含まれています。このガイドの内容は次のとおりです。

- 使用可能な各ポリシーの詳細な説明
- 各条件、アクション、名詞、および動詞のサンプルと構文を含む、ポリシービルダの詳細なユーザガイドとリファレンス
- XSLT スタイルシートを使用したポリシー作成の説明

ポリシーの詳細については『*Policy Builder and Driver Customization Guide*』を参照してください。

接続システム間のパスワード同期 5

5.1 概要

Identity Manager では、パスワードの発行と購読に対するユニバーサルパスワードと接続システムのサポートを利用することによって、双方向パスワード同期が提供されています。

ユーザアカウントのその他の属性と同様に、信頼されたデータソースを選択できます。

5.1.1 パスワードの概要

NDS® パスワード、単純パスワード、配布パスワード、およびユニバーサルパスワードは、異なる目的のために使用されます。eDirectory™ と Identity Manager の以前のバージョンでは、接続システムで更新できるのは NDS パスワードのみで、これは片方向同期でした。

Identity Manager ではユニバーサルパスワードが使用されています。これは、他のアイデンティティボールトのパスワードと同期できる、逆方向の同期が可能なパスワードです。ユニバーサルパスワードは eDirectory 8.7.1 で導入され、3 つの層の暗号化によって保護されています。

NMAS™ は、ユニバーサルパスワードと他のアイデンティティボールトのパスワードの関係を制御します。たとえば、NMAS は、ユニバーサルパスワードと NDS パスワード、単純パスワード、または配布パスワードの同期を保つかどうかを制御します。NMAS は、パスワードを変更しようとする着信要求を受信し、NMAS のパスワードポリシーの設定に従って処理します。

Identity Manager は、アイデンティティボールトパスワードと接続システムのパスワード間の関係を制御します。このために、Identity Manager は配布パスワードを使用します。配布パスワードは、接続システムに提供できるアイデンティティボールトのパスワードです。ユニバーサルパスワードのように、配布パスワードも 3 つの暗号化層で保護されていて、逆方向で同期できます。

NMAS のパスワードポリシーでは、配布パスワードをユニバーサルパスワードと同じにするかどうかを指定できます (設定は、［ユニバーサルパスワードの設定時に配布パスワードを同期する］です)。配布パスワードがユニバーサルパスワードと同じで、接続システムの双方向パスワード同期を使用する場合は、Identity Manager を使用して eDirectory からユニバーサルパスワードを抽出して、その他の接続システムに送信するということに留意してください。パスワードの転送、およびパスワードを保存する接続システムをセキュリティで保護する必要があります 201 ページの第 7 章「セキュリティ : ベストプラクティス」を参照してください。

配布パスワードがユニバーサルパスワードと同じではない場合 (NMAS パスワードポリシーで設定を無効にしているため)、ユニバーサルパスワードまたは NDS パスワードを使用せずに、またはこれらに影響せずに、配布パスワードを使用した接続システム間でパスワードを「トンネル」することができます。トンネルは、接続システム間のみでパスワードを同期します。有効になっている場合、トンネルではアイデンティティボールト / ユニバーサルパスワードは設定されません。

さまざまな eDirectory パスワードの詳細については、『*Novell Modular Authentication Services (NMAS) 2.3 Administration Guide* (http://www.novell.com/documentation/nmas23/index.html)』を参照してください。Identity Manager でパスワード同期を使用する方法については、109 ページのセクション 5.8「パスワード同期の実装」を参照してください。

5.1.2 双方向パスワード同期とは

双方向パスワード同期は、指定した接続システムからパスワードを受け入れる機能および、指定した接続にパスワードを配布する Identity Manager 機能の組み合わせです。

特定の接続システムと双方向でパスワードを同期できるかどうかは、接続システムが何をサポートしているかによって決まります。

接続システムの中には、Identity Manager から修正された新しいパスワードを受け入れ、ユーザの実際のパスワードを Identity Manager に提供できるものもあります。これらの接続システムは、Identity Manager との双方向パスワード同期をサポートしているシステムです。

- Active Directory
- Novell® eDirectory™
- Network Information Services (NIS)
- NT ドメイン

これらの接続システムでは、ユーザは、いずれかのシステムでパスワードを変更して、Identity Manager を介してそのパスワードを他のシステムと同期できます。ただし、

NMAS パスワードポリシーで高度なパスワードルールを使用している場合、ユーザが iManager セルフサービスコンソールでパスワードを変更できるようにすることをお勧めします。このコンソールにはユーザのパスワードが準拠しなければならないすべてのルールが表示されるため、パスワード変更には最適な場所です。

その他の接続システムはユーザの実際のパスワードを提供できないため、完全な双方向パスワード同期をサポートできません。ただし、ドライバ環境設定内にポリシーを定義することによって、これらのシステムは、パスワードを作成するために使用できるデータを提供し、Identity Manager に送信できます。

他のシステムの中には、新しいユーザの初期パスワードの設定またはパスワードの変更、あるいはその両方を含め、Identity Manager からパスワードを受け入れることができるものもあります。83 ページのセクション 5.2「パスワード同期をサポートする接続システム」を参照してください。

5.1.3 Password Synchronization 1.0 と Identity Manager のパスワード同期の比較

表 5-1 比較 : *Password Synchronization 1.0* と *Identity Manager* のパスワード同期

	Password Synchronization 1.0	Identity Manager 2 および 3 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、別個には販売されていません。
プラットフォーム	◆ Active Directory ◆ NT ドメイン ◆ eDirectory	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。 83 ページのセクション 5.2「パスワード同期をサポートする接続システム」を参照してください。
アイデンティティボールトで使用されているパスワード	NDS 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 NDS 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、109 ページのセクション 5.8「パスワード同期の実装」を参照してください。

	Password Synchronization 1.0	Identity Manager 2 および 3 のパスワード同期
Windows 接続システムの主な機能	アイデンティティボールトパスワードが Windows パスワードと同期されるようにパスワードを Identity Manager に送信する場合。NDS パスワードは逆方向に同期できないため、パスワードは NT または AD に戻されていませんでした。	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。
LDAP 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。
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 Identity Manager ポリシーがパスワード同期機能を提供します。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。100 ページのセクション 5.7「パスワード同期をサポートするための、既存のドライバ環境設定のアップグレード」を参照してください。
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。

5.1.4 Identity Manager のパスワード同期の機能

Identity Manager のパスワード同期は双方向です。パスワードは、接続システムから送信されて Identity Manager で受け入れたり、Identity Manager から配布されて接続システムで受け入れたりできます。

- 76 ページの 「接続システムからのパスワードの受け入れ」
- 77 ページの 「接続システムへのパスワードの配布」
- 77 ページの 「データストアおよび接続システムでのパスワードポリシーの適用」
- 78 ページの 「パスワード同期のシナリオ」
- 79 ページの 「ユーザへのパスワード同期失敗の通知」
- 79 ページの 「ユーザのパスワード同期ステータスの確認」

接続システムからのパスワードの受け入れ

DirXML® および Identity Manager の以前のバージョンと同様に、接続システムはアイデンティティボールトにパスワードを発行できます。

Identity Manager がパスワードを受け入れる元の接続システムアプリケーションを指定できます。さらに、Identity Manager が実行されている同じアイデンティティボールト内でユーザのパスワードを更新するか、または Identity Manager が接続システム間のみでパス

ワードを同期する単なる管路または「トンネル」として動作するかどうかも選択できます。つまり、アイデンティティボールトのパスワードを、Identity Manager が接続システムに配布するパスワードと別にすることができます。

一部の接続システム (AD、その他のアイデンティティボールト、NT、および NIS) は、ユーザの実際のパスワードを提供できます。つまり、ユーザが接続システムでパスワードを変更した場合に、その変更を Identity Manager と同期して、その他の接続システムに戻すことができます。

その他の接続システムはユーザの実際のパスワードの提供をサポートしていませんが、名字または従業員 ID に基づいた初期パスワードなど、スタイルシートで生成したパスワードを Identity Manager に提供するように設定できます。

接続システムへのパスワードの配布

Identity Manager のパスワード同期は、共通のパスワードを各接続システムに配布できます。

Identity Manager の以前のバージョンでは、ドライバは接続システム上のユーザアカウントから Identity Manager にパスワードを送信でき、パスワードを使用して eDirectory 内の対応するユーザを更新できました。しかし、eDirectory 内の NDS パスワードは、逆方向に同期できないため、中央の Identity Manager のアイデンティティボールトから複数の接続システムにパスワードを送ることはできませんでした。eDirectory パスワードを取得するには、パスワードが eDirectory に保存される前に、Novell Client などを介して取得する以外に方法はありませんでした。

eDirectory 8.7.3 によって提供されるユニバーサルパスワードは、逆方向の同期が可能で、配布可能です。

Identity Manager は、接続システムからパスワードを受け入れることができます。ユニバーサルパスワードは逆方向の同期が可能であるため、Identity Manager はアイデンティティボールトから、新しいアカウントの初期パスワードの設定やパスワードの変更をサポートする接続システムにパスワードを配布できます。

パスワードの発行元に関係なく、Identity Manager は、接続システムにパスワードを配布する場所であるリポジトリとして配布パスワードを使用します。ユニバーサルパスワードと同様に、配布パスワードでも、パスワードポリシーを適用できます。

パスワードの同期時にユニバーサルパスワードと配布パスワードを使用する方法については、109 ページの 「パスワード同期の実装」を参照してください。

ユーザの他の属性と同様に、どのシステムが信頼されたパスワードのソースなのかを決定できます。Identity Manager は、信頼されたソースから他の接続システムにパスワードを配布します。

双方向パスワード同期は、これをサポートする接続システム間に設定できます。

データストアおよび接続システムでのパスワードポリシーの適用

Identity Manager では、NMAS を呼び出すことによって、着信パスワードにパスワードポリシーを適用できます。接続システムから Identity Manager に発行されるパスワードがポリシーに準拠していない場合は、Identity Manager がそのアイデンティティボールトへのパスワードを受け入れないように指定できます。つまり、ポリシーに準拠しないパスワードはその他の接続システムに配布されません。

さらに、Identity Manager では、接続システムにパスワードポリシーを適用することもできます。Identity Manager に対して発行されたパスワードがポリシーのルールに準拠していない場合、Identity Manager はパスワードを受け入れて配布しないだけでなく、アイデンティティボールト名の現在の配布パスワードを使用して接続システム上の準拠しないパスワードをリセットするように指定できます。

たとえば、パスワードに少なくとも 1 つの数字を含める必要があるとします。しかし、接続システム自体にはそのようなポリシーを適用する機能がありません。接続システムから送られてきて、ポリシーのルールに準拠していないパスワードを Identity Manager でリセットするように指定します。

高度なパスワードルールと Identity Manager のパスワード同期を使用している場合、すべての接続システムのパスワードポリシーを調査して、eDirectory パスワードポリシーの高度なパスワードルールと互換性があることを確認することをお勧めします。この調査は、パスワードを正常に同期するために役立ちます。

NMAS パスワードポリシーが割り当てられているユーザが、接続システムのパスワード同期に参加させるユーザと一致していることを確認する必要があります。

NMAS のパスワードポリシーはツリー中心で割り当てられます。一方、パスワード同期はドライバごとに設定されます。また、ドライバは各サーバにインストールされ、マスタレプリカまたは読み書き可能レプリカ内のユーザのみが管理できます。パスワード同期により期待される結果を取得するには、パスワード同期のドライバを実行するサーバにあるマスタレプリカまたは読み書き可能レプリカのコンテナが、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割り当てたコンテナと一致するようにします。パーティションルートコンテナにパスワードポリシーを割り当てることによって、そのコンテナとサブコンテナ内のすべてのユーザに確実にパスワードポリシーが割り当てられます。

NMAS のパスワードポリシーをユーザに割り当てる方法の詳細については、『*Password Management Administration Guide* (http://www.novell.com/documentation/password_management/index.html)』の「Assigning Password Policies to Users」を参照してください。

パスワード同期のシナリオ

Identity Manager を使用すると、どのシステムが信頼されたパスワードのソースであるかを指定できます。また、管理者はパスワード受け入れの流れも決定します。

Identity Manager のパスワード同期の機能のほとんどは、アイデンティティボールトが提供する、逆方向に同期できるパスワード機能であるユニバーサルパスワードに依存します。しかし、ユニバーサルパスワードを展開する必要がない場合もあります。

Identity Manager のパスワード同期は、配布パスワードにも依存します。ユニバーサルパスワードと同様に、ポリシーを配布パスワードに適用できます。

パスワード同期を実装する基本的な方法については、109 ページの 「パスワード同期の実装」を参照してください。これらのシナリオを組み合わせて、各環境のニーズを満たすことができます。

Novell Client を使用しない Windows でのパスワードの同期

Active Directory および NT ドメインとのパスワード同期に、Novell Client は必要なくなりました。

ユーザへのパスワード同期失敗の通知

「データストアおよび接続システムでのパスワードポリシーの適用」では、Identity Manager はポリシーに準拠しないパスワードを (接続システムから) 受け入れないことによってパスワードポリシーを適用できることを説明しています。

電子メール通知機能を使用すると、ユーザが行ったパスワード変更が成功しなかった場合に、Identity Manager から通知するように指定できます。

シナリオ : NT ドメインからの着信パスワードがパスワードポリシーに準拠しない場合、受け入れないように Identity Manager を設定しました。電子メール通知機能を有効にしました。NMAS のパスワードポリシーの 1 つのルールで、会社名をパスワードとして使用できないよう指定されています。ユーザは、NT ドメインの接続システム上でパスワードを会社名に変更します。NMAS はパスワードを受け入れず、Identity Manager からユーザに、パスワードの変更が同期されなかったことを知らせる電子メールメッセージが送信されます。

この機能を使用するには、電子メールサーバとテンプレートを設定する必要があります。次をカスタマイズできます。

- Identity Manager が送信するメッセージのテキスト
- コピーを管理者に送信する通知

詳細については、147 ページの 「電子メール通知の設定」を参照してください。

ユーザのパスワード同期ステータスの確認

Identity Manager を使用すると、接続システムに問い合わせて、ユーザのパスワード同期のステータスを確認できます。接続システムがパスワードの確認機能をサポートしている場合、パスワードが正常に同期されているかどうかを確認できます。

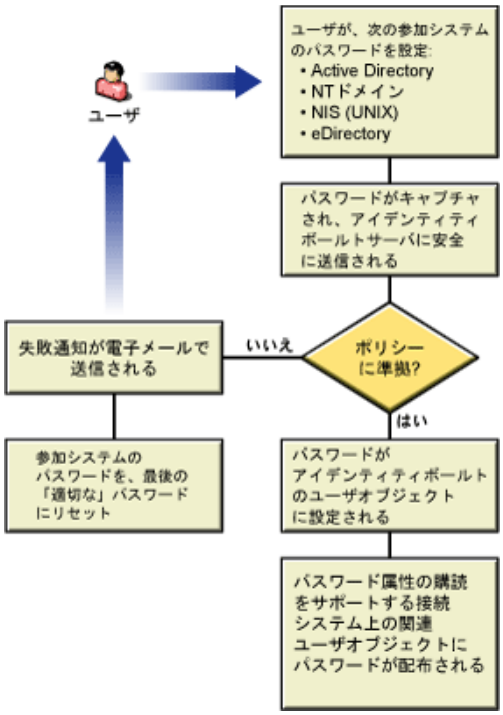
パスワードを確認する方法の詳細については、146 ページの 「ユーザのパスワード同期ステータスの確認」を参照してください。

パスワードの確認をサポートしているシステムのリストについては、83 ページの 「パスワード同期をサポートする接続システム」を参照してください。

5.1.5 パスワード同期のフローの概要

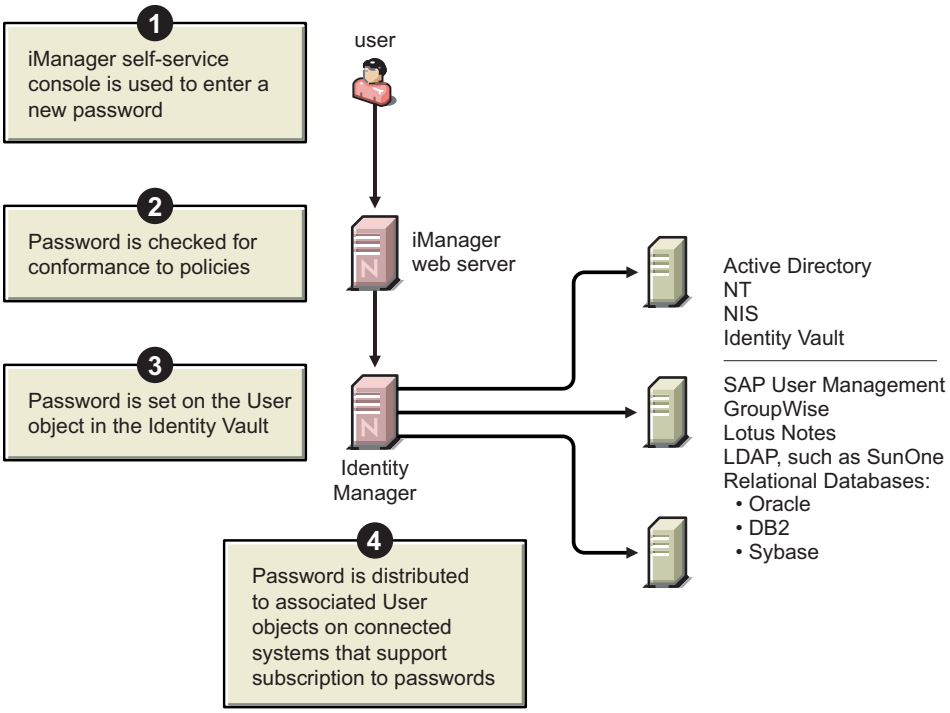
次の図は、接続システムが Identity Manager にパスワードを発行する方法を示しています。

図 *5-1* 接続システムが *Identity Manager* にパスワードを発行する方法



次の図は、Identity Manager が接続システムにパスワードを配布する方法を示しています。

図 5-2 *Identity Manager* が接続システムにパスワードを配布する方法

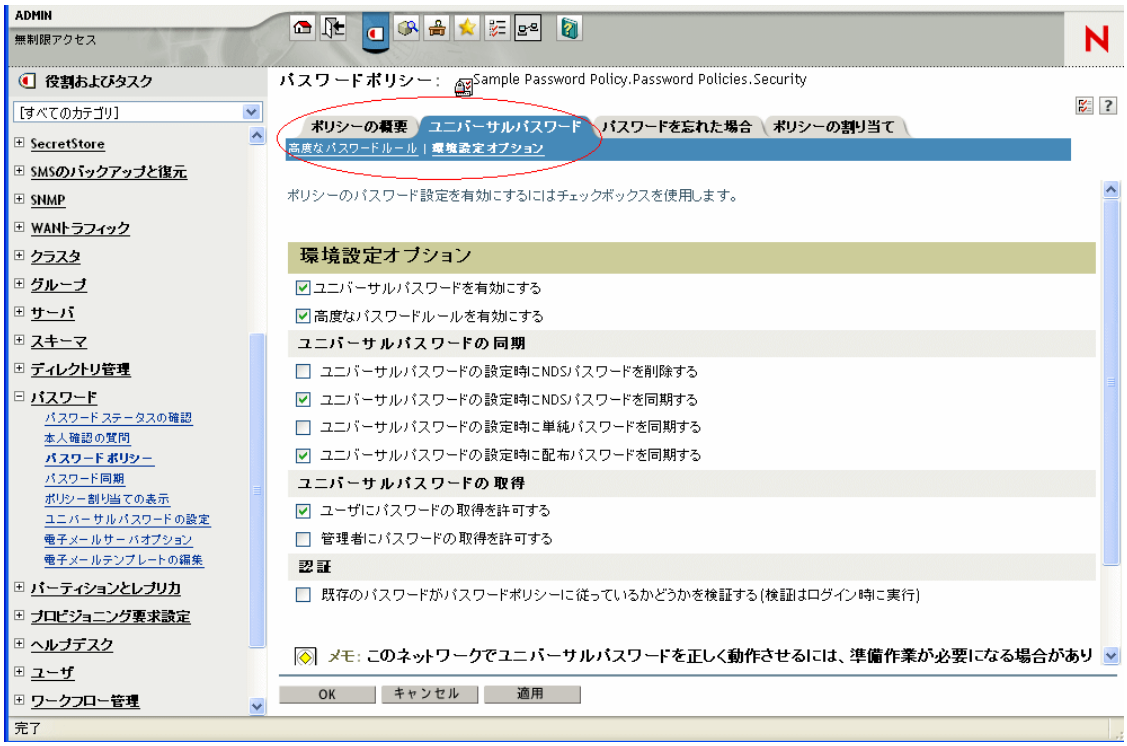


5.1.6 図を表示する方法

このドキュメントでは、iManager でのオプションを説明するために、手順で頻繁に図を使用します。オプションが実際にデスクトップ上にどのように表示されるかは、ブラウザに依存します。

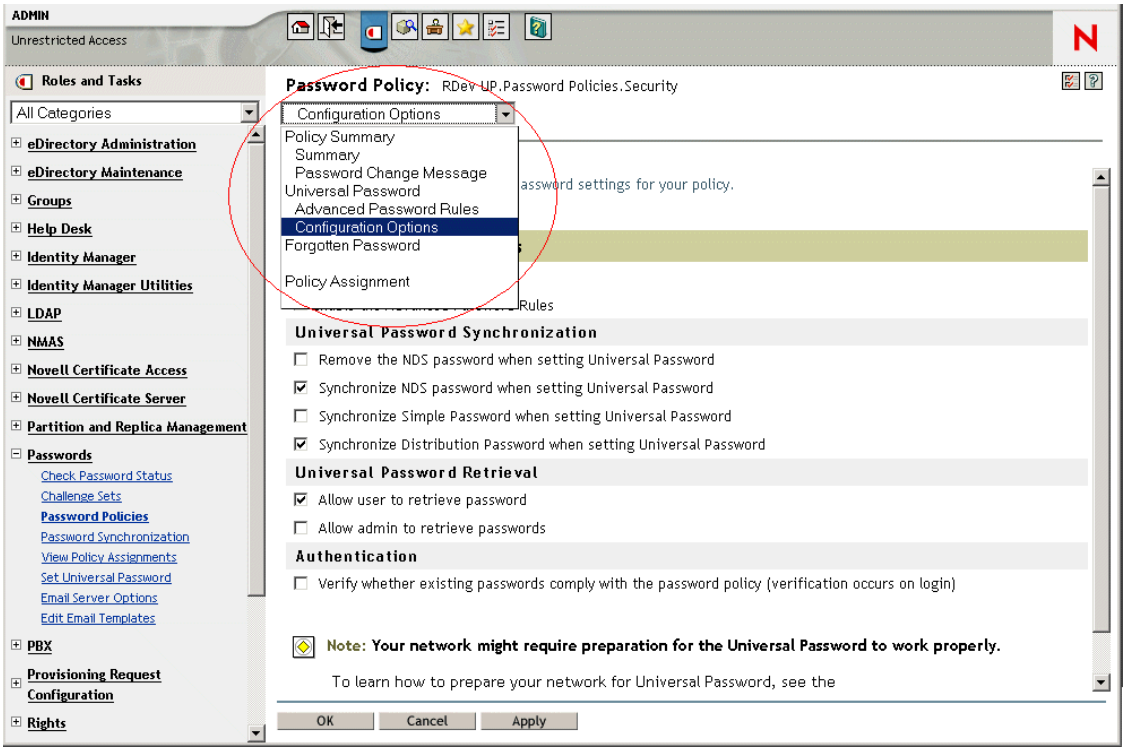
たとえば、Internet Explorer では、iManager のオプションがタブを使用して表示されます。

図 *5-3* *iManager のタブ*



しかし、Firefox ブラウザでは、iManager のオプションはドロップダウンリストを使用して表示されます。

図 5-4 *iManager のドロップダウンリスト*



このドキュメントでは、Firefox ブラウザでの表示に従って図を示しています。

5.2 パスワード同期をサポートする接続システム

ユーザオブジェクトが作成されると、Identity Manager は常に接続システムからパスワードを受け入れることができます。これは、接続システムがユーザの実際のパスワードをそのシステムから提供できない場合でも同じです。

AD、NT、eDirectory、および NIS は Identity Manager からパスワードを受け入れて、ユーザの実際のパスワードを Identity Manager に送信することもできます。つまり、これらのシステムは双方向パスワード同期を完全にサポートしています。

発行者チャネルのドライバ環境設定内でポリシーを定義すると、パスワードを作成するために使用できるデータを他のシステムが提供できます。大部分のドライバのドライバ環境設定例には、名字に基づいてデフォルトのパスワードを提供するポリシー例が含まれています。

接続システムは、Identity Manager からのパスワードを受け入れる各種機能を備えています。一部の接続システムは、新しいアカウントに設定されている初期パスワードの設定をサポートしますが、パスワード変更イベントはサポートしません。

サンプルドライバ環境設定の機能は、ドライバマニフェストに記載されています。以降の表は、ドライバマニフェストにない追加情報を示しています。この表は、新しいアカウントに設定されている初期パスワードをアプリケーションが受け入れるかどうかと、既存のパスワードへの変更を受け入れるかどうかを示しています。マニフェストでは、接続シス

テムがパスワードを受け入れられることだけが示されており、この違いについては示されていません。

類似した機能を持つサンプルドライバ環境設定を参照できるように、ドライバはグループ化されています。

5.2.1 双方向のパスワード同期をサポートするシステム

次の接続システムでは、双方向のパスワード同期がサポートされています。これらは、接続システム上のユーザの実際のパスワードを提供し、Identity Manager からパスワードを受け入れることができます。

表 5-2 双方向のパスワード同期をサポートするシステム

接続システムのドライバ	購読者チャネル アプリケーションが初期パスワードの設定を受け入れることができる	購読者チャネル アプリケーションがパスワードの変更を受け入れることができる	購読者チャネル アプリケーションがパスワードの確認をサポートしている	発行者チャネル アプリケーションがパスワードを提供 (同期) できる
Active Directory	○	○	○	○
eDirectory[1]	○	○	○	○
NT ドメイン	○	○	×	○
NIS	○	○	○	○
SIF	○	○	×	○

[1] アイデンティティボールトツリー間では、ユニバーサルパスワードがユーザに対して有効化されていない場合でも、ユーザに双方向パスワード同期を提供できます。111 ページのセクション 5.8.2「シナリオ 1: NDS パスワードを使用した、2 つのアイデンティティボールト間の同期」を参照してください。

5.2.2 Identity Manager のパスワードを受け入れるシステム

次の接続システムは、Identity Manager からある程度までパスワードを受け入れることができます。これらは、接続システム上のユーザの実際のパスワードを Identity Manager には提供できません。

ユーザの実際のパスワードは提供できませんが、接続システム上の他のユーザデータに基づいて、発行者チャネル上のポリシーを使用してパスワードを作成するように設定できます (サンプルのドライバ環境設定には、名字に基づいたデフォルトのパスワードが示されています)。

表 *5-3* *Identity Manager* のパスワードを受け入れるシステム

接続システムのドライバ	購読者チャネル アプリケーションが初期パスワードの設定を受け入れることができる	購読者チャネル アプリケーションがパスワードの変更を受け入れることができる	購読者チャネル アプリケーションがパスワードの確認をサポートしている	発行者チャネル アプリケーションがパスワードを提供 (同期) できる
Groupwise®	○	○	×	×[2]
JDBC	○[3]	×4	×	×[5]
LDAP	○[6]	○[6]	○	×
Notes	○	○[7]	○[7]	×
SAP User Management	○	○	×	×

[2]GroupWise は 2 つの認証方法をサポートします。

- 独自の認証を提供し、ユーザパスワードを維持します。
- LDAP を使用して eDirectory に対して認証し、パスワードは維持しません。

  このオプションを使用する場合、GroupWise はドライバによって同期されたパスワードを無視します。

[3] 初期パスワードを設定する機能は、Oracle*、MS SQL、MySQL*、Sybase* など、OS ユーザアカウントがデータベースのユーザアカウントと異なるすべてのデータベースで利用できます。

[4]JDBC の Identity Manager ドライバを使用して接続システム上でパスワードを変更できますが、サンプルのドライバ環境設定には示されていません。

[5] パスワードをテーブルに格納する際にデータとして同期できます。

[6] 対象となる LDAP サーバで userpassword 属性を設定できる場合。

[7]Notes ドライバはパスワードの変更を受け入れて、Lotus Notes の HTTPPassword フィールドのパスワードのみを確認できます。

5.2.3 パスワードを受け入れまたは提供しないシステム

次の接続システムはパスワードを受け入れることができません。また、接続システムでサンプルのドライバ環境設定を使用して、ユーザのパスワードを提供することもできません。

ユーザのパスワードを Identity Manager に提供することはできませんが、接続システム上の他のユーザデータに基づいて、発行者チャネル上のポリシーを使用してパスワードを作成するように設定できます (サンプルのドライバ環境設定には、名字に基づいたデフォルトのパスワードが示されています)。

表 *5-4* パスワードを受け入れまたは提供しないシステム

接続システムのドライバ	購読者チャネル アプリケーションが初期パスワードの設定を受け入れることができる	購読者チャネル アプリケーションがパスワードの変更を受け入れることができる	購読者チャネル アプリケーションがパスワードの確認をサポートしている	発行者チャネル アプリケーションがパスワードを提供 (同期) できる
区切りテキスト	×[8]	×[8]	×[8]	×[8]
Exchange 5.5	×	×	×	×
PeopleSoft 3.6	×	×	×	×
PeopleSoft 4.0	×	×	×	×
SAP HR	×	×	×	×

[8] 区切りテキスト用の Identity Manager ドライバには、パスワード同期を直接サポートするドライバシムの機能がありません。ただし、このドライバは、同期先の接続システムによってはパスワードを処理するように設定できます。

5.2.4 パスワード同期をサポートしないシステム

次の接続システムは、パスワード同期での使用には適していません。

表 *5-5* パスワード同期をサポートしないシステム

接続システムのドライバ	購読者チャネル アプリケーションが初期パスワードの設定を受け入れることができる	購読者チャネル アプリケーションがパスワードの変更を受け入れることができる	購読者チャネル アプリケーションがパスワードの確認をサポートしている	発行者チャネル アプリケーションがパスワードを提供 (同期) できる
Avaya* PBX	×	×	×	×
エンタイトルメントサービスドライバ	×	×	×	×
ループバックサービスドライバ	×	×	×	×
手動タスクサービスドライバ	×	×	×	×

5.3 パスワード同期の前提条件

パスワード同期は、次の要素に依存します。

- 87 ページの 「ユニバーサルパスワードのサポート」
- 87 ページの 「ドライバマニフェストで宣言されているパスワード同期機能」
- 87 ページの 「グローバル構成値を使用したパスワード同期の制御」
- 90 ページの 「ドライバ環境設定で必要なポリシー」

- 94 ページの 「パスワード取得のために接続システムにインストールするフィルタ」
- 94 ページの 「ユーザ用に作成した NMAS パスワードポリシー」
- 94 ページの 「NMAS ログインメソッド」

5.3.1 ユニバーサルパスワードのサポート

接続システム間でのパスワード同期に対応するには、Identity Manager でユニバーサルパスワードを使用する必要があります。次を参照してください。

- 『*Password Management Administration Guide* (http://www.novell.com/documentation/password_management/index.html)』の「Deploying Universal Password」
- 96 ページのセクション 5.4.3「ユニバーサルパスワードを使用するための準備作業」

5.3.2 ドライバマニフェストで宣言されているパスワード同期機能

ドライバマニフェストは、接続システムが次のパスワード同期機能をサポートするかどうかを宣言します。

- ユーザの実際のパスワードを Identity Manager に発行する
- Identity Manager のパスワードを受け入れる

  マニフェストでは、初期パスワードの作成の受け入れとパスワード変更の受け入れは区別されません。
- Identity Manager で接続システム上のパスワードを確認し、ユーザのパスワード同期ステータスを決定する

注 : ドライバマニフェストは、ドライバの開発者、またはドライバ環境設定を作成する Identity Manager のエキスパートによって記述されます。ネットワーク管理者が編集するためのものではありません。ドライバマニフェストは、ドライバシムおよび環境設定の実際の機能を表します。マニフェストのみを変更しても機能は変更されません。機能を追加するには、ドライバシム、接続システム、またはドライバ環境設定を拡張する必要があります。

Identity Manager に付属するサンプルのドライバ環境設定はドライバマニフェストエントリを含みます。既存のドライバにこれらを追加するには、100 ページのセクション 5.7「パスワード同期をサポートするための、既存のドライバ環境設定のアップグレード」を参照してください。

5.3.3 グローバル構成値を使用したパスワード同期の制御

グローバル構成値を使用すると、ポリシーで参照できる定数値を設定できます。グローバル構成値はレプリカごとの属性に保持されるため、サーバ変数と呼ばれることもあります。

パスワード同期では、グローバル構成値を使用して Identity Manager に対するパスワードフローの設定を作成できます。ドライバ環境設定内の Identity Manager のパスワード同期ポリシーはグローバル構成値の設定に基づいて動作するように記述されるため、ポリシーを編集せずにパスワードフローを簡単に変更できます。

グローバル構成値を使用して、各接続システムの次の設定を制御できます。

表 *5-6* 接続システムの設定

設定	説明
接続システムから Identity Manager がパスワードを受け入れるかどうか	この設定は、接続システムによって提供されるパスワード、および発行者チャネルのドライバ環境設定内の Identity Manager ポリシーによって作成できるパスワードに適用できます。この設定を無効にすると、両方のタイプのパスワードが除去されるため、パスワードは Identity Manager に到達しません。
Identity Manager が、ユニバーサルパスワードを直接更新する同期方法と、配布パスワードを直接更新する同期方法のどちらを使用するか	Identity Manager はエントリポイント (Identity Manager が更新するパスワード) を制御します。NMAS は、NMAS パスワードポリシーで設定した内容に基づいて各種パスワード間のパスワードのフローを制御します。NMAS パスワードポリシーを表示するには、次のように操作します。 1. iManager で、［パスワード］>［パスワードポリシー］の順に選択します。 2. ［パスワードポリシーリスト］でポリシーを選択します。 3. ［編集］をクリックします。 4. ドロップダウンリストまたはタブからオプションを選択します (使用している iManager のバージョンによります)。 これらの方法を使用するシナリオについては、第 5.8 節「パスワード同期の実装」を参照してください。
接続システムから Identity Manager への着信パスワードに NMAS パスワードポリシーを適用するかどうか	これらのポリシーが適用された場合、準拠しない着信パスワードは Identity Manager のデータストアに書き込まれません。
接続システム上の NMAS パスワードポリシーを適用するために、ポリシールールに準拠しないパスワードをリセットして、Identity Manager が Identity Manager のパスワードを使用するかどうか	このオプションは、接続システムがサポートしない場合は NMAS インタフェース内で淡色表示されます (サポートしているかどうかはドライバマニフェストで宣言されています)。発行者チャネル上でパスワード操作が失敗した後にのみ、パスワードがリセットされます。
接続システムがパスワードを受け入れるかどうか	この設定は Identity Manager によって配布されるパスワードと、購読者チャネルのドライバ環境設定内の Identity Manager ポリシーによって作成できるパスワードの両方に適用されます。この設定を無効にすると、両方のタイプのパスワードが除去されるため、パスワードは接続システムに到達しません。 このオプションは、接続システムがサポートしない場合はインタフェース内で淡色表示されます (サポートしているかどうかはドライバマニフェストで宣言されています)。
パスワードが同期化されなかった場合に、ユーザに電子メールで通知するかどうか	影響を受けるユーザに電子メールを自動的に送信します。

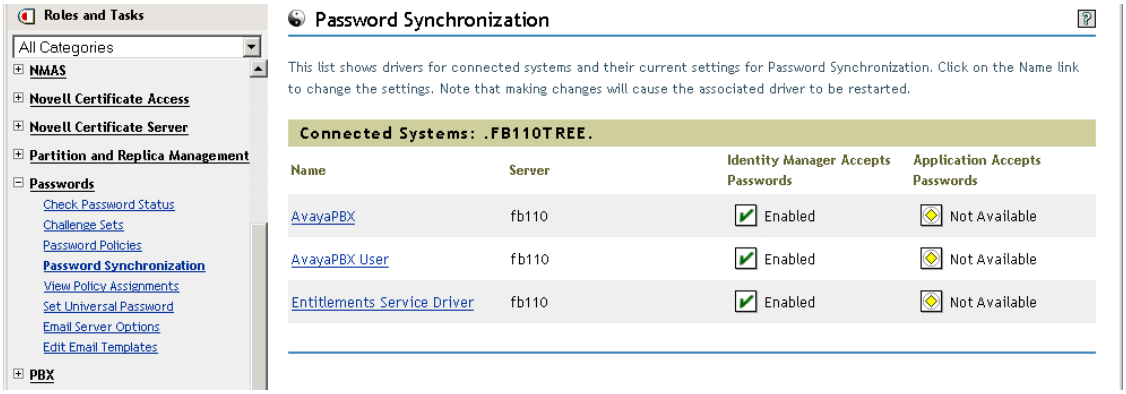
Identity Manager に付属するドライバ環境設定はドライバマニフェストエントリを含みます。既存のドライバにこれらを追加するには、100 ページのセクション 5.7「パスワード同期をサポートするための、既存のドライバ環境設定のアップグレード」を参照してください。

グローバル構成値を編集する

1 iManager で、［パスワード］>［パスワード同期］の順に選択します。

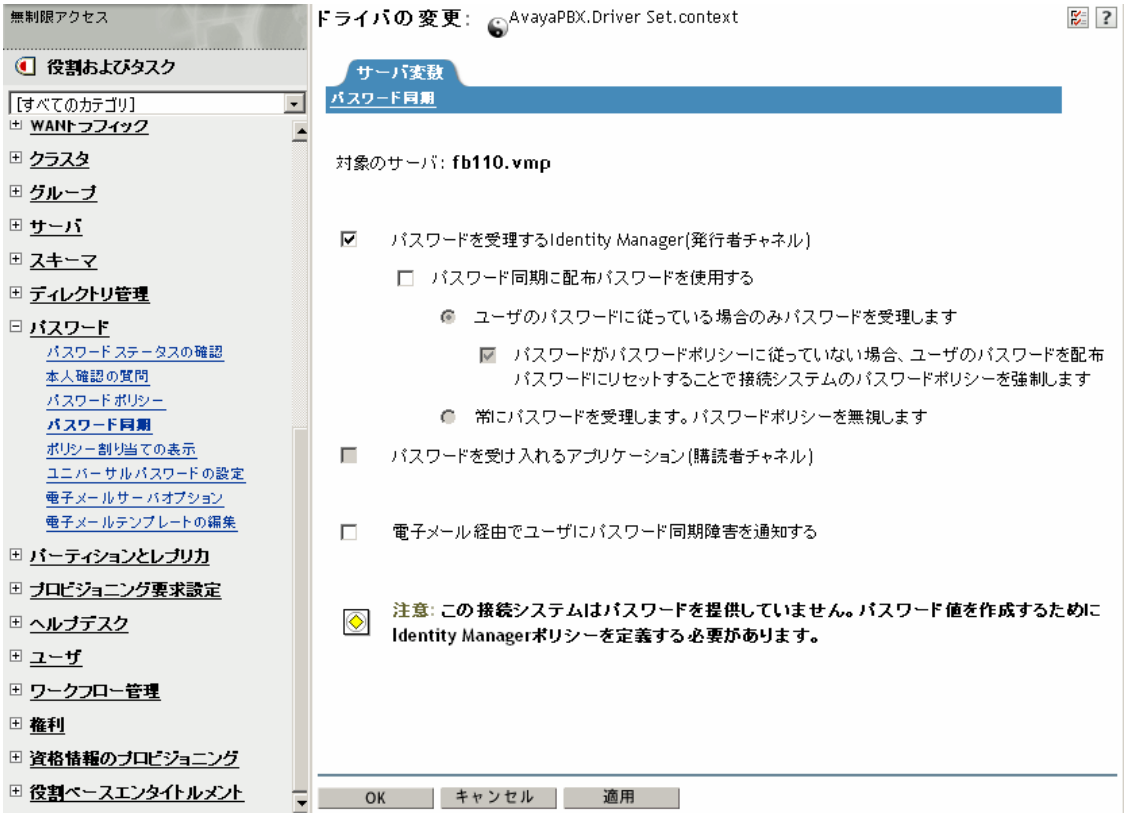
2 ドライバを検索します。

接続システムドライバを検索する場所を指定すると、iManager によって検索されたすべての接続システムドライバに対するパスワードフロー設定の概要が表示されます。



3 設定を表示するために、ドライバ名をクリックします。

［ドライバの変更］ページに、パスワード同期のグローバル構成値が表示されます。



このページのオプションが淡色表示されている場合は、接続システムがそのオプションをサポートしていないことをドライバマニフェストが示しています。

4 変更を加え、［OK］をクリックします。

注 : 各ドライバに別個にグローバル構成値を設定できます。ドライバに対するグローバル構成値は、ドライバセット上のグローバル構成値よりも優先されます。特定のドライバに値を設定すると、より細かく制御できます。このページには、個々のドライバのグローバル構成値だけを表示できます。

ドライバセットオブジェクトにグローバル構成値を設定すると、ドライバが自身の値を持っていない場合に、そのグローバル構成値がそのドライバセット内のドライバによって継承されます。ドライバが自身の設定を持たず、ドライバセットからのグローバル構成値を継承する場合、iManager には値が表示されません。iManager には継承されているグローバル構成値は表示されませんが、グローバル構成値はパスワード同期ポリシーによって適用されます。

5.3.4 ドライバ環境設定で必要なポリシー

各ドライバの発行者チャネルおよび購読者チャネルの Identity Manager ポリシーは、上記のグローバル構成変数の設定に基づいてパスワードフローを制御します。これらのポリシーは Identity Manager のドライバ環境設定に含まれています。

既存のドライバ環境設定を置き換えるのではなく更新する場合は、特定のポリシーを環境設定に追加する必要があります (100 ページのセクション 5.7「パスワード同期をサポートするための、既存のドライバ環境設定のアップグレード」を参照)。パスワード同期を機能させるには、これらのポリシーをドライバ環境設定の正しい場所に指定する必要があります。

- 90 ページの 「発行者コマンド変換セットで必要なポリシー」
- 92 ページの 「発行者入力変換ポリシーセットで必要なポリシー」
- 92 ページの 「購読者コマンド変換ポリシーセットで必要なポリシー」
- 93 ページの 「購読者出力変換ポリシーセットで必要なポリシー」

発行者コマンド変換セットで必要なポリシー

パスワード同期ポリシー名に一覧表示されているポリシーは、一覧表示されている順に存在する必要があります。また、これらは発行者コマンド変換ポリシーセットの最後のポリシーでもある必要があります。

表 *5-7* 発行者コマンド変換セットで必要なポリシー

ドライバ環境設定内の場所	パスワード同期ポリシー名	ポリシーの実行内容
Publisher Command Transformation (発行者コマンド変換)	Password(Pub)-Default Password Policy (パスワード (発行者)- デフォルトパスワードポリシー)	Add オブジェクトにまだパスワードが含まれていない場合は、デフォルトのパスワードを Add オブジェクトに追加します。 このポリシーと Password(Sub)-Default Password Policy (パスワード (購読者)- デフォルトパスワードポリシー) は、変更または削除できる唯一のポリシーです。パスワード同期機能が適切に機能するためには、他のポリシーを変更せずに使用する必要があります。
	Password(Pub)-Check Password GCV (パスワード (発行者)- パスワード GCV の確認)	GCV を確認し、Identity Manager がこの接続システムからパスワードを受け入れるよう指定しているかどうかを判断します。指定していない場合は、すべてのパスワード要素を除去します。 GCV の名前は enable-password-publish で、表示名は［Identity Manager はアプリケーションからのパスワードを受け入れる］です。
	Password(Pub)-Publish Distribution Password (パスワード (発行者)- 配布パスワードの発行)	<password> 要素を、ユニバーサルパスワードを更新できる形式に変換します。 このポリシーが参照する GCV は、次のとおりです。 ◆ publish-password-to-dp ◆ enforce-password-policy
	Password(Pub)-Publish NDS Password (パスワード (発行者)-NDS パスワードの発行)	NDS パスワードを更新するように指定している場合に、<password> 要素が通過できるようにします。指定していない場合は、<password> 要素を除去します。 このポリシーは、publish-password-to-nds という GCV を参照します。
	Password(Pub)-Add Password Payload (パスワード (発行者)- パスワードペイロードの追加)	電子メール通知のために、エンジン内で回覧されるペイロードデータを挿入します。
	Password(Sub)-Add Password Payload (パスワード (購読者)- パスワードペイロードの追加)	電子メール通知のために、エンジン内で回覧されるペイロードデータを挿入します。

発行者入力変換ポリシーセットで必要なポリシー

入力変換に複数のポリシーがある場合、パスワード (発行者)- 購読者の電子メール通知ポリシーは最後に記述することをお勧めします。

表 *5-8* 発行者入力変換ポリシーセットで必要なポリシー

ドライバ環境設定内の場所	パスワード同期ポリシー名	ポリシーの実行内容
Publisher Input Transformation (発行者入力変換)	Password(Pub)-Sub Email Notifications (パスワード (発行者)- 購読者の電子メール通知)	パスワードペイロード情報が送られてきて、ステータスが問題を示す場合、ユーザに電子メールを送信します。電子メールは、eDirectory 内のインターネット電子メールアドレス属性に示されているユーザの電子メールアドレスに送信されます。 このポリシーは、notify-user-on-password-dist-failure という GCV を参照して、通知電子メールを送信するかどうかを決定します。

購読者コマンド変換ポリシーセットで必要なポリシー

パスワード同期ポリシー名に一覧表示されているポリシーは、一覧表示されている順に存在する必要があります。また、これらは購読者コマンド変換ポリシーセットの最後のポリシーでもある必要があります。

表 *5-9* 購読者コマンド変換ポリシーセットで必要なポリシー

ドライバ環境設定内の場所	パスワード同期ポリシー名	ポリシーの実行内容
Subscriber Command Transformation (購読者コマンド変換)	Password(Sub)-Transform Distribution Password (パスワード (購読者)- 配布パスワードの変換)	ユニバーサルパスワードを <password> 要素に変換します。
	Password(Sub)-Default Password Policy (パスワード (購読者)- デフォルトパスワードポリシー)	Add オブジェクトにまだパスワードが含まれていない場合は、デフォルトのパスワードを Add オブジェクトに追加します。 このポリシーと Password(Pub)-Default Password Policy (パスワード (発行者)- デフォルトパスワード) は、変更または削除できる唯一のポリシーです。パスワード同期機能が適切に機能するためには、他のポリシーを変更せずに使用する必要があります。
	Password(Sub)-Check Password GCV (パスワード (購読者)- パスワード GCV の確認)	GCV を確認し、接続システムがパスワードを受け入れるよう指定しているかどうかを判断します。指定していない場合は、すべてのパスワード要素を除去します。 GCV の名前は enable-password-subscribe で、表示名は［アプリケーションは Identity Manager のデータストアのパスワードを受け入れる］です。
	Password(Sub)-Add Password Payload (パスワード (購読者)- パスワードペイロードの追加)	電子メール通知のために、エンジン内で回覧されるパスワードペイロードデータを挿入します。

購読者出力変換ポリシーセットで必要なポリシー

出力変換に複数のポリシーがある場合、パスワード (購読者)- 発行者の電子メール通知ポリシーは最後に記述することをお勧めします。

表 *5-10* 購読者出力変換ポリシーセットで必要なポリシー

ドライバ環境設定内の場所	パスワード同期ポリシー名	ポリシーの実行内容
Subscriber Output Transformation (購読者出力変換)	Password(Sub)-Pub Email Notifications (パスワード (購読者)- 発行者の電子メール通知)	パスワードペイロード情報が送られてきて、ステータスが問題を示す場合、ユーザに電子メールを送信します。 このポリシーは、notify-user-on-password-dist-failure という GCV を参照して、通知電子メールを送信するかどうかを決定します。

5.3.5 パスワード取得のために接続システムにインストールするフィルタ

AD、NT ドメイン、および NIS では、ユーザのパスワードを取得するためにフィルタをインストールする必要があります。

143 ページのセクション 5.9「パスワードフィルタの設定」を参照してください。

5.3.6 ユーザ用に作成した NMAS パスワードポリシー

ユニバーサルパスワードを使用しなくてもパスワード同期の一部の機能は使用できますが、ユーザ用にユニバーサルパスワードを有効にするには NMAS パスワードポリシーを使用する必要があります。また、パスワードポリシーによって、高度なパスワードルールを指定し、ユーザの既存のパスワードがルールに準拠しているかどうか確認するように指定できます。

Identity Manager のパスワード同期を使用するには、パスワードポリシーを理解する必要があります。パスワードポリシーについては、『*Password Management Administration Guide* (http://www.novell.com/documentation/password_management/index.html)』の「Managing Passwords by Using Password Policies」で説明しています。

5.3.7 NMAS ログインメソッド

状況によっては、NMAS 単純パスワードログインメソッドを用意して、パスワード機能を実行できるようにする必要があります。たとえば、LDAP ではこのメソッドが必要です。

ログインメソッドの詳細については、『*Novell Modular Authentication Services (NMAS) 3.0 Administration Guide* (http://www.novell.com/documentation/nmas30/index.html)』を参照してください。

5.4 Identity Manager の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

- 95 ページの 「NDS パスワードからユニバーサルパスワードへの切り替え」
- 95 ページの 「ユーザによるパスワードの変更」

- 96 ページの 「ユニバーサルパスワードを使用するための準備作業」
- 97 ページの 「コンテナの一致」
- 97 ページの 「電子メール通知の設定」

5.4.1 NDS パスワードからユニバーサルパスワードへの切り替え

パスワードポリシーを使用してユーザのグループに対してユニバーサルパスワードをオンにする場合、ユーザはユニバーサルパスワードに値を入力する必要があります。

NDS パスワードを更新するためにこれまでパスワード同期を使用していた場合は、ユーザのパスワードの移行の準備をする必要があります。ユニバーサルパスワードを使用するように切り替えるには、次のいずれかを実行し、ユーザがユニバーサルパスワードを作成するようにします。

- Novell Client を使用している場合、ユニバーサルパスワードをサポートする Novell Client を導入します。

  Identity Manager のパスワード同期には、Novell Client は必要ありません。

  Novell Client を導入した後、ユーザが次回 Novell Client を使用してログインすると、ハッシュ前に NDS パスワードがキャプチャされ、ユニバーサルパスワードを追加するために使用されます (『Password Management Administration Guide』の「Planning Login and Change Password Methods for your Users」を参照してください)。
- Novell Client を使用していない場合は、ユーザに iManager セルフサービスコンソールにログインさせます。このログインメソッドにより、ユニバーサルパスワードに値が入力されます。iManager セルフサービスコンソールにアクセスするには、iManager サーバの /nps に移動します。たとえば、https://www.myiManager.com/nps です。
- ユニバーサルパスワードが有効な LDAP サーバを使用して認証するサービスを通じて、ユーザにログインさせます。たとえば、会社のポータルを介してログインします。

5.4.2 ユーザによるパスワードの変更

ユーザが iManager、iManager セルフサービスコンソール、または Novell Client でパスワードを変更する場合、NMAS パスワードポリシーの高度なパスワードルールが表示されます。ルールを表示すると、ユーザはルールを推測しなくても、ルールに準拠したパスワードを作成できます。

パスワードフローの設定方法によっては、ユーザが接続システムでパスワードを変更すると、パスワードが Identity Manager および他の接続システムと同期されます。ただし、ユーザがパスワードを変更する際、接続システムには、高度なパスワードルールが表示されません。

高度なパスワードルールを必ず適用してルールに準拠しないパスワードの作成を回避したい場合、iManager セルフサービスコンソールまたは Novell Client のみでパスワードを変更するようユーザに要求するか、高度なパスワードルールをユーザに周知徹底させます。

接続システムでは、パスワードポリシーのルールを表示しなくてもユーザはパスワードを変更できます。したがって、ユーザはルールを正しく覚えていない場合があります。ユーザが最初にパスワードを変更する場合、接続システム自体のポリシーのみが適用されま

す。接続システムでルールに準拠しないパスワードをユーザが作成すると、Identity Manager の設定によっては、次の問題が発生することがあります。

- 接続システムから Identity Manager に、使用するパスワードポリシーを適用する設定を有効にしている場合、ユーザの新しいパスワードはアイデンティティボールトに同期されません。ユーザにエラーを通知するよう Identity Manager を設定している場合、電子メールによりパスワードが同期されなかったことがわかります。
- 接続システムの準拠しないパスワードを置き換えるよう Identity Manager を設定している場合、ユーザは、選択した新しいパスワードで接続システムにログインできなくなります。

  Identity Manager は接続システムのパスワードを、ユーザが最後に作成したルールに準拠したパスワードである可能性の高い、配布パスワードにリセットします。

5.4.3 ユニバーサルパスワードを使用するための準備作業

ユニバーサルパスワードを使用する準備をするには、『*Password Management Administration Guide* (http://www.novell.com/documentation/password_management/index.html)』の「Deploying Universal Password」を参照してください。必要な多くの情報がその章にあります。

次のことも考慮してください。

- ユニバーサルパスワードを使用するには、eDirectory 8.7.1 以降が必要です。NetWare® 6.5 は必要ありません。
- Identity Manager のパスワード同期は、ユニバーサルパスワードと配布パスワードの両方に依存しています。配布パスワードは、Identity Manager が接続システムにパスワードを配布する元になるリポジトリです。ユニバーサルパスワードと同様に、NMAS ポリシーも配布パスワードに適用できます。
- Identity Manager に付属の Identity Manager iManager プラグインには、パスワード管理プラグインが含まれています。これらのプラグインを使用すると、パスワードポリシーを作成したり、ユニバーサルパスワードを NDS パスワード、単純パスワード、および配布パスワードと同期させる方法を決定したりできます。

  これらのプラグインは、NetWare 6.5 に付属のユニバーサルパスワードのプラグインを置き換えます。これらについては、『*Password Management Administration Guide* (http://www.novell.com/documentation/password_management/index.html)』の「Managing Passwords by Using Password Policies」で説明しています。
- eDirectory 8.6.2 は、Identity Manager が使用するツリーとしては使用できません。しかし、eDirectory 8.6.2 は、パスワード同期機能のサブセットについてはサポートされています。したがって、環境全体をアップグレードする準備ができていない場合、他のツリーに対して eDirectory 8.6.2 を使用できます。
- ユニバーサルパスワードを展開するためにソフトウェアをアップグレードする場合の影響を最小限に抑える 1 つの方法は、Identity Manager のための別のツリーをアイデンティティボールトとして作成することです。多くの環境では、Identity Manager およびドライバ用にアイデンティティボールトがすでに使用されています。
- ユニバーサルパスワードは、パスワードポリシーの適用や特殊文字の使用など、従来のパスワード管理ツールではサポートされていない機能を提供します。
- NDS パスワードとユニバーサルパスワードとの同期がずれる状態 (「パスワードドリフト」とも呼ばれます) を回避するには、Novell Client および他のユーティリティのアップデートが重要です。『*Password Management Administration Guide* (http://

www.novell.com/documentation/password_management/index.html)』の「Planning Login and Change Password Methods for Your Users」を参照してください。

- Novell Client の最新バージョンはユニバーサルパスワードをサポートしているので、ユーザに対して初めてユニバーサルパスワードを有効にする際に値を入力し、ユーザがパスワードを変更する場合に NMAS パスワードポリシーを表示および適用できます。
- 接続システムでは、パスワードポリシーで作成した高度なパスワードルールは表示されません。現時点では、Novell Client でも高度なパスワードルールは表示されませんが、Novell Client では高度なパスワードルールは適用されます。

  パスワードの変更は iManager セルフサービスコンソールのみで行うようユーザに徹底してください。

  接続システムで、または Novell Client の最新バージョンを使用してパスワードをユーザが変更することを許可する場合には、パスワードポリシールールをユーザに周知徹底し、ルールに準拠した正しいパスワードをユーザが作成するよう、サポートします。
- ConsoleOne® がユニバーサルパスワードをサポートするのは、NetWare® 6.5 以降のサーバ、または最新の Novell Client がインストールされているコンピュータで使用される場合のみであることを、管理者およびヘルプデスクは理解している必要があります。
- 管理者およびヘルプデスクのユーザは、NDS パスワードのみをサポートするユーティリティを使用する意味も理解している必要があります。これらのユーティリティはログインには使用できますが、パスワードの変更には使用できません。この方法により、パスワードドリフトを回避できます。

  『*Novell Modular Authentication Services (NMAS) 3.0 Administration Guide* (http://www.novell.com/documentation/nmas30/index.html)』では、ユニバーサルパスワードのユーティリティおよびサポートが一覧表示してある TID を参照しています。

5.4.4 コンテナの一致

NMAS のパスワードポリシーはツリー中心で割り当てられます。一方、パスワード同期はドライバごとに設定されます。サーバごとにドライバがインストールされ、ドライバはマスタレプリカまたは読み書き可能レプリカのユーザのみ管理できます。

パスワード同期により期待される結果を取得するには、パスワード同期を実行するサーバにあるマスタレプリカまたは読み書き可能レプリカのコンテナが、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割り当てたコンテナと一致するようにします。パーティションルートコンテナにパスワードポリシーを割り当てることによって、そのコンテナとサブコンテナ内のすべてのユーザに確実にパスワードポリシーが割り当てられます。

5.4.5 電子メール通知の設定

電子メール通知機能を使用するには、次のことが必要です。

- iManager の［Notification Configuration (通知設定)］タスクを使用し、電子メールサーバを設定する。
- 必要に応じて、iManager の［Notification Configuration (通知設定)］タスクを使用し、電子メールのテンプレートをカスタマイズする。

- アイデンティティボールトユーザがインターネット電子メールアドレス属性に入力済みであることを確認します。

147 ページのセクション 5.12「電子メール通知の設定」の指示に従います。

5.5 新しいドライバの設定と同期

現在の環境で Password Synchronization 1.0 を使用しておらず、ドライバを作成するか、または既存の環境設定を新しい Identity Manager の環境設定に置き換える場合は、Identity Manager のパスワード同期機能を設定します。

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。

   94 ページのセクション 5.4「Identity Manager の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。

2. ドライバを作成するか、既存のドライバの環境設定を Identity Manager 3 の環境設定に置き換えます。

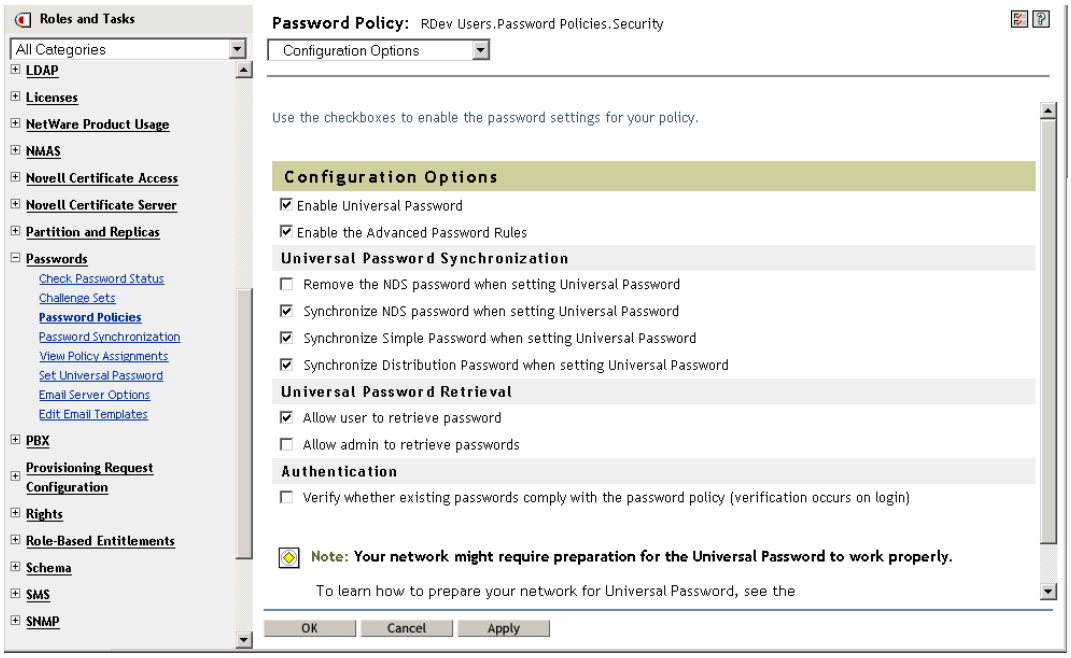
   Identity Manager の環境設定には、Identity Manager ポリシーおよび Identity Manager のパスワード同期に必要なその他の項目が含まれています。新しいドライバ環境設定のサンプルのインポートについては、個々の Identity Manager ドライバのガイド (http://www.novell.com/documentation/beta/dirxmldrivers) を参照してください。

3. ユニバーサルパスワードが有効な NMAS パスワードポリシーを作成し、ユニバーサルパスワードをオンにします。

   『*Password Management Administration Guide* (http://www.novell.com/documentation/password_management/index.html)』の「Creating Password Policies」を参照してください。NetWare 6.5 でユニバーサルパスワードを以前使用したことがある場合は、『*Password Management Administration Guide*』の「(NetWare 6.5 Only) Re-Creating Universal Password Assignments」で説明されている追加手順を参照してください。

   パスワードポリシーは、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。

［環境設定オプション］ページを使用すると、NMAS が同期された異なる種類のパスワードをどのように保持するのかを選択できます。



パスワード同期の使用のシナリオ、および Identity Manager のパスワードポリシーの適用方法については、109 ページのセクション 5.8「パスワード同期の実装」を参照してください。オンラインヘルプも参照してください。

4 (Active Directory、NIS、または NT ドメインのみ) 接続システムで Identity Manager のパスワードをユーザに割り当てる場合は、新しいパスワード同期のフィルタをインストールし、設定します。

手順については、「Identity Manager Drivers (http://www.novell.com/documentation/lg/dirxmldrivers/index.html)」にある各ドライバのドライバ実装ガイドを参照してください。

5 各接続システムで、パスワードフローが正しく設定されていることを確認します。

5a iManager で、［パスワード］>［パスワード同期］の順にクリックし、管理する接続システムのドライバを検索します。

5b パスワードフローの現在の設定を表示します。

これは、グローバル構成値 (GCV) のグラフィカルインタフェースです。ドライバの名前をクリックし、これらを編集します。次の設定を編集できます。

- Identity Manager がシステムからパスワードを受け入れるかどうか。
- どのパスワードを Identity Manager で更新するか。ユニバーサルパスワードを直接更新するか、または配布パスワードを直接更新するか。

  Identity Manager はエントリポイント、つまりどのパスワードを Identity Manager で更新するかを制御します。NMAS は、パスワードポリシーの環境設定オプションで設定した内容に基づいて、各種パスワード間のパスワードのフローを制御します。98 ページのステップ 3 の図を参照してください。

- Identity Manager に入力されるパスワードの変更に、ユーザのパスワードポリシーを適用するかどうか。
- 接続システムにユーザのパスワードポリシーを適用し、準拠しないパスワードをリセットするかどうか。
- この接続システムがパスワードを受け入れるかどうか。
- パスワード同期に失敗した場合、電子メール通知を送信するかどうか。

6 パスワード同期をテストします。

- Identity Manager のパスワードが指定したシステムに配布されることを確認します。
- 指定した接続システムがIdentity Managerにパスワードを公開しているかを確認します。

トラブルシューティングのヒントについては、109 ページのセクション 5.8「パスワード同期の実装」を参照してください。

5.6 Password Synchronization 1.0 のアップグレード

この作業は、Password Synchronization 1.0 で使用されている Active Directory および NT ドメインの既存の Identity Manager ドライバのみに適用されます。

Password Synchronization 1.0 からアップグレードする場合には、正しい手順に従うことが重要です。

手順については、「Identity Manager Drivers (http://www.novell.com/documentation/dirxmldrivers/index.html)」にある Active Directory および NT ドメイン用 Identity Manager ドライバのドライバ実装ガイドを参照してください。

5.7 パスワード同期をサポートするための、既存のドライバ環境設定のアップグレード

ここでは、既存のドライバ環境設定を Identity Manager のサンプル環境設定に置き換えるのではなく、Identity Manager のパスワード同期のサポートを既存のドライバ環境設定に追加する方法について説明します。

パスワード同期に使用する各ドライバにサポートを追加します。これを行うには、「オーバーレイ」設定設定ファイルをインポートし、ポリシー、ドライバマニフェスト、および GCV を一度に追加します。

ポリシー、ドライバマニフェスト、および GCV を追加した後、ドライバフィルタに nspmDistributionPassword 属性も追加する必要があります。

重要 **:** Password Synchronization 1.0 で使用されている Active Directory または NT ドメイン用 Identity Manager ドライバをアップグレードする場合は、「Identity Manager Drivers (http://www.novell.com/documentation/dirxmldrivers/index.html)」にある、Active Directory および NT ドメイン用 Identity Manager ドライバのドライバ実装ガイドのアップグレード手順に従います。

この手順で追加されるポリシーは、ユニバーサルパスワードおよび配布パスワードを使用し、パスワード同期をサポートするためのものです。NDS パスワードのみを同期するために Identity Manager ドライバを使用している場合には、このポリシーは Identity Manager ドライバの環境設定に使用できません。111 ページのセクション 5.8.2「シナリオ 1: NDS パスワードを使用した、2 つのアイデンティティボールト間の同期」で説明するように、NDS パスワードは、これらのポリシーではなく、公開鍵および秘密鍵の属性を使用して同期されます。

- 101 ページの 「ステップ 1: Identity Manager 3 の形式にドライバを変換する」
- 104 ページの 「ステップ 2: ドライバ環境設定への追加」
- 105 ページの 「ステップ 3: フィルタ設定の変更」
- 108 ページの 「ステップ 4: パスワード同期のフローの設定」

前提条件

- ❑ 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。

重要 **:** Password Synchronization 1.0 で使用されている Active Directory または NT ドメイン用 Identity Manager ドライバをアップグレードする場合は、アップグレード手順を確認してから、ドライバシムをインストールします。手順については、「Identity Manager Drivers (http://www.novell.com/documentation/dirxmldrivers/index.html)」にある Active Directory および NT ドメイン用 Identity Manager ドライバのドライバ実装ガイドのアップグレードの説明を参照してください。

5.7.1 ステップ 1: Identity Manager 3 の形式にドライバを変換する

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。

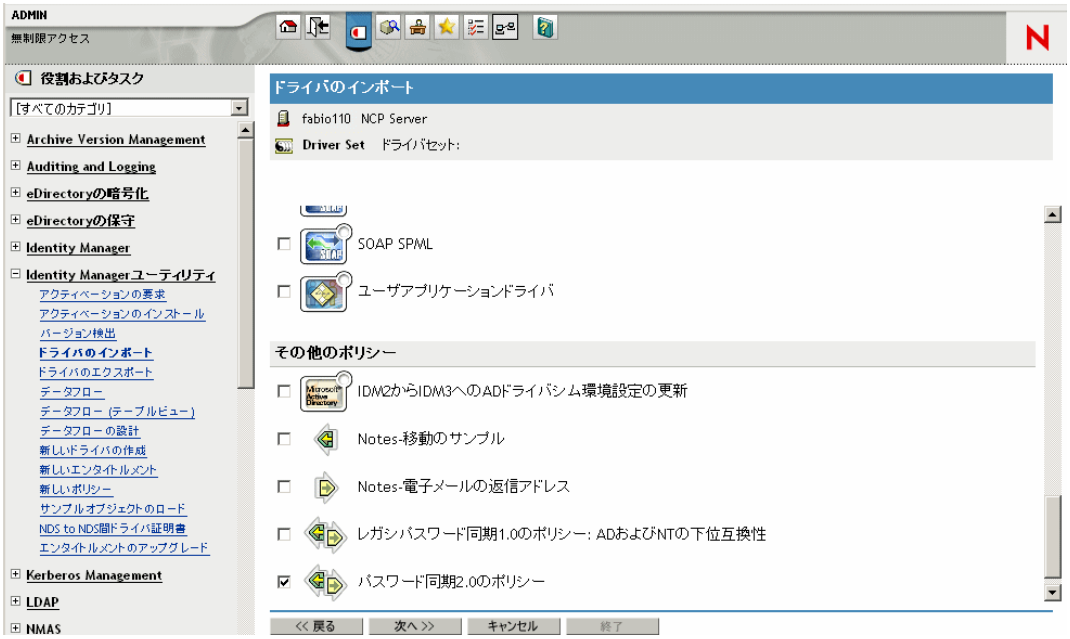
94 ページのセクション 5.4「Identity Manager のパスワード同期およびユニバーサルパスワードを使用するための準備作業」を参照してください。

DirXML® 1.1a を使用している場合、21 ページのセクション 2.3「DirXML 1.1a から Identity Manager 形式へのドライバ環境設定のアップグレード」を参照してください。

2 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。

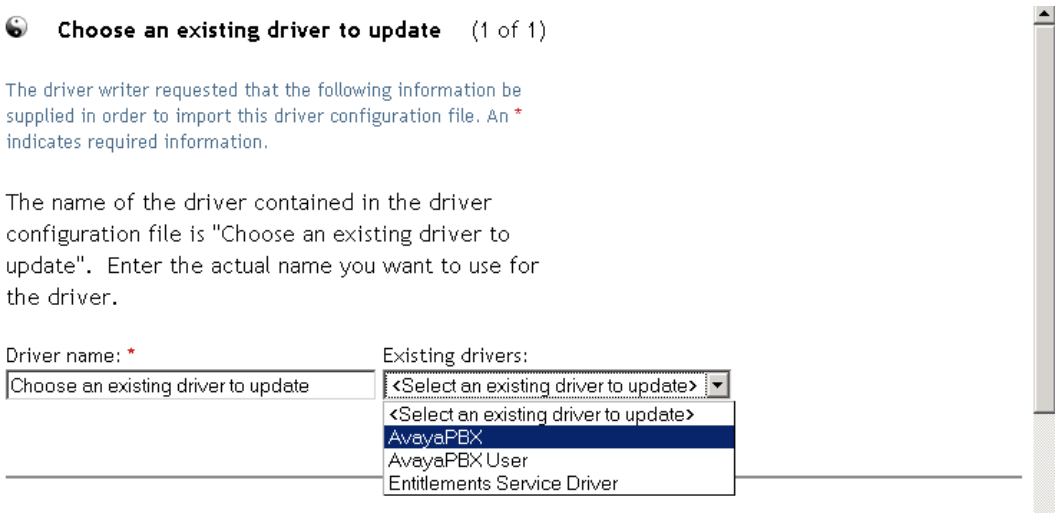
3 既存のドライバの存在するドライバセットを選択し、［次へ］をクリックします。

4 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］までスクロールし、［パスワード同期 2.0 のポリシー］のみを選択します。



5 ［次へ］をクリックします。

6 ［既存のドライバ］ドロップダウンリストで、更新する既存のドライバを選択します。



7 ［接続システム］ドロップダウンリストで、接続システムのタイプを選択します。

ドロップダウンリストにドライバ名が表示されない場合、［その他のシステム］を選択します。

ドライバのタイプに基づき、ドライバインポートウィザードは、ドライバ環境設定の機能と接続システムを示すドライバマニフェストのエントリを作成します。

- 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。

これは、スタイルシートを使用して作成できるパスワードではなく、接続システム上のユーザの実際のパスワードを参照します。これが可能なのは、Active Directory、eDirectory、および NIS のみです。

- 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。

パスワード同期のポリシーが機能するには、正しいドライバマニフェストのエントリが必要です。ドライバマニフェストは、接続システム、Identity Manager のドライバシム、およびドライバ環境設定ポリシーを結合した機能を示し、通常はネットワーク管理者が編集することはできません。

8 ［次へ］をクリックします。

9 保存するドライバマニフェストまたは GCV 値がない場合、［該当ドライバについてすべてを更新］を選択します。

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、GCV、および Identity Manager ポリシーを指定します。

ドライバマニフェストおよび GCV によって、すでに存在する値が上書きされます。Identity Manager 2 ではこれらの種類のドライバパラメータは新しいため、DirXML 1.*x* ドライバには上書きされる既存の値はありません。

パスワード同期のポリシーは、既存のポリシーオブジェクトを上書きしません。単にドライバオブジェクトに追加されます。

注 **:** 保存するドライバマニフェストまたは GCV 値がない場合、［該当ドライバで選択したポリシーのみを更新］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。追加する値がある場合には、手動で貼り付ける必要があります。

---

10 ［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。

5.7.2 ステップ 2: ドライバ環境設定への追加

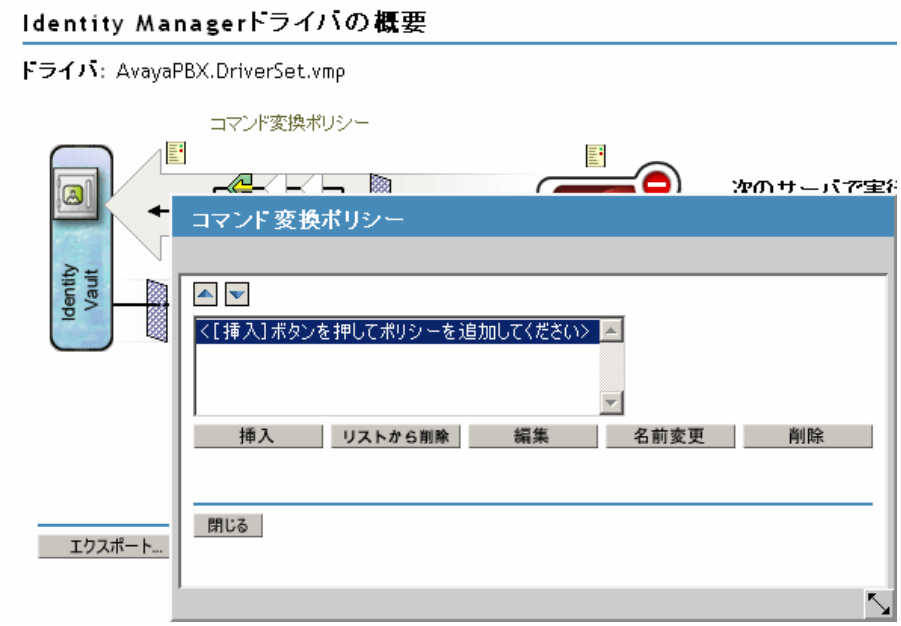
追加するポリシーのリスト、およびその挿入場所については、90 ページのセクション 5.3.4「ドライバ環境設定で必要なポリシー」を参照してください。

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。

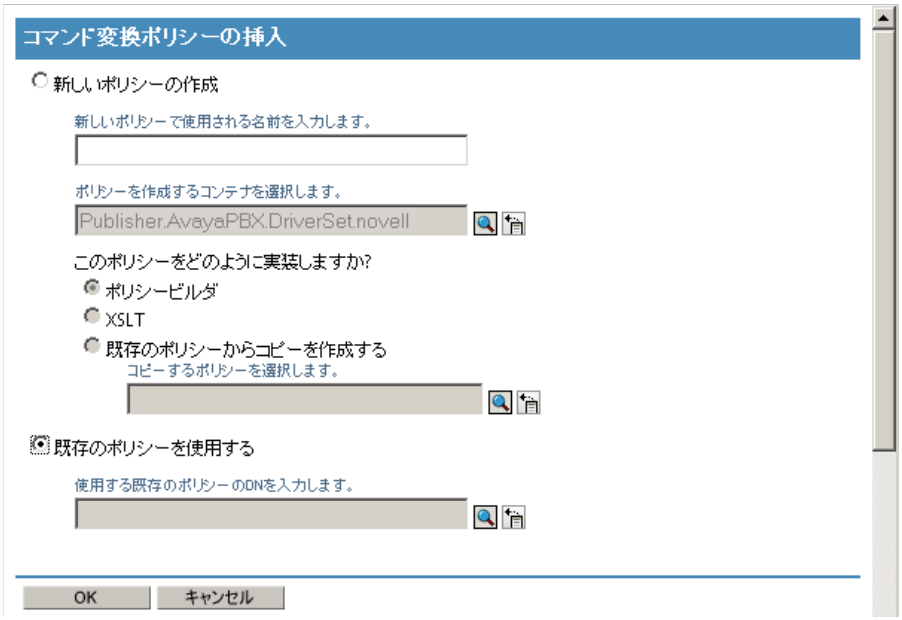
ポリシーセットに複数のポリシーがある場合、これらの Identity Manager のパスワード同期のポリシーが最後に表示されるようにしてください。

ポリシーごとに、次の手順を繰り返します。

1. ［*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検索します。
2. (AvayaPBX などの) 更新したドライバをクリックします。
3. 新しいポリシーを追加する必要がある場所のアイコン (発行者チャネルの［コマンド変換ポリシー］など) をクリックします。



4 ［挿入］をクリックし、新しいポリシーを追加します。



5 ［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。

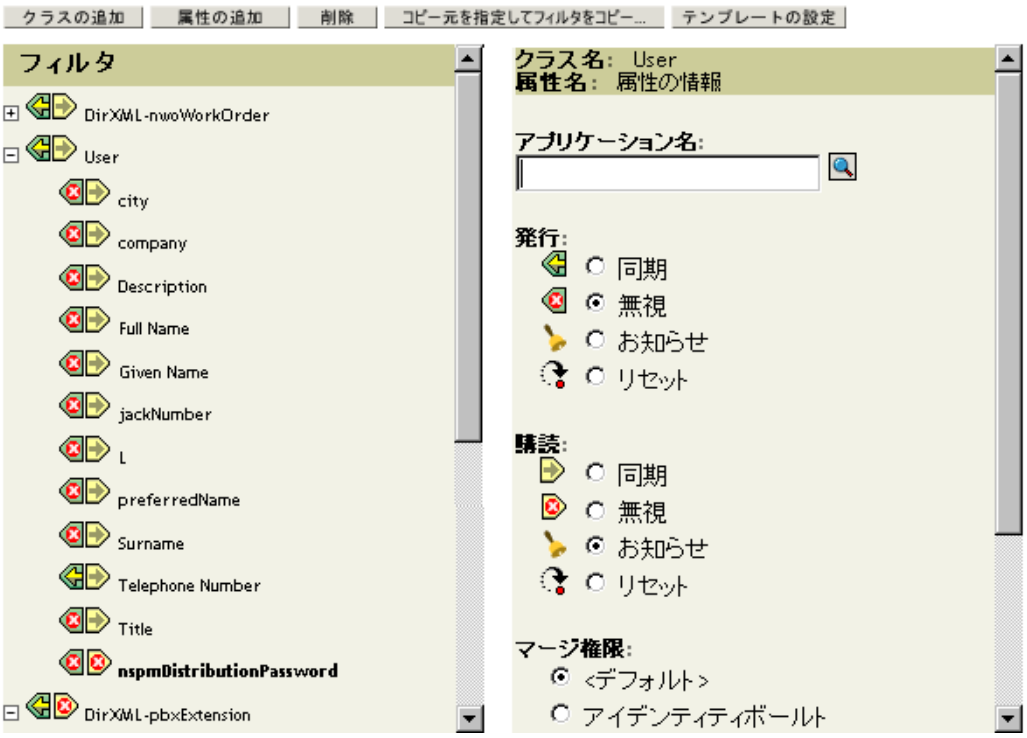
6 新しいポリシーでリストに複数のポリシーがある場合、矢印ボタンを使用して、新しいポリシーをリスト内の正しい場所に移動します。

90 ページのセクション 5.3.4「ドライバ環境設定で必要なポリシー」にリスト表示されている順序にポリシーが表示されていることを確認します。

5.7.3 ステップ 3: フィルタ設定の変更

1 パスワードを同期するオブジェクトクラス (ユーザなど) については、フィルタに nspmDistributionPassword 属性があり、次の設定になっていることを確認します。

- 発行者チャネルについては、フィルタが nspmDistributionPassword 属性を無視するよう設定します。
- 購読者チャネルについては、フィルタが nspmDistributionPassword 属性を通知するよう設定します。



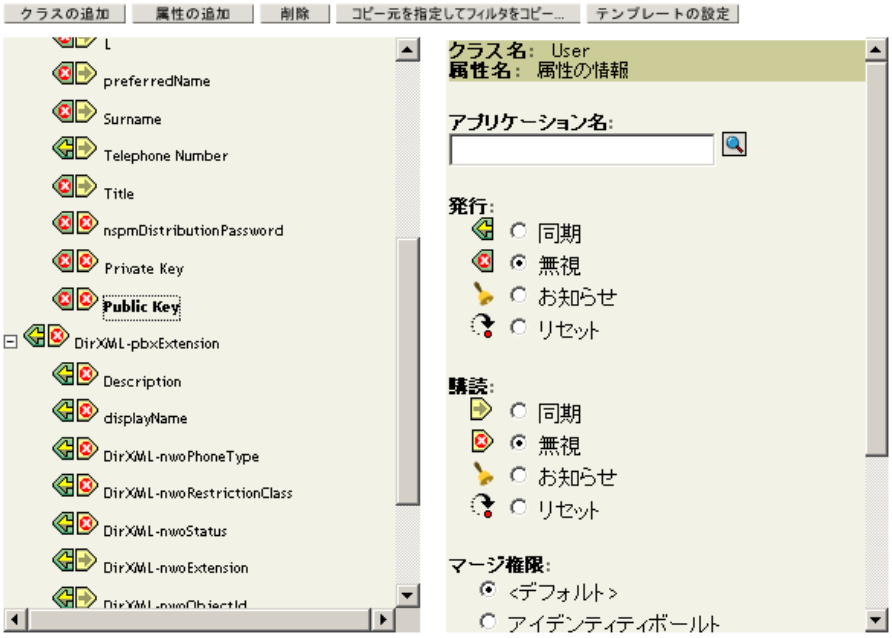
属性を表示するには、スクロールしてクラス (ユーザなど) を選択し、属性をスクロールする必要があります。

nspmDistributionPassword が一覧表示されない場合は、次のように操作します。

1a クラスが選択されていることを確認し、[属性の追加] をクリックします。

1b nspmDistributionPassword までスクロールして選択し、[OK] をクリックします。

2 nspmDistributionPassword 属性が［お知らせ］に設定されているすべてのオブジェクトでは、公開鍵および秘密鍵の属性の両方を［無視］に設定します。



3 パスワード同期に使用するためにアップグレードする各ドライバで、(「Identity Manager 3 の形式にドライバを変換する」の)101 ページのステップ 2 から、この節 (「フィルタ設定の変更」) のステップ 2 までを繰り返します。

この時点で、ドライバには、新しいドライバシム、Identity Manager 形式、およびその他のパスワード同期をサポートするために必要なドライバ環境設定の要素が設定されます。これらの要素は、ドライバマニフェスト、GCV、パスワード同期化ポリシー、およびフィルタ設定です。

4 個々のドライバの導入ガイドで、Identity Manager のパスワード同期の設定に関する追加手順または情報について確認してください。「Identity Manager Drivers (http://www.novell.com/documentation/lg/dirxmldrivers/index.html)」を参照してください。

5 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、ユニバーサルパスワードをオンにします。

『*Password Management Administration Guide* (http://www.novell.com/documentation/password_management/index.html)』の「Creating Password Policies」を参照してください。NetWare 6.5 でユニバーサルパスワードを以前使用したことがある場合は、『*Password Management Administration Guide*』の「(NetWare 6.5 Only) Re-Creating Universal Password Assignments」で説明されている追加手順を参照してください。

パスワードポリシーは、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。

［環境設定オプション］ページには、NMAS が同期された異なる種類のパスワードをどのように保持するのかを選択するオプションがあります。ほとんどの実装では、デフォルト設定で動作します。詳細については、そのページのオンラインヘルプを参照してください。

パスワード同期の使用のシナリオ、およびパスワードポリシーの適用方法については、109 ページのセクション 5.8「パスワード同期の実装」を参照してください。

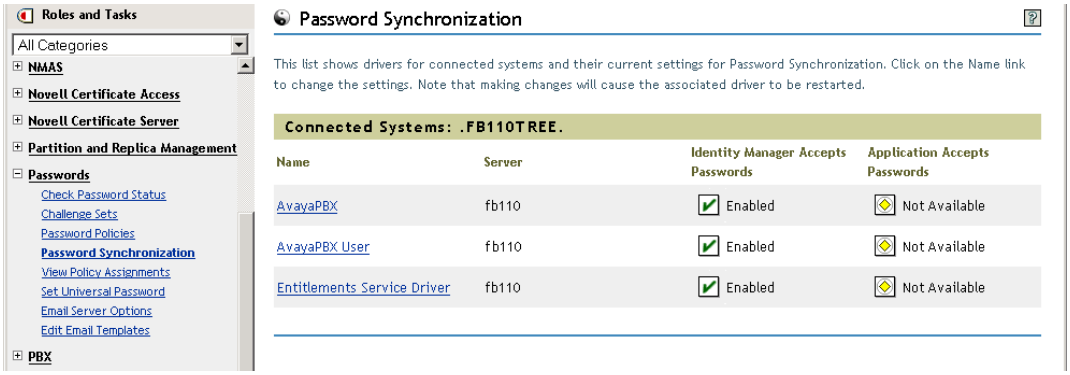
NMAS のパスワードポリシーはツリー中心で割り当てられます。一方、パスワード同期はドライバごとに設定されます。サーバごとにドライバがインストールされ、ドライバはマスタレプリカまたは読み書き可能レプリカのユーザのみ管理できます。

パスワード同期により期待される結果を取得するには、パスワード同期を実行するサーバにあるマスタレプリカまたは読み書き可能レプリカのコンテナが、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割り当てたコンテナと一致するようにします。パーティションルートコンテナにパスワードポリシーを割り当てることによって、そのコンテナとサブコンテナ内のすべてのユーザに確実にパスワードポリシーが割り当てられます。

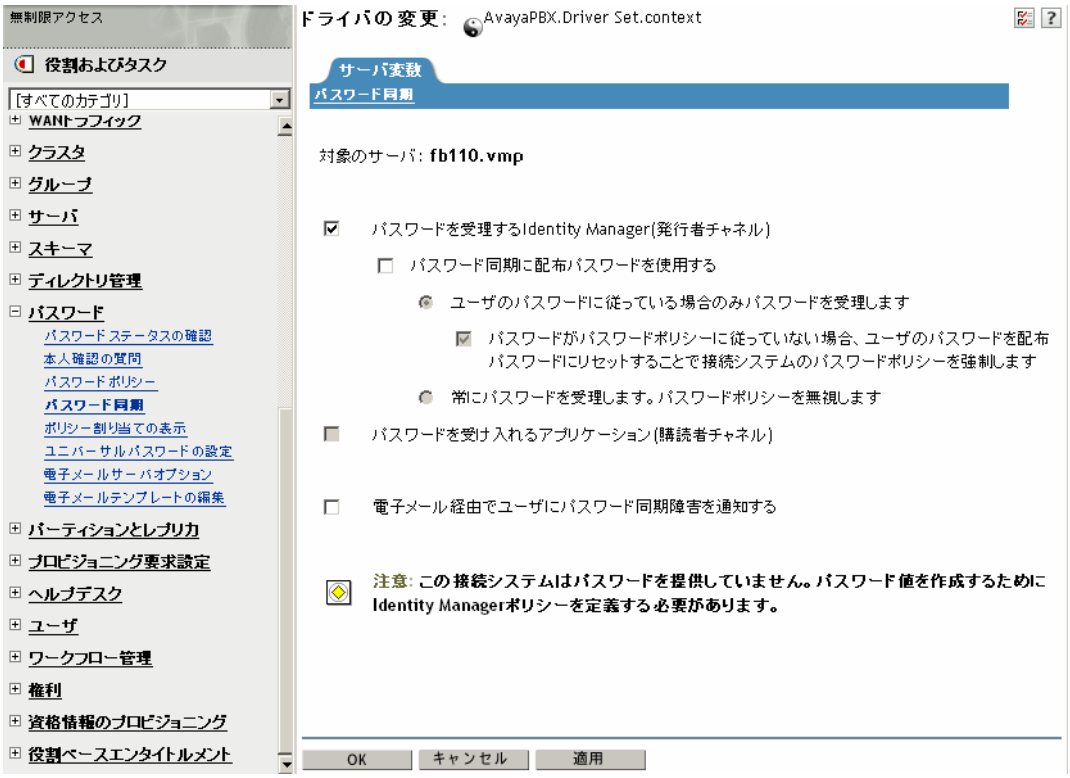
5.7.4 ステップ 4: パスワード同期のフローの設定

パスワードフローが各接続システムに対して希望する方法で設定されていることを確認します。

1. iManager で、［パスワード］>［パスワード同期］の順に選択します。
2. 管理する接続システム用のドライバのツリーまたはコンテナを検索します。



3 ドライバを選択し、パスワードフローの現在の設定を表示します。



このページに、グローバル構成値 (GCV) が一覧表示されます。オプションを選択して変更します。

Identity Manager はエントリポイント、つまりどのパスワードを Identity Manager が更新するかを制御します。NMAS は、［環境設定オプション］で設定したオプションに基づいて、それぞれの異なる種類のパスワード間でのパスワードのフローを制御します (89 ページのステップ 3 に［環境設定オプション］ページが示されています)。［パスワード同期に配布パスワードを使用する］を選択した場合、Identity Manager では配布パスワードが直接使用されます。このオプションをオフにした場合、Identity Manager ではユニバーサルパスワードが直接使用されます。

(図を含む) これらのオプションの詳細については、109 ページのセクション 5.8「パスワード同期の実装」を参照してください。オンラインヘルプも参照してください。

4 パスワード同期をテストします。

Identity Manager のパスワードが指定したシステムに配布されることを確認します。

指定した接続システムが Identity Manager にパスワードを公開しているかを確認します。

トラブルシューティングのヒントについては、109 ページのセクション 5.8「パスワード同期の実装」を参照してください。

5.8 パスワード同期の実装

Identity Manager で提供されているパスワード同期の機能により、いくつかの異なるシナリオを実装できます。この節では、基本シナリオについて説明し、Identity Manager のパ

スワード同期と NMAS パスワードポリシーの設定がパスワード同期の方法にどのように影響を与えるかについて理解するために役立つ情報を提供します。現在の環境のニーズに合わせて、1 つまたは複数のシナリオ使用できます。

- 110 ページのセクション 5.8.1「Identity Manager と NMAS の関係の概要」
- 111 ページのセクション 5.8.2「シナリオ 1: NDS パスワードを使用した、2 つのアイデンティティボールト間の同期」
- 114 ページのセクション 5.8.3「シナリオ 2: ユニバーサルパスワードを使用した同期」
- 124 ページのセクション 5.8.4「シナリオ 3: Identity Manager での配布パスワードの更新による、アイデンティティボールトおよび接続システムの同期」
- 134 ページのセクション 5.8.5「シナリオ 4: トンネリング —Identity Manager での配布パスワードの更新による、アイデンティティボールトではなく接続システムの同期」
- 139 ページの 「シナリオ 5: アプリケーションパスワードの単純パスワードへの同期」

5.8.1 Identity Manager と NMAS の関係の概要

- 110 ページの 「ユーティリティと NMAS」
- 111 ページの 「Identity Manager と NMAS」

ユーティリティと NMAS

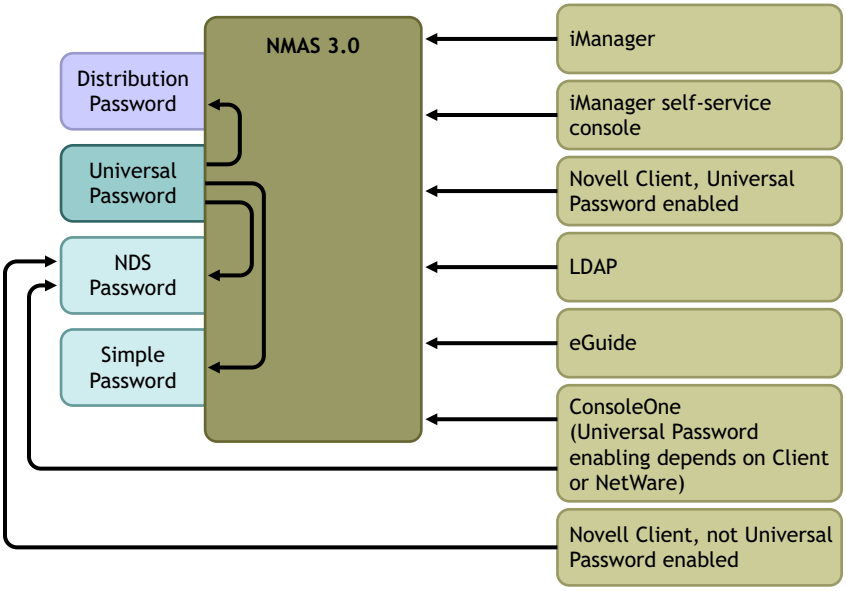
iManager などのユーティリティおよび Novell Client は、特定のパスワードを直接更新せずに、NMAS と通信します。NMAS は、どのパスワードが更新されるのかを決定するエンティティです。

NMAS パスワードポリシーの設定に基づいて、NMAS がアイデンティティボールト内でパスワードを同期します。

ユニバーサルパスワードが有効でないレガシーユーティリティは、NDS パスワードを直接更新します。NMAS と通信し、NMAS がどのパスワードを更新するかを決定するのではありません。ユーザおよびヘルプデスクの管理者が環境内でレガシーユーティリティをどのように使用するかに留意してください。レガシーユーティリティは、NDS パスワードを NMAS と通信せずに直接更新するため、ユニバーサルパスワードと NMAS 2.3 を使用している場合、パスワードドリフト (ユニバーサルパスワードと NDS パスワードとの同期がずれる状態) が発生する場合があります。

たとえば、ユニバーサルパスワードのサポートを確認するには、ユーザが Novell Client をアップグレードしていることを確認し、ヘルプデスクのユーザが ConsoleOne を最新の Novell Client または NetWare リリースのみで使用していることを確認します。

図 5-5 *NMAS を使用したパスワードの同期*



Identity Manager と NMAS

Identity Manager は、「エントリポイント」を制御します (ユニバーサルパスワードまたは配布パスワードのどちらかを直接更新します)。NMAS は、アイデンティティボールト内のパスワード同期のフローを制御します。

シナリオ 1 では、eDirectory の Identity Manager ドライバを使用して、NDS パスワードを直接更新できます。このシナリオは基本的に、DirXML 1.*x* で提供されるものと同じです。

シナリオ 2、シナリオ 3、およびシナリオ 4 では、Identity Manager を使用して、ユニバーサルパスワードまたは配布パスワードのいずれかを更新します。Identity Manager は NMAS と通信して、パスワードを変更します。これにより、NMAS は NMAS パスワードポリシーの設定の決定に基づき他のアイデンティティボールトパスワードを更新し、パスワードを接続システムと同期できるように、NMAS パスワードポリシーから高度なパスワードルールを適用できます。これらのシナリオでは、接続システムに Identity Manager が配布するパスワードは、必ず配布パスワードとなります。

シナリオ 2、シナリオ 3、およびシナリオ 4 の間での違いは、NMAS パスワードポリシーセットとそれぞれの接続システムドライバ用の Identity Manager のパスワード同期の設定の異なる組み合わせにあります。

5.8.2 シナリオ 1: NDS パスワードを使用した、2 つのアイデンティティボールト間の同期

Password Synchronization 1.0 と同様に、eDirectory ドライバを使用して 2 つのアイデンティティボールト間で NDS パスワードを同期できます。このシナリオでは、ユニバーサルパスワードの実装は必要ありません。このシナリオは eDirectory 8.6.2 以降で使用できます。この種類のパスワード同期は、公開鍵と秘密鍵のペアの同期とも呼ばれます。

アイデンティティボールト間でパスワードを同期する場合のみ、この方法を使用する必要があります。この方法は NMAS を使用しないので、接続アプリケーションとパスワードを同期する目的では使用できません。

- 112 ページの 「シナリオ 1 の長所と短所」
- 113 ページの 「シナリオ 1 の設定」
- 114 ページの 「シナリオ 1 のトラブルシューティング」

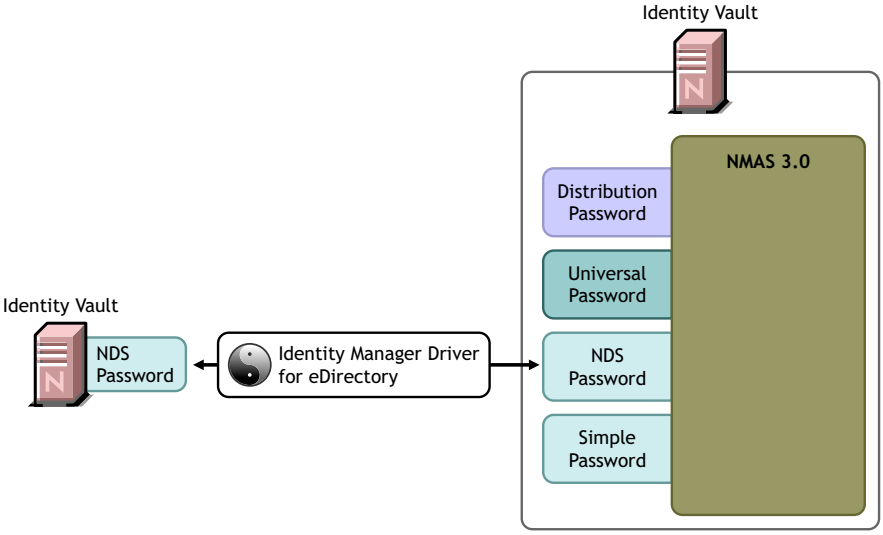
シナリオ 1 の長所と短所

表 *5-11* 長所 : *NDS* パスワードを使用した *eDirectory* 間でのパスワード同期

長所	短所
設定が簡単です。ドライバフィルタに正しい属性を含めるだけです。 各ステージで Identity Manager 3 および eDirectory 8.7.3 を展開する場合、この方法により段階的に展開しやすくなります。 ◆ 新しいパスワード同期のポリシーをドライバ環境設定に追加する必要がない。 ◆ ユニバーサルパスワードをアイデンティティボールトに実装する必要がない。 ◆ eDirectory 8.6.2 以降を実行している接続されたボールトで使用できる。 ◆ NMAS 2.3 は必要ない。 NDS パスワードに設定した基本的なパスワード制限を適用します。	この方法は、アイデンティティボールト間でパスワードを同期します。他の接続システムとパスワードを同期することはできません。 ユニバーサルパスワードまたは配布パスワードは更新されません。 NMAS を使用しないので、別のアイデンティティボールトからのパスワードに対して設定したパスワードポリシーの高度なパスワードルールとの照合によってパスワードを検証できません。 NMAS を使用しないので、パスワードが NMAS パスワードポリシーに準拠していない場合でも、接続されたアイデンティティボールトでパスワードをリセットできません。 同期に失敗したパスワードについては、電子メール通知は使用できません。 iManager のタスクの［パスワードステータスの確認］操作はサポートされていません (この機能では配布パスワードが必要です)。

次の図は、DirXML 1.*x* と同様、eDirectory の Identity Manager ドライバを使用して 2 つのアイデンティティボールト間で NDS パスワードを同期できることを示します。このシナリオでは、NMAS と通信しません。

図 *5-6* *NDS パスワードを使用した、2 つのアイデンティティボールト間の同期*



シナリオ 1 の設定

この種類のパスワード同期を設定するには、ドライバを設定します。

ユニバーサルパスワードの展開

必要ありません。

パスワードポリシーの設定

ありません。

パスワード同期の設定

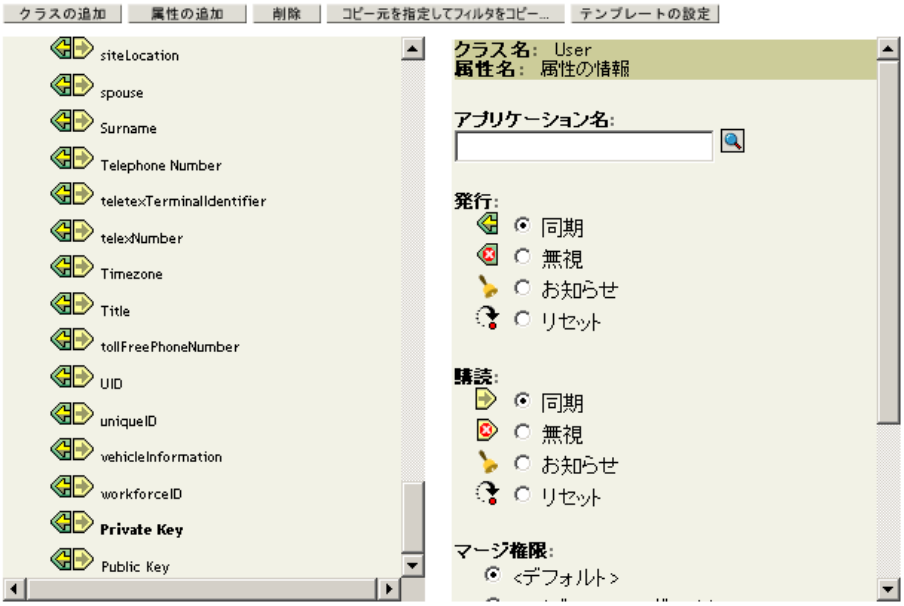
ありません。ドライバの［パスワード同期］ページの設定は、この方法の NDS パスワード同期には影響しません。

ドライバ環境設定

90 ページのセクション 5.3.4「ドライバ環境設定で必要なポリシー」のリストに記載されているパスワード同期のポリシーを削除します。これらのポリシーは、ユニバーサルパスワードおよび配布パスワードをサポートするためのものです。NDS パスワードは、これらのポリシーではなく、公開鍵および秘密鍵の属性を使用して、同期化されます。

両方のアイデンティティボールトドライバのドライバフィルタによって、パスワードを同期するすべてのオブジェクトクラスの公開鍵および秘密鍵の属性が同期されていることを確認します。次の図は、例を示します。

図 *5-7* 秘密鍵と公開鍵の属性の同期



シナリオ 1 のトラブルシューティング

- DStrace オプションをオンにします。
- ドライバフィルタについて、公開鍵と秘密鍵の属性が同期されており、無視されていないことを確認します。
- 159 ページのセクション 5.13「パスワード同期のトラブルシューティング」のヒントも参照してください。

5.8.3 シナリオ 2: ユニバーサルパスワードを使用した同期

Identity Manager では、接続システムのパスワードをアイデンティティボールトのユニバーサルパスワードに同期できます。

ユニバーサルパスワードが更新されると、NMAS パスワードポリシーの設定により、NDS パスワード、配布パスワード、または単純パスワードも更新できます。

接続システムはパスワードを Identity Manager に発行できますが、すべての接続システムがユーザの実際のパスワードを提供できるわけではありません。たとえば、Active Directory はユーザの実際のパスワードを Identity Manager に発行できます。PeopleSoft は PeopleSoft システム自体からパスワードを提供することはできませんが、ユーザの従業員 ID または名字に基づくパスワードなど、ドライバ環境設定のポリシーで作成された初期パスワードは提供できます。すべてのドライバが Identity Manager からパスワードの変更を取得できるわけではありません。83 ページのセクション 5.2「パスワード同期をサポートする接続システム」を参照してください。

- 115 ページの 「シナリオ 2 の長所と短所」

- 116 ページの 「シナリオ 2 の設定」
- 121 ページの 「シナリオ 2 のトラブルシューティング」

シナリオ 2 の長所と短所

表 *5-12* 長所 : ユニバーサルパスワードを使用した同期

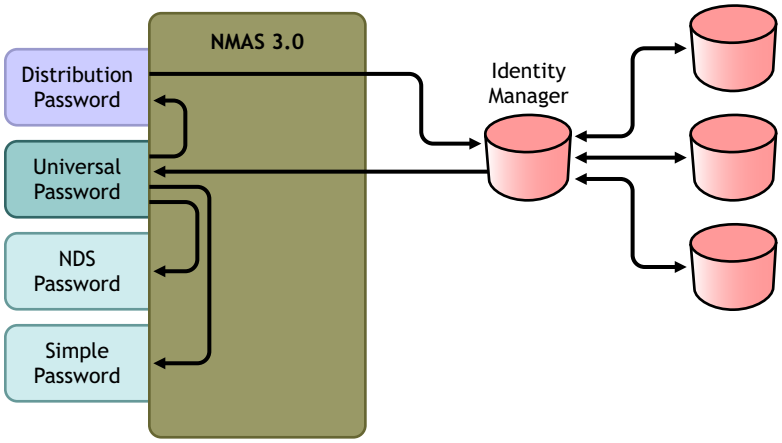
長所	短所
アイデンティティボールトおよび接続システムとのパスワードの同期が可能です。 パスワードを NMAS パスワードポリシーと照合して検証できます。 接続システムから受信したパスワードがパスワードポリシーに準拠していない場合など、失敗したパスワード操作を電子メールで通知できます。 ユニバーサルパスワードが配布パスワードと同期され、接続システムがパスワードの確認をサポートする場合、iManager の［パスワードステータスの確認］タスクをサポートします。 NMAS は、ルールが有効にされている場合、パスワードポリシーの高度なパスワードルールを適用します。接続システムから受信したパスワードがルールに準拠していない場合、エラーが生成され、オプションで指定しているときは電子メール通知が送信されます。 パスワードポリシーのルールを適用しない場合は、NMAS パスワードポリシーの［高度なパスワードルールを有効にする］チェックボックスをオフにできます。	設計上、接続システムのパスワードのリセットはこの方法ではサポートされません。パスワードポリシーの設定によっては、配布パスワードとユニバーサルパスワードが同一でないことがあるためです。

このシナリオの図は、次のフローを示します。

1. パスワードが、Identity Manager を通って来る。
2. Identity Manager が NMAS と通信して、ユニバーサルパスワードを直接更新する。
3. NMAS が、ユニバーサルパスワードを、NMAS パスワードポリシー設定に従って配布パスワードおよびその他のパスワードに同期する。
4. Identity Manager が配布パスワードを取得し、パスワードを受け入れるように設定されている接続システムに配布する。

この図では複数の接続システムが Identity Manager に接続しているように示されていますが、接続システムのドライバごとに設定を作成することに注意してください。

図 *5-8* ユニバーサルパスワードを使用したパスワードの同期



シナリオ 2 の設定

この種類のパスワード同期を設定する

- 116 ページの 「ユニバーサルパスワードの展開」
- 116 ページの 「パスワードポリシーの設定」
- 118 ページの 「パスワード同期の設定」
- 119 ページの 「ドライバ環境設定」

ユニバーサルパスワードの展開

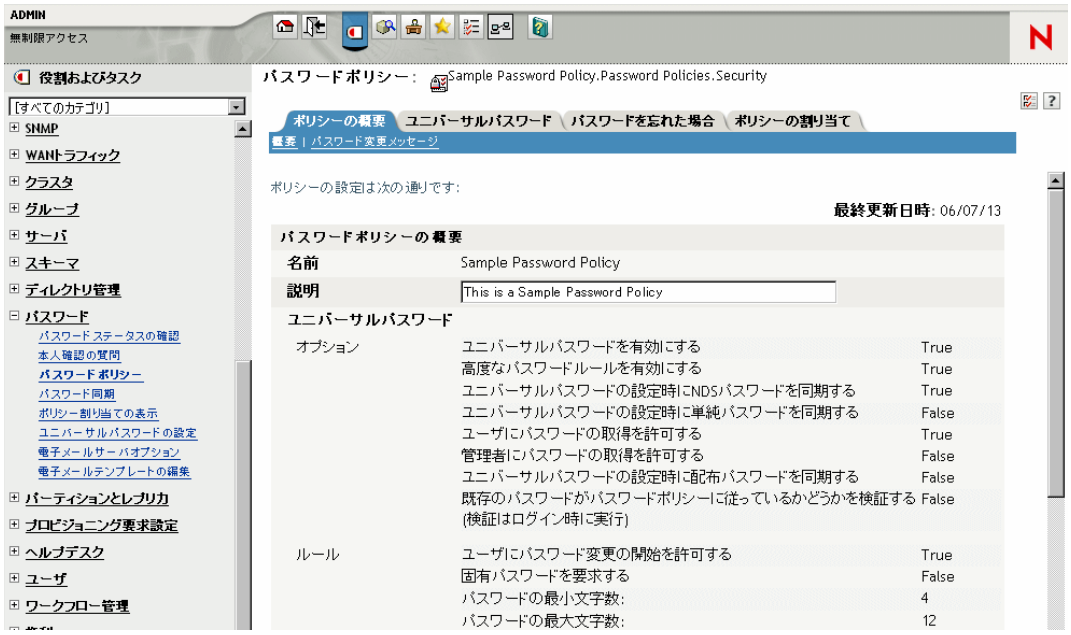
現在の環境でユニバーサルパスワードを使用する準備ができていることを確認します。94 ページのセクション 5.4「Identity Manager のパスワード同期およびユニバーサルパスワードを使用するための準備作業」を参照してください。

パスワードポリシーの設定

NMAS パスワードポリシーが、この種類のパスワード同期を実行したいアイデンティティボールトの一部に割り当てられていることを確認します。

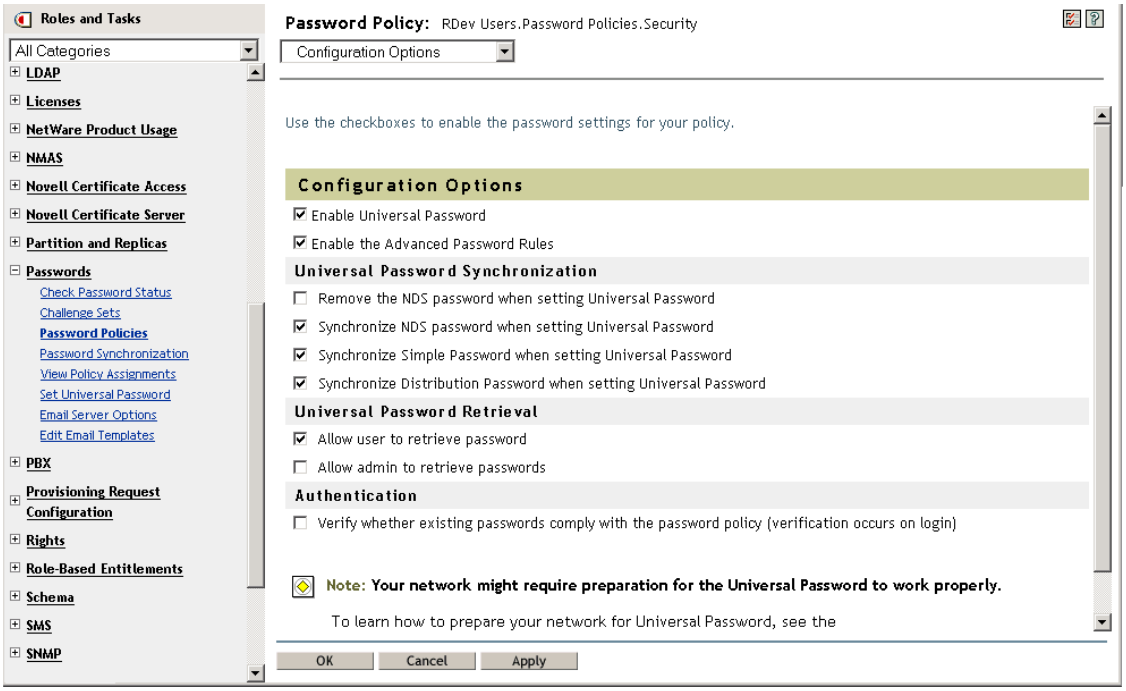
1. iManager で、［パスワード］>［パスワードポリシー］の順に選択します。
2. ポリシーを選択し、［編集］をクリックします。

3 パスワード同期を実行するオブジェクトを参照して選択します。



ツリー構造全体 (セキュリティコンテナのログインポリシーオブジェクトを参照して選択する)、パーティションルートコンテナ、コンテナ、または特定のユーザに、ポリシーを割り当てることができます。管理を簡易化するには、ツリー内のできるだけ高い位置にパスワードポリシーを割り当てることをお勧めします。

4 [パスワードポリシー] で、次のオプションが選択されていることを確認します。



- ユニバーサルパスワードを有効にする

- ユニバーサルパスワードの設定時に *NDS* パスワードを同期する
- ユニバーサルパスワードの設定時に配布パスワードを同期する

  Identity Manager は配布パスワードを取得して接続システムに配布するので、双方向のパスワード同期を可能にするためにこのオプションをオンにすることが重要です。

5 必要に応じ、［パスワードポリシー］の他の設定を完了します。

NMAS は、ルールが有効にされている場合、パスワードポリシーの高度なパスワードルールを適用します。パスワードポリシーのルールを適用しない場合は、［高度なパスワードルールを有効にする］チェックボックスをオフにします。

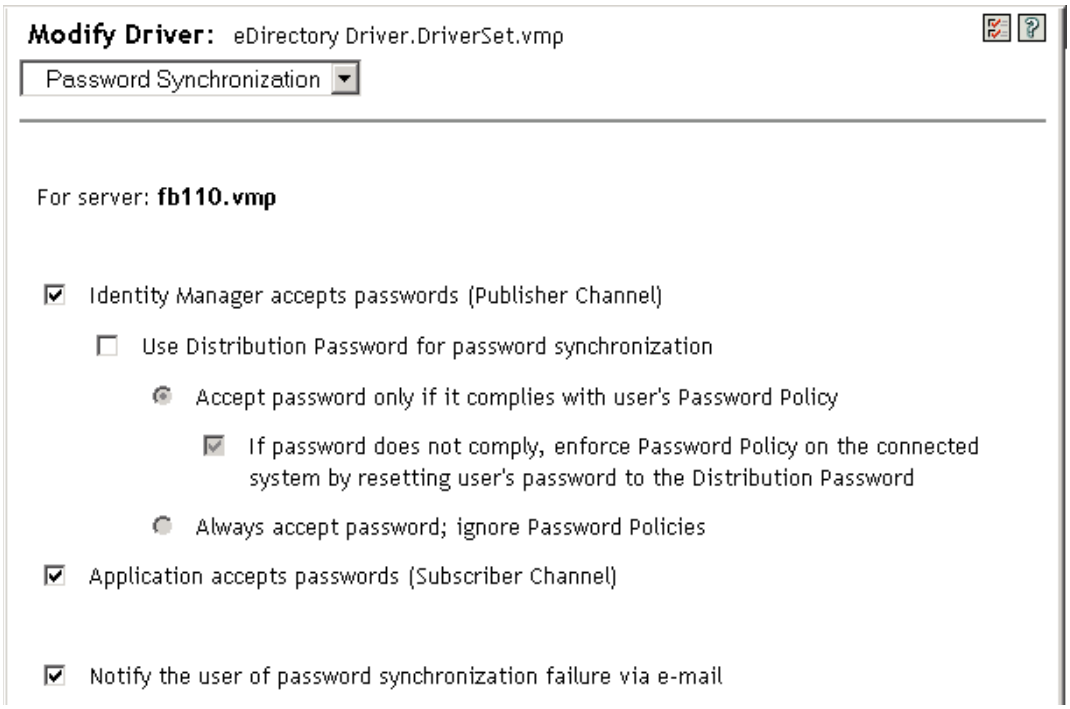
高度なパスワードルールを使用する場合は、パスワードを取得している接続システムのパスワードポリシーと競合しないことを確認します。

パスワード同期の設定

1 iManager で、［パスワード］>［パスワード同期］の順に選択します。

2 接続システムのドライバを検索し、ドライバを選択します。

3 接続システムのドライバの設定を作成します。



次のオプションが選択されていることを確認します。

- パスワードを受理する *Identity Manager(* 発行者チャネル *)*

  ドライバマニフェストに「password-publish」機能が含まれていない場合、メッセージがページに表示されます。これは、パスワードがアプリケーションから取得できず、パスワードを発行するには、ポリシーを使用してドライバ環境設定にパスワードを作成するしかないことをユーザに通知するものです。

- パスワードを受け入れるアプリケーション *(* 購読者チャネル *)*

接続システムがパスワードの受け入れをサポートしない場合、このオプションは淡色表示になります。

これらの設定により、接続システムでサポートされている場合には、双方向のパスワード同期が可能になります。

パスワードの信頼されたソースについては、ビジネスポリシーに合わせて設定を調整できます。たとえば、接続システムがパスワードを取得するが発行しないようにする場合は、［パスワードを受け入れるアプリケーション (購読者チャネル)］のみを選択します。

4 ［パスワード同期に配布パスワードを使用する］がオフになっていることを確認します。

このシナリオでは、Identity Manager がユニバーサルパスワードを直接更新します。接続システムへのパスワードの配布には引き続き配布パスワードが使用されますが、配布パスワードは、Identity Manager ではなく NMAS により、ユニバーサルパスワードから更新されます。

5 (オプション) 必要に応じ、次のオプションを選択します。

- 電子メール経由でユーザにパスワード同期障害を通知する

  電子メール通知には、eDirectory ユーザオブジェクトのインターネット電子メールアドレス属性の入力が必要です。

  電子メール通知は、他に影響を与えません。これらは、電子メールをトリガした XML ドキュメントの処理には影響しません。失敗した場合、操作自体が再試行されない限り、再試行されません。ただし、電子メール通知のデバッグメッセージはトレースファイルに書き込まれます。

ドライバ環境設定

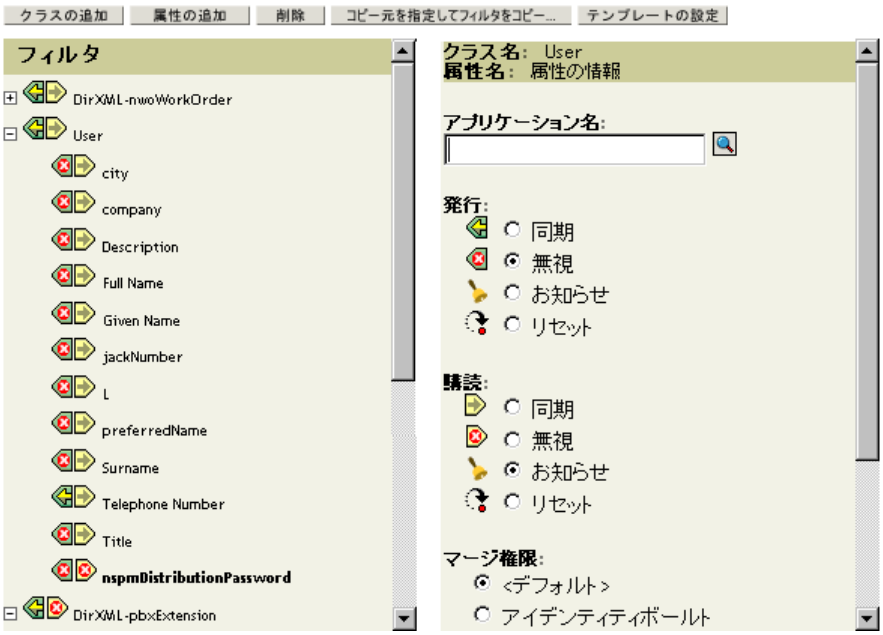
1 必要な Identity Manager スクリプトパスワード同期ポリシーが、パスワード同期に使用する各ドライバのドライバ環境設定に含まれていることを確認します。

ポリシーは、ドライバ環境設定の正しい位置に正しい順序で記述されている必要があります。ポリシーのリストについては、90 ページのセクション 5.3.4「ドライバ環境設定で必要なポリシー」を参照してください。

Identity Manage のサンプル環境設定には、すでにポリシーが含まれています。既存のドライバをアップグレードする場合は、100 ページのセクション 5.7「パスワード同期をサポートするための、既存のドライバ環境設定のアップグレード」のステップを使用してポリシーを追加できます。

2 nspmDistributionPassword 属性について、フィルタを正しく設定します。

- 発行者チャネルについては、ドライバフィルタがすべてのオブジェクトクラスの nspmDistributionPassword 属性を無視するよう設定します。
- 購読者チャネルについては、ドライバフィルタがパスワードの変更を受信するすべてのオブジェクトクラスの nspmDistributionPassword 属性を通知するよう設定します。



3 nspmDistributionPassword 属性が［お知らせ］に設定されているすべてのオブジェクトでは、公開鍵および秘密鍵の属性の両方を［無視］に設定します。

4 パスワードのセキュリティを確保するには、Identity Manager のオブジェクトへの権利を持つユーザを制御していることを確認します。

シナリオ 2 のトラブルシューティング

- 121 ページの 「シナリオ 2 のフローチャート」
- 122 ページの 「アイデンティティボールトへのログインの問題」
- 123 ページの 「パスワードを取得する別の接続システムへのログインのトラブルシューティング」
- 123 ページの 「パスワードのエラーについての電子メールが生成されない」
- 124 ページの 「[オブジェクトパスワードの確認] を使用した場合のエラー」
- 124 ページの 「DSTrace の便利なコマンド」

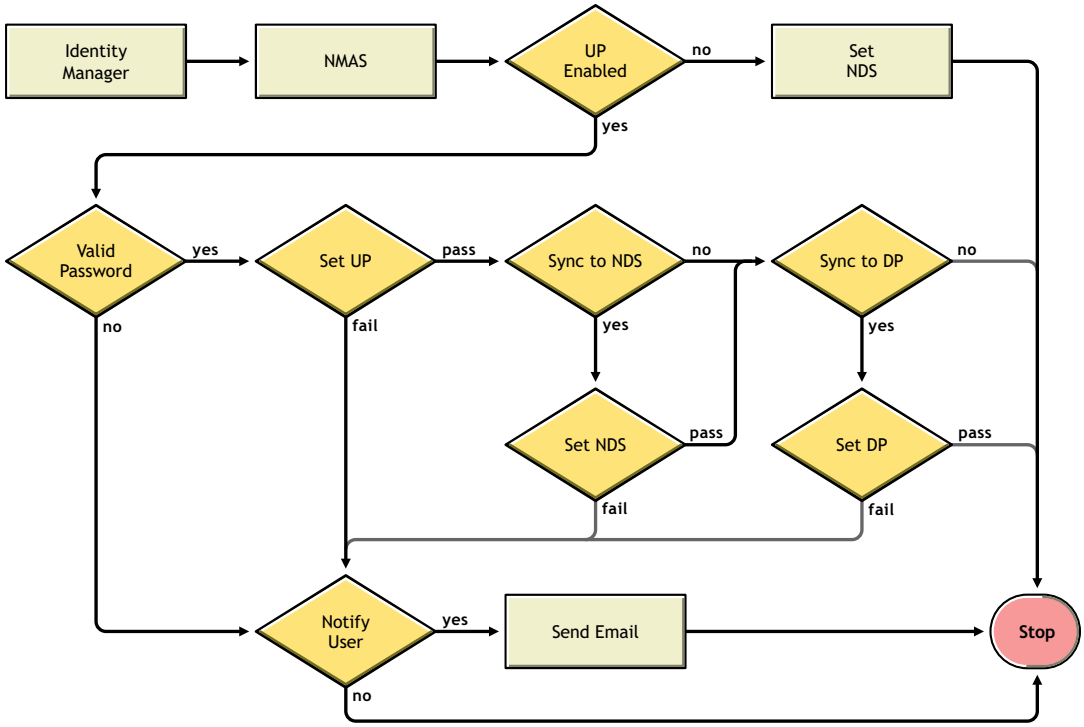
159 ページのセクション 5.13「パスワード同期のトラブルシューティング」のヒントも参照してください。

シナリオ 2 のフローチャート

次のフローチャートは、NMAS が Identity Manager から受信するパスワードの処理の方法を示しています。このシナリオでは、パスワードがユニバーサルパスワードに同期されます。NMAS では、次に基づいてパスワードを処理する方法が決定されます。

- NMAS パスワードポリシーで、ユニバーサルパスワードが有効になっているかどうか。
- 着信パスワードが準拠する必要がある高度なパスワードルールが有効になっているかどうか。
- ユニバーサルパスワードとその他のパスワードとを同期するためのパスワードポリシーに、どのようなその他の設定があるのか。

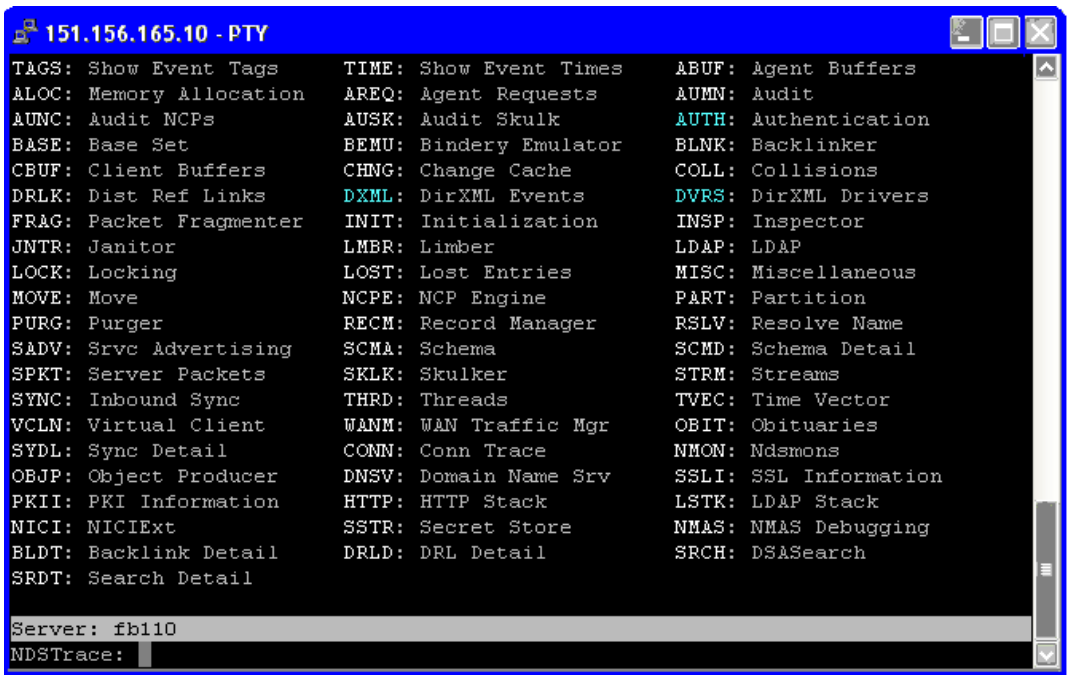
図 **5-9** *NMAS が Identity Manager から受信するパスワードの処理の方法*



アイデンティティボールトへのログインの問題

- DSTrace で、［+AUTH］、［+DXML］、および［+DVRS］の設定をオンにします。

図 **5-10** *DSTrace コマンド*



- <password>または<modify-password>の要素がIdentity Managerに渡されていることを確認します。渡されていることを確認するには、トレース画面のオプションがオンになっていることを確かめます。
- パスワードポリシーのルールに従い、パスワードが有効であることを確認します。
- NMAS パスワードポリシーの設定と割り当てを確認します。ポリシーをユーザに直接割り当て、正しいポリシーが使用されるようにします。
- ドライバの［パスワード同期］ページで、［パスワードを受理する DirXML］が選択されていることを確認します。
- ［パスワードポリシー］で、［ユニバーサルパスワードの設定時に配布パスワードを同期する］が選択されていることを確認します。

パスワードを取得する別の接続システムへのログインのトラブルシューティング

この節では、接続システムが Identity Manager にパスワードを発行しているけれども、パスワードを取得するもう 1 つの接続システムが発行側のシステムからの変更を取得していないように思われる場合の、トラブルシューティングについて説明します。この関係は、第 2 の接続システムとも呼ばれ、第 1 の接続システムから Identity Manager を通じてパスワードを取得することを意味します。

- DSTrace の［+DXML］および［+DVRS］の設定をオンにし、Identity Manager のルール処理を確認します。
- ドライバの Identity Manager のトレースレベルを［3］に設定します。
- ［パスワード同期］の［パスワードを受理する Identity Manager］オプションが選択されていることを確認します。
- ドライバフィルタの nspmDistributionPassword 属性が、119 ページのステップ 2 に説明されているとおりに正しく設定されていることを確認します。
- <*password*> (Addの場合)または<modify-password>の要素が接続システムに送信されていることを確認します。確認するには、DSTrace 画面またはファイルのトレースオプションが、最初の項目で説明したとおり、オンになっていることを確かめます。
- Identity Manager スクリプトパスワードポリシーが、90 ページのセクション 5.3.4「ドライバ環境設定で必要なポリシー」で説明されているとおり、ドライバ環境設定の正しい位置と順序にあることを確認します。
- アイデンティティボールトの NMAS パスワードポリシーを、接続システムにより適用されるパスワードポリシーと比較し、互換性があることを確認します。

パスワードのエラーについての電子メールが生成されない

- DSTrace の［+DXML］の設定をオンにし、Identity Manager のルール処理を確認します。
- ドライバの Identity Manager のトレースレベルを［3］に設定します。
- 電子メールを生成するルールが選択されていることを確認します。
- アイデンティティボールトブジェクトを検証し、ユーザの正しい電子メールアドレスがインターネット電子メールアドレス属性に含まれていることを確認します。
- ［Notification Configuration (通知設定)］タスクで、SMTP サーバと電子メールテンプレートが正しく設定されていることを確認します。147 ページのセクション 5.12「電子メール通知の設定」を参照してください。

［オブジェクトパスワードの確認］を使用した場合のエラー

iManager の［パスワードステータスの確認］タスクにより、ドライバで［オブジェクトパスワードの確認］アクションが発生します。問題が発生した場合は、次を確認します。

- ［オブジェクトパスワードの確認］が -603 を返す場合、アイデンティティボールトブジェクトに nspmDistributionPassword 属性が含まれていません。nspmDistributionPassword 属性に対してドライバフィルタが正しい設定になっていることを確認します。また、パスワードポリシーで［ユニバーサルパスワードの設定時に配布パスワードを同期する］が選択されていることを確認します。
- ［オブジェクトパスワードの確認］が「同期されていません」を返す場合、ドライバ環境設定に適切なパスワード同期のポリシーが含まれていることを確認します。
- アイデンティティボールトの NMAS パスワードポリシーを、接続システムにより適用されるパスワードポリシーと比較し、互換性があることを確認します。
- ［オブジェクトパスワードの確認］は、配布パスワードから操作します。配布パスワードが更新されていない場合、［オブジェクトパスワードの確認］によって、パスワードが同期されていることがレポートされないことがあります。
- Identity Manager ドライバのみについては、［パスワードステータスの確認］は、配布パスワードではなく NDS パスワードを確認することに注意してください。

DSTrace の便利なコマンド

+DXML: Identity Manager ルール処理および可能性のあるエラーメッセージを表示する

+DVRS: Identity Manager ドライバのメッセージを表示する

+AUTH: NDS パスワードの変更を表示する

5.8.4 シナリオ 3: Identity Manager での配布パスワードの更新による、アイデンティティボールトおよび接続システムの同期

このシナリオでは、Identity Manager は配布パスワードを直接更新し、他のアイデンティティボールトパスワードをどのように同期するかは NMAS が決定します。

接続システムはパスワードを Identity Manager に発行できますが、すべての接続システムがユーザの実際のパスワードを提供できるわけではありません。たとえば、Active Directory はユーザの実際のパスワードを Identity Manager に発行できます。PeopleSoft は PeopleSoft システム自体からパスワードを提供することはできませんが、ユーザの従業員 ID または名字に基づくパスワードなど、ドライバ環境設定のポリシーで作成された初期パスワードは提供できます。すべてのドライバが Identity Manager からパスワードの変更を取得できるわけではありません。83 ページのセクション 5.2「パスワード同期をサポートする接続システム」を参照してください。

- 125 ページの 「シナリオ 3 の長所と短所」
- 126 ページの 「シナリオ 3 の設定」
- 130 ページの 「シナリオ 3 のトラブルシューティング」

シナリオ 3 の長所と短所

表 *5-13* 長所 : 配布パスワードの更新による、アイデンティティボールトおよび接続システムの同期

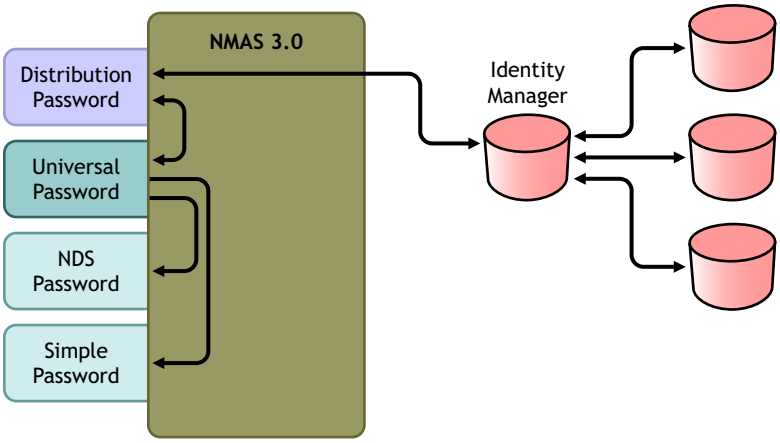
長所	短所
アイデンティティボールトと接続システム間でパスワードを同期できます。 接続システムから受信したパスワードに対して、パスワードポリシーを適用するかどうかを選択できます。 パスワード同期が失敗した場合に通知を送信するよう指定できます。 パスワードポリシーを適用する場合、接続システムのパスワードがパスワードポリシーに準拠しないときに配布パスワードにリセットするよう選択できます。	

このシナリオの図は、次のフローを示します。

1. パスワードが、Identity Manager を通って来る。
2. Identity Manager が NMAS と通信して、配布パスワードを直接更新する。
3. Identity Manager は配布パスワードを使用し、パスワードを受け入れるよう指定した接続システムに配布します。
4. NMAS が、ユニバーサルパスワードを、NMAS パスワードポリシー設定に従って配布パスワードおよびその他のパスワードに同期する。

この図では複数の接続システムが Identity Manager に接続しているように示されていますが、接続システムのドライバごとに設定を作成することに注意してください。

図 *5-11* 配布パスワードの更新による、アイデンティティボールトおよび接続システムの同期



シナリオ 3 の設定

この種類のパスワード同期を設定する

- 126 ページの 「ユニバーサルパスワードの展開」
- 126 ページの 「パスワードポリシーの設定」
- 127 ページの 「パスワード同期の設定」
- 128 ページの 「ドライバ環境設定」

ユニバーサルパスワードの展開

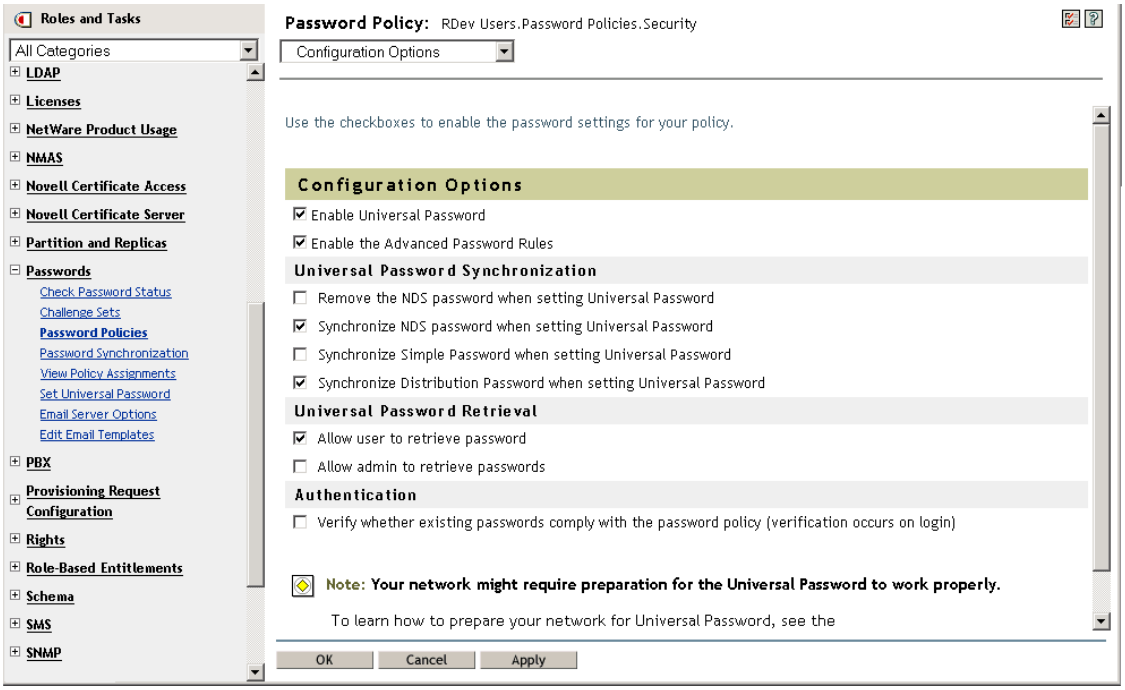
現在の環境でユニバーサルパスワードを使用する準備ができていることを確認します。94 ページのセクション 5.4「Identity Manager のパスワード同期およびユニバーサルパスワードを使用するための準備作業」を参照してください。

パスワードポリシーの設定

1 iManager で、［パスワード］>［パスワードポリシー］の順に選択します。

2 パスワードポリシーが、この種類のパスワード同期を実行したいアイデンティティボールトツリーの一部に割り当てられていることを確認します。パスワードポリシーは、ツリー構造全体、パーティションルートコンテナ、コンテナ、または特定のユーザに割り当てることができます。管理を簡易化するには、ツリー内のできるだけ高い位置にパスワードポリシーを割り当てることをお勧めします。

3 ［パスワードポリシー］で、次のオプションが選択されていることを確認します。



- ユニバーサルパスワードを有効にする
- ユニバーサルパスワードの設定時に *NDS* パスワードを同期する
- ユニバーサルパスワードの設定時に配布パスワードを同期する

Identity Manager は配布パスワードを取得して接続システムに配布するので、双方向のパスワード同期を可能にするためにこのオプションをオンにすることが重要です。

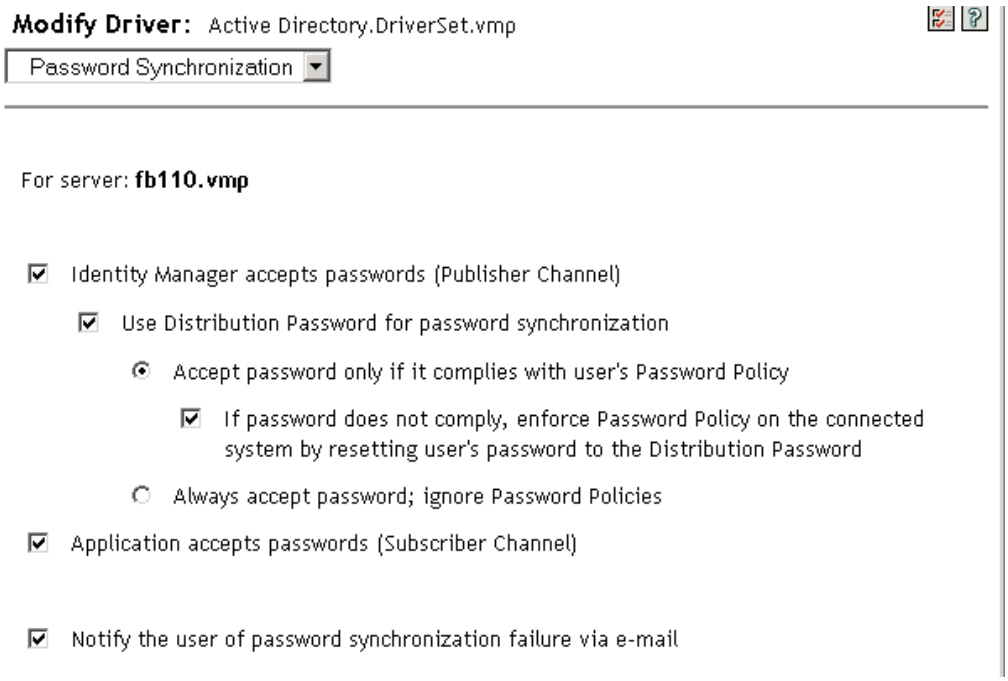
4 高度なパスワードルールを使用する場合は、パスワードを取得している接続システムのパスワードポリシーと競合しないことを確認します。

パスワード同期の設定

1 iManager で、［パスワード］>［パスワード同期］の順に選択します。

2 接続システムのドライバを検索し、ドライバを選択します。

3 接続システムのドライバの設定を作成します。



次のオプションが選択されていることを確認します。

- パスワードを受理する *Identity Manager(* 発行者チャネル *)*
- パスワード同期に配布パスワードを使用する

  ドライバマニフェストに「password-publish」機能が含まれていない場合、メッセージがページに表示されます。これは、パスワードがアプリケーションから取得できず、パスワードを発行するには、ポリシーを使用してドライバ環境設定にパスワードを作成するしかないことをユーザに通知するものです。
- パスワードを受け入れるアプリケーション *(* 購読者チャネル *)*

これらの設定により、接続システムでサポートされている場合には、双方向のパスワード同期が可能になります。

パスワードの信頼されたソースについては、ビジネスポリシーに合わせて設定を調整できます。たとえば、接続システムがパスワードを取得するが発行しないようにする場合は、［パスワードを受け入れるアプリケーション (購読者チャネル)］のみを選択します。

4 ［パスワード同期に配布パスワードを使用する］のオプションを使用し、パスワード同期の NMAS パスワードポリシーを適用させるか無視するかを指定します。

5 (オプション) パスワードポリシーを適用させるように指定した場合、パスワードがポリシーに準拠しない場合に接続システムのパスワードを Identity Manager がリセットするかどうかも指定します。

6 (オプション) 必要に応じ、次のオプションを選択します。

- 電子メール経由でユーザにパスワード同期障害を通知する

  電子メール通知には、eDirectory ユーザオブジェクトのインターネット電子メールアドレス属性の入力が必要です。

  電子メール通知は、他に影響を与えません。これらは、電子メールをトリガした XML ドキュメントの処理には影響しません。失敗した場合、操作自体が再試行されない限り、再試行されません。ただし、電子メール通知のデバッグメッセージはトレースファイルに書き込まれます。

ドライバ環境設定

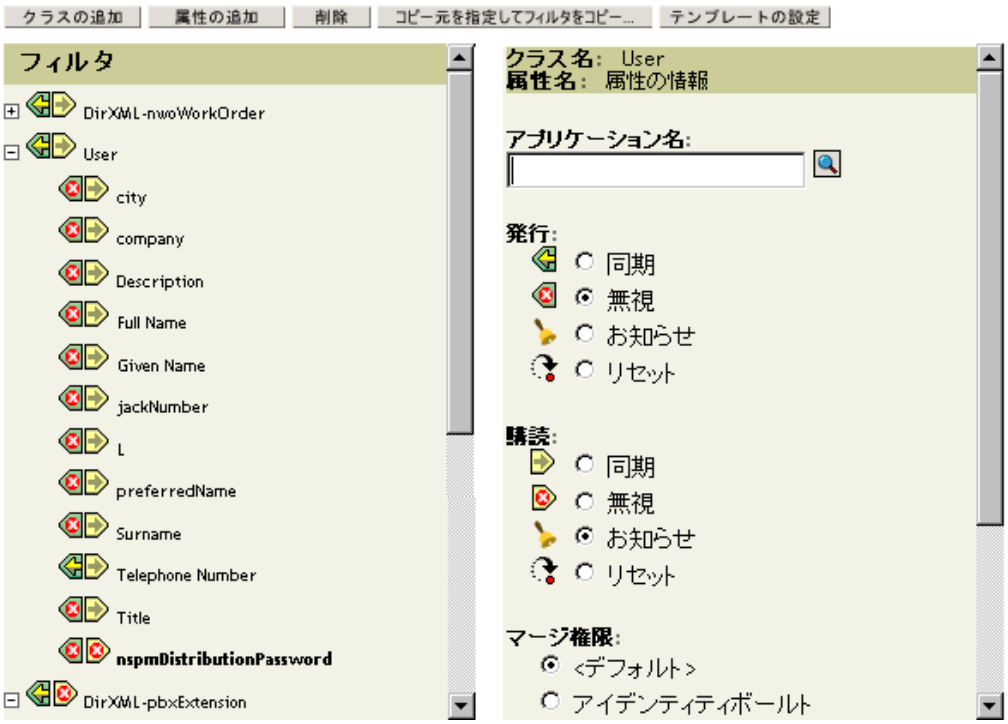
1 必要な Identity Manager スクリプトパスワード同期ポリシーが、パスワード同期に使用する各ドライバのドライバ環境設定に含まれていることを確認します。

ポリシーは、ドライバ環境設定の正しい位置に正しい順序で記述されている必要があります。ポリシーのリストについては、90 ページのセクション 5.3.4「ドライバ環境設定で必要なポリシー」を参照してください。

Identity Manage のサンプル環境設定には、すでにポリシーが含まれています。既存のドライバをアップグレードする場合は、100 ページのセクション 5.7「パスワード同期をサポートするための、既存のドライバ環境設定のアップグレード」のステップを使用してポリシーを追加できます。

2 nspmDistributionPassword 属性について、フィルタを正しく設定します。

- 発行者チャネルについては、ドライバフィルタがすべてのオブジェクトクラスの nspmDistributionPassword 属性を無視するよう設定します。
- 購読者チャネルについては、ドライバフィルタがパスワードの変更を受信するすべてのオブジェクトクラスの nspmDistributionPassword 属性を通知するよう設定します。



3 nspmDistributionPassword 属性が［お知らせ］に設定されているすべてのオブジェクトでは、ドライバフィルタの公開鍵および秘密鍵の属性の両方を［無視］に設定します。

4 パスワードのセキュリティを確保するには、Identity Manager のオブジェクトへの権利を持つユーザを制御していることを確認します。

シナリオ 3 のトラブルシューティング

- 130 ページの 「シナリオ 3 のフローチャート」
- 132 ページの 「eDirectory へのログインのトラブルシューティング」
- 133 ページの 「パスワードを取得する別の接続システムへのログインのトラブルシューティング」
- 133 ページの 「パスワードのエラーについての電子メールが生成されない」
- 134 ページの 「[パスワードステータスの確認] を使用した場合のエラー」
- 134 ページの 「DSTrace の便利なコマンド」

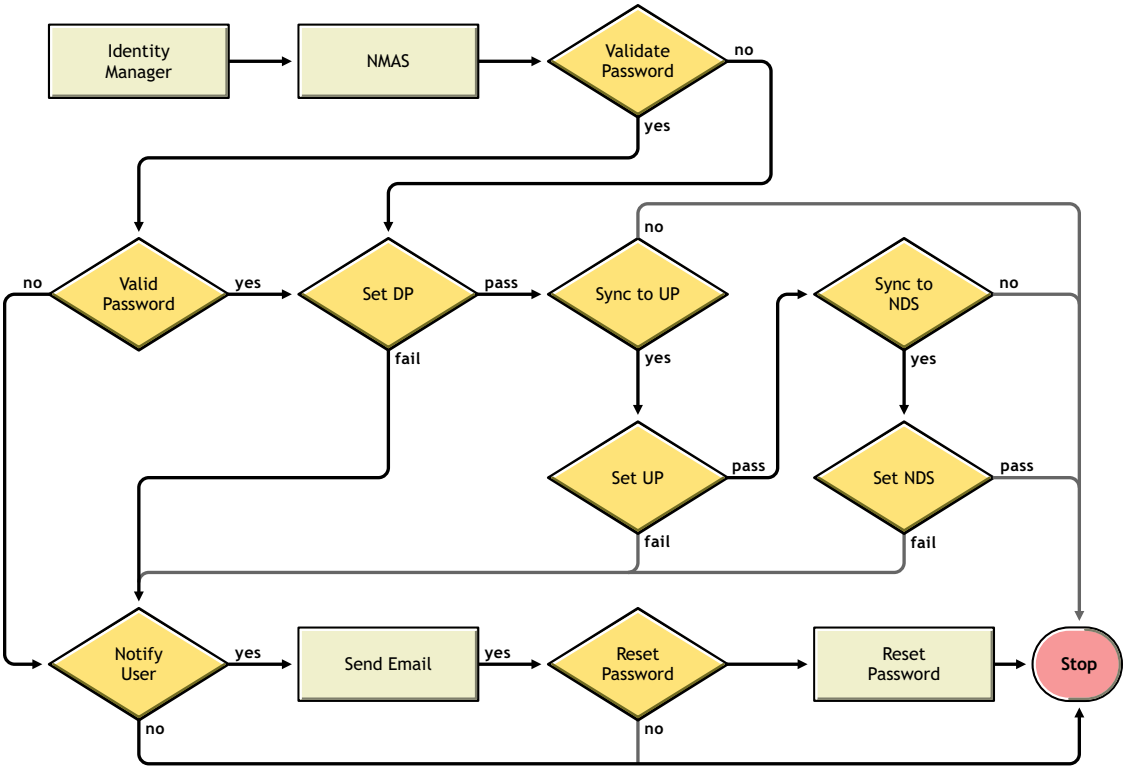
159 ページのセクション 5.13「パスワード同期のトラブルシューティング」のヒントも参照してください。

シナリオ 3 のフローチャート

次のフローチャートは、NMAS が Identity Manager から受信するパスワードの処理の方法を示しています。このシナリオではパスワードが配布パスワードに同期され、NMAS では次が決定されます。

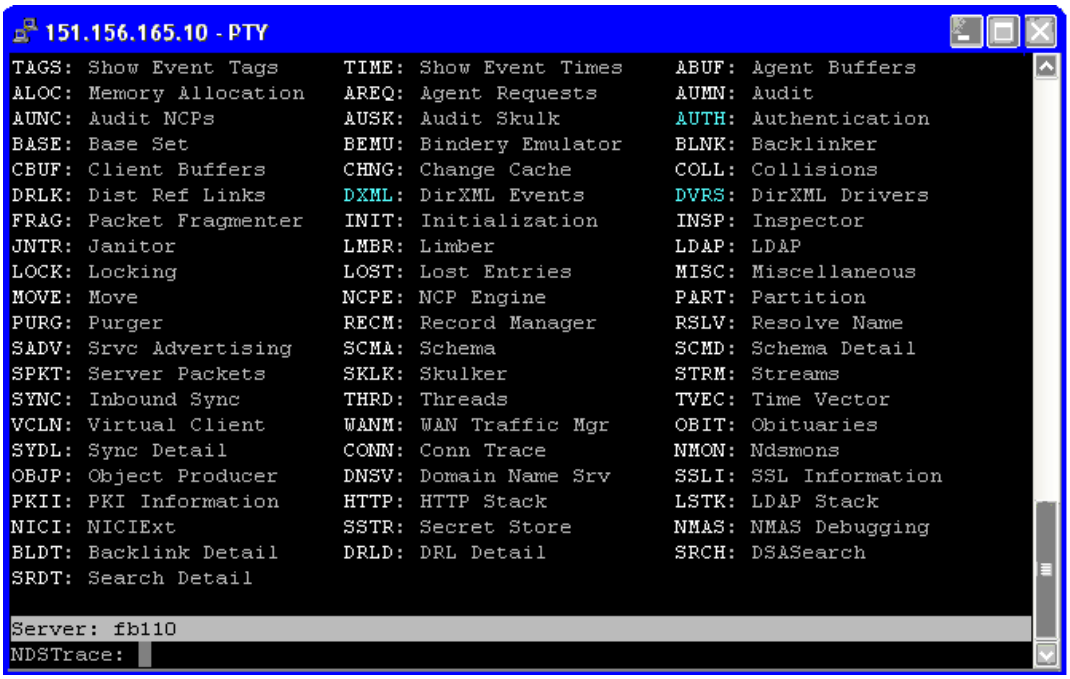
- パスワードポリシーのルールに対して着信パスワードを検証する必要があることを指定したかどうかに基づいた、パスワードの処理方法 (ユニバーサルパスワードおよび高度なパスワードルールが有効になっている場合)。
- ユニバーサルパスワードとその他のパスワードとを同期するためのパスワードポリシーに、どのようなその他の設定があるのか。

図 5-12 配布パスワードに同期される *Identity Manager* のパスワード



- DSTrace で、［+AUTH］、［+DXML］、および［+DVRS］の設定をオンにします。

図 *5-13* *DSTrace コマンド*



- <password>または<modify-password>の要素がIdentity Managerに渡されていることを確認します。確認するには、DSTrace 画面またはファイルのトレースオプションが、最初の項目で説明したとおり、オンになっていることを確かめます。
- NMAS パスワードポリシーのルールに従い、パスワードが有効であることを確認します。
- NMAS パスワードポリシーの設定と割り当てを確認します。ポリシーをユーザに直接割り当て、正しいポリシーが使用されるようにします。
- ドライバの［パスワード同期］ページで、［パスワードを受理する Identity Manager(発行者チャネル)］が選択されていることを確認します。
- ［パスワードポリシー］で、［ユニバーサルパスワードの設定時に配布パスワードを同期する］が選択されていることを確認します。
- ［パスワードポリシー］で、必要に応じて［ユニバーサルパスワードの設定時に NDS パスワードを同期する］が選択されていることを確認します。
- ユーザが Novell Client または ConsoleOne を通じてログインしている場合は、バージョンを確認します。ユニバーサルパスワードが NDS パスワードに同期されていない場合、従来の Novell Client および ConsoleOne からは、アイデンティティボールトにログインできないことがあります。

  ユニバーサルパスワードを認識する Novell Client および ConsoleOne のバージョンが利用できます。『*NMAS 3.0 Administration Guide* (http://www.novell.com/documentation/nmas30/index.html)』を参照してください。

- レガシーユーティリティの中にはNDSパスワードを使用して認証するものがありますが、ユニバーサルパスワードが NDS パスワードに同期されていない場合には、それらもアイデンティティボールトにはログインできません。ほとんどのユーザは NDS パスワードを使用せず、管理者またはヘルプデスクのユーザがレガシーユーティリティへの認証を必要とする場合は、ヘルプデスクのユーザには異なるパスワードポリシーを使用し、異なるユニバーサルパスワード同期のオプションを指定できるようにします。

パスワードを取得する別の接続システムへのログインのトラブルシューティング

この節では、接続システムが Identity Manager にパスワードを発行しているけれども、パスワードを取得するもう 1 つの接続システムが発行側のシステムからの変更を取得していないように思われる場合の、トラブルシューティングについて説明します。この関係は、第 2 の接続システムとも呼ばれ、第 1 の接続システムから Identity Manager を通じてパスワードを取得することを意味します。

- DSTrace の［+DXML］および［+DVRS］の設定をオンにし、Identity Manager のルール処理および可能性のあるエラーを確認します。
- ドライバの Identity Manager のトレースレベルを［3］に設定します。
- ［パスワード同期］ページの［パスワードを受理する Identity Manager(発行者チャネル)］オプションが選択されていることを確認します。
- ［パスワードポリシー］で、［ユニバーサルパスワードの設定時に配布パスワードを同期する］がオフになっていることを確認します。

  Identity Manager は、配布パスワードを使用し、パスワードを接続システムに同期します。ユニバーサルパスワードは、この同期方法の配布パスワードに同期させる必要があります。
- ドライバフィルタの nspmDistributionPassword 属性を確認します。
- <password> 要素 (追加の場合) または <modify-password> 要素が、nspmDistributionPassword 属性の追加操作または変更操作に変換されていることを確認します。確認するには、DSTrace 画面またはファイルのオプションが、最初の項目で説明したとおり、オンになっていることを確かめます。
- Identity Manager スクリプトパスワードポリシーが、90 ページのセクション 5.3.4「ドライバ環境設定で必要なポリシー」で説明されているとおり、ドライバ環境設定の正しい位置と順序にあることを確認します。
- アイデンティティボールトのパスワードポリシーを、接続システムにより適用されるパスワードポリシーと比較し、互換性があることを確認します。

パスワードのエラーについての電子メールが生成されない

- DSTrace の［+DXML］の設定をオンにし、Identity Manager のルール処理を確認します。
- ドライバの Identity Manager のトレースレベルを［3］に設定します。
- 電子メールを生成するルールが選択されていることを確認します。
- アイデンティティボールトブジェクトを検証し、インターネット電子メールアドレス属性に正しい値が含まれていることを確認します。
- ［Notification Configuration (通知設定)］タスクで、SMTP サーバと電子メールテンプレートが設定されていることを確認します。147 ページのセクション 5.12「電子メール通知の設定」を参照してください。

電子メール通知は、他に影響を与えません。これらは、電子メールをトリガした XML ドキュメントの処理には影響しません。失敗した場合、操作自体が再試行されない限り、再試行されません。電子メール通知のデバッグメッセージはトレースファイルに書き込まれます。

［パスワードステータスの確認］を使用した場合のエラー

iManager の［パスワードステータスの確認］タスクにより、ドライバで［オブジェクトパスワードの確認］アクションが実行されます。

- 接続システムがパスワードのチェック機能をサポートすることを確認してください。83 ページのセクション 5.2「パスワード同期をサポートする接続システム」を参照してください。

  接続システムがパスワードチェック機能をサポートするようドライバマニフェストに示されてない場合は、iManager からこの機能を使用することはできません。
- ［オブジェクトパスワードの確認］が -603 を返す場合、アイデンティティボールトブジェクトに nspmDistributionPassword 属性が含まれていません。ドライバフィルタ、および［パスワードポリシー］の［Synchronize Universal to Distribution (ユニバーサルパスワードの設定時に配布パスワードを同期する)］オプションを確認します。
- ［オブジェクトパスワードの確認］が「同期されていません」を返す場合、ドライバ環境設定に Identity Manager パスワード同期の適切なポリシーが含まれていることを確認します。
- アイデンティティボールトのパスワードポリシーを、接続システムにより適用されるパスワードポリシーと比較し、互換性があることを確認します。
- ［オブジェクトパスワードの確認］は、配布パスワードを確認します。配布パスワードが更新されていない場合、［オブジェクトパスワードの確認］によって、パスワードが同期されていることがレポートされないことがあります。
- アイデンティティボールトでは、［パスワードステータスの確認］は、ユニバーサルパスワードではなく NDS パスワードを確認することに注意してください。つまり、ユーザのパスワードポリシーで NDS パスワードをユニバーサルパスワードに同期するよう指定されていない場合は、必ず、パスワードが同期されていないとレポートされます。配布パスワードおよび接続システムのパスワードは同期されないことがありますが、NDS パスワードおよび配布パスワードの両方がユニバーサルパスワードに同期されない限り、［パスワードステータスの確認］は正確とは限りません。

DSTrace の便利なコマンド

+DXML: Identity Manager ルール処理および可能性のあるエラーメッセージを表示する

+DVRS: Identity Manager ドライバのメッセージを表示する

+AUTH: NDS パスワードの変更を表示する

5.8.5 シナリオ 4: トンネリング —Identity Manager での配布パスワードの更新による、アイデンティティボールトではなく接続システムの同期

Identity Manager では、アイデンティティボールトのパスワードはそのままにしながら、接続システム間でパスワードを同期できます。これは「トンネリング」と呼ばれます。

このシナリオでは、Identity Manager が配布パスワードを直接更新します。このシナリオは 124 ページのセクション 5.8.4「シナリオ 3: Identity Manager での配布パスワードの更新による、アイデンティティボールトおよび接続システムの同期」とほとんど同じです。異なる点は、ユニバーサルパスワードおよび配布パスワードは同期されないことです。これは、NMAS パスワードポリシーを使用しないか、または［ユニバーサルパスワードの設定時に配布パスワードを同期する］オプションを無効にしたパスワードポリシーを使用して実行します。

- 135 ページの 「シナリオ 4 の長所と短所」
- 136 ページの 「シナリオ 4 の設定」
- 137 ページの 「シナリオ 4 のトラブルシューティング」

シナリオ 4 の長所と短所

表 *5-14* トンネリングの長所

長所	短所
アイデンティティボールトのパスワードはそのままにしながら、接続システム間でパスワードを同期できます。 パスワードポリシーは必要ありません。 パスワードポリシーを使用している場合、ユニバーサルパスワードを有効にする必要はありません。ただし、使用する環境はユニバーサルパスワードをサポートする必要があります。 接続システムが iManager の［パスワードステータスの確認］タスクをサポートする場合、このシナリオも［パスワードステータスの確認］タスクをサポートします。 パスワード同期が失敗した場合に通知を送信するよう指定できます。 接続システムのパスワードがパスワードポリシーに準拠しない場合、それをリセットできます。 ユニバーサルパスワードおよび高度なパスワードルールが有効になっている場合、パスワードポリシーを適用するよう指定した際はパスワードポリシーが適用され、接続システムのパスワードをリセットできます。	ユニバーサルパスワードおよび高度なパスワードルールが無効になっている場合、パスワードポリシーは適用されず、接続システムのパスワードはリセットできません。

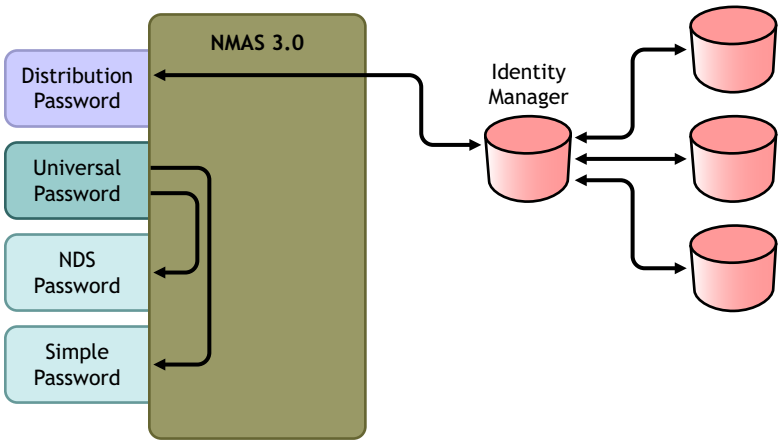
このシナリオの図は、次のフローを示します。

1. パスワードが、Identity Manager を通って来る。
2. Identity Manager が NMAS と通信して、配布パスワードを直接更新する。
3. Identity Manager は配布パスワードを使用し、パスワードを受け入れるよう指定した接続システムにパスワードを配布します。

このシナリオの重要な点は、NMAS パスワードポリシーで、[Synchronize Universal Password with Distribution Password (ユニバーサルパスワードの設定時に配布パスワードを同期する)] が無効になっていることです。配布パスワードとユニバーサルパスワードは同期されないので、Identity Manager は、アイデンティティボールトのパスワードはそのままにしながら、接続システム間でパスワードを同期します。

この図では複数の接続システムが Identity Manager に接続しているように示されていますが、接続システムのドライバごとに設定を作成することに注意してください。

図 5-14 *Identity Manager* での配布パスワードの更新によるトンネリング



シナリオ 4 の設定

この種類のパスワード同期を設定するには、次を設定します。

- 136 ページの 「ユニバーサルパスワードの展開」
- 136 ページの 「パスワードポリシーの設定」
- 137 ページの 「パスワード同期の設定」
- 137 ページの 「ドライバ環境設定」

ユニバーサルパスワードの展開

パスワードポリシーでユニバーサルパスワードを有効にする必要はありません。ただし、現在の環境で、ユニバーサルパスワードをサポートする eDirectory 8.7.3 を使用していることが必要です。94 ページのセクション 5.4「Identity Manager の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。

パスワードポリシーの設定

この方法では、アイデンティティボールトユーザに対するパスワードポリシーの設定は必要ありません。

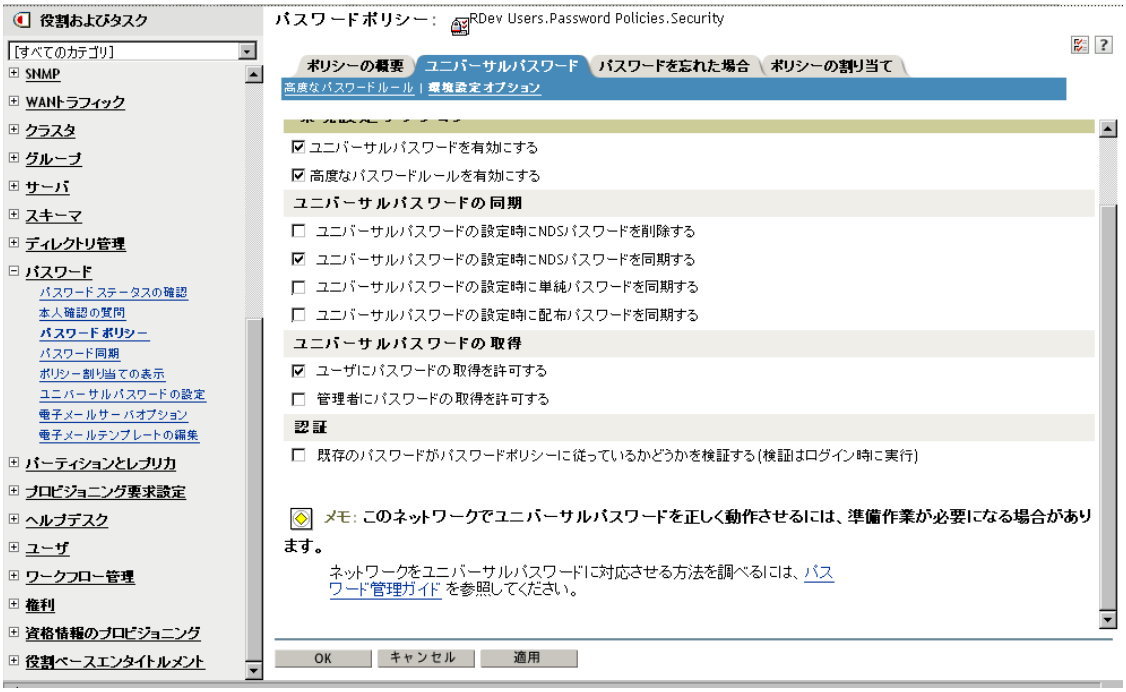
ただし、パスワードポリシーを使用する場合は、次の作業を実行する必要があります。

1 次のオプションがオフになっていることを確認します。

- ユニバーサルパスワードの設定時に配布パスワードを同期する

  アイデンティティボールトのパスワードに影響を与えずにパスワードのトンネリングを実行するには、これが重要です。ユニバーサルパスワードを配布パスワー

ドと同期しないことによって、接続システムに対して Identity Manager が使用する場合にのみ、配布パスワードをそのままにできます。Identity Manager は、アイデンティティボールトのパスワードには影響を与えずに接続システム間でパスワードを配布するルートとして機能します。



2 必要に応じてパスワードポリシーのその他の設定を行います。

パスワードポリシー内のその他のパスワード設定はオプションです。

パスワード同期の設定

124 ページのセクション 5.8.4「シナリオ 3: Identity Manager での配布パスワードの更新による、アイデンティティボールトおよび接続システムの同期」の「パスワード同期の設定」と同じ設定を使用します。

ドライバ環境設定

124 ページのセクション 5.8.4「シナリオ 3: Identity Manager での配布パスワードの更新による、アイデンティティボールトおよび接続システムの同期」の「ドライバ環境設定」と同じ設定を使用します。

シナリオ 4 のトラブルシューティング

パスワード同期がトンネリングのための設定になっている場合、配布パスワードは、ユニバーサルパスワードおよび NDS パスワードと異なるものになります。

- 138 ページの 「パスワードを取得する別の接続システムへのログインのトラブルシューティング」
- 138 ページの 「パスワードのエラーについての電子メールが生成されない」
- 139 ページの 「[パスワードステータスの確認] を使用した場合のエラー」
- 139 ページの 「DSTrace の便利なコマンド」

159 ページのセクション 5.13「パスワード同期のトラブルシューティング」のヒントも参照してください。

パスワードを取得する別の接続システムへのログインのトラブルシューティング

この節では、接続システムが Identity Manager にパスワードを発行しているけれども、パスワードを取得するもう 1 つの接続システムが発行側のシステムからの変更を取得していないように思われる場合の、トラブルシューティングについて説明します。この関係は、第 2 の接続システムとも呼ばれ、第 1 の接続システムから Identity Manager を通じてパスワードを取得することを意味します。

- DSTrace の［+DXML］および［+DVRS］の設定をオンにし、Identity Manager のルール処理および可能性のあるエラーを確認します。
- ドライバの Identity Manager のトレースレベルを［3］に設定します。
- ［パスワード同期］ページの［パスワードを受理する Identity Manager(発行者チャネル)］オプションが選択されていることを確認します。
- ［パスワードポリシー］で、［ユニバーサルパスワードの設定時に配布パスワードを同期する］がオフになっていることを確認します。

  Identity Manager は、配布パスワードを使用し、パスワードを接続システムに同期します。ユニバーサルパスワードは、この同期方法の配布パスワードに同期させる必要があります。
- ドライバフィルタの nspmDistributionPassword 属性が正しく設定されていることを確認します。
- <password> 要素 (追加の場合) と <modify-password> 要素が、nspmDistributionPassword 属性の追加操作または変更操作に変換されていることを確認します。確認するには、DSTrace 画面またはファイルのトレースオプションが、最初の項目で説明したとおり、オンになっていることを確かめます。
- Identity Manager スクリプトパスワードポリシーが、90 ページのセクション 5.3.4「ドライバ環境設定で必要なポリシー」で説明されているとおり、ドライバ環境設定の正しい位置と順序にあることを確認します。
- アイデンティティボールトのパスワードポリシーを、接続システムにより適用されるパスワードポリシーと比較し、互換性があることを確認します。

パスワードのエラーについての電子メールが生成されない

- DSTrace の［+DXML］の設定をオンにし、Identity Manager のルール処理を確認します。
- ドライバの Identity Manager のトレースレベルを［3］に設定します。
- 電子メールを生成するルールが選択されていることを確認します。
- アイデンティティボールトブジェクトを検証し、インターネット電子メールアドレス属性に正しい値が含まれていることを確認します。
- ［Notification Configuration (通知設定)］タスクで、SMTP サーバと電子メールテンプレートを確認します。147 ページのセクション 5.12「電子メール通知の設定」を参照してください。

電子メール通知は、他に影響を与えません。これらは、電子メールをトリガした XML ドキュメントの処理には影響しません。失敗した場合、操作自体が再試行されない限り、再試行されません。電子メール通知のデバッグメッセージはトレースファイルに書き込まれます。

［パスワードステータスの確認］を使用した場合のエラー

iManager の［パスワードステータスの確認］タスクにより、ドライバで［オブジェクトパスワードの確認］アクションが実行されます。

- 接続システムがパスワードのチェック機能をサポートすることを確認してください。83 ページのセクション 5.2「パスワード同期をサポートする接続システム」を参照してください。

  接続システムがパスワードチェック機能をサポートするようドライバマニフェストに示されてない場合は、iManager からこの機能を使用することはできません。
- ［オブジェクトパスワードの確認］アクションが -603 を返す場合、アイデンティティボールトブジェクトに nspmDistributionPassword 属性が含まれていません。Identity Manager 属性フィルタ、および［パスワードポリシー］の［Synchronize Universal to Distribution (ユニバーサルパスワードの設定時に配布パスワードを同期する)］オプションを確認します。
- ［オブジェクトパスワードの確認］アクションが「同期されていません」を返す場合、ドライバ環境設定に Identity Manager パスワード同期の適切なポリシーが含まれていることを確認します。
- アイデンティティボールトのパスワードポリシーを、接続システムにより適用されるパスワードポリシーと比較し、互換性があることを確認します。
- ［オブジェクトパスワードの確認］アクションは、配布パスワードを確認します。配布パスワードが更新されていない場合、［オブジェクトパスワードの確認］によって、パスワードが同期されていることがレポートされないことがあります。

DSTrace の便利なコマンド

+*DXML*: Identity Manager ルール処理および可能性のあるエラーメッセージを表示する

+*DVRS*: Identity Manager ドライバのメッセージを表示する

+*AUTH*: NDS パスワードの変更を表示する

+*DCLN*: NDS DClient メッセージを表示する

5.8.6 シナリオ 5: アプリケーションパスワードの単純パスワードへの同期

このシナリオは、パスワード同期機能の特別な使用方法です。Identity Manager および NMAS を使用し、接続システムからパスワードを取得して、直接アイデンティティボールトの単純パスワードに同期できます。接続システムがハッシュされたパスワードのみを提供する場合、ハッシュを元に戻さずに、単純パスワードに同期できます。他のアプリケーションは、同じクリアテキスト、あるいは LDAP または Novell Client によりハッシュされたパスワードを使用し、アイデンティティボールトに対して認証できます。NMAS コンポーネントは、単純パスワードをログインメソッドとして使用するよう設定されます。

接続システムのパスワードがクリアテキストである場合、そのまま接続システムからアイデンティティボールトの単純パスワードストアに発行できます。

接続システムがハッシュされたパスワード (MD5、SHA、SHA1、または UNIX Crypt がサポートされています) のみを提供する場合、それらのパスワードは、{MD5} のようにハッシュの種類を指定して単純パスワードに発行する必要があります。

同じパスワードで認証する別のアプリケーションについては、ユーザのパスワードを取得し LDAP を使用して単純パスワードに対して認証するよう、アプリケーションをカスタマイズする必要があります。

NMAS は、アプリケーションから取得したパスワードの値と、単純パスワードの値を比較します。単純パスワードとして保存されているパスワードがハッシュ値である場合、NMAS は、アプリケーションのパスワードの値を使用して正しいタイプのハッシュ値を生成してから比較します。アプリケーションから取得したパスワードと単純パスワードが同一である場合、NMAS はユーザを認証します。

このシナリオでは、ユニバーサルパスワードは使用できません。

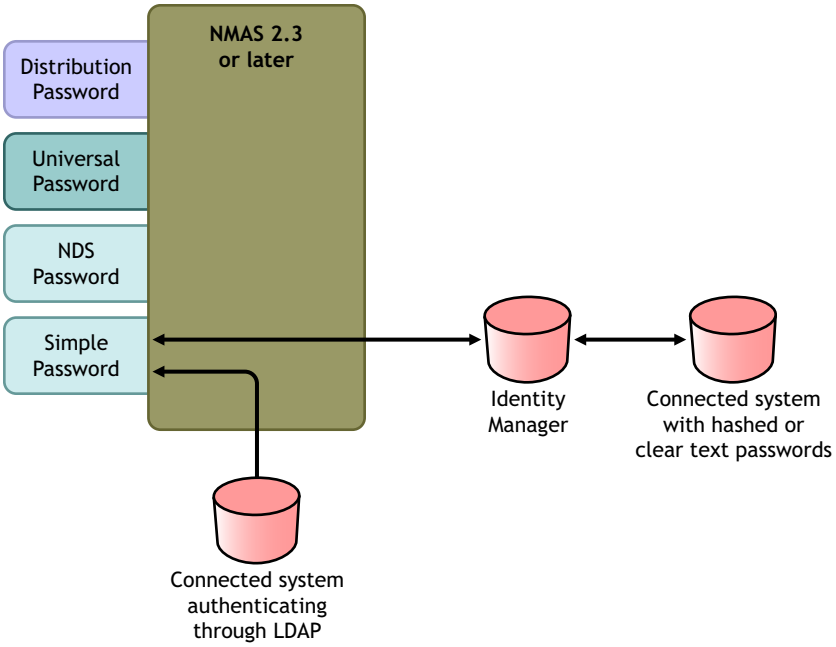
- 140 ページの 「NDS パスワードへの同期の長所」
- 141 ページの 「シナリオ 5 の設定」

NDS パスワードへの同期の長所

表 *5-15* *NDS* パスワードへの同期の長所

長所	短所
◆ 単純パスワードを直接更新できます。 ◆ ハッシュされたパスワードを同期し、ハッシュを戻さずに、複数のアプリケーションでの認証に使用できます。	◆ ユニバーサルパスワードは使用できません。 ◆ パスワードを忘れた場合の機能およびパスワードセルフサービス機能は、NDS パスワードをサポートする程度では使用できますが、単純パスワードについては使用できません。 ◆ [ユニバーサルパスワードの設定] タスクはユニバーサルパスワードに依存しているため、管理者はそのタスクを使用してアイデンティティボールトのユーザのパスワードを設定することはできません。

図 *5-15* *NDS* パスワードへの同期



シナリオ 5 の設定

- 141 ページの 「パスワードポリシーの設定」
- 141 ページの 「パスワード同期の設定」
- 142 ページの 「ドライバ環境設定」

パスワードポリシーの設定

このシナリオでは、ユーザに対するパスワードポリシーの設定は必要ありません。ユニバーサルパスワードは使用できません。

パスワード同期の設定

このシナリオでは、Identity Manager スクリプトを使用して、SAS:Login Configuration 属性を直接変更します。つまり、iManager の［パスワード同期］ページを使用して設定される、パスワード同期のグローバル構成値 (GCV) に影響はありません。

1 フィルタの SAS:Login Configuration 属性が、発行者チャネルおよび購読者チャネルの両方に対して［同期］に設定されていることを確認します。

2 ドライバポリシーで、接続システムからのパスワードを発行するよう設定します。

3 ハッシュされたパスワードについては、ドライバポリシーで、(ハッシュのタイプがアプリケーションからまだ提供されていない場合は) ハッシュのタイプを先頭に付けるよう設定します。

- {MD5}*hashed_password*

  このパスワードは Base 64 でエンコードされています。

- {SHA}*hashed_password*

  このパスワードは Base 64 でエンコードされています。

- {CRYPT}*hashed_password*

クリアテキストパスワードおよび Unix Crypt パスワードハッシュは、Base 64 でエンコードされていません。

4 パスワードを単純パスワードに設定するには、SAS:Login Configuration 属性を変更するようドライバポリシーを設定します。

次の例では、変更操作内で modify-attr 要素を使用して、単純パスワードを MD5 でハッシュされたパスワードに変更する方法を示しています。

```
<modify-attr attr-name="SAS:Login Configuration> <add-value>
<value>{MD5}2tEgXrIHtAnGHOzH3ENslg==</value> </add-value> </
```

```
modify-attr>
```

クリアテキストパスワードについては、次の例に従います。

```
<modify-attr attr-name="SAS:Login Configuration> <add-value>
<value>clearpwd</value> </add-value> </modify-attr>
```

追加操作については、add-attr 要素に次のどちらかを含めます。

```
<add-attr attr-name="SAS:Login Configuration>
<value>{MD5}2tEgXrIHtAnGHOzH3ENslg==</value> </add-attr>
```

または

```
<add-attr attr-name="SAS:Login Configuration> <value>clearpwd</
value> </add-attr>
```

5.9 パスワードフィルタの設定

接続システムの中には、ユーザの実際のパスワードを Identity Manager に提供できるものもあります。

Active Directory、NIS、および NT ドメインでパスワードをキャプチャするには、接続システムにパスワードフィルタをインストールするための設定を行う必要があります。

- 143 ページのセクション 5.9.1「Active Directory および NT ドメインのためのパスワード同期のフィルタの設定」
- 144 ページのセクション 5.9.2「NIS のためのパスワード同期のフィルタの設定」

5.9.1 Active Directory および NT ドメインのためのパスワード同期のフィルタの設定

この情報は、Identity Manager Drivers (http://www.novell.com/documentation/dirxmldrivers/index.html) にある Active Directory および NT ドメイン用 Identity Manager ドライバのドライバ実装ガイドの「Password Synchronization」のセクションにあります。

Active Directory および NT ドメイン用 Identity Manager ドライバは、1 台の Windows コンピュータにのみインストールする必要があります。他のドメインコントローラにはドライバのインストールは必要ありませんが、Identity Manager に送信するパスワードをキャプチャするために、pwfilter.dll ファイルをドメインコントローラごとにインストールする必要があります。

設定と管理を簡素化するために、ドライバがインストールされている Windows コンピュータからすべてのドメインコントローラに対してこの作業を実施するためのユーティリティが用意されています。

5.9.2 NIS のためのパスワード同期のフィルタの設定

NIS 3.0 用の Identity Manager ドライバは、ファイル、NIS、および NIS+ の 3 つの UNIX 認証データストアで動作します。パスワードをキャプチャし NIS 対応の Identity Manager ドライバに送信するために、PAM モジュールが用意されています。

NIS ドライバのための PAM モジュールの展開については、Identity Manager Drivers (http://www.novell.com/documentation/lg/dirxmldrivers/index.html) にある『*Identity Manager Driver for NIS Implementation Guide*』で説明しています。

5.10 パスワード同期の管理

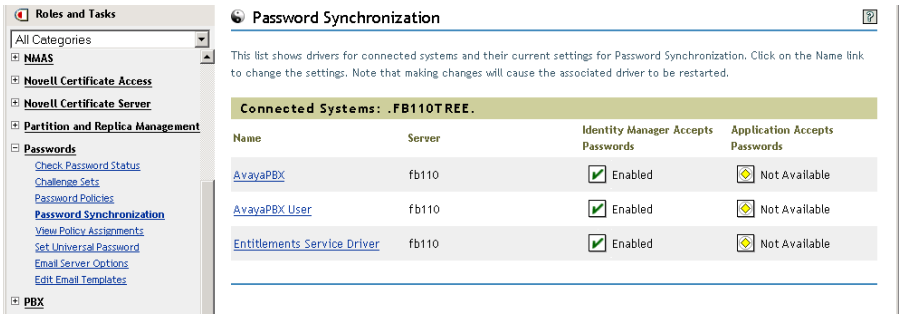
- 144 ページの 「システム間のパスワードフローの設定」
- 146 ページの 「接続システムへのパスワードポリシーの適用」
- 146 ページの 「eDirectory パスワードを同期されたパスワードとは別にそのままにしておく方法」

5.10.1 システム間のパスワードフローの設定

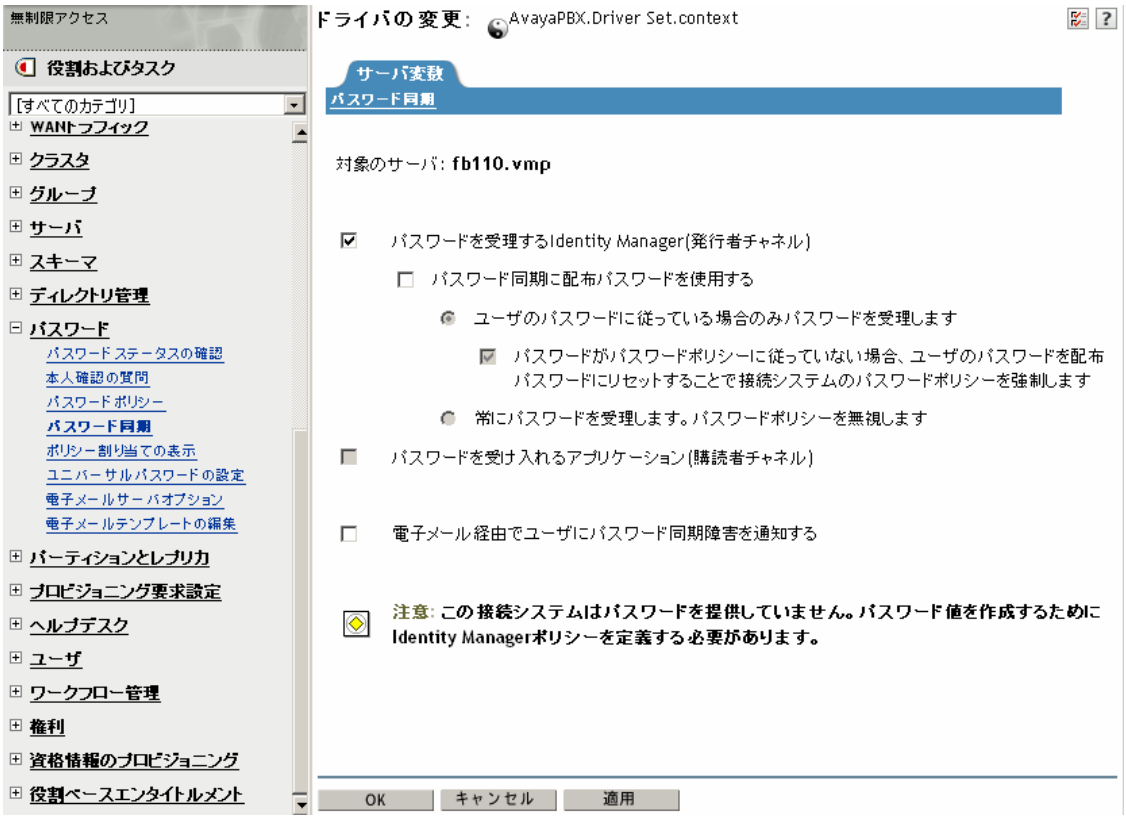
パスワードを受け入れまたは発行するためにシステムがどのように設定されているのかを表示するには、次のように操作します

1. iManager で、［パスワード］>［パスワード同期］の順に選択します。
2. 接続システムのドライバを検索します。

検索結果には、Identity Manager および接続システム間のパスワードフローについての設定が表示されます。



設定を変更するには、接続システムのドライバ名をクリックします。



［ドライバの変更］ページでは、Identity Manager が受信するパスワードにパスワードポリシーを適用するかどうかと、接続システムにパスワードポリシーを適用して接続システムのパスワードをリセットするかどうかを設定できます。

このページの設定は、サーバごとに保存される GCV です。87 ページのセクション 5.3.3「グローバル構成値を使用したパスワード同期の制御」を参照してください。

5.10.2 接続システムへのパスワードポリシーの適用

［高度なパスワードルール］および Identity Manager のパスワード同期を使用している場合は、次を実行することもお勧めします。

1 すべての接続システムのパスワードポリシーを調査します。
2 高度なパスワードルールが接続システム上のパスワードポリシーと互換性があることを確認します。

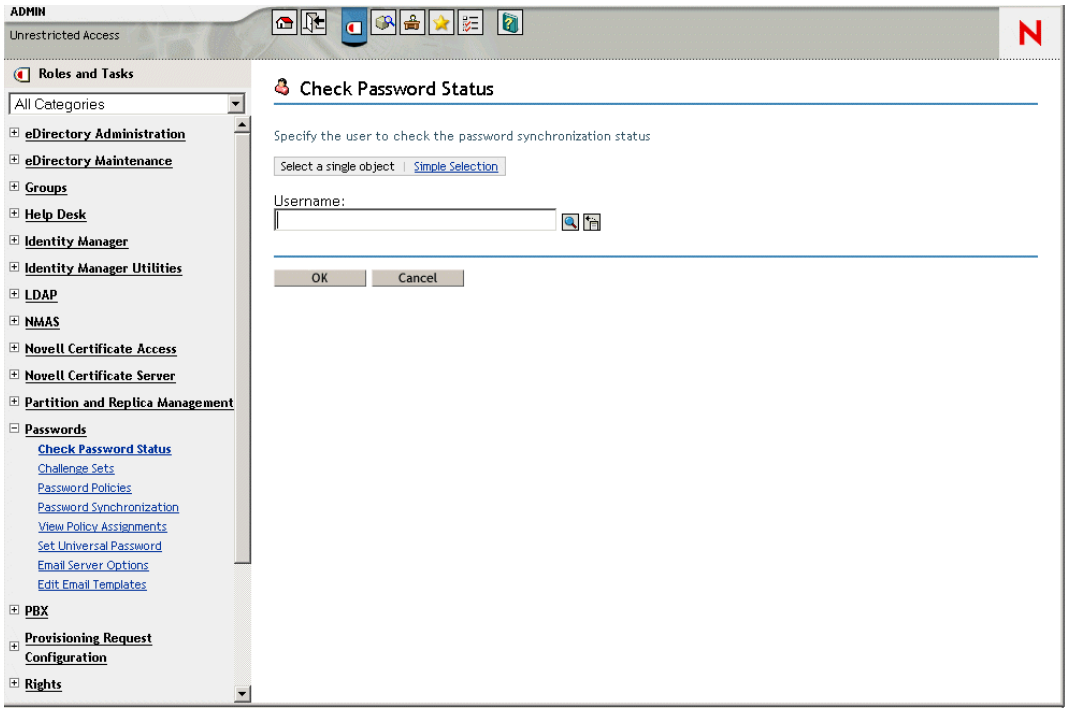
5.10.3 eDirectory パスワードを同期されたパスワードとは別にそのままにしておく方法

このシナリオについては、134 ページのセクション 5.8.5「シナリオ 4: トンネリング — Identity Manager での配布パスワードの更新による、アイデンティティボールトではなく接続システムの同期」で説明しています。

5.11 ユーザのパスワード同期ステータスの確認

特定のユーザの配布パスワードが接続システムのパスワードと同じかどうかを判断できます。

1 iManager で、［パスワード］>［パスワードステータスの確認］の順に選択します。



2 ユーザを参照して選択します。

［パスワードステータスの確認］タスクにより、ドライバで［オブジェクトパスワードの確認］アクションが実行されます。

すべてのドライバがパスワードチェックをサポートするわけではありません。パスワードチェックをサポートするドライバには、ドライバのマニフェストにパスワードチェック機能が含まれている必要があります。iManager では、マニフェストにこの機能が含まれていないドライバにパスワードチェックの操作を送信できません。

［オブジェクトパスワードの確認］アクションは、配布パスワードを確認します。配布パスワードが更新されていない場合、［オブジェクトパスワードの確認］によって、パスワードが同期されていないとレポートされることがあります。

次のいずれかが発生した場合、配布パスワードは更新されません。

- 111 ページのセクション 5.8.2「シナリオ 1: NDS パスワードを使用した、2 つのアイデンティティボールト間の同期」で説明する同期化方法を使用している場合。
- ユニバーサルパスワードを同期している (114 ページのセクション 5.8.3「シナリオ 2: ユニバーサルパスワードを使用した同期」を参照) が、ユニバーサルパスワードを配布パスワードに同期するパスワードポリシーの設定オプションを有効にしていない場合。

注 **:** アイデンティティボールトでは、［パスワードステータスの確認］アクションは、ユニバーサルパスワードではなく NDS パスワードを確認することに注意してください。したがって、ユーザのパスワードポリシーで NDS パスワードをユニバーサルパスワードに同期するよう指定されていない場合は、必ず、パスワードが同期されていないとレポートされます。配布パスワードおよび接続システムのパスワードは同期されないことがありますが、NDS パスワードおよび配布パスワードの両方がユニバーサルパスワードに同期されない限り、［パスワードステータスの確認］は正確とは限りません。

5.12 電子メール通知の設定

iManager のタスクを使用すると、電子メールサーバを指定したり、電子メール通知機能のテンプレートをカスタマイズしたりできます。

パスワード同期およびパスワードセルフサービスから自動化された電子メールをユーザに送信するために、電子メールのテンプレートが提供されています。

テンプレートは作成しません。テンプレートを使用するアプリケーションによって提供されます。電子メールテンプレートは、アイデンティティボールトのテンプレートオブジェクトで、通常は、ツリーのルートにあるセキュリティコンテナに配置されています。これはアイデンティティボールトブジェクトですが、iManager を介してのみ編集する必要があります。

これは、モジュラフレームワークです。電子メールテンプレートを使用する新しいアプリケーションが追加された場合、テンプレートは、それを使用するアプリケーションとともにインストールできます。

iManager での選択に基づき、電子メールを送信するかどうかが制御されます。パスワードを忘れた場合、［ユーザにパスワードを電子メールで送信する］、または［ユーザにヒントを送信する］を選択した場合のみ、電子メール通知が送信されます。『*Password Management Administration Guide* (http://www.novell.com/documentation/password_management/index.html)』の「Providing Users with Forgotten Password Self-Service」を参照してください。

［電子メール経由でユーザにパスワード同期障害を通知する］を選択した場合、失敗したパスワード同期の操作のみ、および指定したドライバに対してのみ電子メールを送信するようにパスワード同期が設定されます。

図 *5-16* パスワード同期の設定

SMTP 認証情報がドライバポリシーに含まれていることも確認する必要があります。

- 148 ページのセクション 5.12.1「前提条件」
- 149 ページのセクション 5.12.2「電子メール通知を送信するための SMTP サーバの設定」
- 150 ページの 「通知のための電子メールテンプレートの設定」
- 151 ページのセクション 5.12.4「ドライバポリシーでの SMTP 認証情報の提供」
- 153 ページのセクション 5.12.5「電子メール通知テンプレートへの独自の置換タグの追加」
- 158 ページのセクション 5.12.6「電子メール通知の管理者への送信」
- 158 ページのセクション 5.12.7「電子メール通知テンプレートのローカライズ」

5.12.1 前提条件

- ❑ アイデンティティボールトユーザがインターネット電子メールアドレス属性に入力済みであることを確認します。
- ❑ パスワード同期の電子メール通知を使用する場合は、パスワード同期のドライバポリシーに SMTP サーバのパスワードが含まれていることを確認します。151 ページのセクション 5.12.4「ドライバポリシーでの SMTP 認証情報の提供」を参照してください。
- ❑ 電子メールアドレスを入力していないユーザがいる可能性がある場合や、すべての失敗操作の通知の電子メールレコードが必要な場合は、ユーザだけではなく、パスワード管理者アカウントにも電子メール通知を送信するよう選択することを検討します。

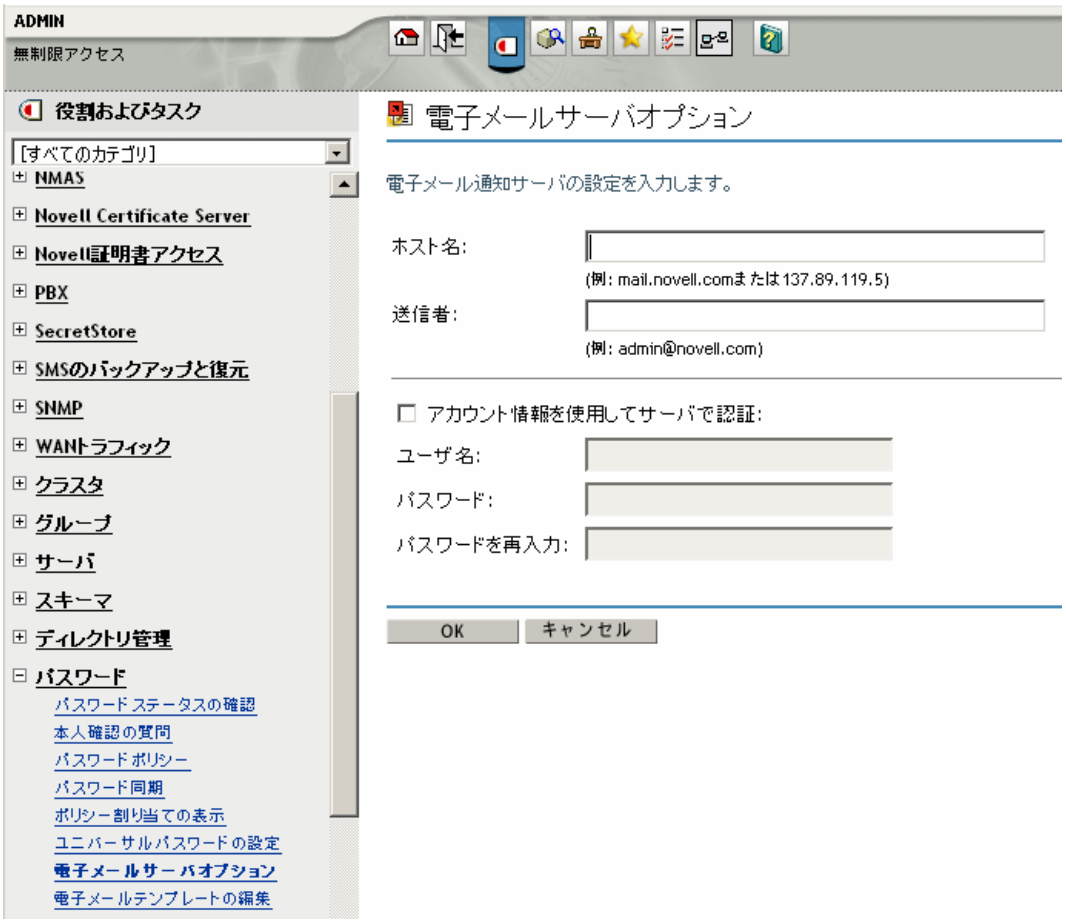
この電子メールアドレスは、Identity Manager のスクリプトポリシーの To フィールドに入力されている必要があります。詳細については、158 ページのセクション 5.12.6「電子メール通知の管理者への送信」を参照してください。

- eDirectory および Identity Manager が UNIX サーバ上にある場合は、サーバは電子メールテンプレートオブジェクトのレプリカを保存する必要があります。

  これらのオブジェクトは、ルートのセキュリティコンテナにあります。つまり、サーバにはルートパーティションのレプリカが必要です。

5.12.2 電子メール通知を送信するための SMTP サーバの設定

1 iManager で、［パスワード］>［電子メールサーバオプション］の順に選択します。



2 次の情報を入力します。

- ホスト名
- 電子メールメッセージの［送信者］フィールドに表示する名前 (Administrator など)
- 必要に応じ、サーバに対して認証するためのユーザ名およびパスワード

3 ［OK］をクリックします。

4 Identity Manager ドライバでパスワード同期を使用しており、電子メール通知機能を使用する場合は、次の作業も必要です。

4a 電子メールを送信する前に SMTP サーバで認証が必要な場合、ドライバポリシーにパスワードが含まれていることを確認します。手順については、151 ページのセクション 5.12.4「ドライバポリシーでの SMTP 認証情報の提供」を参照してください。

ステップ 2 にある［電子メールサーバオプション］ページで指定する認証情報は、パスワードを忘れた場合の通知には十分ですが、パスワード同期の通知には不十分です。

4b 変更に伴い更新する必要のある Identity Manager ドライバを再起動します。

ドライバはテンプレートおよび SMTP サーバ情報を、起動時のみ読み込みます。

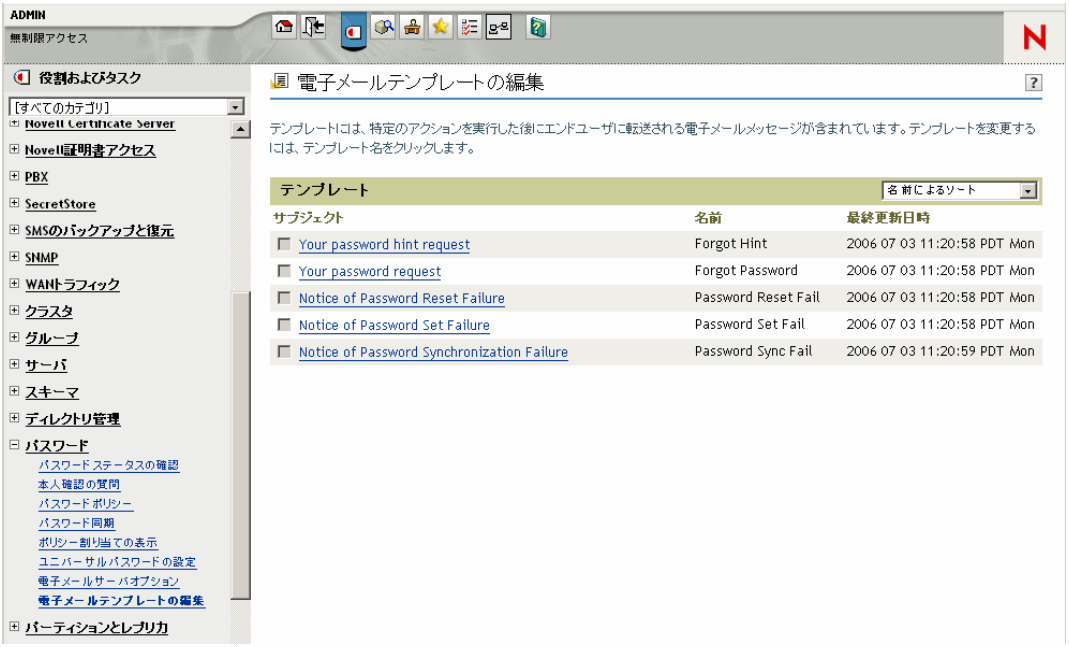
5 150 ページの 「通知のための電子メールテンプレートの設定」の説明に従い、電子メールテンプレートをカスタマイズします。

メッセージを送信する機能を使用する場合は、電子メールサーバの設定後、電子メールテンプレートを使用するアプリケーションから電子メールメッセージを送信できます。

5.12.3 通知のための電子メールテンプレートの設定

テンプレートを独自のテキストでカスタマイズできます。テンプレートの名前は、使用目的を示します。

1 iManager で、［パスワード］>［電子メールテンプレートの編集］の順に選択します。



2 必要に応じてテンプレートを編集します。

置換タグを追加する場合は、追加の作業が必要となることがあります。153 ページのセクション 5.12.5「電子メール通知テンプレートへの独自の置換タグの追加」の指示に従います。

3 変更に伴い更新する必要のある Identity Manager ドライバを再起動します。

ドライバはテンプレートおよび SMTP サーバ情報を、起動時のみ読み込みます。

5.12.4 ドライバポリシーでの SMTP 認証情報の提供

149 ページのセクション 5.12.2「電子メール通知を送信するための SMTP サーバの設定」に従い、SMTP サーバのユーザ名およびパスワードを指定します。パスワードを忘れた場合の電子メール通知については、これで十分です。

ただし、パスワード同期の電子メール通知については、パスワードもドライバポリシーに含める必要があります。メタディレクトリエンジンはユーザ名にはアクセスできますがパスワードにはアクセスできないため、ドライバポリシーでパスワードを提供する必要があります。

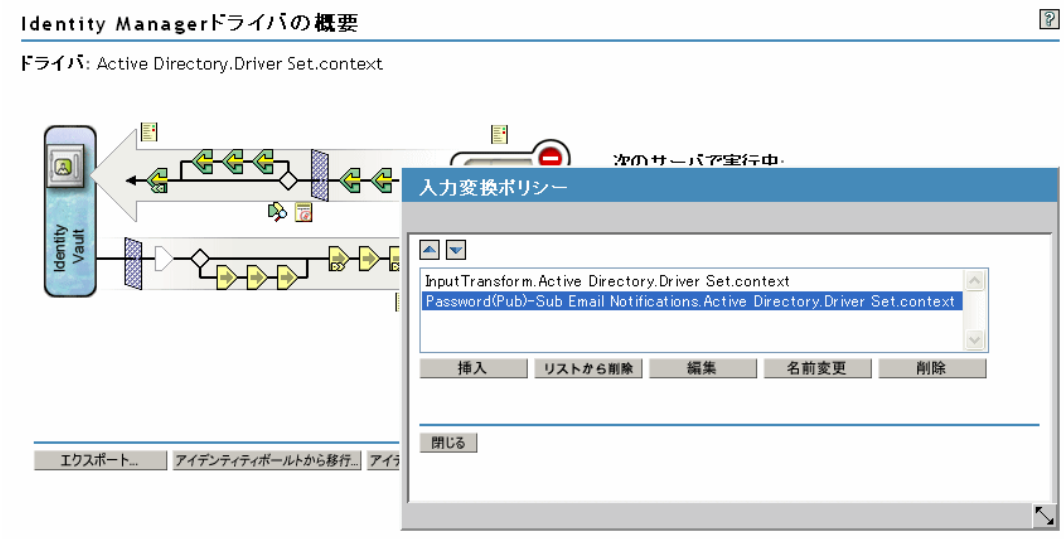
次の条件に該当する場合は、この手順を実行する必要があります。

- SMTP サーバがセキュリティ保護されており、電子メールを送信する前に認証が必要な場合。
- Identity Manager のパスワード同期を Identity Manager ドライバで使用している場合。
- ドライバのパスワード同期の設定で、［電子メール経由でユーザにパスワード同期障害を通知する］を選択した場合。

ドライバポリシーに SMTP サーバのパスワードを追加する

1. パスワード同期を使用するために必要なポリシーがドライバに含まれていることを確認します。

   必要なポリシーは、サンプルのドライバ環境設定で提供されています。また、100 ページのセクション 5.7「パスワード同期をサポートするための、既存のドライバ環境設定のアップグレード」に従い、追加することもできます。
2. iManager で、［Identity Manager］>［Identity Manager の概要］の順に選択します。
3. ドライバセットを検索するか、対象のドライバセットを含むコンテナを参照して選択します。
4. ［Identity Manager ドライバの概要］で、ドライバのアイコンをクリックします。
5. ［入力変換］アイコンまたは［出力変換］アイコンを選択します。



6 ポリシーを選択し、［編集］をクリックします。

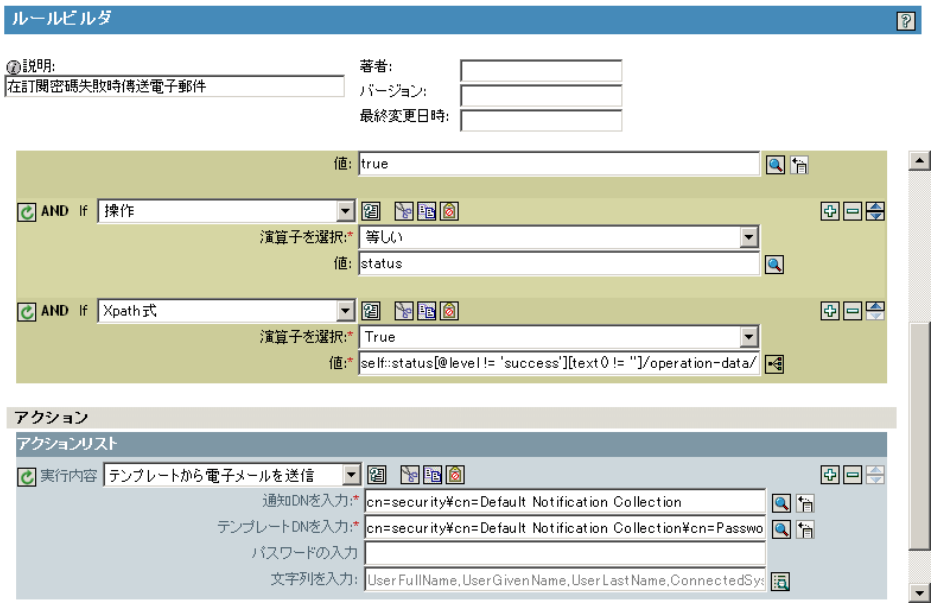
7 ルールをクリックします。

8 ［テンプレートから電子メールを送信］アクションを含むルールで、SMTP サーバのパスワードを指定します。

たとえば、サンプルのドライバ環境設定を使用している場合、次のパスワード同期ポリシーを変更する必要があります。

ポリシーセット	ポリシー名	ルール名
入力変換	Password(Pub)-Sub Email Notifications (パスワード (発行者)- 購読者の電子メール通知)	◆ パスワードを取得できなかった場合に電子メールを送信する ◆ 接続されたシステムのパスワードを Identity Manager データストアのパスワードでリセットできなかった場合に電子メールを送信する
出力変換	Password(Sub)-Pub Email Notifications (パスワード (購読者)- 発行者の電子メール通知)	◆ パスワードの発行操作が失敗した場合に電子メールを送信する

次の図は、パスワードを必要とする［テンプレートから電子メールを送信］アクションの例を示します。



アイデンティティボールトに保存されている場合、パスワードは不明です。

9 ルールを選択し (確認マークを付け)、［OK］をクリックします。

5.12.5 電子メール通知テンプレートへの独自の置換タグの追加

電子メール通知テンプレートには、デフォルトで定義されているタグがいくつかあり、これらを使用すると、ユーザへのメッセージを簡単にパーソナライズできます。また、独自のタグを追加することもできます。

タグを追加できるかどうかは、電子メールテンプレートを使用するアプリケーションによって異なります。

- 153 ページの 「パスワード同期の電子メール通知テンプレートへの置換タグの追加」
- 158 ページの 「パスワードを忘れた場合の電子メール通知テンプレートに対する、置換タグの追加」

パスワード同期の電子メール通知テンプレートへの置換タグの追加

パスワード同期の電子メール通知テンプレートには置換タグを追加できます。ただし、追加されたタグは、電子メール通知テンプレートを参照するすべてのパスワード同期ポリシールールに定義しないと使用できません。[テンプレートから電子メールを送信] アクションを使用する場合、テンプレート内で宣言される置換タグはすべて、アクションの子 arg-strings 要素で定義する必要があります。

たとえば、Identity Manager では、電子メール通知テンプレートに含まれるデフォルトの置換タグを提供しています。Identity Manager では、デフォルトのパスワード同期ポリシーも、ドライバ環境設定で提供されています。電子メールテンプレートで提供されるデフォルトのタグもそれぞれ、電子メールテンプレートが使用するパスワード同期ポリシーの各ルールで定義されています。

たとえば、UserGivenName タグは、Password Set Fail という名前の電子メールテンプレートで定義されているデフォルトのタグの 1 つです。[パスワードを取得できなかった場合に電子メールを送信する] という名前のポリシールールは、[テンプレートから電子メールを送信] アクションの電子メールテンプレートを参照します。パスワードの同期に失敗したときにユーザに通知する場合に、このルールがポリシーで使用されます。同じ UserGivenName タグは、そのルールで arg-string 要素として定義されます。

この例のように、追加する新しい各タグは、電子メールテンプレートと、その電子メールテンプレートを参照するポリシールールの両方で定義する必要があります。これは、ユーザに電子メールを送信する場合に、メタディレクトリエンジンが置換タグの代わりに正しいデータを挿入する方法を認識できるようにするためです。

例として、Identity Manager に付属の Identity Manager ドライバ環境設定にあるタグを参照してください。

次のガイドラインに注意してください。

- 電子メールテンプレートで置換タグと呼ばれる項目は、ポリシービルダのコンテキストではトークンと呼ばれます。
- この節の手順で説明するように、置換タグの引数文字列の定義を簡略化するには、ポリシービルダを使用します。
- 追加するタグは、次のどれかに定義できます。
  - ユーザのソース属性またはターゲット属性

    パスワードを忘れた場合のために電子メールテンプレートにタグを追加する場合とは異なり、アイデンティティボールトのユーザオブジェクトにある属性と同じ

名前を持つタグを追加しただけでは、そのタグを使用できません。パスワード同期の電子メール通知テンプレートで使用するすべてのタグと同様に、電子メールテンプレートを参照するポリシーでも、タグを定義する必要があります。

- グローバル構成値 (GCV)
- XPATH 式

eDirectory ユーザ属性に限定されている、パスワードを忘れた場合のための電子メールテンプレートにあるタグとは対照的です。

- パスワードを忘れた場合のために電子メールテンプレートにタグを追加する場合は、eDirectory のユーザ属性の正確な名前を使用する必要がありますが、置換タグには任意の名前を付けることができます。ただし、電子メールテンプレートを参照するポリシーのタグの定義に使用される名前と一致することが必要です。

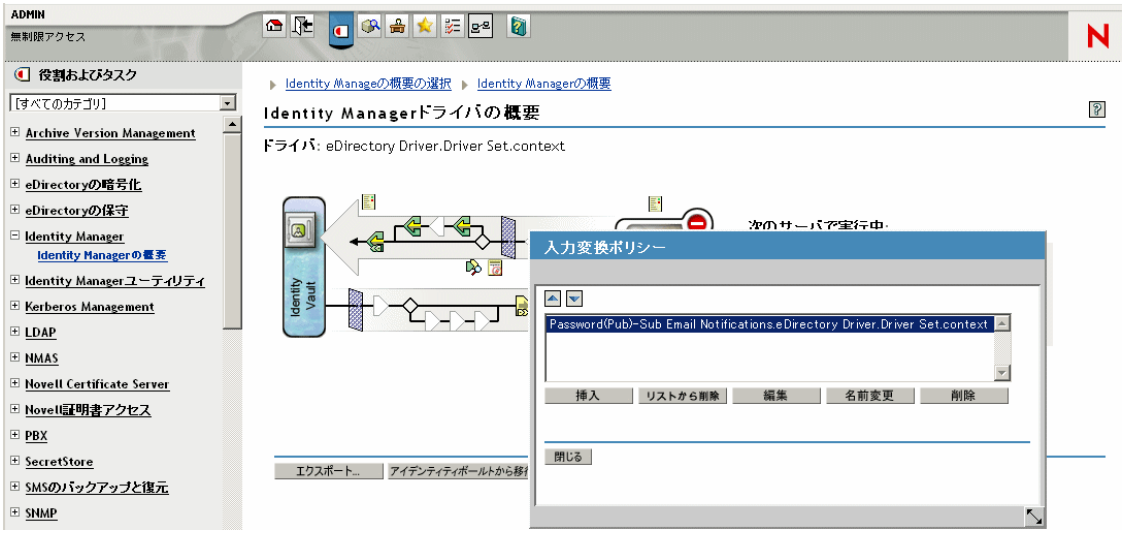
ポリシーにタグを定義するには、電子メール通知テンプレートを参照するポリシーすべてを検索し、ポリシービルダを使用してそれらにタグを追加します。各ポリシーで、テンプレートを参照する各ルールを編集します。

電子メール通知テンプレートを参照するポリシーをすべて確実に検索する 1 つの方法は、ドライバ環境設定をエクスポートし、XML で電子メール通知テンプレートと同じ名前のテンプレートを持つ do-send-e-mail アクションを検索することです。

1. iManager で、［Identity Manager］>［Identity Manager の概要］の順に選択します。
2. 編集するポリシーのあるドライバを含むドライバセットを選択します。
3. 編集するポリシーが設定されているドライバのアイコンをクリックします。
4. 発行者チャネルまたは購読者チャネルで、編集するポリシーが含まれている一連のポリシーをクリックします。

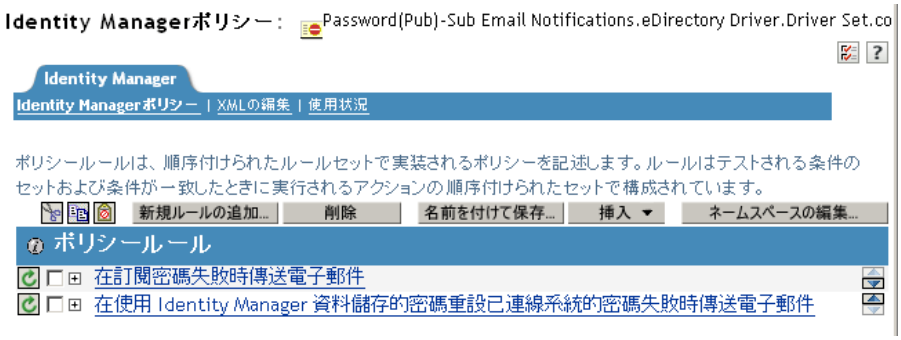
   たとえば、Identity Manager に付属している eDirectory ドライバ用のドライバ環境設定には、パスワード同期の両方の電子メール通知テンプレートを参照する入力変換ポリシーセットのポリシーが含まれます。
5. ポリシーをクリックした後、［編集］をクリックします。

   次の図は、eDirectory ドライバの Password(Pub)-Sub Email Notifications (パスワード (発行者)- 購読者の電子メール通知) ポリシーを編集する方法を示しています。

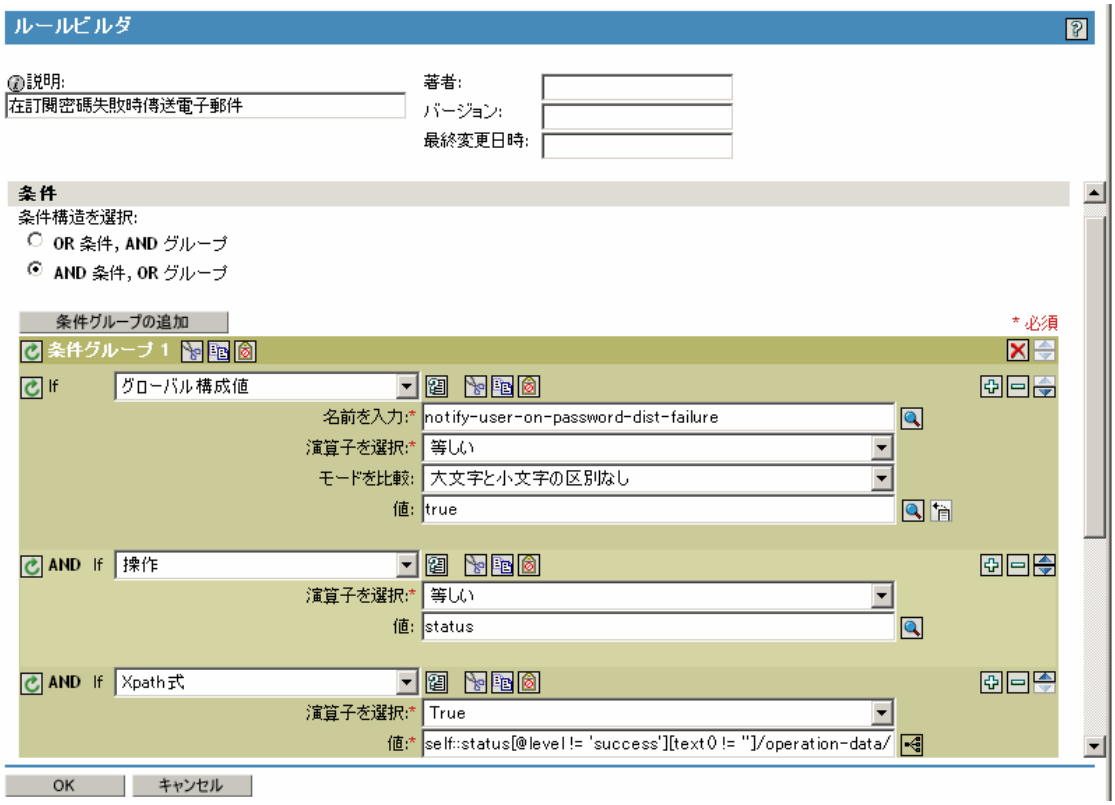


6 開かれたルールのリストから、電子メール通知テンプレートを参照するルールをクリックします。

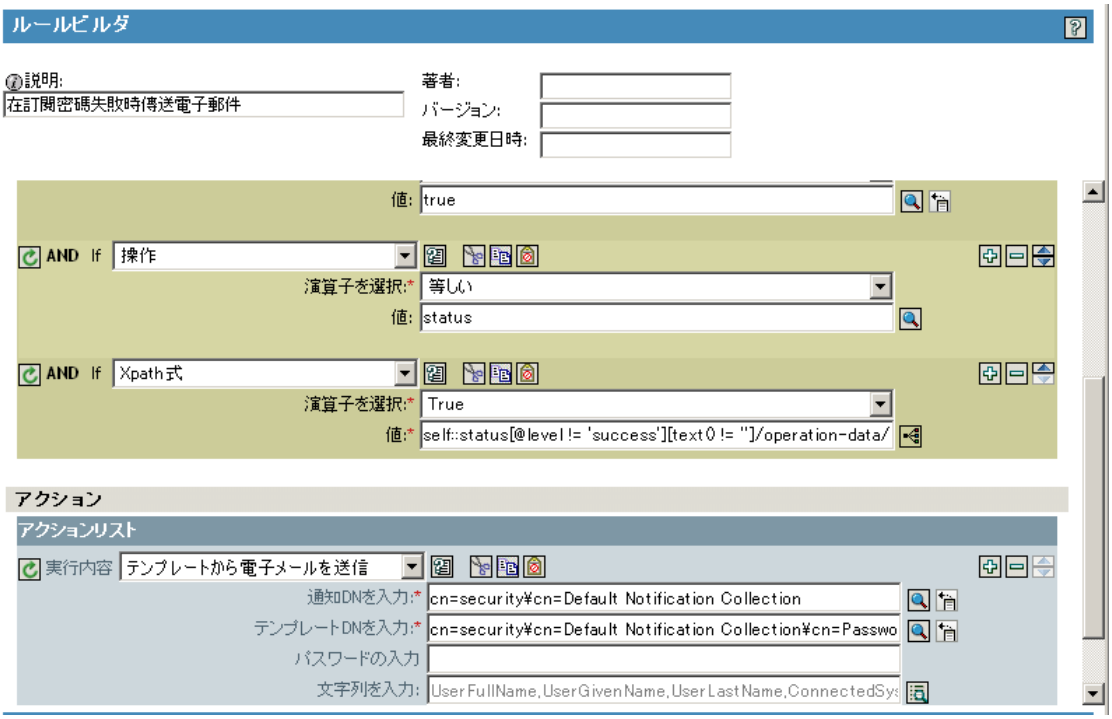
たとえば、Password(Pub)-Sub Email Notifications (パスワード (発行者)- 購読者の電子メール通知) ポリシーでは、このようなルールのリストが表示されます。これらのルールは両方とも、パスワード同期の電子メールテンプレートの 1 つを参照します。両方のテンプレートにタグを追加する場合は、両方のルールを編集する必要があります。



最初のルールをクリックすると、次のページが表示されます。

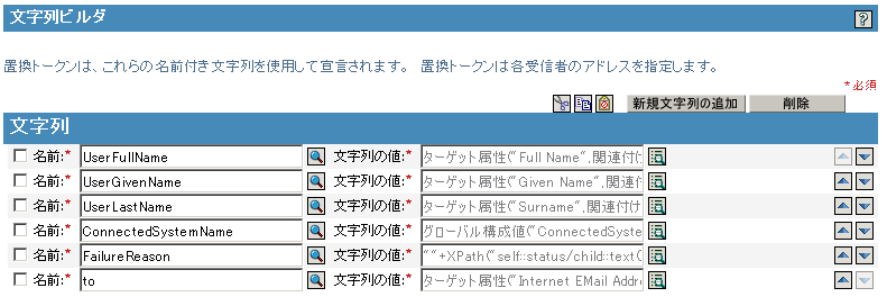


7 ［アクション］セクションまでスクロールします。



8 ［テンプレートから電子メールを送信］ルールを使用する場合は、［文字列を入力］フィールドの［参照ボタン］をクリックします。

［文字列ビルダ］が開きます。この例のルールでは、次の図のような文字列のリストが表示されます。電子メール通知テンプレートに使用されるデフォルトのタグは、このように、Identity Manager ドライバ環境設定の一部であるパスワード同期ポリシーですでに定義されています。デフォルトのタグは、例として使用できます。



9 電子メール通知テンプレートで使用するタグを定義するには、［Append New String (新規文字列の追加)］をクリックし、タグの名前を入力します。

電子メール通知テンプレートで使用する名前と正確に一致する名前であることを確認してください。

10 ［文字列の値］フィールドの［参照］ボタンをクリックすると、タグを簡単に定義できます。

11 ［引数ビルダ］ページでは、電子メール通知テンプレートでこのタグを使用する場合にどの値を引用するかを指定します。

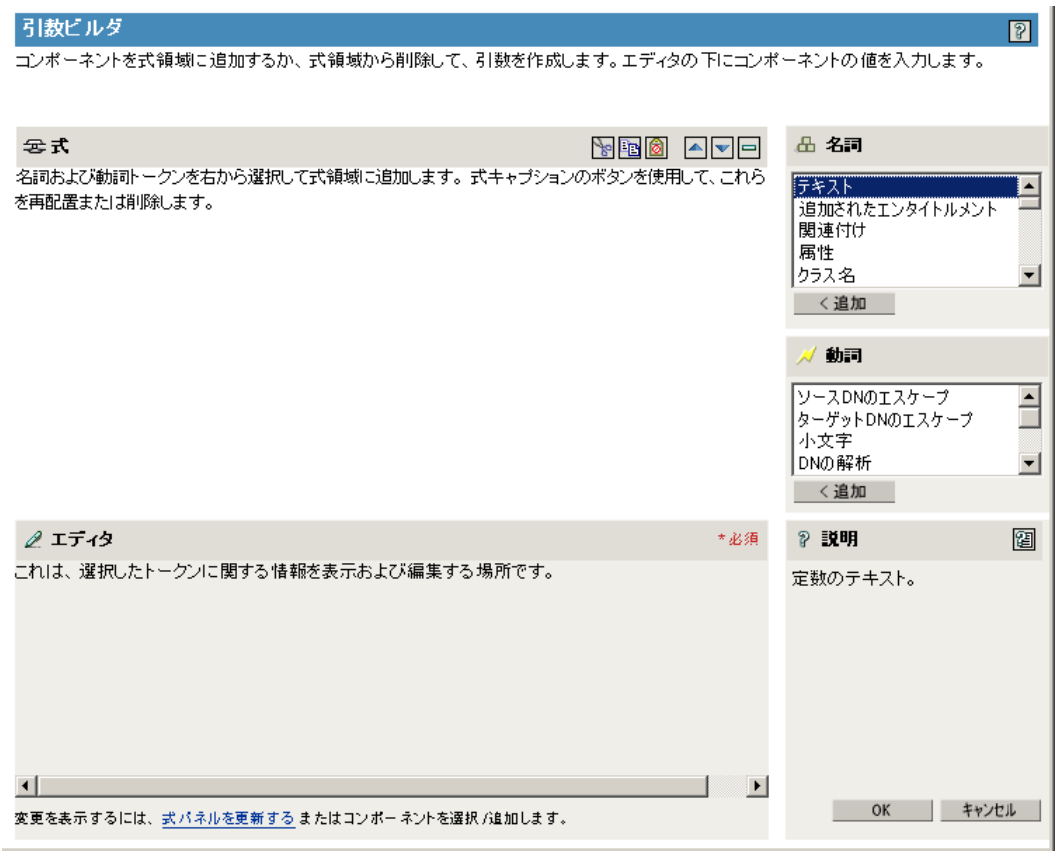
以下のタグを定義できます。

- ユーザのソース属性またはターゲット属性

  パスワードを忘れた場合のために電子メールテンプレートにタグを追加する場合とは異なり、アイデンティティボールトのユーザオブジェクトにある属性と同じ名前を持つタグを追加しただけでは、そのタグを使用できません。パスワード同期の電子メール通知テンプレートで使用するすべてのタグと同様に、電子メールテンプレートを参照するポリシーでも、タグを定義する必要があります。

- グローバル構成値 (GCV)
- XPATH 式

次の図は、タグを定義する方法を示しています。



タグの定義が終了したら［OK］をクリックします。タグが［文字列ビルダ］ページに文字列の 1 つとして表示されます。

12 ［OK］をクリックしてすべてのページを終了し、ポリシーの変更を保存します。

13 電子メール通知テンプレートを参照するすべてのポリシーのルールを編集するには、この手順を繰り返します。

14 ポリシーで定義したタグを電子メール通知テンプレートに追加します。ポリシーで使用した名前と完全に同じ名前を使用します。

これにより、電子メール通知テンプレートの本文で、タグの名前を使用できるようになります。

15 変更内容を保存して、ドライバを再起動します。

パスワードを忘れた場合の電子メール通知テンプレートに対する、置換タグの追加

次のガイドラインに従い、パスワードを忘れた場合の電子メール通知テンプレートにタグを追加できます。

- 追加できるタグは、メッセージの送信先のユーザオブジェクトの LDAP 属性に対応するタグのみです。
- 追加するタグの名前は、ユーザオブジェクトの LDAP 属性の名前と完全に同じであることが必要です。

  LDAP 属性と eDirectory 属性の名前の対応については、LDAP の Identity Manager ドライバのスキーママッピングポリシーを参照してください。
- その他の設定は必要ありません。

5.12.6 電子メール通知の管理者への送信

デフォルトの設定では、電子メール通知はユーザに対してのみ送信されます。Identity Manager に付属のポリシーでは、影響するユーザのアイデンティティボールトブジェクトの電子メールアドレスを使用します。

ただし、パスワード同期のポリシーでは、電子メール通知を管理者に対しても送信できるよう設定できます。設定するには、1 つのポリシーの Identity Manager スクリプトを変更する必要があります。

管理者の電子メールアドレスとトークンを定義し、管理者にブラインドコピーを送信します。

管理者にコピーを送信するには、電子メールを作成するポリシー (通知を送信するためにポリシーが電子メールアドレスを検索する PublishPasswordEmails.xml など) を変更し、追加の <arg-string> 要素と管理者の電子メールアドレスを追加します。

次の例では、追加の arg-string 要素を示しています。

```
<arg-string name="to">

<token-text>Admin@company.com</token-text>

</arg-string>
```

変更後、必ずドライバを再起動するようにしてください。

5.12.7 電子メール通知テンプレートのローカライズ

次のことに注意してください。

- デフォルトのテンプレートは英語で表記されていますが、他の言語を使用するようテキストを編集できます。
- ポリシーの arg-string トークン定義と置換タグの名前が一致するよう、置換タグの名前と定義は英語のままでなければなりません。

- パスワードを忘れた場合の電子メール通知についてのみ、電子メールのエンコード方法を指定するために、portalservlet.properties ファイルに設定を追加する必要があります。次に例を示します。

  ```
  ForgottenPassword.MailEncoding=EUC-JP
  ```

  この設定が存在しない場合、電子メール変換にエンコードは使用されません。
- パスワード同期の電子メールメッセージについては、<mail、<message、および <‘ 要素に charset という名前の XML 属性を指定できます。

  これらの要素の使用の詳細については、電子メールテンプレートについて説明している『*DirXML Driver for Manual Task Service Implementation Guide* (http://www.novell.com/documentation/dirxmldrivers/index.html)』を参照してください。

5.13 パスワード同期のトラブルシューティング

- 109 ページのセクション 5.8「パスワード同期の実装」のヒントを参照してください。
- NMAS に単純パスワードログインメソッドがインストールされていることを確認します。
- eDirectory ログインメソッド、または Identity Manager により同期する接続システムのパスワードに NMAS でパスワードポリシーを適用するサーバに、ツリーのルートのコピーがあることを確認します。
- パスワード同期を必要とするユーザが、パスワードを同期するドライバのある同じサーバに複製されていることを確認します。他のドライバの機能と同様に、ドライバは、同じサーバの、マスタレプリカまたは読み書き可能レプリカに存在するユーザのみを管理できます。
- Web サーバとアイデンティティボールトとの間で SSL が適切に設定されていることを確認します。
- 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にもかかわらず、パスワードがアイデンティティボールトに正しく設定されている場合は、ドライバポリシーのデフォルトのパスワードが、ユーザに適用されるパスワードポリシーに準拠していない可能性があります。

  次のシナリオでは、Active Directory ドライバが使用されています。しかし、他のドライバでも同じ問題が発生する場合があります。

  初期パスワードの提供。ドライバがアイデンティティボールトで Active Directory 内のユーザに一致させるために新しいユーザオブジェクトを作成したときに、Active Directory ドライバにユーザの初期パスワードを提供させたいとします。Active Directory ドライバのサンプル環境設定は、初期パスワードをユーザの追加とは別の操作として送信します。さらに、Active Directory からパスワードが提供されない場合はユーザのデフォルトパスワードを提供するポリシーも含んでいます。

  ユーザの追加とパスワードの設定は別個に実行されるため、この場合は、新しい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常に受信します。ユーザを追加した後すぐに Active Directory ドライバがパスワードを送信するため、デフォルトのパスワードはすぐに更新されます。デフォルトパスワードがユーザのアイデンティティボールトのパスワードポリシーに準拠しない場合、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パスワードがパスワードポリシーに対して短すぎる場合は、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 ドライバがポリシーに準拠する初期パスワードを送信した場合には、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提供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。これらの方法は、初期パスワードが Add イベントに付属しないけれども、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。

- 組織のため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 (［パスワード］>［パスワードポリシー］の順に選択します)。

  初期パスワードが信頼されるアプリケーションから提供されると、デフォルトパスワードを上書きします。

  このオプションを使用することをお勧めします。これは、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が推奨されているためです。

- 発行者チャネルで、デフォルトのパスワードを作成する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。アイデンティティボールトでは、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について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おり、ユーザオブジェクトは一時的にはパスワードなしで存在できます。

- パスワードポリシーはツリー中心で割り当てられます。一方、パスワード同期はドライバごとに設定されます。サーバごとにドライバがインストールされ、ドライバはマスタレプリカまたは読み書き可能レプリカのユーザのみ管理できます。

  パスワード同期により期待される結果を取得するには、パスワード同期を実行するサーバにあるマスタレプリカまたは読み書き可能レプリカのコンテナが、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割り当てたコンテナと一致するようにします。パーティションルートコンテナにパスワードポリシーを割り当てることによって、そのコンテナとサブコンテナ内のすべてのユーザに確実にパスワードポリシーが割り当てられます。

- DSTrace の便利なコマンド :

  +*DXML*: Identity Manager ルール処理および可能性のあるエラーメッセージを表示する

  +*DVRS*: Identity Manager ドライバのメッセージを表示する

  +*AUTH*: NDS パスワードの変更を表示する

  +*DCLN*: NDS DClient メッセージを表示する

エンタイトルメントの作成と使用

6

Identity Manager を使用すると、接続システム間でデータを同期できます。エンタイトルメントにより、ユーザまたはグループに対する条件を設定できます。条件が一致すれば、接続システム内のビジネスリソースへのアクセス権を付与したり、取り消したりするイベントを開始します。これにより、1 レベル上の制御を可能にし、リソースの付与および取り消しを自動化できます。

エンタイトルメントの機能には、エンタイトルメントの作成とエンタイトルメントの管理の 2 つの面があります。エンタイトルメントの作成には、iManager または Designer を使用します。iManager を使用してエンタイトルメントを作成するには、iManager の Identity Manager ユーティリティのヘッダで［エンタイトルメントの作成］オプションを選択します。詳細については、167 ページのセクション 6.4「iManager を介した XML でのエンタイトルメントの記述」を参照してください。

Designer を使用して、エンタイトルメントを作成し、既存の Identity Manager ドライバに展開することもできます。Designer を使用すると、エンタイトルメントを作成するためのグラフィカルインタフェースであるエンタイトルメントウィザードの示すプロセス手順に従って、エンタイトルメントを作成できます。iManager では、シンプルなインタフェースを介してエンタイトルメントを作成しますが、XML エディタを介して付加的なプロパティを追加します。グラフィカルインタフェースが組み込まれているため、エンタイトルメントの作成および編集には Designer を使用することをお勧めします。

エンタイトルメントを作成した後 (または特定の Identity Manager ドライバで事前設定されたエンタイトルメントを使用して)、それらを管理する必要があります。エンタイトルメントは、2 つのパッケージまたはエージェントによって (役割ベースエンタイトルメントポリシーとしての iManager を介して、またはワークフローベースのプロビジョニングのユーザアプリケーションを介して) 管理されます。ワークフローベースのプロビジョニングで使用されるエンタイトルメントについては、「Introduction to Workflow-Based Provisioning」を参照してください。役割ベースエンタイトルメントについては、181 ページのセクション 6.5「役割ベースエンタイトルメントの管理の概要」を参照してください。

条件が一致した場合、役割ベースエンタイトルメントポリシーによりビジネスリソースを付与できます。たとえば、ユーザが条件 1、2、および 3 を満たしている場合、役割ベースエンタイトルメントポリシーを介して、ユーザはグループ H のメンバーになりますが、ユーザが条件 4 および 5 を満たしている場合、グループ I のメンバーになります。このエンタイトルメントがワークフローベースのプロビジョニングを介して機能するには、最初に承認が必要です。

- 192 ページのセクション 6.8「役割ベースエンタイトルメントポリシー間での衝突の解決」
- 198 ページのセクション 6.9「役割ベースエンタイトルメントのトラブルシューティング」
- 199 ページのセクション 6.10「役割ベースエンタイトルメントおよびワークフローベースのプロビジョニングのエンタイトルメントに適用されるエンタイトルメント要素」

6.1 用語

この章で使用される用語を次に示します。

表 *6-1* 用語

用語	説明
エンタイトルメント	接続システム内のビジネスリソースを表すアイデンティティボールトブジェクト。
エンタイトルメントエージェント	エンタイトルメントを付与したり、取り消したりします。役割ベースエンタイトルメントでは、エージェントはエンタイトルメントサービスドライバです。
付与または取り消し	エンタイトルメントの付与または取り消しの解釈は、Identity Manager ドライバのグローバル設定の変数 (GCV) によって制御されます。
エンタイトルメントコンシューマ	エンタイトルメント関連の情報を使用するものすべて。エンタイトルメントコンシューマには、iManager、ユーザアプリケーション、および Identity Manager ポリシーが含まれています。

6.2 エンタイトルメントの作成：概要

- 163 ページのセクション 6.2.1「エンタイトルメントをサポートする、事前設定済みの Identity Manager ドライバ」
- 164 ページのセクション 6.2.2「他の Identity Manager ドライバでのエンタイトルメントの有効化」

エンタイトルメントで何を実行したいのかを事前に知っておく必要があります。エンタイトルメントは、ポリシーを介して Identity Manager ドライバに組み込んだ機能から動作します。これらのドライバポリシーによって、ルールが実装され、アイデンティティボールトと接続システムとの間でイベントが処理されます。Identity Manager ドライバのポリシーで何をするかを指定しない場合、エンタイトルメントは機能しません。たとえば、コマンドポリシーの［Check User Modify for Group Membership (グループメンバシップのユーザ変更を確認する)］ルールの［action (アクション)］セクションを指定しない場合、グループメンバーシップエンタイトルメントの付与または取り消しの試行は無視されます。

すべての接続システムリソースに対する付与および取り消しの機能を正しく設計するためには、Identity Manager で何を実行するのかを正確に知っておく必要があります。次の 4 つのステップの手順は、エンタイトルメントの作成および使用の計画に役立ちます。

1. ビジネスの場で何を実行する必要があるのかを知っておきます。Identity Manager を介してほとんどすべてを設計および実装できますが、定義されていないいくつかの事柄を実装する前に、何をしたいのかを知っておく必要があります。何をしたいのかに関する番号付きリストを作成します。
2. 番号付きリストの 1 つのポイントを表すエンタイトルメントを定義します。値のないエンタイトルメントと値のあるエンタイトルメントを作成できます。値のあるエンタイトルメントは、外部クエリから値を取得できます。管理者が定義した形式にすることも、自由形式にすることもできます。177 ページのセクション 6.4.6「独自のエンタイトルメントを作成するためのエンタイトルメントの例」に例を示しています。
3. Identity Manager ドライバにポリシーを追加し、設計されたエンタイトルメントを実装します。Identity Manager ドライバ用のポリシーを作成するには、接続システムで情報が処理および受信される方法、および Novell® eDirectory™ に情報が保存される方法について、XSLT または DirXML スクリプトに精通している必要があります。優れた DirXML* のプログラマでない限り、これはコンサルタントの仕事です。
4. エンタイトルメントを付与または取り消すための管理エージェントを設定します。自動処理にする場合、役割ベースエンタイトルメントを使用します。手動処理にする場合、ワークフローベースのプロビジョニングを使用します。

6.2.1 エンタイトルメントをサポートする、事前設定済みの Identity Manager ドライバ

Identity Manager には、エンタイトルメント、エンタイトルメントを実装するためのポリシー、およびエンタイトルメントアクティビティのリッスンが有効になっているドライバがすでに含まれている、事前設定済みのいくつかのドライバが付随しています。ドライバを初めてインストールするとき、事前設定済みの要素をドライバの一部にするため、エンタイトルメントを有効にする必要があります。次のドライバはエンタイトルメントをサポートするよう事前設定済みです。

- Active Directory*
- Exchange
- GroupWise®
- LDAP
- NIS
- Lotus* Notes*
- NT ドメイン
- RACF

これらの事前設定済みのドライバでは、上記の 4 つのステップの最初の 3 つが実行されます。ドライバに含まれているエンタイトルメントのタイプの例は、最も一般的なユーザアカウント、グループ、および電子メール配布リストの付与および取り消しの各シナリオで使用できます。具体的には、次のようなシナリオがあります。

- Active Directory: アカウント、グループメンバーシップ、Exchange メールボックスの付与および取り消し

- Exchange 5.5: メールボックスとグループメンバーシップの付与および取り消し
- GroupWise: アカウントの付与および取り消し、配布リストのメンバーの付与および取り消し
- LDAP: ユーザアカウントの付与および取り消し
- Linux* および UNIX*: アカウントの付与および取り消し
- Lotus Notes: ユーザアカウントとグループメンバーシップの付与および取り消し
- NT ドメイン : ユーザアカウントとグループメンバーシップの付与および取り消し
- RACF: グループアカウントとグループメンバーシップの付与および取り消し

これらのエンタイトルメントおよびポリシーの例は、(ユーザの必要を満たしていれば) そのまま使用できます。必要を満たすように変更することもできます。またはこれらを例として使用し、iManager または Designer を使用して独自のエンタイトルメントおよびポリシーを作成できます。繰り返しますが、事前設定済みのドライバのエンタイトルメントを使用するには、事前設定済みのドライバを Designer または iManager で初めて作成するときにエンタイトルメントを有効にする必要があります。事前設定済みのエンタイトルメントは、ドライバを再作成しない限り、後で追加することはできません。

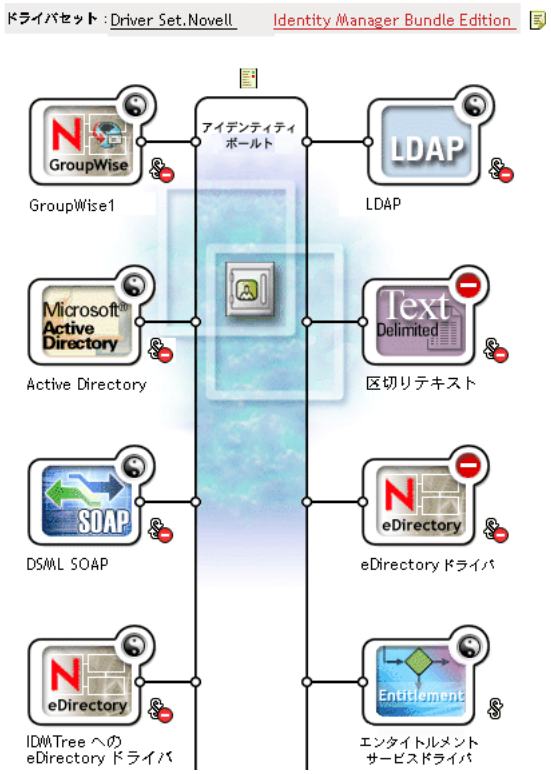
Identity Manager 2.x でエンタイトルメントを使用していて、これらのエンタイトルメントを Identity Manager 3 で使用するには、［Identity Manager ユーティリティ］の［エンタイトルメントのアップグレード］オプションを実行します。

6.2.2 他の Identity Manager ドライバでのエンタイトルメントの有効化

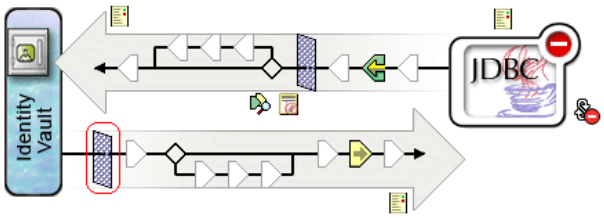
事前設定済みのエンタイトルメントが含まれていない Identity Manager ドライバで、エンタイトルメントを使用することもできます。ドライバでエンタイトルメントのサポートを有効にするには、DirXML-EntitlementRef 属性をドライバフィルタに追加します。これには次の操作を行います。

1. ［Identity Manager］>［Identity Manager の概要］の順に選択します。
2. ドライバがある場所でドライバセットを参照し、［検索］をクリックします。

3. ［Identity Manager の概要］画面で、表示されている［ドライバセット］からドライバオブジェクトを選択します。



4. ［ドライバセット］のドライバをダブルクリックし、ドライバの画面を表示します。アイデンティティボールトの右側の［ドライバフィルタ］アイコンをクリックします (赤い丸で示しています)。



5. ［フィルタ］ページで［属性の追加］を選択し、下部までスクロールして［すべての属性を表示］を選択します。［DirXML-EntitlementRef (DirXML-EntitlementRef)］属性を選択し、［OK］をクリックします。

6. ［フィルタ］ページで［DirXML-EntitlementRef (DirXML-EntitlementRef)］を選択します。［Subscribe (購読)］ヘッダで、［通知］を選択します。［OK］をクリックします。

7. ドライバ上で Designer を介してエンタイトルメントを作成すると、この処理は自動的に実行されます。

6.3 エンタイトルメントの必要条件

- eDirectory 8.7.3 以降
- Identity Manager 2 または 3
- エンタイトルメントサービスドライバ

  エンタイトルメントを使用する場所では、各ドライバセットにエンタイトルメントサービスドライバが存在している必要があります。エンタイトルメントサービスドラ

イバを使用するには、ドライバセットごとに簡単な設定を一度だけ行う必要があります。

- ❑ エンタイトルメントをサポートするドライバ設定

  接続システムでエンタイトルメントを使用する前に、次のいずれかを実行します。

  - ドライバの Identity Manager ドライバ設定をインポートし、そのドライバのエンタイトルメントが有効になっていることを指定する。
  - ドライバがエンタイトルメントをサポートするようにする。これには次の操作を行います。

    a. iManager または Designer を使用してエンタイトルメントを作成します (Designer をお勧めします)。

    b. 164 ページのセクション 6.2.2「他の Identity Manager ドライバでのエンタイトルメントの有効化」で説明したように、DirXML-EntitlementRef 属性をドライバフィルタに追加します。

    c. ステップ 1 で作成したエンタイトルメントを実装するよう、ポリシーを記述します。

6.4 iManager を介した XML でのエンタイトルメントの記述

エンタイトルメントで何が必要なのかを理解するために、有効化されたエンタイトルメントを持ち、事前設定済みのドライバのひとつである Active Directory (AD) のエンタイトルメントおよびポリシーを見てみます。これには、Novell のエンタイトルメント DTD (Document Type Definition) の調査が含まれています。また、DTD に基づいてエンタイトルメントを記述する XML の例も見てみます。

この節では、次の項目について説明します。

6.4.1 エンタイトルメントが有効になっている場合に、Active Directory ドライバによって何が追加されるか

エンタイトルメントが有効な AD ドライバでは、構造に次の変更が加えられました。

- ドライバフィルタに DirXML-EntitlementRef 属性を追加します。DirXML-EntitlementRef 属性により、ドライバフィルタはエンタイトルメントアクティビティをリッスンできます。

- ユーザアカウントのエンタイトルメントを作成します。ユーザアカウントのエンタイトルメントにより、ユーザの Active Directory のアカウントが付与または取り消されます。アカウントが付与されると、ユーザは有効なログオンアカウントを取得できます。アカウントが取り消されると、ドライバがどのように設定されているのかに応じて、ログオンアカウントは無効になるか、削除されます。
- グループメンバーシップのエンタイトルメントを作成します。グループのエンタイトルメントにより、Active Directory のグループのメンバーシップが付与または取り消されます。グループは、アイデンティティボールトのグループと関連付けられている必要があります。メンバーシップが取り消されると、グループからユーザが削除されます。いくつかの外部ツールによって Active Directory 内の制御されているグループにユーザが追加され、ユーザがドライバによって削除されない場合、発行者チャネルではグループメンバーシップエンタイトルメントは適用されません。また、エンタイトルメントが取り消されるのではなく、ユーザオブジェクトから削除された場合、AD ドライバではアクションは行われません。
- Exchange メールボックスエンタイトルメントを作成します。グループのエンタイトルメントにより、Microsoft Exchange のユーザの Exchange メールボックスが付与または取り消されます。
- エンタイトルメント情報を多くのポリシーに追加します。

次のポリシーには、エンタイトルメントが適切に機能するように追加のルールが含まれています。

- InputTransform (ドライバレベル)。このポリシーの［Check Target Of Add Association For Group Membership Entitlements (グループメンバーシップエンタイトルメントに対する add-association の対象を確認する)］ルールでは、グループメンバーシップエンタイトルメントの「add-association」の対象が確認されます。Active Directory で作成されるユーザに割り当てられたグループメンバーシップのエンタイトルメントは、ユーザが正常に作成されるまでは処理できません。add-association は、Active Directory でドライバによってオブジェクトが作成されたことを示します。オブジェクトにもグループエンタイトルメント処理のタグが付いているる場合、すぐに実行されます。
- イベント変換 (発行者チャネル)。このポリシーの［Disallow User Account Delete (ユーザアカウントの削除を禁止する)］ルールでは、アイデンティティボールトのユーザアカウントの削除は拒否されます。ユーザアカウントのエンタイトルメントを使用した場合、アイデンティティボールトではエンタイトルメントによって管理されているユーザアカウントが制御されます。Active Directory で削除しても、アイデンティティボールト内の制御オブジェクトは削除されません。アイデンティティボールト内のオブジェクトを今後変更したり、マージ操作を実行すると、Active Directory でアカウントが再作成される場合があります。
- コマンド (購読者チャネル)。コマンドポリシーには、エンタイトルメントに関する次のルールが含まれています。
  - ［User Account Entitlement Change (Delete Option) (ユーザアカウントエンタイトルメントの変更 (［削除］オプション))］ルール。ユーザアカウントのエンタイトルメントによって、Active Directory の有効なアカウントがユーザに付与されます。エンタイトルメントを取り消すと、［アカウントのエンタイトルメントが取り消された場合］グローバル変数で選択した値に応じて、Active Directory アカウントが無効になるか、または削除されます。エンタイトルメントが変更され、［削除］オプションを選択した場合、このルールが実行されます。
  - ［User Account Entitlement Change (Disable Option) (ユーザアカウントエンタイトルメントの変更 (［無効］オプション))］ルール。ユーザアカウントのエンタイト

ルメントによって、Active Directory の有効なアカウントがユーザに付与されます。エンタイトルメントを取り消すと、［アカウントのエンタイトルメントが取り消された場合］グローバル変数で選択した値に応じて、Active Directory アカウントが無効になるか、または削除されます。エンタイトルメントが変更され、［無効］オプションを選択した場合、このルールが実行されます。

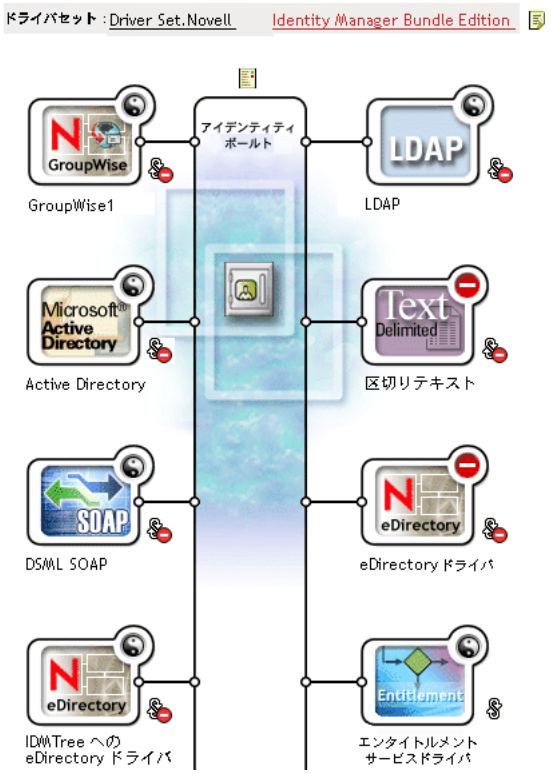
- ［許可される、または取り消されるグループメンバシップのユーザ変更を確認する］ルール。
- ［Check User Modify for Exchange Mailbox Being Granted or Revoked (許可される、または取り消される Exchange メールボックスのユーザ変更を確認する)］ルール。

- 一致 (購読者チャネル)。これは、アカウントのエンタイトルメントです。このポリシーの［Do Not Match Existing Accounts (既存のアカウントに一致しない)］ルール。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でユーザアカウントのエンタイトルメントを使用した場合、エンタイトルメントを付与または取り消すことにより、アカウントが作成および削除されます (または無効になります)。ユーザが Active Directory のアカウントに対する権利を与えられていない場合、デフォルトポリシーは Active Directory の既存のアカウントに一致しません。一致している Active Directory のアカウントにエンタイトルメントポリシーを適用する場合は、このルールを変更または削除します。これにより、Active Directory アカウントが削除されるか、または無効になります。
- 作成 (購読者チャネル)。作成ポリシーには、エンタイトルメントに関する次のルールが含まれています。
  - アカウントのエンタイトルメント : エンタイトルメントが付与されない場合にアカウント作成をブロックします。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でユーザアカウントのエンタイトルメントを使用した場合、アカウントのエンタイトルメントを明確に付与されたユーザに対してのみアカウントが作成されます。エンタイトルメントが付与されない場合、このルールによりユーザアカウント作成が拒否されます。
  - 無効なログインが存在しない場合、アイデンティティボールトのアカウントが有効になります。
  - 追加後にグループのエンタイトルメントの確認の準備をします。追加されたオブジェクトはグループに追加するために存在する必要があるため、追加が完了した後、グループのエンタイトルメントが処理されます。その追加には、追加処理が完了したときに入力変換で確認された運用プロパティのフラグが付けられます。
  - 追加後にエンタイトルメントの交換を確認する必要があることを示します。
  - ユーザ名を Windows ログオン名にマップします。eDirectory ユーザ名の後に userPrincipalName が設定されている場合、eDirectory オブジェクト名と Active Directory ドメインの名前に userPrincipalName を設定します。

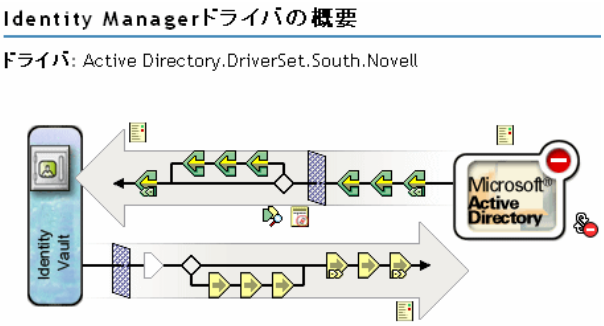
iManager で次のステップを実行すると、各ポリシーの実際の XML コードを表示できます。

1. ［Identity Manager］>［Identity Manager の概要］の順に選択します。
2. ドライバがある場所でドライバセットを参照し、［検索］をクリックします。

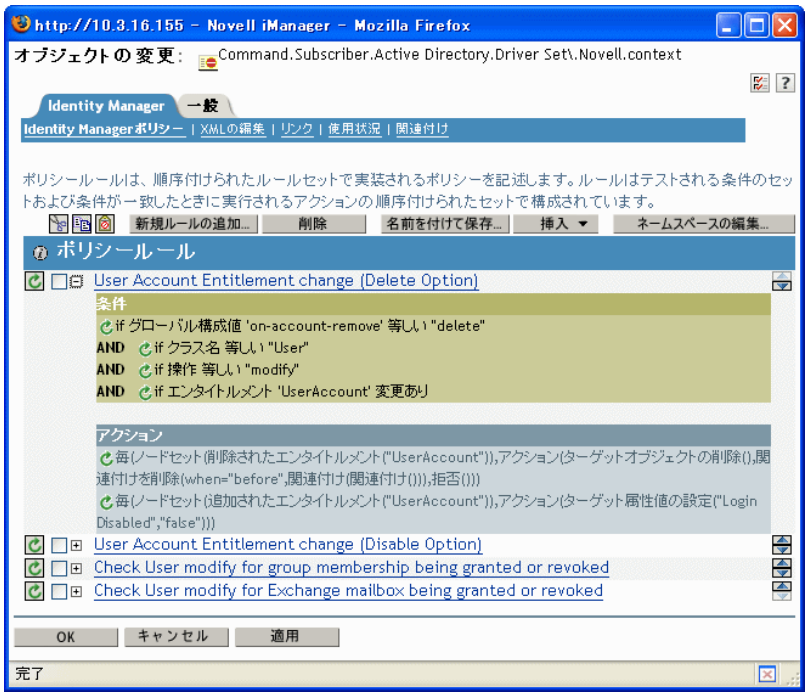
3. ［Identity Manager の概要］ページで、表示されているドライバセットからドライバオブジェクトを選択します。



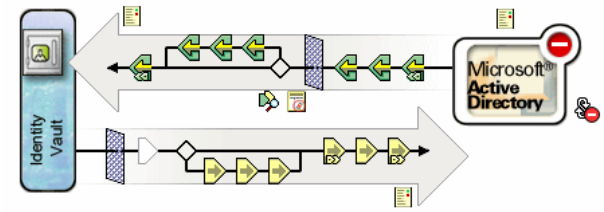
4. ［ドライバセット］のドライバをダブルクリックし、ドライバのページを表示します。ドライバの中央で［すべてのポリシーを表示］アイコンをクリックします (赤い丸で示しています)。



5. ［すべてのポリシーを表示］画面からポリシーを選択すると、ポリシーを構成する条件およびアクションを表示できます。



6. ポリシーの背後にある実際の XML コードを表示するには、ドロップダウンメニューから［XML の編集］を選択します (このメニューのデフォルトは［Identity Manager ポリシー］です)。ポリシーの作成および編集の詳細については、『*Policy Builder and Driver Customization Guide*』を参照してください。また、そのドライバ固有のポリシーを作成するには、選択した Identity Manager ドライバのガイド (http://www.novell.com/documentation/dirxmldrivers/index.html) を参照してください。
7. 有効化されたエンタイトルメントを持つ事前設定済みのドライバ (Active Directory など) に付属しているエンタイトルメントを表示するには、ステップ 1 ～ステップ 4 を実行し、ドライバの中央の［すべてのエンタイトルメントを表示］アイコンを選択します (赤い丸で示しています)。



8. ［エンタイトルメントの管理］ページでエンタイトルメント名をクリックし、XML ビューアにエンタイトルメントを表示します。エンタイトルメントのコードを編集するには、［XML 編集の有効化］をクリックします。

有効化されたエンタイトルメントを持つ Active Directory ドライバには、3 つのエンタイトルメント (ユーザアカウント、グループ、および Exchange メール) が付属しています。

図 6-1 *AD* ドライバに付属しているエンタイトルメント

177 ページのセクション 6.4.6「独自のエンタイトルメントを作成するためのエンタイトルメントの例」の記述サンプルの一部として、これらのエンタイトルメントの XML コードを表示できます。

6.4.2 Novell のエンタイトルメントのドキュメントタイプ定義 (DTD) の使用

いくつかのエンタイトルメントは、有効化されたエンタイトルメントを持つドライバで事前定義されています。これらのエンタイトルメントを使用するか、iManager または Designer で独自のエンタイトルメントを作成できます。独自のエンタイトルメントを作成するには、エンタイトルメントを作成する例として、次の Novell エンタイトルメント DTD を使用します。

この DTD の説明では、iManager を介してこの XML 形式でエンタイトルメントを記述する方法の 4 つの例を示します。XML 形式について詳しくない場合は、より簡単にエンタイトルメントを作成できる Designer のエンタイトルメントウィザードを使用してください。

Novell のエンタイトルメント DTD

```
<!-************************************************************-->
<!-- DirXML Entitlements DTD <!-- Novell Inc. <!-- 1800 South Novell
Place <!-- Provo, UT 84606-6194 <!-- Version=1.0.0 <!-- Copyright 2005
Novell, Inc. All rights reserved --> <!--
********************************************************** --> <!--
Entitlement definition stored in the XmlData attribute of a DirXML-
Entitlement object.--> <!ELEMENT entitlement (values?)> <!ATTLIST
entitlement conflict-resolution (priority | union) "priority" display-
name CDATA #REQUIRED description CDATA #REQUIRED > <!ELEMENT values
(query-app | value+)?> <!ATTLIST values multi-valued (true | false)
"true" > <!ELEMENT value (#PCDATA)> <!ELEMENT query-app (query-xml,
result-set)> <!ELEMENT query-xml ANY> <!ELEMENT result-set (display-
name, description, ent-value)> <!ELEMENT display-name(token-attr |
token-src-dn | token-association)> <!ELEMENT ent-value (token-
association | token-src-dn | token-attr)> <!ELEMENT description
(token-association | token-src-dn | token-attr)> <!ELEMENT token-
```

```
association EMPTY> <!ELEMENT token-attr EMPTY> <!ATTLIST token-attr
attr-name CDATA #REQUIRED > <!ELEMENT token-src-dn EMPTY> <!--
Entitlement reference stored in the DirXML-EntitlementRef attributeof
a DirXML-EntitlementRecipient or a DirXML-SharedProfile object.-->
<!ELEMENT ref (src?, id?, param?)> <!ELEMENT param (#PCDATA)>
<!ELEMENT id (#PCDATA)> <!ELEMENT src (#PCDATA)> <!-- Entitlement
result stored in the DirXML-EntitlementResult attribute of a DirXML-
EntitlementRecipient object.--> <!ELEMENT result(dn, src, id?, param?,
state, status, msg?,timestamp)> <!ELEMENT dn (#PCDATA)> <!ELEMENT
state (#PCDATA)> <!ELEMENT status (#PCDATA)> <!ELEMENT msg ANY>
<!ELEMENT timestamp (#PCDATA)> <!-- Cached query results stored in the
DirXML-SPCachedQuery attribute of a DirXML-Entitlement object.-->
<!ELEMENT items (item*)> <!ELEMENT item (item-display-name?, item-
description?, item-value)> <!ELEMENT item-display-name (#PCDATA)>
<!ELEMENT item-description (#PCDATA)> <!ELEMENT item-value (#PCDATA)>
<!-- Representation of a DirXML-EntitlementRef within the DirXML
Script and within the operation-data of an operation in an XDS
document.--> <!ELEMENT entitlement-impl (#PCDATA)> <!ATTLIST
entitlement-impl name CDATA #REQUIRED src CDATA #REQUIRED id CDATA
#IMPLIED state (0 | 1) #REQUIRED src-dn CDATA #REQUIRED src-entry-id
CDATA #IMPLIED >
```

6.4.3 エンタイトルメント DTD の説明

エンタイトルメント DTD は、定義、参照、結果、キャッシュされたクエリ、および内部の参照情報の 5 つの部分に分けられます。ヘッダは単なるコメントであり、必須ではありません。DTD では、エンタイトルメント定義のヘッダは次のようになります。

<!-- Entitlement definition stored in the XmlData attribute of a DirXML-Entitlement object.-->

ヘッダの次に要素 (ELEMENT) および属性リスト (ATTLIST) が来ます。以下は、エンタイトルメント定義ヘッダの下にある要素および属性の詳しい説明です。これは、エンタイトルメントを作成するときに重点を置く必要があるメインヘッダです。

<!ELEMENT entitlement (values?)>

ルートレベルの要素は、<entitlement> です。これには、単一、オプション、子の <values> 要素を含めることができます。この後ろには属性リストが来ます。これには、conflict-resolution、display-name、および description が含まれています。衝突の解決では、Priority 属性または Union 属性の値を使用します。

conflict-resolution (priority | union) "priority"

役割ベースエンタイトルメントでは、衝突の解決を使用して、値のあるエンタイトルメントが同じオブジェクトに複数回適用された場合に何が発生するのかを決定します。たとえば、ユーザ U がエンタイトルメントポリシー A およびエンタイトルメントポリシー B のメンバーであるとします。それぞれが同じ値のあるエンタイトルメント E を参照していますが、異なる値を持っています。エンタイトルメントポリシー A のエンタイトルメント E は、値を持っています (a、b、c)。エンタイトルメントポリシー B のエンタイトルメント E は、一連の値を持っています (c、d、e)。

衝突の解決の属性により、どの値をユーザ U に適用するのかが決定します。union に設定されている場合、ユーザ U は両方の値 (a、b、c、d、e) に割り当てられます。priority に設

定されている場合、どのエンタイトルメントポリシーがより高い優先度を持っているのかに応じて、ユーザ U は 1 つの値のみを取得します。

エンタイトルメントが単一の値である場合、優先度によって衝突を解決する必要があります。値を結合すると複数の値が適用されるからです。現在では、役割ベースエンタイトルメントがこの属性を使用していますが、今後はワークフローのエンタイトルメントも使用する場合があります。

display-name CDATA #REQUIRED description CDATA #REQUIRED

リテラルのエンタイトルメント名は、エンタイトルメントで表示される文字である必要はありません。Display-name および Description の属性はエンドユーザの表示のためのものです (Designer では、実際のエンタイトルメント名を使用する代わりに、エンタイトルメントの表示名を選択するオプションがあります)。

<!ELEMENT values (query-app | value+)?> <!ATTLIST values multi-valued (true | false) "true"

<values> 要素は必須ではありません。これは、エンタイトルメントに値があることを示します。この要素を使用しない場合、エンタイトルメントには値がないことを示します。値のあるエンタイトルメントの例としては、配布リストを付与するエンタイトルメントがあります。値のないエンタイトルメントの例としては、Active Directory ドライバに付属しているユーザアカウントのエンタイトルメントなど、アプリケーションでアカウントを付与するエンタイトルメントがあります。

値のあるエンタイトルメントは、値を 3 つのソースから受信します。1 つのソースは、(<query-app> 要素によって設計された) 外部アプリケーションです。もう 1 つは、値が列挙されている事前定義されたリストからです (1 つ以上の <value> 要素)。3 番目のソースは、エンタイトルメントのクライアントからです (<value> 子を持たない <values> 要素)。例を使用して、値が機能する様子を説明します。

値のあるエンタイトルメントは single-valued または multi-valued の場合があり、デフォルトは multi-valued です。この制限が適用されるのは、エンタイトルメントのクライアントの作業です。

<!ELEMENT value (#PCDATA)>

エンタイトルメント値は、入力されない文字列です。

<!ELEMENT query-app (query-xml, result-set)>

値が (電子メール配布リストなどの) 外部アプリケーションから生成された場合、<query-xml> 要素を介してアプリケーションクエリを指定する必要があります。<result-set> 要素を介してクエリから結果を抽出します。178 ページの 「例 2: アプリケーションクエリのエンタイトルメント : 外部クエリ」 では、この 2 つの例を示しています。

<!ELEMENT query-xml ANY>

XML クエリは XDS 形式です。接続されたアプリケーションからオブジェクトを検索したり読み取るには、<query-xml> コマンドが使用されます。DirXML ルール、オブジェクトの移行などの機能は、クエリコマンドのドライバの実装に依存します。XML クエリの詳細については、Novell のクエリに関する開発者用マニュアル (http://developer.novell.com/ndk/doc/dirxml/dirxmlbk/ref/ndsdtd/query.html) を参照してください。

<!ELEMENT result-set (display-name, description, ent-value)> <!ELEMENT display-name(token-attr | token-src-dn | token-association)> <!ELEMENT ent-value (token-association | token-src-dn | token-attr)> <!ELEMENT description (token-association | token-src-dn | token-attr)> <!ELEMENT

token-association EMPTY> <!ELEMENT token-attr EMPTY> <!ATTLIST token-attr attr-name CDATA #REQUIRED

外部アプリケーションクエリの結果を解釈するには、結果セットの要素を使用します。対象となるデータは、値の表示名 (display-name 子要素)、値の説明 (description 子要素)、および文字列のエンタイトルメント値 (ent-value 子要素。これは表示されません) の 3 つです。

token 要素の <token-src-dn>、<token-association>、<token-attr> は、実際には、src-dn 属性値、関連付けの値、または任意の属性値を XDS 形式の XML ドキュメントからそれぞれ抽出する、XPATH 形式のプレースホルダです。DTD では、クエリ結果が XDS であると想定されています。

DTD の他のヘッダ

エンタイトルメント DTD の残りのエンタイトルメントのヘッダは異なる機能を持っていますが、エンタイトルメントを作成するときに注目する必要がある項目ではありません。

<!-- Entitlement reference stored in the DirXML-EntitlementRef attribute of a DirXML-EntitlementRecipient or a DirXML-SharedProfile object.-->

DTD のエンタイトルメント参照の部分に保存された情報は、エンタイトルメントオブジェクトを指します。この情報は、(役割ベースエンタイトルメントドライバ、Entitlement.xml、または認証フロードライバ、UserApplication.xml などの) 管理エージェントによって配置されます。これは、接続システムで発生するアクションのトリガイベントです。このヘッダの DTD では何もする必要はありませんが、エンタイトルメントオブジェクトが参照されることを確認するためにこの情報を使用できます。

<!-- Entitlement result stored in the DirXML-EntitlementResult attribute of a DirXML-EntitlementRecipient object.-->

エンタイトルメントの結果部分は、エンタイトルメントが付与されたかまたは取り消されたかに関する結果をレポートします。情報には、イベントの状態またはステータス、および (タイムスタンプを介して) いつイベントが付与または取り消されたのかが含まれています。このヘッダの要素および属性では、何もする必要はありません。

<!-- Cached query results stored in the DirXML-SPCachedQuery attribute of a DirXML-Entitlement object.-->

エンタイトルメントのクエリ部分には、外部アプリケーションから収集されたエンタイトルメント値が含まれています。この情報を表示するためにエンタイトルメントのクライアントが必要である場合、この情報を再度使用できます。これらの値は、エンタイトルメントオブジェクトの DirXML-SPCachedQuery 属性に保存されています。このヘッダの要素および属性では、何もする必要はありません。

<!-- Representation of a DirXML-EntitlementRef within the DirXML Script and within the operation-data of an operation in an XDS document.-->

DTD では複数のドキュメントの値が定義されるため、この EntitlementRef 部分は、実際にはエンタイトルメント定義の一部ではありません。このヘッダの要素および属性では、何もする必要はありません。

6.4.4 Designer を介したエンタイトルメントの作成

176 ページのセクション 6.4.5「iManager でのエンタイトルメントの作成および編集」の例ではエンタイトルメントを記述するための実際の XML コードを示していますが、Identity Manager に付属している Designer ユーティリティを使用すると、エンタイトルメントをより簡単に記述できます。Designer モデラで Identity Manager ドライバをアイデンティティボールトに追加した後、［Outline (アウトライン)］ビューでドライバを右クリックし、［エンタイトルメントの追加］を選択します。エンタイトルメントウィザードでは、エンタイトルメントのタイプの指定を要求され、ステップごとに作成できます。

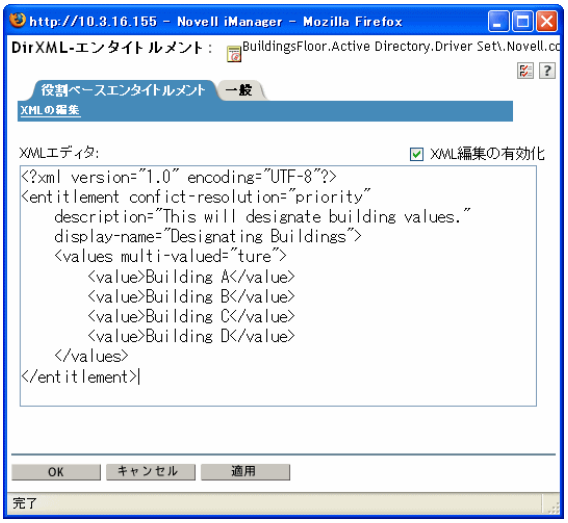
エンタイトルメントウィザードの使用の詳細については、『Designer for Identity Manager 3: Administration Guide』を参照してください。

6.4.5 iManager でのエンタイトルメントの作成および編集

エンタイトルメントの作成には Designer のエンタイトルメントウィザードを使用することをお勧めしますが、iManager を介してエンタイトルメントを作成できます。

1. Identity Manager ユーティリティのヘッダの［Create Entitlements (エンタイトルメントの作成)］オプションを選択します。
2. ［Create Entitlements (エンタイトルメントの作成)］ページで、エンタイトルメントの名前を入力し、オブジェクトブラウザを使用してエンタイトルメントが属している Identity Manager ドライバオブジェクトを検索します。

3. ［作成後に詳細を設定］がオンになっている場合、このエンタイトルメントの要素を定義する［XML エディタ］ページが表示されます。



4. エンタイトルメントに要素を追加するには、［XML 編集の有効化］をオンにします。

注 **:** エンタイトルメントの名前は変更しないでください。エンタイトルメント名を後で変更する場合、エンタイトルメントで実装するポリシー内のすべての参照も変更する必要があります。エンタイトルメント名は、ポリシー内の Ref 属性および Result 属性に保存されます。

6.4.6 独自のエンタイトルメントを作成するためのエンタイトルメントの例

次の 2 つのタイプのエンタイトルメントを作成できます。値のないエンタイトルメントと値のあるエンタイトルメントの 2 つのタイプのエンタイトルメントを作成できます。値のあるエンタイトルメントは、外部クエリ、管理者が定義したリスト、または自由形式から値を取得できます。作成できる 4 つのタイプのエンタイトルメントの例を以下に示します。

注 **:** 右向きの不等号 (<) の付いていない行がある場合、行はラップされており、情報が 2 行 (または 3 行) ではなく、通常は 1 行に表示されていることを意味します。これらは、アカウントのエンタイトルメント以外は、それぞれのタイプの値のあるエンタイトルメント用に作成できる単なる例です。

例 1: アカウントのエンタイトルメント : 値なし

```
<?xml version="1.0" encoding="UTF-8"?> <entitlement conflict-
resolution="priority" description="This is an Account Entitlement"
display-name="Account Entitlement"/>
```

この例では、値のないエンタイトルメントの名前は「Account」です。この後ろには、デフォルト設定の優先度を持つ conflict-resolution 行があります。これはたいていの場合、エンタイトルメントが役割ベースエンタイトルメントに使用されている場合、優先度を持つ RBE によって値が設定されることを意味します (しかし、これは値のないエンタイトルメントの例であるため、値のある設定には適用されません)。エンタイトルメントの説明は「This is an Account Entitlement」であり、表示名は「Account Entitlement」です。これが、アカウントのエンタイトルメントを作成するために必要なすべての情報です。これは、アプリケーションでアカウントを付与するために使用できます。

有効化されたエンタイトルメントを持つ Active Directory ドライバには、ユーザアカウントの付与または取り消しのために Active Directory によって使用される UserAccount エンタイトルメントがあります。

```
<?xml version="1.0" encoding="UTF-8"?> <entitlement conflict-
resolution="union" description="The User Account entitlement grants or
denies an account in ActiveDirectory for the user.When granted, the
user is given an enabled logon account.When revoked, the logon account
is either disabled or deleted depending on how the drive is
configured."display-name="User Account Entitlement"
name="UserAccount"> </entitlement>
```

この例では、衝突の解決は Union です。これにより、エンタイトルメントは割り当てられた値をマージできます (繰り返しますが、値のある設定は値のないエンタイトルメントには適用されません)。［Description］フィールドでは、このエンタイトルメントの使用目的、および作成理由を説明します。これは、エンタイトルメントを今後変更するユーザにとっては便利な情報です。管理エージェントには、ユーザアカウントのエンタイトルメントとして <display-name> が表示されますが、エンタイトルメントの実際の名前は UserAccount です。

例 2: アプリケーションクエリのエンタイトルメント : 外部クエリ

有効なエンタイトルメントを持つ Active Directory ドライバが付属している Group および Exchange メールボックスエンタイトルメントでは、アプリケーションクエリの例を提供しています。イベントを実行するために接続システムからの外部情報が必要な場合、このエンタイトルメントのタイプを使用します。

```
<?xml version="1.0" encoding="UTF-8"?> <entitlement conflict-
resolution="union" description="The Group Entitlement grants or denies
membership in a group in Active Directory.The group must be associated
with a group in the Identity Vault.When revoked, the user is removed
from the group.The group membership entitlement is not enforced on the
publisher channel: If a user is added to a controlled group in Active
Directory by some external tool, the user is not removed by the
driver.Further, if the entitlement is removed from the user object
instead of being simply revoked, the driver takes no action."
display-name="Group Membership Entitlement" name="Group"> <values>
<query-app> <query-xml> <nds dtd-version="2.0"> <input> <query class-
name="Group" scope="subtree"> <search-class class-name="Group"/>
<read-attr attr-name="Description"/> </query> </input> </nds> </query-
xml> <result-set> <display-name> <token-src-dn/> </display-name>
<description> <token-attr attr-name="Description"/> </description>
<ent-value> <token-association/> </ent-value> </result-set> </query-
app> </values> </entitlement>
```

この例では、エンタイトルメントが複数回同じオブジェクトに適用された場合、グループのエンタイトルメントは Union を使用して衝突を解決します。Union 属性により、関連するすべての役割ベースエンタイトルメントポリシーのエンタイトルメントがマージされます。したがって、1 つのポリシーがエンタイトルメントを取り消し、その他のポリシーがエンタイトルメントを付与した場合、最終的にはエンタイトルメントが付与されます。

グループの説明は、ドライバのポリシーのルールを介して何が設定されたかを詳しく説明するため便利です。この説明は、最初にエンタイトルメントを定義するときに、どの程度詳しく説明するのかを知るための良い例です。

<display-name> はグループメンバーシップのエンタイトルメントです。これは役割ベースのエンタイトルメントの iManager などの管理エージェントに表示されます。名前はエンタイトルメントの相対識別名 (RDN) です。表示名を定義しない場合、エンタイトルメントの名前はその RDN です。

初期のクエリ値により、ツリーのトップでグループのクラス名が検索され、サブツリーも検索されます。これらの値は接続されている Active Directory サーバから取得したものであり、<nds> タグでアプリケーションクエリが開始されます。<query-xml> タグで、次に類似した情報をこのクエリが受信します。

```
<instance class-name="Group" src-dn="o=Blanston,cn=group1">
<association>o=Blanston,cn=group1</association> <attr attr-
name="Description"> the description for group1</attr> </instance>
<instance class-name="Group" src-dn="o=Blanston,cn=group2">
<association>o=Blanston,cn=group2</association> <attr attr-
name="Description"> the description for group2</attr> </instance>
<instance class-name="Group" src-dn="o=Blanston,cn=group3">
<association>o=Blanston, cn=group3</association> <attr attr-
name="Description"> the description for group3</attr> </instance> <!--
...->
```

次に、クエリから受け取った情報が、<result-set> タグの下のさまざまなフィールドに挿入されます。たとえば、<display-name> フィールドには o=Blanston,cn=group1 が挿入されます。<description> フィールドには the description for group1 が挿入され、<ent-value> フィールドには o=Blanston,cn=group1 が挿入されます。複数のグループが存在し、クエリの条件を満たしたため、この情報も収集されて他のインスタンスとして表示されました。

注 **:** 関連付け形式の値はすべての外部システムで一意であるため、問い合わせが行われた各外部システムで形式および構文は異なります。

その他の例としては Exchange メールボックスエンタイトルメントがあります。

```
<?xml version="1.0" encoding="UTF-8"?> <entitlement conflict-
resolution="union" description="The Exchange Mailbox Entitlement
grants or denies an Exchange mailbox for the user in Microsoft
Exchange." display-name="Exchange Mailbox Entitlement"
name="ExchangeMailbox"> <values> <query-app> <query-xml> <nds dtd-
version="2.0"> <input> <query class-name="msExchPrivateMDB" dest-
dn="CN=Configuration," scope="subtree"> <search-class class-
name="msExchPrivateMDB"/> <read-attr attr-name="Description"/> <read-
attr attr-name="CN"/> </query> </input> </nds> </query-xml> <result-
set> <display-name> <token-attr attr-name="CN"/> </display-name>
<description> <token-attr attr-name="Description"/> </description>
<ent-value> <token-src-dn/> </ent-value> </result-set> </query-app> </
values> </entitlement>
```

この例では、エンタイトルメントが複数回同じオブジェクトに適用された場合、Exchange メールボックスのエンタイトルメントは Union を使用して衝突を解決します。Union 属性により、関連するすべての役割ベースエンタイトルメントポリシーのエンタイトルメントがマージされます。したがって、1 つのポリシーがエンタイトルメントを取り消し、その他のポリシーがエンタイトルメントを付与した場合、最終的にはエンタイトルメントが付与されます。

説明は、エンタイトルメントが Microsoft Exchange のユーザの Exchange メールボックスを付与または取り消すことを示します。エンタイトルメントの詳細としてはこれで十分です。display-name は Exchange メールボックスのエンタイトルメントです。これは役割ベースエンタイトルメントの iManager などの管理エージェントに表示されます。名前はエンタイトルメントの相対識別名 (RDN) です。表示名を定義しない場合、エンタイトルメントの名前はその RDN です。

初期のクエリ値によって msExchPrivateMDB のクラス名が検索されます。これは、Configuration のコンテナを検索し始め、サブツリーを検索し続ける Microsoft Exchange の機能呼び出しです。これらの値は接続されている Active Directory データベースから取得したものであり、アプリケーションクエリは <nds> タグで開始されます。eDirectory には msExchPrivateMDB のクラスと同等のものがありません。したがって、そのようなクエリを実行する Microsoft Exchange の機能呼び出しに精通している必要があります。しかし、Active Directory ドライバで見つかったルールおよびポリシーがあるため、クエリは完了します。

エンタイトルメントコンシューマでは、クエリによって取得された情報が使用されます。たとえば、DirXML-EntitlementRef 属性を介して、エンタイトルメント値 (ent-value) が Identity Manager ポリシーに渡されます。iManager またはユーザアプリケーションによって表示名および説明情報が表示され、DirXML-SPCachedQuery 属性に保存されます。

例 3: 管理者定義のエンタイトルメント : リスト付き

3 番目の例は、リストエントリを選択した後に付与または取り消しのイベントを作成する管理者定義のエンタイトルメントです。

```
<?xml version="1.0" encoding="UTF-8"?> <entitlement conflict-
resolution="union" description="This will show Administrator-defined
Values"> <display-name="Admin-defined Entitlement"/> <values multi-
valued="true"> <value>Building A</value> <value>Building B</value>
<value>Building C</value> <value>Building D</value> <value>Building
E</value> <value>Building F</value> </values> </entitlement>
```

この例では、エンタイトルメント名は、定義された管理者定義のエンタイトルメントの表示名を持つ管理者定義です (エンタイトルメントの RDN とは異なる表示名にする場合のみ、表示名を設定する必要があります)。conflict-resolution の行は Union の設定を表します。これにより、エンタイトルメントは割り当てられた値をマージできます。

エンタイトルメントの説明は「This will show Administrator-defined Values」です。multi-value 属性は true に設定されます。これにより、エンタイトルメントが値を複数回割り当てることが可能になります。この例では、値は次の会社のビルの文字です。「Building A」から「Building F」。次に、iManager RBE タスクなどのエンタイトルメントのクライアントを介して、またはユーザアプリケーションを介して、ユーザまたは定義されたタスクマネージャはビルの情報を指定できます。これは、Novell eDirectory などの外部アプリケーションに含まれます。

例 4: 管理者定義のエンタイトルメント : リストなし

4 番目の例は、エンタイトルメントがイベントを付与または取り消す前に、値の入力を管理者に強制する管理者定義のエンタイトルメントです。初期の設定ですべての情報を持っていないためにタスクリストを作成できない場合、この種類のエンタイトルメントを使用できます。

```
<?xml version="1.0" encoding="UTF-8"?> <entitlement conflict-
resolution="priority" description="There will be no pre-defined list">
<values multi-valued="false"/> </entitlement>
```

この例では、エンタイトルメント名は管理者定義 (リストなし) であり、表示名のエントリがないときに表示名としてエンタイトルメント名を使用します。衝突の解決がデフォルトである優先度に再度設定されます。つまり、役割ベースエンタイトルメントによってエンタイトルメントが使用された場合、優先度を持つ RBE によって値が設定されます。iManager RBE タスクなどのエンタイトルメントのクライアントを介して、またはユーザアプリケーションを介して、ビルの情報を指定します。これは、eDirectory などの外部アプリケーションに含まれます。

6.4.7 エンタイトルメントの作成のステップの完了

162 ページのセクション 6.2「エンタイトルメントの作成 : 概要」で説明したように、エンタイトルメントの作成の例で、エンタイトルメントの作成および使用の 2 つのステップを通じて、作業方法を紹介しました。これには、ステップ 1 であるエンタイトルメントで何を実行するのかのチェックリストの作成と、ステップ 2 であるチェックリストの項目に対応するためのエンタイトルメントの記述が含まれています。ステップ 3 である、Identity Manager ドライバのポリシーの作成はこの章の範囲外です。ポリシーの作成および編集の詳細については、『*Policy Builder and Driver Customization Guide*』および該当する Identity Manager ドライバのガイド (http://www.novell.com/documentation/idmdrivers/index.html) を参照してください。

エンタイトルメントを作成した後に (または、特定の Identity Manager ドライバで事前設定済みのエンタイトルメントを使用した後に)、それらを管理する必要があります。これはステップ 4 です。エンタイトルメントは、2 つのパッケージまたはエージェントによって、つまり役割ベースエンタイトルメントポリシーとしての iManager を介して、またはワークフローベースのプロビジョニングのユーザアプリケーションを介して管理されます。For entitlements used in workflow-based provisioning, see “Introduction to Workflow-Based Provisioning.” この章の残りの部分では、役割ベースエンタイトルメントに焦点を当てます。

6.5 役割ベースエンタイトルメントの管理の概要

従来、接続システムのエンタイトルメントはドライバごとに管理され、その方法はポリシービルダで作成するポリシーのようなドライバ設定ポリシーの作成と編集に限られていました。この従来型の分散モデルでは、別の管理者が各 Identity Manager ドライバと接続システムを管理することがほとんどで、システムのリソースをユーザが利用できるかどうかを決定するビジネスポリシーは、各接続システムドライバのドライバ設定ポリシーで別々に「ハードコード」されます。

役割ベースエンタイトルメントモデルは、1 人または少数の管理者がエンタイトルメントポリシーを制御する権利を持つ環境に適しています。このような管理者は、Identity Manager 全体を理解している必要がありますが、役割ベースエンタイトルメントインタフェースを使用するために Identity Manager または XSLT または DirXML スクリプトに関する十分な専門知識はなくてもかまいません。

条件が一致した場合、役割ベースエンタイトルメントポリシーによりビジネスリソースを自動的に付与または取り消すことができます。エンタイトルメントとは、リソースへのアクセスの許可書のようなものです。許可書があると指定したリソースにアクセスでき、そのような許可書がないとアクセスできません。実際の例としては、ユーザが条件 1、2、および 3 を満たさない場合は、役割ベースエンタイトルメントポリシーを介してユーザが

グループ H のメンバーになる一方で、ユーザが条件 4 および 5 を満たす場合はユーザがグループ I のメンバーになるように指定できます。

役割ベースエンタイトルメントの管理を設定するには、次の 3 つのステップを行います。

1. まだ実行していない場合は、164 ページのセクション 6.2.2「他の Identity Manager ドライバでのエンタイトルメントの有効化」で説明したとおりに、Identity Manager ドライバオブジェクトの DirXML-EntitlementRef 属性を有効にします。
2. 183 ページのセクション 6.6「エンタイトルメントサービスドライバオブジェクトの作成」で説明したとおりに、エンタイトルメントサービスドライバ (Entitlement.xml) をインストールします。
3. 184 ページのセクション 6.7「エンタイトルメントポリシーの作成」で説明したとおりに、iManager で役割ベースエンタイトルメントポリシーを作成します。

6.5.1 エンタイトルメントサービスドライバの機能方法

役割ベースエンタイトルメントは、エンタイトルメントサービスドライバ (Entitlement.xml) に依存しています。このドライバは、エンタイトルメントポリシーでユーザがメンバーシップを持っているかどうかを監視するエンジンサービスです。ユーザがエンタイトルメントポリシーのダイナミックグループのダイナミックメンバーシップ条件に合致するか、またはそのメンバーシップにスタティックに含まれる場合、エンタイトルメントサービスドライバは、ユーザオブジェクトの DirXML-EntitlementRef 属性の情報を更新します。

163 ページのセクション 6.2.1「エンタイトルメントをサポートする、事前設定済みの Identity Manager ドライバ」に一覧表示したシステムについては、Identity Manager ドライバ設定をインポートするときにエンタイトルメントを有効にできます。Identity Manager には、エンタイトルメント、エンタイトルメントを実装するためのポリシー、およびエンタイトルメントアクティビティのリッスンが有効になっているドライバがすでに含まれている、事前設定済みのいくつかのドライバが付随しています。提供されたポリシーをレビューすることができます。これらのポリシーでは、DirXML-EntitlementRef 属性を監視し、エンタイトルメントを付与または取り消すことにより、エンタイトルメントがサポートされています。

次のいずれかが発生した場合のみ、エンタイトルメントサービスドライバによって DirXML-EntitlementRef 属性が更新されます。

- ［メンバーシップの再評価］タスクを使用した場合
- ツリーのどの部分でユーザを再評価するかを指定した場合
- ユーザが移動した場合
- ユーザが名前変更された場合
- エンタイトルメントポリシーのメンバーシップに使用される属性が変更された場合

エンタイトルメントポリシーを使用すると、接続システム上のエンタイトルメントおよびアイデンティティボールトでの権限を付与することができます。接続システムのエンタイトルメントには、次のものがあります。

- アカウント
- 電子メール配布リストのメンバーシップ
- グループメンバーシップ

- 指定した値が入力された、接続システムで対応するオブジェクトの属性
- 配置
- その他のカスタマイズ可能なエンタイトルメント

エンタイトルメントで作成できるいくつかのオプションについて、有効化されたエンタイトルメントを持つドライバ設定で示しています。

各ドライバセットで使用するエンタイトルメントサービスドライバは 1 つであるため、エンタイトルメントポリシーが管理できるのは、当該ドライバセットに関連付けられているサーバ上の読み書き可能レプリカまたはマスタレプリカに含まれるユーザだけです。

役割ベースエンタイトルメントポリシーの機能は、Identity Manager に基づいています。したがって、接続システムを管理するには、Identity Manager ドライバをインストールして適切に設定し、Identity Manager プラグインをインストールする必要があります。

さらに、エンタイトルメントポリシーの割り当てと Identity Manager ドライバ設定との間に衝突が発生するのを回避するため、ビジネスポリシーと、それらのポリシーが Identity Manager でどのように管理されているかに注意してください。Identity Manager のエンタイトルメントポリシーおよびドライバ設定のポリシーは、属性を管理している間は重複または衝突することはできません。

6.6 エンタイトルメントサービスドライバオブジェクトの作成

エンタイトルメントポリシーを作成するには、エンタイトルメントサービスドライバオブジェクトが必要です。ドライバセットごとに 1 つ作成する必要があります。

オブジェクトがない場合は、[役割ベースエンタイトルメント] の役割およびタスクをクリックした際に、エンタイトルメントサービスドライバオブジェクトを作成するようプロンプトが表示されます。

1 エンタイトルメントサービスドライバがすでにあるかどうかを調べます。

iManager で [役割ベースエンタイトルメント] > [役割ベースエンタイトルメント] の順にクリックし、ドライバセットを選択します。

- [エンタイトルメントサービスドライバはありません] ページが表示された場合は、ステップ 2 に進み、エンタイトルメントサービスオブジェクトを作成します。
- エンタイトルメントポリシーのリストを示す [役割ベースエンタイトルメント] ページが表示された場合は、エンタイトルメントサービスオブジェクトはすでに存在します。このステップを実行する必要はありません。続いて、184 ページのセクション 6.7「エンタイトルメントポリシーの作成」に進みます。

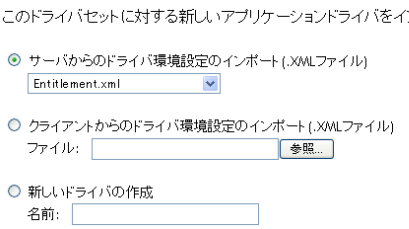
2 [エンタイトルメントサービスドライバはありません] ページで、[はい] をクリックします。

ドライバ作成ウィザードが開きます。

[*DirXML* ユーティリティ] > [ドライバのインポート] の順にクリックすることもできます。

3 ドライバの作成ウィザードのページで、[既存のドライバセットの中] を選択し、[次へ] をクリックします。

4 ［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)］ドロップダウンリストで、［Entitlement.xml］を選択します。



5 エンタイトルメントサービスドライバオブジェクトに名前を付け (またはデフォルトの名前を受け入れ)、［次へ］をクリックします。

正しいドライバ設定ファイルは、自動的に選択されます。ドライバオブジェクトの名前を指定するか、デフォルトを使用します。

6 同等セキュリティを定義するか、管理の役割を除外することをお勧めします。これらの両方に対して Admin ユーザを追加し、［次へ］をクリックします。

7 サマリを確認して、［終了］をクリックします。

エンタイトルメントドライバのドライバシムは、Identity Manager をインストールしたときにデフォルトでインストールされます。エンタイトルメントドライバの設定ファイルは、iManager サーバに Identity Manager プラグインをインストールする際にデフォルトでインストールされます。

ウィザード完了後、エンタイトルメントのプラグインにアクセスし、このドライバセットに対して役割ベースエンタイトルメントポリシーの作成を開始できます。

6.7 エンタイトルメントポリシーの作成

- 186 ページのセクション 6.7.1「エンタイトルメントポリシーのためのメンバーシップの定義」
- 188 ページのセクション 6.7.2「エンタイトルメントポリシーのためのエンタイトルメントの選択」

エンタイトルメントポリシーを作成するには、提供されるウィザードを使用します。

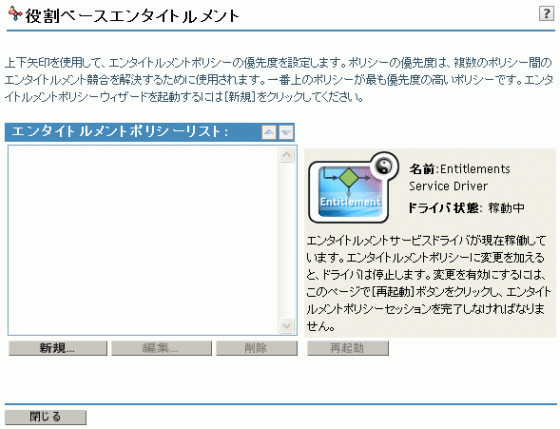
1 エンタイトルメントサービスドライバが設定されていること、および必要なドライバ設定が作成されていることを確認します。

2 iManager で、［役割ベースエンタイトルメント］>［役割ベースエンタイトルメント］の順にクリックします。

3 ドライバセットを選択します。

エンタイトルメントポリシーは、ドライバセットごとに設定します。

既存のエンタイトルメントポリシーのリストが、次の図に示されるページのように開きます。初めて役割ベースのエンタイトルメントを使用する場合は、リストに表示されるポリシーはありません。



4 [新規]をクリックします。

エンタイトルメントポリシーウィザードが開きます。

5 ウィザードのステップ 1 ～ステップ 6 に従って、新しいポリシーを作成します。ウィザードの各ステップについては、オンラインヘルプを参照してください。

5a ステップ 1 で、ポリシーに名前を付けておよび説明を入力します。

5b ステップ 2 で、検索パラメータをフィルタ処理するメンバーシップを定義します。

5c ステップ 3 で、検索条件のメンバーを含めたり除外することによって、スタティックメンバーを定義します。

5d ステップ 4 で、Identity Manager ドライバを選択し、含めるエンタイトルメントを指定します。エンタイトルメントは 167 ページのセクション 6.4「iManager を

介した XML でのエンタイトルメントの記述」で作成しました。［ドライバの追加］をクリックし、追加するエンタイトルメントを選択します。

5e ステップ 5 で、このエンタイトルメントポリシーをトラスティにするオブジェクトを参照します。

5f ステップ 6 で、サマリを読み、エンタイトルメントポリシーが実行したい内容になっていることを確認します。確認後問題なければ［終了］をクリックし、問題があれば［戻る］をクリックします。

6 エンタイトルメントポリシーの作成により、エンタイトルメントサービスドライバがオフになります。［再起動］をクリックしてセッションを完了します。

6.7.1 エンタイトルメントポリシーのためのメンバーシップの定義

Identity Manager ドライバと同様、各エンタイトルメントポリシーが管理できるのは、割り当てられたサーバ上のマスタレプリカまたは読み書き可能レプリカに存在するオブジェクトだけです。各エンタイトルメントポリシーは、特定のサーバに割り当てられている 1 つのドライバセットオブジェクトに関連付けられます。

エンタイトルメントポリシーのメンバーになることができるのは、ユーザオブジェクト (およびユーザのクラスに基づく他のオブジェクトタイプ) だけです。エンタイトルメントポリシーの［メンバーシップ］ページを表示するには、［役割ベースエンタイトルメント］>［役割ベースエンタイトルメント］の順に選択し、エンタイトルメントポリシーリストから編集するエンタイトルメントポリシーをハイライトし、［編集］を選択します。Internet Explorer ブラウザでは［メンバーシップ］タブを選択します。Firefox ブラウザではプルダウンメニューから［ダイナミックメンバーの編集］を選択します。

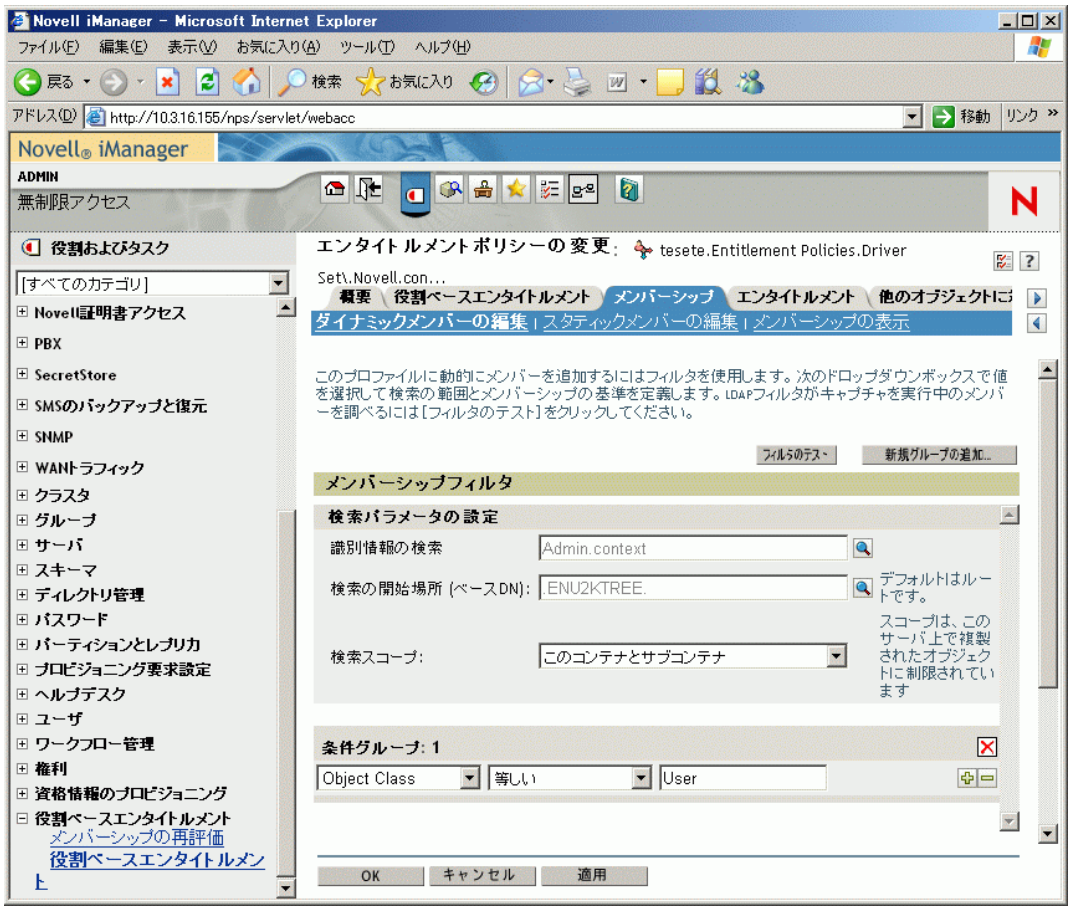
エンタイトルメントポリシーは、ダイナミックグループオブジェクトです。エンタイトルメントポリシーのメンバーシップは、ダイナミックおよびスタティックの 2 つの方法で定義できます。同じエンタイトルメントポリシーで、この両方の方法を使用できます。

- ダイナミック：役職名に「マネージャ」という語が含まれるかなど、オブジェクトの属性値に基づき、メンバーシップの条件を定義できます。指定する条件は、LDAP フィルタに変換されます。

  条件に合致するユーザは自動的にエンタイトルメントポリシーの一部になります。各ユーザを個別にポリシーに追加する必要はありません。ダイナミックメンバーシップは、ダイナミックグループオブジェクトと同様です。

  オブジェクトが変更されダイナミックメンバーシップの条件に合致しなくなった場合は、エンタイトルメントは自動的に取り消されます。

図 6-2 ダイナミックメンバーおよびスタティックメンバーの編集



- スタティック：ダイナミックメンバーシップの条件 (LDAP フィルタ) の作成に加え、特定のユーザを含めたり、除外したりすることができます。

  フィルタの条件に合致しないメンバーは、スタティックに追加できます。フィルタの条件に合致していても、エンタイトルメントポリシーに含める必要がないメンバーは除外できます。

6.7.2 エンタイトルメントポリシーのためのエンタイトルメントの選択

- 188 ページの 「接続システムのアカウント」
- 189 ページの 「電子メール配布リストおよび NOS リストのメンバーシップ」
- 191 ページの 「接続システムの属性値」

エンタイトルメントを使用すると、接続システム上のサービスおよびアイデンティティボールトの権利へのアクセスを付与または取り消すことができます。

インストールする有効なエンタイトルメントを持つドライバは、エンタイトルメントポリシーを使用して割り当てることができるエンタイトルメントのリストに付属しています。エンタイトルメントポリシーで使用できる、独自のエンタイトルメントを作成できます。ドライバが提供できるエンタイトルメントは、ドライバの子オブジェクトです。これは、ドライバおよび接続システムの機能を示すためにドライバ開発者が作成するものです

アイデンティティボールト内のオブジェクトに対するトラスティ権は、エンタイトルメントポリシーのメンバーにすぐに付与されます。デフォルトでは、次にエンタイトルメントポリシーメンバーシップに使用される属性が変更されたとき、またはユーザが別のコンテナに移動されたり名前変更されたりしたときに、接続システムのエンタイトルメントがエンタイトルメントポリシーの各メンバーに付与されます。

接続システムのエンタイトルメントには、次のものがあります。

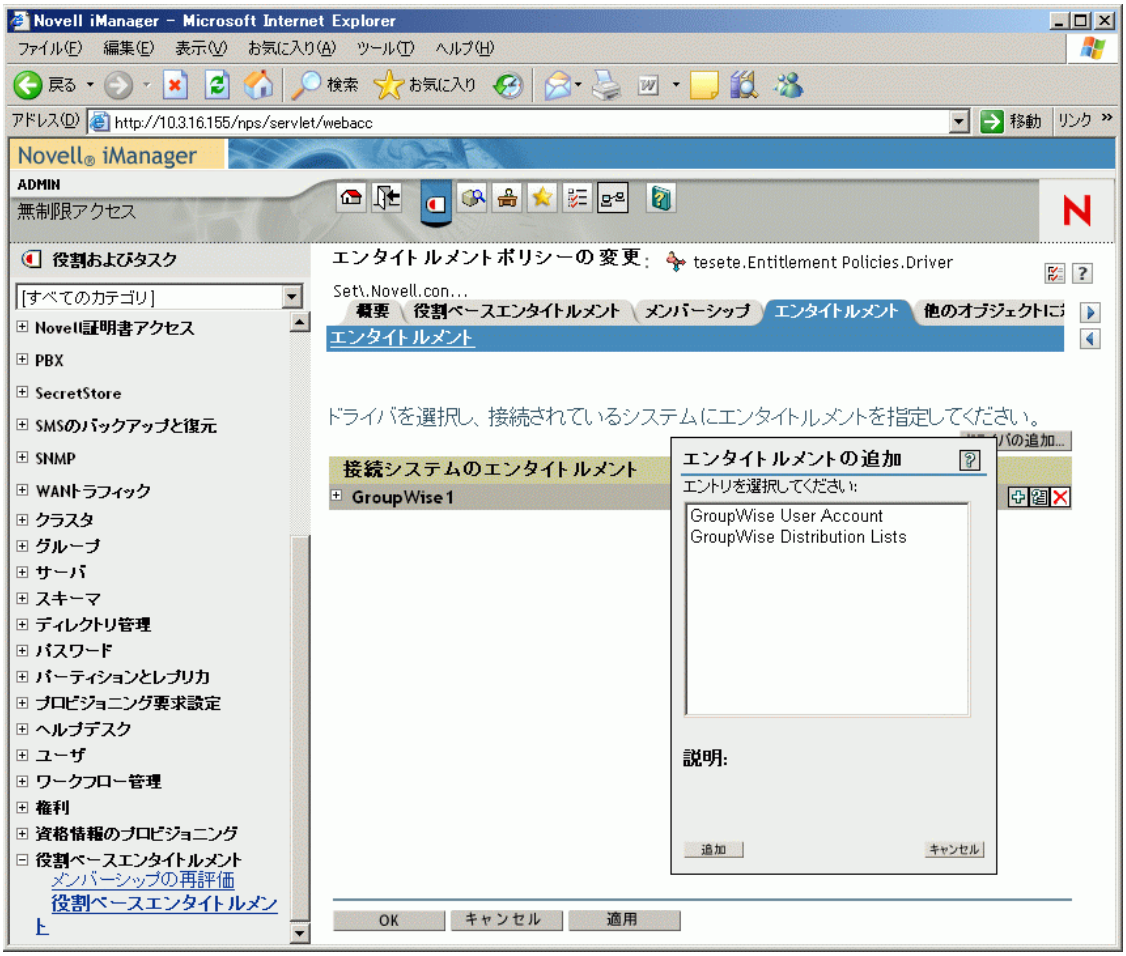
- アカウント
- 電子メール配布リストのメンバーシップ
- NOS リストのグループメンバーシップ
- 指定した値が入力された、接続システムで対応するオブジェクトの属性
- その他のカスタマイズ可能なエンタイトルメント

接続システムのアカウント

エンタイトルメントポリシーにエンタイトルメントを追加するには、[エンタイトルメント] ページに移動してドライバを選択します。ドライバが提供するエンタイトルメントを示すポップアップウィンドウが表示されます。

たとえば、次の図は、GroupWise ドライバにより 2 種類のエンタイトルメントが提供され、リストの先頭に［GroupWise ユーザアカウント］が表示されていることを示します。

図 *6-3* エンタイトルメントを定義するインタフェース



電子メール配布リストおよび NOS リストのメンバーシップ

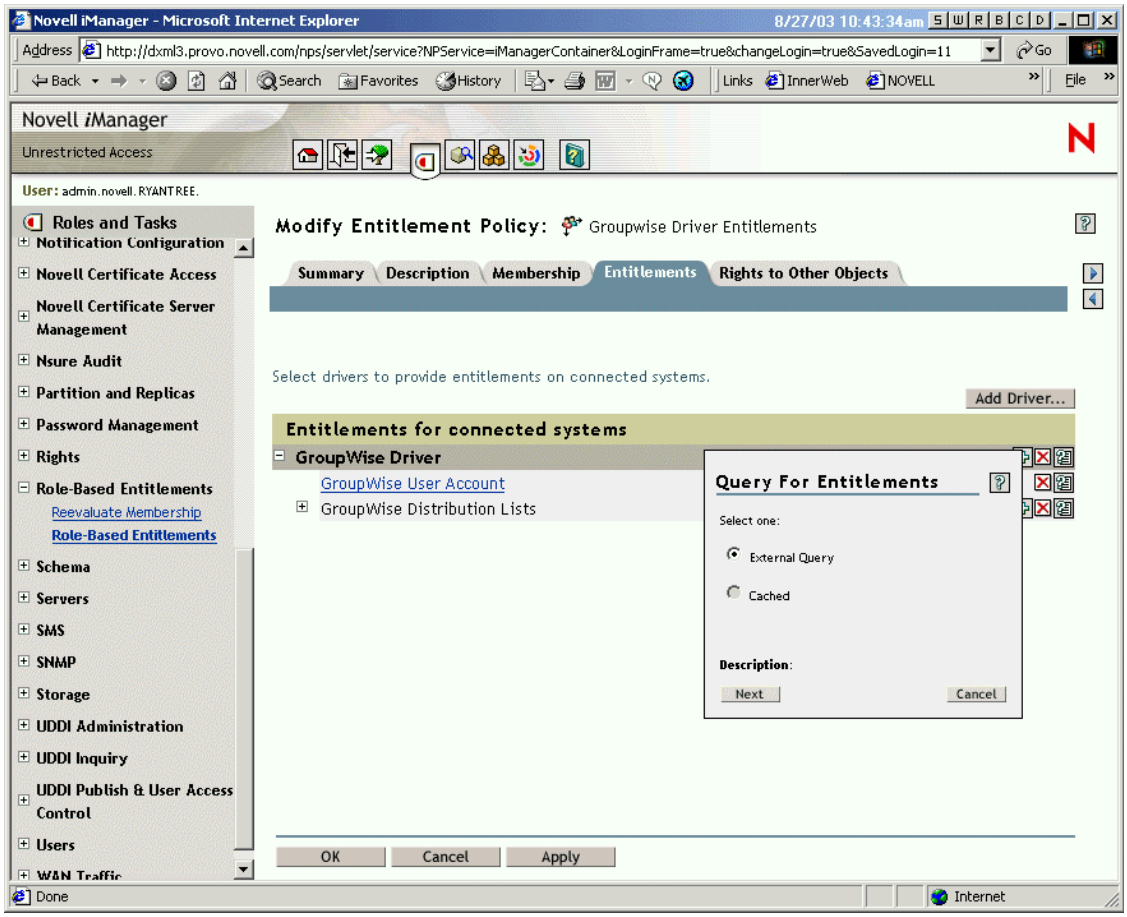
接続システム上のグループにメンバーシップを割り当てるには、ドライバが提供するエンタイトルメントのリストからメンバーシップエンタイトルメントを選択します。

次の図は、［GroupWise 配布リスト］がリストの 2 番目に表示されている例を示します。

図 *6-4* *GroupWise* 配布リストの選択

この例で［GroupWise 配布リスト］を選択した場合、次の図の例のようなクエリポップアップが表示されます。

図 *6-5* エンタイトルメントのクエリ



エンタイトルメントポリシーインタフェースでは、電子メール配布リストまたは NOS リストを問い合わせることができます。クエリが実行された後、キャッシュされたリストを表示するよう選択できます。

ドライバは完全なリストを返すように設定されているので、接続システムに存在するリストから選択できます。

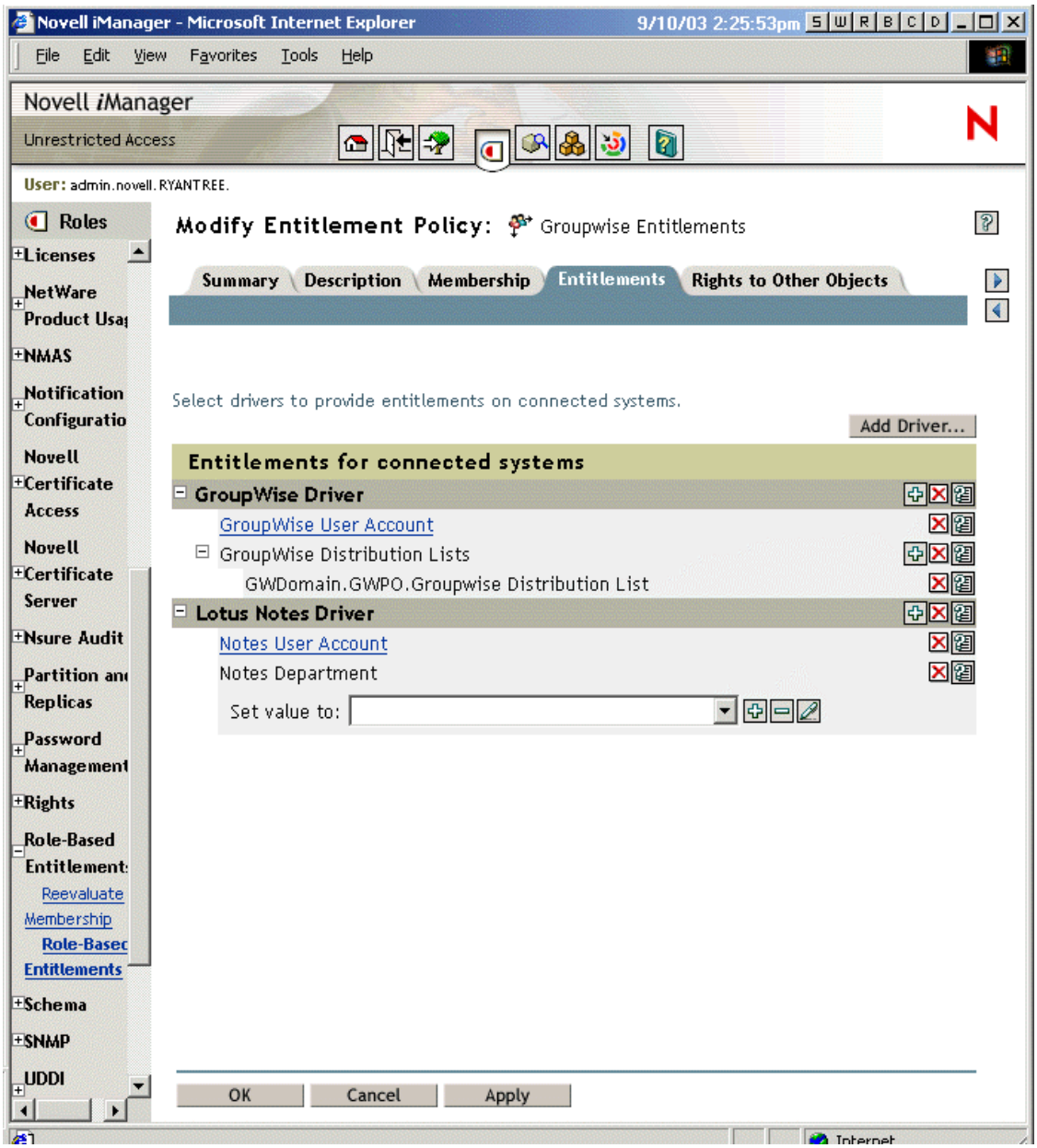
注 **:** 完全なリストを返すクエリではなく、指定したグループ名にリストを制限するようドライバをカスタマイズできます。

接続システムの属性値

接続システムのユーザアカウントには、属性値を割り当てられます。このインタフェースにより、ユーザアカウントに割り当てる値を入力できます。

次の図は、Notes の属性 Department に属性値を追加する例を示します。

図 *6-6* 属性値の追加



6.8 役割ベースエンタイトルメントポリシー間での衝突の解決

- 193 ページのセクション 6.8.1「衝突の概要」
- 194 ページのセクション 6.8.2「各エンタイトルメントの衝突の解決方法の変更」
- 197 ページのセクション 6.8.3「エンタイトルメントポリシーの優先度の設定」

6.8.1 衝突の概要

エンタイトルメントポリシーを作成する場合、特定のユーザに影響を与えるポリシーがそのユーザへのエンタイトルメントの割り当てと衝突する可能性があります。

このような衝突の解決方法を、次に説明します。一部のエンタイトルメントについては、衝突の解決を変更できます。

- 値のないエンタイトルメントが付加された場合。多くの場合、アカウントのエンタイトルメントには値がありません。ユーザがエンタイトルメントポリシーによって接続システムのアカウントを付与される場合、ユーザは接続システムのアカウントを受け取ります。別のエンタイトルメントポリシーが衝突するかどうかは関係なく、結果が付加されます。

  これは常に正しく、アカウント付与についての衝突の解決方法は変更できません。

  値のないエンタイトルメントは、照明のスイッチに例えることができます。「オン」または「オフ」、付与されたか付与されないかです。

  たとえば、「マネージャエンタイトルメントポリシー」によって Jean Chandler 氏に Exchange アカウントが付与されるにもかかわらず、Jean Chandler 氏が、同様に Exchange アカウントを付与する「メールルーム従業員エンタイトルメントポリシー」からは除外されている場合、Jean 氏は Exchange アカウントを取得できます。
- 値のあるエンタイトルメントがデフォルトで付加されるが、優先度に従って解決するよう選択できる場合 - グループメンバーシップなどのエンタイトルメントには、値、または値のある属性のグループ名のリストがあります。デフォルトでは、この種類のエンタイトルメントも付加できます。

  このようなエンタイトルメントの衝突の解決は、必要に応じて変更できます。

  各エンタイトルメントの衝突解決を抑制する設定は、エンタイトルメントで定義されます。ドライバが提供する各種類のエンタイトルメントは、マニフェストに別々に記述されます。値のあるエンタイトルメントは、conflict-resolution 属性を持ちます。conflict-resolution 属性は、エンタイトルメントごとに別々に設定されます。デフォルト設定は「conflict-resolution="priority"」です。「conflict-resolution="union"」も可能です。

  - **conflict-resolution="union" —**「union」という値は、エンタイトルメントが付加可能であることを意味します。ユーザには、ポリシーのメンバーシップにより割り当てられているすべてのエンタイトルメントが付与されます。異なるエンタイトルメント値は追加されるだけで、ユーザはそれらすべてを取得します。

    たとえば、Jameel 氏が、「トレードショーメーリングリスト」という GroupWise の電子メール配布リストのメンバーシップを付与する「トレードショーコントラクタポリシー」のメンバーであり、「トレードショーメーリングリスト」という電子メール配布リストも割り当てる「トレードショーマネージャポリシー」のメンバーシップから除外されている場合でも、電子メール配布リストのメンバーシップが引き続き付与されます。

    別の例を挙げると、「メールルームポリシー」により、「メールルームスタッフ」という Active Directory グループのメンバーシップが Consuela 氏に付与され、「緊急ボランティアによる緊急対応ポリシー」という Active Directory グループのメンバーシップも付与されている場合、Consuela 氏には両方の Active Directory グループのメンバーシップが付与されます。

    この設定では、ポリシーのリスト内のエンタイトルメントポリシーの順序は、エンタイトルメントについては重要ではありません。

- **conflict-resolution="priority" —**「priority」という値は、2 つの異なるポリシー間の値が衝突した場合、または 1 つのポリシーに含まれるユーザが別のポリシーでは除外されている場合、そのユーザに付与されるエンタイトルメントは、エンタイトルメントポリシーのリストでより上位に記述されているエンタイトルメントポリシーのエンタイトルメントのみになることを意味します。

  前の例は、この設定では別の結果となります。

  前の Jameel 氏の例では、GroupWise の電子メール配布リストのエンタイトルメントが「priority」という値を持ち、「トレードショーマネージャポリシー」が「トレードショーコントラクタポリシー」より上位にリスト表示される場合、「トレードショーメーリングリスト」のメンバーシップは、Jameel 氏に付与されません。

  前の Consuela 氏の例では、Active Directory NOS グループメンバーシップのエンタイトルメントが「priority」という値を持ち、「メールルームポリシー」が「緊急ボランティアポリシー」より上位にある場合、Consuela 氏にはメールルームスタッフグループのメンバーシップのみが付与されます。衝突の解決が付加ではなく優先度によって設定されているため、緊急対応グループのメンバーシップは付与されません。

  たとえば、役割ベースエンタイトルメントを使用して別のシステムでは階層構造にユーザを配置するよう環境を設定した場合などは、この機能が役立ちます。任意の 1ヶ所だけにユーザを配置し、同時に 2ヶ所に配置できないようにするとします。

  設定は、ドライバごとに提供される各エンタイトルメントには依存しない点に注意してください。

  原則として、「priority」の設定を使用する場合、管理者またはマネージャのポリシーは、エンドユーザまたは各貢献者のポリシーより上位に配置する必要があります。狭い範囲のメンバーシップを持つグループは、広い範囲のメンバーシップを持つグループよりも上位に配置する必要があります。

6.8.2 各エンタイトルメントの衝突の解決方法の変更

1 iManager で、［Identity Manager］>［Identity Manager の概要］の順にクリックし、ドライバセットを選択します。

ドライバセットに含まれるすべてのドライバのグラフィック画面のページが表示されます。

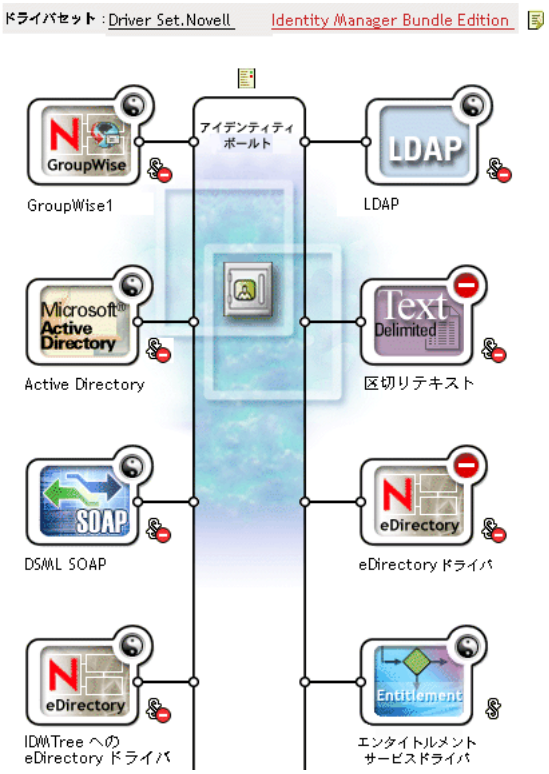
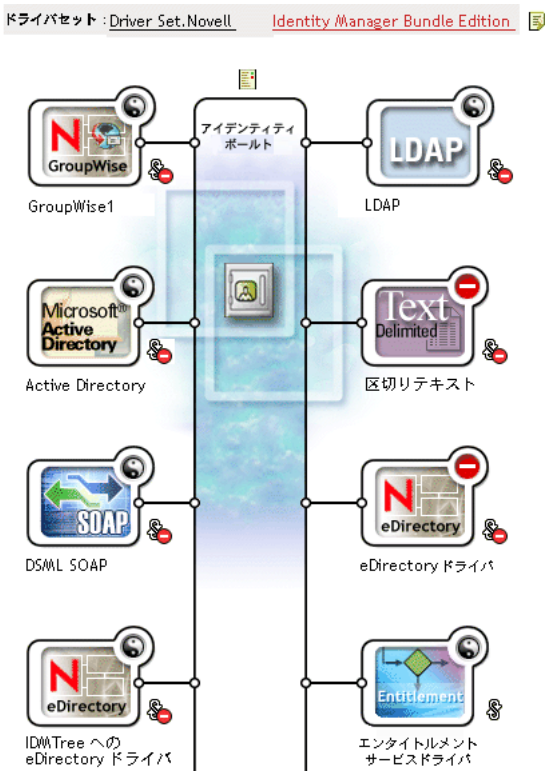


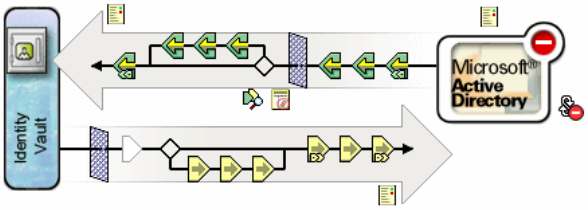
図 6-7 ドライバセット



2 [ドライバ] 状態ボタンをクリックし、[ドライバの停止] を選択します。

3 変更するエンタイトルメントを提供するドライバのドライバアイコンをクリックします。

ドライバのポリシーおよびドライバのアイコンを示すページが表示されます。画面の中央で、[すべてのエンタイトルメントを表示] アイコンを選択します (赤い丸で示しています)。



4 [エンタイトルメントの管理] ページでエンタイトルメント名をクリックし、XML ビューアにエンタイトルメントを表示します。

5 [XML 編集の有効化] チェックボックスをオンにします。

6 XML で、変更するエンタイトルメントの定義を検索します。

たとえば、次の行を検索します。

```
<entitlement conflict-resolution="union" description="Grants
membership to GroupWise Distribution lists" display-name="GroupWise
```

```
Distribution Lists" name="gwDistLists">
```

7 conflict-resolution の値を変更します。次の 2 つの値を指定できます。

```
conflict-resolution="union"
```

```
conflict-resolution="priority"
```

これらの値の詳細については、192 ページの 「役割ベースエンタイトルメントポリシー間での衝突の解決」を参照してください。

8 ［再起動］をクリックし、エンタイトルメントサービスドライバを再起動します。

6.8.3 エンタイトルメントポリシーの優先度の設定

デフォルトでは、エンタイトルメントポリシーのリスト内の順序に意味はありません。これは、Identity Manager に付属のドライバには、各エンタイトルメントの衝突の解決方法として「conflict-resolution="union"」が設定されているためです。

任意のエンタイトルメントを「conflict-resolution="priority,"」に変更した場合、エンタイトルメントポリシーのリスト内の順序は意味を持ちますが、対象となるのは変更したエンタイトルメントについてのみです。これらの値の詳細については、192 ページの 「役割ベースエンタイトルメントポリシー間での衝突の解決」を参照してください。

エンタイトルメントポリシーの順序を変更するには、エンタイトルメントポリシーのリストの横にある矢印ボタンを使用します。リスト内の最初のポリシーは、優先度が最も高いことを示します。

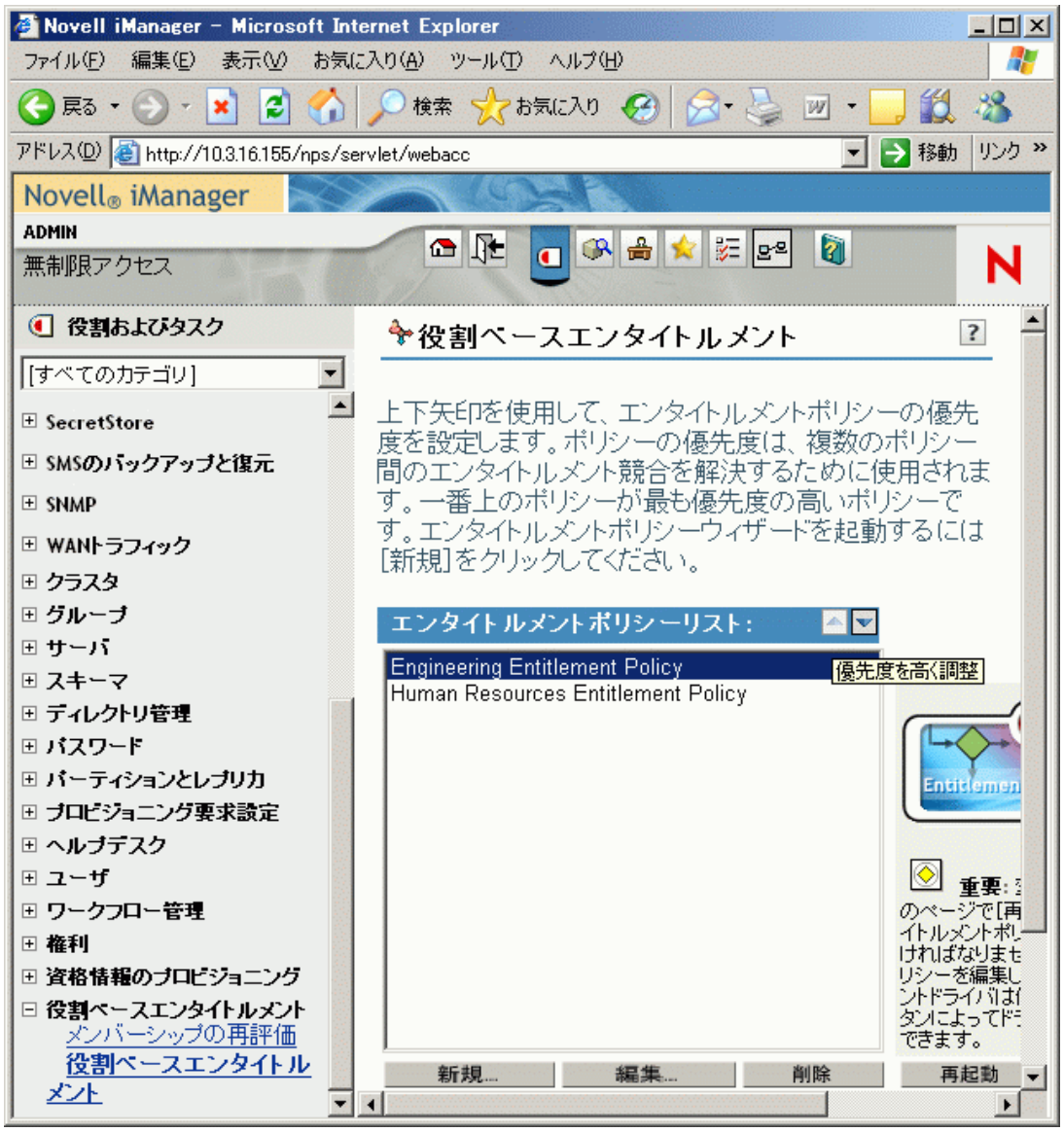
1 iManager で、［役割ベースエンタイトルメント］>［役割ベースエンタイトルメント］の順にクリックします。

2 ドライバセットを検索して選択します。

エンタイトルメントポリシーのリストを示すページが表示されます。

3 矢印ボタンを使用してポリシーをリスト内で上下に移動し、エンタイトルメントポリシーの優先度を変更します。

エンタイトルメントポリシーをリストの最上位に移動すると、最も高い優先度が与えられます。



4 [閉じる] をクリックしてドライバを再起動します。

優先度の変更は、ドライバを再起動するまでは有効になりません。

6.9 役割ベースエンタイトルメントのトラブルシューティング

トラブルシューティングに際しては、次のことに注意してください。

- ポリシーがリストされているページで [新規]、[編集]、または [削除] をクリックしてポリシーを変更すると、エンタイトルメントサービスドライバは停止します。同じページで [再起動] をクリックするまで、ドライバは再起動しません。

この機能は、ポリシーに対する変更が完了していない間は、ドライバが運用環境でエンタイトルメントを付与または取り消しするのを回避するためです。

- 同様に、エンタイトルメントサービスドライバは、同時に複数のユーザがエンタイトルメントポリシーを編集している可能性がある場合は、起動しません。
- 各ドライバセットで使用するエンタイトルメントサービスドライバは1つであるため、エンタイトルメントポリシーが管理できるのは、当該ドライバセットに関連付けられているサーバ上の読み書き可能レプリカまたはマスタレプリカに含まれるユーザだけです。

6.10 役割ベースエンタイトルメントおよびワークフローベースのプロビジョニングのエンタイトルメントに適用されるエンタイトルメント要素

以下の情報は、特定の実装だけでなく、すべてのエンタイトルメントに適用されます。

- 199 ページのセクション 6.10.1「エンタイトルメントの付与または取り消しの意味の制御」
- 200 ページのセクション 6.10.2「データの損失の回避」
- 200 ページのセクション 6.10.3「パスワード同期およびエンタイトルメント」

6.10.1 エンタイトルメントの付与または取り消しの意味の制御

エンタイトルメントの付与または取り消しの結果は、制御できます。各ドライバには、「付与」または「取り消し」の意味を制御するサポートオプションのリストが提供されています。

たとえば、GroupWise アカウントを追加する場合、付与によって実際には無効な状態のアカウントがユーザに付与されるという意味になるよう指定できます。これにより、ユーザがアカウントにアクセスするには、管理者による作業が必要になります。または、アカウントを有効にするように選択でき、これがデフォルトです。

デフォルトでは、ドライバ設定は、データを最も確実に確保できるオプションを使用します。たとえば、管理者がポリシーを変更する際に誤りがあった場合に、意図せずアカウントが失われることがないよう、GroupWise アカウントの削除のデフォルトの意味は「無効」に設定されています。別の例を挙げると、Identity Manager ドライバ設定は、別のシステムのユーザアカウントからの値のあるエンタイトルメントを取り消しません。ユーザに電子メール配布リストのメンバーシップが付与され、後にユーザがエンタイトルメントポリシーの条件に合致しなくなった場合、そのユーザは単にポリシーメンバーシップを取り消されます。アカウントは無効になりますが、グループメンバーシップおよび属性値は削除されません。別の結果が必要な場合は、Identity Manager のベテランユーザがドライバ設定をカスタマイズできます。

エンタイトルメントの取り消しの解釈は特に重要です。役割ベースエンタイトルメント機能を使用すると、研究室環境で結果をテストせずに、運用環境で組織のエンタイトルメントを一括して変更できるためです。

事前設定済みのドライバのグローバル設定の変数を編集すると、付与または取り消しの解釈の設定を変更できます。独自のカスタム設定を作成している場合、エンタイトルメントの付与および取り消しを解釈する GCV を追加できます。

6.10.2 データの損失の回避

役割ベースエンタイトルメントは、ポリシーのメンバーシップに基づき、アカウントなどのエンタイトルメントを一括して変更できるように設計されています。ただし、これは、ポリシーの変更時に誤りがあると問題になる可能性があることを意味します。Identity Manager に付属のドライバ設定では、影響の最も少ない設定が使用されています。GCV を使用して、意図しないデータの損失を回避する方法を理解する必要があります。

たとえば、削除は、アカウントのエンタイトルメントの取り消しを解釈する GCV の値として使用しないことをお勧めします。

新しいエンタイトルメントポリシーを作成または編集する際にデータを保護するもう 1 つの方法は、ポリシーの編集が終了しないうちは、ドライバをオフにして変更できないようにすることです。編集が完了したら、エンタイトルメントポリシーインタフェースの［再起動］ボタンを使用し、ドライバを手動で再起動します。同様に、別のユーザがエンタイトルメントポリシーを編集している可能性がある場合に、［再起動］ボタンを使用してエンタイトルメントサービスドライバを再起動しようとすると、他のユーザの変更作業が完了するまではドライバを再起動しないようにプロンプトが表示されます。

6.10.3 パスワード同期およびエンタイトルメント

73 ページの 「接続システム間のパスワード同期」で説明するとおり、パスワード同期は、役割ベースエンタイトルメントを使用するドライバに対しては、他のドライバと同じ方法で管理されます。

セキュリティ：ベストプラクティス 7

7.1 SSL の使用

SSL が使用できる場合は、すべての転送に対して有効する必要があります。SSL は、メタディレクトリエンジンとリモートローダ (45 ページのセクション 3.2「安全なデータ転送の提供」を参照) の間、メタディレクトリエンジンまたはリモートローダと接続システムの間で有効にする必要があります。

SSL を有効にしないと、パスワードなどの情報をクリアテキスト形式で送信することになります。

7.2 アクセスのセキュリティ保護

アイデンティティボールトおよび Identity Manager のオブジェクトに対するアクセスについては、セキュリティ保護を実行します。

物理的なセキュリティ - アイデンティティボールトがインストールされた物理的なサーバがある場所へのアクセスを保護します。

アクセス権 - Identity Manager オブジェクトの作成およびドライバの設定には、管理者権限が必要です。次を作成または変更する権限を持つユーザを監視および制御します。

- Identity Manager ドライバセット
- Identity Manager ドライバ
- ドライバ設定オブジェクト (フィルタ、スタイルシート、ポリシー)。特に、パスワードの取得または同期に使用するポリシー。
- パスワードポリシーオブジェクト (およびこれらを編集するための iManager タスク)。これらのオブジェクトは、相互に同期するパスワードと、使用するパスワードセルフサービスオプションを制御しているためです。

7.3 パスワードを管理する

接続システム間で情報を交換する場合は、交換のセキュリティを確保するために、予防措置をとる必要があります。特にパスワードにはセキュリティが必要です。

- パスワードヒント属性 (nsimHint) もパブリックに読み込み可能で、これによって、認証を受けていない、パスワードを忘れたユーザは自分のヒントにアクセスできます。

パスワードヒントを使用すると、ヘルプデスクへの問い合わせの手間を削減できます。

セキュリティのため、パスワードヒントは、ユーザの実際のパスワードが含まれていないかどうか確認されます。ただし、パスワードについて多くの情報を与えるパスワードヒントを作成することはできます。

パスワードヒントの使用時にセキュリティを強化するには、次の点に注意してください。

- パスワードセルフサービスに使用されている LDAP サーバ上の nsimHint 属性にのみアクセスを許可する。
- パスワードヒントを受け取る前にユーザが本人確認の質問に答えることを要求する。
- 自分だけが理解できるパスワードヒントを作成するようユーザに注意する。パスワードポリシーの［パスワード変更メッセージ］は、これを実行する 1 つの方法です。『Password Management Administration Guide (http://www.novell.com/documentation/password_management/index.html)』の「Adding a Password Change Message」を参照してください。

パスワードヒントをまったく使用しないよう選択した場合は、どのパスワードポリシーでもパスワードヒントを使用していないことを確認します。パスワードヒントの設定をしないようにするには、先に進んでから、『Password Management Administration Guide (http://www.novell.com/documentation/password_management/index.html)』の「Disabling Password Hint by Removing the Hint Gadget」の説明に従い、パスワードヒントガジェットを完全に削除します。

- 本人確認の質問はパブリックに読み込み可能です。これは、パスワードを忘れた認証されていないユーザが別の方法で認証を受けることができるようにするためです。本人確認の質問を要求することで、パスワードを忘れた場合のセルフサービスのセキュリティが向上します。これは、忘れたパスワードまたはパスワードヒントを受け取る前、またはパスワードをリセットする前に、正しく回答することによってユーザが自らの識別情報を証明する必要があるためです。

  本人確認の質問には不正侵入者ロックアウト設定が適用されるため、不正侵入者による不正な試行回数は制限されています。

  ただし、ユーザはパスワードの手がかりを含む本人確認の質問を作成できます。本人だけが理解できる本人確認の質問と回答を作成するように徹底してください。パスワードポリシーの［パスワード変更メッセージ］は、これを実行する 1 つの方法です。『Password Management Administration Guide (http://www.novell.com/documentation/password_management/index.html)』の「Adding a Password Change Message」を参照してください。

- セキュリティのため、［パスワードを忘れた場合］のアクション［E-mail password to user (ユーザにパスワードを電子メールで送信する)］および［Allow user to reset password (ユーザがパスワードをリセットできるようにする)］は、本人確認の質問に答えるようにユーザに要求している場合にのみ実行できます。
- NMAS™ 2.3.4 では、管理者によって変更されたユニバーサルパスワードに関するセキュリティが強化されました。これは基本的に、以前に NDS® パスワードで提供されていた機能と同じように動作します。

  新しいユーザを作成する場合やヘルプデスクへの問い合わせに応答する場合などに、管理者がユーザのパスワードを変更する場合、パスワードポリシーでパスワードを期限切れにする設定が有効になっていると、パスワードは自動的に期限切れになりま

す。パスワードポリシーのこの設定は、高度なパスワードルールに［パスワードが期限切れになるまでの日数 (0-365)］という名前で存在します。この特定の機能については、日数は重要ではありませんが、設定を有効にする必要があります。

7.4 強力なパスワードポリシーの作成

パスワードポリシーオブジェクトは、パスワードが準拠しているかどうかをアプリケーションで確認できるようにするため、パブリックに読み込み可能です。つまり、認証されていないユーザでも、アイデンティティボールトに問い合わせて、どのパスワードポリシーが設定されているかを確認できます。パスワードポリシーが強力なパスワードの作成を要求する場合、『Password Management Administration Guide (http://www.novell.com/documentation/password_management/index.html)』の「Create Strong Password Policies」に説明されているように、これによりリスクが発生することはありません。

Identity Manager パスワード同期は、ユーザパスワードを簡略化し、ヘルプデスクのコストを削減できるように提供されています。双方向パスワード同期は、109 ページのセクション 5.8「パスワード同期の実装」で説明されているように、eDirectory と接続システム間との間でパスワードを複数の方法で共有できるように提供されています。

ユニバーサルパスワードとパスワードポリシーを使用することで、ユーザに対して強いパスワード要件を適用できます。パスワードポリシーの［高度なパスワードルール］を使用して、パスワードに関する業界のベストプラクティスに従ってください。

たとえば、ユーザパスワードが次のようなルールに準拠するように要求できます。

- 固有のパスワードの要求 -

  ユーザがパスワードを再利用できないようにし、システムが比較のために履歴リストに保存するパスワードの数を制限できます。
- パスワードに使用する文字の最小数の要求 -

  長いパスワードの要求は、パスワードを強化する最適な方法の 1 つです。
- パスワードに使用する数字の最小数の要求 -

  パスワードに 1 つ以上の数値を含めるよう要求することは、不正侵入者が辞書の単語を使用してログインしようとする「辞書攻撃」の防止に役立ちます。
- 特定のパスワードの除外 -

  会社名や地名、または test や admin という単語など、セキュリティリスクになると思われる単語を除外できます。除外リストは辞書全体をインポートするためのものではありませんが、除外単語リストは長くてもかまいません。ただし、長い除外リストを使用すると、ユーザのログインに時間がかかります。「辞書攻撃」を防ぐ方法としては、数字または特殊文字を要求する方が適切です。

ツリーの場所によってパスワード要件が異なる場合は、複数のパスワードポリシーを作成できます。パスワードポリシーは、ツリー全体、パーティションルートコンテナ、コンテナ、または個々のユーザに割り当てることができます (管理を簡略化するために、パスワードポリシーは、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)。

さらに、不正侵入者ロックアウトも選択できます。通常どおり、eDirectory のこの機能では、ログインに何回失敗したらアカウントをロックするかを指定できます。これは、パスワードポリシーの設定ではなく、親コンテナの設定です。『*Novell eDirectory 8.7.3*

Administration Guide (http://www.novell.com/documentation/edir873/edir873/data/afxkmdi.html#amm7bjv)』の「Managing User Accounts」を参照してください。

7.5 接続システムのセキュリティ保護

データを同期する先の接続システムは、そのデータを危険な方法で保存または転送することがあります。

パスワードを交換するシステムは、セキュリティで保護してください。たとえば、LDAP、NIS、および Winsows には、それぞれセキュリティの問題があり、これらのシステムとのパスワード同期を有効にする前に、これらの問題を考慮する必要があります。

多くのソフトウェアベンダは、製品について従う必要のある具体的なセキュリティガイドラインを提供しています。

7.6 Identity Manager の Designer

Identity Manager の Designer を使用する場合は、次の問題を考慮します。

- Identity Manager ドライバを作成または変更する権限を持つユーザを監視および制御します。

  Identity Manager オブジェクトの作成およびドライバの設定には、管理者権限が必要です。
- アイデンティティボールトの管理者パスワードをコンサルタントに付与する前に、管理者に割り当てられる権利を、コンサルタントがアクセスするツリーのエリア内に制限します。
- プロジェクトファイル (.proj) を削除するか、会社のディレクトリに保存します。

  Designer .proj ファイルは、会社のプロジェクトサイトに存続します。コンサルタントは、プロジェクトの完了後にファイルを取得することはできません。
- プロジェクトファイル、ログファイル、およびトレースファイルが必要なくなったら、それらを削除します。
- ラップトップの廃棄または売却を行う前に、プロジェクトファイルが削除されていることを確認します。
- Designer からアイデンティティボールトへの接続は、物理的にセキュアな状態を保ちます。

  そうでない場合、何者かがネットワークを監視し、機密情報を引き出す可能性があります。
- ドキュメントジェネレータを使用してドキュメントを作成する場合、ドキュメントの取り扱いには注意します。

  これらのドキュメントには、パスワードおよび機密データがクリアテキストで含まれている場合があります。
- Designer が eDirectory 属性の読み書きを実行する必要がある場合、属性を暗号化属性としてマークしないでください。

  Designer は、暗号化属性の読み書きができません。
- 機密に属するパスワードを保存しないでください。

現在、Designer プロジェクトは暗号化されていません。パスワードのみがエンコードされています。このため、保存されたパスワードを持つ Designer プロジェクトを共有しないでください。

セッションのパスワードを保存するが、プロジェクトにパスワードを保存しない

a. ［Outline (アウトライン)］の展開ビューで、アイデンティティボールトを右クリックします。

b. ［プロパティ］を選択します。

c. ［環境設定］ページでパスワードを入力し、［OK］をクリックします。

パスワードは、1 セッションにつき 1 つ入力できます。プロジェクトを閉じると、パスワードは消失します。

パスワードをハードドライブに保存するには、手順 1 ～ 3 を実行し、［Save Password (パスワードの保存)］を選択してから［OK］をクリックします。

図 7-1 パスワードの保存

7.7 セキュリティの業界ベストプラクティス

サーバ上の未使用ポートをブロックするなど、セキュリティ対策に関する業界ベストプラクティスに従います。

7.8 機密情報に対する変更のトラッキング

- 205 ページのセクション 7.8.1「iManager を使用したイベントのログ」
- 206 ページのセクション 7.8.2「Designer を使用したイベントのログ」

7.8.1 iManager を使用したイベントのログ

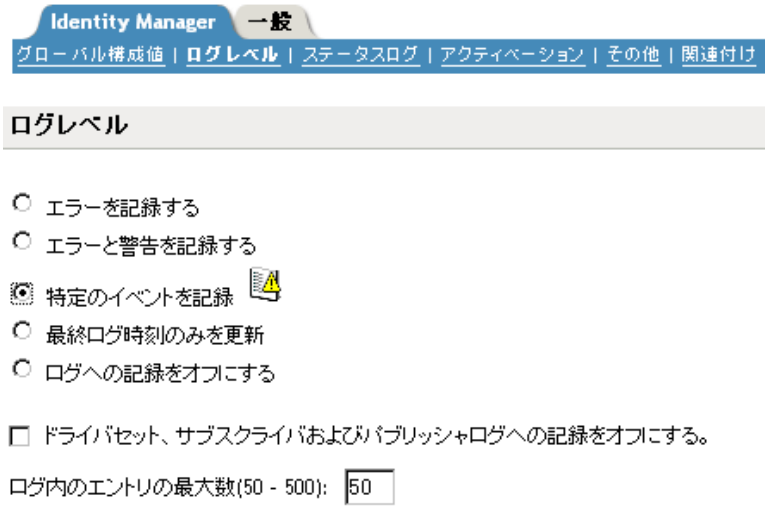
Novell Audit を使用すると、セキュリティにとって重要と思われるイベントのログを記録できます。Novell Audit の詳細については、233 ページの第 10 章「Novell Audit によるログとレポート」を参照してください。

たとえば、特定のアイデンティティボールトのドライバ (またはドライバセット) のパスワードの変更のログを記録するには、次の手順を実行します。

1 ［eDirectory 管理］>［オブジェクトの変更］>［ログレベル］の順に選択します。

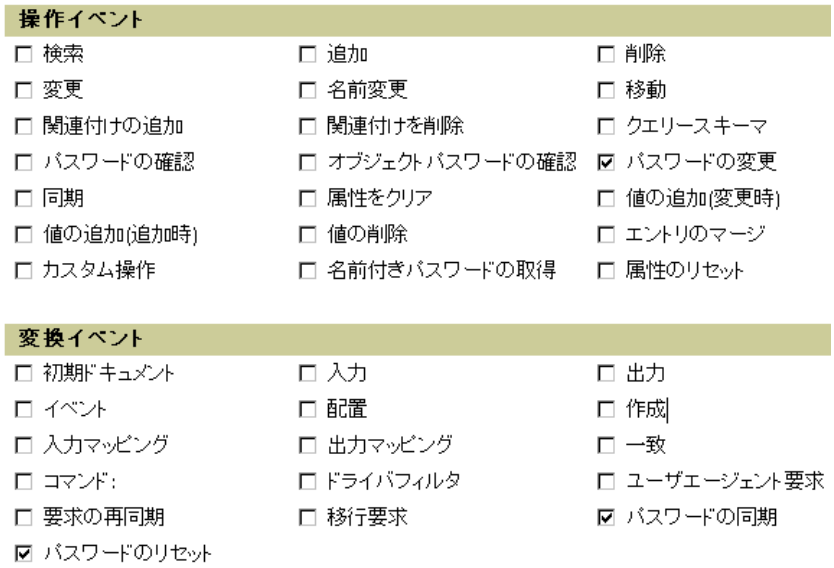
iManage のバージョンにより、ドロップダウンリストまたはタブから選択します。

2 ［特定のイベントを記録］を選択します。



3 具体的なイベントを選択するには、ログイベントアイコン をクリックします。

4 ［イベント］ページで、次を選択します。



- ［操作イベント］で、［パスワードの変更］チェックボックスをオンにします。

  この項目は、NDS のパスワードの直接の変更を監視します。
- ［変換イベント］で、［Password Set (パスワード設定)］および［パスワード同期］の両方のチェックボックスをオンにします。これら 2 つの項目は、ユニバーサルパスワードおよび配布パスワードのイベントを監視します。

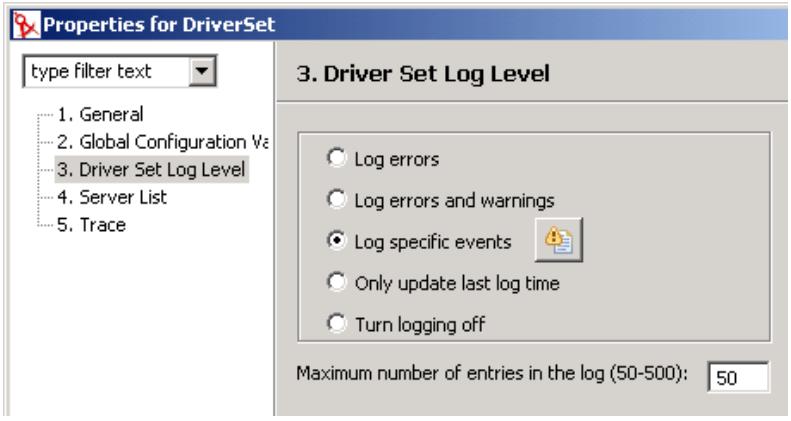
5 ［OK］を 2 回クリックします。

7.8.2 Designer を使用したイベントのログ

ドライバセットまたはドライバに適用されるイベントは、ログを記録できます。

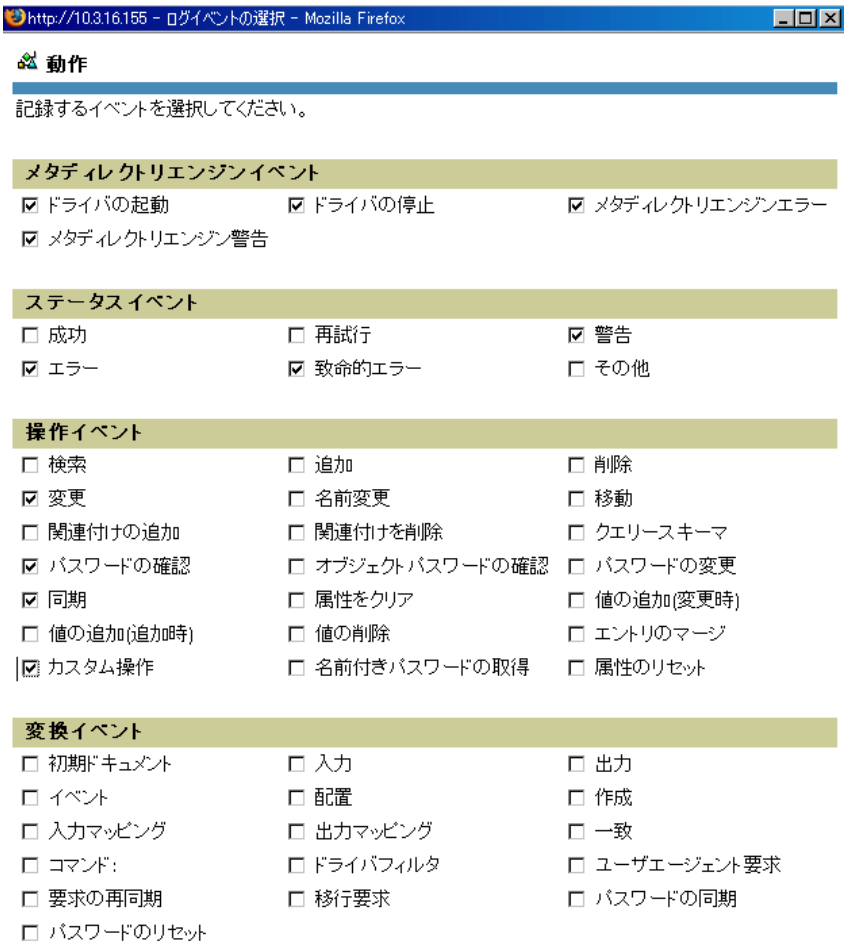
ドライバセットのイベントのログ

1 Designer で、ドライバセットを右クリックしてから［プロパティ］を選択します。



2 ［Driver Set Log Level (ドライバセットのログレベル)］、［特定のイベントを記録］の順に選択します。

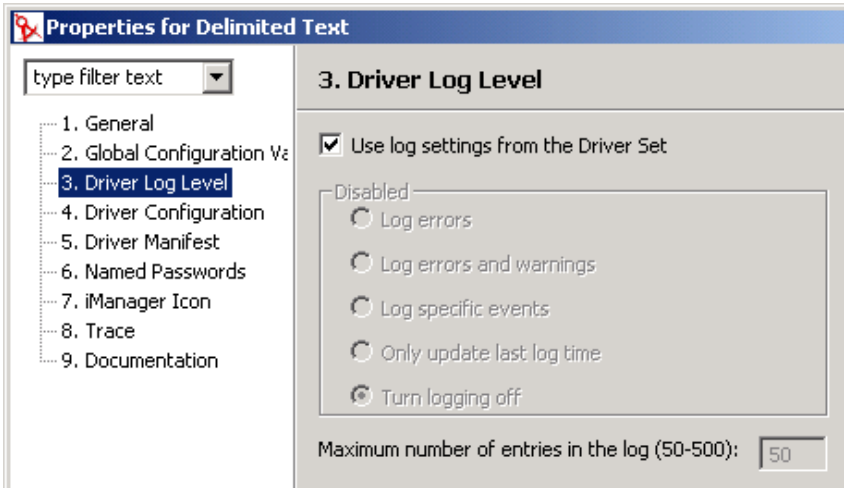
3 ［記録するイベントの選択］アイコンをクリックします。



4 ログを記録するイベントを選択してから、［OK］をクリックします。

ドライバのイベントのログ

1 Designer で、ドライバを右クリックしてから［プロパティ］を選択します。



2 ［Driver Log Level (ドライバのログレベル)］、［特定のイベントを記録］の順に選択します。

ドライバセットの設定をそのまま使用する場合は、［OK］をクリックします。そうでない場合は、［Use log settings from the Driver Set (ドライバセットの設定を使用)］チェックボックスをオフにしてから［特定のイベントを記録］を選択し、［OK］をクリックします。

3 ［記録するイベントの選択］アイコンをクリックします。

4 ログを記録するイベントを選択してから、［OK］をクリックします。

エンジンサービスの管理

8

次のドライバは、外部接続システムではなく、メタディレクトリエンジンサービスに対してのみ使用されます。これらは、Identity Manager をインストールするときに自動的にインストールされます。

8.1 エンタイトルメントサービスドライバ

161 ページの第 6 章「エンタイトルメントの作成と使用」を参照してください。

8.2 手動タスクサービスドライバ

手動タスクサービスドライバは、データイベントが発生したこと、およびユーザ側でアクションが必要かどうかを 1 人または複数のユーザに通知するために開発されました。従業員のプロビジョニングシナリオでは、データイベントが新しいユーザオブジェクトの作成で、ユーザアクションには、eDirectory またはアプリケーションにデータを入力してオフィス番号を割り当てる作業が含まれます。他のシナリオとしては、新しいユーザオブジェクトが作成されたことの管理者への通知、ユーザがオブジェクト上のデータを変更したことの管理者への通知などがあります。

通常、手動タスクサービスドライバの設定には、独立してはいるものの関連性のある 2 つのサブシステムの設定が含まれます。つまり、購読者チャネルのポリシーと電子メールテンプレート、および発行者チャネルの Web サーバテンプレートとポリシーです。

SMTP サーバ名、Web サーバポート番号などのドライバパラメータも設定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。

8.2.1 インストール

- インストール：Identity Manager インストールプログラムを使用して［メタディレクトリサーバ］オプションをインストールするときに、手動タスクサービスのドライバが自動的にインストールされます。
- プラットフォーム：ドライバは、Identity Manager およびリモートローダによってサポートされているプラットフォームで実行されます。
- アクティベーション：ドライバは、別のアクティベーションを必要としません。メタディレクトリエンジンをアクティブにすると、このドライバもアクティブになります。

8.2.2 概要

この節では、さまざまなドライバ機能に関する情報について説明します。

操作モード

次の 2 つの主な操作モードがサポートされています。

- データの直接要求 **:** ユーザが eDirectory にデータを入力することを要求する電子メールメッセージが送信されます (他のアプリケーションによって使用される可能性があります)。メッセージ内の URL をクリックすることにより、電子メールの受信者がメッセージに応答します。URL は、手動タスクサービスドライバの発行者チャネルで実行されている Web サーバを指しています。ユーザは、Web サーバによって生成された動的な Web ページと情報をやりとりし、eDirectory™ を認証して要求されたデータを入力します。
- イベント通知 **:** 発行者チャネルを使用せずに、電子メールメッセージがユーザに送信されます。電子メールメッセージは、単に eDirectory で何かが発生したことを通知したり、または Novell iManager、その他のアプリケーション、またはカスタムインタフェースなどの発行者チャネルの Web サーバ以外の方法を介してデータを要求したりするだけの場合があります。

例 : 購読者チャネルの電子メール、発行者チャネルの Web サーバレスポンス

新しい従業員のマネージャが従業員に部屋番号を割り当てるという、従業員のプロビジョニング例のシナリオを次に示します。

1. eDirectory で新しいユーザオブジェクトが作成されます (会社の人事システム用の DirXML ドライバなど)。
2. 手動タスクサービスドライバの購読者により、ユーザのマネージャおよびマネージャのアシスタントに SMTP メッセージが送信されます。SMTP メッセージには、発行者チャネルの Web サーバを参照する URL が含まれています。URL には、ユーザを識別し、要求されたデータを送信することを承認されたユーザを識別するデータ項目も含まれています。
3. Web ブラウザの HTML 形式を表示するには、マネージャまたはマネージャのアシスタントは電子メールメッセージ内の URL をクリックします。その後、マネージャまたはアシスタントは次の操作を実行します。
    - 誰が電子メールメッセージに応答するのかを識別する方法として、eDirectory ユーザオブジェクトの DN を選択します。

- eDirectory パスワードを入力します。
- 新しい従業員の部屋番号を入力します。
- ［送信］ボタンをクリックします。

4. 手動タスクサービスドライバの発行者チャネルを経由して、新しい従業員の部屋番号が eDirectory に送信されます。

例 : 購読者チャネルの電子メール、発行者チャネルのレスポンスがない場合

次に、資産管理システムで、新しい従業員のマネージャが従業員にコンピュータを割り当てるというシナリオの例を示します。

1. eDirectory で新しいユーザオブジェクトが作成されます (会社の人事システム用の DirXML ドライバなど)。
2. 手動タスクサービスドライバの購読者により、ユーザのマネージャおよびマネージャのアシスタントに SMTP メッセージが送信されます。SMTP メッセージには、資産管理システムへのデータの入力に関する説明が含まれています。
3. マネージャまたはアシスタントが、資産管理システムにデータを入力します。
4. (オプション) 資産管理システムの DirXML ドライバを経由して、コンピュータの識別データが eDirectory に送信されます。

手動タスクサービスドライバによって、電子メールメッセージおよび Web ページがどのように作成されるのか

電子メールメッセージ、HTML Web ページ、および XDS ドキュメントは、すべてドキュメントと見なすことができます。手動タスクサービスドライバによって、ドライバに提供された情報に基づいてドキュメントが動的に作成されます。

テンプレートは、動的な部分または置換部分の、構成された最終のドキュメントが表示される場所を示す置換トークンとともに、ボイラープレートまたはドキュメントの固定部分が含まれている XML ドキュメントです。

手動タスクサービスドライバの購読者チャネルおよび発行者チャネルの両方で、ドキュメントを作成するためのテンプレートが使用されます。購読者チャネルにより電子メールメッセージが作成され、発行者チャネルにより Web ページおよび XDS ドキュメントが作成されます。

ドキュメントの動的な部分は置換データを経由して提供されます。購読者チャネルの置換データは、(コマンド変換ポリシーなどの) 購読者チャネルポリシーによって提供されます。発行者チャネルの置換データは、HTTP データによって Web サーバに提供されます (URL データと HTTP POST データの両方)。手動タスクサービスドライバは、(Web サーバのアドレスなどの) 手動タスクサービスドライバにとって既知の特定のデータを自動的に提供します。

XSLT スタイルシートにより、テンプレートが処理されます。これらのテンプレート処理のスタイルシートは、購読者チャネルまたは発行者チャネルで DirXML ポリシーとして使用されるスタイルシートとは分離しています。

置換データはパラメータとして XSLT スタイルシートに提供されます。スタイルシート処理の出力は、電子メールメッセージの本文、Web ページ、または発行者チャネル上の DirXML への送信として使用されている、XML、HTML、またはテキストドキュメントです。

置換データは、電子メールメッセージの URL を経由して購読者チャネルから発行者チャネルに渡されます。URL には、置換データ項目が含まれているクエリ部分が含まれています。

手動タスクサービスドライバには、電子メールドキュメント、HTML ドキュメント、および XDS ドキュメントを作成するためにテンプレートを処理するのに十分な、事前定義されたスタイルシートが付属しています。他のカスタムのスタイルシートは、必要に応じて、追加の処理オプションを提供するために記述することができます。

ドキュメントを作成する高度な方法も使用できます。その場合、XSLT スタイルシートおよび置換データのみを使用します。テンプレートは使用しません。しかし、このガイドではテンプレートによる方法を使用することを想定しています。これは、XSLT のプログラミング知識なしで設定および管理するには、テンプレートによる方法がより簡単であるためです。

テンプレート

この節では、手動タスクサービスドライバで使用されるドキュメント作成テンプレートについて説明します。

テンプレートは、出力ドキュメントを生成するために、スタイルシートによって処理される XML ドキュメントです。出力ドキュメントは、XML、HTML、またはプレーンテキストです (または、XSLT を使用して生成されるその他のドキュメントです)。

購読者チャネル上の電子メールメッセージテキストを生成したり、発行者チャネル上の動的な Web ページおよび XDS ドキュメントを生成するために、テンプレートが使用されます。

テンプレートには、テキスト、要素、および置換トークンが含まれています。置換トークンは、テンプレートを処理するスタイルシートに提供されたデータによって出力ドキュメントで置換されます。

さまざまな目的のテンプレートの例をいくつか以下に示します。例では、置換トークンは 2 つの $ 記号の間にある文字列であり、太字で示しています。

テンプレートには、アクション要素を含めることもできます。アクション要素は、テンプレート処理のスタイルシートによって解釈された制御要素です。アクション要素については、307 ページの付録 F「手動タスクサービスドライバ : テンプレートのアクション要素について」で説明しています。次の例では、アクション要素も太字で示しています。

次のテンプレートの例は、HTML の電子メールメッセージ本文を生成するために使用されます。

```
<html xmlns:form="http://www.novell.com/dirxml/manualtask/form">
<head></head> <body> Dear $manager$,<p/> <p> This message is to inform
you that your new employee <b>$given-name$ $surname$</b> has been
hired. <p> You need to assign a room number for this individual.Click
<a href="$url$">Here</a> to do this. </p> <p> Thank you,<br/> HR
Department </p> </body> </html>
```

次のテンプレートの例は、プレーンテキストの電子メールメッセージ本文を生成するために使用されます。

```
<form:text xmlns:form="http://www.novell.com/dirxml/manualtask/form">
```

```
Dear $manager$,

This message is to inform you that your new employee $given-name$
$surname$ has been hired.

You need to assign a room number for this individual.Use the following
link to do this:

$url$

Thank you,

The HR Department

</form:text>
```

テンプレートは XML ドキュメントである必要があるため、<form:text> 要素は必須です。<form:text> 要素はテンプレート処理の一部としてストリップされます。

データの入力用に Web ページとして使用される HTML 形式を生成するには、次のテンプレートが使用されます。

```
<html  xmlns:form="http://www.novell.com/dirxml/manualtask/form">
<head> <title>Enter room number for $subject-name$</title> </head>
<body> <link href="novdocmain.css" rel="style sheet" type="text/css"/>
<br/><br/><br/><br/> <form class="myform" METHOD="POST" ACTION="$url-
base$/process_template.xsl"> <table cellpadding="5" cellspacing="10"
border="1" align="center"> <tr><td> <input TYPE="hidden"
name="template" value="post_form.xml"/> <input TYPE="hidden"
name="subject-name" value="$subject-name$"/> <input TYPE="hidden"
name="association" value="$association$"/> <input TYPE="hidden"
name="response-style sheet" value="process_template.xsl"/> <input
TYPE="hidden" name="response-template" value="post_response.xml"/>
<input TYPE="hidden" name="auth-style sheet"
value="process_template.xsl"/> <input TYPE="hidden" name="auth-
template" value="auth_response.xml"/> <input TYPE="hidden"
name="protected-data" value="$protected-data$"/> You are:<br/>
<form:if-single-item name="responder-dn">           <input
TYPE="hidden" name="responder-dn" value="$responder-dn$"/> $responder-
dn$           </form:if-single-item>          <form:if-multiple-items
name="responder-dn">          <form:menu name="responder-dn"/>
</form:if-multiple-items> </td></tr> <tr><td> Enter your password:<br/
> <input name="password" TYPE="password" SIZE="20" MAXLENGTH="40"/> </
td></tr> <tr><td> Enter room number for $subject-name$:<br/> <input
TYPE="text" NAME="room-number" SIZE="20" MAXLENGTH="20"
value="$query:roomNumber$"/> </td></tr> <tr><td> <input TYPE="submit"
value="Submit"/> <input TYPE="reset" value="Clear"/> </td></tr> </
table> </form> </body> </html>
```

XDS ドキュメントを生成するには、次のテンプレートを使用します。

```
<nds> <input> <modify class-name="User" src-dn="not-applicable">
```

```
<association>$association$</association> <modify-attr attr-
name="roomNumber"> <remove-all-values/> <add-value> <value>$room-
number$</value> </add-value> </modify-attr> </modify> </input> </nds>
```

置換トークン

上記のテンプレートの例では、$ で区切られた項目が置換トークンです。たとえば、$manager$ は、マネージャの実際の名前に置換されます。

置換トークンは、テキストまたは XML 属性値のいずれかで表示できます (上記の最初の例の <a> 要素の href 値に注目してください)。

置換データ

置換データは、テンプレートから生成された出力ドキュメントの置換トークンの場所を占める文字列で構成されます。置換データは、購読者チャネルのデータ、発行者チャネルの HTTP データによって提供されるか、またはドライバによって自動的に提供されます。置換データの追加のタイプとしては、Identity Manager を経由して eDirectory から取得されたデータがあります (クエリデータ)。置換データについては、299 ページの付録 D「手動タスクサービスドライバ : 置換データ」でより詳しく説明しています。

購読者チャネルのデータ **:** 購読者チャネルの置換データには、次の 2 つのタイプがあります。最初のタイプは、電子メールメッセージを作成するための、テンプレートでの置換トークンの置換の値として使用されます。2 番目のタイプは、URL が発行者の Web サーバに送信されたときにデータが発行者チャネルで使用可能になるように、URL のクエリ部分にあります。

HTTP データ **:** URL クエリ文字列データ、HTTP POST データ、またはその両方として、発行者チャネルの Web サーバに置換データが提供されます。

自動データ **:** 手動タスクサービスドライバによって、自動データが提供されます。自動データ項目については、305 ページの付録 E「手動タスクサービスドライバ : 自動置換データ項目」で詳しく説明しています。

クエリデータ **:** query: で始まる置換トークンは、eDirectory から現在のデータを取得することを要求していると見なされます。query: の後ろのトークンの部分は、eDirectory オブジェクトの属性の名前です。問い合わせるオブジェクトは、置換データ項目のひとつである association、src-dn、または src-entry-id によって指定されます。項目は、前のセンテンスで表示されている順に考慮されます。

テンプレートのアクション要素

アクション要素は、シンプルなロジック制御、または HTML 形式の HTML 要素を作成するために使用されるテンプレートの namespace-qualified 要素です。要素を修飾するために使用されている名前スペースは、http://www.novell.com/dirxml/manualtask/form にあります。このドキュメントおよび手動タスクサービスドライバで提供されているサンプル テンプレートでは、使用されているプレフィクスがフォームにあります。

上記の例で太字で表示されている要素がアクション要素です。

アクション要素については、307 ページの付録 F「手動タスクサービスドライバ : テンプレートのアクション要素について」で詳しく説明しています。

購読者チャネルの電子メール

手動タスクサービスドライバの購読者チャネルは、電子メールメッセージを送信するように設計されています。これを実行するために、ドライバでは <mail> という名前のカスタム XML 要素がサポートされています。(ユーザの作成などの) いくつかの eDirectory イベントが発生すると、購読者チャネルのポリシーによって <mail> 要素が構成されます。<mail> 要素の例を以下に示します。

```
<mail src-dn="\PERIN-TAO\novell\Provo\Joe"> <to>JStanley@novell.com</
to> <cc>carol@novell.com</cc> <reply-to>HR@novell.com</reply-to>
<subject>Room Assignment Needed for:Joe the Intern</subject> <message
mime-type="text/html"> <stylesheet>process_template.xsl</stylesheet>
<template>html_msg_template.xml</template> <replacement-data> <item
name="manager">JStanley</item> <item name="given-name">Joe</item>
<item name="surname">The Intern</item> <url-data> <item
name="file">process_template.xsl</item> <url-query> <item
name="template">form_template.xml</item> <item name="responder-dn"
protect="yes">\PERIN-TAO\big-org\phb</item> <item name="responder-dn"
protect="yes">\PERIN-TAO\big-org\carol</item> <item name="subject-
name">Joe The Intern</item> </url-query> </url-data> </replacement-
data> <resource cid="css-1">novdocmain.css</resource> </message>
<message mime-type="text/plain">
<stylesheet>process_text_template.xsl</stylesheet>
<template>txt_msg_template.xml</template> <replacement-data> <item
name="manager">JStanley</item> <item name="given-name">Joe</item>
<item name="surname">The Intern</item> <url-data> <item
name="file">process_template.xsl</item> <url-query> <item
name="template">form_template.xml</item> <item name="responder-dn"
protect="yes">\PERIN-TAO\big-org\phb</item> <item name="responder-dn"
protect="yes">\PERIN-TAO\big-org\carol</item> <item name="subject-
name">Joe The Intern</item> </url-query> </url-data> </replacement-
data> </message> <attachment>HR.gif</attachment> </mail>
```

手動タスクサービスドライバの購読者は、<mail> 要素に含まれている情報を使用して、SMTP 電子メールメッセージを構成します。URL を構成して電子メールメッセージに挿入できます。それを使用して、電子メールの受信者はその電子メールメッセージに応答できます。URL は、発行者チャネルの Web サーバを指したり、またはいくつかの他の Web サーバを指すこともできます。

<mail> 要素およびそのコンテンツについては、311 ページの付録 G「手動タスクサービスドライバ :<mail> 要素について」 で詳しく説明しています。

発行者チャネルの Web サーバ

手動タスクサービスドライバの発行者チャネルでは、ユーザが Web ブラウザを介して eDirectory にデータを入力できるように設定されている Web サーバが実行されています Web サーバは、手動タスクサービスドライバの購読者チャネルから送信された電子メールメッセージと組み合わせて機能するように設計されています。

発行者チャネルの Web サーバは、スタティックファイルおよびダイナミックコンテンツの役割を果たします。スタティックファイルの例としては、.css スタイルシート、イメージなどがあります。ダイナミックコンテンツの例としては、URL または HTTP POST データに含まれている置換データに基づいて変更される Web ページがあります。

発行者チャネルの Web サーバは、通常、購読者チャネルによって送信された電子メールに対して、ユーザが eDirectory にデータを入力できるように設定されます。一般的なユーザの Web サーバとの情報のやりとりは、次のとおりです。

1. ユーザが Web ブラウザを使用して、電子メールメッセージから Web サーバに URL を送信します。URL では、動的な Web ページを作成するために使用されたスタイルシート、テンプレート、および置換データが指定されています (通常 HTML 形式が含まれています)。
2. スタイルシートおよび置換データを使用してテンプレートを処理することによって、Web サーバによって HTML ページが作成されます。URL によって参照されるリソースとして、HTML ページがユーザの Web ブラウザに返されます。
3. ブラウザに HTML ページが表示され、要求された情報をユーザが入力します。
4. ブラウザによって、入力された情報が含まれている HTTP POST 要求、および電子メールの URL からのその他の情報が送信されます。電子メールに応答しているユーザの DN およびユーザのパスワードは、POST データにある必要があります。
5. ユーザの DN およびパスワードを使用して、Web サーバによってユーザが認証されます。認証が失敗した場合、POST 要求の結果として、失敗のメッセージが含まれている Web ページが返されます。POST データで指定したスタイルシートおよびテンプレートを使用して、失敗のメッセージを構成できます。認証が成功した場合、処理が続行されます。
6. POST データで指定されたスタイルシートおよびテンプレートを使用して、Web サーバによって XDS ドキュメントが構成されます。XDS ドキュメントが、発行者チャネル上の Identity Manager に送信されます。
7. XDS ドキュメントの送信の結果は、POST データで指定されたスタイルシートおよびテンプレートとともに、データ送信の結果をユーザに示す Web ページを構成するために使用されています。POST 要求の結果として、この Web ページがブラウザに送信されます。

8.2.3 設定

この節では、手動タスクサービスドライバのパラメータおよびテンプレートの設定について説明します。

ドライバ設定

この節では、ドライバオブジェクトのユーザインタフェースの［ドライバ設定］セクションに表示されているパラメータについて説明します。

これらのパラメータの多くは、実際の発行者チャネルの Web サーバ用です。手動タスクサービスドライバの購読者もこれらにアクセスする必要があるため、これらは［ドライバ設定］エリアに表示されます。

ドキュメントベースの DN

このパラメータは、コンテナオブジェクトの eDirectory DN です。手動タスクサービスドライバは、eDirectory またはディスクから (XSLT スタイルシートを含む)XML ドキュメントをロードできます。XML ドキュメントを eDirectory からロードする必要がある場合、ドキュメントがロードされるルートコンテナがこのパラメータによって識別されます。

eDirectory からロードされたドキュメントは、eDirectory オブジェクトの属性値に常駐します。指定しない場合、属性は XmlData です。ドキュメントが含まれているオブジェクトの名前の # 文字の後ろに属性名を追加することにより、属性を指定できます。

たとえば、ドキュメントベースの DN が「novell\Manual Task Documents」に指定されたとします。また、「templates」という名前の「Manual Task Documents」の下にコンテナがあるとします。

「e-mail _template」という名前の DirXML- スタイルシートオブジェクトが「templates」ディレクトリに常駐している場合、XML ドキュメントを参照するために次のリソースの識別子を使用できます。“templates/e-mail _template” or “templates/e-mail _template#XmlData”.

置換データ、URL データ、または HTTP POST データとして、リソースの識別子を提供できます。たとえば、次の要素は購読者チャネルの <message> 要素の下に表示されます。

```
<template>templates/e-mail _template#XmlData</template>
```

ドキュメントのディレクトリ

このパラメータによって、テンプレート、XSLT スタイルシートなどのリソース、および発行者チャネルの Web サーバによるその他のファイルのリソースを配置するために、基本ディレクトリとして使用されるファイルシステムディレクトリが識別されます。値の例は次のとおりです。

Windows	c:\Novell\Nds\mt_files
NetWare	SYS:\SYSTEM\mt_files
UNIX	/usr/lib/dirxml/rules/manualtask/mt_files

HTTP サーバを使用する (true|false)

このパラメータは、発行者チャネルによって Web サーバを実行されるかどうかを示しています。Web サーバを実行する必要がある場合は、パラメータを true に設定します。または、Web サーバを実行する必要がない場合、false に設定します。

レスポンス URL を持たない電子メール、またはその他のアプリケーションを指す URL を持つ電子メールの送信に、手動タスクサービスドライバのみが使用される場合、システムリソースを節約するために HTTP サーバを実行しないでください。

HTTP IP アドレスまたはホスト名

このパラメータを使用すると、発行者チャネルの Web サーバが HTTP 要求をリッスンする複数のローカル IP アドレスを指定できます。

HTTP IP アドレスまたはホスト名のパラメータ値を空白のままにしておくと、発行者チャネルの Web サーバはデフォルトの IP アドレスをリッスンします。単一の IP アドレスを持つサーバの場合は、これで十分です。ドット表記の IP アドレスをパラメータ値として配置すると、発行者チャネルの Web サーバは指定されたアドレスの HTTP 要求をリッスンします。

メールコマンド要素でホスト名またはアドレスが指定されていない場合、HTTP IP アドレスまたはホスト名で指定した値は、URL を構成するために購読者チャネルのメールハン

ドラによって使用されます。［HTTP サーバを使用する (true|false)］のパラメータが false に設定されている場合、メールメッセージの URL の構成で使用するために、HTTP IP アドレスまたはホスト名を使用して Web サーバのアドレスまたは名前を指定できます。

HTTP ポート

このパラメータは整数値であり、着信要求で発行者チャネルの Web サーバがどの TCP ポートをリッスンする必要があるのかを示しています。この値が指定されていない場合、Web サーバ接続で SSL が使用されるかどうかに応じて、ポート番号のデフォルトが 80 または 443 になります。

手動タスクサービスドライバが Identity Manager サーバで実行されている場合 (つまり、リモートマシン上のリモートローダの下で実行されない場合)、HTTP ポートを 80 または 443 以外に設定する必要があります。これは、iMonitor またはその他のプロセスは通常、ポート 80 および 443 を使用しているためです。

KMO の名前

これが空白でない場合、このパラメータは、発行者チャネルの Web サーバによって SSL に使用されるサーバ証明書およびキーが含まれている Directory の暗号化キーオブジェクトの名前になります。

このパラメータを設定すると、発行者チャネルの Web サーバで HTTP 要求の実行に SSL が使用されます。

このパラメータは、すべての Java* キーストアパラメータに優先します (以下を参照)。

eDirectory パスワードは発行者チャネル Web サーバを使用して HTTP POST データに渡されるので、セキュリティ上の理由のため SSL の使用をお勧めします。

キーストアファイルの名前

このパラメータは、キーストアパスワード、証明書の名前 (キーエイリアス)、および証明書パスワード (キーパスワード) と組み合わせて、発行者チャネルの Web サーバによって SSL で使用される証明書およびキーが含まれている Java キーストアファイルを指定するために使用します。

このパラメータを設定すると、発行者チャネルの Web サーバで HTTP 要求の実行に SSL が使用されます。

KMO の名前のパラメータが設定された場合、このパラメータおよび関連付けているパラメータは無視されます。

eDirectory パスワードは発行者チャネル Web サーバを使用して HTTP POST データに渡されるので、セキュリティ上の理由のため SSL の使用をお勧めします。

キーストアパスワード

このパラメータでは、キーストアファイルの名前のパラメータで指定した Java キーストアファイルのパスワードを指定します。

証明書の名前 (キーエイリアス)

このパラメータでは、キーストアファイルの名前のパラメータで指定した Java キーストアファイルで使用するための証明書の名前を指定します。

証明書のパスワード (キーパスワード)

このパラメータでは、証明書の名前 (キーエイリアス) のパラメータを使用して指定した証明書のパスワードを指定します。

購読者設定

購読者チャネルの設定については、この節で説明します。

SMTP サーバ

このパラメータでは、電子メールメッセージを送信するために購読者チャネルで使用される SMTP サーバの名前を指定します。

SMTP のアカウント名

SMTP サーバのパラメータを使用して指定した SMTP サーバで認証が必要とされる場合、このパラメータでは、認証に使用するアカウント名を指定します。使用されるパスワードは、ドライバの認証パラメータに関連付けられているアプリケーションのパスワードです。

デフォルトの「From」アドレス

指定されている場合、これは SMTP で使用される、購読者チャネルによって送信される電子メールメッセージのフィールドの電子メールアドレスです。これが指定されていない場合、購読者に送信された <mail> 要素には <from> 要素が含まれている必要があります。

購読者に送信された <mail> 要素の下の <from> 要素は、このパラメータより優先されます。

追加のハンドラ

指定されている場合、これはスペースで区切られた Java クラス名のリストです。各クラス名は、com.novell.nds.dirxml.driver.manualtask.CommandHandler インタフェースを実装し、カスタム XDS 要素を処理するカスタムクラスです (<mail> のハンドラは組み込みハンドラです)。

カスタムハンドラに関する詳細情報については、325 ページの付録 I「手動タスクサービスドライバ : 購読者チャネルのカスタム要素ハンドラ」を参照してください。

発行者設定

発行者チャネルの設定については、この節で説明します。

追加のサーブレット

空白でない場合、これはスペースで区切られた Java クラス名のリストです。各クラス名は、javax.servlet.http.HttpServer を拡張するカスタムクラスです。カスタムサーブレットを使用して発行者チャネルの Web サーバの機能を拡張できます。

カスタムサーブレットに関する詳細情報については、327 ページの付録 J「手動タスクサービスドライバ : 発行者チャネルのカスタムサーブレット」を参照してください。

購読者チャネルのポリシー

購読者チャネルポリシーの設定は、手動タスクサービスドライバを使用して特定のインストールで何を実行するのかに依存します。しかし、特定のガイドラインが役立ちます。

一般的には、購読者に送信するために <mail> 要素を構成するのに最適な場所は、コマンド変換ポリシーです。その理由は、コマンドがコマンド変換ポリシーに到達するまでに、多くの DirXML エンジン処理が完了しているためです。つまり、追加イベントに対してポリシーの作成が処理されます (たとえば電子メールの構成に必要なすべての属性を持たないオブジェクトに対する追加イベントの拒否の許可)。また、関連付けられていないオブジェクトの変更イベントは、すでに追加イベントに変換されています。

電子メールメッセージを構成する XSLT スタイルシートは、eDirectory に詳細情報を問い合わせる必要がある場合と、ない場合があります。

たとえば、電子メールメッセージが単なる新しい従業員への歓迎のメッセージである場合、次の必要なすべての情報を追加コマンドに含めることができます。名前、名字、およびインターネットの電子メールアドレス。これは、作成ポリシーで、名前、名字、およびインターネットの電子メールアドレスが必要な属性であることを指定して実行します。これにより、必要な情報が含まれている追加コマンドのみがコマンド変換に到達できます。

しかし、電子メールメッセージが従業員のマネージャに対するメッセージである場合、スタイルシートによって eDirectory への問い合わせが実行される必要があります。マネージャ DN は、従業員のユーザオブジェクトの追加イベントから取得できますが、その情報はマネージャのユーザオブジェクトの属性であるため、マネージャの電子メールアドレスを取得するためにクエリを行う必要があります。

また、ドライバに関連付けられているオブジェクトの変更コマンドの結果として電子メール通知機能が生成される場合、変更コマンドに含まれていない情報を取得するためにクエリを実行する必要があります。

コマンドをブロックして、購読者に到達しないようにする

電子メールメッセージが追加イベント以外のイベントから生成される場合、監視されるオブジェクトに対して、追加イベントが購読者に到達する必要があります。追加イベントを購読者に到達させると、生成された関連付けの値が購読者から Identity Manager に返されます。

手動タスクサービスドライバポリシーによって監視される eDirectory オブジェクトが、手動タスクサービスドライバに関連付けられていることが重要です。関連付けられたオブジェクトのみの削除イベント、名前変更イベント、および移動イベントがドライバにレポートされます。また、関連付けられていないオブジェクトの変更イベントは、購読者チャネルのイベント変換後に追加イベントに変換されます。

その他のすべてのコマンド (変更、移動、名前変更、および削除) は、コマンド変換ポリシーによってブロックされ、購読者に到達しないようにする必要があります。購読者は、<add> コマンドおよび <mail> コマンドのみ処理します。その他のコマンドは、購読者によりエラーが返されます。

電子メールメッセージの生成

電子メールメッセージは、送信される電子メールメッセージを説明する <mail> 要素の受信に対して、購読者によって送信されます。<mail> 要素およびそのコンテンツの説明については、311 ページの付録 G「手動タスクサービスドライバ :<mail> 要素について」を参照してください。

すべての Identity Manager イベント (追加、変更、名前変更、移動、削除) に対して、電子メールメッセージを生成できます。

<mail> 要素の <message> 要素の子で提供された置換データは、次の 2 つの主な要因に依存します。

- メッセージ本文の生成に使用されたテンプレート。電子メールテンプレートによって使用される置換項目は、<replacement-data> 要素の子として表示されます。
- 電子メールによって発行者チャネル上のレスポンスが発生する場合に、発行者チャネルの Web ページテンプレートに必要な情報。Web ページテンプレートによって使用される置換項目は、<url-query> 要素の子として表示されます。これは、<url-data> の子であり、<replacement-data> の子でもあります。

発行者チャネルの Web サーバを指す URL を電子メールメッセージに含める必要があり、ユーザから情報を取得するために使用される場合、置換データに少なくとも 1 つの responder-dn 項目が含まれている必要があります。responder-dn 項目の値は、メッセージが送信されるユーザのユーザオブジェクトの DN である必要があります。

テンプレートでクエリの置換トークン (216 ページのセクション「置換データ」を参照) が使用されている場合、<message> 要素の置換データには、src-dn、src-entry-id という名前の項目が含まれているか、または適切な値に関連付けられている必要があります。問い合わせが実行される eDirectory オブジェクトがすでに手動タスクサービスドライバに関連付けられている場合のみ、関連項目を使用できます。関連付けられていないオブジェクトに対して購読者によって生成された関連付けは、クエリが発生したときに eDirectory オブジェクトに記述されていないため使用できません。

<message> 要素で、MIME タイプのメッセージ本文を指定できます。MIME タイプを指定したけれども、スタイルシートが指定されていない場合 (つまり、<message> の <stylesheet> 要素の子がない場合)、2 つのデフォルトのスタイルシート名のどちらかが使用されます。MIME タイプがテキスト / プレーンである場合、デフォルトのスタイルシート名は process_text_template.xsl です。MIME タイプがテキスト / プレーン以外である場合、デフォルトのスタイルシート名は process_template.xsl です。

購読者チャネルの電子メールテンプレート

電子メールテンプレートは、ボイラープレートおよび置換トークンが含まれている XML ドキュメントです。電子メールメッセージ本文のテキストを生成するために、電子メールテンプレートが使用されます。テンプレートに関する一般的な情報については、214 ページのセクション「テンプレート」を参照してください。

電子メールテンプレートで使用されている置換トークンによって、<mail> 要素を構成する購読者チャネルポリシーによって構成された、<replacement-data> 要素の子として提供される必要がある <item> 要素が指定されます。たとえば、電子メールテンプレートに置換トークン $employee-name$ がある場合、<message> 要素の置換データに <item name="employee-name"> 要素がある必要があります。従業員名の項目がない場合、テンプレート内の置換トークンによって占められている場所には、電子メールメッセージ本文のテキストはありません。

プレーンテキスト、HTML、または XML であるメッセージ本文を生成するために、電子メールテンプレートを使用できます。

電子メールテンプレートによってプレーンテキストのメッセージが生成された場合、出力タイプとしてプレーンテキストを指定するスタイルシートによって処理される必要があります。スタイルシートで出力タイプとしてプレーンテキストが指定されていない場合、不

都合な XML エスケーピングが発生します。デフォルトの手動タスクサービスドライバのスタイルシートである process_text_template.xsl は、通常プレーンテキストのテンプレートの処理に使用されます。

発行者チャネルのポリシー

手動タスクサービスドライバの多くの実装では、発行者チャネルのポリシーは必要ありません。これは、Web ページおよび XDS テンプレートを構成することが可能であるので、XDS が必要とする結果を得ることができ、XDS がポリシーによってさらに処理される必要がないためです。

ポリシーが必要な場合、インストール固有になります。

発行者チャネルの Web ページテンプレート

Web ページテンプレートは、ボイラープレートおよび置換トークンが含まれている XML ドキュメントです。Web ページのドキュメント (通常は HTML ドキュメント) を生成するために、Web ページテンプレートが使用されます。テンプレートに関する一般的な情報については、214 ページのセクション「テンプレート」を参照してください。

Web ページテンプレートの置換トークンにより、購読者チャネルの URL クエリデータとしてどの置換データが提供されるのかが指定されます。発行者チャネルの置換データは、HTTP GET 要求の URL クエリ文字列、および HTTP POST 要求の URL クエリ文字列と POST データから取得されます。

購読者チャネルから、電子メールメッセージへ、次に発行者チャネルの Web サーバへの置換データのフローの例としては、次のシナリオを考えてみます。

手動タスクサービスドライバは、新しい従業員に部屋番号を割り当てることを新しい従業員のマネージャに依頼するように設定されています。マネージャに対する電子メールのトリガは、購読者チャネルのコマンド変換ポリシーによって処理される、新しいユーザオブジェクトの <add> コマンドです。

マネージャが電子メールメッセージの URL をクリックすると、マネージャの Web ブラウザに Web ページが表示されます。Web ページでは、誰のためにマネージャが部屋番号を入力しているのかを示す必要があります。

これを実行するために、名前で新しいユーザを識別する置換データ項目が購読者チャネルの <url-query> 要素に含まれています。

```
<item name="subject-name">Joe the Intern</item>
```

これにより、URL クエリ文字列には (他の文字列の間に)「subject-name=Joe%20the%20Intern」が含まれます (“%20” は URL エンコードスペースです)。

マネージャが電子メールメッセージの URL をクリックすると、マネージャの Web ブラウザによって発行者チャネルの Web サーバに URL が送信されます。Web サーバによって、「subject-name」という名前の置換データ項目が「Joe the Intern」という値とともに構成されます。

URL にも指定されている Web ページテンプレートには、置換トークン $subject-name$ が含まれます。Web ページを構成するために Web ページテンプレートがスタイルシートによって処理されると、置換トークンが「Joe the Intern」に置換されます。これにより、

ユーザオブジェクトの作成によって電子メールが送信された従業員の Web ページがカスタマイズされます。

購読者チャネルから発行者チャネルへのトランザクションの詳細情報については、315 ページの付録 H「手動タスクサービスドライバ : 新しい従業員のデータフローのシナリオ」を参照してください。

発行者チャネルの XDS テンプレート

XDS テンプレートは、ボイラープレートおよび置換トークンが含まれている XML ドキュメントです。XDS テンプレートは、手動タスクサービスドライバの発行者チャネルの Identity Manager に送信された XDS ドキュメントを生成するために使用されます。テンプレートに関する一般的な情報については、［概要］セクションの［テンプレート］を参照してください。

XDS テンプレートの置換トークンによって、HTTP POST 要求のデータとして Web サーバに提供されたいくつか置換データが指定されます。

たとえば、次の XDS テンプレートについて考えてみます。

```
<nds> <input> <modify class-name="User" src-dn="not-applicable">
<association>$association$</association> <modify-attr attr-
name="roomNumber"> <remove-all-values/> <add-value> <value>$room-
number$</value> </add-value> </modify-attr> </modify> </input> </nds>
```

HTTP POST データが関連付けの値および room-number の値を提供する必要があることが、テンプレートの置換トークンによって指定されます。

通常、関連付けの値は購読者チャネルで発生します。購読者チャネルの電子メールには、電子メールメッセージに配置される URL のクエリ文字列内の association=some value が配置されます。URL が Web サーバに送信されたときに Web ページを生成するために使用される Web ページテンプレートでは、通常、非表示の INPUT 要素に関連付けの値が配置されます。

```
<INPUT TYPE="hidden" NAME="association" VALUE="$association$"/>
```

非表示の INPUT 要素に関連付けの値を配置すると、「association=some value」のペアが HTTP POST データの一部として送信されます。

次に似た INPUT 要素を使用して、Web ページに room-number の値が入力されます。

```
<input TYPE="text" NAME="room-number" SIZE="20" MAXLENGTH="20"/>
```

マネージャが「1234」と入力して［送信］をクリックした場合、Web ブラウザによって「room-number=1234」が HTTP POST データの一部として送信されます。

次に、Web サーバによって <item name=“association”> 置換データ項目、および XDS テンプレートを処理するときに使用された <item name=“room-number”> 置換データ項目が生成されます。

POST データで指定されたスタイルシートを使用して XDS テンプレートを処理することにより、XDS ドキュメントが生成されます。次に、手動タスクサービスドライバの発行者チャネルで、Identity Manager に XDS ドキュメントが送信されます。

トレースの設定

手動タスクサービスドライバでは、さまざまなトレースレベルのメッセージが出力されます。

レベル	トレースメッセージの説明
0	トレースメッセージはありません
1	トレースの基本的な操作の単一行のメッセージ
2	追加のメッセージはありません (DirXML エンジンは、このレベル以降で XML ドキュメントをトレースします)
3	追加のメッセージはありません
4	テンプレートおよびスタイルシートからの、ドキュメントの構成に関連するメッセージ
5	置換データのドキュメントがトレースされています

8.2.4 追加情報

手動タスクサービスドライバの設定に関する詳細情報については、付録の次の節を参照してください。

- 299 ページの付録 D「手動タスクサービスドライバ : 置換データ」
- 305 ページの付録 E「手動タスクサービスドライバ : 自動置換データ項目」
- 307 ページの付録 F「手動タスクサービスドライバ : テンプレートのアクション要素について」
- 311 ページの付録 G「手動タスクサービスドライバ :<mail> 要素について」
- 315 ページの付録 H「手動タスクサービスドライバ : 新しい従業員のデータフローのシナリオ」
- 325 ページの付録 I「手動タスクサービスドライバ : 購読者チャネルのカスタム要素ハンドラ」
- 327 ページの付録 J「手動タスクサービスドライバ : 発行者チャネルのカスタムサーブレット」

高可用性

9

Identity Manager を共有ストレージで使用し、高可用性を実現できます。クラスタリング環境で Novell® eDirectory™ および Identity Manager を使用するには、いくつかのステップを実行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。

9.1 Linux および UNIX で共有ストレージを使用するための、eDirectory および Identity Manager の設定

この節では、共有ストレージを使用して高可用性クラスタのフェールオーバーを実現できるように、Directory および Identity Manager を設定するステップについて説明します。この節の説明は、特定のクラスタマネージャに固有のものではなく、Linux または UNIX プラットフォーム上の高可用性クラスタの共有ストレージ一般に当てはまります。

基本的な概念は、eDirectory および Identity Manager の状態データは共有ストレージに配置し、サービスを現在実行しているクラスタノードから利用できるようにする必要があるということです。つまり、通常は /var/nds/dib にある eDirectory データストアをクラスタ共有ストレージに再配置する必要があります。Identity Manager の状態データも /var/nds/ にあります。クラスタノード上の各 eDirectory インスタンスは、共有ストレージのデータストアを使用するよう設定する必要があります。その他の eDirectory の設定データも、共有ストレージに常駐する必要があります。

eDirectory データストアの他に、サーバ固有のキーをクラスタノード間で複製するために、NICI (Novell International Cryptographic Infrastructure) のデータも共有する必要があります。一般的には、NICI のデータを共有ストレージに移動するのではなく、NICI のデータを各クラスタノードのローカル保存領域にコピーする方が適切です。クラスタノードがセカンダリ状態になっていて共有ストレージをホストしていない場合でも、クライアントの NICI 機能をクラスタノード上で使用できるようにするために、この方法をお勧めします。

以降の節では、次の前提に基づいて、eDirectory および NICI のデータの共有について説明します。

- NICI、eDirectory、および Identity Manager のデータと設定には、デフォルトのインストール先を使用している。

  Identity Manager のデータについて、eDirectory のデータとは別に説明することはしません。関連する Identity Manager のデータは eDirectory のデータと同じ場所に配置されているためです。
- eDirectory および Identity Manager のインストール手順を熟知している。
- 2 ノードクラスタを使用している。

2 ノードクラスタは、高可用性を実現するために最も一般的に使用されている設定です。ただし、この節で説明する概念は、*n* ノードクラスタにも容易に拡張できます。

この節では、次の項目について説明します。

9.1.1 eDirectory のインストール

注 **:** NICI は、eDirectory インストール手順の一部としてインストールされます。

1. プライマリクラスタノードに eDirectory をインストールします。
2. プライマリクラスタノードで eDirectory を設定します。プライマリクラスタノードに新しいツリーを作成するか、既存のツリーにサーバをインストールします。eDirectory サーバの名前には、UNIX サーバの名前に使用していないものを使用します。クラスタノードの 1 つに固有の名前を使用するのではなく、クラスタに共通の名前を使用してください。
3. セカンダリクラスタノードに、同じバージョンの eDirectory をインストールします。セカンダリクラスタノードでは eDirectory を設定しないでください。

   セカンダリノードには個別のツリーはありません。

9.1.2 Identity Manager のインストール

1. ［メタディレクトリサーバ］オプションを使用して、プライマリクラスタノードに Identity Manager をインストールします。

   インストールプロセスにより、Identity Manager ファイルがインストールされ、Identity Manager で使用する eDirectory ツリーが設定されます。
2. セカンダリクラスタスイッチを使用し、セカンダリクラスタに同じバージョンの Identity Manager をインストールします。次を入力します。

   ```
   dirxml_platform.bin -DCLUSTER_INSTALL="true"
   ```

   インストールでは、［メタディレクトリサーバ］オプションを選択します。

   セカンダリクラスタスイッチを使用すると、Identity Manager ファイルはインストールされますが、追加の eDirectory 設定は実行されません。セカンダリノードには個別のツリーがないので、設定は必要ありません。

9.1.3 NICI データの共有

NICI は、eDirectory、Identity Manager、および Novell クライアントアプリケーションで使用する暗号化サービスを提供します。eDirectory とともに使用する場合、NICI はサーバ固

有のキーを提供します。これらのサーバ固有のキーは、eDirectory がクラスタサービスとして実行されるすべてのクラスタノードで同じでなければなりません。

NICI データの共有には、2 つの方法があります。

- NICI データをクラスタ共有ストレージに配置する。

  この方法の短所は、クラスタノードが共有ストレージをホストしていない場合、NICI に依存するアプリケーションはそのクラスタノード上でエラーを引き起こす点です。
- プライマリサーバからセカンダリサーバのローカル保存領域に NICI データをコピーする。

NICI データをコピーするには、次の手順に従います。

1. セカンダリクラスタノードの /var/novell/nici を、(/var/novell/nici.sav などの) 別の名前に変更します。
2. プライマリクラスタノードからセカンダリクラスタノードに /var/novell/nici ディレクトリをコピーします。

   このためには、scp を使用するか、またはプライマリノードの /var/novell/nici ディレクトリのファイルを作成してセカンダリノードに転送し、セカンダリノードのディレクトリで解凍 (untar) します。

9.1.4 eDirectory および Identity Manager のデータの共有

デフォルトでは、eDirectory は、/var/nds/dib にデータストアを格納します。設定および状態のその他の項目も、/var/nds とそのサブディレクトリに格納されます。eDirectory のデフォルト設定ディレクトリは、/etc です。高可用性クラスタの共有ストレージとともに使用するために eDirectory および Identity Manager を設定するには、次の手順が必要です。これらのステップは、共有ストレージが /shared にマウントされていることを前提としています。

- 229 ページの 「プライマリノード上の手順」
- 230 ページの 「セカンダリノード上の手順」

プライマリノード上の手順

1. /var/nds ディレクトリのサブツリーを /shared/var/nds にコピーします。
2. /var/nds ディレクトリを別の名前 (たとえば /var/nds.sav) に名前変更します。

   必ずしも必要ではありませんが、この時点でバックアップを作成すると、必要に応じて eDirectory を再インストールすることなく作業をやり直すことができます。
3. /var/nds から /shared/var/nds にシンボリックリンク (たとえば ln -s /shared/var/nds /var/nds) を作成します。
4. 次のシンボリックリンクを作成します。

リンク元	リンク先
/shared/var/nds/class16.conf	/etc/class16.conf
/shared/var/nds/class32.conf	/etc/class32.conf

リンク元	リンク先
/shared/var/nds/help.conf	/etc/help.conf
/shared/var/nds/ndsimonhealth.conf	/etc/ndsimonhealth.conf
/shared/var/nds/miscicon.conf	/etc/miscicon.conf
/shared/var/nds/ndsimon.conf	/etc/ndsimon.conf
/shared/var/nds/macaddr	/etc/macaddr

5 /etc/nds.conf のバックアップコピーを作成します。

6 /etc/nds.conf を /shared/var/nds に移動します。

7 /shared/var/nds/nds.conf を編集し、次のエントリをファイルに挿入します (現在のエントリを同じ名前で上書きします)。

- n4u.nds.dibdir=/shared/var/nds/dib
- n4u.server.configdir=/shared/var/nds
- n4u.server.vardir=/shared/var/nds
- n4u.nds.preferred-server=localhost

次のエントリについては、eth0:0 をクラスタ共有 Ethernet インタフェースのインタフェース名に置き換えます。lo も、ローカルホスト Ethernet インタフェースのインタフェース名に置き換えます。

- n4u.nds.server.interfaces=eth0:0@524,lo@524
- http.server.interfaces=eth0:0@8008,lo@8008
- https.server.interfaces=eth0:0@8009,lo@8009

8 /etc/nds.conf から /shared/var/nds/nds.conf へのシンボリックリンクを作成します。

9 ndsd を起動し、ndsd が共有ストレージで動作することを確認します。

10 ndsd を停止します。

11 ndsd を、ホストするリソースのクラスタマネージャのリストに配置します。

12 ndsd をデーモンのリストから削除し、起動時に初期化プロセスによって起動されるようにします。

セカンダリノード上の手順

1 /var/nds ディレクトリを別の名前 (たとえば /var/nds.sav) に名前変更します。厳密には必要ありませんが、バックアップを作成すると、必要に応じて eDirectory を再インストールすることなく作業をやり直すことができます。

2 /var/nds から /shared/var/nds にシンボリックリンクを作成します。

3 /etc/nds.conf のバックアップコピーを作成します。

4 /etc/nds.conf を削除します。

5 /etc/nds.conf から /shared/var/nds/nds.conf へのシンボリックリンクを作成します。

6 ndsd を、ホストするリソースのクラスタマネージャのリストに配置します。

7 ndsd をデーモンのリストから削除し、起動時に初期化プロセスによって起動されるようにします。

プライマリノードおよびセカンダリノードの手順が完了した後、クラスタサービスを起動します。プライマリノードで、eDirectory および Identity Manager が起動します。

9.1.5 Identity Manager ドライバの考慮事項

Identity Manager ドライバのほとんどは、クラスタ設定で実行できます。ただし、次のことを考慮する必要があります。

- 実行可能ドライバ (.jar ファイルまたは共有オブジェクト、あるいはその両方) は、各クラスタノードにインストールする必要があります。
- ドライバがサポートするアプリケーションと同じサーバでドライバを実行する必要がある場合、アプリケーションもクラスタサービスの一部として実行されるよう設定する必要があります。
- ドライバで、ドライバ固有の状態データを保存する場所が設定可能な場合、その場所はクラスタ共有ストレージ上に存在する必要があります。

  たとえば、変更ログなしで使用する LDAP ドライバ、トリガレスモードで使用する JDBC ドライバなどです。
- ドライバが設定データを eDirectory の外部に格納する場合、その設定データは共有ストレージに配置するか、各クラスタノードに複製する必要があります。たとえば、手動タスクドライバのテンプレートディレクトリなどです。

9.2 SuSE Linux についてのケーススタディ

SUSE LINUX Enterprise Server 8 とともに共有ストレージで実行されている Identity Manager の詳細については、TID10093317 (http://support.novell.com/cgi-bin/search/searchtid.cgi?/10093317.htm) を参照してください。

Novell Audit によるログとレポート 10

Identity Manager は、監査とレポーティングに Novell® Audit を使用するように設計されています。

10.1 概要

Novell Audit には、監査、ログ、レポート、および通知などの機能を実現する技術が集約されています。Identity Manager では、Novell Audit と統合することで、ドライバとエンジンのアクティビティに関する現在と過去の状態の詳しい情報が提供されます。この情報は、設定済みのレポート、標準の通知サービス、およびユーザ定義データログなどの一連の機能により提供されます。

Identity Manager イベントのリアルタイムな監視、任意の Identity Manager イベントに関する電子メール通知の送信、Novell Audit を使用した Identity Manager アクティビティについてのレポートの作成などを行うことができます。

Novell Audit に送信されるメッセージのタイプは、レポーティングと通知サービス (RNS) で提供されるものと同様のプラグインを使用して制御されます。ステータス、追加エントリ、検索など、トラックする操作またはデバッグ情報のタイプを選択するには、これらのプラグインに別のレベルを追加します。

レポーティングと通知サービス (RNS)

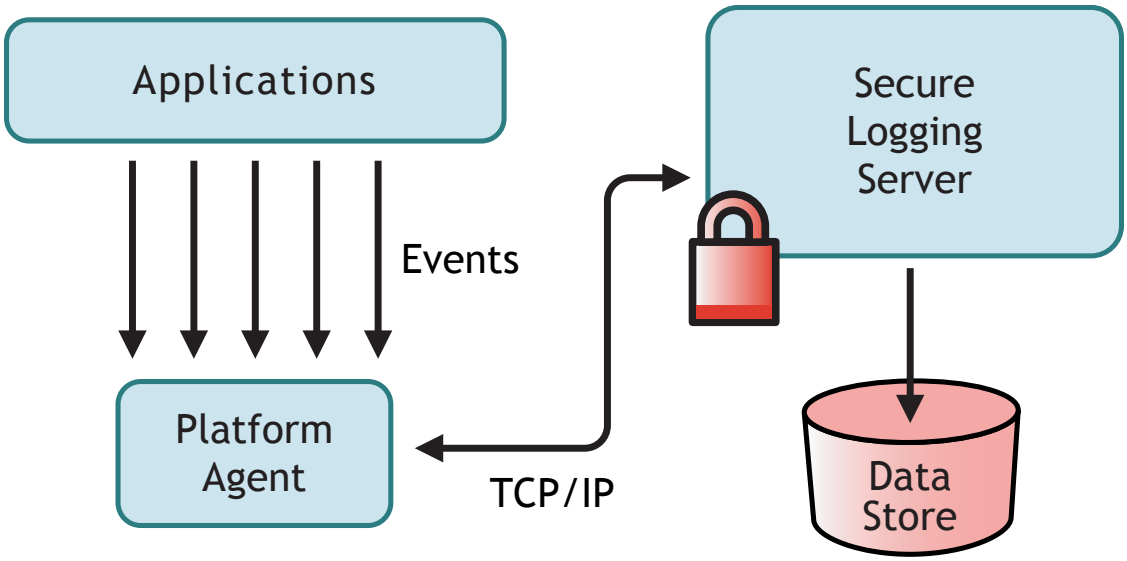
レポーティングと通知サービス (RNS) は、Identity Manager の今後のリリース製品ではサポートされなくなりますが、現在 RNS を使用している場合、メタディレクトリエンジンは引き続き RNS 機能を処理します。Novell Audit は RNS によって提供される機能を拡張している上に、RNS は将来の Identity Manager リリースではサポートされないため、Novell Audit への移行を計画することをお勧めします。RNS のマニュアルについては、『*DirXML 1.1a Administration Guide* (http://www.novell.com/documentation/lg/dirxml11a/dirxml/data/afae8bz.html)』を参照してください。

10.2 Novell Audit

Novell Audit は、中央型のクロスプラットフォームログサービスで、複数のアプリケーションのデータを中央型のデータストアに記録できます。イベントデータのログ後、詳細レポートおよびカスタムクエリを実行し、ログされたイベントに基づく通知を発信できます。

次の図は、Novell Audit の上位レベルのアーキテクチャを示しています。

図 *10-1* アーキテクチャの概要



この図では、Identity Manager は、プラットフォームエージェントを使用して Novell Audit のセキュアログサーバにイベントをレポートするアプリケーションの 1 つです。

10.3 Novell Audit の設定

「概要」で説明したように、Novell Audit は、次の 2 つの基本コンポーネントで構成されます。

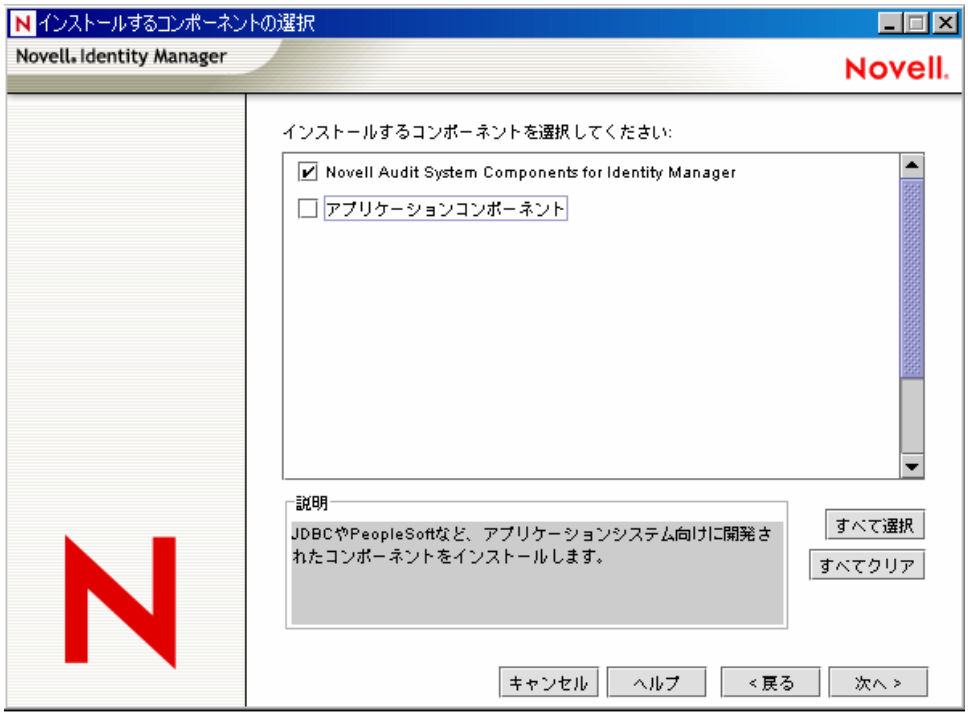
- プラットフォームエージェント
- セキュアログサーバ

プラットフォームエージェントは、Identity Manager とともに動作し、イベントをセキュアログサーバに通信するコンポーネントです。Identity Manager とともにインストールされます。セキュアログサーバは Identity Manager およびその他のアプリケーションからイベントデータを受信するコンポーネントで、Identity Manager とは別に Novell Audit 1.0.3 の一部としてインストールされます。

10.3.1 プラットフォームエージェントの設定

プラットフォームエージェントは、インストール時に［Novell Audit System Components for the Identity Manager］オプションを選択すると、インストールされます。

図 *10-2* *Identity Manager* のインストール



プラットフォームエージェントは Identity Manager のインストール時にインストールすることも、別途インストールすることも可能です。

注 **:** メタディレクトリエンジンの起動後にプラットフォームエージェントをインストールする場合、Identity Manager を再起動してプラットフォームエージェントと Identity Manager をリンクさせる必要があります。Identity Manager がプラットフォームエージェントに接続しようとするのは、起動時のみです。

プラットフォームエージェントをインストールした後は、次の手順に従い、プラットフォームエージェントを設定します。

1 Novell Audit の設定ファイル logevent.cfg をテキストエディタで開きます。このファイルのデフォルトの場所は次のとおりです。

オペレーティングシステム	パス
NetWare®	sys:\etc\logevent.cfg
Windows	*windows_directory*\logevent.cfg
Linux\Solaris	/etc/logevent.conf

2 LogHost パラメータの値を、IP アドレスまたはセキュアログサーバの DNS 名に変更します。

3 Identity Manager を再起動します。

10.3.2 セキュアログサーバの設定

注 **:** Novell Audit のセキュアログサーバは、Identity Manager には含まれていません。セキュアログサーバは Novell Audit 1.0.3 の一部です。Novell Audit 1.0.3 のダウンロードの詳細については、Novell Audit Product Page (http://www.novell.com/products/nsureaudit) を参照してください。

セキュアログサーバは、NetWare 5.1 以降、Windows* NT 4.0、Windows 2000 Server、Windows 2003 Server、Solaris* 8 または 9、および SUSE® Enterprise Linux Server 8 および SUSE 9.0 を含む Linux* の複数のバージョンで実行できます。

セキュアログサーバは、MySQL*、Oracle*、Microsoft* SQL Server、Java* アプリケーション、およびフラットファイルを含む複数の他の場所にイベントを記録できます。Novell Audit には、Novell Audit レポートと呼ばれる、データベースにイベントデータを問い合わせるカスタムアプリケーションが含まれます。この高度なレポーティングツールを使用するには、ODBC コネクタを持つデータストアが必要です。

各プラットフォーム用に、セキュアログサーバの設定手順について説明したクイックスタートガイドが提供されています。また、Novell Audit 1.0.3 のインストールにも含まれています。また、Novell Audit マニュアルの Web サイト (http://www.novell.com/documentation/nsureaudit) にある『*Novell Audit 1.0.3 Administration Guide*』で参照することもできます。

10.4 ログの環境設定

Identity Manager では、いくつかの事前定義されたレベルを使用するか、またはログを記録する各イベントを個別に選択することで、ログを記録するイベントを設定できます。設定の変更もログに記録されます。

242 ページのセクション 10.4.2「ユーザ定義イベント」に説明されているように、ユーザ定義イベントは、ログが有効な場合は常に記録され、メタディレクトリエンジンによるフィルタリングは実行されません。

ログは、ドライバセットまたは各ドライバで設定します。ドライバは、ドライバセットからログ設定を継承できます。ログ情報を含む eDirectory™ 属性の詳細については、244 ページのセクション 10.4.3「eDirectory オブジェクト」を参照してください。

デフォルトでは、重要なイベントとユーザ定義イベントのみがログに記録されます。

10.4.1 ログに記録するイベントの選択

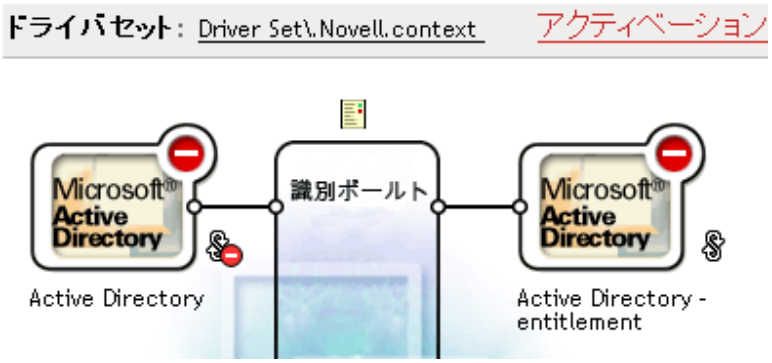
ドライバセットまたは特定のドライバに対するイベントを選択できます。

ドライバセットのイベントのログ記録

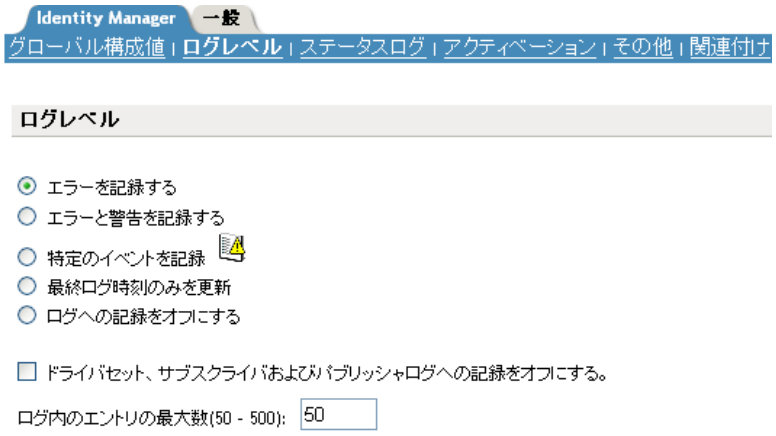
1 iManager で、[Identity Manager] > [Identity Manager の概要] の順に選択し、[次へ] をクリックします。

2 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 ドライバセット名をクリックします。［オブジェクトの変更］ページが表示されます。



4 ［Identity Manager］タブの［ログレベル］を選択します。



5 各自の環境に必要なログのオプションを選択します。

オプション	説明
ログエラー	これは、デフォルトのログレベルです。このオプションは、エラーステータスを持つすべてのイベントと、ユーザ定義イベントをログに記録します。 このオプションを選択すると、10 進数 ID が 196646 のイベントのみを、最初のテキストフィールドにエラーメッセージが格納された状態で受け取ります。
エラーと警告を記録する	このオプションは、エラーまたは警告ステータスを持つすべてのイベントと、ユーザ定義イベントをログに記録します。 このオプションを選択すると、10 進数 ID が 196646 および 196647 のイベントのみを、最初のテキストフィールドにエラーまたは警告のメッセージが格納された状態で受け取ります。

オプション	説明
特定のイベントを記録	このオプションでは、ログに記録する特定のイベントをリストから選択できます。 アイコンをクリックしてイベントを選択します。ユーザ定義イベントは、常にログに記録されます。 エラーまたは警告以外のイベントをログに記録するには、対象のイベントをリストから選択する必要があります。このオプションを選択した場合に、エラーおよび警告のイベントを引き続きログに記録するときは、エラーおよび警告も選択する必要があります。使用できるすべてのイベントのリストについては、240 ページの 「Identity Manager イベント」を参照してください。
最終ログ時刻のみを更新	ユーザ定義イベントのみをログに記録します。イベントが発生した場合、最終ログ時刻が更新されるため、ステータスログで最後のエラーの日付と時刻を参照できます。
ログオフ	ユーザ定義イベントのみをログに記録します。
DriverSet、購読者および発行者ログへの記録をオフにします	ドライバセットオブジェクトのログ、および購読者と発行者のログへのログをオフにします。
ログ内のエントリの最大数	この設定では、ステータスログに記録するエントリの最大数を指定します。詳細については、248 ページのセクション 10.7.2「ステータスログの表示」を参照してください。

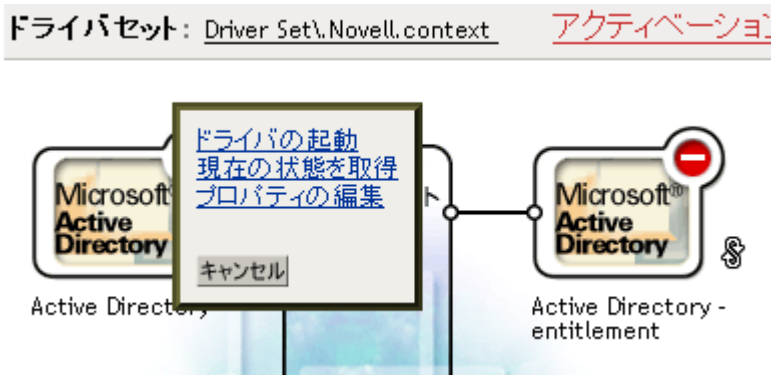
6 ログに記録するイベントをすべて選択したら、［OK］をクリックします。

ドライバのイベントのログ記録

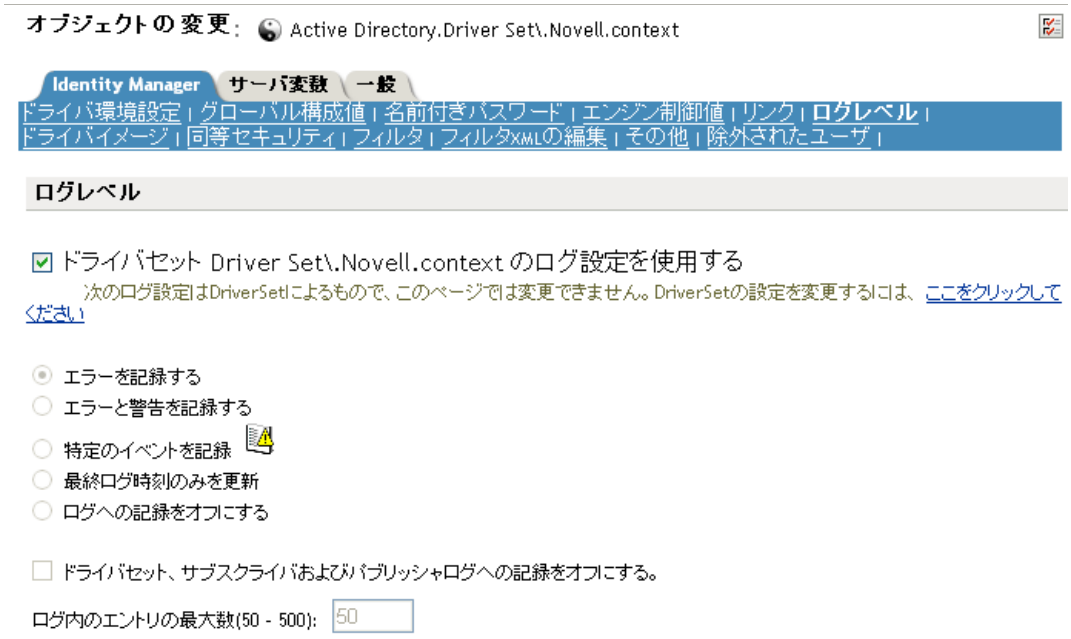
1 iManager で、［Identity Manager］>［Identity Manager の概要］の順に選択し、［次へ］をクリックします。

2 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。

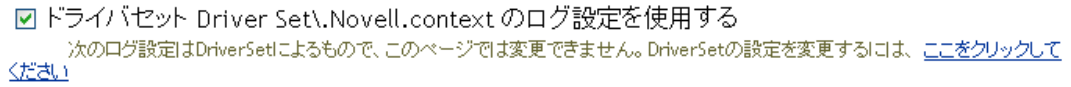
3 ドライバアイコンの右上隅をクリックし、［プロパティの編集］を選択します。



4 ［Identity Manager］タブの［ログレベル］を選択します。



5 (オプション) デフォルトでは、ドライバオブジェクトはドライバセットオブジェクトのログ設定を継承するよう設定されています。このドライバのみに対してログを記録するイベントを選択するには、［use log settings from the Driver Set (ドライバセットのログ設定を使用する)］をオフにします。



6 各自の環境に必要なログのオプションを選択します。

オプション	説明
ログエラー	これは、デフォルトのログレベルです。このオプションは、エラーステータスを持つすべてのイベントと、ユーザ定義イベントをログを記録します。 このオプションを選択すると、10 進数 ID が 196646 のイベントのみを、最初のテキストフィールドにエラーメッセージが格納された状態で受け取ります。
エラーと警告を記録する	このオプションは、エラーまたは警告ステータスを持つすべてのイベントと、ユーザ定義イベントをログに記録します。 このオプションを選択すると、10 進数 ID が 196646 および 196647 のイベントのみを、最初のテキストフィールドにエラーまたは警告のメッセージが格納された状態で受け取ります。

オプション	説明
特定のイベントを記録	このオプションでは、ログに記録する特定のイベントをリストから選択できます。 アイコンをクリックしてイベントを選択します。ユーザ定義イベントは、常にログに記録されます。 エラーまたは警告以外のイベントをログに記録するには、対象のイベントをリストから選択する必要があります。このオプションを選択した場合に、エラーおよび警告のイベントを引き続きログに記録するときは、エラーおよび警告も選択する必要があります。使用できるすべてのイベントのリストについては、240 ページの 「Identity Manager イベント」を参照してください。
最終ログ時刻のみを更新	ユーザ定義イベントのみをログに記録します。イベントが発生した場合、最終ログ時刻が更新されるため、ステータスログで最後のエラーの日付と時刻を参照できます。
ログオフ	ユーザ定義イベントのみをログに記録します。
DriverSet、購読者および発行者ログへの記録をオフにします	ドライバセットオブジェクトのログ、および購読者と発行者のログへのログをオフにします。
ログ内のエントリの最大数	この設定では、ステータスログに記録するエントリの最大数を指定します。詳細については、248 ページのセクション 10.7.2「ステータスログの表示」を参照してください。

7 ログに記録するイベントをすべて選択したら、［OK］をクリックします。

Identity Manager イベント

Identity Manager によってログに記録されるすべてのイベントのリストは、269 ページの付録 C「Identity Manager のイベントとレポート」で記載しています。

ドライバの起動と停止のイベント

Identity Manager では、ドライバが起動または停止されると、イベントが生成されます。次の表に、このようなイベントについて詳しく示します。

表 *10-1* ドライバの起動と停止のイベント

イベント	ログレベル	情報
EV_LOG_DRIVER_START	LOG_INFO	ドライバの起動をログに記録するには、［特定のイベントを記録］オプションを使用してこのイベントを選択する必要があります。
EV_LOG_DRIVER_STOP	LOG_WARNING	ドライバの停止をログに記録するには、［**エラーと警告を記録する**］**を選択するか、**［特定のイベントを記録］オプションを使用してこのイベントを選択します。

これらのイベントに基づいて Novell Audit の通知を作成する方法の詳細については、245 ページのセクション 10.6「イベントに基づく通知の送信」を参照してください。

エラーおよび警告のイベント

Identity Manager では、エラーまたは警告が発生すると、イベントが生成されます。次の表に、このようなイベントの詳細を示します。

表 *10-2* エラーおよび警告のイベント

イベント	ログレベル	情報
DirXML_Error	LOG_ERROR	Identity Manager のすべてのエラーでこのイベントが記録されます。発生した実際のエラーコードは、このイベントに格納されます。 エラーを記録するには、[**ログエラー**]、[**エラーと警告を記録する**] を選択するか、[特定のイベントを記録] オプションを使用してこのイベントを選択します。
DirXML_Warning	LOG_WARNING	Identity Manager のすべての警告でこのイベントが記録されます。発生した実際の警告コードは、このイベントに格納されます。 警告を記録するには、[**エラーと警告を記録する**] を選択するか、[特定のイベントを記録] オプションを使用してこのイベントを選択します。

これらのイベントに基づいて Novell Audit の通知を作成する方法の詳細については、245 ページのセクション 10.6「イベントに基づく通知の送信」を参照してください。

リモートローダのイベント

次のイベントは、リモートローダからログに記録されます。

表 *10-3* リモートローダのイベント

イベント	ログレベル	情報
リモートローダの起動	LOG_INFO	リモートローダの起動をログに記録するには、[特定のイベントを記録] オプションを使用してこのイベントを選択する必要があります。
リモートローダの停止	LOG_INFO	リモートローダの停止をログに記録するには、[特定のイベントを記録] オプションを使用してこのイベントを選択する必要があります。
リモートローダの接続の確立	LOG_INFO	リモートローダの接続の確立をログに記録するには、[特定のイベントを記録] オプションを使用してこのイベントを選択する必要があります。
リモートローダの接続のドロップ	LOG_INFO	リモートローダの接続のドロップをログに記録するには、[特定のイベントを記録] オプションを使用してこのイベントを選択する必要があります。

これらのイベントに基づいて Novell Audit の通知を作成する方法の詳細については、245 ページのセクション 10.6「イベントに基づく通知の送信」を参照してください。

10.4.2 ユーザ定義イベント

Identity Manager では、独自のイベントログを Novell Audit に設定できます。イベントを記録するには、ポリシービルダまたはスタイルシートにあるアクションを使用します。ポリシーを定義する場合にアクセスできるすべての情報を記録できます。

イベント ID

ユーザ定義イベントには、1000 ～ 1999 のイベント ID が割り当てられます。独自のイベントを定義する場合には、この範囲内の値をイベント ID として指定する必要があります。Novell Audit では、この ID は、Identity Manager アプリケーション ID の 003 に結合されます。

ログレベル

ログレベルを使用して、記録されるイベントのタイプに基づいてイベントをグループ化できます。使用可能な定義済みログレベルは次のとおりです。

表 *10-4* ログレベル

ログレベル	説明
log-emergency	メタディレクトリエンジンまたはドライバがシャットダウンされるイベント。
log-alert	早急に注意が必要なイベント。
log-critical	メタディレクトリエンジンまたはドライバの一部が正常に動作しなくなるイベント。
log-error	メタディレクトリエンジンまたはドライバによって処理できるエラーを示すイベント。
log-warning	大きな問題としては取り上げられないネガティブなイベント。
log-notice	管理者が使い方や操作を理解または向上するのに使用できるポジティブまたはネガティブなイベント。
log-info	何らかの重要性を持つポジティブなイベント。
log-debug	サポート担当者またはエンジニアがメタディレクトリエンジンまたはドライバの操作をデバッグするためのイベント。

ポリシービルダを使用したイベントの生成

ポリシービルダでは、［イベントの生成］アクションを選択することで、イベントが記録されます。

1. イベントが生成されるときに満たす必要がある条件を選択し、［イベントの生成］アクションを選択します。
2. イベント ID を指定します。
3. ログレベルを選択します。
4. ［文字列を入力］フィールドの隣にあるアイコンをクリックして、名前付き文字列ビルダを起動します。

5 名前付き文字列ビルダを使用し、カスタムデータフィールドに対応する名前付き文字列を作成します。

6 [OK] をクリックしてポリシービルダに戻り、ポリシーの続きを作成します。

イベントを記録するようにポリシーを設定する方法の詳細については、『*Policy Builder and Driver Customization Guide*』の「"Generate Event"」を参照してください。

ステータスドキュメントを使用したイベントの生成

<xsl:message> 要素を使用してスタイルシートを通じて生成されるステータスドキュメントは、次の表のように指定したステータスドキュメントのレベル属性に対応するイベント ID とともに、Novell Audit に送信されます。

表 *10-5* ステータスドキュメント

ステータスレベル	ステータスイベント ID
成功	EV_LOG_STATUS_SUCCESS (1)
再試行	EV_LOG_STATUS_RETRY (2)
警告	EV_LOG_STATUS_WARNING (3)
エラー	EV_LOG_STATUS_ERROR (4)
致命的エラー	EV_LOG_STATUS_FATAL (5)
ユーザ定義	EV_LOG_STATUS_OTHER (6)

次の例では、EV_LOG_STATUS_ERROR のレベルの、Novell Audit イベント 0x004 および value1=7777 が生成されます。

```
<xsl:message> <status level="error" text1="This would be text1"
value="7777">This data would be in the blob and in text 2, since no
value is specified for text2 in the attributes.</status> </
xsl:message>
```

次の例では、EV_LOG_STATUS_ERROR のレベルの、Novell Audit イベント 0x004 および value1=7778 が生成されます。

```
<xsl:message> <status level="error" text1="This would be text1"
text2="This would be text2" value1="7778">This data would be in the
blob only for this case, since a value for text2 is specified in the
attributes.</status> </xsl:message>
```

10.4.3 eDirectory オブジェクト

この節では、ログデータを格納する、Novell eDirectory の属性について詳しく説明します。これらのオブジェクトは iManager で選択した内容に基づいて自動的に設定されるため、属性を直接変更する必要はありません。

ログに記録する Identity Manager のイベントは、ドライバセットオブジェクトまたはドライバオブジェクトの DirXML-LogEvent 属性に格納されます。属性は複数値整数で、各値はログに記録されるイベント ID を識別します。

イベントをログに記録する前に、エンジンは現在のイベントタイプをこの属性の内容と照合し、イベントをログに記録するかどうかを決定します。

旧バージョンの Identity Manager では、DirXML-DriverTraceLevel 属性を使用してログレベルを設定していました。ログレベルはドライバごとに指定しており、継承はサポートされていませんでした。Identity Manager 2 以降のバージョンでは、ドライバオブジェクトはこの情報をドライバセットオブジェクトから継承できます。ドライバオブジェクトの DirXML-DriverTraceLevel 属性は、ログ設定を決定する際に最優先されます。ドライバオブジェクトに DirXML-DriverTraceLevel 属性が含まれていない場合は、エンジンは親ドライバセットオブジェクトのログ設定を使用します。

10.5 クエリおよびレポート

Novell Audit では、Novell Audit データベースに対してイベントのクエリを実行するため、2 つのツールが用意されています。Novell Audit の iManager プラグイン、および Novell Audit レポート (LReport) です。

Novell Audit iManager プラグインは、Web ベースの JDBC データベースクエリアプリケーションで、ドロップダウンリストとマクロを使用して、クエリをすばやく作成および保存できます。

Novell Audit レポートは、Windows ベースの ODBC 準拠アプリケーションで、SQL クエリステートメントまたは Crystal Decisions Reports を使用し、Oracle および MySQL データストア (または ODBC ドライバをサポートする他のデータベース) に問い合わせることができます。

Novell Audit の iManager プラグインへのアクセス、または Novell Audit レポートの設定を行うには、『*Novell Audit Administration Guide*』の手順に従います。このガイドは、Novell Audit マニュアルの Web サイト (http://www.novell.com/documentation/nsureaudit) で入手できます。

10.5.1 Identity Manager のレポート

Identity Manager で実行される一般的な操作についての情報を簡単に収集するために、Identity Manager では、多数の Crystal Decisions Reports (*.rpt) が用意されています。これらのレポートは、Identity Manager のインストール CD に含まれています。

Novell Audit Report の設定後、これらのレポートは、ユーザが定義したカスタムクエリやレポートとともに実行できます。Novell Audit Report でレポートを使用する方法の詳細については、『*Novell Audit 1.0.3 Administration Guide*』の「Working with Reports in Novell Audit Report (http://www.novell.com/documentation/nsureaudit/nsureaudit/data/alsn2fj.html)」を参照してください。これらのレポートの例については、269 ページの付録 C「Identity Manager のイベントとレポート」の 290 ページのセクション C.11「レポート」を参照してください。

10.5.2 Identity Manager のイベントの表示

1 ［Novell Audit Report Workspace］で［イベント］タブをクリックし、DirXML フォルダを展開します。

このリストには、事前定義済みのすべての Identity Manager イベントが表示されます。リスト内のイベントをダブルクリックし、イベントのプロパティを表示します。

2 Identity Manager イベントのクエリを実行するには、［Workspace (ワークスペース)］でイベントを右クリックし、［Define Query (クエリの定義)］を選択します。

3 ［Query Expert (クエリエキスパート)］が表示されたら、期間を指定し、イベントを確認します。

4 このクエリを実行するには、［Workspace (ワークスペース)］の［Query(クエリ)］タブを選択した後、クエリ名を右クリックして［Run (実行)］を選択します。

クエリは、SQL ステートメントを使用しても作成できます。すべての Identity Manager イベントには、109608 ～ 262144 の 10 進数イベント ID が付けられています。

10.6 イベントに基づく通知の送信

Novell Audit には、特定のイベントが発生した場合、または発生しなかった場合に、通知を送信できる機能があります。1 つまたは複数のイベントと、これらのイベントに含まれる値に基づいて、通知を送信できます。通知は任意のログチャネルに送信できるため、データベース、Java アプリケーションまたは SNMP 管理システム、あるいは他の複数の場所にログを記録できます。

通知の作成の詳細については、『*Novell Audit 1.0.3 Administration Guide*』の「Configuring Filters and Event Notifications (http://www.novell.com/documentation/nsureaudit/nsureaudit/data/al0lg08.html#al0lg08)」を参照してください。

10.7 ステータスログの使用

Novell Audit で提供される機能に加え、Identity Manager は、ドラバセットオブジェクトまたはドライバセットに対して指定した数のイベントを記録します。これらのステータスログには、Identity Manager の現在のアクティビティが示されます。ログが設定サイズに達すると、新しいイベントを記録するスペースを確保するために、ログの古い方の半分は削除されます。このため、長期間追跡したいイベントは、Novell Audit またはレポートと通知サービス (RNS) で記録することをお勧めします。

10.7.1 最大ログサイズの設定

ステータスログは、50 ～ 500 のイベントを保存するよう設定できます。この設定は、ドライバセットオブジェクトに設定してセット内のすべてのドライバで継承することも、セット内のドライバごとに設定することもできます。最大ログサイズは、ログ対象として選択したイベントとは関係なく機能するので、記録するイベントをドライバセットに設定した後、セット内の各ドライバにそれぞれ異なるログサイズを指定できます。

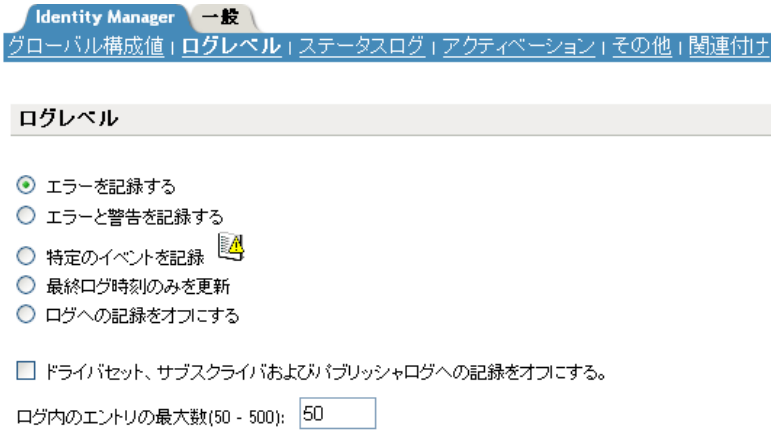
ドラバセットへのログサイズの設定

1 iManager で、［Identity Manager］>［Identity Manager の概要］の順に選択し、［次へ］をクリックします。

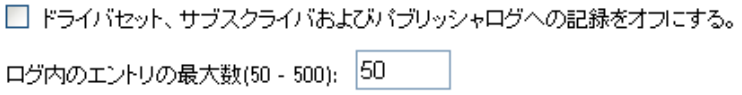
2 ドライバセットオブジェクトを参照して選択し、［検索］をクリックします。

3 ドライバセット名をクリックします。［オブジェクトの変更］ウィンドウが表示されます。

4 ［Identity Manager］タブの［ログレベル］を選択します。



5 ［ログ内のエントリの最大数］フィールドで、最大ログサイズを指定します。



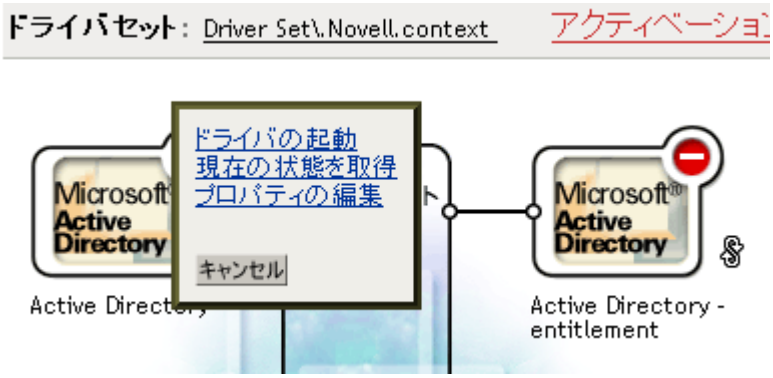
6 最大値を指定したら、［OK］をクリックします。

ドライバへのログサイズの設定

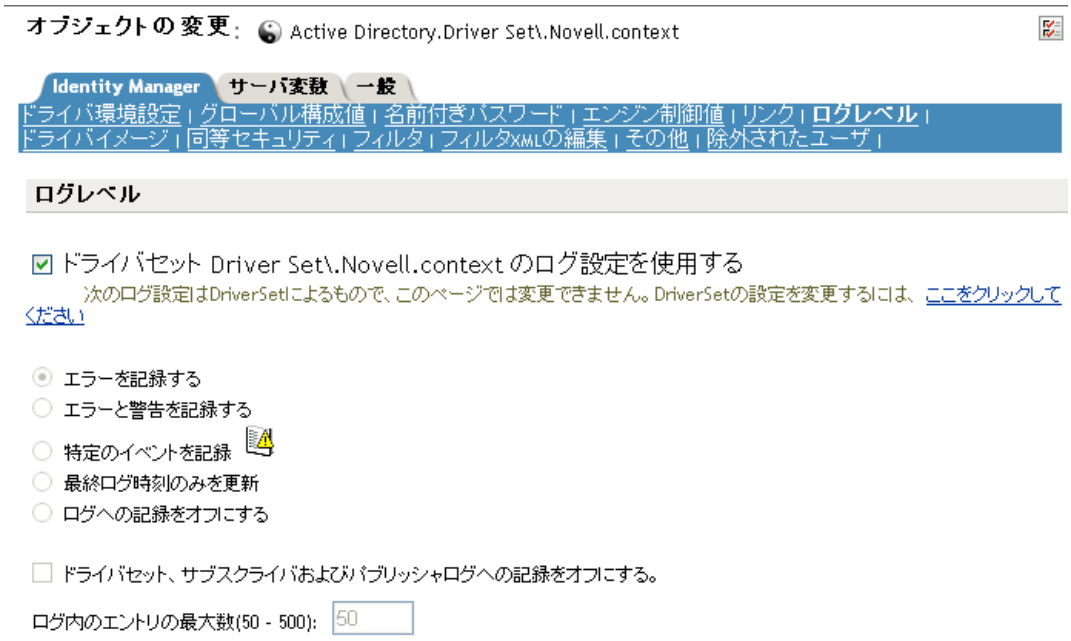
1 iManager で、［Identity Manager］>［Identity Manager の概要］の順に選択し、［次へ］をクリックします。

2 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。

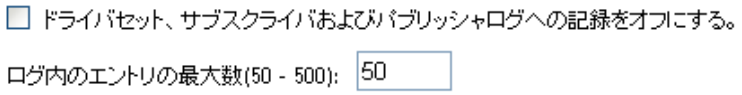
3 ドライバアイコンの右上隅をクリックし、［プロパティの編集］を選択します。



4 ［Identity Manager］タブの［ログレベル］を選択します。



5 ［ログ内のエントリの最大数］フィールドで、最大ログサイズを指定します。



6 最大値を指定したら、［OK］をクリックします。

10.7.2 ステータスログの表示

ステータスログエントリは、iManager ではステータスログアイコン  で表示されます。iManager でこのアイコンが表示されるときは、短期間のログを表示できます。次のステータスログを使用できます。

- ドライバセット
- セット内の各ドライバの発行者チャネル
- セット内の各ドライバの購読者チャネル

発行者チャネルおよび購読者チャネルのステータスログは、関連付けられていないオブジェクトに対する操作拒否など、ドライバにより生成されるチャネル固有のメッセージをレポートします。

ドライバセットのステータスログには、ドライバセットにあるドライバの状態の変化など、エンジンにより生成されるメッセージだけが含まれます。エンジンメッセージはすべてログに記録されます。

DirXML コマンドラインユーティリティ

A

このユーティリティとスクリプトは、すべてのプラットフォームで Identity Manager のインストール中にインストールされます。このユーティリティは次の場所にインストールされます。

- Windows: \Novell\Nds\dxcmd.bat
- NetWare: sys:\system\dxcmd.ncf
- UNIX: /usr/bin/dxcmd

DirXML コマンドラインユーティリティの使用方法には、次の 2 つがあります。

- 249 ページのセクション A.1「対話モード」
- 257 ページのセクション A.2「コマンドラインモード」

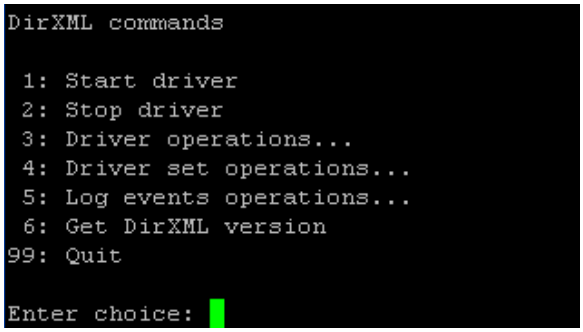
A.1 対話モード

対話モードには、DirXML コマンドラインユーティリティを制御および使用するためのテキストインタフェースが用意されています。

1. コンソールで、「dxcmd」と入力します。
2. Identity Manager オブジェクトに対する十分な権利を持つユーザの名前を入力します。

   例 : admin.novell
3. 上記で指定したユーザのパスワードを入力します。

   例 : novell



4. 実行するコマンドの番号を入力します。

   250 ページの 表 A-1 はオプションの一覧で、使用できる機能を示しています。
5. ユーティリティを終了するには、「99」と入力します。

注 **:** Unix または Linux で eDirectory™ 8.8 を実行している場合、-host および -port パラメータを指定する必要があります。たとえば、「dxcmd -host 10.0.0.1 -port 524」などです。パラメータを指定しない場合、jclient エラーが発生します。

```
novell.jclient.JCException:connect (to address) 111 UNKNOWN ERROR
```

デフォルトでは、eDirectory 8.8 はローカルホストをリッスンしません。DirXML コマンドラインユーティリティは、サーバの IP アドレスやホスト名、および認証可能なポートを解決する必要があります。

表 *A-1* 対話モードのオプション

オプション	説明
1: *Start Driver*	ドライバを起動します。複数のドライバがある場合、各ドライバは番号付きで一覧表示されます。起動するドライバの番号を入力します。
2: *Stop Driver*	ドライバを停止します。複数のドライバがある場合、各ドライバは番号付きで一覧表示されます。停止するドライバの番号を入力します。
3: *Driver operations*	ドライバに対して実行可能な操作が一覧表示されます。複数のドライバがある場合、各ドライバは番号付きで一覧表示されます。実行可能な操作を表示するドライバの番号を入力します。実行可能な操作については、251 ページの 表 A-2 を参照してください。
4: *Driver set operations*	ドライバセットに対して実行可能な操作が一覧表示されます。 • 1: ドライバセットをサーバと関連付けます • 2: ドライバセットのサーバとの関連付けを解除します • 99: 終了します
5: *Log events operations*	Novell Audit を介したイベントのログに対する実行可能な操作を一覧表示します。これらのオプションの詳細については、255 ページの 表 A-5 を参照してください。
6: *Get DirXML version*	インストールされた Identity Manager のバージョンを一覧表示します。
99: *Quit*	DirXML コマンドラインユーティリティを終了します。

図 *A-1* ドライバオプション

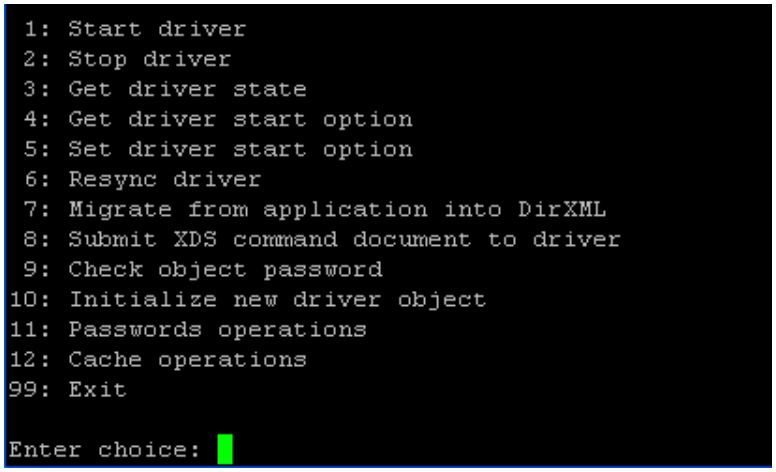


表 *A-2* ドライバオプション

オプション	説明
1: *Start driver*	ドライバを起動します。
2: *Stop driver*	ドライバを停止します。
3: *Get driver state*	ドライバの状態を一覧表示します。 ◆ 0 - ドライバは停止中です ◆ 1 - ドライバを起動しています ◆ 2 - ドライバは実行中です ◆ 3 – ドライバを停止しています
4: *Get driver start option*	現在のドライバの起動オプションを一覧表示します。 ◆ 1 – 使用不可 ◆ 2 – 手動 ◆ 3 – 自動
5: *Set driver start option*	ドライバの起動オプションを変更します。 ◆ 1 – 使用不可 ◆ 2 – 手動 ◆ 3 – 自動 ◆ 99 – 終了
6: *Resync driver*	ドライバの再同期を強制します。時間の遅延に関するプロンプトが次のように表示されます:*Do you want to specify a minimum time for resync?(yes/no):* 「yes」と入力した場合、再同期を実行する日付と時刻を入力します。日付または時刻を入力してください (形式 : 9/27/05 3:27 PM)。 「no」と入力した場合、再同期がすぐに実行されます。
7: *Migrate from application into DirXML*	クエリコマンドが含まれている XML ドキュメントを処理します : XDS クエリドキュメントのファイル名を入力します : Novell nds.dtd (http://developer.novell.com/ndk/doc/dirxml/dirxmlbk/ref/ndsdtd/query.html) を使用して、クエリコマンドが含まれている XML ドキュメントを作成します。 例 : NetWare: sys:\files\query.xml Windows:c:\files\query.xml Linux: /files/query.xml

オプション	説明
8: *Submit XDS command document to driver*	XDS コマンドドキュメントを処理します : XDS コマンドドキュメントのファイル名を入力します : 例 : NetWare: sys:\files\user.xml Windows:c:\files\user.xml Linux: /files/user.xml 応答のファイル名を入力します : 例 : NetWare: sys:\files\user.log Windows:c:\files\user.log Linux: /files/user.log
9: *Check object password*	ドライバに関連付けられた接続システム内のオブジェクトのパスワードを検証します。このパスワードは、オブジェクトの eDirectory パスワード (ユニバーサルパスワードとともに使用される配布パスワード) に一致します。 ユーザ名を入力します :
10: *Initialize new driver object*	新しいドライバオブジェクト上のデータを内部的に初期化します。このオプションはテスト用です。
11: *Password operations*	パスワードオプションは 9 種類あります。これらのオプションの詳細については、253 ページの 表 A-3 を参照してください。
12: *Cache operations*	キャッシュ操作は 5 種類あります。これらのオプションの詳細については、254 ページの 表 A-4 を参照してください。
99: *Exit*	ドライバオプションを終了します。

図 *A-2* パスワード操作

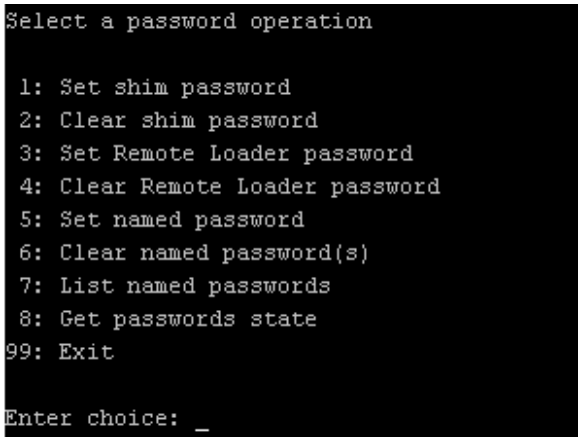


表 *A-3* パスワード操作

操作	説明
1: *Set shim password*	アプリケーションパスワードを設定します。これは、接続システムへの認証に使用しているユーザアカウントのパスワードです。
2: *Clear shim password*	アプリケーションパスワードをクリアします。
3: *Set Remote Loader password*	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。詳細については、43 ページの第 3 章「接続システムの設定」を参照してください。 リモートローダのパスワードを入力し、次にパスワードを再度入力して確認します。
4: *Clear Remote Loader password*	リモートローダのパスワードをクリアし、ドライバオブジェクトでリモートローダのパスワードが設定されていない状態にします。
5: *Set named password*	パスワードまたはその他のセキュリティ情報をドライバに保存できます。詳細については、27 ページのセクション 2.9「名前付きパスワードの使用」を参照してください。 次の 4 つのプロンプトで入力します。 ◆ パスワード名を入力します : ◆ パスワードの説明を入力します : ◆ パスワードの入力 : ◆ パスワードの確認

操作	説明
6: *Clear named passwords*	指定した名前付きパスワード、またはドライバオブジェクトに保存されているすべての名前付きパスワードをクリアします : すべての名前付きパスワードをクリアしますか ? (yes/no) 「yes」と入力した場合、すべての名前付きパスワードがクリアされます。「no」と入力した場合、クリアするパスワード名を指定するよう要求されます。
7: *List named passwords*	ドライバオブジェクトに保存されているすべての名前付きパスワードを一覧表示します。パスワード名およびパスワードの説明が一覧表示されます。
8: *Get password state*	次に対してパスワードが設定されている場合、一覧表示します。 ◆ ドライバオブジェクトパスワード : ◆ アプリケーションのパスワード : ◆ リモートローダパスワード : dxcmd ユーティリティを使用すると、アプリケーションのパスワードおよびリモートローダのパスワードを設定できます。このユーティリティでは、ドライバオブジェクトのパスワードは設定できません。これらが設定されているかいないかが表示されます。
99: *Exit*	現在のメニューを終了し、ドライバオプションに戻ります。

図 *A-3* キャッシュ操作

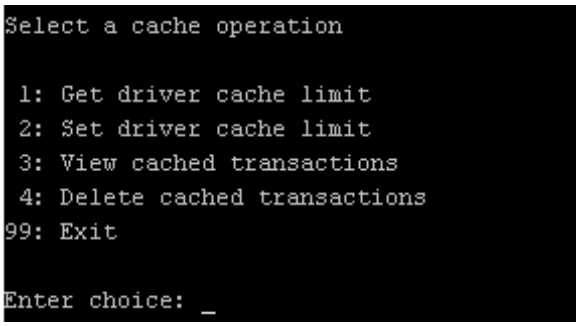


表 *A-4* キャッシュ操作

操作	説明
1: *Get driver cache limit*	ドライバに設定されている現在のキャッシュの制限を表示します。
2: *Set driver cache limit*	ドライバのキャッシュの制限をキロバイトで設定します。値 0 は無制限を意味します。

操作	説明
3: *View cached transactions*	キャッシュに保存されたイベントを使用してテキストファイルが作成されます。表示するトランザクションの数を選択できます。 ◆ オプショントークンを入力します(デフォルト =0): ◆ 返される最大のトランザクションレコードを入力します (デフォルト =1): ◆ 応答のファイル名を入力します :
4: *Delete cached transactions*	キャッシュに保存されているトランザクションを削除します。 ◆ 位置トークンを入力します (デフォルト =0): ◆ 削除する最初のトランザクションのイベント ID 値を入力します (オプション): ◆ 削除するトランザクションレコード数を入力します (デフォルト =1)。
99: *Exit*	現在のメニューを終了し、ドライバオプションに戻ります。

図 *A-4* ログイベントの操作

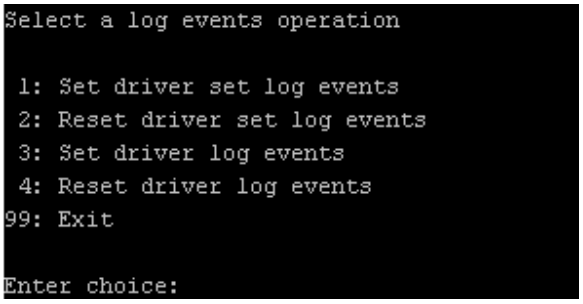


表 *A-5* ログイベントの操作

操作	説明
1: *Set driver set log events*	Novell Audit を介してドライバセットイベントをログに記録できるようにします。ログ記録の対象は 49 項目から選択できます。これらのオプションのリストについては、256 ページの 表 A-6 を参照してください。 ログに記録する項目の番号を入力します。項目を選択したら、「99」と入力して選択を受諾します。
2: *Reset driver set log events*	すべてのログイベントのオプションをリセットします。

操作	説明
3: *Set driver log events*	Novell Audit を介してドライバイベントをログに記録できるようにします。ログ記録の対象は 49 項目から選択できます。これらのオプションのリストについては、256 ページの 表 A-6 を参照してください。 ログに記録する項目の番号を入力します。項目を選択したら、「99」と入力して選択を受諾します。
4: *Reset driver log events*	すべてのログイベントのオプションをリセットします。
99: *Exit*	ログイベント操作のメニューを終了します。

表 *A-6* ドライバセットおよびドライバのログイベント

オプション
1: Status success
2: Status retry
3: Status warning
4: Status error
5: Status fatal
6: Status other
7: Query elements
8: Add elements
9: Remove elements
10: Modify elements
11: Rename elements
12: Move elements
13: Add-association elements
14: Remove-association elements
15: Query-schema elements
16: Check-password elements
17: Check-object-password elements
18: Modify-password elements
19: Sync elements
20: Pre-transformed XDS document from shim
21: Post input transformation XDS document
22: Post output transformation XDS document

オプション
23: Post event transformation XDS document
24: Post placement transformation XDS document
25: Post create transformation XDS document
26: Post mapping transformation <inbound> XDS document
27: Post mapping transformation <outbound> XDS document
28: Post matching transformation XDS document
29: Post command transformation XDS document
30: Post-filtered XDS document <Publisher>
31: User agent XDS command document
32: Driver resync request
33: Driver migrate from application
34: Driver start
35: Driver stop
36: Password sync
37: Password request
38: Engine error
39: Engine warning
40: Add attribute
41: Clear attribute
42: Add value
43: Remove value
44: Merge entire
45: Get named password
46: Unknown
47: Unknown
48: User defined IDs
99: Accept checked items

A.2 コマンドラインモード

コマンドラインモードを使用すると、スクリプトまたはバッチファイルを使用できます。258 ページの 表 A-7 では、使用可能なさまざまなオプション示しています。

コマンドラインオプションを使用するには、使用するオプションを選択し、これらを続けて入力します。

例 : dxcmd -user admin.headquarters -host 10.0.0.1 -password n0vell -start test.driverset.headquarters

コマンドにより、ドライバが起動します。

表 *A-7* コマンドラインオプション

オプション	説明
環境設定	
-user < ユーザ名 >	テストするドライバに対して管理者権限を持つユーザの名前を指定します。
-host < 名前または IP アドレス >	ドライバがインストールされているサーバの IP アドレスを指定します。
-password < ユーザのパスワード >	上記で指定したユーザのパスワードを入力します。
-port < ポート番号 >	ポート番号は、デフォルトのポートが使用されていない場合に指定します。
-q < クワイエットモード >	コマンドが実行されているときに最小限の情報を表示します。
-v < 詳細モード >	コマンドが実行されているときに詳しい情報を表示します。
-? < このメッセージを表示 >	ヘルプメニューを表示します。
-help < このメッセージを表示 >	ヘルプメニューを表示します。
アクション	
-start < ドライバ dn>	ドライバを起動します。
-stop < ドライバ dn>	ドライバを停止します。
-getstate < ドライバ dn>	実行されているドライバまたは停止したドライバの状態を表示します。
-getstartoption < ドライバ dn>	ドライバの起動オプションを表示します。
-setstartoption < ドライバ dn> *<disabled|manual|auto>* *<resync|noresync>*	サーバが再起動した場合に、ドライバをどのように起動するのかを設定します。ドライバが再起動したときに、オブジェクトが再同期されるのかどうかを設定します。
-getcachelimit < ドライバ dn>	ドライバに対して設定されたキャッシュの制限を一覧表示します。
-setcachelimit < ドライバ dn> <0 または正の整数 >	ドライバのキャッシュの制限を設定します。
-migrateapp < ドライバ dn> < ファイル名 >	クエリコマンドが含まれている XML ドキュメントを処理します。 Novell nds.dtd (http://developer.novell.com/ndk/doc/dirxml/dirxmlbk/ref/ndsdtd/query.html) を使用して、クエリコマンドが含まれている XML ドキュメントを作成します。

オプション	説明
-setshimpassword < ドライバ dn> < パスワード >	アプリケーションパスワードを設定します。これは、接続システムへの認証に使用しているユーザアカウントのパスワードです。
-clearshimpassword < ドライバ dn> < パスワード >	アプリケーションパスワードをクリアします。
-setremoteloaderpassword < ドライバ dn> < パスワード >	リモートローダのパスワードを設定します。 リモートローダインスタンスへのアクセスを制御するために、リモートローダのパスワードが使用されます。詳細については、43 ページの第 3 章「接続システムの設定」を参照してください。
<clearremoteloaderpassword < ドライバ dn>	リモートローダのパスワードをクリアします。
-sendcommand < ドライバ dn> < 入力ファイル名 > < 出力ファイル名 >	XDS コマンドドキュメントを処理します。 入力ファイルとして、XDS コマンドドキュメントを指定します。 例 : NetWare: sys:\files\user.xml Windows:c:\files\user.xml Linux: /files/user.log 結果を表示するための出力ファイル名を指定します。 例 : NetWare: sys:\files\user.log Windows:c:\files\user.log Linux: /files/user.log
-setlogevents <dn> < 整数 ...>	ドライバ上の Novell Audit ログイベントを設定します。整数は、ログに記録する項目のオプションです。入力する整数のリストについては、256 ページの 表 A-6 を参照してください。
-clearlogevents <dn>	ドライバ上に設定されているすべての Novell Audit ログイベントをクリアします。
-setdriverset < ドライバセット dn>	ドライバセットをサーバに関連付けます。
-cleardriverset	ドライバセットの関連付けをサーバからクリアします。
-getversion	インストールされた Identity Manager のバージョンを表示します。
-initdriver object <dn>	新しいドライバオブジェクト上のデータを内部的に初期化します。このオプションはテスト用です。
-setnamedpassword < ドライバ dn> < 名前 > < パスワード > [説明]	ドライバオブジェクトの名前付きパスワードを設定します。名前付きパスワードの名前、パスワード、および説明を指定します。

オプション	説明
-clearnamedpassword < ドライバ dn> < 名前 >	指定した名前付きパスワードをクリアします。
-clearallnamedpaswords < ドライバ dn>	特定のドライバ上のすべての名前付きパスワード設定をクリアします。

リモートローダの設定オプション

B

リモートローダは、次の表のオプションによって設定できます。

表 *B-1* リモートローダのオプション

オプション	2 次名	パラメータ	説明
address		IP アドレス	オプションのパラメータ。リモートローダが特定のローカル IP アドレスをリッスンするよう指定します。これは、リモートローダをホストするサーバが複数の IP アドレスを持ち、リモートローダが 1 つのアドレスのみをリッスンしなければならない場合に便利です。 次の 3 つの方法があります。address= アドレス番号 address='localhost' このパラメータを使用しない。 -address を使用しない場合、リモートローダはすべてのローカル IP アドレスをリッスンします。 例 : address=137.65.134.83
-class	-cl	Java クラス名	ホストする Identity Manager アプリケーションシムの Java クラス名を指定します。 たとえば、Java ドライバに対しては次のいずれかを入力します。 -class com.novell.nds.dirxml.driver.ldap.LDAPDriverShim -cl com.novell.nds.dirxml.driver.ldap.LDAPDriverShim Java では、キーストアを使用して証明書を読み取ります。-class オプションと -module オプションは排他的で、どちらか一方を使用できます。 Java クラス名のリストを表示するには、268 ページの 表 B-2 を参照してください。

オプション	2 次名	パラメータ	説明
-commandport	-cp	ポート番号	リモートローダインスタンスが制御目的で使用する TCP/IP ポートを指定します。リモートローダインスタンスがアプリケーションシムをホストしている場合、コマンドポートは、別のリモートローダインスタンスが、シムをホストしているインスタンスと通信するポートになります。リモートローダインスタンスが、アプリケーションシムをホストしているインスタンスにコマンドを送信する場合、コマンドポートは管理インスタンスがリッスンしているポートになります。コマンドポートが指定されていない場合のデフォルトポートは 8000 です。複数の接続ポートとコマンドポートを指定することで、異なるドライバインスタンスをホストしている同じサーバ上でリモートローダの複数のインスタンスを実行できます。 例 : -commandport 8001 -cp 8001
-config	なし	ファイル名	環境設定ファイルを指定します。環境設定ファイルには、config 以外のあらゆるコマンドラインオプションを含めることができます。コマンドラインで指定したオプションは、環境設定ファイル内で指定されたオプションよりも優先されます。 例 : -config config.txt
-connection	-conn	接続設定文字列	Identity Manager リモートインタフェースシムを実行しているメタディレクトリサーバに接続するための接続パラメータを指定します。リモートローダのデフォルトの接続方法は、SSL を使用した TCP/IP です。この接続のデフォルトの TCP/IP ポートは 8090 です。リモートローダの複数のインスタンスを同じサーバ上で実行できます。リモートローダの各インスタンスは別々の Identity Manager アプリケーションシムインスタンスをホストします。リモートローダの各インスタンスに別々の接続ポートとコマンドポートを指定することによって、リモートローダの複数のインスタンスを区別します。 例 : -connection "port=8091 rootfile=server1.pem" -conn "port=8091 rootfile=server1.pem"

オプション	2 次名	パラメータ	説明
-description	-desc	短い説明	トレースウィンドウのタイトルと Novell® Audit のログに使用される短い説明の文字列 (SAP など) を指定します。 例 : -description SAP -desc SAP 環境設定ファイルには、リモートローダコンソールによって長い形式が配置されます。長い形式 (たとえば -description) または短い形式 (たとえば -desc) のいずれかを使用できます。
-help	-?	なし	ヘルプを表示します。 例 : -help -?
-java	-j	なし	Java シムインスタンスに設定されるパスワードを指定します。このオプションは、setpasswords オプションとともに使用した場合にのみ有効です。-class を -setpasswords とともに指定した場合、このオプションは不要です。
-javadebugport	-jdp	ポート番号	指定されたポートでリモートローダインスタンスが Java デバッグを有効にするよう指定します。これは Identity Manager アプリケーションシムの開発者向けの設定です。 例 : -javadebugport 8080 -jdp 8080
keystore			条件付きパラメータ。.jar ファイルに含まれる Identity Manager アプリケーションシムにのみ使用します。 リモートインタフェースシムによって使用される証明書の発行者のルート認証局証明書を含む Java キーストアのファイル名を指定します。通常、これはリモートインタフェースシムをホストしている eDirectory™ ツリーの認証局です。 SSL を実行していて、リモートローダが Java ドライバと通信する必要がある場合、次の key-value ペアを入力します。 keystore=' キーストア名 ' storepass=' パスワード '

オプション	2 次名	パラメータ	説明
-module	-m	モジュール名	ホストする Identity Manager アプリケーションシムを含むモジュールを指定します。 たとえば、ネイティブドライバに対しては次のいずれかを入力します。 -module "c:\Novell\RemoteLoader\Exchange5Shim.dll" -m "c:\Novell\RemoteLoader\Exchange5Shim.dll" または -module "usr/lib/dirxml/NISDriverShim.so" -m "usr/lib/dirxml/NISDriverShim.so" -module オプションでは、ルートファイル証明書が使用されます。-module オプションと -class オプションは排他的で、どちらか一方を使用できます。
-password	-p	パスワード	コマンド認証のパスワードを指定します。このパスワードは、コマンドの発行先のローダインスタンスの setpasswords で指定した最初のパスワードと同じパスワードにする必要があります。コマンドオプション (unload や tracechange など) を指定し、**password** オプションを指定しないと、コマンドの対象となるローダのパスワードを入力するように要求するメッセージが表示されます。 例 : -password novell4 -p novell4
port		10 進数のポート番号	必須パラメータ。リモートローダがリモートインタフェースシムからの接続をリッスンする TCP/IP ポートを指定します。 例 : port=8090
rootfile			条件付きパラメータ。SSL を実行していて、リモートローダがネイティブドライバと通信する必要がある場合、次を入力します。 rootfile=' 信頼できる証明書名 '

オプション	2 次名	パラメータ	説明
-service	-serv	なし、または install/uninstall	インスタンスをサービスとしてインストールするには、アプリケーションシムをホストするために必要なその他の引数とともに引数 install を使用します。たとえば、使用する引数には -module を含める必要がありますが、どの引数にも -connection、- commandport などを含めることができます。 このオプションを指定すると、Win32 サービスがインストールされますが、サービスは起動されません。 サービスとして実行されているインスタンスをアンインストールするには、アプリケーションシムをホストするために必要なその他の引数とともに引数 uninstall を使用します。 このオプションの引数なしのバージョンは、Win32 サービスとして実行されるインスタンスへのコマンドライン内でのみ使用します。これはインスタンスをサービスとしてインストールする際に自動的に設定されます。 例 : -service install -serv uninstall このオプションは rdxml または Java リモートローダでは使用できません。
-setpasswords	-sp	パスワード パスワード	リモートローダインスタンスのパスワード、およびリモートローダが通信するリモートインタフェースシムの Identity Manager ドライバオブジェクトのパスワードを指定します。引数の最初のパスワードは、リモートローダのパスワードです。オプション引数の 2 番目のパスワードは、メタディレクトリサーバのリモートインタフェースシムに関連付けられた Identity Manage ドライバオブジェクトのパスワードです。どちらのパスワードも指定しないか、または両方のパスワードを指定する必要があります。パスワードを指定しないと、リモートローダはパスワードを要求するメッセージを表示します。これは環境設定オプションです。このオプションを使用すると、指定したパスワードがリモートローダのインスタンスに設定されますが、Identity Manager アプリケーションシムはロードされず、ローダの別のインスタンスとも通信しません。 例 : -setpasswords novell4 staccato3 -sp novell4 staccato3

オプション	2 次名	パラメータ	説明
-storepass		キーストアのパスワード	.jar ファイルに含まれる Identity Manager アプリケーションシムにのみ使用します。keystore パラメータで指定した Java キーストアのパスワードを指定します。 例 : storepass=mypassword このオプションは Java リモートローダにのみ適用されます。
-trace	-t	整数	トレースレベルを指定します。これはアプリケーションシムをホストする場合にのみ使用できます。トレースレベルはメタディレクトリサーバで使用されているレベルと同じです。 例 : -trace 3 -t 3
-tracechange	-tc	整数	アプリケーションシムをホストしているリモートローダのインスタンスに、そのトレースレベルを変更するように命令します。トレースレベルはメタディレクトリサーバで使用されているレベルと同じです。 例 : -tracechange 1 -tc 1
-tracefile	-tf	ファイル名	トレースメッセージを書き込むファイルを指定します。トレースメッセージは、トレースレベルがゼロよりも大きい場合にファイルに書き込まれます。トレースメッセージは、トレースウィンドウが開いていなくてもファイルに書き込まれます。 例 : -tracefile c:\temp\trace.txt -tf c:\temp\trace.txt
-tracefilechange	-tfc	なし、またはファイル名	アプリケーションシムをホストしているリモートローダのインスタンスに対し、トレースファイルを使用して起動するように命令するか、またはすでに使用しているファイルを閉じて新しいファイルを使用するように命令します。このオプションを引数なしで使用すると、ホストインスタンスは使用中のすべてのトレースファイルを閉じます。 例 : -tracefilechange c:\temp\newtrace.txt tfc c:\temp\newtrace.txt

オプション	2 次名	パラメータ	説明
-tracefilemax	-tfm	サイズ	トレースファイルがディスク上で使用できる最大サイズを指定します。このオプションを指定すると、tracefile オプションを使用して指定した名前の付いたトレースファイルと、最大 9 個の追加ロールオーバファイルが生成されます。ロールオーバファイルには、メインのトレースファイル名と「"_*n*"」に基づいた名前が付けられます。「n」は 1 ～ 9 の値になります。 サイズのパラメータはバイト数です。K (キロバイト)、M (メガバイト)、または G (ギガバイト) のサフィックスを使用してサイズを指定します。 リモートローダの起動時にトレースファイルのデータが指定した最大サイズよりも大きい場合、10 ファイルすべてのロールオーバが完了するまで、トレースファイルのデータは指定した最大値よりも大きいままになります。 例 : -tracefilemax 1000M -tfm 1000M この例では、トレースファイルの最大サイズは 1GB です。
-unload	-u	なし	リモートローダインスタンスをアンロードします。リモートローダが Win32 サービスとして実行されている場合、このコマンドはサービスを停止します。 例 : -unload -u
-window	-w	On/Off	リモートローダインスタンスでトレースウィンドウのオン / オフを切り替えます 例 : -window on -w off このオプションは Windows プラットフォームのみで使用可能です。Java リモートローダでは使用できません。

オプション	2 次名	パラメータ	説明
-wizard	-wiz	なし	環境設定ウィザードを起動します。このウィザードは、コマンドラインパラメータを指定せずに dirxml_remote.exe を実行しても起動します。このオプションは、環境設定ファイルも指定されている場合に便利です。この場合、ウィザードは環境設定ファイルの値を使用して起動するので、環境設定ファイルを直接編集しなくてもウィザードから設定を変更できます。 例 : -wizard -wiz このオプションは Windows プラットフォームのみで使用可能です。Java リモートローダでは使用できません。

表 *B-2* *Java* クラス名

Java クラス名	ドライバ
com.novell.nds.dirxml.driver.avaya.PBXDriverShim	Avaya PBX ドライバ
com.novell.nds.dirxml.driver.delimitedtext.DelimitedTextDriver	区切りテキストドライバ
com.novell.nds.dirxml.driver.nds.DriverShimImpl	eDirectory ドライバ
com.novell.nds.dirxml.driver.entitlement.EntitlementServiceDriver	エンタイトルメントサービスドライバ
com.novell.gw.dirxml.driver.gw.GWdriverShim	GroupWise ドライバ
com.novell.nds.dirxml.jdbc.JDBCDriverShim	JDBC ドライバ
com.novell.nds.dirxml.driver.ldap.LDAPDriverShim	LDAP ドライバ
com.novell.nds.dirxml.driver.loopback.LoopbackDriverShim	ループバックドライバ
com.novell.nds.dirxml.driver.manualtask.driver.ManualTaskDriver	手動タスクドライバ
com.novell.nds.dirxml.driver.nisdriver.NISDriverShim	NIS ドライバ
com.novell.nds.dirxml.driver.notes.NotesDriverShim	Notes ドライバ
com.novell.nds.dirxml.driver.psoftshim.PSOFTDriverShim	PeopleSoft ドライバ
com.novell.nds.dirxml.driver.SAPShim.SAPDriverShim	SAP HR ドライバ
com.novell.nds.dirxml.driver.sapusershim.SAPDriverShim	SAP ユーザ管理ドライバ
com.novell.nds.dirxml.driver.sifagent.SIFShim	SIF ドライバ
com.novell.nds.dirxml.driver.soap.SOAPDriver	Soap ドライバ
com.novell.idm.driver.ComposerDriverShim	ユーザアプリケーション
be.opns.dirxml.driver.ars.arsremedydrivershim.ARSDriverShim	Remedy ARS 用ドライバ

Identity Manager のイベントとレポート

C

この節では、Identity Manager によって記録されるすべての Novell® Audit イベントを一覧にしています。また、Novel Audit で実行できるレポートの例も示します。レポートの例は、290 ページのセクション C.11「レポート」にあります。

各イベントには、次の情報が保存されています。イベント ID、説明、オリジネータタイトル、ターゲットタイトル、サブターゲットタイトル、Text1 タイトル、Text2 タイトル、Text3 タイトル、Value1 タイトル、Value1 タイプ、Value2 タイトル、Value2 タイプ、Value3 タイトル、Value3 タイプ、グループタイトル、グループタイプ、データタイトル、データタイプ、表示スキーマ。

次のコンポーネントのイベントを表で示します。

C.1 エンジンイベント

次の表は、Novell Audit を介して監査できるエンジンイベントの一覧です。

表 *C-1* エンジンイベントのフィールド : オリジネータタイトル、ターゲットタイトル、およびサブターゲットタイトル

イベント ID	説明	オリジネータタイトル	ターゲットタイトル	サブターゲットタイトル
30001	ステータスは成功です	チャネル	src-dn (dest-dn)	レベル
30002	ステータスは再試行です	チャネル	src-dn (dest-dn)	レベル
30003	ステータスは警告です	チャネル	src-dn (dest-dn)	レベル
30004	ステータスがエラーです	チャネル	src-dn (dest-dn)	レベル

イベント ID	説明	オリジネータタイトル	ターゲットタイトル	サブターゲットタイトル
30005	ステータスは致命的です	チャネル	src-dn (dest-dn)	レベル
30006	ステータスはその他です	チャネル	src-dn (dest-dn)	レベル
30007	検索	チャネル	dest-dn または関連付け	スコープ
30008	エントリの追加	チャネル	dest-dn または関連付け	属性名
30009	エントリの削除	チャネル	dest-dn または関連付け	属性名
3000A	エントリの変更	チャネル	dest-dn または関連付け	属性名
3000B	エントリの名前変更	チャネル	dest-dn または関連付け	オブジェクトタイプ
3000C	エントリの移動	チャネル	dest-dn または関連付け	ターゲットの移動
3000D	関連付けの追加	チャネル	dest-dn	属性名
3000E	関連付けを削除	チャネル		属性名
3000F	クエリースキーマ	チャネル		
30010	パスワードの確認	チャネル	ドライバ	
30011	オブジェクトパスワードの確認	チャネル	dest-dn または関連付け	
30012	パスワードの変更	チャネル	dest-dn または関連付け	
30013	同期	チャネル	dest-dn または関連付け	属性名
30014	XML ドキュメントの入力	チャネル		属性名
30015	入力変換ドキュメント	チャネル		
30016	出力変換ドキュメント	チャネル		
30017	イベント変換ドキュメント	チャネル		
30018	配置ルール変換ドキュメント	チャネル		
30019	作成ルール変換ドキュメント	チャネル		
3001A	入力マッピングルール変換ドキュメント	チャネル		
3001B	出力マッピングルール変換ドキュメント	チャネル		

イベント ID	説明	オリジネータタイトル	ターゲットタイトル	サブターゲットタイトル
3001C	一致ルール変換ドキュメント	チャネル		
3001D	コマンド変換ドキュメント	チャネル		
3001E	発行者フィルタ変換ドキュメント	チャネル		
3001F	ユーザエージェント要求	チャネル		
30020	再同期ドライバ	チャネル	ドライバ	
30021	移行	チャネル	関連付け	属性名
30022	ドライバの起動	ドライバセット	ドライバ	
30023	ドライバの停止	ドライバの停止	ドライバ	
30024	Password Sync	チャネル	オブジェクト	属性名
30025	パスワードのリセット	チャネル	dest-dn または関連付け	属性名
30026	DirXML のエラー	チャネル	オブジェクト	
30027	DirXML の警告	チャネル	オブジェクト	
30028	カスタム操作	チャネル		
30029	属性のクリア	チャネル	dest-dn または関連付け	属性名
3002A	値の追加 - エントリの変更	チャネル	dest-dn または関連付け	属性名
3002B	値の削除	チャネル	dest-dn または関連付け	属性名
3002C	エントリのマージ	チャネル	オブジェクト	属性名
3002D	名前付きパスワードの取得	ドライバまたはチャネル	オブジェクト	
3002E	属性のリセット	チャネル	オブジェクト	チャネル
3002F	値の追加 - エントリの追加	チャネル	dest-dn または関連付け	属性名

表 *C-2* エンジンイベントのフィールド *:Text1* タイトル、*Text2* タイトル、および *Text3* タイトル

イベント ID	説明	Text1 タイトル	Text2 タイトル	Text3 タイトル
30001	ステータスは成功です	Type	ステータスドキュメント	イベント ID
30002	ステータスは再試行です	Type	ステータスドキュメント	イベント ID

イベント ID	説明	Text1 タイトル	Text2 タイトル	Text3 タイトル
30003	ステータスは警告です	Type	ステータスドキュメント	イベント ID
30004	ステータスがエラーです	Type	ステータスドキュメント	イベント ID
30005	ステータスは致命的です	Type	ステータスドキュメント	イベント ID
30006	ステータスはその他です	Type	ステータスドキュメント	イベント ID
30007	検索	オブジェクトタイプ		イベント ID
30008	エントリの追加	オブジェクトタイプ	src-dn	イベント ID
30009	エントリの削除	オブジェクトタイプ	src-dn	イベント ID
3000A	エントリの変更	オブジェクトタイプ	src-dn	イベント ID
3000B	エントリの名前変更	新しい名前	src-dn	イベント ID
3000C	エントリの移動	関連付けの移動	src-dn	イベント ID
3000D	関連付けの追加	関連付け		イベント ID
3000E	関連付けを削除	関連付け		イベント ID
3000F	クエリースキーマ			イベント ID
30010	パスワードの確認			
30011	オブジェクトパスワードの確認			イベント ID
30012	パスワードの変更	オブジェクトタイプ	src-dn	イベント ID
30013	同期	オブジェクトタイプ	関連付け	Type
30014	XML ドキュメントの入力			警告メッセージ
30015	入力変換ドキュメント			警告メッセージ
30016	出力変換ドキュメント			警告メッセージ
30017	イベント変換ドキュメント			警告メッセージ
30018	配置ルール変換ドキュメント			警告メッセージ
30019	作成ルール変換ドキュメント			警告メッセージ
3001A	入力マッピングルール変換ドキュメント			警告メッセージ
3001B	出力マッピングルール変換ドキュメント			警告メッセージ
3001C	一致ルール変換ドキュメント			警告メッセージ

イベント ID	説明	Text1 タイトル	Text2 タイトル	Text3 タイトル
3001D	コマンド変換ドキュメント			警告メッセージ
3001E	発行者フィルタ変換ドキュメント			警告メッセージ
3001F	ユーザエージェント要求			
30020	再同期ドライバ			エラーメッセージ
30021	移行	オブジェクトタイプ		警告メッセージ
30022	ドライバの起動			ドライバのメッセージ
30023	ドライバの停止			ドライバのメッセージ
30024	パスワード同期			
30025	パスワードのリセット		src-dn	
30026	DirXML のエラー	エラーメッセージ		
30027	DirXML の警告	警告メッセージ		
30028	カスタム操作			
30029	属性のクリア		src-dn	イベント ID
3002A	値の追加 - エントリの変更	値	src-dn	イベント ID
3002B	値の削除	値	src-dn	イベント ID
3002C	エントリのマージ	オブジェクトタイプ	チャネル	関連付け
3002D	名前付きパスワードの取得	パスワード名		イベント ID
3002E	属性のリセット			
3002F	値の追加 - エントリの追加	値	src-dn	イベント ID

表 *C-3* エンジンイベントのフィールド *:Value1* タイトル、*Value2* タイトル、および *Value3* タイトル

イベント ID	説明	Value1 タイトル	Value2 タイトル	Value3 タイトル
30001	ステータスは成功です			
30002	ステータスは再試行です			
30003	ステータスは警告です			
30004	ステータスがエラーです			
30005	ステータスは致命的です			
30006	ステータスはその他です			

イベント ID	説明	Value1 タイトル	Value2 タイトル	Value3 タイトル
30007	検索			結果
30008	エントリの追加			結果
30009	エントリの削除			結果
3000A	エントリの変更			結果
3000B	エントリの名前変更			結果
3000C	エントリの移動			結果
3000D	関連付けの追加			結果
3000E	関連付けを削除			結果
3000F	クエリースキーマ			結果
30010	パスワードの確認			
30011	オブジェクトパスワードの確認			
30012	パスワードの変更			結果
30013	同期			結果
30014	XML ドキュメントの入力			
30015	入力変換ドキュメント			
30016	出力変換ドキュメント			
30017	イベント変換ドキュメント			
30018	配置ルール変換ドキュメント			
30019	作成ルール変換ドキュメント			
3001A	入力マッピングルール変換ドキュメント			
3001B	出力マッピングルール変換ドキュメント			
3001C	一致ルール変換ドキュメント			
3001D	コマンド変換ドキュメント			
3001E	発行者フィルタ変換ドキュメント			
3001F	ユーザエージェント要求			結果
30020	再同期ドライバ			結果
30021	移行			

イベント ID	説明	Value1 タイトル	Value2 タイトル	Value3 タイトル
30022	ドライバの起動	状態		
30023	ドライバの停止	状態		
30024	パスワード同期			結果
30025	パスワードのリセット			
30026	DirXML のエラー	コード		
30027	DirXML の警告	コード		
30028	カスタム操作			
30029	属性のクリア			結果
3002A	値の追加 - エントリの変更			結果
3002B	値の削除			結果
3002C	エントリのマージ			
3002D	名前付きパスワードの取得			結果
3002E	属性のリセット			
3002F	値の追加 - エントリの追加			結果

表 *C-4* エンジンイベントのフィールド : データタイプとトリガ

イベント ID	説明	データタイプ	トリガ
30001	ステータスは成功です	XML ドキュメント	多くの異なるイベントの中には、ステータスが成功になるものがあります。これは通常、操作が正常に完了したことを示します。
30002	ステータスは再試行です	XML ドキュメント	多くの異なるイベントの中には、ステータスが再試行になるものがあります。これは、操作が完了せず、操作を後で再試行する必要があることを示します。
30003	ステータスは警告です	XML ドキュメント	多くの異なるイベントの中には、ステータスが警告になるものがあります。これは通常、操作で小さな問題が発生して完了したことを示します。
30004	ステータスがエラーです	XML ドキュメント	多くの異なるイベントの中には、ステータスがエラーになるものがあります。これは通常、操作が正常に完了しなかったことを示します。

イベント ID	説明	データタイプ	トリガ
30005	ステータスは致命的です	XML ドキュメント	多くの異なるイベントの中には、ステータスが致命的になるものがあります。これは通常、操作が正常に完了せず、エンジンまたはドライバを続行できなかったことを示します。
30006	ステータスはその他です	XML ドキュメント	上記で定義した 5 つのレベル以外で処理されたステータスドキュメントでは、その他のステータスでイベントが作成されます。これらのイベントは、スタイルシートまたはルール内でのみ生成されます。
30007	検索	XML ドキュメント	クエリドキュメントが IDM エンジンまたはドライバに送信されるときに発生します。
30008	エントリの追加	XML ドキュメント	オブジェクトが追加されるときに発生します。
30009	エントリの削除	XML ドキュメント	オブジェクトが削除されるときに発生します。
3000A	エントリの変更	XML ドキュメント	オブジェクトが変更されるときに発生します。
3000B	エントリの名前変更	XML ドキュメント	オブジェクトが名前変更されるときに発生します。
3000C	エントリの移動	XML ドキュメント	オブジェクトが移動されるときに発生します。
3000D	関連付けの追加	XML ドキュメント	関連付けが追加されるときに発生します。追加または一致で発生する場合もあります。
3000E	関連付けを削除	XML ドキュメント	オブジェクトが削除されても、関連付けを削除するイベントは発生しません。関連付けが削除されるのは、異なるアプリケーションでユーザオブジェクトが削除されたときです。このとき、削除が「変更」に変換されることによって関連付けが削除されます。
3000F	クエリースキーマ	XML ドキュメント	クエリースキーマ操作が IDM エンジンまたはドライバに送信されるときに発生します。
30010	パスワードの確認		iManager から実行される手動の機能です。
30011	オブジェクトパスワードの確認	XML ドキュメント	ドライバ以外の、オブジェクトのパスワードを確認するために要求が発行されるときに発生します。

イベント ID	説明	データタイプ	トリガ
30012	パスワードの変更	XML ドキュメント	ドライバのパスワードを確認するために要求が発行されるときに発生します。
30013	同期	XML ドキュメント	同期イベントが要求されるときに発生します。
30014	XML ドキュメントの入力	XML ドキュメント	エンジンまたはドライバによって入力ドキュメントが作成されるたびに生成されます。
30015	入力変換ドキュメント	XML ドキュメント	入力変換ポリシーが処理された後で生成されます。ユーザは変換されたドキュメントを表示できます。
30016	出力変換ドキュメント	XML ドキュメント	出力変換ポリシーが処理された後で生成されます。ユーザは変換されたドキュメントを表示できます。
30017	イベント変換ドキュメント	XML ドキュメント	イベント変換ポリシーが処理された後で生成されます。ユーザは変換されたドキュメントを表示できます。
30018	配置ルール変換ドキュメント	XML ドキュメント	配置ルールポリシーが処理された後で生成されます。ユーザは変換されたドキュメントを表示できます。
30019	作成ルール変換ドキュメント	XML ドキュメント	作成ルールポリシーが処理された後で生成されます。ユーザは変換されたドキュメントを表示できます。
3001A	入力マッピングルール変換ドキュメント	XML ドキュメント	ドキュメントを eDirectory スキーマに変換する、スキーマのマッピングルールが処理された後に生成されます。
3001B	出力マッピングルール変換ドキュメント	XML ドキュメント	ドキュメントをアプリケーションスキーマに変換する、スキーマのマッピングルールが処理された後に生成されます。
3001C	一致ルール変換ドキュメント	XML ドキュメント	一致ルールポリシーが処理された後で生成されます。ユーザは変換されたドキュメントを表示できます。
3001D	コマンド変換ドキュメント	XML ドキュメント	コマンド変換ポリシーが処理された後で生成されます。ユーザは変換されたドキュメントを表示できます。

イベント ID	説明	データタイプ	トリガ
3001E	発行者フィルタ変換ドキュメント	XML ドキュメント	発行者チャネルで通知フィルタを処理した後で生成されます。ユーザは変換されたドキュメントを表示できます。
3001F	ユーザエージェント要求	XML ドキュメント	購読者チャネルで、ユーザエージェントの XDS コマンドドキュメントがドライバに送信されるときに発生します。
30020	再同期ドライバ		同期の要求が発行されるときに発生します。
30021	移行		移行の要求が発行されるときに発生します。
30022	ドライバの起動	XML ドキュメント	ドライバが起動するときに発生します。
30023	ドライバの停止	XML ドキュメント	ドライバが停止するときに発生します。
30024	パスワード同期		オブジェクトに配布パスワードまたは単純パスワードを設定するときに生成されます。
30025	パスワードのリセット		パスワード同期操作が失敗した後に、接続されているアプリケーションのパスワードをリセットするときに生成されます。
30026	DirXML のエラー		エンジンで内部エラーが発生するたびに生成されます。
30027	DirXML の警告		エンジンで内部警告が発生するたびに生成されます。
30028	カスタム操作	XML ドキュメント	入力ドキュメントに不明な操作があるときに発生します。不明でない操作の例は、追加、削除、変更などです。
30029	属性のクリア		変更操作に remove-all-value 要素が含まれているときに発生します。
3002A	値の追加 - エントリの変更	値	オブジェクトの変更時に値が追加されるときに発生します。
3002B	値の削除	値	変更操作に remove-value 要素が含まれているときに発生します。
3002C	エントリのマージ	XML ドキュメント	2 つのオブジェクトがマージされるときに発生します。
3002D	名前付きパスワードの取得	XML ドキュメント	名前付きパスワードの取得の操作で生成されます。

イベント ID	説明	データタイプ	トリガ
3002E	属性のリセット	XML ドキュメント	発行者チャネルまたは購読者チャネルで、ドキュメントのリセットが発行されるときに発生します。
3002F	値の追加 - エントリの追加	値	オブジェクトの作成時に値が追加されるときに発生します。

C.2 サーバイベント

次の表は、Novell Audit を介して監査できるサーバイベントの一覧です。

表 *C-5* サーバイベントフィールド : オリジネータタイトル、ターゲットタイトル、およびサブターゲットタイトル

イベント ID	説明	オリジネータタイトル	ターゲットタイトル	サブターゲットタイトル
307D0	設定 : ログイベント	サーバ	ドライバ	属性名
307D1	設定 : ドライバのキャッシュ上限	サーバ	ドライバ	属性名
307D2	設定 : ドライバセット	サーバ	サーバ	属性名
307D3	設定 : ドライバの起動オプション	サーバ	ドライバ	属性名
307D4	ドライバの再同期	サーバ	ドライバ	
307D5	アプリケーションサーバの移行	サーバ	ドライバ	
307D6	シムパスワードセット	サーバ	ドライバ	属性名
307D7	キー付きパスワードセット	サーバ	ドライバ	
307D8	リモートローダのパスワードセット	サーバ	ドライバ	属性名

表 *C-6* サーバイベントフィールド :*Text1* タイトル、*Text2* タイトル、および *Text3* タイトル

イベント ID	説明	Text1 タイトル	Text2 タイトル	Text3 タイトル
307D0	設定 : ログイベント			操作
307D1	設定 : ドライバのキャッシュ上限			

イベント ID	説明	Text1 タイトル	Text2 タイトル	Text3 タイトル
307D2	設定 : ドライバセット	ドライバセット	Type	
307D3	設定 : ドライバの起動オプション			メッセージ
307D4	ドライバの再同期			
307D5	アプリケーションサーバの移行			
307D6	シムパスワードセット			
307D7	キー付きパスワードセット		Type	
307D8	リモートローダのパスワードセット			

表 *C-7* サーバイベントフィールド *:Value1* タイトル、*Value2* タイトル、および *Value3* タイトル

イベント ID	説明	Value1 タイトル	Value2 タイトル	Value3 タイトル
307D0	設定 : ログイベント			結果
307D1	設定 : ドライバのキャッシュ上限	制限容量		結果
307D2	設定 : ドライバセット			結果
307D3	設定 : ドライバの起動オプション	起動オプション		結果
307D4	ドライバの再同期			結果
307D5	アプリケーションサーバの移行			結果
307D6	シムパスワードセット		バージョン	結果
307D7	キー付きパスワードセット			結果
307D8	リモートローダのパスワードセット		バージョン	結果

表 *C-8* サーバイベントフィールド : データタイプとトリガ

イベント ID	説明	データタイプ	トリガ
307D0	設定 : ログイベント	入力バッファ	ドライバまたはドライバセットオブジェクトで、ログイベントの属性が変更されるときに発生します。
307D1	設定 : ドライバのキャッシュ上限		ドライバオブジェクトで、ドライバのキャッシュの上限の属性が変更されるときに発生します。
307D2	設定 : ドライバセット	入力バッファ	ドライバセット / サーバの関連付けが変更されるときに発生します。
307D3	設定 : ドライバの起動オプション	入力バッファ	ドライバオブジェクトで、ドライバの起動オプションが変更されるときに発生します。
307D4	ドライバの再同期		ドライバの再同期が発行されるときに発生します。
307D5	アプリケーションサーバの移行	XML ドキュメント	アプリケーションサーバの移行が発生するときに発生します。
307D6	シムパスワードセット		アプリケーションのパスワードが設定されるときに発生します。
307D7	キー付きパスワードセット		
307D8	リモートローダのパスワードセット		リモートローダのパスワードが設定されるときに発生します。

C.3 リモートローダのイベント

次の表は、Novell Audit を介して監査できるリモートローダイベントの一覧です。

表 *C-9* リモートローダイベントのフィールド : オリジネータタイトル、ターゲットタイトル、およびサブターゲットタイトル

イベント ID	説明	オリジネータタイトル	トリガ
30BB8	リモートローダの起動	インスタンス	リモートローダが起動するときに発生します。
30BB9	リモートローダの停止	インスタンス	リモートローダが停止するときに発生します。
30BBA	リモートローダの接続の確立	インスタンス	リモートローダの接続が確立したときに発生します。
30BBB	リモートローダの接続のドロップ	インスタンス	リモートローダの接続がドロップしたときに発生します。

C.4 詳細ポートレット

表 *C-10* 詳細ポートレットのフィールド : オリジネータタイトル、ターゲットタイトル、およびサブターゲットタイトル

イベント ID	説明	オリジネータタイトル	ターゲットタイトル	サブターゲットタイトル
31400	Delete_Entity	ユーザ名	エンティティ DN	エンティティ定義
31401	Update_Entity	ユーザ名	エンティティ DN	エンティティ定義

表 *C-11* 詳細ポートレットのフィールド : グループタイトル、グループタイプ、およびトリガ

イベント ID	説明	グループタイトル	グループタイプ	トリガ
31400	Delete_Entity	グループ番号	番号	オブジェクトが削除されるときに発生します。
31401	Update_Entity	グループ番号	番号	オブジェクトが変更されるときに発生します。

C.5 パスワード変更ポートレット

表 *C-12* パスワードポートレットの変更フィールド : オリジネータタイトル、ターゲットタイトル、および *Text3* タイトル

イベント ID	説明	オリジネータタイトル	ターゲットタイトル	Text3 タイトル
31420	Change_Password_Failure	イニシエータ ID	ターゲット DN	エラーメッセージ
31421	Change_Password_Success	イニシエータ ID	ターゲット DN	

表 *C-13* パスワードポートレットの変更フィールド :*Value3* タイトル、*Value3* タイプ、およびトリガ

イベント ID	説明	Value3 タイトル	Value3 タイプ	トリガ
31420	Change_Password_Failure	エラー番号	ブール	パスワード変更が失敗したときに発生します。
31421	Change_Password_Success			パスワード変更が成功したときに発生します。

C.6 パスワードを忘れた場合のパスワード変更ポートレット

表 *C-14* パスワードを忘れた場合のパスワード変更ポートレットフィールド : オリジネータタイトル、ターゲットタイトル、および *Text3* タイトル

イベント ID	説明	オリジネータタイトル	ターゲットタイトル	Text3 タイトル
31420	Forgot_Password_Change_Failure	イニシエータ ID	ターゲット DN	エラーメッセージ
31421	Forgot_Password_Change_Success	イニシエータ ID	ターゲット DN	

表 *C-15* パスワードを忘れた場合のパスワード変更ポートレットフィールド :*Value3* タイトル、*Value3* タイプ、およびグループタイトル

イベント ID	説明	Value3 タイトル	Value3 タイプ	グループタイトル
31420	Forgot_Password_Change_Failure	エラー番号	ブール	グループ番号
31421	Forgot_Password_Change_Success			グループ番号

表 *C-16* パスワードを忘れた場合のパスワード変更ポートレットフィールド : グループタイプおよびトリガ

イベント ID	説明	グループタイプ	トリガ
31420	Forgot_Password_Change_Failure	番号	パスワードを忘れた場合の変更が失敗したときに発生します。
31421	Forgot_Password_Change_Success	番号	パスワードを忘れた場合の変更が成功したときに発生します。

C.7 リスト検索ポートレット

表 *C-17* リスト検索ポートレットのフィールド : オリジネータタイトル、ターゲットタイトル、およびグループタイトル

イベント ID	説明	オリジネータタイトル	ターゲットタイトル	グループタイトル
31430	Search_Request	ユーザ ID	検索キー	ユーザ ID
31431	Search_Saved	ユーザ ID	検索キー	ユーザ ID

表 *C-18* リスト検索ポートレットのフィールド : グループタイプ、データタイトル、およびデータタイプ

イベント ID	説明	グループタイプ	データタイトル	データタイプ
31430	Search_Request	番号	XML の検索	文字列
31431	Search_Saved	番号	XML の検索	文字列

表 *C-19* リスト検索ポートレットのフィールド : トリガ

イベント ID	説明	トリガ
31430	Search_Request	ユーザが検索要求を実行したときに発生します。
31431	Search_Saved	ユーザが［マイ保存済み検索］を選択したときに発生します。

C.8 作成ポートレット

表 *C-20* 作成ポートレットのフィールド : オリジネータタイトル、ターゲットタイトル、およびサブターゲットタイトル

イベント ID	説明	オリジネータタイトル	ターゲットタイトル	サブターゲットタイトル
31440	Create_Entity	ユーザ名	エンティティ DN	エンティティ定義

表 *C-21* 作成ポートレットのフィールド : トリガ

イベント ID	説明	トリガ
31440	Create_Entity	オブジェクトが作成されるときに発生します。

C.9 セキュリティコンテキスト

次の表は、Novell Audit を介して監査できるセキュリティイベントの一覧です。

表 *C-22* セキュリティコンテキストのフィールド : オリジネータタイトル、ターゲットタイトル、および *Text1* タイトル

イベント ID	説明	オリジネータタイトル	ターゲットタイトル	Text1 タイトル
31540	Create_Proxy_Definition_Success	イニシエータ ID	定義	詳細
31541	Create_Proxy_Definition_Failure	イニシエータ ID	定義	詳細
31542	Update_Proxy_Definition_Success	イニシエータ ID	定義	詳細
31543	Update_Proxy_Definition_Failure	イニシエータ ID	定義	詳細

イベント ID	説明	オリジネータタイトル	ターゲットタイトル	Text1 タイトル
31544	Delete_Proxy_Definition_Success	イニシエータ ID	定義	詳細
31545	Delete_Proxy_Definition_Failure	イニシエータ ID	定義	詳細
31546	Create_Delegatee_Definition_Success	イニシエータ ID	定義	詳細
31547	Create_Delegatee_Definition_Failure	イニシエータ ID	定義	詳細
31548	Update_Delegatee_Definition_Success	イニシエータ ID	定義	詳細
31549	Update_Delegatee_Definition_Failure	イニシエータ ID	定義	詳細
3154A	Delete_Delegatee_Definition_Success	イニシエータ ID	定義	詳細
3154B	Delete_Delegatee_Definition_Failure	イニシエータ ID	定義	詳細
3154C	Create_Availability_Success	イニシエータ ID	ターゲット	
3154D	Create_Availability_Failure	イニシエータ ID	ターゲット	詳細
3154E	Delete_Availability_Success	イニシエータ ID	ターゲット	詳細
3154F	Delete_Availability_Failure	イニシエータ ID	ターゲット	詳細

表 *C-23* セキュリティコンテキストのフィールド *:Text3* タイトル、データタイトル、およびデータタイプ

イベント ID	説明	Text3 タイトル	データタイトル	データタイプ
31540	Create_Proxy_Definition_Success			
31541	Create_Proxy_Definition_Failure	エラーメッセージ	スタックトレース	文字列
31542	Update_Proxy_Definition_Success			
31543	Update_Proxy_Definition_Failure	エラーメッセージ	スタックトレース	文字列
31544	Delete_Proxy_Definition_Success			
31545	Delete_Proxy_Definition_Failure	エラーメッセージ	スタックトレース	文字列
31546	Create_Delegatee_Definition_Success			
31547	Create_Delegatee_Definition_Failure	エラーメッセージ	スタックトレース	文字列
31548	Update_Delegatee_Definition_Success			
31549	Update_Delegatee_Definition_Failure	エラーメッセージ	スタックトレース	文字列
3154A	Delete_Delegatee_Definition_Success			
3154B	Delete_Delegatee_Definition_Failure	エラーメッセージ	スタックトレース	文字列
3154C	Create_Availability_Success			
3154D	Create_Availability_Failure	エラーメッセージ	スタックトレース	文字列
3154E	Delete_Availability_Success			
3154F	Delete_Availability_Failure	エラーメッセージ	スタックトレース	文字列

表 *C-24* セキュリティコンテキストのフィールド : トリガ

イベント ID	説明	トリガ
31540	Create_Proxy_Definition_Success	プロキシ定義の作成が成功したときに発生します。
31541	Create_Proxy_Definition_Failure	プロキシ定義の作成が失敗したときに発生します。
31542	Update_Proxy_Definition_Success	プロキシ定義の更新が成功したときに発生します。
31543	Update_Proxy_Definition_Failure	プロキシ定義の更新が失敗したときに発生します。
31544	Delete_Proxy_Definition_Success	プロキシ定義の削除が成功したときに発生します。
31545	Delete_Proxy_Definition_Failure	プロキシ定義の削除が失敗したときに発生します。
31546	Create_Delegatee_Definition_Success	委任先定義の作成が成功したときに発生します。
31547	Create_Delegatee_Definition_Failure	委任先定義の作成が失敗したときに発生します。
31548	Update_Delegatee_Definition_Success	委任先定義の更新が成功したときに発生します。
31549	Update_Delegatee_Definition_Failure	委任先定義の更新が失敗したときに発生します。
3154A	Delete_Delegatee_Definition_Success	委任先定義の削除が成功したときに発生します。
3154B	Delete_Delegatee_Definition_Failure	委任先定義の削除が失敗したときに発生します。
3154C	Create_Availability_Success	可用性ステータスの作成が成功したときに発生します。
3154D	Create_Availability_Failure	可用性ステータスの作成が失敗したときに発生します。
3154E	Delete_Availability_Success	可用性ステータスの削除が成功したときに発生します。
3154F	Delete_Availability_Failure	可用性ステータスの削除が失敗したときに発生します。

C.10 ワークフロー

次の表は、Novell Audit を介して監査できるユーザアプリケーションイベントの一覧です。

表 *C-25* ワークフローフィールド : オリジネータタイトル、ターゲットタイトル、およびサブターゲットタイトル

イベント ID	説明	オリジネータタイトル	ターゲットタイトル	サブターゲットタイトル
31520	Workflow_Error	イニシエータ ID		
31521	Workflow_Started	イニシエータ ID		
31522	Workflow_Forwarded	イニシエータ ID	受信者	プロセス名
31523	Workflow_Reassigned	イニシエータ ID	受信者	プロセス名
31524	Workflow_Approved	イニシエータ ID	受信者	プロセス名
31525	Workflow_Refused	イニシエータ ID	受信者	プロセス名
31526	Workflow_Ended	イニシエータ ID	受信者	プロセス名
31527	Workflow_Claimed	イニシエータ ID	受信者	プロセス名
31528	Workflow_Unclaimed	イニシエータ ID	受信者	プロセス名
31529	Workflow_Denied	イニシエータ ID	受信者	プロセス名
3152A	Workflow_Completed	イニシエータ ID	受信者	プロセス名
3152B	Workflow_Timedout	イニシエータ ID	受信者	プロセス名
3152C	User_Message	イニシエータ ID	著者	
3152D	Provision_Error	イニシエータ ID	受信者	プロセス名
3152E	Provision_Submitted	イニシエータ ID	受信者	プロセス名
3152F	Provision_Success	イニシエータ ID	受信者	プロセス名
31530	Provision_Failure	イニシエータ ID	受信者	プロセス名
31531	Provision_Granted	イニシエータ ID	受信者	プロセス名
31532	Provision_Revoked	イニシエータ ID	受信者	プロセス名
31533	Workflow_Retracted	イニシエータ ID	受信者	プロセス名

表 *C-26* ワークフローフィールド :*Text1* タイトル、*Text2* タイトル、および *Text3* タイトル

イベント ID	説明	Text1 タイトル	Text2 タイトル	Text3 タイトル
31520	Workflow_Error	アクティビティ	プロセス ID	エラーメッセージ
31521	Workflow_Started	アクティビティ	プロセス ID	
31522	Workflow_Forwarded	アクティビティ	プロセス ID	
31523	Workflow_Reassigned	アクティビティ	プロセス ID	
31524	Workflow_Approved	アクティビティ	プロセス ID	セカンダリユーザ
31525	Workflow_Refused	アクティビティ	プロセス ID	セカンダリユーザ
31526	Workflow_Ended	アクティビティ	プロセス ID	

イベント ID	説明	Text1 タイトル	Text2 タイトル	Text3 タイトル
31527	Workflow_Claimed	アクティビティ	プロセス ID	セカンダリユーザ
31528	Workflow_Unclaimed	アクティビティ	プロセス ID	セカンダリユーザ
31529	Workflow_Denied	アクティビティ	プロセス ID	セカンダリユーザ
3152A	Workflow_Completed	アクティビティ	プロセス ID	
3152B	Workflow_Timedout	アクティビティ	プロセス ID	
3152C	User_Message		メッセージ	
3152D	Provision_Error	アクティビティ	プロセス ID	エラーメッセージ
3152E	Provision_Submitted	アクティビティ	プロセス ID	
3152F	Provision_Success	アクティビティ	プロセス ID	
31530	Provision_Failure	アクティビティ	プロセス ID	
31531	Provision_Granted	アクティビティ	プロセス ID	
31532	Provision_Revoked	アクティビティ	プロセス ID	
31533	Workflow_Retracted	アクティビティ	プロセス ID	セカンダリユーザ

表 *C-27* ワークフローフィールド *:Value3* タイトル、*Value3* タイプ、およびデータタイトル

イベント ID	説明	Value3 タイトル	Value3 タイプ	データタイトル
31520	Workflow_Error	エラー番号	ブール	スタックトレース
31521	Workflow_Started			
31522	Workflow_Forwarded			
31523	Workflow_Reassigned			
31524	Workflow_Approved			セカンダリユーザタイプ
31525	Workflow_Refused			セカンダリユーザタイプ
31526	Workflow_Ended			
31527	Workflow_Claimed			セカンダリユーザタイプ
31528	Workflow_Unclaimed			セカンダリユーザタイプ
31529	Workflow_Denied			セカンダリユーザタイプ
3152A	Workflow_Completed			
3152B	Workflow_Timedout			
3152C	User_Message			

イベント ID	説明	Value3 タイトル	Value3 タイプ	データタイトル
3152D	Provision_Error	エラー番号	ブール	スタックトレース
3152E	Provision_Submitted			
3152F	Provision_Success			
31530	Provision_Failure			
31531	Provision_Granted			
31532	Provision_Revoked			
31533	Workflow_Retracted			セカンダリユーザタイプ

表 *C-28* ワークフローフィールド : データタイプとトリガ

イベント ID	説明	データタイプ	トリガ
31520	Workflow_Error	文字列	多くの項目で、このイベントが発生します。
31521	Workflow_Started		ワークフローが起動するときに発生します。
31522	Workflow_Forwarded		ワークフローが転送されるときに発生します。
31523	Workflow_Reassigned		ワークフローが再割り当てされるときに発生します。
31524	Workflow_Approved	文字列	ワークフローが承認されるときに発生します。
31525	Workflow_Refused	文字列	ワークフローが拒否されたときに発生します。
31526	Workflow_Ended		ワークフローが終了したときに発生します。
31527	Workflow_Claimed	文字列	ワークフローが要求されたときに発生します。
31528	Workflow_Unclaimed	文字列	
31529	Workflow_Denied	文字列	ワークフローが否認されたときに発生します。
3152A	Workflow_Completed		ワークフローが完了したときに発生します。
3152B	Workflow_Timedout		ワークフローがタイムアウトしたときに発生します。
3152C	User_Message		
3152D	Provision_Error	文字列	多くの項目で、このイベントが発生します。
3152E	Provision_Submitted		

イベント ID	説明	データタイプ	トリガ
3152F	Provision_Success		
31530	Provision_Failure		
31531	Provision_Granted		
31532	Provision_Revoked		
31533	Workflow_Retracted	文字列	ワークフローが撤回されたときに発生します。

C.11 レポート

ここでは、Novell Audit レポートの表示例を示します。実行できるレポートは次のとおりです。

- Administrative Action Report (管理アクションレポート)
- Historical Approval Flow Report (認証フロー履歴レポート)
- Resource Provisioning report (リソースプロビジョニングレポート)
- Specific User Audit Trail (特定ユーザの監査記録)
- Specific User Provisioning (特定のユーザのプロビジョニング)
- User Provisioning (ユーザのプロビジョニング)

図 **C-1** *Administrative Action Report (* 管理アクションレポート *)*

Novell® Audit Report for Identity Manager

Administrative Action Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 5

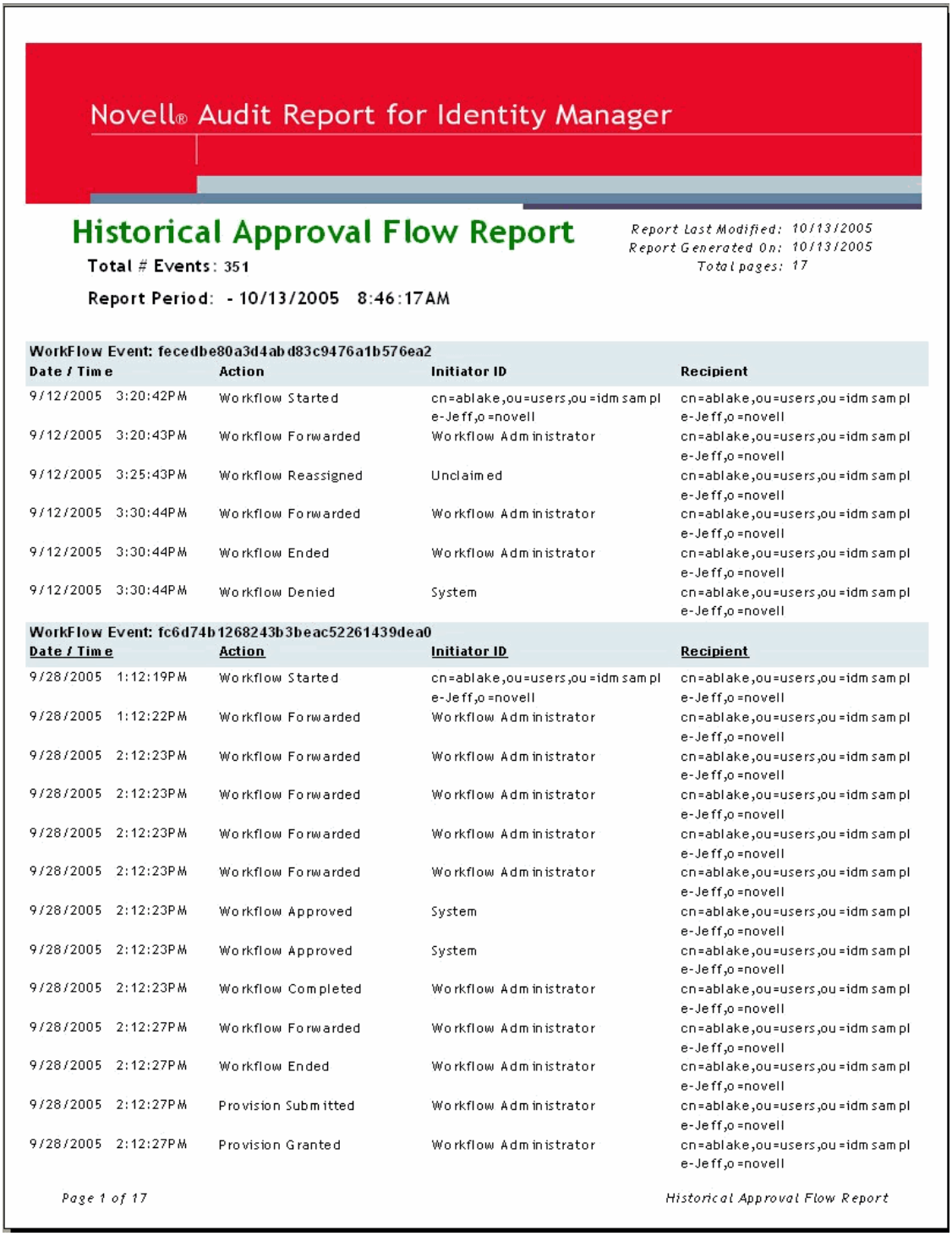
Total # Events: 121

Report Period: - 10/13/2005 8:43:50AM

Date / Time	Administrator	Subject	Action
8/18/2005 5:45:17PM	cn=admin,ou=idmsample-cts10,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:07:40PM	cn=admin,ou=idmsample-cts10,o=novell	cn=testCreateUser11,ou=users,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:09:05PM	cn=admin,ou=idmsample-cts10,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:12:50PM	cn=admin,ou=idmsample-cts10,o=novell	cn=testCreateUser11,ou=users,ou=idmsample-cts10,o=novell	Entity Deleted
8/18/2005 7:13:39PM	cn=admin,ou=idmsample-cts10,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-cts10,o=novell	Entity Deleted
8/23/2005 4:56:39PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Deleted
8/31/2005 12:01:55PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 12:02:18PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Created
8/31/2005 12:19:07PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 12:19:31PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Created
8/31/2005 12:27:58PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 12:28:22PM	cn=admin,ou=idmsample,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample,o=novell	Entity Created
8/31/2005 2:59:39PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 3:24:30PM	cn=admin,ou=idmsample,o=novell	cn=testCreateUser,ou=users,ou=idmsample,o=novell	Entity Created
8/31/2005 8:11:59PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=testCreateUser,ou=users,ou=idmsample-Jeff,o=novell	Entity Deleted
8/31/2005 8:12:23PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=TestCreateGroup,ou=groups,ou=idmsample-Jeff,o=novell	Entity Deleted
8/31/2005 8:12:55PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=admin,ou=idmsample-Jeff,o=novell	Entity Updated
8/31/2005 8:13:03PM	cn=admin,ou=idmsample-Jeff,o=novell	cn=admin,ou=idmsample-Jeff,o=novell	Entity Updated
9/1/2005 10:29:53AM	cn=admin,ou=idmsample-Jeff,o=novell	cn=aa,ou=users,ou=idmsample-Jeff,o=novell	Entity Deleted
9/1/2005 11:31:45AM	cn=admin,ou=idmsample,o=novell	cn=asoprano,ou=users,ou=idmsample,o=novell	Entity Created

Page 1 of 5 *Administrative Action Report*

図 **C-2** *Historical Approval Flow Report (* 認証フロー履歴レポート *)*



Novell® Audit Report for Identity Manager

Historical Approval Flow Report

Total # Events: 351

Report Period: - 10/13/2005 8:46:17AM

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 17

WorkFlow Event: fecedbe80a3d4abd83c9476a1b576ea2

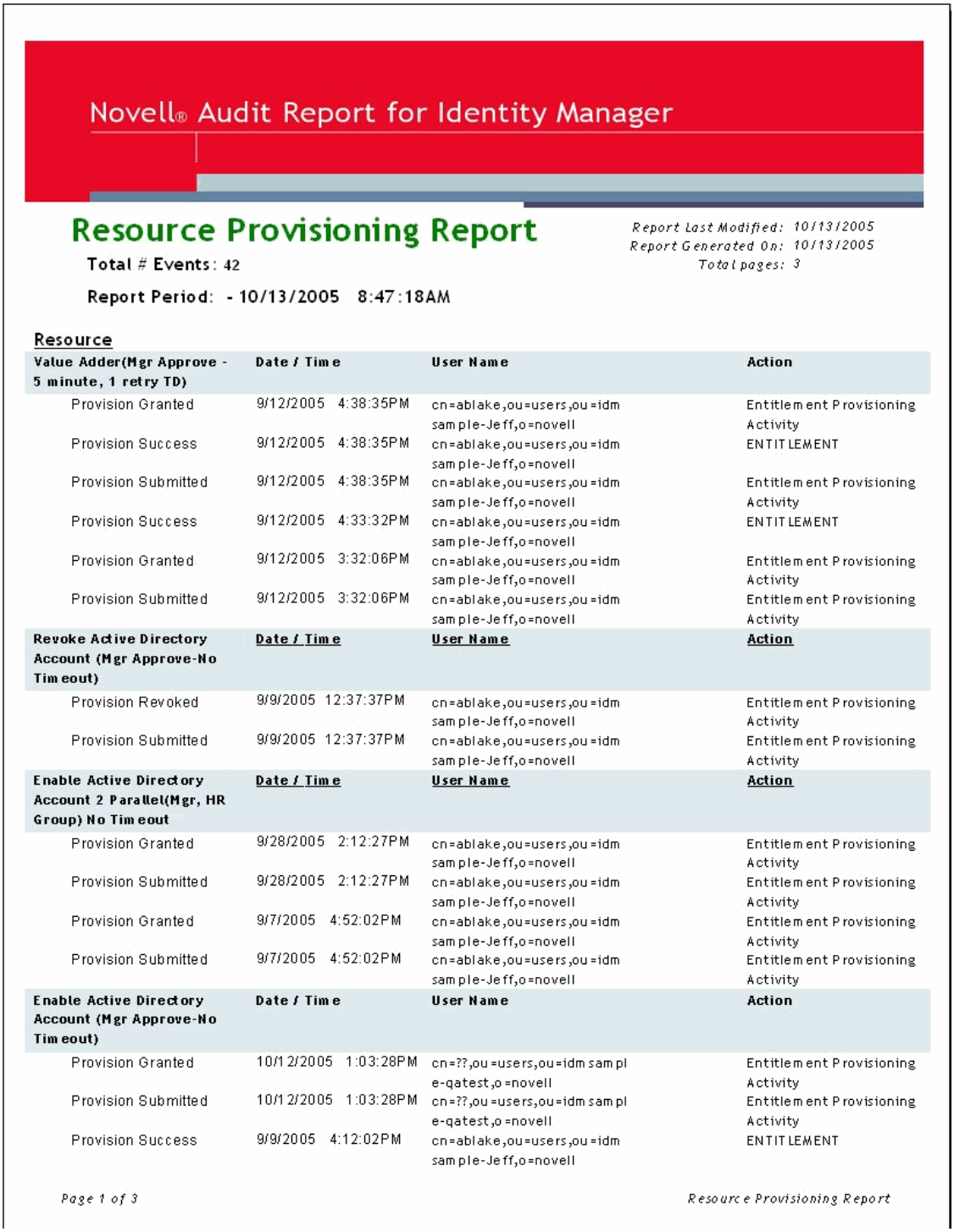
Date / Time	Action	Initiator ID	Recipient
9/12/2005 3:20:42PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:20:43PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:25:43PM	Workflow Reassigned	Unclaimed	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:30:44PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:30:44PM	Workflow Ended	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:30:44PM	Workflow Denied	System	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell

WorkFlow Event: fc6d74b1268243b3beac52261439dea0

Date / Time	Action	Initiator ID	Recipient
9/28/2005 1:12:19PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 1:12:22PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Approved	System	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Approved	System	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:23PM	Workflow Completed	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Workflow Forwarded	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Workflow Ended	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Provision Submitted	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 2:12:27PM	Provision Granted	Workflow Administrator	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell

Page 1 of 17 Historical Approval Flow Report

図 *C-3* *Resource Provisioning report (* リソースプロビジョニングレポート *)*



Novell® Audit Report for Identity Manager

Resource Provisioning Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 3

Total # Events: 42

Report Period: - 10/13/2005 8:47:18AM

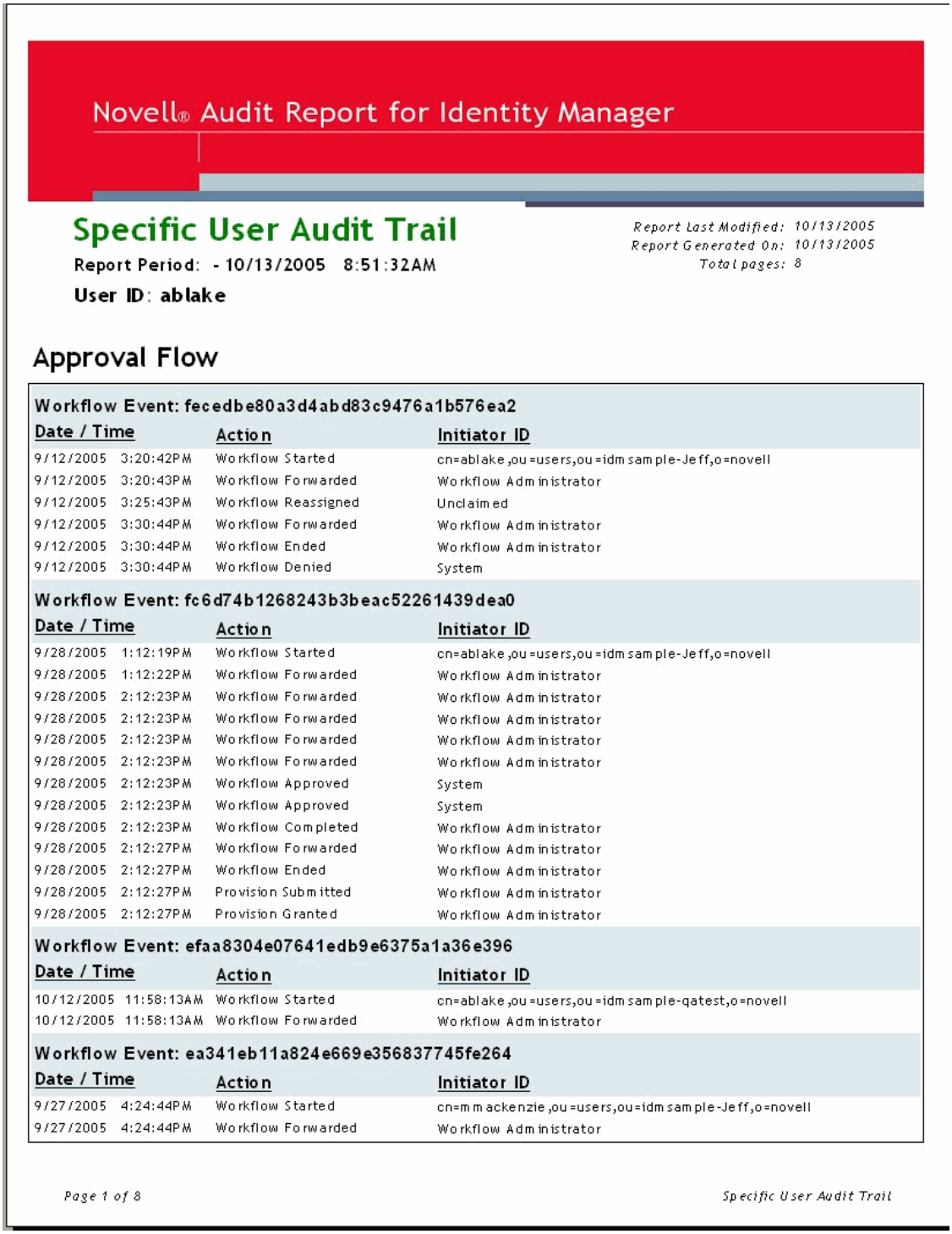
Resource

Value Adder(Mgr Approve - 5 minute, 1 retry TD)	**Date / Time**	**User Name**	**Action**
Provision Granted	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	ENTITLEMENT
Provision Submitted	9/12/2005 4:38:35PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:33:32PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	ENTITLEMENT
Provision Granted	9/12/2005 3:32:06PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 3:32:06PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Revoke Active Directory Account (Mgr Approve-No Timeout)	**Date / Time**	**User Name**	**Action**
Provision Revoked	9/9/2005 12:37:37PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/9/2005 12:37:37PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	**Date / Time**	**User Name**	**Action**
Provision Granted	9/28/2005 2:12:27PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/28/2005 2:12:27PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Granted	9/7/2005 4:52:02PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Provision Submitted	9/7/2005 4:52:02PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	Entitlement Provisioning Activity
Enable Active Directory Account (Mgr Approve-No Timeout)	**Date / Time**	**User Name**	**Action**
Provision Granted	10/12/2005 1:03:28PM	cn=??,ou=users,ou=idm sample-qatest,o=novell	Entitlement Provisioning Activity
Provision Submitted	10/12/2005 1:03:28PM	cn=??,ou=users,ou=idm sample-qatest,o=novell	Entitlement Provisioning Activity
Provision Success	9/9/2005 4:12:02PM	cn=ablake,ou=users,ou=idm sample-Jeff,o=novell	ENTITLEMENT

Page 1 of 3

Resource Provisioning Report

図 **C-4** *Specific User Audit Trail 1 (*特定のユーザの監査記録 *1)*



Novell® Audit Report for Identity Manager

Specific User Audit Trail

Report Period: - 10/13/2005 8:51:32AM

User ID: ablake

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 8

Approval Flow

Workflow Event: fecedbe80a3d4abd83c9476a1b576ea2

Date / Time	Action	Initiator ID
9/12/2005 3:20:42PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/12/2005 3:20:43PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:25:43PM	Workflow Reassigned	Unclaimed
9/12/2005 3:30:44PM	Workflow Forwarded	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Ended	Workflow Administrator
9/12/2005 3:30:44PM	Workflow Denied	System

Workflow Event: fc6d74b1268243b3beac52261439dea0

Date / Time	Action	Initiator ID
9/28/2005 1:12:19PM	Workflow Started	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell
9/28/2005 1:12:22PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Approved	System
9/28/2005 2:12:23PM	Workflow Completed	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Forwarded	Workflow Administrator
9/28/2005 2:12:27PM	Workflow Ended	Workflow Administrator
9/28/2005 2:12:27PM	Provision Submitted	Workflow Administrator
9/28/2005 2:12:27PM	Provision Granted	Workflow Administrator

Workflow Event: efaa8304e07641edb9e6375a1a36e396

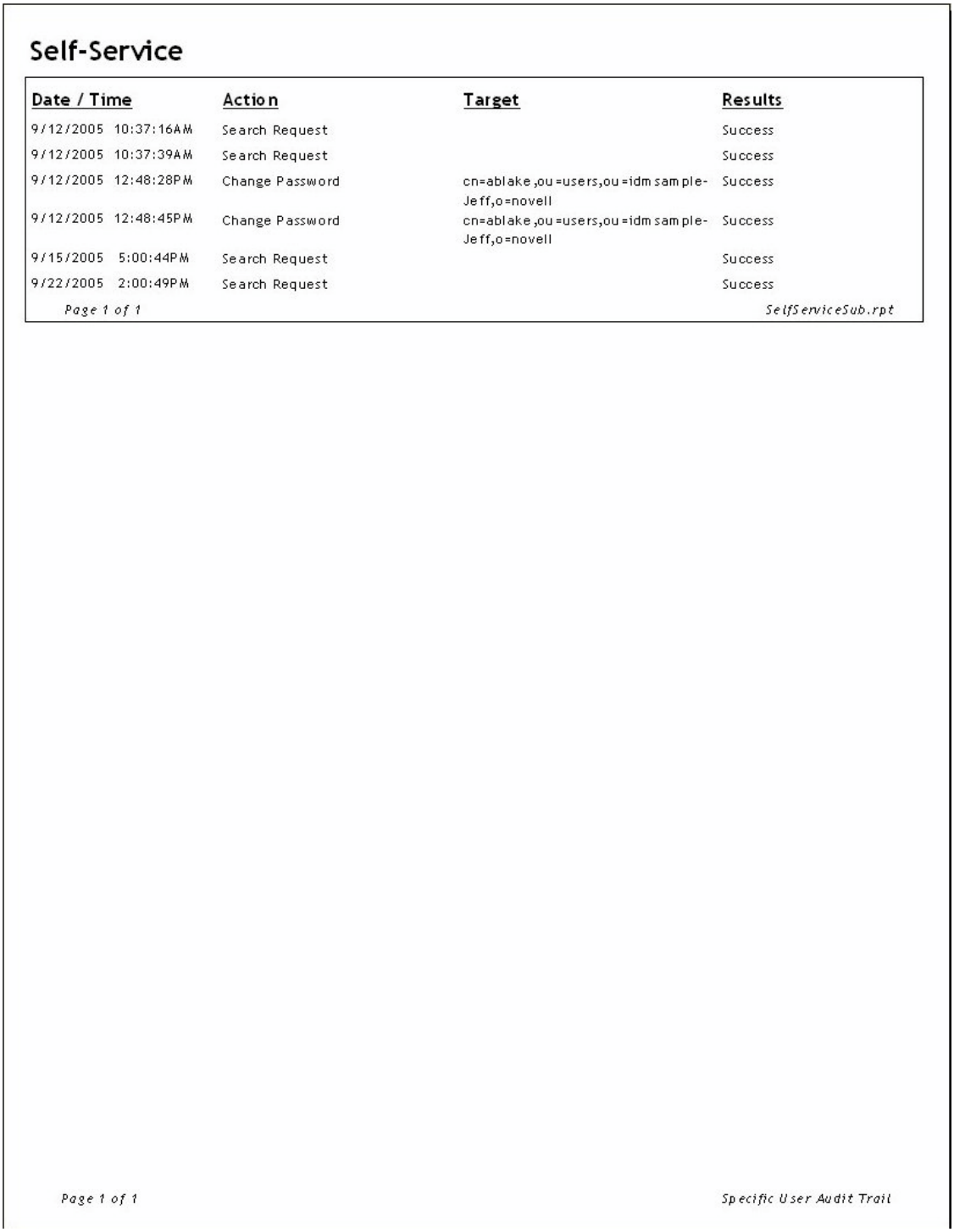
Date / Time	Action	Initiator ID
10/12/2005 11:58:13AM	Workflow Started	cn=ablake,ou=users,ou=idmsample-qatest,o=novell
10/12/2005 11:58:13AM	Workflow Forwarded	Workflow Administrator

Workflow Event: ea341eb11a824e669e356837745fe264

Date / Time	Action	Initiator ID
9/27/2005 4:24:44PM	Workflow Started	cn=mmackenzie,ou=users,ou=idmsample-Jeff,o=novell
9/27/2005 4:24:44PM	Workflow Forwarded	Workflow Administrator

Page 1 of 8 *Specific User Audit Trail*

図 *C-5* *Specific User Audit Trail 2 (* 特定のユーザの監査記録 *2)*



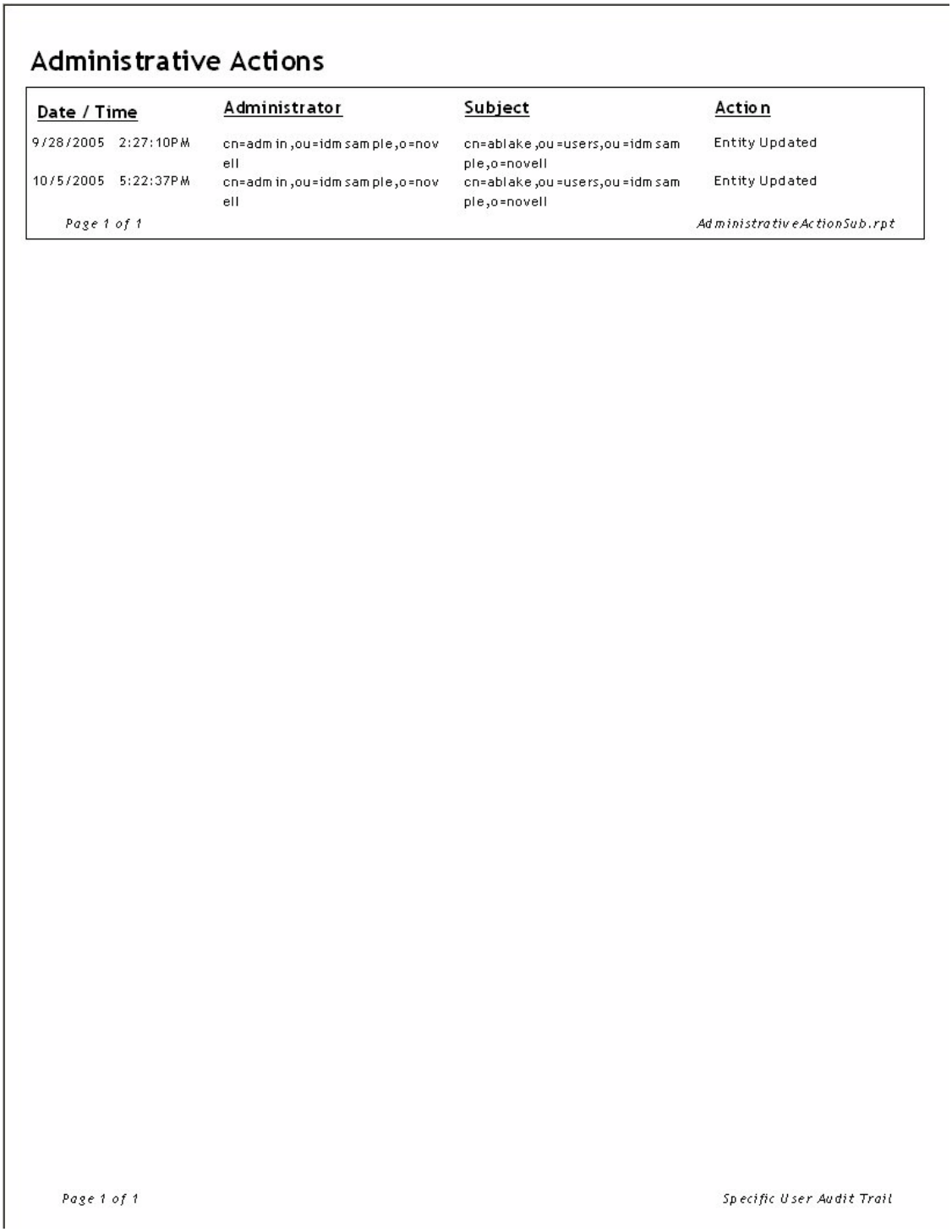
Self-Service

Date / Time	Action	Target	Results
9/12/2005 10:37:16AM	Search Request		Success
9/12/2005 10:37:39AM	Search Request		Success
9/12/2005 12:48:28PM	Change Password	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Success
9/12/2005 12:48:45PM	Change Password	cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Success
9/15/2005 5:00:44PM	Search Request		Success
9/22/2005 2:00:49PM	Search Request		Success

Page 1 of 1 SelfServiceSub.rpt

Page 1 of 1 Specific User Audit Trail

図 ***C-6*** *Specific User Audit Trail 3 (* 特定のユーザの監査記録 *3)*



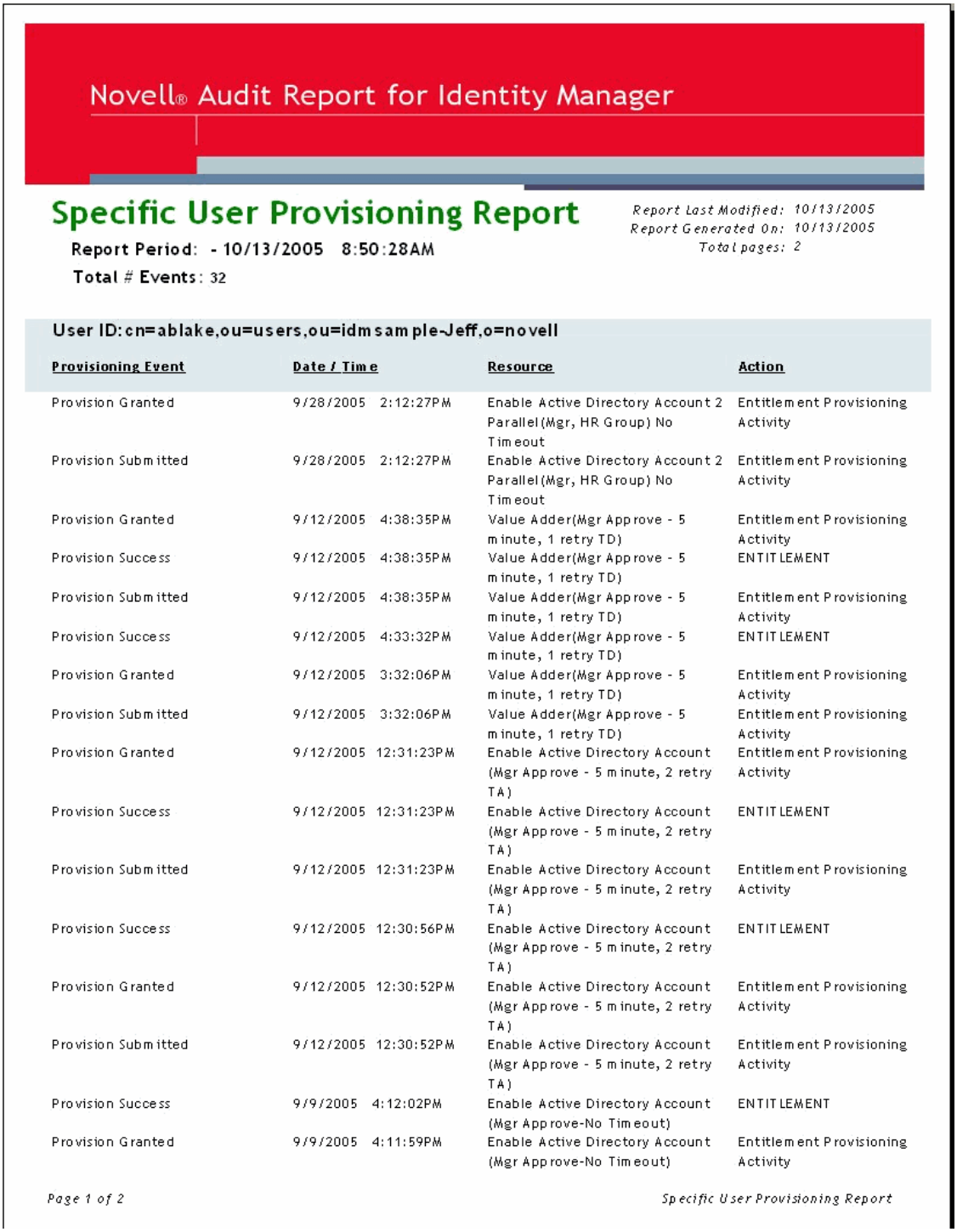
Administrative Actions

Date / Time	Administrator	Subject	Action
9/28/2005 2:27:10PM	cn=admin,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell	Entity Updated
10/5/2005 5:22:37PM	cn=admin,ou=idmsample,o=novell	cn=ablake,ou=users,ou=idmsample,o=novell	Entity Updated

Page 1 of 1 *AdministrativeActionSub.rpt*

Page 1 of 1 *Specific User Audit Trail*

図 C-7 *Specific User Provisioning report (* 特定ユーザのプロビジョニングレポート *)*



Novell® Audit Report for Identity Manager

Specific User Provisioning Report

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 2

Report Period: - 10/13/2005 8:50:28AM

Total # Events: 32

User ID: cn=ablake,ou=users,ou=idmsample-Jeff,o=novell

Provisioning Event	Date / Time	Resource	Action
Provision Granted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Submitted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Granted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Submitted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:33:32PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Granted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Granted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Submitted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:30:56PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Granted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/9/2005 4:12:02PM	Enable Active Directory Account (Mgr Approve-No Timeout)	ENTITLEMENT
Provision Granted	9/9/2005 4:11:59PM	Enable Active Directory Account (Mgr Approve-No Timeout)	Entitlement Provisioning Activity

Page 1 of 2 Specific User Provisioning Report

図 ***C-8*** *User Provisioning report (* ユーザプロビジョニングレポート *)*

Novell® Audit Report for Identity Manager

User Provisioning Report

Total # Events: 42

Report Period: - 10/13/2005 8:54:20AM

Report Last Modified: 10/13/2005
Report Generated On: 10/13/2005
Total pages: 3

User

cn=ablake,ou=users,ou=idmsample-Jeff,o=novell	Date / Time	Resource	Action
Provision Granted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Submitted	9/28/2005 2:12:27PM	Enable Active Directory Account 2 Parallel(Mgr, HR Group) No Timeout	Entitlement Provisioning Activity
Provision Granted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Submitted	9/12/2005 4:38:35PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Success	9/12/2005 4:33:32PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	ENTITLEMENT
Provision Granted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 3:32:06PM	Value Adder(Mgr Approve - 5 minute, 1 retry TD)	Entitlement Provisioning Activity
Provision Granted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Submitted	9/12/2005 12:31:23PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/12/2005 12:30:56PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	ENTITLEMENT
Provision Granted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Submitted	9/12/2005 12:30:52PM	Enable Active Directory Account (Mgr Approve - 5 minute, 2 retry TA)	Entitlement Provisioning Activity
Provision Success	9/9/2005 4:12:02PM	Enable Active Directory Account (Mgr Approve-No Timeout)	ENTITLEMENT
Provision Granted	9/9/2005 4:11:59PM	Enable Active Directory Account (Mgr Approve-No Timeout)	Entitlement Provisioning Activity

Page 1 of 3 *User Provisioning Report*

手動タスクサービスドライバ : 置換データ

D

置換データは、電子メールメッセージ、Web ページ、および XDS ドキュメントを構成するためのテンプレートとして使用される XML ドキュメントで使用されます。実際の置換は、出力ドキュメントの構成の一部として置換を実行する XSLT スタイルシートを持つ、テンプレートドキュメントを処理することにより実行されます。

置換データは、購読者チャネルおよび発行者チャネル上の異なるメカニズムを介して、手動タスクサービスドライバに提供されます。

購読者チャネル

- 置換データは、<mail> 要素の一部として提供されます。
- 提供される置換データの一部は URL データになります。URL データが提供された場合、自動データ項目によって、処理、完了、および置換が実行されます (305 ページの付録 E「手動タスクサービスドライバ : 自動置換データ項目」を参照)。
- 関連付けの値が構成される必要がある (すなわち <mail> 要素が src-dn 属性を持つ) ことが <mail> 要素によって指定された場合、「association」という名前の自動データ項目が置換データに追加されます。

発行者チャネル

- 置換データは、HTTP URL データと HTTP POST データで提供されます。
- 自動 URL 置換データ項目は、置換データに追加された後、テンプレート処理で使用されます。

XML ドキュメントとしてテンプレート処理されている間は、置換データが存在しています。置換データのドキュメントは、replacement-data という名前のパラメータとして、テンプレートを処理するスタイルシートに渡されます。テンプレートが使用されていない場合は、スタイルシートによって XML ドキュメントが直接処理されます。

D.1 データセキュリティ

データ項目は、購読者チャネルによって送信された電子メールに含まれている URL を経由して、購読者チャネルから発行者チャネルに渡されます。URL 内の特定のデータ項目を変更すると、セキュリティ上の問題が生じます。たとえば、URL の購読者チャネルによって提供された URL の responder-dn 値が、発行者チャネルの Web サーバに送信された URL のその他のユーザ DN によって置換された場合、承認されていないユーザが eDirectory 内のデータを変更できる場合があります。

送信された URL 内のデータが、本来購読者チャネルによって提供されたデータと同じであるようにするために、保護されたデータが提供されます。保護されたデータとは、セキュリティ上の理由のため変更できないデータです。このデータは設定によって異なりますが、responder-dn データ項目、および値が変更される eDirectory オブジェクトに対応するデータ項目が常に含まれています。

データ項目は、元の値を暗号化し、暗号化された値を URL クエリ文字列に配置することにより保護されています。発行者の Web サーバが暗号化された値を受信すると、発行者は値の暗号化を解除し、HTTP GET または POST 要求によって提供された暗号化されていないデータ項目との比較に使用します。

データ項目のインスタンスが暗号化されたデータに表示された場合、暗号化されてないデータ項目の値は暗号化されたデータ項目の値の 1 つに一致する必要があります。暗号化されてないデータ項目の値が、暗号化されたデータ項目の値の 1 つに一致しない場合、HTTP 要求は発行者チャネルの Web サーバによって拒否されます。

また、保護されたデータが含まれていないすべての HTTP POST 要求は拒否されます。

例

HTTP POST 要求では、発行者チャネルの Web サーバは、responder-dn という名前の暗号化されてない POST データを使用して、POST データによって提供されたパスワードを確認します。これは、ユーザの eDirectory オブジェクトに対して応答ユーザを認証するために行われます。

購読者チャネルの <url-query> 要素のコンテンツで、次のような 2 つのデータ項目が指定されているとします。

```
<item name="responder-dn" protect="yes">\PERIN-TAO\novell\phb</item>


<item name="responder-dn" protect="yes">\PERIN-TAO\novell\carol</item>
```

購読者チャネルによって生成された URL には、保護されたデータの両方の responder-dn 値が含まれています。

悪意のあるユーザが、電子メールメッセージで生成され送信された URL を取得したとします。悪意のあるユーザは、URL を使用して、eDirectory オブジェクトのデータをユーザが変更することができる HTML 形式を取得します。

Web サーバに送信された HTTP POST 要求で、悪意のあるユーザが暗号化されてない responder-dn 値として eDirectory DN (responder-dn=\PERIN-TAO\novell\wally) を使用します。また、悪意のあるユーザは、Web サーバが実行する認証が成功するように、POST データで自分のパスワードを送信します。

しかし、発行者チャネルの Web サーバが HTTP POST データを受信すると、暗号化された保護データ内での “\PERIN-TAO\novell\wally” の検索が失敗し、POST 要求が拒否されます。

D.2 XML 要素

置換データドキュメントを構成する要素について、次に説明します。XML 属性が要素に対して記述されていない場合、使用できません。

D.2.1 <replacement-data>

<replacement-data> 要素は次の場所に表示されます。

1. 購読者チャネルの <mail> 要素の下の <message> 要素の子として。

手動タスクサービスドライバは、入力された <replacement-data> 要素をスタンドアロンの <replacement-data> 要素に処理し、テンプレート処理に使用します。次の処理が発生します。

a. トークンで指定している <mail> 要素に対して関連付けの値が作成された場合、<item name="association"> 要素が置換データに追加されます。作成された要素の値は、Identity Manager に返された関連付けの値です。

b. <replacement-data> 要素には、<url-data> 要素の子があります。また、構成された URL データが含まれているいくつかの <item> 要素によって <url-data> 要素が置換されます。<url-data> および <url-query> を参照してください。

2. 購読者チャネルまたは発行者チャネルのいずれかで、スタイルシートを使用してドキュメントを構成するときに使用される、置換データのドキュメントのスタンドアロンのトップレベルの要素として。

D.2.2 <item>

<item> 要素は、<replacement-data> 要素、<url-data> 要素、または <url-query> 要素の子になることができます。<item> 要素のコンテンツは、テンプレートでの置換トークンの置き換えで使用されるテキストです。<item> 要素は常に名前属性を使用して名前が付けられます。

<item> 属性

name: name 属性の値には、置換トークンによってこのデータ項目が参照される名前が指定されます。たとえば、name 属性の値が manager の場合、置換トークン $manager$ は <item name="manager"> 要素に含まれている値に置換されます。name 属性は必須です。

protect: <url-query> 要素の子である <item> 要素では、URL クエリ文字列の保護されたデータセクションに項目が追加されるかどうかが protect 属性によって指定されます (<url-query> を参照)。protect 属性がある場合、値は「yes」である必要があります。

事前定義された <item> 名

特定の <item> 要素には、購読者チャネル、発行者チャネル、または両方のチャネルのいずれかに対して事前定義された意味があります。

template: 発行者チャネルは、HTTP GET 要求に対するレスポンスを生成するときに使用する際に、テンプレート項目の値をテンプレートドキュメントの名前として扱います。

<item name="template"> が購読者チャネルで <url-query> 要素の子として表示されると、HTTP GET 要求に応答するときに使用する際に、発行者チャネルの Web サーバにテンプレートドキュメントの名前を指定するために、値が URL クエリデータに配置されます。

responder-dn: 発行者チャネルでは、eDirectory オブジェクトの DN として HTTP POST データの responder-dn 項目の値が使用されます。これに対して、HTTP POST データで提供されたパスワードが検証されます。

Web サーバは、responder-dn 値およびパスワード値が含まれていないすべての HTTP POST 要求を拒否します。また、HTTP POST データに protected-data 項目が含まれていない場合、要求は拒否されます。

購読者チャネルは、<url-query> 要素の下に 1 つ以上の <item name="responder-dn" protect="yes"> 要素を提供します。responder-dn 項目はユーザ認証に使用されるため、これらの項目は保護されている必要があります。

password: HTTP POST データを経由して、発行者チャネルの Web サーバに提供されます。この項目のコンテンツは、POST データの responder-dn 項目によって指定された eDirectory オブジェクトに対して検証されるパスワードです。パスワード項目は通常、HTTP POST 要求の生成に使用される HTML 形式で入力されます。

例 :

```
<INPUT TYPE= "password" NAME="password" SIZE="20" MAXLENGTH="40"/>
```

response-template: HTTP POST データを経由して、Web サーバに提供されます。POST へのレスポンスとして使用される Web ページの生成に使用されます。response-template 項目は通常、HTTP POST 要求を生成するために使用される、HTML 形式の非表示の INPUT 要素を使用して指定されます。

例 :

```
<INPUT TYPE="hidden" NAME="response-template" VALUE="post_form.xml"/>
```

response-stylesheet: HTTP POST データを経由して、Web サーバに提供されます。POST へのレスポンスとして使用される Web ページの生成に使用されます。response-stylesheet 項目は通常、HTTP POST 要求を生成するために使用される、HTML 形式の非表示の INPUT 要素を使用して指定されます。

例 :

```
<INPUT TYPE="hidden" NAME="response-stylesheet"
VALUE="process_template.xsl"/>
```

auth-template: HTTP POST データを経由して、Web サーバに提供されます。ユーザの認証が失敗した場合、POST へのレスポンスとして使用される Web ページの生成に使用されます。auth-template 項目は通常、HTTP POST 要求を生成するために使用される、HTML 形式の非表示の INPUT 要素を使用して指定されます。

例 :

```
<INPUT TYPE="hidden" NAME="auth-template" VALUE="auth_response.xml"/>
```

auth-stylesheet: HTTP POST データを経由して、Web サーバに提供されます。ユーザの認証が失敗した場合、POST へのレスポンスとして使用される Web ページの生成に使用されます。auth-template 項目は通常、HTTP POST 要求を生成するために使用される、HTML 形式の非表示の INPUT 要素を使用して指定されます。

例 :

```
<INPUT TYPE="hidden" NAME="auth-stylesheet"
VALUE="process_template.xsl"/>
```

protected-data: protected-data 項目には、購読者チャネルによって構成された暗号化データが含まれています。購読者チャネルでは、保護されたデータ項目は自動入力されます。

発行者チャネルでは、protected-data 項目は HTTP GET 要求の URL クエリ文字列から取得されます。また、HTTP POST 要求の POST データからも取得されます。

通常保護されたデータ項目は、HTTP GET 要求から Web ページに渡されます。この Web ページは、HTTP GET へのレスポンスを構成するために使用されるテンプレート内の置換トークンを経由し、HTTP POST を生成するために使用されます。

例 :

```
<INPUT TYPE="hidden" NAME="protected-data" VALUE="$protected-data$"/>
```

D.2.3 <url-data>

<url-data> 要素は、購読者チャネルの <message> 要素の下にある <replacement-data> 要素の子です。この要素には、URL を構成するために使用される <item> 要素、および電子メールメッセージの作成で使用するテンプレートに入力される関連データ項目が含まれています。また、<url-query> 要素も含まれています。

手動タスクサービスドライバで使用する場合、URL は次の 5 つのパートから構成されます。

1. http、https、または ftp などのスキーム。
2. www.novell.com または 192.168.0.1 などのホスト。
3. ポート番号。コロンの後に 10 進数の整数を続けます。たとえば、:80 または :8180 です。
4. ファイルまたはリソースの識別子です。通常はファイル名であり、パス情報を含めることができます。たとえば、stylesheets/process_template.xsl です。
5. クエリ文字列。これは、& 文字で区切られた name-value ペアのコレクションです。たとえば、template=form_template.xml&protected-data=AabABJKEL= です。

<url-data> の下の事前定義された <item> 名

次のいずれかでない場合、<url-data> 要素の下の <item> 要素は無視されます。すべての要素がオプションです。

file: URL のファイル部分を指定します。発行者チャネルの Web サーバで使用されている場合、URL に対して返される最初の HTML ページを構成するために使用するスタイルシートがファイル項目によって指定されます。発行者チャネルの Web サーバ以外のサーバを使用している場合、ファイル項目によって、URL が参照するリソースの名前が指定されます。

ファイル項目が表示されない場合、URl ファイル部分のデフォルトは process_template.xsl になります。

scheme: <url-data> 要素の下にあるオプション項目です。この項目が存在する場合、(http または ftp などの)URL のスキーム部分が指定されます。スキーム項目は通常、URL が発行者の Web サーバ以外のサーバを指す場合のみ使用されます。

スキーム項目が表示されない場合、発行者チャネルの Web サーバの設定に応じて、URL スキームのデフォルトは http または https いずれかになります。

host: <url-data> 要素の下にあるオプション項目です。この項目が存在する場合、URL のホスト部分が指定されます。ホスト項目は通常、URL が発行者の Web サーバ以外のサーバを指す場合のみ使用されます。

ホスト項目が表示されない場合、URL ホストのデフォルトは、手動タスクサービスドライバが実行されているサーバの IP アドレス (つまり、発行者チャネルの Web サーバの IP アドレス) になります。

port: <url-data> 要素の下にあるオプション項目です。この項目が存在する場合、URL のポート部分が指定されます。ポート項目は通常、URL が発行者の Web サーバ以外のサーバを指す場合のみ使用されます。

ポート項目が表示されない場合、URL ポートのデフォルトは発行者チャネルの Web サーバが実行されているポートになります。

D.2.4 <url-query>

<url-query> 要素は、<url-data> 要素の子です。この要素には、電子メールメッセージで使用される URL のクエリ部分を構成するための <item> 要素が含まれています。

<url-query> 要素の子として表示される各項目は、name=“value” という形式名のクエリ文字列に配置されます。ここでは、name は <item> 要素の name 属性の値であり、値は <item> 要素の文字列コンテンツです。

<url-query> の下に表示される Item 要素は、「yes」の値の protect 属性を持つことができます。この場合、項目名および値は暗号化され、URL クエリ文字列で生成された name-value ペア内に配置されます。生成された値の名前は protected-data です。値は Base64 でエンコードされており、name-value ペアまたは複数値の属性のペアは暗号化されています。

データを保護すると、発行者チャネルの Web サーバに URL が送信されるときにデータを変更できません。たとえば、電子メールメッセージに応答することを承認されているユーザのみが eDirectory データを変更できるようにするために、responder-dn データ項目を保護する必要があります。

生成された URL が発行者チャネルの Web サーバで使用される場合、<url-query> 要素には、少なくとも 1 つの <item name=“responder-dn” protect=“yes”> 要素が含まれている必要があります。それ以外の場合、Web サーバは HTTP POST 要求を拒否します。

手動タスクサービスドライバ:自動置換データ項目

E

手動タスクサービスドライバは、特定の置換データ項目の要素を自動的に提供します。この節では、これらのデータ項目について説明します。

E.1 購読者チャネルの自動置換データ

購読者チャネルによって処理されているときに、次のデータ項目が replacement-data ドキュメントに自動的に追加されます。

association: <mail> 要素に <association> 要素の子がある場合、または購読者が <add-association> 要素を返した場合、replacement-data ドキュメントに <item name="association"> 要素が追加されます。<item> 要素のコンテンツは、処理される電子メールメッセージに関連付けられた eDirectory オブジェクトの関連付けの値です。関連付けの値は eDirectory オブジェクトには書き込まれない場合があります。したがって、関連付けの値はクエリには使用できません。

url: <item> 要素のコンテンツは、電子メールメッセージで使用される完全な URL です。購読者チャネルでは、<url-data> 要素の下にある次の項目から url 項目が作成されます。スキーム、ホスト、ポート、ファイル、および <url-query> 要素の下の項目。スキーム、ホスト、またはポートが見つからない場合、デフォルト値が使用されます。デフォルト値は、発行者チャネルの Web サーバの設定で決まります。

url-base: <item> 要素のコンテンツは、リソースの識別子 (file) およびクエリ文字列を含まない、生成された URL の一部です。

url-query: <item> 要素のコンテンツは、<url-query> 要素の下の <item> 要素から生成された URL クエリ文字列です。

url-file: <item> 要素のコンテンツは、URL のリソース識別子です。

protected-data: <item> 要素のコンテンツは、<url-query> 要素の下の <item> 要素から取得した、暗号化形式の name-value ペアです。データ値を保護するために、protect 属性が「yes」に設定されている <item> 要素のみが追加されます。保護されたデータの詳細については、299 ページの付録 D「手動タスクサービスドライバ : 置換データ」の「データのセキュリティ」を参照してください。

E.2 発行者チャネルの自動置換データ

発行者チャネルの Web サーバによって処理されているときに、次のデータ項目が replacement-data ドキュメントに自動的に追加されます。

post-status: HTTP POST 要求の処理中に、発行者チャネルの Web サーバによって、<item name="post-status"> 要素が作成され、replacement-data ドキュメントに追加されます。Web サーバへの HTTP POST 要求は、XDS ドキュメントを Identity Manager に送信するための要求です。Identity Manager は、XDS 送信の結果としてステータスドキュメントを返します。<item name="post-status"> 要素のコンテンツは、Identity Manager への送信の結果として、Identity Manager によって返された、<status> 要素のレベル属性の値です。

通常 post-status 項目は、HTTP POST 要求の結果として返される Web ページの構成に使用されます。

post-status-message: HTTP POST 要求の処理中に、発行者チャネルの Web サーバによって、<item name="post-status-message"> 要素が作成され、replacement-data ドキュメントに追加されます。Web サーバへの HTTP POST 要求は、XDS ドキュメントを Identity Manager に送信するための要求です。Identity Manager は、XDS 送信の結果としてステータスドキュメントを返します。<item name="post-status-message"> 要素のコンテンツは、Identity Manager への送信の結果として、Identity Manager によって返された、<status> 要素のコンテンツです。Identity Manager によって返された <status> 要素にコンテンツがある場合のみ、post-status-message 項目が作成されます。

post-status-message 項目は通常、HTTP POST 要求の結果として返される Web ページの構成に使用されます。

url: HTTP GET および HTTP POST 要求の処理中に、発行者チャネルの Web サーバによって、<item name="url"> 要素が作成され、replacement-data ドキュメントに追加されます。<item> 要素は、replacement-data ドキュメントを使用してドキュメントを作成する前に追加されます。Web サーバの設定によって、URL スキーム、ホスト、およびポートが決定されます。

url-base: HTTP GET および HTTP POST 要求の処理中に、発行者チャネルの Web サーバによって、<item name="url-base"> が作成され、replacement-data ドキュメントに追加されます。<item> 要素は、replacement-data ドキュメントを使用してドキュメントを作成する前に追加されます。発行者チャネル上の url-base の <item> 要素のコンテンツは、url の <item> 要素と同じです。

手動タスクサービスドライバ:テンプレートのアクション要素について

F

アクション要素は、シンプルなロジック制御、または HTML 形式の HTML 要素を作成するために使用されるテンプレートドキュメントの namespace-qualified 要素です。要素を修飾するために使用されている名前スペースは、http://www.novell.com/dirxml/manualtask/form にあります。このドキュメントおよび手動タスクサービスドライバで提供されているサンプル テンプレートでは、フォームでプレフィックスが使用されています。

この節で特に説明されていないアクション要素は、(スタイルシートがカスタマイズされない限り) テンプレート処理のスタイルシートによって出力ドキュメントから除かれます。この動作では、たとえば、プレーンテキストの電子メールメッセージのデータを指定するために form:text 要素を使用し、テンプレートを有効な XML にすることができます。

F.1 <form:input>

1 つ以上の置換データ項目があるかどうかに基づいて、1 つ以上の HTML INPUT 要素を生成するために <form:input> 要素が使用されます。作成された INPUT 要素の数は、<form:input> 要素の名前属性によって指定された名前を持つ置換データ項目の数に対応しています。

属性

Name: INPUT 要素を作成するために使用される置換データ項目の名前を指定します。作成された INPUT 要素の名前属性の値として、属性値が使用されます。

type または **TYPE:** 作成された INPUT 要素のタイプ属性の値を指定します。

value: 値属性の値が「yes」と同等である場合、値が置換データ項目の文字列値である、作成された INPUT 要素に値属性が追加されます。値属性の値が「yes」以外である場合、作成された INPUT 要素のコンテンツが置換データ項目の文字列値に設定されます。

例

```
<form:input name="responder-dn" TYPE="hidden" value="yes"/>
```

次のような INPUT 要素を 1 つ以上作成します

```
<INPUT name="responder-dn" TYPE="hidden" value="\PERIN-
TAO\novell\phb"/>
```

F.2 <form:if-item-exists>

条件付きで出力ドキュメントにデータを挿入するには、<form:if-item-exists> 要素が使用されます。<form:if-item-exists> のコンテンツは、指定した項目が置換データに表示される場合のみ処理されます。

属性

Name: 置換データ項目の名前を指定します。1 つ以上の置換データ項目の例が存在する場合、<form:if-item-exists> 要素のコンテンツが処理されます。

例

```
<form:if-item-exists name="post-status-message"> <tr> <td> Status
message was:$post-status-message$ </td> </tr> </form:if-item-exists>
```

この例では、post-status-message という名前の置換データ項目がある場合のみ、行が HTML テーブルに挿入されます。

F.3 <form:if-multiple-items>

form:if-multiple-items 要素は、条件付きで出力ドキュメントにデータを挿入するために使用されます。form:if-multiple-items のコンテンツは、指定した項目が置換データに複数回表示される場合のみ処理されます。

属性

name: 置換データ項目の名前を指定します。置換データ項目の複数の例が存在する場合、form:if-multiple-items のコンテンツが処理されます。

例

```
<form:if-multiple-items name="responder-dn"> <form:menu
name="responder-dn"/> </form:if-multiple-items>
```

この例では、responder-dn という名前を持つ複数の置換データ項目がある場合、HTML SELECT 要素 (<form:menu> を参照) が作成されます。

F.4 <form:if-single-item>

form:if-single-item 要素は、条件付きで出力ドキュメントにデータを挿入するために使用されます。form:if- single -item のコンテンツは、指定した項目が置換データに 1 回だけ表示される場合のみ処理されます。

属性

name: 置換データ項目の名前を指定します。名前付き項目が置換データに 1 回だけ表示される場合、form:if-single-item コンテンツが処理されます。

例

```
<form:if-single-item name="responder-dn"> <input TYPE="hidden"
name="responder-dn" value="$responder-dn$"/> $responder-dn$ </form:if-
single-item>
```

この例では、「responder-dn」という名前の置換データ項目が置換データに 1 つだけある場合に、HTML INPUT 要素およびいくつかの置換テキストが出力ドキュメントに挿入されます。

F.5 <form:menu>

form:menu 要素は、1 つ以上の OPTION 要素の子を持つ HTML SELECT 要素を生成するために使用されます。最初の OPTION 要素の子には、選択したことを示す確認マークが付きます。

属性

name: 置換データ項目の名前を指定します。名前付き項目が置換データに表示された場合、HTML SELECT 要素が出力ドキュメントで作成されます。置換データ内の置換データ項目の各インスタンスで、SELECT 要素の子として HTML OPTION 要素が作成されます。

例

```
<form:menu name="responder-dn"/>
```

この例では、次のような HTML 要素が作成されます。

```
<SELECT name="responder-dn"> <OPTION selected>\PERIN-TAO\big-org\php</
OPTION> <OPTION>\PERIN-TAO\big-org\carol</OPTION> </SELECT>
```

手動タスクサービスドライバ :<mail> 要素について

G

<mail> 要素およびそのコンテンツについては、この節で詳しく説明しています。属性が一覧表示されていない要素の場合、属性が定義されていません。

G.1 <mail>

<mail> 要素およびそのコンテンツでは、SMTP メッセージを構成するために必要なデータが記述されます。

<mail> 属性

src-dn: 電子メールをトリガする、eDirectory オブジェクトの DN 値が含まれています。オブジェクトのデータが、発行者チャネルの Web サーバを経由して電子メールへのレスポンスで変更される場合に必要です。

G.2 <to>

<to> 要素は <mail> 要素の子です。1 つ以上の <to> 要素には、SMTP メッセージの主な受信者の電子メールアドレスが含まれています。少なくとも 1 つの <to> 要素が必要です。各 <to> 要素には、電子メールアドレスが 1 つだけ含まれている必要があります。

G.3 <cc>

<cc> 要素は <mail> 要素の子です。ゼロ以上の <cc> 要素には、SMTP メッセージでの CC の受信者の電子メールアドレスが含まれています。<cc> 要素は必須ではありません。各 <cc> 要素には、電子メールアドレスが 1 つだけ含まれている必要があります。

G.4 <bcc>

<bcc> 要素は <mail> 要素の子です。ゼロ以上の <bcc> 要素には、SMTP メッセージでの BCC の受信者の電子メールアドレスが含まれています。<bcc> 要素は必須ではありません。各 <bcc> 要素には、電子メールアドレスが 1 つだけ含まれている必要があります。

G.5 <from>

<from> 要素は <mail> 要素の子です。<from> 要素には、電子メールの送信者の電子メールアドレスが含まれています。<from> 要素は必須ではありません。<from> 要素がない場合、手動タスクサービスドライバパラメータの一部として提供されたアドレスがデフォルト値になります。

G.6 <reply-to>

<reply-to> 要素は <mail> 要素の子です。<reply-to> 要素には、SMTP メッセージへ返信する送信先エンティティの電子メールアドレスが含まれています。<reply-to> 要素は必須ではありません。

G.7 <subject>

<subject> 要素は <mail> 要素の子です。文字列のコンテンツは、SMTP の件名フィールドを設定するために使用されます。<subject> 要素は必須ではありませんが、使用することをお勧めします。

G.8 <message>

<message> 要素は <mail> 要素の子です。この要素のコンテンツは、SMTP メッセージのメッセージ本文を作成するために使用されます。少なくとも 1 つの <message> 要素が必要です。メッセージ本文を作成するときに (プレーンテキストと HTML、または英語とその他の言語などの)SMTP メッセージの表示方法を選択できるようにする場合、複数の <message> 要素を提供できます。

<message> 属性

mime-type: オプションで、<message> 要素によって構成されたメッセージ本文の MIME タイプを指定します (テキスト / プレーンまたはテキスト /html など)。mime-type 属性がない場合、ドライバは MIME タイプを自動的に検出しようとします。

電子メールクライアントは、最適な表示方法を選択するために SMTP メッセージに複数の表示方法が設定されている場合に、MIME タイプを使用できます。

language: オプションで、<message> 要素によって構成されたメッセージ本文の言語を指定します。値は、SMTP の仕様に従っている必要があります。言語属性がない場合のデフォルト値はありません。

電子メールのクライアントは、最適な表示方法を選択するために SMTP メッセージに複数の表示方法が提供されている場合に、言語仕様を使用できます。

G.9 <stylesheet>

<stylesheet> 要素は、<message> 要素の子です。<stylesheet> 要素のコンテンツは、メッセージ本文の作成に使用される XSLT スタイルシートの名前です。<stylesheet> 要素がない場合、スタイルシートとして process_template.xsl が使用されます。

G.10 <template>

<template> 要素は、<message> 要素の子です。<template> 要素のコンテンツは、メッセージ本文の作成に使用される XML ドキュメントの名前です。<template> 要素がない場合、メッセージ本文を構成するためのメッセージのスタイルシートによって、置換データのドキュメントが処理されます。

G.11 <filename>

<filename> 要素は <attachment> 要素の子です。<filename> 要素のコンテンツはファイル名です。ファイル名を使用して、作成された添付ファイルにファイル名を割り当てます。

G.12 <replacement-data>

<replacement-data> 要素は、<message> 要素の子です。この要素のコンテンツは、メッセージのテンプレートを処理するスタイルシートに対するパラメータとして使用されます。またはテンプレートがない場合は、メッセージのスタイルシートによって直接処理されます。<replacement-data> 要素のコンテンツについては、299 ページの付録 D「手動タスクサービスドライバ : 置換データ」および 305 ページの付録 E「手動タスクサービスドライバ : 自動置換データ項目」で説明しています。

G.13 <resource>

<resource> 要素は、<message> 要素の子です。この要素のコンテンツは、メッセージ本文の SMTP メッセージのリソースに組み込まれるファイルの名前として扱われます。たとえば、HTML メッセージ本文の .css スタイルシートは、リソースとして提供できます。

<resource> 属性

cid: メッセージ本文の URL のリソースを参照するために使用されるコンテンツ ID を指定します。たとえば、.css スタイルシートがリソースにある場合、cid 値は css-1 になります。HTML メッセージ本文では、次の要素を使用して .css スタイルシートを参照できます。

```
<link href="cid:css-1" rel="style sheet" type="text/css">
```

G.14 <attachment>

<attachment> 要素は <mail> 要素の子です。<message> と同じコンテンツを持つことができます。または、コンテンツとしてファイル名を持つことができます。ゼロ以上の <attachment> 要素は、<mail> 要素の子として表示されます。

<attachment> 属性

mime-type: オプションで、アタッチメントの MIME タイプを指定します。mime-type 属性がない場合、ドライバは MIME タイプを自動的に検出しようとします。

language: オプションで、添付ファイルの言語を指定します。言語属性がない場合のデフォルト値はありません。

手動タスクサービスドライバ:新しい従業員のデータフローのシナリオ

H

この節では、新しい従業員を雇用したときに、電子メールメッセージがこの従業員のマネージャに送信されるという場合のデータフローについて、ステップごとに説明していきます。マネージャは、電子メールメッセージによって、そのメールメッセージ内の URL を使用してこの従業員の部屋番号の値を入力するように要求されます。

このシナリオにおける手動タスクサービスドライバの設定内容は、次のとおりです。

H.1 購読者チャネルの設定

フィルタ

クラス **:** ユーザ

属性 **:** 名前、マネージャ、名字

ポリシー

作成ポリシー **:** 名前、マネージャ、および名字の属性がが必要です。

コマンド変換ポリシー **:** <add> を <mail> 要素に変換します。

H.2 発行者チャネルの設定

フィルタ

クラス **:** ユーザ

属性 **:** roomNumber

ポリシー

ありません。

H.3 データフローの説明

次のリストでは、プロセスを介して送信される最も重要なデータ項目は、responder-dn および association です。responder-dn 項目は、Web サーバを介してデータを入力するユーザを認証するために使用されます。association 項目により、データが変更される eDirectory オブジェクトが識別されます。

1. 会社が新しい従業員を雇用しました。会社の人事 (HR) システムに新しい従業員のデータが入力されます。
2. 人事システムの Identity Manager ドライバにより、eDirectory に新しいユーザオブジェクトが作成されます。ユーザ属性には、名前、名字、およびマネージャが含まれています。

3. 新しいユーザオブジェクトに関する次の <add> イベントが、手動タスクサービスドライバの購読者チャネルに送信されます。

```
<nds dtdversion="1.1" ndsversion="8.6"> <input> <add class-
name="User" src-dn="\PERIN-TAO\novell\Provo\Joe" src-entry-
id="281002" timestamp="1023314433#2"> <add-attr attr-
name="Surname"> <value type="string">the Intern</value> <add-attr>
<add-attr attr-name="Given Name"> <value type="string">Joe</value>
<add-attr> <add-attr attr-name="manager"> <value type="dn">\PERIN-
TAO\novell\Provo\phb</value> <add-attr> </add> </input> </nds>
```

   a. 購読者コマンド変換ポリシーでは、マネージャ DN 値を使用して、マネージャの電子メールアドレスおよびマネージャのアシスタントの DN に対して eDirectory にクエリが発行されます。

   b. マネージャにアシスタントがいる場合、アシスタントの電子メールアドレスに対して、購読者コマンド変換によって eDirectory にクエリが発行されます。

   c. 購読者コマンド変換によって <mail> 要素が作成され、<add> コマンド要素が <mail> 要素に置換されます。次の例では、置換データ項目を太字で示しています。

```
<nds dtdversion="1.1" ndsversion="8.6"> <input> <mail src-
dn="\PERIN-TAO\novell\Provo\Joe"> <to>phb@company.com</to>
<cc>carol@company.com</cc> <bcc>HR@company.com</bcc> <reply-
to>HR@company.com</reply-to> <subject>Room Assignment Needed
for:Joe the Intern</subject> <message mime-type="text/html">
<stylesheet>process_template.xsl</stylesheet>
<template>html_msg_template.xml</template> <replacement-data>
<item name="manager">JStanley</item>           <item
name="given-name">Joe</item>          <item name="surname">the
Intern</item> <url-data> <item
name="file">process_template.xsl</item> <url-query>   <item
name="template">form_template.xml</item>               <item
name="responder-dn" protect="yes">\PERIN-TAO\novell\Provo\phb</
item>               <item name="responder-dn"
protect="yes">\PERIN-TAO\novell\Provo\carol</item>
<item name="subject-name">Joe the Intern</item> </url-query> </
url-data> </replacement-data> <resource cid="css-
1">novdocmain.css</resource> </message> </mail> </input> </nds>
```

   d. 手動タスクサービスドライバの購読者は、Nsure™ Identity Manager から <mail> 要素を受信します。

   e. <mail> 要素には src-dn 属性があるため、購読者によって関連付けの値が生成されます。

   f. 電子メールメッセージの作成に使用するために、購読者によって <mail> 要素のデータから置換データのドキュメントが作成されます。URL のクエリ部分には、さまざまなデータ項目があります (「?」の後に続く太字の URL の部分)。発行者チャネルの Web サーバでは、HTTP GET 要求として URL が Web サーバに送信されるときに、これらのデータ項目が使用されます。

```
<replacement-data> <item name="manager">JStanley</item> <item
```

```
name="given-name">Joe</item> <item name="surname">the Intern</
item> <item name="template">form_template.xml</item> <item
name="responder-dn">\PERIN-TAO\novell\Provo\phb</item> <item
name="responder-dn">\PERIN-TAO\novell\Provo\carol</item> <item
name="subject-name">Joe the Intern</item> <item
name="association">1671b2:ee4246a561:-7fff:192.168.0.1</item>
<item name="url-base">https://192.168.0.1:8180</item> <item
name="url-file">process_template.xsl</item> <item
name="protected-data">
rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAARbAA
1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFMAAlw
YXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ4cH
VyAAJbQqzzF/gGCFTgAgAAeHAAAAAPMA0ECEIBRohGPjxEAgEKdXEAfgAEAAAA
uMSFqzHXwtMx8DkRCzkK1O46sEz1u51o3MDvHn+3+fE6SphHr3Hgjli4Jp3rUk
H7y6dXvcu7iq21Vs+9o6iZVzljTIJX/jjRrVZlR5JOuRNhk8JHFZ8FhgsmiIAH
/Fs61k4WmyEcmYfWmfqfBVeThr3Avwcim6ranS5Mm2U5i9Z/DBR13pIAobMpWY
kMaz4+G9e6oovBsiPdp6jSPzbFxcgALI2AMBh4hf9jnx7zOU9Uvd9qXtaE2rR0
AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item> <item name="url-
query">template=form_template.xml&amp;responder-dn=%5CPERIN-
TAO%5Cnovell%5Cprovo%5Cphb&amp;responder-dn=%5CPERIN-
TAO%5Cnovell%5Cprovo%5Ccarol&amp;subject-
name=Joe+the+Intern&amp;association=1671b2%3Aee4246a561%3A-
7fff%3A192.168.0.1&amp;protected-
data=rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAA
RbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB%2BAAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB%2B
AAJ4cHVyAAJbQqzzF%2FgGCFTgAgAAeHAAAAAPMA0ECEIBRohGPjxEAgEKdXEAf
gAEAAAAuMSFqzHXwtMx8DkRCzkK1O46sEz1u51o3MDvHn%2B3%2BfE6SphHr3Hg
jli4Jp3rUkH7y6dXvcu7iq21Vs%2B9o6iZVzljTIJX%2FjjRrVZlR5JouRNhk8J
HFZ8FhgsmiIAH%2FFs61k4WmyEcmYfWmfqfBVeThr3Avwcim6ranS5Mm2U5i9Z%
2FDBR13pIAobMpWYkMaz4%2BG9e6oovBsiPdp6jSPzbFxcgALI2AMBh4hf9jnx7
zOU9Uvd9qXtaE2rR0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item> <item
name="url"> https://192.168.0.1:8180/
process_template.xsl?template=form_template.xml&amp;responder-
dn=%5CPERIN-TAO%5Cnovell%5CProvo%5Cphb&amp;responder-
dn=%5CPERIN-TAO%5Cnovell%5Cprovo%5Ccarol&amp;subject-
name=Joe+the+Intern&amp;association=1671b2%3Aee4246a561%3A-
7fff%3A192.168.0.1&amp;protected-
data=rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAA
RbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB%2BAAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB%2B
AAJ4cHVyAAJbQqzzF%2FgGCFTgAgAAeHAAAAAPMA0ECEIBRohGPjxEAgEKdXEAf
gAEAAAAuMSFqzHXwtMx8DkRCzkK1O46sEz1u51o3MDvHn%2B3%2BfE6SphHr3Hg
jli4Jp3rUkH7y6dXvcu7iq21Vs%2B9o6iZVzljTIJX%2FjjRrVZlR5JouRNhk8J
HFZ8FhgsmiIAH%2FFs61k4WmyEcmYfWmfqfBVeThr3Avwcim6ranS5Mm2U5i9Z%
2FDBR13pIAobMpWYkMaz4%2BG9e6oovBsiPdp6jSPzbFxcgALI2AMBh4hf9jnx7
zOU9Uvd9qXtaE2rR0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREV </item> </
replacement-data>
```

g. 購読者は、html_msg_template.xml with process_template.xsl を処理します。置換データドキュメントはパラメータとしてスタイルシートに渡されます。html_msg_template.xml ドキュメントが続きます。置換トークンは太字で示してい

ます。置換トークンは、置換データのドキュメント内の対応する <item> 要素の値によって置換されます。

```
<html xmlns:form="http://www.novell.com/dirxml/manualtask/
form"> <head> </head> <body> <link href="cid:css-1" rel="style
sheet" type="text/css"/> <p> Dear $manager$, </p> <p> This
message is to inform you that your new employee <b>$given-name$
$surname$</b> has been hired.</p> <p> Please assign a room
number for this individual.Click <a href="$url$">Here</a> to do
this.</p> <p> Thank you,<br/> HR<br/> HR Department </p> </
body> </html>
```

生成された電子メールドキュメントが続きます。置換トークンは、置換データのドキュメント内の対応する <item> 要素の値によって置換されました。

```
<html> <head> <META http-equiv="Content-Type" content="text/
html; charset=UTF-8"> </head> <body> <link href="cid:css-1"
rel="style sheet" type="text/css"> <p> Dear J Stanley, </p> <p>
This message is to inform you that your new employee <b>Joe the
Intern</b> has been hired.</p> <p> Please assign a room number
for this individual.Click <a href="https://192.168.0.1:8180/
process_template.xsl?template=form_template.xml&responder-
dn=%5CPERIN-TAO%5Cnovell%5CProvo%5Cphb&responder-dn=%5CPERIN-
TAO%5Cnovell%5CProvo%5Ccarol&subject-
name=Joe+the+Intern&association=45f0e3%3Aee45e07709%3A-
7fff%3A192.168.0.1&protected-
data=rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACAA
RbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB%2BAAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB%2B
AAJ4cHVyAAJbQqzzF%2FgGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG%2BO3BAgEKdXE
AfgAEAAAAuMU%2FSoFRkebvh2d5SqalF91ttjRY5lyyW5%2B%2FFIfOuDdYikYi
DbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY%2Bi4VoVjUSXS3a8fiXB8moM
dPtLJ%2FGyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL
%2FeFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlP
S0iWzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT">Here</a> to
do this.</p> <p> Thank you,<br> HR<br> HR Department </p> </
body> </html>
```

h. SMTP 電子メールメッセージがマネージャおよびマネージャのアシスタントに送信されます。

i. 購読者によって、<status> 要素および <add-association> 要素が含まれている XML ドキュメントが Identity Manager に返されます。

4. マネージャが電子メールメッセージを開き、［ここをクリック］リンクをクリックします。

5. マネージャの Web ブラウザによって、HTTP GET 要求として発行者チャネルの Web サーバに URL が送信されます。

   a. Web サーバは、次の置換データのドキュメントを作成します。多くのデータ項目は、URL のクエリ部分からのものです。例外は、自動的に生成された項目の url および url-base です。

```
<replacement-data> <item name="association">45f0e3:ee45e07709:-
7fff:192.168.0.1</item> <item name="protected-
data">rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACA
ARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFM
AAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ
4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FifOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item> <item
name="template">form_template.xml</item> <item name="responder-
dn">\PERIN-TAO\novell\Provo\phb</item> <item name="responder-
dn">\PERIN-TAO\novell\Provo\carol</item> <item name="subject-
name">Joe the Intern</item> <item name="url-base">https://
192.168.0.1:8180</item> <item name="url">https://
192.168.0.1:8180</item> </replacement-data>
```

Web サーバは、process_template.xsl スタイルシートを使用して form_templates.xml ドキュメントを処理します。置換トークンおよびアクション要素は太字で示しています。データ項目が HTML POST データの一部として Web サーバに渡されるように、さまざまなデータ項目が非表示の INPUT 要素に配置されています。

また、従業員の roomNumber 属性 (存在する場合) の現在の値を取得する、$query:roomNumber$ 置換トークンがあります。

```
<html  xmlns:form="http://www.novell.com/dirxml/manualtask/
form"> <head> <title>Enter room number for $subject-name$</
title> </head> <body> <link href="novdocmain.css" rel="style
sheet" type="text/css"/> <br/><br/><br/><br/> <form
class="myform" METHOD="POST" ACTION="$url-base$/
process_template.xsl"> <table cellpadding="5" cellspacing="10"
border="1" align="center"> <tr><td> <input TYPE="hidden"
name="template" value="post_form.xml"/> <input TYPE="hidden"
name="subject-name" value="$subject-name$"/> <input
TYPE="hidden" name="association" value="$association$"/> <input
TYPE="hidden" name="response-style sheet"
value="process_template.xsl"/> <input TYPE="hidden"
name="response-template" value="post_response.xml"/> <input
TYPE="hidden" name="auth-style sheet"
value="process_template.xsl"/> <input TYPE="hidden" name="auth-
template" value="auth_response.xml"/> <input TYPE="hidden"
name="protected-data" value="$protected-data$"/> <form:if-
single-item name="responder-dn">   You are:<br/> <input
TYPE="hidden" name="responder-dn" value="$responder-dn$"/>
$responder-dn$  </form:if-single-item>          <form:if-
multiple-items name="responder-dn"> Indicate your identity:<br/
>  <form:menu name="responder-dn"/>         </form:if-multiple-
items> </td></tr> <tr><td> Enter your password:<br/><input
name="password" TYPE="password" SIZE="20" MAXLENGTH="40"/> </
td></tr> <tr><td> Enter room number for $subject-name$:<br/>
```

```
<input TYPE="text" NAME="room-number" SIZE="20" MAXLENGTH="20"
value="$query:roomNumber$"/> </td></tr> <tr><td> <input
TYPE="submit" value="Submit"/> <input TYPE="reset"
value="Clear"/> </td></tr> </table> </form> </body> </html>
```

結果は次の HTML ページのとおりです。

```
<html> <head> <META http-equiv="Content-Type" content="text/
html; charset=UTF-8"> <title>Enter room number for Joe the
Intern</title> </head> <body> <link href="novdocmain.css"
rel="style sheet" type="text/css"> <br><br><br><br> <form
class="myform" METHOD="POST" ACTION="https://192.168.0.1:8180/
process_template.xsl"> <table cellpadding="5" cellspacing="10"
border="1" align="center"> <tr> <td> <input TYPE="hidden"
name="template" value="post_form.xml"> <input TYPE="hidden"
name="subject-name" value="Joe the Intern"> <input
TYPE="hidden" name="association" value="45f0e3:ee45e07709:-
7fff:192.168.0.1"> <input TYPE="hidden" name="response-style
sheet" value="process_template.xsl"> <input TYPE="hidden"
name="response-template" value="post_response.xml"> <input
TYPE="hidden" name="auth-style sheet"
value="process_template.xsl"> <input TYPE="hidden" name="auth-
template" value="auth_response.xml"> <input TYPE="hidden"
name="protected-data"
value="rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHAC
AARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAF
MAAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AA
J4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FIfOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT"> Indicate your
identity:<br> <SELECT name="responder-dn"> <OPTION
selected>\PERIN-TAO\novell\Provo\phb</OPTION> <OPTION>\PERIN-
TAO\novell\Provo\carol</OPTION> </SELECT> </td> </tr> <tr> <td>
Enter your password:<br>

    <input name="password" TYPE="password" SIZE="20"
MAXLENGTH="40"> </td> </tr> <tr> <td> Enter room number for Joe
the Intern:<br> <input TYPE="text" NAME="room-number" SIZE="20"
MAXLENGTH="20" value=""> </td> </tr> <tr> <td> <input
TYPE="submit" value="Submit"> <input TYPE="reset"
value="Clear"> </td> </tr> </table> </form> </body> </html>
```

b. マネージャは Web ページのメニューから eDirectory DN を選択し、パスワードを入力し、新しい従業員の部屋番号を入力し、［送信］をクリックします。

c. Web ブラウザによって、HTTP POST 要求が Web サーバに送信されます。

d. Web サーバが、POST データから次の置換データのドキュメントを作成します。データはさまざまな非表示の <INPUT> 要素にあることに注意してください。マネージャによって入力されたデータは太字で示しています。

```
<replacement-data>   <item name="room-number">cubicle 1234</
item> <item name="template">post_form.xml</item> <item
name="response-template">post_response.xml</item> <item
name="auth-template">auth_response.xml</item> <item
name="association">45f0e3:ee45e07709:-7fff:192.168.0.1</item>
<item name="password" is-sensitive="true"><!-content suppressed
?</item> <item name="protected-
data">rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACA
ARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFM
AAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ
4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FifOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item>  <item
name="responder-dn">\PERIN-TAO\novell\Provo\phb</item> <item
name="auth-style sheet">process_template.xsl</item> <item
name="response-style sheet">process_template.xsl</item> <item
name="subject-name">Joe the Intern</item> <item name="url-
base">https://192.168.0.1:8180</item> <item name="url">https://
192.168.0.1:8180</item> </replacement-data>
```

e. Web サーバによって、responder-dn の項目の値が、保護されたデータに含まれている responder-dn 値に一致することが確認されます。値が一致しない場合、Web サーバは要求を中止します。値が一致した場合、処理が続行されます。

f. HTTP POST 要求を送信するユーザを認証するために、Web サーバによって、<check-object-password>XDS 要求が発行者チャネル上の Identity Manager に送信されます。

```
<nds dtdversion="1.0" ndsversion="8.6"> <source> <product
build="20020606_0824" instance="Manual Task Service Driver"
version="1.1a">DirXML Manual Task Service Driver</product>
<contact>Novell, Inc.</contact> </source> <input> <check-
object-password dest-dn="\PERIN-TAO\novell\Provo\phb" event-
id="chkpwd"> <password><!-- content suppressed --></password>
</check-object-password> </input> </nds>
```

g. Identity Manager によって、<status level=”success”> が返されます。Identity Manager によって成功以外が返された場合、データ項目 auth_template によって指定されたテンプレート、およびデータ項目 auth_stylesheet によって指定されたスタイルシートを使用して、POST の結果として返された Web ページが作成されます。

h. XDS ドキュメントを生成するために、Web サーバは、process_template.XSL スタイルシートを使用して post_form.xml テンプレートを処理します。置換トークンは太字で示しています。

```
<nds> <input> <modify class-name="User" src-dn="not-applicable"
event-id=”wfmod”> <association>$association$</association>
<modify-attr attr-name="roomNumber"> <remove-all-values/> <add-
value> <value>$room-number$</value> </add-value> </modify-attr>
</modify> </input> </nds>
```

i. 発行者により、作成された XDS ドキュメントが Identity Manager に送信されます。

```
<nds> <input> <modify class-name="User" src-dn="not-applicable"
event-id=”wfmod”> <association>45f0e3:ee45e07709:-
7fff:192.168.0.1</association> <modify-attr attr-
name="roomNumber"> <remove-all-values/> <add-value>
<value>cubicle 1234</value> </add-value> </modify-attr> </
modify> </input> </nds>
```

j. Identity Manager によって、結果ドキュメントが返されます。

```
<nds dtdversion="1.1" ndsversion="8.6"> <source> <product
version="2.0">Identity Manager</product> <contact>Novell,
Inc.</contact> </source> <output> <status event-id="wfmod"
level="success"></status> </output> </nds>
```

k. Web サーバによって、置換データ項目 post-status (および置換データ項目 post-status-message) が置換データのドキュメントに追加されます。追加されたデータ項目は太字で示しています。

```
<replacement-data> <item name="room-number">cubicle 1234</item>
<item name="template">post_form.xml</item> <item
name="response-template">post_response.xml</item> <item
name="auth-template">auth_response.xml</item> <item
name="association">45f0e3:ee45e07709:-7fff:192.168.0.1</item>
<item name="password" is-sensitive=”true”><!-content suppressed
?</item> <item name="protected-
data">rO0ABXNyABlqYXZheC5jcnlwdG8uU2VhbGVkT2JqZWN0PjY9psO3VHACA
ARbAA1lbmNvZGVkUGFyYW1zdAACW0JbABBlbmNyeXB0ZWRDb250ZW50cQB+AAFM
AAlwYXJhbXNBbGd0ABJMamF2YS9sYW5nL1N0cmluZztMAAdzZWFsQWxncQB+AAJ
4cHVyAAJbQqzzF/
gGCFTgAgAAeHAAAAAPMA0ECIr9Z1iG+O3BAgEKdXEAfgAEAAAAuMU/
SoFRkebvh2d5SqalF91ttjRY5lyyW5+/
FifOuDdYikYiDbOJb6607S0dPHjQzeVgu6ptIvGqaEQOEjBjDkY+i4VoVjUSXS3
a8fiXB8moMdPtLJ/
GyE8QiwbT4xbkQy48i02k99F2vGmlenRpSP6dD31kZl3dpJ0mGgq2yL/
eFaynKyqnjkHLMexcqD8WlVooaRl1k2RPk5vDYvC8o2bn22OKKbOnSRM5YlPS0i
Wzxo0JVcnVVyt0AANQQkV0ABBQQkVXaXRoTUQ1QW5kREVT</item> <item
name="responder-dn">\PERIN-TAO\novell\Provo\phb</item> <item
name="auth-style sheet">process_template.xsl</item> <item
name="response-style sheet">process_template.xsl</item> <item
```

```
name="subject-name">Joe the Intern</item> <item name="url-
base">https://192.168.0.1:8180</item> <item name="url">https://
192.168.0.1:8180</item> <status event-id="" level="success"></
status>   <item name="post-status">success</item> </
replacement-data>
```

l. Web サーバは、process_template.xsl スタイルシートを使用して post_response.xml テンプレートを処理します。置換トークンおよびアクション要素は太字で示しています。

```
<htm xmlns:form="http://www.novell.com/dirxml/manualtask/form">
<head> <title>Result of post for $subject-name$</title> </head>
<body> <link href="novdocmain.css" rel="style sheet"
type="text/css"/> <br/><br/><br/><br/> <table class="formtable"
cellpadding="5" cellspacing="20" border="1" align="center">
<tr> <td> DirXML reported status = $post-status$ </td> </tr>
<form:if-item-exists name="post-status-message"> <tr> <td>
Status message was:$post-status-message$ </td> </tr> </form:if-
item-exists> </table> </body> </html>
```

m. HTTP POST の結果として、結果の Web ページが返されます。置換データのドキュメントに <form:if-item-exists> 要素によって参照されている post-status-message がないため、表の 2 行目はありません。

```
<html> <head> <META http-equiv="Content-Type" content="text/
html; charset=UTF-8"> <title>Result of post for Joe the
Intern</title> </head> <body> <link href="novdocmain.css"
rel="style sheet" type="text/css"> <br><br><br><br> <table
class="formtable" cellpadding="5" cellspacing="20" border="1"
align="center"> <tr> <td> DirXML reported status = success </
td> </tr> </table> </body> </html>
```

手動タスクサービスドライバ:購読者チャネルのカスタム要素ハンドラ

ドライバは、Simplified Mail Transport Protocol (SMTP) 以外の方法を使用して、ユーザ通知を送信するための拡張メカニズムを提供します。たとえば、顧客が、SMTP を使用するのではなく、Messaging Application Programming Interface (MAPI) を使用して通知を送信する必要があるとします。

通知の送信に SMTP 以外のメカニズムを使用するには、ドライバの購読者チャネルで送信されるカスタム XML 要素を処理する Java クラスを記述する必要があります。

Java カスタム要素ハンドラは、com.novell.nds.dirxml.driver.manualtask.CommandHandler Java インタフェースを実装する必要があります。カスタム要素クラスの名前は、購読者の設定パラメータの［その他のハンドラ］項目で指定されます。

購読者チャネルでコマンド要素が発生した場合、ハンドラのテーブルが検索されます。コマンド要素を処理していることをレポートするハンドラが見つかると、コマンド要素がハンドラに渡されます。次にハンドラは必要な処理を実行します。

ドライバには、組み込まれたコマンド要素のハンドラが 2 つあります。<mail> 要素のハンドラ、および <add> 要素のハンドラです。

カスタムコマンド要素は、カスタムハンドラの作成者が定義します。カスタムコマンド要素の設計は、<mail> 要素から始めるのが妥当です。

カスタム要素は、<mail> 要素が作成されたのと同じ方法で、購読者チャネルのポリシーによって作成されます。

com.novell.nds.dirxml.driver.manualtask.CommandHandler のドキュメント、および多くのユーティリティとサポートクラスのドキュメントは、ドライバに付属の javadocs にあります。javadocs は、配布イメージの中では、manual_task_docs.zip というファイル名になっています。

I.1 発行者チャネルの Web サーバで使用する URL の構成

ドライバの発行者チャネルの Web サーバを安全に使用するには、ユーティリティクラスを使用して、通知メッセージに含まれる URL を構成する必要があります。com.novell.nds.dirxml.driver.manualtask.URLData はこのタスクのために設計されています。

サンプルコードは、このプロセスを説明するための SampleCommandHandler.java にあります。

I.2 スタイルシートおよびテンプレートドキュメントを使用したメッセージドキュメントの作成

SMTP ハンドラが使用するドキュメントを作成する際に、スタイルシート、テンプレートドキュメント、および置換データを組み合わせた、同じ方法を使用すると便利です。これ

を行うには、スタイルシートおよびテンプレートドキュメントを取得し、スタイルシートプロセッサをプログラム的に起動する必要があります。

サンプルコードは、このプロセスを説明するための SampleCommandHandler.java にあります。

I.3 SampleCommandHandler.java

サンプルのカスタムコマンドハンドラのソースコードは、ドライバの配布パッケージに付属しています。ソースコードは、配布イメージ内の manual_task_docs.zip ファイルにあります。

ハンドラは、com.novell.nds.dirxml.driver.manualtask.samples.SampleCommandHandler クラスに実装されています。

サンプルのハンドラは、スタイルシートおよびテンプレートを使用してドキュメントを生成し、結果のドキュメントをファイルに書き込むだけです。

I.3.1 SampleCommandHandler クラスのコンパイル

任意の Java 2 コンパイラを使用して、SampleCommandHandler クラスをコンパイルできます。Java コンパイラのクラスパスに、nxsl.jar、dirxml.jar、collections.jar、および ManualTaskServiceBase.jar を配置する必要があります。

I.3.2 SampleCommandHandler クラスの試行

ドライバの部屋番号のサンプル設定のインポートから開始します。

SampleCommandHandler クラスをコンパイルし、結果のクラスファイルを .jar ファイルに配置します。ドライバを実行しているプラットフォームに適した、DirXML の .jar ファイルディレクトリに .jar ファイルを配置します。

ドライバプロパティの Driver Parameters XML セクションにある <subscriber-options> 要素の下に、次の XML 要素を追加します。

```
<output-path display-name="Sample Output Path"></output-path>
```

ドライバパラメータを編集します。Sample Output Path という名前の項目で、SampleCommandHandler が作成されたドキュメントを記述するディレクトリにパスを配置します。［その他のハンドラ］という名前の項目で、文字列「com.novell.nds.dirxml.driver.manualtask.samples.SampleCommandHandler」を追加します。

購読者チャネルのコマンド変換ポリシーを、SampleCommandHandler.java ファイルと同じディレクトリにある CommandXform.xsl に置換します。

ユーザオブジェクトを作成し、マネージャ参照をユーザオブジェクトに追加します。マネージャが電子メールアドレス値を持っている場合、<sample> コマンド要素が購読者に送信され、SampleCommandHandler によって上記で指定した場所のファイルが記述されます。

手動タスクサービスドライバ:発行者チャネルのカスタムサーブレット

J

ドライバには拡張メカニズムがあり、その他の機能を発行者チャネルの Web サーバに追加できます。［その他のサーブレット］という名前のドライバ設定項目でサーブレットクラスの名前を指定することにより、発行者はカスタムサーブレットをロードできます。

J.1 発行者チャネルの使用

カスタムサーブレットが Identity Manager にデータを送信する必要がある場合、サーブレットはドライバの発行者チャネルを使用する必要があります。これを行うために、com.novell.nds.dirxml.driver.manualtask.ServletRegistrar および com.novell.nds.dirxml.driver.manualtask.PublisherData クラスが用意されています。サンプルコードは、このプロセスを説明するための SampleServlet.java にあります。

J.2 認証

カスタムサーブレットは、情報を送信するユーザを認証する必要があります。サンプルコードは、このプロセスを説明するための SampleServlet.java にあります。しかし、<check-object-password> 要素を使用して実行される認証のタイプでは、eDirectory™ の権利は確認されません。. ドライバオブジェクトが変更を実行する権利を持っている場合、変更を送信するユーザが権利を持っているかどうかにかかわらず、発行者チャネルで送信された変更は許可されます。

購読者チャネルのコマンドハンドラによって生成された URL を使用している場合、responder-dn データ項目が改ざんされていないことを確認するために、com.novell.nds.dirxml.driver.manualtask.URLData クラスを使用して URL を検証する必要があります。この操作の詳細については、javadocs を参照してください。

J.3 SampleServlet.java

サンプルのサーブレットのソースコードは、ドライバの配布パッケージに含まれています。ソースコードは、配布イメージ内の manualtask_driver_docs.zip ファイルにあります。

サーブレットは、com.novell.nds.dirxml.driver.manualtask.samples.SampleServlet クラスに実装されています。

サンプルのサーブレットは、.sample で終了するすべてのリソースに対して HTTP GET 要求を受諾します。HTTP URL のクエリ文字列には、dest-dn 項目、attr-name 項目、および value 項目が含まれている必要があります。

サーブレットはユーザを認証し、ドライバの発行者チャネルを経由して変更要求を Identity Manager に送信します。

J.3.1 SampleServlet クラスのコンパイル

任意の Java 2 コンパイラを使用して、SampleServlet クラスをコンパイルできます。Java コンパイラのクラスパスに、nxsl.jar、dirxml.jar、collections.jar、および ManualTaskServiceBase.jar を配置する必要があります。

J.3.2 SampleServlet クラスの試行

ドライバの部屋番号のサンプル設定のインポートから開始します。

SampleServlet クラスをコンパイルし、結果のクラスファイルを .jar ファイルに配置します。ドライバを実行しているプラットフォームに適した、DirXML の .jar ファイルディレクトリに .jar ファイルを配置します。

ドライバパラメータを編集します。［その他のサーブレット］という名前の項目で、文字列「com.novell.nds.dirxml.driver.manualtask.samples.SampleServlet」を追加します。

発行者チャネルフィルタへの電話番号の追加

次の URL をブラウザで送信します (ブラウザはドライバと同じコンピュータで実行されていると想定します)。

https:localhost:8180/1.sample?dest-dn=username.container&attr-name=Telephone%20Number&value=555-1212

username.container はツリー内のユーザの DN に置き換えてください。